Mobile Network Layer

Seminar Mobile Computing SS 2003

Ingmar Ickerott*
Matrikel-Nr. 908606

17. Juni 2003

Diese Arbeit erörtert die Spezifikation einer Erweiterung des Internet Protokolls (IP), die ein Routing von Datenpaketen zu mobilen Computern im Internet ermöglicht. Das als Mobile IP bezeichnete Protokoll sieht für jeden mobilen Computer im Internet eine feste Adresse (Home Address) vor, die unabhängig von der aktuellen Anbindung an das Internet ist. Außerhalb seines eigenen lokalen Netzes ist dem Rechner zusätzlich eine temporäre Adresse (Care-of Address) zugeordnet, die dem aktuellen Anbindungspunkt an das Internet entspricht. Die Registrierung der wechselnden Adresse erfolgt über einen Heimagenten. Dieser Heimagent sendet Datenpakete, die an die feste Adresse des Computers gesendet werden, mittels eines Tunnelingverfahrens an die temporäre Care-of-Address weiter. Dort werden die Datenpakete entgegengenommen und an den mobilen Computer weitergeleitet.

*Katharinenstr. 3, 49069 Osnabrück, Tel.: 0541-969 4814, Ingmar.Ickerott@uni-osnabrueck.de

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Problemhintergrund

Die im vergangenen Jahrzehnt errichteten mobilen Netzwerke werden in erster Linie zur Übertragung von Sprache eingesetzt. Der Anteil der Datenübertragung ist nach wie vor sehr gering. In Deutschland werden diese Netze im Jahr 2003 von 74% der Bevölkerung genutzt (siehe Abbildung 1a)). In zwei Jahren werden laut einer aktuellen BITKOM[1]-Studie 85% der Deutschen Mobilfunknetze nutzen [BITKOM 2003]. Einen ähnlich starken Anstieg, wie im Bereich der Mobilfunknetze, verzeichnet man bei der Nutzung des Internets (siehe Abbildung 1b)). Aktuell bedienen sich ca. 50% der Bundesbürger der Dienste des Internets. In den nächsten zwei Jahren soll diese Zahl auf 60% steigen [BITKOM 2003]. Im Gegensatz zu den Mobilfunknetzen unterstützt das Internet primär datenbasierte Anwendungen bzw. Dienste. Mobilität steht hierbei nicht im Vordergrund.

Bisher war die (Aufgaben-)Trennung der beiden Netze kein großes Problem. Mit der zunehmenden Verbreitung mobiler Computer (PDAs, Notebook Computer, Pocket PCs, Smartphones etc.) steigt jedoch auf Seiten der Nutzer das Bedürfnis nach datengestützten mobilen Diensten, die jederzeit und überall verfügbar sind. Gewünscht wird ein mobiler Zugriff auf Internetdienste (anytime, anywhere). Einer im Auftrag des Bundesministeriums für Wirtschaft und Arbeit erstellten Studie zur Folge, besitzen im Jahr 2003 europaweit ca. 205 Millionen Menschen ein internetfähiges mobiles Endgerät [Graumann 2002]. Bis zum Jahr 2006 werde diese Zahl voraussichtlich auf 294 Millionen ansteigen. Ca. 31% der Besitzer mobiler Endgeräte würden dann regelmäßig auf Internetdienste zugreifen [Graumann 2002].

Für die mobilen Endgeräte ist heutzutage ein gewisser Grad an Mobilität des Internets bereits vorhanden. Beispielsweise kann der Nutzer eines mobilen Computers von verschiedenen Anbindungspunkten aus eine Verbindung zu seinem Internet-Service-Provider herstellen und so von überall auf dieselben Dienste zugreifen. Diese Form der Mobilität wird als ,,Nomadische Mobilität" (engl. ,,nomadicity") oder auch als ,,Roaming" bezeichnet [Patil 2003]. Bei jedem Ortswechsel bzw. Wechsel des Internetanbindungspunktes ist eine Neueinwahl erforderlich. Für viele Anwendungen ist diese Form der Mobilität des Internets ausreichend.

Insbesondere Funknetze bieten jedoch Potential für eine viel weitreichendere Form der Mobilität. Ziel ist die Schaffung eines Zugangs zum Internet, der den nahtlosen Übergang von Anbindungspunkt zu Anbindungspunkt ohne Abbruch der Verbindung ermöglicht. Es ist offensichtlich, dass dies dann von Vorteil ist, wenn der Internetnutzer sich während einer Internetverbindung frei bewegen will, z.B. während einer Stadterkundung, einer Auto- oder Bahnfahrt. Leider wird diese Form der Mobilität durch die herkömmliche Technologie des Internets nicht unterstützt.

Die Internettechnologie basiert auf einer Reihe einfacher Kommunikationsprotokolle, d.h. Absprachen über den Aufbau, die Überwachung und den Abbau von Kommunika-

[1] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

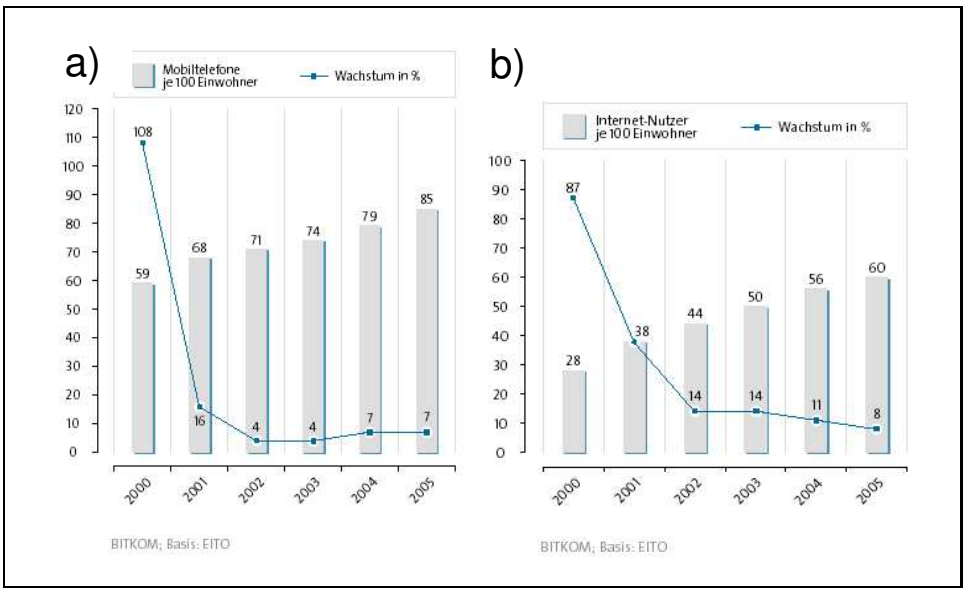

Abbildung 1: Mobilfunk und Internet in Deutschland 2000-2005 [BITKOM 2003]

tionsverbindungen. Das Internet Protokoll (IP) stellt das Fundament dar, auf dem die Vermittlung von Daten zwischen den kommunizierenden Systemen beruht. Dieses auf der sogenannten Vermittlungsebene (engl. ,,Network Layer") agierende Internet Protokoll ist nicht mit einer inhärenten Mobilitätsfunktion ausgestattet worden.

1.2 Problemstellung

Was ist der Grund für die fehlende Mobilitätsunterstützung durch das Internet Protokoll? Das Internet Protokoll wurde 1981 zunächst für das DARPA-Internet (ARPANET) und später für das weltweite Internet im RFC[2] 791 spezifiziert [Postel 1981]. Zur Aufgabe des Internet Protokolls heißt es dort: ,,The internet protocol is specifically limited in scope to provide the functions necessary to deliver a package of bits (an internet datagram) from a source to a destination over an interconnected system of networks" [Postel 1981]. ,,The datagrams are routed from one internet module to another through individual networks based on the interpretation of an internet address. Thus, one important mechanism of the internet protocol is the internet address" [Postel 1981].

Das Protokoll wurde unter der Prämisse definiert, dass ein Internetknoten, d.h. ein Rechner, der das Internet Protokoll verwendet, einen festen, stationären Anbindungspunkt hat, der durch eine eindeutige Adresse (IP-Adresse) identifiziert ist. ,,Current versions of the Internet Protocol make an implicit assumption that a node's point of

[2]Die ,,Requests for Comments" (RFC) sind eine Sammlung technischer und organisatorischer Dokumente über das Internet (ursprünglich das ARPANET), beginnend mit dem Jahr 1969 und herausgegeben von der Internet Engineering Task Force (IETF), einer Untergruppe der Dachorganisation Internet Society (ISOC). Informationen zu RFCs findet man unter der URL: http://www.ietf.org/.

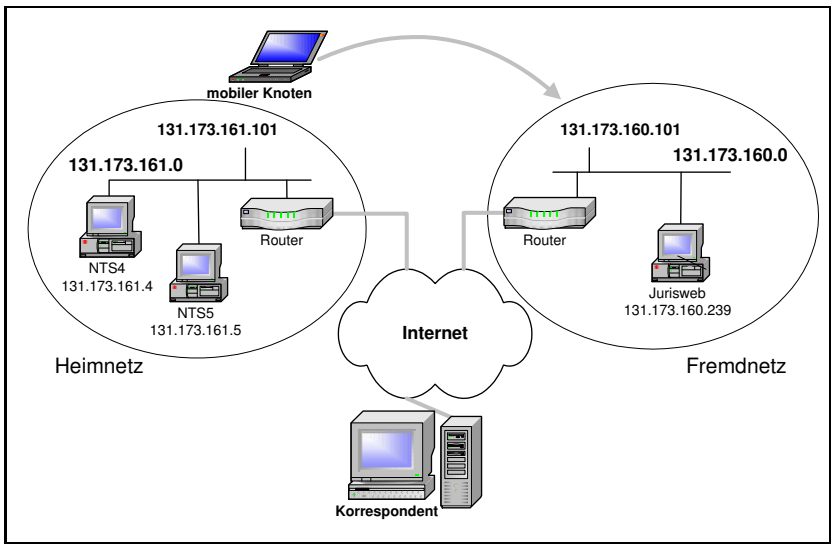

Abbildung 2: Problemstellung

attachment remains fixed" [Perkins 1994]. Die implizite Annahme fixer Standorte ist für eine Zeit, in der es noch keine mobilen Computer gab, angemessen gewesen.

Um Datenpakete senden und empfangen zu können, muss ein Knoten in einem Netzwerk lokalisiert sein, das durch die IP-Adresse bezeichnet wird. Andernfalls sind Datenpakete nicht zustellbar [Perkins 2002]. Damit ein mobiler Knoten seine Fähigkeit zur Kommunikation mit anderen Knoten nach einem Wechsel des Anbindungspunktes bzw. Netzes nicht verliert, muss er also seine IP-Adresse ändern (siehe Abb. 2). Dies hat zur Folge, dass die Datenpakete eines zeitgleich in Korrespondenz stehenden Knotens nicht richtig zugestellt werden können. Die laufende Verbindung zu dem Kommunikationspartner auf Anwendungs- bzw. Dienstebene (z.B. ein Download von Musikdateien per ftp-Dienst) muss unterbrochen und neu aufgebaut werden.

Gegenstand dieser Untersuchung ist eine Erweiterung des Internet Protokolls, die ein nahtloses, unterbrechungsfreies Routing von Datenpaketen zu mobilen Computern im Internet ermöglicht. Das als Mobile IP bezeichnete Protokoll stellt einen Mechanismus bereit, der mobilen Computern den Wechsel des Internetanbindungspunktes erlaubt, ohne die IP-Adresse ändern zu müssen (Mobile Network Layer). Eine Unterbrechung der Kommunikation wird somit vermieden.

1.3 Aufbau der Arbeit

Im zweiten Abschnitt der Arbeit wird zunächst das Internet Protokoll erläutert, da es die Grundlage des Mobilen Internet Protokolls darstellt. Es beinhaltet eine Einordnung des Internet Protokolls in die TCP/IP-Protokollfamilie, um den Aufgabenbereich des Protokolls im Zusammenspiel mit anderen Protokollen abzugrenzen. Wie das Internet Protokoll diese Aufgaben umsetzt, wird anhand der Einzelfunktionen (Adressierung und Fragmentierung) erläutert. Hierbei wird gesondert auf die beiden unterschiedlichen

Standards des Protokolls eingegangen, da für diese andere Voraussetzungen zur Unterstützung von Mobilität gelten. Im dritten Abschnitt, dem Hauptteil der Arbeit, wird die Erweiterung des Internet Protokolls für mobile Anwendungen vorgestellt. Nach einem kurzen Überblick über die Grundfunktion von Mobile IP und der Entstehung des Protokolls werden die neuen Architekturkomponenten erläutert. Anschließend werden die einzelnen Dienste des Mobile IP detailliert dargestellt und die Mobile-IP-Lösungen auf Basis der beiden Internet Protokoll Standards miteinander verglichen. Der Abschnitt endet mit der Betrachtung einiger Umsetzungsbeispiele. Zum Schluss der Arbeit erfolgt eine zusammenfassende Würdigung und ein kurzer Ausblick auf kommende Entwicklungen.

2 Das Internet Protokoll (IP)

2.1 Einordnung in die TCP/IP-Protokollhierarchie

Als Bezugsrahmen für die Kommunikationsarchitektur offener Kommunikationssysteme wurde 1993 von der internationalen Normungsorganisation ISO[3] ein mehrschichtiges Referenzmodell, das Open Systems Interconnection (OSI-)Referenzmodell[4], entwickelt. Anhand OSI-Architektur lassen sich die Bestandteile der Internettechnologie strukturiert erläutern. Auch wenn sich die Protokollfamilie der Internettechnologie (TCP/IP) nicht vollständig nach dem ISO-Standard richtet, so finden sich in beiden Architekturen aufgabenähnliche Schichten wieder, die zur Komplexitätsreduktion der Systemkommunikation beitragen (siehe Abbildung 3). Das OSI-Modell besteht aus sieben hierarchisch angeordneten Schichten. Die für eine Kommunikation erforderlichen Kommunikationsdienste sind nach diesen Schichten eingeteilt, wobei jede Schicht an die jeweils darunter liegende Schicht einen Auftrag formuliert, der von dieser als Dienstleistung für die darüberliegende Schicht erbracht wird [Stahlknecht, Hasenkamp 2002]. Unter den Schichten besteht folgende Aufgabenteilung [Tannebaum 2000]:

1. *Physikalische Schicht (physical layer):* Die ungesicherte Übertragung von Bitfolgen über eine (Teil-)Strecke des Übertragungsweges wird geregelt.

2. *Sicherungsschicht (link layer):* Die Bitübertragung auf Ebene 1 wird durch verschiedene Mechanismen zur Fehlererkennung und -behebung gesichert. Blöcke aus Bitfolgen werden mit Kontrollinformationen versehen.

3. *Vermittlungsschicht (network layer):* Der Auf- und Abbau des gesamten *physikalischen* Übertragungsweges zwischen Datenendgeräten aus gekoppelten Teilstrecken wird gesteuert. Datenpakete werden adressiert und der Nachrichtenweg wird festgelegt (Routing).

[3] International Organization Standardization.
[4] Details zum OSI-Referenzmodell der ISO sind in der Norm DIN EN ISO/IEC 7498 dokumentiert.

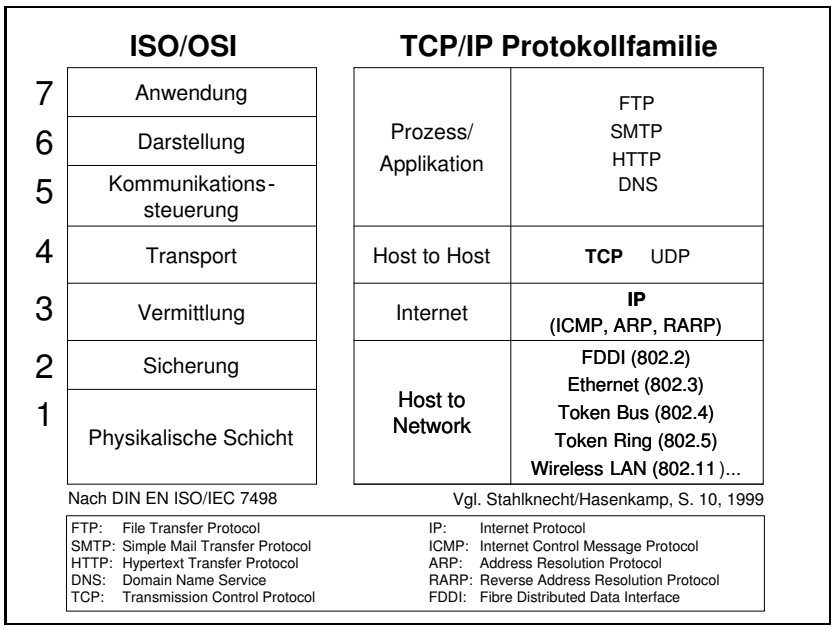

Abbildung 3: ISO/OSI-Referenzmodell und TCP/IP-Protokollfamilie

4. *Transportschicht (transport layer):* Die Daten werden in kleinere Pakete aufgeteilt und an die Vermittlungsschicht weitergeleitet. Auf der Empfängerseite erfolgt eine Kontrolle auf Vollständigkeit. Die *logische* Verbindung zwischen Sender und Empfänger wird überwacht und gesteuert (end-to-end bzw. host-to-host).

5. *Kommunikationssteuerungsschicht (session layer):* Die Kommunikation zwischen den Teilnehmern wird in Form von Sitzungen (sessions) auf der Ebene der Betriebssysteme geregelt.

6. *Darstellungsschicht (presentation layer):* Die Bedeutung der ausgetauschten Daten wird festgelegt. Gegebenenfalls werden die Darstellungsformen umgesetzt.

7. *Anwendungsschicht (application layer):* Anwendungsklassen, die eigentlichen Dienstprogramme, werden definiert.

Der Begriff TCP/IP steht stellvertretend für die Gesamtheit aller Internetprotokolle. Strenggenommen sind das Transmission Control Protocol (TCP) und das Internet Protocol (IP) nur zwei Bausteine der Gesamtarchitektur der Internettechnologie, wenngleich die wichtigsten. Die erwarteten Funktionalitäten der TCP/IP-Bestandteile sind jeweils in den Request for Comments der Internet Engineering Task Force (IETF) beschrieben.

Die Schichten 5 bis 7 sind bei TCP/IP zusammengefasst zur Prozess- bzw. Applikationsschicht. Die Funktionen dieser Schichten werden von Dienstprotokollen, wie dem File Transfer Protocol (FTP) oder dem Simple Mail Transfer Protocol (SMTP), gemeinsam erfüllt (siehe Abbildung 3). Eine Anwendung, die Daten zu einer Anwendung

eines anderen Internetknotens senden möchte, übergibt die zu sendenden Daten an diese Applikationsschicht (bspw. an eines der in Abbildung 3 genannten Protokolle).

Das Protokoll auf der Applikationsschicht erstellt aus den erhaltenen Daten eine Nachricht, bevor diese an ein Transportschichtprotokoll weitergeleitet wird [Washburn, Evans 1994]. Eine Nachricht setzt sich aus den von der Anwendung übermittelten Daten und einem Anwendungskopf zusammen, der für die Applikationsschicht des korrespondierenden Systems Informationen über die gewünschte Datenverwendung enthält.

Auf der Transportschicht (Host-to-Host-Schicht) übernimmt etwa ein verbindungsloses oder ein verbindungsorientiertes Protokoll die Nachricht. Ein verbindungsloses und nicht sehr zuverlässiges Protokoll ist das User Datagram Protocol (UDP)[5] UDP wird als verbindungslos und unzuverlässig bezeichnet, da es einzelne Datagramme zu einem entfernten Knoten überträgt, ohne eine Rückmeldung über den Eingang der Daten zu erwarten [Washburn, Evans 1994]. Zumeist kommt jedoch das Transmission Control Protocol (TCP)[6] zum Einsatz. Dies ist ein verbindungsorientiertes, zuverlässiges Protokoll, d.h. es erfordert, dass eine Verbindung errichtet wird, bevor Daten von einem Rechner an einen anderen übertragen werden können [Washburn, Evans 1994]. Der Datentransfer wird auf Fehler untersucht und gegebenenfalls korrigiert. Sobald die Datenübertragung abgeschlossen ist, wird die Verbindung gelöst. TCP wird von den in Abbildung 3 aufgeführten Protokollen auf der Applikationsebene verwendet. UDP und TCP verwenden 16-Bit-Port-Adressen, um Daten an die betreffenden Dienste der Applikationsschicht zu senden. Datenblöcke, die von TCP an die Vermittlungsschicht (Internetschicht) weitergegeben werden, bezeichnet man für gewöhnlich als Segmente, die von UDP als Datagramme [Washburn, Evans 1994]. Sie umfassen jeweils die von der Applikationsschicht erhaltene Nachricht und einen vorangestellten Transportkopf.

Empfänger ist das in dieser Arbeit im Fokus stehende Internet Protocol (IP) auf Internet- bzw. Vermittlungsebene. Das Internet Protokoll sorgt für eine Übertragung von Datenblöcken von einem Quellrechner zu einem Zielrechner, die über Adressen mit fixer Länge identifiziert sind (vgl. [Postel 1981]). Die Datenblöcke werden auch IP-Datagramme genannt. Das Internet Protokoll ist ein verbindungsloser Datagrammdienst, d.h. es behandelt jedes Datagramm einzelnd und unabhängig von jedem anderen Datagramm. Vom Empfänger der Datagramme wird nicht erwartet, dass dieser den Empfang bestätigt. ,,There are no mechanisms to augment end-to-end data reliability, flow control, sequencing, or other services commonly found in host-to-host protocols" [Postel 1981]. Die Datagramme werden von dem Internet Modul einer TCP/IP-Implementierung erstellt, indem die TCP-Segmente bzw. UDP-Datagramme um einen IP-Steuerungskopf (IP-Header) erweitert werden. Die Datagramme werden anschließend an die nächsttieferliegende Schicht weitergeleitet.

Bei TCP/IP-Netzen werden die Schichten 1 (physikalische Schicht) und 2 (Datensicherungsschicht) des OSI-Modells zu einer Host-to-Network-Schicht zusammengefasst. In Abbildung 3 sind einige der für dies Ebene entwickelten Protokolle aufgelistet. Die Datensicherungskomponente innerhalb dieser Schicht fügt dem von der Internetschicht

[5]UDP ist im RFC 768 spezifiziert.
[6]TCP ist im RFC 761 spezifiziert.

erhaltenen Datagramm einen weiteren Kopf und meist irgendeine Art von Prüfsumme am Ende ein und bildet damit einen Rahmen. Die Bitübertragungskomponente wandelt die Datenbits in die dem Medientyp entsprechenden Signale um und leitet diese an das Schnittstellenkabel weiter. Auf der Host-to-Network-Schicht wird mit 48-Bit-Adressen gearbeitet, die man physikalische Adressen, Medienzugriffsadressen oder auch MAC[7]-Adressen nennt [Washburn, Evans 1994]. Sie sind normalerweise in die Netzkarte eingebrannt.

Ein häufig in TCP/IP-Netzen verwendetes Protokoll auf der Host-to-Network-Ebene ist das Ethernet Protokoll. Zur Steuerung und Kontrolle physischer Netze werden noch eine Reihe weiterer Protokolle eingesetzt. FDDI[8], Token Ring, Token Bus, oder für Funknetze das Wireless LAN sind Beispiele hierfür. Diese Vielfalt macht deutlich, wie heterogen die eingesetzten lokalen Netzwerke und Weitverkehrsnetzwerke (LANs und WANs) sind.

In heterogenen Netzen, die TCP/IP als Kommunikationsprotokoll verwenden, wird IP von einem Verbund zwischengeschalteter Relais, sogenannten Routern[9], verarbeitet und interpretiert. „IP unterstützt die Routenwahl und Informationsübermittlung zwischen kommunizierenden Hosts (und anderen Geräten) und berücksichtigt dabei den Typ der Dienstprimitive, den sie benötigen" [Washburn, Evans 1994]. IP kann auf jedem Netz physikalischer Kabel aufsetzen und fungiert so quasi als kleinster gemeinsamer Nenner heterogener Netze.

2.2 IP-Funktionen

Das Internet Protokoll erfüllt grundsätzlich zwei Funktionen, die im folgenden erläutern werden: Die Adressierung und Fragmentierung von Datagrammen [Postel 1981].

2.2.1 Adressierung

Das Internet Protokoll nutzt die Adresse im IP-Header, um Internet-Datagramme zum Zielort zu übermitteln. „Jede TCP/IP-Kommunikation wird mit der IP-Adresse eingeleitet" [Washburn, Evans 1994]. Die Wahl des Übertragungsweges anhand der IP-Adresse wird Routing genannt [Washburn, Evans 1994]. Eine IP-Adresse wird so konfiguriert, dass sie eine bestimmte Netznummer (Netzwerk-Prefix) und eine eindeutige Host-Verbindung in diesem Netz repräsentiert. Falls mehr als eine Verbindung bei einem Knoten eingerichtet werden soll, muss jede Verbindung durch eine IP-Adresse identifiziert werden. Dies trifft auf Router zu, da diese Verbindungen zu zwei oder mehr Netzen besitzen.

Eine höhere Schicht, z.B. TCP, ruft das Internet Protokoll auf und übergibt neben der IP-Adresse des Zielrechners, die zu senden Daten als eine Gruppe von Segmenten, sowie weitere Parameter als Argumente des Aufrufs [Postel 1981]. Auf Basis der erhaltenen

[7] Medium Access Control.
[8] Fibre Distributed Data Interface.
[9] Router sind Internet-Knoten, die IP-Datagramme weiterleiten, die nicht explizit an sie adressiert sind [Deering, Hinden 2003].

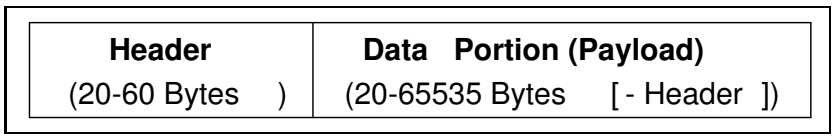

Abbildung 4: IP-Datagrammstruktur

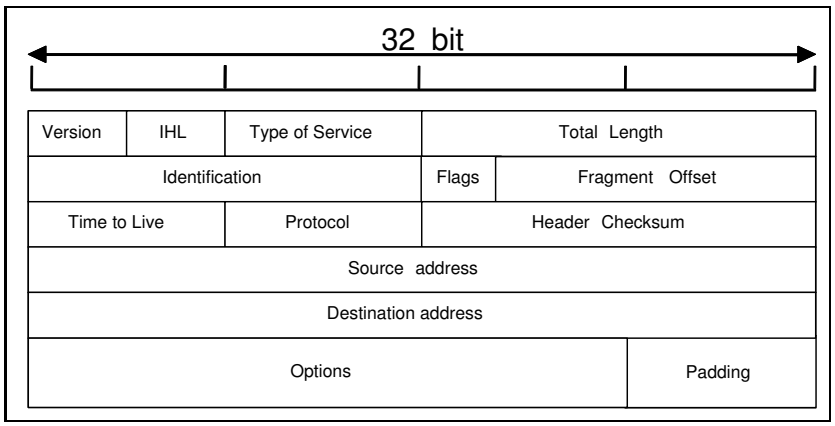

Abbildung 5: IPv4 Header

Informationen erstellt das Internet Protokoll für jedes Segment einen IP-Header, an den das Segment angehängt wird. In der ursprünglichen Spezifikation gemäß RFC 791 umfasst der Header die ersten 20 bis 60 Bytes eines Datagramms, wobei das gesamte Datagramm inklusive Datenteil bis zu 65.535 Bytes umfasst (siehe Abbildung 4).

Aktuell existiert das Internet Protokoll in zwei unterschiedlichen Versionen, der älteren allgemein bekannten Version 4, sowie der neueren Version 6. Die beiden Versionen unterscheiden sich bezüglich der Größe und Struktur des Headers bzw. der Funktion und des Inhalts der Headerfelder.

Der Standard: IP Version 4. Ein IP-Datagramm der Version 4 (IPv4) hat gemäß RFC 791 den in Abbildung 5 gezeigten Headeraufbau. Eine vollständige Beschreibung aller Headerfelder von IPv4 befindet sich in Anhang A. Für die Identifizierung der Quell- und Zielrechnernetzverbindungen sind 32-Bit-IP-Adressen vorgesehen. Die Struktur der IP-Adresse nach IPv4 erlaubt eine Unterscheidung in A-,B- und C-Netze.

Der Standard: IP Version 6. Die neuere Version 6 des Internet Protokolls wird in RFC 2460[10] spezifiziert [Deering, Hinden 1998b]. Im Unterschied zur ursprünglichen Version 4 arbeitet die neue Version 6 mit 128 Bit langen Adressen[11]. Obwohl die IPv6-

[10] Der RFC 2460 befindet sich im Status eines Draft Standard. Ein endgültiger Standard für IPv6 liegt noch nicht vor.

[11] Die Adressierungsarchitektur des IPv6 wurde erst kürzlich überarbeitet und als Proposed Standard im RFC 3513 veröffentlicht [Deering, Hinden 2003].

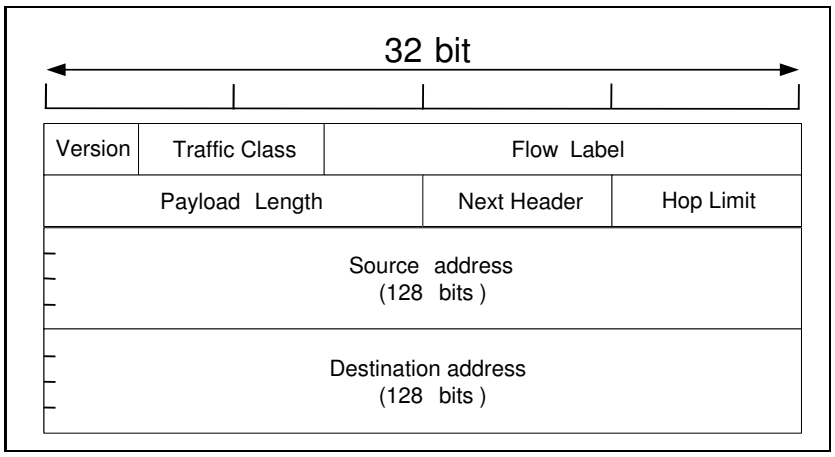

Abbildung 6: IPv6 Header

Adressen vier Mal größer sind, als IPv4-Adressen, ist der Header im Ganzen nur doppelt so groß. Der Kern-Header eines IPv6-Datagramms umfasst weniger Felder als ein IPv4-Header (siehe Abbildung 6). Er kann jedoch je nach Funktion des Datagramms um Anhänge erweitert werden und bietet somit eine flexible Unterstützung für Optionen und Weiterentwicklungen des Protokolls. Mit Hilfe der Optionen werden z.B. Sicherheitsmechanismen unterstützt. Eine vollständige Beschreibung aller Felder im Header eines Version 6 Datagramms befindet sich in Anhang B.

Die Standards IPv4 und IPv6 bieten unterschiedliche Voraussetzungen zur Unterstützung von Mobilität. Ein Großteil dieser Arbeit wird sich mit Mobile IP auf Basis der Version 4 beschäftigen. Auf die Unterschiede zu Mobile IPv6 wird im Anschluss genauer eingegangen. Die Adressierungsfunktion des Internet Protokolls greift auf die Dienste der Teilprotokolle ARP, RARP und ICMP zu, die nun kurz erläutert werden (siehe Abbildung 3).

ARP und RARP. Das Address Resolution Protocol (ARP) der TCP/IP-Protokollfamilie implementiert eine Methode, mit der für einen Host, dessen IP-Adresse bekannt ist, die zugehörige physikalische Adresse (MAC-Adresse) ermittelt wird. Der Sender verschickt ein ARP-Paket per Broadcast an alle angeschlossenen Links und wartet darauf, dass ihm die physikalische Adresse zurückgeschickt wird. Jeder Host führt einen Cache mit bekannten Übersetzungen, um die Umsetzzeit und die notwendigen Broadcasts zu minimieren. Der Cache muss allerdings zyklisch aktualisiert werden. ARP ist im RFC 826 definiert.

Das Reverse Address Resolution Protocol (RARP) bezeichnet ein umgekehrtes ARP zur dynamischen Vergabe von IP-Adressen[12]. Es dient z.B. dazu, einer disklosen Workstation eine IP-Adresse zuzuordnen. Eine Workstation ohne Harddisk zur Speicherung einer IP-Adresse muss sich von einem anderen Rechner, dem RARP-Server, eine IP-Adresse holen. Dazu kommuniziert der sendewillige Client mit dem RARP-Server, der

[12]Alternativ können das BootP-Protokoll und und das DHCP-Protokoll eingesetzt werden.

alle Internet-Adressen für harddisklose Stationen verwaltet. Jedes Netzwerk, an das Stationen ohne Harddisk angeschlossen sind und das das RARP-Protokoll unterstützt, muss demnach einen RARP-Server haben. Das RARP arbeitet auf der Vermittlungsschicht und ist aus dem Address-Resolution-Protokoll (ARP) abgeleitet. Daher benutzt es auch ein ähnliches Datenformat. Das RARP-Protokoll ist im RFC 903 beschrieben.

ICMP. Das Internet Control Message Protocol (ICMP) ist kein Protokoll zur Datenübertragung im eigentlichen Sinn, sondern dient der Übertragung von Statusinformationen und Fehlermeldungen der Protokolle IP, TCP und UDP zwischen IP-Netzknoten. Es werden Datagramme übermittelt, die von dem empfangenden Rechner automatisch beantwortet werden (evtl. schon allein durch die Netzwerkkarte ohne Beteiligung des Betriebssystems). ICMP wird genutzt, um Fehler bei der Übertragung zu erkennen und zu melden[13]. Das ICMP-Protokoll wird von IP wie ein Protokoll einer höheren Schicht behandelt und ist integraler Bestandteil des IP-Protokolls. Daher setzt sich der ICMP-Header auch aus einem IP-Header mit nachfolgenden ICMP-Daten zusammen. ICMP gliedert sich in verschiedene Typen, die jeweils eine bestimmte Funktion auslösen oder einen bestimmten Status deklarieren. Zum Beispiel ist ein ICMP-Datagramm von Typ 9 eine Router-Advertisement-Nachricht, die die Verfügbarkeit des Routers für alle angeschlossenen Links bekannt macht („Router bietet sich an"). Das ICMP-Protokoll ist im RFC 792 veröffentlicht worden.

2.2.2 Fragmentierung

Prinzipiell können die Protokolle höherer Schichten beliebig große Datenmengen senden. Auf physikalischer Schicht herrschen jedoch unterschiedliche Größenbeschränkungen für Rahmen vor. Das IP muss somit einen Mechanismus bereitstellen, mit dem beliebig große Datagramme höherer Schichten in kleinere Einheiten aufgeteilt werden, so dass sie entsprechend den physikalischen Beschränkungen der Host-to-Network-Schicht übertragen werden können. Dieser Mechanismus wird Fragmentierung genannt [Postel 1981].

IP-Datagramme werden dabei in sogenannte Fragmente aufgeteilt. Das IP-Modul erstellt für das Ursprungsdatagramm zwei oder mehr neue Datagramme bzw. Fragmente. Der ursprüngliche Header wird modifiziert in die Fragmente kopiert und der Datenteil auf die Fragmente aufgeteilt. Anschließend werden die Fragmente wie normale Datagramme versandt (bzw. an die Host-to-Network-Schicht weitergeleitet).

Das IP-Modul des Zielknotens setzt die Fragmente in der richtigen Reihenfolge wieder zusammen[14]. Zur Identifikation der Fragmente nutzt das IP die Kombination der Headerfelder: Identification, Source-Destination-Adresspaar und Protocol (vgl. Anhang A).

[13] Z.B. verwenden die Kommandos PING und TRACERT dieses Protokoll.
[14] Router können die Fragmente ausschließlich weiter aufteilen, nicht aber zusammensetzen.

3 Mobile IP

3.1 Überblick und Entstehung

Mobile IP stellt eine Erweiterung des Internet Protokolls (IP) dar, die ein nahtloses Routing von Datenpaketen zu mobilen Computern im Internet ermöglicht. Das Protokoll löst das Mobilitätsproblem auf der Vermittlungsebene. Grundgedanke ist die transparente Integration mobiler Knoten in beliebige Netzwerke. Für die im ISO/OSI-Referenzmodell darüberliegende Protokolle und Anwendungen bleibt die in der Einleitung beschriebene Problematik verdeckt. Zu den Anforderungen an das Protokoll heißt es im RFC 3344: ,,A mobile node must be able to communicate with other nodes after changing its link-layer point of attachment to the Internet, yet without changing its IP address" [Perkins 2002]. Realisiert wird diese Anforderung durch die Einführung einer festen Adresse für mobile Knoten, über die diese stets erreichbar sind, auch wenn sie gar nicht im Heimnetzwerk angebunden sind. Durch die Beibehaltung der IP-Adresse wird eine Unterbrechung der Kommunikation auf höheren Ebenen, die mit verbindungsorientierten Protokollen arbeiten überflüssig.

Darüber hinaus soll eine Kommunikation zwischen Rechnern, die das Mobile IP implementieren und jenen, die Mobile IP nicht unterstützen ohne Probleme möglich sein. ,,A mobile node must be able to communicate with other nodes that do not implement these mobility functions"[Perkins 2002]. Protokollveränderungen auf allen am Netz beteiligten Rechnern zu veranlassen, wäre bei der derzeit existierenden Internetinfrastruktur auch kaum durchsetzbar.

Da Mobile IP vornehmlich in kabellosen Netzen zur Anwendung kommt, sind in der Spezifikation des Protokolls (RFC 3344) weitere Ziele formuliert worden. Mobile IP soll mit geringeren Bandbreiten und höheren Fehlerraten als in traditionellen Netzen arbeiten können. Da mobile Endgeräte batteriebetrieben sind, ist zudem der für die Kommunikation erforderliche Stromverbrauch möglichst gering zu halten. Um diese Ziele zu erreichen, muss Mobile IP mit möglichst wenig und kurzen Nachrichten (Datagrammen) zum Zwecke der Administration arbeiten.

Das mobile Internet Protokoll arbeitet, wie das Internet Protokoll, unabhängig von den Protokollen auf der Host-to-Network-Schicht. Es ist deshalb nicht auf eine Anwendung in homogenen Medien beschränkt. ,,It is just as suitable for mobility across homogeneous media as it is for mobility across heterogeneous media" [Perkins 2002]. Mobile IP unterstützt das Routing unabhängig davon, ob ein mobiler Rechner z.B. von einem Ethernet-Segment in ein anderes oder in ein Wireless-LAN wandert.

Die Trennung von der Host-to-Network-Schicht hat noch eine zweite Implikation auf die Anwendung des Mobile IP. Aufgaben, die von darunter agierenden Protokollen geleistet werden können, sollen von Mobile IP nicht erfüllt werden. So gehört der Handoff zwischen zwei Funk-Transceivern eines Funk-LANs nicht zum Anwendungsfeld von Mobile IP, sondern bleibt die Aufgabe eines entsprechenden Protokolls auf der Host-to-Network-Ebene. ,,One can think of Mobile IP as solving the "macro" mobility management problem. It is less well suited for more "micro" mobility management applications" [Perkins 2002]. Aufgaben des Mirkomobilitätsmanagement innerhalb eines

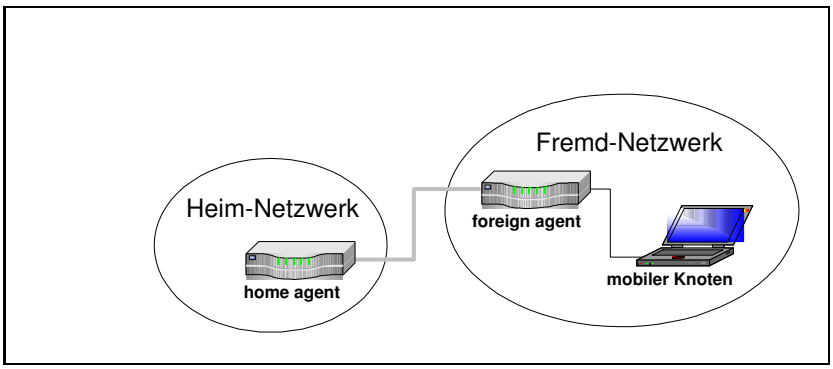

Abbildung 7: Mobile IP Architekturkomponenten

IP-Netzes bzw. -Subnetzes können durch Protokolle auf niedrigerer Ebene mit weniger Overhead effizienter realisiert werden [Perkins 2002].

Die Diskussion um die Entwicklung eines mobilen Internet Protokolls innerhalb der IETF begann in den Jahren 1991 und 1992. Auf den Birds-of-a-feather-Sitzungen der IETF in Atlanta (Juli 1991), Santa Fe (November 1991) und San Diego (März 1992) bildete sich eine Mobile-IP-Arbeitsgruppe. Im 30. Juni 1992 wurde von der IETF offiziell dem Antrag auf Bildung einer Mobile IP Working Group stattgegeben[15].

1994 wurde von den Mitgliedern der Arbeitsgruppe der RFC 1688 veröffentlicht, in dem erste Hinweise auf eine mögliche Mobile-IP-Lösung diskutiert werden. In dem RFC heißt es: ,,Each Mobile Node must have at least one Home-Address which identifies it to other nodes. This Home-Address must be globally unique." [Perkins 1994]. Eine erste umfassende Spezifikation des Protokolls auf Basis von IPv4 erfolgte im RFC 2002 des Jahres 1996 [Perkins 1996]. Der aktuelle Stand der Diskussion wird in dem im Jahr 2002 veröffentlichten RFC 3344 wiedergegeben [Perkins 2002]. Diese Spezifikation hat aktuell bei der Internet Engineering Steering Group (IESG) den Status eines "proposed standards". Darüber hinaus existieren Internet-Drafts zu den Themen Portierung des Protokolls auf IPv6, Routenoptimierung, Sicherheit und Fast Handover, die in dieser Arbeit an jeweils geeigneter Stelle thematisiert werden[16].

3.2 Architekturkomponenten

Die Kommunikationsarchitektur des Mobile IP basiert auf drei funktionalen Einheiten, die als Mobilitätsagenten (mobility agents) bezeichnet werden [Perkins 2002]. Man unterscheidet den mobilen Knoten (mobile node), den Heimagenten (home agent) und den Fremdagenten (foreign agent) (siehe Abbildung 7).

Der mobile Knoten ist ein Host oder Router, der seinen Anbindungspunkt zum Internet von einem Netzwerk oder Subnetzwerk zu einem anderen ändern kann [Perkins 2002].

[15] Ein Archiv der Arbeitsgruppe mit Gesprächsprotokollen, Vorschlägen und Mails findet man unter der URL http://playground.sun.com/pub/mobile-ip/.

[16] Eine umfassende Auflistung aller RFCs und Internet Drafts der Mobile IP Working Group findet man unter der URL http://www.ietf.org/html.charters/mobileip-charter.html.

Er muss dabei seine IP-Adresse nicht ändern, sondern kann, egal von welchem Anbindungspunkt aus er mit einem Korrespondenten kommuniziert, seine konstante IP-Adresse nutzen.

Der Heimagent ist ein Router im Heimnetz des mobilen Knotens. Seine Hauptaufgabe besteht in der Weitersendung von IP-Datagrammen an den mobilen Knoten, wenn dieser sich nicht in seinem Heimnetz befindet. Er muss hierzu Informationen über den aktuellen Standort des mobilen Knotens pflegen.

Der Fremdagent ist ein Router in einem von dem mobilen Knoten besuchten Netzwerk. Während ein mobiler Knoten bei dem Fremdagenten registriert ist, unterstützt der Fremdagent das Routing von Datagrammen vom Heimagenten zum mobilen Knoten.

Der mobile Knoten besitzt eine permanente IP-Adresse in seinem Heimnetzwerk, die Heimadresse (home address). Diese feste IP-Adresse wird genauso verwaltet, wie die Adresse eines stationären Rechners im gleichen Netz. Mit Ausnahme einiger spezieller Nachrichten im Rahmen des Mobilitätsmanagement verschickt der mobile Knoten alle Datagramme mit seiner festen Heimadresse als Quelladresse (source address). Dies geschieht auch, wenn er sich in einem anderen Netzwerk befindet. Die Heimadresse unterliegt nur der Beschränkung, dass sie routable sein muss, d.h. sie darf nicht aus einem der drei privaten IP-Netze stammen. Befindet sich der mobile Knoten in seinem Heimnetzwerk, so arbeitet das Internet Protokoll mit den herkömmlichen Verfahren, d.h. ohne Mobilitätsdienste.

Befindet sich der mobile Knoten in einem fremden Netzwerk, so wird ihm zusätzlich eine temporäre Care-of-Adresse (CoA) zugeordnet, die den aktuellen Anbindungspunkt zum Internet reflektiert [Perkins 2002]. Die CoA ist eine IP-Adresse des Fremdnetzwerkes[17]. Damit der Heimagent Datagramme an den mobilen Knoten senden kann, muss ihm die CoA bekannt gemacht werden. Die CoA ist immer die Zieladresse (destination address) der IP-Datagramme, die von Heimagenten an den mobilen Rechner weitergeleitet werden. Care-of-Adressen können auf zwei unterschiedliche Weisen vergeben werden. Man unterscheidet Foreign-Agent-/ und Co-located-Care-of-Adressen:

Eine Foreign-Agent-CoA ist eine IP-Adresse, welche dem mobilen Rechner von einem Fremdagenten zugewiesen wird. In diesem Fall ist die CoA eine IP-Adresse des Fremdagenten. Sie wird dem mobilen Rechner durch eine sogenannte Agent-Advertisement-Nachricht mitgeteilt. Im RFC 3344 wird diese Methode zur Vergabe von CoA ausdrücklich präferiert. ,,This mode of acquisition is preferred because it allows many mobile nodes to share unnecessary demands on the already limited IPv4 address space" [Perkins 2002].

Eine Co-located-CoA ist eine lokale IP-Adresse des Fremdnetzwerkes, die der mobile Knoten von einer externen Stelle aus erhalten hat und die er einem seiner eigenen Netzwerk-Interfaces zuordnet. Die CoA kann dem mobilen Knoten z.B. dynamisch als temporäre Adresse mit Hilfe des Dynamic Host Configuration Protocol (DHCP[18]) zugewiesen werden. Es kann sich bei der Co-located-CoA allerdings auch um eine Adresse des Fremdnetzes handeln, die dem mobilen Knoten langfristig gehört. Der mobile Knoten verwaltet in diesem besonderen Fall einen statischen Pool von IP-Adressen, die er für

[17] Auch die Care-of-Adresse muss routable sein.

[18] Siehe auch Droms, R.: ,,Dynamic Host Configuration Protocol", RFC 2131, März 1997.

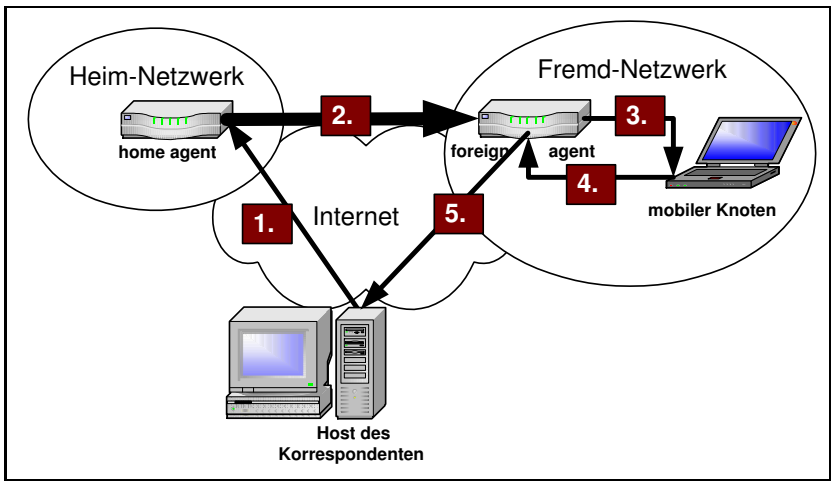

Abbildung 8: Mobile IP Routing

bestimmte Fremdnetzwerke nutzen kann. Wie später noch genauer erläutert wird, ist bei der Vergabe von Co-located-CoA ein Fremdagent nicht nötig, da alle vom Heimagenten an den mobilen Knoten weitergeleiteten Datagramme direkt zum mobilen Knoten geroutet werden, ohne den Fremdagenten zu passieren. Das ist der wichtigste Vorteil bei dieser Vergabemethode. ,,The mode of using a co-located care-of address has the advantage that it allows a mobile node to function without a foreign agent, for example, in networks that have not yet deployed a foreign agent" [Perkins 2002]. Als nachteilig wird festgehalten, dass in jedem Netzwerk ein Pool aus Adressen für besuchende Knoten vorgehalten werden muss. Dies gestaltet sich vor allem in begrenzten Adressräumen von IPv4-Subnetzen problematisch.

Der Heimagent verwaltet die aktuellen Care-of-Adressen des bzw. der mobilen Knoten in einer Verbindungsliste (binding table). In der Liste wird der IP-Heimadresse des mobilen Knoten die temporäre CoA zugeordnet und mit einer Lebensdauer (lifetime) in Sekunden versehen. Damit der Eintrag nicht verfällt, muss er vor Ablauf der Lebensdauer durch eine entsprechende Registrierung erneuert werden.

Der Fremdagent (wenn er existiert) verwaltet eine Besucherliste (visitors table) mit den aktuellen MAC-Adressen der besuchenden Knoten. In der Tabelle stehen neben den MAC-Adressen die IP-Home-Adresse und die IP-Adresse des Heimagenten. Für die Eintragungen in die Besucherliste ist je eine Lebensdauer festgelegt.

3.3 Mobile IP-Routing

Befindet sich der mobile Knoten in einem Fremdnetzwerk, so werden Datagramme, die an die Heimadresse des mobilen Knotens gesendet werden, mittels eines Dreieck-Routingverfahrens (triangular routing) zu dem mobilen Rechner im Fremdnetzwerk weitergeleitet. Die Art des Routings ist davon abhängig, ob das Foreign-Agent- oder das Co-located-Verfahren (s. Abschn. 3.2) zur Anwendung kommt. In Abbildung 8 nutzt der

mobile Knoten eine Foreign-Agent-CoA. Die Kommunikation mit einem korrespondierenden Host läuft dabei wie folgt ab. Der Korrespondent des mobilen Rechners sendet seine IP-Datagramme zur festen Home-Adresse des mobilen Knoten (Schritt 1). Die Datagramme werden mit Hilfe klassischer IP-Routingalgorithmen wie dem Routing-Information-Protocol (RIP[19]) oder dem Open-Shortest-Path-First-Protokoll (OSFP[20]) zum Heimnetzwerk des mobilen Knoten geleitet. Dort "lauscht" der Heimagent, ob Datagramme für den mobilen Rechner eintreffen. Um Datagramme abfangen zu können, muss der Heimagent im Heimnetzwerk vorgeben, die MAC-Adresse des nicht mehr anwesenden mobilen Knotens zu besitzen. Hierbei werden die beiden Mechanismen Proxi ARP[21] und Gratuitous ARP[22] genutzt. Um Datagramme, die an die Heimadresse des mobilen Knotens gerichtet sind, abfangen und weiterleiten zu können, sollte gemäß RFC 3344 ein Heimagent das Netzwerk-Interface auf dem Link implementieren, der zu der Heimadresse des mobilen Knotens gehört[23] [Perkins 2002].

Im nächsten Schritt leitet der Heimagent die empfangenen Datagramme an die in der Verbindungsliste gespeicherte Care-of-Adresse weiter (Schritt 2). In Abbildung 8 ist somit der Fremdagent der Empfänger (Foreign-Agent-CoA); wird hingegen das Co-Located-Verfahren angewandt, so ist der mobile Knoten selbst der Empfänger der weitergeleiteten Datagramme. Der Fremdagent wird nicht aktiv. Die IP-Datagramme werden vom Heimagenten gekapselt und neu adressiert. Das Verfahren wird in Abschnitt 3.4.3 genauer erläutert.

Ob daraufhin Schritt 3 und Schritt 4 nötig sind, hängt von der Existenz des Fremdagenten ab. Bei Anwendung des Foreign-Agent-CoA-Verfahren empfängt der Fremdagent die weitergeleiteten IP-Datagramme und sendet diese weiter an den mobilen Knoten (Schritt 3). Er nutzt hierzu die ihm aus der Besucherliste bekannte MAC-Adresse des Besuchers. Der mobile Knoten besitzt selbst keine IP-Adresse. ,,A mobile node and a prospective or current foreign agent MUST be able to exchange datagrams without relying on standard IP routing mechanisms" [Perkins 2002]. Dies ist wiederum möglich, wenn beide Mobilitätsagenten ein Interface auf dem selben Link besitzen. Sie sind dann in der Lage, Datenaustausch direkt auf der Host-to-Network-Ebene zu betreiben[24].

Die Antwort des mobilen Knotens erfolgt ebenfalls auf der Host-to-Network-Ebene (Schritt 4), d.h. Datenpakete werden zunächst an die MAC-Adresse des Fremdagenten

[19] Im RFC 2453 (G. Malkin, November 1998) ist der Standard von RIP in der Version 2 dokumentiert.

[20] Im RFC 2328 (J. Moy, April 1998) ist der Standard von OSFP in der Version 2 dokumentiert.

[21] Proxi ARP bezeichnet eine Spoofing-Technologie, bei der ein Router einen ARP-Request an Stelle eines entfernten Hosts beantwortet. Damit übernimmt der Router die Verantwortung für die Weiterleitung der Datenpakete an den wirklichen Empfänger. Dies hat den Vorteil, dass der ARP-Request nicht ständig über die entsprechende WAN-Verbindung übertragen werden muss.

[22] Gratuitous ARP wird verwendet, um anderen Knoten im lokalen Segment mitzuteilen, dass der sendende Rechner immer noch online ist. Hierbei werden keine besonderen Informationen außer den jeweiligen Adressen übertragen. Geräte, die die Adresse des Senders bereits in ihrem Cache haben, aktualisieren diese Daten, falls notwendig.

[23] Andere Möglichkeiten werden in der Protokollspezifikation ausdrücklich erlaubt, jedoch nicht genauer erläutert.

[24] Auch in diesem Fall werden andere Mechanismen zur Kommunikation zwischen Fremdagent und mobilen Knoten in der Protokollbeschreibung des RFC 3344 grundsätzlich erlaubt.

gesendet. Der Fremdagent übernimmt für den mobilen Knoten die Rolle eines Default-Routers. Er nimmt die Datagramme entgegen und schickt sie per Standard-IP-Routing weiter zum korrespondierenden Host (Schritt 5). Dabei wird stets die Home-Adresse des mobilen Knotens als Quelladresse (source address) im Datagrammkopf eingetragen. Für den Korrespondenten des mobilen Knotens ist das Dreieck-Routing an keiner Stelle sichtbar.

Bei Anwendung des Co-Located-CoA-Verfahren können die Schritte 3 und 4 übersprungen werden. Der mobile Knoten muss auf dem Link lokalisiert sein, der durch das Netzwerk-Prefix der Care-of-Adresse identifiziert ist. Der Heimagent sendet die weiterzuleitenden Datagramme direkt zum mobilen Knoten. Der mobile Rechner wiederum antwortet dem Korrespondenten ohne Überbrückung durch den Fremdagenten per Standard-IP-Routing.

3.4 Mobile IP-Dienste

Zur Unterstützung des vorgestellten Routingverfahrens stellt Mobile IP eine Reihe von spezifischen Diensten bereit. Zunächst müssen sich sowohl der mobile Knoten als auch der Fremdagent von der Existenz des anderen in Kenntnis setzen. Dies geschieht mit Hilfe der Agentensuche (Abschnitt 3.4.1). Sobald der mobile Knoten erfahren hat, in welchem Netz er sich befindet und wer sein aktueller Fremdagent ist, muss er seinen Heimagenten über den aktuellen Standort informieren und sich dort registrieren (Abschnitt 3.4.2). Die Weiterleitung von Datagrammen durch den Heimagenten an den mobilen Knoten erfolgt mittels eines Tunnelungsverfahrens (Abschnitt 3.4.3). Es folgen Mechanismen zur Optimierung des Mobile-IP-Routingverfahren durch eine Verkürzung des Datagrammweges (Abschnitt 3.4.4) und zur Verbesserung der Sicherheit (Abschnitt 3.4.5).

3.4.1 Agentensuche

Heim- und Fremdagenten müssen ihre Verfügbarkeit für mobile Knoten sichtbar machen. Ebenso sollten mobile Knoten in der Lage sein, entsprechende Informationen zu erfragen. "Agent Discovery is the method by which a mobile node determines whether it is currently connected to its home network or to a foreign network" [Perkins 2002]. Der Agent-Discovery-Mechanismus ermöglicht es dem mobilen Knoten zu erkennen, ob dieser sich in seinem Heim- oder Fremdnetzwerk befindet und ob er in ein anderes Fremdnetzwerk gewechselt ist. Zudem kann der mobile Knoten mittels einer Agent-Discovery-Nachricht die aktuelle Care-of-Adresse erfahren. ,,When connected to a foreign network, the methods [...] also allow the mobile node to determine the foreign agent care-of address [...]" [Perkins 2002].

Mobilitätsagenten (Fremd- und Heimagenten) geben ihre Anwesenheit über sogenannte Agent-Advertisement-Nachrichten bekannt. Agent-Advertisement-Nachrichten werden periodisch (z.B. jede Drittelsekunde) via IP-Multicast an alle angeschlossenen Links gesendet. Vorausgesetzt ein mobiler Knoten hat auf Host-to-Network-Ebene Kontakt mit dem Mobilitätsagenten hergestellt, so erhält er diese Nachricht und kann daraufhin feststellen, ob er sich in seinem Heim- oder in einem Fremdnetzwerk befindet. Mittels ei-

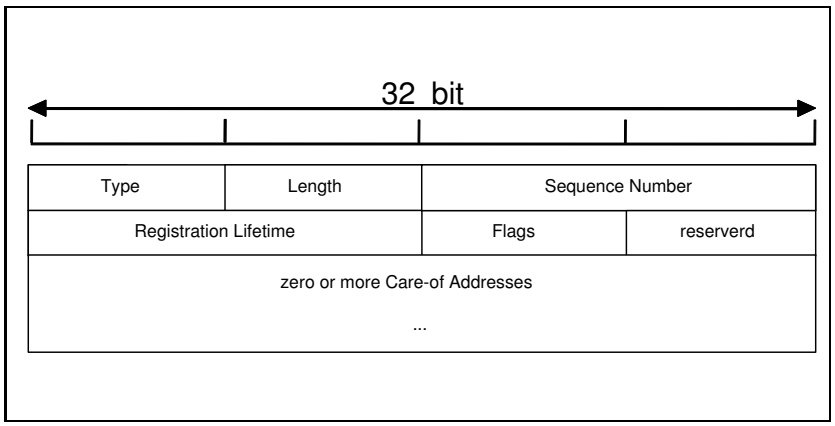

Abbildung 9: Mobility Agent Advertisement Erweiterung

ner Agent-Advertisement-Nachricht gibt der Mobilitätsagent wichtige Routerparamenter und spezifische Optionsparamenter bekannt. Diese sind im Einzelnen:

- Informationen darüber, ob der Router die Funktion eines Heim- oder Fremdagenten übernehmen kann.
- Informationen über eine eventuelle Überlastung des Mobilitätsagenten.
- Informationen darüber, ob minimale Kapselung unterstützt wird (siehe Abschnitt 3.4.3).
- Informationen über den Zwang zur Registrierung bei einem Fremdagenten.
- Informationen über Default-Router.
- Ein Pool von Care-of-Adressen, welche von Mobilen Knoten benutzt werden können.

Optional kann ein mobiler Knoten mit Hilfe einer Agent-Solicitation-Nachricht Mobilitätsagenten dazu auffordern, eine Agent-Advertisement-Nachricht zu senden, um so herauszufinden, ob ein Agent auf dem Link Mobile-IP-Dienste anbietet. Wobei weder Agent-Advertisement- noch Agent-Solicitation-Nachrichten authentifiziert werden müssen.

Mobile IP definiert Agent-Advertisement- und Agent-Solicitation-Nachrichten über Erweiterungen der klassischen ICMP-Nachrichten (ICMP Router Discovery), die im RFC 1256 spezifiziert sind. Den Unterschied zwischen einer herkömmlichen ICMP- und einer Mobile-IP-Agent-Discovery-Nachricht erkennt ein Router bzw. Host nur über die Länge der ICMP-Nachricht (Existenz einer Erweiterung). Der Aufbau einer Mobility-Agent-Advertisement-Erweiterung ist in Abbildung 9 dargestellt. Hinter dem Flag-Feld verstecken sich 7 Parameter, die gesetzt werden können (ein Bit ist reserviert). Sie enthalten die oben bereits aufgelisteten Paramenterinformationen. Jede Agent-Advertisement-Nachricht besitzt ein Registration Lifetime-Feld, welches angibt, wie lange (gemessen in Sekunden) ein Agent bereit ist Registrierungsanfragen anzunehmen. Empfängt ein

mobiler Knoten bis zum Ablauf dieser Lifetime keine Agent-Advertisement-Nachricht, so muss er davon ausgehen, den Kontakt zum Mobilitätsagenten verloren und somit das IP-Segment des Fremdagenten verlassen zu haben. Etwa er sendet daraufhin eine Agent-Solicitation-Nachricht aus, um neue Agenten zu finden, oder er hat bereits vor dem Auslauf der Lifetime eine neue Agent-Advertisement-Nachricht erhalten und registriert sich im nächsten Schritt bei diesem neuen Agenten.

3.4.2 Registrierung

Befindet sich ein mobiler Knoten in einem Fremdnetzwerk, so muss er sich bei seinem Heimagenten registrieren. ,,Mobile IP registration provides a flexible mechanism for mobile nodes to communicate their current reachability information to their home agent" [Perkins 2002]. Im Rahmen der Registrierung erzeugt bzw. modifiziert der Heimagent die Einträge in der Verbindungstabelle (Binding Table). Dies betrifft die Zuordnung der Heimadresse des mobilen Knotens zur aktuellen Care-of-Adresse für eine bestimmte Zeitdauer (Lifetime). Im Einzelnen bietet der Registrierungsdienst von Mobile IP folgende Teildienste:

- Informierung des Heimagenten über die aktuelle Care-of-Adresse.
- Initiierung der Weiterleitung von Datagrammen vom Heimagenten zum mobilen Rechner.
- Erneuerung einer Registrierung, deren Zeit abläuft.
- Deregistrierung des mobilen Rechners bei Wiederkehr in das Heim-Netzwerk.

In der Spezifikation des Protokolls werden zudem folgende, optionale Registrierungsdienste genannt. Ein mobiler Knoten kann mit einer Registierungsnachricht die IP-Adresse des Heimagenten erfragen, falls er diese nicht kennt. Er kann mehrere Care-of-Adressen simultan registrieren, so dass Datagramme vom Heimagenten an alle registrierten Adressen weitergeleitet werden. Auch ist es möglich über Registrierungsnachrichten einzelne CoA zu deregistrieren während andere CoA weiter genutzt werden können.

Benutzt der mobile Knoten eine Foreign-Agent-CoA, so ist der Fremdagent am Registrierungsprozess beteiligt. Bei erfolgter Vergabe einer Co-located-CoA kann die Registrierung auch direkt zwischen dem mobilen Knoten und dem Heimagent erfolgen. Beide Prozeduren erfordern einen Austausch von Registration-Request- Registration-Reply-Nachrichten. Alle Registrierungsnachrichten nutzen das User Datagram Protokoll (UDP) und den Port 434.

Beim Co-located-Verfahren sendet der mobile Knoten seine Registration-Request-Nachricht direkt zum Heimagenten. Beim Foreign-Agent-Verfahren wird die Nachricht durch den Fremdagent überbrückt[25]. In einem Registration-Request wird dem Heimagenten die derzeitige CoA mitgeteilt. Er wird aufgefordert, die für den mobilen Knoten

[25] In der Registration-Request-Nachricht wird (ausnahmsweise) als Quelladresse die Interface-Adresse Fremdnetzwerk und nicht die Heimadresse angegeben.

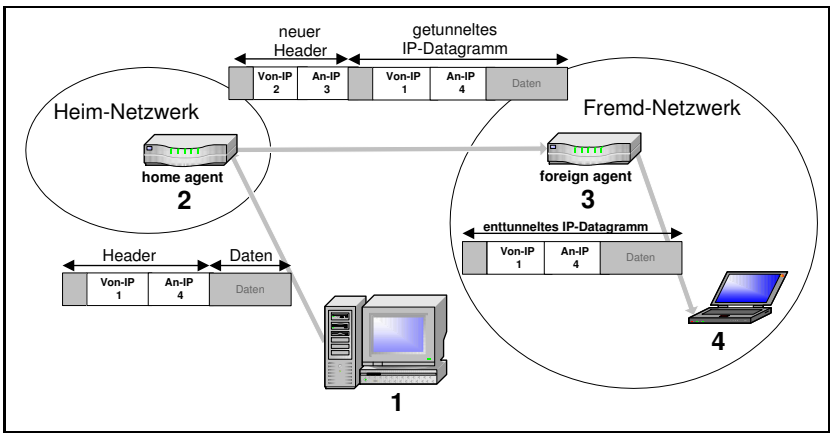

Abbildung 10: Mobile IP Tunneling

bestimmten Datagramme weiterzuschicken. Auch die Registrierung hat eine Lebenszeit, welche vom mobilen Knoten festgelegt wird und vom Heimagenten, falls dies nötig ist, verkleinert werden kann. Läuft die Lebenszeit des Eintrags ab, so wird er vom Heimagenten gelöscht. Um einen Eintrag zu verlängern, muss erneut eine Registration-Request-Nachricht gesandt werden. Zur Derigistrierung bei Heimkehr in das Heimnetzwerk, sendet der mobile Knoten eine Registration-Request-Nachricht mit der Lifetime 0 an den Heimagenten. In der Registration-Reply-Nachricht kann der Heimagent den Request ablehnen oder akzeptieren. Außerdem wird dem mobilen Knoten mitgeteilt, welche Zeitdauer in der Verbindungstabelle eingetragen worden ist.

Damit ein Mindestmaß an Sicherheit eingehalten werden kann, schreibt der RFC 3344 vor, dass über ein Authentifizierungsverfahren die Identität des Absenders einer Registrierungsnachricht sichergestellt sein muss. Hierzu wird eine sogenannte Mobility Security Association zwischen den beteiligten Mobilitätsagenten vereinbart. Die Umsetzung dieses Verfahrens wird in Abschnitt 3.4.5 dieser Arbeit erläutert.

3.4.3 Tunneling

Sobald der Heimagent eine Care-of-Adresse registriert hat, beginnt dieser mit der Weiterleitung der an den mobilen Knoten gerichteten Datagramme. Dabei wird das sogenannte Tunnelungsverfahren angewandt[26] [Perkins 1996]. Zur Definition eines Tunnels heißt es im RFC 3344: ,,The path followed by a datagram while it is encapsulated" [Perkins 2002]. Ein IP-Datagramm wird in einem neuen IP-Datagramm gekapselt. Das bedeutet, der kapselnde Agent fügt einen zusätzlichen 24 Byte großen IP-Header vor das ursprüngliche Datagramm. ,,The model is that, while it is encapsulated, a datagram is routed to a knowledgeable decapsulation agent, which decapsulates the datagram and then correctly delivers it to its ultimate destination." [Perkins 2002]. Der Tunnel beginnt beim Heimagenten und endet beim Interface, das durch die Care-of-Adresse identifiziert ist. In

[26]Das Tunneling- bzw. IP-Kapselungsverfahren wird im RFC 2003 beschreiben.

Abbildung 10 wird das Tunnelungsverfahren bei Existenz eines Fremdagenten, d.h. bei Vergabe der Care-of-Adresse über den Fremdagenten dargestellt(Foreign-Agent-CoA). Endet hingegen der Tunnel direkt beim mobilen Knoten, so muss dieser selbst das Datagramm entkapseln können (Co-located-CoA).

Mobile IP lässt zusätzlich eine mehrstufige Tunnelung von Datagrammen (Kaskadierung) zu. So ist es möglich, dass der Fremdagent selbst ein mobiler Knoten ist. Dies ist z.B. der Fall, wenn ein mobiler Knoten sich in einem Flugzeug befindet und sich bei einem Fremdagenten des Flugzeugnetzwerkes registrieren läßt. Der Fremdagent des Flugzeugnetzwerkes ist wiederum ein mobiler Knoten und registriert sich auf seinem Weg bei unterschiedlichen Fremdagenten. Der mobile Fremdagent gibt den registrierten mobilen Knoten in einer Agent-Advertisement-Nachricht dabei stets seine eigene Heimadresse als Care-of-Adresse an. Auf diese Weise lassen sich mobile Subnetze realisieren. Allerdings wird mit jeder weiteren Stufe der Kaskadierung ein zusätzlicher Tunnel benötigt, der die einzelnen IP-Datagramme größer macht (Ergänzung weiterer Header) und den Weg der Datagramme verlängert (mehrfaches Triangular Routing).

Zur Erhöhung der Effizienz beim Tunneling wurde 1997 von der Mobile IP Working Group ein Verfahren zur minimalen Kapselung vorgeschlagen (RFC 2004) [Perkins 1996]. Beim normalen Verfahren gemäß RFC 2003 wird ein vollständiger, 24 Byte großer Header ergänzt [Perkins 1996]. Äußerer und innerer Header enthalten dabei viele redundante Informationen. Als zusätzlich Information werden jedoch lediglich zwei neue IP-Adressen benötigt, also 8 Byte. Bei der Minimierung wird der ursprüngliche Header modifiziert und um einen 8 bis 12 Byte großen Headeranhang ergänzt. Die alten Quell- und Zieladressen werden durch die neuen Adressen ersetzt und dafür in den Anhang des Headers geschrieben[27] [Perkins 1996].

3.4.4 Routingoptimierung

Das Dreieck-Routing führt zu einer Mehrbelastung des Netzwerkes und der beteiligten Router. Im Extremfall befinden sich der Korrespondent und der mobile Knoten im selben Netzwerk und Datagramme werden dennoch umständlich über einen weit entfernten Heimagenten geroutet. Die Transparenz des Mobile-IP-Routing für den Korrespondenten musste quasi mit Effizienzverlusten erkauft werden. Zur Optimierung des Routing und Lösung dieses Problems hat die Mobile-IP-Working-Group im Februar 2000 einen Internet-Draft mit dem Titel ,,Route Optimization in Mobile IP"[28] veröffentlicht. In ihm werden insbesondere Route-Optimization-Nachrichten und -Erweiterungen zum Basisprotokoll definiert: ,,Using these protocol extensions, correspondent nodes may cache the binding of a mobile node, and then tunnel their datagrams for the mobile node directly to the care-of address, bypassing the mobile node's home agent" [Perkins, Johnson 2000]. D.h. Hosts, welche Routingoptimierung beherrschen, haben die Möglichkeit, die aktuelle CoA eines mobilen Knotens zu speichern. Routingoptimierung erfordert deshalb eine Erweiterung der Fähigkeiten von Mobilitätsagenten. Damit wird allerdings von dem

[27] Fragmentierte Datagramme dürfen nicht minimal gekapselt werden.

[28] Quelle: http://www.ietf.org/proceedings/00jul/I-D/mobileip-optim-09.txt. Route Optimization liegt z.Zt. noch nicht als RFC vor.

Grundsatz der Basisspezifikation abgewichen, dass die Fähigkeiten der Korrespondenten mobiler Knoten nicht erweitert werden müssen.

Darüber hinaus kann mit Hilfe der Routingoptimierung der Übergang des mobilen Knotens von Netzwerk zu Netzwerk nahtloser gestaltet werden, indem vermieden wird, dass bereits versandte Datagramme verworfen werden müssen (Smooth Handoff). ,,Extensions are also provided to allow datagrams in flight when a mobile node moves, and datagrams sent based on an out-of-date cached binding, to be forwarded directly to the mobile node's new binding"[Perkins, Johnson 2000]. Die Routingoptimierung übernimmt somit zwei Aufgaben:

1. Für korrespondierende Rechner wird ein Binding-Cache gepflegt.

2. Zwischen Fremdagenten wird ein Smooth-Handoff-Mechanismus implementiert.

Alle diesbezüglich notwendigen administrativen Nachrichten werden - wie bereits bei der Registrierung - über UDP und den Port 434 versandt. Auch die erforderliche Authentifizierung der Nachrichten erfolgt wie bei der Registrierung[29].

Ein Korrespondent des mobilen Knotens sendet zunächst seine Datagramme an den Heimagenten. Dieser tunnelt die Datagramme zur CoA und schickt nun zusätzlich eine Binding-Update-Nachricht an den Korrespondenten. Nach der Authentizitätsprüfung bestätigt der Korrespondent mit einer Binding-Acknowledge-Nachricht den Erhalt der Nachricht und speichert die aktuelle CoA des mobilen Knoten ein seinem Binding-Cache. Dieser Eintrag wird wiederum mit einer Lebenszeit versehen. Wechselt der mobile Knoten das Netzwerk, so wird zunächst der Heimagent über eine Binding-Warning-Nachricht informiert. Sobald der Heimagent die neue CoA kennt, schickt er dem Korrespondenten eine Binding-Update-Nachricht.

Das effizienzverbessernde Überspringen des Heimagenten bringt jedoch Nachteile beim Netzwerkwechsel (Handoff) des mobilen Knotens mit sich. Datagramme werden kurzzeitig fehlgeleitet. Diese Situation tritt auf, wenn der mobile Knoten sein altes Netzwerk verlassen hat und bei einem neuen Fremdagenten bereits frisch registriert ist, jedoch bei seinem alten Fremdagent aufgrund der noch nicht abgelaufenen Lebenszeit weiterhin eingetragen ist. Datagramme, die der Korrespondent an die verfallende CoA sendet, müssen in diesem Fall umständlich über den Heimagenten geroutet werden, damit sie ankommen können.

Zur Beseitigung dieses Nachteils wird das Verfahren des Foreign-Agent-Smooth-Handoff vorgeschlagen. Gemeinsam mit der Registrierung bei einem neuen Fremdagent fordert der mobile Knoten diesen auf, eine Binding-Update-Nachricht an den alten Fremdagenten zu schicken. Der ursprüngliche Fremdagent bestätigt diese Nachricht daraufhin direkt beim mobilen Knoten. Er hebt die Registrierung des mobilen Knoten umgehend auf, obwohl die Lebenszeit des Eintrags noch nicht abgelaufen ist. Eine Fehlleitung wird vermieden. Smooth Handoff hat den Vorteil, dass der unter Umständen weit entfernte Heimagent hierbei nicht einbezogen werden muss. Das hat ist für die Unterstützung von Streaming-Audio/Video und Voice-over-IP-Anwendungen besonders wichtig.

[29] Zwischen mobilem Knoten, Heimagent und Korrespondent muss eine Mobility Security Association vereinbart werden. Nähere Informationen hierzu werden in Abschnitt 3.4.5 gegeben.

3.4.5 Sicherheit

Bei Mobile IP entsteht ein erhöhtes Sicherheitsproblem durch die Offenheit des Benutzerkreises und der Netzstruktur. Die folgende Liste gibt einen kurzen Überblick über die wesentlichen Einzelprobleme.

- Autentizitätsproblem: Vortäuschung einer falschen Identität.
- Zugriffssteuerungsproblem: Unbefugte Kommunikation bzw. unbefugter Datenzugriff.
- Vertraulichkeitsproblem: Unerlaubtes Abhören von Nachrichten.
- Integritätsproblem: Unerlaubte Verfälschung von Nachrichten.
- Verbindlichkeitsproblem: Der Sender kann nicht nachweisen, dass der Empfänger die Daten erhalten hat.
- Verfügbarkeitsproblem: Behinderung des Dienstangebots.

In der Protokollspezifikation von Mobile IPv4 (RFC 3344) wird lediglich auf die Gefahr der Vortäuschung einer falschen Identität eingegangen. Das Problem wird im Zusammenhang mit der Registrierung (siehe Abschnitt 3.4.2) thematisiert. ,,The registration protocol described in this document will result in a mobile node's traffic being tunneled to its care-of address. This tunneling feature could be a significant vulnerability if the registration were not authenticated" [Perkins 2002]. Registrierungsdatagramme müssen somit immer authorisiert sein. Zu diesem Zweck wird zwischen dem mobilen Knoten und dem Heimagenten eine sogenannte Mobility Security Association vereinbart, welche aus den folgenden drei Bestandteilen aufgebaut ist:

1. Authentifikationsalgorithmus
2. Geheime(r) Schlüssel
3. Sicherungsalgorithmus gegen Replay-Angriffe

Mobiler Knoten und Heimagent halten diese Informationen geheim und übermitteln stets nur einen 4 Byte langen Security Parameter Identifier (SPI), der die gültige Mobility Security Association identifiziert. ,,The SPI selects the authentication algorithm and mode [...] and secret (a shared key, or appropriate public/private key pair) used in computing the Authenticator" [Perkins 2002].

Als Default-Algorithmus zur Authentifikation wird im RFC 3344 ein HMAC-MD5-Algorithmus festgelegt. Andere Algorithmen sind aber erlaubt. MD5 ist ein in Authentifikationsprotokollen verwendeter Algorithmus, der auf einer Einwegübertragung mittels Hash-Funktion und eines Schlüssels basiert. Daher können aus dem Ergebnis keine Rückschlüsse auf den Schlüssel erfolgen. Dem Verfahren nach wird aus einer beliebig langen Nachricht eine 128 Bit lange Information, der so genannte Message Digest, gebildet,

der an die unverschlüsselte Nachricht angehangen wird. Der Empfänger vergleicht den Message Digest mit dem von ihm aus der Information ermittelten Wert. Bei Mobile-IP-Registrierungen wird die 128-Bit-MD5-Prüfsumme über alle Registrierungsdaten und den geheimen Schlüssel gebildet. Die Prüfsumme wird dann zusammen mit dem SPI jedem Registrierungsdatagramm angehängt.

Authentifikation kann nicht nur zwischen dem mobilen Knoten und Heimagent stattfinden, sondern auch zwischen dem mobilen Knoten und Fremdagent oder Heimagent und Fremdagent. Hierbei werden dieselben Mechanismen benutzt.

Der Sicherungsalgorithmus ist erforderlich, da ein Angreifer ohne weiteres die Registrierungsanfragen eines mobilen Knotens abhören könnte, um sie später ein weiteres mal zu versenden (Replay Attack). Vermieden wird eine solche Gefahr durch Sicherstellung der Einmaligkeit des Inhalts einer Registrierungsanfrage. Hierzu werden zwei Verfahren vorgestellt.

Das Time-Stamp-Verfahren sieht einen individuellen Zeitstempel für jede Registrierungsnachricht vor. Die involvierten Mobilitätsagenten müssen hierzu zeitsynchronisiert sein. Da jedoch über spezielle Protokolle (z.B. NTP) die Zeiteinstellung beeinflussbar ist, ist dieses Verfahren nicht sicher.

Das Pseudo-Zufallszahlen-Verfahren arbeitet mit einer 32-Bit Zufallszahl. Die beteiligten Mobilitätsagenten müssen dabei ihre Zufallszahlenreihe synchron halten. Dieses Verfahren ist sicherer als die Time-Stamps-Methode, jedoch ebenfalls angreifbar. Letztlich ist die Stärke eines Authentifikationsmechanismuses abhängig von vielen Faktoren, die nicht in der nötigen Ausführlichkeit in dieser Arbeit besprochen werden können.

Zur Lösung der anderen Sicherheitprobleme werden im RFC 3344 keine Festlegungen getroffen bzw. Vorschläge unterbreitet. ,,Users who have sensitive data that they do not wish others to see should use mechanisms outside the scope of this document (such as encryption) to provide appropriate protection" [Perkins 2002].

3.5 Mobile IPv4 vs. Mobile IPv6

Wie die Mobile IP Working Group vorgeschlagen hat, richtet sich die Mobilitätsunterstützung für IPv6 an dem Design von Mobile IPv4 aus. Mobile IPv6 nutzt ebenfalls das Tunnelungsverfahren, um Datagramme vom Heimnetzwerk zum mobilen Knoten zu routen. Bei IPv6 konnte ist im Gegensatz zu IPv4 von Anfang der Entwicklung an eine Mobilitätsunterstützung berücksichtigt worden. Sie ist aus diesem Grund ein inhärenter Bestandteil von IPv6.

Eine wichtige Verbesserung des Designs von Mobile IPv6 geht auf den bei IPv6 neu hinzugekommenen Autokonfigurationsdienst zurück. Die IP-Konfiguration eines Knoten bei IPv6, d.h. die Vergabe von IP-Adressen, die Einstellungen von Subnetzmasken und Nameservern läuft automatisiert ab. Dafür nutzt IPv6 einen Nachbarschaftserkennungsdienst (neighbor discovery), der auch bei Mobile IPv6 genutzt wird. Der Nachbarschaftserkennungsdienst liefert für einen neuen Knoten im Netz alle notwendigen Parameter zurück, um im Netzwerk auf IP-Ebene eingebunden werden zu können. Ein mobiler Knoten kann also in Fremdnetzwerken mit diesem Dienst eine Care-of-Adresse selbst anfordern, ohne einen Fremdagenten oder einen DHCP-Server fragen zu müssen.

Ein Fremdagent ist bei Mobile IPv6 nicht vorgesehen. Durch den wesentlich größeren Adressraum bei IPv6 entstehen anders als bei IPv4 außerdem keine Probleme bei der Vergabe von Co-located-CoA.

Einen weiteren Vorteil bietet Mobile IPv6 durch die Einbeziehung der Routingoptimierung in den Standard. Das bedeutet, der mobile und der korrespondierende Knoten können bei Mobile IPv6 kommunizieren, ohne den Heimagenten einbeziehen zu müssen.

Außerdem bietet IPv6 eine bessere Unterstützung der Authentifizierung. Sicherheitsinformationen zur Authentifizierung werden bei IPv6 in einer Erweiterung des IP-Headers berücksichtigt und sind somit nicht, wie bei IPv4, ein Teil des Datenpakets (Payloads).

3.6 Umsetzungsbeispiele

Es existieren eine Reihe von frei verfügbaren Implementierungen von Mobile IP. Abbildung 11 gibt einen kurzen Überblick darüber. Neben der Unterscheidung der einzelnen Betriebssysteme spielt auch die Aktualität der entsprechenden Versionen eine Rolle. Beide Informationen sind jeweils abgebildet. Die aufgeführten Beispiele sind, mit Ausnahme der Implementierung von SUN Microsystems, aus universitären Forschungsprojekten hervorgegangen. Die erste industrielle Mobile-IP-Lösung wurde 2001 von Nortel Networks und Qualcomm vorgestellt[30]. Es handelt sich hierbei um eine Anwendung von Mobile IPv4 in einem CDMA2000-Netzwerk. CDMA2000 ist ein Mobilfunknetz der dritten Generation (3G), das von der Organisation 3GPP2 und speziell für den nordamerikanischen Raum entwickelt worden ist. CDMA2000 unterstützt Sprachdienste und paketorientierte Datenübertragung. Der Einsatz von Mobile IP ermöglichst es Nutzern des Datendienstes, von einem 3G-Paket-Netzwerk zu einem anderen zu wandern, ohne dass die Verbindung unterbrochen werden muss.

Weitere kommerzielle Mobile-IP-Lösungen, die sich nach dem vorgestellten ,,Proposed Standard" richten, gibt es von Flarion Technologies[31], Birdstep Technology[32], ipUnplugged[33] und Airvana[34] (letztere für 3GPP2 bzw. CDMA2000). Zwar basieren diese Anwendungen auf dem Standard, jedoch weisen alle Lösungen Erweiterungen zur Verbesserung der Sicherheit und zur Erhöhung der Handoff-Geschwindigkeit auf.

4 Zusammenfassung

Mobile IP realisiert ein Mobilitätsmanagement auf der Vermittlungsebene. Es stellt eine Schlüsseltechnologie für viele mobile Anwendungen dar und bietet eine Möglichkeit zur Realisierung nahtloser Mobilität. Seit 1994 wird an der Entwicklung von Mobile IP gearbeitet. Es ist jedoch nach wie vor nicht standardisiert.

[30] Nähere Informationen sind z.B. auf der Webseite http://www.qualcomm.com/press/pr/releases2001/press57.html zu finden.
[31] http://www.flarion.com/
[32] http://www.birdstep.com/
[33] http://www.ipunplugged.com/
[34] http://www.airvananet.com/

Betriebs-system	IP-Version	Version	Organisation	Mobile IP Lösung
Linux	IPv4	2.2.x	Stanford University	MosquitoNet Mobile IP
			Helsinki University of Technology	Dynamics HUT Mobile IP
		2.0.x	Portland State University	Secure IP Mobile Networking
			State University of New York	Binghamton
		2.0.37	University of Singapore	NUS Mobile IP
		2.0.34	University of Singapore	NUS Mobile IP
			SUN Microsystems	SUN Mobile IP
	IPv6	2.1.9x	Lancaster University	Lancaster Mobile Ipv6 Package
		2.1.59	University of Singapore	NUS Mobile IP
FreeBSD	IPv4	3.3	Carnegie Mellon University	Monarch
		2.2.6	Portland State University	Secure MIP
	IPv6	3.3	Inria	Inria HMIPv6
Solaris	IPv4	2.5.1	SUN Microsystems	SUN Mobile IP
Windows	IPv4	NT 4.0	Politehnica University of Bucharest (zusammen mit GMD Fokus Berlin)	Politehnica University of Bucharest
			National University of Singapore	NUS Mobile IP
		95	National University of Singapore	NUS Mobile IP

Abbildung 11: Überblick bekannter Mobile IP Implementierungen

Mobile IP arbeitet mit neuen Architekturkomponenten, unter denen eine Arbeitsteilung besteht. Allerdings basieren die Mechanismen von Mobile IP größtenteils auf bereits etablierten Verfahren (z.B. IP-in-IP-Kapselung und Verschlüsselungsverfahren). Das Protokoll ist in der Basisversion so spezifiziert worden, dass die Mobilität des Kommunikationspartners für Korrespondenten völlig transparent bleibt. Es ist auch keine zusätzliche Implementierung von Software auf dem System des Korrespondenten erforderlich. Zur Optimierung des Routings müssen jedoch Erweiterungen auf den Hosts implementiert werden.

Als Basis ist IPv6 in vielen Punkten besser geeignet als IPv4. Wobei die bisherigen Implementierungen in erster Linie Mobile-IPv4-Lösungen sind. Die ersten dokumentierten kommerziellen Implementierungen erfolgten in den Jahren 2001 und 2002. Alle bisherigen Anwendungen weisen spezielle und vom vorgestellten Standard abweichende Lösungen zur Verbesserung der Routingeffizienz und der Sicherheit auf. Die größte Herausforderung im Zusammenhang mit Mobile IP stellt die Sicherheit dar. Die grundlegende Architektur von Mobile IP sorgt für systemimmanente Schwachstellen, die selbst durch aufwändige Maßnahmen nur abgeschwächt, nicht aber vollständig beseitigt werden können. Neben konzeptionellen Problemen gilt es auch eine Reihe praktischer Hürden zu nehmen. Beispielsweise die Unverträglichkeit von Firewall-gesicherten Netzwerken mit dem Mobile IP. Ein bedeutender ,,Durchbruch" der Mobile-IP-Technologie wird erst mit der flächendeckenden Einführung von IPv6 erwartet. Dies wird für die Jahre 2005 und 2006 vorausgesagt.

Literatur

[BITKOM 2003] BITKOM: Wege in die Informationsgesellschaft: Status Quo und Perspektiven Deutschlands im internationalen Vergleich. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. Oktober (2003)

[Deering, Hinden 1998b] Deering, S., Hinden, R.: Internet Protocol, Version 6 (IPv6) Specification. Internet Society. **RFC 2460**. Dezember (1998)

[Deering, Hinden 2003] Deering, S., Hinden, R.: Internet Protocol Version 6 (IPv6) Adressing Architecture. Internet Society. **RFC 3513**. April (2003)

[Droms 1997] Droms, R.: Dynamic Host Configuration Protocol. Internet Society. **RFC 2131**. März (1997)

[Graumann 2002] Graumann, S.: Monitoring Informationswirtschaft. 5. Faktenbericht 2002. NFO World Group im Auftrag des Bundesministeriums für Wirtschaft und Arbeit. Oktober (2002)

[Patil 2003] Patil, B.: IP Mobility Ensures Seamless Roaming. Communication Systems Design. http://img.cmpnet.com/commsdesign/csd/2003/feb03/feat1-feb03.pdf . Download am 20.03.2003. Februar (2003)

[Perkins 1994] Perkins, C.: IPng Mobility Considerations. Internet Society. **RFC 1688** (1994)

[Perkins 1996] Perkins, C.: IP Mobility Support. Internet Society. **RFC 2002**. Oktober (1996)

[Perkins 1996] Perkins, C.: IP Encapsulation within IP. Internet Society. **RFC 2003**. Oktober (1996)

[Perkins 1996] Perkins, C.: Minimal Encapsulation within IP. Internet Society. **RFC 2004**. Oktober (1996)

[Perkins 2002] Perkins, C.: IP Mobility Support for IPv4. Internet Society. **RFC 3344**. Nokia Research Center. August (2002)

[Perkins, Johnson 2000] Perkins, C., Johnson, D.B.: Route Optimization in Mobile IP. Mobile IP Working Group. Februar (2000)

[Postel 1980] Postel, J.: Transmission Control Protocol. STD7. Internet Society - USC/Information Sciences Institute. **RFC 761**. January (1980)

[Postel 1980] Postel, J.: User Datagram Protocol. STD6. Internet Society - USC/Information Sciences Institute. **RFC 768**. August (1980)

[Postel 1981] Postel, J.: Internet Protocol. STD5. Internet Society - USC/Information Sciences Institute. **RFC 791**. September (1981)

[Simpson 1994] Simpson, W.: IPng Mobility Considerations. Internet Society - Daydreamer. **RFC 1688**. August (1994)

[Stahlknecht, Hasenkamp 2002] Stahlknecht, P., Hasenkamp, U.: Einführung in die Wirtschaftsinformatik. 10. Auflage. Springer-Verlag. Berlin et. al. (2002)

[Tannebaum 2000] Tannebaum, A. S.: Computer-Netzwerke. 3. Auflage. Markt & Technik Buch- und Sofware Verlag. München (2000)

[Washburn, Evans 1994] Washburn, K., Evans, J.: TCP/IP: Aufbau und Betrieb eines TCP/IP-Netzes. Addison-Wesley. Bonn et. al. (1994)

[Weiser 1991] Weiser, M.: The Computer for the 21st Century. Scientific American. Vol. 265. No. 3. September (1991) S. 94-104

A IPv4 Headerfelder

Version (Länge = 4 Bits): Der Wert im Version-Feld bezeichnet das Format des Internet Headers, in diesem Fall Version 4.

IHL (Länge = 4 Bits): Internet Header Length (IHL) gibt die Länge des Internet Headers in 32-Bit-Worten an und zeigt auf den Anfang des Datenteils. Der Wert ist mindestens 5 und wird bei jedem Knoten neu berechnet.

Type of Service (Länge = 8 Bits): Die ersten drei Bits beschreiben die gewünschte Priorität mit der die Daten durch ein Netzwerk geleitet werden sollen [z.B. 001 Priority, 000 Routine]. Mit den Bits 4,5 und 6 werden Angaben zur gewünschten Behandlung des Datagramms gemacht. Es besteht ein Trade-off bei dieser Festlegung zwischen geringer Verzögerungszeit, hoher Zuverlässigkeit und geringer Durchlaufzeit. Die Bits 7 und 8 sind frei.

Total Length (Länge = 16 Bits): Gesamtlänge des Datagramms, gemessen in Byte (daraus folgt: 2*16 = 65.535 Byte maximal). Mindestgröße der von Hosts akzeptierten Datagramme = 576 Bytes.

Identification (Länge = 16 Bits): Wird zusammen mit der Source-, Destination-Adress- und dem Protocol-Feld genutzt, um Datagrammfragmente bei der Wiederzusammensetzung zu identifizieren.

Flags (Länge = 3*1 Bit): Bit 1 ist immer 0 (reserviert). Bit 2 gibt an, ob das Datagramm fragmentiert werden darf (0=ja, 1=nein). Bit 3 gibt an, ob es das letzte Fragment eines Ursprungsdatagramms ist (0=ja, 1=nein).

Fragment Offset (Länge = 13 Bits): Gibt an, an welche Stelle das Fragment in einem Datagramm gehört, relativ zu dem Beginn des unfragmentierten Originaldatagramms.

Time to Live (Länge = 8 Bits): Gibt die maximale Lebenszeit an, die ein Datagramm auf dem Weg durch das Netz haben darf. Bei jedem Verarbeitungsschritt auf einem Host wird die Lebenszeit um mindestens eine Sekunde verringert (auch wenn dies weniger als eine Sekunde gedauert hat). Bei Wert 0 muss das Datagramm zerstört werden.

Protocol (Länge = 8 Bits): Zeigt das im Datenteil des Datagramms verwendete, höhere Protokoll an.

Header Checksum (Länge = 16 Bits): Ausschließlich für den Headerteil vorgesehene Prüfsumme. Wird berechnet als 16-Bit-Komplement der Komplementsumme aller 16-Bit-Wörter im Header.

Source Address (Länge = 32 Bits): Gibt die IP-Adresse des sendenden Knotens an. Sie wird meistens als eine Vierergruppe von Dezimalzahlen, die durch drei Punkte getrennt sind, dargestellt.

Destination Address (Länge = 32 Bits): Gibt die IP-Adresse des Zielknotens an.

Options (Länge ist variabel): Hier gibt es zwei Möglichkeiten. Es wird entweder nur ein Byte zur Festlegung des Options-Typ genutzt, oder ein Byte zu diesem Zweck, ein weiteres Byte für die Options-Länge, plus die eigentlichen Options-Daten. Es können spezielle Optionen zu Sicherheitseinstellungen, Routingvorgaben vom Quellrechner an die Gateways, Pfadverfolgung und dem Setzen von Zeitstempeln eingesetzt werden.

Padding (Länge ist variabel): Das Padding-Feld stellt lediglich sicher, dass der Header mit einem ganzen 32-Bit-Wort aufhört. Die Padding-Bits sind Null.

B IPv6 Headerfelder

Version (4 Bits): Beschreibt das Format des Internet Headers (hier Version 6).

Traffic Class (8 Bits): Traffic class gibt einen Wert an, mit dem Router zwischen unterschiedlichen Klassen oder Prioritäten von IPv6-Datagrammen unterscheiden können. Die Nutzung dieses Feldes ist noch nicht vollständig geklärt.

Flow Label (20 Bits): Ein Quellrechner kann im Flow-Label-Feld Sequenzen von Paketen markieren, denen ein besonderer Service durch IPv6-Router zukommen soll (z.B. real-time-Service). Die Nutzung dieses Feldes ist noch nicht vollständig geklärt.

Payload Length (16 Bits): Länge des Datenteils, gemessen in Bytes (daraus folgt: 2**16 = 65.535 Bytes maximal). Mindestgröße der von Hosts akzeptierten Datagramme = 576 Bytes.

Next Header (8 Bits): Zeigt das im Datenteil des Datagramms verwendete höhere Protokoll an (wie bei IPv4).

Hop Limit (8 Bits): Gibt die maximale Lebenszeit an, die ein Datagramm auf dem Weg durch das Netz haben darf. Bei jedem Verarbeitungsschritt auf einem Host wird das Hop Limit um Eins verringert. Bei Wert 0 muss das Datagramm zerstört werden.

Source Address (128 Bits): 8 * zwei Byte für die Quelladresse.

Destination Address (128 Bits): 8 * zwei Byte für die Zieladresse