

สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

การจัดการโครงข่ายประสิทธิภาพสูงสำหรับกลุ่มวิจัยแบบไร้สาย

**THE EFFICIENCY NETWORK MANAGEMENT**

**FOR WIRELESS COMMUNICATION RESEARCH GROUP**



โดย

นางสาว พรพิมล จินุพันธ์

นางสาว พิมพ์ลักษณ์ กลิ่นมาลี

ม.พ.  
พ 249 ก  
2548

เลขหมู่.....

62673

เลขทะเบียน.....

วัน,เดือน,ปี... 21 ส.ค. 2549

b.....
i.....

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2548

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

**THE EFFICIENCY NETWORK MANAGEMENT  
FOR WIRELESS COMMUNICATION RESEARCH GROUP**



**A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF  
THE REQUIREMENT FOR THE DEGREE OF  
BACHELOR IN DEPARTMENT OF INFORMATION ENGINEERING  
FACULTY OF ENGINEERING  
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG**

**2005**

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อปริญญานิพนธ์ การจัดการ โครงข่ายประสิทธิภาพสูงสำหรับกลุ่มวิจัย  
แบบไร้สาย

ชื่อนักศึกษา นางสาวพรพิมล จินุพันธ์ รหัสนักศึกษา 45010504  
นางสาวพิมพ์ลักษณ์ กลิ่นมาลี รหัสนักศึกษา 45010540

อาจารย์ที่ปรึกษา อาจารย์สถาพร พรหมวงศ์  
ผศ.พิชฌุ สุพรรณกุล

ระดับการศึกษา ปริญญาตรี วิศวกรรมบัณฑิต  
สาขาวิศวกรรมสารสนเทศ

ภาควิชา วิศวกรรมสารสนเทศ

ปีการศึกษา 2548

---

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง  
อนุมัติให้รับปริญญานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร  
วิศวกรรมศาสตรบัณฑิต



(อาจารย์สถาพร พรหมวงศ์)  
อาจารย์ผู้ควบคุมปริญญานิพนธ์



(ผศ.พิชฌุ สุพรรณกุล)  
อาจารย์ผู้ควบคุมปริญญานิพนธ์

<b>หัวข้อปริญญานิพนธ์</b>	การจัดการ โครงข่ายประสิทธิภาพสูงสำหรับกลุ่มวิจัยแบบไร้สาย	
<b>ชื่อนักศึกษา</b>	นางสาวพรพิมล จินุพันธ์	รหัสประจำตัว 45010504
	นางสาวพิมพ์ลักษณ์ กลิ่นมาลี	รหัสประจำตัว 45010540
<b>อาจารย์ที่ปรึกษา</b>	อาจารย์สถาพร พรหมวงค์	
	ผศ. พิชญ สุพรรณกุล	
<b>ระดับการศึกษา</b>	ปริญญาตรีวิศวกรรมศาสตรบัณฑิต	
	สาขาวิศวกรรมสารสนเทศ	
<b>ภาควิชา</b>	วิศวกรรมสารสนเทศ	
<b>ปีการศึกษา</b>	2548	

### บทคัดย่อ

โครงการนี้ได้ทำการศึกษาและวางระบบ โครงข่ายที่มีประสิทธิภาพสำหรับกลุ่มวิจัยแบบสื่อสารไร้สาย วัตถุประสงค์ของโครงการนี้คือเพื่อออกแบบและจัดการ โครงข่ายให้มีประสิทธิภาพ เสถียรภาพ และความปลอดภัยต่อข้อมูลระดับสูง ได้มีการออกแบบและติดตั้ง ไฟร์วอลล์ (Firewall) DNS เซิร์ฟเวอร์ (DNS Server) เว็บบอร์ด (Web Board) และเซิร์ฟเวอร์ข้อมูลกลาง (FileServer) ไฟร์วอลล์ ใช้สำหรับป้องกันผู้บุกรุก DNS เซิร์ฟเวอร์ ใช้สำหรับสร้างโดเมนลูก (Child Domain) รวมทั้งยังได้ออกแบบ โฮมเพจ (Home Page) และเว็บบอร์ด (Web Board) สำหรับบริการและแลกเปลี่ยนข้อมูลไว้ในเว็บเซิร์ฟเวอร์ เซิร์ฟเวอร์ฐานข้อมูลกลางใช้สำหรับเก็บข้อมูลวิจัยในกลุ่มวิจัยการสื่อสารไร้สาย

**Thesis Title** The Efficiency Network Management For Wireless Communication  
Research Group

**Student** Miss Pornpimol Jinupun ID.45010504  
Miss Pimluck Klinmalee ID.45010540

**Advisor** Mr. Sathaporn Promwong  
Asst.Prof. Pitchaya Supanakoon

**Graduate Level** Bachelor Degree of Information Engineering

**Department** Information Engineering

**Academic Year** 2005

### Abstract

In this project, the efficiency network management for wireless communication research group is studied and managed. The purpose is to design and manage the network which is high efficiency, stable and security. The firewall, DNS, web and central database servers are designed and setup. The firewall is used for protecting the hackers. The DNS server is used for making the child domain. The home page and web board are design for servicing and exchanging acknowledge in the web server. The central database server is used for storing the research database inside the wireless communication research group.

## กิตติกรรมประกาศ

ปริญญาบัตรฉบับนี้มีอาจสำเร็จลุล่วงไปได้ หากขาดความช่วยเหลือจากบุคคลต่าง ๆ  
คั้งนั้นทางคณะผู้จัดทำจึงใคร่ขอขอบพระคุณบุคคลต่าง ๆ ดังต่อไปนี้

ขอขอบพระคุณ อาจารย์สถาพร พรหมวงศ์, ผศ. พิชญ สุพรรณกุล, พี่นิวัฒน์ และ พี่ ๆ ที่  
ศูนย์วิจัยคอมพิวเตอร์ที่คอยให้ความช่วยเหลือ และให้คำแนะนำ ตั้งแต่เริ่มทำโครงการ จนสำเร็จ  
ออกมาเป็นปริญญาบัตรฉบับนี้

นางสาวพรพิมล จินุพันธุ์

นางสาวพิมพ์ลักษณ์ กลิ่นมาลี

คณะผู้จัดทำ



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

# สารบัญ

เรื่อง	หน้า
บทคัดย่อภาษาไทย	ก
บทคัดย่อภาษาอังกฤษ	ข
กิตติกรรมประกาศ	ค
สารบัญ	ง
สารบัญรูป	ช
สารบัญตาราง	ญ
<b>บทที่ 1 บทนำ</b>	
1.1 แนวความคิดและที่มา	1
1.2 จุดประสงค์	2
1.3 ขอบเขตโครงการ	2
1.4 ผลที่คาดว่าจะได้รับ	2
1.5 ขั้นตอนการดำเนินการ	3
<b>บทที่ 2 ทฤษฎีที่เกี่ยวข้อง</b>	
2.1 บทนำ	4
2.2 ไฟร์วอลล์	4
2.2.1 รูปแบบการทำงานของไฟร์วอลล์	6
2.2.2 สถาปัตยกรรมของไฟร์วอลล์	10
2.3 DHCP (Dynamic Host Configuration Protocol)	12
2.4 DNS Server (Domain Name System)	14
2.5 NAT (Network Address Translation)	17
2.6 IPTABLES	22
2.7 Web Server (เว็บเซิร์ฟเวอร์)	28
2.8 Mail Server (เมลเซิร์ฟเวอร์)	32
2.8.1 POP3	32

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญ (ต่อ)

เรื่อง	หน้า
2.8.2 SMTP	36
2.8.3 IMAP	38
2.9 FTP Server	39
<b>บทที่ 3 การออกแบบระบบเครือข่าย</b>	
3.1 ขั้นตอนการออกแบบระบบเครือข่าย	45
3.2 การออกแบบไฟร์วอลล์	46
3.3 การออกแบบเว็บเซิร์ฟเวอร์, DNS เซิร์ฟเวอร์ และ เมล์เซิร์ฟเวอร์	52
3.4 การออกแบบมอนิเตอร์เซิร์ฟเวอร์	53
3.5 การออกแบบเซิร์ฟเวอร์ข้อมูล	54
3.6 การออกแบบโฮมเพจ (Homepage)	54
<b>บทที่ 4 ผลการทดลอง</b>	
4.1 การจัดการระบบเครือข่ายภายใน	56
4.1.1 ไฟร์วอลล์	57
4.1.2 เว็บเซิร์ฟเวอร์, DNS เซิร์ฟเวอร์ และ เมล์เซิร์ฟเวอร์	57
4.1.3 มอนิเตอร์เซิร์ฟเวอร์	57
4.1.4 เซิร์ฟเวอร์ข้อมูล	57
4.2 ผลการทดลองระบบเครือข่าย	58
<b>บทที่ 5 สรุป</b>	
5.1 สรุปการออกแบบเน็ตเวิร์ก	78
5.2 ผลที่ได้รับ	79
5.3 ปัญหา	79
5.4 แนวทางในการพัฒนาโครงการ	80

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญ (ต่อ)

เรื่อง	หน้า
บรรณานุกรม	81
ภาคผนวก ก.	82
ภาคผนวก ข.	87



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญรูป

เรื่อง	หน้า
รูปที่ 2.1 รูปแบบการทำงานของแพ็กเก็ตไฟลเดอร์	7
รูปที่ 2.2 รูปแบบการทำงานของพรีอ็อกซีเซิร์ฟเวอร์เกตเวย์	7
รูปที่ 2.3 สกรีนนิ่ง เราเตอร์	10
รูปที่ 2.4 ดูอัล – โฮม โฮสต์	10
รูปที่ 2.5 สกรีนนิ่ง โฮสต์ อาร์คิเทคเจอร์	11
รูปที่ 2.6 สกรีนลับเน็ตอาร์คิเทคเจอร์	12
รูปที่ 2.7 การร้องขอไอพีแอดเดรส	13
รูปที่ 2.8 โดเมน	14
รูปที่ 2.9 โครงสร้างลำดับชั้นของ DNS	15
รูปที่ 2.10 ขั้นตอนการทำงานของ DNS	16
รูปที่ 2.11 ลักษณะการเชื่อมต่อของ NAT เราท์เตอร์	17
รูปที่ 2.12 ไอพีแอดเดรส ของเครือข่ายภายในกับเครือข่ายภายนอก	18
รูปที่ 2.13 ลักษณะการอ้าง แอดเดรส และ MAP แอดเดรส แบบ Static	19
รูปที่ 2.14 ตัวอย่างการทำงานของ Dynamic NAT	20
รูปที่ 2.15 การ Map แอดเดรส ของ PC เครื่องต่อไป ด้วย Dynamic NAT	21
รูปที่ 2.16 การใช้ NAT Router ของเครื่องพีซีต่างๆ จากเครือข่ายภายใน	21
รูปที่ 2.17 หลักการทำงานของ PHP	31
รูปที่ 3.1 ระบบเน็ตเวิร์คที่ออกแบบมาสำหรับห้องวิจัย	46
รูปที่ 4.1 ระบบเน็ตเวิร์คสำหรับภาคเรียนที่ 1	56
รูปที่ 4.2 ผู้ใช้รับไอพีแอดเดรสอัตโนมัติ	58
รูปที่ 4.3 ผู้ใช้ได้รับไอพีแอดเดรส	59
รูปที่ 4.4 การติดต่อกับเครือข่ายภายนอกโดยผ่าน NAT และ ไฟร์วอลล์	59
รูปที่ 4.5 เว็บบ์เซิร์ฟเวอร์	60
รูปที่ 4.6 ประกาศโดเมนลูกเป็น wis.itc.kmitl.ac.th	61

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญรูป (ต่อ)

เรื่อง	หน้า
รูปที่ 4.7 ชั้นแรกในการเซตเพื่อใช้ฟรีอักษิเซิร์ฟเวอร์	62
รูปที่ 4.8 แสดงการทำงานของ โปรแกรม Trend Micro	63
รูปที่ 4.9 การเข้า FTP ผ่านทาง Dos	64
รูปที่ 4.10 การเข้าFTP ผ่านทางเว็บเบราว์เซอร์	64
รูปที่ 4.11 เมื่อทำการใส่password ให้ถูกต้องตามที่กำหนด	65
รูปที่ 4.12 การเข้าFTPผ่านทาง WinSCP	65
รูปที่ 4.13 เมื่อใส่ username และ password ถูกต้อง	66
รูปที่ 4.14 โปรแกรม Trend InterScan VirusWall	67
รูปที่ 4.15 เป็นการเก็บ log (ล็อก) ต่างๆของ โปรแกรม	67
รูปที่ 4.16 เป็นการล็อกอินเข้ามา	68
รูปที่ 4.17 เมื่อใส่ล็อกอินอย่างถูกต้อง	68
รูปที่ 4.18 เป็นการทดลองส่งเมลออกจาก wis.ite.kmitl.ac.th	69
รูปที่ 4.19 ตรวจสอบการส่งเมล	69
รูปที่ 4.20 ตรวจสอบการส่งเมล	70
รูปที่ 4.21 ทดสอบโดย Reply กลับไปยังเมลเซิร์ฟเวอร์	70
รูปที่ 4.22 ตรวจสอบการรับเมล	71
รูปที่ 4.23 ตรวจสอบการรับเมล	71
รูปที่ 4.24 เป็นการดูกราฟฟิคภายในเครือข่ายแบบเป็นวันและสัปดาห์	72
รูปที่ 4.25 เป็นการดูกราฟฟิคภายในเครือข่ายแบบเป็นเดือนและปี	72
รูปที่ 4.26 เป็นรูปโฮมเพจหน้าแรก	73
รูปที่ 4.27 เป็นการใส่ username และ password	74
รูปที่ 4.28 เมื่อใส่ username และ password ถูกต้อง	74
รูปที่ 4.29 ให้สมาชิกที่ล็อกอินเข้ามาสามารถตั้งกระทู้ได้	75
รูปที่ 4.30 สมาชิกใส่รายละเอียดต่างๆเกี่ยวกับกระทู้	75
รูปที่ 4.31 ผู้ที่เป็นสมาชิกร่วมตอบกระทู้	76
รูปที่ 4.32 ลบกระทู้ที่ไม่เหมาะสมได้	76

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญรูป (ต่อ)

เรื่อง	หน้า
รูปที่ 4.33 สมาชิกสามารถเข้ามาอ่านหรือดาวน์โหลดงานวิจัยได้	77
รูปที่ 4.34 สมาชิกสามารถดาวน์โหลดงานวิจัยได้	77
รูปที่ 5.1 โครงสร้างเครือข่ายที่ทำการออกแบบแบบสมบูรณ์	78



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญตาราง

เรื่อง	หน้า
ตารางที่ 2.1 เปรียบเทียบรูปแบบการทำงานของไฟร์วอลล์ทั้ง 3 ประเภท	9
ตารางที่ 2.2 สรุปรายละเอียดของคำสั่งต่างๆใน POP3	34
ตารางที่ 2.3 แสดงรายละเอียดในคำสั่งต่าง ๆ ของ SMTP ที่ใช้งานอยู่	37
ตารางที่ 2.4 คำสั่งต่างที่ใช้ใน FTP	41
ตารางที่ 2.5 พารามิเตอร์ภายใต้ service ftp	43
ตารางที่ 3.1 บอกถึงแพ็คเกจที่อนุญาตให้ผ่านเข้ามาได้	47
ตารางที่ 3.2 บอกถึงแพ็คเกจที่อนุญาตให้ผ่านออกไปได้	48
ตารางที่ 3.3 บอกถึงแพ็คเกจที่ส่งต่อ	48
ตารางที่ 3.4 บอกถึงกฎของการติดต่อจาก EXTERNET ไป KMITL	49
ตารางที่ 3.5 บอกถึงกฎของการติดต่อจาก KMITL ไป EXTRANET	49
ตารางที่ 3.6 เป็นการสร้างกฎต่างๆของการทำ NAT	50

# บทนำ

## บทที่ 1

### 1.1 แนวความคิดและที่มา

เนื่องจากการจัดการระบบเน็ตเวิร์กภายในห้องกลุ่มวิจัยแบบไร้สายแบบเดิม ยังคงขาดความปลอดภัยและเสถียรภาพ ทำให้กลุ่มวิจัยแบบไร้สายมีปัญหาในการใช้ระบบเครือข่ายภายในและภายนอก รวมถึงเรื่องความปลอดภัย จึงได้ออกแบบการวางระบบเน็ตเวิร์กภายในห้องกลุ่มวิจัยแบบไร้สายใหม่ โดยเน้นในเรื่องความปลอดภัย ความมีเสถียรภาพ รวมทั้งเว็บแอปพลิเคชัน (Web Application )

#### 1.1.1 ความปลอดภัย

ในเรื่องความปลอดภัยแบบเดิม ได้พบปัญหาหลายอย่าง เช่น ใช้ Public IP เพียงอย่างเดียว ซึ่งจำนวนหมายเลขเน็ตเวิร์ก ไม่เพียงพอต่อความต้องการของผู้ใช้ นอกจากนี้ยังทำให้ความปลอดภัยในระบบลดลงด้วย และเกิดปัญหาในเรื่องไอพินกันเนื่องจากผู้ใช้ได้ทำการคอนฟิกไอพินเอง รวมถึงการจัดการสรรไอพีที่ไม่เป็นระบบเป็นต้น จึงได้คิดพัฒนาโดยการทำการออกแบบระบบเน็ตเวิร์กใหม่ให้มีความปลอดภัยมากขึ้น

#### 1.1.2 เสถียรภาพ

ในเรื่องเสถียรภาพนั้นแบบเดิมใช้ Single Box เพียงตัวเดียวซึ่งทำหน้าที่เป็นเกตเวย์ไฟลด์วอล เมื่อพังทำให้ผู้ใช้ภายในไม่สามารถต่อเชื่อมออกเน็ตเวิร์กภายนอกได้ จึงทำการออกแบบให้มีเสถียรภาพมากขึ้น

#### 1.1.3 ความปลอดภัยต่อข้อมูลภายในเครือข่าย

แบบเดิมภายในห้องวิจัยแบบไร้สายนั้นไม่มีการจัดการใดๆเกี่ยวกับข้อมูลของอาจารย์และนักศึกษาซึ่งเป็นข้อมูลที่มีความสำคัญระดับสูง จึงได้คิดพัฒนาให้มีการจัดเก็บเป็นระบบมากขึ้น โดยทำเป็นฐานข้อมูล ให้มีความปลอดภัยระดับสูง

#### 1.1.4 เว็บแอปพลิเคชัน

แต่ก่อนนั้นภายในห้องวิจัยไม่มีระบบบริการภายในห้องทำให้เกิดความยุ่งยากต่างๆ เช่น การดาวน์โหลดงานวิจัย เป็นต้น จึงได้คิดสร้างเว็บไซต์ภายในห้องวิจัยแบบไร้สายขึ้นเพื่อให้มีแจ้งข่าวสาร, ความรู้ต่างๆ รวมถึงทำการสร้างเว็บบอร์ด (Webboard) เพื่อให้ผู้ใช้ภายในห้องวิจัยได้ติดต่อหรือตั้งกระทู้ถาม- ตอบเกี่ยวกับข่าวสาร หรือ วิชาการความรู้ภายในห้องวิจัย

## 1.2 จุดประสงค์

- เพื่อพัฒนาการจัดระบบเน็ตเวิร์คภายในห้องกลุ่มวิจัยแบบไร้สาย
- เพื่อป้องกันการเข้าถึงระบบเครือข่ายจากภายนอก
- เพื่อเก็บข้อมูลจากการทำ thesis ของนักศึกษา ให้เป็นระบบ
- เพื่อแลกเปลี่ยนความรู้ ข่าวสาร ภายในและภายนอกกลุ่มวิจัย

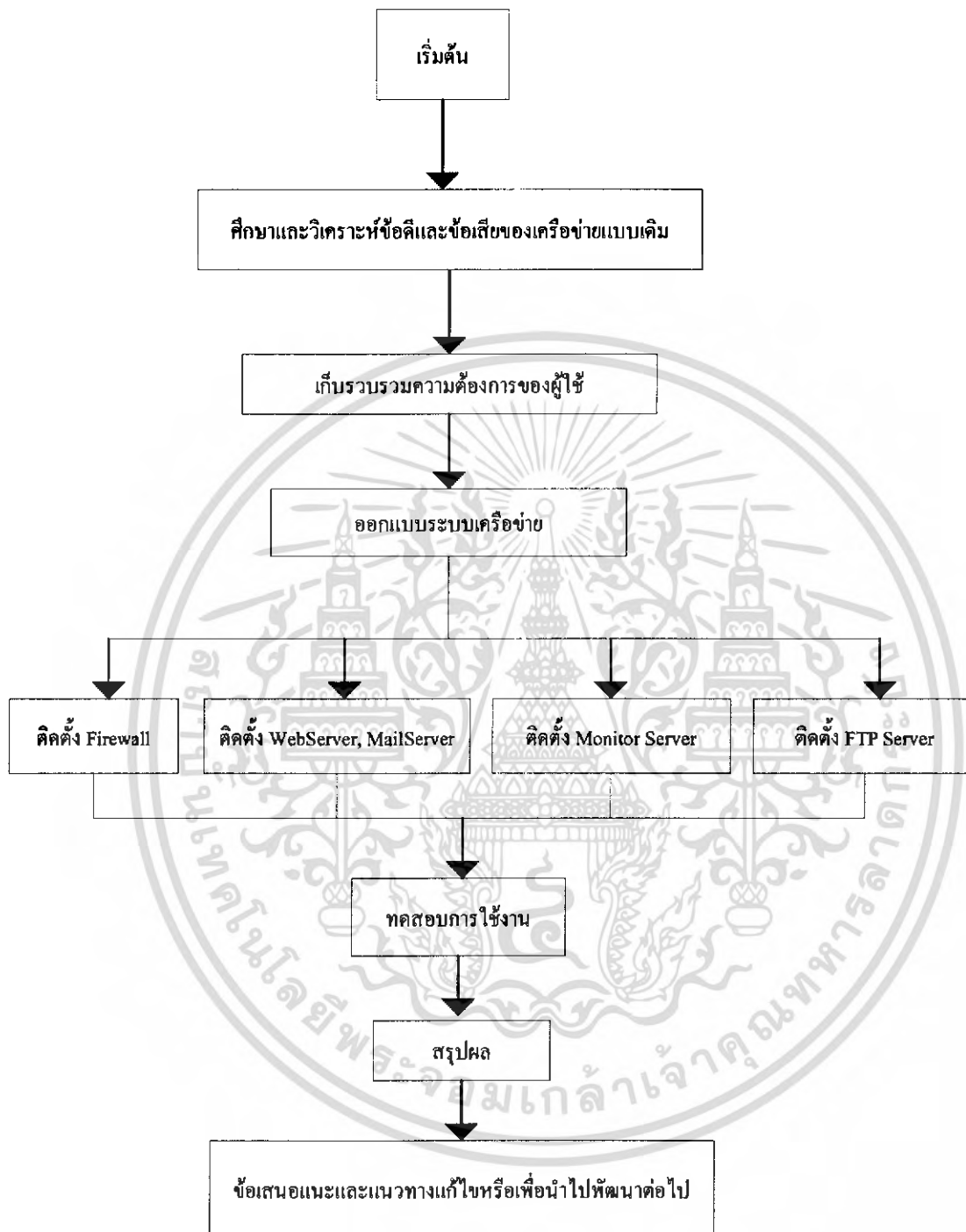
## 1.3 ขอบเขตโครงการ

- ศึกษาระบบเครือข่ายเดิม ว่ามีส่วนดีและส่วนบกพร่องอย่างไร รวมถึงศึกษาความต้องการ และการใช้งานในระบบเครือข่ายของผู้ใช้
- ทำการวางแผน ออกแบบ และวิเคราะห์ ระบบเน็ตเวิร์คให้มีประสิทธิภาพ โดยมีติดตั้งไฟร์วอลล์(Firewall) ออกแบบ โฮมเพจ (Home Page) และเว็บบอร์ด
- เพิ่มระบบความปลอดภัยของเซิร์ฟเวอร์ฐานข้อมูลกลาง (Central Database Server)
- ทำการคอนฟิก (configure) อุปกรณ์ต่าง ๆ ที่ใช้ในการวางระบบเน็ตเวิร์ค

## 1.4 ผลที่คาดว่าจะได้รับ

- ระบบเน็ตเวิร์คที่พัฒนาขึ้นในห้องกลุ่มวิจัยไร้สายมีประสิทธิภาพและเสถียรภาพมากขึ้น สามารถป้องกันการเข้าถึงระบบเน็ตเวิร์คภายในจากภายนอกได้
- ข้อมูลที่ได้จากการทำ thesis ของนักศึกษาถูกเก็บเป็นระบบมากขึ้น
- ผู้ใช้สามารถแลกเปลี่ยนความรู้ ข่าวสาร ภายในและภายนอกกลุ่มวิจัยได้

## 1.5 ขั้นตอนดำเนินการ



รูปที่ 1.1 ขั้นตอนการดำเนินการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## บทที่ 2

### ทฤษฎีที่เกี่ยวข้อง

#### 2.1 บทนำ

ในบทนี้ได้กล่าวถึงทฤษฎีเกี่ยวกับเครือข่าย ซึ่งประกอบไปด้วย อันดับแรกคือ ไฟล์วอลล์ ซึ่งหน้าที่รักษาความปลอดภัยให้กับเครือข่าย อันดับที่สองคือ DHCP ทำหน้าที่กำหนดไอพีแอดเดรสแบบอัตโนมัติให้แก่เครื่องไคลเอนต์ในระบบ อันดับที่สามคือ DNS Server (Domain Name System) ทำหน้าที่แปลงหมายเลขแอดเดรสให้อยู่ในรูปแบบของโดเมนเนม (Domain Name) หรือ แปลงกลับจากโดเมนเนมไปเป็นไอพีแอดเดรส อันดับที่สุดคือ NAT (Network Address Translation) เป็นวิธีการหนึ่งในการแปลงและแปลไอพีแอดเดรสของเครือข่ายภายในให้เป็นไอพีแอดเดรส ซึ่งเป็นที่ยอมรับและสื่อสารบนอินเทอร์เน็ต อันดับที่สุดคือ IPtables เป็นโปรแกรมโอเพ่นซอร์ส สำหรับควบคุมกฎการเข้า-ออกแพ็กเก็ตข้อมูล ในที่นี้จะเป็นส่วนหนึ่งในไฟร์วอลล์เพื่อเพิ่มความปลอดภัยให้แก่ระบบเครือข่ายระบบเครือข่าย อันดับที่สุดคือ Webserver(เว็บเซิร์ฟเวอร์) โดยมีการอัปโหลด (upload) โสมเพจของห้องกลุ่มวิจัยแบบไร้สายไว้ เพื่อความสะดวกในการใช้งานของผู้ใช้เกี่ยวกับแอปพลิเคชันต่างๆ โดยโสมเพจและแอปพลิเคชันต่างๆ ได้ใช้ PHP Hypertext Preprocessor (PHP) ในการสร้างขึ้นเพื่อติดต่อกันระหว่างฝั่งเซิร์ฟเวอร์และไคลเอนต์ (Client) อันดับที่สุดคือ Mail Server ( เมล์เซิร์ฟเวอร์ ) ซึ่งใช้ในการรับส่ง Email (อีเมล) ในเครือข่ายอินเทอร์เน็ต และอันดับที่สุดคือ FTP Server (เอฟทีพี เซิร์ฟเวอร์) เป็นการถ่ายโอนเพิ่มข้อมูลระหว่างเครื่องคอมพิวเตอร์ 2 เครื่อง ซึ่งอยู่บนเครือข่ายอินเทอร์เน็ต

#### 2.2 ไฟร์วอลล์

ไฟร์วอลล์ เป็นเครื่องมือรักษาความปลอดภัยให้กับเครือข่ายภายใน โดยป้องกันผู้บุกรุก (Intrusion) ที่มาจากเครือข่ายภายนอก ถ้าผู้บุกรุกมาจากเครือข่ายภายใน ระบบนี้จะไม่สามารถป้องกันได้ สิ่งที่สามารถป้องกันได้ เช่น ไวรัสคอมพิวเตอร์ (Virus), หนอนคอมพิวเตอร์ (Worm), การโจมตีแบบ DoS (Denial of Service), ม้าโทรจัน (Trojan House), IP Spoofing ฯลฯ

##### โดยมีลักษณะการบุกรุก ดังนี้

- ไวรัสคอมพิวเตอร์ จะแบ่งใช้หรือ ทำลายทรัพยากรของคอมพิวเตอร์ เช่น ไฟล์ข้อมูล, แรม
- หนอนคอมพิวเตอร์ จะแบ่งใช้ทรัพยากรของคอมพิวเตอร์ เช่น เขียนไฟล์ขยะลงบนฮาร์ดดิสก์

จนทำให้ฮาร์ดดิสก์เต็ม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- DoS จะร้องขอบริการ (Service) ต่างๆ จากเซิร์ฟเวอร์ จนทำให้เซิร์ฟเวอร์ล่ม
- ม้าโทรจัน จะซ่อนอยู่ในเครื่องไคลเอนต์หรือเซิร์ฟเวอร์ เมื่อถึงเวลามันจะทำการเปิดพอร์ตของเครื่องนั้นให้กับผู้บุกรุก เช่น แฮกเกอร์สามารถรีโมทเข้ามาควบคุมการทำงานของเครื่องนั้นได้
- IP Spoofing การปลอมหมายเลขไอพีต้นฉบับเพื่อลักลอบเข้ามาในเครือข่าย

ไฟร์วอลล์มีทั้งชนิดฮาร์ดแวร์ เช่น Router ที่ประกอบด้วยฟังก์ชัน Screening Device, Layer 3 Switch และซอฟต์แวร์ ที่เป็น Ipchains, Iptables

วิธีการของไฟร์วอลล์ คือ จำกัดให้มีการผ่านเข้าออกแพ็คเกจข้อมูลได้ที่จุดเดียว (Controlled point) และป้องกันผู้บุกรุกที่พยายามจะเข้ามาในเครือข่าย โดยทำการวิเคราะห์ว่าจะอนุญาตให้แพ็คเกจนั้นผ่านไปหรือไม่ ตามกฎที่กำหนดไว้

สิ่งที่ไฟร์วอลล์สามารถทำได้

- รักษาความปลอดภัย เนื่องจากเป็นจุดเดียวที่เครือข่ายภายในติดต่อกับเครือข่ายภายนอก
- สามารถตรวจสอบ และเก็บล็อกเหตุการณ์ต่าง ๆ ระหว่างการติดต่อของเครือข่ายภายใน และ เครือข่ายภายนอก
- สามารถกำหนดกฎ ในการอนุญาต หรือไม่อนุญาตในการใช้บริการต่าง ๆ ภายในเครือข่าย

สิ่งที่ไฟร์วอลล์ไม่สามารถทำได้

- ไฟร์วอลล์ไม่สามารถป้องกันผู้บุกรุกที่อยู่ภายในเครือข่าย (Internal Network)
- ไฟร์วอลล์ไม่สามารถป้องกันการโจมตีที่ไม่ได้ส่งผ่านไฟร์วอลล์ เช่น ผู้ใช้ภายในเครือข่ายมีการเชื่อมต่อกับอินเทอร์เน็ตในทางอื่นซึ่งไม่ผ่านไฟร์วอลล์ โดยที่ผู้ดูแลระบบไม่รับทราบ เช่น การ Dial-up ไปยังอินเทอร์เน็ตจากเครื่องคอมพิวเตอร์ส่วนบุคคลที่อยู่ภายในเครือข่าย

### ไฟร์วอลล์แบ่งออกได้ 3 ประเภท

1. Packet Filtering เป็นไฟร์วอลล์ระดับพื้นฐาน ใช้สำหรับตรวจสอบ ไอพีแอดเดรส และพอร์ตที่อยู่ต้นทางและปลายทาง รวมทั้งกรองแพ็กเก็ตข้อมูล ทั้ง TCP, UDP ได้
2. Circuit-Level Firewall เป็นไฟร์วอลล์ประเภทพรีออกซีเซิร์ฟเวอร์ ที่เป็นตัวกั้นกลางระหว่างเครือข่ายภายในกับเครือข่ายภายนอก โดยใช้เทคนิค SPI (Stateful Packet Inspection) ซึ่งมีหลักการทำงานเช่นเดียวกับ Packet Filtering และสามารถเพิ่มกฎในการเข้าถึง (Access Rules) เพื่อใช้ในการควบคุมทราฟฟิกได้
3. Application Level Firewall เป็นไฟร์วอลล์ประเภท พรีออกซีเซิร์ฟเวอร์ ที่ทำงานระดับแอปพลิเคชัน มีหน้าที่ป้องกันเครือข่ายภายในกับเครือข่ายภายนอกไม่ให้ติดต่อกันโดยตรง การร้องขอ (Request) และการตอบกลับ (Response) ต้องกระทำผ่าน พรีออกซีเซิร์ฟเวอร์

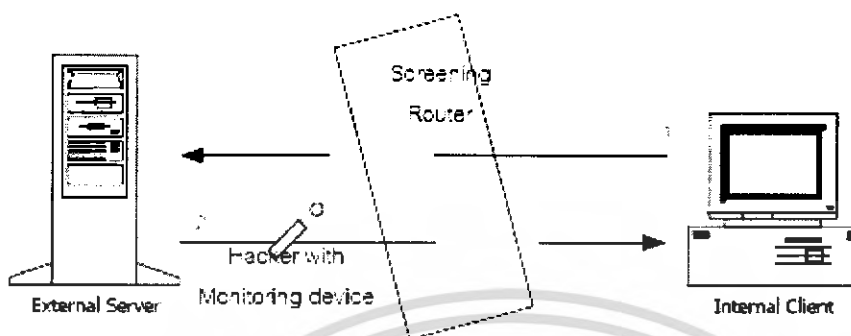
#### 2.2.1 รูปแบบการทำงานของไฟร์วอลล์

สามารถแบ่งรูปแบบการทำงานของไฟร์วอลล์ได้ 3 ประเภท ตามกลวิธีในการป้องกันเครือข่าย สำหรับการดำเนินงานบนเราเตอร์ในเลเยอร์ระดับล่าง จะใช้วิธีการกรองแพ็กเก็ต โดยอาศัยข้อมูลในส่วนเฮดเดอร์ เรียกว่า “แพ็กเก็ตฟิลเตอร์ริง” (Packet Filtering) ส่วนการทำงานในเลเยอร์ระดับสูง จะใช้พรีออกซีเซิร์ฟเวอร์ในการตรวจสอบเนื้อหาภายในแพ็กเก็ตและแสดงผลการตรวจสอบ เรียกว่า “พรีออกซีเซิร์ฟเวอร์เกตเวย์” และประเภทสุดท้าย ใช้สำหรับเก็บสถานะการทำงานไว้เป็นลำดับขั้น เรียกว่า “สเตทฟูลอินสเปกชัน”

##### 2.2.1.1 แพ็กเก็ตฟิลเตอร์ริง

เป็นวิธีที่ใช้กันอย่างแพร่หลาย หลักการทำงานคือ ไฟร์วอลล์จะทำการตรวจสอบแพ็กเก็ตโดยพิจารณาแพ็กเก็ตที่เข้าออกตามกฎที่ตั้งไว้ และวิเคราะห์แพ็กเก็ตเหล่านี้จากเฮดเดอร์ของแพ็กเก็ตนั้น ๆ เช่น แอดเดรสต้นทาง แอดเดรสปลายทาง พอร์ตหรือโพรโตคอล เมื่อแพ็กเก็ตแต่ละแพ็กเก็ตเข้ามาสู่ไฟร์วอลล์ จะนำมาเทียบกับกฎที่ตั้งไว้ หากเข้ากับกฎใดกฎหนึ่ง ก็พิจารณาว่ากฎนั้นมีจุดมุ่งหมายอย่างไรเช่น อนุญาตให้แพ็กเก็ตผ่านไปหรือครีอปแพ็กเก็ตนั้นทิ้งไป และหากไม่เข้ากับกฎใด จะพิจารณาค่าดีฟอลต์ ว่าอนุญาตให้แพ็กเก็ตผ่านไปหรือไม่อนุญาตให้ผ่านไป ซึ่งเป็นกระบวนการทำงานในชั้นเน็ตเวิร์ก (Network Layer) ซึ่งวิธีการนี้เป็นวิธีที่ง่ายและทำงานได้รวดเร็วที่สุด แต่จุดอ่อนคือ ความยากในการกำหนดกฎต่าง ๆ ให้รัดกุม และการติดต่อกันระหว่างโฮสต์ต้นทางและโฮสต์ปลายทางได้โดยตรง อาจส่งผลให้ข้อมูลต่าง ๆ ของโฮสต์ปลายทาง และโฮสต์อื่น ๆ

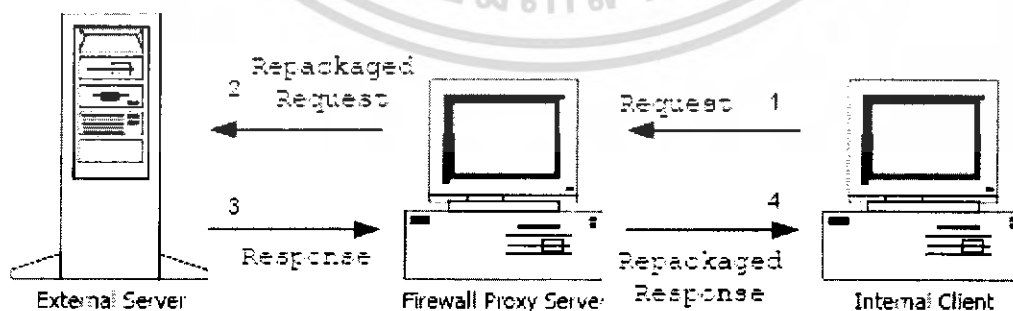
ที่ติดต่อกับโฮสต์ปลายทางถูกโจมตีได้ ไฟร์วอลล์ชนิดนี้สามารถต่อต้านการโจมตีได้หลายชนิด เช่น IP Spoofing, Source Routing Attack, Tiny Fragmentation Attack



รูปที่ 2.1 รูปแบบการทำงานของแพ็คเกจฟิลเตอร์ริง

### 2.2.1.2 พร็อกซีเซิร์ฟเวอร์เกตเวย์ (Proxy-Server Gateway)

พร็อกซีทำงานในชั้นเลเยอร์บน เป็นโปรแกรมแอปพลิเคชันที่ทำงานอยู่ระหว่างสองเครือข่าย โดยจะทำงานในลักษณะของการส่งข้อมูลต่อ เมื่อแพ็คเกจมาถึง พร็อกซีจะแยกข้อมูลส่วนที่เป็นเฮดเดอร์ของแพ็คเกจออก เหลือเพียงข้อมูลในของชั้นแอปพลิเคชัน เช่น กรณีเป็นข้อมูลของเว็บ พร็อกซีจะแยกเฮดเดอร์ออกเหลือเพียงส่วนโพรโตคอล HTTP จากนั้นก็จะนำเฮดเดอร์มาพิจารณาเทียบกับกฎต่าง ๆ ที่กำหนดไว้ หากตรงตามกฎที่อนุญาตให้ส่งต่อ จะนำข้อมูล HTTP นั้นมาประกอบเป็นแพ็คเกจขึ้นมาใหม่ และส่งต่อไปยังเป้าหมาย การทำงานลักษณะเช่นนี้ ทำให้การติดต่อระหว่างผู้ใช้ภายในกับภายนอกไม่ต้องติดต่อกันโดยตรง แต่พร็อกซีต้องรับภาระการทำงานอย่างหนัก ทำให้ประสิทธิภาพในการติดต่อระหว่างเครือข่ายลดลง ทำงานช้า แต่มีความปลอดภัยมากกว่าเนื่องจากการพิจารณาข้อมูลถึงระดับแอปพลิเคชัน แต่สามารถส่งต่อได้เฉพาะโพรโตคอลที่ไฟร์วอลล์รู้จักเท่านั้น



รูปที่ 2.2 รูปแบบการทำงานของพร็อกซีเซิร์ฟเวอร์เกตเวย์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

พรีอ็อกซีเซิร์ฟเวอร์เกตเวย์แบ่งออกได้เป็น 2 ประเภท

- เซอร์किค-เลเวล เกตเวย์ (Circuit – Level Gateway)

เป็นพรีอ็อกซีที่ทำหน้าที่ควบคุมการติดต่อระหว่างเครือข่ายภายในและภายนอก โดยปราศจากช่องว่าง กล่าวคือ จะมีวงจรเสมือน (Virtual Circuit) อยู่ระหว่างโฮสต์ภายในเครือข่ายกับพรีอ็อกซีเซิร์ฟเวอร์ เมื่อมีการร้องขอการติดต่อ (Request) จากเครือข่ายภายใน แพ็กเก็ตจะถูกส่งให้วงจรเสมือนผ่านไปยังพรีอ็อกซีเซิร์ฟเวอร์ ซึ่งจะส่งการร้องขอการติดต่อไปยังอินเทอร์เน็ต หลังจากทำการแปลงหมายเลขไอพีเรียบร้อยแล้ว ในทำนองเดียวกัน การตอบรับ(Response)จากอินเทอร์เน็ต จะถูกส่งมายังพรีอ็อกซีเซิร์ฟเวอร์ผ่านวงจรเสมือน ก่อนส่งกลับให้โฮสต์ต้นทาง โดยในการติดต่อนี้ เครือข่ายภายนอกจะไม่สามารถมองเห็นโฮสต์ใดๆ ภายในเครือข่ายได้เลย การติดต่อแบบนี้จะใช้ในกรณีที่ผู้ใช้ภายในเครือข่ายกับอินเทอร์เน็ตไว้ใจได้เท่านั้น

- แอปพลิเคชัน-เลเวล เกตเวย์ (Application – Level Gateway)

สำหรับแอปพลิเคชันเกตเวย์ นอกจากจะทำงานเช่นเดียวกับวงจรเสมือนแล้ว ยังเพิ่มความสามารถในการตรวจสอบแพ็กเก็ต ทั้งส่วนเฮดเดอร์และส่วนเนื้อหาของข้อมูลภายในแพ็กเก็ต เพื่อหยุดการส่งข้อมูลจากภายนอก และยังสนับสนุนการให้บริการ สำหรับโพรโตคอลแบบต่างๆ คือ Telnet, FTP, HTTP และ SMTP

### 2.2.1.3. สเตทฟูลอินสเป็คชันหรือไดนามิกแพ็กเก็ตฟิลเตอร์ริง

เป็นรูปแบบการทำงานแบบใหม่ ซึ่งพัฒนาจากแพ็กเก็ตฟิลเตอร์ริง ซึ่งเดิมการตัดสินใจ จะพิจารณาจากข้อมูลในส่วนเฮดเดอร์เท่านั้น และพิจารณาเฉพาะแพ็กเก็ตนั้น ๆ โดยไม่ได้พิจารณาความสัมพันธ์ของแพ็กเก็ตก่อนหน้า สเตทฟูลอินสเป็คชันพัฒนาโดยการพิจารณาทั้งในส่วนของข้อมูลที่ใช้ในการตัดสินใจ โดยพิจารณาข้อมูลในส่วนของ Payload และจะพิจารณาความสัมพันธ์ของแพ็กเก็ตที่อยู่ก่อนหน้าประกอบการวิเคราะห์ โดยบันทึกสถานะของข้อมูล เช่น เมื่อมีการส่งข้อมูล ตารางสถานะจะบันทึกหมายเลขพอร์ตต้นทาง หมายเลขพอร์ตปลายทาง เรียกว่า “Saving the state” เมื่อมีแพ็กเก็ตตอบรับ จะนำแพ็กเก็ตที่รับมานั้น เปรียบเทียบกับ “Saving state” ที่บันทึกไว้ว่ามีข้อมูลตรงกันหรือไม่ การทำงานของ สเตทฟูลอินสเป็คชัน จะมีการติดตามสถานะ (State) การทำงานของการเชื่อมต่อแบบ TCP ทำให้สามารถพิจารณารูปแบบการทำงานได้ทุกระบวนการ ไม่ได้พิจารณาเพียงข้อมูลในแต่ละแพ็กเก็ต นอกจากนี้สเตทฟูลอินสเป็คชันยังมีความปลอดภัยมากกว่า เนื่องจากสามารถปิดพอร์ตที่มีหมายเลขมากกว่า 1,024 ได้ เช่น การเชื่อมต่อแบบ TCP โดยเว็บนั้น เริ่มแรกจะติดต่อกันโดยผ่านพอร์ต 80 แต่หลังจากที่ติดต่อกสำเร็จ จะมีการใช้หมายเลข

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

พอร์ตแบบสุ่ม โดยมีหมายเลขมากกว่า 1,024 ซึ่งทำให้ไฟร์วอลล์แบบแพ็คเกจฟิลเตอร์จึงจำเป็นต้องเปิดพอร์ตที่มีหมายเลขมากกว่า 1,024 ตลอดเวลา แต่สแตทพลูจะเปิดพอร์ตเฉพาะเวลาที่มีการเชื่อมต่อผ่านพอร์ตนั้น ๆ เท่านั้น หากแพ็คเกจถูกรตรวจสอบแล้วว่าไม่เป็นไปตามกฎก็จะปิดพอร์ตนั้นทันที สแตทพลูอินสปีคชัน มีข้อจำกัด คือ ไม่รู้จักการทำงานในระดับแอปพลิเคชัน และยังคงเป็นการติดต่อกันระหว่างผู้ใช้ภายในกับภายนอกโดยตรง

ตารางที่ 2.1 เปรียบเทียบรูปแบบการทำงานของไฟร์วอลล์ทั้ง 3 ประเภท

	Packet Filter	Stateful Inspection	ฟร็อกซีเซิร์ฟเวอร์ Gateways
ข้อดี	<ul style="list-style-type: none"> <li>• ประสิทธิภาพดี</li> <li>• ง่ายในการ implement</li> <li>• ไม่ขึ้นกับแอปพลิเคชัน (Application Independent)</li> </ul>	<ul style="list-style-type: none"> <li>• ประสิทธิภาพดี</li> <li>• เปิดพอร์ตเฉพาะเมื่อมีการติดต่อ</li> <li>• สนับสนุนเกือบทุกบริการ</li> </ul>	<ul style="list-style-type: none"> <li>• ไม่เปิดเผยหมายเลขไอพีภายใน</li> <li>• พิจารณาเนื้อหาข้อมูลด้วย</li> <li>• มี User Authentication</li> <li>• เก็บรายละเอียด log ได้มาก</li> </ul>
ข้อเสีย	<ul style="list-style-type: none"> <li>• เปิดหมายเลขไอพีภายใน</li> <li>• มีการเปิดช่องว่างทิ้งไว้ถาวร</li> <li>• No User Authentication</li> <li>• ใช้การเชื่อมต่อโดยตรงกับภายนอก</li> </ul>	<ul style="list-style-type: none"> <li>• No User Authentication</li> <li>• ใช้การเชื่อมต่อโดยตรงกับภายนอก</li> <li>• เปิดหมายเลขไอพีภายใน</li> </ul>	<ul style="list-style-type: none"> <li>• ประสิทธิภาพต่ำกว่า</li> <li>• ต้องมีฟร็อกซีสำหรับทุกๆแอปพลิเคชันที่ใช้</li> <li>• ไม่มีการป้องกันในระดับชั้นที่ต่ำกว่าชั้นแอปพลิเคชัน</li> <li>• เปิดเผยระบบปฏิบัติการ</li> </ul>

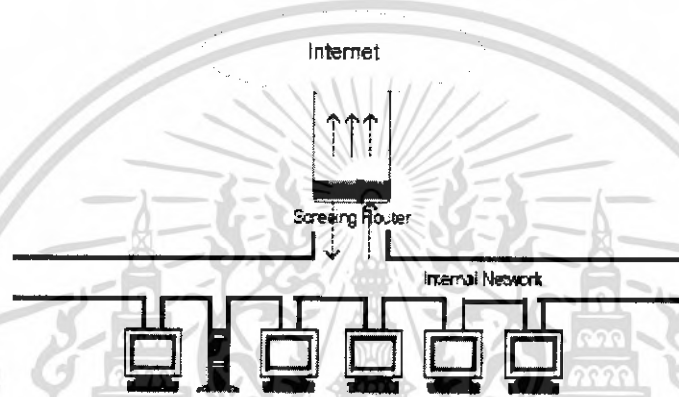
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## 2.2.2 สถาปัตยกรรมของไฟร์วอลล์

### 2.2.2.1 ซิงเกิลบ็อกซ์ (Single Box)

- สกรีนนิ่งเราเตอร์ (Screening Router)

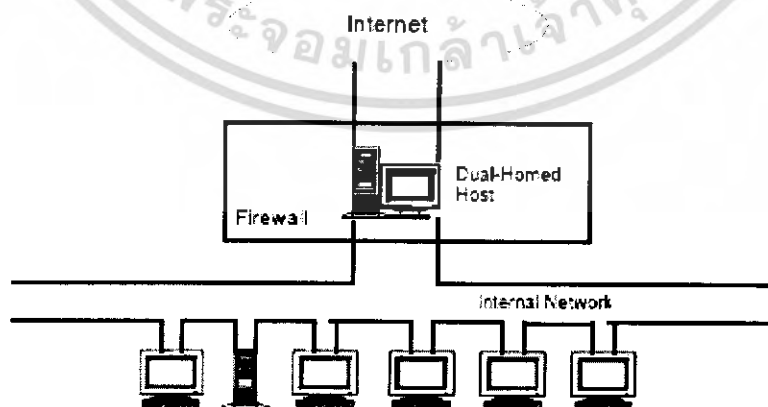
สามารถกรองแพ็กเก็ตตามกฎที่ตั้งไว้ โดยพิจารณาจากข้อมูลในส่วนเฮดเดอร์ของไอพีเท่านั้น เช่น อนุญาตหรือไม่อนุญาตพอร์ตหรือไอพีแอดเดรสใด ไฟร์วอลล์ลักษณะนี้เป็นการเชื่อมต่อระหว่างเครือข่ายภายในและเครือข่ายภายนอก ดังนั้นหากมีการโจมตีที่ไฟร์วอลล์ ซึ่งเป็นตัวหน้าด่านเพียงตัวเดียว หากการโจมตีสามารถผ่านไฟร์วอลล์ได้จะสามารถเข้ามาในเครือข่ายภายในได้



รูปที่ 2.3 สกรีนนิ่งเราเตอร์

- ดูอัล-โฮม โฮสต์ (Dual-Home Host)

เป็นคอมพิวเตอร์ที่เชื่อมต่ออยู่กับเครือข่ายอย่างน้อย 2 เครือข่าย สามารถทำหน้าที่เป็นเราเตอร์ได้ แต่ไม่อนุญาตให้มีการติดต่อผ่านกันโดยตรงโดยไม่ผ่านดูอัล-โฮม โฮสต์ ทำให้คอมพิวเตอร์ต้องรับภาระหนัก จึงเหมาะกับเครือข่ายที่มีข้อมูลเข้าออกน้อย ๆ เนื่องจากสามารถรักษาความปลอดภัยได้มากกว่าสกรีนนิ่งเราเตอร์



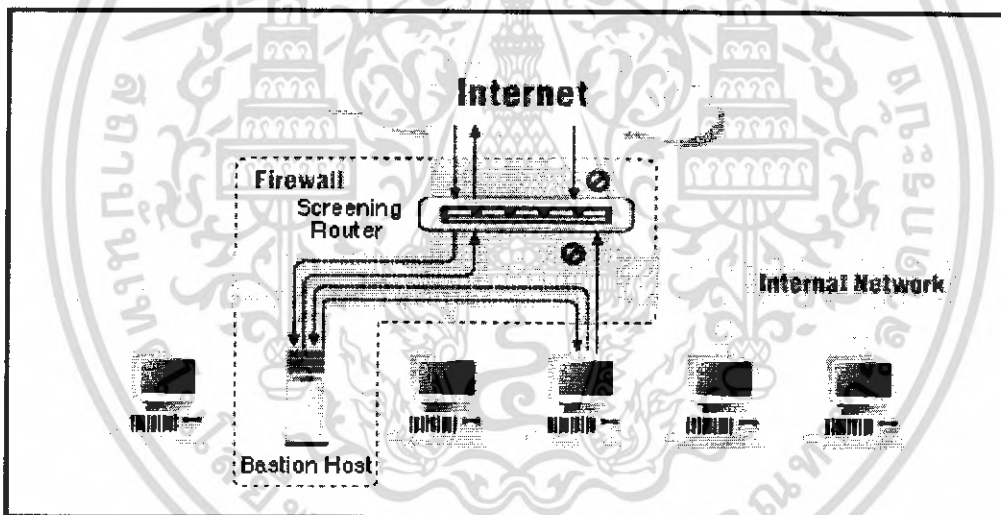
รูปที่ 2.4 สกรีนนิ่งโฮสต์ อาร์คิเทคเจอร์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### 2.2.2.2 มัลติเฟล-เพอโพส บ็อกซ์

- สกรีนนิ่งโฮสต์ อาร์คิเทคเจอร์ (Screen Host Architecture)

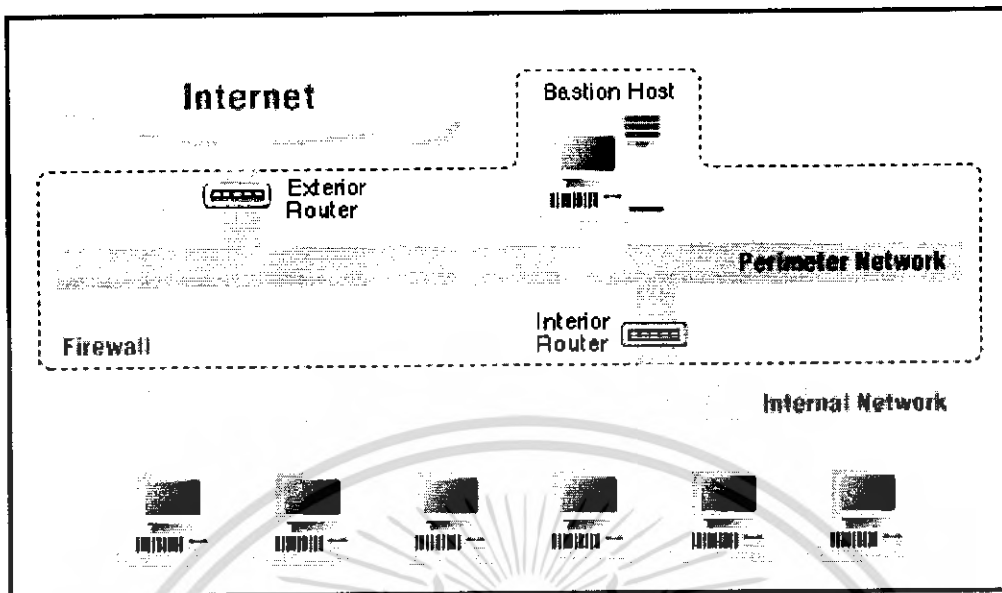
ประกอบไปด้วยไฟร์วอลล์ประเภทแพ็กเก็ตฟิลเตอร์ริงและเบสชันโฮสต์(BastionHost) โดยเบสชันโฮสต์เป็นคอมพิวเตอร์พิเศษ ที่อนุญาตให้มีการเชื่อมต่อกับเครือข่ายภายนอก ซึ่งจะทำหน้าที่เป็นพร็อกซีสำหรับส่งแพ็กเก็ตต่อไปยังเครื่องอื่น ๆ ภายในเครือข่าย ดังนั้นหากมีการบริการใด ๆ ในระบบเบสชันโฮสต์จะต้องรู้จักโปรโตคอลนั้น และเบสชันโฮสต์จะต้องมีการพิสูจน์สิทธิ์ (Authentication) ที่เหมาะสม การเริ่มใช้งานนั้น แพ็กเก็ตจะถูกกรองโดยแพ็กเก็ตฟิลเตอร์ริงเรเตอร์ ก่อนตามกฎที่กำหนดว่าควรจะอนุญาตหรือไม่อนุญาต จากนั้นทำการร้องขอพิสูจน์สิทธิ์กับเบสชันโฮสต์ และให้เบสชันโฮสต์เป็นตัวกลางจัดการเชื่อมต่ออีกครั้งหนึ่ง ข้อเสียของโครงสร้างแบบนี้ ขึ้นอยู่กับการทำงานของฟิลเตอร์ริงเรเตอร์ หากมีการทำงานผิดพลาด เบสชันโฮสต์จะให้บริการทุกการเชื่อมต่อ ทำให้เครือข่ายภายในถูกโจมตีได้ จึงไม่ควรให้บริการที่มีความเสี่ยงสูง เช่น เว็บเซิร์ฟเวอร์



รูปที่ 2.5 สกรีนนิ่งโฮสต์ อาร์คิเทคเจอร์

- สกรีนซับเน็ตอาร์คิเทคเจอร์ (Screened Subnet Architecture)

ต่างจากสถาปัตยกรรมสกรีนนิ่งโฮสต์ ตรงที่ส่วนของเบสชันโฮสต์จะมีการแบ่งเครือข่ายภายในออกจากเครือข่ายที่ให้บริการซึ่งให้ความปลอดภัยมากกว่า ในกรณีนี้จะมีไฟร์วอลล์ถึงสองตัว คือ เรเตอร์ภายนอกและเรเตอร์ภายใน เรเตอร์ภายในจะทำหน้าที่ป้องกันไม่ให้เครือข่ายภายในถูกโจมตี และป้องกันไม่ให้มีการโจมตีจากเครือข่ายภายในได้ โดยจะกรองทั้งแพ็กเก็ตที่มาจากอินเทอร์เน็ตและเบสชันโฮสต์



รูปที่ 2.6 สกรีนสับเน็ตเวิร์กเทกเจอร์

นอกจากนี้ยังประกอบด้วยเครือข่าย DMZ (De-militarize zone) ซึ่งเป็นการวางโฮสต์ที่ไม่น่าเชื่อถือหรือมีความปลอดภัยต่ำ (Untrusted Host) เช่น FTP Server และเว็บไซต์สาธารณะ ไว้ภายในไฟร์วอลล์ ให้แพ็กเก็ตผ่านไปได้ แต่อยู่นอกเครือข่ายภายใน ซึ่งการทำเช่นนี้ไฟร์วอลล์จะทำการเชื่อมต่อกับสามเครือข่าย และการทำเช่นนี้เป็นการเพิ่มประสิทธิภาพ ความปลอดภัย ความน่าเชื่อถือ แต่ไม่ได้เพิ่มระดับของความปลอดภัยในการเข้าถึงจากโฮสต์ที่อยู่ในเครือข่ายภายใน

### 2.3 DHCP (Dynamic Host Configuration Protocol)

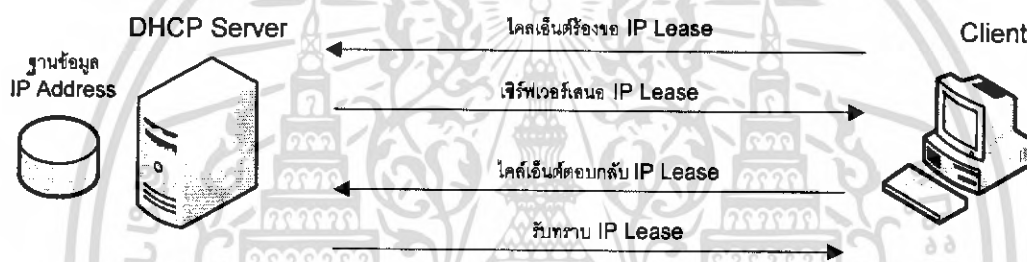
การกำหนดค่าไอพีแอดเดรสให้กับคอมพิวเตอร์แต่ละเครื่องที่เชื่อมต่อภายในเครือข่าย ทำได้ 2 วิธี คือ กำหนดไอพีแอดเดรสแบบตายตัว (Static Addressing Assignment) ซึ่งเครื่องคอมพิวเตอร์ที่ได้รับการกำหนดค่าดังกล่าวจะใช้เลขหมายไอพีแอดเดรสดังกล่าว ในการอ้างอิงตนเองกับการสื่อสารในทุกรูปแบบตลอดเวลา ในกรณีนี้ผู้ดูแลระบบเครือข่ายอาจประสบปัญหาว่าไอพีแอดเดรสที่ได้รับการอนุญาตให้ใช้งานนั้น มีไม่เพียงพอกับจำนวนเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับเครือข่ายภายใน หรืออาจมีเครื่องคอมพิวเตอร์กลุ่มทำการติดต่อสื่อสารไม่บ่อยนัก สามารถทำการจัดสรรเลขหมายไอพีแอดเดรสแบบเป็นครั้งคราว หรือที่นิยมเรียกกันเป็นทางการว่า จัดสรรแบบพลวัต (Dynamic Addressing Assignment)

DHCP เป็นการกำหนดไอพีแอดเดรสแบบอัตโนมัติให้แก่เครื่องไคลเอ็นต์ในระบบ ที่ติดตั้งโปรโตคอล TCP/IP เป็นการลดความซ้ำซ้อนของหมายเลขไอพีแอดเดรส เนื่องจาก DHCP

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เซิร์ฟเวอร์จะเป็นตัวแจกจ่ายไอพีแอดเดรสที่ไม่ซ้ำให้แก่เครื่องไคลเอ็นต์ DHCP เซิร์ฟเวอร์จะขอบเขตในการจ่ายไอพีแอดเดรส โดยผู้ดูแลระบบกำหนดว่าจะเริ่มที่หมายเลขไอพีใด เช่น 192.168.1.10 – 192.168.1.220 หมายถึงมีขอบเขตในการแจกไอพีแอดเดรสอยู่จำนวน 210 เครื่อง เมื่อเครื่องไคลเอ็นต์เริ่มบูตจะทำการขอหมายเลขไอพีแอดเดรส (Subnet Mask, Default Gateway และค่าอื่น ๆ ) จากเครื่อง DHCP เซิร์ฟเวอร์ เครื่อง DHCP เซิร์ฟเวอร์จะส่งไอพีแอดเดรสกลับไปยังไคลเอ็นต์

โดยสามารถแบ่งเป็นขั้นตอนการทำงานได้ดังนี้



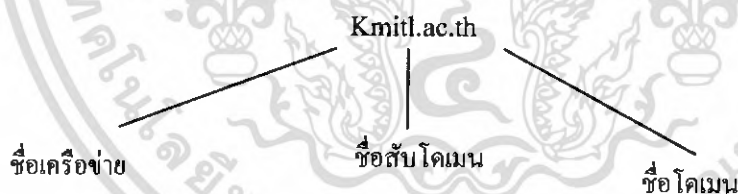
รูปที่ 2.7 การร้องขอไอพีแอดเดรส

- เครื่องไคลเอ็นต์ ทำการค้นหาตำแหน่งที่อยู่ของ DHCP เซิร์ฟเวอร์บนระบบเครือข่ายโดยการส่งแพสเซจ DHCP Discover ออกไปบนเครือข่ายเพื่อร้องขอไอพีแอดเดรส
- เครื่อง DHCP เซิร์ฟเวอร์ทำการค้นหาหมายเลขไอพีแอดเดรสจากฐานข้อมูลในเครื่องเพื่อไม่ให้ซ้ำกัน และส่งแพสเซจ DHCP Offer กลับไปให้เครื่องไคลเอ็นต์ที่ร้องขอ
- เมื่อเครื่องไคลเอ็นต์ได้รับหมายเลขไอพีแอดเดรสเรียบร้อยแล้ว ไคลเอ็นต์จะส่งสัญญาณตอบกลับ DHCP Request มาให้ทราบ
- เครื่องเซิร์ฟเวอร์ DHCP จะส่งสัญญาณ DHCP Ack กลับไปยังเครื่องไคลเอ็นต์เพื่อให้เริ่มใช้งาน (และเซิร์ฟเวอร์ DHCP จะเก็บหมายเลขไอพีแอดเดรส นั้นเอาไว้ไม่ให้เครื่องอื่นใช้ซ้ำ)

## 2.4 DNS Server (Domain Name System)

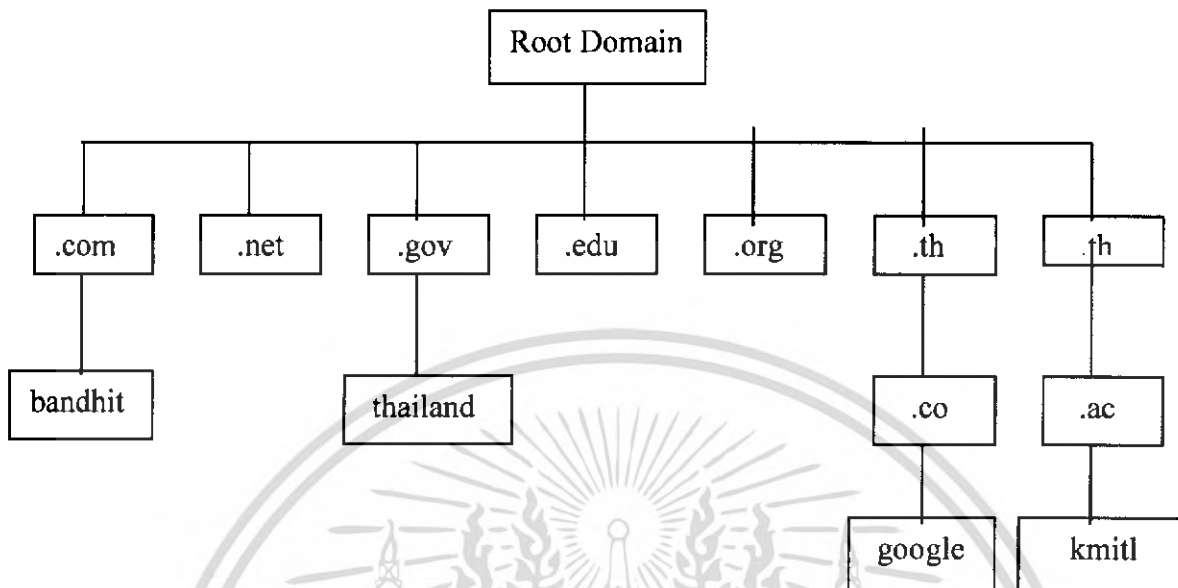
บนเครือข่ายอินเทอร์เน็ตที่มีการเชื่อมโยงผู้คนมากมายเข้าด้วยกัน จะมีหน่วยงาน InterNIC (Internet Network Information Center) เป็นผู้ดูแลเกี่ยวกับการจดทะเบียนเน็ตเวิร์ก หรือ โดเมนที่มีการเชื่อมต่อกับระบบอินเทอร์เน็ต โดยจะดูแลรายชื่อและหมายเลขไอพีแอดเดรส ทั้งหมด ทุกเครื่องจะต้องเชื่อมต่อกันผ่านโปรโตคอล TCP/IP ซึ่งต้องใช้ไอพีแอดเดรสในการอ้างถึง เช่น การเข้าสู่เว็บเซิร์ฟเวอร์ ถ้าเว็บเซิร์ฟเวอร์มีไอพีแอดเดรส เป็น 203.247.62.173 จะต้องใช้ หมายเลขนี้ในการติดต่อ แต่เนื่องจากหมายเลขไอพีแอดเดรส ของเซิร์ฟเวอร์นั้นมีอยู่หลายหมายเลข เป็นเรื่องยากในการจดจำตัวเลขว่าเป็นของเซิร์ฟเวอร์หรือเว็บไซต์ใด จึงมีการกำหนดมาตรฐาน ระบบชื่อโดเมน หรือ DNS (Domain Name System) มาใช้

DNS เป็นระบบแปลงหมายเลขไอพีแอดเดรส ให้อยู่ในรูปแบบของโดเมนเนม หรือ แปลง กลับจากโดเมนเนม เป็นไอพีแอดเดรสได้ หลังจากที่ได้ลงทะเบียนชื่อโดเมนผ่าน ISP จะใช้เวลา ประมาณ 2 วันในการกระจายชื่อโดเมนนี้ไปทั่วโลก ในการตั้งชื่อโดเมนส่วนมากจะใช้ชื่อ หน่วยงาน, บริษัท หรือสถานศึกษา เพื่อให้ง่ายต่อการจดจำ มาตรฐานระบบ DNS ประกอบไปด้วย ชื่อเครือข่าย ชื่อสับโดเมน และชื่อโดเมน เช่น ไอพีแอดเดรส เป็น 203.147.62.173 สามารถ เปลี่ยนเป็นตัวหนังสือ หรือชื่อโดเมนได้ดังนี้



รูปที่ 2.8 โดเมน

จะเห็นว่าชื่อสับโดเมนและโดเมนเป็นอักษรย่อ รูปแบบของโดเมนมีอยู่ 2 แบบด้วยกันคือ โดเมน 2 ระดับ และโดเมน 3 ระดับ

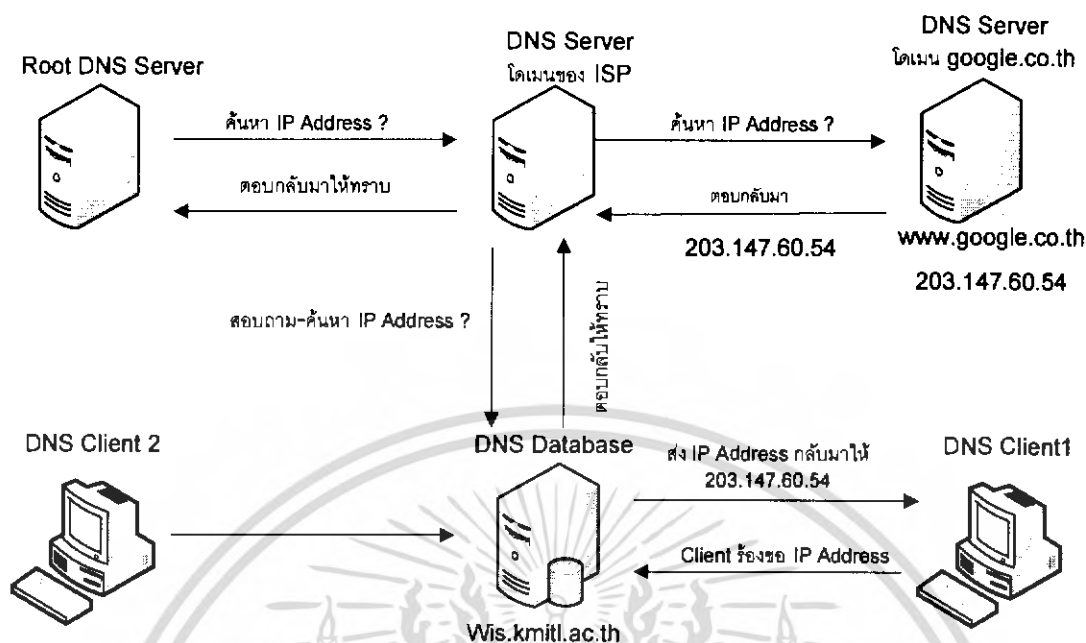


รูปที่ 2.9 โครงสร้างลำดับชั้นของ DNS

DNS มีโครงสร้างแบบต้นไม้ (tree) เป็นลำดับชั้น (hierarchical) ดังรูป ส่วนบนสุดคือ root domain ส่วนรองลงมาจะเป็น โดเมนเนม ที่ระดับที่แล้วแต่การใช้งาน

#### หลักการทำงานของ DNS

DNS ถูกออกแบบให้เป็นฐานข้อมูลแบบกระจาย มีกลไกในการทำงานแบบไคลเอ็นต์-เซิร์ฟเวอร์ โดย DNS Server จะเก็บหมายเลขไอพีแอดเดรส คู่กับชื่อเครื่องแบบโดเมนเนม เรียกว่า Name Resolution ไว้ เพื่อค้นหาชื่อตามการร้องขอของเครื่อง DNS ไคลเอ็นต์ ขั้นตอนการทำงานของ DNS มีดังนี้



รูปที่ 2.10 ขั้นตอนการทำงานของ DNS

- เครื่อง DNS Client ต้องการเชื่อมต่อกับ google.co.th จะส่งการร้องขอหมายเลขไอพีแอดเดรสของเว็บไซต์ www.google.co.th ผ่านกระบวนการ resolver ไปยัง DNS เซิร์ฟเวอร์ บนโดเมนของตน (ในที่นี้คือ Kmitl.ac.th) และถ้าเครื่อง DNS เซิร์ฟเวอร์ ไม่มีข้อมูลเกี่ยวกับเว็บไซต์นี้ จะส่งการร้องขอไปยัง DNS เซิร์ฟเวอร์ ของ ISP ผู้ให้บริการอินเทอร์เน็ต
- DNS เซิร์ฟเวอร์ ของ ISP ทำการค้นหาหมายเลขไอพีแอดเดรสนั้น (ถ้าไม่พบจะส่งไปเพื่อค้นหาใน Root DNS Server อีกต่อหนึ่ง) เมื่อพบแล้วจะส่งกลับมายังเครื่อง DNS Server บนโดเมน kmitl.ac.th
- เครื่อง DNS เซิร์ฟเวอร์ของ kmitl.ac.th จะบันทึกหมายเลขไอพีแอดเดรส ของเว็บไซต์ www.google.co.th ไว้ใน Cache Memory (ถ้ามีการร้องขอไอพีแอดเดรสนี้อีกครั้ง ส่งไปได้ทันที โดยไม่ต้องร้องขออีกครั้ง) จากนั้นจะส่งไอพีแอดเดรสของเว็บไซต์นี้กลับไปให้เครื่อง DNS ไคลเอนต์เพื่อทำการเชื่อมต่อเข้าสู่เว็บไซต์ตามต้องการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

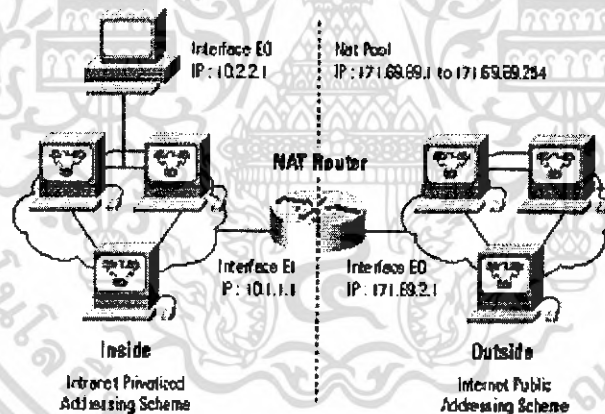
## 2.5 NAT (Network Address Translation)

Network Address Translation (NAT) เป็นวิธีการหนึ่งในการแปลงและแปลไอพีแอดเดรสของเครือข่ายภายในเป็นไอพีแอดเดรสที่สามารถสื่อสารบนอินเทอร์เน็ตได้

NAT สามารถใช้ไอพีแอดเดรสที่เป็น private IP (ซึ่งเป็น ไอพีแอดเดรส ที่ไม่ต้องจดทะเบียนบนอินเทอร์เน็ต) และสามารถซ่อนไอพีแอดเดรสในเครือข่ายภายใน (private IP) ได้ ทำให้เครือข่ายภายในมีความปลอดภัยเพิ่มมากขึ้น

- หลักการทำงานของ NAT

NAT เป็นระบบการอินเตอร์เฟซ (Interface) กับอินเทอร์เน็ต ที่ไม่ขึ้นอยู่กับโพรโตคอล (Protocol) และ แอปพลิเคชันรวมทั้ง อุปกรณ์ฮาร์ดแวร์ ใด ๆ ซึ่งหมายความว่า NAT สามารถนำมาประยุกต์ใช้งานกับ เราท์เตอร์ (Router) หรือคอมพิวเตอร์ที่ทำหน้าที่เป็นเราท์เตอร์ โดยมีอินเตอร์เฟซหนึ่งสำหรับติดต่อกับเครือข่ายภายใน และอีกอินเตอร์เฟซหนึ่งสำหรับการติดต่อกับเครือข่ายภายนอก ตัวอย่างการเชื่อมต่อ เช่น การติดตั้ง NAT ที่ Border เราท์เตอร์ ซึ่งเป็น เราท์เตอร์สำหรับเชื่อมต่อเครือข่ายภายในองค์กรกับเครือข่ายภายนอก



รูปที่ 2.11 ลักษณะการเชื่อมต่อของ NAT เราท์เตอร์

NAT สามารถเชื่อมต่อสื่อสารทั้งในแบบ Inbound และ Outbound คือ สามารถจัดการกับไอพีแอดเดรสที่ผ่านเข้ามา หรือ ไอพีแอดเดรสที่วิ่งออกไปโดยสามารถจัดการกับไอพีแอดเดรสต้นทางและปลายทางได้เป็นอย่างดี

NAT สามารถทำงานในสถานการณ์ 3 ประการ ดังนี้

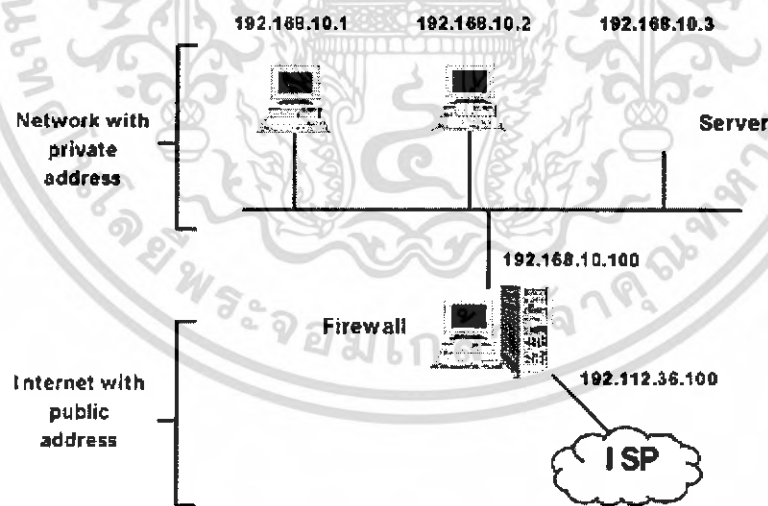
- ทำหน้าที่แปลงและแปล ไอพีแอดเดรสต้นทางที่มาจากเครือข่ายภายใน
- ทำหน้าที่แปลงและแปล ไอพีแอดเดรสต้นทางที่มาจากเครือข่ายภายนอกเช่น อินเทอร์เน็ต
- ทำหน้าที่แปลงและแปล ไอพีแอดเดรสปลายทางภายในเครือข่าย

แม้ว่า NAT สามารถใช้ กับ ไอพีแอดเดรสภายนอก แต่โดยทั่วไป NAT มีไว้เพื่อการแปล ไอพีแอดเดรสภายในเครือข่าย ซึ่งมีจุดประสงค์เพื่อซ่อนไอพีแอดเดรสภายในเครือข่าย และแปลง ไอพีแอดเดรสที่ไม่ต้องจดทะเบียน (private IP) ไปใช้เป็นไอพีแอดเดรสที่จดทะเบียนถูกต้อง ทำให้สามารถวิ่งไปตามเส้นทางบนอินเทอร์เน็ตได้

ชนิดของ NAT

NAT มีอยู่ 2 ชนิด คือ

- Static NAT เป็นการแปลงไอพีแอดเดรสชนิดกำหนดค่าแอดเดรสตายตัวจากเครือข่ายภายในไปยังเครือข่ายภายนอก ส่วนแอดเดรสภายนอกจะไม่มีเปลี่ยนแปลง ดังนั้นความสัมพันธ์ระหว่างไอพีแอดเดรสของเครือข่ายภายนอกและภายในจะเป็นแบบแน่นอนตายตัว



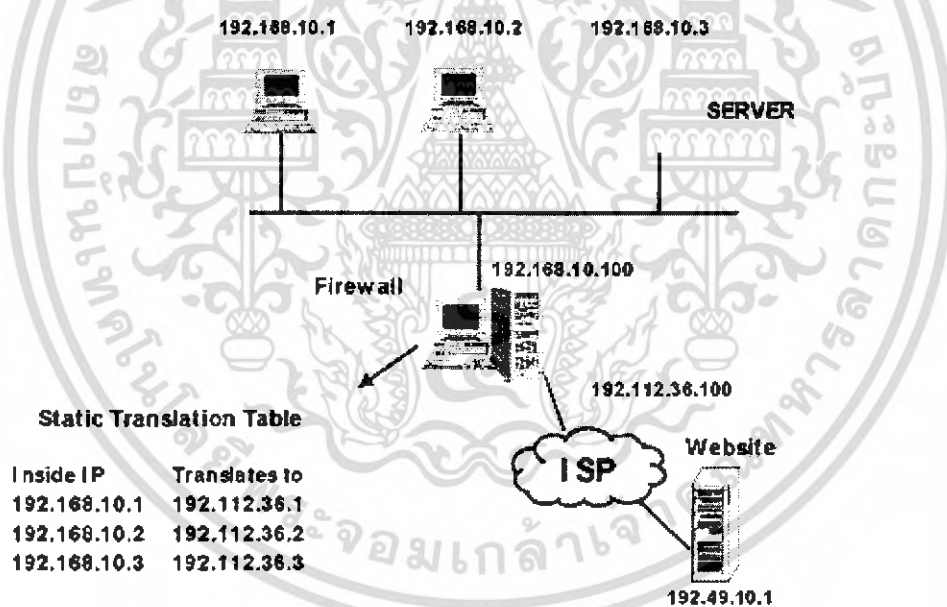
รูปที่ 2.12 ไอพีแอดเดรส ของเครือข่ายภายในกับเครือข่ายภายนอก

จากรูป 2.12 เครื่องคอมพิวเตอร์ส่วนบุคคล และเซิร์ฟเวอร์ภายในเครือข่ายกำหนดใช้แอดเดรสส่วนตัว (Private IP) เมื่อต้องการติดต่อกับเครือข่ายภายนอก ต้องผ่านการแปลงไอพีแอดเดรสก่อนที่จะออกจากเครือข่ายเสมอ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สมมติว่า มีคอมพิวเตอร์ส่วนบุคคลเครื่องหนึ่งซึ่งมี ไอพีแอดเดรส ภายในเป็น 192.168.10.1 ทำการส่งข่าวสารไปที่ อินเทอร์เน็ต โดยอ้าง แอดเดรส ที่ 140.49.10.1 ซึ่งแอดเดรสนี้ เป็น แอดเดรส บนอินเทอร์เน็ต ลักษณะนี้แพ็กเก็ตที่วิ่งออกจากคอมพิวเตอร์เครื่องนั้น จะมี แอดเดรส ต้นทางเป็น 192.168.10.1 ในกรณีนี้ เมื่อแพ็กเก็ต มาถึง NAT Router จะถูกแปลงเป็น 192.112.36.1 ซึ่งเป็น ไอพีแอดเดรส ที่ผู้จัดการเครือข่ายได้กำหนดขึ้น ลักษณะนี้ ทำให้แอดเดรส ภายในสอดคล้องกับแอดเดรสภายนอกอย่างแน่นหนาตายตัว และทุกครั้งที่ติดต่อไปยังภายนอก ต้องใช้ แอดเดรสเดิมเสมอ

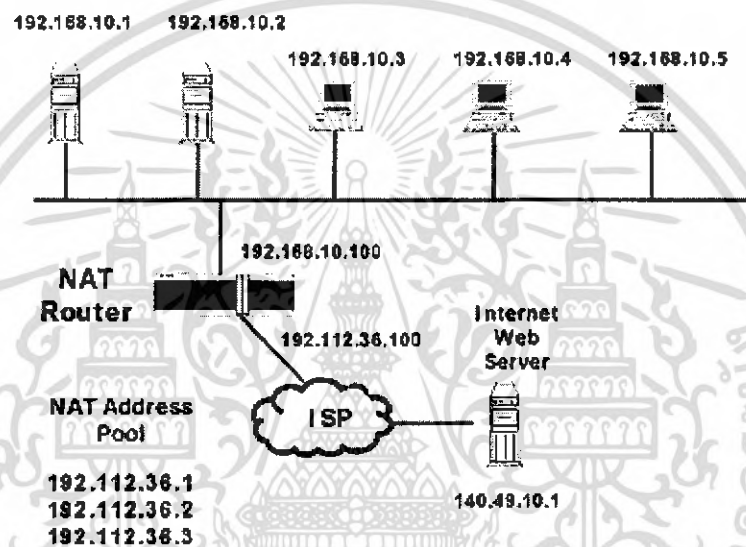
และเมื่อมีการตอบกลับมาจากเว็บไซต์ที่อยู่บนอินเทอร์เน็ต ตัว NAT แพ็กเก็ตเราท์เตอร์ จะใช้กระบวนการย้อนกลับ โดยเราท์เตอร์ทำการพิจารณาค่าแอดเดรสปลายทางบนแพ็กเก็ต ที่ส่งตรงมาจากเว็บไซต์ (140.49.10.1) จากนั้นทำการพิสูจน์เครื่องคอมพิวเตอร์ภายในเครือข่ายที่เว็บไซต์นี้ต้องการติดต่อด้วย และกำหนดไอพีแอดเดรสเพื่อติดต่อกับเครื่องคอมพิวเตอร์ต่อไป ดังรูปที่ 2.13



รูปที่ 2.13 ลักษณะการอ้าง แอดเดรส และ MAP แอดเดรส แบบ Static

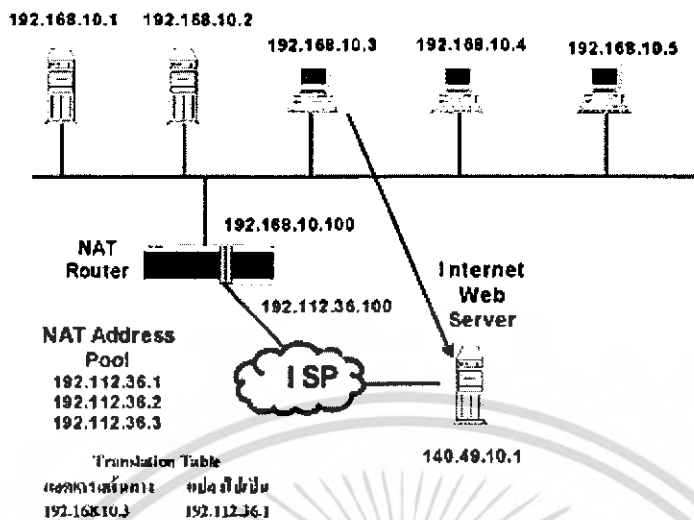
- Dynamic NAT เป็นการนำไอพีแอดเดรสจากกลุ่มของไอพีแอดเดรสที่ร่วมใช้งานกัน หรือที่เรียกว่า แอดเดรส Pool (พลู) มาทำการแปลง จาก แอดเดรส Pool ภายใน ให้เป็น Address Pool สำหรับเครือข่ายภายนอก หรือในทางกลับกัน รูปแบบนี้จะต้องได้รับการจัด Configure โดยผู้ดูแลระบบเครือข่าย แต่หลังจากที่จัดการ Configure เรียบร้อยแล้ว เราท์เตอร์ที่สนับสนุน NAT จะเป็นผู้จ่ายไอพีแอดเดรสให้กับคอมพิวเตอร์อย่างเหมาะสม และเพื่อเพิ่มความเร็ว เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในการทำงาน ผู้บริหารจัดการเครือข่ายจะต้องทำการ Map (แมพ) ระยะเวลาของ ไอพีแอดเดรส หากเป็นไปได้ (ลักษณะนี้ คล้ายกับการทำงานของ DHCP เซิร์ฟเวอร์ ที่ไม่ได้กำหนดเครื่อง PC (พีซี) แต่ละเครื่องให้มีไอพีแอดเดรสที่ตายตัว โดยผู้จัดการเครือข่ายจะกำหนดแอดเดรส ขึ้นมาจำนวนหนึ่ง เป็นระยะหรือช่วงของแอดเดรส เช่น 192.80.20.15 - 192.80.20.50 โดย เครื่องคอมพิวเตอร์จะไม่ได้รับหมายเลขไอพีซ้ำกัน ข้อแตกต่างกันระหว่าง NAT กับ DHCP Server คือ ไอพีแอดเดรส ของ NAT ที่แจกให้กับเครื่องคอมพิวเตอร์ที่เข้า-ออกบนเครือข่าย ดังรูป 2.14



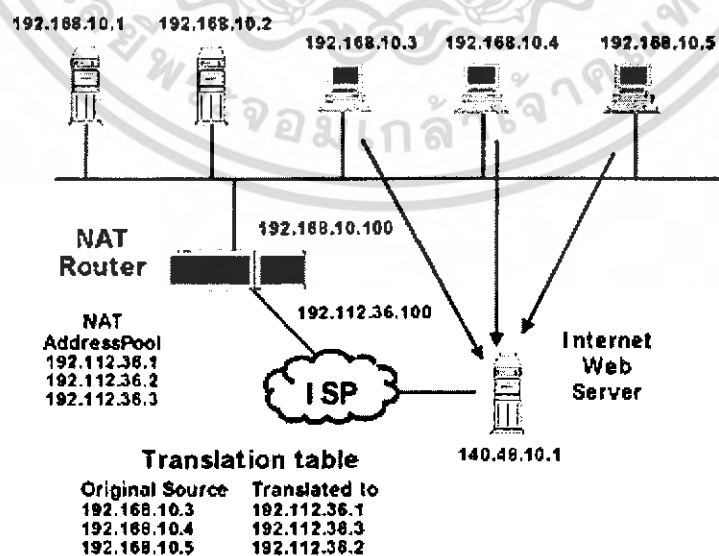
รูปที่ 2.14 ตัวอย่างการทำงานของ Dynamic NAT

Dynamic NAT มีการกำหนดแอดเดรสที่ใช้ติดต่อกับเครือข่ายภายนอกแบบพลวัต คือ ระบบที่กำหนดแอดเดรส จะมีการเปลี่ยนแปลงทุกครั้งที่คอมพิวเตอร์ภายในเครือข่ายนั้นมีการสถาปนาการเชื่อมต่อกับคอมพิวเตอร์ภายนอกเครือข่าย หรืออาจมีการเปลี่ยนเป็นระยะเวลา ดังรูปที่ 2.14



รูปที่ 2.15 การ Map แอดเดรส ของ PC เครื่องต่อไป ด้วย Dynamic NAT

สมมติว่า เครื่องคอมพิวเตอร์ส่วนบุคคลพร้อมด้วยไอพีแอดเดรสภายในเป็น 192.168.10.3 ใช้ HTTP Traffic (เซชที่พีพี ทรานฟฟิก) ไปที่ 140.49.10.1 เมื่อ NAT เราท์เตอร์ได้รับไอพีค้ำค่าแกรมแต่ละแพ็คเก็ต จะทำการดึงแอดเดรสภายนอก (ที่ผ่านการจดทะเบียนแล้ว) จากแอดเดรส Pool (ในที่นี้ คือ 192.112.36.1, 192.112.36.2 และ 192.112.36.3) และทำการเปลี่ยนแอดเดรสต้นทางด้วยแอดเดรสภายนอก ในขณะเดียวกัน NAT เราท์เตอร์จะสร้างตารางที่ประกอบด้วยแอดเดรส ที่ใช้เพื่อแปลง เช่นเดียวกับที่ Static NAT ใช้เพื่อแปลงแอดเดรสแบบตายตัวหน้าตาของตาราง แอดเดรส เป็นไปตามตัวอย่าง รูปที่ 2.16



รูปที่ 2.16 การใช้ NAT Router ของเครื่องพีซีต่างๆ จากเครือข่ายภายใน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในเวลาเดียวกันไอพีดาต้าแกรมที่มาจากคอมพิวเตอร์เครื่องที่สองบนเครือข่ายภายในที่ส่งข่าวสารไปยังเครือข่ายภายนอก จะได้รับการปฏิบัติในทำนองเดียวกันโดย NAT เราท์เตอร์

ตัวอย่าง เช่น NAT เราท์เตอร์ อาจแปลง ไอพีแอดเดรสต้นทาง ที่อยู่ใน IP Header ที่ติดต่อออกไปเพื่อต้องการใช้งาน FTP แอปพลิเคชัน (FTP Application) จาก PC ที่ใช้ แอดเดรส 192.168.10.4 ไปที่ แอดเดรส ต่อไปใน NAT Address Pool ซึ่งประกอบด้วยแอดเดรสจำนวนหนึ่ง (เช่น 192.112.36.1 - 192.112.36.3) และ NAT เราท์เตอร์ จะแปลงแอดเดรส 192.168.10.4 เป็น 192.112.36.3 ส่วนคอมพิวเตอร์อีกเครื่องหนึ่งคือ 192.168.10.5 จะถูกแปลงเป็น 192.112.36.2 หากเครื่องพีซีทั้งสองต้องการติดต่อกับเครือข่ายภายนอก ดังรูปที่ 2-14

เมื่อคอมพิวเตอร์แต่ละเครื่องสิ้นสุดการสื่อสารข้อมูลกับเครือข่ายภายนอกตัว NAT เราท์เตอร์ จะเรียกแอดเดรสภายนอกคืนกลับไปยัง Address Pool เพื่อให้ผู้ใช้รายต่อไป

## 2.6 IPTABLES

รูปแบบการใช้งาน IPtables เบื้องต้น จะมีรูปแบบการใช้งานดังนี้คือ

```
iptables [table] <command> <match> <target/jump>
```

โดยกฎที่กำหนดขึ้นจะเป็นเป็นตัวบอกเคอร์เนลว่าให้กระทำอย่างไร ในกรณีที่เกิดแพ็กเก็ตตรงตามที่ระบุไว้

- [table] หมายถึง ตารางที่ต้องการระบุ เช่น iptables -t nat หมายถึงให้ทำงานกับ nat table ในกรณีที่ไม่ได้ระบุตาราง iptables จะถือว่าคำสั่งดังกล่าวระบุถึง filter table โดยอัตโนมัติ
- <command> จะเป็นคำสั่งให้ iptables ทำในสิ่งที่ต้องการ เช่น iptables -A INPUT ซึ่งหมายถึงให้สร้าง rule ต่อท้าย INPUT chain ใน filter table
- <match> เป็นส่วนที่ใช้ตรวจสอบว่าแพ็กเก็ตมีข้อมูลตรง (match) กับที่ระบุไว้หรือไม่ เช่น มีไอพีแอดเดรสต้นทางเป็น 1.2.3.4
- <target/jump> เป็นตัวระบุว่าเมื่อเจอแพ็กเก็ตที่ match ก็จะทำ (action) ตามที่ระบุไว้ เช่น ถ้าแพ็กเก็ตใดมีไอพีแอดเดรสต้นทางเป็น 1.2.3.4 ให้ DROP แพ็กเก็ตนั้นทิ้งไป

iptables สามารถทำงานได้กับตาราง (table) 3 ตารางหลัก สามารถระบุตารางได้โดยใช้ ออปชัน -t ตามด้วยชื่อ table คือ

1. Filter table ใช้สำหรับกรอง packet มี 3 built-in chain คือ INPUT, OUTPUT, FORWARD
2. NAT table ใช้สำหรับการแปลงแอดเดรส (Network Address Translation) มี 3 built-in chain คือ PREROUTING, POSTROUTING, OUTPUT
3. Mangle table เป็นตารางที่ใช้เปลี่ยนแปลงหรือแก้ไข packet เช่น เปลี่ยนค่า TTL , MARK ซึ่งปกติจะใช้ในการทำ routing ที่มีความซับซ้อนสูง มี 2 built-in chain คือ PREROUTING chain (ใช้แก้ไข packet ก่อนที่จะเข้าสู่ไฟร์วอลล์และก่อนเข้าสู่ routing decision) และ OUTPUT chain (ใช้แก้ไข packet ที่ถูกสร้างโดยไฟร์วอลล์ก่อนที่มันจะถูกส่งไปยัง routing decision) แต่ไม่สามารถทำ network address translation หรือ masquerading ที่ table นี้ได้

การใช้คำสั่ง iptables

- -A เพิ่มกฎใหม่ต่อท้าย chain (Append rule) เช่น  
# iptables -A INPUT -p ALL -i eth0 -j ACCEPT
- -D ลบกฎ (Delete rule) เช่น  
# iptables -D INPUT --dport 80 -j DROP
- -I เพิ่มกฎใหม่ ใน chain (Insert rule) เช่น  
# iptables -I OUTPUT -p ALL -s 127.0.0.1/32 -j ACCEPT
- -R แทนที่กฎเดิม ด้วย rule ใหม่ (Replace rule)
- -L แสดงกฎทั้งหมดใน chain (ถ้าไม่ระบุ chain จะแสดงกฎทั้งหมดใน filter table ทั้งสาม built-in chain) เช่น  
# iptables -L  
# iptables -L -t nat  
# iptables -L INPUT
- -F ลบกฎทั้งหมดใน chain ทิ้ง เช่น  
# iptables -F INPUT  
# iptables -F mychain

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- -Z ใช้ reset byte counter สำหรับทุกกฎใน chain ที่กำหนด เช่น  
# iptables -Z INPUT
- -N ใช้สร้าง chain ใหม่ เช่น  
# iptables -N mychain
- -X ลบ chain ที่ไม่มีกฎซึ่งสามารถลบ user-defined chain ที่ไม่มีกฎได้ แต่ไม่สามารถลบ built-in chain ได้ เช่น  
# iptables -X emptychain
- -P เปลี่ยน default policy ของ chain ค่าที่ใช้ได้คือ ACCEPT, DROP ทั้งนี้ค่านี้มีความสำคัญอย่างมากเพราะหากแพ็กเก็ตถูกส่งเข้ามาใน chain แล้วและไม่เข้ากับกฎใด ๆ เลย แพ็กเก็ตนั้นต้องถูกตัดสินใจโดย default policy ของ chain นั้นๆ เช่น  
# iptables -P FORWARD DROP  
ซึ่งหากแพ็กเก็ตถูกส่งเข้ามายัง FORWARD chain และไม่ตรงกับกฎใด ๆ ใน FORWARD chain จะถูก DROP ทันที
- -E ใช้เปลี่ยนชื่อ chain ใหม่ เช่น  
# iptables -E myoldchain mynewchain

#### การตั้งค่า Match

การตั้งเงื่อนไขของการ match นั้นจะต้องอาศัยความเข้าใจในเรื่อง IP, TCP, UDP และ ICMP มาบ้างพอสมควร จึงจะสามารถตั้งเงื่อนไขที่เหมาะสมและตรงตามความต้องการได้ ซึ่งมีรายละเอียดดังนี้

- การระบุไอพีแอดเดรสต้นทางหรือปลายทาง สามารถระบุไอพีแอดเดรสต้นทางของแพ็กเก็ต โดยใช้ -s หรือ --source หรือ --src และใช้ -d หรือ --destination หรือ --dst สำหรับ destination ไอพีแอดเดรส การระบุไอพีแอดเดรสนั้นสามารถทำได้ 4 แบบ คือ
  1. ใช้ชื่อเต็มแทน เช่น localhost หรือ www.kmitl.ac.th
  2. ระบุไอพีแอดเดรสโดยตรง เช่น 127.0.0.1 หรือ 202.44.204.33
  3. ระบุเป็น group ของไอพีแอดเดรส เช่น 202.44.204.0/24 ซึ่งหมายถึงไอพีแอดเดรสตั้งแต่ 202.44.204.0 - 202.44.204.255
  4. หรืออาจจะใช้ 202.44.204.0/255.255.255.0 แทน 202.44.204.0/24 ได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- การทำInversion

ในบางกรณีนั้นหากต้องการระบุเป็น inverse เช่น อนุญาตให้ทุกไอพียกเว้นไอพีที่ระบุไว้ ซึ่งการใช้คำสั่งดังกล่าวสามารถทำได้ โดยใช้เครื่องหมาย ! นำหน้า argument ที่ต้องการ ( เครื่องหมาย ! หมายถึง NOT ) เช่น -p ! TCP ซึ่งจะ match กับโปรโตคอลทุกตัวที่ไม่ใช่ TCP หรือ -s ! localhost ซึ่งหมายถึงแพ็คเกจที่มีไอพีแอดเดรสต้นทางยกเว้น localhost (127.0.0.1)

- การระบุโปรโตคอล

สามารถระบุโปรโตคอลที่ต้องการได้ดังนี้ คือ TCP, UDP, ICMP หรือสามารถใช้ตัวเลขแทนได้ (สำหรับ \*NIX อ้างอิงได้จาก /etc/protocols) สามารถใช้ได้ทั้งตัวอักษรเล็กหรือใหญ่ (ใช้ได้ทั้ง tcp และ TCP) เช่น -p TCP หรือ -p ! tcp

- การระบุinterface

-i หรือ --in-interface ตามด้วยชื่อ interface ใช้เพื่อระบุ incoming interface แพ็คเก็ตที่จะ match กับกฎนี้ต้องเข้ามาจาก interface ที่กำหนด เช่น -i Eth0 หมายความว่า ทุกแพ็คเก็ตที่เข้ามาทาง Eth0 จะ match กับกฎนี้ ทั้งนี้ชื่อ interface ที่สามารถใช้ได้นั้น สามารถตรวจสอบได้โดยใช้คำสั่ง ifconfig และ -o หรือ --out-interface ตามด้วยชื่อของ interface ใช้เพื่อระบุ outgoing interface ซึ่งหมายถึงแพ็คเกจที่จะ match กับกฎนี้กำลังจะเดินทางผ่าน interface ที่ระบุไว้ เช่น -o Eth1 หรือ -o ! Eth1

#### Match Extension

เป็น netfilter packet ที่อยู่ในช่วงทดลองใช้ รูปแบบการใช้งานให้ใช้ -m แล้วตามด้วย match ที่ต้องการ เช่น -m mac ทั้งนี้มีข้อป้ันให้เลือกใช้งานดังต่อไปนี้

- mac

รูปแบบการใช้งาน: -m mac หรือ --match mac ใช้ตรวจสอบ source MAC address ว่าตรงกับค่าที่ระบุไว้หรือไม่ มีประโยชน์สำหรับ PREROUTING, INPUT chain โดยมีข้อป้ันให้ใช้งานคือ

--mac-source เช่น --mac-source 00:55:81:CC:42:FF

- limit

รูปแบบการใช้งาน: -m limit หรือ --match limit

ใช้เพื่อกำหนดจำนวนของการ match ที่อาจจะมากเกินไปเป็นประโยชน์สำหรับกฎที่วางไว้ เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตอนท้ายสุดของ chain (ใช้ร่วมกันกับ DROP policy) ซึ่งส่วนใหญ่เป็น rule ที่ใช้เก็บข้อมูล ลงล็อกไฟล์ ซึ่งถ้าผู้บุกรุกส่ง packet ที่ไม่เข้าข่ายกฎใดๆ ใน chain จนกระทั่งมาถึงกฎที่ทำหน้าที่เก็บล็อกนี้ ถ้าแพ็คเก็ตที่เข้ามาจำนวนมากก็อาจจะทำให้ฮาร์ดดิสก์เต็มได้ ดังนั้นจึง ต้องใช้จำกัดจำนวนในการเก็บข้อมูลลงล็อก ซึ่งมีออปชันให้ใช้งานดังนี้คือ

--limit ตามด้วยตัวเลข ซึ่งบอกถึงจำนวนครั้งสูงสุดของการ match กับกฎที่ยินยอมต่อ 1 วินาที เช่น --limit 5/s ทั้งนี้ยังสามารถใช้หน่วยเวลาอื่นได้ เช่น /second /minute /hour /day เช่น -m limit --limit 3/minute

### The State Match

รูปแบบการใช้งาน: -m state หรือ --match state เป็น โมดูลที่ใช้ประโยชน์ได้เป็นอย่างดี มี ออปชันให้ใช้งานดังนี้

- NEW

รูปแบบการใช้งาน: -m state --state new หรือ --match state --state new

หมายถึงแพ็คเก็ตที่เป็นตัวสร้างการเชื่อมต่อใหม่

- ESTABLISHED

รูปแบบการใช้งาน: -m state --state established หรือ --match state --state established

หมายถึง แพ็คเก็ตที่เกี่ยวข้องกับการเชื่อมต่อที่สร้างไว้แล้ว เช่น echo-reply packet หรือ แพ็คเก็ตที่ส่งข้อมูลออกไปจากเว็บเซิร์ฟเวอร์เมื่อมี request web service เข้ามา

- RELATED

รูปแบบการใช้งาน: -m state --state related หรือ --match state --state related

เป็นแพ็คเก็ตที่เกี่ยวข้องกับการเชื่อมต่อที่สร้างไว้แล้ว แต่ไม่ใช่ส่วนหนึ่งส่วนใดของ การเชื่อมต่ออื่น เช่น FTP data packet (port 20) ที่เกิดขึ้นจากการใช้คำสั่งใน FTP command (port 21)

- INVALID

รูปแบบการใช้งาน: -m state --state invalid หรือ --match state --state invalid

เป็นแพ็คเก็ตที่ไม่เกี่ยวข้องกับส่วนอื่น เช่น ICMP echo-reply ที่เกิดขึ้น โดยที่ไม่มีเครื่องได้ การส่ง echo-request (กรณีเช่นนี้เกิดขึ้นได้เนื่องจากอาจจะโดน โจมตีแบบ Smurf attack)

`$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT`

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เป็นคำสั่งที่ทำให้ Iptables สามารถทำงานได้ในรูปแบบของ Stateful Inspection ที่แท้จริง โดยกฎนี้จะตรวจสอบแพ็กเก็ต ว่ามีเป็นส่วนหนึ่งของการเชื่อมต่อ ที่สร้างไว้แล้วหรือไม่ (ESTABLISHED) ถ้าใช่จะปล่อยให้ผ่านไป (ACCEPT) และในกรณีที่เครื่องภายในเครือข่าย เรียกใช้ FTP ไปยังเครื่องอื่นในอินเทอร์เน็ตนั้น คำสั่งที่ส่งไปจะใช้ พอร์ตปลายทางเป็น 21 แต่ data พอร์ตที่ใช้สำหรับรับส่งข้อมูลใน FTP นั้นเป็นพอร์ต 20 ซึ่งพอร์ตที่เกิดขึ้นนี้ถือว่ามี ความสัมพันธ์(related) กับพอร์ต 21 ดังนั้นจึงสามารถรับส่งไฟล์ผ่านพอร์ต 20 ได้โดยไม่ต้องสร้างกฎเพิ่มเติม

- NAT Table

เป็นตารางที่ใช้สำหรับทำ Network Address Translation เช่น เปลี่ยนค่าไอพี แอดเดรสต้นทาง , ไอพีแอดเดรสปลายทาง จุดสำคัญ คือ มีเพียงแพ็กเก็ตแรกเท่านั้นที่เข้ามาที่ chain นี้ ส่วนแพ็กเก็ตถัดไปจะถูกกระทำเหมือนแพ็กเก็ตแรกได้รับ ดังนั้นจึงไม่ควร ทำแพ็กเก็ต filtering ที่ chain เหล่านี้

การใช้งานตาราง Nat นั้น ใช้ข้อป้ัน -t nat และ target ที่สามารถใช้งานได้ คือ SNAT, DNAT, Masquerade, Redirect ซึ่งมีรายละเอียดดังนี้

- SNAT

การทำ NAT ต้นทาง จะทำที่ POSTROUTING chain โดย คือทำการเปลี่ยน แอดเดรสต้นทาง ก่อนที่จะส่งแพ็กเก็ตนั้นออกไป ซึ่งสามารถใช้ออบชัน -o (outgoing interface) ร่วมด้วยได้ นอกจากนี้ยังใช้ -j SNAT และ --to--source หรือ --to เพื่อเปลี่ยน ไอพีแอดเดรสหรือพอร์ตไปตามต้องการได้ เช่น

```
##เปลี่ยนไอพีแอดเดรสต้นทางเป็น 1.2.3.4
```

```
# iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 1.2.3.4
```

```
##เปลี่ยนไอพีแอดเดรสต้นทางเป็น 1.2.3.4, 1.2.3.5 หรือ 1.2.3.6
```

```
# iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 1.2.3.4-1.2.3.6
```

```
##เปลี่ยนไอพีแอดเดรสต้นทางเป็น 1.2.3.4 port 1-1023
```

```
# iptables -t nat -A POSTROUTING -p tcp -o eth0 -j SNAT --to 1.2.3.4:1-1023
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- DNAT

การทำ NAT ปลายทาง จะทำภายใต้ PREROUTING chain คือการเปลี่ยนค่า แอดเดรส ปลายทาง หรือพอร์ต ก่อนที่จะส่งแพ็คเก็ตไปยัง routing decision

โดยปกติการใช้งานจะระบุ -j DNAT และใช้ --to-destination หรือ --to และยังสามารถใช้ -i (incoming interface) ร่วมด้วย เช่น

```
##เปลี่ยนแอดเดรสปลายทางเป็น 192.168.1.20
```

```
# iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 192.168.1.20
```

```
##เปลี่ยนแอดเดรสปลายทางเป็น 192.168.1.20, 192.168.1.21 หรือ 192.168.1.22
```

```
# iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 192.168.1.20-192.168.1.22
```

```
##เปลี่ยนแอดเดรสปลายทางของ web traffic เป็น 192.168.1.50 port 8080
```

```
# iptables -t nat -A PREROUTING -p tcp --dport 80 -i eth0 -j DNAT --to 192.168.1.50:80
```

## 2.7 Webserver (เว็บเซิร์ฟเวอร์)

เว็บเซิร์ฟเวอร์ คือ แอปพลิเคชันที่ทำหน้าที่รับ และประมวลผลข้อมูลที่ร้องขอจากผู้ใช้บริการ อินเทอร์เน็ตโดยผ่านทางเว็บเบราว์เซอร์ (Webbrowser) หลังจากเว็บเบราว์เซอร์รับคำสั่งและประมวลผลแล้ว ผลลัพธ์จะถูกส่งกลับไปยังผู้ใช้ โดยแสดงผลในเว็บเบราว์เซอร์นั่นเอง นอกจากนี้เว็บเบราว์เซอร์จะให้บริการในอินเทอร์เน็ตแล้ว ยังสามารถนำมาประยุกต์ใช้ในเครือข่ายภายในองค์กร หรืออินทราเน็ตได้อีกด้วย

เว็บเซิร์ฟเวอร์นั้นเป็นกลไกสำคัญต่อองค์กรต่าง ๆ และช่วยสนับสนุนแอปพลิเคชันใหม่ ๆ ในลักษณะของ Web based Application ซึ่ง linux ได้รวมเอา Apache Web Server อันเป็นเว็บเซิร์ฟเวอร์ที่มีประสิทธิภาพสูง และนิยมใช้มากที่สุดไว้แล้ว และนอกจากตัว Apache เองแล้ว linux ยังมีส่วนประกอบอื่น ๆ ที่เกี่ยวข้องกับการพัฒนาบริการต่าง ๆ บนเว็บให้มาพร้อมกันด้วย เช่น PHP เป็นต้น

## Apache

ในความเป็นจริงแล้ว สถานะของ Apache ในปัจจุบันถูกแบ่งออกในเชิงการประยุกต์ใช้งาน ได้ 2 ทาง คือ การใช้งานทางตรง หรือการใช้งานโดยเน้นหนักไปในฐานะของ HTTP Server ซึ่งถูกนำไปใช้งานเป็นเว็บเซิร์ฟเวอร์โดยตรง ในส่วนนี้ยังสามารถแยกลักษณะการใช้งานออกไปได้อีกหลายทิศทางขึ้นอยู่กับลักษณะของงานและคุณลักษณะพิเศษต่าง ๆ ที่เสริมเข้าไปอีกด้วย ได้แก่

- การใช้งานเป็น Mirror Site ด้วยความสามารถจากโมดูลในกลุ่ม `mod_proxy.c` ทำให้เราสามารถประยุกต์ใช้ Apache เป็นเว็บไซต์ Mirror ได้ โดยสามารถสำเนาเนื้อหาจากเว็บไซต์ที่ได้รับ การอนุญาตแล้วมาให้บริการในเซิร์ฟเวอร์ของเราได้

- ทำหน้าที่เป็น Web Redirector หรือทำหน้าที่เป็นตัวช่วยเปลี่ยนทิศทางของผู้ชมที่มาจากแหล่งต้นทางที่แตกต่างกันให้ไปสู่ URL หรือเซิร์ฟเวอร์ที่กำหนดขึ้นใหม่ได้ ซึ่งมาจากความสามารถของโมดูล `mod_rewrite.c`

- การสร้างเว็บไซต์ส่วนบุคคล หรือ Personal Home Page การใช้งานแบบนี้เป็นที่นิยมมากในสถานศึกษา มหาวิทยาลัย โดยอาศัยการทำงานของโมดูล `mod_userdir.c` จะช่วยให้ยูสเซอร์ทุกคนในเว็บเซิร์ฟเวอร์มีเว็บไซต์ส่วนตัวได้โดยอัตโนมัติ โดยมี URL เป็นชื่อเว็บไซต์นั้นตามด้วยเครื่องหมาย ~ และชื่อของยูสเซอร์นั้น ๆ เช่น ยูสเซอร์ gump ในเซิร์ฟเวอร์ `www.tepleela.ac.th` จะมี URL เป็น `http://www.tepleela.ac.th/~gump/` เป็นต้น ซึ่งทำให้สมาชิก นักเรียน นักศึกษา มีเว็บไซต์เป็นของตนเองที่จะใช้ฝึกหัดสร้างเว็บไซต์ และเผยแพร่ข้อมูลสู่สาธารณะได้ตามต้องการ

- การเป็น Virtual Host ลักษณะนี้เป็นที่นิยมกันมากที่สุดคือ การสร้างเว็บไซต์มากกว่า 1 เว็บไซต์โดยใช้เครื่องเซิร์ฟเวอร์เพียงเครื่องเดียว และใช้หมายเลขไอพีแอดเดรสเพียงหมายเลขเดียวในการอ้างถึงเว็บไซต์หลายชื่อ หรือที่เรียกว่า Name Based Virtual Host ซึ่งช่วยให้ลดค่าใช้จ่ายไปได้มาก

- การเป็นเว็บเซิร์ฟเวอร์ที่สนับสนุนเทคโนโลยีเว็บอื่น ๆ Apache 1.3 และ 2.0 เป็นเพียงหนึ่งในโปรเจกต์ของ The Apache Software Foundation เท่านั้น ยังมีโปรเจกต์อื่น ๆ ที่เป็นโปรเจกต์ต่อเนื่องจากอาปาเช่อีกมากมาย เช่น Jakarta เป็นโปรเจกต์เสริมเพื่อทำให้อาปาเช่สนับสนุน Java Platform โดยหนึ่งในจำนวนโปรแกรมที่เป็นที่รู้จักกันเป็นอย่างดีก็คือ Tomcat 5 ซึ่งเสริมการสนับสนุน Java Servlet 2.4 และ Java Server Pages 2.0

ในทางอ้อม การประยุกต์ใช้อุปกรณ์เว็บเซิร์ฟเวอร์ยังถูกนำมาใช้เพื่อเป็นส่วนประกอบในงานด้านอื่น ๆ อีก โดยอยู่ในฐานะช่องทางติดต่อระหว่างผู้ใช้กับแอปพลิเคชันต่าง ๆ ในลักษณะของ Web based User Interface ซึ่งผู้ใช้อินเทอร์เน็ตทั่วไปมีความคุ้นเคยคืออยู่แล้ว อีกทั้งยังลดการบำรุงรักษาและคอนฟิกในฝั่งเครื่องไคลเอ็นท์ไปได้มากอีกด้วย การใช้งานในทางอ้อมที่ว่ามี ได้แก่

- เป็นยูสเซอร์อินเตอร์เฟซเข้าสู่ยูทิลิตี้ Apache ถูกนำไปพัฒนาร่วมกับซอฟต์แวร์ (Soft ware) ต่าง ๆ มากมายทั้งซอฟต์แวร์เชิงพาณิชย์ และฟรีซอฟต์แวร์ เพื่อใช้เป็นอินเตอร์เฟซที่สะดวกต่อการใช้งานยิ่งขึ้น เช่น ซอฟต์แวร์บริหารจัดการโปรแกรมตรวจสอบและกำจัดไวรัส ซอฟต์แวร์ช่วยการคอนฟิกและใช้งานลินุกซ์เซิร์ฟเวอร์
- เป็นช่องทางแสดงผลข้อมูลระบบและเครือข่าย เนื่องจาก Apache ถูกผนวกเอาไว้กับลินุกซ์เซิร์ฟเวอร์ทุกดิสทริบิวชัน หรือ ถ้าเป็น โอเอสอื่น (Windows, Mac OS X ) ก็สามารติดตั้งใช้งานได้ฟรี และสามารถแสดงผลได้ทั้งตัวอักษร รูปภาพ รูปกราฟ ได้โดยตรง จึงมีการนำเอาปามาใช้งานด้านการแสดงผลข้อมูลระบบ และกราฟสถิติต่าง ๆ มากมาย เช่น MRTG ใช้แสดงข้อมูลกราฟที่ได้ข้อมูลจาก Router หรือ SNMP Server โปรแกรม SARG ใช้แสดงตารางสถิติการเข้าชมเว็บไซต์ของผู้ใช้งาน Squid Proxy Server โปรแกรมประเภท Log Analyzer เป็นต้น
- ใช้เป็น Web Mail ข้อดีของการใช้งานอีเมลผ่านทางเว็บเบราว์เซอร์เป็นสิ่งที่เราต่างทราบกันเป็นอย่างดี Apache ในฐานะที่เป็น Front-End ของระบบอีเมลจึงเป็นงานอีกลักษณะหนึ่งที่เรา นิยมนำมาใช้งานร่วมกับระบบ Mail Server
- เป็นอินเตอร์เฟซของแอปพลิเคชันเฉพาะทาง มีซอฟต์แวร์เป็นจำนวนมากที่พัฒนาโดยทำงานภายใต้สภาพแวดล้อมที่เรียกว่า Web based Applications ทั้งที่เป็นการพัฒนาขึ้นเพื่อใช้งานในองค์กรโดยเฉพาะ และทั้งที่เป็นซอฟต์แวร์สำเร็จรูป เช่น โปรแกรมประเภท Groupware หรือ Web based collaboration ต่าง ๆ ระบบสนับสนุนสารสนเทศภายในองค์กร เป็นต้น

## PHP

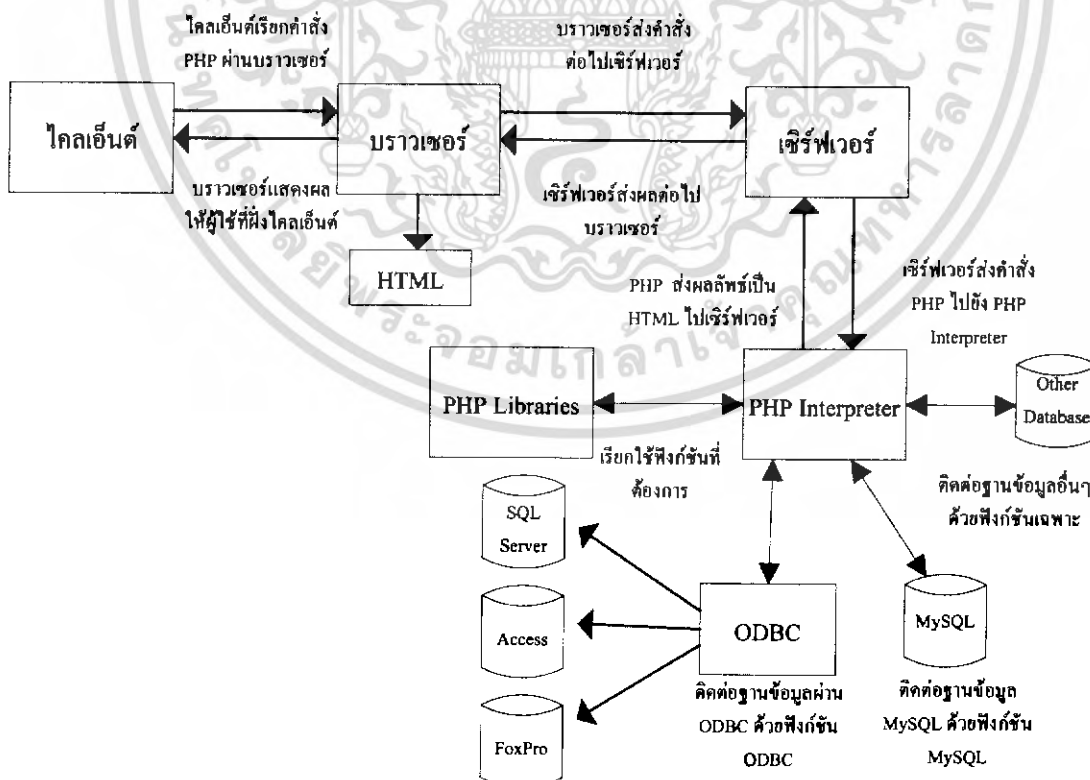
PHP หมายถึง PHP Hypertext Preprocessor ซึ่งเป็นภาษาจำพวก scripting language โดยคำสั่งต่างๆจะเก็บอยู่ในไฟล์ที่เรียกว่า สคริปต์ (script) และเวลาใช้งานต้องอาศัยตัวแปลชุดคำสั่ง ตัวอย่างของภาษาสคริปต์ก็เช่น JavaScript, Perl เป็นต้น ลักษณะของ PHP ที่แตกต่างจากภาษาสคริปต์แบบอื่นๆ คือ PHP ได้รับการพัฒนาและออกแบบมาเพื่อใช้งานในการสร้างเอกสารแบบ HTML โดยสามารถสอดแทรกหรือแก้ไขเนื้อหาได้โดยอัตโนมัติ ดังนั้นจึงกล่าวว่า PHP เป็นภาษาที่เรียกว่า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

server-side หรือ HTML-embedded scripting language ที่ประมวลผลฝั่งเซิร์ฟเวอร์แล้วส่งผลลัพธ์ไปฝั่งไคลเอนต์ผ่านเว็บเบราว์เซอร์ซึ่งเป็นเครื่องมือที่สำคัญชนิดหนึ่งที่จะช่วยให้เราสามารถสร้างเอกสารแบบ Dynamic HTML ได้อย่างมีประสิทธิภาพและมีลูกเล่นมากขึ้น

### หลักการการทำงานของ PHP

เนื่องจาก PHP จะทำงานโดยมีตัวแปรและเอ็กซิคิวต์ที่ฝั่งเซิร์ฟเวอร์ อาจจะเรียกการทำงานว่าเป็น Server Side ส่วนการทำงานของเบราว์เซอร์ของผู้ใช้เรียกว่า Client Side โดยการทำงานจะเริ่มต้นที่ผู้ใช้ส่งความต้องการผ่านเว็บเบราว์เซอร์ทาง HTTP ซึ่งอาจเป็นการกรอกแบบฟอร์ม หรือใส่ข้อมูลที่ต้องการ ข้อมูลเหล่านั้นจะเป็นเอกสาร PHP (เอกสารเหล่านี้จะมีส่วนขยายเป็น PHP หรือ PHP3 แล้วแต่ผู้กำหนด เช่น search.php เป็นต้น) เมื่อเอกสาร PHP เข้ามาถึงเว็บเซิร์ฟเวอร์ก็จะถูกส่งไปให้ PHP เพื่อทำหน้าที่แปลงคำสั่งแล้วเอ็กซิคิวต์คำสั่งนั้น หลังจากนั้น PHP จะสร้างผลลัพธ์ในรูปแบบเอกสาร HTML ส่งกลับไปให้เว็บเซิร์ฟเวอร์เพื่อส่งต่อไปให้เบราว์เซอร์แสดงผลทางฝั่งผู้ใช้ต่อไป (HTTP Response) ซึ่งลักษณะการทำงานแบบนี้ จะคล้ายกับการทำงานของ CGI (Common Gateway Interface) หรืออาจจะกล่าวได้ว่า PHP ก็คือ โปรแกรม CGI ประเภทหนึ่งก็ได้ ลักษณะการทำงานจะเป็นดังรูปข้างล่างนี้



รูปที่ 2.17 หลักการทำงานของ PHP

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## 2.8 Mail Server

Mail Server มีโปรโตคอลหลักที่ใช้ในการรับส่ง Email ในเครือข่ายอินเทอร์เน็ต คือ SMTP (Simple Mail Transport Protocol) ทำหน้าที่ รับและส่ง Email ระหว่าง Mail Server มี POP (Post Office Protocol) และ IMAP (Internet Messages Access Protocol) ช่วยอำนวยความสะดวก ในการที่ไม่ต้องใช้ telnet logon เข้ามายัง Mail Server เพื่ออ่านจดหมาย แต่ใช้ โปรแกรม Email Client เช่น Outlook Express, Eudora ในการอ่านจดหมายซึ่งสะดวกกว่า

การทำงานทั่ว ๆ ไปของ E-mail โดยสรุปมีเพียง 2 ประเภท คือ การส่ง E-mail และการรับ E-mail โดยโปรโตคอล SMTP (Simple Mail Transfer Protocol) จะใช้ขณะที่ User agent (ยูสเซอร์ เอเจนต์) ส่ง E-mail มาที่ MTA (Mail Transfer Agent) (เฉพาะแบบ offline) และใช้ในขณะรับและ ส่ง E-mail ระหว่าง MTA ด้วยกัน สำหรับการรับ mail แบบ offline คือเครื่องที่ผู้ใช้ใช้อ่าน mail ไม่ได้ติดต่อกับเครื่องที่มี mailbox ตลอดเวลา อาจเลือกดาวน์โหลด mail มาเก็บไว้ที่เครื่องของตัวเอง จะมีโปรโตคอลสำหรับรับ E-mail ที่เกี่ยวข้อง ที่ใช้งานกันแพร่หลาย มีอยู่ 2 แบบ คือ โปรโตคอล POP (Post Office Protocol) และ IMAP (Internet Message Access Protocol) ซึ่งจะทำหน้าที่ดาวน์โหลด หรืออัปโหลด (upload) จากเครื่องของผู้ใช้ไปยังเครื่องที่มี MTA อยู่

### 2.8.1 POP3

POP3 เป็นโปรโตคอลที่ทำหน้าที่โหลด E-mail มาจาก MTA ไปยัง User Agent ซึ่งในปัจจุบันได้พัฒนามาจนถึง version 3 แล้ว หรือเรียกย่อ ๆ ว่า POP3 (Post Office Protocol version 3) โปรโตคอลนี้เป็นตัวแรกที่ถูกออกแบบมาเพื่อใช้รับ E-mail และเพื่อให้สนับสนุนการทำงานแบบ offline ซึ่งกลไกของ POP3 นี้จะทำงานในแบบ Offline โดยติดต่อเข้าไปยัง mail server แล้ว ดาวน์โหลด E-mail ทั้งหมดมาไว้ที่ User Agent จากนั้นจะลบ E-mail ที่ server นั้นทิ้งไป เพื่อป้องกันการ download ซ้ำ แต่ผู้ใช้จะทำงานแบบ online กับ server ไม่ได้ เนื่องจากการอ่าน E-mail จะดึง E-mail ที่เก็บไว้ใน User Agent ขึ้นมาให้อ่านหลังจากที่ ดาวน์โหลด มาเก็บไว้ ซึ่งในขณะนั้น อาจไม่ได้ online อยู่กับ network ก็ได้

โปรโตคอลของ POP3 นี้จะทำงานในแบบของไคลเอนต์เซิร์ฟเวอร์ คือ มีโปรแกรม POP Server ใน mail server และ POP Client ในเครื่องของผู้รับ ซึ่งปกติจะฝังอยู่ใน โปรแกรมที่เป็น User Agent เลย โปรแกรมทั้ง 2 จะติดต่อกันโดยใช้คำสั่งที่เป็นรหัส ASCII คือเมื่อด้านที่รับทำคำสั่งก็จะทำงานตามคำสั่งนั้น แล้วตอบกลับมามีค่าเป็น (+OK) หมายถึง ทำงานได้เรียบร้อย หรือ (-ERR) หมายถึง เกิดปัญหาขึ้นทำงานไม่ได้ ซึ่งในคำสั่งที่ต้องมีการตอบกลับและส่งข้อมูลกลับมา โดยประกอบด้วยข้อมูลหลาย ๆ บรรทัดนั้น POP3 จะให้บรรทัดสุดท้ายเป็นเครื่องหมาย (.) ตามด้วย เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปเผยแพร่บนสื่อใด ๆ ไม่่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Carriage Return และ Line Feed หมายถึงการสิ้นสุดชุดข้อมูล แต่ในกรณีที่ข้อมูลบรรทัดสุดท้าย มีข้อมูลที่เป็นจุดด้วย จะใช้เทคนิคที่เรียกว่า Character Stuffing เพื่อแก้ปัญหา โดยจะเติมจุดลงไปอีก 1 ตัว เพื่อเป็นตัวบ่งชี้ว่าข้อมูลนั้นเป็นจุด ซึ่งจะแตกต่างจากสัญลักษณ์แสดงการสิ้นสุดของข้อมูล

การทำงานของ POP3 จะทำงานร่วมกับโปรโตคอล TCP (Transmission Control Protocol) โดยทั่วไป จะใช้ port 110 ในการติดต่อ ขั้นตอนการทำงานของ POP3 จะประกอบด้วย 3 สถานะ คือ สถานะขออนุมัติ, สถานะรับส่งรายการ และสถานะปรับปรุงข้อมูล ซึ่งในแต่ละสถานะจะรับรู้คำสั่งต่าง ๆ ของโปรโตคอลที่แตกต่างกัน ดังนี้

1. สถานะขออนุมัติ (Authorization State) เมื่อเริ่มต้นติดต่อกับเซิร์ฟเวอร์จะเป็นการ เข้าสู่สถานะการขออนุมัติ โดยไคลเอนต์จะต้องแจ้งชื่อผู้ใช้ และ รหัสผ่าน (password) เพื่อขออนุมัติจากเซิร์ฟเวอร์ก่อน โดยไคลเอนต์จะใช้คำสั่ง USER เพื่อระบุชื่อผู้ใช้ หรือคำสั่ง PASS เพื่อกำหนด Password แต่ในกรณีที่ชื่อ Password ถูกเข้ารหัสไว้ และไม่ได้เป็นค่า ASCII ทั่วไป ไคลเอนต์จะใช้คำสั่ง APOP ทำงานแทนคำสั่ง USER และ PASS

2. สถานะรับส่งรายการ (Transaction State) หลังจากที่ได้รับอนุมัติจากเซิร์ฟเวอร์แล้ว ก็จะเข้าสู่สถานะที่ใช้คำสั่งในการทำงานต่าง ๆ

3. สถานะปรับปรุงข้อมูล (Update State) เมื่อ User Agent เลิกใช้งานด้วยคำสั่ง QUIT ของ POP3 เซิร์ฟเวอร์ก็จะเข้าสู่สถานะปรับปรุงข้อมูล เพื่อลบอีเมลที่ดาวน์โหลดเรียบร้อยแล้วออกไป จากนั้นก็จะเข้าสู่สถานะขออนุมัติใหม่โดยอัตโนมัติ เพื่อรอรับการทำงานครั้งต่อไป

สถานะขออนุมัติ (Authorization State)

เมื่อ POP3 Client ติดต่อกับ POP3 Server ก็จะต้องแสดงบรรทัดติดต่อขึ้นมาบรรทัดหนึ่ง และบอกจุดสิ้นสุดด้วย CRLF (Carriage Return Line Feed) ตัวอย่างเช่น

s :+OK POP3 server read

เป็นการตอบรับของ POP3 ซึ่ง POP3 server จะแสดงเครื่องหมาย + บอกการตอบรับว่าในขณะนั้นสามารถให้บริการแก่ Client ตามที่ร้องขอ

เมื่อ POP3 อยู่ในสถานะ Authorization State แล้วก็จะทำการยืนยันแก่ POP3 server โดยมีวิธีการยืนยันอยู่สองวิธี คือ

- คำสั่ง USER รวมกับคำสั่ง PASS
- คำสั่ง APOP

การใช้คำสั่ง USER และคำสั่ง PASS ในขั้นแรก Client ต้องใช้คำสั่ง USER ก่อนถ้า POP3 Server ตอบมาด้วยสถานะบ่งชี้ว่าเป็นเครื่องหมาย + ("OK") เครื่อง client ก็จะใส่คำสั่ง PASS เข้าไปในการทำงานหรือคำสั่ง QUIT เพื่อบอกสถานะว่าหยุดการทำงานถ้าหากสถานะบ่งชี้เป็นเครื่องหมาย - ("ERR") เครื่อง Client ต้องส่งคำสั่งไปใหม่หรือยกเลิกโดยใช้คำสั่ง Quit ไปเลยก็ได้ เมื่อเครื่อง Client ส่งคำสั่ง Pass แล้ว POP3 Server จะใช้ทั้งคำสั่ง USER และ PASS เพื่อพิจารณาว่าเครื่องClientใดสามารถเข้าไปใช้งานภายใน Maildrop ได้

POP3 Server ได้มีการจำกัดการเข้าถึงใน Maildrop เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์เข้าไปทำการเปลี่ยนแปลงหรือลบข้อมูลใน Maildrop ก่อนจะเข้าสู่ช่วง Update State ถ้าการ lock สำเร็จ POP3 Server ก็จะตอบสนองด้วยสถานะการบ่งชี้ เป็น + ขณะนี้ POP3 ก็จะเข้าสู่ช่วง Transaction State ซึ่งไม่มี Message ที่ถูกทำเครื่องหมาย Delete ถ้าไม่สามารถเปิด Maildrop เนื่องจากเหตุผลบางประการ เช่น lock ไม่ได้, Client ปฏิเสธการเข้าถึง Maildrop ที่เหมาะสม หรือ Maildrop ไม่สามารถกระจายข้อมูลได้, Mail Server จะแสดงสถานะบ่งชี้เป็นเครื่องหมาย - ถ้ามีการ lock แต่ POP3 Server ยังแสดงสถานะบ่งชี้เป็นเครื่องหมายลบอยู่ จะต้องดูที่ลำดับการ LOCK ในการปฏิเสธคำสั่ง หลังจากได้รับตัวบ่งชี้สถานะเป็นเครื่องหมายลบ Server ก็จะปิดการติดต่อถ้า Server ยังไม่ปิดการติดต่อเครื่อง Client ก็จะส่งคำสั่งมาอีก หรือไม่ก็ใช้คำสั่ง Quit ออกไปเลยเมื่อ POP3 Server ได้เปิด Maildrop ก็จะส่งหมายเลข Message ไปยังแต่ละ Message ซึ่งขนาดของแต่ละ Messagee จะอยู่ในรูปของเลขฐาน 8 ข้อความแรกใน Maildrop จะได้รับหมายเลข Message เป็น 1 ลำดับที่สอง ก็เป็น 2 ตามลำดับไปเรื่อยๆ คำสั่ง POP3 และหมายเลขจะเป็นเลขฐาน 10

ตารางที่ 2.2 สรุปรายละเอียดของคำสั่งต่างๆใน POP3

คำสั่ง	พารามิเตอร์	สถานะ	รายละเอียด
USER	ชื่อผู้ใช้งาน	ขออนุมัติ	แจ้งชื่อผู้ใช้และระบุ Mailbox ที่จะใช้
PASS	Password	ขออนุมัติ	เป็นคำสั่งที่ใช้ระบุ Password โดยจะใช้ต่อจากคำสั่ง USER
APOP	ชื่อ, Password	ขออนุมัติ	ทำหน้าที่เหมือนคำสั่ง USER และ PASS รวมกันแต่ข้อมูลจะถูกเข้ารหัสก่อนส่งไป
STAT	ไม่ระบุ	รับส่งรายการ	เป็นคำสั่งตรวจสอบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

			สภาพเซิร์ฟเวอร์,ขนาดของอีเมลที่จะดาวน์โหลด
UIDL	หมายเลขข้อความ	รับส่งรายการ	ใช้ตรวจสอบหมายเลขประจำของอีเมล
LIST	หมายเลขข้อความ	รับส่งรายการ	ใช้ตรวจสอบหมายเลขของอีเมล และขนาดของอีเมล
RETR	ข้อความ	รับส่งรายการ	เป็นคำสั่งที่ใช้ส่งข้อมูลของอีเมล
DELE	ข้อความ	รับส่งรายการ	เป็นการระบุเครื่องหมายการลบลงในอีเมลที่จะลบและอีเมลเหล่านั้นจะถูกลบออกจากเมลบ็อกซ์เมื่อใช้คำสั่ง QUIT เมื่อสิ้นสุดการทำงาน
RSET	ไม่ระบุ	รับส่งรายการ	คำสั่งนี้จะยกเลิกเครื่องหมายการลบอีเมลที่เคยกำหนดไว้ด้วยคำสั่ง DELE ออกไปทุก ๆ อีเมล
TOP	หมายเลขข้อความ,จำนวนบรรทัด	รับส่งรายการ	เซิร์ฟเวอร์จะส่งข้อมูลย้อนกลับไปที่เท่ากับจำนวนบรรทัดที่ระบุ
NOOP	ไม่ระบุ	รับส่งรายการ	เป็นคำสั่ง No Operation
QUIT	ไม่ระบุ	รับส่งรายการและขออนุมัติ	ใช้เมื่อจบการทำงาน หากมีอีเมลซึ่งทำเครื่องหมายว่าจะลบไว้ อีเมลเหล่านั้นจะถูกลบจากเมลบ็อกซ์ในขั้นตอนนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### 2.8.2 SMTP

SMTP เป็นโปรโตคอลที่ใช้ส่งอีเมลล์จาก User agent ของผู้ส่งไปยัง MTA ของผู้ส่ง และส่งต่อไปยัง MTA เครื่องอื่น ๆ ที่เป็นจุดผ่านในการเชื่อมต่อไปยังเครื่องของผู้รับ โปรโตคอล SMTP จะทำงานร่วมกับโปรโตคอล TCP โดยใช้พอร์ต 25 ซึ่งคำสั่งต่าง ๆ ของ SMTP จะเป็นลักษณะเดียวกับ POP3 คือเป็น ASCII ลงท้ายด้วย Carriage Return และ Line Feed ส่วนข้อความที่ตอบกลับมาจะนำหน้าด้วยเลข 3 หลัก เป็นสัญลักษณ์แสดงลักษณะการทำงานของคำสั่งที่ได้รับ

เมื่อเริ่มต้นการติดต่อ SMTP จะกำหนดให้ User Agent ของผู้ส่งต้องส่งคำสั่ง HELLO พร้อมกับรายละเอียดด้านผู้ส่งออกไป จากนั้นจะส่งคำสั่ง MAIL เพื่อแจ้งให้เซิร์ฟเวอร์เตรียมรับอีเมลล์ ในส่วนของเซิร์ฟเวอร์เมื่อพร้อมที่จะรับอีเมลล์ก็ตอบรับอีเมลล์ที่รับอีเมลล์ก็ตอบรับกลับมาด้วยคำสั่ง OK จากนั้นที่ด้านส่งก็จะเริ่มส่งโดยใช้คำสั่ง RCPT เพื่อกำหนดอีเมลล์แต่ละฉบับไปที่ส่งไป ซึ่งการส่งข้อมูลของอีเมลล์ก็จะระบุด้วยคำสั่ง DATA

การส่งอีเมลล์ของโปรโตคอล SMTP ได้จัดเตรียมคำสั่งอื่น ๆ ไว้เพื่ออำนวยความสะดวกและคล่องตัวในการทำงาน ซึ่งประกอบด้วย คำสั่ง VRFY เพื่อให้ด้านที่ส่งตรวจสอบรายชื่อว่าผู้ใช้รายนี้มีสิทธิใช้งาน E-mailbox นั้น ๆ หรือไม่ , คำสั่ง EXPN ใช้จัดการและตรวจสอบรายชื่อจากลิสต์รายชื่อ และคำสั่ง TURN ใช้สลับให้ Client ของผู้ส่งทำหน้าที่รับข้อมูลจากเซิร์ฟเวอร์แทน

เมื่อได้รับคำสั่งต่างๆ ของผู้ส่งแล้ว เซิร์ฟเวอร์จะมีหน้าที่ตรวจสอบความถูกต้องของคำสั่ง จากนั้น จึงทำงานตามคำสั่ง แล้วส่งผลตอบกลับมา ส่วนลักษณะของข้อมูลที่ตอบกลับ (Reply Message) นั้นจะเป็นข้อมูลที่อยู่ในรูปของ Text ที่เป็น ASCII โดยจะประกอบด้วยตัวเลข นำหน้าข้อความสามหลัก ทำหน้าที่แสดงสถานะการทำงานของเซิร์ฟเวอร์ และเปลี่ยนสถานะการทำงานของโปรโตคอล SMTP ด้วย ถัดจากตัวเลขจะคั่นด้วยช่องว่างแล้วตามด้วยเครื่องหมาย Carriage Return และ Line Feed ตัวอย่างเช่น 500 Syntax error, command unrecognized หมายถึง คำสั่งที่ส่งไปไม่ถูกต้อง หรือ 503 Bad sequence of commands หมายถึง ลำดับการส่งคำสั่งไม่ถูกต้องเหล่านี้ เป็นต้น

ในการส่ง (E-mail) ของโปรโตคอล SMTP นั้น จะใช้วิธีอ้างถึงเซิร์ฟเวอร์อื่น ๆ ตามแบบ DNS (Domain Name System) เช่นเดียวกับระบบอื่น ๆ ในอินเทอร์เน็ต และยังสามารถส่งอีเมลล์ไปยังผู้รับคนเดียวหรือหลาย ๆ คนพร้อมกันได้ด้วย

ตารางที่ 2.3 แสดงรายละเอียดในคำสั่งต่าง ๆ ของ SMTP ที่ใช้งานอยู่

คำสั่ง	รายละเอียด
DATA	จะเป็นคำสั่งที่ใช้ต่อจาก RCPT เพื่อส่งข้อมูลของอีเมล
SEND	ทำหน้าที่เหมือนคำสั่ง DATA แต่ไม่ค่อยมีผู้ใช้งาน
SOML	ทำหน้าที่เหมือนคำสั่ง DATA แต่ไม่ค่อยมีผู้ใช้งาน
SAML	ทำหน้าที่เหมือนคำสั่ง DATA แต่ไม่ค่อยมีผู้ใช้งาน
VERFY	เป็นคำสั่งที่ใช้เพื่อตรวจสอบความถูกต้องของชื่อและเมลี่บ็อกซ์
EXPN	เป็นคำสั่งเพื่อตรวจสอบรายละเอียดของลิสต์รายชื่อ
HELP	ใช้ตรวจสอบคำสั่งที่สามารถใช้งานได้กับเซิร์ฟเวอร์
NOOP	เป็นคำสั่ง No Operation เมื่อเซิร์ฟเวอร์ได้รับคำสั่งนี้จะตอบ OK กลับมา
QUIT	สิ้นสุดการติดต่อ
RSET	ยกเลิกการส่งข้อมูลในขณะนี้
TURN	เป็นคำสั่งที่สลับหน้าที่ของผู้ส่งข้อมูลมาทำหน้าที่รับข้อมูลแทน
RCPT	เป็นคำสั่งเพื่อระบุอีเมลที่จะส่งทีละฉบับ โดยเป็นคำสั่งที่ใช้ต่อจาก MAIL

#### SMTP Reply Codes ( ตัวเลขแสดงสถานะของคำสั่ง )

- 211 System status, or system help reply
- 214 Help message
- 220 Service ready
- 221 Service closing transmission channel
- 250 Requested mail action okay ,completed
- 251 User not local ; will forward to
- 354 Start mail input ; end with .
- 421 Service not available, closing transmission channel
- 450 Request mail action not taken : mailbox unavailable
- 451 Request action aborted : local error in processing
- 452 Requested action not taken : insufficient system storage
- 500 Syntax error in parameters or arguments

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- 501 Syntax error in parameters or arguments
- 502 Command not implemented
- 503 Bad sequence of commands
- 504 Command parameter not implemented
- 550 Requested action not taken : mailbox unavailable
- 551 User not local ; please try
- 552 Requested mail action aborted : exceeded storage allocation
- 553 Requested action not taken : mailbox name not allowed
- 554 Transaction failed

### 2.8.3 IMAP

IMAP ก็คือ ผู้ใช้สามารถเลือกดาวน์โหลดเฉพาะ (E-Mail) ที่ต้องการได้ โดยไม่จำเป็นต้องโหลดมาทั้งหมดเหมือนโปรโตคอล POP3 นอกจากนี้ IMAP ยังสามารถรองรับการทำงานได้ทั้งแบบ Offline, Online และแบบ Disconnected อีกด้วย ดังนั้นประโยชน์ที่ได้จาก IMAP ก็คือ หากผู้ใช้มีอีเมลแอดเดรสเพียงข้อเดียว แต่มีเครื่องที่ใช้งานอยู่หลายเครื่องก็จะสามารถเลือกดาวน์โหลดเฉพาะอีเมลที่ต้องการมาเก็บไว้ที่เครื่องใดก็ได้ แต่ถ้าเป็น POP3 การดาวน์โหลดจะต้องทำพร้อมกันหมดทุกอีเมล ดังนั้น IMAP จึงเป็นโปรโตคอลที่สามารถทำงานกับสายสื่อสารที่มีความเร็วต่ำได้เป็นอย่างดี

การทำงานของ IMAP นี้เหมือนกับโปรโตคอลอื่น ๆ โดยทำงานร่วมกับ TCP ใช้พอร์ตหมายเลข 143 และแบ่งเป็นสถานะต่าง ๆ ออกเป็น 4 สถานะ โดยในแต่ละสถานะมีวัตถุประสงค์และคำสั่งที่ใช้งานแตกต่างกัน มีรายละเอียดต่าง ๆ ดังนี้

1. สถานะก่อนอนุมัติ (Non-authenticated State) เป็นสถานะที่คำสั่งขอให้ไคลเอนต์ติดต่อเข้ามาเพื่อขออนุมัติใช้ ดังนั้นในด้านไคลเอนต์จะต้องแจ้งชื่อล็อกอิน (Login) ของ Mail Server นั้น และ password (พาสเวิร์ด) ด้วยคำสั่ง LOGIN หรือ AUTHENTICATE ก่อนจึงจะเริ่มใช้งานได้ จากนั้นจึงเปลี่ยนไปเป็นสถานะได้รับการอนุมัติ

2. สถานะได้รับการอนุมัติ (Authenticated State) เป็นสถานะที่สามารถใช้คำสั่งต่าง ๆ ที่เกี่ยวกับการเลือกและใช้งานเมลบ็อกซ์ เช่น คำสั่ง SELECT เพื่อเลือกเมลบ็อกซ์ หรือคำสั่ง CREATE เพื่อสร้างเมลบ็อกซ์ เป็นต้น ในการเลือกเมลบ็อกซ์ด้วยคำสั่ง SELECT หรือ EXAMINE นี้จะเปลี่ยนไปเป็นสถานะการเลือกเมลบ็อกซ์

3. สถานะการเลือกเมลล์บ็อกซ์ (Selected State) เป็นสถานะที่จะเข้าใช้งานอีเมลในแต่ละเมลล์บ็อกซ์ หลังจากที่เลือกเมลล์บ็อกซ์ไว้แล้วในสถานะก่อนหน้านี้

4. สถานะเลิกใช้งาน (Logout State) เมื่อต้องการเลิกใช้งาน หรือสิ้นสุดการทำงานของ IMAP จะเข้าสู่สถานะเลิกใช้งานโดยใช้คำสั่ง LOGOUT

จากสถานะทั้ง 4 นี้ไม่จำเป็นต้องทำงานเรียงต่อกันเสมอไปบางครั้งอาจจะมีการทำงานข้ามจากสถานะหนึ่งไปยังอีกสถานะหนึ่งได้ ตัวอย่างเช่น เมื่อเข้าสู่สถานะที่ได้รับการอนุมัติ (Authenticate State) และลบอีเมลที่ไม่ต้องการใช้งานทิ้งไปด้วยคำสั่ง DELETE แล้วและไม่ต้องการทำงานอื่น ๆ ก็ยังสามารถใช้คำสั่ง LOGOUT เพื่อเปลี่ยนสถานะเป็นเลิกการใช้งาน (Logout State) ได้โดยไม่จำเป็นต้องเข้าสู่สถานะการเลือกเมลล์บ็อกซ์ (Selected State) ก่อน ซึ่งจะเรียกว่า Untagged response หรือ Asterisk tag (\*) ส่วนคำตอบของเซิร์ฟเวอร์ที่เป็นผลการทำงานตามคำสั่งต่าง ๆ ของไคลเอนต์นั้น จะประกอบด้วยคำสั่งทั้งหมด 5 แบบ คือ

- OK แสดงว่าผลการทำงานของคำสั่งนั้น ๆ สำเร็จและเรียบร้อยแล้ว
- NO แสดงว่าการทำงานตามคำสั่งนั้นไม่สำเร็จ
- BAD แสดงว่าคำสั่งที่ส่งไปไม่ถูกต้อง หรือมีพารามิเตอร์ไม่ถูกต้อง
- PREAUTH แสดงว่าไม่จำเป็นต้องใช้คำสั่ง LOGIN เพราะเคยมีการสถานะที่ได้รับการอนุมัติ (Authenticated State) แล้ว
- BYE แสดงว่าเซิร์ฟเวอร์ได้จบการทำงานไปแล้ว

## 2.9 FTP Server

FTP เป็นคำย่อมาจากภาษาอังกฤษว่า File Transfer Protocol เป็นการถ่ายโอนเพิ่มข้อมูลระหว่างเครื่องคอมพิวเตอร์ 2 เครื่อง ซึ่งอยู่บนเครือข่ายอินเทอร์เน็ต ในระบบเครือข่ายอินเทอร์เน็ต มีเครื่องคอมพิวเตอร์ที่ให้บริการการถ่ายโอนเพิ่มข้อมูลเป็นสาธารณะ มีอยู่เป็นจำนวนมาก เรียกเครื่องคอมพิวเตอร์ที่ให้บริการถ่ายโอนเพิ่มข้อมูลนี้ว่า FTP Server

คำสั่งต่างๆที่ใช้ใน FTP

- คำสั่ง dir (สำหรับโปรแกรม FTP ที่เรียกใช้จากคอส หรือ วินโดว์)  
dir เป็นคำสั่งสำหรับดูชื่อเพิ่มข้อมูลและชื่อไดเรกทอรีใน เครื่องคอมพิวเตอร์ปลายทาง

```
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
total 5
lrwx--x--x 3 root    daenon    512 Jan 31 17:33 bin
lrwx--x--x 2 root    daenon    512 Jan 31 17:30 dev
lrwx--x--x 2 root    daenon    512 Jan 31 17:34 etc
lrwxr-xr-x 10 root    daenon    512 Feb  6 11:10 pub
lrwx--x--x 3 root    daenon    512 Jan 31 17:37 usr
226 Transfer complete.
304 bytes received in 0.066 seconds (4.5 Kbytes/s)
ftp>
```

- คำสั่ง `cd` [ไคเรคทอรี]

`cd` เป็นคำสั่งที่ใช้เปลี่ยนไปยัง ไคเรคทอรีย่อยของเครื่องคอมพิวเตอร์ปลายทาง ที่ต้องการ

```
ftp> cd pub
250 CWD command successful.
ftp> cd pics/bmp
250 CWD command successful.
```

- คำสั่ง `cd ..` หรือ `cdup`

`cd ..` หรือ `cdup` เป็นคำสั่งที่ใช้เปลี่ยนไคเรคทอรีขึ้นไปอีกหนึ่งระดับของ เครื่องคอมพิวเตอร์ปลายทาง

```
ftp> cd..
250 CWD command successful.
```

- คำสั่ง `get` [ชื่อแฟ้มต้นทาง] [ชื่อแฟ้มปลายทาง]

`get` เป็นคำสั่งที่ใช้คัดลอกแฟ้มจากคอมพิวเตอร์ปลายทาง ไปยังคอมพิวเตอร์ต้นทาง ในกรณีที่พิมพ์ชื่อแฟ้มปลายทาง เครื่องจะตั้งชื่อแฟ้มปลายทางเหมือนกับชื่อแฟ้มต้นทาง

```
ftp> get door.bmp door.bmp
200 PORT command successful.
150 Opening ASCII mode data connection
226 Transfer complete.
local: door.bmp remote: door.bmp
163958 bytes received in 0.84 seconds (
ftp>
```

- คำสั่ง `mget` [ชื่อแฟ้ม] [ชื่อแฟ้ม]

`mget` เป็นคำสั่งคัดลอก แฟ้มหลาย ๆ แฟ้มจาก คอมพิวเตอร์ปลายทางตาม รูปแบบที่กำหนดมาที่คอมพิวเตอร์ต้นทาง โดยเครื่องจะถามความต้องการที่ละแฟ้มข้อมูล

ถ้าไม่ต้องการให้เครื่องถามทีละไฟล์ให้ใช้คำสั่ง prompt เข้าช่วย

```
ftp> prompt
Interactive mode off.
ftp> mget *.bmp
```

- คำสั่ง quit หรือ bye

quit หรือ bye เป็นคำสั่งที่ใช้ออกจาก ftp

ตารางที่ 2.4 คำสั่งต่างที่ใช้ใน FTP

? [คำสั่ง] / help [คำสั่ง]	แสดงข้อความช่วยเหลือ อธิบายคำสั่งใน ftp
ascii	คัดลอกเพิ่มข้อมูลแบบแอสกี
binary	คัดลอกเพิ่มข้อมูลแบบไบนารี
bell	ให้ส่งเสียงเมื่อคัดลอกเพิ่มข้อมูลเสร็จ
bye	จบการทำงานและออกจาก ftp
cd [ไดเรกทอรี]	เปลี่ยน ไดเรกทอรี ของคอมพิวเตอร์ปลายทาง
cd .. หรือ cdup	เปลี่ยน ไดเรกทอรีของคอมพิวเตอร์ปลายทางขึ้นไปหนึ่งระดับ
lcd [ไดเรกทอรี]	เปลี่ยน ไดเรกทอรีของคอมพิวเตอร์ปลายทาง
close หรือ disconnect	จบการเชื่อมต่อกับคอมพิวเตอร์ปลายทางแต่ยังไม่ออกจาก ftp
dir [ชื่อเพิ่ม]	แสดงรายชื่อเพิ่มของคอมพิวเตอร์ปลายทาง
get [ชื่อเพิ่ม] [ชื่อเพิ่ม]	คัดลอกเพิ่มจากคอมพิวเตอร์ปลายทางมาที่คอมพิวเตอร์ต้นทาง
mget [ชื่อเพิ่ม] [ชื่อเพิ่ม]	คัดลอกเพิ่มจากคอมพิวเตอร์ปลายทางมาที่คอมพิวเตอร์ต้นทางแบบหลายเพิ่ม
put [ชื่อเพิ่ม] [ชื่อเพิ่ม]	คัดลอกเพิ่มจากคอมพิวเตอร์ต้นทางไปไว้ที่คอมพิวเตอร์ปลายทาง
mput [ชื่อเพิ่ม] [ชื่อเพิ่ม]	คัดลอกเพิ่มจากคอมพิวเตอร์ต้นทางไปไว้ที่ คอมพิวเตอร์ปลายทางแบบหลายเพิ่ม
prompt [on] [off]	กำหนดให้มี การโต้ตอบกับผู้ใช้เพื่อเลือกเพิ่มเมื่อใช้ mget ,mput
pwd	แสดงไดเรกทอรีของรีโมตโฮสต์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### 2.9.1 VSFTP

FTP มีหลากหลายชนิด ไม่ว่าจะเป็น WU-FTP, ProFTP, หรือ BSD-FTP ล้วนมีช่องโหว่ที่ถูกค้นพบมากมาย จึงทำให้มีความเสี่ยงต่อการถูกผู้ไม่ประสงค์ดีโจมตีได้ อย่างไรก็ตาม มีอีกโปรแกรมหนึ่งชื่อ VSFTP ซึ่งมีอุปชันด้านความปลอดภัยสำหรับเซิร์ฟเวอร์ FTP ที่เป็น Linux/UNIX ดังนั้น VSFTP จึงเป็นอีกทางเลือกหนึ่งที่ต้องติดตั้งเซิร์ฟเวอร์ FTP และต้องการความปลอดภัยยิ่งขึ้น

#### คุณสมบัติของVSFTP

VSFTP เป็นเดมอน (daemon) ของเซิร์ฟเวอร์ FTP ที่รันบนระบบปฏิบัติการ Linux/UNIX ซึ่งมีคุณสมบัติหลักอยู่ 3 อย่าง ได้แก่

- มีความปลอดภัย
- มีประสิทธิภาพดี
- มีความมั่นคง

ในแง่ของความปลอดภัยนั้น VSFTP ได้ถูกออกแบบมาเพื่อแก้ไขจุดบกพร่องที่พบในการติดตั้ง wu-ftpd, proftpd, และแม้แต่ bsd-ftpd โดยการไม่ใช้บัญชีชื่อ root ซึ่งมีความเสี่ยง และใช้คุณสมบัติด้านความปลอดภัยที่มีประสิทธิภาพอย่าง chroot นอกจากนี้ยังมีการใช้เทคนิคการพัฒนาโปรแกรมอย่างปลอดภัยเพื่อแก้ปัญหาหน่วยความจำล้น (buffer overflows) ด้วย และนอกจากนี้ยังมีการกล่าวถึง vsftpd ในแง่ของความปลอดภัยมากมาย ดังต่อไปนี้

- vsftpd ไม่มีจุดบกพร่องชื่อ "globbing" ซึ่งมีผลกระทบต่อเซิร์ฟเวอร์ FTP หลายแห่ง
- vsftpd ไม่มีจุดบกพร่องชื่อ "globbing" ที่เกี่ยวข้องกับการโจมตีแบบ denial of service

วิธีเริ่มต้นการทำงานของ VSFTP

VSFTP สามารถรันได้ 2 โหมด ได้แก่

1. โหมด stand-alone
2. โหมด inetd/xinetd

การรันผ่านเดมอน inetd หรือ xinetd สามารถควบคุมการทำงานของโปรแกรมได้ง่ายกว่า และเป็นวิธีที่ควรใช้มากกว่าแบบ stand-alone สิ่งสำคัญที่ต้องคำนึงถึงคือ ในการตั้งค่าของ VSFTP นั้น มันจะรับการเชื่อมต่อแบบ anonymous เท่านั้น (สมมติว่าได้สร้างบัญชีชื่อ "ftp" ไปก่อนหน้าแล้ว) ดังนั้นถ้าต้องการอนุญาตให้บัญชีผู้ใช้ในเครื่องสามารถเชื่อมต่อเข้ามาใช้งาน ftp ได้ จะต้องทำการตั้งค่า Pluggable Authentication Modules (PAM) ซึ่งจะกล่าวถึงต่อไปด้วย

### 1.การทำงานแบบ stand-alone

สิ่งที่ต้องทำสำหรับการรัน VSFTP ในโหมด stand-alone ได้แก่

- เพิ่มประโยค "listen = YES" ไว้ในบรรทัดสุดท้ายของไฟล์ /etc/vsftpd.conf
- รันคำสั่ง # /usr/local/sbin/vsftpd &

### 2.การใช้ xinetd

เนื่องจากในที่นี่ได้ทำการทดสอบและใช้งานบนระบบ Red Hat 9 (ซึ่งใช้ xinetd) ดังนั้นจะเน้นที่การดำเนินการติดตั้งในโหมด xinetd

- กรณีรัน inetd
  - เพิ่มบรรทัดต่อไปนี้ในไฟล์ /etc/inetd.d

```
ftp stream tcp nowait root /usr/local/sbin/vsftpd
```

  - รีสตาร์ทเดมอน inetd ด้วยคำสั่ง

```
# kill -SIGHUP <pid of inetd>
```
- กรณีรัน xinetd
  - ไฟล์คอนฟิกกูเรชันสำหรับการเริ่มต้นทำงานของ VSFTP ในเครื่องที่รัน xinetd นั้น อยู่ภายใต้ไคเรกทอรี /etc/xinetd.d โดยมีชื่อว่า vsftpd หากไม่พบไฟล์ดังกล่าว ให้ทำการสำเนาจากตัวอย่างของ vsftpd ที่มากับ VSFTP distribution (/tmp/vsftpd-1.2.0/xinetd.d/vsftpd) มาไว้ในไคเรกทอรีนี้ ในไฟล์ vsftpd นี้ มีพารามิเตอร์จำนวนหนึ่งภายใต้ "service ftp" ซึ่งระบุให้ทราบวิธีการทำงานของเซิร์ฟเวอร์ VSFTP ดังต่อไปนี้

ตารางที่ 2.5 แสดงพารามิเตอร์ภายใต้ service ftp

พารามิเตอร์	ค่าที่กำหนด	ความหมาย
socket_type	stream	เป็นชนิดของ TCP socket ที่ใช้สำหรับ โพรโตคอลนี้ นั่นคือ FTP เป็น TCP stream
wait	no	เกี่ยวกับความสามารถสำหรับ socket ที่จะรับข้อความ
user	root	ผู้ใช้ที่จะเป็นผู้เปิดให้บริการ ftp คือใคร (ในที่นี้คือ root) หมายเหตุ : VSFTP จะลดสิทธิลงทันทีที่เริ่มทำงาน
server	/usr/local/sbin/vsftpd	เป็นตำแหน่งของ โปรแกรมเซิร์ฟเวอร์ที่เกี่ยวข้องกับไฟล์คอนฟิกกูเรชันนี้ ถ้ามีการตั้ง vsftpd ในไคเรกทอรีที่แตกต่างออกไปก็ต้องแก้ไขเปลี่ยนแปลงค่านี้
nice	10	ออปชันนี้ใช้แก้ไขลำดับตารางเวลาดีฟอลต์สำหรับ โพรเซส โดย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		10 คือค่าดีพอลต์ ส่วนค่าสูงสุดคือ 20
disable	no	เซิร์ฟเวอร์นี้ไม่ถูกปิด หรืออีกนัยหนึ่งคือ มันควรเริ่มทำงานทันทีเมื่อ xinetd เริ่มต้นทำงาน
per_source	5	เป็นการระบุจำนวนของการเชื่อมต่อเข้ามาใช้งานในเวลาเดียวกัน จากหมายเลข IP เดียวกัน โดยเพื่อความปลอดภัย ควรตั้งค่าไว้เป็น 5
instances	200	กำหนดจำนวนสูงสุดของการเชื่อมต่อ FTP ไปยังเซิร์ฟเวอร์ในเวลาเดียวกัน ซึ่งมีประโยชน์ต่อการกำหนดโหลดการทำงานของเซิร์ฟเวอร์ โดยเพื่อความปลอดภัยควรตั้งค่าไว้เป็น 200
no_access	No default	เป็นการระบุรายการ IP address ที่ไม่อนุญาตให้เข้าถึงเซิร์ฟเวอร์นี้ เช่น 192.168.1.4

-เมื่อปรับแก้ไฟล์ /etc/xinetd.d/vsftpd เรียบร้อยแล้วให้ทำการรีสตาร์ท xinetd ด้วยคำสั่ง

```
# /etc/init.d/xinetd restart
```

หรือ

```
# service xinetd restart
```

- และเพื่อให้ xinetd เริ่มทำงานทุกครั้งที่เรารีสตาร์ท ให้ใช้คำสั่งต่อไปนี้

```
# chkconfig --add xinetd
```

```
# chkconfig --level 345 xinetd on
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

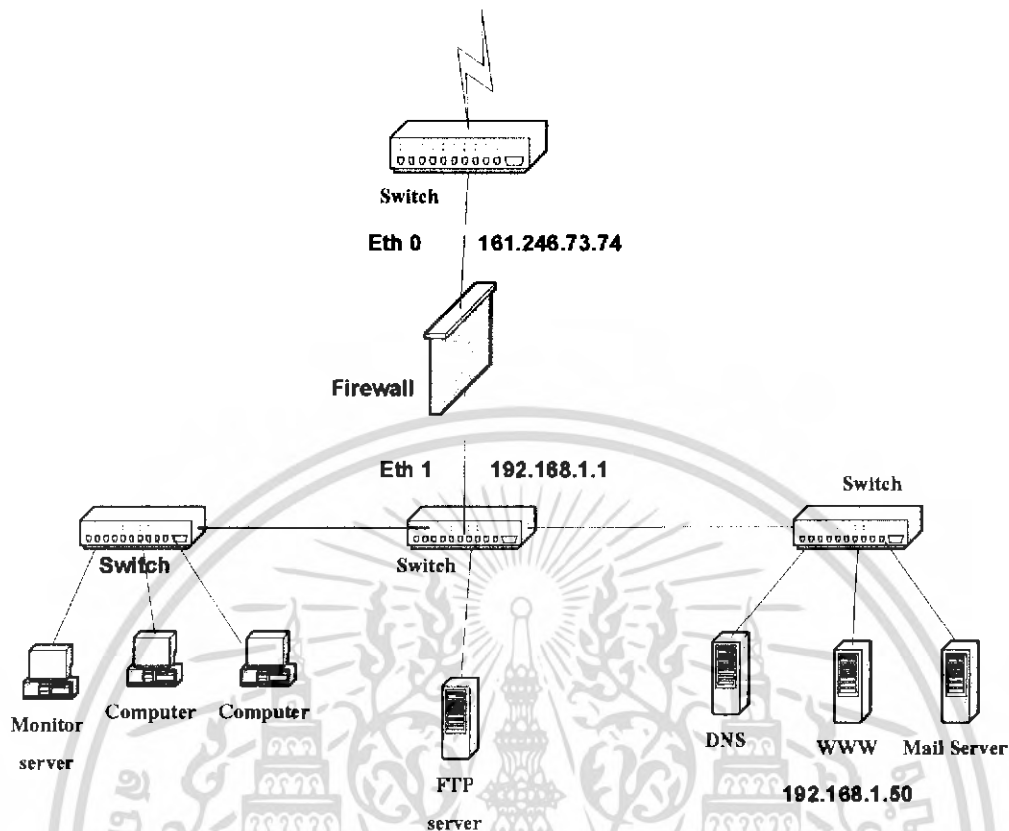
## บทที่ 3

### การออกแบบระบบเครือข่าย

#### 3.1 ขั้นตอนการออกแบบระบบเครือข่าย

1. วิเคราะห์ความต้องการของผู้ใช้ในระบบเครือข่ายห้องวิจัย ความต้องการของผู้ใช้ ได้แก่
  - ต้องการระบบเครือข่ายภายในที่เป็นสัดส่วน แยกจากเครือข่ายภายนอกอย่างชัดเจน
  - ต้องการความปลอดภัยจากการบุกรุกจากบุคคลภายนอกที่ไม่หวังดี
  - ต้องการความปลอดภัยจากการโจมตีจากเครือข่ายภายนอก เช่น ไวรัส โทรเจน
  - ต้องการความสะดวกสบายในการใช้งานเครือข่าย ไม่พบปัญหาในการใช้งาน เช่น การชนกันของไอพี
  - มีการดูแลเรื่อง client ภายในระบบเครือข่าย เช่น การแจ้งเตือนไวรัส
  - ต้องการความสะดวกสบายในการใช้งาน มีบริการต่าง ๆ ในระบบเครือข่าย
  - ต้องการความปลอดภัยระดับสูงแก่เซิร์ฟเวอร์ฐานข้อมูล
2. ศึกษาข้อบกพร่องของระบบเครือข่ายเดิมเพื่อทำการพัฒนาให้ดีขึ้น
3. ออกแบบระบบเครือข่ายเพื่อใช้งานในห้องวิจัย โดยคำนึงถึง
  - ประสิทธิภาพ (Efficiency)
  - ความเป็นประโยชน์ (Available)
  - ความน่าเชื่อถือ (Reliable)
  - ระดับความปลอดภัย
  - งบประมาณ
  - ความยากง่ายในการจัดการและตั้งค่า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.1 ระบบเน็ตเวิร์คที่ออกแบบมาสำหรับห้องวิจัย

จากรูปจะเห็นว่าเป็นระบบเครือข่ายภายใน ที่มีการแยกออกจากเครือข่ายภายนอก โดยใช้ไอพีแอดเดรสที่เป็น Private IP ซึ่งเป็นไอพีที่ไม่สามารถเชื่อมต่อกับเครือข่ายภายนอกได้โดยตรง ดังนั้นจึงต้องทำ NAT (Network Address Translation) เพื่อแปลง Private IP เป็น Public IP และแปลง Public IP เป็น Private IP เพื่อติดต่อกับเครือข่ายภายนอก

การออกแบบเครือข่ายประกอบด้วย

### 3.2 การออกแบบไฟร์วอลล์

ในการออกแบบได้ใช้ไฟร์วอลล์เพื่อเพิ่มความปลอดภัยและเสถียรภาพ ของระบบเครือข่ายภายใน

ไฟร์วอลล์จะเชื่อมต่อกับเครือข่ายภายนอก ซึ่งมีหน้าที่ คือ เป็นเราต์เทอร์ในการหาเส้นทาง และกำหนดกฎการเข้า-ออก ของแพ็กเก็ตของข้อมูล และทำการแปลงแอดเดรสระหว่าง Private IP และ Public IP ซึ่งมีกฎดังนี้

สำหรับแพ็กเก็ตขาเข้า (Inbound Packet)

กำหนดให้กฎดีฟอลต์ ซึ่งเป็นกฎสุดท้ายเมื่อเงื่อนไขแพ็กเก็ตที่ผ่านเข้ามาไม่ตรงกับเงื่อนไขใด ๆ เลย ให้เป็น ขกเลิก (DROP) คือ ไม่ยอมให้แพ็กเก็ตนั้นผ่านเข้ามายังตัวไฟร์วอลล์ได้

INPUT Chain (แพ็กเก็ตที่อนุญาตให้ผ่านเข้ามาได้)

ตารางที่ 3.1 บอกลิงก์แพ็กเก็ตที่อนุญาตให้ผ่านเข้ามาได้

Input Interface	Output Interface	Protocol	Match	Source	Destination	Port	Target
Eth0	-	TCP	-	Any	161.246.73.74	22	ACCEPT
Eth1	-	TCP	-	Any	192.168.1.1	22	ACCEPT
Eth0,Eth1	-	ICMP type 8 (request)	Limit 10/minute	Any	Any		ACCEPT
Eth0,Eth1	-	ICMP type 0 (reply)	Limit 10/minute	Any	Any		ACCEPT
Eth0,Eth1	-	TCP(syn)	Limit 1/s	Any	Any		ACCEPT
Eth0,Eth1	-	-	State ESTABLISHED,RELATED	-	-		ACCEPT
Eth0	-	-	state NEW	-	-		DROP

แพ็กเก็ตที่อนุญาตให้ผ่านเข้ามาได้ แสดงดังตารางที่ 3.1 ซึ่งมีการทำงานดังนี้

- บรรทัดที่หนึ่งเป็นการอนุญาตให้ข้อมูลแพ็กเก็ตเป็นโพรโตคอล TCP พอร์ต 22 (shell) ที่มาจากอินเทอร์เน็ตเฟสภายนอก (Eth0) และปลายทางเป็น 161.246.73.74 ผ่านเข้ามายังตัวไฟร์วอลล์ได้
- บรรทัดที่สองเป็นการอนุญาตให้ข้อมูลแพ็กเก็ตเป็นโพรโตคอล TCP พอร์ต 22 (shell) ที่มาจากอินเทอร์เน็ตเฟสภายใน (Eth1) และปลายทางเป็น 192.168.1.1 ผ่านเข้ามายังตัวไฟร์วอลล์ได้
- บรรทัดที่สามและบรรทัดที่สี่ เป็นการอนุญาตให้ข้อมูลแพ็กเก็ตที่เป็นโพรโตคอล ICMP Type 8,0 ซึ่งเป็น Echo Request และ Echo Reply สามารถผ่านเข้ามายังตัวไฟร์วอลล์ได้ โดยจำกัดจำนวนครั้ง 10 ครั้ง/นาที เพื่อป้องกันการโจมตีแบบ PING FLOOD

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- บรรทัดที่ห้าเป็นอนุญาตให้ข้อมูลแพ็กเก็ตเป็นโพรโทคอล TCP ซึ่งติดต่อโดยวิธี Three Ways Handshake สามารถส่งแพ็กเก็ต SYN ติดต่อกันได้สูงสุดไม่เกิน 1 ครั้ง/วินาที เพื่อป้องกันการโจมตีแบบ SYN FLOOD
- บรรทัดที่หกเป็นอนุญาตให้ข้อมูลแพ็กเก็ตต่าง ๆ ที่ไม่ได้เกิดจากการเริ่มต้นการติดต่อจากเครือข่ายภายนอก สามารถผ่านเข้ามายังไฟร์วอลล์ได้
- บรรทัดที่เจ็ดเป็นการตรวจสอบแพ็กเก็ตที่มาจากภายนอกว่าเป็นแพ็กเก็ตที่เป็นตัวสร้าง การติดต่อใหม่หรือไม่ ถ้าใช่จะไม่ให้ผ่านไปยังไฟร์วอลล์ (DROP)

สำหรับแพ็กเก็ตขาออก (Outbound Packet)

กำหนดให้กฎคิฟอล์ทซึ่งเป็นกฎสุดท้ายเมื่อเงื่อนไขแพ็กเก็ตที่ผ่านเข้ามาไม่ตรงกับเงื่อนไขใด ๆ เลข ให้เป็นยอมรับ (accept) คือ ขอมให้แพ็กเก็ตนั้นผ่านเข้ามายังตัวไฟร์วอลล์ได้

OUTPUT Chain (แพ็กเก็ตที่อนุญาตให้ผ่านออกไปได้)

ตารางที่ 3.2 บอกลังแพ็กเก็ตที่อนุญาตให้ผ่านออกไปได้

Input Interface	Output Interface	Protocol	Match	Source	Destination	Port	Target
-	Any	Any	-	Any	Any	Any	ACCEPT

แพ็กเก็ตที่อนุญาตให้ผ่านออกไปได้ แสดงดังตารางที่ 3.2

สำหรับแพ็กเก็ตส่งต่อ (Forward Packet)

กำหนดให้กฎคิฟอล์ท ซึ่งเป็นกฎสุดท้ายเมื่อเงื่อนไขแพ็กเก็ตที่ผ่านเข้ามาไม่ตรงกับเงื่อนไขใด ๆ เลข ให้เป็นยอมรับ คือ ขอมให้แพ็กเก็ตนั้นผ่านเข้ามายังตัวไฟร์วอลล์ได้ เพื่อให้ง่ายต่อการกำหนดกฎ จึงแบ่งการกฎการส่งต่อ เป็น 2 ชนิด คือ ชนิดที่ส่งจากเครือข่ายภายนอกไปยังเครือข่ายภายใน ซึ่งในที่นี้จะตั้งชื่อกฎนี้ว่า EXTRANET-KMITL และชนิดที่ส่งจากเครือข่ายภายในไปยังเครือข่ายภายนอก ซึ่งในที่นี้จะตั้งชื่อกฎนี้ว่า EXTRANET-KMITL

FORWARD Chain (บอกลังแพ็กเก็ตส่งต่อ)

ตารางที่ 3.3 บอกลังแพ็กเก็ตส่งต่อ

Input Interface	Output Interface	Protocol	Match	Source	Destination	Port	Target

Eth0	Eth1	Any	-	Any	Any	Any	EXTRANET-KMITL
Eth1	Eth0	Any	-	Any	Any	Any	KMITL-EXTRANET

แพ็กเก็ตที่บอกถึงแพ็กเก็ตส่งต่อ แสดงดังรูป 3.3 ซึ่งมีการทำงานดังนี้

- บรรทัดที่หนึ่งเป็นการให้แพ็กเก็ตข้อมูลใด ๆ ที่มาจากอินเตอร์เฟซภายนอก (Output Interface) ที่เป็น Eth0 และจะส่งต่อไปยังอินเตอร์เฟซภายใน (Input Interface) ที่เป็น Eth1 กระโดดไปยัง chain ที่ชื่อว่า EXTRANET-KMITL
- บรรทัดที่สองเป็นการให้แพ็กเก็ตข้อมูลใด ๆ ที่มาจากอินเตอร์เฟซภายใน (Input Interface) ที่เป็น Eth1 และจะส่งต่อไปยัง อินเตอร์เฟซภายนอก (Output Interface) ที่เป็น Eth0 กระโดดไปยัง chain ที่ชื่อว่า KMITL-EXTRANET

#### EXTRANET-KMITL

ตารางที่ 3.4 บอกถึงกฎของการติดต่อกับ EXTRANET ไป KMITL

Input Interface	Output Interface	Protocol	Match	Source	Destination	Port	Target
-	-	-	State ESTABLISHED,RELATED	-	-	-	ACCEPT
-	-	TCP	-	Any	161.246.73.75	80	ACCEPT
-	-	TCP	-	Any	192.168.1.50	80	ACCEPT
-	-	Any	-	Any	Any		DROP

แพ็กเก็ตที่บอกถึงกฎของการติดต่อกับ EXTRANET ไป KMITL แสดงดังรูป 3.4 ซึ่งมีการทำงานดังนี้

- บรรทัดที่หนึ่งเป็นการอนุญาตให้ข้อมูลแพ็กเก็ตต่าง ๆ ที่ไม่ได้เกิดจากการเริ่มต้นการติดต่อกับเครือข่ายภายนอก สามารถผ่านเข้ามายังเครือข่ายภายในได้
- บรรทัดที่สองและบรรทัดที่สามเป็นการอนุญาตให้ข้อมูลแพ็กเก็ตใด ๆ ที่มีปลายทางเป็น 161.246.73.75 พอร์ต 80 สามารถผ่านเข้ามายังเครือข่ายภายใน เพื่อใช้งานเว็บเบราว์เซอร์ได้ และอนุญาตให้ข้อมูลแพ็กเก็ตใด ๆ ที่มีปลายทางเป็น 192.168.1.50 พอร์ต 80 สามารถผ่านเข้ามายังเครือข่ายภายใน เพื่อใช้งานเว็บเบราว์เซอร์ได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- บรรทัดที่สี่ถ้าในกรณีที่แพ็กเก็ตที่กำลังจะเข้ามาไม่ตรงกับเงื่อนไขใด ๆ เลข ก็จะยกเลิกไม่ให้ข้อมูลนั้น ผ่านเข้ามายังเครือข่ายภายในได้ (DROP)

#### KMITL-EXTRANET

ตารางที่ 3.5 บอกรหัสกฎของการติดต่อจาก KMITL ไป EXTRANET

Input Interface	Output Interface	Protocol	Match	Source	Destination	Port	Target
-	-	TCP	-	192.168.1.50	Any	Any	ACCEPT
-	-	UDP	-	192.168.1.50	Any	Any	ACCEPT
-	-	-	State ESTABLISHED,RELATED	Any	Any	Any	ACCEPT
-	-	Any	-	Any	Any	Any	DROP

แพ็กเก็ตที่บอกรหัสกฎของการติดต่อจาก KMITL ไป EXTRANET แสดงดังรูป 3.5 ซึ่งมีการทำงานดังนี้

- บรรทัดที่หนึ่งและบรรทัดที่สอง เป็นการอนุญาตให้ข้อมูลแพ็กเก็ตต่างๆ ทั้งโพรโทคอล TCP และ UDP ที่มาจากแอดเดรสต้นทางคือ 192.168.1.50 สามารถติดต่อกับเครือข่ายภายนอกได้
- บรรทัดที่สามเป็นการอนุญาตให้ข้อมูลแพ็กเก็ตต่าง ๆ ที่ไม่ได้เกิดจากการเริ่มต้นการติดต่อจากเครือข่ายภายนอก สามารถผ่านเข้ามายังเครือข่ายภายในได้
- บรรทัดที่สี่ถ้าในกรณีที่แพ็กเก็ตที่กำลังจะเข้ามา ไม่ตรงกับเงื่อนไขใด ๆ เลข ก็จะยกเลิกไม่ให้ข้อมูลนั้น ผ่านเข้ามายังเครือข่ายภายนอกได้ (DROP)

#### ตาราง NAT

ตารางที่ 3.6 เป็นการสร้างกฎต่างๆของการทำ NAT

CHAIN	Input Interface	Output Interface	Protocol	Source	Destination	Port	To Address	Target
PREROUTING	Eth0	Eth1	-	161.246.73.75	-	80	192.168.1.50	-
PREROUTING	Eth0	-	Any	10.0.0.0/8	Any	Any	-	DROP
PREROUTING	Eth0	-	Any	127.0.0.0/8	Any	Any	-	DROP
PREROUTING	Eth0	-	Any	172.16.0.0/12	Any	Any	-	DROP
PREROUTING	Eth0	-	Any	192.168.1.0/16	Any	Any	-	DROP
POSTROUTING	Eth1	Eth0	Any	192.168.1.0/24	Any	Any	161.246.73.77- 161.246.73.80	-

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แพ็คเกจที่บอกถึงการสร้างกฎต่างๆของการทำ NAT แสดงดังรูป 3.6 ซึ่งมีการทำงานดังนี้

- ในตาราง NAT ประกอบด้วย PREROUTING CHAIN และ POSTROUTING CHAIN
- กำหนดให้ PREROUTING CHAIN เป็นการส่งแพ็คเกจข้อมูล จากอินเตอร์เฟซภายนอก ที่เป็น Eth0 และจะส่งต่อไปยังอินเตอร์เฟซภายในที่เป็น Eth1
- และ POSTROUTING CHAIN เป็นการส่งแพ็คเกจข้อมูล จาก อินเตอร์เฟซภายในที่เป็น Eth1 ส่งต่อไปยัง อินเตอร์เฟซภายนอกที่เป็น Eth0
- มีการทำ static NAT จากแอดเดรสต้นทาง 161.246.73.75 แปลงเป็นแอดเดรส 192.168.1.50 พอร์ต 80 เพื่อใช้งานเว็บเซิร์ฟเวอร์
- และมีการป้องกันการปลอม IP (IP spoofing) ใน PREROUTING CHAIN คือ ถ้ามีแพ็คเกจข้อมูลมาจากอินพุตอินเตอร์เฟซและมีแอดเดรสเป็น 10.0.0.0/8 127.0.0.0/8 172.16.0.0/12 192.168.1.0/16 ซึ่งเป็น private IP ให้ทำการยกเลิกข้อมูลนั้น

ในโครงการนี้ได้ใช้คอมพิวเตอร์ส่วนบุคคลทำหน้าที่เป็นไฟร์วอลล์ภายนอก โดยมีสเปคเครื่องคอมพิวเตอร์ดังนี้

- ซีพียู : Pentium4 3.0GHz
- แรม : 512 MHz
- ฮาร์ดดิสก์ : 40GHz

เทคโนโลยีที่เลือกใช้

- ใช้ระบบปฏิบัติการลินุกซ์เนื่องจาก เป็นระบบปฏิบัติการ โอเพ่นซอร์ส (Opensource) ที่มีเสถียรภาพสูง มีฟังก์ชันการทำงาน ที่ทำหน้าที่เป็นไฟร์วอลล์ด้วย
- ใช้โปรแกรม IPtables ที่เป็น โอเพ่นซอร์ส ในการกำหนดนโยบายต่าง ๆ (Policy )
- InterScan Viruswall (ISVW) ทำหน้าที่ป้องกันไวรัส โดยตรวจสอบที่ HTTP, SMTP และ FTP Service
- โปรแกรม MRTG (Multi Router Traffic Grapher) เพื่อช่วยงานในส่วนของการมอนิเตอร์ และรวบรวมข้อมูลจากระบบเครือข่าย

โปรแกรม MRTG (Multi Router Traffic Grapher) ซึ่งสามารถมอนิเตอร์ระบบเครือข่าย นำข้อมูลมารวบรวมไว้ และนำเสนอเป็นรูปกราฟผ่าน เว็บเพจ โดยผู้จัดการระบบสามารถมอนิเตอร์ข้อมูลผ่าน โปรแกรมเว็บเบราว์เซอร์ได้ทันที แต่คุณสมบัติเหล่านี้ไม่ได้เกิดจากตัวโปรแกรม MRTG

แต่เพียงลำพัง ยังต้องอาศัยโปรแกรมอื่น ๆ เข้ามาสนับสนุนอีกจึงจะสามารถทำงานที่กล่าวไว้ได้ครบถ้วนสมบูรณ์ ซึ่งมีลำดับการทำงานดังนี้

อันดับแรก การที่จะรวบรวมข้อมูลต่าง ๆ จากระบบเครือข่ายมาได้ จำเป็นต้องอาศัยเครื่องมืออะไรก็ได้ที่ทำหน้าที่เป็นตัวแทนของเรา หรือที่ เรียกว่า Agent ใฝ่จับตาความเปลี่ยนแปลงของระบบเครือข่าย และส่งข้อมูลออกมาให้ทราบ ซึ่งโดยปกติจะอาศัยโปรโตคอล SNMP (Simple Network Management Protocol) ซึ่งเป็นคุณสมบัติหนึ่งภายในอุปกรณ์ Router หรือ Switches ทำหน้าที่เป็น Network Management Server

ต่อมาตัวโปรแกรม MRTG จะอ่านข้อมูลผ่าน SNMP Agent ตามระยะเวลาการสุ่มข้อมูลที่กำหนดไว้ แล้วพล็อตกราฟ เป็นไฟล์รูปภาพ เก็บไว้ที่ไดเรกทอรีที่กำหนดไว้

สุดท้ายโปรแกรมที่ทำหน้าที่เป็นเว็บเซิร์ฟเวอร์จะนำเสนอข้อมูลกราฟที่สร้างจาก MRTG ผ่านทางโปรโตคอล HTTP ทำให้สามารถดูกราฟแสดงรายงานการใช้แบนด์วิธได้จากโปรแกรมเว็บเบราว์เซอร์

### 3.3 การออกแบบเว็บเซิร์ฟเวอร์, DNS เซิร์ฟเวอร์ และ เมล์เซิร์ฟเวอร์

เว็บเซิร์ฟเวอร์, DNS เซิร์ฟเวอร์ และ เมล์เซิร์ฟเวอร์ อยู่ในส่วนของเครือข่ายภายในที่มีการทำ Static NAT ผ่านทางไฟร์วอลล์ภายนอก

#### 1. เว็บเซิร์ฟเวอร์

เว็บเซิร์ฟเวอร์ สร้างขึ้นสำหรับบริการการใช้งานต่าง ๆ ให้กับอาจารย์และนักศึกษาภายในห้องวิจัยแบบไร้สาย เช่น โสมเพจสร้างขึ้นเพื่อให้อาจารย์และนักศึกษาภายในห้องวิจัยสามารถค้นหาหรือดาวน์โหลดข้อมูลเกี่ยวกับ Ultra Wideband ได้ง่ายและสะดวกยิ่งขึ้น ทั้งนี้ยังได้จัดทำเว็บบอร์ดขึ้นมาเพื่อให้นักศึกษาที่มีปัญหาหรือคำถามที่เกี่ยวกับ Ultra Wideband ได้มาตั้งกระทู้คำถามไว้บนเว็บบอร์ดได้

#### 2. DNS เซิร์ฟเวอร์

DNS เป็นระบบแปลงหมายเลขไอพีแอดเดรสให้อยู่ในรูปแบบของ โดเมนเนมหรือ แปลงกลับจากโดเมนเนมไปเป็นไอพีแอดเดรสได้ หลังจากที่ได้ลงทะเบียนชื่อโดเมนผ่านISPเรียบร้อยแล้ว ในที่นี้ได้ทำการประกาศสับโดเมน (Subdomain) ชื่อ wis.ite.kmitl.ac.th

#### 3. เมล์เซิร์ฟเวอร์

เมล์เซิร์ฟเวอร์ มีหน้าที่ในการจัดการรับส่งอีเมลล์ของผู้ใช้ภายในห้องวิจัย ทำให้การใช้งานอีเมลล์มีความยืดหยุ่นขึ้น โดยมีแอดเดรสเป็น user@wis.ite.kmitl.ac.th

ในโครงการนี้ได้ใช้คอมพิวเตอร์ส่วนบุคคล ทำหน้าที่เป็นเซิร์ฟเวอร์ โดยมีสเปกเครื่องดังนี้

- ซีพียู : Pentium4 3.0GHz
- แรม : 512 MHz
- ฮาร์ดดิสก์ : 80GHz

เทคโนโลยีที่เลือกใช้

- ใช้ระบบปฏิบัติการลินุกซ์ เนื่องจากเป็นระบบปฏิบัติการ โอเพ่นซอร์สที่มีระบบปฏิบัติการลินุกซ์ เนื่องจากเป็นระบบปฏิบัติการโอเพ่นซอร์สที่มีเสถียรภาพสูง มีฟังก์ชันการทำงาน ที่ทำหน้าที่เป็นไฟร์วอลล์ได้
- Apache Web Server เป็นเว็บเซิร์ฟเวอร์เพราะเป็นโอเพ่นซอร์สและใช้งานง่าย
- PHP เป็น Script สำหรับเขียน \*.php
- MySQL สำหรับจัดการฐานข้อมูล
- PHPMyAdmin สำหรับจัดการระหว่าง PHP และ MySQL
- ใช้ Bind เป็น DNS เซิร์ฟเวอร์ เนื่องจากเป็น โอเพ่นซอร์ส
- ใช้ โปรแกรม Postfix ในการจัดการบริการ SMTP
- ใช้ โปรแกรม ClamAV เป็น Antivirus
- ใช้โปรแกรม Amavisd-New เป็น Antivirus Scanner สำหรับเป็นตัวกลางระหว่าง Postfix และ ClamAV
- ใช้โปรแกรม Squirrel Mail ในการบริหารจัดการเว็บเบสสำหรับติดต่อกับผู้ใช้เมลล์ผ่านเว็บ

### 3.4 การออกแบบมอนิเตอร์เซิร์ฟเวอร์

เป็นเซิร์ฟเวอร์ที่ทำหน้าที่ดูแลจัดการคอมพิวเตอร์ของผู้ใช้ภายในเครือข่าย ทำหน้าที่เป็น DHCP เซิร์ฟเวอร์ สำหรับ แจกไอพีให้แก่เครื่องไคลเอนต์แบบอัตโนมัติและมีโปรแกรมตรวจจับไวรัสในเครือข่ายภายใน สามารถแจ้งเตือนแก่ผู้ใช้ในระบบ มีการเก็บล็อกข้อมูลต่าง ๆ ของการใช้งานระบบเครือข่ายของบุคลากร เพื่อป้องกันและตรวจสอบข้อผิดพลาดการใช้งาน

ในโครงการนี้ได้ใช้คอมพิวเตอร์ส่วนบุคคล ทำหน้าที่เป็นมอนิเตอร์เซิร์ฟเวอร์ โดยมีสเปกเครื่องคอมพิวเตอร์ดังนี้

- ซีพียู : Pentium4 3.0GHz
- แรม : 512 MHz
- ฮาร์ดดิสก์ : 40GHz

เทคโนโลยีที่เลือกใช้

- ใช้ระบบปฏิบัติการ Windows Server 2003 เนื่องจาก เป็นระบบปฏิบัติการที่สามารถติดต่อกับผู้ใช้ได้สะดวก และมีโปรแกรมสนับสนุนมากมาย
- ใช้โปรแกรม Trend Micro ในการตรวจจับไวรัสในเครือข่าย

OfficeScan ทำหน้าที่ป้องกันไวรัสบนเครือข่าย โดยผู้บริหารสามารถจัดการเครื่องลูกข่ายต่างๆ เหล่านี้ได้จากจุดศูนย์กลาง เพื่อง่ายต่อการจัดการ

### 3.5 การออกแบบเซิร์ฟเวอร์ข้อมูล

เป็นเซิร์ฟเวอร์ที่ทำหน้าที่เก็บข้อมูลต่างๆหรือ Thesis สำหรับอาจารย์ในห้องวิจัย ซึ่งมีความสำคัญระดับสูง

ในโครงการนี้ได้ใช้คอมพิวเตอร์ส่วนบุคคล ทำหน้าที่เป็นเซิร์ฟเวอร์ฐานข้อมูล โดยมีสเปคเครื่องคอมพิวเตอร์ดังนี้

- ซีพียู : Pentium4 3.0GHz
- แรม : 512 MHz
- ฮาร์ดดิสก์ : 40GHz

เทคโนโลยีที่เลือกใช้

- ระบบปฏิบัติการลินุกซ์เนื่องจากเป็นระบบปฏิบัติการ โอเพ่นซอร์สที่มีเสถียรภาพสูง
- VSFTP (Very Scure FTP) สำหรับจัดการด้าน FTP ที่มีความปลอดภัยสูง

### 3.6 การออกแบบโฮมเพจ

เนื่องจากภายในห้องวิจัย Wireless Communication Research Group ต้องการโฮมเพจเพื่อให้บุคลากรภายในและภายนอกสามารถมาหาความรู้เกี่ยวกับ Ultra Wide Band ได้อย่างสะดวก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ดังนั้นในโครงการนี้จึงได้คิดสร้างโฮมเพจสำหรับห้องวิจัย Wireless Communication Research Group ขึ้นมา โดยในโฮมเพจประกอบด้วย

- Member (สมาชิก) จะบอกว่ามีบุคคลากรท่านไหนบ้างที่เป็นสมาชิกอยู่ในห้องวิจัยนี้
- Publicist (ผลงานวิจัย) จะบอกถึงบทความวิจัยที่ตีพิมพ์ในวารสารในประเทศและต่างประเทศ
- Links (ลิ้งค์) ซึ่งภายในจะมี links ไปยังที่สำคัญต่างๆที่มีประโยชน์สำหรับห้องวิจัย
- Webmail (เว็บเมล) ซึ่งจะ links ไปยัง Webmail ที่โครงการนี้สร้างขึ้นมาเพื่อบริการเกี่ยวกับการรับส่งอีเมลล์

นอกจากนี้ยังได้สร้างหน้าล็อกอินเพื่อให้ผู้ที่เป็สมาชิกของห้องวิจัยเท่านั้นที่สามารถเข้าไปยังหน้าที่สามารถตั้งเว็บบอร์ดและดาวน์โหลดผลงานวิจัยต่างๆได้ โดยหน้าล็อกอินจะให้กรอกชื่อและ password ถ้าบุคคลใดยังไม่มีการลงทะเบียนใหม่ (New Register) โดยทำการกรอกตามแบบฟอร์มที่สร้างขึ้นเพื่อกำหนด user name และ password แล้วค่อยนำมาใช้ในล็อกอิน ซึ่งเมื่อล็อกอินเสร็จแล้วสามารถตั้งกระทู้ต่างๆได้ โดยอยู่ในการดูแลของผู้ดูแลระบบ ถ้ามีข้อความไม่เหมาะสม ผู้ดูแลระบบเท่านั้นที่สามารถลบกระทู้นี้ได้ หรือจะล็อกอินเข้ามาเพื่อดูว่านโหลดผลงานวิจัยต่างๆมาศึกษาได้

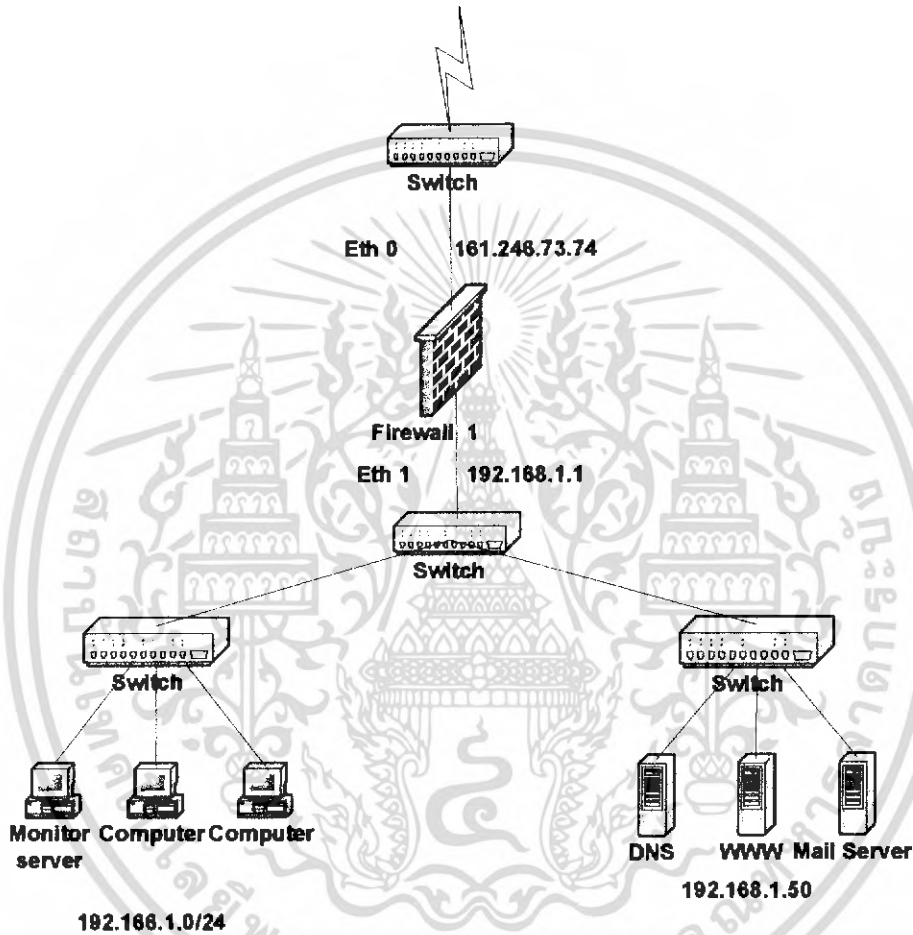
และเมื่อทำการสร้างโฮมเพจเสร็จเรียบร้อยแล้วจะนำไปลงที่ Web Server โดยใช้ Apache Web Server เนื่องจากเป็นเว็บเซิร์ฟเวอร์ที่มีประสิทธิภาพสูง และนิยมใช้มากที่สุด นอกจากนี้ยังใช้ Script language คือ PHP เพราะเป็นไออน์เซอร์สและสามารถติดต่อกับฐานข้อมูลที่ใช้ในโครงการได้ (MySQL)

## บทที่ 4

### ผลการทดลอง

#### 4.1 การจัดการระบบเครือข่ายภายใน

ได้ทำการสร้างเครือข่ายหลักเพียงบางส่วนของกรออกแบบทั้งหมด ซึ่งได้แก่



รูปที่ 4.1 ระบบเน็ตเวิร์ค

จากรูปได้ทำการออกแบบระบบเน็ตเวิร์ค โดยมีรายละเอียดดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

#### 4.1.1 ไฟร์วอลล์

ประกอบด้วย 2 อินเทอร์เฟซสำหรับใช้ในการติดต่อ 2 อัน คือ Eth0 ซึ่งจะมีไอพีแอดเดรส เป็น 161.246.73.74 netmask เป็น 255.255.255.0 เพื่อติดต่อกับเครือข่ายภายนอก และ Eth1 จะมี ไอพีแอดเดรส เป็น 192.168.1.1 netmask เป็น 255.255.255.0 เพื่อติดต่อกับเครือข่ายภายใน โดยมีหน้าที่ คือ

- เป็นเราต์เตอร์ในการหาเส้นทาง
- กำหนดกฎการเข้า-ออก ของแพ็กเก็ตของข้อมูล
- NAT สำหรับ แปลง ไอพีแอดเดรสของเครือข่ายภายใน ให้เป็น ไอพีแอดเดรส ซึ่งเป็นที่ยอมรับที่สามารถสื่อสารบนอินเทอร์เน็ตได้

#### 4.1.2 เว็บเซิร์ฟเวอร์ , DNS เซิร์ฟเวอร์ และ เมล์เซิร์ฟเวอร์

มีไอพีแอดเดรส เป็น 192.168.1.50 netmask เป็น 255.255.255.0 จะทำการแปลงไอพีแอดเดรส (static NAT) จาก 161.246.73.75 เป็น 192.168.1.50 ก่อนที่เครือข่ายภายนอกจะเข้าสู่เว็บเซิร์ฟเวอร์ได้

โดยมีหน้าที่ คือ

- เว็บเซิร์ฟเวอร์ สำหรับโฮมเพจ และ เว็บแอปพลิเคชัน เพื่อบริการผู้ใช้
- DNSเซิร์ฟเวอร์ สำหรับแปลงหมายเลขไอพีแอดเดรสให้อยู่ในรูปของโดเมนเนม หรือ แปลงกลับจากโดเมนเนมไปเป็นไอพีแอดเดรส และประกาศโดเมนลูกของห้องวิจัยเป็น “wis.ite.kmitl.ac.th”
- เมล์เซิร์ฟเวอร์ สำหรับจัดการรับส่งอีเมลล์สำหรับผู้ใช้ในเครือข่าย

#### 4.1.3 มอนิเตอร์เซิร์ฟเวอร์

มีไอพีแอดเดรสเป็น 192.168.1.51 netmask เป็น 255.255.255.0

โดยมีหน้าที่ คือ

- ดูแลจัดการคอมพิวเตอร์ของผู้ใช้ภายในเครือข่าย
- มีโปรแกรมตรวจจับไวรัสในเครือข่ายภายใน สามารถแจ้งเตือนแก่ผู้ใช้ในระบบ
- มีการเก็บล็อกข้อมูลต่าง ๆ ของการใช้งานระบบเครือข่ายของผู้ใช้
- DHCP เซิร์ฟเวอร์ สำหรับแจก ไอพีให้แก่เครื่องไคลเอ็นต์แบบอัตโนมัติ

#### 4.1.4 เซิร์ฟเวอร์ข้อมูล

มีไอพีแอดเดรสเป็น 192.168.1.52 netmask เป็น 255.255.255.0

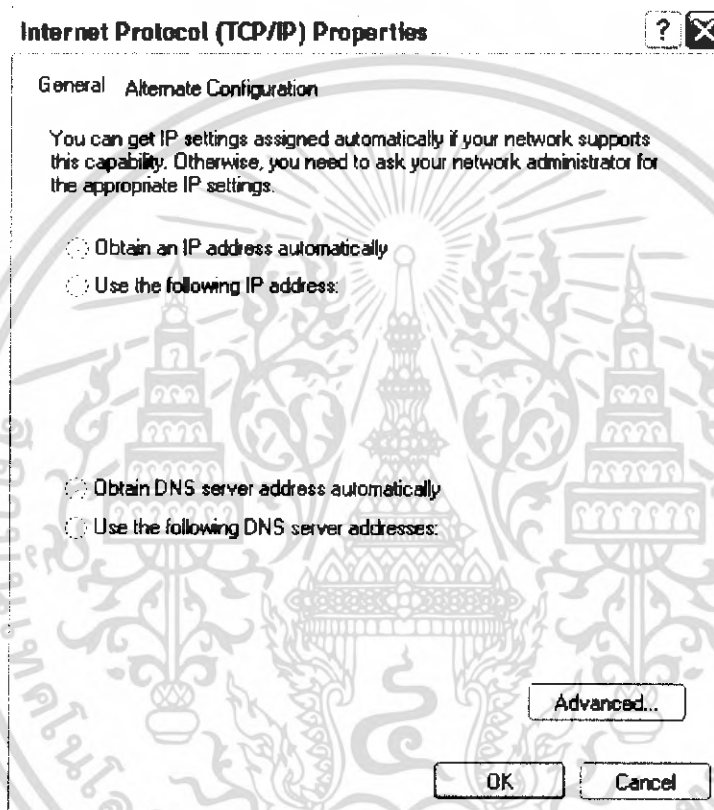
โดยมีหน้าที่ คือ

- เก็บข้อมูลของผู้ใช้ภายในเครือข่าย ที่มีความปลอดภัยสูง

## 4.2 ผลการทดลองระบบเครือข่าย

### 4.2.1 DHCP เซิร์ฟเวอร์

การใช้งาน DHCP



รูปที่ 4.2 ผู้ใช้รับไอพีแอดเดรสอัตโนมัติ

จากรูปที่ 4.2 เป็นการให้ผู้ใช้ที่เครื่องไคลเอนต์เข้าไปที่ Internet Protocol (TCP/IP) Properties และเลือก Obtain an IP Address automatically เพื่อรับไอพีแอดเดรสอัตโนมัติจาก DHCP เซิร์ฟเวอร์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.3 ผู้ใช้ได้รับไอพีแอดเดรส

จากรูปที่ 4.3 เป็นการตรวจสอบหมายเลขไอพีแอดเดรสของเครื่องไคลเอนต์ที่ได้รับการแจกจาก DHCP เซิร์ฟเวอร์ เรียบร้อยแล้ว

#### 4.2.2 NAT และ ไฟร์วอลล์



รูปที่ 4.4 การติดต่อกับเครือข่ายภายนอก โดยผ่าน NAT และ ไฟร์วอลล์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หลังจากได้ทำการสร้าง NAT และ ไฟร์วอลล์ เพื่อให้ผู้ใช้ที่อยู่เครือข่ายภายใน สามารถติดต่อกับเครือข่ายภายนอกได้อย่างสะดวก ปลอดภัย และเครือข่ายภายนอกไม่สามารถมองเห็นเครือข่ายภายในได้ ซึ่งในกรณีนี้จะมีกฎการเข้าออกแพ็กเก็ตเปิดให้ติดต่อเฉพาะเว็บเซิร์ฟเวอร์เท่านั้น จากรูปที่ 4.4 ได้แสดงการติดต่อกับเครือข่ายภายนอกโดยผ่าน NAT และ ไฟร์วอลล์ ที่สร้างขึ้น

### 4.2.3 เว็บเซิร์ฟเวอร์

The screenshot shows a web browser window with the address bar displaying 'http://161.246.73.75/'. The page header includes the name of King Mongkut's Institute of Technology Ladkrabang. The main content area is titled 'Ultra Wide Band Radio System Laboratory' and contains several announcements:

- IWUWBT 2005:** 2005 International Workshop on UWB Technologies (IWUWBT 2005) will be held at Yokosuka Research Park (YRP), Yokosuka, Japan on December 8-10, 2005. Camera-ready submission due, September 15, 2005. Early Registration: Up to November 8, 2005.
- WCRG Welcome Party:** เว็บบอร์ด WCRG เข้าร่วมงานตั้งแต่วันที่ 10 มิถุนายน 2548 เวลาและสถานที่จะแจ้งให้ทราบเร็วๆ นี้
- ISCIT 2005:** International Symposium on Communications and Information Technologies 2005 (ISCIT 2005) will be held at International Convention Center, Beijing, China on October 12-14, 2005. Submission of full paper -> June 15, 2005.

On the left side, there is a 'Login' section with a 'Log in' button and a 'Reset' button. On the right side, there is a 'Calendar' for March 2006 and a 'Link' section.

รูปที่ 4.5 เว็บเซิร์ฟเวอร์

จากรูป เป็นเว็บเซิร์ฟเวอร์ที่ภายในประกอบด้วยเนื้อหาเกี่ยวกับเรื่อง Ultra Wideband รวมถึงลิงค์ต่างๆที่เป็นประโยชน์เช่น เว็บไซต์ที่น่าสนใจสำหรับบุคคลที่สนใจเกี่ยวกับเรื่อง Ultra Wideband นี้ เป็นต้น

## 4.2.4 DNS เซิร์ฟเวอร์

Microsoft Windows [Version 5.0.2600.5512] Copyright (c) 2006 Microsoft Corporation. All rights reserved.  
 Microsoft Internet Explorer  
 File Edit View Favorites Tools Help  
 Back Forward Stop Search Favorites Print  
 http://wis.ite.kmitl.ac.th

EPSON Web-To-Page Print Print Preview

วิทยาลัยเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง  
 King Mongkut's Institute of Technology Ladkrabang

Ultra Wide Band Radio System Laboratory

Calendar  
 march 2006  

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Link

Log in Reset

News Register

WUWBT 2005, 2005 International Workshop on UWB Technologies (IWUWBT 2005) will be held at Yokosuka Research Park (YRP), Yokosuka, Japan on December 8-10, 2005. Camera-ready submission due: September 15, 2005. Early Registration: Up to November 8, 2005

WCRG Welcome Party เชิญสมาชิก WCRG เข้าร่วมงานตั้งแต่วันที่ 10 มิถุนายน 2548 เวลาและสถานที่จะแจ้งให้ทราบเร็วๆ นี้

ISCT 2005, International Symposium on Communications and Information Technologies 2005 (ISCT 2005) will be held at International Convention Center, Beijing, China on October 12-14, 2005. Submission of full paper -> June 15, 2005.

รูปที่ 4.6 ประกาศโดเมนลูกเป็น wis.ite.kmitl.ac.th

ในการทำ DNS เซิร์ฟเวอร์ ได้มีการประกาศโดเมนลูก ซึ่งจากรูปที่ 4.6 จะเห็นได้ว่าได้ประกาศโดเมนลูกให้เป็น wis.kmitl.ac.th ซึ่งทำขึ้นสำหรับห้องวิจัยแบบไร้สายโดยเฉพาะ โดยจะต้องไปทำการจดทะเบียนที่ศูนย์วิจัย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## 4.2.5 มอนิเตอร์เซิร์ฟเวอร์

The screenshot shows the Trend Micro OfficeScan Corporate Edition web interface. The browser title is "Trend Micro OfficeScan Corporate Edition - Microsoft Internet Explorer". The address bar shows "http://192.168.1.51/officeScan/cgi/CM/MasterPwd.exe". The interface includes a navigation menu on the left with options like "Scan Now", "Update Now", "Activate how", and "Restore to Normal". The main content area displays "Client Status" with "Total number of clients : 0" and "Infected clients : 0". Below this, there are sections for "Top Ten Clients with Virus Incidents", "Top Ten Viruses Detected", and "Last Virus Detected", each with a circular placeholder for a chart. At the bottom, there are links for "Home", "Support", "Security Info", and "About", along with the Trend Micro logo.

รูปที่ 4.7 โปรแกรมในการตรวจจับไวรัสหรือความผิดปกติในเครือข่าย

จากรูปเป็นการจัดการดูแลเครื่องไคลเอนต์ ในการตรวจจับไวรัส หรือความผิดปกติภายในเครือข่าย โดยใช้โปรแกรม Trend Micro OfficeScan

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

http://192.168.1.51 - Scan Now - Microsoft Internet Explorer

Scan Now

Click the **Start Notification** button to request the selected clients to perform a manual scan.

Start Notification

Stop Scan

Stop Notification

Computer name

Find

Settings

Close

Help

[Help](#) [Support](#) [Security Info](#) [About](#)

TREND  
Micro

Applet failed - Applet started

Internet

#### รูปที่ 4.8 แสดงการทำงานของโปรแกรม Trend Micro

จากรูปเป็นการแสดงการทำงานของโปรแกรม Trend Micro ตัวอย่างเช่น ในรูปนี้เป็นการสแกน (Scan) ตรวจจับไวรัสของเครื่องไคลเอ็นต์ที่มีไอพีแอดเดรส 192.168.1.51 ซึ่งอยู่ในเครือข่ายภายใน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## 4.2.6 FTP

FTP สามารถเข้าได้ 3 แบบคือ

### 1. เข้าโดยผ่านทาง Dos



รูปที่ 4.9 การเข้า FTP ผ่านทาง Dos

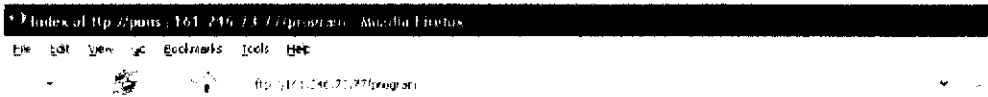
จากรูปเป็นการแสดงการเข้า FTP ผ่านทาง Dos โดย พิมพ์ ftp ตามด้วยหมายเลข ไอพี

### 2. เข้าโดยผ่านทางเว็บเบราว์เซอร์



รูปที่ 4.10 การเข้า FTP ผ่านทางเว็บเบราว์เซอร์

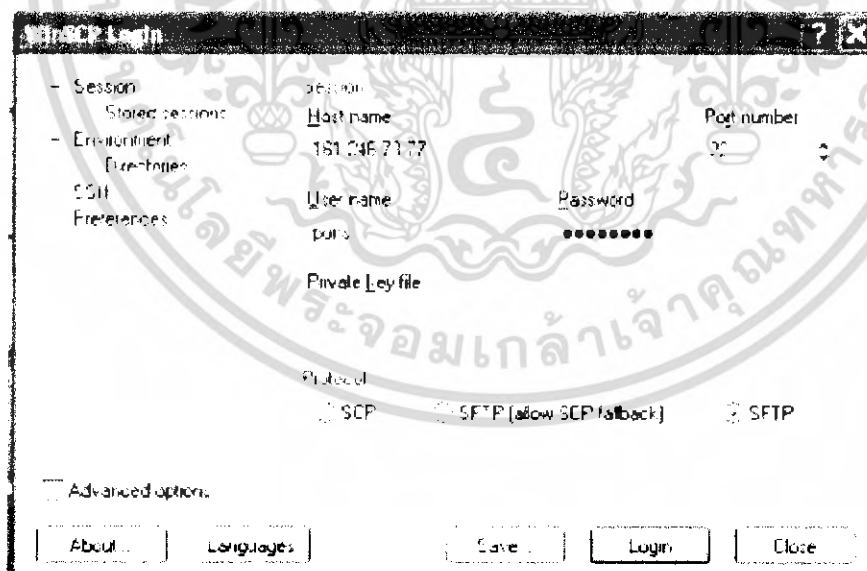
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.11 เมื่อทำการใส่ password ให้ถูกต้องตามที่กำหนด

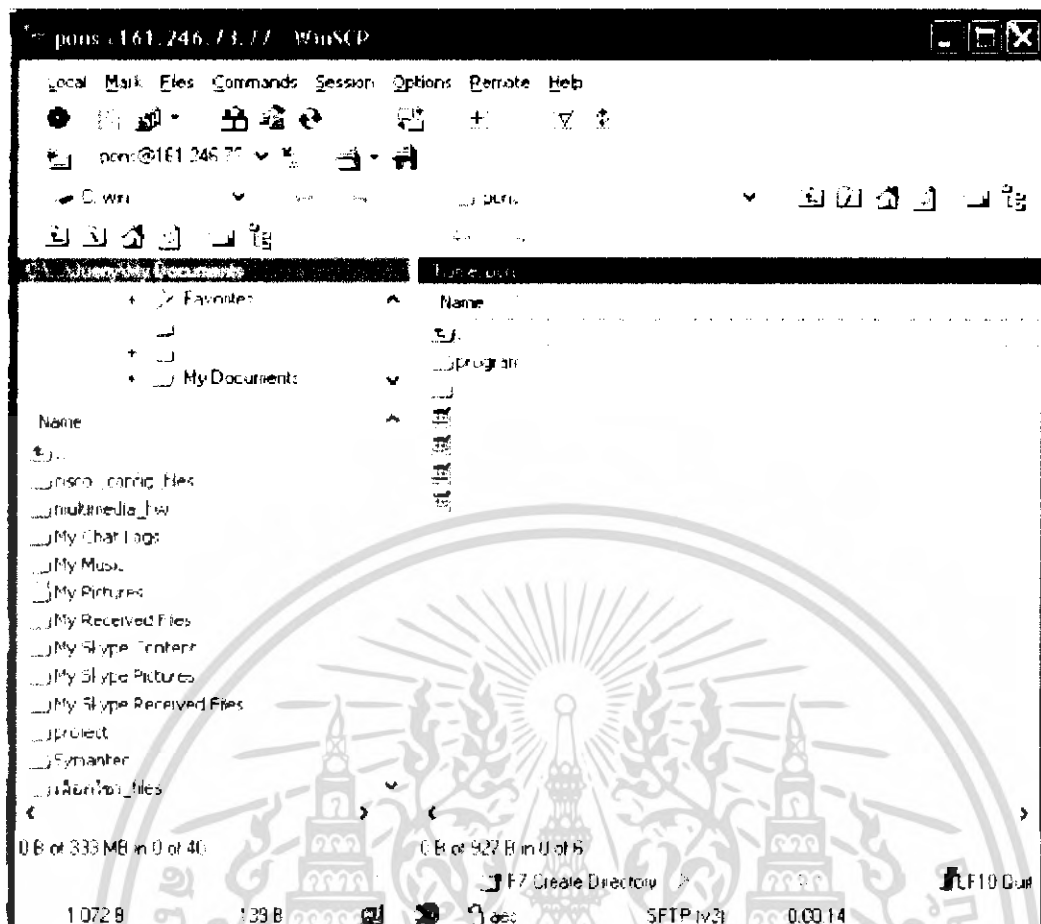
จากรูปที่ 4.10 และ 4.11 เป็นการเข้า FTP โดยผ่านทางเว็บเบราว์เซอร์ ซึ่งเมื่อใส่ password ถูกตามที่กำหนดก็สามารถเข้ามาใช้งานได้

### 3. เข้าโดยผ่านทาง WinSCP



รูปที่ 4.12 การเข้า FTP ผ่านทาง WinSCP

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



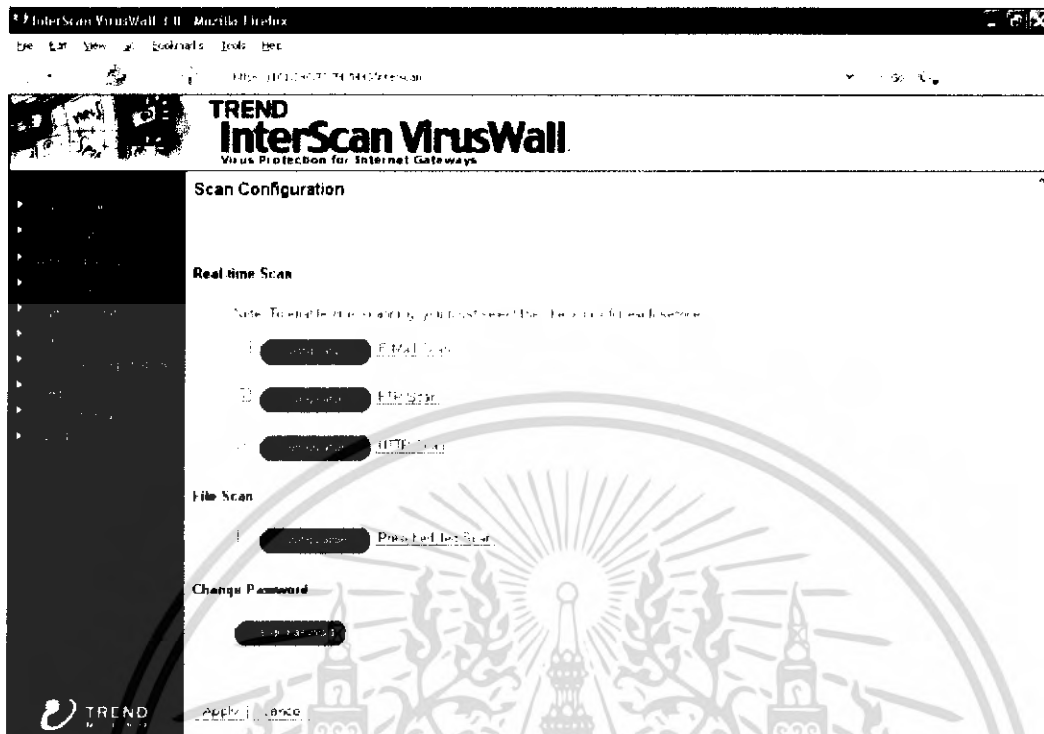
รูปที่ 4.13 เมื่อใส่ username และ password ถูกต้อง

จากรูป 4.12 และ 4.13 เป็นการใช้ FTP ผ่านทาง WinSCP ซึ่งจะให้ได้ Host name, username และ password เมื่อใส่ค่าทั้งหมดถูกต้องก็สามารถใช้งานได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## 4.2.7 Antivirus Gateway

เป็นตัวจับไวรัสโดยวางไว้ที่ไฟร์วอลล์



รูปที่ 4.14 โปรแกรม Trend InterScan VirusWall

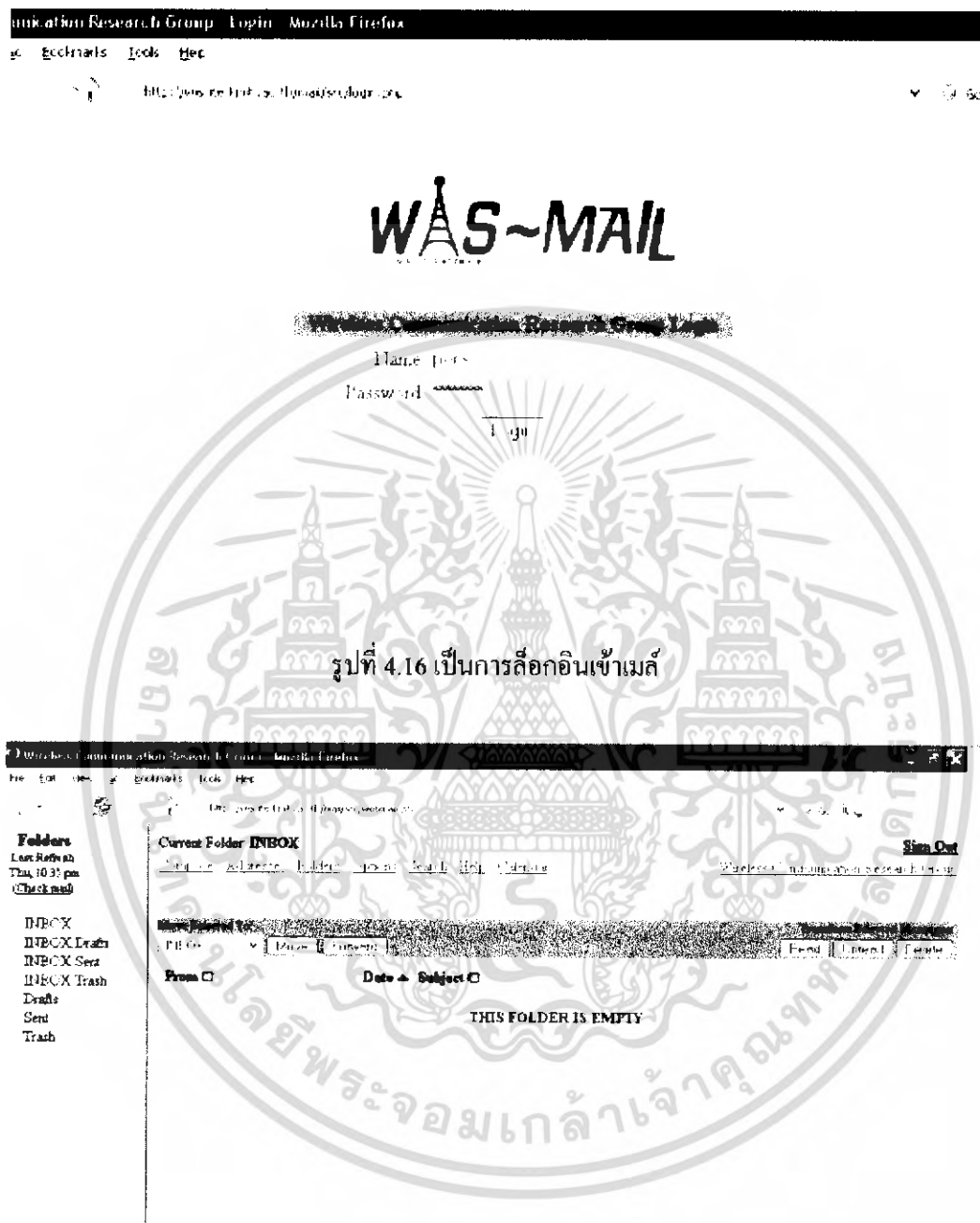


รูปที่ 4.15 เป็นการเก็บ log ( ล็อก ) ต่างๆของโปรแกรม

จากรูป 4.14 และ 4.15 เป็น Antivirus Gateway ที่วางอยู่บนไฟร์วอลล์โดยทำหน้าที่คอยดูเกี่ยวกับไวรัสและเก็บ log ต่างๆเอาไว้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## 4.2.8 Mail Server

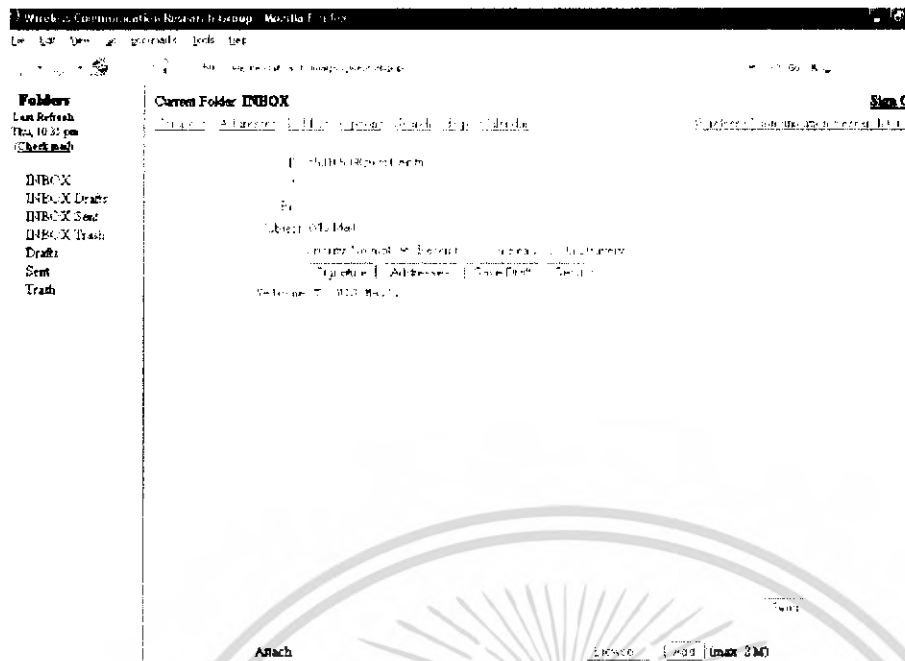


รูปที่ 4.16 เป็นการล็อกอินเข้าเมลล์

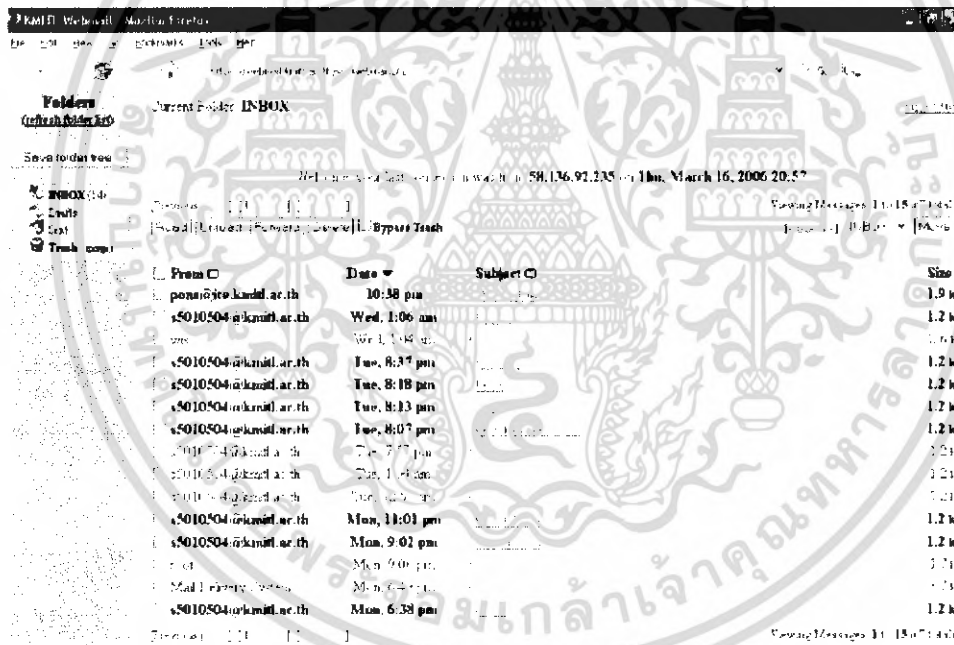
รูปที่ 4.17 เมื่อใส่ล็อกอินอย่างถูกต้อง

จากรูป 4.16 และ 4.17 เป็นการเข้ามาเมลโดยเมื่อใส่รหัสอย่างถูกต้องก็สามารถเข้าใช้เมลล์ของห้องวิจัยได้ โดยแต่ละคนจะมี username และ password

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.18 เป็นการทดลองส่งเมลี่ออกจาก wis.ite.kmitl.ac.th



รูปที่ 4.19 ตรวจสอบการส่งเมลี่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

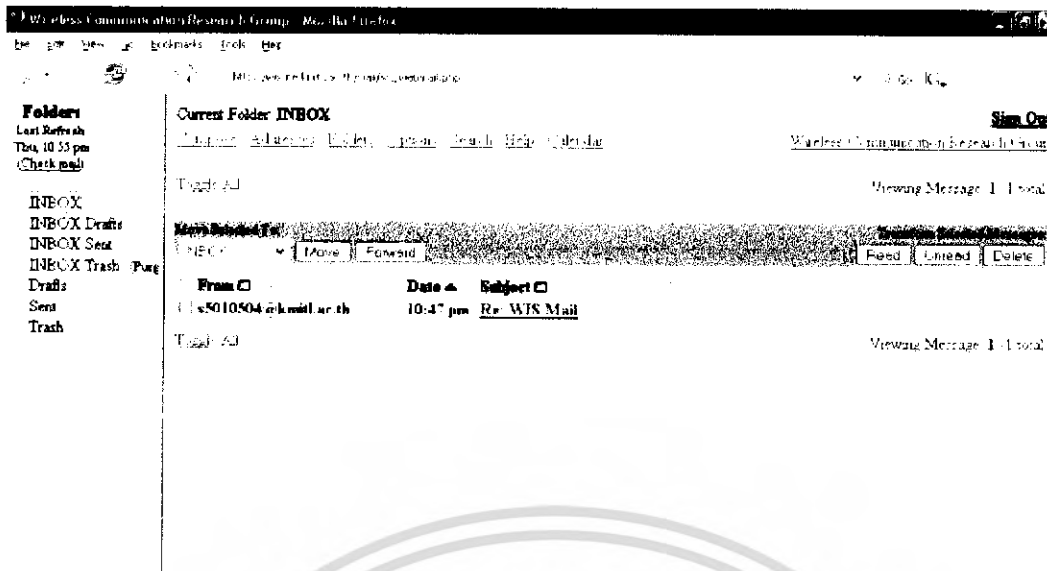
Figure 4.20 shows a screenshot of a webmail interface. The interface displays the current folder as 'INBOX'. The email details are as follows:

- Subject:** WIS Mail
- From:** pons@tc.kmit.ac.th
- Date:** Thu, March 16, 2006 10:35 pm
- To:** 55010504@tc.kmit.ac.th
- Priority:** Normal
- Options:** [Link to view options]

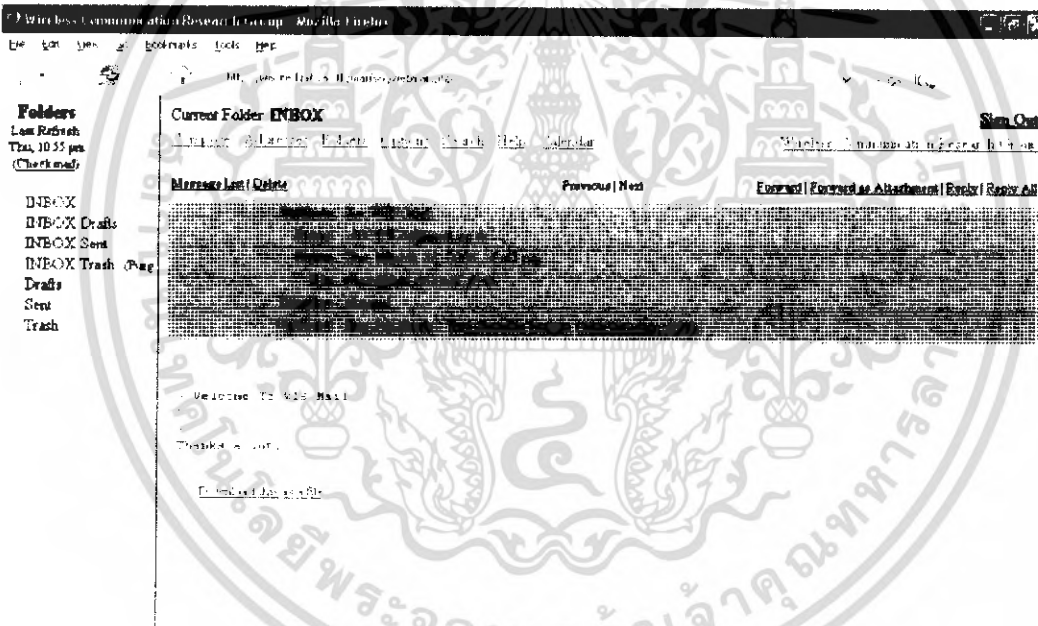
The email content includes a 'Welcome To WIS Mail' message and a 'Thank you' message. The interface also shows a folder list on the left and navigation buttons at the bottom.

รูปที่ 4.21 ทดสอบ โดย reply กับไปยังเมลล์เซิร์ฟเวอร์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.22 ตรวจสอบการรับเมล

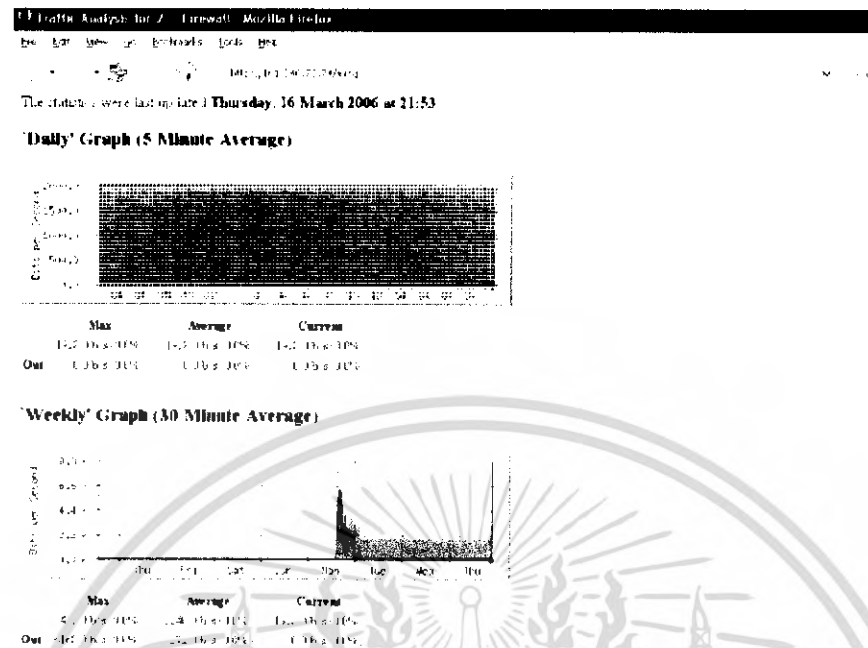


รูปที่ 4.23 ตรวจสอบการรับเมล

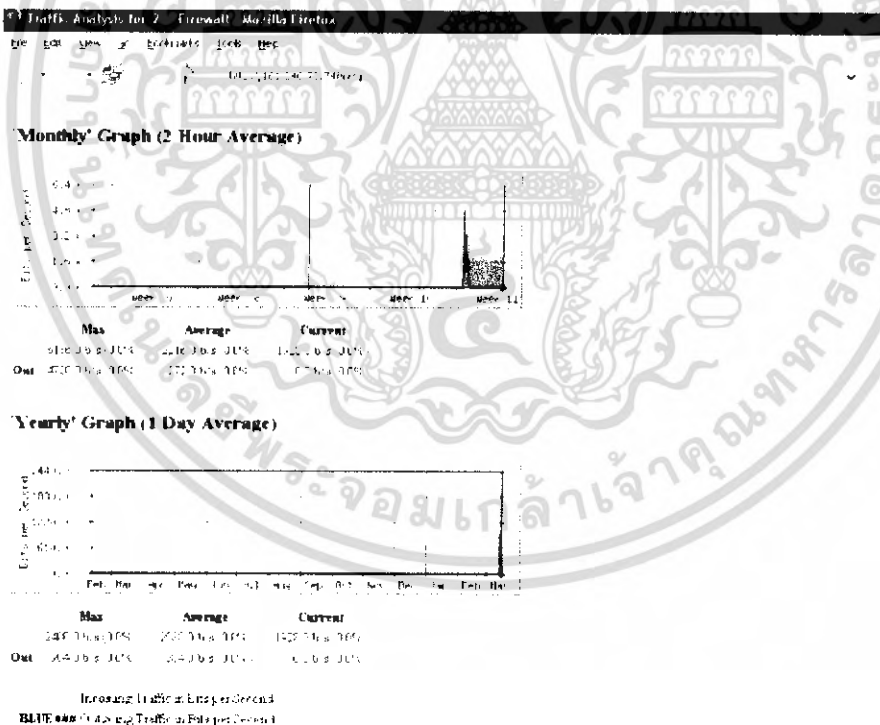
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## 4.2.9 โปรแกรมตรวจจับทราฟฟิก (MRTG)

### MRTG เป็นโปรแกรมตรวจจับทราฟฟิกภายในเครือข่าย



รูปที่ 4.24 เป็นการดูทราฟฟิกภายในเครือข่ายแบบเป็นวันและอาทิตย์



รูปที่ 4.25 เป็นการดูทราฟฟิกภายในเครือข่ายแบบเป็นเดือนและปี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 4.24 และ 4.25 เป็นการ ใช้ซอฟต์แวร์ MRTG วางไว้ที่ไฟร์วอลล์เพื่อดูกราฟฟิกภายในระบบว่าเป็นอย่างใดซึ่งสามารถดูได้แบบทั้งเป็นวัน, อาทิตย์, เดือน, ปี ได้

#### 4.2.10 Homepage

ได้สร้าง Homepage ขึ้นมาเพื่อบริการบุคลากรภายในห้องวิจัย

The screenshot shows a web browser window displaying the homepage of the Ultra Wide Band Radio System Laboratory. The page includes a navigation menu with 'Home', 'News', and 'Publications' buttons. The main content area features several announcements:
 

- IWUWBT 2006:** 2006 International Workshop on UWB Technologies (IWUWBT 2006) will be held at Yokosuka Research Park (YRP), Yokosuka, Japan on December 8-10, 2005. Camera-ready submission due September 16, 2005. Early Registration Up to November 8, 2005.
- WCRG Welcome Party:** เชิญสมาชิก WCRG เข้าร่วมงานเลี้ยงในวันที่ 10 มิถุนายน 2548 เวลาและสถานที่จะแจ้งให้ทราบเร็วๆ นี้
- ISCIT 2005:** International Symposium on Communications and Information Technologies 2005 (ISCIT 2005) will be held at International Convention Center, Beijing, China on October 12-14, 2005. Submission of full paper -> June 15, 2005.

 On the right side, there is a calendar for March 2006. The 'Link' section at the bottom right contains several hyperlinks.

รูปที่ 4.26 เป็นรูปโฮมเพจหน้าแรก

รูปที่ 4.26 เป็นโฮมเพจหน้าแรกซึ่งมีลิงค์ต่างๆให้ทั้งบุคคลภายในและภายนอกสามารถเข้าชมได้แต่การตั้งกระทู้หรือดาวน์โหลดงานวิจัยต้องล็อกอินเพื่อตรวจสอบการเป็นสมาชิกก่อน


เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

File Edit View Favorites Tools Help

Back Search Favorites

http://wls.ite.kmitl.ac.th/

EPSON Web-To-Page Print Print Preview

 สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง  
King Mongkut's Institute of Technology Ladkrabang

**Ultra Wide Band Radio System Laboratory**

**Login**

username: pang  
password: 00000000  
Log in Reset  
New Register

**Calendar**

march 2005

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20
21	22	23	24
25	26	27	28
29	30	31	

**Link**

[www.uwb.org](http://www.uwb.org)  
[www.ieee.org](http://www.ieee.org)  
[www.ieice.org](http://www.ieice.org)

**Ultra Wide Band Radio System Laboratory**

**IWUWBT 2005** 2005 International Workshop on UWB Technologies (IWUWBT 2005) will be held at Yokosuka Research Park (YRP), Yokosuka, Japan on December 8-10, 2005. Camera-ready submission due: September 15, 2005. Early Registration: Up to November 8, 2005

**WCRG Welcome Party** เชิญสมาชิก WCRG เข้าร่วมงานเลี้ยงในวันที่ 10 มิถุนายน 2548 เวลาและสถานที่จะแจ้งให้ทราบเร็วๆ นี้

**ISCIT 2005** International Symposium on Communications and Information Technologies 2005 (ISCIT 2005) will be held at International Convention Center, Beijing, China on October 12-14, 2005. Submission of full paper -> June 15, 2005.

รูปที่ 4.27 เป็นการใส่ username และ password

File Edit View Favorites Tools Help

Back Search Favorites

http://wls.ite.kmitl.ac.th/

EPSON Web-To-Page Print Print Preview

 สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง  
King Mongkut's Institute of Technology Ladkrabang

**Ultra Wide Band Radio System Laboratory**

Home  
Researchs  
Webboard  
Links  
KMITL

**Calendar**

march 2005

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20
21	22	23	24
25	26	27	28
29	30	31	

**Link**

[www.uwb.org](http://www.uwb.org)  
[www.ieee.org](http://www.ieee.org)  
[www.ieice.org](http://www.ieice.org)

**Ultra Wide Band Radio System Laboratory**

**IWUWBT 2005** 2005 International Workshop on UWB Technologies (IWUWBT 2005) will be held at Yokosuka Research Park (YRP), Yokosuka, Japan on December 8-10, 2005. Camera-ready submission due: September 15, 2005. Early Registration: Up to November 8, 2005

**WCRG Welcome Party** เชิญสมาชิก WCRG เข้าร่วมงานเลี้ยงในวันที่ 10 มิถุนายน 2548 เวลาและสถานที่จะแจ้งให้ทราบเร็วๆ นี้

**ISCIT 2005** International Symposium on Communications and Information Technologies 2005 (ISCIT 2005) will be held at International Convention Center, Beijing, China on October 12-14, 2005. Submission of full paper -> June 15, 2005.

รูปที่ 4.28 เมื่อใส่ username และ password ถูกต้อง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 4.27 และ 4.28 เป็นการใส่ username และ password เพื่อให้เฉพาะสมาชิกในห้องวิจัยเท่านั้นที่สามารถเข้ามายังรูปที่ 4.28 ได้ เพื่อทำการตั้งกระทู้หรือตอบกระทู้ รวมถึงดาวน์โหลดงานวิจัยต่างๆ

๕. http://127.0.0.1/read.php  
 Web-10-Page Print Print Preview

คลิกที่นี่เพื่อตั้งกระทู้ใหม่

ลบกระทู้( สำหรับ Admin)

หน้า 11

13 : [ข้อมูลชุมชน](#) ฝึก [2] - (15 มีนาคม 2549 - 02:08:15)  
 12 : [ข่าว สักกะปัด](#) ฝึก [1] - (15 มีนาคม 2549 - 01:55:38)

รูปที่ 4.29 ให้สมาชิกที่ล็อกอินเข้ามาสามารถตั้งกระทู้ได้

Help Search Favorites 22 5

Print Print Preview

ชื่อ  
 email

Submit Reset

รูปที่ 4.30 สมาชิกใส่รายละเอียดต่างๆเกี่ยวกับกระทู้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## ข้อดี uwb

uwb มีข้อดีดังนี้

จาก : [ธีร์](#) - [15 มีนาคม 2549 - 02:08.15]

### ความคิดเห็นที่ 1

uwb จะไร้สายด้วยเทคโนโลยีบลูทูธ

โดย :

### ความคิดเห็นที่ 2

ส่งข้อมูลได้อย่างรวดเร็ว เพราะส่งในรูปแบบของ pulse

โดย : [yock](#)

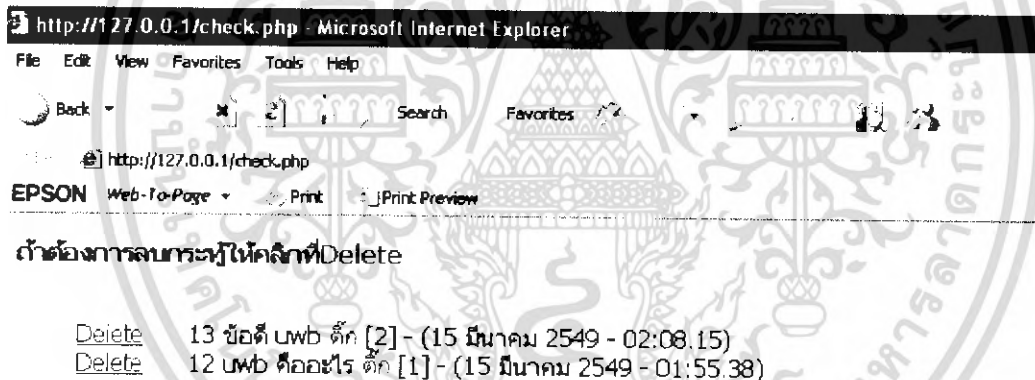
## ร่วมแสดงความคิดเห็นกับกระทู้

ชื่อ :

Email :

รายละเอียด :

รูปที่ 4.31 ผู้ที่เป็นสมาชิกร่วมตอบกระทู้



http://127.0.0.1/check.php - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

http://127.0.0.1/check.php

EPSON Web-To-Page Print Print Preview

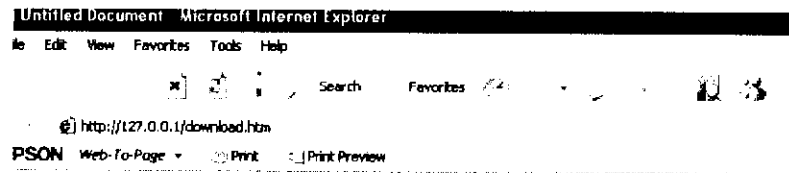
**ดำเนินการลบกระทู้ให้คนที่ Delete**

Delete	13 ข้อดี uwb ดีก [2] - (15 มีนาคม 2549 - 02:08.15)
Delete	12 uwb คืออะไร ดีก [1] - (15 มีนาคม 2549 - 01:55.38)

## รูปที่ 4.32 ลบกระทู้ที่ไม่เหมาะสมได้

จากรูปที่ 4.29 – 4.32 สมาชิกที่ล็อกอินเข้ามามีการตั้งกระทู้และตอบกระทู้ รวมถึงสามารถลบกระทู้ที่ไม่เหมาะสมออกได้ (สำหรับผู้ดูแลระบบเท่านั้น)

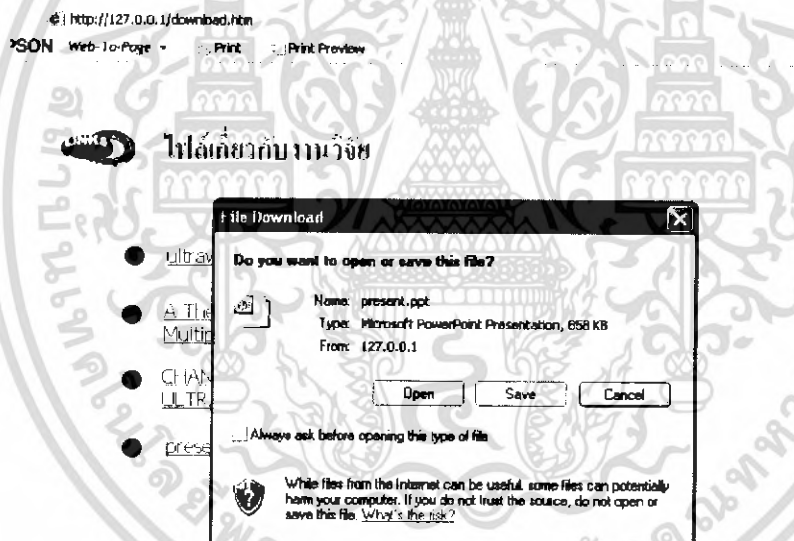
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



## ไฟล์เกี่ยวกับงานวิจัย

- [ultrawideband communication](#)
- [A Theoretical Study of Performance of an Orthogonal Multiplexing Data Transmission Scheme](#)
- [CHANNEL MODELS FOR ULTRAWIDEBAND PERSONAL AREA NETWORKS](#)
- [present](#)

รูปที่ 4.33 สมาชิกสามารถเข้ามาอ่านหรือดาวน์โหลดงานวิจัยได้



รูปที่ 4.34 สมาชิกสามารถดาวน์โหลดงานวิจัยได้

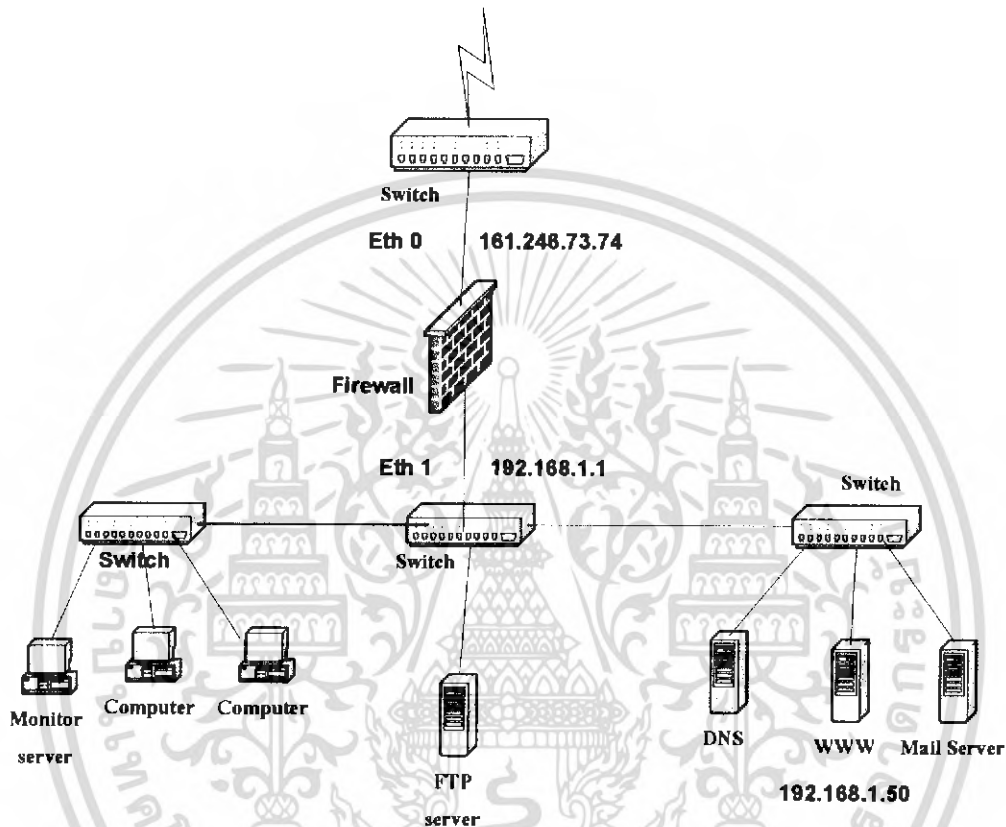
จากรูปที่ 4.33 – 4.34 สมาชิกที่ล็อกอินเข้ามานั้น สามารถเข้ามาอ่านงานวิจัยหรือดาวน์โหลดงานวิจัยของห้องวิจัยนี้ได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## บทที่ 5

### บทสรุปและข้อเสนอแนะ

#### 5.1 สรุปการออกแบบเน็ตเวิร์ก



รูปที่ 5.1 โครงสร้างเครือข่ายที่ทำการออกแบบแบบสมบูรณ์

- ไฟล์วอลล์ สำหรับ ใช้เป็นเกตเวย์ติดต่อกับเครือข่ายภายนอก มีการกำหนดกฎการเข้า-ออก ของแพ็คเก็ตของข้อมูล และทำ NAT เพื่อแปลงแอดเดรสระหว่าง Private IP และ Public IP เพิ่มความปลอดภัยให้แก่เครือข่ายภายใน
- DNS Server สำหรับแปลงหมายเลขไอพีแอดเดรสให้อยู่ในรูปแบบของโดเมนเนม หรือ แปลงกลับจาก โดเมนเนมไปเป็นไอพีแอดเดรส ได้ หลังจากที่ได้ลงทะเบียนชื่อโดเมนผ่าน ISP เรียบร้อยแล้ว และประกาศโดเมนลูกเป็น “wis.kmitl.ac.th”
- เว็บเซิร์ฟเวอร์ สำหรับบริการการใช้งานต่าง ๆ ให้กับอาจารย์และนักศึกษาภายในห้องวิจัยแบบไร้สาย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- DHCPเซิร์ฟเวอร์ สำหรับ แจกไอพีให้แก่เครื่องไคลเอ็นต์แบบอัตโนมัติ
- มอนิเตอร์เซิร์ฟเวอร์ สำหรับดูแลจัดการคอมพิวเตอร์ของผู้ใช้ภายในเครือข่าย สามารถตรวจจับไวรัสในเครือข่ายอินเทอร์เน็ต และแจ้งเตือนแก่ผู้ใช้ในระบบ
- ทำการติดตั้งเมลเซิร์ฟเวอร์ และเซิร์ฟเวอร์ข้อมูล ให้สมบูรณ์
- เพิ่มความปลอดภัยให้แก่ เซิร์ฟเวอร์ข้อมูล
- สร้างเว็บแอปพลิเคชันซึ่งมี การให้ user มาล็อกอิน เพื่อความมั่นคงและตั้งกระทู้เกี่ยวกับในห้องวิจัยได้ เพื่อบริการงานต่าง ๆ ให้แก่ผู้ใช้งานในห้องวิจัย

## 5.2 ผลที่ได้รับ

- ระบบเครือข่ายภายในมีเสถียรภาพ และความปลอดภัยสูง ป้องกันการโจมตีจากเครือข่ายภายนอก ไปยังเครือข่ายภายในได้
- มีการใช้ Antivirus Gateway เพื่อกรอง packet ก่อนเข้ามายังเครือข่ายภายใน
- มีการตรวจจับ traffic ภายในเครือข่าย และวิเคราะห์เป็นกราฟ สำหรับดูแลและวิเคราะห์การใช้งานเครือข่าย
- สามารถใช้งานโดเมนดู “wis.ite.kmitl.ac.th” ได้
- มีเว็บเซิร์ฟเวอร์ เพื่อประกาศข่าวสารต่าง ๆ ได้อย่างสะดวก
- มีการติดตั้ง เมล์เซิร์ฟเวอร์ เพื่อเพิ่มความยืดหยุ่นสำหรับการจัดใช้งานอีเมลล์
- DHCP สามารถทำงานได้อย่างมีประสิทธิภาพ ทำให้ผู้ใช้ไม่พบปัญหาเรื่องการเซตค่าไอพีแอดเดรสซ้ำซ้อน
- มีระบบแจ้งเตือนว่าพบไวรัส ในเครื่องหมายเลขไอพีใด ในระบบ

## 5.3 ปัญหา

### 5.3.1 งบประมาณ

- อุปกรณ์ต่าง ๆ เกี่ยวกับเน็ตเวิร์กมีราคาสูง ดังนั้นจึงเลือกใช้อุปกรณ์ที่สามารถใช้งานระดับปานกลาง
- ซอฟต์แวร์บางตัวที่จำเป็นจะต้องจ่ายค่าลิขสิทธิ์ จึงเลือกใช้ซอฟต์แวร์ที่เป็นโอเพ่นซอร์สซึ่งมีคุณสมบัติรองลงมา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

#### 5.4 แนวทางในการพัฒนาโครงการ

- สามารถพัฒนาในส่วนเซิร์ฟเวอร์ข้อมูล โดยการทำระบบฐานข้อมูล (Database Server) เพื่อสะดวกในการใช้งานยิ่งขึ้น
- เพิ่มระบบความปลอดภัยและระบบตรวจจับผู้บุกรุก (IDS) ในระบบเครือข่าย



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## บรรณานุกรม

อ.บัณฑิต จามรภูติ, คัมภีร์ *Linux Redhat เล่ม 1*, สำนักพิมพ์ Bandhit, พ.ศ.2546

<http://linux.thai.net/>

<http://linux.org>

<http://thaicert.nectec.or.th>



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## โปรแกรมที่ใช้สำหรับกำหนดนโยบายสำหรับเข้า – ออก ของข้อมูล

```
#!/bin/bash
```

```
FW_KMITL_EXT=161.246.73.74
```

```
FW_KMITL_INT=192.168.1.1
```

```
EXTIF=eth0
```

```
INTIF=eth1
```

```
NAT_KMITL=161.246.73.75
```

```
ip addr add 161.246.73.75 dev eth0
```

```
ip addr add 161.246.73.76 dev eth0
```

```
ip addr add 161.246.73.77 dev eth0
```

```
ip addr add 161.246.73.78 dev eth0
```

```
ip addr add 161.246.73.79 dev eth0
```

```
ip addr add 161.246.73.80 dev eth0
```

```
#enable forwarding
```

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
###block ip spoofing
```

```
for f in /proc/sys/net/ipv4/conf/*/rp_filter;
```

```
do
```

```
    echo 1 > $f
```

```
done
```

```
ccho test firewall origin by pons
```

```
#clear policy
```

```
iptables -F
```

```
iptables -t nat -F
```

```
iptables -X
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
#define new policy
```

```
iptables -N KMITL-EXTRANET
```

```
iptables -N EXTRANET-KMITL
```

```
#default policy
```

```
iptables -P INPUT DROP
```

```
iptables -P OUTPUT ACCEPT
```

```
iptables -P FORWARD DROP
```

```
#####input chain#####
```

```
iptables -A INPUT -i $EXTIF -p tcp -d $FW_KMITL_EXT --dport 22 -j ACCEPT
```

```
iptables -A INPUT -i $EXTIF -p tcp -d $FW_KMITL_EXT --dport 25 -j ACCEPT #ken
```

```
iptables -A INPUT -i $INTIF -p tcp -d $FW_KMITL_INT --dport 22 -j ACCEPT
```

```
iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 10/minute -j ACCEPT
```

```
iptables -A INPUT -p icmp --icmp-type echo-reply -m limit --limit 10/minute -j ACCEPT
```

```
iptables -A INPUT -p tcp --syn -m limit --limit 1/s -j ACCEPT
```

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A INPUT -m state --state NEW -i eth0 -j DROP
```

```
#####output chain#####
```

```
#iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
#iptables -A OUTPUT -p icmp -j ACCEPT
```

```
#####forward chain#####
```

```
iptables -A FORWARD -i $EXTIF -o $INTIF -j EXTRANET-KMITL
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
iptables -A FORWARD -i $INTIF -o $EXTIF -j KMITL-EXTRANET
```

```
#####define NAT#####
```

```
iptables -t nat -A PREROUTING -d $SNAT_KMITL -j DNAT --to-destination 192.168.1.50 #
NAT 161.246.73.75 --> 192.168.1.50 ##
```

```
#ipspoofing nat
```

```
iptables -t nat -A PREROUTING -i $EXTIF -s 10.0.0.0/8 -j DROP
```

```
iptables -t nat -A PREROUTING -i $EXTIF -s 127.0.0.0/8 -j DROP
```

```
iptables -t nat -A PREROUTING -i $EXTIF -s 172.16.0.0/12 -j DROP
```

```
iptables -t nat -A PREROUTING -i $EXTIF -s 192.168.1.0/16 -j DROP
```

```
iptables -t nat -A POSTROUTING -o $EXTIF -s 192.168.1.0/24 -d 0/0 -j SNAT --to
161.246.73.77-161.246.73.80
```

```
#iptables -t nat -A POSTROUTING -o $EXTIF -s 192.168.1.0/24 -d 0/0 -j SNAT --to
161.246.73.77
```

```
#####KMITL-EXTRANET#####
```

```
#iptables -A KMITL-EXTRANET -p tcp -s 192.168.1.50 -j ACCEPT
```

```
iptables -A KMITL-EXTRANET -p tcp -s 192.168.1.0/24 -j ACCEPT
```

```
#iptables -A KMITL-EXTRANET -p udp -s 192.168.1.50 -j ACCEPT
```

```
iptables -A KMITL-EXTRANET -p udp -s 192.168.1.0/24 -j ACCEPT
```

```
iptables -A KMITL-EXTRANET -p icmp --icmp-type echo-request -m limit --limit 10/minute -j
ACCEPT
```

```
iptables -A KMITL-EXTRANET -p icmp --icmp-type echo-reply -m limit --limit 10/minute -j
ACCEPT
```

```
#iptables -A KMITL-EXTRANET -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A KMITL-EXTRANET -j DROP
```

```
#####EXTRANET-KMITL#####
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
iptables -A EXTRANET-KMITL -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A EXTRANET-KMITL -p tcp -d $NAT_KMITL --dport 80 -j ACCEPT
iptables -A EXTRANET-KMITL -p tcp -d 161.246.73.75 --dport 21 -j ACCEPT #pons
iptables -A EXTRANET-KMITL -p tcp -d 161.246.73.75 --dport 25 -j ACCEPT #ken
iptables -A EXTRANET-KMITL -p tcp -d 161.246.73.75 --dport 8080 -j ACCEPT #ken
iptables -A EXTRANET-KMITL -p tcp -d 161.246.73.75 --dport 80 -j ACCEPT #ken
iptables -A EXTRANET-KMITL -p tcp -d 192.168.1.50 --dport 80 -j ACCEPT
iptables -A EXTRANET-KMITL -j DROP
```



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- 1      ทำการติดตั้งโปรแกรม postfix, dovecot
- 2      ทำการติดตั้งโปรแกรม clamav, amavisd-new
- 3      ทำการติดตั้งโปรแกรม squirrelmail

#### วิธีการติดตั้ง postfix

- 1      ทำการ unpackage โดยใช้คำสั่ง tar xvfz postfix.tar.gz
- 2      ทำการ compile โปรแกรม โดยใช้คำสั่ง make , make install
- 3      ทำการ config ไฟล์ main.cf ( /etc/postfix/main.cf )

โดยแก้ไข

```
mail_owner = postfix
```

```
myhostname = wis.ite.kmitl.ac.th
```

```
mydomain = ite.kmitl.ac.th
```

```
myorigin = $myhostname
```

```
inet_interfaces = all
```

```
mynetworks_style = class
```

```
mynetworks = 168.100.189.0/28, 127.0.0.0/8, 161.246.73.0/24
```

```
alias_maps = hash:/etc/aliases
```

```
setgid_group = postdrop
```

และเพิ่ม

```
content_filter=smtplib-amavis:[127.0.0.1]:10024
```

```
maildrop_destination_recipient_limit=1
```

ต่อท้ายไฟล์ main.cf เพื่อให้รู้จักโปรแกรม amavis

- 4      ทำการ config ไฟล์ master.cf ( /etc/postfix/master.cf )

ทำการเพิ่ม

```
smtplib-amavis unix - - n - 2 lmtp
```

```
-o lmtp_data_done_timeout=1200
```

```
-o lmtp_send_xforward_command=yes
```

```
127.0.0.1:10025 inet n - n - - smtpd
```

```
-o content_filter=
```

```
-o local_recipient_maps=
```

```
-o relay_recipient_maps=
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

-o smtpd_restriction_classes=
-o smtpd_client_restrictions=
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o mynetworks=127.0.0.0/8
-o strict_rfc821_envelopes=yes
-o smtpd_error_sleep_time=0
-o smtpd_soft_error_limit=1001
-o smtpd_hard_error_limit=1000

```

ต่อท้ายไฟล์ master.cf

- 5 ใช้คำสั่ง postfix start สำหรับรัน โปรแกรม
- 6 ใช้คำสั่ง postfix reload สำหรับการรีโหลดเมื่อมีการ config ค่าใหม่
- 7 ทำการตรวจสอบว่า สามารถใช้งานได้หรือไม่จาก telnet localhost 25

หมายเหตุ

ต้องทำการสร้าง user ก่อน ในที่นี้คือ postfix (useradd postfix )  
 และ group ในที่นี้คือ postdrop ( groupadd postdrop )

## วิธีการติดตั้ง amavisd-new

- 1 ทำการดาวน์โหลด module เบื้องต้น ซึ่งสามารถดาวน์โหลดได้จาก [www.cpan.org](http://www.cpan.org)
  - Archive::Tar (Archive-Tar-x.xx)
  - Archive::Zip (Archive-Zip-x.xx) (1.14 or later should be used!)
  - Compress::Zlib (Compress-Zlib-x.xx)
  - Convert::TNEF (Convert-TNEF-x.xx)
  - Convert::UUlib (Convert-UUlib-x.xxx) (1.05 or later, stick to new versions!)
  - MIME::Base64 (MIME-Base64-x.xx)
  - MIME::Parser (MIME-Tools-x.xxxx) (latest version from CPAN - currently 5.417)
  - Mail::Internet (MailTools-1.58 or later have workarounds for Perl 5.8.0 bugs)
  - Net::Server (Net-Server-x.xx) (version 0.88 finally does setuid right)
  - Net::SMTP (libnet-x.xx, ports/net/p5-Net) (>= libnet-1.16 for performance)
  - Digest::MD5 (Digest-MD5-x.xx) (2.22 or later)
  - IO::Stringy (IO-stringy-x.xxx)
  - Time::HiRes (Time-HiRes-x.xx) (use 1.49 or later, older can cause problems)
  - Unix::Syslog (Unix-Syslog-x.xxx)
  - BerkeleyDB with bdb library 3.2 or later (4.2 or later preferred)

การคอมไพล์ perl module ข้างต้น ให้ติดตั้ง perl compiler ก่อน แล้วทำการ compile โดยใช้คำสั่ง perl makefile.pl  
จากนั้นทำการติดตั้ง perl module จากคำสั่ง make และ make install
- 2 ทำการ unpackage โดยใช้คำสั่ง tar amavisd-new.tar.gz
- 3 ทำการ compile โปรแกรม โดยใช้คำสั่ง make , make install
- 4 ทำการสร้าง user ก่อน ในที่นี้จะใช้ clamav ( useradd clamav)
- 5 และ สร้าง group ในที่นี้จะใช้ clamav (groupadd clamav)
- 6 ทำการสร้าง home directory สำหรับ amavisd
- 7 mkdir /var/amavis
  - mkdir /var/amavis/tmp /var/amavis/var /var/amavis/db
  - chown -R amavis:amavis /var/amavis
  - chmod -R 750 /var/amavis
  - cp amavisd /usr/local/sbin/

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

chown root /usr/local/sbin/amavisd
chmod 755 /usr/local/sbin/amavisd
cp amavisd.conf /etc/
chown root /etc/amavisd.conf
chmod 644 /etc/amavisd.conf
mkdir /var/virusmails
chown amavis:amavis /var/virusmails
chmod 750 /var/virusmails
/usr/local/sbin/amavisd debug

```

- 8 ทดสอบการรัน โปรแกรม /usr/local/sbin/amavisd
- 9 ทำการ config ไฟล์ amavisd.conf (/etc/amavisd.conf )
 

```

$daemon_user = 'clamav';
$daemon_group = 'clamav'

['ClamAV-clamd',
 \&ask_daemon, ["CONTSCAN {} \n", "/var/run/clamav/clamd"],
 qr/\bOK$/, qr/\bFOUND$/,
 qr/^.*?: (?![Infected Archive]).* FOUND$/ ],

$inet_socket_port = 10024;

```
- 10 ทำการตรวจสอบว่า โปรแกรม amavisd สามารถใช้งานได้หรือไม่จาก
 

```

telnet localhost 10024
telnet localhost 10025

```

### วิธีการติดตั้ง clamav

- 1 ทำการ unpackage โดยใช้คำสั่ง tar xvfvz clamav.tar.gz
- 2 ทำการ compile โปรแกรม โดยใช้คำสั่ง make, make check และ make install
- 3 ทำการ config ไฟล์ clamd.conf  
LocalSocket /var/run/clamav/clamd  
User clamav
- 4 ทำการ config ไฟล์ freshclam.conf ให้ทำการ config ค่าตามความเหมาะสม หรือถ้าไม่ต้องการ set ค่า ก็ให้ ทำการคอมเมนต์ที่

#### #Example

5 ทำการทดสอบโปรแกรมทั้งสามโปรแกรมให้ใช้งานร่วมกันได้ โดยทำการทดสอบส่งเมลล์ และแนบไวรัส จากไฟล์ใดเรกทอรี test ของโปรแกรม clamav เพื่อทดสอบ และดูผลจาก log file (/var/log/maillog) และถ้าระบบมีการแจ้งไวรัส และทำการเก็บไฟล์ใน /var/virusmails แสดงว่าระบบสามารถใช้งานได้

### วิธีการติดตั้ง dovecot

- 1 ทำการ unpackage โดยใช้คำสั่ง tar xvfvz dovecot.tar.gz
- 2 ทำการ compile โปรแกรม โดยใช้คำสั่ง make, make install
- 3 ทำการ config ไฟล์ dovecot.conf โดยเพิ่มให้สามารถใช้งานโปรโตคอล pop secure และ imap secure ได้  
protocols = imap imaps pop3 pop3s
- 4 ทำการรัน โปรแกรม dovecot
- 5 ทำการทดสอบโปรแกรมว่าสามารถใช้งานได้ โดยการ telnet localhost 110 เพื่อทำการทดสอบการใช้งานโปรโตคอล pop และ telnet localhost 143 เพื่อทำการทดสอบการใช้งานโปรโตคอล imap