Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Lehrstuhl für Rechnernetze und Telematik

SS 2007

Seminararbeit

Mobile IP
ip mobility support

Jeremi Dzienian

29.01.2008

Betreut durch
Prof. Dr. rer. nat. Christian Schindelhauer
und
Arne Vater

Abstract

Das *Internet Ptotokoll (IP)* wurde entworfen, um Computer in logische Einheiten, sogenannte *Subnetze*, zu unterteilen und so addressieren zu können. Beim Entwurf ging man davon aus, nur stationäre Computer zu addressieren. Bewegt sich nun ein mobiles Gerät von einem Subnetz in ein anderes, so wird diesem eine neue *IP* zugewiesen und alle existierenden Verbindungen werden unterbrochen. Dieses Paper beschreibt das *Mobile IP*-Protokoll (*ip mobility support*), welches es erlaubt eine IP trotz Netzwechsel beizubehalten, so dass das mobile Gerät auch in fremden Netzen mit der selben *IP* erreichbar bleibt. Dabei liegt der Schwerpunkt bei *IPv4*.

Inhaltsverzeichnis

1 Einleitung

Das Protokoll *IPv4*[1], das zur Zeit Standard im westlichen Raum[2] ist, wurde entworfen, um Rechnernetze zu strukturieren und zu addressieren. Es teilt Netze in sogenannte *Subnetze* ein, so dass es möglich ist viele Rechner zu einem großem Netzwerk, dem Internet, zusammenzuschließen, ohne dass die Addressen ausgehen. Außerdem erlaubt die Strukturierung des Internets ein effizientes Routen. Nicht jeder Router muss wissen, wo ein bestimmter Zielrechner zu finden ist.

IPv4 wurde jedoch für stationäre Rechnersysteme entworfen und optimiert (→ [Com06]), so dass Mobilität nur schwerlich möglich ist.

Ein Rechner befindet sich nun meist[3] in einem *Subnetz*, in dem den einzelnen Clients Adressen aus dem Adressraum des *Subnetzes* zugewiesen werden. Was bei stationären Rechnern ideal ist, führt bei mobilen Rechnern[4] zu dem Problem, dass dieses Gerät von einem Netz in ein anderes bewegt werden kann. Das führt dann zu einem Verbindungsabbruch, da dem mobilen Rechner im neuem Netzwerk eine neue *IP-Adresse* des neuen *Subnetzes* zugewiesen wird.

Mobile IP erweitert das *IPv4 Protokoll* darin, das ein mobiles Gerät seine IP beibehalten darf, auch nachdem es das *Subnetz* gewechselt hat. Somit kann eine existierende Verbindung auch Netzwechsel überdauern. Dies geschieht dabei völlig transparent (vgl. 2.1.1), so dass die beteiligten Router nichts davon mitbekommen.

Ich beziehe mich in diesem Paper vorwiedend auch *IPv4*, da es die Grundideen einer *mobilen IP* sehr schön veranschaulicht. *Mobile IPv6* ist eine Erweiterung dieses Protokolls und hat einige Strategien verbessert, so dass z.B. das 2XProblem (2.6) nicht mehr eintritt. Allerdings ist es auch erst mit *IPv6* nutzbar, und es sieht zur Zeit nicht danach aus, als ob Europa anstalten machen würde endlich auf das neue Adressierprotokoll umzusteigen, der sicherlich Millionen, wennn nicht gar Milliarden kostten würde. Und noch macht sich

[1] IP (Internet Protocol) version 4, siehe [ISI81] oder [wik08b]

[2] aus historischen Gründen hat u.A. Europa einen recht breiten Addressraum zugewiesen bekommen, weshalb es noch nicht zur akuter Addressknappheit gekommen ist. Anders sieht es im asiatischem Raum aus; dort ist bereits heute *IPv6* am laufen. (→ [wik08c])

[3] wenn es nicht gerade ein *Gateway* oder ein Server im *WAN* ist.

[4] im allgemeinen Rechner, die über *WLAN* eingebunden sind

der IPv4 Addressbereich nicht allzu bemerkbar, wohl auch aus dem Grund, weil immer wieder neue Erweiterungen hinzugepatscht wurde.

2 Mobile IP mit IPv4

2.1 Anforderungen an das Protokoll

Die *IETF*[5] hat das *Mobile IP Protokoll* entworfen, in dem es mobilen Rechnern ermöglicht wird sich von Netz zu Netz zu bewegen und dabei ihre IP Adresse beizubehalten. Ein solches Protokoll hat, insbesondere wenn es in mobilen System Einsatz findet, bestimmte Anforderungen zu erfüllen, die *Mobile IP* auch reallisiert.

Douglas E. Comer (→ [Com06]) klassifiziert sie und nennt sie *Transparenz*, *Skalierbarkeit*, *Kompatibilität*, *Sicherheit* und *Makro-Mobilität*.

2.1.1 Transparenz

Die Mobilität ist transparent (nicht sichtbar) für alle Anwendungen, Protokolle und Router, die nicht direkt etwas mit der Reallisierung des *Mobile IP* Protokolls zu tun haben.

Außer dem mobilen Rechner selbst und dem Heimnetz müssen keine Instanzen dieses Protokoll verstehen. Genauer: Diese Instanzen bekommen nicht einmal den Einsatz dieses Protokolls mit.

2.1.2 Kompatibilität

Es werden normale *IPv4 Adressen* verwendet, so das eine Kommunikation mit und durch bestehende Netze problemlos möglich ist, auch wenn diese dieses Protokoll nicht reallisiert haben.

Kompatibilität zu bestehenden Systemen ist heutzutage Pflicht in allen Bereichen, da sich ein Umstieg auf eine völlig neue Technologie, bzw. dessen seperate Nutzung, nicht durchsetzten würde, da der administrative Aufwand und die finanzielle Belastung ungleich höher Ausfallen würde.

[5] Internet Engineering Task Force

2.1.3 Skalierbarkeit

Erlaubt Mobilität durch das (langsame) Internet, ohne exzessivem Speichergebrauch oder massiver Bandbreitennutzung. Die gesendeten Nachrichten sollten also möglichst klein sein.

Leider erfüllt das *Mobile IP Protokoll* diese Anforderung nur teilweise. (2X Problem → 2.6) Das *Mobile IPv6 Protokoll* hingegen hat dieses Problem gelöst.

2.1.4 Sicherheit

Das Protokoll muss Sicherheitskonzepte reallisieren, so dass sichergestellt werden kann, dass es sich beim mobilen Rechner auch tatsächlich um den authorisierten Rechner handelt, und nicht einem Angreifer gehört, der die gesendeten Nachrichten abfangen möchte.

2.1.5 Makro Mobilität

Es gibt verschiedene Strategien, die verfolgt werden müssen, wenn sich ein mobiler Rechner sehr schnell bewegt und somit sehr häufig in kurzen Intervallen ein Netzwechsel statt findet. Andere Strategien können genutzt werden, wenn dies nicht erforderlich ist und ein Netzwechsel pro Sekunde ausreicht.

Mobile IP realisiert die *Makro-Mobilität*, also nicht die extrem schnellen Netzwechsel. Dies trifft auf die meisten mobilen Rechner, wie Laptops, zu.

2.2 Überblick über die Funktionsweise des Protokolls

Die größte Herausforderung an das Protokoll ist die Anforderung, das ein mobiles Gerät seine *IP Adresse* behalten darf und man verhindern möchte, das jeder Router für jeden Host eine spezifische Route speichern muss.

Das *Mobile IP Protokoll* löst das Problem, in dem es eine zweite Adresse einführt, die *care-of address*, die nur gültig ist, solange sich der mobile Rechner in einem fremden Netz befindet. Die primäre Adresse (*home address*) wird nicht geändert, egal wo sich der mobile Rechner befindet, und addressiert fest das Heimatnetz. Für alle Applikationen ist nur diese erste Adresse sichtbar und bekannt.

Befindet sich das mobile Gerät im Heimatnetz, so ist nur die *home address* (primäre Adresse) gültig, und alle Addressierungen und Paketzustellungen laufen wie gewohnt. Diese *home address* wird im lokalen Netz, wie üblich, zugewiesen.

Bewegt sich nun der mobile Rechner in ein fremdes Netz, so bekommt der Rechner eine *care-of address* (sekundäre Adresse), die an den *home agent* (für gewöhnlich der Router im Heimnetz) gesendet werden muss. Dieser Agent übernimmt daraufhin den Empfang aller Nachrichten an die *home address* und tunnelt sie mittels *IP-in-IP encapsulation*[6] weiter an den mobilen Rechner.

Ein erneuter Netzwechsel führt zu einer neuen *care-of address* und der mobile Rechner muss diese dem *home agent* mitteilen.

Kommt das mobile Gerät Heim ins Heimatnetz, so informiert es den *home agent*, das die Weiterleitung eingestellt werden muss (*deregister*). Daraufhin nimmt der *home agent* keine Pakete mehr an, die an die *home address* gesendet wurden, und das moblie Gerät kann sie nun direkt empfangen. Ein solcher *deregister* ist übrigens jederzeit freiwillig von mobilem Rechner möglich, wenn die Weiterleitung einfach eingestellt werden soll.

Die Anfragen von dem moblilen Rechner können übrigens immer direkt ans Ziel gesendet werden, indem man im Header als Quelle des Pakets die *home address* angibt.

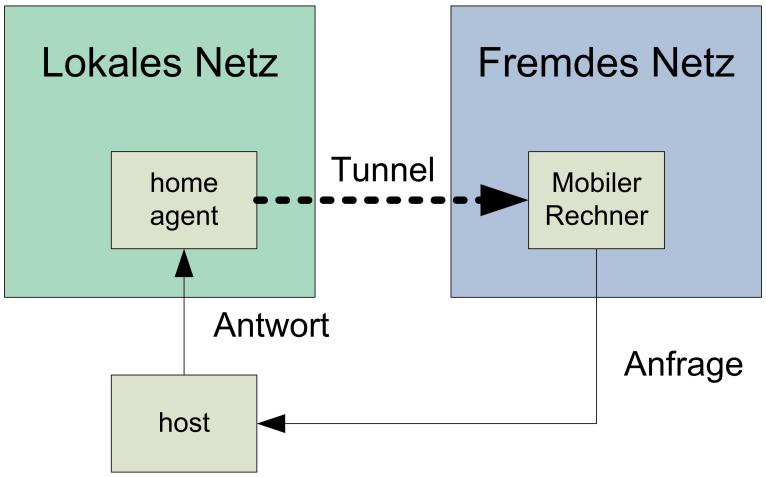

Abbildung 1: Veranschaulichung des Paketversandts

2.3 Die zwei Gesichter der *care-of address*

Es gibt zwei Typen einer *care-of address*, die *co-located care-of address* und die *foreign agent care-of address*. Welche Adresse verfügbar sind, hängt von dem Fremdnetz ab.

[6] Ein weiterer Header wird um das eigentliche Paket gepackt, in dem die neue Adresse steht.

Sie unterscheiden sich primär in der Art, wie sie vergeben werden und der Instanz auf der Seite des Fremdnetztes, die für das Weiterleiten der Nachrichten verantwortlich ist.

2.3.1 *co-located care-of address*

Eine *co-located care-of address* ist die einfachste Variante die zudem auch überall funktioniert. Dabei ist der mobile Rechner selbst für alle administrativen Aufgaben (wie das informieren des *home agents* verantwortlich.

Dabei ermittelt der mobile Rechner (z.B. mittels *DHCP*) eine freie *IP Adresse* in dem Fremdnetz, in dem er sich gerade befindet. Bekommt er eine, so informiert er den *home agent* über die neue temporäre Adresse, unter der er jetzt erreichbar ist.

Allerding ist bei dieser Lösung zusätzliche Software auf dem mobilem Endgerät notwendig, die dann auch Ressourcen verbraucht.

2.3.2 *foreign agent care-of address*

Der zweite Typ einer *care-of address* ist die *foreign agent care-of address*. Er benötigt im Fremdnetz eine aktive Instanz, die für administrative Aufgaben bzgl. *Mobile IP* verantwortlich ist, dem *foreign agent*.

Wenn ein mobiler Rechner ein neues Netz betritt, so muss dieser erst nach dem *foreign agent* in diesem Netz suchen. Dies geschieht über die ICMP-Erweiterung *Mobility agent advertisement extension* (→ **??**). Hat er diesen gefunden, so muss er sich bei diesem als mobiles Gerät *registrieren*. Der *foreign agent* übernimmt dann die Aufgabe getunnelte Pakete entgegenzunehmen und diese dann weiter an den mobilen Rechner zu senden.

Erstaunlicherweise ist es laut [Com06] möglich, das der *foreig agent* dem mobilen Rechner seine eigene IP Adresse zuweist und die Pakete an die mobilen Geräte dann anhand von Hardwareadressen weiterleitet. Dies ist im knappen Addressraum von *IPv4* sicherlich eine wichtige Eigenschaft. Außerdem kann ein *foreign agents* von den mobilen Geräten bestimmte durch den Netzadministrator festgelegte Richtlinien einfordern, die dann befolgt werden müssen.

2.3.3 *co-located care-of address* versus *foreign agent care-of address*

Beide Adressen haben ihre Vor- und Nachteile. Über die mir am wichtigsten erscheinendsten Eigenschaften gibt Tabelle **??** auskunft.

	co-located care-of address	*foreign agent care-of address*
Vorteile	Funktioniert in allen fremden Netzen, da diese keine zusätzlichen Erweiterungen (wie einen *foreign agent*) brauchen (→ Transparenz, Abschnitt 2.1.1)	Netzbetreiber können mobilen Geräten Richtlinien aufzwingen (wie z.B. einen Account), die eine Authentifikation erfordern (→ 2.4.1 in [CP02])
Nachteile	Extra Software auf dem mobilen Endgerät, die zusätzliche Ressourcen verbraucht	das fremde Netz muss eien *foreign agent* bereitstellen (Verantwortlichkeit liegt beim Betreiber des fremden Netzes) und dieser muss gefunden werden

Tabelle 1: Vergleich zwischen *co-located care-of adress* und *foreign agent care-of address*

2.4 Suche nach Agenten (*Agent Discovery*)

Die Suche nach Agenten ist eine Methode, nach der ein mobiler Rechner feststellen kann, ob er sich im Heimnetz oder in einem fremden Netz befindet.

Einerseits kann das mobile Gerät selbst im Netz anfragen, ob ein *foreign agent* existiert. Dies geschieht mit einer Erweiterung im ICMP-Header (siehe **??**.

Auch möglich ist es aber einfach auf eine *Router Advertisement* Nachricht zu warten, die der *foreign agent* periodisch sendet und darin seine Identität bekanntgibt.

2.5 Erkennen von Netzwechseln

Im [CP02] sind zwei Strategien vorgestellt, die verwendet werden können, um Netzwechsel zu erkennen. Diese können - müssen aber nicht - angewandt werden. Der mobile Rechner kann durchaus eine andere, eigene Strategie zum Entdecken von Netzwechseln benutzen.

Egal welche Strategie angewandt wird, der mobile Rechner darf sich nicht öfter als einmal pro Sekunde beim *home agent* registrieren.[7]

[7] Das hängt damit zusammen, das in den Paketen keine kleineren Zeiteinheiten gespeichert werden können, als eine Sekunde.

2.5.1 Algoritmus 1 (Lifetime aufzeichnen)

Die erste Methode besteht darin die *ICMP*[8] Router Advertisement Nachrichten[9] mitzuprotokollieren und die *Lifetime* jedes Paketes zu speichern, so lange es noch nicht abgelaufen ist.

Wenn der mobile Rechner nicht innerhalb der Zeit, bis die aufgezeichnete *ICMP-Lifetime* abläuft, eine neue *ICMP Router Advertisement* Nachricht bekommt (Teil der *Agent Advertisement* Nachricht), dann kann er davon ausgehen, das die Verbindung verloren gegangen ist, er sich also nicht mehr im *Subnetz* befindet.

Dies kann auch passieren, wenn der mobile Rechner eine *Agent Advertisement* Nachricht eines anderen Routers empfängt und dessen *Lifetime* nicht abgelaufen ist. In diesem Fall darf sich der mobile Rechner sofort beim neuen Router anmelden, ohne diesen erst suchen zu müssen.

2.5.2 Algoritmus 2 (Netzwerk Präfixe auswerten)

Die zweite Methode wertet die Netzwerkkennung (Prefix) aus. Unterscheidet sich diese zur letzten bekannten Kennung, so hat ein Netzwechsel stattgefunden.

Diese Methode darf nur angewandt werden, wenn beide Netze die *Prefix Erweiterung* im *ICMP Paket* bereitstellen. Sendet eins dieser Netze keine Kennung, so darf nicht davon ausgegangen werden, das es sich tatsächlich um einen Netzwechsel handelt.

Auch hier darf der sich mobile Rechner sofort beim neuen Router anmelden, wenn die *Lifetime* des empfangenen Pakets noch nicht abgelaufen ist.

2.6 2X Problem (two crossing problem)

Das *2X-Problem* (*two crossing problem*) veranschaulicht, das das *Mobile IP Protokoll* noch nicht ganz ausgereift ist.

Es handelt sich hier um ein Routingproblem, das auftritt, wenn ein Host dem mobilem Rechner ein Paket senden möchte und sich beide im gleichen Netz aufhalten. Klingt nach keiner großen Sache, denn im Optimalfall würde der Host erkennen, das sich sein Ziel im gleichen *Subnetz* befindet und sein Paket gleich zustellen.

[8] Internet Control Message Protocol (→ [wik08a])
[9] Nachrichten, die von Routern in regelmäßigen Zeitabständen gesendet werden, damit u.A. neue Rechner im Netz den Router auffinden können.

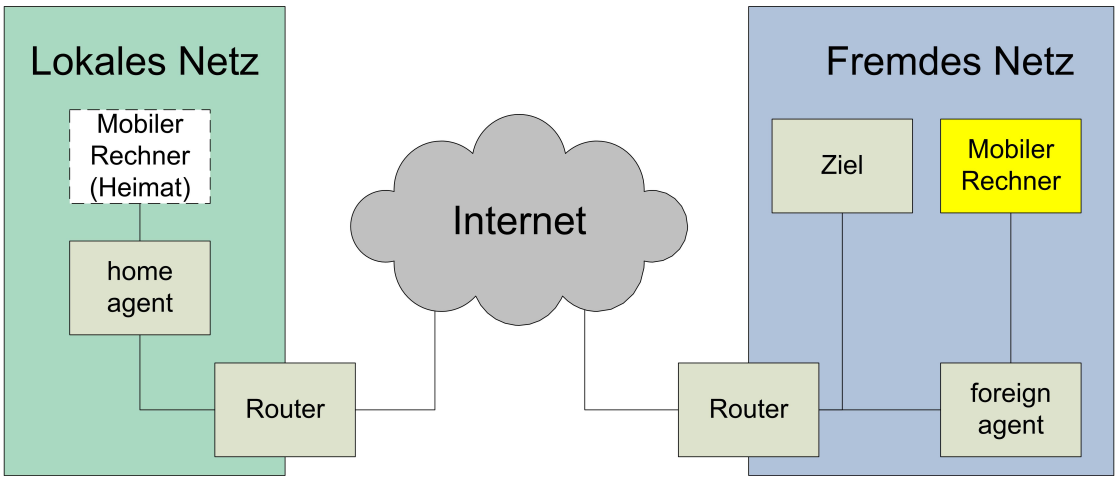

Abbildung 2: Ineffizientes Routen: Wenn das mobile Gerät dem Ziel im gleichem Netz etwas schicken möchte, so wird diese Anfrage zwei mal durch das Internet geleitet.

Leider ist das mobile Gerät zu diesem Zeitpunkt nur unter seiner *home address* bekannt. Aus diesem Grund wird das Paket an den nächstbesten Gateway, also dem Router, geschickt und dann quer durch das Internet in das Heimatnetz des mobilen Rechners zugestellt. Dort nimimt der *home agent* das Paket entgegen, packt es ein und schickt es an die ihm bekannte *care-of address* des mobilen Rechners - unnötigerweise! (vgl. Abbildung 2)

2.7 Kommunkation mit Rechnern im Heimnetz

Wie in 2.2 bereits erwähnt, muss ein *home agent* alle eingehenden Pakete, die and die *home address* gesendet wurden abfangen, wenn sich das moblie Gerät nicht im Haimatnetz befindet.

Dies ist bei eingehenden Nachrichten von außerhalb des Netzes kein Problem (insbesondere dann nicht, wenn der Router gleichzeitig als *home agent* eingesetzt wird).

Anders sieht es aus, wenn ein lokaler Rechner im Heimatnetz ein Paket an das mobile Gerät senden möchte, das sich ja gerade nicht im Netz befindet. Da sich der Zielrechner im gleichem Subnetz befindet (so meint zumindest berechtigterweise der Host), wird das

Paket nicht an den Router weitergesandt, sondern eher eine *ARP*[10] Anfrage durchgeführt, die im lokalem Netz nach der *Hardware Adresse* des Zielrechners fragt, um das Paket direkt zuzustellen.

Wenn sich der mobile Rechner aber nicht im Heimatnetz befindet, so muss der *home agent* die Aufgabe übernehmen und sich quasi als das mobile Gerät ausgeben. Der *home agent* beantwortet *ARP* Anfragen dann mit seiner eigenen *Hardwareadresse*. Auf diese Weise kann der Agent weiterhin alle Pakete weiterleiten, selbst wenn diese aus dem eigenem Subnetz stammen.

3 Mobile IP mit IPv6 (was die Zukunft bringt)

Auch im *IPv6 Protokoll* wird eine mobile IP unterstützt. Die *IETF*[11] entickelte ein Protokoll unter dem Namen *Mobile IPv6*. *Mobile IPv6* ist dabei fester Bestandteil des *IPv6 Protokolls* (→ [JP04]).

Dabei bleibt das Grundkonzept das Gleiche, in dem im Heimatnetz ein *home agent* als Vermittler fungiert und ankommende Pakete an den mobilen Rechner einfach weiterleitet.

Dennoch sind im *IPv6 Protokoll* einige Erweiterungen enthalten, die in *Mobile IP* nicht inbegriffen waren, diese jedoch das reallisieren einer mobilen IP vereinfachen.

Nach [ISI81] ergeben sich unter anderem folgende signifikanten Unterschiede zwischen *Mobile IP* für und *Mobile IPv6*:

- *IPv6* benötigt im Gegensatz zu *IPv4* keine *foreign agents*. Es funktioniert überall, ohne dass ein lokaler Router es unterstützen müsste.
- Durch *IP encapsulation*[12] verursachte *Overhead* ist bei *Mobile IPv6* viel geringer als bei *IPv4*, da normale *IPv6 Routing Header* für die meisten administrativen Nachrichten benutzt werden können.
- Der *Neighbor Unreachability Detection* Mechanismus (→ [NNS98]) im *IPv6* ermöglicht eine symmetrische Kommunikation zwischen dem mobilen Rechner und einem lokalen Router. Das *2X-Problem* (→ 2.6) ist somit nicht mehr vorhanden.

[10] Address Resolution Protocol, → [Plu82]
[11] Interne Engineering Task Force
[12] Tunneln; ein zusätzlicher Header, der über das eigentliche Paket gepackt wird, gibt das neue Ziel an.

- *Mobile IPv6* ist von der *Sicherungsschicht* entkoppelt, da es den *Neighbor Unreachability Detection* Mechanismus, statt ARP[13] verwendet und ist somit viel robuster als *Mobile IP*.

4 Resümee

Mobile IP ist ein Protokoll, das viel verspricht, und es theoretisch auch halten könnte. Allerdings besteht zur Zeit kein Bedarf an diesem Protokoll, weshalb es immer noch ein Randdasein fristet.

Dies resultiert nicht nur aus der geringen Netzabdeckung, die z.B. möglichst flächendeckend sein sollte, damit Applikationen einen kurzzeitigen Verbindungsabbruch nicht bemerken und so Verbindungen beim Netzwechsel überdauern können. Auch ist eine Technik, die Ähnliches leisten kann, zur Zeit viel populärer geworden: *VPN*.

VPN ermöglicht es ebenfalls mobilen Rechnern, sich virtuell im *Heimatnetz* aufzuhalten, und eine lokale IP dieses Netztes zu haben. Dieser Rechner kann dann ebenfalls unter der IP des *Heimatnetzes* angesprochen werden. Die Netzwechsel können hier allerdings nicht so problemlos und leicht (automatisch) vollführt werden, wie es bei dem *Mobile IP Protokoll* der Fall ist, was aber wegen der geringen Netzabdeckung praktisch irrelevant ist.

Ich sehe keine Zukunft für *Mobile IP*, aber sein Nachfolger *Mobile IPv6* könnte durchaus einzug in den praktischen Nutzen haben, wenn Europa den Wechsel von *IPv4* nach *IPv6* vollführt. Dann ist die mobile IP im *Internet Protokoll* integriert.

Vermutlich wird es aber noch recht lange dauern, bis sich die zähe Masse der europäischen Großunternehmen dazu entschließt Millionen für den Wechsel auszugeben, solange das „Patchwork-IPv4-Protokoll“, in dem alle möglichen Erweiterungen hinzugedichtet wurden und werden, noch funktioniert und keine akute Addressnot besteht.

5 Fachwörterverzeichnis

Informatik ist eine recht neue Wissenschaft. Viele Fachbegriffe sind in Englisch gehalten. Für einige gibt es durchaus deutsche equivalente Ausdrücke. Ist dies der Fall - und sind diese auch geläufig - so werde ich diese auch benutzen.

[13] Address Resolution Protocol

Es gibt allerdings auch Wörter, bei denen eine Eindeutschung nur Verwirrung stiften würde, wie z.B. *home agent* (Heimatagent? Heimatvermittler??). Es handelt sich teilweise um Bezeichnungen, die die Autoren von [CP02] oder [JP04] eingeführt haben. Diese Fachbegriffe lasse ich in der englischen Sprache, um den Sinn nicht zu verfälschen. Ich führe diese Begriffe dennoch in der Liste auf.

agent discovery	Suche nach Agenten
ARP	ARP
bandwidth	Bandbreite
care-of address	-
client	Client
co-located care-of address	-
entity	Instanz, Einheit
fixed primary address	stationäre primäre Adresse
foreign agent	-
foreign agent care-of address	-
foreign network	fremdes Netz
header	Header
home agent	-
home network	Heimatnetz
ip address	IP Adresse
lifetime	-
link layer	Sicherungsschicht
memory	Speicher
network service	Netzwerkdienst
overhead	Overhead
routing	(das) Routing
secondary address	zweite Adresse
subnet	Subnetz
tunnel	Tunnel
WLAN	WLAN

Abbildungsverzeichnis

Tabellenverzeichnis

Literatur

[Com06] Comer, Douglas E.: *Internetworking with TCP/IP*. 5. Prentice Hall, 2006. – ISBN 0–13–187671–6

[CP02] C. Perkins, Ed.: *RFC3344 - IP Mobility Support for IPv4*. Network Working Group, Request for Comments, August 2002. – PROPOSED STANDARD

[ISI81] Information Sciences Institute, University of Southern C.: *RFC 791 - Internet Protocol*. Network Working Group, Request for Comments, September 1981. – STANDARD

[JP04] Johnson, D. ; Perkins, C.: *RFC 3775 - Mobility Support in IPv6*. Network Working Group, Request for Comments, June 2004. – PROPOSED STANDARD

[NNS98] Narten, T. ; Nordmark, E. ; Simpson, W.: *RFC 2461 - Neighbor Discovery for IP Version 6 (IPv6)*. Network Working Group, Request for Comments, December 1998. – DRAFT STANDARD

[Plu82] Plummer, David C.: *RFC826 - An Ethernet Address Resolution Protocol*. Network Working Group, Request for Comments, November 1982. – STANDARD

[wik08a] *Internet Control Message Protocol*. Website. January 2008. – http://de.wikipedia.org/wiki/Icmp

[wik08b] *Internet Protocol*. Website. January 2008. – http://en.wikipedia.org/wiki/Internet_Protocol

[wik08c] *IPv6*. Website. January 2008. – http://de.wikipedia.org/wiki/Ipv6