Fachhochschule
Salzburg University
of Applied Sciences

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:	FH-Prof. DI Dr. Gerhard Jöchtl
BetreuerIn:	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

Diese Arbeit beschäftigt sich mit Mobile IPv6 und dem Aufbau eines Prototypen. Sie gliedert sich in einen theoretischen und einen praktischen Teil.

Die Theorie beschäftigt sich mit dem nötigen Basiswissen über Mobile IPv6. Hier werden die verschiedenen Begriffsdefinitionen in der Arbeit aufgelistet und erklärt. Es wird auf die speziellen Mobile IPv6 Header die das Protokoll einführt eingegangen und die generelle Funktionsweise von Mobile IPv6 beschrieben. Da der Umstieg von IPv4 auf IPv6 nur sehr langsam voran geht wurde auch ein Vergleich zwischen Mobile IPv4 und IPv6 in dieser Arbeit behandelt. Außerdem wurde noch eine Erweiterung des Mobile IPv6 Protokolls Namens Network Mobility NEMO betrachtet. Diese Erweiterung hatte sich im Praktischen Teil als Möglichkeit zur Realisierung des Prototypen angeboten.

Der Praktische Teil ist in die Beschreibung von 3 Versuchen aufgegliedert und einer folgenden Analyse der verwendeten Hard und Software sowie der Implementierung der einzelnen Versuche. Die Beschreibung der Versuche gliedert sich in deren Aufbau einer Grafik zum veranschaulichen und dem Ergebnis dieses Versuches. Der Aufbau des folgende Versuch war immer eine weiter Entwicklung des vorherigen. Die Analyse beleuchtet genauer die verwendete Hardware und beschäftigt sich auch mit der Auswahl des richtigen IOS für die Umsetzung. Die Implementierung der einzelnen Versuche analysiert detaillierter Aufbau und Ergebnisse aus den einzelnen Versuchen. Zum Schluss gibt es noch eine Zusammenfassung sowie einen Ausblick in welcher die Erkenntnisse der Arbeit nochmal aufbereitet werden.

Abstract

This is an example for a *short* abstract.

Inhaltsverzeichnis

1 Einleitung

Mit der Einführung des Internet Protkolls 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 werdern 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 **Mobiel 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 correspondant 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 *Extention Header*, der von *Correspondig 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].

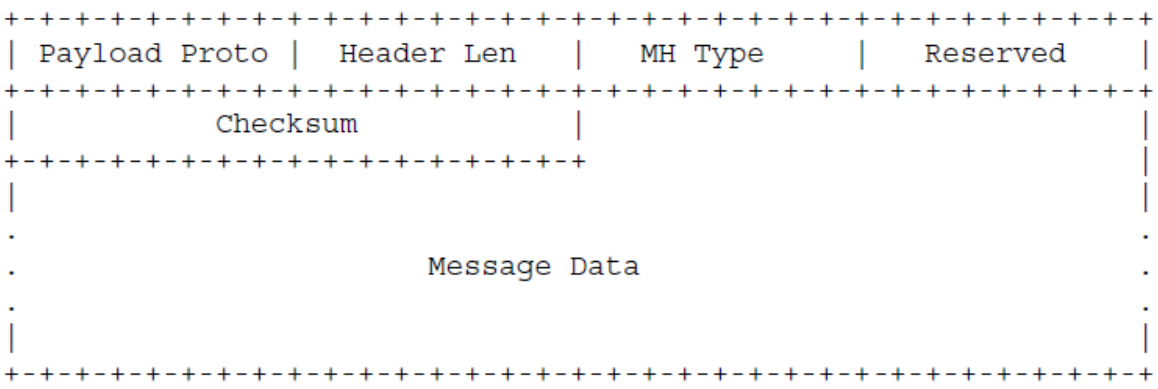

Abbildung 2.1: Format Mobility Header

Die im Header definierten Felder haben folgende Aufgabe.

Feld	*Größe*	*Beschreibung*
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.

MH Wert	*Nachricht*	*Beschreibung*
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 *Home Test Init*, nur wird die Nachricht direkt an den CN geschickt.
3	Home Test Message	Antwort auf *Home Test Init*. Wird vom CN an den mobilen Knoten gesendet.
4	Care-of Test Message	Antwort auf *Care-of Test Init*. 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 einen CN an die CoA eines mobile Node´s zu senden. Dazu wird im IPv6 *Destination address Feld* die CoA des mobile Node´s eigetragen. Sobald das Paket an der CoA ankommt, erhält der mobile Node seine HoA aus dem Routing Header, welche die Endziel Adresse des Paketes darstellt.

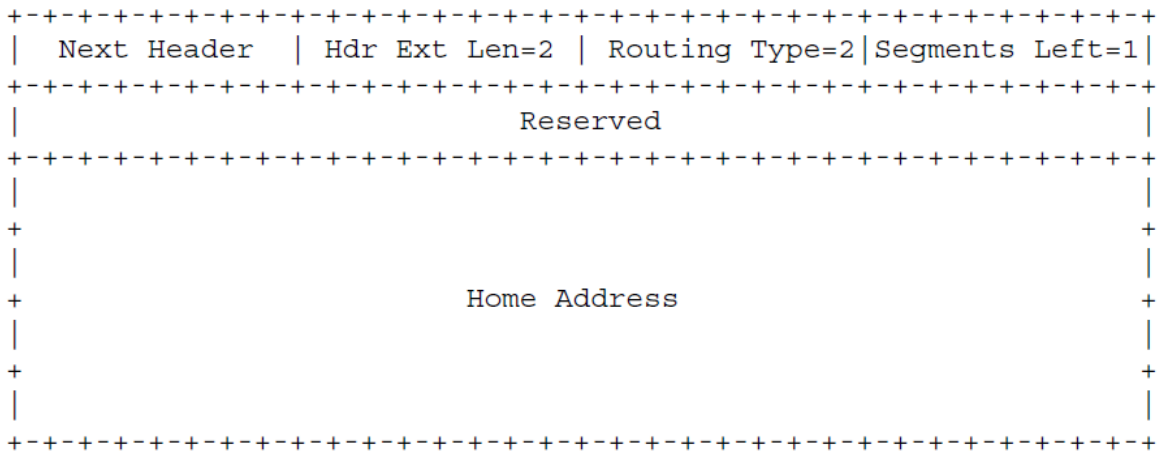

Abbildung 2.2: Format Routing Header Type 2

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 addressiert 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]

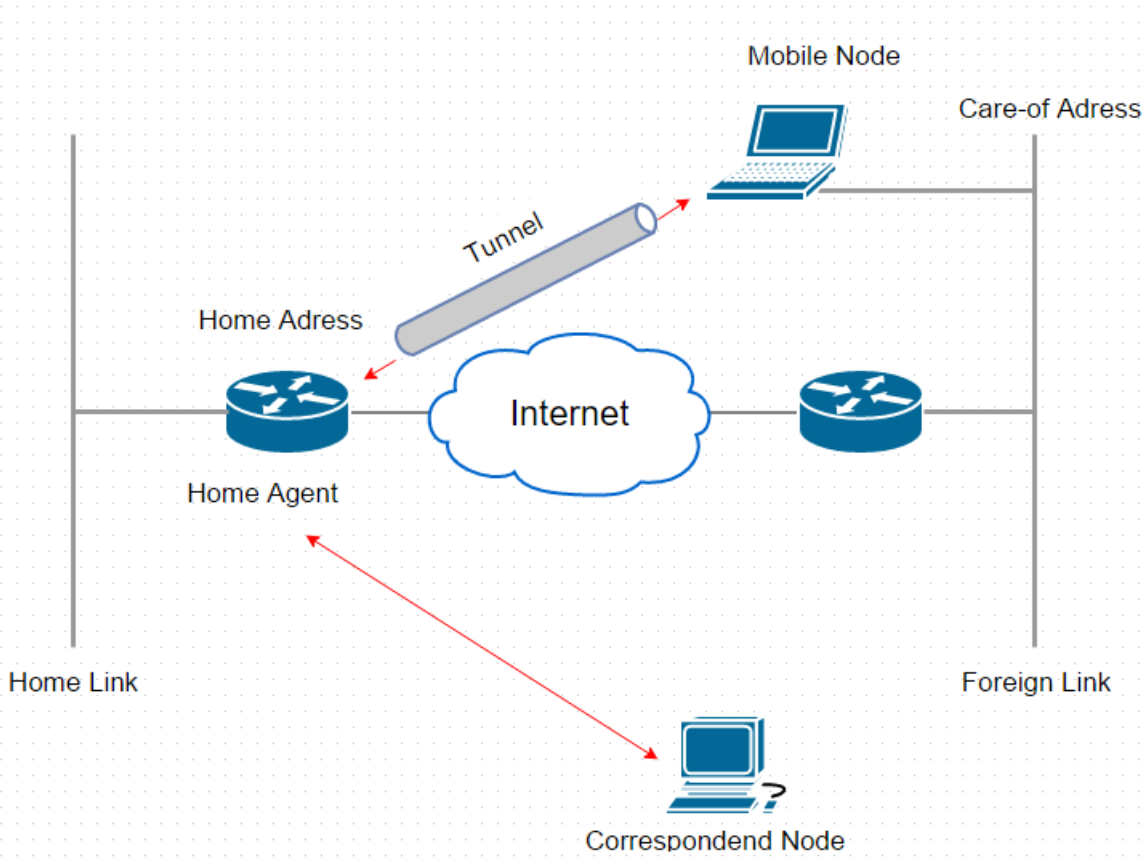

Abbildung 2.3: Bidirectional Tunneling

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 zuordnen 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 Adress 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 nocheinmal grafisch dargestellt.

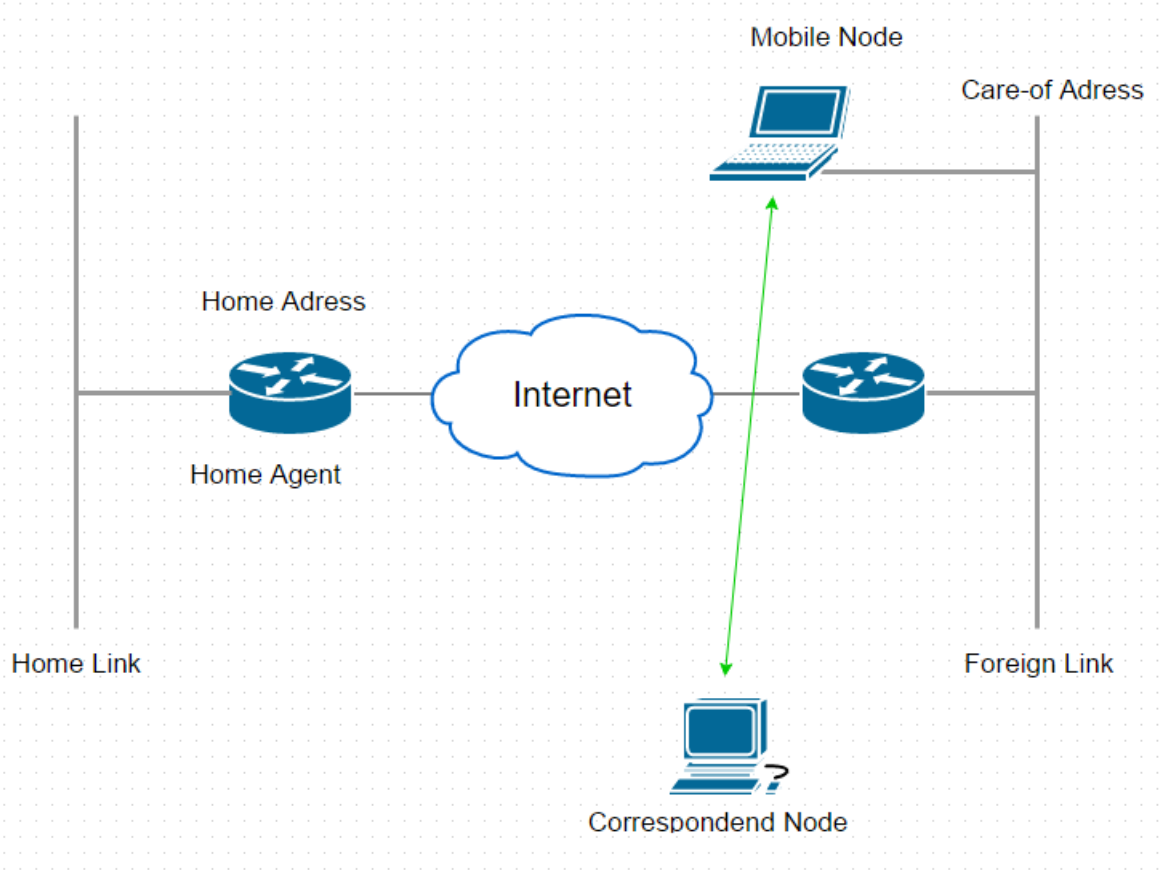

Abbildung 2.4: Route Optimization

Route Optimization unterstützt auch ein Szenario, wenn MN und CN beides mobile Nodes sind. Da hier beide Nodes eine CoA und HoA besitzten, benötigt das Routing der Pakete auch beide Extention Headers. Da jeder Extention 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.

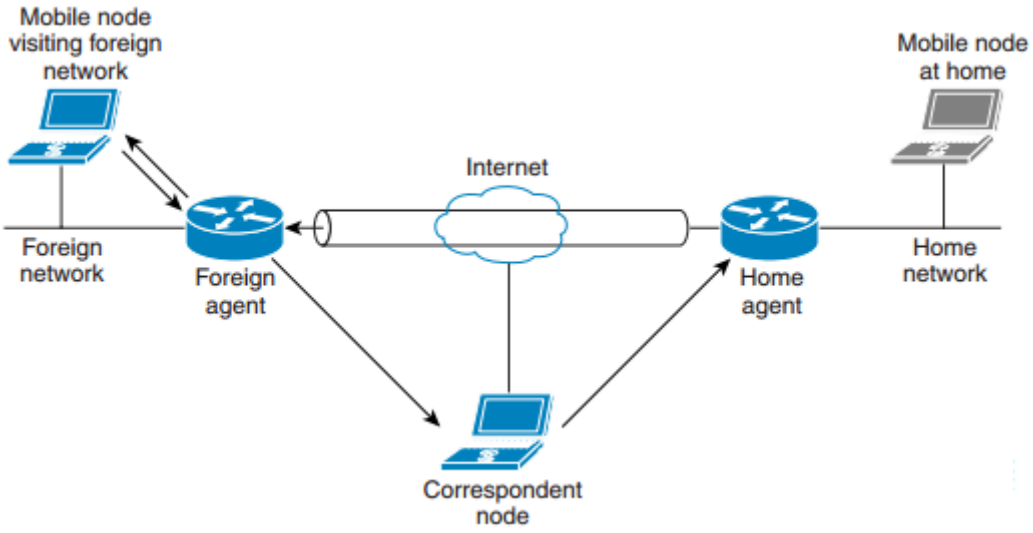

Abbildung 2.5: Mobile IPv4 Szenario

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.

	Mobile IPv4	*Mobile IPv6*
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.

2.6 Network Mobility (NEMO) Basic Support Protocol

Um Mobile IPv6 anwenden zu können ist eine Erweiterung des Technologie Stacks von mobiler Endgeräte erforderlich. Da bei einer wirklichen Umsetzung diese von Smartwatch, Smartphone, Tablet bis hin zu einem Laptop gehen würde, kann man erkennen, dass der Aufwand hierfür eher eine abschreckende Wirkung hat.

Eine Lösung für dieses Problem ist das Network Mobility (NEMO) Basic Support Protokoll. Dieses stellt eine standardisierte Erweiterung für das Mobile IPv6 Protokoll dar welche im RFC-3963 beschrieben wird. Es erlaubt, dass ganze Netzwerke sich bewegen können und die Verbindung trotzdem erhalten bleibt. Dies wird dadurch ermöglicht, dass die gesamte Logik weg von den Endgeräten auf Router hin ausgelagert wird. Dies würde eine erforderliche Aufrüstung der Endgeräte unnötig machen.

Ein wichtiger Teil bei der Umsetzung von NEMO ist die Rückwärtskompatibilität mit Mobile IPv6. Ein in NEMO erstellter Home Agent kann auch als Mobile IPv6 Home Agent fungieren.

Das NEMO Protokoll erweitert die Funktion eines Mobile IPv6 mobilen Knoten um Routing Funktionen, dieser Knoten wird in weiterer Folge als Mobile Router bezeichnet. Dies ist wichtig, da sich der Mobile Router um das Routing zwischen dem aktuellen Verbindungsknoten und dem an ihm hängenden Subnet kümmert.

Als Verbindung zwischen Mobile Router und Home Agent wird ein bidirektionaler Tunnel aufgebaut. Gleich wie bei Mobile IPv6 wird dieser erstellt, sobald der Mobile Router ein Binding Update an den Home Agent schickt.

2.6.1 Funktionsweise

Ein mobiles Netzwerk kann beliebig von einem Access Point zum nächsten wandern, kann aber selbst nur über ein bestimmtes Gateway erreicht werden. Dieses Gateway stellt der Mobile Router dar, welcher das Netzwerk hinter ihm mit den Access Points verbindet. Dies bedeutet, jedes mobile Netzwerk hat zumindest einen Mobile Router. Es besteht aber die Möglichkeit, dass sich ein Mobile Router mit einem anderen verbindet.

Gleich wie bei Mobile IPv6 wird dem Mobile Router von seinem Home Agent eine Home Adresse gegeben. Es ist auch möglich, dass der Mobile Router mehrere Home Adressen zugewiesen bekommt. Diese Adresse leitet er an sein mobiles Netzwerk weiter.

Wenn nun der Mobile Router von einem Access Point zum nächsten wechselt, wird ihm eine CoA zugewiesen, welche er per Binding Update an seinen Home Agent

weiter schickt. Dieser erzeugt in seinem Cash einen Eintrag, in dem die Home Adresse mit der aktuellen CoA eingetragen wird. Um einem Knoten in seinem Netzwerk eine Verbindung nach außen zu ermöglichen, signalisiert der Mobile Router dies seinem Home Agent mit einem speziellen Flag (R) im Binding Update.

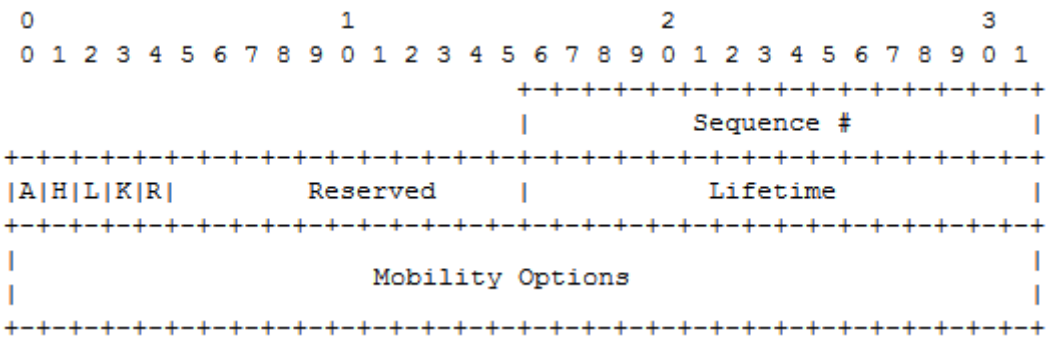

Abbildung 2.6: Binding Update mit R - Flag

Der in Abbildung 2.6 dargestellte Binding Update Header hat das Mobile Router Flag (R) gesetzt welches dem Home Agent mitteilt das es sich um ein Binding Update von einem Mobile Router handelt. Falls dieses Flag auf 0 gesetzt sein sollte nimmt der Home Agent an der Mobile Router verhält sich wie ein gewöhnlicher mobiler Knoten. Dies bedeutet er darf keine Pakete für das mobile Netzwerk an den Mobile Router weiterleiten.

Ein gesetztes Acknowledge (A) Flag bedeutet das der Sender ein Acknowledgement für den Empfang des Binding Updates erwartet. Mit dem Home Registration (H) Flag fragt der Sender den Empfänger ob er als sein Home Agent fungieren kann. Das Link-Local Address Compatibility (L) Flag wird gesetzt wenn der Interface Identifier der Heim Adresse des Senders derselbe ist wie seine Link-local Adresse.
Das Key Management Mobility Capability (K) Flag hat nur für Binding Updates zwischen Knoten und Home Agent Bedeutung. Denn dieses Bit sagt ob die IPsec Verbindung zwischen Knoten und Home Agent einen Netzwechsel des Knoten überstehen würde.

Das Reserved Feld ist ungenützt und muss vom Sender mit 0 initialisiert und vom Empfänger ignoriert werden. Die Sequence Nummer besteht aus einem 16 bit unsigned Integer und hilft dem Empfänger die Binding Updates zu ordnen und dem Sender Acknowledges zuzuordnen.
Die Lifetime ist ein 16 bit unsigned Integer wobei eine Zeiteinheit 4 Sekunden entspricht. Der Wert gibt die Zeiteinheiten an bis das Binding Update als abgelaufen gilt und verworfen wird.
Die Mobility Options ist ein variables Feld, mit der Auflage das der Header ein

vielfaches eines 8 Bit Integer lang ist. Falls der Empfänger die gesendete Option nicht versteht muss er sie verwerfen und den Rest weiter verarbeiten.

Dieses Update kann auch Präfixes des mobilen Netzes enthalten, damit der Home Agent Nachrichten an einen speziellen Knoten weiterleiten kann. Dafür gibt es eine Mobility Header Option, in welchen der Präfix übertragen wird.

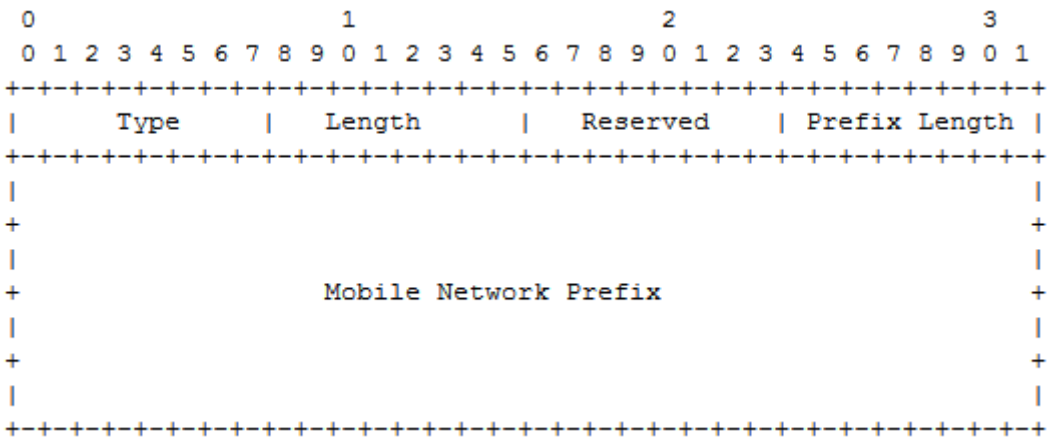

Abbildung 2.7: Mobility Header für Präfixübertragung

Der in Abbildung 2.7 dargestellte Aufbau des Mobile Network Präfix Option Headers hat eine 16 Byte großes Feld für den Netzwerk Präfix. Das Feld Reserved ist ungenutzt muss aber vom Sender auf 0 gesetzt werden und muss vom Empfänger ignoriert werden. Das Length Feld gibt die Länge dieses Headers ohne Type und Prefix Feld an. Es besteht aus 8 Bit unsigned integern. Das Type Feld dient zur Identifikation Mobile Option und hat für diese Option den Wert 6. Wenn dieser Wert vom Empfänger nicht erkannt wird die Option verworfen und der Rest des Binging Updates weiterverarbeitet.

Sollte es mehrere Knoten im mobilen Netzwerk geben und der Mobile Router will eine Paketübertragung zu allen, sendet er alle Netzwerk Präfixes in einer Nachricht. Es besteht die Möglichkeit, dass das ganze Netzwerk statisch konfiguriert ist. In diesen Fall weiß der Home Agent bereits alle Präfixes des mobilen Netzwerks und der Mobile Router wird keine Informationen diesbezüglich versenden. Der Home Agent würde mit der Übermittlung an die Knoten anfangen sobald er vom Mobile Router das Binding Update mit dem Flag (R) empfangen hat.

Sodann sendet er ein Binding Acknowledgement an den Mobile Router und ein bidirektionaler Tunnel wird zwischen den beiden aufgebaut. Die Endpunkte dieses Tunnels sind auf der einen Seite die CoA des Mobile Router und auf der anderen Seite die Adresse des Home Agents.

Wenn nun ein Correspondent Node ein Daten Paket an einen Knoten im mobi-

len Netzwerk sendet, wird das Paket zum Home Agent des gesamten mobilen Netzwerks weitergeleitet. Dieser leitet über den Tunnel das Paket an die aktuelle CoA des Mobile Routers weiter. Bevor der Mobile Router das Paket nun weiterleite überprüft er ob die Source Adresse am äußeren IPv6 Header der des Home Agent entspricht. Falls die Pakete mit IPsec im Tunnel geschützt sind dann entfällt diese Überprüfung. Außerdem muss der Mobile Router die Zieladresse im inneren IPv6 Header nach eine Übereinstimmigkeit mit einem Präfix des mobilen Netzwerks überprüfen. Sollte keine Übereinstimmung gefunden werden und der Präfix unbekannt sein dann wird das Paket noch im Mobile Router verworfen, andernfalls leitet er des Paket an das Interface des Knoten weiter.

Diese Präfixüberprüfung ist nicht notwendig, wenn Home Agent und Mobile Router ein Routing Protokoll im Tunnel verwenden. Dann sendet der Mobile Router anstatt der Präfix Information mit dem Binding Update Routing Protokoll Updates.

3 Praktischer Teil

3.0.1 Aufgabenstellung: Erarbeitung einen Mobile IPv6 Testaufbaus

Dieser Testaufbau sollte unter der Berücksichtigung erstellt werden, ihn in einer Laborübung für den Netzwerkbereich des Studiengangs Informationstechnik und Systemmanagement an der Fachhochschule Salzburg einsetzen zu können.

Der Testaufbau sollte die Grundfunktionen von Mobile IPv6 darstellen und mit dem vorhandenen Laborequipment der FH Salzburg, welches in Tabelle 3.1 aufgelistet wird, realisiert werden. Damit die Funktion und Umsetzung von Mobile IPv6 überhaupt möglich wird, war eine IPv6 Umgebung im Labor zu erstellen, welche als Basisaufbau diente. Dieser Basisaufbau sollte dann mit den entsprechenden Mobile IPv6 Funktionen erweitert werden. Aufgabe war es, den Wechsel eines beliebigen Endgerätes von einem Netz zu einem anderen zu realisieren, wobei dieses Endgerät immer dieselbe IP Adresse behält. Die Umsetzung dieser Eigenschaft von Mobile IPv6 war die Kernaufgabe und wurde daher als ersten Ziel zur Umsetzung ausgewählt.

Je nach Fortschritt und Arbeitsaufwand sollte dieser Aufbau mit anderen Funktionen, wie zum Beispiel der Migration von Mobile IPv6 Paketen in eine IPV4 Umgebung oder Voice over IP, erweitert werden, sodass diese dann dem Umfang einer Laborübung im Netzwerkbereich entsprechen.

3.1 Versuchsaufbauten

3.1.1 Verwendetes Material

In Tabelle 3.1 ist eine Auflistung aller verwendeten Materialien über alle Versuchsaufbauten hinweg. Die genaue Zahl der verwendeten Geräte in den einzelnen Versuchen variiert sowie auch die Verwendeten IOS Versionen, da diese den jeweiligen Versuchsaufbauten angepasst wurde.

Die Geräte selbst sind aus dem Bestand der Fachhochschule Salzburg Studiengang Informationstechnik und Systemmanagement stand Wintersemester 2015. Es wurde dabei bewusst Equipment verwendet welches in Größerer Stückzahl vorhanden war, da die Aufgabenstellung es vorsah, bei erfolgreichem Abschluss des Projekts, dieses als Übungseinheit in den laufenden Unterricht einzubinden.

Gerät	*Anzahl*	*IOS*
Router - Cisco 1841	3	c1841-advipservicesk9-mz.151-4.M10 c1841-adventerprisek9-mz.124-22.YB6
Switch - Catalyst 3550	2	c1841-advipservicesk9-mz.151-4.M10 c1841-adventerprisek9-mz.124-22.YB6
WLAN Interface für Cisco 1841	1	- - -
PC	3	Windows 7

Tabelle 3.1: Auflistung des Laborequipments

3.2 Physischer Aufbau

3.2.1 Versuch I

3.2.1.1 Aufbau

Um mit der richtigen Umsetzung von Mobile IPv6 beginnen zu können, sollte ein Basisaufbau erstellt werden. Dieser Basisaufbau sollte ein kleines Netz darstellen, in welchem nur IPv6 Adressen verwendet werden. Das Netz selbst bestand aus zwei Routern, die über einen seriellen Anschluss verbunden waren. Jeder Router war mit einem Switch verbunden, an welchem je ein Host hing. Dieser Aufbau war dazu gedacht als Basis für weitere Übungen zu dienen, um die verschiedenen Möglichkeiten von Mobile IPv6 zu testen.

Der Mobile IPv6 Funktion wurde am Router Mobile, siehe Grafik 3.1, getestet. Da ein möglichst realistisches Szenario gewählt worden war, wurde dieser Router mit einem WLAN Interface ausgestattet. Dieses WLAN Interface sollte ein WLAN Signal senden, welches in unterschiedliche SSIDs unterteilt war. Diesen SSIDs waren unterschiedlich Adressen zugewiesen, allerdings waren sie ohne jegliche Authentifizierung konfiguriert. Wenn ein Netzwechsel nun initiiert werden sollte war eine der SSIDs zu deaktivieren. So konnte der Netzwechsel der Endgeräte simuliert werden indem sie sich von einer SSID zur nächsten verbinden würden.
Dabei war vor allem der Gedanke ausschlaggebend, dass die zeitliche Ersparnis, die einem Mobile IPv6 ermöglicht indem man trotz Netzwechsel die Verbindung aufrechterhalten kann, dadurch verloren gehen würde, wenn man sein Endgerät von einem Fast Ethernet Port auf einen anderen Stecken musste. Außerdem war die Idee, den Versuchsaufbau um eine VoIP Funktion zu erweitern auch sehr stark mit eingeflossen. Da Smartphones, die über VoIP kommunizieren, trotz eines Netzwechsels die Verbindung nicht neu aufbauen müssten.

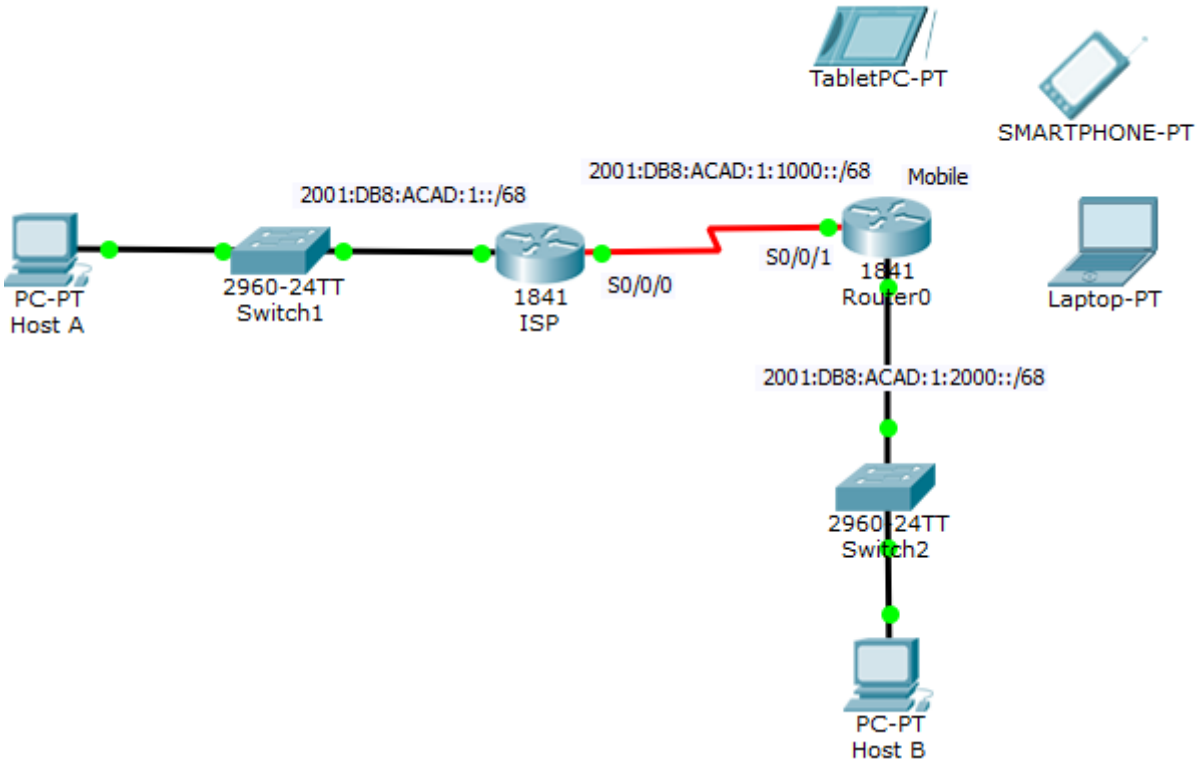

Abbildung 3.1: Basisaufbau Versuch 1

Name	*IP-Adresse*
Ausgangsnetz	2001:DB8:ACAD:1::/64
ISP	
FA 0/0	2001:DB8:ACAD:1::1/68
S 0/0/1	2001:DB8:ACAD:1:1000:1/68
Mobile	
FA 0/1	2001:DB8:ACAD:1:2000::1/68
S 0/0/1	2001:DB8:ACAD:1:1000::2/68
Host A	
FA 0	2001:DB8:ACAD:1::4/68
Host B	
FA 0	2001:DB8:ACAD:1:2000::4/68

Tabelle 3.2: IP Adressen Versuch 1

3.2.1.2 Ergebnisse

Die Funktionen konnten, so wie sie im Aufbau gedacht waren, nicht umgesetzt werden, da im Zuge des praktischen Arbeitens Probleme auftauchten, die nicht zu lösen waren.

Eine Schwierigkeit stellte die Auswahl der richtigen IOS Version für die Router dar. Denn Mobile IPv6 Funktionen wurden nie vollständig in eine IOS Version implementiert, sondern stückchenweise hinzugefügt. So war es bei einer IOS Version so, dass die Mobile IPv6 Befehle nicht in der Auflistung aller möglichen Befehle aufschien aber trotzdem vom System verarbeitet wurden, wenn man sie vollständig per Hand eintippte. Der Vergleich von unterschiedlichen IOS Versionen findet in Kapitel 3.3.3 statt.

Ein Problem entstand durch das verwendete WLAN Interface. Dieses war in der Lage, mit IPv6 Adressen zu arbeiten. Allerdings konnte es keine Mobile IPv6 Befehle interpretieren. Die genauere Ausführung dieses Problems findet in Kapitel 3.4.2 statt. Es konnte auch nicht mit einem anderen WLAN Interface gearbeitet werden, da für die verwendeten Router aus altersbedingten Gründen keine Interfaces mehr produziert werden.

So wurde Versuch I überarbeitet und in Versuch II in adaptierter Form umgesetzt.

3.2.2 Versuch II

3.2.2.1 Aufbau

Da es im Versuch I Probleme mit dem WLAN Interface gab, wurde im Versuch II auf dieses verzichtet. Die Mobile IPv6 Fähigkeiten sollten auf andere Art getestet werden. Ein ausschlaggebender Faktor bei der Überlegung für diesen Aufbau war, ihn mit dem vorhandenen Equipment des Labors zu realisieren. Mit der zusätzlich selbstgewählten Auflage, dass das zur Realisierung verwendete Material in groß genügender Stückzahl vorhanden war, damit ihn mehrere Laborgruppen parallel ausführen könnten. Deswegen wurde ein sehr minimalistischer Versuchsaufbau erarbeitet. Der neue Basisaufbau beinhaltete nun 2 Router, die über einen seriellen Link miteinander verbunden waren. Außerdem war an jedem Router noch je ein Host angehängt. Die Grundidee war es, die einzelnen Interfaces der Router mit unterschiedlichen IP Adressen zu versehen. Der Netzwechsel, und damit der Beweis der Mobile IPv6 Funktionalität, sollte durch das Umstecken der einzelnen Hosts erfolgen.

Dies bedeutet zwar einen längeren zeitlichen Faktor beim Netzwechsel in Kauf nehmen zu müssen, sollte aber trotzdem die Möglichkeiten demonstrieren, immer unter ein und derselben IP Adresse erreichbar zu sein, obwohl sich der Verbindungsknoten nach außen hin geändert hat. Außerdem bestand dadurch die Option, an jedes Interface eines Routers einen beliebigen Host anhängen zu können und eine sofortige Kommunikation untereinander zu ermöglichen. Dies war für eine größere, Gruppenübergreifende Laborübung eine Möglichkeit, Variation ein-

zubringen.

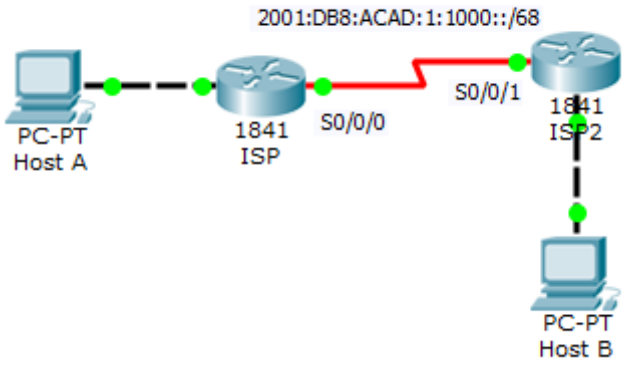

Abbildung 3.2: Basisaufbau Versuch 2

Name	*IP-Adresse*
Ausgangsnetz	2001:DB8:ACAD:1::/64
ISP	
FA 0/1	2001:DB8:ACAD:1:4000::1/68
FA 0/0	2001:DB8:ACAD:1::1/68
S 0/0/1	2001:DB8:ACAD:1:1000:1/68
ISP2	
FA 0/1	2001:DB8:ACAD:1:2000::1/68
FA 0/0	2001:DB8:ACAD:1:3000::1/68
S 0/0/1	2001:DB8:ACAD:1:1000::2/68
Host A	
FA 0	2001:DB8:ACAD:1::4/68
Host B	
FA 0	2001:DB8:ACAD:1:2000::4/68

Tabelle 3.3: IP Adressen Versuch 2

3.2.2.2 Ergebnisse

Im Zuge dieses Versuchsaufbaus ergab sich immer mehr die Problematik der interaktiven Kommunikation zwischen Host und Router. Denn damit der Host immer unter derselben IP Adresse erreichbar sein kann, muss der Host seinem Home Agent mitteilen, wenn er einen Netzwechsel vollzogen hat und unter über welche Adresse er nun erreichbar ist. Auch wenn der Home Agent eine Anfrage weiterleitet und der Host eine direkte Verbindung mit seinem Kommunikationspartner aufbaut, um weniger Redundanz im Netz zu haben, war es nötig, dass der Host in der Lage war, selbst Daten und Informationen zu senden und empfangen.

Auch wenn man auf dynamische Weise eine Adresszuweisung machen wollte war es nötig, dass der Host aktiv kommunizierte. Denn einer der großen Hauptvorteile von Mobile IP ist, dass Applikationen in den oberen Schichten vom Netzwechsel in den unteren nichts mitbekommen. Es ist zwar möglich, einem Host, wenn er sich das erste Mal mit einem Router verbindet, über DHCP eine Adresse zuzuweisen und diesen Router als Home Agent für den Host zu erstellen. Wenn sich der Host jedoch mit einem anderen Netz verbindet, wird im dort wieder eine neue Adresse zugewiesen und diese Adresse, auch ?Care of Adresse? genannt, muss der Host an seinen Home Agent weiterleiten damit dieser in der Lage ist, ihn zu erreichen. Ein erneutes Verbinden mit einer Applikation unter der neu erhaltenen IP Adresse wäre zwar möglich, jedoch widersprüchlich zum Mobile IP Gedanken.

Es stellte sich heraus, dass die verwendeten Host nicht in der Lage waren, diese Interaktionen zu realisieren. Eine genauere Ausführung zu diesem Problem findet sich in Kapitel 3.4.3. Deshalb wurde Versuch II, die neuen Ergebnisse miteinbeziehend, überarbeitet und in Versuch III umgesetzt.

3.2.3 Versuch III

3.2.3.1 Aufbau

Da sich in Versuch II gezeigt hatte, dass die zur Verfügung stehenden Endgeräte nicht Mobile IPv6 fähig waren, nahm Versuch III eine Erweiterung des Mobile IPv6 Protokolls als Grundstein her. Die Network Mobility (NEMO) Erweiterung lagert die Mobile IPv6 Funktionen auf die Router aus. Dies bedeutet, dass der Router in der Lage ist, einen Netzwechseln zu vollziehen und mit ihm ebenso die verbundenen Endgeräte. Dies kann unabhängig von allen Endgeräten passieren, da die Logik komplett am Router verarbeitet wird. Ein Beispiel hierfür sind öffentlichen Verkehrsmittel. Wenn diese eine Internetanbindung im Transportwagen anbieten, werden sich viele Endgeräte mit dem Knoten verbinden. Für die Endgeräte bleibt dieser Verbindungsknoten immer derselbe, der Knoten selbst jedoch ist mit dem Transportmittel in Bewegung und muss sich deshalb immer eine neue Verbindung suchen, vollzieht also immer wieder einen Netzwechsel. Hierbei könnte Mobile IPv6 eine Lösung anbieten, um diesen Netzwechsel zu optimieren.

Der neue Grundaufbau bestand deshalb aus drei Routern. Zwei davon, ISP und ISP2, stellten unterschiedliche Netze dar und der dritte, Mobile Router, einen zwischen den Netzen wechselnden Knoten. Je ein Host war an jeden Router mit dem Ziel angeschlossen, sich untereinander trotz Netzwechsels desselben immer noch erreichen zu können.

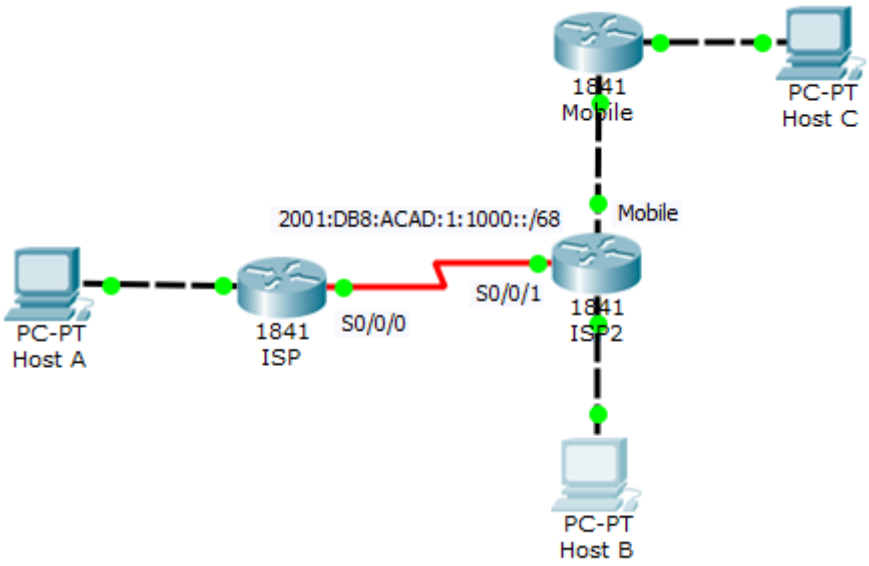

Abbildung 3.3: Basisaufbau Versuch 3

Name	*IP-Adresse*
Ausgangsnetz	2001:DB8:ACAD:1::/64
ISP	
FA 0/1	2001:DB8:ACAD:1:4000::1/68
FA 0/0	2001:DB8:ACAD:1::1/68
S 0/0/1	2001:DB8:ACAD:1:1000:1/68
ISP2	
FA 0/1	2001:DB8:ACAD:1:2000::1/68
FA 0/0	2001:DB8:ACAD:1:3000::1/68
S 0/0/1	2001:DB8:ACAD:1:1000::2/68
Mobile	
FA 0/1	2001:DB8:ACAD:1:3000::3/68
FA 0/0	2001:DB8:ACAD:1:3000::2/68
Host A	
FA 0	2001:DB8:ACAD:1::4/68
Host B	
FA 0	2001:DB8:ACAD:1:2000::4/68
Host C	
FA 0	2001:DB8:ACAD:1:3000::5/68

Tabelle 3.4: IP Adressen Versuch 3

3.2.3.2 Ergebnisse

Ergebnis dieses Versuchsaufbaus war, dass trotz NEMO Erweiterung die Mobile IPv6 Funktionalität nicht hergestellt werden konnte. Am Router konnte NEMO zwar konfiguriert werden, sodass die Endgeräte selbst nicht mehr intelligent genug

für den Informationsaustausch sein mussten. Nachdem aber der Mobile Router seinen Netzwechsel vollzogen hatte, wurden keine Informationen mehr zwischen den Routern ausgetauscht. In Folge war eine Verbindung zwischen den Hosts deshalb nicht herzustellen. Die genaue Ausführung des Problems findet in Kapitel 3.4.4 statt.

3.3 Analyse der Hardware und Software

Um den Aufbau des Mobile IPv6 Szenarios im Netzwerklabor durchführen zu können, musste zuerst die benötigte Hardware und die erforderliche Software ermittelt werden.

Die erste Überlegung für den Aufbau des Szenarios war, den Wechsel zwischen den Netzwerken mittels WLAN zu ermöglichen. Dazu wird ein Wireless Access Point benötigt, dieser sollte durch einen Router mit einem WLAN Interface repräsentiert werden.

Als Router stand ein Cisco 1841 Integrated Services Router zur Verfügung. Der Cisco 1841 Router hat die Möglichkeit verschiedene Interfaces über mehrere Steckplätze aufzunehmen. Ein Steckplatz wurde verwendet um das WLAN Interface einzusetzen. Die Idee war es über dieses WLAN Interface zwei Netzwerke mit verschiedenen Netzwerknamen (SSID) auszustrahlen. Der mögliche Aufbau dieses Szenarios kann der Abbildung 3.1 entnommen werden.

3.3.1 Analyse des WLAN Interfaces

Um den Service des mobilen IPv6 zu implementieren, muss dieses Interface die Konfiguration eines Home Agents unterstützen. Die Überprüfung des Interfaces auf diese Fähigkeit ergab, dass die benötigten Konfigurationsschritte nicht unterstützt werden. Nach ausgiebiger Recherche, unter anderem mit Rücksprache mit dem Hersteller Cisco, musste festgestellt werden, dass die Hardware die Technologie des mobilen IPv6 noch nicht unterstützt. Somit musste die Idee, den Netzwechsel mit Wireless Netzen zu simulieren, durch eine Alternativlösung ersetzt werden. Die Alternative war schnell gefunden, man kann den Netzwechsel auch durch manuelles Stecken der Netzwerkkabel auf verschiedene Interfaces des Routers simulieren. Dabei stellt jedes Interface ein anderes Netzwerk da. Dieses Szenario wir in Punkt 3.4.3 ausführlich beschrieben.

3.3.2 Analyse des Routers

Des Weiteren muss der Router die Mobile IPv6 Konfiguration unterstützen. Diese Konfiguration benötigt die Implementierung eines Home-Agents auf einem Interface des Routers, die Aktivierung des mobilen Routers und die Aktivierung des NEMO Dienstes.
Um die benötigten Dienste zu aktivieren, bedarf es einer richtigen Version des Betriebssystems (IOS) auf den Cisco Routern.
Unter Berücksichtigung der geforderten Services musste eine Recherche angestellt werden, um die korrekte IOS Version zu ermitteln. Nach dem Vergleich der

verschiedenen Features der IOS Versionen konnte das passende Betriebssystem eruiert werden.

3.3.3 Auswahl des IOS

Bei der Suche nach der passenden Software wurde davon ausgegangen, dass das aktuellste IOS alle benötigten Eigenschaften besitzt. Dies erwies sich jedoch als Trugschluss. Man muss das Betriebssystem nach den geforderten Eigenschaften auswählen. Es wurden zwei Versionen in Betracht gezogen, zum einen die aktuelle IOS Version *c1841-advipservicesk9-mz.151-4.M10* und zum anderen die Version *c1841-adventerprisek9-mz.124-22.YB6*.

Gegenüberstellung der beiden IOS Versionen:

Release: / *Service:*	15.1(4)	12.4(22)
IPv6	√	√
Mobile IPv6	√	√
IPv6 Home-Agent	√	√
IPv6 Mobile-Router	×	√
NEMO	×	√

Tabelle 3.5: Gegenüberstellung zweier IOS Versionen

Nach intensiver Erarbeitung der erforderlichen Eigenschaften fiel die Wahl, mit Hilfe der Tabelle 3.5,auf die IOS Version *c1841-adventerprisek9-mz.124-22.YB6*. Die Dienste *Mobile-Router* und *NEMO* sind für die Ausarbeitung des Szenarios dieser Arbeit essentiell und müssen gegeben sein. Der Gedanke hinter der Technologie *NEMO* wird im Abschnitt 2.6 detailliert erläutert.

3.3.4 Analyse der Endgeräte

Die Endgeräte in einer Mobile IPv6 Umgebung müssen IPv6 fähig sein und zusätzlich den Dienst des mobilen IPv6 unterstützen.
Mobile Knoten tauschen mit ihrem Home-Agent Informationen aus. Welche Informationen dabei ausgetauscht werden, wird in Punkt 2.6.1 beschrieben.
Beim Aufbau des Szenarios im Netzwerklabor standen Rechner mit Windows 7 zur Verfügung. Windows 7 ist IPv6 fähig, unterstützt aber den Dienst Mobile IPv6 momentan noch nicht. Unter Windows bietet den Dienst lediglich das Betriebssystem Windows Server 2003. Microsoft gibt an, dass die Technologie für andere

Betriebssysteme noch nicht ausreichend ausgearbeitet wurde und somit noch nicht zu Verfügung steht[5].
Sollten, wie es bei dieser Arbeit vorkommt, die Endgeräte Mobile IPv6 nicht unterstützen, kann *NEMO* Abhilfe verschaffen. Die Funktion von *NEMO* wird im Abschnitt 2.6 genauer erklärt.

3.4 Implementierung

In diesem Abschnitt wird beschrieben, welche Konfigurationen auf den verwendeten Cisco 1841 Router vorgenommen wurden. Im laufe der praktischen Ausarbeitung kam es zu Änderungen des Grundaufbaues und somit wurden verschieden Konfigurationen durchgeführt und evaluiert. Die wesentlichen Anforderungen an die Router liegen neben den Grundvoraussetzungen, wie Routing-Protokolle und die Unterstützung von IPv6, in den Funktionalitäten, welche die Konfiguration von Mobile IPv6 ermöglichen.
Die in den nachfolgenden Kapiteln beschriebenen Konfigurationsschritte wurden der Cisco Dokumentation *Implementing Mobile IPv6* [6] entnommen.

3.4.1 Grundaufbau

Da verschiedene Aufbauten getestet wurden, wurde ein Grundaufbau des Testnetzes erstellt. Auf diesen Grundaufbau basieren alle getesteten Szenarien. Dieser Aufbau wurde zur besseren Veranschaulichung mittels *Cisco Packet Tracer* simuliert. Der nachfolgenden Grafik 3.4 ist dieser Grundaufbau zu entnehmen.

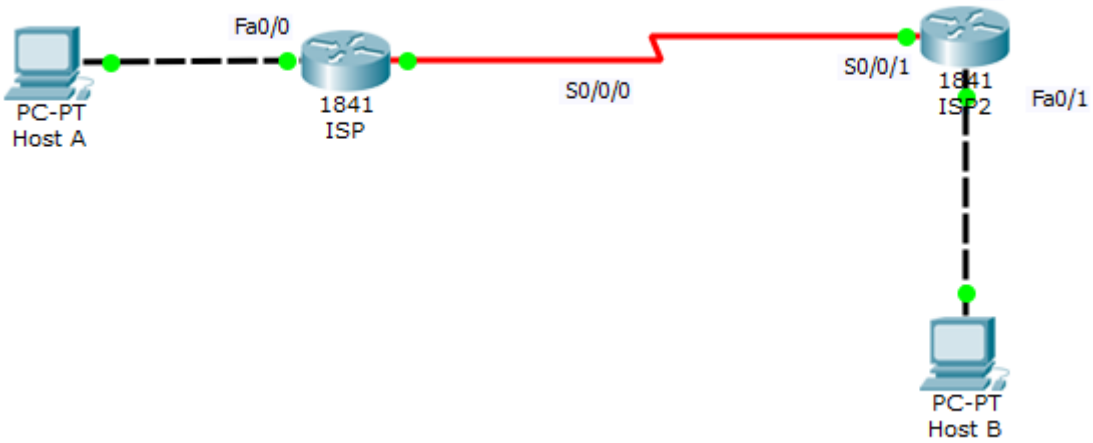

Abbildung 3.4: Grundaufbau

Als Routing-Protokoll für das Testnetzwerk wurde OSPFv3 konfiguriert. OSPFv3 ist ein Routing-Protokoll für IPv6 Adressen. Außerdem beinhaltet OSPFv3 die Neighbor Discovery Funktion, welche dafür zuständig ist eine Liste zu erzeugen,

in der alle benachbarten Router, zu denen eine bidirektionale Verbindung besteht, aufgelistet werden.

Die Adressierung der einzelnen Geräte erfolgte durch Vergabe statischer IPv6 Adressen. Es gäbe auch die Möglichkeit die IPv6 Adressen automatisch durch eine Autokonfiguration zuweisen zu lassen, dies wurde jedoch in dieser Arbeit nicht implementiert.

In Tabelle 3.6 sind die eingerichteten IPv6 Adressen der Router Interfaces und die zu den Hosts vergebenen IPv6 Adressen dargestellt.

Host	**Interface**	**IPv6 Adresse**
ISP	Fa0/0	2001:DB8:ACAD:1::1/68
ISP	S0/0/0	2001:DB8:ACAD:1:1000:1/68
ISP2	Fa0/1	2001:DB8:ACAD:1:2000::1/68
ISP2	S0/0/1	2001:DB8:ACAD:1:1000::2/68
Host A	Fa0	2001:DB8:ACAD:1::4/68
Host B	Fa0	2001:DB8:ACAD:1:2000::4/68

Tabelle 3.6: Für den Grundaufbau verwendete IPv6 Adressen

Eine Auflistung der vorgenommen Grund-Konfigurationen der Router *ISP* und *ISP2* ist im Anhang A zu finden.

3.4.2 WLAN Ansatz

Um die Funktion von Mobile IPv6 zu testen, sollte einen Netzwechsel stattfindend. Dazu wurden zunächst versucht den Netzwechsel mit Hilfe von zwei WLAN Netzen zu simulieren.
Der Aufbau dieses Testnetzwerks ist der Topologie 3.1 zu entnehmen. Die Grundkonfiguration der Router wurde aus Punkt 3.4 verwendet. Es wurden zwei WLAN Netzwerke am Router konfiguriert. Danach sollte es dem Endgerät möglich sein sich jeweils mit einem der beiden Netze zu verbinden. Ein Netz sollte dabei als Heimnetzwerk des Endknotens dienen, das andere Netzwerk sollte ein Fremdnetz darstellen.
Das WLAN Module des Cisco Routers bietet zwei Interfaces, zum einen das Interface *Dot11Radio 0/0/1* und zum anderen das Interface *interface Dot11Radio 0/1/0*.

Für dieses Testszenario wurde das Interface *Dot11Radio 0/1/0* gewählt. Auf diesem Interface wurden zwei Subinterface erstellt. Anschließend wurde jedem VLAN ein

Netzwerk mit eigenem SSID zugewiesen. Für dieses Testnetz erfolgt der Zugriff auf das Netzwerk ohne Authentifizierung.

Die vorgenommene Konfiguration der beiden WLAN Netzwerke am Router *ISP2* ist im Anhang B zu finden.

Das, dem Subinterface *Dot11Radio 0/1/0.1* zugewiesene, Netzwerk sollte als Heimnetz dienen. Nachdem die Subinterface erfolgreich konfiguriert wurden, musste der Router in den *interface configuration mode* versetzt werden. In diesem Zustand wurde anschließend der mobile IPv6 Home-Agent am Interface *Dot11Radio 0/1/0.1* gestartet. Die erforderliche Schritte sind dem folgendem Quellcodeausschnitt 3.1 zu entnehmen.

```
1 ISP2(config)# interface Dot11Radio 0/1/0.1
2 !
3 ISP2(config-if)# ipv6 mobile home-agent
```

Quellcode 3.1: Mobile IPv6 HA am WLAN Interface

Bei dem Versuch, den IPv6 Home-Agent am Interface zu starten, trat jedoch ein Fehler auf. Es stellte sich heraus, dass die Konfiguration eines IPv6 Home-Agents auf dieser Ausführung des WLAN Moduls nicht möglich ist. Eine Konfiguration eines IPv4 Home-Agents ist hingegen möglich und könnte durch einen Tunnel auf IPv6 Adressen angepasst werden. Da sich diese Arbeit ausschließlich mit der Umsetzung unter Verwendung von IPv6 Adressen beschäftigt, war dies keine Option für das Testnetzwerk.
Schlussendlich wurde der WLAN Ansatz durch eine Alternative ersetzt. Die Alternative war es, den Netzwechsel durch Stecken der Netzwerkkabel auf verschiedene Interfaces des Routers zu simulieren. Die Implementierung des neuen Testszenarios folgt im nächsten Abschnitt 3.4.3.

3.4.3 LAN Ansatz

Da der Netzwerkwechsel aufgrund technischer Diskrepanzen nicht mit WLAN Netzen simuliert werden konnte, fiel die Entscheidung auf den Ansatz den Netzwechsel durch ein LAN Netzwerk zu ermöglichen.
Dabei werden an jedem Interface des Routers verschieden Netzwerke konfiguriert. Es ist dann möglich die angeschlossenen Netzwerkkabel auf ein anderes Interface und somit in ein anderes Netzwerk zu stecken.
Der Aufbau dieses Testnetzwerks ist der Topologie 3.2 zu entnehmen.

Wie bei Punkt 3.4.2 wurde die Grundkonfiguration der Router aus Punkt 3.4

übernommen. Am Router *ISP2* war das Interface *fa 0/0* noch nicht unter Verwendung und konnte somit als Home-Agent-Interface genutzt werden.
An diesem Interface wurde der Mobile IPv6 Home-Agent Service konfiguriert, d.h. für den Mobilen Knoten stellte dieses Interface den Home-Agent dar.

Auch hier musste zunächst der Mobile IPv6 Home-Agent Service am Interface initialisiert werden. Der nachfolgende Quellcodeausschnitt 3.2 zeigt die dazu erforderliche Konfiguration.

```
1 ISP2(config)# interface fa 0/0
2 !
3 ISP2(config-if)# ipv6 mobile home-agent
```

Quellcode 3.2: Mobile IPv6 HA am LAN Interface

Um das Interface erfolgreich als Mobile IPv6 Home-Agent zu initialisieren musste dem Interface eine gültige Adresse zugewiesen werden. Für dieses Testnetzwerk wurde die Vergabe von Adressen statisch gehandhabt. Die IPv6 Adresse für das Interface *fa 0/0* kann der Tabelle 3.7 entnommen werden.
Des Weiteren wurde ein zusätzlicher Host in das Testszenario mitaufgenommen. Dieser repräsentiert den mobilen Knoten, welcher mit seinem Home-Agent an Interface *fa 0/0* des Routers *ISP2* verbunden ist.
Der mobile Knoten bzw. der Host wurde dann manuell an das freie Interface *fa 0/1* des Routers *ISP* angeschlossen.
Die beiden IPv6 Adressen des Hosts und des Interfaces *fa 0/1* des Routers *ISP* wurden ebenfalls statisch zugewiesen und konfiguriert und sind wiederum der Tabelle 3.7 zu entnehmen.

Host	**Interface**	**IPv6 Adresse**
ISP	Fa0/1	2001:DB8:ACAD:1:4000::1/68
ISP2	Fa0/0	2001:DB8:ACAD:1:3000::1/68
Host C	Fa0	2001:DB8:ACAD:1:3000::5/68

Tabelle 3.7: IPv6 Adressen

Nachdem alle benötigten IPv6 Adressen konfiguriert waren, wurde der Status des Mobile IPv6 Home-Agent Service überprüft. Der Router *ISP2* wurde dazu auf lokale aktive Home-Agents abgefragt. Der verwendete Quellcode kann dem Ausschnitt 3.2 entnommen werden.

```
ISP2# show ipv6 mobile home-agent
```

Quellcode 3.3: Zeigen lokaler Home-Agents

Die Evaluierung der Ausgabe ergab, dass der Home-Agent Service aktiv ist. Der nächste Schritt war es, Binding Informationen zu erstellen. Binding steht für die Bindung zum Heimnetzwerk, es ist die Assoziation zwischen der Heimadresse und der zugeteilten Care-of-Adresse. Wenn der mobile Knoten das Heimnetz verlässt, sollte der Home-Agent jederzeit wissen unter welcher Care-of-Adresse der Host erreichbar ist. Dazu teilt der mobile Knoten seinem Home-Agent seine temporäre Adresse in Form einer Binding Nachricht mit. Die Binding Nachrichten sind insofern wichtig, damit der Home-Agent weiß, unter welcher Adresse der mobile Knoten erreichbar ist. Der Home-Agent speichert diese Informationen in einer Binding Tabelle und kann somit eingehende Nachrichten an den mobilen Knoten weiterleiten.

Für die Konfiguration von den Binding Parametern ist zunächst eine Access-List notwendig. Mit ihr teilt man dem Home-Agent mit, welche Adressen bzw. welche Adressbereiche die Erlaubnis haben sich mit dem Netz des Home-Agents zu verbinden. Für Testzwecke wurden jegliche Adressen erlaubt. Die Erstellung der IPv6 Access-List ist im folgenden Konfigurationsausschnitt 3.4 aufgeführt.

```
ISP2(config)# ipv6 access-list list1
!
ISP2(config-ipv6-acl)# permit icmp any any
```

Quellcode 3.4: Konfiguration Access-List

Mit der erstellten Access-List wurde anschließend die Binding-Konfiguration durchgeführt. Die Konfiguration beinhaltet eine Vielzahl von Parametern. Es wurde angegeben, welche Access-List betrachtete wird, welche Authentifizierung verwendet werden soll, wie lange das Binding bestehen bleibt, die maximale Anzahl an möglichen Bindungen und das Interval in welcher Zeit die Binding Informationen erneuert werden. Die Binding Konfiguration wurde in folgender Form getätigt:

ISP2(config-ha)# binding access access-list | auth-option | seconds | maximum | refresh

Die Erstellung der Binding Informationen kann dem Quellcodeausschnitt 3.5 entnommen werden.

```
ISP2(config)# ipv6 mobile home-agent
!
ISP2(config-ha)# binding access list1 open 2000 15 20
```

Quellcode 3.5: Konfiguration Binding Informationen

Nachdem die Binding Informationen konfiguriert waren, konnte der Netzwechsel vorgenommen werden. Dazu wurde Host C von seinem Home-Agent (Router *ISP2*) getrennt und mit dem Fremdnetz an Router *ISP* verbunden. Als Konsequenz des Netzwechsels sollte es nun zu Einträgen in die Binding Tabelle des Home-Agents kommen. Ob ein Eintrag in die Binding Tabelle zustande gekommen ist kann mit dem nachfolgenden Quellcode 3.6 überprüft werden.

```
ISP2# show ipv6 mobile binding
```

Quellcode 3.6: Überprüfung der Bindings

Die Kontrolle des Ergebnisses ergab, dass es zu keinem Eintrag in die Binding Tabelle des Home-Agents gekommen ist. Der Grund dafür ist, dass das Betriebssystem der Laborrechner die Implementierung von Mobile IPv6 nicht gewährleistet. Die mobilen Knoten müssen in gewisser Weise intelligent genug sein um Binding Updates zu senden. Windows 7 oder auch Windows XP enthalten zwar IPv6-Funktionalitäten, jedoch stehen keine Möglichkeiten zur Verfügung, die es erlauben würden einen Windows-Rechner als mobilen Knoten oder als Home-Agent zu implementieren. Windows 7 ist lediglich in der Lage mit mobilen Knoten zu kommunizieren, wobei es die Care-of-Adressen der mobilen Knoten in einer Binding Tabellen zur Verfügung stellt. Der Nachweis dafür kann bei Microsoft nachgelesen werden. Dort heißt es, die Technologie sei für die Endsysteme noch nicht ausreichend ausgearbeitet und steht daher noch nicht zu Verfügung [5].

Als Konsequenz daraus wurde nach einer alternativen Lösung gesucht. Eine Alternative bietet NEMO, kurz für Network Mobility. Der Versuch der Implementierung des neuen Testszenarios folgt im nächsten Abschnitt 3.4.4.

3.4.4 NEMO Ansatz

Mit Network Mobility kann man der fehlenden Intelligenz der Endgeräte entgegenwirken. Bei NEMO dient ein mobiler Router als mobiler Knoten. Somit wird ermöglicht, dass der mobile Knoten jederzeit erreichbar bleibt auch wenn dieser in Bewegung ist. Der mobile Router fungiert dabei als Ansprechpartner für den Home-Agnet, über den HA läuft die gesamte Kommunikation. Es werden sozusagen ganze Netzwerkteile bewegt, nicht nur die Endgeräte. Der mobile Router

ist dazu im Stande Binding Updates zu senden. Eine detaillierte Beschreibung der Vorgehensweise bei NEMO befindet sich im Abschnitt 2.6.

Für die Umsetzung dieses Szenarios wurde eine weitere Netzwerktopologie erstellt. Der Aufbau dieses Testnetzwerks ist der Topologie 3.3 zu entnehmen. Die Grundkonfiguration der Router wurde aus Punkt 3.4 verwendet.

Zunächst wurden analog zur Konfiguration aus Abschnitt 3.4.3 das Interface *fa 0/0* des Router *ISP2* als Home-Agent deklariert, eine Access-List erstellt und die Binding Parameter festgelegt. Die erforderlichen Konfigurationsschritte können dem Ausschnitt 3.7 entnommen werden.

```
1  ISP2(config)# interface fa 0/0
2  !
3  ISP2(config-if)# ipv6 mobile home-agent
4  !
5  ISP2(config-if)# exit
6  !
7  ISP2(config)# ipv6 access-list list1
8  !
9  ISP2(config-ipv6-acl)# permit icmp any any
10 !
11 ISP2(config-if)# exit
12 !
13 ISP2(config)# ipv6 mobile home-agent
14 !
15 ISP2(config-ha)# binding access list1 open 2000 15 20
```

Quellcode 3.7: NEMO - HA, ACL und Binding

Anschließend musste der NEMO Service am Home-Agent-Router *ISP2* aktiviert werden. Die administrativen Distanz der NEMO Routen wurde mit 10 festgelegt. Der Quellcodeausschnitt 3.8 zeigt die Konfiguration.

```
1  !
2  ISP2(config-rtr)# distance 10
```

Quellcode 3.8: NEMO am Home-Agent

Als mobiler Router wurde der Router *MobileRouter* in die Topologie aufgenommen. Die Grund-Konfiguration dieses Routers ist im Anhang C zu finden.

Die beiden IPv6 Adressen des mobilen Routers wurden ebenfalls statisch zugewiesen und konfiguriert und sind der Tabelle 3.8 zu entnehmen.

Host	Interface	IPv6 Adresse
MobileRouter	Fa0/0	2001:DB8:ACAD:1:3000::2/68
MobileRouter	Fa0/1	2001:DB8:ACAD:1:3000::3/68

Tabelle 3.8: IPv6 Adressen Mobile Router

Zusätzlich zur der Konfiguration des Home-Agents wurde NEMO am mobilen Router implementiert. Der mobile Router übernimmt wesentlichen Aufgaben, die durch Windows 7 nicht gewährleistet werden, aber essentiell für die Implementierung von Mobile IPv6 sind.
Zuerst wurde die NEMO Funktionalität am Router aktiviert. Anschließend wurde ein *EUI-64* (Extended Unique Identifier) Interface bestimmt, dadurch wird ermöglicht den Interface-Identifier automatisch zu generieren, um eine IPv6 Adresse ohne manuelle Konfiguration oder zusätzliche Dienste wie DHCP zu erhalten.
Als nächster Schritt folgte die Zuweisung des Heimnetzwerkes, damit erfährt der mobile Router sein Heimnetz und kann somit feststellen, wenn er sich in seinem Heimnetzwerk befindet.
Darauf folgend wurde es dem mobilen Router ermöglicht eine Heimadresse zu bilden. Diese Adresse setzt sich aus dem 64 Bit langem Interface-Identifier (*EUI-64*) und dem Subnet Präfix zusammen. Der Subnet Präfix ist ein Netzwerkteil und muss somit mit dem Heimnetz übereinstimmen. Daher wurde dem mobilen Router übergeben, dass die Heimadresse aus Heimnetzwerk und dem Interface-Identifier besteht.
Des Weiteren wurde dem mobilen Router mitgeteilt, dass sich nur eindeutig übereinstimmende IPv6 Präfixe registrieren können. Die Lebensdauer der Registrierung wurde dabei auf 600 Sekunden gesetzt. Nach ablaufen dieser Zeit wird der mobile Router nicht mehr als registriert aufgeführt. Somit wird sichergestellt, dass nur aktive mobile Router aufgelistet werden. Um die Registrierung aufrecht zu erhalten wurden Router-Advertisement Nachrichten in einem gewissen Zeitabstand konfiguriert. Diese Advertisement Nachrichten werden verwendet um die Anwesenheit im Netzwerk kundzutun.
Die Router-Advertisement Nachrichten werden in einem gewissen statischen Intervall ausgesandt, es gibt jedoch auch die Möglichkeit diese Nachrichten zu erzwingen. Dazu werden Router-Solicitation Nachricht an die Multicast Adressen geschickt. Dies kann einen Vorteil bei Änderungen im Netzwerk sein, da man nicht erst auf die Router-Advertisement Nachrichten warten muss. Multicast Adressen

beschreiben eine Gruppe von Adressen, sie werden gleichzeitig angesprochen und erhalten somit alle die Nachrichten.
Das Intervall der Router-Advertisement Nachrichten wurde auf 200 Sekunden gesetzt. Außerdem wurde ein IPv6 Präfix bestimmt, welcher von den Router-Advertisement Nachrichten angesprochen wird. Der Präfix für das Testnetzwerk lautet *2001:db8::/35*.
Abschließend wurde das Interface *fa 0/1* des Router *MobileRouter* als Roaming-Interface deklariert. Roaming ermöglicht es dem mobilen Router in einem Fremdnetz Daten zu empfangen und zu senden.

Die beschriebenen Konfigurationen werden in dem folgendem Quellcodeausschnitt 3.9 aufgelistet und dienen so zur besseren Veranschaulichung.

```
1  MobileRouter(config)# ipv6 mobile router
2  !
3  MobileRouter(IPv6-mobile-router)# eui-interface fa 0/1
4  !
5  MobileRouter(IPv6-mobile-router)# home-network
6  !
7  MobileRouter(IPv6-mobile-router)# home-address home-network
8                                    eui-64
9  !
10 MobileRouter(IPv6-mobile-router)# explicit-prefix
11 !
12 MobileRouter(IPv6-mobile-router)# register lifetime 600
13 !
14 MobileRouter(config)# interface fa 0/1
15 !
16 MobileRouter(config-if)# ipv6 nd advertisement-interval
17 !
18 MobileRouter(config-if)# ipv6 nd ra interval msec 200
19 !
20 MobileRouter(config-if)# ipv6 nd prefix 2001:DB8::/35
21 !
22 MobileRouter(config-if)# ipv6 mobile router-service roam
23 !
24 ISP2(config)# ipv6 router nemo
```

Quellcode 3.9: NEMO am Mobile Router

Nachdem die Konfiguration abgeschlossen war, wurde der Netzwechsel vollzogen. Nun sollte es zu Einträgen in die Binding Tabelle des Home-Agents kommen. Nach Überprüfung der Binding Tabelle musste jedoch festgestellt werden, dass es auch dieses mal zu keinen Einträgen gekommen war.
Nach ergiebiger Recherche und Interpretation der Ergebnisse konnte festgestellt werden, dass die zur Verfügung stehende Hardware im Netzwerklabor einer erfolgreichen Umsetzung im Wege steht.
Die unzureichenden Fähigkeiten der Hardware lässt sich auf die Version zurückzuführen. Aktuellere Versionen bieten demnach eine Vielzahl von Erweiterungen und Neuerungen, welche die Implementierung von Mobile IPv6 begünstigen würde. Jedoch konnte mit NEMO aufgeführt werden, dass Mobile IPv6 auch mit Endsystemen möglich ist, in denen sich Endgeräte befinden, welche nicht dazu in der Lage sind Binding Updates zu senden.

4 Zusammenfassung und Ausblick

Diese Bachelorarbeit befasste sich mit dem Aufbau eines Mobile IPv6 Szenarios im Netzwerklabor. Mobile IPv6 ist ein Protokoll, welches es ermöglicht eine feste IPv6 Adresse einem mobilen Endgerät zuzuweisen und diese auch bei einem Netzwechsel zu behalten.

Um die Vorzüge von Mobile IPv6 zu erläutern wurde eine genaue Beschreibung von Mobile IPv6 aufgeführt. Außerdem wurde ein Vergleich zwischen Mobile IPv4 und Mobile IPv6 gezeigt um die Änderungen darzustellen. Ein großer Vorteil von IPv6 ist, dass die Möglichkeiten zur Adressierung von Systemen von IPv6 gegenüber IPv4 stark gestiegen sind. Somit kann man dem prognostizierten Verbrauch von IP Adressen entgegenwirken. Jedoch musste festgestellt werden, dass bei derzeitigen Entwicklungsstand von Anwendungen und Hardware eine Einführung von Mobile IPv6 aufgrund fehlender Hardware- und Softwareunterstützungen nicht möglich ist.

Nach einer allgemeineren Untersuchung bezüglich der Systemunterstützung von IPv6, muss festgehalten werden, dass auch hier Diskrepanzen bestehen. In den letzten Jahren hat sich viel getan in Richtung IPv6, dennoch gibt es weiter viele Lücken in den Betriebssystemen und in den Routern, welche die Implementierung von IPv6 und insbesondere von Mobile IPv6 nahezu unmöglich machen. So stellte sich zum Beispiel bei dem Versuch einem WLAN Interface eine IPv6 Adresse zuzuweisen heraus, dass dieses IP Adressen der Version 6 nicht unterstützt. Jedoch kann davon ausgegangen werden, dass dieses Problem in naher Zukunft durch Aktualisierungen der Hardware von den Herstellern behoben sein wird. Früher oder später werden zukünftige Konfigurationen von IP Adressen überwiegen auf IPv6 Adressen errichtet.

Im Netzwerklabor wurden nach auftretenden Problemen drei Testszenarien aufgebaut. Jedes der Szenarien konnte verschiedene Probleme beheben. Am Ende jedoch muss festgehalten werden, dass die fehlende Implementierung von Mobile IPv6 eine Umsetzung unmöglich macht. Anhand der dabei gewonnen Erkenntnisse und Erfahrungen lässt sich sagen, dass zum Beispiel die Möglichkeit der Adressvergabe sowie das Subnetting einen großen Vorteil bietet.

Ein Ausblick auf zukünftige Implementierungen bezieht sich hauptsächlich auf die Anschaffung von aktuelleren Hardwareversionen, welche IPv6 im allgemeinen und Mobile IPv6 besser unterstützen und die Implementierung von Mobile IPv6 unter Linux. Linux bietet unter anderem Kernelversionen, welche es erlauben Binding Updates zu erstellen und zu senden. Die Umsetzung mit Linux wurde in dieser

Arbeit jedoch nicht berücksichtigt, könnte aber eine Lösung bieten.

Abschließend lässt sich sagen, dass trotz der zur Zeit mangelhaften Systemunterstützungen die Technologie von Mobile IPv6 ein großes Potential besitzt. Die unzureichende Implementierung von Mobile IPv6 lässt sich wahrscheinlich auf die zu heutigen Zeitpunkt fehlende Notwendigkeit zurückführen. Auf lange Sicht wird die Umstellung zu IPv6 und die damit verbundenen Dienste immer weiter voranschreiten. Es wird also irgendwann zu dem Zeitpunkt kommen, an dem diese Technologien weiter entwickelt und auch umgesetzt werden.

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.

[5] Microsoft Inc., "Understanding Mobile IPv6," Online-Quelle, April 2004, http://www.microsoft.com/en-us/download/details.aspx?id=10905; zuletzt abgerufen am 23.12.2015.

[6] Cisco Systems Inc., "Implementing Mobile IPv6," Online-Quelle, Juli 2012, http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ipv6-15-2mt-book/ip6-mobile.pdf; zuletzt abgerufen am 26.01.2016.

Abkürzungsverzeichnis

HA	...	Home Agent
MN	...	Mobile Node
CN	...	Correspondent Node
CoA	...	Care-of Address
HoA	...	Home Adresse
IOS	...	Internetwork Operating System
MR	...	Mobile Router
NEMO	...	Network Mobility

Abbildungsverzeichnis

Tabellenverzeichnis

Quellcodeverzeichnis

Anhang

Anhang A

Router ISP

```
hostname ISP
!
ipv6 unicast-routing
!
interface FastEthernet0/0
 no ip address
 no shutdown
 duplex auto
 speed auto
 ipv6 address 2001:DB8:ACAD:1::1/68
 ipv6 ospf 1 area 0
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 no shutdown
 ipv6 address 2001:DB8:ACAD:1:1000::1/68
 ipv6 ospf 1 area 0
 no fair-queue
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
ipv6 router ospf 1
 router-id 1.1.1.1
```

Router ISP2

```
hostname ISP2
!
ipv6 unicast-routing
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 no shutdown
 duplex auto
 speed auto
 ipv6 address 2001:DB8:ACAD:1:2000::1/68
 ipv6 ospf 1 area 0
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 no shutdown
 ipv6 address 2001:DB8:ACAD:1:1000::2/68
 ipv6 ospf 1 area 0
!
ipv6 router ospf 1
 router-id 2.2.2.2
```

Anhang B

WLAN Konfiguration

```
Dot11 ssid BAC1
Vlan 1
authentication open
Mbssid Guest-mode
!
Dot11 ssid BAC2
Vlan 2
authentication open
Mbssid Guest-mode
!
Int dot11 0/1/0
no shutdown
Mbssid
ssid BAC1
ssid BAC2
!
configure terminal
interface Dot11Radio 0/1/0.1
encapsulation dot1Q 1 native
!
interface Dot11Radio 0/1/0.2
encapsulation dot1Q 2 native
```

Anhang C

Mobile Router

```
hostname Mobile
!
ipv6 unicast-routing
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:ACAD:1:3000::2/68
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
```