Evaluation von Assured Service für das Internet

Florian Baumgartner und Torsten Braun

Institut für Informatik und angewandte Mathematik
Neubrückstrasse 10, CH-3012 Bern, Schweiz
baumgart|braun@iam.unibe.ch

Zusammenfassung Der Assured Service wurde im Rahmen der Differentiated Services (Diffserv) Arbeitsgruppe der IETF als ein möglicher Diffserv-Dienst vorgeschlagen. Das Paper evaluiert das Konzept der Assured Services anhand von Simulationen verschiedener Netzszenarien und auf UDP bzw. TCP beruhenden Anwendungen. Hierbei wird gezeigt, daß durch Assured Services unterstützte Datenflüsse in Lastfällen wesentlich höhere Dienstgüten (Bandbreite und abhängig von Queuing-Varianten auch Verzögerungen) erreichen als Best-Effort Datenflüsse. Des weiteren wird ein Queuing-Verfahren vorgestellt, welches die Verzögerungen für hochpriore Datenflüsse verbessert und gleichzeitig Reihenfolgevertauschungen minimiert.

1 Einführung

Höherwertige Dienste als Best-Effort Dienste lassen sich mit dem auf RSVP [BZB+97] basierenden Integrated Services Ansatz - zumindest in großen IP-Netzen - aus Skalierungsgründen nicht erreichen [MBB+97]. Als Alternative - speziell für IP-Backbone Netze wurde das Konzept der Differentiated Services entwickelt [BBC+98]. Dieser Beitrag beschreibt in Kapitel 2 einen im Differentiated Services Umfeld definierten Dienst, den Assured Service. Abschnitt 3.1 stellt die Simulationsumgebung und das zur Bewertung von Assured Services verwendete Simulationsmodell dar. Die Ergebnisse der Simulationen werden in Kapitel 4 diskutiert. Dabei werden die in [CW97] veröffentlichten Ergebnisse um Verzögerungsaspekte erweitert Verbesserungsmöglichkeiten vorgeschlagen. Abschnitt 5 diskutiert eine Variante des Queuing-Verfahrens zur zusätzlichen Minimierung von Reihenfolgevertauschungen. Kapitel 6 faßt den Beitrag zusammen und gibt einen Ausblick auf zukünftige Arbeiten.

2 Differentiated Services

Der Differentiated Ansatz [BBC+98] basiert im Gegensatz zur Integrated Services Architektur auf einer Aggregation von Anwendungsdatenflüssen, d.h. Re-

servierungen sollen für eine Menge von zusammengehörenden Flüssen, z.B. für alle Flüsse zwischen zwei Subnetzen, erfolgen.

Hierbei werden die IP-Pakete durch den Benutzer (entweder im Endsystem oder durch einen Router) oder den Service Provider mit unterschiedlichen Prioritäten versehen. Den einzelnen Prioritätsklassen werden in den Routern dann entsprechende Mengen von Ressourcen (insbesondere Bandbreiten) zugewiesen. Ein Internet Service Provider (ISP) kann dadurch seinen Benutzern verschiedene, mit unterschiedlichen Kosten verbundenen Dienstgüteklassen anbieten. Zur Markierung der Pakete wird das sogenannte DS-Feld (Differentiated Services Field) im IP-Header verwendet, welches in IPv4 auf das Type-of-Service Oktett (ToS) und in IPv6 auf das Traffic-Class Oktett abgebildet wird [NBBB98].

Der Assured Service - als ein spezieller Differentiated-Service-Dienst - versucht einen Dienst anzubieten, der zwar nicht wie andere Dienste (z.B. der Premium Service [NJZ97]) Bandbreiten garantieren kann, bei dem aber mit einer hohen Wahrscheinlichkeit davon auszugehen ist, daß die mit hoher Priorität gekennzeichneten Pakete zuverlässig vom ISP übertragen werden. Die Charakteristik des Dienstes richtet sich dabei nach den in den Routern beim Shaping und Policing verwendeten Markierungsverfahren, die meist auf Token Buckets basieren. Die Wahrscheinlichkeit, daß die Pakete korrekt übertragen werden, hängt von der Dimensionierung des Netzes ab. Ein ISP kann zwar die Summe aller Bandbreiten für Assured Services so wählen, daß die Bandbreite des Links mit der niedrigsten Bitrate nicht übertroffen wird. In diesem Fall wird dann im ISP-Netz aber nur ein sehr geringer Anteil der verfügbaren Kapazität allokiert. In der Regel werden aber nicht alle Benutzer ihre Assured Service Pakete über den Engpaß-Link senden, so daß es durchaus sinnvoll erscheint, eine höhere Gesamtbitrate zuzulassen. Allerdings ist es dann nicht ausgeschlossen, daß in ungünstigen Momenten (genau dann wenn alle Anwender Daten über den Engpaß-Link senden) Pakete wegen Überlastungen weggeworfen werden müssen.

Der Benutzer kennzeichnet entweder im Endsystem oder im sogenannten First-Hop-Router zum ISP-Netz die Pakete als hochprior, d.h. versieht sie mit einem A-Bit. Um Änderungen in den Endsystemen zu vermeiden, kann auch der First-Hop-Router die weiterzuleitenden Pakete bezüglich ihrer IP-Adressen und UDP-/TCP-Ports analysieren und dann eine entsprechende Priorität zuordnen. Hierbei ist natürlich auch zu beachten, daß die vereinbarte maximale Rate von hochprioren (A-Bit) Paketen nicht überschritten wird. Dies wird durch

Shaping-Funktionen in den First-Hop-Routern und Re-Shaping-Funktionen in den Border-Routern des Anwenders am Übergang zum ISP-Netz sowie durch Policing im ISP Netz sichergestellt. Der Service-Provider muß aber auf jeden Fall überprüfen, ob sich der Benutzer an die maximale Rate hochpriorer Pakete hält, und muß gegebenenfalls Korrektur-Maßnahmen ergreifen, falls dies nicht der Fall ist. Hierzu werden am Netzeingang der Border-Router des ISP nicht-konforme Pakete als niederprior (out-of-service, out-of-profile) gekennzeichnet.

2.1 Implementierungsaspekte

Zur Implementierung von Assured Services sind in Routern gewisse Modifikationen erforderlich. Im wesentlichen müssen Klassifizierungs-, Markierungs-, Shaping- und Policing-Funktionen in die Router aufgenommen werden. Diese Funktionen sind immer beim Übergang von einem Netz zum anderen erforderlich, zum Beispiel beim Übergang von einem Benutzernetz zum ISP oder auch zwischen ISPs. Zwischen ISPs müssen ähnlich wie zwischen Benutzer und ISP Dienstparameter vereinbart werden.

Abb. 1 zeigt das Funktionsprinzip eines First-Hop-Routers sowie eines Egress Border Routers für Assured Service. Empfangene Pakete werden hierbei jeweils klassifiziert und das A-Bit wird in einem Paket gesetzt, falls es Assured Service erfahren soll. Als Klassifikationsparameter können Quell-, Zieladressen, oder Informationen höhere Protokolle (z.B. Port-Nummern) dienen. Ein reines Best-Effort Paket wird direkt in das Ausgangs-Queuing-System - in der Regel in eine sogenannte RIO-Queue - geschrieben. In dieses Ausgangs-Queuing-System gelangen auch die Assured Service Pakete. Das A-Bit wird nur dann gesetzt, wenn ein Token im Token Bucket vorhanden ist. Ansonsten wird das A-Bit nicht gesetzt bzw. gelöscht, und das Paket wird im folgenden wie ein Best-Effort Paket behandelt. Die Token Buckets werden entsprechend der ausgehandelten Bitraten und Burst-Parameter gefüllt. Der Token Bucket kann dabei mehrere Tokens aufnehmen, so daß kurzzeitige Bursts unterstützt werden können. Die Größe des Buckets hängt von den vereinbarten Burst-Eigenschaften ab. Der Unterschied zwischen einem First-Hop-Router und einem Egress-Border-Router besteht darin, daß der First-Hop-Router ein Paket erstmals klassifiziert und gegebenenfalls diese Klassifikation auch auf Informationen höherer Protokolle (z.B. TCP-Ports, Anwendungstyp) erfolgen kann.

Der ISP muß schließlich prüfen, ob der Anwender sich auch tatsächlich an die vereinbarten Verkehrscharakteristiken hält. Hierzu muß der ISP durch seinen Ingress Border-Router, d.h. der Router, bei dem die Pakete von einer anderen DS-Domäne in die DS-Domäne des ISP eintreten, die Pakete daraufhin überprüfen, ob das vereinbarte Dienstprofil eingehalten wird. Ein Ingress Border-Router des ISPs wird daher das A-Bit der nicht-konformen Assured Service Pakete zurücksetzen.

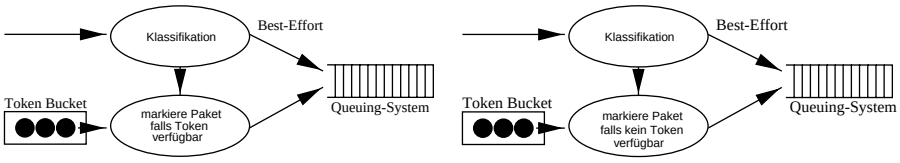

Abbildung1. links: First-Hop-Router und Egress Border-Router für Assured Service; rechts: Ingress Border-Router

2.2 Queuing

Ein wichtiges Element zur Implementierung von Assured Services sind geeignete Queue-Management-Verfahren zum Wegwerfen (Dropping) von Paketen in den Routern, um Überlastsituationen zu vermeiden. Für Assured Services wurde das sogenannte RIO-Queuing-Verfahren vorgeschlagen [CW97]. Als Basismechanismus von RIO wird der Random Early Detection (RED) [BCC+97] Mechanismus verwendet. RED ist ein Verfahren, welches versucht die Queue-Füllstände nicht über ein bestimmtes Limit anwachsen zu lassen, um so immer Reserven für Bursts bereitzuhalten. Dies erfolgt dadurch, daß Pakete bereits weggeworfen werden, wenn der Füllstand noch relativ gering ist. Unterhalb des unteren Schwellwerts werden dabei keine Pakete weggeworfen. Je stärker der Füllstand über den unteren Schwellwert ansteigt, desto höher ist die Dropping-Wahrscheinlichkeit für ein eintreffendes Paket, wobei das Wegwerfen der Pakete zufällig erfolgt und dadurch vermieden wird, daß nur Pakete eines bestimmten Anwendungsdatenflusses gelöscht werden. Erreicht der Füllstand schließlich den oberen Grenzwert, so werden alle Pakete weggeworfen.

RED kann insbesondere die verfügbare Bandbreite unter TCP-Datenflüssen in fairer Weise aufteilen, da Paketverluste automatisch zu einer Reduzierung der Paketrate eines TCP-Datenflusses führen. Problematischer ist die Situation bei nicht-TCP-konformen Datenflüssen wie z.B. auf UDP aufsetzenden Realzeitan-

wendungen oder Multicast-Anwendungen. Anwendungsdatenflüsse, die auf Paketverluste nicht entsprechend mit einer Anpassung der Datenrate reagieren, müssen besonders behandelt werden, um eine Überlastung des Netzes durch solche Datenflüsse zu verhindern.
RIO (RED with In and Out) ist eine Erweiterung des RED-Mechanismus. Für in-profile Pakete und für out-of-profile Pakete ist dabei eine gemeinsame Queue vorgesehen. Allerdings werden zwei unterschiedliche Dropping-Verfahren angewendet. Dieses soll sicherstellen, daß bei Überlast zunächst Best-Effort-Pakete und keine Assured Service Pakete weggeworfen werden. Durch die gemeinsame RIO-Queue können Reihefolgevertauschungen vermieden werden, was speziell für TCP-Implementierungen aus Leistungsaspekten sehr vorteilhaft ist. Der Dropper für out-of-profile Pakete (Out-Dropper) wirft Pakete sehr viel früher weg, d.h. bei einem wesentlich niedrigeren Füllstand als der Dropper für in-profile-Pakete (In-Dropper), d.h. für Pakete mit gesetztem A-Bit. Des weiteren steigen die Dropping-Wahrscheinlichkeiten des Out-Droppers sehr viel stärker an als beim In-Dropper. Dadurch wird versucht, die Wahrscheinlichkeit für das Wegwerfen von in-profile Paketen gering zu halten. Während der Out-Dropper zur Berechnung der Dropping-Wahrscheinlichkeit die Gesamtzahl der in der RIO-Queue enthaltenen Pakete berechnet, legt der In-Dropper nur die in-profile Pakete zugrunde. Ein Nachteil beim Einsatz von RIO-Queuing besteht sicherlich darin, daß in-profile Pakete die gleiche Verzögerung erfahren wie in die Queue aufgenommene out-of-profile Pakete. Durch das Setzen der Dropping-Wahrscheinlichkeit auf 1 für out-of-profile Pakete bei geringen Queue-Längen, kann dieser Nachteil reduziert aber nicht vollständig eliminiert werden.

3 Simulative Bewertung von Assured Services

Ziel der Simulationen ist die Untersuchung von Bandbreite und Verzögerung bei der Interaktion verschiedener Arten von Datenverkehr. So sichert der ISP jeweils zwei Kommunikationspartnern (beispielsweise zum Aufbau eines virtuellen privaten Netzes, VPN) eine bestimmte Bandbreite zu, während gleichzeitig niedrigpriorer Best-Effort-Verkehr transportiert werden soll.

3.1 Simulationsszenario

Zur Evaluation des Assured Service wurden Simulationen des in 2 dargestellten Szenarios vorgenommen. Sechs Netze verschiedener Benutzer mit Client- (C_{1-3})

und Server-Systemen (S_{1-3}) sind über einen ISP miteinander verbunden. In den Benutzer-Netzen sind First-Hop-Router und Border-Router in einem Router zusammengefaßt. Für Verkehr vom Netz mit S_1 zum Netz mit C_1 sind Assured Service Dienstvereinbarungen getroffen, dasselbe gilt für die Netze mit C_1 und S_1. Sämtliche Netz-Links haben eine Kapazität von 1 Mbit/s, so daß der Link zwischen den beiden ISP-Border-Routern den Engpaß darstellt. Im Gegensatz zu [IN98] wird dabei nicht nur die Interaktion von TCP Datenflüssen, sondern das Verhalten der Bandbreiten und Verzögerungen bei verschiedenen Arten von Verkehr (TCP und UDP) untersucht.

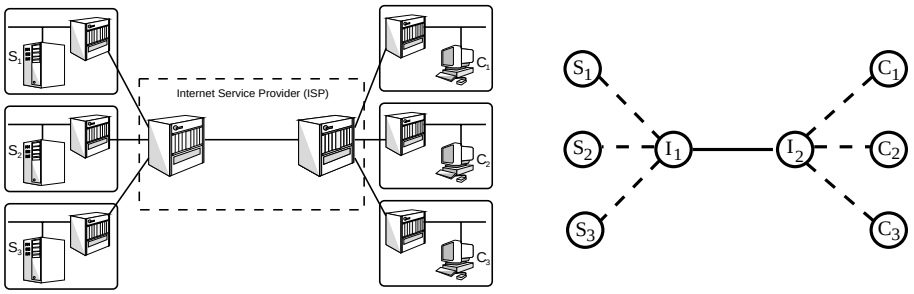

Abbildung2. Simulationsszenario

3.2 Implementierung in ns

Das in Abb. 2 dargestellte Simulationsszenario wurde auf ein Simulationsmodell für den Network Simulator [ns] wie folgt abgebildet. Zur Realisierung von Assured Services in ns wurden zwei Komponenten, sogenannte ns-Queues, implementiert. Die erste Komponente, der Tagger, übernimmt die Funktion des Egress-Border-Routers des Benutzers, d.h. er markiert anhand des Dienstgütenprofils (eine zugesicherten Bandbreite) die vom Kunden an den ISP gesendeten Pakete. Die zweite Komponente entspricht dem in [CW97] beschriebenen RIO Queuing-Verfahren.

Abb. 2 zeigt die Realisierung beschriebenen Topologie in ns. Die beiden Komponenten Tagger und RIO-Queue sind als Linien (Links) dargestellt, d.h. die Tagger-Komponente als gestrichelte Linie, die RIO-Queuing-Komponente als durchgezogene Linie. Hierbei wurde aus Vereinfachungsgründen auf die Modellierung der RIO-Queue in den Benutzer-Routern sowie auf die Tagging-Komponente in den ISP-Routern verzichtet, da sie die Simulation nicht beeinflussen. S_1 bis S_3 entsprechen den Servern, welche die unterschiedlichen Arten

von Verkehr erzeugen, C_1 bis C_3 den entsprechenden Clients. I_1 und I_2 sind Knoten des Internet Service Providers.

Tagger Die Aufgabe der Tagger-Komponente ist die Beurteilung, ob ein Paket innerhalb oder außerhalb des vereinbarten Dienstgütenprofils ist und die entsprechende Markierung zu setzen. Abb. 4 zeigt die Wahrscheinlichkeit für ein Paket als in-profile markiert zu werden in Abhängigkeit von der gesendeten Bandbreite. Die Kurve stellt dabei das vereinbarte Dienstprofil dar. Die übertragene Bandbreite wird aus der Paketgröße und der Zeitspanne zwischen zwei Paketen errechnet, wobei über jeweils beide Größen der exponentiell gewichtete Durchschnitt gebildet wird. Für eine problemlose Interaktion mit TCP/IP ist es dabei essentiell, nur langsam auf Änderungen der Bandbreite zu reagieren.

RIO Queues Generell gibt es zwei Ansätze für die Implementierung des RIO-Verfahrens. Im allgemeinen wird mit einer gemeinsamen Queue für in und out-of-profile Pakete gearbeitet. Die höhere Priorität von in-profile Paketen wird durch eine andere Dropping-Wahrscheinlichkeit realisiert. Neben dem Vorteil der recht einfachen Implementierung stellt dieser Algorithmus sicher, daß die Paketreihenfolge erhalten bleibt.
Eine anderer - hier vorgeschlagener - Ansatz sieht zwei unterschiedliche Queues für in-profile und out-of-profile Verkehr vor. Da die in-Queue bevorzugt geleert wird, kann in Stausituationen der hochpriore Verkehr am normalen Best-Effort Verkehr „vorbeigeleitet“ werden. Gleichzeitig vereinfacht dieses Verfahren die Einhaltung einer maximalen Verzögerung innerhalb der Queue. Der große Nachteil allerdings ist, daß bei Flüssen, die teils aus in-profile und teils aus out-of-profile Paketen bestehen, die Paketreihenfolge vertauscht werden kann.

3.3 Durchführung der Simulationen

Bei den Simulationen wurde das Zusammenwirken verschiedener Arten von Verkehr untersucht. So laufen parallel eine ftp-Verbindung und eine telnet-Sitzung. Zusätzlich ist einer Verbindung mit konstanter Bitrate aktiv, die als nicht TCP konformer Sender eingesetzt wird. Gemessen wird jeweils die erreichte Bandbreite der einzelnen Flüsse und die Verzögerung der Pakete. Gemäß der zugesicherten Bandbreite wird in den Tagger-Komponenten ein Teil der Pakete als in-profile markiert, in der RIO Queue zwischen I_1 und I_2 werden dann bei Überlastung die

einzelnen Pakete mit unterschiedlicher Wahrscheinlichkeit verworfen. Gemessen wird der Verkehr an dem Endpunkt der RIO-Queue am Knoten I2.

4 Ergebnisse

In diesem Kapitel werden die Simulationsergebnisse vorgestellt und diskutiert, die mit dem in Abschnitt 3 dargestellten Simulationsszenario gewonnen wurden. Zunächst wird dabei das Verhalten der untersuchten Datenströme ohne Assured Service Unterstützung untersucht, danach wird der Einfluß von Assured Service Unterstützung analysiert.
Zu Vergleichszwecken wird zunächst das Verhalten der Flüsse ohne Zusicherung von Bandbreiten dargestellt. Abb. 3 zeigt die von den einzelnen Datenflüssen erreichten Bandbreitenwerte, Abb. 3 stellt die Verzögerung der Datenpakete dar. Die einzelnen Datenquellen beginnen dabei zeitlich versetzt zu senden. Statt des RIO-Queuings wurde auf dem Link I_1-I_2 ein einfaches RED-Queuing simuliert, wobei ab einer halbvollen Warteschlange Pakete mit linear steigender Wahrscheinlichkeit verworfen werden. Die ftp- Verbindung zwischen S_1 und C_1 wird in der 10. Sekunde aufgebaut und lastet die Verbindung (maximale Bandbreite 1 Mbit/s) komplett aus, die Telnet-Sitzung zwischen S2 und C2 startet 10 Sekunden später in der 20. Sekunde, verfügt über die gleiche maximale Bandbreite, erzeugt jedoch typischerweise sehr wenig Verkehr. In der 30. Sekunde beginnt S3 Datenpakete mit einer konstanten Bitrate von 0.8 Mbit/s an C3 zu senden. Wie aus Abb. 3 ersichtlich ist, erreicht der aggressive Fluß fast seine volle Bandbreite von 0.8 Mbit/s, der ftp-Sender reagiert aufgrund der in TCP integrierten Staukontrolle auf die Stausituation und drosselt die Bandbreite. Damit erhält der nicht-TCP-konforme CBR-Datenfluß auf Kosten der TCP-konformen ftp-Anwendung den Großteil der verfügbaren Bandbreite.
Die Paketverzögerungen auf den drei Verbindungen verhalten sich erwartungsgemäß weitestgehend identisch. Die telnet-Sitzung wird in der 90. Sekunde, der aggressive CBR-Datenfluß in der 100. Sekunde beendet, so daß ftp wieder die volle Bandbreite bei optimalen Verzögerungen ausnutzen kann.

4.1 Verhalten bei Assured Service

In diesem Abschnitt wird nun der Einfluß einer Assured Service Vereinbarung zwischen den Benutzern und dem ISP untersucht. Hierbei wird zunächst das für

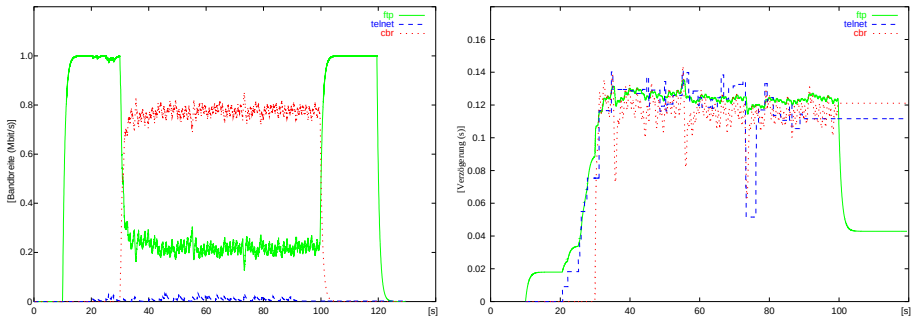

Abbildung3. Bandbreite und Verzögerung der einzelnen Flüsse bei RED und ohne Assured Service

Assured Service vorgeschlagene RIO-Queuing Verfahren herangezogen. Da sich bei den Simulationen zeigte, daß RIO-Queuing in bestimmten Fällen Nachteile bezüglich Verzögerungen verursachen kann, wurde das RIO-Queuing-System durch eine zweifache Queue (eine Queue für in-profile-Pakete, eine weitere für out-of-profile Pakete) ersetzt.

RIO Queuing mit einer Queue Das in Abb. 2 dargestellte Szenario wird nun dahingehend erweitert, daß der ftp-Verbindung und der telnet-Sitzung mit dem Assured Service Bandbreiten zugesichert werden. Als Queuing-Verfahren wird nun die RIO Variante mit einer Queue eingesetzt, die Dropping-Wahrscheinlichkeiten für die beiden verschiedenen Pakettypen ergeben sich aus Abb. 4 und hängen von dem Füllstand der Queue ab. Ist die Queue zu mehr als 40% gefüllt, werden nur noch in-profile Pakete, aber keine out-of-profile Pakete mehr weitergeleitet.

Außer der Zusicherung der Bandbreiten durch Assured Service Unterstützung wurde also das gleiche Simulationsszenario mit den gleichen Senderaten verwendet. Die ftp-Verbindung zwischen S_1 und C_1 erhält eine zugesicherte Bandbreite von 0.5 Mbit/s die Telnet-Sitzung zwischen S_2 und C_2 0.2 Mbit/s. Der aggressive Sender mit konstanter Bitrate (constant bit rate, CBR) erzeugt normalen Best-Effort, d.h. out-of-profile, Verkehr.

Abb. 5 zeigt die erreichten Bandbreiten der einzelnen Flüsse bei Assured Service für die ftp-Verbindung und die Telnet-Sitzung. Im Gegensatz zu dem Szenario ohne Assured Service dominiert nicht der CBR-Datenfluß die verfügbare Bandbreite, sondern Überläßt der ftp-Verbindung die zugesicherte Bandbreite.

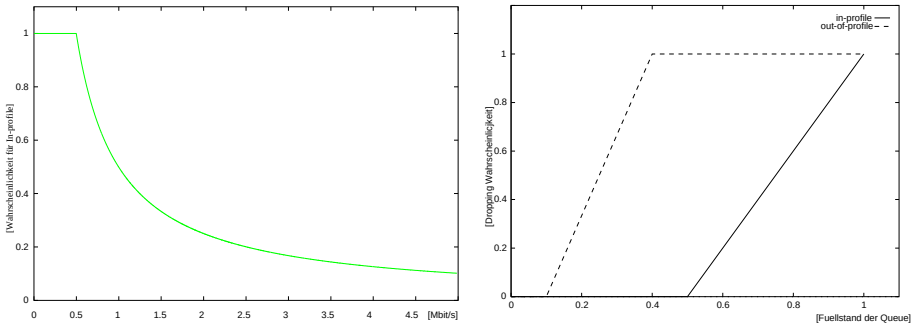

Abbildung4. links: Wahrscheinlichkeit P für in-profile-Tagging bei 500 kbit/s zugesicherter Bandbreite in Abhängigkeit der gesendeten Bandbreite; rechts: Dropping-Wahrscheinlichkeiten für in und out-of-profile Pakete

Ein Nachteil des RIO-Queuing-Verfahrens mit einer Queue besteht darin, daß bei Bursts oder Stausituationen in-profile und out-of-profile Pakete bis zu einem gewissen Füllstand der Queue gleich behandelt werden. Sofern das Netz für in-profile Verkehr ausreichend dimensioniert ist, hängt in Stausituationen die Verzügerung von in-profile Paketen davon ab, bis zu welchem Füllstand der Queue out-of-profile Pakete zugelassen werden. Je früher out-of-profile Pakete verworfen werden, desto geringer ist die maximale Verzügerung der hochprioren Pakete. Damit haben out-of-profile Pakete, die an ihr Ziel gelangen, eine mindestens ebenso gute Verzügerung wie in-profile Pakete (siehe Abb. 5). Da nach Beenden des CBR-Datenflusses und der Telnet-Sitzung nach 100 Sekunden nur noch die ftp-Quelle aktiv bleibt, sinkt die Verzügerung für diese wieder ab. Das ursprüyngliche Minimum wird nicht mehr erreicht, da die Router-Queue sich aufgrund der Dimensionierung der Links nicht wieder komplett leeren kann.

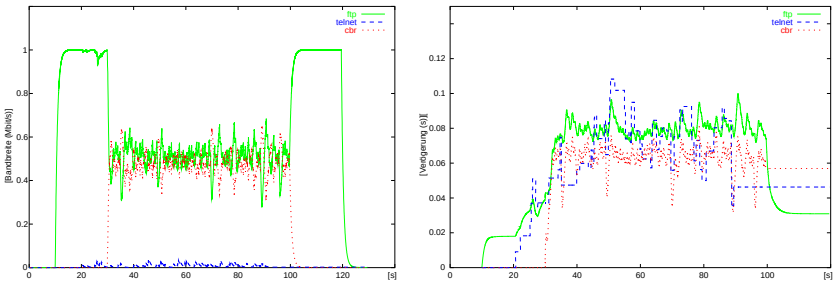

Abbildung5. Bandbreiten und Verzögerung bei RIO-Queuing und Assured Service

RIO Queuing mit zwei Queues Da es wünschenswert ist, mit dem Assured Service neben der Zusicherung von Bandbreite auch eine bestimmte maximale Verzögerung zu unterstützen, liegt es nahe für jeden Pakettyp (in-profile und out-of-profile) eine eigene Queue im Router zu implementieren, da das Verfahren mit einer Queue wie in Abschnitt 4.1 gezeigt, die gleiche Verzögerung für out-of-profile Pakete und in-profile-Pakete generiert. Der Nachteil des auf zwei Queues basierenden Verfahrens ist, daß es zu Paketvertauschungen kommen kann, wenn ein Datenfluß sowohl in-profile als auch out-of-profile Pakete enthält.
Das Simulationsszenario wurde beibehalten, lediglich das Queuing-Verfahren wurde modifiziert. Abb. 6 zeigt die erreichten Bandbreiten der einzelnen Datenflüsse. Das Verhalten bezüglich der Bandbreite entspricht dabei exakt dem des RIO-Queuing-Algorithmus mit einer Queue. In Abb. 6 sind die Verzögerungen aufgetragen. Durch die Bevorzugung der in-profile Queue erfahren die ftp-Verbindung und die telnet-Sitzung eine wesentlich bessere Verzögerung gegenüber Abb. 5) trotz des sehr aggressiven CBR-Datenflusses. Demgegenüber steigen die Verzögerungen des CBR-Datenflusses gegenüber dem RIO-Queuing-Verfahren mit einer Queue jedoch stark an.

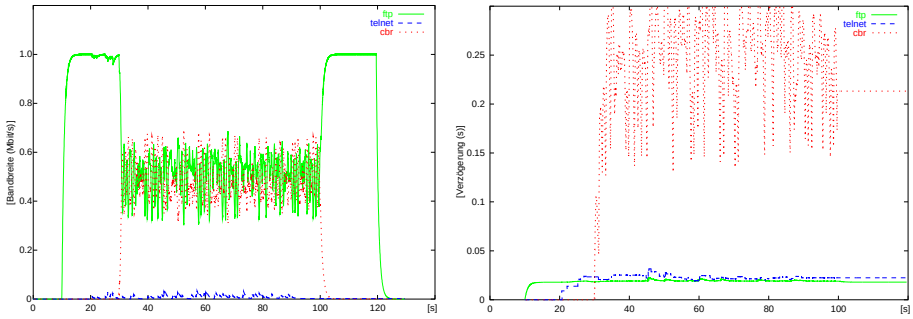

Abbildung6. Bandbreiten und Verzögerung bei RIO-Queuing mit zwei Queues und Assured Service

5 Erweiterung des RIO Verfahrens

Eine Erweiterung des RIO Verfahrens mit zwei Queues ist in Abb. 5 dargestellt. Ziel der Erweiterung ist, die beim RIO-Queuing mit zwei Queues auftretenden Reihenfolgevertauschungen zu minimieren. Bei der Erweiterung sind daher wieder zwei getrennte Queues für in-profile und out-of-profile Pakete vorgesehen.

Zusätzlich wird jedes Paket beim Eintritt in den Router mit einem Zeitstempel versehen, um später die Ankunftsreihenfolge rekonstruieren zu können. Am Ende der Queue befindet sich eine Komponente (Mixer), die - sofern in beiden Queues Pakete vorhanden sind - entscheidet, welcher Pakettyp (d.h. in-profile oder out-of-profile) übertragen werden soll. Im Gegensatz zu dem in Abschnitt 4.1 beschriebenen Verfahren, wird nun dem Router explizit eine maximal erlaubte Verzögerung für in-profile-Pakete vorgegeben. Der Mixer nutzt diese erlaubte Verzögerung aus, um zwischen den einzelnen in-profile Paketen möglichst viele out-of-profile Pakete zu übertragen. Indem der Mixer out-of-profile Pakete, die er nicht reihenfolgegetreu zwischen in-profile-Paketen übertragen kann löscht, ließen sich alle Paketvertauschungen verhindern. Dieser Ansatz wird allerdings hier nicht weiter verfolgt. Alternativ (siehe Abb. 5 wird versucht, die Paketreihenfolge soweit möglich beizubehalten. Abb. 8 zeigt die Anzahl der Paketvertauschungen bei den verschiedenen Queuing-Verfahren mit zwei Queues in Abhängigkeit der Bandbreiten, mit denen der aggressive CBR-Sender sendet. Abb. 8 zeigt die dabei auftretenden Verzögerungen. Dabei wird deutlich, daß bei ftp Paketlaufzeiten auftreten, sie sich im Bereich der vorgeschrieben maximalen Verzögerung bewegen.

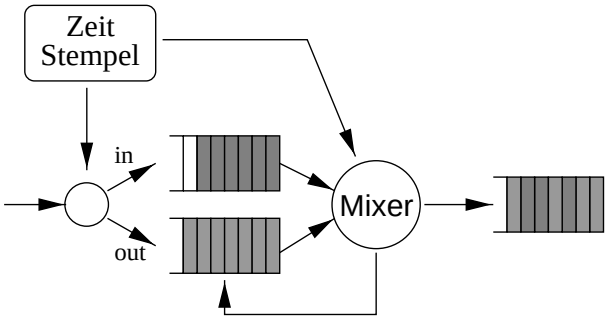

Abbildung7. verbessertes RIO Queuing mit Reihenfolgewiederherstellung

Ein interessantes Ergebnis konnte des weiteren bei der Betrachtung der tatsächlich erreichten Bandbreiten feststellen. So erreicht ftp im gleichen Szenario durch das verbesserte Qeuing-Verfahren eine deutlich höhere, gleichmäßigere Datenrate von ca. 600kbit/s als in Abb. 6. Dies läßt sich dadurch erklären, daß nur ein Teil der ftp Pakete als in-profile übertragen werden und bei dem hier

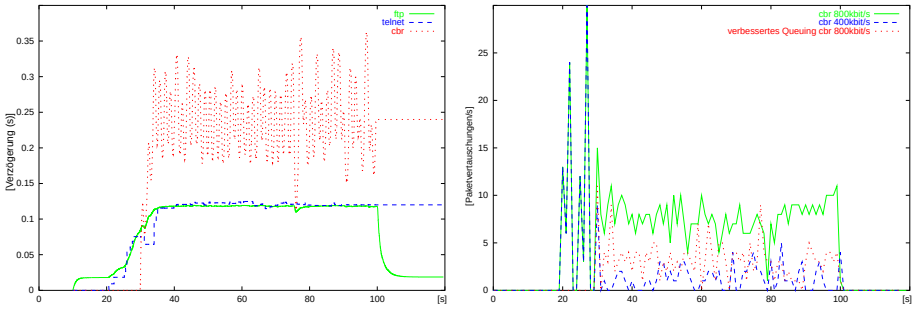

Abbildung8. Verzögerungen der einzelnen Datenflüsse bei einer maximalen Verzögerung von 100 ms für in-profile Traffic im RIO Queue und Anzahl der Paketvertauschungen auf der ftp Verbindung bei unterschiedlichen Senderaten der cbr Quelle

dargestellen Verfahren der ursprüngliche TCP-Datenstrom weniger gestört wird, als bei den anderen RIO Varianten.

6 Zusammenfassung

Die in diesem Beitrag vorgestellten Simulationsergebnisse zeigen, daß der Assured Service einen vielversprechenden Ansatz darstellt, um Dienstgüten in großen IP-Netzen zu unterstützen. Darüber hinaus ist Assured Service durchaus in der Lage, TCP-konforme Datenflüsse auch gegenüber nicht-TCP-konformen Datenflüssen zu schützen. Entscheidend für die Wahrscheinlichkeit, daß mit Hilfe des Assured Service die gewünschte Bandbreite einem Benutzer zur Verfügung gestellt werden kann, ist jedoch eine gute Dimensionierung des Netzes durch den ISP. Hierzu sind sicherlich noch geeignete Methoden und Verfahren zu entwickeln.

Neben der simulativen Bewertung des Assured Service Konzepts schlägt der Beitrag auch diverse Verbesserungen für Queuing-Mechanismen vor, um für Datenflüsse, die durch den Assured Service unterstützt werden, nicht nur höhere Bandbreitenwerte aber auch bessere verzögerungseigenschaften zu erzielen. Hierzu wurde ein Algorithmus vorgestellt, welcher in der Lage ist nicht nur Verzögerungen zu begrenzen, sondern auch Reihenfolgevertauschungen möglichst gering zu halten. Zukünftige Arbeiten werden den Assured Service und die in diesem Zusammenhang vorgeschlagenen Modifikationen der Queuing-Verfahren auch für HTTP-Verkehr bewerten.

Literatur

[BBC+98] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weis. An architecture for differentiated services. Internet Draft `draft-ietf-diffserv-arch-02.txt`, October 1998. work in progress.

[BCC+97] B. Braden, D. Clark, J. Crowcroft, B. Davie, S. Deering, D. Estrin, S. Floyd, V. Jacobson, G. Minshall, C. Partridge, L. Peterson, L. Ramakrishnan, S. Shenker, J. Wroclawski, and L. Zhang. Recommendations on queue management and congestion avoidance in the internet. Internet Draft `draft-irtf-e2e-queue-mgt-00.txt`, March 1997. work in progress.

[BZB+97] B. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin. Resource reservation protocol (rsvp) -version 1 functional specification. Request for Comments 2205, September 1997.

[CW97] D. Clark and J. Wroclawski. An approach to service allocation in the internet, work in progress. Internet Draft `draft-clark-diff-svc-alloc-00.txt`, Juli 1997. work in progress.

[FJ95] Sally Floyd and Van Jacobson. Link-sharing and resource management models for packet networks. *IEEE/ACM Transactions on Networking*, 3(4), August 1995.

[IN98] J. Ibanez and K. Nichols. Preliminary simulation evaluation of assured service. Internet Draft `draft-ibanez-diffserv-assured-evald-00.txt`, August 1998. work in progress.

[Kes91] S. Keshav. *Congestion Control in Computer Networks*. PhD thesis, Berkeley, September 1991.

[MBB+97] A. Mankin, F. Baker, B. Braden, S. Bradner, M. O'Dell, A. Romanow, A. Weinrib, and L. Zhang. Resource reservation protocol (rsvp) version 1 applicability statement. Request for Comments 2208, September 1997.

[NBBB98] K. Nichols, S. Blake, F. Baker, and D. Black. Definition of the differentiated services field (ds field) in the ipv4 and ipv6 headers. Internet Draft `draft-ietf-diffserv-header-04.txt`, October 1998. work in progress.

[NJZ97] K. Nichols, Van Jacobson, and L. Zhang. A two-bit differentiated services architecture for the internet. Internet Draft `draft-nichols-diff-svc-arch-00.txt`, November 1997. work in progress.

[ns] Ucb/lbnl/vint network simulator - ns (version 2). URL: http://www-mash.CS.Berkeley.EDU/ns/.