INSTITUT FÜR INFORMATIK
DER TECHNISCHEN UNIVERSITÄT MÜNCHEN

Diplomarbeit

Vergleich von Entwicklungen für Quality of Service für IP-Netze

Bearbeiter:	Martin Friedrich
Aufgabensteller:	Prof. Dr. Heinz-Gerd Hegering
Betreuer:	Holger Schmidt Norbert Wienold

INSTITUT FÜR INFORMATIK
DER TECHNISCHEN UNIVERSITÄT MÜNCHEN

Diplomarbeit

Vergleich von Entwicklungen für Quality of Service für IP-Netze

Bearbeiter:	Martin Friedrich
Aufgabensteller:	Prof. Dr. Heinz-Gerd Hegering
Betreuer:	Holger Schmidt Norbert Wienold

Abgabetermin:	15. Februar 2000

Hiermit versichere ich, daß ich die vorliegende Diplomarbeit selbständig verfaßt und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 15. Februar 2000

. . . .
(Unterschrift des Kandidaten)

Zusammenfassung

Diese Diplomarbeit befaßt sich mit Entwicklungen für Quality of Service in IP-Netzen.

Differentiated Services ist eine Architektur, um in einem IP-Netz mehrere Dienstgüten für den Kommunikationsdienst des Internet Protocols bereitzustellen. Eine weiterer Ansatz für mehrere Dienstgüten in einem IP-Netz ist *Integrated Services*. Integrated Services definiert Dienstgüten für Kommunikationen in IP-Netzen auf OSI-Schicht 4. Mit *Resource Reservation Protocol* existiert ein Protokoll, mit dem für eine Kommunikation diese Dienstgüten angefordert werden können. Diese Entwicklungen werden vorgestellt.

Die Kommunikationsdienste auf OSI-Schicht 3 und 4 stützen sich auf die Kommunikationsdienste der verwendeten Netztechnologien ab. Eine Betrachtung der Kommunikationsdienste und Dienstgüten von bestimmten Netztechnologien zeigt, deren Grundlagen für Dienstgüten auf höheren Schichten.

Es wird eine Kriterienkatalog erarbeitet, um Entwicklungen für Quality of Service vergleichen zu können.

Anhand dieses Kriterienkatalogs wird ein Vergleich der Entwicklungen Differentiated Service und die Kombination Integrated Services und Resource Reservation Protocol durchgeführt. Bei diesem Vergleich werden die Einflüsse der zugrunde liegenden Netztechnologien mit betrachtet. Hierfür muß man zuerst untersuchen, wie die Entwicklungen auf die einzelnen Netztechnologien aufsetzen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einführung

IP-Netze, d.h. Netze mit Protokollen aus der TCP/IP-Protokollfamilie (Transmission Control Protocol/Internet Protocol), sind weit verbreitet. Auf der Basis dieser Protokolle wurden viele Anwendungsprotokolle, wie FTP, SMTP und Telnet, entwickelt. Diese Anwendungen haben gemeinsam, daß sie relativ wenig Anforderungen an die *Dienstgüte* (Quality of Service, QoS) des *Kommunikationsdienstes* eines IP-Netzes stellen. Die Übertragungszeit ist ein Beispiel für einen Parameter, der die Dienstgüte eines Kommunikationsdienstes beschreiben kann.

Da in IP-Netzen diese Anwendungen lange Zeit dominant waren, hat man dort wenige Anstrengungen dem Thema Quality of Service gewidmet. Doch folgende Impulse haben dafür gesorgt, daß die Bemühungen verstärkt werden:

- **Neue Anwendungsgebiete mit höheren Dienstgüteanforderungen**
  Die Steigerung des Leistungsvermögens von Netztechnologien und Arbeitsplatzrechnern macht neue Anwendungen, wie zum Beispiel die Internettelefonie und die Videoübertragung, möglich. Diese Anwendungen haben erhöhte Ansprüche an die benötigte Bandbreite und die Übertragungszeiten, die mit den klassischen Anwendungen nicht zu vergleichen sind.

- **Neue Netztechnologien mit Dienstgüteunterstützung**
  Neuere Netztechnologien, wie Asynchronous Transfer Mode (ATM), wurden mit dem Ziel entwickelt, mehrere Dienstgüten bereitzustellen. Jedoch ist die Nutzung dieser Dienstgüten durch die TCP/IP-Protokolle, die hierfür nur schwache Kontrollstrukturen besitzen, behindert.

- **Vereinheitlichung der OSI-Schicht 3 Protokolle nach IP**
  Bisher wurden für Anwendungsgebiete mit speziellen Dienstgüteansprüchen proprietäre Netztechnologien mit eigenem Protokoll der OSI-Schicht 3 eingesetzt. Mit der Ausbreitung der Vernetzung legen immer mehr Netzbetreiber Wert darauf, daß ihre Netze mit anderen verbunden werden. Dies legt die Verwendung eines einheitlichen OSI-Schicht 3 Protokolls nahe, ohne jedoch auf die gewünschte Dienstgüte verzichten zu müssen. Für die Entscheidung, IP als das einheitliche OSI-Schicht 3 Protokoll, sprechen mehrere Gründe: das IP-Protokoll ist offengelegt und mit dem Internet steht eine große Infrastruktur zur Verfügung.

- **Ökonomische Gründe**
  Höhere Ansprüche an die Dienstgüte führen zu dem Gebrauch von mehr Kommunikationsressourcen, um diese bereitzustellen. Um die Kosten für ein Netz so gering wie möglich zu halten, versucht man die Kommunikationsressourcen möglichst gut auszunutzen. Zu diesem Zweck sind mehrere verschiedene Dienstgüten wünschenswert, die den Nutzern des Kommunikationsdienstes nur soviel Ressourcen geben wie sie benötigen.

Die *Internet Engineering Task Force* (IETF), eine Interessengemeinschaft zur Verbesserung des Internets, arbeitet an Lösungsmöglichkeiten mehrere Dienstgüten in einem IP-Netz den Anwendungen anzubieten (siehe Abbildung 1).

Diese Arbeit befaßt sich mit der Dienstgüte (Quality of Service) in IP-Netzen. Die wichtigsten Begriffe für diese Arbeit werden in den nächsten zwei Abschnitten eingeführt.

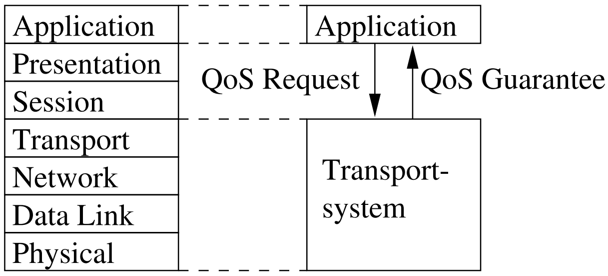

Abbildung 1: Anforderung einer Dienstgüte

1.1 Dienst, Dienstgüte und Dienstklasse

Ein Kommunikationsdienst, kurz *Dienst*, wird von einer Instanz der Schicht-(N) des *Open System Interconnection* Referenzmodells (OSI-RM) (siehe Abbildung 2) einer Instanz der übergeordneten Schicht-(N+1) bereitgestellt [Hals 96][HeAb 93]. Die Instanz der Schicht-(N) wird daher als Diensterbringer und die der Schicht-(N+1) als Dienstnutzer bezeichnet. Für die Schicht-(N+1) erscheint der Dienst einer Instanz der Schicht-(N) wie eine

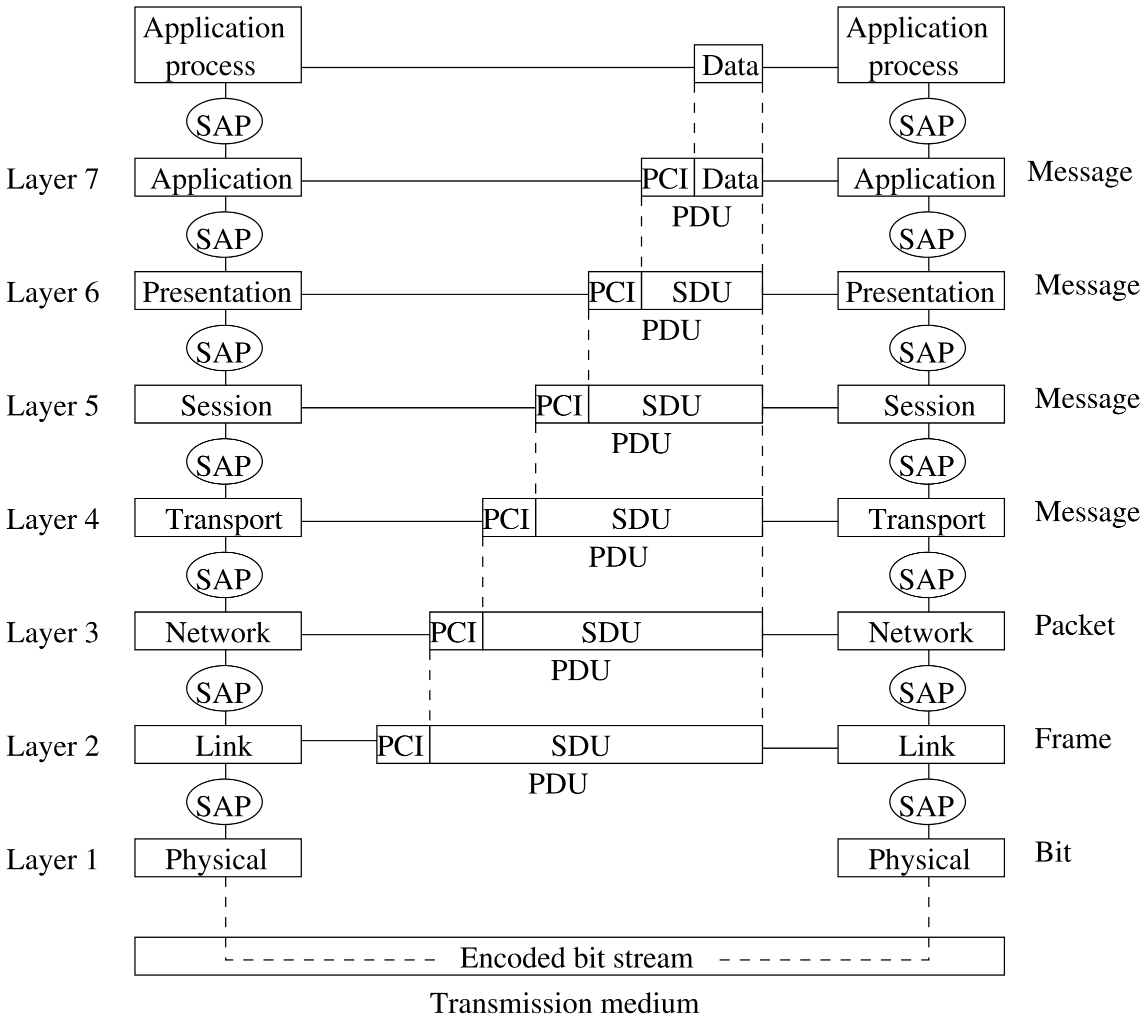

Abbildung 2: OSI-Referenzmodell

virtuelle Kommunikation auf Schicht-(N). Die Kommunikation zwischen den Schicht-(N)- und Schicht-(N+1)-Instanzen (Nachbarinstanzen) erfolgt mittels *Dienstprimitive* (Service Primitives) an den *Dienstzugangspunkten* (Service Access Point, SAP) der Schicht-(N)-Instanzen, die Kommunikation zwischen Schicht-(N)-Instanzen (Partnerinstanzen) mittels *Protocol Data Units* (PDUs).

Um den Dienst der Schicht-(N)-Instanz zu nutzen, stellt man eine Anforderungsprimitive (Request Primitive) an dessen SAP. Diese Anforderung wird der Partnerinstanz mit einer Indication Primitive angezeigt. Den Dienst einer Instanz kann man in zwei Typen einteilen: *Bestätigt* (Confirmed) und *Unbestätigt* (Unconfirmed) (siehe Abbildung 3). Der

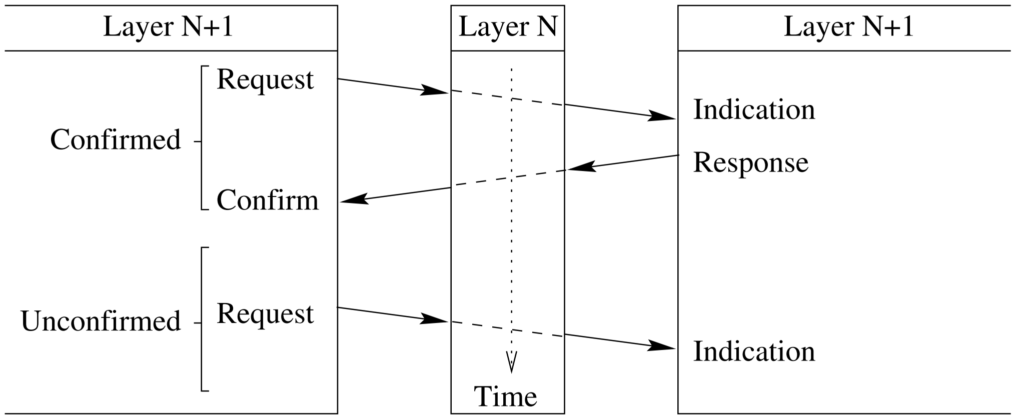

Abbildung 3: Dienstprimitive [Hals 96]

bestätigte Dienst zeichnet sich dadurch aus, daß die eine Instanz auf eine Indication Primitive reagiert und eine Response Primitive absetzt. Dies wird dann der Partnerinstanz mit einer Confirm Primitive angezeigt.

Dienstprimitive haben mehrere Parameter. Der Parameter für die zu übertragenden Daten wird als *Service Data Unit* (SDU) bezeichnet. Mit der Dienstprimitive und ihren Parametern erzeugt eine Schicht-(N)-Instanz eine *Protocol Data Unit* (PDU je nach OSI-Schicht auch als Nachricht, Paket oder Frame bezeichnet; siehe Abbildung 2). Die PDU der Schicht-(N)-Instanz besteht dabei aus einer Protocol Control Information (PCI, der Header und gegebenenfalls noch ein Trailer) und der SDU für die Schicht-(N)-Instanz (entspricht (N+1)-PDU).

Unter dem Begriff *Dienstgüte* faßt man alle Eigenschaften (Parameter), mit denen ein Netznutzer die Qualität eines Kommunikationsdienstes charakterisieren kann, zusammen.

In jeder Schicht des OSI-Referenzmodells werden Dienste erbracht. Die Dienstgüte eines Dienstes wird durch alle seine Eigenschaften, die ein Dienstnutzer am SAP des Dienstes beobachten kann, bestimmt. Diese Eigenschaften werden durch die Implementierungen aller darunterliegenden Schichten beeinflußt.

Beispiele für Dienstgüteparameter sind:

- **Übertragungsverzögerung** (Transfer Delay)
  Die Zeitspanne zwischen einen `DATA.request` (Dienstprimitve, um eine Übertragung

von Daten zu initiieren) und dem daraus resultierenden `DATA.indication` (Dienstprimitive, die den Erhalt von Daten anzeigt).

- **Durchsatz** (Throughput)
  Die Anzahl von SDU-Octets, die in einem festen Zeitintervall erfolgreich übertragen werden.

- **Verlust** (Loss)
  Der Prozentsatz, der bei der Übertragung verlorengegangenen PDUs.

Für Kommunikationsdienste mit vergleichbarer Dienstgüte wird der Begriff *Dienstklasse* verwendet.

1.2 IP-Netze

Ein IP-Netz ist ein *Packet-Switching Network*. Ein Packet-Switching Network besteht aus Knoten, die miteinander verbunden sind. Die Knoten des IP-Netzes sind die *Router* (Knoten auf OSI-Schicht 3), *Gateways* (Knoten auf OSI-Schicht 4 und höher) oder *Hosts* (Knoten auf OSI-Schicht 3 und höher). *Subnetze* stellen die Verbindung zwischen mehreren Hosts her. Damit Hosts aus verschiedenen Subnetzen miteinander kommunizieren können, sind die Subnetze durch Router oder Gateways verbunden (siehe Abbildung 4). Ihre Aufgabe

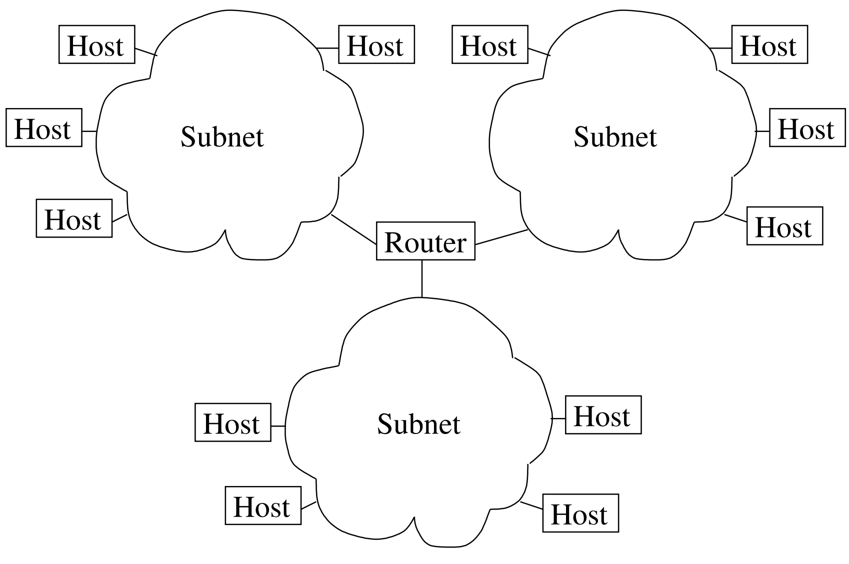

Abbildung 4: IP-Netz

ist es, PDUs von einem Subnetz in ein anderes zu übertragen.

Ein Subnetz wird durch eine Netzadresse eingegrenzt. Die Netzadresse ist ein Präfix, als Netzmaske bezeichnet, einer IP-Adresse (z.B. 172.16.0). Alle Hosts mit diesem Präfix in ihrer IP-Adresse gehören zu diesem Subnetz. Ein Subnetz wird mittels Netztechnologie der OSI-Schicht 2 und abwärts aufgebaut. In einem Subnetz können Netztechnologien, wie Ethernet und ATM, mit unterschiedlichen Diensten und auch unterschiedlicher Dienstgüte zum Einsatz kommen.

1.3 Aufgabenstellung

Ziel dieser Diplomarbeit ist es Entwicklungen für Quality of Service in IP-Netzen zu vergleichen. Diese Aufgabe teilt sich in vier Teilaufgaben:

1. **Vorstellung von Entwicklungen für Quality of Service auf OSI-Schicht 3 und 4**
   In Kapitel 2 werden die Entwicklungen *Differentiated Services*, *Integrated Services* und *Resource Reservation Protocol* vorgestellt. Diese Entwicklungen ermöglichen es, für einen Kommunikationsdienst auf OSI-Schicht 3 oder 4 eine bestimmte Dienstgüte zu erhalten.

2. **Analyse der Dienste und Dienstgüten spezieller Netztechnologien**
   Die Entwicklungen auf OSI-Schicht 3 und 4 bauen ihre Dienstgüten auf den Kommunikationsdiensten der OSI-Schicht 1 und 2 auf. Die Netztechnologien Sonet/SDH, ATM und Ethernet verfügen über Kommunikationsdienste der OSI-Schicht 1 und 2[1]. Diese Netztechnologien werden in Kapitel 3 auf ihre Dienste und Dienstgüten untersucht.

3. **Erstellung eines Kriterienkatalogs zum Vergleich von Entwicklungen für Quality of Service in IP-Netzen**
   In Kapitel 4 wird ein Kriterienkatalog erstellt, anhand dessen die Entwicklungen für Quality of Service verglichen werden können.

4. **Anwendung des Kriterienkatalogs**
   Hier wird gezeigt, wie die Entwicklungen der OSI-Schicht 3 und 4 auf den einzelnen Netztechnologien aufsetzen. Auf die Kombinationen der Technologien aus erstens und zweitens wird dann der Kriterienkatalog angewandt (siehe Kapitel 5).

[1] nicht für Sonet/SDH

2 Entwicklungen für QoS auf OSI-Schicht 3 und 4

In diesem Abschnitt sollen Lösungsansätze vorgestellt werden, mit denen mehrere Dienstgüten auf OSI-Schicht 3 und 4 angefordert und bereitgestellt werden können.

Maßgeblichen Anteil an diesen Entwicklungen hat dabei die *Internet Engineering Task Force* (IETF), eine Interessengemeinschaft von Personen und Institutionen, die sich mit der Weiterentwicklung des Internets befassen. Die IETF teilt ihre Aufgaben in Arbeitsgruppen auf, die wohl wichtigsten Arbeitsgruppen, die sich mit der Dienstgüte auf OSI-Schicht 3 und 4 beschäftigen, sind:

- **Differentiated Services (DiffServ)**
- **Integrated Services (IntServ)**
- **Resource ReSerVation Protocol (RSVP)**

Die Methode, *Traffic Control* genannt, mit der verschiedene Dienstgüten in einem Packet Switching Network erzeugt werden, kann auf folgende Funktionsweise aus Abbildung 5 zurückgeführt werden.

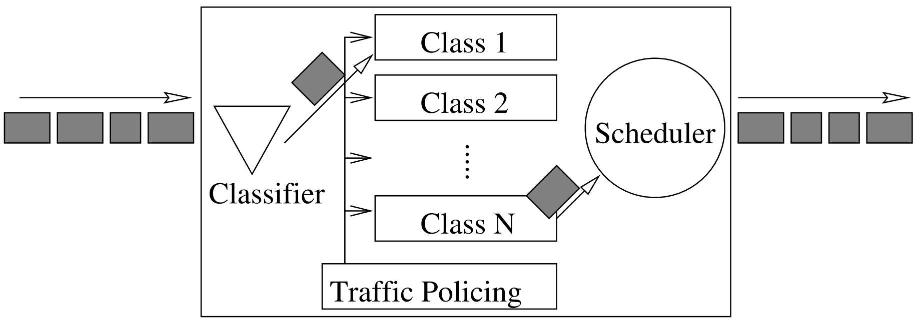

Abbildung 5: Traffic Control

Die wesentlichen Elemente des Traffic Control sind der *Classifier*, die *Classes*, der *Scheduler* und das *Traffic Policing*.

Der Classifier hat die Aufgabe, die eingehenden PDUs in Klassen einzuteilen. In eine Klasse kommen die PDUs, die eine bestimmte Dienstgüte erhalten sollen. Nach den Kriterien, die für die Einteilung dienen, lassen sich zwei Typen von Classifiern unterscheiden:

- **Behavior Aggregate (BA) Classifier**
  Die IP-Pakete werden nach dem DSCP im Header klassifiziert (siehe Abschnitt 2.2).
- **Multi-Field (MF) Classifier**
  Dieser Classifier verwendet mehrere Header-Felder, wie zum Beispiel Quell-, Zieladresse, Protokoll ID, Quell- und Zielport, um Nachrichten zu klassifizieren (siehe Abschnitt 2.3.2).

In den Klassen werden Queues für das Zwischenspeichern von PDUs benutzt. Der Scheduler wählt die PDUs für den Weitertransport aus den Queues nach einer bestimmten Strategie aus. Die Auswahlstrategie beeinflußt zum Beispiel die Transportverzögerung der PDUs, da sie die Wartezeit dieser in den Queues mitbestimmt. Ein weiteres Beispiel für einen Dienstgüteparameter auf den der Scheduler Einfluß nimmt, ist die Bandbreite für den Verkehr einer Klasse. Die Queues und der Scheduler sind hauptsächlich für das Auflösen von kurzfristigen Staus (Congestion) zuständig. Kurzfristige Staus entstehen, wenn über einen relativ kurzen Zeitraum mehr PDUs weitergeleitet werden müssen als möglich ist.

Langfristige Staus können für die einzelnen Klassen mit dem Traffic Policing vermieden oder beschränkt werden. Langfristige Staus treten auf, wenn über einen längeren Zeitraum oder sogar ständig mehr PDUs an einem Knoten im Netz ankommen als weitergeleitet werden können. Die Folge ist, daß die Queues für das Zwischenspeichern der PDUs überlaufen oder nicht mehr geleert werden können. Eine Methode langfristige Staus zu beseitigen ist es PDUs zu verwerfen (Dropping), dies beeinflußt den Dienstgüteparameter Verlust (Loss). Das Traffic Policing kann dafür sorgen, daß die Datenmenge, die ins Netz gelangt, und somit an den Knoten eintrifft, kontrolliert wird. Die Kontrolle der Datenmenge kann zur Staukontrolle dienen.

Ein erster Ansatz, PDUs unterschiedliche Behandlung zukommen zu lassen, ist *IP Precedence.*

2.1 IP Precedence

IP Precedence kann man als den Vorläufer der im nächsten Abschnitt vorgestellten Entwicklung ansehen. IP Precedence nutzt den Inhalt der ersten sechs Bits des *Type of Service* Feldes (ToS-Feld) im Internet Protocol Version 4 (IPv4) Header als Klassifizierungskriterium (siehe Abbildung 6).

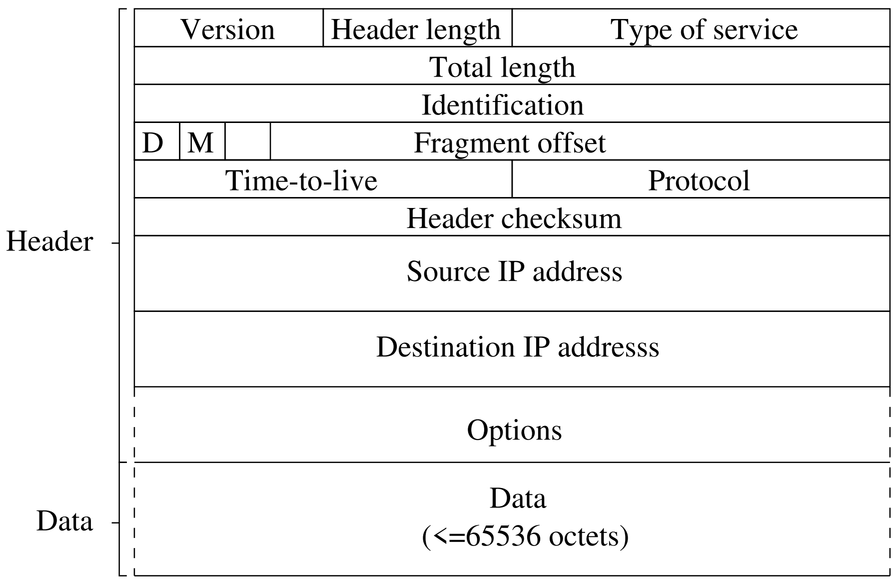

Abbildung 6: Internet Protocol Version 4 Header [Hals 96]

Die ersten drei Bits (Precedence) geben die Priorität eines Pakets an. In den nächsten drei Bits wird dem Netz mitgeteilt, welche der drei Dienstgüteparameter: Übertragungsverzögerung (Delay), Durchsatz (Throughput) und Zuverlässigkeit (Reliability) beim Transport des Pakets zu beachten sind (siehe Abbildung 7).

[Post 81] definiert sieben Prioritäten für das Precedence-Feld. Diese Prioritäten sollen für den Verkehr der Klassen aus Tabelle verwendet werden (siehe Tabelle 1).

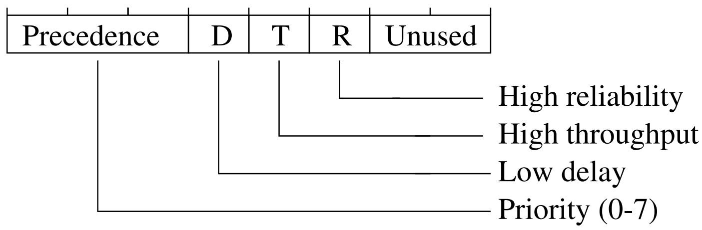

Abbildung 7: ToS-Feld [Hals 96][Post 81]

Wert	Verkehr
111	Network Control
110	Internetwork Control
101	CRITIC/ECP
100	Flash Override
011	Flash
010	Immediate
001	Priority
000	Routine

Tabelle 1: Precedence-Klassen [Post 81]

Der Inhalt des ToS-Felds kann dann in den Routern oder Datenendeinrichtungen (DEE, engl. Data Terminal Equipment abgekürzt DTE) als Information für das Scheduling und das Dropping genutzt werden.

2.2 Differentiated Services

Differentiated Services (DiffServ) [NBBB 98] nutzt analog zu IP Precedence den Inhalt des ToS-Feldes des IPv4 Headers für die Klassifizierung der IP-Pakete. Mit der Einführung des Internet Protocol Version 6 (IPv6) soll das *Traffic Class* Feld verwendet werden. Diese beiden 8-Bit Felder werden bei DiffServ einheitlich *Differentiated Services* Feld (DS-Feld) bezeichnet. Durch Setzen des DS-Feldes im IP-Header kann eine Anwendung die Dienstgüte seiner IP-Pakete bestimmen (siehe Abbildung 8). DiffServ ist eine OSI-Schicht 3 Entwicklung.

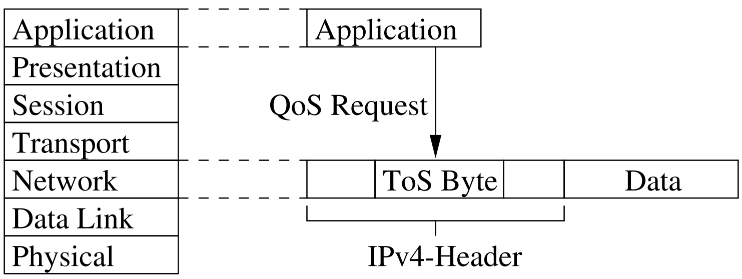

Abbildung 8: QoS-Anforderung mit DiffServ

In den ersten sechs Bits des DS-Feldes, *Differentiated Services CodePoint* (DSCP), wird die Zugehörigkeit zu den vordefinierten Klassen kodiert, die restlichen zwei Bits, *Currently*

Unused (CU), bleiben ungenutzt (siehe Abbildung 9).

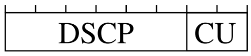

Abbildung 9: Differentiated Services Feld

Die IETF reserviert sich 32 der 64 möglichen DSCP-Werte für die Standardisierung von Klassen. Die restlichen Werte stehen zur freien Verfügung.

Ein Standard beinhaltet den oder die DSCP-Werte und ein *Per-Hop Behavior* (PHB). Das Per-Hop Behavior beschreibt das Forwarding-Verhalten des Schedulers. Es wird also keine Implementierung vorgeschrieben, sondern nur die Anforderungen an diese. Das PHB bezieht sich auf eine Klasse (ein DSCP-Wert) oder auf mehrere Klassen (mehrere DSCP-Werte). Im zweiten Fall spricht man von einer PHB-Group.

Zwei Standards wurden bis jetzt verabschiedet:

- **Expedited Forwarding PHB** [JNP 99] und
- **Assured Forwarding PHB-Group** [HBWW 99].

Der *Traffic Conditioner* [BBC+ 98] übernimmt bei DiffServ das Traffic Policing, um zusammen mit dem PHB eine Dienstgüte für eine (Gruppen-)Klasse zu implementieren. Auf den Traffic Conditioner wird im nächsten Abschnitt noch näher eingegangen.

Einen Bereich in dem DiffServ-fähige Geräte (DS nodes) einheitliche Dienste zur Verfügung stellen, nennt man *Differentiated Services Domain* (siehe Abbildung 10).

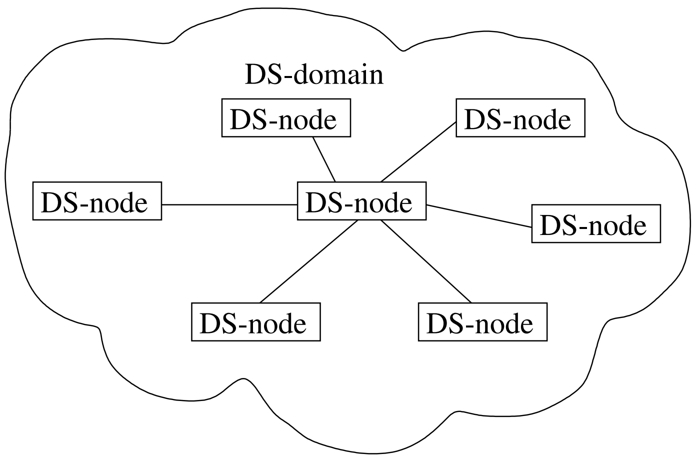

Abbildung 10: Differentiated Services Domain

2.2.1 DS-Dienstgüten

Mit den beiden bis jetzt standardisierten PHBs hat man zwei Dienstgüten beabsichtigt.

Premium Service Der *Premium Service* [JNP 99] macht sich den Expedited Forwarding PHB zu nutze, um einen Dienst zu erzeugen, der eine Leitung simulieren soll. Aus dieser Absicht heraus ergeben sich folgende Anforderungen an den Dienst:

- kein Verlust aufgrund von Staus (Congestion Loss)
- geringe Übertragungsverzögerung
- wenig Jitter[2]
- zugesicherte Bandbreite

Wie diese Dienstgüte implementiert werden kann, soll anhand eines Beispieles (siehe Abbildung 11) erklärt werden.

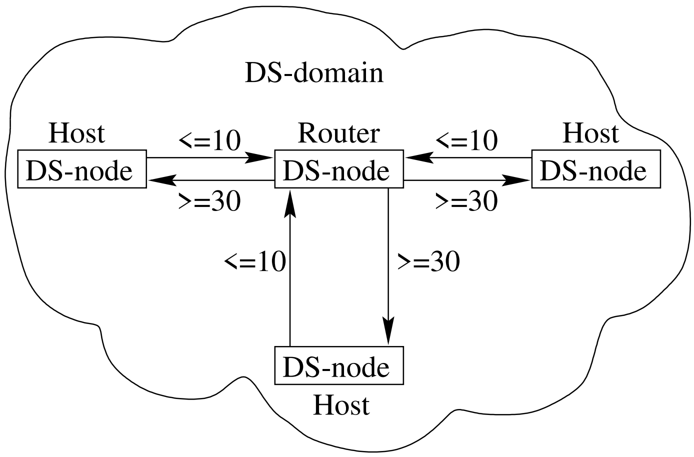

Abbildung 11: Premium Service

Drei DS-Geräte (Hosts) wollen den Premium Service nutzen. Ein DS-Gerät (Router) verbindet die drei Hosts. Für den Verkehr der mit dem EF-PHB weitergeleitet werden soll, ist eine minimale Bandbreite zu reservieren. Für die Hosts sollen dies 10 und den Router 30 Einheiten sein. Der Premium Service verlangt, daß der Eingangsverkehr an allen DS-Geräten, der weitergeleitet werden soll, kleiner ist, als die für den Ausgangsverkehr vorhandene Bandbreite. Wäre dies nicht der Fall, würde es zu längeren Verzögerungen oder gar Verlusten kommen, was den Ansprüchen dieses Dienstes widerspricht. Für die Einhaltung dieser Bedingung sorgen die Traffic Conditioners in den Endgeräten, die bei Überschreiten der erlaubten Bandbreite Pakete verwerfen, puffern oder einer anderen Dienstgüte zuordnen können. Eben diese Aufgaben erfüllen die folgenden Bestandteile eines Traffic Conditioners:

- **Meter**
  Dieser Bestandteil mißt den Verkehr der Klasse, überschreitet er z.B. eine maximale Bandbreite, so kann er dies dem Marker, Dropper oder Shaper mitteilen (siehe Abbildung 12).
- **Marker**
  Der Marker kann dem DSCP-Feld einen neuen Wert zuweisen, und damit ein IP-Paket einer anderen Klasse zuordnen.
- **Dropper**
  Der Dropper kann einzelne IP-Pakete verwerfen.

[2] Schwankungen der Übertragungsverzögerungen

- **Shaper**
  Der Shaper kann IP-Pakete verzögern, und damit das Verkehrsprofil verändern.

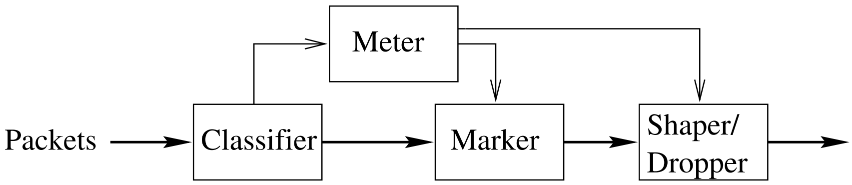

Abbildung 12: Classifier und Traffic Conditioner

Für das Beispiel verlangt die Einhaltung der obigen Bedingung, daß die Hosts nicht mehr als 10 Einheiten senden dürfen.

Assured Service Der *Assured Service* [HBWW 99] basiert auf der Assured Forwarding PHB-Group. Dieser Dienst verlangt einen geringen Verlust (Congestion Loss) unter der Voraussetzung, daß eine vorkonfigurierte Bitrate nicht überschritten wird.

Die Assured Forwarding PHB-Group vereint drei Klassen zu einer sogenannten Assured Forwarding-Klasse (AF-Klasse), der eine minimale Bandbreite zugesichert wird. Mit den drei Unterklassen kann man nun Prioritäten für das Dropping der Pakete in der AF-Klasse vergeben (siehe Abbildung 13).

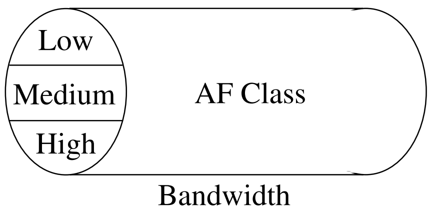

Abbildung 13: Assured Forwarding Class

2.3 Integrated Services und Resource Reservation Protocol

Die Arbeitsgruppen Integrated Services und Resource Reservation Protocol arbeiten an einer weiteren Lösungsmöglichkeit für Dienstgüten im IP-Netz. Die Arbeit an dieser Lösungsmöglichkeit ist in zwei Hauptgebiete unterteilt:

- **Integrated Services (IntServ)**
  IntServ arbeitet an einem verbesserten Internet Service Modell, d.h. die Arbeitsgruppe definiert Dienstgüten für IP-Netze. Desweiteren werden die Anforderungen und Schnittstellen für eine Implementierung dieser Dienstgüten standardisiert.

- **Resource Reservation Protocol (RSVP)**
  Die Arbeitsgruppe RSVP arbeitet an dem gleichnamigen Protokoll, ein Protokoll für die Reservierung von Kommunikationsressourcen der an der Übertragung beteiligten Elemente.

2.3.1 Integrated Services

IntServ und DiffServ verfolgen unterschiedliche Ziele. DiffServ definiert eine Architektur mit der unterschiedliche Dienstgüten bereitgestellt werden können, spezifiziert aber nicht spezielle Dienstgüten oder Dienstklassen. IntServ definiert die Dienstklassen und läßt ihre Bereitstellung offen.

Integrated Services hat bis jetzt zwei Dienstklassen für Kommunikationsdienste auf OSI-Schicht 4 standardisiert:

- **Controlled-Load Service (CLS)** [Wroc 97b]
  Der Controlled-Load Service soll in etwa die Dienstgüte bereitstellen, den ein IP-Netz unter geringer Auslastung erbringt, ohne dabei von der tatsächlichen Auslastung abhängig zu sein. Dies bedeutet, daß folgende zwei Bedingungen erfüllt sind:
  1. Der Verlust aufgrund von Stauungen im Netz muß gering sein.
  2. Ein hoher Prozentsatz der IP-Pakete darf die minimale Übertragungsverzögerung nicht wesentlich überschreiten.
- **Guaranteed Service (GS)** [SPG 97]
  Der Guaranteed Service kann durch folgende zwei Bedingungen beschrieben werden:
  1. Dem Verkehr wird eine Bandbreite versprochen, wenn sich die Anwendung an diese Bandbreite hält, gibt es keinen Verlust durch Stauungen.
  2. Dem Verkehr innerhalb der Bandbreite wird eine maximale Transportverzögerung zugesagt.

2.3.2 Resource Reservation Protocol

Das RSVP-Protokoll [BZB+ 97] ist ein Signalisierungsprotokoll der OSI-Schicht 4 mit dem Anwendungen Ressourcen eines Netzes anfordern können. Das Netz gewährt diese Anforderungen oder lehnt sie ab. Durch Angabe der gewünschten IntServ-Dienstgüte kann eine Anwendung die für diese Dienstgüte benötigten Ressourcen spezifizieren. Für den Datentransport werden gängige Schicht 4 Protokolle, wie zum Beispiel TCP und UDP, eingesetzt (siehe Abbildung 14).

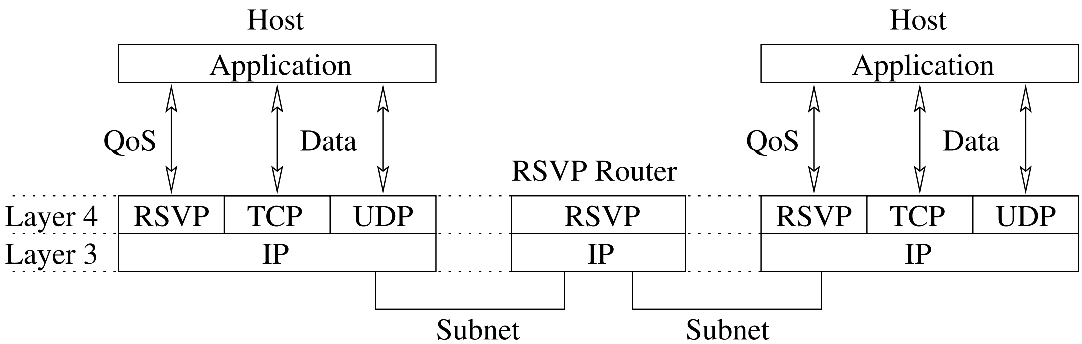

Abbildung 14: Dienstgüte-Signalisierung mit RSVP

RSVP trennt klar zwischen den Aufgaben, Bereitstellung von Ressourcen und Anforderung von Ressourcen. Für die Anforderung ist RSVP zuständig für die Bereitstellung das Traffic Control.

Mit RSVP-PDUs werden die Anforderungen zu den RSVP-Protokoll-Instanzen (RSVP-Prozesse), die für die einzelnen Subnetze verantwortlich sind, transportiert. Dort versucht der RSVP-Prozeß die Ressourcen im Subnetz anzufordern. Eine Anforderung kann aus zwei Gründen abgelehnt werden. Der erste Grund ist, daß eine Person nicht berechtigt ist die Dienstgüte anzufordern. Dies stellt RSVP durch Anfrage beim *Policy Control* fest (siehe Abbildung 15). Der zweite Grund ist, daß nicht genügend Ressourcen vorhanden

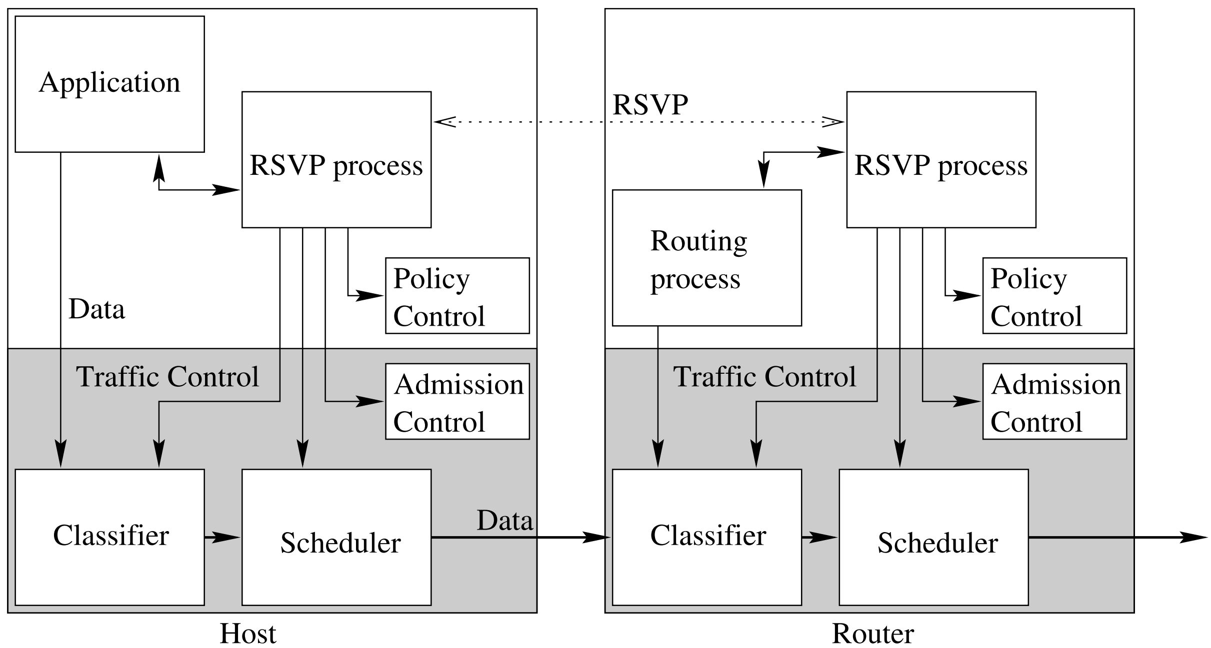

Abbildung 15: RSVP im Host und Router

sind. Dies erfährt RSVP vom Traffic Control, daß die Anforderung der Ressourcen ablehnt. Das Traffic Control besteht aus den Teilen: *Classifier*, *Scheduler* und *Admission Control*. Das Admission Control hat die Ressourcen zu verwalten. Es überprüft, ob einem Fluß eine Dienstgüte gewährt werden kann, ohne die Dienstgüten bestehender Flüsse zu gefährden. Kann die Dienstgüte gewährt werden, sorgen der Classifier und der Scheduler für die richtige Behandlung der PDUs eines Flusses.

Um die Anforderungen zu den RSVP-Prozessen zu bringen, sind zwei Phasen nötig:

- Es wird ein Pfad zwischen einem Sender und den Empfängern im Netz festgelegt.
- Auf diesem Pfad werden die Anforderungen gestellt.

RSVP besitzt die PDUs *Path* und *Resv* für diese zwei Phasen. Mit Path-PDUs wird der Pfad für einen Fluß im Netz festgelegt. Sie werden von einem RSVP-Prozeß des Senders erzeugt und dann von einem RSVP-Prozeß über den nächsten zum Empfänger gesendet. Ein Empfänger legt die Reservierung fest und sendet eine Resv-Nachricht auf dem Pfad zurück zum Sender (siehe Abbildung 16).

Eine Path-PDU hat folgenden Aufbau:

```
<Path Message> ::= <Common Header> [ <INTEGRITY> ]
                   <SESSION> <RSVP_HOP>
                   <TIME_VALUES>
```

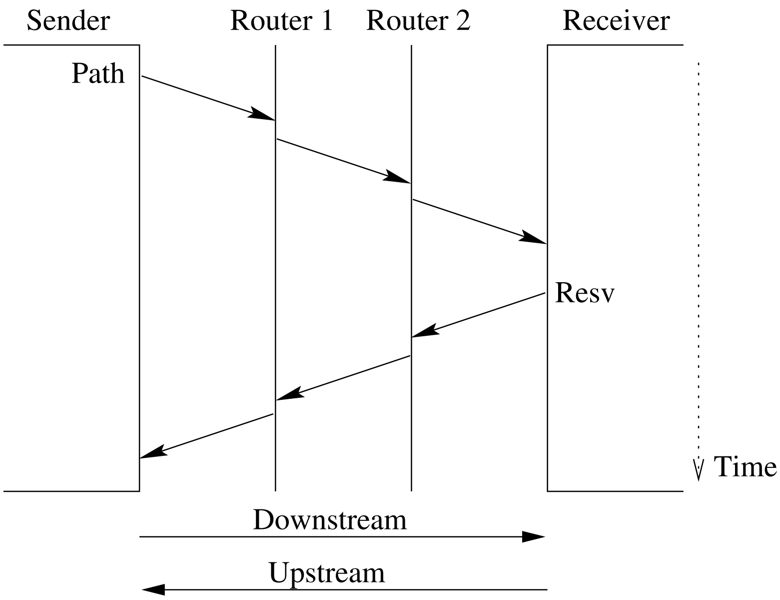

Abbildung 16: Reservierung

```
                    [ <POLICY_DATA> ... ]
                    [ <sender descriptor> ]
<sender descriptor> ::= <SENDER_TEMPLATE> <SENDER_TSPEC>
                         [ <ADSPEC> ]
```

Im Header einer RSVP-Nachricht ist das Feld *Time To Live* (TTL). Dieses Feld ermöglicht es nicht RSVP-fähige Geräte auf dem Pfad zu erkennen. Jeder Router verringert das Feld TTL im IP-Header, aber nur ein RSVP-Router verringert das TTL-Feld im RSVP-Header. Unterscheiden sich beide, dann wurde eine RSVP-PDU von einem nicht RSVP-fähigen Router weitergeleitet.

Das Objekte `POLICY_DATA` überträgt die Daten die ein RSVP-Prozeß dem Policy Control übergibt. Mit dem Objekt `INTEGRITY` wird die Authentizität eine RSVP-Nachricht sichergestellt. Die Bedeutung von `TIME_VALUES` wird später erklärt.

Es soll nun genauer beleuchtet werden, welche Aufgaben die Path-PDU erfüllt.

1. **Sie identifiziert den Datenfluß.**
   Um die Flüsse einzeln behandeln zu können, müssen die Daten und die RSVP-PDUs den Flüssen zugeordnet werden können. Durch einen Identifikator wird die Zugehörigkeit der Path-PDUs zu einem Fluß festgelegt. Der Identifikator eines Flusses besteht aus den Objekten `SESSION` und `SENDER_TEMPLATE`. In `SESSION` wird die IP-Adresse des Empfängers, das verwendete Transportprotokoll und weitere Demultiplex-Information, z.B. Portnummer bei TCP und UDP, angegeben. `SENDER_TEMPLATE` enthält die IP-Adresse des Senders und die Demultiplex-Information des Transportprotokolls.

2. **Sie legt den Weg für den Datenfluß im Netz fest.**
   Es muß ein Pfad für den Datenfluß festgelegt werden, damit die PDUs eines Flusses alle den Weg entlang des Pfad folgen. Denn nur hier erfolgen die Reservierungen und die PDUs erhalten ihre Dienstgüte. Zur Aufzeichnung des Pfads dient das Objekt

`RSVP_HOP`. Hier wird die IP-Adresse des letzten Geräts mit einem RSVP-Prozeß, das von der Path-Nachricht durchlaufen wurde, festgehalten. Diese IP-Adresse speichert ein RSVP-Prozeß und ersetzt es durch die eigene. Mit diesem Verfahren wird der Weg der Nachricht festgehalten.

3. **Sie beschreibt den Datenfluß, der vom Sender erzeugt wird.**
Zur Erzeugung der Information über die Dienstgüte des Flusses, benötigt der Empfänger eine Beschreibung des Datenflusses, den der Sender erzeugt. Der Verkehr, der vom Sender erzeugt wird, wird mit `SENDER_TSPEC` beschrieben. Ein Bestandteil den alle `SENDER_TSPEC`, enthalten ist der `TOKEN_BUCKET_TSPEC` [ShWr 97] mit folgender Information:

    - **Peak Data Rate**
    Die Peak Data Rate ist die maximale Bitrate mit der die Anwendung Daten aufs Netz schicken darf.
    - **Token Bucket Rate (TBR)**
    Die Token Bucket Rate und die Token Bucket Size sind Bezeichnungen, die dem *Leaky-Bucket Algorithmus* entspringen (siehe Abbildung 17). Bestandteile des

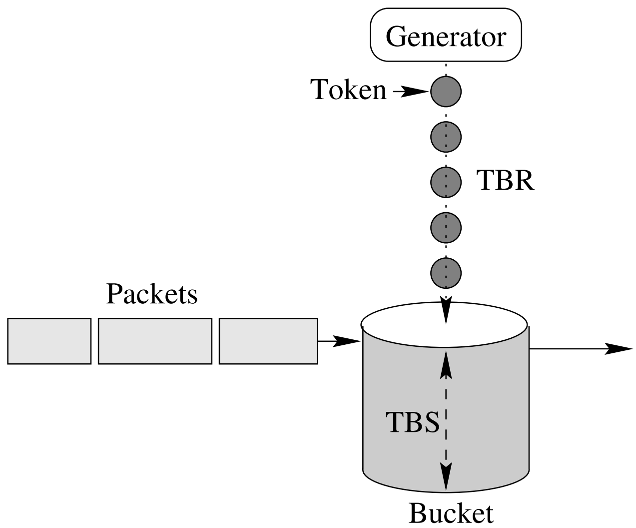

Abbildung 17: Leaky Bucket Algorithmus

Leaky Bucket Algorithmus sind ein Bucket und ein Generator. Der Generator erzeugt Token mit der Rate TBR. Diese Token werden in einem Eimer (Bucket) aufgefangen. Die Größe des Eimer ist die Token Bucket Size (TBS). Für jede Einheit (z.B. Octet), die gesendet werden will, muß ein Token aus dem Eimer entnommen werden. Sind keine Token mehr vorhanden, muß die Einheit weggeworfen werden. Werden weniger Token aus dem Eimer genommen, wie reinfallen, so läuft der Eimer über und Token gehen verloren. Die Token Bucket Rate und die Token Bucket Size begrenzen somit die maximale Datenmenge, die in einem Zeitraum der Länge $T = \frac{TBS}{TBR}$ erzeugt werden darf.

Außerdem kann mit dem Leaky Bucket Algorithmus die *Burstiness* des Verkehrs beschrieben werden. Ist ein Verkehrsprofil durch relativ niedrige Bitraten über einen langen Zeitraum geprägt, daß durch relativ kurzfristige Übertragung mit hohen Bitraten unterbrochen ist, so werden diese kurzen Phasen als *Bursts* bezeichnet (siehe Abbildung 18). Bei gleicher durchnittlicher Bitrate braucht ein Verkehr mit Bursts eine größere TBS als einer ohne.

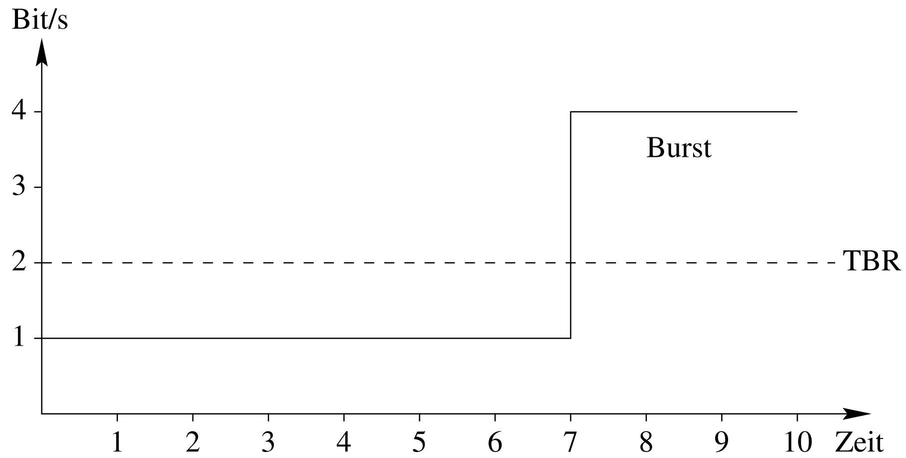

Abbildung 18: Token Bucket Rate

- **Token Bucket Size (TBS)**
- **Minimum Policed Unit**
  Die Minimum Policed Unit ist die minimale Paketgröße, die eine Anwendung verwendet. Sie enthält die Header aller Protokolle überhalb von IP.
- **Maximum Packet Size**
  Die Maximum Packet Size ist die maximale Paketgröße.

4. **Sie liefert die Information über die gewünschte Dienstgüte und das Netz.** Im Objekt `ADSPEC` kann der Sender Vorschläge für die gewünschte Dienstgüte machen [Wroc 97a]. Dieses Objekt enthält auch die Information, die auf dem Weg durch das Netz für die gewünschten Dienstgüte gesammelt wurde (z.B. ob die gewünschten Dienstgüten verfügbar sind).

Die Resv-PDU hat folgenden Aufbau:

```
<Resv Message> ::= <Common Header> [ <INTEGRITY> ]
                   <SESSION> <RSVP_HOP>
                   <TIME_VALUES>
                   [ <RESV_CONFIRM> ] [ <SCOPE> ]
                   [ <POLICY_DATA> ]
                   <STYLE> <flow descriptor list>
<flow descriptor list> ::= <empty> |
                           <flow descriptor list> | <flow descriptor>
```

Die Resv-Nachricht enthält die Objekte `SCOPE` und `RESV_CONFIRM`. Das Objekt `SCOPE` wird verwendet, um einen Effekt, der durch den Wildcard-Filter entstehen kann, vorzubeugen (siehe [BZB+ 97]). Mit `RESV_CONFIRM` kann der Empfänger die Bestätigung einer Reservierung veranlassen. Die Bedeutung der anderen Objekte wird anhand der beiden Aufgaben der Resv-Nachricht erklärt.

Die Aufgaben der Resv-PDU sind:

1. **Legt den Identifikator fest.**
Der Identifikator ist abhängig von der verwendeten Reservierungsart. RSVP kennt drei Reservierungsarten (siehe Tabelle 2). Ein RSVP-Fuß wird durch `SESSION` und

Sender Selection	Reservation	
	Distinct	Shared
Explicit	Fixed-Filter (FF) Style	Shared-Explicit (SE) Style
Wildcard	(None defined)	Wildcard-Filter (WF) Style

Tabelle 2: RSVP Reservierungsarten

`FILTER_SPEC` identifiziert und durch `FLOWSPEC` charakterisiert. `FILTER_SPEC` trägt den selben Inhalt (identifiziert Sender), wie `SENDER_TEMPLATE` in der Path-Nachricht. Der *Fixed-Filter* (FF) nutzt `SESSION` und `FILTER_SPEC`, um einen Fluß zu identifizieren.

```
<flow descriptor list> ::= <FLOWSPEC> <FILTER_SPEC> |
                           <flow descriptor list> <FF flow descriptor>
<FF flow descriptor> ::= [ <FLOWSPEC> ] <FILTER_SPEC>
```

Mit einer Resv-Nachricht kann ein Empfänger mehrere RSVP-Flüsse reservieren lassen. Ein RSVP-Fluß nach dem FF kann einen Sender und einen Empfänger (siehe Abbildung 19) haben, wird in `SESSION` eine Multicast-Adresse verwendet, aber auch mehrere Empfänger (siehe Abbildung 20). Auf jeden Falls gibt es nur einen Sender. Der *Wilcard-Filter* (WF) läßt `FILTER_SPEC` und damit den Sender offen. Ein

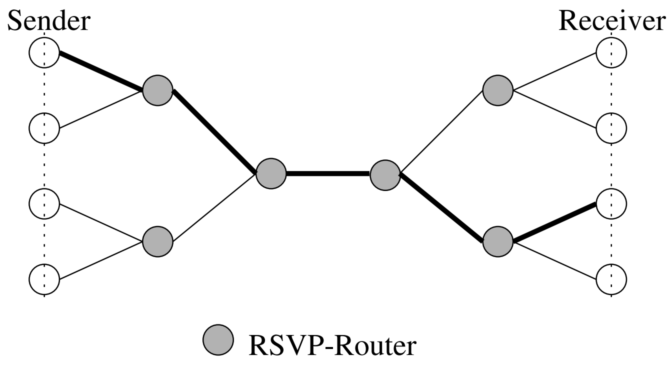

Abbildung 19: Unicast

RSVP-Fluß kann also von mehreren Sendern genutzt werden, damit lassen sich die Ressourcen besser ausnutzen.

```
<flow descriptor list> ::= <WF flow descriptor>
<WF flow descriptor> ::= <FLOWSPEC>
```

Ein RSVP-Fluß kann somit Many-to-One (siehe Abbildung 21) oder Many-to-Many (siehe Abbildung 22) sein. Der Filter *Shared-Explicit* (SE) erlaubt es ebenfalls, wie

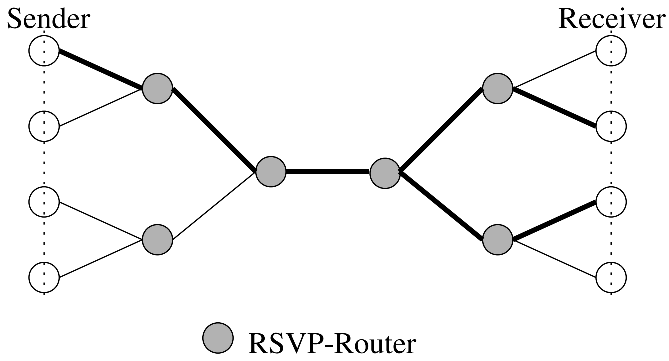

Abbildung 20: Multicast

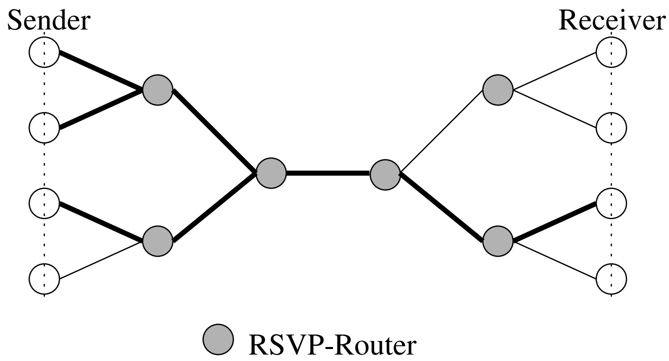

Abbildung 21: Many-to-One

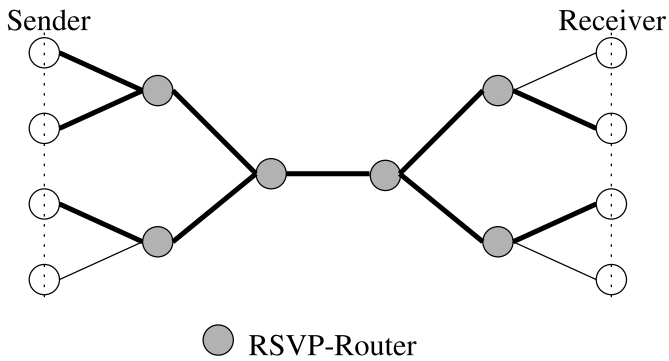

Abbildung 22: Many-to-Many

der Wildcard-Filter, daß sich mehrere Sender einen RSVP-Fluß teilen. Der Unterschied zum WF-Filter ist, daß die Sender explizit benannt werden müssen. Dies erfolgt durch eine Liste von `FILTER_SPEC`.

```
<flow descriptor list> ::= <SE flow descriptor>
<SE flow descriptor> ::= <FLOWSPEC> <filter spec list>
<filter spec list> ::= <FILTER_SPEC>
                     | <filter spec list> <FILTER_SPEC>
```

Ein Beispiel für eine sinnvolle Anwendung für eine Shared-Reservierung wäre eine Audio-Konferenz, denn es gibt hier immer nur einen Sprecher und damit einen Sender gleichzeitig.

2. **Legt die Reservierung fest.**
   Die zu reservierende Dienstgüte und die dafür benötigten Parameter werden in `FLOWSPEC` übergeben. Der Aufbau des `FLOWSPEC` ist durch den IntServ-Dienst [Wroc 97a] gegeben. Für Controlled-Load ist er wie der `TOKEN_BUCKET_TSPEC` aufgebaut. Garanteed Service besitzt neben `TOKEN_BUCKET_TSPEC` noch weitere Parameter [SPG 97], auf einige wird später noch eingegangen.
   Ein RSVP-Fluß kann mehrere Empfänger haben, daher können in einem RSVP-Prozeß mehrere Resv-Nachrichten für den selben Fluß, aber mit unterschiedlichem `FLOWSPEC`, eingehen (siehe graue Knoten in Abbildung 23). Trifft bei einem RSVP-

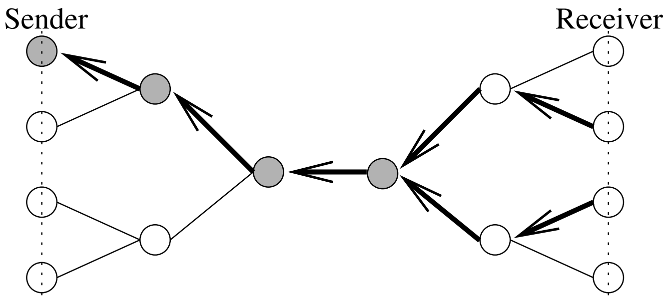

Abbildung 23: Verschmelzen von Datenflüssen

   Prozeß eine Resv-Nachricht für einen bereits bestehenden Fluß ein, dann erzeugt er einen neuen `FLOWSPEC`, ändert die Reservierung entsprechend, und sendet ihn mit einer Resv-Nachricht Richtung Sender oder er verwirft die Resv-Nachricht. Ersteres tritt ein, wenn ein Empfänger dieses Flusses mit der bereits bestehenden Reservierung nicht befriedigt werden kann. Es wird dann ein `FLOWSPEC` generiert, der die Bedürfnisse aller Empfänger erfüllt. Falls der eingehende `FLOWSPEC` geringere Anforderungen an den Fluß stellt, wird die Resv-Nachricht verworfen, um den Overhead des RSVP-Protokolls so klein wie möglich zu halten.

RSVP verwendet sogenannte *Soft States*, d.h. die Zustände [BrZh 97], die durch Path- und Resv-Nachrichten in den RSVP-Prozessen erzeugt werden, werden nach Ablauf eines Intervalls gelöscht. Das Löschen eines Zustand führt zur Freigabe der Ressourcen. Jeder RSVP-Prozeß sendet periodisch Path- und Resv-Nachrichten für die vorhandenen Zustände. Die Dauer einer Periode wird mit dem Wert des Objekt `TIME_VALUES` festgelegt. Erhält ein RSVP-Prozeß ein Path- oder Resv-PDU, dann wird das Timeout-Intervall des entsprechenden Zustands hochgesetzt. Das Timeout-Intervall ist so gewählt, das es eine Anzahl an RSVP-Path- und RSVP-Resv-Verlusten verkraftet. Die RSVP-PDUs werden mit der Best Effort (BE) Dienstgüte transportiert. Die Best Effort-Dienstgüte gibt keine Garantien für Dienstgüteparameter.

Neben der Path- und Resv-PDU kennt RSVP noch fünf weitere PDUs auf die hier noch kurz eingegangen werden soll:

- **PathErr**
  Die PathErr (Path Error) Nachricht berichtet Fehler in der Bearbeitung von Path-Nachrichten.

- **ResvErr**

Die ResvErr (Reservation Error) Nachricht berichtet Fehler bei der Bearbeitung von Resv-Nachrichten.

- **PathTear**
  Die PathTear (Path Teardown) Nachricht löscht den Zustand, der durch Path- und Resv-Nachrichten in den RSVP-Prozessen erzeugt wurde.

- **ResvTear**
  Die ResvTear (Reservation Teardown) löscht den Zustand, der durch die Resv-Nachrichten entstand.

- **ResvConf**
  ResvConf (Reservation Confirmation) Nachrichten können gesendet werden, um eine Reservierung zu bestätigen. Der Erhalt einer ResvConf-Nachricht muß keine Bestätigung einer End-zu-End-Reservierung bedeuten.

In diesem Kapitel wurden einige Dienstgüten auf OSI-Schicht 3 (z.B. Premium Service) und 4 (z.B. Guaranteed Service) erwähnt. Für die Erzeugung dieser Dienstgüten werden die Kommunikationsdienste von Netztechnologien verwendet. Im nächsten Kapitel werden einige Netztechnologien auf ihre Dienste und Dienstgüten untersucht.

3 Netztechnologien

Die Dienstgüte auf OSI-Schicht 3 und 4 setzt sich aus den Mechanismen in diesen Schichten und den Kommunikationsdiensten mit ihren Dienstgüten auf OSI-Schicht 2 zusammen. Im vorigen Abschnitt haben wir Mechanismen auf Schicht 3 und 4 kennengelernt, nun wollen wir gängige Netztechnologien (OSI-Schicht 2 abwärts) auf ihre Dienste und Dienstgüten untersuchen. Geeignete Dienste können dann von der OSI-Schicht 3 und 4 angefordert werden, um eine gewünschte Dienstgüte auf Schicht 3 und 4 zu erreichen (siehe Abbildung 24).

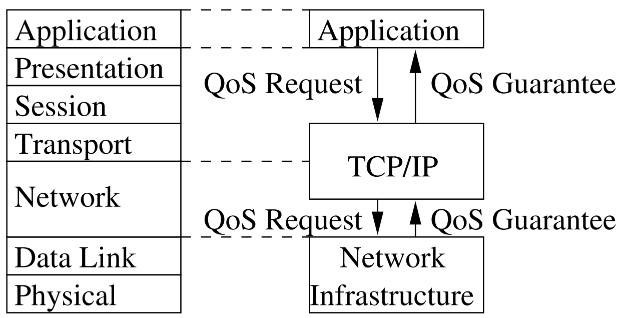

Abbildung 24: QoS-Anforderung an die Netzwerktechnologie

3.1 Sonet/SDH

Synchronous Digital Hierarchy (SDH) wurde von Bellcore in den USA unter dem Titel *Synchronous Optical Network* (Sonet) entwickelt [Hals 96]. Wie der Name schon sagt, handelt es sich um eine synchrone (alle Geräte sind mit einem einzigen Zeitgeber synchronisiert) Netztechnologie auf OSI-Schicht 1. SDH kommt in vielen Netzen auf Schicht 1 zum Einsatz, zum Besipiel ISDN oder ATM.

Als Übertragungsmedium werden Glasfaserkabel verwendet, die in der Grundvariante mit einer Übertragungsrate von 155,52 Mbit/s betrieben werden.

Die Übertragung von Daten erfolgt in Frames der Größe 2430 Octet, die alle 125 μs erzeugt werden. Ein Frame gliedert sich in 9 Segmente der Größe 270 Octet. Ein Segment besitzt einen 9 Octet Header und 261 Octet Payload (siehe Abbildung 25).

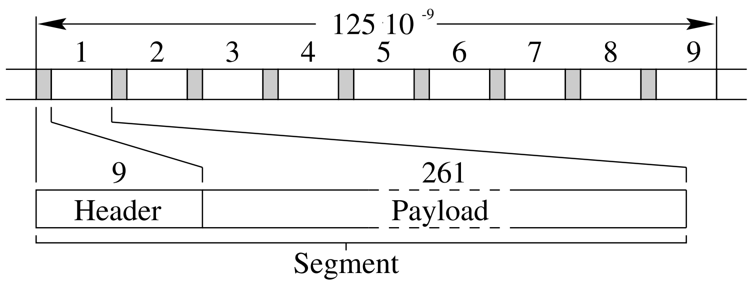

Abbildung 25: SDH-Segment

Damit ergibt sich der Frame-Aufbau aus Abbildung 26. SDH erlaubt die Realisierung

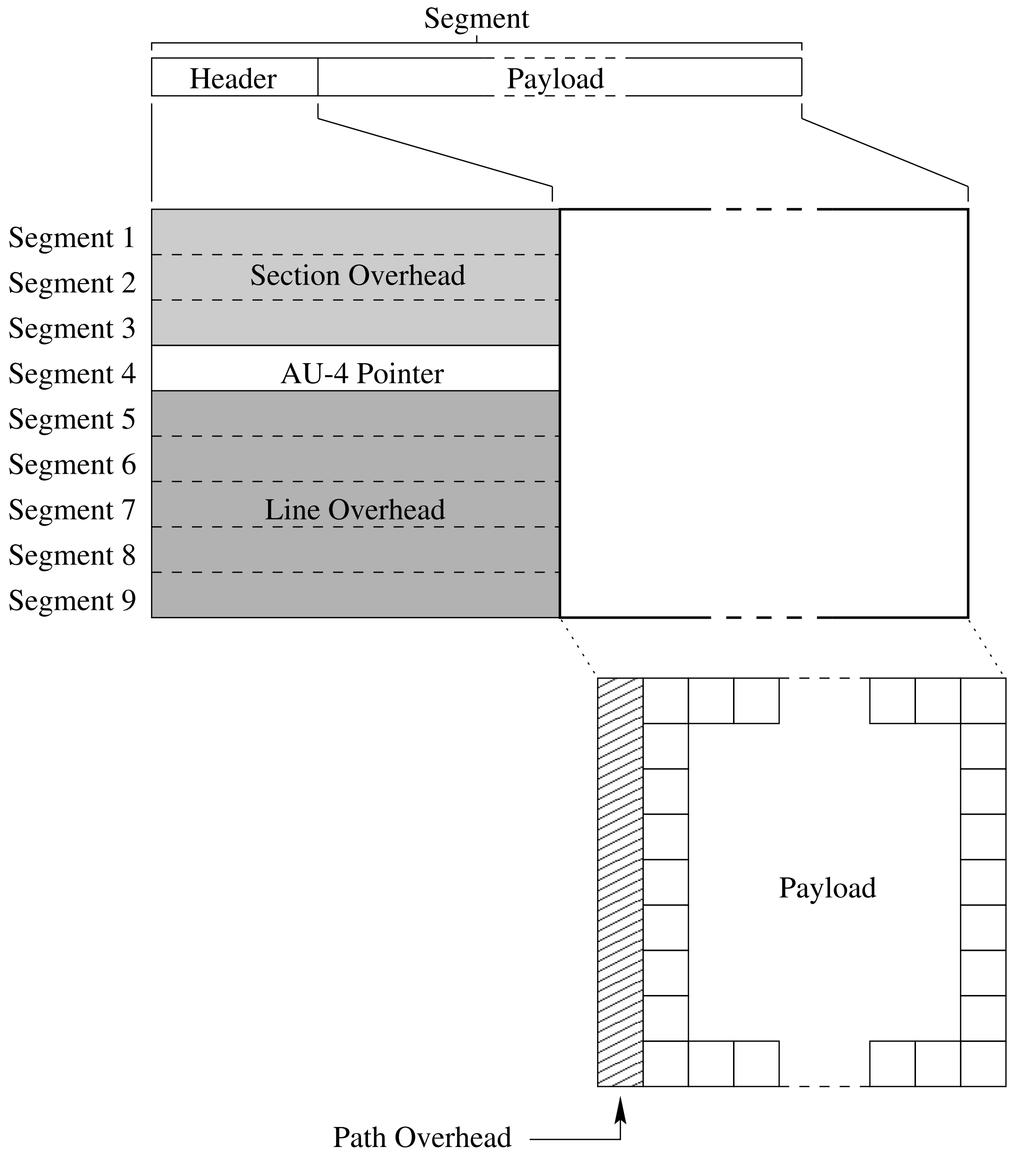

Abbildung 26: SDH-Frame

von Übertragungskanälen fester Bandbreite durch Multiplexen in den Payload-Block. OSI-Schicht 1 Switches werden verwendet, um die Übertragungskanäle von einem Endgerät zu einem anderen zu schalten (siehe Abbildung 27).

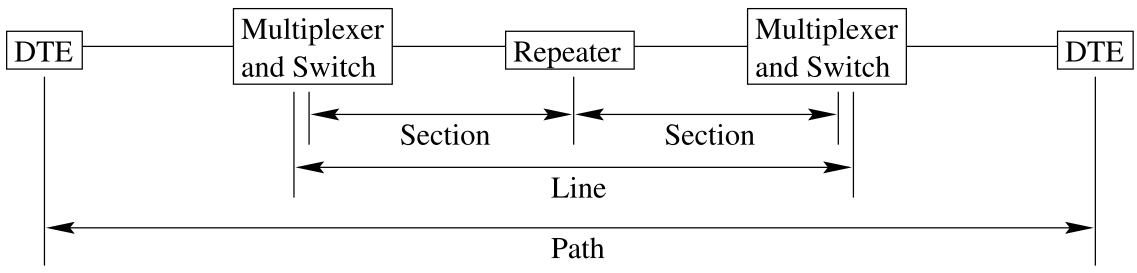

Abbildung 27: SDH-Netz

Die Overhead-Octets haben Bedeutung für verschiedene Abschnitte einer Übertragungsstrecke:

- **Section Overhead**
  Steuerung der Strecke zwischen 2 Repeater oder Multiplexer und Repeater.
- **AU-4 Pointer**
  Mit diesem Pointer kann der Block aus Path Overhead und Payload innerhalb der Rahmen (dicke Line in Abbildung 26) zweier aufeinander folgenden Frames verschoben werden. Dies wird verwendet um Frequenzschwankungen zu kompensieren.
- **Line Overhead**
  Steuerung zwischen zwei Multiplexer über Repeater hinweg.
- **Path Overhead**
  Steuerung zwischen zwei Endgeräten.

3.1.1 Dienstgüte von Sonet/SDH

Der Dienst von Sonet/SDH stellt sich einer übergeordneten Schicht als eine Octets übertragende Leitung mit fester Bandbreite dar.

3.2 Asynchronous Tranfer Mode (ATM)

ATM ist eine neuere Netztechnologie, die aus dem WAN-Bereich kommt, aber neuerdings auch im MAN- und LAN-Bereich eingesetzt wird [all 95][Hals 96][Marc 97] [ATM-UNI 94][ATM Europe 97]. Ziel von ATM ist es, eine Grundlage für ein öffentliches Hochgeschwindigkeitsnetz (Broadband Integrated Services Digital Network, B-ISDN) zu sein. Dies verlangt, daß sowohl Sprache, Video und Daten über dieses transportiert werden können.

Ein ATM-Netz besteht aus ATM-Switches. Ein Switch steht an Knotenpunkten des Netzes, an denen mehrere Übertragungskanäle zusammenlaufen (siehe Abbildung 28). Die

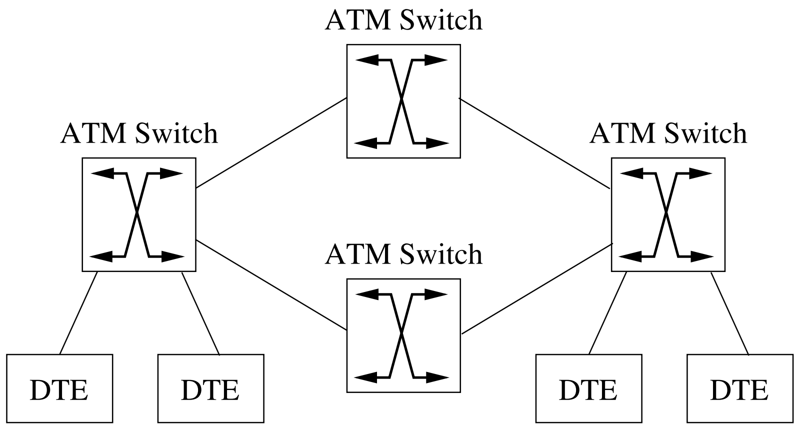

Abbildung 28: ATM-Netz

Aufgabe eines ATM-Switch ist, eingehende Pakete fester Größe (53 Octest), die bei ATM

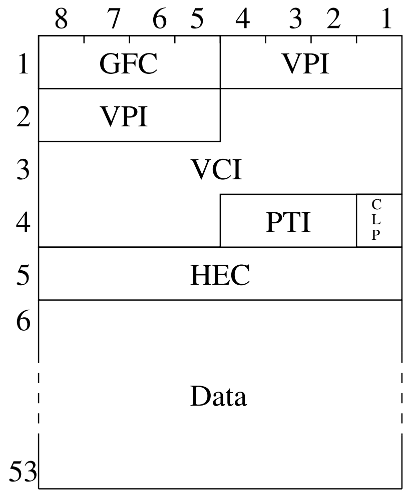

Abbildung 29: ATM-Zelle [Hals 96]

Zellen (Cells) genannt werden (siehe Abbildung 29), von einem Eingangsport zu einem Ausgangsport zu lenken.

Vor Beginn einer Übertragung von Zellen wird eine virtuelle Verbindung im Netz eingerichtet. Nach der Art auf die dies erfolgt, können zwei Typen von Verbindungen unterschieden werden:

- **Permanente Verbindungen (Permanent Virtual Connections, PVC)**
  Diese Verbindungen werden im Zuge des Managements eines ATM-Netzes eingerichtet.

- **Geschaltete Verbindungen (Switched Virtual Connections, SVC)**
  Diese Verbindungen werden während des Betriebs mit einem Signalisierungsprotokoll auf- und abgebaut.

Durch die beiden Felder *Virtual Path Identifier* (VPI) und *Virtual Channel Identifier* (VCI) einer ATM-Zelle wird die virtuelle Verbindung identifiziert, zu der die Zelle gehört. Dieser Identifikator hat aber nur lokale Bedeutung, d.h. zwischen zwei Switches. Für das Weiterleiten einer Zelle wird der Eintrag für seinen Eingangsport und Identifikator in der Routing-Tabelle gesucht. Die Einträge in den Routing-Tabellen der Switches werden beim Verbindungsaufbau erzeugt. Die Felder VPI und VCI der Zelle werden durch die Werte für den Ausgangsport aus der Routing-Tabelle ersetzt und dann wird die Zelle an den Ausgangsport geleitet.

Bei der Suche nach einem Eintrag in der Routing-Tabelle kann entweder nur der VPI oder VPI und VCI verwendet werden. Wird das Routing nur nach dem VPI vorgenommen, spricht man von einer *Virtual Path Connection* (VPC), ansonsten von einer *Virtual Channel Connection* (VCC). Veranschaulicht wird dies durch Abbildung 30.

ATM besitzt ein eigenes Referenzmodell (siehe Abbildung 31). Im ATM-Referenzmodell gibt es folgende Schichten:

- **Physical Layer**
  Entspricht der Physical Layer im OSI-RM. Die Transmission Convergence Sublayer sorgt in dieser Schicht dafür, daß mehrere unterschiedliche Übertragungstechniken genutzt werden können.

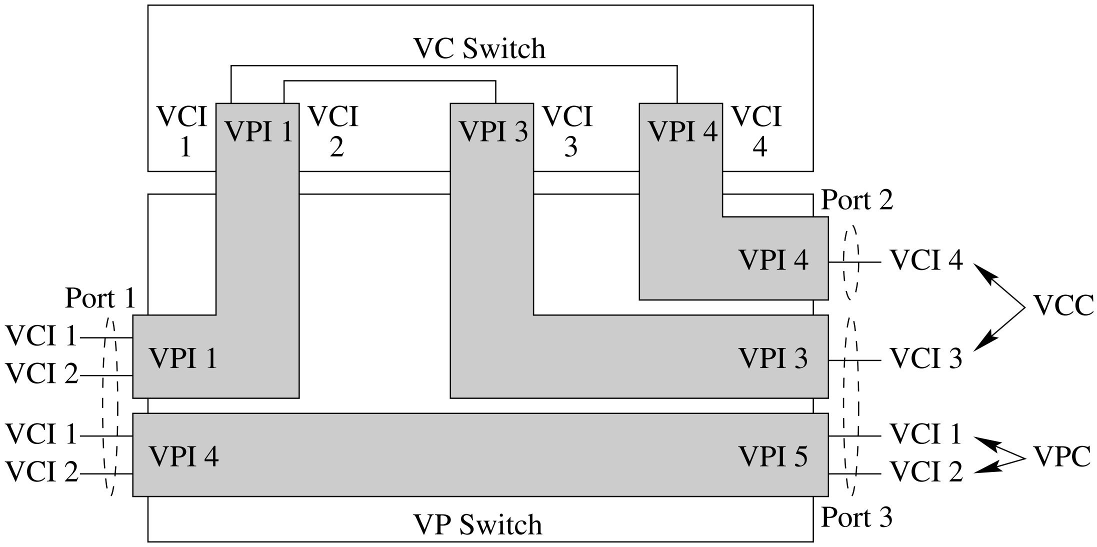

Abbildung 30: VPI und VCI

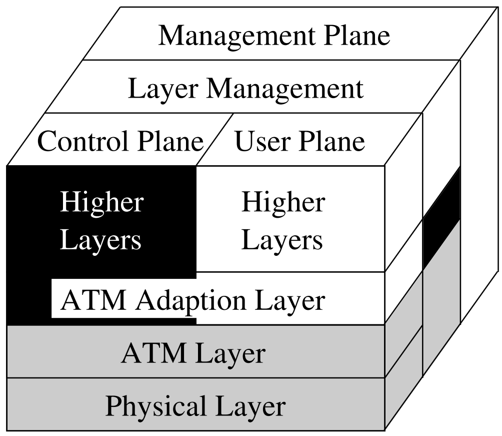

Abbildung 31: ATM-Referenzmodell [ATM-UNI 94, Seite 9]

- **ATM Layer**
  Diese Schicht ist für die Einrichtung von Verbindungen und für die Übertragung von Zellen durchs Netz verantwortlich.

- **ATM Adaption Layer (AAL)**
  In der ATM Adaption Layer werden Dienste für Anwendungen oder höhere Protokoll, wie IP und AppleTalk, angeboten. Diese Schicht besteht aus zwei Unterschichten, *Convergence Sublayer* (CS) und *Segmentation and Reassembly* (SAR) *Sublayer*. Die Segmentation and Reassembly Sublayer sorgt für die Zerlegung der SDUs, die die Größe von Zellen überschreiten, in Zellen und den umgekehrten Vorgang. Die Convergence Sublayer implementiert den Dienst der AAL.

- **Higher Layers**
  Hier sind Protokolle angesiedelt, die die AAL nutzen.

Neben den Schichten gibt es im ATM-Referenzmodells die Ebenen, welche folgende sind:

- **User Plane**
  Die Protokolle der User Plane dienen dem Datentransport zwischen den Anwendungen.

- **Control Plane**
  Die Protokolle der Control Plane werden für Signalisierungen verwendet. Das User-Network Interface (UNI) Protokoll ist ein Protokoll dieser Ebene, das für den Auf- und Abbau von virtuellen Verbindungen dient.

- **Management Plane**
  Die Management Plane besitzt zwei Funktionen, das *Plane Management* und das *Layer Management*.

3.2.1 Dienstgüte von ATM

Die beiden wichtigen Schichten für die Dienstgüte von ATM sind die ATM Layer und die ATM Adaption Layer.

Für den Zelltransport ist die ATM Layer verantwortlich. Der unbestätigte Kommunikationsdienst der ATM Layer besitzt zwei Dienstprimitive:

- `ATM-DATA.request(SDU-Type, Loss-Priority, ATM-SDU)`

- `ATM-DATA.indication(Congestion-Experienced, SDU-type, Loss-Priority, ATM-SDU)`

Bevor mit der `ATM-DATA.request` Dienstprimitive der Transport von Daten erfolgen kann, muß mit dem User-Network Interface (UNI) Signalisierungsprotokoll [ATM-UNI 94][ATM-UNI 96] eine virtuelle Verbindung eingerichtet werden. Bei der Einrichtung der virtuellen Verbindung wird für diese eine Dienstgüte bestimmt. Die Dienstgüte der ATM Layer wird mit folgenden Parametern beschrieben:

- **Cell Error Rate (CER)**
  Gibt den Prozentsatz der mit Fehlern übetragenen Zellen an. Dieser Wert ist von der Technologie in der Physical Layer abhängig und kann daher nicht verhandelt werden.

- **Cell Missinsertion Rate (CMR)**
  Die Rate der in den Switches falsch weitergeleiteten Zellen. Auch dieser Parameter ist nicht verhandelbar, er ist von der Hardware abhängig.

- **Cell Loss Rate (CLR)**
  Prozentsatz der bei der Übertragung verloren gegangenen Zellen. Dieser Wert ist verhandelbar, da er von Faktoren wie Pufferkapazität und Bandbreite abhängt.

- **Maximum Cell Transfer Delay (maxCTD)**
  Die maximale Verzögerung einer Zelle zwischen Sender und Empfänger.

- **peak-to-peak Cell Delay Variation (peak-to-peak CDV)**
  Die maximale Schwankung der Verzögerungszeiten beim Zelltransport.

Neben diesen Parametern, die die Übertragung betreffen, besitzt die ATM Layer noch die Parameter, die den Verkehr beschreiben. Folgende Parameter werden verwendet, um die benötigten Ressourcen zu bestimmen:

- **Sustainable Cell Rate (SCR)**
  Eine andauernde Zelltransferrate, das Mittel der Zelltransferraten über die Dauer der Verbindung.

- **Minimum Cell Rate (MCR)**
  Die minimale Zelltransferrate mit der gesendet wird.

- **Peak Cell Rate (PCR)**
  Die maximale Zelltransferrate mit der gesendet wird.

- **Maximum Burst Size (MBS)**
  Die Maximum Burst Size gibt die Anzahl der Zellen an, die in einem Zeitintervall T mit der PCR gesendet werden dürfen.

- **Cell Delay Variation Tolerance (CDVT)**
  Maximaler Jitter. Der maximale Jitter kann nicht verhandelt werden [ATM-UNI 96].

- **Severely-Errored Cell Block Ratio (SECBR)**
  Der Prozentsatz der fehlerhaften Blöcke. Dieser Parameter kann nicht verhandelt werden. Ein Block ist eine Folge der Länge N von aufeinander folgenden Zellen einer Verbindung. Ein Block ist fehlerhaft, wenn mehr als M Zellen verloren, falsch weitergeleitet oder beschädigt sind.

Für eine Einrichtung einer virtuellen Verbindung müssen nicht alle verhandelbaren Parameter angegeben werden. Welche Parameter benötigt werden hängt von der gewünschten Dienstklasse ab. Die ATM Layer besitzt die folgenden fünf Dienstklassen [ATM-UNI 94] [ATM-UNI 96][ATM-TM 96]:

- **Constant Bit Rate (CBR)** (siehe Abbildung 32)
  Dieser Dienstklasse steht eine fest definierte Bandbreite zur Verfügung (PCR). Verkehr dieser Dienstklasse setzt hohe Anforderungen an die Übertragungszeiten (maxCTD) und die Schwankungen der Übertragungszeiten (peak-to-peak CDV).

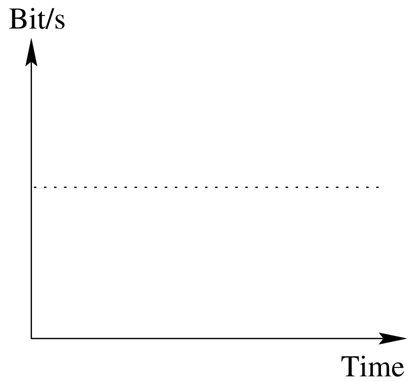

Abbildung 32: CBR

- **Real-Time Variable Bit Rate (rtVBR)** (siehe Abbildung 34)
  Dieser Dienst ist für Anwendungen gedacht, deren Übertragungsraten zeitlich variieren. Der erzeugte Verkehr wird mit PCR, SCR und MBS beschrieben. Analog CBR werden auch hier hohe zeitliche Anforderungen gestellt.

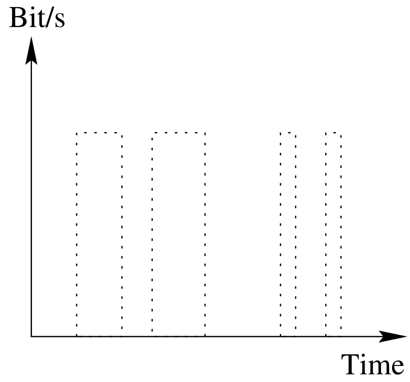

Abbildung 33: ABR

- **Non-Real-Time Variable Bit Rate (nrtVBR)**
  Der Dienst entspricht rt-VBR, jedoch ohne zeitliche Anforderungen.
- **Unspecified Bit Rate (UBR)**
  Es werden keine speziellen Dienstgüteparameter vereinbart.
- **Available Bit Rate (ABR)** (siehe Abbildung 33)
  Für diesen Dienst wird eine minimale (MCR) und maximale Übertragungsrate (PCR) angegeben. Das Netz teilt dem Sender (Feedback) die Verfügbarkeit von Bandbreite zwischen diesen beiden Werten mit. Der Sender paßt dann seine Datenmenge die Gegebenheiten im Netz an.

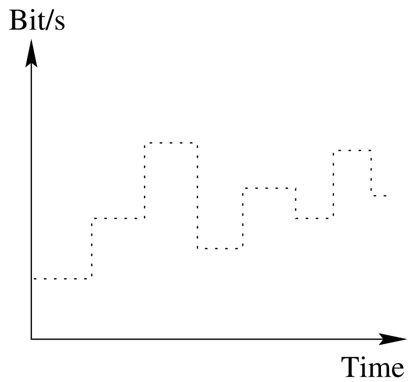

Abbildung 34: VBR

In Tabelle 3) ist zusammengefaßt, welche Parameter für die einzelnen Dienstklassen verwendet werden.

Die *ATM Adaption Layers* (AAL) bauen ihre anwendungsbezogenen Dienste auf dem Dienst der ATM Layer auf. Manche dieser AALs gehen mit einer bestimmten Dienstklasse der ATM Layer einher. Die Dienste der ATM Adaption Layer sind:

- **AAL 1**
  Dieses Protokoll sorgt für einen konstanten Datenstrom zwischen Sender und Empfänger, der von Verlust betroffen sein darf. Dafür daß der Datenstrom im Falle eines Zellverlusts aber nicht unterbrochen wird, muß das Protokoll sorgen. Für das

<table>
<tr><th rowspan="2">Attribute</th><th colspan="5">ATM Layer Service Category</th></tr>
<tr><th>CBR</th><th>rtVBR</th><th>nrtVBR</th><th>UBR</th><th>ABR</th></tr>
<tr><td>Traffic Parameters:</td><td colspan="5"></td></tr>
<tr><td>PCR and CDVT</td><td colspan="3">specified</td><td>specified</td><td>specified</td></tr>
<tr><td>SCR, MBS, CDVT</td><td>n/a</td><td colspan="2">specified</td><td colspan="2">n/a</td></tr>
<tr><td>MCR</td><td colspan="3">n/a</td><td>n/a</td><td>specified</td></tr>
<tr><td>QoS Parameters:</td><td colspan="5"></td></tr>
<tr><td>peak-to-peak CDV</td><td colspan="2">specified</td><td colspan="3">unspecified</td></tr>
<tr><td>maxCTD</td><td colspan="2">specified</td><td colspan="3">unspecified</td></tr>
<tr><td>CLR</td><td colspan="3">specified</td><td>unspecified</td><td></td></tr>
<tr><td>Other Attributes:</td><td colspan="5"></td></tr>
<tr><td>Feedback</td><td colspan="4">unspecified</td><td>specified</td></tr>
</table>

Tabelle 3: Parameter der ATM Layer Dienstklassen [ATM-TM 96, Seite 14]

Erkennen eines Verlust nutzt AAL 1 eine Sequenznummer (SN) (siehe Abbildung 35).

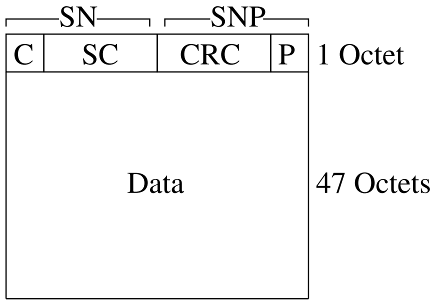

Abbildung 35: AAL 1 Format

- **AAL 2**
  Dieses Protokoll versucht den Datenstrom in der selben Weise auszugeben, wie er am SAP der Sender-AAL angekommen ist. Der Unterschied zum AAL 1 Dienst liegt darin, daß auch eine variable Datenrate unterstützt wird. Das IT-Feld (Information Type) gibt an, ob es sich beim Inhalt der Zelle um den Beginn, eine Fortsetzung oder das Ende einer Nachricht handelt. AAL 2 wird von [ATM-UNI 96] nicht unterstützt. Abbildung 36 zeigt eine AAL 2 PDU.

- **AAL 3/4**
  Der Dienst dieses Protokolls soll für einen verbindungslosen gesicherten Datentransfer dienen. Im Falle von Fehlern in den Zellen oder von Verlusten von Zellen, was durch die Sequenznummer (SN) und der Prüfsumme (CRC) in den Zellen (siehe Abbildung 37) erkannt wird, werden diese erneut übertragen. Damit ist die Übertragung einer PDU gesichert.

- **AAL 5**
  Dieses Protokoll besitzt einen verbindungslosen ungesicherten Dienst. Hier wird auf die Sicherung verzichtet, da diese oft in höheren Protokollen (z.B. TCP) erfolgt.

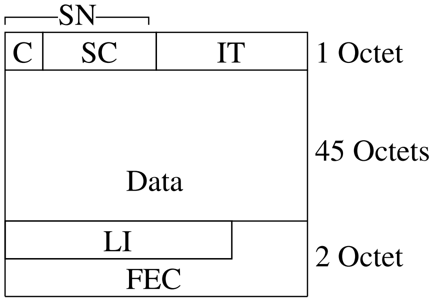

Abbildung 36: ALL 2 Format

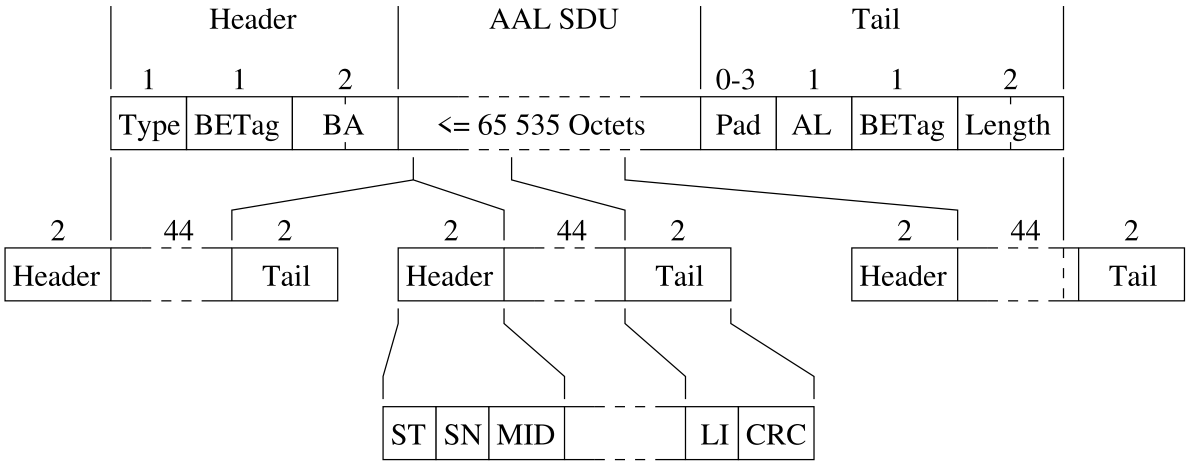

Abbildung 37: ALL 3/4 Format

Durch diese Vereinfachung wird der Overhead der PDU (siehe Abbildung 38) geringer als der der AAL 3/4 gehalten, weshalb man auch von der *Simple and Efficient Adaption Layer* (SEAL) spricht.

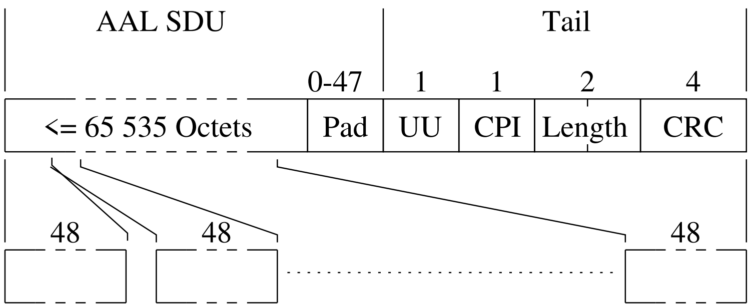

Abbildung 38: ALL 5 Format

3.3 Ethernet/IEEE 802

3.3.1 Das klassische Ethernet/IEEE 802

Ethernet ist wohl die am häufigsten verwendete Netztechnologie im LAN-Bereich. Das Ethernet wurde vom Xerox Palo Alto Research Center anfang der 70er Jahre entwickelt

[HeLa 92]. Später beteiligten sich die Firmen DEC und Intel an der Entwicklung des Ethernet. Diese drei Firmen (abgekürzt DIX) verabschiedeten 1980 die Spezifikation Ethernet V1.0. Das *Institute of Electrical and Electronics Engineers* (IEEE) arbeitete ausgehend von der Version 1.0 des Ethernets eigene Entwürfe aus, an diese dann DIX seine Version 1.0 anzupassen versuchte. Das Resultat war die Spezifikation DIX Ethernet V2.0. Die weiteren Beschreibungen beziehen sich auf die Spezifikationen des Institute of Electrical and Electronics Engineers.

Das Ethernet verwendet eine Bus-Topologie, alle Datenendeinrichtungen (DEE) sind dabei an ein Kabel, das an beiden Enden durch einen Widerstand abgeschlossen ist, angeschlossen (siehe Abbildung 39).

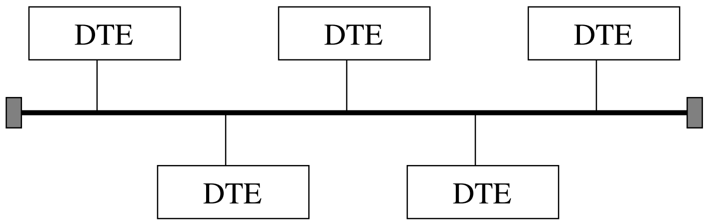

Abbildung 39: Ethernet

Für eine Übertragung zwischen den Datenendeinrichtungen verwendet die Ethernet-Technologie Protokolle der Schichten 2b bis 1 (siehe Abbildung 40) im OSI-Referenzmodell. Die Schicht 2 besteht bei Ethernet aus zwei Teilschichten *Logical Link Control* (LLC) (in IE-

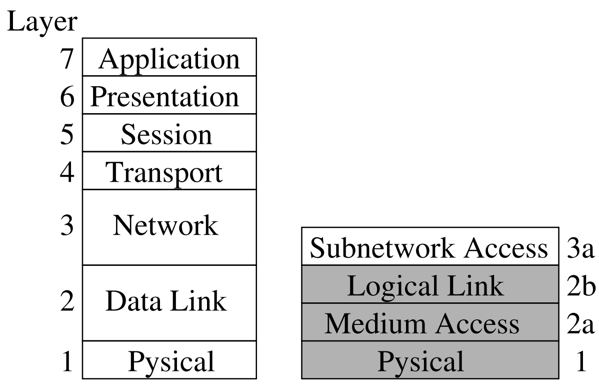

Abbildung 40: Schichten der Ethernet-Technologie

EE 802.2 spezifiziert) und *Medium Access Control* (MAC) (standardisiert in IEEE 802.3). Die LLC-Schicht verwirklicht die Funktionalität von gängigen OSI-Schicht 2 Protokollen, wie z.B. *High-Level Data Link Control* (HDLC). Da sich beim Ethernet die Datenendeinrichtungen ein Medium für die Übertragung untereinander teilen, ist ein Verfahren für den Zugriff auf dieses notwendig. Dieses Verfahren ist in Schicht 2a angesiedelt.

Auf der LLC-Schicht stehen drei Dienste zur Verfügung:

- **Unacknowledged Connectionless Mode Service**
  Ein Datagramm-Dienst.

- **Connectionmode Service**
  Ein verbindungsorientierter Dienst.

- **Acknowledged Connectionless Mode Service**
  Ein bestätigter Datagramm-Dienst.

Die Service Access Points dieser drei Dienste besitzen die Dienstprimitiven aus Tabelle 4.

Dienst	Dienstgruppe	Dienst- primitive	Verwendung
1	DL-UNITDATA	request indication	Datagramm-Austausch
2	DL-CONNECT	request indication response confirm	Verbindungsaufbau
	DL-DATA	request indication	Datenaustausch
	DL-DISCONNECT	request indication	Verbindungsabbau
	DL-RESET	request indication response confirm	Wiederaufbau
	DL-CONNECTION-FLOW-CONTROL	request indication	Flußsteuerung
3	DL-DATA-ACK	request indication	Datagramm-Übergabe
	DL-DATA-ACK-STATUS	indication	Quittungsmeldung
	DL-REPLY	request indication	Sendeaufruf
	DL-REPLY-STATUS	indication	Empfangsanzeige
	DL-REPLY-UPDATE	request	Voranzeige Sendeaufruf
	DL-REPLY-UPDATE-STATUS	indication	Bestätigung Voranzeige

Tabelle 4: LLC-Dienstprimitive [HeLa 92]

Das LLC-Protokoll ist in Anlehnung an das HDLC-Protokoll entstanden. LLC-Frames sind nach Abbildung 41 aufgebaut. Die in DSAP und SSAP enthaltenen Adressen dienen

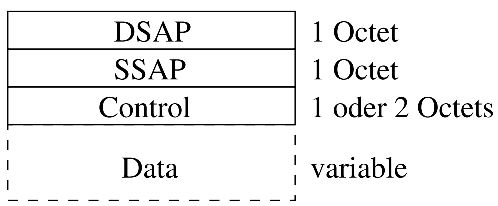

Abbildung 41: LLC-Format

für das Demultiplexen an den SAPs des Ziels (DSAP) und der Quelle (SSAP). Mit diesen Werten wird der LLC-Dienst und die Instanz der übergeordneten Schicht adressiert. Im Control-Feld werden der Frametyp und gegebenenfalls Sequenznummern angegeben.

Für den Transport der LLC-Frames greift dieses Protokoll auf die Dienstprimitve der MAC-Schicht zurück, welche folgende sind:

- `MA-UNITDATA.request(Source Address, Destination Address, Data, Priority, Service Class)`
- `MA-UNITDATA.indication(Destination Address, Source Address, Data, Reception Status, Priority, Service Class)`
- `MA-UNITDATA-STATUS.indication(Destination Address, Source Address, Transmission Status, Provided Priority, Provided Service Class)`

Auf Schicht 2a gibt es nur einen unbestätigten verbindungslosen Dienst. Die Übertragung einer SDU auf OSI-Schicht 2a erfolgt mit dem MAC-Frame aus Abbildung 42.

Preamble	7 Octets
Start Frame Delimiter	1 Octet
Destination Address	2 oder 6 Octets
Source Address	2 oder 6 Octets
Length	2 Octets
Data	variable
PAD	variable
FCS	4 Octets

Abbildung 42: MAC-Format

Das Mediumzugriffsverfahren hat dafür zu sorgen, daß ein MAC-Frame auf das Medium entlassen wird. Das Verfahren, das der Standard IEEE 802.3 für den Zugriff definiert, wird Carrier Sense Multiple Access with Collision Detect (CSMA/CD) genannt. Die Funktionsweise ist wie folgt (siehe Abbildung 43):

1. Liegt ein Frame zur Übertragung vor, muß die DEE überprüfen, ob das Medium momentan nicht genutzt wird.

2. Ist das Medium ungenutzt, kann nach 9,6 Mikrosekunden mit der Übertragung begonnen werden.

3. Falls eine Übertragung im Gange ist, muß gewartet werden bis diese vorbei ist, dann kann aber sofort übertragen werden.

4. Während der Übertragung muß das Medium abgehört werden, ob keine anderes Datenendgerät auch sendet, und somit die Übertragung stört.

5. Wird die Übertragung gestört (Kollision), muß ein Störsignal (Jam-Signal) auf das Medium gesendet werden.

6. Nachdem das Jam-Signal gesendet wurde, wird gemäß der Backoff-Strategie gewartet. Nach der Wartezeit wird mit Schritt 1 fortgefahren.

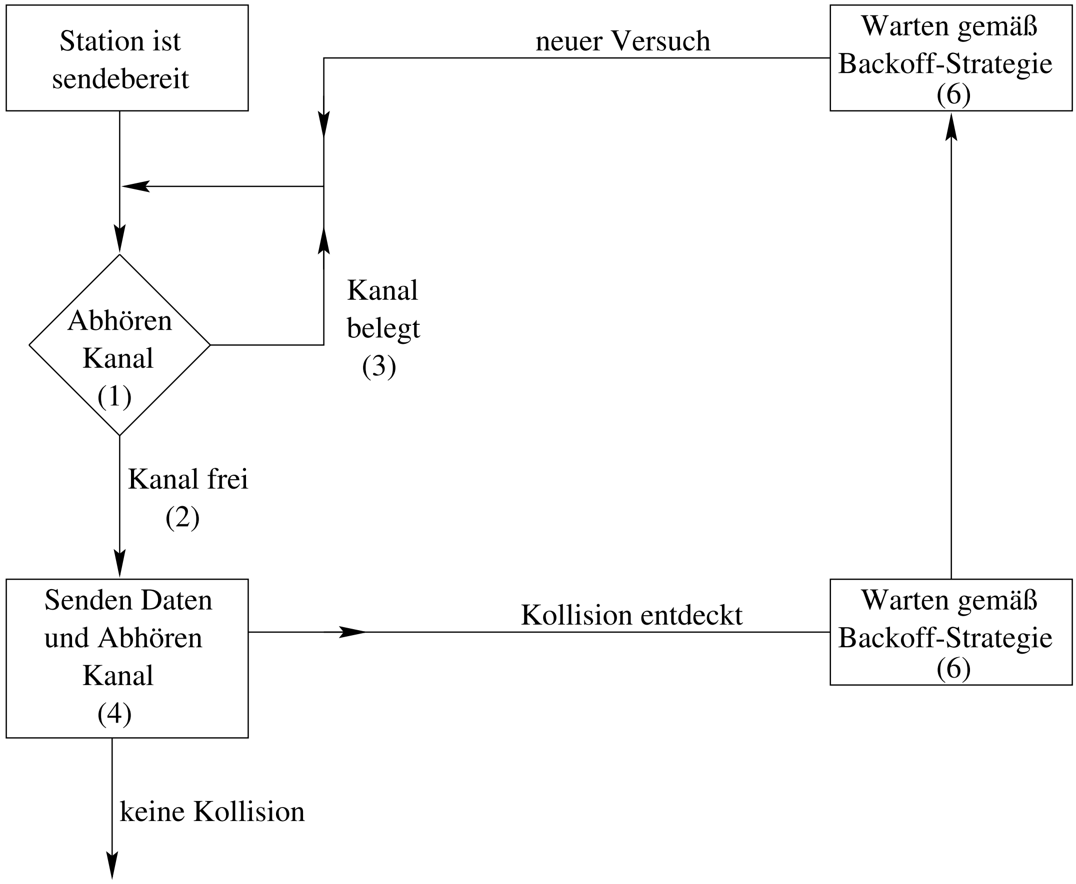

Abbildung 43: CSMA/CD-Zugriffsverfahren [HeLa 92]

Die Wartezeit gemäß der Backoff-Strategie wird wie folgt berechnet: $i \cdot SlotTime$. Die $SlotTime$ ist durch die Übertragungszeit eines Paketes mit Minimalgröße (64 Octets) bestimmt $(51,2\mu s)$. Die Zahl i ist eine gleichverteilte Zufallsgröße aus dem Intervall $[0;2^k]$, wobei $k = \min(n, 10)$ ist. n ist die Nummer des Wiederholungsversuchs, sie ist auf maximal 16 beschränkt. Wird diese Zahl erreicht wird eine Fehlermeldung zurückgegeben. Wichtige Werte des Ethernets können der Tabelle 5 entnommen werden.

Übertragungsrate	10Mbit/s
Maximale Paketgröße	1518 Octets
Minimale Paketgröße	64 Octets
Jam-Signal	32Bit

Tabelle 5: Werte des Ethernets

3.3.2 Bridge und Switch

Bridge Das Ethernet ist in seiner räumlichen Ausbreitung beschränkt, diese Einschränkung wurde in den frühen 80-igern mit der Einführung von Bridges beseitigt. Bridges übernehmen dabei die Funktion mehrere Ethernets zu einem größeren Netz zu verbinden (siehe Abbildung 44). Mit einer Bridge ist es auch möglich auf OSI-Schicht 2 verschiedene Netztechnologien, wie z.B. Ethernet, Token Bus und Token Ring, zu koppeln.

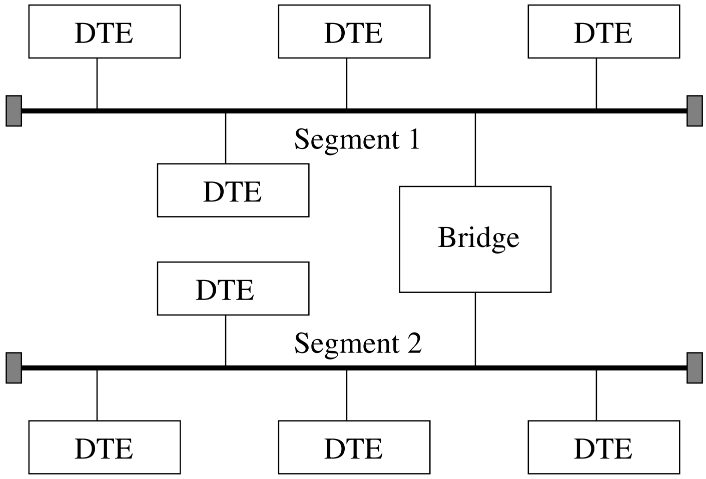

Abbildung 44: Bridge

Die Bridge arbeitet auf OSI-Schicht 2. Ihre Hauptaufgabe ist es, die an den Ports eingehenden Pakete auf Fehler zu untersuchen und anhand der Schicht 2 Adressen an die entsprechenden Ausgangsports zu leiten. Bridges unterhalten für jeden Ausgangsport mindestens eine Queue, um momentane Staus zu beseitigen. Bridges, die dem neusten Standard [IEEE-P802.1D/D17] folgen, besitzen mindestens zwei und maximal acht Queues für einen Ausgangsport, jede dieser Queues stellt eine Verkehrsklasse dar. Anhand der *User Priority*, die nach dem neuen Standard [IEEE-P802.1Q/D11], im Ethernet-Paket transportiert werden kann, werden die Pakete auf die Einzelnen Verkehrsklassen aufgeteilt. Die Queues werden dann mit einem Prioritätsscheduling-Verfahren geleert (siehe Abbildung 45).

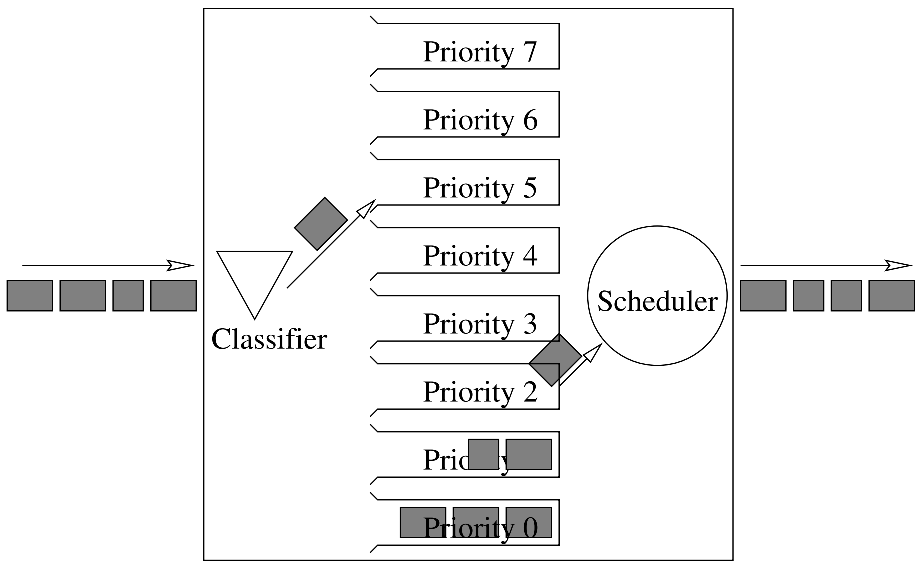

Abbildung 45: Funktion in einer Bridge

Switch Eine Tendenz, um das Leistungsvermögen des Ethernets mit der klassischen Bus-Topologie zu verbessern, besteht darin, die DEE mit einer Stern-Topologie zu verbinden. Im Zentrum dieser Topologie sitzt ein *Switch* (siehe Abbildung 46), der die Aufgabe hat an

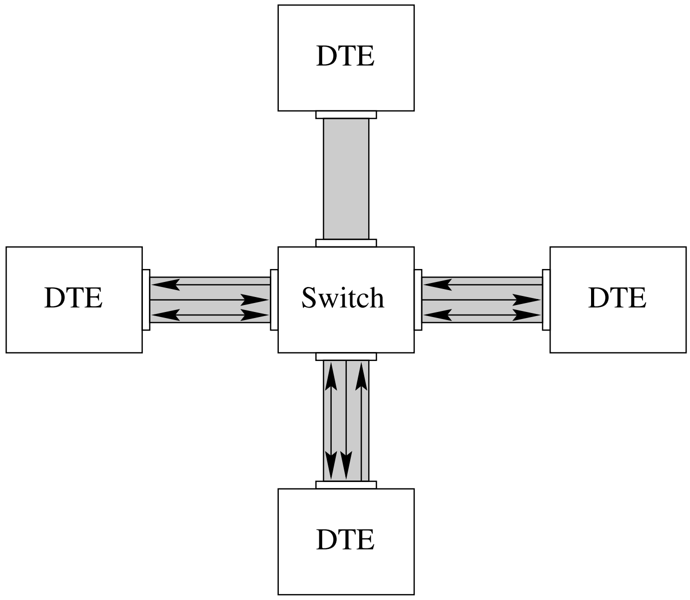

Abbildung 46: Switch

den Eingangsports eintreffende Pakete auf die Ausgangsports zu schicken. Jede Datenendeinrichtung besitzt eine Sende-, eine Empfangs- und eine Jam-Signal-Leitung. Damit kann ein Duplex-Betrieb (gleichzeitiges Senden und Empfangen) ermöglicht werden. Kollisionen können nur auftreten, wenn eine Empfangsleitung einer Datenendeinrichtung besetzt ist und eine andere Datenendeinrichtung an diese senden will [Hals 96].

Ersetzt man den Switch durch eine *Multiport Bridge*, dann verfügt jeder Ausgangsport mindestens über einen Puffer und damit können keine Kollisionen mehr auftreten. Die Multiport Bridge wird auch als Switch bezeichnet. Jede Leitung von einer Datenendeinrichtung zum Switch und jede Leitung vom Switch zu einer Datenendeinrichtung stellt ein Segment dar. Wegen des Umstandes, daß es nur einen Sender pro Segment gibt, spricht man von *Microsegmentation*.

3.3.3 Dienstgüte des Ethernet

Harte Garantien für Dienstgüteparameter, wie maximale Übertragungsverzögerung und maximaler Verlust, anzugeben, ist beim Shared-Ethernet aufgrund des CSMA/CD-Verfahrens schwierig bis geradezu unmöglich. Man denke hier an den Fall, daß zwei Sender zufällig immer zum gleichen Augenblick versuchen auf das Medium zuzugreifen und sich so gegenseitig am Senden hindern.

In einem Switched-Ethernet (ein Sender pro Segment) spielt das CSMA/CD-Verfahren keine Rolle. Die Dienstgüte vom und zum Switch ist durch die Eigenschaften des Übertragungsmediums bestimmt. Ein neuerer Switch verfügt über mehrere Queues für einen Ausgangsport. Aus diesen Queues werden die PDUs mit einem Prioritätsscheduling ausgewählt. Die zwei Dienstgüteparameter die hierdurch beeinflußt werden, sind die Übertragungsverzögerung und der Verlust. Beide sind von der *Last* (Load) des Verkehrs mit der selben Priorität und derer mit höheren Prioritäten abhängig.

4 Kriterienkatalog

In diesem Kapitel wird ein Kriterienkatalog erarbeitet, um Technologien für Quality of Service vergleichen zu können. Für einen Vergleich müssen Kriterien gefunden werden. Bleibt die Frage, wer oder was liefert die Kriterien?

Die Anwort auf diese Frage hängt von der konkreten Zielsetzung des Kriterienkatalogs ab.

4.1 Ziele des Kriterienkatalogs

Der Kriterienkatalog soll dem Vergleich von Technologien für Quality of Service dienen. Die Technologien werden von Personen eingesetzt. Diese Personen haben gewisse Ansprüche an die Technologien. Es lassen sich zwei Personengruppen anhand der Ansprüche, die sie an die Technologien stellen, unterscheiden:

- **Dienstnutzer**
  Die Technologien bieten dem Dienstnutzer Kommunikationsdienste mit ihren Dienstgüten an. Die Dienstnutzer stellen ihre Ansprüche an die Dienste und Dienstgüten der Technologien.

- **Diensterbringer**
  Der Diensterbringer stellt die Technologien dem Dienstnutzer zur Verfügung. Er ist daran interessiert, daß die Dienstnutzer, als seine Kunden, mit den Kommunikationsdiensten zufrieden sind. Darüber hinaus möchte der Diensterbringer seine Ressourcen (z.B. Router, Leitungen, Arbeitszeit u.s.w.) möglichst effizient einsetzen, um Kosten zu sparen und damit wettbewerbsfähig zu sein. Der Diensterbringer stellt sein Ansprüche an den Ressourcenbedarf der Technologien.

Das erste Ziel des Kriterienkatalogs ist, daß ein Vergleich anhand der Ansprüche der Dienstnutzer und Dienserbringer durchgeführt wird.

Das zweite Ziel des Kriterienkatalogs ist, daß er auf alle Technologien, auch zukünftige, anwendbar ist. Er darf also nicht auf den Vergleich spezieller Technologien zugeschnitten sein.

4.2 Ermittlung von Kriterien

Es werden nun die Kriterien des Katalogs ermittelt. Das erste Ziel des Kriterienkatalogs ist, daß ein Vergleich anhand der Ansprüche von Dienstnutzer und Diensterbringer durchgeführt wird. Die Folgerung für das Erreichen dieses Ziels ist, deren Ansprüche als Kriterien zu verwenden.

Die Ansprüche und damit die Kriterien sind für Dienstnutzer und Diensterbringer unterschiedlich. Damit die Personengruppen die für sie relevanten Kriterien möglichst schnell erkennen, werden sie in zwei Kategorien im Kriterienkatalog eingeteilt. Eine weitere Unterteilung der Kriterien ist wünschenswert, damit das zu einer bestimmten Anforderung passende Kriterium schnell gefunden wird. Diese Baumstruktur erlaubt es einem Anwender des Kriterienkatalogs die für seine Ansprüche wichtigsten Kriterien zuerst zu betrachten, damit kann frühzeitig erkannt werden, falls eine Technologie ungeeignet ist.

Bei der Ermittlung der Kriterien sollen möglichst Kategorien für deren Einteilung gesucht werden.

4.2.1 Mögliche Kriterien für den Dienstnutzer

Es sollen nun mögliche Kriterien, die die Ansprüche des Dienstnutzers beschreiben, gesucht werden. Ein Dienstnutzer hat gewisse Ansprüche an die Dienstgüte eines Kommunikationsdienstes. Diese Ansprüche können beim Zugang zu einem Dienst gegenüber dem Netz geäußert werden. Dies kann mit Parametern von Dienstprimitiven erfolgen. Das *Open Systems Interconnection* TCP-Protokoll (OSI-TCP-Protokoll) [Hals 96][Adam 97] ist ein Beispiel für ein Protokoll dessen Dienstprimitive zum Verbindungsaufbau viele Optionen zur Dienstgütespezifizierung besitzt. Die Optionen können Tabelle 6 und 7 entnommen werden. Alle diese Optionen sind Kandidaten für Kriterien.

Parameter	**Beschreibung**
Throughput	Die maximale Anzahl von in Service Data Units (SDUs) enthaltenen Bytes, die in einer Zeiteinheit vom Service Provider erfolgreich über die Verbindung übertragen werden können
Transit Delay	Die Zeitspanne zwischen dem Absetzen eines `data.request` und dem korrespondierenden `data.indication`.
Residual Error Rate	Die Wahrscheinlichkeit, daß eine SDU fehlerhaft übertragen, verloren oder dupliziert wird.
Establishment Delay	Die Zeitspanne zwischen dem Absetzen eines `connect.-request` und dem korrespondierenden `connect.confirm`.
Establishment Failure Probability	Die Wahrscheinlichkeit, daß eine angeforderte Verbindung aufgrund nur vom Service Provider beeinflußbarer Zustände nicht innerhalb der maximal akzeptable Zeit aufgebaut werden konnte
Transfer Failure Probability	Die Wahrscheinlichkeit, daß die beobachtete Leistung unter der Berücksichtigung von *Transit Delay*, *Residual Error Rate* oder *Throughput* schlechter als das spezifizierte Niveau ist.
Resilience	Die Wahrscheinlichkeit, daß der Service Provider von sich aus die Verbindung innerhalb einer Zeiteinheit freigibt oder zurücksetzt
Release Delay	Die Zeitspanne zwischen dem Absetzen einer `disconnect.request` Primitive durch den Dienstnutzer und der durch den Service Provider abgesetzten korrespondierenden `disconnect.indication` Primitive.
Release Failure Probability	Die Wahrscheinlichkeit, daß der Service Provider nicht in der Lage ist, die Verbindungen innerhalb einer spezifizierten maximalen Freigabeverzögerung freizugeben.

Tabelle 6: OSI leistungsbezogene QoS-Parameter [Adam 97]

Gleiches gilt für die Parameter mit denen beim Aufbau einer virtuellen Verbindung in einem ATM-Netz die Dienstgüte spezifiziert wird. ATM verwendet zum Verbindungsaufbau ein Protokoll, das UNI-Signalisierungsprotokoll [ATM-UNI 94][ATM-UNI 96], das für die Spezifizierung der Dienstgüte die Parameter aus Tabelle 8 bereitstellt.

Die Dienstgüte muß aber nicht beim Verbindungsaufbau spezifiziert werden, sie kann vertraglich mit dem Diensterbringer festgelegt werden. Die Diensterbringer haben sich Ge-

Parameter	**Beschreibung**
Protection	Das Ausmaß mit dem ein Service Provider versucht, unautorisiertes Anzeigen und Manipulieren von Daten zu verhindern. Das Schutzniveau ist qualitativ spezifiziert durch: 1. kein Schutz 2. Schutz gegen passives Anzeigen 3. Schutz gegen Veränderung, Hinzufügung oder Löschen 4. eine Kombination aus zweitens und drittens
Priority	Höher priorisierte Verbindungen werden vor niedriger priorisierten behandelt. Pakete von niedriger priorisierten Verbindungen werden im Falle eines Staus vor denen von höher priorisierten gelöscht.
Cost Determinants	Ein Parameter, um die maximal akzeptablen Kosten für eine Verbindung zu definieren. Dieser kann in absoluten oder relativen Thermen definiert sein.

Tabelle 7: OSI nicht-leistungsbezogene QoS-Parameter [Adam 97]

Parameter	**Beschreibung**
Cell Error Rate (CER)	Gibt den Prozentsatz der mit Fehlern übertragenen Zellen an. Dieser Wert ist von der Technologie in der Physical Layer abhängig und kann daher nicht verhandelt werden.
Cell Loss Rate (CLR)	Prozentsatz der bei der Übertragung verloren gegangenen Zellen.
Maximum Cell Transfer Delay (maxCTD)	Die maximale Verzögerung einer Zelle zwischen Sender und Empfänger.
Peak-to-peak Cell Delay Variation (CDV)	Die maximale Schwankung der Verzögerungszeiten beim Zelltransport.
Sustainable Cell Rate (SCR)	Die Zelltransferrate mit der gesendet wird.
Minimum Cell Rate (MCR)	Die minimale Zelltransferrate mit der gesendet wird.
Peak Cell Rate (PCR)	Die maximale Zelltransferrate mit der gesendet wird.
Maximum Burst Size (MBS)	Die Maximum Burst Size gibt die Anzahl der Zellen an, die in einem Zeitintervall T mit der PCR gesendet werden dürfen.

Tabelle 8: Parameter des UNI-Signalisierungsprotokolls

danken darüber gemacht, mit welchen Parametern sie die Dienstgüte mit dem Kunden vereinbaren können. Ein Resultat so einer Überlegung entstand bei der *International Telecommunication Union - Telecommunication* (ITU-T) [Adam 97]. Sie schlägt die Parameter aus Tabelle 9) vor.

Bei der Betrachtung aller möglichen Kriterien fällt auf, daß Parameter mit unterschied-

Parameter	**Beschreibung**
Access Delay	Der Wert der vergangenen Zeit zwischen absetzen des Zugangsgwunsches und Zugang
Incorrect Access Probability	Das Verhältnis der Anzahl aller Zugangsversuche, die in einem inkorrekten Zugang endeten, zur Gesamtanzahl aller Zugansgversuche.
Access Denial Probability	Das Verhältnis der Anzahl aller Zugangsversuche, die in einer Zugangsverweigerung endeten, zur Gesamtanzahl aller Zugansgversuche.
User Information Transfer Delay	Der Wert der vergangenen Zeit zwischen dem Start des Transfers und dessen Erfolg einer spezifizierten Benutzerdaten-Einheit
User Information Transfer Rate	Gesamtanzahl aller erfolgreich übertragenen Benutzerdaten-Einheiten, geteilt durch die Übertragungszeit.
User Information Error Probability	Das Verhältnis aller inkorrekt übertragenen Dateneinheiten zu allen übertragenen Einheiten.
User Information Misdelivery Probability	Das Verhältnis aller fehlgeleiteten Benutzerdaten-Einheiten zu allen übertragenen Benutzerdaten-Einheiten.
User Information Loss Probability	Das Verhältnis aller verlorengegangenen Benutzerdaten zu allen übertragenen Benutzerdaten.
Disengagement Delay	Die vergangene Zeit zwischen dem Start eines Zugangs-Abbau-Versuches und des erfolgreichen Zugangsabbaus.
Incorrect Disengagement Probability	Das Verhältnis aller Zugangs-Abbau-Versuche, die in einem inkorrektem Zugangsabbau endeten, zur gesamtanzahl aller Zugangs-Abbau-Versuche.
Disengagement Denial Probability	Das Verhältnis der Gesamtanzahl aller verweigerten Zugangs-Abbau-Versuche zu der Gesamtanzahl aller Zugangs-Abbau-Versuche.

Tabelle 9: ITU-T QoS Parameter [Adam 97]

lichem Namen ähnliche Absichten verfolgen. Darauf soll bei der Auswahl der Kriterien geachtet werden.

Als weitere Kriterien für den Dienstnutzer könnten Eigenschaften bestehender Technologien in Frage kommen. So wären folgende Kriterien denkbar:

- Geht eine Reservierung vom Sender oder vom Empfänger aus?
- Können verschiedene Empfänger einer Multicast-Kommunikation unterschiedliche Dienstgüten erhalten?
- Ist eine Technologie Microflow- oder Aggregat-orientiert?
- u.s.w.

Auf technologie-spezifische Eigenschaften als Quelle für Kriterien wird verzichtet. Technologie-spezifische Eigenschaften können sehr unterschiedlich sein und sind damit oft nur bedingt auf neuere odere andere Technologien anwendbar. Damit kann mit ihnen das Ziel, daß der Kriterienkatlog auf alle Technologien einsetzbar ist, nicht erreicht werden. Der Dienstnutzer ist eigentlich auch nicht an den Eigenschaften der Technologien interessiert, sondern eher am Einfluß dieser auf die zu erhaltenden Dienste und Dienstgüten.

Jetzt da eine Menge von möglichen Kriterien zur Verfügung steht, soll eine vernünftige Auswahl getroffen werden.

4.2.2 Auswahl der Kriterien für den Dienstnutzer

Das Problem bei der Aufstellung von Kriterien für den Dienstnutzer ist, daß seine Anforderungen an die Dienste und Dienstgüten oft sehr spezifisch sind. Das Resultat sind sehr viele verschiedene Anforderungen. Bei der Aufstellung des Kriterienkatalogs besteht daher die Gefahr, daß einige oder viele dieser Anforderungen nicht berücksichtigt werden.

Um dennoch eine Vielzahl an Anforderungen mit wenigen allgemein einsetzbaren Kriterien abzudecken, soll ein Kriterium folgenden Aufbau haben:

$$Kriterium_{Voraussetzungen}$$

Ziel der Anwendung eines Kriteriums ist es, Aussagen über die Technologie treffen zu können. Diese Aussagen können quantitativ, qualitativ oder relativ sein. Die Aussagen werden unter bestimmten Voraussetzungen gemacht. Dies ermöglicht es, ein Kriterium einer Technologie anzupassen und vernünftige Aussagen über die Technologie zu machen. Spezifische Anforderungen können so oft, durch geeignete Voraussetzungen für ein Kriterium, ausgedrückt werden. Für die Erfüllung einer Anforderung gilt, daß sowohl die Aussage zu einem Kriterium als auch dessen Voraussetzungen der Anforderung entsprechen.

Es folgt nun die Auswahl der Kriterien für den Dienstnutzer aus den möglichen Kandidaten des Abschnitts 4.2.1.

Eine Kommunikation kann man in drei Phasen gliedern. In der ersten Phase wird der Zugang zu einem Dienst hergestellt.

- **Zugangsphase (Access)**
  Die Dienstgüteparameter für die Zugangsphase sind:
  - *Establishment Delay, Access Delay*
    Diese Parameter drücken die Zeit aus, die für den Zugang zu einem Dienst benötigt wird. Dieser Parameter ist vom Zugangsverfahren abhängig, das ein Teil der Technologien sein kann. Dieses Kriterium wird unter dem Namen *Access Delay* in den Katalog aufgenommen.
  - *Establishment Failure Probability, Access Denial Probability, Incorrect Access Probability*
    Mit diesen Parameter werden die Fälle, die zu keinem korrekten Zugang führen, beschrieben. Keinen oder falschen Zugang erhält man, wenn Fehler im Netz auftreten, wie z.B. es sind keine Ressourcen vorhanden. Diese Fehler treten nur in einem Netz aber nicht in einer Technologie auf, daher sind diese Parameter für den Vergleich von Technologien nicht angemessen. Diese Parameter werden nicht in den Kriterienkatalog aufgenommen.
- **Übertragungsphase (Transfer)**
  Die Dienstgütepatameter für die Übertragungsphase sind:

- *Throughput, User Information Transfer Rate, SCR, MCR, PCR*
  Diese Parameter drücken alle Übertragungsraten aus. Die Übertragungsrate wird unter dem Namen *Transfer Rate* als Kriterium in den Katalog aufgenommen. Auf *SCR*, *MCR* und *PCR* soll verzichtet werden, da nur sehr allgemeine Kriterien für die Ansprüche des Dienstnutzers aufgenommen werden sollen.
- *Residual Error Rate, User Information Error Probability, CER, User Information Misdelivery, CMR*
  Bei der Übertragung von Daten können Fehler auftreten. Diese Parameter drücken die Häufigkeit aller oder nur einen Teil dieser Fehler aus. Sie sind von der Qualität der verwendeten Hardware (z.B. Leitungen, Router und Switch) abhängig und nicht von der Technologie. Diese Parameter werden nicht aufgenommen.
- *Transit Delay, User Information Transfer Delay, maxCTD*
  Die Übertragungsverzögerung wird mit diesen Parametern angegeben. Die Übertragungsverzögerung wird unter dem Begriff *Transfer Delay* im Kriterienkatalog erscheinen. Auf *maxCTD* wird verzichtet, da nur sehr allgemeine Kriterien aufgenommen werden sollen.
- *CDV*
  Dieser Parameter drückt den Jitter[3] aus. Das Kriterium *Jitter* wird im Kriterienkatalog aufgenommen.
- *User Information Loss Probability, CLR*
  Der Verlust von Daten tritt aufgrund von Fehlern und Staus auf. Diese Parameter drücken einen (*CLR*) oder beide Ursachen (*User Information Loss Probability*) aus. Da Fehler bei der Betrachtung der Technologien ausgeschlossen sind, wird nur ein Kriterium *Loss* einführen. Dieses Kriterium drückt den Verlust aufgrund von Staus aus.
- *Transfer Failure Probability*
  Transfer Failure Probability wird auch kein Kriterium im Katalog sein. Dieser Parameter drückt die Fehler aus, von vorgegebenen Dienstgütewerten in einem Netz abzuweichen. Die Abweichung von Dienstgüteparametern wird durch Fehler in einem realen Netz eintreten. Bei der Betrachtung von Technologien gibt es keine Fehler.
- *Resilience*
  Dieser Parameter ist als Kriterium ungeeignet, da es beim Vergleich von Technologien einen realen Service Provider nicht gibt.

- **Zugangsabbauphase (Release)**
  Die Dienstgüteparameter der Zugangsabbauphase sind:
  - *Release Delay, Disengagement Delay*
    Diese Parameter drücken die Zeit aus, die für den Abbau eines Dienstes benötigt wird. Für diese Parameter wird ein Kriterium namens *Release Delay* in den Katalog aufgenommen.

[3] Der Begriff Jitter wird für die Varianz der Übertragungszeiten verwendet.

- *Release Failure Probability, Incorrect Disengagement Probability, Disengagement Denial Probability*
  Mit diesen Parametern werden die Fälle, die zu keinem korrekten Abbau eines Zugangs führen, beschrieben. Keiner oder falscher Abbau eines Zugangs entsteht, wenn Fehler im Netz auftreten. Fehler treten nur in einem Netz aber nicht in einer Technologie auf, daher sind diese Parameter für den Vergleich von Technologien nicht angemessen. Diese Parameter werden nicht in den Kriterienkatalog aufgenommen.

Die restlichen Parameter die nicht in diese drei Phasen passen sind:

- *Protection*
  Dieser Parameter drückt den Schutz eines Kommunikationsdienstes aus. Es sollen drei Kriterien, die den Schutz vor verschiedenen Angriffen beschreiben, in den Katalog einfließen: *Theft of Service*, *Listening* (Abhören einer Kommunikation) und *Change* (unbemerkte Veränderung von Daten). Von Theft of Service spricht man, wenn jemand den Kommunikationsdienst einer anderen Person nutzt. Die drei Kriterien sollen zur Kategorie *Protection* gehören.

- *Priority*
  Mit diesem Parameter wird eine Priorität angegeben. Diese Priorität wird im Staufall verwendet, um die Auswahl der Daten zu steuern, die zur Staubeseitigung verworfen werden. Auf ein Kriterium *Priority* wird verzichtet, da es technologie-spezifisch ist.

- *Cost Determinants*
  Mit diesem Parameter werden die maximal akzeptablen Kosten einer Verbindung festgelegt. Kriterien, die sich auf die Kosten beziehen, folgen beim Diensterbringer.

Die Kriterien für den Dienstnutzer zeigt die Abbildung 47.

Nun folgen die Kriterien des Diensterbringers.

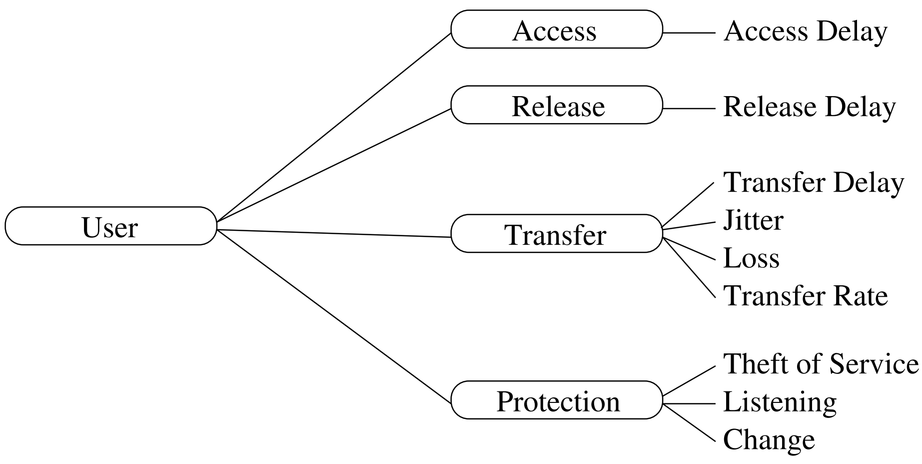

Abbildung 47: Kriterien des Dienstnutzers

4.2.3 Diensterbringer

Der Diensterbringer stellt die vom Kunden verlangten Dienste und Dienstgüten bereit. Die Anforderungen des Diensterbringers an die Technologien zielen darauf hin, mit ihnen die Bereitstellung der Dienste und Dienstgüten so effizient wie möglich zu gestalten. Das Netzmanagement befaßt sich mit allen Aufgaben, die bei der Bereitstellung eines Netzes anfallen. In [HeAb 93, Seite 87 ff] werden drei Dimensionen vorgeschagen, um die Managementaufgaben einzuteilen:

1. **Funktionale Dimension**
   Hier werden die Managementaufgaben Funktionsbereichen zugeordenet.

2. **Zeitliche Dimension**
   Der Managementprozeß wird hier in Phasen eingeteilt, in denen die Managementleistung erbracht wird.

3. **Dimension der Szenarien**
   In dieser Dimension wird das Management entsprechend dem Zielobjekt mit dem es sich befaßt unterteilt.

In der dritten Dimension werden die Managementaufgaben in Komponenten-, System-, Anwendungs- und Enterprise-Management unterteilt. Die Netzmanagementaufgaben fallen in das Komponentenmanagement. Damit finden wir alle Netzmanagementaufgaben in den zwei Dimensionen der Abbildung 48 [HeAb 93].

Die weitere Vorgehensweise bei der Ermittlung von Kriterien sieht folgendermaßen aus: In jeder Aufgabengruppe der funktionalen Dimension sollen Kriterien für die Managementaufgaben gefunden werden. Die Managementaufgaben einer Aufgabengruppe können aus den Phasen Planung, Realisierung und Betrieb stammen. Die Aufgabengruppen dienen als Kategorien für die Kriterien des Diensterbringers.

In jeder Aufgabengruppe der funktionalen Dimension fallen durch die Managementaufgaben Kosten an, um die Dienste und Dienstgüten zur Verfügung zu stellen (z.B. Personalkosten und Kosten für das Equipment). Ein Netz möglichst effizient zu betreiben bedeutet, bei gleicher Leistung möglichst wenig Kosten zu verursachen. Daher sollen für die wichtigsten Einflüsse auf die Kosten Kriterien in den Aufgabengruppen gefunden werden.

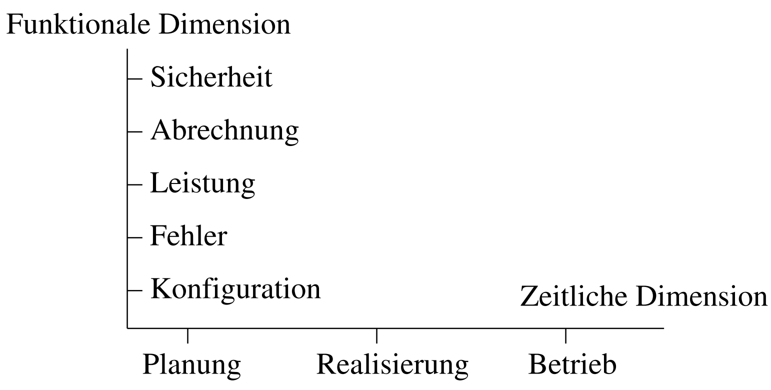

Abbildung 48: Dimensionen des Managements

Konfigurationsmanagement Das Konfigurationsmanagement besteht aus der Aufgabe, die Ressourcen eines Kommunikationsnetzes anzupassen, damit die Kommunikationsleistung in der erwünschten Form erbracht wird.

Die Kosten für die Konfiguration einer Technologie wird durch die Zeit, in der die Dienste des Netzes nicht oder verspätet genutzt werden, bestimmt. Die Unkosten laufen in dieser Zeit weiter, aber die Einnahmen fallen aus. Die Zeit für die Konfiguration wird mit dem Kriterium *Configuration Delay* in den Katalog aufgenommen.

Fehlermanagement Für einen Netzbetreiber ist es wichtig, daß die Verfügbarkeit des Netzes möglichst hoch ist, für dies zu sorgen ist die zentrale Aufgabe des Fehlermanagements.

Um die Verfügbarkeit hoch zu halten, müssen Fehler möglichst schnell erkannt und behoben werden. Bei Netzen mit Dienstgütegarantien sind Verstöße gegen diese auch als Fehler zu werten.

Da ein Netz im Fehlerfall seine Dienste oder Dienstgüten nicht erbringen kann, gehen Einnahmen verloren. Das Kriterium *Repair Delay* gibt die Zeit für die Wiederherstellung von Diensten und Dienstgüten an.

Leistungsmanagement Beim Leistungsmanagement versucht man ein möglichst gutes Funktionieren eines Netzes zu erreichen.

Um die Kosten für das Equipment möglichst gering zu halten, soll dieses möglichst gut genutzt werden. Die Nutzung des Equipments soll anhand der für die Übertragung wichtigen Ressourcen gemessen werden:

- Bandbreite
- Speicher
- Verarbeitungsleistung

Für jede Ressource führen wir ein Kriterium ein: *Bandwidth*, *Memory* und *Processing Power*. Diese Kriterien sollen den Bedarf an diesen Ressourcen für die Dienstgütebereitstellung ausdrücken.

Eine Dienstgütebereitstellung ist mit der Reservierung von Ressourcen verbunden. Um Ressourcen effizient zu nutzen, sollten sie möglichst schnell freigegeben werden, wenn sie nicht mehr gebraucht werden. Das Kriterium *Resource Release Delay* gibt die Zeit an, die für das Freigeben der Ressourcen benötigt wird.

Abrechnungsmanagement Da das Bereitstellen und Unterhalten eines Netzes mit Kosten verbunden ist, möchte der Netzbetreiber diese Kosten auf die Nutzer des Netzes verteilen. Wie die Kosten verteilt werden, wird vom Netzbetreiber festgelegt, das Abrechnungsmanagement hat nun die Aufgabe alle Maßnahmen, die für die Durchführung dieser Verteilungspolitik notwendig sind, durchzuführen.

Es sollen Kriterien für den Vergleich von Technologien für Quality of Service gefunden werden. Diese Technologien können unterschiedlich gut geeignet für ein Abrechnungssystem und eine Abrechnungspolitik sein. Je nach Eignung wird der Aufwand für das Abrechnungsmanagement variieren. Da ausschließlich Technologien ohne ein Abrechnungssystem betrachtet werden, können für das Abrechnungsmanagement kaum Aussagen getroffen werden. Daher soll hier auf ein Kriterium verzichtet werden.

Sicherheitsmanagement Das Sicherheitsmanagement soll eine Mißnutzung des Netzes vermeiden, d.h. es muß der Zugriff auf Daten und Kommunikationsressourcen kontrolliert werden.

In der Kategorie Protection des Dienstnutzers wurden schon Kriterien gefunden, die die Sicherheit eines Kommunikationsdienstes beschreiben. Damit diese Kriterien erfüllt werden, muß bei der Konfiguration des Netzes gesorgt werden, deshalb soll hier auf ein Kriterium verzichtet werden.

Damit ergibt sich der Kriterienkatalog aus Abbildung 49.

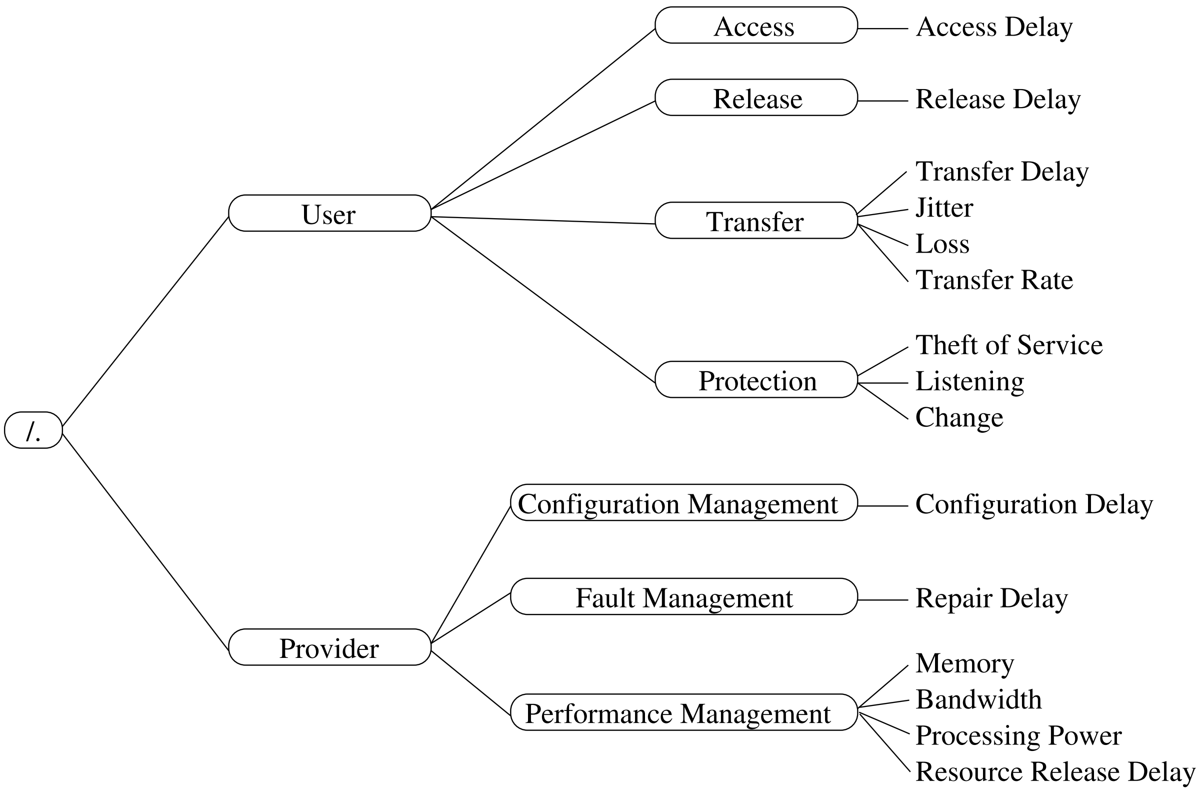

Abbildung 49: Kriterienkatalog

5 Anwendung des Kriterienkatalogs

In diesem Abschnitt wird der Kriterienkatalog aus Kapitel 4 beispielhaft auf ausgewählte Technologiekombinationen mit Dienstgüteunterstützung angewandt. Es werden die Technologien IntServ/RSVP und DiffServ mit den Netztechnologien Sonet/SDH, ATM, Ethernet kombiniert und verglichen. Die Wahl von IntServ/RSVP oder DiffServ als konstante Technologie und Variation der darunterliegenden Netztechnologie zeigt die Unterschiede, die durch die Netztechnologie entstehen (siehe Abbildungen 50 und 51). Der Vergleich

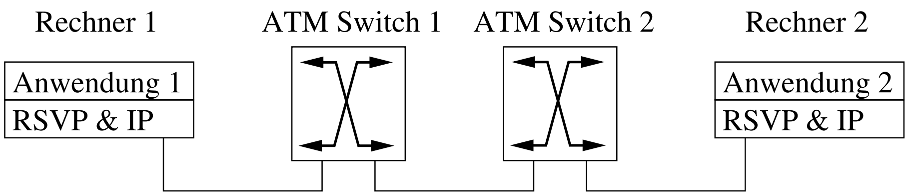

Abbildung 50: ATM-Netz mit RSVP

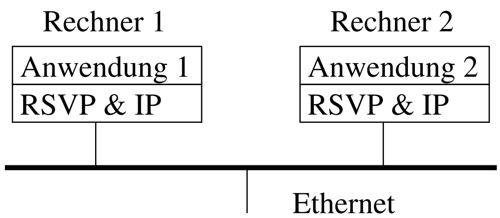

Abbildung 51: Ethernet mit RSVP

von DiffServ und IntServ/RSVP unter Verwendung der gleichen Netztechnologie zeigt den Unterschied zwischen IntServ/RSVP und DiffServ (siehe Abbildung 50 und 52). Ein letztes

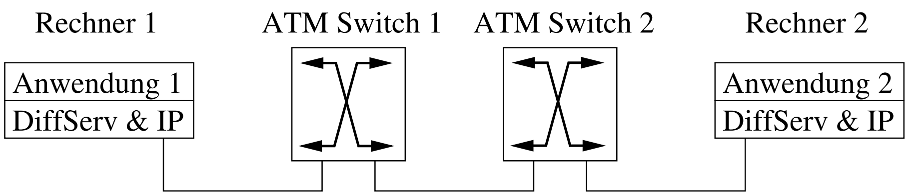

Abbildung 52: ATM-Netz mit DiffServ

Beispiel soll zeigen, wie die Entwicklungen IntServ/RSVP und DiffServ zusammenarbeiten können. Hier wird der Einfluß der Netztechnologien der OSI-Schicht 1 und 2 außer Acht gelassen (siehe Abbildung 53).

Die folgenden Abschnitte folgen dem selben Aufbau. Zuerst wird erläutert, wie die Entwicklungen von Schicht 3 und 4 auf die Schichten 1 und 2 aufsetzen, als nächstes wird der Kriterienkatalog auf dieses Beispiel angewandt.

5.1 IntServ/RSVP über Sonet/SDH

Die Sonet/SDH-Technologie ermöglicht eine duplex Punkt-zu-Punkt Verbindung fester Bandbreite zwischen zwei IP-Geräten. Für eine Übertragung von OSI-Schicht 4 Protokoll-

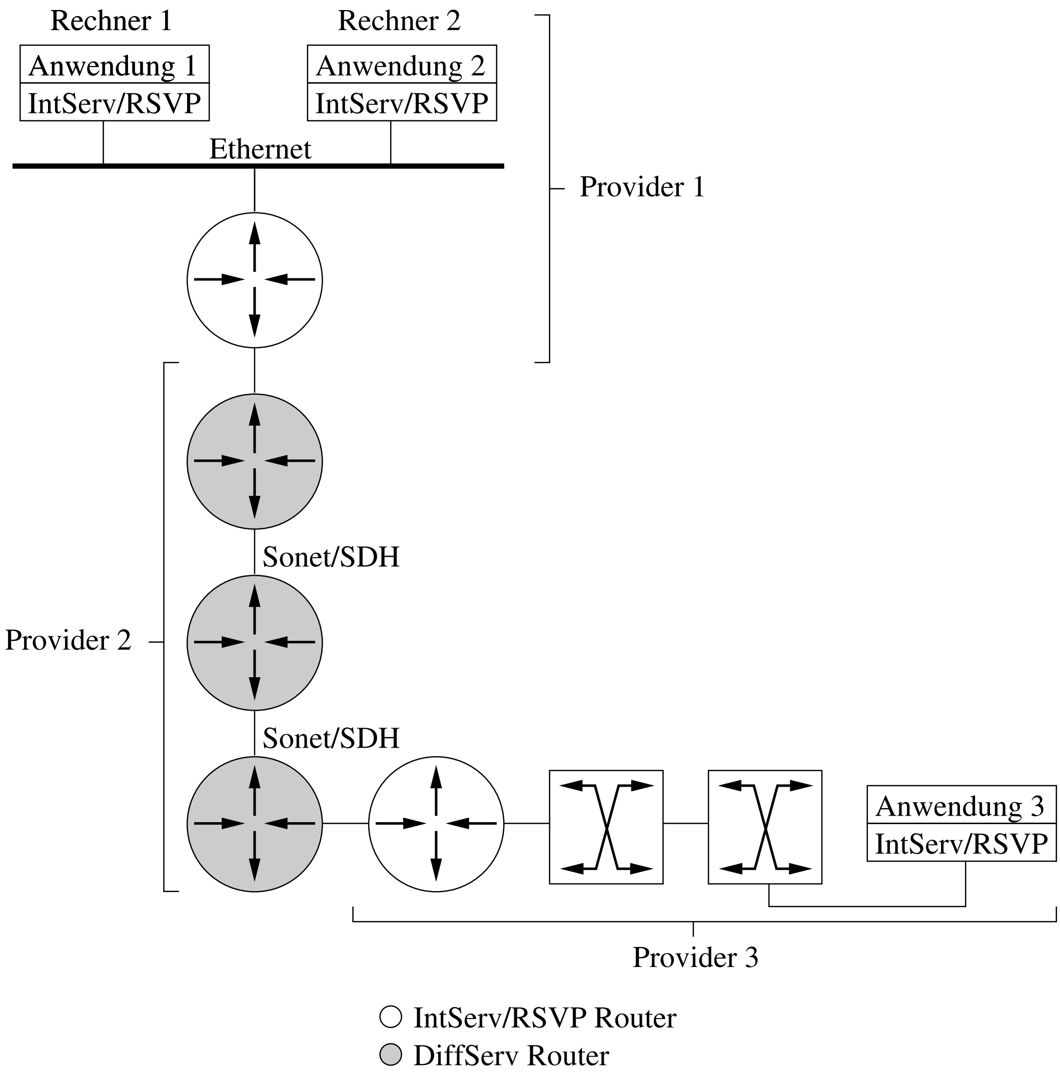

Abbildung 53: Netz mit IntServ/RSVP und DiffServ

PDUs werden diese in den Payload-Block des SDH-Frames geschrieben (siehe Abbildung 54). Die PDUs im Payload-Block kommen in einem Bytestrom beim Empfänger an. Dieser muß den Anfang und das Ende einer PDU erkennen, damit er die PDU aus dem Bytestrom herauslösen kann. Zu diesem Zweck wird ein HDLC-ähnliches Framing [Simp 94b][Trillium 97] verwendet. Der Anfang und das Ende werden mit dem Flag 01111110 gekennzeichnet. Die anderen Felder dieses Frames, mit Ausnahme der Prüfsumme, werden nicht benötigt. Innerhalb dieses Frames befindet sich eine PDU des *Point-to-Point Protocols* (PPP) [Simp 94a] (siehe Abbildung 55, grau HDLC-PDU und weiß PPP-PDU). Die Aufgaben die PPP erfüllt, wird durch folgende Hauptkomponenten bestimmt:

- Einer Methode für das Verpacken von Paketen unterschiedlicher OSI-Schicht 3 Protokolle.

- Ein Link Control Protocol (LCP) für die Einrichtung, die Konfiguration und den Test der Data Link-Verbindung.
  Mit dem LCP kann z.B. die maximale Paketgröße, das Authentifikationsverfahren

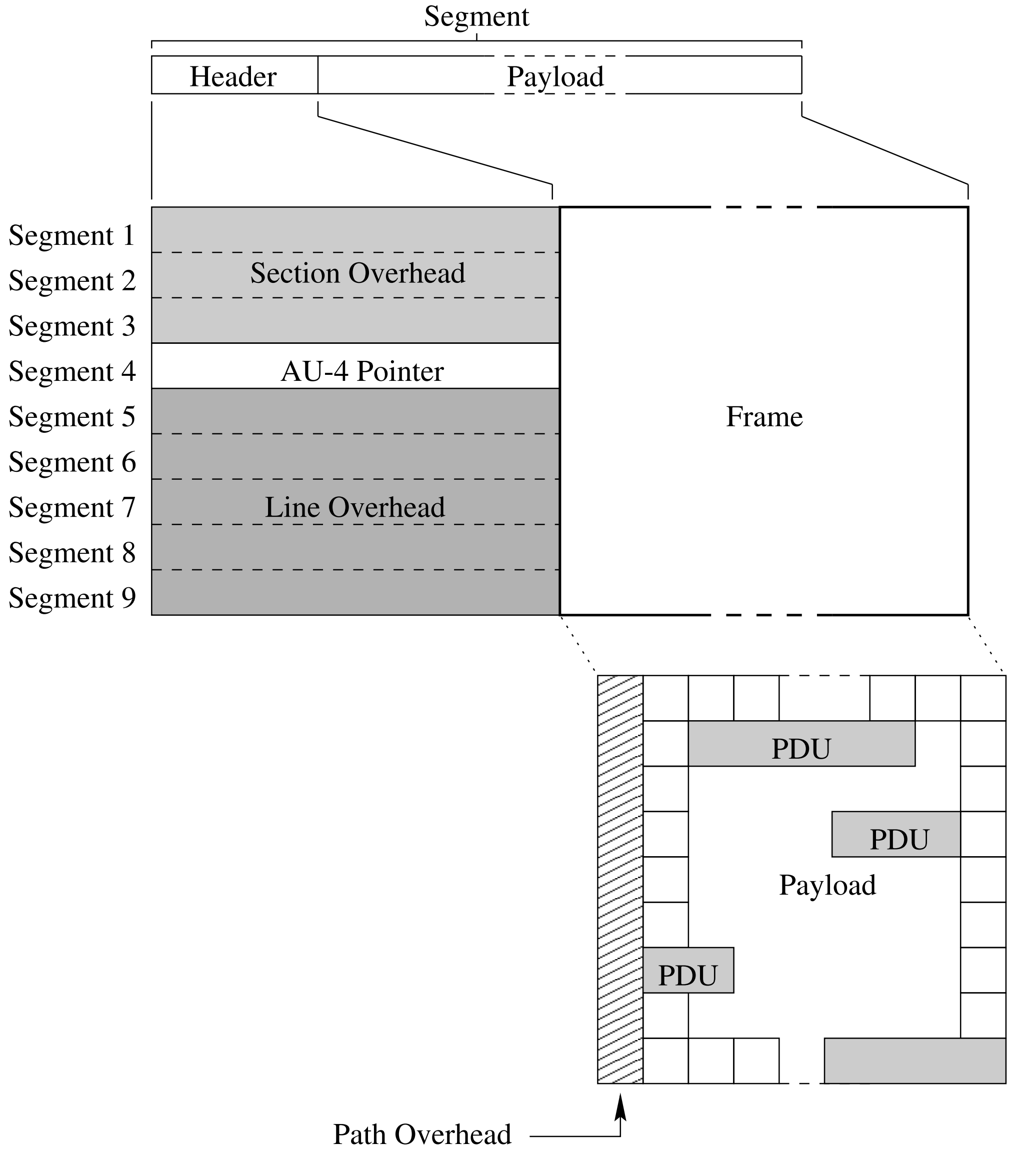

Abbildung 54: OSI-Schicht 4 Protokoll-PDUs im Payload-Block

Flag	Address	Control	Protocol Id	Information	Padding	FCS	Flag
01111110	11111111	00000011	1 or 2 Octets	variable	variable	2 or 4 Octets	01111110

Abbildung 55: HDLC/PPP-Frame

aber auch ein Kompressionsverfahren für die Felder Address und Control festgelegt werden.

- Eine Familie von Network Control Protocols (NCP), die die verschiedenen Network Layer-Protokolle einrichten und konfigurieren.
  Das NCP für IP ist Internet Protocol Control Protocol (IPCP) [McGr 92], es ermöglicht z.B. eine dynamische IP-Adressenvergabe beim Verbindungsaufbau.

Eine PPP-PDU kann ein OSI-Schicht 3 Protokoll, ein LCP- oder ein NCP-PDU enthalten, durch das Feld Protokoll-ID wird die Zugehörigkeit zu diesen drei Bereichen bestimmt.

Tabelle 10 zeigt einige dieser Werte [McGr 92][Simp 94a][RePo 94].

Wert	Protokoll
94	Internet Protocol
32801	Internet Protocol Control Protocol
49185	Link Control Protocol

Tabelle 10: ProtocolId-Werte

Der Protokoll-Stack für die Übertragung über Sonet/SDH sieht in RSVP-fähigen-Geräten wie in Abbildung 56 aus.

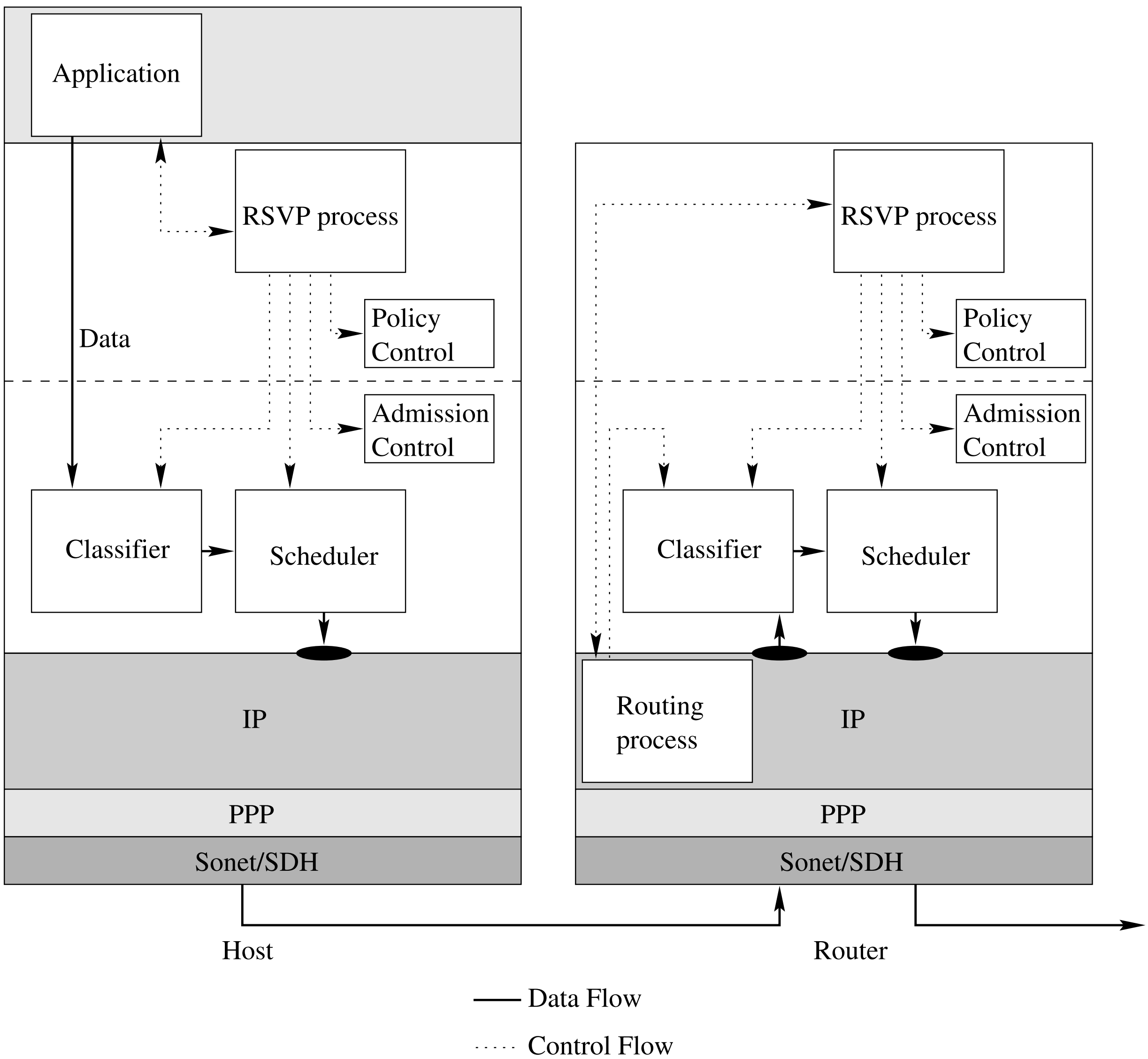

Abbildung 56: IntServ/RSVP über Sonet

In den nächsten Abschnitten wird untersucht, ob und wie die IntServ-Dienste über/SDH Sonet übertragen werden können.

5.1.1 Controlled-Load Service

Der Controlled-Load Service soll in etwa die Dienstgüte besitzen, die ein Netz unter geringer Last zeigt. Eine Anwendung, die den Controlled-Load Service verwendet, kann folgendes annehmen:

- Ein hoher Prozentsatz der gesendeten Pakete erreicht den Empfänger.
- Ein hoher Prozentsatz der empfangenen Pakete überschreitet nicht wesentlich die minimale Transportverzögerung.

Um diese beiden Bedingungen einzuhalten sollte ein Netzelement dafür sorgen, daß es nicht sehr häufig zu größeren Verzögerungen durch den Aufenthalt in Warteschlangen (Queuing Delay) und Verlusten aufgrund von Staus (Congestion Loss) kommt.

Treffen nun mehrere CLS-Pakete gleichzeitig an einem Netzelement für einen Ausgangsport ein, so kommt es zu Stauungen (siehe schwarze Blöcke in Abbildung 57). Damit es

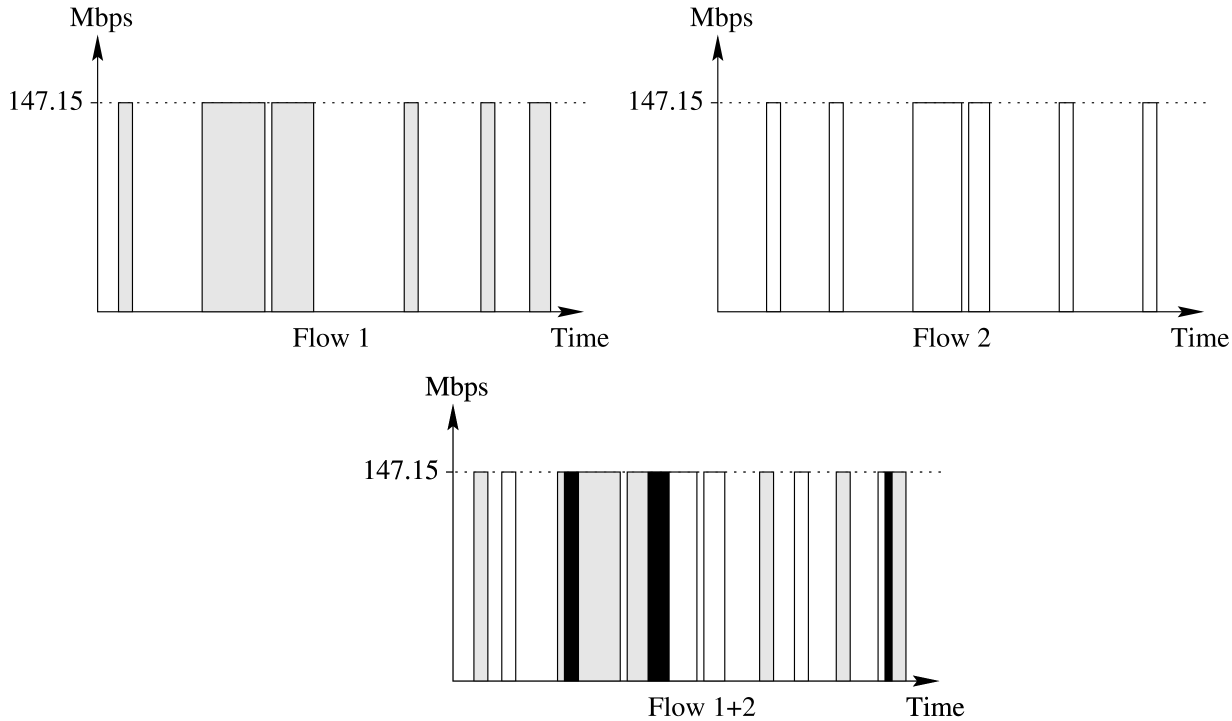

Abbildung 57: Flußbeispiel 1

nur selten größere Stauungen gibt, wird die Bandbreite für die CLS-Flüsse, vom Admission Control verwaltet. Dies setzt die Wahrscheinlichkeit herunter, daß sich zwei Pakete überschneiden können. Zu Überschneidungen kann es nur kommen, wenn mehrere Quellen für die CLS-Flüsse in einem Element existieren, da die CLS-Pakete auf der Leitung sequentiell übertragen werden. In Routern sind die Quellen die Eingangsports. Bei Endgeräten sind dies die Anwendungen. Nun kann es vorkommen, daß die Quellen immer gleichzeitig ihre CLS-Pakete liefern. Stauungen sind somit, unabhängig von der Übertragungsrate der Quellen, unvermeidlich (siehe Abbildung 58). Die Frage ist also, kann man einen CLS bei der Existenz mehrerer Quellen erreichen? Die Antwort liegt in der Interpretation der minimalen Übertragungszeit.

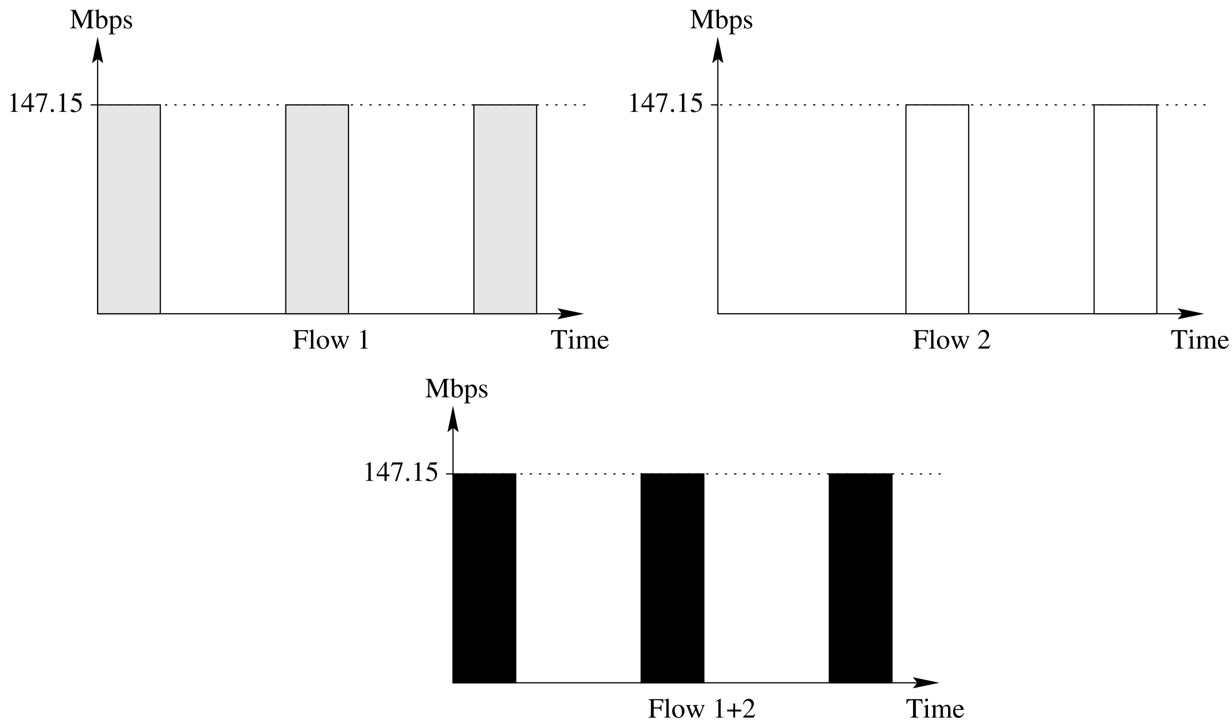

Abbildung 58: Flußbeispiel 2

1. Die Minimale Übertragungszeit ist die tatsächliche minimale Übertragungszeit. CLS-Pakete werden bei Sonet/SDH mit der Übertragungsrate des Mediums transportiert. Die minimale Übertragungszeit resultiert aus dieser Übertragungsrate ohne irgendwelche Verzögerungen aufgrund von Stauungen.

2. Die Minimale Übertragungszeit ist die Übertragungszeit eines Paketes mit der Token Bucket Rate. Ein CLS-Fluß reserviert sich einen Anteil der Bandbreite (TBR) des Mediums. Er betrachtet das Medium als einen Kanal mit dieser Bandbreite und nicht als einen Kanal mit der vollen Bandbreite.

Die zweite Interpretation der minimalen Bandbreite ist mit dem CLS zu verwenden, obwohl dies nicht explizit im Standard [Wroc 97b] verwerkt ist.

Die Admission Control kann prinzipiell auf zwei Arten feststellen, ob ein weiterer CLS-Fluß von Router und Leitung unterstützt wird unter der Voraussetzung, daß die bestehenden Flüsse ihren Dienst beibehalten können.

- **Static Admission Control**
  Die Entscheidung wird anhand der Charakteristik des Flusses (`FLOWSPEC`) vorgenommen. Dieser Ansatz ist bei wenigen Flüssen oder Flüssen deren Verhalten stark variiert geeignet. Hier orientiert man sich an dem schlechtesten Fall, der mit angegebenen Charakteristiken entstehen kann.

- **Measurement-based Admission Control**
  Die Entscheidung wird anhand der Beobachtung des CLS-Verkehrs vorgenommen. Man schließt hier von der aktuellen Verwendung der Ressourcen auf die zukünftige. Dies ist natürlich nur sinnvoll, wenn die Flüsse ihr Verhalten kaum ändern und

bei mehreren Flüssen, da es dann eher wahrscheinlich ist, daß sich Änderungen gegenseitig aufheben können. Dieses Verfahren erlaubt eine bessere Ausnutzung der Ressourcen.

Es ist auch eine Admission Control Implementierung denkbar, die sich den Bedingungen anpaßt und zwischen den beiden Alternativen wechselt.

Damit die Bedingungen auch in Anwesenheit des Best-Effort-Verkehrs erfüllt sind, kann ein Scheduler mit zwei Prioritäten (siehe Abbildung 59) eingesetzt werden. Dieser Scheduler wählt erst alle CLS-Pakete aus bevor ein BE-Paket genommen wird. Die Funktion dieses

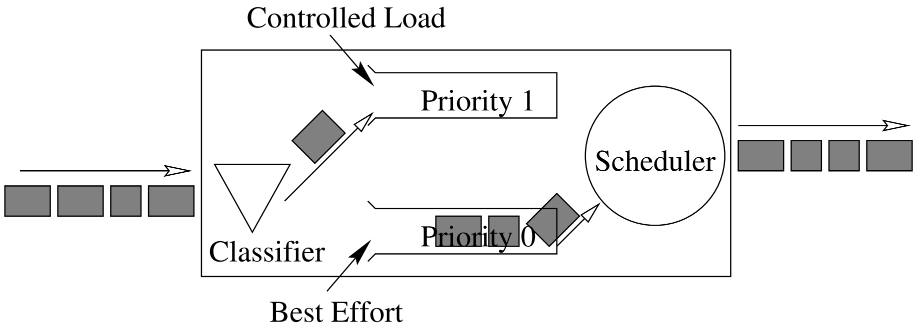

Abbildung 59: CLS mit Prioritätsscheduling

Scheduler ist nur korrekt, wenn sich alle CLS-Flüsse an ihren `FLOWSPEC` (siehe Abschnitt 2.3.2) halten.

5.1.2 Guaranteed Quality of Service

Der Guaranteed Service (GS) versucht den Dienst des *Fluid Model* nachzuahmen. Der Dienst des Fluid Model entspricht einer Leitung mit Bandbreite R zwischen Sender und Empfänger. Damit ergeben sich folgende Bedingungen an den GS-Dienst:

- Zugesicherte Bandbreite
- Maximale Übertragungsverzögerung
- Kein Verlust aufgrund von Stauungen (Congestion Loss)

Ein Fluß dem die Bandbreite R garantiert ist und dessen Bursts nicht größer als TBS sind hat eine maximale Übertragungsverzögerung von:

$$TransferDelay \leq \frac{TBS}{R} + MPL \qquad \text{mit:} \qquad R \geq TBR$$

MPL	Minimale Übertragungsverzögerung (Minimum Path Latency)
TBS	Maximale Größe eines Bursts (Token Bucket Size)
R	Übertragungsrate des Flusses (R)

Minimum Path Latency (MPL) ist die minimale Übertragungsverzögerung und $\frac{TBS}{R}$ die maximale Queuing Delay beim Auftreten eines Bursts.

In einem IP-Netz treten weitere Verzögerungen aufgrund von Queuing, Scheduling und Serialisierung auf, die zum Abweichen vom Fluid Model führen. Sie werden mit den folgenden Parametern beschrieben:

- **D**
  Der Wert D drückt die Verzögerung aus, die von der Bitrate R unabhängig ist.

- **C**
  Der Wert C drückt die Verzögerung aus, die von der Bitrate R abhängig ist.

Fehlerwert D In D wird z.B. die Verarbeitungsverzögerung in den IP-Geräten und die Verzögerung durch den Scheduler ausgedrückt. Der Scheduler bestimmt die Reihenfolge in der die Pakete gesendet werden. Durch die Existenz mehrere Flüsse können mehrere Pakete sendebereit sein, daher können andere Pakete dem GS-Paket eines Flusses vorgezogen werden, was zu einer weiterern Verzögerung und zum Abweichen vom Fluid Model führt. Damit eine maximale Übertragungsverzögerung eines Pakets zugesichert werden kann, darf der Scheduler nicht mehr als eine bestimmte Anzahl an Paketen diesem bevorzugen. Ist diese Anzahl unabhängig von der Übertragungsrate des Flusses, so übt sie Einfluß auf diesen Fehlerwert aus.

Fehlerwert C Der Fehlerwert C representiert eine Verzögerung, die über die durch das Fluid Model bestimmte hinaus geht. C ist von der Bitrate R in `FLOWSPEC` der Resv-Nachricht abhängig ist. Der Dienst des Fluid Model orientiert sich an einer bitweisen Übertragung der Daten. Bei Sonet/SDH werden Daten in Paketen übertragen, der Unterschied dieser beiden Ansätze wird mit dem Fehlerwert C ausgedrückt. Besitzt ein Fluß eine Leitung mit Bandbreite R und er schöpft diese Kapazität voll aus, so sieht die Übertragung wie im unteren Teil der Abbildung 60 aus. Bei Sonet/SDH erhält nicht jeder Fluß eine eigene Leitung, sondern die PDUs werden auf eine Leitung mit höherer Bandbreite gemultiplexed. Ein GS-Fluß erhält mit der Rate R Token für das Senden von Daten. Da erst mit dem Senden eines Pakets begonnen wird, wenn ein Token für das letzte Bit des Pakets vorliegt, muß das erste Bit eines Pakets $\frac{MTU}{R}$ (MTU ist die maximale Paketgröße) Sekunden warten bis es gesendet wird (siehe senkrechte Line in Abbildung 60). Dies ist

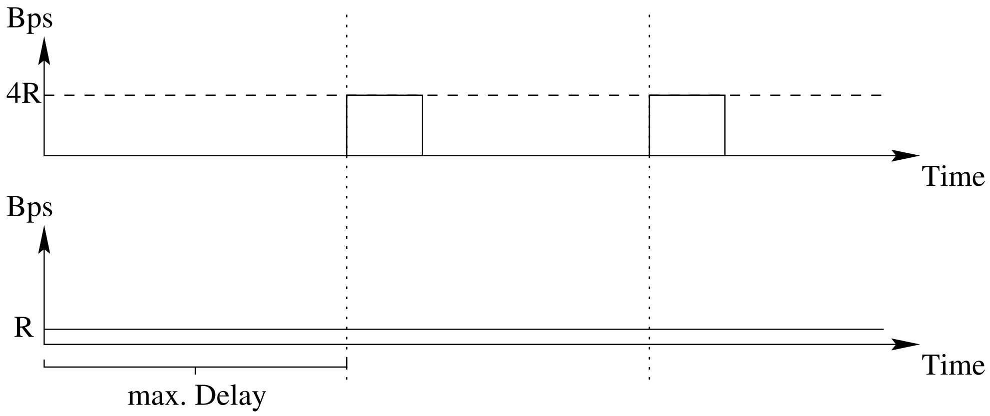

Abbildung 60: Paketierungsverzögerung für einen Fluß mit Bandbreite R

auch die maximale Verzögerung die Daten durch eine Paketübertragung erhalten können.

Wählt man eine größere Übertragungsrate für einen Fluß, dann reduziert sich die Verzögerung bis zum Senden des Pakets (vergleiche Abbildung 60 mit 61).

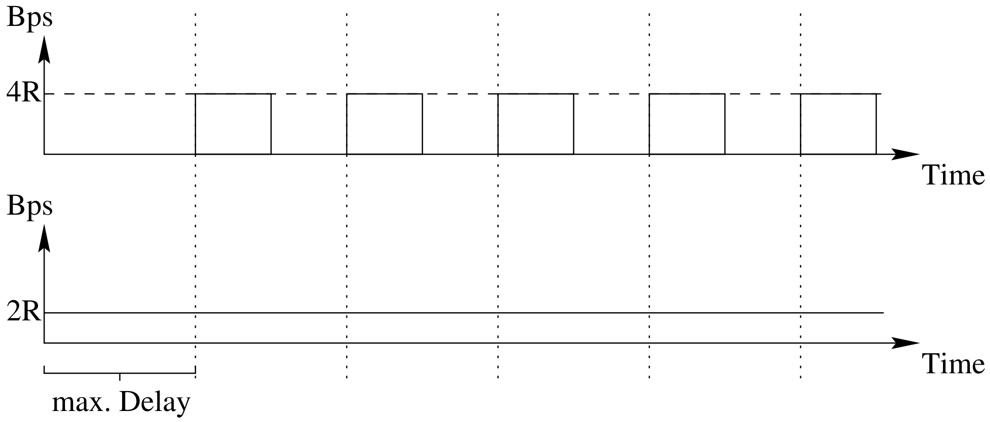

Abbildung 61: Paketierungsverzögerung für einen Fluß mit Bandbreite *2R*

Maximale Übertragungsverzögerung Mit den zusätzlichen Verzögerungen ergibt sich eine maximale Übertragungsverzögerung für einen Fluß mit Guaranteed Service zu:

$$TransferDelay \leq \frac{MBS}{R} + \frac{Ctot}{R} + Dtot + MPL$$

Ctot Die Summe aller Fehlerwerte C auf dem Pfad vom Sender zum Empfänger.
Dtot Die Summe aller Fehlerwerte D auf dem Pfad vom Sender zum Empfänger.

5.1.3 Anwendung des Kriterienkatalogs

Es folgt nun die Anwendung des Kriterienkatalogs aus Kapitel 4 auf die Technologiekombination IntServ/RSVP über Sonet/SDH. Mit f wird im folgenden ein Fluß bezeichnet, der durch das Tupel (Source IP Address, Source Port, Protocol, Destination Port, Destination IP Address) identifiziert wird. Der Fluß f wird mit folgenden Parametern durch einen Empfänger eingerichtet:

- Token Bucket Rate (TBR)
  Die Token Bucket Rate gibt die maximale Übertragungsrate an, mit der über einen längeren Zeitraum gesendet werden darf (siehe Abschnitt 2.3.2).

- Token Bucket Size (TBS)
  Die Token Bucket Size gibt die maximale Datenmenge an, die mit der Peak Data Rate gesendet werden darf.

- Peak Data Rate (PDR)
  Die Peak Data Rate gibt die maximale kurzfristige Übertragungsrate an.

- Minimum Policed Unit (MPU)
  Alle Datenmengen, die kleiner als die Minimum Policy Unit sind, werden behandelt als hätten sie die mit MPU spezifizierte Größe.

- Maximum Packet Size (MPS)
  Die maximale Paketgröße die erlaubt ist.

- Minimum Path Latency (MPL)
  Die minimale Übertragungszeit.

- Rate (R)
  Die zugesicherte Übertragungsrate für einen Fluß.

- Slack Term (ST)
  Definiert die Verzögerung, die ein Empfänger zusätzlich zu best möglichen maximalen Übertragungszeit erlaubt.

Im Fall eines Mulitcast-Flusses (d.h. Destination IP Address ist eine Multicast-Adresse) können diese Parameter für jeden Empfänger unterschiedliche Werte haben. Durch einen Index wird der Empfänger identifiziert, der den Wert eines Parameters bestimmt. (z.B. ist TBR_e die TBR des Empfängers e).

Die Kriterien werden in zwei Schritten angewandt:

1. Im ersten Schritt werden die Kriterien für IntServ/RSVP unabhängig von der Netztechnologie angewandt. Dies erfolgt nur einmal für jede Technologie der OSI-Schicht 3 und 4.

2. Im zweiten Schritt werden die Änderungen aufgrund der Netztechnologie bestimmt.

Anwendung des Kriterienkatalogs auf IntServ/RSVP unabhängig von der Netztechnologie:

User→Access→Access Delay	
Voraussetzungen:	Ein Fluß nutzt Guaranteed Service oder Controlled-Load Service
Kriterium:	Eine maximale Zugangszeit kann nicht angegeben werden, da RSVP-Nachrichten mit der BE-Dienstgüte transportiert werden. Der Transport mit der BE-Dienstgüte garantiert weder eine maximale Übertragungszeit für RSVP-Nachrichten noch deren Übertragung überhaupt. Die minimale Zugangszeit ist durch die minimale *Round Trip Delay* (Die Round Trip Delay ist die Zeit, die Daten vom Sender zum Empfänger und wieder zurück benötigen) nach unten beschränkt. Hierzu kommt noch die Verarbeitungszeit in den RSVP-Prozessen. Die Zugangszeit, falls keine RSVP-Nachrichtenverluste vorkommen, wird ca. in der Größenordnung von Dezisekunden liegen.
Voraussetzungen:	Ein Fluß nutzt Best Effort
Kriterium:	Die Zugangsverzögerung ist Null

User→Release→Release Delay	
Voraussetzungen:	keine
Aussage:	Der Zugang ist mit dem Erhalt einer Teardown-Nachricht von einer Anwendung beim RSVP-Prozeß beendet. Diese Nachricht wird z.B. mit klassischen Interprozeßkommunikationsmechanismen übertragen und ist bei den heutigen Rechnern vernachlässigbar gering.

User→Transfer→Transfer Delay	
Voraussetzungen:	Ein Fluß f verwendet Guaranteed Service
Aussage:	Die maximale Übertragungsverzögerung ist beschränkt. Im Vergleich zu DiffServ kann IntServ/RSVP unter ähnlichen Bedingungen niedrigere obere Schranken für die Übertragungsverzögerung garantieren (siehe 5.3.4). Die minimale Übertragungsverzögerung ist durch *MPL* beschränkt.
Voraussetzungen:	Ein Fluß f verwendet Controlled-Load Service
Aussage:	Die maximale Übertragungsverzögerung ist nicht beschränkt. Die minimale Übertragungsverzögerung ist durch MPL beschränkt.
Voraussetzungen:	Ein Fluß verwendet Best Effort
Aussage:	Die maximale Übertragungsverzögerung ist nicht beschränkt. Die minimale Übertragungszeit ist durch MPL beschränkt.

User→Transfer→Jitter	
Voraussetzungen:	Ein Fluß f verwendet Guaranteed Service
Aussage:	Der maximale Jitter ist beschränkt. Aus der Tatsache, daß IntServ/RSVP in der Lage ist niedrigere maximale Übertragungsverzögerungen als DiffServ zu liefern, wird geschlossen, daß auch der maximale Jitter niedriger als bei DiffServ ist.
Voraussetzungen:	Verwendung des Controlled-Load Service
Aussage:	Der maximale Jitter ist nicht beschränkt.
Voraussetzungen:	Ein Fluß verwendet Best Effort
Aussage:	Der maximale Jitter ist nicht beschränkt.

User→Transfer→(Congestion) Loss	
Voraussetzungen:	Ein Fluß f verwendet Guaranteed Service
Aussage:	Der Verlust aufgrund von Stauungen ist Null
Voraussetzungen:	Ein Fluß f verwendet Controlled-Load Service
Aussage:	Der maximale Verlust ist niedrig. Der minimale Verlust kann Null sein.
Voraussetzungen:	Ein Fluß verwendet Best Effort Service
Aussage:	Der maximale Verlust kann hundert Prozent sein. Der minimale Verlust kann Null sein.

User→Transfer→Transfer Rate	
Voraussetzungen:	Ein Fluß f verwendet Guaranteed Service
Aussage:	Die maximale Übertragungsrate ist das Maximum der TBR aller Empfänger des Flusses. Die minimale Übertragungsrate ist die vom Empfänger selbst reservierte Übertragungsrate (TBR_e).
Voraussetzungen:	Ein Fluß f verwendet Controlled-Load Service
Aussage:	Die maximale Übertragungsrate ist das Maximum der TBR aller Empfänger des Flusses. Die minimale Übertragungsrate ist TBR.
Voraussetzungen:	Ein Fluß verwendet Best Effort
Aussage:	Die maximale Übertragungsrate ist die verfügbare Übertragungsrate des Mediums Die minimale Übertragungsrate ist Null.

User→Protection→Theft of Service	
Voraussetzungen:	keine
Aussage:	IntServ/RSVP bietet Schutz vor dem Diebstahl einer Dienstgüte RSVP stellt eine Möglichkeit bereit, daß sich der Nutzer einer Dienstgüte ausweisen muß. Diesen Ausweis stellt das Objekt `POLICY_DATA` dar, dessen Echtheit mit dem Objekt `INTEGRITY` sichergestellt ist.

User→Protection→Listening	
Voraussetzungen:	keine
Aussage:	Schutz vor dem Abhören ist möglich Das Abhören eines Flusses kann mit IPSEC verhindert werden [Atki 95a] [Atki 95c]. Da dies aber den TCP- oder UDP-Header verschlüsselt, kann das Traffic Control auf die Objekte Protocol, Source Port und Destination Port in diesen Headern nicht zugreifen. In [BeO' 97] werden Möglchkeiten bereitgestellt, dieses Problem zu umgehen. Daher können wir sagen, daß ein Schutz vor dem Abhören, falls beabsichtigt, gegeben ist.

User→Protection→Change	
Voraussetzungen:	keine
Aussage:	Schutz vor unbemerkten Veränderung ist gegeben. Mit [Atki 95b] ist ein Verfahren gegeben, die Veränderung von verschlüsselten oder unverschlüsselten Daten zu erkennen.

Provider→Configuration Management→Configuration Delay	
Voraussetzungen:	keine
Aussage:	Die Konfiguration für IntServ/RSVP umfaßt das Setzen von Parametern des Traffic Control, des Admission Control und des Policy Control. Diese Arbeit muß im Idealfall nur für die Inbetriebnahme einer Komponente (Router und Host) erfolgen.

Provider→Fault Management→Repair Delay	
Voraussetzungen:	Der Fehler kann umgangen werden.
Aussage:	IntServ/RSVP besitzt ein Verfahren, um Fehler (z.B. Routerausfall oder Leitung unterbrochen) zu umgehen. Dieses Verfahren stellt eine Reservierung über einen alternativen Pfad zum Empfänger her.

Provider→Performance Management→Bandwidth	
Voraussetzungen:	keine
Aussage:	Von der verfügbaren Bandbreite des Übertragungsmediums werden ca. 60 Bit/s für die Aufrechterhaltung eines IntServ-Flusses verwendet. DiffServ benötigt keine Bandbreite für das Aufrechterhalten von Flüssen.

Provider→Performance Management→Memory	
Voraussetzungen:	keine
Aussage:	Der Speicherbedarf ist bei IntServ/RSVP größer als bei DiffServ. Bei IntServ/RSVP wird für jeden Fluß ein Zustand im RSVP-fähigen Gerät (Host und Router) erzeugt. Die Größe des Zustands ist von der Art des Flusses (Unicast oder Multicast) und auch von der Implementierung der RSVP-Prozesse abhängig. Die Größe eines Zustand wird aber $>$ 100 Byte sein ([BrZh 97]). Der Speicherbedarf für Puffer ist auch größer als bei DiffServ einzuschätzen.

Provider→Performance Management→Processing Power	
Voraussetzungen:	keine
Aussage:	Die Verarbeitungsleistung, die bei IntServ/RSVP erbracht werden muß, ist größer einzuschätzen als bei DiffServ. Neben der eigentlichen Aufgabe, das Weiterleiten von Nachrichten, müssen in den RSVP-fähigen Geräten (Host und Router) die RSVP-Nachrichten bearbeitet werden. Die RSVP-Nachrichten werden nicht nur zum Auf- und Abbau einer Reservierung, sondern auch zu deren Weiterbestehen benötigt. Zu diesem Zweck werden in regelmäßigen Abständen (ca. 30 Sekunden [BZB+ 97]) Path- und Resv-Nachrichten gesendet. Die Verarbeitungsleistung pro Datennachricht ist auch höher als bei DiffServ einzuschätzen.

Provider→Performance Management→Resource Release Delay	
Voraussetzungen:	keine
Aussage:	Die maximale Zeit für das Freigeben von Ressourcen ist beschränkt. Die Freigabe der Ressourcen erfolgt spätestens nach Ablauf des Timers für die Lebenszeit des Reservierungszustands in einem RSVP-Prozeß. Die Lebenszeit für einen Timer ist < 2 Minuten (Wert nach [BZB+ 97]). Da die Timer der Reservierungen eines Flusses nacheinander ablaufen können, kann sich die Freigabe der letzten Ressourcen einige Minuten hinziehen. Die minimale Freigabezeit der Ressourcen ist durch MPL beschränkt. Beendet der Empfänger den Zugang, dann werden mit dem Erreichen der Teardown-Nachricht beim Sender die letzten Ressourcen freigegeben.

Änderungen aufgrund der Netztechnologie:

Provider→Performance Management→Bandwidth	
Voraussetzungen:	keine
Aussage:	Von der verfügbaren Bandbreite des Übertragungsmediums (ca. 95% der Übertragungsrate des Mediums [Trillium 97]) werden ca. 60 Bit/s für die Aufrechterhaltung eines IntServ-Flusses verwendet. DiffServ benötigt keine Bandbreite für das Aufrechterhalten von Flüssen.

5.2 IntServ/RSVP über ATM

ATM als Infrastruktur für IntServ/RSVP bietet zwei Möglichkeiten [CBB+ 98]:

1. **Multiplexen auf statisch eingerichtete virtuelle Verbindungen**
   ATM virtuelle Verbindungen werden zwischen den IP-Geräten eingerichtet. Ein Scheduler bestimmt die Reihenfolge der PDUs, die über die virtuelle Verbindung übertragen werden. Bei diesem Ansatz werden ATM virtuellen Verbindungen analog wie Sonet/SDH Punkt-zu-Punkt-Verbindungen verwendet.

2. **Virtuelle Verbindungen für RSVP-Flüsse**
   Für RSVP-Flüsse werden eigene virtuelle Verbindungen verwendet (siehe Abbildung 62), diese werden je nach Bedarf auf- und abgebaut.

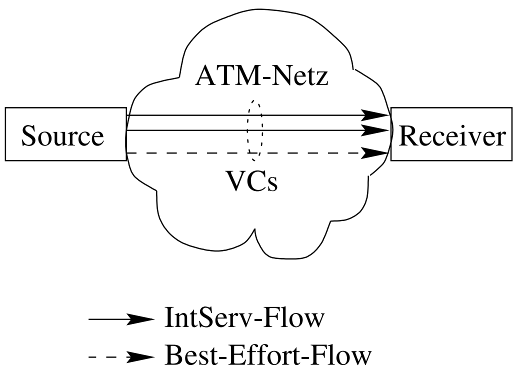

Abbildung 62: IntServ/RSVP über SVCs

Hier ein paar Vorteile dieser Ansätze [CBB+ 98].
Vorteile des ersten Ansatzes:

- **Einfache Lösung**
  Die Lösung von IntServ/RSVP über ATM ist analog zu der von IntServ/RSVP über Sonet/SDH. Es sind nur geringere Anpassungen an die Übertragungstechnik nötig.

- **Geringere Verbindungsaufbauzeit**
  Da die virtuellen Verbindungen bereits vorhanden sind, muß keine weitere Verzögerung beim Aufbau eines IntServ-Flusses in Kauf genommen werden.

Vorteile des zweiten Ansatzes:

- **Dynamische Reservierung**
  Die Reservierungen im ATM-Netz orientieren sich am momentanen Bedarf.

- **Dienstgüte besser vorhersagbar**
  Durch die Verwendung einer virtuellen Verbindung für einen Fluß ist dessen Dienstgüte besser vorhersagbar. Beim ersten Ansatz erfolgt ein zweimaliges Multiplexen. Erst werden die PDUs verschiedener Flüsse auf eine virtuelle Verbindung übertragen und dann werden die ATM-Zellen unterschiedlicher Verbindungen auf das Medium übertragen. Beim zweiten Ansatz übernimmt ATM das Multiplexen (Scheduling) der Flüsse, das Traffic Control und das Admission Control (siehe Abbildung 63).

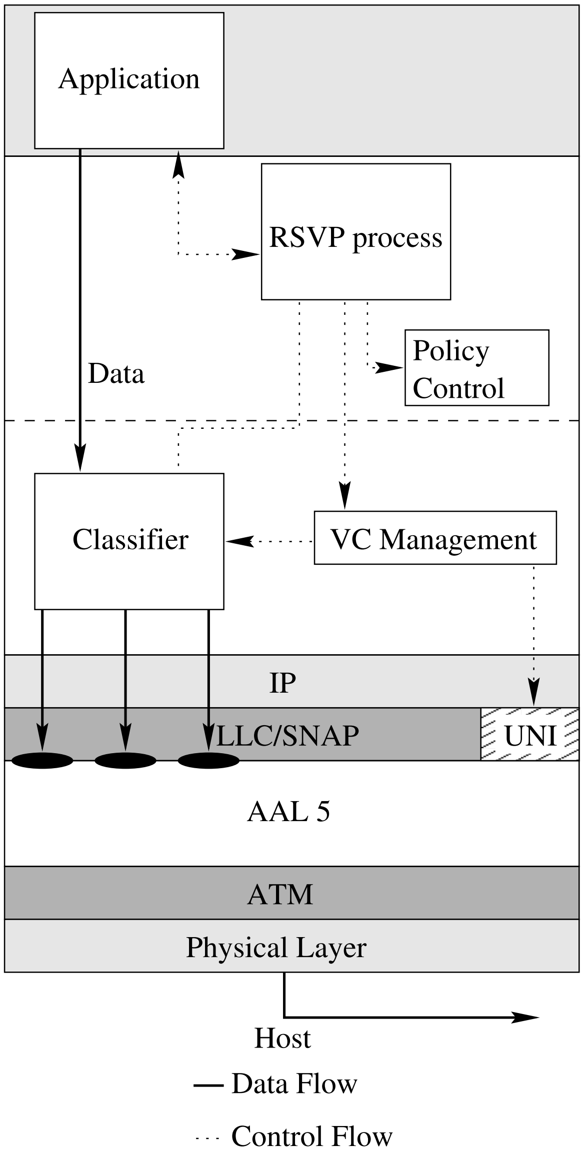

Abbildung 63: IntServ/RSVP im ATM-fähigen Sender

Der zweite Ansatz verlangt nach einer Infrastruktur, die es ermöglicht eine virtuelle Verbindung mit einer bestimmten Dienstgüte aufbauen zu können. Dafür muß aber zur IP-Adresse eines Empfangsgerätes die ATM-Adresse bekannt sein. Zur Lösung dieses Problems kann auf CLIP, LANE und MPOA zurückgegriffen werden. Diese werden in den nächsten drei Abschnitten vorgestellt.

5.2.1 Classical IP over ATM

Classical IP over ATM (CLIP) [Laub 94][Hals 96] bildet die logische Netzstruktur eines IP-Netzes in einem ATM-Netz nach. Hierfür werden die ATM-Endgeräte in Subnetze eingeteilt. Diese Subnetze können über Router, die ATM-Subnetze miteinander oder ATM-Subnetze mit Nicht-ATM-Subnetze verbinden, kommunizieren. Für die Adressverwaltung im ATM-Subnetz ist der ATM Address Resolution Protocol Server (ATMARP-Server) und der Multicast Address Resolution Server (MARS) [TaAm 97], eine Erweiterung des

ATMARP-Server, verantwortlich (siehe Abbildung 64). Jedes ATM-Gerät, daß zu einem

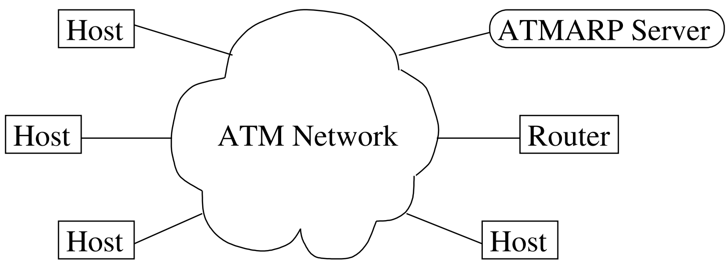

Abbildung 64: Logisches IP Subnetz mit ATM

ATM-Subnetz gehören soll, wird mit der ATM-Adresse des ATMARP-Servers des Subnetzes konfiguriert. Die ATM-Geräte teilen dem ATMARP-Server ihr (IP-Adress, ATM-Adress)-Paar mit. Für eine Kommunikation zwischen ATM-Geräten innerhalb eines Subnetzes wird die zu einer IP-Adresse gehörende ATM-Adresse des Kommunikationspartners beim ATMARP-Server erfragt. Mit dieser Information kann dann eine virtuelle Verbindung aufgebaut werden.

Ursprünglich war nur vorgesehen eine virtuelle Verbindung zwischen zwei Geräten zu schalten, über die alle Daten laufen sollten. Daher war es notwendig eine Demultiplex-Möglichkeit zwischen ATMARP- und IP-Paketen zu haben, Dies liefert der Logical Link Control/Subnetwork Access Protocol Header (LLC/SNAP-Header) [Hein 93] verpackt. Die Übertragung dieses Frames (LLC/SNAP und IP-Paket oder ATMARP-Paket) erfolgt dann mit der ATM Adaption Layer 5 (siehe Abbildung 65). Der LLC-Header entspricht dem des

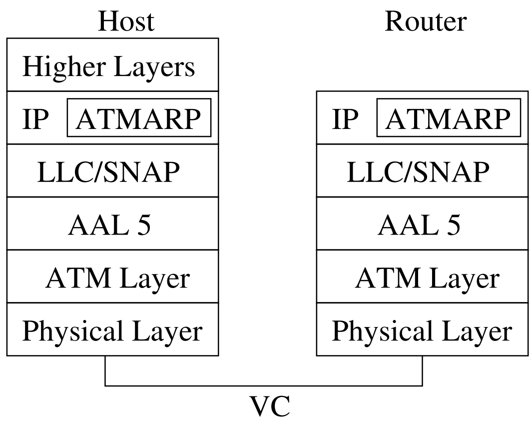

Abbildung 65: Protokollstack für Classical IP over ATM

IEEE 802.2 Standard (siehe Abbildung 41 in Abschnitt 3.3.1). Die Werte der einzelnen Felder sind bei CLIP fest vorgegeben. Der SNAP-Header besteht aus zwei Feldern, dem Organizationally Unique Identifier (OUI) und dem Protocol Identifier (PID). Der OUI gibt die Organisation an, die den PID-Wert festgelegt hat. Zusammen geben sie an, welchem Protokoll die SDU angehört (siehe Abbildung 66). Ein ATMARP-Paket hat den PID-Wert 0x08-06 und ein IP-Paket 0x08-00.

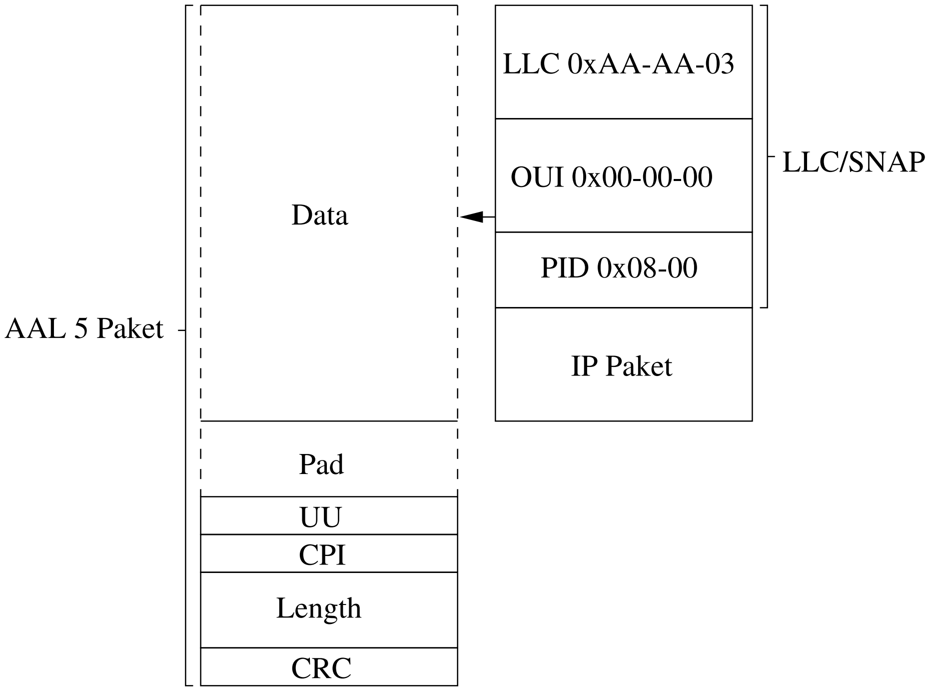

Abbildung 66: IP-Paket in AAL 5

5.2.2 LAN Emulation

LAN Emulation (LANE) [af- 97][ATM-LANE 99][Hals 96] wurde definiert, um ein Ethernet/802.3 oder ein Token Ring/802.5 LAN auf einem ATM-Netz zu emulieren. Da LANE auf der OSI-Schicht 2 operiert, kann jedes Schicht 3 Protokoll verwendet werden. Ein emuliertes LAN (ELAN) ist mit einem LAN-Segment vergleichbar, es kann über Bridges und Router mit anderen Segmenten oder Subnetzen verbunden werden. Um ein ELAN auf einem ATM-Netz zu implementieren werden drei Server verwendet (siehe Abbildung 67):

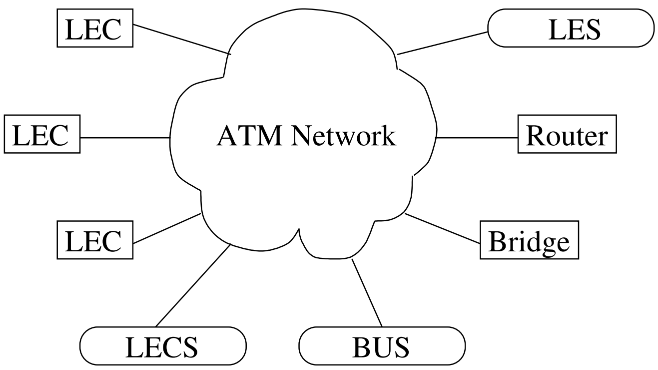

Abbildung 67: ATM LAN

- **LAN Emulation Configuration Server (LECS)**
  Ein ATM-Netz kann mehrere ELANs enthalten, ein oder mehrere LECSs haben die Aufgabe die LAN Emulation Clients (LECs) einer bestimmten Policy folgend den ELANs zuzuteilen.

- **LAN Emulation Server (LES)**
  Der LES implementiert die Kontrollfunktionen eines ELANs. Bei ihm können Unicast- und Multicast-MAC-Adressen registriert werden. Er wird befragt, um die MAC-Adresse einer ATM-Adresse zuzuordnen und damit eine virtuelle Verbindung zum Kommunikationspartner aufzubauen. Ab Version 2 können mehrere virtuelle Verbindungen mit bestimmter Dienstgüte errichtet werden. Ein ELAN besitzt nur einen LES.

- **Broadcast and Unknown Address Server (BUS)**
  Der BUS simuliert das gemeinsam genutzte Medium eines Ethernets oder Token Rings im ATM-Netz. Pakete, die an den BUS geschickt werden, werden von diesem an mehrere LECs gesendet.

5.2.3 Multiprotocol over ATM

Multiprotocol over ATM (MPOA) [ATM-MPOA 99] versucht den Nachteil von CLIP und LANE zu beseitigen. Da Pakete oder Frames bei CLIP und LANE den logischen Weg über Bridges und Router durchs ATM-Netz folgen, fällt mehrmals die Aufgabe des Zusammenfügens der ATM-Zellen zu Paketen oder Frames an. Dies erhöht den Aufwand im Netz und verschlechtert die Dienstgüte einer Übertragung. Außerdem kann der Weg über den Router zum Engpaß im Netz werden. MPOA ermöglicht es, daß ATM-Geräte innerhalb eines ATM-Netzes aus unterschiedlichen Subnetzen eine virtuelle Verbindung (Short-Cut) zwischen einander schalten können und somit direkt miteinander kommunizieren können (siehe Abbildung 68). Die zwei Bestandteile von MPOA sind:

- **MPOA Client (MPC)**
  Der MPC ist in jedem ATM-Gerät, daß einen Short-Cut schalten will. Mit ihm kann eine Anfrage an einen MPOA Server nach der ATM-Adresse des dem Empfänger am nächsten liegenden ATM-Geräts gestellt werden.

- **MPOA Server (MPS)**
  Der MPS Anwortet auf die Anfragen der MPCs. Zur Ermittlung der Adresse wird das *Next Hop Resolution Protocol* (NHRP) [LKP$^+$ 98] verwendet.

Diese drei Entwicklungen ermöglichen es IntServ/RSVP virtuelle Verbindungen auf- und abzubauen. Für den Einsatz von IntServ/RSVP in einem ATM-Netz gibt es aber noch einige Probleme zu lösen.

5.2.4 VC-Management

Werden virtuelle Verbindungen für jeden IntServ-Fluß eingerichtet, müssen zwei Probleme, die aufgrund der Unterschiede von ATM und IntServ/RSVP auftreten, gelöst werden:

- **Dynamische Reservierungsänderungen**
  RSVP ermöglicht es, daß eine bestehende Reservierung geändert werden kann, bei ATM ist das nicht so einfach.

- **Heterogene Empfänger**
  RSVP ist Empfänger orientiert, d.h. die Reservierung wird vom Empfänger vorgenommen, bei ATM ist es genau umgekehrt. Dies birgt ein Problem bei Multicast-Verbindungen, die zwar auch ATM erlaubt, jedoch bekommt hier jeder Empfänger

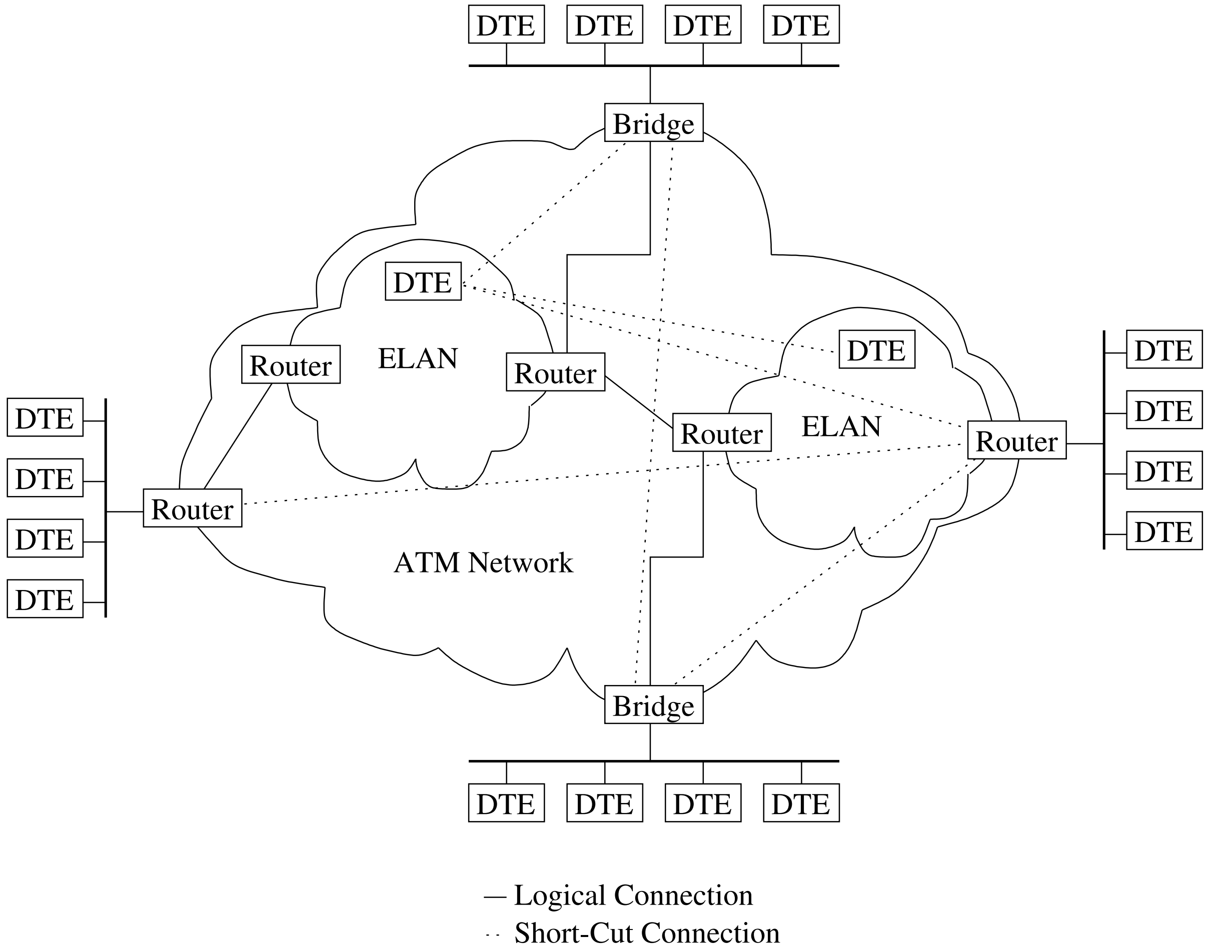

Abbildung 68: Short-Cuts mit MPOA

die gleiche Dienstgüte. Bei RSVP dagegen kann die Dienstgüte eines Mulicast-Flusses für verschiedene Empfänger unterschiedlich sein.

Das erste Problem wird durch das Ersetzen einer virtuellen Verbindung durch eine neue gelöst. Für die Lösung des zweiten Problem werden mehrere Möglichkeiten vorgeschlagen.

Data-VC-Management Die folgenden drei Modelle zeigen, welche Ansätze es für den Aufbau von virtuellen Verbindungen für einen Multicast-Fluß gibt [CBB+ 98]:

- **Voll-heterogenes Modell** (Full Heterogeneity Model siehe Abbildung 69)
  Für jeden Empfänger wird ein VC eingerichtet. Dieser VC kann die Dienstgüte erhalten, die auch tatsächlich gebraucht wird. Die Daten werden kopiert und jedem VC übergeben, dies kann natürlich bei gleichem Weg der VCs zu Bandbreitenverschwendung führen.

- **Homogenes Modell** (Homogenous Model siehe Abbildung 70)
  Ein Multicast-VC wird für alle Empfänger eines Flusses verwendet. Der VC muß natürlich allen Dienstgüteansprüchen genügen. Den Empfängern, die eigentlich weniger Ansprüche haben, müssen mehr Ressourcen als sie verlangen zugesprochen werden. Hat ein Empfänger geringere Ansprüche an die Dienstgüte, so kann ihm der

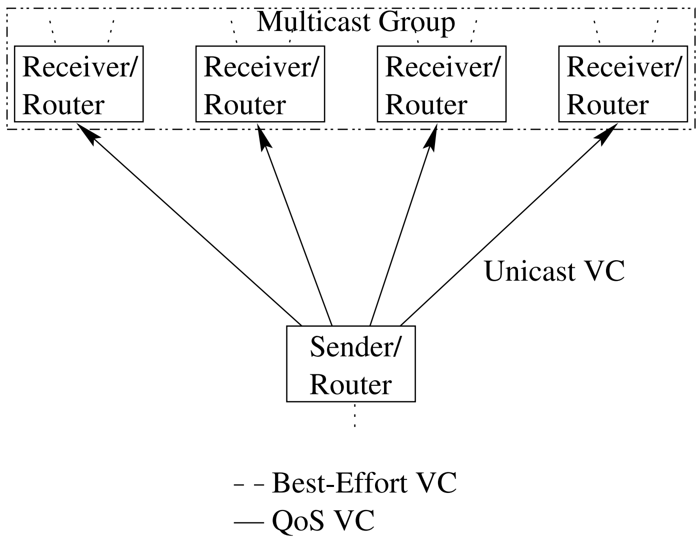

Abbildung 69: Full Heterogeneity

Dienst, aus Ressourcenmangel verweigert werden, obwohl genügend Ressourcen für seine Ansprüche vorhanden wären. Dafür muß ein Paket nur in einen VC gegeben werden und eine mehrfache Übertragung im geteilten Pfad kann vermieden werden.

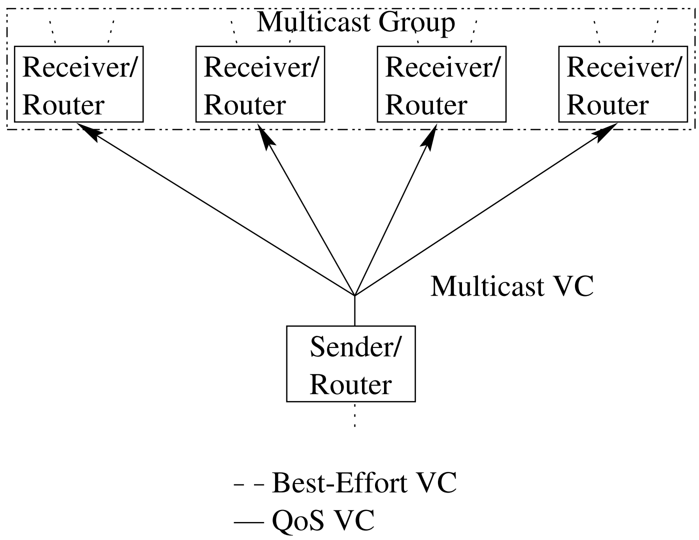

Abbildung 70: Homogenous

- **Beschränkt-heterogenes Modell** (Limited Heterogeneity Model siehe Abbildung 71)
  Für jeden Empfänger kann zwischen einem Mulitcast-VC mit Best-Effort-Dienstgüte oder einem Mulicast-VC mit einer weiteren Dienstgüte, die alle anderen Empfänger dieser Sitzung genügt, gewählt werden. Dieser Ansatz ist ein Kompromiß zwischen den Vor- und Nachteilen des voll-heterogenen und homogenen Modells.

Kontroll-VC-Management Neben den Daten müssen auch die RSVP-Nachrichten über virtuelle Verbindungen transportiert werden. Wie virtuelle Verbindungen zu diesem

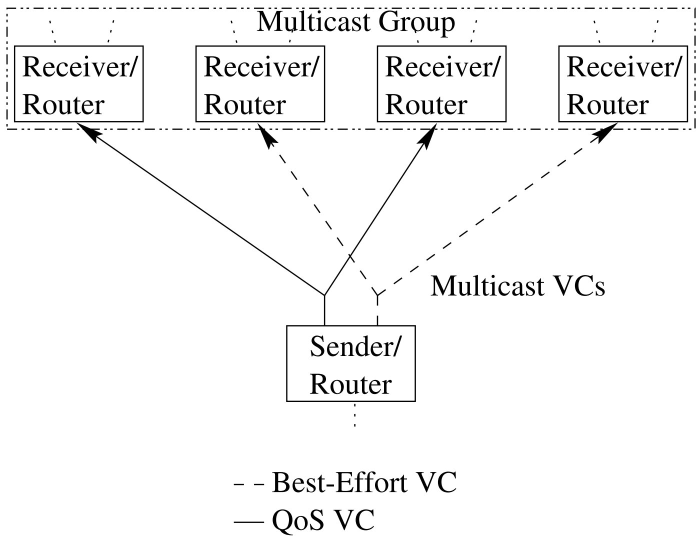

Abbildung 71: Limited Heterogeneity

Zweck genutzt werden können, zeigen die vier folgenden Vorschläge:

- **RSVP-Nachrichten und Daten in den selben VCs**
  Die RSVP-Nachrichten werden über die selben VCs wie die Daten transportiert. Somit werden keine zusätzlichen VCs benötigt. Leider kann Datenverkehr, der seine Reservierung überschreitet, dazu führen, daß RSVP-Nachrichten verloren gehen. RSVP kann ein gewisses Maß an Verlust ertragen, doch wird dieses überschritten, so kann dies zu wiederholtem Auf- und Abbau von VCs führen. Aus diesem Grund wird von diesem Ansatz abgeraten. Dieses Problem tritt natürlich so bei der Verwendung eines Best-Effort-VCs nicht auf, da hier das Maß für die Reservierung nicht angegeben wird und somit die Reservierung auch nicht überschritten werden kann. Doch auch hier kann es aufgrund von Stauungen im Netz zu Paketverlusten kommen.

- **Eigener VC für die RSVP-Nachrichten eines Flusses**
  Für jeden RSVP-Fluß wird ein eigener VC für die RSVP-Nachrichten eingerichtet. Der Vorteil dieses Ansatzes liegt in der Garantie für die Übertragung von RSVP-Nachrichten auf Kosten vieler VCs.

- **Geteilte Multicast-VCs für die RSVP-Nachrichten**
  Eine RSVP-Nachricht kann einen oder mehrere Empfänger haben, diese Empfänger werden zu Gruppen zusammengefaßt. Für jede unterschiedliche Gruppe wird ein Multicast-VC eingerichtet. Die RSVP-Flüsse mit gleicher Empfänger-Gruppe teilen sich einen VC für die RSVP-Nachrichten. Bei einem neuen RSVP-Fluß muß also überprüft werden, ob ein VC für die Empfänger-Gruppe existiert. Wenn ja, dann kann dieser genutzt werden, ansonsten muß ein neuer eingerichtet werden.

- **Ein VC für jeden Empfänger**
  Für jeden Empfängen einer RSVP-Nachricht wird ein VC erzeugt. Diesen VC teilen sich alle RSVP-Flüsse für RSVP-Nachrichten zu diesem Empfänger. Dies verlangt daß die RSVP-Nachrichten für Multicast-Verbindungen mehrfach transportiert werden, ohne dabei geteilte Strecken effizienter nutzen zu können. Dieser Ansatz liefert aber

eine geringere Anzahl an VCs für die RSVP-Nachrichten als der vorige und ist zudem leichter zu managen.

Bleibt noch die Frage, mit welchen Parametern im UNI-Signalisierungsprotokoll die virtuellen Verbindungen eingerichtet werden.

5.2.5 Service Mapping

Dieser Abschnitt befaßt sich mit den verschiedenen Möglichkeiten die IntServ-Dienste auf ATM-Dienste abzubilden [GaBo 98].

Ein RSVP-fähiges IP-Gerät, daß an ein ATM-Netz angeschlossen ist, hat die Aufgabe beim Erhalt einer Resv-Nachricht eine virtuelle Verbindung mit geeigneter Dienstgüte zum letzten Sender der Resv-Nachricht aufzubauen. Zu diesem Zweck übergibt der RSVP-Prozeß die hierfür nötigen Informationen dem UNI-Signalisierungsprotokoll [ATM-UNI 94] [ATM-UNI 96] (siehe RSVP$\xrightarrow{QoS}$UNI in Abbildung 72).

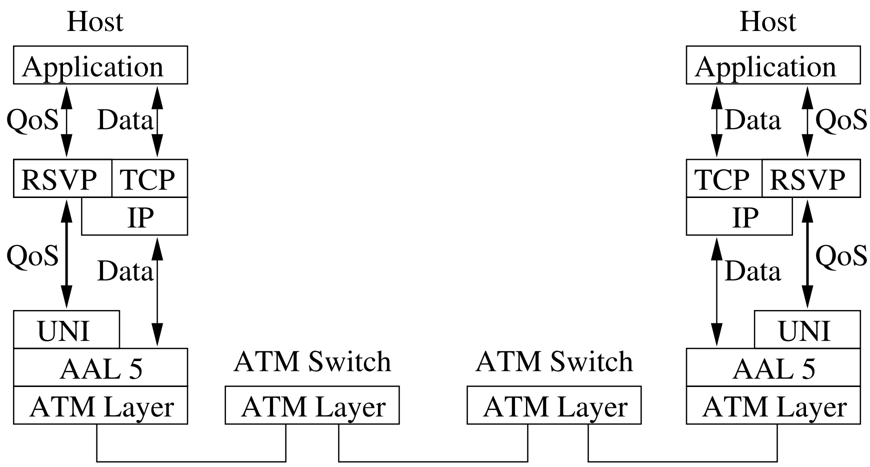

Abbildung 72: QoS-Signallisierung mit RSVP und ATM UNI

Das UNI-Signalisierungsprotokoll nutzt diese Information, um folgende Informationselemente einer SETUP-PDU [ATM-UNI 94] [ATM-UNI 96] zu füllen:

- Calling and Called Party Addressing Information
- AAL Parameters
- Broadband Low Layer Information
- Broadband Bearer Capability
- Traffic Descriptors
- QoS Class an Parameters

Auf diese Informationselemente wird genauer eingegangen.

Calling and Called Party Adressing Information Für den Aufbau einer virtuellen Verbindung zu einem bestimmten Gerät muß man dessen ATM-Adresse kennen. Durch `RSVP_HOP` der Resv-Nachricht ist aber nur die IP-Adresse gegeben. Um eine virtuelle Verbindung zu einem Gerät mit bestimmter IP-Adresse aufzubauen, können CLIP, LANE oder MPOA verwendet werden.

AAL Parameters und Broadband Low Layer Information Ein Transport von IP-Paketen über ein ATM-Netz erfolgt in der SDU der ATM Adaption Layer 5. Nun gibt es zwei Möglichkeiten, um mit einem IP-Paket weiter umzugehen:

- Keine weitere Verpackung
- Verpackung in einem LLC/SNAP-Frame [Hein 93]

Da hier die Nutzung einer virtuellen Verbindung auf IP-Pakete beschränkt ist, ist eine Verpackung mit [Hein 93] (ermöglicht das Demultiplexen verschiedener Pakettypen) nicht nötig. Jedoch erlaubt das UNI-Signalisierungsprotokoll [ATM-UNI 96] dies momentan noch nicht.

Dem Endpunkt einer virtuellen Verbindung wird mit den Parametern der Broadband Low Layer Information mitgeteilt, daß es sich bei einem von der AAL übergebenem Paket um ein in ein LLC/SNAP-Frame verpacktes IP-Paket handelt (siehe Tabelle 11).

Broadband Low Layer Information	
User Information Layer 2 Protocol	12 (LLC/SNAP)
User Information Layer 3 Protocol	11 (IP-Paket)
ISO/IEC TR 9577 IPI	204 (IP-Paket)

Tabelle 11: Broadband Low Layer Information

Die AAL 5 benötigt als Parameter, die maximale Größe der von ihr zu transportierenden Pakete (CPCS-SDU). Beim Verbindungsaufbau wird die maximale IP-Paketgröße (Maximale Paket Size) spezifiziert, damit muß zur maximalen IP-Paketgröße noch der LLC/SNAP-Header (8 Octet) addiert werden, um die CPCS-SDU-Größe zu erhalten. Mit dem Parameter SSCS Type wird die Service Specific Convergence Sublayer bestimmt, gewöhnlich wird keine verwendet (daher 0 in Tabelle 12).

AAL Parameter	
AAL Type	5
Forward CPCS-SDU Size	Maximum Packet Size + 8
Backward CPCS-SDU Size	Maximum Packet Size + 8
SSCS Type	0

Tabelle 12: AAL-Parameter

Broadband Bearer Capability Für die Dienstklasse, auf der der Dienst der ATM Adaption Layer 5 aufbauen soll, wurden für die IntServ-Dienste die Vorschläge aus Tabelle 13 gemacht. Diese Dienste werden in Broadband Bearer Capabilty spezifiziert (siehe Tabelle

Integrated Services to ATM Service Mapping	
Guaranteed Service (GS)	Constant Bit Rate (CBR) Real-Time Variable Bit Rate (rtVBR)
Controlled Load Service (CLS)	Non-Real-Time Variable Bit Rate (nrtVBR) Available Bit Rate (ABR)
Best Effort (BE)	Unspecified Bit Rate (UBR) Available Bit Rate (ABR)

Tabelle 13: Abbildung von IntServ-Diensten auf ATM Layer Dienstgüteklassen

Type	Bearer Class	ATM Transfer Capability
Constant Bit Rate (CBR)	16	5
Real-Time Variable Bit Rate (rtVBR)	16	9
Non-Real-Time Variable Bit Rate (nrtVBR)	16	10
Available Bit Rate (ABR)	16	12
Unspecified Bit Rate (UBR)	16	10

Tabelle 14: Broadband Bearer Capabiliy-Werte für Dienstgüteklassen

14).

Folgen nun die Informationselemente, die in Abhängigkeit von der verwendeten IntServ-Dienstgüte gesetzt werden. Die IntServ-Dienstgüte wird mit folgenden Parametern spezifiziert:

- Token Bucket Rate (TBR)
  Die Token Bucket Rate gibt die maximale Übertragungsrate an, mit der über einen längeren Zeitraum gesendet werden darf (siehe Abschnitt 2.3.2).

- Token Bucket Size (TBS)
  Die Token Bucket Size gibt die maximale Datenmenge an, die mit der Peak Data Rate gesendet werden darf.

- Peak Data Rate (PDR)
  Die Peak Data Rate gibt die maximale kurzfristige Übertragungsrate an.

- Minimum Policed Unit (MPU)
  Alle Datenmengen, die kleiner als die Minimum Policy Unit sind, werden behandelt als hätten sie die mit MPU spezifizierte Größe.

- Maximum Packet Size (MPS)
  Die maximale Paketgröße die erlaubt ist.

- Minimum Path Latency (MPL)
  Die minimale Übertragungszeit.

- Rate (R)
  Die zugesicherte Übertragungsrate für einen Fluß.

- Slack Term (ST)
  Definiert die Verzögerung, die ein Empfänger zusätzlich zur best möglichen maximalen Übertragungszeit erlaubt.

Guaranteed Service (GS) Der Guaranteed Service verlangt, daß eine maximale End-zu-End-Übertragungszeit eingehalten wird. Daher muß die Übertragungszeit über eine virtuelle Verbindung nach oben beschränkt sein. Die Dienstgüteklassen nrtVBR, ABR und UBR scheiden daher aus, da sie dies nicht garantieren können. CBR und rtVBR erlauben es die maximale Übertragungszeit[4] mit dem Parameter *End-to-End Transit Delay* für eine virtuelle Verbindung vorzugeben.

Die Implementierung dieses Dienstes benötigt die zwei Parameter C und D. Diese Werte drücken die Abweichung vom Fluid Model aus, daß den Dienst einer eigenen Leitung mit fester Bandbreite zwischen Sender und Empfänger beschreibt. Jedes Bit wird auf der Leitung mit der minimalen Übertragungszeit transportiert, bei ATM variiert diese Zeit durch das Multiplexen von Zellen. Jedoch kann CBR und rtVBR mit dem Parameter *Acceptable Cell Delay Variation* (CDV) das Zurückbleiben eines Bits hinter der minimalen Übertragungszeit beschränken. Der Fehlerwert C kann vernachlässigt werden, da die Zellen relativ klein sind und damit der Unterschied zu einer bitweisen Übertragung minimal ist. Damit ergeben sich die Fehlerwerte für den ATM-Abschnitt einer Übertragung zu:

$$D\_ATM = CDV$$

$$C\_ATM = 0$$

Beim Aufbau einer virtuellen Verbindung erlaubt der Parameter Slack Term einen Spielraum für die tatsächliche Reservierung. Nimmt man einen bestimmten Anteil des Slack Term-Wertes (S_ATM) in Anspruch ergeben sich die Parameter der Reservierung zu:

$$CTD = D\_ATM + MPL + S\_ATM$$

$$CDV = D\_ATM + S\_ATM$$

Extended-QoS-Parameters	
Acceptable Forward CDV	$D\_ATM + S\_ATM$
Forward End-to-End CTD	$D\_ATM + MPL + S\_ATM$

Tabelle 15: Extended QoS Parameters

Traffic Descriptor für Guaranteed Service mit rtVBR PCR, SCR und MBS werden für rtVBR verwendet, diese entsprechen den Parametern Peak Data Rate, Rate und Token Bucket Size bei IntServ (siehe Tabelle 16).

Eine ATM-Zelle enthält ein Cell Loss Priority Bit. Dieses Bit teilt die ATM-Zellen einer virtuellen Verbindung in zwei Klassen ein. Traffic Descriptor Parameter können sich auf die erste Klasse (CLP=0) oder beide Klassen (CLP=0+1) beziehen. Erlaubte Kombinationen

[4] nrtVBR erlaubt dies nur aus Kompatibilitätsgründen zur ITU-T

Traffic Descriptor für rtVBR	
Forward PCR CLP=0+1	Peak Data Rate
Forward SCR CLP=0	Rate
Forward MBS (CLP=0)	Token Bucket Size
Forward Frame Discard Bit	1
Backward Frame Discard Bit	1
Tagging Forward Bit	1 (Tagging requested)
Tagging Backward Bit	1 (Tagging requested)

Tabelle 16: Traffic Descriptor für rtVBR

sind [ATM-UNI 96, Seiten 105 und 106] zu entnehmen. Der GS-Dienst verlangt, daß Pakete, die nicht mit den Werte von TBR, TBS und PDR konform sind, mit dem Best Effort-Dienst transportiert werden sollen. Bei VBR kann dies durch die Verwendung von VBR.3 (siehe [ATM-TM 96]) nachgeahmt werden. Bei nicht konformen Zellen wird das CLP-Bit gesetzt und es gilt für diese Zellen keine Garantie für eine Übertragung. VBR.3 wird mit dem Tagging Bit-Wert 1 signalisiert.

Traffic Descriptor für Guaranteed Service mit CBR CBR verwendet den Traffic Descriptor Parameter PCR. Sein Wert wird auf die Token Bucket Rate gesetzt (siehe Tabelle 17).

Traffic Descriptor für CBR	
Forward PCR CLP=0+1	Rate
Forward Frame Discard Bit	1
Backward Frame Discard Bit	1
Tagging Forward Bit	0 (Tagging not requested)
Tagging Backward Bit	0 (Tagging not requested)

Tabelle 17: Traffic Descriptor für CBR

Controlled-Load Service (CLS) Der Controlled-Load Service stellt keine so hohen Ansprüche an die Übertragungszeit. Virtuelle Verbindungen mit der nrtVBR und der ABR Dienstgüte sind für den CLS geeignet. Beide erfüllen die Ansprüche an den zu erwartenden Verlust. Für die Übertragungszeit wird beim CLS verlangt, daß die aus der Übertragung mit der Token Bucket Rate (TBR) folgende Übertragungszeit für die meisten Pakete nicht wesentlich überschritten wird. Die virtuellen Verbindungen sichern eine Übertragung mit den Raten SCR und MCR zu, damit werden auch die Werte für die Übertragungszeit erreicht. Die Traffic Descriptoren für die beiden virtuellen Verbindungen stehen in Tabelle 18 und 19.

Best Effort (BE) Best Effort stellt keine Anforderungen an die Dienstgüte. UBR ist die passende Dienstklasse der ATM Layer für Best Effort. Dieser Dienst wird wie nrtVBR kodiert, jedoch muß der Best Effort Indicator vorhanden sein und die Dienstgüteklasse (QoS Class) Null (bedeutet nicht spezifiziert) verwendet werden. Für den Traffic Descriptor ist nur die PCR erlaubt.

Traffic Descriptor für nrtVBR	
Forward PCR CLP=0+1	Peak Data Rate
Forward SCR CLP=0	Token Bucket Rate
Forward MBS (CLP=0)	Token Bucket Size
Forward Frame Discard Bit	1
Backward Frame Discard Bit	1
Tagging Forward Bit	1 (Tagging requested)
Tagging Backward Bit	1 (Tagging requested)

Tabelle 18: Traffic Descriptor für nrtVBR

Traffic Descriptor für ABR	
Forward PCR CLP=0+1	Peak Data Rate
Forward MCR CLP=0	Token Bucket Rate
Forward Frame Discard Bit	1
Backward Frame Discard Bit	1
Tagging Forward Bit	1 (Tagging requested)
Tagging Backward Bit	1 (Tagging requested)

Tabelle 19: Traffic Descriptor für nrtVBR

5.2.6 Anwendung des Kriterienkatalogs

Die Anwendung des Kriterienkatalogs erfolgt in zwei Schritten. Der erste Schritt, die Anwendung des Kriterienkatalogs auf IntServ/RSVP unabhängig von der Netztechnologie, wurde schon in Abschnitt 5.1.3 durchgeführt. Der zweite Schritt, die Änderungen aufgrund der Netztechnologie, wird nun für ATM durchgeführt. Es werden nur die Kriterien aufgeführt, die einer Änderung unterworfen sind, die restlichen können Abschnitt 5.1.3 entnommen werden:

User→Access→Access Delay	
Voraussetzungen:	Ein Fluß nutzt Guaranteed Service oder Controlled-Load Service
Kriterium:	Eine maximale Zugangszeit kann nicht angegeben werden, da RSVP-Nachrichten mit der BE-Dienstgüte transportiert werden, welche weder eine maximale Übertragungszeit für RSVP-Nachrichten noch deren Übertragung überhaupt garantiert. Die minimale Zugangszeit ist durch die minimale Round Trip Delay nach unten beschränkt. Hierzu kommt noch die Verarbeitungszeit in den RSVP-Prozessen. Die Zugangsaufbauzeit ist im Gegensatz zu Sonet/SDH größer, da hier noch die Verbindungsaufbauzeiten der virtuellen Verbindungen anfällt.
Voraussetzungen:	Ein Fluß nutzt Best-Effort
Kriterium:	Die Zugangsverzögerung ist Null

User→Transfer→Transfer Delay	
Voraussetzungen:	Ein Fluß f verwendet Guaranteed Service
Aussage:	Die maximale Übertragungsverzögerung ist beschränkt. Der Wert für die maximale Übertragungsverzögerung wird durch das ATM-Netz bestimmt. ATM verwendet Zellen zur Übertragung, diese Zellen sind im Vergleich zu Paketen, die bei Sonet/SDH verwendet werden, ziemlich klein. Dies entspricht eher der bitorientierten Übertragung des Fluid Model, damit ist der Fehlerwert C vernachlässigbar gering. Die geringe Größe von Zellen wirkt sich auch positiv auf den Fehlerwert D aus, mit dem der maximale Jitter, der nicht von der Bitrate abhängig ist, ausgedrückt wird. Aufgrund dieser Überlegungen ist zu erwarten, daß die maximale Übertragungsverzögerung geringer ist als bei Sonet/SDH. Im Vergleich zu DiffServ kann IntServ/RSVP unter ähnlichen Bedingungen niedrigere obere Schranken für die Übertragungsverzögerung garantieren (siehe 5.3.4). Die minimale Übertragungsverzögerung ist durch *MPL* beschränkt.
Voraussetzungen:	Ein Fluß f verwendet Controlled-Load Service
Aussage:	Die maximale Übertragungsverzögerung ist nicht beschränkt. Die minimale Übertragungsverzögerung ist durch *MPL* beschränkt.
Voraussetzungen:	Ein Fluß verwendet Best Effort
Aussage:	Die maximale Übertragungsverzögerung ist nicht beschränkt. Die minimale Übertragungszeit ist durch MPL beschränkt.

User→Transfer→Jitter	
Voraussetzungen:	Ein Fluß f verwendet Guaranteed Service
Aussage:	Der maximale Jitter ist beschränkt. Die Überlegungen, die bei der Ermittlung von *Transfer Delay* angestellt wurden, führen zu dem Schluß, daß auch der Jitter im Vergleich zu Sonet/SDH geringer ist. Aus der Tatsache, daß IntServ/RSVP in der Lage ist niedrigere maximale Übertragungsverzögerungen als DiffServ zu liefern, wird geschlossen, daß auch der maximale Jitter niedriger als bei DiffServ ist.
Voraussetzungen:	Verwendung des Controlled-Load Service
Aussage:	Der maximale Jitter ist nicht beschränkt.
Voraussetzungen:	Ein Fluß verwendet Best Effort
Aussage:	Der maximale Jitter ist nicht beschränkt.

Provider→Configuration Management→Configuration Delay	
Voraussetzungen:	keine
Aussage:	Die Konfiguration für IntServ/RSVP umfaßt das Setzen von Parametern des Policy Control und die Einrichtung von CLIP, LANE oder MPOA. Diese Arbeit muß im Idealfall nur für die Inbetriebnahme eines Netzes erfolgen.

Provider→Performance Management→Bandwidth	
Voraussetzungen:	keine
Aussage:	Die verfügbare Bandbreite für IP-Pakete auf dem Übertragungsmedium beträgt ca. 80% [Trillium 97] der Übertragungsbandbreite des Mediums. Ein Teil dieser Bandbreite wird für die Übertragung von RSVP-Nachrichten genutzt, ca. 60 bps pro Fluß. Die verfügbare Bandbreite ist bei ATM kleiner als bei der Nutzung von Sonet/SDH.

Provider→Performance Management→Resource Release Delay	
Voraussetzungen:	keine
Aussage:	Die maximale Zeit für das Freigeben von Ressourcen ist beschränkt. Die Freigabe der Ressourcen erfolgt spätestens nach Ablauf des Timers für die Lebenszeit des Reservierungszustands in einem RSVP-Prozeß. Die Lebenszeit für einen Timer ist $<$ 2 Minuten (Wert nach [BZB$^+$ 97]). Da die Timer der Reservierungen eines Flusses nacheinander ablaufen können, kann sich die Freigabe der letzten Ressourcen einige Minuten hinziehen. Die Zeit für den Abbau der virtuellen Verbindung fällt dabei kaum ins Gewicht. Die minimale Freigabezeit der Ressourcen ist durch MPL und die Abbauzeiten der virtuellen Verbindungen beschränkt. Beendet der Empfänger den Zugang, dann werden mit dem Erreichen der Teardown-Nachricht beim Sender die letzten Ressourcen freigegeben.

5.3 RSVP/IntServ über IEEE 802.3/Ethernet

Wenden wir uns jetzt der Frage zu, wie und ob die Dienste von IntServ über ein Ethernet funktionieren. Das CSMA/CD-Verfahren für den Zugriff auf das Medium stellt jedoch ein erhebliches Problem dar, vorhersagbare Garantien von einem Ethernet zu bekommen. Dies trifft nicht nur bei hoher Last zu, sondern auch bei geringer Last. Zum Beispiel kann bei zwei Sendern eine Übertragung nicht garantiert werden, da sie immer gleichzeitig zu senden versuchen können und sich somit gegenseitig daran hindern können. Dies kann so oft geschehen bis die maximale Zahl der Wiederholungsversuche zuende geht.

Für die Lösung dieses Problems wurden folgende Möglichkeiten überlegt:

- **Zugriffsverfahren ändern**
  Die Idee ist das CSMA/CD-Zugriffsverfahren durch ein anderes abzulösen. Dies löst das eigentliche Problem, IntServ/RSVP über IEEE 802.3/Ethernet, nicht, sondern verlagert es auf eine Neuentwicklung. Eine Konsequenz dieses Ansatzes wäre, daß ein großer Teil der Hardware (z.B. Netzwerkkarten) ausgetauscht werden müßte. Das Ziel sollte es aber sein die Hardware weiter zu nutzen.

- **Zugriffsverfahren erweitern**
  Es wäre auch denkbar auf dem CSMA/CD-Zugriffsverfahren eine Softwareerweiterung zu implementieren. Diese Lösungsidee verliert mit dem momentanen Trend hin zu immer weniger Sender pro Segment bis hin zur Microsegmentierung an Bedeutung.

Im nächsten Abschnitt befassen wir uns mit einer Architektur, die auf eine Lösung oder Lösungsversuch in einer Umgebung aus wiederholten Segmenten abzielt.

5.3.1 Bandwidth Manager

Wie in Abschnitt 3.3.1 schon erwähnt, wird Ethernet durch IEEE 802.2 und IEEE 802.3 standardisiert. Die IEEE hat in den 802.x Standards noch weitere Netztechnologien, wie Token Ring und Token Bus u.s.w., spezifiziert. Diese Netztechnologien haben alle die selbe LLC Layer (IEEE 802.2), und damit den selben SAP zur Data Link Layer. Für die Kopplung von mehreren gleichen oder verschiedenen dieser Netze hat die IEEE den Standard 802.1 verabschiedet (siehe Abbildung 73). Dies ermöglicht es ein Netz aus mehreren

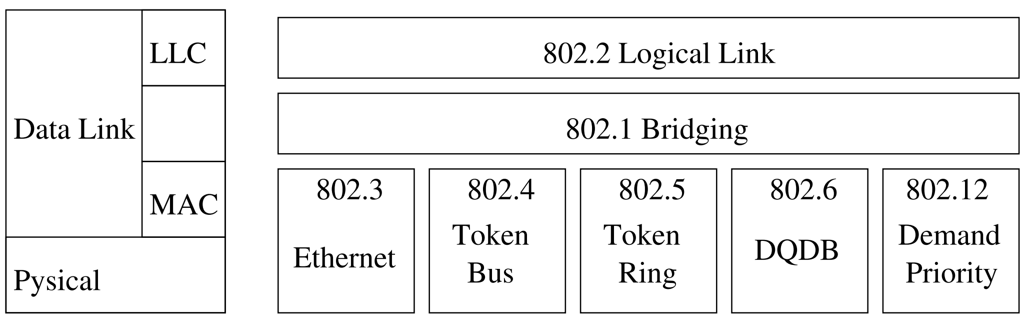

Abbildung 73: IEEE Standards

Netztechnologien aufzubauen.

Da alle 802 Netztechnologien die selbe LLC Layer haben, liegt es nahe mit dem dort vorkommenden Parameter User Priority, ähnlich wie bei DiffServ, die Zugehörigkeit eines

Frames zu einer Verkehrsklasse zu bestimmen. Technologien wie Token Ring zum Beipiel nutzen diesen Wert für den Zugriff auf das gemeinsam genutzte Medium, bei Ethernet wird er dagegen weder transportiert noch genutzt. Die User Priority kann in den Bridges und Switches verwendet werden, um dort das Scheduling der Frames zu steuern. Für Ethernet stellt der neue Standard 802.1p eine Möglichkeit dar, diesen Wert zu übertragen, um damit auch in den Bridges und Switches Verwendung zu finden. Verschiedene Dienste können dann auf OSI Schicht 2 Geräten, ähnlich wie bei DiffServ, durch Classifier, Queues und Scheduler erreicht werden (siehe Abschnitt 3.3.2). Mit der Einschränkung, daß dort nur ein Prioritätsscheduling möglich ist. Die Aufgabe des Admission erfüllt in einem 802-Netz der *Bandwidth Manager* [SSS+ 99].

Der Bandwidth Manager besteht aus zwei Modulen:

- **Requester Module (RM):**
  Dieses Modul enthält jede DEE, die an einer Reservierung Teil nimmt.

- **Bandwidth Allocator (BA):**
  Dieses Modul ist für die Zuteilung der Ressourcen im Subnetz verantwortlich.

Beim Bandwidth Allocator sind zwei Implementierungsarten denkbar:

- **Zentralisiert** (siehe Abbildung 74)
  Die Funktion des Bandwidth Allocator wird von einem Gerät im Subnetz erbracht. Dieses sollte die Topologie des Subnetzes kennen, damit die Ressourcen möglichst effizient vergeben werden können. Ein Centralized Bandwidth Allocator kann zum Engpaß im Netz werden. Der Vorteil dieses Ansatzes liegt darin, daß Netzknoten (Switches und Bridges) die Funktionalität des Bandwidth Allocators nicht benötigen, wie viele der heutigen Produkte.

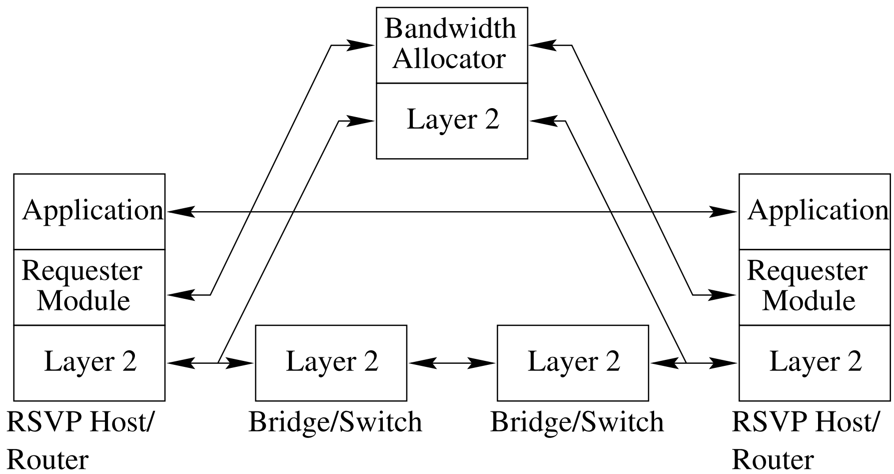

Abbildung 74: Centralized Bandwidth Allocator

- **Verteilt** (siehe Abbildung 75)
  Beim Distributed Bandwidth Allocator ist die Funktionalität des Bandwidth Allocators auf alle Geräte (Switches, Bridges und Hosts) verteilt. Die Endgeräte besitzen zusätzlich noch ein Requester Modul. Für eine Reservierung kommunizieren die Distributed Bandwidth Allocator, die auf dem Weg vom Sender zum Empfänger liegen,

untereinander, ob auf diesem Weg genügend Ressourcen bereitstehen. Dieser Ansatz ähnelt dem, den RSVP auf OSI-Schicht 3 verfolgt und damit muß auch hier die Topologie nicht bekannt sein.

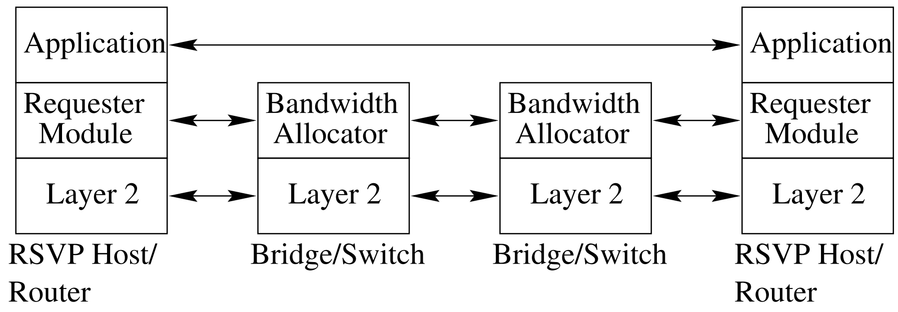

Abbildung 75: Distributed Bandwidth Allocator

Requester Modul im Sender Wollen wir nun genauer auf die Funktion des Requester Moduls im Sender eingehen (siehe Abbildung 76). Das Requester Modul erhält Anfragen

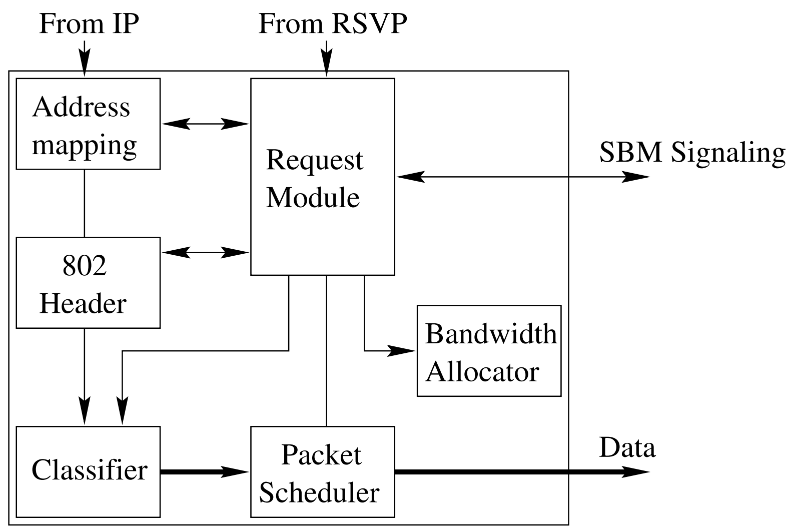

Abbildung 76: Sender [SSS+ 99, Seite 19]

von RSVP, ob ein Fluß vom Subnetz gewährt werden kann. Mit einem Signalisierungsprotokoll, wie zum Beispiel SBM [YHBB 99], wird diese zum Bandwidth Allocator weitergeleitet. Im verteilten Fall muß diese Anfrage zu zwei Instanzen des Bandwidth Allocator, dem lokalen und dem nächsten in Richtung Empfänger, geschickt werden. Die Adresse des nächsten Bandwidth Allocator wird vom Address Mapping bereitgestellt, die ihrerseit diese beim Address Resolution Protocol erfragen kann.

Das Requester Modul erhält bei erfolgreicher Reservierung vom Bandwidth Allocator eine User Priority zurück, mit der die Pakete des Flusses gesendet werden sollen. Die Zuordnung der User Priority zu den Flüssen wird in einer Tabelle (802 Header) aufbewahrt. Diese Information wird vom Classifier den Paketen mitgegeben.

Requester Modul im Empfänger Die Aufgabe des Requester Modul im Empfänger sieht wesentlich einfacher aus (siehe Abbildung 77). Es muß der lokalen Bandwidth Alloca-

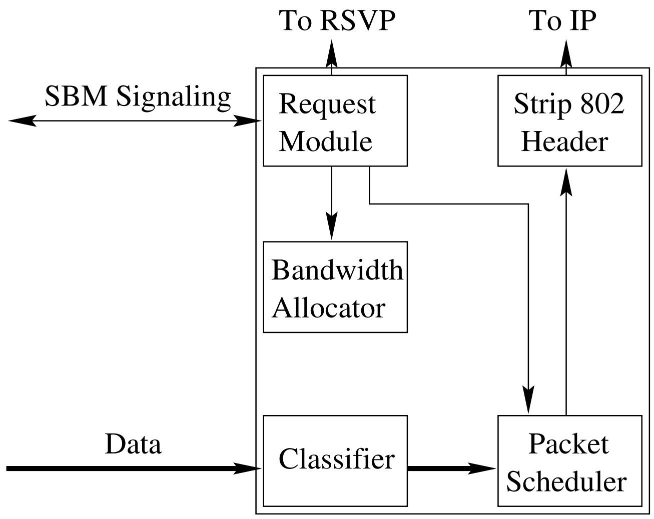

Abbildung 77: Receiver [SSS+ 99, Seite 20]

tor konsultieren, ob genügend Ressourcen für den eingehenden Fluß (z.B. Empfangspuffer) zur Verfügung stehen. Falls ein Classifier und Scheduler für den Eingangsverkehr verwendet werden, kann er diese konfigurieren.

Bandwidth Allocator in der Bridge/Switch Beim verteilten Ansatz besitzt jede Bridge/Switch einen Bandwidth Allocator und dieser kann die vorhandenen Ressourcen konfigurieren (siehe Abbildung 78). Jeder Port einer Bridge besitzt ein Modul (IN SBM) für

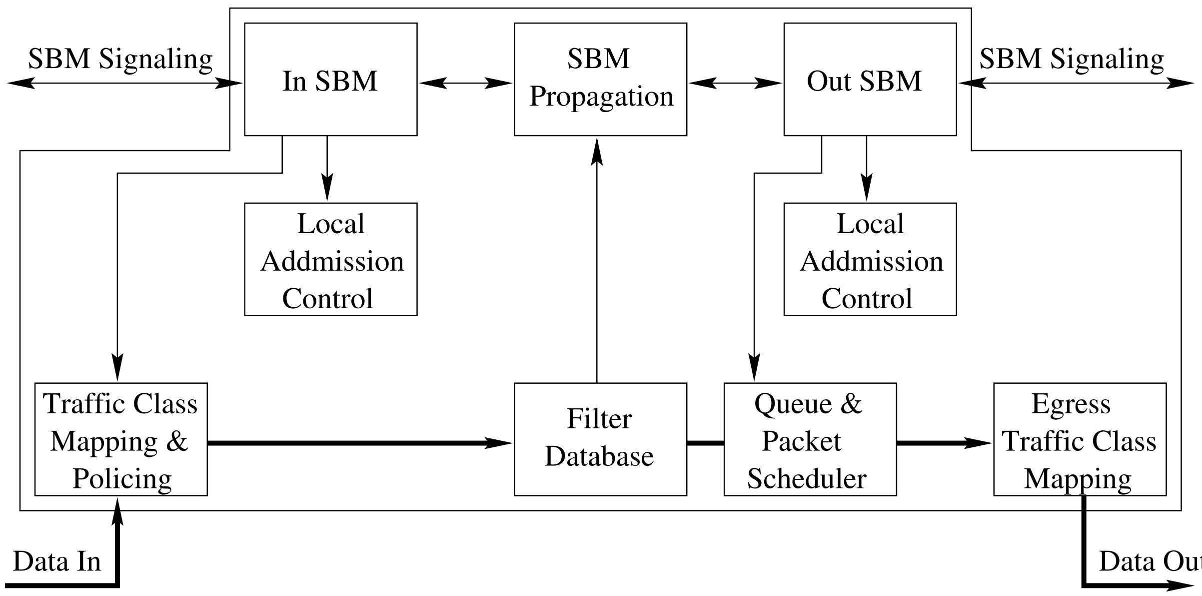

Abbildung 78: Switch [SSS+ 99, Seite 22]

eingehende Signalisierungsnachrichten. Analog zum Empfänger wird hier beim Erhalt einer Anfrage überprüft, ob genügend Ressourcen für den Eingangsverkehr vorhanden sind. Ist dies der Fall wird unter Zuhilfenahme der Routing-Datenbank (Filter Database) die Anfrage durch das SBM Propagation Modul an das OUT SBM Modul des entsprechenden Ports weitergereicht. Dies überprüft die Ressourcen für den Ausgangsverkehr an diesem Port und kann den Classifier, die Queues und den Scheduler konfigurieren. Der Eingangsverkehr kann auf seine Konformität zu den vereinbarten Parametern geprüft werden. Außerdem kann eine Abbildung in eine andere Verkehrsklasse erfolgen (User Priority ändern). Diese Aufgaben erfüllt das Ingress Traffic Class Mapping and Policing Modul. Eine Abbildung kann auch vor dem Senden eines Paketes durch das Egress Traffic Class Mapping Modul erfolgen.

5.3.2 Subnet Bandwidth Manager

Subnet Bandwidth Manager (SBM) ist ein Signalisierungsprotokoll für das Admission Control in IEEE 802 Netzen [YHBB 99]. SBM basiert auf der Architektur des *Bandwitdh Manager* (BM).

Ein Gerät, das in der Lage ist als Bandwidth Allocator zu agieren, wird als SBM-fähig bezeichnet. Gibt es in einem Segment mehrere SBM-fähige Geräte, dann wird ein Gerät als *Designated Subnet Bandwidth Manager* (DSBM) ausgewählt. Der DSBM übernimmt die Aufgabe des Bandwidth Allocator im Segment. Sind Segmente über nicht SBM-fähige Geräte (Switch und Bridge) verbunden, dann werden sie wie ein Segment behandelt. Damit kann SBM seine Implementierungsart, verteilt oder zentral, den Bedingungen im Netz geeignet wählen. Die Requester Module werden als *Designated Subnet Bandwidth Manager Client* (DSBM-Client) bezeichnet.

Die Aufgabe eines DSBM ist es Anfragen, ob genügend Ressourcen für einen Fluß im Segment zur Verfügung stehen, zu beantworten. Die dafür notwendigen Daten sind in der Resv-PDU von RSVP enthalten. Die Idee von SBM ist, die RSVP-PDUs um einige Objekte zu erweitern und dann über DSBMs eines Subnetzes lenken. Der DSBM sendet die SBM-Resv-PDUs, die erfolgreich das Admission Control bestanden haben zum nächsten RSVP-Prozeß. Dort angekommen werden die zusätzlichen Objekte wieder gelöscht und die Resv-PDU dem RSVP-Prozeß übergeben. Dies ist gleichbedeutend mit dem erfolgreichen Bestehen des Admission Control (siehe Abbildung 79).

Dieses Verfahren spart Zeit und Bandbreite, da nicht erst nach Erhalt einer Resv-PDU vom RSVP-Prozeß eine Anfrage bei den DSBM des Subnetzes erfolgen muß. Damit die Resv-PDUs den Weg über die DSBM des Subnetzes folgen, werden die Path-PDUs über diese gelenkt und in den SBM-fähigen Geräten der Weg analog zu RSVP festgehalten (siehe Abbildung 80).

Die RSVP-PDUs erhalten im Subnetz zusätzliche Objekte. Die Objekte und ihre Aufgaben sind:

- `RSVP_HOP_L2`
  Dieses Objekt wird verwendet, damit nicht jedes SBM-fähige Gerät (z.B. Bridge) das Routing nach IP-Adressen unterstützen muß. Es trägt die MAC-Adresse des nächsten RSVP-HOPs (`RSVP_HOP`).

- `LAN_NHOP`
  In `LAN_NHOP` wird die IP-Adresse und die MAC-Adresse des SBM-fähigen Geräts im Subnetz spezifiziert, an die die RSVP-Nachricht gerichtet ist.

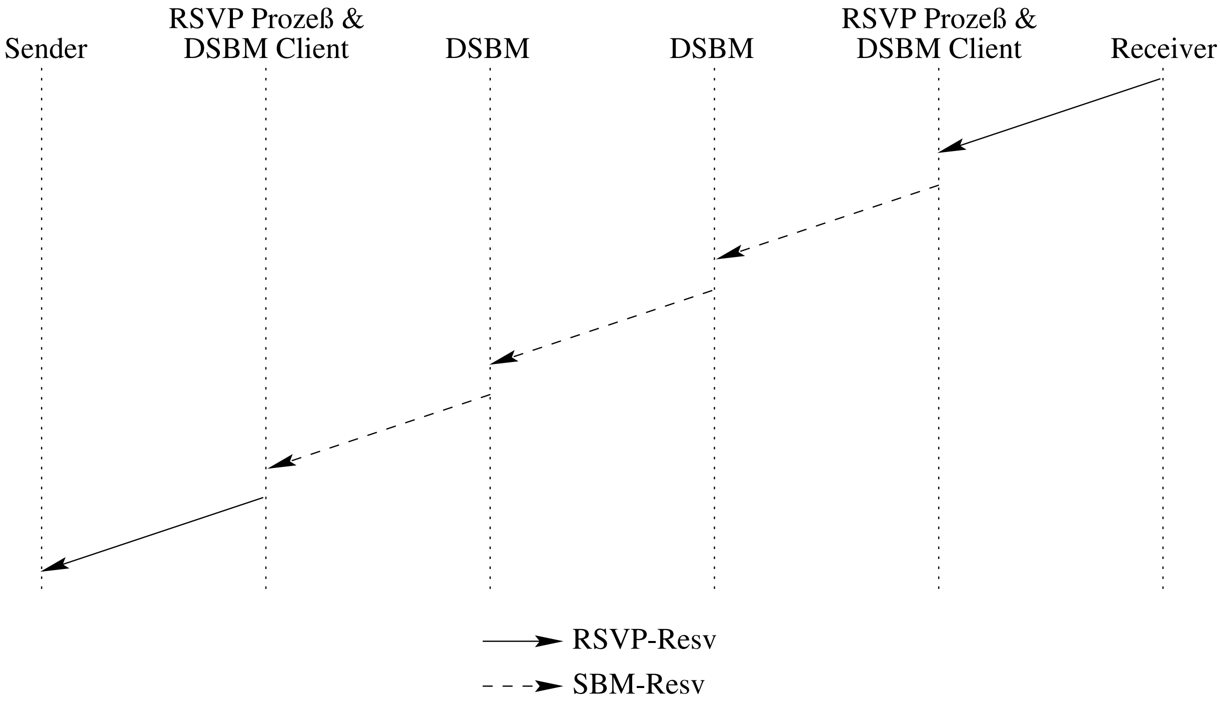

Abbildung 79: Übertragung einer RSVP-Resv-PDU mit SBM

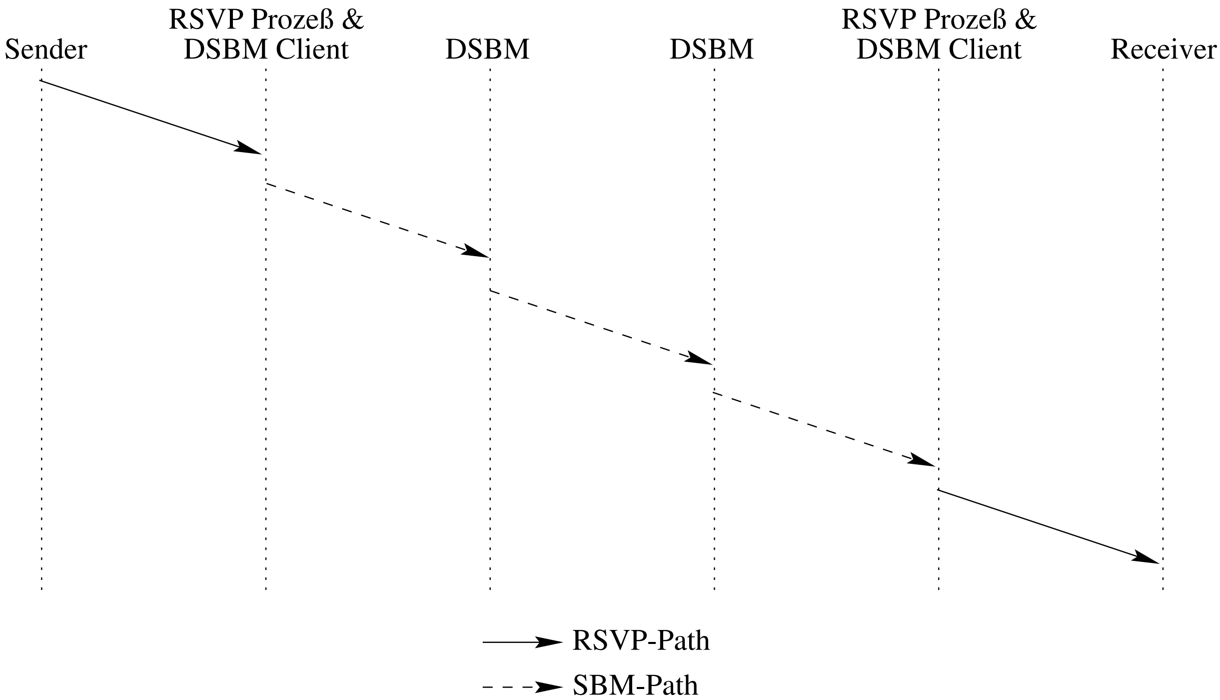

Abbildung 80: Übertragung einer RSVP-Resv-PDU mit SBM

- `TCLASS`
  Diese Objekt wird für den Transport der User Priority zum DSBM-Client verwendet.

5.3.3 Controlled-Load Service

Der Controlled-Load Service kann sowohl in einem Shared als auch einem Switched Ethernet erzielt werden. Für ein Switched Ethernet kann dies ähnlich der Einrichtung dieser Dienstgüte bei Sonet/SDH mit dem Prioritätsscheduling, daß modernere Bridges und Switches unterstützen müssen, erfolgen. Ein Shared-Ethernet unter geringer Last leistet eine Dienstgüte, die mit dem CLS verträglich ist. Die Ursache von Verlusten und Verzögerungen in einem Shared Ethernet sind die Kollisionen beim Zugriff auf das Medium. Viele Untersuchungen zeigten, daß die Anzahl der Kollisionen von der Last abhängt. Die Last von IntServ-Flüssen wird mit dem DSBM kontrolliert. Damit die Last vom BE-Verkehr nicht unbegrenzt den IntServ-Verkehr stören kann wurde das Objekt `NON_RESV_SEND_LIMIT` eingeführt. Mit diesem Objekt wird den Endstationen mitgeteilt, wieviel BE-Verkehr sie senden dürfen.

5.3.4 Guaranteed Service

Wie in der Einleitung schon erwähnt kann man für ein Shared Ethernet keine maximale Übertragungszeit und die Übertragung an sich garantieren, damit ist auch der Guaranteed Service hier nicht zu erzielen.

Für ein Switched Ethernet sieht dies anders aus. Hier läßt sich diese Dienstgüte mit einem Prioritätsscheduling erreichen. Anna Charny [Anna 98] zeigte, daß in einem DiffServ-Netz mit Prioritätsscheduling für das EF-PHB eine Schranke für die Übertragungszeit existiert. Diese Schranke ist:

$$D_h = h(1+\alpha)^{H-1}\left(\frac{\alpha b_{max}}{r_{min}} + \max\left(\frac{MTU}{C}\right)\right)$$

h	Anzahl der Hops für diesen Fluß
H	maximale Anzahl der Hops im Netz
α	maximale Nutzung des priorisierten Verkehrs aller Kanäle
b_{max}	maximaler Leaky Bucket Burst unter allen Flüssen
r_{min}	minimale Leaky Bucket Burst Rate aller Flüsse im Netz
C	verfügbare Bandbreite des Mediums

Diese Erkenntnis läßt sich auf das Switched-Ethernet übertragen, da auch hier ein Prioritätsscheduler auf Aggregate angewandt wird. Ein Aggregat besteht aus einer Menge von PDUs, die den gleichen Differentiated Services CodePoint (DSCP) oder die gleiche User Priority haben. Da die Einhaltung aller obigen Parameter beim Flußaufbau überprüft werden können, sind die Voraussetzungen gegeben, um einen vordefinierten Verzögerungswert einzuhalten.

Ein EF-PHB läßt sich also, durch Abbildung des Differentiated Services CodePoint (DSCP) auf eine User Priority in Switched-Ethernet erzeugen. Prinzipiell kann in einem Switched-Ethernet DiffServ funktionieren, solange das Per Hop Behavior mit dem Prioritätsscheduling implementiert werden kann. Dies ist für das AF-PHB schon nicht mehr möglich.

Die maximale Übertragungszeit für PDUs mit einem Aggregat-Scheduling ist unter ähnlichen Bedingungen größer als die für ein Microfluß-Scheduling einzuschätzen. Ein Microfluß ist ein Fluß zwischen Anwendungen, der durch das Tupel (Source IP Address, Source Port, Protocol ID, Destination Port, Destination IP Address) identifiziert wird. Dies kann man sich wie folgt klar machen, treffen kurz vor einer PDU eines Microflusses sehr viele Bursts (größere PDU-Mengen) von anderen Flüssen ein, dann werden bei einem Aggregat-Scheduling alle diese PDUs zuerst gesendet. Ein Microfluß-Scheduler, der einzelne Flüsse seperat behandelt, kann PDUs vor zuvor eingetroffenen PDUs senden und somit die Gesamtverzögerung, die durch einen kurzfristigen Stau resultiert, besser auf alle PDUs der Warteschlangen verteilen, was die maximale Verzögerung eines Flusses herabsetzt.

5.3.5 Anwendung des Kriterienkatalogs

Die Anwendung des Kriterienkatalogs erfolgt in zwei Schritten. Der erste Schritt, die Anwendung des Kriterienkatalogs auf IntServ/RSVP unabhängig von der Netztechnologie, wurde schon in Abschnitt 5.1.3 durchgeführt. Der zweite Schritt, die Änderungen aufgrund der Netztechnologie, wird nun für Ethernet durchgeführt. Es werden nur die Kriterien aufgeführt, die einer Änderung unterworfen sind, die restlichen können Abschnitt 5.1.3 entnommen werden:

Es werden die Kriterien für zwei Typen des Ethernets bestimmt. Der erste Typ ist ein Shared-Ethernet, d.h. die Sender greifen mit dem CSMA/CD-Verfahren auf ein gemeinsam genutztes Medium zu. Zu beachten ist daß es bei diesem Typ den Guaranteed Service nicht gibt. Der zweite Typ ist ein Switched-Ethernet, hier gibt es nur einen Sender pro Segment (Microsegmentation) und das CSMA/CD-Verfahren spielt keine Rolle (außer der Verzögerung von 9,6 Mikrosekunde vor dem Zugriff auf das Medium).

User→Transfer→Transfer Delay (Shared)	
Voraussetzungen:	Ein Fluß f verwendet Controlled-Load Service
Aussage:	Die maximale Übertragungsverzögerung ist nicht beschränkt.
	Die minimale Übertragungsverzögerung ist durch MPL beschränkt.
Voraussetzungen:	Ein Fluß verwendet Best Effort
Aussage:	Die maximale Übertragungsverzögerung ist nicht beschränkt.
	Die minimale Übertragungszeit ist durch MPL beschränkt.

User→Transfer→Jitter (Shared)	
Voraussetzungen:	Verwendung des Controlled-Load Service
Aussage:	Der maximale Jitter ist nicht beschränkt.
Voraussetzungen:	Ein Fluß verwendet Best Effort
Aussage:	Der maximale Jitter ist nicht beschränkt.

User→Transfer→(Congestion) Loss (Shared)	
Voraussetzungen:	Ein Fluß f verwendet Controlled-Load Service
Aussage:	Der maximale Verlust ist niedrig
	Der minimale Verlust kann Null sein
Voraussetzungen:	Ein Fluß verwendet Best Effort Service
Aussage:	Der maximale Verlust kann hundert Prozent sein.
	Der minimale Verlust kann Null sein.

User→Transfer→Transfer Rate (Shared)	
Voraussetzungen:	Ein Fluß f verwendet Controlled-Load Service
Aussage:	Die maximale Übertragungsrate ist max(TBR) Die minimale Übertragungsrate ist TBR verringert um den maximalen Verlust (Loss).
Voraussetzungen:	Ein Fluß verwendet Best Effort
Aussage:	Die maximale Übertragungsrate ist durch den Wert von `NON_RESV_SEND_LIMIT` beschränkt. Die minimale Übertragungsrate ist Null.

User→Transfer→Transfer Delay (Switched)	
Voraussetzungen:	Ein Fluß f verwendet Guaranteed Service
Aussage:	Die maximale Übertragungsverzögerung ist beschränkt. Für die Übertragung der Nachrichten werden diese beim Ethernet in Aggregate eingeteilt. Mit einem Prioritätsscheduling, daß Switches und Brigdes unterstützen, kann zwar für die Nachrichten in den Aggregaten eine maximale Übertragungsverzögerung erreicht werden. Der Wert für die maximale Übertragungsverzögerung ist aufgrund der Übertragung in Aggregaten schlechter als für ATM und Sonet/SDH einzuschätzen. Die minimale Übertragungsverzögerung ist durch MPL beschränkt.
Voraussetzungen:	Ein Fluß f verwendet Controlled-Load Service
Aussage:	Die maximale Übertragungsverzögerung ist nicht beschränkt. Die minimale Übertragungszeit ist durch MPL beschränkt.
Voraussetzungen:	Ein Fluß verwendet Best Effort
Aussage:	Die maximale Übertragungsverzögerung ist nicht beschränkt. Die minimale Übertragungszeit ist durch MPL beschränkt.

User→Transfer→Transfer Delay (Switched)	
Voraussetzungen:	Ein Fluß f verwendet Guaranteed Service
Aussage:	Der maximale Jitter ist beschränkt. Wegen der des schlechteren Werts für die maximale Übertragungsrate, ist auch für den maximalen Jitter ein schlechterer Wert zu erwarten als bei Sonet/SDH und ATM.
Voraussetzungen:	Ein Fluß f verwendet Controlled-Load Service
Aussage:	Der maximale Jitter ist nicht beschränkt. Die minimale Übertragungszeit ist durch MPL beschränkt.
Voraussetzungen:	Ein Fluß verwendet Best Effort
Aussage:	Der maximale Jitter ist nicht beschränkt. Die minimale Übertragungszeit ist durch MPL beschränkt.

Provider→Performance Management→Bandwidth	
Voraussetzungen:	keine
Aussage:	Die verfügbare Bandbreite auf dem Übertragungsmedium beträgt ca. 98% der Übertragungsbandbreite. Ein Teil dieser Bandbreite wird für die Übertragung von RSVP-Nachrichten genutzt, ca. 60 bps pro Fluß.

5.4 DiffServ über Sonet/SDH

Sonet/SDH stellt eine Verbindung fester Bandbreite bereit. Analog zu Abschnitt 5.1 können über diese IP-Pakete in PPP-Frames übertragen werden.

Ein zentraler Bestandteil von DiffServ sind die Per-Hop Behaviors (PHBs). Wie die PHBs für Aggregate in einem Sonet/SDH-Netz erzeugt werden können, wird in den zwei folgenden Abschnitten gezeigt.

5.4.1 Expedited Forwarding PHB

Ein Scheduling-Algorithmus, der ein EF-PHB haben soll, muß folgende Bedingungen erfüllen [JNP 99]:

1. wenig Verlust
2. geringe Übertragungszeit
3. wenig Jitter
4. zugesicherte Bandbreite

Das erste Beispiel für einen Scheduler, mit dem das EF-PHB erzielt werden kann, ist ein Prioritätsscheduler (siehe Abbildung 81). Es werden immer sendebereite Pakete der

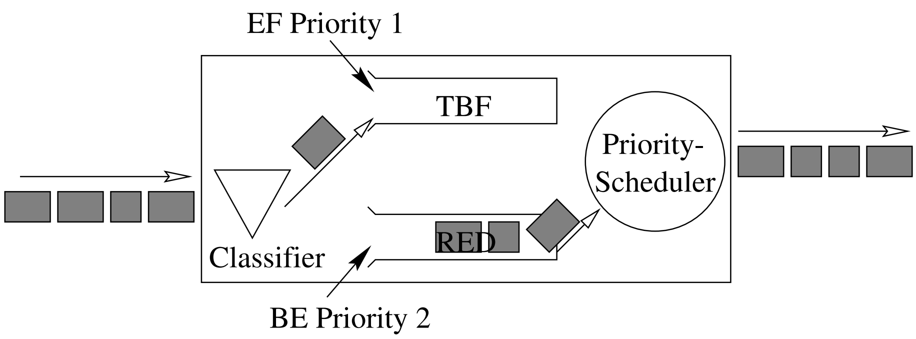

Abbildung 81: Expedited Forwarding PHB mit Prioritätsscheduling

höheren Priorität zuerst gesendet. Daß der Verkehr einer höheren Priorität keinen unbeschränkten Einfluß auf den Verkehr niedrigerer Priorität nehmen kann, verhindert ein *Token Bucket Filter* Algorithmus (TBF, siehe Abschnitt 2.3.2).

In der Klasse für den Best-Effort-Verkehr wird das Verfahren *Random Early Detection* (RED) eingesetzt. Ziel dieses Verfahrens ist es bei Anzeichen eines langfristigen Staus durch das Verwerfen von PDUs den TCP-Verkehr zu drosseln.

Eine zweite Möglichkeit für einen Scheduler ist der *Class Based Queuing* (CBQ) Scheduler (siehe Abbildung 82). Dieser Scheduler stellt einer Klasse Bandbreite bis zu einem definierten Wert bereit.

5.4.2 Assured Forwarding PHB Group

Eine Möglichkeit einen Scheduler für die AF-PHB-Gruppe zu implementieren beruht auf dem CBQ. Für jede AF-Klasse wird eine Klasse im CBQ eingerichtet, dieser Klasse wird

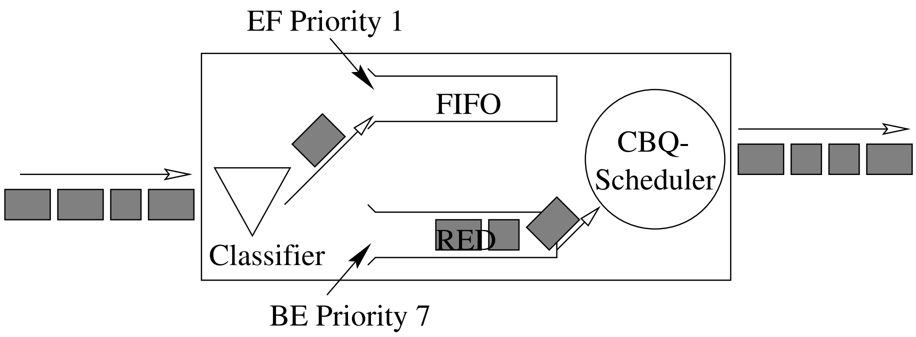

Abbildung 82: Expedited Forwarding PHB mit CBQ-Scheduling

ein Minimum an Bandbreite zugesichert. Als ein Verfahren für das Verwerfen von Paketen, daß den Bedingungen der AF-PHB-Gruppe entspricht, wählen wir GRED.

Das Verfahren *generalized RED* (GRED) [lin 99a] entspricht dem RED-Verfahren, jedoch werden hier die Prioritäten der AF-Klasse für die Auswahl der PDUs für das Dropping verwendet.

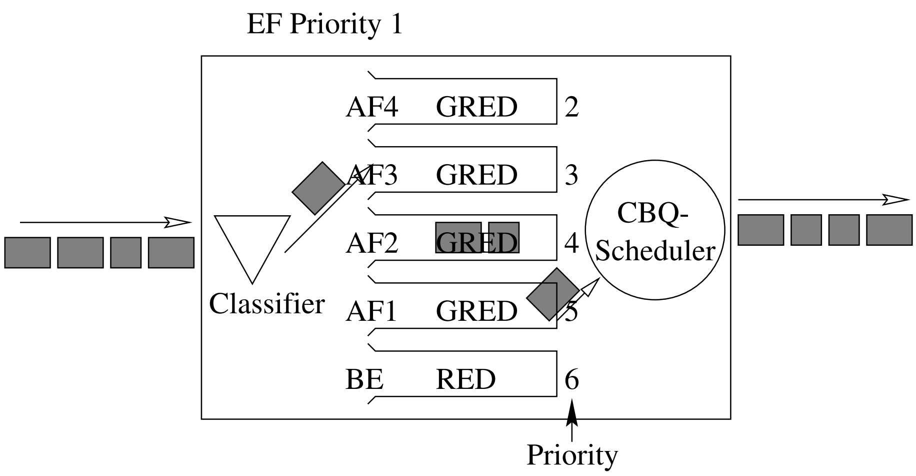

Abbildung 83: Assured Forwarding PHB Group mit CBQ-Scheduling

5.4.3 Anwendung des Kriterienkatalogs

Für die Anwendung des Kriterienkatalogs werden Dienstgüten gebraucht. Es sollen die Dienstgüten

- Premium Service
- Assured Service

aus Abschnitt 2.2 verwendet werden.

Die Flüsse, die diese Dienstgüten erhalten, werden durch das Tupel (Source IP Address, Differentiated Service CodePoint (DSCP), Destination IP Address) identifiziert. Die Flüsse werden beim Eintritt in das Netz auf die Einhaltung eines Verkehrsprofils geprüft, dies soll mit einem Token Bucket Filter erfolgen.

Für einen Microflüsse, der den selben Identifikator besitzen, müssen die Aussagen, die für den Gesamtfluß (alle Microflüsse mit diesem Identifikator) gemacht werden, nicht gelten. Da es nicht sichergestellt ist, daß alle Microflüsse mit diesem Identifikator das Verkehrsprofil des Gesamtflusses einhalten, ist die Voraussetzung für den Erhalt der Dienstgüte nicht gegeben. Dies zeigt, wie eine Anforderung an die Dienstgüte eines Microflusses, aufgrund nicht zutreffender Voraussetzungen, nicht erfüllt werden kann.

Analog bei der Anwendung des Kriterienkatalogs auf IntServ/RSVP wird auch bei DiffServ der Kriterienkatalog erst unabhängig von der Netztechnologie angewandt. Dann folgen die Änderungen aufgrund der Netztechnologie.

Anwendung des Kriterienkatalogs auf DiffServ unabhängig von der Netztechnologie:

User→Access→Access Delay	
Voraussetzungen:	keine
Kriterium:	Die maximale Zugangszeit ist Null.

User→Release→Release Delay	
Voraussetzungen:	keine
Aussage:	Die maximale Abbauzeit eines Zugangs ist Null.

User→Transfer→Transfer Delay	
Voraussetzungen:	Ein Fluß verwendet den Premium Service
Aussage:	Die maximale Übertragungsverzögerung ist beschränkt. Die maximale Übertragungsverzögerung ist bei vergleichbaren Bedingungen schlechter als bei IntServ/RSVP einzuschätzen (siehe 5.3.4)
Voraussetzungen:	Ein Fluß verwendet den Assured Service
Aussage:	Die maximale Übertragungsverzögerung ist nicht beschränkt. Die minimale Übertragungsverzögerung ist durch MPL beschränkt.
Voraussetzungen:	Ein Fluß verwendet Best Effort
Aussage:	Die maximale Übertragungsverzögerung ist nicht beschränkt. Die minimale Übertragungszeit ist durch MPL beschränkt.

User→Transfer→Jitter	
Voraussetzungen:	Ein Fluß verwendet den Premium Service
Aussage:	Der maximale Jitter ist beschränkt. Dies erfolgt aus der Tatsache, daß die maximale Übertragungsverzögerung beschränkt ist. Dadurch, daß die maximale Übertragungsverzögerung größer als bei IntServ/RSVP einzuschätzen ist, folgt auch, daß der maximalen Jitter größer als bei IntServ/RSVP ist.
Voraussetzungen:	Ein Fluß verwendet den Assured Service
Aussage:	Der maximale Jitter ist nicht beschränkt.
Voraussetzungen:	Ein Fluß verwendet Best Effort
Aussage:	Der maximale Jitter ist nicht beschränkt.

User→Transfer→(Congestion) Loss	
Voraussetzungen:	Ein Fluß verwendet den Premium Service
Aussage:	Der Verlust aufgrund von Stauungen ist Null
Voraussetzungen:	Ein Fluß verwendet den Assured Service
Aussage:	Der maximale Verlust ist niedrig Der minimale Verlust kann Null sein.
Voraussetzungen:	Ein Fluß verwendet Best Effort Service
Aussage:	Der maximale Verlust kann hundert Prozent sein. Der minimale Verlust kann Null sein.

User→Transfer→Transfer Rate	
Voraussetzungen:	Ein Fluß verwendet den Premium Service
Aussage:	Die maximale Übertragungsrate ist TBR. TBR ist die Token Bucket Rate des Token Bucket Filter der beim Eintritt des Flusses ins Netz, diesen auf sein Verkehrsprofil prüft. Die minimale Übertragungsrate ist TBR.
Voraussetzungen:	Ein Fluß verwendet den Aussured Service
Aussage:	Die maximale Übertragungsrate ist TBR. Die minimale Übertragungsrate ist TBR.
Voraussetzungen:	Ein Fluß verwendet Best Effort
Aussage:	Die maximale Übertragungsrate ist die maximale Übertragungsrate auf dem Medium. Die minimale Übertragungsrate ist Null.

User→Protection→Theft of Service	
Voraussetzungen:	keine
Aussage:	Ein Schutz ist nach [NBBB 98][BBC+ 98] gewährleistet.

User→Protection→Listening	
Voraussetzungen:	keine
Aussage:	Schutz vor dem Abhören ist möglich. Das Abhören eines Flusses kann, wie bei IntServ/RSVP, mit IPSEC verhindert werden [Atki 95a][Atki 95c].

User→Protection→Change	
Voraussetzungen:	keine
Aussage:	Schutz vor unbemerkten Veränderung ist gegeben. [Atki 95b] bietet den Authentification Header, um die Daten vor einer Veränderung zu Schützen.

Provider→Configuration Management→Configuration Delay	
Voraussetzungen:	keine
Aussage:	DiffServ besitzt kein Verfahren, um die Flüsse einzurichten. Es muß daher im schlechtesten Fall jeder neue Fluß manuell eingerichtet werden. Dies umfaßt die Konfiguration der auf dem Pfad des Flusses liegenden Router. Da diese Arbeit für jeden neuen Fluß anfallen kann ist der Konfigurationsaufwand höher als bei IntServ/RSVP zu bewerten.

Provider→Fault Management→Repair Delay	
Voraussetzungen:	keine
Aussage:	DiffServ verfügt über kein Verfahren Fehler automatisch zu korrigieren. Eine manuelle Reparatur wird wahrscheinlich mehrere Minuten oder Stunden dauern. Im Gegensatz dazu kann IntServ/RSVP Fehler automatisch umgehen.

Provider→Performance Management→Bandwidth	
Voraussetzungen:	keine
Aussage:	DiffServ benötigt weniger Bandbreite als IntServ/RSVP, da keine RSVP-Nachrichten auf dem Medium transportiert werden müssen.

Provider→Performance Management→Memory	
Voraussetzungen:	keine
Aussage:	DiffServ benötigt weniger Speicher als IntServ/RSVP, da hier keine Zustände für Flüsse gehalten werden.

Provider→Performance Management→Processing Power	
Voraussetzungen:	keine
Aussage:	Die Verarbeitungsleistung für DiffServ ist geringer als für IntServ/RSVP einzuschätzen. Es müssen keine RSVP-Nachrichten verarbeitet werden. Die gesamte Verarbeitungsleistung steht den Daten zur Verfügung.

Provider→Performance Management→Resource Release Delay	
Voraussetzungen:	keine
Aussage:	DiffServ bietet kein Verfahren, um die Ressourcen freizugeben. Erfolgt dies manuell wird es sicherlich mehrere Minuten bis Stunden dauern.

Änderungen aufgrund der Netztechnologie:

Provider→Performance Management→Bandwidth	
Voraussetzungen:	keine
Aussage:	DiffServ benötigt weniger Bandbreite als IntServ/RSVP, da keine RSVP-Nachrichten auf dem Medium transportiert werden müssen. Es stehen 95% der Übertragungsbandbreite des Mediums zur Verfügung.

5.5 DiffServ über ATM

Ein zentraler Bestandteil der DiffServ-Architektur sind die Per-Hop Behaviors (PHB). In den folgenden zwei Abschnitten wird gezeigt, wie EF-PHB und AF-PHB mit virtuellen Verbindungen von ATM erzeugt werden.

5.5.1 Expedited Forwarding PHB

EF PHB soll laut [JNP 99] für den Aufbau eines Dienstes mit folgenden Anforderungen an die Dienstgüte verwendbar sein:

1. wenig Verlust
2. geringe Übertragungszeit
3. wenig Jitter
4. zugesicherte Bandbreite

Die Anforderungen nach wenig Jitter und geringer Übertragungszeit lassen nur die beiden Dienstklassen CBR und rtVBR der ATM Layer in Frage kommen [ATM-UNI 94][ATM-UNI 96].

Für die Bandbreite wird gefordert, daß ihr über alle Zeiträume, die mindestens so lang sind, wie für das Senden einer MTU mit der geforderten Bandbreite gebraucht wird, wenigstens eine vorgegebene Menge zugesichert ist. Eine maximale Bandbreite sollte ebenfalls spezifiziert werden, damit der Einfluß auf den anderen Verkehr beschränkt bleibt. rtVBR ist für EF besser geeignet, da hier Bursts (IP-Pakete) mit einer Bitrate bis hin zur verfügbaren Bitrate des Mediums transportiert werden können. Wohingegen die Übertragung bei CBR mit der Peak Cell Rate erfolgt, die in der Regel kleiner ist als die verfügbare Übertragungsrate des Mediums. Damit kommt rtVBR der Anforderung nach geringer Übertragungszeit mehr entgegen [MAK 99].

Traffic Descriptor	
Peak Cell Rate (PCR) (CLP=0+1)	Line Rate
Sustained Cell Sate (SCR)	configured Rate
Maximum Burst Size (MBS)	maximum PDU Size

Tabelle 20: EF-PHB mit rtVBR

5.5.2 Assured Forwarding PHB Group

Die Assured Forwarding PHB Group stellt mehrere AF Klassen bereit, deren Pakete Prioritäten für das Verwerfen besitzen. Einer AF Klasse wird eine minimale Bandbreite, innerhalb derer es geringen Verlust gibt, zugeordnet, die jedoch überschritten werden kann. Der zusätzliche Verkehr kann die vorhandenen Ressourcen langfristig überschreiten und damit zu Stauungen führen. Die Stauungen werden durch das Verwerfen von Paketen beseitigt. Müssen Pakete verworfen werden, dann werden von einer Menge diejenigen mit der höheren Priorität zuerst ausgewählt werden. ATM Dienstklassen unterstützen maximal mit der Cell

Loss Priority (CLP) zwei Prioritäten. AF-PHB kann aber mehr Priortäten unterstützen, daher wäre die Verwendung der CLP eine Einschränkung.

Eine Lösung beruht auf der ABR Dienstklasse und einem aktiven Warteschlangenverwaltungsverfahren, wie z.B. das GRED-Verfahren [MAK 99]. Mit Minimum Cell Rate (MCR) kann bei ABR eine minimale Bandbreite reserviert werden. Das ATM-Netz teilt dem Sender die momentan zusätzlich verfügbare Bandbreite mit. Mit dieser Bandbreite können Pakete mit minimalem Verlust gesendet werden. Ein Verfahren wie *generalized RED* (GRED) [lin 99a] sorgt dafür, daß die Pakete mit höherer Verlustpriorität zuerst gelöscht werden, wenn die Länge der Warteschlange für die virtuelle Verbindung anwächst.

Traffic Descriptor	
Peak Cell Rate (PCR) (CLP=0+1)	Line Rate
Minimum Cell Rate (MCR)	minimum Bandwidth allocated to an AF Class

Tabelle 21: AF-PHB mit ABR

5.5.3 Anwendung des Kriterienkatalogs

Die Anwendung des Kriterienkatalogs erfolgt in zwei Schritten. Der erste Schritt, die Anwendung des Kriterienkatalogs auf DiffServ unabhängig von der Netztechnologie, wurde schon in Abschnitt 5.4.3 durchgeführt. Der zweite Schritt, die Änderungen aufgrund der Netztechnologie, wird nun für ATM durchgeführt. Es werden nur die Kriterien aufgeführt, die einer Änderung unterworfen sind, die restlichen können Abschnitt 5.4.3 entnommen werden:

Provider→Performance Management→Bandwidth	
Voraussetzungen:	keine
Aussage:	DiffServ kann die ganze Bandbreite der virtuellen Verbindung nutzen. Eine virtuelle Verbindung kann maximal 80% der Übertragungsbandbreite des Übertragungsmediums nutzen.

5.6 IntServ/RSVP über DiffServ

DiffServ und IntServ/RSVP haben ihre Vor- und Nachteile. Die wesentlichen Nachteile von IntServ/RSVP sind die Zustände und der Verarbeitungsaufwand für jeden Fluß. In großen Netzen mit dementsprechend großer Anzahl an Flüssen kann dies zu Engpässen führen. DiffServ arbeitet mit Aggregaten von Flüssen und kennt daher dieses Problem nicht. In diesem Abschnitt wird gezeigt, wie IntServ/RSVP über ein DiffServ-Netz funktioniert [ZYB+ 99]. Damit können in Bereichen eines Netzes die Nachteile von IntServ/RSVP durch die Vorteile von DiffServ umgangen werden.

Das Prinzip für IntServ/RSVP über ein DiffServ-Netz ist vergleichbar mit IntServ/RSVP über ein Switched-Ethernet. In einem Switched-Ethernet werden durch Setzen der User Priority im Frame-Header die PDUs der IntServ-Flüsse Verkehrsklassen mit einer angemessenen Dienstgüte zugewiesen, in einem DiffServ-Netz erfolgt dies durch Setzen des Differentiated Service Code Point (DSCP) im Differentiated Service Feld (DS-Feld) eines Paket-Headers. Das Setzen des DSCP erfolgt in einem IntServ-fähigen Gerät (Host oder Router) vor dem Eintritt einer PDU in das DiffServ-Netz. Für das Admission Control gibt es drei Möglichkeiten:

- **Statische Bereitstellung von Ressourcen**
  DiffServ wird behandelt als würde es Verbindungen mit fester Dienstgüte zwischen IntServ/RSVP-fähigen Geräten bereitstellen. Das letzte IntServ/RSVP-fähige Gerät vor dem DiffServ-Netz übernimmt das Admission Control für diese Verbinungen.

- **Dynamische Bereitstellung von Ressourcen mit RSVP**
  Das DiffServ-Netz besitzt RSVP-fähige Geräte. Jedes RSVP-fähige Gerät übernimmt das Admission Control für die Verbinungen zum nächsten RSVP-fähigen Gerät. Die Information über die IntServ-Dienstgüte wird genutzt, um für die Fluß-Aggregate ausreichend Ressourcen zu reservieren.

- **Dynamische Bereitsellung von Ressourcen mit Aggregat-RSVP** [BDFI 99]
  Das DiffServ-Netz besitzt Aggregat-RSVP-fähige Geräte. Das letzte RSVP- und Aggregat-RSVP-fähige Gerät vor dem DiffServ-Netz erzeugt für die Microflüsse Aggregat-RSVP-PDUs. Aggregat-RSVP ist ein Signalisierungsprotokoll für die Reservierung von Aggregat-Flüssen. Im DiffServ-Netz wird Aggregat-RSVP analog zu RSVP in einem IntServ-Netz eingesetzt. Die RSVP-PDUs werden wie Daten im DiffServ-Netz behandelt.

5.6.1 Anwendung des Kriterienkatalogs

Es soll nun der Kriterienkatalog auf das DiffServ-Netz, mit RSVP und Aggregat-RSVP, angewendet werden. Die Änderungen für die Kriterien aus 5.4.3 sind:

Dynamische Bereitstellung von Ressourcen mit RSVP:

Provider→Configuration Management→Configuration Delay	
Voraussetzungen:	keine
Aussage:	Die Konfiguration für DiffServ/RSVP umfaßt das Setzen von Parametern des Traffic Control, des Admission Control und des Policy Control. Diese Arbeit muß im Idealfall nur für die Inbetriebnahme eines Netzes erfolgen.

Provider→Fault Management→Repair Delay	
Voraussetzungen:	Der Fehler kann umgangen werden.
Aussage:	DiffServ/RSVP besitzt ein Verfahren, um Fehler (z.B. Routerausfall oder Leitung unterbrochen) zu umgehen. Dieses Verfahren stellt eine Reservierung über einen alternativen Pfad zum Empfänger her.

Provider→Performance Management→Resource Release Delay	
Voraussetzungen:	keine
Aussage:	Die maximale Zeit für das Freigeben von Ressourcen ist beschränkt. Die Freigabe der Ressourcen erfolgt spätestens nach Ablauf des Timers für die Lebenszeit des Reservierungszustands in einem RSVP-Prozeß. Die Lebenszeit für einen Timer ist < 2 Minuten (Wert nach [BZB$^+$ 97]). Da die Timer der Reservierungen eines Flusses nacheinander ablaufen können, kann sich die Freigabe der letzten Ressourcen einige Minuten hinziehen. Die Zeit für den Abbau der virtuellen Verbindung fällt dabei kaum ins Gewicht. Die minimale Freigabezeit der Ressourcen ist durch MPL beschränkt.

Provider→Performance Management→Bandwidth	
Voraussetzungen:	keine
Aussage:	Ein Teil der Bandbreite wird für die Übertragung von RSVP-Nachrichten genutzt, ca. 60 bps pro Fluß. Der Bedarf an Bandbreite entspricht IntServ/RSVP.

Provider→Performance Management→Memory	
Voraussetzungen:	keine
Aussage:	Der Speicherbedarf für Zustände bei DiffServ/RSVP entspricht dem von IntServ/RSVP. Bei DiffServ/RSVP wird für jeden Fluß ein Zustand im RSVP-fähigen Gerät (Host und Router) erzeugt. Die Größe des Zustands ist von der Art des Flusses (unicast oder multicast) und auch von der Implementierung der RSVP-Prozesse abhängig. Die Größe eines Zustand wird aber > 100 Byte sein ([BrZh 97]). Der Speicherbedarf für Puffer ist größer als bei DiffServ einzuschätzen.

Provider→Performance Management→Processing Power	
Voraussetzungen:	keine
Aussage:	Die Verarbeitungsleistung, die bei DiffServ/RSVP erbracht werden muß, enspricht der Verarbeitungsleistung die bei IntServ/RSVP für die Bearbeitung von RSVP-Nachrichten erbracht wird. Neben der eigentlichen Aufgabe, das Weiterleiten von Nachrichten, müssen in den RSVP-fähigen Geräten (Host und Router) die RSVP-Nachrichten bearbeitet werden. Die RSVP-Nachrichten werden nicht nur zum Auf- und Abbau einer Reservierung, sondern auch zu deren Weiterbestehen benötigt. Zu diesem Zweck werden in regelmäßigen Abständen (ca. 30 Sekunden [BZB+ 97]) Path- und Resv-Nachrichten gesendet.

Dynamische Bereitstellung von Ressourcen mit Aggregat-RSVP:

Provider→Configuration Management→Configuration Delay	
Voraussetzungen:	keine
Aussage:	Die Konfiguration für DiffServ/RSVP umfaßt das Setzen von Parametern des Traffic Control, Admission Control und Policy Control. Diese Arbeit muß im Idealfall nur für die Inbetriebnahme eines Netzes erfolgen.

Provider→Fault Management→Repair Delay	
Voraussetzungen:	Der Fehler kann umgangen werden.
Aussage:	DiffServ/RSVP besitzt ein Verfahren, um Fehler (z.B. Routerausfall oder Leitung unterbrochen) zu umgehen. Dieses Verfahren stellt eine Reservierung über einen alternativen Pfad zum Empfänger her.

Provider→Performance Management→Resource Release Delay	
Voraussetzungen:	keine
Aussage:	Die maximale Zeit für das Freigeben von Ressourcen ist beschränkt. Die Freigabe der Ressourcen erfolgt spätestens nach Ablauf des Timers für die Lebenszeit des Reservierungszustands in einem RSVP-Prozeß. Die Lebenszeit für einen Timer ist $<$ 2 Minuten (Wert nach [BZB+ 97]). Da die Timer der Reservierungen eines Flusses nacheinander ablaufen können, kann sich die Freigabe der letzten Ressourcen einige Minuten hinziehen. Die Zeit für den Abbau der virtuellen Verbindung fällt dabei kaum ins Gewicht. Die minimale Freigabezeit der Ressourcen ist durch MPL beschränkt.

Provider→Performance Management→Bandwidth	
Voraussetzungen:	keine
Aussage:	Ein Teil der Bandbreite wird für die Übertragung von Aggregat-RSVP-Nachrichten und den RSVP-Nachrichten genutzt. Werden die Aggregat-Flusse nicht zu häufig verändert, kann die verwendete Bandbreite für Aggregat-RSVP-Nachrichten vernachlässigt werden.

Provider→Performance Management→Memory	
Voraussetzungen:	keine
Aussage:	Der Speicherbedarf für Aggregat-RSVP-Zustände kann aufgrund deren geringen Anzahl auch vernachlässigt werden.

Provider→Performance Management→Processing Power	
Voraussetzungen:	keine
Aussage:	Die Verarbeitungsleistung kann für Aggregat-RSVP-Nachrichten aufgrund deren geringen Anzahl vernachlässigt werden und entspricht in etwa DiffServ (ohne Aggregat-RSVP).

5.7 Zusammenfassung

Die Ergebnisse des Vergleichs von IntServ und DiffServ ist in Tabelle 22 zusammengefaßt.

Kriterium	IntServ	DiffServ
Access Delay		$\oplus$
Release Delay		
Transfer Delay	$\oplus$	
Jitter	$\oplus$	
Loss		
Transfer Rate		
Theft of Service		
Listening		
Change		
Configuration Delay	$\oplus$	
Repair Delay	$\oplus$	
Bandwidth		$\oplus$
Memory		$\oplus$
Processing Power		$\oplus$
Resource Release Delay	$\oplus$	

Tabelle 22: IntServ DiffServ

Mit $\oplus$ wird angegeben, welche Technologie bei diesem Kriterium besser abschneidet. Fehlt ein $\oplus$, dann sind die Technologien für ein Kriterium ebenbürtig. Die Kriterien *Transfer Delay*, *Jitter*, *Loss*, *Transfer Rate* sind von der verwendeten Dienstgüte abhängig. Für die Dienstgüteparameter maximalen Jitter und die maximale Übertragungszeit kann IntServ (unter vergleichbaren Bedingungen) bessere Werte garantieren, deshalb das $\oplus$.

6 Ergebnis und weiterführende Arbeiten

Als Ergebnis dieser Arbeit kann festgehalten werden, daß keine der Entwicklungen DiffServ und IntServ/RSVP der anderen eindeutig überlegen ist.

Weiter ist festzustellen, daß die Wahl der Netztechnologie von Bedeutung ist. So ist zum Beispiel der Einsatz eines Shared-Ethernet in Bereichen, wo eine maximale Übertragungszeit verlangt wird, nicht sinnvoll. In Bereichen in denen Wert auf einen geringen Jitter gelegt wird, wird ATM seine Stärken ausspielen.

Wie stark diese Vor- und Nachteile ins Gewicht fallen, ist vom Einsatzgebiet abhängig.

Für manche Netze kann es sinnvoll sein, beide Technologien einzusetzen, jede in einem bestimmten Bereich. Dies kann es ermöglichen die Grenzen der einen Technologie durch die andere zu umgehen. So könnte als zukünftige Arbeit der Einsatz der Technologien für ein reales Netz untersucht werden. Hier kann dann der Kriterienkatalog verwendet werden, um die Wahl für eine Technologie im ganzen oder in einem Bereich eines Netzes zu treffen. In realen Netzen stehen zusätzliche Informationen bereit, die für einige oder alle Kriterien genauere oder zusätzliche Aussagen ermöglichen.

Abkürzungsverzeichnis

A

AAL	ATM Adaption Layer
ABR	Available Bit Rate
AF	Assured Forwarding
ATM	Asynchronous Tranfer Mode
ATM UNI	Asynchronous Tranfer Mode User-Network Interface

B

BE	Best Effort

C

CBR	Constant Bit Rate
CBQ	Class Bases Queuing
CLIP	Classical IP over ATM
CLS	Controlled Load Service
CSMA/CD	Carrier Sense Multiple Access with Collision Detection

D

DEE	Daten-End-Einrichtung
DiffServ	Differentiated Services
DTE	Data Terminal Equipment

E

ELAN	Emulated LAN

F

FTP	File Transfer Protocol

G

GS	Guaranteed Service

H

HDLC	High-Level Data Link Control

I

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IntServ	Integrated Services
IP	Internet Protocol
ISO	International Standards Organization
ISP	Internet Service Provider
ITU-T	International Telecommunications Union - Telecommunications

L

LANE	LAN Emulation

LLC/SNAP	Logical Link Control/SubNetwork Attachment Point
M	
MAC	Medium Access Control
MPOA	MuliProtocol Over ATM
MTU	Maximum Transmission Unit
N	
nrtVBR	Non-Real-Time Variable Bit Rate
O	
OSI	Open System Interconnection
OSI-RM	Open System Interconnection Referenzmodell
P	
PDU	Protocol Data Unit
PPP	Point to Point Protocol
PVC	Permanent Virtual Connection
Q	
QoS	Quality of Service
R	
RFC	Request For Comments
RSVP	Resource ReSerVation Protocol
RTD	Round Trip Delay
rtVBR	Real-Time Variable Bit Rate
S	
SAP	Service Access Point
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEAL	Simple and Efficient Adaption Layer
SMTP	Simple Mail Transfer Protocol
SVC	Switched Virtual Connection
T	
TCP	Transmission Control Protocol
TTL	Time To Live
U	
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
V	
VC	Virtual Connection

Literatur

[Adam 97] ADAMCZYK, M.: *Konzept zur Überwachung des Quality of Service für das Händlernetz der BMW AG.* Diplomarbeit, Technische Universität München, August 1997.

[af- 97] *LAN Emulation over ATM, Version 2 — LUNI Specification.* Approved Specification af-lane-0084.000, ATM Forum, Juli 1997.

[all 95] *ATM Internetworking.* Specification, Cisco Systems, Inc., Mai 1995.

[Anna 98] ANNA CHARNY: *Delay Bounds In a Network With Aggregate Scheduling.* Technischer Bericht Cisco Systems, 1998.

[Atki 95a] ATKINSON, R.: *RFC 1825: Security Architecture for the Internet Protocol.* RFC, IETF, August 1995.

[Atki 95b] ATKINSON, R.: *RFC 1826: IP Authentication Header.* RFC, IETF, August 1995.

[Atki 95c] ATKINSON, R.: *RFC 1827: IP Encapsulating Security Payload (ESP).* RFC, IETF, August 1995.

[ATM Europe 97] *ATM in Europe: The User Handbook.* Specification, ATM Forum, Juli 1997.

[ATM-LANE 99] *LAN Emulation over ATM Version 2 - LNNI Specification.* Specification af-lane-0112.000, ATM Forum, Februar 1999.

[ATM-MPOA 99] *Multi-Protocol Over ATM Version 1.1.* Specification af-mpoa-0114.000, ATM Forum, Mai 1999.

[ATM-TM 96] *Traffic Management Specification Version 4.0.* Specification af-tm-0056.000, ATM Forum, April 1996.

[ATM-TM 99] *Traffic Management Specification Version 4.1.* Specification af-tm-0121.000, ATM Forum, März 1999.

[ATM-UNI 94] *ATM User-Network Interface Specification Version 3.1.* Specification af-uni-0010.002, ATM Forum, September 1994.

[ATM-UNI 96] *ATM User-Network Interface (UNI) Signalling Specification Version 4.0.* Specification af-sig-0061.000, ATM Forum, Juli 1996.

[BBC+ 98] BLAKE, S., D. BLACK, M. CARLSON, E. DAVIES, Z. WANG und W. WEISS: *RFC 2475: An Architecture for Differentiated Services.* RFC, IETF, Dezember 1998.

[BDFI 99] BAKER, FRED, BRUCE DAVIE, FRANCOIS LE FAUCHEUR und CAROL ITURRALDE: *Aggregation of RSVP for IPv4 and IPv6 Reservations.* Internet Draft, IETF, 12 1999.

[BeO' 97] BERGER, L. und T. O'MALLEY: *RFC 2207: RSVP Extensions for IPSEC Data Flows.* RFC, IETF, September 1997.

[Berg 98a] BERGER, L.: *RFC 2379: RSVP over ATM Implementation Guidelines.* RFC, IETF, August 1998.

[Berg 98b] BERGER, L.: *RFC 2380: RSVP over ATM Implementation Requirements.* RFC, IETF, August 1998.

[Bern 99] BERNET, Y.: *Format of the RSVP DCLASS Object.* Internet Draft, IETF, 10 1999.

[BLT 99] BAKER, FRED, BOB LINDELL und MOHIT TALWAR: *RSVP Cryptographic Authentication.* Internet Draft, IETF, 03 1999.

[BrZh 97] BRADEN, R. und L. ZHANG: *RFC 2209: Resource ReSerVation Protocol (RSVP) — Version 1 Message Processing Rules.* RFC, IETF, September 1997.

[BZB+ 97] BRADEN, ED., R., L. ZHANG, S. BERSON, S. HERZOG und S. JAMIN: *RFC 2205: Resource ReSerVation Protocol (RSVP) — Version 1 Functional Specification.* RFC, IETF, September 1997.

[CBB+ 98] CRAWLEY, E., L. BERGER, S. BERSON, F. BAKER, M. BORDEN und J. KRAWCZYK: *RFC 2382: A Framework for Integrated Services and RSVP over ATM.* RFC, IETF, August 1998.

[GaBo 98] GARRETT, M. und M. BORDEN: *RFC 2381: Interoperation of Controlled-Load Service and Guaranteed Service with ATM.* RFC, IETF, August 1998.

[Hals 96] HALSALL, FRED: *Data Communications, Computer Networks and Open Systems.* Addison–Wesley, vierte Auflage, 1996.

[HBWW 99] HEINANEN, J., F. BAKER, W. WEISS und J. WROCLAWSKI: *RFC 2597: Assured Forwarding PHB Group.* RFC, IETF, Juni 1999.

[HeAb 93] HEGERING, H.-G. und S. ABECK: *Integriertes Netz– und Systemmanagement.* Addison–Wesley, 1993.

[Hein 93] HEINANEN, JUHA: *RFC 1483: Multiprotocol Encapsulation over ATM Adaptation Layer 5.* RFC, IETF, Juli 1993.

[HeLa 92] HEGERING, HEINZ-GERD und ALFRED LÄPPLE: *Ethernet – Basis für Kommunikationsstrukturen.* Datacom-Verlag, 1992.

[IEEE-P802.1D/D17] IEEE-802.1-WG: *IEEE P802.1D/D17 - Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Common specifications – Part 3: Media Access Control (MAC) Bridges.* Technischer Bericht IEEE, Mai 1998.

[IEEE-P802.1Q/D11] IEEE-802.1-WG: *Draft Standard P802.1Q/D11 - IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks.* Technischer Bericht IEEE, Juli 1998.

[JNP 99] JACOBSON, V., K. NICHOLS und K. PODURI: *RFC 2598: An Expedited Forwarding PHB.* RFC, IETF, Juni 1999.

[LaHa 98] LAUBACH, M. und J. HALPERN: *RFC 2225: Classical IP and ARP over ATM.* RFC, IETF, April 1998.

[Laub 94] LAUBACH, M.: *RFC 1577: Classical IP and ARP over ATM.* RFC, IETF, Januar 1994.

[lin 99a] *Differentiated Services on Linux.* Specification, EPFL ICA, Juni 1999.

[lin 99b] *Linux Network Traffic Control – Implementation Overview.* Specification, EPFL ICA, April 1999.

[LKP+ 98] LUCIANI, J., D. KATZ, D. PISCITELLO, B. COLE und N. DORASWAMY: *RFC 2332: NBMA Next Hop Resolution Protocol (NHRP).* RFC, IETF, April 1998.

[MAK 99] MALIS, ANDY, SIAMACK AYANDEH und ANAND KRISHNAMURTHY: *Mapping to ATM classes of service for Differentiated Services Architecture.* Internet Draft, IETF, 10 1999.

[Marc 97] MARC NEITZNER: *Thematische Aufbereitung neurer Netzwerktechnologien für vorlesungsbegleitende Übung.* Studienarbeit, April 1997.

[McGr 92] MCGREGOR, G.: *RFC 1332: The PPP Internet Protocol Control Protocol (IPCP).* RFC, IETF, Mai 1992.

[NBBB 98] NICHOLS, K., S. BLAKE, F. BAKER und D. BLACK: *RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.* Technischer Bericht Dezember 1998.

[Post 81] POSTEL, J.: *RFC 791: Internet Protocol.* RFC, IETF, September 1981.

[RePo 94] REYNOLDS, J. und J. POSTEL: *RFC 1700: ASSIGNED NUMBERS.* RFC, IETF, Oktober 1994.

[ShWr 97] SHENKER, S. und J. WROCLAWSKI: *RFC 2215: General Characterization Parameters for Integrated Service Network Elements.* RFC, IETF, September 1997.

[Simp 94a] SIMPSON, W.: *RFC 1661: The Point-to-Point Protocol (PPP).* RFC, IETF, Juli 1994.

[Simp 94b] SIMPSON, W.: *RFC 1662: PPP in HDLC-like Framing.* RFC, IETF, Juli 1994.

[SPG 97] SHENKER, S., C. PARTRIDGE und R. GUERIN: *RFC 2212: Specification of Guaranteed Quality of Service.* RFC, IETF, September 1997.

[SSS+ 99] SEAMAN, M., ANDREW SMITH, VIJAY SRINIVASAN, W. PACE und A. GHANWANI: *A Framework for Providing Integrated Services Over Shared and Switched IEEE 802 LAN Technologies.* Internet Draft, IETF, 06 1999.

[TaAm 97] TALPADE, R. und M. AMMAR: *RFC 2149: Multicast Server Architectures for MARS-based ATM multicasting.* RFC, IETF, Mai 1997.

[Trillium 97] *Comparison of IP-over-SONET and IP-over-ATM Technologies.* Specification 1072006.11, Trillium Digital Systems, Inc., November 1997.

[Wroc 97a] WROCLAWSKI, J.: *RFC 2210: The Use of RSVP with IETF Integrated Services.* RFC, IETF, September 1997.

[Wroc 97b] WROCLAWSKI, J.: *RFC 2211: Specification of the Controlled-Load Network Element Service.* RFC, IETF, September 1997.

[YHBB 99] YAVATKAR, R., D. HOFFMAN, Y. BERNET und F. BAKER: *SBM (Subnet Bandwidth Manager): A Protocol for RSVP-bases Admission Control over IEEE 802-style networks.* Internet Draft, IETF, Mai 1999.

[ZYB+ 99] ZHANG, LIXIA, R. YAVATKAR, FRED BAKER, BRUCE DAVIE, PETER FORD, BOB BRADEN, JOHN WROCLAWSKI, M. SPEER, Y. BERNET und EYAL FELSTAINE: *A Framework For Integrated Services Operation Over Diffserv Networks.* Internet Draft, IETF, 09 1999.