

# **Ein durch QoS erweitertes Internet**

## **Vortrag Nummer 12**

**Vorlesung: Protokolle für Multimedia Kommunikation**

## 1. Einführung

Mit dem Wachstum des Internets und der Intranets und dem Wunsch nach Verteilten Multimedia Anwendungen steigt der Bedarf nach einer Möglichkeit die Qualität der verwendeten Netzwerkdienste zu bestimmen. Sowohl Telekommunikationsfirmen wie auch alle Content Provider, wie Fernseh- und Radiosender, wünschen sich eine Möglichkeit, im Voraus ihre Anforderungen an das Netzwerk, beziehungsweise an die Datenverbindung zum Kunden, zu stellen und auch zu erfahren, ob diese Anforderungen erfüllt werden können um dem Kunden eine in der Qualität gesicherte Dienstleistung anbieten zu können. Wer möchte schon für ein Fernsehprogramm bezahlen, das genau im spannendsten Moment wegen eines Filetransfers irgendeines anderen Netzwerkbenutzers unterbrochen wird?

Das heutige Internet bieten leider keine Möglichkeiten Qualität und Leistung der Übertragungen zu bestimmen. Die simplen Ansätze wie ein Type-of-Service Feld im IPv4 Header erfüllen die Wünsche nach Kontrolle und Garantie der Netzwerkqualität keineswegs und werden auch nicht überall unterstützt.

Es wurden im Laufe der Zeit mehrere verschiedene Ansätze zur Lösung dieser Problematik erarbeitet. Einige dieser Ansätze wie IP Version 6, Integrated Services Architecture (IntServ), Differentiated Services Architecture (DiffServ), Resource Reservation Protokoll (RSVP) und Multiprotocol Label Switching (MPLS) möchte ich in diesem Text kurz erklären und ihre Vor- und Nachteile etwas beleuchten.

Alle diese Protokolle sind noch in der Entwicklung und sind somit nicht als endgültige Lösungen anzusehen. Auch fehlen zur Zeit die "Kritischen Applikationen" für die breite Masse, die dann mit Hilfe dieser Protokolle eventuell bessere Leistungen erbringen können.

## 2. Integrated Services Architekture - IntServ

### 2.1 Ein Überblick

IntServ führt drei Service Klassen ein. Dies sind die Guaranteed-Service Class, die Verzögerungsgarantien ermöglicht, die Controlled-Load-Service Class, die Verzögerungsgarantien für die statistischen Mittelwerte dieser Parameter ermöglicht und somit nicht oft die gewünschten Verzögerungen verletzt, und die altbekannte Best-Effort Service Class, die weiter aufgeteilt wird in drei Unterkategorien: Interaktive Burst (Web), Interactive Bulk (FTP) und Asynchronous (EMail).

Die garantierte wie auch die kontrollierte Service Klasse verlangen eine Möglichkeit der Signalisierung wie auch der Zugangskontrolle. Diese Signalisierung wie auch die Zugangskontrolle muss für jeden einzelnen Datenstrom möglich sein. Obwohl die IntServ Architektur nicht an ein spezielles Signalisierungsprotokoll gebunden ist wird doch RSVP als *das* Signalisierungsprotokoll von IntServ betrachtet.

### 2.2 Vorteile von IntServ

Der grosse Vorteil der IntServ Architektur besteht darin dass durch die drei Service Klassen genau diejenigen Wünsche erfüllt werden können, die für die Multimedia Anwendungen benötigt werden. Die garantierte Service Klasse entspricht beispielsweise genau dem was man sich für kritische, fehlerintolerante Applikationen wünscht. Ein weiterer Vorteil ist, dass die Best-Effort Class genau dem entspricht was zur Zeit im Internet vorhanden ist und somit all jene nicht kritischen Applikationen die heute problemlos funktionieren in diese Klasse fallen und somit auch unterstützt werden.

### 2.3 Nachteile von IntServ

Ende-zu-Ende Garantien können natürlich nur dann unterstützt werden wenn alle Knoten entlang des Kommunikationspfades die IntServ Architektur unterstützen.

Da pro Datenstrom Garantien abgegeben werden ergeben sich massive Skalierungsprobleme im Kern des Internets. Es sind einfach zu viele Datenströme vorhanden und man wird auf die selben Probleme stossen wie es auch bei den Routern und ihren Routingtabellen geschehen ist bevor man das Klassenlose

Interdomainrouting (CIDR) eingeführt hat (das dann die Grösse der Tabellen verkleinern konnte). Eine Lösung zu diesem Problem könnte analog zu dem Routingtabellenproblem gefunden werden indem man nicht pro Datenstrom sondern pro Datenstromklasse Garantien vergibt. Dies ist auch genau der Lösungsansatz, den DiffServ verfolgt wie weiter unten gezeigt wird.

### **3. Differentiated Services - DiffServ**

#### **3.1 Ein Überblick**

Wie man bei der IntServ Architektur gesehen hat, wird das Vergeben von Garantien pro Datenstrom vermutlich massive Skalierungsprobleme aufwerfen und benötigt auch ein Signalisierungsprotokoll entlang des ganzen Datenflusspfades. Wenn man allerdings die Datenströme in Datenstromklassen klassifiziert und nur Garantien für die ganze Klasse vergibt, so ergibt sich daraus eine einfachere und skalierbarere Architektur.

Diese Skalierbarkeit wird dadurch erreicht, dass nur Garantien für den Grenzverkehr zwischen den Domains vertraglich festgelegt werden. Das Ressourcenmanagement innerhalb einer Domain untersteht der alleinigen Verantwortung des entsprechenden Service Providers, der natürlich auch innerhalb der Domain für genügend Kapazitäten sorgen muss, so dass die Grenzverträge eingehalten werden können.

Jedes Paket das eine DiffServ Domain erreicht wird an der Grenze zur Domain klassifiziert und im Header im sogenannten DS Code Point (DSCP) als zu einer bestimmten Klasse gehörig markiert. Innerhalb der Domain wird das Forwarding-Verhalten alleine durch diese Markierung bestimmt und es ist dem Service Provider überlassen entsprechende Ressourcen zur Verfügung zu stellen um seine Grenzverträge zu erfüllen.

#### **3.2 Vorteile von DiffServ**

Die DiffServ Architektur ist ein eleganter Weg die pro Datenstrom vorhandenen Statusinformationen so zu minimieren, dass das bei IntServ auftretende Skalierungsproblem umgangen wird. Sie ermöglicht es den Service Provider unterschiedliche Preise für unterschiedliche Qualitäten von Diensten zu verrechnen.

Die Klassen in der DiffServ Architektur sind ohne Signalisierungsprotokoll implementierbar was wieder zu einer beträchtlichen vereinfachung der Architek-

tur führt. Das Aggregieren von Datenströmen zu Klassen ermöglicht es relative Services für Applikationen anzubieten, also sind damit Aussagen der folgenden Form möglich: Service A wird mit einer kleineren Verzögerung als Service B bedient. Weiter ist das Bereitstellen der entsprechenden Ressourcen innerhalb der Domain der alleinige Verantwortungsbereich des Service Providers dieser Domain und kann somit mit den altbekannten Hilfsmitteln statisch erfolgen. Lediglich die Paketklassifizierung an der Grenze der Domain und das Auswerten des DSCP Feldes innerhalb der Domain ist neu (was ja fast einem Label Switching entspricht wie man weiter unten sehen wird). Dies reduziert die Arbeitslast auf den internen Routern der Domain nochmals drastisch.

### **3.3 Nachteile von DiffServ**

Gleichzeitig verschiedene Services mit verschiedenen Qualitätsansprüchen über das selbe Netzwerk zu bedienen ist eine komplizierte Aufgabe. Die DiffServ Architektur macht diese Aufgabe nicht einfacher. Im Gegenteil - In der DiffServ Architektur wurde entschieden viele der Problematiken einfach in die Netzwerkbereitstellung und Netzwerkverfügbarkeit zu verschieben. Natürlich sind dies Aufgabenstellungen die schon heute gelöst werden und sie sind deshalb dem Service Provider nicht neu. Allerdings ist das Bereitstellen von Netzwerkkapazitäten für ein Netzwerk das mit verschiedenen Qualitätsklassen operiert etwas Neues und ist auch ein noch nicht sehr erforschtes Gebiet. Ohne massiven Ressourcenüberschuss innerhalb der Domain kann durch Engpässe innerhalb der Domain das Erfüllen der Grenzverträge gefährdet werden.

Das Bereitstellen von Ende-zu-Ende Diensten durch Zusammenfügen von lokalen Verträgen ist ein nichtriviales Forschungsgebiet auf dem noch viel Arbeit geleistet werden muss, insbesondere falls dies auf eine automatische Art mit Hilfe von Protokollen geschehen soll.

#### **4. Das neue Internet Protokoll - IPv6**

IPv6 wurde als Nachfolger von IPv4 konzipiert und ermöglicht es Datenströme mit Labels ähnlich dem DSCP Feld in IPv4 zu versehen und das ohne dass Felder von verschiedenen Protokoll Headern zusammengefügt werden müssen. Dies ermöglicht eine feiner granulierten Datenstrom Identifikation und erleichtert auch das Behandeln von Datenströmen wo Sicherheitsbelange tangiert werden, wie etwas bei der Verschlüsselung von Datenpaketinhalten (wo auch die Portnummern mitverschlüsselt werden und somit das Paketklassifizieren verunmöglicht wird). IPv6 beinhaltet natürlich noch mehr Änderungen, die aber im Zusammenhang mit QoS nicht von besonderer Bedeutung sind.

#### **5. Das Ressourcen Reservations Protokoll - RSVP**

RSVP basiert auf dem Konzept von "Sessionen". Eine Session besteht aus mindestens einen Datenstrom und ist definiert in Bezug auf eine "Zieladresse", genauer gesagt Zieladresse, Zielport und Protokollidentifikation. Das Ziel kann eine Multicastadresse sein, wodurch auch Gruppen von Zielen enthalten sind.

In RSVP ist ein Datenstrom definiert als ein Teil der Pakete einer Session. Ein Datenstrom fließt also nur in eine Richtung und kommt auch nur von einem Sender.

Path Nachrichten werden in periodischen Abständen in Richtung des Empfängers geschickt und etablieren einen Pfad Zustand entlang allen Routern des Weges. Resv Nachrichten werden periodisch in Richtung des Senders geschickt und etablieren die Reservation der Ressourcen entlang des Weges. Um den Overhead zu reduzieren werden Path und Resv Nachrichten die den Zustand eines Routers ändern nicht sofort weitergesandt, sondern jeder Router versendet periodisch seine eigenen Path und Resv Nachrichten betreffend der Datenstrominformationen die er hat. Jede Resource hat eine Lebenszeit, die durch die nächste Path oder Resv Nachricht wieder erhöht wird. Läuft die Lebenszeit ab, wird die Resource wieder freigegeben.

Um die Antwortzeiten zu erhöhen wurde ein Mechanismus namens "Lokale Reparatur" implementiert. Er besteht daraus dass jeder Router der eine Routingänderung sieht sofort eine Path Nachricht entlang des neuen Weges schickt und der Empfänger dieser Nachricht auch sofort mit einer Recv Nachricht zur Ressourcenallokation antwortet.

Natürlich gibt es auch Nachrichten um die Reservationen gewollt und unmittelbar wieder freizugeben (Teardown Nachrichten). Man muss beachten, dass alle diese Nachrichten in unbestätigter Form versendet werden.

RSVP ermöglicht mehrere Arten von Reservationen. Die Reservationen werden durch Filter Typen spezifiziert von denen es drei Arten gibt:

- Wild-card Filter: Jeder Datenstrom einer Session teilt die zugeordnete Resource mit den Anderen.
- Shared-explicit Filter: Explizite definierte Datenströme teilen sich die selbe Resource.
- Fixed Filter: Garantiert dass ein Datenstrom das exklusive Nutzungsrecht der Resource bekommt.

## **6. Multiprotokoll Label Switching - MPLS**

Um die Effizienz von Paket-Forwarding zu erhöhen wurde nach neuen Wegen gesucht, da die aktuelle Bus-Architektur von Routern nur bis zur 1 Gb/s Grenze skaliert.

Ein MPLS Paket hat einen Header, der entweder zwischen Link-Layer und Netzwerk-Layer eingefügt oder innerhalb eines schon existierenden Headers eingebaut ist (wie zum Beispiel der Virtuelle Pfad/Kanal Identifyer (VPI/VCI) in ATM). Dieser Header enthält ein Label Feld, ein Time to Live Feld, ein Service Klasse Feld (Class of Service - CoS), ein Stack Indicator, ein Next Header Type und eine Checksumme.

MPLS definiert eine fundamentale Unterscheidung zwischen der Gruppierung der in der selben Art weiterzuleitenden Pakete (FEC - Forwarding Equivalence Class) und den eigentlichen Labels die die Pakete markieren. Dies geschieht um die Flexibilität zu erhöhen. Bei jedem Knoten können alle Pakete mit der selben FEC auf das selbe lokale Label gemappt werden. Es kann aber auch sein, dass es aus anderen Gründen gewünscht ist, verschiedene Labels zu benutzen, um beispielsweise verschiedene Qualitäten von Datenströmen zu unterscheiden.

Die Klassifizierung eines Paketes zu einer FEC geschieht einmal beim Eintreten in das Netzwerk. MPLS fähige Router (Label-Switched Routers LSRs) benutzen danach nur noch das FEC und das CoS Feld um die Forwarding- und Klassifizierungsentscheidung zu treffen. MPLS Pakete können mehrere Labels besitzen die in Stack Form behandelt werden (LIFO). Nur jeweils das oberste Label wird betrachtet. Dadurch ist es sehr einfach möglich, Paket-Tunnels aufzubauen.

Mehrere MPLS fähige Router spielen zusammen, um einen Pfad zu definieren (Label-Switched Path - LSP). Es gibt zwei Arten diesen Pfad zu bestimmen. Entweder jeder Router bestimmt selbständig den nächsten Hop (Hop-by-Hop Routing), oder der Pfad wird explizit (meist durch den Ingress Router, also den Eingangsrouten zum Netzwerk) bestimmt.

MPLS braucht einen Mechanismus um die Labels zu verteilen und damit einen Pfad aufzusetzen. Die Architektur besteht nicht auf ein bestimmtes Protokoll sondern definiert eine Gruppe von Protokollen mit verschiedenen Eigenschaften (Label Distribution Protokoll - LDP) sowohl in IP (unbestätigt) als auch in TCP (bestätigt). Auch RSVP kann als LDP, verwendet werden um die Label Zuweisung zu triggern.

Betreffend QoS ermöglicht MPLS, durch das CoS Feld, verschiedene Service Klassen zu unterscheiden und ihnen dadurch auch verschiedene Labels zuzuweisen. Natürlich kann die Label Zuweisung sogar auf einer Benutzerbasis geschehen.

MPLS und Multilayerrouting ermöglichen eine generelle, sehr effiziente Paket-forwarding Technik die für High-Speed Datentransfers sehr gut geeignet ist. MPLS wird inzwischen auch in Hardware supportet und ermöglicht so Geschwindigkeiten jenseits von 1Gb Routern.

## **7. Schlussfolgerungen**

Wie wir gesehen haben gibt es einige neue vielversprechende Ansätze die früher oder später im Internet implementiert werden könnten. Vorallem hinsichtlich Ende-zu-Ende Qualitätssicherung wird viel davon abhängen in welchem Masse diese Lösungen flächendeckend im Internet implementiert werden.

Von allen Vorschlägen die wir diskutiert haben scheint in meinen Augen die DiffServ Architektur die erfolgversprechendste zu sein, da sie einfach zu implementieren und auch ohne massives Umdenken schnell zu begreifen ist. Sie ermöglicht allerdings nur eine relative Unterscheidung von Qualitätsklassen und das Verhalten von aggregierten Datenströmen ist noch nicht sehr gut erforscht.

Leider stellt DiffServ zur Zeit nur einen Rahmen dar, der von den einzelnen Service Providern mit Leben gefüllt werden muss.



## 8. Anhang - Literaturangaben

- [1] Y. Bernett: The Complementary Roles of RSVP and Differentiated Services in the Full-service QoS Network; IEEE Communications Magazine, Vol 38, No. 2, February 2000, pp 154-161
  
- [2] L. Mathy, C. Edwards, D. Hutchison: The Internet: A Global Telecommunications Solution? IEE Network, Vol. 14, No. 4, July/August 2000, pp 46-57
  
- [3] Prof. Dr. Burkhard Stiller: Protokolle für Multimediakommunikation; WS 2000/2001, Eidgenössische Technische Hochschule Zürich, Departement für Elektrotechnik und Departement für Informatik