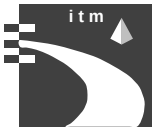
Universität Karlsruhe
Fakultät für Informatik
Institut für Telematik
76128 Karlsruhe



Netzwerk-Management und Hochgeschwindigkeits-Kommunikation

Teil XVI

Seminar SS 1997

Herausgeber:
Roland Bless
Stefan Dresler
Günter Schäfer
Claudia Schmidt
Hajo Wiltfang

Universität Karlsruhe
Institut für Telematik

Interner Bericht 18/97
ISSN 1432–7864

Zusammenfassung

Der vorliegende Interne Bericht enthält die Beiträge zum Seminar „Netzwerk-Management und Hochgeschwindigkeits-Kommunikation“, das im Sommersemester 1997 zum sechzehnten Mal stattgefunden hat.

Die Themenauswahl kann grob in folgende drei Blöcke gegliedert werden:

1. Ein Block ist der ATM-Technologie gewidmet. Im ersten Beitrag wird die *Sicherheit* der Kommunikation in ATM-Netzen untersucht und bestehende Ansätze vorgestellt. Der zweite Beitrag beschreibt die *Unterstützung für Dienstqualitäten* in ATM-Netzen.

2. Ein zweiter Block beschäftigt sich mit fortgeschrittenen Techniken im Internet. Hier werden zum einen *Routing-Mechanismen* vorgestellt, welche die Erbringung von Dienstqualitäten im Internet ermöglichen sollen, und zum anderen wird erläutert, welche Technologie zur Verfügung steht, um *Multimediale Konferenzen im Internet* abzuhalten.

3. Der dritte Block umfaßt den Themenbereich fortgeschrittene LAN-Technologien. Hier wird die „Fibre-Channel Technologie“ vorgestellt, die Übertragungsgeschwindigkeiten im Gbit/s-Bereich ermöglicht.

Abstract

This Technical Report includes student papers produced within small lessons called seminar of “Network Management and High Speed Communications”. For the sixteenth 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 three blocks:

1. One block is devoted to ATM technology. At first, *security* of communication in ATM networks is examined and existing approaches are described. Subsequently, a description of support for *quality of service in ATM networks* is given.

2. A second block deals with advanced Internet technologies. The first article shows *routing mechanisms* that should provide quality of service in the Internet. The second article describes which support currently exists in the Internet to provide *multimedia conferences*.

3. The third block deals with new and advanced LAN technologies. A technology for transmitting data in the range of Gbit/s is presented: the „Fibre Channel“.

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 sechzehnte 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 Wintersemester 1997/98 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:

Sichere Kommunikation in ATM-Netzen

Mit der zunehmenden Nutzung moderner Hochleistungsnetze auch für „nicht-akademische“ Zwecke wächst auch der Bedarf für eine Unterstützung grundlegender Sicherheitsdienste in diesen Netzen. In dem Beitrag „Sichere Kommunikation in ATM-Netzen“ werden die an ATM-Netze zu stellenden Sicherheitsanforderungen motiviert und drei aktuelle Ansätze auf diesem Gebiet miteinander verglichen.

Unterstützung für Dienstqualitäten in ATM-Netzwerken

Fortgeschrittene Anwendungen (beispielsweise Telemedizin, Telerobotik, computerunterstütztes Gruppenarbeiten, Video-Konferenzen, usw.) benötigen sehr unterschiedliche Kommunikationsdienste. Ein diensteintegrierendes Netzwerk, wie etwa Breitband-ISDN (B-ISDN), muß daher auch in der Lage sein, diese verschiedenen Dienste geeignet zu unterstützen. Für audio-visuelle Daten werden insbesondere Dienste benötigt, die eine gewisse Dienstqualität (Quality of Service – QoS) garantieren. Durch Dienstqualitätsparameter wie etwa Durchsatz, Ende-zu-Ende Verzögerung, Verzögerungsschwankung (Delay-Jitter) oder Zuverlässigkeit, werden die Anforderungen an einen Kommunikationsdienst ausgedrückt, der durch geeignete Mechanismen die Einhaltung der Vorgaben des Dienstnutzers sicherstellen muß. Daher wurden für ATM-basierte Netzwerke (ATM ist die Basistechnologie für B-ISDN) verschiedene Dienstkategorien und Dienstqualitätsparameter definiert, die eine entsprechende Unterstützung ermöglichen sollen. Dieser Beitrag zeigt den Umfang auf, in dem Dienstqualitäten derzeit in ATM-Netzen unterstützt werden und welche Mechanismen dazu vorgesehen sind.

Qualitätsbasiertes Routing im Internet

Anfang 1997 formte sich in der IETF (Internet Engineering Task Force) eine neue Arbeitsgruppe „QoS Routing“ mit dem Ziel, ein Rahmenwerk sowie Techniken für ein qualitätsbasiertes Routing im Internet zu definieren. Dieses qualitätsbasierte Routing soll Wege durch das Internet finden und verwalten, die einzelne Datenströme in der geforderten Dienstqualität unterstützen. Im besonderen müssen dabei bereits existierende Routingprotokolle, wie beispielsweise OSPF (Open Shortest Path First) um Aspekte der Dienstqualität erweitert werden. Der Beitrag „Qualitätsbasiertes Routing im Internet“ stellt die ersten Arbeiten der QoS Routing Arbeitsgruppe vor. Dabei stehen erste Definitionen für ein Rahmenwerk zum Routing sowie Erweiterungen des OSPF-Protokolls im Mittelpunkt.

Multimediale Konferenzen im Internet

In den letzten Jahren wurde die Forderung nach multimedialen Konferenzen im Internet immer massiver, es fehlte jedoch an der entsprechenden Infrastruktur. Im besonderen existierte kein Protokoll zur Verwaltung und Koordination von Multimedia-Sitzungen. Aus diesem Grund etablierte sich die Arbeitsgruppe „Multiparty Multimedia Session Control“ (kurz: mmusic) der IETF (Internet Engineering Task Force). Das Ziel dieser Gruppe besteht darin, Protokolle für die Aushandlung der Sitzungsteilnehmer, der Kommunikationstopologie und der Medienkonfiguration zu definieren. Erste Ergebnisse bilden die Sitzungsverwaltungsprotokolle SDP (Session Description Protocol), SAP (Session Announcement Protocol) und SIP (Session Initiation Protocol) sowie das Protokoll RTSP (Real-Time Streaming Protocol) zur Kontrolle der Übertragung von Audio und Video. In dem Beitrag „Multimediale Konferenzen im Internet“ werden die existierenden Protokolle der MMUSIC-Arbeitsgruppe mit ihren wichtigsten Charakteristiken vorgestellt.

Fibre Channel-GBit/s im Rechner und LAN

Fibre Channel ist ursprünglich eine Technologie, um verschiedene Komponenten eines Rechners (Peripheriegeräte) miteinander zu verbinden. So können z.B. Festplatten oder Videokameras über Fibre Channel angeschlossen werden. Diese neue Technologie erlaubt extrem hohe Datenübertragungsraten bis in den Gbit/s-Bereich und zeichnet weiterhin durch große Reichweite (bis zu 10km) und flexible Konfigurationen (Topologien) aus. Doch die Fibre Channel Technologie bietet weit mehr: sie ermöglicht eine Vernetzung von Komponenten und Rechnern zum „Gigabit-LAN“ und stellt eine Alternative bzw. eine Konkurrenz zur ATM-Technologie dar. Dieser Beitrag gibt einen Überblick über die Fibre Channel-Technologie.

Sichere Kommunikation in ATM-Netzen

Jochen Katz

Kurzfassung

Bei der Einführung des Asynchronen Transfer Modus (ATM) wurde die Datensicherheit zunächst vernachlässigt. In der Protokollhierarchie des ATM befinden sich deshalb keine Dienste zur Authentifizierung oder für Datensicherheit. Diese Arbeit gibt einen Überblick über die Artikel von Deng et. al. [DeGL95], Chuang [Chua95] und Stevenson et. al. [StHB95], die sich damit befassen, wie die Kommunikation über ATM sicherer gestaltet werden kann.

Zunächst werden anhand eines Frameworks des ATM-Forums [Foru97] die Sicherheitslücken von ATM beschrieben. Forderungen an ein sicheres ATM-Netzwerk werden aufgestellt. Anschließend werden die drei Artikel vorgestellt, analysiert und verglichen. Kriterien für diesen Vergleich sind unter anderem: die angebotenen Sicherheitsdienste, die Unterbringung dieser Dienste im Schichtenmodell und die notwendigen Änderungen im Netzwerk.

1 Einleitung

ATM erfreut sich aufgrund der Fähigkeit, unterschiedlichste Anwendungsanforderungen zu erfüllen, immer größerer Beliebtheit. Mit zunehmender Verbreitung werden auch mehr schützenswerte Informationen, die das Ziel von Angriffen sind, über ATM-Netze transportiert.

Solche Angriffe haben häufig das Ziel, anderen Teilnehmern die Benutzung von Netzdiensten zu verweigern (Denial of Service) bzw. einen Datenaustausch zwischen zwei Stationen mitzuhören oder die Daten dabei zu verändern.

Abgewehrt werden solche Angriffe durch Verschlüsselung der Daten, so daß nur die gewünschten Teilnehmer diese entschlüsseln können. Digitale Signaturen sorgen dafür, daß der Empfänger nachprüfen kann, woher die empfangenen Daten stammen.

Diese Verschlüsselung und Authentifizierung kann natürlich auf der Anwenderschicht erfolgen. Allerdings bleiben dann die Funktionen aller darunterliegenden Schichten ungeschützt. Insbesondere können noch Angriffe auf das Netz selbst erfolgen. Ein Bereitstellen von Sicherheitsdiensten auf der Netzebene ist also notwendig.

Dieser Beitrag gibt zunächst eine Einführung in die Funktionsweise von ATM anhand des Protokollreferenzmodells (PRM) des Broadband Integrated Services Digital Net-

work (B-ISDN[1]). Anschließend wird das Security Framework des ATM-Forums vorgestellt, das die Gefahren in ATM-Netzen beschreibt und Forderungen an ein sicheres ATM-Netz aufstellt. Danach wird detailliert beschrieben, wie in den drei Vorschlägen ein sicherer Verbindungsaufbau stattfindet und wie die Benutzerdaten geschützt werden. Abschließend werden die drei Lösungen miteinander verglichen.

2 Einführung in ATM

ATM ist eine zellorientierte Datenübertragungstechnik, die als Transportmechanismus für das B-ISDN ausgewählt wurde. Abbildung 1 zeigt das Protokollreferenzmodell des B-ISDN.

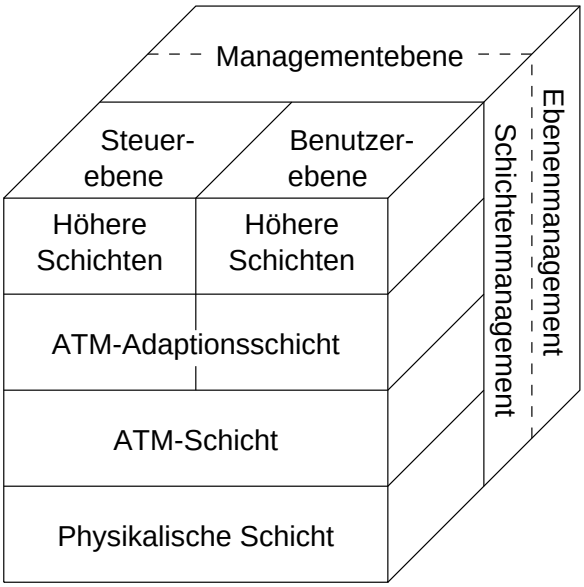


Abbildung 1: Protokollreferenzodell des B-ISDN

2.1 Die Ebenen

Die Benutzerebene (User Plane) ist für den Transport der Benutzerdaten zuständig.

Innerhalb der Steuerebene (Control Plane) werden über Signalisierung Verbindungen auf- und abgebaut und überwacht. Beim Verbindungsaufbau werden die Kanalidentifikation (Virtual Channel Identifier, VCI) und die Pfadidentifikation (Virtual Path Identifier, VPI) für die Verbindung der ATM-Schicht vergeben.

Die Managementebene ist unterteilt in das Ebenen- und das Schichtenmanagement. Das Ebenenmanagement koordiniert die Funktionen und Abläufe der drei Ebenen, und das Schichtenmanagement ist für Metasignalisierung und den Austausch von Managementinformationen (Operation and Maintenance, OAM) verantwortlich. Metasignalisierung wird benötigt, um die Signalisierungskanäle der Steuerebene aufzubauen,

[1]B-ISDN: ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) Standard für ein universelles, weltweit einheitliches Hochgeschwindigkeitsnetz zur Übertragung von Sprach-, Daten-, Bild-, und Videodiensten. [Kyas95]

abzubauen und zu überprüfen. OAM-Zellen, die teilweise im Benutzerkanal gesendet werden, dienen der Überwachung der Verfügbarkeit eines Pfades, der Messung der Netzwerkleistung und zum Weiterleiten von Fehlern und Alarmen.

2.2 Die Schichten

Die physikalische Schicht paßt die Zellen der ATM-Schicht an das verwendete Übertragungsmedium an und überträgt sie.

Auf der ATM-Schicht findet der Transport der ATM-Zellen statt. Zellen werden in unidirektionalen Kanälen (Virtual Channel, VC) übertragen. Ein Bündel von Kanälen wird zu Pfaden (Virtual Path, VP) zusammengefaßt. Die Kanal- und Pfadkennungen haben im Allgemeinen keine durchgehende Gültigkeit vom Sender zum Empfänger, sie werden in zwischenliegenden Switches umgesetzt. Ein Switch kann dabei komplette Pfade umsetzen, wobei die VCIs unverändert bleiben, oder Pfade aufspalten und neue zusammensetzen, wobei sich auch die VCIs ändern.

Die Anpassungsschicht (ATM Adaptation Layer, AAL) hat die Aufgabe, die Anforderungen der Anwendungen auf die Zellstruktur der ATM-Schicht abzubilden. Es wurden insgesamt fünf AAL-Typen definiert. Eingesetzt wird aber vor allem der AAL-Typ-5 (AAL5). Die AAL5 besteht aus einer Segmentierungs/Assemblierungsteilschicht (SAR) und einer Konvergenzteilschicht (CS). Die Datenpakete werden von der CS mit einem Trailer versehen und auf ein Vielfaches von 48 Byte aufgefüllt. Die SAR teilt sie auf und übergibt sie der ATM-Schicht.

2.3 Signalisierung

Der grundlegende Ablauf eines erfolgreichen Verbindungsaufbaus kann Abbildung 2 entnommen werden.

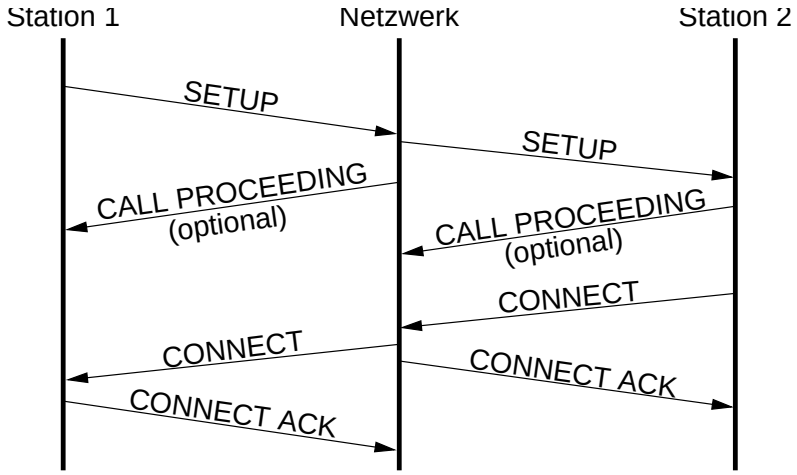


Abbildung 2: Signalisierung beim Verbindungsaufbau

Über den von der Metasignalisierung bereitgestellten Kanal werden die Nachrichten ausgetauscht. Da die Signalisierung flexibel sein muß, wird für die unterschiedlichen Nachrichtentypen nur ein fester Rahmen vorgegeben. Innerhalb dieses Rahmens werden

die Informationen über Informationselemente (Information Elements, IE) ausgetauscht. In der SETUP-Nachricht wird über IEs unter anderem der geforderte AAL-Typ und die ATM-Zellrate der Verbindung angegeben. Die optionale Nachricht Call Proceeding dient dazu, die verfügbare Zeit zum Herstellen der Verbindung zu verlängern.

3 Das Security Framework des ATM-Forums

In diesem Kapitel werden anhand des ATM Security Frameworks des ATM-Forums [Foru97] zunächst die Hauptziele eines sicheren ATM-Netzwerks vorgestellt. Dann wird erläutert, wodurch diese Ziele bedroht werden. Abschließend werden die Forderungen des ATM-Forums an ein sicheres ATM-Netzwerk vorgestellt.

3.1 Allgemeine Ziele eines sicheren Netzes

Die vier Hauptziele des Netzbetreibers und der Netzbenutzer sind:

- Vertraulichkeit (Confidentiality)

  Daten, die gespeichert oder übertragen werden, dürfen nur demjenigen zugänglich sein, für den sie bestimmt sind.

- Datenintegrität (Integrity)

  Nachrichten (Informationen, Daten) sind gegen unrechtmäßiges Löschen, Verfälschung, Verzögerung, und Wiederholung zu schützen.

- Verantwortlichkeit (Accountability)

  Jeder ist für die Auswirkungen seiner Aktivitäten verantwortlich. Der Netzbetreiber kann feststellen, welche Netzdienste benutzt wurden, sowie wann und von wem sie benutzt wurden.

- Verfügbarkeit (Availability)

  Die Dienste des Netzes müssen den autorisierten Benutzern zugänglich sein. Für den Netzbetreiber muß das Netzmanagement verfügbar sein.

3.2 Gefahren in ATM-Netzen

Bedrohungen des Netzes, die durch falsche/fehlende Administration oder die ohne Absicht durch falsche Benutzung entstehen, werden hier nicht näher behandelt. Die hier aufgeführten Bedrohungen entstehen durch bewußte Angriffe auf das ATM-Netz.

Die folgenden Bedrohungen werden identifiziert:

- Maskierung (Masquerade), d.h. jemand gibt vor, ein anderer zu sein.

  In der SETUP-Nachricht gibt es zwar ein Informationselement, das den Initiator identifiziert, dieses ist aber optional und wird vom Initiator gesetzt. Der Gerufene hat keine Möglichkeit, die Korrektheit dieser Information zu überprüfen.

- Mithören (Monitoring) von Daten die übertragen werden.

  In der Firma, bei der Stevenson (siehe Abschnitt 4.1) beschäftigt ist, wurde ein Protokollanalysator erfolgreich eingesetzt, um Loginsequenzen mitzuschreiben.

- Unberechtigter Zugriff auf Daten oder Ressourcen

  Im öffentlichen Netz kann auf die Daten aller Kanäle zugegriffen werden. Dies kann z.B. in einem Switch, einem Repeater oder auch direkt am Übertragungsmedium geschehen.

- Verlust oder Verfälschung von Informationen.

  Im B-ISDN-PRM ist kein Dienst enthalten, der erkennt, wenn Daten gelöscht, eingefügt, verändert, umgeordnet, wiederholt oder verzögert werden, sofern die Protokolle eingehalten werden.

- Die Benutzung eines Dienstes wird abgestritten (Repudiation).

  Es wird zwar ein Logbuch über Kommunikationsvorgänge geführt, trotzdem kann der Netzbetreiber nicht zuverlässig genug nachweisen, daß jemand einen bestimmten Dienst benutzt hat.

- Fälschung (Forgery), d.h. jemand gibt vor, Zellen abgeschickt oder empfangen zu haben, obwohl dies nicht geschehen ist.

- Dienstverweigerung (Denial of Service). Andere Benutzer werden davon abgehalten, einen Dienst zu benutzen.

  Mit Hilfe der RESTART-Nachricht[2] können Verbindungen (VC) anderer Teilnehmer beendet werden, da die Herkunft dieser Nachricht nicht überprüft wird.

3.3 Forderungen an ein sicheres ATM-Netz

Nachdem das ATM-Forum die Bedrohungen analysiert hat, wurden Forderungen aufgestellt, die ein sicheres ATM-Netz erfüllen muß.

1. Authentifizierung der Nachrichtenherkunft
2. Vertraulichkeit von Verbindungen und Nachrichten
3. Schutz der Nachrichten vor Veränderung, Wiederholung, Verfälschung, Löschen
4. Benutzerauthentifizierung auf Endsystemebene
5. Zugriffskontrolle
6. Verantwortlichkeit der Benutzer für Aktionen im Netz
7. Führen eine Logbuchs über sicherheitsrelevante Ereignisse und die Möglichkeit, dieses auszuwerten

[2] Die RESTART-Nachricht wird vom Netzwerk oder von einem Endsystem bei Fehlern benutzt, um die andere Station zu veranlassen, alle Ressourcen eines oder mehrerer Kanäle freizugeben.

8. Auslösen von Alarmen beim Auftreten von speziellen sicherheitsrelevanten Ereignissen
9. Wiederherstellung der Netzfunktion nach erfolgreichen oder versuchten Angriffen auf die Sicherheit
10. Ein Sicherheitsmanagement muß vorhanden sein

4 Vorstellung der Lösungen

In diesem Abschnitt werden die drei Lösungen vorgestellt. Überlegungen, die in mehreren Vorschlägen vorkommen werden nur einmal beschrieben.

4.1 Der Vorschlag von Stevenson et. al.

Stevenson [StHB95] führt zwischen dem als sicher geltenden ATM-LAN und dem unsicheren öffentlichen ATM-WAN eine Crypto-unit ein, die für eine sichere Übertragung über das WAN zuständig ist. Außerdem müssen noch zwei Server über das WAN erreichbar sein, die die Crypto-units mit Zertifikaten und Informationen über die Zugriffskontrolle versorgen. Die Informationen dieser Server haben eine begrenzte Lebensdauer und werden in regelmäßigen Abständen erneuert. Diese Erneuerung findet unabhängig von den sonstigen Aufgaben der Crypto-units statt, die Server müssen also nicht bei jedem Verbindungsaufbau abgefragt werden.

4.1.1 Der Verbindungsaufbau

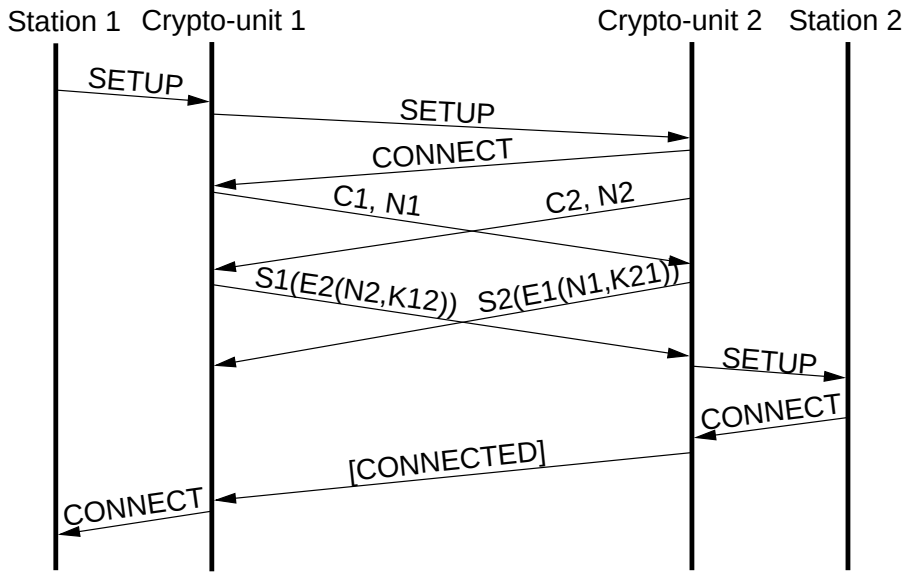


Abbildung 3: Sicherer Verbindungsaufbau nach Stevenson

Für den Verbindungsaufbau stellt Stevenson ein einfaches Protokoll gemäß Abbildung 3 vor. Alternativen zu diesem Protokoll, wie Punkt-zu-Mehrpunkt-Verbindungen, werden in [SHBW95] vorgestellt.

Ci	Zertifikat von Crypto-unit i
Ni	Zufallszahl (Nonce) von Crypto-unit i
Si(X)	X signiert mit dem privaten Schlüssel von Crypto-unit i
Ei(X)	X verschlüsselt mit dem öffentlichen Schlüssel von Crypto-unit i
Kij	Schlüssel für den Datenstrom von i nach j
CONNECTED	Nachricht über die erfolgreiche Verbindung zur Station 2

Tabelle 1: Erklärung zu Abbildung 3

Bevor die Verbindung zwischen zwei Endsystemen aufgebaut wird, handeln die beteiligten Crypto-units für jede Richtung einen Session Key aus, die für die Verschlüsselung der Benutzerdaten verwendet werden. Diese Aushandlung findet normalerweise im Benutzerkanal statt, kann aber auch über einen zusätzlich eingerichteten Kanal abgewickelt werden. Dies ist z.B. bei Punkt-zu-Mehrpunkt-Verbindungen nötig, bei denen kein Rückkanal zur Verfügung steht. Die Hauptanforderung an das Authentifizierungsprotokoll ist, daß das Zeitlimit bis zum Senden der Connect-Nachricht nicht überschritten wird. Die Zufallszahlen verhindern das Wiederholen der Nachrichten.

4.1.2 Verschlüsselung der Benutzerdaten

Es ist möglich, auf der physikalischen Schicht zu verschlüsseln (siehe Abbildung 4a). Dadurch kann auf dem Übertragungsmedium nur noch ein kontinuierlicher Datenstrom ohne Strukturinformationen mitgehört werden. Allerdings werden die Daten in jedem Switch im Klartext verarbeitet. Verschlüsselung in der physikalischen Schicht sollte daher nur zusätzlich zu Verschlüsselung auf höheren Schichten verwendet werden.

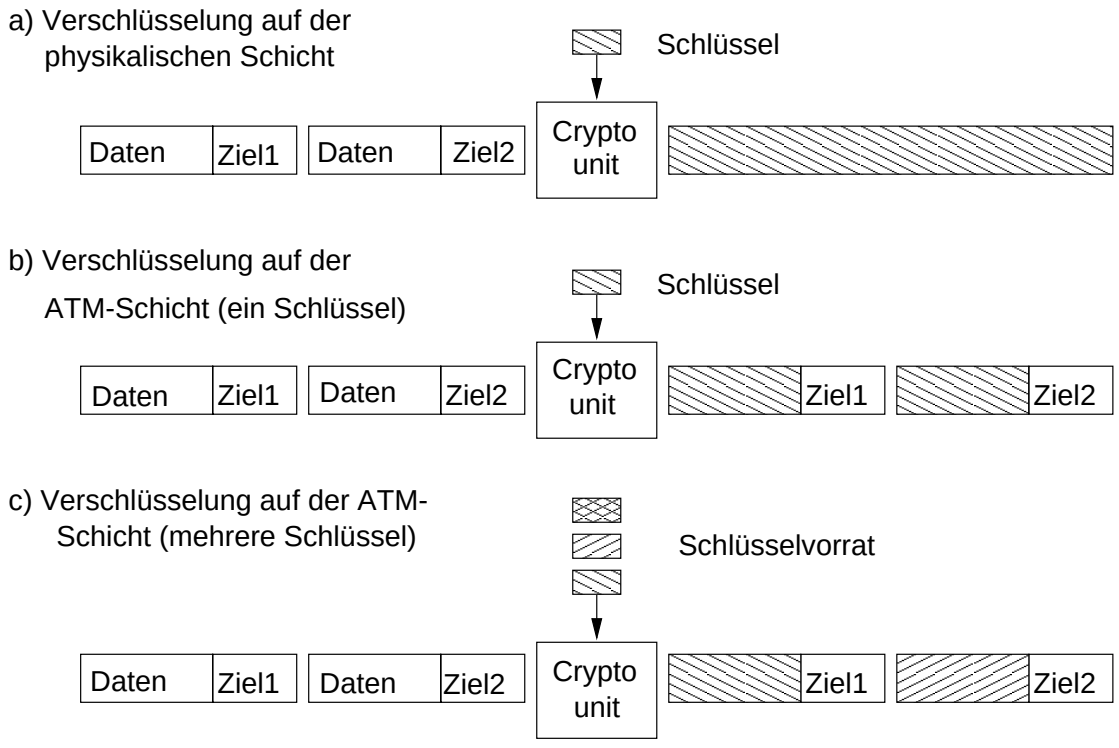


Abbildung 4: Verschiedene Möglichkeiten der Verschlüsselung

Stevenson schlägt deshalb eine Verschlüsselung in der ATM-Schicht vor, d.h. der Zellkopf (Header) wird nicht verschlüsselt. Da es nicht besonders sicher erscheint, alle Zellen mit dem gleichen Schlüssel zu verschlüsseln (siehe Abbildung 4b), bleibt nur die Möglichkeit, für jeden Kanal einen eigenen Schlüssel zu verwenden (siehe Abbildung 4c).

Da die Zellen aller Kanäle in einen kontinuierlichen Datenstrom gemultiplext werden, muß die Crypto-unit in der Lage sein, den Schlüssel nach jeder Zelle zu wechseln. Bei 622 Mbps kann alle 700ns ein Schlüsselwechsel stattfinden, da eine Zelle innerhalb dieser Zeit übertragen wird und zwei aufeinanderfolgende Zellen zu verschiedenen Kanälen gehören können. Im UNI-Protokoll beträgt die Anzahl der möglichen Kanäle 2^{24}, d.h. innerhalb 700ns muß anhand von VCI und VPI ein Schlüssel aus 2^{24} bestimmt und geladen werden. Anschließend müssen noch die Daten verschlüsselt werden. Die Verwendung eines asymmetrischen Verschlüsselungsalgorithmus ist daher nicht möglich. Zur Beschleunigung der Verschlüsselung könnten die 48 Byte in mehrere Blöcke aufgespalten und parallel verarbeitet werden. Hierbei sind Einschränkungen des eingesetzten Chiffrierverfahrens zu beachten.

Es gibt Verschlüsselungsalgorithmen, die bei Verlust eines Teils der Daten die Synchronisation verlieren, so daß alle nachfolgenden Daten falsch entschlüsselt werden. Dies ist z.B. beim Data Encryption Standard (DES) im Output-Feedback-Modus der Fall. Andere Algorithmen (DES im Electronic-Codebook-Modus oder DES im Cipher-Block-Chaining-Modus) erholen sich nach einem Datenverlust, d.h. nur ein Teil der Daten wird falsch entschlüsselt.

Da ATM-Zellen mit einer Wahrscheinlichkeit von ca. 10^{-9} (bei 622 Mbps ist das eine Zelle in 15 Minuten) verloren gehen, muß man sich entweder auf die zweitgenannten Algorithmen beschränken, oder man muß dafür sorgen, daß der Empfänger in regelmäßigen Abständen in einen definierten Zustand gesetzt wird.

Stevenson setzt auf die flexiblere zweite Lösung und definiert Verschlüsselungsketten, die aus aufeinanderfolgenden ATM-Zellen eines Kanals bestehen. Am Ende einer solchen Kette wird der Empfänger synchronisiert. Es muß nun geklärt werden wie und wann der Empfänger synchronisiert werden kann.

Der optimale Zeitpunkt einer Synchronisation wäre am Ende einer AAL-PDU, da bei einem Zellverlust sowohl die betroffene PDU, als auch die betroffene Kette erneut übertragen werden muß. In der ATM-Schicht sind aber die PDU-Grenzen der AAL nicht bekannt, sie dürfen aufgrund des Schichtenprinzips nicht bekannt sein. Die Crypto-unit kennt vom Verbindungsaufbau die Bandbreite eines jeden Kanals. Da die PDU-Größe etwa proportional zur belegten Bandbreite ist, schlägt Stevenson vor, Synchronisationszellen periodisch in Abhängigkeit von der belegten Bandbreite zu senden.

Die Information über das Ende einer Verschlüsselungskette kann nicht im Kopf der ATM-Zelle übertragen werden, da dort keine Bits frei sind. Aus diesem Grund schlägt Stevenson vor, am Ende einer Kette eine Synchronisationszelle zu senden. Diese Zelle muß im gleichen Kanal übertragen werden, da ATM die Reihenfolge nur innerhalb eines Kanals garantiert. Es könnten OAM-Zellen oder normale Datenzellen verwendet werden. Stevenson ist gegen die Verwendung von OAM-Zellen, da dies nicht kompatibel zu existierender ATM-Hardware wäre. Zur Synchronisation soll die Crypto-unit in den Datenstrom zusätzliche Benutzerdatenzellen einfügen, die im Datenfeld ein spezielles

Bitmuster enthalten. Empfängt eine Crypto-unit eine Zelle mit diesem Bitmuster, interpretiert sie diese als Synchronisationszelle. Hierdurch wird allerdings ein neues Problem geschaffen. Enthält eine Benutzerzelle dieses Bitmuster, wird diese Zelle auch als Synchronisationszelle betrachtet und aus dem Datenstrom entfernt. Die empfangende Crypto-unit setzt sich zurück und die nachfolgenden Daten werden falsch entschlüsselt. Bei der erneuten Übertragung der betreffenden PDU könnte das gleiche wieder passieren. Diese Situation kann eventuell nur durch einen erneuten Verbindungsaufbau behoben werden.

4.2 Der Vorschlag von Chuang

Chuang [Chua95] geht vom gleichen Netzmodell aus wie Stevenson. Auch er führt eine zentrale Hardwarekomponente (CryptoNode) ein, die sich allerdings im Gatewayswitch befindet. Verbindungen, die gesichert werden müssen, werden über diesen zusätzlichen Knoten geleitet.

4.2.1 Der Verbindungsaufbau

Chuang möchte beim Authentifizierungs- und Schlüsselaustauschprotokoll sehr flexibel sein, daß auch zukünftige Anforderungen erfüllt werden können. Aus diesem Grund soll es möglich sein, ein Verfahren mit 3-Wege-Handshake zu verwenden. Das zugehörige Signalisierungsprotokoll muß also auch ein 3-Wege-Verfahren sein.

Weil das UNI Protokoll von ATM auf 2 Wege begrenzt ist, weicht Chuang auf das Signalisierungsprotokoll der Multi-Service Network Connection Management Architecture (MSN-CMA [Cros95]) aus. Dabei liegt die gesamte Netzkontrolle und das Netzmanagement bei einigen Servern. Möchte eine Station eine Verbindung aufbauen, signalisiert sie dies einem geeigneten Server über einen entfernten Prozeduraufruf (Remote Procedure Call, RPC). Der Server sucht im Netzwerk einen geeigneten Weg, informiert die andere Station über den Verbindungswunsch und ändert in den Switches die Routingtabellen.

4.2.2 Verschlüsselung der Benutzerdaten

Auch er kommt zu dem Schluß, daß Benutzerdaten auf der ATM-Schicht verschlüsselt werden und daß für jeden VC ein eigener Schlüssel verwendet werden sollte. Dieser Schlüssel soll in periodischen Abständen (abhängig von der Datenrate) gewechselt werden, um nicht zu viele Daten mit dem selben Schlüssel zu verschlüsseln. Er verlangt, daß bei einer Verbindung mit 130 Mbps der Schlüssel etwa alle zehn Sekunden gewechselt wird.

Synchronisation der CryptoNodes wird durch Einfügen einer zusätzlichen ATM-Zelle (CryptoTag) in den Benutzerdatenstrom erreicht. Hierbei verletzt Chuang bewußt das Prinzip des Schichtenmodells, denn der CryptoTag soll an den PDU-Grenzen der AAL eingefügt werden. Der CryptoTag besteht aus einer speziellen AAL5-PDU, bei der das CPI-Feld[3] auf einen reservierten Wert gesetzt wird. Über den CryptoTag werden

[3]Der Common Part Identifier ist ein 8 Bit langes Feld im AAL5 Trailer, das bisher noch nicht benutzt wird.

Schlüsselwechsel und Initialisierungsvektoren (IV) für das Entschlüsseln der nachfolgenden Zellen ausgetauscht. Zudem ist eine digitale Signatur (Message Authentication Code, MAC) enthalten, die die zuvor gesendete AAL-PDU und auch den CryptoTag authentifiziert (siehe Abbildung 5).

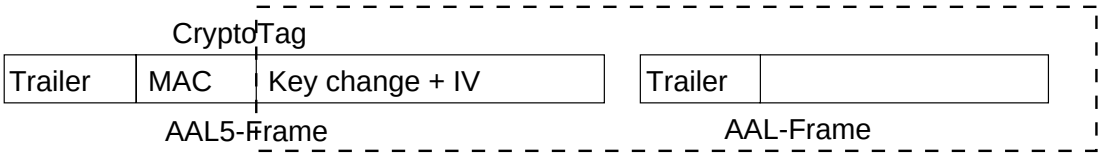


Abbildung 5: Authentifizierung durch den CryptoTag

Der CryptoNode, der die verschlüsselten Daten empfängt, muß die letzte Zelle jeder AAL-PDU so lange verzögern, bis der MAC überprüft wurde. Falls der MAC nicht korrekt ist, wird die verzögerte Zelle verworfen, wodurch das Endsystem keine gültige AAL-PDU erhält.

Chuang unterscheidet zwischen Integrity und Confidentiality, um möglichst flexibel zu sein. Eine Erweiterung des CryptoTags ist möglich, da hierzu unterschiedliche CPI-Werte verwendet werden können.

4.3 Der Vorschlag von Deng et. al.

Auch Deng [DeGL95] betrachtet das private ATM Netz als sicher, da hier der Betreiber physikalischen Zugriff hat. Allerdings führt er keine zentrale Komponente ein, sondern führt die Verschlüsselung und Authentifizierung in den Endsystemen durch.

4.3.1 Der Verbindungsaufbau

Deng definiert 12 neue Informationselemente (siehe Tabellen 2 und 3), jeweils 6 Informationselemente werden in der SETUP und der CONNECT Nachricht übertragen. Mit den IE 1-4 und 5-8 handeln die beiden Stationen einen Sicherheitskontext aus. Die IE 9-10 und 11-12 realisieren eine Authentifizierung und den Schlüsselaustausch nach X.509.

4.3.2 Verschlüsselung der Benutzerdaten

Auch Deng isoliert die ATM-Schicht und die AAL als mögliche Schichten für eine Verschlüsselung der Benutzerdaten. Da aber zusätzlich noch eine Authentifizierung ermöglicht werden soll, bleibt für ihn nur noch die AAL als optimale Lösung, da eine Authentifizierung die Übertragung zusätzlicher Daten erfordert und in der SAR ohnehin schon eine Segmentierung vorgenommen wird.

Deng führt in der AAL zwischen CS und SAR eine neue Schicht ein, die er Data Protection Layer (DPL) nennt. Dies hat vor allem den Vorteil, daß beliebige Verschlüsselungs- und Authentifizierungsalgorithmen eingesetzt werden können, da eine etwaige Datenexpansion von der SAR ohne zusätzlichen Aufwand abgefangen wird.

IE für SETUP-Nachricht		IE für CONNECT-Nachricht	
Nr	Name und Inhalt	Nr	Name und Inhalt
1	Assoziazionsidentifikator der rufenden Station	5	Assoziazionsidentifikator der gerufenen Station
2	Vorschlag für die zu verwendende Sicherheitsstufe bei Verschlüsselung und Authentifizierung der Daten	6	Gewählte Sicherheitsstufe
3	Liste der möglichen Parameter für die Verschlüsselung der Benutzerdaten	7	Gewählte Parameter für Verschlüsselung
4	Liste der möglichen Parameter für die Authentifizierung der Benutzerdaten	8	Gewählte Parameter für Authentifizierung
9	Zertifikat der rufenden Station	11	Zertifikat der gerufenen Station
10	$S_A\{T_A, B, E_B\{K_A\}\}$	12	$S_B\{T_B, A, E_A\{K_B\}\}$

Tabelle 2: Neue Informationselemente

Erklärung für die Informationselemente 10 und 12	
$S_X\{D\}$	Die Daten D signiert mit dem privaten Schlüssel von Endsystem X
T_X	Aktueller Zeitstempel von Endsystem X, um Wiederholungen zu erkennen
$E_X\{D\}$	Die Daten D verschlüsselt mit dem öffentlichen Schlüssel von Endsystem X
K_X	Der Schlüssel zur Verschlüsselung der Daten von X zum anderen Endsystem

Tabelle 3: Erklärung zu Tabelle 2

5 Vergleich der drei Lösungen

Die drei vorgestellten Lösungen konzentrieren sich auf die Anforderungen 1 - 4 des ATM-Forums aus Abschnitt 3.3. Die restlichen Anforderungen, die hauptsächlich für den Netzbetreiber von Interesse sind, werden nicht betrachtet.

Beim Verbindungsaufbau findet bei den drei Vorschlägen eine gegenseitige Authentifizierung der beteiligten Stationen statt. Zufallszahlen oder Zeitstempel verhindern eine Wiederholung der Nachrichten. Während bei Deng und Chuang die Authentifizierung über die Signalisierung abgewickelt wird, geschieht dies bei Stevenson im Benutzerkanal bzw. einem zusätzlich aufgebauten Kanal.

Gemeinsam ist allen drei Lösungen, daß die Authentifizierung der Benutzerdaten (wenn sie angeboten wird) in der AAL implementiert wird, da eine Authentifizierung immer die Übertragung zusätzlicher Daten bedeutet, was in der ATM-Schicht aufgrund der festgelegten Zellgröße nicht möglich ist. Die Benutzerdaten werden auch nicht vor Wiederholung geschützt, da dies in höheren Schichten besser erkannt werden kann und

eine Überladung der unteren Schichten mit zu vielen Funktionen vermieden werden soll.

Die Lösung von Stevenson erfordert keine Änderung am UNI. Es muß eine komplexe Hardwarekomponente zwischen LAN und WAN eingefügt werden. Änderungen an den Stationen oder im öffentlichen Netz sind nicht nötig, abgesehen von zwei Servern, die Zertifikate und Zugriffskontrollinformationen bereithalten. Stevenson bietet für die Benutzerdaten keine Authentifizierung an. Ein Aushandeln von Sicherheitsparametern ist weder beim Verbindungsaufbau, noch während der Verbindung möglich. Für die Dauer der Verbindung wird nur ein Schlüssel verwendet, um die Daten zu schützen.

Für Dengs Lösung muß das UNI erweitert werden und im PRM eine neue Teilschicht eingefügt werden. Das Aushandeln von Sicherheitsparametern ist sowohl beim Verbindungsaufbau, als auch während der Verbindung durch DPL-PDUs möglich. Das Authentifizierungsprotokoll bleibt allerdings auf zwei Phasen begrenzt. Für die Verschlüsselung und die Authentifizierung der Benutzerdaten verwendet Deng den gleichen Schlüssel, d.h. wenn dieser bekannt ist können sowohl die Benutzerdaten entschlüsselt, als auch authentifizierte Benutzerdaten erzeugt werden. Da die Sicherheitsdienste in der AAL angesiedelt sind, bleiben die AAL-Header ungeschützt. Dengs Lösung hat allerdings drei große Vorteile: Das Einfügen von zusätzlichen Zellen für das Sicherstellen der Synchronisation zwischen Sender und Empfänger entfällt, die Anforderung an die Geschwindigkeit des Schlüsselwechsels ist nicht so hoch und die Sicherheitsparameter können in jedem Endsystem festgelegt werden.

Chuangs Lösung ist sehr flexibel: Beim Verbindungsaufbau können die Sicherheitsparameter und das Schlüsselaustauschprotokoll ausgehandelt werden. Für Verschlüsselung und Authentifizierung der Benutzerdaten werden verschiedene Schlüssel verwendet, die auch während der Verbindung gewechselt werden können. Allerdings verstößt Chuangs Lösung gegen das Schichtenprinzip und gegen die Philosophie des ATM-Forums, das die Netzkontrolle und das Netzmanagement dezentral organisiert hat. Chuangs Lösung erfordert auf jeden Fall eine Neustrukturierung des öffentlichen Netzes, da er die Signalisierung des MSN-CMA übernehmen möchte. Zudem muß der CryptoNode eine Umsetzung der UNI-Signalisierung im LAN auf die MSN-CMA-Signalisierung im WAN vornehmen oder im LAN muß ebenfalls die MSN-CMA-Signalisierung eingeführt werden. Hinzu kommt, daß die Signalisierung des MSN-CMA auf RPCs basiert und RPCs bisher durch keine Sicherheitsmaßnahmen geschützt sind. Eine Implementierung von Chuangs Lösung setzt also auch eine Veränderung beim RPC voraus.

Auch die Anforderungen an den CryptoNode sind höher als bei Stevenson: Es wird zusätzlich ein MAC berechnet, alle Zellen werden auf das Ende einer AAL-PDU untersucht und die letzte Zelle jeder AAL-PDU muß verzögert werden, bis der MAC überprüft wurde.

Einen Überblick geben Tabellen 4 und 5.

6 Schlußbetrachtungen

In diesem Beitrag wurde gezeigt, daß Sicherheitsdienste in ATM-Netzen eingeführt werden müssen. Für eine Plazierung dieser Dienste kommen die ATM-Schicht und die AAL in Frage. Beide Möglichkeiten haben Nachteile: Bei einer Implementierung in der

	Stevenson	Deng	Chuang
Verbindungsaufbau geschützt durch	Authentifizierung, Verschlüsselung, Wiederholungserkennung	Authentifizierung, Verschlüsselung, Wiederholungserkennung	Authentifizierung, Verschlüsselung, Wiederholungserkennung
Aushandelbare Dienste	keine	Integrity und Confidentiality: Algorithmus, Schlüsselgröße;	Integrity und Confidentiality: Algorithmus, Schlüsselgröße; Schlüsselaustauschprotokoll
Authentifizierungsprotokoll	Gegenseitige Authentifizierung basierend auf Zufallszahlen und asymmetrischer Kryptographie	X.509 (2-Weg-Protokoll, asymmetrisch mit Zeitstempel)	2 oder 3-Weg-Protokolle frei wählbar
Übertragung von Schlüssel und Authentifizierung	Benutzerkanal oder eigener Kanal	Signalisierung	Signalisierung basierend auf RPC
Änderungen am UNI-Signalisierungsprotokoll	nein	ja: 12 neue IE	ja: Protokoll wird durch Signalisierung des MSN-CMA ersetzt

Tabelle 4: Vergleich der drei Lösungen (Teil1)

ATM-Schicht ist es sehr aufwendig, einen MAC zu übertragen und für die Synchronisation des Empfängers zu sorgen. Diese Probleme gibt es bei einer Implementierung in der AAL nicht, dafür bleiben aber die Header der AAL ungeschützt.

Hohe Anforderungen werden an die Verschlüsselungsgeschwindigkeit und an die Geschwindigkeit des Schlüsselwechsels gestellt. Für die Verschlüsselung der Benutzerdaten kann daher nur ein symmetrisches Verschlüsselungsverfahren eingesetzt werden.

Eine Einführung von Sicherheitsdiensten sollte nur wenige Änderungen im ATM-Netz voraussetzen. Diese Anforderung erfüllt der Vorschlag von Stevenson am besten. Die meisten Änderungen erfordert der Vorschlag von Chuang: Das Signalisierungsprotokoll muß durch ein neues ersetzt werden, und da dieses die Sicherheitsanforderungen ebenfalls nicht erfüllt, müssen in diesem erst Sicherheitsdienste implementiert werden.

	Stevenson	Deng	Chuang
Ort der Verschlüsselung	in dedizierten Knoten (Crypto-units) zwischen LAN und WAN	in jedem Endsystem	im Gatewayswitch
Unterscheidung zwischen Confidentiality und Integrity	-	ja, aber gleiche Schlüssel	ja
Schlüsselwechsel während Datenaustausch	nein	ja	ja
Confidentiality implementiert in	ATM-Schicht	AAL	ATM-Schicht
Integrity implementiert in	nicht vorhanden	AAL	AAL
Synchronisation des Empfängers	ATM Benutzerdatenzelle	DPL-PDU	spezielle AAL5-PDU
Einfluß auf Sicherheitsparameter	Administrator der Crypto-unit	Konfiguration in jeder Station	Administrator des Gateways
Hauptprobleme	Key agility, keine Integrity	AAL-Header nicht geschützt, Zeitstempel werden benötigt, gleiche Schlüssel für Confidentiality und Integrity	Key agility, Verzögerung von Zellen, RPC nicht sicher, Umstellung des öffentlichen Netzmanagements

Tabelle 5: Vergleich der drei Lösungen (Teil 2)

Literatur

[Chua95] Shaw-Cheng Chuang. *Securing ATM Networks.* Cambridge University ATM Document Collection 4 (The Green Book). 1995.

[Cros95] S. A. Crosby. *Performance Management in ATM-Networks.* PhD thesis, University of Cambridge. 1995.

[DeGL95] Robert H. Deng, Li Gong und Aurel A. Lazar. *Securing Data Transfer in Asynchronous Transfer Mode Networks.* Proceedings of GLOBECOM'95, Singapore. 1995.

[Foru97] ATM Forum. *Security Framework for ATM Networks (Draft).* ATM Forum Technical Committee. 1997.

[Kyas95] Othmar Kyas. *ATM-Netzwerke.* DATACOM-Bergheim. 1995.

[SHBW95] Daniel Stevenson, Nathan Hillery, Greg Byrd und D. Winkelstein. *Design of a key agile cryptographic system for OC-12c Rate ATM.* Symposium on Network and Distributed System Security. 1995.

[StHB95] Daniel Stevenson, Nathan Hillery und Greg Byrd. Secure Communications in ATM Networks. *Communications of the ACM* 38(2), Feb 1995, S. 45–52.

Abbildungsverzeichnis

Tabellenverzeichnis

Unterstützung für Dienstqualitäten in ATM-Netzwerken

Jörg Afflerbach

Kurzfassung

Die ATM-Technologie ist zu dem Zweck konzipiert worden, eine große Vielfalt von Diensten zu unterstützen, die jeweils unterschiedliche Anforderungen an die Dienstqualität haben. In diesem Beitrag wird der Begriff der Dienstqualität in ATM-Netzwerken präzisiert. Mit Hilfe von Verkehrs- und Dienstqualitätsparametern werden die Dienstkategorien des ATM-Forums vorgestellt, die als Grundlage für Konzepte und Mechanismen zur Diensterbringung dienen.

1 Einführung

Sowohl Telekommunikationsanwendungen als auch deren Benutzer haben sehr unterschiedliche Qualitätsanforderungen an die Eigenschaften von Telekommunikationsverbindungen. Derartige Anforderungen, wie beispielsweise die Einhaltung einer maximalen Verzögerung, welche die Daten während der Übertragung innerhalb des Netzwerkes erfahren, oder die maximal tolerierbare Fehlerrate, werden unter dem Begriff *Dienstqualität (Dienstgüte, Quality of Service – QoS)* zusammengefaßt. Dienstqualität kann weiterhin aufgefaßt werden als die qualitativen und quantitativen Eigenschaften, die einen Dienst näher spezifizieren.

Im folgenden wird der Begriff der Dienstqualität speziell für ATM-Netzwerke genauer beschrieben. Zu diesem Zweck werden verschiedene Parameter eingeführt, mit deren Hilfe sich mehrere Kategorien unterschiedlicher Dienstqualität definieren lassen. Anschließend werden Mechanismen zur Diensterbringung vorgestellt, die für die Aufrechterhaltung der Dienstqualität über die Dauer einer ATM-Verbindung sorgen sollen.

2 Dienstkategorien und Dienstklassen im ATM

Die Einführung eines diensteintegrierenden Netzwerkes in der Gestalt von *Breitband-ISDN (B-ISDN)* zusammen mit *ATM (Asynchronous Transfer Mode)* als Basistechnologie macht es möglich, ein vielfältiges Spektrum von Telekommunikationsanwendungen zu unterstützen, das sich von der gewöhnlichen Dateiübertragung bis hin zu Audio-, Video- und Multimedia-Applikationen erstreckt. Um den verschiedenen Anforderungen der einzelnen Anwendungen gerecht werden zu können, wäre es notwendig, jeder

Anwendung einen speziell für sie geeigneten Dienst zur Verfügung zu stellen, der die benötigte Dienstqualität anbietet. Da dies nicht praktikabel ist, klassifiziert man die Dienste entsprechend ihrer Dienstqualität. Eine Anwendung kann nun auf eine der Dienstklassen zurückgreifen, um die gewünschte Dienstqualität zu erhalten. Trotz der unterschiedlichen Qualitätsanforderungen kann man auf diese Weise allen Anwendungen eine angemessene Dienstqualität bieten.

2.1 Dienstkategorien

Sowohl die International Telecommunications Union – Telecommunications Sector (ITU-T) als auch das ATM-Forum haben für die ATM-Schicht mehrere Klassen von Diensten vorgeschlagen. Im folgenden wird ausschließlich der Ansatz des ATM-Forums vorgestellt [Foru96a, Foru96b], der die Unterteilung der Dienste in fünf *Dienstkategorien* vorsieht. Diese Dienstkategorien unterscheiden sich im wesentlichen hinsichtlich der Unterstützung, die sie für Echtzeit-Anwendungen bieten. Echtzeit-Anwendungen, wie interaktive Audio- und Video-Applikationen, stellen strenge Anforderungen an die maximale Verzögerung und die Verzögerungsschwankung der zu übertragenden Dateneinheiten (siehe Abschnitt 3.2). Für traditionelle Datenübertragungsanwendungen, die ohne Echtzeit-Garantien auskommen, sind dagegen Verzögerung und Verzögerungsschwankung nicht von Bedeutung. Die Dienstkategorien der ATM-Schicht sind aufgeschlüsselt in

- *Constant Bit Rate (CBR)*,
- *Real-Time Variable Bit Rate (rt-VBR)*,
- *Non-Real-Time Variable Bit Rate (nrt-VBR)*,
- *Unspecified Bit Rate (UBR)* und
- *Available Bit Rate (ABR)*.

Die *Constant Bit Rate* Dienstkategorie ist dazu gedacht, solche Echtzeit-Anwendungen zu unterstützen, die während der gesamten Verbindungsdauer mit einer konstanten Bitrate senden wollen und daher eine fest zugewiesene Menge an „Bandbreite“ benötigen. Mit Bandbreite ist hier die Übertragungskapazität gemeint, die das Netzwerk der Verbindung zur Verfügung stellt. Die Nutzung der CBR Dienstkategorie ist aber nur dann sinnvoll, wenn die Anwendung tatsächlich mit einer konstanten Übertragungsrate arbeitet und so die ihr zur Verfügung stehende Bandbreite jederzeit voll ausnutzt. Beispiele für Anwendungen, die CBR nutzen, sind Telefon- und Videokonferenz-Systeme, die einen unkomprimierten Audio- oder Videostrom übertragen, etwa um keine zusätzliche Verzögerung durch Kompression und Dekompression hinnehmen zu müssen. Echtzeit-Anwendungen, die nicht mit einer statischen, sondern einer variablen Übertragungsrate arbeiten, wie sie zum Beispiel für komprimiertes Video benötigt wird, würden bei der Nutzung von CBR Netzwerk-Ressourcen verschwenden und sollten statt dessen auf die *Real-Time Variable Bit Rate* Dienstkategorie zurückgreifen. Da bei letzterer nur die im Mittel benötigten Ressourcen reserviert werden, kann die Übertragungskapazität des Netzwerkes effizienter ausgenutzt werden. Allerdings muß dabei eine geringe Menge

an Zellverlusten in Kauf genommen werden, was die Anwendungen aber in der Regel tolerieren können.

Während CBR und rt-VBR Echtzeit-Anwendungen unterstützen, bieten die übrigen drei Kategorien keine Echtzeit-Unterstützung an. Diese drei Dienstkategorien sind daher nur für Anwendungen geeignet, die keine besonderen Anforderungen an Verzögerung und Verzögerungsschwankung haben. Die *Non-Real-Time Variable Bit Rate* Dienstkategorie ist für Anwendungen gedacht, die mit einer variablen Übertragungsrate arbeiten und keine Echtzeit-Anforderungen haben. Durch Reservierung der im Mittel benötigten Bandbreite wird bei der Nutzung von nrt-VBR eine gewisse Höchstdauer der Übertragung nicht überschritten. Daher eignet sich die nrt-VBR Dienstkategorie für antwortzeitkritische Transaktionen, wie sie beispielsweise beim Online-Banking oder bei Flugbuchungen auftreten. Für Anwendungen ohne Echtzeit-Anforderungen, die hingegen keine Dienstgarantien benötigen, erzielt die *Unspecified Bit Rate* Dienstkategorie die bestmögliche Übertragung ohne jegliche Garantie. Der Vorteil von UBR besteht insbesondere in der Ausnutzung der „Restbandbreite“ und den daraus resultierenden günstigen Tarifen. Beispiele für Anwendungen, welche die UBR Dienstkategorie nutzen, sind traditionelle Anwendungen der Rechner-Rechner-Kommunikation wie E-Mail oder File Transfer. Falls eine derartige Anwendung ihre Übertragungsrate an die momentane Netzlast anpassen kann, empfiehlt sich die Nutzung der *Available Bit Rate* Dienstkategorie. Zusätzlich zur Reservierung einer minimal akzeptablen Zellrate verspricht ABR eine geringe Zellverlustrate, wodurch eine niedrigere Übertragungsverzögerung als bei der UBR Dienstkategorie erreicht werden kann. Neben den Beispielanwendungen der UBR Dienstkategorie sind Terminalemulation sowie Operationsausführungen in verteilten Systemen (Remote Procedure Call) als typische Anwendungen für ABR zu nennen.

2.2 Dienstklassen

Auch die der ATM Schicht übergeordnete ATM Adaptation Layer (AAL) bietet verschiedene Klassen von Diensten an, um den unterschiedlichen Anforderungen der Dienste der höheren Schichten gerecht werden zu können. Aus den Unterschieden der Dienste bezüglich der Zeitbeziehung zwischen Sender und Empfänger, der Bitrate und des Verbindungsmodus ergeben sich die vier *Dienstklassen A, B, C* und *D* (siehe Tabelle 1). *Klasse A* ist für Dienste gedacht, die mit einer konstanten Bitrate arbeiten und bei denen eine Zeitbeziehung zwischen Sender und Empfänger besteht – also für Dienste mit Echtzeit-Anforderungen. *Klasse B* wird dagegen bei Diensten mit Echtzeit-Anforderungen verwendet, die keine konstante Bitrate benötigen. Verbindungsorientierte Dienste mit variabler Bitrate und ohne Zeitbeziehung zwischen Sender und Empfänger, wie sie in der traditionellen Rechner-Rechner-Kommunikation Verwendung finden, nutzen *Klasse C*. *Klasse D* ist ebenfalls für die Rechner-Rechner-Kommunikation ausgelegt, im Gegensatz zu Klasse C aber für verbindungslose Dienste.

Obwohl keine feste Zuordnung der vier Dienstklassen zu den Diensttypen der AAL oder den Dienstkategorien der ATM-Schicht besteht, ist es naheliegend, Dienste der Klasse A mit Hilfe des AAL-1 Diensttyps zu erbringen, da dieser die Übertragung konstanter Bitraten unterstützt. Auf der ATM-Schicht bietet sich die Verwendung der CBR Dienstkategorie an. Für Klasse B eignet sich der AAL-Diensttyp 2 in Verbindung mit der rt-VBR Dienstkategorie. Die AAL-Diensttypen 3/4 und 5 können gleichermaßen die Dienste der Klassen C und D erbringen. Da AAL-3/4 jedoch einen

Dienstklassse	A	B	C	D
Bitrate	konstant	variabel		
Zeitbeziehung	vorhanden		nicht vorhanden	
Verbindungsmodus	verbindungsorientiert			verbindungslos
AAL-Diensttyp	AAL-1	AAL-2	AAL-3/4 AAL-5	

Tabelle 1: Die vier Dienstklassen der AAL

erheblich höheren Overhead als AAL-5 mit sich bringt, wird AAL-3/4 üblicherweise nur für verbindungslose Dienste der Klasse D eingesetzt [Gora95].

3 Verkehrs- und Dienstqualitätsparameter im ATM

In diesem Abschnitt werden *Verkehrsparameter* und *Dienstqualitätsparameter* eingeführt, die beide zur Beschreibung der Dienstkategorien verwendet werden [Foru96b]. Im allgemeinen kann man auch die Verkehrsparameter als Dienstgüteparameter auffassen. Da Verkehrsparameter einen Zellenstrom charakterisieren, können sie aber auch für Dienste ohne Dienstqualitätsanforderungen angegeben werden, was die Unterscheidung zwischen Verkehrsparametern und Dienstqualitätsparametern sinnvoll macht.

3.1 Verkehrsparameter

Der Zellenstrom, den eine Anwendung an ein ATM-Netzwerk übergibt, wird mit Hilfe von *Verkehrsparametern* charakterisiert. Zu den Verkehrsparametern gehören

- *Peak Cell Rate (PCR)*,
- *Sustainable Cell Rate (SCR)*,
- *Maximum Burst Size (MBS)* und
- *Minimum Cell Rate (MCR)*.

Peak Cell Rate (PCR) Die *Peak Cell Rate* R_p ist eine obere Schranke für die Zellrate einer ATM-Verbindung. Sie wird definiert als $R_p = \frac{1}{T} \quad \left[\frac{\text{Zellen}}{\text{s}}\right]$, wobei T der minimale zeitliche Abstand zwischen der Ankunft zweier aufeinanderfolgender ATM-Zellen ist. T wird *Peak Emission Intervall* der Verbindung genannt[1].

Sustainable Cell Rate (SCR) Die *Sustainable Cell Rate* R_s ist eine obere Schranke für die durchschnittliche Zellrate einer ATM-Verbindung, gemessen in $\left[\frac{\text{Zellen}}{\text{s}}\right]$. Da $R_s \leq R_p$ gilt, kann das Netzwerk die Ressourcen effizienter zuweisen, wenn die *SCR* spezifiziert ist.

[1]Diese anschauliche Definition des *Peak Emission Intervalls* ist lediglich eine grobe Annäherung an die sehr technische Definition des ATM-Forums (vgl. [Foru96b, Abschnitt 4.4.3 und Anhang C.2]).

Maximum Burst Size (MBS) Die *Maximum Burst Size* gibt an, wieviele Zellen maximal bei einer Zellrate von R_p Zellen pro Sekunde unmittelbar hintereinander gesendet werden können.

Minimum Cell Rate (MCR) Die *Minimum Cell Rate* R_m ist die minimale Zellrate, die vom Netzwerk garantiert wird. Sie wird gemessen in $\left[\frac{\text{Zellen}}{\text{s}}\right]$ und wird ausschließlich in der ABR Dienstkategorie verwendet (siehe Abschnitt 3.3).

Cell Delay Variation Tolerance (CDVT) Ein weiterer Parameter, der jedoch nicht zu den Verkehrsparametern zählt (vgl. [Foru96b, Anhang C.4.1]), ist die *Cell Delay Variation Tolerance*. Sie wird vom Netzwerkbetreiber festgelegt und drückt die akzeptable Abweichung der Zellenankunftszeiten vom Peak Emission Intervall T aus.

3.2 Dienstqualitätsparameter

Die Ende-zu-Ende Dienstqualität einer Verbindung in der ATM-Schicht wird durch *Dienstqualitätsparameter* bestimmt. Die folgenden drei Parameter werden zwischen der Telekommunikationsanwendung und dem Netzwerk im Rahmen eines Verkehrsvertrages (siehe Abschnitt 4.1) ausgehandelt:

- *Cell Transfer Delay (CTD)*,
- *Cell Delay Variation (CDV)* oder *Jitter* und
- *Cell Loss Ratio (CLR)*.

Nicht vorgesehen ist dagegen die Aushandlung von

- *Cell Error Ratio (CER)*,
- *Severely Errored Cell Block Ratio (SECBR)* und
- *Cell Misinsertion Rate (CMR)*.

Cell Transfer Delay (CTD) Die *Cell Transfer Delay (Zellübertragungsverzögerung)* $T(k)$, gemessen in [s], gibt die Ende-zu-Ende Verzögerung der Zelle k an, also die Zeit, die zwischen dem Senden des ersten Bits und dem Empfangen des letzten Bits dieser Zelle vergeht. Die für die Anwendung maximal akzeptable *CTD* wird T_{max} genannt.

Cell Delay Variation (CDV) Auf seinem Weg durch das Netzwerk durchläuft ein Zellenstrom einen oder mehrere Vermittlungsknoten (ATM-Switches), in denen die ankommenden Zellen verschiedener Verbindungen gemultiplext werden. Das führt dazu, daß einige Zellen warten müssen, während andere weitergeleitet werden. Außerdem können Zellen durch den Einsatz von *Operations and Maintenance (OAM) Zellen* verzögert werden, die zu Überwachungs- und Verwaltungszwecken in den Zellenstrom eingefügt werden. Abhängig davon, ob derartige Ereignisse auftreten, ergeben sich für die Zellen eines Zellenstromes verschieden lange Zellübertragungsverzögerungen. Diese Schwankung der *CTD* heißt *Cell Delay Variation* oder auch *Jitter*.

Es existieren zwei Methoden, um die *CDV* zu messen: die *One-Point CDV* und die *Two-Point CDV*. Die Schwankung der Zellankunftszeiten wird bei der One-Point CDV an einem einzigen Meßpunkt beobachtet, während die Two-Point CDV mit zwei verschiedenen Meßpunkten arbeitet. Die One-Point CDV $V_1(k)$ der Zelle k ist definiert als $V_1(k) = t_r(k) - t_a(k)$, wobei $t_r(k)$ für die Referenzankunftszeit und $t_a(k)$ für die tatsächliche Ankunftszeit der Zelle k steht. $t_a(k)$ wird nur an einem einzigen Punkt im Netzwerk gemessen, zum Beispiel am User Network Interface (UNI). Die Two-Point CDV $V_2(k)$ der Zelle k ist definiert als $V_2(k) = T(k) - T_r$, wobei $T(k)$ für die *Cell Transfer Delay* der Zelle k steht und T_r für die *CTD* einer definierten Referenz-Zelle. $T(k)$ sowie T_r werden zwischen zwei Punkten im Netzwerk gemessen, beispielsweise am UNI des sendenden Endsystems und am UNI des empfangenden Endsystems.

Von der Zellübertragungsverzögerung hängt es unter anderem ab, ob eine ATM-Zelle als *erfolgreich übertragen* oder *verlorengegangen* gilt. Trifft eine gesendete Zelle beim Empfänger „pünktlich“ innerhalb von T_{max} Sekunden fehlerfrei ein, so spricht man von einer *erfolgreich übertragenen Zelle*. Eine Zelle, die den Empfänger nicht erreicht, oder bei ihrer Ankunft Verspätung hat, so daß ihre Nutzdaten unbrauchbar geworden sind, wird als *verlorengegangen* betrachtet. Des weiteren können Störeinflüsse die Ursache für *fehlerhafte* und *falsch eingefügte Zellen* sein. Eine Zelle, die zwar rechtzeitig beim Empfänger ankommt, jedoch Fehler aufweist, heißt *fehlerhafte Zelle*. Aufgrund unentdeckter Fehler im Zellkopf kann beim Empfänger eine ATM-Zelle eintreffen, die nicht vom Sender abgeschickt wurde. Man spricht dann von einer *falsch eingefügten Zelle*. Unter Zuhilfenahme dieser Begriffe lassen sich nun die übrigen Dienstqualitätsparameter definieren.

Cell Loss Ratio (CLR) Die *Cell Loss Ratio (Zellverlustrate)* gibt das Verhältnis von verlorengegangenen Zellen zu insgesamt gesendeten Zellen für die gesamte Verbindungsdauer an.

$$CLR = \frac{\text{Verlorengegangene Zellen}}{\text{Insgesamt gesendete Zellen}}$$

Cell Error Ratio (CER) Die *Cell Error Ratio (Zellfehlerrate)* gibt das Verhältnis von fehlerhaften Zellen zu insgesamt übertragenen Zellen für die gesamte Verbindungsdauer an.

$$CER = \frac{\text{Fehlerhafte Zellen}}{\text{Erfolgreich übertragene Zellen} \; + \; \text{Fehlerhafte Zellen}}$$

Severely Errored Cell Block Ratio (SECBR) Das Verhältnis von schwer fehlerhaften Zellblöcken zu insgesamt übertragenen Zellblöcken einer Verbindung heißt *Severely Errored Cell Block Ratio*.

$$SECBR = \frac{\text{Schwer fehlerhafte Zellblöcke}}{\text{Insgesamt übertragene Zellblöcke}}$$

Ein *Zellblock* ist eine Folge von n übertragenen, aufeinanderfolgenden Zellen. Falls mehr als m der n Zellen eines Zellblocks fehlerhaft, verlorengegangen oder falsch eingefügt sind, handelt es sich um einen *schwer fehlerhaften Zellblock*.

Cell Misinsertion Rate (CMR) Die *Cell Misinsertion Rate* gibt an, wie oft falsch eingefügte Zellen innerhalb eines bestimmten Zeitintervalls aufgetreten sind.

$$CMR = \frac{\text{Falsch eingefügte Zellen}}{\text{Zeitintervall}}$$

Die *CMR* wird als Rate und nicht als Verhältnis (Ratio) definiert, da die Anzahl der falsch eingefügten Zellen nicht von der Anzahl der übertragenen Zellen abhängt.

3.3 Definition der Dienstkategorien

Mit Hilfe der Verkehrs- und Dienstqualitätsparameter werden die Dienstkategorien im folgenden genau definiert. Dabei hängt es von der jeweiligen Dienstkategorie ab, welche Parameter spezifiziert werden.

Constant Bit Rate (CBR) Benutzt eine Anwendung die *Constant Bit Rate* Dienstkategorie, wird ihr eine feste Menge an Bandbreite zugewiesen, die durch die *Peak Cell Rate* R_p bestimmt wird. Da die Bandbreite der Anwendung exklusiv zur Verfügung steht, darf diese jederzeit R_p Zellen pro Sekunde senden. Um Echtzeit-Anwendungen unterstützen zu können, werden die Dienstqualitätsparameter *Cell Transfer Delay*, *Cell Delay Variation* und *Cell Loss Ratio* spezifiziert.

Real-Time Variable Bit Rate (rt-VBR) *Real-Time Variable Bit Rate* Verbindungen werden durch die *Peak Cell Rate*, die *Sustainable Cell Rate* und die *Maximum Burst Size* charakterisiert. Vom Sender wird erwartet, daß er mit einer variablen Bitrate sendet. Auch bei der rt-VBR Dienstkategorie sind *CTD, CDV* und *CLR* Bestandteil der Spezifikation.

Non-Real-Time Variable Bit Rate (nrt-VBR) Auch für *Non-Real-Time Variable Bit Rate* Verbindungen ist burstartiger Verkehr typisch, der ebenfalls durch *PCR, SCR* und *MBS* charakterisiert wird. Anwendungen, die den ausgehandelten Verkehrsvertrag (siehe Abschnitt 4.1) einhalten, wird eine niedrige *Cell Loss Ratio* garantiert. Da nrt-VBR keine Unterstützung für Echtzeit-Anwendungen zur Verfügung stellt, sind keine Beschränkungen hinsichtlich der Verzögerung von Zellen (*CTD* und *CDV*) festgelegt.

Dienstkategorie	CBR	rt-VBR	nrt-VBR	UBR	ABR
PCR	•	•	•	•	•
SCR	—	•	•	—	—
MBS	—	•	•	—	—
MCR	—	—	—	—	•
CTD	•	•	×	×	×
CDV	•	•	×	×	×
CLR	•	•	•	×	(•)

Tabelle 2: Verkehrs- und Dienstqualitätsparameter der Dienstkategorien

Unspecified Bit Rate (UBR) Die *Unspecified Bit Rate* Dienstkategorie spezifiziert lediglich die *PCR* als Verkehrsparameter. Da keine Schranken im Hinblick auf Verzögerung und Zellverlust (*CTD, CDV* und *CLR*) festlegt werden, bietet UBR keinerlei Garantien an und ist somit auch nicht für Echtzeit-Anwendungen geeignet.

Available Bit Rate (ABR) Anwendungen, die die *Available Bit Rate* Dienstkategorie verwenden, haben Zugriff auf die momentan ungenutzte Bandbreite. Die von der Anwendung maximal benötigte Menge an Bandbreite wird auch hier durch die *Peak Cell Rate* R_p definiert, während die minimal akzeptable Zellrate durch die *Minimum Cell Rate* R_m festgelegt wird. So kann der Anwendung eine Zellrate garantiert werden, die aufgrund der variierenden Netzlast zwischen R_m und R_p schwankt. Dadurch bedingt können keine Garantien bezüglich der Zellübertragungsverzögerung und der Verzögerungsschwankung gegeben werden, weswegen weder *CTD* noch *CDV* spezifiziert werden. Echtzeit-Anwendungen werden demnach nicht unterstützt. In der Regel sollten ABR Verbindungen aber eine niedrige *Cell Loss Ratio* erreichen, damit die für ABR typischen Anwendungen möglichst zügig abgewickelt werden können. Ob die *CLR* spezifiziert wird, ist jedoch vom Netzwerk abhängig.

Tabelle 2 faßt zusammen, in welcher Dienstkategorie welche Parameter spezifiziert (•) bzw. nicht spezifiziert (×) bzw. nicht verwendbar (—) sind. Die Aufteilung der Bandbreite eines Mediums auf vier Verbindungen, von denen jede eine andere Dienstkategorie in Anspruch nimmt, ist in Abbildung 1 skizziert.

4 Mechanismen zur Diensterbringung

4.1 Der Verkehrsvertrag

Wenn eine Anwendung eine neue ATM-Verbindung aufbauen möchte, muß sie dem Netzwerk mitteilen, welche Anforderungen sie an die Dienstqualität dieser neuen Verbindung stellt. Diese Anforderungen werden durch die Dienstqualitätsparameter *CTD, CDV* und *CLR* beschrieben, die mit dem Netzwerk ausgehandelt werden. Weiterhin gibt die Anwendung dem Netzwerk die Eigenschaften des zukünftig zu erwartenden

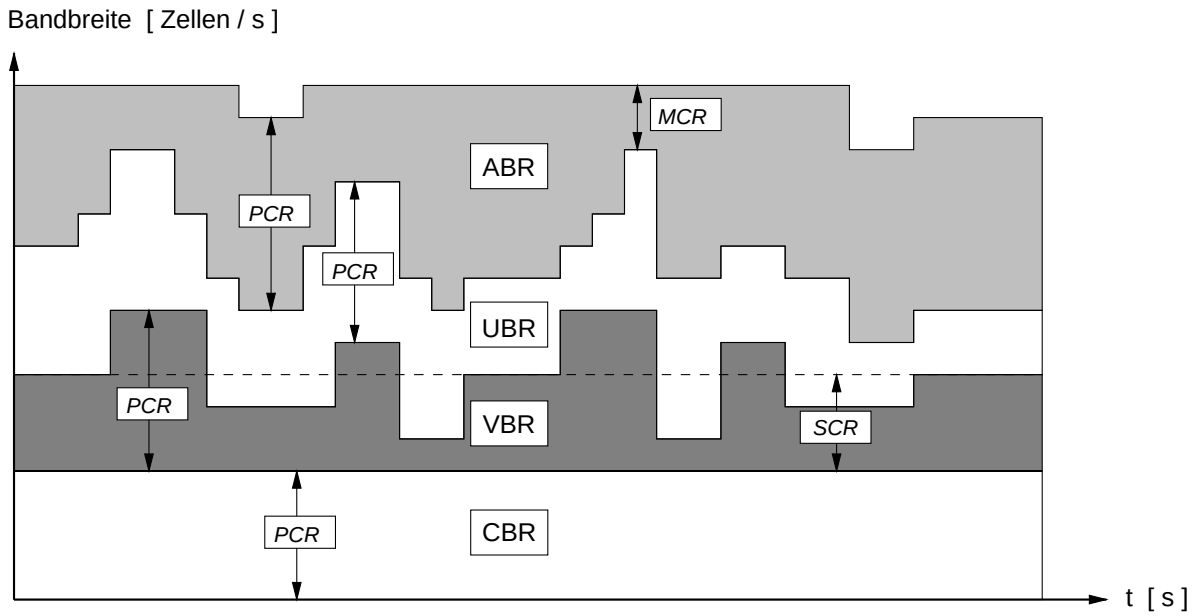


Abbildung 1: Aufteilung der Bandbreite auf vier ATM-Verbindungen

Zellenstromes in Form des *Source Traffic Deskriptors* bekannt. Im Source Traffic Deskriptor sind die Verkehrsparameter *PCR, SCR, MBS* und *MCR* zusammengefaßt. Gemeinsam mit der *CDVT* und der in Abschnitt 4.2 beschriebenen Definition der *Konformität* bildet er den *Connection Traffic Deskriptor*.

Der Connection Traffic Deskriptor und die Dienstqualitätsparameter sind Bestandteile eines *Verkehrsvertrages (Traffic Contract)*, der für jede Richtung der Verbindung zwischen Anwendung und Netzwerk ausgehandelt wird. In diesem Verkehrsvertrag verpflichtet sich das Netzwerk, die vereinbarte Dienstqualität zu garantieren, solange der von der Anwendung gesendete Zellenstrom die im Vertrag festgelegten Verkehrsparameter einhält.

4.2 Der Generic Cell Rate Algorithmus

ATM-Zellen, welche die Verkehrsparameter des Verkehrsvertrages einhalten, heißen *konforme Zellen*. Mit Hilfe des *Generic Cell Rate Algorithmus (GCRA)* wird festgestellt, ob eine Zelle konform ist. Eine Realisierung des GCRA als *Leaky Bucket Algorithmus* zeigt das Flußdiagramm in Abbildung 2.

Der Algorithmus arbeitet mit einem Zähler X sowie zwei Parametern, dem Inkrement I und dem Limit L. Falls bei Ankunft einer ATM-Zelle $X \leq L$ gilt, ist die Zelle konform und der Zähler wird um I erhöht. Im Fall $X > L$ wird die eingetroffene Zelle als nicht-konform eingestuft. In jedem Fall erniedrigt sich der Zähler X pro Zeiteinheit um 1, sofern er dabei nicht negativ wird. Dieses Dekrementieren des Zählers wird mit Hilfe von $t_a(k)$, dem Ankunftszeitpunkt der k-ten Zelle, und t_c, dem Ankunftszeitpunkt der letzten konformen Zelle, ausgedrückt. Wie der Name schon verrät, kann der Leaky Bucket Algorithmus als Eimer mit einem Fassungsvermögen von $L + I$ Litern aufgefaßt werden. Dieser Eimer ist mit X Litern Wasser gefüllt, von denen pro Zeiteinheit 1 ℓ durch ein Loch im Boden des Eimers ablaufen. Jede ankommende ATM-Zelle kann nun als eine Kanne angesehen werden, die I Liter Wasser enthält. Falls die gesamte

Wassermenge der Kanne noch in den Eimer passen würde, ohne daß dieser überläuft ($X \leq L$), wird sie in den Eimer geschüttet. Die mit der Kanne gedanklich assoziierte Zelle gilt dann als konform. Das Beispiel in Abbildung 3 verdeutlicht den Ablauf des Leaky Bucket Algorithmus. Hier wird $I = 4$ und $L = 2$ angenommen. Bei der Ankunft der ersten Zelle wird der Zähler X mit 0 und die Variable t_c mit $t_a(1)$ initialisiert, so daß im Beispiel $t_c = t_a(1) = 2$ gilt. Es ergibt sich, daß Zelle 1 konform ist, woraufhin X um I erhöht wird und somit den Wert 4 aufweist. Auch die zweite Zelle ist konform, da die Hilfsvariable X' das Limit L erreicht, jedoch nicht übersteigt. X wird wiederum um I erhöht und erhält den Wert 6. Außerdem wird t_c auf den Wert von $t_a(2)$ gesetzt, so daß nun $t_c = 4$ gilt. Da bei der dritten Zelle schließlich $X' = 3 > L$ gilt, wird diese als nicht-konform eingestuft. Die vierte Zelle dagegen wird wieder als konform erkannt, so daß nun $X = 6$ und $t_c = 8$ gilt.

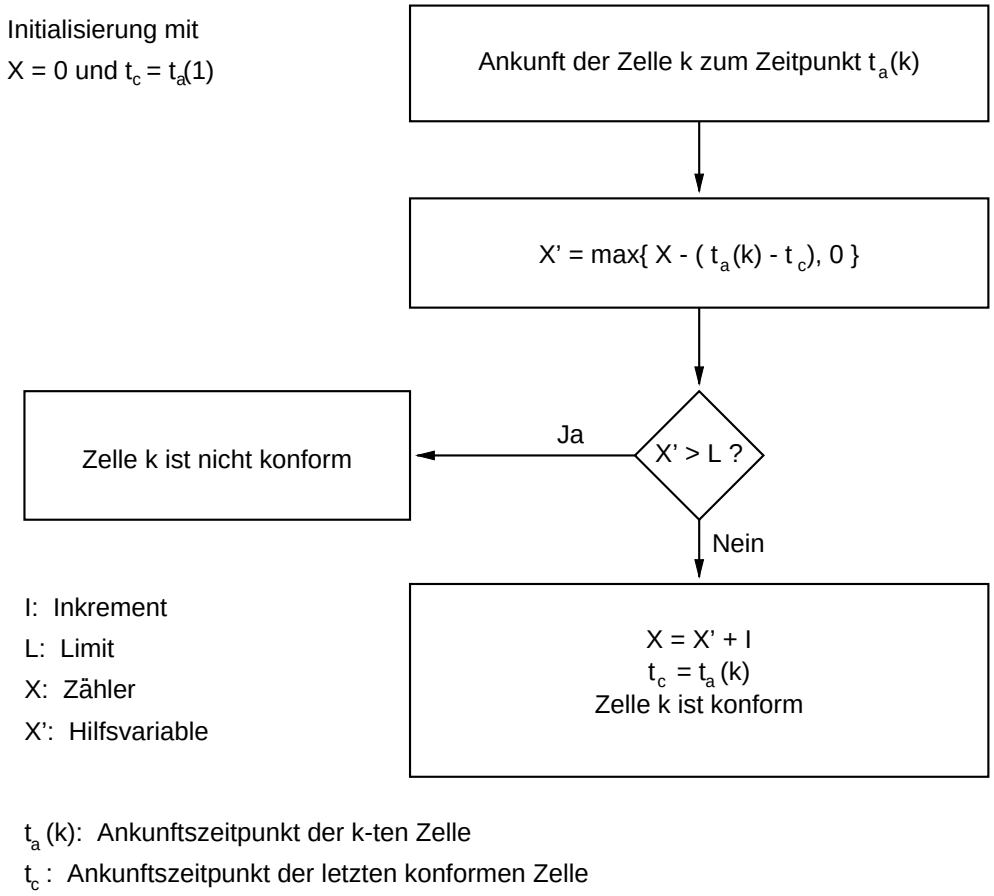


Abbildung 2: Flußdiagramm des Leaky Bucket Algorithmus

4.3 Verkehrs- und Staukontrolle

Unvorhersehbare Schwankungen im Verkehrsaufkommen oder Fehler innerhalb des Netzwerkes können eine Überlast im Netzwerk bewirken. Solche *Überlastsituationen* sind dadurch gekennzeichnet, daß das Netzwerk nicht mehr in der Lage ist, allen derzeit bestehenden Verbindungen die benötigte Menge an Ressourcen zur Verfügung zu stellen. Folglich kann nicht für jede Verbindung die vereinbarte Dienstqualität aufrechterhalten werden. Durch den Einsatz geeigneter Verkehrs- und Staukontrollmechanismen wird angestrebt, Anzahl und Dauer von Überlastsituationen möglichst gering zu

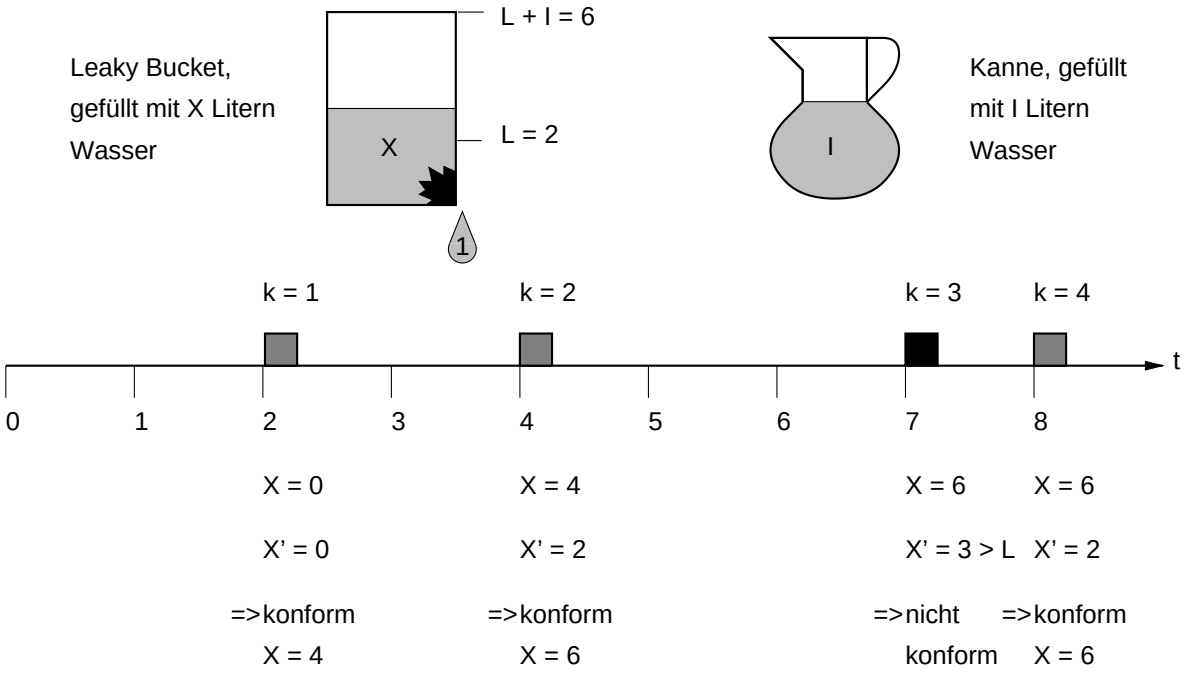


Abbildung 3: Beispielablauf des Leaky Bucket Algorithmus

halten. Aufgabe der *Verkehrskontrolle* ist es, durch präventive Maßnahmen die Überlastung des Netzwerkes zu vermeiden, während die *Staukontrolle* bei bereits bestehender Überlastsituation deren Auswirkungen begrenzen und den Stau beheben soll. Folgende Mechanismen werden vorgestellt:

- *Connection Admission Control (CAC)*,
- *Usage Parameter Control (UPC)*,
- *Prioritätskontrolle*,
- *Traffic Shaping*,
- *Ratenbasierte Flußkontrolle*.

Connection Admission Control (CAC) Die Maßnahmen, die das Netzwerk beim Verbindungsaufbau ergreift, um zu entscheiden, ob die Verbindung angenommen oder abgelehnt werden soll, heißen *Connection Admission Control*. Im Rahmen dieser Zugangskontrolle wird ein Verbindungsaufbauwunsch nur dann akzeptiert, wenn ausreichend Ressourcen in Form von Bandbreite und Pufferspeicher verfügbar sind, um der neuen Verbindung die geforderte Dienstqualität Ende-zu-Ende zuzusichern. Gleichzeitig muß auch sichergestellt sein, daß die vereinbarten Dienstqualitäten der bereits bestehenden Verbindungen nicht durch die neue Verbindung beeinträchtigt werden. Die für diese Entscheidung nötigen Informationen erhält die CAC aus dem Verkehrsvertrag. Da zur Garantie der Dienstqualität von CBR, rt-VBR oder nrt-VBR Verbindungen die benötigten Ressourcen vom Netzwerk reserviert werden müssen, ist die CAC beim Verbindungsaufbau erforderlich. Das gilt auch für ABR Verbindungen, die eine *Minimum Cell Rate* $R_m > 0$ fordern. Die Verwendung der CAC für UBR Verbindungen ist optional.

Usage Parameter Control (UPC) Würde eine Anwendung ihren Verkehrsvertrag nicht einhalten, nähme sie zusätzliche Netzwerk-Ressourcen, insbesondere die von anderen Verbindungen, in Anspruch. Da dies eine massive Einschränkung der Dienstqualitäten der anderen Verbindungen nach sich zöge, müssen die Netzwerk-Ressourcen vor derartigen Übergriffen geschützt und die ausgehandelten Verkehrsverträge durchgesetzt werden. Aus diesem Grund kontrolliert die *Usage Parameter Control* am User Network Interface (UNI) die vom Endsystem kommenden Zellenströme. Als Teil der UPC überwacht die sogenannte *Network Parameter Control (NPC)* die Verbindungen am Network Node Interface (NNI).

Die Überwachung des Zellenstromes einer Verbindung kann zum Beispiel mit Hilfe des Generic Cell Rate Algorithmus aus Abschnitt 4.2 geschehen. Konforme Zellen werden von der UPC normal weiterbefördert, während nicht-konforme Zellen entweder gekennzeichnet (tagged) oder verworfen (discarded) werden. Die Kennzeichnung einer nicht-konformen Zelle, geschieht durch das Setzen des *Cell Loss Priority (CLP) Bits* im Zellkopf und ist nur dann möglich, wenn das CLP Bit noch nicht gesetzt ist. Ist bei einer nicht-konformen Zelle das CLP Bit bereits gesetzt, so wird sie verworfen.

Prioritätskontrolle Die Aufgabe der *Prioritätskontrolle* besteht darin, weitestgehend zu verhindern, daß in einer Überlastsituation Zellen verworfen werden, die wichtige Nutzdaten transportieren, während Zellen mit weniger relevanten Nutzdaten erfolgreich übertragen werden. Durch gezieltes Setzen des CLP Bits kann die sendende Anwendung jeder Zelle eine Priorität zuordnen. Eine gesetztes CLP Bit macht eine Zelle zu einer niederprioren Zelle, deren Nutzdaten weniger wichtig sind. In Überlastsituationen werden diese Zellen von der UPC zuerst verworfen. Zellen, die wichtige Daten transportieren, sollten also als hochpriore Zellen mit gelöschtem CLP Bit gesendet werden. Droht bei der Ankunft einer derartigen hochprioren Zelle in einem ATM-Switch ein Pufferüberlauf, so kann eine Zelle mit niedriger Priorität aus dem Puffer verdrängt werden, um Platz für die neue hochpriore Zelle zu schaffen. Des weiteren besteht die Möglichkeit, Zellen mit hoher Priorität in den ATM-Switches bevorzugt weiterzuleiten, damit sie die Verzögerungsbeschränkungen besser einhalten können.

Traffic Shaping Durch den Einsatz von *Traffic Shaping* werden die Charakteristika des Zellenstromes einer Verbindung verändert, um die Effizienz des Netzwerkes zu erhöhen oder die Konformität des Zellenstromes zu sichern. Die Modellierung des Zellenstromes kann beispielsweise durch eine Verringerung der *Peak Cell Rate* oder eine Begrenzung der *Maximum Burst Size* erzielt werden. Weiterhin kann man die *Cell Delay Variation* einschränken, indem man die Zellen in angemessenen Abständen weiterleitet. Zu beachten ist jedoch, daß durch Traffic Shaping die Dienstqualität der Verbindung nicht beeinträchtigt werden darf und daß die Reihenfolge der Zellen erhalten bleiben muß. Die Orte, an denen Traffic Shaping eingesetzt wird, sind vom jeweiligen Netzwerk abhängig. Beispielsweise kann innerhalb eines sendenden Endsystems die Konformität des gesendeten Zellenstromes durch Traffic Shaping sichergestellt und so das Verwerfen von Zellen durch die UPC vermieden werden.

Ratenbasierte Flußkontrolle Die *ratenbasierte Flußkontrolle* sorgt dafür, daß der Sender einer ABR Verbindung *Feedback-Informationen* erhält, anhand derer er gegebenenfalls seine Senderate dynamisch an die Netzlast anpassen kann. Um diese

Informationen zu bekommen, fügt der Sender in regelmäßigen Abständen *Resource Management (RM) Zellen* in den Zellenstrom ein, die vom Empfänger zurückgeschickt werden. Sowohl der Empfänger als auch die Vermittlungsknoten können die RM-Zellen mit Feedback-Informationen bestücken und auch ihrerseits RM-Zellen generieren, um sie an den Sender zu schicken. Ein überlasteter oder voll ausgelasteter Vermittlungsknoten kann darüber hinaus das *Explicit Forward Congestion Indication (EFCI) Bit* im Zellkopf einer gewöhnlichen vorbeikommenden ATM-Zelle setzen, um dem Endsystem auf der Empfängerseite die Überlastung mitzuteilen. Dieses wird daraufhin unter Zuhilfenahme von RM-Zellen den Sender informieren.

Die dynamische Anpassung der Senderate geht folgendermaßen vor sich. Der Sender einer ABR Verbindung erhöht seine Senderate schrittweise bis auf maximal R_p Zellen pro Sekunde, bis ihm die RM-Zellen einen Stau melden. In diesem Fall und auch dann, wenn die RM-Zellen ganz ausbleiben, liegt offensichtlich eine Überlastung im Netzwerk vor, so daß der Sender seine Senderate schrittweise drosseln wird – notfalls bis auf R_m Zellen pro Sekunde. Sobald kein Stau mehr angezeigt wird, kann die Senderate wieder erhöht werden. Zusätzlich kann dem Sender die erlaubte Senderate auch explizit mitgeteilt werden.

5 Zusammenfassung

Da ATM-Netzwerke vielen verschiedenen Anwendungen eine geeignete Dienstqualitätsunterstützung bieten sollen, hat das ATM-Forum die Dienste in fünf Dienstkategorien eingeteilt. Die CBR Dienstkategorie unterstützt Echtzeit-Anwendungen mit konstanter Bitrate, wie sie zum Beispiel bei unkomprimiertem Video vorliegt. Die Notwendigkeit unkomprimierte Videoströme in Echtzeit zu übertragen und damit knappe Netzwerk-Ressourcen zu belegen, besteht bei der heutigen Kompressionstechnik fast nicht mehr, so daß viele Echtzeit-Anwendungen nach entsprechender Datenkompression mit der rt-VBR Dienstkategorie auskommen sollten. Dennoch hat auch die CBR Dienstkategorie ihre Existenzberechtigung. In Bereichen wie der Telefonie oder der Telemedizin könnte sich die geringe Zellverlustrate, welche die rt-VBR Dienstkategorie mit sich bringt, störend oder sogar gefährlich auswirken. Weiterhin ist es nicht allen Anwendungen möglich, ihre Daten entsprechend zu komprimieren. Als Beispiel seien wieder telemedizinische Anwendungen genannt. Schließlich ist die durch Kompression und Dekompression entstehende Verzögerung manchmal nicht mit den Echtzeit-Anforderungen einer Anwendung zu vereinbaren. In diesen Fällen kommt man also um den Einsatz von CBR nicht herum. Auch die Existenz der drei Dienstkategorien nrt-VBR, UBR und ABR für Anwendungen ohne Echtzeit-Anforderungen ist berechtigt. Während UBR keine Garantien bietet, kann bei ABR die minimal akzeptable Übertragungsrate und die Zellverlustrate festgelegt werden. Die nrt-VBR Dienstkategorie kann darüber hinaus durch Spezifikation der mittleren Zellrate eine gewisse Höchstdauer der Übertragung garantieren. Von den Qualitätsanforderungen und auch von den akzeptablen Kosten für die Verbindung hängt es ab, welche der drei letztgenannten Dienstkategorien eine Anwendung nutzt.

Jede der fünf Dienstkategorien hat also ihre Existenzberechtigung. Nach heutigen Maßstäben ist durch diese Klassifizierung allen denkbaren Telekommunikationsanwendungen eine geeignete Dienstqualitätsunterstützung gegeben. Dennoch ist die Einführung weiterer Dienstkategorien in Zukunft nicht ausgeschlossen.

Die optimale Ausnutzung der Dienste von ATM wird erst mit der Entwicklung von neuen Anwendungen erreicht werden, die von vorne herein auf die Nutzung der ATM-Technologie ausgerichtet sind. Der Zugriff auf das Netzwerk wird dann über ein ATM-basiertes *Application Programming Interface (API)* abgewickelt werden. Mit Hilfe des APIs können die Fähigkeiten der ATM-Technologie zukünftig kostengünstig nutzbar gemacht werden, so daß die Vorteile, die ATM im Vergleich zu anderen Technologien mitbringt, deutlich hervortreten werden.

Literatur

[DePr95] Martin DePrycker. Traffic Control in ATM Networks. In *Asynchronous Transfer Mode – Solution for Broadband ISDN*, Kapitel 7. Ellis Horwood, 2. Auflage, 1995.

[DePr96] Martin DePrycker. *Asynchronous Transfer Mode.* Prentice Hall Verlag, München. 3. Auflage, 1996.

[Foru96a] The ATM Forum. ATM Service Categories: The Benefits to the User. White Paper, The European Market Awareness Committee, Mai 1996.

[Foru96b] The ATM Forum. Traffic Management Specification Version 4.0. Technical Specification, Technical Committee, April 1996.

[Garr96] Mark W. Garrett. A Service Architecture for ATM: From Applications to Scheduling. *IEEE Network*, Mai/Juni 1996, S. 6 – 14.

[Gora95] Walter J. Goralski. *Introduction to ATM Networking.* McGraw-Hill, New York. 1995.

[Jung96] Jae-Il Jung. Quality of Service in Telecommunications. *IEEE Communications Magazine*, August 1996, S. 108 – 117.

[Kyas95] Othmar Kyas. *ATM-Netzwerke: Aufbau, Funktion, Performance.* DATACOM Buchverlag, Bergheim. 2. Auflage, 1995.

[McSp95] David E. McDysan und Darren L. Spohn. *ATM: Theory and Application.* McGraw-Hill, New York. 1995.

Abbildungsverzeichnis

Tabellenverzeichnis

Qualitätsbasiertes Routing im Internet

Zhenbo Wang

Kurzfassung

Die im Internet immer häufiger auftretenden modernen Anwendungen verlangen gewisse Garantien bei der Dienstqualität, z.B. ist die Durchführung einer Telekonferenz nur dann sinnvoll, wenn die Verzögerung unter einem bestimmten Maximalwert liegt. Das Internet Protokoll IP wurde für eine bestmögliche Datenübertragung („best-effort“) entwickelt und bietet keine Garantie der Dienstqualität. Um die Dienstqualitätsanforderungen im Internet zu unterstützen, ist es notwendig, das Internet-Routing um Aspekte der Dienstqualität zu erweitern. Beim QoS(Quality of Service)-Routing geht es darum, Wege, die geforderten Qualitäten (z.B. Bandbreite, Verzögerung usw.) erfüllen, im Internet zu finden und zu verwalten. In diesem Beitrag werden einige Anforderungen an das qualitätsbasierte Routing beschrieben. Die während der Entwicklung entstandenen Fragen werden diskutiert. Ein Rahmenwerk zum qualitätsbasierten Routing wird vorgestellt. Das bereits existierende Routingprotokoll OSPF (Open Shortest Path First) wird um Aspekte der Dienstqualität erweitert.

1 Einführung

Die bis heute existierenden Routingprotokolle konzentrieren sich meistens nur auf die Topologie des Netzwerkes und berücksichtigen dabei die Auslastung von Netzwerkressourcen (wie Bandbreite) nicht. Deshalb sind sie nicht zur Unterstützung von Datenverkehr mit Dienstqualitätsanforderungen geeignet. Folgendes Beispiel wird diese Ansicht demonstrieren:

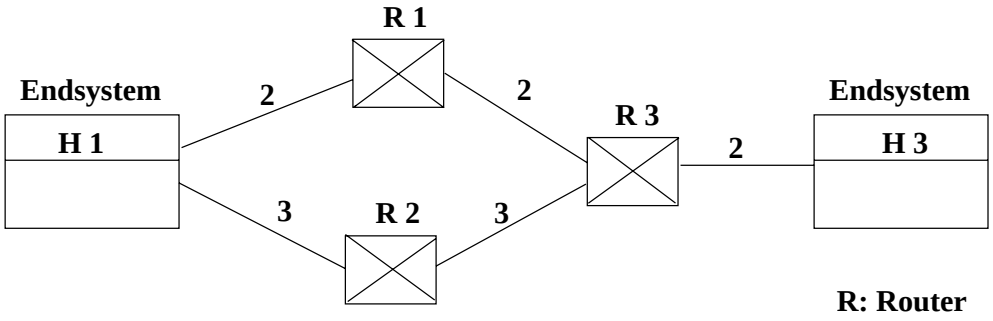


Abbildung 1: Ein einfaches Routing Beispiel.

Angenommen Endsystem H1 sendet Daten mit einer Datenrate von 100 kbit/s zu Endsystem H3. Das Routingprotokoll z.B. OSPF berechnet den kürzesten Weg zum

Ziel anhand der Netz-Topologie: H1→R1→R3→H3. Ein Problem tritt auf, wenn der Router R1 nicht genügend Ressourcen an seinem Anschluß zu Router R3 hat, um die Anforderung von 100 kbit/s zu erfüllen. Der Weg H1→R2→R3→H3, der zwar die Anforderung von 100 kbit/s befriedigen kann, wird nicht benutzt, weil das Routingprotokoll nur den kürzesten Weg betrachtet. Die Grundidee solche Protokolle zu verbessern ist, daß die Routingprotokolle zusätzlich die Ressourceninformationen neben der Topologieinformation bei der Wegewahl betrachten. Damit bilden Topologie und Ressourceninformation des Netzes die zwei entscheidenden Faktoren beim qualitätsbasierten Routing. Bei der erweiterten Version von OSPF– QOSPF (Quality Open Shortest Path First) wird für die Verbindung dann bei obigem Beispiel der passende Weg H1→R2→R3→H3 gesucht. Man sieht, der jetzt ausgesuchte Weg ist nicht mehr der kürzeste Weg, aber er hat die nötigen Ressourcen für die geforderte Qualität der Verbindung.

Um allgemeine Qualitätsanforderungen wie eine garantierte minimale Bandbreite und maximale Verzögerung zu unterstützen, sollen die folgenden Erweiterungen im Internet repräsentiert werden [RaNa96]:

1. neue zusätzliche Dienstklassen neben der „best-effort“ Dienstklasse, um gewisse Garantien bei Durchsatz und Verzögerung für die Anwendung sicherzustellen.
2. ein Mechanismus, der erlaubt, daß die Anwendungen dem Netzwerk ihre Dienstqualitätsanforderungen signalisieren.
3. Mechanismen für das Verkehrsmanagement in den Endsystemen und Routern.

Die IETF(Internet Engineering Task Force) hat bereits erste Ergebnisse zu den beiden ersten Anforderungen erarbeitet. Zusätzliche Dienstklassen neben der „best-effort“ Dienstklasse und ein Ressourcenreservierungsprotokoll (RSVP) wurden definiert. RSVP wird benutzt, um die Ressourcen des Netzwerkes zu reservieren und dadurch die gewünschten Dienste zu erlangen. Die Anforderung an das Verkehrsmanagement wird auch von Firmen, die sich mit Netzwerkaspekten beschäftigen, entwickelt.

Mit der qualitätsbasierten Internet-Routing-Architektur sollen qualitätsorientierte Wege im Internet für Verbindungen in Bezug auf die gegenwärtige Topologie und Verkehrssituation dynamisch gefunden werden. Bei einer solcher Routing-Architektur ist die Wegewahl für eine Verbindung sowohl von Netzwerk-Zustandsinformationen (z.B. die verfügbare Bandbreite bei verschiedenen Links) als auch von Qualitätsanforderungen der Verbindung abhängig. Die qualitätsbasierte Routing-Architektur ist gut geeignet für eine effiziente Nutzung der Ressourcen und daraus folgt ein vorteilhaftes Netzwerk-Engineering.

Es ist offensichtlich nicht wirtschaftlich, ausschließlich die Ressourcen im Netzwerk auszubauen, um die Dienstqualitätsanforderungen zu befriedigen. Man soll auch sich bemühen, die effiziente Nutzung der Ressourcen zu erziehen. Öffentliche oder private Netzwerkbetreiber verlangen zum Beispiel, maximalen Datenverkehr unter minimaler Ressourcenauslastung zu erzielen. Unter folgenden Umständen, wird ein QoS-Routing benötigt:

- Erstens: ohne QoS-Routing, verteilen Protokolle wie RSVP (Resource Reservation Protocol) zwar die Dienstqualitätsanforderungen an die Router, aber es wird

nicht garantiert, daß ein passender Weg zwischen Sender und Empfänger gefunden und benutzt wird.

- Zweitens: ein qualitätsbasiertes Routing-Verfahren ist viel ökonomischer, d.h. beim qualitätsbasierten Routing werden Ressourcen effizienter benutzt als beim traditionellen Routing (z.B. IP-Routing). Mit einem zustandsabhängigen Routing wird mehr Datenverkehr und höhere Leistung geschaffen im Vergleich zu einem zustandsunabhängigen Routing.

Qualitätsbasiertes Routing soll deswegen als eine wesentliche Komponente im Rahmenwerk des Internets integriert sein, um die Qualitätsanforderungen der Anwendungen zu unterstützen.

2 Anforderungen an qualitätsbasiertes Routing

Der erste Schritt bei der Entwicklung einer qualitätsbasierten Routing-Architektur betrachtet die Anforderungen, die unbedingt befriedigt werden müssen. Wir betrachten am Anfang nur die folgenden zugrundeliegenden Anforderungen:

Metrik

- Unterstützung für mehrere Metriken (Bandbreite, Verzögerung usw.).
- Die Fähigkeit zur dynamischen Bestimmung eines Weges, der die Anforderungen (z.B. Bandbreite und Verzögerung) befriedigen kann.
- Die Dienstqualität soll auch verschiedene Typen von Verbindungen unterstützen: Unicast und Multicast.
- Unterstützung für heterogene Dienstqualitätsanforderungen von Empfängern.

Robustheit

- Die Fähigkeit zur Entdeckung von dynamischen Änderungen der Ressourcenkapazität eines Links und geeignete Reaktionen.
- Die Fähigkeit zur Weiterführung des Wegewahl-Prozesses trotz mehrfachen Mißerfolgen.

Effizienz

- Die Fähigkeit zur Schaffung einer Verbindung für einen kurzlebigen (short-lived) Datenaustausch mit minimalem Aufwand.
- Die Fähigkeit zur effizienten Benutzung der Netzwerkressourcen durch die Verteilung der Verkehrslast und eine globale Zugangskontrolle.
- Minimierung der allgemeinen Kosten für das Routing.

- Unterstützung der Ressourcenkontrolle, d.h. die Fähigkeit zur Begrenzung des Ressourceverbrauchs für verschiedene Verkehrsklassen.

Skalierbarkeit und Priorität

- Routing in einem Netzwerk mit einer umfangreichen Menge von Links und Knoten oder in einem Netzwerk mit großer Reichweite.
- Unterstützung für priorisierte Verbindungen, d.h. Verbindungen mit höherer Priorität sollen mit Vorrang aufgebaut werden gegenüber denen mit niedrigerer Priorität.

Interdomain-Routing

- Bei diesem Bereich soll man sich einige Gedanken über die Anforderungen an das Interdomain-Routing machen. Welche Informationen sollen an der Grenze zwischen zwei administrativen Domainen ausgetauscht werden? Diese Frage muß sorgfältig beantwortet werden. Auf jeden Fall soll eine Strategie eingeführt werden, um den Austausch der Routing-Informationen zwischen zwei Organisationen einzuschränken.

Ein aus solchen Anforderungen resultierendes Routing ist höher entwickelt als das bisherige Internet-Routing. Im nächsten Abschnitt möchten wir einige Probleme, die bei der Realisierung der qualitätsbasierten Internet Routing-Architektur auftreten, diskutieren.

3 Probleme beim qualitätsbasierten Routing

3.1 Informationsverbreitung

Beim Link-State-Routing hält jeder Knoten die Informationen über die Topologie des Netzes und berechnet daraus beispielsweise die kürzesten Wege für die Verbindung – typischerweise mit dem Verfahren von Dijkstra. Um die Anforderung an die Dienstqualität zu berücksichtigen, muß jeder Router zusätzlich die Verfügbarkeit der direkt verbundenen Links und seine eigene Ressourcenverfügbarkeit überwachen. Das Link-State-Routing erfordert, daß die Router ihren lokalen Ressourcenzustand (z.B. verfügbare Linkkapazität, Verzögerung usw.) und die lokale Topologieinformation durch das ganze Netzwerk verbreiten. Viele Routingprotokolle fluten die Informationen, um Änderungen periodisch zu verbreiten. Da diese Information von allen Knoten nach einer gewissen Verzögerung bei einem neuen Knoten eintrifft, kennt er dann die komplette Topologie und den Zustand des Netzwerks. Die Verbreitung von Zustandsinformationen kann hohen Kommunikations- und Berechnungsaufwand verursachen. Für ein effizientes qualitätsbasiertes Routing ist ein solches Fluten der Information nicht gut geeignet. Als alternative Technik wird z.B. ein baumbasiertes Vorwärts-Verfahren vorgeschlagen, um den Verbreitungsaufwand zu reduzieren. Falls die Zustandswerte der Links sich innerhalb einer kurzen Periode sehr schnell ändern. Die Änderungen sollen dann besser quantisiert werden, um die Quote der Verbreitungen zu reduzieren. Es ist klar, daß, je ungenauere Informationen beim Router vorhanden sind, desto unwahrscheinlicher ein geeigneter Weg gefunden wird. Aber für die Beschaffung sehr genauer Informationen bei den Routern muß man auch hohen Aufwand in Kauf nehmen.

3.2 Algorithmus für einen Unicast-Weg

Seien die Zustandsinformationen von jedem Router bekannt, wie sollen dann die Wege für Unicast-Verbindungen berechnet werden? Die Berechnung eines „passenden" Weges für eine gegebene Verbindung ist nicht schwer: Jeder Router eliminiert alle unpassenden Links und Knoten, d.h. die die angeforderten Qualitäten nicht unterstützen können, von seiner lokalen Repräsentation der Netzwerktopologie. Mit dieser geänderten Topologie wird dann ein Ende-zu-Ende-Weg kalkuliert. Aber bei der Untersuchung von leitungsvermittelten Netzwerken hat sich gezeigt, daß solche Routingentscheidungen sogar im Fall einer limitierten Topologie inakzeptabel sind. Mit diesem Algorithmus werden weniger Verbindungen im Netz zugelassen als eigentlich möglich sind. Außerdem gibt es manchmal Informationsverlust bei der Aggregation der Zustandsinformationen, womit die richtige Routingentscheidung verhindert wird.

Ein Routing-Verfahren mit „lokaler Zugangskontrolle" wird von der Arbeitsgruppe Integrated Services IETF definiert. Das Routing-Verfahren bestimmt den Weg für eine Verbindung, solange die Zugangskontrollkriterien jedes auf dem Weg stehenden Routern der Verbindung passen. Diese Art von Zugangskontrolle berücksichtigt nur die Ressourcen bei jedem einzelnen Router, und nimmt keine Rücksicht auf den globalen Ressourcenverbrauch. Um mehr Effizienz beim Routing zu erzielen, soll eine zusätzliche Schicht für Zugangskontrolle („Higher Level Admission Control") implementiert werden. Diese sogenannte höhere Schicht für die Zugangskontrolle betrachtet die Ressourcenanforderungen von jeder Verbindung und die verfügbaren Ressourcen. Dann entscheidet sie, ob es in Bezug auf die gesamte Sicht günstig ist, eine Verbindung aufzunehmen. Deshalb kann eine einzelne Verbindung vielleicht abgelehnt werden, obwohl ein passender Weg dazu existiert. Denn das System findet, daß durch die Aufnahme dieser Verbindung die gesamte Anzahl der förderbaren Verbindungen verringert wird.

Die Wegewahl für eine Verbindung mit mehreren Anforderungen an die Dienstqualität ist ein schwieriges Problem. In der Tat ist für manche Kombinationen mit Anforderungen an die Dienstqualität das Problem bereits NP-vollständig. Algorithmen werden vorgeschlagen, wie ein Weg mit Anforderungen an Bandbreite und Verzögerung berechnet werden kann [WaCr96].

3.3 Prioritäten

Wenn eine kritische Verbindung höherer Priorität als andere Verbindungen bewilligt wird, so muß ein Mechanismus im Netzwerk implementiert sein, um die Priorität zu erkennen. Hier wird angenommen, daß das Reservierungsprotokoll (RSVP) die Priorität der Verbindung signalisieren kann. Es gibt zwei Aspekt bei der Priorisierung.

1. Es muß eine Strategie vorhanden sein, um zu entscheiden, welcher Benutzer welche Prioritäten für seine Verbindungen setzen kann?

2. Eine Verbindung mit höherer Priorität soll gewisse Vorteile haben gegenüber einer mit niedrigerer Priorität bezüglich der Erfüllung von Dienstqualitätsanforderungen.

Der Routing-Mechanismus zur Implementierung der Priorität basiert auf der Kombination von Verdrängung und dynamischem Rerouting der Verbindung mit niedrigen

Priorität. Ein Beispiel: Ein Router versucht bei der Wegewahl für eine gegebene Verbindung zuerst einen Weg zu finden, der genügend Ressourcen für die Dienstqualitätsanforderung der Verbindung besitzt. Wenn es nicht klappt, versucht der Router dann, eine Verbindung mit niedrigerer Priorität zu verdrängen, damit die freigegebenen Ressourcen für die Verbindung mit höherer Priorität genutzt werden können. Somit wird ein passender Weg für die Verbindung mit höherer Priorität gefunden. Der Router versucht dann mit derselben Prozedur Wege für die verdrängten Verbindungen zu finden.

3.4 Ressourcenkontrolle

Sind mehrere Dienstklassen vorhanden, so ist es nötig, den Verkehrsbedarf jeder Dienstklasse zu bestimmen. Zu diesem Zweck, soll der Administrator des Netzwerkes die Ressourcen der Router und Links auf die verschiedenen Dienstklassen aufteilen. Aus einer zu strengen Aufteilung resultiert vielleicht eine ineffiziente Nutzung der Ressourcen des Netzwerkes, weil es vorkommen kann, daß bei einer Dienstklasse übermäßiger Datenverkehr und zugleich bei einer anderen Dienstklasse nur wenig Verkehr herrscht. Deshalb ist es wünschenswert, die freien Ressourcen dem Datenverkehr zuzuteilen, der solche Ressourcen dringend braucht. Diese Art von gemeinsamer Benutzung der Ressourcen soll nur vernünftig kontrolliert werden, um zu vermeiden, daß einige Dienstklassen die nicht ihnen gehörenden Ressourcen für lange Zeit benutzen und dadurch den Datenverkehr anderer Dienstklassen verhindern. Solche Kontrollen sind Aufgabe des Routings. Bei dem Routing-Verfahren sollen die „lokale Ressourcen aufteilung“ und „gemeinsame Nutzung der Ressourcen” implementiert werden. Das Design eines geeigneten Routing-Verfahrens und wie ein solches Verfahren ins qualitätsbasierte Routing integriert werden soll, braucht noch weitere Forschungsarbeit.

3.5 Qualitätsbasiertes Routing für Multicast-Verbindung

Die Berechnung qualitätsbasierter Wege für Multicast-Verbindungen ist ein kompliziertes Problem, besonders wenn „Higher Level Admission Control “ noch einbezogen ist. Die dynamische Änderung der Empfängermenge und die Heterogenität der Empfänger machen das Problem schwierig. Bei der Erweiterung von MOSPF (Multicast Extension of Open Shortest Path First) zu QMOSPF, ist das wesentliche Problem die Skalierbarkeit.

Die Ziele von qualitätsbasiertem Routing für Multicast-Verbindungen sind folgende:

1. Skalierbarkeit für große Gruppe mit dynamischer Mitgliedschaft.
2. Robustheit bezüglich der Änderung der Topologie.
3. Unterstützung empfängerinitiierten, heterogenen Reservierungen.
4. Unterstützung gemeinsamer Reservierungen.
5. Unterstützung einer globalen Zugangskontrolle, d.h. die administrative Kontrolle für den Ressourcenverbrauch bei Multicast-Verbindungen.

Ein mögliches Modell für Multicast-Verbindungen operiert folgendermaßen: Der Sender benachrichtigt periodisch seine Empfänger über die Charakteristik des Datenverkehrs. Nach dem Empfang der Nachrichten generiert ein Empfänger eine Nachricht zur Reservierung der Ressourcen entlang des ganzen Weg der Verbindung. Andere Modelle sind auch möglich, aber das oben vorgestellte Modell entspricht dem gegenwärtigen RSVP-Modell.

Das Multicast-Routing versucht einen Weg vom Sender zu jedem Empfänger zu finden, der die Reservierungsanforderungen erfüllen kann. Das Routing versucht vielleicht gleichzeitig die Nutzung der Netzwerkressourcen zu maximieren und die gesamt zugeteilte Bandbreite für die Multicast-Verbindung zu minimieren, oder andere Merkmale zu optimieren.

4 Bestimmung der Dienstqualität und Ressourcenreservierung

Für moderne multimediale Anwendungen ist es hilfreich, die Anforderungen an die Dienstqualität zu signalisieren, auszuhandeln und die benötigten Ressourcen zu reservieren. So kann den Anwendungen der gewünschte Dienst garantiert werden. Das qualitätsbasierte Routing-Modell hat einige Implikationen auf die Signalisierung. Unter diesem Routing-Modell müssen die verlangten Dienstqualitäten der Verbindung spezifiziert werden bevor ein geeigneter Weg dafür gewählt wird. Im Gegensatz dazu, wird bei RSVP zuerst ein Weg zugrundegelegt, dann werden die Ressourcen reserviert. Das RSVP benutzt eine PATH-Nachricht, um die Empfänger über die Kommmunikationssitzung und die Charakteristik des Datenverkehrs zu benachrichtigen und Zustandsinformation in den Routern zu erstellen. Beim qualitätsbasierten Routing ist die letzte Funktion nicht nützlich, weil die Wegewahl nur von den Empfängeranforderungen abhängig ist. Kombiniert man das gegenwärtige RSVP-Modell und das qualitätsbasierte Routing, dann wird bei dem Aufbau einer Unicast-Verbindung verlangt, daß eine PATH-Nachricht von dem Sender zum Empfänger entlang des „best-effort“ Weges gesendet wird. Der Empfänger sendet eine RESERVE-Nachricht nachdem ein geeigneter Weg erfolgreich gefunden wurde.

Der Weg für eine Multicast-Verbindung unter der gegenwärtigen RSVP-Spezifikation ist der IP(Internet Protokoll)-Multicastbaum. Um Wünsche nach einer bestimmten Dienstqualität zu äußern, muß jeder Empfänger eine RESERVE-Nachricht in die Richtung der Wurzel des Baums senden. Unterwegs sollen die Link- und Routerressourcen reserviert werden. Dieses Verfahren erstellt den Multicastbaum unabhängig von den Dienstqualitätsanforderungen. Deswegen wird es keine Garantie dafür geben, daß der Empfänger die Ressourcen erfolgreich reservieren kann, um die gewünschte Dienstqualität zu bekommen.

Eine mögliche Lösung für qualitätsbasiertes Multicast-Routing ist, daß die für die PATH-Nachricht benutzten Verbindungen und die für den späteren Datentransport benutzten Verbindungen getrennt werden sollen, d.h. sie laufen nicht unbedingt auf demselben Weg.

Eine andere Methode kann den Multicastbaum schon mit Hilfe von den in der PATH-Nachricht erhaltenen Informationen bestimmen. Das bedeutet, der Verbindungsbaum

wird durch die Kenntnis über die Empfängermenge und die dazu angenommene maximale Ressourcenreservierung bei jedem Router aufgebaut. Ein möglicher Nachteil einer solchen Methode ist, daß ein Verbindungsbaum nicht gefunden wird, obwohl es möglich ist. Die Ursache ist, daß die angenommene maximale Reservierung höher als die tatsächlich von dem Empfänger gewünschte Reservierung ist.

Wir sehen, daß das RSVP-Modell nicht reibungslos mit qualitätsbasierten Routing zusammenarbeitet. Wie dieses Problem gelöst wird, ist noch eine offene Frage.

5 Intradomain-Routing und Interdomain-Routing

5.1 Intradomain-Routing

Es gibt mehrere Vorschläge dazu, wie das qualitätsbasierte Routing innerhalb einer Domain realisiert werden kann. Diese reichen von On-Demand-Wegekalkulation, welche auf der aktuellen Zustandsinformationen basiert, bis zu angebotenen Wegen für bestimmte Dienstklassen. Zusätzliche Aspekte zur Leistungsoptimierung führen zu verschiedenen Lösungskonzepten. Jenachdem welche Technik benutzt wird, kann das Intradomain-Routing sowohl sehr hoch entwickelt als auch sehr einfach sein. Übrigens sind die geförderten Dienstklassen sowie die unterstützten Dienstqualitäten für die jeweilige Dienstklasse auch von Domain zu Domain verschieden. Wichtig ist daher, wie Anforderungen auf einer höheren Ebene für Intradomain-Routing bestimmt werden sollen, damit sowohl das qualitätsbasierte Routing im Internet unterstützt wird als auch die maximale Autonomie bei der Entwicklung des Lösungskonzepts erlaubt ist.

Es muß eine minimale Menge von Anforderungen geschaffen werden, damit sich das Intradomain-Routing zum qualitätsbasierten Routing entwickeln kann [CNRS96]:

1. Das Routing-Verfahren muß entweder einen der Dienstqualität entsprechenden Weg für eine Verbindung bereitstellen, oder darauf hinweisen, daß wegen gewisser Gründe der verlangte Weg nicht verfügbar ist und damit die Verbindung nicht aufgebaut werden kann.

2. Das Routing-Verfahren muß Probleme auf dem aktuellen Weg anzeigen, wenn beispielsweise die Netztopologie sich ändert.

3. Das Routing-Verfahren muß bestmögliche Verbindungen ohne jede Signalisierungsanforderung bedienen. Das heißt, bestmögliche Anwendungen und Protokolle können ohne jede Änderung mit einem qualitätsbasierten Intradomain-Routing benutzt werden.

4. Das Routing-Verfahren soll qualitätsbasiertes Multicasting unterstützen, welches heterogene Empfänger und eine „gemeinsame Reservierung“ erlaubt.

Zusätzlich sind die folgenden Eigenschaften auch zu empfehlen:

- Die Fähigkeit zur Optimierung der Ressourcenbenutzung.
- Implementierung einer Zugangskontrolle auf einer höheren Ebene, um die Nutzung der gesamten Ressourcen für die einzelne Verbindung zu beschränken.

5.2 Interdomain-Routing

Das Interdomain-Routing-Modell ist in Abbildung 2 gezeigt:

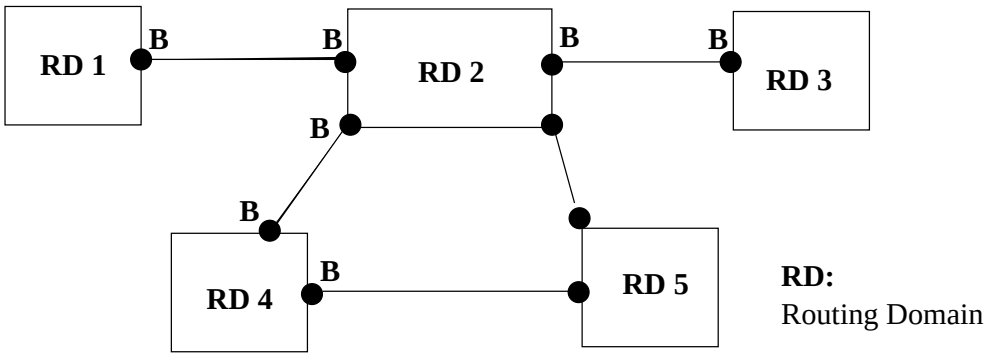


Abbildung 2: Das Interdomain-Routing-Modell.

Domainen tauschen die standardisierten Routinginformationen durch die Randknoten B aus. In diesem Modell kann jede Domain selbst wieder aus mehreren Domainen bestehen, d.h. das Interdomain-Routing-Modell besitzt eine hierarchische Struktur. Und jede auf der tiefsten Ebene liegende Domain basiert auf dem qualitätsbasierten Intradomain-Routing. Bei einer solcher Struktur entstehen folgende Fragen [CNRS96]:

1. Welche Informationen sollen zwischen den Domainen ausgetauscht werden?
2. Wie sind die externen Routinginformationen innerhalb einer Domain repräsentiert?
3. Wie werden die Interdomain-Wege kalkuliert?
4. Welche Art von Kontrolle soll bei der Interdomain-Wegewahl benutzt werden?
5. Wie wird das qualitätsbasierte Multicast-Routing auf der Interdomain-Ebene realisiert?

Auf einer hohen Ebene ist die Antwort zu diesen Fragen abhängig von dem Routing-Paradigma. Besonders wenn wir über das Paradigma des Link-State-Routings nachdenken, besteht der Informationsaustausch zwischen Domainen aus abstrakten Repräsentationen von den Domainen in Form von logischen Knoten und Links und der dazuhörigen Eigenschaften und Ressourcenauslastung. Die hierarchische Struktur der Domain kann auch durch eine hierarchische Link-State-Repräsentation mit geeigneter Aggregation der Metriken dargestellt werden.

Link-State-Routing ist nicht unbedingt vorteilhaft für das Interdomain-Routing aus folgenden Gründen:

1. Ein Vorteil des Intradomain-Link-State-Routings ist, daß die detaillierten Link-State-Informationen benutzt werden, um die Wege nach den angeforderten Qualitäten zu berechnen. Die Aggregation von Zustandsinformation und Metriken beim Interdomain-Routing schwächt diesen Vorteil wesentlich.

2. Domainen wollen vielleicht keine Details über ihre interne Topologie oder die Verfügbarkeit ihrer Ressourcen bekannt zu machen.

3. Skalierbarkeit beim Interdomain-Routing kann nur dann erreicht werden, wenn der Informationsaustausch zwischen Domainen relativ selten ist. Deshalb sieht es praktisch so aus, daß der Informationsaustausch zwischen Domainen so weit wie möglich begrenzt werden soll.

Aus der Beschränkung des Informationsaustausches zwischen Domainen resultiert die Einfachheit und die Skalierbarkeit des Routings. Der Informationsaustausch soll gewisse Basisfunktionen ermöglichen:

1. Bestimmung der Erreichbarkeit verschiedener Ziele.

2. Ein schleifenfreier Weg für die Verbindung.

3. Aggregation von Adressen wenn möglich.

4. Bestimmung der Dienstqualität, die der Weg besitzen soll.

5. Bestimmung mehrerer optionalen Wege für ein gegebenes Ziel basierend auf der Dienstklasse.

Diese Eigenschaften werden durch die Benutzung von qualitätsbasierten Wegevektoren, Link-State-Verfahren oder anderen Interdomain-Routing-Verfahren realisiert. Die Kernfrage beim Interdomain-Routing ist vor allem, welche (minimale) Information zwischen verschiedenen Domainen ausgetauscht werden soll, damit ein Ende-zu-Ende qualitätsbasiertes Routing realisiert werden kann. Neben dieser Frage sollen weitere Anforderungen befriedigt werden, um die qualitätsbasierte Interdomain-Routing-Architektur aufzubauen.

6 OSPF(Open Shortest Path First)-Erweiterung

6.1 Netzwerk-Ressourceninformation

OSPF (Open Shortest Path First) ist ein Link-State-Verfahren. Bei diesem Verfahren speichert jeder Knoten die vollständige Topologie des Netzes und er berechnet daraus lokal die kürzesten Wege. Beim qualitätsbasierten OSPF wird ein Weg für eine Verbindung basierend auf der Topologie, der Netzwerk-Ressourceninformation und der Anforderung an die Dienstqualität berechnet. Bei einem von QOSPF ausgesuchten Weg wird die Dienstqualitätsanforderung einer Verbindung unterstützt, aber es ist nicht unbedingt der kürzeste Weg.

Die Netzwerk-Ressourceninformation besteht aus den verfügbaren Link-Ressourcen und den existierenden Reservierungen bei einem Router. Diese Ressourceninformation wird gesendet in Form von Link-Resource-Advertisements (RES-LSAs) und Resource-Reservation-Advertisements (RRAs) [ZSSC96].

Es ist ungünstig, bei jeder Änderung der Ressourcenverfügbarkeit eine neue RES-LSA-Nachricht zu generieren, unabhängig davon ob diese Änderung überhaupt Einfluß auf

den Datenverkehr hat. Daher muß ein Algorithmus geschaffen werden, der nur bei einer wichtigen Änderung eine neue RES-LSA-Nachricht erzeugt. Die Resource-Reservation-Advertisement-Nachricht (RRA) beschreibt die Ressourcenreservierung bei einem Router für eine bestimmte Verbindung (Quelle, Ziel). Die RRAs sind besonders bei der neuen Berechnung des Verbindungsbaums für die Verbindung hilfreich. Eine neue RRA-Nachricht wird generiert, wenn eine oder mehrere Reservierungen sich geändert haben.

6.2 Wegewahl

Bei QOPSF basiert die Berechnung eines qualitätsbasierten Weges für eine Verbindung auf der Quelladresse, der Zieladresse und Anforderungen an Dienstqualität, unabhängig davon ob es sich um Unicast oder Multicast handelt. Im Gegensatz dazu basiert Unicast-OSPF auf der Zieladresse. Es gibt zwei Gründe für die Einbeziehung der Quelladresse bei QOSPF [ZSSC96]:

1. Ressourcenreservierungen und RRAs (Reservation Advertisements) basieren allgemein auf Quelladresse und Zieladresse.
2. Wenn das (Quelle, Ziel)-Routing benutzt wird, können Verbindungen mit gleicher Zieladresse aber von unterschiedlichen Quellen verschiedene Wege nutzen.

Die Benutzung der Quelladresse bei QOSPF bedeutet nicht, daß die Quelle Wurzel des verteilten Baumes sein muß. Es bedeutet nur, daß die Routing-Tabelle nicht nur das Ziel sondern auch die Quelle berücksichtigt.

Eine Frage bleibt noch offen: soll die Routing-Tabelle vor oder nach der Nachfrage berechnet werden. In Bezug auf diese Frage gibt es entsprechende Verfahren. Bei dem vorberechneten Verfahren wird die Routing-Tabelle vor dem Aufbau der Verbindung hergestellt und periodisch erneuert. Ein geeigneter Weg wird anschließend für die Verbindung gefunden. Es kann aber vorkommen, daß der zugeteilte Weg nicht mehr geeignet ist, weil die für die Berechnung der Routing-Tabelle benutzten Informationen nicht mehr aktuell sind.

Daher ist es in manchen Situationen besser, wenn es z.B. nur eine geringe Anzahl von Anfragen nach einem qualitätsbasierten Weg gibt, die Berechnung des Weges auf Anfrage durchzuführen. Der Vorteil von diesem Verfahren ist, daß die Berechnung einen besseren Weg durch die Benutzung der aktuellsten Verfügbarkeitsinformation finden kann. Ein weiterer Vorteil der Berechnung auf Anfrage ist, daß diese Methode Speicherplätze beim Router spart.

7 Verwandte Arbeiten

Qualitätsbasiertes Routing im Internet ist ein schwieriges Problem. Auf der Intradomain-Ebene soll ein Routing-Verfahren mit einigen der obengenannten Basisanforderungen entwickelt werden. Die kommerziellen Lösungsanbieter für Routingproblem wie Cascade, FORE und Stratacom demonstrieren eine Menge von den gewünschten

qualitätsbasierten Routingeigenschaften. Eine Zusammenfassung der Arbeiten in den verschiedenen Gebieten wird in folgenden Abschnitten vorgestellt.

Unter den Intradomain-Routing-Verfahren benutzt das Link-State-Routing-Protokoll OSPF, die verteilte Zustandsinformation. Die Netzwerk-Topologieinformation wird bei OSPF durch das ganze Netzwerk verbreitet. Jeder Knoten besitzt seine eigene Sicht auf den Netzwerkzustand, und ein „Shortest Path"-Algorithmus wird zur Berechnung der zielbasierten Routing-Tabelle benutzt. OSPF kennt zwei Hierarchieebenen (Area, Backbone). Im Vergleich zu OSPF, verlangt ein qualitätsbasiertes Link-State-Routing die dynamische Ausbreitung der Link- und Knoteninformation, wenn die entsprechende Ressourcenverfügbarkeit sich ändert. Aus Gründen der Skalierbarkeit, sollte eine baumbasierte Ausbreitung anstatt des Flutens benutzt werden. Ein qualitätsbasiertes Routing sollte eine Wegewahl auf Anfrage benutzen. Daraus entsteht aber ein höherer Aufwand bei den Routern. Ein effizientes Verfahren sollte diesen Aufwand minimieren.

Interdomain-Routingprotokolle, wie BGP (Border Gateway Protocol) haben sich auf die Kontrolle des Informationflusses zwischen verschiedenen administrativen Domainen konzentriert. Deswegen besitzen sie keine detaillierte Zustandsinformation über die Routing-Domainen. BGP benutzt einen Distanz-Vektor-Algorithmus und berechnet den Weg zum Ziel mit einem zielorientierten „Hop by Hop" Vorwärtsverfahren. Qualitätsbasiertes BGP benötigt noch weitere Arbeiten.

Unter den neueren Verfahren nutzt Source-Demand-Routing (SDR) die Wegewahl auf Anfrage bei den Routern. Ein strenges und lockeres Source-Routing werden implementiert. Das SDR-Verfahren kann für Intradomain-Routing und Interdomain-Routing benutzt werden. Die Nimrod-Architektur berücksichtigt viele Konzepte zur Behandlung der Skalierbarkeit und spezielle Methoden für die Wegewahl.

IP-Multicasting konzentriert sich auf die Erstellung von Multicastbäumen abhängig von der Änderungen der Topologie und der Gruppenmitgliedschaft. Dabei werden teilweise die unterliegenden Unicast-Routingprotokolle zur Erstellung der Multicastbäume benutzt. Ähnlich dem qualitätsbasierten OSPF, ist es auch möglich, ein qualitätsbasiertes MOSPF zu entwickeln.

Viele aktuelle Multicast-Routingprotokolle, wie „Protocol-Independent" Multicast und „Core-Based Trees" hängen nicht von den speziellen Unicast-Routing-Verfahren ab. Sie benötigen nur umfassende Änderungen, um Anforderungen an die Dienstqualität zu integrieren.

8 Zusammenfassung und Schlußfolgerung

Es gibt mehrere Gründe, das qualitätsbasierte Routing als eine wesentliche Komponente in der zukünftigen Internet-Infrastruktur zu betrachten. Der erste Schritt bei der Entwicklung einer qualitätsbasierten Routing-Architektur ist die Spezifikation ihrer Anforderungen. In der Praxis, muß man diese Anforderungen für das Interdomain-Routing noch genauer untersuchen. In diesem Beitrag, werden einige potentielle Anforderungen an die Berechnung des Weges, die Effizienz, die Robustheit und die Skalierbarkeit präsentiert. Einige Probleme, die bei der Realisierung der qualitätsbasierten Routing-Architektur entstehen, werden diskutiert. Die Schlußfolgerung ist, daß das qualitätsbasierte Routing ein Problem mit großer Herausforderung ist. Jeder wichtige Bestandteil

davon wie Wegewahl, Skalierbarkeit, und administrative Kontrolle besitzt seine eigenen Probleme, die bei der Entwicklung der Routing-Architektur berücksichtigt werden müssen.

Literatur

[CNRS96] E. Crawley, R. Nair, B. Rajagopalan und H. Sandick. A Framework for QoS-based Routing in the Internet. *Internet Draft „draft-ietf-qosr-framework-00.txt“*, März 1996.

[GuOW96] R. Guerin, A. Orda und D. Willianms. QoS Routing Mechanisms and OSPF Extensions. *Internet Draft „draft-guerin-qos-routing-ospf-00.txt“*, November 1996.

[RaNa96] B. Rajagopalan und R. Nair. Quality of Service (QoS)-Based Routing in the Internet Some Issues. *Internet Draft „draft-nair-qos-based-routing-01.txt“*, Oktober 1996.

[WaCr96] Z. Wang und J. Crowcroft. QOS Routing for Supporting Resource Reservation. *http://boom.cs.ucl.ac.uk/staff/zwang/pub.html*, 1996.

[ZSSC96] L. Zhang, C. Sanchez, B. Salkewicz und E. Crawley. Quality of Service Extensions to OSPF or Quality of Service Path First Routing (QOSPF). *Internet Draft „draft-zhang-qos-ospf-00.txt“*, Juni 1996.

Abbildungsverzeichnis

Multimediale Konferenzen im Internet

Michael Judaschke

Kurzfassung

Der vorliegende Beitrag befaßt sich mit den Mechanismen zur Realisierung von Multimedia-Konferenzen im Internet. Dies beinhaltet zum einen die Bekanntgabe der Daten, die für den Empfang einer Konferenz notwendig sind, als auch den Austausch von Befehlen, die der Steuerung von Sitzungskomponenten, wie zum Beispiel Video-Server, dienen. Hierzu werden die zur Kontrolle einer Sitzung eingesetzten Protokolltypen SDP (Session Description Protocol), SIP (Session Initiation Protocol), SAP (Session Announcement Protocol) und RTSP (Real Time Stream Control Protocol) vorgestellt. Mit den Protokollen SDP, SIP und SAP wird eine Verteilung der Sitzungseckdaten vorgenommen. Die Kontrolle des Empfanges der Sitzung obliegt dann dem RTSP. Unter einer Sitzung wird in diesem Zusammenhang eine Menge von multimedialen Datenströmen verstanden, die durch den Empfänger synchronisiert werden. Eine Testumgebung, in der die vorgestellten Mechanismen zum Teil bereits umgesetzt werden, ist das MBone. Die Gewährleistung von Echtzeitbedingungen, Dienstqualität und die Problematik des Routing sind explizit kein Thema dieses Beitrages.

1 Einleitung

Multimediale Konferenzen, das sind vom Grundsatz her nichts weiter als Konferenzen im Internet, die sich der Video- und Audioübertragung bedienen. Beispiele hierfür sind Bildtelefon, Videokonferenzen oder auch“ video-on-demand“-Lösungen. Das *Bildtelefon* stellt hierbei noch die einfachste Form der multimedialen Kommunikation dar. Zwei Teilnehmer unterhalten sich über das Internet und erhalten durch die auf beiden Seiten installierte Kamera die Möglichkeit, ihren Gesprächspartner auch zu sehen. Für diese Kommunikation werden zwei Punkt-zu-Punkt-Verbindungen benötigt, die im Idealfall eine garantierte Bandbreite zur Verfügung stellen würden.

Videokonferenzen werden durch die Vielzahl der Benutzer komplexer, da jeder im schlechtesten Fall jeden sehen und hören will. Die Frage bleibt nur: "Wie wird diese Kommunikation realisiert?!". Als naive Lösung wird man zwischen jedem einzelnen Teilnehmer eine Punkt-zu-Punkt-Verbindung etablieren. Dies hätte jedoch zur Folge, daß bei n Teilnehmern n*(n-1)/2 Verbindungen benötigt werden. Neben einer erheblichen Netzbenutzung ist natürlich auch der Sender bei dieser Lösung stark belastet, da jedes Paket kopiert und n-1-mal verschickt werden muß. Man stelle sich eine Podiumsdiskussion im Internet vor, an der vier Gesprächsteilnehmer und ein Auditorium

mit 1.500 Zuhörern teilnimmt. Jedes Paket müßte 1503-mal verschickt werden. Ziel ist also die Adressierung einer Gruppe von Empfängern.

Die Realisierung dieser Gruppenkommunikation erfolgte über die Einführung von sogenannten Multicast-Adressen, über die jedes Gruppenmitglied angesprochen werden kann. So kann mit einem Paket eine unbeschränkte Anzahl von Empfängern erreicht werden. Die Verteilung dieser Pakete erfolgt dann über eine Baumstruktur, in der die (multicast-fähigen) Router dafür sorgen, daß die eingehenden Multicast-Pakete an alle Netzknoten weitergeleitet werden, über die Gruppenmitglieder erreicht werden. Der Kopiervorgang wird somit in die Router verlagert und die Netzlast durch die Einfachnutzung von Wegen reduziert. Die Integration von neuen Empfängern wird dadurch sehr vereinfacht, da diese lediglich ihre Teilnahme an einer Multicast-Gruppe bekannt geben müssen. Diese Bekanntgabe erfolgt zunächst an das Gateway des eigenen lokalen Netzes und wird solange weitergereicht, bis ein Router erreicht wird, an den bereits Pakete für die fragliche Gruppe weitergeleitet werden. Dieser Router veranlaßt dann, daß man die entsprechenden Pakete erhält. Analog funktioniert das Ausscheiden aus einer Gruppe.

Multicast-Adressen werden in der Regel nicht statisch vergeben d.h. zu Beginn einer Übertragung wird jedem Datenstrom eine IP-Adresse zugeordnet. Nach Beendigung der Konferenz fallen diese Adressen an den Adreßpool zurück. Für diese dynamische Adressvergabe ist der Class-D-Adreßraum reserviert.

Ein Beispiel für den Versuch Multimedia-Konferenzen über das Internet zu veranstalten, ist das MBone (Multicast Backbone)[1]. Hier wird das Problem, daß die meistens Router im Internet nicht multicast-fähig sind, durch Tunneling umgangen. Die Multicast-Pakete werden hierbei in "normalen" IP-Pakete eingepackt und so zwischen multicastfähige Teilnetzen verschickt. Innerhalb dieser Teilnetze können dann die Multicast-Pakete verschickt werden.

Das dritte Beispiel für multimediale Anwendungen ist *Video-on-demand*. Dies ist das Abrufen von Videos, die auf Medien-Server gespeichert werden. Hierfür wird wieder nur eine Unicast-Verbindung benötigt. Dieser Abruf soll aber zum einen gegen Entgelt und zum zweiten, was entscheidender ist, in Echtzeit erfolgen, da der Benutzer während der Übertragung das Video anschauen möchte. Desweiteren sollte der Benutzer, die Möglichkeit haben sein Video anzuhalten, vorzuspulen etc..

Die soeben umrissenen Anwendungen haben Anforderungen, für die das Internet nicht ausgelegt ist. Es muß also mit Hilfe von Protokollen eine Adaption der vorhandenen Dienste an diese Anforderungen erfolgen. Diese Anpassung wird zum Teil direkt in der Anwendung oder aber unter Zuhilfenahme neuer Protokolle, die auf die Transportdienste (UDP und TCP) des Internets aufsetzen, realisiert. Die Übertragung der multimedialen Datenströme erfolgt dann über RTP (Real Time Transport Protocol). Desweiteren wurde eine Reihe von Protokolltypen entwickelt, die der Steuerung der Konferenzen dient. Diese Protokolle werden im folgenden behandelt.

[1] Nähere Informationen sind unter http://www.mbone.com/ verfügbar.

2 Die Protokollfamilie für multimediale Anwendungen

Um den Echtzeitanforderungen der Multimedia-Anwendungen Rechnung zu tragen, mußte zunächst ein neuer Transportdienst entworfen werden. Dieser Dienst wurde durch die Protokolltypen RTP [SJCF96] und RTCP (Real-Time-Transport-Control-Protocol) realisiert. RTP ist ein Transportdienst, der auf UDP aufsetzt und für die kontinuierlichen Auslieferung des Datenstromes sorgt. Da RTP keine Dienstqualität garantiert, wurde als zweite Komponente dieses Dienstes RTCP entwickelt. Mit RTCP wird die Dienstqualität zwar nicht garantiert aber zumindest überwacht. Wir haben also für die Datenübertragung eines Dokumentes, z.B. ein Tondokument, zwei Prozesse mit je einem Port. Mit RTP und RTCP läßt sich also bereits eine Datenübertragung steuern. Für die Steuerung der Sitzung werden aber noch weitere Protokolltypen benötigt. Diese sind SDP, SAP, SIP und RTSP. SDP ist ein Format, in dem Sitzungsparameter ausgetauscht werde. Es wird zum Beispiel von SAP verwendet, um die Sitzungsdaten an alle potentiellen Empfänger zu verteilen. SIP dient der Integration neuer, sendender Teilnehmer, zum Beispiel eines Videoservers, und RTSP dient der Kontrolle der laufenden Sitzung. Mit RTSP können hierzu Befehle an einzelne Teilnehmer verschickt werden. Diese vier Protokolle sind ähnlich wie HTTP text-basiert und setzen auf UDP und TCP auf. Dies soll insbesondere der einfachen Integration in die bestehende Internet-Infrastruktur dienen und zum zweiten die Verständlichkeit für den Endbenutzer erhöhen.

3 Protokolle zur Steuerung einer Sitzung: RTSP

RTSP (Real-Time Stream Control Crotocol) [Schu96] ist das Steuerungselement einer Sitzung. Im Gegensatz zu den im Abschnitt 4 besprochen Protokollen, die der Bekanntgabe von Parametern dienen, können Sitzungsteilnehmer, Benutzer wie auch integrierte Server mit RTSP Befehle austauschen. RTSP-Pakete können hierzu mit einem Transport-Protokoll wie zum Beispiel TCP oder UDP übertragen werden. Die Anwendung, die RTSP verwendet, sollte aber mindestens TCP unterstützen.

Da RTSP auch über verbindungslose Dienste wie UDP verschickt werden kann, wird jede Nachricht bestätigt. Erfolgt keine Bestätigung innerhalb der RTT (round-trip-time), so wird das Packet einfach noch einmal verschickt. Die RTT wird initial auf 500 ms gesetzt, kann aber an die reale Zeit (nach unten) angepaßt werden. Dies ist insbesondere in kleinen Netzen sinnvoll, da ansonsten zuviel Zeit bis zum Timeout vergeht.

Zur Unterscheidung der einzelnen Anforderungen werden Sequenznummern vergeben. RTSP gewährt aber trotz der Sequenznummer keine reihenfolgegetreue Auslieferung der Pakete. Die Applikation hat über die Sequenznummer lediglich die Möglichkeit, eine geänderte Reihenfolge zu erkennen und dann eine Fehlerbehandlung einzuleiten.

Ein RTSP-Anfrage-Paket gliedert sich in drei Abschnitte: Den Nachrichtenkopf, eine Parameterliste und einen Nachrichtenteil (Message-Body). Eine minimale Nachricht beinhaltet lediglich den Nachrichtenkopf, der Methodenname, Sitzungsname, Versionsnummer und Sequenznummer enthält. Eine RTSP-Anwort unterscheidet sich vom

Aufbau nur im Nachrichtenkopf. Mit diesem wird Versionsnummer, eine Statusmeldung (siehe 3.2) und die Sequenznummer des Referenzpaketes angegeben. Durch die einfache Struktur (textbasiert, einfacher Aufbau) kann der Funktionsumfang von RTSP jederzeit erweitert werden. Zur Zeit sind bereits eine Reihe von Methoden definiert.

3.1 Die Methoden

Mit der Methode GET kann ein potentieller Teilnehmer von einem Server die Sitzungsparameter abfordern. Der Server verschickt dann ein Paket mit den Sitzungsdaten an den Anfragenden. Dieser hat zusätzlich mittels eines ACCEPT-Parameters die Möglichkeit zu spezifizieren, in welchem Format die Antwort zu erfolgen hat. Dies ist vor allem dann sinnvoll, wenn der potentielle Teilnehmer lediglich Pakete in einem bestimmten Format auswerten kann.

Multimedia-Konferenzen sind ein dynamisches Forum. Mit GET exestiert eine Methode, mit der Empfänger durch die Übermittlung der Sitzungsdaten die Möglichkeit zur Integration in eine Sitzung erhalten. Da aber auch Sender zu einer Sitzung hinzukommen können, ist es notwendig alle Teilnehmer über Veränderungen des Gesamtzustandes zu informieren. Hierzu werden mit der Methode SESSION alle Sitzungsparameter (IP-Adressen, Ports etc.) im SDP-Format (siehe Abschnitt 4.1) verschickt. Eine selektive Aktualisierung der Daten erfolgt nicht, da durch die Versendung der kompletten Sitzungdaten auch die Eliminierung von Teilnehmer und damit die Freigabe von IP-Adressen ermöglicht wird.

Die Methode SET_PARAMETER dient der Festlegung einzelner Parameter einer laufenden Sitzung. Hierzu gehören Port-Adressen für TCP und UDP-Streams, Netzwerkadressen (IP4 und IP6 werden zur Zeit unterstützt), Größe der Dateneinheiten, Übertragungsgeschwindigkeit und die TTL. Der Unterschied zum SESSION-Befehl besteht darin, daß Änderungen der Anzahl der Sender unberücksichtigt bleiben. Das Gegenstück zur SET_PARAMETER-Methode ist die GET_PARAMETER-Methode. Sie dient der Abfrage einzelner [d.h. pro Anfrage ein Parameter] Parameter. Abgefragt werden können alle Parameter, die mittels SET_PARAMETER gesetzt werden können. Bei mehr als einem Parameter sollte GET verwendet werden.

Es kann nun auch die Situation eintreten, daß der mit GET abgefragte Server nicht für die Sitzung zuständig ist. In diesem Fall kann zum einen eine einfache Fehlermeldung verschickt werden oder aber, sofern Informationen über die korrekte Adresse vorliegen, die Anfrage durch die Methode REDIRECT beantwortet werden. REDIRECT schickt hierzu die Anfrage zurück und gibt mit dem Parameter *LOCATION* im Header die URL eines anderen Servers an, an die die GET-Anfrage gerichtet werden sollte. Optional kann auch ein Zeitpunkt spezifiziert werden, ab dem die Umleitung Gültigkeit besitzt.

Bislang wurden lediglich Methoden vorgestellt, die der Verwaltung einer Sitzung dienen. Die Stärke von RTSP liegt aber in der VCR-Funktionalität, d.h. der Möglichkeit, Datenströme einer Sitzung auf einem beliebigen Server zu speichern und Video- als auch Audiodaten in eine laufende Sitzung einzuspielen. Den Anwendungen stehen hierzu zur Zeit die Methoden PLAY, RECORD und STOP zur Verfügung. PLAY fordert zum Abspielen einer Video-/ Audiosequenz oder einer Präsentation auf. Da man davon ausgehen kann, daß in der Regel nicht eine komplette Sequenz abgespielt werden soll, wird der Parameter *RANGE* übergeben. Dieser gibt dann Start- und

Endpunkt der Übertragung an. Start und Ende können relativ zum angeforderten Medium sein: z.B. lasse die ersten 10 Minuten fort und spiele dann 45 Minuten – > *RANGE: smpte=0:10:00-0:55:00* oder als absolute Zeit im NTP-Format (Network Time Protokoll) angegeben werden. Das Pendant der PLAY-Methode ist RECORD. RECORD fordert zum Aufnehmen einer Sitzung oder eines bestimmten Datenstroms auf. Sofern die Sitzung bereits besteht, soll die Aufnahme sofort beginnen. Ansonsten muß die Uhrzeit als absolute Zeit übergeben werden. STOP dient der Beendigung einer laufenden Übertragung eines Datenstromes (z.B. ein Video, das gerade abgespielt wird).

Eine Anfrage zum Aufnehmen oder Abspielen kann selbstverständlich auch abgelehnt werden. In diesem Fall muß aber im Antwort-Paket mitgeteilt werden, welchen Methoden erlaubt sind. Dies erfolgt mit dem Parameter *ALLOW*.

Abschließend bedarf es noch einer Verabschiedung eines Teilnehmers, mit der ein aktiver Teilnehmer seine Teilnahme beenden kann oder aber, zum Beispiel im Fall eines Video-Servers, mit der die Sitzungsteilnahme explizit beendet wird. Hierfür steht die BYE Methode zur Verfügung.

Optional zu diesen Methoden, die für die direkte Steuerung der Sitzung verwendet werden, können mit einem RTSP-Paket noch zusätzliche Parameter übergeben werden. Diese dienen der genaueren Spezifikation der Anfrage bzw. Antwort. So kann durch die Angabe der Parameter *TRANSPORT, SPEED, TTL, LOCATION* eine recht genaue Beschreibung der Wunschsitzung erfolgen. Sofern ein Nachrichtenteil enthalten ist, muß noch dessen Länge und der Inhalttyp übergeben werden. (Parameter *CONTENT-LENGTH* und *CONTENT-TYPE*).

3.2 Die Status-Meldungen

Der wichtigste Inhalt einer Antwort besteht aus Statusmeldungen. Hierfür wurden Statuscodes definiert, die bereits im wesentlichen in HTTP benutzt werden. Die wichtigsten Antwortklassen werden im folgenden vorgestellt.

War die Anfrage erfolgreich, so wird dies mit einem Statuscode der Klasse 2xx, üblicherweise 200= OK, bestätigt.

Nun kann aber auch der Fall eintreten, daß der gewünschte Dienst lokal nicht erbracht werden konnte. In diesem Fall muß die Anfrage umgeleitet werden. Umleitungen werden mit Statuscodes der Klasse 3xx angezeigt. Hierbei wird die Anfrage an den Absender zurückgeschickt und dieser erhält über den Parameter *LOCATION* eine oder mehrere IP-Adressen, an die die Anfrage gerichtet werden sollte.

Fehlermeldungen sind die unangenehmere aber dennoch häufig auftretende Variante von Rückmeldungen. Es kann zwischen zwei Ebenen unterscheiden, auf denen diese erzeugt werden. Dies ist die Benutzerebene (die Instanz, die angefragt wurde) und die Betriebssystemebene (der Server).

Auf der Benutzerebene werden Fehlermeldungen erzeugt falls die Anfrage unautho-risiert oder verboten ist, oder aber die Diensterbringung nicht akzeptiert werden kann. Für den Fall, daß die vorliegenden Angaben nicht ausreichen, um den angeforderten Dienst zu erfüllen, erhält der Sender ein entsprechendes Feedback. Der Sender muß

dann die Anfrage mit den erforderlichen Angaben wiederholen. Desweiteren kann auch ein Formatfehler aufgetreten sein, so daß die Nachricht überhaupt nicht interpretiert werden konnte. Die Ablehnung einer Anfrage kann aber auch als Ursache eine zu geringe Bandbreite für die Übertragung haben. Diese Fehlermeldungen werden in der Klasse 4xx zusammengefaßt.

Für Fehlermeldungen des Servers, die in der Klasse 5xx definiert sind, gibt es im wesentlichen vier Ursachen. Der angefragte Dienst ist nicht implementiert, kann aufgrund mangelnder Kapazitäten zur Zeit nicht erfüllt werden oder aber die benutzte RTSP-Version wird nicht unterstützt. Desweiteren kann es zu Gateway-Fehlern kommen, wie zum Beispiel eine falsche Gateway-Adresse oder einem Timeout des Gateway.

Da diese Meldung nach Möglichkeit auch für den Benutzer (den Menschen) verständlich sein soll, wird neben dem Statuscode auch die Meldung in Klartext anzeigt.

3.3 Nachrichtenteil

Methoden, Parameter und Statuscodes sind genau spezifiziert. Um weitere Informationen an den Kommunikationspartner zu übergeben, ist im Paketformat ein Nachrichtenteil vorgesehen. In diesem können Sitzungsdaten im SDP-Format (siehe Abschnitt 4.1), RTP-Pakete oder einfach Klartext übertragen werden. Der Empfänger der Nachricht ersieht aus den Parametern *CONTENT-LENGTH* und *CONTENT-TYPE* ob ein Nachrichtenteil folgt und welchen Inhalt dieser hat.

3.4 Ein Beispielpaket mit Antwort

PLAY donald_duck/video RTSP/1.0 3
Range: smpte 0:0:00-
A fordert D auf, ein Video mit der Bezeichnung Donald Duck abzuspielen. Das Video soll vom Start bis zum Ende abgespielt werden. Die Anfrage wird im Format der RTSP-Version 1.0 gestellt und erhält die laufende Nummer 3

RTSP/1.0 200 3 OK
D beantwortet die Anfrage positiv

4 Protokolle für die Integration von Teilnehmern: SDP, SAP und SIP

4.1 SDP

SDP (Session Description Protocol) [HaJa97] spezifiziert ein Format, in dem Sitzungsparameter vorliegen sollten. Dieses Format wird zum Beispiel bei der Initialisierung mit SIP- oder SAP-Paketen (siehe Abschnitt 4.2 und 4.3) benutzt. Alternativ können diese Sitzungsbeschreibungen auch als Email verschickt oder als Datei im WWW abgelegt werden. In diesem Fall kann jedoch nicht davon ausgegangen werden, daß nur potentielle Empfänger, die Sitzungsdaten erhalten. (Nutzungsbeschränkungen server- oder clientseitig können nicht berücksichtigt werden).

4.1.1 Sitzungsparameter

In einem SDP-Paket werden als minimale Informationen die SDP-Version, der Initiator einer Sitzung , die Sitzungskennung, der Sitzungsname und die IP-Adressen, an die die Datenströme der Sitzung geschickt werden, als Parameter übergeben. Die Email-Adresse oder die Telefonnummer des Initiators müssen angegeben werden, damit eine Kontaktaufnahme einfach erfolgen kann. Desweiteren muß zusätzlich angegeben werden, wann die Konferenz stattfinden soll und welche Medien (zum Beispiel Video oder Audio) benutzt werden. (diese Angaben werden später in Abschnitt 4.1.3 behandelt)

Die Sitzungskennung muß weltweit eindeutig sein. Hierzu wird eine lokal eindeutige Sitzungsidentifikationsnummer verwendet, die in Kombination mit dem Benutzername des Initiators und der IP-Adresse des Endsystems diese Anforderung erfüllt. Als Verbindungsdaten werden die IP-Multicast-Adressen angegeben, die der Sitzung angehören. Sollte die Sitzungsbeschreibung verschlüsselt sein, so muß ein Hinweis auf den Schlüssel übergeben werden, so daß der Empfänger die Möglichkeit zur Entschlüsselung erhält. Diese Schlüsselkennung muß jedoch lokal nicht eindeutig sein, d.h. dem Empfänger können zu einer Schlüsselkennung veschiedene Schlüssel vorliegen. Im Zweifelsfall müssen alle in Frage kommenden Schlüssel ausprobiert werden. Neben diesen minimalen Angaben können weitere Angaben als Parameter übergeben werden. Hierzu zählen eine kurze Sitzungsbeschreibung in Klartext, eine WWW-Adresse, um mehr Informationen zu erhalten und die Vorgabe einer gewünschten Bandbreite. Diese Angaben sind lediglich als Hilfestellung für den Benutzer zu sehen.

Zusätzliche Informationen können als Attribute übergeben werden. Hierzu zählen Schlüsselwörter, Konferenztypen und Kategorien, die der Suche dienen, und Angaben über die Tools, die empfängerseitig gestartet werden sollten. Neue Attributtypen können jederzeit hinzukommen und so den Nutzungsumfang von SDP erweitern.

4.1.2 Zeitangaben

Der Zeitpunkt, zu der die Sitzung/ Konferenz stattfindet, wird mit der Startzeit und Stopzeit angegebenen. Die Stopzeit gibt hierbei die absolute Endzeit an, also im Falle von Folgeterminen, ist das Ende der letzten Sitzung gemeint. Diese Angabe erfolgt in Sekunden lt. dem NTP und ist erforderlich. Da eine Konferenz auch Folgetermine haben kann, können in einem separaten Feld Wiederholungen und Folgetermine definiert werden. Angegeben wird dann das Wiederholungsintervall, die Konferenzdauer und möglicherweise mehrere Offsets zur Startzeit. Als Wiederholung wird in diesem Zusammenhang ein regelmäßiger Termin verstanden, der zum Beispiel wöchentlich stattfindet. Für den Fall , daß aber die Konferenz mehrere Termine pro Woche hat, werden die Offsets benutzt um die Startpunkte jedes weiteren Termines anzugeben. Auch für dieses Feld erfolgt die Angabe i.d.R. in Sekunden, für eine bessere Verständlichkeit kann aber auch eine Schreibweise im Format d (Tage) h (Stunden) und m (Minuten) gewählt werden.

Mit einem Zeitzonen-Feld, kann neben der Zeitzone auch ein Offset für die Umstellung der Sommerzeit angegeben werden. Man bedenke, daß Sitzungen weltweit zu empfangen sind.

4.1.3 Medien-Beschreibung

Bislang wurden lediglich allgemeine Eckdaten der Sitzung beschrieben. Um die Datenströme der einzelnen Medien zu empfangen, bedarf es aber noch der Medienbeschreibung. Diese gibt Auskunft über Medienart, also Video/ Audio/ Text, die Port-Adresse zur Prozeßspezifikation, das verwendete Transport-Protokoll, üblicherweise RTP über UDP, und das Übertragungsformat. Eine mögliche Beschreibung wäre somit „m=video 34552/2 RTP/AVP 31“, es handelt sich also um ein Video, das über die Ports 34552 (RTP) und 34553 (RTCP) anzusprechen ist. AVP heißt in diesem Zusammenhang „Audio und Video Profil“ und gibt ein spezielles Format an, in dem Video und Audiodaten in RTP-Paketen gepackt werden). So können zum Beispiel mehrere Audiokanäle innerhalb eines Paketes verschickt werden, was bei Stereoaufnahmen von Nutzen ist. Mit der Formatnummer kann dann zwischen MPEG, Wave-Dateien etc. unterschieden werden. Desweiteren besteht die Möglichkeit über das Attribut a=rtpmap zusätzliche Informationen über den Typ zu übergeben oder aber sogar eigene Formate zu testen. Optional können noch ein Medientitel, ein Verschlüsselungstyp und Verbindungsdaten übergeben werden, sofern diese von den Daten der Sitzung abweichen.

4.1.4 Ein Beispielpaket

v= 0
gibt die Versionsnummer an
o= mjudaschke 0815 4711 IN IP4 129.13.42.100
Sitzungskennung bestehend aus: Benutzername, Sitzungsnummer, Instanznummmer, Netzbezeichnung, hier Internet, IP-Version und IP-Adresse
s= donald_duck
Sitzungsbezeichnung
i= ein Beispielpaket, um SDP zu veranschaulichen
Kurzbeschreibung der Sitzung
u= http://www.uni-karlsruhe.de/ un9w
Homepage auf der weitere Informationen über die Sitzung abrufbar sind
e= un9w@rz.uni-karlsruhe.de (Michael Judaschke)
Email-Adresse des Initiators
t= 2873397496 2973404696
Start- und Endzeit der Sitzung
r=7d
die Sitzung wird wöchentlich wiederholt
m= audio 3456/2 RTP/AVP 0
c= IN IP4 224.2.17.12/ 128
Der Audiostrom wird an die Multicast-IP-Adresse 224.2.17.12 Port-Nummern 3456 und 3457 geschickt. Als Transportprotokoll wird RTP/ AVP benutzt.
m=video 2232/2 RTP/ AVP 31
c= IN IP4 224.2.17.13/ 128
Der Videostrom wird an die Multicast-IP-Adresse 224.2.17.13 Port-Nummern 2232 und 2233 geschickt. Als Transportprotokoll wird RTP/ AVP benutzt.

4.2 Das SAP-Paket

SAP (Session Announcement Protocol) [Hand96] beinhaltet die Sitzungsparameter und wird verwendet um die Sitzungsdaten an den potentiellen Benutzerkreis zu verteilen. Die Verteilung der Daten erfolgt in regelmäßigen Abständen und muß bis zum Sitzungsbeginn mindest ein Mal erfolgt sein. Die periodische Bekanntgabe hat zum einen den Zweck, die Sitzung aufrecht zu erhalten und hat natürlich den Vorteil, daß mögliche Teilnehmer, die erst später hinzukommen, die Daten auch erhalten.

Der Hauptbestandteil eines SAP-Paketes sind die Sitzungsdaten, die in einem Textfeld im SDP-Format übertragen werden. Um möglichem Mißbrauch vorzubeugen, besteht die Möglichkeit die Daten zu authentifizieren und zu verschlüsseln. Die Authentifizierung erfolgt mit Hilfe eines Authentifizierungskopfes und soll sicherstellen, daß Pakete wirklich vom angegebenen Absender stammen. Eine weitere Sicherheitslücke ist das Abhören. Um dies zu verhindern, kann die Beschreibung verschlüsselt werden und es wird dann eine Schlüssel-ID übermittelt. Diese Schlüssel-ID dient als Zeiger auf einen Schlüssel beim Empfänger. Falls diese beim Empfänger nicht eindeutig ist, muß er verschiedene Schlüssel ausprobieren. Neben diesen Sicherheitsaspekten bietet SAP auch die Möglichkeit durch gzip-Kompression die Datenmenge zu reduzieren und damit die Übertragungsgeschwindigkeit zu erhöhen. Sollte dies der Fall sein, muß die Kompression vor der Verschlüsselung geschehen.

Neben dieser regelmäßigen Bekanntgabe können mittels SAP auch Sitzungsparameter geändert oder auch die komplette Sitzung gelöscht werden. Um zu unterscheiden, welchem Zweck (einfache Mitteilung/ Löschen) ein SAP-Paket dient, wird ein „message-type“-bit gesetzt.

4.2.1 Der Rundruf

Wie bereits erwähnt werden SAP regelmäßig verschickt. Nun fragt sich aber, an wen die Pakete geschickt werden. Ein Broadcast über das komplette Internet ist ebensowenig sinnvoll wie die Adressierung jedes einzelnen potentiellen Epfängers. Da eine Gruppe angesprochen werden soll, erfolgt der Versand also an eine Multicast-Adresse. Hier gibt es zwei Mechanismen:

1. Die öffentliche Sitzung:

   Existiert keine genaue Vorstellung über den potentiellen Benutzerkreis, oder soll die Sitzung aus anderen Gründen für jeden zugänglich gemacht werden, so wird das SAP-Paket an eine weltweit eindeutig bestimmte Adresse geschickt. Diese lautet 224.2.127.254 mit dem UDP-Port 9875.

   In diesem Fall besteht über eine vorgegebene TTL oder eine Verschlüsselung die Möglichkeit, den Benutzerkreis einzuschränken. Die TTL dient hier jedoch nur dazu, zu bestimmen, welche maximale Laufzeit die Pakete haben dürfen, und stellt damit lediglich eine räumliche Selektion dar.

   Diese Form der Verbreitung der Daten ist für alle öffentlichen Konferenzen gedacht. Sie hat den Vorteil, daß potentielle Teilnehmer nur eine wohldefinierte Multicast-Adresse abhören müssen und so weiterer administrativer Aufwand auf der Benutzerseite ausbleibt.

2. Die private Sitzung:

   Nun kann es aber auch durchaus sein, daß eine Konferenz über das Internet abgewickelt werden soll, diese dennoch nicht öffentlich ist. Dies kann zum Beispiel dann der Fall sein, wenn ein kleines Unternehmen die Kosten für Standleitungen sparen und deshalb die Infrastruktur des Internets benutzen möchte.

   Um eine solche private Sitzung abzuhalten, wird zunächst ein Pool von Multicast-Adressen, zum Beispiel 239.16.32.0 - 239.16.32.255, benötigt. Dieser kann dann benutzt werden, um die Konferenz mit den vorgestellten Mechanismen durchzuführen. Als Rundruf-Adresse wird dabei laut Konvention die höchste (also hier 239.16.32.255) des Adressenpools benutzt.

   Die potentiellen Teilnehmer müssen dann nur noch informiert werden, auf welchen Rundrufadressen sie mithören müssen. Im schlechtesten Fall wird zu diesem Zweck jedem potentiellen Teilnehmer die Rundrufadresse per Email mitgeteilt. Nach diesem anfänglichen Mehraufwand, kann dann aber jede Sitzung per Rundruf einbestellt werden.

4.3 SIP

SIP (Session Initiation Protocol) [ScHS97] ist ein Protokoll, das verwendet wird um neue Sender in einer Sitzung zu integrieren. Hierzu kann auf zwei Methoden zurück gegriffen werden: INVITE und OPTIONS. Mit INVITE kann ein neuer Teilnehmer oder aber auch z.B. ein Medienserver aufgefordert werden, an einer Sitzung teilzunehmen. Die Aktivität geht also von einem Sitzungsteilnehmer aus. OPTIONS hingegen bietet dem Benutzer die Möglichkeit eine Anfrage zu stellen. Er kann dann an einer Sitzung teilnehmen, sofern Kapazitäten vorhanden sind. Die SIP-Pakete werden an eine eindeutige URI verschickt, wie zum Beispiel die Email-Adresse, einer Kombination aus Benutzername und IP-Adresse oder dem login auf einem bestimmten Rechner. Die empfangende Instanz ist dann immer eine Applikation, die die Sitzungsverwaltung übernimmt. SIP verwendet für den Datentransport UDP oder TCP.

Da jede Anfrage beantwortet werden muß, gibt es folglich SIP-Anfragen und SIP-Antworten, die sich, wie auch bei RTSP, im Format unterscheiden. Es wird mit diesen beiden Paketen aber ausschließlich die Initialisierung durchgeführt. Eine SIP-Session gibt es nicht.

4.3.1 SIP-Anfragen

Die Anfrage besteht aus einer Anfragezeile, die Methode, Adresse des Empfängers und die SIP-Version enthält, und einer oder mehrerer Nachrichten. Diese bestehen aus einem Kopf und einem optionalem Fließtext.

Nachrichtenkopf und Nachrichtentext:
: Da die Angaben der Anfragezeile gerade einmal ausreichen, um das Paket zuzustellen und an den richtigen Prozeß zu leiten, bedarf es für eine Beantwortung noch zusätzlicher Angaben. Diese werden in den Nachrichten konkretisiert. Eine Angabe die auf jeden Fall im Nachrichtenkopf stehen muß, ist dabei die Adresse des Initiators der Anfrage. Optional können dann im Kopf weitere Angaben

gemacht werden. Hierzu zählen das Datum, das Transportprotokoll, die Länge und Typ des Nachrichtentextesoder auch ein ACCEPT-Language Parameter, der angibt in welcher Sprache die Fehlermeldung im Klartext erscheinen soll. Es kann zusätzliche auch eine Auflistung der Stationen enthalten sein, die auf dem Weg zum Empfänger passiert wurden. (Via: ...) Dies schützt den Sender davor, daß er an einen Server verwiesen wird, der die Anfrage bereits weitergeleitet hat.

Ein mögliche Anfrage hat somit folgendes Format

INVITE 128.16.64.19/65729 SIP/2.0
Einladung an IP-Adresse 128.16.64.19 Portnummer 65729. Verwendete SIP-Version ist 2.0
Via: SIP/2.0 /UDP 239.123.123.1 :44582
Via: SIP/2.0 /UDP 128.16.64.19
IP-Adressen der Stationen, die die Anfrage bereits weitergeleitet haben
From: mj@anywhere.de
Absender der Einladung
ACCEPT-Language: German
Fehlermeldungen sollen in Deutsch ausgegeben werden

4.3.2 Die SIP-Antwort

Die Anwort auf eine SIP-Anfrage besteht, ähnlich wie diese, aus einer Statuszeile und einem darauffolgenden Nachrichtenfeld. Der wichtigste Inhalt der Antwort ist, wie bei RTSP, mit dem Statuscode gegeben.

Statusmeldungen: Die Statuscodes werden in die gleichen Klassen wie bei RTSP eingeteilt. Es kommen lediglich zwei Klassen hinzu. Die ist zum einen die Klasse der 1xx-Nachrichten, die der Zwischenbenachrichtigung dient, falls die Anfrage nicht zugestellt wurde aber weiterhin der Versuch unternommen wird, die Anfrage zuzustellen. Zum anderen kommt die Klasse der 6xx-Nachrichten hinzu, die für Suchfehler verwendet wird.

Nachrichtenkopf und Nachrichtentext:

Der Nachrichtenkopf und Nachrichtentext in seiner Funktionalität und Aufbau den anderen Protokollen. Lediglich drei Parameter sollen hier noch kurz vorgestellt werden.

1. Retry-After wird in den Antworten mit Statuscode 451 (busy), 404 (not-found) und 503 (Service unavailable) verwendet. Der Retry-After-Wert gibt an, ab welchem Zeitpunkt eine erneute Anfrage an den Server sinnvoll erscheint. Die Angabe kann als relativer oder absoluter Zeitwert erfolgen.
2. Reason gibt den Ablehnungsgrund im Klartext an.
3. Confirm dient als Aufforderung zur Bestätigung der Einladung. Sollte in der Antwort confirm = required gesetzt sein, so muß der Client die Anfrage mit confirm = true wiederholen.

Eine mögliche Anwort hat also folgendes Format

SIP/2.0 200 128.16.19/ 65729
Einladung wird angenommen From: mj@anywhere.de
Via: SIP/2.0 /UDP 239.123.123.1 :44582
Via: SIP/2.0 /UDP 128.16.64.19
Contact-host: 131.215.131.147
Die Anfrage wird jedoch vom Host mit der IP-Adresse 131.215.131.147 bearbeitet
Confirm: required
die Einladung soll wiederholt werden, eine Bestätigung wird gefordert.

5 Eine Beispielsitzung

Um noch die Funktionsweise der vorgestellten Protokolle zu veranschaulichen, wurde eine Beispielsitzung betrachtet. An dieser Sitzung sollen zunächst drei Teilnehmer beteiligt werden. Thema der Konferenz sind die skandalösen Steuerhinterziehungen eines gewissen Dagobert Duck.

Zunächst muß die Sitzung unter einer neuen, noch freien Multicast-Adresse allokiert werden. Hierzu wurden für die Videoübertragung die IP-Adresse 224.2.7.13 und für den Ton die IP-Adresse 224.2.7.12 gewählt. Diese Daten werden dann mit einem SAP-Paket an die globale Adresse 224.2.127.254 mit dem UDP-Port 9875 geschickt, so daß der erste Teilnehmer auf Sendung gehen kann. Im folgenden werden noch SIP-Einladungen an Walt Disney und Theus Waigel geschickt, die diese gerne (mit SIP) annehmen. Da beide auch über Kamera und Mikrofon verfügen ,werden ihnen Multicast-Adressen für die Video- und Audioübertragung zugeteilt. Diese Veränderung der Sitzungumgebung wird per RSTP-Session wieder an unsere globale IP-Adresse geschickt.

Der Datenverkehr wird nun über die bekannten Adressen und Ports auf der Basis von RTP/RTCP abgewickelt. Die Steuerung der Sitzung erfolgt dann mit RTSP-Paketen.

Einer der drei Teilnehmer, Walt Disney, möchte nun um seine Aussagen über die Tüchtigkeit und Ehrbarkeit des von ihm vertretenen Dagobert Duck zu untermauern, ein Video abspielen. Hierzu schickt er eine Einladung an seinen Video-Server in Amerika. Da dieser zur Zeit im Zuge von video-on-demand vollständig überlastet ist, wird seine Anfrage abgelehnt. Der Retry-After-Parameter gibt an, daß der Server in zirka 5 Stunden wieder verfügbar sein wird. Nach diesem Fehlschlag verschickt Disney eine zweite Einladung, diesmal an seinen Video-Server in Paris. Dieser kann den gesuchten Film auch nicht bieten, liefert aber in seiner Fehlermeldung eine alternative Adresse in China. Der Server in China wird eingeladen und er antwortet mit einem einfachen OK. Für diesen Server wird eine neue Multicast-Adresse reserviert, auf der das Video gesendet wird. Die Veränderung der Sitzungsdaten wird dann wieder per RTSP-Session-Paket an die globale IP-Adresse geschickt.

Nach der vollständigen Integration aller aktiven Teilnehmer wird der Video-Server per RTSP-PLAY aufgefordert, das von Disney gewünschte Video abzuspielen. Der Server beantwortet die Anfrage mit einem OK und beginnt dann das Video an die ihm zugeordnete Multicast-Adresse zu senden. Während des Abspielens, das zirka 2 Stunden dauert, wird in regelmäßigen Abständen ein SAP-Paket mit den Sitzungsdaten an die globale IP-Adresse geschickt.Nachdem die Teilnehmer das Video zu einem großen Teil

gesehen haben, sind sie von Dagoberts Unschuld und Tugendhaftigkeit überzeugt und das Video kann angehalten werden. Hierzu wird ein RTSP-Paket mit STOP-Befehl an den Server geschickt. Dieser quittiert den Erhalt, stoppt das Video und verabschiedet sich aus der Sitzung per RTSP-BYE-Paket. Der geändert Zustand wird wieder an die globale IP-Adresse gemeldet.

Die Diskussion wird noch eine Weile vorgesetzt, am späten Abend jedoch aufgrund der Ermüdung aller Teilnehmer eingestellt. Hierzu wird mittels eines SAP-Paketes die Sitzung ganz einfach gelöscht.

6 Resümee

Die vorgestellten Protokolle befinden sich zur Zeit noch in der Spezifikation. Es ist daher davon auszugehen, daß noch kleinere Veränderungen im Protokollformat vorgenommen werden. Es ist weiterhin zu erwarten, daß, ähnlich wie bei HTTP, lediglich eine geringe Anzahl von Parametern, Attributen und Methoden von Anwendungen unterstützt werden muß. Durch den einfachen Aufbau der Paketformate ist aber insbesondere bei den Protokollen SDP und RTSP eine einfache Adaption an die individuellen Bedürfnisse des Anwenders bzw. der Anwendung möglich. Die Hauptproblematik, die bei der Realisierung von multimedialen Konferenzen im Internet noch besteht, ist die mangelnde Multicastfähigkeit der meisten Router im Internet. Dadurch sind die vorgestellt Mechanismen auf Testumgebungen wie das MBone beschränkt.

Literatur

[HaJa97] M. Handley und Van Jacobsen. SDP: Session Description Protocol. *internet-draft*, Marz 1997.

[Hand96] M. Handley. SAP: Session Announcement Protocol. *internet-draft*, November 1996.

[ScHS97] H. Schulzrinne, M. Handley und E. Schooler. SIP: Session Initiation Protocol. *internet-draft*, Marz 1997.

[Schu96] H. Schulzrinne. A real-time stream control protocol (RTSP). *internet-draft*, November 1996.

[Schu97] H. Schulzrinne. RTP Profile for Audio and Video Conferences with Minimal Control. *internet-draft*, Marz 1997.

[SJCF96] H. Schulzrinne, Van Jacobsen, S. Casner und R. Frederick. RTP: A Transport Protocol for Real-Time Applications. *RFC 1889*, Januar 1996.

Fibre Channel – GBit/s im Rechner und LAN

Timm Reinstorf

Kurzfassung

Fibre Channel tritt an, die immer weiter steigenden Qualitätsanforderungen jetziger und zukünftiger Anwendungen an die Übertragungstechnologien (wie Dateientransport, Videoübertragung in Echtzeit usw.) zu erfüllen. Dabei vereinigt Fibre Channel sowohl Kanaltechnologie als auch Netzwerktechnologie in sich und bietet damit mit einer einheitlichen Technologie einen sehr flexiblen Weg zur Integration verschiedener Bauteile im Rechner selbst, sowie einzelner Rechner im Netz untereinander. Hohe Übertragungsgeschwindigkeiten bis zu 1 GBit/s sowie die Reichweite bis zu 10 km und die geringen Latenzzeiten von Fibre Channel Kanälen machen Fibre Channel zu einer interessanten Alternative zu bisherigen Standards.

1 Einleitung

Ende der achtziger Jahre stellte sich immer deutlicher heraus, daß der größte Engpaß zukünftiger und teils auch schon damaliger Anwendungen die zu geringe Datenübertragungsleistungen zwischen Rechnern und ihren Peripheriegeräten sein würden. Während Prozessoren durch höhere Taktung immer schneller wurden, verbesserte sich die Übertragungsleistung der Kanaltechnologien kaum. So mußte der Prozessor immer größere Zeitspannen auf die Beendigung von Datenübertragungsoperationen warten. Zusätzlich wurden die Mengen der zu übertragenden Daten beispielsweise durch multimediale Anwendungen immer größer. Vor allen Dingen Anwendungen im medizinischen Bereich, Visualisierungsanwendungen oder die Verarbeitung von Satellitenbildern stießen an die Grenzen herkömmlicher Kanaltechnologien, die nicht mehr als beispielsweise 20 MByte/s (Wide-SCSI) übertragen konnten.

1988 begann deshalb die „Task Group for Device Level Interfaces" der amerikanischen Standardisierungsbehörde ANSI eine neue Kanaltechnologie zu definieren, welche die bisherigen Engpässe beseitigen sollte: den *Fibre Channel*. Fibre Channel sollte die Nachteile anderer Übertragungstechniken vermeiden und wurde am Anfang zum Beispiel als Alternative zu HIPPI (*High Performance Parallel Interface*) gesehen. Fibre Channel basiert im Gegensatz zu letzteren nicht auf paralleler, sondern auf serieller Übertragung. Der grundlegende Standard FC-PH (*Fibre Channel Physical and Signaling Interface*, siehe Abschnitt 3) sieht derzeit Übertragungsleistungen bis zu 1062 Mbit/s vor. Erweiterungen des Standards gehen aber noch weiter, so daß sich abzeichnet, daß mit Geschwindigkeiten von 1 Gbit/s Fibre Channel noch nicht ausgereizt ist (siehe Abschnitt 4).

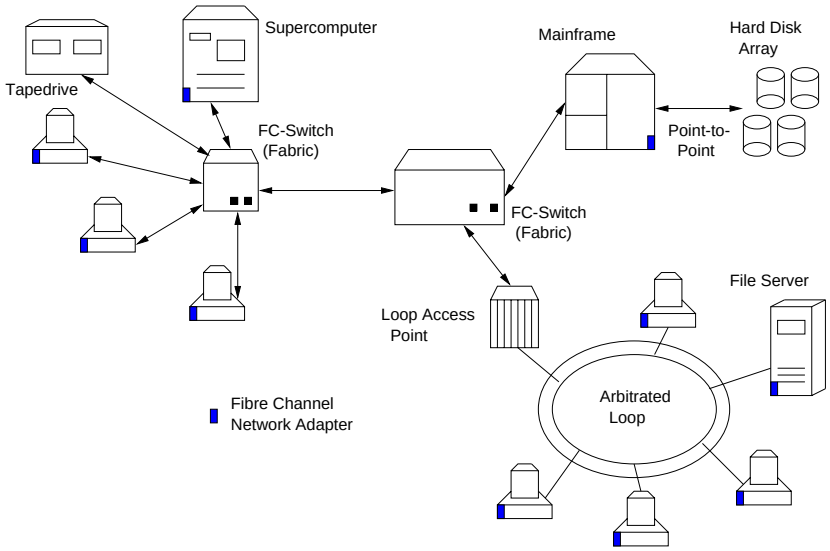


Abbildung 1: Beispiel eines Fibre Channel Systems

Inzwischen wurde zusätzlich das Potential von Fibre Channel als Netzwerktechnologie entdeckt und damit steht Fibre Channel auch in Konkurrenz zu ATM (*Asynchronous Transfer Mode*). Dabei kommt neben den hohen erzielbaren Geschwindigkeiten ein weiteres wesentliches Merkmal von Fibre Channel zur Geltung: die große Flexibilität des Standards. Er erlaubt die einfache Migration von bestehenden Systemen hin zu Fibre Channel Systemen durch die Unterstützung vieler Protokolle aus der Kanal- und Netzwerktechnik und bietet damit einen Schutz für frühere Investitionen. Die Benutzung der gleichen Technik als Kanal- und Netzwerktechnologie ist ein weiterer Vorteil. Gerade heutzutage, wo die Vernetzung der Rechner untereinander, aber auch mit Druckern und Speicherplatten immer mehr um sich greift, erscheint Fibre Channel als *die* Technologie der Zukunft. Ein beispielhaftes Fibre Channel System zeigt Abbildung 1.

In den folgenden Abschnitten wird der Aufbau von Fibre Channel Systemen und deren Architektur näher beschrieben, sowie ein Überblick über die betreffenden Standards gegeben. Abschließend werden einige Einsatzmöglichkeiten für Fibre Channel vorgestellt.

2 Fibre Channel Systeme

2.1 Nodes

Mit *Node* werden die Einheiten in Fibre Channel Systemen bezeichnet, die durch Fibre Channel miteinander verbunden sind. Ein Node kann also ein Rechner in einem Netzwerk, aber zum Beispiel auch ein einzelnes Ein-/Ausgabegerät wie eine Festplatte, eine Videokamera oder ein Drucker sein. Der Teil eines Nodes, der diesen mit dem Fibre Channel Link (dem physikalischen Kabel) verbindet, wird mit N_port (*Node port*) bezeichnet. Ein Node kann einen oder auch mehrere N_ports besitzen. Jeder Port besitzt eine 24-bit Adresse, die ihm beim *Fabric-Login* von der Fabric zugewiesen wird und eindeutig unter allen an der Fabric angeschlossenen Ports ist.

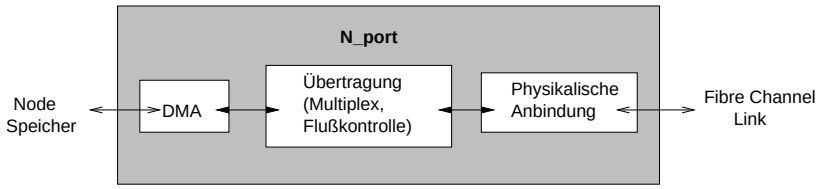


Abbildung 2: Beispielhafte Struktur eines N_port's

Die N_ports übernehmen die Umsetzung der Daten aus dem Node-Speicher (Puffer) auf das physikalische Medium. Dabei ist durch den Standard nicht festgelegt, welche der dafür zu erbringenden Leistungen – wie Flußkontrolle, Fehlererkennung usw. – als Hardware im N_port oder als Software im Node selbst realisiert sein sollte. Diese Flexibilität des Standards erlaubt sowohl leistungsfähige und damit teurere Lösungen bei denen Funktionen als Hardware im N_port realisiert sind, als auch kostengünstigere Varianten von Fibre Channel Geräten, die auf Softwarerealisierungen angewiesen und dadurch langsamer sind. Abbildung 2 zeigt beispielhaft die Struktur eines N_ports, der u.a. die Flußkontrolle hardwareseitig vornimmt. Folgender Unterabschnitt beschreibt die verschiedenen möglichen Verbindungstopologien von Nodes.

2.2 Topologien

Zu Beginn der Standardisierung von Fibre Channel waren zwei Verbindungskonzepte vorgesehen: das der *Fabric* und *Punkt-zu-Punkt* (Point-to-Point). Bei Punkt-zu-Punkt Verbindungen werden zwei N_ports bidirektional ohne zusätzliche Bauteile verbunden. Dazu wird je ein *Fibre Channel Link* für jede der beiden Richtungen benutzt. An Fabrics können dagegen mehrere Nodes oder andere Fabrics bidirektional (ebenso über zwei Links) an die F_ports (*Fabric ports*) der Fabric angeschlossen werden. Die Verbindungstopologie bleibt dabei verborgen. Die „Intelligenz" des Netzwerkes steckt in der Fabric (zu weiteren Informationen über das Routing bei Fibre Channel siehe [Sach94]).

Um auch kostengünstige Fibre Channel Lösungen zu ermöglichen, wurde in einer Erweiterung (FC-AL) des Standards eine zusätzliche Verbindungstopologie standardisiert: die *Arbitrated Loop*. Die Geräte sind dabei unidirektional über ihre *Loop Ports* (L_ports) in einer Ringstruktur miteinander verbunden (siehe Abbildung 3) und teilen sich untereinander ein Medium (*shared media*). Die Arbitrierung für das Medium erfolgt unter Berücksichtigung verschiedener Node-Prioritäten dezentral zwischen den angeschlossenen Nodes. Bei dieser Verbindungstopologie wird die Fabric eingespart. Loops unterliegen aber einigen Einschränkungen. So müssen alle Verbindungen in einem Loop die gleiche Datenrate benutzen, während hingegen Nodes, die über eine Fabric verbunden sind, unterschiedliche Datenraten verwenden können. Zusätzlich ist die Anzahl der Geräte in einem Loop auf 127 beschränkt. Zu einem beliebigen Zeitpunkt kann jeweils nur eine Verbindung zwischen zwei L_ports existieren. Erst wenn die beiden beteiligten L_ports die Verbindung wieder abgebaut haben, können zwei andere L_ports Daten austauschen. Loops könnten zum Beispiel als Kanal in einem Rechner eingesetzt werden, an dem verschieden Peripheriegeräte angeschlossen werden (vgl. [Frym95]).

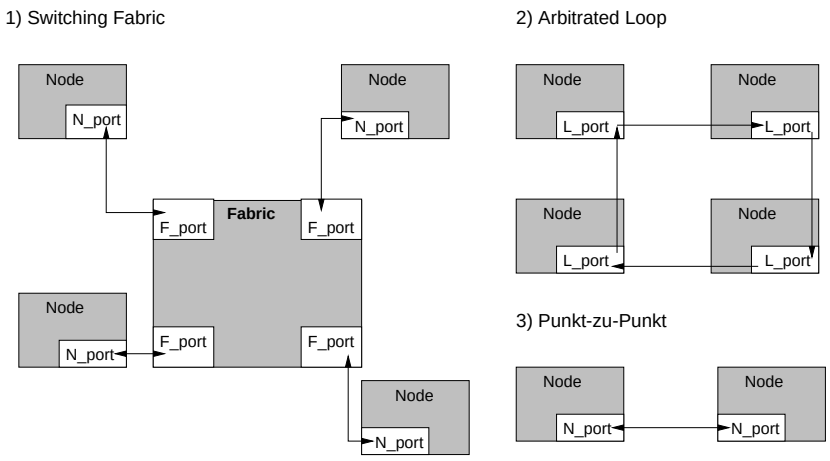


Abbildung 3: Fibre Channel - Topologien

Alle drei Verbindungstopologien sind zueinander interoperabel, das heißt ein Node (ein sogenannter *Loop Access Point*) in einem Loop kann zum Beispiel zusätzlich eine Verbindung zu einer Fabric besitzen und dadurch Daten von allen Nodes im Loop aus dem Loop „heraus" versenden. Die Ports solcher Nodes werden mit FL_ports und als NL_ports bei einer zusätzlichen Punkt-zu-Punkt Verbindung bezeichnet.

3 Fibre Channel - Protokollarchitektur

3.1 Überblick

Der Fibre Channel Standard ist in fünf Schichten (FC-0 bis FC-4, siehe Abbildung 4) strukturiert. Die Grundlagen der Fibre Channel Technik sind dabei in den drei Schichten FC-0 bis FC-2 festgesetzt, die im Standardisierungsdokument FC-PH (*Fibre Channel Physical and Signaling Interface*) beschrieben sind. Sie decken die Funktionalität der Schichten 1 (Physikalische Grundlagen) und 2 (Gesicherter Zugriff auf das Datenübertragungsmedium) des ISO/OSI Referenzmodells ab. In den Schichten FC-0 bis FC-2 werden zum Beispiel verwendbare Medien angegeben, sowie die Zeichenkodierung, Fehlererkennung und Flußkontrolle definiert. Diese Schichten werden näher in den Unterabschnitten 3.2 bis 3.4 beschrieben.

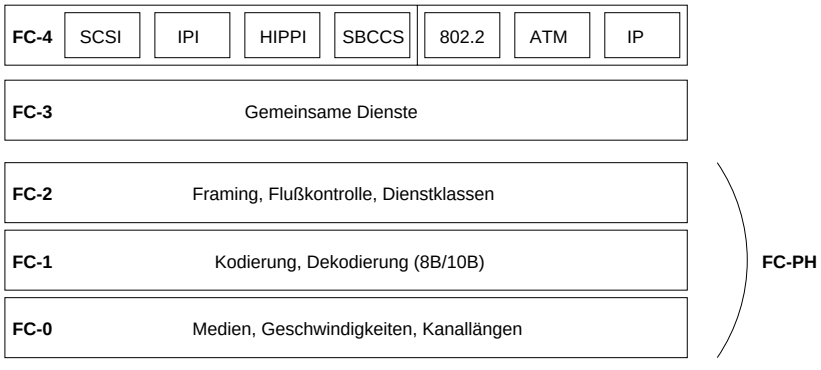


Abbildung 4: Schichten des Fibre Channel-Standards

Die auf den FC-PH aufsetzenden Schichten FC-3 und FC-4 beschäftigen sich mit höheren Funktionen und der Benutzung von existierenden Kanal- und Netzwerkprotokollen basierend auf Fibre Channel.

3.2 FC-0 : Medien, Geschwindigkeiten, Längen

Der Teil FC-0 des Standardisierungsdokuments FC-PH legt die *physikalischen Grundlagen* für Fibre Channel fest. Dazu gehören die verwendbaren Verbindungskabel, benutzbare Geschwindigkeiten und maximale Länge einer Verbindung von einem Port zum nächsten ohne zwischengeschaltete Repeater. FC-0 folgt dem Trend von Fibre Channel in vielen Bereichen flexibel zu sein: Die physikalischen Festlegungen sind keinesfalls starr. Es können außer Glasfaserkabeln je nach Anwendung und benötigter Geschwindigkeit auch Koaxialkabel oder sogar verdrillte Kupferkabel als Fibre Channel Links benutzt werden. Dadurch ergeben sich vielfältige Konfigurationen: Geschwindigkeiten mit 131, 265, 531 und 1062 Mbit/s und Maximallängen von 10 m (Miniatur-Koaxialkabel bei einer Signalrate von 1 Gbit/s) bis hin zu 10 km (Glasfaserkabel bei Signalraten bis zu 1 Gbit/s). Den Signalraten von 131 bis zu 1062 Mbit/s entsprechen Nutzdatenraten von 12,5 bis zu 100 MByte/s, die sich aus dem Overhead der Kodierung (siehe Abschnitt 3.3) berechnen. Zusätzlich zu den verwendbaren Medien und dadurch resultierenden Geschwindigkeiten und Kabellängen, definiert FC-0 in Abhängigkeit davon auch die benötigte Transmittertechnik in den jeweiligen Ports. Die möglichen Konfigurationen sind in Tabelle 1 dargestellt.

Außerdem spezifiziert FC-0 das Sicherheitssystem *Open Fibre Control system* (OFC) für Links mit Kurzwellenlaser. Tritt ein Schaden der Glasfaser auf, verringern sofort Sender und Empfänger ihre Leistung und gehen automatisch nach Reparatur des Schadens wieder zur vollen Leistung zurück (siehe [Megg94]).

3.3 FC-1 : Kodierung/Dekodierung

Die Schicht 1 des *Physical and Signaling Interface* legt das *Übertragungsprotokoll*, also wie Daten über die physikalische Leitung (festgelegt durch FC-0, vgl. Abschnitt 3.2) übertragen werden, Steuerungszeichen und Fehlerbehandlung fest.

Eine grundlegende Spezifikation ist dabei die Kodierung des Datenstroms vor dem Senden und entsprechend die Dekodierung beim Empfänger. Der Datenstrom wird in 8-bit Zeichen zerlegt, welche jeweils vor der Übertragung in 10-bit Übertragungszeichen kodiert und in Wörtern von vier Übertragungszeichen (also 40 Bits) gesendet werden. Diese von IBM[1] lizensierte 8B/10B Kodierung erlaubt einerseits eine sichere Synchronisation und einfache Taktrückgewinnung, andererseits lassen sich so außer 256 verschiedenen Datenzeichen zusätzliche Steuerungszeichen übertragen. Einige Steuerungszeichen dürfen in einem Datenstrom niemals vorkommen, so daß mit ihrer Hilfe eine Synchronisation auf Zeichen oder Wortgrenzen möglich ist. Auch das *Idle*-Steuerungszeichen, das zwischen einzelnen *Frames* (siehe Abschnitt 3.4.1) gesendet wird, dient zur Synchronisation. Dekodiert der Empfänger ein Übertragungszeichen, das weder Datenzeichen noch Steuerungszeichen ist, liegt ein Übertragungsfehler vor: ein sogenannter *code violation error*.

[1] IBM verwendet eine 8B/10B Kodierung im ESCON Standard

Medium	*Datenrate (MByte/s)*	*Signalrate (Mbit/s)*	*Entfernung*	*Transmitter*
9-μm-Mono-	25	265,62	bis 10 km	Longwave Laser
mode Glasfaser	50	531,25	bis 10 km	Longwave Laser
50-μm-Multi-	25	265,62	2 km	Shortwave Laser
mode Glasfaser	50	531,25	1 km	Shortwave Laser
	100	1062,5	bis 10 km	Longwave Laser
62,5-μm-Multi-	12,5	131,5	1,5 km	Longwave LED
mode Glasfaser	25	265,62	1 km	Longwave LED
Video-Koaxial-	12,5	131,81	100 m	ECL
Kabel	25	265,62	75 m	ECL
	50	531,25	50 m	ECL
	100	1062,5	25 m	ECL
Miniatur-Koaxial-	12,5	131,81	40 m	ECL
Kabel	25	265,62	30 m	ECL
	50	531,25	20 m	ECL
	100	1062,5	10 m	ECL
Shielded Twisted	12,5	133,81	100 m	ECL
Pair	25	265,62	50 m	ECL

LED Light Emitting Diode — *ECL* Emitter Coupled Logic

Tabelle 1: Einsetzbare Medien und damit erreichbare Geschwindigkeiten (Quelle [GuWi95])

Jedes zu übertragende 8-bit Zeichen besitzt zwei verschiedene 10-bit Kodierungen. Der Sender ermittelt für jedes Zeichen anhand des binären Parameters RD (*Running Disparity*) die zu verwendende Kodierung. Der Empfänger dekodiert jedes empfangene Zeichen anhand der momentanen RD und berechnet die neue RD mit dem gerade empfangenen Zeichen. Kann der Empfänger zu der aktuellen RD kein Codewort finden, zeigt er dem Sender eine *disparity violation condition* an (vgl. [Megg94]). Der Sender und der Empfänger sind nach der Übertragung des ersten Zeichens (für das der Empfänger noch beide Kodierungen zuläßt) auf eine RD synchronisiert. Die Benutzung der Running Disparity dient einerseits dem Ziel, eine möglichst gute Gleichstromfreiheit bei der Übertragung zu erreichen, andererseits der Erkennung von Übertragungsfehlern. Die Kodierungsregeln erlauben dem Empfänger alle ungeradzahligen Bitfehler und einige andere – wie einen *code violation error* – zu erkennen (vgl. [Sach94]).

3.4 FC-2 : Flußkontrolle, Rahmenprotokolle

Das Signalisierungsprotokoll (festgelegt in FC-2) stellt die Mechanismen für eine Übertragung von Anwendungsdaten über Fibre Channel bereit und bietet dafür verschiedene *Dienstklassen* an.

Die Hauptaufgabe des Signalisierungsprotokolls ist die Zerlegung des Datenstroms in sogenannte *Frames* sowie die Bereitstellung einer Flußkontrolle zwischen den Kommunikationspartnern, die je nach in Anspruch genommenem Dienst anders ausfällt. Außer den Frames führt die FC-2 Schicht aber noch weitere „Blöcke" ein, die hierachisch aufeinander aufbauen (einige Blöcke benutzen also andere) und im folgenden vorgestellt werden. Im Anschluß daran folgt die Vorstellung der von Fibre Channel angebotenen Dienste, die in Klassen eingeteilt sind (Unterabschnitt 3.4.2).

3.4.1 Übertragungsblöcke

Ordered Sets
Ordered Sets dienen allgemein der Übertragung von Steuerungsdaten als auch anwendungsspezifischer Daten. Ordered Sets bestehen aus einem Übertragungswort (vier Übertragungszeichen, entsprechend 40 bzw. 32 Bit). Mit Hilfe der Ordered Sets wird unter anderem die im Abschnitt 3.2 angesprochene Synchronisation auf Wortgrenzen erreicht, oder das Steuerungszeichen *Idle* implementiert. Ebenso sind die einen Frame begrenzenden *Start-of-Frame* und *End-of-Frame* Symbole (SOF und EOF; siehe Abbildung 5) Ordered Sets. Zu Ordered Sets gehören auch sogenannte *Primitive Signals*, die nicht in Zusammenhang mit anderen Konstrukten – wie etwa die SOF und EOF mit Frames – auftreten. Beispiele für Primitive Signals sind das *Idle*-Signal und *Receiver Ready* (R_RDY), welches anzeigt, daß der Interfacebuffer des empfangenden Ports wieder bereit ist, weitere Frames aufzunehmen.

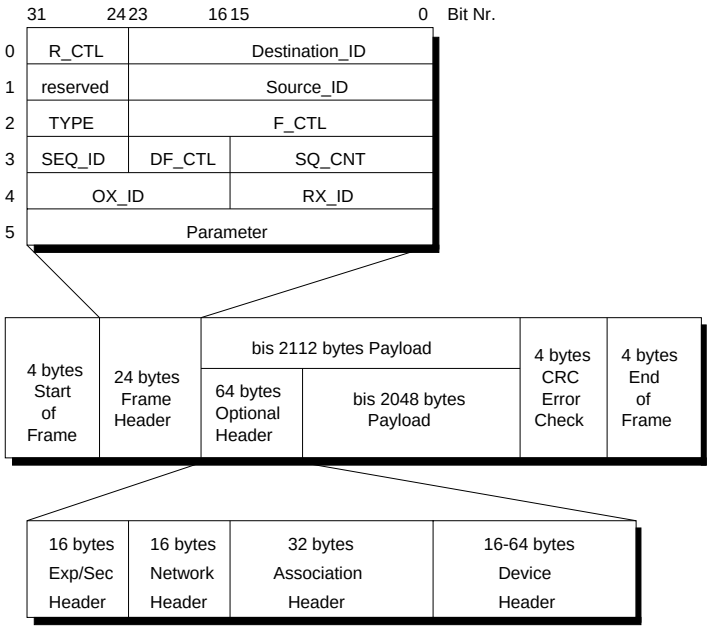


Abbildung 5: Genereller Aufbau eines Frames (Quelle: [Asso94])

Das Konzept der *Primitive Sequence* beruht ebenso auf Ordered Sets. Es dient dazu, der Gegenstelle spezielle Zustände mitzuteilen. Dazu wird ohne Unterbrechung ein Ordered Set solange mehrfach hintereinander gesendet, bis die Gegenstelle zum Beispiel auch mit einer Primitive Sequence reagiert. Durch FC-2 festgelegte Primitive Sequences sind zum Beispiel *Offline* (OLS), *Not Operational* (NOS), *Link Reset* (LR) und zur Antwort darauf ein *Link Reset Response* (LRR). Offline zeigt an, daß der das

Offline sendende Port abgeschaltet wird. Andere Ports ignorieren daraufhin Fehlermeldungen, die bei Verbindungsversuchen mit diesem Port auftreten. Not Operational sendet ein Port an sein Gegenüber, falls er kein ordentliches Signal empfangen konnte – beispielsweise weil er sich nicht auf den Sender synchronisieren konnte. LR und LRR werden benutzt, um eine dedizierte Verbindung (siehe Teilabschnitt 3.4.2, Klasse 1) abzubauen.

Frames
Frames sind logische Übertragungsblöcke, in denen die zu übertragenden Nutzdaten als sogenannter *Payload* eingepackt werden. Der Payload besteht dabei aus Ordered Sets, welche die Daten beinhalten. Es gibt zwei Klassen von Frames, *Data* und *Link_Control* Frames. Letztere übernehmen Steuerungsaufgaben und sind in *Acknowledge* (ACX) und *Link_Response* Frames unterteilt. Link_Response Frames melden Annahmeverweigerungen und Busy Zustände. Data Frames können *Link_Data* oder *Device_Data* Frames sein, je nachdem, ob der Frame zwischen Peripheriegeräten oder in einem Netzwerk ausgetauscht wird.

Ein Frame kann eine variable Länge von bis zu 2148 Bytes haben. Davon sind mindestens 36 Bytes Overhead, so daß sich 2112 Bytes als größtmögliche Datenpaketlänge ergeben. Der von einer Anwendung zu versendende Datenstrom wird in Pakete von maximal 2112 Bytes zerlegt, die jeweils innerhalb eines Frames verschickt werden.

Abbildung 5 zeigt die generelle Struktur eines Frames. Er wird von den Ordered Sets SOF und EOF begrenzt. Auf den Start-of-Frame folgt der Frame Header, der die IDs des Quell- und Zielports des Frames, sowie außer einigen Steuerungsinformationen den Typ des Protokolls, welches die Daten im Payload sendet, enthält. Dieses Protokoll kann ein Fibre Channel spezifisches sein oder ein auf Fibre Channel adaptiertes Protokoll (siehe Abschnitt 3.6). Die weiteren Parameter im Frame Header (SEQ_ID, SEQ_CNT, OX_ID und RX_ID) werden in den entsprechenden Abschnitten über die *Sequences* und die *Exchanges* (siehe unten) angesprochen. Dem Payload folgt ein 32-bit CRC (*Cycle Redundancy Check*) Feld, das der Erkennung von Übertragungsfehlern dient.

Sequences
Eine Sequence besteht aus einem oder mehreren Frames und beinhaltet die gesamten Daten eines Sendebefehls, die eventuell aufgrund ihrer Größe in mehrere Frames aufgeteilt werden mußten. Die Länge einer Sequenz ist unbegrenzt. Eine Sequenz ist unidirektional, wird also nur in einer Richtung übertragen. Jeder Frame hat in seinem Frame Header eine eindeutige Sequenz-ID (SEQ_ID) und Sequenznummer (SEQ_CNT; siehe Abbildung 5). Die Gegenseite kann mit Hilfe dieser Parameter den ursprünglichen Datenstrom wiederherstellen und an die nächsthöhere Protokollschicht weiterleiten. Die Fehlerkorrektur, die von einem höheren Protokoll erbracht werden muß, arbeitet gewöhnlich auf Sequenzen. Die Protokollschicht FC-2 liefert nur eine Fehlererkennung und -anzeige, so daß ein fehlender oder fehlerhafter Frame in einer Sequenz die erneute Übertragung der gesamten Sequenz impliziert.

Exchanges
Unter einem Exchange sind ein oder mehrere Sequenzen zusammengefaßt, die zusammen eine logische Kommunikation bilden. Dies kann zum Beispiel eine Anfrage und die zugehörige Antwort eines höheren Protokolls sein. Sequenzen können dabei abwechselnd (aber nie gleichzeitig) in unterschiedliche Richtungen (bezogen auf zwei N_ports)

übertragen werden, das heißt ein Exchange kann unidirektional oder bidirektional sein. In jedem Frame Header ist die ID des Initiators und die des Beantworters (OX_ID und RX_ID) gespeichert, wodurch ein Exchange eindeutig identifiziert wird.

3.4.2 Dienstklassen

FC-2 definiert die verschiedenen Dienstklassen, die Fibre Channel bietet. Dieses sind die Klassen 1 bis 3 und eine Kombination davon, die *Intermix* genannt wird. Als Ergänzung wurde in der Erweiterung des FC-PH (FC-EP) zusätzlich eine Klasse 4 definiert. Die Eigenschaften der einzelnen Klassen spiegeln die Anforderungen heutiger und (hoffentlich) künftiger Anwendungen wider. Eine Übersicht über die Charakteristik der Klassen 1 bis 3 gibt die Tabelle 2.

Klasse 1 stellt einen verbindungsorientierten Dienst mit dedizierter Leitung bereit (Leitungsvermittlung, bidirektionaler Datenaustausch). In einer Verbindungsaufbauphase wird ein Pfad zwischen den beiden an der Kommunikation beteiligten Ports festgelegt (also die genaue Route auch durch Fabrics hindurch). Danach kann auf diesen Teilen der Leitung nur noch Kommunikation zwischen den beiden betreffenen Teilnehmern erfolgen, Frames anderer Verbindungen werden nicht übertragen. Dadurch kann eine bestimmte Bandbreite garantiert werden, da die gesamte Bandbreite den beiden Teilnehmern exklusiv zur Verfügung steht. Außerdem ist die Übertragung von Daten über eine Klasse 1-Verbindung sehr effizient, da die Route der Frames nicht für jeden Frame erneut gefunden werden muß. Die Nachteile von Klasse 1 Verbindungen liegen sowohl in der langen Dauer des Verbindungsaufbaus, die bei 3 km schon 20 μs dauert, als auch in der auschließlichen Nutzung der Leitung durch zwei Ports. Außerdem bedingt die Flußkontrolle unter Umständen hohe Latenzzeiten (vgl. Teilabschnitt 3.4.3).

Klasse 2 ist ein verbindungsloser, aber gesicherter Dienst. Jeder Frame wird einzeln geroutet und Frames können auf einer Leitung gemultiplext werden. Die Klasse 2 bietet keine Bandbreitengarantien mehr, verringert dafür aber die Latenzzeiten.

Klasse 3 verhält sich wie die Klasse 2 ohne Empfangsbestätigung (unbestätigter Datagrammdienst). Die Benutzung von Klasse 3 kann bei Anwendungen, bei denen eine Sendewiederholung im Fehlerfalle unnütz wäre (zum Beispiel Videoübertragung), sinnvoll sein.

Intermix erlaubt eine Kombination der Klassen 1 bis 3. Hierbei wird eine Leitung für eine Klasse 1 Verbindung mit der gesamten Bandbreite reserviert. Wird diese Bandbreite allerdings nicht voll ausgenutzt, so können stattdessen auch Frames der Klassen 2 und 3 übertragen werden. Die vorhandene Bandbreite wird durch diesen Dienst damit maximal ausgenutzt.

Klasse 4 ist nicht im FC-PH enthalten, sondern wird als Erweiterung in FC-EP eingehen. Die Klasse 4 wird einen verbindungsorientierten Dienst zur Verfügung stellen, der sowohl anteilige Bandbreiten als auch Latenzzeiten garantiert, wie es zum Beispiel Echtzeitanwendungen erfordern.

Charakteristik	Klasse 1	Klasse 2	Klasse 3
Funktion	Dedizierte Verbindung	Multiplex (Frame Switched)	Datagramm
Fabric kann Frames wegwerfen	Nein	Nein	Ja
Verbindungstyp zwischen Ports	Eins zu Eins	Viele zu Vielen	
Initiale Verzögerung	Ja	Nein	Nein
Unidirektionale Verbindung	optional	Nicht möglich	
Ende-zu-Ende Flußkontrolle	Ja	Ja	Nein
Puffer-zu-Puffer Flußkontrolle	Nur beim 1. Frame	Ja, durch die Fabric	Ja, nur N_port zu F_port
Fabric kann Frames ablehnen	Nein	Ja, bei Routingproblemen	Nein (Frame wird weggeworfen)
Garantierte Reihenfolgetreue	Ja	Hängt von der Fabric ab	

Tabelle 2: Charakteristik der Dienstklassen 1 bis 3 (Quelle: [Asso94])

3.4.3 Flußkontrolle

Die Flußkontrolle verhindert den Überlauf von Empfangspuffern der Ports, in dem erst dann weitere Frames gesendet werden, wenn entweder der Empfängerport den Empfang des vorherigen Frames bestätigt (Klasse 1, vgl. Teilabschnitt 3.4.2) oder der Sendeport ein R_RDY-Signal (*Receiver Ready*) bekommt (Klasse 2 und 3). Die dynamische Größe des Empfangspuffers wird dem Sender vor dem Senden mitgeteilt („Es sind noch x Pufferplätze frei"). Die Art der verwendeten Flußkontrolle (Ende-zu-Ende oder Puffer-zu-Puffer) hängt von der benutzten Dienstklasse ab.

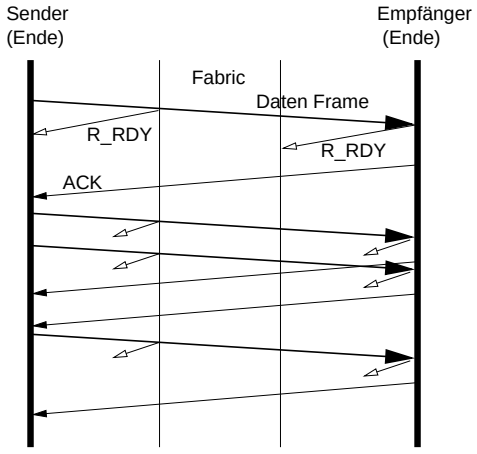


Abbildung 6: Klasse 1 Flußkontrolle

In Klasse 1 findet immer eine *Ende-zu-Ende* Flußkontrolle statt (siehe Abbildung 6). Der Sender sendet entsprechend der Puffergröße des Empfängers ein oder mehrere Frames ab. Danach wartet er auf die Empfangsbestätigungen (*Acknowledge*, ACK) des Empfängers. Nach dem Empfang eines ACKs kann der Sender wieder einen Frame senden. Sendet der Empfänger anstatt eines ACK einen *Reject* Frame, so konnte der Frame nicht angenommen werden und der Sender muß die Daten wiederholen.

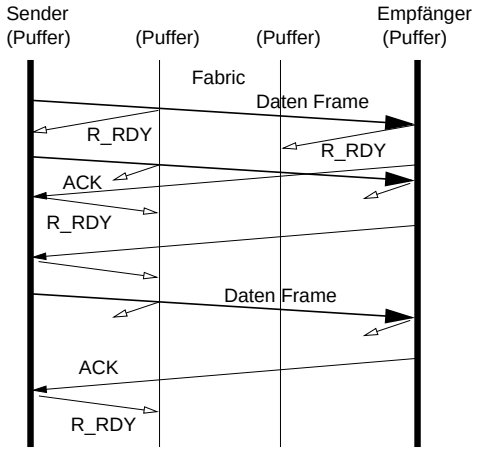


Abbildung 7: Klasse 2 Flußkontrolle

Klasse 2 verwendet eine *Puffer-zu-Puffer* Flußkontrolle. Dabei bezeichnet „Puffer" einen Port, der auf dem Weg vom Sender zum Empfänger liegt (siehe Abbildung 7). Der Sender schickt sofort weitere Frames, nachdem er ein *Receive Ready* (R_RDY) Signal von dem mit ihm verbundenen nächsten Port erhalten hat. Dadurch kann die Situation entstehen, daß der Empfänger den Frame nicht annehmen kann, da sein Empfangspuffer voll ist. In diesem Fall schickt er dem Sender ein *Busy* Signal, das den Sender zum Wiederholen der Sendung auffordert. Der Empfänger quittiert den Empfang der Frames mit einem ACK.

Die Flußkontrolle der Klasse 3 findet wie in der Klasse 2 auf Pufferebene statt (Puffer-zu-Puffer). Da aber keine Empfangsbestätigungen gesendet werden, kann auf vom Empfänger abgewiesene oder fehlerhafte Frames nicht reagiert werden.

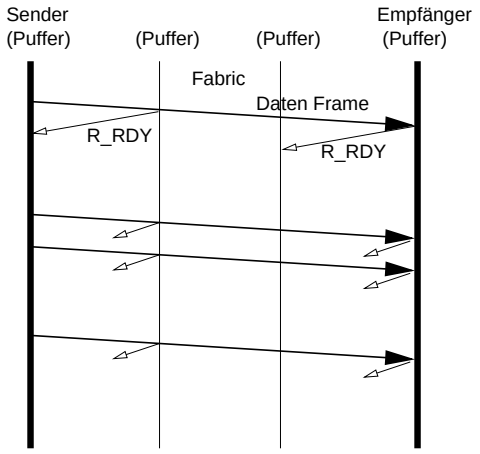


Abbildung 8: Klasse 3 Flußkontrolle

3.5 FC-3: Allgemeine Servicedienste

Der Standard sieht für die Schicht FC-3 die Spezifikation von allgemein zu benutzenden Diensten vor. Folgende drei Konzepte sind bereits spezifiziert:

Striping dient zur Erhöhung der Bandbreite, in dem Daten über mehrere Ports und parallele Leitungen gesendet werden.

Hunt Groups erlauben mehrere Ports unter einer Aliasadresse zusammenzufassen, so daß alle diese Ports Frames an diese Adresse annehmen können und dadurch die Wahrscheinlichkeit von Geschwindigkeitseinbußen aufgrund belegter Ports verringert wird.

Multicast ermöglicht effiziente Gruppenkommunikation. Mit Multicast können eine Teilmenge oder alle (Broadcast) an einer Fabric angeschlossenen Ports eine Übertragung erhalten.

3.6 FC-4: Schnittstelle zu den Anwendungen

Ein weiterer wichtiger Teil des Fibre Channel Standards ist die Schicht FC-4, denn diese Schicht soll sicherstellen, daß Fibre Channel möglichst einfach und schnell in der Praxis eingesetzt werden kann. Ein neuer Kommunikations-Standard, selbst wenn er neue Geschwindigkeitsstufen erreicht, nützt in der Praxis nur wenig, wenn er keine Möglichkeit bietet, vorhandene Protokolle mit diesem zu benutzen.

Erfreulicherweise existieren einige sogenannte „Mapping Protokolle" für viele der wichtigsten Kanal- und Netzwerkprotokolle (siehe Abbildung 4). Darunter sind sowohl Umsetzungsstandards für Protokolle, die hauptsächlich im Supercomputerumfeld verwendet werden (IPI, HIPPI), aber auch solche, die eine größere Verbreitung im Massenmarkt haben (SCSI). Im Netzwerkbereich werden unter anderem ATM (*Asynchronous Transfer Mode*) und IP (*Internet Protocol*) unterstützt.

4 Status der Standards

4.1 Standardisierungsdokumente

Im Umfeld des Standardisierungsdokumentes FC-PH, das bereits fertiggestellt ist, sind vielzählige weitere Dokumente entstanden, die sich detaillierter mit Fibre Channel Fragen beschäftigen (siehe Tabelle 3).

4.2 Organisationen und Gremien

Das große Potential des Fibre Channel Standards lenkte schon früh das Interesse von Rechner- und Peripheriegeräteherstellern auf sich. Diese Gruppe war sehr an einer schnellen und wirtschaftlichen, praktikablen Nutzung der Fibre Channel Technologie interessiert. Aus diesem Grund wurde Anfang 1993 die *Fibre Channel Association*

FC-SB:	Umsetzung des *Single Byte Command Code Set* (SBCCS)
FC-FP:	Umsetzung von HIPPI-FP (*High Performance Parallel Interface Framing Protocol*)
FC-LE:	Umsetzung von IEEE 802.2 (*Link Encapsulation*, LLC)
FC-I3:	Umsetzung von IPI-3
SCSI-3-FCP:	Umsetzung von SCSI-3 (*Small Computer System Interface*)
SCSI-GPP:	Umsetzung des Generic Packetized Protocol
FC-ATM:	Umsetzung von ATM (*ATM Adaption Layer 5*, AAL5)
FC-AL:	Arbitrated Loop
FC-SW:	Switch Fabric
FC-FG:	Generic Fabric Requirements
FC-EP:	Fibre Channel Enhanced Physical, kompatible Erweiterung von FC-PH
FC-GS:	Generic Services
FC-IG:	Fibre Channel Implementation Guide

Tabelle 3: Fibre Channel Standards (Quelle: [GuWi95])

(FCA) gegründet, ein Verband von namhaften Herstellern, der sich zum Ziel setzte einerseits die Arbeit des Standardisierungskomitees X3T9.3 (*Task Group for Devive Level Interfaces*) des *Technical Commitee for I/O Interfaces* (X3T9) der ANSI Behörde zu unterstützen, andererseits aber auch Marketing für Fibre Channel zu betreiben und Produkte vorzustellen.

Ebenfalls Anfang 1993 wurde unabhängig von der FCA die *Fibre Channel System Initiative* (FCSI) von IBM, Sun und HP ins Leben gerufen, die einige Beschränkungen der Optionsvielfalt des Fibre Channel Standards zur einfacheren Umsetzung in reale Produkte empfahl. Dabei hing es vom Anwendungsgebiet ab, welche Teilmengen der Fibre Channel Optionen in welchen Produkten sinnvoll einsetzbar seien. Im Zuge der Arbeit der FCSI entstanden eine Reihe von Dokumenten, die zum Beispiel IP und SCSI über Fibre Channel, aber auch die Benutzung von Fibre Channel in bestimmten Projekten der Raumfahrtindustrie beschreiben und welche Herstellern von Fibre Channel Produkten als Richtlinien dienen sollen.

4.3 Produkte

Die ersten Fibre Channel Produkte hatten noch sehr mit Schwierigkeiten zu kämpfen, die spezifizierten Geschwindigkeiten auch real anbieten zu können. Viele der ersten Produkte waren in GaAs (*Galliumarsenid*) Schaltkreistechnik gefertigt, die zwar hohe Schaltgeschwindigkeiten erlaubt, aber für den größeren Markt unbezahlbar ist.

Im Laufe des Jahres 1994/95 kamen aber verstärkt auch CMOS-basierte Produkte auf den Markt, die durchaus die Hoffnung weckten, daß Fibre Channel Technologie doch bezahlbar wird. Inzwischen gibt es weit über 30 Hersteller, die auf verschiedenen Gebieten – je nach Branche – Fibre Channel Produkte anbieten. Ein Bereich betrifft Speicherperipheriegeräte. Dort existieren mittlerweile zahlreiche Fibre Channel fähige Geräte, wie zum Beispiel Festplatten. Dieser Bereich basiert aus Kostengründen hauptsächlich auf Arbitrated Loop Systemen und hat möglicherweise das größte Potential die Fibre Channel Technologie im Massenmarkt zu etablieren. Hersteller wie IBM und

Ancor bieten aber auch Fibre Channel Systeme an, die auf einer Fabric als Verbindungstopologie bauen (Switches, Hubs, Adapterkarten). Erst allmählich kommen die ersten Generationen von Geräten auf den Markt, welche die Kinderkrankheiten der ersten Produkte abgelegt haben. Große Probleme entstanden am Anfang durch kuriose Konfigurationsprobleme („Karte xy läuft nur im 1. Slot des Rechners z") und durch Kompatibilitätsprobleme bei Verbindungen von Geräten unterschiedlicher Hersteller. Diese Probleme scheinen gelöst zu sein und so ist mit einer weiteren Verbreitung von Fibre Channel in Zukunft verstärkt zu rechnen.

5 Zusammenfassung und Ausblick

5.1 Anwendungsgebiete für Fibre Channel

Fibre Channel kann überall dort eingesetzt werden, wo ATM auch eingesetzt werden könnte, auch wenn Fibre Channel einige Vorteile gegenüber ATM besitzt. Die Vorteile zieht Fibre Channel hauptsächlich aus seiner Herkunft aus der Kanaltechnologie, wodurch Fibre Channel selbst noch kürzere Verzögerungen als ATM erreicht. Ein weiterer Pluspunkt von Fibre Channel liegt in der Flexibilität und dem Zusammenarbeiten mit vielen Protokollumgebungen. Auch die gebotenen Geschwindigkeiten sind vergleichbar oder sogar um einiges höher als die von ATM bereitgestellten Datenraten. Insgesamt neigt Fibre Channel mehr zum LAN- und rechnerinternen Einsatz, während hingegen ATM größtenteils im Backbone und WAN-Umfeld benutzt wird. Somit ist eine Existenz beider Standards nebeneinander durchaus vorstellbar und wahrscheinlich.

Eingesetzt wurde Fibre Channel in der Vergangenheit hauptsächlich im professionellen Supercomputerumfeld. Beispielsweise wird Fibre Channel in Kliniken verwendet, um Röntgenbilder und ähnlich große Datenmengen in Echtzeit von Operationsräumen oder Intensivstationen zu Arztbüros zu transportieren. Ein weiteres Einsatzgebiet für Fibre Channel sind Publishing Anwendungen, die große Bild- (oft mit 16 Millionen Farben) und Textdaten zwischen Filialen und Druckereien austauschen müssen. Genauso könnte auch die (Trick-) Filmindustrie vom Fibre Channel Gebrauch machen, um die riesigen dort anfallenden Datenmengen zu bewältigen (vgl. [GoKe95]).

5.2 Ausblick

Insgesamt scheint Fibre Channel den Anforderungen im zukünftigen Informationszeitalter im lokalen Netzwerk und rechnerinternem Kanal-Bereich am besten zu gegnügen. Geschwindigkeiten im Gbits/s Bereich (2, 4, 8 und 16 Gbit/s sind als Erweiterungen für die Zukunft vorgesehen), bis zu 10 km Verbindungslängen und eine große Flexibilität in allen Bereichen (zum Beispiel Umsetzung vorhandener Protokolle) untermauern diesen Anspruch. Da zusätzlich die praktischen Realisierungen von Fibre Channel Produkten immer zahlreicher, ausgereifter und preiswerter werden, steht einem weiten Einsatz von Fibre Channel im ganzen Anwendungsspektrum der datenintensiven Übertragung nichts mehr im Wege. Dies wird zudem durch die breite Akzeptanz von Fibre Channel bei den größten Anbietern von Datenübertragungslösungen bekräftigt.

Literatur

[Asso94] The Fibre Channel Association. Fibre Channel Reference Card, Version 2.0. Juli 1994.

[Frym95] E. M. Frymoyer. Fibre Channel Fusion: Low Latency, High Speed. *Data Communications*, Februar 1995.

[GoKe95] W. Goralski und G. Kessler. Fibre Channel: Standards, Applications, and Products. *http://www.hill.com/personnel/gck/fibre_channel.html*, Dezember 1995.

[GuWi95] M. Gumbold und M. Willem. Bypass für den Datenstau. *iX*, April 1995, S. 146–158.

[Megg94] Z. Meggyesi. Fibre Channel Overview. *http://www.cern.ch/HSI/fcs/spec/overview.htm*, 1994.

[Sach94] M. W. Sachs. *High Performance Networking: Technology and Protocols.* Fibre Channel. A.N. Tantawy (Hrsg.); Kluver. 1994.

[SaVa96] M. W. Sachs und A. Varma. Fibre Channel and Related Standards. *IEEE Communcations Magazine*, August 1996, S. 40–49.

[Schn95] G. Schnurer. Fire, Fibre, SSA. *c't*, Juni 1995, S. 126–134.

[WaFr95] P. Walford und E. Frymoyer. Providing Interoperable High Speed Connections with Fibre Channel Technology. *ConneXions*, März 1995, S. 24–34.

Abbildungsverzeichnis

Tabellenverzeichnis