สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

ต้นแบบโปรแกรมจำลองข้อมูลทราฟฟิคทดสอบระบบเครือข่าย

PROTOTYPE OF SIMULATION PROGRAM FOR TESTING IP NETWORK

T146489

โดย

ชวนาท นิพัทธมานนท์

CHAWANAT NIPATTMANON

อาจารย์ที่ปรึกษา

ดร. สุภกิจ นุตยะสกุล

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ว.ท.
T274n
2558

b.00264251
b.12844259x
i.

เลขหมู่.....
เลขทะเบียน 146489
รับ.เดือน.ปี 23 พ.ค. 2560

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ 2

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ 2 ปีการศึกษา 2558

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

PROTOTYPE OF SIMULATION PROGRAM FOR TESTING IP NETWORK

CHAWANAT NIPATTMANON

A REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF THE COURSE INDEPENDENT STUDY 2

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

KING MONKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2/2015

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

COPYRIGHT 2016

FACULTY OF INFORMATION TECHNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABAN

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ใบรับรองการศึกษาอิสระ 2 (Independent Study 2)

เรื่อง

ต้นแบบโปรแกรมจำลองข้อมูลทราฟฟิคทดสอบระบบเครือข่าย

PROTOTYPE OF SIMULATION PROGRAM FOR TESTING IP NETWORK

ชวนาท นิพัทธมานนท์

รหัสประจำตัว 57606107

ขอรับรองว่ารายงานฉบับนี้ ข้าพเจ้าไม่ได้คัดลอกมาจากที่ใด

รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของ

การศึกษาอิสระ 2 หลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)

ภาคเรียนที่ 2 ปีการศึกษา 2558

.....อาจารย์ที่ปรึกษา

(ผศ.ดร.สุกภิจ นุตยะสกุล)

.....กรรมการสอบ

(รศ.ดร.พรฤดี เนติโสภากุล)

.....กรรมการสอบ

(ผศ.ดร.สุเมธ ประภาวัต)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อ	ต้นแบบโปรแกรมจำลองข้อมูลทราฟฟิคทดสอบระบบเครือข่าย
รหัสนักศึกษา	57606107
นักศึกษา	นายชวนาท นิพัทธมานนท์
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	เทคโนโลยีสารสนเทศและการจัดการ
ปีการศึกษา	2558
อาจารย์ที่ปรึกษา	ดร. สุภกิจ นุตยะสกุล

บทคัดย่อ

สารนิพนธ์ฉบับนี้เสนอการพัฒนารูปแบบการทดสอบข้อมูลของระบบการทำงานของระบบเครือข่ายทั้งไอพีเวอร์ชั่น 4 และ 6โดยใช้โปรแกรมซอคเกตที่สร้างจากซีชาร์ปช่วยในการรับ-ส่งสืบเนื่องจากในปัจจุบันหมายเลขไอพีที่ใช้ในระบบเครือข่ายที่ใช้กันปัจจุบัน ไม่เพียงพอต่อความต้องการ ทำให้ทุกองค์กรต้องเริ่มเข้าสู่การใช้งานหมายเลขไอพีเวอร์ชัน6เมื่อมีการเปลี่ยนผ่านเข้าสู่ระบบเครือข่ายใหม่ ต้องมีการทำการทดสอบภายก่อนใช้งานจริง โดยจะมุ่งเน้นไปที่เลเยอร์3 และเลเยอร์4 ตามหลักโอเอสไอ โมเดล (OSI model) ซึ่งกรณีศึกษานี้ต้องการซอคเกตโปรแกรมฝั่งส่งจะทำการอ่านค่าข้อมูลที่ต้องการจำลองจากเอกซ์เอ็มแอลไฟล์ ส่งไปยังซอคเกตโปรแกรมฝั่งรับ ซึ่งอาจจะมีการให้ตัวซอคเกตโปรแกรมเปิดเซอร์วิสต่างๆไว้ได้โดยง่าย โดยไม่จำเป็นต้องย้ายโปรแกรมที่ทำงานจริง มาลงบนคอมพิวเตอร์หรือเซิร์ฟเวอร์เพื่อทดสอบ ซึ่งจะตอบโจทย์ความสะดวกในการทดสอบมากกว่า

ส่วนโปรแกรมโอเพ่นซอสที่มีอยู่นั้น ส่วนใหญ่ยังไม่สนับสนุนการทำงานของไอพีเวอร์ชัน 6 หรือไม่สามารถกำหนดต้นทางได้มากกว่า 1 หมายเลขไอพีแอสเดรส ทำให้ไม่ตอบโจทย์ที่ว่าถ้าต้องการทดสอบหลายหมายเลขไอพี ต้องทำการทดสอบหลายครั้ง ซึ่งจะต่างจากกรณีศึกษานี้ที่จะทำให้ทดสอบครั้งเดียวพร้อมกับหลายหมายเลขไอพีแอสเดรสไปยัง ปลายทางเดียวกัน โดยการทดสอบนั้นจะแบ่งระบบเครือข่ายไอพีเวอร์ชัน6ตามรูปแบบของเร้าติ้ง ทั้งในส่วนของระบบเครือข่ายเฉพาะบริเวณ(LAN) และระบบเครือข่ายบริเวณกว้าง(WAN).

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

รายงานการศึกษาอิสระฉบับนี้สำเร็จลงได้ เนื่องด้วยได้รับความกรุณาจากอาจารย์ที่ปรึกษา ผศ.ดร. สุภกิจ นุตยะสกุล ที่เสียสละเวลาให้ความช่วยเหลือ ให้คำแนะนำ สนับสนุนชี้แนะแนวทางในการศึกษา วิเคราะห์ และพัฒนาโปรแกรมต้นแบบ จนกระทั่งโปรแกรมที่พัฒนาสามารถนำมาใช้งานได้ ในการทำงานปัจจุบัน ต้องขอกราบขอบพระคุณเป็นอย่างสูง

ขอขอบคุณกำลังใจจากบุคคลคนในครอบครัว รวมถึงกัลยาณมิตรทุกท่านที่ได้ให้ความช่วยเหลือสนันสนุนด้วยดีเสมอมา

คุณประโยชน์อันบังเกิดจากรายงานการศึกษาอิสระฉบับนี้ ข้าพเจ้าขอมอบให้แก่บิดา มารดา ผู้ซึ่งเป็นที่รักและทรงพระคุณอันประเสริฐ

ชวนาท นิพัทธมานนท์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

หน้า

บทคัดย่อภาษาไทย I

บทคัดย่อภาษาอังกฤษ II

กิตติกรรมประกาศ III

สารบัญ IV

สารบัญตาราง VI

สารบัญรูป VII

บทที่ 1 บทนำ 1

1.1 ประวัติความเป็นมาและความสำคัญของปัญหา 2

1.2 วัตถุประสงค์ของโครงการ 3

1.3 ขอบเขตของโครงการ 3

1.3.1 ขอบเขตของโปรโตรคอลที่เลือกทดสอบ 4

1.3.2 ขอบเขตของเนตเวิร์ก 4

1.3.3 ขอบเขตของภาษาคอมพิวเตอร์ 5

1.4 แผนการดำเนินงาน 6

1.5 เทคโนโลยีที่ใช้ในการพัฒนาระบบ 6

1.6 ประโยชน์จะได้รับ 7

บทที่ 2 ทฤษฎีและเทคโนโลยีที่เกี่ยวข้อง 8

2.1 ภาพรวมของไอพีเวอร์ชั่น6 8

2.2 ภาพรวมของเทคโนโลยีที่ใช้ในโครงงาน 12

2.3 เทคโนโลยีที่เกี่ยวข้องกับการพัฒนาระบบ 14

2.4 สรุป 21

บทที่ 3 ระบบโปรแกรมที่พัฒนาและรูปแบบการทดลอง 23

3.1 ซีเควนไดอะแกรม (Sequence Diagram) 23

3.2 แอคทิวิตี้ไดอะแกรมของซอคเกตโปรแกรม (Activity Diagram) 24

3.2.1 ซอคเกตโปรแกรมของฝั่งเซิร์ฟเวอร์(ฝั่งรับ) 24

3.2.2 ซอคเกตโปรแกรมของฝั่งไคลเอนต์(ฝั่งส่ง) 25

3.3 เนตเวิร์กไดอะแกรม (Network Diagram) 26

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ(ต่อ)

หน้า

3.4 การสร้างซอคเกตโปรแกรมโดยใช้ซีชาร์ป 27

3.4.1 การสร้างโปรแกรมของการรับแพคเก็จจากระบบเครือข่าย 29

3.4.2 การสร้างโปรแกรมของการส่งแพคเก็จจากระบบเครือข่าย 31

3.5 การสร้างเอกสารเอกซ์เอ็มแอล 33

3.6 การติดตั้งระบบเครือข่าย ในการทดลอง 35

3.6.1 ระบบเครือข่าย บนเร้าเตอร์ตัวเดียว 35

3.6.2 ระบบเครือข่าย แบบการใช้งานภายในองค์กร 35

3.6.3 ระบบเครือข่าย แบบการใช้งานระหว่างองค์กร 37

3.7 การทำงานของไวร์ชาร์ก 39

3.8 สรุป 44

บทที่ 4 การทดลองและผลการทดลอง 45

4.1 รูปแบบการทดลอง 45

4.1.1 การรับส่ง-ข้อมูล ผ่านระบบเครือข่าย บนเร้าเตอร์เพียงตัวเดียว 45

4.1.2 การรับส่ง-ข้อมูล ผ่านระบบเครือข่าย แบบการใช้งานภายในองค์กร 49

4.1.3 การรับส่ง-ข้อมูล ผ่านระบบเครือข่าย แบบการใช้งานระหว่างองค์กร 61

4.2 ผลการทดลอง 71

4.2.1 การทดลองรับส่ง-ข้อมูล ผ่านระบบเครือข่าย บนเร้าเตอร์เพียงตัวเดียว 71

4.2.2 การทดลองรับส่ง-ข้อมูล ผ่านระบบเครือข่าย แบบการใช้งานภายในองค์กร 73

4.2.3 การทดลองรับส่ง-ข้อมูล ผ่านระบบเครือข่าย แบบการใช้งานระหว่างองค์กร 76

4.3 สรุป 79

บทที่ 5 สรุปผล 80

5.1 สรุปการทดลอง 80

5.1.1 การรับส่ง-ข้อมูล ผ่านระบบเครือข่าย บนเร้าเตอร์เพียงตัวเดียว 81

5.1.2 การรับส่ง-ข้อมูล ผ่านระบบเครือข่าย แบบการใช้งานภายในองค์กร 84

5.1.3 การรับส่ง-ข้อมูล ผ่านระบบเครือข่าย แบบการใช้งานระหว่างองค์กร 88

5.2 ปัญหาและอุปสรรค 88

5.3 ข้อจำกัดของโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง 90

5.4 การเปรียบเทียบกับโปรแกรมที่อยู่ 90

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

5.5 สรุป 93

บรรณานุกรม 94

ประวัติผู้เขียน 95

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญตาราง

ตารางที่ หน้า

4.1 แสดงค่าผลการทดสอบการรับ-ส่งผ่านเร้าเตอร์ตัวเดียวแบบไอพีเวอร์ชั่น4 72

4.2 แสดงค่าผลการทดสอบการรับ-ส่งผ่านเร้าเตอร์ตัวเดียวแบบไอพีเวอร์ชั่น6 73

4.3 แสดงค่าผลการทดสอบการรับ-ส่งผ่านเครือข่ายในองค์กรแบบไอพีเวอร์ชั่น4 74

4.4 แสดงค่าผลการทดสอบการรับ-ส่งผ่านเครือข่ายในองค์กรแบบไอพีเวอร์ชั่น6 75

4.5 แสดงค่าผลการทดสอบการรับ-ส่งผ่านเครือข่ายระหว่างองค์กรแบบไอพีเวอร์ชั่น4 77

4.6 แสดงค่าผลการทดสอบการรับ-ส่งผ่านเครือข่ายระหว่างองค์กรแบบไอพีเวอร์ชั่น6 78

5.1 แสดงผลการเปรียบเทียบระหว่างโปรแกรมที่พัฒนากับโปรแกรมที่มีอยู่ 92

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป

รูปที่ หน้า

1.1 รูปแสดงแบบการทดสอบการใช้งานบนเร้าเตอร์ตัวเดียว....4
1.2 รูปแสดงแบบการทดสอบการใช้งานภายในองค์กร....4
1.3 รูปแสดงแบบการทดสอบการใช้งานภายระหว่างองค์กร....5
2.1 รูปแสดงเวอร์ชันของไอพี (IP version number)....9
2.2 รูปแสดงการแบ่งโซนผู้ดูแลการกำหนดหมายเลขไอพีในอินเทอร์เนต....10
2.3 รูปแสดงการใช้งานของIPv4 ของจำนวนผู้ใช้งานกับที่มีอยู่จริง....10
2.4 รูปแสดงหลักการของซอคเกตโปรแกรม....19
2.5 รูปแสดงการดักจับข้อมูลทราฟฟิค....21
3.1 รูปแสดงซีเควนไดอะแกรมการทำงานของโปรแกรมจำลองข้อมูลทราฟฟิค....23
3.2 รูปแสดงแอคทิวิตี้ไดอะแกรมการทำงานของฝั่งรับ....24
3.3 รูปแสดงแอคทิวิตี้ไดอะแกรมการทำงานของฝั่งส่ง....25
3.4 รูปแสดงแบบการทดสอบที่1....26
3.5 รูปแสดงแบบการทดสอบที่2....26
3.6 รูปแสดงแบบการทดสอบที่3....27
3.7 รูปแสดงการสื่อสารกันระหว่างซอคเกตโปรแกรมฝั่งเซิร์ฟเวอร์และไคลเอนต์....28
3.8 รูปแสดงวินโดวส์ฟอร์มของโปรแกรมจำลองข้อมูลทราฟฟิคฝั่งไคลเอนต์....29
3.9 รูปแสดงวินโดวส์ฟอร์มของโปรแกรมจำลองข้อมูลทราฟฟิคฝั่งเซิร์ฟเวอร์....29
3.10 รูปแสดงการใช้โปรแกรมไวร์ชาร์ก....40
3.11 รูปแสดงการเลือกอินเทอร์เฟสที่ต้องการดักจับแพคเก็ต....41
3.12 รูปแสดงแพคเก็ตที่ถูกดักจับได้....41
3.13 รูปแสดงขั้นตอนเมื่อหยุดจับแพคเก็ต....41
3.14 รูปแสดงขั้นตอนเมื่อฟิลเตอร์แพคเก็ต TCP....42
3.15 รูปแสดงหน้าโปรแกรมไวร์ชาร์ก....43
4.1 รูปแสดงการตรวจสอบการเชื่อมต่อการทดสอบไอพีเวอร์ชั่น 4 ข้อ4.1.1....46
4.2 รูปแสดงการตั้งค่าโปรแกรมจำลองทราฟฟิคฝั่งเซิร์ฟเวอร์ไอพีเวอร์ชั่น 4 ข้อ 4.1.1....47
4.3 รูปแสดงการตรวจสอบการเชื่อมต่อการทดสอบไอพีเวอร์ชั่น 6 ข้อ4.1.1....48
4.4 รูปแสดงการตั้งค่าโปรแกรมจำลองทราฟฟิคฝั่งเซิร์ฟเวอร์ไอพีเวอร์ชั่น 6 ข้อ 4.1.1....49
4.5 รูปแสดงการตรวจสอบการเชื่อมต่อการทดสอบไอพีเวอร์ชั่น 4 ข้อ4.1.2....54

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป (ต่อ)

รูปที่ หน้า

4.6 รูปแสดงการตั้งค่าโปรแกรมจำลองทราฟฟิคฝั่งเซิร์ฟเวอร์ไอพีเวอร์ชั่น 4 ข้อ 4.1.2.....55
4.7 รูปแสดงการตรวจสอบการเชื่อมต่อการทดสอบไอพีเวอร์ชั่น 6 ข้อ4.1.2.....60
4.8 รูปแสดงการตั้งค่าโปรแกรมจำลองทราฟฟิคฝั่งเซิร์ฟเวอร์ไอพีเวอร์ชั่น 6 ข้อ 4.1.2.....61
4.9 รูปแสดงการตั้งค่าโปรแกรมจำลองทราฟฟิคฝั่งเซิร์ฟเวอร์ไอพีเวอร์ชั่น 4 ข้อ 4.1.3.....66
4.10 รูปแสดงการตั้งค่าโปรแกรมจำลองทราฟฟิคฝั่งเซิร์ฟเวอร์ไอพีเวอร์ชั่น 6 ข้อ 4.1.3.....71
5.1 รูปแสดงค่าข้อมูลพีแคปไฟล์ตั้งต้น_1.....81
5.2 รูปแสดงค่าข้อมูลพีแคปไฟล์ตั้งต้น_2.....81
5.3 รูปแสดงค่าข้อมูลพีแคปไฟล์จากการทดลองเครือข่ายเร้าเตอร์ตัวเดียวแบบไอพีเวอร์ชั่น4_1 ...82
5.4 รูปแสดงค่าข้อมูลพีแคปไฟล์จากการทดลองเครือข่ายเร้าเตอร์ตัวเดียวแบบไอพีเวอร์ชั่น4_2 ...82
5.5 รูปแสดงค่าข้อมูลพีแคปไฟล์จากการทดลองเครือข่ายเร้าเตอร์ตัวเดียวแบบไอพีเวอร์ชั่น6_1 ...83
5.6 รูปแสดงค่าข้อมูลพีแคปไฟล์จากการทดลองเครือข่ายเร้าเตอร์ตัวเดียวแบบไอพีเวอร์ชั่น6_2 ...83
5.7 รูปแสดงค่าข้อมูลที่ดักจับเมื่อ2ไคลเอนต์ส่งมาเซิร์ฟเวอร์พร้อมกันแบบไอพีเวอร์ชั่น4 84
5.8 รูปแสดงค่าข้อมูลพีแคปไฟล์จากการทดลองเครือข่ายในองค์กรแบบไอพีเวอร์ชั่น4 85
5.9 รูปแสดงค่าข้อมูลที่ดักจับเมื่อ2ไคลเอนต์ส่งมาเซิร์ฟเวอร์พร้อมกันแบบไอพีเวอร์ชั่น6 86
5.10 รูปแสดงค่าข้อมูลพีแคปไฟล์จากการทดลองเครือข่ายในองค์กรแบบไอพีเวอร์ชั่น6 87

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 1
บทนำ

ปัจจุบันได้มีการคาดการจากหน่วยงานที่ทำหน้าที่แจกจ่ายหมายเลขไอพีแอสแดรส (AFRINIC, ARIN, APNIC, LACNIC, RIPE NCC) โดยทั่วโลกจะสามารถรองรับหมายเลขไอพีแอสแดรสเวอร์ชั่น 4(IPv4 Address)ได้ถึงช่วงปี 2020 เท่านั้น แต่ก็ยังเป็นแค่การคาดการณ์ ดังนั้นเพื่อรองรับสถานการณ์นั้น ทางกลุ่มของหน่วยงานที่แจกจ่าย IP Address จึงได้เริ่มมีการแจกจ่ายและใช้งานหมายเลขไอพีแอสแดรสชุดใหม่ที่เรียกว่า หมายเลขไอพีแอสแดรสเวอร์ชั่น 6(IPv6 address).

ด้วยเหตุนี้หลายประเทศในทวีปเอเชีย และยุโรป ได้มีความตื่นตัวที่จะปรับเปลี่ยนนระบบเครือข่าย โดยมีอัตราที่มากกว่าประเทศในทวีปแทบอเมริกาเหนือ เนื่องมาจากปัญหาการขาดแคลนหมายเลขไอพีแอสแดรสเวอร์ชั่น 4ทำให้บริษัทผู้นำทางด้านเทคโนโลยี ซึ่งล้วนตั้งอยู่ในภูมิภาคเอเชียนี้ อาทิเช่นญี่ปุ่นและเกาหลีใต้ ต่างให้การสนับสนุนและผลักดันธุรกิจภาคเอกชน ให้เริ่มหันมาเอาจริงเอาจังในการให้บริการหมายเลขไอพีแอสแดรสเวอร์ชั่น 6 มากขึ้น

นอกจากนี้โลกของระบบมือถือที่ได้เปลี่ยนแปลงอย่างรวดเร็ว ก็มีความจำเป็นที่จะต้องนำเอาหมายเลขไอพีแอสแดรสเวอร์ชั่น 6มาใช้งาน โดยเริ่มจากการทำระบบทดสอบที่อุปกรณ์ และรบบเครือข่ายภายในที่ใช้งานหมายเลขไอพีแอสแดรสเวอร์ชั่น 6เหมือนกัน เช่นเดียวกับการพัฒนาเครือข่าย และความสามารถของอีปกรณ์ในปัจจุบันสำหรับติดต่อสื่อสารระหว่างอุปกรณ์เครื่องใช้ไฟฟ้าต่างๆ (IP Camera, Smart TV) ก็เป็นส่วนนึงที่ทำให้ต้องนำหมายเลขไอพีแอสแดรสเวอร์ชั่น6 มาใช้งาน จากการสำรวจพบว่าบริษัทผู้ผลิตเครื่องใช้ไฟฟ้าต่างให้ความสนใจที่จะพัฒนาซอฟแวร์เพื่อรองหมายเลขไอพีแอสแดรสเวอร์ชั่น 6 เข้ากับอุปกรณ์ของตนเช่น ค่าย Apple ที่ผลิตโทรศัพท์เคลื่อนที่ไอโฟน(iphone)ได้ออกระบบปฏิบัติการ IOS 8 เพื่อรองรับการทำงานของหมายเลขไอพีแอสเดรสเวอร์ชั่น6 หรือ ค่ายมือถือซัมซุง(SAMSUNG)ก็ได้มีโปรแกรมให้เครื่องสามารถรองรับหมายเลขไอพีแอสแดรสเวอร์ชั่น 6 ได้เช่นกัน แม้กระทั้งเฟสบุค(facebook)ก็มีหมายเลขไอพีแอสแดรสเวอร์ชั่น6 เป็น 2620:0:1cfe:face:b00c::3/96 หรือ www.google.com ก็มีการใช้งานหมายเลขไอพีแอสแดรสเวอร์ชั่น 6 เรียบร้อยแล้ว

แต่การที่จะเริ่มดำเนินการใช้ระบบเครือข่ายไอพีเวอร์ชั่น 6 (IPv6 Network) นั้นย่อมต้องมีการทดสอบภายในก่อน แต่ด้วยข้อจำกัดของอุปกรณ์ ในองค์กร หรือ ข้อมูลดาต้าทราฟฟิค ที่จะนำมาใช้ทดสอบนั้น ก็อาจจะเป็นปัญหาส่วนนึงในการทดสอบ ทั้งค่าใช้จ่ายในการทดสอบการขนย้ายอุปกรณ์ในการทดสอบซึ่งทำให้เกิดความคิดในการพัฒนาซอคเกตโปรแกรม เพื่อใช้เป็นโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริงเพื่อใช้ทดสอบระบบเครือข่ายไอพีเวอร์ชัน 6(IPv6

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

network) ด้วยการดักจับทราฟฟิคเดิมเป็น พีแคปไฟล์ และมีการสร้างเอกสารเอกซ์เอ็มแอล เพื่อเป็นตัวเรียกข้อมูลไปยังข้อมูลทราฟฟิค

เมื่อมีการเปลี่ยนผ่านเข้าสู่ระบบเครือข่ายใหม่ ต้องมีการทำการทดสอบภายก่อนใช้งานจริง โดยโปรแกรมที่พัฒนาจะมุ่งเน้นไปที่เลเยอร์3 และเลเยอร์4 ตามหลักโอเอสไอ โมเดล (OSI model) ซึ่งกรณีศึกษานี้ต้องการซอคเกตโปรแกรมฝั่งไคลเอนต์จะทำการอ่านค่าข้อมูลทราฟฟิคจำลอง ก่อนจะส่งไปยังซอคเกตโปรแกรมฝั่งเซิร์ฟเวอร์ ซึ่งซอคเกตโปรแกรมนี้เองจะทำหน้านี้รับ-ส่งข้อมูลทราฟฟิคจำลอง โดยไม่จำเป็นต้องย้ายโปรแกรมที่ทำงานจริง มาลงบนคอมพิวเตอร์หรือเซิร์ฟเวอร์เพื่อทดสอบ หรือการนำอุปกรณ์หลายๆเครื่อง มาใช้งานเพื่อให้ได้มาซึ่งข้อมูลจริง ทำให้โปรแกรมนี้ตอบโจทย์ความสะดวกในการทดสอบมากกว่า และ

ส่วนโปรแกรมโอเพ่นซอสที่มีอยู่นั้น ส่วนใหญ่ยังไม่สนับสนุนการทำงานของไอพีเวอร์ชัน 6 และที่สำคัญคือไม่สามารถจำลองพฤติกรรมที่แท้จริงของระบบได้(Network behavior) ซึ่งเป็นสิ่งที่สำคัญในการที่จะทดสอบระบบเครือข่ายใหม่ นอกจากนี้ยังไม่สามารถกำหนดต้นทางได้มากกว่า 1 หมายเลขไอพีแอสเดรส ทำให้ไม่ตอบโจทย์ที่ว่าถ้าต้องการทดสอบหลายหมายเลขไอพี ต้องทำการทดสอบหลายครั้ง ซึ่งจะต่างจากกรณีศึกษานี้ที่จะทำให้ทดสอบครั้งเดียวพร้อมกับหลายหมายเลขไอพีแอสเดรสไปยัง ปลายทางเดียวกัน โดยการทดสอบนั้นจะแบ่งระบบเครือข่ายไอพีเวอร์ชัน6ตามรูปแบบของเร้าติ้ง ทั้งในส่วนของระบบเครือข่ายเฉพาะบริเวณ(LAN) และระบบเครือข่ายบริเวณกว้าง(WAN).

1.1 ประวัติความเป็นมา และความสำคัญของปัญหา

อธิบายเริ่มจากหมายเลขไอพีแอสแดรสซึ่งที่มีมาจาก 2 ส่วนรวมกัน คือ อินเทอร์เนตโปรโตรคอล (IP : Internet Protocol) และแอสแดรส (Address)โดยอินเทอร์เน็ตโปรโตรคอลหมายถึง กฎ, รูปแบบมาตรฐานที่กำหนดขึ้นเพื่อทำให้อุปกรณ์เน็ตเวิร์กสามารถสื่อสารกันได้ ซึ่งในระบบเน็ตเวิร์กต้องมีอุปกรณ์ที่ทำหน้าเป็นผู้ส่ง และผู้รับ ดังนั้นจึงจำเป็นต้องรู้ถึง ที่อยู่ของผู้ส่ง (sender address) และที่อยู่ของผู้รับ(receiver address) ความหมายอีกส่วนของ แอสแดรส คือ หมายเลขไอพีแอสแดรส ซึ่งมันจะทำหน้าที่ระบุตัวตนของอุปกรณ์เน็ตเวิร์ก โดยแต่และอุปกรณ์เน็ตเวิร์กที่อยู่บนระบบเครือข่าย หรือระบบอินเทอร์เนตนั้นก็จะมีหมายเลขไอพีแอสแดรสที่ระบุตัวตนของมันเอง และแตกต่างกันออกไป

สาเหตุที่ต้องเปลี่ยนจากหมายเลขไอพีแอสแดรสเวอร์ชั่น4ไปเป็นหมายเลขไอพีแอสแดรสเวอร์ชั่น6 เนื่องจากการการใช้งานของผู้ใช้งาน และอุปกรณ์จำนวนมากในระบบเครือข่ายทำให้หมายเลขไอพีที่ใช้งานในปัจจุบันหมายเลขไอพีแอสแดรสเวอร์ชั่น4เริ่มขาดแคลน และกำลังจะหมดไป ทางหน่วยงานมาตรฐานสากลจึงจำเป็นต้องเริ่มใช้งานหมายเลขไอพีรูปแบบใหม่ซึ่งเรียก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ทั่วไปว่าหมายเลขไอพีแอสแดรสเวอร์ชั่น6 หลายประเทศได้เข้าสู่ช่วงประกาศเริ่มการใช้งานภายในอนาคตอันใกล้นี้รวมทั้งอีกหลายประเทศทั่วโลกก็มีแผนที่จะประกาศใช้งานต่อไปโดยสาเหตุหลักที่ทำให้ต้องโบกมือลาไอพีแอสแดรสเวอร์ชั่น4 ก็คือ การเพิ่มขึ้นของจำนวนอุปกรณ์เน็ตเวิร์ก, การเพิ่มขึ้นของจำนวนผู้ใช้งานและ การโตขึ้นแบบก้าวกระโดดของระบบอินเทอร์เนต
ทั้งที่ไอพีแอสแดรสเวอร์ชั่น4สามารถจะรองรับได้แค่ 4ล้านเลขหมาย ซึ่งในปัจจุบันไม่เพียงพอต่อความต้องการของผู้ที่ใช้งานทั่วโลกมีอุปกรณ์ที่ใช้งานโดยต้องมีหมายเลขไอพีกำกับจำนวนมากขึ้น เช่น โทรศัพท์, คอมพิวเตอร์, โทรทัศน์, รถยนต์ และอื่นๆจะขอยกตัวอย่างการเปลี่ยนแปลงระบบโทรศัพท์ที่จากเดิม ใช้งานผ่านระบบโทรศัพท์ แต่ในทุกวันนี้โทรศัพท์ตามที่ทำงาน หรือทางบ้านได้มีการเปลี่ยนเป็นผ่านระบบอินเทอร์เนต

1.2 วัตถุประสงค์ของโครงการ

1. สามารถช่วยลดค่าใช้จ่ายทุนขององค์กร (Capital Expenditure) ได้ เนื่องจากไม่จำเป็นต้องมีอุปกรณ์มากในการทำสอบ ไม่จำเป็นต้องใช้สถานที่มากในการทดสอบ
2. สามารถช่วยเพิ่มรายรับขององค์กร(Revenue & Income) เมื่อองค์กรต้องลงทุนเปลี่ยนเป็นระบบเครือข่ายไอพีเวอร์ชั่น6 เพื่อให้บริการลูกค้า
3. สามารถช่วยลดความยุ่งยาก ขั้นตอนในการทดสอบ ไม่จำเป็นต้องย้ายโปรแกรมต่างๆ มาลงบนคอมพิวเตอร์หรือเซิร์ฟเวอร์หลายๆเครื่องเพื่อทดสอบ ซึ่งจะตอบโจทย์ความสะดวกในการทดสอบมากกว่า
4. ข้อมูลทราฟฟิคที่ใช้ในการทดสอบนั้น เป็นพฤติกรรมจริงบนระบบเครือข่ายเดิม (Network Behavior)
5. ตัวโปรแกรมสามารถจำลองข้อมูลทราฟฟิคได้ทั้งระบบเครือข่ายไอพีเวอร์ชั่น4 และไอพีเวอร์ชั่น6

1.3 ขอบเขตของโครงการ

เริ่มจากการสร้างโปรแกรมจำลองทราฟฟิคเสมือนจริง โดยใช้ซอคเกตโปรแกรมในการรับ-ส่งข้อมูลทราฟฟิค ซึ่งทราฟฟิคนั้นจะเป็นการดักจับข้อมูลมากจากโปรแกรมไวร์ชาร์ก ออกมาในรูปพีแคปไฟล์(Pcacp file) นอกจากนั้นยังมีการสร้างเอกสารเอกซ์เอ็มแอล เป็นตัวเก็บค่าพารามิเตอร์และชี้ไปยังพีแคปไฟล์ซึ่งเก็บข้อมูลทราฟฟิคเดิม ในส่วนของการทดสอบโปรแกรมที่พัฒนานั้นจะมีการสร้างระบบเครือข่ายขึ้นมาทั้งระบบเครือข่ายไอพีเวอร์ชั่น4 และ เวอร์ชั่น6 เพื่อนำมาทดสอบการรับส่งข้อมูลระหว่างโปรแกรมฝั่งรับและฝั่งส่ง

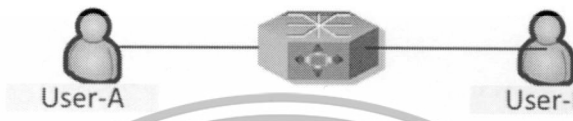
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.3.1 ขอบเขตของโปรโตรคอลที่เลือกทดสอบ

- โปรโตรคอลสำหรับการโอนย้ายแฟ้มข้อมูล (FTP)
- โปรโตรคอลสำหรับการแลกเปลี่ยนข้อมูลผ่านทางอินเทอร์เน็ต (HTTP)
- โปรโตรคอลสำหรับการรับ-ส่งจดหมายอิเลคทรอนิกส์ (SMTP)

1.3.2 ขอบเขตของเนตเวิร์ก

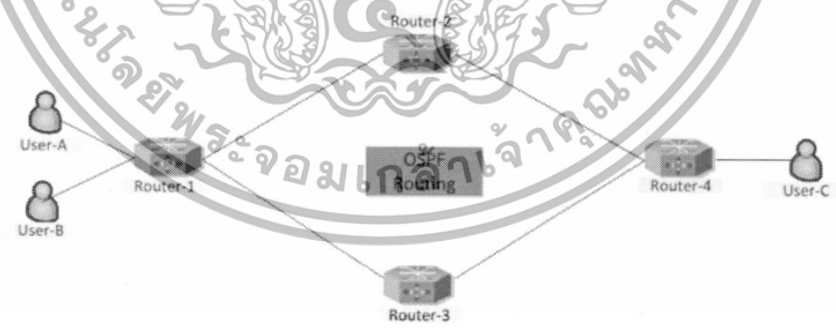
- การใช้งานบนเร้าเตอร์ตัวเดียว (local router)



รูปที่ 1.1 รูปแสดงแบบการทดสอบการใช้งานบนเร้าเตอร์ตัวเดียว

จากรูปที่ 1.1 จะเป็นไดอะแกรมแสดงรูปแบบการทดสอบรับส่งข้อมูลทราฟฟิคจำลองระหว่างผู้ใช้งาน A และ ผู้ใช้งาน B โดยมีการลงโปรแกรมที่สามารถเก็บข้อมูลการรับ-ส่งที่ชื่อว่าไวร์ชาร์ก (wireshark) บนคอมพิวเตอร์ของผู้ใช้งาน A และ ผู้ใช้งาน B เพื่อที่จะนำไปวิเคราะห์ ว่าเมื่อข้อมูลทราฟฟิคที่ส่งจาก ผู้ใช้งาน A แล้วผู้ใช้งาน B สามารถรับข้อมูลทราฟฟิคที่ส่งมาได้ครบหรือไม่ และใช้เวลาในการรับส่งเป็นเท่าไร

- การใช้งานภายในองค์กร (LAN)



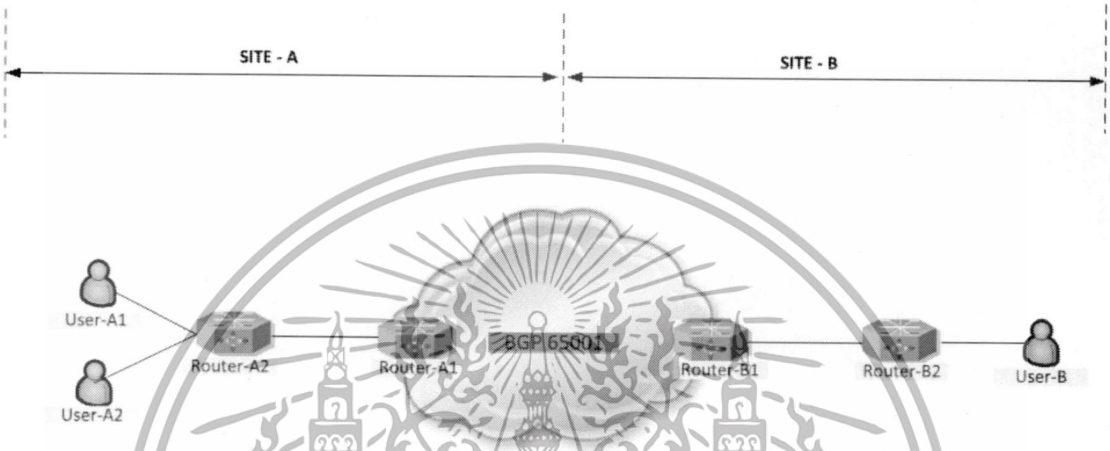
รูปที่ 1.2 รูปแสดงแบบการทดสอบการใช้งานภายในองค์กร

จากรูปที่ 1.2 จะเป็นไดอะแกรมแสดงรูปแบบการทดสอบส่งข้อมูลทราฟฟิคจำลองจากผู้ใช้งาน A และ B โดยเป็นข้อมูลทราฟฟิคของโปรโตรคอลที่แตกต่างกัน ไปยังผู้ใช้งาน C ซึ่งจะผ่านระบบเครือข่ายที่เป็นรูปแบบภายในออฟฟิศองค์กรเดียวกัน โดยที่เร้าเตอร์ตัวที่ 1, 2, 3 และ 4 สามารถทำงานได้ทั้งในรูปแบบของการกำหนดเร้าติ้งโดยคำสั่ง(Static routing) หรือการกำหนดเร้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ติ้งโดยคำสั่งอัตโนมัติ(Dynamic routing) เพื่อให้ได้ระบบเครือข่ายที่สมบูรณ์ที่สามารถให้ผู้ใช้งานรับ-ส่ง ข้อมูลหากันได้ นอกจากนี้จะมีการลงโปรแกรมที่สามารถเก็บข้อมูลการรับ-ส่ง ที่ชื่อว่าไวร์ชาร์ก(wireshark) บนคอมพิวเตอร์ของผู้ใช้งาน A, B และ C เพื่อที่จะนำข้อมูลที่ได้ไปวิเคราะห์ ว่าเมื่อข้อมูลทราฟฟิคที่ส่งจาก ผู้ใช้งาน A, B ไปยังผู้ใช้งาน C ว่าปลายทางผู้ใช้งาน C สามารถรับข้อมูลทราฟฟิคที่ส่งมาได้ครบหรือไม่ และใช้เวลาในการรับส่งเป็นเท่าไร

- การใช้งานระหว่างองค์กร (WAN)



รูปที่ 1.3 รูปแสดงแบบการทดสอบการใช้งานภายระหว่างองค์กร

จากรูปที่ 1.3 จะเป็นไดอะแกรมแสดงรูปแบบการทดสอบส่งข้อมูลทราฟฟิคจำลองจากผู้ใช้งาน A1 และ A2 โดยเป็นข้อมูลทราฟฟิคของโปรโตรคอลที่แตกต่างกัน ไปยังผู้ใช้งาน B ซึ่งจะผ่านระบบเครือข่ายที่เป็นรูปแบบระหว่างองค์กร โดยที่เร้าเตอร์คู่ระหว่าง A1 และ A2 รวมทั้งคู่ระหว่าง B1 และ B2 สามารถทำงานได้ทั้งในรูปแบบของการกำหนดเร้าติ้งโดยคำสั่ง(Static routing) หรือการกำหนดเร้าติ้งโดยคำสั่งอัตโนมัติ(Dynamic routing) โดยที่การเชื่อมกันระหว่างองค์กร A และ B เราจะใช้การเชื่อมต่อแบบเร้าเตอร์ ที่อยู่ต่างองค์กร โดยเลือกใช้ BGP routing นอกจากนี้จะมีการลงโปรแกรมที่สามารถเก็บข้อมูลการรับ-ส่ง ที่ชื่อว่าไวร์ชาร์ก (wireshark) บนคอมพิวเตอร์ของผู้ใช้งาน A1, A2 และ ผู้ใช้งาน B เพื่อที่จะนำข้อมูลที่ได้ไปวิเคราะห์ ว่าเมื่อข้อมูลทราฟฟิคที่ส่งจากผู้ใช้งาน A1, A2 ไปยังผู้ใช้งาน B ว่าปลายทางผู้ใช้งาน B สามารถรับข้อมูลทราฟฟิคที่ส่งมาได้ครบหรือไม่ และใช้เวลาในการรับส่งเป็นเท่าไร

1.3.3 ขอบเขตของภาษาคอมพิวเตอร์

- ภาษาโปรแกรมเอกเอ็มแอล (XML)
  - การสร้างไฟล์เอกซ์เอ็มแอล ที่ระบุที่เก็บไฟล์พีแคป (Pcap file)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- การสร้างไฟล์เอกซ์เอ็มแอล ที่ระบุที่ค่าพารามิเตอร์ต่างๆ เช่น หมายเลขไอพีแอสเดรสเวอร์ชัน, โปรโตรคอล พอร์ท (Protocol port), โปรโตรคอล ไทป์ (Protocol type)

- ภาษาโปรแกรมซีชาร์ป (C# Programming Language)
  - ซอคเกตโปรแกรมของฝั่งเซิร์ฟเวอร์
  - ซอคเกตโปรแกรมของฝั่งไคลเอนต์
  - โปรแกรมของการอ่านพารามิเตอร์จากเอกสารเอกซ์เอ็มแอล
  - โปรแกรมของการแปลงและส่งต่อพีแคปไฟล์
  - การสร้างหน้าวินโดวส์ฟอร์ม

1.4 แผนการดำเนินงาน

1. ศึกษาข้อมูลและกระบวนการการทำงานของระบบเครือข่ายไอพีเวอร์ชั่น6
2. ศึกษาข้อมูลและกระบวนการการทำงาน และวิธีการเรียกข้อมูลทราฟฟิคจากไฟล์ภาษา XML
3. ศึกษาข้อมูลและกระบวนการเขียนซอคเกตโปรแกรม โดยภาษาซีชาร์ป เพื่อใช้ในการรับ-ส่งข้อมูล
4. ออกแบบ ตัวรูปแบบโปรแกรมที่จะพัฒนาที่ใช้งาน
5. ออกแบบ และจำลองระบบเครือข่ายไอพีเวอร์ชั่น4 ที่จะดักจับพฤติกรรมทราฟฟิคแบบเดิม
6. จัดเก็บข้อมูลพฤติกรรมทราฟฟิคแบบเดิมไว้ในรูปแบบไฟล์พีแคป (Pcap file)
7. ทดสอบการจำลองข้อมูลทราฟฟิคที่สร้างขึ้น บนเครือข่ายไอพีเวอร์ชั่น 6 ที่สร้างขึ้น โดยนำโปรแกรมที่สร้างขึ้นมาใช้งาน
8. วิเคราะห์ และสรุปผล การทดสอบ เพื่อติดตามแก้ไขปัญหา พร้อมประเมินและหาแนวทางแก้ไขหากเกิดข้อผิดพลาด

1.5 เทคโนโลยีที่ใช้ในการพัฒนาระบบ

1. ภาษาที่ใช้ในการทดสอบ : C#, XML
2. ระบบเนตเวิร์คที่ใช้ในการทดสอบ : IPv4, IPv6
3. โปรโตรคอล ต่างๆ ที่ใช้ในการทดสอบ
   - 3.1 เร้าท์ติ้งโปรโตรคอล : Local router, Static routing, Dynamic routing.
   - 3.2 แอพพลิเคชั่นโปรโตรคอล : FTP, HTTP, SMTP

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4. อุปกรณ์เครือข่ายที่ใช้ในการทดสอบ : Cisco ME3600, Cisco ASR1001

5. โปรแกรมที่ใช้ในการวิเคราะห์ข้อมูล : ไวร์ชาร์ก (Wireshark)

1.6 ประโยชน์จะได้รับ

1. สามารถช่วยลดค่าใช้จ่ายทุนขององค์กร (Capital Expenditure)และเพิ่มรายรับขององค์กร (Revenue & Income) เมื่อองค์กรต้องลงทุนเปลี่ยนเป็นระบบเครือข่ายไอพีเวอร์ชั่น6 เพื่อให้บริการลูกค้า
2. สามารถช่วยลดความยุ่งยาก การจัดหาจัดเตรียม และขั้นตอนในการทดสอบระบบเครือข่ายไอพีเวอร์ชั่น6 ได้
3. สามารถจำลองพฤติกรรมข้อมูลทราฟฟิคได้เสมือนจริงที่สุด

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2
ทฤษฎีและหลักการที่ใช้ในโครงการ

หลักการในการสร้างแบบจำลองข้อมูลทราฟฟิค ที่จะทดสอบระบบเครือข่ายไอพีเวอร์ชั่น6 ที่จะสามารถช่วยลดความยุ่งยาก ขั้นตอนในการทดสอบ ไม่จำเป็นต้องย้ายโปรแกรมต่างๆ มาลงบนคอมพิวเตอร์หรือเซิร์ฟเวอร์หลายๆเครื่องเพื่อทดสอบ ซึ่งจะตอบโจทย์ความสะดวกในการทดสอบมากกว่า อย่างแรกต้องคำนึงถึง
เทคโนโลยี และโปรโตรคอลที่สอดคล้องกับการใช้งานจริง ในชีวิตประจำวันของคนทั่วไป ซึ่งจะแบ่งออกเป็น 2 ส่วน ประกอบไปด้วย โปรโตรคอลที่ใช้ในการทดสอบ และระบบเครือข่ายรูปแบบต่างๆ ที่ใช้ในการทดสอบ

ก่อนที่จะทำการทดสอบข้อมูลทราฟฟิคต่างๆ ที่ทำงานบนระบบเครือข่ายไอพีเวอร์ชั่น6 ต้องมีการรู้ และอธิบายการทำงานต่างๆของระบบเครือข่ายไอพีเวอร์ชั่น6 ให้ได้ดีเสียก่อน เมื่อรู้และทราบถึงการทำงานของระบบเครือข่ายไอพีเวอร์ชั่น6 แล้วนั้น ก็จะสามารถเขียนซอคเกตโปแกรม ซึ่งเขียนโดยภาษาโปรแกรมซีชาร์ป ที่จะนำมาใช้ในการเขียนเพื่อควบคุมการรับ-สั่งข้อมูลทราฟฟิคระหว่างคอมพิวเตอร์ 2 เครื่องขึ้นไป ร่วมทั้งการเรียกข้อมูลจากไฟล์เอกซ์เอ็มแอล ซึ่งในไฟล์เอกซ์เอ็มแอลนั้นจะเป็นจุดที่จะบอกว่าให้ไปเรียก ไฟล์พีแคป(Pcap file) ที่จะเก็บข้อมูลทราฟฟิคจากเน็ตเวิร์กเดิม (network behavior) เพื่อส่งข้อมูลนี้ในการทดสอบระบบเครือข่ายไอพีเวอร์ชั่น6 นั่นเอง

ส่วนของรูปแบบของระบบเครือข่ายนั้น จะมีการจำลองรูปแบบระบบเครือข่ายทั้งส่งผ่านข้อมูลทราฟฟิคข้ามผ่านเร้าเตอร์ตัวเดียว(local router), การให้ข้อมูลทราฟฟิคข้ามระบบเครือข่ายโดยการกำหนดเส้นทางควบคุมด้วยชุดคำสั่ง (Static routing)และ การให้ข้อมูลทราฟฟิคข้ามระบบเครือข่ายโดยการกำหนดเส้นทางควบคุมด้วยชุดคำสั่งอัตโนมัติ (Dynamic routing) เพื่อให้สอดคล้องกับข้อมูลทราฟฟิคที่พวกใช้ในชีวิตประจำวันให้มากที่สุด

2.1 ภาพรวมของไอพีเวอร์ชั่น6

อธิบายเริ่มจากหมายเลขไอพีแอสแดรสซึ่งที่มีมาจาก 2 ส่วนรวมกัน คือ อินเทอร์เนตโปรโตรคอล (IP : Internet Protocol) และแอสแดรส (Address)โดยอินเทอร์เน็ตโปรโตรคอลหมายถึง กฎ, รูปแบบมาตรฐานที่กำหนดขึ้นเพื่อทำให้อุปกรณ์เน็ตเวิร์กสามารถสื่อสารกันได้ ซึ่งในระบบเน็ตเวิร์กต้องมีอุปกรณ์ที่ทำหน้าเป็นผู้ส่ง และผู้รับ ดังนั้นจึงจำเป็นต้องรู้ถึง ที่อยู่ของผู้ส่ง (sender address) และที่อยู่ของผู้รับ(receiver address) ความหมายอีกส่วนของ แอสแดรส คือ หมายเลขไอพีแอสแดรส ซึ่งมันจะทำหน้าที่ระบุตัวตนของอุปกรณ์เน็ตเวิร์ก โดยแต่และอุปกรณ์เน็ต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เวิร์กที่อยู่บนระบบเครือข่าย หรือระบบอินเทอร์เนตนั้นก็จะมีหมายเลขไอพีแอสแดรสที่ระบุตัวตนของมันเอง และแตกต่างกันออกไป

รูปที่ 2.1 จะกล่าวถึงในปัจจุบันที่มีการใช้ไอพีแอสแดรสเวอร์ชั่น4(IP version4) และยังมีการดำเนินการใช้งานไอพีแอสแดรสเวอร์ชั่น6 (IP version6) ควบคู่กันไป หลายท่านอาจจะสงสัยและ เวอร์ชั่น 1,2,3 หรือ เวอร์ชั่น 7,8,9 มันมีอยู่หรือไม่ คำตอบก็คือมีอยู่ครับ ตามมาตรฐานที่ถูกบัญญัติขึ้นโดย IETF(Internet Engineering Task Force)ซึ่งเป็นหน่วยงานมาตรฐานสากลของโลก โดยเวอร์ชั่นของไอพี (IP version number) จะมีตั้งแต่ 0 – 15 และใช้งานแตกต่างกันไปรวมทั้งที่ยังไม่ประกาศใช้งาน และสำรองเอาไว้ โดยที่ทั่วโลกใช้กันเป็นมาตรฐานคือไอพีแอสแดรสเวอร์ชั่น4 และไอพีแอสแดรสเวอร์ชั่น6 นั่นเอง

IP Version Numbers

Registration Procedures
IETF Standards Action
Reference
[RFC2780]

IP version ที่ใช้งานอยู่ในปัจจุบัน

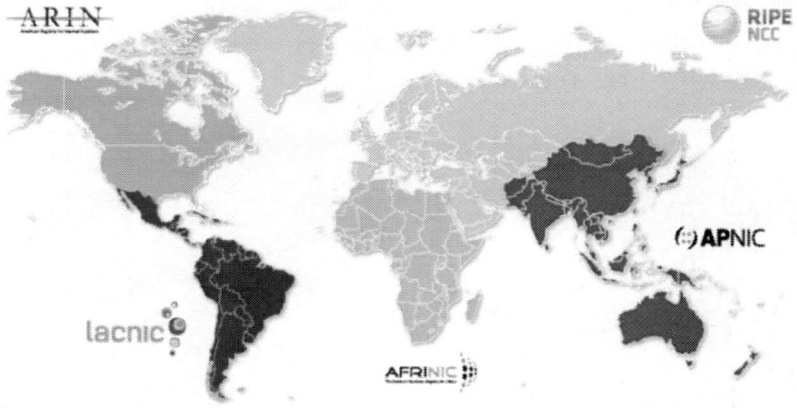
IP version ใหม่ ที่ทั่วโลกเริ่มนำมาใช้งาน

Decimal	Keyword	Version	Reference
0-1		Reserved	[Jon_Postel][RFC4928]
2-3		Unassigned	[Jon_Postel]
4	IP	Internet Protocol	[RFC791][Jon_Postel]
5	ST	ST Datagram Mode	[RFC1190][Jim_Forgie]
6	IPv6	Internet Protocol version 6	[RFC1752]
7	TP/IX	TP/IX: The Next Internet	[RFC1475]
8	PIP	The P Internet Protocol	[RFC1621]
9	TUBA	TUBA	[RFC1347]
10-14		Unassigned	[Jon_Postel]
15		Reserved	[Jon_Postel]

รูปที่ 2.1 รูปแสดงเวอร์ชันของไอพี (IP version number)

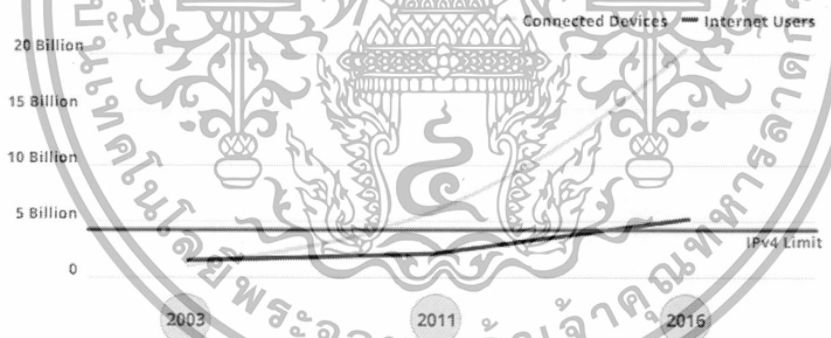
เมื่อรู้แล้วว่าหมายเลขไอพีแอสแดรสคืออะไร แล้วใครคือผู้ที่จะแจกจ่ายหมายเลขไอพีแอสแดรสให้ หรือสามารถกำหนดขึ้นเองได้ คำตอบคือจะมีหน่วยงานสากลที่ทำหน้าที่ควบคุมดูแลจัดสรรหมายเลยไอพีทั่วโลก การจัดสรรหมายเลขระบบอิสระ การจัดการแบ่งโซนดูแลระบบการตั้งชื่อโดเมน ประเภทสื่อ ตลอดจนหมายเลขและสัญลักษณ์อื่นที่เกี่ยวข้องกับอินเทอร์เน็ตโปรโตรคอลนั่นก็คือองค์กรที่กำหนดหมายเลขอินเทอร์เนต (Internet Assigned Numbers Authority,IANA) ซึ่งจะแบ่งเขตการแจกจ่ายไอพี ทั่วโลกแบ่งขอบเขตเป็นโซน(Regional Internet Registries) ซึ่งแบ่งเป็น 5 โซนคือ AFRINIC, APNIC, ARIN, LACNIC และ RIPE NCC ดังรูปที่ 2.2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.2 รูปแสดงการแบ่งโซนผู้ดูแลการกำหนดหมายเลขไอพีในอินเทอร์เนต

เกิดคำถามขึ้นอีกครั้งใช่หรือไม่ครับ ว่าเอาไอพี ที่แจกโดยองค์การหลัก 5 องค์กรที่แบ่งตามโซน มาใช้งานได้เลยหรือไม่ คำตอบคือยังไม่ได้ครับ เพราะว่าการแจกจ่ายไอพีจนถึงมือพวกใช้งานนั้นจะต้องผ่านมีหลายขั้นตอนครับ เริ่มจากองค์การกำหนดหมายเลขอินเทอร์เน็ต(IANA) แบ่งออกเป็นโซน ยกตัวอย่างเช่น ประเทศไทย ตั้งอยู่ในทวีปเอเชีย จะถูกแจกจ่ายหมายเลขไอพีโดย APNIC (Asia Pacific Network Information Centre) จากนั้นก็จะเป็นหน้าที่ขององค์กรในประเทศ ที่จะแจกจ่ายให้กับพวกบริษัทต่างๆต่อไป โดยประเทศไทยได้รับการแจกจ่ายหมายเลขไอพี มากเป็นอันดับ10 ของ APNIC



รูปที่ 2.3 รูปแสดงการใช้งานของIPv4 ของจำนวนผู้ใช้งานกับที่มีอยู่จริง

รูปที่ 2.3 เป็นรูปที่แสดงถึงความคาดการณ์ว่านในอนาคตข้างหน้า IPv4 จะไม่เพียงพอต่อการใช้งาน โดยสาเหตุหลักที่ทำให้ต้องโบกมือลาไอพีแอสแดรสเวอร์ชั่น4มีอยู่ 3 สาเหตุหลัก คือ

1. การเพิ่มขึ้นของจำนวนอุปกรณ์เนตเวิร์ก
2. การเพิ่มขึ้นของจำนวนผู้ใช้งาน
3. การโตขึ้นแบบก้าวกระโดดของระบบอินเทอร์เนต

ปัญหาหลักของหมายเลขไอพีที่มีอยู่ในปัจจุบัน คือไอพีแอสแดรสเวอร์ชั่น4สามารถจะลองรับได้แค่ 4ล้านเลขหมาย ซึ่งในปัจจุบันไม่เพียงพอต่อความต้องการของผู้ที่ใช้งานทั่วโลกมีอุปกรณ์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ที่ใช้งานโดยต้องมีหมายเลขไอพีกำกับจำนวนมากขึ้น เช่น โทรศัพท์, คอมพิวเตอร์ และโทรทัศน์ เป็นต้น

ความสำคัญของการมีไอพีแอสแดรสที่ไม่ซ้ำกันและสามารถเห็นกันได้ทั่วโลก คือช่วยผลักดันการพัฒนา แอพพลิเคชั่นแบบ peer-to-peer ที่ต้องการ หมายเลขไอพีจริงเป็นจำนวนมาก เช่นการทำ file sharing, online gaming ซึ่งแอพพลิเคชั่นเหล่านี้มีข้อจำกัดภายใต้ไอพีแอสแดรสเวอร์ชั่น4 เนื่องจากไม่มีหมายเลขไอพีจริง เพียงพอในเวลานี้

ไอพีแอสแดรสเวอร์ชั่น6 จะใช้ระบบเลขฐาน2จำนวน 128 บิต ดังนั้นจึงมีจำนวนหมายเลขไอพีแอสแดรสเวอร์ชั่น6 มีได้มากสุดถึง 2 ยกกำลัง 128 เลขหมายเลข นั่นคือจำนวนที่มากพอที่ประชากรทั่วโลกได้ใช้ไปอีกนานเลยทีเดียว ตัวอย่างหมายเลขไอพีแอสแดรสเวอร์ชั่น6 สามารถเขียนได้ตามแบบด้านล่าง

ตัวอย่างที่ 1 : 2001:0abc:85a3:0000:0000:0000:0F16:7654

ตัวอย่างที่ 2 : 2001:abc:85a3:0000:0000:0000:F16:7654

ตัวอย่างที่ 3 : 2001:abc:85a3::F16:7654

โดยทั้ง 3 ตัวอย่างด้านบนนั้น คือการแสดงหมายเลขไอพีแอสแดรสเวอร์ชั่น 6 ที่มีหมายเลขเดียวกัน แต่มีรูปแบบการเขียนที่แตกต่างกัน ซึ่งตัวอย่างที่1 คือการเขียนรูปแบบเต็ม ต่อมาคือตัวอย่างที่2 สามารถตัดเลข 0 ที่อยู่ข้างหน้าสุดของแต่ละช่วงออกไปได้เราเรียกว่า ลีดดิ้งซีโร่ (Leading Zero) ต่อมาคือตัวอย่างที่3 เป็นรูปแบบที่ย่อ โดยใช้ดับเบิ้ลโคลอน (Double Colon [::]) แทนจำนวนเลข 0 ที่อยู่ติดๆกันของแต่ละช่วงได้ โดยการเขียนหมายเลขไอพีแอสแดรสเวอร์ชั่น6 1 หมายเลข สามารถใช้ดับเบิ้ลโคลอน ได้แค่ครั้งเดียวเท่านั้น

แน่นอนว่าไอพีแอสแดรสเวอร์ชั่น 6 ที่ถูกออกแบบมานั้นย่อมมีประสิทธิภาพในทำงานได้ดีกว่าไอพีแอสแดรสเวอร์ชั่น4 โดยข้อผิดพลาดที่พบในไอพีเวอร์ชั่น4 นั้นจะถูกแก้ไขในไอพีเวอร์ชั่น6 นอกเหนือไปจากจำนวนหมายเลขไอพีแอสแดรสที่เพิ่มมากขึ้น สิ่งที่สำคัญที่สุดคือไอพีแอสแดรสเวอร์ชั่น 6 มีการปรับปรุงเฮดเดอร์ (header) ให้มีขนาดคงที่ และง่ายต่อการประมวลผลที่เร้าท์เทอร์ โดยบางส่วนของเฮดเดอร์ (header field) ที่ไม่จำเป็นจะถูกตัดออกเพื่อเป็นการลดโหลด การประมวลผลที่เร้าท์เทอร์ระหว่างทาง อีกทั้งยังเป็นการเพิ่มความสามารถพิเศษให้กับเครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2 ภาพรวมของเทคโนโลยีที่ใช้ในโครงงาน

- ภาษาโปรแกรมเอกซ์เอ็มเอล (XML: Extensible Markup Language)

ในการจำลองการทดสอบรูปแบบข้อมูลทราฟฟิคนั้น เราจะสร้างไฟล์เอกซ์เอ็มแอล เพื่อเป็นไฟล์ที่จะเป็นตัวชี้ หรือกำหนดว่า จะไปเลือกใช้ ไฟล์พีแคป(Pcap file) ไหน หรือสามารถกำหนดข้อมูลที่จะป้อนให้กับโปรแกรมซอคเกตก็ได้

รูปแบบการสร้างไฟล์เอกซ์เอ็มแอล โดยใส่ข้อมูลที่จะส่งผ่านโปรแกรมซอคเกต

```
<Root>
    <data>
        <PcapFile>C:\Users\Thel2oot\Desktop\test.pcap</PcapFile>
        <IP>fe80::414a:b5c6:73cf:7461%4</IP>
        <Port>1979</Port>
        <Protocol>UDP</Protocol>
    </data>
</Root>
```

รูปแบบการสร้างไฟล์เอกซ์เอ็มแอล โดยมีหลายไฟล์ที่จะส่งผ่านโปรแกรมซอคเกต

```
<Root>
    <XMLFile>C:\Users\Thel2oot\Desktop\test1.xml</XMLFile>
    <XMLFile>C:\Users\Thel2oot\Desktop\test2.xml</XMLFile>
    <XMLFile>C:\Users\Thel2oot\Desktop\test3.xml</XMLFile>
    <XMLFile>C:\Users\Thel2oot\Desktop\test3.xml</XMLFile>
</Root>
```

- ภาษาโปรแกรมซีชาร์ป (C# Programming Language)

แน่นอนว่าเมื่อมีระบบเครือข่าย มีรูปแบบการจำลองข้อมูลแล้ว มีไฟล์ข้อมูลทราฟฟิคที่ต้องการส่งแล้ว อีกสิ่งหนึ่งที่ต้องมีก็คือ โปรแกรมซอคเกต ที่จะเป็นโปรแกรมที่สร้างขึ้นมาเพื่อใช้ในการรับ-ส่งข้อมูลทราฟฟิค ซึ่งในโครงงานนี้จะใช้ภาษาโปรแกรมซีชาร์ปเข้ามาช่วยนั่นเอง โดยภาษาโปรแกรมซีชาร์ปคือภาษาคอมพิวเตอร์ประเภทโปรแกรมเชิงวัตถุ(object-oriented programming) ที่รองรับการพัฒนาเพื่อมาใช้งานด้านภาษาโปรแกรมสำหรับระบบเครือข่าย (network programming). ซึ่งการเขียนใช้ภาษาโปรแกรมซีชาร์ป เพื่อสร้างโปรแกรมซอคเกตนั้นจะแบ่งออกเป็นทั้ง

- โปรแกรมของการรับแพคเก็จจากเครือข่ายไอพีเวอร์ชั่น6

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- โปรแกรมของการส่งแพคเก็จจากเครือข่ายไอพีเวอร์ชั่น6
- โปรแกรมของการอ่านไฟล์เอกซ์เอ็มแอล
- การสร้างหน้าจอของโปรแกรม

- โปรโตรคอลสำหรับการโอนย้ายแฟ้มข้อมูล (FTP : File Transfer Protocol)

สาเหตุที่เลือกใช้ โปรโตรคอลสำหรับการโอนย้ายแฟ้มข้อมูลเพราะโลกปัจจุบันของ ต้องมีการใช้งานการถ่ายโอนไฟล์ ระหว่างเครื่องคอมพิวเตอร์ เช่น เจ้าหน้าที่ห้องสมุดเข้าไปดึงข้อมูลหนังสือ จาก ดาต้าเบส เซิร์ฟเวอร์ หรือ อาจารย์เข้าไปยัง เซิร์ฟเวอร์ส่วนกลางของสถาบัน เพื่อนถ่ายโอนไฟล์ ลงเซิร์ฟเวอร์ เพื่อให้นักศึกษาถ่าย ถ่ายโอนข้อมูลไปศึกษา นั่นคือรูปแบบการถ่ายโอนไฟล์ระหว่างผู้ใช้งาน (client) กับเครื่องคอมพิวเตอร์ส่วนกลาง ซึ่งต้องยอมรับว่าปัจจุบันมีการใช้งานของการโอนย้ายแฟ้มข้อมูลส่วนนี้เป็นจำนวนมากดังนั้นแล้ว ข้อมูลทราฟฟิคส่วนนี้ก็มีใช้อยู่เป็นจำนวนไม่น้อยเลยที่จะนำมาทำเป็นรูปแบบข้อมูลทราฟฟิคจำลอง

- โปรโตรคอลสำหรับแลกเปลี่ยนข้อมูลผ่านทางอินเทอร์เนต (HTTP : Hypertext Transfer Protocol)

สาเหตุที่เลือกใช้ โปรโตรคอลสำหรับการแลกเปลี่ยนข่าวสารผ่านทางอินเทอร์เนตเพราะปัจจุบันแล้วมีการใช้อินเทอร์เนตเพื่อความบันเทิง หรือ เพื่อการเรียนรู้ โดยใช้งานผ่าน WWW ที่จะเรียกใช้เวบเบาเซอร์ ทั้ง Firefox, Google Chrome เป็นต้นแน่นอนโปรโตรคอลนี้ นั้นใช้สำหรับสื่อสารแลกเปลี่ยนสารสนเทศผ่านอินเทอร์เน็ต โดยหลักแล้วใช้ในการรับเอกสารข้อความหลายมิติที่นำไปสู่การเชื่อมต่างๆ

- โปรโตรคอลสำหรับการรับ-ส่งจดหมายอิเลคทรอนิกส์ (SMTP : Simple Mail Transfer Protocol)

สาเหตุที่เลือกใช้ โปรโตรคอลสำหรับการรับ-ส่งจดหมายอิเลคทรอนิกส์ เพราะปัจจุบันการทำงานตามองค์กรต่างๆ รวมถึงนักศึกษา ต้องมีการใช้งานจดหมายอิเลคทรอนิกส์หรืออีเมล์ (email) ภายในองค์กร หรือสถาบันอยู่แล้ว ซึ่งโปรโตรคอลสำหรับการรับ-ส่งจดหมายอิเลคทรอนิกส์ นั้นจะใช้ในการรับ-ส่งในเครือข่ายอินเทอร์เน็ต สำหรับภายในองค์กร รวมถึงระหว่างเครื่องบริการอื่น ๆ ซึ่งสามารถส่งจดหมายอิเลคทรอนิกส์ ไปยังผู้ใช้ได้ทั่วโลก

- การใช้งานบนเร้าเตอร์ตัวเดียว (local router)

การทดสอบแบบ ใช้งานบนเร้าเตอร์ตัวเดียวนั้น จะทำการทดสอบโดย เครื่องคอมพิวเตอร์ต้นทาง และปลายทาง ต่อกันอยู่บนอุปกรณ์เนตเวิร์ก ตัวเดียวกัน เพื่อทดสอบว่าสามารถรับ-ส่งข้อมูลทราฟฟิค ผ่านหมายเลขไอพีแอสเดรสเวอร์ชั่น6ได้จริง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- การใช้งานภายในองค์กร (LAN)

การทดสอบบนระบบเครือข่ายรูปแบบการใช้งานภายในองค์กรนั้น จะทำการสร้างข้อมูลเร้าติ้งระหว่างอุปกรณ์เนตเวิร์ก ซึ่งอาจจะมีทั้งการให้ข้อมูลทราฟฟิคข้ามระบบเครือข่ายไอพีเวอร์ชั่น6 โดยการกำหนดเส้นทางควบคุมด้วยชุดคำสั่ง (Static routing)และ การให้ข้อมูลทราฟฟิคข้ามระบบเครือข่ายไอพีเวอร์ชั่น6 โดยการกำหนดเส้นทางควบคุมด้วยชุดคำสั่งอัตโนมัติ (Dynamic routing) ที่นิยมใช้กันในองค์กรต่างๆ เพื่อทดสอบว่าข้อมูลทราฟฟิคสามารถใช้งานได้จริง

- การใช้งานระหว่างองค์กร (WAN)

การทดสอบบนระบบเครือข่ายรูปแบบใช้งานระหว่างองค์กรนั้น จะจำลองการเชื่อมต่อระบบเครือข่ายข้ามองค์กร โดยจะใช้โปรโตรคอลในการเชื่อมต่อระหว่างองค์กร ที่เรียกว่า BGP Routing ส่วนภายในองค์กรแต่ละฝั่งจะมีทั้งระบบเครือข่ายไอพีเวอร์ชั่น6 ที่กำหนดเส้นทางควบคุมด้วยชุดคำสั่ง (Static routing)และ ระบบเครือข่ายไอพีเวอร์ชั่น6 ที่กำหนดเส้นทางควบคุมด้วยชุดคำสั่งอัตโนมัติ (Dynamic routing)เพื่อทดสอบว่าข้อมูลทราฟฟิคสามารถใช้งานได้จริง

2.3 เทคโนโลยีที่เกี่ยวข้องกับการพัฒนาระบบ

โปรโตรคอลสำหรับการโอนย้ายแฟ้มข้อมูล (FTP : File Transfer Protocol)

โปรโตรคอลสำหรับการโอนย้ายแฟ้มข้อมูลเป็นโปรโตรคอลที่ถูกกำหนดเพื่อการถ่ายโอนข้อมูลหรือการอัพโหลด/ดาวน์โหลด ข้อมูลระหว่างอุปกรณ์คอมพิวเตอร์ หรือบนอินเทอร์เนต โดยโปรโตรคอลสำหรับการโอนย้ายแฟ้มข้อมูล จะแบ่งออกเป็น 2 ส่วน คือ โปรแกรมที่ถูกติดตั้งไว้ที่เครื่องเซิร์ฟเวอร์ (FTP Server) ที่จะทำหน้าที่ให้บริการการถ่ายโอนไฟล์ หากมีการเชื่อมต่อ และเรียกใช้จากผู้ใช้งาน อีกส่วนคือโปรแกรมที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งาน (FTP Client) ที่จะทำหน้าที่เชื่อมต่อไปยังเซิร์ฟเวอร์ และทำการอัพโหลด/ดาวน์โหลด แฟ้มข้อมูล,ไฟล์ หรือเรียกเข้าไปเพื่อแก้ไขข้อมูลในไฟล์ หรือทำการลบไฟล์ เป็นต้น

โปรโตรคอลสำหรับการโอนย้ายแฟ้มข้อมูลนี้มีส่วนช่วยเป็นอย่างมากสำหรับชีวิตประจำวันของคนทั่วไป ซึ่งใช้ในการถ่ายโอนข้อมูลให้เป็นไปได้ง่ายมากขึ้นอาทิเช่น เจ้าหน้าที่ห้องสมุด, นักศึกษาเข้าไปดึงข้อมูลหนังสือ จาก ดาต้าเบส เซิร์ฟเวอร์ หรือ อาจารย์เข้าไปยังเซิร์ฟเวอร์ส่วนกลางของสถาบัน เพื่อน ถ่ายโอนไฟล์ ลงเซิร์ฟเวอร์ เพื่อให้นักศึกษาถ่าย ถ่ายโอนข้อมูลไปศึกษา นั่นคือรูปแบบการถ่ายโอนไฟล์ระหว่างผู้ใช้งานกับเครื่องเซิร์ฟเวอร์หรือองค์กรต่างๆ สามารถมีข้อมูลมากมายหลายรูปแบบที่ต้องการสื่อสารแลกเปลี่ยนกัน เช่น ข้อมูลข่าวสารประจำวัน บทความ ข้อมูลของทางแผนก ของทางบริษัท เป็นต้น สามารถที่จะการโอนย้ายแฟ้มข้อมูลจากเครื่องเซิร์ฟเวอร์มายังอีกเครื่องของผู้เรียกใช้งานได้อย่างรวดเร็ว โปรโตรคอลสำหรับการโอนย้ายแฟ้มข้อมูลจะเป็นตัวช่วยให้การได้รับข้อมูลเหล่านี้สามารถทำได้ง่ายยิ่งขึ้นเพียง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

อยู่ หน้าจอคอมพิวเตอร์เท่านั้น ผู้ใช้งานสามารถใช้ ถ่ายโอนข้อมูลจำนวนมากจากเครื่องเซฮเวอร์มายังแฟ้มข้อมูลบนคอมพิวเตอร์ของผู้เรียกใช้งานได้

โปรโตรคอลสำหรับการแลกเปลี่ยนข้อมูลผ่านทางอินเทอร์เนต (HTTP : Hypertext Transfer Protocol)

โปรโตรคอลสำหรับการแลกเปลี่ยนข้อมูลผ่านทางอินเทอร์เนตเป็นโปรโตรคอลที่ใช้ในการร้องขอ และตอบกลับ ระหว่างเครื่องผู้ใช้งานที่ใช้เว็บเบาเซอร์ กับเครื่องเซิร์ฟเวอร์ โดยทำงานบนโปรโตคอล TCP โดยจะใช้พอร์ตหมายเลข 80 รวมถึงใช้ในการทำงานร่วมกันกับสารสนเทศของสื่อผสม เพื่อให้ได้รับซึ่งทรัพยากรที่เชื่อมโยงกันระหว่างผู้ใช้งานและเครื่องเซิร์ฟเวอร์

โดยเมื่อทำการเรียกโปรแกรมพวกเว็บเบาเซอร์ อาทิเช่น Firefox, Google Chrome, Safari, Opera และ Microsoft Internet Explorer เพื่อเรียกดูข้อมูลหรือเว็บเพจ โปรแกรมเว็บเบาเซอร์จะทำงานโดยใช้หลักการโปรโตรคอลสำหรับการแลกเปลี่ยนข้อมูลผ่านทางอินเทอร์เนตซึ่ง โปรโตรคอลนี้ทำให้เซิร์ฟเวอร์ส่งข้อมูลมาให้เบาเซอร์ของผู้ใช้งานตามต้องการ และเบาเซอร์จะนำข้อมูลมาแสดงผลบนจอภาพได้อย่างถูกต้อง โดยการแลกเปลี่ยนข้อมูล ระหว่างผู้ใช้งานปลายทาง (Client)และ เครื่องเซิร์ฟเวอร์ จะมีการส่งข้อมูลแบบไม่ได้ทำการเข้ารหัส ระหว่างกันใ

โปรโตรคอลสำหรับการรับ-ส่งจดหมายอิเลคทรอนิกส์ (SMTP : Simple Mail Transfer Protocol)

โปรโตรคอลสำหรับการรับ-ส่งจดหมายอิเลคทรอนิกส์เป็นโปรโตรคอล เพื่อกำหนดไว้ใช้ในการรับ-ส่งจดหมายอิเลคทรอนิกส์ หรืออีเมล์ (e-mail) ในอินเทอร์เน็ต ซึ่งผู้ใช้งานส่งไปยังเครื่องบริการอื่น ๆ หรือผู้ใช้งานคนอื่นๆที่อยู่ภายใต้องค์กรเดียวกัน ซึ่งสามารถส่งจดหมายอิเลคทรอนิกส์ไปได้ทั่วโลก

โปรโตรคอลสำหรับการรับ-ส่งจดหมายอิเลคทรอนิกส์ก็เหมือนผู้ให้บริการส่งจดหมายแบบทั่วไป แต่จดหมายนี้มันอยู่ในรูปแบบดิจิทัลไม่สามารถจับต้องไม่ได้ โดยตามแต่ละองค์กรก็จะมีการกำหนดสิทธิ์ หรือต้องตรวจสอบผู้ใช้งานก่อนเลยว่าเป็นผู้ใช้งาน หรือลูกค้าองค์กร หรืออยู่ในฐานข้อมูลขององค์กรหรือไม่ ถ้าอยู่ในระบบก็จะยอมให้ส่งจดหมายอิเลคทรอนิกส์ออกไปดังนั้น โปรโตรคอลนี้เปรียบเสมือนเซิร์ฟเวอร์ขาออกของจดหมายอิเลคทรอนิกส์ซึ่งจะถูกตั้งค่าโดยผู้ดูแลหรือมาจากผู้ให้บริการ (email server hosting)ซึ่งแต่ละองค์กรก็ยังมีข้อกำหนดแตกต่างกันไป อาทิเช่นกำหนดให้ส่งอีเมล์ได้ไม่เกินกี่ฉบับ ต่อชัวโมง หรือกี่ฉบับต่อวัน หรือ มีพื้นที่ในการจัดเก็บอีเมล์จำนวนเท่าไร เป็นต้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปแบบการกำหนดเส้นทางเร้าท์โดยคำสั่งด้วยตัวเอง (Static Routing)

การกำหนดเส้นทางของเร้าท์โดยคำสั่งด้วยตัวเอง เข้าไปยังอุปกรณ์เร้าเตอร์(Router) จะเป็นแบบค่าคงที่ไม่สามารถปรับเปลี่ยนรูปแบบเส้นทางของเร้าท์ได้โดยอัตโนมัติ จนกว่าจะเข้าไปแก้ไขด้วยตัวเองอีกครั้งซึ่งเร้าติ้งมีขึ้นเพื่อบอกให้เร้าเตอร์ทราบว่า หากต้องการจะส่งข้อมูลทราฟฟิค ในรูปแบบที่เรียกว่าแพ็กเก็ต (Packet) ไปยังเน็ตเวิร์กแอดเดรสต่างๆ จะต้องส่งไปที่เส้นทางใด ออกทางอินเทอร์เฟส (interface)หรือส่งไปหาอุปกรณ์เร้าเตอร์ตัวถัดไปเป็นตัวไหน(Next Hop Address) โดยการกำหนดค่าเส้นทางเร้าท์วิธีการนี้หากเป็นเส้นทางที่ยาว ซับซ้อน มีอุปกรณ์เร้าเตอร์จำนวนมาก และมีเน็ตเวิร์กแอดเดรสต่างๆจำนวนมาก ผู้ดูแลระบบเครือข่ายก็จะต้องใช้เวลามากในการกำหนดค่าเส้นทางของเร้าท์เข้าไปในเร้าเตอร์แต่ละตัว ตลอดเส้นทางบนระบบเครือข่าย โดยหลังจากที่ทำการกำหนดค่าลงไปแล้วนั้น สามารถดูค่าเส้นทางของเร้าท์ต่างๆที่อยู่ในเร้าเตอร์ได้โดยดูจากตารางข้อมูลเส้นทางทั้งหมด(Routing Table) สมมติว่าเรามีทางออกให้กับแพ็กเก็ต ได้หลายเส้นทางบนเร้าเทอร์นั้น จะต้องมีการกำหนดค่าที่จะใช้ในการเลือกว่าเส้นทางไหนจะเป็นทางเลือกที่ดีที่สุด ส่วนเส้นที่ไม่ได้ถูกเลือกจะเป็นเส้นทางสำรอง ในกรณีที่เส้นทางหลักเกิดความเสียหาย โดยจะกำหนดค่าที่เรียกว่าค่าลำดับความสำคัญ(AD : Administrative Distance) การกำหนดเส้นทางของเร้าท์เข้าไปในตัวเร้าเตอร์ด้วยตัวเองนั้น จะมีค่าลำดับความสำคัญที่ดีกว่า การกำหนดเส้นทางของเร้าท์เข้าไปในตัวเร้าเตอร์โดยคำสั่งอัตโนมัติ (Dynamic Routing)

รูปแบบการกำหนดเส้นทางเร้าท์โดยคำสั่งแบบอัตโนมัติ (Dynamic Routing)

การกำหนดเส้นทางเร้าท์โดยคำสั่งแบบอัตโนมัติ เป็นการสั่งให้เร้าเตอร์ เริ่มการใช้งานของเร้าติ้งโปรโตคอล(Routing Protocol)ที่คำนวณเส้นทางอัตโนมัติขึ้นมา ซึ่งจะลดภาระของผู้ดูแลระบบเครือข่าย และทำให้การจัดการเน็ตเวิร์กขององค์กรเป็นไปได้อย่างง่ายดาย เมื่อเริ่มการใช้งานเร้าติ้งโปรโตคอลที่เป็นแบบอัตโนมัติ ขึ้นบนเร้าเตอร์แล้วนั้น มันจะเริ่มกำหนดค่าเส้นทางต่างๆ ว่าเน็ตเวิร์กแอสแดรสนี้ต้องออกไปยังอินเทอร์เฟสใดของเร้าเตอร์ เร้าเตอร์ตัวถัดไปเป็นตัวไหนบ้าง จากนั้นเร้าเตอร์เพื่อนบ้านแต่ละตัวที่อยู่ข้างๆกัน (Neighbor router) ก็จะทำการแลกเปลี่ยนข้อมูลเส้นทางเร้าท์ระหว่างกัน ทำให้เกิดฐานข้อมูลของเส้นทางเร้าท์ และเร้าท์เตอร์แต่ละตัวก็จะทำการบันทึกเส้นทาง ทางออกที่ดีที่สุดเข้าไปในเร้าติ้งเทเบิล ทำให้เกิดข้อมูลเส้นทางเร้าท์ที่มีความสมบูรณ์ และที่สำคัญเมื่อระบบเครือข่ายมีการเปลี่ยนแปลง หรือเส้นทางใดเกิดเสียหายเร้าติ้งโปรโตคอลแบบอัตโนมัติ จะยังสามารถรู้ถึงความเปลี่ยนแปลงต่างๆบนอินเทอร์เฟสมันจะทำการอัพเดทข้อมูลเร้าติ้งของตัวมันเอง และอัพเดทข้อมูลส่งต่อไปให้เร้าเตอร์เพื่อนบ้านภายในระบบเครือข่ายตามเน็ตเวิร์กโทโพโลยีต่อไป ทำให้เร้าติ้งเทเบิลได้รับการปรับปรุงให้สอดคล้องกับสภาพความเป็นจริงของระบบเครือข่ายภายในเน็ตเวิร์กโทโพโลยีโดยอัตโนมัติ ยกตัวอย่างเช่น เร้าเตอร์เพื่อนบ้านเกิดเสียหายทำให้ปิดตัวลง อินเทอร์เฟสของเร้าเตอร์จะดาวน์ แสดงว่าเส้นทางนี้ไม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

สามารถผ่านไปได้ เร้าเตอร์จะหาเส้นทางอื่นในการส่งแพ็กเก็ตออกไป หรือในเคสที่สายไฟเบอร์ระหว่างอุปกรณ์เร้าเตอร์ที่ต่อกับเร้าเตอร์เพื่อนบ้านที่เป็นเส้นทางหลักเสียหาย (WAN Link Failure) ทำให้ระบบเครือข่ายภายในเน็ตเวิร์กโทโพโลยีมีปัญหา เร้าเตอร์ก็จะหาเส้นทางอื่นในการส่งแพ็กเก็ตออกไปเช่นกัน ซึ่งเป็นความสามารถที่หาไม่ได้ในการใช้กำหนดเส้นทางเร้าท์โดยคำสั่งด้วยตัวเอง (Static Routing)การกำหนดเส้นทางเร้าท์โดยคำสั่งแบบอัตโนมัติ จะมีการทำงานที่รวดเร็วมากเมื่อการเกิดเสียหายภายในระบบ โดยใช้เวลาในการกลับมาให้บริการ (Convergence Time) ที่ดีกว่า และทำให้ระบบมีความเสถียรมากกว่า วิธีการกำหนดเส้นทางเร้าท์โดยคำสั่งแบบอัตโนมัตินั้นมีให้เลือกใช้หลายโปรโตรคอลด้วยกัน ซึ่งที่เป็นที่นิยมกันและใช้ในการทดลองนี้ คือ OSPF (Open Shortest Path First) และ BGP (Border Gateway Protocol) ซึ่งทั้ง 2 เป็นโปรโตรคอลที่ใช้กันอย่างแพร่หลาย ร่วมถึงเป็นมาตรฐานสากล(Open Standard) ที่อุปกรณ์ของทุกผู้ผลิตจำเป็นต้องมีรองรับ

OSPF จัดเป็นเร้าท์ติ้งโปรโตรคอลสำหรับการหาเส้นทางเร้าท์ที่ใช้ภายในระบบเครือข่ายอิสระเดียวกัน (AS : Autonomous Systems)ที่เชื่อมโยงกัน เกือบทุกองค์กรนิยมใช้ OSPFกับระบบเครือข่ายภาพในองค์กร ซึ่งได้รับความนิยมและมีสำคัญมากในปัจจุบัน OSPF และโปรโตรคอลนี้สามารถสนับสนุนการทำงานทั้งระบบเครือข่ายไอพีเวอร์ชั่น4 และระบบเครือข่ายไอพีเวอร์ชั่น6 โดยโปรโตรคอลนี้มีอัลกอริทึ่มในการค้นหาเส้นทางเร้าท์ด้วยตัวเอง ซึ่งเปรียบเสมือนว่าตัวของเร้าเตอร์ที่กำลังใช้งาน OSPF นั้นจะรับรู้การเปลี่ยนแปลงในระบบเครือข่ายได้อย่างรวดเร็ว รวมถึงสามารถรองรับการขยายตัวของระบบเครือข่ายในอนาคตได้ด้วย ซึ่งถ้ามีเร้าเตอร์เพิ่มเข้ามาในระบบเครือข่าย ก็เพียงตั้งค่าในเร้าเตอร์ ให้ทำงานด้วย OSPF ที่ใช้ในระบบเครือข่าย ณ ขณะนั้น เพียงเท่านี้อัลกอริทึ่มของโปรโตรคอลจะทำงานเรียนรู้เส้นทางภายในเครือข่าย และใช้ในการป้องกันเร้าท์ติ้งลูปในระบบเครือข่าย พร้อมทั้งอัพเดทกันภายในระบบเครือข่ายว่ามีเร้าเตอร์ตัวใหม่เพิ่มเข้ามา โดยเร้าเตอร์ตัวนี้เป็นปลายทางของหมายเลขไอพีแอสแดรสอะไรบ้าง และต้องไปเส้นทางไหนถึงจะดีที่สุด การเลือกเส้นทางของเร้าท์ติ้งโปรโตรคอล OSPF จะใช้การคำนวณโดยถ้าเส้นทางไหนที่มีค่าของแบนวิธท์ (Bandwidth)มากตลอดทั้งเส้นทาง ก็จะเลือกเส้นทางเร้าท์นั้นเป็นเส้นทางหลัก

<u>ข้อดีของ OSPF</u>

- มีการสนับสนุนการแบ่งเน็ตเวิร์กเป็นลำดับขั้น (Hierarchical Network)ช่วยให้สามารถขยายระบบเครือได้กว้างมาก เพราะสามารถแบ่งระบบเป็นระบบย่อยๆ โดยมีจุดศูนย์กลางในการแลกเร้าท์ติ้งที่ระบบเครือข่ายที่เป็นลำดับชั้นบน
- มีการใช้อัลกอริทึมที่เรียกว่า Diijkstra ในการค้นหาเส้นทาง และป้องกันเราติ้งลูป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
146489

- มีการสนับสนุนระบบเร้าท์ติ้งที่เรียกว่า Classless Routing และ CIDR (Classless Interdomain Routing)ทำให้สามารถประกาศเส้นทางเร้าท์ติ้งของหมายเลขไอพีแอสแดรสได้เป็นแบบย่อย

- มีความสามารถในการลดขนาดของเราติ้งเทเบิล โดยใช้วิธีการ Route Summarization

- มีความสามารถในการอัพเดตเร้าท์ติ้ง ที่ควบคุมการส่งได้ โดยจะอัพเดทเมื่อมีการเปลี่ยนแปลงในระบบเครือข่ายเท่านั้น

- มีความสามารถในการสนับสนุน ความปลอดภัยภายในระบบเครือข่าย โดยก่อนที่จะเชื่อมต่อเพื่อสร้างเร้าท์ติ้งเทเบิ้ล อาจจะมีการตั้งค่ารหัสสำหรับการคุยกับของ OSPF ในระบบเครือข่ายนั้น

BGP จัดเป็นโปรโตรคอลที่ใช้สำหรับการแลกเปลี่ยนข้อมูลของเส้นทางระหว่างเครือข่ายอิสระ เชื่อมต่อเครือข่ายย่อยหลายๆเครือข่ายที่อยู่คนละ AS (Inter Autonomous System) ในระบบเครือข่ายแบบอัตโนมัติ เร้าท์ติ้งโปรโตรคอล BGP ได้รับความนิยมใช้บนระบบอินเตอร์เน็ต ใช้ในการแลกเปลี่ยนค่าในการค้นหาเส้นทางเร้าท์สำหรับอินเทอร์เน็ต เพื่อเลือกเส้นทางที่ดีที่สุด และถูกใช้งานทางฝั่งผู้ให้บริการระบบเครือข่ายอินเทอร์เน็ต (ISP)ด้วยผู้ใช้งานระบบเครือข่ายภายในองค์กรทั่วไป เช่น มหาวิทยาลัย หรือบริษัทต่างๆ ส่วนใหญ่จะใช้การกำหนดเส้นทางเร้าท์โดยคำสั่งแบบอัตโนมัติ พวก OSPF ในการค้นหาเส้นทางเร้าท์ของระบบเครือข่ายภายในองค์กร แต่องค์กรโดยส่วนใหญ่ก็จำเป็นที่ต้องมีการติดต่อระหว่างเครือข่ายภายนอก โดยต่อไปฝั่งผู้ให้บริการระบบเครือข่ายอินเทอร์เน็ตจะใช้เร้าท์ติ้งโปรโตรคอล BGPในการเชื่อมต่อ เมื่อเร้าท์ติ้งโปรโตรคอล BGP ถูกใช้งานระหว่างเครือข่ายอิสระ หลายๆเครือข่ายจะเรียกว่าเป็นการเชื่อมต่อระบบเครือข่ายรูปแบบ External BGP (EBGP) แต่ถ้า ใช้สำหรับงานเชื่อมต่อระบบเครือข่ายย่อยภายในเครือข่ายอิสระเดียวกันจะถูกอ้างอิงว่าเป็น Interior BGP (IBGP)

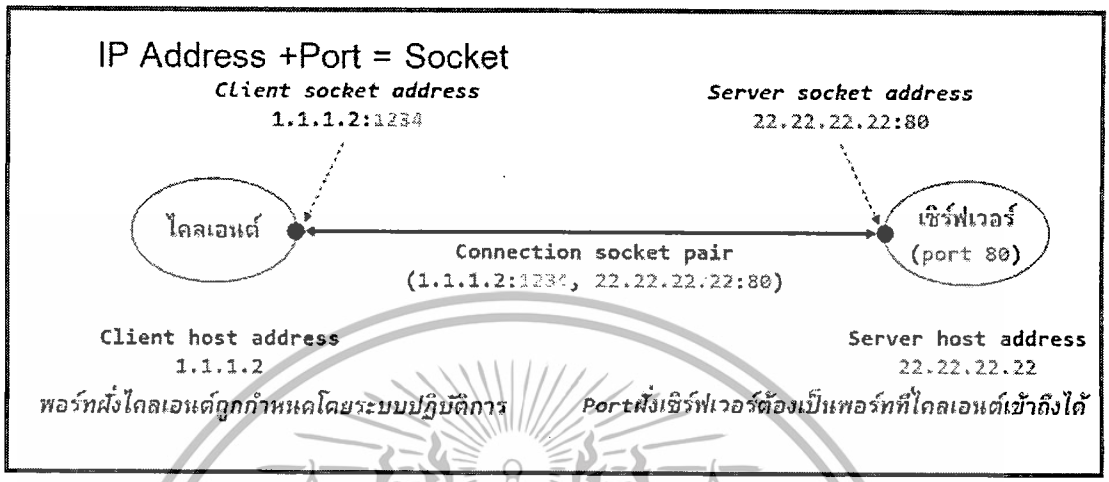
ซอคเกตโปรแกรมโดยภาษาโปรแกรมซีชาร์ป (Socket Program by C#)

ส่วนนี้จัดว่าเป็นส่วนสำคัญพอๆกับระบบเครือข่ายที่ใช้ในการทดสอบ นั้นก็คือการสร้างโปรแกรมจำลองข้อมูลทราฟฟิคจำลอง ซึ่งก็คือการทำซอคเกตโปรแกรม ที่ใช้ในการรับส่งข้อมูลทราฟฟิคระหว่างเซิร์ฟเวอร์ และ ไคลเอนต์นั่นเอง โดยเราจะแบ่งซอคเกตโปรแกรมออกเป็น 2 รูปแบบคือซอคเกตโปรแกรมฝั่งเซิฟร์เวอร์ (Server Socket Program) และ ซอคเกตโปรแกรมฝั่งไคลเอนต์ (Client Socket Program)

ซอคเกตโปรแกรมฝั่งเซิฟร์เวอร์ (Server Socket Program) เป็นโปรแกรมที่ทำงานบนเครื่องที่มีซอคเกต ที่ผูกกับพอร์ทบนเครื่องและรอการเรียกเข้า (request) โดยจะถูกส่งมาจากฝั่งไคลเอนต์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ซอคเกตโปรแกรมฝั่งไคลเอนต์ (Client Socket Program) จะต้องรู้ว่าหมายเลขไอพีแอสเดรสของเครื่องที่มีซอคเกตโปรแกรมฝั่งเซิฟร์เวอร์ทำงานอยู่ และพอร์ทที่เครื่องนั้นรอการเรียกเข้า (request) ด้วย



รูปที่ 2.4 รูปแสดงหลักการของซอคเกตโปรแกรม

รูปที่ 2.4 จะแสดงถึงหลักการของ ซอคเกต(Socket) ที่ได้เชื่อมต่อการสื่อสารระหว่างจุดสองจุด (เครื่องสองเครื่อง) แบบไปกลับได้ระหว่างโปรแกรมสองโปรแกรม (ฝั่งเซิร์ฟเวอร์ กับ ไคลเอนต์) ภายในเครือข่ายเดียวกัน โดยซอคเกตจะหมายถึง ที่อยู่ของเครื่อง (IP Address) กับที่อยู่ของโปรแกรมในเครื่อง (Port)

"ที่อยู่ของเครื่อง (IP Address) + ที่อยู่ของโปรแกรมในเครื่อง (Port) = ซอคเกต (Socket)"

โดยการสร้างโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริงนี้ จะใช้ C# ในการสร้าง โดยใน C# นั้นจะมีโปรโตรคอลในการเชื่อมต่อนั้น 2 แบบ คือ TCP/IP และ UDP/IP โดยส่วนของ Microsoft .Net framework นั้นจะมี namespace 2 ส่วน ที่ใช้สำหรับพวกอินเทอร์เนตโปรโตรคอล (Internet protocol)เพื่อทำให้ซอคเกตโปรแกรมของสามารถที่จะรับส่งข้อมูลผ่านอินเทอร์เนตได้

```
using System.Net;
using System.Net.Sockets;
```

ถัดมาจะเป็นส่วนการเริ่มสร้างการเชื่อมต่อระหว่างเซิร์ฟเวอร์และไคเอนต์ โดยจะมีรูปแบบตามด้านล่าง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปแบบการทำงานของโปรแกรมฝั่งไคลเอนต์

สร้างการเชื่อมต่อไปยังเซิร์ฟเวอร์ --->ส่งการเรียก (request)ไปยังเซิร์ฟเวอร์ --->รับการตอบรับ (response)จากเซิร์ฟเวอร์

รูปแบบการทำงานของโปรแกรมฝั่งเซิร์ฟเวอร์

เซิร์ฟเวอร์จะรอการเรียกเข้า (request) จากไคลเอนต์ --->เซิร์ฟเวอร์ได้รับการเรียกเข้า (request) จากไคลเอนต์ --->เซิร์ฟเวอร์ส่งการตอบรับ(response)ไปไคลเอนต์

ภาษาโปรแกรมเอกซ์เอ็มแอล (XML)

ภาษาโปรแกรมเอกซ์เอ็มแอล (XML : Extensible Markup Language) คือภาษาโปรแกรมที่เน้นสำหรับการใช้งานทั่วไป เพื่อไว้ใช้ติดต่อกันในระบบที่มีความแตกต่างกัน เช่น การใช้คอมพิวเตอร์มี่มีระบบปฏิบัติการคนละรูปแบบ หรืออาจจะเป็นคนละโปรแกรมประยุกต์ ที่จำเป็นต้องการสื่อสารข้อมูลระหว่างกัน ซึ่งในการค้นคว้าอิสระนี้เราจะสร้างเอกสารเอกซ์เอ็มแอลขึ้นมาเพื่อจำลองเป็นโปรโตรคอลรูปแบบต่างๆ และมีการกำหนดขนาดของแพคเก็จที่จะถูกส่งลงบนเอกสารเอกซ์แอลนี้

การสร้างเอกสารรูปแบบ XML จะมี2ส่วนคือ กำหนดชื่อแท็ก (Element) และชื่อแอตทิบิวต์ (Attribute) ให้ได้ตามความต้องการของเอกสารเอกซ์เอ็มแอลที่จะใช้งาน โดยเอกสารเอกซ์เอ็มแอลนั้นจะต้องมีความเป็นเวลฟอร์ม (Well-formed) หมายถึงเอกสารที่มีการใช้รูปแบบของเอกซ์เอ็มแอล (XML Syntax) ถูกต้องจามมาตรฐาน มีการปิด-เปิดแท็กที่สมบูรณ์ ทำให้เอกสารเอกซ์เอ็มแอล ถูกใช้ในการติดต่อกับระบบที่ต่างกัน เนื่องจากมีความสะดวก และง่าย ดังนั้นการนำเอกสารรเอกซ์เอ็มแอลไปใช้งาน จะสนใจแต่ข้อมูลที่เน้นด้วยการแท็ก โดยดีทีดี (DTD) และ ซคีม่า (Schema) จะเป็นตัวกำหนดว่าเอกสารเอกซ์เอ็มแอลนั้น จะต้องมีแท็กอะไร อย่างไร ภายในแท็กนั้นจะมีแท็ก แอตทิบิวต์ หรือข้อมูลอะไรได้บ้าง

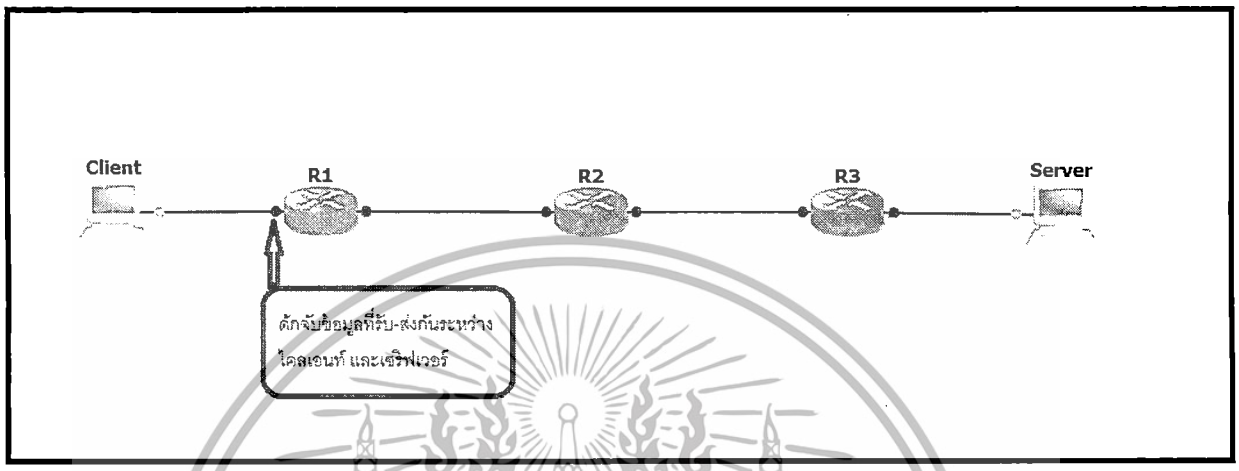
โปรแกรมวิเคราะห์ข้อมูลระบบเครือข่าย ไวร์ชาร์ก (WireShark)

โปรแกรมวิเคราะห์ข้อมูลระบบเครือข่ายไวร์ชาร์ก เป็นโปรแกรมที่นิยมใช้ในการวิเคราะห์ข้อมูลที่รับ-ส่งกันบนเครือข่ายเนตเวิร์ก โดยสนับสนุนโปรโตรคอลต่างๆ หลากหลายมาตรฐาน สามารถดูการรับ-ส่งข้อมูลได้ทั้งแบบต่อเนื่อง (realtime) และดูย้อนหลังได้จากค่าที่บันทึกไว้ โปรแกรมตัวนี้สามารถทำงานได้บนหลายระบบปฏิบัติการ

การทำงานของโปรแกรมไวร์ชาร์ก มีอยู่ 2 ขั้นตอน คือ ขั้นตอนแรกโปรแกรมจะทำการดักจับข้อมูลที่รับ-ส่ง และบันทึกข้อมูลทุกอย่างที่ผ่านเนตเวิร์กโมดูลที่ผู้ใช้งานกำหนด อาจจะเป็นผ่านเนตเวิร์กอินเทอร์เฟสที่เป็นการ์ดแลน(LAN network interface) หรือเนตเวิร์กอินเทอร์เฟสแบบไร้สาย (wireless network interface) อีกขั้นตอนคือกขั้นตอนการแสดงผล ส่วนนี้อยู่ที่ผู้ใช้งานต้องการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จะให้แสดงผลข้อมูลการรับ-ส่งทั้งหมดบนเครือข่ายเนตเวิร์ก หรือว่าต้องการเพียงแค่บางโปรโตรคอลที่สนใจเท่านั้น ซึ่งสามารถดูได้ตั้งแต่ ข้อมูลแพคเก็จนี้ส่งมาตอนเวลาเท่าไร ข้อมูลในแพคเก็จมีอะไรบ้าง เป็นโปรโตรคอลอะไร ใช้พอร์ตอะไรในการส่ง เป็นต้น เพื่อที่จะช่วยในการวิเคราะห์เวลาระบบเครือข่ายในองค์กรมีปัญหา เกิดจากสาเหตุใดได้บ้าง ทั้งนี้ทั้งนั้นก็ขึ้นอยู่กับเนตเวิร์กทลู (Network Tools) รูปแบบอื่นที่จะนำมาช่วยในการวิเคราะห์ร่วมกันด้วย



รูปที่ 2.5 รูปแสดงการดักจับข้อมูลทราฟฟิค

จากรูปที่ 2.5 จะเป็นการอธิบายขั้นตอนการทำงานของโปรแกรมไวร์ชาร์ก โดยจะเป็นการดักจับแพคเก็จที่ทางไคลเอนท์จะส่งข้อมูลไปหาทางเซริฟเวอร์ เพื่อที่จะนำข้อมูลที่ได้จากเน็ตเวิร์กเดิม มาทำการตัดค่าเพื่อใช้ในการทดสอบระบบเครือข่ายไอพีเวอร์ชั่น6 หลังจากนั้นเราจะนำข้อมูลทราฟฟิคเดิมที่ดักจับได้จากโปรแกรมไวร์ชาร์ก ไปทำการใช้ในการทดลองทดอสบระบบเครือข่ายไอพีเอวร์ชั่น6 โดยจะมีไฟล์เอกซ์เอ็มแอลเป็นตัวเรียกใช้งานไฟล์พีแคป นั่นเอง

2.4 สรุป

ในการค้นคว้าอิสระเรื่องการสร้างโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง โดยใช้ข้อมูลทราฟฟิคเดิมที่ถูกดักจับในรูปพีแคปไฟล์เพื่อทดสอบระบบเครือข่ายไอพีเวอร์ชั่น6 ปัจจัยสำคัญคือการลดความยุ่งยาก ขั้นตอนในการทดสอบโดยไม่จำเป็นต้องย้ายโปรแกรมต่างๆ มาลงบนคอมพิวเตอร์หรือเซิร์ฟเวอร์หลายๆเครื่องเพื่อทดสอบ ทำให้มีความสะดวกสบายมากกว่าการทดสอบแบบเดิม โดยการพัฒนาโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริงขึ้นมากซอคเกตโปรแกรมจากภาษาซีชาร์ป

นอกจากนี้ยังมีเอกสารเอกซ์เอ็มแอลที่สร้างขึ้นเพื่อใช้สำหรับเป็นตัวเก็บค่าพารามิเตอร์ต่างๆ และเป็นพ้อยท์เตอร์ชี้ไปยังที่เก็บพีแคปไฟล์ เพื่อให้สะดวกเวลาต้องการจำลองการส่งหลายรูปแบบก็สามารถเรียก เอกสารเอกซ์เอ็มแอลบนโปรแกรมได้เลย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

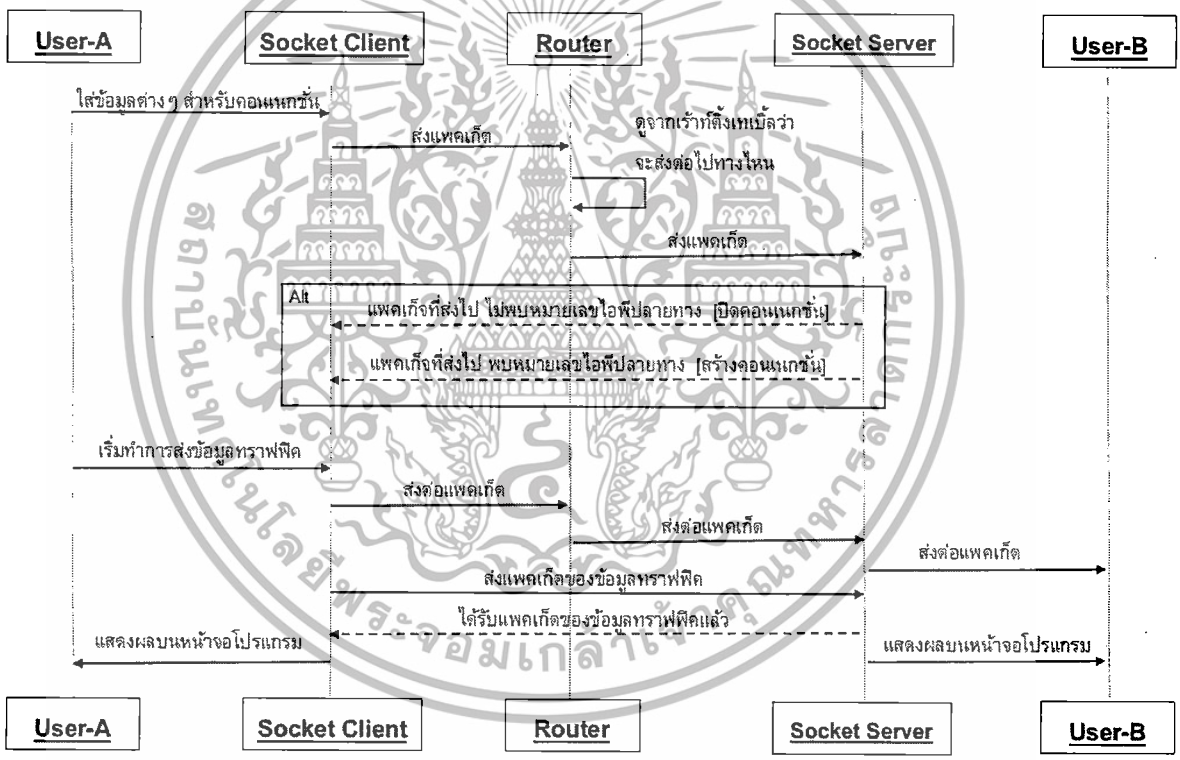
ส่วนสำคัญหลักคือระบบเครือข่ายทั้งไอพีเวอร์ชั่น 4 และ 6 ที่จะมีการจำลองการทดสอบหลากหลายรูปแบบเพื่อให้สอดคล้องกับการใช้งานในชีวิตประจำวัน รูปแบบเร้าท์ติ้งโปรโตรคอลแบบต่างๆ ทราฟฟิคโปรโตรคอลต่างๆ รวมถึงข้อมูลทราฟฟิคเดิมที่เก็บมาจากระบบเครือข่ายเดิม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 3
ระบบโปรแกรมที่พัฒนาและรูปแบบการทดลอง

เมื่อรู้และทราบถึงหลักการทำงานของระบบเครือข่าย และโปรแกรมต่างๆ ที่จะนำมาสร้างเพื่อใช้ทดสอบระบบเครือข่ายไอพีเวอร์ชั่น6 แล้วนั้นในบทนี้จะเป็นขั้นตอนการสร้างโปรแกรมซอคเกต ที่ใช้ในการรับ-ส่งข้อมูลทราฟฟิค การสร้างเอกสารเอกซ์เอ็มแอลที่เป็นไฟล์เรียกใช้งานไฟล์พีแคป การเก็บข้อมูลจากโปรแกรมไวร์ชาร์กเพื่อเป็นข้อมูลทราฟฟิคเสมือนจริง รวมทั้งการสร้างระบบเครือข่ายต่างๆ

3.1 ซีเควนไดอะแกรม (Sequence Diagram)



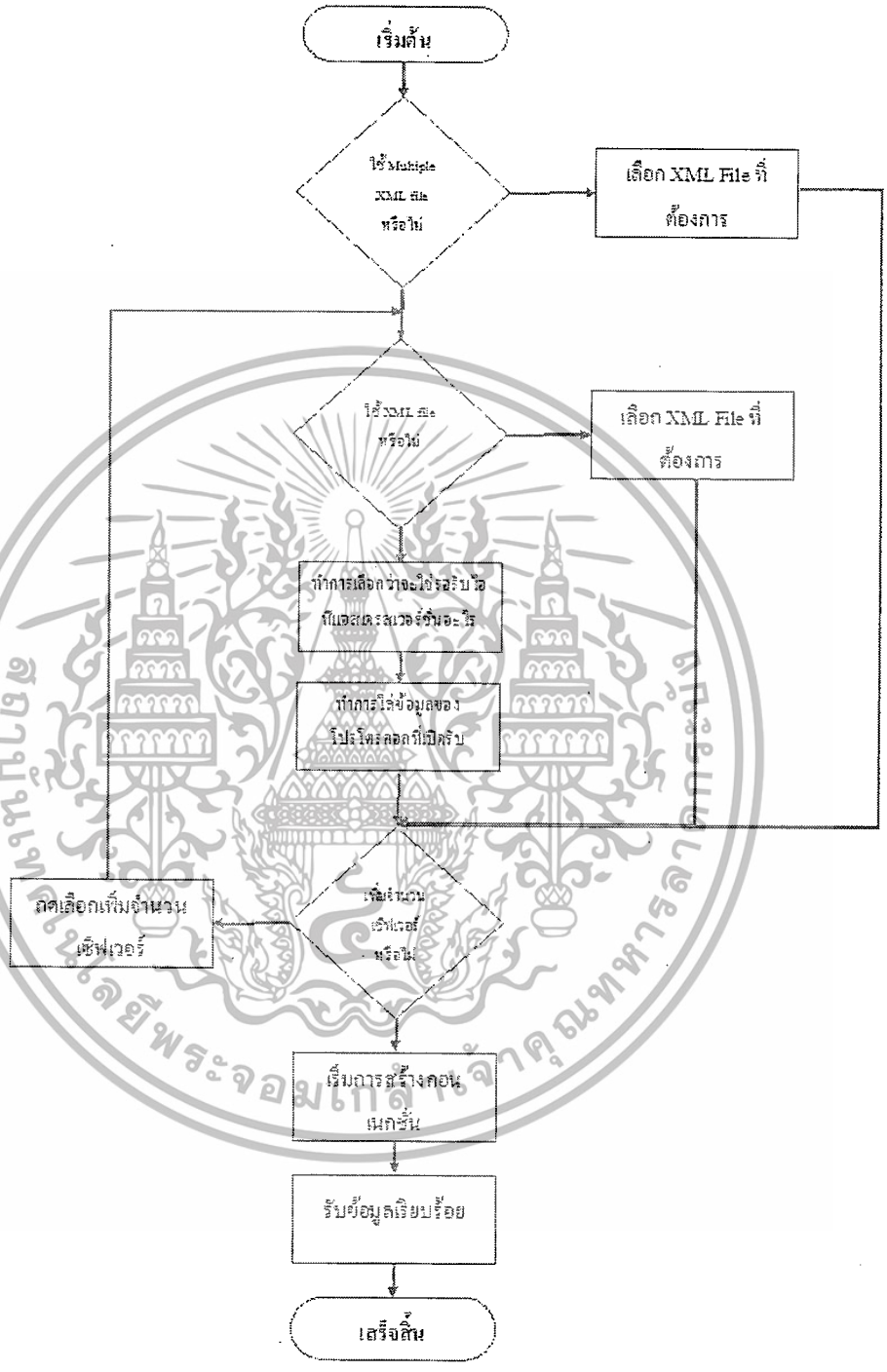
รูปที่ 3.1 รูปแสดงซีเควนไดอะแกรมการทำงานของโปรแกรมจำลองข้อมูลทราฟฟิค

จากรูปที่ 3.1 จะเป็นการอธิบายขั้นตอนการทำงานของโปรแกรมจำลองข้อมูลทราฟฟิคที่พัฒนาขึ้นมา โดยจะแสดงเป็นซีเควนตั้งแต่ยูสเซอร์ A ที่เป็นไคลเอนต์ เริ่มทำการติดต่อสร้างเซสชั่นของโปรแกรมไปยังฝั่งของยูสเซอร์ B ที่เป็นเซิร์ฟเวอร์ ก่อนที่จะสร้างคอนเนกชั่น และรับส่งข้อมูลระหว่างกัน รวมถึงขั้นตอนการทำงานของโปรแกรมจำลองข้อมูลทราฟฟิค ที่มีการเช็คค่าพารามิเตอร์ต่างๆ ว่าถ้าโอเคจะเป้นอย่างไร ถ้าผิดรูปแบบจะเป็นอย่างไร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.2 แอคทิวิตี้ไดอะแกรมของซอคเกตโปรแกรม (Activity Diagram)

3.2.1 ซอคเกตโปรแกรมของฝั่งเซิร์ฟเวอร์(ฝั่งรับ)

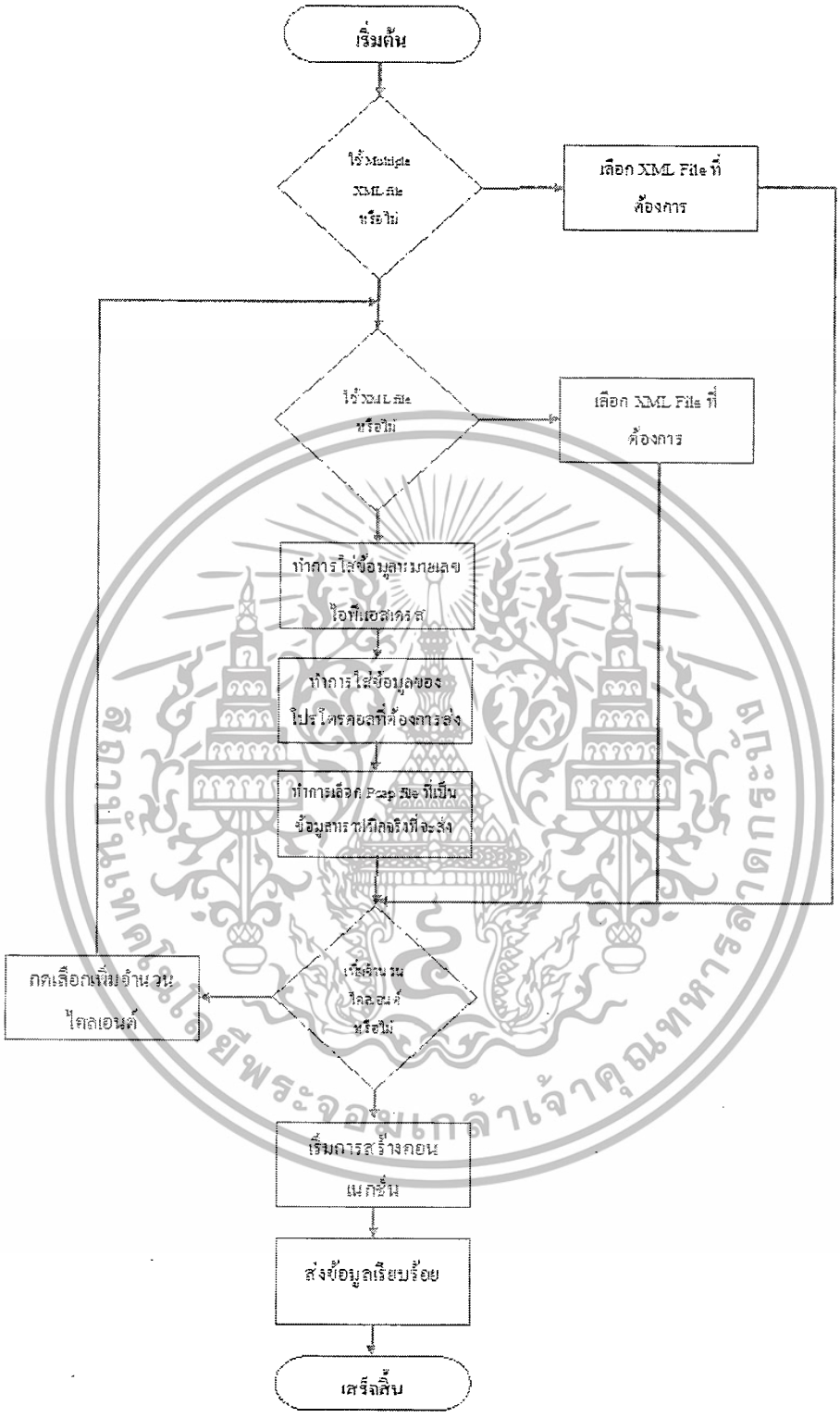


รูปที่ 3.2 รูปแสดงแอคทิวิตี้ไดอะแกรมการทำงานของฝั่งรับ

จากรูปที่ 3.2 จะเป็นการอธิบายขั้นตอนการทำงานของโปรแกรมจำลองข้อมูลทราฟฟิคฝั่งรับ ว่ามีกระบวนการ การทำงานเป็นอย่างไร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.2.2 ซอคเกตโปรแกรมของฝั่งไคลเอนต์(ฝั่งส่ง)



รูปที่ 3.3 รูปแสดงแอคทิวิตี้ไดอะแกรมการทำงานของฝั่งส่ง

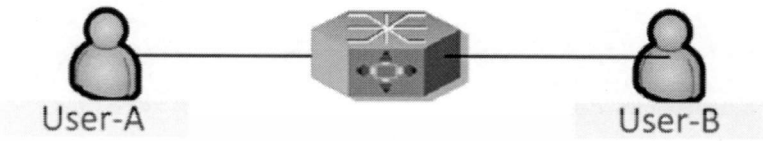
จากรูปที่ 3.3 จะเป็นการอธิบายขั้นตอนการทำงานของโปรแกรมจำลองข้อมูลทราฟฟิคฝั่งส่ง ว่ามีกระบวนการ การทำงานเป็นอย่างไร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3 เนตเวิร์กไดอะแกรม (Network Diagram)

- การใช้งานบนเร้าเตอร์ตัวเดียว (local router)

การทดสอบแบบ ใช้งานบนเร้าเตอร์ตัวเดียวนั้น จะทำการทดสอบโดย เครื่องคอมพิวเตอร์ต้นทาง และปลายทาง ต่อกันอยู่บนอุปกรณ์เนตเวิร์ก ตัวเดียวกัน เพื่อทดสอบว่าสามารถรับ-ส่งข้อมูลทราฟฟิค ผ่านหมายเลขไอพีแอสเดรสเวอร์ชั่น6ได้จริง



รูปที่ 3.4 รูปแสดงแบบการทดสอบที่1

- การใช้งานผ่านระบบแลน (LAN)

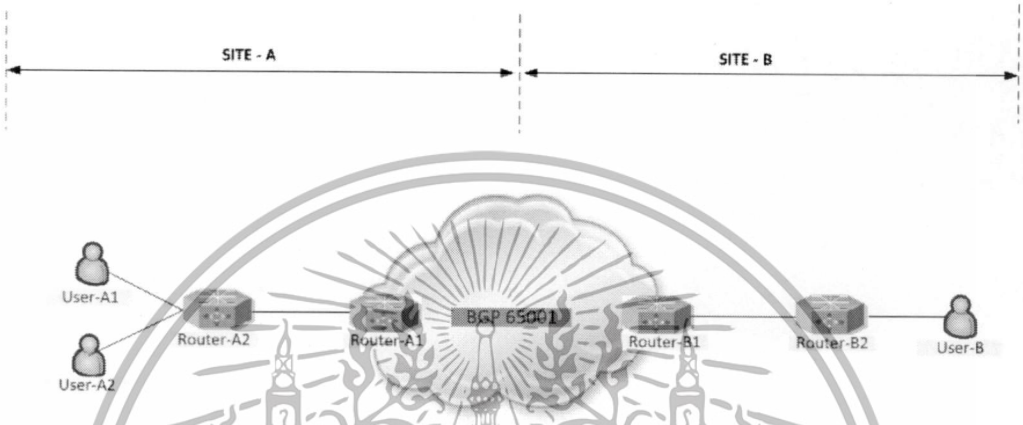
การทดสอบบนระบบเครือข่ายรูปแบบการใช้งานภายในองค์กรนั้น จะทำการสร้างข้อมูลเร้าติ้งระหว่างอุปกรณ์เนตเวิร์ก ซึ่งอาจจะมีทั้งการให้ข้อมูลทราฟฟิคข้ามระบบเครือข่ายไอพีเวอร์ชั่น6 โดยการกำหนดเส้นทางควบคุมด้วยชุดคำสั่ง (Static routing)และ การให้ข้อมูลทราฟฟิคข้ามระบบเครือข่ายไอพีเวอร์ชั่น6 โดยการกำหนดเส้นทางควบคุมด้วยชุดคำสั่งอัตโนมัติ (Dynamic routing) ที่นิยมใช้กันในองค์กรต่างๆ เพื่อทดสอบว่าข้อมูลทราฟฟิคสามารถใช้งานได้จริง

รูปที่ 3.5 รูปแสดงแบบการทดสอบที่2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- การใช้งานผ่านระบบแวน (WAN)

การทดสอบบนระบบเครือข่ายรูปแบบใช้งานระหว่างองค์กรนั้น จะจำลองการเชื่อมต่อระบบเครือข่ายข้ามองค์กร โดยจะใช้โปรโตรคอลในการเชื่อมต่อระหว่างองค์กร ที่เรียกว่า BGP Routing ส่วนภายในองค์กรแต่ละฝั่งจะมีทั้งระบบเครือข่ายไอพีเวอร์ชั่น6 ที่กำหนดเส้นทางควบคุมด้วยชุดคำสั่ง (Static routing)และ ระบบเครือข่ายไอพีเวอร์ชั่น6 ที่กำหนดเส้นทางควบคุมด้วยชุดคำสั่งอัตโนมัติ (Dynamic routing)เพื่อทดสอบว่าข้อมูลทราฟฟิคสามารถใช้งานได้จริง



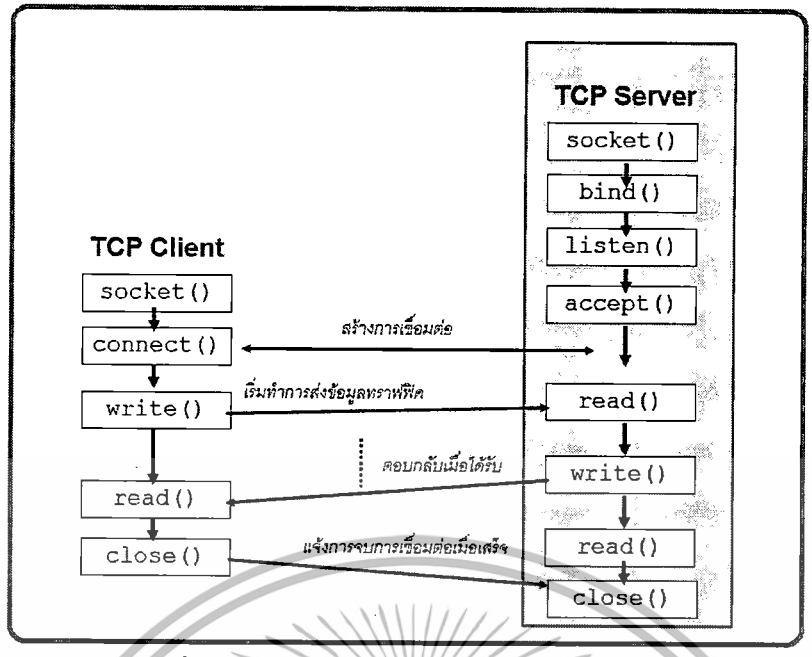
รูปที่ 3.6 รูปแสดงแบบการทดสอบที่3

3.4 การสร้างซอคเกตโปรแกรมโดยใช้ซีชาร์ป

ส่วนนี้จัดว่าเป็นส่วนสำคัญพอๆกับระบบเครือข่ายที่ใช้ในการทดสอบ นั้นก็คือการสร้างโปรแกรมจำลองข้อมูลทราฟฟิคจำลอง ซึ่งก็คือการทำซอคเกตโปรแกรม ที่ใช้ในการรับส่งข้อมูลทราฟฟิคระหว่างเซิร์ฟเวอร์ และ ไคลเอนต์นั่นเอง โดยเราจะแบ่งซอคเกตโปรแกรมออกเป็น 2 รูปแบบคือซอคเกตโปรแกรมฝั่งเซิร์ฟเวอร์ (Server Socket Program) และ ซอคเกตโปรแกรมฝั่งไคลเอนต์ (Client Socket Program)

เมื่อโปรแกรมมีการสร้างการเชื่อมต่อระหว่างเซิร์ฟเวอร์ และไคลเอนต์แล้ว ก็จะเริ่มทำการส่งข้อมูลทราฟฟิคเสมือนจริงผ่านทางซอคเกตนั้นเองด้านล่างจะเป็นรูปที่ 3.7 จะเป็นการอธิบายการทำงานของซอคเกตโปรแกรม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.7 รูปแสดงการสื่อสารกันระหว่างซอคเกตโปรแกรมฝั่งเซิร์ฟเวอร์และไคลเอนต์

เริ่มแรกทั้งซอคเกตโปรแกรมฝั่งไคลเอนต์ และเซิร์ฟเวอร์ จะใช้วินโดวส์ฟอร์ม (Windows Form) โดยฟอร์มนี้เพื่อรับค่าพารามิเตอร์ของทั้งฝั่งเซิร์ฟเวอร์และไคลเอนต์ ตามรูปที่ 3.8 และ 3.9

<u>ซอคเกตโปรแกรมฝั่งเซิร์ฟเวอร์ จะใช้ฟอร์มนี้เพื่อรับค่าพารามิเตอร์ดังนี้</u>

- เวอร์ชั่นไอพีแอสเดรส ว่าจะเป็นไอพีเวอร์ชั่น 4 หรือเวอร์ชั่น 6
- หมายเลขพอร์ทที่เปิดรับบนซอคเกตโปรแกรมฝั่งเซิร์ฟเวอร์
- รูปแบบของอินเทอร์เนตโปรโตรคอลว่าเป็น TCP หรือ UDP

โดยค่าพารามิเตอร์ทั้งหมดนี้ สามารถเรียกใช้ได้จากเอกสารเอกซ์เอ็มแอลที่มีค่าพารามิเตอร์ระบุอยู่ก็ได้

นอกจากนี้ยังมีค่าแสดงผลด้านขวาของวินโวส์ฟอร์มที่แสดงจำนวนข้อมูลทั้งหมดที่รับเป็นไบต์ และเวลาทั้งหมดที่ใช้งาน

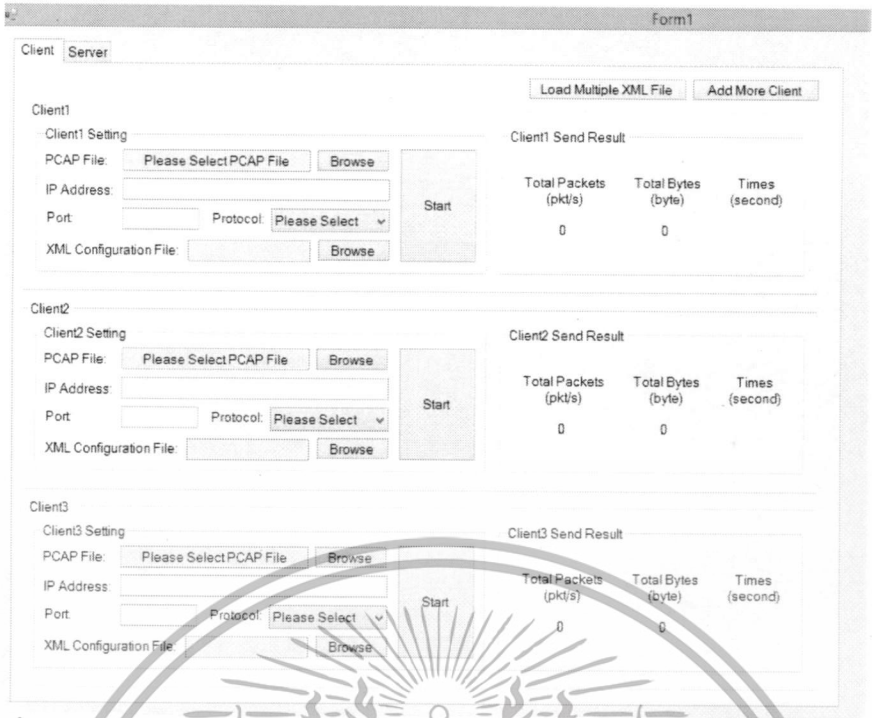
<u>ซอคเกตโปรแกรมฝั่งไคลเอนต์ จะใช้ฟอร์มนี้เพื่อรับค่าพารามิเตอร์ดังนี้</u>

- หมายเลขไอพีแอสเดรสเวอร์ชั่น 4 หรือเวอร์ชั่น 6
- ไฟล์พีแคป ที่เป็นเสมือนข้อมูลจำลองเสมือนจริง ที่ต้องการส่งจากฝั่งไคลเอนต์
- หมายเลขพอร์ทที่เปิดรับบนซอคเกตโปรแกรมฝั่งเซิร์ฟเวอร์
- รูปแบบของอินเทอร์เนตโปรโตรคอลว่าเป็น TCP หรือ UDP

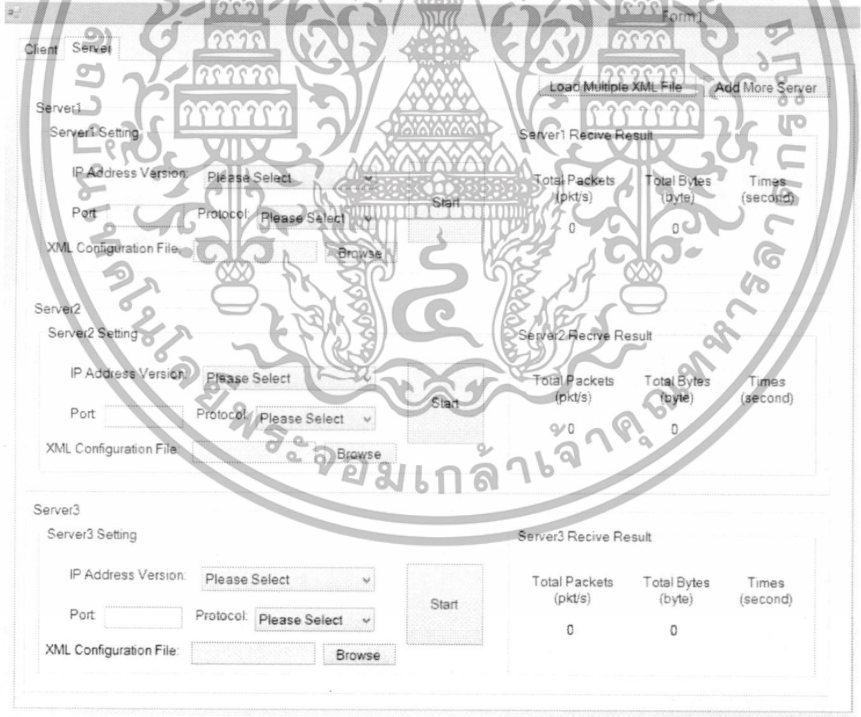
โดยค่าพารามิเตอร์ทั้งหมดนี้ สามารถเรียกใช้ได้จากเอกสารเอกซ์เอ็มแอลที่มีค่าพารามิเตอร์ระบุอยู่ก็ได้

นอกจากนี้ยังมีค่าแสดงผลด้านขวาของวินโวส์ฟอร์มที่แสดงจำนวนข้อมูลทั้งหมดที่ส่งเป็นไบต์ และเวลาทั้งหมดที่ใช้งาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.8 รูปแสดงวินโดวส์ฟอร์มของโปรแกรมจำลองข้อมูลทราฟฟิคฝั่งไคลเอนต์



รูปที่ 3.9 รูปแสดงวินโดวส์ฟอร์มของโปรแกรมจำลองข้อมูลทราฟฟิคฝั่งเซิร์ฟเวอร์

3.4.1 การสร้างโปรแกรมของการรับแพคเก็จจากระบบเครือข่าย

ซอคเกตโปรแกรมฝั่งเซิร์ฟเวอร์ (Server Socket Program) เป็นโปรแกรมที่ทำงานบนเครื่องที่มีซอคเกต ที่ผูกกับพอร์ทบนเครื่องและรอการเรียกเข้า (request) โดยจะถูกส่งมาจากฝั่งไคลเอนต์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ขั้นตอนที่ 1:ของการทำซอคเกตโปรแกรมฝั่งเซิร์ฟเวอร์ (Create Socket)
เริ่มจากการระบุเวอร์ชั่นของไอพีแอสเดรส และโปรโตรคอลพอร์ท ที่ต้องการใช้งาน เพื่อเปิดรอรับการติดต่อ (Listen) แบบ TCP หรือ UDP

```
AddressFamily addVersion;
if(version==4)
   addVersion=AddressFamily.InterNetwork;
else
   addVersion = AddressFamily.InterNetworkV6;
Socket listener = new Socket(addVersion, SocketType.Stream, ProtocolType.Tcp);
if (version == 4)
   listener.Bind(new IPEndPoint(IPAddress.Any, port));
else
   listener.Bind(new IPEndPoint(IPAddress.IPv6Any, port));
```

ขั้นตอนที่ 2: ของการทำซอคเกตโปรแกรมฝั่งเซิร์ฟเวอร์ (Listening)
ถัดมาคือการรอรับการเรียกเข้าจากโปรแกรมฝั่งไคลเอนต์ โดยจะต้องทำการสร้าง infinite loop สำหรับจัดการเรื่องการเรียกเข้าจากโปรแกรมฝั่งไคลเอนต์

ขั้นตอนที่ 3:ของการทำซอคเกตโปรแกรมฝั่งเซิร์ฟเวอร์ (Accept Request)
เมื่อซอคเกตโปรแกรมฝั่งเซิร์ฟเวอร์ ได้รับการเรียกเข้าจากโปรแกรมฝั่งไคลเอนต์ ก็จะเริ่มอ่านข้อมูลทราฟฟิคที่ถูกส่งมาจากฝั่งไคลเอนต์

```
listener.Listen(0);
Console.WriteLine("Waiting for incoming connections on " + port);
serverSocket[index] = listener.Accept();
listener.Close();
byte[] b = new byte[65536];
int len;
while ((len = serverSocket[index].Receive(b)) != 0)
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ขั้นตอนที่ 4:ของการทำซอคเกตโปรแกรมฝั่งเซิร์ฟเวอร์ (Get Request)
เมื่อมีการส่งข้อมูลเข้ามาจากไคลเอนต์ ให้ทำการวนลูป รับข้อมูล (หน่วยเป็นไบต์) พร้อมทั้งประมวลผล

```
System.Console.WriteLine("RX: " + System.Text.ASCIIEncoding.ASCII.GetString(b, 0, len));
b = new byte[65536];
```

ขั้นตอนที่ 5 : ของการทำซอคเกตโปรแกรมฝั่งเซิร์ฟเวอร์ (Reply)
ถัดมาเป็นขั้นตอนการตอบกลับของทางฝั่งเซิร์ฟเวอร์ เมื่อได้รับข้อมูลจากทางไคลเอนต์ก็จะทำการตอบกลับไปว่าได้รับแล้ว พร้อมทั้งแสดงค่าผลลัพธ์ด้านซ้ายของวินโดวส์ฟอร์ม

```
Invoke(new MethodInvoker(delegate { serverPackets[index].Text = "" +
(int.Parse(serverPackets[index].Text) + 1); }));
Invoke(new MethodInvoker(delegate { serverBytes[index].Text = "" +
(int.Parse(serverBytes[index].Text) + len); }));
Invoke(new MethodInvoker(delegate { serverButtons[index].Text = "start"; }));
Invoke(new MethodInvoker(delegate { isServerRun[index] = false; }));
Invoke(new MethodInvoker(delegate { serverTimes[index].Text = string.Format("{0:0.00}",
(DateTime.Now - serverStartTime[index]).TotalSeconds); }));
```

3.4.2 การสร้างโปรแกรมของการส่งแพคเก็จจากระบบเครือข่าย

ซอคเกตโปรแกรมฝั่งไคลเอนต์ (Client Socket Program) จะต้องรู้ว่าหมายเลขไอพีแอสเดรส ของเครื่องที่มีซอคเกตโปรแกรมฝั่งเซิฟร์เวอร์ทำงานอยู่ และพอร์ทที่เครื่องนั้นรอการเรียกเข้า (request) ด้วย
ขั้นตอนที่ 1 :ของการทำซอคเกตโปรแกรมฝั่งไคลเอนต์ (Create Socket)
ขั้นตอนแรกของการทำซอคเกตโปรแกรมฝั่งไคลเอนต์คือการสร้างซอคเกต เพื่อใช้สำหรับติดต่อไปยังโปรแกรมฝั่งเซิร์ฟเวอร์ คือระบุค่าพารามิเตอร์ของหมายเลขไอพีแอสเดรสและโปรโตรคอลพอร์ทที่ต้องการส่งไป

```
IPAddress ipa = IPAddress.Parse(ip);
IPEndPoint ipeh = new IPEndPoint(ipa, port);
AddressFamily addVersion;
if (version == 4)
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
        addVersion = AddressFamily.InterNetwork;
    else
        addVersion = AddressFamily.InterNetworkV6;
    if (type == "TCP")
        clientSocket[index] = new Socket(addVersion, SocketType.Stream, ProtocolType.Tcp);
    else
        clientSocket[index] = new Socket(addVersion, SocketType.Dgram, ProtocolType.Udp);
    clientSocket[index].Connect(ipeh);
```

โดยเมื่อมีใส่ค่าหมายเลขไอพีแอสเดรสที่อาจจะเป็นไอพีเวอร์ชั่น4 หรือเวอร์ชั่น6 ของที่อยู่ซอคเกตโรปแกรมฝั่งเซิร์ฟเวอร์ลงไป โปรแกรมจะทำการเช็คว่าเป็นหมายเลขไอพีแอสเดรสเวอร์ชั่นอะไร

```
private int checkIPversion(string input)
{
    if (input.Contains(".") || input.Contains(":"))
    {
        IPAddress address;
        if (IPAddress.TryParse(input, out address))
        {
            switch (address.AddressFamily)
            {
                case AddressFamily.InterNetwork:
                    return 4;
                case AddressFamily.InterNetworkV6:
                    return 6;
                default:
                    return 0;
```

<u>ขั้นตอนที่ 2 :</u> ของการทำซอคเกตโปรแกรมฝั่งไคลเอนต์ (Request)

ขั้นตอนแรกของการทำซอคเกตโปรแกรมฝั่งไคลเอนต์คือส่งการเรียก (Request)ไปยังโปรแกรมฝั่งเซิร์ฟเวอร์ โดยจะทำการแปลงข้อมูลที่ต้องการส่งให้เป็นไบต์ (Byte) และทำการส่งผ่านซอคเกตโปรแกรมที่สร้างขึ้น

```
byte[] b = System.Text.ASCIIEncoding.ASCII.GetBytes(filename);
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โดยในส่วนนี้ข้อมูลทราฟฟิคจะเรียกจากพีแคปไฟล์ โดยใช้คำสั่งด้านล่าง

```
PcapFile dump = new PcapFile(filename);
byte[] data = System.Text.ASCIIEncoding.ASCII.GetBytes(filename);
```

จากนั้นก็ต้องมีคำสั่งที่ใช้ส่งการเรียก (request) ไปยังซอคเกตโปรแกรมฝั่งเซิร์ฟเวอร์

```
clientSocket[index].Send(data);
Console.WriteLine("{0}.{1}: Packet is {2} bytes", packet.Seconds, packet.Microseconds, data.Length);
```

ขั้นตอนที่ 3 : ของการทำซอคเกตโปรแกรมฝั่งไคลเอนต์ (แสดงผล)

สุดท้ายเมื่อทำการส่งข้อมูลทราฟฟิคไปฝั่งเซิร์ฟเวอร์ครบตามขนาดไฟล์พีแคปที่ต้องการแล้ว ก็จะแสดงผลค่าผ่านวินโดวส์ฟอร์มออกมา

```
dump.Close();
Invoke(new MethodInvoker(delegate { clientButtons[index].Text = "Start"; }));
Invoke(new MethodInvoker(delegate { isClientRun[index] = false; }));
Invoke(new MethodInvoker(delegate { clientTimes[index].Text = string.Format("{0:0.00}", (DateTime.Now - clientStartTime[index]).TotalSeconds); }));
clientThread[index].Abort();
```

3.5 การสร้างเอกสารเอกซ์เอ็มแอล

รูปแบบของเอกสารเอกซ์เอ็มแอล จะมีการทำขึ้นมาสำหรับเป็นส่วนช่วยของโปรแกรม โดยสามารถแบ่งออกได้เป็น 2 ส่วนใหญ่ๆ คือ ส่วนของเอกสารที่ใช้ในการเรียกเอกสารเอกซ์เอ็มแอลหลายๆอัน กับอีกส่วนคือ ส่วนที่เป็นเอกสารเอกซ์เอ็มแอลที่ใช้ระบุค่าพารามิเตอร์ต่างๆ เพื่อใช้ระบุลงในโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง

โครงสร้างของเอกสารเอกซ์เอ็มแอลที่ใช้เรียกไปยังเอกสารอื่นๆ

```
<Root>
        <XMLFile>C:\Users\TheRouter\Desktop\test1.xml</XMLFile>
        <XMLFile> C:\Users\TheRouter\Desktop\test2.xml</XMLFile>
        <XMLFile> C:\Users\TheRouter\Desktop\test3.xml</XMLFile>
</Root>
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โครงสร้างเอกสารส่วนนี้จะเป็นส่วนที่ใช้สำหรับที่ต้องการจำลองสร้างเซิร์ฟเวอร์ หรือไคลเอนต์หลาย ๆ ตัว และไม่ต้องการที่จะระบุค่าที่ละค่าบนตัวโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง ก็สามารถที่จะสร้างเป็นเอกสารเอซ์เอ็มแอลที่ระบุค่าพารามิเตอร์ต่างๆไว้ได้ก่อน จากนั้นก็ใช้โครงสร้างเอกสารนี้ในการเรียกเอกสารเอกซ์เอ็มแอลต่างๆ ขึ้นมาใช้งาน

โครงสร้างของเอกสารเอกซ์เอ็มแอลที่ใช้ระบุค่าพารามิเตอร์ต่างๆ ฝั่งเซิร์ฟเวอร์

```
<Root>
    <data>
        <IPVersion>6 </IPVersion>
        <Port>1234</Port>
        <Protocol>TCP</Protocol>
    </data>
</Root>
```

โครงสร้างเอกสารส่วนนี้จะเป็นส่วนที่ใช้สำหรับที่ระบุค่าพารามิเตอร์ของฝั่งเซิร์ฟเวอร์ เพื่อที่จะเรียกใช้เช่นค่าหมายเลขไอพีแอสเดรส, ค่าของโปรโตรคอลพอร์ท งานผ่านหน้าต่างโปรแกรม

โครงสร้างของเอกสารเอกซ์เอ็มแอลที่ใช้ระบุค่าพารามิเตอร์ต่างๆ ฝั่งไคล์เอนต์

```
<Root>
    <data>
        <PcapFile> C:\Users\TheRouter\Desktop\test1.pcap </PcapFile>
        <IP>2001:1234:DDDD:CCCC::2</IP>
        <Port> 1234</Port>
        <Protocol>TCP</Protocol>
    </data>
</Root>
```

โครงสร้างเอกสารส่วนนี้จะเป็นส่วนที่ใช้สำหรับที่ระบุค่าพารามิเตอร์ของฝั่งไคล์เอนต์ต่างๆ เช่นค่าหมายเลขไอพีแอสเดรส, ค่าของโปรโตรคอลพอร์ท, ค่าพารามิเตอร์ที่จะไปเรียกใช้พีแคปไฟล์ที่ต้องการ โดยจะเรียกใช้งานเอกสารเอกซ์เอ็มแอลนี้ผ่านหน้าต่างโปรแกรม โดยที่ไม่ต้องไประบุค่าที่ละค่านั่นเอง

จากโครงสร้างเอกสร้างเอกสารตามตัวอย่างด้านบนนั้นจะเห็นว่า เอกสารเอกซ์เอ็มแอลที่สร้างขึ้นนั้นเปรียบเสมือนพอยท์เตอร์ที่จะเป็นตัวชี้ไปยังไฟล์พีแคป ที่จะเป็นไฟล์ที่เก็บข้อมูลทราฟฟิคที่ดักจับจากระบบเดิม หลังจากนั้นขั้นตอนคือ จะใส่ค่าในเอกซ์เอ็มแอลไฟล์ หรือระบุค่าเองลงบน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ แสวงหาผลประโยชน์ทางการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง เพื่อที่จะระบุค่าหมายเลขไอพีแอสเดรส ค่าโปรโตรคอลพอร์ท นั่นเอง

3.6 การติดตั้งระบบเครือข่าย ในการทดลอง

ส่วนนี้จะแสดงขั้นตอนสำคัญคือเรื่องการติดตั้งระบบเครือข่าย โดยจะเป็นรูปแบบการคอนฟิกระบบเครือข่ายไอพีเอวร์ชั่น 6 บนอุปกรณ์ที่เป็นยี่ห้อซิสโก้ (CISCO) ตามอุปกรณ์ที่ทำมาใช้ในการทดลอง และจะอธิบายเป็นที่ละขั้นไปแบ่งตามระบบเครือข่ายที่ทดสอบในการทดลอง

3.6.1 ระบบเครือข่าย บนเร้าเตอร์ตัวเดียว

ส่วนนี้มาถึงขั้นตอนการคอนฟิก เพื่อตั้งค่าของเร้าเตอร์ที่นำมาใช้กับการจำลองนี้ ซึ่งจะอธิบายเป็นที่ละขั้นไป

1. เริ่มด้วยการเปิดฟีเจอร์ ไอพีเวอร์ชั่น6 บนเร้าเตอร์ (enable ipv6 feature) ซึ่งในการทำไอพีเวอร์ชั่น6 บนเร้าเตอร์ คำสั่งนี้จะเป็นคำสั่งแรก ที่ต้องคอนฟิก โดยการพิมพ์คำสั่งด้านล่าง

```
Router(config)# ipv6 unicast-routing
```

2. เลือกอินเทอร์เฟส ที่ต่อกับอุปกรณ์ไอพีเวอร์ชั่น6 หรือ ที่ต้องกันในระบบเครือข่าย และมีความต้องการที่ต้องคอนฟิกเป็นไอพีเวอร์ชั่น6 โดยการพิมพ์คำสั่งด้านล่าง

- รูปแบบคำสั่ง

```
Router(config)# interface [type fastethernet/gigabitethernet/tengigethernet] [slot/port]
```

- ตัวอย่างอินเทอร์เฟสฟาสอีเทอร์เนต พอร์ตที่0/0 ต้องใช้งานไอพีเวอร์ชั่น6

```
Router(config)# interface fastethernet0/0
```

3.ใส่ค่าหมายเลขไอพีแอสเดรสเวอร์ชั่น6 ให้กับอินเทอร์เฟส โดยการพิมพ์คำสั่งด้านล่าง

- รูปแบบคำสั่ง

```
Router(config-if)# ipv6 address ipv6_address_prefix/prefix_length [eui-64]
```

- ตัวอย่างต้องกำหนดหมายเลขไอพีเวอร์ชั่น6 2001:1cc1:dddd::2/64 ลงบนอินเทอร์เฟสนี้

```
Router(config-if)# ipv6 address 2001:1cc1:dddd::2/64
```

3.6.2 ระบบเครือข่าย แบบการใช้งานภายในองค์กร

ส่วนนี้มาถึงขั้นตอนการคอนฟิก เพื่อตั้งค่าของเร้าเตอร์ที่นำมาใช้กับการจำลองรูปแบบการใช้งานภายในองค์กร ซึ่งจะอธิบายเป็นที่ละขั้นไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1. เริ่มด้วยการเปิดฟีเจอร์ ไอพีเวอร์ชั่น6 บนเร้าเตอร์ (enable ipv6 feature) ซึ่งในการทำไอพีเวอร์ชั่น6 บนเร้าเตอร์ คำสั่งนี้จะเป็นคำสั่งแรก ที่ต้องคอนฟิก โดยการพิมพ์คำสั่งด้านล่าง

Router(config)# ipv6 unicast-routing

2. เลือกอินเทอร์เฟส ที่ต่อกับอุปกรณ์ไอพีเวอร์ชั่น6 หรือ ที่ต้องกันในระบบเครือข่าย และมีความต้องการที่ต้องคอนฟิกเป็นไอพีเวอร์ชั่น6 โดยการพิมพ์คำสั่งด้านล่าง

- รูปแบบคำสั่ง

Router(config)# interface [type fastethernet/gigabitethernet/tengigethernet] [slot/port]

- ตัวอย่างอินเทอร์เฟสฟาสอีเทอร์เนต พอร์ตที่0/0 ต้องใช้งานไอพีเวอร์ชั่น6

Router(config)# interface fastethernet0/0

3.ใส่ค่าหมายเลขไอพีแอสเดรสเวอร์ชั่น6 ให้กับอินเทอร์เฟส โดยการพิมพ์คำสั่งด้านล่าง

- รูปแบบคำสั่ง

Router(config-if)# ipv6 address ipv6_address_prefix/prefix_length [eui-64]

- ตัวอย่างต้องกำหนดหมายเลขไอพีเวอร์ชั่น6 2001:1cc1:dddd::2/64 ลงบนอินเทอร์เฟสนี้

Router(config-if)# ipv6 address 2001:1cc1:dddd::2/64

4.ขั้นตอนถัดมาจะเป็นการสร้างรูปแบบไดนามิคเร้าท์ติ้งโดยใช้โปรโตรคอลโอเอสพีเอฟ (OSPF Routing Protocol) ที่ใช้สำหรับ ระบบเครือข่ายไอพีเอวร์ชั่น 6 ซึ่งจะมีขั้นตอนต่าง ๆ ตามด้านล่าง

- รูปแบบคำสั่งในการสร้างโอเอสพีเอฟเร้าท์ติ้งสำหรับระบบเครือข่ายไอพีเวอร์ชั่น 6

Router(config)# ipv6 router ospf [Process id]

Router(config-if)# router-id [ipv4 address]

- รูปแบบคำสั่งในการระบุอินเทอร์เฟสที่ต้องการให้ใช้งานโอเอสพีเอฟเร้าท์ติ้งสำหรับระบบเครือข่ายไอพีเวอร์ชั่น 6

Router(config-if)# interface fastethernet0/0

Router(config-if)# ipv6 router ospf area [area-id]

5.ขั้นตอนถัดมาจะเป็นการสร้างรูปแบบไดนามิคเร้าท์ติ้งโดยใช้โปรโตรคอลโอเอสพีเอฟ (OSPF Routing Protocol) ที่ใช้สำหรับ ระบบเครือข่ายไอพีเอวร์ชั่น 6 ซึ่งจะมีขั้นตอนต่าง ๆ ตามด้านล่าง

- รูปแบบคำสั่งในการสร้างโอเอสพีเอฟเร้าท์ติ้งสำหรับระบบเครือข่ายไอพีเวอร์ชั่น 6

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Router(config)# ipv6 router ospf [Process id]

Router(config-if)# router-id [ipv4 address]

- รูปแบบคำสั่งในการระบุอินเทอร์เฟสที่ต้องการให้ใช้งานโอเอสพีเอฟเร้าท์ติ้งสำหรับระบบเครือข่ายไอพีเวอร์ชั่น 6

Router(config-if)# interface fastethernet0/0

Router(config-if)# ipv6 router ospf area [area-id]

- รูปแบบคำสั่งที่ใช้ในการตรวจสอบความถูกต้องของโอเอสพีเอฟเร้าท์ติ้งสำหรับระบบเครือข่ายไอพีเวอร์ชั่น 6

Router# show ipv6 ospf neighbor

Router# show ipv6 ospf database

Router# show ipv6 ospf

Router# show ipv6 route ospf

3.6.3 ระบบเครือข่าย แบบการใช้งานระหว่างองค์กร

ส่วนนี้มาถึงขั้นตอนการคอนฟิก เพื่อตั้งค่าของเร้าเตอร์ที่นำมาใช้กับการจำลองรูปแบบการใช้งานระหว่างองค์กร ซึ่งจะอธิบายเป็นที่ละขั้นไป

1. เริ่มด้วยการเปิดฟีเจอร์ ไอพีเวอร์ชั่น6 บนเร้าเตอร์ (enable ipv6 feature) ซึ่งในการทำไอพีเวอร์ชั่น6 บนเร้าเตอร์ คำสั่งนี้จะเป็นคำสั่งแรก ที่ต้องคอนฟิก โดยการพิมพ์คำสั่งด้านล่าง

Router(config)# ipv6 unicast-routing

2. เลือกอินเทอร์เฟส ที่ต่อกับอุปกรณ์ไอพีเวอร์ชั่น6 หรือ ที่ต้องกันในระบบเครือข่าย และมีความต้องการที่ต้องคอนฟิกเป็นไอพีเวอร์ชั่น6 โดยการพิมพ์คำสั่งด้านล่าง

- รูปแบบคำสั่ง

Router(config)# interface [type fastethernet/gigabitethernet/tengigethernet] [slot/port]

- ตัวอย่างอินเทอร์เฟสฟาสอีเทอร์เนต พอร์ตที่0/0 ต้องใช้งานไอพีเวอร์ชั่น6

Router(config)# interface fastethernet0/0

3.ใส่ค่าหมายเลขไอพีแอสเดรสเวอร์ชั่น6 ให้กับอินเทอร์เฟส โดยการพิมพ์คำสั่งด้านล่าง

- รูปแบบคำสั่ง

Router(config-if)# ipv6 address ipv6_address_prefix/prefix_length [eui-64]

- ตัวอย่างต้องกำหนดหมายเลขไอพีเวอร์ชั่น6 2001:1cc1:dddd::2/64 ลงบนอินเทอร์เฟสนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Router(config-if)# ipv6 address 2001:1cc1:dddd::2/64

4.ขั้นตอนถัดมาจะเป็นการสร้างรูปแบบไดนามิคเร้าท์ติ้งโดยใช้โปรโตรคอลโอเอสพีเอฟ (OSPF Routing Protocol) ที่ใช้สำหรับ ระบบเครือข่ายไอพีเอวร์ชั่น 6 ซึ่งจะมีขั้นตอนต่าง ๆ ตามด้านล่าง

- รูปแบบคำสั่งในการสร้างโอเอสพีเอฟเร้าท์ติ้งสำหรับระบบเครือข่ายไอพีเวอร์ชั่น 6

Router(config)# ipv6 router ospf [Process id]

Router(config-if)# router-id [ipv4 address]

- รูปแบบคำสั่งในการระบุอินเทอร์เฟสที่ต้องการให้ใช้งานโอเอสพีเอฟเร้าท์ติ้งสำหรับระบบเครือข่ายไอพีเวอร์ชั่น 6

Router(config-if)# interface fastethernet0/0

Router(config-if)# ipv6 router ospf area [area-id]

5.ขั้นตอนถัดมาจะเป็นการสร้างรูปแบบการกำหนดเร้าท์ติ้งโดยใช้สแตติกเร้าท์ติ้ง (Static Routing) ที่ใช้สำหรับ ระบบเครือข่ายไอพีเวอร์ชั่น 6 ซึ่งจะมีขั้นตอนต่าง ๆ ตามด้านล่าง

- รูปแบบคำสั่งในการสร้างสแตติกเร้าท์ติ้ง (Static Routing) สำหรับเครือข่ายไอพีเวอร์ชั่น 6

Router(config)# ipv6 route [Destination prefix] [interface gateway] [ipv6 address nexthop]

- รูปแบบคำสั่งที่ใช้ในการตรวจสอบความถูกต้องของสแตติกเร้าท์ติ้ง (Static Routing) สำหรับระบบเครือข่ายไอพีเวอร์ชั่น 6

Router# show ipv6 route static

6.ขั้นตอนถัดมาจะเป็นการสร้างรูปแบบไดนามิคเร้าท์ติ้งโดยใช้โปรโตรคอลโอเอสพีเอฟ (OSPF Routing Protocol) ที่ใช้สำหรับ ระบบเครือข่ายไอพีเอวร์ชั่น 6 ซึ่งจะมีขั้นตอนต่าง ๆ ตามด้านล่าง

- รูปแบบคำสั่งในการสร้างโอเอสพีเอฟเร้าท์ติ้งสำหรับระบบเครือข่ายไอพีเวอร์ชั่น 6

Router(config)# ipv6 router ospf [Process id]

Router(config-route)# router-id [ipv4 address]

- รูปแบบคำสั่งในการระบุอินเทอร์เฟสที่ต้องการให้ใช้งานโอเอสพีเอฟเร้าท์ติ้งสำหรับระบบเครือข่ายไอพีเวอร์ชั่น 6

Router(config-if)# interface fastethernet0/0

Router(config-if)# ipv6 router ospf area [area-id]

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- รูปแบบคำสั่งที่ใช้ในการตรวจสอบความถูกต้องของโอเอสพีเอฟเร้าท์ติ้งสำหรับระบบเครือข่ายไอพีเวอร์ชั่น 6

Router# show ipv6 ospf neighbor

Router# show ipv6 ospf database

Router# show ipv6 ospf

Router# show ipv6 route ospf

7.ขั้นตอนถัดมาจะเป็นการสร้างรูปแบบไดนามิคเร้าท์ติ้งโดยใช้โปรโตรคอลบีจีพี (BGP Routing) ที่ใช้สำหรับ ระบบเครือข่ายไอพีเอวร์ชั่น 6 ซึ่งจะมีขั้นตอนต่าง ๆ ตามด้านล่าง

- รูปแบบคำสั่งในการสร้างบีจีพีเอฟเร้าท์ติ้งสำหรับระบบเครือข่ายไอพีเวอร์ชั่น 6

router BGP [AS number]

BGP router-id [ipv4 address]

neighbor [ipv6 address peering] remote-as [remote AS number]

!

address-family ipv6

redistribute [static|connected|ospf|rip|eigrp]

neighbor [ipv6 address peering] activate

neighbor [ipv6 address peering] soft-reconfiguration inbound

exit-address-family

!

!

- รูปแบบคำสั่งที่ใช้ในการตรวจสอบความถูกต้องของบีจีพีเร้าท์ติ้งสำหรับระบบเครือข่ายไอพีเวอร์ชั่น 6

Router# show bgp ipv6 unicast summay

Router# show bgp ipv6 unicast

Router# show ipv6 route bgp

3.7 การทำงานของไวร์ชาร์ก

ขั้นตอนการติดตั้งโปรแกรมดักจับแพคเก็ตไวร์ชาร์ก โดยทั่วไปแล้วโปรแกรมนี้มีทั้งเวอร์ชั่นที่สามารถติดตั้งบน ระบบปฏิบัติการวินโดว์ และระบบปฏิบัติการลีนุกซ์ แต่ที่ใช้ในการทดสอบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

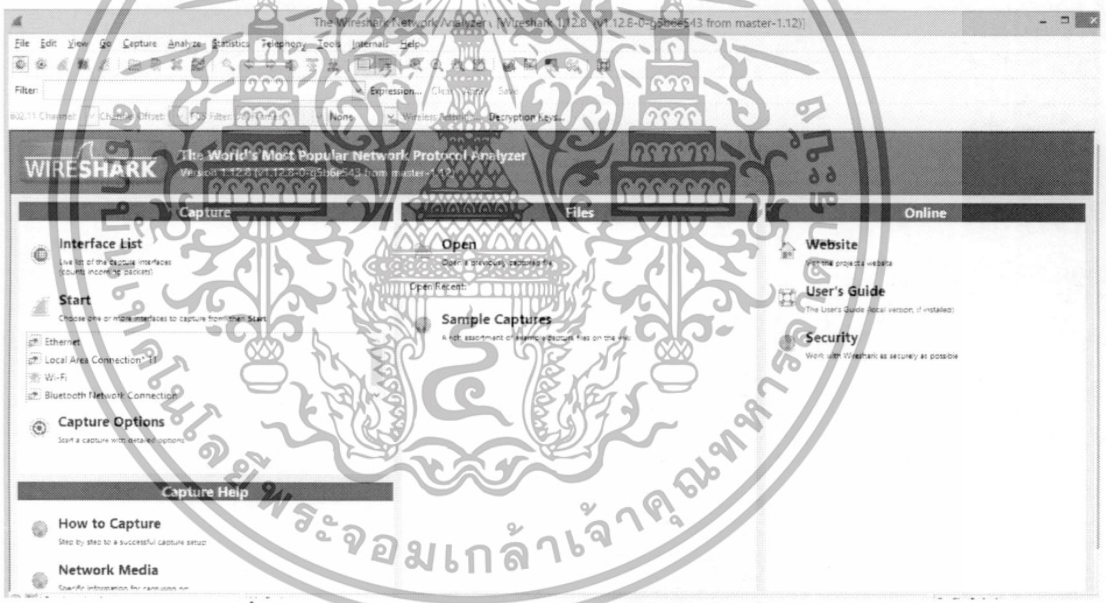
นี้จะเป็นเวอร์ชั่นบนระบบปฏิบัติการวินโดว์ เนื่องจากการจะต้องใช้คอมพิวเตอร์เป็นตัวมอนิเตอร์และคอมพิวเตอร์ที่ใช้ในการทดสอบนี้ ติดตั้งระบบปฏิบัติการวินโดว์

ขั้นตอนการติดตั้ง

1. สามารถ ดาวน์โหลดโปรแกรมไวร์ชาร์ก ได้ที่ http://www.wireshark.org/download.html
2. หน้าเวบไซต์จะแสดงเวอร์ชั่นใหม่ล่าสุด ซึ่งสามารถเลือกลงตามระบบปฏิบัติการที่ต้องการได้
3. การลงโปรแกรมไวร์ชาร์กนั้น ระหว่างการลงจะมีการถามว่าต้องลงโปรแกรม WinPcap ด้วยหรือไม่ ซึ่งโปรแกรม WinPcap นี้จะช่วยในการดักจับแพคเก็ตนั่นเอง
4. ติดตั้งทุกอย่างให้เรียบร้อย

ขั้นตอนการใช้งานโปรแกรมไวร์ชาร์ก

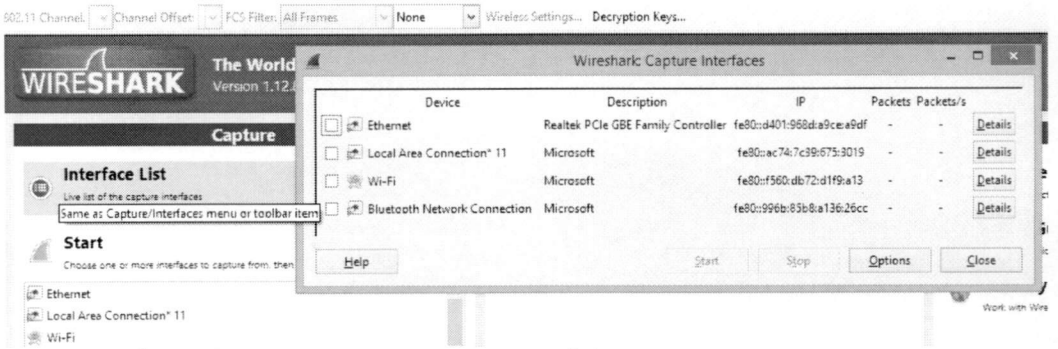
1. ดับเบิ้ลคลิ๊กเพื่อเปิดโปรแกรมไวร์ชาร์ก จากโปรแกรมทูลบาร์ รูปด้านล่างคือหน้าตาของโปรแกรมไวร์ชาร์ก



รูปที่ 3.10 รูปแสดงการใช้โปรแกรมไวร์ชาร์ก

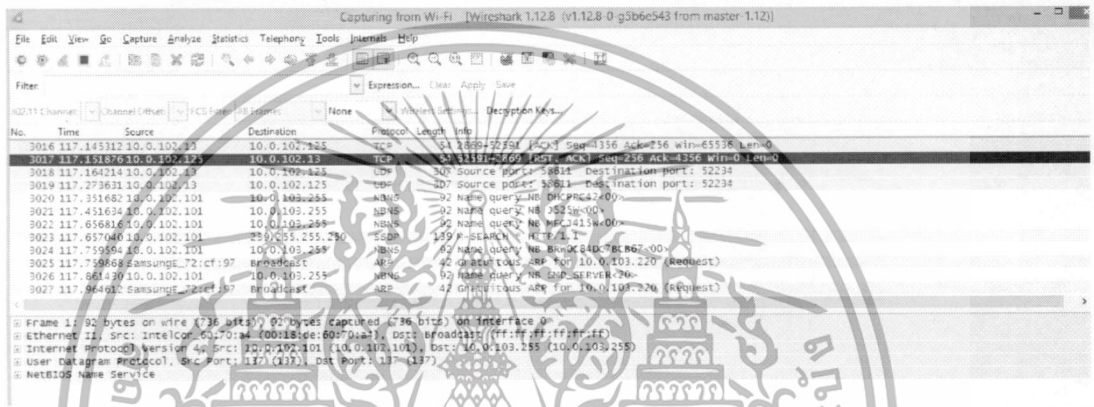
2. เลือกอินเทอรเฟสของคอมพิวเตอร์ ที่ต้องการจะดักจับแพคเก็ต โดยเลือกที่ เมนูบาร์ capture จากนั้น เลือก interface

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



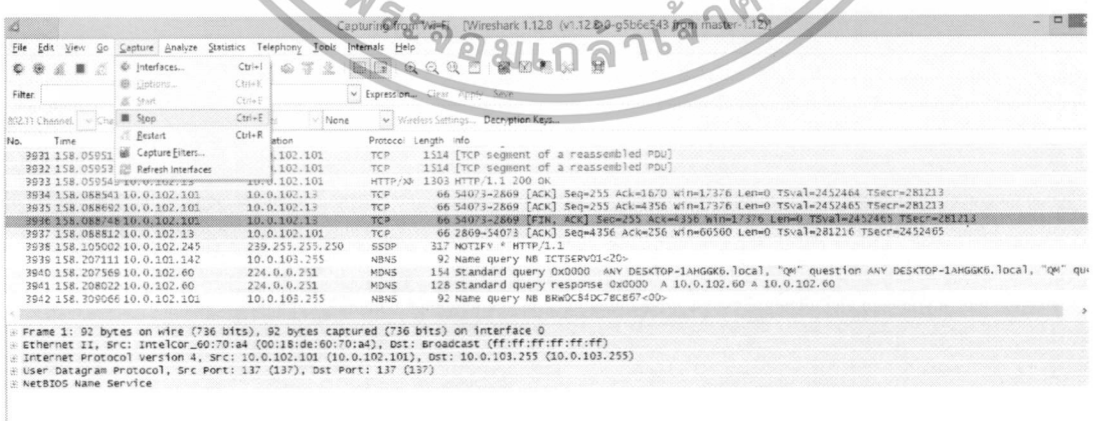
รูปที่ 3.11 รูปแสดงการเลือกอินเทอร์เฟสที่ต้องการดักจับแพคเก็ต

3. หลังจากที่เลือกแล้วให้ กดสตาร์ท เพื่อเริ่มต้นการดักจับแพคเก็ต



รูปที่ 3.12 รูปแสดงแพคเก็ตที่ถูกดักจับได้

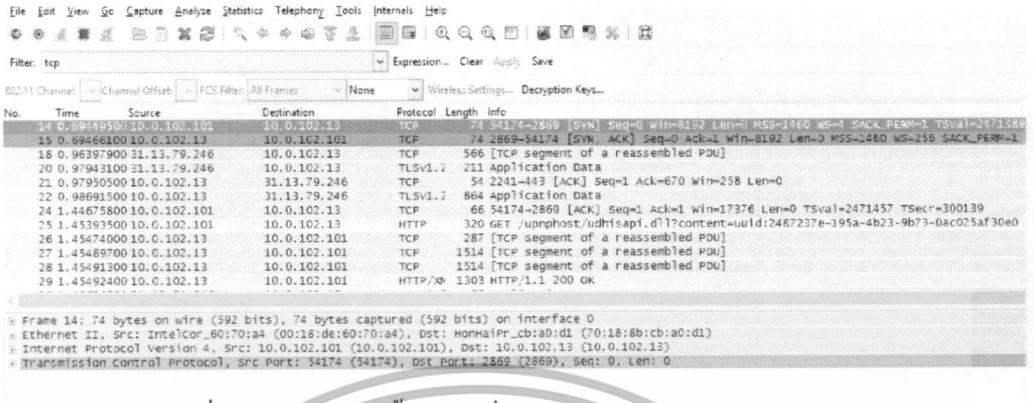
4. เมื่อเริ่มต้นดักจับแพคเก็ตแล้ว สามารถดูข้อมูลได้แบบเรียลไทม์ ตามรูปตัวอย่างด้านล่าง
5. เมื่อต้องการหยุด ให้กด ctrl+e หรือ ไปที่เมนูบาร์ capture จากนั้นเลือก stop โปรแกรมก็จะหยุดการดักจับข้อมูลแพคเก็ต



รูปที่ 3.13 รูปแสดงขั้นตอนเมื่อหยุดจับแพคเก็ต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6. จากนั้นสามารถที่จะฟิลเตอร์ (filter) ข้อมูลเฉพาะที่ต้องการได้ สมมติต้องการเฉพาะโปรโตรคอลทีซีพี (TCP) ก็พิมพ์ลงไปบน แทบฟิลเตอร์ จากนั้นกด แอฟไฟน์ (apply) จะได้เฉพาะข้อมูลแพคเก็ตที่เกี่ยวกับโปรโตรคอลทีซีพี่ ตามต้องการ



รูปที่ 3.14 รูปแสดงขั้นตอนเมื่อฟิลเตอร์แพคเก็ต TCP

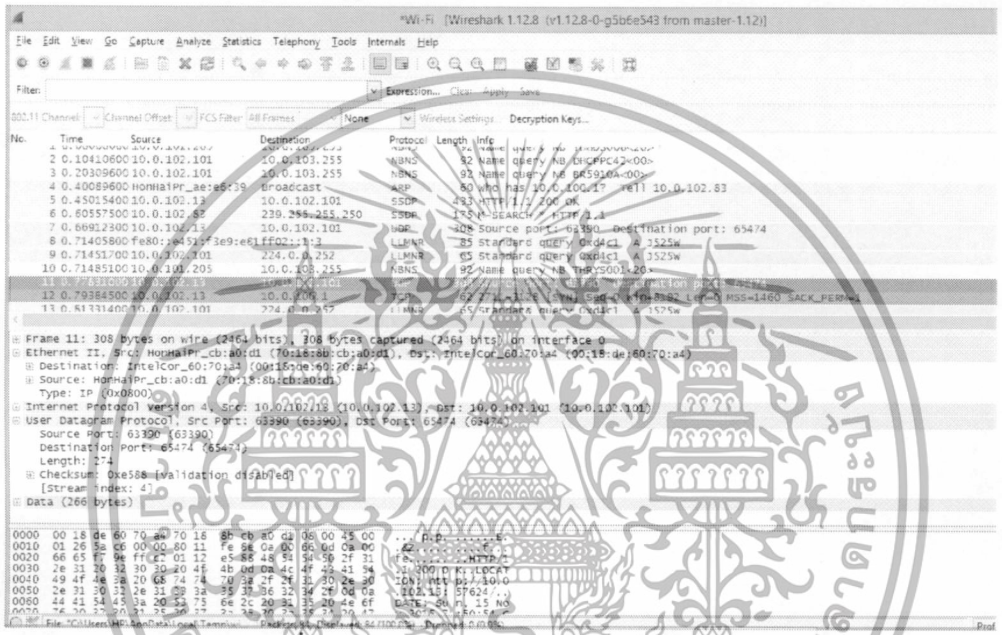
7. จากนั้น ถ้าต้องการเซฟเป็นไฟล์เพื่อนำมาวิเคราะห์ หรือเปรียบเทียบในครั้งต่อไปก็สามารถทำได้ โดยไปที่เมนูบาร์ เลือกไฟล์(file) จากนั้นกดเลือก เซฟแอส (save as) แล้วตั้งชื่อไฟล์ตามต้องการ จะได้ไฟล์นามสกุล .pcap ออกมา
8. การใช้งานโปรแกรมไวร์ชาร์กเพื่อการทำงานนั้นจำเป็นต้องศึกษารายละเอียดจากหน้าจอแสดงผลของโปรแกรมให้ถูกต้อง โดยโปรแกรมไวร์ชาร์กนั้น จะแบ่งส่วนแสดงผลออกเป็นดังนี้

- ส่วนที่ 1 - แสดงชื่อโปรแกรมและ แสดงอินเทอร์เฟสที่กำลังดักจับข้อมูลผ่านอินเทอร์เฟสนั้นอยู่ หรือชื่อไฟล์ที่กำลังเปิดแสดงผลอยู่
- ส่วนที่ 2 - เมนูบาร์ แสดงรายละเอียดเมนูต่างๆ ของโปรแกรมไวร์ชาร์ก
- ส่วนที่ 3 - คีย์ลัด อาทิเช่น ปุ่มสตาร์ท ปุ่มสต๊อป ปุ่มเซฟไฟล์ ปุ่มลบไฟล์ การขยาย/ย่อไฟล์ และรูปแบบการฟิลเตอร์ต่างๆ เป็นต้น
- ส่วนที่ 4 - ฟิลเตอร์ข้อมูลที่ต้องการ เป็นแถบที่ให้ใส่โปรโตรคอล หรือ พอร์ต หรือ หมายเลขไอพีแอสแดรส ที่ต้องการวิเคราะห์ เป็นต้น
- ส่วนที่ 5 - แสดงข้อมูลของแพคเก็ตที่ถูกดักจับข้อมูลไว้ โดยมีการแบ่งเป็นทั้งหมด 7 คอลัมน์ ได้แก่ No (ลำดับของแพคเก็ตที่ถูกดักจับได้), Time (เวลาของแพคเก็ตที่ถูกดักจับได้), Source (หมายเลขไอพีแอดเดรสต้นทางที่ส่งแพคเก็ตมา), Destination (หมายเลขไอพีแอดเดรสปลายทางของแพคเก็ต), Protcol (โปรโตรคอลที่อยู่ในแพคเก็ต), length (ความยาวของแพคเก็ตที่ดักจับไว้ได้ หน่อยเป็นไบต์) และ Info (ข้อมูลที่อยู่ในแพคเก็ต)
- ส่วนที่ 6 - แสดงข้อมูล รายละเอียดทั้งหมดทีอยู่ในแพคเก็ตของส่วนที่ 5 ซึ่งจะถูกแสดงโดยละเอียด อาทิเช่น ลำดับที่เท่าไร เป็นข้อมูลแพคเก็ตที่ส่งมาจากหมายเลขไอพีแอสเดรสต้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ทางอะไร หมายเลขพอร์ตต้นทางเบอร์อะไร ต้นทางแมคแอสแดรสอะไร เป็นข้อมูลแพคเก็ตที่ถูกส่งไปหมายเลขไอพีแอสเดรสปลายทางอะไร หมายเลขพอร์ตปลายทางเบอร์อะไร ปลายทางแมคแอสแดรสอะไร ค่าการเช็คซัม ถูกต้องแล้วหรือไม่ เป็นโปรโตรคอลประเภทไหน เป็นต้น

- ส่วนที่ 7 - แสดงข้อมูลที่อยู่ในแพคเก็ตที่ถูกดักจับ คล้ายกับส่วนที่ 6 แต่แสดงในรูปแบบของแอสกี้
- ส่วนที่ 8 - แสดงจำนวนแพคเก็ตที่ถูกดักจับไว้ได้ ถูกนำมาแสดงคิดเป็นกี่เปอร์เซ็นต์ และถ้านำมาแสดงไม่ครบแสดงว่าถูกดรอปไปกี่เปร์เซ็นต์



รูปที่ 3.15 รูปแสดงหน้าโปรแกรมไวร์ชาร์ก

9. การใช้งานฟิลเตอร์ เพื่อที่จะเฉพาะข้อมูลแพคเก็ตที่ให้ความสนใจนำมาวิเคราะห์เท่านั้น ส่วนนี้จะช่วยกรองสิ่งที่ไม่ต้องการวิเคราะห์ออกไป สามารถดูตัวอย่างการฟิลเตอร์ ตามด้านล่าง

ip.addr == 192.168.1.1

ip.src == 192.168.1.1 and ip.dst == 192.168.1.10

ip.src == 192.168.1.1	ip.dst == 192.168.2.1
ip.src != 192.168.1.1	ip.dst != 192.168.2.1
tcp.port == 123	udp.port == 3456
tcp.dstport == 123	udp.dstport == 3456
tcp.srcport == 123	udp.srcport == 3456

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เครื่องหมายเปรียบเทียบ ที่สำคัญของโปรแกรมไวร์ชาร์ดมีดังต่อไปนี้

== เป็นเครื่องหมายที่สื่อความว่า equal

!= เป็นเครื่องหมายที่สื่อความว่า not equal

> เป็นเครื่องหมายที่สื่อความว่า greater than

< เป็นเครื่องหมายที่สื่อความว่า less than

>= เป็นเครื่องหมายที่สื่อความว่า greater or equal

<= เป็นเครื่องหมายที่สื่อความว่า lessthan or equal

เครื่องหมาย logical expression สำคัญของโปรแกรมไวร์ชาร์ดมีดังต่อไปนี้

&& เป็นเครื่องหมายที่สื่อความว่า and

|| เป็นเครื่องหมายที่สื่อความว่า or

! เป็นเครื่องหมายที่สื่อความว่า not

^^ เป็นเครื่องหมายที่สื่อความว่า xor

3.8 สรุป

จากบทนี้ทำให้เข้าใจถึงวิธีการสร้าง และรูปแบบการทำงาน ของโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง การสร้างเอกสารเอกซ์เอ็มแอลเพื่อที่ใช้ในการระบุค่าพารามิเตอร์ต่างๆที่ต้องกรอกลงบนโปรแกรม และใช้ทำหน้าที่ดึงไฟล์พีแคป์ที่เป็น ไฟล์ที่ทำหน้าที่เก็บข้อมูลที่ดักจับทราฟฟิคมาจากระบบเครือข่ายเดิม รวมถึงวิธีการสร้างระบบเครือข่ายไอพีเวอร์ชั่น6 ที่จะใช้ในการทดลองในบทถัดไปด้วย ซึ่งความรู้เรื่องระบบเครือข่ายจะนำมาช่วยในการคอนฟิก บนอุปกรณ์เร้าเตอร์เพื่อสร้างเส้นทางทราฟฟิคระหว่างผู้ใช้งานนั้นเอง ส่วนโปรแกรมภาษาซีชาร์ปนั้น เป็นการนำมาสร้างโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง เพื่อให้คอมพิวเตอร์ระหว่างเซิร์ฟเวอร์และไคลเอนต์สามารถรับส่งข้อมูลระหว่างกันได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4

การทดลองและผลการทดลอง

จากข้อมูลของบทที่ 3 ทั้งในส่วนของตัวโปรแกรมที่จำลองข้อมูลทราฟฟิคเสมือนจริง ที่ใช้ในการรับ-ส่งข้อมูล การสร้างเอกสารเอกซ์เอ็มแอลเพื่อใช้เรียกไฟล์พีแคป ข้อมูลการติดตั้งระบบเครือข่ายไอพีเวอร์ชั่น6 รวมถึงขบวนการขั้นตอนในการเก็บไฟล์พีแคป ขั้นตอนต่อไปจะเป็นการนำไปทำสอบกับระบบเครือข่ายจำลองที่สร้างขึ้น เพื่อทดสอบและหาค่าเปรียบเทียบว่า สามารถข้อมูลจริงที่เก็บมาจากระบบเครือข่ายไอพีเวอร์ชั่นปัจจุบันนั้น เมื่อมีการเปลี่ยนแปลงเป็นระบบเครือข่ายไอพีเวอร์ชั่น6 โปรแกรมที่สร้างขึ้นนั้นก็สามารถจำลองข้อมูลทราฟฟิคที่เสมือนจริงได้โดยไม่จำเป็นต้องมาทำการติดตั้งอุปกรณ์จำนวนมากมายเพื่อทดสอบนั้นเอง ดังนั้นในบทนี้จะพูดถึงระบบเครือข่ายที่ทดสอบ ขั้นตอนการทำงานของโปรแกรม การแสดงผลของโปรแกรม รวมถึงจดบันทึกค่าตามผลการทดลองเพื่อนำไปเปรียบเทียบและสรุปต่อไป

4.1 รูปแบบการทดลอง

4.1.1 การรับส่ง-ข้อมูล ผ่านระบบเครือข่าย บนเร้าเตอร์เพียงตัวเดียว

ในส่วนของรูปแบบการทดลองที่ 1 นั้น เราจะใช้การรับ-ส่งข้อมูลทราฟฟิค ข้ามผ่านอุปกรณ์เครือข่ายแค่ตัวเดียวเท่านั้น เพื่อทดสอบให้เทียบกันว่า เวลาการไฟล์ข้อมูลต้นแบบที่เก็บมาจากระบบเครือข่ายจริง เมื่อนำมาใช้บนระบบเครือข่ายที่ใช้ในการทดสอบการติดตั้ง ก็ยังคงได้ค่าของข้อมูลทราฟฟิคแบบเดิม

โดยส่วนของการทดลองนี้ เราจะใช้อุปกรณ์เนตเวิร์ก ยี่ห้อ CISCO รุ่น ME3600X มาใช้ในการทดสอบ และอุปกรณ์ ปลายทางที่เป็นคอมพิวเตอร์ 2 เครื่อง ที่จะจำลองเป็นตัวรับ และตัวส่งในระบบเครือข่าย

ระบบเครือข่ายไอพีเวอร์ชั่น 4

ส่วนนี้จะเป็นการตั้งค่าอุปกรณ์เน็ตเวิร์กที่ใช้ในการทดสอบ โดยเริ่มจากการเปิดรูปแบบการทำงานเร้าท์ติ้งให้อุปกรณ์ พร้อมทั้ง ตั้งค่าหมายเลขไอพีแอสเดรสของแต่ละพอร์ท ที่ต่อกับคอมพิวเตอร์ที่ทดสอบ

```
ip routing
ip cef
!
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

interface GigabitEthernet0/10

description connect to Client

no switchport

ip address 11.11.11.1 255.255.255.0

load-interval 30

!

interface GigabitEthernet0/20

description connect to Server

no switchport

ip address 22.22.22.1 255.255.255.0

load-interval 30

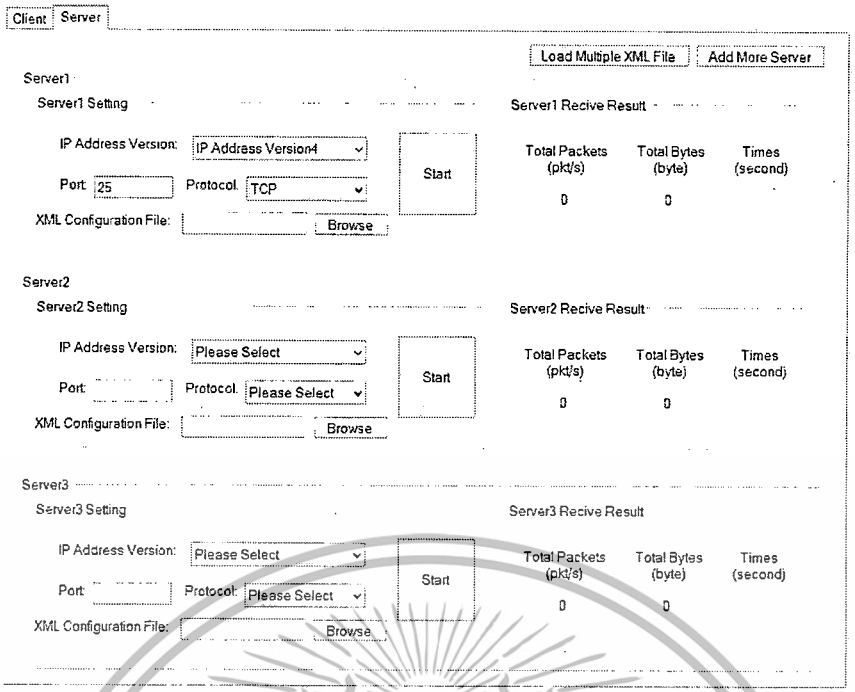
!

หลังจากนั้นก็ทำการตั้งค่าหมายเลขไอพีแอสเดรสให้กับคอมพิวเตอร์ที่ใช้ในการทดสอบ แล้วต่อด้วยการทดสอบการเชื่อมต่อ (connectivity test) เพื่อทดสอบว่าเซิร์ฟเวอร์สามารถติดต่อสื่อสารกับคอมพิวเตอร์ที่ทำหน้าที่เป็นตัวส่งได้

รูปที่ 4.1 รูปแสดงการตรวจสอบการเชื่อมต่อการทดสอบไอพีเวอร์ชั่น 4 ข้อ4.1.1

ขั้นตอนต่อไป คือการตั้งค่าบนโปรแกรมซอคเกต ที่ใช้ในการรับ-ส่ง ข้อมูลทราฟฟิค โดยที่ฝั่งเซิร์ฟเวอร์จะทำการตั้งค่า ไอพีแอสเดรสเวอร์ชั่น และโปรโตรคอลพอร์ท ตามที่ต้องการ ในขณะทางด้านฝั่งส่งก็ต้องทำการตั้งค่าที่ไคลเอนท์ ก็ต้องบอกหมายเลขไอพีแอสเดรสของเซิร์ฟเวอร์ที่ต้องการส่ง และเลือกข้อมูลทราฟฟิคที่เป็นพีแคปไฟล์ ที่ต้องการส่งผ่านระบบเครือข่าย รวมถึงโปรโตรคอลพอร์ทปลายทางด้วย โดยการทดลองนี้เราเลือกที่จะใช้โปรโตรคอลพอร์ทหมายเลข 25 ในการทดลอง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.2 รูปแสดงการตั้งค่าโปรแกรมจำลองทราฟฟิคฝั่งเซิร์ฟเวอร์ไอพีเวอร์ชั่น 4 ข้อ 4.1.1

ระบบเครือข่ายไอพีเวอร์ชั่น 6

ส่วนนี้จะเป็นการตั้งค่าอุปกรณ์เน็ตเวิร์กที่ใช้ในการทดสอบระบบเครือข่ายไอพีเวอร์ชั่น6 โดยเริ่มจากการเปิดรูปแบบการทำงานเร้าท์ติ้งเพื่อสนับสนุนการทำงานของไอพีเวอร์ชั่น6 ให้อุปกรณ์ พร้อมทั้ง ตั้งค่าหมายเลขไอพีแอสเดรสเวอร์ชั่น6 ของแต่ละพอร์ท ที่ต่อกับคอมพิวเตอร์ที่ทดสอบ

```
ip routing
ipv6 unicast- routing
ip cef
!
interface GigabitEthernet0/10
 description connect to Client
 no switchport
no ip address
 load-interval 30
 ipv6 address 2001:1234::1/64
!
interface GigabitEthernet0/20
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

description connect to Server

no switchport

no ip address

load-interval 30

ipv6 address 2001:4321::1/64

!

หลังจากนั้นก็ทำการตั้งค่าหมายเลขไอพีแอสเดรสเวอร์ชั่น6 ให้กับคอมพิวเตอร์ที่ใช้ในการทดสอบ แล้วต่อด้วยการทดสอบการเชื่อมต่อ (connectivity test) เพื่อทดสอบว่าเซิร์ฟเวอร์สามารถติดต่อสื่อสารกับคอมพิวเตอร์ที่ทำหน้าที่เป็นตัวส่งได้

รูปที่ 4.3 รูปแสดงการตรวจสอบการเชื่อมต่อการทดสอบไอพีเวอร์ชั่น 6 ข้อ4.1.1

ขั้นตอนต่อไป คือการตั้งค่าบนโปรแกรมซอคเกต ที่ใช้ในการรับ-ส่ง ข้อมูลทราฟฟิค โดยที่ฝั่งเซิร์ฟเวอร์จะทำการตั้งค่า ไอพีแอสเดรสเวอร์ชั่น เป็นเอาร์ชั่น6 และ โปรโตรคอลพอร์ท ตามที่ต้องการ ในขณะทางด้านฝั่งส่งก็ต้องทำการตั้งค่าที่ไคลเอนท์ ก็ต้องบอกหมายเลขไอพีแอสเดรสเวอร์ชั่น 6 ของเซิร์ฟเวอร์ที่ต้องการส่ง และเลือกข้อมูลทราฟฟิคที่เป็นพีแคปไฟล์ ที่ต้องการส่งผ่านระบบเครือข่าย รวมถึงโปรโตรคอลพอร์ทปลายทางด้วย โดยการทดลองนี้เราเลือกที่จะใช้โปรโตรคอลพอร์ทหมายเลข 25 ในการทดลอง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 4.4 รูปแสดงการตั้งค่าโปรแกรมจำลองทราฟฟิคฝั่งเซิร์ฟเวอร์ไอพีเวอร์ชั่น 6 ข้อ 4.1.1

4.1.2 การรับส่ง-ข้อมูล ผ่านระบบเครือข่าย แบบการใช้งานภายในองค์กร

ในส่วนของรูปแบบการทดลองที่ 2 นั้น เราจะใช้การรับ-ส่งข้อมูลทราฟฟิค ข้ามผ่านอุปกรณ์เครือข่ายที่ใช้งานเร้าท์ติ้งโปรโตรคอลรูปแบบOSPF และมีการส่งจากคอมพิวเตอร์ที่ทำหน้าที่ส่งทราฟฟิคจำนวน2เครื่อง มาที่คอมพิวเตอร์ตัวรับเพียงเครื่องเดียว เพื่อทดสอบให้เทียบกันว่า เวลาการไฟล์ข้อมูลต้นแบบที่เก็บมาจากระบบเครือข่ายจริง เมื่อนำมาใช้บนระบบเครือข่ายที่ใช้ในการทดสอบการติดตั้งที่ผ่านอุปกรณ์เน็ตเวิร์กหลายๆเครื่อง ก็ยังคงได้ค่าของข้อมูลทราฟฟิคแบบเดิม

โดยส่วนของการทดลองนี้ เราจะใช้อุปกรณ์เนตเวิร์ก ยี่ห้อ CISCO รุ่น ME3600X จำนวน 4 เครื่อง มาใช้ในการทดสอบ และอุปกรณ์ ปลายทางที่เป็นคอมพิวเตอร์ 3 เครื่อง โดยจะจำลองเป็นตัวรับ 1 เครื่อง และตัวส่ง 2 เครื่อง ในระบบเครือข่าย

ระบบเครือข่ายไอพีเวอร์ชั่น 4

ส่วนนี้จะเป็นการตั้งค่าอุปกรณ์เน็ตเวิร์กที่ใช้ในการทดสอบ โดยเริ่มจากการเปิดรูปแบบการทำงานเร้าท์ติ้งให้อุปกรณ์ พร้อมทั้ง ตั้งค่าหมายเลขไอพีแอสเดรสของแต่ละพอร์ท ที่เชื่อมต่อกัน ก่อนจะเริ่มการตั้งค่าเร้าท์ติ้งรูปแบบ OSPF เพื่อให้ระบบเครือข่ายแลกเปลี่ยนเส้นทางกันโดยใช้โปรโตรคอลชนิดนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Router 1

ip routing

ip cef

!

!

interface Loopback 0

ip address 1.1.1.1 255.255.255.255

!

interface GigabitEthernet0/10

description connect to Client_1

no switchport

ip address 11.11.11.1 255.255.255.0

load-interval 30

!

interface GigabitEthernet0/20

description connect to Client_2

no switchport

ip address 12.12.12.1 255.255.255.0

load-interval 30

!

interface GigabitEthernet0/23

description connect to Router_2

no switchport

ip address 10.10.12.1 255.255.255.252

load-interval 30

!

interface GigabitEthernet0/24

description connect to Router_3

no switchport

ip address 10.10.13.1 255.255.255.252

load-interval 30

!

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
!
router ospf 10
 router-id 1.1.1.1
 network 1.1.1.1 0.0.0.0 area 0
 network 11.11.11.1 0.0.0.0 area 0
 network 12.12.12.1 0.0.0.0 area 0
 network 10.10.12.1 0.0.0.0 area 0
 network 10.10.13.1 0.0.0.0 area 0
 !
!
### Router 2 ###
ip routing
ip cef
!
!
interface Loopback 0
 ip address 2.2.2.2 255.255.255.255
!
interface GigabitEthernet0/23
 description connect to Router_1
 no switchport
 ip address 10.10.12.2 255.255.255.252
 load-interval 30
!
interface GigabitEthernet0/24
 description connect to Router_4
 no switchport
 ip address 10.10.24.2 255.255.255.252
 load-interval 30
!
!
router ospf 10
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
 router-id 2.2.2.2
 network 2.2.2.2 0.0.0.0 area 0
 network 10.10.12.2 0.0.0.0 area 0
 network 10.10.24.2 0.0.0.0 area 0
 !
!
```

Router 3

```
ip routing
ip cef
!
!
interface Loopback 0
 ip address 3.3.3.3 255.255.255.255
!
```

interface GigabitEthernet0/23

```
 description connect to Router_1
 no switchport
 ip address 10.10.13.2 255.255.255.252
 load-interval 30
!
```

interface GigabitEthernet0/24

```
 description connect to Router_4
 no switchport
 ip address 10.10.34.2 255.255.255.252
 load-interval 30
!
!
router ospf 10
 router-id 3.3.3.3
 network 3.3.3.3 0.0.0.0 area 0
 network 10.10.13.2 0.0.0.0 area 0
 network 10.10.34.2 0.0.0.0 area 0
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
!
!
### Router 4 ###
ip routing
ip cef
!
!
interface Loopback 0
 ip address 4.4.4.4 255.255.255.255
!
interface GigabitEthernet0/10
 description connect to Server
 no switchport
 ip address 22.22.22.1 255.255.255.0
 load-interval 30
!
interface GigabitEthernet0/23
 description connect to Router_2
 no switchport
 ip address 10.10.24.1 255.255.255.252
 load-interval 30
!
interface GigabitEthernet0/24
 description connect to Router_3
 no switchport
 ip address 10.10.34.1 255.255.255.252
 load-interval 30
!
!
router ospf 10
 router-id 4.4.4.4
 network 4.4.4.4 0.0.0.0 area 0
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

network 22.22.22.1 0.0.0.0 area 0

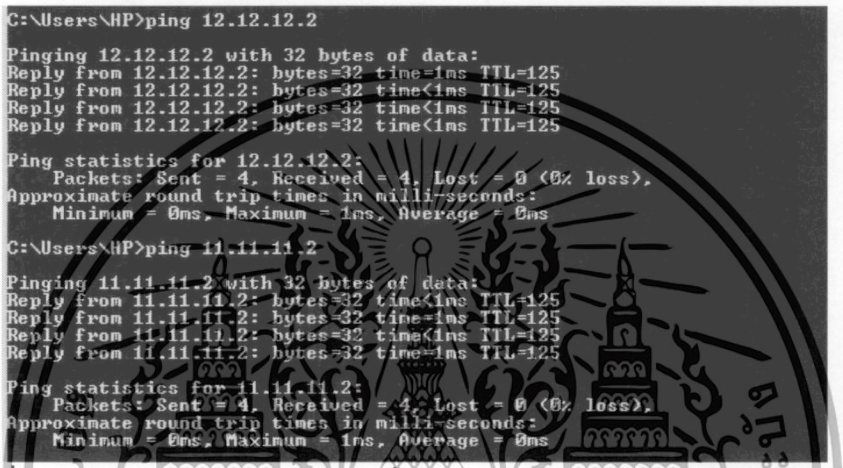
network 10.10.24.1 0.0.0.0 area 0

network 10.10.34.1 0.0.0.0 area 0

!

!

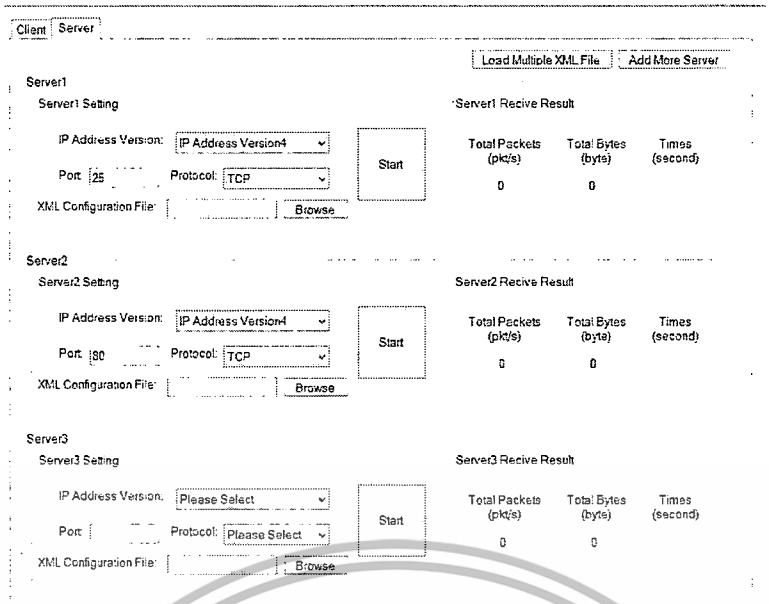
หลังจากนั้นก็ทำการตั้งค่าหมายเลขไอพีแอสเดรสให้กับคอมพิวเตอร์ที่ใช้ในการทดสอบ แล้วต่อด้วยการทดสอบการเชื่อมต่อ (connectivity test) เพื่อทดสอบว่าเซิร์ฟเวอร์สามารถติดต่อสื่อสารกับคอมพิวเตอร์ที่ทำหน้าที่เป็นตัวส่งทั้ง 2 เครื่องได้



รูปที่ 4.5 รูปแสดงการตรวจสอบการเชื่อมต่อการทดสอบไอพีเวอร์ชั่น 4 ข้อ4.1.2

ขั้นตอนต่อไป คือการตั้งค่าบน โปรแกรมซอคเกต ที่ใช้ในการรับ-ส่ง ข้อมูลทราฟฟิค โดยที่ฝั่งเซิร์ฟเวอร์จะทำการตั้งค่า ไอพีแอสเดรสเวอร์ชั่น และโปรโตรคอลพอร์ท ตามที่ต้องการ ในขณะทางด้านฝั่งส่งก็ต้องทำการตั้งค่าที่ไคลเอนท์ ก็ต้องบอกหมายเลขไอพีแอสเดรสของเซิร์ฟเวอร์ที่ต้องการส่ง และเลือกข้อมูลทราฟฟิคที่เป็นพีแคป ไฟล์ ที่ต้องการส่งผ่านระบบเครือข่าย รวมถึงโปรโตรคอลพอร์ทปลายทางด้วย โดยการทดลองนี้เราเลือกที่จะใช้โปรโตรคอลพอร์ทหมายเลข 25 และ 80 ในการทดลอง โดยที่ผู้ส่ง 1(Client1) จะส่งข้อมูลทราฟฟิคของระบบเครือข่ายเดิม มาในรูปแบบของข้อมูลที่เป็นโปรโตรคอลพอร์ท 80 และที่ผู้ส่ง 2(Client2) จะส่งข้อมูลทราฟฟิคของระบบเครือข่ายเดิม มาในรูปแบบของข้อมูลที่เป็นโปรโตรคอลพอร์ท 25

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.6 รูปแสดงการตั้งค่าโปรแกรมจำลองทราฟฟิคฝั่งเซิร์ฟเวอร์ไอพีเวอร์ชั่น 4 ข้อ 4.1.2

ระบบเครือข่ายไอพีเวอร์ชั่น 6

ส่วนนี้จะเป็นการตั้งค่าอุปกรณ์เน็ตเวิร์กที่ใช้ในการทดสอบระบบเครือข่ายไอพีเวอร์ชั่น6 โดยเริ่มจากการเปิดรูปแบบการทำงานเร้าท์ติ้งเพื่อสนับสนุนการทำงานของไอพีเวอร์ชั่น6 พร้อมทั้งตั้งค่าหมายเลขไอพีแอสเดรสเวอร์ชั่น6 ของแต่ละพอร์ท ที่เชื่อมต่อกันในระบบเครือข่าย ก่อนจะเริ่มการตั้งค่าเร้าท์ติ้งรูปแบบ OSPFv3 เพื่อให้ระบบเครือข่ายแลกเปลี่ยนเส้นทางของระบบเครือข่ายไอพีเวอร์ชั่น 6

Router 1

ip routing

ipv6 unicast-routing

ip cef

!

!

interface Loopback 0

ip address 1.1.1.1 255.255.255.255

!

interface GigabitEthernet0/10

description connect to Client_1

no switchport

no ip address

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
 load-interval 30
 ipv6 address 2001:1234::1/64
 ipv6 ospf 10 area 0
!
interface GigabitEthernet0/20
 description connect to Client_2
 no switchport
 no ip address
 load-interval 30
 ipv6 address 2002:1234::1/64
 ipv6 ospf 10 area 0
!
interface GigabitEthernet0/23
 description connect to Router_2
 no switchport
 no ip address
 load-interval 30
 ipv6 address 2001:DDD2::1/64
 ipv6 ospf 10 area 0
!
interface GigabitEthernet0/24
 description connect to Router_3
 no switchport
 no ip address
 load-interval 30
 ipv6 address 2001:DDD3::1/64
 ipv6 ospf 10 area 0
!
!
ipv6 router ospf 10
 router-id 1.1.1.1
!
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
!
### Router 2 ###
ip routing
ipv6 unicast-routing
ip cef
!
!
interface Loopback 0
 ip address 2.2.2.2 255.255.255.255
!
interface GigabitEthernet0/23
 description connect to Router_1
 no switchport
 no ip address
 load-interval 30
 ipv6 address 2001:DDD2::2/64
 ipv6 ospf 10 area 0
!
interface GigabitEthernet0/24
 description connect to Router_4
 no switchport
 no ip address
 load-interval 30
 ipv6 address 2001:CCC2::2/64
 ipv6 ospf 10 area 0
!
!
ipv6 router ospf 10
 router-id 2.2.2.2
 !
!
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Router 3

```
ip routing
ipv6 unicast-routing
ip cef
!
!
interface Loopback 0
 ip address 3.3.3.3 255.255.255.255
!
interface GigabitEthernet0/23
 description connect to Router_1
 no switchport
 no ip address
 load-interval 30
 ipv6 address 2001:DDD3::2/64
 ipv6 ospf 10 area 0
!
interface GigabitEthernet0/24
 description connect to Router_4
 no switchport
 no ip address
 load-interval 30
 ipv6 address 2001:CCC3::2/64
 ipv6 ospf 10 area 0
!
!
ipv6 router ospf 10
 router-id 3.3.3.3
 !
!
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Router 4

ip routing

ipv6 unicast-routing

ip cef

!

!

interface Loopback 0

ip address 4.4.4.4 255.255.255.255

!

interface GigabitEthernet0/10

description connect to Server

no switchport

no ip address

load-interval 30

ipv6 address 2001:4321::1/64

ipv6 ospf 10 area 0

!

interface GigabitEthernet0/23

description connect to Router_2

no switchport

no ip address

load-interval 30

ipv6 address 2001:CCC2::1/64

ipv6 ospf 10 area 0

!

interface GigabitEthernet0/24

description connect to Router_3

no switchport

no ip address

load-interval 30

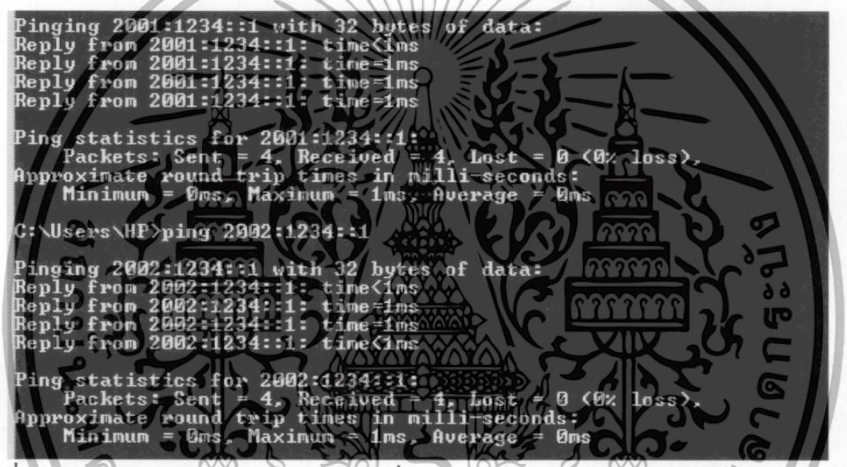
ipv6 address 2001:CCC3::1/64

ipv6 ospf 10 area 0

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
!
!
ipv6 router ospf 10
 router-id 4.4.4.4
 !
!
```

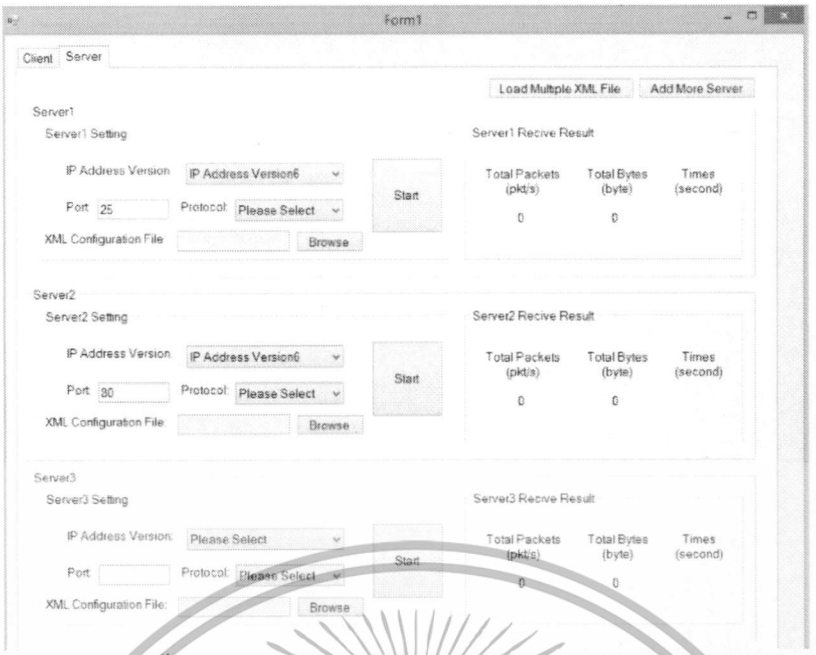
หลังจากนั้นก็ทำการตั้งค่าหมายเลขไอพีแอสเดรสเวอร์ชั่น6 ให้กับคอมพิวเตอร์ที่ใช้ในการทดสอบ แล้วต่อด้วยการทดสอบการเชื่อมต่อ (connectivity test) เพื่อทดสอบว่าเซิร์ฟเวอร์สามารถติดต่อสื่อสารกับคอมพิวเตอร์ทั้ง 2เครื่องที่ทำหน้าที่เป็นตัวส่งได้



รูปที่ 4.7 รูปแสดงการตรวจสอบการเชื่อมต่อการทดสอบไอพีเวอร์ชั่น 6 ข้อ4.1.2

ขั้นตอนต่อไป คือการตั้งค่าบนโปรแกรมซอคเกต ที่ใช้ในการรับ-ส่ง ข้อมูลทราฟฟิค โดยที่ฝั่งเซิร์ฟเวอร์จะทำการตั้งค่า ไอพีแอสเดรสเวอร์ชั่น6 และโปรโตรคอลพอร์ท ตามที่ต้องการ ในขณะทางด้านฝั่งส่งก็ต้องทำการตั้งค่าที่ไคลเอนท์ ก็ต้องบอกหมายเลขไอพีแอสเดรสเวอร์ชั่น 6 ของเซิร์ฟเวอร์ที่ต้องการส่ง และเลือกข้อมูลทราฟฟิคที่เป็นพีแคปไฟล์ ที่ต้องการส่งผ่านระบบเครือข่าย รวมถึงโปรโตรคอลพอร์ทปลายทางด้วย โดยการทดลองนี้เราเลือกที่จะใช้โปรโตรคอลพอร์ทหมายเลข 25 และ 80 ในการทดลอง โดยที่ผู้ส่ง 1(Client1) จะส่งข้อมูลทราฟฟิคของระบบเครือข่ายเดิม มาในรูปแบบของข้อมูลที่เป็นโปรโตรคอลพอร์ท 80 และที่ผู้ส่ง 2(Client2) จะส่งข้อมูลทราฟฟิคของระบบเครือข่ายเดิม มาในรูปแบบของข้อมูลที่เป็นโปรโตรคอลพอร์ท 25

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.8 รูปแสดงการตั้งค่าโปรแกรมจำลองทราฟฟิคฝั่งเซิร์ฟเวอร์ไอพีเวอร์ชั่น 6 ข้อ 4.1.2

4.1.3 การรับส่งข้อมูล ผ่านระบบเครือข่าย แบบการใช้งานระหว่างองค์กร

ในส่วนของรูปแบบการทดลองที่ 3 นั้น เราจะใช้การรับ-ส่งข้อมูลทราฟฟิค ข้ามผ่านอุปกรณ์เครือข่ายที่ใช้งานเร้าท์ติ้งโปรโตรคอลรูปแบบ Static , OSPF และ BGP โดยมีการส่งจากคอมพิวเตอร์ที่ทำหน้าที่ส่งทราฟฟิคจำนวน 2 เครื่อง มาที่คอมพิวเตอร์ตัวรับเพียงเครื่องเดียว เพื่อทดสอบให้เทียบกันว่า เวลาการไฟล์ข้อมูลต้นแบบที่เก็บมาจากระบบเครือข่ายจริง เมื่อนำมาใช้บนระบบเครือข่ายที่ใช้ในรูปแบบเร้าท์ติ้งที่ทำการทดสอบนั้น รวมถึงผ่านอุปกรณ์เน็ตเวิร์กหลายๆ เครื่อง ก็ยังคงได้ค่าของข้อมูลทราฟฟิคแบบเดิม

โดยส่วนของการทดลองนี้ เราจะใช้อุปกรณ์เนตเวิร์ก ยี่ห้อ CISCO รุ่น ME3600X จำนวน 2 เครื่อง และ ASR1001 จำนวน 2 เครื่อง มาใช้ในการทดสอบ และอุปกรณ์ ปลายทางที่เป็นคอมพิวเตอร์ 3 เครื่อง โดยจะจำลองเป็นตัวรับ 1 เครื่อง และตัวส่ง 2 เครื่อง ในระบบเครือข่าย

ระบบเครือข่ายไอพีเวอร์ชั่น 4

ส่วนนี้จะเป็นการตั้งค่าอุปกรณ์เน็ตเวิร์กที่ใช้ในการทดสอบ โดยเริ่มจากการเปิดรูปแบบการทำงานเร้าท์ติ้งให้อุปกรณ์ พร้อมทั้ง ตั้งค่าหมายเลขไอพีแอสเดรสของแต่ละพอร์ท ที่เชื่อมต่อกัน ก่อนจะเริ่มการตั้งค่าเร้าท์ติ้งของฝั่ง A ให้แลกเปลี่ยนเร้าท์โดยใช้เร้าท์ติ้งโปรโตรคอล OSPF และฝั่ง B ใช้ static route ในการแลกเปลี่ยนข้อมูล จากนั้นจะเชื่อมต่อฝั่ง A และ B ให้แลกเปลี่ยนเร้าท์ โดยใช้เร้าท์ติ้งโปรโตรคอล BGP ในส่วนของคอมพิวเตอร์ที่จะรันโปรแกรมซอคเกตนั้น จะทำการกำหนดค่าหมายเลขไอพีแอสเดรสตามต้องการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Router 1

ip routing

ip cef

!

!

interface Loopback 0

ip address 1.1.1.1 255.255.255.255

!

interface GigabitEthernet0/10

description connect to Client_1

no switchport

ip address 11.11.11.1 255.255.255.0

load-interval 30

!

interface GigabitEthernet0/20

description connect to Client_2

no switchport

ip address 12.12.12.1 255.255.255.0

load-interval 30

!

interface GigabitEthernet0/24

description connect to Router_2

no switchport

ip address 10.10.12.1 255.255.255.252

load-interval 30

!

!

router ospf 10

router-id 1.1.1.1

network 1.1.1.1 0.0.0.0 area 0

network 11.11.11.1 0.0.0.0 area 0

network 12.12.12.1 0.0.0.0 area 0

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
 network 10.10.12.1 0.0.0.0 area 0
 !
!
### Router 2 ###
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!
interface GigabitEthernet0/0/0
 description connect to Router_1
 ip address 10.10.12.2 255.255.255.252
!
interface GigabitEthernet0/0/1
 description connect to Router_3
 ip address 10.10.23.1 255.255.255.252
!
router ospf 10
 router-id 2.2.2.2
 network 2.2.2.2 0.0.0.0 area 0
 network 10.10.12.2 0.0.0.0 area 0
 !
!
router bgp 65001
 bgp router-id 2.2.2.2
 bgp log-neighbor-changes
 neighbor 10.10.23.2 remote-as 65001
 !
 address-family ipv4
  redistribute connected
  redistribute ospf 10 internal external
  neighbor 10.10.23.2 activate
  neighbor 10.10.23.2 soft-reconfiguration inbound
 exit-address-family
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
!
!

### Router 3 ###
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
!
interface GigabitEthernet0/0/0
 description connect to Router_4
 ip address 10.10.34.2 255.255.255.252
!
interface GigabitEthernet0/0/1
 description connect to Router_2
 ip address 10.10.23.2 255.255.255.252
!
ip route 22.22.22.0 255.255.255.0 GigabitEthernet0/0/0 10.10.34.1
 !
!
router bgp 65001
 bgp router-id 3.3.3.3
 bgp log-neighbor-changes
 neighbor 10.10.23.1 remote-as 65001
 !
 address-family ipv4
  redistribute connected
  redistribute static
  neighbor 10.10.23.1 activate
  neighbor 10.10.23.1 soft-reconfiguration inbound
 exit-address-family
 !
!
### Router 4 ###
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

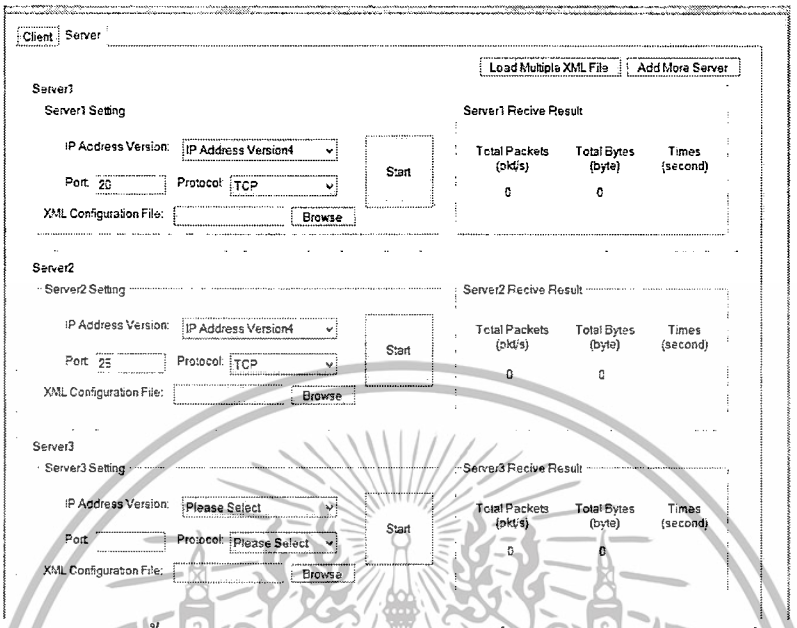
```
ip routing
ip cef
!
!
interface Loopback 0
 ip address 4.4.4.4 255.255.255.255
!
interface GigabitEthernet0/10
 description connect to Server
 no switchport
 ip address 22.22.22.1 255.255.255.0
 load-interval 30
!
interface GigabitEthernet0/24
 description connect to Router_3
 no switchport
 ip address 10.10.34.1 255.255.255.252
 load-interval 30
!
!
ip route 11.11.11.0 255.255.255.0 GigabitEthernet0/24 10.10.34.2
ip route 12.12.12.0 255.255.255.0 GigabitEthernet0/24 10.10.34.2
 !
!
```

หลังจากนั้นก็ทำการตั้งค่าหมายเลขไอพีแอสเดรสให้กับคอมพิวเตอร์ที่ใช้ในการทดสอบ แล้วต่อด้วยการทดสอบการเชื่อมต่อ (connectivity test) เพื่อทดสอบว่าเซิร์ฟเวอร์สามารถติดต่อสื่อสารกับคอมพิวเตอร์ที่ทำหน้าที่เป็นตัวส่งทั้ง 2 เครื่องได้

ขั้นตอนต่อไป คือการตั้งค่าบนโปรแกรมซอคเกต ที่ใช้ในการรับ-ส่ง ข้อมูลทราฟฟิค โดยที่ฝั่งเซิร์ฟเวอร์จะทำการตั้งค่า ไอพีแอสเดรสเวอร์ชั่น และโปรโตรคอลพอร์ท ตามที่ต้องการ ในขณะทางด้านฝั่งส่งก็ต้องทำการตั้งค่าที่ไคลเอนท์ ก็ต้องบอกหมายเลขไอพีแอสเดรสของเซิร์ฟเวอร์ที่ต้องการส่ง และเลือกข้อมูลทราฟฟิคที่เป็นพีแคปไฟล์ ที่ต้องการส่งผ่านระบบเครือข่าย รวมถึงโปรโตรคอลพอร์ทปลายทางด้วย โดยการทดลองนี้เราเลือกที่จะใช้โปรโตรคอลพอร์ทหมายเลข 20

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

และ 25 ในการทดลอง โดยที่ผู้ส่ง 1(Client1) จะส่งข้อมูลทราฟฟิคของระบบเครือข่ายเดิม มาในรูปแบบของข้อมูลที่เป็นโปรโตรคอลพอร์ท 25 และที่ผู้ส่ง 2(Client2) จะส่งข้อมูลทราฟฟิคของระบบเครือข่ายเดิม มาในรูปแบบของข้อมูลที่เป็นโปรโตรคอลพอร์ท 20



รูปที่ 4.9 รูปแสดงการตั้งค่าโปรแกรมจำลองทราฟฟิคฝั่งเซิร์ฟเวอร์ไอพีเวอร์ชั่น 4 ข้อ 4.1.3

ระบบเครือข่ายไอพีเวอร์ชั่น 6

ส่วนนี้จะเป็นการตั้งค่าอุปกรณ์เน็ตเวิร์กที่ใช้ในการทดสอบระบบเครือข่ายไอพีเวอร์ชั่น6 โดยเริ่มจากการเปิดรูปแบบการทำงานเร้าท์ติ้งให้อุปกรณ์ พร้อมทั้ง ตั้งค่าหมายเลขไอพีแอสเดรสเวอร์ชั่น 6 ของแต่ละพอร์ท ที่เชื่อมต่อกัน ก่อนจะเริ่มการตั้งค่าเร้าท์ติ้งของฝั่ง A ให้แลกเปลี่ยนเร้าท์โดยใช้เร้าท์ติ้งโปรโตรคอล OSPFv3 และฝั่ง B ใช้การแลกเปลี่ยนเร้าท์ติ้งโดยใช้ static routing จากนั้นจะเชื่อมต่อฝั่ง A และ B ให้แลกเปลี่ยนเร้าท์ โดยใช้เร้าท์ติ้งโปรโตรคอล BGP ที่ใช้ส่วนของ IPv6 unicast ในส่วนของคอมพิวเตอร์ที่จะรันโปรแกรมซอคเกตนั้น จะทำการกำหนดค่าหมายเลขไอพีแอสเดรสตามต้องการ

Router 1

ip routing

ipv6 unicast-routing

ip cef

!

!

interface Loopback 0

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
 ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet0/10
 description connect to Client_1
 no switchport
 no ip address
 ipv6 address 2001:1234::1/64
 ipv6 ospf 10 area 0
!
interface GigabitEthernet0/20
 description connect to Client_2
 no switchport
 no ip address
 ipv6 address 2002:1234::1/64
 ipv6 ospf 10 area 0
!
interface GigabitEthernet0/24
 description connect to Router_2
 no switchport
 no ip address
 ipv6 address 2001:DDD1::1/64
 ipv6 ospf 10 area 0
!
!
ipv6 router ospf 10
 router-id 1.1.1.1
!
```

Router 2

```
ipv6 unicast-routing
!
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!
interface GigabitEthernet0/0/0
 description connect to Router_1
 no ip address
 ipv6 address 2001:DDD2::2/64
 ipv6 ospf 10 area 0
!
interface GigabitEthernet0/0/1
 description connect to Router_3
 no ip address
 ipv6 address 2001:ABCD::1/64
 ipv6 ospf 10 area 0
!
!
ipv6 router ospf 10
 router-id 2.2.2.2
 !
!
router bgp 65001
 bgp router-id 2.2.2.2
 bgp log-neighbor-changes
 neighbor 2001:ABCD::2 remote-as 65001
 !
 address-family ipv6
  redistribute connected
  redistribute ospf 10 internal external
  neighbor 2001:ABCD::2 activate
  neighbor 2001:ABCD::2 soft-reconfiguration inbound
 exit-address-family
 !
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
!

### Router 3 ###
ipv6 unicast-routing
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!
interface GigabitEthernet0/0/0
 description connect to Router_4
 no ip address
 ipv6 address 2001:CCC2::2/64
!
interface GigabitEthernet0/0/1
 description connect to Router_2
 no ip address
 ipv6 address 2001:ABCD::2/64
!
!
ipv6 route 2001:4321::/64 GigabitEthernet0/0/0 2001:CCC2::1
 !
!
router bgp 65001
 bgp router-id 3.3.3.3
 bgp log-neighbor-changes
 neighbor 2001:ABCD::1 remote-as 65001
 !
 address-family ipv6
  redistribute connected
  redistribute static
  neighbor 2001:ABCD::1 activate
  neighbor 2001:ABCD::1 soft-reconfiguration inbound
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

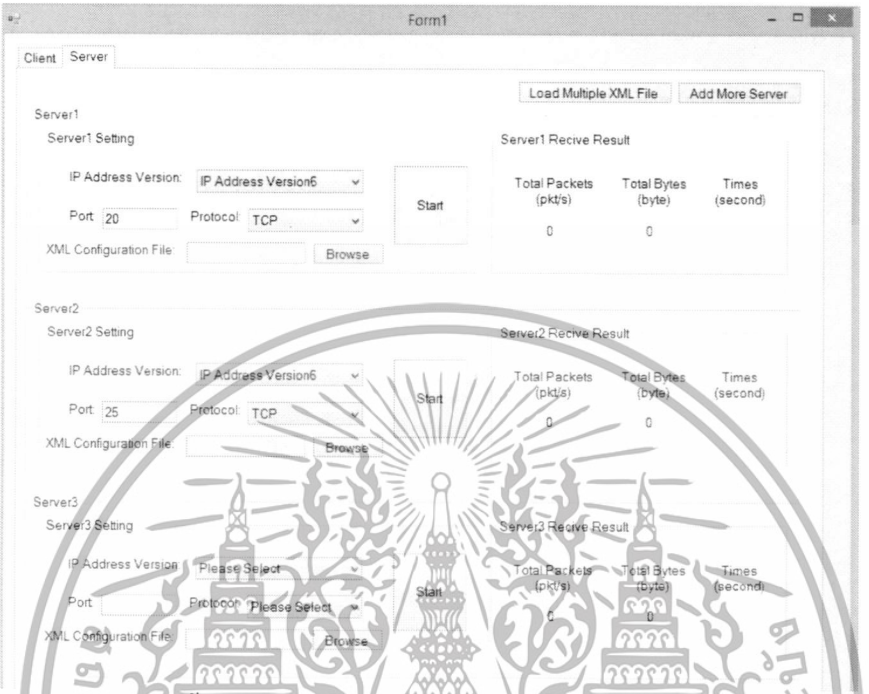
```
 exit-address-family
 !
### Router 4 ###
ip routing
ipv6 unicast-routing
ip cef
!
interface Loopback 0
 ip address 4.4.4.4 255.255.255.255
!
interface GigabitEthernet0/10
 description connect to Server
 no switchport
 no ip address
 ipv6 address 2001:4321::1/64
!
interface GigabitEthernet0/24
 description connect to Router_3
 no switchport
 no ip address
 ipv6 address 2001:CCC2::1/64
!
ipv6 route  2001:1234::/64 GigabitEthernet0/24 2001:CCC2::2
ipv6 route  2002:1234::/64 GigabitEthernet0/24 2001:CCC2::2
 !
```

หลังจากนั้นก็ทำการตั้งค่าหมายเลขไอพีแอสเดรสเวอร์ชั่น6 ให้กับคอมพิวเตอร์ที่ใช้ในการทดสอบ แล้วต่อด้วยการทดสอบการเชื่อมต่อ (connectivity test) เพื่อทดสอบว่าเซิร์ฟเวอร์สามารถติดต่อสื่อสารกับคอมพิวเตอร์ทั้ง 2เครื่องที่ทำหน้าที่เป็นตัวส่งได้

ขั้นตอนต่อไป คือการตั้งค่าบนโปรแกรมซอคเกต ที่ใช้ในการรับ-ส่ง ข้อมูลทราฟฟิค โดยที่ฝั่งเซิร์ฟเวอร์จะทำการตั้งค่า ไอพีแอสเดรสเวอร์ชั่น6 และโปรโตรคอลพอร์ท ตามที่ต้องการ ในขณะทางด้านฝั่งส่งก็ต้องทำการตั้งค่าที่ไคลเอนท์ ก็ต้องบอกหมายเลขไอพีแอสเดรสเวอร์ชั่น 6 ของเซิร์ฟเวอร์ที่ต้องการส่ง และเลือกข้อมูลทราฟฟิคที่เป็นพีแคปไฟล์ ที่ต้องการส่งผ่านระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เครือข่าย รวมถึงโปรโตรคอลพอร์ทปลายทางด้วย โดยการทดลองนี้เราเลือกที่จะใช้โปรโตรคอลพอร์ทหมายเลข 20 และ 25 ในการทดลอง โดยที่ผู้ส่ง 1(Client1) จะส่งข้อมูลทราฟฟิคของระบบเครือข่ายเดิม มาในรูปแบบของข้อมูลที่เป็นโปรโตรคอลพอร์ท 25 และที่ผู้ส่ง 2(Client2) จะส่งข้อมูลทราฟฟิคของระบบเครือข่ายเดิม มาในรูปแบบของข้อมูลที่เป็นโปรโตรคอลพอร์ท 20



รูปที่ 4.10 รูปแสดงการตั้งค่าโปรแกรมจำลองทราฟฟิคฝั่งเซิร์ฟเวอร์ไอพีเวอร์ชั่น 6 ข้อ 4.1.3

4.2 ผลการทดลอง

หลังจากได้ทำการทดสอบตามการทดลองรูปแบบต่างๆ ขั้นตอนต่อไปคือส่วนของการบันทึกผลการทดลอง เพื่อที่จะนำมาเปรียบเทียบผลของข้อมูลทราฟฟิคที่ทำการเก็บจาก ระบบเครือข่ายเดิมที่ใช้งาน และนำมาทดสอบส่งผ่านระบบเครือข่ายที่ทำการทดสอบ โดยใช้โปรแกรมซอคเกตที่สร้างขึ้นนั้น ว่าผลของข้อมูลนั้นมีค่าลงเดิม และสามารถใช้งานได้จริง

4.2.1 การทดลองรับส่ง-ข้อมูล ผ่านระบบเครือข่าย บนเร้าเตอร์เพียงตัวเดียว

จากการทดลองรับ-ส่งข้อมูลผ่านระบบเครือข่ายที่เป็นแบบเร้าเตอร์เพียงตัวเดียว ทั้งบนระบบเครือข่ายไอพีเวอร์ชั่น4 และไอพีเวอร์ชั่น 6 โดยใช้โปรแกรมจำลองข้อมูลทราฟฟิค ที่สร้างขึ้นนั้น ผลการทดลองพบว่าความถูกต้องของข้อมูลเมื่อเทียบกับ พีแคปไฟล์ที่เก็บข้อมูลทราฟฟิคจากระบบเครือข่ายไอพีเวอร์ชั่น4 เดิมนั้น พบว่าข้อมูลของทราฟฟิคที่รับส่งนั้น เหมือนเครือข่ายเดิม 100% และการส่งผ่านข้อมูลทราฟฟิคบนเครือข่ายไอพีเวอร์ชั่น6 นั้นทำงานได้เร็วกว่าระบบเครือข่ายไอพีเวอร์ชั่น4 ตรงตามหลักทฤษฎี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การทดลองบนระบบเครือข่ายไอพีเวอร์ชั่น 4

จากการทดลองรับ-ส่งข้อมูลบนระบบเครือข่ายไอพีเวอร์ชั่น4 โดยใช้โปรแกรมจำลองข้อมูลทราฟฟิค ที่สร้างขึ้นนั้น ผลการทดลองได้ว่า การส่งข้อมูลทั้งหมด 1268256 ไบต์ นั้น ผ่านระบบเครือข่ายที่เป็นแบบเร้าเตอร์เพียงตัวเดียวจะใช้เวลาในการรับ-ส่ง ทั้งหมด 26.938 วินาที และความถูกต้องของข้อมูลเมื่อเทียบกับ พีแคปไฟล์ที่เก็บข้อมูลทราฟฟิคจากระบบเครือข่ายเดิมนั้น พบว่าข้อมูลของทราฟฟิคที่รับส่งนั้น เหมือนเครือข่ายเดิม 100%

ตารางที่ 4.1 แสดงค่าผลการทดสอบการรับ-ส่งผ่านเร้าเตอร์ตัวเดียวแบบไอพีเวอร์ชั่น4

ครั้งที่	ระบบเครือข่าย	รูปแบบระบบเครือข่าย	รูปแบบการส่ง	ขนาดข้อมูลทั้งหมด (Byte)	เวลาที่ใช้งานทั้งหมด (Second)	ความถูกต้องของข้อมูล(%)
1	IPv4	รูปแบบที่1	one Client	1268246	27.66	100
2	IPv4	รูปแบบที่1	one Client	1268246	27.08	100
3	IPv4	รูปแบบที่1	one Client	1268246	27.08	100
4	IPv4	รูปแบบที่1	one Client	1268246	26.37	100
5	IPv4	รูปแบบที่1	one Client	1268246	26.5	100
ค่าเฉลี่ย				1268246	26.938	100

การทดลองบนระบบเครือข่ายไอพีเวอร์ชั่น 6

จากการทดลองรับ-ส่งข้อมูลบนระบบเครือข่ายไอพีเวอร์ชั่น6 โดยใช้โปรแกรมจำลองข้อมูลทราฟฟิค ที่สร้างขึ้นนั้น ผลการทดลองได้ว่า การส่งข้อมูลทั้งหมด 1268256 ไบต์ นั้น ผ่านระบบเครือข่ายที่เป็นแบบเร้าเตอร์เพียงตัวเดียวจะใช้เวลาในการรับ-ส่ง ทั้งหมด 26.254 วินาที และความถูกต้องของข้อมูลเมื่อเทียบกับ พีแคปไฟล์ที่เก็บข้อมูลทราฟฟิคจากระบบเครือข่ายเดิมที่เป็นระบบเครือข่ายไอพีเวอร์ชั่น 6 นั้น พบว่าข้อมูลของทราฟฟิคที่รับส่งนั้น เหมือนเครือข่ายเดิม 100%

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.2 แสดงค่าผลการทดสอบการรับ-ส่งผ่านเร้าเตอร์ตัวเดียวแบบไอพีเวอร์ชั่น6

ครั้งที่	ระบบเครือข่าย	รูปแบบระบบเครือข่าย	รูปแบบการส่ง	ขนาดข้อมูลทั้งหมด(Byte)	เวลาที่ใช้งานทั้งหมด (Second)	ความถูกต้องของข้อมูล (%)
1	IPv6	รูปแบบที่1	one Client	1268246	26.19	100
2	IPv6	รูปแบบที่1	one Client	1268246	26.68	100
3	IPv6	รูปแบบที่1	one Client	1268246	26.18	100
4	IPv6	รูปแบบที่1	one Client	1268246	26	100
5	IPv6	รูปแบบที่1	one Client	1268246	26.22	100
ค่าเฉลี่ย				1268246	26.254	100

4.2.2 การทดลองรับส่ง-ข้อมูล ผ่านระบบเครือข่าย แบบการใช้งานภายในองค์กร

จากการทดลองรับ-ส่งข้อมูลผ่านระบบเครือข่ายที่เป็นแบบเครือข่ายแลนซ์ แบบการใช้งานภายในองค์กร ทั้งบนระบบเครือข่ายไอพีเวอร์ชั่น4 และไอพีเวอร์ชั่น 6 โดยใช้โปรแกรมจำลองข้อมูลทราฟฟิค ที่สร้างขึ้นนั้น ผลการทดลองพบว่าความถูกต้องของข้อมูลเมื่อเทียบกับ พีแคปไฟล์ที่เก็บข้อมูลทราฟฟิคจากระบบเครือข่ายไอพีเวอร์ชั่น4 เดิมนั้น พบว่าข้อมูลของทราฟฟิคที่รับส่งนั้นเหมือนเครือข่ายเดิม 100% และการส่งผ่านข้อมูลทราฟฟิคบนเครือข่ายไอพีเวอร์ชั่น6 นั้นทำงานได้เร็วกว่าระบบเครือข่ายไอพีเวอร์ชั่น4 ตรงตามหลักทฤษฎี

จากการทดลองจะเห็นว่าค่าที่ได้ของผู้ส่งที่1 ใช้เวลามากกว่า การส่งผ่านข้อมูลทราฟฟิคจำลอง บนระบบเครือข่ายที่เป็นแบบเร้าเตอร์เพียงตัวเดียวเพราะ บนระบบเครือข่ายย่อมมีการดีเลย์และค่าต้านๆต่างๆ นั้นเอง หรือกรณีที่ผู้ส่งที่2 ส่งข้อมูลทราฟฟิคจำลอง โดยใช้เวลาน้อยกว่าผู้ส่งที่1 นั้น ก็เนื่องจากเป็นคอมพิวเตอร์คนละรุ่นกัน และส่วนฮาร์ดแวร์ของพอร์ทแลนซ์ก็ผู้ผลิตต่างกันนั่นเอง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การทดลองบนระบบเครือข่ายไอพีเวอร์ชั่น 4

จากการทดลองรับ-ส่งข้อมูลบนระบบเครือข่ายไอพีเวอร์ชั่น4 โดยใช้โปรแกรมจำลองข้อมูลทราฟฟิค ที่สร้างขึ้นนั้น ผลการทดลองได้ว่า การส่งข้อมูลทั้งหมด 1268256 ไบต์ นั้น ผ่านระบบเครือข่ายที่เป็นแบบเร้าเตอร์เพียงตัวเดียวจะใช้เวลาในการรับ-ส่ง ทั้งหมด 38.23 วินาที โดยผู้ส่งที่1 ใช้เวลาการรับ-ส่งข้อมูลทั้งหมด 38.23 วินาที แต่ในส่วนของผู้ส่งที่2 ใช้เวลาการรับ-ส่งข้อมูลทั้งหมด 16.818 วินาที และความถูกต้องของข้อมูลเมื่อเทียบกับ พีแคปไฟล์ที่เก็บข้อมูลทราฟฟิคจากระบบเครือข่ายเดิมนั้น พบว่าข้อมูลของทราฟฟิคที่รับส่งนั้น เหมือนเครือข่ายเดิม 100% ทั้งการรับ-ส่งข้อมูลจาก ผู้ส่งที่1 และ 2

การทดลองบนระบบเครือข่ายไอพีเวอร์ชั่น 6

จากการทดลองรับ-ส่งข้อมูลบนระบบเครือข่ายไอพีเวอร์ชั่น6 โดยใช้โปรแกรมจำลองข้อมูลทราฟฟิค ที่สร้างขึ้นนั้น ผลการทดลองได้ว่า การส่งข้อมูลทั้งหมด 1268256 ไบต์ นั้น ผ่านระบบเครือข่ายที่เป็นแบบเร้าเตอร์เพียงตัวเดียวจะใช้เวลาในการรับ-ส่ง ทั้งหมด 25.874 วินาที โดยผู้ส่งที่1 ใช้เวลาการรับ-ส่งข้อมูลทั้งหมด 25.874 วินาที แต่ในส่วนของผู้ส่งที่2 ใช้เวลาการรับ-ส่งข้อมูลทั้งหมด 15.648 วินาที และความถูกต้องของข้อมูลเมื่อเทียบกับ พีแคปไฟล์ที่เก็บข้อมูลทราฟฟิคจากระบบเครือข่ายเดิมที่เป็นระบบเครือข่ายไอพีเวอร์ชั่น 6 นั้นพบว่าข้อมูลของทราฟฟิคที่รับส่งนั้น เหมือนเครือข่ายเดิม 100% ทั้งการรับ-ส่งข้อมูลจาก ผู้ส่งที่1 และ 2

ตารางที่ 4.3 แสดงค่าผลการทดสอบการรับ-ส่งผ่านเครือข่ายในองค์กรแบบไอพีเวอร์ชั่น4

ครั้งที่	ระบบเครือข่าย	รูปแบบระบบเครือข่าย	อุปกรณ์ส่ง	ขนาดข้อมูลทั้งหมด (Byte)	เวลาที่ใช้งานทั้งหมด (Second)	ความถูกต้องของข้อมูล(%)
1	IPv4	รูปแบบที่2	Client 1	1268246	38.21	100
			Client 2	1268246	16.8	100
2	IPv4	รูปแบบที่2	Client 1	1268246	38.24	100
			Client 2	1268246	17.64	100
3	IPv4	รูปแบบที่2	Client 1	1268246	38.16	100
			Client 2	1268246	16.64	100

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.3 (ต่อ)

ครั้งที่	ระบบเครือข่าย	รูปแบบระบบเครือข่าย	อุปกรณ์ส่ง	ขนาดข้อมูลทั้งหมด (Byte)	เวลาที่ใช้งานทั้งหมด (Second)	ความถูกต้องของข้อมูล(%)
4	IPv4	รูปแบบที่2	Client 1	1268246	38.1	100
			Client 2	1268246	16.77	100
5	IPv4	รูปแบบที่2	Client 1	1268246	38.44	100
			Client 2	1268246	16.24	100
ค่าเฉลี่ย			Client 1	1268246	38.23	100
			Client 2	1268246	16.818	100

ตารางที่ 4.4 แสดงค่าผลการทดสอบการรับ-ส่งผ่านเครือข่ายในองค์กรแบบไอพีเวอร์ชั่น6

ครั้งที่	ระบบเครือข่าย	รูปแบบระบบเครือข่าย	อุปกรณ์ส่ง	ขนาดข้อมูลทั้งหมด (Byte)	เวลาที่ใช้งานทั้งหมด (Second)	ความถูกต้องของข้อมูล(%)
1	IPv6	รูปแบบที่2	Client 1	1268246	26.5	100
			Client 2	1268246	15.33	100
2	IPv6	รูปแบบที่2	Client 1	1268246	25.81	100
			Client 2	1268246	15.77	100
3	IPv6	รูปแบบที่2	Client 1	1268246	25.83	100
			Client 2	1268246	15.88	100

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.4 (ต่อ)

ครั้งที่	ระบบเครือข่าย	รูปแบบระบบเครือข่าย	อุปกรณ์ส่ง	ขนาดข้อมูลทั้งหมด (Byte)	เวลาที่ใช้งานทั้งหมด (Second)	ความถูกต้องของข้อมูล(%)
4	IPv6	รูปแบบที่2	Client 1	1268246	25.6	100
			Client 2	1268246	15.74	100
5	IPv6	รูปแบบที่2	Client 1	1268246	25.63	100
			Client 2	1268246	15.52	100
ค่าเฉลี่ย			Client 1	1268246	25.874	100
			Client 2	1268246	15.648	100

4.2.3 การทดลองรับส่ง-ข้อมูล ผ่านระบบเครือข่าย แบบการใช้งานระหว่างองค์กร

จากการทดลองรับ-ส่งข้อมูลผ่านระบบเครือข่ายที่เป็นแบบเครือข่ายแวนซ์ แบบการใช้งานระหว่างองค์กร ทั้งบนระบบเครือข่ายไอพีเวอร์ชั่น4 และไอพีเวอร์ชั่น 6 โดยใช้โปรแกรมจำลองข้อมูลทราฟฟิค ที่สร้างขึ้นนั้น ผลการทดลองพบว่าความถูกต้องของข้อมูลเมื่อเทียบกับ พีแคปไฟล์ที่เก็บข้อมูลทราฟฟิคจากระบบเครือข่ายไอพีเวอร์ชั่น4 เดิมนั้น พบว่าข้อมูลของทราฟฟิคที่รับส่งนั้นเหมือนเครือข่ายเดิม 100% และการส่งผ่านข้อมูลทราฟฟิคบนเครือข่ายไอพีเวอร์ชั่น6 นั้นทำงานได้เร็วกว่าระบบเครือข่ายไอพีเวอร์ชั่น4 ตรงตามหลักทฤษฎี

จากการทดลองจะเห็นว่าค่าที่ได้ของผู้ส่งที่1 ใช้เวลามากกว่า การส่งผ่านข้อมูลทราฟฟิคจำลอง บนระบบเครือข่ายที่เป็นแบบเร้าเตอร์เพียงตัวเดียวเพราะ บนระบบเครือข่ายย่อมมีการดีเลย์และค่าต้านๆต่างๆ นั้นเอง หรือกรณีที่ผู้ส่งที่2 ส่งข้อมูลทราฟฟิคจำลอง โดยใช้เวลาน้อยกว่าผู้ส่งที่1 นั้น ก็เนื่องจากเป็นคอมพิวเตอร์คนละรุ่นกัน และส่วนฮาร์ดแวร์ของพอร์ทแลนซ์ก็ผู้ผลิตต่างกันนั่นเอง

การทดลองบนระบบเครือข่ายไอพีเวอร์ชั่น 4

จากการทดลองรับ-ส่งข้อมูลบนระบบเครือข่ายไอพีเวอร์ชั่น4 โดยใช้โปรแกรมจำลองข้อมูลทราฟฟิค ที่สร้างขึ้นนั้น ผลการทดลองได้ว่า การส่งข้อมูลทั้งหมด 1268256 ไบต์ นั้น ผ่านระบบเครือข่ายที่เป็นแบบเร้าเตอร์เพียงตัวเดียวจะใช้เวลาในการรับ-ส่ง ทั้งหมด 37.396 วินาที โดยผู้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ส่งที่1 ใช้เวลาการรับ-ส่งข้อมูลทั้งหมด 37.396 วินาที แต่ในส่วนของผู้ส่งที่2 ใช้เวลาการรับ-ส่งข้อมูลทั้งหมด 16.ภ/ภ วินาที และความถูกต้องของข้อมูลเมื่อเทียบกับ พีแคปไฟล์ที่เก็บข้อมูลทราฟฟิคจากระบบเครือข่ายเดิมนั้น พบว่าข้อมูลของทราฟฟิคที่รับส่งนั้น เหมือนเครือข่ายเดิม 100% ทั้งการรับ-ส่งข้อมูลจาก ผู้ส่งที่1 และ 2

การทดลองบนระบบเครือข่ายไอพีเวอร์ชั่น 6

จากการทดลองรับ-ส่งข้อมูลบนระบบเครือข่ายไอพีเวอร์ชั่น6 โดยใช้โปรแกรมจำลองข้อมูลทราฟฟิค ที่สร้างขึ้นนั้น ผลการทดลองได้ว่า การส่งข้อมูลทั้งหมด 1268256 ไบต์ นั้น ผ่านระบบเครือข่ายที่เป็นแบบเร้าเตอร์เพียงตัวเดียวจะใช้เวลาในการรับ-ส่ง ทั้งหมด 25.67 วินาที โดยผู้ส่งที่1 ใช้เวลาการรับ-ส่งข้อมูลทั้งหมด 25.67 วินาที แต่ในส่วนของผู้ส่งที่2 ใช้เวลาการรับ-ส่งข้อมูลทั้งหมด 15.71 วินาที และความถูกต้องของข้อมูลเมื่อเทียบกับ พีแคปไฟล์ที่เก็บข้อมูลทราฟฟิคจากระบบเครือข่ายเดิมที่เป็นระบบเครือข่ายไอพีเวอร์ชั่น 6 นั้นพบว่าข้อมูลของทราฟฟิคที่รับส่งนั้นเหมือนเครือข่ายเดิม 100% ทั้งการรับ-ส่งข้อมูลจาก ผู้ส่งที่1 และ 2

ตารางที่4.5 แสดงค่าผลการทดสอบการรับ-ส่งผ่านเครือข่ายระหว่างองค์กรแบบไอพีเวอร์ชั่น4

ครั้งที่	ระบบเครือข่าย	รูปแบบระบบเครือข่าย	อุปกรณ์ส่ง	ขนาดข้อมูลทั้งหมด (Byte)	เวลาที่ใช้งานทั้งหมด (Second)	ความถูกต้องของข้อมูล(%)
1	IPv4	รูปแบบที่3	Client 1	1268246	38.86	100
			Client 2	1268246	16.14	100
2	IPv4	รูปแบบที่3	Client 1	1268246	39.15	100
			Client 2	1268246	16.36	100
3	IPv4	รูปแบบที่3	Client 1	1268246	38.65	100
			Client 2	1268246	16.22	100
4	IPv4	รูปแบบที่3	Client 1	1268246	39.05	100
			Client 2	1268246	16.66	100

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.5 (ต่อ)

ครั้งที่	ระบบเครือข่าย	รูปแบบระบบเครือข่าย	อุปกรณ์ส่ง	ขนาดข้อมูลทั้งหมด (Byte)	เวลาที่ใช้งานทั้งหมด (Second)	ความถูกต้องของข้อมูล(%)
5	IPv4	รูปแบบที่3	Client 1	1268246	31.27	100
			Client 2	1268246	16.74	100
ค่าเฉลี่ย			Client 1	1268246	37.396	100
			Client 2	1268246	16.424	100

ตารางที่ 4.6 แสดงค่าผลการทดสอบการรับ-ส่งผ่านเครือข่ายระหว่างองค์กรแบบไอพีเวอร์ชั่น6

ครั้งที่	ระบบเครือข่าย	รูปแบบระบบเครือข่าย	อุปกรณ์ส่ง	ขนาดข้อมูลทั้งหมด (Byte)	เวลาที่ใช้งานทั้งหมด (Second)	ความถูกต้องของข้อมูล(%)
1	IPv6	รูปแบบที่3	Client 1	1268246	25.64	100
			Client 2	1268246	15.8	100
2	IPv6	รูปแบบที่3	Client 1	1268246	25.75	100
			Client 2	1268246	15.75	100
3	IPv6	รูปแบบที่3	Client 1	1268246	25.68	100
			Client 2	1268246	15.59	100
4	IPv6	รูปแบบที่3	Client 1	1268246	25.71	100
			Client 2	1268246	15.74	100

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.6 (ต่อ)

ครั้งที่	ระบบเครือข่าย	รูปแบบระบบเครือข่าย	อุปกรณ์ส่ง	ขนาดข้อมูลทั้งหมด (Byte)	เวลาที่ใช้งานทั้งหมด (Second)	ความถูกต้องของข้อมูล(%)
5	IPv6	รูปแบบที่3	Client 1	1268246	25.57	100
			Client 2	1268246	15.67	100
ค่าเฉลี่ย			Client 1	1268246	25.67	100
			Client 2	1268246	15.17	100

4.3 สรุป

จากการทดลองรับ-ส่งข้อมูลผ่านระบบเครือข่ายที่เป็นแบบข้ามเร้าเตอร์ตัวเดียว, แบบเครือข่ายแวนซ์ การใช้งานระหว่างองค์กร และแบบเครือข่ายแวนซ์ การใช้งานระหว่างองค์กร ทั้งบนระบบเครือข่ายไอพีเวอร์ชั่น4 และไอพีเวอร์ชั่น 6 โดยใช้โปรแกรมจำลองข้อมูลทราฟฟิค ที่สร้างขึ้นนั้น ผลการทดลองพบว่าความถูกต้องของข้อมูลเมื่อเทียบกับ พีแคปไฟล์ที่เก็บข้อมูลทราฟฟิคจากระบบเครือข่ายไอพีเวอร์ชั่น4 เดิมนั้น พบว่าข้อมูลของทราฟฟิคที่รับส่งนั้น เหมือนเครือข่ายเดิม 100% และการส่งผ่านข้อมูลทราฟฟิคบนเครือข่ายไอพีเวอร์ชั่น6 นั้นทำงานได้เร็วกว่าระบบเครือข่ายไอพีเวอร์ชั่น4 ตรงตามหลักทฤษฎี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5
สรุปผล

จากการทดลอง และผลการทดลองในบทที่ 4 นั้นทำให้ได้ข้อมูลที่จะสามารถนำมาวิเคราะห์ และสรุปผลเกี่ยวกับการใช้และประสิทธิภาพโปรแกรมซอคเกต ที่จำลองข้อมูลทราฟฟิคเสมือนจริง เพื่อมาทำการทดสอบการใช้งานของเซอร์วิสแบบต่างๆ บนระบบเครือข่ายที่สร้างใหม่ทั้งบนไอพีเวอร์ชั่น4 และไอพีเวอร์ชั่น6 จากการทดลองรับ-ส่งข้อมูลผ่านระบบเครือข่ายที่เป็นแบบข้ามเร้าเตอร์ตัวเดียว, แบบเครือข่ายแวนซ์ การใช้งานระหว่างองค์กร และแบบเครือข่ายแวนซ์ การใช้งานระหว่างองค์กร ซึ่งผลการทดลองพบว่าความถูกต้องของข้อมูลเมื่อเทียบกับ พีแคปไฟล์ที่เก็บข้อมูลทราฟฟิคจากระบบเครือข่ายไอพีเวอร์ชั่น4 เดิมนั้น 100%

นอกจากนี้จะกล่าวถึงข้อจำกัดของตัวโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริงนี้ และปัญหา, อุปสรรค และการแก้ไขปัญหาที่พบเจอหรือเกิดขึ้น ตั้งแต่การสร้างตัวโปรแกรมจำลองข้อมูลทราฟฟิคจนกระทั่งการทดลอง

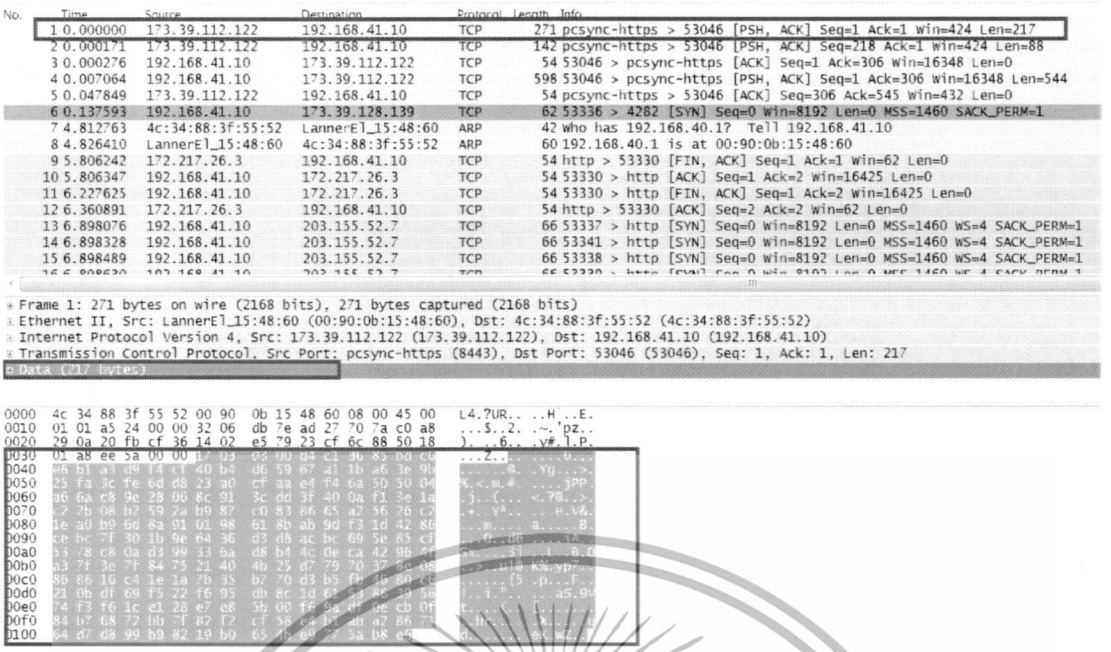
5.1 สรุปการทดลอง

จากผลการทดลองในบทที่ 4 ที่ทราบว่า นั้น ทำให้ได้ข้อมูลที่จะสามารถนำมา วิเคราะห์และสรุปผลเกี่ยวกับการใช้และประสิทธิภาพโปรแกรมซอคเกต ที่จำลองข้อมูลทราฟฟิคเสมือนจริง เพื่อมาทำการทดสอบการใช้งานของเซอร์วิสแบบต่างๆ บนระบบเครือข่ายที่สร้างใหม่ทั้งบนไอพีเวอร์ชั่น4 และไอพีเวอร์ชั่น6 จากการทดลองรับ-ส่งข้อมูลผ่านระบบเครือข่ายที่เป็นแบบข้ามเร้าเตอร์ตัวเดียว, แบบเครือข่ายแวนซ์ การใช้งานระหว่างองค์กร และแบบเครือข่ายแวนซ์ การใช้งานระหว่างองค์กร ซึ่งผลการทดลองพบว่าความถูกต้องของข้อมูลเมื่อเทียบกับ พีแคปไฟล์ที่เก็บข้อมูลทราฟฟิคจากระบบเครือข่ายไอพีเวอร์ชั่น4 เดิมนั้น 100%

จากรูปด้านล่างจะเป็นข้อมูลของพีแคปไฟล์ตั้งต้น ที่เราดักจับข้อมูลที่ใช้งานจริง จะเห็นว่าข้อมูลลำดับที่ 1 นั้น มีขนาดของข้อมูลอยู่ที่ 271 ไบต์ โดยข้อมูลสามารถดูได้จากตัวภาษาแบบเฮสกี้ (ASCII) ที่ปรากฏอยู่ในส่วนแสดงข้อมูลของโปรแกรมดักจับแพ็คเก็ตไวร์ชาร์ก

- รูปแรกจะแสดงข้อมูลของพีแคปไฟล์ตั้งต้น ที่มีการส่งข้อมูลทราฟฟิคเดียว
- รูปที่สองจะเป็นการแสดงข้อมูลของพีแคปไฟล์ตั้งต้น ที่ในการส่ง ส่งจาก 2 แพ็คเก็จออกไปเพียงแพ็คเก็ต เดียวแต่ได้ข้อมูลทราฟฟิคครอบคลุมทั้งหมด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



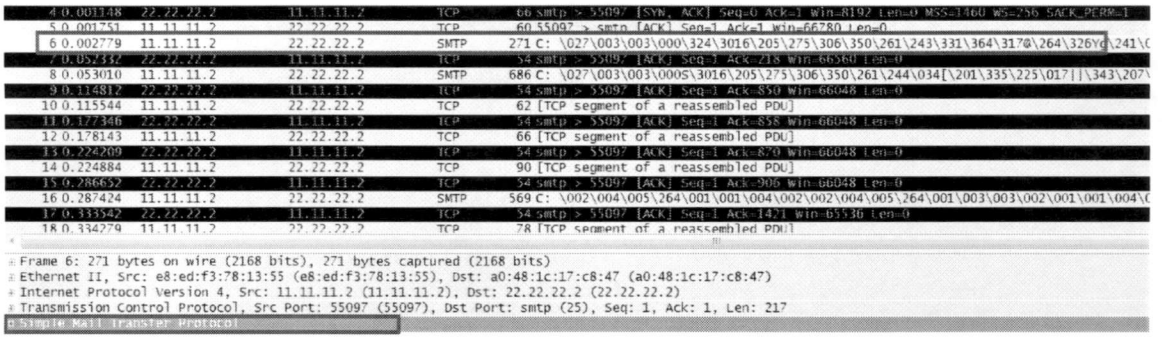
รูปที่ 5.1 รูปแสดงค่าข้อมูลพีแคปไฟล์ตั้งต้น_1

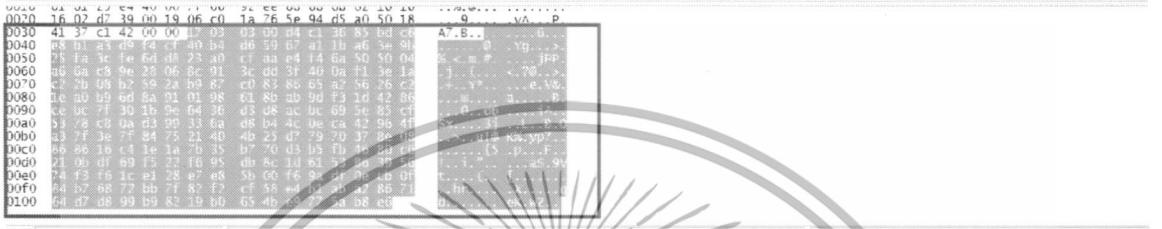
รูปที่ 5.2 รูปแสดงค่าข้อมูลพีแคปไฟล์ตั้งต้น_2

5.1.1 การรับส่ง-ข้อมูล ผ่านระบบเครือข่ายบนเร้าเตอร์ตัวเดียว

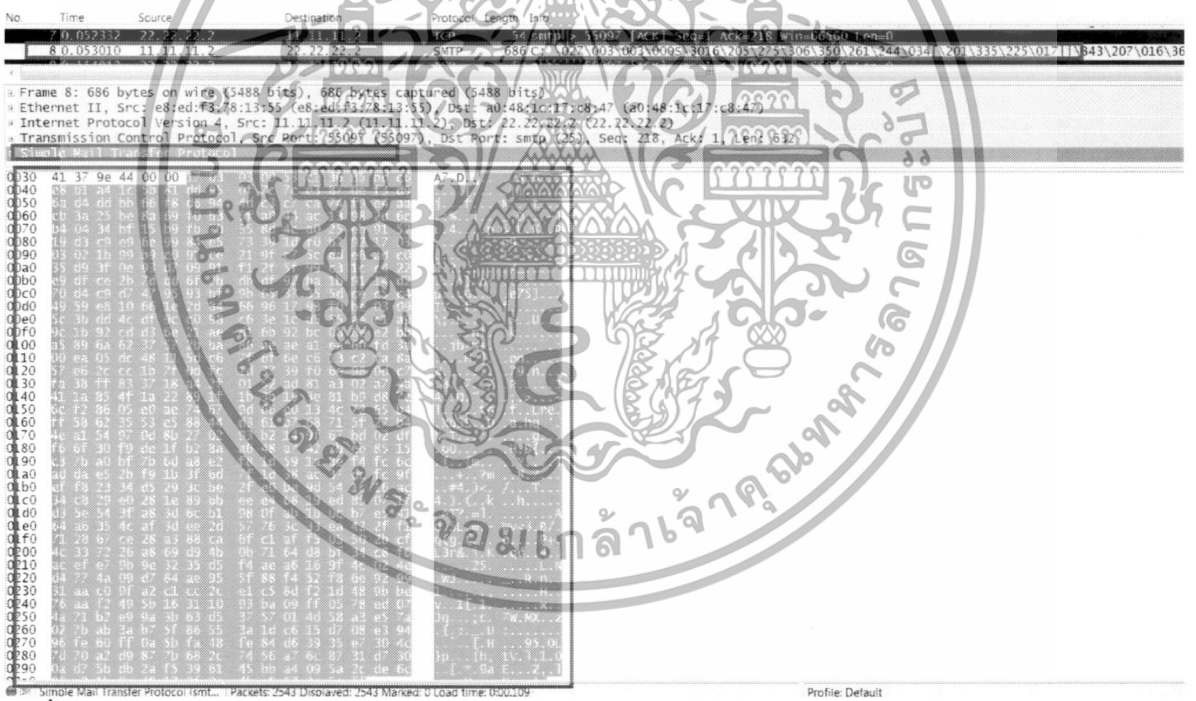
จากการบันทึกค่าการทดลองที่เราทดสอบโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง โดยการส่งข้อมูลจากพีแคปไฟล์ที่ดักจับบนระบบเครือข่ายเดิมมา แล้วจำลองเปลี่ยนโปรโตรคอลพอร์ทในการส่งในระบบเครือข่ายไอพีเวอร์ชั่น4 จากค่าจะแสดงให้เห็นว่า ข้อมูลทั้งหมดนั้น เทียบกันตามภาษาเฮสกี้แล้วพบว่า เหมือนกับส่วนของพีแคปไฟล์ตั้งต้น จึงทำให้สรุปได้ว่า โปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริงนั้น สามารถใช้งานทดแทน การที่เราจะต้องติดตั้งเซิร์ฟเวอร์ เพื่อลงเซอร์วิสการทำงานเหมือนของเดิม ซึ่งเป็นการเสียเวลาและเปลืองต้นทุน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้





รูปที่ 5.3 รูปแสดงค่าข้อมูลพีแคปไฟล์จากการทดลองเครือข่ายเร้าเตอร์ตัวเดียวแบบไอพีเวอร์ชั่น4_1

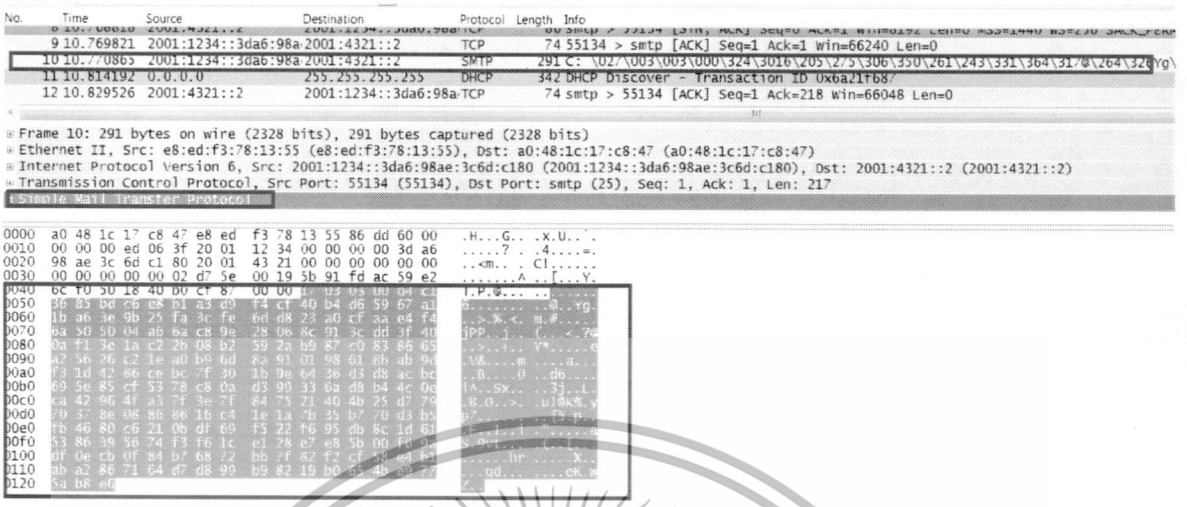


รูปที่ 5.4 รูปแสดงค่าข้อมูลพีแคปไฟล์จากการทดลองเครือข่ายเร้าเตอร์ตัวเดียวแบบไอพีเวอร์ชั่น4_2

ส่วนถัดมาคือบันทึกค่าการทดลองที่เราทดสอบโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง โดยการส่งข้อมูลจากพีแคปไฟล์ที่ดักจับบนระบบเครือข่ายเดิมมา แล้วจำลองเปลี่ยนโปรโตรคอล พอร์ทในการส่งในระบบเครือข่ายไอพีเวอร์ชั่น6 จากค่าจะแสดงให้เห็นว่า ข้อมูลทั้งหมดนั้น จากการเทียบภาษาเฮสกี้แล้วพบว่า เหมือนกับส่วนของพีแคปไฟล์ตั้งต้น จึงทำให้สรุปได้ว่า โปรแกรม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จำลองข้อมูลทราฟฟิคเสมือนจริงนั้น สามารถใช้งานทดแทน การที่เราจะต้องติดตั้งเซิร์ฟเวอร์ เพื่อลงเซอร์วิสการทำงานเหมือนของเดิม ซึ่งเป็นการเสียเวลาและเปลืองต้นทุน



รูปที่ 5.5 รูปแสดงค่าข้อมูลพีแคปไฟล์จากการทดลองเครือข่ายเร้าเตอร์ตัวเดียวแบบไอพีเวอร์ชั่น6_1

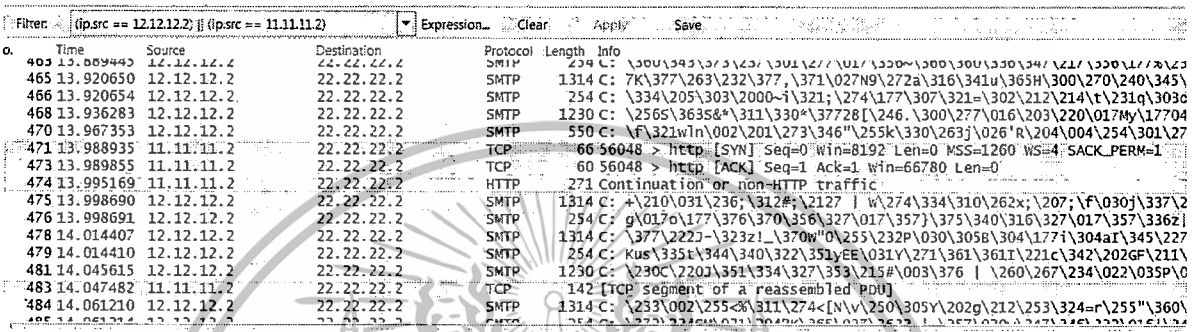
รูปที่ 5.6 รูปแสดงค่าข้อมูลพีแคปไฟล์จากการทดลองเครือข่ายเร้าเตอร์ตัวเดียวแบบไอพีเวอร์ชั่น6_2

จากการทดลองโดยใช้โปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง ส่งข้อมูลทราฟฟิคการระบบเครือข่ายที่เป็นแบบเร้าท์เตอร์ตัวเดียวนั้น ทั้งแบบไอพีเวอร์ชั่น4 และไอพีเวอร์ชั่น6 จะแสดงให้เห็นว่า โปรแกรมดังกล่าว สามารถใช้งานได้จริง สามารถส่งข้อมูลทราฟฟิคที่ดักเก็บมาจากระบบเครือข่ายเดิมได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.1.2 การรับส่ง-ข้อมูล ผ่านระบบเครือข่าย แบบการใช้งานภายในองค์กร

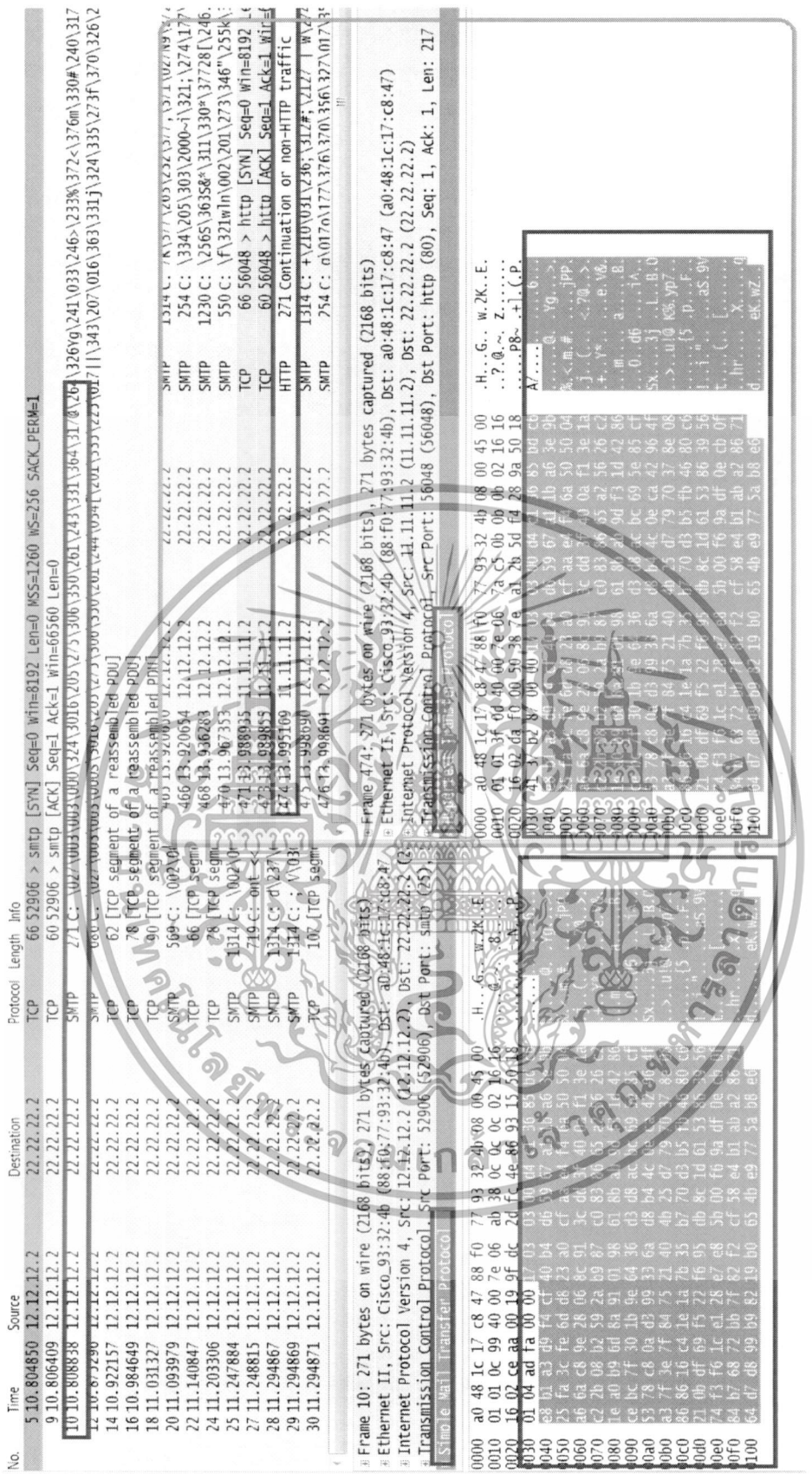
จากการบันทึกค่าการทดลองที่เราทดสอบโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง โดยการส่งข้อมูลจากพีแคปไฟล์ที่ดักจับบนระบบเครือข่ายเดิมมา แล้วจำลองเปลี่ยนโปรโตรคอลพอร์ทในการส่งในระบบเครือข่ายไอพีเวอร์ชั่น4 โดยมีเครื่องคอมพิวเตอร์ที่ทำหน้าที่ส่งจำนวน 2 เครื่อง และมีเครื่องคอมพิวเตอร์ทำหน้าที่รับ 1 เครื่อง โดยถ้าดูจากพีแคปไฟล์ที่เราดักจับแพ็คเก็ตไว้ก็จะเห็นว่ามีข้อมูลทราฟฟิคส่งมากจากทั้งเครื่องหมายเลขไอพีแอสเดรส 11.11.11.2 และ 12.12.12.2 จริง



รูปที่ 5.7 รูปแสดงค่าข้อมูลที่ดักจับเมื่อ2โคลเอนต์ส่งมาเซิร์ฟเวอร์พร้อมกันแบบไอพีเวอร์ชั่น4

ต่อเนื่องกันมา เมื่อวิเคราะห์ข้อมูลที่ดักจับได้นั้น เทียบกันตามภาษาเฮสกี้แล้วพบว่าข้อมูลทราฟฟิคที่ฝั่งส่งทั้ง 2 ส่งมาให้เซิร์ฟเวอร์นั้น ได้ข้อมูลทราฟฟิคเหมือนกับส่วนของพีแคปไฟล์ตั้งต้น จึงทำให้สรุปได้ว่า โปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริงนั้น สามารถใช้งานทดแทน การที่เราจะต้องติดตั้งเซิร์ฟเวอร์ เพื่อลงเซอร์วิสการทำงานเหมือนของเดิม ซึ่งเป็นการเสียเวลาและเปลืองต้นทุน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.8 รูปแสดงค่าข้อมูลพีแคปไฟล์จากการทดลองเครือข่ายในองค์กรแบบไอพีเวอร์ชั่น4

ส่วนถัดมาคือบันทึกค่าการทดลองที่เราทดสอบโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง

โดยการส่งข้อมูลจากพีแคปไฟล์ที่ดักจับบนระบบเครือข่ายเดิมมา แล้วจำลองเปลี่ยนโปรโตรคอล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

พอร์ทในการส่งในระบบเครือข่ายไอพีเวอร์ชั่น6 โดยมีเครื่องคอมพิวเตอร์ที่ทำหน้าที่ส่งจำนวน 2 เครื่อง และมีเครื่องคอมพิวเตอร์ทำหน้าที่รับ 1 เครื่อง โดยถ้าดูจากพีแคปไฟล์ที่เราดักจับแพ็คเก็ตไว้ก็จะเห็นว่ามีข้อมูลทราฟฟิคส่งมากจากทั้งเครื่องหมายเลขไอพีแอสเดรส 2001:1234::2/64 และ 2002:1234::2/64 จริง

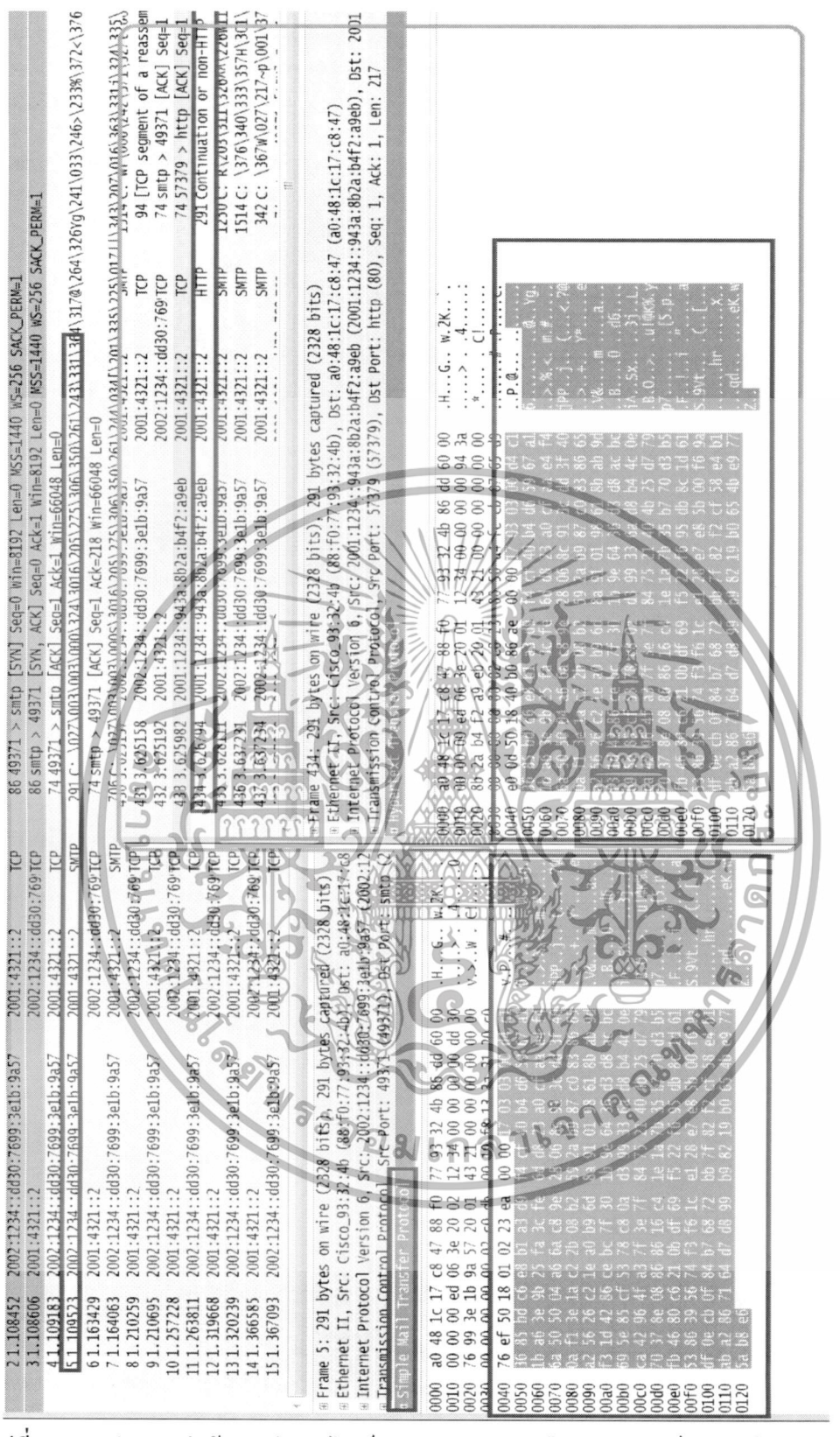
No.	Time	Source	Destination	Protocol	Length	Info
596	4.045022	2001:4321::2	2002:1234::dd30:769	TCP	74	smtp > 49371 [ACK] Seq=1 Ack=290306 Win=66048 Len=0
597	4.068432	2001:1234::943a:8b2a:b4f2:a9eb	2001:4321::2	HTTP	1514	Continuation or non-HTTP traffic
598	4.068433	2001:1234::943a:8b2a:b4f2:a9eb	2001:4321::2	HTTP	559	Continuation or non-HTTP traffic
599	4.068525	2001:4321::2	2001:1234::943a:8b2	TCP	74	http > 57379 [ACK] Seq=1 Ack=3394 Win=66048 Len=0
600	4.076204	2002:1234::dd30:7699:3e1b:9a57	2001:4321::2	SMTP	1514	C: ik)f\373\216\265\263p\032a\301q\316\314q\326s\234\20
601	4.076209	2002:1234::dd30:7699:3e1b:9a57	2001:4321::2	TCP	94	[TCP segment of a reassembled PDU]
602	4.076285	2001:4321::2	2002:1234::dd30:769	TCP	74	smtp > 49371 [ACK] Seq=1 Ack=291766 Win=66048 Len=0
603	4.091853	2002:1234::dd30:7699:3e1b:9a57	2001:4321::2	SMTP	1514	C: O\343\316\267"\260\372}u\370\225\v\366\363\310\345\3
604	4.091855	2002:1234::dd30:7699:3e1b:9a57	2001:4321::2	TCP	94	[TCP segment of a reassembled PDU]
605	4.091906	2001:4321::2	2002:1234::dd30:769	TCP	74	smtp > 49371 [ACK] Seq=1 Ack=293226 Win=66048 Len=0
606	4.099490	2001:1234::943a:8b2a:b4f2:a9eb	2001:4321::2	HTTP	1199	Continuation or non-HTTP traffic
607	4.115147	2001:1234::943a:8b2a:b4f2:a9eb	2001:4321::2	HTTP	1514	Continuation or non-HTTP traffic
608	4.115148	2001:1234::943a:8b2a:b4f2:a9eb	2001:4321::2	TCP	82	[TCP segment of a reassembled PDU]
609	4.115197	2001:4321::2	2001:1234::943a:8b2	TCP	74	http > 57379 [ACK] Seq=1 Ack=5967 Win=66048 Len=0

รูปที่ 5.9 รูปแสดงค่าข้อมูลที่ดักจับเมื่อ2ไคลเอนต์ส่งมาเซิร์ฟเวอร์พร้อมกันแบบไอพีเวอร์ชั่น6

ต่อเนื่องกันมา เมื่อวิเคราะห์ข้อมูลที่ดักจับได้นั้น เทียบกันตามภาษาเฮสกี้แล้วพบว่าข้อมูลทราฟฟิคที่ฝั่งส่งทั้ง 2 ส่งมาให้เซิร์ฟเวอร์นั้น ได้ข้อมูลทราฟฟิคเหมือนกับส่วนของพีแคปไฟล์ตั้งต้น จึงทำให้สรุปได้ว่า โปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริงนั้น สามารถใช้งานทดแทน การที่เราจะต้องติดตั้งเซิร์ฟเวอร์ เพื่อลงเซอร์วิสการทำงานเหมือนของเดิม ซึ่งเป็นการเสียเวลาและเปลืองต้นทุน

โดยรูปที่ 5.10 ที่เป็นผลจากการทดลองโดยใช้โปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริงส่งข้อมูลทราฟฟิคการระบบเครือข่ายที่เป็นแบบแลนซ์ ที่ใช้งานเครือข่ายภายในองค์กร ทั้งแบบไอพีเวอร์ชั่น4 และไอพีเวอร์ชั่น6 จะแสดงให้เห็นว่า โปรแกรมดังกล่าว สามารถใช้งานได้จริง สามารถส่งข้อมูลทราฟฟิคที่ดักเก็บมาจากระบบเครือข่ายเดิมได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.10 รูปแสดงค่าข้อมูลพีแคปไฟล์จากการทดลองเครือข่ายในองค์กรแบบไอพีเวอร์ชั่น6

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.1.3 การรับส่ง-ข้อมูล ผ่านระบบเครือข่าย แบบการใช้งานระหว่างองค์กร

จากการบันทึกค่าการทดลองที่เราทดสอบโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง โดยการส่งข้อมูลจากพีแคปไฟล์ที่ดักจับบนระบบเครือข่ายเดิมมา แล้วจำลองเปลี่ยนโปรโตรคอลพอร์ทในการส่งในระบบเครือข่ายไอพีเวอร์ชั่น4 โดยมีเครื่องคอมพิวเตอร์ที่ทำหน้าที่ส่งจำนวน 2 เครื่อง และมีเครื่องคอมพิวเตอร์ทำหน้าที่รับ 1 เครื่อง โดยถ้าดูจากพีแคปไฟล์ที่เราดักจับแพ็คเก็ตไว้ก็จะเห็นว่ามีข้อมูลทราฟฟิคส่งมากจากทั้งเครื่องหมายเลขไอพีแอสเดรส 11.11.11.2 และ 12.12.12.2 จริง และจากข้อมูลทราฟฟิคที่ดักจับได้ ก็นำมาวิเคราะห์ข้อมูล เทียบกันตามภาษาเฮสกี้แล้วพบว่า ข้อมูลทราฟฟิคที่ฝั่งส่งทั้ง 2 ส่งมาให้เซิร์ฟเวอร์นั้น ได้ข้อมูลทราฟฟิคเหมือนกับส่วนของพีแคปไฟล์ตั้งต้น จึงทำให้สรุปได้ว่า โปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริงนั้น สามารถใช้งานได้อย่างมีประสิทธิภาพ

ส่วนถัดมาคือบันทึกค่าการทดลองที่เราทดสอบโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง โดยการส่งข้อมูลจากพีแคปไฟล์ที่ดักจับบนระบบเครือข่ายเดิมมา แล้วจำลองเปลี่ยนโปรโตรคอลพอร์ทในการส่งในระบบเครือข่ายไอพีเวอร์ชั่น6 โดยมีเครื่องคอมพิวเตอร์ที่ทำหน้าที่ส่งจำนวน 2 เครื่อง และมีเครื่องคอมพิวเตอร์ทำหน้าที่รับ 1 เครื่อง โดยถ้าดูจากพีแคปไฟล์ที่เราดักจับแพ็คเก็ตไว้ก็จะเห็นว่ามีข้อมูลทราฟฟิคส่งมากจากทั้งเครื่องหมายเลขไอพีแอสเดรส 2001:1234::2/64 และ 2002:1234::2/64 โดยเมื่อวิเคราะห์ข้อมูลทราฟฟิคที่ดักจับได้นั้น เทียบกันตามภาษาเฮสกี้แล้วพบว่าข้อมูลทราฟฟิคที่ฝั่งส่งทั้ง 2 ส่งมาให้เซิร์ฟเวอร์นั้น ได้ข้อมูลทราฟฟิคเหมือนกับส่วนของพีแคปไฟล์ตั้งต้น จึงทำให้สรุปได้ว่า โปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริงนั้นสามารถใช้งานได้จริง

จากการทดลองโดยใช้โปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง ส่งข้อมูลทราฟฟิคการระบบเครือข่ายที่เป็นแบบแลนซ์ ที่ใช้งานเครือข่ายภายในองค์กร ทั้งแบบไอพีเวอร์ชั่น4 และไอพีเวอร์ชั่น6 จะแสดงให้เห็นว่า โปรแกรมดังกล่าว สามารถใช้งานได้จริง สามารถส่งข้อมูลทราฟฟิคที่ดักเก็บมาจากระบบเครือข่ายเดิมได้

5.2 ปัญหาและอุปสรรค

นอกจากข้อสรุปการทำงานของโปรแกรมจำลองทราฟฟิคเสมือนจริง ที่พบว่าทำงานได้มีประสิทธิภาพ ไม่จำเป็นต้องไปตั้งเซิร์ฟเวอร์หลายๆตัวมาทำการทดสอบ หรือไม่ต้องไปโยกผู้ใช้งานจริงเพื่อมาทดสอบระบบเครือข่ายใหม่แล้วนั้น ยังจะกล่าวถึงข้อจำกัดของตัวโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริงนี้ และปัญหา, อุปสรรค และการแก้ไขปัญหา ที่พบเจอ หรือเกิดขึ้น ตั้งแต่การสร้างตัวโปรแกรมจำลองข้อมูลทราฟฟิคจนกระทั่งการทดลอง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ปัญหาและอุปสรรคด้านระบบเครือข่ายไอพีเวอร์ชั่น 6

ปัญหาที่สำคัญของการสร้างเครือข่ายไอพีเวอร์ชั่น6 นั้น ส่วนใหญ่จะเกิดขึ้นเนื่องจากความไม่ชำนาญการในการสร้างระบบ (configuration) หรือความไม่เข้าใจความหมายของคำสั่ง ที่จะต้องใส่ลงไปบนอุปกรณ์ระบบเครือข่าย เช่น เร้าเตอร์ เป็นต้น เนื่องจากระบบเครือข่ายไอพีเวอร์ชั่น6 นั้น ค่อนข้างเป็นเทคโนโลยีที่ใหม่ และระบบการแสดงตัวหมายเลขแอสเดรส แตกต่างจากไอพีเวอร์ชั่นปัจจุบันอย่างสิ้นเชิง

โดยปัญหา และอุปสรรคที่เจอนั้นสามารถแก้ไขได้โดยการศึกษาค้นคว้า จากไฟล์ดาต้าชีทของบริษัทซิสโก้ ที่มีการอธิบายคำสั่งต่างๆ และกระบวนการขั้นตอนต่างๆ ในการที่จะสร้างระบบเครือข่ายไอพีเวอร์ชั่น 6 ขึ้นมา รวมถึงมีคำสั่งที่จะสามารถนำมาใช้แก้ไขปัญหาเบื้องต้น

ปัญหาและอุปสรรคด้านโปรแกรมจับข้อมูลไวร์ชาร์ก

ปัญหาที่สำคัญของโปรแกรมไวร์ชาร์กนั้น คือการติดตั้งโปรแกรม เนื่องจากมีการติดตั้งโปรแกรมไวร์ชาร์กที่ไม่ได้เป็นเวอร์ชั่นล่าสุด บนคอมพิวเตอร์ที่ใช้ในการทดลองซึ่งเป็นระบบปฏิบัติการที่เป็น 64 บิต ทำให้เวลาเปิดใช้งานครั้งที่ 2 มีปัญหา โดยปัญหาที่เกิด ตัวโปรแกรมไม่สามารถที่จะเลือกอินเทอร์เฟส ที่จะต้องการใช้ดักจับแพคเก็ตได้

โดยปัญหา และอุปสรรคที่เจอนั้นสามารถแก้ไขได้โดยการลงโปรแกรมไวร์ชาร์กเวอร์ชั่นใหม่ ที่ทางบริษัทของโปรแกรมได้ทำการแก้ไขปัญหานี้แล้ว

ปัญหาและอุปสรรคด้านการสร้างโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง

ปัญหาที่สำคัญของการทำซอคเกตโปรแกรมมิ่ง โดยโปรแกรมซีชาร์ปนั้นต้องใช้เวลาในการศึกษาทำความเข้าใจ พร้อมทั้งหาบุคคลผู้มีความเชี่ยวชาญด้านการใช้งานภาษาซีชาร์ปเข้ามาช่วย รวมถึงข้อจำกัดด้านต่างๆ ของระบบปฏิบัติการวินโวส์ ที่ส่งผลต่อการทำซอคเกตโปรแกรมมิ่ง

โดยปัญหา และอุปสรรคที่เจอนั้นสามารถแก้ไขได้โดยการปรึกษา และขอความช่วยเหลือจากผู้เชี่ยวชาญด้านโปรแกรมมิ่ง ส่วนในข้อจำกัดของระบบปฏิบัติการวินโดวส์ที่อาจจะส่งผลกระทบของโปรแกรมที่สร้าง ส่วนนี้ได้ศึกษาแล้วว่า อาจจะไม่ส่งผลมากหนักต่อตัวโปรแกรม อาทิ เช่น ระบบปฏิบัติการวินโดวส์ไม่สามารถให้ระบุค่าของโปรโตรคอลพอร์ทต้นทางได้ เนื่องจากเป็นด้านความปลอดภัยของระบบ ซึ่งส่วนนี้ทำให้ตัวโปรแกรมไม่สามารถควบคุมค่าการส่งของโปรโตรคอลพอร์ทต้นทางได้

ปัญหาและอุปสรรคด้านโปรแกรมเอกซ์เอ็มแอล

ปัญหาที่สำคัญของการเขียนเอ็กซ์เอ็มแอลไฟล์ คือจะทำอย่างไรให้ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปเขียนเพื่อทดสอบระบบเครือข่ายเองได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โดยปัญหา และอุปสรรคที่เจอนั้น อาจจะมองว่าเป็นส่วนเสริมการทำงานของตัวโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง เลยได้ทำการพัฒนาโปรแกรมให้สามารถกรอก ข้อมูลต่างๆใส่ได้โดยไม่ต้องพึ่งพาเอ็กซ์เอ็มแอลไฟล์ ส่วนเอ็กซ์เอ็มแอลไฟล์ ก็ได้สร้างรูปแบบการเขียนที่เข้าใจง่ายเพื่อที่ผู้ใช้งาน สามารถเข้าใจและนำไปปรับปรุงให้เขากับระบบที่ต้องการทดสอบได้

<u>ปัญหาและอุปสรรคด้านการติดตั้งระบบเครือข่ายบนอุปกรณ์จริง</u>

ส่วนนี้เป็นจุดหลัก จุดสำคัญของโครงการนี้ ปัญหาส่วนใหญ่คือเรื่องทรัพยากร ซึ่งอุปกรณ์เน็ตเวิร์กที่มีอยู่บางรุ่นไม่สามารถอัพเดทซอฟแวร์ เพื่อให้สนับสนุนการทำงานระบบเครือข่ายไอพีแอสเดรสเวอร์ชั่น6 ได้ หรืออุปกรณ์บางรุ่นที่จะนำมาทดสอบเป็นอุปกรณ์ที่ตกรุ่นแล้วไม่เป็นที่นิยมในระบบเครือข่ายแล้ว

โดยปัญหา และอุปสรรคที่เจอนั้น ได้ทำการแก้ไขโดยเปลี่ยนอุปกรณ์เน็ตเวิร์กมาใช้รุ่น ASR1001 และ ME3600 เพื่อให้เหมาะสมกับองค์กรต่างๆในประเทศไทยที่นิยมใช้อุปกรณ์รุ่นนี้ในระบบเครือข่าย

5.3 ข้อจำกัดของโปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริง

1. โปรแกรมจำลองข้อมูลทราฟฟิคเสมือนจริงที่พัฒนาขึ้นนี้จะเน้นไปในส่วนของเลเยอร์ 3(Network layer)และเลเยอร์4(Transport layer) เท่านั้น เช่นเดียวกับโปรแกรมโอเพ่นซอร์สทั่วไป.
2. ความเร็วในการส่งข้อมูลทราฟฟิคของโปรแกรมที่พัฒนาขึ้นอยู่กับฮาร์ดแวร์ และระบบปฏิบัติการของคอมพิวเตอร์ที่ใช้งาน
6. การทดลองนี้ไม่รวมถึง การทดสอบข้อมูลทราฟฟิค ที่เป็นพวก SSL VPN เนื่องจาก การทำงานของ SSL VPN เป็นส่วนของแอพพลิเคชั่น และเป็นการใช้งานด้วยการเข้ามาจากข้างนอก (remote)
7. การทดลองนี้ไม่รวมถึง การทดสอบข้อมูลทราฟฟิค ที่เป็นพวกของ PS/CS core network ซึ่งมีโปรโตรคอลที่ซับซ้อนกว่า ในเรื่องของการแปลงหมายเลขโทรศัพท์ ให้เป็น หมายเลขไอพีแอสเดรส

5.4 การเปรียบเทียบกับโปรแกรมที่อยู่

กล่าวถึงการเปรียบเทียบของโปรแกรมจำลองทราฟฟิคที่มีอยู่ในปัจจุบัน โปรแกรมที่นำมาเปรียบเทียบด้วยนั้น ประกอบไปด้วย โปรแกรม TCP replay, โปรแกรม Ostinato, โปรแกรม iPerf

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

และ โปรแกรม CapTipper. ฟีเจอร์การทำงานที่นำมาเปรียบเทียบกับโปรแกรมต้นแบบที่พัฒนานั้น จะประกอบไปด้วย

1. การเป็นโปรแกรมแบบโอเพ่นซอร์ส (open-source software) : จากการทดสอบและศึกษาทุกโปรแกรมที่นำมาเปรียบเทียบ เป็นโปรแกรมแบบโอเพ่นซอร์ส

2. โปรแกรมสนับสนุนการทำงานรูปแบบ GUI : จากการทดสอบและศึกษา พบว่าโปรแกรม TCP replay และโปรแกรม CapTipper ทำงานในรูปแบบคอมมานด์ไลน์ (command line) ไม่มีการใช้หน้า GUI ในการใช้งานโปรแกรม

3. โปรแกรมสามารถใช้งานได้บนหลายๆรูปแบบระบบปฏิบัติการคอมพิวเตอร์ : จากโปรแกรมที่เราพัฒนานั้น ถ้าจะให้ทำงานกับระบบปฏิบัติการที่เป็นพวกลีนุกซ์ต้องมีการแก้ไขโค้ดในตัวโปรแกรม ซึ่งตรงนี้เป็นข้อจำกัดของโปรแกรมที่พัฒนาอยู่แล้ว และยังพบว่าโปรแกรม TCP replay และโปรแกรม CapTipper รองรับแต่ระบบปฏิบัติการวินโดวส์

4. โปรแกรมสามารถรองรับการทำงานของไอพีเวอร์ชั่น 4 และเวอร์ชั่น 6 : จากการทดสอบและศึกษา ทุกโปรแกรมที่นำมาเปรียบเทียบในปี 2016 รองรับการทำงานแบบไอพีเอวร์ชั่น 6 เกือบทุกโปรแกรมยกเว้นโปรแกรม CapTipper แต่ถ้าเทียบในปี 2015 ที่เริ่มพัฒนาโปรแกรมต้นแบบนี้ โปรแกรมเทียบทั้ง iPerf, CapTipper นั้น ไม่รองรับการทำงานแบบไอพีเวอร์ชั่น 6.

5. โปรแกรมสามารถรองรับการทำงานของโปรโตรคอลแบบ TCP และ UDP : จากการทดสอบและศึกษา เกือบทุกโปรแกรมรองรับการทำงานทั้ง TCP และ UDP ยกเว้นโปรแกรม CapTipper

6. โปรแกรมสามารถรองรับการทำงานของหลากหลายโปรโตรคอลที่เป็นมาตรฐานสากล : จากการทดสอบและศึกษา มีเพียงโปรแกรม CapTipper ที่รองรับการทำงานเฉพาะโปรโตรคอล HTTP เท่านั้น

7. ในการใช้งานสามารถจำลองได้หลายๆเซิร์ฟเวอร์ และหลายๆไคลเอนต์ : จากการทดสอบและศึกษา มีเพียงโปรแกรมต้นแบบ กับโปรแกรม iPerf (2016) เท่านั้นที่สามารถจำลองได้หลายๆเซิร์ฟเวอร์ และหลายๆไคลเอนต์ ในขณะที่ iperf(2015) ที่เริ่มพัฒนาโปรแกรมต้นแบบนี้ โปรแกรม iPerf ยกไม่รองรับการทำงานแบบนี้

8. โปรแกรมมีฟีเจอร์ดักจับแพคเก็ตในตัวหรือไม่ : จากการทดสอบและศึกษา มีเพียงโปรแกรม Ostinato เท่านั้นที่มีฟีเจอร์นี้ แต่ก็เป็นเพียงการที่โปรแกรมนี้ไปเรียกใช้งานโปรแกรมไวร์ชาร์กเท่านั้น ไม่ได้มีฟีเจอร์ถูกสรางขึ้นมาในโปรแกรมเอง

9. โปรแกรมสามารถทำการ replay pcap file ได้หรือไม่ : จากการทดสอบและศึกษา มีเพียงโปรแกรม iPerf(2015,2016) ที่ไม่รองรับการทำงานนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 5.1 แสดงผลการเปรียบเทียบระหว่างโปรแกรมที่พัฒนากับโปรแกรมที่มีอยู่

Feature	โปรแกรมเทียบ				
	Project program	Tcpreplay	Ostinato	iPerf	CapTipper
1. Open-Source Software	Y	Y	Y	Y	Y
2. GUI supported	Y	N	Y	Y	N
3. Cross-platfrom	N	N	Y	Y	N
4. Support both IPv4 and IPv6	Y	Y	Y	Y	N
5. Support both TCP and UCP	Y	N	Y	Y	N
6. Support for the most common standard protocols	Y	Y	Y	Y	N
7. Client and server can have multiple simultaneous connections	Y	N	N	Y	N
8. Capture network traffic	N	N	Y	N	N
9. Replay pcap traffic	Y	Y	Y	N	Y

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.5 สรุป

โปรแกรมจำลองข้อมูลทราฟฟิคเสมือจริงที่พัฒนาขึ้น สามารถช่วยลดค่าใช้จ่ายทุนขององค์กร (Capital Expenditure)และเพิ่มรายรับขององค์กร(Revenue & Income) เมื่อองค์กรต้องลงทุนเปลี่ยนเป็นระบบเครือข่ายเดิม ให้เป็นระบบเครือข่ายใหม่ทั้งบนไอพีเวอร์ชั่น4 หรือ ไอพีเวอร์ชั่น6 เพื่อให้บริการลูกค้า โดยสามารถช่วยลดความยุ่งยาก การจัดหาจัดเตรียม และขั้นตอนในการทดสอบระบบเครือข่ายใหม่ได้ ซึ่งจากผลการทดลองนั้นสามารถยืนยันได้เป็นอย่างดีว่าประสิทธิภาพของโปรแกรมที่พัฒนาขึ้นมานั้น สามารถจำลองข้อมูลทราฟฟิคเสมือนจริง เพื่อมาทำการทดสอบการใช้งานของเซอร์วิสแบบต่างๆ บนระบบเครือข่ายที่สร้างใหม่ทั้งบนไอพีเวอร์ชั่น4 และไอพีเวอร์ชั่น6 จากการทดลองรับ-ส่งข้อมูลผ่านระบบเครือข่ายที่เป็นแบบข้ามเร้าเตอร์ตัวเดียว, แบบเครือข่ายแวนซ์ การใช้งานระหว่างองค์กร และแบบเครือข่ายแวนซ์ การใช้งานระหว่างองค์กร ซึ่งผลการทดลองพบว่าความถูกต้องของข้อมูลเมื่อเทียบกับ พีแคปไฟล์ที่เก็บข้อมูลทราฟฟิคจากระบบเครือข่ายไอพีเวอร์ชั่น4 เดิมนั้น 100%

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ประวัติผู้เขียน

ชื่อผู้เขียน	ชวนาท นิพัทธมานนท์
วันเกิด	16 มิถุนายน 2530
สถานที่เกิด	กรุงเทพมหานคร
วุฒิการศึกษาระดับปริญญาตรี	วิศวกรรมศาสตร์บัณฑิต (สารสนเทศ) คณะวิศวกรรมศาสตร์
สถานที่สำเร็จการศึกษา	สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหาร ลาดกระบัง
ปีการศึกษาที่สำเร็จการศึกษา	2551
การทำงาน	วิศวกรผู้ประสานงานลูกค้า (High Touch Engineer) แผนกงานดูแลด้านเทคโนโลยี (Focused Technical Support) บริษัท ซิสโก้ ซีสเต็มส์ (ประเทศไทย) จำกัด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Microsoft. **Developer Network.** [Online] เข้าถึงได้จาก:https://msdn.microsoft.com/en-us/library/4as0wz7t(v=vs.110).aspx (วันที่สืบค้น : 14 มกราคม 2559)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้