

Aufbau eines Mobile IPv6 Szenarios im Netzwerklabor

BACHELORARBEIT 1

durchgeführt am Bachelorstudiengang
Informationstechnik & System-Management
Fachhochschule Salzburg GmbH

vorgelegt von:

Riccardo Martin

Michael Pfnür

Daniel Zotter

Studiengangsleiter:

BetreuerIn:

FH-Prof. DI Dr. Gerhard Jöchl

FH-Ass. Prof. Dipl. Phys. Judith Schwarzer

Salzburg, Januar 2016

Eidesstattliche Erklärung

Ich/Wir versichere(n) an Eides statt, dass ich/wir die vorliegende Bachelorarbeit ohne fremde Hilfe und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel angefertigt und alle aus ungedruckten Quellen, gedruckter Literatur oder aus dem Internet im Wortlaut oder im wesentlichen Inhalt übernommenen Formulierungen und Konzepte gemäß den Richtlinien wissenschaftlicher Arbeiten zitiert, bzw. mit genauer Quellenangabe kenntlich gemacht habe(n). Diese Arbeit wurde in gleicher oder ähnlicher Form weder im In- noch im Ausland in irgendeiner Form als Prüfungsarbeit vorgelegt und stimmt mit der durch die Begutachter/Begutachterinnen beurteilten Arbeit überein.

Salzburg, 10.12.15	1310555039	Riccardo Martin
Ort, Datum	Personenkennzeichen	Unterschrift des/der Studierenden

Salzburg, 10.12.15	1310555048	Michael Pfnür
Ort, Datum	Personenkennzeichen	Unterschrift des/der Studierenden

Salzburg, 10.12.15	1310555048	Daniel Zotter
Ort, Datum	Personenkennzeichen	Unterschrift des/der Studierenden

Danksagung

Zunächst möchten wir uns an dieser Stelle bei all denjenigen bedanken, die uns während der Anfertigung dieser Bachelorarbeit unterstützt haben.

Ganz besonders danken möchten wir in erster Linie unserer Betreuerin, Frau FH-Ass. Prof. Dipl. Phys. Judith Schwarzer, für ihre ausgiebige Unterstützung. Durch stetiges Hinterfragen und konstruktive Kritik verhalf sie uns zu einer durchdachten Herangehensweise und Umsetzung. Dank ihrer Erfahrung im Bereich der Netzwerktechnik konnte sie uns immer wieder in unserer Recherche und bei unseren Fragen unterstützen. Vielen Dank für Zeit und Mühen, die Sie in unsere Arbeit investiert haben.

Auch möchten wir uns bei der Fachhochschule Salzburg bedanken, die das benötigte Equipment und die Räumlichkeiten zur Verfügung gestellt hat.

Kurzzusammenfassung

Dies ist ein Beispiel für eine *kurze* Kurzzusammenfassung.

Abstract

This is an example for a *short* abstract.

Inhaltsverzeichnis

Abkürzungsverzeichnis	I
Abbildungsverzeichnis	II
Tabellenverzeichnis	III
Quellcodeverzeichnis	IV
1 Einleitung	1
1.1 Motivation und Aufgabenstellung	1
1.2 Aufbau und Kapitelübersicht	1
2 Theoretischer Teil	2
2.1 Begriffsdefinition	2
2.2 Mobility Header	4
2.2.1 Home Address Option	5
2.3 Routing Header Type 2	6
2.4 Funktionsweise	6
2.4.1 Bidirectional Tunneling	6
2.4.2 Route Optimization	7
2.5 Vergleich Mobile IPv4 zu Mobile IPv6	8
2.5.1 Funktionsweise Mobile IPv4	9
2.5.2 Unterschiede	9
Literaturverzeichnis	11

Abkürzungsverzeichnis

HA	...	Home Agent
MN	...	Mobile Node
CN	...	Correspondent Node
CoA	...	Care-of Address
HoA	...	Home Adresse

Abbildungsverzeichnis

2.1	Format Mobility Header	4
2.2	Format Routing Header Type 2	6
2.3	Bidirectional Tunneling	7
2.4	Route Optimization	8
2.5	Mobile IPv4 Szenario	9

Tabellenverzeichnis

2.1	Beschreibung Mobility Header Felder	4
2.2	Mobility Nachrichtentypen	5
2.3	Unterschiede Mobile IPv4 / Mobile IPv6	10

Quellcodeverzeichnis

1 Einleitung

Mit der Einführung des Internet Protokolls IPv6 im Jahre 1998 wurde ein Nachfolger für das bis zu diesem Zeitpunkt alleinig verwendete IPv4 auf den Weg gebracht. IPv6 soll als Nachfolger von IPv4 dieses in absehbarer Zeit ablösen, was eine alleinige Nutzung der Version 6 des Internet Protokolls zur Folge hat.

Aus diesem Grund wird in der nachfolgenden Arbeit ein Einsatzbereich dieses Protokolles betrachtet.

1.1 Motivation und Aufgabenstellung

Das Thema **Aufbau eines Mobile IPv6 Szenarios im Netzwerklabor** wurde für diese Bachelor Arbeit gewählt, da die Anzahl mobiler Endgeräte Ende 2014 schon *7.9 Milliarden* betrug und in den nächsten Jahren stetig steigen wird. Dies ist ein gewichtiger Grund warum die Anwendung von Mobile IPv6 und den daraus resultierenden Vorteilen in der Zukunft zunehmend Beachtung geschenkt werden sollte. Führt man sich nur einmal vor Augen wie oft ein Mobilgerät einen Netzwechsel bei einer Fahrt mit dem Zug von München nach Hamburg vollzieht, so ist leicht ersichtlich, dass diese Technologie in Zukunft von enormer Bedeutung sein wird (genaue Erklärung der Funktionsweise in Abschnitt ??). Unter diese verschiedenen Gesichtspunkte, war es uns ein Anliegen, dieses Thema zu erarbeiten und zu vertiefen.

1.2 Aufbau und Kapitelübersicht

Der Aufbau dieser Arbeit wie folgend gegliedert. In Kapitel 1 wird mit einer kurzen Einleitung auf das Theme hingeführt, sowie die Motivation für die Bearbeitung dieser Aufgabenstellung und die Aufgabenstellung selbst dargestellt.

Kapitel 2 befasst sich mit der theoretischen Erklärung von **Mobile IPv6** und der für das Verständnis nötigen Beschreibung einiger Fachbegriffe dieses Themas. Weiterhin wird ein kurzer Vergleich zwischen **Mobile IPv4** und **Mobile IPv6** gezogen und die sich daraus ergebenden Vor- und Nachteile dargestellt.

In Kapitel 3 wird der physische Aufbau des Netzwerks, die dort verwendeten Materialien (Router, Switch etc.), eine Analyse der Hardware und der Software sowie die Implementation der Konfigurationen näher beschrieben und dargestellt.

Im letzten Kapitel werden die Ergebnisse, welche sich ergaben noch einmal zusammengefasst und ein Ausblick in die weiter Zukunft beschrieben.

In Anhang sind zuletzt noch das Literaturverzeichnis, Abkürzungsverzeichnis, Abbildungsverzeichnis, Tabellenverzeichnis und Quellcodeverzeichnis zu finden.

2 Theoretischer Teil

Mobile IPv6 ist ein Protokoll, dass von der IETF entwickelt wurde, welches es ermöglicht eine feste IPv6 Adresse einem mobilen Endgerät zuzuweisen und diese auch bei einem Netzwechsel zu behalten. Da das Mobile IPv6 Protokoll einen anderen Header verwendet als das Standard IPv6 Protokoll, werden in Abschnitt 2.2 der **Mobility Header, Routing Header Type 2** sowie dessen Funktionen und Einsatzbereiche beschrieben. Im Folgenden wird auf die theoretische Funktionsweise von **Mobile IPv6** eingegangen, sowie der Unterschied zwischen den Versionen Mobile IPv4 und IPv6 betrachtet. Die für das Verständnis von Mobile IPv6 wichtigen Begriffe werden im Abschnitt 2.1 erklärt[1].

2.1 Begriffsdefinition

Home Adresse

Die *Home Adresse* ist eine Unicast Adresse welche dem Mobilen Knoten zugewiesen wird, sie wird als permanente Adresse dieses Knoten benutzt. Diese befindet sich innerhalb des Home Links des mobilen Knoten. IP Routing Mechanismen schicken an die Home Adresse gerichtete Pakete an den Home Link. Falls es mehrere Präfixe auf dem Home Link gibt, kann ein Mobiler Knoten auch mehrere Home Adressen besitzen.

Home Subnetz Präfix

Unter *Home Subnetz Präfix* versteht man das IP-Subnetzpräfix, dass der Home Adresse des mobilen Knoten entspricht.

Home Link

Der *Home Link*, ist der Link an welchem das Home-Subnetzpräfix definiert ist.

Mobiler node

Ein *Mobiler node* ist ein Knoten, welcher seinen Standort wechseln kann (z.B. Laptop, Mobil Telefon etc.). Dieser Knoten bleibt aber auch unter seiner Home Adresse erreichbar, wenn er von seinem *Heimnetz A* in ein *Fremdnetz B* wechselt.

Correspondent node

Ein *Correspondent node* ist ein peer (gleichberechtigter Teilnehmer) Knoten mit dem der mobile Knoten kommuniziert. Der correspondent node kann ein mobiler oder stationärer Knoten sein.

Foreign Subnet Präfix

Unter *Foreign Subnet Präfix* versteht man jedes Subnet Präfix, das nicht dem Home Subnet Präfix des mobilen Knotens entspricht.

Foreign Link

Ist jeder Link, der nicht dem Home Link des mobilen Knotens entspricht.

Care-of Adresse

Die *Care-of Adresse* ist eine Unicast Adresse, die dem mobilen Knoten in einem fremden Netz zugewiesen wird. Ein mobiler Knoten kann auch mehrere Care-of Adressen besitzen (z.B. mit verschiedenen Präfixes), die Care-of Adresse mit der er bei seinem *Home Agent* registriert ist, wird als „*Primary*“ *Care-of Adresse* bezeichnet.

Home Agent

Als *Home Agent* wird der Router bezeichnet der sich am *Home Link* des mobilen Knotens befindet und wo die aktuelle *Care-of Adresse* des mobilen Knoten registriert ist. Wenn sich der mobile Knoten nicht im Heimnetz befindet, fängt der *Home Agent* die Pakete, die an die Home Adresse des mobilen Knoten im Heimnetz gerichtet sind ab, „verpackt“ diese und sendet sie über einen Tunnel an die registrierte *Care-of Adresse* des mobilen Knoten.

Binding

Als *Binding* versteht man die Zuordnung der *Home Adresse* des mobilen Knotens, der *Care-of Adresse* des mobilen Knotens für die noch verbleibende lifetime.

Registrierung

Unter *Registrierung* versteht man, wenn ein Binding Update von einem mobilen Knoten an seinen Home Agent oder an einen Corresponding Node geschickt und von diesen registriert wird.

Binding Authentisierung

Damit ein Corresponding Node weiss, dass ein Absender berechtigt ist das Binding zu ändern, muss eine Registrierung bei einem Corresponding Node autorisiert werden.

Proxy Neighbor Discovery

Damit ein Home Agent am Home Link alle an den mobile Node adressierten Pakete abfangen kann, muss er sich als dieser ausgeben. Daher schickt er im Namen

des mobile Nodes ein *Neighbor Advertisement* an die *All-Nodes Multicast Adresse*. Nun werden alle Pakete die für den mobile Node bestimmt sind an den Home Agent gesendet. Dadurch agiert der Home Agent am Link sozusagen als Proxy für den mobile Node[2].

2.2 Mobility Header

Für das *Mobile IPv6 Protokoll* wurde ein extra *Mobility Header* eingeführt. Dieser ist ein *Extension Header*, der von *Corresponding Nodes*, *mobilen Knoten* und *Home Agents* genutzt wird. Er kommt in allen Nachrichten, die mit dem Herstellen und Verwalten von Bindings zu tun haben vor. Das Format des Mobility Headers ist in Abbildung 2.1 dargestellt[1].

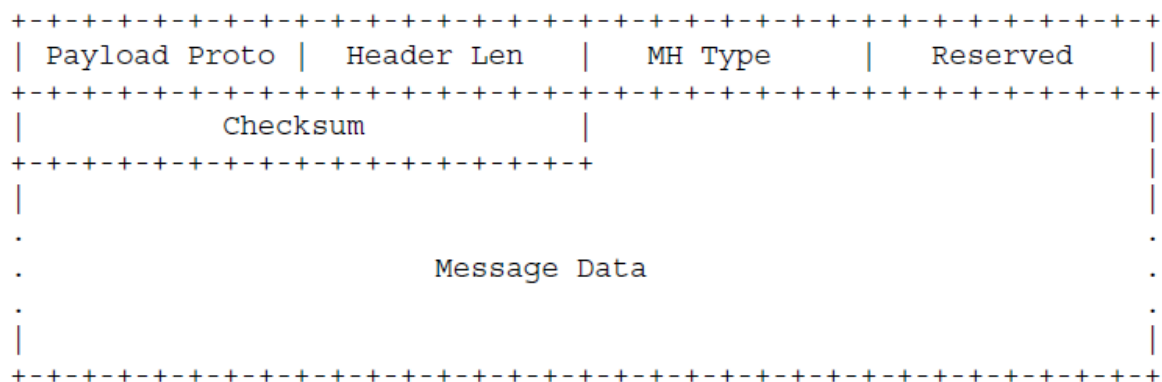


Abbildung 2.1: Format Mobility Header

Die im Header definierten Felder haben folgende Aufgabe.

<i>Feld</i>	<i>Größe</i>	<i>Beschreibung</i>
Payload Proto	1 Byte	Entspricht dem next Header Feld
Header Len	1 Byte	Länge des Mobility Header
MH Type	1 Byte	Identifiziert die betreffende Mobility Nachricht siehe Tabelle
Reserved	1 Byte	Reserviert für zukünftige Benutzungen. Der Wert MUSS mit 0 von Sender initialisiert werden und MUSS vom Empfänger ignoriert werden
Checksum	1 Byte	Enthält die Checksum vom Mobility Header
Data	variabel	Enthält die Daten entsprechend des MH Type

Tabelle 2.1: Beschreibung Mobility Header Felder

Im Folgenden werden die verschiedenen *Mobility Nachrichtentypen* aufgezeigt um den Ablauf in einem *Mobile IPv6 Szenario* richtig zu verstehen.

<i>MH Wert</i>	<i>Nachricht</i>	<i>Beschreibung</i>
0	Binding Refresh Request	Fordert den mobilen Knoten auf, sein Binding zu aktualisieren. Wird vom CN's verschickt
1	Home Test Init	Eine vom mobilen Knoten verschickte Nachricht um einen Return routability Prozess zu initialisieren und einen Home keygen token vom CN zu erhalten. Diese Nachricht ist getunnelt durch den Home Agent, wenn sich der mobile Knoten nicht zu Hause befindet.
2	Care-of Test Init	Wie <i>Home Test Init</i> , nur wird die Nachricht direkt an den CN geschickt.
3	Home Test Message	Antwort auf <i>Home Test Init</i> . Wird vom CN an den mobilen Knoten gesendet.
4	Care-of Test Message	Antwort auf <i>Care-of Test Init</i> . Wird vom CN an den mobilen Knoten gesendet.
5	Binding Update Message	Wird von einem mobilen Knoten verwendet um andern Knoten seine neue CoA mitzuteilen
6	Binding Acknowledgement Message	Wird verwendet um den Empfang eine Binding Updates zu bestätigen.
7	Binding Error	Wird vom CN verwendet um einen Fehler in Bezug auf Mobility zu signalisieren.

Tabelle 2.2: Mobility Nachrichtentypen

2.2.1 Home Address Option

Wird *Home Address Option* verwendet, so steht im Extension Header der Wert **60** für *Next Header Value*. Sie wird verwendet, wenn ein mobile Node ein Paket sendet und sich nicht in seinem Heimnetz befindet, um dem Empfänger die Home Adresse des mobile Node mitzuteilen[1].

2.3 Routing Header Type 2

Für Mobile IPv6 wurde ein neuer Routing Header definiert, der als *Routing Header Type 2* bezeichnet wird. Dieser erlaubt es Pakete direkt von einem CN an die CoA eines mobile Node's zu senden. Dazu wird im IPv6 *Destination address Feld* die CoA des mobile Node's eingetragen. Sobald das Paket an der CoA ankommt, erhält der mobile Node seine HoA aus dem Routing Header, welche die Endziel Adresse des Paketes darstellt.

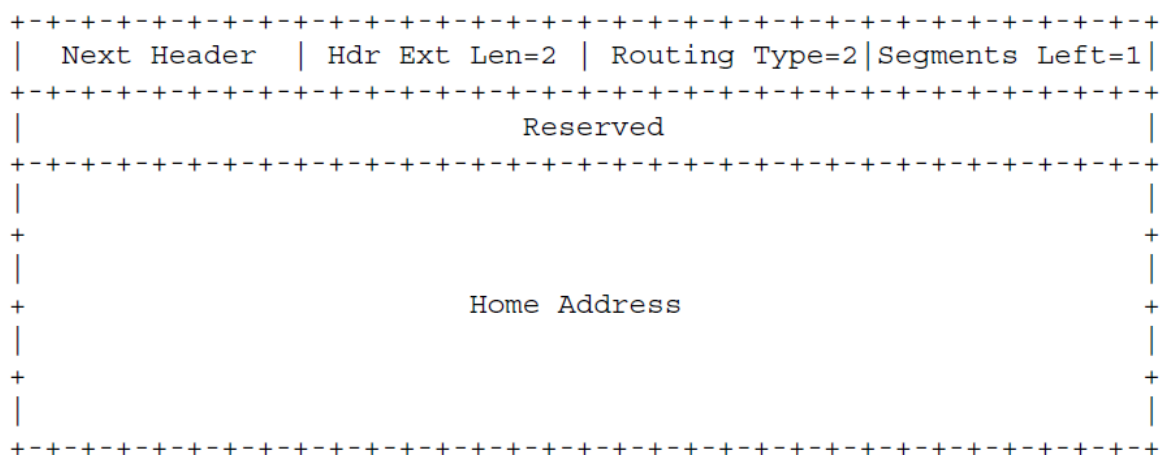


Abbildung 2.2: Format Routing Header Type 2

Wie in Abbildung 2.2 ersichtlich ist, steht im *Hdr Ext Len* Feld eine 2, was bedeutet, dass der Header immer die gleiche Länge besitzt. Das *Routing* Feld besitzt immer den Type 2, da es sich um den *Routing Header Type 2* handelt. Im *Segments Left* Feld steht immer eine 1, da nur ein Adresseintrag für diesen Header erlaubt ist[1].

2.4 Funktionsweise

Für den Ablauf von Mobile IPv6 gibt es zwei mögliche Verfahren, einmal das *Bidirectional Tunneling* und zum Anderen das *Route Optimization* Verfahren.

2.4.1 Bidirectional Tunneling

Beim Bidirectional Tunneling sind der mobile Knoten und der Home Agent über einen Tunnel miteinander verbunden. Pakete die von einem Correspondent Node an einen mobil Node gesendet werden, passieren vor der Zustellung den entsprechenden Home Agent des Mobile Nodes. Alle Pakete die an den mobile Node adressiert sind werden durch den Home Agent abgefangen. Dies geschieht durch *Proxy Neighbor Discovery*. Wenn sich der mobile Node nicht im Heimnetz aufhält, werden die vom CN an ihm gesendeten Pakete vom HA verpackt. Alle erkannten Pakete werden an die beim Home Agent in ein neues Paket verpackt, an die

registrierte CoA des mobile Node adressiert und über den Tunnel gesendet. Am anderen Ende werden die Pakete vom Netzwerk Layer des MN entpackt bevor diese an die oberen Layer weitergegeben werden.

Ähnlich läuft es ab wenn der MN Pakete sendet. Hier werden den verpackten Paketen 40 Byte als Tunnel Header hinzugefügt und unter Verwendung der CoA des MN an den HA über den Tunnel gesendet. Dies wird als *reverse tunneling* bezeichnet. Beim HA werden die Pakete entpackt, der Tunnel Header entfernt und die modifizierten Pakete durch das Internet an den entsprechenden CN gesendet. In Abbildung 2.3 ist der Ablauf grafisch dargestellt.[3]

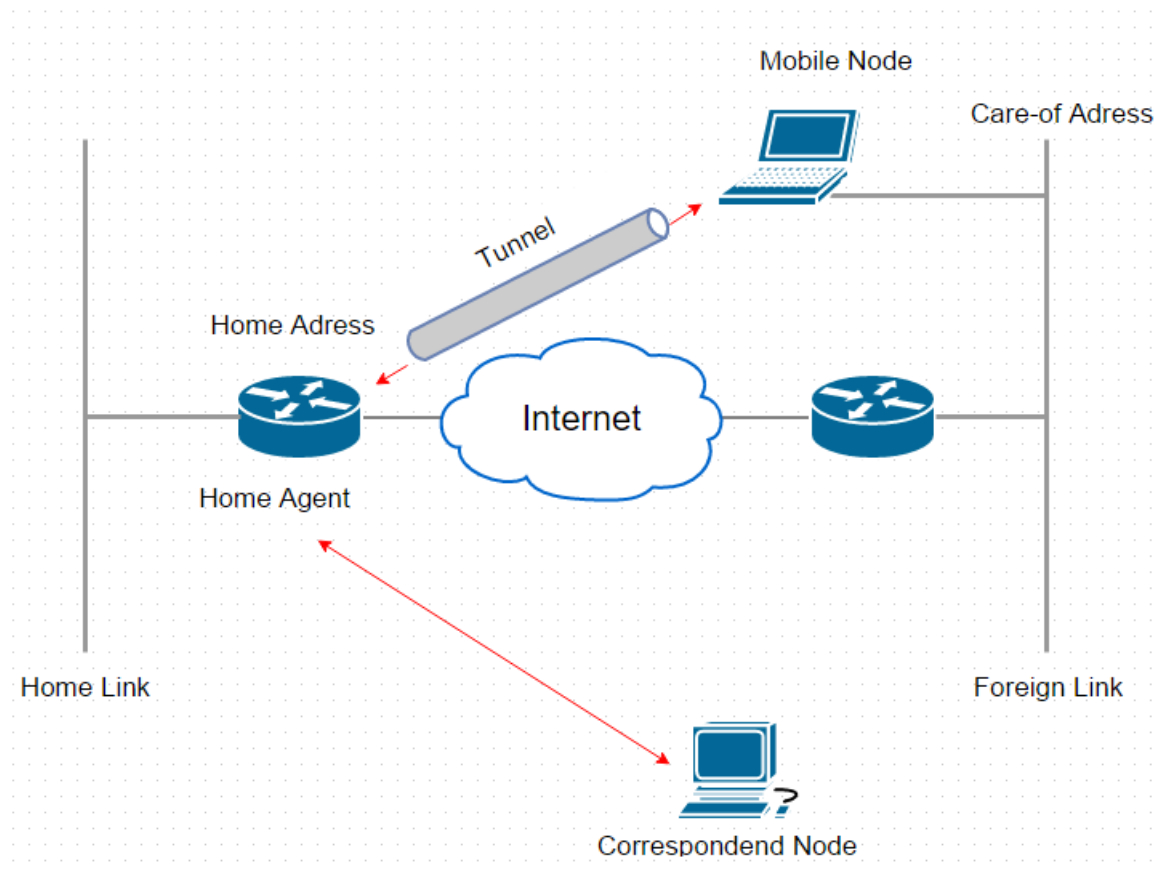


Abbildung 2.3: Bidirectional Tunneling

2.4.2 Route Optimization

Bei dem *Route Optimization* Verfahren, können Pakete direkt zwischen einem CN und einem MN gesendet werden. Die *Binding Update Messages* (BU) werden nicht nur an den HA geschickt, sondern auch an alle beteiligten CNs. Der Zweck ist das Binden der momentanen Adresse des MN an seine HoA. Jeder CN besitzt eine sogenannte *Binding Cache* Tabelle um von einem MN die CoA zu dessen HoA zuzuordnen zu können. Ein MN besitzt eine ähnliche Tabelle um feststellen zu können ob ein CN *Bidirectional Tunneling* oder *Route Optimization* verwendet. Daher ist es

wichtig, BUs in regelmäßigen Abständen zu senden um eine korrekte Zuordnung von CoA zu HoA sicherzustellen. Sendet ein MN ein Paket an einen CN, so benutzt das *Route Optimization* Verfahren die *Home Address Option* Header Erweiterung. Sendet allerdings ein CN ein Paket an einen MN wird der sogenannte *Type 2 Routing Header* verwendet. Bei Route Optimization, kann im Vergleich zum Bidirectional Tunneling das Delay verringert werden, da kein extra Tunnel Header notwendig ist.

In Abbildung 2.4 ist das Verfahren noch einmal grafisch dargestellt.

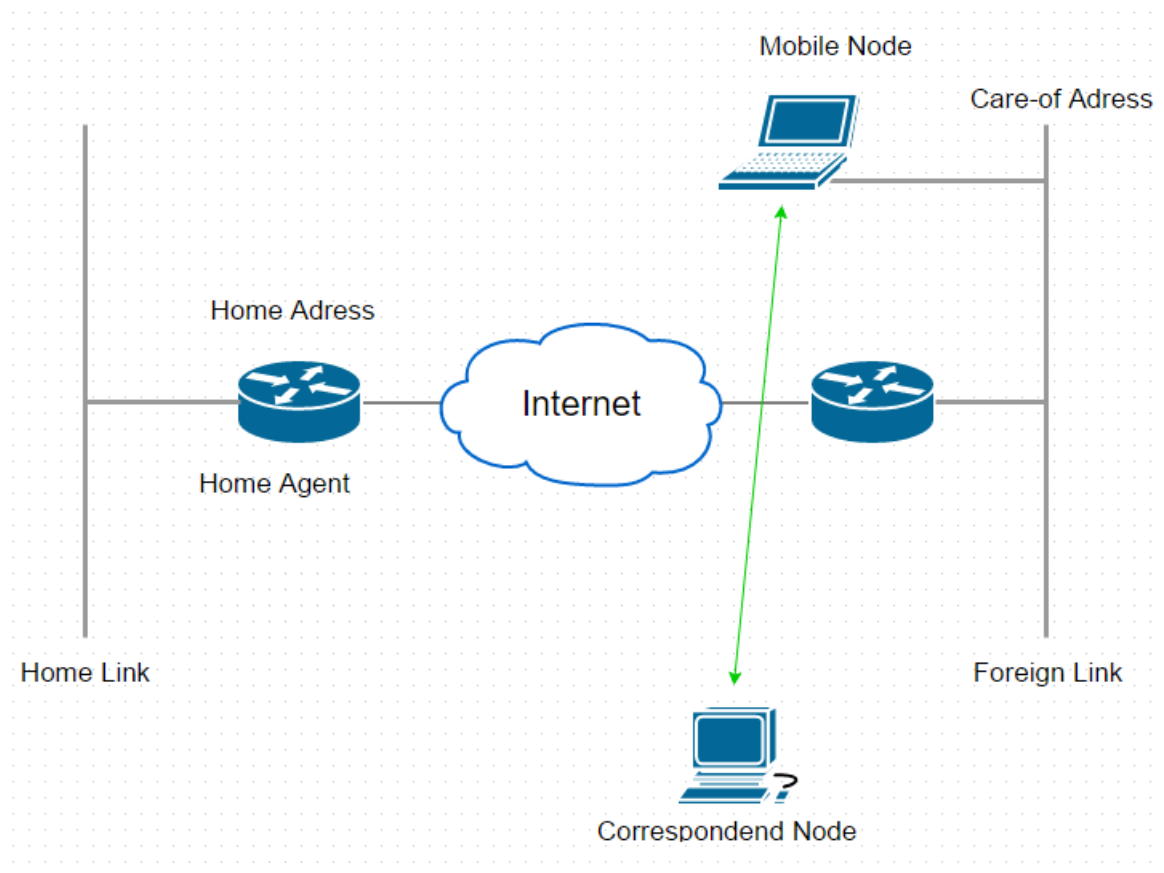


Abbildung 2.4: Route Optimization

Route Optimization unterstützt auch ein Szenario, wenn MN und CN beides mobile Nodes sind. Da hier beide Nodes eine CoA und HoA besitzen, benötigt das Routing der Pakete auch beide Extension Headers. Da jeder Extension Header eine Größe von **24 Byte** hat ergibt sich ein gesamter Overhead für das Senden von Paketen zwischen zwei mobile Nodes von **48 Byte**[3].

2.5 Vergleich Mobile IPv4 zu Mobile IPv6

Um einen Vergleich zwischen Mobile IPv4 und IPv6 zu ziehen, wird zuerst noch einmal kurz auf die Funktionsweise/Ablauf bei Mobile IPv4 eingegangen. Das in

Abbildung 2.5 dargestellte Szenario, soll die Unterschiede zwischen beiden Versionen verdeutlichen, sowie die Vor- bzw. Nachteile der einzelnen Versionen aufzeigen.

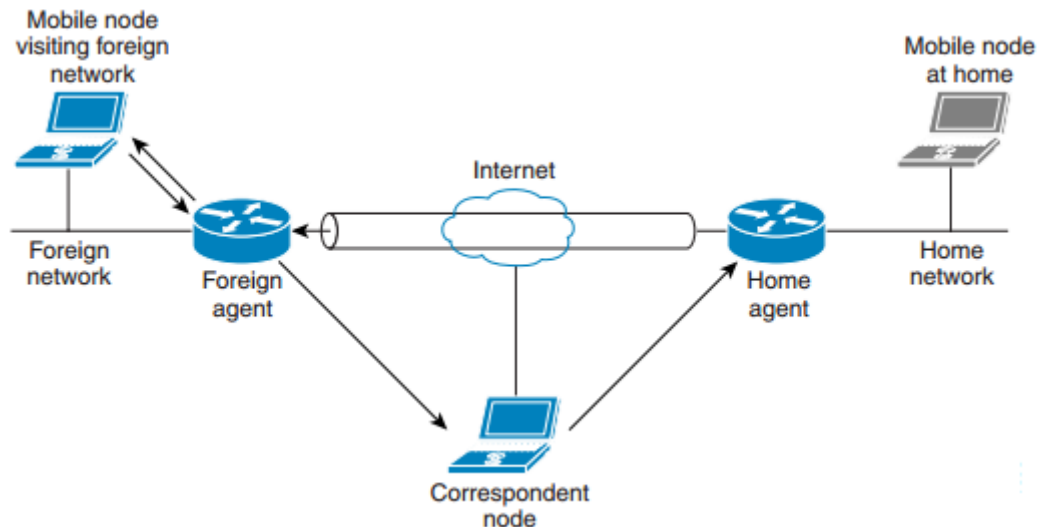


Abbildung 2.5: Mobile IPv4 Szenario

2.5.1 Funktionsweise Mobile IPv4

Hält sich der MN im Heimnetz auf, so teilt er seinem HA seine HoA mit. Wenn der MN jetzt in ein fremdes Netz (Foreign network) wie in Abbildung 2.5 dargestellt wechselt, meldet er sich beim Foreign Agent an. Dieser weist ihm ein CoA zu unter der der MN im fremden Netz erreichbar ist. Sendet jetzt ein CN ein Paket an einen MN der sich in einem fremden Netz befindet, so geht diese Paket zuerst an den Home Agent des MN. Dieser verpackt das Paket und sendet es an den Foreign Agent in dessen Netz sich der MN befindet. Über den Foreign Agent wird das Paket an den MN weitergeleitet.

Sendet der MN ein Paket, so wird dieses über den Foreign Agent direkt an den CN gesendet.

2.5.2 Unterschiede

Betrachtet man die beiden verschiedenen Version Mobile IPv4 und Mobile IPv6 so werden einige Unterschiede ersichtlich. Diese werden nachfolgend stichpunktartig aufgeführt[4].

- Bei *Mobile IPv6* wird der Overhead im Vergleich zu Mobile IPv4 reduziert, da hier beim Senden eines Paketes an einen MN bevorzugt der *IPv6 Routing Header* anstelle von IP encapsulation verwendet wird.
- Im Gegensatz zur Version 4 werden bei Mobile IPv6 Features wie *Neighbor*

Discovery oder *Auto Address Configuration* verwendet, was keine speziellen Router als *Foreign Agents* mehr nötig macht.

- *Route Optimization* ist ein fester Bestandteil in Mobile IPv6 und nicht eine Erweiterung (die nicht von allen Nodes unterstützt wird) wie in Mobile IPv4. Daraus ergibt sich die Möglichkeit, das ein CN ein Paket direkt an einen MN schickt, wodurch der Nachteil des *triangle routing* von IPv4 beseitigt wird.
- Der HA bei Mobile IPv6 verwendet *neighbor discovery* anstelle von *ARP* wie es in Mobile IPv4 der Fall ist, um Pakete abzufangen die an den MN adressiert sind.
- Bei Mobile IPv6 stellt es kein Problem mehr da, wenn Router in einem fremden Netz *ingress filtering* verwenden, da der MN nun seine *Care-of Adresse* im IP Header des Paketes verwendet.
- Mobile IPv6 verwendet *IPsec* für Binding Updates anstelle von eigenen Sicherheitsmechanismen wie es bei IPv4 der Fall ist.

In der nachfolgenden Tabelle 2.3 werden die wichtigsten Unterschiede noch einmal kurz dargestellt.

	<i>Mobile IPv4</i>	<i>Mobile IPv6</i>
Foreign Agent	✓	x
Route Optimization	Erweiterung	✓
Paketidentifizierung durch den HA	ARP	Neighbor Discovery
Probleme mit ingress filtering	✓	x
Sicherung der Binding Updates	eigene Mechanismen	IPsec

Tabelle 2.3: Unterschiede Mobile IPv4 / Mobile IPv6

Wie aus dem Vergleich zwischen *Mobile IPv4* und *Mobile IPv6* ersichtlich wird, wurde versucht die Schwächen, die bei der Version 4 vorhanden waren in der Version 6 zu beheben. Einer der wichtigsten Punkte hierbei, war die Sicherung der Binding Updates sowie die Verringerung des Overheads.

Literaturverzeichnis

- [1] C. Perkins, E. Tellabs, and D. Johnson, "Mobility support in ipv6," Internet Engineering Task Force (IETF), Request for Comments 6275, July 2011.
- [2] J.-M. Combes, S. Krishnan, and G. Daley, "Securing neighbor discovery proxy," Internet Engineering Task Force (IETF), Request for Comments 5909, July 2010.
- [3] H. Zolfagharnasab, "Reducing packet overhead in mobile ipv6," *International Journal of Distributed and Parallel Systems (IJDPS)*, vol. 3, no. 3, May 2012.
- [4] F. Nada, "Performance analysis of mobile ipv4 and mobile ipv6," *The International Arab Journal of Information Technology*, vol. 4, no. 2, April 2007.

