



สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

ความน่าเชื่อถือได้ของโฮมเอเจนต์ระหว่างการย้ายข้ามเครือข่ายของการ  
เคลื่อนที่บนไอพีเวอร์ชันหก

HOME AGENT RELIABILITY DURING HANDOVER OF MOBILE IPv6



อดิศักดิ์ บุชรานันท์  
ADISAK BUSARANUN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต  
สาขาวิชาวิศวกรรมสารสนเทศ  
บัณฑิตวิทยาลัย  
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง  
พ.ศ.2549

ISBN 974-15-2813-2

**HOME AGENT RELIABILITY DURING HANDOVER OF MOBILE IPv6**

**ADISAK BUSARANUN**

**A THESIS SUBMITTED IN PARTIAL FULFILLMENT  
OF THE REQUIREMENT FOR THE DEGREE OF  
MASTER OF ENGINEERING IN INFORMATION ENGINEERING  
SCHOOL OF GRADUATE STUDIES  
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG**

**2006**

**ISBN 974-15-2813-2**

**COPYRIGHT 2006**

**SCHOOL OF GRADUATE STUDIES**

**KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG**

หัวข้อวิทยานิพนธ์	ความน่าเชื่อถือได้ของโสมเอเงินท์ระหว่างการย้ายข้ามเครือข่ายของการเคลื่อนที่บนไอพีเวอร์ชันหก
นักศึกษา	นายอดิศักดิ์ บุษรานั้นท์
รหัสนักศึกษา	47061116
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมสารสนเทศ
พ.ศ.	2549
อาจารย์ผู้ควบคุมวิทยานิพนธ์	ผศ. พิชญ์ สุพรรณกุล
อาจารย์ผู้ควบคุมวิทยานิพนธ์ร่วม	ดร. พนิดา พงษ์ไพบูลย์

#### บทคัดย่อ

ในวิทยานิพนธ์นี้ ได้ทำการศึกษาการทำงานของการทำงานของการย้ายข้ามเครือข่ายบนการเคลื่อนที่ของไอพีเวอร์ชันหก (MIPv6) ได้ทดสอบตัวแปรต่าง ๆ ที่มีผลกระทบต่อค่าล่าช้าของเวลาการย้ายข้ามเครือข่ายไอพีเวอร์ชันหก โดยมีจุดมุ่งหมายอยู่ 2 อย่าง อย่างแรกคือปรับปรุงเวลาความล่าช้าในการย้ายข้ามเครือข่าย อย่างที่สองพัฒนาให้โสมเอเงินท์ (HA) ที่ไม่สามารถทำงานได้ ให้ใช้ HA สำรองทำงานแทน ในการทดลองได้ทำบนเครือข่ายพื้นที่เฉพาะแห่งไร้สาย (WLAN) สามเครือข่าย โดยใช้โปรแกรมการเคลื่อนที่ของ IPv6 บนระบบปฏิบัติการลินุกซ์ (MIPL) ซึ่งมีจุดประสงค์เพื่อให้การย้ายข้ามเครือข่ายเป็นไปได้อย่างต่อเนื่องและเพิ่มความน่าเชื่อถือได้ของระบบ

<b>Thesis Title</b>	Home Agent Reliability during Handover of Mobile IPv6
<b>Student</b>	Mr. Adisak Busaranun
<b>Student ID.</b>	47061116
<b>Degree</b>	Master Degree
<b>Program</b>	Information Engineering
<b>Year</b>	2006
<b>Thesis Advisor</b>	Asst. Prof. Pichaya Supanakoon
<b>Thesis Advisor cooperate</b>	Dr. Panita Pongpaibool

### **ABSTRACT**

This thesis studies the handover procedure of mobile IPv6 and investigates various factors affecting the delay during inter-network handover. The goals are two folds. First is to improve handover delay when a mobile node moves to different networks. Second is to provide reliability to the Mobile IPv6 infrastructure. This is done by setting up a backup Home Agent (HA) to replace the primary HA when the primary HA fails. The experiments are performed on real testbed of 3 wireless local area networks (WLANs) using Mobile IPv6 for Linux (MIPL) implementation.

## กิตติกรรมประกาศ

วิทยานิพนธ์เล่มนี้สำเร็จได้ด้วยความกรุณาของอาจารย์ที่ปรึกษา ผศ. พิชญ์ สุพรรณกุล และอาจารย์ที่ปรึกษาร่วม คร. พนิดา พงษ์ไพบูลย์ ที่ให้ความช่วยเหลือ ให้คำชี้แนะช่วยแก้ปัญหา ตลอดจนให้ความรู้และประสบการณ์ที่ดีแก่ข้าพเจ้า ซึ่งท่านทั้งสองเป็นผู้มีความรู้ที่สูงมากมีเมตตาต่อข้าพเจ้า ข้าพเจ้าขอนับถือมา ณ ที่นี้

ขอขอบพระคุณ อ. สถาพร พรหมวงศ์ และ อ. มนชัย แซ่มซ้อย กรรมการสอบหัวข้อและโครงสร้างวิทยานิพนธ์ที่ได้ให้คำแนะนำ สนับสนุนจนทำให้วิทยานิพนธ์นี้สำเร็จลงได้

ขอขอบคุณสถาบันบัณฑิตวิทยาศาสตร์และเทคโนโลยีไทย (Thailand Graduate Institute of Science and Technology) ที่ให้ทุนสนับสนุนในการศึกษาและวิจัย ขอขอบคุณพี่ๆ ในทีม TGIST ทุกคนที่ให้คำปรึกษาแนะนำ

ขอขอบคุณหัวหน้างาน เพื่อนร่วมงานฝ่ายอินเทอร์เน็ตยุคหน้า ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ที่สนับสนุนประสานงานให้ความร่วมมือในการศึกษาทำการวิจัยในห้องปฏิบัติการนี้สำเร็จลงได้

สุดท้ายต้องขอขอบคุณบิดา มารดา น้องสาวของข้าพเจ้า เมื่อยามท้อแท้ก็ได้ท่านช่วยชี้แนะและเป็นกำลังใจให้กับข้าพเจ้า

สำหรับคุณงามความดีประโยชน์อันใดที่เกิดจากวิทยานิพนธ์นี้ ข้าพเจ้าขอมอบให้กับบุคคลที่ได้กล่าวมาแล้วข้างต้น

อดิศักดิ์ บุษรานันท์

# สารบัญ

	หน้า
บทคัดย่อภาษาไทย.....	I
บทคัดย่อภาษาอังกฤษ.....	II
กิตติกรรมประกาศ.....	III
สารบัญ.....	IV
สารบัญตาราง.....	VII
สารบัญรูป.....	VIII
รายการคำย่อและสัญลักษณ์.....	X
บทที่ 1 บทนำ.....	1
1.1 ความเป็นมาและความสำคัญของปัญหา.....	1
1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา.....	2
1.3 สมมติฐานของการศึกษา.....	2
1.4 ทฤษฎีหรือแนวความคิดที่ใช้ในการวิจัย.....	2
1.5 การเปรียบเทียบวิธีที่นำเสนอกับวิธีการแบบพื้นฐาน.....	3
1.6 ขอบเขตการวิจัย.....	3
1.7 ขั้นตอนของการศึกษา.....	4
บทที่ 2 ทฤษฎี IPv6.....	5
2.1 การใช้งาน IPv6.....	5
2.2 การใช้งานเครือข่าย MIPv6.....	6
2.2.1 ความแตกต่างระหว่าง MIPv4 กับ MIPv6.....	6
2.2.2 MIPv6.....	6
2.2.3 การใช้งานเครือข่าย MIPv6.....	7
2.2.4 องค์ประกอบของข่าวสารที่ใช้แลกเปลี่ยนของ MIPv6.....	8
2.3 การพัฒนาบนระบบปฏิบัติการต่างๆ.....	14
2.3.1 การพัฒนาบนระบบปฏิบัติการลินุกซ์.....	14
2.3.2 การพัฒนาบนระบบปฏิบัติการบีเอสดี.....	14

## สารบัญ (ต่อ)

	หน้า
บทที่ 3 การเพิ่มประสิทธิภาพของการเคลื่อนย้ายข้ามเครือข่าย IPv6.....	15
3.1 การทดลอง MIPv6.....	15
3.2 ตัวแปรที่มีผลกระทบต่อ การเคลื่อนย้ายเครือข่าย.....	16
3.3 ค่าพารามิเตอร์ที่นำมาศึกษา.....	17
3.4 การทดสอบการย้ายข้ามในแต่ละกรณี.....	18
3.5 ผลการทดลองและการวิเคราะห์.....	18
3.5.1 การตรวจจับการเคลื่อนย้ายกับส่วนประกอบของการล่าช้า.....	18
3.5.2 ผลกระทบที่เกิดจากการประกาศค่าเกตเวย์.....	19
3.5.3 ผลกระทบที่เกิดจากค่าการร้องขอของเกตเวย์.....	21
3.5.4 ผลกระทบที่เกิดจากการเช็คการซ้กันของไอพี.....	21
บทที่ 4 การเพิ่มความน่าเชื่อถือได้ของ โฮมเอจิ้นท์ (HA).....	25
4.1 การศึกษาและรวบรวมข้อมูล.....	25
4.1.1 ปัญหาที่ต้องศึกษา.....	25
4.1.2 งานวิจัยอื่นที่เกี่ยวข้อง.....	25
4.1.3 การตรวจสอบสถานะของ HA โดยใช้ทีซีพีแบบสามพันช์ 3 ทาง (TCP 3 way handshake).....	27
4.2 การวิเคราะห์และออกแบบระบบ.....	29
4.3 การสร้างระบบจำลองการทำงาน.....	29
4.4 ทฤษฎีของการสร้างความน่าเชื่อถือได้ของระบบ.....	30
4.5 การหาพารามิเตอร์เพื่อเพิ่มความน่าเชื่อถือ.....	31
4.6 ผลการทดลอง.....	32
4.6.1 โฮมเอจิ้นท์ใช้งานไม่ได้เมื่ออยู่ที่โฮม.....	32
4.6.2 การใช้งานไม่ได้ของโฮมเอจิ้นท์เมื่ออยู่ต่างเครือข่ายและไม่ได้ใช้ การจัดเส้นทางที่ดี.....	33
4.6.3 การใช้งานไม่ได้ของโฮมเอจิ้นท์เมื่ออยู่ต่างเครือข่ายและใช้ การจัดเส้นทางที่ดี.....	33

## สารบัญ (ต่อ)

	หน้า
4.6.4 การวัดช่วงเวลาที่ใช้งานไม่ได้เมื่ออยู่นอกเครือข่ายบ้าน.....	34
บทที่ 5 สรุปผลการวิจัย และข้อเสนอแนะ.....	38
เอกสารอ้างอิง.....	40
ภาคผนวก ก. โปรแกรมที่ใช้ในการเคลื่อนที่ MIPv6.....	41
ภาคผนวก ข. บทความวิจัยที่ได้รับการตีพิมพ์ในวิทยานิพนธ์.....	49
ประวัติผู้เขียน.....	59

## สารบัญตาราง

ตารางที่	หน้า
3.1 พารามิเตอร์ที่นำมาศึกษา.....	17
3.2 การเชื่อมต่อกรณีที่ 1.....	18
3.3 การเชื่อมต่อกรณีที่ 2.....	19
3.4 การเชื่อมต่อกรณีที่ 3.....	19
3.5 สรุปเวลาในการย้ายข้ามเครือข่ายของ MIPv6 ของกรณีที่ 1 ถึง 3.....	23
4.1 การทดลองการใช้งานไม่ได้ ณ เวลาหนึ่ง.....	31
4.2 สรุปเวลาในการกู้กลับเพื่อใช้งานได้ตามปกติของกรณีที่ 4.....	36

# สารบัญรูป

รูปที่	หน้า
2.1 ขนาดแอดเดรสของ IPv4 และ IPv6.....	5
2.2 การใช้งาน MIPv6 จากการเปลี่ยนเครือข่าย IP .....	7
2.3 รูปแบบข่าวสารของ BU.....	8
2.4 รูปแบบข่าวสารของ BA.....	8
2.5 รูปแบบข่าวสารของ HoTI.....	9
2.6 รูปแบบข่าวสารของ HoT.....	9
2.7 รูปแบบข่าวสารของ CoTI.....	9
2.8 รูปแบบข่าวสารของ CoT.....	10
2.9 การร้องขอเพื่อค้นหาโฮมเอจิ้นท์.....	10
2.10 การตอบกลับเมื่อพบโฮมเอจิ้นท์.....	11
2.11 การจัดเส้นทางแบบติดต่อดังตรง.....	11
2.12 การเคลื่อนย้ายข้ามเครือข่าย MIPv6 แบบโดยรวม.....	12
2.13 กระบวนการแลกเปลี่ยนข้อมูลระหว่าง MIPv6.....	12
2.14 โปรแกรมที่ใช้ใน MIPv6.....	13
3.1 ฟังก์ชันทดลองย้ายข้ามเครือข่ายของ MIPv6.....	15
3.2 การตรวจจับข้อมูลที่แลกเปลี่ยนกันระหว่างการย้ายข้ามเครือข่ายบน MIPv6.....	16
3.3 การเปรียบเทียบการล่าช้าเมื่อย้ายข้ามไปเครือข่ายต่าง ๆ เมื่อกำหนดให้ค่า RtrAdvinterval เป็น (0.03,0.07) วินาที.....	20
3.4 การแปรผันระหว่างการตรวจจับการเคลื่อนย้ายและค่าการประกาศเกตเวย์ (3,10) .....	21
3.5 การแปรผันระหว่างการตรวจจับการเคลื่อนย้ายและค่าการประกาศเกตเวย์ (0.1,0.5).....	21
3.6 การเปรียบเทียบความเร็วในการย้ายข้ามเครือข่ายเมื่อปรับค่าการประกาศเกตเวย์ .....	22
3.7 การเช็คว่าเวลาที่ผ่านไปได้มากที่สุดในการย้ายข้ามเครือข่าย.....	23
4.1 การติดต่อบน HAHA.....	26
4.2 การติดต่อบน VHAR.....	26
4.3 ขั้นตอนในการสร้าง TCP ทำการติดต่อ.....	27
4.4 ฟังก์ชันทดลองการเคลื่อนที่ของ IPv6.....	29
4.5 ฟังก์ชันการทำงานของ HA1 และ HA2.....	30

## สารบัญรูป (ต่อ)

รูปที่	หน้า
4.6 การทำงานของการตรวจวัดสถานะของ HA .....	32
4.7 สถานะ MN สนนทากับ CN ที่เครือข่ายบ้าน.....	33
4.8 สถานะ MN สนนทากับ CN ที่เครือข่ายอื่นและไม่ได้ใช้การจัดเส้นทางที่ดี.....	33
4.9 สถานะ MN สนนทากับ CN ที่เครือข่ายอื่นและใช้การจัดเส้นทางที่ดี.....	34
4.10 เปรียบเทียบการใช้งานไม่ได้ของระบบกับค่าเวลาคงอยู่ของ CN.....	35
4.11 การเปรียบเทียบค่าเวลาคงอยู่ของ CN เทียบกับค่าเวลาการกู้กลับของ HA.....	36
4.12 เวลาการกู้กลับของ HA ในแต่ละกรณี.....	36

## รายการคำย่อและสัญลักษณ์

ไอพี (Internet Protocol)	IP
ทีซีพี (Transmission Control Protocol)	TCP
ยูดีพี (User Datagram Protocol)	UDP
ไอซีเอ็มพี (Internet Control Message Protocol)	ICMP
ไอพีเวอร์ชันสี่ (Internet Protocol Version 4)	IPv4
ไอพีเวอร์ชันหก (Internet Protocol Version 6)	IPv6
การเคลื่อนที่ของ IPv6 (Mobile Internet Protocol Version 6)	MIPv6
โนดเคลื่อนที่ (Mobile Node)	MN
โนดคู่สนทนา (Corresponding Node)	CN
โฮมเอเจนต์ (Home Agent)	HA
โฮมแอดเดรส (Home Address)	HoA
แอดเดรสที่เครือข่ายใหม่ (Care-of Address)	CoA
ฟอเรนทเอเจนต์ (Foreign Agent)	FA
แอสเซสพ้อย (Access Point)	AP
เครือข่ายพื้นที่เฉพาะแห่งไร้สาย (Wires LAN)	WLAN
โปรแกรม MIPv6 บนระบบปฏิบัติการลินุกซ์ (Mobile Internet Protocol for Linux)	MIPL
ผลรวมของการล่าช้าของการย้ายข้ามเครือข่าย (Time Total)	TH
เวลาตรวจจับการเคลื่อนย้าย (Time Detection)	TD
เวลาการติดตั้งแอดเดรส (Time Configuration)	TC
เวลาการลงทะเบียนการติดต่อ (Time Registrations)	TR
เวลาการจัดเส้นทางที่เหมาะสมที่สุด (Time Optimization)	TO
เวลาในการใช้งานไม่ได้ (Time Down)	Tdown
เวลาตรวจพบ HA1 ใช้งานไม่ได้ (Time Detect)	Tdetect
เวลาการกู้กลับของระบบ (Time Restore)	Trestore
เวลาการกู้กลับของ HA (Time Recovery)	Trecovery
คณะทำงานกลุ่มวิศวกรอินเทอร์เน็ต (Internet Engineer Task Force)	IETF
ข่าวสารการปรับปรุงการติดต่อ (Binding Update)	BU
ข่าวสารแจ้งว่าได้รับการติดต่อ (Binding Acknowledgement)	BA
ข่าวสารเริ่มต้นทดสอบเครือข่ายบ้าน (Home Test Init)	HoTI

## รายการคำย่อและสัญลักษณ์ (ต่อ)

ข่าวสารสิ้นสุดทดสอบเครือข่ายบ้าน (Home Test)	HoT
ข่าวสารเริ่มต้นทดสอบการดูแล (Care-of Test Init)	CoTI
ข่าวสารสิ้นสุดทดสอบการดูแล (Care-of Test)	CoT
ข่าวสารการขอรับข้อมูลใหม่ (Binding Refresh Request)	BRR
ข่าวสารผิดพลาด (Binding Error)	BER
การร้องขอเพื่อค้นหาโฮมเอเจนต์ (Home Agent Address Discovery Request)	HADRq
การตอบกลับเมื่อพบโฮมเอเจนต์ (Home Agent Address Discovery Reply)	HADRp
การเช็คการซ้ำกันของ IP (Duplicate Address Detection)	DAD
รายการ (HA Home Agent List)	HAL
การร้องขอ (Synchronies)	SYN
การรอการตอบรับ (Synchronies/Acknowledge)	SYN/ACK
การตอบรับ (Acknowledge)	ACK
การที่ลูกข่ายเรียกขอไอพีจากเกตเวย์ (Router Solicitations)	RS
เกตเวย์ประกาศให้กับลูกข่าย (Router Advertisement)	RA
นาที (Minute)	m
วินาที (Second)	s
เวลา (Time)	t

งานจริงกับสภาวะแวดล้อมที่ใช้ในเครือข่ายไร้สาย ซึ่งมีจุดประสงค์เพื่อให้การย้ายข้ามเครือข่ายเป็นไปได้อย่างต่อเนื่องและเพิ่มความน่าเชื่อถือได้ของระบบ

## 1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

วัตถุประสงค์ของวิทยานิพนธ์ฉบับนี้ คือ ศึกษา การเคลื่อนที่ของ MIPv6 ศึกษาวิธีการย้ายข้ามเครือข่ายของ MIPv6 ศึกษาผลกระทบต่อเครือข่ายข้ามเครือข่ายของ MIPv6 หลังจากนั้น จะนำข้อมูลที่ได้จากการศึกษาทั้งหมดนี้มาวิเคราะห์และเพิ่มความน่าเชื่อถือให้กับ MIPv6

## 1.3 สมมติฐานของการศึกษา

ในการใช้งาน MIPv6 จะเกิดการขัดจังหวะขึ้นเมื่อทำการเปลี่ยนที่อยู่ไปอยู่เครือข่ายใหม่ทำให้มีการเกิดช่วงเวลาที่ใช้งานไม่ได้ขึ้น เป็นผลทำให้ขาดการติดต่อในช่วงเวลาหนึ่งซึ่งวิทยานิพนธ์ฉบับนี้ได้ตั้งสมมุติของการล่าช้ามา 3 กรณี กรณีแรกคือใช้ค่าเดิมของ โปรแกรมเพื่อเป็นฐานในการวิเคราะห์ กรณีที่สองคือได้ทำการปรับลดการร้องขอของเกตเวย์จาก MN กรณีที่สามคือทำการลดการตรวจสอบที่ซ้ำซ้อนของ IP เพื่อไม่ให้เกิดการล่าช้าในการจัดการคอนฟิก ส่วนการวิจัยเพื่อเพิ่มความน่าเชื่อถือให้กับระบบเมื่อเกิดการใช้งานไม่ได้ โดยกำหนดให้มี HA หลักและ HA สำรอง เมื่อ HA หลักใช้งานไม่ได้ HA สำรองจะเข้ามาปฏิบัติหน้าที่แทน HA หลักโดยอัตโนมัติแล้วเมื่อ HA กลับมาพร้อมใช้งานได้ก็จะกลายมาทำหน้าที่เป็น HA สำรองแทน ขั้นตอนนี้จะสลับไปเรื่อยๆ เมื่อ HA ตัวใดตัวหนึ่งตาย

## 1.4 ทฤษฎีหรือแนวความคิดที่ใช้ในการวิจัย

ความล่าช้าของการย้ายข้ามเครือข่ายเป็นสาเหตุหนึ่งที่ทำให้การติดต่อสื่อสารเกิดการติดขัดขาดความราบรื่น จึงจำเป็นต้องหาวิธีเพื่อลดการล่าช้าของการย้ายข้ามเครือข่ายให้เสมือนว่าไม่เกิดอะไรขึ้นในการย้ายข้ามครือข่ายนั้น ซึ่งจะต้องมีการทำให้การย้ายไปแต่ละเครือข่ายมีค่าตัวแปรที่ดีที่สุดเพื่อนำมาใช้และลดความล่าช้าทั้งยังเพิ่มความน่าเชื่อถือให้รองรับกับระบบ โดยเมื่อมีการย้ายข้ามเครือข่ายแล้วเกิดมี HA [2], [3], [4] ตัวใดตัวหนึ่งใช้งานไม่ได้

หน้าที่หลักของ HA คือจัดการให้มีการย้ายไปเครือข่ายต่างๆ ได้อย่างราบรื่นและสำเร็จ ถ้าเกิดเหตุการณ์ที่ HA ใช้งานไม่ได้ขึ้นจะทำให้การย้ายข้ามไปยังเครือข่ายอื่นไม่สำเร็จ การจดจำ IP เดิมไม่สามารถทำได้ทำให้การเชื่อมต่อถูกตัดขาด จึงมีการสร้าง HA สำรองอีกตัวเพื่อทดแทน HA หลัก เมื่อ HA หลักเมื่อไม่สามารถทำงานได้ HA สำรองจะทำงานแทน โดยอัตโนมัติ ซึ่งจะมีค่าของการรับประกันการใช้งานไม่ได้เพื่อสร้างความน่าเชื่อถือได้ให้กับระบบ

ได้นำเสนอการตรวจสอบที่ทำการวัดอย่างละเอียดเพื่อหาประสิทธิภาพที่ดีที่สุดที่สามารถนำมาใช้ลดการล่าช้าของการย้ายข้ามเครือข่าย โดยนำค่าเวลาที่ตรวจจับได้ในหน่วยไมโครวินาทีมาคำนวณซึ่งทำให้ได้เวลาแต่ละช่วงที่มีความเที่ยงตรงสูง แล้วนำเวลาแต่ละช่วงมารวมกันเพื่อหาค่าการล่าช้าทั้งหมดของการย้ายข้ามเครือข่าย

การใช้ HA หลายตัวเป็นวิธีของการสร้าง HA เสมือน โดยแต่ละตัวจะมีหน้าที่ในการทำงานเพื่อรองรับการใช้งานไม่ได้ของแต่ละตัว โดยจะต้องมี HA อย่างน้อยที่สุด 3 ตัว คือมี HA หลัก HA สำรอง และ HA รอการทำงาน ซึ่งในวิทยานิพนธ์นี้จะทำการออกแบบระบบที่ทำให้มีจำนวนของ HA ที่จำเป็นต้องใช้ลดลง โดยใช้แค่ HA หลักกับ HA สำรอง 2 ตัวเท่านั้น

## 1.5 เปรียบเทียบวิธีนำเสนอกับวิธีการแบบพื้นฐาน

วิธีสำหรับการลดความล่าช้าของระบบ MIPv6 มีอยู่หลายวิธีด้วยกัน เช่น ใช้การจับข้อความที่เริ่มส่งจนถึงข้อความที่ตอบรับ และใช้การ PING เพื่อวัดและวิเคราะห์ผล [5], [6], [7] แต่จะได้ความละเอียดแค่ช่วงของการ PING ในแต่ละ 1 วินาที ซึ่งเป็นช่วงเวลาที่มีความละเอียดไม่เพียงพอ ทำให้ไม่สามารถทราบช่วงเวลาที่ใช้ส่งข้อความระหว่าง MN CN และ HA ที่เที่ยงตรง ซึ่งในวิทยานิพนธ์ฉบับนี้ได้ใช้วิธีตรวจจับข้อมูล [8] ที่มีการจับในแต่ละช่วงเวลาของการส่งข้อความ โดยมีความละเอียดในหน่วย 1/1000000 วินาที ทำให้ทราบเวลาที่ถูกต้องที่เที่ยงตรงมากขึ้น ถึงแม้ว่าได้มีการวัดประสิทธิภาพของระบบ MIPv6 แต่ก็ไม่ได้มีการพิจารณาค่าการจัดการเส้นทางที่ดีที่สุดดังนั้น ในวิทยานิพนธ์นี้จึงได้ทำการพิจารณาหาเวลาตรวจจับการเคลื่อนย้าย (TD) เวลาการติดตั้งแอดเดรส (TC) เวลาการลงทะเบียนการติดต่อ (TR) และเวลาการจัดการเส้นทางที่เหมาะสมที่สุด (TO)

งานอีกส่วนศึกษาการเพิ่มความน่าเชื่อถือได้ของระบบ MIPv6 ซึ่งเมื่อเกิด HA ตัวหลักไม่สามารถทำงานได้จะมีตัวสำรองเข้ามาทำหน้าที่แทนแล้วสามารถสลับการทำงานกันได้

## 1.6 ขอบเขตการวิจัย

ศึกษาวิธีการย้ายข้ามเครือข่ายของระบบ MIPv6 โดยทำการวัดช่วงเวลาในแต่ละช่วงที่ใช้ในการส่งข้อมูลสำหรับติดต่อสื่อสารกัน หลังจากนั้นนำช่วงเวลาในแต่ละช่วงที่วัดได้มาวิเคราะห์หาเหตุของความล่าช้าในการย้ายข้ามเครือข่าย

ศึกษาถึงผลกระทบของตัวแปรที่เกิดจากการปรับเปลี่ยนค่าตามความเหมาะสมของเครือข่ายเพื่อให้เกิดประสิทธิภาพที่ดีที่สุด

ออกแบบสร้างระบบ MIPv6 ที่มีความน่าเชื่อถือได้ของระบบเพิ่มขึ้น เมื่อเกิดเหตุการณ์ที่ HA ใช้งานไม่ได้

## 1.7 ขั้นตอนของการศึกษา

วิทยานิพนธ์ฉบับนี้ได้แบ่งเนื้อหาออกเป็น 6 บทด้วยกันคือ

บทที่ 1 กล่าวถึงบทนำ ซึ่งประกอบไปด้วยความเป็นมาและความสำคัญของปัญหา ความมุ่งหมายและวัตถุประสงค์ของการศึกษา สมมุติฐานของการศึกษา ทฤษฎีหรือแนวคิดที่ใช้ในการวิจัย เปรียบเทียบกับงานวิจัยอื่น ขอบเขตการวิจัย และขั้นตอนการศึกษา

บทที่ 2 กล่าวถึงทฤษฎี IPv6 ซึ่งประกอบไปด้วยการใช้งาน IPv6 การใช้งานเครือข่าย MIPv6 และการพัฒนาระบบปฏิบัติการต่าง ๆ

บทที่ 3 กล่าวถึงการศึกษาประสิทธิภาพของการเคลื่อนย้ายเครือข่ายเคลื่อนที่ ซึ่งประกอบไปด้วย MIPv6 ตัวแปรที่มีผลกระทบต่อ การเคลื่อนย้ายเครือข่าย ค่าพารามิเตอร์ที่นำมาศึกษา การทดสอบการย้ายข้ามเครือข่ายในแต่ละกรณี และผลการทดลองและวิเคราะห์

บทที่ 4 กล่าวถึงการศึกษาความน่าเชื่อถือได้ของ HA ซึ่งประกอบไปด้วยการศึกษาและรวบรวมข้อมูล การวิเคราะห์และออกแบบระบบ การสร้างระบบจำลองการทำงาน ทฤษฎีของการสร้างความน่าเชื่อถือได้ของระบบ การหาประสิทธิภาพของพารามิเตอร์เพื่อเพิ่มความน่าเชื่อถือ และผลการทดลอง

บทที่ 5 เป็นสรุปผลการวิจัย และข้อเสนอแนะ

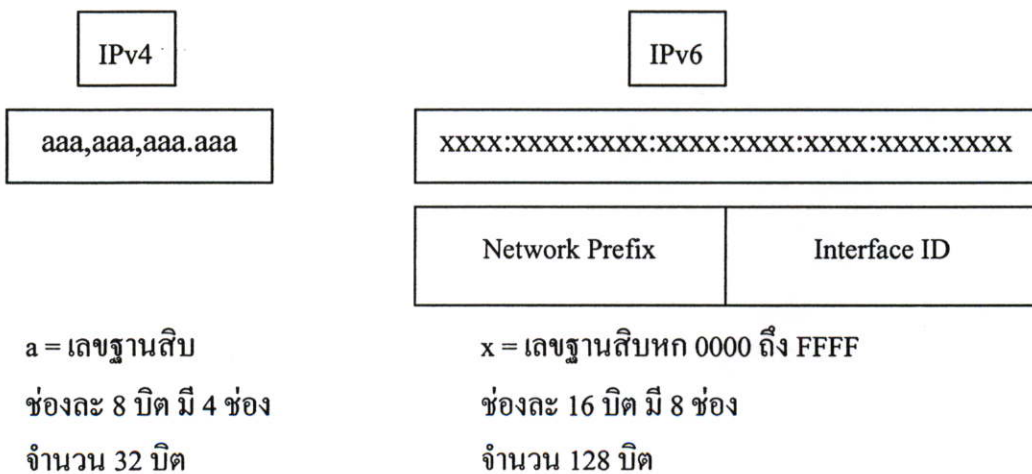
## บทที่ 2

# ทฤษฎี IPv6

ทฤษฎีของ MIPv6 อาศัยการอ้างอิงจาก RFC 3775 [1] เพื่อเป็นแนวทางในการดำเนินการวิจัย และยังมีงานวิจัยอื่นที่ทำการวิจัยเรื่องเกี่ยวกับการย้ายข้ามเครือข่ายเหมือนกันแต่จะมีวิธีแตกต่างกันไป ในวิทยานิพนธ์ฉบับนี้ได้มีวิธีและแนวคิดดังจะกล่าวต่อไปนี้

### 2.1 การใช้งาน IPv6

ทุกวันนี้ใช้หมายเลข IP แอดเดรสบนมาตรฐานของ IPv4 ซึ่งเป็นมาตรฐานในการส่งข้อมูลในเครือข่ายอินเทอร์เน็ตตั้งแต่ปี ค.ศ. 1981 [9], [10] ทั้งนี้การขยายตัวของอินเทอร์เน็ตในช่วงที่ผ่านมาเมื่ออัตราการเติบโตที่รวดเร็ว หมายเลข IP แอดเดรสที่ใช้ในปัจจุบันกำลังถูกใช้หมดไป ไม่เพียงพอต่อความต้องการในอนาคต จนคาดคะเนกันว่าหมายเลข IP แอดเดรสของ IPv4 จะไม่เพียงพอต่อความต้องการในปี ค.ศ. 2010 ซึ่งหากเกิดขึ้นจะทำให้ไม่สามารถเชื่อมต่ออุปกรณ์เครือข่ายเข้ากับอินเทอร์เน็ตเพิ่มได้อีก คณะทำงานกลุ่มวิศวกรรมอินเทอร์เน็ต (IETF) ตระหนักถึงปัญหาสำคัญดังกล่าวจึงได้พัฒนา IP รุ่นใหม่ขึ้นมาคือ IPv6 เพื่อทดแทน IP รุ่นเดิม มีการปรับปรุงประสิทธิภาพหลาย ๆ ประการเพื่อรองรับกับการประยุกต์ใช้งานใหม่ ๆ ที่จะเกิดขึ้นในอนาคต และเพิ่มประสิทธิภาพในการประมวลผลแพ็กเก็ตให้ดีขึ้น ทำให้ตอบสนองต่อการขยายตัวและความต้องการใช้งานเทคโนโลยีบนเครือข่ายอินเทอร์เน็ตในอนาคตได้อย่างดี



รูปที่ 2.1 ขนาดแอดเดรสของ IPv4 และ IPv6

จากรูปที่ 2.1 แสดงขนาดแอดเดรสของ IPv4 และ IPv6 ซึ่งจะเห็นได้ว่า IPv6 มีแอดเดรสเพิ่มขึ้นเป็น 128 บิต ทำให้มีจำนวนแอดเดรสจำนวนมากถึง  $3.4 \times 10^{38}$  หมายเลข (340,282,366,920,938,463,463,374,607,431,768,211,456) IPv4 มีประมาณ 4 พันล้าน IP ซึ่งหมายความว่าในอนาคตอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ จะมีหมายเลข IP แอดเดรสเป็นของตัวเอง เช่น เครื่องใช้ไฟฟ้าในครัวเรือน ตู้เย็น โทรทัศน์ เครื่องปรับอากาศ ซึ่งสามารถส่งงานเครื่องใช้ไฟฟ้าเหล่านี้ผ่านอินเทอร์เน็ตได้ มีการคำนวณไว้ว่า IPv6 จะทำให้มีจำนวนแอดเดรสได้หลายพันหมายเลขสำหรับทุก ๆ พื้นที่หนึ่งตารางเมตรของพื้นผิวโลก

ตัวอย่างหมายเลข IPv6 มีลักษณะประกอบไปด้วย กลุ่มตัวเลข 8 กลุ่มเขียนคั่นกันด้วยเครื่องหมาย : โดยแต่ละกลุ่มคือเลขฐาน 16 จำนวน 4 ตัว (16 บิต) เช่น

3FFE:085B:1F1F:0000:0000:00A9:1234

เขียนย่อได้คือ

3FFE:85B:1F1F::A9:1234

ทั้งนี้ก็มีเงื่อนไขในการเขียนรูปแบบย่อคือ หากมีเลขศูนย์ด้านหน้าของกลุ่มใดสามารถละไว้ได้ ทำติดกันได้เพียงครั้งเดียว ถ้ามี 0 เพิ่มมาอีกจะละไว้ไม่ได้เพื่อไม่ให้เกิดความสับสน เช่น 3FFE:085B:0000:0000:1FFF:0000:0000:1234 เขียนย่อได้เป็น 3FFE:85B:0000:0000:1FFF::1234

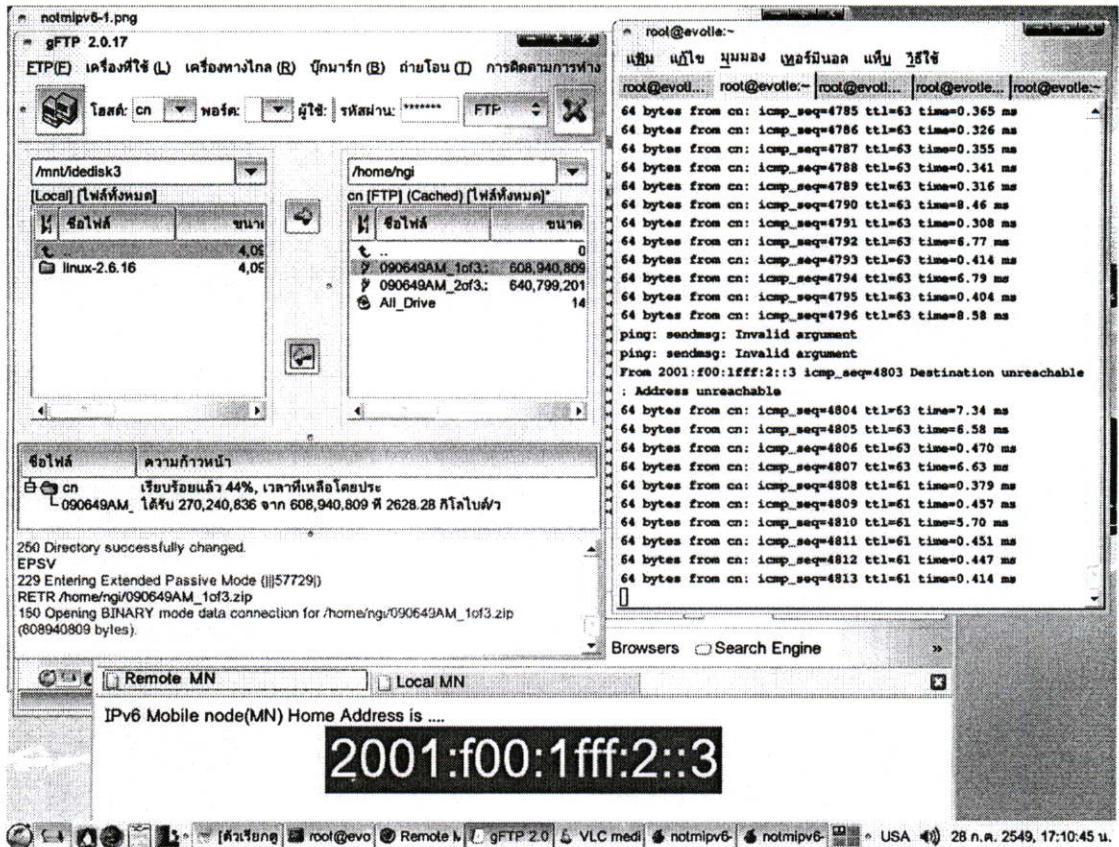
## 2.2 การใช้งานเครือข่าย MIPv6

### 2.2.1 ความแตกต่างระหว่าง MIPv4 กับ MIPv6

MIPv4 จะใช้ตัวพอร์เรนท์เอเจนต์ (Foreign Agent : FA) ควบคู่กับ HA ในระหว่างการย้ายข้ามเครือข่าย ไม่มีการทำการจัดเส้นทางที่ดี (Route Optimization) และไม่สนับสนุนการทำการตรวจสอบตัวตนเพื่อเพิ่มความปลอดภัยในระหว่างการย้าย

### 2.2.2 MIPv6

MIPv6 คือ การใช้งานอินเทอร์เน็ตแบบเคลื่อนที่บนเครือข่าย IPv6 โดยปกติคอมพิวเตอร์พกพาหรือโน้ตบุคสามารถใช้งานตามที่ตั้งต่าง ๆ คล้ายกับการใช้งานโทรศัพท์เคลื่อนที่เพียงแต่คอมพิวเตอร์จะใช้ IP แอดเดรสแทนหมายเลขโทรศัพท์ การกำหนด IP แอดเดรสให้กับเครื่องคอมพิวเตอร์จะเหมือนกับหมายเลขโทรศัพท์เวลาย้ายเครือข่าย มาตรฐาน MIPv6 จึงถูกกำหนดขึ้นมาโดยให้เครื่องคอมพิวเตอร์มี IP แอดเดรสสองชุด ชุดแรกเป็น HoA ชุดที่สองเป็น CoA จากนั้นทุกการติดต่อกับ HoA ก็จะถูกส่งต่อโดยตัวกลางหรือ HA มายัง CoA โดยมีการสะดุดเพียงช่วงเวลาหนึ่งแล้วยังสามารถติดต่อกันได้อย่างต่อเนื่อง คือทั้งผู้รับและผู้ส่งไม่ต้องเปลี่ยนแปลง IP แอดเดรสใด ๆ ด้วยตนเอง การทำงานของ MIPv6 ได้แสดงไว้ในรูปที่ 2.2



รูปที่ 2.2 การใช้งาน MIPv6 จากการเปลี่ยนเครือข่าย IP

จากรูปที่ 2.2 เป็นการใช้โปรแกรมการรับส่งไฟล์เมื่อ MN สนทนากับ CN ด้วยซึ่ง CN จะทำการจดจำ IP-HoA ตลอดการติดต่อ ถ้า MN ได้ทำการย้ายข้ามเครือข่ายไปอีกเครือข่ายทาง ซึ่งเมื่อย้ายไปแล้วจะได้รับ IP-CoA ทำให้ CN ที่ทำการสนทนากับ MN ด้วย เกิดการหลุดการติดต่อช่วงที่ เกิดข้อความ “Destination unreachable” ไม่สามารถติดต่อกับ MN ได้ต้องทำการเชื่อมการติดต่อใหม่ แต่ถ้าสนับสนุน MIPv6 จะรอประมาณช่วงเวลานึงจึงสามารถใช้งานได้

### 2.2.3 การใช้งานเครือข่าย MIPv6

องค์ประกอบของ MIPv6 ประกอบไปด้วย

MN โหนดที่ติดต่อสื่อสารกับ CN โดยใช้ หมายเลข IP เดิมที่ MN ใช้อยู่ที่เครือข่ายเดิมและจะใช้ หมายเลข IP เดิมนี้ ในการสื่อสารตลอดระยะทางที่ MN ได้เคลื่อนย้ายไป

CN โหนดที่ติดต่อสื่อสารกับ MN โดยติดต่อจากหมายเลข IP เดิมของ MN ก่อนย้ายและหลังย้ายเครือข่ายไปเรื่อยๆ

HA แลกเปลี่ยนการติดต่อระหว่าง MN และ CN ระหว่างทำการย้ายเครือข่าย

เครือข่ายบ้าน เป็นเครือข่ายเดิมที่ MN ยังไม่เคยเคลื่อนย้าย

HoA ไอพีที่ MN ใช้ติดต่อกับ CN เมื่ออยู่เครือข่ายเดิม

เครือข่ายใหม่ เป็นเครือข่ายที่ MN ได้เคลื่อนย้ายไปอยู่

CoA ไอพีที่ได้รับมาจากเครือข่ายใหม่เมื่อ MN ได้ย้ายไปเครือข่ายใหม่นั้นๆ

**Return Routability** เป็นการเริ่มต้นแลกเปลี่ยนข่าวสารเพื่อทำการจัดเส้นทางที่เหมาะสม

**Route Optimization** การติดต่อสื่อสารกันแบบเส้นทางที่เหมาะสม

**L2 Handover** เป็นการย้ายข้ามจากเครือข่ายที่หนึ่งไปเครือข่ายอื่น ในระดับชั้นที่ 2 (Layer2) เช่น การย้ายข้ามจากแอสเสสพ้อย (AP) ที่ 1 ไปแอสเสสพ้อย (AP) ที่ 2

**L3 Handover** เป็นการย้ายข้ามจากเครือข่ายที่หนึ่งไปเครือข่ายอื่น ในระดับชั้นที่ 3 (Layer3) เช่น การได้รับ IP จาก AP1 มาเป็น IP จาก AP2

#### 2.2.4 องค์ประกอบของข่าวสารที่ใช้แลกเปลี่ยนของ MIPv6

องค์ประกอบของข่าวสารที่ใช้แลกเปลี่ยนของ MIPv6 ประกอบไปด้วย

ข่าวสารการปรับปรุงการติดต่อ (BU) MN ใช้ออกให้ HA ได้รับทราบว่าได้มีการย้ายไปเครือข่ายใหม่ดังรูปที่ 2.3

- \* Source Address = care-of address
- \* Destination Address = correspondent
- \* Parameters:
  - + home address

#### รูปที่ 2.3 รูปแบบข่าวสารของ BU

ข่าวสารแจ้งว่าได้รับการติดต่อ (BA) เมื่อ HA รับทราบจะตอบกลับด้วย BA ดังรูปที่ 2.4

- \* Source Address = correspondent
- \* Destination Address = care-of address
- \* Parameters:
  - + sequence number

#### รูปที่ 2.4 รูปแบบข่าวสารของ BA

ข่าวสารเริ่มต้นทดสอบเครือข่ายบ้าน (HoTI) ส่งข้อมูลแลกเปลี่ยนผ่านต่อของ HA เพื่อคุยสื่อสารกันแบบสามเหลี่ยมจาก MN ไปหา CN ดังรูปที่ 2.5

- \* Source Address = home address
- \* Destination Address = correspondent
- \* Parameters:
  - + home init cookie

### รูปที่ 2.5 รูปแบบข่าวสารของ HoTI

ข่าวสารสิ้นสุดทดสอบเครือข่ายบ้าน (HoT) ตอบกลับการคุยแบบสามเหลี่ยมเพื่อเริ่มการสื่อสารแบบการจัดเส้นทางที่เหมาะสมดังรูปที่ 2.6

- \* Source Address = correspondent
- \* Destination Address = home address
- \* Parameters:
  - + home init cookie
  - + home keygen token
  - + home nonce index

### รูปที่ 2.6 รูปแบบข่าวสารของ HoT

ข่าวสารเริ่มต้นทดสอบการดูแล (CoTI) ส่งข้อมูลเพื่อเริ่มการสื่อสารแบบการจัดเส้นทางที่เหมาะสมดังรูปที่ 2.7

- \* Source Address = care-of address
- \* Destination Address = correspondent
- \* Parameters:
  - + care-of init cookie

### รูปที่ 2.7 รูปแบบข่าวสารของ CoTI

ข่าวสารสิ้นสุดทดสอบการดูแล (CoT) ตอบกลับการส่งข้อมูลเพื่อรับทราบการจัดเส้นทางที่เหมาะสมดังรูปที่ 2.8

<ul style="list-style-type: none"> <li>* Source Address = correspondent</li> <li>* Destination Address = care-of address</li> <li>* Parameters: <ul style="list-style-type: none"> <li>+ care-of init cookie</li> <li>+ care-of keygen token</li> <li>+ care-of nonce index</li> </ul> </li> </ul>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

รูปที่ 2.8 รูปแบบข่าวสารของ CoT

ข่าวสารการขอรับข้อมูลใหม่ (BRR) เป็นการนับเวลาเพื่อขอรับข้อมูลใหม่โดย CN จะทำการส่งไปขอกับ MN

ข่าวสารผิดพลาด (BER) เป็นการส่งข้อมูลผิดพลาดของ CN ไปหา HoA ของ MN ไม่ได้ การร้องขอเพื่อค้นหาโฮมเอจেন্ট (HADRq) เป็นการร้องขอเพื่อค้นหา HA ของ MN ดังรูปที่ 2.9

Type	Code	Checksum
Identifier		Reserved

รูปที่ 2.9 การร้องขอเพื่อค้นหาโฮมเอจেন্ট

การตอบกลับเมื่อพบโฮมเอจেন্ট (HADRp) เป็นการได้รับข้อมูลว่ามี HA อยู่ในเครือข่ายเดียวกัน และ MN เก็บเป็นข้อมูลในการใช้งาน HA ไว้ใน HAL ดังรูปที่ 2.10

Type	Code	Checksum	
Identifier		M	O
Reserved			
Option ....			

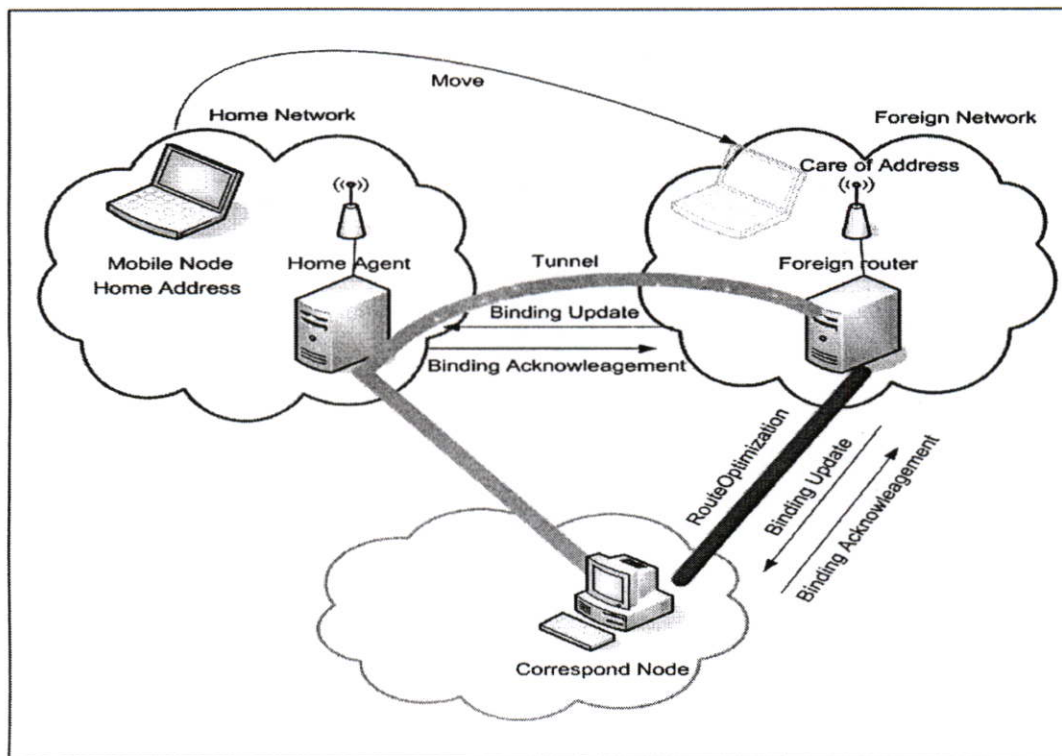
### รูปที่ 2.10 การตอบกลับเมื่อพบ โฮมเอจันท์

การจัดเส้นทางติดต่อแบบโดยตรง (Type 2 Routing Header) เป็นการติดต่อสื่อสารกันโดยตรงจากเครือข่ายใหม่อาศัย IP ใหม่เป็นเส้นทางโดยมีเฮดเดอร์ที่แนบ IP เก่าทำให้คู่สนทนายังสามารถคุยกับ IP เก่าได้อย่างต่อเนื่องดังรูปที่ 2.11

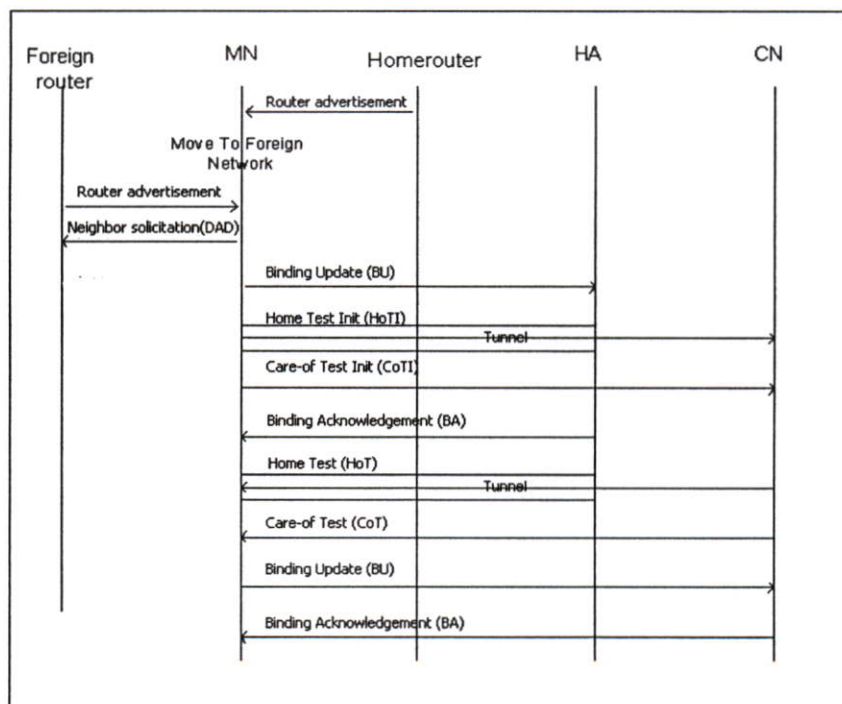
Next Header	Hdr Ext Len=2	Routing Type=2	Segments Left=1
Reserved			
Home Address			

### รูปที่ 2.11 การจัดเส้นทางแบบติดต่อโดยตรง

MIPv6 ได้จัดการการเคลื่อนที่ของ MN โดยระบุแต่ละ MN ด้วย HoA ที่คงที่ โดยไม่ต้องคำนึงถึงว่าจะอยู่ที่เครือข่ายไหนในอินเทอร์เน็ต เครือข่ายดั้งเดิมที่ MN เคยอยู่เรียกว่า *เครือข่ายบ้าน* เมื่อ MN ได้เคลื่อนที่ออกจากเครือข่ายบ้านไปยังเครือข่ายอื่น MN จะต้องส่งข่าวสารเกี่ยวกับตำแหน่งใหม่และ IP แอดเดรสใหม่ไปยัง HA ในเครือข่ายบ้าน เครือข่ายบ้านจะสามารถแปลความหมายและส่งต่อข้อมูลไปยัง MN ที่ตำแหน่งใหม่ได้ แอดเดรสใหม่ของ MN ที่ *เครือข่ายใหม่* เรียกว่า CoA ดังรูปที่ 2.12



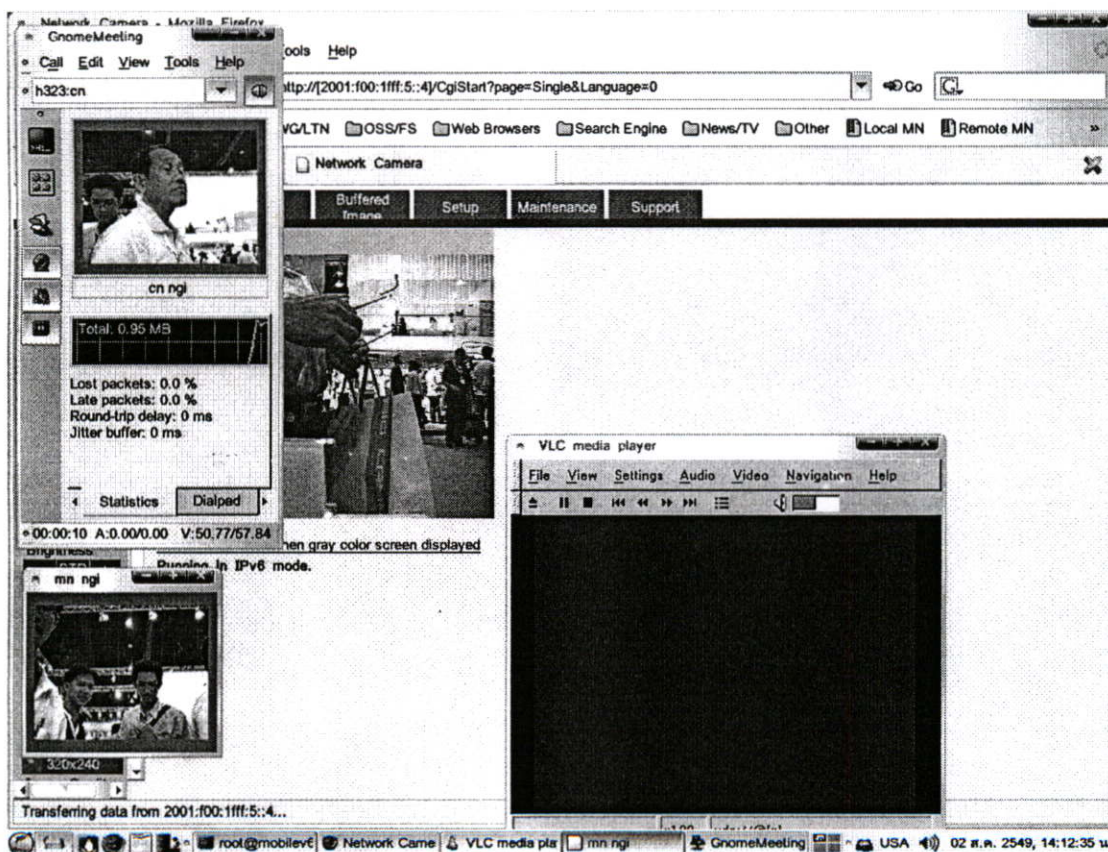
รูปที่ 2.12 การเคลื่อนย้ายข้ามเครือข่าย MIPv6 แบบ โดยรวม



รูปที่ 2.13 กระบวนการแลกเปลี่ยนข้อมูลระหว่าง MIPv6

กระบวนการการทำสัญญา ระหว่าง MIPv6 ได้แสดงไว้ในรูปที่ 2.13 หลังจาก MN ได้ย้ายไปยังเครือข่ายใหม่ จะมี IP แอดเดรสสองชุด ชุดแรกเป็นเสมือนบ้านมีแอดเดรสเดิมเรียกว่า HoA ชุดที่สองเป็นเสมือนเลขที่ชั่วคราวซึ่งได้มาเวลาย้ายเครือข่ายเรียกว่า CoA เมื่อ MN ส่ง BU ไปยัง HA เพื่อประกาศ CoA ให้เครือข่ายบ้านทราบ HA ตอบรับโดย BA กลับไป เมื่อ CN ต้องการติดต่อกับ MN จะติดต่อผ่าน HA โดยที่ HA จะส่งต่อข้อมูลจาก CN ให้ MN ผ่านท่อของ HA เพื่อส่งข้อมูลต่อไปยัง CN การสร้างเส้นทางแบบสามเหลี่ยมจะทำโดย MN และ CN แลกเปลี่ยนข้อมูลกัน MN จะทำการส่ง HoTI ไปบอกผ่านท่อของ HA และข้อมูลตอบรับของ CN ผ่านท่อของ HA คือ HoT อีก ข้อมูลหนึ่งแลกเปลี่ยนเพื่อให้ CN สนทนาโดยตรงกับ MN โดยไม่ผ่านท่อ HA คือ CoTI และ CoT ภายหลังจากนั้นส่งข้อมูล โดยใช้ BU และ BA เป็นขั้นตอนสุดท้ายที่ MN จะทำการติดต่อโดยตรงกับ CN

โปรแกรมที่นิยมนำมาใช้ใน MIPv6 ได้แก่พวกเผยแพร่ภาพ การส่งข้อมูลแบบกระจายภาพ ไปหลายๆลูกข่ายดังรูปที่ 2.14



รูปที่ 2.14 โปรแกรมที่ใช้ใน MIPv6

## 2.3 การพัฒนาบนระบบปฏิบัติการต่างๆ

ได้มีการพัฒนา MIPv6 บนระบบลินุกซ์ [11] ฟรีบีเอสดี (FreeBSD) [12] วินโดวส์ ซึ่งในวิทยานิพนธ์ฉบับนี้ได้ใช้ MIPL บนระบบลินุกซ์ มาวิเคราะห์และหาผลสรุปเพื่อหาค่าเวลาการย้ายข้ามเครือข่ายที่ดีที่สุด ที่ทำให้ MN และ CN สามารถติดต่อกันได้ดั้งเดิม

### 2.3.1 การพัฒนาบนระบบปฏิบัติการลินุกซ์

ในระบบปฏิบัติการลินุกซ์ได้มีผู้พัฒนาขึ้นมาหลากหลายโปรแกรมขึ้นอยู่กับความถนัดของผู้พัฒนาว่าถนัดกับระบบไหนมากกว่ากันแต่ทั้งนี้ทั้งนั้นก็อ้างอิงตามมาตรฐาน RFC 3775 ซึ่งจะมีเว็บไซต์ที่ทำการพัฒนาบนลินุกซ์ดังต่อไปนี้

- <http://www.mobile-ipv6.org>
- <http://www.linux-ipv6.org>

### 2.3.2 การพัฒนาบนระบบปฏิบัติการบีเอสดี

ในระบบปฏิบัติการบีเอสดีได้มีผู้พัฒนาขึ้นมาหลากหลายโปรแกรมขึ้นอยู่กับความถนัดของผู้พัฒนาว่าถนัดกับระบบไหนมากกว่ากันแต่ทั้งนี้ทั้งนั้นก็อ้างอิงตามมาตรฐาน RFC 3775 ก็จะมีเว็บไซต์ที่ทำการพัฒนาบนบีเอสดีดังต่อไปนี้

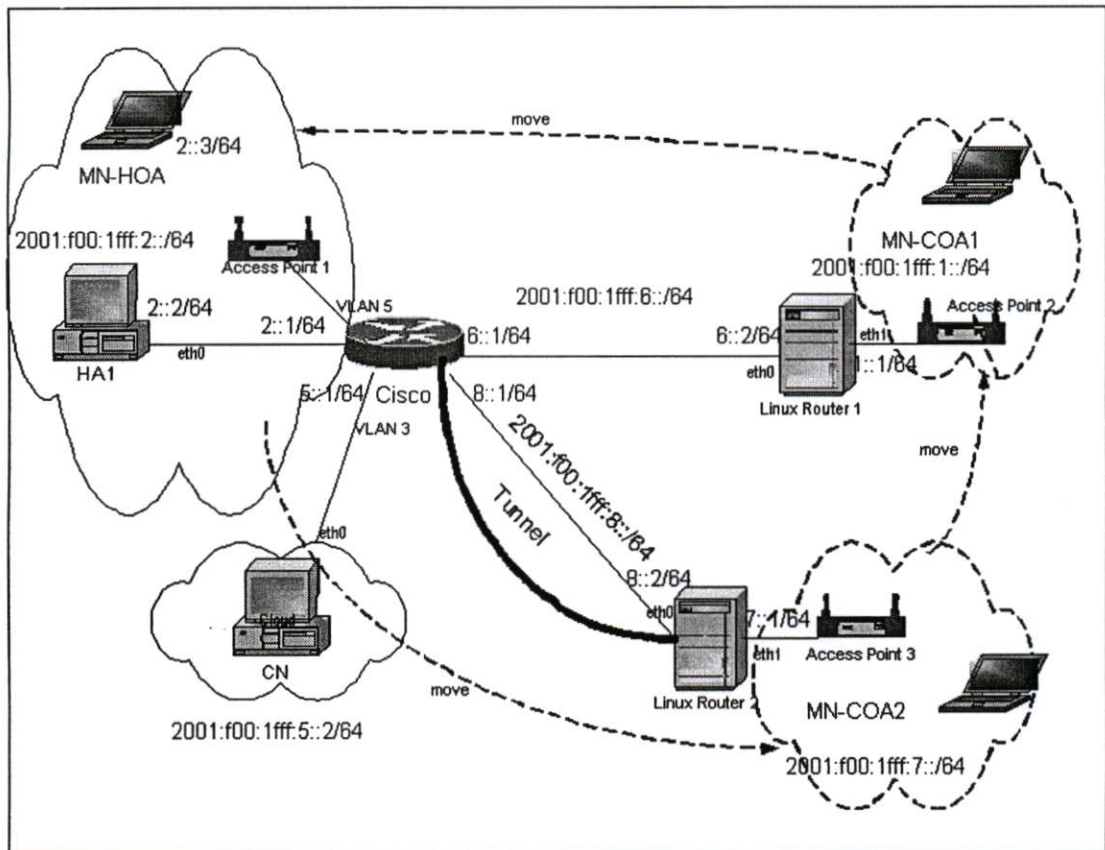
- <http://www.mobileip.jp/>
- <http://www.kame.net>
- <http://www.tahi.org/>
- <http://www.sfc.wide.ad.jp/InternetCAR>
- <http://www.sfc.wide.ad.jp/NEMO/>
- <http://www.sfc.wide.ad.jp/MIP6>

### บทที่ 3

## การเพิ่มประสิทธิภาพของการเคลื่อนย้ายข้ามเครือข่าย IPv6

วัตถุประสงค์ของบทนี้ศึกษาประสิทธิภาพในแง่ของความล่าช้า วิธีของการย้ายข้ามเครือข่ายผล  
กระทบต่อการย้ายข้ามของตัวแปรเพราะฉะนั้นต้องเริ่มศึกษาองค์ประกอบของความล่าช้า (Delay)  
และการปรับค่าตัวแปรเพื่อให้เหมาะสมกัน ทำให้ได้ค่าเวลาการย้ายข้ามเครือข่ายน้อยที่สุด

### 3.1 การทดลอง MIPv6



รูปที่ 3.1 ผังการทดลองย้ายข้ามเครือข่ายของ MIPv6

ในการทดลองจะประกอบไปด้วย WLAN 3 เครื่องข่ายเชื่อมต่อกันตามรูปที่ 3.1 ทุกอุปกรณ์  
ใช้ลินุกซ์ TLE 7.0 พัฒนาจากพื้นฐานฟิโดรา (Fedora) ใช้เคอร์เนล 2.6.11 ส่วน MN HA1 HA2 และ  
CN จะใช้โปรแกรม MIPv6 บนระบบปฏิบัติการลินุกซ์ชื่อ MIPv6-2.0-RC3 [11] การคอนฟิก  
สำหรับ MN HA และ CN จะอยู่ในคู่มือตาม [14]

### 3.2 ตัวแปรที่มีผลกระทบต่อ การเคลื่อนย้ายเครือข่าย

ในการทดลองได้ทำการเคลื่อนย้าย MN ไประหว่าง 3 จุดการเข้าถึง โดยเริ่มจากบ้านไปเครือข่ายหนึ่งแล้วสู่อีกเครือข่ายหนึ่งและก็กลับบ้าน สมมุติฐานของการหาค่าการล่าช้าของการย้ายข้ามเครือข่ายจะเริ่มตั้งแต่ MN เริ่มเคลื่อนที่ไปจนสิ้นสุดการทำเส้นทางที่เหมาะสมที่สุด พารามิเตอร์สำหรับจำแนกการวัดการล่าช้าของการย้ายข้ามเครือข่ายประกอบไปด้วย TD TR และ TO โดยที่จะนิยามแต่ละพารามิเตอร์ดังต่อไปนี้

TD	A0	--- Execute script run move to new access point ---					
TC	A1	837	180.055904	fe80::205:5 dff:fe50:702 d ff02::1	ICMPv 6	Router advertisement	
	A2	847	183.376717	MN-CoA 2 HA MIPv 6	Binding Update		
TR		Sequence number: 48705					
		850	184.187264	MN-HoA CN MIPv6	Home Test Init		
		851	184.187641	MN-CoA 2 CN MIPv 6	Care-of Test Init		
		856	184.199596	CN MN-CoA 2 MIPv 6	Care-of Test		
TO	A3	858	184.386406	HA MN-CoA 2 MIPv 6	Binding Acknowledgement		
		Sequence number: 48705					
		879	189.188427	MN-HoA CN MIPv6	Home Test Init		
		882	189.194183	CN MN-HoA MIPv6	Home Test		
	883	189.194592	MN-CoA 2 CN MIPv 6	Binding Update			
	Sequence number: 8819						
		890	190.197799	CN MN-CoA 2 ICMPv 6	Echo reply		

รูปที่ 3.2 การตรวจจับข้อมูลที่แลกเปลี่ยนกันระหว่างการย้ายข้ามเครือข่ายบน MIPv6

TD นิยามเป็นเวลาร้องขอที่ MN เริ่มย้ายและสร้างการเชื่อมต่อใหม่กับจุดเข้าถึงใหม่ (ตัวอย่างเช่น การสำรวจพบลิงค์ภายในของการเชื่อมต่อของเกตเวย์)

$$TD = A1 - A0 \quad (3.1)$$

TC นิยามเป็นเวลาร้องขอการติดตั้งแอดเดรส IPv6 ให้ใช้งานในเครือข่ายใหม่ ในช่วงนี้จะมี การเช็คการซ้ำกันของ IP (DAD)

$$TC = A2 - A1 \quad (3.2)$$

TR นิยามเป็นเวลาระหว่างที่ MN ร้องขอ BU ถึง HA เพื่อรอ HA ตอบกลับ BA

$$TR = A3 - A2 \quad (3.3)$$

TO นิยามเป็นเวลาร้องขอของแอดเดรสใหม่ของ IPv6 ที่ได้ติดต่อโดยตรงกับ CN โดยในช่วงนั้นมีการคุยในขั้นตอนการสร้างเส้นทางแบบสามเหลี่ยมด้วยก่อนที่ MN จะติดต่อโดยตรงกับ CN ผ่าน COA

$$TO = A4 - A3 \tag{3.4}$$

เมื่อ A1, A2, A3 และ A4 มีนิยามดังแสดงในรูปที่ 3.2

ซึ่งจะได้ผลรวมของการล่าช้าของการย้ายข้ามเครือข่าย (TH) เป็น

$$TH = TD + TC + TR + TO \tag{3.5}$$

ในการทดลองได้ใช้โปรแกรมตรวจจับแพ็กเก็ตชื่ออีเทอร์เรียล (Ethereal) [8] ได้นำเวลาที่รันสคริปต์ย้ายเครือข่ายโดยใช้คำสั่ง iwconfig และหาความแตกต่างระหว่างเวลารันกับเวลาที่เริ่มจับแพ็กเก็ต และ MN ได้รับ BA ที่มาจาก CN จากการจับแพ็กเก็ตสามารถแยกแต่ละช่วงเวลาได้ดังแสดงในรูปที่ 3.2

### 3.3 ค่าพารามิเตอร์ที่นำมาศึกษา

พารามิเตอร์ทั้งหมดที่นำมาศึกษาได้มีการกำหนดค่าไว้ดังแสดงในตารางที่ 3.1 ซึ่งแต่ละพารามิเตอร์มีนิยามดังต่อไปนี้ ซึ่งค่าเหล่านี้เป็นค่าที่โปรแกรมลินุกส์กับโปรแกรมแจกไอพีมีการกำหนดมาให้อยู่แล้ว ได้ทำการนำค่าเหล่านี้เป็นเกณฑ์แล้วปรับเปลี่ยนค่าตัวแปรของโปรแกรมเพื่อเพิ่มประสิทธิภาพของระบบ MIPv6

ตารางที่ 3.1 พารามิเตอร์ที่นำมาศึกษา

พารามิเตอร์การหาเส้นทาง	ค่าของพารามิเตอร์
MinRtrAdvInterval	3 s
MaxRtrAdvInterval	10 s
Router_solicitations	3
Router_solicitation_interval	4 s
Router_solicitation_delay	1 s
DAD RetransTimer	1000 ms
DupAddrDetectTransmit	1
MN IPSec	Off

MinRtrAdvInterval คือ ค่าน้อยที่สุดที่เกตเวย์จะทำการประกาศให้กับลูกข่าย

MaxRtrAdvInterval คือ ค่ามากที่สุดที่เกตเวย์จะทำการประกาศให้กับลูกข่าย

Router\_solicitations คือ การที่ลูกข่ายเรียกขอไอพีจากเกตเวย์

Router\_solicitation\_interval คือ ช่วงเวลาการที่ลูกข่ายเรียกขอไอพีจากเกตเวย์

Router\_solicitation\_delay คือ ช่วงเวลาการล่าช้าที่ลูกข่ายเรียกขอไอพีจากเกตเวย์

DAD RetransTimer คือ ค่าในการวนซ้ำการซ้ำกันของข้อมูล

DupAddrDetectTransmit คือ การใช้งานที่มีการเช็คการซ้ำกันของไอพีถ้าค่าเป็น 1 คือเช็ค ถ้าเป็น 0 ไม่ทำการเช็คการซ้ำกันของไอพี

MN IPSec คือ การเช็คเรื่องของความปลอดภัยในการเข้าใช้งานการเคลื่อนย้ายข้าม เครือข่าย

### 3.4 การทดสอบการย้ายข้ามในแต่ละกรณี

#### กรณีที่ 1

ทำการปรับเปลี่ยนค่า MinRtrAdvInterval (MinRA) และ MaxRtrAdvInterval (MaxRA) ตามลำดับดังนี้ RtrAdvinterval (RA) = (0.03,0.07), (0.01,0.5), (0.5,1.5), (1,3) และ (3,10)

#### กรณีที่ 2

ใช้การปรับเปลี่ยนเหมือนกรณีที่ 1 แต่จะให้ค่า Router\_solicitations (RS) เป็น 1 วินาที

#### กรณีที่ 3

ใช้การปรับเปลี่ยนเหมือนกรณีที่ 1 แต่ให้มีค่า DupAddrDetectTransmit (DAD) เป็น 0 คือ ไม่ต้องทำการเช็ค IP

ในแต่ละกรณีได้ทำการทดสอบในช่วง 60 นาทีทำการเคลื่อนย้าย MN จาก RCOA2 ไป RCOA1 แล้วกลับเครือข่ายเดิม ทำการเก็บค่าทุกช่วงการย้ายแล้วนำข้อมูลที่ได้มาวิเคราะห์

### ตารางที่ 3.2 การเช็คค่ากรณีที่ 1

กรณีที่ 1
sysctl -w net.ipv6.conf.default.router_solicitation_delay=1
sysctl -w net.ipv6.conf.default.router_solicitation_interval=4
sysctl -w net.ipv6.conf.all.router_solicitation_delay=1
sysctl -w net.ipv6.conf.all.router_solicitation_interval=4
sysctl -w net.ipv6.conf.eth1.router_solicitation_delay=1
sysctl -w net.ipv6.conf.eth1.router_solicitation_interval=4
sysctl -w net.ipv6.conf.ip6tnl1.router_solicitation_delay=1
sysctl -w net.ipv6.conf.ip6tnl1.router_solicitation_interval=4

### ตารางที่ 3.3 การเซ็ตค่ากรณีที่ 2

กรณีที่ 2
<pre>sysctl -w net.ipv6.conf.default.router_solicitation_delay=0 sysctl -w net.ipv6.conf.default.router_solicitation_interval=1 sysctl -w net.ipv6.conf.all.router_solicitation_delay=0 sysctl -w net.ipv6.conf.all.router_solicitation_interval=1 sysctl -w net.ipv6.conf.eth1.router_solicitation_delay=0 sysctl -w net.ipv6.conf.eth1.router_solicitation_interval=1 sysctl -w net.ipv6.conf.ip6tnl1.router_solicitation_delay=0 sysctl -w net.ipv6.conf.ip6tnl1.router_solicitation_interval=1</pre>

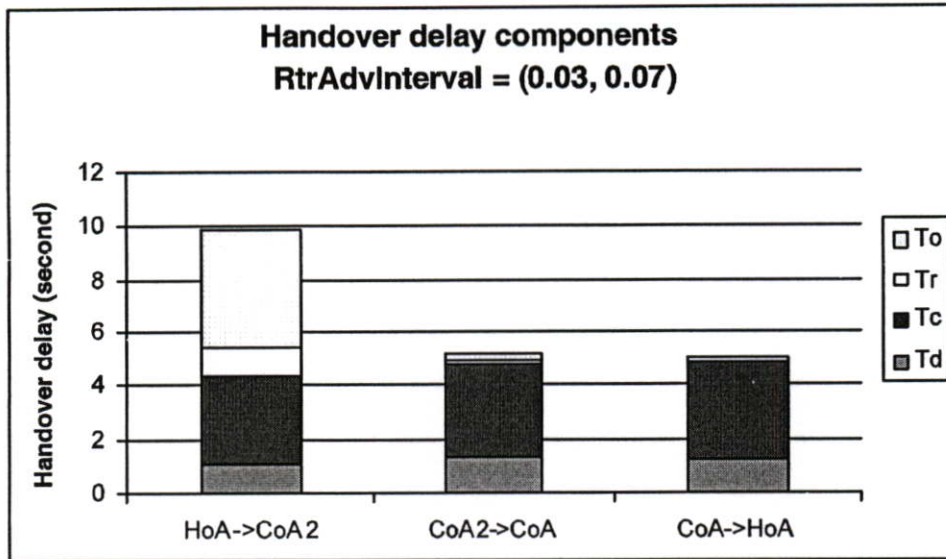
### ตารางที่ 3.4 การเซ็ตค่ากรณีที่ 3

กรณีที่ 3
<pre>sysctl -w net.ipv6.conf.default.router_solicitation_delay=0 sysctl -w net.ipv6.conf.default.router_solicitation_interval=1 sysctl -w net.ipv6.conf.all.router_solicitation_delay=0 sysctl -w net.ipv6.conf.all.router_solicitation_interval=1 sysctl -w net.ipv6.conf.eth1.router_solicitation_delay=0 sysctl -w net.ipv6.conf.eth1.router_solicitation_interval=1 sysctl -w net.ipv6.conf.ip6tnl1.router_solicitation_delay=0 sysctl -w net.ipv6.conf.ip6tnl1.router_solicitation_interval=1</pre>

## 3.5 ผลการทดลองและการวิเคราะห์

### 3.5.1 การตรวจจับการเคลื่อนย้ายกับส่วนประกอบของการล่าช้า

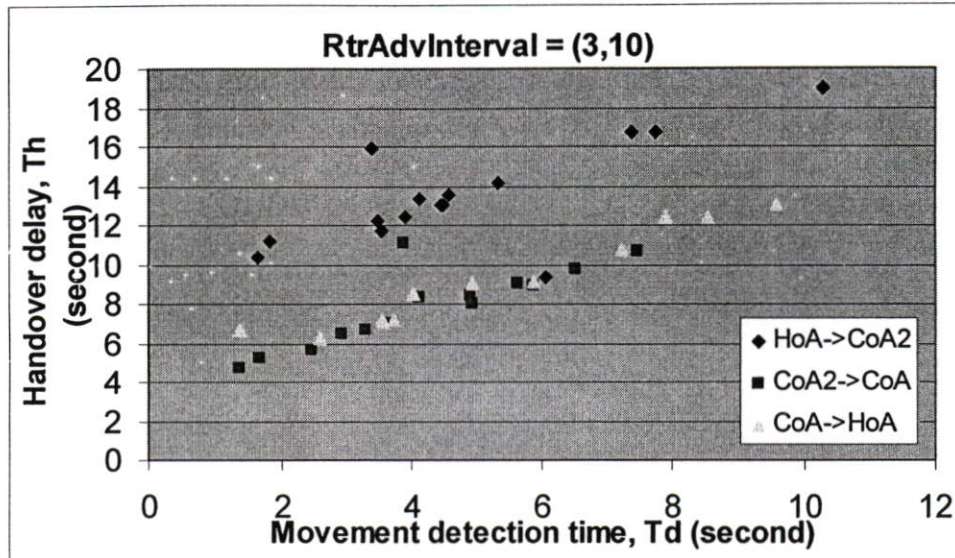
รูปที่ 3.3 แสดงการเปรียบเทียบการล่าช้าเมื่อย้ายไปเครือข่ายต่าง ๆ เมื่อกำหนดให้ค่า  $RtrAdvinterval = (0.03, 0.07)$  วินาที จะเห็นว่าการเคลื่อนย้ายจากบ้านไปเครือข่าย CoA2 ค่าการล่าช้าจะสูงกว่าเมื่อเคลื่อนย้ายจาก CoA2 ไป CoA และจาก CoA ไป HoA คือกลับบ้านเพราะการแลกเปลี่ยนค่าระหว่างบ้านไปเครือข่าย CoA2 มีการแลกเปลี่ยนผ่านท่อของ HA ทำให้ต้องสร้างท่อเพื่อใช้เวลาในการคุยกันเพื่อการจัดเส้นทางที่เหมาะสม แล้วไปที่เครือข่าย CoA ก็ไม่ต้องเสียเวลาสร้างท่อคุยกันเพียงคุยแค่ CoT กับ CoTI เท่านั้นก็สามารถสร้างเส้นทางที่เหมาะสมได้ ส่วนตอนกลับที่ไม่ต้องใช้การคุยกันผ่านท่อของ HA เพราะที่ HA จะมีตัวเก็บตัวพักข้อมูลไว้ การคุยกันจะจดจำ HoA เดิมในการคุยตามมาตรฐาน RFC 3775



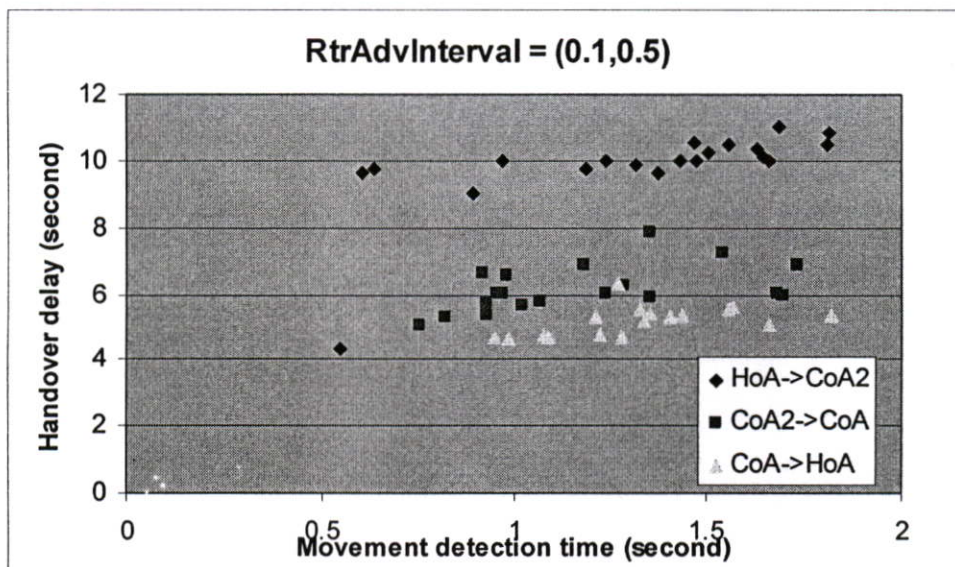
**รูปที่ 3.3** การเปรียบเทียบการล่าช้าเมื่อย้ายข้ามไปเครือข่ายต่าง ๆ เมื่อกำหนดให้ค่า RtrAdvInterval เป็น (0.03,0.07) วินาที

### 3.5.2 ผลกระทบที่เกิดจากการประกาศค่าเกตเวย์

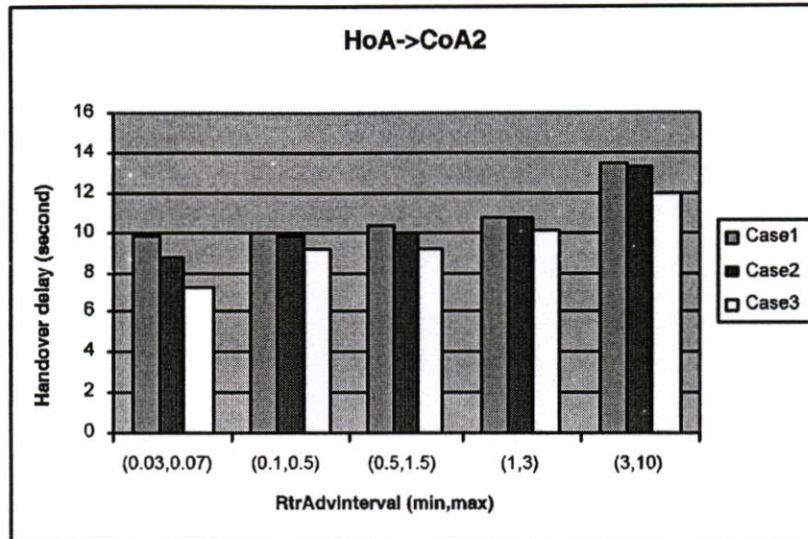
ในการทดลองได้ศึกษาการประกาศค่าเกตเวย์ที่มีผลกระทบต่อ TD ซึ่งมีผลต่อ TH เมื่อทำการย้ายเครือข่าย บนระบบลินุกซ์เกตเวย์จะมีการสุ่มค่าของการประกาศเกตเวย์ระหว่างค่าที่ต่ำที่สุดจนถึงค่าที่สูงที่สุด ในอันดับแรกได้กำหนดตามค่าเดิมของโปรแกรมคือ  $MinRtrAdvInterval = 3$  และ  $MaxRtrAdvInterval = 10$  รูปที่ 3.4 แสดงความสัมพันธ์ระหว่างการตรวจจบการเคลื่อนย้ายและค่าการประกาศจากตัวจัดการเส้นทาง จากรูปที่ 3.4 แสดงค่าการวัดแบบจุดของ  $RA = (3,10)$  เทียบกับค่า TD กราฟที่ได้จะคล้ายเส้นตรงขึ้นไปหมายความว่าถ้าลดค่าของการล่าช้าจะต้องลดการตรวจจบให้เร็วขึ้น ส่วนในรูปที่ 3.5 แสดงค่าการวัดแบบจุดของ  $RA = (0.1,0.5)$  เทียบกับค่า TD ค่าที่ได้ของ TD จะดีขึ้นแสดงว่ามีการแปรผันตามค่า RA ซึ่งจะได้ค่าอยู่ระหว่าง 0.6-1.7 วินาที จะเห็นว่าจะได้ค่า TD ที่ไม่สามารถน้อยกว่า 0.5 วินาที ถึงแม้จะปรับค่า RA ให้น้อยที่ (0.03,0.07) แล้วก็ตามเหตุที่เป็นอย่างนั้นเพราะเมื่อมีการส่งค่าถี่มากขึ้นจะเกิดความหนาแน่นของอัตราการส่งเกิดข้อมูลที่ไม่จำเป็นเกิดขึ้นในระหว่างชั้น 2 ดังที่ได้กล่าวไว้ ซึ่งได้ข้อสรุปว่าการกำหนดค่า RA ให้น้อยกว่า 0.5 ไม่ได้ช่วยให้ TD ดีขึ้นและไม่สามารถทำให้ลดค่าการล่าช้าของการเคลื่อนที่ได้



รูปที่ 3.4 การแปรผันระหว่างการตรวจจับการเคลื่อนย้ายและค่าการประกาศเขตเวลาที่ค่า (3,10)



รูปที่ 3.5 การแปรผันระหว่างการตรวจจับการเคลื่อนย้ายและค่าการประกาศเขตเวลาที่ค่า (0.1,0.5)



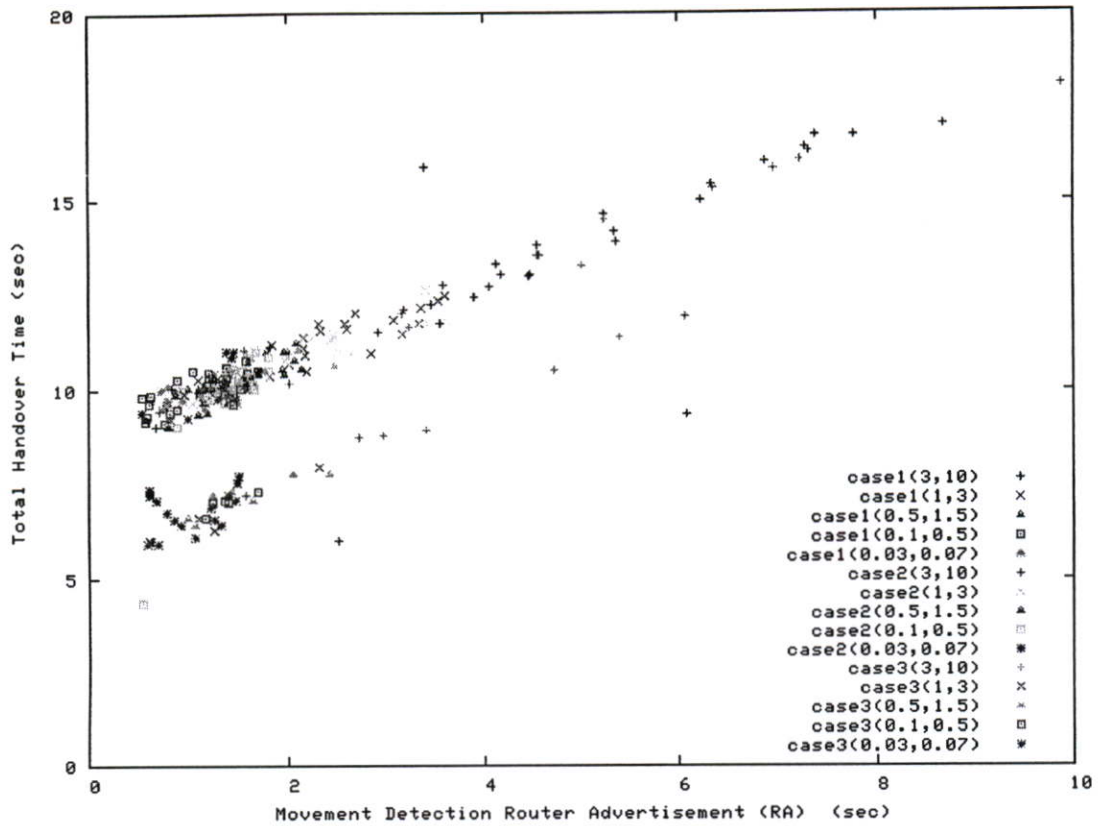
รูปที่ 3.6 การเปรียบเทียบความเร็วในการย้ายข้ามเครือข่ายเมื่อปรับค่าการประกาศเกตเวย์

### 3.5.3 ผลกระทบที่เกิดจากค่าการร้องขอของเกตเวย์

รูปที่ 3.6 แสดงการเปรียบเทียบในแต่ละกรณีของค่าของการประกาศจากตัวจัดการเส้นทาง ในกรณีที่ 1 ถ้าลดค่า RtrAdvinterval ให้น้อยกว่า 0.5 ก็ไม่สามารถลดค่าการล่าช้าของการเคลื่อนย้ายได้ ดังนั้นต้องพยายามหาวิธีอื่นที่จะมาช่วยลดการล่าช้านี้ ในกรณีที่ 2 จะลดค่า Router\_solicitations ซึ่งค่าเดิมคือร้องขอทุก 3 วินาที เปลี่ยนมาเป็น 1 วินาทีคือไม่ต้องรอถึง 3 วินาทีถึงร้องขอเพียงแค่วเวลาถึง 1 วินาที MN จะทำการร้องขอค่าไอพีใหม่จากเกตเวย์แทนที่จะต้องรอ ทำให้ช่วยลดการหนาแน่นของเครือข่ายเพราะไม่ต้องมีการกระจายข้อมูลมาก เหมาะกับเครือข่ายขนาดกลาง

### 3.5.4 ผลกระทบที่เกิดจากการเช็คการซ้ำกันของไอพี

ตอนนี้ต้องการลดค่าการล่าช้าลงอีก จากหัวข้อ 3.5.1 ทำการลดแค่ TD ซึ่งยังสามารถที่จะลดค่าของ TC เพื่อให้ค่าการล่าช้าของการเคลื่อนย้ายลดลงได้อีก โดยการปรับ DAD เพื่อที่ว่าเมื่อ MN ได้ย้ายไปเครือข่ายใหม่ไม่จำเป็นต้องเช็ค IP ในเครือข่ายใหม่ก็จะทำการจดจำ IP เดิมเพื่อใช้ในการติดต่อกับ CN จากรูปที่ 3.6 กรณีที่ 3 ค่าที่ได้จากการเคลื่อนย้ายทั้งหมดจะได้ค่าที่น้อยกว่าในกรณีที่ 1 และ 2 เพราะไม่ต้องเสียเวลาเช็ค IP เหมาะกับในเครือข่ายขนาดเล็กที่ผู้ดูแลจัดการได้ง่ายทั่วถึง แต่ก็ไม่ควรใช้ในเครือข่ายใหญ่ ๆ ซึ่งโอกาสในการซ้ำกันของ IP มีสูงผู้ดูแลไม่สามารถที่จะรู้ได้ว่าจะมีโอกาสในการซ้ำกันของ IP จากผู้ใช้เองโดยไม่ได้ใช้การรับจาก RADVD ซึ่งจะทำหน้าที่การแจกไอพีตามมาตรฐาน EUI-64 (โดยใช้แอดเดรส MAC มาคำนวณเพื่อใช้เป็น IP ใหม่)



รูปที่ 3.7 การเช็คค่าเวลาที่เป็นไปได้มากที่สุดในการย้ายข้ามเครือข่าย

รูปที่ 3.7 แสดงการเช็คค่าเวลาที่เป็นไปได้มากที่สุดในการย้ายข้ามเครือข่าย จะเห็นได้ว่า ช่วงเวลาที่ใช้ในการย้ายข้ามเครือข่ายในทุกกรณีจากเครือข่ายบ้านไปเครือข่ายเพื่อนบ้านจะอยู่ที่ ช่วงเวลา 10 วินาที จึงสรุปได้ว่าการย้ายข้ามเครือข่ายจะใช้เวลาประมาณ 10 วินาที ถึงจะทำให้การ สนทนาระหว่าง MN ที่กับ CN สามารถติดต่อสื่อสารกันได้เหมือนเดิม ทำให้การใช้งานเกิดสะดุด ในช่วงการย้ายข้ามเครือข่าย

ตารางที่ 3.5 สรุปเวลาในการย้ายข้ามเครือข่ายของ MIPv6 ของกรณี 1 ถึง 3

กรณี	ค่าเฉลี่ยเวลาไปเครือข่ายอื่น	ค่าเฉลี่ยเวลากลับเครือข่ายเดิม
1	~11 Sec	~5 sec
2	~10 Sec	~5 Sec
3	~9 Sec	~5 Sec

ตารางที่ 3.5 แสดงการสรุปเวลาในการย้ายข้ามเครือข่ายของ MIPv6 ของกรณี 1 ถึง 3 จะ เห็นว่าถ้าสามารถลด DAD ลงจะทำให้ความล่าช้าของการย้ายข้ามเครือข่ายลดลงกว่ากรณี 1 และ

2 อย่างชัดเจน แต่ในเครือข่ายการใช้งานจริง ถ้าไม่มีการเซ็คการซ้ำกันจะก่อให้เกิดความเสี่ยงของกรณีเกิดการชนกันของ IP เพิ่มขึ้น ทำให้เกิดการใช้งานไม่ได้เกิดขึ้น ส่งผลเสียต่อองค์กรและธุรกิจ ในเครือข่ายขนาดเล็กที่มีผู้ดูแลระบบสามารถรู้เครื่องลูกข่ายของผู้ใช้งานทุกเครื่อง เมื่อเกิดการชนกันของ IP แล้วตรวจสอบเจอและแก้ไขได้ทันที ก็สามารถนำกรณีที่ 3 มาใช้งานได้โดยมีประสิทธิภาพมากขึ้น แต่ถ้าเครือข่ายขนาดใหญ่ที่มีลูกข่ายจำนวนมาก จะเป็นการยากต่อผู้ดูแลระบบที่ต้องมาหาเครื่องที่เกิดการชนกันของ IP ลูกข่ายที่มีจำนวนมาก จะทำให้เสียเวลาในการตรวจสอบ กว่าจะค้นพบก็ทำให้เกิดผลเสียต่อองค์กรและธุรกิจไปแล้ว ในการแจก IP บางทีอาจจะไม่ได้รู้ถึงระดับแม่คเอดเตรส เช่น โปรแกรม RADVD [18] ถ้าเป็น DHCPv6 [19] ที่มีความสามารถรู้แม่คเอดเตรสของเครื่องลูกข่าย จะสามารถทราบได้ง่ายขึ้นเมื่อเกิดการชนกันของ IP ดังนั้น การใช้กรณีที่ 3 เพื่อลดความล่าช้าของการย้ายข้ามเครือข่ายจะเหมาะกับเครือข่ายขนาดเล็กที่ผู้ดูแลระบบจัดการได้ทั่วถึงทราบได้ทันทีก่อนจะเกิดการใช้งานไม่ได้ ถ้าเป็นเครือข่ายขนาดใหญ่ก็จะต้องมีโปรแกรมที่จัดการเกี่ยวกับแม่คเอดเตรสหรือเครื่องที่สามารถตรวจสอบตัวตนได้ว่าเป็นใคร ทำให้ผู้ดูแลระบบสามารถจัดการแก้ไขได้ทันเวลา

## บทที่ 4

# การเพิ่มความน่าเชื่อถือได้ของโฮมเอจेंट (HA)

### 4.1 การศึกษาและรวบรวมข้อมูล

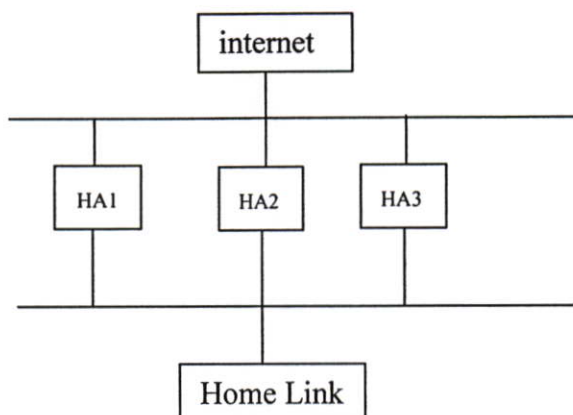
ในวิทยานิพนธ์ฉบับนี้ได้ทำการศึกษาค้นคว้าจาก [2]-[4] เพื่อเป็นข้อมูลอ้างอิงในการวิจัย และทำการพัฒนาต่อโดยมีรายละเอียดดังต่อไปนี้

#### 4.1.1 ปัญหาที่ต้องศึกษา

ในการใช้งานอินเทอร์เน็ตหรือติดต่อกับคู่สนทนาแล้วเกิดอุปกรณ์ที่เป็นประตูทางออกไม่สามารถเชื่อมต่อกับโลกอินเทอร์เน็ตได้ ก็จะทำให้เกิดการใช้งานไม่ได้ ถ้าไม่มีระบบสำรองต้องรอจนกว่าอุปกรณ์ที่ทำหน้าที่นั้นกลับขึ้น ถึงจะสามารถใช้งานต่อได้ซึ่งในปัจจุบันการติดต่อผ่านโลกอินเทอร์เน็ตมีความจำเป็นอย่างสูงทั้งในภาคการศึกษา ธุรกิจ อุตสาหกรรม อื่นๆอีกมากมายที่ใช้โลกอินเทอร์เน็ต ขาดการติดต่อเปรียบเสมือนถนนขาดไม่สามารถเดินทางหาผู้กันได้ในวิทยานิพนธ์นี้จึงได้ศึกษาถึงวิธีที่จะทำให้เกิดการใช้งานได้อย่างต่อเนื่องเมื่อเกิดอุปกรณ์ตัวหลักใช้งานไม่ได้ก็จะมีตัวสำรองมาแทนที่เพื่อเป็นตัวหลักแทน

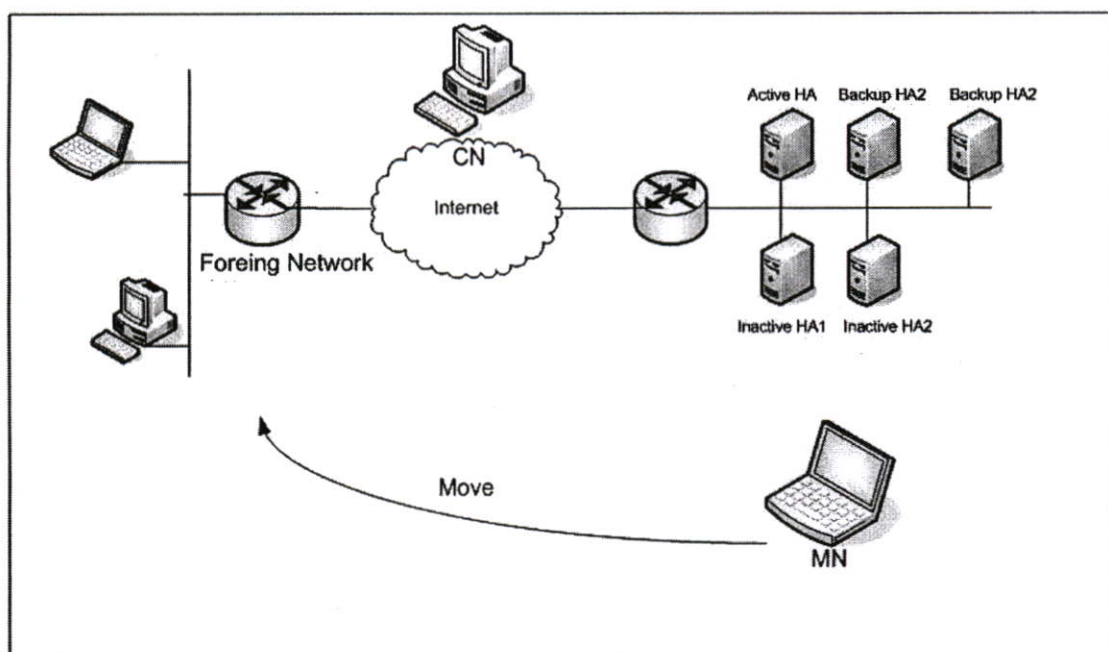
#### 4.1.2 งานวิจัยอื่นที่เกี่ยวข้อง

รูปที่ 4.1 แสดงการติดต่อแบบ HAHA [2] [3] ในโพรโทคอลแบบ HAHA จะใช้การเพิ่มความสามารถเดิมจาก RFC 3775 [1] โดยการใช้แอดเดรสเดิมทุก HA แต่ต่างกันที่ลิงค์โลคอลมีรายการ HA (HAL) และเพิ่มการทำงานในการเลือก HA เพื่อรับทราบว่า HA ตัวไหนใช้งานไม่ได้โดยใส่รายละเอียดเข้าไปในการส่งข้อมูลให้รับข่าวสารที่ปรับปรุงใหม่จาก MN ไปบอกแก่ HAL ส่วน HA ก็จะทำการขอข้อมูลข่าวสารที่ปรับปรุงใหม่เพื่อขอข้อมูลการส่งที่มีอยู่ก่อนที่เก็บไว้ในที่พักข้อมูลเพื่อรับทราบว่า HA ตัวไหนใช้งานไม่ได้ไปแล้วบ้าง สามารถให้ HA ใน HAL ขึ้นมาทำงานแทนได้



รูปที่ 4.1 การติดต่อแบบ HAHA

ในโพรโทคอลแบบ VCHAR [4] จะมี HA เพื่อสร้างความน่าเชื่อถือ 3 ตัวขึ้นไปคือมี HA หลัก HA สำรอง และ HA ที่ยังไม่ได้ทำหน้าที่ โดย HA หลักเมื่อเกิดการใช้งานไม่ได้จะมีการส่งข้อมูลเพื่อขอทำการส่งข้อมูลเพื่อติดต่อกับ HA สำรอง และ HA สำรองจะขึ้นมาทำหน้าที่แทน ส่วน HA ที่ยังไม่ได้ทำหน้าที่เป็นตัวที่ยังไม่ได้ใช้งาน การติดต่อแบบ VCHAR ได้แสดงไว้ในรูปที่ 4.2

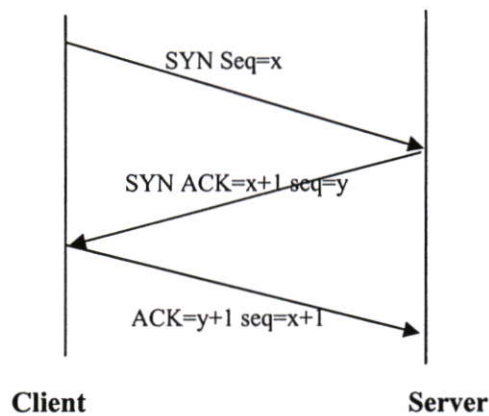


รูปที่ 4.2 การติดต่อแบบ VCHAR

ในวิทยานิพนธ์ฉบับนี้ได้ทำการศึกษาการก๊อปปี้แบบง่ายที่ใช้งานจริงได้ และมี HA แค่สองตัวก็สามารถทำงานแทนกันได้ โดยใช้โพรโทคอล TCP แบบสัมพันธ์ 3 ทางมาทำการตรวจสอบ มี

HA1 ทำงานเป็น HA หลัก HA2 เป็น HA สำรอง เมื่อ HA หลักเกิดใช้งานไม่ได้จะมี HA สำรองเข้ามาทำงานแทนที่ และแทนตัวเองเป็น HA1 และเมื่อ HA1 สามารถทำงานได้ดั้งเดิมก็จะแทนตัวเองเป็น HA2 คอยทำงานเมื่อเกิด HA หลักทำงานไม่ได้อีก สลับการกู้กลับการทำงานกันไป ได้ทำการแก้ไขค่าของโปรแกรม MIPL โดยแก้ค่าเวลาคงอยู่ของ CN ให้ตอบสนองต่อการใช้งานไม่ได้ของ HA

#### 4.1.3 การตรวจสอบสถานะของ HA โดยใช้ทีซีพีแบบสามพันช์ 3 ทาง (TCP 3 way handshake)



รูปที่ 4.3 ขั้นตอนในการสร้าง TCP ทำการติดต่อ

ในงานวิจัยที่เลือกใช้การรูปแบบทีซีพีแบบสามพันช์ 3 ทาง เพราะมีความน่าเชื่อถือดีกว่าแบบอื่นเพราะมีการสร้างการเชื่อมต่อที่รอการตอบสนอง ถ้าไม่สามารถเชื่อมต่อได้จะมีการส่งข้อมูลมาบอก ต่างกับโพรโทคอลแบบยูดีพี (UDP) ซึ่งส่งอย่างเดียวไม่รอการตอบกลับและไอซีเอ็มพี (ICMP) ซึ่งอาจเกิดมีการเชื่อมต่อไม่ถึงเมื่อเครือข่ายเกิดมีปริมาณการส่งข้อมูลมากๆ แต่ตัวแม่ข่ายยังทำงานก็ไม่สามารถทราบแน่ชัดว่าแม่ข่ายใช้งานไม่ได้จริงหรือไม่จริง

การใช้งานโพรโทคอลทีซีพีแบบสามพันช์ 3 ทาง เป็นการสร้างความสัมพันธ์ระหว่างแม่ข่ายและลูกข่ายเพื่อทราบสถานะการเข้าใช้งานกัน มีการส่งการร้องขอ (SYN) การรอการตอบรับ (SYN/ACK) และการตอบรับ (ACK) เมื่อแม่ข่ายและลูกข่ายได้ทำการติดต่อผ่าน 3 ข้อความนี้แล้วก็จะสามารถสร้างทีซีพีแบบสามพันช์ 3 ทาง ได้และพร้อมที่จะติดต่อสื่อสารกันผ่านโพรโทคอล TCP

การจัดการการเชื่อมต่อแบบทีซีพีแบบสามพันช์ 3 ทาง การสร้างการติดต่อของ TCP นั้นจะเรียกทางฝั่งที่ต้องการสร้างการติดต่อว่าลูกข่าย และเรียกอีกฝั่งที่ถูกเรียกว่าแม่ข่าย โดยที่ในการสร้างการติดต่อนั้นจะเริ่มจากการประยุกต์ใช้งานของลูกข่ายที่ต้องการสร้างการเชื่อมต่อ ซึ่งจะใช้คำสั่ง (ยกตัวอย่างโดยใช้ภาษา perl)

หลังจากนั้น TCP ของทางลูกข่ายจะทำการสร้าง TCP การติดต่อกับแม่ข่ายโดยมีขั้นตอนดังต่อไปนี้

ขั้นที่ 1: TCP ทางลูกข่ายจะส่ง TCP ลำดับข้อมูล ไปยัง TCP ของทางแม่ข่าย โดยที่ลำดับข้อมูลนี้จะไม่ยังมีข้อมูลใด ๆ แต่จะทำการตั้งค่าบิต SYN ในส่วนหัวของลำดับข้อมูลให้มีค่าเป็น 1 พร้อมทั้งตั้งค่า `client_isn` ซึ่งเป็นหมายเลขลำดับเริ่มต้นขึ้นมา และใส่ในลำดับข้อมูล แล้วจึงส่งลำดับข้อมูลนี้ไปยังแม่ข่าย และเนื่องจากลำดับข้อมูลนี้มีการกำหนดบิต SYN เป็น 1 จึงเรียกลำดับข้อมูลนี้ชื่อหนึ่งว่า SYN ลำดับข้อมูล

ขั้นที่ 2: เมื่อทางแม่ข่ายได้รับ SYN ลำดับข้อมูล ก็จะส่ง SYN/ACK ลำดับข้อมูล กลับไปให้ลูกข่าย โดยที่ SYN/ACK ลำดับข้อมูลนี้ก็ยัง ไม่มีข้อมูลใด ๆ แต่จะมีลักษณะสำคัญ 3 อย่างคือ 1) บิต SYN จะกำหนดเป็น 1 และ 2) ค่า ACK ในส่วนหัวจะกำหนดให้มีค่าเป็น `client_isn+1` และ 3) จะตั้งค่า `server_isn` ซึ่งเป็นหมายเลขลำดับเริ่มต้นขึ้นมา และใส่ลงใน `server_isn`

ขั้นที่ 3 หลังจากทางลูกข่ายได้รับ SYN/ACK ลำดับข้อมูลแล้ว ก็จะส่งลำดับข้อมูลสุดท้ายไปให้แม่ข่ายอีกโดยที่ 1) ได้กำหนดให้บิต SYN เป็น 0 และ 2) กำหนดค่าใน `server_isn` เป็น `client_isn+1` และ 3) กำหนดค่า ACK เป็น `server_isn+1`

หลังจาก 3 ขั้นตอนข้างบน (ซึ่งจะเรียกกระบวนการนี้ว่าแบบที่ซีพีแบบสัมพันธ์ 3 ทาง) ทางเสร็จแล้ว จะหมายถึงการสร้าง TCP ทำการติดต่อเสร็จแล้ว จากนั้นก็จะเป็นการเริ่มส่งข้อมูลระหว่างกัน โดย ลำดับข้อมูลที่จะใช้การส่งข้อมูลนั้นจะต้องกำหนดบิต SYN เป็น 0 เสมอ ขั้นตอนในการสร้างTCP ทำติดต่อแสดงไว้ในรูปที่ 4.3

หลังจากเสร็จสิ้นการรับ/ส่งข้อมูลแล้ว เมื่อต้องการที่จะเปิดการติดต่อทางลูกข่ายจะส่งลำดับข้อมูลที่กำหนดค่าบิต FIN เป็น 1 ไปให้ทางแม่ข่าย หลังจากนั้นแม่ข่ายจะส่งการตอบรับลำดับข้อมูลไปให้ทางลูกข่าย แล้วจะรอระยะเวลาหนึ่งเพื่อให้แน่ใจว่าทางลูกข่ายได้รับการตอบรับลำดับข้อมูลแล้ว (กรณีที่ทางลูกข่ายไม่ได้รับอาจเนื่องจากข้อมูลผิดพลาดจนทำให้ทางลูกข่ายใช้เวลาหมดก็จะส่ง FIN ลำดับข้อมูลไปให้แม่ข่ายใหม่ ทางแม่ข่ายก็จะส่งการตอบรับลำดับข้อมูลให้ใหม่เช่นกัน เมื่อแม่ข่ายแน่ใจว่าไม่มีการส่งใหม่ก็จะส่ง FIN ลำดับข้อมูลกลับไปให้ทางลูกข่าย

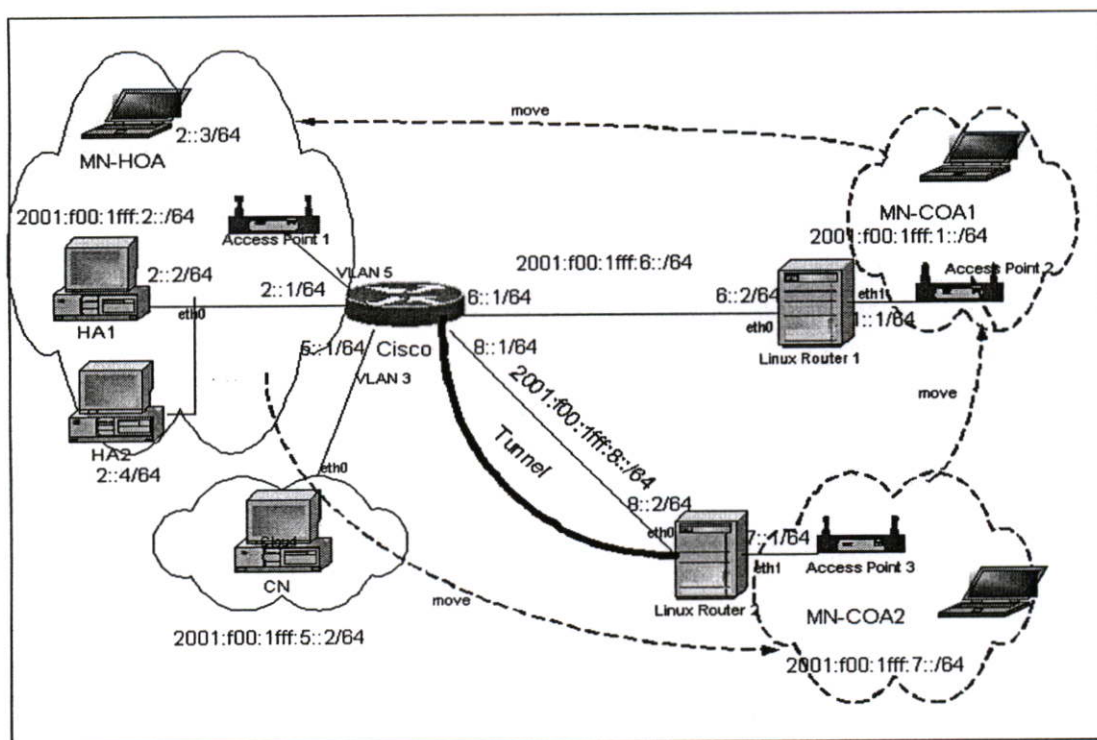
เมื่อทางลูกข่ายได้รับ FIN ลำดับข้อมูลแล้ว จะทำการส่งการตอบรับลำดับข้อมูลไปให้ทางแม่ข่าย แล้วจะรอระยะเวลาหนึ่ง (โดยปกติจะประมาณ 30วินาที หรืออาจเป็นค่าที่เหมาะสมตามแต่จะกำหนดไว้) เพื่อให้แน่ใจว่าทางแม่ข่ายได้รับแล้ว เมื่อครบเวลาที่รอทางลูกข่ายก็จะปลดปล่อยทรัพยากรต่าง ๆ แล้วปิดการติดต่ออย่างสมบูรณ์ ส่วนทางด้านแม่ข่ายเมื่อได้รับการตอบรับลำดับข้อมูลจะทำการปิดการติดต่อเช่นเดียวกัน

## 4.2 การวิเคราะห์และออกแบบระบบ

ได้ทำการศึกษาหาวิธีที่สามารถสร้างความน่าเชื่อถือขึ้นมาโดยจำลองเครือข่าย 3 เครือข่าย ให้มี HA 2 ตัว โดย HA1 เป็น HA หลัก HA2 เป็น HA สำรองเพื่อรอการทำงานเมื่อ HA หลักไม่สามารถใช้งานได้ หลักในการสร้างความน่าเชื่อถือคือทำให้เวลาเกิดการใช้งานไม่ได้ของระบบมีค่าน้อยที่สุด

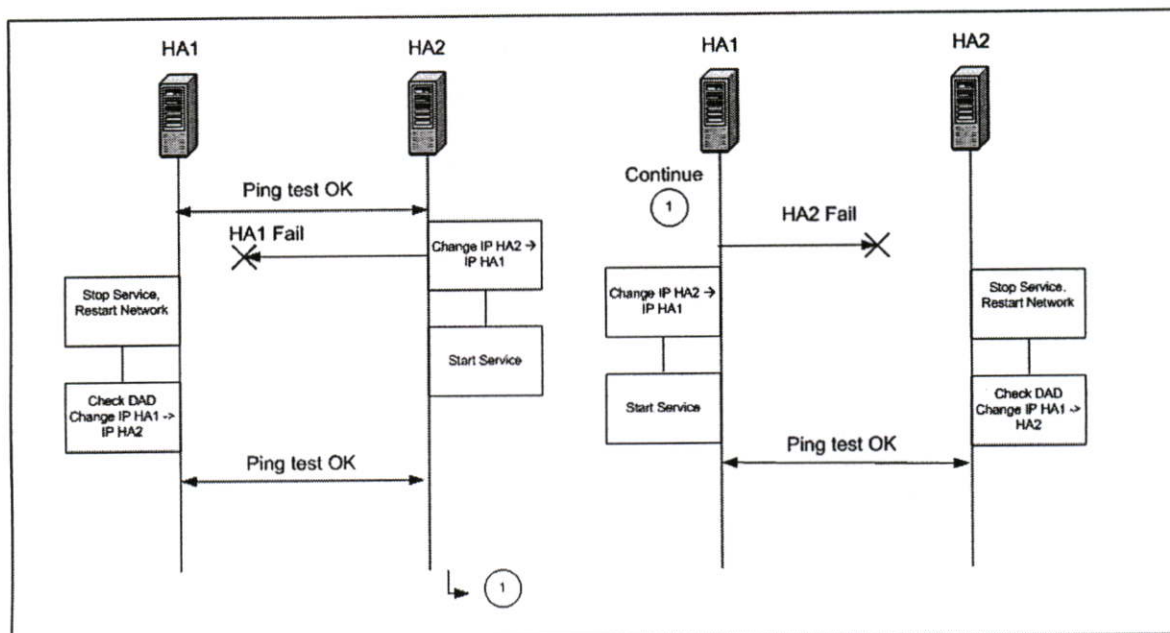
## 4.3 การสร้างระบบจำลองการทำงาน

ในการทดลองจะประกอบไปด้วย WLAN 3 เครือข่ายเชื่อมต่อกันตามรูปที่ 4.4 ทุกอุปกรณ์ใช้ลินุกซ์ TLE 7.0 (อิงจากพื้นฐานพีโครา ใช้เคอร์เนล 2.6.11) MN HA1 HA2 และ CN จะใช้โปรแกรม MIPv6 บนระบบปฏิบัติการลินุกซ์ชื่อ MIPv6-2.0-RC3 [11] การคอนฟิกสำหรับ MN HA และ CN จะอยู่ในคู่มือการใช้งานการเคลื่อนที่ของ IPv6 [14] ได้ทำการสร้างเส้นทางเพื่อเชื่อมเครือข่าย 3 เครือข่าย ในเครือข่ายบ้านจะมี HA ทำหน้าที่เป็นประตูออกสู่เครือข่ายอื่น ส่วนเครือข่ายอื่นก็จะมีเกตเวย์ของแต่ละเครือข่ายเพื่อจัด IP และเป็นประตูสู่เครือข่ายอื่น



รูปที่ 4.4 ผังการทดลองการเคลื่อนที่ของ IPv6

#### 4.4 ทฤษฎีของการสร้างความน่าเชื่อถือได้ของระบบ



รูปที่ 4.5 ผังการทำงานของ HA1 และ HA2

ในการทดลองได้ทำการเคลื่อนย้าย MN ไประหว่าง 3 จุดการเข้าถึง โดยเริ่มจากบ้านไปเครือข่ายหนึ่งแล้วผู้อีกเครือข่ายหนึ่งและก็กลับบ้าน สมมุติฐานของการหาค่าการล่าช้าของการย้ายข้ามเครือข่ายจะเริ่มตั้งแต่ MN เริ่มเคลื่อนที่ไปจนถึงสิ้นสุดการทำเส้นทางที่เหมาะสมที่สุด ลำดับขั้นของผังการทำงานของ HA1 และ HA2 จากรูปที่ 4.5 ซึ่งจะมีขั้นตอนดังต่อไปนี้

1. ทำการรันโปรแกรมเช็การเชื่อมต่อที่ HA1 และ HA2 ตั้งการทำงานของโปรแกรมเช็การเชื่อมต่อในเวลาที่กำหนดไว้ใน crontab (ในการทดลองเช็ทุก 1 นาที)
2. ให้ HA1 เป็น HA หลักในการจัดการ MN และ CN
3. เมื่อ HA1 ไม่สามารถทำงานได้โปรแกรมเช็การเชื่อมต่อจะทำการเปลี่ยน IP ของ HA2 ให้เป็น IP ของ HA1
4. เมื่อ HA2 เปลี่ยนเป็น IP ของ HA1 โปรแกรมจะทำการเปิดบริการที่จำเป็นต้องใช้ (ห้ามรัน radvd [18] ทั้งสองตัวพร้อมกัน MN อาจเกิดสับสน)
5. ถ้าทำการแก้ไขหรือปรับปรุงให้ HA1 พร้อมใช้งานแล้วก็นำมาเข้าระบบได้เลย ให้ทำการหยุดบริการของ HA1 ที่จะนำมาเข้าระบบและใช้โปรแกรมเช็การซ้ากันของข้อมูลมาช่วยเมื่อทำการเปิดการทำงานของเครือข่าย
6. เมื่อ HA2 ไม่สามารถทำงานได้ จะมีหลักการคล้ายกับที่ได้กล่าวมาแล้วสลับกันวนลูปไปเรื่อย ๆ เมื่อเกิด HA ใดตัวหนึ่งตายหรือไม่สามารถทำงานได้

#### 4.5 การหาพารามิเตอร์เพื่อเพิ่มความน่าเชื่อถือ

ได้ใช้โปรแกรม at บนระบบปฏิบัติการลินุกซ์เพื่อจำลองการใช้งานไม่ได้ของ HA1 ที่เป็น HA หลัก โดยให้ HA1 เกิดการใช้งานไม่ได้และโปรแกรมเช็คเริ่มทำงานที่เวลาเท่ากันแต่ในโปรแกรมการเช็คจะมีการนับอีกว่าจะให้เริ่มเช็คนับไปที่วินาทีถึงจะตรวจสอบดังตารางที่ 4.1 เมื่อ HA2 ตรวจสอบพบว่า HA1 ตายแล้วจะทำการแทนที่ตัวเองไปเป็น HA1 และรันโปรแกรม MIPL เพื่อทำงานต่อไป เมื่อ HA1 ฟิ้นก็จะแทนตัวเองเป็น HA2 เพื่อเป็นตัวสำรองไว้ทำงานต่อเมื่อเกิดการที่ HA หลักไม่ทำงานอีก จะสลับการทำงานไปเรื่อย ๆ การทำงานของการตรวจวัดการทดสอบได้แสดงไว้ในรูปที่ 4.6

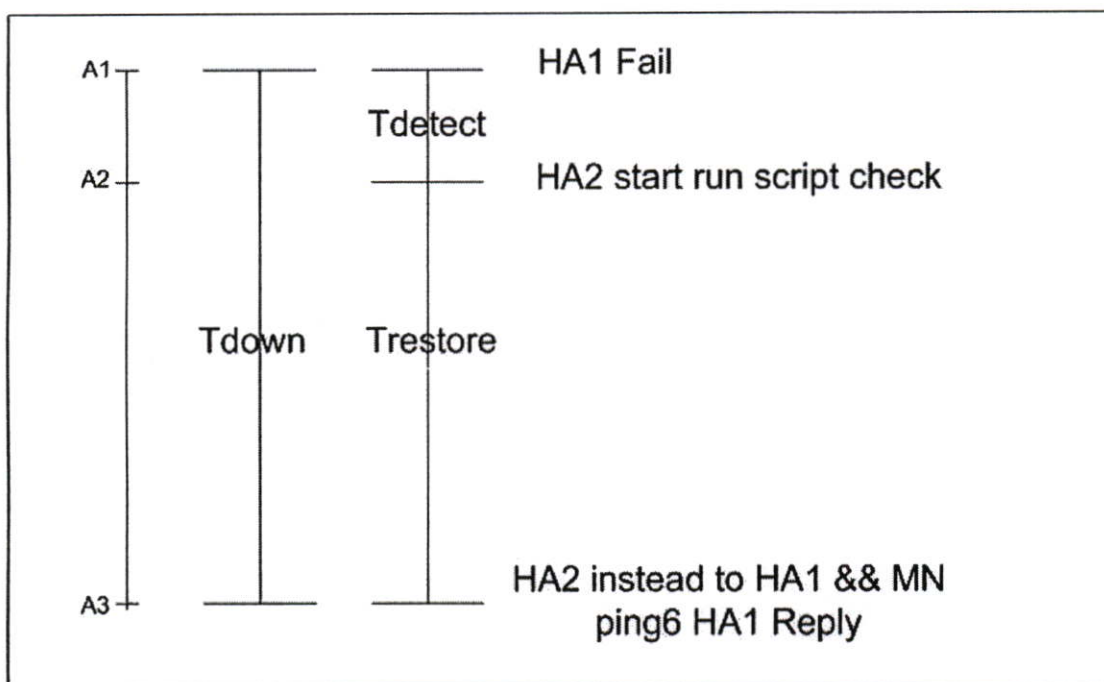
ได้ทำการวัดในแต่ละกรณีใน 1 ชั่วโมงโดยมีการทำให้ HA หลักตายทุก ๆ 10 นาที และทำการเช็คโดยเลือกช่วงเวลาเลวร้ายที่สุด คือ 60 วินาที ช่วงเวลาปานกลาง 30 วินาที และช่วงที่เช็คดีที่สุดคือ 1 วินาที โดยใช้คำสั่ง at บนระบบปฏิบัติการลินุกซ์ มาเป็นตัวกำหนดเวลาในการใช้งาน สัมหลวกับเวลาตรวจสอบเท่ากัน แต่จะมีช่วงการนับอีกว่าจะให้เช็คทุก 60 วินาที 30 วินาที หรือ 1 วินาที ในการทดลองได้เขียนโปรแกรมเช็คโดยใช้ TCP แบบสัมพันธ์สามทาง โดยมีการเปิดพอร์ตแม่ข่าย ลูกข่ายเมื่อถึงเวลาเช็คจะรัน โปรแกรมเพื่อไปใช้พอร์ตนั้น ถ้าใช้ได้แสดงว่า HA หลักยังคงทำงานได้อยู่ แต่ถ้าเข้าไปใช้งานพอร์ตนั้นไม่ได้ แสดงว่า HA หลักไม่สามารถใช้งานได้ จึงทำให้ HA สำรองมีการรันโปรแกรม เมื่อถึงช่วงเวลการรัน โปรแกรมจะเปลี่ยนตัวเองให้เป็น HA หลัก แทน HA เดิมที่ใช้งานไม่ได้ แล้วรันโปรแกรม MIPL เพื่อให้ MN และ CN ยังสามารถสนทนาได้ เมื่อเกิดการย้ายข้ามเครือข่าย

ตารางที่ 4.1 การทดลองการใช้งานไม่ได้ ณ เวลาหนึ่ง

HA1	เวลา (นาที)	HA2	เวลา (นาที)
Up-ha1	0	Up-ha2	0
Fail	1	Check	1
Up-ha2	2	-	-
Check	10	Fail	10
-	-	Up-ha2	11
Fail	20	Check	20
Up-ha2	21	-	-
Check	30	Fail	30
-	-	Up-ha2	31

ตารางที่ 4.1 การทดลองการใช้งานไม่ได้ ณ เวลาหนึ่ง (ต่อ)

HA1	เวลา (นาที)	HA2	เวลา (นาที)
Fail	40	Check	40
Up-ha2	41	-	-
Check	50	Fail	50
-	-	Up-ha2	51



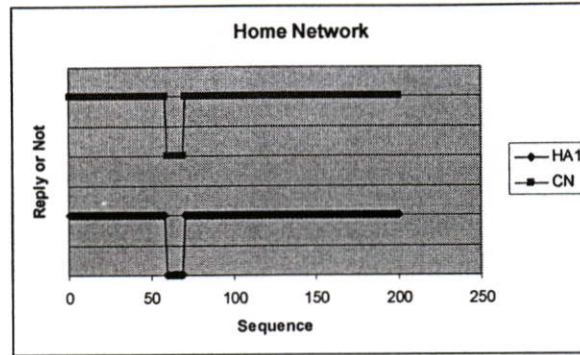
รูปที่ 4.6 การทำงานของการตรวจวัดสถานะของ HA

#### 4.6 ผลการทดลอง

ได้ทำการทดลองค่าเวลาคงอยู่ของ CN ที่ 60 วินาที แล้วทำการทดสอบดังตารางที่ 4.1 ใน 60 นาที แล้วนำข้อมูลมาวิเคราะห์

##### 4.6.1 โฮมเอเจนท์ใช้งานไม่ได้เมื่ออยู่ที่โฮม

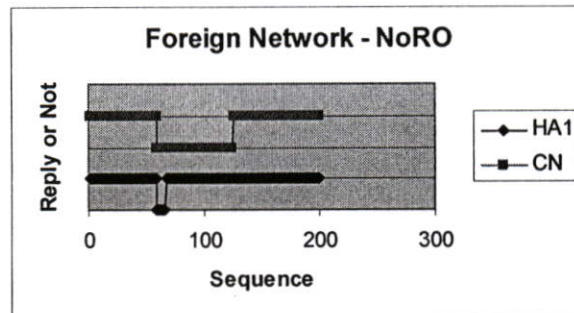
รูปที่ 4.7 แสดงสถานะ MN สนนทากับ CN ที่เครือข่ายบ้าน ซึ่งจะเห็นได้ว่าเมื่อ MN อยู่ที่เครือข่ายบ้านและได้ทำการติดต่อสนทนากับ CN เมื่อ HA1 ดายจะทำให้การสนทนาระหว่าง MN และ CN หยุดชะงักเพราะว่า HA1 ได้เป็นเกตเวย์ของ MN เพื่อส่งต่อข้อมูลไปหา CN



รูปที่ 4.7 สถานะ MN สนทนากับ CN ที่เครือข่ายบ้าน

#### 4.6.2 การใช้งานไม่ได้ของโฮมเอเจนต์เมื่ออยู่ต่างเครือข่ายและไม่ได้ใช้การจัดเส้นทางที่ดี

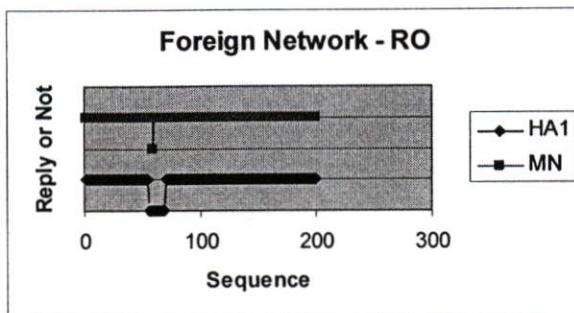
รูปที่ 4.8 แสดงสถานะ MN สนทนากับ CN ที่เครือข่ายอื่นและไม่ได้ใช้การจัดเส้นทางที่ดี เมื่อ MN อยู่ที่เครือข่ายอื่นและไม่ได้ใช้การจัดเส้นทางที่ดี จะได้กราฟคล้ายแบบที่อยู่บ้าน แต่การสนทนากันระหว่าง MN และ CN จะต้องรอเวลาคงอยู่ของ CN บวกไปอีก 60 วินาที



รูปที่ 4.8 สถานะ MN สนทนากับ CN ที่เครือข่ายอื่นและไม่ได้ใช้การจัดเส้นทางที่ดี

#### 4.6.3 การใช้งานไม่ได้ของโฮมเอเจนต์เมื่ออยู่ต่างเครือข่ายและใช้การจัดเส้นทางที่ดี

รูปที่ 4.9 แสดงสถานะ MN สนทนากับ CN ที่เครือข่ายอื่นและใช้การจัดเส้นทางที่ดี เมื่อ MN อยู่ที่เครือข่ายอื่นและใช้การจัดเส้นทางที่ดี การสนทนากันระหว่าง MN และ CN จะยังสื่อสารกันได้แม้ HA1 จะใช้งานไม่ได้ แต่เมื่อแลกเปลี่ยนข่าวสารกันแล้วและได้ทำการจัดเส้นทางที่ดี การคุยกันจะไม่ผ่านท่อของ HA1 การสื่อสารจึงต่อเนื่องไม่ขาดช่วง



รูปที่ 4.9 สถานะ MN สนทนากับ CN ที่เครือข่ายอื่นและใช้การจัดเส้นทางที่ดี

4.6.4 การวัดช่วงเวลาที่ใช้งานไม่ได้เมื่ออยู่นอกเครือข่ายบ้าน

ได้ทำการทดสอบโดย ping HA หลัจากเครื่อง MN ทิ้งไว้ ได้ทำการวัดการกู่กลับของ HA โดยทำการ ทำให้ HA1 ดายในทุก ๆ 10 นาที ทำการทดสอบจำนวน 5 ครั้ง โดยในโปรแกรมได้มีการ ประวิงค่าสำหรับการเช็ค ได้สู่มการเช็คตั้งแต่การเริ่มเช็คเมื่อเวลาผ่านไป 1 วินาที 30 วินาที และ 60 วินาที จะมีตัวแปรที่ศึกษาคือ

เวลาการใช้งานไม่ได้ (*Tdown*): เริ่มนับตั้งแต่ HA1 ดายจน HA2 กู่กลับเป็น HA1 แล้วตอบ กลับไปที่ MN

$$Tdown = A3 - A1 \tag{4.1}$$

เมื่อ *A1* เป็นเวลาที่ HA1 ดาย และ *A3* เป็นเวลาที่ HA2 กู่กลับเป็น HA1 แล้วตอบกลับไปที่ MN

เวลาตรวจพบของ HA1 ใช้งานไม่ได้ (*Tdetect*): เวลาที่ตรวจพบว่า HA1 ตัวหลักตายแล้ว HA2 สำรองขึ้นมาทำงานแทนที่ HA1 หลัก

$$Tdetect = A2 - A1 \tag{4.2}$$

เวลาการกู่กลับของระบบ (*Trestore*): เริ่มนับตั้งแต่รัน โปรแกรมตรวจสอบจนถึง HA2 กู่กลับ เป็น HA1 แล้ว ตอบกลับไปที่ MN

$$Trestore = A3 - A2 \tag{4.3}$$

เมื่อ *A2* เป็นเวลาที่รัน โปรแกรมตรวจสอบ

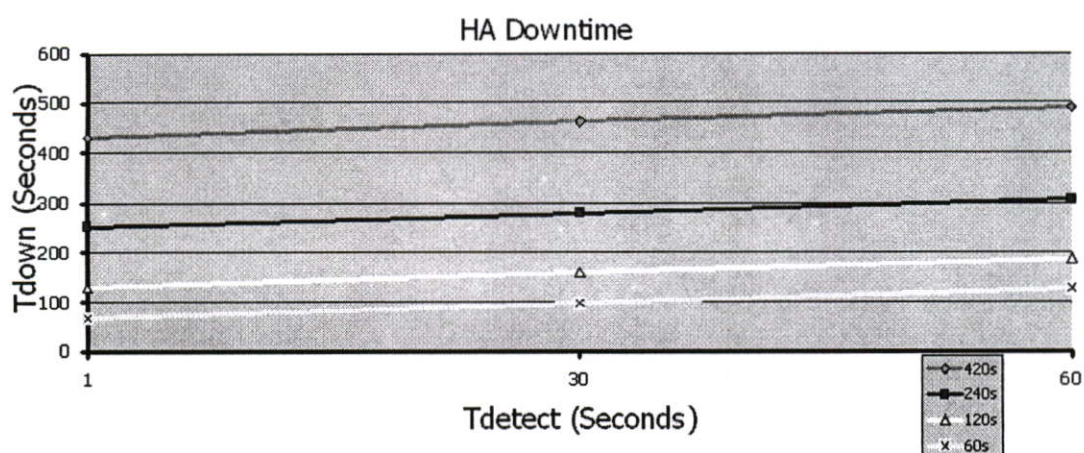
เวลาการกู่กลับของ HA (*Trecovery*): เป็นช่วงเวลาการแทนที่ของ HA2 ไปเป็น HA1

$$Trecovery = Trestore - Tlcn \tag{4.4}$$

ได้กำหนดให้ค่าคงอยู่ของ CN = 60, 120, 240 และ 420 วินาที ที่ HA1 จะรัน โปรแกรมแม่ข่าย

โดยเปิดพอร์ตไว้รอการเชื่อมต่อจาก HA2 โดยใช้โปรแกรม TCP แบบสัมพันธ์ 3 ทาง เชื่อมต่อกับแม่ข่ายที่อยู่กับ HA1 ถ้า HA1 ใช้งานไม่ได้ จะทำการแทนที่ตัวเองไปเป็น HA1

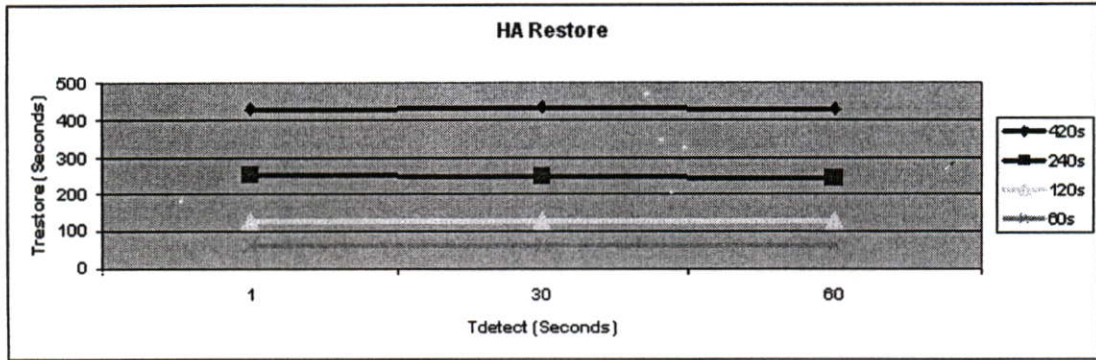
รูปที่ 4.10 แสดงการเปรียบเทียบการใช้งานไม่ได้ของระบบกับค่าเวลาดังอยู่ของ CN เวลาของการใช้งานไม่ได้ทั้งระบบจะแปรผันตรงระหว่างเวลาดังอยู่ของ CN กับ  $T_{down}$  และเวลาดังอยู่ของ CN จะแปรผันตรงกับช่วงเวลาที่เช็คค่าเริ่มการนับ เวลาดังอยู่ของ CN จะเกิดขึ้นเมื่อ MN ไม่สามารถติดต่อกับ HA1 ได้ โดยจะมีข้อความผิดพลาดว่าติดต่อไม่ได้เกิดขึ้น ในช่วงนั้นจะทำให้ MN ส่งข้อมูลเพื่อแจ้งสถานะไป CN ทำการเปลี่ยนค่าเวลาดังอยู่เป็น 0 เมื่อ MN คุยกับ HA1 ได้แล้วและทำการส่งข้อมูลเพื่อแจ้งสถานะไปหา HA1 ค่าคงอยู่ของ MN และ CN จะไม่เป็น 0 จะแปรผันตามค่าที่กำหนดไว้ในเวลาดังอยู่ของ CN



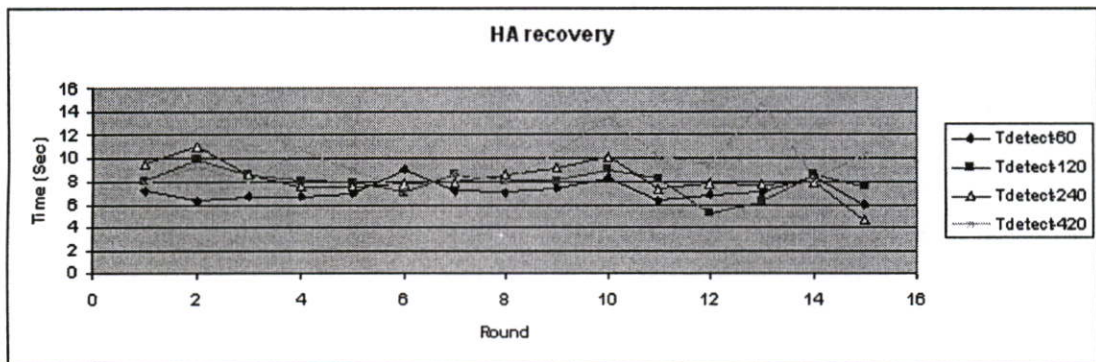
รูปที่ 4.10 เปรียบเทียบการใช้งานไม่ได้ของระบบกับค่าเวลาดังอยู่ของ CN

รูปที่ 4.11 แสดงการเปรียบเทียบค่าเวลาดังอยู่ของ CN เทียบกับค่าเวลาการกู้กลับของ HA ค่าเวลาการกู้กลับไม่แปรผันกับช่วงเวลาที่เช็ค อย่างไรก็ตาม การเปลี่ยนเวลาตรวจเจอการใช้งานไม่ได้ของ HA จาก 1 วินาที 30 วินาที และ 60 วินาที ค่าเวลาที่ใช้ในการกู้กลับไม่แตกต่างกัน ต่อมาได้ทำการเปลี่ยนค่าคงอยู่ของ CN เป็น 60, 120, 240 และ 420 วินาที และหาค่าเฉลี่ยในการใช้งานไม่ได้ 5 ครั้ง

ในรูปที่ 4.12 แสดงเวลาการกู้กลับของ HA ในแต่ละกรณี ค่าความน่าเชื่อถือของ HA1 และ HA2 ในการกู้กลับเมื่อใดตัวหนึ่งใช้งานไม่ได้จะอยู่ที่ค่าประมาณ 4 วินาทีจนถึง 16 วินาที แล้วหักจากค่าของโปรแกรมตรวจสอบอีก 2 วินาที ที่เผื่อไว้ 2 วินาทีเพราะรอให้ระบบปฏิบัติการทำการสร้างการเชื่อมต่อใหม่ แล้วถูกข่ายเชื่อมต่อได้ไม่เกิดการหยุดทำงานของโปรแกรม ค่าที่ได้จะเป็นค่าที่ใกล้เคียงกันแม้ว่าจะปรับค่าคงอยู่ของ CN เป็นค่า 60, 120, 240 และ 420 วินาทีแล้วก็ตาม



รูปที่ 4.11 การเปรียบเทียบค่าเวลาคงอยู่ของ CN เทียบกับค่าเวลาการกู้กลับของ HA



รูปที่ 4.12 เวลาการกู้กลับของ HA ในแต่ละกรณี

ตารางที่ 4.2 สรุปเวลาในการกู้กลับเพื่อใช้งานได้ตามปกติของกรณีที่ 4

กรณี 4	$T_{down}$ การติดต่อระหว่าง MN และ CN	$T_{restore}$ การติดต่อระหว่าง MN และ HA
ใช้งานเมื่ออยู่ที่บ้าน	~10 วินาที (ขึ้นอยู่กับ HA เพราะเป็นเกตเวย์ในเครือข่าย)	~10 วินาที
ใช้งานเมื่ออยู่นอกบ้านโดยไม่ได้ทำการจัดเส้นทาง	66 Sec (ขึ้นอยู่กับค่า life time CN) + กับช่วงเวลาทำงานแทนของตัวสำรอง ดังรูปที่ 4.10	~10 วินาที
ใช้งานเมื่ออยู่นอกบ้านโดยทำการจัดเส้นทาง	~1-2 วินาที (ขึ้นอยู่กับสภาพแวดล้อมของเครือข่ายในระดับเลเยอร์ 2)	~10 วินาที

ตารางที่ 4.2 แสดงการสรุปเวลาในการกู้กลับเพื่อใช้งานได้ตามปกติของกรณีที่ 4 ซึ่งเป็น การทำให้ระบบมีความน่าเชื่อถือ สร้างความมั่นใจให้กับผู้ดูแลระบบ ไม่ให้เกิดการใช้งานไม่ได้เป็น ระยะเวลาสั้นเมื่อ HA หลักใช้งานไม่ได้ ในกรณีนี้ได้สร้าง HA สำรองเพื่อสำรองไว้เมื่อ HA หลัก ตายหรือใช้งานไม่ได้ ซึ่งในวิทยานิพนธ์ฉบับนี้ได้ใช้หลักการของ TCP แบบสามพันธมิตร 3 ทาง [20] มา สร้างเป็นวิธีจัดการในการตรวจสอบ และแก้ไขเหตุการณ์ที่เกิดการใช้งานไม่ได้ขึ้นเป็นเวลานาน โดยมาวิเคราะห์หาค่าที่เป็นไปได้มากที่สุดที่จะทำให้การใช้งานไม่ได้สั้นสุดมาเปรียบเทียบกับ การเกิดการตายในช่วงเวลาต่าง ๆ เพื่อมาช่วยผู้ดูแลระบบ เช่น ถ้าให้มีการติดต่อกันระหว่าง MN และ CN โดยการจัดเส้นทางที่ดี การใช้งานไม่ได้ของ MN และ CN จะน้อยมากหรือแทบไม่มีเพราะ คุยกันโดยเส้นทางตรงไม่ต้องผ่านท่อส่งผ่านของ HA ในการจัดการเพื่อให้ระบบสามารถกลับมาใช้ งานได้ดั้งเดิม ผู้ดูแลระบบก็ควรเลือกให้เหมาะสมกับลักษณะของเครือข่าย

## บทที่ 5

### สรุปผลการวิจัย และข้อเสนอแนะ

ในวิทยานิพนธ์ฉบับนี้ได้นำเสนอวิธีการลดการล่าช้าของการย้ายข้ามเครือข่ายโดยทำการทดสอบปรับค่าตัวแปรต่าง ๆ ที่คิดว่ามีผลกระทบต่อ การย้ายข้ามเครือข่าย ได้นำวิธีการวัดเพื่อหาค่าเวลาที่ย้ายในแต่ละช่วงเพื่อดูว่าช่วงไหนใช้เวลาสำหรับดำเนินการมากที่สุด ซึ่งสามารถสรุปในแต่ละช่วงได้ดังนี้ คือ TD, TC TR และ TO จะเห็นได้ว่า TC จะมีค่ามากที่สุด ถ้าลด TC ได้จะสามารถลดเวลาการย้ายข้ามเครือข่ายได้เร็ว ซึ่งได้ทำการลดค่า TC โดยการลด DAD ซึ่งผลที่ได้เป็นไปตามสมมุติฐานที่ว่าถ้าลดการเช็การซ้ำกันของ IP ได้ก็จะลดเวลาในการตรวจสอบ IP ที่จะได้ในแต่ละเครือข่าย

การทดลองต่อมาในวิทยานิพนธ์ฉบับนี้คือการเพิ่มความน่าเชื่อถือให้กับระบบ เมื่อมีการย้ายข้ามเครือข่ายจะสามารถสร้างความน่าเชื่อถือให้กับระบบได้ มีการรับประกันการใช้งานให้ MN กับ CN ยังสามารถสนทนาติดต่อได้ตลอดการย้ายข้ามเครือข่าย ถึงแม้จะมี HA เกิดการใช้งานไม่ได้ก็ยังมี HA สำรองมาทำหน้าที่แทน ทำให้การติดต่อไม่หยุดชะงักไป

การตรวจสอบให้ได้เร็วที่สุดเมื่อเกิดมีการใช้งานไม่ได้ของ HA จึงได้ทำการศึกษาว่าถ้าเกิด HA ทำงานไม่ได้แล้วภายใน 1 วินาทีสามารถตรวจจับได้ว่า HA เกิดใช้งานไม่ได้ ภายใน 1 วินาทีสามารถรู้ทันทีเลยก็สามารถกู้กลับได้อย่างรวดเร็ว แต่ในความเป็นจริงถ้ามีการตรวจสอบทุกๆวินาทีก็จะมี การส่งข้อมูลกันอย่างมหาศาล ถ้าในเครือข่ายมีขนาดของการรับส่งข้อมูลไม่ใหญ่พอจะทำให้ในเครือข่ายเกิดความล่าช้าในการส่งข้อมูล

ในอนาคตการใช้งาน MIPv6 จะแพร่หลายมากขึ้น เนื่องจากมีความสะดวกที่ไม่ต้องปรับเปลี่ยน IP มีการใช้งานที่ต่อเนื่องเกิดการติดขัดที่น้อย ทำให้การทำงานค่อนข้างต่อเนื่อง ในวิทยานิพนธ์ฉบับนี้ได้ศึกษาวิธีการลดค่าความล่าช้าของการย้ายข้ามเครือข่ายในแต่ละกรณี นำมาวิเคราะห์เพื่อหาแนวทางในการลดการล่าช้าของการย้ายข้ามเครือข่าย ช่วยลดการเกิดความซ้ำซ้อนในการจัดการเครือข่าย การลดจำนวนการส่งแพ็กเก็ตที่ส่งคู่กัน และการป้องกันการเกิดความหนาแน่นในเครือข่าย

จากที่กล่าวมาข้างต้นสามารถสรุปเป็นประเด็นหลักได้ 4 ประเด็นดังนี้คือ

1. ความล่าช้าในการย้ายข้ามเครือข่ายในแบบปรับเปลี่ยค่ามากที่สุดและค่าน้อยสุดของ RA
2. ความล่าช้าในการย้ายข้ามเครือข่ายในแบบที่มีการปรับเปลี่ยค่า RS
3. ความล่าช้าในการย้ายข้ามเครือข่ายในแบบที่มีการเช็ค DAD
4. การป้องกันการเกิดการใช้งานไม่ได้เมื่อ HA หลักตายสามารถกู้กลับได้อย่างรวดเร็ว

ปัญหาที่พบคือโปรแกรมหยุดทำงาน ต้องทำการปิดโปรแกรมแล้วเริ่มการทำงานการเชื่อมต่อของระบบปฏิบัติการใหม่ แล้วทำการเปิดโปรแกรมใหม่เพื่อให้ใช้งานได้ดังเดิม บางครั้งการสร้างท่อส่งผ่านกรอบเพื่อแลกเปลี่ยนเส้นทางระหว่าง MN และ CN ค้าง เมื่อย้ายกลับมาที่บ้าน HA ต้องปิดท่อส่งผ่านที่ HA ก่อนจึงจะสามารถใช้งานได้

แนวทางการพัฒนาต่อไปคือพัฒนาวิธีที่สามารถลดเวลาการย้ายข้ามเครือข่ายโดยการปรับ DAD หรือให้การใช้ช่วงเวลา TC น้อยลงหรือการใช้ช่วง TD ให้สามารถตรวจพบ IP ได้เร็วขึ้น ก็สามารถลดการล่าช้าในการย้ายข้ามเครือข่ายได้ อีกทั้งการสร้างความน่าเชื่อถือให้กับระบบการย้ายข้ามเครือข่ายให้สามารถย้ายได้อย่างต่อเนื่อง สามารถรับรู้ตัวพักข้อมูลที่ส่งไปแล้วของ HA เก่า ก่อนที่ HA เก่าจะไม่สามารถใช้งานได้

การคาดการณ์ได้ก่อนที่ HA จะใช้งานไม่ได้ทำให้สามารถกู้กลับได้เร็วขึ้น มีการเคลื่อนย้ายได้อย่างรวดเร็วและราบรื่นไม่เกิดการสะดุด

## เอกสารอ้างอิง

- [1] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
- [2] V. Devarapalli, R. Wakikawa and P. Thubert, "Local HA to HA protocol", draft-devarapalli-mip6-nemo-local-haha-01.txt, March 2006.
- [3] R. Wakikawa, P. Thubert and V. Devarapalli "Inter Home Agents Protocol Specification", draft-wakikawa-mip6-nemo-haha-spec-01.txt, March 2006.
- [4] J. Faizan, H. El-Rewini and M. Khalil, "Virtual Home Agent Reliability Protocol for Mobile IPv6 based Networks," 2005 International Conference on Wireless Networks, Communications and Mobile Computing, vol. 2, pp. 1295 – 1300, June 2005.
- [5] MIPv6 Analyzer, <http://www.cavone.com/mipv6-analyzer>.
- [6] W. Werapun and A. Unakul, "An Experimental Mobile IPv6 For Linux Testbed System", NCSEC2003, pp. 403-405 September 2003.
- [7] MIPv6 Testing Report, SCE, Nanyang Technological University, NTU-test-report.
- [8] A network protocol analyzer, [www.ethereal.com](http://www.ethereal.com).
- [9] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460, December 1998.
- [10] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," RFC 2461, December 1998.
- [11] Mobile IPv6 for Linux, <http://www.mobile-ipv6.org>.
- [12] Kame IPv6, <http://www.kame.net>.
- [13] Nectec Mobile IPv6 TestBed, [www.ipv6.nectec.or.th/~zpop/mipv6](http://www.ipv6.nectec.or.th/~zpop/mipv6).
- [14] Usage Website, <http://www.nautilus6.org/doc/misc-network-mobility-jsf-20040913-KuntzR.pdf>.
- [15] P. Pongpaibool, C. Chan-in, A. Busaranun, C. Charnsripinyo, "Prepare Next Generation Internet", NAC2005, March 2005.
- [16] Conta, A. And S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," RFC 2463, December 1998.
- [17] Linux IPv6 Router Advertisement Daemon (radvd), <http://www.litech.org/radvd/>.
- [18] DHCPv6 @ Sourceforge, <http://dhcpv6.sourceforge.net/>.
- [19] Transmission Control Protocol, <http://www.scit.wlv.ac.uk/~jphb/comms/tcp.html>.

## ภาคผนวก ก.

## โปรแกรมที่ใช้ในการเคลื่อนที่ MIPv6

## โปรแกรม MIPv6 HA (Home Agent)

```
# This is an example of mip6d Home Agent configuration file

NodeConfig HA;

## If set to > 0, will not detach from tty
DebugLevel 10;

## List of interfaces where we serve as Home Agent
#Interface "eth0";
Interface "eth1";

#DoRouteOptimizationCN disabled;
#DoRouteOptimizationMN disabled;
##
## IPsec configuration
##

UseMnHaIPsec disabled;

## Key Management Mobility Capability
KeyMngMobCapability disabled;
```

### โปรแกรม MIPv6 MN (Mobile Node)

```
# This is an example of mip6d Mobile Node configuration file

NodeConfig MN;

## If set to > 0, will not detach from tty
DebugLevel 10;

## Support route optimization with other MNs
DoRouteOptimizationCN enabled;

## Use route optimization with CNs
DoRouteOptimizationMN enabled;

UseCnBuAck disabled;

Interface "eth0" {
    MnIfPreference -1;
}
MnRouterProbesRA 1;
MnRouterProbesLinkUp 0;

MnHomeLink "eth0" {
    HomeAgentAddress 2001:f00:1fff:2::2;
    HomeAddress 2001:f00:1fff:2::3/64;
}

##
## IPsec configuration
##

UseMnHaIPsec disabled;

## Key Management Mobility Capability
KeyMngMobCapability disabled;
```

### โปรแกรม MIPv6 CN (Corresponding Node)

```
# This is an example of mip6d Correspondent Node configuration file

NodeConfig CN;

## If set to > 0, will not detach from tty
DebugLevel 10;

## Support route optimization with MNs
DoRouteOptimizationCN enabled;
```

### โปรแกรม Ethereal ตรวจสอบ ICMPv6 Protocol

No.	Time	Source	Destination	Protocol	Info
880	122.114397	2001:f00:1fff:2::3	2001:f00:1fff:2::2	ICMPv6	Echo request
Frame 880 (118 bytes on wire, 118 bytes captured)					
Ethernet II, Src: 00:0b:fd:c6:4f:a3, Dst: 00:05:5d:50:70:2d					
Internet Protocol Version 6					
Version: 6					
Traffic class: 0x00					
Flowlabel: 0x00000					
Payload length: 64					
Next header: ICMPv6 (0x3a)					
Hop limit: 64					
Source address: 2001:f00:1fff:2::3 (2001:f00:1fff:2::3)					
Destination address: 2001:f00:1fff:2::2 (2001:f00:1fff:2::2)					
Internet Control Message Protocol v6					

### โปรแกรม Ethereal ตรวจสอบ RA

No.	Time	Source	Destination	Protocol	Info
881	122.489766	fe80::205:5dff:fe50:702d	ff02::1	ICMPv6	Router advertisement
Frame 881 (110 bytes on wire, 110 bytes captured)					
Ethernet II, Src: 00:05:5d:50:70:2d, Dst: 33:33:00:00:00:01					
Internet Protocol Version 6					
Version: 6					
Traffic class: 0x00					
Flowlabel: 0x00000					
Payload length: 56					
Next header: ICMPv6 (0x3a)					
Hop limit: 255					
Source address: fe80::205:5dff:fe50:702d (fe80::205:5dff:fe50:702d)					

### โปรแกรม Ethereal ตรวจสอบ RA (ต่อ)

Destination address: ff02::1 (ff02::1)
Internet Control Message Protocol v6

### โปรแกรม Ethereal ตรวจสอบ NS

No.	Time	Source	Destination	Protocol	Info
885	122.637295	::	ff02::1:ffc6:4fa3	ICMPv6	Neighbor solicitation
Frame 885 (78 bytes on wire, 78 bytes captured)					
Ethernet II, Src: 00:0b:fd:c6:4f:a3, Dst: 33:33:ff:c6:4f:a3					
Internet Protocol Version 6					
Version: 6					
Traffic class: 0x00					
Flowlabel: 0x00000					
Payload length: 24					
Next header: ICMPv6 (0x3a)					
Hop limit: 255					
Source address: :: (::)					
Destination address: ff02::1:ffc6:4fa3 (ff02::1:ffc6:4fa3)					
Internet Control Message Protocol v6					

### โปรแกรม Ethereal ตรวจสอบ MIPv6 Binding Update

No.	Time	Source	Destination	Protocol	Info
882	122.491212	2001:f00:1fff:7:20b:fdff:fec6:4fa3	2001:f00:1fff:2::2	MIPv6	Binding Update
Frame 882 (110 bytes on wire, 110 bytes captured)					
Ethernet II, Src: 00:0b:fd:c6:4f:a3, Dst: 00:05:5d:50:70:2d					
Internet Protocol Version 6					
Version: 6					
Traffic class: 0x00					

## โปรแกรม Ethereal ตรวจสอบ MIPv6 Binding Update (ต่อ)

Flowlabel: 0x00000

Payload length: 56

Next header: IPv6 destination option (0x3c)

Hop limit: 64

Source address: 2001:f00:1fff:7:20b:fdff:fec6:4fa3 (2001:f00:1fff:7:20b:fdff:fec6:4fa3)

Destination address: 2001:f00:1fff:2::2 (2001:f00:1fff:2::2)

### Destination Option Header

Next header: Mobile IPv6 (0x87)

Length: 2 (24 bytes)

PadN: 4 bytes

Option Type: 201 (0xc9) - Home Address Option

Option Length : 16

Home Address : 2001:f00:1fff:2::3 (2001:f00:1fff:2::3)

### Mobile IPv6

Payload protocol: IPv6 no next header (0x3b)

Header length: 3 (32 bytes)

Mobility Header Type: Binding Update (5)

Reserved: 0x00

Checksum: 0x7e3e

### Binding Update

Sequence number: 16768

1... .... = Acknowledge (A) flag: Binding Acknowledgement requested

.1.. .... = Home Registration (H) flag: Home Registration

..0. .... = Link-Local Compatibility (L) flag: No Link-Local Address Compatibility

...0 .... = Key Management Compatibility (K) flag: No Key Management Mobility

### Compatibility

Lifetime: 65535 (262140 seconds)

### Mobility Options

PadN: 2 bytes

### โปรแกรม Ethereal ตรวจสอบ MIPv6 Binding Update (ต่อ)

Alternate care-of address: 2001:f00:1fff:7:20b:fdff:fec6:4fa3  
(2001:f00:1fff:7:20b:fdff:fec6:4fa3)

### โปรแกรม Ethereal ตรวจสอบ MIPv6 Binding Acknowledgement

No.	Time	Source	Destination	Protocol	Info
1002	138.118354	2001:f00:1fff:5::2	2001:f00:1fff:7:20b:fdff:fec6:4fa3	MIPv6	Binding Acknowledgement

Frame 1002 (110 bytes on wire, 110 bytes captured)

Ethernet II, Src: 00:05:5d:50:70:2d, Dst: 00:0b:fd:c6:4f:a3

Internet Protocol Version 6

Version: 6

Traffic class: 0x00

Flowlabel: 0x00000

Payload length: 56

Next header: IPv6 routing (0x2b)

Hop limit: 62

Source address: 2001:f00:1fff:5::2 (2001:f00:1fff:5::2)

Destination address: 2001:f00:1fff:7:20b:fdff:fec6:4fa3

(2001:f00:1fff:7:20b:fdff:fec6:4fa3)

Routing Header, Type 2

Next header: Mobile IPv6 (0x87)

Length: 2 (24 bytes)

Type: 2

Segments left: 1

Home Address : 2001:f00:1fff:2::3 (2001:f00:1fff:2::3)

Mobile IPv6

Payload protocol: IPv6 no next header (0x3b)

Header length: 3 (32 bytes)

Mobility Header Type: Binding Acknowledgement (6)

Reserved: 0x00

Checksum: 0xe8cf

Binding Acknowledgement

Status: Binding Update accepted (0)

0... .... = Key Management Compatibility (K) flag: No Key Management Mobility

Compatibility

Sequence number: 50281

Lifetime: 105 (420 seconds)

Mobility Options

PadN: 6 bytes

Binding Authorization Data

Authenticator: B06C1945DE53E9FC278FB304

## โปรแกรม Ethereal ตรวจสอบ Route Optimization โดยใช้ Routing Type 2

No.	Time	Source	Destination	Protocol	Info
909	125.120647	2001:f00:1fff:2::2	2001:f00:1fff:7:20b:fdff:fec6:4fa3	ICMPv6	Echo reply
Frame 909 (142 bytes on wire, 142 bytes captured)					
Ethernet II, Src: 00:05:5d:50:70:2d, Dst: 00:0b:fd:c6:4f:a3					
Internet Protocol Version 6					
Version: 6					
Traffic class: 0x00					
Flowlabel: 0x000000					
Payload length: 88					
Next header: IPv6 routing (0x2b)					
Hop limit: 62					
Source address: 2001:f00:1fff:2::2 (2001:f00:1fff:2::2)					
Destination address: 2001:f00:1fff:7:20b:fdff:fec6:4fa3 (2001:f00:1fff:7:20b:fdff:fec6:4fa3)					
Routing Header, Type 2					
Next header: ICMPv6 (0x3a)					
Length: 2 (24 bytes)					
Type: 2					
Segments left: 1					
Home Address : 2001:f00:1fff:2::3 (2001:f00:1fff:2::3)					
Internet Control Message Protocol v6					

## โปรแกรมที่ใช้ใน HA หลัก

```
#!/bin/perl -w
use IO::Socket::INET6;
my $sock = IO::Socket::INET6->new(Listen    => 1,
                                  LocalAddr => ':::',
                                  LocalPort => 9876,
                                  Reuse     => 1,
                                  Proto    => 'tcp');
die "Could not create socket: $!\n" unless $sock;
my $new_sock = $sock->accept();
while(1) {
    # $new_sock->recv($text,128);
    # if($text ne ''){
    #   print "\nReceived message '", $text, "'\n";
    # }
}
# close($sock);
```

## โปรแกรมที่ใช้ใน HA สำรอง

```
#!/bin/perl -w
use IO::Socket::INET6;
my $sock = IO::Socket::INET6->new(
                                  PeerAddr => 'hal',
                                  PeerPort => 9876,
                                  Proto    => 'tcp');
die "Could not create socket: $!\n" unless $sock;
# print $sock "Hello World!\n";
close($sock);
```

## ภาคผนวก ข.

## ผลงานวิจัยที่ได้รับการตีพิมพ์ในวิทยานิพนธ์

1. **A. Busaranun**, P. Pongpaibool and P. Supanakoon, "Handover Performance of Mobile IPv6 on Linux Testbed", Electrical Engineering, Computer, Telecommunications, and Information Technology Association Annual Conferences (ECTI-CON 2006), pp. 384-387, Ubon Ratchathani, 10-13 May 2006.
2. **A. Busaranun**, P. Pongpaibool and P. Supanakoon, "Simple Implement of Home Agent Reliability for Mobile IPv6 Network", Have been published in The International Conference on Analog and Digital Techniques in Electrical Engineering (TENCON 2006), HONG KONG, 14-17 November 2006.

# ECTI-CON 2006

THE 2006 ECTI INTERNATIONAL CONFERENCE



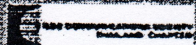
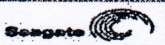
ECTI  
2006

## Enter to the Proceeding

Proceedings of the 2006 Electrical Engineering/ Electronics, Computer, Telecommunications and Information Technology (ECTI) International Conference

May 10-13, 2006

Ubonburi Hotel, Ubon Ratchathani, THAILAND



# Handover Performance of Mobile IPv6 on Linux Testbed

Adisak Busaranun<sup>1</sup>, Panita Pongpaibool<sup>2</sup> And Pichaya Supanakoon<sup>1</sup>

<sup>1</sup>Department of Information Engineering, Faculty of Engineering

King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, THAILAND.

E-mail: {s7061116,kspichay}@kmitl.ac.th

<sup>2</sup>Next Generation Internet Laboratory, National Electronics and Computer Technology Center,  
112 Thailand Science Park, Phahol Yothin Road, Klong Luang, Pathumthani 12120, THAILAND.

E-mail: panita@nectec.or.th

## ABSTRACT

This paper studies the handover procedure of mobile IPv6 and investigates various factors affecting the delay during inter-network handover. The experiments are performed over three wireless LAN networks using Mobile IPv6 for Linux (MIPL) implementation. The goal is recommend guidelines for parameter setting such that the handover delay is minimized.

Keywords: IPv6, Mobile IPv6, handover delay

## 1. INTRODUCTION

IPv6 will play an important role in the future Internet communications. IPv6, with its 128-bit addresses, will significantly increase the Internet address space over the current 32-bit address space of IPv4. The large address space will accommodate rapid growth of the Internet by allowing virtually every device in the world to have a distinct IP address. Apart from the large address space, IPv6 simplifies network management tasks through address auto-configuration and hierarchical route management.

One potential use of IPv6 is for mobile application. The next generation network is expected to be dominated by mobile devices. Typically, when a mobile node (MN) moves to a new network, its IP address must change accordingly. This causes existing TCP/IP connections to terminate. The MN must re-establish the connection in order to continue the conversation. Mobile IPv6 protocol [1] is designed to solve this problem by allowing the MN to continue receiving packets through existing connections and remain reachable while roaming to a new network.

Although TCP/IP connections are not terminated during the movement, there is a brief period of disruption. This is the time required for the MN to register its new location with an agent in its home network who will later forward the packets destined to MN to the new location. We call this disruption period *handover delay*.

In this paper, we study handover delay performance of mobile IPv6 when MN moves among three networks. The experiments use Mobile IPv6 for Linux (MIPL) implementation. The goals of our study are to identify factors affecting the handover delay and to recommend guidelines for setting these parameters such that the handover delay is minimized.

## 2. PREVIOUS WORK

Many articles propose new techniques and enhancements to reduce the handover delay in mobile IPv6 [2]. It is not our goal here to modify the existing mobile IPv6 standard. However, we want to work with the current mobile IPv6 standard (RFC 3775) and investigate rules or guidelines for network administrators to improve handover performance of their mobile IPv6 services.

This work focuses on mobile IPv6 implementation on Linux. Previous reports on real measurements of mobile IPv6 handover performance on Linux testbed include [3][4][5]. However, none of these reports uses a complete implementation of RFC 3775. For example, the measurements in [3] do not consider delay for route optimization, and the implementation used by [4] and [5] do not implement return routability. Moreover, the measurements in [4] are very coarse grained since it measures the delay using ping packets. Although measurements in [3][5] use packet capture tool to capture arrival time of all packets, both did not specify exact starting point of the handover delay. Our measurements include all steps in the standard mobile IPv6 handover, including route optimization and return routability. We use Ethereal software to capture the fine-grain time interval, and we control the starting time of each movement so that we know exactly when each movement begins.

## 3. MOBILE IPV6 HANDOVER

Mobile IPv6 manages movement of the MN by identifying each MN with its static home address (HoA), regardless of its location in the Internet. The original network where the MN belongs to is called *home network*. When the MN moves away from home, it must send information about its new location and new IP address to a *home agent* (HA) in the home network. The home agent can then intercept and forward packets to the MN at the new location. The new address of MN at a *foreign network* is called *care-of address* (CoA).

The signaling process during the mobile IPv6 handover is illustrated in Fig. 1. After the MN moves to the foreign network, it will create a CoA using a prefix received in the router advertisement message. The MN then performs duplicate address detection (DAD) to check validity of this new address. Once the CoA is configured, the mobile IPv6 signaling starts. MN registers its CoA with HA via the *binding update message*. HA confirms the registration with

*binding acknowledgement*. At this point MN can continue to receive packets from existing connections. However, the communication between MN and its corresponding node (CN) must go through a HA tunnel. To create a direct route between MN and CN, MN must initiate a route optimization procedure. This procedure begins with a return routability process, whereby MN and CN exchange a pair of keys to authenticate each other. One key is exchanged via the HA tunnel using Home Test Init (HoTI) and Home Test (HoT) messages. The other key is exchanged directly between MN and CN using Care-of Test Init (CoTI) and Care-of Test (CoT) messages. Afterwards, MN can register its CoA directly with CN using binding update and binding acknowledgement messages.

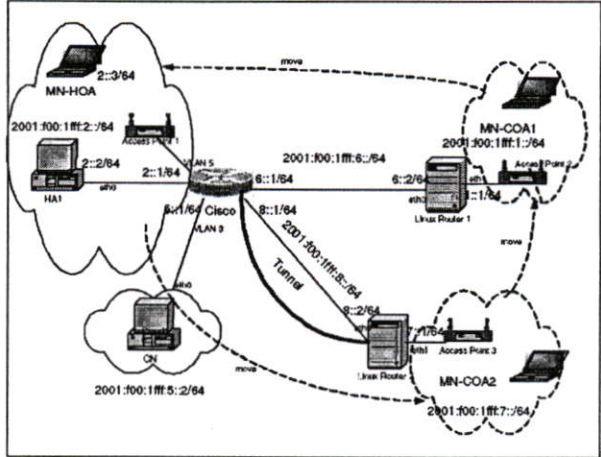


Fig.2: Our mobile IPv6 testbed configuration

4. EXPERIMENTS

4.1 Mobile IPv6 Testbed

Our testbed consists of three wireless LAN networks interconnected as shown in Fig. 2. All devices, except access points and Cisco router, use Linux TLE 7.0 (Fedora Core-based, Linux kernel 2.6.11). The MN, HA, and CN use Mobile IPv6 for Linux (MIPL) version 2 RC 3 patches [6]. The MIPL configurations for MN, HA, and CN follow those in [7].

4.2 Handover Delay Measurements

In our experiments, we force the MN to switch between three access points—from home network to one foreign network to another foreign network, and back to the home network. We measure the handover delay starting from the time the MN starts moving until the completion of route optimization. We identify four components of mobile IPv6 handover delay as follows.

*Movement detection time (Td)*: this is the time required by the MN to detect and establish that it has moved to a new point of attachment (i.e. the discovery of a new on-link router).

*Address configuration time (Tc)*: this is the time required to configure a new globally routable IPv6 address on the MN. This includes duplicate address detection (DAD) period.

*Binding registration time (Tr)*: this is the time between the dispatch of a binding update signal from MN to HA and the receipt of a binding acknowledgement signal from HA.

*Route optimization time (To)*: this is the time required to register the new IPv6 address with the CNs. This includes the return routability procedure which, if used, must occur before a binding update is sent by the MN to a CN. Therefore, the overall handover delay (Th) is

$$Th = Td + Tc + Tr + To.$$

We use Ethereal packet capture software and mark packet arrival time for each delay component. For *Td*, we mark the execution time of the "iwconfig" command and the time MN receives the first router advertisement message from a foreign router. For *Tc*, we measure the period after router advertisement message arrives until MN sends out the binding update to HA. *Tr* is thus the period between the sending of binding update and the receipt of binding acknowledgement from HA. At this point, traffic can resume. However, the mobile IPv6 handover continues to set up a direct route between MN and CN. Therefore, *To* is measured up to the time MN receives the binding acknowledgement from CN. Fig. 3 shows a sample packet trace from Ethereal and the marking of each delay component. Note that due to current bugs in the MIPL v.2 RC3, we need to turn off the binding acknowledgement message from CN [6]. Thus, in our experiments, *To* is measured up to the time the binding update is sent from MN to CN.

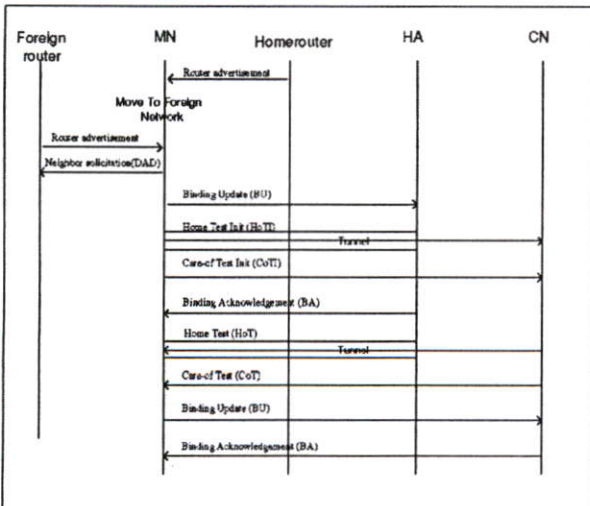


Fig.1: Signaling messages during mobile IPv6 handover

5. RESULTS

The delay results presented in this section are averaged over at least 15 movement trials. HoA to CoA2 indicates the movement from home network to the first foreign network. CoA2 to CoA is the movement between two foreign networks, and CoA to HoA is the movement from the second foreign network to home network. Unless noted other-

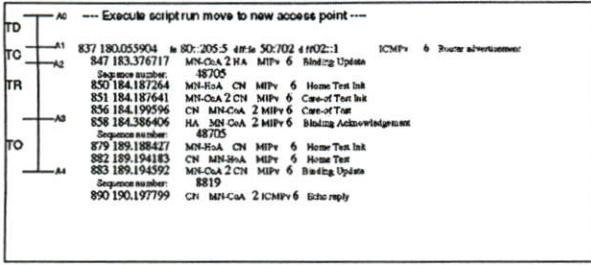


Fig. 3: Packet traces during mobile IPv6 handover

Table 1: Default Mobile IPv6 Parameters

MinRtrAdvInterval	3 s
MaxRtrAdvInterval	10 s
Router solicitations	3 s
Router solicitation interval	4 s
Router solicitation delay (random delay)	1 s
DAD RetransTimer	1000 ms
DupAddrDetectTransmit	1(enable)
UseMnHalPsec	Disabled
DoRouteOptimizationMN	Enabled
DoRouteOptimizationCN	Enabled

wise, the mobile IPv6 parameters are configured with the default values (see Table 1).

### 5.1 Movement direction vs. Delay Components

Fig. 4 compares handover delay component in each movement direction. We set the router advertisement interval at minimum, between 0.03 and 0.07 seconds. The handover delay is longest when MN moves out of home network and shortest when MN returns home. This difference is due to the return routability procedure which occurs during route optimization. When MN first moves away from home network, it has to exchange two keys with CN, one via the HA tunnel and the other via the direct path. However, when MN returns home, it does not have to exchange any key [1]. In addition, we find the movement between two foreign networks also requires less time. Looking at packet traces, we find that it is because MN exchanges only the CoTI/CoT messages with CN, and not the HoTI/HoT messages.

Another point worth noting is that the address configuration time ( $T_c$ ) dominates a significant portion of the handover delay, approximately 2 seconds. This is certainly the effect of DAD procedure since by default MN must wait at least 1000 ms of DAD *RetransTimer*.

### 5.2 Effect of Router Advertisement Interval

In the second set of experiments, we consider the effect of router advertisement interval on movement detection time ( $T_d$ ) and on the overall handover delay ( $T_h$ ). On Linux routers, the period between each router advertisement message is randomly selected between the *MinRtrAdvInterval* and *MaxRtrAdvInterval*. First, we try the default interval of (3,10). Fig. 5a shows  $T_d$  scattering be-

tween 2-12 seconds, and  $T_h$  growing at a linear proportion with  $T_d$ , with the slope of approximately 1. This means that to reduce  $T_h$  we should reduce  $T_d$ , and hence reduce router advertisement interval. Moreover, the difference between each movement direction also prevails as in Fig. 4, i.e., handover from home network takes longer than handover from foreign network. To confirm this finding, we try a different router advertisement interval. Fig. 5b shows a scatter plot for the interval of (0.1,0.5). A brief glance confirms that similar relationship exists in both Fig. 5a and Fig. 5b. However, to our surprise, reducing router advertisement interval does not always reduce  $T_d$ . The  $T_d$  values in Fig. 5b are distributed in the range of 0.6-1.7 seconds. As we further vary the router advertisement interval, we find  $T_d$  never goes below 0.5 second. We suspect that this 0.5 second overhead is probably due to layer 2 handover. This finding agrees with the finding in [4]. Therefore, at this point we conclude that the router advertisement interval should never be set below 0.5 second since it does not help reduce the handover delay.

### 5.3 Effect of Router Solicitation Interval

Fig. 6 (case 1) measures the average handover delay for different router advertisement intervals. This figure confirms that reducing router advertisement interval below 0.5 second does not help reduce  $T_h$ . So we investigate other ways to reduce  $T_h$  further. Without waiting for a router advertisement, MN may send a router solicitation message to request a router prefix directly. Fig. 6 (case 2) compares the handover delay when the router solicitation ( $R_s$ ) is reduced from the default 3 seconds to 1 second, router solicitation interval from 4 seconds to 1 second, and router solicitation delay from 1 second to 0. As expected, reducing  $R_s$  will reduce  $T_h$ . Although, time saved by using router solicitation is quite small, the bandwidth saving (for not having to send out router advertisement too frequently) could be significant, especially in networks with a small numbers of nodes.

### 5.4 Effect of Duplicate Address Detection

As we mention in Section 5.1 that a significant portion of  $T_h$  is due to  $T_c$ . In order to reduce  $T_c$ , we experiment with the DAD procedure. Typically, MN must perform DAD by sending a neighbor solicitation message with a destination being the MN's new address. If no node replies within *RetransTimer*, MN can assume the new address is unique on that network. In our testbed, DAD procedure will take at least 1 second which is the default *RetransTimer*. Fig. 6 (case 3) measures  $T_h$  when we turn off DAD on MN. It shows benefit of  $T_h$  reduction exists under all ranges of router advertisement intervals. However, turning off DAD is only acceptable in a small network where address assignment is based on EUI-64 (use MAC address), and only one router advertises the prefix. In a large network, it is not recommended because we may not have a complete control on address assignment strategies of all nodes.

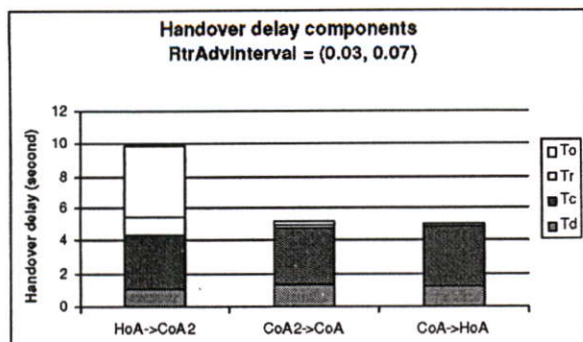


Fig. 4: Comparison of delay component in different movement direction

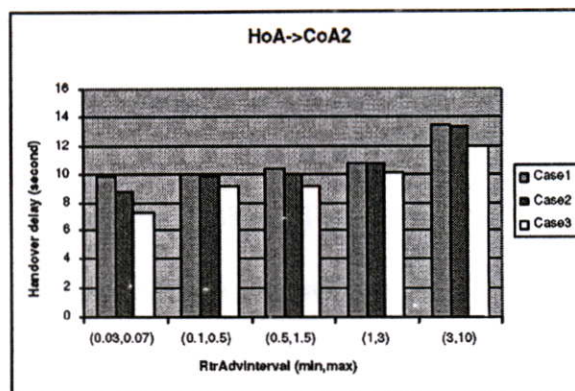


Fig. 6: of router advertisement interval, router solicitation interval and duplicate address detection

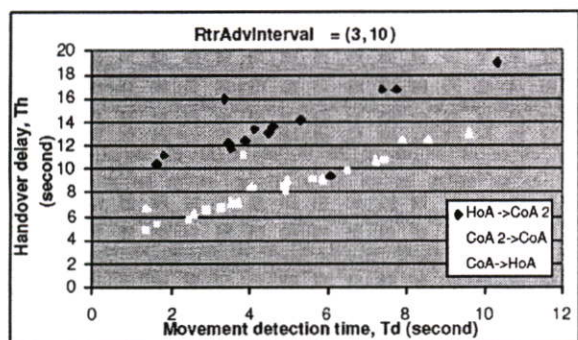


Fig. 5a

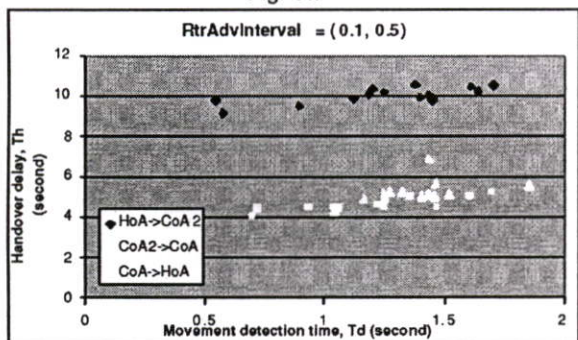


Fig. 5b

Fig. 5: Relationship of movement detection time and handover delay under different router advertisement intervals

## 6. CONCLUSION AND FUTURE WORK

This paper studies the mobile IPv6 handover operation on a Linux IPv6 testbed, and evaluates factors that affect the handover delay. In particular, we investigate the effects of movement direction, router advertisement interval, router solicitation interval, and duplicate address detection procedure. We find the handover delay when MN first moves out of home network to be much longer than the delay when MN returns home, due to the return routability procedure. Moreover, we find the handover delay to be directly proportional to the router advertisement interval. But the benefit of reducing router advertisement interval is only evident for the interval of more than 0.5 second.

Below 0.5 second, the overhead of lower-layer handover becomes dominant. In addition, router solicitation interval and duplicate address detection delay can help reduce the handover delay further. However, we do not recommend skipping DAD unless in a controlled testbed. In conclusion, the findings presented in this paper only apply to small networks. More studies are required to come up with guidelines for a large network environment.

Our future work includes scalability study of the MIPL implementation. We need to evaluate whether the mobile IPv6 MIPL is ready to be deployed in a campus or enterprise networks where WLAN exists. In addition, we plan to study new techniques for reducing DAD delay without turning off DAD completely.

## References

- [1] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
- [2] N. Montavont and T. Noel, Handover management for Mobile Nodes in IPv6 Networks, IEEE Communication Magazine:38-43, August 2002.
- [3] P. Cavone, MIPv6 Analyzer, <http://www.cavone.com/mip6-analyzer>.
- [4] W. Werapun and A. Unakul, An Experimental Mobile IPv6 For Linux Testbed System, NCSEC2003, September 2003.
- [5] MIPv6 Testing Report, SCE, Nanyang Technological University, NTU-test-report.
- [6] Mobile IPv6 for Linux, <http://www.mobile-ipv6.org>.
- [7] A. Busaranun, Mobile IPv6 for Linux HOWTO, <http://www.ipv6.nectec.or.th/zpop/mip6/>.
- [8] P. Pongpaibool, C.Chan-in, A. Busaranun, C. Charnsripiyo, "Prepare Next Generation Internet", NAC2005, March 2005.
- [9] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.
- [10] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.
- [11] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.
- [12] Conta, A. and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 2463, December 1998.
- [13] M. Crawford "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.
- [14] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 2373, July 1998.
- [15] Nectec Linux TLE, [www.opentle.org](http://www.opentle.org).
- [16] A network protocol analyzer, [www.ethereal.com](http://www.ethereal.com)

# Simple Implement of Home Agent Reliability for Mobile IPv6 Network

Adisak Busaranun<sup>1</sup>, Panita Pongpaibool<sup>3</sup> and Pichaya Supanakoon<sup>1,2</sup>

<sup>1</sup>Department of Information Engineering, Faculty of Engineering,

<sup>2</sup>Research Center for Communications and Information Technology (ReCCIT)  
King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, THAILAND  
{s7061116, kspichay}@kmitl.ac.th

<sup>3</sup>Next Generation Internet, National Electronics and Computer Technology Center  
112 Phahol Yothin Rd, Klong Luang, Pathumthani 12120, THAILAND  
panita@nectec.or.th

## Abstract

*This paper studies the home agent (HA) reliability with TCP. The experiments are performed with two HAs and a backup HA. When the main mobile IPv6 HA fails, the backup HA is used for standby and recovery services instead. The goal of this paper is to minimize the recovery time.*

*Keywords: IPv6, mobile IPv6, home agent (HA).*

## 1. Introduction

IPv6 will play an important role in the future Internet communications. IPv6, with its 128-bit address spaces, will significantly increase the Internet address space over the current 32-bit address spaces of IPv4. The large address spaces will accommodate rapid growth of the Internet by allowing virtually every device in the world to have a distinct IP address. Apart from the large address spaces, IPv6 simplifies network management tasks through address auto-configuration and hierarchical route management.

One potential use of IPv6 is for mobile application. The next generation network is expected to dominate by mobile devices. Typically, when a mobile node (MN) moves to a new network, its IP address must change accordingly. This causes existing TCP/IP connections to terminate. The MN must re-establish the connection in order to continue the conversation. Mobile IPv6 [1] is designed to solve this problem by allowing the MN to continue receiving packets through existing connections and remain reachable while roaming to a new network.

In the world of Internet has communication any time, which compounds the information data, images and sounds. If connection or equipment is lost, it affects to the business very much.

In this paper, we study worst and minimal cases that are possible to recover services for home agent (HA) can communicate between MN and corresponding node (CN) smoothly.

## 2. Previous Works

Many articles proposed new techniques and enhancements about HA reliability such as below.

The increment of standard capability [1] is used for the HAAA protocol [2]-[3]. The HA list is used with HA switch that increases the operation to correspond with failure. They used the binding synchronization by putting the option in binding information update from MN to HA list. The binding information is used with HA to request the data of binding cache.

There are three HAs for conforming the reliability of VHAAR protocol [4]. That are active, backup and inactive HAs. The active HA is used for main service. If it fails, the data is sent to make the binding synchronization with backup HA. After that, the backup HA is instead used for service. Another is waited for inactive HA.

In this paper, we used two HAs and study a simple recovery used by TCP check. We set that HA1 is a main HA and HA2 is a standby HA. When HA1 fails, HA2 is used for standby and recovery services instead. This IPv6 mobile network system is implemented in our laboratory and investigated its reliability.

## 3. Mobile IPv6 Handover

Mobile IPv6 manages the movement of the MN by identifying each MN with its static home address (HoA), regardless of its location in the Internet. The original network where the MN belongs to is called a *home network*. When the MN moves away from home, it must send information about its new location and new IP address to HA in the home network. The HA can then intercept and forward packets to the MN at the new location. The new address of MN at a *foreign network* is called *care-of-address* (CoA).

The signaling process during the mobile IPv6



### 5.1.1 HA fail in home

Figure 4 shows the status of MN at home network when it communicates with CN. From the figure, we can see that the communications between MN and CN are disconnected when HA1 fails. That is because the HA1 is the gateway of MN and route to CN.

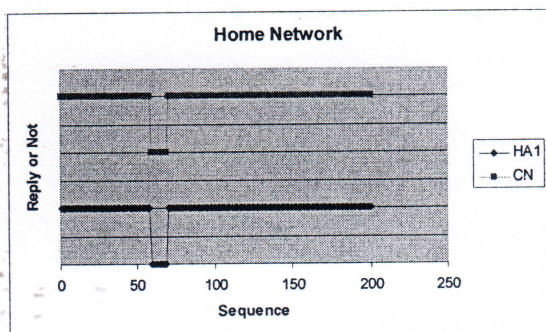


Fig 4: Status of MN at home network.

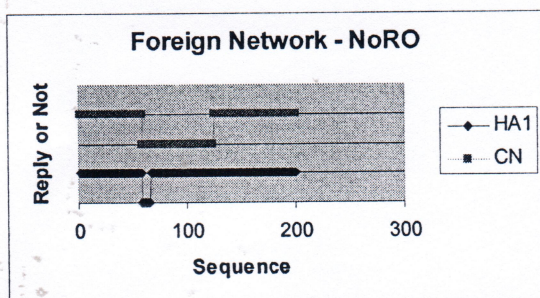


Fig 5: Status of MN at foreign network with no route optimization.

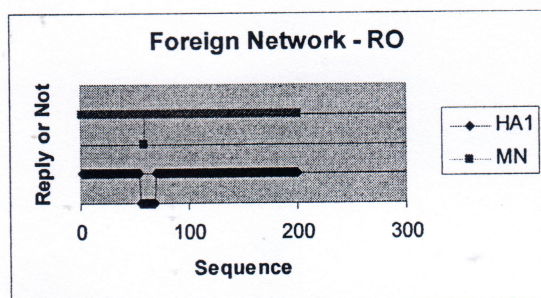


Fig 6: Status of MN at foreign network with route optimization.

### 5.1.2 HA Fail in Foreign Network with no route optimization

Figure 5 shows the status of MN at foreign network with no route optimization. From the figure, we can see that the results are almost the same with Fig. 4 but the communications between MN and CN have waiting time about CN life time plus 60 second.

### 5.1.3 HA Fail in Foreign Network with route optimization

Figure 6 shows the status of MN at foreign network with route optimization. From the figure, we can see that they can communicate even if HA1 fails. After the information exchange and route optimization, the communications are not via the tunnel of HA1. Therefore, the communications are smooth.

## 5.2 Measurement gain time

The recovery of HA is measured [6]. HA1 is set to fail 5 times. The duration of each time is 10 minutes. The delayed time of TCP check is set to be 1, 30 and 60 seconds. The time period checks for HA are shown in Fig. 7. The time parameters for checking are defined as follow.

Down time ( $T_{down}$ ) is defined as a period of time during the HA1 downs. That is

$$T_{down} = A3 - A1,$$

(1) where  $A1$  and  $A3$  are the times that HA1 begins to fail and reply, respectively.

Restore Time ( $T_{restore}$ ) is defined as a period of time during the HA1 restores. That is

$$T_{restore} = A3 - A2,$$

where  $A2$  is the time that HA1 begins to check the scrip.

Recovery Time ( $T_{recovery}$ ) is defined as a period of time during the HA1 recovers. That is

$$T_{recovery} = T_{restore} - T_{litch}$$

where  $T_{litch}$  is the *CN lifetime* and is set to be 60, 120, 240 and 420 seconds.

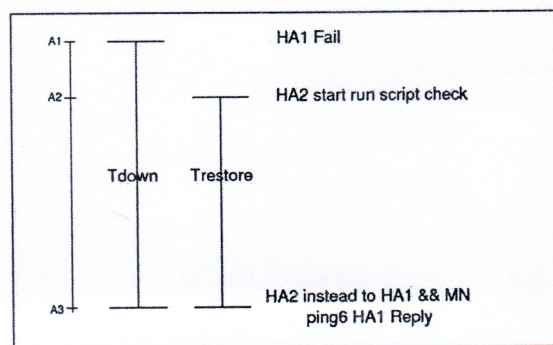


Fig 7: Time period checks for HA.

TCP check at HA1 runs script server and opens socket for waiting HA2. It is a client that checks the connection by using TCP 3-way handshake to HA1. If it fails, HA2 is used for standby and recovery services instead.

## 6. Results

The CN lifetime compared with HA down time is shown in Fig. 8. The down time is proportional with CN lifetime while CN lifetime is propotional with the checked

time. The value of CN lifetime is happen when MN cannot communicate with HA1. It has "Binding Error" then MN sends "Binding Update" to CN lifetime for resetting update lifetime to zero. When MN can communicate to HA1 again, it will send "Binding Update" to HA1 and the lifetime of MN is not equal to zero.

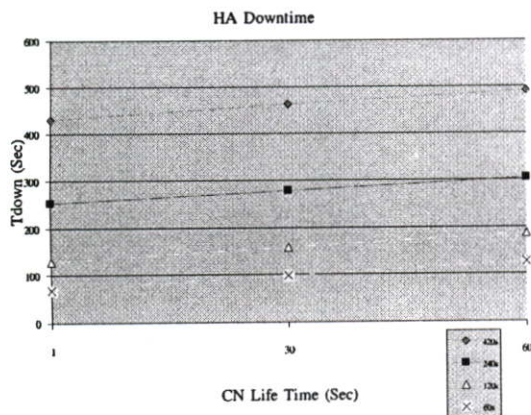


Fig 8: CN lifetime compared with HA down time.

Figure 9 shows the CN lifetime compared with HA restore. The HA restore is not proportional with the checked time. The HA restore does not change when the checked times are changed to 1, 30 and 60 seconds. The CN lifetime is changed to 60, 120, 240 and 420 seconds and the mean value of five time failures are evaluated and plotted the graphs as shown in this figure.

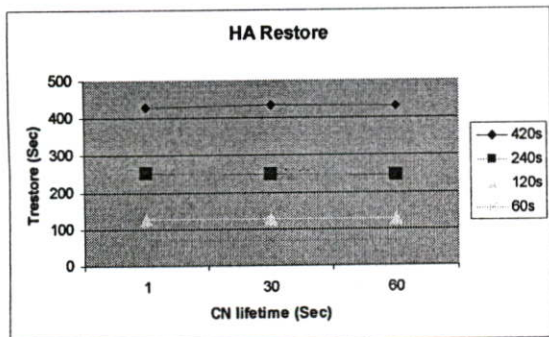


Fig 9: CN lifetime compared with HA restore.

Figure 10 shows HA recovery. The values of HA1 and HA2 reliability recoveries are about 4 to 15 seconds. That is because the script of TCP check waits 2 seconds for checking the connection. The wait interface of Linux absolutely fails and each delay appears from 2-layer in wireless.

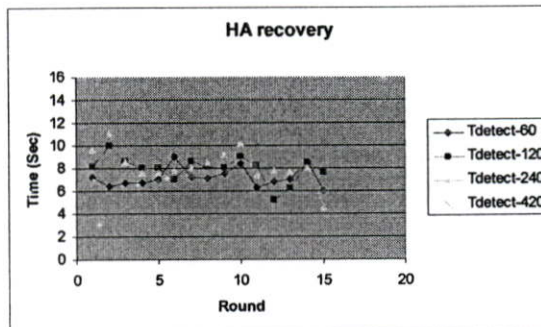


Fig 10: HA recovery in each case

### 7. Conclusions and Future Works

In our experiments and results indicate that the reliability of HA with network system of mobile IPv6 is increased. It protects the loss of communication between MN and CN when HA fails. If MN and CN are communicated with route optimization, the loss communication is a small problem for this system. If MN stays at home and does not use the route optimization, it becomes the big problem although the recovery time is set to about 60 – 420 seconds follow adjusting CN lifetime.

In the future work, the down time is reduced less than 60 seconds at home network. Then, the foreign network cannot use the route optimization, so the predict protocol for telling MN when HA2 detects the failure of HA1 is developed for no wait time of check.

### References

- [1] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
- [2] V. Devarapalli, R. Wakikawa and P. Thubert, "Local HA to HA protocol", draft-devarapalli-mip6-nemo-local-haha-01.txt, March 2006.
- [3] R. Wakikawa, P. Thubert and V. Devarapalli "Inter Home Agents Protocol Specification", draft-wakikawa-mip6-nemo-haha-spec-01.txt, March 2006.
- [4] J. Faizan, H. El-Rewini and M. Khalil, "Virtual Home Agent Reliability Protocol for Mobile IPv6 based Networks," 2005 International Conference on Wireless Networks, Communications and Mobile Computing, vol. 2, pp. 1295 – 1300, June 2005.
- [5] Nectec Mobile IPv6 TestBed, [www.ipv6.nectec.or.th/~zpop/mip6](http://www.ipv6.nectec.or.th/~zpop/mip6)
- [6] A network protocol analyzer, [www.ethereal.com](http://www.ethereal.com)

## ประวัติผู้เขียน

ชื่อ – นามสกุล	นายอดิศักดิ์ บุษรนนท์
วัน เดือน ปีเกิด	23 ธันวาคม พ.ศ. 2520
ที่อยู่	1/218 ป๊อปปูล่าคอน โคมินิยม ตึก C1 ห้อง04/32 เมืองทองธานี ต.บางพูน อ.ปากเกร็ด จังหวัดนนทบุรี 11120
ประวัติการศึกษา	
พ.ศ. 2541	ระดับปริญญาวิชาชีพชั้นสูง สาขาเทคนิคคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
พ.ศ. 2543	สำเร็จการศึกษาปริญญาตรีวิทยาศาสตร์บัณฑิต สาขาเทคโนโลยี สารสนเทศ เอกการสื่อสาร จากภาควิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี
ประสบการณ์การทำงาน	
ปัจจุบัน	ตำแหน่งผู้ช่วยนักวิจัย 1 ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์ แห่งชาติ 2546-2547 ตำแหน่งวิศวกรเครือข่าย บริษัท โมโนเทคโนโลยี 2543-2546 ตำแหน่งวิศวกรทั่วไป บริษัท จัสมินอินเตอร์เน็ต