Mobile IPv4 - RFC 3220

Joachim Schiele

7. Dezember 2005

Inhaltsverzeichnis

1 Motivation

Diese Ausarbeitung behandelt die Thematik **Mobile IPv4** und versucht die wesentlichen Konzepte zu vermitteln. Dabei beziehe ich mich ausschließlich auf das **RFC 3220**[1]. Das Hauptanwendungsgebiet von **Mobile IPv4** liegt, wie man aus dem Namen leicht erahnen kann, im mobilen Bereich, also immer da wo Computer ihren Ort schnell wechseln und damit verbunden auch ihren Uplink ins Internet. **Mobile IPv4** ist die Schlüsseltechnologie, welche mobiles Roaming überhaupt erst ermöglicht. Mittlerweile haben sich auch andere Technologien etabliert, wie etwa TMip[2], welches auch transparentes Roaming ermöglicht ohne spezielle Anforderungen an den Klient zu stellen. Jedoch ist TMip, was unter [3] zu finden ist, nicht RFC 3220 konform. Die häufigste Anwendung wird wohl schlechthin bei wireless LAN Knotenpunkten liegen, also Handhelds, Handys, Laptops und anderen Technologien.

Eine der größten Komplikationen bei Mobile IPv4 ist, dass die IP Adresse des mobilen Gerätes (von nun an Mobile Host) für Verbindungen nach außen immer gleich bleiben muss, sich jedoch das Routing zum Rechner selbstständig ändern kann. Um dies zu realisieren benötigt man zusätzliche Rechner, die dann als Gateway dienen und die Verbindungen des Mobile Hosts nach seinem eigentlichen Adressenwechsel trotzdem offen halten. Das Ziel ist nämlich für die Gegenstelle im Internet eine immer gleich bleibende Adresse zu liefern. Man könnte dies mit NAT vergleichen, bei welchem die dynamische Adresse am Gateway durch eine offizielle ersetzt wird. Allerdings gibt es noch mehr Anforderungen, wie etwa [2]:

- **Transparenz**: Die Mobilität soll für die höheren Protokollschichten nicht sichtbar sein und alle geöffneten TCP-Verbindungen sollen den Ortswechsel überdauern solange keine Datenübertragung stattfindet.
- **Kompatibilität**: Es darf keine Änderung bei den stationären Endsystemen (Rechner und Router) notwendig sein. Die mobilen Endgeräte müssen das gleiche Adressformat besitzen wie die stationären Hosts.
- **Sicherheit**: Die Authentifikation der Endgeräte muss überprüft werden.
- **Effizienz**: Die Endgeräte haben meist nur eine geringe Bandbreite.
- **Skalierbarkeit**: Es muss ohne große Änderungen möglich sein, eine große Menge mobiler Endgeräte zu verwalten.

2 Grundlegende Probleme

Wie man schnell sieht, existiert eine gewisse Problematik. Unter IPv4 wird angenommen, dass jede Route von oder zu einem Rechner(Anbindungspunkt) mittels einer IP eindeutig festgestellt werden kann. Daraus ergibt sich, dass eine IP-Adresse, falls diese Daten empfangen soll, sich auch in dem zugeteilten Netzwerksegment befinden muss. Falls diese Bedingung nicht erfüllt werden kann, so können keine Daten empfangen, eventuell aber gesendet werden (NAT). Diese kommen jedoch nirgendwo an bzw. sie verenden am Gateway, der zwar weiß, dass er die Daten an (192.168.1.4) senden soll, es aber keine Möglichkeit gibt in dieses Netz zu routen. Wenn ein Rechner nun seinen Anbindungspunkt ändert, so verliert er die Möglichkeit wie gewohnt zu kommunizieren. Es müsste also mindestens eine der folgenden Bedingungen erfüllt sein:

1. Ein Rechner muss seine IP-Adresse immer dann ändern, wenn er einen neuen Anbindungspunkt erhält (also Wechsel des Netzes).
2. Alternativ könnte bei jedem Anbindungspunktwechsel eine neue Route zu dem Rechner erstellt und propagiert werden.

Jedoch sind beide Ansätze ungeeignet. Der erste macht es unmöglich einem mobilen Rechner den Transportlayer und höhere Layer transparent zu halten, so dass Verbindungen zu außen stehenden Rechnern[3] nach Eintritt in ein neues Netz weiterbestehen können. Der zweite Ansatz ist nicht realisierbar, da Routingprotokolle des Internets[4] meist träge auf Änderungen reagieren und sich mobile Rechner sehr schnell durch viele verschiedene Netzabschnitte bewegen können. Dies würde zu viel Aufwand für das gesamte Routing bedeuten (Skalierungsproblem). Nebenbei bemerkt sind Protokolle wie AODV und DSR gerade für solche (bzw. sehr ähnliche) Situationen erfunden worden. Allerdings sind diese für mobile IPv4 nicht von besonderer Bedeutung. Diese Problematik war der Startschuss für die Erfindung von mobile IPv4 und wird u.A. näher in RFC 3220 beschrieben.

[1] Vgl. [1]
[2] *http://www.slyware.com/projects_tmip.shtml*
[3] Etwa dem Webserver aus folgendem Beispiel.
[4] OSPF/RIP

3 Anforderung an die Protokolle

Ein mobiler Knotenpunkt (Mobile Host) muss, nachdem er die Linklayer-Adresse geändert hat, mit anderen Knotenpunkten kommunizieren können, obwohl er seine IP nicht geändert hat. Außerdem muss ein Knotenpunkt immer mit anderer bestehender Hardware, also Knotenpunkten, kompatibel bleiben, auch wenn diese nicht die selben Mobilitätsfunktionen implementiert haben. Es werden keine Protokollerweiterungen in Rechnern oder Routern benötigt. Alle Nachrichten, die vom Knotenpunkt ausgehen und dessen Position im Netz ändern, müssen natürlich authentisiert werden, da ein Angreifer sonst den Datenverkehr einfach umleiten könnte (Spoofing).

In vielen Fällen wird wireless LAN das Mittel der Wahl sein und damit sind weitere komplizierte Anforderungen verbunden. Zum einen eine niedrige Bandbreite, und damit eine erhöhte Fehlerrate als bei herkömmlichen Netzwerken. Zudem laufen mobile Geräte oft mit Batterie. Also muss sowohl der Stromverbrauch als auch das Datenvolumen minimiert werden. Die Sendedauer sollte kurz sein und die Anzahl der zu sendenden Kontrollnachrichten gering. All diesen Anforderungen versucht mobile IPv4 gerecht zu werden.

4 Prinzipielle Funktionsweise

Ein mobiler Client bekommt jeweils zwei Adressen zugewiesen, eine primäre Adresse (**Home Adresse**), also die Adresse des **Home Agents**, und eine sekundäre Adresse (**Care of Adresse, kurz COA**). Wenn der mobile Client nun in ein neues Netz gelangt, so bekommt er automatisch eine Adresse zugewiesen, die COA, welche er dann seinem **Home Agent** mitteilt. Der **Home Agent** selbst besitzt die zum Internet hin echte eindeutige IP Adresse welche der Mobile Host indirekt zum Empfang verwendet. Falls der **Home Agent** nun Daten empfängt welche eigentlich für den mobile Client bestimmt sind, dann wird er diese an die COA senden, also dem Mobile Host (IP to IP Kapselung).

Der Mobile Host kann jederzeit Daten direkt an jeden Rechner ins Internet senden (Abbildung 1). In einigen fällen kann jedoch eine Firewall, welche auf dem Internet-Router im Care of Agent Netz läuft, die Absenderadresse welche vom Mobile Host auf die des Home Agents (Home Adresse) setzt, fälschlicherweise als nicht erlaubte Absenderadresse filtern. Eine Lösung zu diesem Problem wäre den ausgehenden Datenverkehr auch über den Home Agent laufen lassen. (Problem: Umweg, Latenzzeiten, doppletes Datenaufkommen)
Falls der Web Server nun eine Antwort an den Mobile Client senden will, so verläuft der Paketstrom immer über den Home Agent (Abbildung 2), da der Mobile Host die Daten via IP to IP Kapselung empfängt, nie direkt.

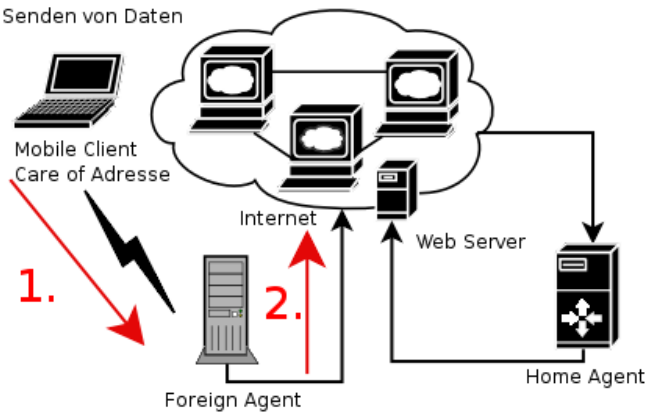

Abbildung 1: Senden von Daten

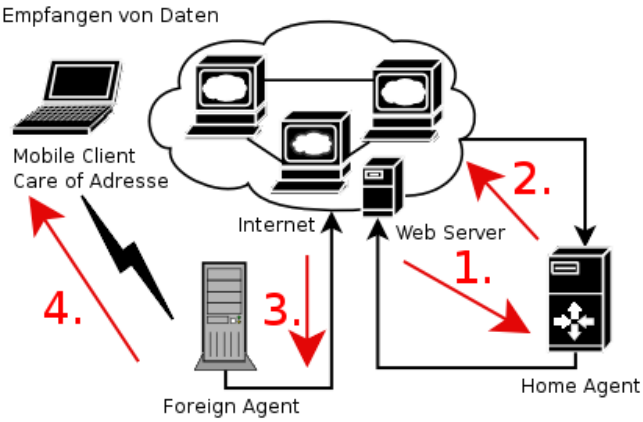

Abbildung 2: Empfangen von Daten

Eine Erweiterung des Protokolls zur Sicherstellung, dass niemand die Daten mitlesen oder ändern kann wird durch den Hin- und Rückweg sämtlichen Datenverkehrs über den Home Agent realisiert. Hier könnte die Verbindung dann vollkommen verschlüsselt werden (VPN/ipsec).

- Das Senden von Daten zu einem Webserver: ..... (Abbildung 1)
  Der Mobile Host sendet Daten an den Foreign Agent **(1)**, welcher die Daten direkt an den Webserver weiterleitet **(2)**. Wie wir im nächsten Abschnitt sehen werden, gibt es zwei mögliche Verfahren Daten zu senden: **„Co Located Care-Of-Address“** oder **„Foreign Agent Care-Of-Address“**. Im ersteren Fall wird kein Foreign Agent verwendet. Jedoch im zweiten Fall (wie in Abbildung 1/2 illustriert).
- Das Empfangen von Daten: ..... (Abbildung 2)
  Da direktes Rücksenden der Daten, an die COA, nicht funktionieren würde, weil sonst der Linklayer nicht mehr transparent arbeiten würde, muss hier ein Umweg über den Home Agent realisiert werden.

Der Webserver sendet seine Antwort nun an den Home Agent **(1)**. Praktisch betrachtet existiert für den Webserver eigentlich nur eine Verbindung zum Home Agent. Dieser sendet nun die empfangen Daten über das Internet zum Foreign Agent **(2) und (3)**. Der Foreign Agent leitet die empfange Antwort des Webservers nun an die COA **(4)**.

4.1 Mögliche Verfahren IP Adressen zu beziehen:

Wenn ein Mobile Host nun in ein neues Netzwerk kommt, so muss er eine andere IPv4 Adresse beziehen um wieder Kontakt mit dem Internet zu erhalten. Es gibt nach RFC3220 zwei Verfahren, welche diese Aufgabe bewerkstelligen:

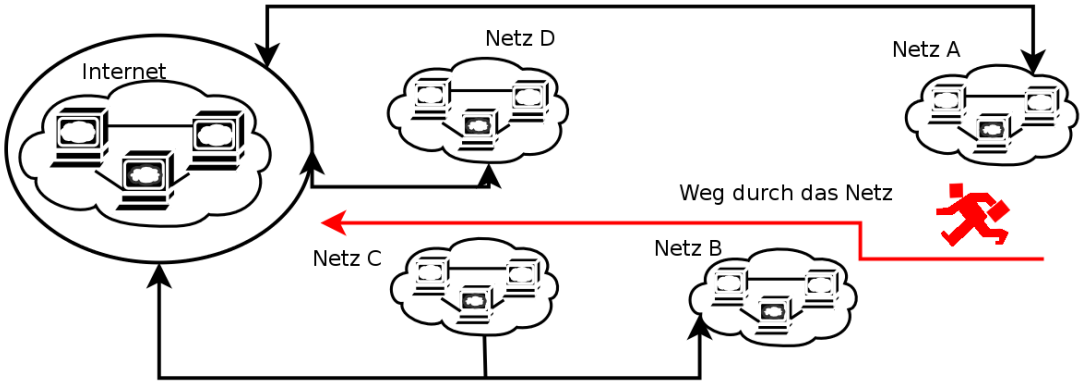

Abbildung 3: Weg durch verschiedene Netze

1. **„Co Located Care Of Address“**
   RFC3220: Eine *“co located care of address“* ist eine care of Adresse[5] welche der Mobile Host, z.B. durch DHCP oder einer vorher festgelegte IP Adresse, erhalten hat. Diese IP ist gleichzeitig seine COA. Der Datenverkehr fungiert nicht gleich, wie im zweiten Fall unten (also 2), etwa mittels eines *Foreign Agents*. Datenverkehr fungiert jedoch äquivalent dazu, da der Host selbst auch quasi *Foreign Agent* ist. Pakete welche der Mobile Host erhält müssen von diesem selbst entpackt werden, da der Host selbst den Endpunkt des Tunnels darstellt, hierzu aber unten mehr. Dieser Arbeitsschritt wird normalerweise vom *Foreign Agent* übernommen.

   In Worten der Wikipedia: Hier übernimmt der Mobile Host das Forward Management. Er benutzt die Home Adresse (für die höheren Protokollschichten) und die COA (für die niedrigen) dabei gleichzeitig. Die COA wird dem Mobile Host dabei aus einem lokalen IP-Adresspool (z.B. via DHCP) zugewiesen, wie es auch bei einem stationären Host geschehen würde. Deshalb können die lokalen Router nicht unterscheiden, ob der Host ein mobiler oder ein stationärer ist.
   Der Vorteil liegt hier darin, dass auf der lokalen Infrastruktur aufgesetzt werden kann und kein Foreign Agent notwendig ist. Ein Nachteil ist die Adressenknapheit bei IPv4, so kann ein Foreign Agent ganze Netze mit einer IP Adresse verwalten.

2. **„Foreign Agent Care Of Address“**
   RFC3220: Eine *„Foreign Agent care of address“* ist eine care of Adresse welche von einem *Foreign Agent*, mittels der **„Foreign Agent Advertisement“** Nachricht, vergeben wird. In diesem Fall ist die *COA* die IP Adresse des Foreign Agents. In diesem Modus stellt der Foreign Agent den Endpunkt des Tunnels dar. Wenn er eingekapselte[6] Daten erhält, so werden diese entpackt und an den Mobile Host weitergereicht. Dies ist im Vergleich zum *„co located care of address“* Modus die bevorzugte Variante, weil es vielen mobilen Hosts über die selbe IP Zugang gibt und dies den schon knappen Vorrat an IPv4 Adressen nicht weiter belastet.

   In Worten der Wikipedia: Hier wird dem Mobile Host die COA von einem speziellen Rechner (Foreign Agent) des fremden Netzwerkes zugewiesen. Dazu muss sich der Mobile Host zuvor beim Foreign Agent anmelden und bekommt dann eine Netzwerkspezifische IP Adresse zugewiesen. Der Foreign Agent übernimmt bei dieser Variante die Weiterleitung der Daten an die COA.
   Um sich beim Foreign Agent anzumelden, benötigt der Mobile Host zunächst einmal dessen Adresse.

[5] IPv4 Adresse
[6] Dies bezieht sich auf die IP Datagramme, da komplette IPv4 Pakete wiederum in IPv4 Pakete eingepackt werden.

4.2 Finden des Foreign Agents

Nachdem der moblie Host im fremden Netz angemeldet ist, sendet er eine **„ICMP Router Solicitation Nachricht“** aus. Diese Nachricht braucht laut RFC 3220 nicht authentifiziert sein. Der Foreign Agent sieht diese Nachricht und beantwortet sie mit einer **„ICMP Router Advertisement Nachricht“**, welche durch eine „Mobility Agent Advertisement Extension„ erweitert ist. Dank der Erweiterung, erhält der Mobile Host alle Informationen welche nötig sind:

Aufbau des „Agent Advertisement“

1. Link-Layer Felder: Link Layer Ziel-Adresse in Bezug auf die „Solicitation-Nachricht“.
2. IP-Felder:
   TTL muss auf 1 stehen.
   Ziel Adresse: 224.0.0.1 oder die limitierte Broadcast-Adresse 255.255.255.255
3. ICMP-Felder: Das Codefeld wird wie folgt interpretiert:
   (a) 0 Der Mobile Agent behandelt jeglichen Datenverkehr wie ein Router.
   (b) 16 Der Mobile Agent routet keine Daten. Jedoch gibt es ein gewisses Minimum an Daten, welche er routen muss.

Das ICMP-Router-Advertisement kann, muss aber keine, Adressen von Routern im Netz enthalten.
Der Mobile Host kann sich nun mittels der Mobile IP Registrierungsprozedur registrieren lassen.

Für IPv6 gibt es erweiterte Varianten wie Mobile IPv6, „Hierarchical Mobile IPv6„ und „Fast Mobile IPv6 “. Dank der erweiterten Routing-Fähigkeiten von IPv6 ist hier u.A. die Möglichkeit hinzugekommen, Pakete ohne Umweg über den Home-Agent direkt an den mobilen Rechner zu schicken.

Ein Mobile Host weiß nun für eine vom Foreign Agent festgelegte Zeit, dass in diesem Netzsegment ein Foreign Agent existiert, da diese Information in dem „Agent Advertisement“ enthalten ist. Der Foreign Agent muss „Agent Advertisements“ periodisch senden, auch wenn kein Mobile Host eine Anfrage gesendet hat, denn ein Mobile Host behält die Information über die Existenz des Foreign Agent nur für eine gewisse Zeit im Speicher, danach verwirft er sie und wartet auf andere Angebote von anderen Foreign Agents. Der Intervall in dem „Agent Advertisements“ vom Foreign Agent gesendet werden, sollte nicht länger als 1/3 der Lebensdauer des Paketes selbst sein. Zusätzlich muss ein kleiner zufälliger Wert zum Sendeintervall addiert werden, der Sinn besteht darin mit anderen Routern eine Kollision zu vermeiden.

Eine andere wichtige Bedingung ist, dass ein Foreign Agent zwar ausgelastet sein darf und bei zu vielen Anfragen die Anfragen selbst verweigern kann, jedoch muss sichergestellt sein, dass er weiterhin „Agent Advertisements“ sendet. So kann garantiert werden, dass schon registrierte Mobile Hosts nicht denken, sie wären nicht mehr in Empfangsweite zu ihrem Foreign Agent.

4.3 Die Registrierung

Mobile IP Registration stellt für Mobile Hosts einen flexibelen Mechanismus bereit um Informationen wie Erreichbarkeit dem Home Agent mitzuteilen. Dies sind Methoden welche dazu verwendet werden:

1. Weiterleitungsanfragen (forwarding) beim eintreten in ein fremdes Netz.
2. Dem Home Agent die COA mitteilen.
3. Eine Registrierung erneuern, falls sie am Ablaufen ist.
4. Abmeldung vom fremden Netz, falls das Heimatnetz in Reichweite ist.

In einer Registrierungsnachricht werden Informationen zwischen einem Mobile Host, ev. dem Foreign Agent und dem Home Agent ausgetauscht. Die Registrierung erzeugt oder ändert eine Verbindung mit dem Home Agent und assoziiert eine COA für einen bestimmten Zeitabschnitt mit dem Home Agent. Jedoch gibt es noch andere Möglichkeiten welche während der Registrierungsprozedur möglich sind:

1. Finden der home Adresse, falls der Mobile Host noch nicht konfiguriert ist bzw über diese Information nicht verfügt.
2. Das Aufrechterhalten von mehreren gleichzeitigen Registrierungen, so dass eine Kopie von jedem Datenpaket an jede aktive COA getunnelt wird.
3. Abmelden einer bestimmten COA während andere Verbindungen erhalten bleiben.

4.4 Registrierungsübersicht

Es gibt zwei unterschiedliche Registrierungsprozeduren. Eine mit, bzw über einen Foreign Agent, während die andere diesen nicht braucht und dies mittels direkter Kommunikation mit dem Home Agent bewerkstelligen kann. Die folgenden Regeln legen fest, welche von beiden Methoden verwendet wird:

1. Wenn ein mobiler Host eine Adresse von einem Foreign Agent bezogen hat, dann muss er sich auch über diesen registrieren.
2. Wenn ein mobiler Host eine „co located care of Adresse“ verwendet, er jedoch am selben Link „Foreign Agent Advertisements“ erhält, dann sollte er über diesen registrieren falls das R-Bit in der empfangenen „Agent Advertisement“ Nachricht gesetzt ist.
3. Wenn ein mobiler Host eine „co located COA“ verwendet, muss er sich direkt beim Home Agent registrieren.
4. Wenn ein mobiler Host in sein Heimatnetz zurückkehrt und sich bei seinem Home Agent abmeldet (deregistriert), dann muss der Mobile Host sich wieder direkt bei seinem Home Agent registrieren.

Beide Registrationsvarianten verwenden Registration Request and Registration Reply messages um zu kommunizieren. Falls die Registrierung über einen Foreign Agent gemacht wird, werden folgende 4 Nachrichten benötigt:

1. Der Mobile Host sendet ein Registration Request zu seinem zugehörigen Foreign Agent um den Registrierungsprozess zu initialisieren.
2. Der Foreign Agent erhält und verarbeitet die Registrierungsanfrage (registration Request) und sendet ihn dann dem Home Agent (via Relay).
3. Der Home Agent sendet sein Antwort (Registration Reply) dem Foreign Agent worin entweder eine Annahme oder eine Ablehnung enthalten ist.
4. Der Foreign Agent verarbeitet das Registration Reply und sendet es dann dem Mobile Host um diesen über den Status seiner Anfrage in Kenntnis zu setzen.

Falls der Mobile Host alternativ direkt beim Home Agent registriert, unterscheidet sich diese Registrierungsprozedur etwas von der Vorherigen:

1. Der Mobile Host sendet ein Registration Request zum Home Agent.
2. Der Home Agent sendet einen Registration Reply zum Mobile Host und akzeptiert oder lehnt die Verbindung ab.

Als Protokoll sollte für die Registrierungsnachrichten UDP verwendet werden. Dabei sind Parameter wie die Headerchecksum nach RFC 3220 zu beachten.

4.5 Registration Reply

Der Reply enthält alle nötigen Informationen um den Mobile Host über den Status seiner Anfrage zu informieren. Zusätzlich findet sich auch die Laufzeit bzw Lebensdauer der zu registrierenden Verbindung. Die Antwort (Reply) kann weniger Umfang haben als die Registrierungsanfrage. Der Home Agent hat die Nachricht authentisiert. Dabei sind die im RFC 3220 vorgeschlagen ev. Änderungen der Lebenszeit zu beachten, da eine Änderung im Reply seitens des Home Agents zu Komplikationen mit der Konfiguration des Foreign Agents erzeugen kann.

5 Routing Überlegungen

Im folgenden Teil soll kurz umrissen werden wie Datagramme von unterschiedlichen Typen geroutet werden. Dabei kommt es auf die verwendete Topologie an, wie: mobile nodes, Home Agents, und (ev.) Foreign Agents.

5.1 Einkapselung von IP-Datagrammen: (Encapsulation Types)

Home Agents und Foreign Agents müssen Datenpakete, mittels IP in IP Einkapselung, tunneln können. Zusätzlich muss der Mobile Host welcher „co locate COA“ verwendet auch IP in IP Einkapselung unterstützen. **„Minimale Einkapselung“** wie **„GRE Einkapselung“** sind alternative Einkapselungsmethoden welche optional implementiert sein können.

5.2 Unicast Datagramm-Routing

5.2.1 Mobile Host Überlegungen

Falls sich der Mobile Host im Heimnetzwerk befindet, ist das Routing wie bei jedem anderen Rechner, über einen Router geschalten. Wenn sich ein Mobile Host an einem fremden Netzwerk anmeldet muss ein standard Router gewählt werden, die Wahl befolgt diese Regeln:

1. Falls ein Mobile Host eine Foreign Agent COA verwendet, kann er ev. den Foreign Agent als default Router wählen. Die MAC Adresse ist aus dem Agent Advertisement bekannt. Alternativ kann der Foreign Agent via „ICMP Router Advertisement“ eine Liste an Routern angeben aus der der Mobile Host wählt.

2. Wenn ein Mobile Host direkt mit dem Home Agent verbunden ist, also co located COA, dann sollte er sich den Router aus den ICMP Router Advertisement Nachrichten beziehen. Zu beachten ist u.A. der Netzwerkprefix.

Es gibt hier noch einige weitere wichtige Regeln, siehe RFC 3220.

5.2.2 Foreign Agent Überlegungen

Der Foreign Agent muss Datagramme routen welche er von registrierten mobilen Hosts empfängt. Er muss mindestens die IP „Header“-Prüfsumme prüfen und diese auch neu berechnen, wenn er die TTL erniedrigt um es an den nächsten Router weiter zu geben.

Ein Foreign Agent darf kein Broadcast-ARP verwenden um die MAC Adresse eines Mobile Hosts zu bekommen. Die MAC darf er nur aus einem Agent Solicitation oder Registration Request entnehmen welcher der Mobile Host gesendet hat. Das ARP-Cache eines Foreign Agent darf nicht verfallen bevor die Besucherliste, in der alle Registrierten Mobile Hosts stehen, abgelaufen ist.

Es gibt hier noch einige weitere wichtige Regeln, siehe RFC 3220.

5.2.3 Home Agent Überlegungen

Wenn die Lebenszeit für eine mobile Verbindung ausläuft bevor der Home Agent eine gültige Registrierungsanfrage erhalten hat, wird die mobile Verbindung von der Liste der registrierten Mobile Hosts entfernt. Der Home Agent darf dann wegen der abgelaufenen Verbindung keine Registrierungsantwort senden. Der Eintrag im Foreign Agent, über die Verbindung zum Home Agent, wird auf Grund des Zeitgebers (timer), der bei beiden Computern gleichzeitig abläuft, auch ihn über den Timeout in Kenntnis setzen. Wenn die Verbindung von Home Agent zu Mobile Host abgelaufen ist, darf der Home Agent diese dann komplett verwerfen, jedoch nicht z.B. die Verbindungen zu anderen Rechnern wie z.B. den Webserver, da es jeder Zeit möglich sein muss diese wieder aufzubauen. Der Sinn von Mobile IPv4 besteht ja darin, dass sich ein Mobile Host bei beliebig vielen Foreign Agents bedienen kann und dabei die Verbindungen die er mit der echten IP über den Home Agent macht nicht verloren gehen.

Es gibt hier noch einige weitere wichtige Regeln, siehe RFC 3220.

5.3 Broadcast Datagramme

Falls ein Home Agent ein Broadcast-Datagramm empfängt, darf er diese nicht weiterreichen (forwarden). Falls ein Mobile Host während der Registrierung das ’B’ Bit in seinem Registration Request angegeben hat, darf der Home Agent das Datagramm weitergeben (forwarden).

Falls das ’D’ Bit während der Registrierung gesetzt war ist alles viel komplizierter und sollte genau, wie in RFC 3220 vorgeschlagen wird, abgehandelt werden.

5.4 Multicast Datagramm Routing

Falls ein Mobile Hosts multicasts empfangen will, muss er einer multicast Gruppe beitreten (join). Es gibt hierfür zwei Wege. Er kann diese Gruppe über einen lokalen multicast Router im besuchten Netzwerk beitreten oder alternativ auch die home Adresse des Home Agents verwenden. Dies wird durch den bidirektionalen Tunnel erreicht. Dabei muss der Home Agent allerdings auch multicast Router sein, was nicht immer der Fall sein wird. Der Mobile Host tunnelt IGMP Nachrichten zu seinem Home Agent und dieser forwarded die multicast Datagramme durch den Tunnel zum Mobile Host. Datagramme welche vom Mobile Host zum Home Agent getunnelt werden, sollten als Zieladresse die Adresse des Home Agents verwenden.

Es gibt hier noch einige weitere wichtige Regeln, siehe RFC 3220.

6 Mobile Routers

Ein mobiler Host kann die Funktion eines Routers übernehmen und somit für ein ganzes Subnetz verantwortlich sein. Dann bewegt sich jeweils ein ganzes Netzwerk, z.B. in einem Flugzeug, Schiff, Zug, Auto, Fahrrad oder in Herzschrittmachern einer Wandergruppe von Rentnern. Die Rechner welche an den mobilen Router angeschlossen sind, können jeweils normale PCs sein oder auch mobile PCs wie PDA, Laptop, ..., solche Netzwerke nennt man wieder Erwartens: mobile Netzwerke.

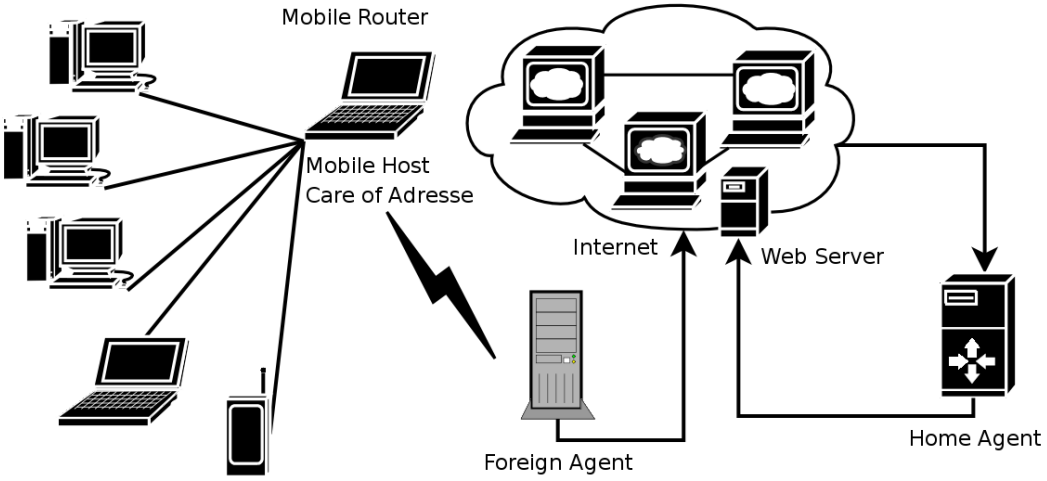

Abbildung 4: Ein Mobile Router versorgt 5 andere Teilnehmer mit einer Internetanbindung.

7 Sicherheitsaspekte

Da sich wireless LAN Verbindungen im mobilen Bereich durchgesetzt haben, sind hier noch einige Komplikationen im Spiel wie „passive eavesdropping“, „aktive replay Attacken“ und andere aktive Attacken. Um hier mehr Sicherheit garantieren zu können werden einige Verfahren implementiert:

7.1 Message Authentication Codes

Home Agents und Mobile Hosts müssen Authentifizierung implementiert haben. Der Standardalgorithmus hierfür ist HMAC-MD5 mit einer Schlüsselgröße von 128 Bits. Selbiges gilt auch für den Foreign Agent. Die Schlüsselverteilung ist manuell.

Da die *prefix+suffix* Verwendung von MD5, zur Sicherung von Daten, als unsicher gilt, sollte dies nur zur Rückwertskompatibilität implementiert sein. Alle Neueren Implementierungen sollten **keyed MD5** verwenden.

Zitat aus der „The Encyclopedia of Networking and Telecommunications“:

„Keyed MD5 is a technique for using MD-5. Basically, a sender appends a randomly generated key to the end of a message, and then hashes the message and key combination to create a message digest. Next, the key is removed from the message and encrypted with the sender's private key. The message, message digest, and encrypted key are sent to the recipient, who opens the key with the sender's public key (thus validating that the message is actually from the sender). The recipient then appends the key to the message and runs the same hash as the sender. The message digest should match the message digest sent with the message.“

7.2 Wichtige Sicherheitsüberlegungen im Protokoll

Ein großes Problem stellt auch die Verwendung von Tunneln dar, da ein bösartiger User den Datenverkehr via wireless LAN einfach umleiten könnte. Um dies zu verhindern sind die ARP-Anfragen wie die Datenverbindungen selbst unbedingt zu authentifizieren.

7.3 Schlüsselverwaltung

Diese Spezifikation benötigt einen strengen Authentifikationsmechanismus: keyed MD5 welcher sehr viele potenzielle Attacken unwirksam macht. In Umgebungen wie einer Firma sollten alle Verbindungen authentifiziert sein um verlässliche Sicherheit zu bekommen.

7.4 Privatsphäre

Wer Wert auf absolute Anonymität legt, sollte jeglichen ausgehenden Verkehr über den Home Agent tunneln und die Verbindung auf Linklayer-Ebene verschlüsseln.

7.5 Eingangsfilter

Falls eine Firewall beim Senden von Daten ein Problem wird, sollte auch hier der gesamte Datenverkehr welcher geblockt ist über den Home Agent getunnelt werden. Ein Problem kann sein, dass ein Router keine Absenderadressen akzeptiert, welche er im lokalen Netz (192.168.1.x) nicht erwartet.

7.6 Replay Protection für Registrierungsanfragen

Das Identifizierungsfeld wird dazu verwendet um den Home Agent prüfen zu lassen, ob eine Registrierungsnachricht eine neu generierte Nachricht eines Mobile Hosts ist. Um dies zu bewerkstelligen werden timestamps und nonces verwendet. Der Sinn besteht darin, dass nicht ein schon registrierter bösartiger Mobile Host Registrierungsdatagramme anderer Mobile Hosts abfängt und die Verbindung abhört. Zeitstempel müssen implementiert sein während Nonces optional sind.

Die Art der Verbindungssicherung muss beim Verbindungsaufbau vom Mobile Host und Home Agent festgelegt werden.

7.6.1 Replay Protection mit Verwendung von Zeitstempel

Das Prinzip von Zeitstempeln ist es die Zeit in einer Anfrage mitzusenden. Der Empfänger prüft diese und vergleicht sie mit seiner Lokalzeit. Abweichungen über einen bestimmten Wert, hier 7 Sekunden, führen dazu, dass das Request verworfen wird. Dies setzt voraus, dass beide Rechner über eine genaue Systemzeit verfügen.

Falls Zeitstempel verwendet werden, muss der Mobile Host das Identificationfeld auf ein 64 Bit Wert gesetzt haben, wie es im NTP Format getan wird. Da hier auch Zufallszahlen verwendet werden ist es wie bei allen Krypographischen Verfahren wichtig, gute Zufallszahlen zu haben.

Wenn nun ein Home Agent eine Registration Anfrage bekommt und diese die *Authorization Enabling Extension* gesetzt hat, so muss er das Identificationfeld genau prüfen. Um dies als gültig zu bestätigen muss die Zeit, also die hohen 32 Bits, fast gleich sein und die restlichen Bits (als Zahl interpretiert) müssen jeweils größer sein, als die in der ev. vorhergegangenen Registrierungsanfrage.

Falls die Anfrage nun als korrekt erkannt wurde, muss der Home Agent das Identification Feld kopieren und in der Antwort mitsenden. Falls die Anfrage nicht gültig war, so kopiert er seine lokale Zeit und setzt die empfangenen niederen 32 Bits der Anfrage in seine Antwort mit ein. Er sendet dann die Antwort mit dem Code 133 (identification mismatch) als Registrierungsantwort und lehnt die Registrierung des Mobile Host hiermit ab.

7.6.2 Replay Protection mit Verwendung von Nonces

Das Prinzip von *Nonce Replay Protection* ist, dass der Host A eine zufällige Nummer in das Datenpaket inkludiert. Host B empfängt diese und setzt diese auch wieder in die Antwort mit ein wie auch eine eigene zufällige Nummer die Host B erstellt. Dieses Prinzip wird für jedes weitere Paket mit jeweils neuen Nummern wiederholt. So kann sicher gestellt werden, dass die Pakete jeweils neu sind und nicht etwa von einem bösen User, welcher alte Paketsequenzen einfach wiederholt sendet. Dies bietet allerdings keinen Schutz gegen aktive Echtzeitmanipulationen.

8 Implementierungen

Hier eine ganz allgemein gehaltene Übersicht, wo mobile IPv4 schon implementiert wurde. Dies ist kein objektiver Vergleich der Implementierungen sondern mehr eine Liste an Projekten und deren eigene Beschreibungen - die Liste erhebt keinen Anspruch vollständig zu sein.

8.1 *http://dynamics.sourceforge.net/*

Dynamics HUT Mobile IP der Helsinki-Universität: diese Implementierung unterstützt Kernel 2.2 und 2.4. Die Software läuft auch unter Microsoft-Betriebssystemen, wenn die Cygwin-DLLs installiert sind. Leider hat die Helsinki-Universität im Oktober 2001 die Entwicklung eingestellt.

8.2 *http://www.monarch.cs.cmu.edu/mobile_ipv4.html*

IETF Mobile IPv4 for 4.4BSD-based Unix systems:

The Rice Monarch Project implementation of IETF Mobile IP directly supports both NetBSD and FreeBSD. The current version of the software is Release 1.1.0 and supports NetBSD 1.1 and FreeBSD 2.2.2. Earlier versions of the code have also run on older releases of NetBSD. The code should be easily portable to other systems based on 4.4BSD (or at least based on the Berkeley Net/3 networking kernel source), including BSDI, OpenBSD, and other versions of NetBSD and FreeBSD. Our implementation, since Release 1.0.0, fully conforms to the IETF standard Mobile IP protocol for IPv4, as specified in RFC 2002, and includes both IP-in-IP and minimal encapsulation support (RFC 2003 and RFC 2004).

8.3 *HP − UX MobileIPv4*

The HP-UX Mobile IPv4 product will run on any HP9000 server or workstation running HP-UX version 11i (11.11). The product can run on either 32-Bit or 64-Bit HP9000 platforms.

9 Zukunftsaussichten & Vergleich mit IPv6

Hier einige wichtige Änderungen von mobile IPv4 zu mobile IPv6 die ich für erwähnenswert erachte. Der Vergleich stammt von HP und ist Online unter [4] zu finden.

1. IPv4 addresses are 32 bits long IPv6 addresses are 128 bits long, which almost surely eliminates the possibility of using-up all the addresses in IPv6.
2. Mobile IPv4 uses tunnel routing to deliver data-packets to Mobile Nodes Mobile IPv6 uses tunnel routing and source routing with IPv6 Type 2 routing headers.
3. Mobile IPv4 deploys Foreign Agents for Mobile Node movement detection and to decapsulate data-packets addressed to the Mobile Node's Care-of Address Mobile IPv6 Mobile Nodes decapsulate messages sent to its Care-of Address itself and uses IPv6 Router Advertisements for movement detection, thereby eliminating the need for Foreign Agents.
4. Mobile IPv4 uses Agent Discovery for Movement Detection Mobile IPv6 uses IPv6 Router Discovery.
5. Mobile IPv4 Route Optimization is an extension to the protocol, not part of the base RFC; requires pre-configured and static security associations; and, was difficult to operate with ingress-filtering routers Mobile IPv6 Route Optimization is a fundamental part included in the protocol; provides integrated Return Routability to dynamically secure Route Optimization; and, operates effectively with ingress-filtering routers.
6. Mobile IPv4 reverse tunneling is an extension to the protocol Mobile IPv6 bi-directional tunneling is part of the core protocol.
7. Mobile IPv4 uses one Home Address Mobile IPv6 uses a globally routable Home Address and a link-local Home Address.
8. Mobile IPv4 uses ARP to determine the link layer address of neighbors Mobile IPv6 uses IPv6 Neighbor Discovery and is de-coupled from any given link layer.
9. Mobile IPv4 Dynamic Home Agent Address Discovery uses a directed broadcast approach and returns separate replies from each Home Agent to the Mobile Node Mobile IPv6 Dynamic Home Agent Address Discovery uses anycast addressing and returns a single reply to the Mobile Node.
10. Mobile IPv4 Mobile Nodes can obtain Care-of Addresses via Agent Discovery, DHCP, and manual configuration Mobile IPv6 Mobile Nodes can obtain Care-of Addresses via Stateless Address Auto-configuration, DHCP, and manual configuration
11. Mobile IPv4 uses Foreign Agent Care-of Address and a co-located Care-of Address Mobile IPv6 Care-of Addresses are all co-located.

10 Literaturverweis:

[1] C. Perkins, Ed., Wood, J., "IP Mobility Support for IPv4",
RFC 3220, January 2002, http://www.ietf.org/rfc/rfc3220.txt

[2] Wikipediaautoren bis zum 11. Sep 2005, "Mobile IPv4", Sep 2005,
http://de.wikipedia.org/wiki/Mobile_IP

[3] Spenneberg, Ralf, "Laufend online.Roaming mit gleich bleibender IP-Adresse",
Linuxmagazin 01/2004, Jan 2004,
http://www.linux-magazin.de/Artikel/ausgabe/2004/01/mobile_ip/mobile_ip.html

[4] "Chapter 1. Introducing HP-UX Mobile IPv6" in: Mobile IPv6 Administrator's Guide, 2001-2004,
http://docs.hp.com/en/5990-8592/ch01s01.html