

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/298969536>

# Mobilität für das Internet mit dem Mobile Internet Protocol

Article · January 2010

---

CITATIONS

0

READS

569

1 author:

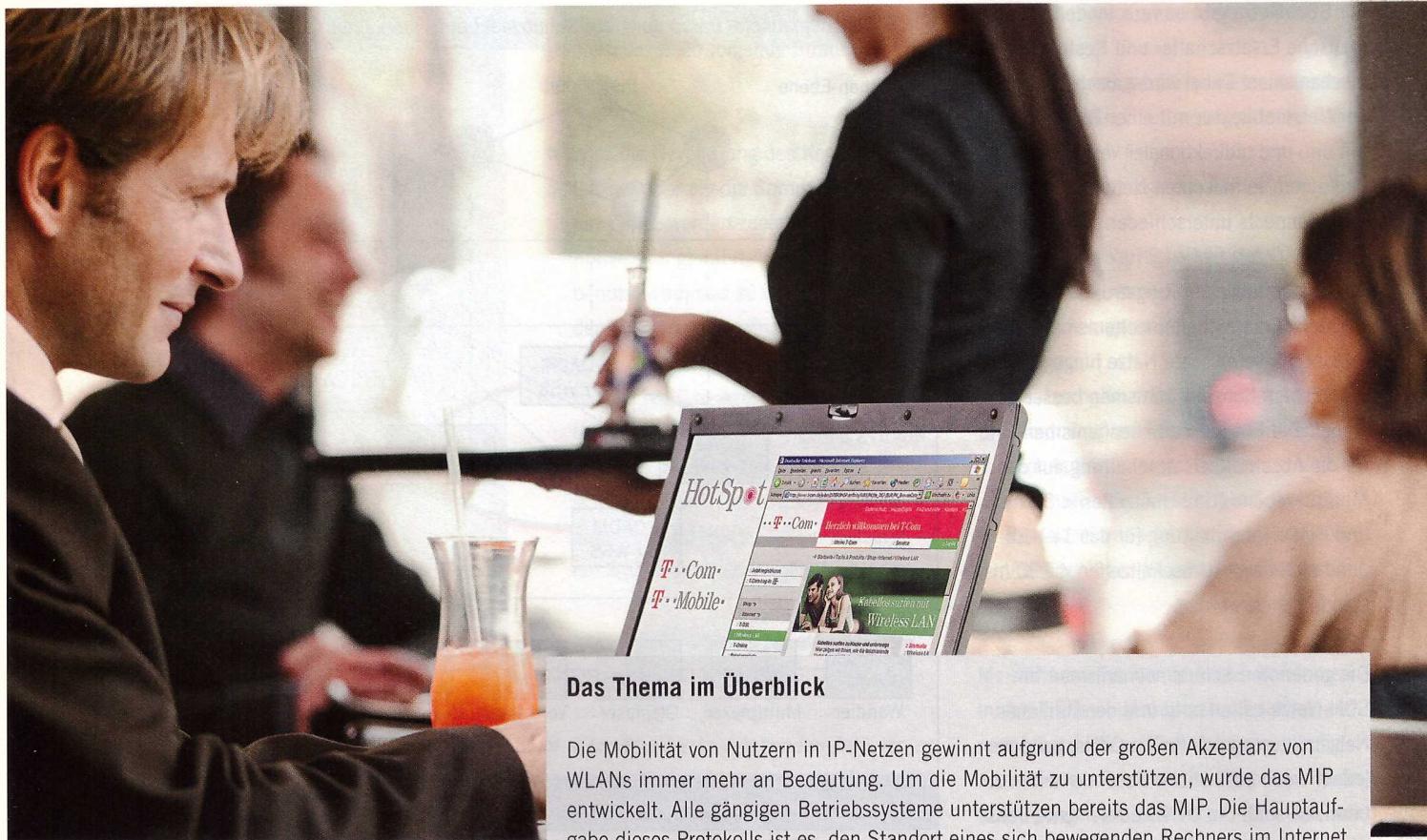


Anatol Badach

University of Applied Sciences Fulda

295 PUBLICATIONS 123 CITATIONS

[SEE PROFILE](#)



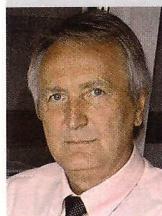
### Das Thema im Überblick

Die Mobilität von Nutzern in IP-Netzen gewinnt aufgrund der großen Akzeptanz von WLANs immer mehr an Bedeutung. Um die Mobilität zu unterstützen, wurde das MIP entwickelt. Alle gängigen Betriebssysteme unterstützen bereits das MIP. Die Hauptaufgabe dieses Protokolls ist es, den Standort eines sich bewegenden Rechners im Internet zu erkennen und sicherzustellen, dass alle Datenpakete für diesen Rechner auch ihren Bestimmungsort erreichen, unabhängig davon, wo sich dieser Rechner gerade befindet.

# Mobilität für das Internet mit dem Mobile Internet Protocol

Alle neuen Laptops verfügen heute über einen WLAN-Adapter. Das MIP ermöglicht eine uneingeschränkte Nutzung dieser Adapter und unterstützt damit die Mobilität der Internetnutzer. So kann ein Nutzer z.B. während einer aktiven Verbindung ein Subnetz wechseln, ohne die Verbindung abbrechen zu müssen. Weil es zwei Generationen des Internetprotokolls gibt – die Versionen IPv4 und IPv6 – ist auch zwischen MIPv4 und MIPv6 zu unterscheiden. Beide Konzepte verfolgen zwar die gleichen Ziele, sind aber unterschiedlich. Dieser Beitrag beschäftigt sich mit MIPv4 – hier als MIP bezeichnet.

### Der Autor



Prof. Dr.-Ing. Anatol Badach lehrt an der Hochschule Fulda im Fachbereich Angewandte Informatik, Telekommunikation und Netzwerke. Er ist Autor mehrerer Fachbücher.

### Ziele von MIP

Mobile Rechner mit Internet-Anschluss (Laptops und Netbooks mit WLAN-Adaptoren) werden immer beliebter. Daher wird ein Konzept benötigt, mit dem die Mobilität in IP-Netzen unterstützt werden kann. Die IETF hat hierfür das Protokoll MIP erarbeitet, das für tragbare Rechner gedacht ist, um diese effektiv in IP-Netzen einsetzen zu können. Beispielsweise kann ein mobiler Rechner mit dem MIP während einer bestehenden Verbindung seinen Standort in einem Netz-

werk wechseln, ohne dass die aktuell „laugenden“ Anwendungen neu gestartet oder die bestehenden Verbindungen zu anderen Rechnern unterbrochen werden müssen. Das Protokoll MIP kann damit als eine Erweiterung des Internetprotokolls in Hinblick auf die Unterstützung von Mobilität angesehen werden.

### Mobilität in IP-Netzen

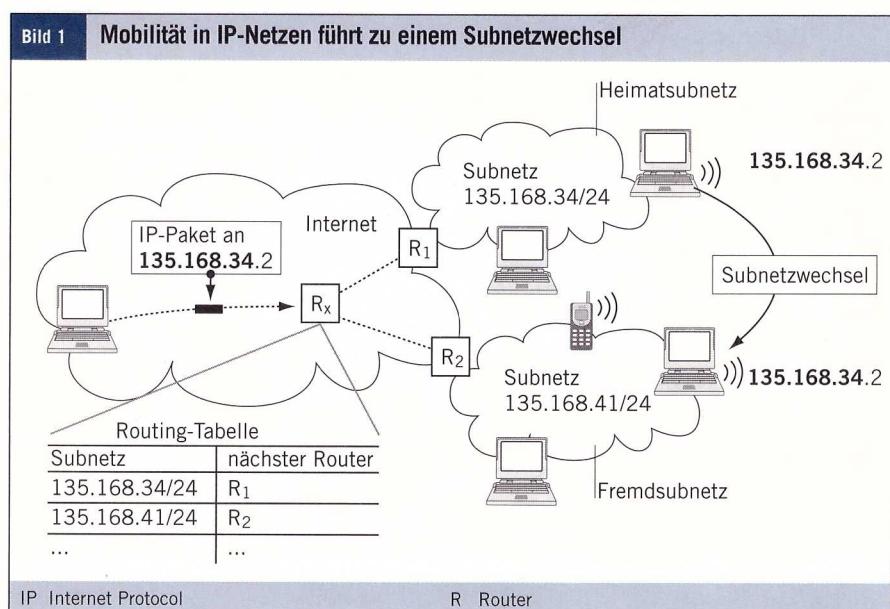
Das Problem der Unterstützung der Mobilität von Laptops in IP-Netzen ist mit der Verfol-

gung des aktuellen Standorts von Rechnern im Netz verbunden. Ein IP-Netz stellt eine Vernetzung mehrerer IP-Subnetze<sup>1</sup> dar, die mithilfe von Routern miteinander verbunden werden. Der Standort von Rechnern in IP-Netzen wird durch ihre IP-Adressen bestimmt. Eine IP-Adresse hat folgende Struktur:

$$\text{IP-Adresse} = (\text{Subnetz-ID}, \text{Rechner-ID})$$

Ein Rechner mit einer IP-Adresse in einem IP-Netz gehört daher immer zu einem IP-Subnetz. Dies bedeutet, dass jeder Rechner nur in einem bestimmten IP-Subnetz beheimatet ist. Daher wird vom **Heimatsubnetz** eines Rechners gesprochen. Die IP-Adresse des Rechners in seinem Heimatsubnetz kann deshalb als **Heimat-IP-Adresse** (kurz **Heimatadresse**) betrachtet werden. Bei einem mobilen Rechner muss jedoch damit gerechnet werden, dass er sein Heimatsubnetz verlässt und sich vorübergehend in einem **Fremdssubnetz** aufhält. Dies führt zu einem Subnetzwechsel, wie er in Bild 1 dargestellt ist: Im hier gezeigten Beispiel sendet ein Rechner im Internet ein IP-Paket – einem Brief entsprechend – an den mobilen Zielrechner im Subnetz 135.168.34/24. Der Router R<sub>x</sub> im Internet leitet dieses IP-Paket anhand seiner Routing-Tabelle an den Router R<sub>1</sub> am Internetzugang zum Heimatsubnetz des Zielrechners weiter. Da der Zielrechner sein Heimatsubnetz aber verlassen hat, kann das ankommende IP-Paket den Zielrechner – ohne Einsatz von MIP – nicht erreichen.

Normalerweise werden die Pakete an einen Rechner, die vom Internet adressiert wurden, immer in sein Heimatsubnetz transportiert. Hat ein mobiler Rechner aber sein Heimatsubnetz verlassen, müssen die an ihn adressierten IP-Pakete entsprechend in das Fremdssubnetz, in dem sich dieser mobile Rechner gerade aufhält, umgeleitet werden. Im Fremdssubnetz muss dem mobilen „**Gastrechner**“, um ihn auch innerhalb dieses Fremdssubnetzes eindeutig lokalisieren zu können, übergangsweise eine neue IP-Adresse mit der Subnetz-ID des Fremdssubnetzes zugewiesen werden. Damit der Gastrechner in einem Fremdssubnetz aus dem



Internet erreicht werden kann, muss dieses Fremdssubnetz dem Router R<sub>1</sub> am Internetzugang zu seinem Heimatsubnetz bekannt sein, sonst kann er die aus dem Internet für den mobilen Rechner ankommenen IP-Pakete nicht in das Fremdssubnetz umleiten. Eine solche Umleitung von IP-Paketen wird mit dem MIP umgesetzt.

### Anforderungen an MIP

An das MIP werden folgende Anforderungen gestellt:

- Ein mobiler Rechner muss immer – auch beim Verlassen seines Heimatsubnetzes – unter seiner Heimatadresse erreichbar sein.
- Die bereits im mobilen Rechner laufenden Anwendungen und bestehenden Beziehungen, wie z.B. Verbindungen über TCP zu anderen Rechnern, dürfen beim Verlassen eines Subnetzes nicht unterbrochen werden.
- Es soll gewährleistet sein, dass ein mobiler Rechner auch mit stationären Rechnern kommunizieren kann, also auch mit solchen Rechnern, die das MIP nicht unterstützen.
- In stationären Rechnern sollten keine Erweiterungen für die Kommunikation mit mobilen Rechnern erforderlich sein.
- Die mobilen Rechner sollten mindestens den gleichen Sicherheitsanforderungen

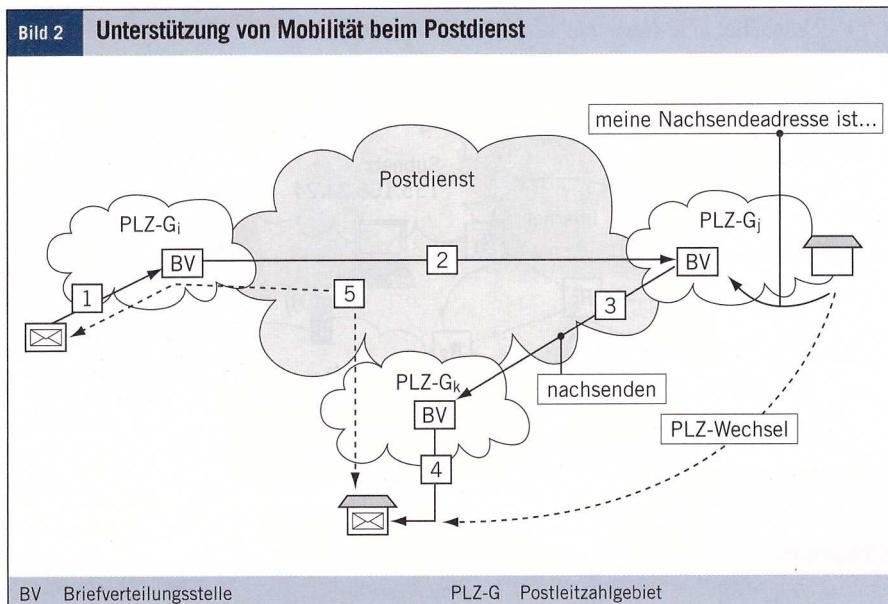
genügen, die für stationäre Rechner gelten. Dies betrifft beispielsweise die Implementierung von Mechanismen für die Authentifizierung von Nutzern.

### Funktionsweise

#### Beispiel Postdienst

Das Internet ist kein einzelnes physikalisches Netz, sondern stellt einen Dienst für die Übermittlung von IP-Paketen in einem weltweiten Verbund unterschiedlicher physikalischer Übermittlungsnetze dar. Logisch gesehen stellt das Internet eine Nachbildung des weltweiten Briefpostdienstes dar, wobei ein IP-Paket einem Brief und eine IP-Adresse einer postalischen Adresse entspricht. Der Postdienst baut auf einer Vernetzung von Postleitzahlgebieten auf. Das Internet demgegenüber stellt eine Vernetzung von IP-Subnetzen dar. Somit würde ein IP-Subnetz einem Postleitzahlgebiet entsprechen. Auch beim Postdienst findet eine Unterstützung von Mobilität statt. Sie besteht darin, dass ein Brief nach dem Umzug eines Adressaten an dessen neue Adresse – als **Nachsendeadresse** bezeichnet – nachgeschickt werden kann (Bild 2). Diese Unterstützung der Mobilität beim Postdienst lässt sich folgendermaßen zusammenfassen:

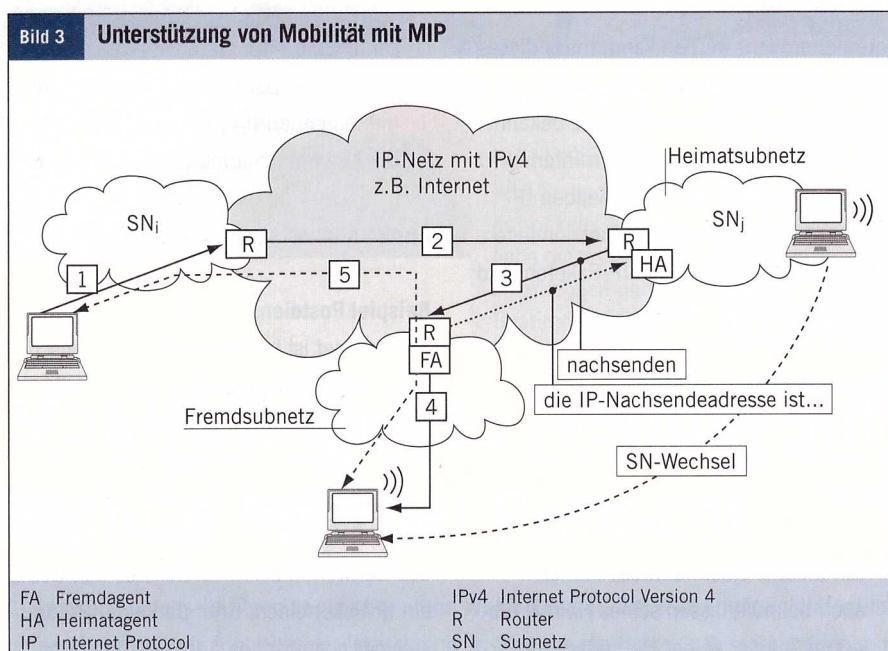
<sup>1</sup> Siehe hierzu den Beitrag „Subnetzmasken – Grundlage für das Subnetting“, WissenHeute 9/2007, S. 15 ff.



wird als **HoA** bezeichnet. Hat ein mobiler Rechner sein Heimatsubnetz verlassen und hält sich aktuell in einem Fremdsubnetz auf, müssen die für ihn ankommenden IP-Pakete in das Fremdsubnetz geschickt werden. Dies entspricht der Nachsendung von Briefen beim Postdienst. In Bild 3 ist das Prinzip der Mobilität nach dem MIP dargestellt.

Beim MIP werden zwei Funktionsmodule, die sogenannten **Mobility Agents**, für die „Betreuung“ von mobilen Rechnern definiert. Ein Mobility Agent kann

- Heimatagent (HA, Home Agent) oder
- Fremdagent (FA, Foreign Agent)



sein. Ein HA wird in der Regel als Funktionsmodul auf einem Router am Internetzugang im Heimatsubnetz installiert. Er wird vom mobilen Rechner immer darüber informiert, in welchem Fremdsubnetz sich dieser aktuell aufhält. Der HA leitet dann die im Heimatsubnetz ankommenden und an den mobilen Rechner adressierten IP-Pakete in dieses Fremdsubnetz um.

Der Mobility Agent in einem Subnetz, der für alle mobilen Gastrechner in diesem Subnetz zuständig ist, wird als FA bezeichnet. Wie ein HA wird ein FA in der Regel als Funktionsmodul auf einem Router am Internetzugang installiert.

Wie in Bild 3 dargestellt ist, unterscheidet MIP folgende Schritte im Verlauf der Kommunikation zwischen einem stationären und einem mobilen Rechner:

Ein IP-Paket, das an einen mobilen Rechner im Subnetz SN<sub>j</sub> adressiert ist, wird an den Router des Quellrechners im Subnetz SN<sub>i</sub> übermittelt (1). Das IP-Paket wird vom Subnetz SN<sub>i</sub> an das Heimatsubnetz SN<sub>j</sub> des Zielrechners übermittelt (2). Der mobile Zielrechner hat sein Heimatsubnetz aber verlassen. Daher müssen die an ihn adressierten IP-Pakete in das Fremdsubnetz, in dem er sich als Gastrechner gerade aufhält, weitergeleitet werden. Um dies zu ermöglichen, wird im Fremdsubnetz dem mobilen Gastrechner eine vorläufige IP-Adresse zugewie-

Der Brief wird an eine Briefverteilungsstelle übergeben (1). Der Brief wird von der Briefverteilungsstelle im Postleitzahlgebiet des Absenders an die Briefverteilungsstelle (an das Postamt) des Adressaten übermittelt (2). Der Adressat hat sein Postleitzahlgebiet zwar verlassen und ist unter einer neuen Adresse zu erreichen, hat aber dem Postamt in seinem „alten“ Postleitzahlgebiet eine Nachsendeadresse mitgeteilt. Der Brief wird an die Briefverteilungsstelle des Postleitzahlgebiets aus der Nachsendeadresse transportiert (3). Der Brief wird an die Nachsendeadresse übergeben (4). Es kann danach ein direkter Briefaustausch zwischen Adressat und Absender stattfinden (5).

Die Unterstützung von Mobilität in IP-Netzen mit dem MIP arbeitet nach dem gleichen Prinzip, und es werden ähnliche Schritte unternommen, wobei allerdings zwischen dem MIPv4 und dem MIPv6 zu unterscheiden ist.

#### Konzept von MIPv4

Die Art und Weise der Unterstützung von Mobilität in Netzen mit dem Internetprotokoll IPv4 beschreibt MIPv4 – kurz MIP. Das grundlegende Konzept des MIP wird in den Internetstandards der IETF als RFC 3344 und RFC 4721 spezifiziert.

Die IP-Adresse eines Rechners in seinem Heimatsubnetz ist seine **Heimatadresse** und

sen, um ihn innerhalb dieses Fremdsubnetzes zu lokalisieren. Diese Adresse wird als **CoA** bezeichnet und stellt eine **Nachsende-IP-Adresse** dar. Die CoA des Gastrechners ist auch dem FA bekannt und dieser übermittelt sie an den HA im Heimatsubnetz des Gastrechners. Auf diesem Weg wird die CoA auch dem HA als Nachsendeadresse bekannt gemacht. Das IP-Paket wird vom HA an die CoA weitergeleitet (3). Das IP-Paket wird im Fremdsubnetz an den betreffenden Gastrechner übermittelt (4). Zwischen den beiden Rechnern kann – allerdings nur über den FA – eine Kommunikation stattfinden (5).

### Vergleich von HoA und CoA

Die **HoA** eines mobilen Rechners ist die IP-Adresse, unter der dieser seinen Kommunikationspartnern bekannt ist. Sie wurde ihm in seinem Heimatsubnetz zugeordnet und bleibt auch dann erhalten, wenn der mobile Rechner das Heimatsubnetz verlassen hat und in ein Fremdsubnetz hereingegangen ist oder sich von einem Fremdsubnetz in ein anderes Fremdsubnetz hinein bewegt hat.

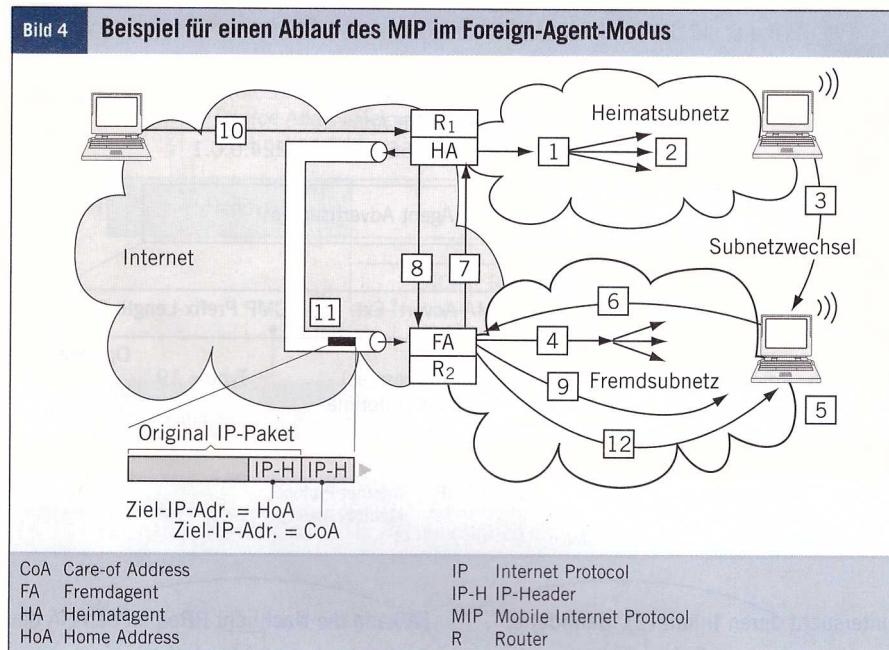
Die Subnetz-ID der HoA ist mit der Subnetz-ID, die stationäre Rechner und Router im Heimatsubnetz des mobilen Rechners besitzen, identisch.

Die **CoA** ist eine IP-Adresse, die ein mobiler Rechner nur dann benutzt, wenn er ein Fremdsubnetz besucht. Die CoA ist somit die IP-Adresse, an die alle an die HoA des mobilen Rechners gerichteten Pakete in ein Fremdsubnetz umgeleitet werden. Daher stellt die CoA eine Nachsende-IP-Adresse dar, die sich immer dann ändert, wenn der mobile Rechner zwischen Fremdsubnetzen wechselt.

### Funktionen des MIP

Für die Unterstützung der Mobilität in IP-Netzen stellt das MIP folgende Funktionen zur Verfügung:

**Agent Discovery:** Dies ist die Nutzung eines Agenten, um feststellen zu können, ob ein Subnetzwechsel stattgefunden hat.



**Registrierung:** Dies ist die Eintragung der aktuellen Nachsende-IP-Adresse eines mobilen Rechners beim HA, damit dieser die ankommenden Pakete in das Fremdsubnetz nachsenden kann, in dem sich der mobile Rechner aktuell aufhält.

**MIP-Routing:** Dies ist das Prinzip, nach dem Pakete an einen mobilen Rechner und von einem mobilen Rechner über mehrere Subnetze übermittelt werden können.

### Betriebsarten von MIPv4

Beim MIP sind zwei Betriebsarten (Modi) zu unterscheiden:

#### ■ Foreign-Agent-Modus:

In diesem Modus ist ein FA im Fremdsubnetz vorhanden und die CoA stellt die IP-Adresse des FA dar. Alle Gastrechner, die sich im Subnetz dieses Agenten aufhalten, nutzen die gleiche CoA als Nachsendeadresse. Somit verweist die CoA auf die aktuelle Zugehörigkeit des mobilen Rechners zu einem Subnetz hin.

#### ■ Colocated-Modus:

In diesem Modus ist im Subnetz, in dem sich ein mobiler Rechner als Gast aufhält, kein FA vorhanden. Jedem Gastrechner in diesem Fremdsubnetz wird nach Bedarf mithilfe des Protokolls

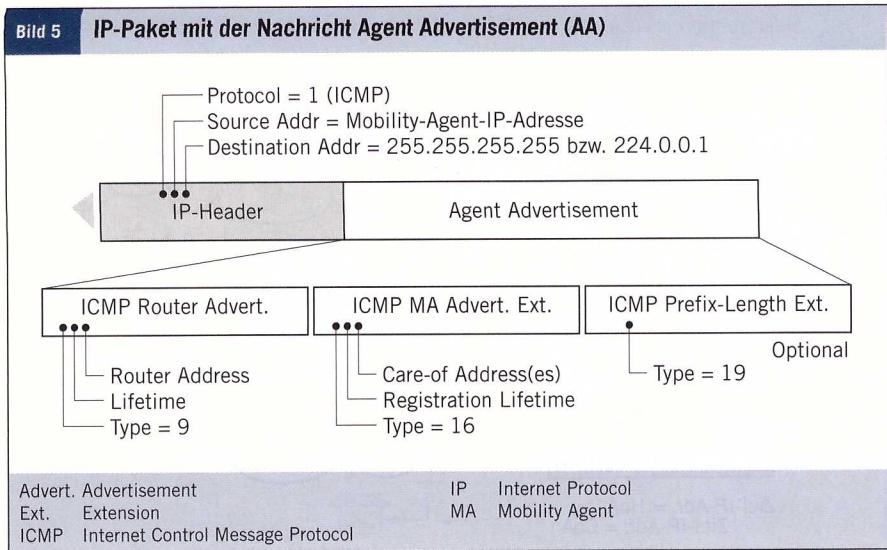
DHCP eine eindeutige CoA zugewiesen. In diesem Fall wird die CoA als **Colocated CoA** bezeichnet.

### Beispiel für einen Ablauf des MIP

Folgende Schritte lassen sich beim Ablauf (Bild 4) des MIP unterscheiden:

Zunächst befindet sich der mobile Rechner in seinem Heimatsubnetz, das über den Router R<sub>1</sub> mit dem Internet verbunden ist. Der in diesem Router untergebrachte HA zeigt seine Präsenz an (1), indem er periodisch die Nachricht AA als IP-Broadcast oder -Multicast sendet (Bild 5). In der Nachricht AA ist das Subnetz, in dem dieser HA positioniert ist, angegeben. Somit kann jeder mobile Rechner, der in diesem Subnetz beheimatet ist, durch die Auswertung von AA feststellen, ob er sein Heimatsubnetz verlassen hat. Auf dem gleichen Weg kann jeder mobile Rechner, der sich in diesem Subnetz nur als Gast aufhält, feststellen, ob ein Subnetzwechsel stattgefunden hat. Die Prinzipien, nach denen ein mobiler Rechner das Verlassen seines Heimatsubnetzes oder einen Subnetzwechsel erkennen kann, werden im Weiteren erklärt.

Um festzustellen, ob er sich im Heimatsubnetz oder in einem Fremdsubnetz befindet, hört der mobile Rechner ständig AAs ab und



untersucht deren Inhalt (2). Befindet er sich im Heimatsubnetz, verhält er sich so wie jeder stationäre Rechner und macht keinen Gebrauch von der MIP-Funktion.

„Wandert“ der mobile Rechner im IP-Netz und hat sein Heimatsubnetz bereits verlassen (3), dann befindet er sich in einem Fremdsubnetz und ist dort ein Gastrechner. Dies muss er aber selbst feststellen und dementsprechend dem HA im Router  $R_1$  am Zugang zu seinem Heimatsubnetz seinen Standort mitteilen.

Der Mobility Agent im Fremdsubnetz, der als FA für den Gastrechner gilt, sendet ebenfalls periodisch die Nachricht AA (4).

Der Gastrechner hört die Nachricht AA im Fremdsubnetz wie im Heimatsubnetz ab und untersucht deren Inhalt (5). So erkennt er, dass er sich in einem Fremdsubnetz befindet. Die IP-Adresse des Fremdagentsen (also die CoA) dient ihm übergangsweise als seine vorläufige IP-Adresse im Fremdsubnetz. Der mobile Rechner muss dann beim FA verlassen, dass die CoA bei seinem Heimatagenten HA als seine Nachsendeadresse registriert wird. Der HA erhält damit Informationen darüber, in welches Fremdsubnetz er die Datenpakete nachsenden muss.

Der Gastrechner sendet an den FA die Nachricht RReq (6). Diese Nachricht (s. Bild 10) enthält die IP-Adresse des HA im Heimatsubnetz des mobilen Gastrechners, und der

FA kann die Nachricht RReq an den HA des Gastrechners weiterleiten.

Der FA leitet die Nachricht RReq mit der CoA als Nachsendeadresse an den HA weiter (7). Nach dem Empfang von RReq ist dem HA damit der Standort des mobilen Rechners bekannt. Er weiß aufgrund der CoA, an welchen FA er die im Heimatsubnetz eintreffenden und an den mobilen Rechner adressierten IP-Pakete weiterleiten muss.

Der HA des mobilen Rechners antwortet dem FA mit der Nachricht RRep (8).

Nach dem Eintreffen der Nachricht RRep beim FA wird diese vom FA an den mobilen Gastrechner weitergeleitet, um diesem die Registrierung seiner CoA beim HA zu bestätigen (9).

Ein stationärer Rechner am Internet hat ein IP-Paket an den mobilen Rechner abgeschickt (10). Da dieser mobile Rechner im IP-Netz weiterhin unter seiner HoA bekannt ist, wird dieses IP-Paket in sein Heimatsubnetz übermittelt. Die an ihn adressierten IP-Pakete werden vom HA auch dann weiter empfangen, wenn der mobile Rechner das Heimatsubnetz verlassen hat. Der HA verfügt über eine Liste mit Angaben darüber, welche Rechner sein Subnetz – und folglich ihr Heimatsubnetz – verlassen haben und in welchen Fremdsubnetzen sie sich aktuell befinden. Diese Liste stellt eine Tabelle mit

den Zuordnungen „Heimatadresse → Nachsendeadresse“ also mit „HoA → CoA“ dar. Sie wird auch als **Mobility Binding Table** (s. Abs. Registrierung beim Heimatagenten) bezeichnet. Das an die Heimatadresse gesendete IP-Paket wird vom HA in ein neues IP-Paket eingekapselt (11), was als **IP-in-IP-Encapsulation** bezeichnet wird, und an den FA des aktuellen Fremdsubnetzes geschickt. Dabei wird das Originalpaket in ein äußeres IP-Paket „eingekapselt“, wobei die Ziel-IP-Adresse im äußeren IP-Header die CoA des mobilen Rechners darstellt. Da die CoA in diesem Fall die IP-Adresse des FA ist, entsteht logisch gesehen ein **Tunnel** zwischen HA und FA. Der HA kann aber nicht erkennen, ob der mobile Rechner im Fremdsubnetz selbst oder der FA der Endpunkt des Tunnels ist.

Das vom FA über den Tunnel empfangene IP-Paket wird an den mobilen Gastrechner ausgeliefert (12). Da sich der mobile Rechner und der FA im gleichen Subnetz befinden, werden die IP-Pakete vom FA direkt an den mobilen Gastrechner gesendet: In Link-Layer-Frames an die Link-Layer-Adresse des Gastrechners, beispielsweise in einem LAN in MAC-Frames an seine MAC-Adresse.

## Agent Discovery beim MIP

Als Agent Discovery wird der Prozess bezeichnet, bei dem ein mobiler Rechner erkennen möchte, ob er sich in seinem Heimatsubnetz oder in einem Fremdsubnetz aufhält und ob er sich gerade von einem Fremdsubnetz in ein anderes Fremdsubnetz hineinbewegt hat. Dieser Prozess ermöglicht es, jeden Subnetzwechsel eines mobilen Rechners zu erkennen. Mithilfe von Agent Discovery können folgende Fälle entdeckt werden:

- Ein mobiler Rechner hat sein Heimatsubnetz verlassen und hält sich als Guest in einem Fremdsubnetz auf.
- Ein mobiler Gastrechner hat sich von einem Fremdsubnetz in ein anderes Fremdsubnetz hineinbewegt.
- Ein mobiler Rechner ist in sein Heimatsubnetz zurückgekehrt.

Diese Fälle müssen entsprechend beim HA des mobilen Rechners registriert werden.

Um Agent Discovery zu nutzen, sendet jeder Mobility Agent (HA und/oder FA) periodisch, und nur in sein Subnetz, die Nachricht AA (s. Bild 5) mit der Ziel-IP-Adresse entweder als Multicast-Adresse 224.0.0.1 (All systems on this link) oder als Broadcast-Adresse 255.255.255.255 (Limited Broadcast). Die Nachricht AA wird nicht in andere Subnetze weitergeleitet. Wie in Bild 5 dargestellt ist, setzt sich die Nachricht AA aus mehreren Nachrichten des Protokolls ICMP zusammen. Hierzu gehören die folgenden Nachrichten:

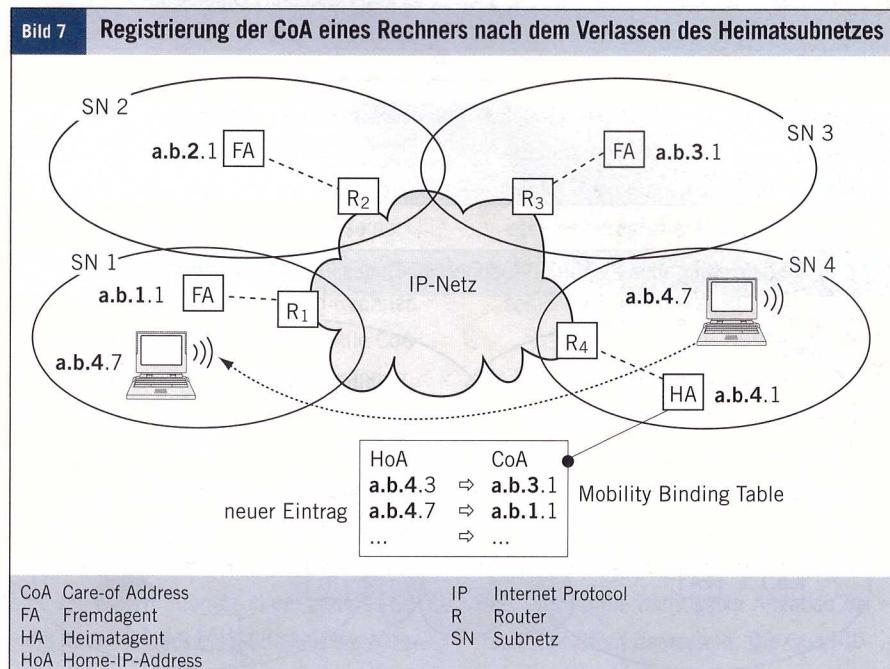
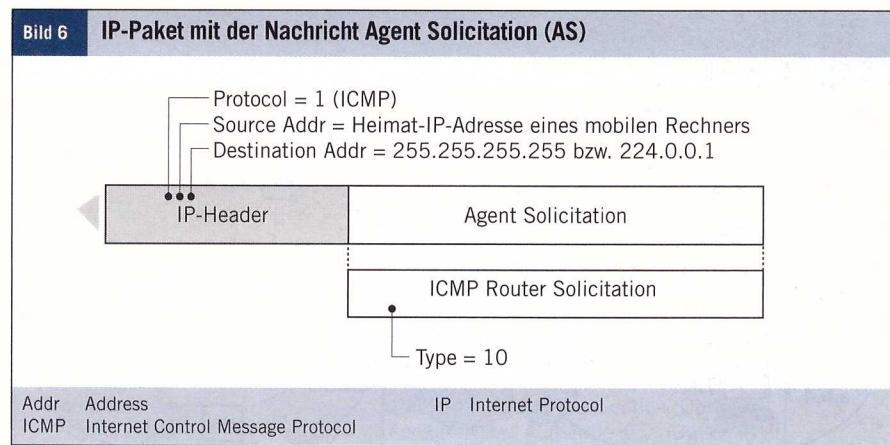
- ICMP Router Advertisement mit den IP-Adressen der Router
- Mobility Agent Advertisement mit der CoA und der Gültigkeitsdauer der Registrierung (Registration Lifetime)
- Prefix-Length Extension nach Bedarf mit der Länge des Präfixes einer CoA

Alternativ zum periodischen Aussenden kann AA auch direkt von einem mobilen Rechner angefordert werden. Hierfür sendet ein mobiler Rechner die Nachricht AS, also **Agent Solicitation**. Wie in Bild 6 dargestellt ist, entspricht die Nachricht AS der ICMP-Nachricht Router Solicitation. Jeder Mobility Agent antwortet direkt nach Empfang von AS mit einem AA. Ein mobiler Rechner sendet AS, wenn er keine „Geduld“ hat, auf die nächste periodische Übermittlung von AA zu warten oder weil er schnell von Subnetz zu Subnetz wechselt.

#### Erkennen, dass das Heimatsubnetz verlassen wurde

Anhand der Angaben in den Agent Advertisements, die die Mobility Agents gesendet haben, kann der mobile Rechner erkennen, ob er sich in seinem Heimatsubnetz oder in einem Fremdssubnetz aufhält (s. Bild 4). Dies geschieht nach der folgenden Regel:

- Ist die Subnetz-ID in der CoA **gleich** der Subnetz-ID der Heimat-IP-Adresse, hält sich der mobile Rechner im Heimatsubnetz auf.



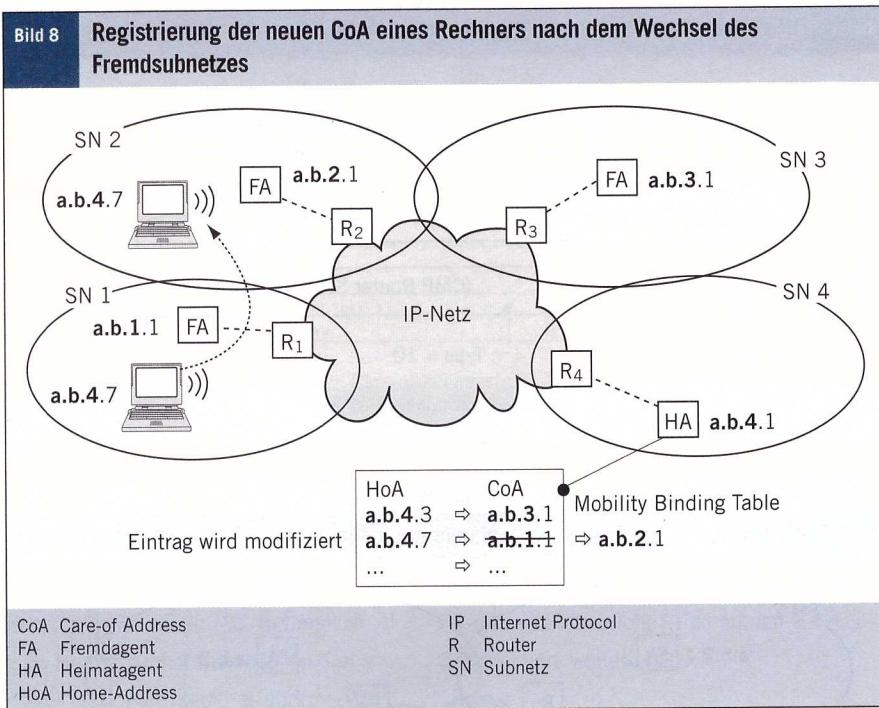
- Ist die Subnetz-ID in der CoA **nicht gleich** der Subnetz-ID der Heimat-IP-Adresse, hält sich der mobile Rechner in einem Fremdssubnetz auf.

Falls sich ein mobiler Rechner in einem Fremdssubnetz aufhält, sind weitere zwei Fälle zu unterscheiden:

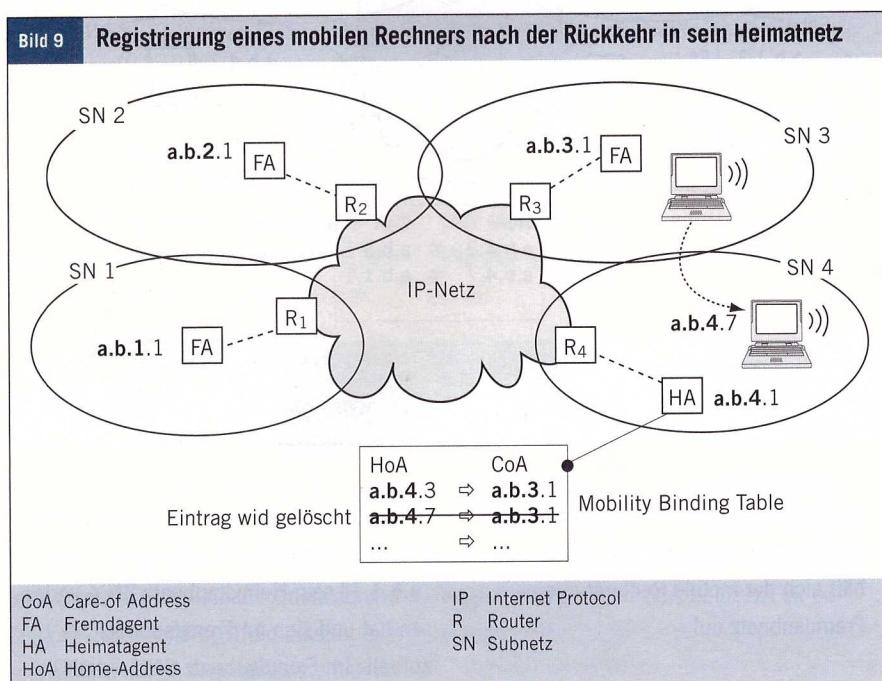
- Es hat **kein Subnetzwechsel** stattgefunden: Der mobile Rechner hält sich im Fremdssubnetz auf und dies wurde seinem Heimatagenten bereits mitgeteilt.
- Ein Subnetzwechsel hat stattgefunden: Der mobile Rechner hat gerade sein Heimatsubnetz verlassen oder sich aus einem Fremdssubnetz in ein anderes hineinbewegt. Dieser Subnetzwechsel wurde dem Heimatagenten noch nicht mitgeteilt.

In Bild 7 ist als Beispiel der Fall dargestellt, dass der mobile Rechner mit seiner HoA „a.b.4.7“ sein Heimatsubnetz SN 4 verlassen hat und sich im Fremdssubnetz SN 1 aufhält. Im Fremdssubnetz SN 1 erhält er eine CoA als Nachsendeadresse und teilt diese seinem Heimatagenten mit. Dies wird als **Registrierung der CoA** bezeichnet.

Der Heimatagent muss die vorläufige CoA des mobilen Rechners kennen, damit er die in seinem Heimatsubnetz ankommenden IP-Pakete, die die HoA für den mobilen Rechner aufweisen, an die CoA in das Fremdssubnetz weiterleiten kann. Der Heimatagent dient so als Weiterleitungsinstanz für alle IP-Pakete, die an mobile Rechner adressiert sind, die sich aktuell in Fremdsnetzen aufhalten.



in ein anderes Fremdsubnetz dargestellt. Um eine solche Situation zu erkennen, muss der mobile Rechner feststellen, ob er die letzten zwei aufeinanderfolgenden Nachrichten AA entweder im gleichen Subnetz oder in verschiedenen Subnetzen empfangen hat, ob also die letzten zwei aufeinanderfolgenden AAs vom Fremdagente des gleichen Subnetzes stammen. Dies lässt sich entweder über einen Vergleich der Subnetz-IDs oder anhand der Angabe Lifetime im ICMP Router Advertisement feststellen. Die Zeitdauer Lifetime gibt an, wann der mobile Rechner spätestens das nächste AA seitens eines gleichen Agenten empfangen sollte.



Innerhalb der Lifetime werden in der Regel mehrere AAs gesendet. Erhält ein mobiler Rechner innerhalb der Lifetime kein neues AA desselben Agenten, so kann er annehmen, dass er das Subnetz dieses Agenten verlassen hat. In diesem Fall ändert sich die CoA des mobilen Rechners und muss dem Heimatagenten mitgeteilt werden. Bei der Registrierung wird dann der entsprechende Eintrag in der Mobility-Binding-Tabelle des Heimatagenten angepasst.

Besucht der mobile Rechner nach wie vor das gleiche Subnetz, so ist keine neue Registrierung notwendig, solange die vorhergehende noch nicht abgelaufen ist. Wie lange die Registrierung bei einem Heimatagenten gültig ist, wird in seinen Advertisements als Registration Lifetime angegeben (s. Bild 5).

In einem Fremdsubnetz besteht aber auch die Möglichkeit, dass es dort keinen Mobility Agent gibt. Hat ein Subnetzwechsel stattgefunden und ein mobiler Rechner hat sich aus einem Fremdsubnetz in ein anderes Fremdsubnetz bewegt, in welchem es keinen Mobility Agent gibt, dann bekommt er keine AAs mehr. In diesem Fall nimmt der mobile Rechner zunächst an, dass er sich im Heimatsubnetz befindet und sein Heimatagent zurzeit gestört ist. Folglich versucht er, die von ihm abgehenden IP-Pakete an den Default-Router<sup>2</sup> in seinem Heimatsubnetz

In Bild 7 ist im Subnetz SN 1 ein Mobility Agent dargestellt, der für den Gastrechner einen Fremdagente darstellt. Die CoA des Gastrechners ist die IP-Adresse des Fremdagents im SN 1. Durch die Registrierung beim Heimatagenten wird in der Mobility-Binding-Tabelle beim HA die Zuordnung: **a.b.4.7  $\rightarrow$  a.b.1.1** (HoA  $\rightarrow$  CoA) eingetragen. Damit können die mit der HoA **a.b.4.7** in das Heimatsubnetz SN 4 für den mobilen Rechner ankommenden IP-Pakete vom HA an seine CoA **a.b.1.1** im SN 1 weitergeleitet werden.

### Erkennen des Wechsels eines Fremdsubnetzes

Ein mobiler Rechner muss selbst feststellen können, ob ein Subnetzwechsel stattgefunden und er sich dabei aus einem Fremdsubnetz in ein anderes Fremdsubnetz hineinbewegt hat. In einem neuen Fremdsubnetz ist er als Gastrechner unter einer anderen Nachsendeadresse CoA erreichbar, und diese muss er seinem Heimatagenten mitteilen.

Als Beispiel ist in Bild 8 die Bewegung eines mobilen Rechners aus einem Fremdsubnetz

<sup>2</sup> **Default-Router:** Der Router, der für einen Rechner in seinem Subnetz als Übergang in andere Subnetze dient.

zu senden. Falls dieser antwortet, hält sich der mobile Rechner höchstwahrscheinlich im Heimatsubnetz auf.

Ist dies aber nicht der Fall, dann kann der mobile Rechner annehmen, dass er sich in einem Fremdsubnetz befindet, in dem es keinen Mobility Agent gibt. Er versucht dann, von einem DHCP-Server im Fremdsubnetz eine vorläufige Nachsendeadresse CoA zu erhalten. War der Versuch erfolgreich, kann der mobile Rechner die so erhaltene Adresse (**Colocated CoA**) als seine Nachsendeadresse nutzen und sich beim Heimatagenten registrieren lassen.

### Erkennen der Rückkehr in das Heimatsubnetz

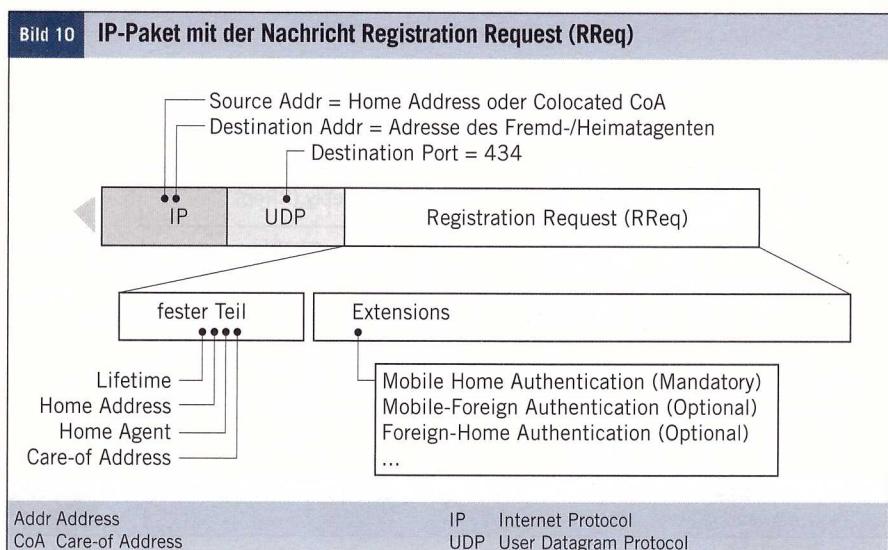
Ein mobiler Rechner muss selbst feststellen können, ob ein Subnetzwechsel stattgefunden hat und ob er dabei aus einem Fremdsubnetz in sein Heimatsubnetz zurückgekehrt ist (Bild 9). Ist das der Fall, muss er seinen Heimatagenten darüber informieren.

Um feststellen zu können, ob der mobile Rechner in ein Fremdsubnetz gewechselt hat oder in das Heimatsubnetz zurückgekehrt ist, vergleicht er die IP-Adresse des Absenders in von ihm empfangenen AAs mit der IP-Adresse des Heimatagenten. Sind beide identisch, ist er in sein Heimatsubnetz zurückgekehrt. In diesem Fall muss er dem Heimatagenten noch mitteilen, dass seine CoA als Nachsendeadresse keine Bedeutung mehr hat. Dieser Vorgang wird als **Deregistrierung** bezeichnet. Der mobile Rechner sollte in seinem Heimatsubnetz für alle Rechner unter seiner HoA erreichbar sein. Hierfür muss der betreffende Eintrag mit der Zuordnung HoA → CoA in der Mobility-Binding-Tabelle beim Heimatagenten dieses mobilen Rechners gelöscht werden. Von diesem Zeitpunkt an ist der mobile Rechner nur noch unter seiner HoA erreichbar.

### Registrierung beim Heimatagenten

#### Registrierung der HoA

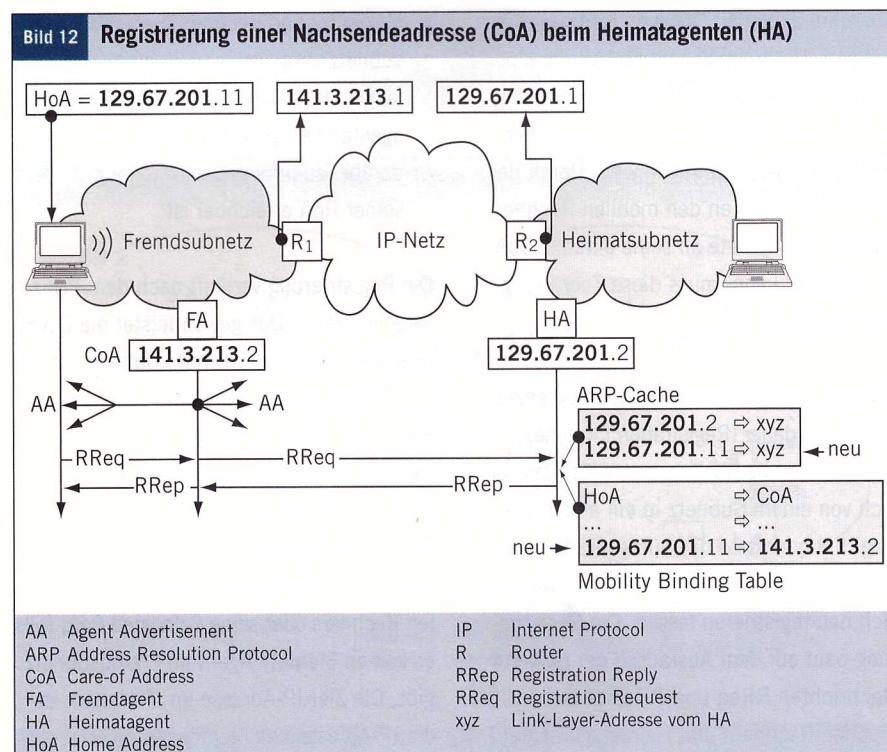
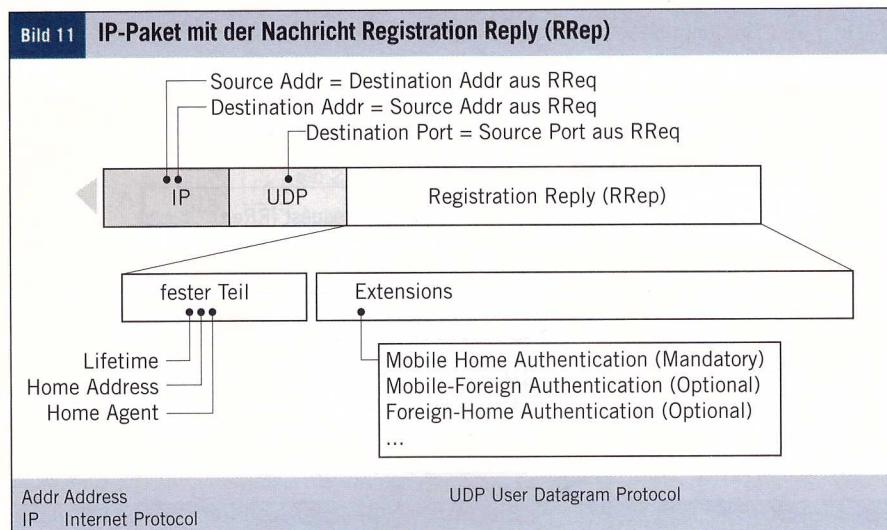
Durch die Registrierung werden die Heimatagenten über die aktuellen Standorte der von ihnen „betreuten“ mobilen Rechner, also



über ihre aktuellen Nachsendeadressen, informiert. Der Heimatagent enthält die Mobility-Binding-Tabelle, in der die Zuordnung der HoA des mobilen Rechners zu seiner aktuellen CoA eingetragen wird. Damit der Heimatagent die an den mobilen Rechner adressierten Pakete an seine aktuelle CoA weiterleiten kann, muss diese Zuordnung immer aktuell sein.

Jede Registrierung hat nur eine begrenzte Gültigkeitsdauer (Registration Lifetime). Sobald der mobile Rechner entdeckt, dass er sich von einem Subnetz in ein anderes bewegt hat oder dass die Gültigkeit der aktuellen Registrierung abgelaufen ist, muss er sich neu registrieren lassen. Die Registrierung baut auf dem Austausch der beiden Nachrichten RReq und RRep zwischen mobilen Rechnern und Heimatagenten auf, gegebenenfalls unter Beteiligung von Fremdagagenten. Ein mobiler Rechner muss beim Heimatagenten jeden bei ihm stattgefundenen Subnetzwechsel registrieren lassen:

- Hat sich der mobile Rechner in ein fremdes Subnetz hineinbewegt, dies soeben erkannt und bereits eine Nachsendeadresse in diesem neuen Fremdsubnetz erhalten, dann muss er den Heimatagenten über seine neue CoA informieren, also diese neue CoA bei ihm registrieren lassen. Hierbei kann es sich entweder um die CoA eines Fremdagagenten oder um eine Colocated CoA handeln.
  - Ist der mobile Rechner in sein Heimatsubnetz zurückgekehrt und hat dies erkannt, dann muss er sich beim Heimatagenten deregistrieren lassen, um diesen darüber zu informieren, dass er nur unter seiner HoA erreichbar ist.
- Die Registrierung verläuft nach dem Prinzip Request/Reply. Das gewährleistet die Zuverlässigkeit der Übermittlung. Daher kann für den Transport der Nachrichten RReq und RRep das verbindungslose und unzuverlässige Protokoll UDP verwendet werden. In Bild 10 sind die wichtigsten Angaben der Nachricht RReq dargestellt. Die Quell-IP-Adresse im IP-Header ist die HoA des mobilen Rechners oder seine Colocated CoA, falls es keinen Mobility Agent im Fremdsubnetz gibt. Die Ziel-IP-Adresse im IP-Header ist die IP-Adresse des Fremdagagenten oder des Heimatagenten, falls die vorläufige IP-Adresse des mobilen Rechners eine Colocated CoA ist. Jede Nachricht RReq enthält einen festen Teil mit einer konstanten Länge (Fixed-Length Portion). Sie kann aber auch einen Teil mit einer variablen Länge enthalten, in dem nach Bedarf bestimmte zusätzliche Angaben, die sogenannten Extensions, übermittelt werden können. In RReq sind unter anderem folgende Angaben enthalten:
- Lifetime: Gültigkeitsdauer der Registrierung
  - HoA: Heimat-IP-Adresse des mobilen Rechners



- Home Agent: IP-Adresse des Heimatagenten
- CoA: IP-Adresse des Fremdagents und/oder Colocated CoA

In Bild 11 ist ein IP-Paket mit der Nachricht RRep dargestellt. Sie enthält unter anderem folgende Angaben: Lifetime, HoA und Home Agent. Diese Angaben haben die gleiche Bedeutung wie in der Nachricht RReq.

#### Registrierung einer CoA

Die Registrierung einer CoA beim Heimatagenten ist in Bild 12 dargestellt: Hat ein

mobile Rechner nach dem Empfang einer Nachricht AA erkannt, dass er sich in einem neuen Fremdsubnetz befindet und folglich eine neue CoA hat, muss er die CoA beim Heimatagenten registrieren lassen. Um die Registrierung zu initiieren, sendet er die Nachricht RReq. Da hier ein Fremdagente vorhanden ist, wird RReq zunächst an diesen geschickt und von ihm an den Heimatagenten weitergeleitet. Die IP-Adresse des Fremdagents ist dem mobilen Rechner bereits aus der von ihm empfangenen Nachricht AA bekannt. Der Heimatagent prüft nach dem Empfang einer Nachricht RReq zunächst

ihre Gültigkeit mit der Angabe Lifetime. Ist Lifetime nicht gleich Null, die Gültigkeit also noch nicht abgelaufen, trägt der Heimatagent folgende Zuordnungen ein:

- im ARP-Cache: Zuordnung der HoA des mobilen Rechners zu der Link-Layer-Adresse xyz des HA (HoA → xyz)
- in der Mobility-Binding-Tabelle: Zuordnung der HoA des mobilen Rechners zu der IP-Adresse des FA

Dadurch werden die von allen Rechnern im Heimatsubnetz an die HoA des mobilen Rechners adressierten Pakete zuerst an den Heimatagenten im Router gesendet (Eintrag im ARP-Cache) und danach vom Heimatagenten an diese CoA weitergeleitet (Eintrag in der Mobility-Binding-Tabelle). Ist Lifetime in RReq gleich Null, so wird diese Nachricht als DRRq interpretiert. Hat der Heimatagent einen RReq mit Lifetime nicht gleich Null empfangen, trägt er in seinem ARP-Cache und in seiner Mobility-Binding-Tabelle die entsprechenden Zuordnungen ein und sendet eine Nachricht RRep zurück, um mitzuteilen, dass die Registrierung erfolgreich war. Die Nachricht RRep nimmt den umgekehrten Weg wie RReq. Wenn der mobile Rechner in einer vorgegebenen Zeit kein RRep erhält oder die Registrierung ungültig war, sendet er RReq erneut.

#### Registrierung einer Colocated CoA

Die Registrierung einer Colocated CoA – also einer Nachsendeadresse in einem Fremdsubnetz ohne FA – beim Heimatagenten ist in Bild 13 dargestellt: Hat ein mobiler Rechner erkannt, dass er sich in einem neuen Fremdsubnetz befindet, in dem es keinen Mobility Agent gibt, kann er sich vom DHCP-Server eine vorläufige IP-Adresse ausleihen. Diese IP-Adresse (Colocated CoA), muss er dem Heimatagenten mitteilen. Da kein FA vorhanden ist, wird die Nachricht RReq direkt an den Heimatagenten geschickt. Hat der Heimatagent den RReq empfangen, trägt er folgende Zuordnungen ein:

- im ARP-Cache: Zuordnung der HoA des mobilen Rechners zu der Link-Layer-Adresse xyz des HA (HoA → xyz)

- in der Mobility-Binding-Tabelle:  
Zuordnung der HoA des mobilen Rechners zu seiner Colocated CoA

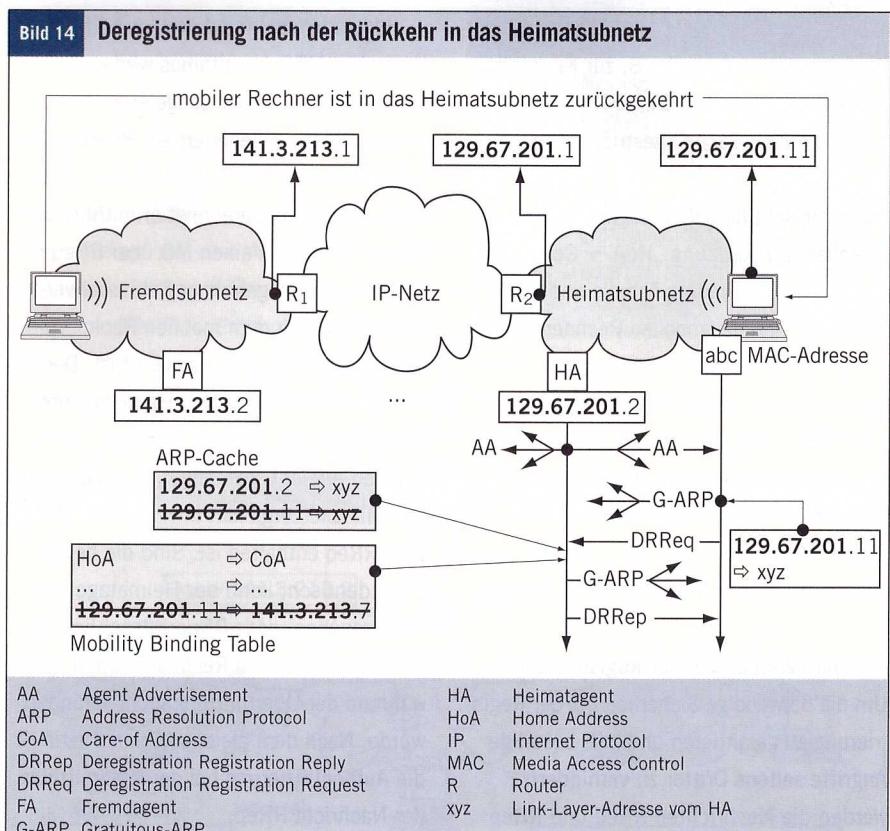
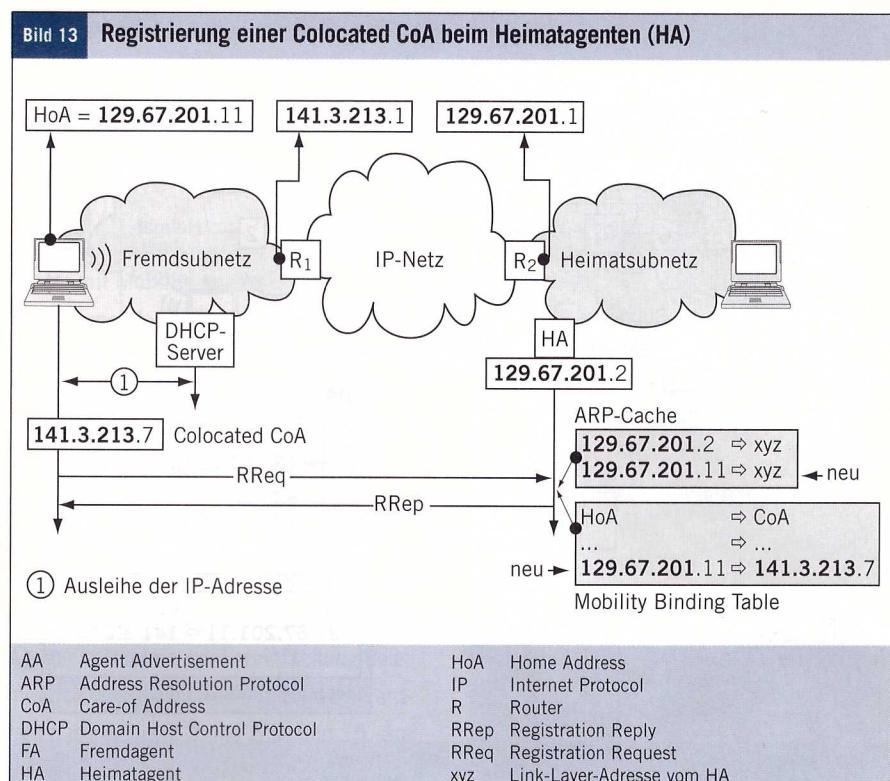
Danach sendet er eine Nachricht RRep an den mobilen Rechner zurück, um diesem mitzuteilen, dass die Registrierung erfolgreich war.

### Deregistrierung beim Heimatagenten

Ist ein mobiler Rechner in sein Heimatsubnetz zurückgekehrt und hat dies anhand der vom HA empfangenen Nachricht AA erkannt, muss er allen Rechnern in seinem Heimatsubnetz mitteilen, dass er im Heimatsubnetz erreichbar ist. Dies wird als **Deregistrierung** bezeichnet (Bild 14).

Ein mobiler Rechner, der in sein Heimatsubnetz zurückgekehrt ist, muss den anderen Rechnern in seinem Heimatsubnetz mitteilen, dass sie alle an seine HoA adressierten IP-Pakete direkt an ihn und nicht an den Heimatagenten senden sollen. Sie können die IP-Pakete in Link-Layer-Frames direkt an seine Link-Layer-Adresse (in LANs an seine MAC-Adresse) senden. Um dies zu erreichen, wird an alle Rechner im Heimatsubnetz eine Nachricht nach dem Protokoll ARP mit der Zuordnung: „seine HoA → seine Link-Layer-Adresse“ als Broadcast-Nachricht gesendet. Damit können sich alle Rechner im Heimatsubnetz des mobilen Rechners seine Link-Layer-Adresse – in einem LAN wäre es seine MAC-Adresse – eintragen, um die IP-Pakete daraufhin direkt an ihn senden zu können. Die dargestellte Vorgehensweise bedeutet aber eine Modifikation des Protokolls ARP und wird daher als **Gratuitous ARP** bezeichnet. Ein mobiler Rechner muss somit während einer Deregistrierung dem Heimatagenten mitteilen, dass er aktuell nur noch unter seiner HoA – und nicht unter der CoA – erreichbar ist, und dass der Heimatagent die an ihn adressierten IP-Pakete nicht mehr an den Fremdagagenten senden soll, sondern direkt an ihn.

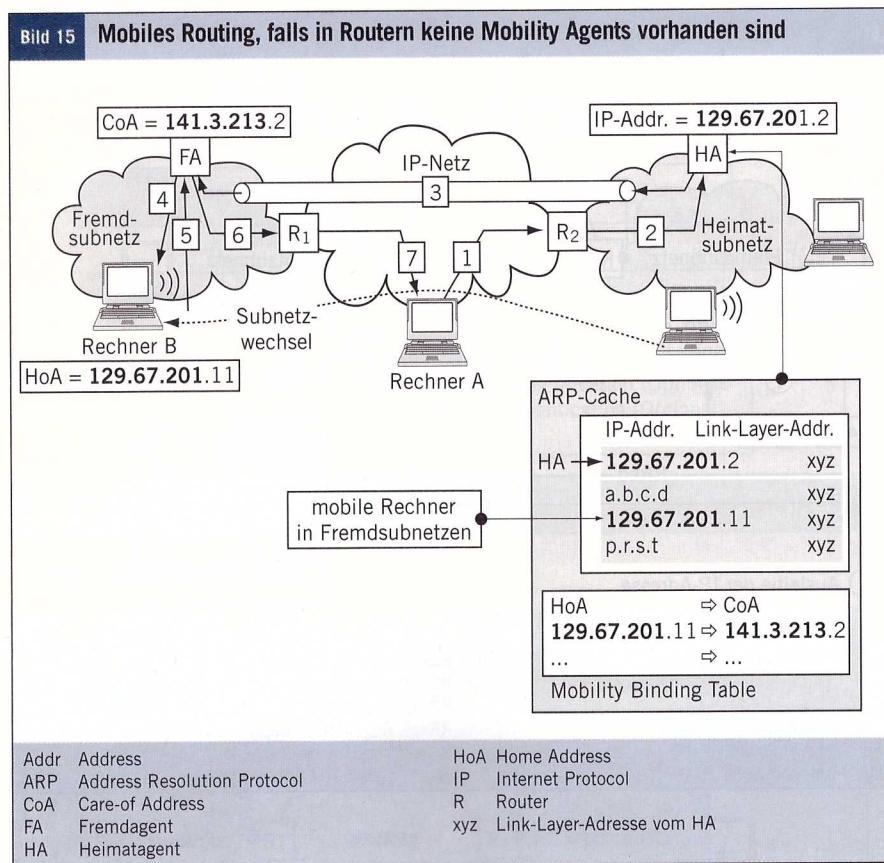
Hervorzuheben ist, dass die Nachricht RReq mit Lifetime Null als **DRReq** dient. Eine solche Nachricht wird vom mobilen Rechner



gesendet, um eine Deregistrierung beim Heimatagenten zu veranlassen.

Hat der Heimatagent DRReq empfangen, sendet er zuerst eine Nachricht nach dem

Protokoll Gratuitous ARP, um den anderen Rechnern in seinem Heimatsubnetz mitzuteilen, für welche Heimatadressen mobiler Rechner die IP-Pakete an ihn zum Weiterleiten gesendet werden sollen. Die anderen



Rechner nehmen damit z.B. zur Kenntnis, dass der Eintrag „**129.67.201.11 → xyz**“ in seinem ARP-Cache „gestrichen“ wurde.

Danach löscht der Heimatagent die entsprechende Zuordnung „HoA → CoA“ aus seiner Mobility-Binding-Tabelle und leitet die an die HoA des mobilen Rechners adressierten IP-Pakete nicht mehr an den Fremdagagenten weiter. Anschließend sendet er an den mobilen Rechner eine Nachricht RRep mit Lifetime Null zurück. Diese Nachricht wird als DRRep interpretiert. Nach der Deregistrierung ist der mobile Rechner nur noch unter seiner Heimatadresse erreichbar.

#### Authentifizierung bei der Registrierung

Um die notwendige Sicherheit bei der Registrierung zu garantieren und z.B. bösartige Angriffe seitens Dritter zu verhindern, werden die Nachrichten RReq und RRep authentifiziert. Insbesondere müssen die Nachrichten vor Angriffen Dritter geschützt werden, in denen die mobilen Rechner den Heimatagenten ihre aktuellen CoAs mitteilen. Zur Authentifizierung werden der MD5-Algorithmus und das Feld MHA in RReq und RRep verwendet.

Nach dem MD5-Algorithmus wird eine Prüfsumme MD mit fester Länge errechnet. Ein mobiler Rechner generiert ein RReq und füllt alle Felder, mit Ausnahme des Feldes MHA, aus. Dann berechnet er mithilfe des MD5-Algorithmus einen MD über RReq. Hierbei wird ein geheimer Schlüssel verwendet, der nur dem mobilen Rechner und seinem Heimatagenten bekannt ist. Der MD wird im Feld MHA an den Heimatagenten übermittelt. Hat die Nachricht den Heimatagenten erreicht, berechnet er seinen eigenen MD und vergleicht ihn mit dem, der in dem RReq enthalten ist. Sind die beiden MDs identisch, kann der Heimatagent davon ausgehen, dass RReq tatsächlich vom „richtigen“ mobilen Rechner stammt und während der Übermittlung nicht verändert wurde. Nach dem gleichen Prinzip verläuft die Authentifizierung bei der Übermittlung der Nachricht RRep.

#### Mobiles IP-Routing

##### Router ohne Mobility Agents

Das Routing von IP-Paketen zu einem mobilen Rechner, der sich in seinem Heimatnetz aufhält, unterliegt keinen speziellen Routing-

Regeln. Es funktioniert wie das klassische Routing von IP-Paketen zu einem beliebigen Rechner ohne Unterstützung von Mobilität. Ein modifiziertes Routing ist aber dann notwendig, wenn IP-Pakete an einen mobilen Rechner geschickt werden, der sich zu dem Zeitpunkt in einem Fremdsubnetz aufhält. In diesem Fall wird vom mobilen Routing gesprochen. Wenn die eingesetzten Router keine Mobility Agents aufweisen, läuft das mobile Routing nach dem in Bild 15 dargestellten Prinzip ab:

Sendet der Rechner A ein IP-Paket an die HoA des mobilen Rechners B, werden alle Pakete mit der HoA dieses Rechners als Zieladresse zum Router R<sub>2</sub> an der Grenze zu seinem Heimatsubnetz übermittelt (1). Der Router R<sub>2</sub> muss diese IP-Pakete an den Heimatagenten weiterleiten (2). Hierfür wird eine spezielle Lösung eingesetzt. Diese Lösung ist auch notwendig, damit alle Rechner aus dem Heimatsubnetz des mobilen Rechners, der sich aktuell in einem Fremdsubnetz aufhält, diesen im Fremdsubnetz erreichen können.

Da die an die HoA des mobilen Rechners gesendeten IP-Pakete nicht an den Heimatagenten des Heimatsubnetzes adressiert sind, kann er sie normalerweise nicht empfangen. Damit die IP-Pakete, die an die HoA eines mobilen Rechners, der sich gerade in einem Fremdsubnetz aufhält, adressiert sind, dennoch an den Heimatagenten übermittelt werden können, muss dieser die sogenannte **Proxy-ARP-Funktion** unterstützen: Die IP-Pakete aller mobilen Rechner eines Subnetzes, die sich in Fremdsubnetzen aufhalten, müssen an den Heimatagenten dieses Subnetzes übermittelt werden. Dies bedeutet, dass diese IP-Pakete in LL-Frames an die LL-Adresse des Heimatagenten (im LAN an seine MAC-Adresse) geschickt werden müssen. Der Heimatagent arbeitet so, als ob er der **Vertreter (Proxy)** aller mobilen Rechner wäre, die sich in Fremdsubnetzen aufhalten. Das ARP beim Heimatagenten muss daher die Proxy-ARP-Funktion unterstützen. Wie in Bild 15 dargestellt ist, enthält der ARP-Cache des Heimatagenten auch eine Tabelle mit der Zuordnung der

LL-Adresse des Heimatagenten zu den HoAs aller mobilen Rechner, die sich aktuell in Fremdsubnetzen aufhalten und bereits beim Heimatagenten registriert sind.

Weil der Router  $R_2$  für das Absenden eines IP-Paketes beispielsweise mit der Heimatadresse **129.67.201.11** die entsprechende LL-Adresse benötigt, sendet er eine Broadcast-Anfrage nach dem Protokoll ARP, um diese LL-Adresse zu ermitteln. Auf diese ARP-Anfrage reagiert der Heimatagent und sendet die ARP-Antwort mit der Zuordnung **129.67.201.11 → xyz** an den Router  $R_2$ . Dies führt dazu, dass das IP-Paket (s. Bild 15) direkt an den Heimatagenten gesendet wird (2), es wird also in einem LL-Frame mit der LL-Zieladresse xyz des Heimatagenten geschickt. Hat der Heimatagent das IP-Paket mit der Heimatadresse eines mobilen Rechners, der sich aktuell in einem Fremdsubnetz aufhält, empfangen, so nimmt er, wie bereits in Bild 4 dargestellt wurde, eine sogenannte **IP-in-IP-Encapsulation** vor. Hierbei wird das Original-IP-Paket in ein äußeres IP-Paket eingekapselt und im Header dieses äußeren Paketes wird die Nachsendeadresse CoA des mobilen Rechners als Zieladresse eingetragen. Das so eingekapselte Original-IP-Paket wird an die CoA gesendet. Dieser Vorgang wird als **Tunneling** bezeichnet. Dabei „tunnelt“ der Heimatagent das eingekapselte Original-IP-Paket an die CoA, ohne zu wissen, ob sich der mobile Rechner selbst oder ein Fremdagente am Ende des Tunnels befindet (3).

Im dargestellten Beispiel führt der Tunnel zum Fremdagente. Hier wird das Original-IP-Paket „ausgepackt“. Anhand der Ziel-IP-Adresse des inneren Original-IP-Paketes leitet der Fremdagente es an den mobilen Gastrechner weiter (4). Um aber das IP-Paket an einen mobilen Gastrechner senden zu können, muss der Fremdagente zuerst mithilfe des Protokolls ARP die LL-Adresse dieses Gastrechners abfragen. Der Fremdagente dient als Default-Gateway für alle mobilen Gastrechner, weil Gastrechner keinen „normalen“ Router im Fremdsubnetz kennen. Sollte der Zielrechner B eine Antwort an den Rechner A übermitteln, so über-

gibt er das entsprechende IP-Paket zuerst an den Fremdagente (5) und dieser sendet es dann an den Router  $R_1$  (6). Im weiteren Verlauf wird das IP-Paket nach den normalen Routing-Prinzipien zum Zielrechner A übermittelt (7).

### Router mit Mobility Agents

Um das mobile Routing vollständig erklären zu können, wurde in Bild 15 angenommen, dass die eingesetzten Router die Mobilität, also die Funktion von Mobility Agents, nicht unterstützen. Falls die Mobility Agents jedoch in den Routern untergebracht sind (Bild 16), ergeben sich einige Vorteile. Bei einem Vergleich der Bilder 15 und 16 zeigt sich, dass die Implementierung von Mobility Agents in Routern zur Vereinfachung des mobilen Routing führt. In diesem Fall entfallen die Schritte 2 und 6 in Bild 15. So mit verläuft die analysierte Übermittlung nur noch in fünf Schritten. Falls der Heimatagent im Router untergebracht ist, wird die Proxy-ARP-Funktion beim Heimatagenten nicht mehr benötigt.

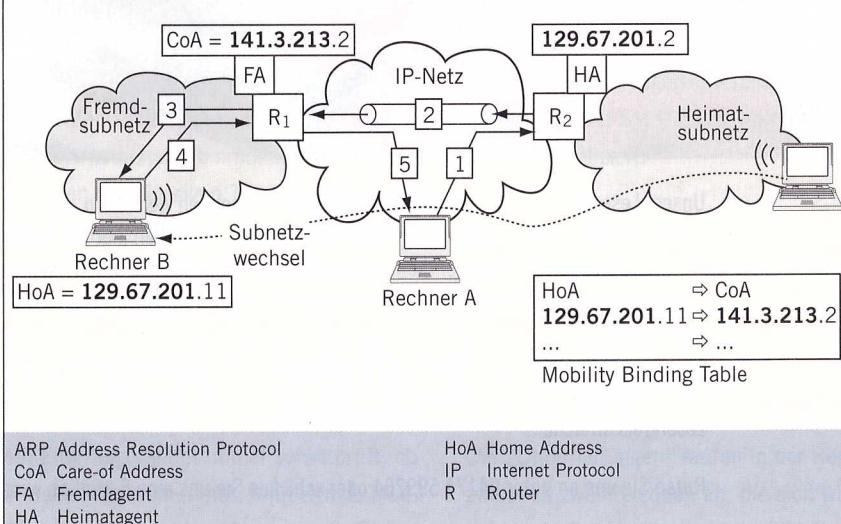
### Ausblick

Um die Mobilität von tragbaren Rechnern auch in Netzen mit dem IPv6 zu ermöglichen, wurde im Jahr 2004 als RFC 3775 das Protokoll MIPv6 veröffentlicht. Das Protokoll MIPv6 funktioniert anders als das MIPv4, beispielsweise verwendet es keine

### Verwendete Abkürzungen

AA	Agent Advertisement
ARP	Address Resolution Protocol
AS	Agent Solicitation
CoA	Care-of Address
DHCP	Dynamic Host Configuration Protocol
DRRq	Deregistration Request
FA	Foreign Agent
G-ARP	Gratuitous ARP
HA	Home Agent
HoA	Home Address
ICMP	Internet Control Message Protocol
ID	Identification
IETF	Internet Engineering Task Force
IP	Internet Protocol
LAN	Local Area Network
LL	Link Layer
MAC	Media Access Control
MD	Message Digest
MHA	Mobile Home Authentication
MIP	Mobile Internet Protocol
MIPv4	Mobile IPv4
RFC	Request for Comments
RRep	Registration Reply
RReq	Registration Request
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WLAN	Wireless Local Area Network

Bild 16 Mobiles Routing, falls in Routern Mobility Agents vorhanden sind



Fremdagente mehr. Es ist zu erwarten, dass in den nächsten Jahren fast alle Router im Internet in der Lage sein werden, die Funktionen von Mobility Agents zu unterstützen, also als Heimatagenten und Fremdagente zu arbeiten. Tragbare Rechner werden in Zukunft dann auch über eine entsprechende Software für die Unterstützung von Mobilität verfügen.

(Ar)

#### Literaturhinweise und Internetadressen

- Badach, Anatol; Hoffmann, Erwin: Technik der IP-Netze, TCP/IP inkl. IPv6. München: Carl Hanser Verlag, 2007.
- Perkins, Charles: Mobile IP; Design Principles and Practices. Massachusetts: Addison-Wesley Longman, 1998.
- Solomon, James: Mobile IP, The Internet Unplugged. New Jersey: Prentice Hall, 1998.
- [www.ietf.org/dyn/wg/charter/mip4-charter.html](http://www.ietf.org/dyn/wg/charter/mip4-charter.html)  
(entnommen am 15.11.2009)
- [www.mobileip.org](http://www.mobileip.org) (entnommen am 15.11.2009)
- [www.ietf.org/old/2009/ids.by.wg/mobileip.html](http://www.ietf.org/old/2009/ids.by.wg/mobileip.html)  
(entnommen am 15.11.2009)

- [www.networksorcery.com/enp/protocol/mobileip.htm](http://www.networksorcery.com/enp/protocol/mobileip.htm)  
(entnommen am 15.11.2009)
- [www.tcpipguide.com/free/t\\_InternetProtocolMobilitySupportMobileIP.htm](http://www.tcpipguide.com/free/t_InternetProtocolMobilitySupportMobileIP.htm) (entnommen am 15.11.2009)
- <http://docs.sun.com/app/docs/doc/816-4554/miptm-1?a=view> (entnommen am 15.11.2009)