

Schriftliche Ausarbeitung zum Thema
Betreiberübergreifende QoS-Konzepte im Internet

im Rahmen des

Hauptseminars Telekommunikation
im Sommersemester 2001

am

Lehrstuhl für Kommunikationsnetze
Prof. Dr.-Ing. Jörg Eberspächer

Autor:

Daniel Rögelein
Matr.-Nr. 1969320

Betreuer:

Dipl.-Ing. Anton Riedl

Inhaltsverzeichnis

1	Gegenwärtige Dienstgüte- Situation im Internet	3
1.1	Technische Realisierung	3
1.1.1	Bereich des Backbones	3
1.1.2	Bereich des Zugangsnetzes	4
1.2	Nachweisverfahren der erbrachten Dienstgüte	4
1.3	Fazit zur gegenwärtigen Situation	5
2	Vorstellung Quality of Service – Ansätze	5
2.1	Schicht-2 Quality of Service Mechanismen	5
2.2	IPv4 Type of Service-Oktett	6
2.3	Integrated Services (IntServ)	6
2.4	Differentiated Services (DiffServ)	7
3	Einführung in die Differentiated Services- Architektur	7
3.1	Allgemeines betreiberübergreifendes DiffServ- Szenario	7
3.2	Die DiffServ- Region	8
3.3	Die DiffServ- Domäne	8
3.3.1	Begrenzung (Boundary)	9
3.3.2	Innenbereich (Interior)	11
3.4	Dienstleistungsspezifikation mittels DiffServ	11
3.5	Technische Realisierung von Per Hop Behaviours	13
3.6	Vorstellung wichtiger Per Hop Behaviours	13
3.6.1	Class Selector PHB Group, Default PHB	13
3.6.2	Assured Forwarding PHB	14
3.6.3	Expedited Forwarding PHB	15
3.7	Kombination von Boundary und Interior- Bereich	15
3.8	Per Domain Behaviour	16
3.8.1	Bulk Handling PDB	17
3.8.2	Best Effort PDB	17
3.8.3	Assured Rate PDB	17
3.8.4	Virtual Wire PDB	18
3.9	Zusammenfassung DiffServ	21
4	Bandwidth Broker	22
4.1	Generelle Systembeschreibung	22
4.2	Anwendungsszenario	23
4.3	Interaktion mit IntServ/RSVP	24

Einleitung

Datenkommunikation hat sich im Zeitraum des letzten Jahrzehnts zu einem entscheidenden Bestandteil und treibenden Faktor zeitgemäßen Wirtschaftsgeschehens entwickelt und ist auf dem besten Wege, ihre zunehmend an Bedeutung gewinnende Rolle auch im gesellschaftlichen Alltag zu manifestieren.

Diese Entwicklung ist vor allem darin begründet zu sehen, daß durch die Vorzüge moderner Computertechnologie, welche die Integration verschiedenartiger Information (Bild, Ton, Text) räumlich verteilter Quellen an der Benutzerschnittstelle eines Systems erlaubt, die Möglichkeit besteht, Abläufe und Organisationsstrukturen direkt auf Ebene einheitlicher Datenverarbeitungssysteme abzubilden und somit Einsparungspotentiale freizusetzen.

Wesentliche Motivation für Unternehmen bei der Einführung auf dieser Technologie basierender Systeme war und ist vor allem die Möglichkeit, die Verfügbarkeit von Information von örtlichen Abhängigkeiten zu lösen, um beispielsweise bei der Realisierung von Dienstleistungen regionale Vorteile des Arbeitsmarktes ausnutzen zu können.

Am Beispiel der technischen und organisatorischen Realisierung heutiger *Support Center* sind die sich abzeichnende Entwicklung und daraus abzuleitende zukünftige Anforderungen an die Technologie am eindrucksvollsten illustrierbar.

Im heutigen Regelfall werden die Anrufer von Service- Nummern je nach Tageszeit an *Call Center* in unterschiedlichen Ländern vermittelt. Die Betreuer, welche Anfragen zumeist über Telefonverbindung entgegennehmen, greifen über das Firmennetzwerk direkt auf Kundendaten und bisherige Vorgänge zu. Zur Realisierung solcher Netzwerk-Standortanbindungen zeichnet sich gegenwärtig die Tendenz ab, die entsprechenden Datenflüsse des Unternehmens in IP- basierten Netzen großer Betreiber, welche Teil des weltweiten *Internet* sind (beziehungsweise einen Teil dessen bilden), zu „tunneln“.

Neben dem Betrieb der Datenanbindung des *Support Centers* ist zusätzlich die Inanspruchnahme (internationaler) Telefonie- Dienstleistungen erforderlich. Bereits heute geht das Bestreben vieler Unternehmen daher dahin, eine Integration der Sprachkommunikation in das vorhandene (standortübergreifende) Datennetz vorzunehmen. *Voice over IP (VoIP)* stellt hierbei eine weit entwickelte und durch große Hersteller von Netzwerkkomponenten bereits angebotene IP- basierte Technologie dar, welche jedoch hohe Anforderungen an die Qualität der Vermittlung der Pakete eines Gespräches auf dem gesamten Verbindungsweg innerhalb des IP- Netzes stellt.

Es ist weiterhin anzumerken, daß sowohl der Vertrieb von Produkten als auch die entsprechenden Servicedienstleistungen in zunehmendem Maße in die Internet- Seiten der Hersteller integriert werden. Der hieraus resultierende Synergieeffekt erlaubt es beispielsweise, die vorhandene Information direkt zur individuellen Gestaltung der Internet- Supportseite jedes einzelnen Kunden zu nutzen und die Vermittlung eines zuständigen technischen Betreuers zu beschleunigen, indem im Idealfall eine direkte Bild- und Ton- Verbindung („Videokonferenz“) zum Kunden- PC (oder zukünftig mobilem Endgerät) aufgebaut wird.

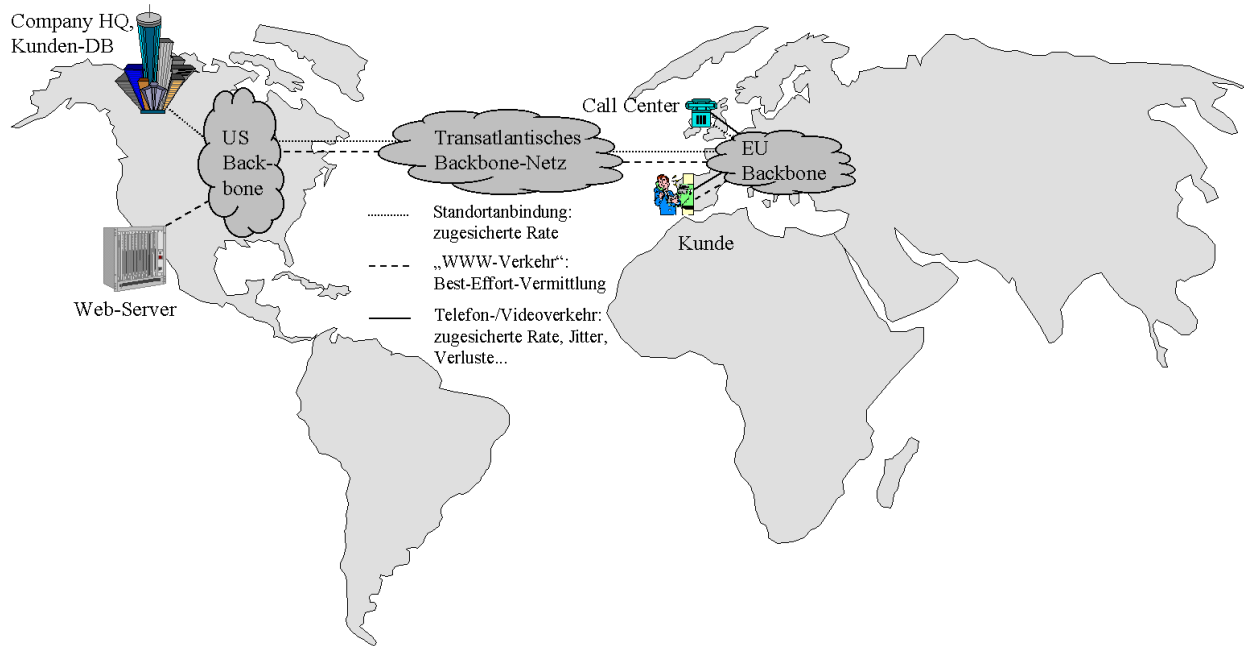


Abbildung 1: Szenario der Anforderungen an betreiberübergreifende Dienstgüte

Wie in Abbildung 1 illustriert, können die Lokationen von Internet- Support- Server (zumeist verteiltes System zwecks Lastausgleich), Kundendatenbank, technischem Betreuer im Support Center sowie Kunde, welche nach dem beschriebenen Szenario alle über ein IP- basiertes Netz (das *Internet*) kommunizieren, international gestreut sein. Es wird deutlich, daß zur Erzielung der durch die unterschiedlichen Anwendungen erforderten „Ende- zu Ende“- Dienstgüte die Notwendigkeit besteht, die priorisierte Vermittlung der Datenpakete über die Bereiche (Netzgrenzen) aller involvierter Netzbetreiber übergreifend sicherzustellen.

Hierbei sind Mechanismen erforderlich, welche die bevorzugte Behandlung statischer Verbindungen sicherstellen (beispielsweise diejenige der Anbindung des *Support Centers* an das Unternehmensnetz), sowie solche, die nach Bedarf die Dienstgüte „dynamischer“ Verbindungen auf dem gesamten Verkehrsweg aushandeln (die multimediale Verbindung zwischen Kunde und technischem Betreuer).

Das geschilderte Szenario stellt als Einführung in die nachfolgenden technischen Ausführungen ein realistisches Beispiel gegenwärtiger Entwicklung dar und motiviert die Vorzüge *betreiberübergreifender IP Quality of Service (QoS)- Konzepte* aus einem Vergleich mit heute üblichen Methoden zur Realisierung von Dienstgüte.

1 Gegenwärtige Dienstgüte- Situation im Internet

Während die auf dem Internet Protokoll (IP) basierenden Quality of Service-Mechanismen, im Kontext dieser Ausarbeitung vor allem die in Abschnitt 3 eingeführten *Differentiated Services (DiffServ)*, noch weitgehend in Standardisierungsprozessen begriffen und von einer flächendeckenden Verfügbarkeit weit entfernt sind, geht das Bestreben von Betreibern großer Internet- Backboneetze dahin, die Leistungsfähigkeit und Übertragungsqualität ihrer Infrastruktur durch heute gängige technische Möglichkeiten zu optimieren, um ihre Stellung im Wettbewerb behaupten zu können.

1.1 Technische Realisierung

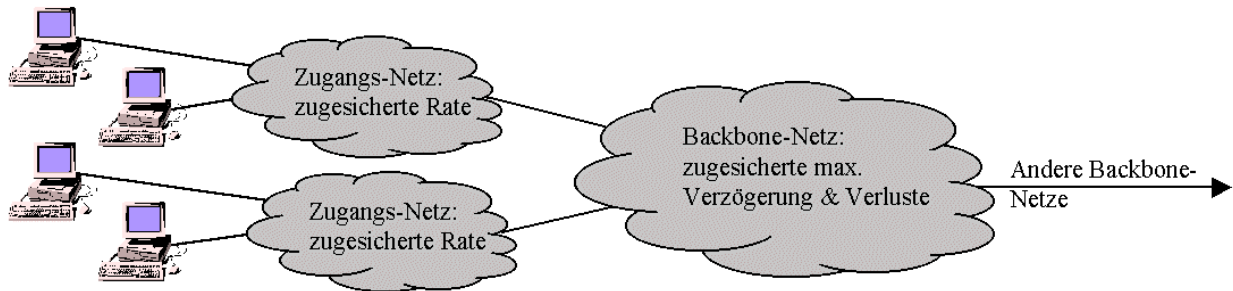


Abbildung 2: Differenzierung Backbone / Zugangnetz

1.1.1 Bereich des Backbones

Eine Betrachtung heutiger Dienstleistungsspezifikationen, sogenannter *Service Level Agreements (SLAs)* (nach [1], [2], [3]), welche die technischen Rahmenbedingungen zu Vertragsverhältnissen beschreiben, zeigt auf, anhand welcher Größen Betreiber die Qualität ihrer Netze dokumentieren. Dieses sind im Bereich des Backbones vor allem die Netzverfügbarkeit (Backbone Network Availability), Paketverluste sowie die Backbone- Verzögerungszeit.

Während die Netzverfügbarkeit, welche zumeist mit 100% angegeben wird, vor allem durch organisatorische Maßnahmen wie redundante Auslegung wichtiger Strecken und Netzwerkkomponenten erreicht werden kann, stehen Betreiber bei der Optimierung von Backbone- Verzögerungszeit sowie Paketverlusten vor einer anspruchsvollen Aufgabe.

Die Forderung nach geringen Paketverlusten (typisch $< 1\%$) verlangt nach einer ausreichenden Dimensionierung der Pufferplätze in paketvermittelnden Systemen (Routern), so daß möglichst wenige Pakete aufgrund von Überläufen verworfen werden müssen.

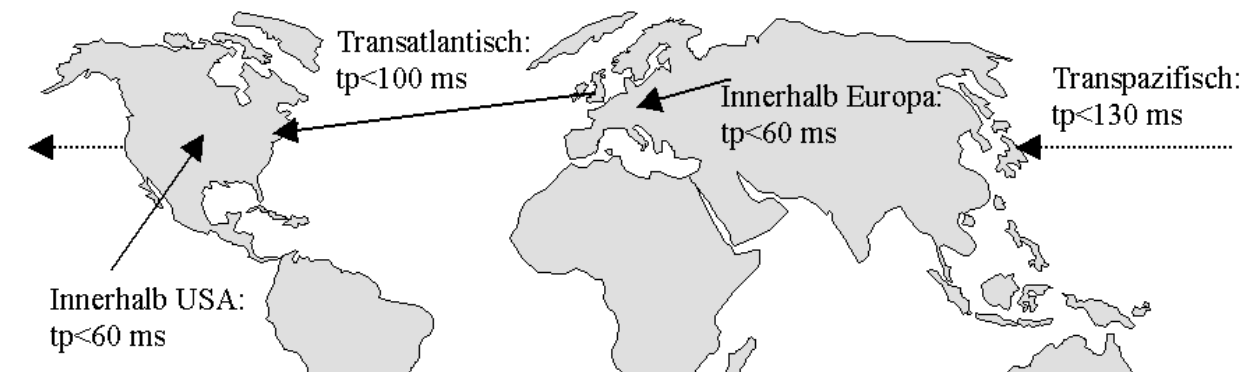


Abbildung 3: Typische Verzögerungszeiten im Backbone-Bereich

Um hingegen die Verzögerung (siehe Abbildung 3), welche Pakete beim Durchlaufen eines Netzabschnitts erfahren, niedrig zu halten, ist neben der Optimierung der Verkehrslenkung (Routing) vor allem dafür Sorge zu tragen, daß die mittleren Füllstände der Warteschlangen möglichst gering gehalten werden.

Eine Lösung dieses Problems wird zumeist dadurch erreicht, daß bei der Netzplanung die Bedingung beachtet wird, daß die Summe der mittleren Raten r_i aller eingehenden Verkehrsflüsse eines Routers kleiner als diejenige der abgehenden Rate R gehalten wird (zu erfüllen für alle möglichen Flußrichtungen).

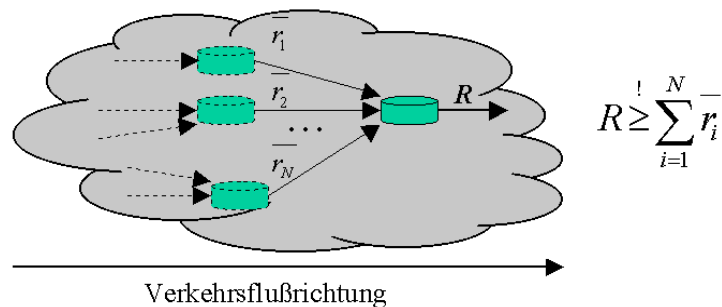


Abbildung 4: Link- Dimensionierung beim Over-Provisioning

Dem gewünschten Effekt niedriger Pufferfüllstände stehen hierbei jedoch die hohen Investitionskosten der beabsichtigten Überdimensionierung (zu englisch: *Over Provisioning*) entgegen.

1.1.2 Bereich des Zugangsnetzes

Ein weiterer interessanter Aspekt heutiger *Service Level Agreements* ist die Dienstgüte-Spezifikation im Bereich des Zugangsnetzes, welches den Teil der Infrastruktur umfaßt, der zur Einbindung des Kunden bzw. des Kundennetzes in das (Backbone-) Netz eines Service Providers dient.

Neben üblichen Werten der Verfügbarkeit von mehr als 99,5% wird vor allem für den Bereich der Kundenanbindung eine feste Bitrate garantiert, was heute durch die Netzbetreiber verbreitet durch Konzeption des Zugangsnetzes auf der Grundlage von Übertragungstechnologien, welche derartige Reservierungen zulassen (Beispiel *ATM*), realisiert wird.

1.2 Nachweisverfahren der erbrachten Dienstgüte

Die in *Service Level Agreements* getroffenen Aussagen zur erbrachten Dienstgüte werden zumeist durch Angabe von gemittelten Meßwerten und deren Meßmethoden untermauert. Hierbei stellt sich heraus, daß vor allem in Bezug auf Ermittlung von Verzögerungszeiten und Paketverlusten das verbreitete *ICMP Echo Request / Reply-Verfahren* („Ping“) zum Einsatz kommt, welches durch den Betreiber an relevanten Punkten innerhalb des Netzes in regelmäßigen Abständen automatisiert ausgeführt wird und dessen Meßwerte den Kunden verfügbar gemacht werden. Hierbei sind zwei Feststellungen über die Aussagekraft dieser Mittelwerte als Entscheidungsgrundlage für die Realisierbarkeit von Anwendungen, welche hohe Übertragungsgüte erfordern, von Bedeutung. Erstens können hohe Paketgrößen zu größeren Verzögerungszeiten führen und das gehäufte Aussenden von Paketen (*Bursts*) die Verlustwahrscheinlichkeit steigern. Es wäre aus Kundensicht wünschenswert, hier nach Verkehrscharakteristik differenzierte Zusagen erhalten zu können. Zweitens läßt sich aus der vorherrschenden Angabe des Meßintervalls zur Mittelwertbildung zu einem Monat ableiten, daß für kurze Zeiträume (wie beispielsweise die Dauer von Videokonferenzen) die Möglichkeit besteht, daß zugesicherte Größen durch das Netz nicht eingehalten werden, sich dieses aber im Monatsmittel und somit vertraglich nicht auswirken würde.

1.3 Fazit zur gegenwärtigen Situation

Unter Rekapitulation des in der Einleitung skizzierten Szenarios wird nun ersichtlich, daß die Umsetzung der dort gestellten Forderungen mit Hilfe der heute im Bereich des Internet üblichen technischen Möglichkeiten und Qualitätszusagen, den Verkehr nach „besten Kräften“ (*Best Effort*) zu vermitteln, nicht praktikabel ist.

Heute verbreitet zum Einsatz kommende Schicht- 2 QoS- Mechanismen finden zumeist dort Anwendung, wo Strecken mit zugesicherter Bitrate bzw. hoher Übertragungsqualität realisiert werden sollen. Die hierfür erforderliche exklusive Reservierung von Leitungskapazität ist jedoch mit hohen Kosten verbunden.

Bei Betrachtung des gegenwärtigen Wettbewerbs unter Betreibern von Internet-Backbonenetzen läßt sich zusammenfassend feststellen, daß wesentliche (beworbene) Unterscheidungsmerkmale durch Verzögerungszeiten sowie die zum Einsatz kommenden Abrechnungsmethoden (zumeist nach Volumen) angegeben sind. Dem Kunden steht zumeist nur die Wahlfreiheit bezüglich der Bitrate seiner eigenen Anbindung offen. Die zukünftige Entwicklung wird hier deutlich machen, daß neben den technischen Aspekten der Einführung von QoS- Mechanismen vor allem die Vermarktung neuartiger Dienste einen wesentlichen Beitrag zur Belebung des Wettbewerbes leisten wird (nach [4]). Es ist daher auch Anliegen dieser Ausarbeitung, einen Einblick in die hierbei entstehenden Möglichkeiten der Dienstleistungsspezifikation zu vermitteln (siehe 3.4).

Der folgende Abschnitt gibt nun einen generellen Überblick darüber, welcher Ansätze sich ein Netzbetreiber zur Einführung differenzierter Dienstgüte innerhalb seines Netzes bedienen kann, und wie diese das gegenständliche Thema des Zusammenspiels mehrerer Betreiber fördern.

2 Vorstellung Quality of Service – Ansätze

Wird versucht, aus früheren sowie den in jüngster Vergangenheit entstandenen Ansätzen zur Erzielung von Dienstgüte denjenigen herauszugreifen, welcher das Zusammenwirken mehrerer Betreiber im Internet zur Realisierung der in der Einführung exemplarisch beschriebenen Anforderungen am effektivsten unterstützt, wird die Wahl auf einen Ansatz fallen, welcher rein auf dem Internet Protokoll (IP) basiert, eine ausgeprägte Schnittstelle an den (Netz-) Grenzen zwischen Betreibern aufweist und gut skalierbar ist. Im folgenden werden einige Möglichkeiten kurz vorgestellt und ihr Nutzen diskutiert.

2.1 Schicht-2 Quality of Service Mechanismen

Diese Mechanismen genügen für sich genommen den unter 2 genannten Forderungen alleine deshalb nicht, weil sie die dritte Schicht (des ISO/OSI- Modells, hier das IP- Protokoll) nicht mit einschließen. Ihre noch heute weit verbreitete Anwendung ist vor allem historisch begründet zu sehen, da die Entwicklung weit vor den in jüngster Vergangenheit vorgeschlagenen QoS- Ansätzen der dritten Schicht erfolgte und legt nahe, daß sie zu Zwecken des Investitionsschutzes auch in zukünftige Konzepte integrierbar sein müssen (nach [4]). Während bei diesen frühen Ansätzen noch davon ausgegangen wurde, daß qualitativ anspruchsvolle Dienste zukünftig direkt auf Schicht 2 aufbauen würden (Beispiel: *Voice / Video over ATM*), erscheinen heute Überlegungen notwendig, wie vorhandene Netzstrukturen, die Schicht 2 QoS unterstützen, im Kontext der IP basierten Dienstgüte in der Art weiter verwendet werden können, daß sie zur technischen Realisierung von an der Schnittstelle zwischen Betreibern definierter IP- Dienstgüte genutzt werden können. Die Feststellung aus

Abschnitt 1.1.2, daß heute Schicht 2 QoS- Mechanismen verbreitet im Bereich dieser Schnittstelle ihren Einsatz finden, untermauert die Notwendigkeit dieser Überlegungen. Auf diese Thematik wird in Abschnitt 3.5 näher eingegangen.

2.2 IPv4 Type of Service-Oktett

Bereits in 1981 spezifizierte die *Internet Engineering Task Force (IETF)* eine einfache Möglichkeit zur unterschiedlichen Priorisierung von Pakettypen (siehe [5]), bei welcher durch Setzen einzelner Bits des sogenannten „*Type of Service - Oktetts*“ im Header jedes IP-Paketes zwischen acht Prioritätsstufen (*Precedence*) gewählt und der Wunsch nach Minimierung von Verzögerung und monetären Kosten sowie nach Maximierung des Durchsatzes und der Zuverlässigkeit (*Type of Service*) (nach [6]) durch den Absender des Paketes ausgedrückt werden konnte.

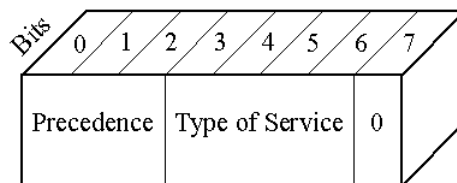


Abbildung 5: IPv4 ToS-Oktett

Der *Type of Service*- Ansatz nach [6] hat sich im Zuge der Entwicklung des Internet nicht behaupten können, lediglich die *Precedence*- Klassen können im Rahmen von „gewichteten Pufferverfahren“ (Beispiel: *Weighted Random Early Detection*) in modernen Routern bedeutsam sein (nach [7]).

Das *Type of Service*- Oktett selbst gewinnt im Zusammenhang mit den im Anschluß vorgestellten *Differentiated Services* eine neue Bedeutung (siehe 3).

2.3 Integrated Services (IntServ)

Die *Integrated Services* (definiert durch die *IETF* in [8]) basieren vor allem darauf, daß die Dienstgüte einzelner Verbindungen auf dem gesamten Verbindungsweg sicherstellt wird, indem für jeden Fluß (*Flow*) in jedem Router exklusive Kapazität reserviert wird. Hierbei kann für einen Fluß, welcher durch wichtige Header- Felder der Protokolle der Schichten 3 und 4 gekennzeichnet ist (Quell-/Zieladresse, Quell-/Zielanschluß, Schicht-4-Protokoll) zwischen den Diensten *Controlled Load* (ähnlich *Best Effort*, vgl. 1.3) sowie *Guaranteed Service* (zugesicherte Bitrate und max. Verzögerung) gewählt werden. Die Nachteile dieses Ansatzes liegen vor allem darin begründet, daß jedes System, welches an einer *IntServ*- Verbindung beteiligt ist (Endsysteme sowie Router), ein einheitliches Reservierungsprotokoll, heute zumeist das *Resource Reservation Protocol (RSVP)*, beherrschen muß, sowie durch die Notwendigkeit der Zustandsspeicherung jedes Flusses in jedem betroffenen Router den Möglichkeiten zur Skalierung absehbare Grenzen gesetzt sind. Da allgemein gesprochen jedem Router eines Verbindungsweges die gleichen Aufgaben zukommen, lassen sich auch schwerlich sinnvolle Schnittstellen zwischen Betreibern definieren.

Als eigenständiger Dienst bilden die *Integrated Services* daher keine solide Basis für betreiberübergreifende Dienstgüte. Der Ansatz der Differenzierung nach Flüssen hat im Teilnehmerbereich jedoch eine praktische Bedeutung, weshalb am Übergang zum Backbone- Bereich zukünftig eine Interaktion stattfinden muß (siehe 4.3).

2.4 Differentiated Services (DiffServ)

Beim *Differentiated Services (DiffServ)*- Ansatz sind die unter 2 genannten Voraussetzungen im Vergleich zu ähnlichen Diensten in ausgeprägtem Maße erfüllt. Dem Bereich der Netzgrenze kommt hierbei ein komplexer Aufgabenteil zu, bei welchem in den Bereich eines *DiffServ*- Netzes eintretende Pakete je nach der Dienstgüte, welche sie erfahren sollen, markiert werden. Router innerhalb des Netzes behandeln Pakete nur in Abhängigkeit dieser Markierung, ohne beispielsweise eigene Entscheidungen über deren Inhalt treffen zu müssen. Diese Grundstruktur bürgt für die Eignung der *Differentiated Services* zur Definition von Schnittstellen zwischen Betreibern und bietet das erforderliche technische Potential, betreiberübergreifende Dienstleistungen zu spezifizieren.

3 Einführung in die Differentiated Services- Architektur

Im folgenden wird ein grundlegender Einblick in den Aufbau der *Differentiated Services*-Architektur nach [9] gegeben, wobei dargestellt wird, wie die im Zusammenhang mit der betreiberübergreifenden Kommunikation stehende Problematik auf die technische Ebene abgebildet werden kann.

3.1 Allgemeines betreiberübergreifendes DiffServ- Szenario

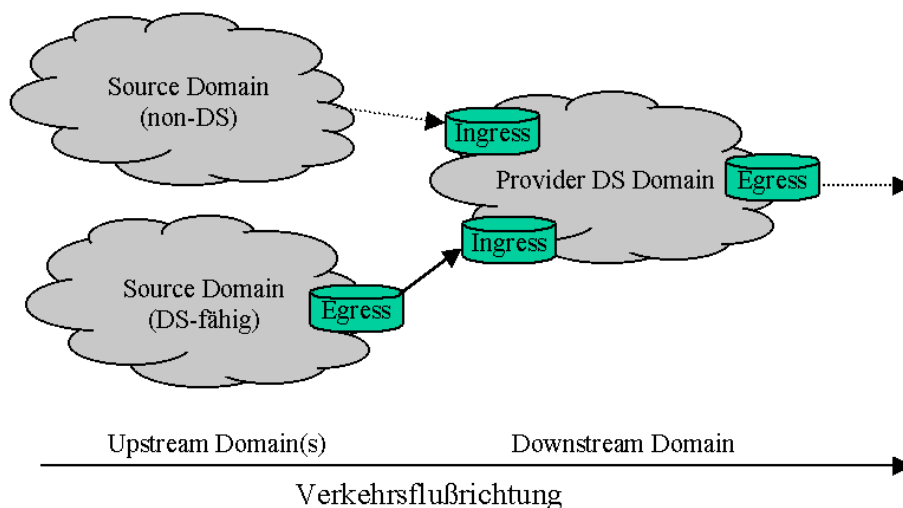


Abbildung 6: Allgemeines DiffServ- Szenario

Bei Betrachtung eines (gerichteten) Datenflusses, welcher *Differentiated Services* über die Bereiche mehrerer Domänen hinweg in Anspruch nimmt, haben die Daten in der *Source Domain* ihren Ursprung und werden von dieser an eine *Provider DS Domain* geleitet. Während die *Source Domain* den Datenfluß noch nicht notwendigerweise mit *DiffServ*- Mechanismen behandelt haben (beziehungsweise *DiffServ*- fähig sein) muß, findet deren Anwendung beim Betreten der *Provider DS Domain* zwingend statt. Im Verlauf des Weitertransports sendet bei zwei in Flußrichtung benachbarten Domänen eine *Upstream Domain* ihre Daten jeweils an eine *Downstream Domain*.

Besondere Maßnahmen sind zu ergreifen, wenn Datenaustausch zwischen *DiffServ*- Domänen stattfinden soll, welche nicht einer *DiffServ*- Region angehören und somit nicht notwendigerweise eine einheitliche Auffassung von *Differentiated Services*- Definitionen haben, sowie falls Verkehr mit Domänen ausgetauscht werden soll, welche die *Differentiated Services*- Architektur nicht unterstützen („non-DS“). Auf diese Fälle, welche Anpassungen auf Ebene der Mechanismen erfordern, wird im Zusammenhang mit der Behandlung der *Per Hop Behaviours* (siehe 3.6) eingegangen.

3.2 Die DiffServ- Region

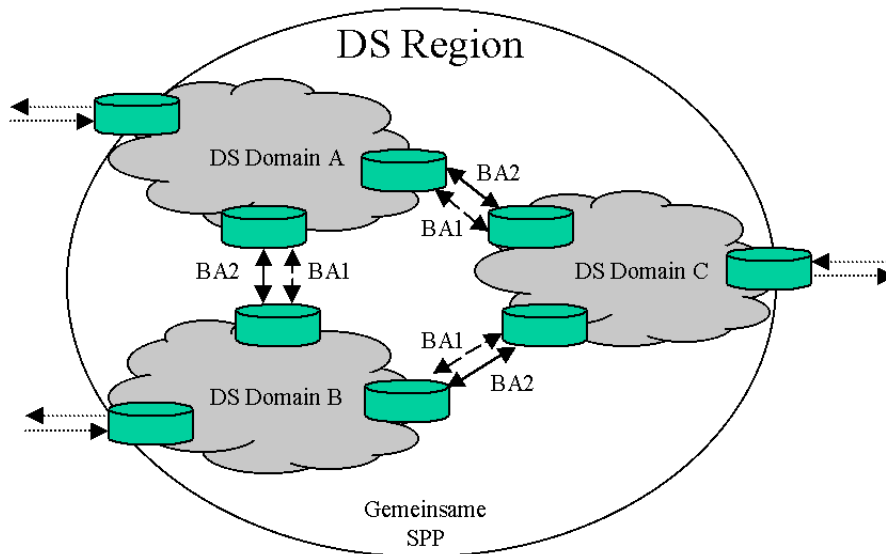


Abbildung 7: DiffServ- Region

Die *DiffServ- Region* (nach [9]) bildet einen organisatorischen Rahmen für betreiberübergreifende *Quality of Service- Dienste*. Sie umfaßt definitionsgemäß eine oder mehrere aneinander angrenzende *DiffServ- Domänen* (siehe 3.3), die in der Lage sind, *Differentiated Services* entlang von Pfaden innerhalb der Region anzubieten, welche durch die eingeschlossenen Domänen verlaufen

Nachdem beim Zusammenschluß mehrerer *DiffServ- Domänen* zu einer *DiffServ- Region* nicht vorgeschrieben ist, daß eine einheitliche Abbildung von *Differentiated Services Code Points* (siehe 3.3.1, Marker) auf *Per Hop Behaviours* (siehe 3.3.2) angewendet werden müßte, ist zur Sicherstellung der übergreifenden Dienstgütereigenschaften die Aushandlung von *Traffic Conditioning Agreements* für alle Verkehrsflüsse zwischen Domänen erforderlich (nach [9]). Signifikante Unterschiede im Vergleich zur Kommunikation zweier administrativ autonomer *DiffServ- Domänen* bestehen diesbezüglich nicht. Um aber technisches Rationalisierungspotential aus dem organisatorischen Zusammenschluß der *DiffServ- Region* freisetzen zu können, wird empfohlen, daß sich alle *DiffServ- Domänen* einer *DiffServ- Region* einer einheitlichen *Service Provisioning Policy (SPP)*, welche die Konfiguration der *Traffic Conditioner* (siehe 3.3.1) sowie die Abbildung von *Traffic Streams auf Behaviour Aggregates* (siehe 3.3.1, Marker) beschreibt, bedienen.

3.3 Die DiffServ- Domäne

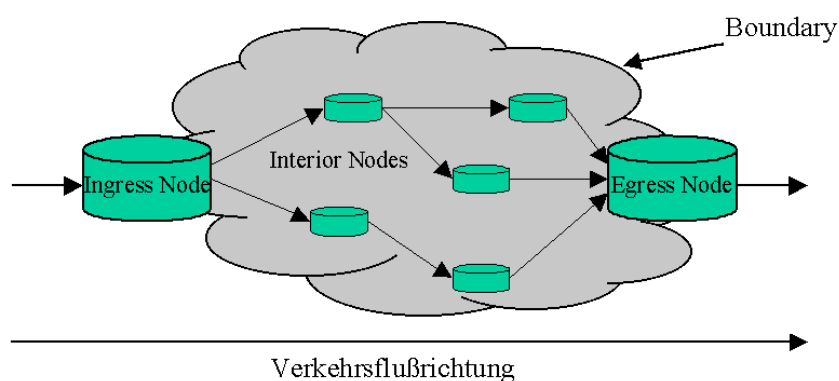


Abbildung 8: DiffServ- Domäne

3.3.1 Begrenzung (Boundary)

Die „Begrenzung“ einer *DiffServ- Domäne (Boundary)*, siehe Abbildung 8) umfaßt diejenigen Knoten, die entweder die Schnittstelle zu anderen Netzen bilden oder an die Endsysteme direkt angeschlossen sind, welchen die Domäne Dienste im Sinne der *Differentiated Services* anbietet. Bei der Betrachtung eines gerichteten Datenflusses, welcher über die *DiffServ- Domäne* übergreift, treten die Pakete beim sogenannten *Ingress Node* ein und beim *Egress Node* wieder aus. (Anmerkung: Bidirektionale Kommunikation, wie sie den üblichen Fall darstellt, muß daher für beide Richtungen getrennt betrachtet werden.)

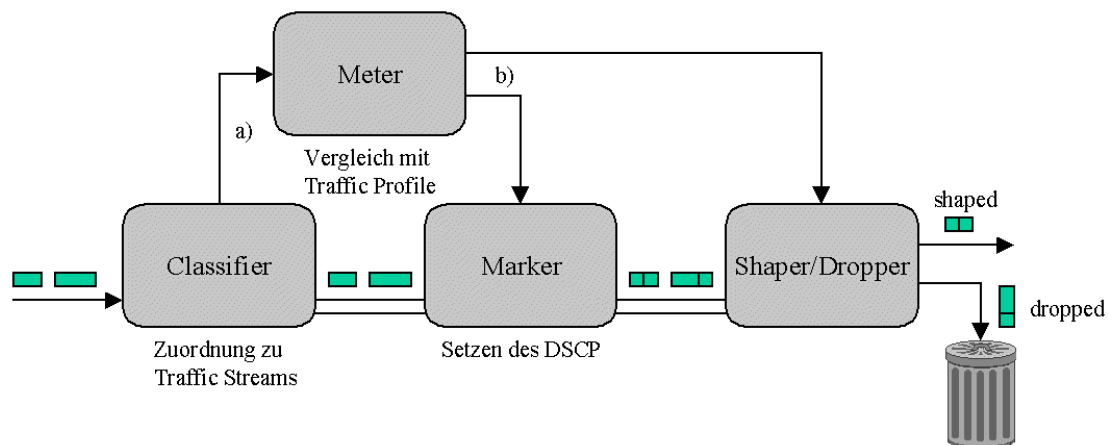


Abbildung 9: Darstellung *Boundary Node: Traffic Conditioner Block (TCB)*

Den *Boundary Nodes* kommt bei der Realisierung von *DiffServ-* Diensten der anspruchsvollste Aufgabenteil zu. Durchquert ein Datenfluss hier die Domänengrenze, widerfahren ihm eine Reihe von Maßnahmen, welche in Abhängigkeit von den zu erfüllenden Dienstgütereigenschaften festzulegen sind.

Diese Definitionen erfolgen - nach *Traffic Stream* (siehe Marker) getrennt - im Rahmen von *Traffic Conditioning Specifications (TCSs)* (nach [10]), zukünftiger Bestandteil von *Service Level Specifications (SLS)*, welche zur Beschreibung von Dienstleistungen im Rahmen von *SLAs* herangezogen werden. Die *Traffic Conditioning Specifications* umfassen Regeln für die Klassifizierung von Paketen sowie Angaben darüber, wie der Verkehr dem *Traffic Profile* entsprechend im Regelfall zu formen ist (siehe *Shaper*). In den in die *SLAs* eingebetteten *Traffic Conditioning Agreements (TCAs)* kann beispielsweise - ebenfalls nach *Traffic Stream* getrennt - das Vorgehen bei Mißachtung des *Traffic Profiles* festgelegt werden.

Die Instanzen innerhalb der *Boundary Nodes* (siehe Abbildung 9), welcher sich die vorgenannten Maßnahmen bedienen, werden im folgenden eingeführt:

Classifier

Die Auswahl einer Klasse von Paketen, welche die im zugehörigen *TCS* spezifizierte Behandlung beim Durchqueren der Boundary einer Domäne (*Conditioning*) sowie beim Durchlaufen jedes Routers (*Per Hop Behaviour*, siehe 3.3.2) in ihrem Inneren erfahren soll, erfolgt durch den *Classifier*.

Hierbei wird unterschieden zwischen:

- *Multi Field (MF) Classification*: Diese stellt den üblichen Fall beim erstmaligen Betreten einer *DiffServ*-fähigen Domäne durch einen Fluß dar, bei welchem Pakete anhand von Headerfeldern der Schichten 3 bis 7 klassifiziert werden.
- *Behaviour Aggregate Classification*: Hat bei einem Datenstrom bereits ein *Marking*-Prozeß stattgefunden (siehe *Marker*), da dieser beispielsweise aus einer anderen *DiffServ*- Domäne stammt (*Upstream Domain*, siehe 3.1), werden die Pakete anhand des (bereits zuvor gesetzten) *Differentiated Services Code Points (DSCP)*, (siehe *Marker*) klassifiziert.

Alle von einem speziellen *Classifier* selektierten Pakete formen einen sogenannten *Traffic Stream*.

Meter

Der *Classifier* signalisiert seine Selektion an den sogenannten *Meter* (Abbildung 9 a), welcher die temporären Eigenschaften (beispielsweise mittlere Datenrate) jedes *Traffic Streams* mißt und mit den im *Traffic Profile* spezifizierten Anforderungen vergleicht. Die Aussage, ob die Pakete des *Traffic Streams* dem Profil genügen (*in-profile*) oder nicht (*out-of-profile*), wird an den *Marker* sowie *Shaper/Dropper* signalisiert (Abbildung 9 b)

Marker

Im regulären Fall, so das *Traffic Profile* eingehalten wird, ordnet der *Marker* die Pakete des *Traffic Streams* einem sogenannten *Behaviour Aggregate (BA)* zu. Ein *BA* wird innerhalb einer *DiffServ*- Domäne durch einen *Differentiated Services Code Point (DSCP)* eindeutig gekennzeichnet, welcher im *Type of Service*- Feld der IPv4- Header (siehe 2.2) beziehungsweise dem *Traffic Class Octett* bei IPv6 kodiert wird (nach [11]).

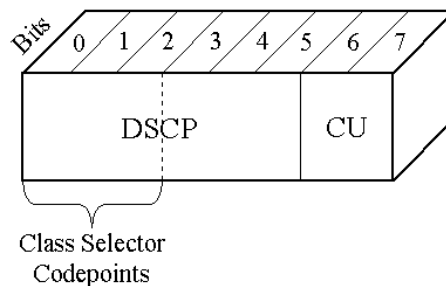


Abbildung 10: DiffServ Codepoint Feld

Die Vorgehensweise, welche bei Nicht-Einhaltung des *Traffic Profiles* anzuwenden ist, kann innerhalb des *Traffic Conditioning Agreements* definiert werden. War der *Traffic Stream* bereits durch einen *DSCP* gekennzeichnet (*BA Classification*) und soll beispielsweise aufgrund der vorgenannten Verletzung einen neuen Codepoint (eventuell mit niedrigerer Priorität) erhalten, wird dies als *Re-Marking* bezeichnet.

Shaper/Dropper

Falls eine kurzzeitige Überschreitung des *Traffic Profiles* erlaubt oder den vertraglichen Vereinbarungen des *TCSs* (vgl. 3.4) entsprechend die *Provider DS Domain* selbst für die Einhaltung des Profils zuständig ist, wird der Datenfluß diesem entsprechend durch den *Shaper* geformt.

Eine restriktivere Vorgehensweise bei Mißachtung des *Traffic Profiles* durch die *Source Domain* ist das Verwerfen (*Policing*) von Paketen, welches durch den *Dropper* ausgeführt wird.

Nachdem die beschriebenen Maßnahmen beim Durchlaufen des *Ingress Nodes* (siehe Abbildung 8) angewandt wurden, sind alle Pakete mit einem (gültigen) *DSCP* versehen, entsprechend den jeweiligen *Traffic Profiles* geformt (mit Ausnahme von Fehlkonfigurationen oder Mißachtung der *TCSs* durch die *Source Domain*) und können innerhalb der *Provider DS Domain* vermittelt werden.

Die Instanzen des *Traffic Conditioner Blocks* (siehe Abbildung 9) können auch innerhalb von *Egress Nodes* vorhanden sein, da eine *DiffServ- Domäne* im Rahmen ihrer möglichen Funktion als *Source Domain* auch zur Sicherstellung eines *Traffic Profiles* des austretenden Verkehrs verpflichtet sein kann.

3.3.2 Innenbereich (Interior)

Die *DiffServ- Domäne* (Abbildung 8) umfaßt - vereinfacht gesprochen - in ihrem Inneren sämtliche *DiffServ- fähigen Knoten (Interior Nodes)* eines Netzes, die mit allen Paketen eines *Behaviour Aggregates* auf einheitliche Weise verfahren.

Die „von außen“ beobachtbare Behandlung, die ein einzelnes Paket somit in immer derselben Weise beim Durchlaufen jedes Routers auf seinem Verkehrsweg innerhalb der Domäne erfährt, wird als *Per Hop Behaviour (PHB)* bezeichnet.

Eine wichtige Aufgabe des Betreibers besteht darin, die Auswahl passender *Per Hop Behaviours* für die zu vermittelnden *Behaviour Aggregates* zu treffen und eine geeignete technische Realisierung der *PHBs* innerhalb seines Netzes zu wählen (siehe 3.5).

Die *Interior Nodes* wählen das *Per Hop Behaviour* jedes Paketes individuell auf Grundlage dessen *DSCPs*.

Einen genaueren Einblick in die Eigenschaften der wichtigsten *Per Hop Behaviours* vermittelt Kapitel 3.6.

Die Anwendung von *Per Hop Behaviours* in Verbindung mit den Regeln des *Traffic Conditionings* führen schließlich zu einer (von außen) beobachtbaren Ausprägung von Dienstgüte für spezifische *Traffic Streams*, wie sie durch das *Service Level Agreement* vertraglich zugesichert wurde. Dieses Verhalten, welches eine *DiffServ- Domäne* bei äußerer Betrachtung bei der Vermittlung eines *Traffic Streams* zeigt, wird durch den unter 3.8 vorgestellten Begriff „*Per Domain Behaviour*“ beschrieben.

3.4 Dienstleistungsspezifikation mittels DiffServ

Durch das Modell der Klassifizierung und Konditionierung des Verkehrs an den Netzgrenzen ergeben sich vielfältige Möglichkeiten zur Formulierung neuer Dienstleistungen, die vor allem auf der *Multi Field Classification* gründen. Im folgenden werden einige Ansätze zur Klassifizierung in Abhängigkeit der jeweiligen Schicht des ISO/OSI- Modells aufgezeigt.

Schicht 3

Klassifizierung nach dieser Schicht erlaubt vor allem eine regionale Differenzierung der angebotenen Dienstleistungen (nach Quell- /Zieladresse). Auch die betreiberübergreifende Vermittlung von Daten mit „konstanter“ Dienstgüte beruht auf der *Behaviour Aggregate Classification* (siehe 3.3.1) der dritten Schicht.

Schicht 4

In der vierten Schicht kann eine Unterscheidung nach verwendetem Transportprotokoll sowie nach Port- Nummer erfolgen. Hierbei besteht vor allem die Möglichkeit, nach speziellen Anwendungen, welchen allgemein anerkannte („*well known*“) Ports zugehören, zu differenzieren.

Schicht 7

Die Einbeziehung der siebten Schicht läßt die Möglichkeit zu, selbst im Rahmen der Daten einer speziellen Anwendung Unterscheidungen zuzulassen. Einem Benutzer könnten beispielsweise je nach dessen persönlicher Wahl des CoDecs in einer Videokonferenz- Anwendung unterschiedliche Dienstgütern zur Verfügung gestellt werden.

Im Zuge der Einführung von Dienstgüternmechanismen muss aber auch die Vorgehensweise bei Fehlfunktionen und Inkompatibilitäten vertraglich geregelt sein.

Handhabung von out-of-profile Verkehr

Entspricht ein Verkehrsfluß nicht dem ausgehandelten *Traffic Profile*, könnten vertraglichen Vereinbarungen im *Traffic Conditioning Agreement* gemäß die Pakete entweder verworfen oder einem *Behaviour Aggregate* niedriger Priorität zugewiesen werden. Falls innerhalb der Domäne noch ausreichend Übertragungskapazität zur Verfügung stünde, könnte auch der reguläre Transport zu höheren Tarifen angeboten werden. Für diesen Fall bietet sich das *Assured Forwarding PHB* an (siehe 3.6.2), welches es beispielsweise erlaubt, daß *out-of-profile*- Pakete solange mit normaler Dienstgüte vermittelt werden, wie ausreichend Kapazität zur Verfügung steht. Im Falle von Stausituationen würden Pakete dieses *Traffic Streams* aber bevorzugt vor *in-profile*- Paketen verworfen.

Handhabung falsch klassifizierten Downstream- Verkehrs

Zwischen zwei Domänen kann die Vereinbarung getroffen worden sein, daß die Klassifizierung von Paketen bereits in der *Source Domain* erfolgt, um dieser beispielsweise größere Entscheidungsfreiheit über die gewünschte Dienstgüte einzelner Flüsse einzuräumen. Neben den bereits angesprochenen Überlegungen zur Verfahrensweise mit *out-of-profile*- Verkehr (*Remarking*) ist hier im speziellen das Vorgehen vertraglich festzulegen, falls Pakete mit ungültigen *DSCPs* empfangen werden.

Verkehr aus DiffServ- inkompatiblen Netzen

Wird Verkehr aus Netzen angenommen, welche zwar die *DiffServ*- Architektur nicht unterstützen, aber dennoch *QoS*- Dienstleistungen in Anspruch nehmen wollen, können sämtliche zur Erzielung der gewünschten Dienstgüte erforderlichen Maßnahmen innerhalb der *Provider DS Domain* erfolgen (vgl. 3.1). Es würden hierbei beispielsweise vertragliche Vereinbarungen getroffen, mit welcher maximalen (mittleren) Datenrate Pakete durch die *DiffServ*- Domäne mit einer garantierten Dienstgüte vermittelt werden können. Ein Sonderfall dieses Szenarios, nämlich daß durch die *Source Domain* keine besondere Dienstgüte gewünscht wird, kann durch Verwendung des sogenannten *Default Codepoints* (siehe 3.6.1) für den entsprechenden *Traffic Stream* innerhalb der *Provider DS Domain* abgedeckt werden.

Ein weiterer relevanter Gesichtspunkt ist der Dienstgüthenachweis bei *DiffServ*-Verbindungen. Ein wesentlicher Fortschritt im Vergleich zu den sehr allgemeinen Zusicherungen in heutigen *Service Level Agreements* wird bereits durch die exakte Spezifikation von Randbedingungen für Verkehrseigenschaften einzelner *Traffic Streams* innerhalb der *DiffServ Service Level Specifications* erreicht. Die programmatische Einbeziehung des Dienstgüthenachweises in die *Differentiated Services*- Architektur erfolgt durch die *Per Domain Behaviours*, wie sie unter 3.8 vorgestellt werden.

Die hier gemachten Beispiele sollen illustrieren, unter welchen vertraglichen Rahmenbedingungen *DiffServ*- Dienstleistungen spezifiziert werden können und erheben keinen Anspruch auf Vollständigkeit.

3.5 Technische Realisierung von Per Hop Behaviours

Die Implementierung von Per Hop Behaviours bildet die technische Grundlage des priorisierten Transports von Daten innerhalb einer *DiffServ*- Domäne. Wie in 3.3.2 bereits angesprochen, äußert sich die Anwendung eines PHBs in der Art, wie Pakete beim Durchlaufen eines *Interior Nodes* behandelt werden. Dieses Verhalten kann durch Größen wie Paketverluste, Verzögerung oder Jitter beschrieben werden und wird erzielt, indem ein Router Paketen eines *Behaviour Aggregate* dessen PHB entsprechend Ressourcen zuteilt (nach [9]). Die *DiffServ*- Architektur sagt dabei nichts darüber aus, welche technischen Maßnahmen zur Realisierung dieser Zuteilung anzuwenden sind. Eine generelle Vorgehensweise ist die Verwendung von Mechanismen zur Bitratenreservierung und Warteschlangen- Verwaltung, wie sie in komplexen IP- Routern üblicherweise implementiert sind.

Eine weitere Möglichkeit zur Realisierung von *Per Hop Behaviours* besteht darin, Daten auf Übertragungstrecken zu vermitteln, auf welchen Schicht-2 QoS- Mechanismen implementiert sind. Die Erscheinung des PHBs ist dann maßgeblich durch das Verhalten des Schicht-2 Mechanismus bestimmt. Da einige dieser Mechanismen dynamische Aushandlung von Verbindungsparametern zulassen bzw. bereits Ansätze unternommen wurden, deren Schicht-2 Aufbau um an das *DiffServ*- Modell angelehnte Dienstgüteparameter zu erweitern, hat sich die *IETF* dieser Thematik unter anderem jüngst in [12] angenommen.

Die Bedeutung von Schicht-2 QoS- Mechanismen für betreiberübergreifende Dienstgütekonzepete wurde in 2.1 dargelegt.

3.6 Vorstellung wichtiger Per Hop Behaviours

Im folgenden wird auf die drei wichtigsten PHBs, namentlich *Class Selector (CS)*, *Assured Forwarding (AF)* sowie *Expedited Forwarding (EF)* eingegangen, und ausgesuchte Besonderheiten bei deren betreiberübergreifenden Einsatz angesprochen.

3.6.1 Class Selector PHB Group, Default PHB

Die PHBs der *Class Selector PHB Group* wurden in [11] definiert, um eine Abwärtskompatibilität zum IPv4 *ToS*-Schema aufrechtzuerhalten, wobei anhand der ersten drei Bits (0..2) des *ToS- Bytes* bzw. *DSCPs* zwischen den unter 2.2 vorgestellten *Precedence*- Klassen unterschieden werden kann. Dies stellt eine Möglichkeit dar, einheitliche Dienstgüte zwischen *DiffServ*- und *ToS*- kompatiblen Netzen erreichen zu können, indem die *CS PHBs* das selbe Verhalten wie *Precedence*- fähige Nodes zeigen. Die drei *Type of Service Bits* (3..5) werden hierbei nach [11] und [10] nicht mehr unterstützt und müssen bei Verwendung der *CS PHBs* innerhalb des *DSCPs* auf „0“ gesetzt werden. (Anmerkung: Das vierte Bit (6), welches nach [6] für die Minimierung der monetären Kosten vorgesehen war, fällt nun in den *Currently Unused*- Bereich,

welcher nicht für die Nutzung durch *DiffServ* vorgesehen ist (siehe Abbildung 10). Es wird daher im Zusammenhang mit den *CS PHBs* nicht angegeben, auf welchen Wert es zu setzen ist.)

Einen Sonderfall der *CS PHBs* stellt das *Default Per Hop Behaviour (DE PHB)* dar, welches durch den *DSCP* „000000“ gekennzeichnet und für die Verwendung im Sinne von „*Best Effort*“- Zustellung (vgl. 1.3) vorgesehen ist.

3.6.2 Assured Forwarding PHB

Das *AF PHB* definiert nach [13] vier Klassen *AF_x*, welchen auf den Verbindungsstrecken innerhalb einer *DiffServ- Domäne* unterschiedliche Bitraten zugewiesen werden können. Diese Klassen werden weiterhin in je drei unterschiedliche „*Drop Precedence*“- Gruppen *y* unterteilt (*AF_xy*). Je höher die *Drop Precedence y* eines Paketes einer Klasse *x* im Vergleich zu anderen Paketen der selben Klasse ist, desto eher wird dieses Paket beispielsweise bei Stausituationen verworfen.

	Klasse 1	Klasse 2	Klasse 3	Klasse 4
Niedr. Drop Prec.	AF11, DSCP 001010	AF21, DSCP 010010	AF31, DSCP 011010	AF41, DSCP 100010
Mittlere Drop Prec.	AF12, DSCP 001100	AF22, DSCP 010100	AF32, DSCP 011100	AF42, DSCP 100100
Hohe Drop Prec.	AF13, DSCP 001110	AF23, DSCP 010110	AF33, DSCP 011110	AF43, DSCP 100110

Tabelle 1: AF PHB Codepoints

Mit Hilfe des *Assured Forwarding PHBs* lassen sich nur schwer Aussagen über Paketverzögerungen oder Jitter treffen, da zum einen die Verwendung von *Traffic Conditioning* an den *Ingress Nodes* nicht vorgeschrieben ist, und zum anderen die Wechselwirkung von Paketen der gleichen *AF- Klasse* mit unterschiedlicher *Drop Precedence* nicht- trivial beschreibbar ist. Das *AF PHB* kann aber andererseits auf Grund dieser geringen Anforderungen an die *Ingress Nodes* seine spezifizierten Merkmale relativ gut in heutigen „*Over- Provisioned*“- Netzen entfalten (nach [13]).

Beim betreiberübergreifenden Einsatz ist vor allem darauf zu achten, daß innerhalb einer *AF- Klasse* keine Veränderung der Paketreihenfolge auftritt. Dies kann dadurch realisiert werden, daß innerhalb einer Domäne Pakete einer Klasse separat aggregiert werden und an jeder Domänengrenze eine statische gegenseitige Zuordnung von *AF- Klassen* definiert wird. Dies ist vor allem dann zu beachten, wenn *DiffServ- Domänen* nicht innerhalb einer *DiffServ- Region* organisiert sind und somit keine einheitliche *Service Provisioning Policy* verwenden (vgl. 3.2).

Obwohl die theoretischen Anforderungen an die *Ingress Nodes* zur Erfüllung der Dienstgüte- Vorgaben gering sind, sollte ein Betreiber die Rate aller ankommenden *AF Behaviour Aggregates* auf denjenigen Wert nach oben beschränken, welcher sich aus der Summe aller mit *Upstream Domains* ausgehandelter *SLAs* ergibt, um sich vor möglichen „*Denial of Service*“- Attacken - beispielsweise einer großen Menge von Paketen der höchsten Klasse mit niedrigster *Drop Precedence*, welche alle anderen Pakete im Netz „verdrängen“ könnte - zu schützen.

3.6.3 Expedited Forwarding PHB

Das *EF PHB* (nach [14], [15]) (*DSCP 101110*) stellt (nach bisherigem Stand) die größtmögliche Dienstgüte bei Paketvermittlung durch einen *Interior-Node* dar, was aus technischer Sicht bedingt, daß - ähnlich dem „*Over-Provisioned*“- Modell (vgl. Abbildung 4) - für jedes *DiffServ Aggregat* die Summe der maximalen Zuflußraten an jedem Router innerhalb der Domäne geringer oder gleich derjenigen der abfließenden Raten gehalten werden muß. Dies führt zu möglichst geringen Pufferfüllständen und damit Paketverzögerungen. Um diese Forderungen erfüllen zu können, impliziert die Definition des *EF PHBs* restriktive Anforderungen an die *Ingress Router* dahingehend, die Zuflußraten in der gewünschten Weise zu beschränken.

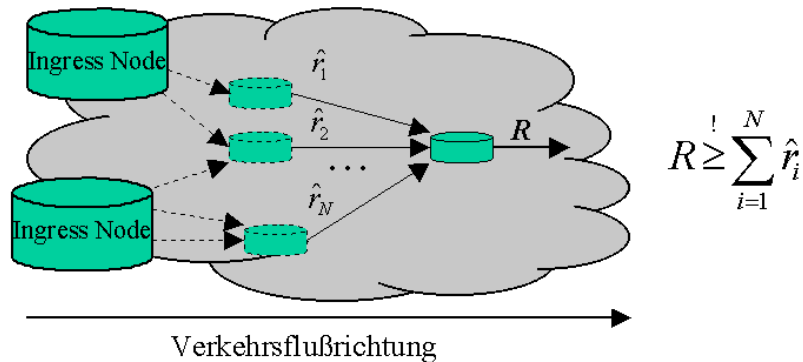


Abbildung 11: Link- Dimensionierung beim EF PHB

Zur Vermeidung der Anfälligkeit gegen „*Denial of Service*“- Attacken gelten neben den vorgenannten Bedingungen an das *Traffic Conditioning* die bereits beim *AF PHB* (3.6.2) gestellten Forderungen. An Netzgrenzen ist zusätzlich dafür Sorge zu tragen, daß beim *Re-Marking* das *EF PHB* nur auf sich selbst abgebildet wird, um die hohe Dienstgüte auch über mehrere Domänen hinweg sicherstellen zu können (nach [14]).

3.7 Kombination von Boundary und Interior- Bereich

Anhand der vorgestellten Definition des *EF PHBs* kann nachvollzogen werden, daß die Möglichkeiten, welche die Definition des Begriffs *Per Hop Behaviour* zur Spezifikation von Dienstgüte im Sinne der *Differentiated Services* zuläßt, durch die Beschränkung des Begriffs auf das Verhalten Domänen- interner Nodes begrenzt sind.

Die Spezifikation anspruchsvoller QoS- Dienste, welche sich *Per Hop Behaviours* wie des *EF PHBs* bedienen, die ihre geforderten Eigenschaften nur unter Randbedingungen erfüllen können, wird immer zusätzliche Bedingungen an die Umgebung der *Interior Nodes*, also die *Domain Boundary*, beinhalten müssen.

Während beim *Assured Forwarding PHB* nur Empfehlungen über einzusetzende *Traffic Conditioning*- Maßnahmen ausgesprochen wurden, ist bei der Definition des *Expedited Forwarding PHBs* eine Lösung darin gesucht worden, diese Forderungen in die exemplarische Beschreibung des Dienstes „*Virtual Leased Line*“, welcher mit Hilfe dieses *PHBs* realisiert werden kann, einzubetten (vgl. [14]).

Als einen weitergehenden Ansatz zur Beschreibung von QoS- Diensten wurde der Begriff des *Per Domain Behaviours* (siehe 3.8) durch die *IETF* geprägt, welcher diesen Aspekt neben einer Fülle anderer Gesichtspunkte abdeckt.

3.8 Per Domain Behaviour

Die Bezeichnung *Per Domain Behaviour (PDB)* (nach [16]) deutet bereits an, daß dieses den begrifflichen Rahmen bilden soll, die Behandlung eines Verkehrsflusses beim Durchlaufen einer *DiffServ- Domäne* beschreiben zu können.

Ein *Per Domain Behaviour* stellt ein technisches Gerüst dar, welches die gemeinsame Definition von *Traffic Conditioning-* Maßnahmen und zu verwendenden *Per Hop Behaviours* zur Spezifikation einer speziellen Ausprägung domänenübergreifender Dienstgüte erlaubt. *Klassifizierungs-* Regeln können optional mit einbezogen werden und die Entscheidungen eines überlagerten „*Admission Control*“- Prozesses (siehe 4.1) reflektieren. Ergänzend hierzu können in einer *PDB- Definition* Aussagen darüber getroffen werden, wie sich das Verhalten in Abhängigkeit des Betriebs- und Auslastungszustandes der verwendeten Ressourcen beschreiben läßt. Dies kann sich in der Nennung von Möglichkeiten zur Ausnutzung freier Ressourcen („kurzzeitige“ Eigenschaften des *PDBs*) bis hin zur Definition restriktiver Bedingungen der generellen Anwendbarkeit des *PDBs* widerspiegeln. Eine Änderung „langzeitiger“ Eigenschaften kann beispielsweise bei Topologieänderungen (Ausfällen) auftreten, was am Beispiel einer Ringstruktur illustriert wird:

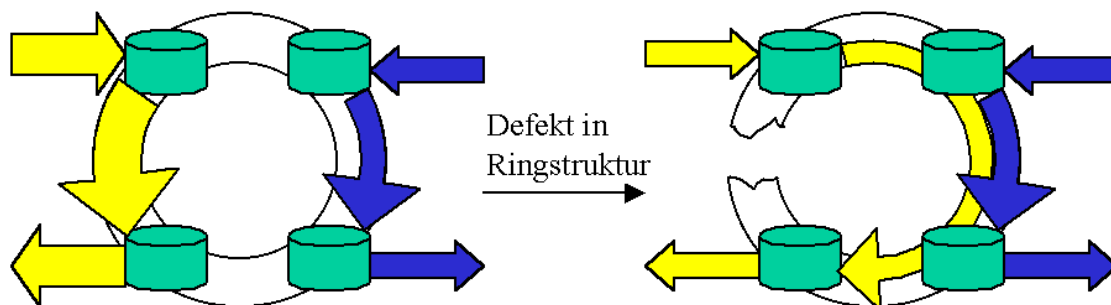


Abbildung 12: Änderung langfristiger PDB- Eigenschaften am Beispiel Ringstruktur

Der Begriff des *Per Domain Behaviours* stellt in schlüssiger Weise den praktischen Bezug zu kommerziellem Netzbetrieb her, da die Spezifikationen sowohl auf Realisierungsrichtlinien abgebildet werden können, als auch das beobachtbare Verhalten der *DiffServ- Domäne* bei der Vermittlung eines Datenflusses beschreiben, welches zur Dienstleistungsspezifikation in *Service Level Specifications* angeführt werden kann (nach [16]).

Die Abstraktion der Dienstgütebeschreibung auf den Bereich der Domänengrenze unter Angabe von Randbedingungen der Anwendbarkeit erlaubt eine vorteilhafte Modularisierung des *DiffServ-* Konzeptes, bei welcher die *Per Domain Behaviours* „Bausteine“ zur Realisierung betreiber- übergreifender Dienstgüte- Konzepte darstellen. Der hohe Abstraktionsgrad unterstützt dies, da er die Möglichkeit eröffnet, Aussagen über die gegenseitige Beeinflussung von Datenflüssen zu treffen, welche durch den Bereich eines Verbundes von *DiffServ- Domänen* vermittelt werden (nach [17]).

Im folgenden werden die bislang durch die *IETF* vorgeschlagenen *Per Domain Behaviours* eingeführt und nach Angemessenheit die Abhängigkeit ihrer Eigenschaften von den jeweils bedeutsamen Randbedingungen beleuchtet.

3.8.1 Bulk Handling PDB

Das *BH PDB* (nach [18]) beschreibt die Eigenschaft einer Domäne, eine bestimmte Klasse von Paketen bevorzugt nur dann zu vermitteln, falls die Ressourcen des Netzes gerade von keinem anderen Verkehrstyp in Anspruch genommen werden. Daraus ist abzuleiten, daß das *BH PDB* die niedrigste „Dienstgüte“ innerhalb der *Differentiated Services* darstellt, welche noch unterhalb derer der klassischen *Best Effort*- Vermittlung anzusiedeln ist.

Die Realisierung innerhalb der Domäne soll entweder mit Hilfe eines *Class Selector PHBs* (siehe 3.6.1) niedriger *Precedence* oder durch ein *Assured Forwarding PHB* (siehe 3.6.2) niedriger Klasse und höchster *Drop Precedence* erfolgen.

Falls in vertraglichem Rahmen mit *Upstream Domains* keine besonderen Vereinbarungen zur Klassifizierung ausgehandelt wurden, soll diese am *Ingress Node* erfolgen und eine „angemessene Zielgruppe“ von Paketen (Bulk Mail, Napster Traffic) für das *BH PDB* selektieren (nach [18]).

Das *BH PDB* stellt weiterhin keine expliziten Anforderungen an das *Traffic Conditioning*, da die definierten Eigenschaften bereits dadurch erreicht werden, daß *Interior Nodes* Pakete bei fehlenden Ressourcen (Pufferüberläufen) selbst verwerfen.

3.8.2 Best Effort PDB

Die wesentliche Eigenschaft des *BE PDBs* (nach [16]) ist die Vermittlung des Verkehrs in genau der Weise, wie es in heutigen „*Over-Provisioned*“- Netzen der Fall ist. Entsprechende *Service Level Specifications* können somit ähnliche charakteristische Größen umfassen wie sie bereits eingangs für die gegenwärtige Situation beschrieben wurden (vgl. 1.1.1).

3.8.3 Assured Rate PDB

Das *AR PDB* (nach [19]) ist geeignet, Verkehrsflüsse zu vermitteln, welche einer zugesicherten Datenrate bedürfen (*Committed Information Rate CIR*), aber keine besonderen Anforderungen an Verzögerungszeiten oder *Jitter* (Abweichung von der mittleren Verzögerungszeit) stellen. Um den Begriff der *CIR* ausreichend zu spezifizieren, enthält die Definition des *PDBs* Angaben zum Zeitintervall der Mittelwertbildung bei der Messung sowie zur maximalen *Burst Size*, welche hierbei akzeptiert wird. Hält ein Verkehrsfluß die *CIR* ein, sollen die enthaltenen Pakete nur minimale Verluste erfahren, welche innerhalb von *Service Level Specifications* als Prozentangaben dokumentiert werden können (vgl. 1.2).

Gemäß der Definition des *AR PDBs* wird weiterhin die Möglichkeit beschrieben, daß Verkehrsflüsse bei verfügbaren Ressourcen innerhalb des Netzes zusätzliche Kapazität in Anspruch nehmen können, ohne daß hierbei jedoch die vorgenannten Zusicherungen durch den Betreiber eingehalten werden müßten. Eine Obergrenze der Bitrate kann durch eine optionale *Peak Information Rate (PIR)* angegeben werden.

In Bezug auf das *Traffic Conditioning* wird vorgegeben, daß Pakete aus Flüssen, welche die *Committed Information Rate* nicht überschreiten, einer Klasse des *Assured Forwarding PHBs* (siehe 3.6.2) mit niedriger *Drop Precedence* zugeordnet werden. Ob diese Klassifizierung in der *Source Domain* oder *Provider DS Domain* erfolgt, ist durch den Provider innerhalb von *Service Level Specifications* festzulegen. Wird durch das *Metering* ein Überschreiten der *CIR* festgestellt, aber noch Ressourcen innerhalb des Netzes zur Verfügung stehen sollten, sind die betroffenen Pakete dem *AF PHB* der selben Klasse, jedoch höheren *Drop Precedence*- Stufen zuzuordnen.

Es empfiehlt sich, daß bei der Spezifikation einer *Peak Information Rate* diejenigen Pakete, welche diese Rate überschreiten, durch den *Dropper* verworfen werden (siehe Abbildung 9). Auf dieselbe Weise ist mit Paketen zu verfahren, welche eine maximale Paketgröße überschreiten.

Nachdem insgesamt vier unterschiedliche Klassen AF_x des *AF PHBs* definiert sind, besteht die Möglichkeit, innerhalb einer Domäne vier Instanzen des *Assured Rate PDBs* zu etablieren.

3.8.4 Virtual Wire PDB

Die Nachbildung einer Festverbindung (dedizierte Leitung, *Dedicated* oder *Leased Line*) stellt den größtmöglichen Anspruch an einen *Quality of Service*- Dienst, da sie Zusagen über garantierte Bitrate, geringe Paketverzögerungszeiten sowie eng begrenzte *Jitter*-Eigenschaften erfordert und keine Paketverluste zulässig sind. Das *Virtual Wire Per Domain Behaviour* (*VW PDB*) (nach [20]) stellt hierbei einen geeigneten Ansatz dar. Vergleichbar mit der Spezifikation des „*Virtual Leased Line*“- Dienstes, dessen sich die Definition des *EF PHBs* beispielhaft zur Beschreibung seiner Eigenschaften bedient (vgl. 3.7), basiert dieses *PDB* auf dem *Over-Provisioned*- Modell zur Sicherstellung geringer Pufferfüllstände und Paketverzögerungszeiten. Die anspruchsvolle Aufgabe besteht in der Definition von Randbedingungen der Anwendbarkeit des *PDBs*, unter welchen es die gewünschten *Jitter*- Eigenschaften aufweist.

Die Grundlage zur Erfüllung der im *VW PDB* beschriebenen Eigenschaften bildet die Verwendung des *Expedited Forwarding PHBs* im *Interior*- Bereich sowie die Anwendung geeigneter *Traffic Conditioning*- Maßnahmen, hier insbesondere des *Policings*, an der Domänengrenze. Abweichend von den zuvor beschriebenen Realisierungen des *Over-Provisioned*- Modells (vgl. 1.1.1 und 3.6.3) wird im Zusammenhang mit dem *VW PDB* gefordert, daß die *maximale* (nicht mittlere) Zuflußrate eines *Behaviour Aggregates* an jedem beteiligten *Interior*- Router die minimale Abflußrate zu keinem Zeitpunkt überschreitet (vgl. Abbildung 11). Hieraus ist abzuleiten, daß Pakete, welche diese Bedingung im *Interior*- Bereich auch nur für die Dauer ihrer Vermittlung verletzen würden, durch das *Policing* zu verwerfen sind.

Um die Randbedingungen bestimmen zu können, unter welchen das *VW PDB* seine Eigenschaften erfüllen kann, ist eine theoretische Analyse zur Ermittlung der *Jitter*-Begrenzung erforderlich, welche in vollem Umfang der Definition des *VW PDBs* zu entnehmen ist und hier - mit Rücksicht auf den Themenschwerpunkt der Ausarbeitung - nur kurz und in anschaulicher Weise dargestellt wird.

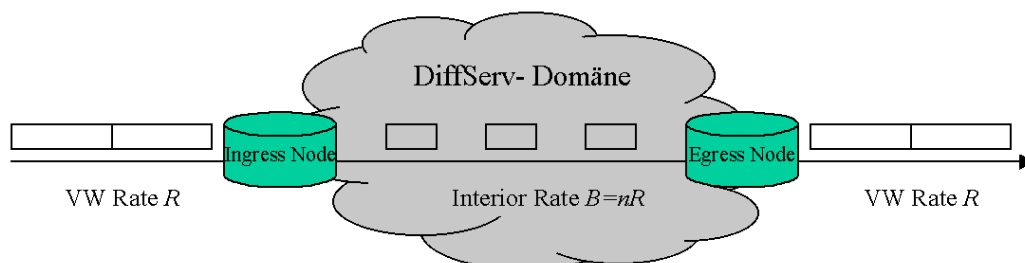


Abbildung 13: VW Aggregat beim Durchqueren einer DiffServ-Domäne ($n=2$)

Betrachtet wird nach Abbildung 13 ein *Virtual Wire* Aggregat der Rate R , welches den Bereich einer *DiffServ-Domäne*, also sämtliche involvierte *Interior Nodes* (nicht dargestellt), mit einer Rate von $B=nR$ ($n>1$) durchquert.

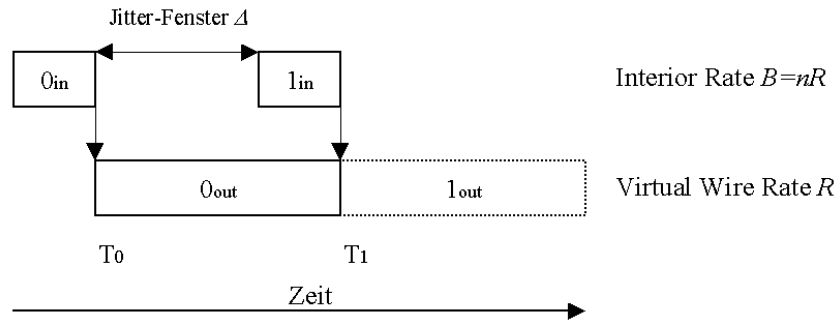


Abbildung 14: Egress Node: Darstellung des Jitter- Fensters

Nach Abbildung 14 ist erkennbar, daß Pakete des *VW* Aggregats der Größe S , welche den *Egress Router* mit Rate B betreten, bei ihrer Ankunft um den als *Jitter-Fenster* D bezeichneten Zeitraum vom erwarteten Zeitpunkt des Eintreffens abweichen können, ohne die unterbrechungsfreie Ausgabe des Datenstroms auf dem *Virtual Wire*- Link zu gefährden. Hierbei muß lediglich die Bedingung erfüllt sein, daß das letzte Bit des Pakets k vor dem Zeitpunkt

$$T_k = k \cdot \frac{S}{R}$$

am *Egress Router* eingetroffen sein muß.

Aus dieser Feststellung läßt sich die Zeitdauer des *Jitter- Fensters* berechnen zu:

$$\Delta = \frac{S}{R} - \frac{S}{n \cdot R} = \frac{S}{R} \cdot \frac{n-1}{n}$$

In der Praxis kann diese Formel genutzt werden, die maximale Rate R zu ermitteln, welche allen Flüssen des *Virtual Wire* Aggregats zugewiesen werden kann.

$$R = \frac{S}{\Delta} \cdot \frac{n-1}{n}$$

Zur Ermittlung der Parameter n und D sind grundsätzliche Überlegungen zur Netzdimensionierung dahingehend erforderlich, unter welchen Voraussetzungen die Eigenschaften des *VW PDBs* innerhalb der *DiffServ- Domäne* sichergestellt werden können.

Zunächst ist die Annahme erforderlich, daß sich Pakete unterschiedlicher Flüsse des *Virtual Wire* Aggregats an keiner Stelle innerhalb des Netzes gegenseitig beeinflussen. Sie bedingt, daß sämtliche Permutationen (im Falle $n=2$ die Vertauschung) von *VW*- Paketen innerhalb eines „Zeitfensters“ (gestrichelte Rechtecke in Abbildung 15), wie sie innerhalb von Routern beispielsweise durch Pufferung entstehen können, die kontinuierliche Ausgabe des Datenstroms bei den *Egress Nodes* nicht beeinträchtigen dürfen (*Jitter Independence*).

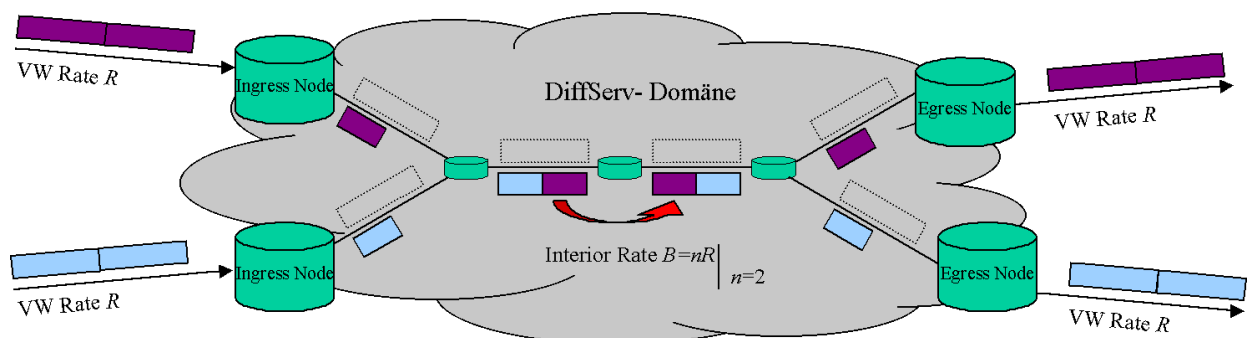


Abbildung 15: Aggregation von *VW*- Flüssen

Abbildung 15 ist anschaulich zu entnehmen, daß die Bedingung der *Jitter Independence* erfüllt werden kann, wenn durch geeignete Wahl des Parameters n je ein Paket sämtlicher auf einem *Interior Link* „parallel“ zu vermittelnder Flüsse des VW Aggregats innerhalb eines Zeitfensters übertragen werden kann.

Eine Schwierigkeit besteht darin, daß im allgemeinen Fall Flüsse innerhalb der Domäne an beliebiger Stelle konvergieren bzw. divergieren können. Falls eine statische Dimensionierung des Parameters n angestrebt wird, ist der *Worst Case* (siehe Abbildung 16 a)) der maximalen Anzahl parallel zu vermittelnder Flüsse innerhalb der gesamten Domäne anzunehmen.

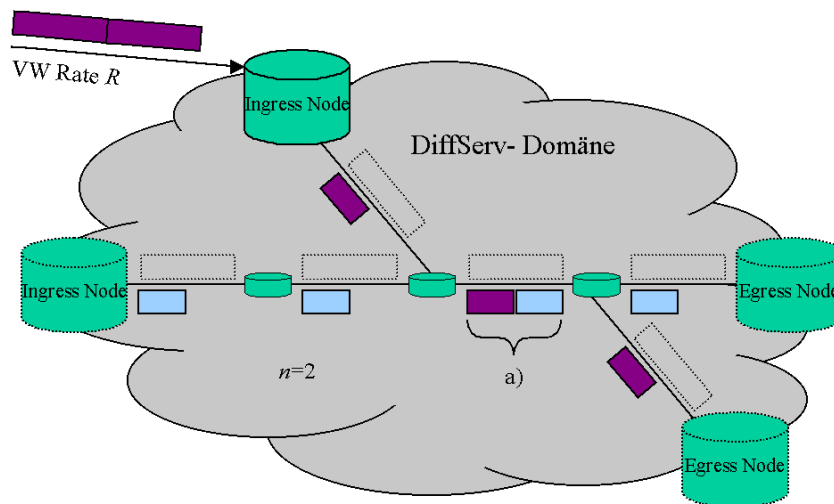


Abbildung 16: Dimensionierung nach Worst Case

Auch der Fall unterschiedlicher VW Raten der einzelnen Flüsse erfordert weitergehende Überlegungen. Es muß sichergestellt sein, daß Pakete von Flüssen geringerer Raten, welchen ein größeres Zeitfenster bei der Vermittlung zur Verfügung steht, nicht kleinere Zeitfenster von Flüssen höherer Raten blockieren (siehe Abbildung 17).

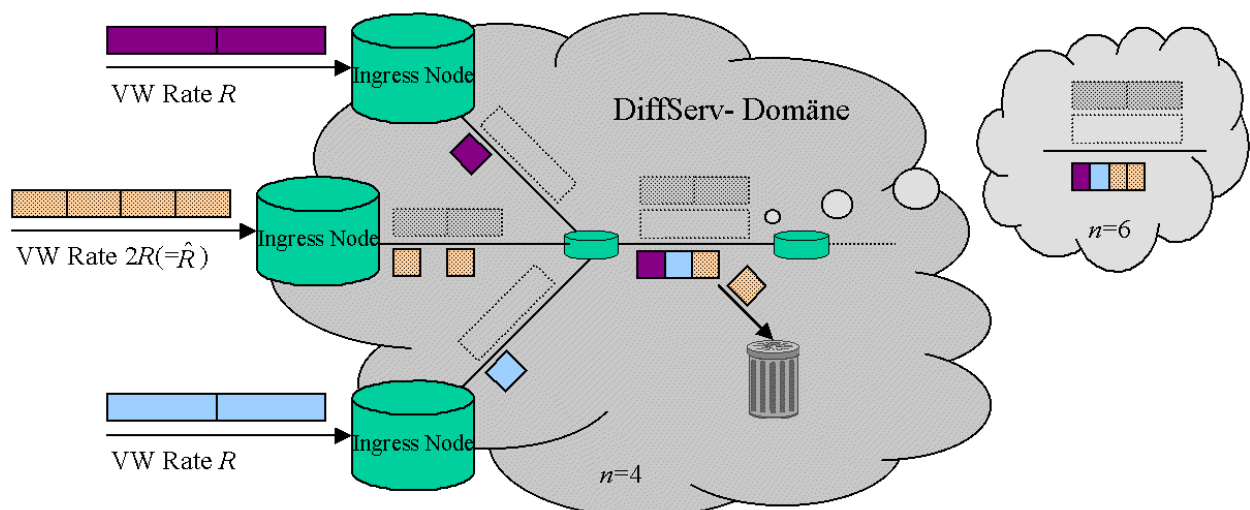


Abbildung 17: Gegenseitige Blockierung von VW-Flüssen bei unterschiedlichen Raten

Eine mögliche Lösung dieses Problems besteht darin, die Dimensionierung des Parameters n anhand des Produktes aus Anzahl maximaler paralleler Flüsse und maximaler Rate \hat{R} vorzunehmen, wobei die Abbildung 16 zugrundeliegenden Überlegungen mit zu berücksichtigen sind. Der in Abbildung 17 für $n=6$ skizzierte Fall zeigt, daß somit die gegenseitige Blockierung vermieden werden kann, jedoch ein Drittel der Leitungskapazität ungenutzt bleibt.

Nach Klärung der Dimensionierung des Parameters n sind abschließende Überlegungen zur Größe des *Jitter Fenster*- Parameters D notwendig, welcher (wiederum) im Sinne einer *Worst- Case*- Analyse der maximalen Verzögerung gleichgesetzt wird, die Pakete des Aggregats beim Durchlaufen der Domäne erfahren können.

Da sich gemäß der vorgenannten Überlegungen Pakete des *VW* Aggregats - bei konsistenter Dimensionierung der Domäne - nicht gegenseitig blockieren können und nach Definition des zugrundeliegenden *EF PHBs* Router diese Pakete bevorzugt vor anderem Verkehr vermitteln, verbleibt als einzige Verzögerungsquelle pro Router das Fertigstellen eines Nicht- *EF*- Paketes. Dieser Vorgang nimmt maximal ein Zeitintervall von

$$t_h = S/B$$

in Anspruch, so daß bei einem Netzdurchmesser von D die maximale Gesamtverzögerung eines *VW*- Paketes beim Durchqueren einer *DiffServ*- Domäne zu

$$t_h \cdot D = \Delta$$

angegeben werden kann.

Es ergibt sich bei Einsetzen in die Ausgangsgleichung:

$$\Delta = \frac{S}{R} \cdot \frac{n-1}{n} = D \frac{S}{n \cdot R} \Rightarrow n-1 = D \Rightarrow \underline{n = D+1},$$

so daß n mindestens einen Wert von $n_{min}=2$ annehmen muß und die Rate R , welche die für *Virtual Wire* Aggregate zur Verfügung stehende Bitrate beschreibt, nach oben durch

$$R_{max} = \frac{B}{n_{min}} = \frac{B}{2}$$

beschränkt ist.

3.9 Zusammenfassung DiffServ

Anhand der beispielhaft angeführten Definitionen von *Per Domain Behaviours* konnte nachvollzogen werden, in welcher Weise sich die dort gemachten Angaben auf technische Realisierungsrichtlinien abbilden lassen und wie Abhängigkeiten der *PDB*- Eigenschaften von inneren Zuständen einer *DiffServ*- Domäne beschrieben werden.

Am Beispiel *Virtual Wire* ist erkennbar, daß der Implementierung des *PDBs* innerhalb einer *DiffServ*- Domäne ein anspruchsvoller Dimensionierungsprozeß vorangestellt werden muß, welcher mit der Größe der Netzwerk- Topologie und maximalen „Teilnehmerzahl“ an Komplexität gewinnt. Im Sinne einer statischen Auslegung sind hierbei die technischen Anforderungen, die sich aus den mit Kunden abgeschlossenen *Service Level Agreements* ergeben, auf die Netzwerkstruktur des *Interior*- Bereichs abzubilden und die *Ingress*- Nodes in einer Weise zu konfigurieren, daß die Spezifikationen der *SLAs* durch die *Upstream Domains* exakt eingehalten werden. Diese Feststellung bringt mit sich, daß der Dimensionierungs- Prozeß mit Änderungen der Vertragsverhältnisse jeweils von neuem angestoßen werden muß, um die verfügbaren Ressourcen weiterhin effektiv nutzen und die zugesicherten Eigenschaften gewährleisten zu können.

Da dieser Ansatz einen großen administrativen Aufwand mit sich bringt und insbesondere die Möglichkeit der wirtschaftlichen Implementierung des *Virtual Wire PDBs* fraglich wäre, läge es vor allem im Kontext der netzübergreifenden Verfügbarkeit von QoS- Diensten im Interesse der Betreiber, eine dynamische Zuweisung verfügbarer Ressourcen nach Bedarf an potentielle Nutzer von QoS- Dienstleistungen realisieren zu können.

Diese Möglichkeit beinhaltet das Konzept des *Bandwidth Brokers*, welches in dieser Ausarbeitung abschließend vorgestellt wird.

4 Bandwidth Broker

4.1 Generelle Systembeschreibung

Der Begriff des *Bandwidth Brokers (BB)* (nach [21]) beschreibt eine Instanz innerhalb einer *DiffServ- Domäne*, welche Entscheidungen über die Zuweisung von internen Netzwerk- Ressourcen aufgrund der *Service Level Specifications* mit benachbarten Domänen und lokaler Richtlinien zur Erbringung von QoS- Diensten trifft.

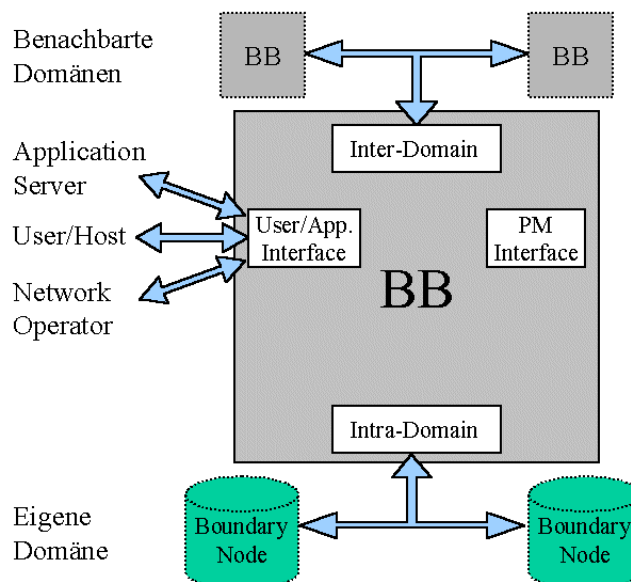


Abbildung 18: Schematische Darstellung Bandwidth Broker (nach [22])

Der *Policy Manager (PM)* (vgl. [23]) stellt hierbei eine übergeordnete (administrative) Instanz dar, welche sich des *BBs* zur Durchsetzung der auf einem *Policy Server (PS)* hinterlegten Richtlinien bedient (vgl. Abbildung 18).

Wie am Beispiel des *Virtual Wire PDBs* (siehe 3.8.4) ersichtlich ist, basiert die Entscheidung zur Bereitstellbarkeit angeforderter QoS- Dienste aus technischer Sicht auf Kenntnissen über die interne Netzstruktur sowie deren (theoretischen) Auslastungszustand, und reflektiert sich in Konfigurationsänderungen der Router, welche aus den Dienstleistungs- Anforderungen abzuleiten sind. Betroffen hiervon sind vor allem die *Boundary Nodes*, welche durch *Traffic Conditioning-* Maßnahmen die Einhaltung von *Service Level Specifications* sicherstellen. Im Rahmen des geschilderten Szenarios ist der *Bandwidth Broker* folglich aufgrund der Notwendigkeit der konsistenten Verfügbarkeit dieser Zustandsinformation exklusiv berechtigt, Änderungen an der Konfiguration der Domänen- eigenen Router vorzunehmen (nach [21]). Das *Intra- Domain-* Interface (siehe Abbildung 18) stellt hierbei die Schnittstelle dar, über welche die Router mit Anwendungsschicht- Protokollen wie dem *Simple Network Management Protocol (SNMP)*, *Telnet* oder dem durch die *IETF* in [24] spezifizierten *Common Open Policy Service (COPS)* konfiguriert werden können.

Einer Entscheidung über Ressourcen- Zuteilung durch den *Bandwidth Broker* geht eine Anfrage voraus, welche entweder innerhalb der *DiffServ- Domäne* ihren Ursprung hat (*Resource Allocation Request RAR* über das *User/Application Interface*), oder von einem *Bandwidth Broker* aus einer benachbarten Domäne stammt (*Inter- Domain Interface*). Lokale Anfragen können ferner direkt vom Benutzer initiiert werden (*User/Host*) oder von einem *Application Server / Gateway* stammen (siehe Abbildung 18).

4.2 Anwendungsszenario

Im folgenden wird ein Szenario betrachtet, nach welchem Benutzer a in Domäne A mit Benutzer g in Domäne C kommunizieren möchte. Domäne A kann hierbei ein großes *DiffServ- fähiges Firmennetz* oder das Zugangsnetz eines *Internet Service Providers* umfassen. Jede dieser Domänen besitzt nach [21] (mindestens) einen zuständigen *Bandwidth Broker BB*, welcher den *Resource Allocation Request* von a beziehungsweise die Anfragen benachbarter *BB* bearbeitet. Dem ersten Router in Verkehrsflußrichtung nach a kommt dabei nach 3.3.1 die Funktion eines *Ingress Nodes* zu.

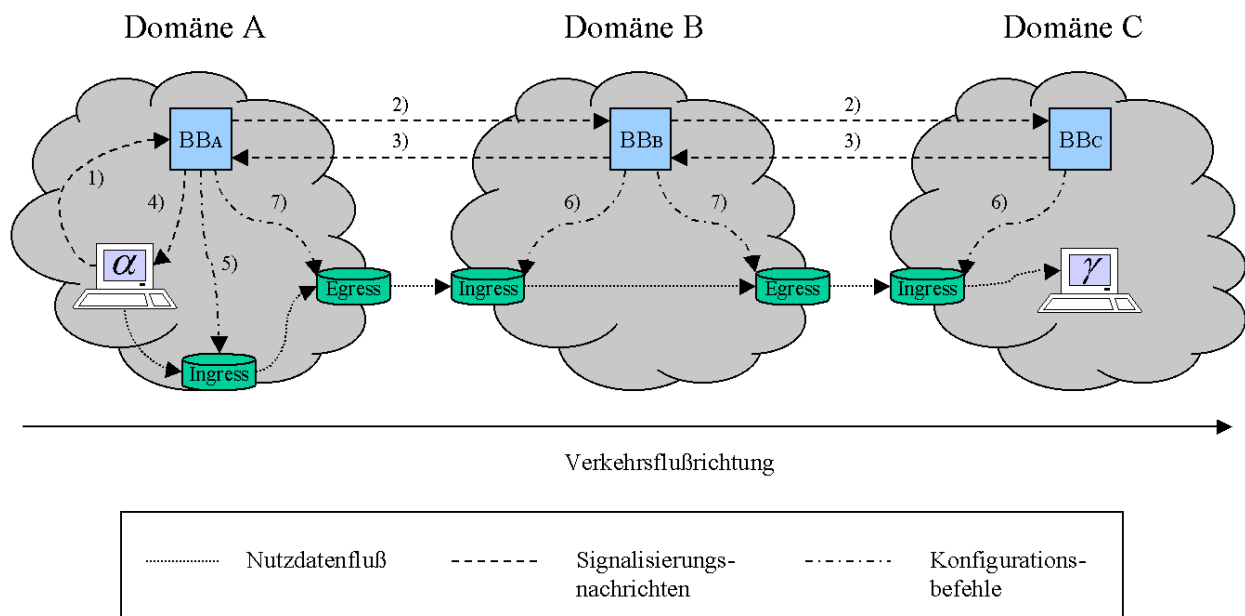


Abbildung 19: Domänenübergreifende Bandwidth Broker- Kommunikation

Zunächst gibt a seinen Verbindungswunsch gegenüber dem lokalen *Bandwidth Broker* BB_A in Form eines *Resource Allocation Requests* bekannt (Abbildung 19 1)). Ein *RAR* beinhaltet nach [21] die Dienstart, erforderliche Übertragungsrate, maximale *Burst- Größe* sowie Zeitpunkt und Dauer der gewünschten Reservierung.

BB_A ermittelt daraufhin, ob es sich um eine lokale oder Domänen- übergreifende Reservierung handelt und überprüft, ob innerhalb der eigenen Domäne ausreichende Ressourcen für die Einrichtung der Reservierung zur Verfügung stehen. Sollte diese Bedingung erfüllt sein, fordert BB_A die zusätzliche Kapazität auf dem Link zu Domäne B bei BB_B an (2)), welcher nach Prüfung der lokalen Ressourcen eine ähnliche Aushandlung mit BB_C durchführt. Sollte die Anfrage von allen *Bandwidth Brokern* auf dem Verbindungsweg von a nach g positiv bestätigt worden sein (3)), wird a die Reservierung zugesagt (4)) und werden die *Boundary Router* in den betroffenen Domänen entsprechend konfiguriert.

Innerhalb der *Source Domain A* muß anhand der Dienstart des *RAR* das *Traffic Conditioning* des *Ingress Nodes* in der Weise konfiguriert werden, daß für die Zeitdauer der Reservierung eine Zuordnung des Datenstroms zu einem entsprechenden *Behaviour Aggregate* durchgeführt wird (5). Die *Ingress Nodes* aller anderen Domänen müssen instruiert werden, die zusätzliche Datenrate beim *Traffic Conditioning* des *BAs* zu berücksichtigen (6). Während eine genaue Spezifikation der zulässigen Datenrate pro *BA* in den *Ingress Nodes* erforderlich ist, um eine mißbräuchliche Nutzung (physikalisch) freier Leitungskapazität durch die *Upstream Domains* zu verhindern, kann das *Traffic Conditioning* in den *Egress Nodes* aus Gründen der Beschränkung des Administrationsaufwands auf die mit der *Downstream Domain* jeweils ausgehandelte maximale Datenrate pro *BA* konfiguriert werden. Sollte jedoch nicht in dieser Weise vorgegangen werden, ist auch das *Traffic Conditioning* in diesen *Nodes* anzupassen (7).

(Im Sinne einer bidirektionalen Kommunikationsbeziehung ist der geschilderte Ablauf sowohl von *a* als auch von *g* aus zu initiieren.)

Die Aushandlung der Reservierung kann je nach der Art der *Service Level Specifications* zwischen zwei aneinander angrenzenden Domänen unterschiedlich ausfallen. Im beschriebenen Fall wurde die Verfügbarkeit der gewünschten Ressourcen auf dem gesamten Verbindungsweg („*End-to-End*“, nach [22]) durch Signalisierungsnachrichten zwischen benachbarten *Bandwidth Brokern* sichergestellt. Wenn zwischen zwei Domänen eine fest vereinbarte Höchstgrenze eines *Behaviour Aggregates* vertraglich festgelegt wurde und der *Bandwidth Broker* der *Upstream Domain* einen Reservierungswunsch mit der noch verfügbaren Rate abdecken kann, können Teile der Signalisierung entfallen. Insbesondere wird in diesem Fall keine Bestätigung der Reservierung vom *Bandwidth Broker* der *Downstream Domain* erwartet, sondern dem anfordernden System sofort eine Zusage erteilt (*Immediate Response*, nach [22]). Probleme treten bei dieser Methode dann auf, wenn weiter in *Downstream*- Richtung gelegene Domänen den ankommenden Verkehr beispielsweise aufgrund fehlender Kapazitäten am *Ingress* verwerfen. Denkbar ist die Anwendung des *Immediate Response*- Verfahrens jedoch bei Diensten, welche eine bevorzugte Behandlung von Daten zwar anstreben, jedoch nicht garantieren.

4.3 Interaktion mit IntServ/RSVP

Wie im Zuge der Vorstellung der *Integrated Services* unter 2.3 bereits angedeutet, kann beispielsweise mit Hilfe der *Bandwidth Broker* ein Übergang von Fluß- basierter Dienstgüte (*Per-Flow*), auf die leichter zu handhabenden aggregierten Flüsse der *DiffServ*- Architektur geschaffen werden.

Die *BB* können in der Art konfiguriert werden, die Pakete des *Resource Reservation Protocol* abzufangen und die darin geforderte Dienstgüte auf die *DiffServ*- Architektur abzubilden. Nach den zuvor beschriebenen Verfahren zur Aushandlung mit benachbarten Domänen kann eine weitere Kommunikation mit den betroffenen Endsystemen über *RSVP* stattfinden.

Auf diese Weise ist es auch möglich, Dienstgüte auf einem Verbindungsweg auszuhandeln, welcher *DiffServ*- inkompatible Domänen enthält, die jedoch über *RSVP* (*IntServ*)- fähige Router verfügen. Bei der Reservierung wird hierzu neben der *Bandwidth Broker*- Signalisierung auch eine entsprechende *RSVP*- Anfrage mit übermittelt, welche dann nur von den *RSVP*- Routern der inkompatiblen Domänen ausgewertet wird.

Zusammenfassung

Ausgehend von der gegenwärtigen Dienstgüte- Situation im Internet wurden bestehende *Quality of Service*- Ansätze vorgestellt und ihr heutiger praktischer Nutzen sowie möglicher Einsatz in zukünftigen Konzepten diskutiert. Die *Differentiated Services* wurden als adäquate Basis für betreiberübergreifende QoS- Konzepte identifiziert und in angemessener Ausführlichkeit vorgestellt.

Es wurde veranschaulicht, wie sich mit ihrer Hilfe betreiberübergreifende Dienstgüte-Konzepte auf Basis statischer, vertraglich festgelegter Kenngrößen realisieren lassen, sowie im Hinblick auf die durch Teilnehmer initiierte Kommunikation eine Möglichkeit aufgezeigt, dynamische Reservierungen über Netzgrenzen hinweg vorzunehmen.

Unter Anwendung dieser Kenntnisse läßt sich das in der Einleitung skizzierte, betreiberübergreifende Dienstgüte- Szenario beispielsweise wie folgt realisieren:

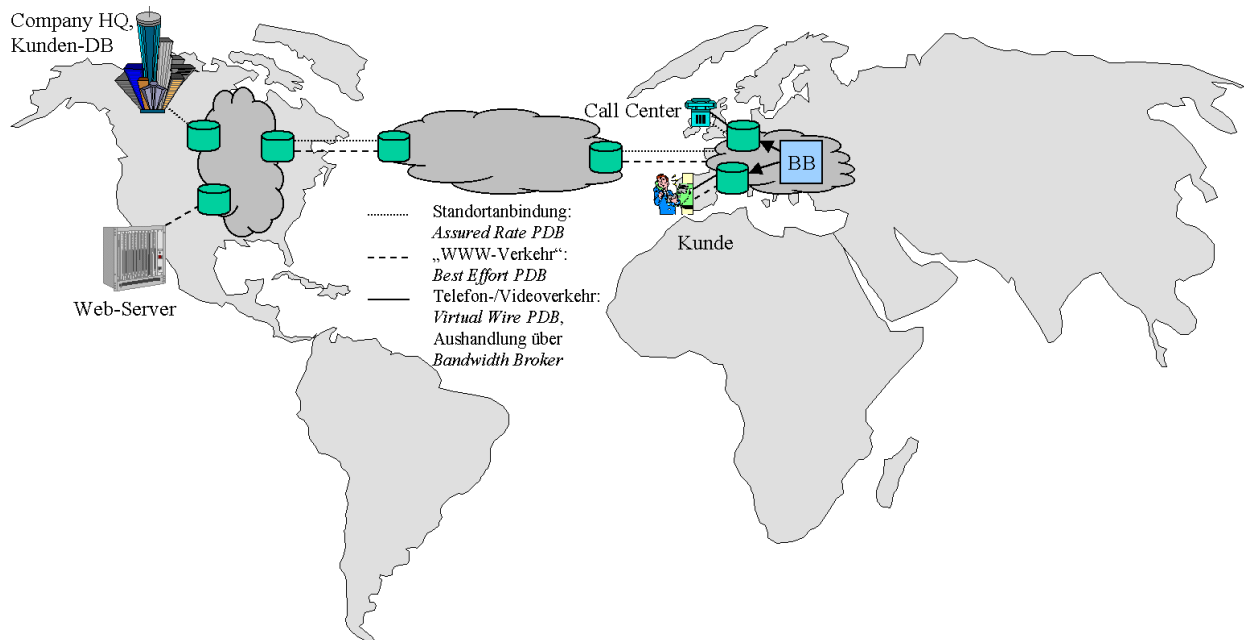


Abbildung 20: Szenario der möglichen Realisierung betreiberübergreifender Dienstgüte

Literaturverzeichnis

- [1] UUNET USA: Leased Line SLA.
<http://www.uu.net/us/support/sla/service-supported/uudirect.xml>, 2001.
- [2] WORLDCOM: Internet Service Level Agreement.
http://www.worldcom.com/terms/service_level_guarantee/t_sla_terms.phtml, 2001.
- [3] Cable&Wireless IDC: global.net SLA.
http://www.cw.com/th_19.asp?ID=jp_8_10_3_en, 2001.
- [4] CISCO: Designing Service Provider Core Networks to Deliver Real-Time Services.
http://www.cisco.com/warp/public/cc/pd/rt/12000/tech/ipra_wp.htm, 2001.
- [5] Postel; Information Sciences Institute, University of Southern California:
RFC 791, INTERNET PROTOCOL, DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION.
<http://www.ietf.org/rfc/rfc0791.txt>, 1981.
- [6] Almquist; IETF Network Working Group:
RFC 1349, Type of Service in the Internet Protocol Suite.
<http://www.ietf.org/rfc/rfc1349.txt>, 1992.
- [7] CISCO: DiffServ Frequently Asked Questions.
http://www.cisco.com/warp/public/cc/pd/iosw/ioft/ioqo/tech/dffs_qa.htm, 2001.
- [8] Braden, Clark, Shenker; IETF Network Working Group:
RFC 1633, Integrated Services in the Internet Architecture: an Overview.
<http://www.ietf.org/rfc/rfc1633.txt>, 1994.
- [9] Blake, Black, Carlson, Davies, Wang, Weiss; IETF Network Working Group:
RFC 2475, An Architecture for Differentiated Services.
<http://www.ietf.org/rfc/rfc2475.txt>, 1998.
- [10] Grossman; IETF Diffserv Working Group: DRAFT, New Terminology for Diffserv.
<http://www.ietf.org/internet-drafts/draft-ietf-diffserv-new-terms-04.txt>, 2001.
- [11] Nichols, Blake, Baker, Black; IETF Network Working Group:
RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.
<http://www.ietf.org/rfc/rfc2474.txt>, 1998.
- [12] Black, Brim, Carpenter, Le Faucheur; IETF Diffserv Working Group:
DRAFT, Per Hop Behavior Identification Codes.
<http://www.ietf.org/internet-drafts/draft-ietf-diffserv-2836bis-02.txt>, 2001.
- [13] Heinanen, Baker, Weiss, Wroclawski; IETF Network Working Group:
RFC 2597, Assured Forwarding PHB Group.
<http://www.ietf.org/rfc/rfc2597.txt>, 1999.
- [14] Jacobson, Nichols, Poduri; IETF Network Working Group:
RFC 2598, An Expedited Forwarding PHB.
<http://www.ietf.org/rfc/rfc2598.txt>, 1999.

- [15] Charny, Baker, Davie, Le Boudec, Courtney, Firoiu, Ramakrishnam;
IETF Network Working Group:
DRAFT, Supplemental Information for the New Definition of the EF PHB.
<http://www.ietf.org/internet-drafts/draft-ietf-diffserv-ef-supplemental-01.txt>, 2001.
- [16] Nichols, Carpenter; IETF Network Working Group:
RFC 3086, Definition of Differentiated Services Per Domain Behaviors and Rules for their Specification.
<http://www.ietf.org/rfc/rfc3086.txt>, 2001.
- [17] Nichols; Packet Design INC.: IP Quality of Service in the IETF.
<http://www.icc00.org/present/ba2kmn.pdf>, 2000.
- [18] Carpenter, Nichols; IETF Diffserv Working Group:
DRAFT, A Bulk Handling Per-Domain Behaviour for Differentiated Services.
<http://www.ietf.org/internet-drafts/draft-ietf-diffserv-pdb-bh-02.txt>, 2001.
- [19] Seddigh, Nandy, Heinanen; IETF Diffserv Working Group:
DRAFT, An Assured Rate Per-Domain Behaviour for Differentiated Services.
<http://www.ietf.org/internet-drafts/draft-ietf-diffserv-pdb-ar-00.txt>, 2001.
- [20] Jacobson, Nichols, Poduri; IETF Diffserv Working Group:
DRAFT, The 'Virtual Wire' Per-Domain Behaviour.
http://www.packetdesign.com/Docs/vw_pdb_0.pdf, 2000.
- [21] Nichols, Jacobson; CISCO, Zhang; UCLA:
DRAFT, A Two-bit Differentiated Services Architecture for the Internet.
<ftp://ftp.ee.lbl.gov/papers/dsarch.pdf>, 1999.
- [22] Neilson, Wheeler, Reichmeyer, Hares; Internet2 Qbone BB Advisory Council:
A Discussion of Bandwidth Broker Requirements for Internet2 Qbone Deployment.
http://www.merit.edu/internet/working.groups/i2-qbone-bb/doc/BB_Req7.pdf, 1999.
- [23] CISCO: COPS QoS Policy Manager 2.0.
http://www.cisco.com/warp/public/cc/pd/wr2k/qoppmn/prodlit/qpcop_ds.pdf, 2000.
- [24] Chan, Seligson, Durham, Gai, McCloghrie, Herzog, Reichmeyer, Yavatkar, Smith;
IETF Network Working Group:
RFC 3084, COPS Usage for Policy Provisioning (COPS-PR).
<http://www.ietf.org/rfc/rfc3084.txt>, 2001.