Mobile IPv6: Mobilität im zukünftigen Internet

Seminar Kommunikation & Multimedia WS 2002/2003
Institut für Betriebssysteme und Rechnerverbund
Technische Universität Braunschweig

Autor: Karim El Jed
Betreuer: Marc Bechler

1. Abstract

Mobilität gewinnt im Laufe der Zeit immer mehr an Bedeutung. Ist es vor ein paar Jahren noch verpönt gewesen ein Handy zu besitzen, so wird man heute ungläubich angeschaut wenn man keines besitzt. In Zukunft werden die Menschen auch mit Ihren Handys oder anderen mobilen Geräten das Internet benutzen wollen. Dafür benötigt man aber eine Infrastruktur im Internet, die diese steigende Anzahl an mobilen Teilnehmern auch effizient handhaben kann. Diese Arbeit beschäftigt sich mit dem Protokoll Mobile IPv6, welches die Grundlage für Mobilität im Internet der Zukunft sein wird.

2. Einführung

Es ist bereits rund dreißig Jahre her, dass das Internet Protokoll Version 4 (IPv4) eingeführt wurde. In dieser langen Zeit haben sich viele Anforderungen an das Internet geändert. IPv4 wird diesen Anforderungen nicht mehr gerecht und mobile, internetbasierte Multimedia-Dienste können erst dann vollkommen bereitgestellt werden, wenn das Internet verbessert wird. Das größte Problem dabei ist wohl der gewaltige Aufschwung, also die stetig steigende Benutzerzahl, des Internets. Nach einer Schätzung der Internet Engineering Task Force (IETF) wird es etwa im Jahr 2010 keine freien IP-Adressen mehr geben. Diese Schätzungen beziehen sich aber nur auf PC-basierte Internetanschlüsse. Wenn man die Einführung von UMTS betrachtet und somit die steigende Anzahl mobiler Endgeräte mit IP-Anschluss einbezieht, wird der Vorrat an IP-Adressen wohl schon viel eher aufgebraucht sein. „Nach Angaben und Prognosen der Europäischen Kommission wird der Anteil der Mobilfunkbenutzer an der Gesamtbevölkerung im Jahr 2003 auf 65% steigen“.

Bereits seit Anfang der 90er Jahre arbeitet die IETF an einem Nachfolger für IPv4. Zwischen 1995 und 1996 wurde aus verschiedenen Entwürfen zum Internet Protokoll next Generation (IPnG) ein einheitlicher Standard entwickelt. Dieses Protokoll ist aber eher unter dem Namen IPv6 bekannt.

Das Wort Mobilität gewinnt im Informationszeitalter immer mehr an Bedeutung. Mobilität wurde bereits durch ein zusätzliches Protokoll realisiert, dem Mobile IPv4. Dieses Protokoll konnte aber aufgrund einiger Schwächen nicht wirklich überzeugen. Bei der Entwicklung von IPv6 legte man also auch großes Augenmerk auf die Unterstützung von mobilen Geräten und entwickelte den „Mobility Support in IPv6“.

Nachdem einige Begriffe aus dem Bereich Mobilität geklärt wurden, gibt es in Kapitel 4 eine Einführung in Mobile IPv4. Dabei werden auch die Vor- und Nachteile dieses Protokolls besprochen. Kapitel 5 beschäftigt sich mit dem eigentlichen Thema dieser Seminararbeit, dem Mobile IPv6. Am Ende werden die beiden Protokolle gegeneinander verglichen und ein Ausblick auf die zukünftige Entwicklung gegeben.

3. Begriffsdefinitionen

Um die Funktionsweise von Mobile IP verstehen zu können, bedarf es der Klärung von ein paar Begriffen aus dem mobilen Wortbereich. Die wichtigsten davon werden hier definiert:

Node	Ein Knoten (Gerät) der IP implementiert (z.B. ein Host oder Router).
Mobile Node	Ein Knoten, der seine Anbindung von einem Link zu einem anderen wechseln kann und weiterhin unter seiner Heimatadresse (home address) zu erreichen ist.
Correspondent Node	Ein Knoten mit dem ein mobiler Knoten kommuniziert. Dieser Knoten kann sowohl stationär als auch mobil sein.
Care-of-Adresse	Eine IP-Adresse die einem mobilen Knoten zugewiesen ist, wenn er einen foreign link besucht. Ein mobiler Knoten kann mehrere care-of-adressen besitzen. Diejenige, die bei dem Home Agent des Knotens registriert ist, nennt man primary Care-of-Adresse.
Home Agent	Ein Router, der sich im Heimatnetzwerk des mobilen Knotens befindet und bei dem er seine aktuelle Care-of-Adresse registrieren lässt. Befindet sich der mobile Knoten nicht in seinem Heimatnetz, dann fängt der Home Agent seine Pakete ab, kapselt sie in eine andere Nachricht und tunnelt sie an die primäre Care-of-Adresse.
Foreign Agent	Ist ein Router, der dem mobilen Knoten in einem fremden Netzwerk Routing Services bietet. Er entpackt und vermittelt getunnelte Pakete, die er vom Home Agent des mobilen Knotens erhält. Für ausgehende Pakete dient er dem mobilen Knoten als Default Router.
Binding	Bezeichnet die Verbindung der Heimatadresse eines mobilen Knotens mit seiner Care-of-Adresse.

Tunneln	Ein IP-Paket wird in das Nutzdatenfeld eines neuen IP-Paketes gesteckt und verschickt. Liest der Empfänger die Nutzdaten des empfangenen Paketes aus, so erhält er das ursprüngliche Paket.

4. Mobile IPv4

Mobile IPv4 ermöglicht das transparente Routen von IP-Paketen zu mobilen Knoten im Internet. Unabhängig von ihrer Position, also ihrem Anschluss ans Internet, werden Mobile Nodes durch ihre Heimatadresse identifiziert. Befindet sich solch ein Knoten in einem anderen Netzwerk als seinem Heimatnetzwerk, so bekommt er eine zusätzliche Care-of-Adresse. Der Mobile Node muss diese Care-of-Adresse bei seinem Home Agent registrieren. Pakete die nun für den Mobile Node bestimmt sind werden vom Home Agent abgefangen und an ihn getunnelt.

4.1 Funktionsweise von Mobile IPv4

Die folgende Betrachtung ist in einer etwas vereinfachten Form gehalten, um das Verständnis über die Funktionsweise von Mobile IPv4 zu erleichtern.

1. Home bzw. Foreign Agents senden regelmäßig eine Nachricht aus, sogenannte Agent Advertice messages, in denen sie sich als Agenten identifizieren.

2. Erhält ein mobiler Knoten solch eine Nachricht kann er feststellen, ob er sich in seinem Heimatnetzwerk befindet oder nicht.

3. Stellt er fest, dass er in sein Heimatnetzwerk gewechselt hat, so teilt er seine Rückkehr seinem Home Agent mit.

4. Stellt er fest, dass er in ein fremdes Netz gewechselt hat, so benutzt er als Care-of-Adresse die IP-Adresse des Foreign Agent oder er ermittelt eine eigene via DHCP[1] (Colocated Care-of-Adresse). Im ersten Fall muss sich der mobile Knoten beim Foreign Agent registrieren, im zweiten Fall ist es optional.

5. Hat der mobile Knoten eine neue Care-of-Adresse, so teilt er sie seinem Home Agent mit.

6. Pakete, die nun an die Heimatadresse des mobilen Knotens gesendet werden, werden vom Home Agent abgefangen. Er kapselt sie in eine neue Nachricht, die an die Care-of-Adresse des mobilen Knotens gesendet wird. Dieses Verfahren nennt man Tunneln. Im Falle einer Colocated Care-of-Adresse erhält der mobile Knoten die eingekapselte Nachricht direkt, im anderen Fall erhält der Foreign

[1] DHCP = Dynamic Host Configuration Protocol (ist laut Definition zur dynamischen Konfiguration von IP-Netzen fähig).

Agent die Nachricht, packt das Original aus und schickt es an den mobilen Knoten.

7. Möchte der mobile Knoten nun antworten, so kann er die Nachricht direkt (über den Foreign Agent) an den Empfänger senden. Er muss dazu nicht den Home Agent verwenden.

4.2 Ein Kommunikationsbeispiel

Nun wollen wir uns mal einen Kommunikationsvorgang zwischen einem mobilen Knoten und einem Host in einem Diagramm anschauen:

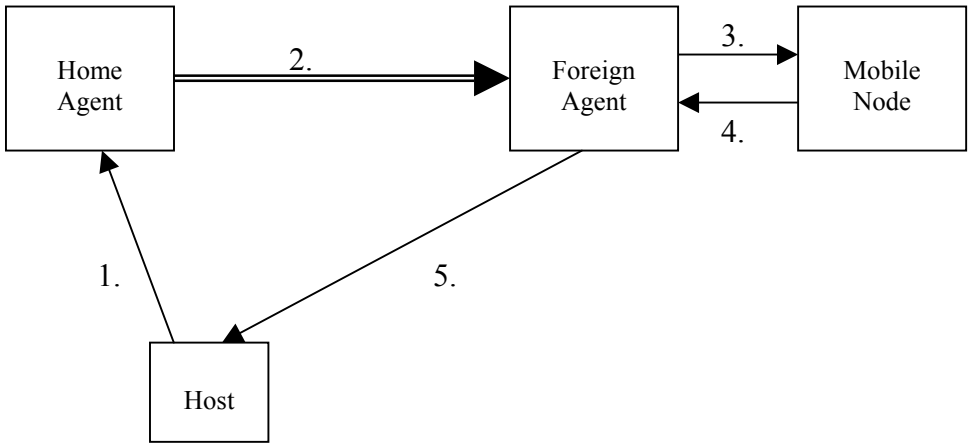

Abbildung 1: Dreiecks-Routing in Mobile IPv4

Ein Host schickt eine Nachricht an den Mobilen Knoten (1). Der Home Agent fängt diese Nachricht ab, kapselt die Nachricht ein und tunnelt sie an die registrierte Care-of-Adresse (2). Der Foreign Agent entkapselt die Nachricht und schickt sie weiter an den Mobile Node (3). Der Mobile Node will eine Antwort an den Host schicken. Der Foreign Agent dient ihm dabei als Default Router (4). Der Foreign Agent schickt die Nachricht direkt an den Host (5).

4.3 Vor- und Nachteile von Mobile IPv4

Mobile IPv4 ist ein Protokoll das sowohl seine Stärken als auch Schwächen hat. Das liegt aber sicherlich daran, dass in IPv4 die Mobilität nicht vorgesehen war. Man musste aber auf diesem Protokoll aufbauen.

(+) Die Benutzung eines Foreign Agent ist in Mobile IPv4 optional. Ein mobiler Knoten kann sich mittels des DHCP eine IP-Adresse zuweisen lassen. Besitzt er eine Colocated Care-of-Adresse kann er selbst als Foreign Agent fungieren.

Mobile IPv4 wird somit auch in Netzwerken unterstützt, die noch keinen Foreign Agent installiert haben.

(+) Andererseits bringt die Benutzung eines Foreign Agents den Vorteil, dass viele mobile Knoten ein und die selbe Care-of-Adresse benutzen können. In den Zeiten der IP-Adressen-Knappheit ist dies ein wichtiger Faktor.

(-) Wenn man das obige Beispiel betrachtet wird eines schnell deutlich. Die Kommunikation vom Host zum mobilen Knoten läuft immer über den Home Agent. Dieses sogenannte Dreiecks-Routing ist natürlich sehr ineffizient. Da nicht davon auszugehen ist, dass der Gesprächspartner des mobilen Knotens auch Mobile IPv4 versteht, kann der mobile Knoten ihm nicht seine neue Adresse mitteilen. Er muss davon ausgehen, dass er mit dieser Information nichts anfangen kann.

(-) Diese Situation verschlimmert sich noch, wenn der Router im fremden Netzwerk es nicht erlaubt Nachrichten mit einer Absender-IP-Adresse zu senden, die nicht konform zum (Sub-)Netzwerk ist. Dies ist z.B. bei der Benutzung eines Ingress-Filters der Fall. In diesem Fall muss auch der mobile Knoten die Daten über den Home Agent verschicken. Man spricht hier von „Reverse Tunneling“. Dies führt zu großen Verzögerungen, erhöhter Netzlast. Die Netzlast wird desto größer, je mehr mobile Knoten über ihren Home Agent kommunizieren. Mobile IPv4 eignet sich somit nicht für eine große Anzahl von mobilen Knoten. Es hat somit eine schlechte Skalierbarkeit.

(-) Beim Tunneln werden Daten versendet, die für den Empfänger nicht wirklich von Bedeutung sind (Redundanz).

5. Mobile IPv6

Nachdem man die Schwächen von Mobile IPv4 erkannt hatte, musste man sich überlegen, wie man es besser machen könnte. Die Entwicklung von IPv6 ist somit die Gelegenheit um auch ein besseres Mobilitätsprotokoll zu entwerfen. Die Entwicklung des Internets spielt dabei natürlich auch eine große Rolle. Die Struktur des Internets und die Anwendungen die darauf basieren haben sich in den letzten Jahren stark verändert und werden sich auch in der Zukunft noch stark verändern. Somit sind ergänzend zu den Anforderungen die an Mobile IPv4 gestellt wurden, in Mobile IPv6 weitere hinzugekommen:

- **Abwärtskompatibilität zu IP**
  Der Nachrichtenaustausch von und zu mobilen Knoten muss auch über Knoten gehen können, die nur IPv4 beherrschen. Das Finden des Pfades zum Empfänger muss für sie transparent sein.

- **Authentifizierte Registrierung**
  Der derzeitige Aufenthaltsort eines mobilen Knotens muss durch ein spezielles Modul verwaltet werden. An- und Abmeldungen müssen gesichert sein. Damit

wird verhindert, dass sich ein Angreifer als mobiler Knoten ausgibt und den Datenstrom abfängt.

- **Skalierbarkeit**
  Durch die sinkenden Preise von mobilen Endgeräten und derer somit steigenden Anzahl, muss die Erweiterbarkeit von Teilnetzen mit Mobilfunktionalität in besonderem Maße gewährleistet sein.

- **Sicherheit**
  Auf das Thema Sicherheit musste natürlich in Zeiten der Kommerzialisierung des Internets besonders geachtet werden. In IPv6 wurden deshalb viele Mechanismen zur Sicherheit aufgenommen. Aus Platzgründen können wir auf diese hier jedoch nicht weiter eingehen.

5.1 Ein Kommunikationsbeispiel

Die Funktionsweise von Mobile IPv6 entspricht im weitesten Sinne der von Mobile IPv4. Wir wollen diese kurz anhand eines Diagramms erläutern:

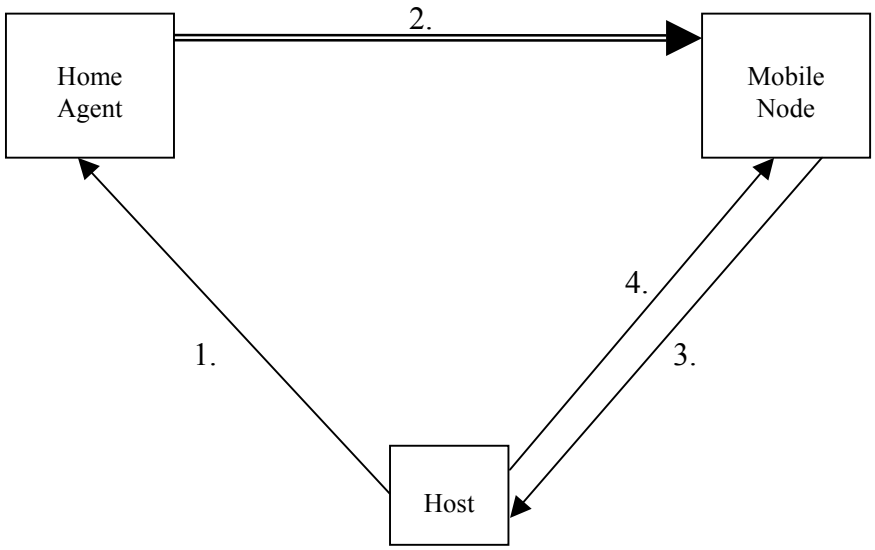

Abbildung 2: Kommunikation in Mobile IPv6

Der Host sendet ein Paket an die Heimatadresse des mobilen Knotens (1). Der Home Agent fängt dieses Paket ab, packt es in ein neues Paket und tunnelt dieses an die Care-of-Adresse des mobilen Knotens (2). Der mobile Knoten entpackt das Paket und kann nun an die ursprüngliche Absenderadresse direkt antworten. Dabei benutzt er seine Care-of-Adresse als Absender (3). Der Host übernimmt diese Binding-Information und speichert die Care-of-Adresse des mobilen Knotens ab. Er schickt eine Antwort mit der Binding-Acknowledge-Option an den mobilen Knoten. Die nachfolgende Kommunikation kann nun direkt zwischen den beiden Kommunikationspartnern erfolgen (4).

Ganz so einfach ist das Ganze natürlich nicht. Um die Funktionsweise von Mobile IPv6 etwas besser verstehen zu können, müssen wir erst mal einen kleinen Blick auf das Neighbour-Discovery-Protokoll werfen.

5.2 Neighbour Discovery

Das Neighbour-Discovery-Protokoll für IPv6 dient dazu, die Adressen benachbarter Knoten festzustellen. Hosts benutzen dieses Protokoll auch, um zu erfahren, an welche Router sie ihre Pakete schicken können. Eine weitere Anwendung dieses Protokolls besteht darin, Änderungen im Netzwerk festzustellen, welche „Nachbarn" noch erreichbar sind und welche nicht. Änderungen von Adressen lassen sich somit natürlich auch feststellen.
Wir werden bei der Erklärung der Funktionsweise von Mobile IPv6 auch einige Funktionen dieses Protokolls benötigen, die hier nun kurz erläutert werden:

Router Discovery
Für das Router Discovery werden zwei Nachrichten benötigt. Router-Advertisement-Nachrichten werden von den Routern periodisch an alle anderen Knoten versendet. Darin übermitteln sie Informationen über ihre Adresse, ihre Lebensdauer, usw. Für Mobile IPv6 hat man noch ein Bit hinzugefügt. Mit diesem Bit kann der Router angeben, ob er auch als Home Agent fungieren kann. Ein Router kann auch außerhalb dieser Periode eine Router-Advertisement-Nachricht an einen einzelnen Host schicken. Dies geschieht, wenn der Host ihm eine Router-Solicitation-Nachricht schickt.

Neighbour Discovery
Neighbour Discovery funktioniert ähnlich wie Router Discovery. Hierbei schicken Hosts eine Neighbour-Solicitation-Nachricht an alle anderen Knoten, um deren Adresse zu erfahren. Dabei übermitteln sie natürlich auch ihre eigene Adresse. Neighbour Solicitations können auch an einen bestimmten Knoten gesendet werden, um seine Erreichbarkeit zu überprüfen (Neighbour Reachability). Die Antwort auf eine Neighbour-Solicitation-Nachricht ist die Neighbour-Advertisement-Nachricht. Ein Host kann aber auch unaufgefordert diese Nachricht versenden, wenn sich z.B. seine Adresse geändert hat und er andere Knoten darüber informieren will.

5.3 Funktionsweise im Detail

Um Mobile Ipv6 etwas besser verstehen zu können, gibt es nun einen detaillierteren Überblick über die Funktionsweise des Protokolls.

Home Agent Discovery
Befindet sich der Mobile Node in seinem Heimatnetzwerk, so kann er die Home Agents mittels Router Discovery ermitteln. Befindet er sich in einem fremden Netzwerk so kann er eine ICMP[2] Home-Agent-Address-Discovery-Request-Nachricht an die „Mobile IPv6 Home-Agents" Anycast-Adresse in seinem Heimatnetzwerk senden. Dies

[2] ICMP = Internet Control Message Protocol

kann z. B. nötig sein, wenn der Router, der dem Mobile Node als Home Agent diente, während seiner Abwesenheit durch einen anderen Router ersetzt wurde.

Bewegung
Ein Mobile Node kann immer überprüfen, ob sein Default-Router noch erreichbar ist (Neighbour Reachability). Ist dies nicht der Fall, so muss er mittels Router Discovery nach einem anderen Router suchen. Hat der neue Default-Router nun eine andere Subnetzwerkadresse als der alte Default-Router, so spricht man von einer Bewegung des Knotens.

Ermitteln einer Care-of-Adresse
Hat ein Mobile Node also eine Bewegung seinerseits bemerkt, muss er sich eine neue Care-of-Adresse zulegen. Es besteht die Möglichkeit, dass der Mobile Node im fremden Netzwerk eine feste IP-Adresse vom Administrator zugewiesen bekommen hat. Ist dies nicht der Fall, benutzt er die Address Autoconfiguration (z.B. DHCPv6). Dabei erstellt er sich aus seiner eigenen MAC-Adresse und noch anderen Informationen, die er z.B. von den Routern erhalten hat, eine Adresse. Danach prüft er mittels Duplicate Address Detection, ob schon jemand die eben erstellte Adresse hat.

Binding Update beim Home Agent
Nachdem der Mobile Node erfolgreich eine neue Care-of-Adresse angelegt hat, muss er sie durch eine Binding-Update-Nachricht seinem Home Agent mitteilen. Diese Nachricht enthält die Heimatadresse des Mobile Node und als Absender dient die neue Care-of-Adresse. Erhält der Mobile Node ein Binding Acknowledge, so weiß er, dass seine Care-of-Adresse nun bei seinem Home Agent als primäre Care-of-Adresse registriert ist.

Funktion des Home Agent
In den bisherigen Betrachtungen sind wir immer davon ausgegangen, dass alle Pakete, die für den Mobile Node bestimmt waren, über den Home Agent geschickt wurden. Nun gibt es aber meistens mehrere Router in einem Netzwerk. Hat ein Home Agent also festgestellt, dass einer seiner Mobile Nodes nicht mehr zuhause ist, dann sendet er in seinem Namen die Neighbour-Advertisment-Nachrichten und gibt als Zieladresse seine eigene Adresse an. Somit ist der Mobile Node noch immer für die anderen Knoten erreichbar. Sie müssen nur alle Nachrichten für ihn an die soeben erhaltene Adresse des Home Agent schicken. Natürlich antwortet der Home Agent für den Mobile Node auch auf Neighbour Solicitations. Nachrichten innerhalb des Netzwerkes, die für den Mobile Node bestimmt sind, werden somit immer an den Home Agent geschickt, der sie an den Mobile Node weiterleitet.

Tunneln von Paketen
Der Home Agent nimmt alle Pakete, die er für den Mobile Node empfangen hat und kapselt sie in ein neues Paket. Indem er das ursprüngliche Paket nicht verändert, kann der Mobile Node beim Entpacken des ursprünglichen Pakets die Absender Adresse des Correspondent Nodes sehen. Des weiteren weiß er somit, dass der Absender seine Care-of-Adresse nicht kennt und kann sie ihm mitteilen, sofern dies nicht unerwünscht ist.

Binding Update beim Correspondent Node
Ähnlich wie beim Home Agent schickt der Mobile Node seinem Gesprächspartner eine Binding-Update-Nachricht. Der Correspondent Node kann somit direkt mit dem Mobile Node kommunizieren. Die entstehende Redundanz durch das Tunneln ist also sehr gering.

Mobilität in der Transportschicht
Mobile IPv6 bekommt von der Transportschicht ein Paket, dass an den Correspondent Node geschickt werden soll. Mobile IPv6 setzt die Home Address Option (HAO) im Header und gibt als Absender seine Care-of-Adressean. Empfängt der Corespondant Node ein Paket mit gesetzter HAO, dann tauscht er die Care-of-Adresse, die sich im äußeren IP-Header des Pakets befindet, mit der zuvor gespeicherten Heimatadresse des Mobile Node aus. Nach dem er die HAO wieder deaktiviert hat, gibt er das Paket an die Transportschicht weiter. Für diese ist somit die Mobilität des Mobile Nodes nicht sichtbar. Abbildung 3 zeigt eine sehr vereinfachte Darstellung dieses Vorgangs.
Der Correspondent Node setzt in seinen Paketen die Routing Header Option (RHO) und fügt in den Routing-Header die Heimatadresse des Mobile Node ein. Somit wird erreicht, dass das Paket auch an den richtigen Empfänger gegeben wird.

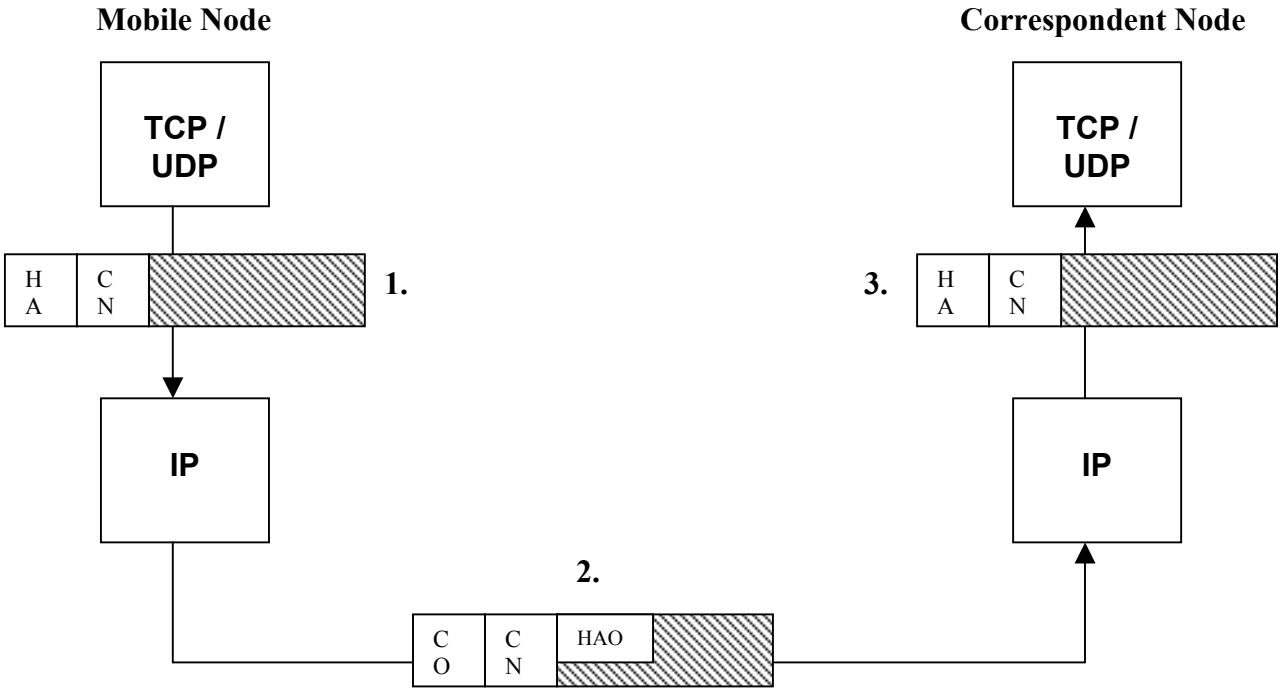

Abbildung 3: Mobilität in der Transportschicht

HA = Heimatadresse des Mobile Nodes
CO = Care-of-Adresse des Mobile Nodes
CN = Adresse des Correspondant Node
HAO = Home Adress Option

6. Vergleich: Mobile IPv4 vs. Mobile IPv6

Der größte Unterschied zwischen Mobile IPv4 und Mobile IPv6 ist wohl der, dass bei Mobile IPv6 der mobile Knoten seinem Kommunikationspartner mitteilen kann, wie seine neue Adresse lautet. Dieser kann dann nach Erhalt der Nachricht die nächsten Pakete direkt an diese neue Adresse schicken. Dadurch dass nicht mehr alle Pakete zum Mobile Node getunnelt werden müssen, gibt es weniger Redundanz. Die Netzauslastung ist geringer und die Skalierbarkeit wurde somit um einiges verbessert. Auch in Netzwerken mit „Ingress"-Filterung ist kein Reverse Tunneling mehr nötig. Der Mobile Node gibt seine Care-of-Adresse als Absender an, welche beim Empfänger durch seine Heimatadresse ausgetauscht wird.

In Mobile IPv6 gibt es auch keine Foreign Agents mehr. Der Vorteil, dadurch IP-Adressen einzusparen, weil mehrere Mobile Nodes über ein und den selben Foreign Agent zu erreichen sind, ist bei IPv6 nicht mehr relevant. Durch die 128 Bit Adressen wird es vorerst mehr als genug davon geben.

Zusätzlich zu diesen Unterschieden gibt es noch weitere, die im Rahmen dieses Seminars keine Erwähnung gefunden haben. Einige sollten aber trotzdem an dieser Stelle aufgeführt werden:

- Routenoptimierung ist fester Bestandteil des Protokolls
- Routenoptimierung wird sicher ausgeführt, auch ohne vorher ausgemachte Security-Associations
- Multicast-Pakete müssen nicht an den Home Agent getunnelt werden
- Mobile IPv6 ist von der Sicherungsschicht abgekoppelt, indem es Neighbour Discovery anstatt von ARP[3] benutzt. Das Protokoll ist somit robuster
- Durch Dynamic Home Agent Address Discovery[4] bekommt ein Mobile Node nur eine Antwort von einem einzigen Home Agent und nicht wie bei Mobile IPv4 von mehreren

7. Ausblick

Die vielen Anforderungen, die Mobile IPv4 an die Infrastruktur von Netzwerken stellt (Home- und Foreign Agents, kein Source-Routing bzw. Ingress-Filter, Tunneln von Paketen) haben bisher verhindert, dass Mobile IPv4 weitläufig verbreitet ist. Mit der Einführung von Mobile IPv6 sollen diese Barrieren verringert werden. Das neue Protokoll ist ausgereifter und besser durchdacht als das alte. Das liegt aber auch daran, dass bei Mobile IPv4 auch noch IPv4 als Grundlage diente. Das neue Protokoll verhält sich wie ein reines Netzwerkschicht-Protokoll in dem es unabhängig sowohl von der Sicherungsschicht als auch von der Transportschicht arbeitet. Leider steht der Verbreitung von Mobile IPv6 natürlich das noch immer nicht abgeschlossene Standardisierungsverfahren im Weg. Mobile IPv6 wird sich aber sicherlich durchsetzen können und „das" Protokoll in Sachen Mobilität werden. Mit der Einführung von UMTS in Verbindung mit Mobile IPv6 könnte die Verbreitung von IPv6 einen kräftigen

[3] ARP = Address Resolution Protocol
[4] ICMP-Nachricht um die Adressen von Home Agents zu bestimmen

Schub bekommen und den Wechsel zum Internet der Zukunft beschleunigen. Aber das hängt, wie so vieles, (fast) allein von den Konsumenten ab.

Literatur:

[1] David B. Johnson: Mobility Support in IPv6, IETF Mobile IP Working Group, 2002

[2] B. Kölmel, M. Hubschneider: Nutzererwartungen an Location Based Services Ergebnisse einer empirischen Analyse

[3] Das deutsche IP-Forum – http://www.ipv6-net.org

[4] Mobility Support for IPv4, RFC 3344

[5] K. Hartwig, J. Simon: Einsatz von IP Version 6 und IP Mobility in der dritten Mobilfunkgeneration, 2002

[6] Neighbour Discovery for IPv6, RFC 2461