Diplomarbeit

Ressourcenreservierung für Mobile Systeme

von

cand. inform. Jörg Diederich

Technische Universität Braunschweig
Institut für Betriebssysteme und Rechnerverbund

Aufgabenstellung und Betreuung

Prof. Dr. M. Zitterbart
Dipl.-Inform. A. Fieger

Braunschweig
31. Juli 1998

Erklärung

Ich versichere, die vorliegende Arbeit selbständig und nur unter Benutzung der angegebenen Hilfsmittel angefertigt zu haben.

Braunschweig, den 31. Juli 1998 Unterschrift

Kurzfassung

Mobile IP bietet Systemen im Internet, die über ein drahtloses Netz angeschlossen sind, die Möglichkeit zu Mobilität im Weitverkehrsbereich. Mit RSVP (Resource ReSerVation Protocol) können Ressourcen im Internet reserviert werden, um zeitkritische Datenströme mit Dienstgüte versehen zu können. Diese Arbeit analysiert das Zusammenwirken beider Ansätze, um auch mobilen Teilnehmern im Internet den Empfang von mit Dienstgüte behafteten Datenströmen zu ermöglichen. Dabei findet zusätzlich eine Betrachtung des indirekten Transportansatzes statt. Dieser teilt eine Transportverbindung zwischen einem mobilen und einem stationären System in zwei separate Verbindungen für die drahtgebundene bzw. die drahtlose Strecke, um den Durchsatz einer solchen Transportverbindung zu erhöhen.

Die Betrachtung von Mobile IP unter dem Aspekt der Dienstgüte ergibt, daß ein mobiles System im Falle eines Ortswechsels eine längere Unterbrechung der Verbindung zum Internet erfährt, sofern es sich nicht in der Nähe seines Heimatnetzwerkes befindet. Diese Arbeit schlägt ein Protokoll als Erweiterung für Mobile IP vor, durch welches die Unterbrechungszeit deutlich verringert wird: das sog. Fast-Forwarding Protokoll.

Abstract

Mobile IP supports wide area mobility for mobile systems in the Internet. RSVP (Resource ReSerVation Protocol) reserves resources in the network so that the transmission of data with a certain quality of service (QoS) within the Internet becomes possible. This work analyses how both approaches work together to support the transmission of data with a certain QoS to mobile systems. Additionally, the analysis considers the indirect transport model which splits a connection between a mobile system and a fixed system into two separate subconnections: One for the wired link and another one for the wireless link. In this way, this approach improves the throughput between both systems.

When taking QoS into account, the analysis of Mobile IP shows that a mobile system looses its connection to the Internet for quite a long time, when it moves to another place, as long as it is not nearby its home network. This work proposes a protocol as an enhancement to Mobile IP to reduce this time of interruption: the so-called Fast-Forwarding Protocol.

Aufgabenstellung

Die Entwicklung neuartiger, funkbasierter Übertragungstechnologien ermöglicht die Anbindung mobiler Teilnehmer an das Internet. Allerdings unterstützen die derzeit am Markt verfügbaren Systeme lediglich Mobilität im lokalen Bereich, Mobilitätsunterstützung im Weitverkehrsbereich kann durch den Mobile IP Lösungsansatz gewährleistet werden. Sollen neben traditionellen Diensten auch Datendienste mit zeitkritischen Datenströmen unterstützt werden, so sind zusätzlich Protokolle zur Ressourcenreservierung — beispielsweise RSVP — notwendig.

Bedingt durch sich ändernde Routen zum Mobilteilnehmer müssen auch Reservierungen auf Teilstrecken gelöscht bzw. neu etabliert werden. Unmittelbar nach einem durch Mobile IP veranlaßten Routenwechsel sollten auch die entsprechenden Reservierungen angepaßt werden.

Im Rahmen dieser Diplomarbeit soll untersucht werden, inwieweit Änderungen an RSVP notwendig sind, um dieses Protokoll sinnvoll auch über drahtlose Teilstrecken einsetzen zu können. Die Interaktion von Mobile IP und RSVP ist genauer zu beleuchten. Beispielsweise sind hierbei Wechselwirkungen bedingt durch fehlende Abstimmung der Timer in RSVP bzw. Mobile IP zu analysieren. Darüberhinaus sind Betrachtungen anzustellen, inwieweit es sinnvoll und machbar ist, Teile der RSVP-Funktionalität auf den Previous-Hop RSVP-Router zu verlagern, um den Kommunikationsoverhead über den drahtlosen Link zu reduzieren. Dabei ist zu berücksichtigen, daß der Previous-Hop RSVP-Router unter Umständen als Transportgateway für indirekte Transportverbindungen fungiert und somit zusätzlich QoS-Aspekte beachtet werden müssen.

Soweit es die existierenden Implementierungen von Mobile IP und RSVP zulassen, sind Teile der erarbeiteten Lösungen zur Behebung der identifizierten Probleme in diese Implementierungen zu integrieren.

Die Hinweise zur schriftlichen Ausarbeitung von Studien- und Diplomarbeiten sind zu beachten.

Laufzeit: 6 Monate

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einleitung

Diese Diplomarbeit betrachtet die Kombination von Mobilität und einer Reservierung von Ressourcen am speziellen Beispiel von Mobile IP für die Mobilität und RSVP (Resource ReSerVation Protocol) für die Reservierung von Ressourcen.

Motivation

Die Verbreitung mobiler Systeme steigt in großem Maße, seitdem die Leistungsfähigkeit dieser ehemals leistungsschwachen, portablen Computer stark gestiegen ist und sie den stationären Personal Computern in nichts nachstehen. Mit Hilfe von Mobile IP können diese mobilen Systeme an ein beliebiges Netzwerk im Internet angeschlossen werden und sind für alle Systeme aus dem Internet zu erreichen. Außerdem unterstützt Mobile IP auch die Mobilität des mobilen Systems während einer laufenden Datenübertragung.

Desweiteren finden Multimedia-Anwendungen eine zunehmende Verbreitung, die besondere Anforderungen an die Dienstgüte einer Datenübertragung stellen. Sie benötigen z. B. geringe Verzögerungen für Audiodaten oder hohe Bandbreiten im Falle einer Videokonferenz. Um diese Anforderungen zu erfüllen, müssen Ressourcen im Netzwerk reserviert werden. RSVP (Resource ReSerVation Protocol) ist ein Protokoll, welches die für die Reservierung notwendigen Informationen im Netzwerk propagiert.

Durch neue Technologien bei der funkbasierten Datenübertragung kann auch ein System, welches an einem drahtlosen Netzwerk angeschlossen ist, die genannten Multimedia-Anwendungen benutzen.

Die Kombination von Mobile IP und RSVP soll es dem mobilen System zusätzlich ermöglichen, Multimedia-Anwendungen zu benutzen und währenddessen den Anschlußpunkt an das Internet in Folge von Mobilität zu wechseln.

Probleme bei der Verwendung von TCP (Transmission Control Protocol) für eine zuverlässige Datenübertragung zwischen einem stationären und einem mobilen System können mit dem indirekten Transportansatz behoben werden. Dabei wird eine Transportverbindung zwischen einem stationären und einem mobilen System in eine Verbindung über die drahtgebundene Strecke und eine weitere über die drahtlose Strecke aufgeteilt.

Aufgabe dieser Diplomarbeit

Diese Diplomarbeit betrachtet die Kombination von Mobile IP und RSVP unter Berücksichtigung des indirekten Transportansatzes. Dabei entstehen Probleme, weil RSVP und Mobile IP jeweils unabhängig voneinander entwickelt wurden. Diese Probleme werden analysiert und Lösungen bzw. Lösungsansätze vorgestellt, welche dann zusätzlich auf die Integrierbarkeit des indirekten Transportansatzes überprüft werden.

Desweiteren stellt diese Arbeit unabhängig von RSVP eine Betrachtung von Mobile IP unter dem Aspekt der Dienstgüte an, z. B. eine Analyse der Dauer einer Unterbrechung im Falle eines Ortswechsels des mobilen Systems. Außerdem wird eine allgemeine Analyse von RSVP unter dem Gesichtspunkt der Mobilität unternommen, z. B. im Bezug auf die Wiederherstellung einer Reservierung nach einem Ortswechsel des mobilen Systems.

Kernaussage

Das Ergebnis dieser Diplomarbeit ist, daß sich Mobile IP und RSVP unter Berücksichtigung des indirekten Transportansatzes mit vernünftigem Aufwand kombinieren lassen. Dennoch sind einige Modifikationen an Mobile IP und wenige an RSVP nötig, um die Zusammenarbeit zwischen beiden Protokollen zu optimieren.

Begrenzung

Diese Arbeit geht nicht auf die in der Literatur häufig behandelte Problematik ein, daß nach einem Funkzellenwechsel eines mobilen Teilnehmers nicht genügend Ressourcen in der neuen Funkzelle verfügbar sind. Das Problem der suboptimalen Wege in Mobile IP und einer damit verbundenen Ressourcenverschwendung wird ebenfalls nicht ausführlich betrachtet.

1.1 Verwandte Arbeiten

Die Literatur zum Thema Mobilität mit Mobile IP und Dienstgüte mit RSVP läßt sich in vier Teilbereiche gliedern:

1. Vorschläge zur Kombination von Mobile IP und RSVP.
2. Verbesserungen von Mobile IP, um dieses an die Übertragung von mit Dienstgüte behafteten Daten anzupassen (keine spezielle Betrachtung von RSVP).
3. Verbesserungen an RSVP, damit es auch für mobile Teilnehmer nutzbar ist (keine spezielle Betrachtung von Mobile IP).
4. Allgemeine Literatur zur Kombination von Mobilität und Dienstgüte.

Die Literatur aus dem ersten Teilbereich steht inhaltlich dieser Arbeit sehr nahe, sie gibt ebenso einen Überblick über die allgemeine Problematik der Kombination von Mobile IP und RSVP.

Mobile IP und RSVP

Andreoli et al. [AndBlé96] schlagen vor, den Sender eines Datenstroms, der eine bestimmte Dienstgüte mittels RSVP erhalten soll, zu Beginn der Datenübertragung über den aktuellen Aufenthaltsort des mobilen Teilnehmers zu informieren. Dadurch kann der Sender die direkte Strecke zum aktuellen Aufenthaltsort des mobilen Empfängers reservieren. Der Wechsel eines Subnetzes während der Datenübertragung ist nicht vorgesehen.

Rajagopalan [Raj96] gibt fünf Aussagen über die Kombination von Mobile IP und RSVP: Erstens kann ein mobiler Teilnehmer von RSVP keine harten Dienstgütegarantien bekommen, weil diese aufgrund der Schwankungen in der Charakteristik eines Funkkanals (z. B. schwankende Fehlerraten) nicht zu garantieren sind. Zweitens sollte es für den Sender und den Empfänger möglich sein, die Charakteristik der Übertragungsstrecke zu erfahren, um die Datenübertragung vom Sender und die dazugehörige Reservierung daran anpassen zu können. Drittens müssen die Unterbrechungszeiten und die Datenverluste bei der Bewegung eines mobilen Systems minimiert werden. Viertens soll die Strecke vom Sender zum Empfänger möglichst kurz sein, um nicht unnötig Ressourcen zu reservieren. Und schließlich fünftens muß eine Gruppenkommunikation mit RSVP an die Mobilität einzelner Gruppenmitglieder angepaßt werden.

Jain et al. [JaiRal98] verwenden anstelle von Mobile IP ein alternatives Protokoll namens *Mobile IP mit Location Registers*. Vor dem Senden einer Nachricht zu einem mobilen Teilnehmer muß der Sender eine Anfrage an das Location Register über den aktuellen Aufenthaltsort des mobilen Systems stellen. Dieses vermeidet in Mobile IP auftretende ungünstige Routen vom Sender zum mobilen Empfänger und reduziert außerdem den von Mobile IP erzeugten Overhead. Diese Vorgehensweise ist aber nur für begrenzte lokale Netze vorgesehen, nicht für eine Internet-weite Mobilität.

Anpassungen von Mobile IP an Dienstgüte

Woo und Leung [WooLeu96] reduzieren die Paketverluste, wenn ein Mobilteilnehmer das Subnetz wechselt, indem sie Mobile IP um einen Mechanismus zum Puffern der Daten bei einem Subnetzwechsel erweitern. Sie erreichen damit eine Erhöhung des Datendurchsatzes einer TCP-Verbindung zum mobilen Empfänger.

Cáceres und Padmanabhan [CácPad96] schlagen ein hierarchisches Management der Mobilität im Internet vor, um die Unterbrechungszeiten beim Subnetzwechsel eines mobilen Systems gering zu halten. Damit bleiben lokale Ortswechsel bis zu einem gewissen Grad transparent für andere in das Weiterleiten der Daten involvierte Systeme, die sehr weit vom aktuellen Aufenthaltsort des mobilen Systems entfernt sind. Eine Besonderheit ist dabei, daß jede Funkzelle ein eigenes Subnetz darstellt und sich damit sehr viele Subnetzwechsel ergeben.

Anpassungen von RSVP an Mobilität

Talukdar et al. [TalBad98] beschreiben eine Netzwerkarchitektur, die auch mobilen Systemen Dienstgüte durch eine Vorreservierung von Ressourcen garantieren kann, die unabhängig von der Mobilität des System ist. Dazu muß allerdings das Bewegungsmuster des mobilen Teilnehmers im voraus bekannt sein. Um eine solche mobilitätsunabhängige Dienstgüte zu realisieren, reserviert diese Netzwerkarchitektur Ressourcen auf allen Strecken vom Sender zu den Funkzellen, in die sich das mobile System bewegen wird. Dabei unterscheidet man zwischen einer *aktiven Reservierung* auf der Strecke zu der Funkzelle, in der sich das mobile System gerade befindet, und *passiven Reservierungen* auf den Strecken zu den Funkzellen, in die sich das mobile System noch bewegen wird. Für eine effiziente Ausnutzung der Ressourcen können passive Reservierungen von anderen System verwendet werden, solange das reservierende mobile System diese nicht in Anspruch nimmt. Die Signalisierung der für die aktiven und passiven Reservierungen benötigten Daten übernimmt MRSVP [TalBad98a], ein modifiziertes RSVP.

Allgemeine Literatur zum Thema Mobilität und Dienstgüte

Singh [Sin96] stellt fest, daß der Einfluß der Mobilität eines Systems auf die Dienstgüte der zu empfangenden Daten unvermeidlich ist. Da die Mobilität eines Systems nicht vorhersagbar ist, kann das Netzwerk die Dienstgüte für ein mobiles System nach einem Funkzellenwechsel unter Umständen nicht mehr garantieren. Zum Beispiel kann sich ein mobiles System in eine Funkzelle bewegen, in der keine oder nur noch wenig Bandbreite verfügbar ist. Für eine solche Situation kann das mobile System mit dem neuen Dienstgüteparameter „Loss profile“ angeben, welche Daten unbedingt zu erhalten sind und welche in einer solchen Situation vom Netzwerk verworfen werden können. Desweiteren garantiert der Ansatz, daß beim Funkzellenwechsel keine Unterbrechung auftritt, indem mehrere benachbarte Funkzellen eine Gruppe bilden und Daten zum mobilen System per Multicast in alle Funkzellen einer Gruppe ausgestrahlt werden.

1.2 Gliederung der Arbeit

Dieses Kapitel gibt eine kurze Einführung in das Thema und die dazu vorhandene Literatur. Die Kapitel 2, 3 und 4 enthalten die Grundlagen von Mobile IP, dem indirekten Transportansatz und RSVP, die für das Verständnis dieser Arbeit benötigt werden. Leser, die mit diesen Grundlagen vertraut sind, können diese drei Kapitel überspringen. Kapitel 5 beschäftigt sich mit den Problemen, die sich aus der Kombination von Mobile IP und RSVP unter Berücksichtigung des indirekten Transportansatzes ergeben. Ein Lösungsvorschlag stellt das Fast-Forwarding Protokoll dar, welches das Kapitel 6 im Detail beschreibt. Die Implementierung der in dieser Arbeit vorgeschlagenen Modifikationen an RSVP und Mobile IP beschreibt das Kapitel 7, wobei zusätzlich Messungen die positiven Auswirkungen dieser Modifikationen bestätigen. Abschließend erfolgt im Kapitel 8 eine Zusammenfassung der Ergebnisse mit Hinweisen, an welchen Stellen weitere Untersuchungen notwendig sind. Anhang A erläutert kurz die in dieser Arbeit oft gebrauchten Begriffe mit der Angabe der Seite, auf der sie eingeführt werden. Anhang B enthält die Formate der Mobile IP-Nachrichten und weiterer Nachrichten, die für die Modifikationen an Mobile IP nötig sind.

Kapitel 2

Die Konzepte von Mobile IP

Da sich ein wesentlicher Teil dieser Diplomarbeit mit Erweiterungen von Mobile IP beschäftigt, ist dieses eigenständige Kapitel einer Einführung in die Konzepte von Mobile IP gewidmet. Grundsätzliche Kenntnisse des Internet Protokollstacks (TCP/IP, ARP) sind für das Verständnis dieses Kapitels notwendig (siehe z. B. [Tan92, S. 431ff]).

2.1 Motivation für die Einführung von Mobile IP

Im Internet werden IP-Pakete anhand der darin enthaltenen Zieladresse zum Empfänger geleitet (das sog. *IP-Standardrouting*). Dabei enthält die IP-Adresse eines Systems implizit Informationen über den Anschlußpunkt des Systems an das Internet. Abbildung 2.1 zeigt ein Beispielszenario, in dem sich das System mit der IP-Adresse 134.169.34.117 im Subnetz 134.169.34.0 befindet, welches seinerseits im Klasse-B Netz 134.169.0.0 liegt. Somit müssen

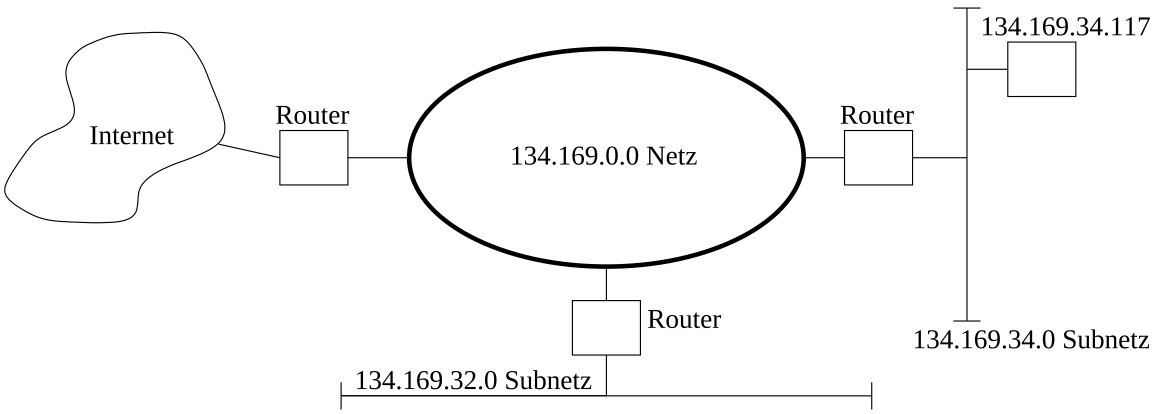

Abbildung 2.1: Aufbau eines Klasse-B Netzes

die Zwischensysteme keine Information über den Aufenthaltsort einzelner stationärer Systeme speichern. Sie können IP-Pakete anhand der Netzkennung weiterleiten, die bei einer

Klasse-B IP-Adresse aus den höherwertigen 16 Bits besteht. Im Beispiel wird ein IP-Paket an die Zieladresse 134.169.34.117 zunächst anhand der Netzkennung 134.169 bis zum 134.169.0.0 Netz transportiert. Dann gelangt es anhand der Subnetzkennung 134.169.34 in das entsprechende Subnetz, in dem es an den Empfänger ausgeliefert wird.

Problem: Auslieferung von IP-Paketen an mobile Systeme

Um ein mobiles System an das Internet anschließen zu können, benötigt es ebenfalls eine IP-Adresse. Da ein Mobilteilnehmer im allgemeinen einer bestimmten Organisation oder Institution zugeordnet ist, bekommt das mobile System eine IP-Adresse in dem Netzwerk oder Subnetz dieser Organisation, dem sog. *Heimatsubnetz*. Die IP-Adresse heißt dann *Heimatadresse*. Bewegt sich der mobile Teilnehmer aus diesem Heimatsubnetz heraus in ein anderes, sog. *fremdes Subnetz*, entsteht folgendes Problem: Pakete an die Heimatadresse gelangen mittels des oben beschriebenen IP-Standardroutings ins Heimatsubnetz, nicht aber zum aktuellen Aufenthaltsort des mobilen Systems.

Ohne den Einsatz von Mobile IP gibt es zwei Möglichkeiten, dem Mobilteilnehmer auch in einem fremden Subnetz den Empfang von IP-Paketen zu ermöglichen:

1. Alle Zwischensysteme speichern Informationen über den aktuellen Aufenthaltsort des mobilen Teilnehmers und senden IP-Pakete dorthin anstelle in das Heimatsubnetz.

2. Das mobile System erhält eine neue IP-Adresse im fremden Subnetz.

Die erste Möglichkeit ist nicht skalierbar für eine sehr große Anzahl von mobilen Systemen, weil die Anzahl der zu speichernden Informationen linear mit der Anzahl der Mobilteilnehmer wächst. Es werden also sehr große Speicher in den Zwischensystemen benötigt. Außerdem steigt der Aufwand für das Suchen innerhalb dieser gespeicherten Informationen für jedes einzelne Paket, welches ein Zwischensystem weiterleiten soll. Schließlich führt jeder Subnetzwechsel eines Mobilteilnehmers zu einer Anpassung der Aufenthaltsinformation in den Zwischensystemen.

Bei der zweiten Möglichkeit stellt sich die Frage, woher ein System die momentane IP-Adresse eines mobilen Systems bekommt, wenn es Daten an dieses senden möchte. Selbst wenn es dieses Wissen hat, führt ein Subnetzwechsel des mobilen Systems z. B. zu einem Abbruch einer bestehenden TCP-Verbindung: Pakete, die weiterhin die IP-Adresse aus dem alten Subnetz als IP-Zieladresse haben, gelangen in das alte Subnetz und damit nicht zum Mobilteilnehmer im neuen Subnetz.

Mobile IP [Per96] bietet eine Lösung des beschriebenen Problems. Die folgenden Abschnitte geben eine Einführung in Mobile IP.

2.2 Zielsetzung und Voraussetzungen

Bei der Entwicklung von Mobile IP wurden die folgenden Ziele verfolgt:

- Das mobile System soll über eine einzige IP-Adresse erreichbar sein. Damit ist die Mobilität des Systems transparent für alle anderen Systeme im Internet.

- Die Implementierung soll möglichst wenige Systeme im Internet betreffen, so daß der Änderungsaufwand im Internet gering bleibt.
- Die Signalisierung muß Sicherheitsaspekte beachten, damit die Änderung der Route zu einem Mobilteilnehmer nicht für das Umleiten von Daten mißbraucht werden kann.
- Da die Bandbreite auf drahtlosen Teilstrecken meist geringer ist als auf drahtgebundenen, soll die Anzahl und Größe der Signalisierungsnachrichten minimal sein.

Voraussetzungen zum Betrieb von Mobile IP sind:

- IP-Pakete werden anhand der IP-Zieladresse weitergeleitet und nicht z. B. entlang eines vom Sender vorgegebenen Weges (Source Routing).
- Um der Signalisierung von Mobile IP genügend Zeit zur Vollendung zu geben, sollten Subnetzwechsel nicht häufiger als einmal pro Sekunde auftreten.

Mobile IP ist **nicht** notwendig, wenn ein mobiles System:

- IP-Pakete versendet, weil das weiterhin das IP-Standardrouting leisten kann.
- sich im Heimatsubnetz aufhält.

Ist das mobile System über ein zelluläres Mobilfunknetz an das Internet angeschlossen, bedeutet ein Funkzellenwechsel nicht notwendigerweise eine Involvierung von Mobile IP: Wechselt der mobile Teilnehmer die Funkzelle, bleibt aber in demselben Subnetz, ist keine Änderung von Routen und damit keine Mobile IP Signalisierung notwendig.

2.3 Architektur und Datenfluß

Dieser Abschnitt beschreibt die grundsätzliche Funktionsweise von Mobile IP anhand des Datenflusses und führt die dazu benötigten neuen Netzwerkkomponenten ein.

2.3.1 Der grundsätzliche Ablauf

IP-Pakete für ein mobiles System gelangen zunächst immer in dessen Heimatsubnetz. Wenn es sich nicht dort aufhält, nimmt der sog. *Home Agent* alle Pakete für das mobile System entgegen. Der Mobilteilnehmer zeigt jeden Subnetzwechsel beim Home Agent an, die sog. *Registrierung*. Dabei sendet er diesem die *Care-of Adresse*, eine IP-Adresse, unter der er im fremden Subnetz per IP-Standardrouting zu erreichen ist. Somit ist der Home Agent in der Lage, alle Pakete zum mobilen System, die bei ihm ankommen, an die Care-of Adresse weiterzuleiten.

Die Care-of Adresse reflektiert den momentanen Aufenthaltsort des Mobilteilnehmers in einem fremden Subnetz. Sie kann einerseits zu einem sog. *Foreign Agent* gehören, der die vom Home Agent weitergeleiteten Pakete im fremden Subnetz annimmt und zum Mobilteilnehmer weiterleitet. Andererseits kann sie auch eine temporäre IP-Adresse sein, die das mobile System für die Dauer seines Aufenthalts im fremden Subnetz bekommt. In beiden Fällen ist zu beachten, daß das mobile System beim Senden eines Paketes weiterhin seine Heimatadresse als Absender verwendet, damit eventuelle Antworten über den Home Agent zum Mobilteilnehmer gelangen. Verwendet es die Care-of Adresse als Absender, gelangt eine Antwort nach einem Subnetzwechsel weiterhin in das alte Subnetz.

Diese zwei Ausprägungen der Care-of Adresse bestimmen zwei Betriebsarten von Mobile IP, die im folgenden genauer betrachtet werden. Zunächst erfolgt aber eine gesonderte Betrachtung der Strecke vom Home Agent zur Care-of Adresse.

2.3.2 Der Tunnel vom Home Agent zur Care-of Adresse

Der Home Agent kann ein IP-Paket, das per IP-Standardrouting in das Heimatsubnetz gelangt ist, nicht ohne eine zusätzliche Verarbeitung in das fremde Subnetz weiterleiten. Damit die eigentliche Zieladresse des Paketes, die Heimatadresse des mobilen Systems, für die Zwischensysteme auf dem Weg vom Home Agent in das fremde Subnetz unsichtbar bleibt, kapselt der Home Agent das IP-Paket in ein weiteres ein, welches als Zieladresse die Care-of Adresse besitzt. Damit entsteht ein sog. *IPIP-Paket*. Dieses kann nun per IP-Standardrouting zur Care-of Adresse in das fremde Subnetz gelangen, wo das ursprüngliche Paket wieder ausgepackt und an den Mobilteilnehmer übergeben wird. Diesen Mechanismus nennt man *Tunneln*, die Strecke, auf der sich die IPIP-Pakete bewegen, einen *IPIP-Tunnel* [Per96a].

2.3.3 Betriebsart 1: Mobile IP mit einem Foreign Agent

In einer Betriebsart von Mobile IP ist die Care-of Adresse die IP-Adresse eines Foreign Agents. Teil a) der Abbildung 2.2 zeigt den Datenfluß mit den einzelnen involvierten Instanzen, Teil b) einen schematischen Ablauf.

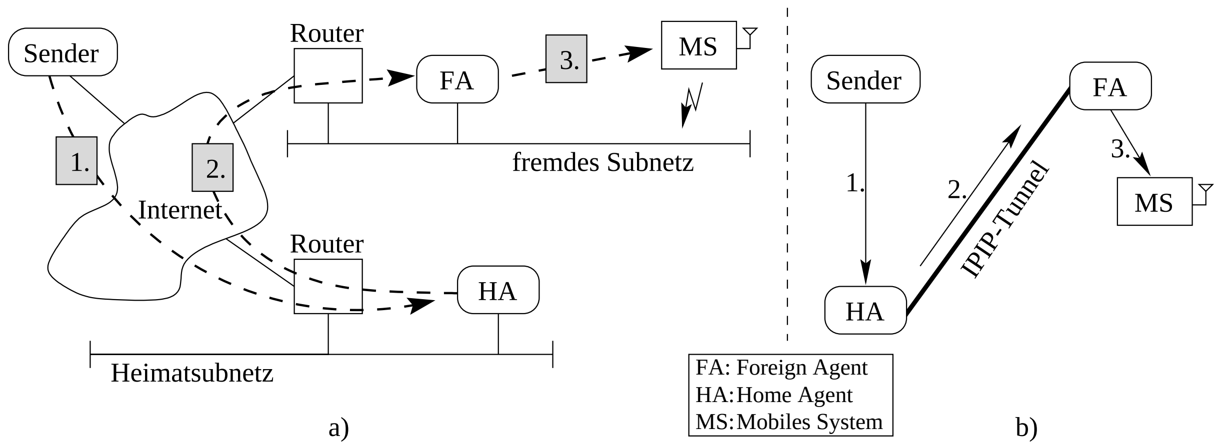

Abbildung 2.2: Mobile IP mit einem Foreign Agent

Zunächst gelangen IP-Pakete für das mobile System in das Heimatsubnetz (1.Pfeil), wo sie der Home Agent (HA) in Empfang nimmt. Dieser tunnelt das Paket zum Foreign Agent (FA) (2.Pfeil), der es als getunneltes Paket identifiziert und auspackt. Danach sendet er das ursprüngliche Paket zum mobilen System (MS), welches sich in demselben Subnetz befindet wie der Foreign Agent (3.Pfeil).

Es ist in der Mobile IP Spezifikation nicht festgelegt, ob ein *Mobility Agent* (der Home Agent oder der Foreign Agent) ein separates System im Heimatsubnetz bzw. fremden Subnetz sein soll, wie das in Teil a) der Abbildung dargestellt ist, oder ob beide jeweils auch direkt auf dem Router angesiedelt sein können. Deswegen wird im folgenden die schematische Betrachtung der Vorgänge gemäß Teil b) vorgezogen.

2.3.4 Betriebsart 2: Der co-located Betrieb

Sollte im fremden Subnetz kein Foreign Agent zur Verfügung stehen, kann das mobile System in den sog. *co-located Betrieb* gehen. In diesem Fall erhält es im fremden Subnetz durch einen hier nicht näher beschriebenen Mechanismus (z. B. DHCP) eine temporäre IP-Adresse (die sog. *co-located Care-of Adresse*), die es als Care-of Adresse dem Home Agent meldet. Dadurch ergibt sich die in Abbildung 2.3 dargestellte Situation:

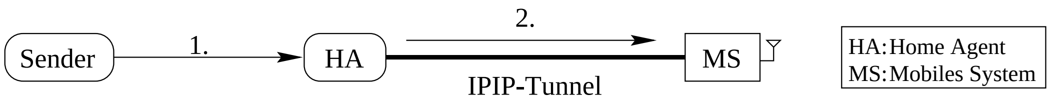

Abbildung 2.3: Mobile IP im co-located Betrieb

Vom Sender gelangen die IP-Pakete für den mobilen Teilnehmer in das Heimatsubnetz, wo sie der Home Agent empfängt. Wieder kapselt er die Pakete ein, diesmal aber mit der co-located Care-of Adresse, d. h. der temporären IP-Adresse des mobilen Systems als Zieladresse. Per IP-Standardrouting gelangen die Pakete direkt zum mobilen System, welches diese auspackt und dem Inhalt entsprechend verarbeitet.

2.3.5 Vergleich der Betriebsarten

Der co-located Betrieb hat gegenüber dem mit einem Foreign Agent den Vorteil, daß im fremden Subnetz keine explizite Unterstützung für Mobile IP durch einen Foreign Agent vorhanden sein muß. Es ist lediglich ein Mechanismus für eine temporäre Zuteilung von IP-Adressen notwendig. Dazu muß allerdings in jedem Subnetz, das ein mobiler Teilnehmer besuchen könnte, ein Pool von temporären IP-Adressen freigehalten werden. Da die verfügbaren IP-Adressen in IP Version 4 aber bereits knapp werden, ist dies der größte Nachteil des co-located Betriebes.

Vorteile des Betriebes eines Foreign Agents sind, daß keine zusätzlichen IP-Adressen benötigt werden. Außerdem bleibt der Overhead für die Übertragung des zusätzlichen IPIP-

Headers auf die drahtgebundene Strecke vom Home Agent zum Foreign Agent beschränkt, weil bereits der Foreign Agent die Pakete auspackt.

Die Mobile IP Spezifikation empfiehlt, den co-located Betrieb wegen des Problems der Belegung von IP-Adressen nur ausnahmsweise dann zu verwenden, wenn kein Foreign Agent zur Verfügung steht. Sonst ist der Betrieb mit einem Foreign Agent vorzuziehen.

Tabelle 2.1 gibt eine Bewertung der beiden Betriebsarten im Überblick:

Betrieb mit einem Foreign Agent	Co-located Betrieb
+ keine zusätzlichen IP-Adressen im fremden Subnetz belegt + weniger Overhead auf dem drahtlosen Link – Foreign Agent im fremden Subnetz notwendig	+ Mobilitätsunterstützung durch Foreign Agent nicht notwendig – Belegung von IP-Adressen im fremden Subnetz – zusätzlicher Overhead auf der drahtlosen Strecke

Tabelle 2.1: Gegenüberstellung der beiden Betriebsarten von Mobile IP

2.3.6 Das Mobile System als Sender: Dreiecksrouting

Vom mobilen System gesendete Pakete werden grundsätzlich mittels des IP-Standardroutings weitergeleitet. Dadurch ergibt sich das sog. *Dreiecksrouting* (siehe Abbildung 2.4 am Beispiel des Betriebes mit einem Foreign Agent).

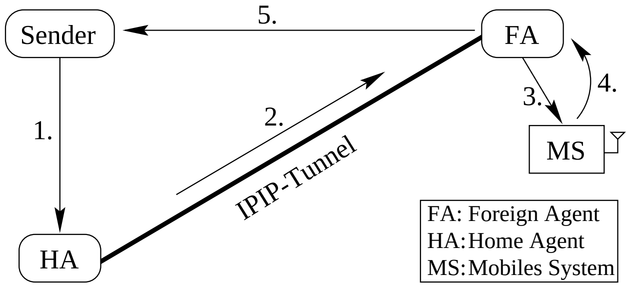

Abbildung 2.4: Dreiecksrouting in Mobile IP

Daten von einem Sender zu einem mobilen Teilnehmer in einem fremden Subnetz nehmen den Umweg über den Home Agent (1.), der als einziger den Aufenthaltsort des mobilen Teilnehmers kennt und die Daten an die Care-of Adresse tunnelt (2.). In der Abbildung nimmt der Foreign Agent die Daten entgegen und leitet sie zum Mobilteilnehmer (3.).

Wenn das mobile System Daten an den Sender zurücksendet, gehen sie in diesem Beispiel zunächst an den Foreign Agent (4.), der hier also sein Default-Router ist. Von dort gelangen die Daten per IP-Standardrouting zum Sender (5.). Das mobile System kann die Daten aber auch über jeden anderen Router im fremden Subnetz versenden, wie das z. B. beim co-located Betrieb geschieht.

Der Weg vom Mobilteilnehmer zum Sender ist also ein anderer als der umgekehrte Weg. Es ergibt sich für die gesamte Strecke Sender ⇒ Home Agent ⇒ Mobilteilnehmer ⇒ Sender eine *Dreiecksroute*. Einzige Ausnahme ist, wenn auch der vom IP-Standardrouting ausgewählte Weg vom Mobilteilnehmer zum Sender zufällig über den Home Agent führt.

Somit können Daten zum Mobilteilnehmer eine deutlich höhere Verzögerung erfahren als Daten von diesem, z. B. wenn sich der Sender und der mobile Teilnehmer in demselben Subnetz befinden, das Heimatsubnetz aber in größerer Entfernung liegt. Auch in diesem Fall nehmen Daten vom Sender zum mobilen Teilnehmer den Umweg über den Home Agent. Abhilfe schafft die im Abschnitt 2.7 vorgestellte Route Optimization.

2.3.7 Rückkehr ins Heimatsubnetz

Kehrt ein Mobilteilnehmer in sein Heimatsubnetz zurück, soll er wieder selbst für sich bestimmte IP-Pakete entgegennehmen, also ohne Unterstützung von Mobile IP arbeiten [Per96, S. 56]. Dazu informiert er den Home Agent über seine Rückkehr ins Heimatsubnetz, damit der Home Agent keine Pakete mehr für ihn entgegennimmt. Dieser Vorgang heißt *Deregistrierung*.

2.4 Die Signalisierung

Dieser Abschnitt betrachtet die Signalisierungen in Mobile IP, die zur Gewährleistung der oben beschriebenen Unterstützung eines mobilen Teilnehmers im Internet benötigt werden. Die wichtigste Funktion ist dabei die Benachrichtigung des Home Agents über den aktuellen Aufenthaltsort des mobilen Teilnehmers. Mobile IP stellt dafür zwei Dienste zur Verfügung: Agent Discovery und die Registrierung. Zunächst soll aber noch kurz der Mechanismus der Mobile IP Erweiterung dargestellt werden.

2.4.1 Mobile IP Erweiterungen

Mobile IP versendet Registrierungsnachrichten mittels UDP, beim Agent Discovery nutzt es zur Signalisierung bereits vorhandene Protokollmechanismen von ICMP. Um bei Bedarf Mobile IP-eigene Daten versenden zu können, hängt Mobile IP an die verwendete ICMP-Nachricht eine oder mehrere eigene Dateneinheiten an, für die ein allgemeines Format existiert: Die *Mobile IP Erweiterung*. Diese kommt aber auch bei der Erweiterung von mit UDP versendeten Registrierungsnachrichten um optionale Dateneinheiten zum Einsatz.

2.4.2 Agent Discovery

Ein mobiles System benötigt drei Informationen, um seinen Home Agent über seinen aktuellen Aufenthaltsort informieren zu können:

1. Hat ein Subnetzwechsel stattgefunden?

2. Wenn ja, befindet sich das mobile System im Heimatsubnetz oder in einem fremden Subnetz?

3. Falls in einem fremden Subnetz, stehen Foreign Agents zur Verfügung oder muß der co-located Betrieb verwendet werden?

Sofern diese Fragen nicht die Sicherungsschicht auf dem mobilen System beantworten kann, schafft in Mobile IP der Mechanismus des *Agent Discovery* Abhilfe [Per96, S. 14-24].

Protokollablauf

Es gibt zwei Varianten für den Ablauf von Agent Discovery:

1. Alle Mobility Agents senden periodisch *Agent Advertisement* Nachrichten an eine Multicast-Adresse, mit der sie Informationen über den angebotenen Dienst verbreiten. Dies ist die Standardvariante.

2. Erhält ein mobiles System keine periodischen Agent Advertisements, sendet es eine *Agent Solicitation* Nachricht in das lokale Netz, auf die dann die Mobility Agents mit Agent Advertisements antworten.

In jedem Fall kommen beim Mobilteilnehmer eine oder mehrere Agent Advertisements an, sofern es eine Verbindung auf der Sicherungsschicht zum fremden Subnetz gibt und mindestens ein Mobility Agent existiert. Aus diesen Agent Advertisements kann das mobile System die im vorherigen Abschnitt genannten Informationen gewinnen.

Nachrichtenformate

Eine Agent Solicitation entspricht einer ICMP Router Solicitation [Dee91] und enthält keine Mobile IP-spezifischen Daten. Eine Agent Advertisement besteht aus einer ICMP Router Advertisement [Dee91] mit mindestens einer Mobile IP Erweiterung: der sog. *Mobility Agent Advertisement*. Sofern ein Mobility Agent, der als Foreign Agent arbeitet, diese Agent Advertisement aussendet, enthält diese mindestens eine Care-of Adresse. Das genaue Format ist in Abschnitt B.1.2 dargestellt.

Erkennen eines Subnetzwechsels

Mobile IP bietet zwei Möglichkeiten, wie ein mobiles System einen Subnetzwechsel erkennen kann.

1. Die periodisch ausgesendeten Agent Advertisements sind nur eine bestimmte Lebensdauer gültig. Erhält der Mobilteilnehmer keine periodischen Agent Advertisements mehr von dem Mobility Agent, der das mobile System zuletzt unterstützt hat, läuft die Lebensdauer der Agent Advertisement ab, und sie wird ungültig. Dies ist ein Hinweis auf einen Subnetzwechsel. Das mobile System wertet in diesem Fall andere Agent Advertisements aus, die noch gültig sind, oder sendet eine Agent Solicitation, um von einem neuen Mobility Agent Unterstützung zu erhalten.

   Die Mobile IP Spezifikation empfiehlt, die Lebensdauer einer Agent Advertisement dreimal so groß zu wählen wie die Periode, mit der sie versendet werden. Da dieses Versenden mit einem unzuverlässigen Protokoll geschieht, können so zwei aufeinanderfolgende Agent Advertisements verloren gehen, ohne daß das mobile System fälschlicherweise einen Subnetzwechsel vermutet.

2. Voraussetzung für die zweite Möglichkeit ist, daß eine Agent Advertisement zusätzlich die Information enthält, welcher Teil der darin enthaltenen Care-of Adressen zur Subnetzkennung gehört (die sog. Prefix-Lengths Erweiterung [Per96, S. 18]). Damit kann das mobile System einen Subnetzwechsel anhand einer neu empfangenen Agent Advertisement erkennen, indem es die Subnetzkennung des Absenders der neuen Agent Advertisement mit der des bisherigen Mobility Agents vergleicht.

Heimatsubnetz oder fremdes Subnetz

Als zweites benötigt der mobile Teilnehmer die Information, ob er sich nach einem Subnetzwechsel in seinem Heimatsubnetz oder einem fremden Subnetz befindet. Dazu vergleicht er die IP-Adresse des Absenders einer Agent Advertisement mit der ihm bekannten Adresse seines Home Agents. Sind beide identisch, befindet er sich im Heimatsubnetz und muß sich beim Home Agent deregistrieren. Ist der Vergleich negativ, muß er sich bei einem Foreign Agent registrieren (bzw. direkt beim Home Agent im Falle des co-located Betriebes).

Auswahl des Foreign Agent

Wenn der Mobilteilnehmer in ein fremdes Subnetz wechselt, benötigt er die Adresse eines Foreign Agents zur Registrierung. Dazu wartet er auf die Ankunft einer Agent Advertisement und wertet die Flags sowie die Care-of Adressen aus. Kann der Foreign Agent das mobile System unterstützen, führt dieses eine Registrierung mit dem Foreign Agent durch; kann der Foreign Agent das mobile System nicht unterstützen, wartet dieses auf eine weitere Agent Advertisement von einem anderen Mobility Agent in dem Subnetz.

2.4.3 Die Registrierung

Die Mobile IP Registrierung erfüllt drei Funktionen:

1. Die Aufforderung an einen Foreign Agent, den mobilen Teilnehmer lokal zu unterstützen, d. h. Daten, die der Home Agent zum Foreign Agent tunnelt, an den mobilen Teilnehmer auszuliefern. Diese Funktion entfällt beim co-located Betrieb.

2. Die Information des Home Agents über den aktuellen Standort des mobilen Systems.

3. Die periodische Erneuerung einer Registrierung, damit sie weiterhin gültig bleibt.

Da Abschnitt 2.3.4 bereits die Nachteile des co-located Betriebes aufführt und im Verlauf dieser Diplomarbeit keine weitere Betrachtung dieser Betriebsart stattfindet, geht dieser Abschnitt nur auf die Registrierung im Falle des Betriebs eines Foreign Agents im fremden Subnetz ein.

Der Registrierungsvorgang

Abbildung 2.5 stellt schematisch den Signalisierungsfluß von Mobile IP bei einer Registrierung aus einem fremden Subnetz dar:

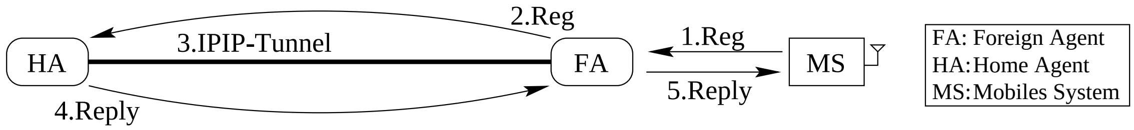

Abbildung 2.5: Registrierung des mobilen Systems mit einem Foreign Agent

Damit der Foreign Agent erkennt, daß sich das mobile System lokal aufhält, sendet dieses nach einem Subnetzwechsel in den Bereich des Foreign Agents eine *Registrierungsanforderung* zunächst zum Foreign Agent (1.Reg). Dieser speichert die darin enthaltenen Informationen und leitet sie zum Home Agent weiter (2.Reg). Der Home Agent prüft, ob die Registrierung korrekt ist und ob er das mobile System unterstützen kann. Ist die Prüfung positiv, richtet er den IPIP-Tunnel ein (3.) und sendet eine *Registrierungsantwort* über den Foreign Agent (4.Reply) zum mobilen System (5.Reply), die eine Bestätigung der Registrierungsanforderung enthält. Diese Nachricht soll im folgenden *Accept-Nachricht* genannt werden. Ist die Registrierung nicht möglich, richtet der Home Agent keinen Tunnel ein und sendet eine Registrierungsantwort mit einer Ablehnung via dem Foreign Agent zum mobilen Teilnehmer, die sog. *Deny-Nachricht.* Wird im folgenden von *Mobile IP Nachrichten* gesprochen, meint der Begriff sowohl Registrierungsanforderungen als auch Registrierungsantworten.

Es kann der Fall auftreten, daß der Foreign Agent den Mobilteilnehmer nicht unterstützen kann. Dann sendet er die Registrierungsanforderung nicht an den Home Agent (2.Reg), sondern schickt eine Deny-Nachricht mit einer Information über den Grund der Ablehnung zurück zum mobilen System.

Periodische Registrierungsanforderungen

Gemäß der Mobile IP Spezifikation sollen Registrierungsanforderungen periodisch ausgesendet werden. Jede Registrierung hat auf einem Mobility Agent nur eine bestimmte Lebensdauer. Wenn diese überschritten wird, d. h. der sog. *Registrierungstimer* abläuft, ohne daß der Mobility Agent eine erneute periodische Registrierungsanforderung bekommen hat, löscht der Mobility Agent die Registrierung. Damit geht er davon aus, daß das mobile System keine Mobile IP Unterstützung mehr benötigt, sich aber nicht abgemeldet hat. Gleiches gilt auch für das mobile System, auch dort hat eine Registrierung nur eine bestimmte Lebensdauer, die bei Überschreitung zum Löschen der Registrierung führt. Dies tritt dann auf, wenn das mobile System auf die periodisch ausgesendeten Registrierungsanforderungen keine Registrierungsantworten erhält.

Das Löschen einer Registrierung kann die folgenden Gründe haben:

1. Der mobile Teilnehmer hat das Subnetz gewechselt. Der Foreign Agent im alten Subnetz bekommt keine Mitteilung über den Wechsel und kann somit die Registrierung nur implizit über den Registrierungstimer löschen.

2. Das mobile System wird einfach ausgeschaltet, ohne daß der Home Agent eine Abmeldung bekommt (z. B. durch leere Akkus).

3. Durch die spezielle Charakteristik von Datenübertragungen per Funk kann es vorkommen, daß ein Mobilteilnehmer den Kontakt auf der Sicherungsschicht zum Subnetz verliert. In diesem Fall kann auch eine ordnungsgemäße Abmeldung beim Home Agent nicht gelingen.

4. Mobile IP Nachrichten werden mittels UDP versendet und können im Netz verloren gehen (Bitfehler, Überlastung der Zwischensysteme). Die Lebensdauer einer Registrierung sollte deswegen laut Mobile IP Spezifikation dreimal so groß sein wie die Periode, mit der die Registrierungsanforderungen versendet werden. Damit führt der Verlust einer oder zweier Mobile IP Nachrichten nicht automatisch zur Beendigung der Registrierung.

Aushandeln der Lebensdauer einer Registrierung

Es gibt drei verschiedene Werte für die Lebensdauer einer Registrierung in den bisher vorgestellten Nachrichten:

1. Die in der Agent Advertisement gibt die maximale Lebensdauer an, die der Foreign Agent bereit zu gewähren ist.

2. Die in der Registrierungsanforderung gibt unter Berücksichtigung der ersten die Lebensdauer an, die das mobile System maximal unterstützen kann.

3. Die in der Registrierungsantwort stellt die wirklich genutzte Lebensdauer dar, die der Home Agent in Abhängigkeit von den ersten beiden Werten ermittelt hat.

Durch das Versenden dieser drei Nachrichten zwischen Foreign Agent, mobilem System und dem Home Agent wird also auch die Lebensdauer einer Registrierung zwischen diesen Systemen vereinbart.

Die Deregistrierung

Bei der Rückkehr von einem fremden Subnetz in sein Heimatsubnetz muß sich ein Mobilteilnehmer bei seinem Home Agent deregistrieren. Die dazu an den Home Agent versendete *Deregistrierungsanforderung* entspricht einer Registrierungsanforderung, nur daß die Lebensdauer der Registrierung Null ist. Der Home Agent antwortet auf diese Deregistrierung mit einer Registrierungsantwort, deren Lebensdauer ebenfalls auf Null steht.

2.4.4 Sicherheit

Die Signalisierung von Mobile IP bietet verschiedene Möglichkeiten, von Unbefugten mißbraucht zu werden, um an nicht für sie bestimmte Daten zu gelangen. Die folgenden Abschnitte stellten kurz die in der Mobile IP Spezifikation [Per96] betrachteten Schutzmechanismen vor, sofern sie für die folgenden Kapitel dieser Arbeit von Bedeutung sind.

Authentifizierung

Da durch den Registrierungsvorgang der Home Agent Pakete für einen Mobilteilnehmer an ein fremdes Subnetz sendet, kann dieser Vorgang von einem Unbefugten dazu mißbraucht werden, selbst an für einen mobilen Teilnehmer bestimmte Daten zu gelangen. Aus diesem Grund müssen Registrierungsanforderungen authentifiziert werden, so daß nur der Mobilteilnehmer selbst auf dem Home Agent die Einrichtung eines Tunnels veranlassen kann. Sowohl die Registrierungsanforderung als auch die Registrierungsantwort werden durch das Anhängen einer speziellen Mobile IP Erweiterung authentifiziert, die nur der Home Agent bzw. das mobile System auf ihre Echtheit überprüfen kann [Per96, S. 32ff].

Replay Protection

Wenn eine Registrierungsanforderung authentifiziert ist, kann ein potentieller Angreifer zwar den Inhalt der Nachricht nicht mehr verändern. Er kann sie aber zwischenspeichern und wiederverwenden, wenn das mobile System in ein anderes Subnetz gewechselt ist, um dann den Tunnel vom Home Agent wieder in das alte Subnetz umzuleiten. Vor solchen Attacken soll die sogenannte *Replay Protection* schützen. Diese existiert in zwei Varianten [Per96, S. 68]:

1. Replay Protection durch Zeitstempel
2. Replay Protection durch Nonces

Bei der ersten Variante bekommt jede Mobile IP Nachricht die aktuelle Uhrzeit vom Sender als Zeitstempel in das 64 Bit große Identifikationsfeld mitgegeben. Der Empfänger ignoriert die Nachricht, wenn deren Zeitstempel älter als der Zeitstempel der zuletzt davor empfangenen Nachricht ist.

Bei der zweiten Variante wird das 64 Bit große Identifikationsfeld der Mobile IP Nachricht für eine *Nonce* verwendet, die aus zwei gleich großen Teilen besteht. Das Prinzip funktioniert nur zwischen zwei Systemen, die wechselseitig jeweils genau eine Nachricht zum anderen System senden und dann auf eine Antwort warten müssen.

Funktionsweise der Replay Protection durch Nonces Abbildung 2.6 zeigt den Ablauf einer Mobile IP Registrierung mit Nonces.

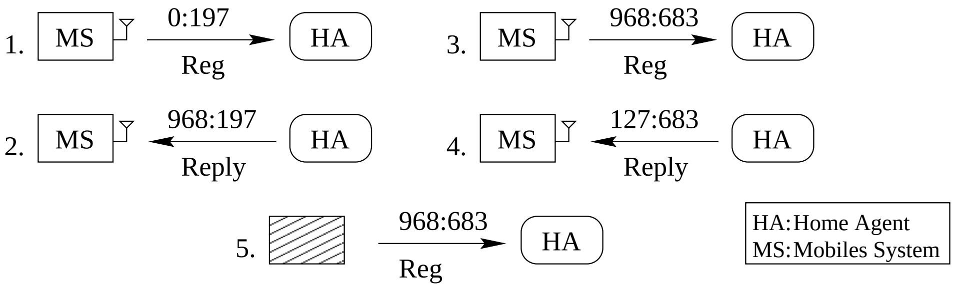

Abbildung 2.6: Ablauf einer Registrierung mit Nonces als Replay Protection

Bei Beginn einer Kommunikation sendet das mobile System (MS) eine Registrierungsanforderung (1.), in deren Nonce es in seine Hälfte eine neue, zufallsgenerierte 32-Bit Zahl einsetzt. In der Abbildung wird diese durch die dreistellige Dezimalzahl 197 symbolisiert. Der andere Teil muß beim Anfang einer Kommunikation Null sein, weil der Mobilteilnehmer noch keine Nachricht vom Home Agent (HA) empfangen hat. Wenn die vom Home Agent erhaltene Registrierungsanforderung (Reg) korrekt durch das mobile System authentifiziert ist, kann der Home Agent den zum mobilen System gehörigen Teil der Nonce (197) in seine Antwort kopieren und generiert selbst eine neue Zufallszahl für den eigenen Teil (968). Zunächst muß er die Registrierung ablehnen (2.), weil der eigene Teil der Nonce aus der Registrierungsanforderung leer war. Die Registrierungsantwort enthält aber jetzt eine komplette Nonce mit zwei gültigen Teilen, so daß das mobile System eine neue Registrierung starten kann. Dazu kopiert es bei 3. den zum Home Agent gehörigen Teil der Nonce aus der letzten Registrierungsantwort (968) in die neue Registrierungsanforderung und generiert selbst eine neue Zufallszahl für den eigenen Teil (683). Der Home Agent stellt nach Empfang der Registrierungsanforderung fest, daß der eigene Teil der Nonce aus dieser Nachricht dem eigenen Teil der letzten vom Home Agent versendeten Registrierungsantwort entspricht. Damit akzeptiert er die Registrierung und sendet eine Registrierungsantwort (4.) an den mobilen Teilnehmer, wieder mit einem neuen eigenen Teil der Nonce (127).

Versucht ein Angreifer, wie in Schritt 5 dargestellt, die Registrierungsanforderung aus Schritt 3 zu wiederholen, ist der zum Home Agent gehörende Teil der Nonce (968) ungleich demselben Teil der Nonce aus der letzten vom Home Agent gesendeten Registrierungsantwort (127). Der Home Agent erkennt also den Angriff und muß die Registrierung ablehnen.

2.5 Das interne Verhalten bei einer Registrierung

Die Mobile IP Instanzen mobiles System, Foreign Agent und Home Agent müssen für eine Registrierung verschiedene Aktionen ausführen, die im folgenden beschrieben werden. Wie im vorigen Abschnitt findet auch hier keine Betrachtung des co-located Betriebes statt.

2.5.1 Das Mobile System

Das mobile System speichert seinen Zustand in insgesamt drei Zustandsvariablen:

1. Die *Ortsvariable* beinhaltet, ob sich das mobile System im Heimatsubnetz (atHome), im fremden Subnetz (atForeign) oder an einem unbekannten Ort befindet (atInit).

2. Die *Registrierungsvariable* speichert, ob das mobile System registriert ist (True) oder nicht (False).

3. Die *Wartevariable* ist True, wenn das mobile System eine Registrierungsanforderung ausgesendet hat und noch auf eine Antwort wartet, oder False sonst.

Durch sechs verschiedene Eingabeereignisse kann sich der Zustand des mobilen Systems ändern:

1. SNW-HN: Subnetzwechsel des mobilen Systems in sein Heimatsubnetz

2. SNW-FN: Subnetzwechsel in ein fremdes Subnetz

3. Accept: Eintreffen einer Accept-Nachricht vom Home Agent

4. Deny: Eintreffen einer Deny-Nachricht vom Home Agent (oder auch vom Foreign Agent, wenn dieser das mobile System nicht unterstützen kann)

5. Period: Aussenden einer periodischen Registrierungsanforderung in einem fremden Subnetz, wenn das mobile System bereits registriert ist

6. Timeout: Ablaufen des Registrierungstimers für eine Registrierung

Daraus ergibt sich der in Abbildung 2.7 dargestellte Zustandsautomat, der im folgenden Abschnitt erläutert wird.

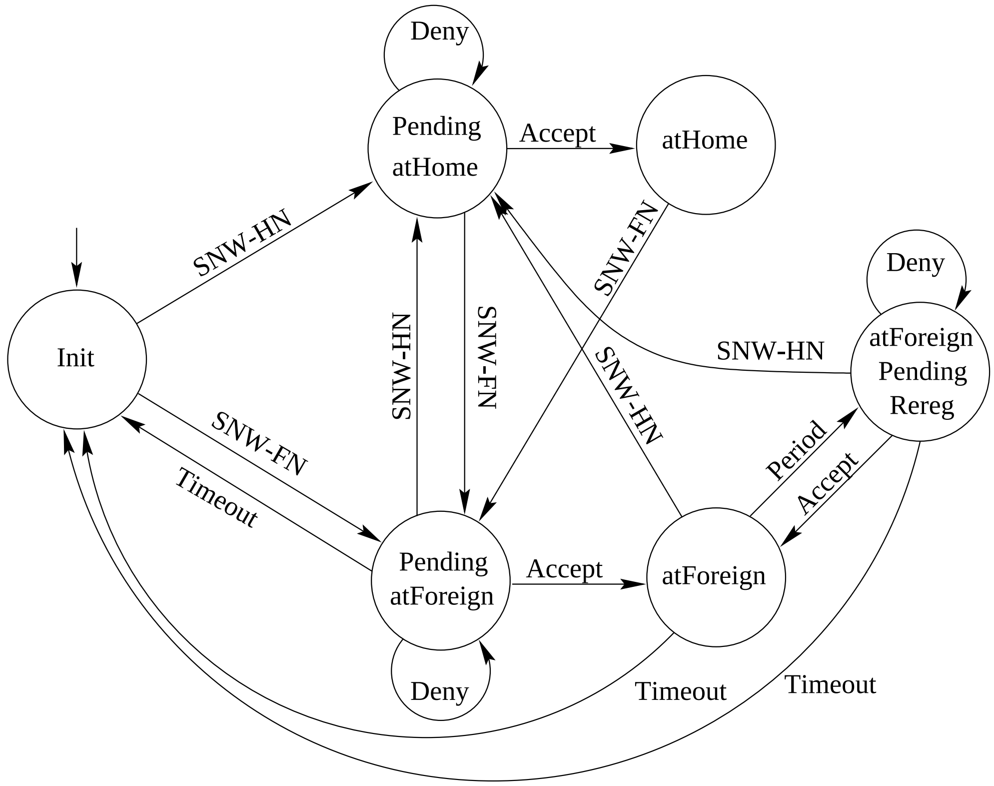

Abbildung 2.7: Zustandsautomat einer Registrierung für das mobile System

Dynamische Betrachtung: Ereignisse und Zustandsübergänge

Der Startzustand ist der „Init"-Zustand. Stellt das mobile System mittels Agent Discovery fest, daß es sich im Heimatsubnetz befindet, sendet es eine Deregistrierungsanforderung und geht in den „Pending atHome"-Zustand über, d. h. es wartet auf eine Antwort vom Home Agent. Akzeptiert der Home Agent die Deregistrierung, wechselt es in den Zustand „atHome", kann damit also im Heimatsubnetz ohne Mobile IP Unterstützung arbeiten. Lehnt der Home Agent sie ab, wiederholt der Mobilteilnehmer die Deregistrierung.

Wechselt das mobile System in ein fremdes Subnetz, geht es in den Zustand „Pending atForeign" über und sendet eine Registrierungsanforderung über den Foreign Agent zum Home Agent. Akzeptieren der Home Agent und der Foreign Agent die Registrierung, nimmt das mobile System den Zustand „atForeign" ein. Es kann also mit Unterstützung von Mobile IP auch im fremden Subnetz aus dem gesamten Internet erreicht werden. Wird die Registrierung abgelehnt, wiederholt der Mobilteilnehmer die Registrierung.

Im fremden Subnetz müssen laut Mobile IP Spezifikation Registrierungsanforderungen periodisch ausgesendet werden. Läuft eine solche Periode ab, geht das mobile System in den Zustand „atForeign Pending Rereg" über, wartet also auf eine Antwort auf die erneute Registrierung. Akzeptiert der Home Agent diese, setzt das mobile System den Registrierungstimer neu, nimmt aber darüberhinaus keine weiteren Änderungen vor. Im Falle einer

Ablehnung wiederholt es die Registrierung erneut. Bleiben die Registrierungsanforderungen unbeantwortet und der Registrierungstimer läuft ab, geht das mobile System in den „Init"-Zustand über, um auf einen Subnetzwechsel zu warten bzw. sich erneut einen Mobility Agent mittels Agent Discovery zu suchen.

Betrachtung der Zustände

Tabelle 2.2 stellt die Zustandsvariablen mit den einzelnen Zuständen in eine Relation. Befindet sich das mobile System im Zustand „Init", ist der Wert der Registrierungsvariable

Zustand	Ortsvariable	Registrierungsvar.	Wartevariable
Init	atInit	True/False	True/False
Pending atHome	atHome	False	True
atHome	atHome	True	False
Pending atForeign	atForeign	True	False
atForeign	atForeign	False	True
atForeign Pending Rereg	atForeign	True	True

Tabelle 2.2: Relation Zustände – Zustandsvariablen auf dem mobilen System

sowie der Wartevariable nicht von Bedeutung. Die Zustandstripel (atHome, False, False) sowie (atForeign, False, False) sind nicht erreichbar, weil ein mobiles System sowohl im Heimatsubnetz als auch im fremden Subnetz immer registriert ist oder eine Registrierung versucht. Sonst befindet es sich im Zustand „Init". Das Zustandstripel (atHome, True, True) tritt ebenfalls nicht auf, weil dieses einem „atHome Pending Rereg"-Zustand entspräche. Im Heimatsubnetz gibt es aber keine periodische Wiederholung der Registrierung, sondern nur die einmalige Deregistrierung.

Änderungen beim Routing

Wechselt das mobile System in den Zustand „atHome", muß es das Routing (i. a. die Routingtabelle) entsprechend anpassen [Per96, S. 56f]. Die Konfiguration sieht dabei genauso aus wie bei einem stationären System in diesem Subnetz.

Geht es in den Zustand „atForeign" über, sind zwei Neueinträge in der Routingtabelle nötig: Ein Eintrag, daß der Foreign Agent lokal erreichbar ist, und ein zweiter für den Default-Router. Die IP-Adresse des Default-Routers kann in einer Agent Advertisement enthalten sein, das mobile System kann aber auch den Foreign Agent als Default-Router nutzen, sofern dieser als Router konfiguriert ist. Alle weiteren Einträge, die noch von einer Registrierung in einem anderen fremden Subnetz oder dem Heimatsubnetz stammen, müssen gelöscht werden.

Das ARP-Verhalten

Beim Aufenthalt des mobilen Teilnehmers in einem fremden Subnetz darf er keine ARP-Anfragen stellen oder ARP-Antworten [Ste94] geben. Einzige Ausnahme ist, daß er auf eine ARP-Anfrage des Foreign Agents mit einer Unicast ARP-Antwort reagieren darf [Per96, S. 62ff]. Nach erfolgreicher Deregistrierung im Heimatsubnetz schaltet er seine normale ARP-Funktionalität wieder ein.

2.5.2 Der Foreign Agent

Ein Foreign Agent muß für jeden unterstützten Mobilteilnehmer den aktuellen Zustand speichern; es gibt davon vier verschiedene:

1. Init: Der mobile Teilnehmer ist im Moment nicht beim Foreign Agent registriert.

2. Pending: Das mobile System hat zum ersten Mal eine Registrierungsanforderung an den Foreign Agent gesendet, der sie an den Home Agent weitergereicht hat. Der Foreign Agent wartet nun auf eine Antwort vom Home Agent.

3. Confirmed: Der Home Agent hat die Registrierung akzeptiert und eine Accept-Nachricht geschickt, die der Foreign Agent an den Mobilteilnehmer weitergeleitet hat.

4. Pending Rereg: Das mobile System hat eine periodische Registrierungsanforderung an den Foreign Agent gesendet, die dieser weiter an den Home Agent geleitet hat. Der Foreign Agent wartet auf eine Antwort vom Home Agent.

Die folgenden Eingabeereignisse können auftreten:

1. Reg(ok): Der Foreign Agent hat vom mobilen System eine Registrierungsanforderung erhalten, die der Foreign Agent akzeptiert und an den Home Agent weitergegeben hat.

2. Reg(n.ok): Der Foreign Agent hat die Registrierungsanforderung nicht akzeptiert und eine Deny-Nachricht an den mobilen Teilnehmer gesendet.

3. Accept: Der Home Agent hat die Registrierung akzeptiert und eine Accept-Nachricht zum Foreign Agent geschickt.

4. Deny: Der Home Agent hat die Registrierung abgelehnt und eine Deny-Nachricht zum Foreign Agent gesendet.

5. Timeout: Die Registrierung eines mobilen Teilnehmers beim Foreign Agent ist abgelaufen (vgl. Seite 15).

Abbildung 2.8 veranschaulicht die Zustandsübergänge.

Für eine erfolgreiche Registrierung ergibt sich der folgende Ablauf auf dem Foreign Agent: Der Foreign Agent erhält die erste Registrierungsanforderung und wechselt in den

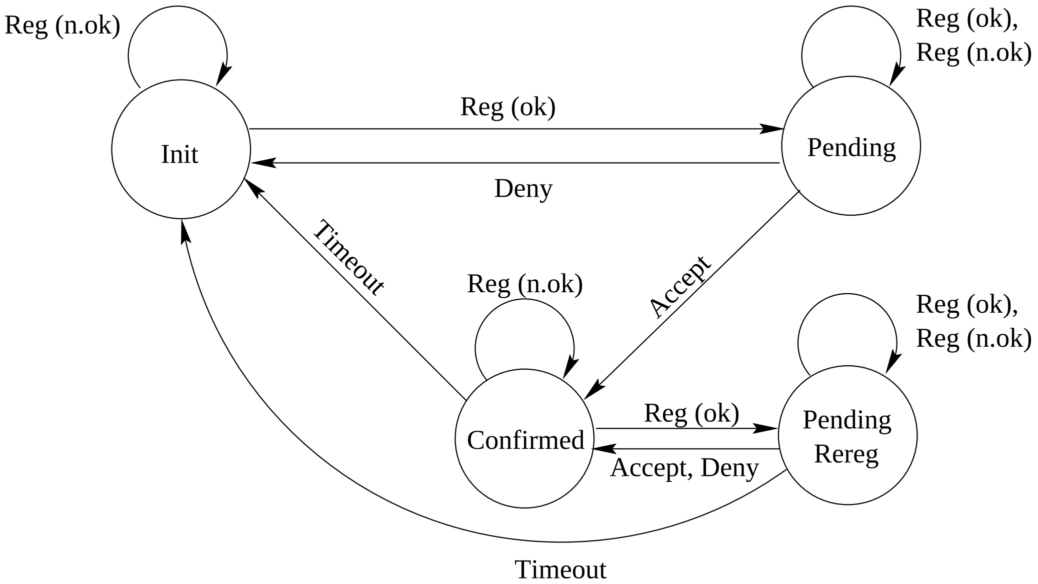

Abbildung 2.8: Zustandsautomat einer Registrierung für den Foreign Agent

„Pending"-Zustand, wenn er die Registrierung akzeptiert. Danach leitet er die Registrierungsanforderung zum Home Agent weiter, der eine Registrierungsantwort sendet. Enthält diese eine Annahme der Registrierung, geht der Foreign Agent in den „Confirmed"-Zustand über und leitet die Nachricht zum Mobilteilnehmer. Solange dieser nicht das Subnetz wechselt, sendet er periodische Registrierungsanforderungen, so daß der Foreign Agent zwischen dem „Pending Rereg"- und dem „Confirmed"-Zustand hin und her wechselt.

Änderungen beim Routing: Die lokale Unterstützung

Die einzige wesentliche Aktion, die ein Foreign Agent ausführen muß, ist die Einrichtung der *lokalen Unterstützung* für den mobilen Teilnehmer, wenn der Foreign Agent vom Zustand „Pending" in den „Confirmed"-Zustand wechselt. Darunter versteht man, daß er Pakete für den mobilen Teilnehmer durch die Einrichtung eines lokalen Eintrages in der Routingtabelle auf das lokale Netz aussendet und ggf. auch Pakete von diesem weiterleitet. Dementsprechend muß der Foreign Agent bei einem Timeout-Ereignis die lokale Unterstützung für den betroffenen mobilen Teilnehmer beenden, also die lokale Route wieder aus der Routingtabelle entfernen.

2.5.3 Der Home Agent

Der Home Agent muß wie der Foreign Agent auch für jeden unterstützten mobilen Teilnehmer einen eigenen Zustandsautomaten verwalten. Drei Zustände gibt es:

1. Init: Der Aufenthaltsort des mobilen Teilnehmers ist dem Home Agent nicht bekannt.

2. atHome: Der Mobilteilnehmer befindet sich im Heimatsubnetz und hat sich deregistriert.

3. atForeign: Das mobile System befindet sich in einem fremden Subnetz und hat sich korrekt registriert.

Eingabeereignisse sind:

1. Dereg(ok): Der Home Agent hat eine Deregistrierungsanforderung bekommen, die der Home Agent akzeptiert hat.

2. Dereg(n.ok): Der Home Agent hat eine Deregistrierungsanforderung abgelehnt.

3. Reg(ok): Eine Registrierungsanforderung ist beim Home Agent eingetroffen, die der Home Agent akzeptiert hat.

4. Reg(n.ok): Eine Registrierungsanforderung ist beim Home Agent eingetroffen, die der Home Agent abgelehnt hat.

5. Timeout: Der Registrierungstimer für einen mobilen Teilnehmer im fremden Subnetz ist abgelaufen.

Damit ergibt sich der in Abbildung 2.9 dargestellte Zustandsautomat:

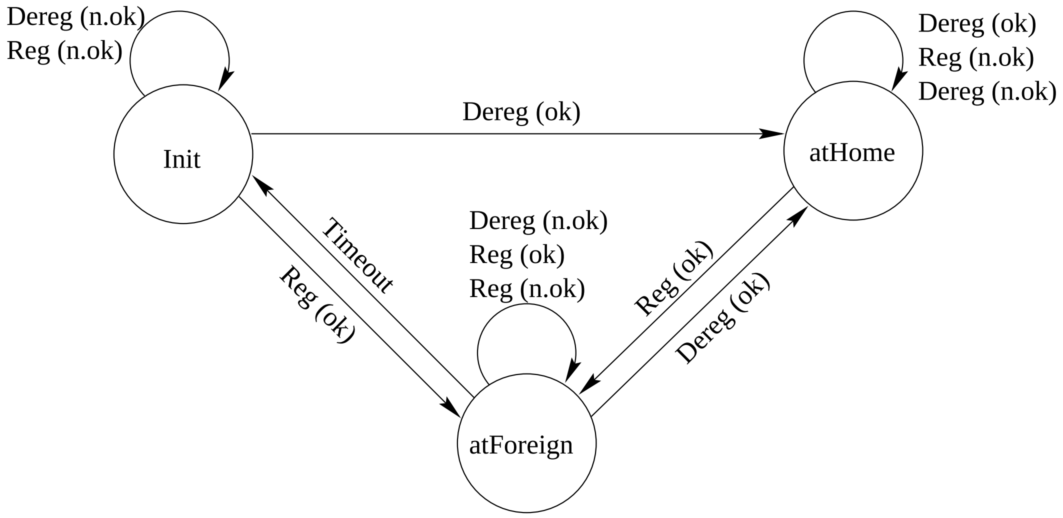

Abbildung 2.9: Zustandsautomat einer Registrierung für den Home Agent

Eine akzeptierte Registrierungsanforderung führt zu einem Übergang in den Zustand „atForeign“, eine akzeptierte Deregistrierungsanforderung zum Übergang in den „atHome“-Zustand. Abgelehnte Mobile IP Nachrichten führen aus Sicherheitsgründen grundsätzlich zu keiner Zustandsänderung (vgl. Abschnitt 2.4.4). Tritt im Zustand „atForeign“ ein Timeout auf, beendet der Home Agent die Unterstützung für den mobilen Teilnehmer.

Die Unterstützung des mobilen Systems durch den Home Agent

Wechselt der Zustand eines mobilen Systems auf dem Home Agent in den „atForeign"-Zustand, muß der Home Agent die folgenden Schritte ausführen, um dem mobilen Teilnehmer Unterstützung zu gewähren:

1. Einrichten eines Proxy-ARP [Ste94] Eintrages auf die IP-Adresse des mobilen Systems, damit der Home Agent für den Mobilteilnehmer bestimmte Pakete empfangen kann.

2. Aussenden einer Gratuitous-ARP [Ste94] Nachricht, damit alle Systeme im lokalen Netz den alten Eintrag für das mobile System im ARP-Cache löschen und Nachrichten zum Mobilteilnehmer an den Home Agent senden.

3. Einrichten eines IPIP-Tunnels zu der in der Registrierungsanforderung angegebenen Care-of Adresse.

4. Eintragen einer Route zum mobilen System in den eingerichteten Tunnel.

Findet ein Übergang in den Zustand „atHome" statt, löscht der Home Agent den Proxy-ARP Eintrag und teilt diese Änderung wiederum per Gratuitous-ARP allen lokalen Systemen mit. Danach löscht der Home Agent den Tunnel und die Route in den Tunnel.

2.6 Mobile IP und Multicast

Damit ein Mobilteilnehmer in einem fremden Subnetz Multicast-Daten empfangen kann, können zwei verschiedene Mechanismen angewendet werden:

1. Er empfängt Multicast-Daten von einem lokalen Multicast-Router.

2. Er bittet den Home Agent, Multicast-Daten durch den Tunnel vom Home Agent zur Care-of Adresse zu senden [AchBak96].

Die erste Möglichkeit ist die einfache Variante, weil dabei Mobile IP und Multicasting voneinander unabhängig bleiben. Dazu muß allerdings im fremden Subnetz ein Multicast-Router vorhanden sein. Ein weiterer Nachteil ist, daß der Mobilteilnehmer nach einem Subnetzwechsel unter Umständen keine Multicast-Daten mehr empfangen kann, weil der Wert des TTL-Feldes in den Multicast-Paketen zu klein ist.

Vorteile der zweiten Methode sind, daß dem mobilen Teilnehmer der Aufenthalt im fremden Subnetz transparent bleibt, er kann dieselben Dienste wie im Heimatsubnetz erhalten. Dadurch, daß die Multicast-Daten per Unicast über den Tunnel geleitet werden, ergibt sich auch kein Problem mit zu kleinen TTL-Werten. Ein Nachteil ist, daß der Home Agent gleichzeitig ein Multicast-Router sein muß. Desweiteren ist diese zweite Möglichkeit sehr viel komplexer als die erste Lösung. Außerdem versendet der Home Agent die Daten zum mobilen System durch den Tunnel per Unicast. Damit gehen die Vorteile des Multicasting (Einsparen von Bandbreite im Netzwerk) verloren.

Tabelle 2.3 faßt die Eigenschaften der beiden Alternativen nochmals zusammen.

Empfang von Multicast-Daten über ...	
einen lokalen Multicast-Router	den Home Agent
+ kein Mobile IP nötig – Multicast-Router im fremden Subnetz benötigt – TTL-Feld des IP-Paket kann Mobilität begrenzen	+ Transparenz der Mobilität für den mobilen Teilnehmer + kein Problem mit TTL-Werten – Home Agent muß Multicast-Router sein – komplexe bidirektionale Tunnel erforderlich

Tabelle 2.3: Vergleich der Alternativen zum Empfang von Multicast-Daten

2.7 Erweiterung zu Mobile IP: Route Optimization

Um das Problem des Dreiecksroutings zu umgehen, wird das Verfahren der *Route Optimization* vorgeschlagen [JohPer97] (siehe Abbildung 2.10).

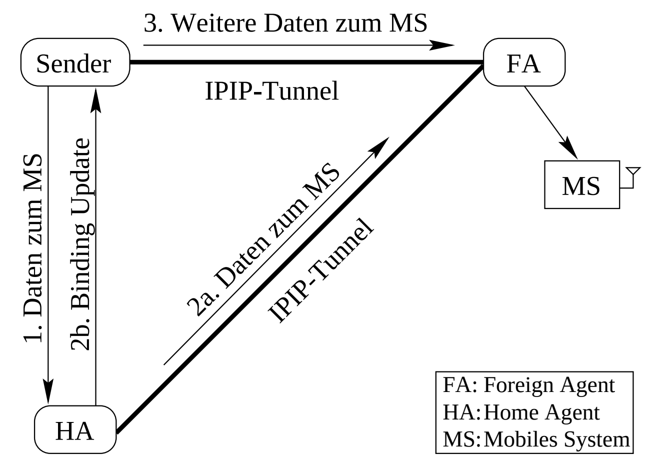

Abbildung 2.10: Route Optimization

Wenn von einem Sender Daten beim Home Agent (HA) ankommen (1.), leitet dieser die Daten wie in Mobile IP über einen Tunnel an den Mobilteilnehmer (MS) weiter (2a.). Zusätzlich informiert der Home Agent den Sender über die neue Care-of Adresse des mobilen Systems (mittels einer *Binding Update* Nachricht, 2b.), so daß der Sender folgende Daten für den mobilen Teilnehmer selbst zu diesem tunneln kann (3.). Diese Information hält der Sender in einem sog. *Binding Cache*, sie ist wie die Information in einem Mobility

Agent mit einer Lebensdauer behaftet.

Wechselt ein Mobilteilnehmer das Subnetz, gelangen Daten zum ihm weiterhin zum alten Foreign Agent. In dem Fall sendet der alte Foreign Agent eine Nachricht an den Home Agent, der eine Binding Update Nachricht mit der neuen Care-of Adresse des mobilen Systems an den Sender schickt.

Als zusätzliche Funktion der Route Optimization wird ein sog. *Smooth Handoff* unterstützt. Nach einem Subnetzwechsel kann der mobile Teilnehmer durch eine sog. *Previous Foreign Agent Notification Erweiterung* den neuen Foreign Agent über seinen alten Aufenthaltsort informieren. Dieser informiert den alten Foreign Agent über den Subnetzwechsel. Dazu sendet er im neuen Subnetz eine Binding Update Nachricht an den alten Foreign Agent mit der neuen Care-of Adresse des mobilen Systems. Dadurch kann der alte Foreign Agent Daten in das neue Subnetz weiterleiten, die von Sendern mit alten Einträgen im Binding Cache kommen. Außerdem kann der alte Foreign Agent Ressourcen freigeben, die der mobile Teilnehmer bei seinem Aufenthalt im alten Subnetz belegt hat, ohne auf den Ablauf der Registrierungstimer warten zu müssen.

2.8 Zusammenfassung

Die Entwickler von Mobile IP haben die in Abschnitt 2.2 angesprochenen Ziele zum großen Teil verwirklicht:

- Der mobile Teilnehmer ist über die Heimatadresse für alle Systeme aus dem Internet erreichbar.
- Änderungen am Internet erstrecken sich lediglich auf die Einrichtung von Mobility Agents.
- Mobile IP Nachrichten werden authentifiziert und mittels Replay Protection gegen unbefugte Wiederholungen geschützt.

Das letztgenannte Ziel, Anzahl und Größe der Signalisierung gering zu halten, ist nicht vollständig erreicht worden. Die Größe der Nachrichten ist zwar gering, aber das periodische Aussenden insbesondere der Agent Advertisements führt zu einem nicht zu vernachlässigenden Overhead.

Kapitel 3

Der indirekte Transportansatz

Dieses Kapitel gibt einen kurzen Überblick über die Funktion des indirekten Transportansatzes in Verbindung mit TCP/IP sowie die Gründe für seine Einführung. Zum besseren Verständnis sollte die grundsätzliche Funktionsweise von TCP bekannt sein, die z. B. von Stevens [Ste94] erläutert wird.

3.1 Motivation

Mobile IP sorgt dafür, daß ein mobiler Teilnehmer aus dem Internet erreichbar ist, auch wenn er sich nicht in seinem Heimatsubnetz befindet. Die Anbindung des mobilen Systems geschieht auf der Netzwerkschicht, wobei die Mobilität des Teilnehmers für darüber liegende Schichten, z. B. der Transportschicht, transparent bleibt. Sollen mittels TCP Daten zuverlässig zwischen einem stationären und einem mobilen Teilnehmer übertragen werden, ergeben sich Probleme durch die Staukontrolle von TCP [Ste97]. Der nächste Abschnitt motiviert zunächst die Notwendigkeit der Staukontrolle, danach folgt die Beschreibung der in TCP realisierten Staukontrolle. Abschließend erfolgt eine Beschreibung der Probleme einer Datenübertragung mittels TCP zu einem mobilen Teilnehmer.

Motivation für eine Staukontrolle

Erhält ein Zwischensystem mehr Pakete zum Weiterleiten als es verarbeiten kann, speichert es sie zunächst in einer Warteschlange. Das Zwischensystem muß Pakete verwerfen, wenn es weiterhin zuviele Pakete bekommt und der für die Warteschlange verfügbare Speicher erschöpft ist. Um eine solche *Überlastsituation* an dem Zwischensystem zu beheben, müssen die Sender, welche die Überlast verursachen, ihre Übertragungsrate absenken. Dann kann das Zwischensystem freiwerdenden Verarbeitungskapazitäten nutzen, um die Pakete in der Warteschlange abzuarbeiten und anschließend wieder in einen Betrieb ohne Überlast überzugehen.

Als erstes muß also ein sendendes System eine Überlastsituation im Netz erkennen können, um dann zweitens im Falle einer solchen Situation diese zu beheben, indem es die

Übertragungsrate absenkt. Beide Verfahren, Erkennung und Behebung einer Überlastsituation, werden in der sog. *Staukontrolle* zusammengefaßt.

Die Staukontrolle von TCP

Die Erkennung einer Überlastsituation durch die Staukontrolle von TCP erfolgt *implizit*, kommt also ohne zusätzliche Signalisierung zwischen dem überlasteten Zwischensystem und den sendenden Systemen aus. TCP vermutet immer dann eine Überlastsituation, wenn Paketverluste eintreten, d. h. wenn auf dem Sender die Bestätigungen für versendete Pakete ausbleiben.

Dieses einfache Erkennungsverfahren beachtet nicht, daß Paketverluste in drahtgebundenen Netzen nicht nur aufgrund von überlasteten Zwischensystemen, sondern auch durch Bitfehler entstehen können. In einem solchen Fall verwirft die Sicherungsschicht auf dem Empfänger das verfälschte Paket, so daß die Transportschicht das Paket nicht ausgeliefert bekommt. In den heutigen drahtgebundenen Netzwerken sind die Bitfehlerraten allerdings sehr niedrig, so daß Paketverluste aufgrund von Bitfehlern selten sind: Mehr als 99% aller Paketverluste treten aufgrund überlasteter Zwischensysteme auf.

Die Staukontrolle von TCP kann also nicht zwischen Paketverlusten aufgrund einer Überlastsituation oder wegen Bitfehlern unterscheiden und unternimmt fälschlicherweise auch im letzteren Fall eine Behebung der vermeintlichen Überlastsituation. Der Vorteil des Verfahrens, daß für die Erkennung einer Überlastsituation keine zusätzliche Signalisierung im Netzwerk notwendig ist, kompensiert aber den Nachteil dieser falschen Reaktion im Falle von selten auftretenden Bitfehlern.

Zur Behebung einer Überlastsituation im Netz reduziert TCP die Übertragungsrate auf dem Sender. Kommen wieder Bestätigungen für versendete Pakete beim Sender an, geht TCP davon aus, daß die Überlastsituation vorbei ist und hebt die Übertragungsrate in einer sog. „Slow-Start-Phase“ bzw. der darauf folgenden „Probing-Phase“ langsam wieder an, um nicht erneut eine Überlastsituation zu provozieren.

Problem: TCP über eine drahtlose Strecke

Die spezielle Charakteristik einer Funkübertragung bewirkt, daß Paketverluste nicht wie bei einer drahtgebundenen Übertragung hauptsächlich wegen einer Überlastung von Zwischensystemen auftreten. Erstens sind die Bitfehlerraten viel höher als in drahtgebundenen Netzen und damit nicht vernachlässigbar. Zweitens können auch Unterbrechungen der Funkverbindung durch Funkschatten oder einen Funkzellenwechsel des mobilen Teilnehmers auftreten.

Überträgt man Daten mit TCP über eine drahtlose Strecke, bewirken auch Paketverluste wegen Bitfehlern oder Verbindungsunterbrechungen fälschlicherweise eine Aktivierung der Staukontrolle von TCP. Insbesondere die Slow-Start- bzw. Probing-Phase führen zu Durchsatzeinbußen, weil Paketverluste bei einer funkbasierten Übertragung recht häufig sind und damit die durch das Übertragungsfenster der Flußkontrolle vorgegebene maximale Datenrate nur selten erreicht wird. Abbildung 3.1 zeigt eine mögliche Situation:

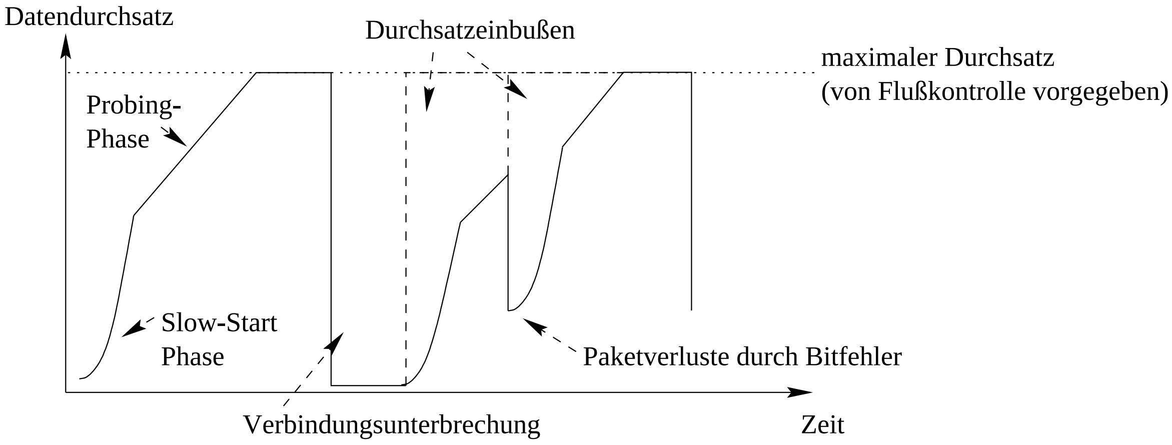

Abbildung 3.1: Datendurchsatz über eine drahtlose Strecke

Zu Beginn der Übertragung geht TCP auf dem Sender in die Slow-Start-Phase und anschließend in die Probing-Phase über, um die Übertragungskapazität der Zwischensysteme zu überprüfen. In diesem Fall gibt es keine Probleme und der Durchsatz erreicht den von der Flußkontrolle vorgegebenen Maximalwert. Durch eine Verbindungsunterbrechung (z. B. beim Handover) sinkt der Durchsatz auf Null, bei Wiederherstellung der Verbindung beginnt TCP erneut mit der Slow-Start- und Probing-Phase. Diese Lastreduktion ist nicht notwendig, weil keine Überlast im Netz vorliegt; eigentlich könnte TCP wieder mit dem maximalen Durchsatz senden. Dadurch kommt es zu den angegebenen Durchsatzeinbußen.

Den zweiten Einbruch bei der Übertragungsrate haben Bitfehler verursacht, so daß z. B. die Sicherungsschicht mehrere Pakete verworfen hat. Der Empfänger ist zwar noch zu erreichen, zeigt aber dem Sender an, daß Pakete verlorengegangen sind. Daraufhin drosselt TCP die Übertragungsrate. Anschließend beginnt wieder die Slow-Start- und Probing-Phase. Erneut sind die Durchsatzeinbußen unnötig, weil keine Stausituation vorhanden ist. TCP müßte lediglich die Ursache der Paketverluste kennen (Bitfehler), um dann keine Staukontrolle auszulösen. Stattdessen sollte es nur die fehlerhaften Pakete wiederholen und könnte weiter mit maximaler Übertragungsrate senden.

3.2 Lösung: Indirekte Transportverbindung

In der Literatur existieren verschiedene Vorschläge zur Beseitigung der beschriebenen Probleme. Sie lassen sich danach ordnen, auf welcher Schicht des ISO/OSI-Protokollstacks Veränderungen vorgenommen werden. Der hier vorgestellte *indirekte Transportansatz* beruht auf Änderungen in der Transportschicht. Aus organisatorischen Gründen ist jedoch eine Änderung des Transportschichtprotokolls TCP nicht im gesamten Internet durchführbar.

Deswegen schlagen Bakre und Badrinath [BakBad95] vor, eine Verbindung zwischen einem mobilen und einem stationären Teilnehmer in zwei Teile zu unterteilen: eine Verbindung für die drahtgebundene Strecke und eine zweite für die drahtlose Strecke. TCP verwaltet dabei unverändert die erstgenannte Verbindung. Das Transportprotokoll auf der drahtlosen Strecke kann aber speziell an die Probleme der funkbasierten Datenübertragung angepaßt werden. Die Koppelung der beiden Verbindungen geschieht auf einer Station nahe beim drahtlosen Link mittels eines *Transport Gateways*. Für diese Station ist die Basisstation vorgesehen, die den mobilen Teilnehmer gerade bedient.

Beim indirekten Transportansatz besteht eine Verbindung also nicht mehr Ende-zu-Ende zwischen zwei Systemen, sondern nur noch indirekt über das Transport Gateway. Abbildung 3.2 stellt die indirekte Transportverbindung graphisch dar:

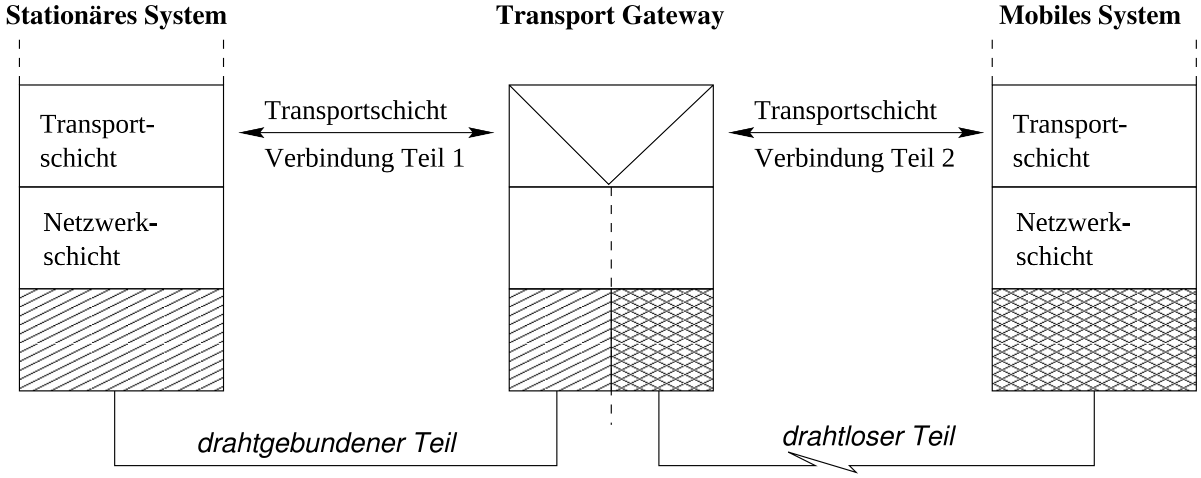

Abbildung 3.2: Mobilität mit einem Transport Gateway

Die Vorteile dieses indirekten Transportansatzes sind:

- Trennung der Fluß- und Staukontrolle auf der drahtgebundenen Strecke von der auf der drahtlosen.
- Fest angeschlossene Teilnehmer sind von keinen Änderungen betroffen.
- Beachtung der speziellen Charakteristik einer funkbasierten Übertragung: Dadurch daß das Transport Gateway räumlich nah am mobilen System ist, können bei Paketverlusten auf der drahtlosen Strecke schnelle lokale Übertragungswiederholungen zwischen dem Transport Gateway und dem Mobilteilnehmer stattfinden. Im Gegensatz zu einer Ende-zu-Ende Übertragungswiederholung spielen die Signallaufzeiten zwischen Sender und Empfänger eine untergeordnete Rolle.
- Dadurch daß die Mobilität nicht mehr transparent für die Transportschicht auf dem mobilen System ist, kann diese Probleme bei der Übertragung im Detail an eine Anwendung melden. Damit kann die Anwendung den Benutzer über die Art des Problems informieren, so daß dieser darauf reagieren kann, z. B. seinen Standort wechseln, wenn er sich in einem Funkschatten befindet.

3.2.1 Migration des Transport Gateway

Bewegt sich der mobile Teilnehmer, muß das Transport Gateway ebenfalls verlagert werden, damit es sich weiterhin räumlich nah am mobilen System befindet und schnelle lokale Übertragungswiederholungen vornehmen kann. Diesen Verlagerung nennt man *Migration.*

Bei einer Migration müssen sowohl die Sende- und Empfangspuffer als auch der aktuelle Zustand der Transportverbindung vom alten zum neuen Transport Gateway übertragen werden. Damit sich währenddessen keine Änderungen an den Puffern bzw. dem Zustand der Verbindung ergeben, schlagen Bakre und Badrinath [BakBad95] vor, daß während der Migration keine Daten fließen sollen. Es ergibt sich die sog. *Migrationspause.*

3.2.2 Delayed Migration

Das im vorherigen Abschnitt betrachtete Vorgehen bei einer Migration hat einen großen Nachteil: Jeder Funkzellenwechsel führt zu einer Migration und damit zu häufigen migrationsbedingten Unterbrechungen der Transportverbindung.

Abhilfe können die folgenden Vorschläge bringen [FieZit97, Bög96]:

1. Das Transport Gateway wird auf einem Router im dem Subnetz aufgesetzt, in dem sich der mobile Teilnehmer befindet. Dadurch ist eine Migration nur noch bei einem Subnetzwechsel, nicht bei jedem Funkzellenwechsel nötig.

2. Eine Migration findet mit Verzögerung statt, um die Migrationspause zu verkleinern. Dies nennt man eine sog. *Delayed Migration.* Außerdem können noch während der Migration Daten fließen, was die Migrationspause weiter reduziert.

Delayed Migration und Mobile IP

Verwendet man Mobile IP, um für ein mobiles System die Erreichbarkeit auf der Netzwerkschicht zu gewährleisten, bietet es sich an, in einem fremden Subnetz das Transport Gateway auf dem Foreign Agent zu plazieren.

Abbildung 3.3 zeigt den Datenfluß bei einer verzögerten Migration.

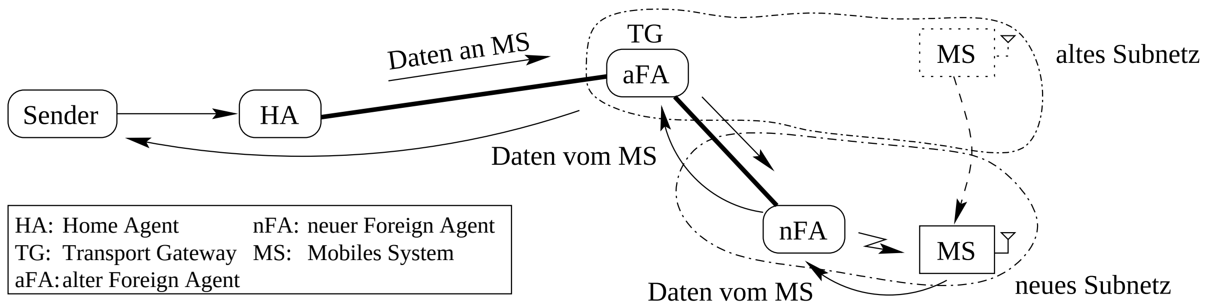

Abbildung 3.3: Indirekte Transportverbindung mit Delayed Migration

Wenn der Mobilteilnehmer (MS) das Subnetz wechselt, muß er bei einer verzögerten Migration zunächst auch die Mobile IP Registrierung beim Home Agent verzögern. Der neue Foreign Agent (nFA) meldet sich dazu nicht direkt beim Home Agent an, sondern sorgt dafür, daß der alte Foreign Agent (aFA) einen Tunnel zum neuen Foreign Agent eröffnet und alle Daten zum mobilen Teilnehmer an den neuen Foreign Agent weiterleitet. Damit kann das Transport Gateway zunächst auf dem alten Foreign Agent verbleiben, was z. B. sinnvoll ist, wenn der Mobilteilnehmer schnell zwischen zwei Subnetzen wechselt (oszilliert). Die Daten vom Sender zum mobilen Empfänger nehmen also den Weg Sender $\Rightarrow$ aFA $\Rightarrow$ nFA $\Rightarrow$ MS. Zu beachten ist, daß auch Daten vom mobilen System in das Festnetz den Weg über den alten Foreign Agent nehmen müssen, damit sie das Transport Gateway passieren. Deswegen ist die Einrichtung eines bidirektionalen Tunnels zwischen altem und neuen Foreign Agent notwendig.

Den Datenfluß nach Beendigung einer Migration zeigt Abbildung 3.4.

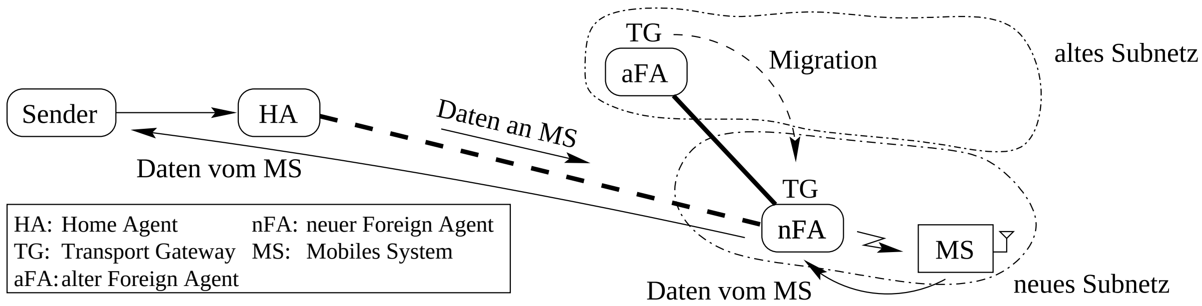

Abbildung 3.4: Indirekte Transportverbindung nach einer Migration

Anhand bestimmter Kriterien, die hier nicht weiter erläutert werden, entscheidet der neue Foreign Agent, wann die Migration beginnen soll. Nach Beendigung der Migration kann sich das mobile System direkt beim Home Agent registrieren. Danach ist der alte Foreign Agent nicht mehr an der Kommunikation beteiligt, Daten nehmen den Weg über den Tunnel vom Home Agent zum neuen Foreign Agent (in der Abbildung gestrichelt dargestellt).

3.3 Zusammenfassung

Die Verwendung von TCP bei einer drahtlosen Übertragung führt zu Problemen, die der indirekte Transportansatz durch die Einrichtung eines Transport Gateways lösen kann. Der Ansatz der Delayed Migration verbessert dieses Konzept hinsichtlich kürzerer Unterbrechungen bei einem Funkzellenwechsel.

Für die folgenden Kapitel ist von besonderer Bedeutung, daß alle Daten vom und zum mobilen System das Transport Gateway passieren müssen, damit dieses korrekt funktionieren kann.

Kapitel 4

Einführung in RSVP

Die folgenden Abschnitte dienen einer kurzen Einführung in die Prinzipien und die Funktionsweise von RSVP (Resource ReSerVation Protocol).

4.1 Motivation

Im heutigen IP-basierten Internet gibt es zwei Dienste für die Übertragung von Daten, die sich hinsichtlich der Dienstgüte unterscheiden: einen zuverlässigen Dienst (TCP) und einen unzuverlässigen (UDP).

Neue Anwendungen im Bereich Multimedia stellen aber zusätzlich zur Zuverlässigkeit weitere Anforderungen an eine Datenübertragung, z. B. bei der Übertragung von Audio- oder Videodaten. Dazu sind die Qualitätsparameter Jitter, Bandbreite und Verzögerung zu betrachten. Die vorhandene Internet-Architektur kann keine Dienstgüte im Bezug auf diese Qualitätsparameter garantieren.

Damit Multimedia-Anwendungen mit den genannten Dienstanforderungen das Internet nutzen können, müssen Ressourcen im Netzwerk reserviert werden. Dadurch kann das Netzwerk der Anwendung die geforderte Dienstgüte für eine Datenübertragung garantieren. Die Reservierung übernimmt ein sogenanntes *Ressourcenmanagement*, welches aus vier Teilen besteht [SchmZit95]:

1. Die Anforderungen einer Multimedia-Anwendung an eine Datenübertragung müssen zunächst genau definiert werden. Dazu spezifiziert ein *qualitätsorientiertes Dienstgütemodell* neue Qualitätsparameter wie Jitter, Bandbreite und Verzögerung, aber auch die bereits vorhandene Zuverlässigkeit. Diese können deterministisch oder statistisch garantiert werden. Im Falle einer deterministischen Garantie hält das Netzwerk die geforderten Qualitätsparameter in jedem Fall ein, bei einer statistischen Garantie nur mit einer gegebenen Wahrscheinlichkeit.

2. Die *Ressourcenverwaltung* übernimmt in jedem System, welches in die Datenübertragung involviert ist, die initiale Einrichtung und den abschließenden Abbau einer benötigten Ressourcenreservierung. Bei der Einrichtung prüft sie auch, ob sie die

geforderte Reservierung überhaupt gewähren kann (Zugangskontrolle). Außerdem verteilt sie während der Datenübertragung die lokalen Ressourcen an die einzelnen Reservierungen.

3. Die *Verkehrskontrolle* auf einem System ordnet alle eingehenden Daten zu einer oder auch keiner Reservierung zu, bearbeitet die Daten abhängig von dieser Klassifizierung und leitet sie weiter. Sie achtet dabei darauf, daß der Datenstrom die beim Aufbau der Reservierung vereinbarte Charakteristik hat.

4. Eine Anwendung muß zu Beginn einer Datenübertragung ihre Reservierungsanforderung allen betroffenen Systemen im Netzwerk mitteilen, damit das Ressourcenmanagement über die eintreffenden Daten informieren können. Diese Signalisierung übernimmt das *Reservierungsprotokoll*.

RSVP (Resource ReSerVation Protocol) stellt ein solches Reservierungsprotokoll dar.

4.1.1 Beschränkungen

Die Funktion von RSVP besteht **nicht** darin, die Ressourcen im Netzwerk zu reservieren. RSVP ist lediglich dafür zuständig, allen beteiligten Systemen im Netzwerk die zur Reservierung der Ressourcen notwendigen Daten zu signalisieren. Eine genaue Beschreibung dieser Daten gehört ebenfalls nicht zur RSVP-Spezifikation; RSVP befördert diese Daten opaque, d. h. ohne deren Informationsgehalt zu kennen.

Außerdem enthält RSVP kein eigenes Routingprotokoll, es benötigt aber eines, um seine Signalisierung zu realisieren. Die RSVP-Spezifikation [BraZha97] stellt nur generische Anforderungen an das verwendete Routingprotokoll, so daß auch andere Protokolle als das im Moment verwendete Internet Protokoll (IP) zum Einsatz kommen können.

Desweiteren erfolgen in der RSVP-Spezifikation keine detaillierten Betrachtungen zu Sicherheitsfragen [BraZha97, S. 25]. Diese sind Gegenstand zusätzlicher Spezifikationen; in dieser Arbeit werden sie nicht weiter betrachtet.

4.2 Entwurfsziele und Designprinzipien

Zwei Konzepte haben den Entwurf von RSVP maßgeblich beeinflußt: Gruppenkommunikation (Multicast) und Dienstgüte. Daraus entstanden die folgenden sieben Ziele für den Entwurf von RSVP [ZhaDee93, S. 9]:

1. Die Reservierung von Ressourcen für Multicast-Datenströme soll auf die speziellen Bedürfnisse für heterogene Empfänger zugeschnitten werden können.

2. RSVP soll die Dynamik in der Zusammensetzung einer Multicast-Gruppe angemessen behandeln.

3. RSVP soll Multicast-Reservierungen von verschiedenen Empfängern aggregieren, um Ressourcen im Netzwerk effizient zu nutzen.

4. Bei einer Gruppenkommunikation mit mehreren Sendern soll ein Empfänger frei wählen können, welchen Sender er über die reservierte Strecke empfangen möchte; eine Reservierung soll also bei der Einrichtung unabhängig von den die reservierte Strecke nutzenden Daten sein.

5. RSVP nutzt selbst ein Routingprotokoll für die Signalisierung. Sollte sich die Route zwischen Sender und Empfänger ändern, soll RSVP die Reservierung automatisch anpassen.

6. Der Protokolloverhead von RSVP soll gering sein, damit RSVP auch für Gruppenkommunikation mit vielen Teilnehmern möglich ist (Skalierbarkeit).

7. RSVP soll ein modulares Design besitzen, um es von den anderen Instanzen des Ressourcenmanagements möglichst unabhängig zu halten.

Die ersten vier Ziele beziehen sich also auf Aspekte der Gruppenkommunikation, das fünfte Ziel auf die Interaktion zwischen Routingprotokoll und RSVP. Ziel sechs und sieben sind eher allgemeingültig gehalten.

Um diese Ziele zu erreichen, wurden sechs Designprinzipien aufgestellt:

1. RSVP bietet nur unidirektionale Reservierungen an und spricht daher immer explizit von einem Sender und einem Empfänger. Der sog. *empfängerorientierte Ansatz* von RSVP beinhaltet, daß der Empfänger eine Reservierung vornimmt. Nur dieser weiß, welche Dienstgüte er von einem Sender erhalten will und auch verarbeiten kann, und ist damit besser als der Sender dazu in der Lage, eine Reservierung zu spezifizieren und zu initiieren (betrifft Ziel 1).

2. Ein Zwischensystem entscheidet nicht anhand eines Paketes, ob dieses Paket eine Dienstgüte erfährt, sondern anhand einer Spezifikation des Reservierenden, welche Pakete eine Reservierung nutzen dürfen. Damit kann der Empfänger eine Reservierung für Daten von verschiedenen Sendern verwenden (betrifft Ziel 4).

3. Um Ressourcen bei einer Gruppenkommunikation aggregieren und gleichzeitig den Anforderungen der verschiedenen Anwendungen gerecht werden zu können, muß RSVP verschiedene Reservierungsstile bereitstellen (betrifft Ziel 3).

4. Die Informationen, die Zwischensysteme über den Status einzelner Reservierungen halten müssen, sind mit einer Lebensdauer versehen und müssen periodisch erneuert werden. Dies kennzeichnet den sogenannten *Soft-State Ansatz* (siehe Abschnitt 4.4) (betrifft Ziele 2 und 5).

5. Der Protokolloverhead von RSVP im Fall der Gruppenkommunikation wird durch das Aggregieren der Signalisierungsnachrichten begrenzt: Das sog. *Merging*. Außerdem kann RSVP den Overhead durch die Lebensdauer einer Reservierung (siehe Designziel 4) beeinflussen, indem es diese Lebensdauer erhöht. Damit ist eine periodische Wiederholung der Reservierung weniger oft notwendig (betrifft Ziel 6).

6. RSVP bietet generische Schnittstellen für den Transport der Reservierungsdaten, zur Verkehrskontrolle und zum Routingprotokoll (betrifft Ziel 7).

Obwohl die Reservierungsstile und das Merging einen wesentlichen Teil von RSVP ausmachen, werden beide nicht näher beschrieben, weil sie für diese Arbeit nicht relevant sind.

Die folgenden Abschnitte stellen einige Funktionen von RSVP heraus, die für die weiteren Kapitel dieser Arbeit von Bedeutung sind. Eine vollständige Einführung in RSVP bieten Zhang et al. [ZhaDee93], detaillierte Einblicke gibt die RSVP-Spezifikation [BraZha97].

4.3 Protokollablauf und Terminologie

Dieser Abschnitt betrachtet den Protokollablauf von RSVP aus dem Blickwinkel des Routings, weil gerade diese Betrachtung für die Kombination mit Mobile IP in den folgenden Kapiteln relevant ist.

4.3.1 Allgemeines

RSVP kann von einer Punkt-zu-Punkt Kommunikation bis zu einer Multipeer Kommunikation mit mehreren Sendern und Empfängern alle Kommunikationsarten unterstützen. Eine solche Kommunikationsbeziehung zwischen einem oder mehreren Sendern und einem einzelnen oder auch einer Gruppe von Empfängern heißt allgemein *RSVP-Sitzung*. Dabei unterscheidet RSVP explizit zwischen Sender und Empfänger, der Datenfluß in einer RSVP-Sitzung ist also an die Richtung von den Sendern zu den Empfängern gebunden, die im folgenden *downstream* heißen soll. Die umgekehrte Richtung heißt dementsprechend *upstream*. Für die Reservierung einer bidirektionalen Datenübertragung sind zwei RSVP-Sitzungen mit entgegengesetzter Richtung nötig.

4.3.2 Der Protokollablauf im Überblick

RSVP benötigt für den grundsätzlichen Protokollablauf zunächst zwei Nachrichten: die *Path-Nachricht* und die *Resv-Nachricht*. Eine Resv-Nachricht enthält Informationen über die vom Empfänger initiierte Reservierung. Sie gelangt vom Empfänger upstream und bewirkt, daß in allen beteiligten Systemen der *RSVP-Dämon*, die Instanz von RSVP auf einem System, eine Reservierung vornimmt. RSVP sendet Path-Nachrichten downstream, damit jeder RSVP-Dämon einen sog. *Path State Block* einrichten kann. Dieser enthält Informationen für das Weiterleiten von Resv-Nachrichten upstream entlang des umgekehrten Pfades, den die Daten nehmen. Es müssen also erst Path-Nachrichten downstream versendet werden, damit anschließend anhand der Path State Blocks Resv-Nachrichten zum Sender gelangen können.

Beide Nachrichten sowie einige zusätzliche werden im folgenden im Detail beschrieben. Abbildung 4.1 zeigt das Aussenden der Path-Nachrichten für ein Multicast-Szenario mit einem Sender und mehreren Empfängern sowie die Reservierung eines einzelnen Empfängers.

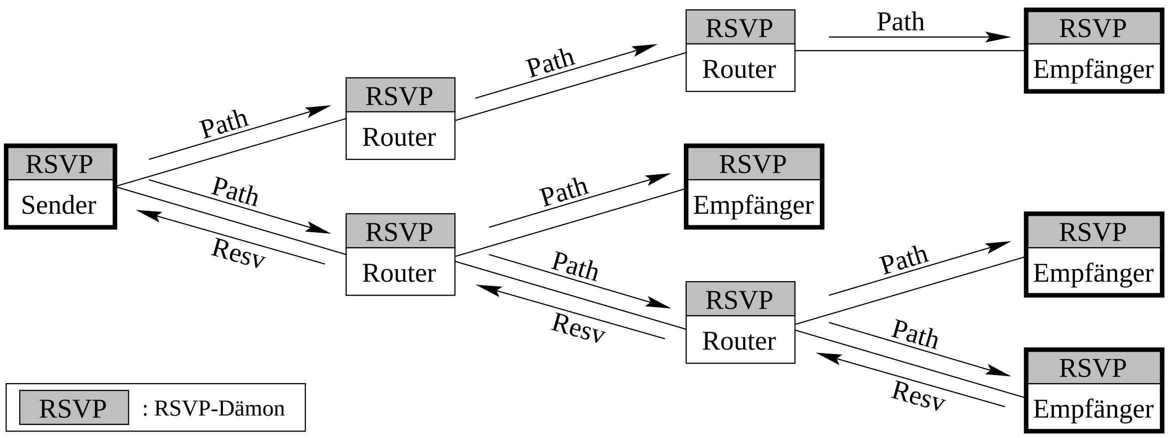

Abbildung 4.1: Protokollablauf in RSVP

4.3.3 Verwendete Nachrichten

Path-Nachricht Gemäß dem ersten Designziel initiiert ein Empfänger eine Reservierung. Da aber der vom Routingprotokoll gewählte Weg eines Paketes vom Empfänger zum Sender nicht notwendigerweise dem vom Sender zum Empfänger entspricht, schickt der Sender zunächst eine Path-Nachricht downstream. Jeder RSVP-Dämon auf den Zwischensystemen speichert die in der Path-Nachricht enthaltene Information in einem Path State Block. Anschließend leitet er sie mittels des Routingprotokolls downstream, so daß sie zum jeweils nächsten Zwischensystem, dem sog. *Next Hop*, gelangt.

Resv-Nachricht Eine upstream gesendete Resv-Nachricht muß exakt den umgekehrten Weg nehmen wie die Daten downstream. Das ist wichtig, damit Ressourcen in den Zwischensystemen reserviert werden, über die auch der Datenfluß erfolgt. Das IP-Standardrouting leitet eine Resv-Nachricht nicht auf diese geforderte Weise weiter. Sie kann einen anderen Weg nehmen als die Daten downstream. Damit wären dann Ressourcen in den falschen Zwischensystemen reserviert. Aus diesem Grund sendet ein RSVP-Dämon Resv-Nachrichten immer direkt zu dem System, von dem er die letzte Path-Nachricht erhalten hat. Dieses System ist der sog. *Previous Hop*. Resv-Nachrichten werden also *hop-by-hop* gesendet. Abbildung 4.2 gibt einen Überblick über die bisher eingeführten Begriffe.

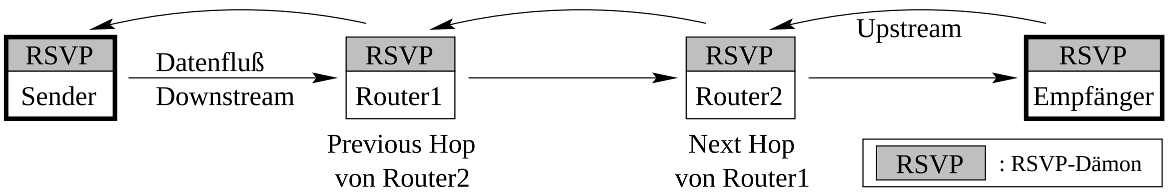

Abbildung 4.2: Terminologie in RSVP

Path-Nachrichten sind also in erster Linie dazu da, an die Zwischensysteme die Informationen zu verbreiten, die für das Senden der Resv-Nachrichten upstream notwendig sind. Sie tragen aber zusätzlich auch noch eine Beschreibung der Charakteristik des Datenstroms vom Sender, auf die diese Arbeit nicht weiter eingeht.

PathTear-Nachricht Wenn ein Sender die Datenübertragung beendet, schickt er eine *PathTear-Nachricht* downstream, die alle Systeme ohne Verzögerung bearbeiten und zum Next Hop weiterleiten müssen. Dadurch werden in jedem Zwischensystem die Path State Blocks und auch alle Reservierungen gelöscht.

ResvTear-Nachricht Möchte ein Empfänger seine Reservierung nicht mehr nutzen, sendet er eine *ResvTear-Nachricht* upstream, so daß die Zwischensysteme die reservierten Ressourcen wieder freigeben können. Hat der Empfänger als einziger eine Reservierung für einen Datenstrom reserviert, gelangt die ResvTear-Nachricht direkt bis zum Sender. Nutzen mehrere Empfänger gleichzeitig die Reservierung dieses Datenstroms, wird die ResvTear-Nachricht nur bis zu dem Punkt im Netzwerk propagiert, an dem die gemeinsame Nutzung der Ressourcen beginnt. Somit bleibt die Reservierung für die anderen Nutzer der Reservierung erhalten.

Fehlernachrichten Tritt auf einem System bei der Reservierung ein Fehler auf, sendet es eine *ResvErr-Nachricht* downstream, so daß der Empfänger Kenntnis von der mißlungenen Reservierung erhält. Analog dazu sendet ein System eine *PathErr-Nachricht* upstream zum Sender, wenn bei der Verarbeitung der Path-Nachricht ein Fehler aufgetreten ist.

4.3.4 Der Ablauf mit der Schnittstelle zur Ressourcenverwaltung

Der Ablauf einer Reservierung in Verbindung mit der Ressourcenverwaltung [BraZha97, S. 9] ist wie folgt: der RSVP-Dämon auf dem Empfänger bekommt von der Anwendung die Reservierungsanforderung. Zunächst muß er prüfen, ob es bereits einen Path State Block gibt, also schon einmal eine Path-Nachricht vom Sender angekommen ist. Ist die Reservierung aus der Sicht des RSVP-Dämon korrekt, gelangt sie zur Ressourcenverwaltung, die auf dem Empfänger lokale Ressourcen wie CPU-Zeit oder Pufferkapazitäten reserviert. Anschließend sendet der RSVP-Dämon eine Resv-Nachricht zum RSVP-Dämon auf dem Previous Hop. Dieser prüft ebenfalls, ob die Nachricht aus Sicht von RSVP korrekt ist und gibt die Reservierungsanforderung an die Ressourcenverwaltung. Diese muß nun wieder lokale Ressourcen reservieren, aber zusätzlich auch Bandbreite auf der Strecke zum Next Hop. Wie der Vorgang konkret abläuft, hängt von der verwendeten Übertragungstechnologie ab; z. B. ist auf Übertragungsmedien mit CSMA-CD (z. B. Ethernet) keine Reservierung von Bandbreite möglich. Abschließend gelangt die Resv-Nachricht weiter hop-by-hop zum Sender. Damit ist die gesamte Strecke vom Sender zum Empfänger reserviert, sofern die Reservierung auf allen beteiligten Zwischensystemen erfolgreich war.

4.4 Der Soft-State Ansatz

Die von den Path- bzw. Resv-Nachrichten an die Zwischensysteme ausgelieferten Informationen sind nur für eine bestimmte Lebensdauer gültig (Designprinzip 4). Im normalen Betrieb müssen diese periodisch wiederholt werden, damit die Informationen über den gesamten benötigten Zeitraum Gültigkeit besitzen. Tritt ein Fehler auf, z. B. ein Systemabsturz oder der Verlust der Netzwerkanbindung eines Systems, so daß die periodischen Wiederholungen ausbleiben, läuft auf den betroffenen Systemen der Timer für die Lebensdauer ab. Die belegten Ressourcen können dann freigegeben werden, so daß keine dauerhafte Belegung von Ressourcen auftreten kann. Die Tatsache, daß Zustandsinformationen nur eine begrenzte Zeit gültig sind, führt zu der Bezeichnung „Soft-State“.

4.4.1 Wiederholungen mit variabler Periode

Bei der Etablierung einer Reservierung gelangt eine vom Sender generierte Path-Nachricht unmittelbar und ohne Verzögerung von einem Zwischensystem zum nächsten, damit ein schneller Aufbau der Path State Blocks in den Zwischensystemen möglich ist. Analog werden Resv-Nachrichten für eine schnelle Reservierung ohne Verzögerung hop-by-hop upstream gesendet.

Die periodischen Wiederholungen der Path- bzw. Resv-Nachrichten geschehen aber unabhängig voneinander zwischen je zwei Systemen. Die Dauer einer Periode jeder einzelnen Wiederholung variiert zufallsgesteuert, damit nicht alle Zwischensysteme gleichzeitig Wiederholungen generieren und so eine kurzzeitige hohe Last im Netzwerk auslösen. Im Unterschied zur Etablierung einer Strecke ist ein schnelles Weiterleiten nicht notwendig, weil die Reservierung bereits vorhanden ist. Die Wiederholung verfolgt nur den Zweck, ein Ablaufen des Lebensdauer-Timers zu verhindern.

Das führt zu dem folgenden Verhalten: Die periodische Wiederholung z. B. einer Path-Nachricht kann zeitlich gesehen zuerst zwischen dem dritten und vierten Router, dann zwischen dem ersten und zweiten, danach zwischen dem sechsten und siebten usw. ausgeführt werden.

4.4.2 Etablierung einer Reservierung auf einer neuen Route

Das periodische Aussenden der Path-Nachrichten hat noch einen weiteren Effekt: Eine Änderung in der Route vom Sender zum Empfänger kann automatisch erkannt werden. Abbildung 4.3 zeigt eine mögliche Situation:

Die Route vom Sender zum Empfänger wechselt von Sender–A–B–C–D–Empfänger zu Sender–A–F–G–D–Empfänger. Sobald Router A eine neue periodische Path-Nachricht sendet, gelangt sie über die neue Route zum Router F. Dieser hat noch keinen Path State Block und sendet die Nachricht daher unmittelbar an den Router G weiter, für den dasselbe gilt. Der Router D hingegen hat bereits einen Path State Block, allerdings mit einem anderen Previous Hop, so daß er die Path-Nachricht nicht weiterleitet. Für alle Reservierungen, die zu derselben RSVP-Sitzung wie die Path-Nachricht gehören, sendet er Resv-Nachrichten

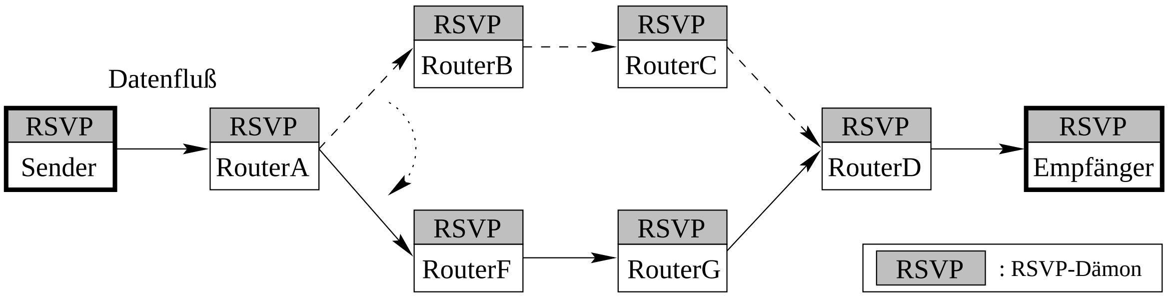

Abbildung 4.3: Routenänderung mit RSVP

upstream, d. h. zu Router G. Sowohl der Router G als auch der Router F richten bei Erhalt dieser Nachricht eine neue Reservierung ein und senden sie unverzüglich weiter. Damit ist die gesamte Strecke wieder neu reserviert, ohne daß der Sender oder der Empfänger in die Signalisierung involviert war.

Löschen der Reservierung der alten Strecke Im gezeigten Beispiel läuft auf dem Router B der Timer für die Lebensdauer z. B. der Path-Nachricht ab, weil er keine periodischen Path-Nachrichten vom Router A mehr erhält. Daraufhin löscht er den betroffenen Path State Block sowie dazugehörige Reservierungen, generiert eine PathTear-Nachricht und sendet sie downstream, um eine zügige Freigabe der Path State Blocks zu gewährleisten. Ohne diese PathTear-Nachricht würden zwar die Timer auf allen Systemen der alten, nicht mehr benutzten Route ebenfalls ablaufen und damit ein Löschen der Daten verursachen. Das gewählte Verfahren ist aber schneller. Router D ignoriert diese PathTear-Nachricht, weil sie von einem anderen Previous Hop kommt als die letzte Path-Nachricht.

Empfang zweier Path-Nachrichten Solange die Strecken B–C–D und F–G–D parallel bestehen, die alte Strecke also noch nicht gelöscht wurde, erhält der Router D Path-Nachrichten von zwei Routern: Router C und Router G. Da er nicht weiß, welche von beiden Strecken momentan aktiv ist (im gezeigten Beispiel kann das Routingprotokoll nach kurzer Zeit die Path-Nachrichten wieder entlang der alten Route senden), und welche demnächst einen Timeout bekommt, muß er Resv-Nachrichten an beide Router versenden. Damit existieren parallele Ressourcenreservierungen auf der alten und der neuen Strecke.

4.4.3 Verlust von Path- bzw. Resv-Nachrichten

Da RSVP-Nachrichten sich auf ein unzuverlässiges Übertragungsprotokoll stützen, muß der Timer für die Lebensdauer so gewählt sein, daß der Verlust einer Nachricht nicht sofort zum Löschen der Reservierung oder des Path State Blocks führt. Deswegen soll die Periode für die Wiederholung der Nachrichten K-mal kleiner sein als der Startwert des Lebensdauer-Timers. Dann können $K - 1$ aufeinanderfolgende Nachrichten verloren gehen, ohne die

Reservierung bzw. den Path State Block zu löschen. Die RSVP-Spezifikation [BraZha97] schlägt $K = 3$ vor.

4.5 Local Repair

Die in Abschnitt 4.4.2 gezeigte Etablierung einer Reservierung nach einer Routenänderung hat den Nachteil, daß bei einem derzeitigen Periodenwert von 20 bis 40 Sekunden erst nach maximal dieser Zeit die neue Route wieder vollständig reserviert ist. Als Alternative zu dieser Methode gibt es die Methode des *Local Repair* [BraZha97, S. 48]. Dabei sendet das Routingprotokoll ein Signal an RSVP, wenn eine Änderung einer Route eingetreten ist, damit RSVP eine neue Path-Nachricht downstream entlang der neuen Route senden kann. Die Path-Nachricht wird dabei verzögert gesendet, damit das Routingprotokoll die Routenänderung mit Sicherheit beendet hat. Die RSVP-Spezifikation empfiehlt eine Verzögerung von zwei Sekunden.

4.6 RSVP-Sitzung über IPIP-Tunnel

Befindet sich auf der Strecke vom Sender zum Empfänger ein IPIP-Tunnel, entsteht eine in Abbildung 4.4 dargestellte Situation:

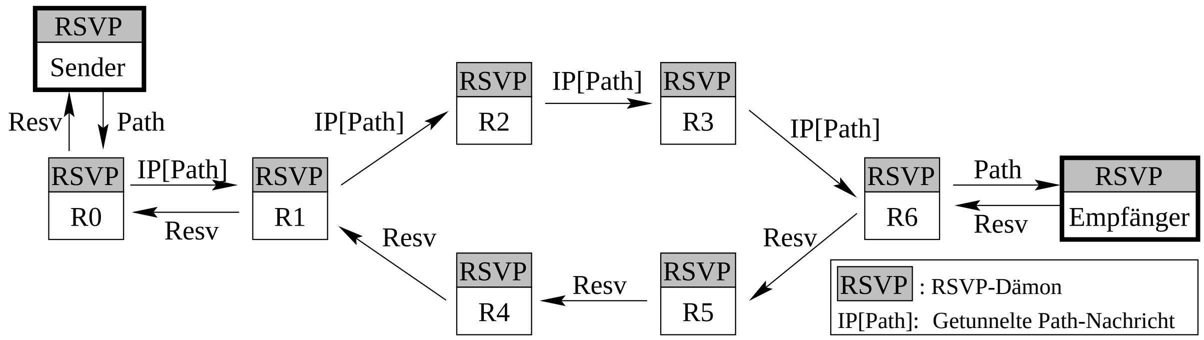

Abbildung 4.4: Problem: RSVP-Sitzung mit einem IPIP-Tunnel

Zwischen den Routern R0 und R6 besteht ein IPIP-Tunnel. R0 kapselt Path-Nachrichten vom Sender in ein weiteres IP-Paket ein (symbolisiert durch IP[Path]) und sendet dieses Paket zum Tunnelendpunkt R6, welcher die ursprüngliche Path-Nachricht auspackt und zum Empfänger leitet. Die Router R1, R2 und R3 konnten dabei keine Path State Blocks einrichten, weil sie die in einem IPIP-Paket eingekapselte Path-Nachricht nicht als solche erkennen konnten.

Eine Resv-Nachricht vom Empfänger gelangt hop-by-hop zum Router R6. Da die Router R1, R2 und R3 die Path-Nachricht nicht erkennen konnten, hat der Router R6 den Router R0 als Previous Hop und sendet die Resv-Nachricht an diesen, den er (vermeintlich) für seinen direkten Vorgänger hält. Per IP-Standardrouting gelangt die Resv-Nachricht auf einem möglicherweise anderen Weg zum Router R0, der dann eine Reservierung zu seinem vermeintlichen Next Hop, dem Router R6 vornehmen müßte. Dies ist nicht möglich, weil es sich bei der Strecke R0–R6 um mehrere Hops handelt. Damit ist die Strecke von R0 nach R6 nicht korrekt reserviert.

Abbildung 4.5 zeigt eine Lösung des Problems nach Krawczyk et al. [KraTer97].

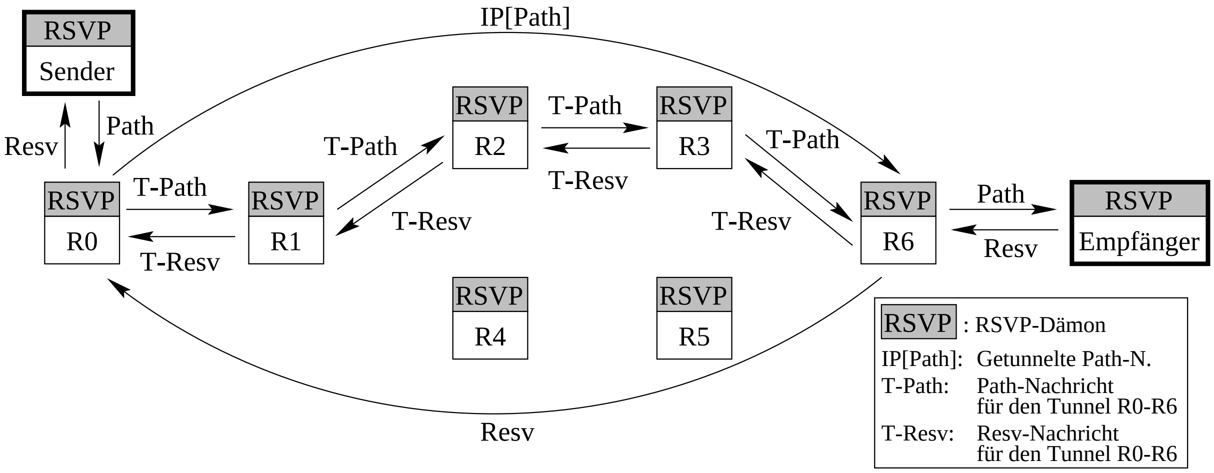

Abbildung 4.5: Spezielle RSVP-Tunnelsitzung

Wenn der Router R0 eine Path-Nachricht einkapselt, muß er eine sogenannte *RSVP-Tunnelsitzung* zwischen dem Tunnelanfangs- und endpunkt, d. h. R0 und R6 initiieren, also eine Path-Nachricht zum Tunnelendpunkt senden (in der Abbildung mit T-Path gekennzeichnet). Diese bewirkt die Einrichtung der Path State Blocks auf den Routern R1, R2 und R3. Gelangt eine Resv-Nachricht zum Tunnelendpunkt R6, muß dieser zunächst eine Reservierung der RSVP-Tunnelsitzung vornehmen, indem er eine Resv-Nachricht zum Tunnelanfang (T-Resv) schickt. Nachdem eine Bestätigung über den Erfolg der Reservierung vom Tunnelanfang zum -endpunkt gelangt ist, kann der Router R6 die ursprüngliche Resv-Nachricht zum Router R0 senden. Da die Reservierung zwischen R0 und R6 bereits vorhanden ist, kann die Resv-Nachricht auf einem beliebigen Weg zu R0 geleitet werden.

4.7 Zusammenfassung

Die Einführung von RSVP erfordert Änderungen an den bestehenden Netzwerkstrukturen in großem Umfang; für eine vollständige Signalisierung müssen alle Zwischensysteme RSVP-Unterstützung gewährleisten. Außerdem ist für eine schnelle Anpassung einer Reservierung an eine Routenänderung eine Verzahnung zwischen RSVP und dem darunterliegenden Routingprotokoll notwendig. Schließlich muß eine Reservierung von IPIP-Tunneln separat betrachtet werden.

Kapitel 5

Detaillierte Problemanalyse

Diese Diplomarbeit behandelt die Bereitstellung einer Ressourcenreservierung mit RSVP für Mobilteilnehmer, die mit Hilfe von Mobile IP an das Internet angeschlossen sind. Zusätzlich soll für zuverlässige Transportverbindungen der indirekte Transportansatz mit unterstützt werden. Dieses Kapitel analysiert die sich daraus ergebenden Probleme, stellt mögliche Lösungen dar und bewertet diese.

Zunächst erfolgt eine allgemeine Betrachtung von Mobile IP unter dem Aspekt der Dienstgüte. Danach werden Probleme bei der Kombination von Mobile IP mit dem indirekten Transportansatz dargestellt. Es folgt anschließend eine Analyse von RSVP unter dem allgemeinen Aspekt der Mobilität. Abschließend wird die Kombination von Mobile IP und RSVP behandelt.

Vorbetrachtung: Der co-located Betrieb von Mobile IP

Der co-located Betrieb von Mobile IP hat unter dem Blickwinkel von Dienstgüte zusätzlich zu den in Abschnitt 2.3.5 genannten Nachteilen einige weitere:

- Das Einkapseln der Daten beim Tunneln belegt nicht nur wie bei der Verwendung eines Foreign Agents auf der drahtgebundenen Strecke zusätzliche Bandbreite, sondern auch auf dem drahtlosen Link.

  Der Overhead beträgt 20 Bytes für den zusätzlichen IP-Header. Bei einer Paketlänge von 1500 Bytes gehen etwa 1%, bei 600 Bytes etwa 3% der Bandbreite für diesen Overhead verloren. Im Falle von Anwendungen mit extrem kurzen Paketen (etwa telnet) können auch deutlich höhere Werte erreicht werden. Zusätzlich kann noch durch das Einkapseln der Daten eine Fragmentierung des IPIP-Paketes notwendig sein. Fan et al. [FanHen98] stellen eine weitergehende Betrachtung des durch Mobile IP erzeugten Overheads an.

- Das in Abschnitt 5.1.5 vorgestellte Forwarding Protokoll ist nicht realisierbar, weil nach einem Subnetzwechsel des Mobilteilnehmers kein Tunnelendpunkt mehr existiert.

Desweiteren ist ein Transport Gateway aus dem indirekten Transportansatz nur schwer in diese Betriebsart von Mobile IP zu integrieren:

1. Es stellt sich die Frage nach der Plazierung des Transport Gateways auch im fremden Subnetz (vgl. Abschnitt 5.2.1).

2. Selbst wenn es einen Platz gäbe, bliebe das Problem, daß Pakete zum mobilen System getunnelt und erst dort ausgepackt werden. Das System, welches das Transport Gateway realisiert, müßte also alle eingehenden Pakete auf getunnelte Pakete untersuchen. Enthält ein getunneltes Paket ein TCP-Paket für einen mobilen Teilnehmer mit einer bestehenden indirekten Transportverbindung, muß das Transport Gateway dieses Paket bearbeiten. Sonst leitet das System dieses Paket gemäß seiner Routingfunktionalität weiter. Diese Tests wären sehr aufwendig und würden das Weiterleiten von Paketen auf dem System verzögern.

Wegen dieser Nachteile wird im folgenden die Annahme gemacht, daß ein Foreign Agent vorhanden ist, wenn sich ein mobiler Teilnehmer in einem fremden Subnetz befindet. Eine weitere Betrachtung des co-located Betriebes erfolgt nicht.

5.1 Mobile IP und Dienstgüte

Schließt man ein mobiles System mittels Mobile IP an das Internet an, ergeben sich für die Übermittlung von Daten mit einer bestimmten Dienstgüte Probleme, die in Mobile IP inhärent vorhanden sind. Eine Analyse dieser Probleme führt dieser Abschnitt durch. Probleme, die sich aus der Kombination von Mobile IP und RSVP ergeben, werden separat im Abschnitt 5.4 betrachtet.

5.1.1 Dreiecksrouting

Das Dreiecksrouting in Mobile IP führt ggf. dazu, daß der Weg vom Sender zum mobilen Teilnehmer über den Home Agent wesentlich länger ist als die direkte Verbindung zwischen beiden (eine Betrachtung des Overheads erfolgt bei Fan et al. [FanHen98]). Dadurch können Daten zum mobilen System eine höhere Verzögerung als Daten von diesem erfahren. In Verbindung mit einer Ressourcenreservierung führt das Dreiecksrouting außerdem dazu, daß wegen des Umwegs über den Home Agent mehr Ressourcen als notwendig reserviert werden müssen. Der Ansatz der Route Optimization [JohPer97] kann dieses Problem beheben, weswegen diese Arbeit nicht weiter darauf eingeht.

5.1.2 Schnelles Agent Discovery Verfahren

Beim Agent Discovery existieren zwei Probleme im Bezug auf die Übertragung mit Dienstgüte behafteter Daten:

1. Das regelmäßige Aussenden von Agent Advertisements mit einer Periode p ($p > 1s$ [Per96, S. 19]) führt zur Reduzierung der für Nutzdaten verfügbaren Bandbreite auf dem Funkkanal.

   Dabei beträgt die Größe einer Agent Advertisement circa 70 Bytes: 20 Bytes für die ICMP-Nachricht mit der Mobility Agent Advertisement Erweiterung plus die Länge des IP-Headers von 20 Bytes plus die Nachrichtenkopflänge des Sicherungsschichtprotokolls, z. B. 28 Bytes bei Ethernet. Da Agent Advertisements mittels IP Multicast versendet werden, geht für jeden Mobility Agent im Subnetz nur maximal 70 bps der Bandbreite einer Funkzelle bei einer Periode p von einer Sekunde verloren. Somit ist dieses Problem auch im Falle einer drahtlosen Verbindung mit niedriger Bandbreite (etwa GSM mit 9.600 bps) nicht von Bedeutung.

2. Für die Erkennung eines Subnetzwechsels in Mobile IP werden zwei Algorithmen vorgeschlagen (vgl. Seite 12). In beiden Fällen muß das mobile System jeweils mindestens auf eine neue Agent Advertisement warten, bis es einen Subnetzwechsel erkennen kann. Da Agent Advertisements periodisch mit der Periode p gesendet werden, vergeht bis zu eine Periode p ($p > 1s$), bis das mobile System nach einem Subnetzwechsel die erste Agent Advertisement erhält. Erst dann kann es den Wechsel des Subnetzes mittels Mobile IP initiieren. Während dieser Zeit ist es nicht in der Lage, Daten zu empfangen oder zu senden. Für zeitkritische Daten, die eine geringe Verzögerung benötigen (z. B. Audiodaten), ist die Dauer der Unterbrechung von bis zu einer Sekunde zu lang.

Um das zweite Problem zu verringern, könnte man die Periode p kleiner wählen, z. B. auf 10 ms. Dann beträgt allerdings die durch die Agent Advertisements belegte Bandbreite bereits ungefähr 7.000 bps, mehr als 70% der in GSM derzeit verfügbaren Bandbreite. Das ist somit keine praktikable Lösung.

Lösungsvorschlag

Die hier vorgestellte Lösung ist eine Kombination aus zwei bereits in der Mobile IP Spezifikation [Per96] angesprochenen Mechanismen: Der Signalisierung eines Funkzellenwechsels durch die Sicherungsschicht und der Verwendung von Agent Solicitation. Es ergibt sich das sog. *schnelle Agent Discovery Verfahren.*

Bei einem Funkzellenwechsel sendet die Sicherungsschicht auf dem mobilen System, die das Umschalten zu einer anderen Basisstation ausgelöst hat, ein Signal an Mobile IP, daß sich der mobile Teilnehmer in einer neuen Funkzelle befindet. Mobile IP sendet daraufhin eine Agent Solicitation in das lokale Netz, um anhand der als Antwort gesendeten Agent Advertisement entscheiden zu können, ob ein Subnetzwechsel oder nur ein Funkzellenwechsel innerhalb desselben Subnetzes stattgefunden hat. Im ersten Fall kann das mobile System auch die Entscheidung treffen, ob es sich im Heimatsubnetz oder in einem fremden Subnetz befindet und welche Mobility Agents zur Verfügung stehen (vgl. Abschnitt 2.4.2). Abbildung 5.1 zeigt den Kommunikationsablauf zwischen den einzelnen Instanzen und Protokollschichten.

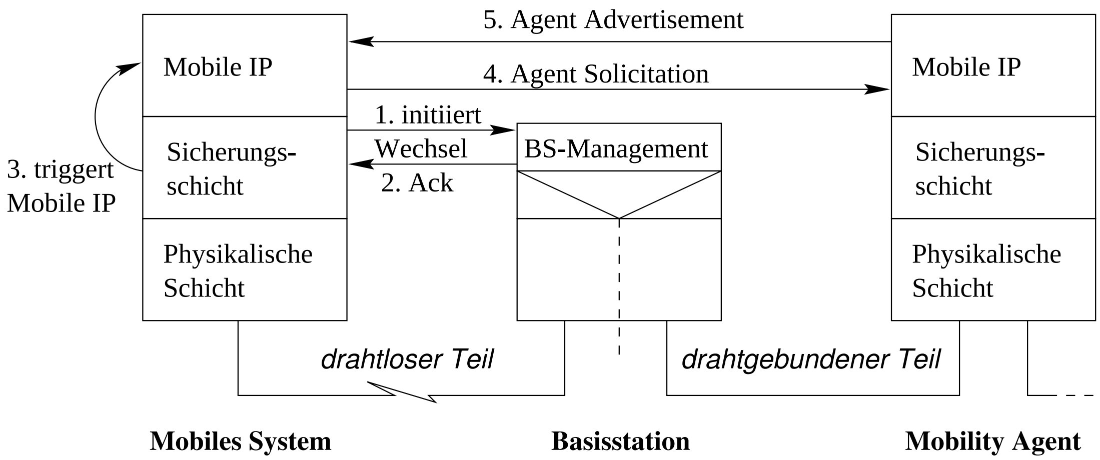

Abbildung 5.1: Schnelles Agent Discovery Verfahren

Bewertung des schnellen Agent Discovery Verfahrens

Dieses Verfahren hat die folgenden Vorteile:

1. Die Sicherungsschicht überwacht ständig die Verbindungsqualität auf dem drahtlosen Link und führt einen Funkzellenwechsel durch, sobald die Verbindungsqualität zu einer benachbarten Zelle besser ist als die in der momentan genutzten Funkzelle. Da ein Funkzellenwechsel eine notwendige Bedingung für einen Subnetzwechsel ist (wenn auch nicht hinreichend, nicht jeder Funkzellenwechsel ist auch ein Subnetzwechsel), reicht es aus, nur bei jedem Funkzellenwechsel zu überprüfen, ob auch ein Subnetzwechsel vorliegt. Es ist nicht notwendig, dies periodisch zu tun, sofern die Sicherungsschicht Mobile IP bei einem Funkzellenwechsel benachrichtigt. Damit ist die im ersten Problem genannte Belegung der Bandbreite durch Agent Advertisements auf das absolut notwendige Maß reduziert (eine Agent Solicitations ($\sim$ 50 Bytes) + eine Agent Advertisement ($\sim$ 70 Bytes) $\approx$ 120 Bytes pro Funkzellenwechsel).

2. Da die Sicherungsschicht einen Funkzellenwechsel auslöst, ist es auf jeden Fall die schnellste Vorgehensweise, wenn diese Schicht die Information über einen Wechsel direkt an Mobile IP weitergibt. Es ist insbesondere auch schneller, als wenn sich Mobile IP diese Information selbst über periodische Agent Advertisements beschafft. Damit ist auch das zweite Problem gelöst.

Ein Nachteil ist, daß ohne periodische Agent Advertisements ein Mobilteilnehmer den Ausfall seines Mobility Agents nicht erkennen kann. Dazu gibt es zwei Lösungsmöglichkeiten: Als erstes könnte das Home Agent Redundancy Protocol (HARP) [ChaBin97] verwendet werden, welches den Ausfall eines Home Agents behandelt. Dort übernimmt ein anderer Mobility Agent die Rolle des ausgefallenen. Man müßte HARP dann aber auch auf Foreign Agents anwenden. Bei der zweiten Lösung könnten die Mobility Agents zusätzlich zu dem in diesem Abschnitt vorgestellten Verfahren die Agent Advertisements periodisch aussenden. Die Periode sollte aber so gewählt werden, daß sich nicht wieder der oben angesprochene Nachteil der Belegung von Bandbreite ergibt. Im folgenden wird die Ausfallproblematik nicht weiter betrachtet.

Ein weiterer Nachteil entsteht, wenn es mehrere Mobility Agents in einem Subnetz gibt: Dann erhält das mobile System nach Versenden einer Agent Solicitation eine Antwort von jedem Mobility Agent. Da die Agent Solicitation einer ICMP Router Solicitation entspricht, kann das mobile System zusätzlich auch von im Subnetz vorhandenen Routern eine ICMP Router Advertisements erhalten, die es aber wegen der fehlenden Mobility Agent Advertisement Erweiterung ignoriert. In beiden Fällen wird geringfügig mehr Bandbreite benötigt, pro Agent Advertisement etwa 70 Bytes, für eine Router Advertisement etwa 60 Bytes. Im allgemeinen ist die Anzahl der Mobility Agents sowie der Router in einem Subnetz und damit die zusätzlich benötigte Bandbreite aber klein, so daß dieser Nachteil vernachlässigt werden kann.

Schließlich kann noch ein Nachteil hinsichtlich der Belegung von Bandbreite entstehen: Befinden sich sehr viele, häufig wechselnde Mobilteilnehmer in einem Subnetz, so daß sich im Durchschnitt zwei oder mehr Funkzellenwechsel pro Sekunde ergeben, belegt das schnelle Agent Discovery Verfahren mehr Bandbreite als das periodische Aussenden der Agent Advertisements. Man kann das allerdings begrenzen, indem die Mobility Agents Antworten auf Agent Solicitations nicht an eine Multicast-Adresse senden, sondern an die Unicast Adresse des mobilen Teilnehmers. Bei entsprechender Funktionalität der Basisstationen (vgl. Abschnitt 5.3.5) gelangt die Agent Advertisement per Unicast nur in die Funkzelle, in der sich der Mobilteilnehmer befindet, der die Agent Solicitation ausgesendet hat. Damit wird nur Bandbreite in dieser Funkzelle sowie auf dem drahtgebundenen Teil des lokalen Netzes belegt, welcher aber i. a. über eine größere Bandbreite als der drahtlose Teil verfügt. Das Problem bleibt dann nur noch erhalten, wenn sich viele mobile Teilnehmer in einer Funkzelle mit häufigen Funkzellenwechseln aufhalten. In diesem Fall ergibt sich aber allein schon wegen der großen Anzahl der Mobilteilnehmer ein Problem hinsichtlich der Bandbreite in der Funkzelle. Daher soll dieses Szenario nicht weiter verfolgt werden.

Unzuverlässigkeit der Übertragung

Sowohl Agent Solicitations als auch Agent Advertisements werden mittels UDP versendet, so daß Verluste dieser Nachrichten auftreten können. Das mobile System muß also nach dem Absenden einer Agent Solicitation einen Timer starten, damit es bei einem Ablauf des Timers eine Übertragungswiederholung anstoßen kann. Um das schnelle Agent Advertisement Verfahren robust zu gestalten, sendet das mobile System initial zwei Agent Solicitations. Damit entsteht durch den Verlust einer Agent Solicitations keine Zeitverzögerung, die benötigte Bandbreite erhöht sich aber leicht auf 170 Bytes pro Funkzellenwechsel. Erhält es dann immer noch keine Antwort, muß es weitere Agent Solicitations schicken. Um den Funkkanal und die eigene Energieversorgung nicht unnötig zu belasten, sollte das mobile System die Übertragung der Agent Solicitations begrenzen. Dazu verwendet es einen sog. exponentiellen Backoff Timer, bei dem der Abstand zwischen zwei aufeinanderfolgenden Nachrichten exponentiell mit der Anzahl der versendeten Nachrichten wächst. Dies ist insbesondere dann wichtig, wenn das mobile System selbst keinen Kontakt zu einer Basisstation z. B. wegen eines Funkschattens bekommen kann, aber mit der Übertragung der Agent Solicitations andere Mobilteilnehmer an der Funkübertragung hindert.

Zusammenfassung

Tabelle 5.1 bewertet nochmals die Eigenschaften des schnellen Agent Discovery Verfahrens:

Vorteile	Nachteile
+ Geringer Bandbreitenbedarf von 170 Bytes bei weniger als einem Funkzellenwechsel pro Sekunde, wenn eine Agent Solicitation nicht mehrere Agent bzw. Router Advertisements als Antwort bewirkt und wenn keine Verluste auftreten. + Geringer Zeitbedarf zum Erkennen eines Subnetzwechsels, wenn keine Verluste von Nachrichten auftreten.	– Keine Erkennung eines Ausfalls des Mobility Agents.

Tabelle 5.1: Bewertung des schnellen Agent Discovery Verfahrens

5.1.3 Explizites Beenden der lokalen Unterstützung

Wechselt ein mobiler Teilnehmer von einem fremden Subnetz in ein anderes Subnetz, erhält der Foreign Agent im alten Subnetz keine Information über den Wechsel. Da dieser weiterhin die lokale Unterstützung für das mobile System aufrecht erhält, kann er den mobilen Teilnehmer nicht mehr erreichen. Ist er gleichzeitig auch noch Router in dem Subnetz, kann das gesamte Subnetz das mobile System nicht erreichen, weil er für diesen bestimmte Daten weiterhin in das lokale Netz anstelle ins Heimatsubnetz leitet. Erst wenn der Registrierungstimer abläuft und der alte Foreign Agent die lokale Unterstützung beendet, kann er und möglicherweise das von ihm versorgte Subnetz den mobilen Teilnehmer über den Home Agent wieder erreichen.

Lösung: Die Mobile IP-Ende Nachricht

Um dieses Problem zu beheben, muß der alte Foreign Agent explizit über einen Subnetzwechsel des Mobilteilnehmers informiert werden, so daß er die lokale Unterstützung für das mobile System beenden kann. Diese Information erhält er mittels einer sog. *Mobile IP-Ende Nachricht.*

Grundsätzlich kommen zwei Instanzen für das Senden dieser Nachricht in Frage: der Home Agent und das mobile System, denn beide kennen sowohl den alten als auch den neuen Foreign Agent.

1. Der Home Agent benachrichtigt den alten Foreign Agent.

   Diese Variante hat die folgenden Vorteile:

   - Diese zusätzliche Signalisierung läuft über den drahtgebundenen Teil des Netzwerks.
   - Dem mobilen System bleibt diese Meldung verborgen, es sind damit keine Änderungen am Mobile IP auf dem mobilen System nötig.
   - Der Home Agent kann die Mobile IP-Ende Nachricht zeitgleich mit der Accept-Nachricht absenden.

2. Das mobile System benachrichtigt den alten Foreign Agent.

   In dieser Variante kann das mobile System die Mobile IP-Ende Nachricht erst absenden, wenn es vom Home Agent die Accept-Nachricht erhalten hat. Damit wird die Mobile IP-Ende Nachricht geringfügig verzögert. Außerdem belegt die Mobile IP-Ende Nachricht zusätzliche Bandbreite auf der drahtlosen Strecke.

Beide Varianten sind in etwa gleichwertig, die Belegung von Bandbreite auf der drahtlosen Strecke gibt allerdings unter dem Gesichtspunkt der Dienstgüte den Ausschlag, weswegen als Lösung des Problems der Home Agent die Mobile IP-Ende Nachricht zum alten Foreign Agent schickt. Abbildung 5.2 gibt noch einmal einen Überblick. Dabei entsprechen die einzelnen Schritte der Registrierung denen aus der Abbildung 2.5.

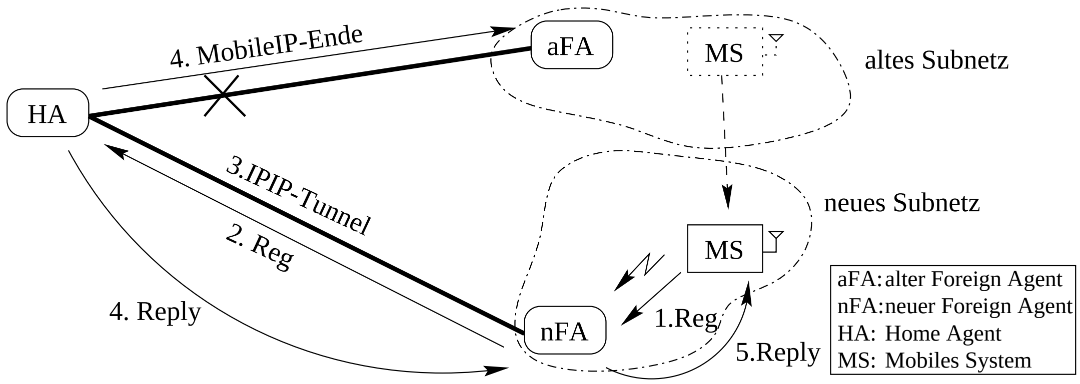

Abbildung 5.2: Benachrichtigung des alten Foreign Agents nach einem Subnetzwechsel

Im Falle der Route Optimization hat das Versenden einer Binding Update Nachricht an den alten Foreign Agent beim Smooth Handoff denselben Effekt wie das Versenden einer Mobile IP-Ende Nachricht.

Unzuverlässigkeit der Übertragung

Mobile IP-Ende Nachrichten werden mittels UDP verschickt. Dadurch ist ein Verlust oder eine Verdoppelung der Mobile IP-Ende Nachricht möglich:

Der Verlust einer Mobile IP-Ende Nachricht entspricht exakt dem bisherigen Vorgehen in Mobile IP, den alten Foreign Agent nicht über einen Subnetzwechsel zu informieren und hat keine weiteren Konsequenzen außer den zu Beginn dieses Abschnittes angesprochenen Nachteilen. Verdoppelte Mobile IP-Ende Nachrichten ignoriert der alte Foreign Agent, weil er die lokale Unterstützung bereits beendet hat. Damit führt die Versendung der Mobile IP-Ende Nachricht mittels UDP zu keinen Problemen.

Sicherheit

Ein Problem stellt aber der Mißbrauch der Mobile IP-Ende Nachricht durch Unbefugte dar. Diese kann zwar nicht wie z. B. die Registrierungsanforderung zu einer Umleitung von Daten mißbraucht werden, wohl aber für die Unterbrechung des von Mobile IP für ein mobiles System zur Verfügung gestellten Dienstes.

Da nur der Home Agent Mobile IP-Ende Nachrichten aussendet, kann eine Authentifizierung zwischen Home Agent und altem Foreign Agent Abhilfe schaffen. Dieses soll aber in dieser Arbeit nicht näher betrachtet werden. Eine ausführliche Diskussion dazu erfolgt im Verfahren der Route Optimization [JohPer97] am Beispiel der Binding Update Nachricht.

5.1.4 Plazierung der Agenten im Subnetz

Ein weiterer Faktor, der die Dienstgüte der zu einem Mobilteilnehmer gesendeten Daten beeinflussen kann, ist die Plazierung der Mobility Agents im Subnetz. Dabei lassen sich zwei Fälle unterscheiden:

1. Ein Mobility Agent wird auf einem Router plaziert.
2. Ein Mobility Agent wird auf einem separaten System plaziert, welches kein Router ist.

Ein Nachteil der ersten Variante ist (möglicherweise) eine hohe Belastung des Routers, weil er zusätzlich zu seinen Routing-Aufgaben noch die Aufgaben eines Mobility Agents und evtl. auch noch die des Transport Gateways übernehmen muß (siehe Abschnitt 5.2.1). Dadurch können Probleme hinsichtlich des Qualitätsparameters Verzögerung entstehen. Außerdem ist ein so zentralisiertes System auch fehleranfälliger.

Ein Nachteil der zweiten Variante ist das doppelte Versenden aller Daten auf dem Heimatsubnetz, wenn sich der Mobilteilnehmer nicht dort befindet. Dann gelangen die Daten für diesen mobilen Teilnehmer vom Router zum Home Agent und vom Home Agent wieder zum Router, sofern sich der Sender der Daten außerhalb des Heimatsubnetzes befindet. Zusätzlich werden die Daten dann noch zweimal über das fremde Subnetz geleitet: einmal vom Router zum Foreign Agent und dann von diesem zum mobilen Teilnehmer. Dies belegt Bandbreite auf der drahtgebundenen Strecke, welche aber in größerem Umfang zur

Verfügung steht als Bandbreite auf dem drahtlosen Teil. Außerdem erfahren die Nutzdaten eine zusätzliche Verzögerung, weil mehr Router in das Weiterleiten der Daten verwickelt sind als bei der ersten Variante. Tabelle 5.2 stellt nochmals die Vor- und Nachteile der beiden Varianten gegenüber.

Mobility Agent auf einem Router	Mobility Agent nicht auf einem Router
+ Daten laufen nicht doppelt über das Subnetz – ggf. hohe Belastung des Routers – Fehleranfälligkeit	+ geringere Ausfallwahrscheinlichkeit, weil Aufgaben verteilt sind – Belegung von Bandbreite, dadurch daß Daten zweimal durch das Subnetz laufen – größere Verzögerung durch mehr involvierte Router

Tabelle 5.2: Die beiden Varianten zur Plazierung der Mobility Agents

Es lassen sich keine endgültigen Aussagen treffen, welche der beiden Varianten optimaler hinsichtlich Dienstgüte ist. Die Plazierung eines Mobility Agents hängt von der konkreten Situation eines einzelnen Subnetzes ab, z. B. von der Belastung des Routers oder auch von der Art der gewährten Dienstgüte (garantierte Qualitätsparameter vs. statistische).

5.1.5 Analyse eines Weitverkehrsszenario: Fast-Forwarding

In einem Weitverkehrsszenario, d. h. bei einer großen Entfernung zwischen Heimatsubnetz und fremden Subnetz, treten die folgenden Probleme auf, wenn Daten an einen Mobilteilnehmer im fremden Subnetz gesendet werden sollen:

1. Wechselt der mobile Teilnehmer das Subnetz, sind alle Daten, die sich schon auf dem Weg in das alte Subnetz innerhalb des IPIP-Tunnels befinden, unzustellbar.

2. Der Mobilteilnehmer ist erst wieder zu erreichen, wenn eine Registrierungsanforderung beim Home Agent angekommen ist. Erst dann kann der Home Agent wieder Daten an den aktuellen Aufenthaltsort des mobilen Teilnehmers weiterleiten. Die Zeit, in der das mobile System nicht erreichbar ist (die sog. *Mobile IP Handover-Zeit*), beträgt also mindestens die Signallaufzeit vom Mobilteilnehmer zum Home Agent. Dazu kommen aber auch noch die Verarbeitungs- und Pufferzeiten in den beteiligten Zwischensystemen. Auf dem mobilen System beträgt die Dauer der Unterbrechung mindestens die doppelte Signallaufzeit: Die Registrierungsanforderung benötigt die einfache Signallaufzeit, um zum Home Agent zu gelangen; dann dauert es noch einmal solange, bis die ersten Daten vom Home Agent eintreffen.

Das folgende Beispiel verdeutlicht diese Aussagen anhand von konkreten Werten.

Beispiel für ein Weitverkehrsszenario

Das Heimatsubnetz eines mobilen Teilnehmers befinde sich an der Ostküste der U.S.A., sein aktueller Aufenthaltsort sei an der Westküste. Damit ergibt sich eine Entfernung von etwa 5.000 km zwischen dem Heimatsubnetz und dem fremden Subnetz. Der mobile Teilnehmer sei über ein drahtloses LAN mit 2 Mbps an das Internet angeschlossen. Da sich die Signale mit Lichtgeschwindigkeit ($c = 200.000\frac{km}{s}$) fortpflanzen, ergibt sich eine Signallaufzeit von $\frac{5.000\,km}{200.000\,\frac{km}{s}} = 25\,\text{ms}$. Die Pfadkapazität beträgt in diesem Beispiel:

$$2.000.000\,\frac{\text{Bits}}{\text{s}} \times 25\,\text{ms} = 50.000\,\text{Bits} \approx 6.000\,\text{Byte}$$

Es gehen also bis zu 6.000 Bytes bei jedem Subnetzwechsel verloren, wenn der stationäre Sender Daten kontinuierlich zum mobilen Teilnehmer überträgt.

Die Laufzeit einer Registrierungsanforderung vom mobilen System zum Home Agent läßt sich nicht fest bestimmen, weil die Anzahl der Zwischensysteme und die Verarbeitungszeit in diesen nicht bekannt ist. Die Laufzeit beträgt aber mindestens die 25 ms Signallaufzeit. Die Unterbrechung auf dem mobilen System beträgt mindestens 50 ms.

Beide Probleme lassen sich durch das *Fast-Forwarding Protokoll* beheben.

Das Fast-Forwarding Protokoll

Abbildung 5.3 zeigt den Datenfluß, wenn das Fast-Forwarding Protokoll zum Einsatz kommt. Meldet sich ein Mobilteilnehmer in einem neuen fremden Subnetz beim neuen

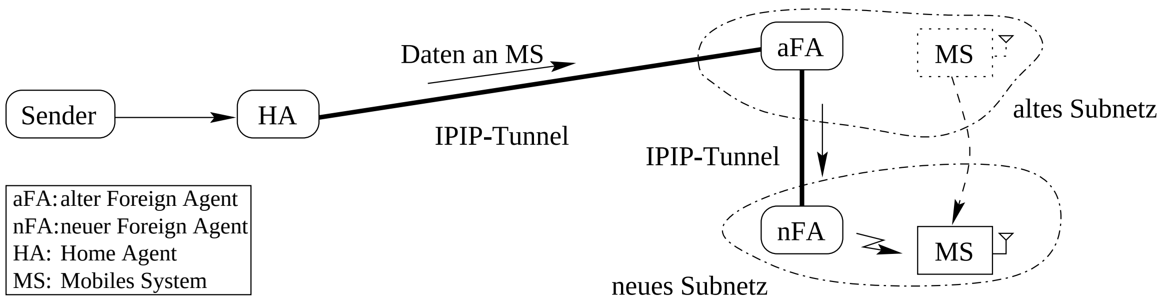

Abbildung 5.3: Datenfluß vom Home Agent zum mobilen System mit Fast-Forwarding

Foreign Agent (nFA) an, sendet er mit der Registrierungsanforderung die Adresse des alten Foreign Agent (aFA). Dadurch ist der neue Foreign Agent in der Lage, den alten über den Subnetzwechsel zu informieren. Dieser beendet daraufhin seine lokale Unterstützung für den mobilen Teilnehmer und leitet stattdessen alle Daten für diesen in einen IPIP-Tunnel an den neuen Foreign Agent weiter. Somit ist der Mobilteilnehmer wieder über die Strecke HA–aFA–nFA erreichbar. Dabei meldet sich der neue Foreign Agent nicht mehr direkt beim Home Agent an.

Bewertung des Fast-Forwarding Protokolls

Es ergeben sich zwei Vorteile, wenn man das Fast-Forwarding Protokoll einsetzt:

- Da die Strecke HA–aFA auch nach dem Wechsel des mobilen Teilnehmers zum neuen Foreign Agent weiter in Benutzung ist, gibt es aufgrund von Pfadkapazitäten keine Datenverluste. Daten zum mobilen System kann der alte Foreign Agent weiterleiten, sobald die Signalisierung zwischen dem alten und dem neuen Foreign Agent abgeschlossen ist.

- Die MobileIP Handover-Zeit verringert sich deutlich auf die Zeit, die für die Signalisierung zwischen dem mobilen System und dem neuen Foreign Agent und anschließend zwischen dem neuen und dem alten Foreign Agent benötigt wird. Diese ist in einem Weitverkehrsszenario deutlich geringer als die Zeit für die Signalisierung zwischen dem Home Agent und dem mobilen Teilnehmer, weil der alte Foreign Agent sich räumlich in der Nähe des neuen Foreign Agents befindet.

  Ist das nicht der Fall, kann man davon ausgehen, daß nicht ein Wechsel von einer Funkzelle in eine benachbarte den Subnetzwechsel ausgelöst hat, sondern daß z. B. das mobile System ausgeschaltet und in einem anderen Subnetz wieder eingeschaltet wurde. Dann ist aber in keinem Falle eine kurze MobileIP Handover-Zeit möglich.

Der Nachteil dieses Protokolls liegt darin, daß durch das Fast-Forwarding ein Router zusätzlich (der alte Foreign Agent) in das Weiterleiten der Daten zum Mobilteilnehmer verwickelt ist. Dieser muß die eingehenden getunnelten Pakete auspacken, weil er der Tunnelendpunkt ist, und anschließend wieder einpacken, weil er zugleich auch Tunnelanfang des Tunnels zum neuen Foreign Agent ist. Dadurch ergibt sich eine weitere Verzögerung der Daten zum Mobilteilnehmer. Insbesondere wenn das Fast-Forwarding mehrfach hintereinander angewendet wird, kommt bei jedem Subnetzwechsel ein weiterer Mobility Agent auf der Strecke HA–MS dazu, es bildet sich eine sog. *Forwardingkette* (siehe Abbildung 5.4).

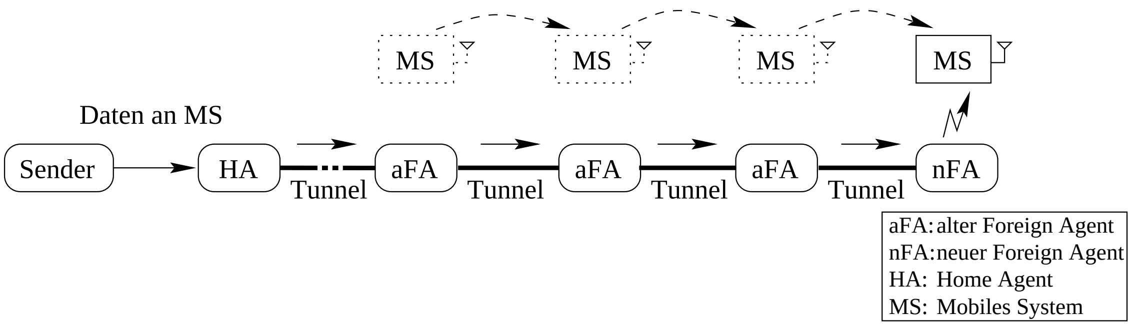

Abbildung 5.4: Die Forwardingkette

Ab einem gewissen Zeitpunkt ist es effektiver, daß bei einem erneuten Wechsel des Subnetzes der neue Foreign Agent direkt mit dem Home Agent Kontakt aufnimmt, anstelle die Forwardingkette weiter zu verlängern (vgl. Abschnitt 6.1.2). Die Bestimmung dieses Zeitpunktes ist nicht Gegenstand dieser Arbeit.

Tabelle 5.3 faßt die Eigenschaften des Fast-Forwarding Protokolls zusammen.

Vorteile	Nachteile
+ Keine Verluste durch Pfadkapazitäten beim Subnetzwechsel + Kürzere Mobile IP Handover-Zeiten (abhängig von der Entfernung zwischen Heimatsubnetz und dem fremden Subnetz)	– höhere Verzögerung der Daten wegen einer größeren Anzahl in das Forwarding der Daten involvierter Router

Tabelle 5.3: Bewertung des Fast-Forwardings

Vergleich: Fast-Forwarding und Route Optimization

Auch im Falle der Route Optimization wird eine Benachrichtigung des alten durch den neuen Foreign Agent vorgeschlagen, um Daten, die sich noch auf dem Weg vom Home Agent zum alten Foreign Agent befinden, an den Mobilteilnehmer ausliefern zu können. Neu am Fast-Forwarding Protokoll ist, daß dieses Weiterleiten nicht temporär sondern dauerhaft ist: Die Route Optimization sieht das Weiterleiten nur solange vor, bis der Sender der Daten die Binding Update Nachricht mit dem neuen Aufenthaltsort des mobilen Teilnehmers erhalten hat. Beim Fast-Forwarding Protokoll hingegen erhalten weder der Home Agent noch (bei einer Kombination mit der Route Optimization) der Sender Kenntnis über einen Subnetzwechsel.

5.1.6 Fazit

Probleme bei der Kombination von Mobile IP mit Daten, die eine bestimmte Dienstgüte erfahren sollen, ergeben sich durch große Unterbrechungszeiten beim Handover eines Mobilteilnehmers. Diese lassen sich durch ein schnelles Agent Discovery Verfahren und das Fast-Forwarding Protokoll verringern. Damit der Mobilteilnehmer nach einem Subnetzwechsel auch vom alten Foreign Agent aus noch erreichbar ist, sollte dieser mittels einer Mobile IP-Ende Nachricht über den Subnetzwechsel informiert werden.

5.2 Mobile IP und der indirekte Transportansatz

Dieser Abschnitt betrachtet Probleme, die sich im Falle einer Kombination von Mobile IP mit dem indirekten Transportansatz (vgl. Kapitel 3) ergeben.

5.2.1 Plazierung des Transport Gateways

Um den indirekten Transportansatz in Mobile IP zu integrieren, stellt sich zunächst die Frage, auf welches System das Transport Gateway aufgesetzt werden soll. Die wichtigste Bedingung dafür ist, daß alle Daten zum und vom Mobilteilnehmer das Transport Gateway passieren müssen. Es lassen sich zwei Fälle unterscheiden:

1. Der Mobilteilnehmer befindet sich in einem fremden Subnetz:

   In diesem Fall ist die Entscheidung einfach: Da alle Daten für das mobile System den Foreign Agent passieren, kann das Transport Gateway auf dem Foreign Agent plaziert werden (vgl. Abschnitt 3.2.2). Für den Fall, daß der mobile Teilnehmer sendet, muß er den Foreign Agent als Default-Router auswählen, so daß auch alle gesendeten Daten den Foreign Agent und damit das Transport Gateway passieren. Allerdings sollte der Foreign Agent keine ICMP-Redirect Nachrichten an das mobile System schicken [Per96, S. 57], falls der Foreign Agent selbst kein regulärer Router im fremden Subnetz ist.

2. Das mobile System ist im Heimatsubnetz:

   Im Heimatsubnetz soll das mobile System ohne jegliche Mobile IP Unterstützung funktionieren, als wäre es ein fest installiertes System [Per96, S. 56]. Dadurch gibt es aber kein System, auf welches das Transport Gateway mit der oben angeführten Bedingung aufgesetzt werden könnte. Abbildung 5.5 zeigt eine mögliche Situation in einem lokalen Netz mit mehreren Routern: Es können Daten sowohl über den Router R1 als auch über den Router R2 zum Mobilteilnehmer gelangen.

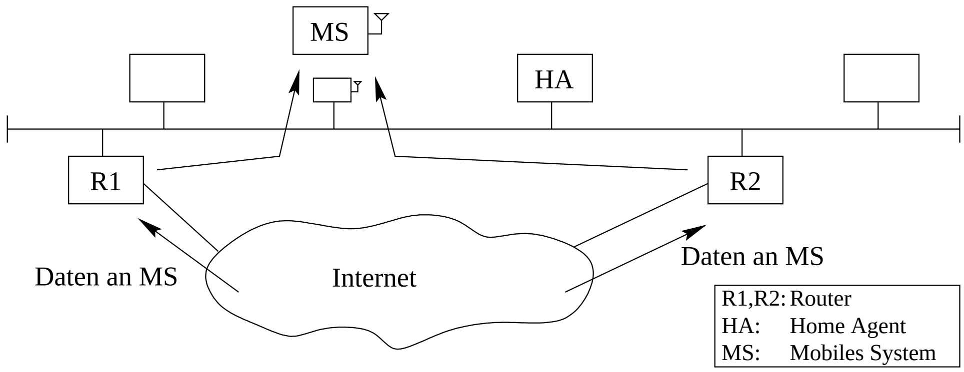

Abbildung 5.5: Problem: Plazierung des Transport Gateways im Heimatsubnetz

Lösung: Lokale Unterstützung durch den Home Agent

Man benötigt also ein System im Heimatsubnetz, über welches sämtlicher Datenverkehr vom und zum Mobilteilnehmer läuft. Der Home Agent ist dafür gut geeignet, weil er bereits die benötigte Funktionalität hat: Befindet sich der mobile Teilnehmer in einem fremden Subnetz, muß er alle Daten für diesen mittels ProxyARP entgegennehmen und zur Care-of Adresse weiterleiten. Hält sich das mobile System im Heimatsubnetz auf, behält der Home Agent diese Funktionalität bei. Er liefert allerdings die Daten nicht an die Care-of Adresse sondern lokal an die Heimatadresse des mobilen Systems aus. Dieses Vorgehen wird im folgenden als *Lokale Unterstützung durch den Home Agent* bezeichnet. Das mobile System führt im Heimatsubnetz den Home Agent als Default-Router, so daß Daten vom Mobilteilnehmer ebenfalls immer erst den Home Agent passieren. Damit kann das Transport Gateway auf dem Home Agent plaziert werden (siehe Abbildung 5.6).

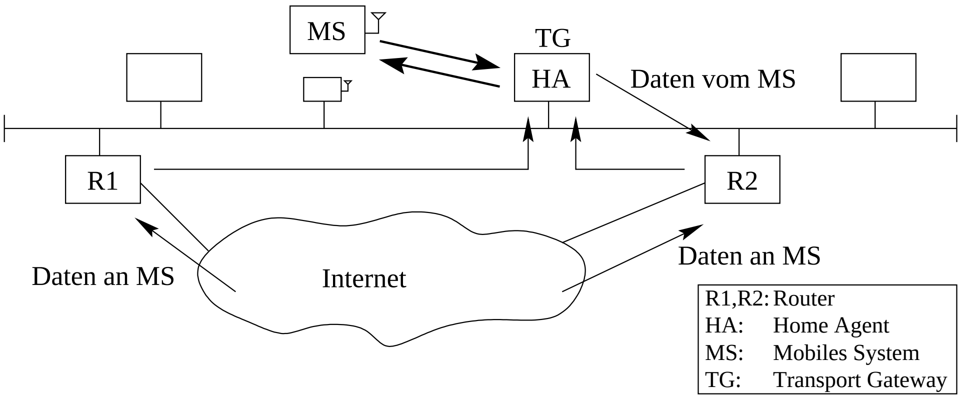

Abbildung 5.6: Lokale Unterstützung durch den Home Agent

Ein Nachteil ist, wie in Abschnitt 5.1.4 dargestellt, daß Nachrichten zum und vom mobilen Teilnehmer zweimal über das lokale Netz laufen, wenn der Home Agent nicht auf einem Router plaziert ist. Da die Datenrate der heutigen lokalen Netze aber deutlich höher ist als die einer drahtlosen Übertragung, spielt das nur eine untergeordnete Rolle.

Desweiteren sollte analog zur lokalen Unterstützung durch den Foreign Agent die lokale Unterstützung durch den Home Agent ebenfalls mit einer Lebensdauer versehen werden. Dies führt dazu, daß der mobile Teilnehmer auch Deregistrierungsanforderungen im Heimatsubnetz periodisch aussenden muß. Ohne diese Lebensdauer nimmt der Home Agent dauerhaft Pakete für das mobile System entgegen und leitet sie erneut auf das lokale Netz, auch wenn das mobile System z. B. ausgeschaltet ist.

5.2.2 Delayed Migration beim Subnetzwechsel

Wird bei einem Wechsel des Subnetzes die Migration des Transport Gateways verzögert, sind drei Szenarien zu beachten:

1. Das mobile System wechselt von einem fremden Subnetz in ein anderes.

2. Es wechselt vom Heimatsubnetz in ein fremdes Subnetz.

3. Es kehrt von einem fremden Subnetz in das Heimatsubnetz zurück.

Die Delayed Migration stellt bereits Betrachtungen über das erste Szenario an. Das zweite stellt kein Problem dar, wenn wie im vorherigen Abschnitt dargelegt, alle Daten zum mobilen System im Heimatsubnetz den Weg über den Home Agent nehmen. Das Transport Gateway kann also nach einem Wechsel vom Heimatsubnetz in ein fremdes Subnetz zunächst auf dem Home Agent verbleiben. Ein Problem ergibt sich aber für das dritte Szenario:

Da der Foreign Agent im fremden Subnetz nach einer Deregistrierung keine Daten zum mobilen Teilnehmer mehr empfängt, muß die Deregistrierung bis zur Migration des Transport Gateways vom alten Foreign Agent zum Home Agent verzögert werden. Sonst wäre das Transport Gateway nicht mehr funktionsfähig, weil die Daten zum Mobilteilnehmer dieses nicht mehr passieren. Solange die Migration des Transport Gateway noch nicht stattgefunden hat, muß der Datenfluß zum mobilen System wie in der Abbildung 5.7 dargestellt aussehen.

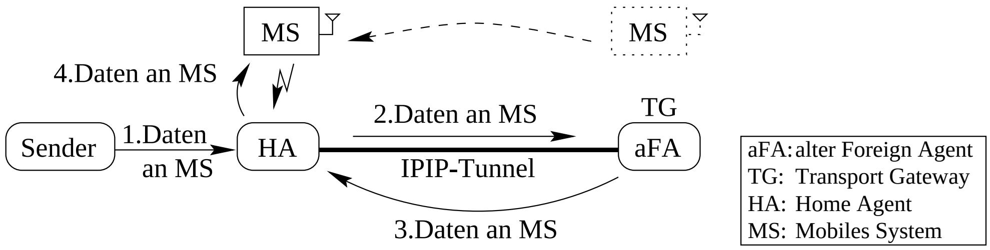

Abbildung 5.7: Delayed Migration: Rückkehr ins Heimatsubnetz

Der Home Agent muß alle Daten zum mobilen System, die nicht vom alten Foreign Agent kommen, zunächst durch den IPIP-Tunnel an den alten Foreign Agent weiterleiten, so daß das Transport Gateway evtl. vorhandene TCP-Pakete bearbeiten kann. Anschließend sendet der alte Foreign Agent die Daten zurück zum Home Agent, der sie an den Mobilteilnehmer ausliefert. In diesem Fall ist eine schnelle Migration des Transport Gateways anzustreben.

5.2.3 Fazit

Im Falle einer Kombination von MobileIP und indirektem Transportansatz muß beachtet werden, daß der Datenfluß zu einem Mobilteilnehmer immer über das System mit dem Transport Gateway verläuft. Eine aktive Rolle des Home Agents mittels der lokalen Unterstützung eines mobilen Systems kann diese Anforderung auch im Heimatsubnetz garantieren.

5.3 Mobilität und RSVP

In diesem Abschnitt werden allgemeine Probleme dargestellt, die sich bei der Betrachtung von RSVP unter dem Aspekt der Mobilität ergeben. Die Analyse von speziell bei der Kombination von RSVP und Mobile IP auftretenden Problemen geschieht in Abschnitt 5.4. Der unmittelbar folgende Abschnitt betrachtet die Designprinzipien von RSVP unter dem Blickwinkel der Mobilität, die Abschnitte 5.3.2 bis 5.3.4 beschäftigen sich mit Problemen im Falle der Mobilität zwischen Subnetzen. Abschnitt 5.3.5 dagegen betrachtet Mobilität innerhalb eines LAN (Local Area Network) in Verbindung mit RSVP.

5.3.1 Die Designprinzipien von RSVP

Von den sieben Entwurfszielen bzw. sechs Designprinzipien (vgl. Abschnitt 4.2) haben sich vier als besonders wichtig für die Kombination von RSVP mit Mobilität herausgestellt:

1. Betrachtung von heterogenen Empfängern durch eine empfängerorientierte Reservierung (1.Prinzip).

2. Anpassung an Routenänderungen durch den Soft-State bzw. Local Repair Ansatz (Ziel 5 bzw. 4.Prinzip).

3. Modularisierung: Trennung der Ressourcenreservierung von anderen Modulen (u.a. dem verwendeten Routingprotokoll) (Ziel 7 bzw. 6.Prinzip).

4. Reduktion des Protokolloverheads (Ziel 6).

Empfängerorientierte Reservierung Der erste Punkt ist für mobile Teilnehmer wichtig, weil in heutigen Netzwerken auf einer drahtlosen Strecke eine um mehrere Größenordnungen niedrigere Bandbreite zur Verfügung steht als auf einer drahtgebundenen Strecke. Sie liegt z. B. bei 100 Mbps bei Fast-Ethernet und 2 Mbps bei WaveLAN. Zusätzlich treten bei einer Funkübertragung mehr Bitfehler auf, die wegen Übertragungswiederholungen eine höhere Verzögerung der Daten bewirken können. In einer homogenen Umgebung mit stationären Teilnehmern ist im Falle einer Gruppenkommunikation eine Einigung auf eine Dienstgüte noch zentral vom Sender aus organisiert denkbar. In einer heterogenen Umgebung mit mobilen und stationären Teilnehmern ist das wegen der signifikant unterschiedlichen Qualitätsparameter Bandbreite und Verzögerung nicht sinnvoll: Die gemeinsamen Qualitätsparameter müßten dann immer auf die Teilnehmer mit den niedrigsten Werten eingestellt werden, also auf mobile Teilnehmer. Eine empfängerorientierte Reservierung kann besser auf die Bedürfnisse der einzelnen Gruppenmitglieder eingehen.

Außerdem muß sich bei einer empfängerinitiierten Reservierung der Sender nicht um Mobilität kümmern, weil der mobile Teilnehmer selbst für eine Reservierung verantwortlich ist. Tatsächlich muß sich in RSVP nicht einmal der Empfänger um Mobilität kümmern, die Anpassung einer Route übernimmt RSVP selbst.

Anpassung an Routenänderungen Prinzipiell stellt der zweite Punkt einen guten Ansatz dar, eine Anpassung der reservierten Routen dynamisch und automatisch vom System vornehmen zu lassen. Wie im Abschnitt 5.3.2 dargestellt, ist der in RSVP vorhandene Mechanismus des Local Repair aber für eine schnelle Wiederherstellung einer Reservierung nach einem Subnetzwechsel zu langsam und bedarf einer Verbesserung.

Modularisierung Dieser Punkt ist insofern passend, als daß er es erlaubt, das IP-Standardrouting durch das Mobile IP Routingprotokoll zu erweitern, ohne Veränderungen an RSVP vornehmen zu müssen.

Reduktion des Protokolloverheads Dieser vierte Punkt ist für die effiziente Nutzung drahtloser Links mit niedrigen Bandbreiten wichtig. Die Aggregierung von RSVP-Nachrichten spielt in den heutigen drahtlosen Netzen allerdings noch keine Rolle, weil sie erst in den Zwischensystemen zu einer Reduktion des Overheads führt und heutige Netze nur auf dem letzten Hop zum mobilen Teilnehmer drahtlos sind. Erst die Einführung von mobilen Routern macht die Aggregierung zur Reduktion des Overheads auch unter dem Aspekt der Mobilität interessant.

Desweiteren muß für die effiziente Nutzung der Bandbreite einer funkbasierten Datenübertragung die Periode, mit der RSVP-Nachricht gesendet werden, möglichst groß sein.

Fazit

Anhand der Entwurfsziele und Designprinzipien ist RSVP also auch für die Ressourcenreservierung von mobilen Teilnehmern gut geeignet. Es konnten keine Probleme identifiziert werden, welche die Verwendung von RSVP durch einen Mobilteilnehmer grundsätzlich in Frage stellen. Dennoch gibt es Probleme, die in den folgenden Abschnitten detailliert dargestellt werden.

5.3.2 Erkennen einer Routenänderung

RSVP ist in der Lage, Änderungen der Route zu einem Empfänger durch den Local Repair Ansatz zu beheben. Solche Routenänderungen treten auf, wenn sich die Topologie der Router z. B. wegen der Überlastung oder des Ausfalls eines einzelnen Routers ändert und damit auch die Route vom Sender zum Empfänger. In der RSVP-Spezifikation [BraZha97, S. 49] wird vorgeschlagen, bei der Benachrichtigung von RSVP durch das Routingprotokoll zwei Sekunden zu warten, bevor RSVP eine Path-Nachricht entlang der neuen Route versendet. Für ein mobiles System ist diese Wartezeit für eine schnelle Erneuerung einer Reservierung nach einem Subnetzwechsel zu lang.

Außerdem verwenden einige RSVP Implementierungen kein Local Repair, weil dieser Mechanismus optional ist. In solchen RSVP-Implementierungen wird die Reservierung der neuen Strecke nach einem Subnetzwechsel erst nach Ablauf der Soft-State Timer neu vorgenommen (vgl. Abschnitt 4.4.2).

Deshalb sollte das Routingprotokoll, welches nach einem Subnetzwechsel die Änderung der Route zum mobilen Teilnehmer vornimmt, unmittelbar nach dieser Änderung RSVP benachrichtigen, damit dieses die Reservierung auf der neuen Strecke vornehmen kann.

Der Nachteil dieser Methode ist allerdings die Verzahnung des Routingprotokolls mit RSVP, welches der Idee der Abstraktion der Schichten widerspricht. Dieses Prinzip wird aber auch in anderen Bereichen z. B. für eine effektivere Implementierung von Hochleistungsnetzen häufiger durchbrochen.

5.3.3 Subnetzwechsel mit Ablehnung der Reservierung

Zwei Gründe können dazu führen, daß eine Erneuerung einer Reservierung nach einem Subnetzwechsel abgelehnt wird:

1. Auf der drahtgebundenen Strecke sind nicht genügend Ressourcen frei (z. B. Bandbreite oder Puffer in einem Zwischensystem).

2. Die Funkzelle, in die das mobile System gewechselt hat, verfügt über keine freien Kapazitäten mehr (z. B. Bandbreite), um das mobile System zu unterstützen.

Dieser letzte Fall ist der am häufigsten eintreffende Fall, er kann allerdings auch auftreten, wenn ein Funkzellenwechsel ohne Subnetzwechsel vorliegt.

In der Literatur wird diese Problematik häufig behandelt, diese Arbeit stellt aber hierzu keine weiteren Betrachtungen an.

5.3.4 Explizites Löschen von belegten Ressourcen

Hat sich eine Routenänderung auf einer mit RSVP reservierten Strecke ergeben, bewirkt erst ein Ablaufen der Soft-State Timer die Freigabe der Ressourcen auf der alten Strecke. Damit sind im schlechtesten Fall für die Dauer einer Soft-State Periode nicht mehr benötigte Ressourcen im Netz reserviert. Diese Vorgehensweise ist akzeptabel für Topologieänderungen in drahtgebundenen Netzwerken, weil diese relativ selten vorkommen. Routenänderungen zu Mobilteilnehmern treten allerdings in Folge von Subnetzwechseln häufiger auf, insbesondere bei einer großen zu erwartenden Zahl von mobilen Systemen. Das hat zur Folge, daß ständig eine größere Menge an Ressourcen im Netz auf nicht mehr benötigten Routen belegt ist. Dadurch reduziert sich die verfügbare Bandbreite, was sich insbesondere auf drahtlosen Strecken wegen der dort niedrigen Bandbreiten negativ auswirkt.

Lösungsvorschlag Deswegen sollte also bei einer Routenänderung nicht nur, wie im vorherigen Abschnitt vorgeschlagen, RSVP für das Wiederherstellen einer Reservierung nach einem Subnetzwechsel eine Nachricht vom Routingprotokoll erhalten. Zusätzlich sollte RSVP auch eine Information bekommen, um eine alte Reservierung explizit aufheben zu können.

Mobile Sender

Für mobile Sender ergibt sich noch ein zusätzliches Problem. In RSVP wird Bandbreite auf einer Strecke immer von dem System reserviert, welches eine Resv-Nachricht erhalten hat, und zwar für die Teilstrecke, von der die Resv-Nachricht gekommen ist (vgl. Abschnitt 4.3.4). Ein mobiler Sender reserviert also Bandbreite auf der drahtlosen Strecke, wohingegen bei einem mobilen Empfänger der Previous Hop die Reservierung auf dem drahtlosen Link vornimmt. Im Falle eines Funkzellenwechsels des mobilen Senders heißt das, daß die Ressourcen auf dem drahtlosen Link nicht explizit freigegeben werden können, wohingegen bei einem mobilen Empfänger der Previous Hop die Freigabe der Ressourcen übernehmen kann.

Dieses Problem muß je nach verwendeter Übertragungstechnologie gelöst werden, die Freigabe der Bandbreite muß ein anderes System als der mobile Sender übernehmen können.

5.3.5 RSVP in einem lokalen Netz mit mehreren Funkzellen

Dieser Abschnitt soll eine Ressourcenreservierung auf einem lokalen Netz mit mehreren Funkzellen betrachten und welche Probleme sich dabei ergeben. Dabei muß man zwischen Multicast und Unicast RSVP-Sitzungen unterscheiden.

Das Szenario

Gegeben sei das folgende Szenario für ein lokales Netz mit einem Broadcastmedium (typischerweise Ethernet) mit mehreren Funkzellen (vgl. Abbildung 5.8), wobei jede Funkzelle von einer Basisstation (BS) bedient wird.

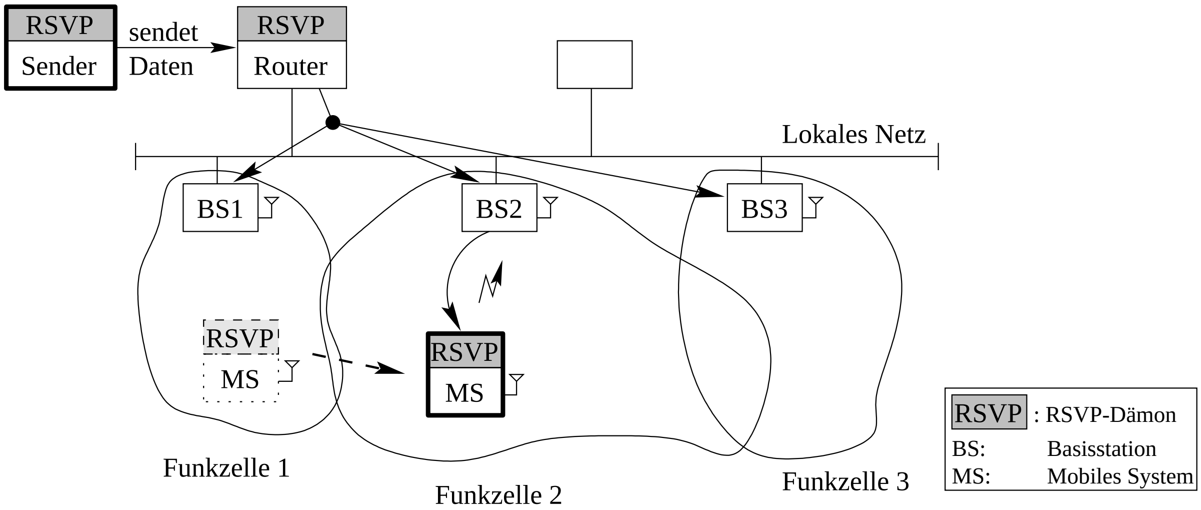

Abbildung 5.8: Szenario: RSVP-Betrieb in einem lokalen Netz mit mehreren Funkzellen

Die Basisstationen sollen als Brücken [Tan92, S. 47] konfiguriert sein, d. h. sie verbinden die Funkzelle und das lokale Festnetz auf der Sicherungsschicht. Für die Vermittlungsschicht stellen das lokale Netz und die Funkzellen ein gemeinsames Subnetz dar (z. B. ein IP-Subnetz). Die Basisstationen sollen Unicast-Datenverkehr nur in die Funkzelle weiterleiten, in der sich der Empfänger aufhält. Multicast- und Broadcast-Datenverkehr müssen die Basisstationen in alle Funkzellen ausstrahlen.

Unicast RSVP-Sitzung

Im Falle der Unicast RSVP-Sitzung ergibt sich ein Problem, wie auf der Sicherungsschicht Reservierungen vorgenommen werden sollen. Man muß dabei zwischen einem mobilen Empfänger und einem mobilen Sender unterscheiden.

Ablauf mit einem mobilen Empfänger Abbildung 5.9 stellt den Ablauf einer Reservierung im Falle eines mobilen Empfängers dar. Als erstes bekommt der Router eine

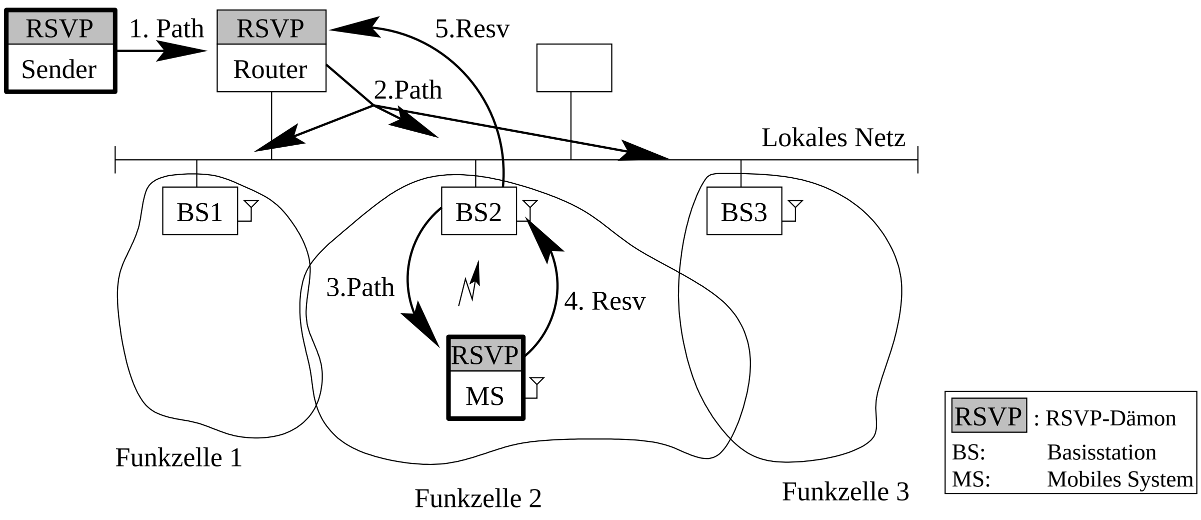

Abbildung 5.9: Unicast RSVP-Sitzung in einem lokalen Netz mit mehreren Funkzellen

Path-Nachricht vom Sender (1.Path) und leitet sie in das lokale Netz weiter (2.Path), so daß alle Basisstationen diese empfangen. Da in ihr eine Unicast Zieladresse angegeben ist, gibt nur die Basisstation (in der Abbildung BS2) die Nachricht weiter, in deren Funkzelle sich der Mobilteilnehmer befindet (3.Path). Das mobile System kann dann eine Reservierung anstoßen. Dazu reserviert es zunächst die lokalen Ressourcen (z. B. CPU-Zeit, Puffer) und sendet eine Resv-Nachricht an den Previous Hop, also den Router (4.Resv). Die Basisstation empfängt diese Nachricht und gibt sie unbearbeitet an den Router weiter (5.Resv). Dieser muß die Reservierung für die Strecke zum mobilen System vornehmen. Dazu sendet er eine Reservierungsanfrage an die Ressourcenverwaltung, die diese Anfrage entsprechend der verwendeten Übertragungstechnologie in eine Reservierung auf dem Medium umsetzen muß. Die Ressourcenverwaltung kann zunächst nur Ressourcen auf dem lokalen Netz reservieren. Bei der Reservierung in der Funkzelle treten die folgenden Probleme auf:

1. Der Router hat weder im RSVP-Dämon noch in der Ressourcenverwaltung das Wissen, in welcher Funkzelle sich der Mobilteilnehmer gerade befindet.

2. Die Strecke vom Router zum mobilen System ist aus der Sicht von RSVP nur eine Strecke; physikalisch gesehen sind es aber zwei Strecken mit möglicherweise sehr verschiedenen Eigenschaften (z. B. hinsichtlich Bandbreite, Fehlerrate etc.).

Ablauf mit einem mobilen Sender Bei einem mobilen Sender treten die obigen Probleme in ähnlicher Weise auf. Der mobile Sender muß die gesamte Strecke zum Next Hop reservieren. Das funktioniert für die drahtlose Strecke, zusätzlich ist aber auch noch eine Reservierung der Strecke von der Basisstation zum Router notwendig. Damit muß ein RSVP-Dämon erneut Ressourcen auf zwei Strecken mit verschiedenen Übertragungstechnologien reservieren.

Lösungsvorschläge Es gibt zwei grundsätzliche Ansätze zur Lösung dieser Probleme:

1. Der Router reserviert die gesamte Strecke vom Router zum mobilen System.

2. Die Basisstationen übernehmen Reservierung in ihren Funkzellen, indem sie einen RSVP-Dämon aufgesetzt bekommen, der die Reservierungen in der Funkzelle verwalten und initiieren kann.

Zentrale Reservierung durch den Router Für diesen ersten Ansatz ist es notwendig, daß der Router eine Reservierungsanfrage des RSVP-Dämon an die Basisstation weitergibt, weil er selbst kein Wissen über Reservierungen in einzelnen Funkzellen hat. Dazu könnte man ein neues Protokoll zwischen dem Router und den Basisstationen verwenden, damit der Router eine Reservierungsanfrage an die Basisstationen weitergeben und diese eine Bestätigung bzw. Ablehnung zurücksenden können. Da es aber viele verschiedene Funkübertragungstechniken und dementsprechend unterschiedliche Basisstationen gibt, müßte dieses Protokoll aus Kompatibilitätsgründen für alle möglichen Basisstationen verwendbar sein. Sonst bräuchte der Router für jede Übertragungstechnologie eine separate Protokollimplementierung. Dieser Ansatz soll aber wegen der großen Komplexität in dieser Arbeit nicht weiter betrachtet werden.

RSVP auf den Basisstationen Ein einfachere Lösung der Probleme stellt der zweite Ansatz dar. Er macht die physikalische Trennung der Strecke vom Router zum mobilen Teilnehmer auch für RSVP sichtbar. Dabei gibt es zwei Alternativen:

1. Die Basisstation wird zu einem gewöhnlichen Router.

2. Die Basisstation wird um so wenige RSVP-Funktionen wie möglich erweitert und behält sonst die Rolle einer Brücke.

Nachteile der ersten Alternative sind, daß für jede Funkzelle innerhalb eines lokalen Netzes ein eigenes Subnetz auf Vermittlungsschichtebene entsteht und man dafür eine eigene Subnetzadresse braucht. Außerdem müßte der Router für jeden Mobilteilnehmer einen eigenen Eintrag in der Routingtabelle halten, der sich auch noch bei jedem Funkzellenwechsel ändert. Diese Alternative ist also nicht praktikabel.

Deshalb wird im folgenden der Ablauf einer Unicast RSVP-Reservierung bei der zweiten Alternative betrachtet (siehe Abbildung 5.10). Empfängt die Basisstation eine Nachricht

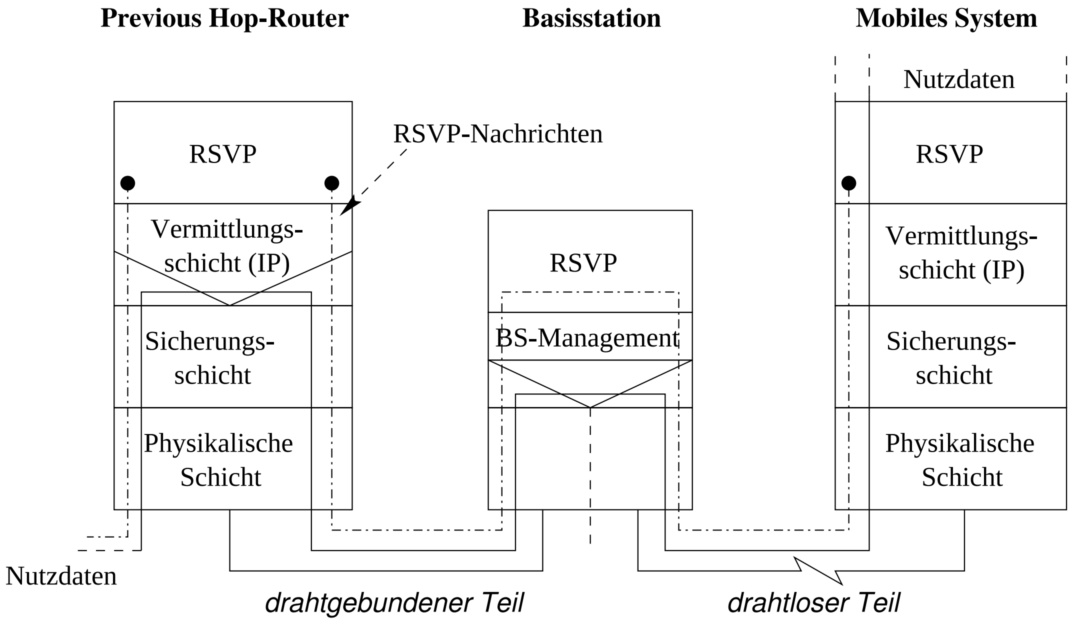

Abbildung 5.10: Daten- und Kontrollfluß im Protokollstack mit RSVP auf einer Basisstation

für einen mobilen Teilnehmer, welcher sich in ihrem Bereich befindet, muß sie diese auf RSVP-Nachrichten untersuchen. Solche leitet sie nicht sofort weiter, sondern liefert sie an den eigenen RSVP-Dämon aus. Dieser speichert die benötigten Informationen lokal im Path State Block und schickt die RSVP-Nachricht weiter an das mobile System. Er trägt aber nicht sich selbst als Previous Hop in die Path-Nachricht ein, weil die Brücke keine Netzwerkschicht erhalten soll und damit auch keine Netzwerkadresse.

Nachrichten, die aus der Funkzelle kommen, muß die Basisstation ebenfalls daraufhin untersuchen, ob es RSVP-Nachrichten sind. Sendet das mobile System eine Resv-Nachricht, wird diese an den RSVP-Dämon auf der Basisstation übergeben, der die Reservierung auf dem drahtlosen Link vornimmt. Dazu muß auf der Basisstation auch eine Verkehrskontrolle sowie eine Ressourcenverwaltung (vgl. Seite 34) implementiert sein. Sollten die angeforderten Ressourcen auf dem drahtlosen Link nicht verfügbar sein, schickt der RSVP-Dämon auf der Basisstation eine ResvErr-Nachricht zurück zum mobilen Teilnehmer.

Die Vorteile dieses Vorgehens sind:

- Die Reservierung auf der drahtlosen Strecke wird auch auf der Sicherungsschicht von der Reservierung auf dem lokalen Netz getrennt.
- Es ist keine zusätzliche Signalisierung zwischen dem Router und den Basisstationen notwendig, weil die RSVP-Nachrichten ohnehin die Basisstation passieren.

Als Nachteile ergeben sich:

- Die Komplexität einer Basisstation wächst. Der Speicherbedarf für die Path State Blocks und die Informationen über die Reservierungen ist aber dadurch begrenzt, daß eine Basisstation nur eine bestimmte maximale Anzahl mobiler Teilnehmer versorgen kann. Damit ergibt sich auch nicht das Problem einer effizienten Suche in diesen Daten, welches momentan für Zwischensysteme im drahtgebundenen Netz mit einer großen Anzahl möglicher Reservierungen in der Diskussion ist.

Zusammenfassung Die Reservierung einer Unicast RSVP-Sitzung in einem lokalen Netz mit mehreren Funkzellen erfordert also eine spezielle Funktionalität, die entweder eine zentrale Ressourcenreservierung auf dem Router oder eine verteilte durch RSVP-Dämonen auf den Basisstationen bereitstellen kann. Tabelle 5.4 stellt nochmals die Vor- und Nachteile der beiden Varianten gegenüber.

Zentrale Ressourcenreservierung auf dem Router	RSVP-Dämon auf der Basisstation
+ geringere Komplexität der Basisstationen – neues Protokoll erforderlich – abhängig von Übertragungstechnologie	+ Trennung der Reservierung auf der drahtgebundenen Strecke von der in der Funkzelle auch aus Sicht von RSVP – hohe Komplexität der Basisstationen

Tabelle 5.4: Zentrale vs. verteilte Ressourcenreservierung im lokalen Netz

Multicast RSVP-Sitzung

Im Falle einer Multicast RSVP-Sitzung kann zusätzlich zu den Problemen einer Unicast RSVP-Sitzung das Problem auftreten, daß die Multicast-Daten Bandbreite in allen Funkzellen belegen. Zunächst stellt aber Abbildung 5.11 eine Multicast RSVP-Sitzung mit einem mobilen Empfänger im lokalen Netz dar.

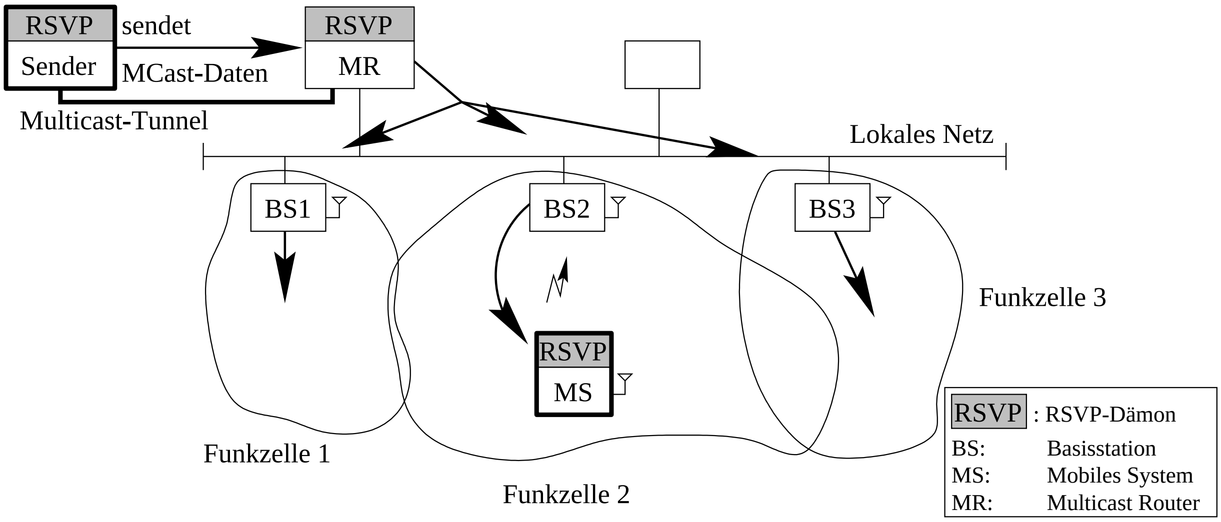

Abbildung 5.11: Multicast RSVP-Sitzung in einem lokalen Netz mit mehreren Funkzellen

Ablauf mit einem mobilen Empfänger Ein Mobilteilnehmer tritt mittels einer Join-Nachricht an den Multicast-fähigen Router einer gewünschten Multicast-Gruppe bei. Der Sender überträgt die Multicast-Daten zum Router, welcher sie auf das lokale Netz zu den Basisstationen weiterleitet. Diese haben keine Information, welche von den mobilen Teilnehmern in ihrem Bereich sich in welcher Multicast-Gruppe befinden, weil die Verwaltung der Multicast-Gruppen auf der Vermittlungsschicht realisiert ist, wohingegen die Basisstationen das drahtlose Netz mit dem lokalen auf der Sicherungsschicht verbinden. Daher müssen alle Basisstationen die Multicast-Daten in ihre Funkzelle ausstrahlen, was dort zu einer Verschwendung von Bandbreite führt.

Eine von einem Mobilteilnehmer ausgehende Reservierung verursacht wie im vorherigen Abschnitt dargestellt, ebenso die Frage, wie Ressourcen auf der heterogenen Strecke vom Router zum mobilen System reserviert werden sollen. RSVP-Dämonen auf den Basisstationen können hier erneut Abhilfe schaffen.

Lösung: Multicast-Router mit Mobilitätsunterstützung Eine Lösung dieses Problems liegt in der Erweiterung der Multicast-Router um eine Mobilitätsunterstützung. Empfängt ein solcher Router Multicast-Daten, für die nur sehr wenige mobile Gruppenteilnehmer im lokalen Netz Interesse gezeigt haben, sendet er diese Daten in ein IPIP-Paket eingekapselt per Unicast an die mobilen Systeme. Somit leiten nur die Basisstationen die Multicast-Daten weiter, in deren Funkzellen mobile Teilnehmer Interesse für diese Daten bekundet haben. Dementsprechend müßte dann auch der RSVP-Dämon auf dem Multicast-Router an Mobilität angepaßt werden und eingehende Path-Nachrichten für eine Multicast-Zieladresse in Path-Nachrichten für die Unicast-Adresse der entsprechenden mobilen Systeme umwandeln. Eine RSVP-Tunnelsitzung ist in diesem Fall nicht notwendig, weil auf der Strecke vom Multicast-Router zum mobilen System kein weiterer Hop dazwischenliegt.

Insgesamt würde also eine Multicast RSVP-Sitzung in eine Unicast RSVP-Sitzung umgewandelt, deren Probleme bereits der vorangegangene Abschnitt betrachtet hat. Multicast-Daten mit vielen mobilen Gruppenteilnehmern im lokalen Netz sollten dagegen ohne Umwandlung in Unicast-Daten weitergesendet und damit auch in allen Funkzellen propagiert werden. Das Umwandeln der Multicast-Daten in Unicast-Daten würde in diesem Fall mehr Bandbreite belegen.

Mobile Sender Bei einer Multicast RSVP-Sitzung mit einem mobilen Sender tritt dasselbe Problem auf wie mit einem mobilen Empfänger, wenn das mobile System direkt an die Multicast-Adresse sendet: Die Basisstationen leiten die Multicast-Daten in alle Funkzellen weiter. Um dies zu umgehen, sollte der mobile Teilnehmer die Daten per Unicast an den Multicast-Router schicken. Falls im lokalen Netz Empfänger für diese Multicast-Daten vorhanden sind, kann der oben erwähnte Mechanismus zum Versenden verwendet werden: Der Multicast-Router sendet Daten per Unicast, wenn nur sehr wenige mobile Gruppenmitglieder vorhanden sind oder per Multicast, wenn es viele Mitglieder sind.

Funkzellenwechsel mit RSVP-Dämonen auf den Basisstationen

Wechselt ein Mobilteilnehmer innerhalb eines lokalen Netzes die Funkzelle (siehe Abbildung 5.8), sind in der neuen Funkzelle keine Ressourcen reserviert. Eine Neureservierung mittels Local Repair findet nicht statt, weil sich der Previous Hop (hier: der Router) des mobilen Teilnehmers nicht geändert hat.

Als ein Lösungsvorschlag könnten die RSVP-Dämonen auf den Basisstationen der alten bzw. der neuen Funkzelle im Falle eines Funkzellenwechsels alle Daten austauschen, die für eine Reservierung in der neuen Funkzelle benötigt werden. Da viele Basisstationen bereits untereinander Nachrichten für Kontrollzwecke austauschen, wäre es eine einfache Lösung, hier eine weitere solche Kontrollnachricht hinzuzufügen. Nach einem Funkzellenwechsel kann die neue Basisstation Ressourcen in ihrer Funkzelle reservieren oder eine Fehlermeldung an den mobilen Teilnehmer senden, falls nicht genügend frei sind. Der RSVP-Dämon auf dem Router und auf dem mobilen System bemerken in diesem Falle den Funkzellenwechsel nicht.

5.3.6 Fazit: Mobilität und RSVP

Bewegt sich ein mobiles System zwischen Subnetzen, ergibt sich die Problematik der Kommunikation zwischen RSVP und dem Routingprotokoll. Letzteres sollte eine Routenänderung an RSVP zur Erneuerung bzw. Freigabe einer Reservierung melden. In einem lokalen Netz stellt die Heterogenität des Netzwerkes durch die Kopplung von Funkzellen und dem lokalem Netz auf der Sicherungsschicht ein Problem dar, welches durch die Einrichtung eines RSVP-Dämon auf jeder Basisstation gelöst werden kann.

5.4 Mobile IP und RSVP

Dieser Abschnitt betrachtet abschließend die Probleme, die sich aus der Kombination von Mobile IP und RSVP ergeben.

Vorbetrachtung: Mobile Sender

Die Motivation der Einführung von Mobile IP war, daß Daten **für** einen mobilen Teilnehmer nicht mehr mit dem IP-Standardrouting zu diesem gelangen können, wenn er sich mit seiner Heimatadresse in ein fremdes Subnetz begeben hat. Daten **von** einem Mobilteilnehmer in einem fremden Subnetz können dagegen ohne Mobile IP Unterstützung gesendet werden.

Desweiteren bietet RSVP nur Reservierungen für Simplexverbindungen an, unterscheidet also strikt zwischen Sender und Empfänger.

Aus beiden Aussagen folgt, daß Mobile IP für eine RSVP-Sitzung mit einem mobilen Sender nicht notwendig ist. Deswegen beschränken sich alle weiteren Betrachtungen von Problemen im Bezug auf RSVP und Mobile IP auf (RSVP-typische) Simplexverbindungen mit mobilen Empfängern.

Anmerkungen Wenn ein mobiler Sender das Subnetz wechselt, findet also keine Mobile IP-Signalisierung statt. Dennoch sollte die Reservierung auf der neuen Route erneuert werden. Wie beim Local Repair Verfahren beschrieben, kann das Routingprotokoll (also IP) RSVP im Falle einer Routenänderung benachrichtigen. Eine Betrachtung dessen ist aber nicht Gegenstand dieser Arbeit.

Im Falle einer Datenübertragung von einem mobilen System mit zuverlässigen Protokollen wie z. B. TCP ergibt sich das Problem, daß ohne die Unterstützung von Mobile IP Bestätigungen nicht zum Mobilteilnehmer gelangen können. In diesem Fall ist dann doch eine Mobile IP-Unterstützung notwendig. Da aber für Bestätigungen keine Reservierungen erfolgen sollen, kann die oben genannte Einschränkung aufrecht erhalten werden.

Vorbetrachtung: Multicast RSVP-Sitzungen

Wenn ein Mobilteilnehmer in einem fremden Subnetz als Empfänger einer Multicast RSVP-Sitzung beitritt, ist kein Mobile IP nötig, sofern in diesem fremden Subnetz Multicast-Unterstützung vorhanden ist. Abbildung 5.12 zeigt den Ablauf einer Multicast-Reservierung in einem fremden Subnetz.

Der Mobilteilnehmer sendet als erstes eine Join-Nachricht an den Multicast-Router MR (1.Join), der seinerseits dafür sorgt, daß die angeforderten Multicast-Daten und die Path-Nachrichten über den Multicast-Tunnel bei ihm ankommen (2.MCast-Daten). Dabei muß für den Multicast-Tunnel eine RSVP-Tunnelsitzung eingerichtet werden. Anschließend sendet der Multicast-Router die Daten an den mobilen Teilnehmer weiter (3.MCast-Daten).

Somit ist die IP-Adresse des mobilen Systems, wie bei IP Multicast üblich, nur dem lokalen Multicast-Router bekannt, weiter aufwärts im Multicast-Baum werden nur Multicast-Adressen verwendet. Das Problem des Weiterleitens von (Unicast-)Daten an den Mobilteil-

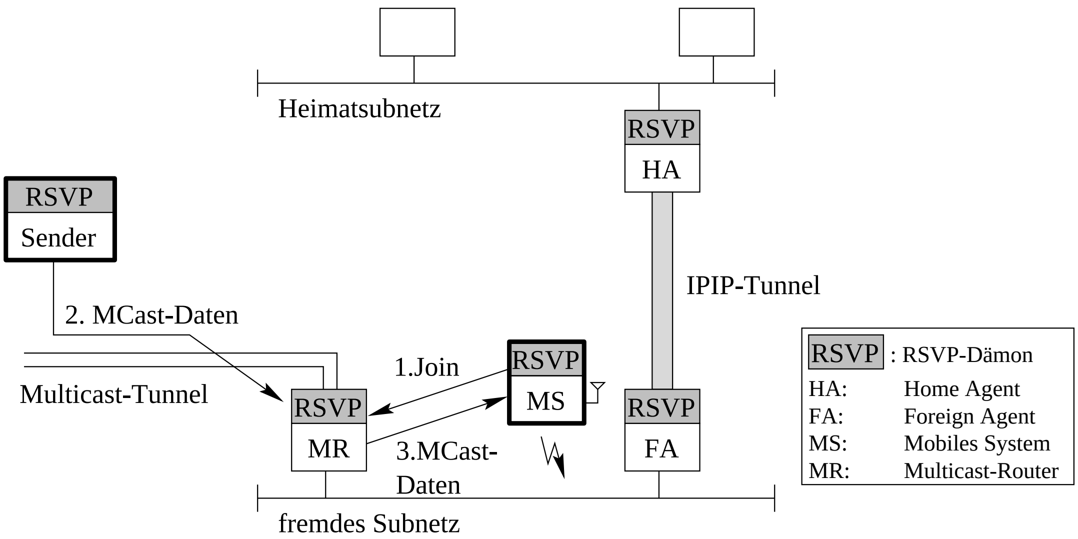

Abbildung 5.12: Multicast RSVP-Sitzung mit mobilem Empfänger im fremden Subnetz

nehmer, die oben genannte Motivation von Mobile IP, stellt sich also bei Multicast-Daten nicht. Die Reservierung der Strecke vom Multicast-Sender zum mobilen Empfänger geschieht genauso wie mit einem stationären Empfänger. Mobile IP ist für den Empfang von Multicast-Daten prinzipiell nicht notwendig.

Abschnitt 2.6 behandelt allerdings einige Ausnahmefälle, bei denen doch Mobile IP für die Bereitstellung von Multicast-Daten verantwortlich sein sollte. Diese Ausnahmefälle sollen aber im Zusammenhang mit RSVP nicht weiter betrachtet werden.

Subnetzwechsel des Mobilen Systems

Bei einem Subnetzwechsel meldet sich der mobile Teilnehmer bei dem Multicast-Router des neuen Subnetzes erneut mit einer Join-Nachricht an. Die Multicast-Daten können aber verzögert werden, wenn dieser Multicast-Router keine Daten für die gewünschte Gruppe empfängt und sich erst selbst an den Multicast-Baum für die angeforderte Gruppe anschließen muß.

Damit RSVP die Strecke zum mobilen Teilnehmer schnell reservieren kann, sollte das Multicast-Protokoll ein Signal an RSVP geben, wenn sich ein mobiler Teilnehmer bei einem neuen Multicast-Router anmeldet (vgl. Abschnitt 5.3.2).

Acharya et al. [AchBak96] betrachten die Problematik der Kombination von Mobile IP und IP Multicast im Detail.

Nach diesen beiden Vorbetrachtungen beziehen sich die folgenden Aussagen auf Unicast RSVP-Sitzungen, d. h. auf eine von RSVP reservierte Strecke zwischen genau einem Sender und genau einem mobilen Empfänger.

5.4.1 Signalfluß in einer Unicast RSVP-Sitzung mit Mobile IP

Dieser Abschnitt betrachtet die zwischen den Systemen ausgetauschten RSVP-Nachrichten, wenn ein mit Mobile IP unterstützter Mobilteilnehmer Empfänger in einer RSVP-Sitzung ist. Hierbei treten zwei Fälle auf: Der Mobilteilnehmer befindet sich in einem fremden Subnetz oder im Heimatsubnetz.

Mobiler Empfänger im fremden Subnetz

Eine RSVP-Sitzung zwischen einem stationären Sender und einem mobilen Empfänger in einem fremden Subnetz zeigt Abbildung 5.13.

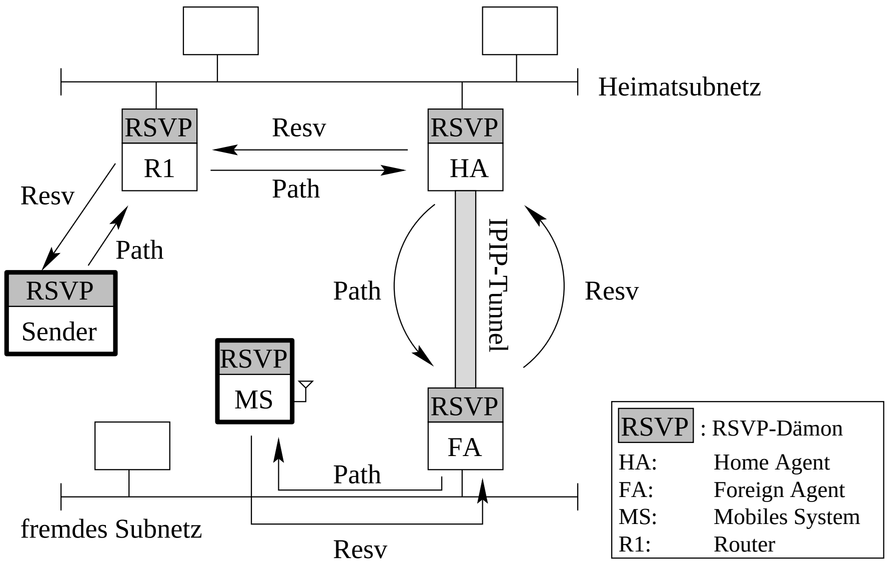

Abbildung 5.13: Unicast RSVP-Sitzung mit mobilem Empfänger im fremden Subnetz

Der Sender schickt die Path-Nachricht an die Heimatadresse des mobilen Empfängers, die per IP-Standardrouting bis in das Heimatsubnetz gelangt. Dort empfängt der Home Agent alle Nachrichten für das mobile System mittels Proxy-ARP (vgl. Abschnitt 2.5.3), also auch die Path-Nachricht. Er kapselt die Path-Nachricht in ein IPIP-Paket ein und sendet es zum Foreign Agent, welcher die Path-Nachricht wieder auspackt und an den mobilen Empfänger ausliefert.

Die Resv-Nachricht dagegen gelangt hop-by-hop über den umgekehrten Weg der Path-Nachricht vom Empfänger zum Sender. Das mobile System sendet die Resv-Nachricht an den Foreign Agent, seinen Previous Hop, der sie an den Home Agent (den Previous Hop des Foreign Agents) mittels IP-Standardrouting schickt. Von dort wird sie wieder hop-by-hop bis zum Sender geleitet. Wie in Abschnitt 4.6 dargelegt, muß der Tunnel zwischen dem Home Agent und dem Foreign Agent eine separate Reservierung bekommen.

Mobiler Empfänger im Heimatsubnetz

Für einen Mobilteilnehmer im Heimatsubnetz zeigt Abbildung 5.14 das Szenario, sofern man die Existenz eines Transport Gateways und damit die lokale Unterstützung durch den Home Agent einbezieht (vgl. Abschnitt 5.2.1).

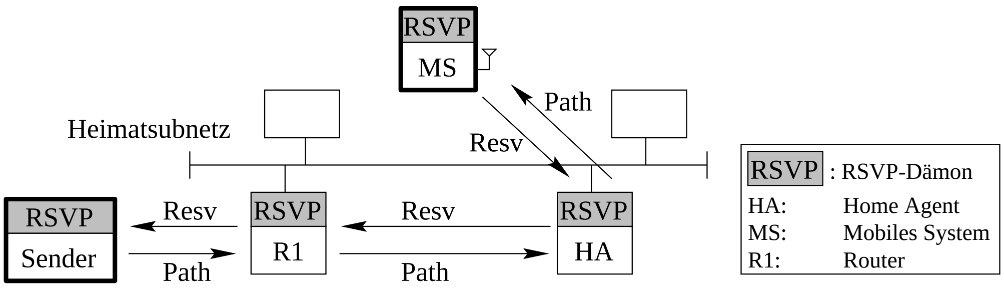

Abbildung 5.14: Unicast RSVP-Sitzung mit mobilem Empfänger im Heimatsubnetz

Die Vorgehensweise entspricht der aus der Abbildung 5.13, nur daß der Home Agent die Path-Nachrichten zum mobilen System nicht an den Foreign Agent tunnelt, sondern direkt auf das lokale Netz sendet. Resv-Nachrichten gelangen über den Home Agent und den Router R1 im Heimatsubnetz hop-by-hop zum Sender.

Fazit

Die Kombination von RSVP und MobileIP funktioniert also im Hinblick auf das Routing, allerdings erfordert der Tunnel zwischen Home Agent und Foreign Agent die Erstellung einer RSVP-Tunnelsitzung. Zusätzlich zu den RSVP-Dämonen auf allen beteiligten Routern sowie dem Sender und dem Empfänger, müssen auch RSVP-Dämonen auf den Mobility Agents betrieben werden, damit eine durchgehende Reservierung von Ressourcen möglich ist.

Man kann hier ebenfalls erkennen, daß zweimal Ressourcen auf dem lokalen Netz reserviert werden müssen (R1–HA, HA–MS), wenn ein Mobility Agent nicht gleichzeitig auf dem Router angesiedelt ist. Das gleiche gilt für ein fremdes Subnetz.

5.4.2 Erkennen einer Routenänderung

Wie in Abschnitt 5.3.2 dargestellt, ist der Local Repair Mechanismus von RSVP für das Erkennen von Routenänderungen zu langsam. Für eine schnellere Erkennung müssen zwei verschiedene Möglichkeiten für einen Subnetzwechsel betrachtet werden: Der Mobilteilnehmer wechselt in das Heimatsubnetz oder in ein fremdes Subnetz.

Subnetzwechsel ins Heimatsubnetz

In diesem Fall ist der Protokollablauf für eine schnelle Routenerkennung sehr einfach (siehe Abbildung 5.15).

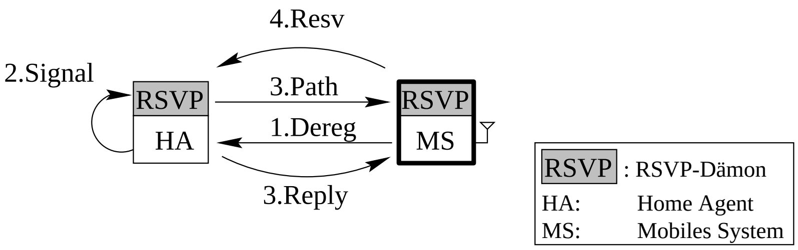

Abbildung 5.15: Sofortige Path-Nachrichten bei mobilem Empfänger im Heimatsubnetz

Zunächst sendet das mobile System eine Deregistrierungsanforderung an den Home Agent (1.Dereg). Dieser gibt ein Signal (2.) mit der IP-Adresse des mobilen Systems an den RSVP-Dämon auf dem Home Agent, der für alle Unicast RSVP-Sitzungen mit der übergebenen IP-Adresse als Zieladresse sofort eine Path-Nachricht an den mobilen Teilnehmer schickt (3.Path). Zugleich sendet er die Registrierungsantwort an diesen (3.Reply). Beim Erhalt der Path-Nachricht stellt der RSVP-Dämon auf dem mobilen System fest, daß er einen neuen Previous Hop hat und sendet sofort eine Resv-Nachricht an den Home Agent (4.Resv).

Sollte der Home Agent die Deregistrierung ablehnen, gelangen die Path-Nachrichten weiterhin über die alte Route zum alten Foreign Agent und sorgen damit für keine Erneuerung der Reservierung. Sobald aber das mobile System eine neue, erfolgreiche Deregistrierungsanforderung schickt, wird auch das Signal an den RSVP-Dämon auf dem Home Agent erneut gesendet. Damit stellt die Ablehnung der Deregistrierung kein Problem dar.

Subnetzwechsel in ein fremdes Subnetz

Nach einem Subnetzwechsel in ein fremdes Subnetz ändert sich nur die Strecke vom Home Agent zum mobilen Teilnehmer, daher muß nur dieser Teil der Strecke von RSVP neu reserviert werden. Dabei ist es unerheblich, ob der mobile Teilnehmer vom Heimatsubnetz oder von einem anderen fremden Subnetz kommt. Abbildung 5.16 dokumentiert den Protokollablauf bei der Kombination von Mobile IP und RSVP.

Nachdem das mobile System mittels Agent Discovery einen Subnetzwechsel erkannt hat, schickt es eine Registrierungsanforderung (1.Reg) an den neuen Foreign Agent (nFA), der sie an den Home Agent weiterleitet (2.Reg). Wenn dieser die Registrierung akzeptiert, setzt er die entsprechenden Einträge in der Routingtabelle und eröffnet den Tunnel zum neuen Foreign Agent (3.). An den RSVP-Dämon sendet er ein Signal mit der IP-Adresse des mobilen Systems (4.). Dieser sendet sofort Path-Nachrichten für alle Unicast RSVP-Sitzungen, die die übergebene IP-Adresse als Zieladresse haben, in Richtung des mobilen Teilnehmers (5.Path), d. h. zunächst zum neuen Foreign Agent. Dazu muß erst eine neue

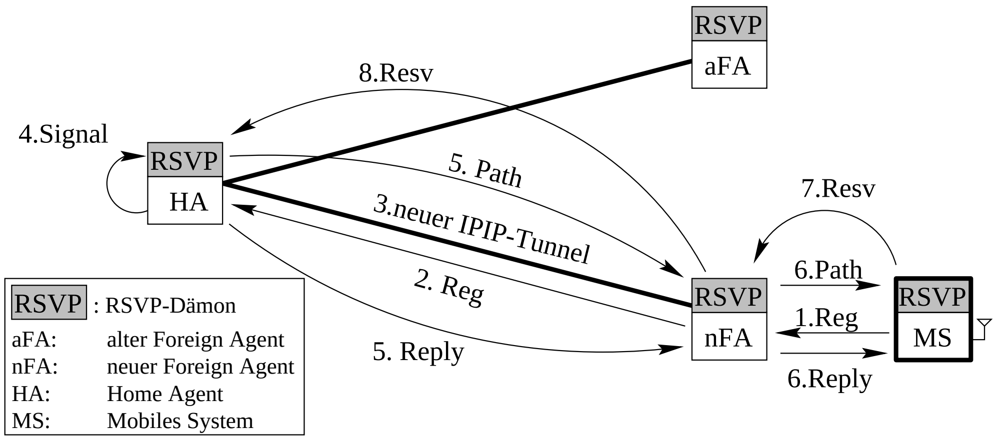

Abbildung 5.16: Sofortige Path-Nachrichten bei mobilem Empfänger im fremden Subnetz

RSVP-Tunnelsitzung zwischen dem Home Agent und dem neuen Foreign Agent eröffnet werden. Zeitgleich sendet der Home Agent die Registrierungsantwort an den neuen Foreign Agent (5.Reply). Dieser leitet beide Nachrichten zum Mobilteilnehmer weiter (6.Path, 6.Reply). Anhand dieser neuen Path-Nachricht stellt der RSVP-Dämon auf dem mobilen System fest, daß sein Previous Hop vom alten zum neuen Foreign Agent gewechselt hat. Deswegen sendet er sofort eine Wiederholung seiner letzten Resv-Nachricht (7.Resv) an den neuen Foreign Agent, die dieser an den Home Agent weiterleitet (8.Resv). Damit wird mit minimaler Zeitverzögerung die Reservierung auf der neuen Strecke aufgebaut.

Sollte der Home Agent die Registrierung nicht akzeptieren, wird die Path-Nachricht entlang der alten, bereits reservierten Strecke gesendet. Wie im vorherigen Abschnitt bei der Deregistrierung stellt dies kein Problem dar, weil der RSVP-Dämon bei der ersten erfolgreichen Registrierung ebenfalls wieder ein Signal erhält.

Problem: RSVP-Nachrichten überholen Mobile IP-Nachrichten

Da der Home Agent die Path-Nachricht und die Registrierungsantwort zeitgleich sendet, kann es vorkommen, daß die Path-Nachricht schneller beim Foreign Agent ist als die Registrierungsantwort. In diesem Fall ist die Path-Nachricht nicht korrekt zustellbar, weil der Foreign Agent seine lokale Unterstützung (Setzen der Routen etc.) für das mobile System erst beim Eintreffen der Registrierungsantwort einrichtet [Per96, S. 48]. Der Foreign Agent würde die Path-Nachricht wieder per IP-Standardrouting in das Heimatsubnetz leiten.

Lösung: Frühe lokale Unterstützung Eine einfache Lösung dieses Problems besteht darin, die lokale Unterstützung auf dem Foreign Agent bereits beim Eintreffen der Registrierungsanforderung vom Mobilteilnehmer zu errichten, also nach 1.Reg in der Abbildung.

Das hat den Nachteil, daß Mobile IP geringfügig komplexer wird, weil der Foreign Agent bei einem Ablehnen der Registrierung durch den Home Agent oder beim Verlust der Registrierungsanforderung die lokale Unterstützung wieder beenden muß. Die erfolgreiche Mobile IP Registrierung hat von dieser Vorgehensweise keine Nachteile.

Ein weiteres Problem ergibt sich im Bereich der Sicherheit: Sendet ein Angreifer eine unauthentifizierte Registrierungsanforderung an einen Foreign Agent, errichtet dieser trotz der falschen Authentifizierung zunächst die lokale Unterstützung für den mobilen Teilnehmer. Erst der Home Agent kann die Authentifizierung überprüfen. Der Angreifer kann also vom Foreign Agent Daten bekommen, die für den Mobilteilnehmer bestimmt sind, solange die Ablehnung der Registrierung vom Home Agent noch nicht beim Foreign Agent eingetroffen ist. Da allerdings auch noch kein IPIP-Tunnel vom Home Agent zum Foreign Agent besteht, bekommt der Angreifer nur Daten, die zufällig mittels IP-Standardrouting zum Foreign Agent gelangen (wenn er z. B. gleichzeitig Router für das lokale Netz ist).

Problem: Oszillierende Subnetzwechsel

Wechselt ein Mobilteilnehmer unmittelbar nach einem Subnetzwechsel wieder zurück in das alte Subnetz, kann die Situation entstehen, daß die Strecke vom Home Agent zum mobilen Teilnehmer nicht korrekt reserviert wird.

Wenn auf der Strecke vom Home Agent zum alten Foreign Agent die alte Reservierung noch intakt ist, gelangt eine auf das Signal vom Mobile IP auf dem Home Agent ausgesendete Path-Nachricht nur bis zum Next Hop. Dieser hat bereits einen Path State Block und leitet die Path-Nachricht deshalb nicht unmittelbar weiter (vgl. Abschnitt 4.4.1). Sendet der RSVP-Dämon auf dem mobilen System eine periodische Resv-Nachricht, bevor der alte Foreign Agent eine Path-Nachricht generiert hat, gelangt diese zum neuen Foreign Agent. Dies liegt daran, daß der RSVP-Dämon auf dem mobilen System die letzte Path-Nachricht vom neuen Foreign Agent erhalten hat und somit diesen als seinen Previous Hop gespeichert hat.

Ein weiteres Problem entsteht durch die variablen Perioden zur Wiederholung der Resv-Nachrichten. Es kann vorkommen, daß ein Teil der Reservierung auf der Strecke vom alten Foreign Agent zum Home Agent durch den Ablauf der Timer für die Lebensdauer bereits gelöscht ist, wohingegen z. B. die Reservierung zwischen dem mobilen Teilnehmer und dem alten Foreign Agent noch existiert. Wenn das mobile System eine Resv-Nachricht generiert und der alte Foreign Agent noch eine bestehende Reservierung hat, leitet dieser die Resv-Nachricht auch nicht unmittelbar weiter. Damit ist nicht die gesamte Strecke vom mobilen Teilnehmer zum Home Agent reserviert.

Lösung: Sofortige Path- bzw. Resv-Nachricht Die Lösung des ersten Problems besteht darin, Path-Nachrichten so zu kennzeichnen, daß jeder RSVP-Dämon auf den Zwischensystemen unabhängig von einem bereits bestehenden Path State Block die Path-Nachricht sofort weiterleitet. Ein solche Nachricht soll kurz *ImmPath-Nachricht*[1] heißen. Dementsprechend bekommen auch Resv-Nachrichten ein solches Kennzeichen, um auf der

[1] Der Anfang leitet sich von engl. immediate ab.

Strecke vom alten Foreign Agent zum Home Agent ohne Verzögerung eine Reservierung einzurichten. Sie sollen kurz *ImmResv-Nachrichten* heißen.

Nach einem Subnetzwechsel sendet der Home Agent also eine ImmPath-Nachricht zum Mobilteilnehmer, die ohne Rücksicht auf bereits bestehende Path State Blocks schnellstmöglich die Strecke zum mobilen System bewältigt. Dieses reagiert mit einer ImmResv-Nachricht, welche die Ressourcen ebenfalls schnellstmöglich reserviert. Um eine unnötige Signalisierung zu vermeiden, sollte der Home Agent die ImmResv-Nachricht nicht weiterleiten, weil die Strecke vom Home Agent zum Sender weiterhin unverändert ist.

Detaillierter Ablauf der Signalisierung beim Subnetzwechsel

Abbildung 5.17 zeigt nochmals die vollständige Signalisierung zwischen den Instanzen von Mobile IP und RSVP in einem Weg-Zeit-Diagramm. Dabei ist die Signalisierung eines Subnetzwechsels durch Mobile IP sowie das Aussenden von ImmPath- bzw. ImmResv-Nachrichten berücksichtigt.

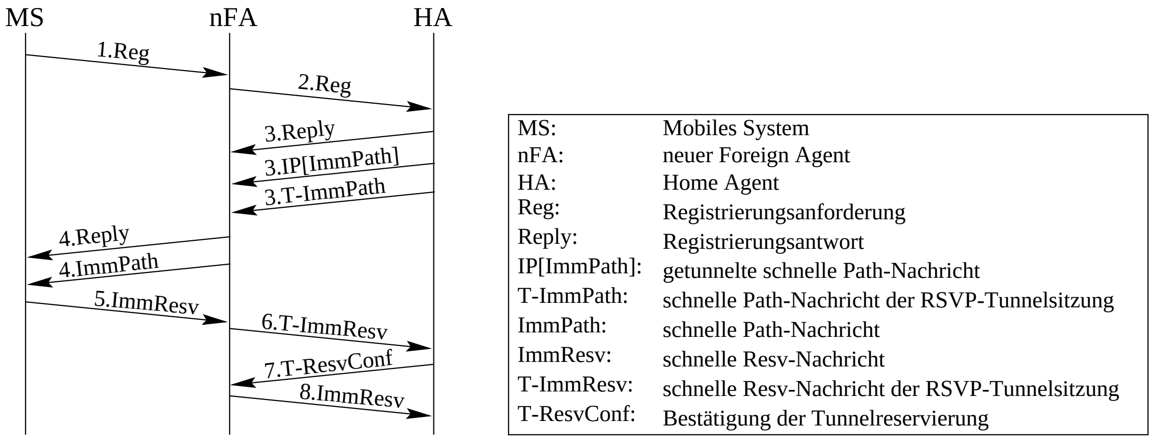

Abbildung 5.17: Weg-Zeit-Diagramm für eine Wiederherstellung einer RSVP-Sitzung

Die Zeit, die nach einem Subnetzwechsel in ein fremdes Subnetz für die Wiederherstellung einer über Mobile IP bestehenden RSVP-Sitzung benötigt wird, setzt sich zusammen aus: (Angaben in Klammern beziehen sich auf die obige Abbildung)

- der Signallaufzeit für die Registrierungsanforderung vom mobilen System zum neuen Foreign Agent (1.Reg)
- der Signallaufzeit für die Registrierungsanforderung vom neuen Foreign Agent zum Home Agent (2.Reg)
- der Signallaufzeit zwischen dem Home Agent und dem neuen Foreign Agent für die getunnelte ImmPath-Nachricht (3.IP[ImmPath]) sowie der ImmPath-Nachricht der RSVP-Tunnelsitzung (3.T-ImmPath), wobei ein zeitgleiches Versenden möglich ist

- der Signallaufzeit zwischen dem Foreign Agent und dem Mobilteilnehmer für die ImmPath-Nachricht (4.ImmPath)
- der Signallaufzeit zwischen dem mobilen System und dem neuen Foreign Agent für die ImmResv-Nachricht (5.ImmResv)
- der Signallaufzeit zwischen dem neuen Foreign Agent und dem Home Agent für das Versenden der Resv-Nachricht für die RSVP-Tunnelsitzung (6.T-ImmResv)
- der Signallaufzeit zwischen dem Home Agent und dem neuen Foreign Agent für die Bestätigung der Tunnel-Reservierung (7.T-ResvConf)
- und der Signallaufzeit für die eigentliche ImmResv-Nachricht (8.ImmResv)

Den genauen Ablauf einer Tunnelreservierung findet man bei Krawczyk et al. [KraTer97, 4.3]. Dort steht insbesondere, daß die mit „8.ImmResv“ gekennzeichnete ImmResv-Nachricht so lange verzögert wird, bis die Bestätigung der Tunnelreservierung eingetroffen ist.

Die Abbildung enthält nicht, daß zwischen dem neuen Foreign Agent und dem Home Agent beliebig viele Zwischensysteme in das Weiterleiten der Nachrichten involviert sein können. Dies ist deswegen wichtig, weil noch die Zeiten zur Verarbeitung der einzelnen Nachrichten auf den System beachtet werden müssen. Insbesondere die Zeit für die Verarbeitung von Path- bzw. Resv-Nachrichten in den Zwischensystemen ist nicht zu vernachlässigen.

Der überwiegende Anteil der Zeit zum Wiederherstellen einer Reservierung nach einem Subnetzwechsel besteht aber aus der Zeit, die zum Aufbau der neuen RSVP-Tunnelsitzung benötigt wird sowie aus den Signallaufzeiten zwischen Home Agent und Foreign Agent, sofern zwischen beiden eine große Entfernung liegt.

Fazit: Erkennen einer Routenänderung

Dieser Abschnitt hat gezeigt, wie im Detail eine Wiederherstellung einer mit RSVP vorgenommenen Reservierung aussieht, wenn Mobile IP einen Subnetzwechsel an den RSVP-Dämon signalisiert. Zusätzlich werden eine frühe lokale Unterstützung durch den Foreign Agent sowie sofortige Path- bzw. Resv-Nachrichten für den korrekten Ablauf benötigt.

5.4.3 Explizites Löschen von Ressourcen

Wie schon in Abschnitt 5.3.4 dargestellt, dauert es in RSVP eine Soft-State Periode s, bis die Ressourcen auf einer nicht mehr benötigten Strecke implizit, d. h. durch den Ablauf der Timer, freigegeben werden. Die lokale Unterstützung eines Foreign Agent für einen Mobilteilnehmer hört nach einer Zeit l auf, wenn der Foreign Agent in dieser Zeit keine weiteren Accept-Nachricht vom Home Agent für dieses mobile System bekommt.

Sollte $l < s$ sein, löscht der Foreign Agent die lokale Unterstützung für das mobile System, bevor auf einem der Router auf der Strecke vom Home Agent zum alten Foreign Agent die Soft-State Periode abläuft und eine PathTear-Nachricht downstream generiert wird. Diese gelangt dann per IP-Standardrouting vom Foreign Agent in das Heimatsubnetz des Mobilteilnehmers. Der Home Agent verwirft allerdings die PathTear-Nachricht, weil sie von einem anderen Previous Hop (dem alten Foreign Agent) kommt als die letzte Path-Nachricht (vgl. dazu das Verhalten von Router D in Abschnitt 4.4.2). Somit führt dieser Fall zwar zu keinem Fehler, aber dennoch zu einer unnötigen Signalisierung. Außerdem ist die für diese Arbeit verwendete RSVP-Implementierung diesbezüglich fehlerhaft, so daß der Fall vermieden werden sollte.

Lösung: Explizite Freigabe der Ressourcen Für eine bessere Ausnutzung der Netzwerkressourcen und um den obigen Fall $l < s$ zu umgehen, sollten nicht mehr genutzte Ressourcen explizit freigeben werden. Dabei treten zwei verschiedene Fälle auf:

1. Der Mobilteilnehmer kommt von einem fremden Subnetz.

2. Er wechselt vom Heimatsubnetz in ein fremdes.

Im ersten Fall sendet der Home Agent eine PathTear-Nachricht an den alten Foreign Agent. Sollte er zusätzlich, wie in Abschnitt 5.1.3 vorgeschlagen, eine MobileIP-Ende Nachricht an diesen senden, muß beachtet werden, daß die PathTear-Nachricht vor der MobileIP-Ende Nachricht ankommt. Andernfalls tritt dieselbe Situation wie beim oben beschriebenen Fall $l < s$ ein, daß eine PathTear-Nachricht per IP-Standardrouting vom Foreign Agent wieder zurück zum Heimatsubnetz gelangt. Da das Beenden der lokalen Unterstützung nicht so zeitkritisch ist wie der Abbau der Ressourcen, kann als einfache Lösung die MobileIP-Ende Nachricht zeitverzögert gesendet werden.

Im zweiten Fall muß nur die Reservierung auf dem Heimatsubnetz zwischen Home Agent und dem mobilen System gelöscht werden. Das bedeutet, daß der RSVP-Dämon auf dem Home Agent eine Nachricht an die Ressourcenverwaltung sendet, daß die Ressourcen freigegeben werden können. Eine weitere RSVP-Signalisierung ist nicht erforderlich.

5.4.4 Erneute Betrachtung des Weitverkehrsszenarios

Betrachtet man den Ablauf im Falle einer Wiederherstellung einer Reservierung aus Abbildung 5.17 und nimmt das explizite Löschen von Ressourcen aus dem vorherigen Abschnitt hinzu, kommt man bei Betrachtung eines Weitverkehrsszenarios zu den folgenden Aussagen:

- Die Zeit für einen Aufbau einer Tunnelreservierung beim Wechsel in ein fremdes Subnetz ist der bestimmende Faktor für die Dauer einer Unterbrechung der Reservierung. Legt man das Szenario aus Abschnitt 5.1.5 zugrunde, ergibt sich allein eine Signallaufzeit von 75 ms zwischen dem neuen Foreign Agent und dem Home Agent, bis die Tunnelreservierung etabliert ist. Dabei sind noch keine Verarbeitungszeiten in den Zwischensystemen einbezogen.

- Wird nach einem Wechsel von einem fremden Subnetz in ein anderes zuerst der Tunnel zum neuen Foreign Agent reserviert, kann die neue Reservierung wegen mangelnder Ressourcen nicht zustande kommen. Sind diese Ressourcen noch von der alten Tunnelreservierung belegt, blockiert diese den Aufbau der neuen. Diese Situation tritt insbesondere beim Weitverkehrsszenario auf, weil dann ein großer Teil des alten und des neuen Tunnels mit hoher Wahrscheinlichkeit eine identische Route benutzen.

- Wird dagegen zuerst die alte Tunnelreservierung explizit gelöscht, kann in der Zeit zwischen dem Löschen der alten und dem Reservieren der neuen Tunnelstrecke eine andere Reservierung die freiwerdenden Ressourcen nutzen, so daß die Tunnelreservierung wie schon im vorherigen Fall abgelehnt werden kann. Außerdem käme in diesem Fall noch die Zeit für den Abbau der Tunnelreservierung zur Dauer der Unterbrechung der Reservierung hinzu.

Aus diesen Gründen wird erneut das Fast-Forwarding Protokoll (siehe Abschnitt 5.1.5) zur Lösung der genannten Probleme vorgeschlagen. Es ergeben sich zusätzlich zu den bereits genannten Vorteilen noch die folgenden:

- Die Dauer der Unterbrechung einer Reservierung reduziert sich, weil kein kompletter Auf- und Abbau der Tunnelreservierung vom neuen Foreign Agent zum Home Agent notwendig ist. Es wird zusätzlich zu der in Abschnitt 5.1.5 genannten Signalisierung noch die Zeit zum Aufbau einer Tunnelreservierung zwischen altem und neuen Foreign Agent benötigt. Da beide aber räumlich dicht beieinanderliegen, dauert deren Aufbau weniger lange als der komplette Auf- und Abbau einer Tunnelreservierung zwischen Home Agent und Foreign Agent.

- Eine Zurückweisung einer Reservierungsanforderung durch die Blockierung der Ressourcen oder das Übernehmen der alten Ressourcen durch eine andere Reservierung auf der langen Strecke vom Home Agent zum alten Foreign Agent ist nicht möglich, weil diese Strecke weiterhin benutzt wird.

Die sich zusätzlich ergebenden Nachteile sind:

- Bei einer Vielzahl von Mobilteilnehmern haben die Foreign Agents einen höheren Verwaltungsaufwand für die Tunnel zwischen den Foreign Agents.

- Die Komplexität des Fast-Forwarding Protokolls ist höher als die von Mobile IP.

5.4.5 Betrachtung des Protokolloverheads

Eine funkbasierte Datenübertragung zeichnet sich insbesondere dadurch aus, daß weniger Bandbreite zur Verfügung steht als bei einer drahtgebundenen Übertragung. Dieser Abschnitt stellt Betrachtungen darüber an, ob sich bei der Kombination von RSVP und Mobile IP Möglichkeiten zur Reduktion der Bandbreite ergeben, welche die über den drahtlosen Link gesendeten Protokollnachrichten belegen. Die folgenden Tabellen zeigen die existierenden Nachrichten, ihre Größe und wie häufig diese versendet werden. Paketgrößen beziehen sich auf die Größe eines IP-Paketes, dazu kommt also noch die Länge des Protokollkopfes der Sicherungsschicht.

Mobile IP Nachrichten

Tabelle 5.5 zeigt von Mobile IP gesendete Nachrichten:

Nachricht	Größe	Auftreten
Agent Advertisement	ca. 70 Bytes	Periodisch (bis zu einmal pro Sekunde)
Registrierungsanforderung	ca. 80 Bytes	Periodisch mit fester, aber frei wählbarer Periode
Deregistrierungsanforderung	ca. 80 Bytes	Einmalig bei Anmeldung im Heimatsubnetz[a]
Registrierungsantwort	ca. 80 Bytes	Periodisch mit derselben Periode wie eine Registrierungsanforderung

[a]Erst durch die in Abschnitt 5.2.1 vorgeschlagenen Änderungen wird auch diese Nachricht periodisch.

Tabelle 5.5: Größe, Periode und Auftreten von Mobile IP-Nachrichten

Periodische Agent Advertisements können, wie in Abschnitt 5.1.2 beschrieben, eingespart werden, wenn man das schnelle Agent Discovery Verfahren einsetzt. Die Periode der drei anderen Mobile IP-Nachrichten dient dazu, eine lokale Unterstützung der Mobility Agents beenden zu können, wenn das mobile System ausfällt und sich nicht korrekt abmelden kann. Das explizite Beenden der lokalen Unterstützung sollte bewirken, daß dieser Mechanismus nur selten zum Einsatz kommt: Es kann entweder eine Mobile IP-Ende Nachricht verloren gehen oder das mobile System so ausgeschaltet werden, daß der Home Agent keine neue Anmeldung erhält und damit auch keine Mobile IP-Ende Nachricht generieren kann. Da aber die lokale Unterstützung nicht viele Ressourcen belegt, z. B. einen Tunnel und einen Eintrag in der Routingtabelle, aber insbesondere keine Bandbreite, kann die Periode so groß gewählt werden, daß der dabei entstehende Overhead vernachlässigbar klein ist.

RSVP Nachrichten

Tabelle 5.6 führt von RSVP gesendete Nachrichten auf (vgl. Abschnitt 4.3). Die ResvConf-Nachricht wird nur auf Anforderung des Empfängers versendet, sie findet daher hier keine Betrachtung.

Path- bzw. Resv-Nachrichten werden periodisch versendet, um in den einzelnen Zwischensystemen einen Soft-State zu implementieren. Dadurch können die Zwischensysteme belegte, aber nicht mehr benötigte Ressourcen automatisch nach einer Periode freigegeben. Hinsichtlich der geringen Bandbreite drahtloser Links ist es sinnvoll, diese Soft-State Funktionalität beizubehalten. Der Overhead von max. 500 Bytes alle 30 Sekunden, also 130 bps ist sehr gering. Versendet man dennoch die RSVP-Nachrichten nicht periodisch, kann eine

Nachricht	Größe	Auftreten
Path-Nachricht	≈ 100-250 Bytes[a]	Periodisch alle 30 s±50%
Resv-Nachricht	≈ 100-250 Bytes[b]	Periodisch alle 30 s±50%
PathTear-Nachricht	≈ 100 Bytes	Einmalig
ResvTear-Nachricht	≈ 100 Bytes	Einmalig
PathErr-Nachricht	≈ 100 Bytes	Einmalig
ResvErr-Nachricht	≈ 100 Bytes	Einmalig

[a] abhängig z. B. von der Größe der transportierten Senderspezifikation (T-Spec)
[b] abhängig vom verwendeten Reservierungsstil

Tabelle 5.6: Größe, Periode und Auftreten von RSVP-Nachrichten

dauerhafte Blockierung von Ressourcen entstehen, selbst wenn man, wie in Abschnitt 5.4.3 beschrieben, Ressourcen explizit freigibt. Der Absturz eines mobilen Systems kann eine solche Situation verursachen.

Kombination von Mobile IP und RSVP

Durch die Kombination von Mobile IP und RSVP ergibt sich eine weitere Möglichkeit, den Protokolloverhead zu reduzieren. Beide Protokolle senden ihre Nachrichten periodisch, um zu überprüfen, ob der mobile Teilnehmer noch vorhanden ist. Beim gleichzeitigen Betrieb von beiden Protokollen genügt es, wenn nur eines von den beiden seine Nachrichten auf dem drahtlosen Link periodisch versendet. Bei Bedarf bekommt dann das andere Protokoll ein Signal, wenn ein mobiler Teilnehmer nicht mehr erreichbar ist.

Drei Alternativen sind denkbar:

1. Mobile IP sendet weiterhin periodische Registrierungsanforderungen über den drahtlosen Link, RSVP die Path- bzw. Resv-Nachrichten nur noch, wenn sich eine Änderung in der Path- bzw. Resv-Nachricht ergeben hat.

2. RSVP sendet periodische Path- bzw. Resv-Nachrichten und Mobile IP keine periodischen Registrierungsanforderungen.

3. Für den drahtlosen Link wird ein neues Protokoll eingeführt, welches die Signalisierung von Mobile IP und RSVP übernimmt.

Die dritte Alternative entspricht einem speziellen Routingprotokoll für den drahtlosen Link, welches gleichzeitig Dienstgüte bereitstellen kann. Dieses zu spezifizieren ist sehr aufwendig und wird hier deswegen nicht weiter verfolgt.

Der erste Alternative entspricht am ehesten den bisherigen Verbesserungsvorschlägen: Mobile IP übernimmt für RSVP die Überwachung, ob ein mobiler Teilnehmer noch vorhanden ist und kann dementsprechend wie z. B. beim expliziten Löschen von Ressourcen (siehe Abschnitt 5.4.3) ein Signal an RSVP geben, wenn der Timer für die Lebensdauer einer Registrierung abgelaufen ist. Diese Signalisierung findet zwischen Mobile IP und RSVP auf dem letzten Router vor der drahtlosen Strecke statt, im allgemeinen also auf dem Foreign Agent bzw. dem Home Agent. Im Falle eines mobilen Empfängers stellt dies kein Problem dar, weil der Router der Previous Hop ist und damit für die Reservierung der Ressourcen auf der drahtlosen Strecke verantwortlich ist. Generiert dieser Previous Hop eine ResvTear-Nachricht, werden nur die lokalen Ressourcen auf dem mobilen Empfänger nicht freigegeben.

Nachteile aller drei Alternativen sind, daß sie sich nur für Unicast RSVP-Sitzungen einsetzen lassen, weil in Multicast RSVP-Sitzungen die Mobility Agents nicht in die RSVP-Signalisierung involviert sind (siehe Abschnitt 5.4). Zusätzlich müssen bei der ersten Alternative die RSVP-Nachrichten zuverlässig versendet werden. Wegen der i. a. auf dem drahtlosen Link höheren Fehlerrate kann z. B. eine Path-Nachricht zum mobilen Empfänger verloren gehen, so daß das mobile System keine Reservierung vornehmen kann.

Unter Verwendung des schnellen Agent Discovery Verfahrens ergibt sich durch Mobile IP keine wesentliche Belegung von Bandbreite. In RSVP sind Path- bzw. Resv-Nachrichten kritisch zu betrachten, insbesondere weil zur Zeit diskutiert wird, die Periode zu verringern. Auf der drahtlosen Strecke können sie eingespart werden, wenn Mobile IP beim Ausfall eines mobilen Teilnehmers RSVP informiert.

5.4.6 Mobile IP und RSVP: Fazit

Die Integration von Mobile IP und RSVP ist also prinzipiell ohne weiteres machbar. Anpassungen sind bei der Kommunikation zwischen beiden Protokollen sowie für eine kürzere Dauer der Unterbrechung einer Reservierung nötig, außerdem auch für die Wiederherstellung einer Reservierung nach einem Subnetzwechsel. Darüberhinaus können Synergieeffekte aus der Kombination von Mobile IP und RSVP zu einer Reduktion des Protokolloverheads führen.

5.5 Zusammenfassung

Dieses Kapitel hat in einer detaillierte Analyse gezeigt, daß die Kombination von Mobilität (Mobile IP) mit der Gewährung von Dienstgüte (RSVP) unter Berücksichtigung des indirekten Transportansatzes möglich ist. Identifizierte Probleme beziehen sich hauptsächlich auf zu lange Unterbrechungszeiten im Falle eines Subnetzwechsels und die Kommunikation zwischen Ressourcenreservierungs- und mobilem Routingprotokoll.

Kapitel 6

Das Fast-Forwarding Protokoll

Dieses Kapitel beschreibt das in Abschnitt 5.1.5 eingeführte Fast-Forwarding Protokoll im Detail. Zunächst wird der Ablauf des Protokolls dargestellt. Danach erfolgt eine Betrachtung der Probleme, die sich aus der Verwendung eines unzuverlässigen Übertragungsprotokolls für die Signalisierung ergeben. Anschließend wird die Kombination des Fast-Forwarding Protokolls mit anderen Konzepten, z. B. dem indirekten Transportansatz betrachtet, gefolgt von Überlegungen zur Sicherheit hinsichtlich Angriffen von außen.

6.1 Protokollablauf und Terminologie

Den erfolgreichen bzw. nicht erfolgreichen Ablauf des Fast-Forwarding Protokolls betrachtet dieser Abschnitt. Er gibt außerdem eine Einführung in die verwendeten Begriffe. Anschließend erfolgen Betrachtungen über Besonderheiten beim Protokollablauf.

Erfolgreicher Abschluß des Fast-Forwarding Protokolls

Abbildung 6.1 zeigt eine erfolgreiche Registrierung eines mobilen Teilnehmers in einem fremden Subnetz unter Verwendung des Fast-Forwarding Protokolls:

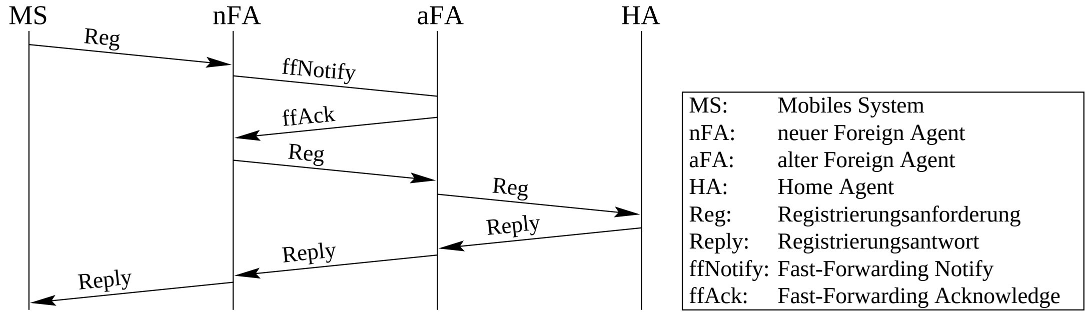

Abbildung 6.1: Weg-Zeit-Diagramm: Erfolgreiche Registrierung mit Fast-Forwarding

Zunächst meldet sich der Mobilteilnehmer nach einem Subnetzwechsel beim Foreign Agent des neuen Subnetzes, dem sog. *neuen Foreign Agent* (nFA), mit einer Registrierungsanforderung an. Mit dieser sendet er zusätzlich die IP-Adresse desjenigen Foreign Agents, bei dem er zuvor angemeldet war, dem sog. *alten Foreign Agent* (aFA). Damit signalisiert der mobile Teilnehmer dem neuen Foreign Agent, daß er den Fast-Forwarding Protokollablauf wünscht. Der neue Foreign Agent muß nun prüfen, ob er eine Registrierung mit dem Fast-Forwarding Protokoll unterstützen kann. Im positiven Fall beginnt er mit der frühen lokalen Unterstützung für das mobile System und sendet eine *Fast-Forwarding Notify* (ffNotify) Nachricht an den alten Foreign Agent. Dieser prüft ebenfalls, ob er in der Lage ist, das Fast-Forwarding Protokoll für diesen mobilen Teilnehmer zu unterstützen, z. B. ob er einen weiteren Tunnel eröffnen kann. Falls ja, löscht er seine lokale Unterstützung für das mobile System und eröffnet einen Tunnel zum neuen Foreign Agent, in den er alle vom Home Agent ankommenden, für den mobilen Teilnehmer bestimmte Nachrichten weiterleitet. Ab diesem Zeitpunkt ist die Verbindung zwischen Home Agent und Mobilteilnehmer wieder hergestellt, es können wieder Daten zu letzterem gelangen. Zuletzt sendet der alte Foreign Agent eine *Fast-Forwarding Acknowledge* (ffAck) Nachricht als Bestätigung an den neuen Foreign Agent. Damit ist die Signalisierung des Fast-Forwarding Protokolls abgeschlossen.

Periodische Registrierung Da auch bei der Erweiterung von Mobile IP um das Fast-Forwarding Protokoll eine Registrierung nur für eine bestimmte Lebensdauer gültig sein soll, müssen auch weiterhin Registrierungsanforderungen zum Home Agent gelangen. Aus diesem Grund leitet der neue Foreign Agent unmittelbar nach dem Empfangen der Bestätigung vom alten Foreign Agent die Registrierungsanforderung vom mobilen System an den alten Foreign Agent weiter. Dieser sendet die (modifizierte) Nachricht (siehe Abschnitt 6.1.1) an den Home Agent weiter, welcher seinen Registrierungstimer neu initialisieren kann. Da für den Home Agent das Fast-Forwarding transparent ist, sendet er die Registrierungsantwort an den alten Foreign Agent. Dieser erhält damit auch die Gelegenheit, seinen Registrierungtimer neu zu setzen. Er leitet diese Nachricht anschließend an den neuen Foreign Agent weiter, der ebenfalls seinen Timer erneuert und die Nachricht dem mobilen Teilnehmer übergibt. Damit hat auch dieser die Rückmeldung bekommen, daß die Mobile IP Signalisierung erfolgreich war und kann seine Timer entsprechend setzen.

Diese Mobile IP Signalisierung findet zwar wieder zwischen Home Agent und Mobilteilnehmer statt und benötigt wegen des Weitverkehrsszenarios eine gewisse Zeit; da aber nur der Kontroll- und nicht der Datenfluß betroffen ist, wird die Mobile IP Handover-Zeit nicht negativ beeinflußt.

Ablehnen des Fast-Forwardings

Drei Gründe können auftreten, warum das Fast-Forwarding Protokoll nicht erfolgreich angewendet werden kann:

1. Der neue Foreign Agent hat nicht genug Ressourcen.

2. Der neue Foreign Agent kennt das Fast-Forwarding Protokoll nicht und ignoriert die vom mobilen System mit der Registrierungsanforderung versendete IP-Adresse des alten Foreign Agents.

3. Der alte Foreign Agent hat nicht genug Ressourcen, kann z. B. keinen Tunnel zum neuen Foreign Agent eröffnen.

Im letzten Fall sendet der alte Foreign Agent eine *Fast-Forwarding Negative Acknowledge* (ffNack) Nachricht als Ablehnung an den neuen Foreign Agent (siehe Abbildung 6.2).

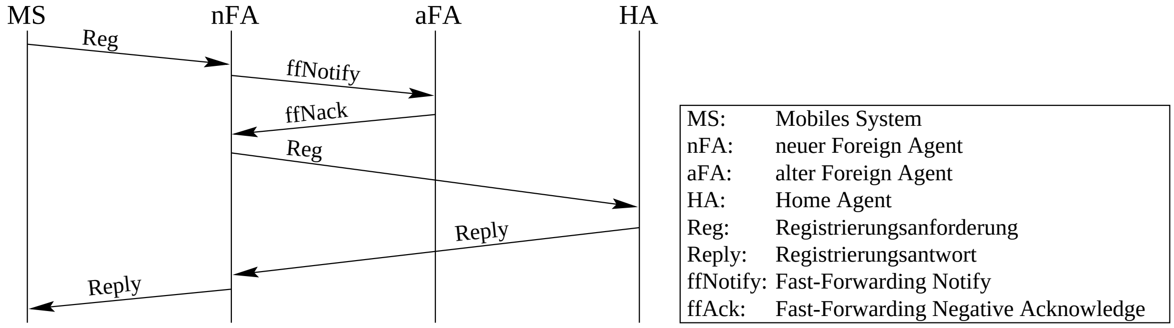

Abbildung 6.2: Weg-Zeit-Diagramm: Registrierung vom alten Foreign Agent abgelehnt

In allen drei Fällen muß sich der neue Foreign Agent direkt beim Home Agent anmelden, er initiiert damit einen Subnetzwechsel wie in Mobile IP.

Die Forwardingkette

Wendet man das Fast-Forwarding Protokoll mehrfach hintereinander an, wird bei jedem Subnetzwechsel ein weiterer Foreign Agent in das Forwarding der Nachrichten an den mobilen Teilnehmer verwickelt. Es bildet sich eine sog. *Forwardingkette* (siehe Abbildung 6.3).

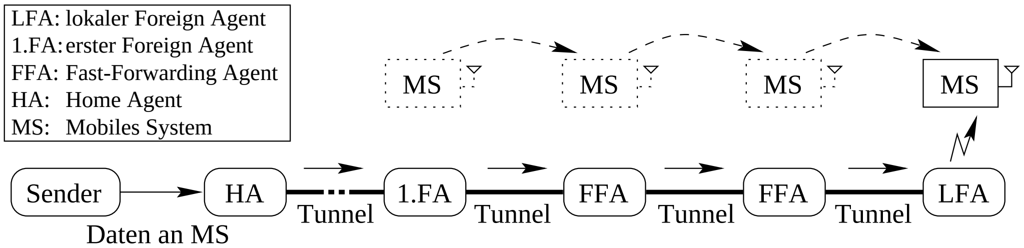

Abbildung 6.3: Die Forwardingkette

Der Foreign Agent, der über einen wegen des Weitverkehrsszenarios langen Tunnel direkten Kontakt zum Home Agent hat, wird *erster Foreign Agent* (1.FA) genannt, der

Foreign Agent mit direktem Kontakt zum mobilen System heißt *lokaler Foreign Agent* (LFA). Alle Foreign Agents zwischen dem Home Agent und dem lokalen Foreign Agent werden *Fast-Forwarding Agents* (FFA) genannt, weil ihre einzige Aufgabe darin besteht, alle Daten zum Mobilteilnehmer unverzüglich weiterzuleiten. Der erste Foreign Agent ist also ein besonderer Fast-Forwarding Agent. Sollte sich auf der Strecke vom Home Agent zum mobilen System nur ein Foreign Agent befinden (wie im ursprünglichen Mobile IP), gibt es keine Fast-Forwarding Agents, der Foreign Agent aus Mobile IP entspricht dann dem lokalen Foreign Agent.

Damit wird der alte Foreign Agent bei einem erfolgreichen Ablauf des Fast-Forwardings zu einem Fast-Forwarding Agent, d. h. er hat keinen direkten Kontakt zum mobilen Teilnehmer. Der neue Foreign Agent wird zum lokalen Foreign Agent, der als einziger Foreign Agent in der Forwardingkette eine lokale Unterstützung für den Mobilteilnehmer bereitstellt.

6.1.1 Modifikation der Registrierungsanforderung

Beim Weiterleiten der unmodifizierten Registrierungsanforderung vom Mobilteilnehmer zum Home Agent ergibt sich das folgende Problem:

In der Registrierungsanforderung setzt das mobile System nach einem Subnetzwechsel als Care-of Adresse die des neuen Foreign Agents ein. Nach erfolgreicher Beendigung des Fast-Forwardings leitet der neue Foreign Agent die Registrierungsanforderung weiter, so daß sie zum Home Agent kommt. Dieser wertet sie aus und stellt im Vergleich mit der letzten Registrierungsanforderung fest, daß eine neue Care-of Adresse vorliegt. Deswegen leitet er einen Subnetzwechsel ein, d. h. eröffnet einen Tunnel zum neuen Foreign Agent und sendet die Registrierungsantwort direkt zu diesem. Das Fast-Forwarding würde somit nicht funktionieren.

Lösung Dem Home Agent muß vorgetäuscht werden, daß der mobile Teilnehmer immer noch beim ersten Foreign Agent in der Forwardingkette angemeldet ist. Dann sendet der Home Agent weiterhin alle Daten zum mobilen Teilnehmer in den Tunnel zum ersten Foreign Agent, also entlang der Forwardingkette. Ein erster Ansatz ist, daß der erste Foreign Agent in jeder Registrierungsanforderung, die er vom mobilen System erhält, die Care-of Adresse durch seine eigene Adresse ersetzt. Dieses Vorgehen muß aus Sicherheitsgründen aber noch modifiziert werden (siehe Abschnitt 6.6.1).

6.1.2 Beenden des Fast-Forwardings

Wie schon am Ende vom Abschnitt 5.1.5 gesagt, gibt es Situationen, in denen die direkte Registrierung des neuen Foreign Agents beim Home Agent gegenüber dem Fortsetzen des Fast-Forwardings vorzuziehen ist. Abbildung 6.4 zeigt eine beispielhafte Situation.

Das mobile System bewegt sich räumlich gesehen mit jedem Subnetzwechsel näher an sein Heimatsubnetz heran, so daß sich z. B. für die Strecke über die Forwardingkette eine höhere Verzögerung ergibt als für die direkte Strecke vom Home Agent zum lokalen Foreign

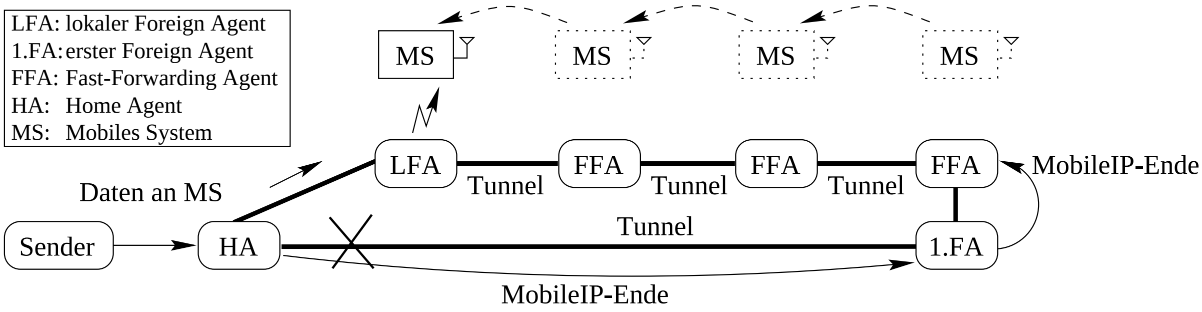

Abbildung 6.4: Beenden des Fast-Forwardings

Agent. In diesem Fall soll sich der lokale Foreign Agent direkt beim Home Agent anmelden, der dann eine Mobile IP-Ende Nachricht entlang der alten Forwardingkette schickt, um die belegten Ressourcen (Tunnel etc.) wieder freizugeben.

Damit erhält eine Mobile IP-Ende Nachricht durch das Fast-Forwarding Protokoll eine erweiterte Semantik: Sie wird jetzt nicht mehr nur an den alten Foreign Agent geschickt, um die lokale Unterstützung nach einem Subnetzwechsel aufzuheben (siehe Abschnitt 5.1.3). Zusätzlich dient sie auch als Nachricht für Fast-Forwarding Agents, das Fast-Forwarding für einen bestimmten mobilen Teilnehmer zu beenden.

Eine Betrachtung, unter welchen Bedingungen dieses Vorgehen anzuwenden ist oder wie man ermittelt, ob die Strecke über die Forwardingkette „schlechter“ ist als die direkte Verbindung, erfolgt in dieser Arbeit nicht.

6.2 Schleifenbildung und deren Behebung

Abbildung 6.5 zeigt eine Situation, in der ein Mobilteilnehmer in ein Subnetz zurückwechselt, in dem er bereits gewesen ist.

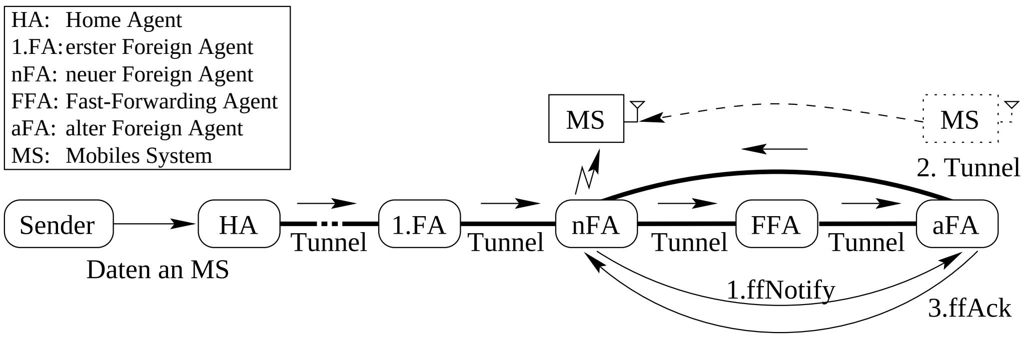

Abbildung 6.5: Schleifenbildung in einer Forwardingkette

Der Mobility Agent in dem neuen Subnetz soll bis vor dem letzten Subnetzwechsel den

Mobilteilnehmer als Fast-Forwarding Agent unterstützt haben, so daß seine Registrierungstimer noch nicht abgelaufen sind. Wendet man den oben geschilderten Protokollablauf an, kommt es zur in der Abbildung dargestellten Situation:

Zunächst sendet der neue Foreign Agent eine Nachricht an den alten Foreign Agent (1.ffNotify), der daraufhin einen Tunnel zum neuen Foreign Agent aufbaut (2.Tunnel) und eine Bestätigung an diesen sendet (3.ffAck). Sobald der neue Foreign Agent aber mit der lokalen Unterstützung für den Mobilteilnehmer beginnt, gelangen Daten für diesen nicht mehr in den Tunnel zum Fast-Forwarding Agent FFA, sondern werden lokal ausgeliefert. Es hat sich eine sog. *Routingschleife* auf der Strecke nFA–FFA–aFA–nFA gebildet, die nicht mehr in den regulären Datentransfer vom Home Agent zum mobilen Teilnehmer involviert ist. Damit können die Tunnel auf der Strecke nFA–FFA–aFA gelöscht werden. Der alte Foreign Agent muß erst gar keinen direkten Tunnel zum neuen Foreign Agent eröffnen. Der einzig denkbare Verwendungszweck ist, daß durch die Routingschleife Daten, die sich bereits auf der alten Strecke nFA–aFA befinden, über den direkten Tunnel vom alten zum neuen Foreign Agent doch noch zum Mobilteilnehmer gelangen. Da die Fast-Forwarding Agents aber relativ dicht beieinander liegen, ist die Datenmenge eher klein und dieses Vorgehen unnötig.

Im hier gezeigten Fall einer Schleifenbildung ist der normale Ablauf des Fast-Forwarding Protokolls mit dem Aussenden der Fast-Forwarding Notify und Fast-Forwarding Acknowledge überflüssig.

Lösung Eine Lösung dieses Problems wird in Abbildung 6.6 dargestellt:

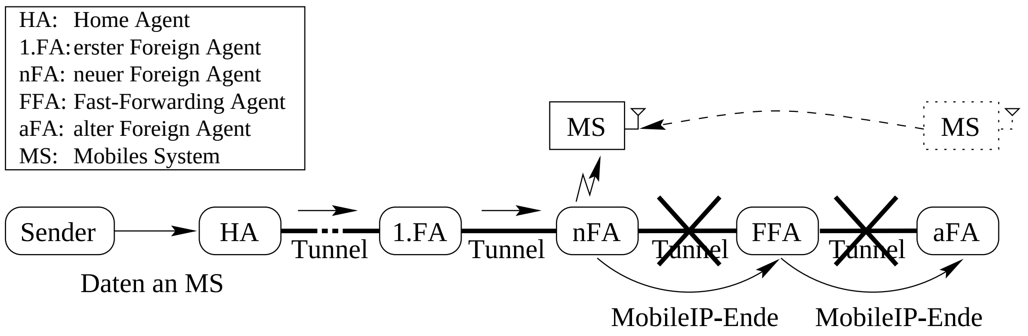

Abbildung 6.6: Schleifenbehebung in einer Forwardingkette

Anstelle eine Fast-Forwarding Notify an den alten Foreign Agent zu schicken, hört der neue Foreign Agent auf, Daten zum Mobilteilnehmer in den Tunnel zum Fast-Forwarding Agent zu senden, und beginnt mit der lokalen Unterstützung für das mobile System. Anschließend schickt er eine Mobile IP-Ende Nachricht an den Fast-Forwarding Agent FFA, damit dieser weiß, daß er nicht mehr Mitglied der Forwardingkette ist und die dadurch belegten Ressourcen (z. B. Tunnel) freigeben kann. Dieser leitet die Mobile IP-Ende Nachricht weiter, so daß sie hop-by-hop bis zum Ende der Forwardingkette, also zum alten Foreign Agent, gelangt.

6.2.1 Erkennung einer Schleife in der Forwardingkette

Im Falle einer Schleifenbehebung stellt sich die Frage, wie ein neuer Foreign Agent, bei dem sich ein Mobilteilnehmer lokal anmeldet, erkennt, ob eine Schleife vorliegt.

Notwendige Bedingung Im ersten Ansatz prüft der neue Foreign Agent, ob er bereits für das sich anmeldende mobile System einen Tunnel zu einem anderen Fast-Forwarding Agent eingerichtet hat, d. h. er selbst als Fast-Forwarding Agent arbeitet. In diesem Fall kann eine Schleife vorliegen (notwendige Bedingung).

Das Beispiel in Abbildung 6.7 zeigt aber, daß dies keine hinreichende Bedingung ist:

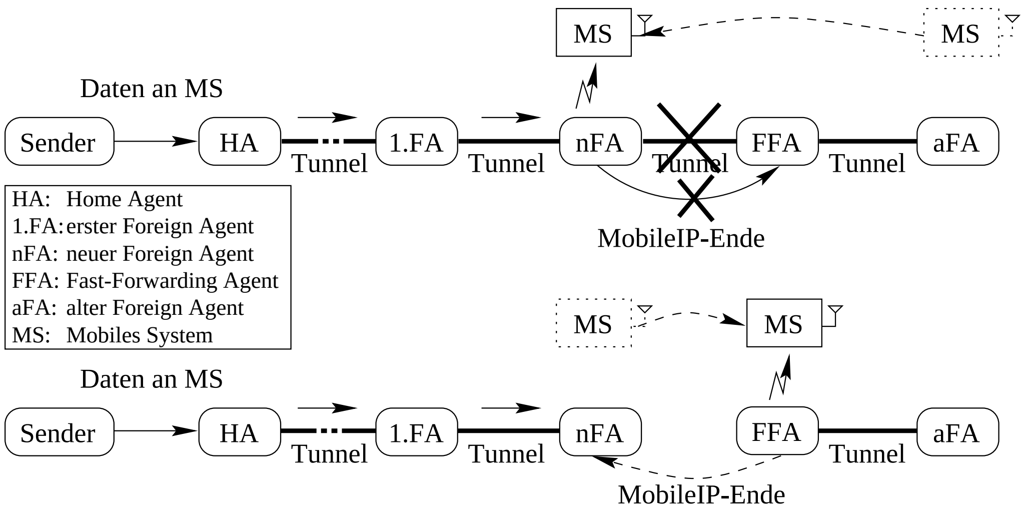

Abbildung 6.7: Schleifenerkennung bei verlorengegangener Mobile IP-Ende Nachricht

Zunächst wechselt der Mobilteilnehmer wie in Abbildung 6.6 vom alten zum neuen Subnetz und meldet sich beim neuen Foreign Agent nach der oben genannten Vorgehensweise mit Schleifenauflösung an. Die Mobile IP-Ende Nachricht zum Fast-Forwarding Agent soll jedoch in diesem Szenario verlorengehen. Dadurch kann zwar der neue Foreign Agent noch den Tunnel zum Fast-Forwarding Agent FFA löschen, der Tunnel von letzterem zum alten Foreign Agent aFA bleibt aber erhalten. Zwei Fälle können eintreten:

1. Wechselt der mobile Teilnehmer, wie im unteren Teil der Abbildung 6.7 dargestellt, zum Subnetz des Fast-Forwarding Agents FFA und meldet sich bei diesem an, ergäbe eine Prüfung durch den FFA anhand der notwendigen Bedingung, daß eine Schleife vorliegt (sofern der Registrierungstimer noch nicht abgelaufen ist). Durch diese Fehlannahme würde dieser eine Mobile IP-Ende Nachricht an den neuen Foreign Agent schicken und selbst nur die lokale Unterstützung für den Mobilteilnehmer errichten. Die Verbindung HA–FFA ist aber unterbrochen, d. h. der mobile Teilnehmer ist vom Home Agent nicht mehr zu erreichen.

2. Wechselt der mobile Teilnehmer anstelle zum Fast-Forwarding Agent zurück zum alten Subnetz, stellt der alte Foreign Agent fest, daß er selbst das mobile System zuletzt lokal unterstützt hat (wenn der Registrierungstimer noch nicht abgelaufen ist). Daraufhin unternimmt er überhaupt nichts, obwohl auch hier die Verbindung HA–aFA unterbrochen ist.

Das Problem besteht also immer dann, wenn der Mobilteilnehmer zu einem Foreign Agent kommt, der sich in einem durch eine verlorengegangene Mobile IP-Ende Nachricht abgehängten Teil einer Forwardingkette befindet, wobei der Registrierungstimer des Foreign Agents noch nicht abgelaufen ist.

Hinreichende Bedingung Eine Lösung liegt darin, daß der neue Foreign Agent in seiner Eigenschaft als Fast-Forwarding Agent alle Registrierungsanforderungen vom mobilen System in Richtung Home Agent weiterleiten muß. Befindet er sich wegen des Verlustes einer Mobile IP-Ende Nachricht in einem abgehängten Teil einer Forwardingkette, verpaßt er mindestens eine Registrierungsanforderung, nämlich die, die das Aussenden derjenigen Mobile IP-Ende Nachricht ausgelöst hat, die dann verlorengegangen ist.

Damit läßt sich also eine hinreichende Bedingung für die Erkennung einer Schleife formulieren: Wenn der neue Foreign Agent das mobile System als Fast-Forwarding Agent unterstützt und zusätzlich ihn alle Registrierungsanforderungen vom mobilen System passiert haben, dann ist es sicher, daß eine Schleife vorliegt und daß zumindestens bei der letzten Registrierung die Strecke vom Home Agent zum neuen Foreign Agent noch intakt gewesen ist. Hat der neue Foreign Agent dagegen mindestens eine Registrierungsanforderung verpaßt, kann er davon ausgehen, daß eine Mobile IP-Ende Nachricht verlorengegangen ist. Damit liegt keine Schleife vor, er kann also den normalen Ablauf des Fast-Forwarding Protokolls mit dem Senden einer Fast-Forwarding Notify initiieren.

Erkennung des Verlustes einer Mobile IP-Ende Nachricht Für die Erkennung, ob ein Fast-Forwarding Agent alle bisherigen Registrierungsanforderungen erhalten hat, gibt es zwei Möglichkeiten:

1. Einführung einer Sequenznummer in der Registrierungsanforderung

2. Verwenden der Nonces (vgl. Seite 17)

Die zweite Möglichkeit hat den Vorteil, daß keine zusätzliche Signalisierung nötig ist, falls Replay Protection mit Nonces in der Mobile IP Implementierung realisiert ist. Die Implementierung von Nonces ist aber optional [Per96, S. 68]. Andernfalls bietet die erste Möglichkeit eine gleichwertige Funktionalität mit dem Nachteil einer geringfügig erweiterten Registrierungsanforderung.

Die Vorgehensweise ist wie folgt: Der Fast-Forwarding Agent speichert immer die Sequenznummer bzw. die Nonce aus der zuletzt erhaltenen Registrierungsantwort. Meldet sich ein mobiles System direkt bei einem Fast-Forwarding Agent an, vergleicht dieser im ersten Fall, ob die neue Sequenznummer direkt auf der gespeicherten folgt, und im zweiten

Fall, ob die höherwertigen 32 Bits der neuen Nonce mit den höherwertigen 32 Bits der alten Nonce übereinstimmen. Ist der Test positiv, liegt eine Schleife vor. Ist er negativ, hat der Fast-Forwarding Agent mindestens eine Registrierungsanforderung verpaßt, damit ist eine Mobile IP-Ende Nachricht verlorengegangen. Da es dann keine Schleife gibt, kann der Fast-Forwarding Agent in seiner Eigenschaft als neuer Foreign Agent einen Tunnel vom alten Foreign Agent mittels einer Fast-Forwarding Notify anfordern.

6.3 Unzuverlässigkeit der verwendeten Nachrichten

Wie im vorherigen Abschnitt gezeigt, entstehen Probleme, weil sowohl Mobile IP als auch das Fast-Forwarding Protokoll ihre Nachrichten mit einem unzuverlässiges Protokoll verschicken. Deswegen sollen in diesem Abschnitt alle Nachrichten von Mobile IP und dem Fast-Forwarding Protokoll auf die Konsequenzen durch Verlust, Reihenfolgevertauschung und Verdopplung untersucht werden.

6.3.1 Registrierungsanforderung

Eine Registrierungsanforderung kann so lange im Netz verzögert werden, daß das mobile System eine Wiederholung anstößt. Damit besteht die Möglichkeit, daß zwei gleiche Registrierungsanforderungen beim Home Agent ankommen. Beide enthalten aber dieselben Nonces bzw. Sequenznummern, so daß der Home Agent die Verdopplung durch die Replay Protection erkennen kann. Diese dient eigentlich als Schutz gegen durch ein fremdes System verdoppelte Registrierungsanforderungen (vgl. Seite 16), sie bewirkt aber allgemein die Erkennung von verdoppelten Nachrichten. Eine Reihenfolgevertauschung von Nachrichten kann in Mobile IP und dem Fast-Forwarding Protokoll nicht auftreten, weil beide Protokolle nur jeweils eine einzelne Nachricht versenden und dann auf eine Antwort warten.

Verlorene Registrierungsanforderungen Problematisch sind Verluste von Registrierungsanforderungen in Verbindung mit Subnetzwechseln. Abbildung 6.8 zeigt ein Beispiel.

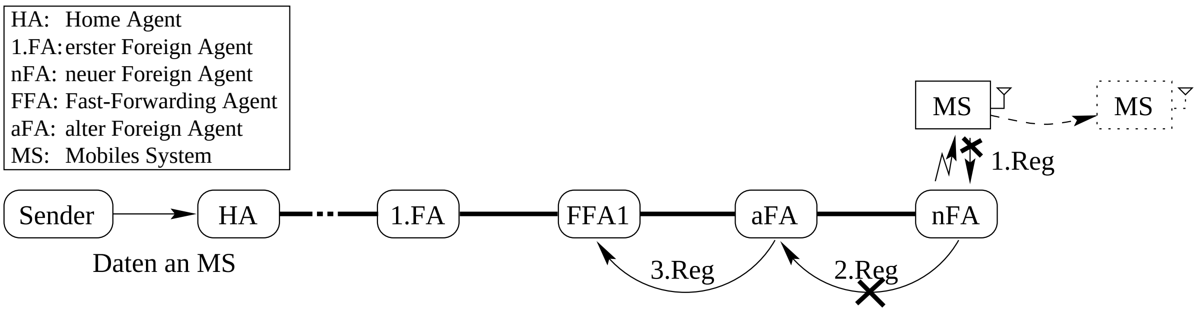

Abbildung 6.8: Verlust einer Registrierungsanforderung vor einem Subnetzwechsel

Dem mobilen System ist nicht bekannt, ob die Registrierungsanforderung auf dem drahtlosen Link zum neuen Foreign Agent verlorengegangen ist (1.Reg) oder innerhalb der Forwardingkette, also nach Beendigung des Fast-Forwarding Protokolls (2.Reg). Im ersten Fall bestünde der Tunnel zwischen dem alten und dem neuen Foreign Agent noch nicht, während im zweiten Fall diese Verbindung vorhanden wäre. Wechselt der Mobilteilnehmer in ein anderes Subnetz, bevor er die Registrierungsanforderung wiederholen kann, gibt es auf dem mobilen System und auch bei dem Mobility Agent des neuen Subnetzes keine zuverlässige Information, ob die Forwardingkette nutzbar ist oder nicht.

Als erste Lösung könnte das mobile System den Foreign Agent als letzten Foreign Agent angeben, bei dem die letzte erfolgreiche Registrierung stattgefunden hat. Das funktioniert aber dann nicht mehr, wenn die erfolglose Registrierung bei einem Fast-Forwarding Agent stattgefunden hat und er anschließend zu einem Fast-Forwarding Agent in einem möglicherweise abgehängten Teil der Forwardingkette wechselt. Abbildung 6.9 zeigt ein solches Szenario.

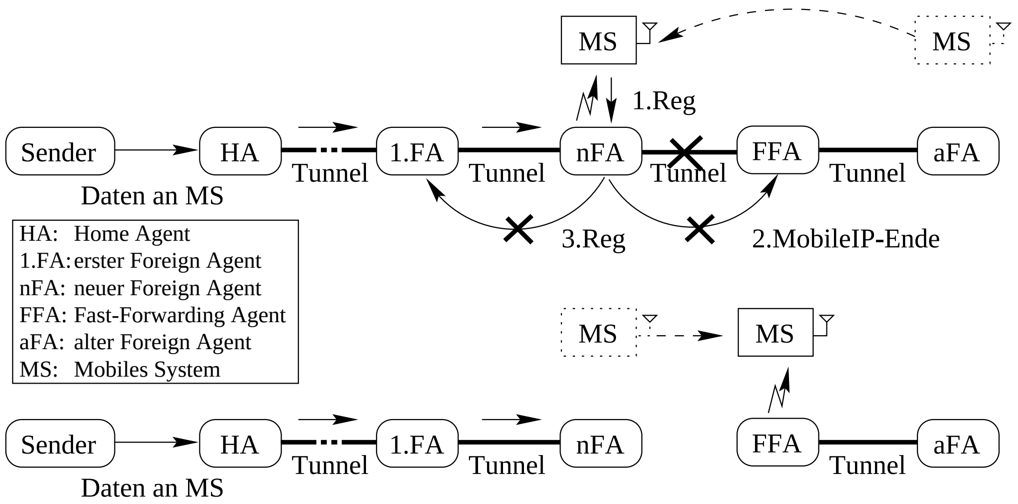

Abbildung 6.9: Verlust einer Registrierungsanforderung bei einem Fast-Forwarding Agent

Das mobile System war korrekt beim alten Foreign Agent angemeldet und wechselt nun zu einem ehemaligen Fast-Forwarding Agent, der damit zu seinem neuen Foreign Agent wird. Diesem sendet er eine Registrierungsanforderung (1.Reg), so daß der neue Foreign Agent eine Schleifenauflösung betreibt und den Tunnel zu FFA löscht. Die anschließend ausgesendete MobileIP-Ende Nachricht geht in diesem Szenario aber verloren, ebenso die Registrierungsanforderung auf dem Weg zum Home Agent (3.Reg). Wechselt der Mobilteilnehmer, wie im unteren Teil der Abbildung dargestellt, zu einem anderen ehemaligen Fast-Forwarding Agent, bevor er die verlorengegangene Registrierungsanforderung wiederholt, entsteht das folgende Problem: Als erste Lösung soll der Mobilteilnehmer den alten Foreign Agent in der Registrierungsanforderung als denjenigen Foreign Agent angeben, bei dem er zuletzt erfolgreich registriert war. Der Fast-Forwarding Agent FFA unternimmt eine Schleifenerkennung, weil er noch als Fast-Forwarding Agent für das mobile System arbeitet, und stellt fest, daß er eine Registrierungsanforderung verpaßt hat (1.Reg). Daraus folgert er, daß keine Schleife vorliegt und initiiert das Fast-Forwarding Protokoll mit dem alten Foreign Agent, indem er eine Fast-Forwarding Notify an diesen schickt. Daß die Forwardingkette auf der Strecke HA–FFA aber unterbrochen ist, kann er nicht feststellen.

Lösung Da diese Situation des Verlustes einer Nachricht kombiniert mit einem Subnetzwechsel vor der Wiederholung der Registrierung ein selten auftretender Fall ist, wird hier eine einfache Lösung vorgeschlagen, um das Fast-Forwarding Protokoll nicht durch die Fehlerbehandlung vieler Spezialfälle unnötig komplex zu gestalten: Falls das mobile System eine Registrierung mit einem Foreign Agent nicht erfolgreich beenden konnte und danach zu einem anderen Subnetz wechselt, soll das Fast-Forwarding Protokoll nicht angewendet werden; d. h. der Foreign Agent im neuen Subnetz muß sich in diesem Fall direkt beim Home Agent anmelden.

6.3.2 Registrierungsantwort

Für die Verdopplung bzw. Reihenfolgevertauschung gelten dieselben Aussagen wie bei Registrierungsanforderungen. Der Verlust einer Registrierungsantwort bedeutet zwar, daß zumindest das Fast-Forwarding Protokoll erfolgreich abgeschlossen wurde und die Forwardingkette damit intakt bzw. bei einer Schleifenauflösung nicht mehr intakt ist. Da aber das mobile System nicht unterscheiden kann, ob die Registrierungsanforderung oder die Registrierungsantwort verlorengegangen ist, gibt es als einfache Lösung im Falle eines Verlustes einer Registrierungsantwort in Kombination mit einem Subnetzwechsel ebenfalls nur den Weg der direkten Registrierung beim Home Agent.

6.3.3 Nachrichten des Fast-Forwarding Protokolls

Kommt eine Fast-Forwarding Notify für ein mobiles System bei einem Mobility Agent an, der dieses bereits als Fast-Forwarding Agent unterstützt, ignoriert er diese Nachricht. Doppelt beim neuen Foreign Agent ankommenden Fast-Forwarding Bestätigungen bzw. Ablehnungen ignoriert dieser ebenfalls. Reihenfolgevertauschungen spielen keine Rolle, da das Fast-Forwarding Protokoll nicht mehr als eine Nachricht pro Anmeldung je Richtung austauscht.

Für den Verlust einer dieser drei Nachrichten gilt dieselbe Aussage wie beim Verlust einer Registrierungsanforderung: Das mobile System kann nicht feststellen, ob die Fast-Forwarding Notify verloren ging und damit der alte Foreign Agent noch keinen Tunnel zum neuen Foreign Agent eröffnet hat, oder ob eine Bestätigung bzw. Ablehnung verlorengegangen ist und damit möglicherweise ein Tunnel besteht. Auch hier bleibt als einfache Lösung nur die direkte Registrierung des neuen Foreign Agents beim Home Agent.

6.3.4 Fazit

Durch das Versenden der Nachrichten des Fast-Forwarding Protokolls und von Mobile IP mit einem unzuverlässigen Transportprotokoll können also komplexe Situationen entstehen, die nur mit großen Schwierigkeiten unter Beibehaltung des Fast-Forwarding zu beheben sind. Da diese Situationen nur selten eintreten, soll als einfache Lösung das Fast-Forwarding beendet werden.

6.4 Fast-Forwarding und Route Optimization

Um die Problematik des Dreiecksroutings in Mobile IP zu beheben, wurde das Verfahren der Route Optimization [JohPer97] vorgeschlagen. Dieses läßt sich sehr gut mit dem Fast-Forwarding Protokoll einsetzen, weil die Route Optimization hauptsächlich Änderungen am Sender (Binding Cache) und am Home Agent (Senden der Binding Update Nachricht) vornimmt. Das Fast-Forwarding Protokoll dagegen betrifft hauptsächlich Änderungen am Foreign Agent und (wenige) am mobilen System (siehe Abschnitt 7.5.1). Bei der Route Optimization nimmt das Verfahren zum Smooth Handoff zwar auch Änderungen am Foreign Agent vor; diese decken sich in vielen Dingen mit den Mechanismen des Fast-Forwarding Protokolls, z. B. entspricht die Binding Update Nachricht in der Funktion der Fast-Forwarding Notify. Bei einer Kombination beider Verfahren sind also zusätzliche Synergieeffekte zu erwarten, diese sollen in dieser Arbeit aber nicht weiter betrachtet werden.

Damit lassen sich sowohl das Problem des Dreiecksroutings als auch das der langen Unterbrechungszeiten bei Weitverkehrsszenarien beheben. Voraussetzung ist allerdings auch hier, daß der Betrieb mit einem Foreign Agent Verwendung findet, nicht der co-located Betrieb.

6.5 Fast-Forwarding mit indirektem Transportansatz

In den folgenden Abschnitten findet eine Betrachtung der bisher entwickelten Konzepte des Fast-Forwarding Protokolls unter Berücksichtigung des indirekten Transportansatzes statt. Dabei muß die Plazierung des Transport Gateways und die Beendigung einer Forwardingkette beachtet werden.

6.5.1 Plazierung des Transport Gateways

Im Falle einer Kombination des Fast-Forwarding Protokolls mit dem indirekten Transportansatz entsteht wie in Abschnitt 5.2.1 das Problem der Plazierung des Transport Gateways. Grundsätzlich kommen alle Fast-Forwarding Agents und der lokale Foreign Agent in Frage, weil alle Daten zum mobilen System diese passieren.

Transport Gateway auf dem lokalen Foreign Agent

Im ersten Ansatz soll sich das Transport Gateway immer auf dem lokalen Foreign Agent befinden, so daß die Verbindung für die drahtlose Strecke möglichst kurz ist. Damit nicht bei jedem Subnetzwechsel eine Migration nötig ist, wird hier der Ansatz der Delayed Migration betrachtet. Im Falle eines Subnetzwechsels verbleibt das Transport Gateway also zunächst noch auf dem alten Foreign Agent, so daß die Verbindung für die drahtlose Strecke auf der Strecke vom alten Foreign Agent zum Mobilteilnehmer besteht. Das Transport Gateway wird erst später zu einem geeigneten Zeitpunkt migriert. Für die Bestimmung dieses Zeitpunktes ist noch ein geeignetes Verfahren zu entwickeln, was aber in dieser Arbeit nicht betrachtet wird.

Abbildung 6.10 zeigt ein Beispiel einer verzögerten Migration in einer Forwardingkette.

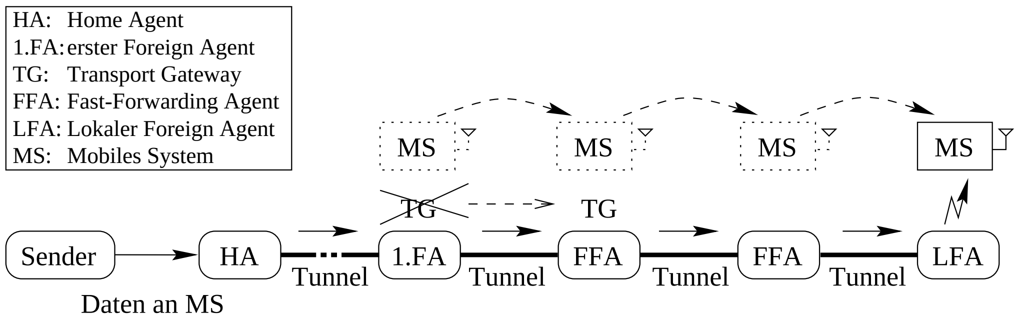

Abbildung 6.10: Plazierung des Transport Gateways unter Einsatz des Fast-Forwardings

Das Transport Gateway ist migriert worden, nachdem der Mobilteilnehmer vom ersten Foreign Agent zum jetzigen ersten Fast-Forwarding Agent gewechselt hat. Wechselt der mobile Teilnehmer sehr schnell in weitere Subnetze, wird das Transport Gateway nicht bei jedem Subnetzwechsel auf den entsprechenden neuen Foreign Agent migriert, damit nicht bei jedem Wechsel eine Migrationspause entsteht. In der Abbildung hat das mobile System die letzten beiden Subnetzwechsel sehr schnell vollzogen, so daß das Transport Gateway immer noch beim ersten Fast-Forwarding Agent lokalisiert ist. Die verzögerte Migration kann so auch mit oszillierenden Subnetzwechseln umgehen, das Transport Gateway bleibt dann ebenfalls fest auf einem Foreign Agent.

Problem Schleifenauflösung Es treten allerdings Probleme in Verbindung mit der Schleifenauflösung auf. Abbildung 6.11 zeigt dazu ein Beispiel.

Plaziert man das Transport Gateway auf dem lokalen Foreign Agent, kann durch eine Schleifenauflösung die Situation auftreten, daß sich das Transport Gateway nicht mehr auf der Strecke vom Home Agent zum Mobilteilnehmer befindet und damit nicht mehr funktionstüchtig ist. Diese Situation kann auch im Falle einer verzögerten Migration auftreten.

Man könnte als erste Lösung die Errichtung der lokalen Unterstützung auf dem neuen Foreign Agent so lange verzögern, bis das Transport Gateway vom alten zum neuen For-

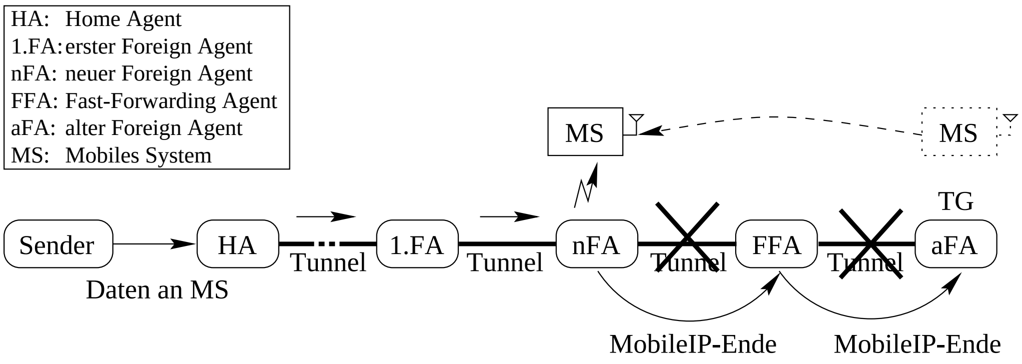

Abbildung 6.11: Problem: Schleifenauflösung und Plazierung des Transport Gateways

eign Agent migriert ist. Die Unterbrechung der Verbindung zum mobilen System wäre dann aber sehr lang.

Alternativ könnte man, wie in Abschnitt 6.2 erwähnt, die Tunnel auf der Strecke nFA–FFA–LFA bestehen lassen und zusätzlich einen direkten Tunnel vom alten Foreign Agent zum neuen eröffnen. Dann müßte der neue Foreign Agent alle Daten für den mobilen Teilnehmer, die vom Sender kommen, durch den Tunnel zum Fast-Forwarding Agent senden. Erhält er dieselben Daten vom alten Foreign Agent, muß er sie lokal an das mobile System ausliefern. Auf diese Weise könnte das Transport Gateway zunächst auf dem alten Foreign Agent verbleiben, es bekäme auch weiterhin alle Daten zum mobilen Teilnehmer zur Bearbeitung. Nachteil dieses Vorgehens ist, daß die Daten zum Mobilteilnehmer einen Umweg über den alten Foreign Agent nehmen und daß das Weiterleiten der Daten auf dem neuen Foreign Agent komplexer wird.

Lösung: Transport Gateway auf ersten Foreign Agent Ein einfachere Lösung liegt darin, das Transport Gateway auf einen kaum von Subnetzwechseln betroffenen Mobility Agent zu legen: den ersten Foreign Agent. Dieser befindet sich unabhängig von Schleifenauflösungen immer in der Forwardingkette, außer der mobile Teilnehmer kehrt in das Heimatsubnetz zurück oder die Forwardingkette wird beendet.

Vorteil dieses Verfahrens ist, daß eine Migration des Transport Gateways nur selten vorgenommen werden muß.

Ein Nachteil ist, daß die Strecke vom Transport Gateway zum mobilen Teilnehmer länger wird und größtenteils drahtgebunden ist. Die Aufteilung der Verbindung durch den indirekten Transportansatz hatte ursprünglich den Zweck, die drahtlose Strecke von der drahtgebundenen zu trennen. Desweiteren laufen auf dieser Strecke Nachrichten zum mobilen System noch durch mehrere Tunnel, was einen zusätzlichen Overhead beinhaltet. Da aber eine direkte Verbindung zum Home Agent dem weiteren Benutzen der ungünstigeren Forwardingkette unter bestimmten Voraussetzungen vorgezogen wird (siehe Abschnitt 6.1.2), sollte sich dieser zusätzliche Overhead sowie die Länge der Strecke vom ersten Foreign Agent mit dem Transport Gateway zum mobilen System in Grenzen halten.

6.5.2 Mobiles System als Sender

Ein weiteres Problem des indirekten Transportansatzes ist, daß auch alle vom mobilen Teilnehmer gesendeten Daten das Transport Gateway passieren müssen. Das heißt in diesem Fall, daß das mobile System seine zu sendenden Daten zunächst zum System mit dem Transport Gateway schicken muß, welches sie dann an den Empfänger weiterleitet. Dieses kann einen Umweg bedeuten. Das Transport Gateway sollte allerdings nicht allzu weit entfernt vom Subnetz liegen, in dem sich der Mobilteilnehmer gerade befindet, weil sonst eine Beendigung des Fast-Forwarding in Betracht gezogen würde (vgl. Abschnitt 6.1.2). Man könnte in das Kriterium, wann die Forwardingkette aufzugeben ist, auch die Betrachtung des indirekten Transportansatzes einfließen lassen.

Für das Versenden der Nachrichten vom mobilen System zum Transport Gateway existieren zwei Möglichkeiten:

1. Das mobile System selbst tunnelt die Nachrichten direkt zum Transport Gateway.
2. Es sendet alle Daten zum lokalen Foreign Agent, der sie über einen bidirektionalen Tunnel zu seinem Vorgänger in der Forwardingkette sendet, der sie dann ebenfalls zum Vorgänger schickt, bis sie beim ersten Foreign Agent angekommen sind.

Die erste Möglichkeit ist am einfachsten zu implementieren. Das mobile System kapselt lediglich alle zu sendenden Pakete in einen zusätzlichen IPIP-Header ein, so daß dann das IP-Standardrouting die Pakete zum Transport Gateway befördert. Ein Nachteil ist aber, daß für die Implementierung des Fast-Forwarding Protokolls das mobile System eine weitere Veränderung erfährt, obwohl dieses für das mobile System transparent bleiben sollte.

Die zweite Möglichkeit ist dagegen sehr aufwendig zu implementieren, da die Fast-Forwarding Agents alle empfangenen Nachrichten daraufhin untersuchen müssen, ob sie von einem mobilen Teilnehmer gesendet wurden, den sie als Fast-Forwarding Agent unterstützen. Dies erfordert eine Änderung an der Netzwerkfunktionalität des Betriebssystems. Der Vorteil wäre aber, daß das mobile System weiterhin nichts von der Existenz des Fast-Forwarding Protokolls wüßte.

Tabelle 6.1 stellt beide Verfahren nochmals gegenüber.

Mobiler Sender sendet direkt zum ersten Foreign Agent	Daten vom mobilen System gelangen hop-by-hop zum ersten Foreign Agent
+ einfach zu implementieren – Änderungen am mobilen System notwendig	+ Fast-Forwarding Protokoll weiterhin transparent für das mobile System – großer Implementierungsaufwand

Tabelle 6.1: Vergleich: Daten vom mobilen System zum Transport Gateway

6.5.3 Wechseln des ersten Foreign Agents

Sollte eine Forwardingkette aufgegeben werden müssen (siehe Abschnitt 6.1.2), fordert die Integration des indirekten Transportansatzes eine spezielle Behandlung beim Wechsel. Abbildung 6.12 zeigt ein Beispiel hierfür.

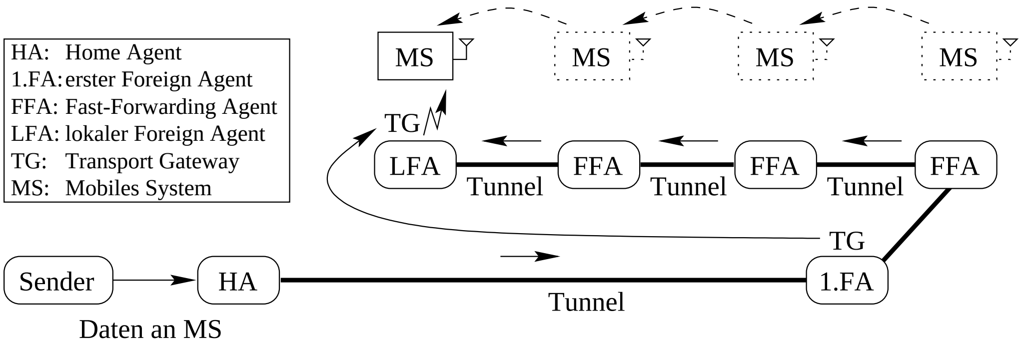

Abbildung 6.12: Wechsel des ersten Foreign Agents mit einem Transport Gateway

Der lokale Foreign Agent darf in diesem Fall nicht einfach einen Mobile IP Subnetzwechsel durch eine direkte Registrierung beim Home Agent initiieren, weil sich dann das Transport Gateway nicht mehr auf der Strecke vom Home Agent zum mobilen System befände. Als erstes muß der lokale Foreign Agent dem ersten Foreign Agent eine Nachricht senden, daß er eine direkte Registrierung mit dem Home Agent vornehmen will. Damit wird die Migration des Transport Gateways vom ersten Foreign Agent zum neuen angestoßen. Ist der Wechsel vollzogen, erfolgt das normale Vorgehen bei einer Registrierung, d. h. der lokale Foreign Agent sendet die Registrierungsanforderung an den Home Agent. Dieser sendet von nun an die Daten an den mobilen Teilnehmer nicht mehr an den ehemaligen ersten Foreign Agent, sondern an den lokalen Foreign Agent, der damit neuer erster Foreign Agent ist. Entlang der alten Forwardingkette sendet der Home Agent eine Mobile IP-Ende Nachricht, um die belegten Ressourcen (Tunnel etc.) wieder freizugeben.

6.5.4 Fehlerbehebung beim indirekten Transportansatz

Der in Abschnitt 6.3 vorgestellte Mechanismus zum Behandeln von verlorengegangenen Mobile IP bzw. Fast-Forwarding Protokoll Nachrichten benötigt bei der zusätzlichen Integration des indirekten Transportansatzes ebenfalls geringfügige Anpassungen. Im genannten Abschnitt wurde vorgeschlagen, beim Verlust einer Nachricht mit anschließendem Subnetzwechsel eine direkte Registrierung mit dem Home Agent vorzunehmen. Ein Transport Gateway befände sich dann aber nicht mehr auf der Strecke vom Home Agent zum mobilen System. Deswegen sollte sich der lokale Foreign Agent als Modifikation des Verfahrens nicht direkt beim Home Agent, sondern beim ersten Foreign Agent anmelden, sofern das mobile System beim ersten Foreign Agent erfolgreich registriert war. Sollte allerdings bereits beim Wechsel zum ersten Foreign Agent eine Nachricht verlorengegangen sein, so daß das mobile

System nicht mit Sicherheit weiß, ob es beim ersten Foreign Agent angemeldet war, bleibt keine andere Vorgehensweise als eine direkte Registrierung beim Home Agent.

6.5.5 Fazit

Durch die Kombination des Fast-Forwarding Protokolls mit dem indirekten Transportansatz ist es notwendig, das Transport Gateway auf dem ersten Foreign Agent in der Forwardingkette zu plazieren. Desweiteren sollte sich der lokale Foreign Agent bei einer Beendigung einer Forwardingkette wegen einer mißlungenen Registrierung nicht beim Home Agent, sondern beim ersten Foreign Agent anmelden, um eine Migration des Transport Gateways zu verhindern. Schließlich muß noch beachtet werden, daß der mobile Teilnehmer alle Daten über das System mit dem Transport Gateway versendet.

6.6 Sicherheitsbetrachtungen

Die Betrachtung von Sicherheitsaspekten umfaßt zwei Bereiche: erstens inwiefern bereits bestehende Sicherheitsvorkehrungen in Mobile IP durch das Fast-Forwarding Protokoll beeinflußt werden und zweitens inwieweit neue Mechanismen für das Fast-Forwarding Protokoll notwendig sind.

6.6.1 Modifikation der Care-of Adresse

Registrierungsanforderungen zwischen dem Home Agent und dem mobilen System müssen in Mobile IP authentifiziert werden, damit eine Umleitung von Daten, die für einen Mobilteilnehmer bestimmt sind, an unbefugte Dritte nicht möglich ist (siehe Abschnitt 2.4.4). Die Modifikation der Care-of Adresse in einer Registrierungsanforderung durch den ersten Foreign Agent (siehe Abschnitt 6.1.1) verursacht damit das Problem, daß die Authentifizierung nach dieser Veränderung nicht mehr gültig ist.

Zwei Vorgehensweisen zur Lösung sind hierbei denkbar, um den vorhandenen Authentifizierungsmechanismus weiterhin benutzen zu können:

1. Das mobile System trägt nicht die Adresse des lokalen, sondern die des ersten Foreign Agents als Care-of Adresse in die Registrierungsanforderung ein.

2. Der erste Foreign Agent verändert nicht die Care-of Adresse in der Registrierungsanforderung, sondern hängt an das Ende des vom mobilen System authentifizierten Teils der Registrierungsanforderung eine Mobile IP Erweiterung mit seiner IP-Adresse an. Auf diese Weise signalisiert er dem Home Agent, daß eine Forwardingkette besteht, so daß dieser den Tunnel zum ersten Foreign Agent beibehält und auch die Registrierungsantwort weiterhin an den ersten Foreign Agent schickt.

Die erste Variante hat gegenüber der zweiten den Vorteil, daß für den Home Agent das Fast-Forwarding Protokoll weiterhin transparent ist, er also nicht modifiziert werden muß. Allerdings ist erneut das mobile System in die Implementierung des Fast-Forwarding Protokolls involviert, weil dieses sich die Adresse des ersten Foreign Agent merken muß. Dies ist aber bereits im Rahmen der Fehlerbehebung (vgl. Abschnitt 6.5.4) in Verbindung mit dem indirekten Transportansatz nötig.

Aufwendiger wird das Ablehnen des Fast-Forwarding durch den alten Foreign Agent: Sendet das mobile System die Adresse des ersten Foreign Agent als Care-of Adresse und der alte Foreign Agent kann das Fast-Forwarding nicht bereitstellen, darf der neue Foreign Agent die Registrierungsanforderung nicht direkt an den Home Agent senden: Dadurch daß die Care-of Adresse die Adresse vom ersten Foreign Agent ist, sähe der Home Agent keine Notwendigkeit, eine direkte Verbindung zum neuen Foreign Agent aufzubauen. Für diesen Fall muß der neue Foreign Agent eine Nachricht an das mobile System senden, daß ein Fast-Forwarding nicht möglich ist, so daß dieses eine neue, authentifizierte Registrierungsanforderung mit der Adresse des neuen Foreign Agents als Care-of Adresse senden kann. Damit ist das mobile System in noch größerem Umfang in die Signalisierung des Fast-Forwarding Protokolls involviert.

Die zweite Variante hebt die Transparenz des Fast-Forwarding Protokolls für den Home Agent auf, er muß die Registrierungsanforderung zusätzlich auf Mobile IP Erweiterungen untersuchen und entsprechend reagieren, wenn eine Erweiterung anzeigt, daß das Fast-Forwarding Protokoll vorliegt. Diese Erweiterung muß allerdings nicht authentifiziert werden, weil damit keine Veränderung von Routen, sondern das Beibehalten einer Route bewirkt wird. Somit kann ein Unbefugter durch das Anhängen der Mobile IP Erweiterung mit seiner IP-Adresse lediglich eine direkte Registrierung des mobilen Teilnehmers verhindern, aber nicht unbefugt Daten für den mobilen Teilnehmer zu sich selbst umleiten.

Tabelle 6.2 bewertet beide Lösungen im Überblick:

Mobiles System ändert die Care-of Adresse	Erster Foreign Agent hängt Mobile IP Erweiterung an
+ Fast-Forwarding Protokoll weiterhin transparent für den Home Agent – Modifikationen am mobilen System notwendig – Komplexer Protokollablauf, wenn der alte Foreign Agent das Fast-Forwarding ablehnt	+ Fast-Forwarding Protokoll transparent für das mobile System + Ablehnung des Fast-Forwardings durch den alten Foreign Agent weiterhin unkompliziert – Home Agent in das Fast-Forwarding Protokoll involviert

Tabelle 6.2: Vergleich: Modifikation der Care-of Adresse

6.6.2 Sicherheit für Fast-Forwarding Nachrichten

Es sind zwei neue Nachrichten für das Fast-Forwarding Protokoll notwendig: Fast-Forwarding Notify und Fast-Forwarding Acknowledge bzw. Negative Acknowledge.

1. Fast-Forwarding Notify

   Hierbei handelt es sich um eine sicherheitskritische Nachricht, weil sie Auslöser für den Aufbau einer neuen Route beim alten Foreign Agent ist. Abbildung 6.13 zeigt einen möglichen Angriff von außerhalb.

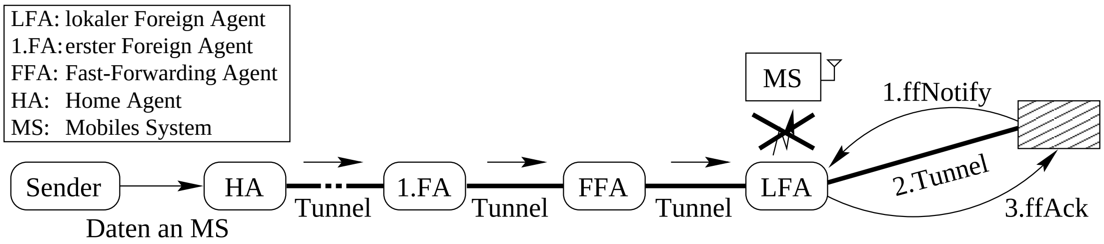

Abbildung 6.13: Versuch der Umleitung von Daten mit dem Fast-Forwarding Protokoll

   Der Angreifer sendet dazu eine Fast-Forwarding Notify mit seiner IP-Adresse als die des neuen Foreign Agents an den lokalen Foreign Agent, bei dem sich der mobile Teilnehmer gerade befindet. Der lokale Foreign Agent geht davon aus, daß der Mobilteilnehmer das Subnetz gewechselt haben muß, eröffnet einen Tunnel zum Angreifer und sendet eine Bestätigung an diesen. Fortan werden alle für den mobilen Teilnehmer bestimmten Daten an den Angreifer weitergeleitet, bis das mobile System die nächste periodische Registrierungsanforderung an den lokalen Foreign Agent sendet. Erst dann errichtet der lokale Foreign Agent wieder die lokale Unterstützung und leitet die Daten nicht mehr in den Tunnel zum Angreifer.

   Um dieses Problem zu umgehen, sollte eine Authentifizierung zwischen dem neuen und dem alten Foreign Agent stattfinden. Dazu könnte das mobile System beim Registrieren mit dem lokalen Foreign Agent Authentifizierungsinformationen austauschen, die es dann nach einem Subnetzwechsel auch dem neuen Foreign Agent zukommen läßt. Eine genauere Betrachtung des Verfahren wird in dieser Arbeit nicht unternommen. Da die Nachrichten des Fast-Forwarding Protokolls den in der Route Optimization verwendeten Nachrichten ähneln, können die dortigen Betrachtungen [JohPer97] auch für eine Sicherheitsbetrachtung der Nachrichten des Fast-Forwarding Protokolls herangezogen werden.

2. Fast-Forwarding Acknowledge / Negative Acknowledge

   Diese Nachrichten sind sicherheitsunkritisch, weil sie nur als Antwort des alten Foreign Agents auf die bereits authentifizierte Fast-Forwarding Notify gesendet werden. Empfängt ein Mobility Agent eine von beiden Nachrichten unerwartet, ignoriert er sie.

Die Mobile IP-Ende Nachricht Als weiteres muß noch eine Betrachtung der Mobile IP-Ende Nachricht mit der erweiterten Semantik stattfinden (vgl. Abschnitt 6.1.2), weil sie nicht mehr nur vom Home Agent sondern auch beim Beenden des Fast-Forwardings oder im Falle einer Schleifenauflösung (siehe Abschnitt 6.2) von einem Fast-Forwarding Agent gesendet werden kann. Da die Mobile IP-Ende Nachricht in diesem Fall immer vom Vorgänger in der Forwardingkette kommt, könnten beide beim Aufbau der Forwardingkette Daten austauschen, um die Mobile IP-Ende Nachricht zu authentifizieren. Dieses soll aber in dieser Arbeit nicht weiter behandelt werden.

Fazit der Sicherheitsbetrachtungen

Bei der Einführung des Fast-Forwarding Protokolls muß man also beachten, daß die Authentifizierung der Registrierungsanforderung zwischen dem Home Agent und dem Mobilteilnehmer eine Modifikation dieser Nachricht nicht ohne weiteres zuläßt. Desweiteren bietet das Fast-Forwarding Möglichkeiten zur Umleitung von Daten an Unbefugte, welches aber zusätzliche Authentifizierungsmechanismen verhindern können.

6.7 Zusammenfassung

Das Fast-Forwarding Protokoll reduziert also die Unterbrechungszeit beim Subnetzwechsel eines mobilen Teilnehmers und zusätzlich die Datenverluste, sofern ein Weitverkehrsszenario vorliegt. Es müssen allerdings gesondert die Folgen der Verwendung eines unzuverlässigen Signalisierungsprotokolls betrachtet werden, weil sich sonst die korrekte Funktion des Fast-Forwarding Protokolls nicht gewährleisten läßt. Desweiteren kann man den indirekten Transportansatz in das Fast-Forwarding Protokoll eingliedern, wobei aber insbesondere die Plazierung des Transport Gateways Probleme bereitet. Die Betrachtungen zur Sicherheit des Fast-Forwarding Protokolls ergeben, daß ein Schutz gegen die Umleitung von Daten an Unbefugte mit vernünftigem Aufwand möglich ist.

Kapitel 7

Implementierung und Messungen

Dieses Kapitel gibt einen detaillierten Einblick in die Implementierung der Konzepte aus den Kapiteln 5 und 6. Diese ist abhängig von der vorhandenen Testumgebung, die im ersten Abschnitt beschrieben wird. Desweiteren belegen Messungen die Aussagen aus den vorangegangenen Kapiteln.

7.1 Die Testumgebung

In diesem Abschnitt erfolgt eine Betrachtung der verwendeten Hard- und Software sowie der daraus resultierenden Testszenarien.

Die Hardware Die mobile Ausrüstung besteht aus einem Notebook mit einem WaveLAN Netzwerkadapter, der als mobiles System fungiert, und zwei Basisstationen. Die maximale Übertragungsrate auf der drahtlosen Strecke beträgt 2 Mbps. Die Router zur Kopplung der Basisstationen, die Mobility Agents sowie die für RSVP benötigten Systeme sind PCs, die über ein 100 Mbps Fast-Ethernet miteinander verbunden sind.

Die Software Alle genannten Systeme verfügen über Linux als Betriebssystem. Die für Linux vorhandenen Implementierungen von RSVP und Mobile IP sind nicht ohne weiteres lauffähig gewesen, so daß dort Anpassungen vorgenommen werden mußten. Die Linux-Portierung von RSVP [Vir97] wurde dabei für den Transport von RSVP Nachrichten mittels RawIP erweitert. Dafür muß im Linux-Kernel das sog. Router-Alert [Kat97] vorhanden sein, was zur Zeit nur in den Entwicklerversionen des Linux-Kernels (Version 2.1.x) der Fall ist.

Die verwendete Mobile IP Implementierung [GupDix96] mußte deswegen von den stabilen Linux-Kerneln auf die Entwicklerkernel portiert werden. Dabei hat sich in den Entwicklerkerneln insbesondere die Verwendung von IPIP-Tunneln verändert (siehe dazu Abschnitt 7.2.1).

Testszenarien Mit der zur Verfügung stehenden Hardware sind zwei Testszenarien möglich. Abbildung 7.1 zeigt ein Szenario, in dem sich das mobile System sowohl im Heimatsubnetz als auch in einem fremden Subnetz aufhalten kann.

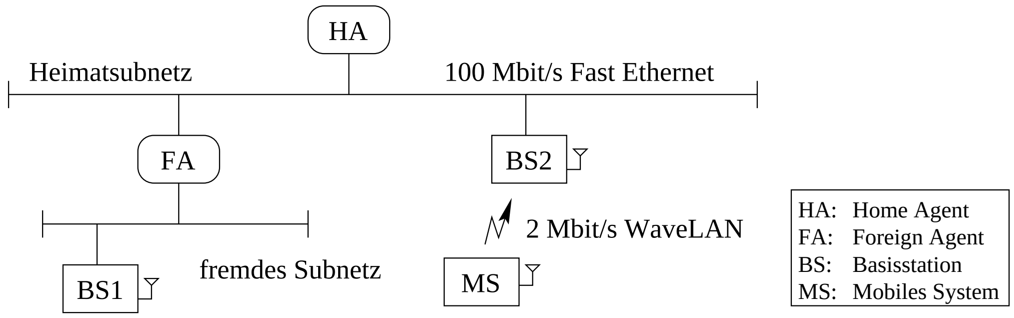

Abbildung 7.1: Testszenario mit Heimatsubnetz und einem fremden Subnetz

Das zweite Testszenario ist in Abbildung 7.2 dargestellt: Das mobile System kann sich zwischen zwei fremden Subnetzen hin- und her bewegen. Dementsprechend gibt es auch zwei Foreign Agents.

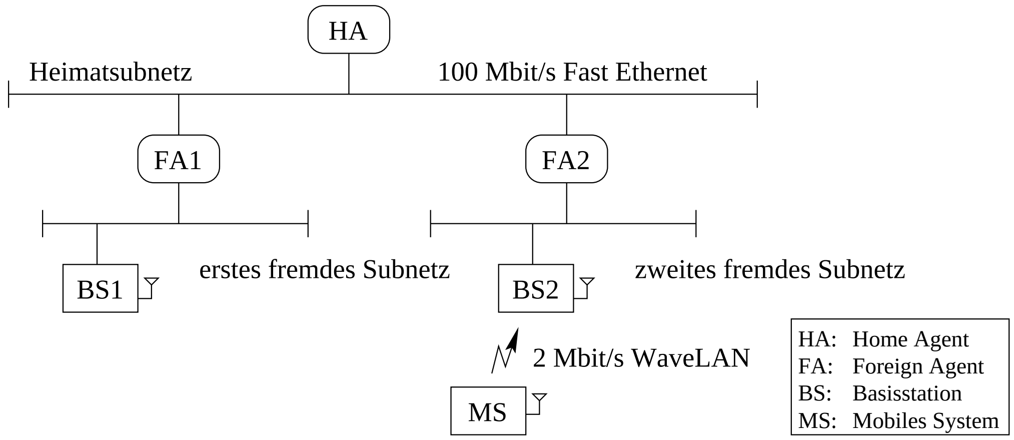

Abbildung 7.2: Testszenario mit zwei fremden Subnetzen

Als drittes Szenario wäre noch der Betrieb beider Basisstationen in einem Subnetz denkbar. Da aber dann bei einem Funkzellenwechsel kein Subnetzwechsel stattfindet und damit Mobile IP nicht involviert ist, fand keine weitere Betrachtung dieses Szenarios statt.

7.1.1 Einschränkungen durch die Testumgebung

Für die Implementierung der in den Kapiteln 5 und 6 entworfenen Konzepte ergaben sich die folgenden Einschränkungen hinsichtlich der Reservierung von Ressourcen:

- Es konnte keine Reservierung von Bandbreite vorgenommen werden, da diese Funktionalität für Ethernet-Netze bzw. Ethernet-ähnliche Netze wie WaveLAN nicht zur Verfügung steht.

- Unter Linux stand keine Ressourcenverwaltung und keine Verkehrskontrolle für RSVP zur Verfügung.

Die Betrachtung der Ressourcenreservierung mittels RSVP beschränkte sich also auf die Signalisierung der RSVP-Nachrichten.

Außerdem ergaben sich die folgenden Beschränkungen:

- Die Vor- und Nachteile der Plazierung der Mobility Agents im Subnetz (siehe Abschnitt 5.1.4) konnten für die fremden Subnetze nicht überprüft werden. In beiden gibt es jeweils nur ein System pro Subnetz, weswegen der Router und der Mobility Agent auf einem System plaziert sein müssen.

- Es stand keine Implementierung des indirekten Transportansatzes zur Verfügung. Die dazu entworfenen Konzepte wurden in Teilen implementiert, konnten aber nicht getestet werden.

- Die Messungen konnten keine RSVP-Tunnelsitzung berücksichtigen, weil es für Linux keine Implementierung eines IPIP-Tunnels gab, welcher Reservierungen mit RSVP ermöglicht.

- Es konnten keine Messungen bei einer größeren Belastung der Systeme durch viele Reservierungen und viele mobile Teilnehmer gemacht werden, weil nur ein mobiles System zur Verfügung stand.

7.2 Die Mobile IP Implementierung

In diesem Abschnitt soll eine Betrachtung von einigen Besonderheiten der Mobile IP Implementierung stattfinden, auf die sich die folgenden Abschnitte beziehen.

7.2.1 Die Verwendung von IPIP-Tunneln in Linux 2.1.x

In den Entwicklerversionen des Linux-Kernels hat sich die Behandlung von IPIP-Tunneln gegenüber den stabilen Linux 2.0.x Kerneln deutlich verändert: In Linux 2.0.x muß für jeden Tunnel ein neues Modul geladen werden. In Linux 2.1.x erledigt ein einziger sog. „Tunnel-Master“ diese Arbeit. Es steht auch eine größere Anzahl von Tunneln zur Verfügung, was insbesondere im Hinblick auf das Fast-Forwarding Protokoll von großer Bedeutung ist. Der grundsätzliche Ablauf zur Errichtung eines Tunnels hat sich nur an einer Stelle geändert: Am Tunnelendpunkt muß nicht mehr das Modul zum Auspacken der eingekapselten Tunneldaten geladen sein, diese Funktionalität ist im neuen Tunnel-Modul enthalten. Zusätzlich muß aber ein Tunnel mit der IP-Adresse des Tunnelanfangs als Endpunkt eröffnet sein (im folgenden das *Tunnelgegenstück* genannt). Damit sind IPIP-Tunnel in Linux 2.1.x immer bidirektional.

7.2.2 Die lokale Unterstützung im fremden Subnetz

In der ursprünglichen Implementierung von Mobile IP für Linux [GupDix96] bedeutet das Errichten einer lokalen Unterstützung für einen Mobilteilnehmer im fremden Subnetz lediglich, daß der Foreign Agent die IP-Adresse des mobilen Systems in seine Routingtabelle mit einer lokalen Route einträgt.

Abschnitt 4.6 der Mobile IP Spezifikation fordert aber, daß ein mobiler Teilnehmer im fremden Subnetz keine ARP-Anfragen oder ARP-Antworten senden darf. Die ursprüngliche Implementierung von Mobile IP konnte dies nicht berücksichtigen, weil es in den Linux-Kerneln der Version 2.0.x keine Möglichkeit gibt, auf einem mobilen System die ARP-Funktionalität abzuschalten, ohne die Netzwerkfunktionalität des mobilen Systems ganz zu unterbinden. In den für diese Arbeit verwendeten Entwicklerkerneln ist die Möglichkeit aber vorhanden, diese ARP-Funktionalität abzuschalten, so daß die für diese Arbeit an der Mobile IP-Implementierung vorgenommenen Änderungen davon Gebrauch machen können.

Die Mobile IP Implementierung befindet sich vollständig im Userspace, d. h. außerhalb des Kernels, was sich auch durch die im Rahmen dieser Arbeit vorgenommenen Erweiterungen nicht ändern sollte. Dadurch ergeben sich aber die folgenden Probleme.

Adreßauflösung auf dem mobilen System

Wenn das mobile System nach einem Subnetzwechsel eine Agent Advertisement vom Foreign Agent erhält, bewirkt das Ausschalten von ARP auf dem mobilen System, daß die MAC-Adresse des Foreign Agents nicht automatisch im ARP-Cache gespeichert wird. Versucht der Mobilteilnehmer eine Registrierungsanforderung an den Foreign Agent zu senden, von dem die Agent Advertisement kam, kann er keine zuverlässige Auflösung der IP-Zieladresse vornehmen, weil er keine ARP-Anfragen senden darf. Damit kann er die Registrierungsanforderung nicht versenden.

Eine Lösung besteht aus der Erweiterung der Agent Advertisements um die MAC-Adresse des sendenden Mobility Agents. Damit kann das mobile System manuell einen Eintrag im ARP-Cache für eine spätere Adreßauflösung vornehmen. Diese sog. *MAC-Adressen Erweiterung* wurde in das bestehende Konzept der Mobile IP Erweiterungen eingebettet, ihr Format ist in Abschnitt B.2.1 dargestellt.

Damit ändert sich der Ablauf einer Registrierung auf dem mobilen System wie folgt:

1. Es erhält vom Foreign Agent eine Agent Advertisement mit dessen MAC-Adresse.
2. Für diesen Foreign Agent richtet es einen permanenten Eintrag im ARP-Cache ein.
3. Schließlich sendet es die Registrierungsanforderung an den Foreign Agent, wobei der permanente Eintrag im ARP-Cache eine Adreßauflösung ermöglicht.

Adreßauflösung auf dem Foreign Agent

Auf dem Foreign Agent existiert ein ähnliches Problem: Bekommt dieser die Registrierungsanforderung vom mobilen System, kann er nicht den Paketkopf für die Sicherungsschicht lesen, um die MAC-Adresse des mobilen Systems zu erhalten. Dies ist nicht möglich, weil die Implementierung von Mobile IP nicht im Linux-Kernel liegt. Der Foreign Agent benötigt diese MAC-Adresse aber, wenn er die Registrierungsantwort an den Mobilteilnehmer weiterleiten soll. Vom mobilen Teilnehmer bekommt er die MAC-Adresse ebenfalls nicht, weil dieser nicht auf ARP-Anfragen reagiert. Grundsätzlich sollte der Foreign Agent die Zuordnung IP-Adresse zur MAC-Adresse des mobilen Systems in seinem ARP-Cache speichern, wenn er die Registrierungsanforderung von diesem erhält. Es hat sich aber herausgestellt, daß die Abfrage dieses Eintrages nicht immer zuverlässig funktioniert. In dem Fall kann auch der Foreign Agent die Registrierungsantwort nicht ausliefern.

Als Lösung bietet sich hier an, die MAC-Adresse des mobilen Systems bei der Konfiguration des Foreign Agents mit anzugeben. In der vorliegenden Mobile IP Implementierung wird jeder Foreign Agent bereits mit der IP-Adresse aller zugelassenen mobilen Systeme konfiguriert, um eine Authentifikation zwischen Foreign Agent und Home Agent zu ermöglichen. Daher besteht eine einfache Lösung des Problems darin, bei der Konfiguration zusätzlich noch die MAC-Adresse des mobilen Systems hinzuzufügen.

Damit unternimmt der Foreign Agent die folgenden Schritte zur Errichtung der lokalen Unterstützung:

1. Der Foreign Agent richtet für das mobile System einen permanenten Eintrag im ARP-Cache ein.

2. Er fügt einen lokalen Eintrag mit der IP-Adresse des mobilen Systems in seine Routingtabelle ein.

3. Schließlich errichtet er das Tunnelgegenstück zum Home Agent.

7.3 Modifikationen an Mobile IP

Dieser Abschnitt zeigt Implementierungsdetails der in Abschnitt 5.1 entwickelten Konzepte, die unter Berücksichtigung der vorhandenen Testumgebung implementiert werden konnten.

7.3.1 Schnelles Agent Discovery Verfahren

Die Implementierung des schnellen Agent Discovery Verfahrens betrifft nur das mobile System, weil das Verarbeiten von Agent Solicitations auf den Mobility Agents bereits vorhanden ist. Sie ist abhängig von der verwendeten Sicherungsschicht. Die folgenden Ausführungen beziehen sich also im speziellen auf die WaveLAN Technologie. Deswegen sind zunächst einige Erläuterung hinsichtlich der WaveLAN Implementierung der Sicherungsschicht nötig.

Die WaveLAN Implementierung der Sicherungsschicht

Das WaveLAN-System, bestehend aus dem Netzwerkadapter und der dazugehörigen Treibersoftware, kennt zwei Zustände:

1. Es empfängt die Daten von genau einer Basisstation (sog. *Single-Modus*).

2. Es empfängt Daten von allen Basisstationen, die in seinem Empfangsbereich liegen (sog. *Multi-Modus*)

Der Single-Modus ist der Normalfall, eine Basisstation sendet ein genügend starkes Signal, so daß eine Kommunikation zwischen Basisstation und mobilem System möglich ist. Bewegt sich ein Mobilteilnehmer aus dem Versorgungsbereich einer Basisstation heraus, erkennt das WaveLAN-System zunächst nur, daß das Signal der alten Basisstation schwächer wird. Um die Signalstärke einer neuen Basisstation messen zu können, muß es in den Multi-Modus wechseln und die Signalstärken der zu empfangenden Basisstationen vergleichen. Ist eine andere Basisstation besser zu empfangen, wechselt es zur dieser und geht wieder in den Single-Modus über. Andernfalls bleibt es bei der alten Basisstation.

Schnittstelle zur Netzwerkschicht An die Netzwerkschicht sendet das WaveLAN-System jeweils ein Signal, wenn es zwischen den beiden Modi hin- und her wechselt. Die Netzwerkschicht kann dann eine Anfrage starten, aus welchem Grund das Signal gesendet wurde. Drei Antworten sind möglich:

1. Das WaveLAN-System ist in den Multi-Modus übergegangen, um die Signalstärken aller Basisstationen zu testen (MULTI_AP).

2. Es ist vom Multi-Modus in den Single-Modus übergegangen, ohne die Basisstation zu wechseln (OLD_AP).

3. Es hat die Basisstation gewechselt, nachdem die Überprüfung im Multi-Modus eine andere Basisstation mit größerer Signalstärke ergeben hat (NEW_AP).

Schnelles Agent Discovery für WaveLAN

Abbildung 7.3 zeigt den Zustandsautomat des mobilen Systems beim schnellen Agent Discovery, wenn das WaveLAN-System Signale an Mobile IP sendet:

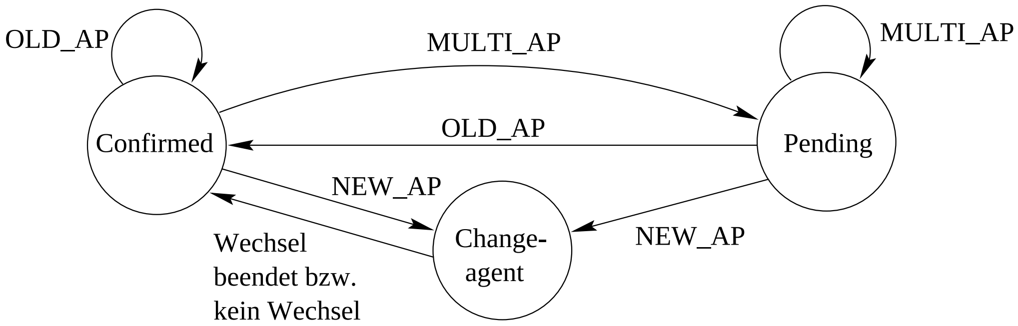

Abbildung 7.3: Zustandsautomat für das schnelle Agent Discovery Verfahren

Der grundsätzliche Ablauf ist wie folgt: Zunächst befindet sich das mobile System im „Confirmed"-Zustand, d. h. das WaveLAN-System empfängt auf der Sicherungsschicht Daten von genau einer Basisstation. Auf der Netzwerkschicht ist das mobile System bei einem Mobility Agent registriert. Geht das WaveLAN-System in den Multi-Modus über, sendet es ein Signal an Mobile IP. Dieses wechselt in dem hier dargestellten Zustandsdiagramm zum „Pending"-Zustand. Hat das WaveLAN-System die Prüfung der Signalstärken beendet, kann es zwei verschiedene Signale an Mobile IP senden: Im ersten Fall ist es bei der alten Basisstation geblieben (OLD_AP), damit kann Mobile IP ohne weitere Aktionen wieder in den „Confirmed"-Zustand zurückkehren. Im zweiten Fall (NEW_AP) ist es zu einer anderen Basisstation gewechselt. Dann muß Mobile IP prüfen, ob auch ein Subnetzwechsel vorliegt und geht in den Zustand „Changeagent" über. Dabei sendet Mobile IP, wie in Abschnitt 5.1.2 dargestellt, Agent Solicitations aus. Anhand der als Antwort gesendeten Agent Advertisements kann das mobile System entscheiden, ob ein Subnetzwechsel vorliegt und im positiven Fall eine Registrierungsanforderung abschicken. Auf jeden Fall kehrt es nach Beendigung dieser Prüfung in den „Confirmed"-Zustand zurück.

Es gibt zwei initiale Zustände: Beim Starten von Mobile IP auf dem mobilen System prüft dieses zunächst, ob das WaveLAN-System bei einer Basisstation angemeldet ist. Wenn ja, wird die Vorgehensweise wie bei einem Subnetzwechsel angestoßen, d. h. das mobile System sendet eine Agent Solicitation aus. Der initiale Zustand ist also der „Changeagent"-Zustand. Befindet sich das WaveLAN-System dagegen im Multi-Modus, empfängt das mobile System Daten von mehreren Basisstationen, also unter Umständen auch Agent Advertisements aus mehreren Subnetzen. Dann geht Mobile IP auf dem mobilen System initial in den „Pending"-Zustand über und wartet mit der Registrierung, bis das WaveLAN-System wieder in den Single-Modus wechselt und ein Signal schickt.

Die folgenden Bemerkungen sollen die Gestaltung des Automaten motivieren:

- Der „Pending"-Zustand mußte wegen des Multi-Modus des WaveLAN-Systems eingeführt werden. Schaltet dieses in jenen Zustand, hört Mobile IP unter Umständen Agent Advertisements von mehreren Subnetzen. Dies tritt auf, wenn sich der mobile Teilnehmer gerade an der Grenze zwischen zwei oder mehreren Subnetzen befindet und das WaveLAN-System Signale von mehreren Basisstationen empfangen kann. Würde Mobile IP alle Agent Advertisements aus den verschiedenen Subnetzen auswerten, könnte es nur schwer über einen Subnetzwechsel entscheiden. Um diese Komplexität vom mobilen System fernzuhalten, ignoriert es alle Agent Advertisements, wenn es sich im „Pending"-Zustand befindet.

- Der Zustand „Changeagent" ist eigentlich die Ausgabefunktion für den Zustandsübergang von „Pending" nach „Confirmed". Aus dem folgenden Grund ist er ein separater Zustand: Signale werden in Linux asynchron verarbeitet, d. h. sie können den sequentiellen Programmablauf an jeder beliebigen Stelle unterbrechen. Da aber die Routine zum Wechseln des Subnetzes relativ viel Zeit beanspruchen kann, könnte die Situation entstehen, daß das WaveLAN-System eine erneute Prüfung der Signalstärke veranlaßt und ein weiteres Signal an Mobile IP sendet. Dann müßte die

Implementierung die Situation beachten, daß eine Signalverarbeitungsroutine sich selbst unterbrechen könnte.

Als Lösung nimmt die Signalverarbeitungsroutine selbst nur den Zustandsübergang vom „Pending“ in den „Changeagent“-Zustand vor. Der eigentliche Mechanismus für die Prüfung, ob ein Subnetzwechsel vorliegt, und eine eventuelle Ausführung des Subnetzwechsels befindet sich in der Hauptprogrammschleife und damit im sequentiellen Programmfluß.

- Normalerweise entscheidet die Sicherungsschicht über den Wechsel von einer Basisstation zu einer anderen anhand der Signalstärken. Für Testzwecke ist es aber möglich, daß der Benutzer auf dem mobilen System die Basisstation wechselt. Dafür ist der direkte Zustandsübergang vom „Confirmed“-Zustand nach „Changeagent“ nötig.

7.3.2 Die Notify-Nachricht: ein neuer Nachrichtentyp

Für die Implementierung der in den vorangehenden Kapiteln beschriebenen Konzepte benötigt man in Mobile IP einige neue Nachrichten. Da diese alle ähnlich aufgebaut sind, wurde nur ein allgemeiner Typ hinzugefügt: die *Notify-Nachricht*. Ihr Format ist in Abschnitt B.2.2 dargestellt.

7.3.3 Die lokale Unterstützung im Heimatsubnetz

Wie in Abschnitt 5.2.1 begründet, muß für die Integration des indirekten Transportansatzes in Mobile IP sämtlicher Datenverkehr zum mobilen Teilnehmer den Home Agent passieren, damit auf dem Home Agent das Transport Gateway realisiert werden kann. Der grundsätzliche Ablauf der lokalen Unterstützung im Heimatsubnetz ist ähnlich der in Abschnitt 7.2.2 beschrieben lokalen Unterstützung in einem fremden Subnetz.

Zunächst ist auf dem Home Agent ein Proxy-ARP Eintrag für das mobile System nötig, wenn das mobile System sich im Heimatsubnetz befindet. Damit auf eine ARP-Anfrage nicht der Home Agent *und* das mobile System antworten, darf dieses ebenfalls keine ARP-Antworten senden. Ebenso muß der Home Agent einen permanenten Eintrag im ARP-Cache für das mobile System errichten und das mobile System einen für den Home Agent, damit beide Daten zueinander senden können. Um diese permanenten Einträge vornehmen zu können, sendet der Home Agent wie alle Foreign Agents ebenfalls seine MAC-Adresse in der Agent Advertisement. Die MAC-Adresse des mobilen Systems erhält er ebenso wie ein Foreign Agent mittels der Konfiguration.

Problem: ProxyARP im Heimatsubnetz

Bei der Nutzung von Proxy-ARP im Heimatsubnetz trat allerdings ein grundsätzliches Problem auf: Der Home Agent antwortet nicht auf eine ARP-Anfrage mit der IP-Adresse des mobilen Systems, obwohl er einen Proxy-ARP Eintrag für diese Adresse besitzt. Bevor der Linux-Kernel auf eine solche ARP-Anfrage antwortet, prüft er, wie er selbst das betroffene System erreichen kann. Ist es über dasselbe Interface zu erreichen, von dem die ARP-Anfrage gekommen ist, geht er davon aus, daß das System selbst auf die ARP-Anfrage antworten kann und sendet deswegen keine ARP-Antwort.

Um den Kernel nicht zu ändern, benötigt man ein zusätzliches Kernelmodul: das Mobile IP-Dummy Modul oder kurz *MIPdum* Modul. Ähnlich dem in Linux vorhandenen Dummy Modul [Hol94] stellt es ein virtuelles Netzwerkinterface zur Verfügung. Seine einzige Funktion ist, alle empfangenen Pakete auf ein anderes reales Interface unverändert weiterzuleiten.

Mit diesem Modul ist es möglich, die oben genannte Prüfung durch den Kernel zu umgehen, indem man auf dem Home Agent eine Route zum mobilen System über das MIPdum Interface errichtet: Für den Kernel ist das mobile System nicht mehr auf demselben Interface zu erreichen, von dem eine ARP-Anfrage kam. Dies ist immer gültig, weil das MIPdum Interface niemals Daten empfängt, sondern nur sendet.

Mittels dieses MIPdum Moduls ist es also möglich, daß der Home Agent ARP-Anfragen für die MAC-Adresse des mobilen Systems beantwortet.

Die Errichtung der lokalen Unterstützung auf dem Home Agent besteht somit aus den folgenden Schritten:

1. Der Home Agent richtet einen Proxy-ARP Eintrag für das mobile System ein.

2. Er sendet eine Gratuitous-ARP Nachricht an alle lokalen Systeme, damit diese ihren Eintrag für das mobile System im ARP-Cache als ungültig markieren.

3. Für das mobile System errichtet er einen permanenten Eintrag im ARP-Cache.

4. Schließlich trägt er eine Route zum mobilen System über das MIPdum Interface ein.

Bei einem Subnetzwechsel von einem fremden Subnetz ins Heimatsubnetz fallen die Schritte eins und zwei weg, da der Proxy-ARP Eintrag bereits besteht.

7.3.4 Frühe lokale Unterstützung

Wie auf Seite 73 dargelegt, können RSVP-Nachrichten Mobile IP Nachrichten überholen. Deswegen ist es günstiger, die lokale Unterstützung für einen mobilen Teilnehmer auf einem Foreign Agent schon zu errichten, wenn der Foreign Agent die Registrierungsanforderung vom Mobilteilnehmer erhalten hat. Die konkrete Vorgehensweise ist dieselbe wie in Abschnitt 7.2.2. Es wird also eine lokale Route angelegt, ein permanenter Eintrag in den ARP-Cache eingetragen sowie das Tunnelgegenstück eröffnet.

Sollte allerdings der Home Agent einen Registrierungswunsch ablehnen, müssen diese drei Maßnahmen wieder rückgängig gemacht werden, um nicht unnötig Ressourcen zu belegen. Geringfügige Änderungen gibt es deswegen im Zustandsautomaten für den Foreign Agent (siehe Abbildung 7.4). In diesem ist auch bereits die explizite Beendigung der lokalen Unterstützung durch die Mobile IP-Ende Nachricht dargestellt.

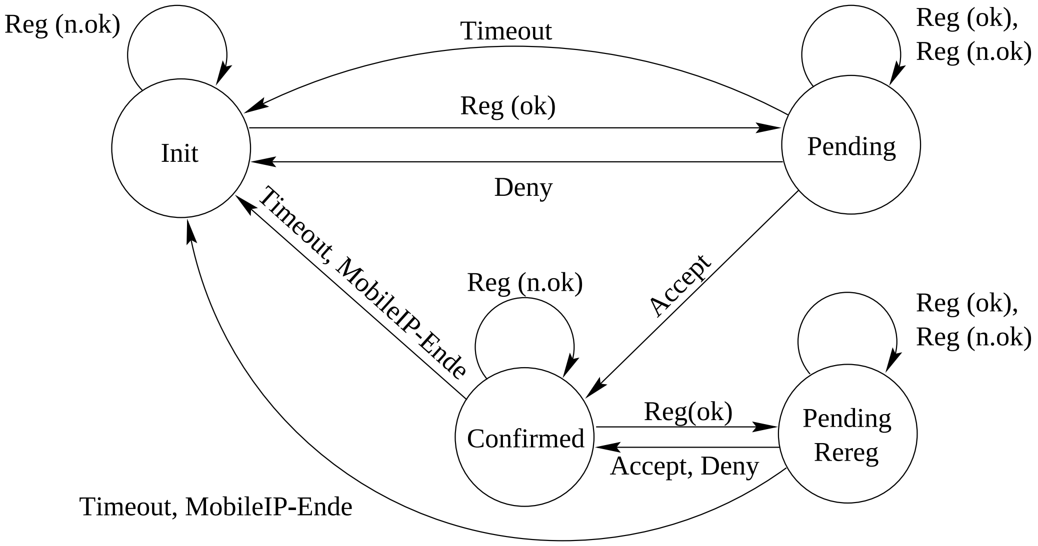

Abbildung 7.4: Zustandsautomat des Foreign Agents bei früher lokaler Unterstützung

Da alle Ressourcen bereits früh belegt werden, muß der Foreign Agent auch die dazugehörigen Registrierungstimer früh in Gang setzen. Das bedeutet aber, daß Timeouts auch im Zustand „Pending" auftreten können.

7.3.5 Explizites Beenden der lokalen Unterstützung

Um dem alten Foreign Agent den Subnetzwechsel eines mobilen Teilnehmers mitzuteilen, sendet der Home Agent eine MobileIP-Ende Nachricht an den alten Foreign Agent (siehe Abschnitt 5.1.3). Diese wird als eine Notify-Nachricht implementiert und trägt im wesentlichen nur die IP-Adresse des mobilen Systems, für das die lokale Unterstützung beendet werden soll.

Bei der Verarbeitung muß der alte Foreign Agent überprüfen, ob er überhaupt das mobile System, dessen Adresse in der MobileIP-Ende Nachricht versendet wurde, lokal unterstützt. Falls ja, beendet er die lokale Unterstützung, indem er das Gegenstück zum IPIP-Tunnel, die lokale Route aus der Routingtabelle und den permanenten Eintrag im ARP-Cache löscht.

7.4 Änderungen an RSVP

Dieser Abschnitt betrachtet die Erweiterungen, die zur RSVP Implementierung hinzugefügt wurden. Diese Erweiterungen beziehen sich auf die sog. RAPI (RSVP Application Programming Interface), der Schnittstelle zwischen RSVP und einer beliebigen Anwendung.

7.4.1 Signalisierung einer Routenänderung

Wie in Abschnitt 5.4.2 dargestellt, muß Mobile IP dem RSVP-Dämon ein Signal senden, wenn ein Subnetzwechsel stattgefunden hat, damit die Ressourcen auf der neuen Strecke schnell reserviert werden können.

Die dazu benötigte Schnittstelle zwischen dem Routingprotokoll und RSVP wird bereits in der RSVP-Spezifikation erwähnt [BraZha97, S. 62]. Sie kommt z. B. im Falle einer Änderung der Route vom Sender zum Empfänger beim Local Repair Mechanismus zum Einsatz. Die in der RSVP -Implementierung vorhandene Schnittstelle (der sog. RSRR: Routing Support for Resource Reservations) war aber unter dem Betriebssystem Linux nicht nutzbar.

Als temporäre Lösung wurde deswegen die RAPI [BraZha97, S. 55ff] um einen weiteren Befehl erweitert:

```
IMMEDIATE_PATH_REFRESH (DestAddress)
```

Auf dem Home Agent laufen nach einem Subnetzwechsel also die folgenden Schritte ab: Um das Signal an den RSVP-Dämon zu senden, eröffnet Mobile IP eine Verbindung zum RSVP-Dämon und sendet den neuen RAPI-Befehl mit der IP-Adresse des mobilen Systems (DestAddress) an diesen. Der RSVP-Dämon durchsucht die Liste seiner RSVP-Sitzungen und sendet für alle Sitzungen, die die übergebene IP-Adresse des mobilen Systems als RSVP-Zieladresse haben, eine neue Path-Nachricht.

Wenn allerdings die RSRR-Schnittstelle für Linux zur Verfügung steht, sollte die hier genannte Signalisierung auf diese Schnittstelle umgestellt werden.

7.4.2 Explizites Löschen einer Reservierung

Gemäß Abschnitt 5.4.3 sollen nicht mehr benötigte Reservierungen auf der Route vom Home Agent zum alten Foreign Agent freigegeben werden, indem Mobile IP bei einem Subnetzwechsel ein Signal an RSVP sendet. Bei der Implementierung dieses Konzeptes traten dieselben Probleme auf wie bei der Signalisierung einer Routenänderung im vorangegangenen Abschnitt. Deswegen wurde die RAPI um einen weiteren Befehl erweitert:

```
IMMEDIATE_PATH_TEAR (RSVP-DestAddress, IP-DestAddress)
```

Die erste übergebene Adresse stellt die Unicast-Zieladresse der RSVP-Sitzung dar, d. h. die des mobilen Empfängers. Die zweite Adresse ist die IP-Adresse des alten Foreign Agents.

Auf diesen Befehl hin sendet der RSVP-Dämon auf dem Home Agent eine PathTear-Nachricht an den alten Foreign Agent. Der zweite Parameter wird aus dem folgenden Grund benötigt:

Die PathTear-Nachricht darf nicht per IP-Standardrouting zum mobilen System versendet werden, weil sie dann den Weg zum mobilen System über den neuen Foreign Agent nehmen würde. Mithilfe des zweiten Parameters kann der RSVP-Dämon auf dem Home Agent die PathTear-Nachricht mittels IP-Standardrouting direkt zum alten Foreign Agent senden.

Da diese Nachricht aber nicht durch den Tunnel zum Foreign Agent gelangt, müßte bei einer Berücksichtigung einer RSVP-Tunnelsitzung zusätzlich auch noch eine PathTear-Nachricht zum Freigeben der durch den Tunnel reservierten Ressourcen versendet werden.

7.5 Das Fast-Forwarding Protokoll

Dieser Abschnitt beschreibt die Implementierung der im Kapitel 6 beschriebenen Konzepte des Fast-Forwarding Protokolls. Diese Beschreibung enthält implizit auch die Implementierung der frühen lokalen Unterstützung (vgl. Abschnitt 7.3.4).

Zunächst findet eine Betrachtung der notwendigen Änderungen auf dem mobilen System statt, gefolgt von der eigentlichen Implementierung des Fast-Forwarding Protokolls auf dem Foreign Agent. Die in Abschnitt 6.6 betrachteten Maßnahmen zur Sicherheit wurden nicht implementiert.

7.5.1 Änderungen auf dem Mobilen System

Für das Fast-Forwarding Protokoll sollten möglichst keine Modifikationen am mobilen System vorgenommen werden, damit das Fast-Forwarding Protokoll ohne Kenntnis des mobilen Systems ablaufen kann. Dennoch waren zwei Änderungen nötig:

1. Das mobile System muß beim Senden der Registrierungsanforderung die IP-Adresse des alten Foreign Agents an den neuen Foreign Agent übergeben.

2. Wegen der Unzuverlässigkeit der Mobile IP Nachrichten in Verbindung mit dem indirekten Transportansatz ist es nötig, daß das mobile System bei einer nicht erfolgreich abgeschlossenen Registrierung dem neuen Foreign Agent die IP-Adresse des ersten Foreign Agent übergibt (siehe Abschnitt 6.5.4).

Übergabe der IP-Adressen

Das mobile System übergibt die IP-Adresse des alten bzw. des ersten Foreign Agents mithilfe einer Mobile IP Erweiterung, der sog. *alten Foreign Agent-Erweiterung*, die an das Ende einer Registrierungsanforderung angehängt wird. Ihr Format ist im Abschnitt B.2.4 im Anhang dargestellt.

7.5.2 Änderungen am Foreign Agent

Die Implementierung des Fast-Forwarding Protokolls erfordert in der Hauptsache Änderungen am Foreign Agent, die dieser Abschnitt darstellt.

Nachrichten des Fast-Forwarding Protokolls

Das Fast-Forwarding Protokoll benötigt drei Nachrichten: Fast-Forwarding Notify, Fast-Forwarding Acknowledge und Fast-Forwarding Negative Acknowledge. Diese werden in das Konzept der Notify-Nachricht eingegliedert.

Alle drei Nachrichten enthalten die IP-Adresse des mobilen Systems, damit der Empfänger weiß, welcher Mobilteilnehmer vom Fast-Forwarding Protokoll betroffen ist.

Wegen der veränderten Semantik der Mobile IP-Ende Nachricht beim Fast-Forwarding Protokoll (siehe Abschnitt 6.1.2), gibt eine weitere IP-Adresse in der Notify-Nachricht den Urheber der Mobile IP-Ende Nachricht an. Dazu gibt es zwei Varianten: Der Home Agent oder ein Fast-Forwarding Agent sendet die Mobile IP-Ende Nachricht.

1. Sollte eine Forwardingkette aufgelöst werden (vgl. Abbildung 6.4), meldet sich der lokale Foreign Agent direkt beim Home Agent (bzw. beim ersten Foreign Agent) an, der dann eine Mobile IP-Ende Nachricht hop-by-hop entlang der Forwardingkette sendet. Diese gelangt dann auch zum lokalen Foreign Agent, der die lokale Unterstützung für den mobilen Teilnehmer aber nicht beenden soll. Deswegen wird in diesem Fall in der zweiten IP-Adresse der Notify-Nachricht die des lokalen Foreign Agents eingetragen, dem eigentlichen Verursacher der Auflösung der Forwardingkette. Dieser kann somit die Mobile IP-Ende Nachricht ignorieren.

2. Im Zuge einer Schleifenauflösung sendet der neue Foreign Agent eine Mobile IP-Ende Nachricht an seinen ehemaligen Nachfolger in der Forwardingkette. Falls diese Nachricht wegen ungünstiger Umstände, z. B. einer Routingschleife, zum neuen Foreign Agent zurückkommen sollte, kann der neue Foreign Agent anhand der zweiten IP-Adresse erkennen, daß diese von ihm ausgegangen ist. Damit wird er sie nicht weiterleiten und auch nicht die lokale Unterstützung für das mobile System beenden.

Zustandsautomat

Für den Zustandsautomat eines Foreign Agents (siehe Abschnitt 2.5.2) ergeben sich durch das Fast-Forwarding Protokoll drei weitere Eingabeereignisse:

1. ffNotify: Der Foreign Agent hat eine Fast-Forwarding Notify erhalten und soll in Zukunft das mobile System als Fast-Forwarding Agent unterstützen.

2. ffAck: Der mit der Fast-Forwarding Notify angesprochene Foreign Agent unterstützt das Fast-Forwarding Protokoll und hat eine Fast-Forwarding Acknowledge an den Foreign Agent zurückgeschickt.

3. ffNack: Der so angesprochene Foreign Agent unterstützt das Fast-Forwarding Protokoll nicht und hat die Fast-Forwarding Notify mit einer Fast-Forwarding Negative Acknowledge beantwortet.

Zusätzlich kann ein Foreign Agent zwei weitere Zustände einnehmen:

1. PendingNotify: Der lokale Foreign Agent hat dem alten Foreign Agent eine Fast-Forwarding Notify geschickt und wartet auf die Antwort.

2. Fastforward: Der Foreign Agent hat vom nächsten Foreign Agent in der Forwardingkette eine Fast-Forwarding Notify bekommen, diese bestätigt und sendet nun Daten an den Mobilteilnehmer entlang der Forwardingkette. Der Zustand kennzeichnet also, daß der Foreign Agent als Fast-Forwarding Agent arbeitet.

Damit ergibt sich der in der Abbildung 7.5 erweiterte Zustandsautomat, wobei das Versenden einer MobileIP-Ende Nachricht (siehe Abschnitt 7.3.5) und die frühe lokale Unterstützung (siehe Abschnitt 7.3.4) bereits eingearbeitet sind.

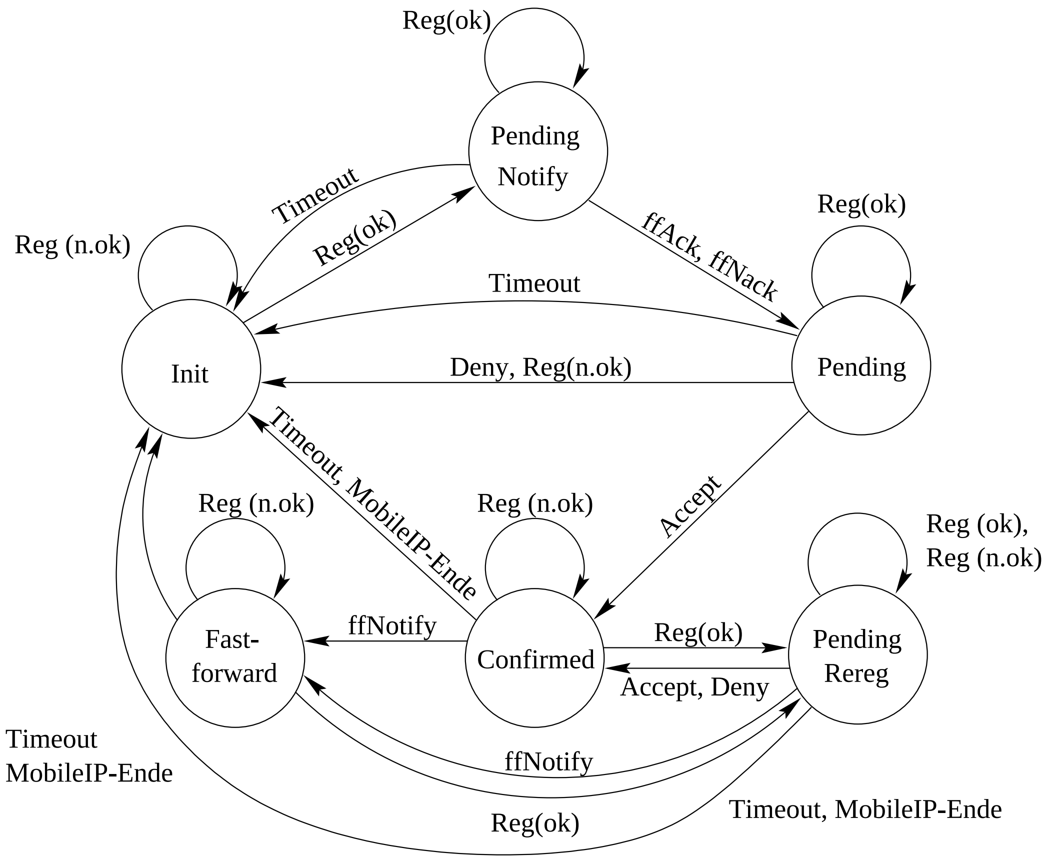

Abbildung 7.5: Zustandsautomat des Foreign Agents beim Fast-Forwarding Protokoll

Die folgenden Abschnitte beschreiben das Vorgehen des Foreign Agents in den beiden neuen Zuständen.

PendingNotify Ein lokaler Foreign Agent wechselt in den „Pending Notify“-Zustand, wenn er vom mobilen System eine Registrierungsanforderung mit angehängter IP-Adresse des alten Foreign Agents bekommt. Dem alten Foreign Agent sendet er eine Fast-Forwarding Notify und wartet in diesem Zustand auf eine Antwort. Sendet der alte Foreign Agent eine Fast-Forwarding Acknowledge, geht der lokale Foreign Agent in den „Pending"-Zustand über. Daraufhin sendet er die Registrierungsanforderung über die Forwardingkette zum Home Agent und wartet auf die Registrierungsantwort. Sollte der alte Foreign Agent eine Fast-Forwarding Negative Acknowledge senden, wechselt der lokale Foreign Agent auch in den Zustand „Pending", sendet die Registrierungsanforderung aber direkt zum Home Agent bzw. zum ersten Foreign Agent (vgl. Abschnitt 6.5).

Geht die Fast-Forwarding Notify verloren, erhält der lokale Foreign Agent nach einer gewissen Zeit eine erneute Registrierungsanforderung vom mobilen System. Dadurch verändert sich aber sein Zustand nicht, er wartet dann weiterhin auf eine Antwort.

Fastforward Ein lokaler Foreign Agent wechselt in den „Fastforward"-Zustand, wenn er von einem anderen Foreign Agent eine Fast-Forwarding Notify erhält und mit einer Fast-Forwarding Acknowledge bestätigt. Das mobile System hat also das Subnetz gewechselt und wünscht die Anwendung des Fast-Forwarding Protokolls. Damit wird dieser Foreign Agent zum Fast-Forwarding Agent für das mobile System: Er leitet alle Registrierungsanforderungen zu seinem Vorgänger in der Forwardingkette und alle Registrierungsantworten zu seinem Nachfolger.

Der Fast-Forwarding Agent verläßt diesen Zustand, wenn er direkt vom mobilen System eine Registrierungsanforderung bekommt. In diesem Fall geht er in den „Pending Rereg"-Zustand über (Schleifenauflösung), weil das mobile System bereits einmal bei ihm erfolgreich registriert war. Bei einem Timeout oder beim Erhalt einer Mobile IP-Ende Nachricht wechselt der Fast-Forwarding Agent direkt in den „Init"-Zustand.

7.6 Nicht implementierte Konzepte

Die folgenden Konzepte fanden bei der Implementierung keine Berücksichtigung:

- Route Optimization.
- Ausfall eines Mobility Agents beim schnellen Agent Discovery Verfahren.
- Authentifizierung einer Mobile IP-Ende Nachricht.
- Periodische Deregistrierungsanforderung im Falle einer frühen lokalen Unterstützung.
- Delayed Migration beim Subnetzwechsel.
- Subnetzwechsel in RSVP mit Ablehnung einer Reservierung wegen nicht vorhandener Ressourcen.
- RSVP-Dämonen auf Basisstationen.
- Tunneln von Multicast-Daten durch den Home Agent an das mobile System.

- Signalisierung einer IPIP-Tunnel-Reservierung durch RSVP.
- Reduktion des Protokolloverheads bei der Kombination von Mobile IP und RSVP.
- Tunneln der Nachrichten von einem mobilen Teilnehmer zum ersten Foreign Agent mit dem Transport Gateway.
- Authentifizierung der Nachrichten des Fast-Forwarding Protokolls.

7.7 Messungen

Dieser Abschnitt soll die in den vorangegangenen Kapiteln getroffenen Aussagen durch Meßwerte verifizieren.

7.7.1 Das schnelle Agent Discovery Verfahren

Hinsichtlich des schnellen Agent Discovery Verfahrens wurde überprüft, wie schnell ein mobiles System mit diesem Verfahren die gewünschten Informationen erhält. Dabei ist zu beachten, daß sowohl Agent Solicitations als auch Agent Advertisements mittels UDP versendet werden und damit verloren gehen können. Drei verschiedene Messungen haben die folgenden Ergebnisse geliefert:

1. Bei einer unbelasteten Netzverbindung vom mobilen System zum Mobility Agent dauert es 5 ms in beiden Testszenarien (vgl. Abschnitt 7.1) vom Aussenden der Agent Solicitation bis zum Eintreffen der Agent Advertisement auf dem mobilen System. Hierbei treten keine Verluste von Nachrichten auf.

2. Im Falle einer Belastung der drahtgebundenen Strecke vom Mobility Agent zur Basisstation ergibt sich eine Verzögerung von bis zu 90 ms. Dabei gehen im Durchschnitt die ersten beiden ausgesendeten Agent Solicitations verloren.

3. Bei einer Belastung der drahtlosen Strecke beträgt die Verzögerung bis zu 500 ms, weil viele Agent Solicitations bzw. Agent Advertisements verloren gehen. Das mobile System wiederholt die Agent Solicitations mittels eines exponentiellen Backoff-Timers, deswegen verursacht ein Verlust von etwa zehn aufeinanderfolgenden Agent Solicitations die angegebene Verzögerung.

Die Belastung des Netzwerkes wurde mithilfe des Befehls `ping -f -l 100000` erzeugt, welcher den angegebenen Teil des Netzwerkes mit einer Datenrate von etwa 1.5 Mbps in den ersten zehn Sekunden belastet.

7.7.2 Erkennung einer Routenänderung in RSVP

Dieser Abschnitt gibt Meßwerte über die Dauer der Reservierung einer neuen Strecke nach einem Subnetzwechsel. Dabei werden die Werte, wenn nur das Ablaufen der Soft-State Timer eine Reservierung der neuen Strecke bewirkt, mit denen verglichen, wenn Mobile IP ein Signal über einen Subnetzwechsel gibt.

Die verwendete RSVP-Implementierung

Die verwendete RSVP-Implementierung verfügt über keinen Local Repair Mechanismus zur Benachrichtigung von RSVP im Falle einer Routenänderung. Deswegen wird die Reservierung nach einer Routenänderung erst nach Ablauf des Soft-State Timers erneuert. Messungen haben bestätigt, daß es nach einem Subnetzwechsel bis zu eine komplette Soft-State Periode (30 s $\pm$ 50%) dauert, bis der Home Agent eine Path-Nachricht wiederholt.

Desweiteren haben Messungen ergeben, daß es bis zu eine weitere Soft-State Periode dauert, bis das mobile System eine Resv-Nachricht generiert, nachdem es nach einem Subnetzwechsel die Path-Nachricht vom neuen Previous Hop erhalten hat. Hier zeigt sich ein Fehler in der Implementierung: Erhält ein RSVP-Dämon eine Path-Nachricht mit einem anderen Previous Hop als die letzte erhaltene Path-Nachricht, sollte er sofort für alle dazugehörigen Reservierungen eine Resv-Nachricht generieren [BraZha97, S. 49]. Diese Funktionalität bietet die verwendete Implementierung nicht.

Es ergibt sich also insgesamt eine Zeit von bis zu 90 Sekunden, bis nach einem Subnetzwechsel eine Strecke wieder vollständig reserviert ist. In dem verwendeten Testszenario ist kein weiteres System in das Weiterleiten der Path-Nachricht vom Home Agent zum Foreign Agent involviert. Sollte das der Fall sein, wird sich aber die genannte Zeit nicht wesentlich erhöhen, weil die beteiligten Zwischensysteme auf der Route zum neuen Subnetz noch keinen Path State Block für die RSVP-Sitzung besitzen und die Path-Nachricht damit unmittelbar weiterleiten. Selbst in einem Weitverkehrsszenario ist die für die Verarbeitung und das Weiterleiten der Path-Nachricht benötigte Zeit im Vergleich zu den genannten 90 Sekunden zu vernachlässigen. Weil die Zwischensysteme auch noch keine Informationen über eine Reservierung besitzen, leiten sie auch die Resv-Nachricht vom mobilen System unmittelbar weiter, auch hier erhöht sich die Zeit für die Wiederherstellung der Reservierung nicht wesentlich.

Signalisierung durch Mobile IP

Mit der in Abschnitt 5.4.2 dargestellten Signalisierung eines Subnetzwechsels durch Mobile IP ergeben sich folgende Resultate für das erste Testszenario:

1. Wechsel in ein fremdes Subnetz: Es dauert etwa 40 ms vom Absenden des Signals durch Mobile IP auf dem Home Agent, bis die schnelle Resv-Nachricht wieder vom mobilen System beim Home Agent ankommt.

2. Wechsel zum Heimatsubnetz: Es dauert etwa 25 ms bis zur Ankunft der schnellen Resv-Nachricht.

Bei diesen Zahlen muß aber beachtet werden, daß in den verwendeten Testszenarien die fremden Subnetze direkt am Heimatsubnetz angeschlossen sind. Damit ergibt sich so gut wie keine Verzögerung der Daten zwischen Heimatsubnetz und fremden Subnetz, welche aber in einem realen Szenario auf die Zeit beim Wechsel in ein fremdes Subnetz addiert werden muß.

Beide Messungen fanden in einem Netzwerk mit geringer Belastung statt, es traten also keine Verluste von Nachrichten auf.

7.7.3 Das Fast-Forwarding Protokoll

Dieser Abschnitt vergleicht das Fast-Forwarding Protokoll mit einer herkömmlichen Registrierung in Mobile IP. Dabei soll die Mobile IP Handover-Zeit gemessen werden (vgl. Abschnitt 5.1.5). Messungen in Verbindung mit einer RSVP-Tunnelsitzung waren nicht möglich, weil keine Implementierung dieser Tunnel zur Verfügung stand.

Um ein Weitverkehrsszenario zu simulieren, wurden die beiden Foreign Agents modifiziert: Sie verzögern Daten vom Heimatsubnetz in die beiden fremden Subnetz und auch umgekehrt um eine beliebig wählbare Dauer. Der Datenaustausch zwischen den beiden fremden Subnetzen ist davon nicht betroffen, obwohl auch dieser Verkehr im Testszenario über das Heimatsubnetz läuft.

Dauer der Unterbrechung bei einer Registrierung

Wenn ein mobiles System das Subnetz wechselt, erhält es für eine gewisse Zeit keine Daten vom Home Agent. Dieser Abschnitt vergleicht die Dauer dieser Unterbrechung bei einer herkömmlichen Registrierung mit Mobile IP mit der modifizierten Registrierung unter Verwendung des Fast-Forwarding Protokolls.

Herkömmliche Registrierung Im Falle einer herkömmlichen Mobile IP Registrierung muß die Registrierungsanforderung vom mobilen Teilnehmer über den Foreign Agent zum Home Agent gelangen, bis das mobile System wieder für den Home Agent erreichbar ist. Es dauert dann noch einmal dieselbe Zeit, bis die ersten Daten (insbesondere die Registrierungsantwort) wieder beim Home Agent ankommen. Insgesamt gibt es Datenverkehr auf vier Teilstrecken:

1. Die Registrierungsanforderung vom mobilen System zum Foreign Agent (unverzögert)
2. Die Registrierungsanforderung vom Foreign Agent zum Home Agent (verzögert)
3. Daten und die Registrierungsantwort vom Home Agent zum Foreign Agent (verzögert)
4. Daten und die Registrierungsantwort vom Foreign Agent zum mobilen System (unverzögert).

Die gesamte Zeit der Unterbrechung aus Sicht des mobilen System beträgt ohne künstliche Verzögerung etwa 20 ms. Verzögert man alle Daten zwischen dem Heimatsubnetz und dem fremden Subnetz, kommt dieser Wert auf die Dauer der künstlichen Verzögerung hinzu. Bei einer Verzögerung von 100 ms beträgt der Wert 220 ms, im Falle einer Verzögerung von 150 ms liegt er bei 320 ms usw. Diese Messungen wurden im Falle eines unbelasteten Netzwerkes vorgenommen, so daß keine Verluste von Nachrichten auftraten.

Registrierung mit dem Fast-Forwarding Protokoll Bei einer Registrierung mit dem Fast-Forwarding Protokoll ist diese Unterbrechungsdauer unabhängig von der künstlichen Verzögerung. Auch hier ergeben sich vier Teilstrecken:

1. Die Registrierungsanforderung vom mobilen System zum neuen Foreign Agent (unverzögert)
2. Die Fast-Forwarding Notify vom neuen zum alten Foreign Agent (unverzögert)
3. Daten und die Fast-Forwarding Acknowledge vom alten zum neuen Foreign Agent (unverzögert)
4. Daten vom neuen Foreign Agent zum mobilen System (unverzögert)

Der Wert der Verzögerung liegt ebenfalls bei etwa 20 ms.

Fazit: Unterbrechungsdauer Die Dauer einer Unterbrechung während einer Registrierung in einem fremden Subnetz kann also bei einer herkömmlichen Registrierung mit Mobile IP sehr groß werden, abhängig von der Verzögerungszeit zwischen dem Heimatsubnetz und dem fremden Subnetz. Im Falle einer Registrierung mit dem Fast-Forwarding Protokoll ist diese Dauer nahezu konstant und nur abhängig von der Verzögerungszeit zwischen dem alten und dem neuen Subnetz.

Durchsatzmessungen mit TCP

Um die herkömmliche Registrierung mit Mobile IP mit der Registrierung unter Verwendung des Fast-Forwarding Protokolls zu vergleichen, wurde der Durchsatz einer TCP-Verbindung zwischen dem Home Agent und dem mobilen System gemessen. Als Verfahren zur Übertragungswiederholung kam das in TCP übliche Go-Back-N Verfahren zum Einsatz, obwohl die Linux 2.1.x Kernel auch selektive Übertragungswiederholungen nach RFC 2018 [MatMah96] zur Verfügung stellen. Zur Erkennung eines Subnetzwechsels wurde das schnelle Agent Discovery Verfahren angewendet. Während der Übertragung der Daten wechselte das mobile System mehrfach von einem fremden Subnetz zum anderen.

Die Messungen wurden zweimal durchgeführt: Einmal mit zwei Subnetzwechseln pro Minute und einmal mit vier. Jede Meßreihe umfaßte zehn verschiedene Verzögerungen: 0, 10, 20, 40, 60, 80, 100, 120, 150 und 200 Millisekunden. Jede einzelne Messung dauerte 60 Sekunden und wurde acht Mal wiederholt. Messungen, die um mehr als die Hälfte vom

Mittelwert abwichen, wurden nicht berücksichtigt, weil dann meistens externe Faktoren die Messung stark beeinflußt haben. Der Datendurchsatz einer Transportverbindung mit TCP ist besonders empfindlich gegenüber externen Einflüssen wegen der Staukontrolle von TCP. Die Übertragung auf dem Funkkanal war nahezu verlustfrei, die gemessene Fehlerrate lag unterhalb von einem Prozent.

Messung ohne Funkzellenwechsel Um das Verhalten von TCP ohne Funkzellenwechsel bei unterschiedlichen Verzögerungen studieren zu können, wurden in einer ersten Messung nur die Übertragungsraten in Abhängigkeit von der Verzögerung betrachtet. Abbildung 7.6 zeigt das Ergebnis.

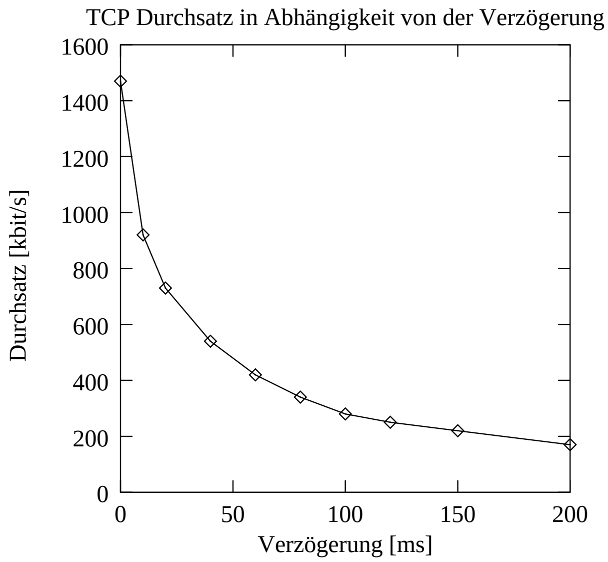

Abbildung 7.6: Ergebnis der Messung des Durchsatzes ohne Subnetzwechsel

Man sieht, wie der Datendurchsatz exponentiell mit der Verzögerung zwischen dem Home Agent als Sender und dem mobilen System als Empfänger fällt. Es ist allerdings möglich, daß dieser Verhalten von der TCP-Implementierung im Linux 2.1.x Kernel abhängig ist. Diese Messung sollte deshalb noch mit anderen TCP-Implementierungen durchgeführt werden, um diese Werte zu überprüfen.

Die Tunnel als Störfaktoren Bei einer ersten Meßreihe ohne Subnetzwechsel stellte sich heraus, daß die Tunnel zwischen dem Home Agent zu den beiden Foreign Agents die Meßwerte erheblich beeinflußten, wenn die Daten verzögert wurden. Es traten nicht nachzuvollziehende und sehr unregelmäßige Schwankungen der Übertragungsraten ein. Die obige Messung wurde ohne das Tunneln der TCP-Pakete vom Home Agent zum Foreign Agent durchgeführt, der Home Agent leitete die Daten direkt zu den Foreign Agents.

Für den folgenden Vergleich zwischen den Messungen mit bzw. ohne Fast-Forwarding ist es aber unerheblich, ob die Daten getunnelt werden. Der durch das Tunneln verursachte

Overhead besteht nur aus der Übertragung eines zusätzlichen IP-Headers und einer evtl. Bearbeitungszeit für das Aus- und Einkapseln der getunnelten Pakete. Es ist zwar denkbar, daß dieser Overhead den Datendurchsatz negativ beeinflußt. Da dieses aber beide Messungen in gleichem Maße betrifft, verändert es den Vergleich zwischen beiden Messungen nicht.

Der Tunnel zwischen dem alten und dem neuen Foreign Agent beim Fast-Forwarding wurde dagegen beibehalten. Dieser hat die Messungen nicht beeinflußt, weil die Daten zwischen dem alten und neuen Foreign Agent nicht verzögert wurden.

Zwei Subnetzwechsel pro Minute Abbildung 7.7 zeigt den zeitlichen Verlauf des Datendurchsatzes bei einer TCP-Verbindung, wenn das mobile System zweimal pro Minute das Subnetz wechselt.

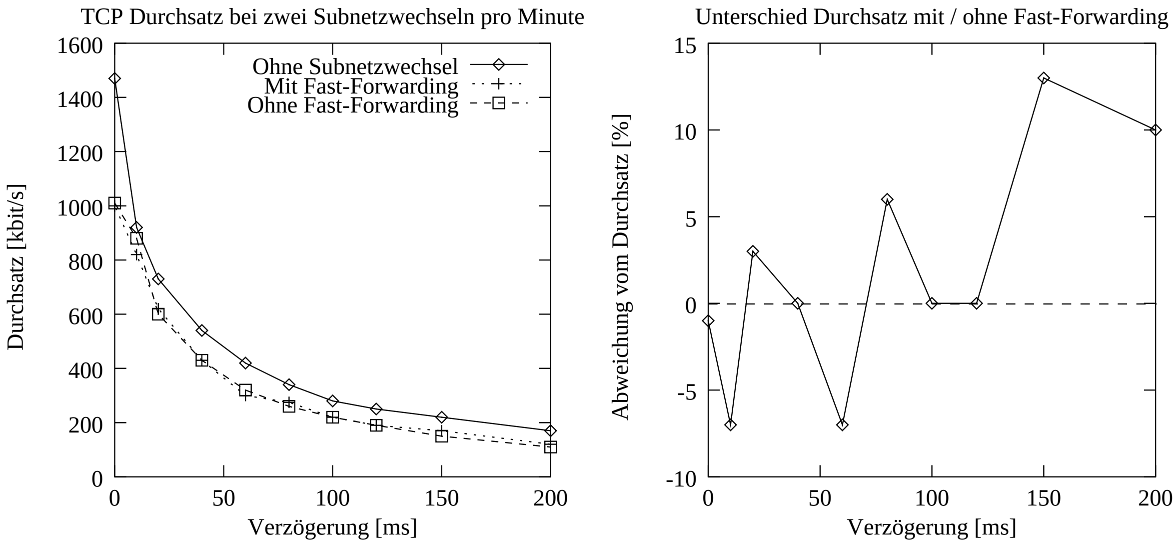

Abbildung 7.7: Ergebnis der Messung des Durchsatzes mit zwei Subnetzwechseln / min

Die Unterbrechung der Verbindung dauert pro Subnetzwechsel nur etwa die in Abschnitt 7.7.3 genannten 20 ms mit Fast-Forwarding bzw. bis zu 440 ms ohne Fast-Forwarding. Die Staukontrolle in TCP bewirkt aber, daß der Durchsatz bei beiden Verfahren für die Registrierung dennoch um bis zu 30% gegenüber der Messung ohne Subnetzwechsel fällt.

Diese Verluste sind insbesondere bei einer geringen Verzögerung von Null bis zehn Millisekunden sehr groß. Dies liegt daran, daß bei den geringen Verzögerungen die drahtlose Strecke sehr stark ausgelastet ist und Verluste von Paketen aufgrund von Kollisionen häufig auftreten. Diese Verluste betreffen dann auch die Agent Solicitations bzw. Registrierungsanforderungen, so daß der Registrierungsvorgang mehr Zeit benötigt und die Verluste beim Durchsatz bewirkt.

Einen geringen Vorteil des Fast-Forwardings aufgrund der kürzeren Verbindungsunterbrechung zeigt der rechte der Teil der obigen Abbildung. Für dieses Diagramm wurde der Unterschied im Durchsatz zwischen einer Registrierung mit bzw. ohne Fast-Forwarding prozentual berechnet. Bei einer Verzögerung von 60 ms lag der Durchsatz der Registrierung mit Fast-Forwarding z. B. um 7% unter dem Durchsatz ohne Fast-Forwarding, bei 100 ms war der Durchsatz beider Verfahren identisch. Insgesamt ist in diesem Diagramm zu sehen, daß bis zu einer Verzögerung von 150 ms beide Verfahren einen annähernd gleichen Durchsatz haben. Der Durchsatz beider Verfahren bewegt sich in einem Bereich von $\pm 8\%$, wobei diese Schwankungen schon allein auf das sprunghafte Verhalten von TCP zurückgeführt werden können.

Ab einer Verzögerung von 150 ms erzielt man bei einer Registrierung mit dem Fast-Forwarding einen um etwa zehn Prozent höheren Durchsatz, wobei man diesen Wert aber auch wieder unter Berücksichtigung der von TCP selbst verursachten Schwankungen sehen muß.

Vier Subnetzwechsel pro Minute Abbildung 7.8 zeigt den Verlauf des Datendurchsatzes bei einer TCP-Verbindung, wenn das mobile System viermal pro Minute das Subnetz wechselt.

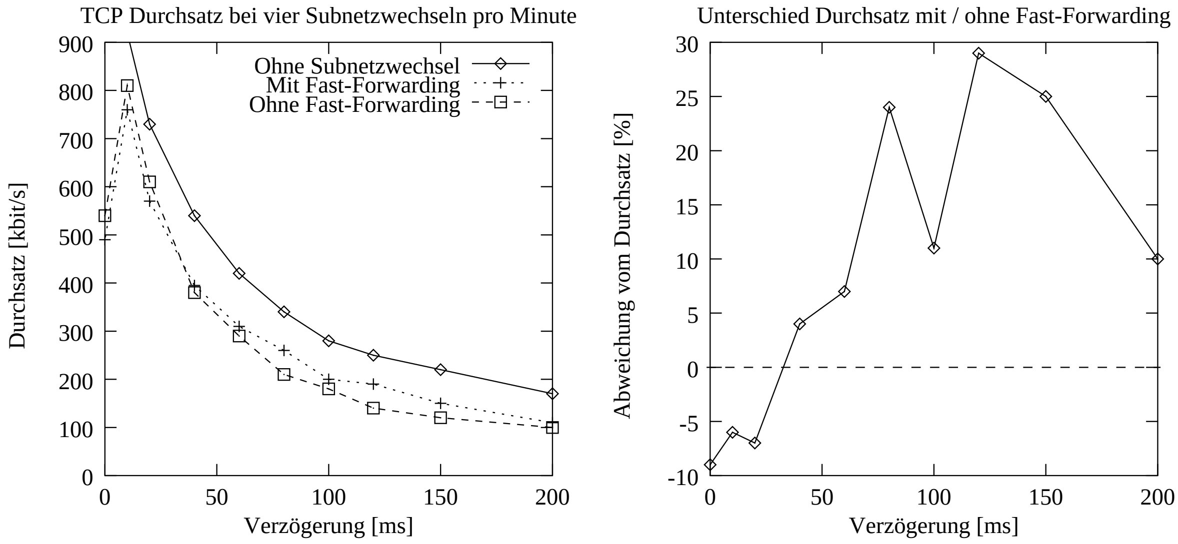

Abbildung 7.8: Ergebnis der Messung des Durchsatzes mit vier Subnetzwechseln / min

Im linken Diagramm läßt sich bereits ein Vorteil der Registrierung mit dem Fast-Forwarding erkennen. Ab einer Verzögerung von 80 ms liegt der Durchsatz erkennbar über dem der Registrierung ohne Fast-Forwarding.

Wie bereits bei der Messung mit zwei Subnetzwechseln pro Minute kann man auch hier sehen, daß der Durchsatz bei geringen Verzögerungen sehr niedrig ist. Dies ist ebenfalls auf verlorene Nachrichten des Agent Discovery Verfahrens bzw. der Registrierung und damit eine längere Dauer der Registrierung zurückzuführen

In rechten Diagramm der Abbildung wird der Vorteil der Registrierung mit Fast-Forwarding beim Durchsatz noch deutlicher. Zunächst hat im Falle einer Verzögerung von weniger als 80 ms die Registrierung ohne Fast-Forwarding einen höheren Durchsatz. Dies kann darauf zurückgeführt werden, daß beim Fast-Forwarding der Tunnel zwischen dem alten und dem neuen Foreign Agent einen gewissen Overhead erzeugt, es kann sich aber auch um für TCP typische Schwankungen handeln. Ab einer Verzögerung von 80 ms liegt der Durchsatz beim Fast-Forwarding aber deutlich über dem des herkömmlichen Verfahrens in Mobile IP, auch wenn man die für TCP typischen Schwankungen in der Übertragungsrate in die Überlegungen mit einbezieht.

Den Grund für den höheren Durchsatz bei einer Registrierung mit Fast-Forwarding illustriert die folgende Abbildung 7.9.

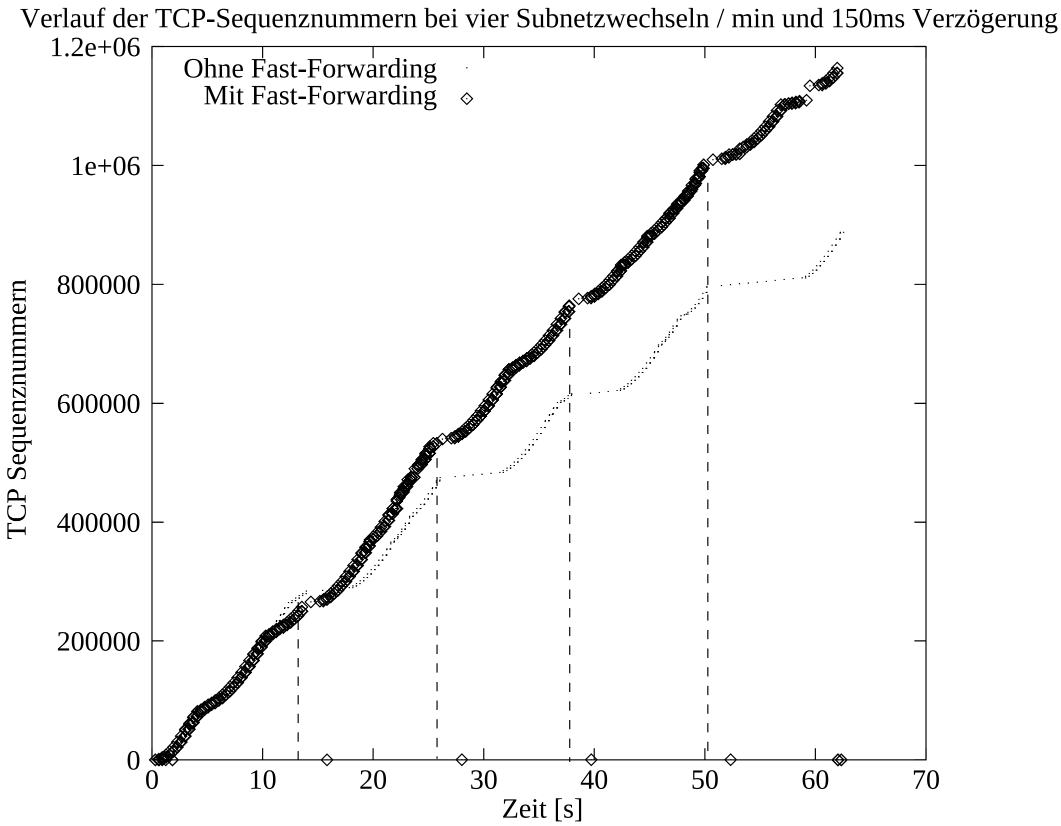

Abbildung 7.9: Auswertung bei 150 ms Verzögerung und vier Subnetzwechseln / min

In dieser Abbildung sind auf der y-Achse die TCP-Sequenznummern aufgetragen, die ein Mitschnitt des Datenverkehrs einer Messung mittels `tcpdump` [JacLer97] ergeben hat. Die x-Achse gibt die fortschreitende Zeit an, die Messung hat also 60 Sekunden gedauert. Die senkrechten, gestrichelten Linie geben die Zeitpunkte an, zu denen ein Subnetzwechsel vorgenommen wurde.

Man kann in diesem Diagramm erkennen, daß bei Verwendung des Fast-Forwarding Protokolls (obere Kurve) die Datenübertragung nach einem Subnetzwechsel sehr viel schneller wieder aufgenommen wird als bei einer Registrierung ohne Fast-Forwarding. Ohne Verwendung des Fast-Forwarding Protokolls dauert es bei der in diesem Beispiel verwendeten Verzögerung von 150 ms etwa 320 ms, bis wieder Daten vom Home Agent zum mobilen System gelangen können. Mit Verwendung des Fast-Forwarding Protokolls beträgt diese Unterbrechung nur etwa 20 ms.

7.7.4 Fazit

Die Messungen haben also ergeben, daß ein mobiles System durch das schnelle Agent Discovery Verfahren einen Subnetzwechsel sehr viel schneller erkennen kann als durch periodisch ausgesendete Agent Advertisements. Die Erkennung einer Routenänderung in RSVP wird durch das von Mobile IP an den RSVP-Dämon gesendete Signal bei einem Subnetzwechsel ebenfalls erheblich beschleunigt. Schließlich bewirkt das Fast-Forwarding Protokoll eine deutliche Verkürzung der Mobile IP Handover-Zeit nach einem Subnetzwechsel, wenn zwischen dem Heimatsubnetz und dem fremden Subnetz eine Verzögerung von etwa 80 ms oder mehr vorliegt.

7.8 Zusammenfassung

Die in diesem Kapitel dargestellte Implementierung der Konzepte, insbesondere des Fast-Forwarding Protokolls, paßt sich also ohne größere Probleme in die vorhandenen Implementierungen von Mobile IP und RSVP ein. Änderungen auf dem mobilen System sind in der Hauptsache für das schnelle Agent Discovery Verfahren und in geringem Umfang für das Fast-Forwarding Protokoll nötig. Der Home Agent ist beim Senden von Mobile IP-Ende Nachrichten an den alten Foreign Agent, bei der Integration des indirekten Transportansatzes in Mobile IP und bei der Signalisierung zwischen Mobile IP und RSVP von Änderungen betroffen. Die Foreign Agents sind in großem Umfang in die Implementierung des Fast-Forwarding Protokolls und der frühen lokalen Unterstützung involviert.

Schwierigkeiten bei der Implementierung gab es an zwei Stellen:

1. Adreßauflösung beim Agent Discovery auf dem mobilen System.
2. Verwendung von ProxyARP im Heimatsubnetz.

Das erste konnte durch das zusätzliche Versenden der MAC-Adresse der Mobility Agents in den Agent Advertisements gelöst werden. Im zweiten Fall wurde das MIPdum Interface eingerichtet, um ProxyARP auch im Heimatsubnetz verwenden zu können. Beide Probleme ließen sich bei einer Mobile IP Implementierung, die teilweise im Kernel liegt, umgehen.

Kapitel 8

Zusammenfassung und Ausblick

Mobile IP und RSVP lassen sich im Grundsatz gut miteinander kombinieren, auch unter Berücksichtigung des indirekten Transportansatzes. Bei der Integration der Protokollabläufe muß beachtet werden, daß eine Ressourcenreservierung zu einem mobilen Empfänger eine separate Reservierung des IPIP-Tunnels zwischen dem Home Agent und dem Foreign Agent erfordert.

Die Betrachtung von Mobile IP unter dem Aspekt der Dienstgüte ergibt, daß die Zeit für die Erkennung eines Subnetzwechsels von bis zu einer Sekunde zu lang ist. Diese läßt sich durch ein schnelles Agent Discovery Verfahren unter Einbeziehung der Sicherungsschicht auf etwa fünf Millisekunden verkürzen. Dieses Verfahren reduziert auch den Protokolloverhead, den Mobile IP verursacht. Außerdem erfährt ein mobiles System, welches sich weit von seinem Heimatsubnetz entfernt hat und dann das Subnetz wechselt, eine lange Unterbrechung der Verbindung wegen der langen Umlaufzeit zwischen Heimatsubnetz und fremden Subnetz. Das Fast-Forwarding Protokoll verringert diese Unterbrechungszeit und zusätzlich mögliche Datenverluste beim Wechsel. In Abhängigkeit von der Entfernung zwischen dem Heimatsubnetz und dem fremden Subnetz kann der Datendurchsatz im Falle einer TCP-Verbindung um bis zu 20% steigen. Desweiteren verhindert das Fast-Forwarding Protokoll, daß die Wiederherstellung einer Ressourcenreservierung auf der Strecke vom Heimatsubnetz zum fremden Subnetz bei jedem Subnetzwechsel notwendig wird.

Bei der Kombination von Mobile IP und dem indirekten Transportansatz ist die Plazierung des Transport Gateways im Heimatsubnetz problematisch. Durch eine spezielle lokale Unterstützung durch den Home Agent kann das Transport Gateway auf diesem realisiert werden.

Die Analyse von RSVP unter dem Aspekt der Mobilität ergibt eine mangelnde Abstimmung zwischen RSVP und dem Routingprotokoll. Dadurch benötigt die Wiederherstellung einer Reservierung nach einem Subnetzwechsel des mobilen Systems bis zu 30 Sekunden. Eine Signalisierung zwischen beiden Protokollen kann diese Zeit in Abhängigkeit von der Entfernung zwischen dem Heimatsubnetz und dem fremden Subnetz deutlich verkürzen. Desweiteren ergibt die Untersuchung von RSVP in Verbindung mit Mobilität in einem lokalen Netz, daß RSVP-Dämonen auf allen Basisstationen plaziert werden sollten, um eine Reservierung in den einzelnen Funkzellen des lokalen Netzes zu ermöglichen.

Ausblick

Die Implementierung konnte wegen der vorhandenen Testumgebung nicht alle in dieser Arbeit vorgestellten Konzepte berücksichtigen. Das schnelle Agent Discovery Verfahren, der grundsätzliche Protokollablauf des Fast-Forwarding Protokolls sowie die Signalisierung einer Routenänderung an RSVP nach einem Subnetzwechsel wurden vollständig implementiert. Allerdings konnten keine umfassenden Tests mit mehreren Basisstationen und mobilen Systemen durchgeführt werden. Es bleibt also noch zu überprüfen, wie sich ein größeres Szenario auf die Implementierung auswirkt. Dennoch konnten Messungen an einem einfachen Testszenario die Vorteile dieser beiden Verfahren bestätigen.

Außerdem ist die Integration des indirekten Transportansatzes in die Implementierung zu untersuchen. Messungen hinsichtlich des Datendurchsatzes bei der Kombination des Fast-Forwarding Protokolls mit dem indirekten Transportprotokoll wären von Interesse.

Auf konzeptioneller Ebene ist für den indirekten Transportansatz noch ein Verfahren zu entwickeln, welches über den Beginn einer verzögerten Migration eines Transport Gateways entscheidet.

Das Konzept der Route Optimization sollte ebenfalls noch auf eine Integration in die hier vorgestellten Ansätze untersucht werden, weil sich dadurch ein eventueller Umweg auf der Strecke vom Sender zu einem mobilen Empfänger vermeiden läßt.

Schließlich sind noch Kriterien beim Fast-Forwarding Protokoll zu erarbeiten, wann eine Forwardingkette zu beenden ist und damit eine direkte Verbindung in das Heimatsubnetz vorzuziehen ist.

Anhang A

Glossar

Dieser Anhang gibt Auskunft über die in dieser Arbeit verwendeten Begriffe, die in der linken Spalte angegeben sind. Bei Bedarf findet man dort auch die englischen Originalbegriffe. Rechts davon befindet sich eine kurze Erklärung mit der Angabe der Seite, auf welcher der Begriff eingeführt wird und sich also eine weitergehende Erklärung befindet.

Accept-Nachricht	Registrierungsantwort mit einer Bestätigung des vom mobilen System angeforderten Dienstes 14
alter Foreign Agent	Foreign Agent in dem Subnetz, aus dem sich ein mobiles System entfernt hat 84
Agent Advertisement	von Mobility Agents ausgesendete Nachricht, um Informationen über den angebotenen Mobile IP Dienst im Subnetz zu verbreiten 12
Agent Solicitation	vom mobilen System ausgestrahlte Nachricht, um Agent Advertisements von den Mobility Agents anzufordern 12
Agent Discovery	Verfahren, damit das mobile System einen Subnetzwechsel erkennen kann 12
Care-of Adresse	IP-Adresse, unter welcher der Home Agent das mobile System in einem fremden Subnetz erreichen kann 7
co-located Betrieb	Betriebsart von Mobile IP, bei der das mobile System selbst die Daten im fremden Subnetz entgegennimmt 9
co-located Care-of Adresse	Care-of Adresse beim co-located Betrieb 9
Delayed Migration	Verzögerung einer Migration 31

Deny-Nachricht	Registrierungsantwort mit einer Ablehnung des vom mobilen System angeforderten Dienstes . . . 14
Deregistrierung	Anmeldung des mobilen Systems beim Home Agent im Falle einer Rückkehr ins Heimatsubnetz . . . 11
Deregistrierungs-anforderung	Nachricht, die das mobile System bei einer Deregistrierung an den Home Agent schickt . . . 16
Dreiecksroute (triangular route)	Daten nehmen zum mobilen System einen anderen Weg als von diesem . . . 10
downstream	Richtung des Datenflusses in einer RSVP-Sitzung: vom Sender zum Empfänger . . . 36
erster Foreign Agent	in einer Forwardingkette der Foreign Agent mit direktem Kontakt zum Home Agent . . . 85
Fast-Forwarding Acknowledge	Nachricht des Fast-Forwarding Protokolls, mit der ein alter Foreign Agent dem neuen das Weiterleiten der Daten bestätigt 84
Fast-Forwarding Agent	alle Mobility Agents in einer Forwardingkette, die keinen direkten Kontakt zum mobilen System haben . . . 86
Fast-Forwarding Negative Acknowledge	wie eine Fast-Forwarding Acknowledge, nur lehnt der alte Foreign Agent das Weiterleiten ab . . . 85
Fast-Forwarding Notify	Nachricht des Fast-Forwarding Protokolls, mit der ein neuer Foreign Agent einen alten zum Weiterleiten der Daten auffordert . . . 84
Fast-Forwarding Protokoll	Erweiterung von Mobile IP, um die Unterbrechungsdauer und Paketverluste im Falle eines Subnetzwechsels zu reduzieren 52
Foreign Agent	System im fremden Subnetz, welches Daten für das mobile System entgegennimmt . . . 7
Forwardingkette	Aneinanderreihung von mehreren Fast-Forwarding Agent durch das mehrfache Anwenden des Fast-Forwarding Protokolls . . 85
fremdes Subnetz (foreign network)	Jedes Netzwerk, das nicht dem Heimatsubnetz entspricht . . . 6

frühe lokale Unterstützung	wie eine lokale Unterstützung, nur wird sie vor dem Eintreffen der Registrierungsantwort auf dem Foreign Agent errichtet 73
Heimatsubnetz (home network)	Das Netzwerk, zu dem die Heimatadresse gehört 6
Heimatadresse (home address)	IP-Adresse, unter der das mobile System grundsätzlich zu erreichen ist 6
Home Agent	System im Heimatsubnetz, welches Pakete für das mobile System zu dessem aktuellen Aufenthaltsort weiterleitet 7
Indirekter Transportansatz	Trennung der Transportverbindung zwischen einem stationären und einem mobilen Teilnehmer in zwei Teile 29
IPIP-Paket	IP-Paket, das in ein weiteres IP-Paket eingekapselt ist 8
IPIP-Tunnel	Strecke, auf der sich IPIP-Pakete mit derselben Zieladresse bewegen 8
IP-Standardrouting	Das Weiterleiten eines IP-Paketes anhand der Zieladresse ...5
Lebensdauer	Eine Registrierung ist nur diese bestimmte Zeit gültig, weswegen sie periodisch wiederholt werden muß 15
Local Repair	Methode zur schnellen Wiederherstellung einer Reservierung nach einer Routenänderung 41
Lokale Unterstützung	Mechanismus auf einem Mobility Agent, um ein mobiles System in demselben Subnetz mittels Mobile IP zu unterstützen 22, 56
lokaler Foreign Agent	Foreign Agent mit direktem Kontakt zum mobilen System .86
Migration	Verlagerung des Transport Gateways auf ein anderes System 31
Migrationspause	Unterbrechung der Verbindung zu einem mobilen Teilnehmer während der Migration des Transport Gateways 31
Mobile IP	Erweiterung zum Internet Protokoll (IP) für die Unterstützung von Mobilität 5
Mobile IP-Ende Nachricht	Nachricht an den Foreign Agent im alten Subnetz, daß das mobile System das Subnetz gewechselt hat 49

Mobile IP-Erweiterung	Mechanismus zur Erweiterung von Mobile IP-Nachrichten . . 11
Mobile IP Handover-Zeit	Dauer der Unterbrechung der Datenübertragung vom Home Agent zum mobilen System bei einem Subnetzwechsel 51
Mobile IP-Nachricht	Registrierungsanforderung oder Registrierungsantwort 14
Mobility Agent	Home Agent oder Foreign Agent 9
Mobility Agent Advertisement	Mobile IP Erweiterung in einer Agent Advertisement 12
neuer Foreign Agent	Foreign Agent im Subnetz, zu dem ein mobiles System gewechselt ist 84
Next Hop	nächstes Zwischensystem in Richtung des Empfängers in einer RSVP-Sitzung 37
Notify-Nachricht	Oberklasse für alle drei Fast-Forwarding Nachrichten 110
Path-Nachricht	transportiert die Daten eines Path State Blocks downstream zum Empfänger einer RSVP-Sitzung 36
PathTear-Nachricht	transportiert die Information über das Ende einer RSVP-Sitzung downstream 38
Previous Hop	nächstes Zwischensystem in Richtung des Senders in einer RSVP-Sitzung 37
Path State Block	Information in jedem RSVP-Dämon, die für das Weiterleiten der Resv-Nachrichten benötigt werden 36
Registrierung (registration)	Benachrichtigung des Home Agents über den aktuellen Aufenthaltsort des mobilen Systems 7
Registrierungsanforderung (registration request)	Nachricht, die das mobile System bei einer Registrierung an den Home Agent schickt 14
Registrierungsantwort (registration reply)	Nachricht, die der Home Agent als Antwort auf eine Registrierungsanforderung an das mobile System schickt 14

Registrierungstimer	Timer auf den Mobility Agents und dem mobilen System, der die Lebensdauer einer Registrierung überwacht 15
Replay Protection	Schutzmechanismus gegen das wiederholte Aussenden authentifizierter Mobile IP-Nachrichten 16
ResvTear-Nachricht	transportiert die Information über das Ende einer Reservierung upstream 38
Ressourcenverwaltung	Instanz auf einem Zwischensystem, welche die verfügbaren lokalen Ressourcen verwaltet 33
Resv-Nachricht	transportiert die Reservierungsanforderung eines Empfängers in RSVP zum Sender 36
Route Optimization	Verfahren zur Erweiterung von Mobile IP, um das Dreiecksrouting zu verhindern 25
Routingschleife	tritt beim Fast-Forwarding auf, wenn ein mobiles System in ein Subnetz gelangt, in dem es schon war 88
RSVP	Protokoll zur Signalisierung einer Ressourcenreservierung ..33
RSVP-Tunnelsitzung	spezielle RSVP-Sitzung zur Reservierung eines IPIP-Tunnels 42
RSVP-Dämon	Instanz von RSVP auf jedem in einer Reservierung involvierten Zwischensystem 36
RSVP-Sitzung	Kommunikationsbeziehung mit einer Ressourcenreservierung durch RSVP 36
Schnelles Agent Discovery	Verbesserung des Agent Discovery Verfahrens aus Mobile IP mit kürzeren Unterbrechungszeiten bei einem Subnetzwechsel ..45
Soft-State Ansatz	alle Informationen über eine Reservierung sind nur eine bestimmte Lebensdauer gültig 35
Staukontrolle	Verfahren zum Erkennen und Beheben von Überlastsituationen auf Zwischensystemen bei einer Transportverbindung 28
Transport Gateway	System zur Kopplung der beiden Transportverbindung des indirekten Transportansatzes 30

Tunnelgegenstück	in Linux 2.1.x notwendiges Pendant eines Tunnels, so daß ein Tunnel immer bidirektional ist 105
upstream	Gegensatz zu downstream: Übertragung vom Empfänger zum Sender 36
Verkehrskontrolle (traffic control)	Instanz auf jedem Zwischensystem, die eine konkrete Dienstgüte durch z. B. ein Schedulingverfahren realisiert 34

Anhang B

Nachrichtenformate

In diesem Anhang befinden sich die Formate der in Mobile IP bzw. für die Erweiterungen von Mobile IP verwendeten Nachrichten.

B.1 Mobile IP

B.1.1 Die Mobile IP Erweiterung

Die Mobile IP Erweiterung, die im Abschnitt 2.4.1 dargestellt wird, hat das in Abbildung B.1 gezeigte Format.

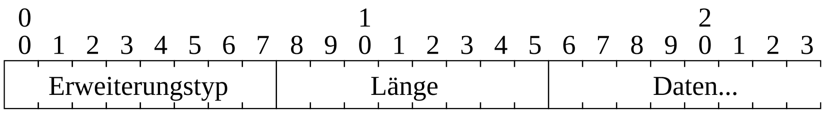

Abbildung B.1: Die Mobile IP Erweiterung

Das erste Feld (Erweiterungstyp) trägt eine eindeutige Kennung für die jeweilige Mobile IP Erweiterung. Das zweite Feld enthält die Anzahl der Datenbytes, die auf das Längenfeld folgen. Diese Datenbytes sind bei jeder einzelnen Erweiterung verschieden.

B.1.2 Die Mobility Agent Advertisement Erweiterung

Abbildung B.2 zeigt das Format der Mobility Agent Advertisement Erweiterung.

Diese Mobile IP Erweiterung enthält am Schluß keine, eine oder mehrere Care-of Adressen. Kommt die Agent Advertisement von einem Foreign Agent, ist ein bestimmtes Bit im Flags-Feld gesetzt und mindestens eine Care-of Adresse am Ende vorhanden. Der Foreign Agent paßt das Längenfeld entsprechend der Anzahl N der versendeten Care-of Adressen an. Das Feld „Lebensdauer einer Registrierung“ enthält die Lebensdauer, die der die Agent Advertisement versendende Mobility Agent maximal unterstützen kann (vgl. Seite 15). Die übrigen Felder sind für das Verständnis dieser Arbeit nicht notwendig (vgl. [Per96, S. 16f]).

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

Erweiterungstyp(=16)	Länge(=6+4*N)	Sequenznummer
Lebensdauer einer Registrierung		Flags
0 bis N Care-of Adressen		

Abbildung B.2: Die Mobility Agent Advertisement Erweiterung

B.1.3 Mobile IP Nachrichten für die Registrierung

Mobile IP Nachrichten werden mittels UDP auf festen Ports versendet. Sie beginnen mit einem 8 Bit großen Typfeld, welches die Art der Mobile IP Nachricht festlegt. Zwei verschiedene Mobile IP Nachrichten sind spezifiziert:

1. Die Registrierungsanforderung (siehe Abbildung B.3)

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

Typ (=1)	Flags	Lebensdauer einer Registrierung
Heimatadresse des mobilen Systems		
IP-Adresse des Home Agent		
Care-of Adresse		
Identifikation		

Abbildung B.3: Aufbau der Registrierungsanforderung

Das Typ-Feld kennzeichnet diese Mobile IP Nachricht als Registrierungsanforderung; das Flags-Feld enthält Informationen über zusätzlich vom Home Agent angeforderte Dienste. Die Lebensdauer in Sekunden gibt an, wie lange die Registrierung beim Home Agent ohne erneutes Eintreffen einer Registrierungsanforderung gültig sein soll. Dieser Wert entspricht der maximal vom mobilen System unterstützen Lebensdauer. Die Heimatadresse kennzeichnet, von welchem Mobilteilnehmer diese Registrierungsanforderung ausgegangen ist, die IP-Adresse des Home Agents das Ziel der Nachricht. Letztere benötigt der Foreign Agent, wenn er vom Mobilteilnehmer eine Registrierungsanforderung empfangen hat, um sie an den Home Agent weiterleiten zu können. Die Care-of Adresse teilt dem Home Agent mit, unter welcher Adresse der Mobilteilnehmer im fremden Subnetz erreichbar ist. Das Identifikationsfeld wird im Abschnitt 2.4.4 erläutert und dient zu Sicherheitszwecken.

2. Die Registrierungsantwort (siehe Abbildung B.4):

Bits 0–7	Bits 8–15	Bits 16–31
Typ (=3)	Code	Lebensdauer einer Registrierung
Heimatadresse des mobilen Systems		
IP-Adresse des Home Agent		
Identifikation		

Abbildung B.4: Aufbau der Registrierungsantwort

Im Format unterscheidet sie sich in drei Dingen von der Registrierungsanforderung:

(a) Das Typ-Feld kennzeichnet eine Registrierungsantwort.

(b) Anstelle des Flags-Feldes wird ein Code-Feld gesendet. Eine Null in diesem Feld zeigt an, daß der Home Agent die Registrierung akzeptiert hat; eine Eins, daß er sie nur mit einer Einschränkung akzeptiert. Andere Werte stehen für verschiedene Fehlermeldungen [Per96, S. 31f], deren einzelne Werte aber für diese Arbeit nicht von Bedeutung sind. Diese Arbeit unterscheidet nur zwischen einer Accept-Nachricht und einer Deny-Nachricht, unabhängig vom konkreten Wert des Code-Feldes.

(c) Eine Care-of Adresse wie in der Registrierungsanforderung tritt nicht auf.

B.2 Erweiterungen zu Mobile IP

B.2.1 Die MAC-Adressen Erweiterung

Die für die lokale Unterstützung eines mobilen Systems benötigte MAC-Adressen Erweiterung (siehe Abschnitt 7.2.2) hat das in der folgenden Abbildung B.5 gezeigte Format.

Bits 0–7	Bits 8–15	Bits 16–31
Erweiterungstyp(=20)	Länge(=6)	MAC-Adresse des
Foreign Agents, der diese Agent Advertisement ausgesendet hat		

Abbildung B.5: Die MAC-Adressen Erweiterung

Nach den für eine Mobile IP Erweiterung üblichen Feldern Typ und Länge folgt die MAC-Adresse des Mobility Agents, die aus einem sechs Byte großen Feld besteht. Dadurch ergibt sich für das Längenfeld ebenfalls der Wert 6; für den Typ der Mobile IP Erweiterung hat die MAC-Adressen Erweiterung zunächst den Wert 20 erhalten.

B.2.2 Die Notify-Nachricht

Die in dieser Arbeit in Mobile IP hinzugefügten Nachrichten haben das in Abbildung B.6 dargestellte allgemeine Format einer Notify-Nachricht.

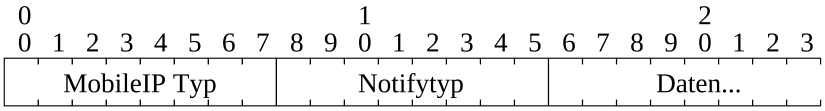

Abbildung B.6: Die Notify-Nachricht

Sie beginnt wie die anderen Mobile IP Nachrichten (siehe Abschnitt 2.4.3) mit einem acht Bit großen Feld zur Identifizierung des Typs, zunächst bekommt sie die Typnummer vier. Darauf folgt ein weiteres acht Bit großes Feld zur Unterscheidung der einzelnen Notify-Nachrichten, gefolgt von einem variabel großen Feld für die in der Notify-Nachricht transportierten Daten.

B.2.3 Die Mobile IP Ende Nachricht (alte Semantik)

Die Mobile IP-Ende Nachricht hat das in Abbildung B.7 dargestellte Aussehen.

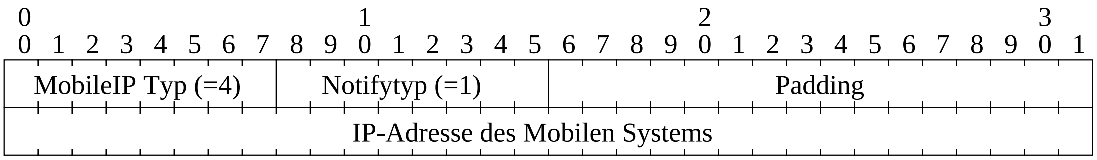

Abbildung B.7: Die Mobile IP-Ende Nachricht

Der Notifytyp ist die Eins, danach folgt ein Paddingfeld zum Ausrichten der folgenden Felder auf 32 Bit Grenzen. Die anschließenden vier Bytes tragen die IP-Adresse des mobilen Systems, für das der Empfänger dieser Nachricht die lokale Unterstützung beenden soll.

B.2.4 Die alte Foreign Agent Erweiterung

Die Erweiterung der Registrierungsanforderung um die Adresse des alten Foreign Agents zeigt Abbildung B.8.

Erweiterungstyp und Länge sind die typischen Felder für eine Mobile IP Erweiterung. Das Paddingfeld dient lediglich zum Ausrichten der folgenden IP-Adresse auf eine 32 Bit Grenze. Der Adreßtyp spiegelt den Zustand des mobilen Systems bei einem Subnetzwechsel wider und gibt gleichzeitig an, was für eine IP-Adresse sich im folgenden Feld befindet.

0–7	8–15	16–23	24–31
Erweiterungstyp(=35)	Länge(=6)	Adreßtyp	Padding
IP-Adresse des alten bzw. ersten Foreign Agents			

Abbildung B.8: Die alte Foreign Agent-Erweiterung

- ISINVALID: Das mobile System ist zum Zeitpunkt des Wechsels bei keinem Foreign Agent erfolgreich angemeldet gewesen. Daher trägt das folgende Feld keine gültige IP-Adresse.
- ISREREGISTER: Das mobile System ist bereits erfolgreich beim momentanen Foreign Agent angemeldet, deswegen braucht es keine IP-Adresse mitzuliefern (kein Subnetzwechsel). Es handelt sich um eine Wiederholung einer Registrierungsanforderung.
- ISOLDFA: Es hat ein Subnetzwechsel stattgefunden, wobei das mobile System erfolgreich beim alten Subnetz angemeldet war. Das folgende Feld trägt also die IP-Adresse des alten Foreign Agents, damit die Initiierung des Fast-Forwarding Protokolls möglich ist.
- ISFIRSTFA: Im alten Subnetz konnte das mobile System keine erfolgreiche Registrierung durchführen. Eine vorherige Registrierung mit dem ersten Foreign Agent war allerdings erfolgreich. Dadurch kann der neue Foreign Agent mit dem ersten Foreign Agent das Fast-Forwarding Protokoll durchführen, so daß ein evtl. vorhandenes Transport Gateway auf dem ersten Foreign Agent nicht umgangen wird (siehe Abschnitt 6.5.4).

B.2.5 Die Nachrichten des Fast-Forwarding Protokolls

Alle Nachrichten des Fast-Forwarding Protokolls haben das in Abbildung B.9 gezeigte Aussehen.

0–7	8–15	16–31
MobileIP Typ (=4)	Notifytyp	Padding
IP-Adresse des Mobilen Systems		
IP-Adresse des Urhebers dieser Notifynachricht		

Abbildung B.9: Format der Nachrichten des Fast-Forwarding Protokolls

Die Fast-Forwarding Notify erhält den Notifytyp zwei, die Fast-Forwarding Acknowledge die drei und die Fast-Forwarding Negative Acknowledge die vier. Die Mobile IP-Ende Nachricht mit der erweiterten Semantik (vgl. Abschnitt 6.1.2) erhält den Notifytyp eins.

Literaturverzeichnis

[AchBak96] A. Acharya, A. Bakre, B.R. Badrinath, *IP Multicast Extensions for Mobile Internetworking*, in: Proceedings of the 15th Annual Joint Conference of the IEEE Computer and Communications Societies (Infocom), San Francisco, CA, U.S.A., 24–28. März 1996, S. 67–74.
URL: http://paul.rutgers.edu/~acharya/frames_publications.html

[AndBlé96] G. Andreoli, N. Bléfari-Melazzi, M. Listani, M. Palermo, *Mobility management in IP networks providing real-time services*, in: Proceedings of the International Conference on Universal Personal Communications (ICUPC), Cambridge, Mass., U.S.A.,29. September–2. Oktober 1996, S. 774–777.

[BakBad95] A.Bakre, B.R.Badrinath, *I-TCP: Indirect TCP for Mobile Hosts*, in: Proceedings of the 15th International Conference on Distributed Computing Systems (ICDCS), Vancouver, Canada, Mai 1995, S. 136–143.
URL: http://athos.rutgers.edu/~badri/dataman/indirect.html

[Bög96] A. Böger: *Migrationsunterstützung für Mobile Systeme*, Diplomarbeit, Technische Universität Braunschweig, Dezember 1996.

[BraZha97] R. Braden (ed.), L. Zhang, S. Berson, S. Herzog, S. Jamin: *Resource ReSerVation Protocol (RSVP) — Version 1 Functional Specification*, RFC 2205, Internet Engineering Task Force (IETF), September 1997.

[CácPad96] R. Cáceres, V.N. Padmanabhan, *Fast and Scalable Handoffs for Wireless Internetworking*, in: Proceedings of the 2nd International Conference on Mobile Computing and Networking (MobiCom), Rye, New York, U.S.A., 10.–12. November 1996.

[ChaBin97] B. Chambless, J. Binkley, *HARP — Home Agent Redundancy Protocol*, Internet Draft, Internet Engineering Task Force (IETF), Oktober 1997. Work in progress.

[Dee91] S. Deering (ed.), *ICMP Router Discovery Messages*, RFC 1256, Internet Engineering Task Force (IETF), September 1991.

[FanHen98] C. Fan, B. Henckel, M. Mateescu, R. Ruppelt, *Interoperability Analysis and TCP Performance in a Heterogeneous Mobile-IP Environment*, in: Proceedings of the 9th IEEE Workshop on Local and Metropolitan Area Networks (LANMAN), Banff, Alberta, Canada 17.–20. Mai 1998.
URL: http://www.fokus.gmd.de/research/cc/mobra/employees/brigitte.henckel/

[FieZit97] A. Fieger, M. Zitterbart, *Evaluation of Migration Support for Indirect Transport Protocols*, 2nd Global Internet Conference in conjunction with Globecom '97, Phoenix, Arizona, U.S.A., 5.–6. November 1997.
URL: http://www.ibr.cs.tu-bs.de/general/papers.html#HLK

[GupDix96] V. Gupta, A. Dixit: *Mobile IP for Linux (ver. 1.00)*, Dept. of Computer Science, State University of New York, Binghamton, NY 13902.
URL: http://anchor.cs.binghamton.edu/~mobileip/

[Hol94] N. Holloway, Dummy-Modul im Linux-Kernel Version 2.1.x: `linux/drivers/dummy.c`, 1994.

[JacLer97] V. Jacobson, C. Leres, S. McCanne, **`tcpdump - dump traffic on a network`**, 1997.
URL: http://www-nrg.ee.lbl.gov/nrg.html

[JaiRal98] R. Jain, T. Raleigh, C. Graff, M. Bereschinsky, *Mobile Internet Access and QoS Guarantees Using Mobile IP and RSVP with Location Registers*, in: Proceedings of the IEEE International Conference on Communications (ICC), Atlanta, Georgia, U.S.A., 7.–11. Juni 1998, S. 1690-1695.

[JohPer97] D.B. Johnson, C. Perkins, *Route Optimization in Mobile IP*, Internet Draft, Internet Engineering Task Force (IETF), Juli 1997. Work in progress.

[Kat97] D. Katz, *IP Router Alert Option*, RFC 2113, Internet Engineering Task Force (IETF), Februar 1997.

[KraTer97] J. Krawczyk, J. Wroclawski, A. Terzis, L. Zhang: *RSVP Operation over IP Tunnels*, Internet Draft, Internet Engineering Task Force (IETF), August 1997, Work in Progress.

[MatMah96] M. Mathis, J. Mahdavi, S. Floyd, A. Romanow, *TCP Selective Acknowledgment Options*, RFC 2018, Internet Engineering Task Force (IETF), Oktober 1996.

[Per96] C. Perkins, (ed.) *IP Mobility Support*, RFC 2002, Internet Engineering Task Force (IETF), Oktober 1996.

[Per96a] C. Perkins, *IP Encapsulation within IP*, RFC 2003, Internet Engineering Task Force (IETF), Oktober 1996.

[Raj96] B. Rajagopalan, *Mobility and Quality of Service in the Internet*, 3rd International Workshop on Mobile Multimedia Communications (MoMuc-3), Princeton NJ, U.S.A., 25.–27. September 1996.

[SchmZit95] C. Schmidt, M. Zitterbart: *Reservierung von Netzwerk-Ressourcen — Ein Überblick über Protokolle und Mechanismen*, in: Praxis der Informationsverarbeitung und Kommunikation Vol. 18, Nr. 3, K.G. Saur Verlag, München, 1995.

[Sin96] S. Singh, *Quality of Service Guarantees in Mobile Computing*, in: J. Computer Communications Vol. 19, 1996, S. 359–371.
URL: http://www.cs.sc.edu/~singh/papers.html

[Ste94] W.R. Stevens, *TCP/IP Illustrated, Volume 1: The Protocols*, Addison-Wesley, 1994.

[Ste97] W. Stevens, *TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms*, RFC 2001, Internet Engineering Task Force (IETF), Januar 1997.

[TalBad98] A.K. Talukdar, B.R. Badrinath, A. Acharya, *Integrated Services Packet Networks with Mobile Host: Architecture and Performance*, to appear in: Journal of the Wireless Networks, Januar 1998.
URL: http://athos.rutgers.edu/~badri/dataman/qos.html

[TalBad98a] A.K. Talukdar, B.R. Badrinath, A. Acharya, *MRSVP: A Reservation Protocol for an Integrated Services Packet Network with Mobile Hosts*, Submitted for publication, April 1998.
URL: http://athos.rutgers.edu/~badri/dataman/qos.html

[Tan92] A.S. Tanenbaum, *Computer-Netzwerke*, 2.Aufl., Wolfram's Fachverlag, 1992.

[WooLeu96] W. Woo, V.C.M. Leung, *Handoff Enhancements in Mobile-IP Environment*, in: Proceedings of the IEEE International Conference on Universal Personal Communications (ICUPC), Cambridge, Massachusetts, U.S.A., 29. September–2. Oktober 1996, S. 760–764.

[Vir97] V. Virgilio: RSVP Portierung von Release 4.1a4 für Linux 2.0.x., 1997.
URL: ftp://ipv6.cere.pa.cnr.it/pub/rsvp/linux_rel4.1.a4.tgz

[ZhaDee93] L. Zhang, S. Deering, D. Estrin, S. Shenker, D. Zappala, *RSVP: A New Resource ReSerVation Protocol*, in: IEEE Network, September 1993, S. 8–18.
URL: http://www.isi.edu/div7/rsvp/pub.html