Mobile IP

Seminar

Mobile/Wireless Networking

Frank Völlinger

Inhaltsverzeichnis

1. EINFÜHRUNG

In der heutigen Internetwelt ist Mobilität ein wichtiger Aspekt geworden. Dies ist zurückzuführen auf die weite Verbreitung und ständig wachsende Anzahl von portablen Computereinheiten, wie z. B. Palmtops und Notebooks, die mittlerweile zu akzeptablen Preisen angeboten werden und den stationären Vertretern kaum noch in etwas nachstehen. Sie verfügen über hohe Rechenleistung, große Speicherkapazitäten, multimediale Fähigkeiten und bieten einfachen Netzzugang. Gleichzeitig wächst die Gesamtanzahl von Hosts und Netzwerken exponentiell.

Wireless Networks mit hohen Datenraten sind heute verfügbar und bieten gerade in Verbindung mit mobilen Hosts einen hohen Komfort, da sich der Benutzer idealerweise unter ständiger Verbindung zum Netz beliebig umher bewegen kann. Diese Mechanismen werden aber von den traditionellen Internetprotokollen nicht unterstützt. Einen Ortswechsel eines Hosts mit fester IP Adresse setzt aufwendige Umkonfigurierungen am Gerät und entsprechende administrative Kenntnisse beim Benutzer voraus. Mobile IP stellt eine Erweiterung des Protokolls dar, die es ermöglicht einen Host immer unter der selben Adresse zu erreichen, unabhängig von seiner Position im Netz. Die ersten Versionen boten entweder Sicherheit oder Routenoptimierung, neuere Implementierungen bieten jedoch beides.

Es besteht eine Authentifizierungspflicht, so daß sich kein böswilliger Host als ein anderer ausgeben kann und somit z. B. dessen Pakete stehlen kann. Mobile IP ist so konzipiert, daß wenn irgendwann bessere Sicherheitsstandards im Internet verfügbar sind, einfach auf diese umgestellt werden kann, vorerst aber zumindest das Level der derzeitigen allgemein vorhandenen Sicherheit im Internet bewahrt wird.

Im folgenden Kapitel 2 werden die notwendigen **Nodes** (damit sind Hosts oder Router gemeint) für Mobile IP und deren Funktionen beschrieben. In Kapitel 3 wird die Funktionsweise des Protokolls anhand eines Beispiels leicht verständlich erklärt, worauf in Kapitel 4 und 5 dann detaillierter eingegangen wird bis hin zu der konkreten Bedeutung von einzelnen Bits in den Mobile IP Paketen. Kapitel 6 schließlich bildet die Zusammenfassung.

2. NODES UND IHRE AUFGABEN

Durch die Zusammenarbeit folgender *Nodes* und Mobile IP, ist das zustellen von Paketen und an- und abmelden vom Netz für den Benutzer völligtransparent.

2.1. MOBILE HOST

Ein **Mobile Host** (**MH**) ist eine Endgerät mit fester IP Adresse, z. B. ein Laptop, das an verschiedene Netze anschließbar ist und dabei die selbe Adresse beibehält. Man sagt, der mobile Host sei *zu Hause* (englisch: *at home*), wenn er mit seinem Heimatnetz verbunden ist. In diesem Zustand operiert er genau so wie jeder fest installierte Host und ist nicht bei seinem *Home Agent* (s. 2.2.) registriert. Er verwaltet seinen Paketverkehr selbst und führt keine Mobile Internet Protokolle aus.

Ist ein *Mobile Host* mit einem fremden Netzwerk verbunden, so hat er sich unmittelbar nach dem Verbinden mit dem neuen Netz, bei seinem *Home Agent* registriert, was soviel bedeutet wie er hat ihm mitgeteilt wo er sich jetzt befindet. Die Registrierung erfolgte entweder direkt beim *Home Agent* oder über einen *Foreign Agent* (s. 2.3.), der im fremden Netzwerk ausfindig gemacht wurde. Alle Pakete die für den mobilen Host bestimmt sind, bekommt er von seinem *Home Agent* zu seinem aktuellen Standort weitervermittelt. Kehrt er nach Hause zurück deregistriert er sich bei seinem *Home Agent* und ist für seinen Datenverkehr wieder selbst zuständig.

Dasselbe trifft auch für mobile Router zu, auf deren Besonderheiten doch hier nicht genauer eingegangen wird.

2.2. HOME AGENT

Mobile IP wird hauptsächlich durch einen **Home Agent** (**HA**) möglich gemacht. Der *Home Agent* weiß jeder Zeit über den Aufenthaltsort der *Mobile Hosts* (s. 2.1.) bescheid für die er zuständig ist. Ist ein *MH* zu Hause, verhält sich der *Home Agent* ihm gegenüber passiv, andernfalls fängt er an den *MH* adressierte Pakete auf dem Heimatnetz ab und stellt leitet sie an ihn weiter.

Vom *HA* wird eine Liste verwaltet, in der kein, ein oder mehrere Aufenthaltsorte pro mobilem Host eingetragen sind. Diese Registrierungseinträge beinhalten unter anderem auch die Gültigkeit des Eintrags, nach dessen Ablauf sie gelöscht werden. Für die Registrierungsnachrichten zwischen *MH* und *HA* werden Sicherheitsverfahren angewandt, um sich vor böswilligen Attacken zu schützen (s. 5.1.2.).

2.3. FOREIGN AGENT

Bei Eintritt in ein fremdes Netzwerk, wendet sich ein *Mobile Host* (s. 2.1.) normalerweise an einen **Foreign Agent** (**FA**), welcher für ihn eine **care-of address** bereitstellt. Diese *care-of address* ist im Normalfall die eigene IP Adresse des *Foreign Agents* und bildet in Verbindung mit der eigenen IP Adresse des *MH* den Basisparameter für den Registrierungseintrag. Der *MH* registriert sich bei einem *FA* und über diesen bei seinem *Home Agent* (s. 2.2.). Im Fall ohne *FA* würde der *MH* auf einem in diesem Dokument nicht weiter ausgeführten Weg eine **co-located care-of address** vom fremden Netzwerk zugewiesen bekommen und direkt mit seinem *Home Agent* Kontakt aufnehmen.

Der *FA* führt eine sogenannte **visitor list** (deutsch: *Besucher Liste*), die alle derzeit bei ihm registrierten *MHs* enthält, ähnlich der Liste des *Home Agents*. Auch hier werden die Einträge sofort nach Ablauf des zugehörigen Zeitlimit gelöscht. Beabsichtigt ein *Mobile Host* einen Aufenthalt über das registrierte Zeitlimit hinaus, muß er sich vor dessen Ablauf re-registrieren, um eine unterbrechungslose Verbindung aufrecht zu erhalten. Zwischen *FA* und *MH* bzw. *HA* können die selben Sicherheitsmechanismen wie zwischen *MH* und *HA* eingesetzt werden, vorgeschrieben sind bis jetzt allerdings nur einfachere Funktionalitäten

2.4. CACHE AGENT

Aufenthaltsorte von *Mobile Hosts* (s. 2.1.) werden durch die Adresse eines *MH* in Verbindung mit seiner momentanen *care-of address* (s. 2.3.) spezifiziert. Diese Daten, ergänzt um einige weitere, wie z. B. ein Zeitstempel, werden bei Bedarf als **binding update messages** verschickt und von einem **Cache Agent** (**CA**) gespeichert und in einer Liste verwaltet, dem **binding cache** . Will man Routenoptimierung realisieren bedient man sich eines *Cache Agents* , denn dieser kann Pakete direkt an einen *MH* schicken, anstatt den Umweg über dessen zugehörigen *Home Agent* (s. 2.2.) zu gehen, vorausgesetzt der *CA* hat einen *binding cache* Eintrag für den entsprechenden *MH*. Es erhalten die *binding update messages* ihre Gültigkeit und werden zu *binding cache* Einträgen erst nach dem sie authentifiziert worden sind und sie werden gelöscht wenn ihr Zeitlimit abgelaufen ist.

Natürlich können *Nodes* mehrere der in diesem Kapitel beschriebenen Funktionen übernehmen; so kann z. B. ein *MH* gleichzeitig *CA* sein und so direkt mit einem anderen *MH* kommunizieren oder ein *HA* stellt für fremde *MHs* im eigenen Netzwerk einen *FA* dar.

3. FUNKTIONSWEISE EINES MOBILE INTERNET PROTOKOLLS ANHAND EINES BEISPIELS

In diesem Kapitel wird die Funktionsweise von Mobile IP anschaulich beschrieben, wozu ein graphisch dargestelltes Beispielnetzwerk herangezogen wird. Es werden alle wichtigen Konstellationen der *Nodes* im Netzwerk behandelt, so daß daraus ein zusammenhängendes Verständnis für das Protokoll resultiert. Der Detaillierungsgrad beinhaltet jedoch keine spezifischen technischen Informationen, wie z. B. Timergrößen und Bitstrukturen der Protokollnachrichten; dieses findet man in den nächsten 2 Kapiteln genau beschrieben. Abbildung 1 zeigt eine Legende über die in den Beispielen verwendeten Symbole:

Abbildung 1

3.1. SZENARIO: DER MOBILE HOST IST ZU HAUSE

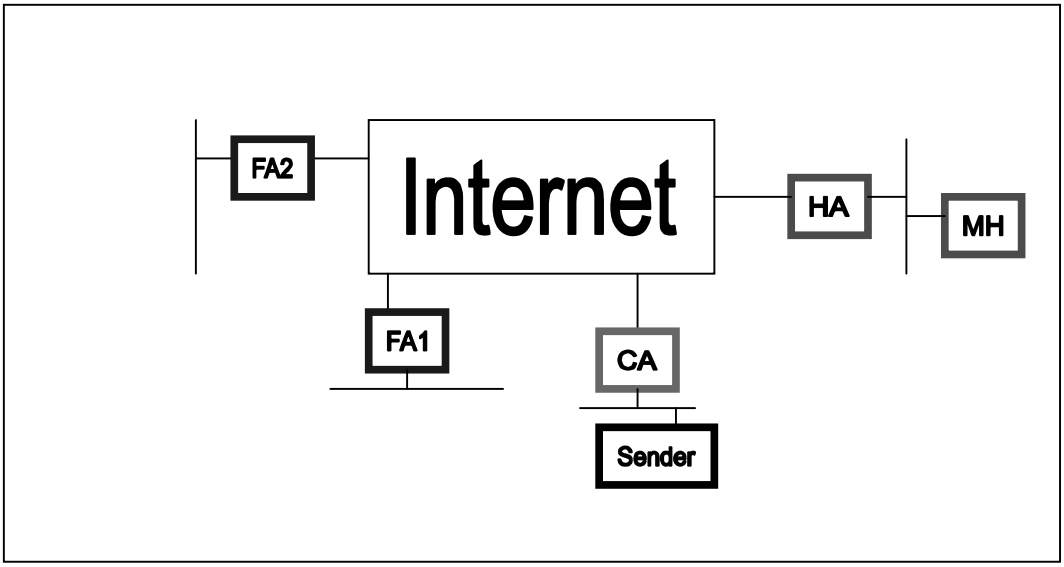

Abbildung 2

Der *Mobile Host* befindet sich in seinem Heimatnetz, er ist *zu Hause*. Somit verhält er sich genauso wie ein normaler, stationärer Host es auch tut. Er ist bei seinem *Home Agent* nicht reg istriert, dieser ist aber möglicherweise sein default Router. An dieser Stelle sei erwähnt, daß der Sendeprozess des *MHs* grundsätzlich dem eines immobilen Hosts gleicht, es sei denn es wird *Reverse Tunneling* (s. 4.1.1.) verwendet. Deshalb wird in diesem Do kument hauptsächlich der Fall des Empfangens von Paketen besprochen.

Es werden von dem *Home Agent* ständig **Agent Advertisement message s** (s. 4.1.) verschickt, in denen der *HA* seine Präsenz verkündet. Daraus kann der *Mobile Host* folgern, daß er zu Hause ist. Die *Advertisement messages* enthalten einen Zeitstempel, denn sie sind nur befristet gültig. Solange eine neue *message* eintrifft bevor die vorhergehende ihre Gültigkeit verliert, geht der *MH* davon aus, daß er sich zu Hause befindet. Im Rahmen der Kapazität eines *HAs* können beliebig viele *MHs* von ihm verwaltet werden.

Der Sender, ein beliebiger Host aus einem anderen Netzwerk, schickt Pakete an den *MH*. Der *Cache Agent* ist dabei der default Router von dem Sender, dessen *CA* Funktionalität in dieser Konstellation jedoch nicht von Bedeutung ist. Besonderheiten von Mobile IP treten erst auf, wenn der mobile Host sein Heimatnetz verläßt; dieser Vorgang wird nun in den nächsten Unterkapiteln beschrieben.

3.2. SZENARIO: DER MOBILE HOST WIRD AN EIN FREMDES NETZWERK ANGESCHLOSSEN

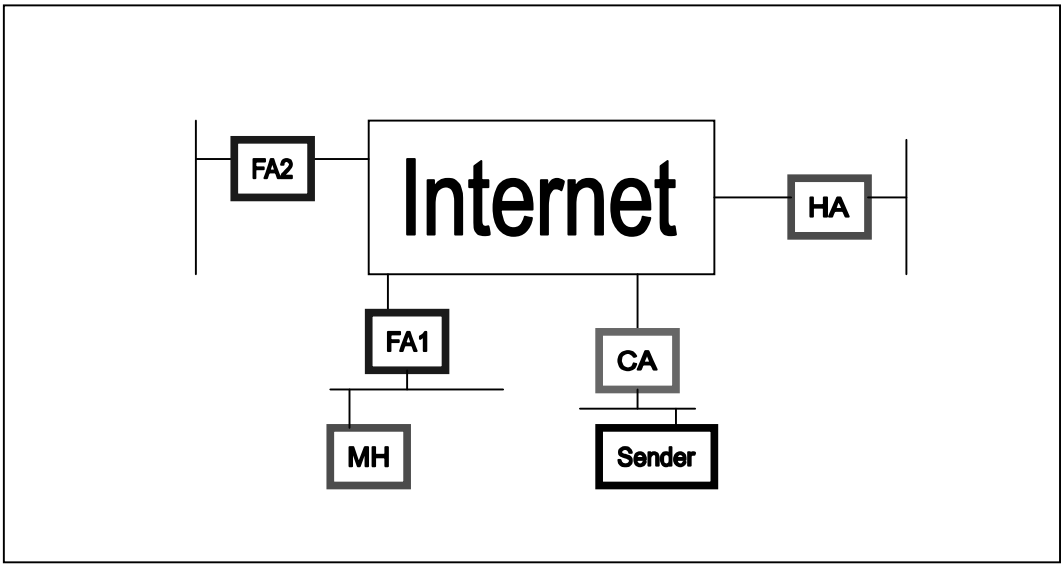

Abbildung 3

Wie in Abbildung 3 zu erkennen ist wurde der *Mobile Host* jetzt mit einem fremden Netzwerk verbunden bzw. in dessen Sendebereich bewegt, wenn es sich um ein Wireless Network handelt. Die letzte *Advertisement message* von seinem *Home Agent* ist wahrscheinlich schon lange nicht mehr gültig oder wird demnächst ablaufen, so daß der *MH* wahrnimmt, daß er nicht mehr zu Hause ist. Es besteht auch die Möglichkeit für den *MH* den Wechsel zu einem anderen Netz dadurch festzustellen, daß die *Prefix-Lengths Extension* benutzt wird, die in Unterkapitel 4.1.2. genauer beschrieben ist.

In unserem Szenario verschickt der *Foreign Agent* 1 ebenfalls *Advertisement messages*, was im allgemeinen auch der Fall sein sollte, aber nicht unbedingt erforderlich ist (s. 3.4.). Sobald vom *MH* eine solche Nachricht empfangen wird, wird er sogleich versuchen sich bei dem *FA* zu registrieren. Dazu schickt er an den *FA* 1 eine **Registration Request message** , die der *FA* an den *HA* weiterleiten soll. Darin enthalten ist u nter anderem die Adresse des *HA*, die aus der *Advertisement message* erhaltene *care-of address* (s. 2.3.) und eine Verschlüsselung, die zwingend vorgeschrieben ist und auf einem geteilten Geheimnis zwischen *MH* und *HA* basiert. Existiert ein solches Sicherheits verfahren auch zwischen *MH* und *FA* bzw. zwischen *FA* und *HA* muß auch dieses verwendet werden. Das kann z. B. der Fall sein, wenn alle Geräte im Besitz der selben Organisation sind. Ansonsten ist zwischen *MH* und *FA* bzw. *FA* und *HA* ein vereinfachtes Verfahren a nzuwenden (s. 5.1.3. bzw. 5.2.3. Sicherheitsmechanismen).

Hat der *FA* noch freie Kapazitäten in seiner *visitor list* (s. 2.3.), wird er die *Request message* an den *HA* weiterleiten. Dieser bestätigt den *Request* mit einer **Registration Reply message**, die besagt, daß der *MH* nun bei seinem *HA* registriert ist und einen Zeitstempel enthält, da der Eintrag auch nur befristet gültig ist. Der *MH* muß sich also vor Ablauf der Gültigkeitsfrist re-registrieren, um konstante Verbindung zu halten. Die *Reply message* wird vom *FA* an den *MH* weitergeleitet und der Prozess des Registrierens wäre abgeschlossen. Zusätzlich erstellt der *MH* noch einen **registration key** für diese Sitzung mit dem *FA*, der als Schlüssel zu späteren Authentifizierungszwecken zwischen den*Nodes* benutzt werden kann (s. 3.4.).

Es besteht in manchen Fällen auch die Möglichkeit für den *MH* durch niedrigere Netzwerkschichten eine *co-located care-of address* (s. 2.3.) vom fremden Netzwerk zur Verfügung gestellt zu bekommen und dann mit seinem *HA* direkt zu kommunizieren, was hier jedoch nicht weiter ausgeführt werden soll.

Vom Sender werden wieder Pakete an den *MH* verschickt, die wie gewöhnlich die IP Adresse des *Mobile Hosts* enthalten. Deshalb erreichen sie auch dessen Heimatnetz, wo sie jetzt allerdings von dem *Home Agent* abgefangen werden, da dieser einen Registrierungseintrag von dem *MH* vorfindet. Das Paket wird vom *HA* nun an den *MH* **getunnelt**, was bedeutet, daß es nochmals in einen IP Header um den ursprünglichen Header eingepackt wird. Der neue Header enthält die *care-of address* des *MH* und wird somit wie ein gewöhnliches Paket zum *FA* 1 über Router, die nicht notwendigerweise Mobile IP implementieren müssen, zugestellt. Der *FA* 1 entpackt das Paket aus dem äußeren IP Header und leitet es an den *MH* weiter.

Das senden von Daten an *MH* ist somit für den Sender immer gleich, unabhängig von der Position des mobilen Hosts.

3.3. SZENARIO: ROUTEN OPTIMIERUNG

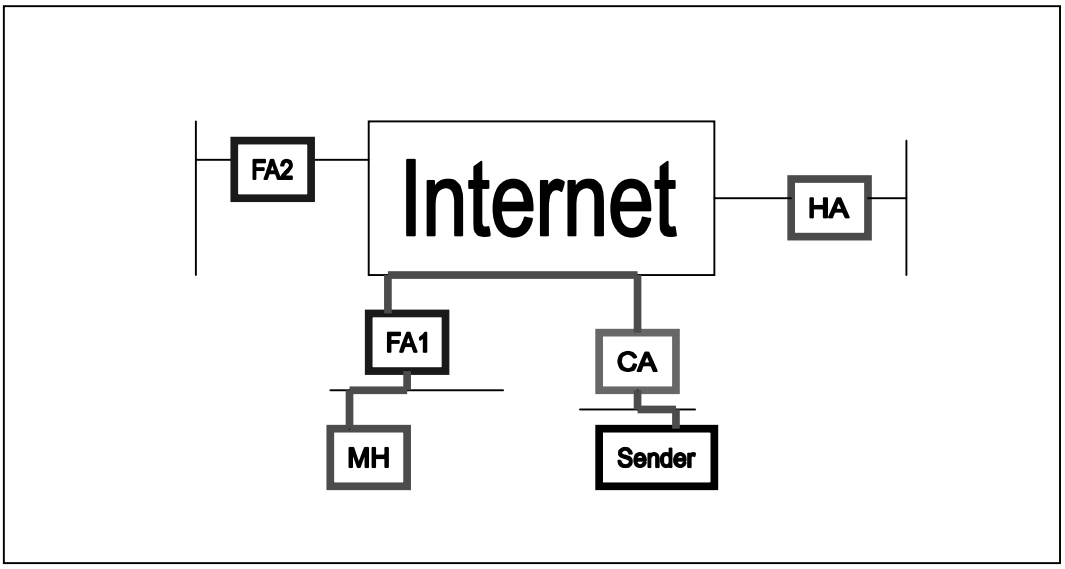

Abbildung 4

Fängt der *Home Agent* ein Paket bestimmt für den *Mobile Host* ab, weil sich jener nicht im Heimatnetzwerk befindet und *tunnelt* (s. 3.2.) es weiter zu dem aktuellen Aufenthaltsorts des *MHs* – in unserem Beispiel *Foreign Agent* 1 - , sollte der *HA* auch eine *binding update message* (s. 2.4.) an den Sender schicken. Kann der Sender als *Cache Agent* fungieren, speichert er diese als *binding cache* Eintrag, nachdem sie über den *HA* authentifiziert wurde für die Dauer ihrer angegebenen Gültigkeit. Dieselben Updates können auch von *FAs* verschickt werden, wenn an sie fälschlicherweise ein für einen *MH* bestimmtes Paket *getunnelt* wurde, das sie selbst wieder weiter *tunneln* müssen, weil der *MH* gar nicht bei dem *FA* registriert ist. Das kann z. B. passieren, wenn der *binding cache* des Senders nicht auf dem aktuellsten Stand ist, weil der *MH* vor kurzer Zeit in ein anderes Netzwerk gewechselt ist. Auch diese Nachrichten müssen natürlich auch erst über den *HA* authentifiziert werden, bevor, sie in die Liste übernommen und verwendet werden. Kennt der *FA* den neuen Aufenthaltsort des *MHs* nicht schickt er statt der *binding update message*, eine **binding warning message**, die den Sender veranlassen soll eine **binding request message** an den *HA* zu schicken, welche eine explizite Anforderung einer *binding update message* ist.

Die *binding update messages* werden vom Empfänger nicht notwendigerweise bestätigt, aber für das nächste falsch *getunnelte* Paket wird wieder eine *update message* generiert und somit die Wahrscheinlichkeit erhöht, daß der Sender die Nachricht erhält, falls die vorhergehende verloren ging. Wenn nach ein paar Paketen immer noch weitere von dem selben Sender eintreffen, muß die Rate der zurückgesendeten update *messages* rapide heruntergeschraubt werden, um das Netz nicht unnötig zu belasten, da der Sender wahrscheinlich keine *CA* Funktionalität besitzt.

Da wir in unserem Beispiel absichtlich einen beliebigen Sender gewählt haben, setzen wir keine *CA*-Fähigkeiten voraus. Der *Home Agent* würde also anfangs Updates als Antwort auf eintreffende Pakete von dem Sender zurückschicken, die die *care-of address* von *FA* 1 enthalten, aber die Senderate bald erheblich herab drosseln. Dennoch verhält es sich in unserem Fall anders, da, wie aus Abbildung 4 ersichtlich, sich der Sender eines Routers bedient, welcher ein *CA* ist. Dieser „schnüffelt“ sozusagen in die IP Pakete hinein, die er dem Sender zustellt und gelangt somit an das Wissen über die *binding update message*. Er läßt die Nachricht vom *HA* authentifizieren und speichert sie sodann in seinem *binding cache*. Weitere Pakete vom Sender an den *Mobile Host* werden von dem *Cache Agent* von nun ab direkt zu dem *Foreign Agent* 1 *getunnelt*, was in Abbildung 4 graphisch dargestellt ist.

Man sieht an diesem Beispiel deutlich, daß Routenoptimierung auch funktionieren kann, wenn der Sender kein Mobile IP implementiert, was besonders zu Beginn der Einführung, wenn Mobile IP noch nicht allzu weit verbreitet ist, einen großen Vorteil darstellt. Die Optimierung ist umso effektiver, je kleiner die Distanz zwischen *CA* und Sender.

3.4. SZENARIO: DER MOBILE HOST WIRD IN EIN ANDERES EBENFALLS FREMDES NETZWERK BEWEGT

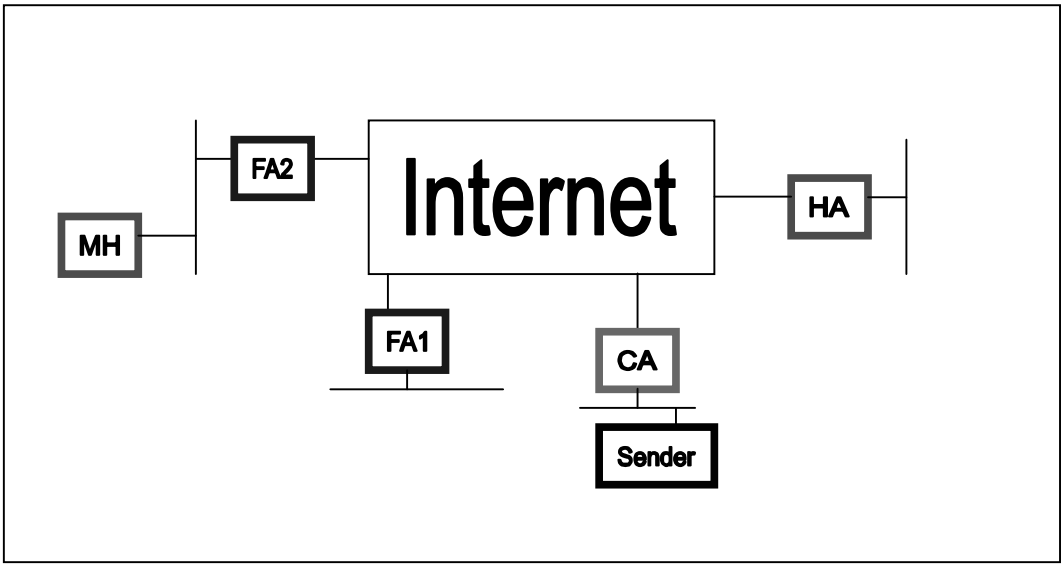

Abbildung 5

Unser *Mobile Host* hat das Netzwerk mit *Foreign Agent* 1 verlassen und befindet sich jetzt in einem neuen ebenfalls fremden Netzwerk. Hier sei der *Foreign Agent* 2 vertreten, der allerdings keine *Advertisement messages* verschickt, obwohl ein *FA* dies im Allgemeinen tun sollte. Das Ausbleiben der *Advertisement messages* veranlaßt den *MH* eine **Agent Solicitation message** (s. 4.2.) auf das Netzwerk zu geben, was eine Aufforderung an jeden Home und *Foreign Agent* in diesem Netz ist eine *Advertisement message* zu senden. Abbildung 5 zeigt, daß dies in unserem Szenario nur für einen Agent und zwar *FA* 2 zutrifft, welcher auch antwortet. Daraufhin registriert sich der *MH* über den *FA* 2 bei seinem *HA* auf die selbe Weise wie schon weiter oben in Unterkapitel 3.2. beschrieben.

An *FA* 1 schickt der *MH* (evtl. via *FA* 2) nun eine **binding notification message**, die jenem den neuen Aufenthaltsort des *MHs* mitteilt. Das Authentifizierungsverfahren basiert auf der selben Methode wie das zwischen *MH* und seinem *HA*, nur das hier als geteiltes Geheimnis der *registration key* verwendet wird, der vom *MH* zuvor nach seiner Registrierung bei *FA* 1 erstellt wurde (s. 3.2.).

Nehmen wir an der Sender schickt jetzt wieder Pakete an den *MH* und der letzte *binding cache* Eintrag von dem *Cache Agent* ist noch nicht verfallen. Somit *tunnelt* der *CA* die Pakete, wie auch zuvor an *FA* 1. Wie wir wissen bietet dieser zwar keinen Service in Form eines *Foreign Agents* für den *MH* an, aber kennt seine neue Position und kann die Pakete an den wirklichen Aufenthaltsort von dem *MH* weiter *tunneln*. Gleichzeitig schickt er eine *binding update message* an den *CA*, was diesen veranlaßt, nach erfolgreicher Authentifizierung, seinen *binding cache* upzudaten. Die folgenden Pakete werden von dem *CA* ab sofort direkt zu *FA* 2 *getunnelt*.

3.5. SZENARIO: HEIMKEHR DES MOBILE HOSTS

Es herrscht wieder die selbe Topologie, wie sie bereits in Abbildung 2 dargestellt wurde. Der *Mobile Host* ist zurück in seinem Heimatnetz. Sofort nach Erhalt der ersten *Advertisement message* von seinem *Home Agent*, weiß er, daß er sich wieder zu Hause befindet und deregistriert sich bei diesem. Jetzt operiert er wieder, wie ein traditioneller stationärer Host es auch tut und der *HA* fängt keine Pakete mehr für den *MH* ab.

Es wurde bewußt im vorherigen Szenario darauf verzichtet, den *MH* nach seiner Registrierung beim *FA* 2, ein *registration key* (s. 3.2.) zu erstellen, da auch dieser Fall behandelt werden soll. Der *MH* informiert also seinen Vorgänger, *FA* 2, nicht über seinen jetzigen Aufenthaltsort, d. h. sendet keine *binding notification message* an diesen. Der *binding cache* des *CAs* sei wieder nicht auf dem neusten Stand und es werden von ihm aus weiterhin Pakete an *FA* 2 verschickt. Statt einer *binding update message* wird von *FA* 2 jetzt eine *binding warning message* (s. 3.3 .) generiert und an den *CA* gesendet und statt das erhaltene Paket zu dem *HA weiterzutunneln*, was ihm ja nicht möglich wäre, setzt er einen **special tunnel** ein, um das Paket an den *HA* des *MHs* zu senden. Das *special tunnel* Paket enthält sowohl in dem eigentlichen, als auch in dem zusätzlichen IP Header die Heimatadresse des *MHs* und wird unabhängig von sämtlichen *binding cache* Einträgen irgendwelcher Router auf dem Weg direkt zum Heimatnetzwerk des *MHs* getunnelt. *Special tunneling* wird benutzt, um kreisende Pakete zu vermeiden, die auf Grund der Inkonsistenz von *binding cache* s verschiedener Router entstehen können. Da der *MH* sich gerade zu Hause befindet, kann er das Paket nun selbst entgegennehmen, andernfalls wäre es von seinem *HA* zu ihm *getunnelt* worden.

4. ADVERTISEMENT UND SOLICITATION *MESSAGES*

In diesem Kapitel wird die technische Realisierung des Entdeckens von Agents durch einen *Mobile Host* genauer beschrieben. *Agent Advertisement messages* werden von Agents generiert und dazu benutzt ihren Service anzupreise n. *Agent Solicitation messages* sind eine explizite Aufforderung von einem *MH* an alle Agents in einem Netzwerk, eine *Advertisement message* zu senden.

4.1. AGENT ADVERTISEMENT MESSAGES

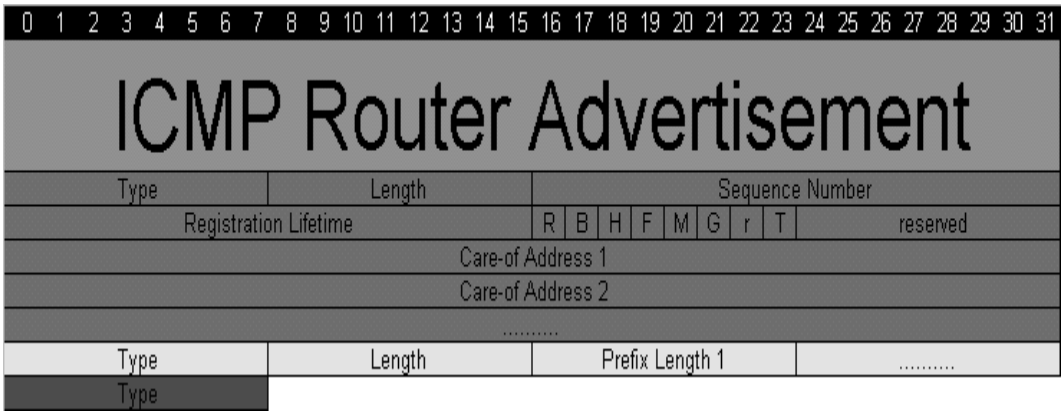

Abbildung 6

Die Agent *Advertisement message* stellt eine Erweiterung der *ICMP Router message* dar und schließt sich dieser an. Optional kann noch eine *Prefix-Lengths Extension* (s. 4.1.2.) und/oder eine *One-Byte Padding Extension* (s. 4.1.3.) angehängt werden. Ein Home oder *Foreign Agent* sollte so konfiguriert sein, daß er periodisch *Advertisements* verschickt, kann aber auch so eingestellt sein, daß er nur auf *Solicitation messages* antwortet. Falls der Agent kontinuierlich *messages* versendet, sollte das Intervall zwischen zwei Nachrichten nicht größer als ein Drittel der Lebensdauer des ICMP Pakets sein. Der Abstand zwischen zwei Nachrichten sollte leicht variieren und zufällig gewählt werden, um eine Synchronisation mit anderen Routern zu vermeiden.

4.1.1. Bedeutung der Felder der Agent Advertisement Extension

Die in Abbildung 6 grün unterlegten Felder bilden die *Agent Advertisement Extension* und haben folgende Bedeutungen:

Type: Der Typ einer *Agent Advertisement Extension* ist 16.

Length: Die Länge setzt sich zusammen aus Sequence Number, Registration Lifetime, Flags, den reserved Bits und N, der Anzahl der *Care-of addresses*, also: 6+(4*N)

Sequence Number: Die laufende Nummer der *message*. Nach dem Booten des *Agents* wird bei 0 begonnen und dann ein Schritten von 1 aufwärts gezählt. Nach einem Rollover allerdings wird bei 256 begonnen, um dem *MH* so die Information darüber bereitstellen zu können, warum ein kleinerer Wert als bei vorherigen Nachrichten benutzt wurde.

Registration Lifetime: Die maximale Zeit in Sekunden, die der Agent in einer *Registration Request message* (s. 5.1.) bereit ist zu akzeptieren. Wenn alle Bits der Wert 1 besitzen, ist die Zeit als unendlich anzunehmen. Diese Feld ist völlig unabhängig von dem Lifetime Feld in dem ICMP Block.

Care-of address n: Mögliche *care-of addresses* (s. 2.3.), die zur Verfügung stehen. Ein *MH* soll immer versuchen, die erste Adresse in der Liste zu benutzten. Ist ihm das nicht gewährt, soll er schrittweise die folgenden Adressen ausprobieren.

Im folgenden werden die Bedeutungen der Flags erklärt:

R: Registrierung bei diesem *Foreign Agent* ist zwingend, auch wenn der *MH* eine *co-located care-of address* (s. 2.3.) benutzt. Das kann z. B. sinnvoll sein, wenn dem *MH* der Service in Rechnung gestellt wird.

B: Der *Foreign Agent* hat im Moment keine freie Kapazitäten und kann deshalb keinen Service für weitere *MHs* anbieten.

H: Der Agent dient als *Home Agent* in diesem Netzwerk.

F: Der Agent dient als *Foreign Agent* in diesem Netzwerk.

M: Dieser Agent kann Pakete verarbeiten, die mit der **minimal encapsulation** verpackt worden sind. Dieses Verfahren verzichtet auf die Felder im inneren IP Paket, die die selben Informationen, wie äußere Felder enthalten und stellt sie beim Auspacken wieder her. Dadurch werden anstatt 20 Bytes Overhead nur 8 - 12 Bytes produziert.

G: Diese Agent kann Pakete verarbeiten, die mit dem **GRE encapsulation** verpackt worden sind.

T: Der *Foreign Agent* bietet die Funktionalität **Reverse Tunneling**. Wenn *reverse tunneling* eingesetzt wird werden Daten, die vom *MH* gesendet werden zuerst zu seinem *Home Agent* *getunnelt* und von dort aus an den eigentlich bestimmten Empfänger weitergeleitet. So kann der *MH* z. B. seinen momentanen Aufenthaltsort geheim halten; für den Empfänger befindet sich der *MH* zu Hause.

r & reserved: Diese Bits sind für eventuell später entstehende Zwecke reserviert und werden immer mit dem Wert 0 codiert. Sie werden vom Empfänger ignoriert.

4.1.2. Die Prefix-Lengths Extension

Die **Prefix-Lengths Extension** kann an eine *Advertisement message* angehängt werden und beinhaltet die Netzwerkkennungen (NetIDs) der im ICMP Block gelisteten Router. Durch vergleichen der Kennungen kann der *MH* feststellen, ob er in ein anderes Netzwerk bewegt worden ist. Dieses Verfahren kann natürlich nur verwendet werden, wenn sowohl der vorherige Agent, als auch der nachfolgende die *Prefix-Length Extension* verwenden. In Abbildung 6 sind die zur *Prefix-Lengths Extension* gehörigen Felder gelb unterlegt und besitzen folgende Bedeutungen:

Type: Der Typ einer Agent *Prefix-Lengths Extension* ist 19.

Lengths: Die Anzahl der im ICMP Block gelisteten Router Adressen (Num Addrs Feld im ICMP Block), welches bei *Agent Advertisement messages* den Wert 0 annehmen kann.

Prefix Length n: Die NetID von Router n. Für alle im ICMP Block gelisteten Router werden hier nacheinander die NetIDs aufgezählt.

4.1.3. Die One-Byte Padding Extension

Die **One-Byte Padding Extension** dient lediglich dazu die Gesamtanzahl der Bytes der kompletten Nachricht bei Bedarf auf eine gerade Anzahl zu ergänzen, was von manchen IP Protokollen verlangt wird. Die Extension besteht, wie in Abbildung 6 rot unterlegt zu sehen ist, nur aus einem einzigen Feld mit folgender Bedeutung:

Type: Der Typ einer *One-Byte Padding Extension* ist 0.

4.2. AGENT SOLICITATION MESSAGES

Eine *Agent Solicitation message* gleicht einer ICMP Router *Solicitation message*, mit dem einzigen Unterschied, daß das Feld TTL (Time to live, deutsch: Lebensdauer) den Wert 1 haben muß.

5. REGISTRATION UND REPLY MESSAGES

Kapitel 5 beschreibt die technische Realisierung von dem Registrierungsprozess eines *Mobile Hosts* bei seinem *Home Agent* und gegebenenfalls zusätzlich bei einem *Foreign Agent*. *Registration Request messages* werden von einem *Mobile Host* direkt an seinen *Home Agent* bzw. zu einem *Foreign Agent*, zur Aufnahme und Weiterleitung an den *HA*, geschickt. Der *HA* generiert eine *Registration Reply message* und schickt diese direkt an den *MH* bzw. an den zwischengeschalteten *FA*, zur Aufnahme und Weiterleitung an den *MH*.

5.1. REGISTRATION REQUEST MESSAGES

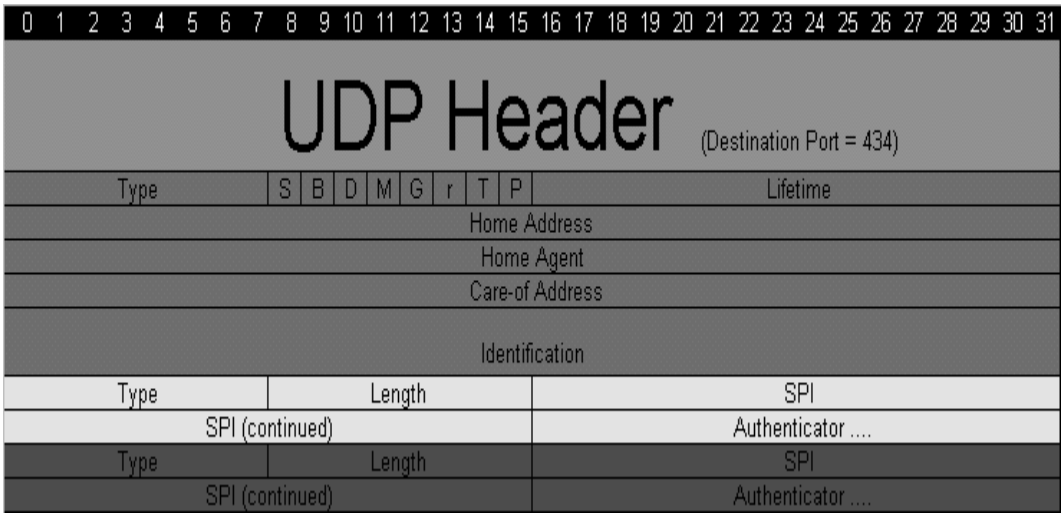

Abbildung 7

Die *Registration Request messages* werden via UDP gesendet, wobei das Feld Destination Port im UDP Header auf den Wert 434 gesetzt wird. Es muß eine *Authorization Enabling Extension* (s. 5.1.2.) angefügt sein, die zwischen *Mobile Host* und *Home Agent* gilt. Optional kann eine weitere **Mobile-Foreign Authentication Extension** (s. 5.1.3.) folgen, die wie der Name schon sagt, zwischen *Mobile Host* und *Foreign Agent* gilt. Falls vom *HA* keine Antwort in Form einer *Registration Reply message* zurückkommt, weil z. B. einer der beiden Nachrichten im Internet verloren ging, wird die *Request message* nochmals übertragen. Das Intervall zwischen zwei Sendungen, darf dabei nicht größer sein als die angeforderte Lebensdauer für die Registrierung im Lifetime Feld. Gleichzeitig muß es mindestens so groß sein, wie die Zeit, die eine Nachricht zweimal vom Sender und zurück braucht, zuzüglich 100 Millisekunden und wenn erwünscht weiterer 200 Millisekunden Satelliten Delay. Auf keinen Fall darf das Intervall kleiner als eine Sekunde sein und der Abstand zur nächsten Sendung sollte mindestens doppelt so groß sein, wie der des vorherigen Intervalls, aber selbstverständlich nicht größer als das erlaubte Maximum.

Zwischen dem *Request*-Teil und der *Authorization Enabling Extension* können noch andere, nicht der Authentifizierung dienende, *Extensions* eingefügt werden, die für den *HA* bestimmt sind. Für den *FA* bestimmte *Extensions*, die nicht zu Authentifizierungszwecken eingesetzt werden, können zwischen *Authorization Enabling Extension* und *Mobile-Foreign Authentication Extension* eingesetzt werden. Auf *Extensions*, die dafür in Frage kämen wird in diesem Dokument nicht näher eingegangen.

5.1.1. Bedeutung der Felder der Registration Request message

Die in Abbildung 7 grün unterlegten Felder bilden die *Registration Request message* und haben folgende Bedeutungen:

Type: Der Typ einer *Registration Request message* ist 1.

Lifetime: Die Anzahl der Sekunden, bevor die Registrierung als ungültig angesehen wird, wobei eine unendliche Zeit durch alle Bits auf 1 dargestellt wird und mit einem Wert von 0, eine Deregistrierung erwünscht ist. Der *Home Agent* kann natürlich eventuell nur eine kleinere als die gewünschte Lifetime erlauben und wird dann entsprechend antworten (s. 5.2.).

Home Address: Die IP Adresse des *Mobile Hosts*.

Home Agent: Die IP Adresse des *Home Agents* des *MHs*.

Care-of Address: Die IP Adresse für das andere Ende des Tunnels vom *HA* aus gesehen.

Identification: Eine 64 Bit Nummer, die von dem *MH* erstellt wurde und dazu dient, Registration *Requests* mit dem zugehörigen *Registration Reply* zu assoziieren und sich vor Replay Versuchen von böswilligen Hosts zu schützen.

Im folgenden werden die Bedeutungen der Flags erklärt:

S: Der *MH* wünscht, daß der *HA* mehrere *bindings* für ihn gleichzeitig verwaltet, anstatt das vorherige *binding* zu überschreiben. Wenn der *HA* dies unterstützt, dupliziert er jedes Paket und schickt eine Kopie an jede Adresse für jedes *binding*. Das kann z. B. sinnvoll sein, wenn der *MH* in einem *Wireless network* ständig zwischen mehreren *FAs* hin und her bewegt wird.

B: Der *MH* wünscht, daß Broadcast Nachrichten von seinem Heimatnetzwerk an ihn *weitergetunnelt* werden.

D: Der *MH* benutzt eine *co-located care-of address* (s. 2.3.).

M: *Minimal encapsulation* ist von *MH* erwünscht (s. 4.1.1.).

G: *GRE encapsulation* ist von *MH* erwünscht.

T: Der *MH* fordert *Reverse Tunneling* (s. 4.1.1.) an.

P: Der *MH* möchte seinen Aufenthaltsort geheim halten, was somit dem *HA* verbietet *binding update messages* an andere *Nodes* zu verschicken. Statt dessen wird er auf Anfragen antworten, daß der *MH* zu Hause sei.

r: Diese Bits sind für eventuell später entstehende Zwecke reserviert und werden immer mit dem Wert 0 codiert. Sie werden vom Empfänger ignoriert.

5.1.2. Die Authorization Enabling Extension

Genau eine **Authorization Enabling Extension** ist für jeden Registration *Request* zwingend vorgeschrieben. Sie dient als Sicherheitscode zwischen *MH* und *HA* und basiert auf einem geteilten Geheimnis zwischen diesen *Nodes*. In Abbildung 7 ist dieser Teil gelb unterlegt und enthält folgende Felder:

Type: Der Typ einer *Authorization Enabling Extension* ist 32.

Length: 4 Bytes plus die Länge des Authenticators.

SPI: SPI steht für Securi ty Parameter Index, der das Verschlüsselungsverfahren für den Authenticator bestimmt. Die Werte 0 – 255 sind reserviert und dürfen auf keinen Fall benutzt werden.

Authenticator: Der Authenticator ist von variabler Länge und besteht, wenn defaultmäßig keyed-MD5 prefix+suffix mode benutzt wird, aus einer Checksumme über das geteilte Geheimnis der *Nodes*, die Felder der *Request* oder *Reply message* und die dieser Extension und nochmals das geteilte Geheimnis.

5.1.3. Die Mobile-Foreign Authentication Extension

Eine *Mobile-Foreign Authentication Extension* ist nicht vorgeschrieben, kann aber am Ende einer *Registration Request message* stehen und dient der Sicherheit zwischen *Mobile Host* und *Foreign Agent* . In Abbildung 7 sind die Felder der möglichen Extension rot unterlegt und haben folgende Bedeutung:

Type: Der Typ einer *Authorization Enabling Extension* ist 33.

Length: 4 Bytes plus die Länge des Authenticators.

SPI: s. 5.1.2..

Authenticator: s. 5.1.2..

5.2. REGISTRATION REPLY MESSAGES

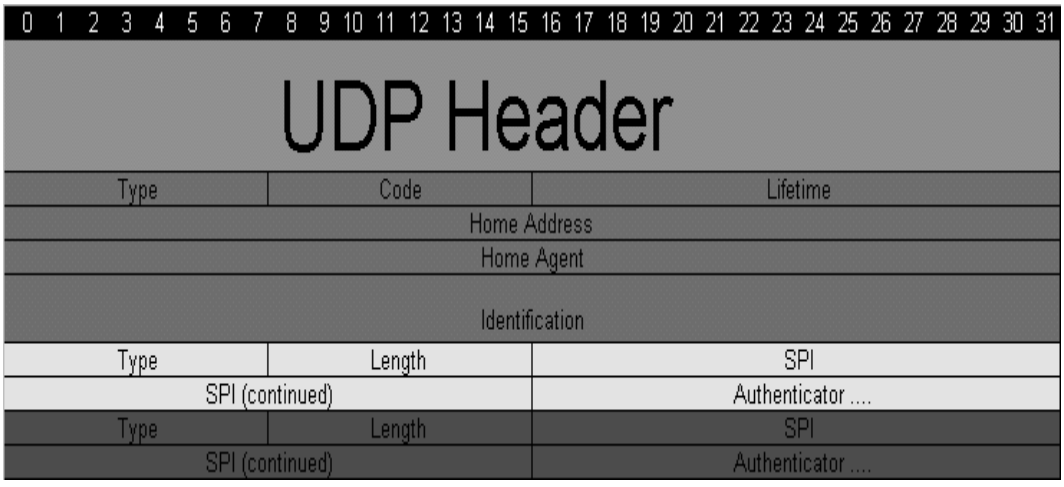

Abbildung 8

Registration Reply messages werden auch in UDP Paketen gesendet, wobei das Feld Destination Port im UDP Header aus dem Feld Source Port des zugehörigen *Requests* kopiert wird. Es muß eine *Authorization Enabling Extension* (s. 5.1.2.) angefügt sein, die zwischen *Mobile Host* und *Home Agent* gilt. Optional kann eine weitere **Foreign-Home Authentication Extension** (s. 5.2.3.) folgen, die wie der Name schon sagt, zwischen *Foreign Agent* und *Home Agent* gilt. *Reply messages* werden nicht bestätigt und auch somit nicht nochmals übertragen.

Zwischen dem *Reply*-Teil und der *Authorization Enabling Extension* können noch andere, nicht der Authentifizierung dienende, *Extensions* eingefügt werden, die für den *MH* bestimmt sind. Für den *FA* bestimmte *Extensions*, die nicht zu Authentifizierungszwecken eingesetzt werden, können zwischen *Authorization Enabling Extension* und *Mobile-Foreign Authentication Extension* eingesetzt werden. Auf *Extensions*, die dafür in Frage kämen wird in diesem Dokument nicht näher eingegangen.

5.2.1. Bedeutung der Felder der Registration Reply message

Die in Abbildung 8 grün unterlegten Felder bilden die *Registration Reply message* und haben folgende Bedeutungen:

Type: Der Typ einer *Registration Reply message* ist 3.

Code: Der Wert gibt Aufschluß über das Resultat des korrespondierenden *Requests*. Anhang A enthält eine Liste der momentan gültigen Werte.

Lifetime: Wenn der *Request* erfolgreich war, beinhaltet diese Feld die registrierte Lebensdauer, die kleiner sein kann, als ursprünglich angefordert.

Home Address: Die IP Adresse des *Mobile Hosts*.

***Home Agent*:** Die IP Adresse des *Home Agents* des *MHs*.

Identification: Eine 64 Bit Nummer, die von dem *MH* erstellt wurde und dazu dient, *Registration Requests* mit dem zugehörigen *Registration Reply* zu assoziieren und sich vor Replay Versuchen von böswilligen Hosts zu schützen.

5.2.2. Die Authorization Enabling Extension

Die Felder der *Authorization Enabling Extension* sind in Abbildung 8 gelb unterlegt. Siehe zur Erklärung der Felder bitte 5.1.2..

5.2.3. Die Foreign-Home Authentication Extension

Eine *Foreign-Home Authentication Extension* ist nicht vorgeschrieben, kann aber am Ende einer *Registration Reply message* stehen und dient der Sicherheit zwischen *Foreign Agent* und *Home Agent* . In Abbildung 8 sind die Felder der möglichen Extension rot unterlegt und haben folgende Bedeutung:

Type: Der Typ einer *Authorization Enabling Extension* ist 34.

Length: 4 Bytes plus die Länge des Authenticators.

SPI: s. 5.1.2..

Authenticator: s. 5.1.2..

6. ABSCHLUßBEMERKUNGEN

Leider bringt Mobile IP auch einige Nachteile mit sich, wie z. B. der zusätzliche Overhead, der durch das *Tunneling* verursacht wird oder die zusätzliche Netzbelastung durch das *Indirect Routing* über den *HA*. Eventuell können auch Probleme mit Firewalls oder schnellen Wechseln zwischen Netzen, die kürzer sind, als eine Sekunde, auftreten. Trotzdem wird Mobile IP wird ein immer wichtigerer Teil des Internets werden, da in den letzten Jahren immer mehr mobile Computer und *Wireless Networks* auf den Markt kamen und nicht nur die Gesamtanzahl der Internetnutzer steigt, sondern auch der relative Anteil an mobilen Nutzern.

Wünschenswert für einen Benutzer, wäre es in Zukunft, die Möglichkeit zu haben, ständig mit dem Internet verbunden zu sein. Denkbar wäre z. B., daß ein Notebook traditionell über ein Kabel an ein firmeninternes LAN angeschlossen ist, es aber nach dem ausstöpseln sich automatisch mit einem *Wireless LAN* verbindet und der Benutzer sich unter ständiger Verbindung zum Netz in der Firma umher bewegen kann, wobei der *Mobile Host* eventuell zwischen mehreren *Wireless LANs* hin und her wechselt. Darüber hinaus kann das Notebook mit auf Reisen genommen werden und immer noch Verbindung halten, wenn der *MH* auf ein in der Zukunft verfügbares *Wireless WAN* umschaltet.

Ein großer Vorteil von Mobile IP ist, daß es auf das bestehende Internet Protokoll aufgesetzt wird, d. h. Pakete werden durch *Tunneling* geroutet und Router auf dem Weg müssen nicht notwendigerweise Mobile IP implementieren. Somit kann das Protokoll schon von Organisationen eingesetzt werden, auch wenn es noch keine weite Verbreitung gefunden hat und Router im Internet können je nach Bedarf nach und nach aufgerüstet werden, ohne eventuell durchgehenden Mobile IP Verkehr zu behindern.

ANHANG A: LISTE DER BEDEUTUNG DER WERTE IM CODE FELD VON REGISTRATION REPLY MESSAGES

Die Codes lassen sich in drei Gruppen Gliedern:

0 – 8	Erfolgscodes
64 – 99	Fehlercodes vom *Foreign Agent*
128 – 192	Fehlercodes vom *Home Agent*

Typ	Beschreibung
0	registration accepted
1	registration accepted without simultaneous bindings
64	reason unspecified
65	administratively prohibited
66	insufficiant resources
67	mobile node failed authentication

68 home agent failed authentication

69 requested Lifetime too long

70 poorly formed *Request*

71 poorly formed *Reply*

72 requested encapsulation unavailable

73 reserved and unavailable

74 requested reverse tunnel unavailable

75 reverse tunnel is mandatory and 'T' bit not set

76 mobile node too distant

77 invalid *care-of address*

78 registration timeout

80 home network unreachable (ICMP error received)

81 home agent host unreachable (ICMP error received)

82 home agent port unreachable (ICMP error received)

88 home agent unreachable other ICMP error received

96 nonzero homeaddr required

97 missing NAI

98 missing home agent

99 missing home address

128 reason unspecified

129 administratively prohibited

130 insufficiant resources

131 mobile node failed authentication

132 foreign agent failed authentication

133 registration Identification mismatch

134 poorly formed request

135 too many simultaneous bindings

136 unknown home agent address

137 requested reverse tunnel unavailable

138 reverse tunnel is mandatory and 'T' bit not set

139 requested encapsulation unavailable