HASSO-PLATTNER-INSTITUT
für Softwaresystemtechnik GmbH

Mobilität & Technik
Schwerpunkt Mobile IP

Ausarbeitung im Proseminar Internet Ökonomie

am Institut für Informatik, Universität Potsdam

Ivo Köhler 706144

SS 2003

Gliederung

Einleitung

Überblick

Hauptteil

Zusammenfassung

Einleitung

I. Evolution der Mobilfunknetze

Bevor wir uns dem eigentlichen Inhalt dieser Ausarbeitung widmen, werde ich einen kurzen historischen Abriss der Mobilfunknetze geben.
Wie in Abbildung I.a zu erkennen ist, können wir Mobilfunknetze in 4 Klassen unterteilen.

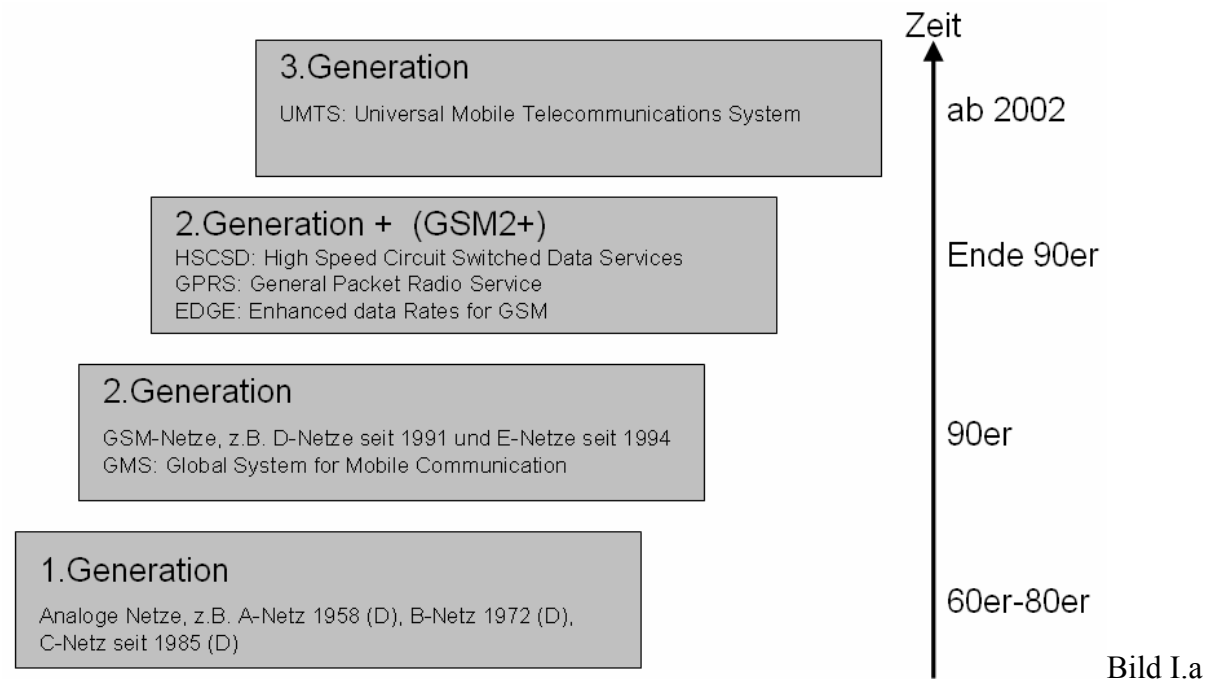


Bild I.a

Mobilfunknetze der so genannten 1. Generation waren die ersten Mobilfunknetze.
Sie beruhten auf analoger Technik und zu ihnen zählten:

- A-Netz
- B-Netz
- C-Netz

Während es sich bei den A und B-Netzen um reine Forschungsnetze handelte, kam es mit dem C-Netz zur ersten erfolgreichen Ausprägung eines kommerziellen Mobilfunknetzes in Deutschland.

C-Netz Telefon
der Firma Grundig

In den Achtzigern und zu Beginn der Neunziger wurden dann Netze der 2. Generation entwickelt und auf den Markt gebracht.
Zu diesen GSM-Netzen (Abb. I.b) zählten in Deutschland:

- D-Netze (ab 1991)
- E-Netze (1994)

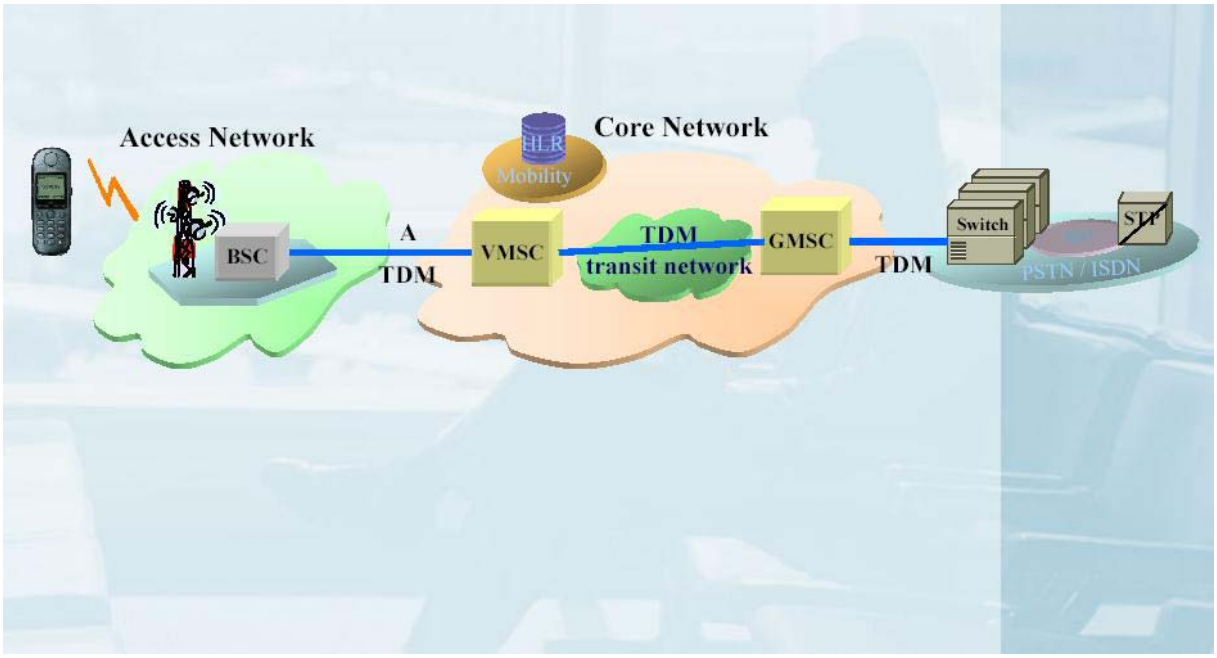


Bild I.b – Struktur eines GSM-Netzes

Netze die den „Global System for Mobile Communication“ (GSM) Standard unterstützen brachten den wirklichen Durchbruch in der Mobilkommunikation. Durch den rapiden Fall der Preise für mobile Endgeräte kam es zu einem enormen Wachstum in diesem Sektor. Durch die immer größer werden Bedeutung der mobilen Datenkommunikation wurden die GSM Netze Ende der Neuziger durch verschiedene Services erweitert.
Zu diesen Services gehören:

- HSCSD: High Speed Circuit Switched Data Services
- GPRS: General Packet Radio Service
- EDGE: Enhanced data Rates for GSM

Diese erweiterten GSM Netze nennt man GSM+ Netze (Abb. I.c) und gehören damit der Klasse der 2. Generation+ an.

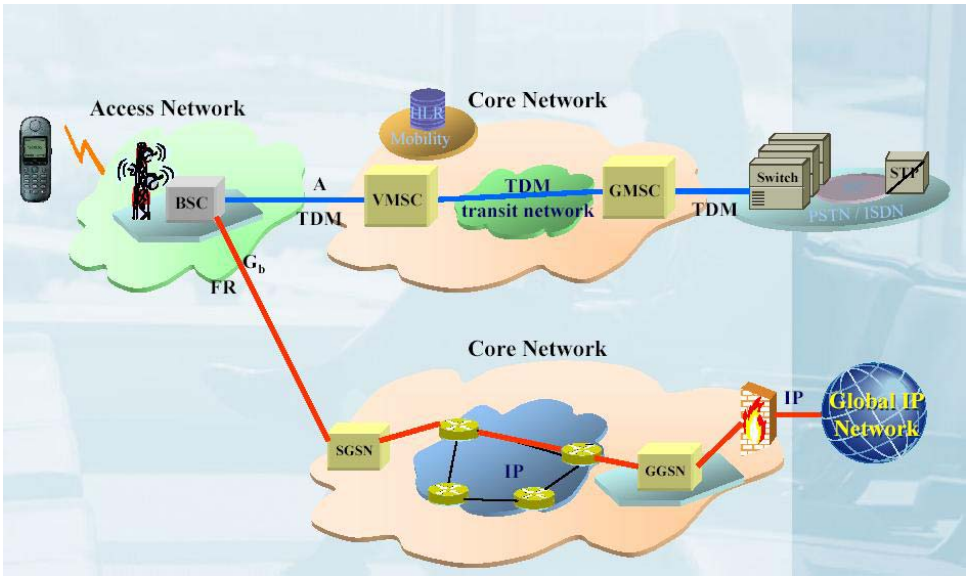


Bild I.c – Struktur eines GSM+ Netzes

Ab 2002 kam es dann zur Ausprägung der 3. Generation der Mobilfunknetze (Abb. I.d). Die UMTS Netze (Universal Mobile Telecommunications System) erweitern das herkömmliche GSM Netz mit einer völlig neuen Art des Netzzugangs für mobile Endgeräte (wie Palms oder Notebooks) durch das UTRAN (UMTS-Terrestrical-Radio-Access-Network).

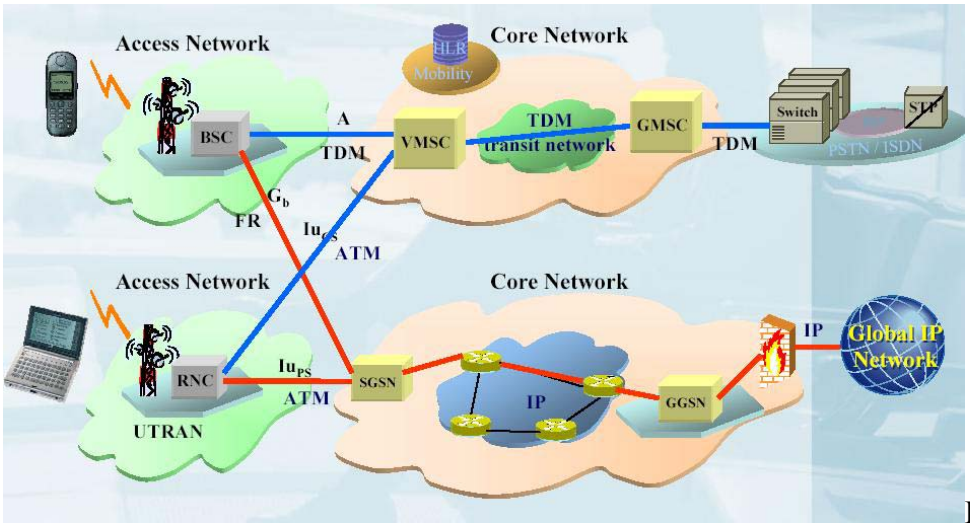


Bild I.d

II. Internetprotokoll IPv6

Im Zuge der Einführung von Mobilfunknetzen der 3. Generation muss man auch über die Einführung des Internetprotokolls der „Next Generation“ IPv6 sprechen. UMTS Netze implementieren im Kernnetzwerk dieses Protokoll. Der Anteil für die Mobilität, Mobilitätserkennung und Mobilitätsmanagement dieses Protokolls ist das so genannte Mobile IPv6, welches im weiteren Teil dieser Ausarbeitung näher diskutiert wird.

III. Situation ohne Mobile IP

In der heutigen Internetwelt ist Mobilität ein wichtiger Aspekt geworden. Dies ist zurückzuführen auf die weite Verbreitung und ständig wachsende Anzahl von portablen Computereinheiten, wie z.B. Notebooks oder Palmtops, da in den letzten Jahren die Preise für

solche mobilen Einheiten akzeptable Regionen erreicht haben und sie ihren stationären Vertretern in Sachen Rechenleistung, Speicherkapazität und multimedialen Fähigkeiten in nichts mehr nachstehen.

Bevor wir Mobile IP und dessen Implementierung aber näher kennen lernen, schauen wir uns an, welchen Standard die heutigen Netzwerke in der Regel aufweisen.
Die Situation in heutigen IP Netzwerken bietet keine guten Vorraussetzungen für Mobilität, da jedem Endgerät in einem Subnetz eine feste und damit statische IP zugeordnet wird. Dabei spielt es keine Rolle ob es sich um einen stationären Desktop Rechner oder um ein mobiles Notebook handelt. Eine solche feste IP besteht aus einem Netzwerk- (erstes Oktett) und einem Hostanteil (restliche drei Oktette) (siehe Bild III.a). Unter einem Oktett versteht man eine 8-Bit Binäradresse, die in der Regel zum besseren Verständnis als Dezimalzahl zwischen 0 und 255 dargestellt wird.

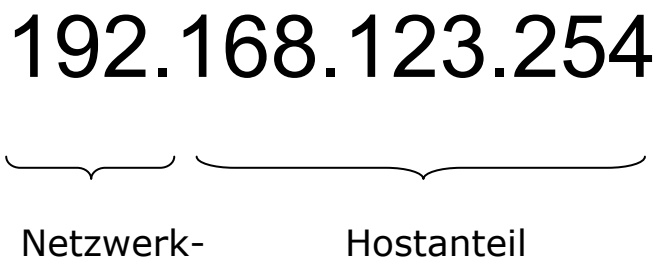


Bild III.a

Diese statische IP ist auch für mobile Endgeräte notwendig, da Netzwerk-Schichten die über IP liegen (z.B. TCP – Transport Layer in OSI) dies voraussetzen.

IV. Problem: Mobilität

Die Anforderungen, die die Mobilität der Endgeräte mit sich bringt, wurden bei der Entwicklung des IP-Protokolls leider nicht berücksichtigt. Der oben beschriebene Aufbau bedingt nun, dass mobile Geräte beim Anschluss an ein fremdes Netzwerk auch dessen Netzwerkanteil der IP-Adresse annehmen, damit die topologische Korrektheit der IP-Adressen gewährleistet bleibt. Protokolle die – von höherer Ebene aus – das IP-Protokoll nutzen (wie beispielsweise TCP) benötigen zum Halten der Verbindung aber eine feste IP als "Ansprechpartner". Daraus ergeben sich nur beschränkte Möglichkeiten, Mobilität auch mit dem bestehenden Protokoll zu realisieren: Wie beschrieben erhält das mobile Gerät bei jedem Neuanschluss an ein fremdes Netzwerk eine neue IP-Adresse. Damit höhere Schichten wie TCP die Pakete aber nicht ins Nirwana schicken, ist es nun nötig, jeden Router (weltweit)

über diese neue IP-Adresse in Kenntnis zu setzen, um zu sichern, dass alle von einem beliebigen Absender an die alte IP-Adresse gesendeten Pakete den neuen Zielort erreichen. Dass dies nicht mit vertretbarem Aufwand an Datentraffic und Overhead-Zeit möglich ist, dürfte einleuchten.
So ist es mit der momentanen Lösung in IPv4 nicht sinnvoll möglich, Mobilität von Endgeräten zu implementieren. Die Lösung ist Mobile IP, eine Technik die die bestehen den Mechanismen von IPv4 erweitert und ergänzt. Diese Mechanismen werden vollständig im IPv6 (schrittweise Einführung bis zum Jahre 2003 geplant) enthalten sein und mit ausreichender Verbreitung von IPv6 zur allgemeinen Nutzung zur Verfügung stehen.

Überblick

I. Terminologie

Im Folgenden werden einige zentrale Begriffe verwendet, die bereits die wichtigsten Akteure der Mobile IP Architektur darstellen. Damit diese bekannt sind, sei an dieser Stelle ein kurzer Überblick gegeben. Die Namensgebung basiert auf der in anderen Arbeiten und Normen zu Mobile IP vorgefundenen, um eine Einordnung dieser Ausarbeitung in bestehendes Wissen oder eine Verknüpfung mit anderen Arbeiten zu erleichtern.
Der **Mobile Host (MH)** ist ein beliebiges, mobiles Endgerät, dessen Ziel es ist, stets unter einer festen IP erreichbar zu sein. Das kann z.B. ein Notebook mit Netzwerkanschluss sein (egal ob kabelgebunden oder wireless), ein PDA oder auch jeder andere normale Rechner der das IP-Protokoll nutzt. Wie "mobil" das Gerät dabei wirklich ist, soll heissen, wie oft die potentielle Mobilität tatsächlich genutzt wird, spielt dabei keine Rolle.
Als **Correspondent Node (CN)** wird der Kommunikationspartner zum Mobile Host bezeichnet. Der Correspondent Node kann natürlich seinerseits auch wieder ein Mobile Host sein. Die vorgestellten Techniken und Mechanismen laufen dann in beiden statt in nur einer Richtung ab. Der Einfachheit und Übersichtlichkeit halber wird der Correspondent Node aber im Folgenden wie ein beliebiger, das IP Protokoll nutzender statischer Rechner behandelt. Selbstverständlich kommuniziert ein Mobile Host in der Regel mit vielen Correspondent Nodes gleichzeitig. Der **Home Agent (HA)** ist ein im Heimatnetzwerk des Mobile Host installierter Rechner. Er hat daher denselben IP-Netzwerkanteil wie der Mobile Host.
Foreign Agents (FA) sind die Ansprechpartner der Mobile Hosts, die in fremden Netzwerken installiert sind und die den Mobile Hosts bestimmte Mobile IP Funktionalität zur Verfügung stellen. Die genauen Aufgaben und Arbeitsweisen von Home und Foreign Agents werden im Folgenden genauer dargestellt.

II. Lösungsansatz

Die Grundidee von Mobile IP basiert auf derselben Idee wie das Nachsendeverfahren der Deutschen Post. Ein bei vorübergehender oder dauerhafter Abwesenheit gestellter Nachsendeauftrag veranlasst, dass die heimische Postfiliale alle an den betreffenden Haushalt adressierten Sendungen abfängt und an den neuen Wohnort oder den Urlaubsort weiterleitet. Diese Aufgabe übernimmt in Mobile IP der im Heimatnetzwerk installierte Home Agent. Er leitet die Pakete an den Foreign Agent des Netzwerks weiter, in dem sich der Mobile Host gerade befindet. Dieser FA stellt die Pakete dann netzwerkintern an den Mobile Host zu. Aus diesem Aufbau ergibt sich eine Reihe von Forderungen. Zunächst benötigen sowohl Home Agent als auch Foreign Agent Kenntnis über den momentanen Aufenthaltsort des Mobile Host. Der Home Agent benötigt im Grunde als Aufenthaltort nur die Angabe des momentan zuständigen Foreign Agent an den er ankommende Pakete für den Mobile Host weiterleiten soll. Zu diesem Zwecke verwaltet der Home Agent eine Liste aller Mobile Hosts, die ihn als Home Agent sehen. Sind die Mobile Hosts im Heimatnetzwerk, so melden sie sich beim Home Agent an, eine Umleitung der Pakete ist nicht nötig. Ist der betreffende Mobile Host nicht im Heimatnetzwerk registriert, so ist er entweder nicht erreichbar, oder an ein fremdes Netzwerk angeschlossen. Letzteres bekommt der Home Agent – samt der Adresse des momentan zuständigen Foreign Agents – ebenfalls mitgeteilt (wie das geht wird später erläutert). Der Foreign Agent muss den Mobile Host kennen, um diesem eingehende Pakete zustellen zu können. Dies läuft über die MAC-Adresse des Mobilen Endgeräts, die der Foreign Agent gemeinsam mit der mobilen IP-Adresse in seiner Visitor List speichert, einer Tabelle aller momentan an diesem Netzwerk angeschlossenen fremden Mobile Hosts.

Hauptteil

I. Szenario I – MH im Heimnetzwerk

Betrachten wir zunächst den einfachsten Fall. Der Mobile Host ist in seinem Heimatnetzwerk angeschlossen. Diese Lösung funktionierte ja bereits ohne Mobile IP. Mobile IP soll daher beim Anschluss des Endgeräts ans Heimatnetzwerk zwar einsatzbereit sein und somit jederzeit den Wechsel in ein anderes Netzwerk ermöglichen, die Technologie darf aber den Standardfall nicht durch Performanzeinbußen stören. Die Zusatzmaßnahmen zu Mobile IP sollten im Idealfall vom Benutzer gar nicht als vorhanden bemerkt werden.
Wird ein Mobile Host im Heimatnetzwerk angeschlossen, so kommt es zu folgendem Standardablauf:
Der Home Agent (wie auch jeder Foreign Agent) versendet sogenannte Agent Advertisement Messages, durch die der Mobile Host seinen Ansprechpartner im Netzwerk findet. Diese Agent Advertisement Messages (AAM) werden sehr häufig ausgesendet (nicht unbedingt in regelmässigen Zeitabständen, um einem Synchronisieren mit anderen Foreign Agents vorzubeugen), um neu dazugekommenen Mobile Hosts eine baldige Registrierung und somit kurze Offline-Zeiten zu ermöglichen.
In kabelgebundenen Netzen ist es relativ simpel für jeden möglichen Anschlussort genau einen zuständigen Agent zu identifizieren, in kabellosen Netzen muss diese Auswahl (bei mehreren möglichen) über bestimmte Parameter, wie etwa Signalstärke oder einen vorberechneten Weg (dies ist sinnvoll etwa entlang einer Autobahn oder Zugstrecke) erfolgen.
Die Agent Advertisement Messages enthalten neben den Anmeldedaten des aussendenden Agents auch einen Gültigkeits-Zeitstempel, der verhindern soll, dass ein Mobile Host, der das Sendegebiet des Agents verlässt, weiterhin lange Zeit versucht, sich mit diesem zu verbinden. Empfängt also nun unser Mobile Host eine AAM, so erkennt er aus den enthaltenen Daten, dass er im Heimatnetzwerk ist und meldet sich bei seinem Home Agent an. Dieser braucht nun nichts weiter zu tun, als ankommende Pakete für den Mobile Host wie ein normaler Router weiterzuleiten. Der Registrierungsprozess muss nicht wiederholt werden, da der Mobile Host dem Home Agent bei einem Netzwerkwechsel seinen neuen Aufenthaltsort bekanntgibt. Ein Abschalten des Mobile Hosts führt dazu, dass Pakete an den MH nicht zugestellt werden können und somit verloren gehen. In diesem Punkt besteht kein Unterschied zur bisherigen Lösung ohne Mobile IP.
Die Unterscheidung zwischen bekanntem Mobile Host (sieht den Agent als Home Agent) und fremdem Mobile Host (sieht den Agent als Foreign Agent) macht der Agent selber anhand vordefinierter Benutzerlisten. Dies eröffnet zum einen natürlich Vorteile bei der Rechtevergabe und beim Entwerfen der Sicherheitspolicies, zum anderen müsste bei einem umbekannten Mobile Host dieser ja beim jeweiligen Home Agent registriert werden um eine Weiterleitung zu ermöglichen. Doch dazu mehr im nächsten Kapitel.

II. Szenario II – MH wird an fremdes Netzwerk angeschlossen

Nachdem wir gerade den Basisfall (MH ist im Heimnetzwerk angeschlossen) kennen gelernt haben, bewegt sich der MH jetzt in ein fremdes Netzwerk. An das Wissen darüber, dass er sein Heimatnetzwerk verlassen hat, kommt er, indem er bemerkt, dass die letzte Agent Advertisement Messages seines Home Agents ihre Gültigkeit verloren hat oder er eine solche Nachricht eines Foreign Agents empfängt. Mit dem Erhalt einer AAM eines fremden Agenten versucht sich der MH bei seinem Home Agent zu melden um diesem seinen derzeitigen Aufenthaltsort bekannt zu geben. Dieser Registrierungsprozess erfolgt über die Registration

Request Message (Mobile Host → Home Agent) und der Registration Reply Message (Home Agent → Mobile Host). Nachdem die Registrierung abgeschlossen ist, ist dem HA der aktuelle Aufenthaltsort des MH bekannt und auch beim gerade zuständigen Foreign Agent ist der MH auf der Visitor List eingetragen (Bild II.a). Diese Mechanismen zur Registrierung stellen naturgemäß eine mögliche Schwachstelle der Sicherheit da. Auf potentielle Gefahren und die Absicherung dieser Mechanismen wird im 10. Kapitel an einem Beispiel eingegangen.
Wenn jetzt ein beliebiger Correspondent Node dem MH Datenpakete schicken will, so geschieht dies analog zum Szenario I. Weil der Sender die Daten an die feste IP des mobilen Endgerätes schickt, landen diese natürlich im Heimatnetzwerk. Da sich der Mobile Host beim Home Agent registriert hat, weiß dieser, dass der MH momentan in einem Fremdnetzwerk angeschlossen ist. Er fängt die Pakete die an den MH adressiert sind ab und tunnelt diese durch Paket-Kapselung an die Care-of-Adress. Diese bezeichnet in der Regel den Foreign Agent, der dann die getunnelten Pakete empfängt, sie "auspackt" und sie schließlich an den MH weiterleitet (Bild II.b).
Die Mobilität des MH spielt für den Correspondent Node somit keine Rolle, es ist also keine Änderung oder Erweiterung auf der Senderseite nötig, was die Einführung von Mobile IP natürlich stark vereinfacht, was eine rasche Verbreitung sehr begünstigt.

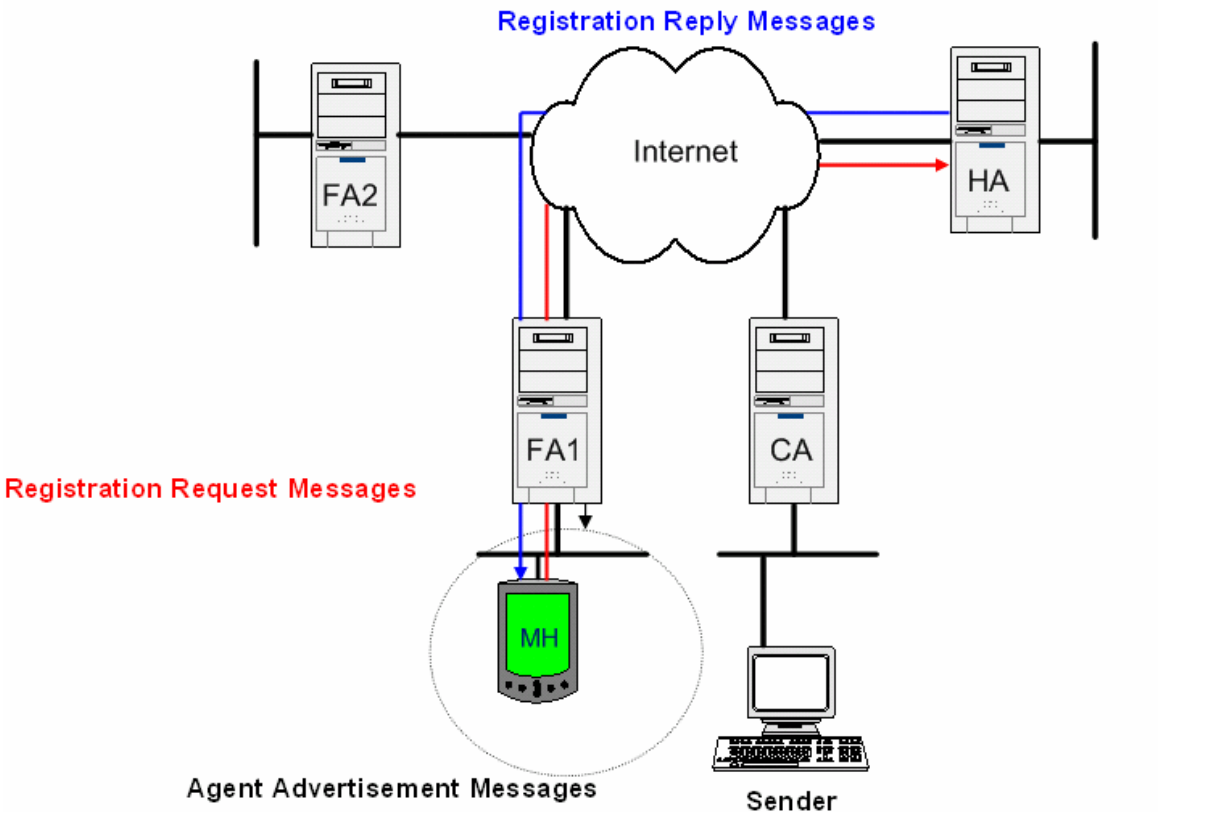


Bild II.a

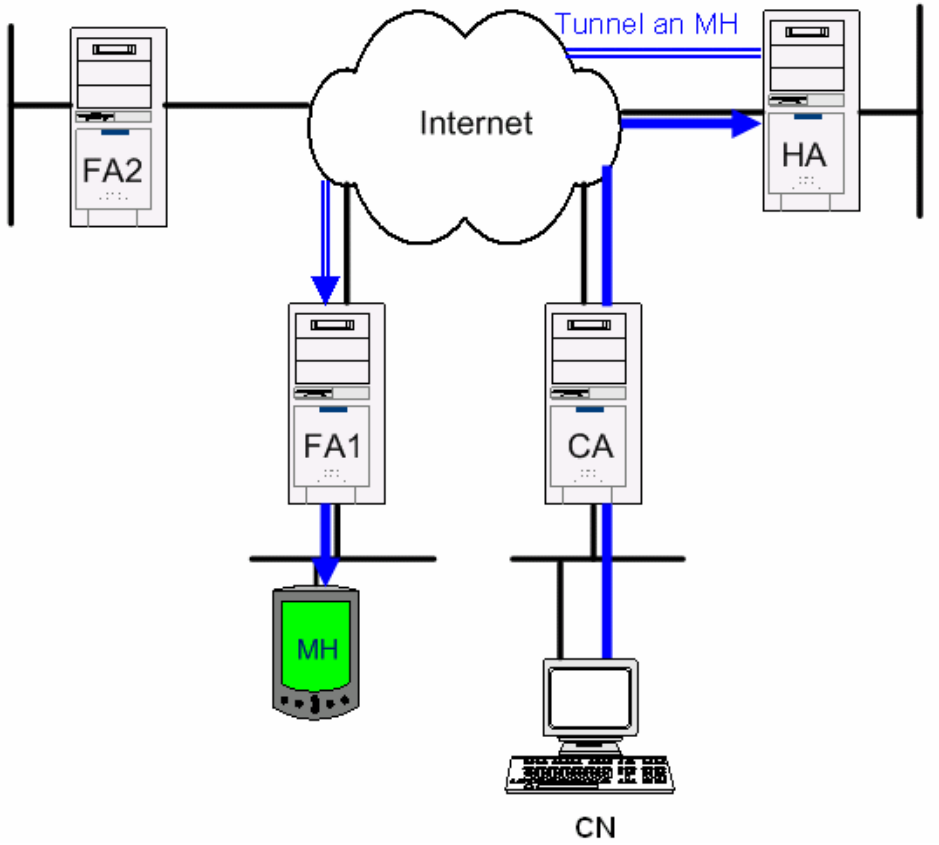


Bild II.b

III. Tunnelling

In Kapitel II wurde uns ein Szenario vorgestellt, in dem unser MH nur noch unter seiner festen IP erreichbar war, weil der HA die betroffenen Datenpakete abfängt und sie durch einen „Tunnel“ an den FA schickt. Beschäftigen wir uns nun etwas näher mit dem Prinzip der Pakettunnelung und -kapselung.
Die an den MH adressierten Pakete die in seinem Heimatnetzerk ankommen, bestehen aus einem IP Header und der eigentlich Nutzlast (siehe Bild III.a)

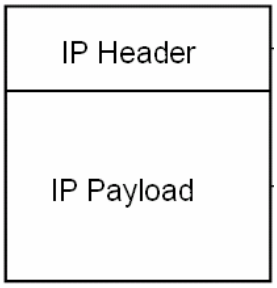


Bild III.a

Ist der MH zur Zeit in einem anderen Netzwerk angeschlossen, so muss der HA diese Pakete an die bei der Registrierung genannte CoA weiterleiten. Deshalb nimmt er das gesamte Paket und packt es erneut ein. Der neue IP Header ist nun die registrierte Care-of-Adresse und die neue Nutzlast ist das komplette ursprüngliche Paket. Diesen Vorgang nennt man auch Kapselung (engl. Encapsulation – Bild III.b)

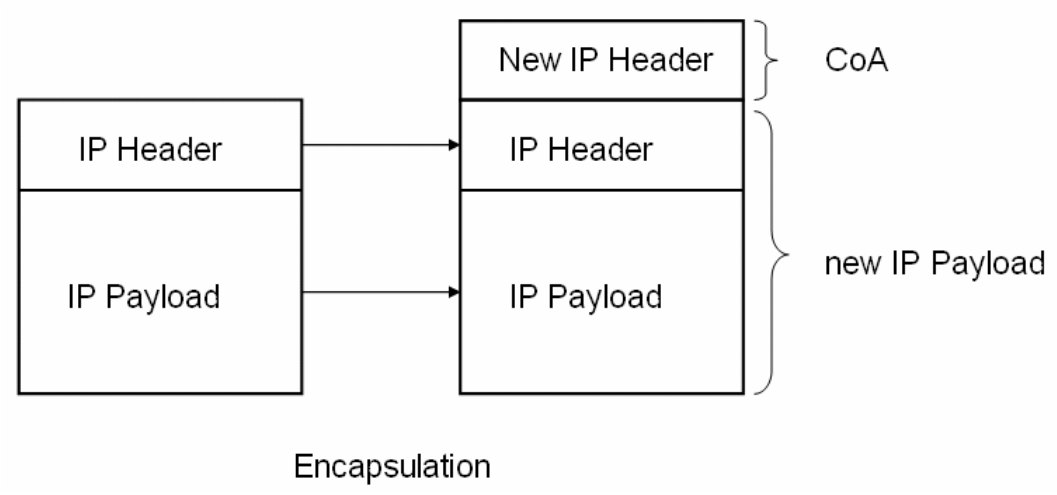


Bild III.b

IV. Problem: Triangle Routing

Wir wissen nun, dass Datenpakete den MH auch erreichen, wenn dieser sich in einem anderen Netzwerk aufhält. Der HA übernimmt für uns also die Aufgabe des „Paketzustellers“. So schön einfach dieses Verfahren jedoch für einen beliebigen Correspondent Node sein mag, so hat es doch erhebliche Nachteile. Weil alle Pakete den Umweg über den HA machen müssen wird unter Umständen das Netz unnötig belastet. Die Pakete laufen nun nicht mehr den einfachsten, also kürzesten Weg zwischen Sender und Empfänger, sondern nehmen stets den Umweg über den jeweiligen Home Agent des Empfängers (Mobile Host). Besonders deutlich wird dieser Umweg, wenn sich der MH im selben Subnetz wie der CN befindet. Denn statt die Pakete direkt intern an den MH zuzustellen, werden sie erst zum HA geschickt, der womöglich auf der anderen Seite der Welt steht, um danach über denselben – oder einen sehr ähnlichen – Weg zurückgeschickt zu werden. Bild IV.a soll dies verdeutlichen.

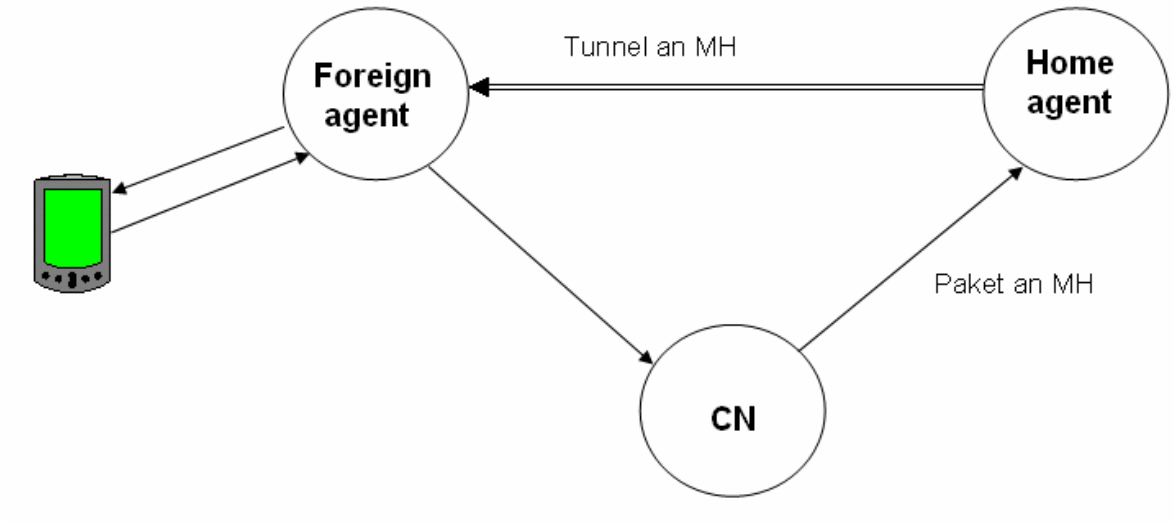


Bild IV.a

V. Routen Optimierung (Binding Update)

Um solche unnötigen Laufwege von Pakete zu vermeiden und die Performanz der Datenübertragung zu steigern, sehen wir uns nun die Methoden der Routen Optimierung an, die Mobile IP vorsieht. Zunächst lernen wir nach Home Agent und Foreign Agent einen weiteren wichtigen Akteur in Mobile IP kennen, den sog. **Cache Agent (CA)**. Dieser CA kann sich den aktuellen Aufenthaltsort unseres MH merken, indem er sich die benötigten Informationen darüber in einem Binding Cache genannten Puffer speichert. Wenn nun ein solcher CA den Auftrag bekommt, Pakete an die feste IP eines MH zuzustellen und er über einen gültigen Eintrag zu dieser IP in seinem Binding Cache verfügt, so tunnelt er das Paket direkt an die im Speicher befindliche CoA. Die Tunnelung erfolgt analog zu dem Verfahren, das in Kapitel III für den Home Agent vorgestellt wurde.
Ein optimaler Weg für das Paket wird natürlich erreicht, wenn der Sender selbst über einen solchen Binding Cache verfügt, weil dann die Pakete direkt an das aktuelle Netz (genauer: den aktuellen Foreign Agent) unseres MH geschickt werden können. Diese Funktionalität wird aber auf Seiten des Correspondent Node nicht vorausgesetzt. Ein dazwischen liegender Router, vorzugsweise ein Edge Router1, übernimmt diese Aufgabe, falls es der CN nicht selbst tut.
Nun stellt sich aber die Frage, wie ein CA an die Informationen über den aktuellen Aufenthaltsort des MH gelangt. Durch Bild V.a wird dieser Vorgang illustriert. Der HA schickt eine sogenannte Binding Update Message an den Correspondent Node, wenn dieser vom CN ein zu tunnelndes Paket für den MH empfängt (vgl. Kapitel II). Diese Binding Update Message, die neben der betroffenen IP-Adresse des Mobile Hosts und der entsprechenden aktuellen Care-of-Adresse auch eine begrenzte Gültigkeit (über Zeitstempel realisiert) enthält, wird von allen Cache Agents auf dem Weg zum CN in entsprechenden Caches gespeichert.

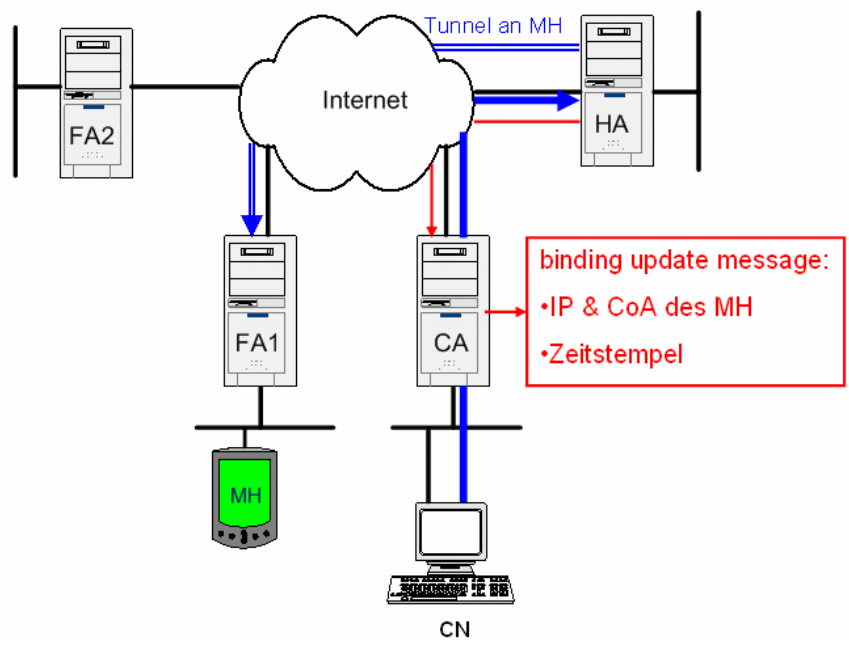


Bild V.a

Verfügt unser CN nicht über die Funktionalität eines CA, so wird er die Binding Update Message nicht beachten und weitere Pakete wieder an das Heimatnetzwerk des MH schicken. Diese Pakete durchlaufen dann alle Router in Richtung Heimatnetzwerk des MH, bis zum ersten Router auf dem Weg, der Cache Agent-Funktionalität besitzt. Dieser tunnelt die Pakete

[1] Edge Router, allgemein: an der Grenze zwischen 2 Netzwerken eingerichteter Router, hier Internet und Intranet

dann aufgrund seines aktuellen Binding Cache Eintrags auf direktem Weg (ohne Umweg über den HA) zum emtsprechenden Foreign Agent (Bild V.b).

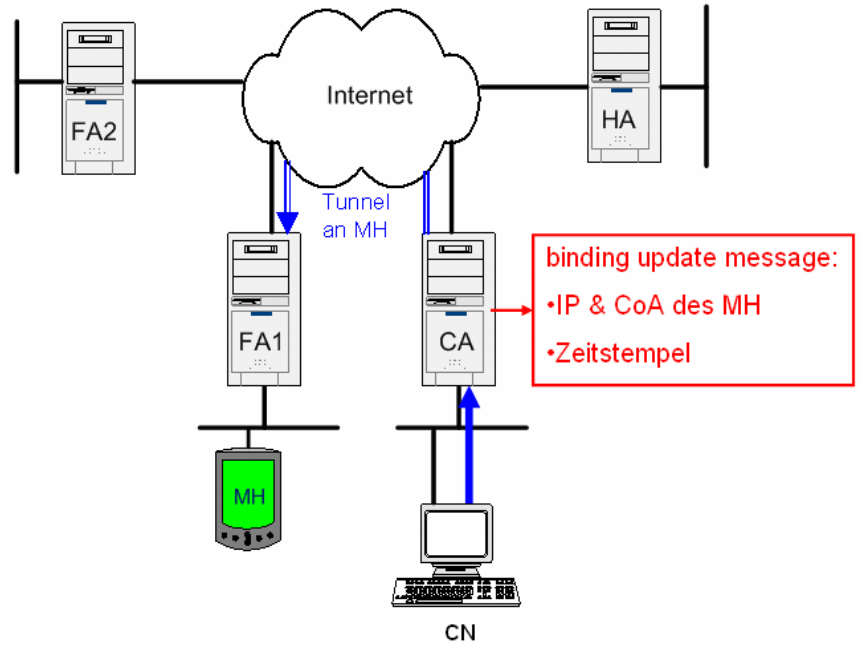


Bild V.b

VI. Szenario III – MH bewegt sich in weitere fremde Netzwerke

Die gerade vorgestellten Mechanismen zur Routen Optimierung sind es dann allerdings, die weitere Probleme nach sich ziehen. Diese treten dann auf, wenn sich ein Mobile Host in ein drittes oder in weitere Netzwerke bewegt.
Doch der Reihe nach: Stellt ein Mobile Host durch Empfangen der Agent Advertisement Message eines neuen Foreign Agent fest, dass er sich in einem anderen, neuen Fremdnetzwerk befindet, so registriert er sich natürlich wieder – wie beim ersten Netzwerkwechsel – per Registration Request Message mit neuer CoA bei seinem Home Agent. Dieser kann nun eintreffende Pakete wieder an die richtige Adresse weiterleiten. Parallel benachrichtigt der MH aber auch seinen letzten Foreign Agent per Binding Update Message über seine neue CoA. Daraus folgt, dass jeder Foreign Agent über Cache Agent Funktionalität verfügen muss, da ansonsten bei jedem Netzwechsel eine hohe Gefahr von Paketverlusten entsteht. Nun ist es dem alten FA möglich, an den MH adressierte Pakete an den neuen FA weiterzuleiten. Diese Pakete können in der Offline-Zeit ankommen, die zwischen Disconnect vom alten Fremdnetzwerk und der Registrierung bei HA und altem FA entsteht. Eine andere Möglichkeit ist, dass Cache Agents noch über Einträge in Ihrem Binding Cache verfügen, die auf die alte CoA verweisen. Solange der Eintrag sein Verfallsdatum noch nicht erreicht hat und auch kein Binding Update den alten Eintrag überschrieben hat, leitet der CA eintreffende Pakete für den betroffenen MH noch an den alten FA weiter. Geschieht dies, so tunnelt der alte FA die Pakete an den neuen FA weiter und informiert gleichzeitig den Home Agent des betroffenen Mobile Hosts per sogenannter Binding Warning Message darüber, dass der paketsendende Cache Agent nicht auf dem aktuellen Stand ist. Der Home Agent hat nun die Aufgabe, diesen Cache Agent – und analog zum allerersten Binding Update auch alle auf dem Weg dorthin liegenden – per Bindung Update Message auf den aktuellen Stand zu bringen. Dies hat 2 positive Effekte: Zum einen werden Weiterleitungsketten2 - zumindest bis zu einer bestimmten Wechselfrequenz – vermieden und zum zweiten wird der

[2] siehe Kapitel VII – "Probleme bei Szenario III – Motivation für Hierarchisches Mobile IP"

FA entlastet, der ansonsten bei hoher MH-Fluktuation viel Traffic für die Weiterleitung von Paketen an ehemalige Besucher aufbringen müsste.

VII. Probleme bei Szenario III – Motivation für Hierarchisches Mobile IP

Anhand von drei Beispielen soll nun gezeigt werden, welche Probleme beim Routen von Datenpaketen über Mobile IP entstehen können.
Die folgenden Beispiele sind rein theoretischer Natur und entstammen keinerlei Experimenten. Sie dienen lediglich dazu grundlegende Probleme zu erkennen und dessen Lösung schneller Aufzufassen.

Beispiel 1: Wir gehen davon aus, dass wir uns in einem Wireless Network befinden und die Zellengröße 40m beträgt. D.h. ein sich bewegender mobiler Host verweilt bei einer Geschwindigkeit von 5-6 km/h (etwa 1,5m/s) rund 27s in einer Zelle des Netzes, bevor es in eine andere Zelle wechselt. Wenn wir ferner davon ausgehen, dass der gesamte Registrierungsprozess (Registration Request + Registration Reply + evtl. Verzögerungen) rund eine Sekunde dauert, dann bleiben dem mobilen Endgerät noch 26 Sekunden zum Übertragen von Nutzdaten innerhalb dieser Zelle. Aus diesem Verhältnis zwischen Nutzdaten und Overvead lässt sich ein Wirkungsgrad von ca. 96% ermitteln. Wir sehen also dass bei langsamen Geschwindigkeiten, z.B. ein Fußgänger, keine größeren Probleme durch die Registrierung auftreten (Bild VII.a).

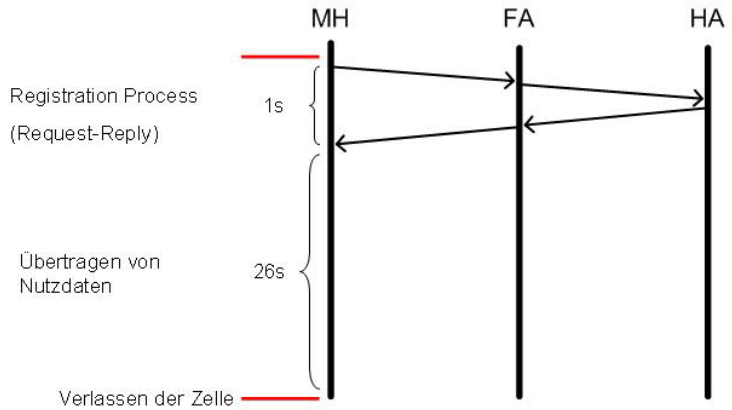


Bild VII.a

Beispiel 2: Nachdem nun unser Notebook durch einen Fußgänger transportiert wurde, bewegt es sich jetzt z.B. in einem Zug. Wir gehen davon aus dass dessen Geschwindigkeit bei 72 km/h (also 20 m/s) liegt. Bei einer Zellengröße von immer noch 40m, verweilt der Mobile Host also nur noch 2 Sekunden in jeder Zelle, bevor es zu einem Wechsel kommt. Wie wir in Bild VII.b erkennen können liegt der Wirkungsgrad nun nur noch bei 50%, da von den 2 Sekunden die wir uns in einer Zelle befinden nur eine Sekunde zum Übertragen von Nutzdaten zur Verfügung steht.

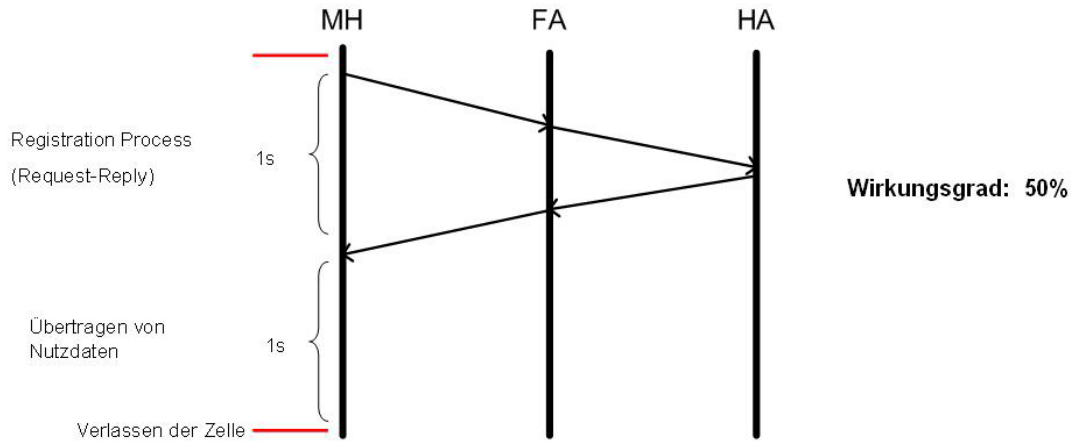


Bild VII.b

Beispiel 3: Als letztes Beispiel betrachten wir nun eine noch schnellere Fortbewegung, z.B in einem Auto. Wir nehmen an wir bewegen uns mit einer Geschwindigkeit von rund 144 km/h (also 40 m/s). D.h. für unser Notebook, es befindet sich nur noch eine Sekunde in jeder Zelle. Das daraus resultierende Problem wird schnell auf Bild VII.c deutlich. Der Wirkungsgrad bei einer solchen Geschwindigkeit ist nun auf 0% gesunken, da die gesamte Zeit die wir uns in einer Zelle befinden, dazu benötigt wird um den Mobile Host bei seinem HA anzumelden. Ist diese Registrierung abgeschlossen könnte ja eigentlich die Übertragung von Nutzdaten beginnen, aber im selben Moment verlassen wir die Zelle und eine neue Registrierung wird somit notwendig.

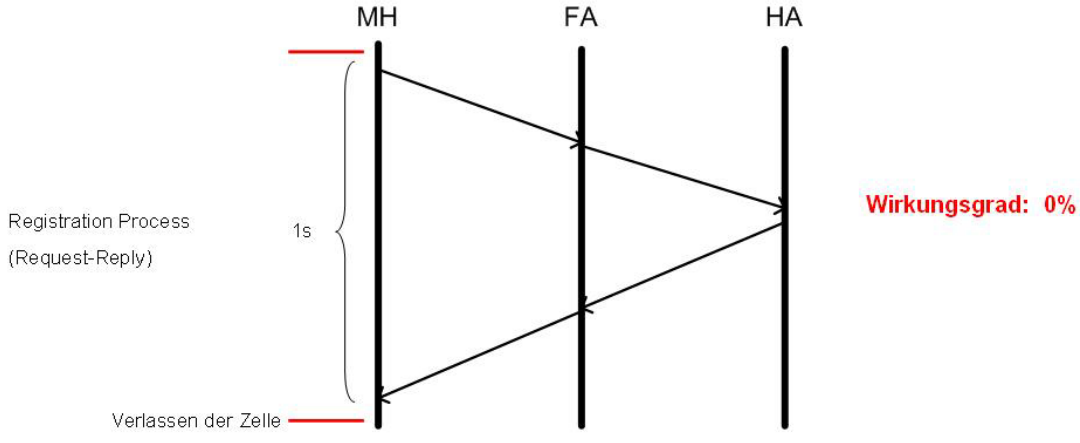


Bild VII.c

Diese 3 kurzen Beispiele sollten verdeutlichen, dass durch den Registierungsprozess vom MH über den FA bishin zum HA schnell ein enormer Overhead mit erheblichen Verzögerungen entstehen kann. Es gilt also nun die Zeit eines solchen Prozesses möglichst klein zu halten und Möglichkeiten zu finden, den unter Umständen langen Weg vom FA zum HA nicht für jeden Zellenwechsel durchlaufen zu müssen. Eine mögliche Lösung dieses Problems, das sogenannte hierarchische Mobile IP soll im folgenden Kapitel beschrieben werden.

VIII. Hierarchisches Mobile IP

In den Szenarien I bis III haben wir die Situation vorgefunden, dass sich in jedem Fremdnetz, in das sich unser Mobile Host bewegt, genau ein FA befindet. Im Gegensatz dazu befinden sich bei den hierarchisches Mobile IP unterstützenden Architekturen viele dieser FAs in einem Netz. Diese Agenten bilden eine baumartige Struktur, die auf Bild VIII.a dargestellt wird.

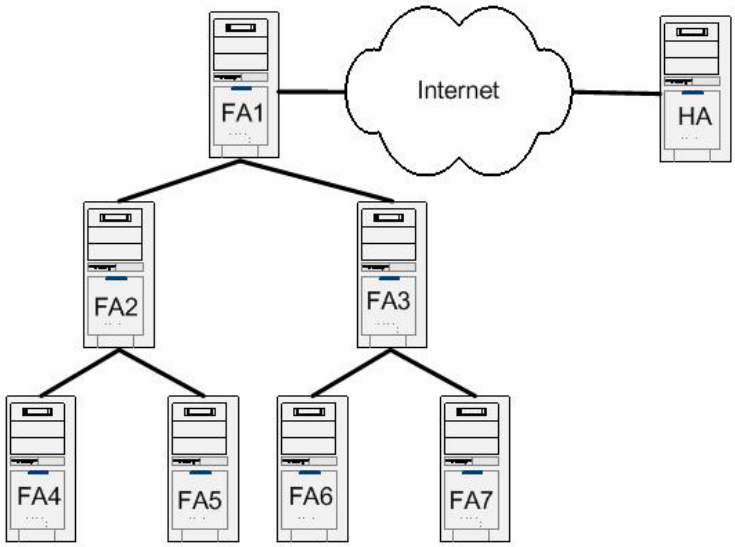
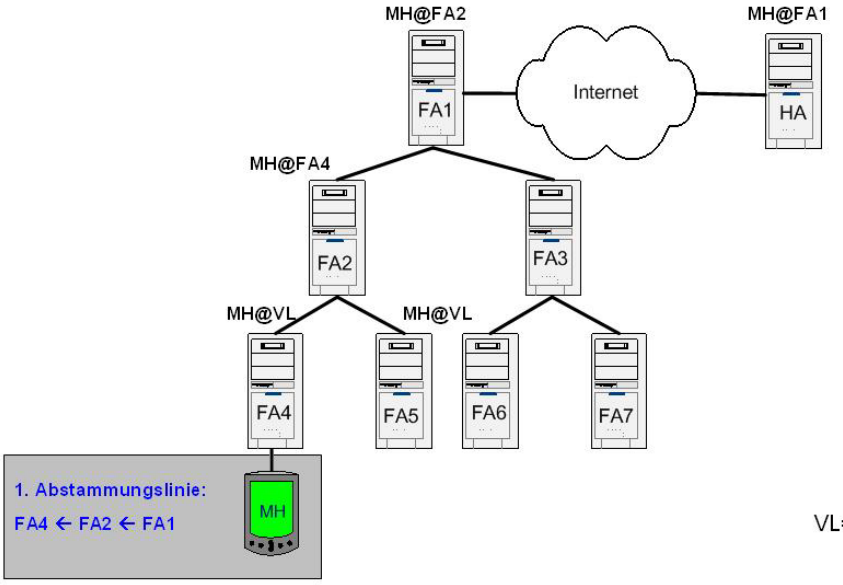


Bild VIII.a

Bewegt sich nun ein MH in eine Zelle für die FA4 zuständig ist, so erhält er zusammen mit der bekannten Agent Advertisement Message eine Abstammungslinie. Diese gibt ihm die Reihe der FAs an, die für ihn zuständig sind. Die nun folgende Registrierung beim HA, erfolgt im Gegensatz zu den Szenarien I – III nicht direkt vom FA4 zum HA, sondern schrittweise, über alle dazwischen liegenden FAs. Das bedeutet also, dass FA2 von FA4 gemeldet wird dass der MH bei ihm angeschlossen ist. Im zweiten Schritt meldet der FA2 dem FA1, dass der MH über ihn erreichbar ist. Und der hierarchisch höchste Agent FA1 registriert schließlich den MH bei seinem Home Agent. Nach diesem Anmeldungeprozess weiß also der HA, das er den MH über FA1 erreichen kann, FA1 kann den MH über FA2 erreichen und FA2 über FA4. Deutlicher wird dies auf dem Bild VIII.b



VL=*Visitor List*

Bild VIII.b

Nachdem nun alle betroffenen Agents über den aktuellen Aufenthaltsort des MH Bescheid wissen, erreichen alle für unseren Mobile Host bestimmten Datenpakete auch ihr Ziel. Der wirkliche Vorteil von Mobile IP wird aber erst nach einem erneuten Netzwechsel klar. Wechselt nun der MH von der Zelle für die FA4 zuständig ist, zur Zelle für die FA5 zuständig ist kommt es zu folgendem, im Vergleich mit nicht-hierarchischem Mobile IP deutlich vereinfachten und verkürzten Registrierungsprozess: Mit der Agent Advertisment Message die unser MH von FA5 erhält, bekommt er auch eine neue Abstammungslinie. Beim Vergleich seiner letzten gültigen Abstammungslinie (in unserem Fall, die von FA4) mit der eben erhaltenen, kann er den Crossover-Router ermitteln. Als Crossover Router wird derjenige Foreign Agent bezeichnet, der der hierarchisch höchste auf dem Weg zum HA ist, der noch von diesem Wechsel „betroffen“ ist. Für den eben vollzogenen Zellenwechsel, würden wir also FA2 als Crossover identifizieren. Nun werden schrittweise alle betroffenen FAs informiert, d.h. nur der Cache von FA2 und FA4 muss aktualisiert werden, da der MH jetzt nicht mehr über FA4, sondern über FA5 zu erreichen ist. Dagegen bleiben die Cache-Einträge von FA1 und besonders die des HA gültig, weil sich aus ihrer Sicht die Position des MH nicht geändert hat. Im Bild VIII.c ist der eben beschriebene Zellenwelchsel dargestellt. Nun wird deutlich das der Registrierungsprozess bis zum Crossover Router wesentlich schneller und effizienter vollzogen werden kann, als eine komplette Registrierung vom MH bis zum HA. Gerade das Auslassen dieses Datenaustauschs über das Internet (von FA1 zum HA), das mit allen möglichen Verbindungsengpässen aufgrund hohen Datenaufkommens belastet ist, verspricht dabei die grössten Performance-Steigerungen. Das nächste Kapitel befasst sich mit der Realisierung eines solchen Zellenwechsels und dem damit verbundenen Handoff zwischen den betroffenen FAs. Hierfür soll auch noch eine weitere Größe eingeführt werden, die Handoff-Latency, die in diesem Kapitel benötigt wird. Die Handoff-Latency gibt uns die Zeit an, die ein Paket vom MH zum Crossover Router und zurück benötigt (die sogenannte Roundtrip Time).

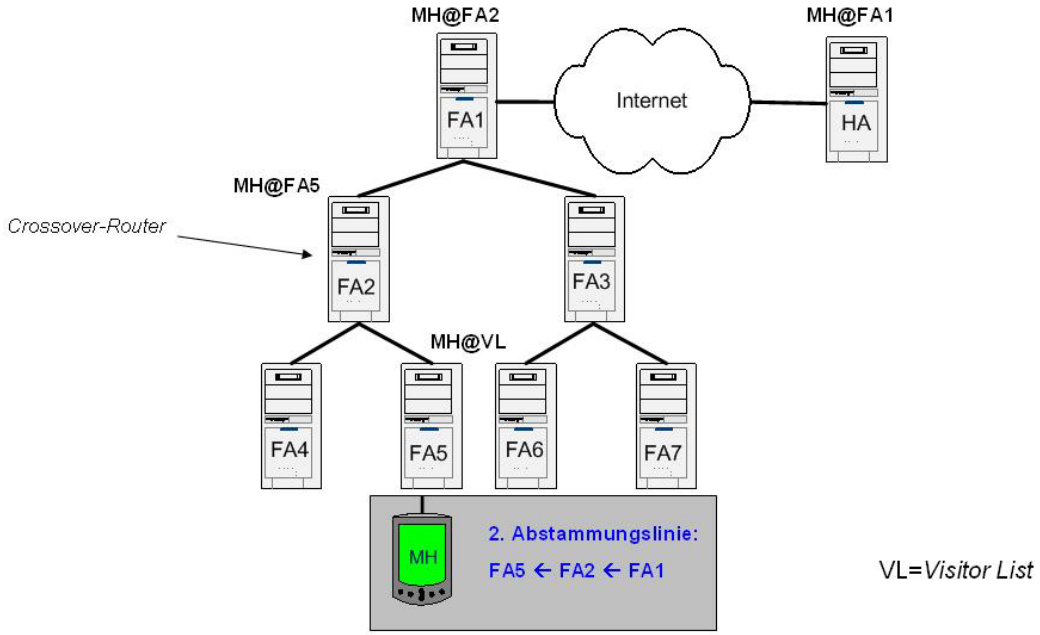


Bild VIII.c

IX. Handoffs (Hard Handoff vs. Semisoft Handoff)

Beim hierarchischen Mobile IP ist es einem Mobile Host nicht möglich, zu einem bestimmten Zeitpunkt bei mehr als einem Foreign Agent registriert zu sein. Bei kabelgebundenen Netzen ist dieser Umstand selbstverständlich, dasselbe gilt aber auch für WLANs. Aus der Architektur des hierarchischen Mobile IP ergibt sich der Vorteil einer kürzeren und schnelleren Registrierungsprozedur bei jedem Wechsel des Anschlussorts. Wie schon oben beschrieben sendet der Mobie Host eine sogenannte Route Update Nachricht über die neue Basisstation zum Crossover Router. Es gibt darüberhinaus jedoch 2 Möglichkeiten, wie dieser Handoff genau durchgeführt wird, den Hard und den Semisoft Handoff. Der Hard Handoff ist die einfachere Lösung, bei der es unter Umständen aber beim Zellenwechsel für kurze Zeit zur Nicht-Erreichbarkeit des Mobile Host kommt. Nach dem Anschluss an den neuen FA wird die oben angesprochene Route Update Nachricht gesendet. Nachdem der Crossover Router die Information erhalten hat ist die Verbindung wieder hergestellt und die Kommunikation kann weiter gehen. In der Zeit zwischen Aufgeben des Anschlusses am alten FA und dieser erneuten Sendebereitschaft – wie schon erwähnt auch Handoff-Latency genannt – sind allerdings Datenverluste kaum zu verhindern. Laufen Pakete zum alten FA, so können diese nur gerettet werden indem Sie später nachgesandt werden. Dies kann jedoch verhältnismäßig lange dauern und die Reihenfolge der Pakete durcheinander bringen, was weitere Probleme nach sich zieht.
Abhilfe schafft die zweite Möglichkeit, der sogenannte Semisoft Handoff. Auch hier sendet der Mobile Host eine Route Update Nachricht an den Crossover Router, die die neue Abstammunglinie beinhaltet. Allerdings geschieht das vor dem eigentlichen Zellenwechsel. Das bedeutet natürlich, dass er seinen neuen Anschlussort bereits kennen muss. Erst nachdem diese Nachricht am Crossover Router registriert worden ist und die daraufhin gesendete Quittung vom Mobile Host empfangen wurde findet der Wechsel des MH zum neuen FA wirklich statt. Während der Handoff Latency werden also Pakete für den MH vom Crossover Router aus über beide Wege weitergeleitet, womit dem Verlust von Paketen wirksam vorgebeugt wird. Nach dem Anschluss am neuen FA muss der MH noch beim Crossover Router den alten Weiterleitungsweg „abschalten“, auch dies geschieht über eine Route Update Message. Auch hier kann es jedoch zu Unregelmässigkeiten im Paketstrom kommen (Vertauschungen, doppelter Empfang, verlorene Pakete), allerdings nur, wenn die Laufzeiten der Pakete über die alte und die neue Abstammungslinie signifikant voneinander abweichen.

Zusammenfassung

I. Bestehende Probleme

Selbstverständlich gibt es noch einige Probleme, die auf dem Weg zur Marktreife zu bewältigen sind. Einige seien hier kurz vorgestellt. So ist es nicht ganz unproblematisch, getunnelte Pakete auf Ihren Inhalt zu überprüfen. Ohne diese Möglichkeit ist aber die gesonderte Behandlung bestimmter Arten von Datenströmen nicht zu bewerkstelligen. Um eine solche Art Quality of Service Dienste also auch unter Verwendung der Mobile IP Mechanismen realisieren zu können muss also noch ein Weg gefunden werden, getunnelte Pakete entsprechend ihres Inhaltes zu markieren.
Auch die im Hauptteil vorgestellten Sicherheitsanforderungen sind noch nicht vollständig umgesetzt. Da die Sicherheit allerdings – wie in fast jeder Kommunikationstechnologie – auch hier ein sehr weites Problem- und Aufgabenfeld darstellt, soll auf diese Probleme nicht weiter eingegangen werden, als dies im Hauptteil schon geschehen ist. Zuguterletzt besteht noch Handlungsbedarf bei der Registrierung. Diese ist bei schneller Mobilität noch nicht optimal und erzeugt zuviel Overhead, was die Effizienz der Kommunikation spürbar beeinträchtigen kann (hier sei nochmal auf Kapitel 7 im Hauptteil hingewiesen). Eine Overhead-arme Verbindung muss auch bei schneller Bewegung durch die Fremdnetzwerke (z.B. bei Autos, Zügen oder sogar Flugzeugen) gewährleistet sein.

II. Ausblick & Hinweis auf Test Sessions

Die Mobile IP Mechanismen sind vollständig im IPv6 Protokoll enthalten und werden damit ab 2003 (dann beginnt die schrittweise Einführung von IPv6) zur Verfügung stehen. Auch die Bildung einer eigenen Mobile IP Workgroup durch die IETF zeigt die Bedeutung dieser Technologie. Das auch die Wirtschaft großes Interesse daran zeigt, wird nicht zuletzt durch die zahllosen, bereits laufenden Test Sessions deutlich, mit denen die Unternehmen erste Erfahrungen auf diesem Gebiet sammeln. Im Folgenden seien kurz die wichtigsten drei Mobile IP Test Sessions und eine stichwortartige Auflistung deren Eigenschaften und Besonderheiten genannt:

- **MIPL MOBILE IPV6 FOR LINUX**
  URL: http://www.mipl.mediapoli.com/ (OS: Linux 2.4)
  Bemerkungen:
  - Kernelpatch und User-Daemon
  - IPv6
  - MIPL ging aus dem HUT-Projekt (s.u.) hervor
  - Intergration von IPSEC und der AAA-Erweiterung

- MICROSOFT IPV6
  URL: http://research.microsoft.com/msripv6/ (OS: Windows NT/2000)
  Bemerkungen:
  - nur für MHs
  - integriert in den IPv6-Stack

- Dynamics - HUT (Helsinki University of Technology) Mobile IP
  URL: http://www.cs.hut.fi/Research/Dynamics/index.html
  (OS: Linux 2.1-2.4, Windows (nur MH))
  Bemerkungen:

- aktuellste Implementierung
- Kernelmodul (für den IPIP-Tunnel) und Userspace-Daemon
- Konfigurationsassistenten, Webinterface für HA und FA
- Verschlüsselung über RSA möglich
- kommerzielle Variante: Lifix GO! - http://www.lifix.fi
- auch für alle Windows-Versionen verfügbar(nur MH)
- Reverse Tunneling
- hierarchische Anordnung von FAs => Nutzung eines privaten Adreßraumes
- Care-Of Adressen möglich

III. Quellen

(1) Mobile IP working group der IETF
www.ietf.org/html.charters/mobileip-charter.html

(2) „Seminar-Vortrag: Mobile IP" von Jochen Witte
www.zib.de/schintke/lehre/mobile-computing/ausarbeitung-mobile-ip-witte.pdf

(3) TU Braunschweig - Vorlesung Mobilkommunikation SS 2002
(Prof. Dr. Lars Wolf)
www.ibr.cs.tu-bs.de/lehre/ss02/mk/pdf-2x2/K09a-Netzwerkprotokolle.pdf

(4) Tutorial „Mobile Networking Through Mobile IP" (Charles E. Perkins)
www.computer.org/internet/v2n1/perkins.htm

(5) Vortrag: „GSM Mobile Networks - Procedures and Scenarios" von Dipl. Ing. Ingo Schacht (Siemens Mobile) am HPI, 26.06.2003

(6) Busch, Wolthusen „Netzwerksicherheit" von Spektrum Akademischer Verlag, 2002 (ISBN 3-8274-1373-7)

(7) Kurose, Ross "Computernetzwerke - Ein Top-Down Ansatz mit Schwerpunkt Internet" von Pearson Higher Education, 2002 (ISBN 3-8273-7017-5)