

ห้องสมุดคณะเทคโนโลยีสารสนเทศ พระจอมเกล้าลาดกระบัง

ระบบจัดการบริการระยะไกลผ่านเว็บสำหรับระบบปฏิบัติการฟรีบีเอสดี

WEB-BASED REMOTE SERVICE MANAGEMENT SYSTEM FOR  
FREEBSD



ฉพ.  
พ 6735  
8555



เลขหมู่..... 04899  
เลขทะเบียน.....  
วัน,เดือน,ปี - 6 พ.ย. 2551

b.11980965.....  
i.....

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน  
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ  
คณะเทคโนโลยีสารสนเทศ  
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง  
ภาคเรียนที่ 1 ปีการศึกษา 2550

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

**WEB-BASED REMOTE SERVICE MANAGEMENT SYSTEM FOR  
FREEBSD**



**A SYSTEM DEVELOPMENT PROJECT OF THE REQUIREMENT  
FOR THE DEGREE OF  
MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY  
FACULTY OF INFORMATION TECNOLOGY  
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG**

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1/ 2007



**COPYRIGHT 2007**

**FACULTY OF INFORMATION TECHNOLOGY**

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

เอกสารนี้เป็นเอกสารสงวนลิขสิทธิ์สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปเผยแพร่ในเชิงพาณิชย์

ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อ	ระบบจัดการบริการระยะไกลผ่านเว็บสำหรับระบบปฏิบัติการพีอีเอสดี
นักศึกษา	นายพิทักษ์ วงศ์อินทร์
รหัสนักศึกษา	47066122
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2550
อาจารย์ที่ปรึกษา	ผศ. อัครินทร์ คุณกิตติ

### บทคัดย่อ

ในระบบสารสนเทศแบบกระจายซึ่งเครื่องให้บริการมีการกระจายอยู่หลายที่ในเครือข่ายนั้น การบริหารจัดการเครื่องให้บริการระยะไกล เป็นเรื่องที่ยากจะยุ่งยากและใช้เวลามากสำหรับผู้ดูแลระบบ เพื่อลดภาระของผู้ดูแลระบบจึงมีแนวคิดที่จะพัฒนาระบบที่มีเครื่องที่ทำหน้าที่เป็นตัวกลางในการรับคำสั่งต่างๆจากผู้ดูแลระบบ และทำหน้าที่ในการส่งต่อคำสั่งเหล่านั้นไปยังเครื่องที่ให้บริการปลายทางอีกทีผ่านช่องทางที่มีความปลอดภัย ผู้ดูแลระบบสามารถทำการกำหนดค่าคอนฟิกูเรชันของเครื่องให้บริการปลายทางได้ โดยระบบจะนำข้อมูลจากผู้ดูแลระบบไปสร้างเป็นไฟล์คอนฟิกูเรชันเก็บไว้ที่เครื่องตัวกลาง เพื่อรอคำสั่งในการส่งไฟล์ดังกล่าวไปยังเครื่องให้บริการปลายทางต่อไป นอกจากนี้ผู้ดูแลระบบสามารถสั่งให้เครื่องให้บริการปลายทางทำการสำรองไฟล์ระบบของตัวเองเพื่อนำไปใช้ในกระบวนการกู้คืนระบบต่อไป ในการพัฒนาระบบนั้นได้มีการพัฒนาในรูปแบบของระบบสารสนเทศบนเว็บไซต์ (Web-based User Interface) เพื่อสะดวกในการเข้าใช้งานอย่างกว้างขวางจากผู้ดูแลระบบ มีส่วนของการป้อนข้อมูลที่จำเป็นสำหรับระบบ การจัดการไฟล์คอนฟิกูเรชันต่างๆ การบริหารจัดการเครื่องให้บริการปลายทาง รวมไปถึงการสำรองและกู้คืนไฟล์ระบบ

ระบบนี้ออกแบบมาเพื่อเป็นอีกทางเลือกให้แก่ผู้ดูแลระบบ โดยจะมีการติดตั้งโปรแกรมทั้งหมดไว้ที่เครื่องตัวกลางเพียงแห่งเดียว แตกต่างจากระบบอื่นที่จำเป็นต้องติดตั้งโปรแกรมไว้ที่เครื่องให้บริการทุกเครื่อง ซึ่งจะช่วยให้ช่วยลดภาระในการติดตั้งโปรแกรมของผู้ดูแลระบบ และลดการสิ้นเปลืองทรัพยากรบนเครื่องให้บริการปลายทางได้ อีกทั้งเนื่องจากระบบมีการสำรองไฟล์คอนฟิกูเรชัน และอิมเมจไฟล์ระบบของเครื่องให้บริการปลายทางทั้งหมดไว้ที่เครื่องตัวกลาง ดังนั้นกระบวนการในการกู้คืนระบบจะทำได้ง่ายขึ้น เมื่อเครื่องให้บริการใดๆเสียหายไม่สามารถใช้งานได้ ผู้ดูแลระบบสามารถนำเครื่องสำรองมาใช้แทนได้ โดยระบบจะทำการการกู้คืนไฟล์ระบบของเครื่องสำรองโดยใช้อิมเมจไฟล์ระบบของเครื่องให้บริการเดิมที่ได้ทำการสำรองไว้แล้ว

<b>Title</b>	Web-based Remote Service Management System for FreeBSD
<b>Student</b>	Mr. Pitak Wongin
<b>Student ID.</b>	47066122
<b>Degree</b>	Master of Science
<b>Programme</b>	Information Science
<b>Academic Year</b>	2007
<b>Advisor</b>	Asst.Prof.Akharin Khunkitti

## ABSTRACT

In distributed system environment, managing services that are widely distributed over network is a complex and time-consuming process for administrator. To solve this problem, we plan to design the system that has a centralize server for receives commands from administrator and then send these commands to another remote serviced machines again via the secure channel. Administrator can configure all serviced machine via centralize server, the system will create configuration files then send them to the remote machined that was selected. This system can download file system images of the remote serviced machine and collect them on the centralize server. This image file is used for recovery process. For widely used, this system was designed with web-based user interface, that has the web pages for manage configuration files, manage remote serviced machine and for backup/recovery process. Administrator can use this system everywhere via web browser.

Differences from another systems, to conserve the resource of serviced machine and reduce the tasks of administrator to install many programs or agents on every serviced machine, at this system, all programs were installed on the centralize server only. Because configuration files and file system images of all serviced machine were collected on the centralize server, so the recovery process will be easily. When the remote serviced machine was crashed, administrator can replace the existing machine with the spared machine. The recovery process will restore file system of the spared machine with the image file of existing machine.

## กิตติกรรมประกาศ

โครงการพัฒนาระบบงานนี้ไม่อาจสำเร็จได้ด้วยดี หากไม่ได้รับความช่วยเหลือและร่วมมือจากหลาย ๆ ฝ่ายด้วยกัน โดยเฉพาะอย่างยิ่งท่านอาจารย์อัครินทร์ คุณกิตติ อาจารย์ที่ปรึกษาโครงการพัฒนาระบบงานนี้ที่สละเวลา แรงกาย แรงใจ ในการดูแล เอาใจใส่ แนะนำและช่วยเหลือ ขอบคุณเพื่อน ๆ พี่ๆ รุ่น 17.1 ทุกคนที่มีส่วนสนับสนุน ให้กำลังใจและเป็นທີ່ปรึกษา และขอขอบพระคุณ บิดา มารดา อันเป็นที่เคารพอย่างสูง ที่ได้ให้ความรักและความเอาใจใส่ กำลังใจที่ไม่เคยขาดหาย ข้าพเจ้าขอระลึกในพระคุณและขอกราบขอบพระคุณมา ณ ที่นี้

พิทักษ์ วงศ์อินทร์



# สารบัญ

	หน้า
บทคัดย่อภาษาไทย.....	I
บทคัดย่อภาษาอังกฤษ.....	II
กิตติกรรมประกาศ.....	III
สารบัญ.....	IV
สารบัญตาราง.....	VI
สารบัญรูป.....	VII
บทที่ 1 บทนำ.....	1
1.1 ความเป็นมาของโครงการ.....	1
1.2 วัตถุประสงค์ของโครงการ.....	1
1.3 ขอบเขตของโครงการ.....	2
1.4 องค์ประกอบของระบบงาน.....	2
1.5 ขั้นตอนการพัฒนาระบบ.....	3
1.6 ประโยชน์ที่คาดว่าจะได้รับ.....	4
บทที่ 2 การบริหารจัดการเครื่องให้บริการปลายทางระยะไกล.....	5
2.1 การใช้ Secure Shell ในการเข้าถึงระบบจากระยะไกล.....	5
2.2 การจัดตารางการทำงานอัตโนมัติ (crontab).....	15
2.3 การสำรองข้อมูล.....	17
บทที่ 3 การวิเคราะห์ระบบ.....	22
3.1 ความต้องการของระบบงาน.....	22
3.2 ภาพรวมของระบบจัดการบริการระยะไกลผ่านเว็บ.....	23
3.3 แบบจำลองเชิงแนวคิดของระบบ.....	26
3.3.1 Use case model.....	
- Use case diagram.....	26
- Use case description.....	27
- Activity diagram.....	32
3.3.2 Structural model.....	42
- Class diagram.....	42
3.3.3 Behavioral models.....	44
- Sequence diagram.....	44

# สารบัญ (ต่อ)

	หน้า
บทที่ 4 การออกแบบระบบ .....	52
4.1 การออกแบบฐานข้อมูล.....	52
4.1.1 Entity Relationship Diagram .....	52
4.1.2 Data Dictionary .....	53
4.1.2 โครงสร้างของไฟล์ข้อมูล.....	54
บทที่ 5 การพัฒนาระบบ .....	56
5.1 การวางแผนปฏิบัติงาน .....	56
5.2 การวางแผนโครงสร้างของระบบ.....	56
5.3 การปรับแต่งระบบเบื้องต้น .....	58
5.4 การพัฒนาระบบจัดการบริการระยะไกลผ่านเว็บ .....	59
5.5 การทดสอบระบบ .....	67
บทที่ 6 บทสรุปและแนวทางพัฒนาในอนาคต.....	83
6.1 ข้อจำกัดของระบบ.....	83
6.2 บทสรุปและแนวทางในการพัฒนาในอนาคต.....	83
บรรณานุกรม.....	85
ภาคผนวก.....	86
ภาคผนวก ก. การติดตั้งโปรแกรมที่เกี่ยวข้อง.....	87
ภาคผนวก ข. การติดตั้งระบบจัดการบริการระยะไกลผ่านเว็บ.....	90
ภาคผนวก ค. คู่มือการใช้งานระบบจัดการบริการระยะไกลผ่านเว็บ.....	91
ประวัติผู้เขียน.....	110

# สารบัญตาราง

หน้า

ตารางที่	
4.1 Data Dictionary ของตาราง Remote Machine.....	53
4.2 Data Dictionary ของตาราง Services.....	53
4.3 Data Dictionary ของตาราง Services_and_Machines.....	53
4.4 Data Dictionary ของตาราง Configfile .....	54



# สารบัญรูป

หน้า

รูปที่

2.1 ตัวอย่างการทำงานของผู้ดูแลระบบ.....	5
2.2 ขั้นตอนการการติดตั้งและใช้งาน public keys และ private keys 1.....	7
2.3 ขั้นตอนการการติดตั้งและใช้งาน public keys และ private keys 2.....	8
2.4 ขั้นตอนการการติดตั้งและใช้งาน public keys และ private keys 3.....	8
2.5 ขั้นตอนการการติดตั้งและใช้งาน public keys และ private keys 4.....	9
2.6 ขั้นตอนการการติดตั้งและใช้งาน public keys และ private keys 5.....	9
2.7 ขั้นตอนการการติดตั้งและใช้งาน public keys และ private keys 6.....	9
2.8 ขั้นตอนการการติดตั้งและใช้งาน public keys และ private keys 7.....	10
2.9 ขั้นตอนการทำงาน ของ SSH.....	11
2.10 ขั้นตอนการทำงาน ของ SSH เมื่อใช้ ssh-agent.....	14
3.1 ภาพรวมของระบบจัดการบริการระยะไกลผ่านเว็บ.....	23
3.2 Use Case Diagram ระบบจัดการบริการระยะไกลผ่านเว็บ.....	26
3.3 Activity Diagram ของยูสเคส Login.....	32
3.4 Activity Diagram ของยูสเคส Create User Profile.....	33
3.5 Activity Diagram ของยูสเคส Create System Information.....	34
3.6 Activity Diagram ของยูสเคส Manage Configuration Files.....	35
3.7 Activity Diagram ของยูสเคส Manage Service Machine.....	36
3.8 Activity Diagram ของยูสเคส Send Configuration File.....	37
3.9 Activity Diagram ของยูสเคส Backup File System.....	39
3.10 Activity Diagram ของยูสเคส Recovery File System.....	41
3.11 Class Diagram ของระบบ.....	42
3.12 Sequence Diagram ของยูสเคส Create User Profile.....	44
3.13 Sequence Diagram ของยูสเคส Create System Information.....	45
3.14 Sequence Diagram ของการสร้างไฟล์คอนฟิกูเรชันขึ้นมาใหม่.....	46
3.15 Sequence Diagram ของการแก้ไขไฟล์คอนฟิกูเรชันที่มีอยู่แล้ว.....	47
3.16 Sequence Diagram ของการลบไฟล์คอนฟิกูเรชันที่มีอยู่แล้ว.....	47
3.17 Sequence Diagram ของยูสเคส Manage Serviced Machine.....	48
3.18 Sequence Diagram ของยูสเคส Send Configuration File.....	49

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า

ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

# สารบัญรูป (ต่อ)

หน้า

รูปที่

3.19 Sequence Diagram ของยูสเคส Backup File System.....	50
3.20 Sequence Diagram ของยูสเคส Recovery File System.....	51
4.1 Entity Relationship Diagram.....	52
5.1 โครงสร้างของระบบจัดการบริการระยะไกลผ่านเว็บ.....	57
5.2 แผนภาพโครงสร้างของระบบ.....	60
5.3 หน้าจอการเรียกใช้งาน โปรแกรมในส่วน Login.....	60
5.4 หน้าจอการเรียกใช้งาน โปรแกรมในส่วน Information Management.....	61
5.5 การทำงานในส่วนของการจัดการไฟล์คอนฟิกูเรชัน.....	62
5.6 การทำงานในส่วนของการจัดการเครื่องให้บริการ 1.....	63
5.7 การทำงานในส่วนของการจัดการเครื่องให้บริการ 2.....	63
5.8 การทำงานในส่วนของการส่งไฟล์คอนฟิกูเรชัน.....	64
5.9 การทำงานในส่วนของการสำรองไฟล์ระบบ.....	65
5.10 การทำงานในส่วนของการสำรองไฟล์ระบบ (ต่อ).....	65
5.11 การทำงานในส่วนของการกู้คืนระบบให้เครื่องปลายทาง.....	66
5.12 การทำงานในส่วนของการแก้ไขข้อมูลผู้ใช้.....	66
5.13 โครงสร้างของระบบที่ใช้ในการทดสอบ 1.....	67
5.14 ผลการการทดสอบฟังก์ชันการจัดการเครื่องให้บริการปลายทาง 1.....	68
5.15 ผลการการทดสอบฟังก์ชันการจัดการเครื่องให้บริการปลายทาง 2.....	69
5.16 ผลการการทดสอบฟังก์ชันการจัดการเครื่องให้บริการปลายทาง 3.....	69
5.17 ผลการการทดสอบฟังก์ชันการจัดการเครื่องให้บริการปลายทาง 4.....	70
5.18 โครงสร้างของระบบที่ใช้ในการทดสอบ 2.....	71
5.19 ผลการการทดสอบฟังก์ชันการการส่งไฟล์คอนฟิกูเรชัน 1.....	72
5.20 ผลการการทดสอบฟังก์ชันการการส่งไฟล์คอนฟิกูเรชัน 2.....	72
5.21 ผลการการทดสอบฟังก์ชันการการส่งไฟล์คอนฟิกูเรชัน 3.....	73
5.22 ผลการการทดสอบฟังก์ชันการการส่งไฟล์คอนฟิกูเรชัน 4.....	74
5.23 ผลการการทดสอบฟังก์ชันการการส่งไฟล์คอนฟิกูเรชัน 5.....	74
5.24 โครงสร้างของระบบที่ใช้ในการทดสอบ 3.....	75
5.25 ผลการการทดสอบฟังก์ชันการสำรองไฟล์ระบบ 1.....	76

# สารบัญรูป (ต่อ)

หน้า

รูปที่

5.26 ผลการทดสอบฟังก์ชันการสำรองไฟระบบ 2.....	76
5.27 อิมเมจของไฟระบบทั้งหมดที่ Centralize Server มี.....	77
5.28 โครงสร้างของระบบที่ใช้ในการทดสอบ 4.....	78
5.29 ผลการทดสอบฟังก์ชันการกู้คืนไฟระบบ 1.....	78
5.30 ผลการทดสอบฟังก์ชันการกู้คืนไฟระบบ 2.....	79
5.31 ผลการทดสอบฟังก์ชันการกู้คืนไฟระบบ 3.....	80
5.32 ผลการทดสอบฟังก์ชันการกู้คืนไฟระบบ 4.....	80
5.33 ผลการทดสอบฟังก์ชันการกู้คืนไฟระบบ 5.....	81
5.34 ผลการทดสอบฟังก์ชันการกู้คืนไฟระบบ 6.....	81
5.35 ผลการทดสอบฟังก์ชันการกู้คืนไฟระบบ 7.....	81
5.36 ผลการทดสอบฟังก์ชันการกู้คืนไฟระบบ 8.....	81
5.37 ผลการทดสอบฟังก์ชันการกู้คืนไฟระบบ 9.....	82
ค.1 การล็อกอินเข้าสู่ระบบ.....	91
ค.2 การกำหนดต่างๆค่าให้ระบบ.....	92
ค.3 การของการเพิ่มเครื่องให้บริการให้กับระบบ.....	92
ค.4 การของการเพิ่มบริการต่างๆค่าให้กับระบบ.....	93
ค.5 การของการเลือกประเภทของบริการให้กับระบบ.....	93
ค.6 การของการเพิ่มบริการต่างๆค่าให้กับระบบ.....	93
ค.7 เมนูในการเข้าสู่ส่วนของการกำหนดบริการให้แก่เครื่องให้บริการ.....	94
ค.8 การกำหนดบริการให้แก่เครื่องให้บริการ.....	94
ค.9 การกำหนดบริการให้แก่เครื่องให้บริการ (ต่อ).....	95
ค.10 เมนูในการกำหนดไฟล์คอนฟิกูเรชันให้กับบริการ.....	95
ค.11 การกำหนด ไฟล์คอนฟิกูเรชันให้แก่บริการ.....	96
ค.12 การกำหนด ไฟล์คอนฟิกูเรชันให้แก่บริการ (ต่อ).....	96
ค.13 การทำงานในส่วนของลบข้อมูล.....	97
ค.14 การทำงานในส่วนของการจัดการไฟล์คอนฟิกูเรชัน.....	97
ค.15 ขั้นตอนการสร้าง ไฟล์คอนฟิกูเรชันขึ้นมาใหม่.....	98
ค.16 ขั้นตอนการสร้าง ไฟล์คอนฟิกูเรชันขึ้นมาใหม่.....	98

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า

ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อ IX และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญรูป (ต่อ)

หน้า

รูปที่	หน้า
ค.17 การกำหนดค่าคอนฟิกูเรชันให้กับไฟล์ที่สร้างขึ้น	99
ค.18 ข้อความยืนยันความถูกต้องจากระบบ	99
ค.19 ขั้นตอนการแก้ไขไฟล์ที่สร้างไว้แล้ว 1	100
ค.20 ขั้นตอนการแก้ไขไฟล์ที่สร้างไว้แล้ว 2	100
ค.21 ขั้นตอนการดาวน์โหลดไฟล์คอนฟิกูเรชัน	101
ค.22 ขั้นตอนการลบไฟล์คอนฟิกูเรชัน	101
ค.23 ขั้นตอนการอัปเดตไฟล์คอนฟิกูเรชัน	101
ค.24 การทำงานในส่วนของการจัดการเครื่องให้บริการ	102
ค.25 ชนิดของบริการต่างๆ	102
ค.26 การทำงานในส่วนของการจัดการบริการ	103
ค.27 ผลการทำงานเมื่อผู้ดูแลระบบกดปุ่ม stop	103
ค.28 ฟังก์ชันการทำงานที่ระบบสามารถทำได้	104
ค.29 การทำงานในส่วนของการส่งไฟล์คอนฟิกูเรชัน	104
ค.30 ขั้นตอนส่งไฟล์คอนฟิกูเรชันไปยังปลายทาง 1	105
ค.31 ขั้นตอนส่งไฟล์คอนฟิกูเรชันไปยังปลายทาง 2	105
ค.32 ขั้นตอนส่งไฟล์คอนฟิกูเรชันไปยังปลายทาง 3	106
ค.33 การตรวจสอบความถูกต้องของไฟล์คอนฟิกูเรชัน	106
ค.34 การทำงานในส่วนของการสำรองไฟล์ระบบ	107
ค.35 ขั้นตอนการการสำรองไฟล์ระบบ	108
ค.36 การทำงานในส่วนของการกู้คืนระบบ	108
ค.37 ขั้นตอนการการกู้คืนระบบ	109
ค.38 ข้อความยืนยันจากระบบ	109

# บทที่ 1

## บทนำ

### 1.1 ความเป็นมาของโครงการ

ปัจจุบัน ระบบเครือข่ายส่วนใหญ่จะมีการกระจายเครื่องให้บริการต่างๆออกเป็นหลายๆเครื่อง เช่น DNS Server, DHCP Server หรือ Proxy Server เป็นต้น การบริหารจัดการและกำหนดค่า Configuration ต่างๆของแต่ละบริการเป็นเรื่องที่ค่อนข้างจะยุ่งยากสำหรับผู้ดูแลระบบ เนื่องจากเครื่องให้บริการมีการกระจายอยู่หลายที่ เพื่อลดภาระของผู้ดูแลระบบจึงมีแนวคิดที่จะพัฒนาระบบที่มีเครื่องที่ทำหน้าที่เป็นตัวกลางในการรับคำสั่งต่างๆจากผู้ใช้เช่นค่า Configuration ต่างๆ คำสั่งในการเปิด ปิดการใช้งานบริการ รวมถึงคำสั่งในการสำรองและกู้คืน ไฟล์ระบบของแต่ละเครื่องให้บริการในเครือข่าย ซึ่งเครื่องที่ให้บริการอื่นๆจะทำหน้าที่เป็นผู้รับบริการ (Subscriber) จากตัวกลางอีกที โดยในการทำงานนั้นผู้ดูแลระบบจะเข้าไปบริหารจัดการและกำหนดค่า Configuration ของแต่ละบริการผ่านทางเครื่องที่ทำหน้าที่เป็นตัวกลาง ซึ่งเมื่อเครื่องดังกล่าวได้รับข้อมูลแล้วก็จะทำการส่งคำสั่งที่ต้องการไปยังเครื่องที่ให้บริการอื่นๆตามที่ผู้ดูแลระบบกำหนด ผ่านช่องทางที่มีความปลอดภัยเพื่อความปลอดภัยข้อมูล ซึ่งระบบนี้สามารถทนต่อความเสียหาย (Fault Tolerance) ได้เป็นอย่างดี เนื่องจากเครื่องให้บริการจะทำการสำรองข้อมูลไฟล์ระบบทั้งหมดส่งมาเก็บไว้ที่ตัวกลาง เมื่อเครื่องให้บริการใดๆเสียหายหรือไม่สามารถใช้งานได้ ผู้ดูแลระบบสามารถนำเครื่องสำรองมาใช้งานแทนได้ทันที เนื่องจากระบบสามารถทำการกู้คืน โดยทำการส่งข้อมูลไฟล์ระบบทั้งหมดของเครื่องบริการเดิมจากตัวกลางให้แก่เครื่องสำรอง และเมื่อเครื่องให้บริการเดิมได้ทำการซ่อมแซมแก้ไขจนสามารถใช้งานได้ตามปกติแล้ว ระบบก็ยังสามารถกู้คืน (Recovery) ข้อมูลไฟล์ระบบทั้งหมดให้เครื่องให้บริการได้อีกด้วยตามกลไกเดิม

โดยในการออกแบบระบบนี้ได้เลือกใช้ระบบปฏิบัติการพีริเอสดีในการติดตั้งบริการ (Service) ต่างๆ และส่วนติดต่อผู้ใช้นั้นได้มีการพัฒนาในรูปแบบของระบบสารสนเทศบนเว็บไซด์ (Web-based User Interface) เพื่อสะดวกในการเข้าใช้งานอย่างกว้างขวางจากผู้ดูแลระบบ

### 1.2 วัตถุประสงค์ของโครงการ

1. เพื่อช่วยลดภาระผู้ดูแลระบบในการกำหนดค่า Configuration ให้กับเครื่องให้บริการต่างๆที่อยู่ภายใต้การควบคุมได้
2. เพื่อเพิ่มความสะดวกให้แก่ผู้ดูแลระบบในการกำหนดค่า Configuration ให้กับบริการต่างๆจากสถานที่อื่นเมื่อไม่ได้อยู่ที่หน้าเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นเครื่องให้บริการ เนื่องจากการติดต่อผ่านทางเว็บ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3. สามารถบริหารจัดการเครื่องให้บริการต่างๆที่อยู่ภายใต้การควบคุมเช่นการเปิด ปิด หรือเรียกดูสถานะการทำงานของบริการนั้นๆได้
4. เพื่อเพิ่มความสามารถในการสำรอง (Backup) กู้คืน (Recovery) ข้อมูลไฟล์ระบบทั้งหมดของเครื่องให้บริการในกรณีที่มีความเสียหายเกิดขึ้น
5. เพิ่มความสามารถในการคงทนต่อความเสียหาย (Fault Tolerance) ของระบบให้ดียิ่งขึ้น โดยสามารถสั่งให้เครื่องให้บริการทำการ Backup ข้อมูลหรือไฟล์ระบบโดยอัตโนมัติตามเวลาที่กำหนดไว้ และสามารถกู้คืนข้อมูลดังกล่าวได้เมื่อระบบเกิดความเสียหาย
6. พัฒนาระบบที่มีการใช้งานและการติดต่อผ่านเว็บเพื่อความยืดหยุ่นในการใช้งาน

### 1.3 ขอบเขตของโครงการ

1. พัฒนาระบบที่สามารถทำงานได้บนระบบปฏิบัติการฟรีเบสดี
2. พัฒนาระบบที่เป็นลักษณะเป็นเว็บแอปพลิเคชัน สามารถเรียกใช้งานระบบได้จากเว็บเบราว์เซอร์
3. ระบบมีความยืดหยุ่นในการทำงาน สามารถรองรับเครื่องให้บริการได้มากกว่า 1 เครื่อง
4. ระบบสามารถสร้าง แก้ไข และสามารถส่งไฟล์คอนฟิกูเรชันไปยังเครื่องให้บริการปลายทางได้ โดยระบบสามารถตรวจสอบเพื่อแจ้งเตือนแก่ผู้ใช้งานทราบว่า มีบุคคลอื่นทำการแก้ไขไฟล์ดังกล่าวโดยตรงที่เครื่องให้บริการปลายทางหรือไม่ก่อนทำการส่ง
5. ในการบริหารจัดการบริการที่ติดตั้งที่เครื่องให้บริการปลายทางนั้น จะเน้นไปที่บริการที่ติดตั้งผ่าน Ports เท่านั้น
6. ระบบสามารถทำการสำรองและกู้คืนไฟล์ระบบให้แก่เครื่องให้บริการปลายทางได้

### 1.4 องค์ประกอบของระบบงาน

ระบบงานประกอบด้วยองค์ประกอบต่างๆ ดังต่อไปนี้

1.4.1 เครื่องคอมพิวเตอร์เซิร์ฟเวอร์ตัวกลาง ระบบปฏิบัติการ FreeBSD ทำหน้าที่เก็บค่า Configuration ของบริการต่างๆ ซึ่งได้รับการเตรียมความพร้อมดังนี้

- ติดตั้งระบบปฏิบัติการ FreeBSD version 6.0
- ติดตั้งส่วนให้บริการเว็บเซิร์ฟเวอร์สำหรับเป็นส่วนติดต่อกับผู้ใช้เพื่อใช้ในการควบคุมระบบ โดยเลือกใช้ Apache เวอร์ชัน 2.0.53
- ติดตั้งซอฟต์แวร์ภาษา โดยเลือกใช้ PHP เวอร์ชัน 5
- ติดตั้งระบบจัดการฐานข้อมูล MySQL
- เขียนโปรแกรม Shell Script บนเครื่องตัวกลาง เพื่อทำหน้าที่ลดขั้นตอนในการทำงานต่างๆ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- เปิดการใช้งาน SSH (Secure Shell)
- สร้างกุญแจคู่ เพื่อใช้ในการติดต่อไปยังเครื่องให้บริการปลายทาง
- เปิดการใช้งาน Crontab เพื่อใช้ตั้งเวลาในการทำงานต่างๆ
- ติดตั้งโปรแกรมระบบจัดการบริการระยะไกลผ่านเว็บ

#### 1.4.2 เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นเครื่องให้บริการ ทำหน้าที่ให้บริการตามซอฟต์แวร์ที่ติดตั้งไว้ ซึ่งได้รับการเตรียมความพร้อมดังนี้

- ติดตั้งระบบปฏิบัติการ FreeBSD version 6.0
- ติดตั้งซอฟต์แวร์ที่ทำหน้าที่ให้บริการต่างๆตามชนิดของบริการที่ต้องการเช่น Squid Proxy Server, IPFIREWALL หรือ Apache Web Server เป็นต้น
- เปิดการใช้งาน SSH (Secure Shell)
- นำกุญแจสาธารณะ (Public Key) ของเครื่องตัวกลางมาเก็บไว้เพื่อให้เครื่องตัวกลาง สามารถติดต่อเข้ามาได้

#### 1.4.3 เครื่องคอมพิวเตอร์ไคลเอ็นท์ ที่ใช้ควบคุมระบบจัดการบริการระยะไกลผ่านเว็บ ซึ่งได้รับการเตรียมความพร้อมดังนี้

- ติดตั้งระบบปฏิบัติการ Windows XP Professional
- ติดตั้งโปรแกรมเว็บเบราว์เซอร์ สำหรับติดต่อกับเว็บเซิร์ฟเวอร์

### 1.5 ขั้นตอนในการพัฒนาระบบ

ประกอบไปด้วยขั้นตอนต่างๆ ดังนี้

#### 1.5.1 ศึกษาความเป็นไปได้ในการพัฒนาระบบ

เพื่อกำหนดขอบเขตของปัญหาและวางแผนวิธีการพัฒนาโปรแกรม รวมถึงกำหนดเป้าหมายในการพัฒนาโครงการ โดยศึกษา ดังนี้

- ศึกษาวิธีการติดตั้งและการทำงานของซอฟต์แวร์ต่างๆ ที่ใช้สำหรับการสร้างระบบ ได้แก่ ระบบปฏิบัติการ FreeBSD และบริการ (Service) ต่างๆเช่น SSH, Apache Web Server, MySQL, PHP Extension เป็นต้น
- ศึกษาหลักการ ทฤษฎี รวมถึงข้อดีข้อเสียของระบบสารสนเทศแบบกระจาย
- ศึกษาหลักการออกแบบ ติดตั้งเครือข่ายและบริการ (Service) ต่างๆที่จำเป็นในเครือข่าย
- ศึกษาวิธีการเขียน Shell Script Programming

- ศึกษาวิธีการวิเคราะห์และออกแบบระบบโดยใช้ UML (Unified Modeling Language)
- ศึกษาการใช้งานโปรแกรมภาษา PHP Extension เพื่อพัฒนาโปรแกรมประยุกต์ ใน ส่วนของการติดต่อกับผู้ใช้งาน

### 1.5.2 การวิเคราะห์และออกแบบ

ทำการวิเคราะห์และออกแบบรวมถึงกำหนดความต้องการของโครงการพัฒนาระบบ โดยใช้ UML (Unified Modeling Language) ในการออกแบบแบบจำลองเชิงแนวคิด (Conceptual Models)

### 1.5.3 การพัฒนาและทดสอบ

- ทำการติดตั้งเครื่องคอมพิวเตอร์ทั้งหมดตาม Topology ที่ได้ออกแบบไว้และทดสอบการเชื่อมต่อ
- และกำหนดค่า Configuration เบื้องต้นให้แก่เครื่องคอมพิวเตอร์เซิร์ฟเวอร์ตัวกลางและเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นเครื่องให้บริการและทดสอบการทำงานและการเชื่อมต่อ
- ทำการพัฒนาและทดสอบระบบจัดการบริการระยะไกลผ่านเว็บและทดสอบการทำงานของระบบในฟังก์ชันต่างๆ

### 1.5.4 การทดลองใช้งานและปรับปรุงแก้ไข

- นำระบบมาทดลองใช้งานและปรับปรุงแก้ไขเพื่อให้สามารถใช้งานได้ถูกต้องและง่ายยิ่งขึ้น

## 1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้พัฒนาความรู้ความเข้าใจเรื่องการทำงานกับระบบปฏิบัติการฟรีบีเอสดี
2. ได้พัฒนาความรู้ความเข้าใจเรื่องการทำงานของบริการ (Service) ต่างๆ เช่น Squid Proxy Server, IPFWALL หรือ IPNAT บนระบบปฏิบัติการ FreeBSD
3. ได้พัฒนาความรู้ความสามารถในการวิเคราะห์ ออกแบบและพัฒนาระบบงานและสามารถนำไปใช้ประโยชน์ต่อการทำงานในอนาคตได้
4. ได้โปรแกรมประยุกต์ที่ผู้ดูแลระบบหรือผู้ใช้งานทั่วไป สามารถบริหารจัดการและการกำหนดค่า Configuration ของบริการ (Service) ต่างๆ โดยสะดวก รวดเร็ว และ ง่ายต่อการใช้งานยิ่งขึ้นในลักษณะการทำงานแบบเว็บ
5. ได้พัฒนาความรู้ในการออกแบบระบบที่มีประสิทธิภาพ สามารถมีความคงทนต่อความเสียหาย (Fault Tolerance) และสามารถกู้คืน (Recovery) ระบบ ได้เมื่อเกิดความเสียหาย

## บทที่ 2

# การบริหารจัดการเครื่องให้บริการปลายทางระยะไกล

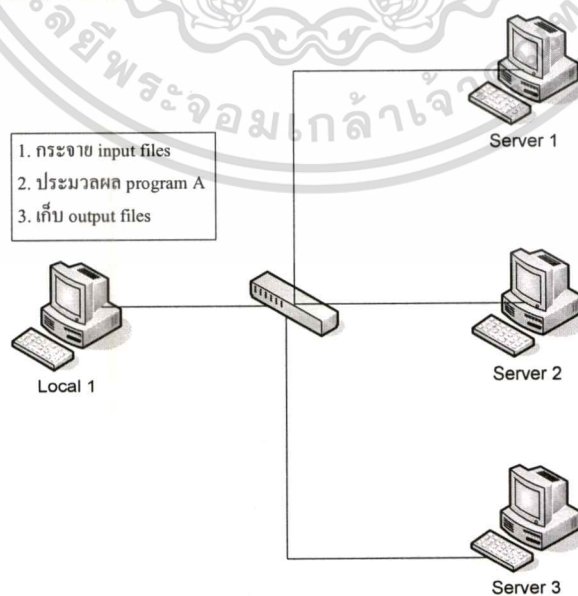
บทนี้จะนำเสนอกระบวนการสำคัญ ที่จำเป็นในการบริหารจัดการเครื่องให้บริการปลายทางระยะไกล โดยจะนำเสนอเกี่ยวกับการติดต่อสื่อสารระหว่างเครื่องต้นทางและปลายทาง การจัดการตารางการทำงานอัตโนมัติ และการสำรองข้อมูล ซึ่งเป็นฟังก์ชันการทำงานที่สำคัญมากของระบบนี้

### 2.1 การใช้ Secure Shell ในการเข้าถึงระบบจากระยะไกล

ในการที่จะใช้งานเครื่องคอมพิวเตอร์ที่ใช้ระบบ Unix หลายๆเครื่องให้ประมวลผลพร้อมๆกันในรูปแบบ parallel computing, distribute computing, หรือ cluster computing ได้นั้น ผู้ดูแลระบบจำเป็นต้องสามารถสั่งงานให้เครื่องคอมพิวเตอร์เหล่านั้นประมวลผลหรือถ่ายเทไฟล์ข้อมูลระหว่างกันได้โดยไม่ต้องใช้ password ยกตัวอย่างเช่น ตัวอย่างเช่นผู้ดูแลระบบใช้เครื่องคอมพิวเตอร์ชื่อ local1 อยู่และมี เครื่องคอมพิวเตอร์เครื่องอื่นๆอีก 3 เครื่องได้แก่เครื่อง server1, server2, และ server3 ดังรูปที่ 2.1 ผู้ดูแลระบบต้องการที่จะทำงานต่อไปนี้

1. คัดลอกข้อมูล input files จากเครื่อง local1 ไปยัง server1, server2 และ server3
2. หลังจากนั้นต้องการ execute program A บนเครื่องดังกล่าว
3. คัดลอกข้อมูล output files กลับมายังเครื่อง local1 ของผู้ดูแลระบบ

การทำงานในลักษณะนี้เป็นเรื่องที่ยุ่งยากมากหากผู้ดูแลระบบต้องพิมพ์ Password ทุกครั้งเมื่อต้องการจะทำ remote execution หรือ transfer files ดังนั้นการทำงานร่วมกันโดยไม่ต้องพิมพ์ password จึงมีประโยชน์มากกับการทำงานในลักษณะนี้



รูปที่ 2.1 ตัวอย่างการทำงานของผู้ดูแลระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### 2.1.1 telnet และ rsh

ในการติดต่อเข้าใช้งานเครื่องคอมพิวเตอร์ในระบบเครือข่ายนั้นผู้ดูแลระบบสามารถทำได้หลายวิธี วิธีที่เก่าแก่และเป็นที่ยุติกันทั่วไปก็คือการใช้โปรแกรม telnet ยกตัวอย่างเช่นถ้าผู้ดูแลระบบต้องการล็อกอินเข้าใช้เครื่อง server ชื่อ ft.cs.tu.ac.th ซึ่งมีหมายเลขไอพีคือ 10.0.2.1 ผู้ดูแลระบบสามารถใช้คำสั่ง telnet ft.cs.tu.ac.th หรือ telnet 10.0.2.1 เพื่อทำการดังกล่าวได้ ซึ่งนอกจากคำสั่ง telnet แล้วผู้ดูแลระบบยังสามารถใช้คำสั่ง rsh (remote shell) หรือ rlogin (remote login) ในระบบ Unix เพื่อ log in เข้าสู่ระบบได้ด้วยยกตัวอย่างเช่น rsh ft.cs.tu.ac.th -l kasidit หรือ rlogin ft.cs.tu.ac.th -l kasidit โดยที่ kasidit คือ account ของผู้ดูแลระบบ

ข้อเสียของทั้งสองวิธีนั้นคือมีปลอดภัยน้อย โปรแกรม telnet และ rsh นั้นจะส่งชื่อ account และ password ไปที่เครื่อง server ไปบนระบบเครือข่ายโดยไม่มีการเข้ารหัสซึ่งทำให้ผู้ไม่หวังดีสามารถขโมยข้อมูลดังกล่าวจากระบบเครือข่ายได้

ในการที่จะทำงานโดยไม่ใส่ password นั้นผู้ดูแลระบบสามารถใช้ rsh และ rlogin ได้ โดยการสร้าง file ชื่อ .rhosts ไว้ที่ \$HOME directory ของ user บนเครื่อง server และระบุชื่อของ local คอมพิวเตอร์ แต่ก็ไม่ปลอดภัยอีกเพราะถ้า hacker เข้ามาที่เครื่อง local คอมพิวเตอร์ ได้เขาก็สามารถเข้าใช้เครื่อง server ได้ทันที

### 2.1.2 การใช้ ssh

เพื่อความปลอดภัยในการใช้งานเครื่อง server และในการสื่อสารระหว่างเครื่อง local คอมพิวเตอร์กับ server ผู้ดูแลระบบสามารถใช้โปรแกรม secured shell หรือ ssh ในการ login โดยใช้คำสั่ง

```
$ ssh kasidit@ft.cs.tu.ac.th
```

ซึ่งจะสร้างการติดต่อที่มีการเข้ารหัสข้อมูลระหว่างโปรแกรม ssh บนเครื่อง local คอมพิวเตอร์กับโปรแกรม ssh ซึ่งทำงานอยู่บนเครื่องเซิร์ฟเวอร์ (ft.cs.tu.ac.th)

ในการทำงานของ ssh นั้น ssh จะให้บริการการ remote login ผู้เครื่อง server ในหลายรูปแบบตามการติดตั้งของผู้ใช้ โดยคร่าวๆ ssh จะตรวจสอบว่าผู้ใช้ติดตั้ง ssh-agent ไว้หรือเปล่า ถ้าใช่ก็จะให้ ssh-agent ช่วยจัดการการ remote login แต่ถ้าไม่มี ssh-agent ก็จะดูว่าผู้ใช้ติดตั้ง public keys และ private keys หรือไม่ ถ้ามีก็จะใช้ keys ในการ remote login ถ้าไม่มี ก็จะถามหา password เป็นทางเลือกสุดท้าย

วิธีการเหล่านี้มีระดับของความปลอดภัยแตกต่างกันไป แต่อย่างไรก็ตามทุกๆวิธีก็ การส่งข้อมูลระหว่างเครื่องจะมีการเข้ารหัสซึ่งปลอดภัยกว่า telnet และ rsh

### 2.1.3 การติดตั้งและใช้งาน public keys และ private keys เพื่อการ remote login

การ login โดยใช้ ssh แบบใช้ public และ private keys นั้นผู้ดูแลระบบต้องติดตั้ง keys ก่อนซึ่งมีขั้นตอนดังตัวอย่างต่อไปนี้

1. เครื่อง local คอมพิวเตอร์ของผู้ดูแลระบบชื่อ somtum.cs.tu.ac.th และเครื่อง server ชื่อ ft.cs.tu.ac.th ในขั้นแรกนั้นผู้ดูแลระบบต้องสร้าง private key และ public key โดยใช้คำสั่ง ssh-keygen ดังรูปที่ 2.2

```

kasidit@ft.cs.tu.ac.th: /home/kasidit
[kasidit@somtum ~]$
[kasidit@somtum ~]$
[kasidit@somtum ~]$
[kasidit@somtum ~]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kasidit/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kasidit/.ssh/id_rsa.
Your public key has been saved in /home/kasidit/.ssh/id_rsa.pub.
The key fingerprint is:
d8:0c:72:9c:fb:c0:2e:5d:c8:5e:29:7c:8c:60:c8:85 kasidit@somtum.cs.tu.ac.th
[kasidit@somtum ~]$
[kasidit@somtum ~]$ ls -l .ssh
total 8
-rw----- 1 kasidit kasidit 951 Sep 3 02:43 id_rsa
-rw-r--r-- 1 kasidit kasidit 236 Sep 3 02:43 id_rsa.pub
[kasidit@somtum ~]$
[kasidit@somtum ~]$

```

รูปที่ 2.2 ขั้นตอนการติดตั้งและใช้งาน public keys และ private keys

โปรแกรม ssh-keygen จะสร้าง private key ในรูปแบบ binary และจะให้ user ใส่ข้อความเรียกว่า passphrase เพื่อนำไปเข้ารหัส private key นั้นก่อนที่จะจัดเก็บลงใน file \$HOME/.ssh/id\_rsa โปรแกรม ssh-keygen จะใช้ private key มาสร้าง public key ใน file \$HOME/.ssh/id\_rsa.pub ด้วยจะสังเกตว่า permission flag ของ files id\_rsa นั้นคือ 600 ของ id\_rsa.pub คือ 644 และของ directory .ssh คือ 700 โปรแกรม ssh, scp และอื่นๆในตระกูลของนี้จะเคร่งครัดกับเรื่อง permission มาก

2. ทำการ copy public key ของผู้ดูแลระบบใน file \$HOME/.ssh/id\_rsa.pub ไปที่ เครื่อง ssh-server และเก็บข้อมูลลงในไฟล์ \$HOME/.ssh/authorized\_keys ใน account ของผู้ดูแลระบบบนเครื่อง ssh-server นั้นดังรูปที่ 2.3

```

kasidit@ft.cs.tu.ac.th: /home/kasidit/.ssh
[kasidit@somtum ~]$
[kasidit@somtum ~]$ cd $HOME/.ssh
[kasidit@somtum ~/.ssh]$ scp id_rsa.pub kasidit@ft.cs.tu.ac.th:id_rsa_somtum.pub
Warning: Permanently added 'ft.cs.tu.ac.th,203.146.19.24' (RSA) to the list of known hosts.
kasidit@ft.cs.tu.ac.th's password:
id_rsa.pub                                1008 236          3.3MB/s   00:00
[kasidit@somtum ~/.ssh]$
[kasidit@somtum ~/.ssh]$ ssh kasidit@ft.cs.tu.ac.th
kasidit@ft.cs.tu.ac.th's password:
[kasidit@ft kasidit]$
[kasidit@ft kasidit]$ mkdir .ssh
[kasidit@ft kasidit]$ chmod 700 .ssh
[kasidit@ft kasidit]$ cd .ssh
[kasidit@ft .ssh]$

```

รูปที่ 2.3 ขั้นตอนการการติดตั้งและใช้งาน public keys และ private keys

จากภาพข้างบน ตอนแรกผู้ดูแลระบบอยู่บนเครื่อง somtum.cs.tu.ac.th แล้ว cd ไปที่ \$HOME/.ssh และ copy file id\_rsa.pub ไปไว้ที่เครื่อง ft.cs.tu.ac.th ภายได้ไฟล์ชื่อ id\_rsa\_somtum.pub ใน \$HOME directory ของ account ของผู้ดูแลระบบที่นั่น จะเห็นว่าโปรแกรม scp จะถาม password ของผู้ดูแลระบบเพื่อใช้ในการ access เครื่อง ft.cs.tu.ac.th

3. หลังจากนั้นผู้ดูแลระบบต้อง log in เข้าสู่เครื่อง ft.cs.tu.ac.th แล้วสร้าง directory .ssh ถ้าไม่มีอยู่แล้ว และต้องเปลี่ยน permission flag ของ .ssh เป็น 700 (or drwx-----) แล้วก็ cd ไปใน .ssh เพื่อ copy file id\_rsa\_somtum.pub ไปไว้ใน file ชื่อ authorized\_keys และเปลี่ยน permission ของ authorized\_keys เป็น 600 (หรือ -rw-----) ดังรูปที่ 2.4

```

[kasidit@somtum ~/.ssh]$
[kasidit@somtum ~/.ssh]$ ssh kasidit@ft.cs.tu.ac.th
kasidit@ft.cs.tu.ac.th's password:
[kasidit@ft kasidit]$
[kasidit@ft kasidit]$ mkdir .ssh
[kasidit@ft kasidit]$ chmod 700 .ssh
[kasidit@ft kasidit]$ cd .ssh
[kasidit@ft .ssh]$
[kasidit@ft .ssh]$ cp ../id_rsa_somtum.pub authorized_keys
[kasidit@ft .ssh]$
[kasidit@ft .ssh]$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEA0SpSariA84XvppWp+1KCJ7YFOAIRc9xrVw/cNb8jXCanBHEmm5xE94f2i3FvNtG7hff8d/rqA4iAp97415wXo3VLGbPQpkJ5Pw8ZvCfsZpEqfSqvqro940j0eI9jJxjthfhdWYPA2iRC0VMvpEa0wNG5Q6bPyhI3M5E= kasidit@somtum.cs.tu.ac.th
[kasidit@ft .ssh]$
[kasidit@ft .ssh]$ chmod 600 authorized_keys
[kasidit@ft .ssh]$
[kasidit@ft .ssh]$

```

รูปที่ 2.4 ขั้นตอนการการติดตั้งและใช้งาน public keys และ private keys

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

#### 4. logout จากเครื่อง ft.cs.tu.ac.th ดังรูปที่ 2.5

```
[kasidit@ft .ssh]$
[kasidit@ft .ssh]$ exit
logout
Connection to ft.cs.tu.ac.th closed.
[kasidit@somtum ~/.ssh]$
[kasidit@somtum ~/.ssh]$
```

รูปที่ 2.5 ขั้นตอนการการติดตั้งและใช้งาน public keys และ private keys

5. หลังจากนั้นเมื่อผู้ดูแลระบบ log in เข้าสู่เครื่อง ft.cs.tu.ac.th ด้วยโปรแกรม ssh ดังรูปที่ 2.6 ระบบก็จะถามหา passphrase (ข้อความที่ผู้ดูแลระบบใส่ตอนที่ผู้ดูแลระบบสร้าง keys โดยใช้คำสั่ง ssh-keygen) แทนที่จะเป็น password

```
[kasidit@somtum ~/.ssh]$
[kasidit@somtum ~/.ssh]$ ssh kasidit@ft.cs.tu.ac.th
Enter passphrase for key '/home/kasidit/.ssh/id_rsa':
[kasidit@ft kasidit]$
[kasidit@ft kasidit]$
```

รูปที่ 2.6 ขั้นตอนการการติดตั้งและใช้งาน public keys และ private keys

ถ้า ssh ยังถามหา password อยู่ นั่นหมายถึงการติดตั้ง files และ directories ต่างๆบนเครื่อง somum.cs.tu.ac.th และ ft.cs.tu.ac.th ยังไม่ถูกต้องให้ไปตรวจสอบชื่อ files และ permission flag ให้เป็นไปตามที่ ssh กำหนด

#### 6. logout ออกมาจาก ft.cs.tu.ac.th กลับมาที่ somtum ดังรูปที่ 2.7

```
[kasidit@ft kasidit]$ exit
logout
Connection to ft.cs.tu.ac.th closed.
[kasidit@somtum ~/.ssh]$
[kasidit@somtum ~/.ssh]$ cd
[kasidit@somtum ~]$
[kasidit@somtum ~]$
```

รูปที่ 2.7 ขั้นตอนการการติดตั้งและใช้งาน public keys และ private keys

### 2.1.4 การใช้งาน ssh-agent เพื่อการ remote login โดยไม่ใช้ passphrase

ถึงจุดนี้ผู้ดูแลระบบได้สร้าง public keys และ private keys และติดตั้ง keys ทั้งสองเพื่อการ remote login เรียบร้อยแล้ว ในขั้นถัดไปผู้ดูแลระบบจะใช้โปรแกรม ssh-agent เพื่อให้ผู้ดูแลระบบสามารถใช้คำสั่ง ssh เพื่อ run command หรือ remote login และใช้คำสั่ง scp เพื่อ copy files ข้ามเครื่องได้โดยไม่ต้องใส่ passphrase บนเครื่อง local คอมพิวเตอร์ (หรือ somtum.cs.tu.ac.th ตามตัวอย่าง) ผู้ดูแลระบบต้องใช้คำสั่ง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

`$ eval `ssh-agent` หรือ $ ssh-agent tcsh`

คำสั่งแรกจะ run โปรแกรม ssh-agent เป็น background process แล้วให้โปรแกรม eval ทำการ set environment variables \$SSH\_AUTH\_SOCK และ \$SSH\_AGENT\_PID เป็นตามค่าที่ ssh agent ตั้งขึ้น หลังจากนั้นจะกลับมารอรับคำสั่งจาก shell ตามเดิม ส่วนคำสั่งที่สองจะทำงานคล้ายกันแต่ว่ามันจะ run sub shell ตัวใหม่ซึ่งในตัวอย่างข้างบนเป็น tcsh มารอรับ คำสั่งจากผู้ใช้อีกต่อไป ผู้ดูแลระบบสามารถเรียกดูข้อมูลของ ssh-agent ได้โดยใช้คำสั่ง `$ ps -fp $SSH_AGENT_PID`

```
[kasidit@somtum ~]$
[kasidit@somtum ~]$ ssh-agent tcsh
[kasidit@somtum ~]$
[kasidit@somtum ~]$ ps -fp $SSH_AGENT_PID
UID      PID  PPID  C  STIME TTY          TIME CMD
kasidit  1605  1604  0  03:12 ?            00:00:00 ssh-agent tcsh
[kasidit@somtum ~]$
[kasidit@somtum ~]$ ssh-add -l
The agent has no identities.
[kasidit@somtum ~]$
[kasidit@somtum ~]$ ssh-add
Enter passphrase for /home/kasidit/.ssh/id_rsa:
Identity added: /home/kasidit/.ssh/id_rsa (/home/kasidit/.ssh/id_rsa)
[kasidit@somtum ~]$
[kasidit@somtum ~]$ ssh-add -l
1024 d8:0c:72:9c:fb:c0:2e:5d:c8:5e:29:7c:8c:60:c8:85 /home/kasidit/.ssh/id_rsa (RSA)
[kasidit@somtum ~]$
```

รูปที่ 2.8 ขั้นตอนการการติดตั้งและใช้งาน public keys และ private keys

มีโปรแกรม ssh-agent อย่างเดียวนั้นอาจจะไม่เพียงพอ การที่ ssh-agent จะมีประโยชน์ขึ้นมาได้นั้นผู้ดูแลระบบจำเป็นต้อง load private key เข้าไปไว้ใน memory ด้วย ในการ load นี้ผู้ดูแลระบบใช้โปรแกรม ssh-add ดังตัวอย่างข้างบน คำสั่ง “ssh-add -l” จะ list finger print ของ private key ที่มีอยู่ใน memory ของ sshagent ผู้ดูแลระบบจะใช้คำสั่ง ssh-add เฉยๆ เพื่อ load private key ไปไว้ใน memory ของ agent จากตัวอย่างข้างบน ssh-add จะไปมองหา private key จาก file \$HOME/.ssh/id\_rsa แล้วจะถาม passphrase จากผู้ใช้เพื่อเอาไปถอดรหัสของ private key แล้วเอาไปเก็บไว้ใน memory ของ ssh-agent โปรแกรม ssh-agent จะทำหน้าที่เป็นตัวแทนของผู้ใช้ในการใช้ private key เพื่อทำการพิสูจน์ตัวตนของผู้ใช้กับเครื่อง server ในระหว่างที่มีการใช้งานคำสั่ง ssh และ scp ต่อไป ซึ่งแสดงดังรูปที่ 2.8

### 2.1.5 การใช้คำสั่ง ssh และ scp

หลังจากนี้เมื่อผู้ดูแลระบบใช้คำสั่ง ssh และ scp ผู้ดูแลระบบไม่จำเป็นต้องใส่ passphrase อีกต่อไปเพราะโปรแกรมทั้งสองจะทำงานร่วมกับ ssh-agent เพื่อให้การส่งงานข้ามเครื่องเป็นไปโดยอัตโนมัติ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## การใช้งาน ssh

การใช้งาน ssh มีรูปแบบดังนี้ `$ ssh account@remote-machine command`

โดยที่ระบบจะส่งคำสั่ง command ไปทำงานบนเครื่อง remote-machine ภายใต้อccount และแสดง output หรือ error บน screen ยกตัวอย่างเช่น

- `$ ssh kasidit@ft.cs.tu.ac.th "ls -l"`

จะ run คำสั่ง "ls -l" บนเครื่อง ft.cs.tu.ac.th ภายใต้อccount "kasidit" และแสดงผลบน screen

- `$ ssh kasidit@ft.cs.tu.ac.th "cat /etc/abcd"`

จะ run คำสั่ง "cat /etc/passwd" บนเครื่อง ft.cs.tu.ac.th ภายใต้อccount "kasidit" และแสดงผลบน screen

- `$ ssh kasidit@ft.cs.tu.ac.th "cat /etc/abcd" > output-local`

จะ run คำสั่ง "cat /etc/abcd" บนเครื่อง ft.cs.tu.ac.th ภายใต้อccount "kasidit" และ redirect output ไปเก็บใน file output-local บน local คอมพิวเตอร์

- `$ ssh kasidit@ft.cs.tu.ac.th "cat /etc/passwd > output-remote"`

จะ run คำสั่ง "cat /etc/abcd" บนเครื่อง ft.cs.tu.ac.th ภายใต้อccount "kasidit" และ redirect output ไปเก็บใน file output-remote บน remote คอมพิวเตอร์ (ft.cs.tu.ac.th)

## การใช้งาน scp

การใช้งาน scp มีรูปแบบดังนี้ `$ scp source-location destination-location` และมีการทำงานดังตัวอย่างต่อไปนี้

- `$ scp fileA kasidit@ft.cs.tu.ac.th:fileAA`

copy file ชื่อ "fileA" จาก local คอมพิวเตอร์ ไปที่เครื่อง remote คอมพิวเตอร์ (ft.cs.tu.ac.th) ไปไว้ใน \$HOME directory ของ account "kasidit" ในชื่อ "fileAA"

- `$ scp kasidit@ft.cs.tu.ac.th:/tmp/fileB mystuffs/fileB`

copy file ชื่อ "fileB" ใน /tmp directory จากเครื่อง ft.cs.tu.ac.th มาไว้ที่ directory "mystuffs" ในชื่อเดิม

- `$ scp -r mystuffs kasidit@ft.cs.tu.ac.th:mystuffs`

copy ข้อมูลใน directory mystuffs ทั้งหมดไปไว้ที่ directory mystuffs บนเครื่อง ft.cs.tu.ac.th option

### 2.1.6 เปรียบเทียบความปลอดภัยระหว่างการใช้ agent และ public และ private key และ password

การใช้ public และ private keys ในการ login สู่ remote server หรือตั้งงานบน remote server นั้นปลอดภัยกว่าการใช้ password เพราะว่าการใช้ password นั้นถ้า account name และ password ถูกขโมยไปคนที่ขโมยก็สามารถใช้ข้อมูลเหล่านี้ login เข้าสู่ remote server ได้ ในกรณีที่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ใช้ public และ private keys นั้นผู้ใช้ต้องใช้ account name, private key, และ passphrase เพื่อ login เข้าสู่ remote server โปรแกรม ssh จะมองหา private key จาก file `$HOME/.ssh/id_rsa` ซึ่งถูกเข้ารหัสไว้ด้วย passphrase ดังนั้นในขณะที่ ssh ทำงานจึงต้องการ passphrase มาถอดรหัสเพื่อนำ private key มาใช้งาน ผู้ที่ต้องการเข้าถึง account ของผู้ดูแลระบบจะต้องมีทั้งสองอย่างนี้ถึงจะ login เข้าสู่เครื่องให้บริการได้

ส่วนในกรณีที่ผู้ดูแลระบบใช้ ssh-agent คนที่ต้องการขโมย private key ต้องสามารถเข้าไปดึงเอาข้อมูลมาจาก memory ของ ssh-agent โดยตรงซึ่งเป็นเรื่องที่ยากมาก

### 2.1.7 การทำงานของ ssh



รูปที่ 2.9 ขั้นตอนการทำงานของ SSH

จากรูปที่ 2.9 ssh มีขั้นตอนการทำงานดังนี้

(1) โปรแกรม ssh สร้าง connection กับโปรแกรม sshd (หรือ ssh server) บน remote คอมพิวเตอร์แล้วส่ง public key จากไฟล์ `$HOME/.ssh/id_rsa.pub` ไปให้ sshd โดยที่ sshd จะรับ public key ไว้แล้วส่ง public key ของตัวเองกลับไป

(2) โปรแกรม ssh จะเช็คว่ามี public key ของ sshd อยู่แล้วหรือไม่ ถ้าไม่มีก็จะเอา public key ที่ได้รับมาไปเข้า Hash function เพื่อสร้าง finger print ออกมาแล้วถามผู้ว่าผู้ใช้ยอมรับ finger print ของ remote ssh server อันนี้หรือไม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

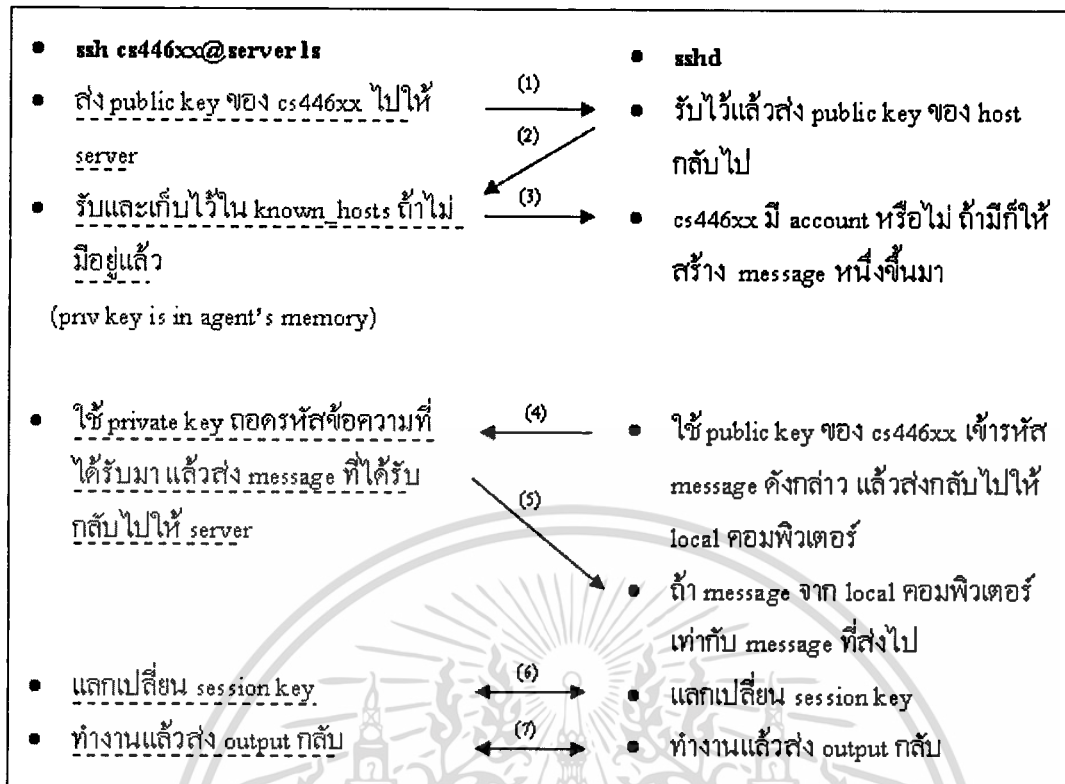
(3) ถ้าผู้ใช้ยอมรับ ssh ก็จะตอบ ok กลับไปให้ sshd ซึ่งหลังจากนั้น sshd จะไปเช็คว่ามี account cs446xx อยู่บนเครื่อง remote server หรือไม่ ถ้ามีก็จะสร้างข้อความ (message) ขึ้นมาหนึ่งข้อความ เพื่อใช้ส่งระหว่างเครื่องเพื่อทดสอบความถูกต้อง public และ private keys ของทั้งฝั่ง client และ server

(4) Sshd จะไปอ่านเอา public key ของ cs446xx ออกมาจากไฟล์ `~cs446xx/.ssh/authorized_keys` และเอา public key ไปเข้ารหัสข้อความ (message) แล้วส่งข้อความที่เข้ารหัสแล้วไปให้โปรแกรม ssh บน local คอมพิวเตอร์

(5) โปรแกรม ssh จะไปดึงเอา private key ออกมาจาก file `$HOME/.ssh/id_rsa` บนเครื่อง local คอมพิวเตอร์และต้องทำการถาม passphrase จากผู้ใช้เพื่อนำไปถอดรหัส file `$HOME/.ssh/id_rsa` เพื่อให้ได้ private key ที่แท้จริงออกมาใช้งาน เมื่อได้ private key นั้นมาแล้ว ssh ก็จะใช้ private key ในการถอดรหัสข้อความ (encrypted message) ที่ได้รับมาจาก sshd แล้วส่งผลลัพธ์ (ซึ่งควรจะเป็นตัว message) กลับไปให้ sshd โปรแกรม sshd จะนำเอาข้อความที่ ssh ส่งมาไปเปรียบเทียบกับ message ที่มันสร้างขึ้นใน step 3 ถ้าเหมือนกันก็แสดงว่า ssh มี private key ที่ถูกต้องและ sshd มีข้อมูล public key ที่ถูกต้อง

(6) หลังจากนั้นทั้ง ssh และ sshd จะแลกเปลี่ยนข้อมูลกันและสร้าง secret key ขึ้นมาตัวหนึ่งซึ่งเป็นที่รู้กันทั้ง 2 ฝั่ง ผู้ดูแลระบบเรียกว่า session key ทั้ง ssh กับ sshd จะใช้ session key นี้สำหรับการเข้าและถอดรหัสข้อมูลที่ส่งระหว่างเครื่องทั้งสองต่อไป

(7) จากตัวอย่างนี้ ssh ก็จะใช้ session key เข้ารหัส "ls" แล้วส่งข้อมูลไปให้ sshd ซึ่งจะใช้ session key ของมันถอดรหัสข้อมูลที่ส่งมา เมื่อ sshd ได้ "ls" ออกมาแล้วมันก็จะออกคำสั่ง ls บน remote คอมพิวเตอร์ แล้วเอา output ที่ได้ส่งกลับไปให้ ssh ซึ่งในการส่งนี้ sshd และ ssh ก็จะใช้ session key ในการเข้าและถอดรหัสเช่นกัน



รูปที่ 2.10 ขั้นตอนการทำงานของ SSH เมื่อใช้ ssh-agent

จากรูปที่ 2.10 ในกรณีที่ผู้ดูแลระบบใช้ ssh-agent นั้น ssh จะส่งต่อคำสั่งที่ได้รับให้กับ ssh-agent ซึ่งจะทำงานแทน ssh ตั้งแต่ ขั้นตอนที่ 1 จนจบ ดังแสดงด้วยตัวอักษรที่ขีดเส้นใต้ด้วยเส้นปะ จะสังเกตว่าใน ขั้นตอนที่ 4 นั้น ssh-agent ไม่จำเป็นต้องถาม passphrase จากผู้ใช้เพื่อนำไปถอดรหัส private key เนื่องจากมี private key ที่ได้รับการถอดรหัสแล้วเก็บไว้ในหน่วยความจำ และพร้อมที่จะใช้งานทันที

## 2.2 การจัดตารางการทำงานอัตโนมัติ (crontab)

คำสั่ง Crontab เป็นคำสั่งในการทำ Schedule ในการสั่งโปรแกรม หรือ Script ต่าง ๆ ทำงานตามเวลาที่กำหนด บนระบบ Unix/Linux ซึ่งอำนวยความสะดวกได้เป็นอย่างมาก งานบางอย่างที่จำเป็นต้องทำซ้ำๆ ในเวลาเดียวกันไม่ว่าจะทุกวัน ทุกสัปดาห์ หรือทุกเดือน เช่นสั่งให้ clear log ของ Squid ทุกเที่ยงคืนของวันอาทิตย์

คำสั่งและ option ของ crontab มีดังนี้

**Crontab [-u user] {-l | -r | -e} file**

#crontab <filename> การนำเอาคำสั่ง crontab เข้ามาจาก ไฟล์อื่น

#crontab -e การแก้ไข crontab ด้วยเอดิเตอร์ดีฟอลต์เช่น vi

#crontab -l ดูคำสั่ง crontab ทั้งหมดที่มีอยู่

#crontab -r ลบคำสั่ง crontab ที่มีทั้งหมด

#crontab -u user เป็นคำสั่งของผู้ดูแลระบบเท่านั้น เพื่อใช้ดู แก้ไข ลบ crontab ของ user แต่

ละคน

Format ของคำสั่ง crontab มีทั้งหมด 6 fields ดังนี้

minute	hour	day	month	day of week	command
--------	------	-----	-------	-------------	---------

**minute** มีค่า 0 - 59 เวลาเป็นนาที จะสั่งให้คำสั่งที่กำหนดทำงานทันทีเมื่อถึงนาทีที่กำหนด

**hour** มีค่า 0 - 23 เวลาเป็นชั่วโมง จะสั่งให้คำสั่งที่กำหนดทำงานทันทีเมื่อถึงชั่วโมงที่

กำหนด

**day** มีค่า 1 - 31 เวลาเป็นวัน จะสั่งให้คำสั่งที่กำหนดทำงานทันทีเมื่อถึงวันที่กำหนด

**month** มีค่า 1 - 12 เวลาเป็นเดือน จะสั่งให้คำสั่งที่กำหนดทำงานทันทีเมื่อถึงเดือนที่

กำหนด

**day of week** มีค่า 0 - 6 โดยที่วันของแต่ละสัปดาห์ มีค่าดังนี้ (อาทิตย์ = 0, จันทร์ = 1,

อังคาร = 2, พุธ = 3, พฤหัสบดี = 4, ศุกร์ = 5 ,เสาร์ = 6 )

ตัวอย่างเช่น

**0 0 \* \* 0 /usr/local/squid/sbin/squid -k rotate**

เป็นการสั่งให้ Clear log ของ Squid ทุกเที่ยงคืนของวันอาทิตย์

## 2.2.1 ตัวอย่างการใช้ crontab จากไฟล์ที่สร้างไว้

ผู้ดูแลระบบสามารถใช้คำสั่ง crontab เพื่อสั่งงานให้ server ทำงานตามวันเวลาที่ผู้ดูแลระบบต้องการได้ดังนี้

สร้างไฟล์ เช่น

```
# ee test.cron <-- ใช้ editor ee ในการสร้างไฟล์ชื่อ test.cron
```

พิมพ์ข้อความต่อไปนี้ลงไปในไฟล์

```
0 5 * * * cp /home/kitti/data1.txt /home/kitti/data2.txt
```

อธิบาย:

0 คือ นาทีที่ 0 ซึ่งค่าเป็นไปได้คือ (0-59)

5 คือ ตีห้า ซึ่งค่าเป็นไปได้คือ (0-23)

\* คือ ทุกวัน ซึ่งค่าเป็นไปได้คือ (1-31)

\* คือ ทุกเดือน ซึ่งค่าเป็นไปได้คือ (1-12)

\* คือ ทุกวันของสัปดาห์ ซึ่งค่าเป็นไปได้คือ (0-6)

จากนั้นทำการบันทึกไฟล์นี้

การสั่งให้ crontab ให้ทำงานตามวันเวลาดังกล่าวใช้คำสั่งดังต่อไปนี้

```
# crontab kitti.cron <-- เป็นการสั่งให้ crontab ทำงานตามวันเวลาดังกล่าว
```

## 2.2.2 ปัญหาของ crontab กับเวลา (System Clock)

บางครั้งเมื่อผู้ดูแลระบบสั่งให้ crontab ทำงานแล้ว crontab ไม่ยอมทำงานอาจเนื่องมาจากเวลา (System Clock) ของ BIOS บนเครื่องเซิร์ฟเวอร์ไม่ตรงกับของระบบปฏิบัติการ FreeBSD ทางแก้ไขคือ เซตวัน เวลา ใหม่ด้วยคำสั่ง date เช่น date 200602100950 หมายถึงวันที่ 10 กุมภาพันธ์ พ.ศ. 2006 เวลา 9.50น. จากนั้นสั่งรัน crontab ใหม่อีกครั้ง

## 2.2.3 ปัญหาของพาทคำสั่ง

ในการกำหนดคำสั่งให้ crontab ทำงาน จะต้องกำหนดพาทหรือไคเรกทอรีปลายทางให้ถูกต้องด้วยเช่น จะตั้งเวลาเพื่อสั่ง shutdown เครื่องด้วย crontab ผู้ดูแลระบบต้องกำหนดพาทของคำสั่งในการชัตดาวน์ด้วยเช่น

```
30 20 * * sat /sbin/shutdown -h now
```

แต่ถ้าใส่พาทผิดเช่น /bin/sh/shutdown -h now จะได้รับข้อความแจ้งเตือนว่า ... “/bin/sh:

line 1 shutdown: command not found”

## 2.3 การสำรองข้อมูล

การสำรองข้อมูลเป็นการป้องกันการสูญเสียชีวิตข้อมูล จากข้อผิดพลาดที่เกิดจากข้อผิดพลาดในการทำงานของมนุษย์ การทำงานผิดพลาดของระบบและอุปกรณ์เกิดความเสียหาย ซึ่งจะอยู่นอกเหนือการควบคุม

### 2.3.1 ผู้มีหน้าที่ในการสำรองข้อมูล

ใช้งานส่วนใหญ่จะเข้าใจว่างานสำรองข้อมูลจะเป็นหน้าที่ของผู้ดูแลระบบเท่านั้น แต่ในความเป็นจริงแล้วก็เป็นหน้าที่ของผู้ใช้งานด้วย เนื่องจากผู้ดูแลระบบจะสำรองข้อมูลตามระยะเวลาที่กำหนดไว้เท่านั้น เช่นสำรองข้อมูลสัปดาห์ละครั้งหรือเดือนละครั้ง ถ้าข้อมูลสูญหายหลังจากที่สำรองข้อมูลไว้แล้วก็สามารถเรียกคืนได้ แต่ถ้าข้อมูลเสียหายก่อนที่จะทำการสำรองข้อมูลก็ไม่สามารถเรียกคืนกลับมาได้ ระยะเวลาของการสำรองข้อมูลที่ปลอดภัยที่สุดก็คือการสำรองข้อมูลทันทีที่มีการเปลี่ยนแปลง ซึ่งผู้รับผิดชอบในงานแต่ละอย่างเท่านั้นจึงจะทราบระยะเวลาที่เหมาะสมในการสำรองข้อมูล ดังนั้นผู้ดูแลระบบจึงแบ่งหน้าที่ในการสำรองข้อมูลออกเป็นสองส่วนคือ

- การสำรองข้อมูลโดยผู้ใช้งานทั่วไป
- การสำรองข้อมูลโดยผู้ดูแลระบบ

#### การสำรองข้อมูลโดยผู้ใช้งานทั่วไป

ถึงแม้ว่าจะมีระบบสำรองข้อมูลรวมอยู่แล้ว การสำรองข้อมูลโดยผู้ใช้งานทั่วไปก็ยังมีความจำเป็นอยู่ เนื่องจากการสำรองข้อมูลตามความต้องการของผู้ใช้งานเองแยกจากระบบสำรองข้อมูลรวม ซึ่งได้เปรียบดังนี้

- เลือกช่วงเวลาสำรองข้อมูลได้เองจะให้อยู่แค่ไหนก็ได้
- สามารถเรียกคืนข้อมูลได้ด้วยตนเองไม่ต้องขอความช่วยเหลือจากผู้ดูแลระบบ

การสำรองข้อมูลของผู้ใช้งานมักจะสำรองข้อมูลแล้วเก็บลงไฟล์ มากกว่าที่จะเก็บลงเทป เนื่องจากผู้ใช้งานทั่วไปจะไม่มีสิทธิ์ในการเขียนและอ่านเทป และมักจะใช้คำสั่ง tar หรือ cp ในการสำรองข้อมูล และคำสั่ง gzip ในการบีบอัดข้อมูล

#### การสำรองข้อมูลโดยผู้ดูแลระบบ

ถึงแม้ว่าผู้ใช้งานจะทำหน้าที่สำรองข้อมูลของตนเองอยู่แล้ว ผู้ดูแลระบบก็ยังคงทำหน้าที่สำรองข้อมูลอยู่ เนื่องจากผู้ใช้งานไม่มีสิทธิ์เข้าถึงข้อมูลของผู้ใช้งานคนอื่นและไม่มีสิทธิ์เข้าถึงข้อมูลในส่วนของระบบปฏิบัติการ ดังนั้นผู้ดูแลระบบจึงต้องทำหน้าที่สำรองข้อมูลในส่วนนี้สำรองข้อมูลโดยผู้ดูแลระบบนั้นจะทำการสำรองข้อมูลทั้งหมดในระบบตามระยะเวลาที่กำหนด โดยแบ่งเป็นการสำรองข้อมูลทั้งไฟล์ซิสเต็มและการสำรองข้อมูลบางส่วน

การสำรองข้อมูลบางส่วนของไฟล์ซิสเต็ม มักจะควบคู่ไปกับการสำรองข้อมูลทั้งไฟล์ซิสเต็ม เพื่อความรวดเร็วในการเรียกคืนข้อมูล เช่น สำรองข้อมูลรายชื่อผู้ใช้งาน รหัสผ่าน สคริปต์การเปิดปิดเครื่อง ฯลฯ แยกออกมาอีกชุดหนึ่งเพื่อให้เรียกคืนข้อมูลได้อย่างรวดเร็ว เนื่องจากการเรียกคืนข้อมูลทั้งไฟล์ซิสเต็มจะใช้เวลาานาน ผู้ดูแลระบบอาจจะใช้คำสั่ง tar หรือคำสั่ง cp ธรรมดาในการสำรองข้อมูลบางส่วนได้

### 2.3.2 การสำรองข้อมูลบางส่วนด้วยคำสั่ง tar

คำสั่ง tar จะทำหน้าที่รวบรวมไฟล์หรือไดเรกทอรีจำนวนมาก เก็บเป็นไฟล์ๆ เดียวหรือเก็บลงเทป โดยมีรูปแบบคำสั่งที่ใช้สำหรับระบบการสำรองข้อมูลดังนี้

tar [ctxvf] [ชื่ออุปกรณ์หรือไฟล์ผลลัพธ์] [ไดเรกทอรีหรือไฟล์ต้นฉบับ]

ออปชัน การใช้งาน

c สร้างไฟล์ tar จากไฟล์หรือ ไดเรกทอรีที่กำหนด

x เปลี่ยนไฟล์ tar เป็นไฟล์หรือ ไดเรกทอรีเดิม

t ขอชื่อไฟล์และ ไดเรกทอรีที่เก็บไว้ในรูปแบบ tar

v ขอดูรายละเอียดการทำงาน

f ระบุไฟล์หรืออุปกรณ์ที่ใช้เก็บข้อมูล

ตัวอย่างที่ 1 การใช้คำสั่ง tar ในการสำรองข้อมูลบางส่วนผู้ดูแลระบบทำสำรองรายชื่อผู้ใช้งาน โดยใช้คำสั่ง tar สำรองข้อมูลไฟล์ /etc/passwd และไฟล์ /etc/group เก็บไว้ก่อนที่จะเพิ่มรายชื่อผู้ใช้งานใหม่เข้าในระบบ ซึ่งจะทำทุกครั้งก่อนที่จะมีการเพิ่มรายชื่อผู้ใช้งาน เพื่อความสะดวกและรวดเร็วในการทำงาน ผู้ดูแลระบบจะสำรองข้อมูลเก็บไปเป็นไฟล์แทนที่จะเป็นเทปในการทำงาน

```

1: #mkdir /backup
2: #cd /etc
3: #tar cvf /backup/15April2001.tar passwd group
4: a passwd 2 Blocks
5: a group 1 Blocks
6: #tar tvf /backup/15April2001.tar
7: Blocksize = 20
8: -rw-r-r-- 0/0 838 Apr 16 16:18:51 2001 passwd
9: -rw-r-r-- 3/4 838 Apr 5 13:32:49 2000 group
10: #cd /tmp
11: #tar xvf /backup/15April2001.tar
12: blocksize = 20
13: x passwd, 838 bytes, 2 tape blocks
14: x group, 341 bytes, 1 tape blocks
15: #ls -al
16: -rwxr-xr-x 1 bin bin 341 Apr 16 16:18 group
17: -rw-r--r-- 1 root system 838 Apr 16 16:18 passwd
18: #

```

### คำอธิบาย

บรรทัดที่ 1 สร้างไดเรกทอรีสำหรับเก็บข้อมูลที่สำรองด้วยคำสั่งไฟล์ คำสั่ง mkdir

บรรทัดที่ 2 ใช้คำสั่ง cd ย้ายไดเรกทอรีไปยังไดเรกทอรีที่เก็บไฟล์ที่ต้องการสำรองข้อมูล

บรรทัดที่ 3 ใช้คำสั่ง tar ในการเก็บรวมไฟล์ passwd และ group เป็นไฟล์ /backup/15April2001.tar

บรรทัดที่ 4-5 ผลลัพธ์หน้าจอของคำสั่ง tar

บรรทัดที่ 6 ใช้คำสั่ง tar ออปชัน tvf เพื่อดูรายชื่อไฟล์ที่เก็บไว้ในไฟล์ /backup/15April2001.tar

บรรทัดที่ 7-9 รายละเอียดชื่อไฟล์ที่เก็บไว้ในไฟล์ /backup/15April2001.tar

บรรทัดที่ 10 ใช้คำสั่ง cd เปลี่ยนไดเรกทอรีไปยังไดเรกทอรีชั่วคราวของระบบ (/tmp)

บรรทัดที่ 11 ใช้คำสั่ง tar ออปชัน xvf เพื่อเรียกคืนไฟล์ลงไว้ในไดเรกทอรีปัจจุบัน

บรรทัดที่ 12-14 ขั้นตอนการเรียกคืนข้อมูล

เอกสารนี้เป็นเอกสารที่จัดทำขึ้นเพื่อใช้ในการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า

ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บรรทัดที่ 15 แสดงรายชื่อไฟล์ที่เรียกค้น ด้วยคำสั่ง "ls -al"

บรรทัดที่ 16-17 แสดงผลลัพธ์ของคำสั่ง "ls -al"

ตัวอย่างที่ 2 การบีบอัดข้อมูลและขยายข้อมูลด้วยคำสั่ง gzip, gunzip

หลังจากที่สำรองข้อมูลด้วยคำสั่ง tar แล้ว จะทำการบีบอัดข้อมูลอีกครั้งด้วยคำสั่ง gzip เพื่อให้ใช้เนื้อที่ในการจัดเก็บน้อยลง และใช้คำสั่ง gunzip เมื่อต้องการขยายข้อมูลจากการบีบอัด

รูปแบบคำสั่ง gzip [ชื่อไฟล์], gunzip [ชื่อไฟล์.gz]

```

1: #cd /backup
2: #ls -al
3: total 26
4: drwxr-xr-x 2 root system 8192 Apr 16 16:45 .
5: drwxr-xr-x 22 root system 8192 Apr 16 16:45 ..
6: -rw-r--r-- 1 root system 10240 Apr 16 16:45 15April2001.tar
7: #gzip 15April2001.tar
8: #ls -al
9: drwxr-xr-x 2 root system 8192 Apr 16 16:45 .
10: drwxr-xr-x 22 root system 8192 Apr 16 16:45 ..
11: -rw-r--r-- 1 root system 785 Apr 16 16:45 15April2001.tar.gz
12: #gunzip 15April2001.tar.gz
13: #ls -al
14: drwxr-xr-x 2 root system 8192 Apr 16 16:45 .
15: drwxr-xr-x 22 root system 8192 Apr 16 16:45 ..
16: -rw-r--r-- 1 root system 10240 Apr 16 16:45 15April2001.tar
17: #
  
```

### คำอธิบาย

บรรทัดที่ 1 ใช้คำสั่ง cd ย้ายไดเรกทอรีไปยังไดเรกทอรีที่เก็บไฟล์ที่ต้องการบีบอัดข้อมูล

บรรทัดที่ 2 ใช้คำสั่ง "ls -al" เพื่อแสดงรายชื่อและขนาดของไฟล์

บรรทัดที่ 3-6 แสดงผลลัพธ์ของคำสั่ง ls ไฟล์ 15April2001.tar มีขนาด 10240 ไบต์

## ห้องสมุดคณะเทคโนโลยีสารสนเทศ พระจอมเกล้าลาดกระบัง

บรรทัดที่ 7 ใช้คำสั่ง `gzip` ในการบีบอัดข้อมูลให้ไฟล์ `15April2001.tar` ให้เป็นไฟล์ `15April2001.tar.gz`

บรรทัดที่ 8 ใช้คำสั่ง `"ls -al"` เพื่อดูรายชื่อไฟล์และขนาดของไฟล์ที่เกิดจากการบีบอัดข้อมูล

บรรทัดที่ 11 ขนาดของไฟล์ที่เกิดจากการบีบอัดข้อมูลลดลงเหลือ 785 ไบต์

บรรทัดที่ 12 ใช้คำสั่ง `gunzip` ในการขยายข้อมูลจากไฟล์ `15April2001.tar.gz` ให้เป็นไฟล์ `15April2001.tar`

บรรทัดที่ 16 แสดงขนาดไฟล์ที่ขยายกลับคืนเท่าเดิม 10240 ไบต์

เนื้อหาที่น่าสนใจในบทนี้ คือเนื้อหาบางส่วนที่มีความสำคัญอย่างมากในการพัฒนาระบบจัดการบริการระยะไกลผ่านเว็บ โดยผู้พัฒนาได้เลือกใช้บริการที่มีอยู่แล้วในระบบปฏิบัติการฟรีบีเอสดี ซึ่งผู้ใช้สามารถใช้งานได้ทันทีโดยไม่ต้องจัดหาติดตั้งเพิ่มเติม

ในส่วนของการติดต่อสื่อสารไปยังเครื่องให้บริการปลายทาง ผู้พัฒนาได้เลือกใช้ SSH (Secure Shell) ซึ่งเป็นบริการที่มีความปลอดภัยสูง ฟังก์ชันการทำงานส่วนใหญ่ของระบบต่างก็จำเป็นต้องใช้บริการนี้แทบทั้งสิ้น และในการสำรองไฟล์ระบบนั้นผู้พัฒนาใช้ `crontab` ร่วมกับคำสั่ง `tar` ซึ่งเป็นคำสั่งพื้นฐานที่ใช้งานได้ง่ายและไม่ซับซ้อนมากนัก เพื่อให้ผู้ที่จะนำไปพัฒนาต่อสามารถเข้าใจกระบวนการทำงานของระบบได้อย่างรวดเร็ว

## บทที่ 3

# การวิเคราะห์ระบบ

### 3.1 ความต้องการของระบบงาน

#### 3.1.1 Functional Requirements

1. สามารถป้อนข้อมูลที่จำเป็นสำหรับการกำหนดค่า Configuration ต่างๆสำหรับแต่ละบริการ (Service) ในเครื่องให้บริการได้
2. สามารถเพิ่ม ลบ หรือ แก้ไขไฟล์ Configuration ต่างๆที่สร้างขึ้นเพื่อแต่ละบริการ (Service) ในเครื่องให้บริการ ได้
3. สามารถจัดการเครื่องให้บริการต่างๆที่อยู่ภายใต้การควบคุมเช่นการเปิด ปิด หรือเรียกดูสถานะการทำงานของบริการต่างๆได้
4. สามารถกำหนดเวลาให้เครื่องให้บริการทำการ Backup ไฟล์ระบบทั้งหมดซึ่งอยู่ในรูปแบบของไฟล์อิมเมจได้ โดยสามารถระบุเวอร์ชันหรือวัน เดือน ปี ที่สำรองข้อมูล และสามารถดาวน์โหลดไฟล์ดังกล่าวมาเก็บไว้ที่ Centralize Server ได้โดยอัตโนมัติ
5. สามารถทำการ Recovery ไฟล์ระบบทั้งหมดตามเวอร์ชันที่ต้องการให้กับเครื่องที่ให้บริการในกรณีที่เกิดความเสียหายได้
6. สามารถทำการ Backup ค่า Configuration ของแต่ละบริการ (Service) ให้อยู่ในรูปแบบของไฟล์ และสามารถทำการดาวน์โหลด (Download) มาเก็บไว้ยังเครื่องคอมพิวเตอร์ใดๆได้
7. สามารถทำการอัปโหลด (Upload) ค่า Configuration ของแต่ละบริการ (Service) ซึ่งอยู่ในรูปแบบของไฟล์จากเครื่องคอมพิวเตอร์ใดๆไปยัง Centralize Server ได้โดยตรง โดยไม่ต้องผ่านขั้นตอนการ Configuration จากระบบ

#### 3.1.2 Non-functional Requirements

##### Recovery Requirement

- เมื่อเครื่องให้บริการใดๆเสียหายหรือไม่สามารถใช้งานได้ เมื่อมีการนำเอาเครื่องสำรองมาใช้งานแทน ระบบสามารถทำการกำหนดค่า Configuration ต่างๆรวมถึงไฟล์ระบบทั้งหมดสำหรับเครื่องสำรองดังกล่าวให้เหมือนเดิมตามที่เครื่องให้บริการเดิมเคยมีได้
- เมื่อเครื่องให้บริการเดิมได้ทำการซ่อมแซมแก้ไขจนสามารถใช้งานได้ตามปกติแล้ว ระบบต้องสามารถกู้คืนค่า Configuration ต่างๆรวมถึงไฟล์ระบบทั้งหมดที่เคยกำหนดไว้แล้วได้

##### Security Requirement

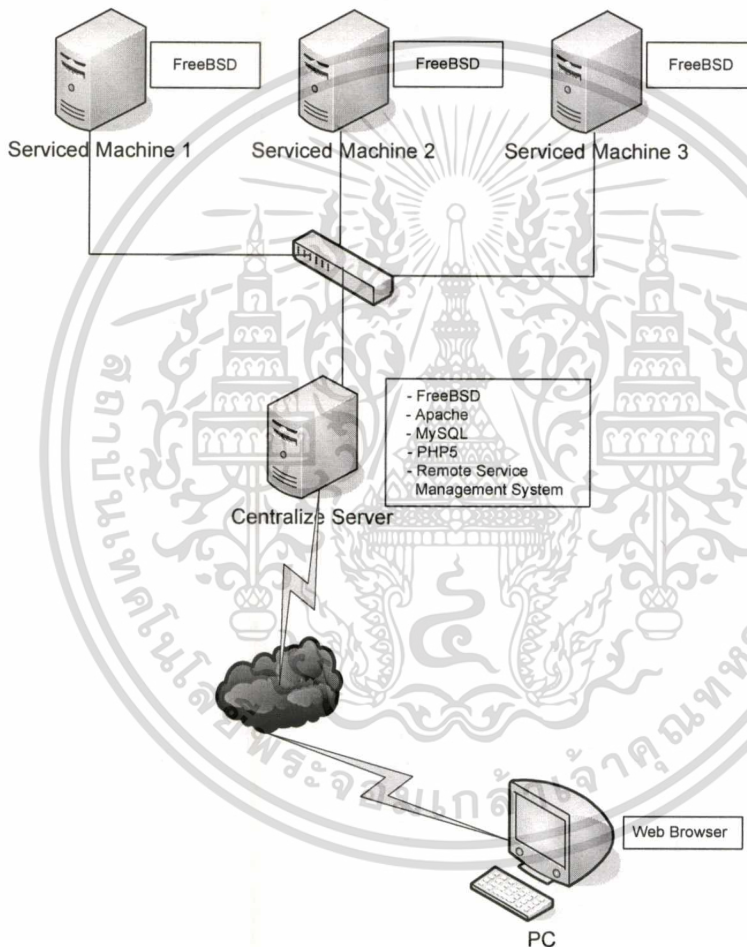
- ระบบมีความปลอดภัยในการรับส่งข้อมูลระหว่าง Centralize Server และ Service ต่างๆ โดยข้อมูลทั้งหมด จะส่งผ่าน SSH (Secure Shell) ซึ่งมีการเข้ารหัสข้อมูลระหว่างการติดต่อ จึงมีความปลอดภัยสูง

- มีการกำหนดสิทธิในการใช้งานระบบ โดยที่จะสามารถใช้งานระบบได้นั้นจะต้องเป็นผู้ที่ได้รับอนุญาตจากผู้ดูแลระบบเท่านั้น

#### Other Requirement

- โปรแกรมทั้งหมดจะติดตั้งที่ Centralize Server เท่านั้น โดยใช้บริการที่มีอยู่แล้วในระบบปฏิบัติการในการติดต่อสื่อสารระหว่างเครื่อง ไม่มีการติดตั้งโปรแกรมเพิ่มเติมบนเครื่องปลายทาง

### 3.2 ภาพรวมของระบบจัดการบริการระยะไกลผ่านเว็บ



รูปที่ 3.1 ภาพรวมของระบบจัดการบริการระยะไกลผ่านเว็บ

จากรูปที่ 3.1 ระบบจัดการบริการระยะไกลผ่านเว็บจะถูกติดตั้งบน Centralize Server ซึ่งพัฒนาโดยใช้ภาษา PHP ในการทำงานของระบบนั้น ผู้ใช้งานจะทำการกำหนดค่า configuration ต่างๆในแต่ละบริการของเครื่องให้บริการแต่ละเครื่องที่ต้องการ ดังแสดงในรูปคือ Serviced Machine1, 2 และ 3 ตามลำดับผ่านทาง Web Browser ซึ่งจะเป็นการทำงานในลักษณะของ Text Editor โดยใช้ความรู้ความสามารถของผู้ดูแลระบบในการกำหนดค่า configuration เอง ทั้งนี้เพื่อเอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่นิยมนำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ความยืดหยุ่นและครอบคลุมทุกๆบริการ โดยไฟล์ configuration ที่สร้างเสร็จแล้วจะถูกเก็บไว้ที่ Centralize Server เพื่อรอรับคำสั่งจากผู้ดูแลระบบสำหรับส่งไฟล์ดังกล่าวไปยังเครื่องให้บริการต่างๆที่อยู่ภายใต้การควบคุมต่อไป

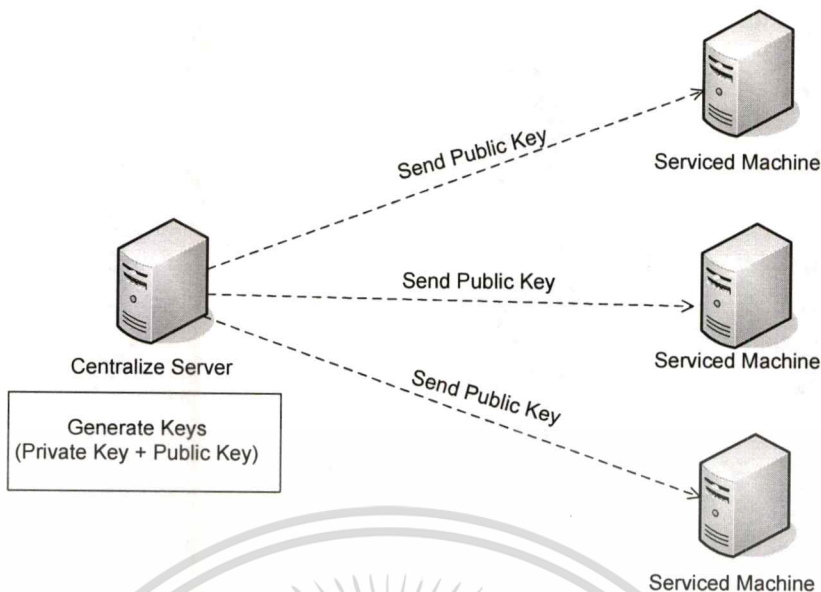
ระบบสามารถกำหนดให้เครื่องให้บริการทำการ Backup ไฟล์ระบบทั้งหมดให้อยู่ในรูปแบบของไฟล์อิมเมจได้อัตโนมัติ โดยการใช้ การทำงานของ crontab มาช่วยซึ่งผู้ใช้สามารถกำหนดเวลาได้ผ่านทาง Web Browser

ในกรณีที่เครื่องให้บริการใดๆเสียหายหรือไม่สามารถใช้งานได้ ระบบสามารถทำการกู้คืนระบบได้โดยทำการส่งอิมเมจของไฟล์ระบบของเครื่องบริการเดิมจาก Centralize Server ให้แก่เครื่องสำรองที่นำมาใช้งานแทน และเมื่อเครื่องที่ให้บริการเดิมได้ทำการซ่อมแซมแก้ไขจนสามารถใช้งานได้ตามปกติแล้ว ระบบจะสามารถกู้คืน (Recovery) ข้อมูลไฟล์ระบบทั้งหมดให้เครื่องให้บริการเดิมได้ตามปกติเดิม ซึ่งการทำงานทั้งหมดผู้ดูแลระบบจะเรียกใช้งานผ่านทาง Web Browser เช่นกัน

ผู้ดูแลระบบสามารถบริหารจัดการเครื่องให้บริการต่างๆที่อยู่ภายใต้การควบคุมเช่นการเปิดปิด หรือเรียกดูสถานะการทำงานของบริการนั้นๆได้ ผ่านทาง Web Browser โดยในการทำงานนั้น Centralize Server จะส่งคำสั่งต่างๆ (command) ไปยังเครื่องให้บริการที่อยู่ภายใต้การควบคุมผ่านทาง SSH (Secure Shell)

#### หลักการทำงานของระบบ

1. ระบบทั้งหมดจะถูกติดตั้งที่ Centralize Server
2. ไฟล์คอนฟิกูเรชันทั้งหมดจะถูกเก็บไว้ที่ Centralize Server เช่นกัน เพื่อรอการส่งไปยัง Serviced Machine ต่อไป
3. เมื่อ Serviced Machine ถูกสั่งให้ทำการสำรองไฟล์ระบบแล้ว อิมเมจของไฟล์ระบบจะถูกดาวน์โหลดมาเก็บไว้ที่ Centralize Server เพื่อนำไปใช้ในการ Recovery ต่อไป
4. การติดต่อระหว่าง Centralize Server และ Serviced Machine จะติดต่อผ่าน SSH (Secure Shell) ดังนั้น Serviced Machine ที่จะติดต่อต้องเปิดบริการ Secure Shell ไว้ด้วยโดย Centralize Server จะทำการสร้างกุญแจคู่ขึ้นมา จากนั้นจึงนำกุญแจสาธารณะของตัวเอง (Public Key) ไปเก็บไว้ที่ Serviced Machine ที่อยู่ภายใต้การควบคุม



5. การจัดการ Serviced Machine ทุกอย่างทำได้โดยการส่งคำสั่งไปยัง Serviced Machine ผ่านทาง Secure Shell เช่น `# ssh root@192.168.1.1 "ls -al"` เป็นต้น
6. คำสั่งในการสั่ง start, stop, restart บริการที่ติดตั้งอยู่บน Serviced Machine ทำได้โดยการสั่งรัน Shell Script ใน `/usr/local/etc/rc.d` ซึ่งเป็น Script ที่ถูกสร้างขึ้นโดยอัตโนมัติเมื่อมีการติดตั้งบริการดังกล่าวผ่าน Port ตัวอย่างเช่น

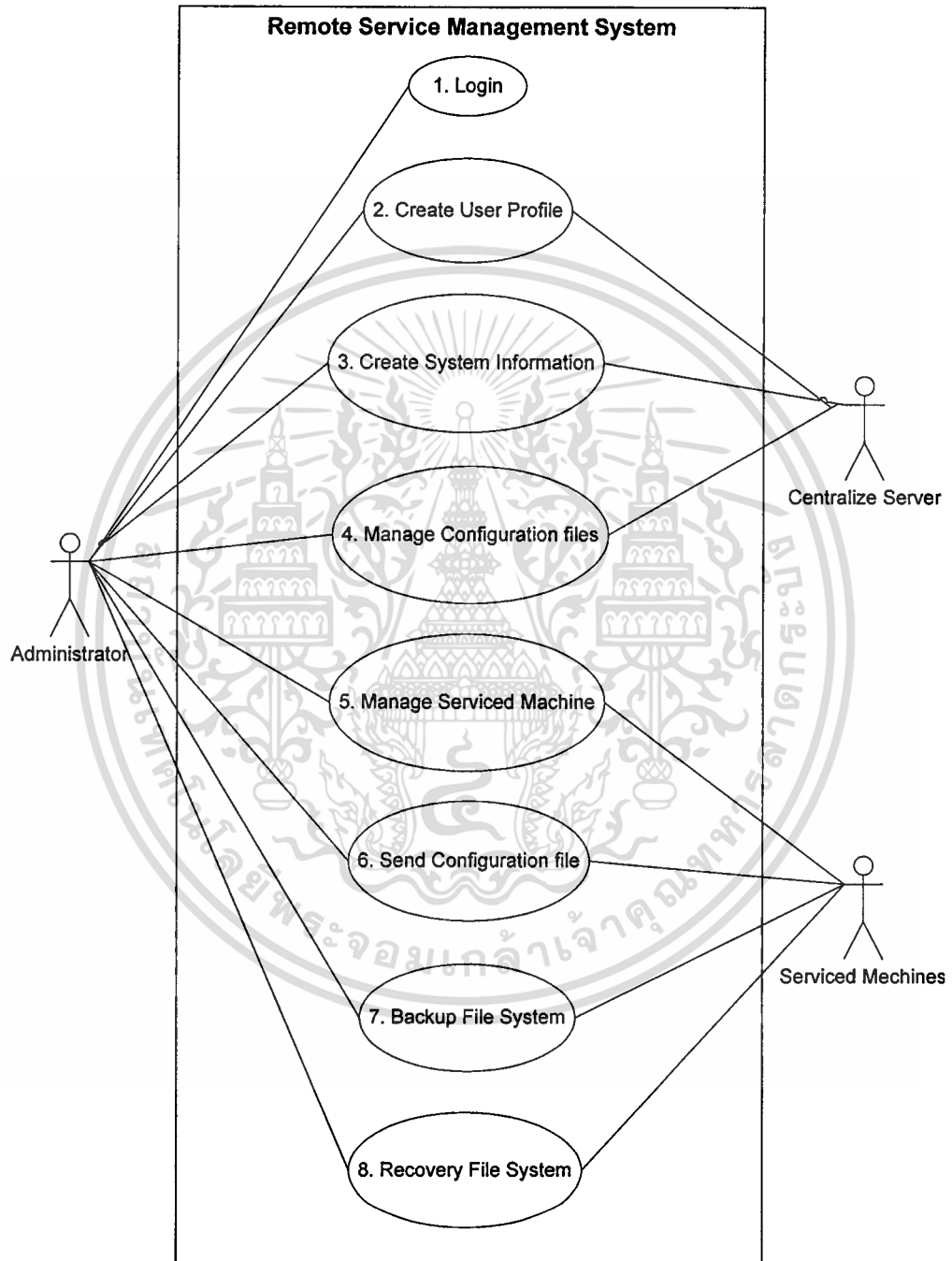
```
# ssh root@192.168.1.1 "/usr/local/etc/rc.d/apache22.sh restart"
```

7. การส่งไฟล์คอนฟิกูเรชันที่สร้างไว้และอิมเมจของไฟล์ระบบไปยัง Serviced Machine จะส่งผ่าน SFTP ซึ่งเป็นบริการที่ Secure Shell มีไว้ให้ โดยระบบจะมีการสร้าง Shell Script ไว้เพื่อรวมขั้นตอนทั้งหมดในการส่งข้อมูลไว้ในคำสั่งเดียว เมื่อต้องการส่งจะทำการรัน Shell Script ดังกล่าวได้เลยเช่น `# ./auto_ftp.sh` เป็นต้น
8. การสั่งให้ Serviced Machine ทำการสำรองไฟล์ระบบ ทำได้โดยการสร้างไฟล์ crontab ที่ทำการกำหนดเวลาในการสำรองข้อมูลไว้แล้ว (โดยใช้คำสั่ง tar) เก็บไว้ที่ Centralize Server จากนั้นทำการส่งไฟล์ดังกล่าวไปยัง Serviced Machine พร้อมกับคำสั่งเพื่อให้ Serviced Machine เริ่มทำงานไฟล์ crontab ดังกล่าว เมื่อถึงเวลาที่กำหนด Serviced Machine ก็จะทำการสำรองข้อมูลทันที

### 3.3 แบบจำลองเชิงแนวคิดของระบบ (Conceptual Models)

#### 3.3.1 Use case model

##### - Use case diagram



รูปที่ 3.2 Use Case Diagram ระบบจัดการบริการระยะไกลผ่านเว็บ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### - คำอธิบายของแต่ละ Actor

Administrator คือ ผู้ดูแลระบบที่มีสิทธิในการใช้งานระบบระบบจัดการบริการระยะไกลผ่านเว็บ Centralize Server คือ เครื่องคอมพิวเตอร์หรือเครื่องให้บริการที่ทำการติดตั้งระบบจัดการบริการระยะไกลผ่านเว็บ ซึ่งทำหน้าที่เป็นตัวกลางในการรองรับคำสั่งจากผู้ดูแลระบบเพื่อใช้ในการบริหารจัดการเครื่องให้บริการระยะไกลที่อยู่ภายใต้การควบคุม รวมไปถึงทำหน้าที่สำรอง ไฟล์คอนฟิกูชัน และไฟล์ซิสเต็มเครื่องให้บริการดังกล่าวด้วย

Serviced Machines คือ เครื่องให้บริการระยะไกลที่อยู่ภายใต้การควบคุม ที่ผู้ดูแลระบบต้องการบริหารจัดการ

### - Use case description

Use Case: Create User Profile

**Brief Description:** ทำการสร้าง Username และ Password ของผู้ใช้

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องทำการ Login เข้าสู่ระบบและได้รับสิทธิ์การใช้งานเป็น Admin

**Basic Flows:**

1. ผู้ดูแลระบบเรียก Web page ขึ้นเพื่อทำการสร้างข้อมูลรายละเอียดเกี่ยวกับ Username และ Password ของผู้ที่จะมีสิทธิ์เข้าใช้ระบบ
2. ระบบตรวจสอบข้อมูลของผู้ใช้
3. ระบบบันทึกข้อมูลเข้าสู่ระบบ

**Alternative Flows:**

- 2a. กรอกข้อมูลไม่ครบ: ระบบแจ้งให้ Administrator กรอกข้อมูลให้ครบ และ ทำข้อ 1

**Postcondition:** -

Use Case: Create System Information

**Brief Description:** จัดการข้อมูลทุกอย่างของระบบในฐานะข้อมูล ทั้งเครื่องให้บริการ บริการที่ติดตั้งอยู่และไฟล์ configuration เป็นต้น

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องทำการ Login เข้าสู่ระบบและได้รับสิทธิ์การใช้งานเป็นผู้ดูแลระบบ

**Basic Flows:**

1. Administrator เรียก Web page ขึ้นเพื่อทำการจัดการข้อมูลในฐานะข้อมูลตามที่ผู้ดูแลระบบต้องการเช่น ข้อมูลของเครื่องให้บริการ ข้อมูลของแต่ละบริการ การเพิ่มบริการให้แก่เครื่องให้บริการ และการเพิ่มไฟล์คอนฟิกูเรชันให้แก่แต่ละบริการ เป็นต้น
2. ระบบตรวจสอบความถูกต้องของข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### 3. ระบบบันทึกข้อมูลเข้าสู่ระบบ

**Postcondition:** -

**Use Case:** Manage Configuration Files

**Brief Description:** จัดการ ไฟล์ Configuration ทั้งหมดที่เก็บไว้ที่ Centralize Server

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องทำการ Login เข้าสู่ระบบและได้รับสิทธิ์การใช้งานเป็นผู้ดูแลระบบ

**Basic Flows:**

1. ระบบแสดงไฟล์คอนฟิกูเรชันทั้งหมด
2. ผู้ดูแลระบบทำการเลือกฟังก์ชันการทำงานที่ต้องการ
3. ระบบแสดงผลการทำงานให้ผู้ดูแลระบบทราบ

**Alternative Flow:**

2a. สร้างไฟล์ใหม่:

- ผู้ดูแลระบบป้อนชื่อไฟล์ที่ต้องการสร้าง
- ระบบสร้างไฟล์ดังกล่าวขึ้นมาเพื่อให้ผู้ดูแลระบบทำการกำหนดค่าต่างๆตามความต้องการ
- ระบบทำการบันทึกไฟล์ดังกล่าว

2b แก้ไขไฟล์ที่มีอยู่แล้ว

- ผู้ดูแลระบบเลือกไฟล์ที่ต้องการ
- ระบบเปิดไฟล์ดังกล่าวขึ้นมาเพื่อให้ผู้ดูแลระบบทำการแก้ไขและกำหนดค่าต่างๆตามความต้องการ
- ระบบทำการบันทึกไฟล์ดังกล่าว

2c ลบไฟล์ที่ไม่ต้องการทิ้ง

- ผู้ดูแลระบบเลือกไฟล์ที่ต้องการ
- ระบบแจ้งเตือนให้ผู้ดูแลระบบทำการยืนยันการทำงาน
- ผู้ดูแลระบบทำการยืนยันการทำงาน
- ระบบทำการลบไฟล์ดังกล่าว

**Postcondition:** -

**Use Case:** Send Configuration File

**Brief Description:** ทำการส่ง ไฟล์ Configuration ไปยังเครื่องให้บริการที่อยู่ภายใต้การควบคุม

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องทำการ Login เข้าสู่ระบบและได้รับสิทธิ์การใช้งานเป็นผู้ดูแลระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

**Basic Flows:**

1. ผู้ดูแลระบบทำการเลือกเครื่องให้บริการที่ต้องการ
2. ระบบทำการติดต่อไปยังเครื่องให้บริการดังกล่าว
3. ระบบแสดง Service ทั้งหมดที่ติดตั้งบนเครื่องให้บริการนี้
4. ผู้ดูแลระบบทำการเลือก Service ที่ต้องการ
5. ระบบแสดงไฟล์ Configuration ทั้งหมดบริการนี้มีอยู่
6. ผู้ดูแลระบบทำการเลือกไฟล์ Configuration ที่ต้องการส่ง
7. ผู้ดูแลระบบกำหนดชื่อไฟล์ปลายทางและระบุตำแหน่งปลายทางที่ต้องการส่งไฟล์ดังกล่าวไป
8. ระบบทำการสร้างไฟล์ Shell Script เพื่อสั่งให้ Centralize Server ทำการส่งไฟล์ Configuration ไปยังเครื่องให้บริการปลายทางตามที่ผู้ดูแลระบบต้องการผ่านทาง SFTP
9. ระบบตรวจสอบไฟล์ปลายทางว่ามีการเปลี่ยนแปลงโดยผู้อื่นหรือไม่
10. ระบบสั่งให้ Centralize Server ทำการรันไฟล์ Shell Script ดังกล่าวที่ได้สร้างไว้

**Alternative Flow:**

- 2a. หากเครื่องให้บริการติดต่อไม่ได้ระบบจะแสดงข้อความเตือนแก่ผู้ดูแลระบบ
- 6a. ผู้ดูแลระบบสามารถตรวจสอบความถูกต้องและทำการแก้ไขไฟล์ที่เลือกไว้ ก่อนทำการส่งได้
- 9a. หากไฟล์ปลายทางมีการเปลี่ยนแปลงโดยผู้อื่น ระบบจะแจ้งทางเลือกแก่ผู้ดูแลระบบว่าต้องการจะส่งไฟล์ที่เลือกไว้ไปแทนที่ไฟล์เดิมหรือไม่

**Postcondition** ไฟล์ Configuration จะถูกส่งไปยังเครื่องให้บริการปลายทางตามที่กำหนดไว้

**Use Case:** Manage Serviced Machine

**Brief Description:** ผู้ดูแลระบบบริหารจัดการเครื่องให้บริการที่อยู่ภายใต้การควบคุม

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องทำการ Login เข้าสู่ระบบและได้รับสิทธิ์การใช้งานเป็น Admin

**Basic Flows:**

1. ผู้ดูแลระบบทำการเลือกเครื่องให้บริการที่ต้องการ
2. ระบบทำการติดต่อไปยังเครื่องให้บริการดังกล่าว
3. ผู้ดูแลระบบเลือกคำสั่งที่ต้องการจัดการเช่น การสั่ง Restart machine และ การสั่งเปิด ปิด หรือดูสถานะของแต่ละบริการที่เครื่องปลายทางให้บริการอยู่
4. ระบบส่งคำสั่งดังกล่าวไปยังเครื่องให้บริการที่อยู่ภายใต้การควบคุม
5. ระบบแสดงผลการทำงานให้ผู้ดูแลระบบทราบ

**Alternative Flow:**

- 2a. หากเครื่องให้บริการติดต่อไม่ได้ระบบจะแสดงข้อความเตือนแก่ผู้ดูแลระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น เมื่อนำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

**Postcondition:** คำสั่งจะถูกส่งไปยังเครื่องให้บริการปลายทางตามที่กำหนดไว้

**Use Case:** Backup File System

**Brief Description:** กำหนดเวลาในการ Backup หรือเวลาในการ Download อิมเมจของไฟล์ระบบ จาก Service ที่ต้องการ โดยอัตโนมัติ หรือทำการ Download โดยทันที

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องทำการ Login เข้าสู่ระบบและได้รับสิทธิ์การใช้งานเป็น Admin

**Basic Flows:**

1. ผู้ดูแลระบบทำการเลือกเครื่องให้บริการที่ต้องการ
2. ระบบทำการติดต่อไปยังเครื่องให้บริการดังกล่าว
3. ผู้ดูแลระบบกำหนดเวลาในการสั่งให้เครื่องให้บริการทำการสำรองไฟล์ระบบ
4. ระบบนำข้อมูลที่กำหนดมาทำการสร้าง shell script ที่มีคำสั่งในการให้เครื่องตัวกลางทำการสั่งให้เครื่องให้บริการทำการสำรองไฟล์ระบบของตัวเองด้วยคำสั่ง tar รวมถึงคำสั่งในการดาวน์โหลดอิมเมจของไฟล์ระบบที่ทำการสำรองแล้วมาเก็บไว้ที่เครื่องตัวกลางผ่านทาง SFTP
5. ระบบนำข้อมูลที่กำหนดมาทำการสร้างไฟล์ contrab ซึ่งใช้ในการกำหนดตารางเวลาสำหรับกระบวนการในการสั่งรันไฟล์ shell script ที่ได้สร้างไว้แล้ว
6. ระบบสั่งให้เครื่องตัวกลางทำการรันไฟล์ contrab ที่ได้สร้างขึ้น

**Alternative Flow:**

- 2a. หากเครื่องให้บริการติดต่อไม่ได้ระบบจะแสดงข้อความเตือนแก่ผู้ดูแลระบบ
- 3a. ผู้ดูแลระบบสามารถสั่งให้เครื่องให้บริการทำการสำรองไฟล์ระบบทันทีนอกเหนือจากการกำหนดเวลาไว้ล่วงหน้า โดยระบบจะสั่งรันไฟล์ shell script ทันทีโดยไม่ต้องรันไฟล์ crontab

**Postcondition:**

1. อิมเมจของไฟล์ระบบในแต่ละเครื่องให้บริการจะถูกดาวน์โหลดมาเก็บไว้ที่ Centralize Server เพื่อนำไปใช้ในการ Recovery ต่อไป

**Use Case:** Recovery File System

**Brief Description:** ระบบส่งอิมเมจของไฟล์ระบบ ไปยัง Service ที่ต้องการ

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องทำการ Login เข้าสู่ระบบและได้รับสิทธิ์การใช้งานเป็น Admin

**Basic Flows:**

1. ผู้ดูแลระบบทำการเลือกเครื่องให้บริการที่ต้องการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษานั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2. ระบบทำการติดต่อไปยังเครื่องให้บริการดังกล่าว
3. ผู้ดูแลระบบเลือกเวอร์ชันของอิมเมจไฟล์ระบบที่ต้องการ
4. ระบบทำการสร้างไฟล์ Shell Script เพื่อสั่งให้ Centralize Server ทำการส่งไฟล์อิมเมจที่ผู้ดูแลระบบเลือกไว้ไปเครื่องให้บริการปลายทางที่ผู้ดูแลระบบต้องการผ่านทาง SFTP
5. ระบบสั่งให้ทำการรันไฟล์ Shell Script ดังกล่าวที่ได้สร้างไว้
6. ระบบส่งคำสั่งให้เครื่องให้บริการทำการกู้คืนระบบโดยใช้อิมเมจของไฟล์ระบบที่ได้รับ โดยใช้คำสั่ง tar

**Alternative Flow:**

- 2a. หากเครื่องให้บริการติดต่อไม่ได้ระบบจะแสดงข้อความเตือนแก่ผู้ดูแลระบบ

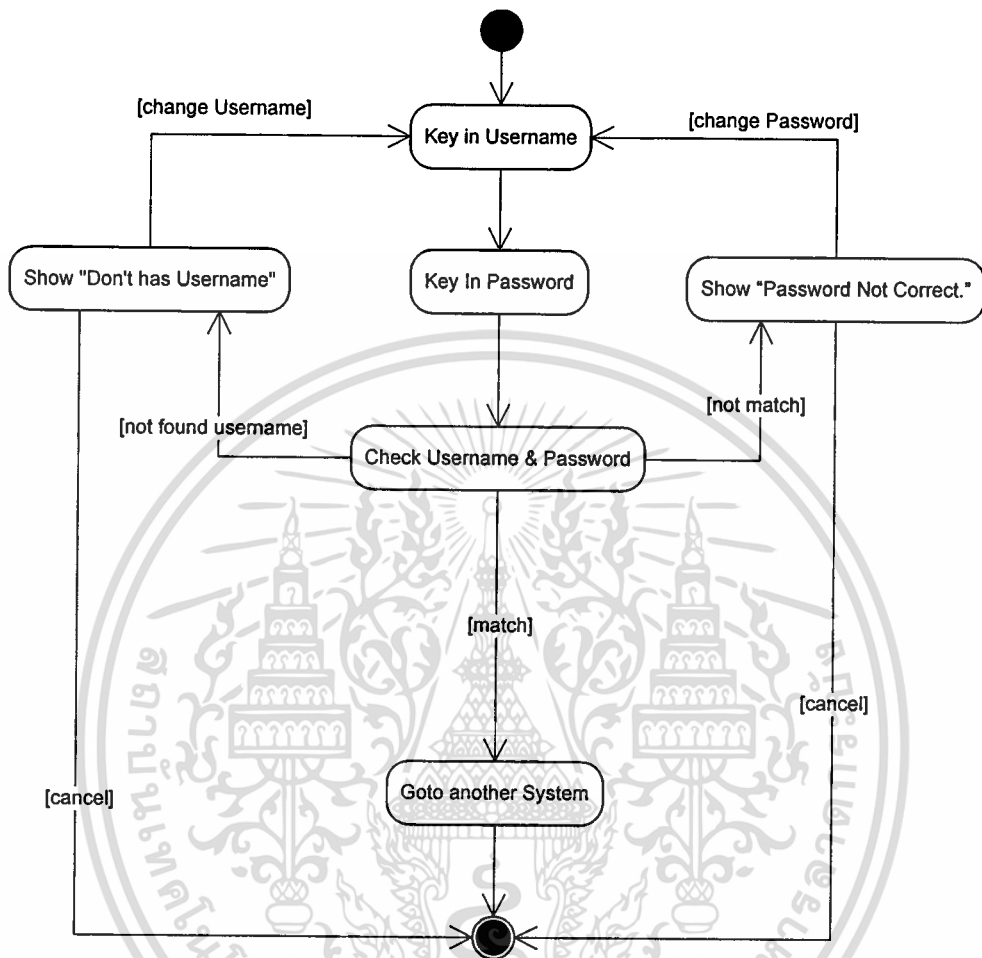
**Postcondition:**

1. อิมเมจของไฟล์ระบบจะถูกส่งไปยังเครื่องให้บริการที่อยู่ภายใต้การควบคุมตามที่กำหนดไว้



## - Activity Diagram

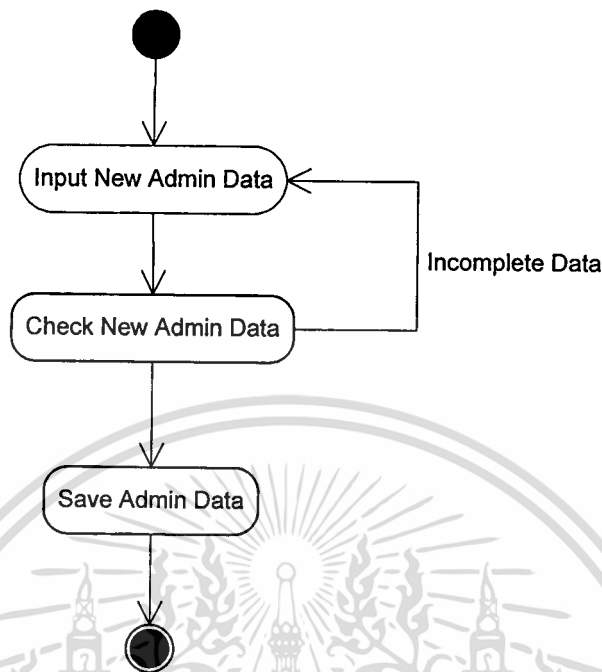
### 1. Login



รูปที่ 3.3 Activity Diagram ของยูสเคส Login

จากรูปที่ 3.3 ก่อนการใช้งานระบบผู้ใช้งานต้องทำการล็อกอินเข้าสู่ระบบก่อน โดยระบบจะทำการตรวจเช็คทั้งชื่อผู้ใช้และรหัสผ่านว่าถูกต้องหรือไม่ หากถูกต้องผู้ใช้งานจะได้รับสิทธิเป็นผู้ดูแลระบบ ซึ่งจะสามารถใช้งานระบบได้ต่อไป

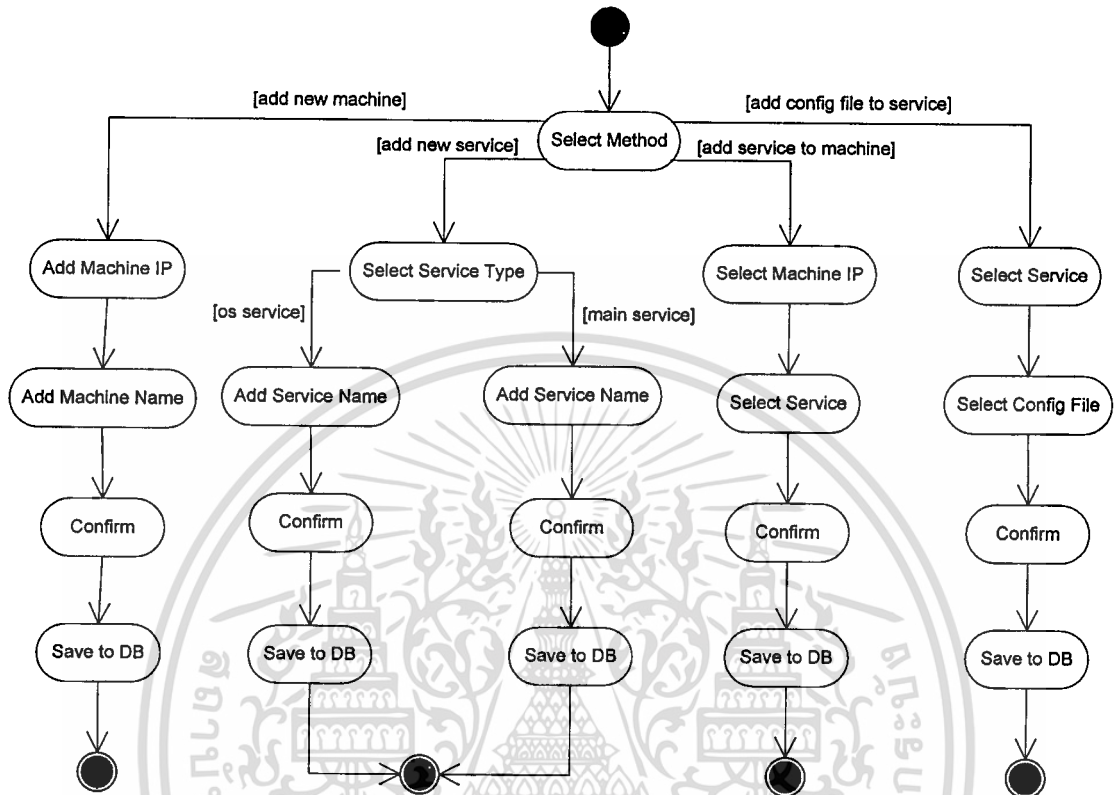
## 2. Create User Profile



รูปที่ 3.4 Activity Diagram ของยูสเคส Create User Profile

จากรูปที่ 3.4 แสดงขั้นตอนในการเพิ่มข้อมูลของผู้ที่มีสิทธิใช้งานระบบ โดยระบบจะตรวจสอบก่อนว่าชื่อผู้ใช้และรหัสผ่านว่าถูกต้องหรือไม่ หากถูกต้องผู้ใช้งานคนดังกล่าวจะมีสิทธิใช้งานระบบต่อไป

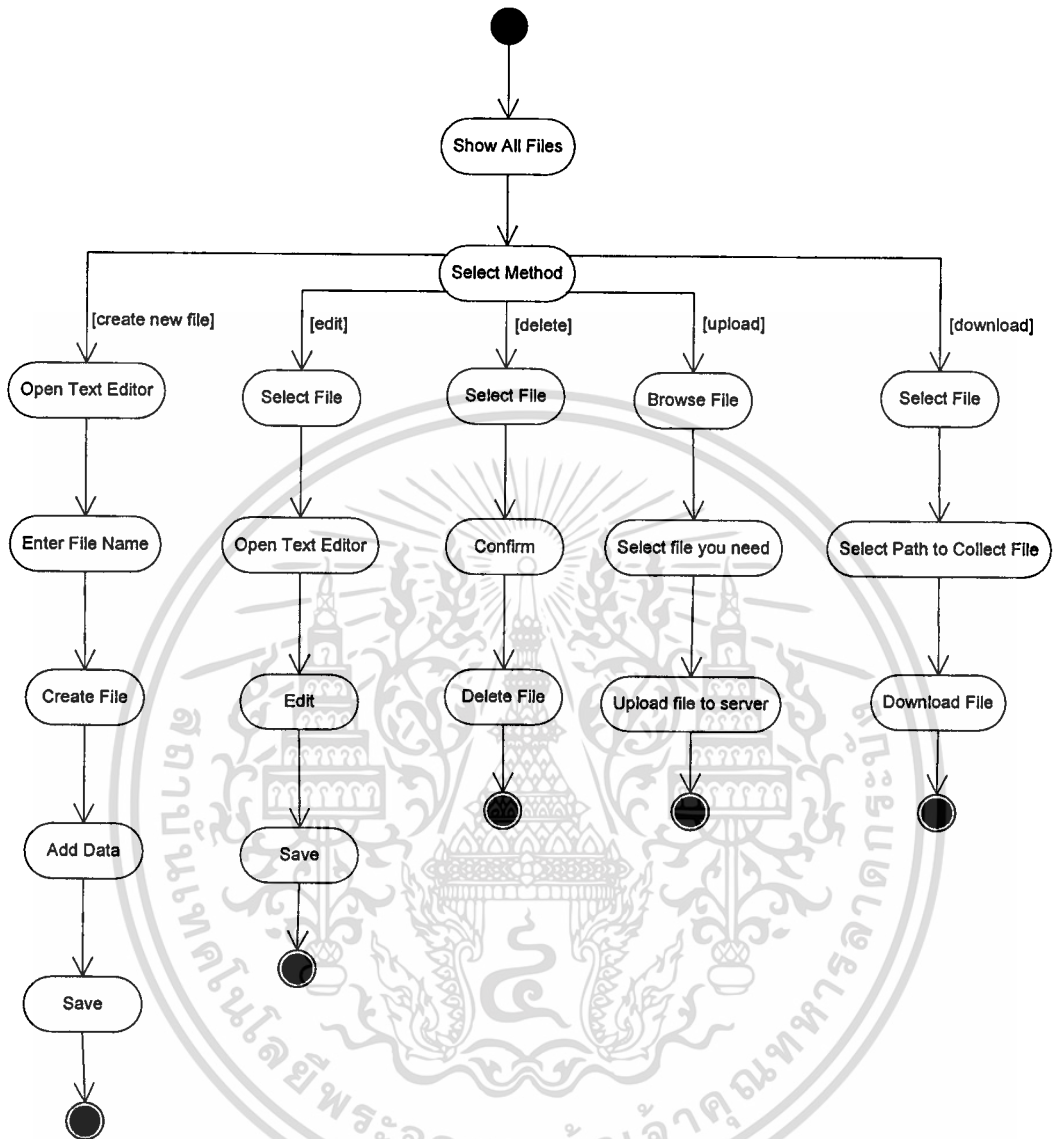
### 3. Create System Information



รูปที่ 3.5 Activity Diagram ของยูสเคส Create System Information

จากรูปที่ 3.5 ก่อนการใช้งานระบบในส่วนอื่นๆ ผู้ดูแลระบบต้องทำการเพิ่มข้อมูลต่างๆ เช่น ข้อมูลของเครื่องให้บริการปลายทาง ข้อมูลของแต่ละบริการที่ทำการติดตั้งลงในเครื่องให้บริการ และข้อมูลของไฟล์คอนฟิกูเรชันที่แต่ละบริการมี เป็นต้น โดยข้อมูลทั้งหมดจะถูกเก็บไว้ในฐานข้อมูล เพื่อให้ระบบนำข้อมูลดังกล่าวมาใช้ในฟังก์ชันอื่นๆต่อไป

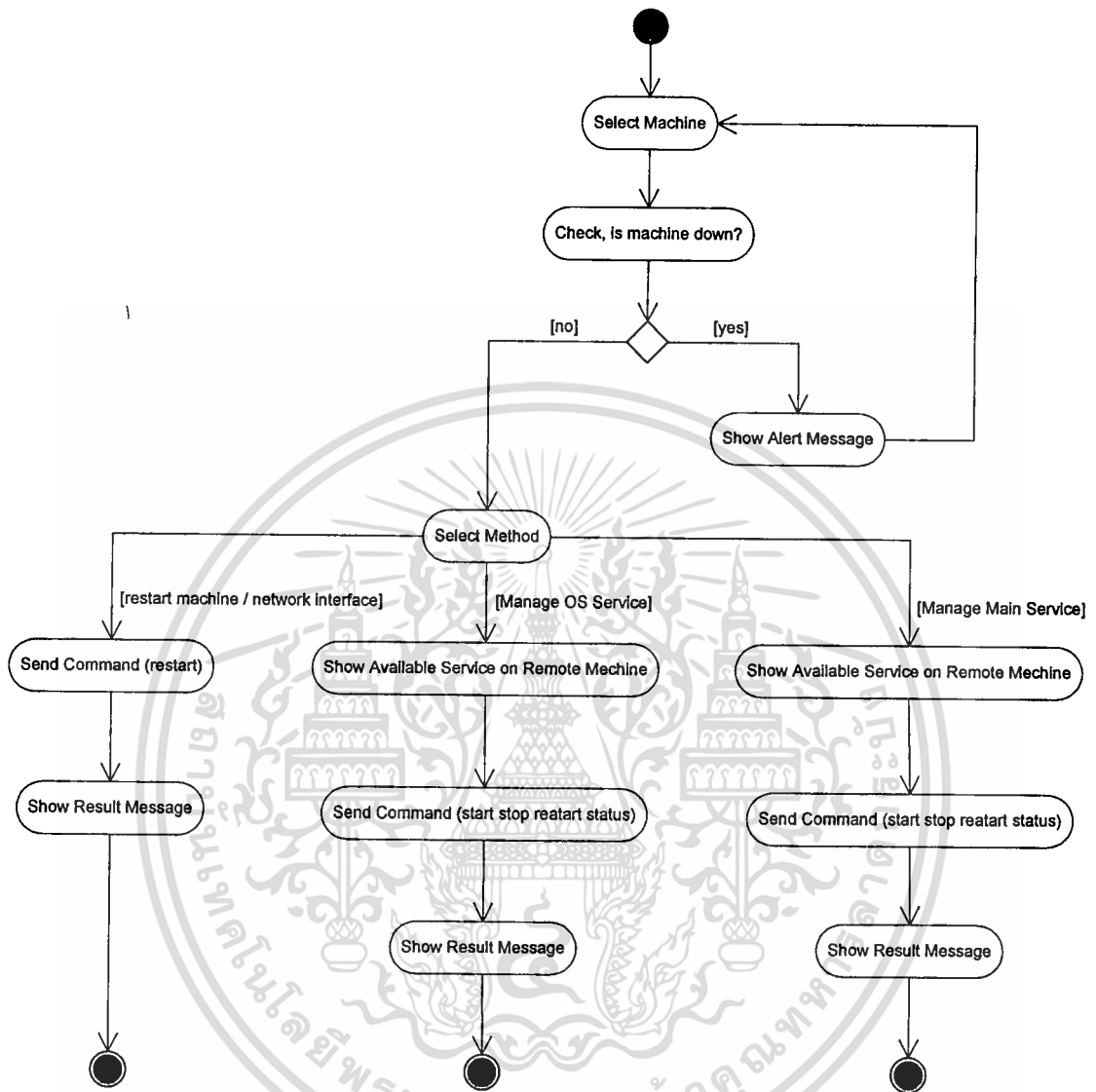
## 4. Manage Configuration Files



รูปที่ 3.6 Activity Diagram ของยูสเคส Manage Configuration Files

จากรูปที่ 3.6 ผู้ดูแลระบบสร้างไฟล์คอนฟิกูเรชันขึ้นมาแล้วทำการกำหนดค่าคอนฟิกูเรชันต่างๆ ที่เหมาะสมตามความต้องการบริการนั้นๆ โดยไฟล์ที่สร้างขึ้นจะถูกจัดเก็บไว้ในไดเรกทอรีที่ชื่อว่า config\_file ในเครื่องตัวกลาง (Centralize Server) โดยผู้ดูแลระบบสามารถจัดการไฟล์เหล่านี้ได้โดยตรงทั้งการลบทิ้ง เปิดไฟล์ขึ้นมาเพื่อแก้ไข ความผิดพลาดมาเก็บไว้ที่เครื่องส่วนตัว หรืออัปโหลดไฟล์อื่นๆจากเครื่องส่วนตัวไปยังเครื่องตัวกลางได้โดยไม่ต้องทำการสร้างใหม่

## 5. Manage Service Machine

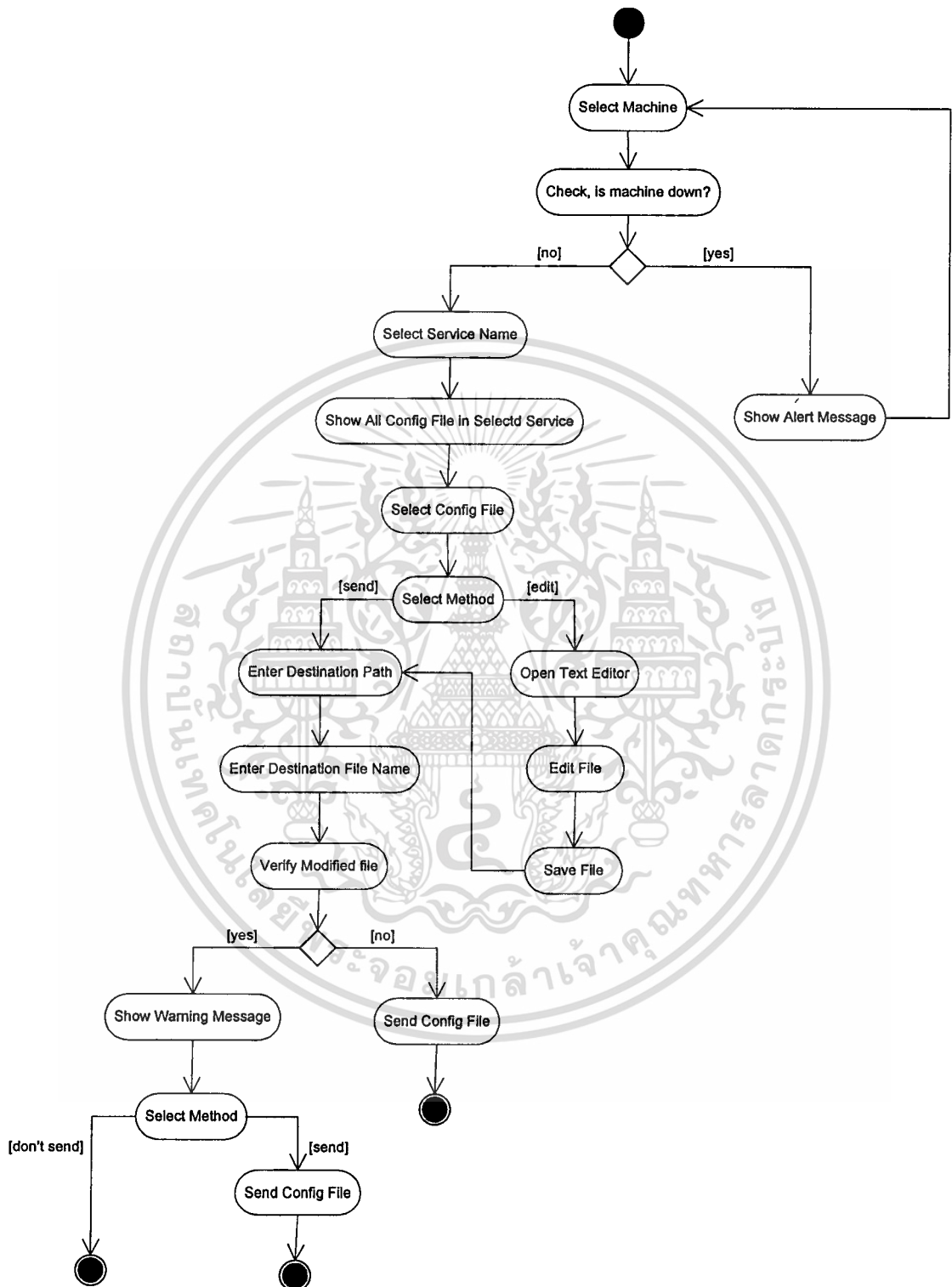


รูปที่ 3.7 Activity Diagram ของยูสเคส Manage Service Machine

จากรูปที่ 3.7 ก่อนที่ดำเนินใดๆระบบจะทำการตรวจสอบก่อนว่าเครื่องให้บริการปลายทางสามารถติดต่อได้หรือไม่ หากติดต่อได้ระบบจะดำเนินการต่อไป

ผู้ดูแลระบบสามารถทำการบริหารจัดการบริการต่างๆที่เครื่องให้บริการปลายทางมิได้ เช่น หยุดการทำงาน เริ่มการทำงานใหม่ หรือตรวจสอบสถานะการทำงานเป็นต้น โดยในการทำงานนั้นระบบจะนำหมายเลขไอพีของเครื่องให้บริการปลายทาง บริการที่ผู้ดูแลระบบเลือก และคำสั่งที่ผู้ดูแลระบบต้องการไปสร้างเป็นไฟล์ Shell Script และสั่งรันไฟล์ดังกล่าว เพื่อส่งคำสั่งที่ผู้ดูแลระบบต้องการไปยังเครื่องให้บริการปลายทางต่อไป

## 6. Send Configuration File



รูปที่ 3.8 Activity Diagram ของยูสเคส Send Configuration File

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 3.8 ก่อนที่ดำเนินการส่งไฟล์ ระบบจะทำการตรวจสอบก่อนว่าเครื่องให้บริการปลายทางสามารถติดต่อได้หรือไม่ หากติดต่อได้ระบบจะดำเนินการต่อไป

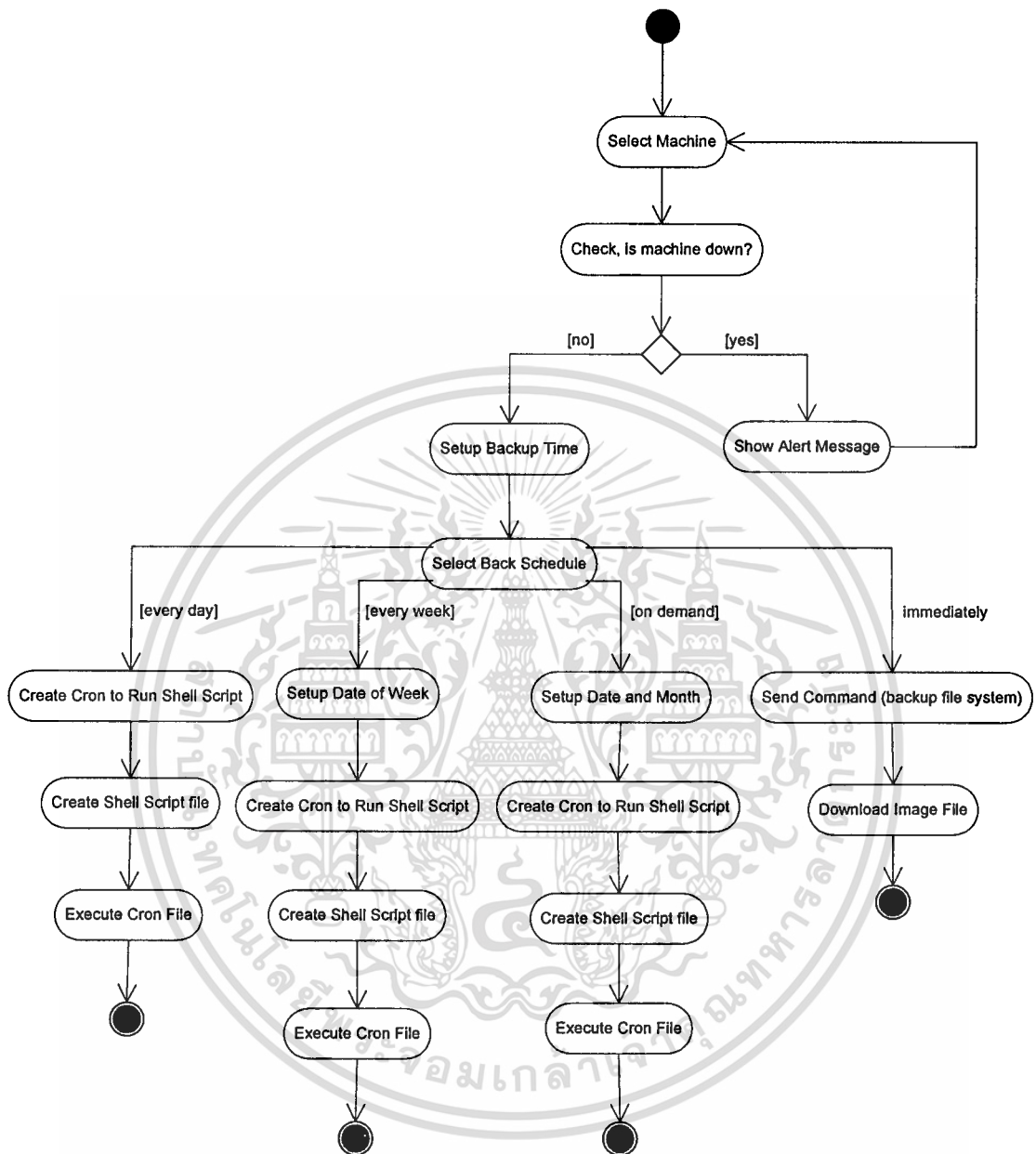
ผู้ดูแลระบบสามารถเลือกได้ว่าจะส่งไฟล์ที่เลือกไว้ทันทีหรือเปิดไฟล์ดังกล่าวขึ้นมาดูเพื่อตรวจสอบความถูกต้องหรือแก้ไขได้ ก่อนทำการส่ง

เพื่อความยืดหยุ่นในการใช้งานผู้ดูแลระบบสามารถกำหนดได้เองว่าจะทำการส่งไฟล์ที่เลือกไว้ไปยังตำแหน่งปลายทางที่ใด และสามารถกำหนดได้ว่าจะให้ไฟล์นี้มีชื่ออะไร

ก่อนจะทำการส่งไฟล์ระบบจะทำการตรวจสอบก่อนว่าชื่อไฟล์ที่จะส่งไปที่ปลายทางมีการเปลี่ยนแปลงจากบุคคลอื่นหรือไม่ ซึ่งขั้นตอนในการตรวจสอบจะเป็นดังนี้

- หลังจากการส่งไฟล์ทุกครั้งระบบจะทำการส่งคำสั่งไปยังเครื่องให้บริการปลายทางเพื่อทำการเก็บรายละเอียดของไฟล์ดังกล่าวเช่น ขนาด เวลาที่ทำการเปลี่ยนแปลง มาไว้ในไฟล์ lastmod เช่น squid.conf.lastmod เป็นต้น
- ซึ่งคำสั่งที่ใช้ในการเก็บรายละเอียดของเครื่องให้บริการปลายทางมีลักษณะดังต่อไปนี้  
ssh root@192.168.0.1 "ls -al /usr/local/etc/squid/squid.conf"
- ผลลัพธ์ที่เก็บไว้ในไฟล์ lastmod จะมีลักษณะดังนี้  
-rw-r--r-- 1 root wheel 121246 Oct 12 14:26 /usr/local/etc/squid/squid.conf
- ก่อนทำการส่งไฟล์ระบบจะทำการส่งคำสั่งไปยังเครื่องให้บริการปลายทางด้วยคำสั่งเดิมเพื่อทำการเก็บรายละเอียดของไฟล์ที่เลือกไว้ จากนั้นจึงนำมาเปรียบเทียบกับไฟล์ lastmod ที่เก็บไว้จากการส่งครั้งล่าสุด
- หากผลลัพธ์ที่ออกมาเหมือนกันแสดงว่าไฟล์ดังกล่าวไม่มีการเปลี่ยนแปลง ระบบจะทำการส่งไฟล์ไปยังเครื่องให้บริการปลายทาง
- หากผลลัพธ์ที่ออกมาไม่เหมือนกันแสดงว่าไฟล์ดังกล่าวถูกเปลี่ยนแปลงโดยบุคคลอื่น ระบบจะแจ้งเตือนให้ผู้ดูแลระบบทราบ เพื่อให้ผู้ดูแลระบบเลือกว่าจะส่งไฟล์ที่เลือกไว้ไปแทนที่ไฟล์เดิมหรือไม่

## 7. Backup File System



รูปที่ 3.9 Activity Diagram ของยูสเคส Backup File System

จากรูปที่ 3.9 ก่อนที่ดำเนินใ้ระบบจะทำการตรวจสอบก่อนว่าเครื่องให้บริการปลายทางสามารถติดต่อได้หรือไม่ หากติดต่อได้ระบบจะดำเนินการต่อไป

ผู้ดูแลระบบเลือกเครื่องให้บริการปลายทางที่ต้องการ และทำการกำหนดเวลาที่ต้องการให้เครื่องดังกล่าวสำรองไฟล์ระบบของตัวเองโดยมีขั้นตอนการทำงานดังนี้

1. ระบบจะนำหมายเลขไอพีของเครื่องให้บริการปลายทางไปสร้างเป็นไฟล์ Shell Script ซึ่งทำหน้าที่ยังนี้

- ตั้งให้เครื่องเครื่องให้บริการปลายทางสำรองไฟล์ระบบของตัวเองโดยใช้ คำสั่ง tar เมื่อการสำรองเสร็จสิ้นจะทำให้ได้อิมเมจไฟล์ระบบที่มีรูปแบบดังนี้ หมายเลขไอพี@วันที่ที่ทำการสำรองข้อมูล.tar.gz เช่น 192.168.0.1@16-09-07.tar.gz เป็นต้น
- เมื่อการสำรองข้อมูลเสร็จสิ้นระบบจะทำการดาวน์โหลดอิมเมจของไฟล์ระบบดังกล่าวมาเก็บไว้ที่เครื่องตัวกลาง
- ตัวอย่างของไฟล์ Shell Script ซึ่งในตัวอย่างชื่อไฟล์ 192.168.0.1.sh จะมีลักษณะดังนี้

```
ssh root@192.168.0.1 "rm /tmp/fs_backup/192.168.0.1"
```

```
ssh root@192.168.0.1 "tar -zcvf /tmp/fs_backup/192.168.0.1@12-10-2007.tar.gz /"
```

```
sftp root@192.168.0.1 << END_SCRIPT
```

```
cd /tmp/fs_backup/
```

```
get 192.168.0.1*
```

```
quit
```

```
END_SCRIPT
```

```
mv 192.168.0.1* /backup/fs_backup/
```

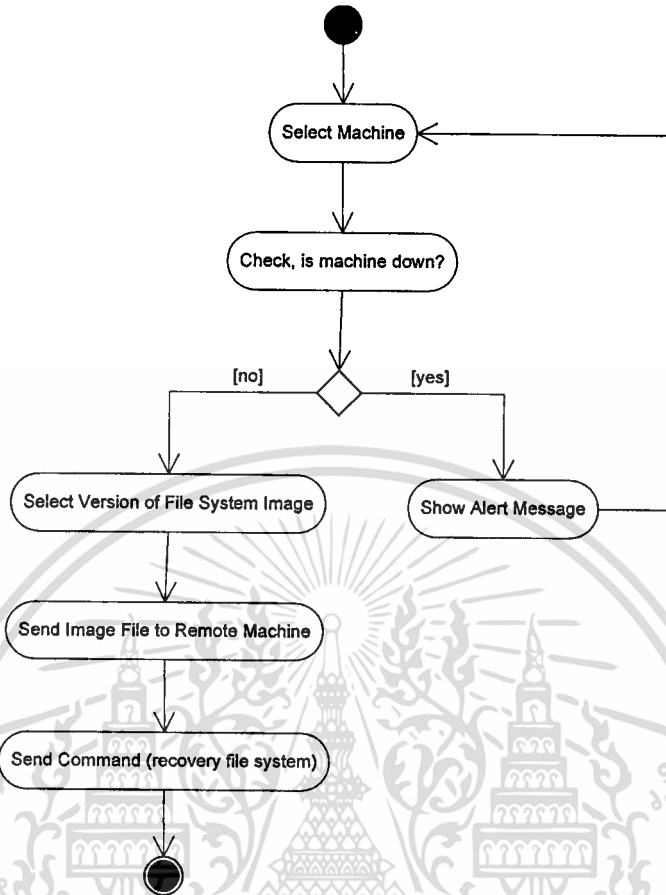
```
exit 0
```

2. ระบบจะนำเวลาที่ผู้ดูแลระบบกำหนดไว้สร้างเป็นไฟล์ crontab ที่ทำหน้าที่ในการตั้งเวลาในการรันไฟล์ Shell Script ที่สร้างไว้ล่วงหน้าตามตารางเวลาที่กำหนด ดังตัวอย่าง

```
30 23 * * * /usr/local/www/apache22/data/test/192.168.0.1.sh
```

3. หากผู้ดูแลระบบเลือกที่จะสั่งให้เครื่องให้บริการปลายทางทำการสำรองไฟล์ระบบทันที ระบบจะไม่ทำการสร้างไฟล์ crontab แต่จะทำการรันไฟล์ Shell Script ทันที

## 8. Recovery File System



รูปที่ 3.10 Activity Diagram ของยูสเคส Recovery File System

จากรูปที่ 3.10 ก่อนที่ดำเนินใคๆระบบจะทำการตรวจสอบก่อนว่าเครื่องให้บริการปลายทางสามารถติดต่อได้หรือไม่ หากติดต่อได้ระบบจะดำเนินการต่อไป

เมื่อผู้ดูแลระบบทำการเลือกเครื่องให้บริการปลายทางที่ต้องการและทำการระบบเลือกเวอร์ชันของอิมเมจไฟล์ระบบที่ต้องการแล้ว ระบบจะนำหมายเลขไอพีและอิมเมจไฟล์ระบบที่ผู้ดูแลระบบเลือกไปสร้างเป็นไฟล์ Shell Script ซึ่งมีการทำงานดังนี้

- ส่งคำสั่งให้เครื่องตัวกลาง (Centralize Server) ทำการส่งไฟล์อิมเมจที่ผู้ดูแลระบบเลือกไว้ไปยังเครื่องให้บริการปลายทางที่ผู้ดูแลระบบต้องการผ่านทาง SFTP
- ส่งคำสั่งให้เครื่องให้บริการทำการกู้คืนระบบจากอิมเมจของไฟล์ระบบที่ได้รับโดยใช้คำสั่ง tar ซึ่งไฟล์ Shell Script จะมีลักษณะดังนี้

```
scp 192.168.0.1@12-10-2007.tar.gz root@192.168.0.1:/tmp/fs_backup/192.168.0.1@12-10-2007.tar.gz
```

```
ssh root@192.168.0.1 "tar -xzvpf /tmp/fs_backup/192.168.0.1@12-10-2007.tar.gz -C /
```

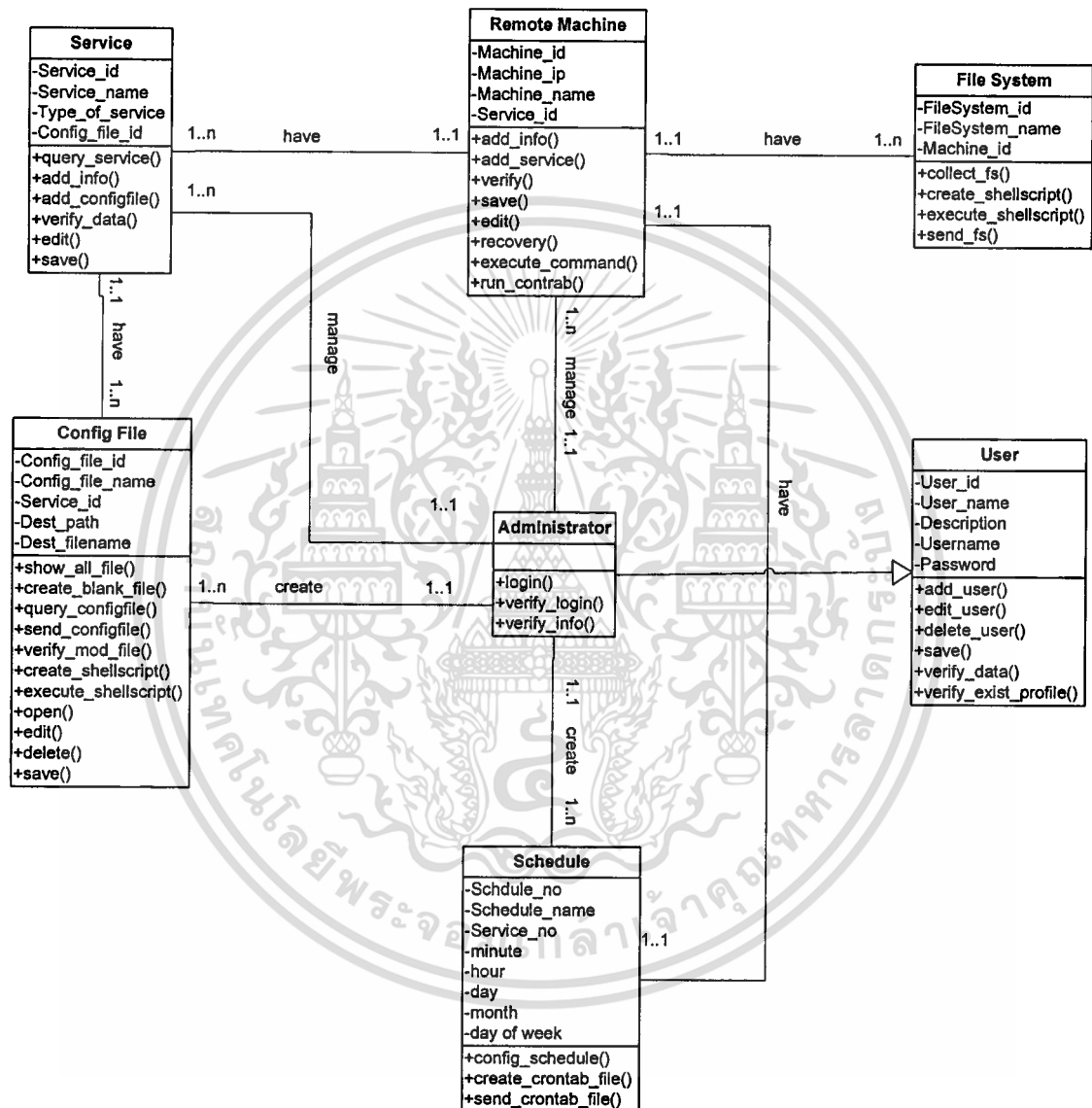
- จากนั้นระบบทำการรันไฟล์ Shell Script ดังกล่าวที่ได้สร้างไว้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### 3.3.2 Structural model

#### - Class diagram

เป็นการมองโครงสร้างข้อมูลของระบบ ซึ่งในที่นี้ใช้ Class Diagram เพื่อแสดงโครงสร้างข้อมูลของระบบ



รูปที่ 3.11 Class Diagram ของระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## Class diagram ของระบบนี้ประกอบด้วย 7 คลาสดังนี้

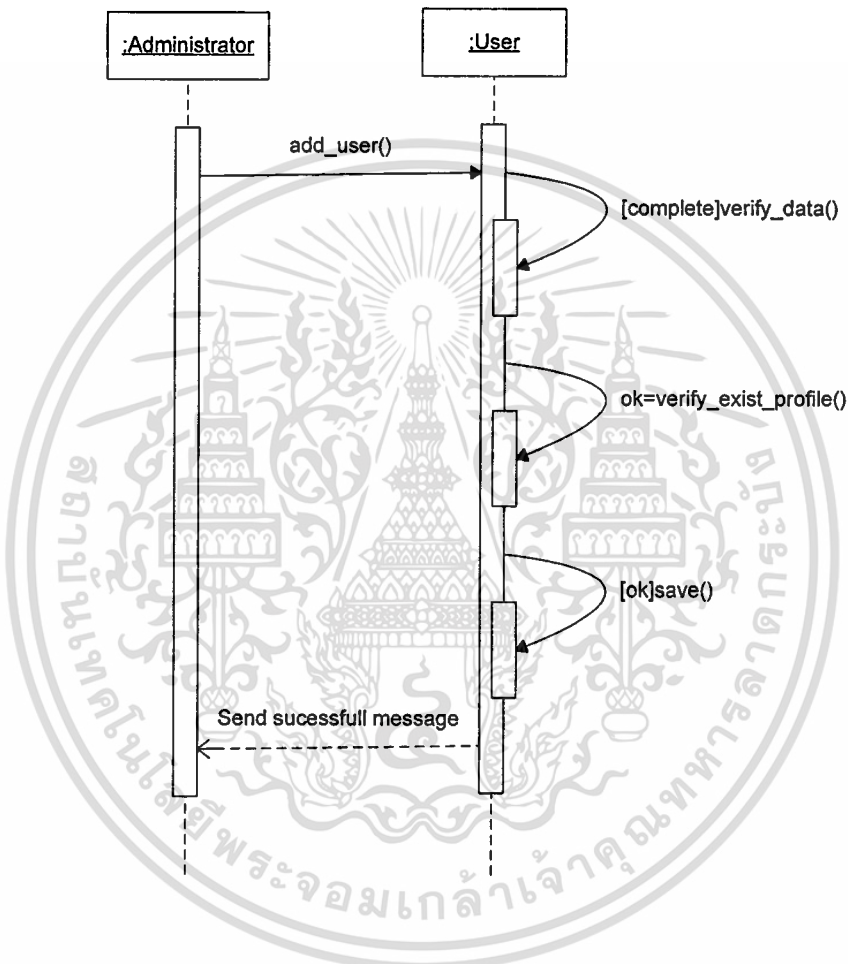
- **User** เป็นคลาสที่เก็บข้อมูลของผู้ใช้
- **Administrator** เมื่อมีการเพิ่มข้อมูลผู้ใช้งานในฐานข้อมูลแล้ว ผู้ใช้คนดังกล่าวจะมีสิทธิ์เป็นผู้ดูแลระบบซึ่งสามารถใช้งานระบบได้
- **Remote Machine** เป็นคลาสที่เก็บข้อมูลของเครื่องให้บริการที่อยู่ภายใต้การควบคุม
- **Service** เป็นคลาสที่เก็บข้อมูลของแต่ละบริการ
- **File System** เป็นคลาสที่เก็บอิมเมจของไฟล์ระบบของแต่ละบริการ
- **Config File** เป็นคลาสที่เก็บไฟล์ Configuration ของแต่ละบริการ
- **Schedule** เป็นคลาสที่สร้างตารางเวลาในการสำรอง (Backup) อิมเมจของไฟล์ระบบ

### ภาพรวมของระบบคือ

- Administrator มีความสัมพันธ์กับคลาส Service ซึ่ง Administrator หนึ่งคนจะสามารถจัดการ Service ได้หลาย Service ตามจำนวนของ Service (บริการ) ที่มี
- Administrator มีความสัมพันธ์กับคลาส Remote Machine ซึ่ง Administrator หนึ่งคนจะสามารถจัดการเครื่องให้บริการที่อยู่ภายใต้การควบคุม ได้หลายเครื่อง
- Administrator มีความสัมพันธ์กับคลาส Config File ซึ่ง Administrator หนึ่งคนจะสามารถสร้างไฟล์ Configuration ได้หลายไฟล์ตามจำนวนของบริการที่มี
- Administrator มีความสัมพันธ์กับคลาส Schedule ซึ่ง Administrator หนึ่งคนจะสามารถกำหนดตารางเวลาในการสำรอง (Backup) อิมเมจของไฟล์ระบบได้หลายตารางตามจำนวนของเครื่องให้บริการที่อยู่ภายใต้การควบคุม
- โดยที่ Service แต่ละ Service สามารถมี ไฟล์ Configuration ได้มากกว่าหนึ่งไฟล์ตามความต้องการของบริการนั้นๆ
- โดยที่เครื่องให้บริการแต่ละเครื่องสามารถมีอิมเมจของไฟล์ระบบได้มากกว่าหนึ่งไฟล์ (หลายเวอร์ชัน)
- เครื่องให้บริการแต่ละเครื่องจะสามารถกำหนดตารางเวลาในการสำรอง (Backup) อิมเมจของไฟล์ระบบได้เพียงหนึ่งตารางเท่านั้น

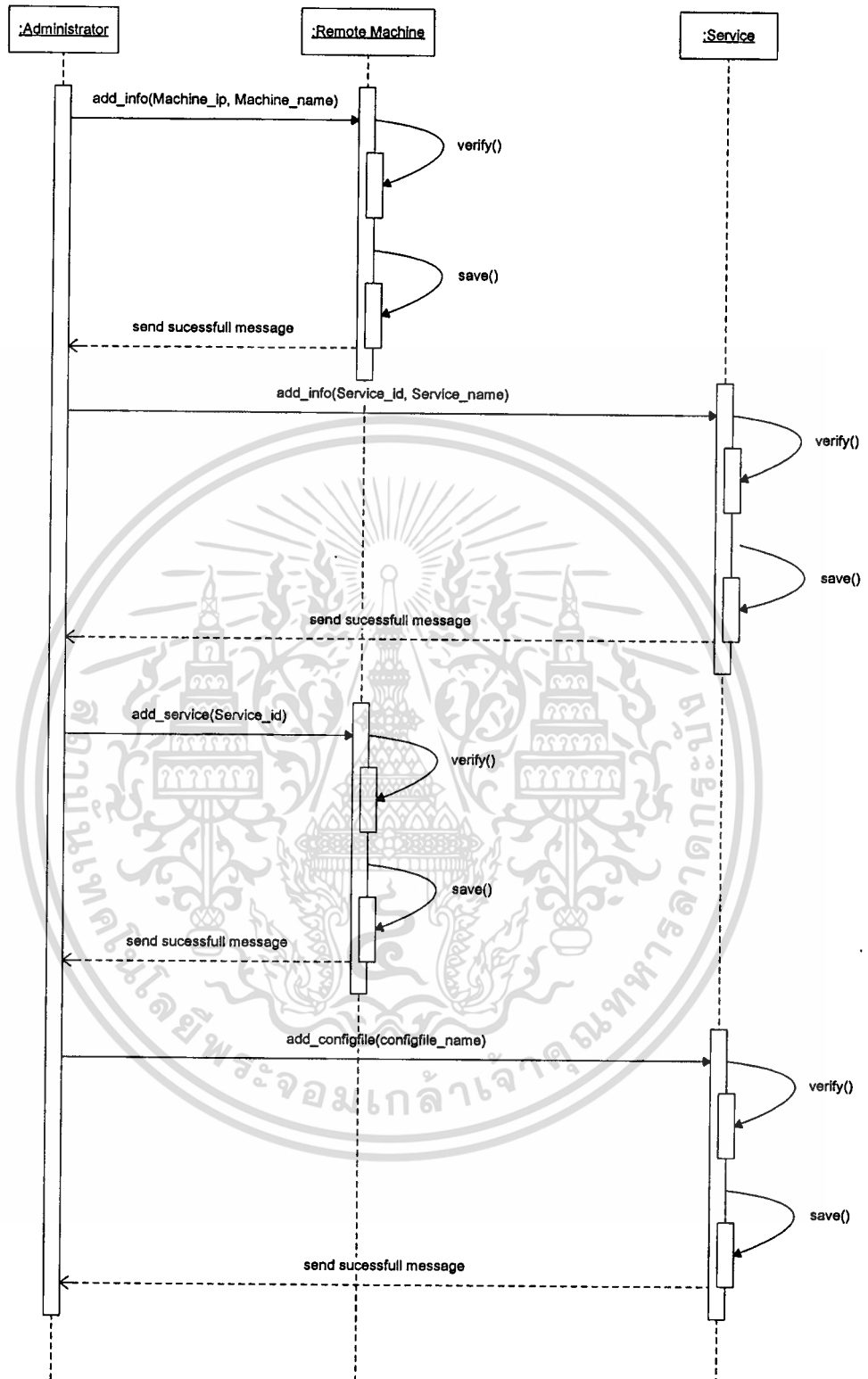
### 3.3.3 Behavioral Model

เป็นการมองกระบวนการของระบบหรือกลไกของระบบ โดยมองในลักษณะพฤติกรรมของระบบว่าระบบทำงานอย่างไร ซึ่งในที่นี้ใช้ Sequence Diagram เพื่ออธิบายกลไกของระบบในลักษณะพฤติกรรมของระบบ



รูปที่ 3.12 Sequence Diagram ของยูสเคส Create User Profile

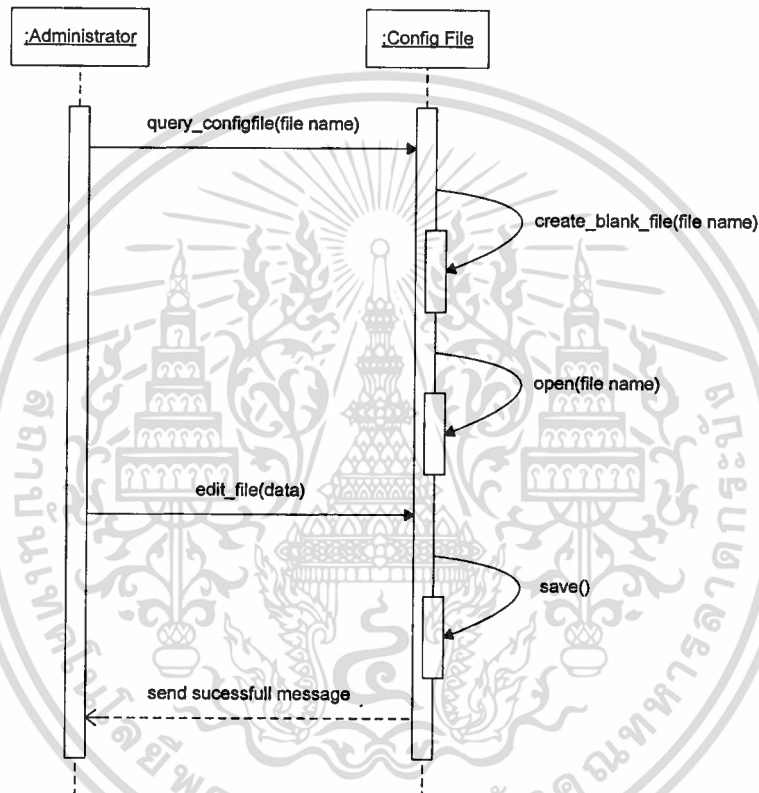
จากรูปที่ 3.12 เป็นการแสดงการทำงานของ การ Create User Profile โดยเมื่อมีการป้อนข้อมูลของผู้ใช้คนใหม่เข้าไประบบจะทำการตรวจสอบข้อมูลว่าครบถ้วนสมบูรณ์หรือไม่ หากสมบูรณ์แล้วก็จะตรวจสอบต่อไปว่า มีข้อมูลของผู้ใช้คนนี้หรือยัง ถ้ายังไม่มีก็จะทำการบันทึก และแสดงข้อความยืนยันให้ผู้ใช้และระบบทราบ



รูปที่ 3.13 Sequence Diagram ของยูสเคส Create System Information

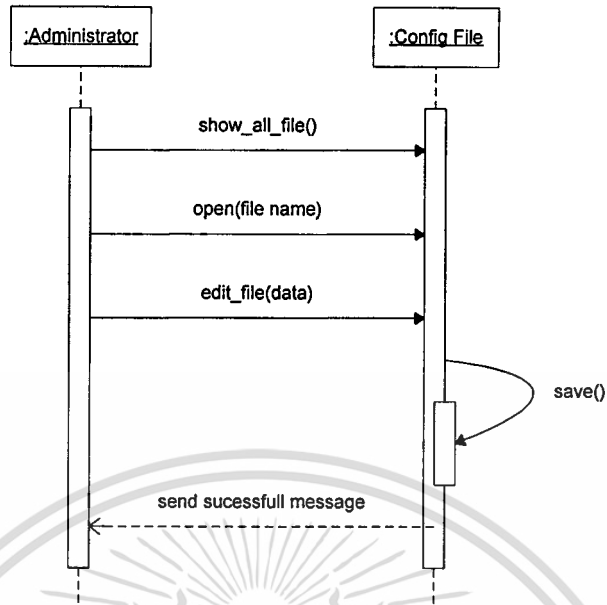
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 3.13 เป็นการแสดงการทำงานของการทำงานของการเพิ่มข้อมูลทุกอย่างของระบบลงในฐานข้อมูล โดยผู้ดูแลระบบจะต้องทำการป้อนข้อมูลของเครื่องให้บริการปลายทาง และข้อมูลของบริการทั้งหมดก่อน จากนั้นจึงทำการกำหนดว่าเครื่องให้บริการแต่ละเครื่องมีบริการอะไรบ้าง และแต่ละบริการมีไฟล์คอนฟิกูเรชันที่ไฟล์ ไฟล์อะไรบ้าง ตามลำดับ ซึ่งข้อมูลเหล่านี้จะถูกนำไปใช้ในฟังก์ชันอื่นๆของระบบต่อไป โดยเมื่อผู้ดูแลระบบป้อนข้อมูลเสร็จแล้ว ระบบจะตรวจสอบความถูกต้อง หากไม่มีข้อผิดพลาดก็จะทำการบันทึกข้อมูล และแจ้งผลการทำงานให้ผู้ดูแลระบบทราบ



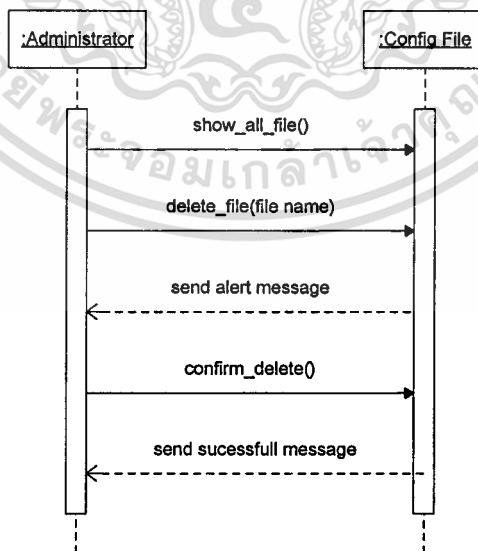
รูปที่ 3.14 Sequence Diagram ของการสร้างไฟล์คอนฟิกูเรชันขึ้นมาใหม่

จากรูปที่ 3.14 แสดงการทำงานของ การสร้างไฟล์คอนฟิกูเรชันขึ้นมาใหม่โดยเมื่อผู้ดูแลระบบทำการเลือกฟังก์ชันการทำงานนี้ ระบบจะทำการสร้างไฟล์เปล่าขึ้นมาตามชื่อไฟล์ที่กำหนด เพื่อให้ผู้ดูแลระบบทำการกำหนดค่า configuration ต่างๆตามความต้องการของบริการที่ผู้ดูแลระบบกำหนด



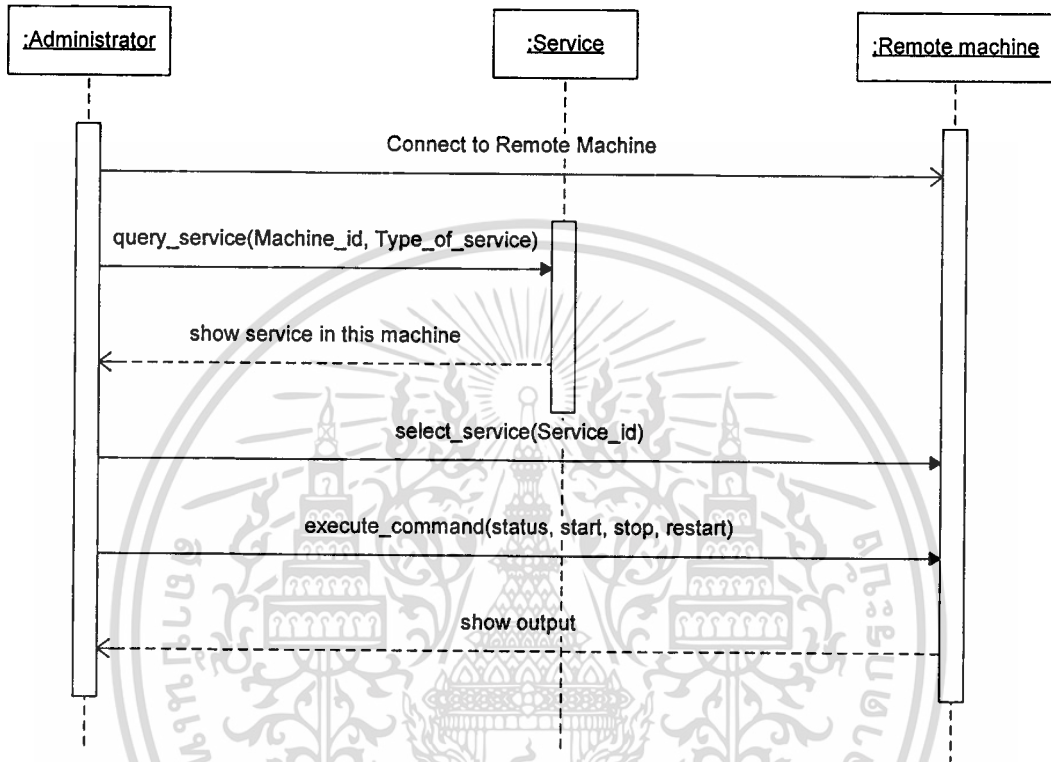
รูปที่ 3.15 Sequence Diagram ของการแก้ไขไฟล์คอนฟิกูเรชันที่มีอยู่แล้ว

จากรูปที่ 3.15 แสดงการทำงานของ การแก้ไขไฟล์คอนฟิกูเรชันที่มีอยู่แล้ว โดยเมื่อผู้ดูแลระบบทำการเลือกฟังก์ชันการทำงานนี้ ระบบจะทำการเปิดไฟล์มาตามชื่อไฟล์ที่ผู้ดูแลระบบเลือก เพื่อให้ผู้ดูแลระบบทำการกำหนดและแก้ไขค่า configuration ต่างๆตามที่ต้องการ เมื่อแก้ไขเสร็จแล้วระบบจะทำการบันทึกไฟล์ดังกล่าวและแจ้งผลการทำงานให้ผู้ดูแลระบบทราบ



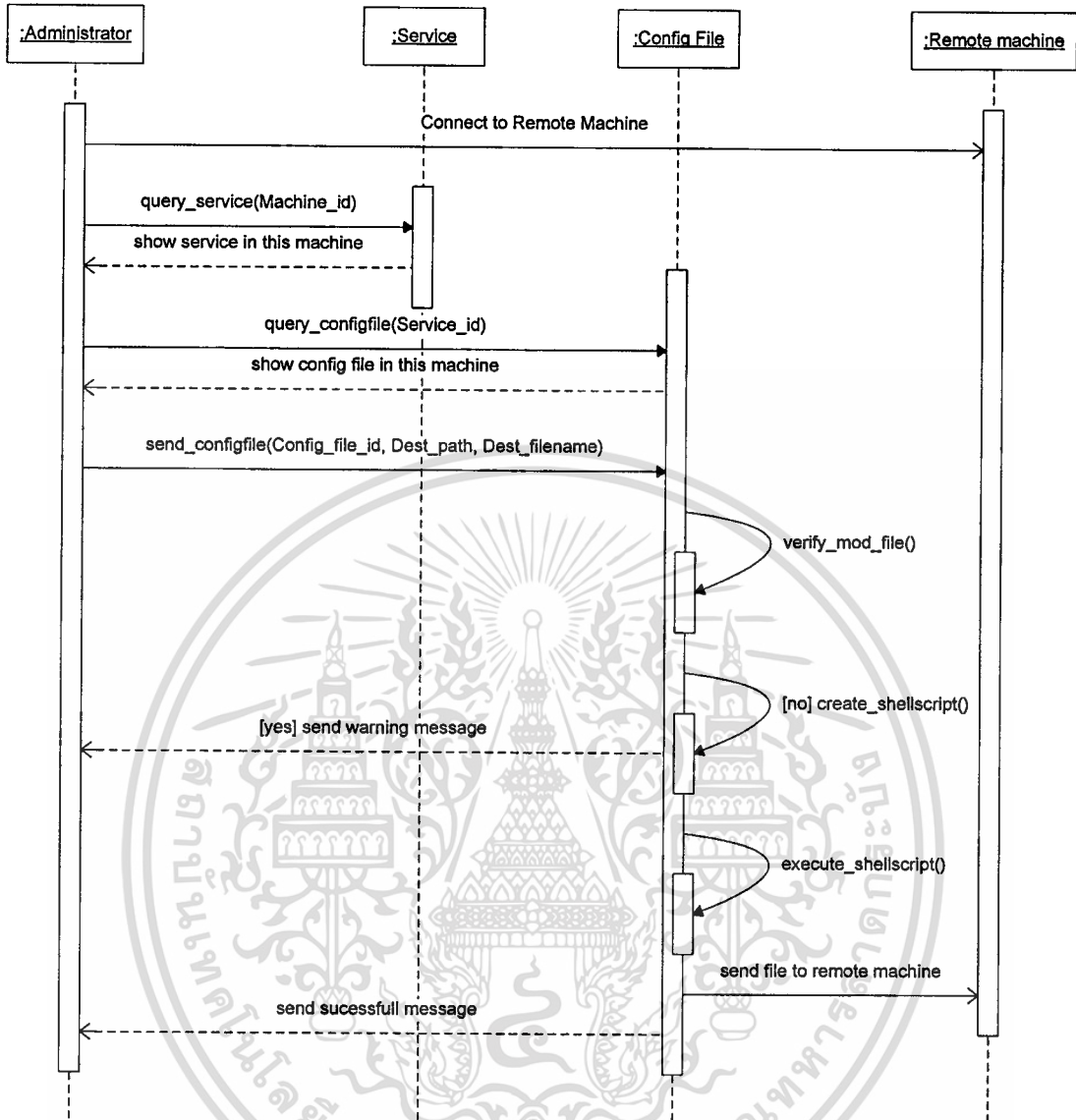
รูปที่ 3.16 Sequence Diagram ของการลบไฟล์คอนฟิกูเรชันที่มีอยู่แล้ว

จากรูปที่ 3.16 แสดงการทำงานของ การลบไฟล์คอนฟิกูเรชันที่มีอยู่แล้ว โดยเมื่อผู้ดูแลระบบทำการเลือกไฟล์ที่ต้องการจะลบ ระบบจะทำการแจ้งเตือนเพื่อให้ผู้ดูแลระบบทำการยืนยัน เมื่อผู้ดูแลระบบทำการยืนยันแล้วระบบจะทำการลบไฟล์ดังกล่าวและแจ้งผลการทำงานให้ผู้ดูแลระบบทราบ



รูปที่ 3.17 Sequence Diagram ของยูสเคส Manage Serviced Machine

จากรูปที่ 3.17 แสดงการทำงานของยูสเคส Manage Serviced Machine โดยผู้ดูแลระบบต้องทำการเลือกเครื่องให้บริการที่ต้องการก่อน จากนั้นระบบจะทำการติดต่อไปยังเครื่องให้บริการดังกล่าว หากติดต่อได้ ระบบจะแสดงบริการทั้งหมดที่เครื่องให้บริการดังกล่าวมีเพื่อให้ผู้ดูแลระบบทำการเลือก เมื่อผู้ดูแลระบบเลือกได้แล้วจึงทำการกำหนดคำสั่งที่ต้องการเช่นคำสั่ง Restart เครื่องที่ให้บริการ คำสั่งเปิด ปิด หรือดูสถานะการทำงานของบริการที่เครื่องดังกล่าวให้บริการอยู่เป็นต้น ระบบจะทำการส่งคำสั่งดังกล่าวไปยังเครื่องให้บริการที่ผู้ดูแลระบบกำหนดไว้ จากนั้นระบบจะแจ้งผลการทำงานให้กับผู้ดูแลระบบทราบ

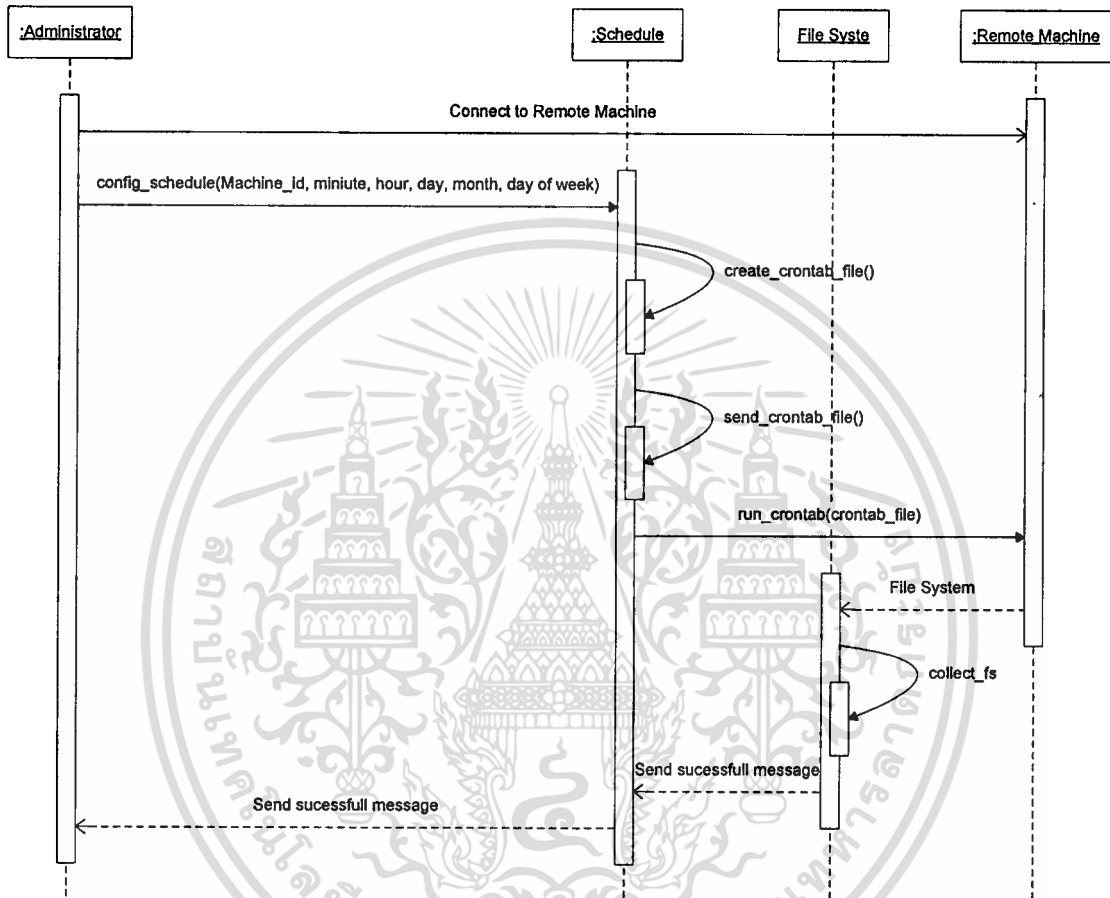


รูปที่ 3.18 Sequence Diagram ของยูสเคส Send Configuration File

จากรูปที่ 3.18 แสดงการทำงานของยูสเคส Send Configuration File โดยผู้ดูแลระบบต้องทำการเลือกเครื่องให้บริการที่ต้องการก่อน จากนั้นระบบจะทำการติดต่อไปยังเครื่องให้บริการดังกล่าว หากติดต่อได้ ระบบจะแสดงบริการทั้งหมดที่เครื่องให้บริการดังกล่าวมีเพื่อให้ผู้ดูแลระบบทำการเลือก

เมื่อผู้ดูแลระบบเลือกได้แล้ว ระบบจะแสดงไฟล์คอนฟิกูเรชันทั้งหมดที่บริการดังกล่าวมี เพื่อให้ผู้ดูแลระบบทำการเลือกอีกครั้ง เมื่อเลือกได้แล้ว ผู้ดูแลระบบต้องทำการกำหนดชื่อไฟล์ปลายทางและ ระบุตำแหน่งปลายทางที่ต้องการส่งไฟล์ดังกล่าวไปเพื่อความชัดเจนในการทำงาน

ก่อนส่งไฟล์ดังกล่าวระบบจะตรวจสอบก่อนว่าไฟล์ดังกล่าวถูกเปลี่ยนแปลงจากผู้อื่นหรือเปล่า หากไม่มีการเปลี่ยนแปลง ระบบจะทำการส่งไฟล์ดังกล่าวและแจ้งผลการทำงานให้กับผู้ดูแลระบบทราบ แต่หากไฟล์ดังกล่าวเกิดถูกเปลี่ยนแปลงโดยผู้อื่นระบบจะแจ้งเตือนให้ผู้ดูแลระบบทราบและให้ผู้ดูแลระบบเลือกว่าจะส่งไฟล์นี้ไปแทนที่ไฟล์เดิมหรือไม่

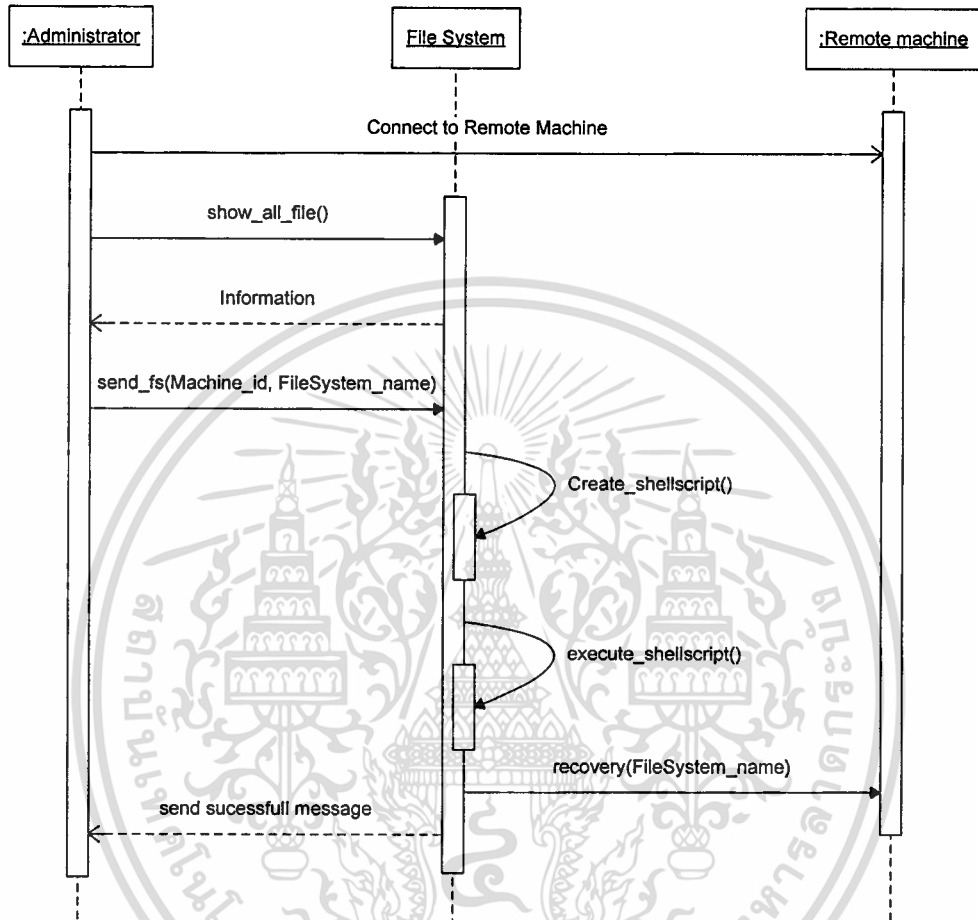


รูปที่ 3.19 Sequence Diagram ของยูทิลิตี้ Backup File System

จากรูปที่ 3.19 แสดงการทำงานของยูทิลิตี้ Backup File System โดยผู้ดูแลระบบต้องทำการเลือกเครื่องให้บริการที่ต้องการก่อน จากนั้นระบบจะทำการติดต่อไปยังเครื่องให้บริการดังกล่าว หากติดต่อได้ ระบบจึงจะทำงานต่อไป

ผู้ดูแลระบบทำการกำหนดช่วงเวลาที่ต้องการให้เครื่องให้บริการทำการสำรองไฟล์ระบบให้อยู่ในรูปแบบของอิมเมจไฟล์ ระบบจะนำข้อมูลดังกล่าวไปสร้างเป็นไฟล์ crontab จากนั้นระบบจะทำการส่งไฟล์ crontab ดังกล่าวไปยังเครื่องให้บริการปลายทาง พร้อมทั้งส่งคำสั่งให้เครื่องให้บริการทำการสั่งให้ไฟล์ crontab ทำงานด้วย

เมื่อเครื่องให้บริการปลายทางสำรองไฟล์ระบบเสร็จสิ้นแล้ว ระบบจะทำการดาวน์โหลดไฟล์อิมเมจที่สำรองไว้ มาเก็บที่เครื่องตัวกลาง เมื่อการทำงานเสร็จสิ้นแล้วระบบจะแจ้งผลการทำงานให้กับผู้ดูแลระบบทราบ



รูปที่ 3.20 Sequence Diagram ของยูสเคส Recovery File System

จากรูปที่ 3.20 แสดงการทำงานของยูสเคส Recovery File System โดยผู้ดูแลระบบต้องทำการเลือกเครื่องให้บริการที่ต้องการก่อน จากนั้นระบบจะทำการติดต่อไปยังเครื่องให้บริการดังกล่าว หากติดต่อได้ ระบบจึงจะทำงานต่อไป

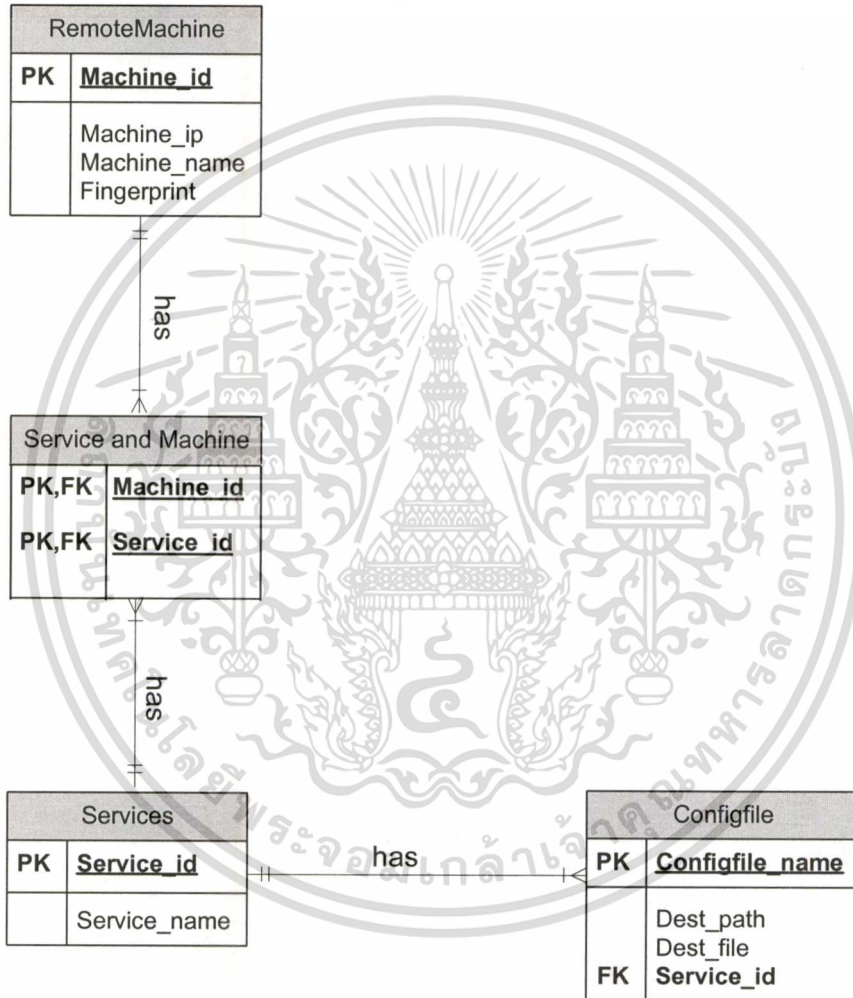
จากนั้นผู้ดูแลระบบจึงเลือกอิมเมจของไฟล์ระบบที่ต้องการ ระบบจะนำข้อมูลดังกล่าวไปสร้างเป็นไฟล์ Shell Script และทำการส่งรันเพื่อให้ Centralize Server ทำการส่งอิมเมจของไฟล์ระบบไปยังเครื่องให้บริการปลายทาง พร้อมด้วยคำสั่งให้เครื่องให้บริการปลายทางใช้ไฟล์นี้ในการกู้คืนระบบ เมื่อการทำงานเสร็จสมบูรณ์แล้วระบบจะแจ้งผลการทำงานให้กับผู้ดูแลระบบทราบ

# บทที่ 4

## การออกแบบระบบ

### 4.1 การออกแบบฐานข้อมูล

#### 4.1.1 Entity Relationship Diagram



รูปที่ 4.1 Entity Relationship Diagram

จากรูปที่ 4.1 ระบบจัดการบริการผ่านเว็บ จัดเก็บข้อมูลจำนวน 4 ตารางในฐานข้อมูลคือ

1. **RemoteMachine** ทำหน้าที่จัดเก็บข้อมูลของเครื่องให้บริการปลายทาง
2. **Services** ทำหน้าที่จัดเก็บบริการทั้งหมดที่ผู้ดูแลระบบเพิ่มเข้าไปในระบบ
3. **Services and Machines** เป็น Bridge Entity ซึ่งใช้ในการแปลงความสัมพันธ์จาก เมนนี่ทูเมนนี่ (M:N) ให้กลายเป็นวันทูเมนนี่ (1:M) ซึ่งจากการออกแบบจะพบว่า เครื่อง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ให้บริการ 1 เครื่องสามารถติดตั้งบริการได้หลายบริการ และแต่ละบริการก็สามารถที่ ถูกติดตั้งในเครื่องให้บริการได้หลายเครื่องเช่นกัน ดังนั้นจะตาราง RemoteMachine จึง มีความสัมพันธ์กับตาราง Services แบบเมเนนี่ทูเมเนนี่ (M:N) แต่โครงสร้างของ ฐานข้อมูลเชิงสัมพันธ์ไม่รองรับความสัมพันธ์แบบนี้ ดังนั้นจึงต้องทำการแปลงก่อน โดยใช้ Bridge Entity เข้ามาช่วย

4. **Configfile** ทำหน้าที่จัดเก็บข้อมูลของแต่ละบริการว่ามีไฟล์คอนฟิกูเรชันที่ไฟล์ ไฟล์ อะไรบ้าง

#### 4.1.2 Data Dictionary

อธิบายรายละเอียดและ โครงสร้างของแต่ละตาราง ดังแสดงในตารางที่ 4.1 – ตารางที่ 4.6

ตารางที่ 4.1 Data Dictionary ของตาราง Remote Machine

ชื่อเขตข้อมูล	ชนิดข้อมูล	ขนาด	คำอธิบาย	Key
Machine_id	integer	4	รหัสของเครื่องให้บริการปลายทาง	PK
Machine_ip	varchar	24	หมายเลขไอพีเครื่องให้บริการ ปลายทาง	
Machine_name	varchar	24	ชื่อของเครื่องให้บริการปลายทาง	
Fingerprint	text	1024	Fingerprint ของเครื่องให้บริการ ปลายทาง	

ตารางที่ 4.2 Data Dictionary ของตาราง Services

ชื่อเขตข้อมูล	ชนิดข้อมูล	ขนาด	คำอธิบาย	Key
Service_id	integer	4	รหัสของของบริการ	PK
Service_name	varchar	24	ชื่อของบริการ	

ตารางที่ 4.3 Data Dictionary ของตาราง Services\_and\_Machines

ชื่อเขตข้อมูล	ชนิดข้อมูล	ขนาด	คำอธิบาย	Key
Machine_id	integer	4	รหัสของเครื่องให้บริการปลายทาง	PK,FK
Service_id	integer	4	รหัสของของบริการที่ติดตั้งบน เครื่องให้บริการนั้นๆ	PK,FK

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.4 Data Dictionary ของตาราง Configfile

ชื่อเขตข้อมูล	ชนิดข้อมูล	ขนาด	คำอธิบาย	Key
ConfigFile_name	varchar	24	ชื่อของไฟล์คอนฟิกูเรชัน	PK
Dest_path	varchar	32	ตำแหน่งปลายทางของไฟล์	
Dest_file	varchar	32	ชื่อของไฟล์ปลายทาง	
Service_id	integer	4	รหัสของของบริการ	FK

## 4.2 โครงสร้างของไฟล์ข้อมูล

อธิบายโครงสร้างของไฟล์ต่างๆที่ใช้ในการจัดเก็บข้อมูลที่จำเป็นในการทำงานของระบบ

### 4.2.1 ไฟล์ backup.cron

เป็นไฟล์ที่ใช้จัดเก็บตารางเวลาในการสั่งให้เครื่องให้บริการปลายทางทำการสำรองไฟล์ระบบของตัวเอง ตามเวลาที่ผู้ดูแลระบบกำหนด มีโครงสร้างดังนี้

minute	hour	day	month	day of week	command
--------	------	-----	-------	-------------	---------

- **minute** มีค่า 0 - 59 เวลาเป็นนาที จะสั่งให้คำสั่งที่กำหนดทำงานทันทีเมื่อถึงนาทีที่กำหนด
- **hour** มีค่า 0 - 23 เวลาเป็นชั่วโมง จะสั่งให้คำสั่งที่กำหนดทำงานทันทีเมื่อถึงชั่วโมงที่กำหนด
- **day** มีค่า 1 - 31 เวลาเป็นวัน จะสั่งให้คำสั่งที่กำหนดทำงานทันทีเมื่อถึงวันที่กำหนด
- **month** มีค่า 1 - 12 เวลาเป็นเดือน จะสั่งให้คำสั่งที่กำหนดทำงานทันทีเมื่อถึงเดือนที่กำหนด
- **day of week** มีค่า 0 - 6 โดยที่วันของแต่ละสัปดาห์ มีค่าดังนี้ (อาทิตย์ = 0, จันทร์ = 1, อังคาร = 2, พุธ = 3, พฤหัสบดี = 4, ศุกร์ = 5 ,เสาร์ = 6 )
- **command** คือคำสั่งหรือไฟล์สคริปต์ที่ต้องการให้ทำงาน  
โดยไฟล์ backup.cron จะมีตัวอย่างดังนี้

```
30 23 * * * /usr/local/www/apache22/data/test/192.168.0.1.sh
```

### 4.2.2 ไฟล์ .lastmod

เป็นไฟล์ที่ใช้จัดเก็บการเปลี่ยนแปลงล่าสุดของไฟล์คอนฟิกูเรชันที่ส่งไปยังเครื่องให้บริการปลายทาง มีโครงสร้างดังนี้

Permission	Owner	Group	Size	Date-Time	File name
------------	-------	-------	------	-----------	-----------

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- **Permission** คือ ชนิดและสิทธิของไฟล์
  - **Owner** คือ เจ้าของไฟล์
  - **Group** คือ กลุ่มของเจ้าของไฟล์
  - **Size** คือ ขนาดของไฟล์
  - **Date-Time** คือ วัน-เวลาล่าสุดที่ทำการแก้ไขไฟล์
  - **File name** คือ ชื่อไฟล์และไคเรกทอรีที่เก็บไฟล์
- โดยไฟล์ .lastmod ซึ่งในตัวอย่างคือไฟล์ squid.conf.lastmod จะมีลักษณะดังนี้
- ```
-rw-r--r-- 1 root wheel 121246 Oct 12 14:26 /usr/local/etc/squid/squid.conf
```

#### 4.2.3 ไฟล์ user.conf

เป็นไฟล์ที่ใช้จัดเก็บชื่อผู้ใช้และรหัสผ่านของผู้ดูแลระบบ มีโครงสร้างดังนี้

User name: Password

- **User name** คือ ชื่อผู้ใช้งาน
  - **Password** คือ รหัสผ่าน
- โดยไฟล์ user.conf จะมีลักษณะดังนี้ **admin01:biaoNrb1w1YSc**

## บทที่ 5

### การพัฒนาระบบ

ในการพัฒนาโปรแกรมระบบจัดการบริการระยะไกลผ่านเว็บ ได้มีการกำหนดแผนการพัฒนา ดังนี้

#### 5.1 การวางแผนปฏิบัติงาน

ได้เลือกใช้ระบบปฏิบัติการและซอฟต์แวร์ดังต่อไปนี้

##### 1. ระบบปฏิบัติการเลือกใช้ FreeBSD 6.0

เป็นระบบปฏิบัติการแบบยูนิกซ์ที่ได้รับความนิยมอย่างแพร่หลาย และไม่ต้องเสียค่าใช้จ่าย โดยระบบปฏิบัติการ FreeBSD นั้นเป็นระบบปฏิบัติการที่มีความปลอดภัยสูงกว่าระบบยูนิกซ์แบบ Open Source ทั่วไป

##### 2. เว็บเซิร์ฟเวอร์ที่รองรับการทำงานของ PHP และ MySQL เลือกใช้ Apache เวอร์ชัน 2.2

Apache เป็นซอฟต์แวร์สำหรับให้บริการเว็บเซิร์ฟเวอร์ (HTTP/Web Server) ผ่านทางโปรโตคอล HTTP โดยเป็นซอฟต์แวร์แบบ Open Source สามารถนำมาใช้งานได้โดยไม่มีค่าใช้จ่าย

##### 3. ซอฟต์แวร์ภาษา เลือกใช้ PHP เวอร์ชัน 5

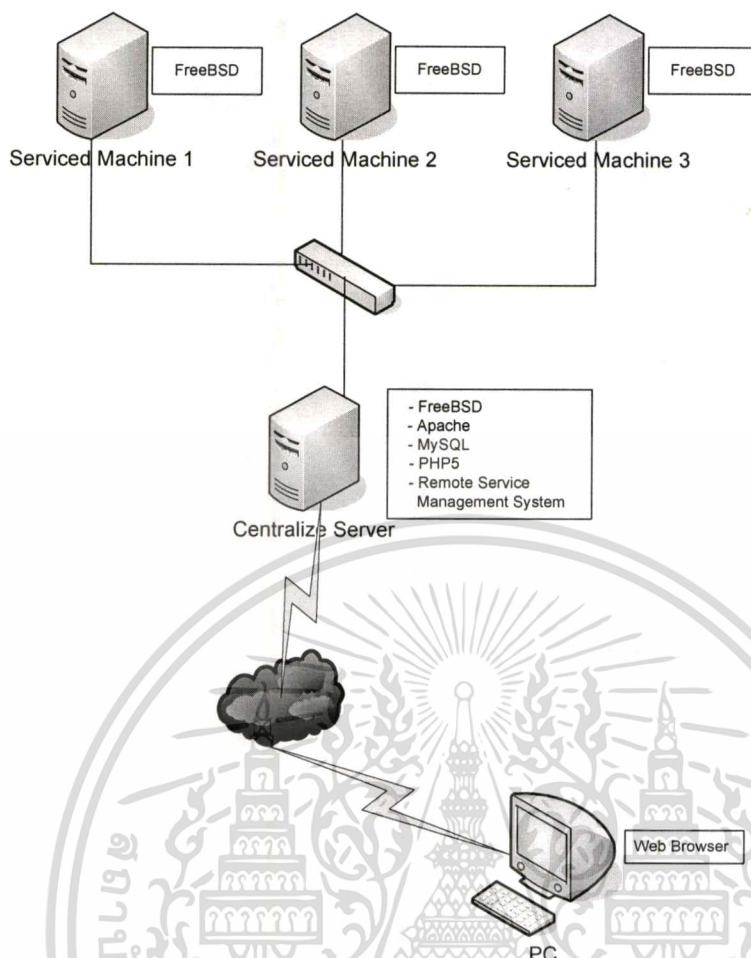
PHP Extension เป็น scripting language ที่ทำงานร่วมกับ HTML โดยสามารถเขียนแทรกเข้าไปใน HTML โดย PHP เป็น Open Source ที่สามารถใช้ได้กับหลายๆระบบปฏิบัติการไม่ว่าจะเป็น windows, UNIX, Linux และยังสามารถรองรับการติดต่อกับฐานข้อมูลได้หลายชนิด

##### 4. ซอฟต์แวร์ระบบฐานข้อมูล เลือกใช้ MySQL เวอร์ชัน 5

MySQL เป็นโปรแกรมฐานข้อมูลที่นิยมใช้กันอย่างแพร่หลาย และมีประสิทธิภาพสามารถนำมาใช้ทดแทน โปรแกรมฐานข้อมูลที่มีจำหน่ายในเชิงพาณิชย์ได้

#### 5.2 การวางแผนโครงสร้างของระบบ

โครงสร้างของระบบจัดการบริการระยะไกลผ่านเว็บจะแสดงดังรูปที่ 4.1



รูปที่ 5.1 โครงสร้างของระบบจัดการบริการระยะไกลผ่านเว็บ

จากรูปที่ 5.1 ระบบจัดการบริการระยะไกลผ่านเว็บจะถูกติดตั้งบน Centralize Server ซึ่งพัฒนาโดยใช้ภาษา PHP ในการทำงานของระบบนั้น ผู้ใช้งานจะทำการกำหนดค่า configuration ต่างๆในแต่ละบริการของเครื่องให้บริการแต่ละเครื่องที่ต้องการ ดังแสดงในรูปคือ Serviced Machine1, 2 และ 3 ตามลำดับ ผ่านทาง Web Browser ซึ่งจะเป็นการทำงานในลักษณะของ Text Editor โดยใช้ความรู้ความสามารถของผู้ดูแลระบบในการกำหนดค่า configuration เอง ทั้งนี้เพื่อความยืดหยุ่นและครอบคลุมทุกๆบริการ โดยไฟล์ configuration ที่สร้างเสร็จแล้วจะถูกเก็บไว้ที่ Centralize Server เพื่อรอรับคำสั่งจากผู้ดูแลระบบสำหรับส่งไฟล์ดังกล่าวไปยังเครื่องให้บริการต่างๆที่อยู่ภายใต้การควบคุมต่อไป

ระบบสามารถกำหนดให้เครื่องให้บริการทำการ Backup ไฟล์ระบบทั้งหมดให้อยู่ในรูปแบบของไฟล์อิมเมจได้อัตโนมัติ โดยการใช การทำงานของ crontab มาช่วยซึ่งผู้ใช้สามารถกำหนดเวลาได้ผ่านทาง Web Browser

ในกรณีที่เครื่องให้บริการใดๆเสียหายหรือไม่สามารถใช้งานได้ ระบบสามารถทำการกู้คืนระบบได้โดยทำการส่งอิมเมจของไฟล์ระบบของเครื่องบริการเดิมจาก Centralize Server ให้แก่เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เครื่องสำรองที่นำมาใช้งานแทน และเมื่อเครื่องที่ให้บริการเดิมได้ทำการซ่อมแซมแก้ไขจนสามารถใช้งานได้ตามปกติแล้ว ระบบจะสามารถกู้คืน (Recovery) ข้อมูลไฟล์ระบบทั้งหมดให้เครื่องให้บริการเดิมได้ตามกลไกเดิม ซึ่งการทำงานทั้งหมดผู้ดูแลระบบจะเรียกใช้งานผ่านทาง Web Browser เช่นกัน

ผู้ดูแลระบบสามารถบริหารจัดการเครื่องให้บริการต่างๆที่อยู่ภายใต้การควบคุมเช่นการเปิดปิด หรือเรียกดูสถานะการทำงานของบริการนั้นๆได้ ผ่านทาง Web Browser โดยในการทำงานนั้น Centralize Server จะส่งคำสั่งต่างๆ (command) ไปยังเครื่องให้บริการที่อยู่ภายใต้การควบคุม ผ่านทาง SSH (Secure Shell) ซึ่งเป็นช่องทางที่มีความปลอดภัยสูง

### 5.3 การปรับแต่งระบบเบื้องต้น

ก่อนการใช้งานระบบนั้นเครื่องตัวกลาง (Centralize Server) และเครื่องให้บริการปลายทาง (Serviced Machine) จะต้องมีการปรับแต่งระบบเบื้องต้นดังนี้

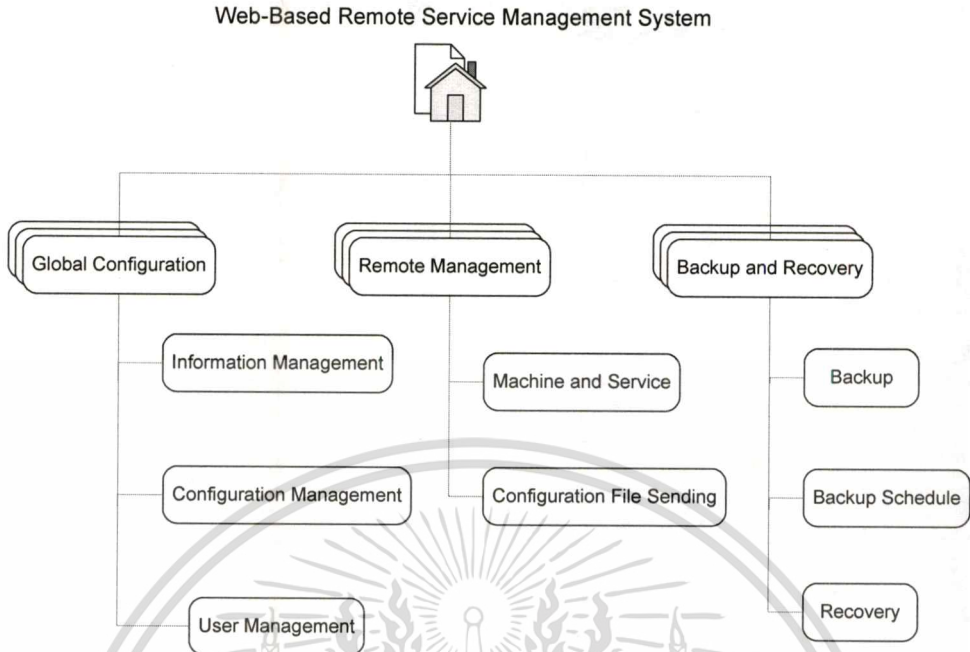
1. เครื่องตัวกลาง (Centralize Server)
  - เปิดการใช้งาน SSH (Secure Shell) โดยการเพิ่มคำสั่ง `sshd_enable="YES"` ในไฟล์ `/etc/rc.conf`
  - สร้างกุญแจคู่ขึ้นมาโดยใช้คำสั่ง `ssh-keygen -t rsa` โดยกุญแจจะถูกสร้างขึ้น 2 กุญแจคือ `id_rsa` และ `id_rsa.pub` ซึ่งจะถูกเก็บไว้ที่ `/root/.ssh/`
  - เปิดการใช้งาน Crontab โดยการเพิ่มคำสั่ง `cron_enable="YES"` ในไฟล์ `/etc/rc.conf`
2. เครื่องให้บริการปลายทาง (Serviced Machine)
  - เปิดการใช้งาน SSH (Secure Shell) โดยการเพิ่มคำสั่ง `sshd_enable="YES"` ในไฟล์ `/etc/rc.conf`
  - เนื่องจากบางคำสั่งซึ่งเป็นคำสั่งระดับโอเปอเรชัน เช่นคำสั่งเริ่มการทำงานของเครื่องใหม่ (restart) ผู้ใช้งานทั่วไปไม่สามารถสั่งการได้ นอกจาก root เท่านั้น ดังนั้นเพื่อให้เครื่องตัวกลางสามารถควบคุมเครื่องให้บริการปลายทางได้ เครื่องให้บริการจึงจำเป็นต้องอนุญาตให้ เครื่องตัวกลางสามารถเข้าถึงยูสเซอร์ root ได้ผ่านทาง Secure Shell โดยการเพิ่มคำสั่ง `PermitRootLogin yes` ในไฟล์ `/etc/ssh/sshd_config`
  - นำกุญแจสาธารณะซึ่งในที่นี้คือ `id_rsa.pub` ของเครื่องตัวกลาง มาเพิ่มลงในไฟล์ `/root/.ssh/authorized_keys` เพื่อให้เครื่องตัวกลาง สามารถติดต่อเข้ามาได้

## 5.4 การพัฒนาระบบจัดการบริการระยะไกลผ่านเว็บ

การพัฒนาระบบจัดการบริการระยะไกลผ่านเว็บพัฒนาโดยโปรแกรมภาษา PHP โดยระบบจะมีฟังก์ชันการทำงานดังนี้

1. สามารถป้อนข้อมูลที่จำเป็นสำหรับการกำหนดค่า Configuration ต่างๆสำหรับแต่ละบริการ (Service) ในเครื่องให้บริการได้
2. สามารถเพิ่ม ลบ หรือ แก้ไขไฟล์ Configuration ต่างๆที่สร้างขึ้นเพื่อแต่ละบริการ (Service) ในเครื่องให้บริการ ได้
3. สามารถจัดการเครื่องให้บริการต่างๆที่อยู่ภายใต้การควบคุมเช่นการเปิด ปิด หรือเรียกดูสถานะการทำงานของบริการต่างๆได้
4. สามารถกำหนดเวลาให้เครื่องให้บริการทำการ Backup ไฟล์ระบบทั้งหมดซึ่งอยู่ในรูปแบบของไฟล์อิมเมจได้ โดยสามารถระบุเวอร์ชันหรือวัน เดือน ปี ที่สำรองข้อมูล และสามารถดาวน์โหลดไฟล์ดังกล่าวมาเก็บไว้ที่ Centralize Server ได้โดยอัตโนมัติ
5. สามารถทำการ Recovery ไฟล์ระบบทั้งหมดตามเวอร์ชันที่ต้องการให้กับเครื่องที่ให้บริการในกรณีที่เกิดความเสียหายได้
6. สามารถทำการ Backup ค่า Configuration ของแต่ละบริการ (Service) ให้อยู่ในรูปแบบของไฟล์ และสามารถทำการดาวน์โหลด (Download) มาเก็บไว้ยังเครื่องคอมพิวเตอร์ใดๆได้
7. สามารถทำการอัปโหลด (Upload) ค่า Configuration ของแต่ละบริการ (Service) ซึ่งอยู่ในรูปแบบของไฟล์จากเครื่องคอมพิวเตอร์ใดๆไปยัง Centralize Server ได้โดยตรง โดยไม่ต้องผ่านขั้นตอนการ Configuration จากระบบ

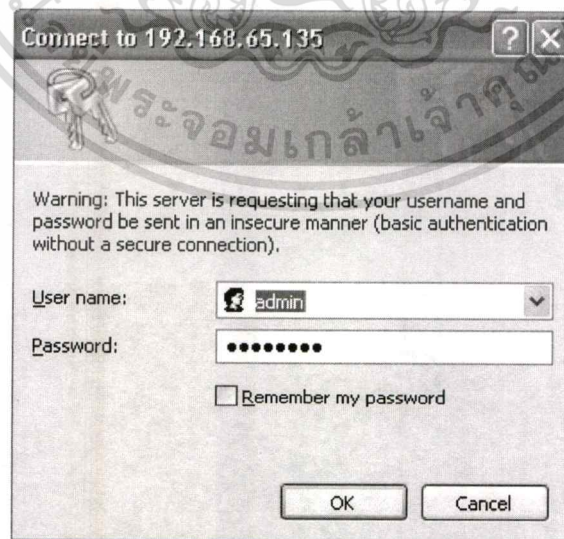
## แผนภาพแสดงโครงสร้างของระบบ



รูปที่ 5.2 แผนภาพแสดงโครงสร้างของระบบ

โดยมีระบบรูปแบบการทำงานดังนี้

ทำการล็อกอินเข้าสู่ระบบ(จะอยู่ในส่วนของยูสเคส Login)โดยในครั้งแรกใช้ชื่อรหัสล็อกอินของระบบเป็นadmin และรหัสผ่านเป็น “password” จากนั้นระบบจะตรวจเช็คข้อมูลผู้ใช้(จะอยู่ในส่วนของยูสเคส create user profile)



รูปที่ 5.3 หน้าจอการเรียกใช้งานโปรแกรมในส่วน Login

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากนั้นผู้ดูแลระบบทำการป้อนข้อมูลระบบ ซึ่งได้แก่การเพิ่มเครื่องให้บริการ เพิ่มบริการ กำหนดว่าเครื่องให้บริการแต่ละเครื่องมีบริการอะไรบ้าง รวมไปถึงการกำหนดว่าแต่ละบริการมีไฟล์คอนฟิกูเรชันที่ไฟล์อะไรบ้าง (ซึ่งจะอยู่ในส่วนของ ยูสเคส Create System Information) จากเมนู Global Configuration แล้วเลือก Information Management ระบบจะแสดงดังรูปที่ 5.4

Power by FreeBSD

MENU

- Global Configuration
  - Information Management
  - Config File Management
  - User Management
- Remote Management
  - Machine and Service
  - Configuration file sending
- Backup and Recovery
  - Backup
  - Backup Schedule
  - Recovery

SUPPORT

- Help

Information Management

Please select method: --select--

>>Remote Machine

| Machine_id | Machine_ip  | Machine_name |                |
|------------|-------------|--------------|----------------|
| 1030       | 192.168.0.1 | Proxy Server | <edit>   <del> |
| 1039       | 192.168.1.1 | Proxy Server | <edit>   <del> |

Add new machine

Machine IP:

Machine Name:

Fingerprint:

\*Insert fingerprint of remote machine from  
"/etc/ssh/ssh\_host\_dsa\_key.pub"

Add to Database:

รูปที่ 5.4 หน้าจอการเรียกใช้งานโปรแกรมในส่วน Information Management

ผู้ดูแลระบบสามารถจัดการไฟล์คอนฟิกูเรชัน ได้เช่น สร้างไฟล์ขึ้นมาใหม่ แก้ไขไฟล์ลบไฟล์ทิ้ง รวมไปถึงการอัปโหลดไฟล์จากเครื่องส่วนตัวยังเครื่องที่ติดตั้งระบบ และสามารถดาวน์โหลดไฟล์จากระบบมาเก็บไว้ที่เครื่องส่วนตัวได้ (ซึ่งจะอยู่ในส่วนของ ยูสเคส Manage Configuration File) โดยการใช้งานในส่วนของ Global Configuration แล้วเลือก config file Management ระบบจะแสดงดังรูปที่ 5.5

Power by FreeBSD

Web-based Remote Service Management System

**MENU**

- Global Configuration
  - Information Management
  - Config File Management
  - User Management
- Remote Management
  - Machine and Service
  - Configuration file sending
- Backup and Recovery
  - Backup
  - Backup Schedule
  - Recovery

**SUPPORT**

**Configuration File Management**

file to upload:

file types allowed: gif, jpg, jpeg, png, bxt, sh, doc, rtf, htm, dmg, gz, cron, conf

Method:

admin tools: <delete all files> | <create new file>

| FILE NAME   | FILE TYPE | FILE SIZE | FUNCTIONS                |
|-------------|-----------|-----------|--------------------------|
| httpd.conf  | CONF      | 16.26 KB  | <edit>   <dl>   <delete> |
| inetd.conf  | CONF      | 5.20 KB   | <edit>   <dl>   <delete> |
| php.conf    | CONF      | 73 bytes  | <edit>   <dl>   <delete> |
| php.ini     | INI       | 40.35 KB  | <edit>   <dl>   <delete> |
| rc.conf     | CONF      | 1.92 KB   | <edit>   <dl>   <delete> |
| squid.conf  | CONF      | 118.40 KB | <edit>   <dl>   <delete> |
| test.txt    | TXT       | 63 bytes  | <edit>   <dl>   <delete> |
| test123.txt | TXT       | 19 bytes  | <edit>   <dl>   <delete> |

### รูปที่ 5.5 การทำงานในส่วนของการจัดการไฟล์คอนฟิกูเรชัน

ผู้ดูแลระบบสามารถจัดการเครื่องให้บริการปลายทางและบริการ ที่ติดตั้งในเครื่องนั้นๆ ได้ เช่นควบคุมการเปิดปิดบริการ และเริ่มการทำงานของเครื่องใหม่ เป็นต้น (ซึ่งจะอยู่ในส่วนของ ยูส เคส Manage Serviced Machine) โดยใช้งานในส่วนของ Remote Management แล้วเลือก Machine and Service ซึ่งระบบจะแสดงเครื่องให้บริการปลายทางทั้งหมดที่ผู้ดูแลระบบทำการบันทึกไว้ และฟังก์ชันการทำงานที่สามารถทำได้ ดังรูปที่ 5.6 และ รูปที่ 5.7

**MENU**

- Global Configuration
  - Information Management
  - Config File Management
  - User Management
- Remote Management
  - Machine and Service
  - Configuration file sending
- Backup and Recovery
  - Backup
  - Backup Schedule
  - Recovery

**SUPPORT**

- Help
- Contact

**Machine and Service Management**

>>All Remote Machines in Database

| Machine_id | Machine_ip  | Machine_name |
|------------|-------------|--------------|
| 1030       | 192.168.0.1 | Proxy Server |
| 1039       | 192.168.1.1 | Proxy Server |

Please select remote machine and method.

Machine :   
\*select machine you want to manage.

Manage Application services :   
\*services you installed later to use as server such as squid, apache, mysql etc.

Manage OS services :   
\*some services that include from operating system such as ssh, cron, netif etc.

Restart Machine :   
\*restart remote machine you select.

Restart Network Interface :   
\*restart network interface on remote machine you select.

รูปที่ 5.6 การทำงานในส่วนของการจัดการเครื่องให้บริการ 1

**Web-based Remote Service Management System**

Power by FreeBSD

**MENU**

- Global Configuration
  - Information Management
  - Config File Management
  - User Management
- Remote Management
  - Machine and Service
  - Configuration file sending
- Backup and Recovery
  - Backup
  - Backup Schedule
  - Recovery

**Service Management**

Machine IP:   
Machine Name :

>>All services which are installed on this machines

| Machine_ip  | Machine_name | service_name |
|-------------|--------------|--------------|
| 192.168.0.1 | Proxy Server | squid        |

Please select service you want to manage.

Service:  Method:

output:

รูปที่ 5.7 การทำงานในส่วนของการจัดการเครื่องให้บริการ 2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ผู้ดูแลระบบสามารถส่งไฟล์คอนฟิกูเรชันไปยังเครื่องให้บริการปลายทาง (ซึ่งจะอยู่ใน ส่วนของ ยูสเคส Send Comfiguration File) โดยใช้งานในส่วนของ Remote Management แล้วเลือก Configuration File Sending ดังรูปที่ 5.8

Power by FreeBSD

**MENU**

- Global Configuration
  - Information Management
  - Config File Management
  - User Management
- Remote Management
  - Machine and Service
  - Configuration file sending
- Backup and Recovery
  - Backup
  - Backup Schedule
  - Recovery

**SUPPORT**

- Help

**Configuration file Sending**

Machine IP: 192.168.0.1

Service Name: squid

| Service_name | ConfigFile_name |
|--------------|-----------------|
| squid        | squid.conf      |

Please select configuration file you want to manage.

Configuration File : squid.conf

Edit Configuration File:

Send Configuration File: /usr/local/etc/squid  
Enter destination path here. (use '/' not '\ or '\\, no trailing '/')

Enter destination file name here.

รูปที่ 5.8 การทำงานในส่วนของการส่งไฟล์คอนฟิกูเรชัน

ผู้ดูแลระบบสามารถทำการสำรองไฟล์ระบบของเครื่องให้บริการปลายทาง (ซึ่งจะอยู่ใน ส่วนของ ยูสเคส Backup File System) โดยการใช้งานในส่วนของ Backup and Recovery แล้วเลือก Backup ซึ่งระบบจะแสดง ดังรูปที่ 5.9

Web-based Remote Service Management System

Power by FreeBSD

**MENU**

- Global Configuration
  - Information Management
  - Config File Management
  - User Management
- Remote Management
  - Machine and Service
  - Configuration file sending
- Backup and Recovery
  - Backup
  - Backup Schedule
  - Recovery

**Backup**

Machine IP : 192.168.0.1

Backup time : 12 : 00

Please select backup schedule that you want.

Every Day    daily backup

Every week    day of week

On Demand    date / month

Immediately    backup file system now!

backup

### รูปที่ 5.9 การทำงานในส่วนของการสำรองไฟล์ระบบ

หลังจากทำการกำหนดตารางเวลาแล้ว ผู้ดูแลระบบสามารถดูตารางการสำรองไฟล์ระบบของเครื่องให้บริการปลายทางได้ โดยการใช้งานในส่วนของ Backup and Recovery แล้วเลือก Backup Schedule ซึ่งระบบจะแสดง ดังรูปที่ 5.10

Web-based Remote Service Management System

Power by FreeBSD

**MENU**

- Global Configuration
  - Information Management
  - Config File Management
  - User Management
- Remote Management
  - Machine and Service
  - Configuration file sending

**Backup Schedule**

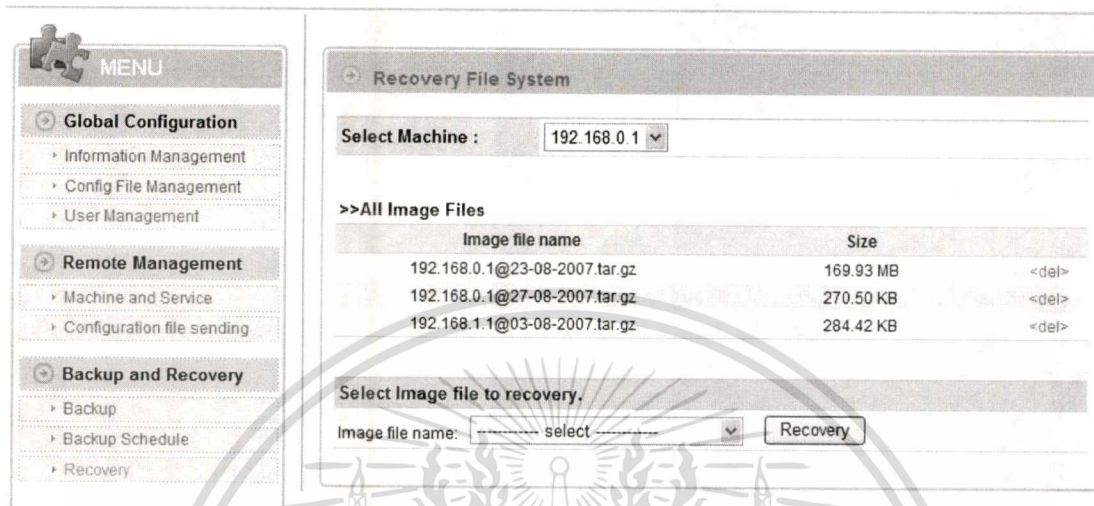
>>All Schedule

| No. | Time    | Day | Month | Day of Week | Remote Machine    |
|-----|---------|-----|-------|-------------|-------------------|
| 1   | 23 : 30 | *   | *     | *           | 192.168.0.1 <del> |
| 2   | 20 : 20 | *   | *     | sun         | 192.168.1.1 <del> |

### รูปที่ 5.10 การทำงานในส่วนของการสำรองไฟล์ระบบ (ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ผู้ดูแลระบบสามารถทำการกู้คืนระบบของเครื่องให้บริการปลายทาง (ซึ่งจะอยู่ในส่วนของ ยูสเทส Recovery File System) โดยการใช้งานในส่วนของ Backup and Recovery แล้วเลือก Recovery ดังรูปที่ 5.11



รูปที่ 5.11 การทำงานในส่วนของการกู้คืนระบบของเครื่องให้บริการปลายทาง

ระบบสามารถทำการเปลี่ยนแปลงชื่อผู้ใช้งานไปถึงรหัสผ่านของผู้ที่มีสิทธิใช้งานระบบได้ (ซึ่งจะอยู่ในส่วนของ ยูสเทส Create User Profile) โดยการใช้งานในส่วนของ Global Configuration แล้วเลือก User Management ดังรูปที่ 5.12



รูปที่ 5.12 การทำงานในส่วนของการแก้ไขข้อมูลผู้ใช้

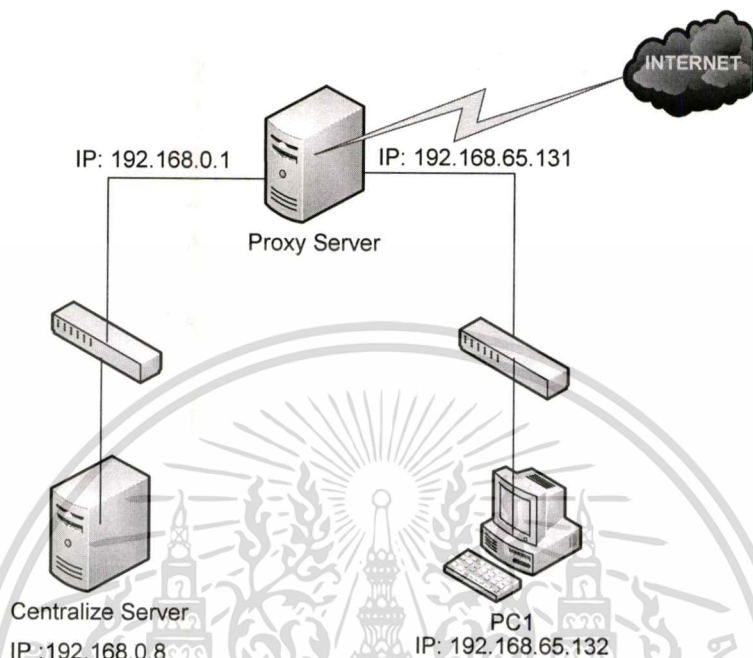
หมายเหตุ รายละเอียดและวิธีการใช้งานของโปรแกรมได้จัดไว้ใน ภาคผนวก ก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## 5.5 การทดสอบระบบ

การทดสอบฟังก์ชันการจัดการเครื่องให้บริการปลายทาง (Machine and Service Management)

โครงสร้างของระบบที่ใช้ในการทดสอบจะเป็นดังรูปที่ 5.13



รูปที่ 5.13 โครงสร้างของระบบที่ใช้ในการทดสอบ 1

PC1 เป็นเครื่องไคลเอนท์ ซึ่งเชื่อมต่ออินเทอร์เน็ตผ่าน Proxy Server โดย Proxy Server เป็นเครื่องให้บริการที่อยู่ภายใต้การควบคุมของ Centralize Server เริ่มต้นเข้าใช้งานระบบในส่วน

ของ Remote Management แล้วเลือก Machine and Service จากนั้นทำการกำหนดหมายเลขไอพีของเครื่องให้บริการปลายทางเป็น 192.168.0.1 ซึ่งเป็น

หมายเลขไอพีของ Proxy Server

เลือกที่ปุ่ม Manage Application Services ระบบจะแสดงผลดังรูปที่ 5.14

**Please select remote machine and method.**

**Machine :**    
\*select machine you want to manage.

**Manage Application services :**    
\*services you installed later to use as server such as squid, apache, mysql etc.

**Manage OS services :**    
\*some services that include from operating system such as ssh, cron, netif etc.

**Restart Machine :**    
\*restart remote machine you select.

**Restart Network Interface :**    
\*restart network interface on remote machine you select.

**Service Management**

**Machine IP:** 192.168.0.1  
**Machine Name :** newFreeBSD for testing

>>All services which are installed on this machines

| Machine_ip  | Machine_name           | service_name |
|-------------|------------------------|--------------|
| 192.168.0.1 | newFreeBSD for testing | squid        |

**Please select service you want to manage.**

| Service                            | Method                                                                                                                                                |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="text" value="squid"/> | <input type="button" value="status"/> <input type="button" value="start"/> <input type="button" value="stop"/> <input type="button" value="restart"/> |

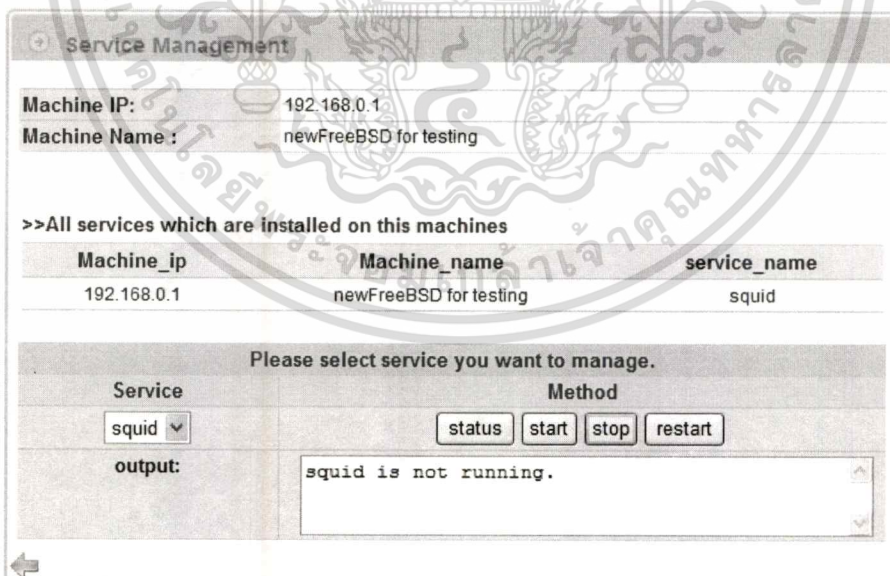
**output:** squid is running as pid 1112 1114.

รูปที่ 5.14 ผลการทดสอบฟังก์ชันการจัดการเครื่องให้บริการปลายทาง 1

จากรูปที่ 5.14 จะเห็นว่า บริการที่ชื่อ squid ซึ่งเป็นบริการ Web Proxy กำลังทำงานอยู่ ดังนั้นเครื่อง PC1 จะสามารถเชื่อมต่ออินเทอร์เน็ตได้ดังรูปที่ 5.15



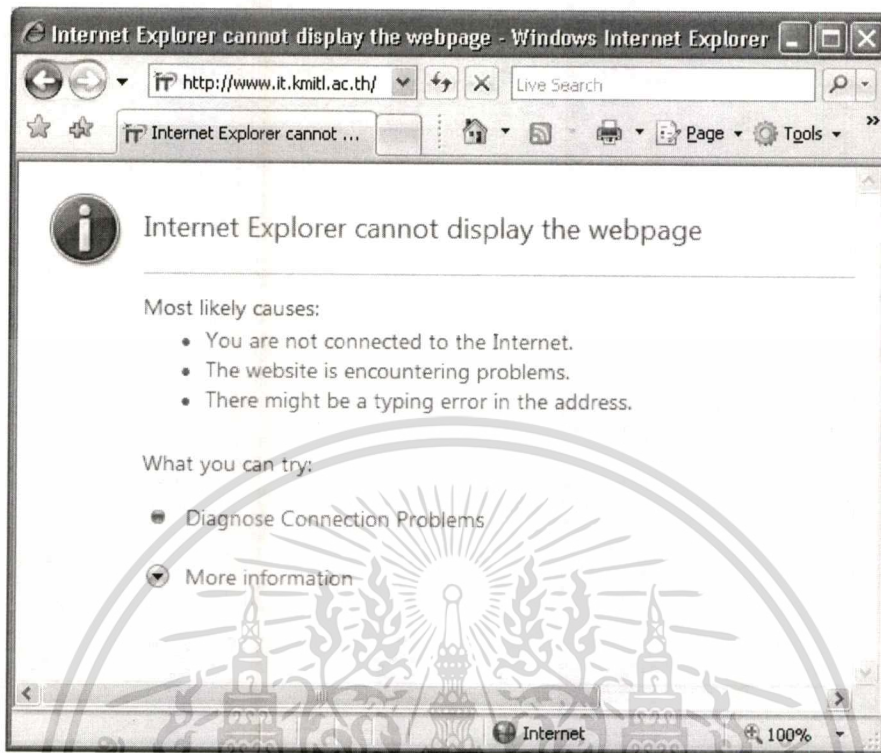
รูปที่ 5.15 ผลการทดสอบฟังก์ชันการจัดการเครื่องให้บริการปลายทาง 2  
หยุดการทำงานของ squid โดยกดที่ปุ่ม stop ระบบจะแสดงผลการทำงานดังรูปที่ 5.16



รูปที่ 5.16 ผลการทดสอบฟังก์ชันการจัดการเครื่องให้บริการปลายทาง 3

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เมื่อ Squid ไม่ทำงานเครื่อง PC1 จะไม่สามารถเชื่อมต่ออินเทอร์เน็ตได้ดังรูปที่ 5.17



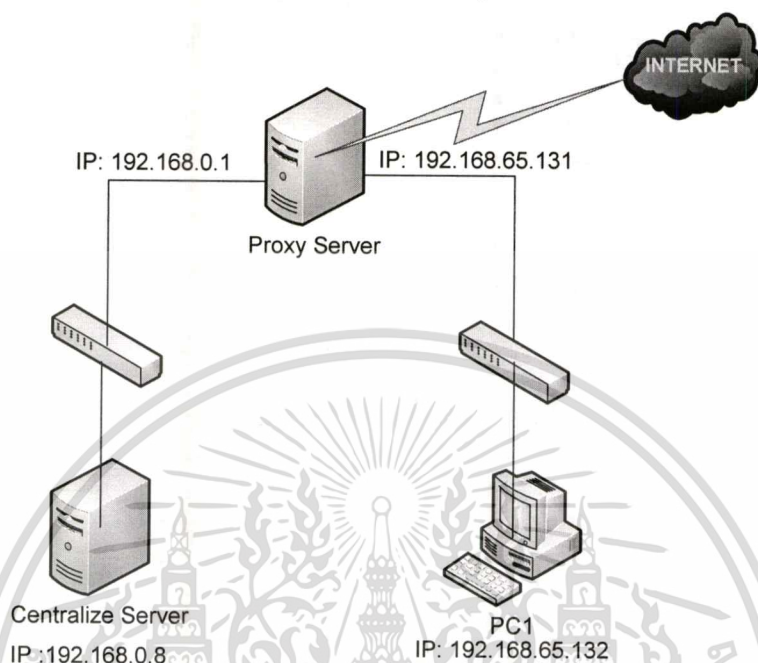
รูปที่ 5.17 ผลการทดสอบฟังก์ชันการจัดการเครื่องให้บริการปลายทาง 4

### สรุปผลการทดสอบ

ฟังก์ชันการจัดการเครื่องให้บริการปลายทางสามารถทำงานได้อย่างถูกต้องตามที่ออกแบบไว้ เมื่อสั่งให้บริการใดหุคการทำงาน ผู้ใช้งานที่ใช้บริการนั้นๆอยู่ก็จะไม่สามารถใช้งานได้เช่นกัน ดังตัวอย่างจะเห็นว่าเมื่อผู้ดูแลระบบหุคการทำงานของ Squid ผู้ใช้งานที่ PC1 จะไม่สามารถเข้าถึงเว็บเพจใดๆได้เลย

## การทดสอบฟังก์ชันการส่งไฟล์คอนฟิกูเรชันไปยังเครื่องให้บริการปลายทางตามบริการที่เครื่อง นั้นมี (Configuration File Sending)

โครงสร้างของระบบที่ใช้ในการทดสอบจะเป็นดังรูปที่ 5.18



รูปที่ 5.18 โครงสร้างของระบบที่ใช้ในการทดสอบ 2

PC1 เป็นเครื่องไคลเอ็นท์ ซึ่งเชื่อมต่ออินเทอร์เน็ตผ่าน Proxy Server โดย Proxy Server เป็นเครื่องให้บริการที่อยู่ภายใต้การควบคุมของ Centralize Server เริ่มต้นเข้าใช้งานระบบในส่วน  
ของ Remote Management แล้วเลือก Configuration File Sending

จากนั้นทำการกำหนดหมายเลขไอพีของเครื่องให้บริการปลายทางเป็น 192.168.0.1 ซึ่งเป็น  
หมายเลขไอพีของ Proxy Server เลือกบริการที่ชื่อ squid และเลือกไฟล์คอนฟิกูเรชันที่ชื่อ  
squid.conf

กำหนดตำแหน่งปลายทางที่เก็บไฟล์คอนฟิกูเรชันอยู่ ซึ่งในที่นี้คือ /usr/local/etc/squid  
และชื่อไฟล์ปลายทางชื่อ squid.conf ดังรูปที่ 5.19

**Configuration file Sending**

Machine IP: 192.168.0.1

Service Name: squid

| Service_name | ConfigFile_name |
|--------------|-----------------|
| squid        | squid.conf      |

**Please select configuration file you want to manage.**

Configuration File : squid.conf <= select configuration file that you want.

Edit Configuration File:

Send Configuration File:

Enter destination path here. (use '/', not '\', or '\\', no trailing '/')

Enter destination file name here.

รูปที่ 5.19 ผลการทดสอบฟังก์ชันการการส่งไฟล์คอนฟิกูเรชัน 1

เมื่อกดปุ่ม Send ระบบจะแสดงผลดังรูปที่ 5.20

**Verify Configuration File**

Remote Machine you want to send this file: 192.168.0.1

Configuration file you want to send: squid.conf

Destination file you want to replace: squid.conf

Destination path you want to send this file: /usr/local/etc/squid

Some person had just modified this file on the remote machine.  
If you send this file, the existing file will be replaced with this file immediately.  
Are you sure to send this file now.

รูปที่ 5.20 ผลการการทดสอบฟังก์ชันการการส่งไฟล์คอนฟิกูเรชัน 2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 5.20 จากผลลัพธ์แสดงว่ามีบุคคลอื่นทำการเปลี่ยนแปลงไฟล์ดังกล่าวโดยตรงที่เครื่องให้บริการปลายทาง ระบบจึงแจ้งเตือนให้ผู้ดูแลระบบทราบ และให้เลือกว่าจะส่งไฟล์นี้หรือไม่ เพราะหากตกลงที่จะส่ง ไฟล์ที่ส่งไปนี้จะทับไฟล์เดิมที่มีอยู่แล้วทันที

ทำการส่งไฟล์เดิมอีกครั้งหนึ่ง โดยครั้งนี้ให้ทำการแก้ไขไฟล์ก่อนส่งโดยจากรูปที่ 5.19 ให้กดที่ปุ่ม edit ระบบจะเปิดไฟล์ดังกล่าวขึ้นมา ทำการเพิ่มข้อมูลลงไปดังรูปที่ 5.21

```

acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 21         # ftp
acl Safe_ports port 443 563    # https, snews
acl Safe_ports port 70        # gopher
acl Safe_ports port 210       # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280       # http-mgmt
acl Safe_ports port 488       # gss-http
acl Safe_ports port 591       # filemaker
acl Safe_ports port 777       # multiling http
acl CONNECT method CONNECT

acl kmitl url_regex -i kmitl
http_access deny kmitl

# TAG: http_access
#   Allowing or Denying access based on defined access lists
#
#   Access to the HTTP port:
#   http_access allow/deny (hostname

```

รูปที่ 5.21 ผลการทดสอบฟังก์ชันการการส่งไฟล์คอนฟิกูเรชัน 3

จากนั้นทำการบันทึกโดยกด Save และทำการส่งไฟล์เดิมอีกครั้งตามขั้นตอนเดิม ระบบจะแสดงผลดังรูปที่ 5.22

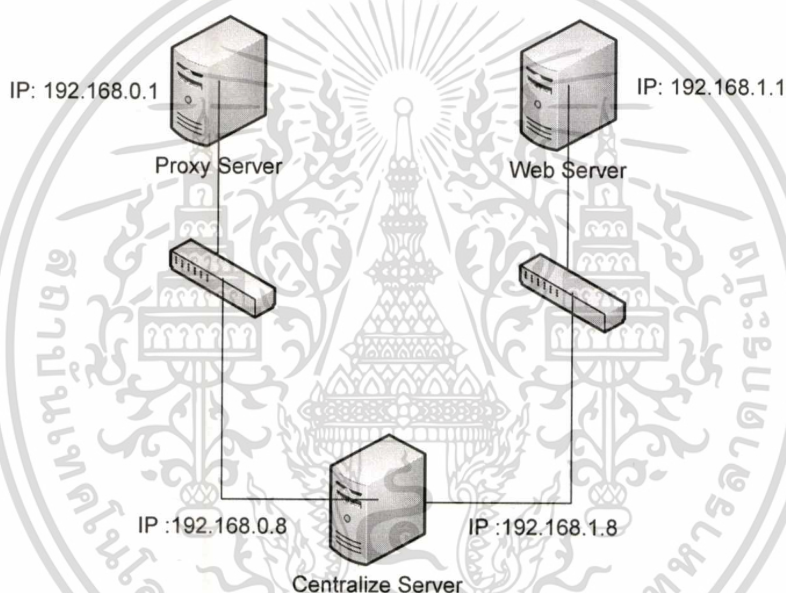


## สรุปผลการทดสอบ

ฟังก์ชันการส่งไฟล์คอนฟิกูเรชัน สามารถทำงานได้อย่างถูกต้องตามที่ออกแบบไว้ ระบบมีการแจ้งเตือนผู้ดูแลระบบ เมื่อมีบุคคลอื่นทำการเปลี่ยนแปลงไฟล์คอนฟิกูเรชัน โดยตรงที่เครื่องให้บริการปลายทาง และเมื่อทำการแก้ไขค่าคอนฟิกูเรชันใหม่ และส่งไฟล์ดังกล่าวไปยังปลายทางแล้ว ค่าคอนฟิกูเรชันของเครื่องให้บริการปลายทางเปลี่ยนแปลงไปตามที่ผู้ดูแลระบบกำหนด ซึ่งแสดงให้เห็นว่าไฟล์คอนฟิกูเรชันดังกล่าวส่งไปถึงปลายทางตามตำแหน่งที่กำหนดได้อย่างถูกต้อง

## การทดสอบฟังก์ชันการสำรองไฟล์ระบบของเครื่องให้บริการปลายทาง (Backup)

โครงสร้างของระบบที่ใช้ในการทดสอบจะเป็นดังรูปที่ 5.21



รูปที่ 5.24 โครงสร้างของระบบที่ใช้ในการทดสอบ 3

จากรูปที่ 5.24 Proxy Server และ Web Server เป็นเครื่องให้บริการที่อยู่ภายใต้การควบคุมของ Centralize Server การเข้าใช้งานระบบนี้ ทำได้โดยเลือกเมนูในส่วนของ Backup and Recovery แล้วเลือก Backup

จากนั้นทำการกำหนดหมายเลขไอพีของเครื่องให้บริการปลายทางเป็น 192.168.0.1 ซึ่งเป็นหมายเลขไอพีของ Proxy Server ทำการเลือกเวลาและช่วงเวลาที่ต้องการซึ่งในการทดสอบครั้งนี้จะเลือกที่จะสำรองข้อมูลทันที ดังนั้นจึงไม่จำเป็นต้องกำหนด Backup time คลิกเลือกที่ Immediately แล้วกด Backup ได้เลย ดังรูปที่ 5.25

**Backup Schedule**

Machine IP : 192.168.0.1

Backup time : hour : minute

Please select backup schedule that you want.

Every Day daily backup

Every week day of week

On Demand date / month

Immediately backup file system now!

Warning !!  
Don't close this page until the sucessfull message was appear.

backup

รูปที่ 5.25 ผลการทดสอบฟังก์ชันการสำรองไฟล์ระบบ 1

รอนระบบทำงานเสร็จสิ้น ระบบจะแสดงข้อความดังรูปที่ 5.26

**The backup schedule was completely.**

Click ok to close this this page.

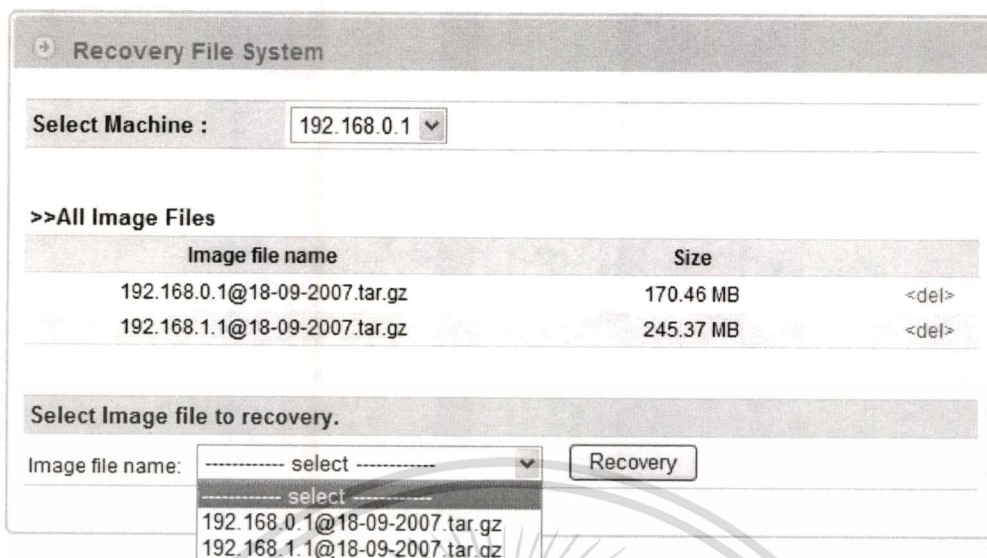
ok

รูปที่ 5.26 ผลการทดสอบฟังก์ชันการสำรองไฟล์ระบบ 2

จากนั้นทำตามขั้นตอนเดิมอีกครั้งโดยเปลี่ยนหมายเลขไอพีของเครื่องให้บริการปลายทางเป็น 192.168.1.1 ซึ่งเป็นหมายเลขไอพีของ Web Server

เมื่อการทำงานเสร็จสมบูรณ์ เข้าสู่เมนู Backup and Recovery แล้วเลือก Recovery ระบบจะแสดงอิมเมจไฟล์ระบบทั้งหมด จะเห็นว่ามิมเมจไฟล์ระบบอยู่ 2 ไฟล์คือ 192.168.0.1@18-09-2007.tar.gz และ 192.168.1.1@18-09-2007.tar.gz ซึ่งเป็นไฟล์ที่เกิดขึ้นจากการทำงานก่อนหน้านี้ สังเกตได้จากชื่อไฟล์จะอยู่ในรูปแบบ หมายเลขไอพีของเครื่องปลายทาง@วันเดือนปีที่ทำการสำรองข้อมูล.tar.gz ดังรูปที่ 5.27

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



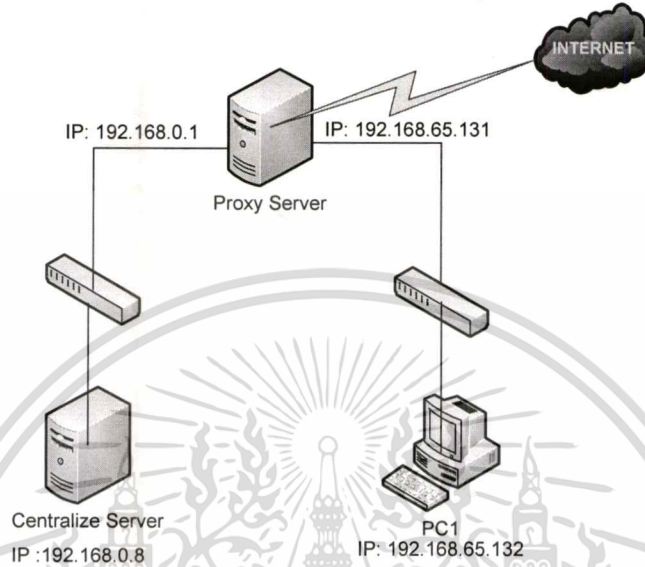
รูปที่ 5.27 อิมเมจของไฟล์ระบบทั้งหมดที่ Centralize Server มี

### สรุปผลการทดสอบ

ฟังก์ชันการสำรองไฟล์ระบบสามารถทำงานได้อย่างถูกต้องตามที่ออกแบบไว้ โดยเมื่อผู้ดูแลระบบสั่งให้ระบบทำการสำรองไฟล์ระบบของเครื่องให้บริการปลายทางที่เลือกไว้ ระบบสามารถดำเนินการได้ถูกต้อง ทำให้สามารถดาวน์โหลดอิมเมจไฟล์ระบบที่อยู่ในรูปแบบที่ออกแบบไว้มาเก็บไว้ที่ Centralize Server ได้เพื่อรองรับการกู้คืนระบบต่อไป

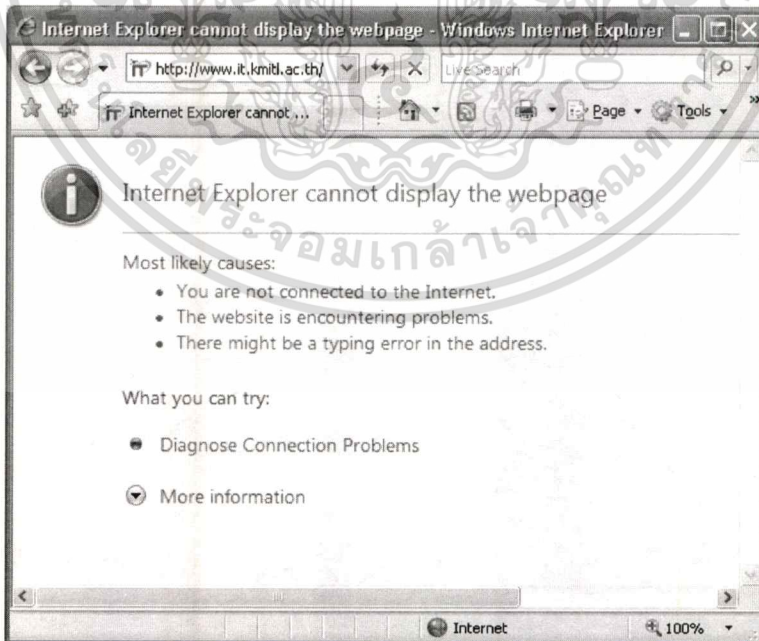
## การทดสอบฟังก์ชันการกู้คืนไฟล์ระบบให้กับเครื่องให้บริการปลายทาง (Recovery)

จากโครงสร้างของระบบเดิมในรูปที่ 5.24 ผู้ดูแลระบบได้นำ Proxy Server ออกไป แล้วนำเครื่องสำรองอีกเครื่องมาใช้แทน ซึ่งเครื่องสำรองนี้ได้ทำการติดตั้งระบบปฏิบัติการกำหนดหมายเลขไอพีให้เหมือนเดิม และได้ทำการปรับแต่งระบบเบื้องต้นตามหัวข้อที่ 5.3 เรียบร้อยแล้ว



รูปที่ 5.28 โครงสร้างของระบบที่ใช้ในการทดสอบ 4

เนื่องจากเครื่องสำรองยังไม่ได้ติดตั้ง Squid ดังนั้น PC1 จะไม่สามารถเชื่อมต่ออินเทอร์เน็ตได้ดังรูปที่ 5.29



รูปที่ 5.29 ผลการการทดสอบฟังก์ชันการกู้คืนไฟล์ระบบ 1

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เข้าสู่เมนู Global Configuration แล้วเลือก Information Management ทำการแก้ไข Fingerprint ของ Proxy Server ใหม่ด้วย Fingerprint ของเครื่องสำรองดังรูปที่ 5.30

**Information Management**

Please select method:

---

**>>Remote Machine**

| Machine_id | Machine_ip  | Machine_name |                                                                                        |
|------------|-------------|--------------|----------------------------------------------------------------------------------------|
| 1030       | 192.168.0.1 | Proxy Server | <input type="button" value="&lt;edit&gt;"/> <input type="button" value="&lt;del&gt;"/> |
| 1040       | 192.168.1.1 | Web Server   | <input type="button" value="&lt;edit&gt;"/> <input type="button" value="&lt;del&gt;"/> |

---

**Add new machine**

Machine IP:

Machine Name:

---

**Fingerprint Management**

Machine IP:

Machine Name :

Existing Fingerprint:

IBpjKipshoJFX9QS2PP/vH6ggw9qSdfCqEbmRyHOPTzYj  
gYVnNEdiLvqYKIqH5u/0c6QveohgnvdtSZEhagIP77RNo  
TWAtH0JFNe6J+ndcz/hMJGRfjKfcaK2R7wyGjuAG6TwKV  
fqGgCYibojJlIqeVTZhe/hUvT4i6QGDZN84W/Q==

---

**Modify Fingerprint**

New Fingerprint :

ACBAIJFFLhfs33XGkz0ZZTL2m3g53sLkeYQqkV6X0pMM  
WM1xX9XpsooyK6lmbpgk4ImeArGqgeN88ekYzgZcsKmaf  
0UsZI1Y6dkm6cbh9Xsba86jnGQjdYxX5ilP/hXYzZ7YaF  
xko6jKEJqE2cJbfbBaly5HH80pVr73GzxXEJZpsV

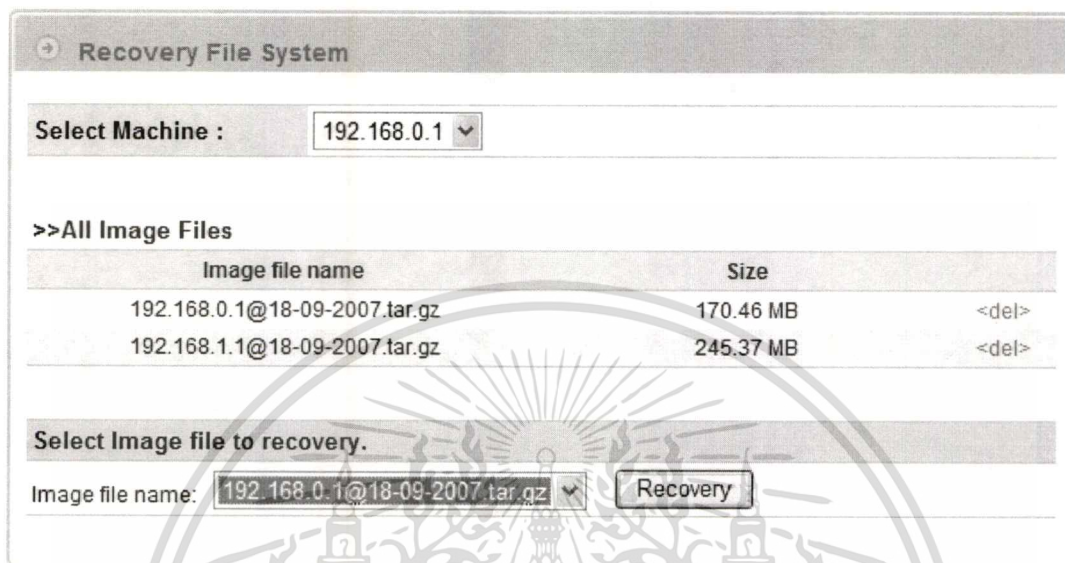
\*Insert fingerprint of remote machine from  
"/etc/ssh/ssh\_host\_dsa\_key.pub"

Change fingerprint :

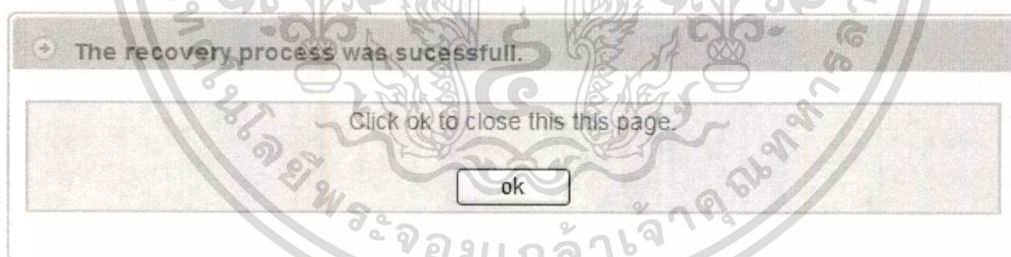
รูปที่ 5.30 ผลการทดสอบฟังก์ชันการกู้คืนไฟล์ระบบ 2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เข้าสู่เมนู Backup and Recovery แล้วเลือก Recovery ระบบจะแสดงอิมเมจไฟล์ระบบทั้งหมด เลือกหมายเลขไอพีเป็น 192.168.0.1 และเลือกไฟล์อิมเมจที่ชื่อ 192.168.0.1@18-09-2007.tar.gz จากนั้นกด Recovery ดังรูปที่ 5.31



รูปที่ 5.31 ผลการทดสอบฟังก์ชันการกู้คืนไฟล์ระบบ 3  
รอนระบบทำงานเสร็จสิ้น ระบบจะแสดงข้อความดังรูปที่ 5.32



รูปที่ 5.32 ผลการทดสอบฟังก์ชันการกู้คืนไฟล์ระบบ 4

จากนั้นทำการแก้ไข Fingerprint อีกครั้งด้วย Fingerprint เดิมของ Proxy Server ตามขั้นตอนที่ผ่านมา

ตรวจสอบที่เครื่องสำรอง จะเห็นว่า kernel ของระบบเปลี่ยนจาก GERNERIC ซึ่งเป็น kernel ดิพอลท์ของระบบปฏิบัติการกลายเป็น MAINGATE ซึ่งเป็น kernel ที่ผ่านการคอมไพล์แล้ว ดังรูปที่ 5.33 และรูปที่ 5.34

```

Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.
FreeBSD 5.5-RELEASE #0: Tue May 23 14:58:27 UTC 2006
root@perseus.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC
Timecounter "i8254" frequency 1193182 Hz quality 0
CPU: Intel(R) Pentium(R) M processor 1.60GHz (1595.47-MHz 686-class CPU)
Origin = "GenuineIntel" Id = 0x6d8 Stepping = 8
Features=0xfe9fbff<FPU, UME, DE, PSE, TSC, MSR, PAE, MCE, CX8, APIC, SEP, MTRR, PGE, MCA
OV, PAT, CLFLUSH, DTS, ACPI, MMX, FXSR, SSE, SSE2, SS>
real memory = 268435456 (256 MB)
avail memory = 252952576 (241 MB)
CPI APIC Table: <PTLTD APIC >

```

รูปที่ 5.33 ผลการทดสอบฟังก์ชันการกู้คืนไฟลัระบบ 5

```

Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.
FreeBSD 5.5-RELEASE #0: Tue Jul 25 00:19:22 ICT 2006
root@newFreeBSD.localdomain:/usr/src/sys/i386/compile/MAINGATE
Timecounter "i8254" frequency 1193182 Hz quality 0
CPU: Intel(R) Pentium(R) M processor 1.60GHz (1635.94-MHz 686-class CPU)
Origin = "GenuineIntel" Id = 0x6d8 Stepping = 8
Features=0xfe9fbff<FPU, UME, DE, PSE, TSC, MSR, PAE, MCE, CX8, APIC, SEP, MTRR, PGE, MCA
OV, PAT, CLFLUSH, DTS, ACPI, MMX, FXSR, SSE, SSE2, SS>
real memory = 268435456 (256 MB)
avail memory = 252952576 (241 MB)
CPI APIC Table: <PTLTD APIC >

```

รูปที่ 5.4 ผลการทดสอบฟังก์ชันการกู้คืนไฟลัระบบ 6

เมื่อทดลองตรวจดูโปรเซสการทำงานของ squid จะเห็นว่า เครื่องสำรองไม่มีโปรเซสการทำงานของ squid อยู่เนื่องจากยังไม่ได้ทำการติดตั้ง ดังรูปที่ 5.35

```

Spare# ps -aux | grep squid
Spare# █

```

รูปที่ 5.35 ผลการทดสอบฟังก์ชันการกู้คืนไฟลัระบบ 7

แต่หลังจากทำการกู้คืนไฟลัระบบแล้ว จะเห็นว่า เครื่องสำรองมีโปรเซสของ squid กำลังทำงานอยู่ อีกทั้งชื่อเครื่องยังเปลี่ยนกลับไปเป็น newFreeBSD เหมือนเดิมตามที่ Proxy Server เคยใช้อยู่ ดังรูปที่ 5.34

```

newFreeBSD# ps -aux | grep squid
squid 461 0.0 0.6 3140 1480 ?? Is 3:08AM 0:00.0
squid 465 0.0 2.4 6680 6040 ?? S 3:08AM 0:00.4
squid 474 0.0 0.2 1192 556 ?? Is 3:08AM 0:00.0
root 572 0.0 0.3 1424 872 v0 R+ 3:31AM 0:00.0
newFreeBSD# █

```

รูปที่ 5.36 ผลการทดสอบฟังก์ชันการกู้คืนไฟลัระบบ 8

และเมื่อทำงานเสร็จสมบูรณ์ ทดลองเชื่อมต่ออินเทอร์เน็ตอีกครั้งจาก PC1 จะเห็นว่า PC1 สามารถกลับมาเชื่อมต่ออินเทอร์เน็ตได้เหมือนเดิม ดังรูปที่ 5.37

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.37 ผลการทดสอบฟังก์ชันการกู้คืนไฟล์ระบบ 9

### สรุปผลการทดสอบ

ฟังก์ชันการกู้คืนไฟล์ระบบสามารถทำงานได้อย่างถูกต้องตามที่ออกแบบไว้ โดยเมื่อผู้ดูแลระบบสั่งให้ระบบทำการกู้คืนไฟล์ระบบให้กับเครื่องสำรองที่เตรียมไว้ ระบบสามารถดำเนินการได้ถูกต้อง ทำให้เครื่องสำรองสามารถทำงานแทน Proxy Server เครื่องเดิมได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## บทที่ 6

# บทสรุปและแนวทางพัฒนาในอนาคต

### 6.1 ข้อจำกัดของระบบ

ระบบนี้พัฒนาขึ้นมาบนระบบปฏิบัติการฟรีบีเอสดีซึ่งจุดเด่นของระบบปฏิบัติการนี้คือสามารถติดตั้งโปรแกรมหรือบริการต่างๆผ่านพอร์ต (Port) โดยไม่จำเป็นต้องดาวน์โหลดโปรแกรมมาไว้ที่เครื่องแล้วคอมไพล์เอง

ด้วยเหตุนี้กระบวนการในการทำงานทั้งหมดของระบบนี้ จึงเน้นไปที่การจัดการบริการหรือโปรแกรมที่ทำการติดตั้งผ่านพอร์ตทั้งหมด ตัวอย่างเช่น คำสั่งในการสั่ง start, stop, restart บริการที่ติดตั้งอยู่บนเครื่องให้บริการปลายทางสามารถทำได้โดยการสั่งรัน Shell Script ใน /usr/local/etc/rc.d ซึ่งเป็น Script ที่ถูกสร้างขึ้นโดยอัตโนมัติเมื่อมีการติดตั้งบริการดังกล่าวผ่านพอร์ต ตัวอย่างเช่น

```
# ssh root@192.168.1.1 "/usr/local/etc/rc.d/apache22.sh restart"
```

ดังนั้นหากบริการหรือโปรแกรมใดๆ ผู้ใช้งานทำการดาวน์โหลดมาคอมไพล์หรือติดตั้งเอง ระบบนี้จะไม่สามารถทำงานหรือจัดการบริการนี้ได้

### 6.2 บทสรุปและแนวทางในการพัฒนาในอนาคต

ระบบสารสนเทศในปัจจุบันส่วนใหญ่มักจะมีลักษณะเป็นระบบสารสนเทศแบบกระจาย ซึ่งการออกแบบระบบในลักษณะนี้สามารถทำให้ประสิทธิภาพโดยรวมของระบบดีมากขึ้น แต่สิ่งที่ตามมาก็คือ การบริหารจัดการและการบำรุงรักษาจะทำได้ยากขึ้นเช่นกัน

ปัจจุบันมีซอฟต์แวร์มากมายที่ผลิตขึ้นมาเพื่อช่วยเหลือผู้ดูแลระบบ ในการบริหารจัดการเครื่องให้บริการต่างๆในระบบสารสนเทศแบบกระจาย โดยซอฟต์แวร์แต่ละตัวต่างก็มีข้อดีข้อเสียแตกต่างกันไป ระบบจัดการบริการระยะไกลผ่านเว็บ เป็นอีกหนึ่งทางเลือกสำหรับผู้ดูแลระบบ ซึ่งนอกจากจะมีส่วนติดต่อผู้ใช้เป็นแบบเว็บซึ่งง่ายต่อการใช้งาน และสามารถใช้งานได้อย่างกว้างขวางแล้ว ระบบนี้ยังถูกออกแบบมาให้ง่ายต่อการติดตั้ง โดยการติดตั้งโปรแกรมหรือระบบจะติดตั้งไว้ที่เครื่องตัวกลาง (Centralize Server) เท่านั้นโดยไม่ยุ่งเกี่ยวกับเครื่องให้บริการปลายทาง (Serviced Machine) เลย

จากเดิมหากผู้ดูแลระบบต้องการจะจัดการหรือควบคุมเครื่องให้บริการใดๆ ผู้ดูแลระบบอาจจำเป็นต้องติดตั้งโปรแกรมที่ทำหน้าที่เป็นเอเจนต์ (Agent) ไว้ที่เครื่องดังกล่าวด้วยหรือหากเป็นระบบสารสนเทศแบบเว็บ อย่างน้อยที่สุดผู้ดูแลระบบจำเป็นต้องติดตั้งเว็บเซิร์ฟเวอร์ (Web Server) ไว้ด้วย ซึ่งบางครั้งเครื่องดังกล่าวอาจจะไม่จำเป็นต้องใช้ เป็นการสิ้นเปลืองทรัพยากรโดย

เอกสารนี้เป็นเอกสารที่สงวนลิขสิทธิ์ไว้เพื่อการเผยแพร่เท่านั้น ไม่อนุญาตให้เผยแพร่โดยไม่ผ่านการคัดค้าน  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เปล่าประโยชน์ ระบบจัดการบริการระยะไกลผ่านเว็บจึงออกแบบมาให้ใช้บริการที่มีอยู่แล้วในระบบปฏิบัติการมาช่วยในการติดต่อสื่อสารระหว่างเครื่องตัวกลางและเครื่องให้บริการปลายทาง ซึ่งทำให้จะลดภาระของผู้ดูแลระบบในการติดตั้งและไม่สิ้นเปลืองทรัพยากรในเครื่องให้บริการปลายทางมากจนเกินไป

จากการที่ระบบทั้งหมดถูกติดตั้งอยู่ที่เครื่องตัวกลางเพียงแห่งเดียวทำให้เกิดข้อดีอีกอย่างหนึ่งก็คือ ไฟล์คอนฟิกูเรชันทั้งหมดจะเก็บสำรองไว้ที่เครื่องตัวกลางด้วยการกู้คืนค่าคอนฟิกูเรชัน รวมถึงการสำเนาค่าคอนฟิกูเรชันจากอีกเครื่องหนึ่งไปสู่อีกเครื่องหนึ่งจะทำให้สะดวกยิ่งขึ้น นอกจากนี้ระบบยังสามารถสั่งการให้เครื่องให้บริการปลายทางทำการสำรองไฟล์ระบบทั้งหมดของตัวเองมาเก็บไว้ที่เครื่องตัวกลางได้ ซึ่งจะเกิดผลดีในกรณีที่เครื่องดังกล่าวเสียหายไปไม่สามารถทำงานได้ ผู้ดูแลระบบสามารถนำเครื่องอื่นมาสำรองใช้ก่อนได้ โดยระบบสามารถส่งอีเมลไฟล์ระบบของเครื่องให้บริการเดิมไปยังเครื่องสำรอง เพื่อให้เครื่องสำรองทำการกู้คืนไฟล์ระบบจากไฟล์ดังกล่าว และเมื่อเครื่องให้บริการเดิมได้ทำการซ่อมแซมแก้ไขจนสามารถใช้งานได้ตามปกติแล้ว ระบบก็ยังสามารถกู้คืนข้อมูลไฟล์ระบบทั้งหมดให้เครื่องให้บริการได้อีกด้วย ตามกลไกเดิม

จะเห็นว่าระบบจัดการบริการระยะไกลผ่านเว็บมีข้อดีในเรื่องของการสำรอง การกู้คืนทั้งไฟล์คอนฟิกูเรชันและไฟล์ระบบทั้งหมดรวมไปถึงการติดตั้งที่ไม่ยุ่งยาก แต่การที่ระบบและข้อมูลทั้งหมดถูกเก็บไว้ที่เครื่องตัวกลางเพียงเครื่องเดียว ดังนั้นหากเครื่องตัวกลางเกิดเสียหายไปไม่สามารถใช้งานได้ระบบนี้ก็จะเป็นที่ใช้งานไม่ได้เช่นกัน ดังนั้นผู้ดูแลระบบควรมีกลไกในการป้องกันหรือบำรุงรักษาเครื่องตัวกลางให้มีความคงทนต่อความเสียหายด้วย (Fault Tolerance)

แนวทางในการพัฒนาในอนาคตนั้น ผู้พัฒนามีแนวคิดที่จะพัฒนาให้ระบบนี้สามารถรองรับโปรแกรมหรือบริการที่ติดตั้งได้ทุกแบบ ไม่จำกัดเฉพาะโปรแกรมที่ติดตั้งผ่านพอร์ตแต่เพียงอย่างเดียว และมีแนวคิดที่จะเพิ่มฟังก์ชันการทำงานให้มากขึ้นรองรับการบริหารจัดการเครื่องให้บริการปลายทางให้ครอบคลุมทุกฟังก์ชันการทำงานให้มากที่สุด

## บรรณานุกรม

- กษิต ศาณูเชี่ยว. 2548. การทำงานข้ามเครื่อง UNIX คอมพิวเตอร์โดยไม่มี password. กรุงเทพฯ : ภาควิชาศาสตร์คอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์.
- กิตติ ภัคดีวัฒนกุล และกิตติพงษ์ กลมกล่อม. 2544. UML วิเคราะห์และออกแบบระบบเชิงวัตถุ. กรุงเทพฯ : เคทีพีคอมพิวเตอร์คอนซัลท์.
- กิตติพงษ์ สุวรรณราช. 2547. การบริหารและจัดการเครือข่ายอินเทอร์เน็ตด้วยระบบปฏิบัติการ FreeBSD. กรุงเทพฯ : ออฟเซ็ทเพรส.
- กิตติศักดิ์ เจริญโภคานนท์. 2548. คู่มือเรียนเขียนเว็บอ้อมเมริค์ด้วย PHP5. กรุงเทพฯ : ชัคเซสมีเดีย.
- บัณฑิต จามรภูมิ. 2549. คู่มือระบบยูนิกซ์ FreeBSD เล่ม 1. กรุงเทพฯ : บัณฑิตเพลส.
- สมศักดิ์ โชคชัยชุกุล. 2547. อินไซด์ PHP5. กรุงเทพฯ : โปรวิชั่น.
- สรวิศ กอสุวรรณศิริ. 2544. เสริมแต่งโฮมเพจครั้งใหม่! ให้มีชีวิตชีวาด้วย JavaScript. กรุงเทพฯ : วิตตี้ กรุ๊ป.
- Booch, G., Jacobson, I., and Rumbaugh, J. 1997. **The UML specification documents**. Santa Clara, CA.: Rational Software Corp.
- Damien Miller. 2002. **SSH tips, tricks & protocol tutorial**. [Online]. Available : <http://www.mindrot.org/~djm/auug2002/ssh-tutorial.pdf>
- Fred Blaise. 2006. **Remote backup using ssh, tar and cron**. [Online]. Available : <http://hostlibrary.com/Remotebackupusingsshtarandcron-how-to.html>
- The FreeBSD Documentation Project. 2007. **FreeBSD Handbook**. [Online]. Available : [http://www.freebsd.org/doc/en\\_US.ISO8859-1/books/handbook/](http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/)
- The Object Management Group, Inc., “OMG Unified Modeling Language Specification.” OMG-UML Manual Version 1.4, September 2001.



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## ภาคผนวก ก

# การติดตั้งโปรแกรมที่เกี่ยวข้อง

ขั้นตอนการติดตั้งระบบต่าง ๆ ที่เกี่ยวข้องกับระบบจัดการบริการระยะไกลผ่านเว็บนั้นส่วนใหญ่จะทำการติดตั้งผ่าน Ports สะดวกในการติดตั้งและมีความยืดหยุ่นมากกว่า โดย Ports จะทำการดาวน์โหลดโปรแกรมต่าง ๆ ที่มีสัมพันธ์กันมาติดตั้งให้โดยอัตโนมัติ ซึ่งโปรแกรมที่ต้องจะติดตั้งคือ Apache2.2, php5 และ MySQL Server ส่วนที่เหลือจะเป็นโปรแกรมที่สัมพันธ์กับโปรแกรมทั้งหมดนี้ Ports จะดาวน์โหลดโปรแกรมที่เหลือมาติดตั้งให้โดยอัตโนมัติ

### การติดตั้ง Apache 2.2 ผ่าน Ports

ไปยังไดเรกทอรีต่อไปนี้ `/usr/ports/www/apache22` แล้วพิมพ์คำสั่งดังตัวอย่าง

```
# cd /usr/ports/www/apache22
?WITH_LDAP_MODULES=yes\
?WITH_MYSQL=yes\
?WITH_SSL_MODULES=yes\
?WITH_THREADS=yes\
?install && make clean
```

ระบบจะทำการติดตั้ง Apache 2.2 จนเสร็จสิ้น

จากนั้นทำการแก้ไขไฟล์ `httpd.conf` ในไดเรกทอรี `/usr/local/etc/apache2/httpd.conf`

ดังต่อไปนี้

```
AddHandler cgi-script .cgi .pl
```

```
DocumentRoot "/usr/local/www/data"
```

โดย `"/usr/local/www/data"` คือไดเรกทอรีที่ติดตั้งระบบ หรืออาจจะติดตั้งไว้ใน User

Directory แทนก็ได้ โดยอาจจะสร้างไดเรกทอรี `public_html` ไว้ในโฮมไดเรกทอรีของผู้ใช้ และทำการติดตั้งโปรแกรมไว้ในไดเรกทอรีนี้

เมื่อติดตั้งโปรแกรมเสร็จแล้วทำการสั่งให้ Apache เริ่มทำงานด้วยคำสั่ง

```
# /usr/local/etc/rc.d/apache start
```

เพื่อให้ Apache 2.2 รันทุกครั้งที่เปิดเครื่องให้ทำการเพิ่มคำสั่ง `apache22_enable="YES"` ลง

ในไฟล์ `rc.conf` ในไดเรกทอรี `/etc/rc.conf`

### การติดตั้ง Php5 จาก Ports

ทำตามขั้นตอนดังต่อไปนี้

```
# cd /usr/ports/lang/php5
```

```
# make config
```

ทำการเลือกค่าออฟชั่นต่างๆตามที่ต้องการ จากนั้นทำการติดตั้งโดยคำสั่งต่อไปนี้

```
#make install clean
```

เมื่อติดตั้งเสร็จแล้วทำการแก้ไขไฟล์ php.ini ตามขั้นตอนดังต่อไปนี้

```
# cp /usr/local/etc/php.ini-recommended /usr/local/etc/php.ini
```

```
# vi /usr/local/etc/php.ini
```

ทำการแก้ไขข้อมูลดังนี้

```
default_charset = "tis-620"
```

```
upload_tmp_dir = "/tmp/uptmp"
```

```
session.save_path = "/tmp/sesstmp"
```

จากนั้นทำการรีสตาร์ท Apache ด้วยคำสั่งดังต่อไปนี้

```
# /usr/local/etc/rc.d/apache22.sh restart
```

### การติดตั้ง Extensions ต่างๆของ PHP5

ทำตามขั้นตอนดังต่อไปนี้

```
# cd /usr/ports/lang/php5-extensions
```

```
# make config
```

เลือก extention ต่างๆตามที่ต้องการ

```
# make install clean
```

จากนั้นทำการรีสตาร์ท Apache ด้วยคำสั่งดังต่อไปนี้

```
# /usr/local/etc/rc.d/apache22.sh restart
```

ทำการทดสอบภาษา php โดยการสร้างไฟล์ info.php ขึ้นมาเก็บไว้

```
ที่ /usr/local/www/data/
```

```
#vi /usr/local/www/data/info.php
```

โดยมีข้อมูลดังนี้

```
<?php
```

```
phpinfo();
```

```
?>
```

จากนั้นก็ทำการเปิดเว็บเบราว์เซอร์เรียกไปที่ <http://server/info.php> โดย server เป็นหมายเลขไอพี หรือชื่อของเซิร์ฟเวอร์ที่ติดตั้ง Apache อยู่ หากการติดตั้งถูกต้อง เว็บเบราว์เซอร์จะแสดงข้อมูลเกี่ยวกับเวอร์ชันของ PHP และข้อมูลต่างๆ แต่หากการติดตั้งไม่ถูกต้องเว็บเบราว์เซอร์จะแสดงผลออกมาเป็นชอร์ตสโคดเช่นเดิม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## การติดตั้งโปรแกรม MySQL Server 5 จาก Ports

ทำตามขั้นตอนดังต่อไปนี้

```
# cd /usr/ports/databases/mysql50-server
```

```
# make \
```

```
? WITH_CHARSET=tis620 \
```

```
? WITH_XCHARSET=all \
```

```
? WITH_COLLATION=tis620_thai_ci \
```

```
? make install with_db_dir=/usr/local/db-mysql && make clean
```

โดยที่ /usr/local/db-mysql เป็นไดเรกทอรีที่ต้องการติดตั้งฐานข้อมูล หากไม่มีการกำหนดฐานข้อมูลจะถูกติดตั้งที่ /var/db/mysql ซึ่งโดยปกติจะมีพื้นที่น้อยเกินไป หรืออาจเข้าไปแก้ไขไฟล์ Makefile ในส่วน db\_dir แทน จากนั้น Ports ก็จะทำการตรวจสอบว่าโปรแกรมที่เกี่ยวข้องกับ mysql323-server ติดตั้งในระบบหรือยัง ถ้ายังไม่ได้ติดตั้งจะไปทำการดาวน์โหลดโปรแกรมเหล่านั้นมาติดตั้งให้โดยอัตโนมัติ หากไม่มีข้อผิดพลาดแจ้งขึ้นมาในระหว่างการทำงานแสดงว่าโปรแกรม MySQL ได้ถูกติดตั้งและสามารถใช้งานได้

การปรับแต่งไฟล์ my.cnf

ทำตามขั้นตอนดังต่อไปนี้

```
# cp /usr/local/share/mysql/my-medium.cnf /etc/my.cnf
```

```
# chown root:sys /etc/my.cnf
```

```
# chmod 644 /etc/my.cnf
```

```
# rehash
```

จากนั้นก็ทำการสั่งให้ mysql server เริ่มทำงานครับ

```
#!/usr/local/etc/rc.d/mysql.server start
```

จากนั้นเพิ่มผู้ใช้งาน ในที่นี้จะสร้างผู้ใช้งานที่ชื่อ root

```
#mysqladmin -u root password '*****'
```

เพื่อให้ MySQL ทำงานทุกครั้งที่เปิดเครื่องทำการเพิ่มข้อมูล mysql\_enable="YES" ลงไป

ในไฟล์ /etc/rc.conf

## ภาคผนวก ข

# การติดตั้งระบบจัดการบริการระยะไกลผ่านเว็บ

เพื่อให้การติดตั้งทำได้ง่ายและสะดวก ผู้พัฒนาจึงได้ทำการสร้างสคริปต์ขึ้นมาเพื่อลดขั้นตอนในการติดตั้ง โดยเมื่อทำการส่งรันสคริปต์ดังกล่าว สคริปต์จะทำการขยายตัวโปรแกรมที่บีบอัดไว้ สร้างไคเร็กทอรีที่จำเป็น และสร้างฐานข้อมูลที่จำเป็นต่อระบบโดยอัตโนมัติ

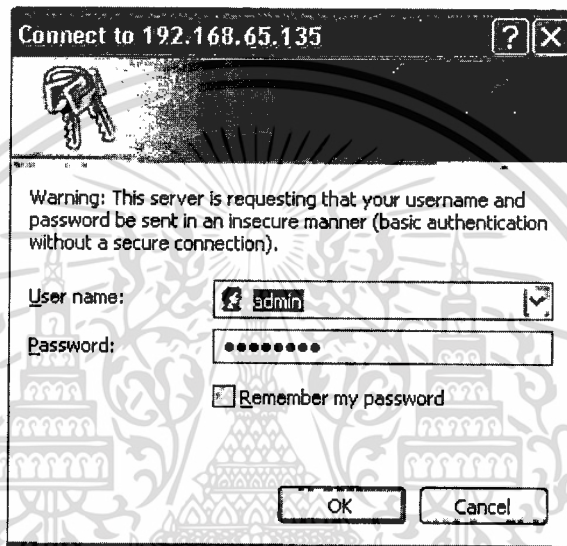
ขั้นตอนในการติดตั้งระบบจัดการบริการระยะไกลผ่านเว็บ

- นำไฟล์ของ โปรแกรมไปเก็บไว้ในเครื่องที่ทำหน้าที่เป็นเครื่องตัวกลาง ซึ่งมี 2 ไฟล์คือ
  1. wrsm.tar.gz ซึ่งเป็นตัวโปรแกรมที่ถูกบีบอัดไว้
  2. install.sh ซึ่งเป็นสคริปต์ที่ทำหน้าที่ติดตั้งระบบโดยอัตโนมัติ
- รันไฟล์ install.sh โดยคำสั่งต่อไปนี้ `#!/install.sh`
- ระบบแสดงผลการทำงาน เมื่อสิ้นก็จะสามารถใช้งานระบบได้ทันที
- ทดสอบระบบโดยใช้เว็บเบราว์เซอร์เรียกดังนี้ <http://192.168.65.135/WRSM/index.php>
- หากเว็บเบราว์เซอร์แสดงผลเว็บเพจได้ แสดงว่าการติดตั้งเสร็จสมบูรณ์
- ทดสอบฟังก์ชันการทำงานของระบบตามที่ต้องการ

## ภาคผนวก ค

# คู่มือการใช้งานระบบจัดการบริการระยะไกลผ่านเว็บ

1. เรียกการใช้งานโปรแกรมให้เรียกใช้งาน โดยพิมพ์ url โปรแกรม ดังนี้  
“http://local\_ip/index.php” โดยค่า local\_ip เป็นค่าของ ip address ของเซิร์ฟเวอร์ ระบบจะแสดงผลการทำงานดังรูปที่ 1
2. ทำการล็อกอินเข้าสู่ระบบดังรูป



รูปที่ ค.1 การล็อกอินเข้าสู่ระบบ

3. ระบบจะมีฟังก์ชันการทำงานดังต่อไปนี้
  1. การกำหนดค่าให้ระบบ (Information Management)
  2. การจัดการกับไฟล์คอนฟิกูเรชัน (Configuration File Management)
  3. การจัดการเครื่องให้บริการปลายทางและบริการที่ติดตั้งในเครื่องนั้นๆ (Machine and Service Management)
  4. การส่งไฟล์คอนฟิกูเรชันไปยังเครื่องให้บริการปลายทางตามบริการที่เครื่องนั้นมี (Configuration File Sending)
  5. การสำรองไฟล์ระบบของเครื่องให้บริการปลายทาง (Backup)
  6. การกู้คืนเครื่องให้บริการปลายทาง (Recovery)

### การกำหนดค่าให้ระบบ (Information Management)

ผู้ดูแลระบบสามารถใช้งานฟังก์ชันนี้ด้วยการใช้งานในส่วนของ Global Configuration แล้วเลือก Information Management ระบบจะแสดงดังรูปที่ ค.2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

**MENU**

- Global Configuration
  - Information Management
  - Config File Management
  - User Management
- Remote Management
  - Machine and Service
  - Configuration file sending
- Backup and Recovery
  - Backup
  - Backup Schedule
  - Recovery

**SUPPORT**

- Help

**Information Management**

Please select method:

**>>Remote Machine**

| Machine id | Machine Ip  | Machine name |                |
|------------|-------------|--------------|----------------|
| 1030       | 192.168.0.1 | Proxy Server | <edit>   <del> |
| 1039       | 192.168.1.1 | Proxy Server | <edit>   <del> |

**Add new machine**

Machine IP:

Machine Name:

Fingerprint:

\*Insert fingerprint of remote machine from "/>

Add to Database:

### รูปที่ ค.2 การทำงานในส่วนของการกำหนดค่าต่างๆทำให้ระบบ

ผู้ดูแลระบบสามารถทำการเพิ่มหมายเลขไอพี ชื่อและ Fingerprint ซึ่งได้จากไฟล์ /etc/ssh/ssh\_host\_dsa\_key.pub ของเครื่องให้บริการปลายทางที่อยู่ภายใต้การควบคุม จากนั้นกด add ดังรูปที่ ค.3

**Add new machine**

Machine IP:

Machine Name:

Fingerprint:

\*Insert fingerprint of remote machine from  
"/>

Add to Database:

### รูปที่ ค.3 การทำงานในส่วนของการเพิ่มเครื่องให้บริการให้กับระบบ

ผู้ดูแลระบบสามารถเพิ่มบริการทั้งหมดที่มีได้ โดยเลือกเมนู add new service ดังรูปที่ ค.4

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

**Information Management**

Please select method:

>>Remote Machine

| Machine_id | Machine_ip  | Machine_name |                |
|------------|-------------|--------------|----------------|
| 1030       | 192.168.0.1 | Proxy Server | <edit>   <del> |
| 1040       | 192.168.1.1 | Web Server   | <edit>   <del> |
| 1041       | 192.168.3.1 | firewall     | <edit>   <del> |

**Add new machine**

Machine IP:

Machine Name:

รูปที่ ค.4 การทำงานในส่วนของการเพิ่มบริการต่างๆค่าให้กับระบบ

ผู้ดูแลระบบสามารถเลือกได้ว่าจะเพิ่มบริการแบบใดเข้าไปซึ่งมี 2 แบบ คือบริการที่ผู้ดูแลระบบติดตั้งเองเพื่อให้เครื่องดังกล่าวทำหน้าที่เป็นเครื่องให้บริการ และบริการที่มีอยู่แล้วในระบบปฏิบัติการดังรูปที่ ค.5

**Information Management**

Please select method:

>>Application Service

| Service_id | Service_name | Type of service:                        |       |
|------------|--------------|-----------------------------------------|-------|
| 2001       | squid        | <input type="text" value="--select--"/> |       |
| 2002       | apache22     | <input type="text" value="--select--"/> | <del> |
| 2003       | mysql-server | <input type="text" value="--select--"/> | <del> |
| 2006       | mtrg         | <input type="text" value="--select--"/> | <del> |

**Add new service**

Service name:

รูปที่ ค.5 การทำงานในส่วนของการเลือกประเภทของบริการให้กับระบบ

ผู้ดูแลระบบสามารถทำการเพิ่มบริการ โดยการพิมพ์ชื่อบริการ จากนั้นกด add ดังรูปที่ ค.6

**Add new service**

Service name:

รูปที่ ค.6 การทำงานในส่วนของการเพิ่มบริการต่างๆค่าให้กับระบบ

จากรูปที่ ค.7 เป็นการกำหนดว่าเครื่องให้บริการใดมีบริการอะไรติดตั้งอยู่บ้าง โดยการเลือก

เมนู add services to machine

เอกสารนี้เป็นเอกสารที่สงวนลิขสิทธิ์สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

**Information Management**

Please select method:

>>Application Service  Type of service:

| Service_id | Service_name |       |
|------------|--------------|-------|
| 2001       | squid        | <del> |
| 2002       | apache22     | <del> |
| 2003       | mysql-server | <del> |
| 2006       | mtrg         | <del> |
| 2033       | PF           | <del> |

**Add new service**

Service name:

รูปที่ ค.7 เมนูในการเข้าสู่ส่วนของการกำหนดบริการให้แก่เครื่องให้บริการ

ผู้ดูแลระบบทำการเลือกเครื่องให้บริการที่ต้องการดังรูปที่ ค.8

**Information Management**

Please select method:

>>Services and Remote machine

| Service_id | Service_name |             |
|------------|--------------|-------------|
|            |              | 192.168.0.1 |
|            |              | 192.168.1.1 |
|            |              | 192.168.0.5 |
|            |              | 192.168.2.2 |
|            |              | 192.168.3.1 |

Please select machine first.

**Add services to this remote machine**

Service name:

รูปที่ ค.8 การทำงานในส่วนของการกำหนดบริการให้แก่เครื่องให้บริการ

เมื่อผู้ดูแลระบบเลือกเครื่องให้บริการที่ต้องการแล้วระบบจะแสดงบริการที่เครื่องให้บริการนั้นมีอยู่ ซึ่งผู้ดูแลระบบสามารถเพิ่มได้โดยเลือกจาก select box แล้วจึงกด add ดังรูปที่

ค.9

**Information Management**

Please select method:

>> Services and Remote machine select machine

| Service_id | Service_name |
|------------|--------------|
| 2001       | squid <del>  |

Add services to this remote machine

Service name:

- select--
- squid
- apache22
- mysql-server
- mtrg
- PF

รูปที่ ค.9 การทำงานในส่วนของการกำหนดบริการให้แก่เครื่องให้บริการ (ต่อ)

ในการกำหนดไฟล์คอนฟิกูเรชันให้กับบริการใดๆทำได้โดยการเลือกเมนู add config files to service ดังรูปที่ ค.10

**Information Management**

Please select method:

>> Services and Remote machine select machine

| Service_id | Service_name |
|------------|--------------|
| 2001       | squid <del>  |

Add services to this remote machine

Service name:

- select--
- add new machine
- add new service
- add services to machine
- add config files to service

รูปที่ ค.10 เมนูในการเข้าสู่ส่วนของการกำหนดไฟล์คอนฟิกูเรชันให้กับบริการ

## ผู้ดูแลระบบทำการเลือกบริการที่ต้องการดังรูปที่ ค.11

**Information Management**

Please select method:

>>Configuration files in Service select service

| ConfigFile_id | ConfigFile_name |
|---------------|-----------------|
|               | squid           |
|               | apache22        |
|               | mysql-server    |
|               | mtrg            |
|               | PF              |

Please select service first

Add configuration files to this service

configuration file name:   >>manage files

ที่ ค.11 การทำงานในส่วนของการกำหนดไฟล์คอนฟิกูเรชันให้แก่บริการ

เมื่อผู้ดูแลระบบเลือกบริการที่ต้องการแล้วระบบจะแสดงไฟล์คอนฟิกูเรชันที่บริการนั้นมีอยู่ ซึ่งผู้ดูแลระบบสามารถเพิ่มได้โดยเลือกจาก select box แล้วจึงกด add ดังรูปที่ ค.12

**Information Management**

Please select method:

>>Configuration files in Service select service

| ConfigFile_id | ConfigFile_name |       |
|---------------|-----------------|-------|
| 3002          | httpd.conf      | <del> |
| 3003          | php.ini         | <del> |
| 3004          | php.conf        | <del> |

Add configuration files to this service

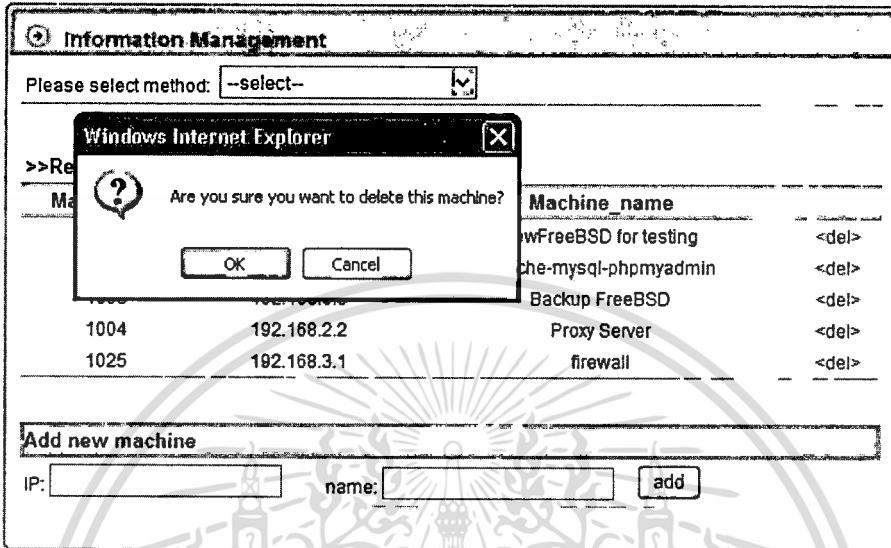
configuration file name:   >>manage files

- select--
- php.ini
- php.conf
- squid.conf
- httpd.conf
- rc.conf
- inetd.conf
- test2.txt

ที่ ค.12 การทำงานในส่วนของการกำหนดไฟล์คอนฟิกูเรชันให้แก่บริการ (ต่อ)

ซึ่งไฟล์คอนฟิกูเรชันที่ปรากฏใน select box นั้นคือไฟล์ที่ผู้ดูแลระบบสร้างขึ้นจากฟังก์ชันการจัดการกับไฟล์คอนฟิกูเรชัน ซึ่งจะกล่าวถึงในหัวข้อต่อไป

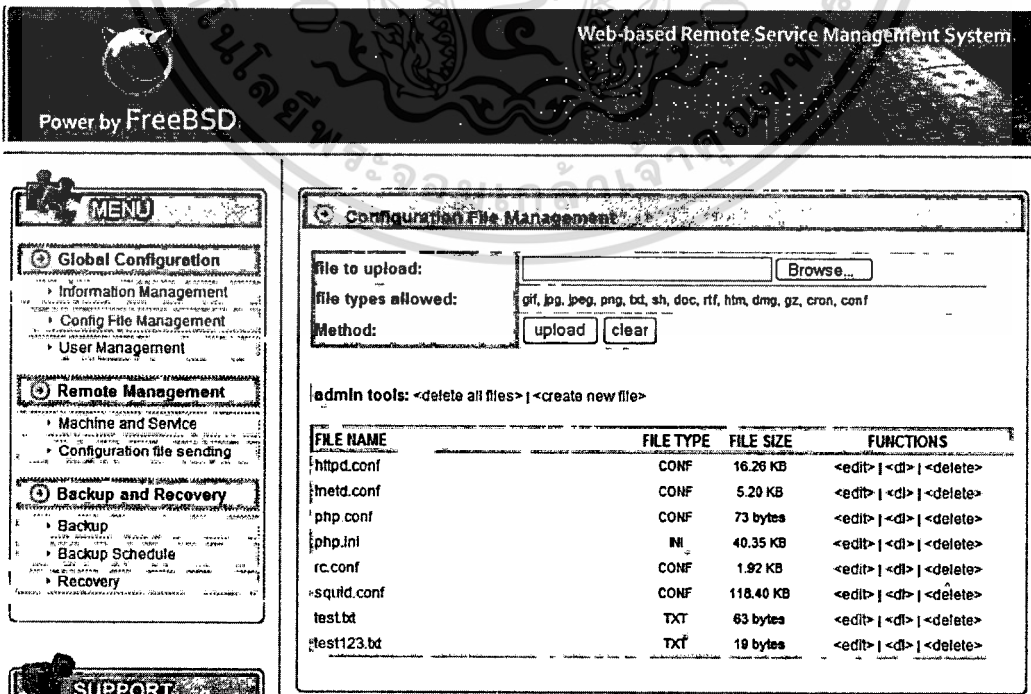
ข้อมูลทั้งหมดที่ผู้ดูแลระบบกำหนดสามารถลบทิ้งได้โดยการเลือกที่ <del> โดยระบบจะแจ้งเตือนให้ผู้ดูแลระบบทำการยืนยันการทำงานก่อนทุกครั้งดังรูปที่ ค.13



รูปที่ ค.13 การทำงานในส่วนของการลบข้อมูล

**การจัดการไฟล์คอนฟิกูเรชัน (Configuration File Management)**

ผู้ดูแลระบบสามารถใช้งานฟังก์ชันนี้ด้วยการใช้งานในส่วนของ Global Configuration แล้วเลือก config file Management ระบบจะแสดงดังรูปที่ ค.14



รูปที่ ค.14 การทำงานในส่วนของการจัดการไฟล์คอนฟิกูเรชัน

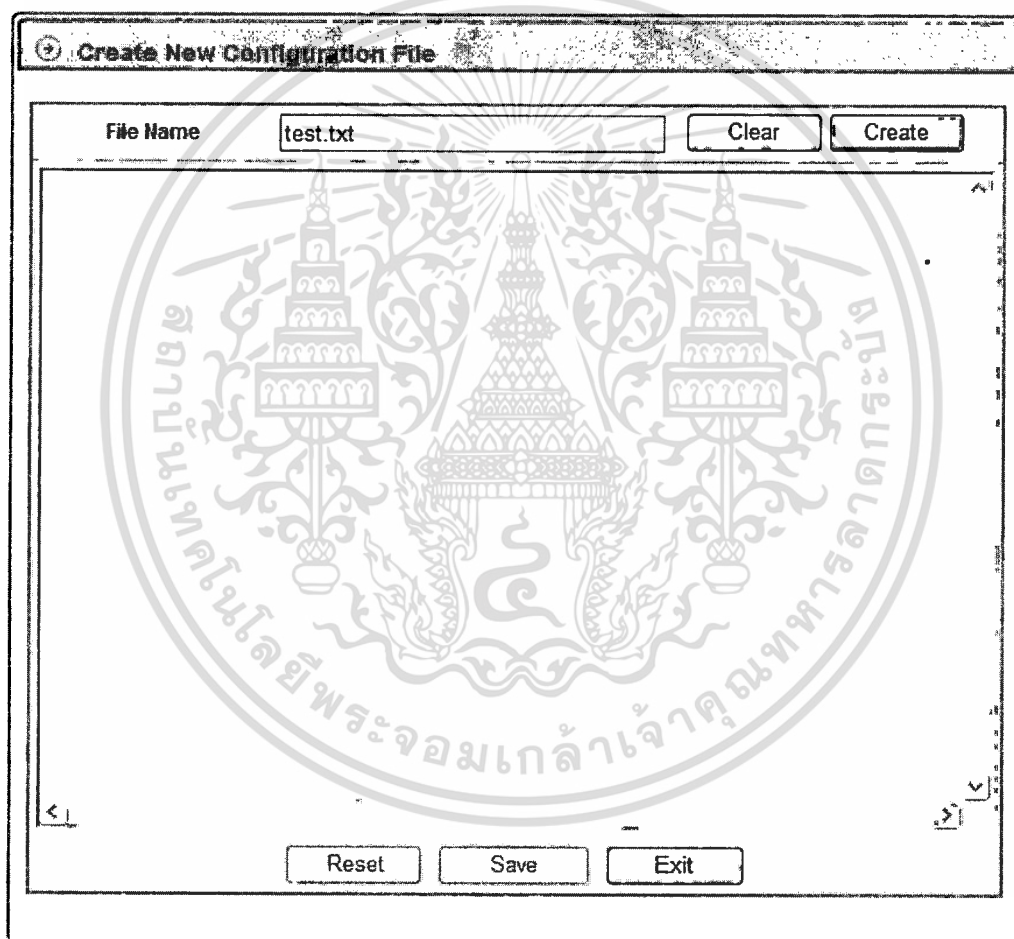
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น มิอนุญาตให้เผยแพร่ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ผู้ดูแลระบบสามารถสร้างไฟล์คอนฟิกูเรชันขึ้นมาใหม่ได้ โดยเลือกที่ <create new file> ระบบจะทำการเปิด text editor ขึ้นมา ให้ผู้ใช้ทำการกำหนดชื่อไฟล์ที่ต้องการ แล้วจึงกด Create ดังรูปที่ ค.15 และ รูปที่ ค.16

**admin tools:** <delete all files> | <create new file>

| FILE NAME  | FILE TYPE | FILE SIZE | FUNCTIONS                |
|------------|-----------|-----------|--------------------------|
| httpd.conf | CONF      | 16.26 KB  | <edit>   <dl>   <delete> |
| inetd.conf | CONF      | 5.20 KB   | <edit>   <dl>   <delete> |

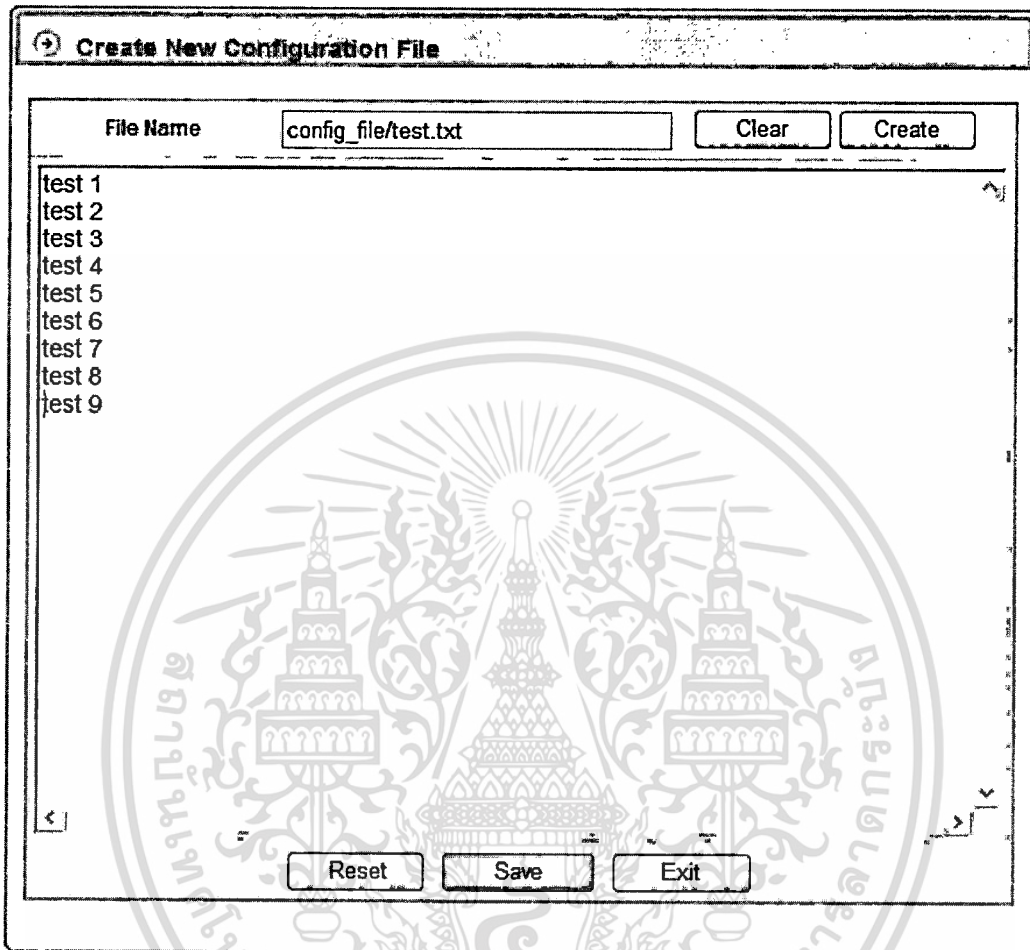
รูปที่ ค.15 ขั้นตอนการสร้างไฟล์คอนฟิกูเรชันขึ้นมาใหม่



รูปที่ ค.16 ขั้นตอนการสร้างไฟล์คอนฟิกูเรชันขึ้นมาใหม่

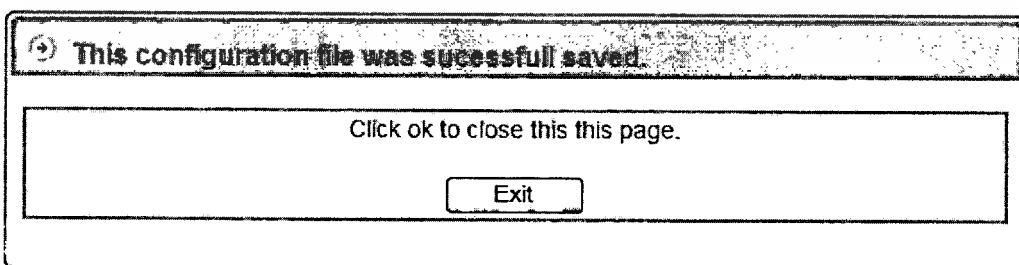
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เมื่อระบบสร้างไฟล์เสร็จแล้วผู้ดูแลระบบสามารถกำหนดค่าคอนฟิกูเรชันได้ตามต้องการ  
เมื่อกำหนดเสร็จแล้ว จึงกดปุ่ม Save เพื่อทำการบันทึกไฟล์ดังกล่าว



รูปที่ ค.17 การทำงานในส่วนของการกำหนดค่าคอนฟิกูเรชันให้กับไฟล์ที่สร้างขึ้น

หากไม่มีข้อผิดพลาดระบบจะแสดงข้อความยืนยันดังรูป ที่ ค.18

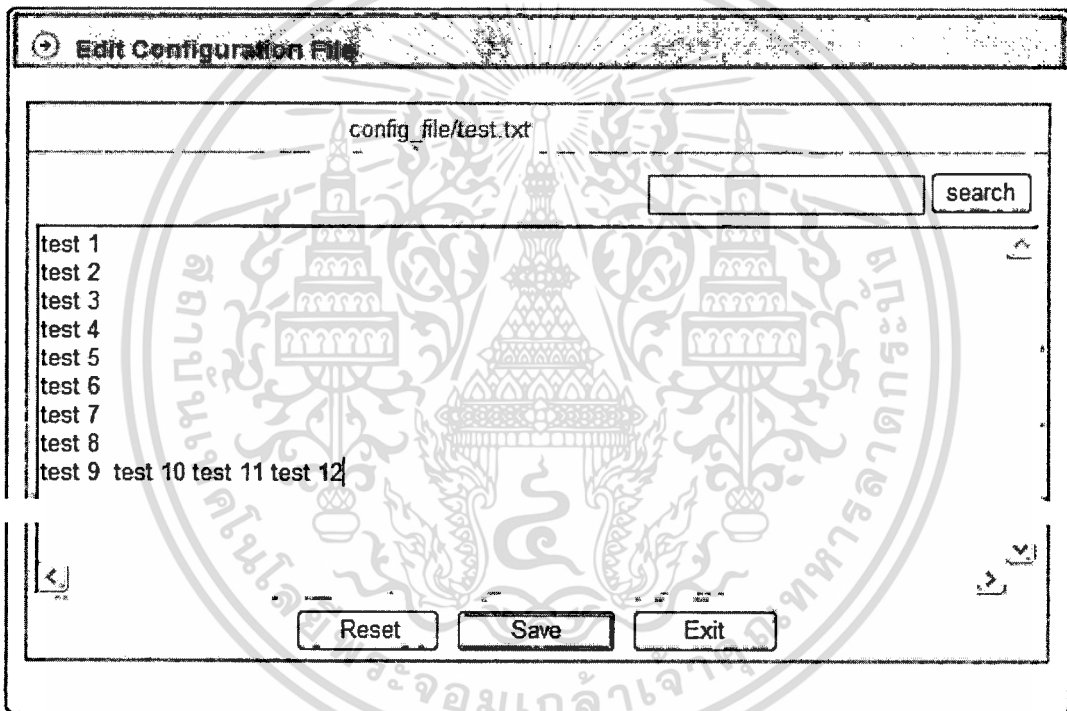


รูปที่ ค.18 ข้อความยืนยันความถูกต้องจากระบบ

ผู้ดูแลระบบสามารถเปิดไฟล์ที่สร้างไว้แล้วขึ้นมาแก้ไขได้โดยเลือกที่ <edit> ดังรูปที่ ค.19 และรูปที่ ค.20 โดยระบบจะเปิดไฟล์ดังกล่าวขึ้นมา เมื่อผู้ดูแลระบบทำการแก้ไขแล้วให้กด Save หากไม่มีข้อผิดพลาด ระบบแสดงข้อความยืนยัน ซึ่งใช้กลไกเดียวกันกับการสร้างไฟล์ขึ้นมาใหม่  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

| FILE NAME  | FILE TYPE | FILE SIZE | FUNCTIONS                |
|------------|-----------|-----------|--------------------------|
| httpd.conf | CONF      | 16.26 KB  | <edit>   <dl>   <delete> |
| inetd.conf | CONF      | 5.20 KB   | <edit>   <dl>   <delete> |
| php.conf   | CONF      | 73 bytes  | <edit>   <dl>   <delete> |
| php.ini    | INI       | 40.35 KB  | <edit>   <dl>   <delete> |
| rc.conf    | CONF      | 1.92 KB   | <edit>   <dl>   <delete> |
| squid.conf | CONF      | 118.34 KB | <edit>   <dl>   <delete> |
| test.txt   | TXT       | 63 bytes  | <edit>   <dl>   <delete> |
| test2.txt  | TXT       | 41 bytes  | <edit>   <dl>   <delete> |

รูปที่ ค.19 ขั้นตอนการแก้ไขไฟล์ที่สร้างไว้แล้ว 1

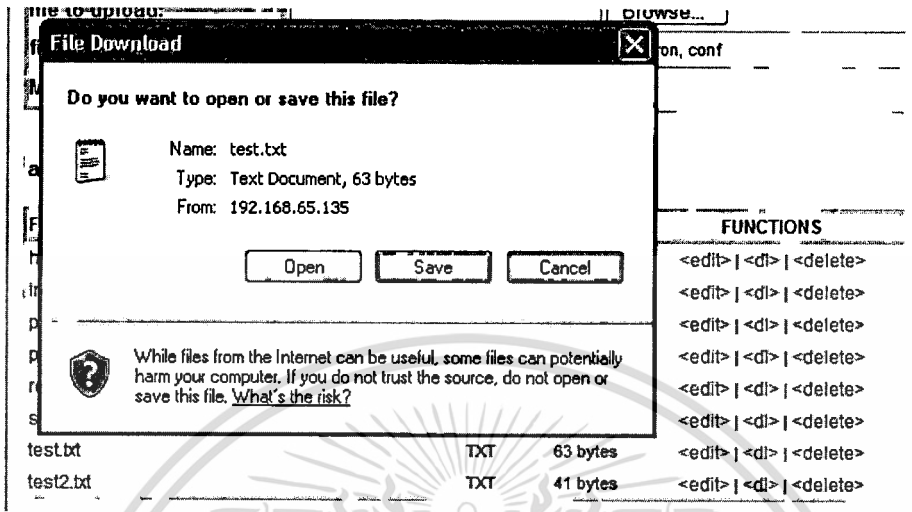


รูปที่ ค.20 ขั้นตอนการแก้ไขไฟล์ที่สร้างไว้แล้ว 2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

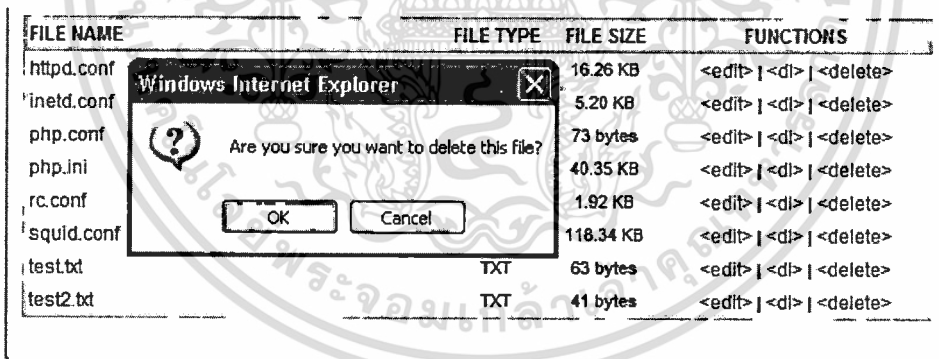
ผู้ดูแลระบบทำการดาวน์โหลดไฟล์คอนฟิกูเรชันมาเก็บไว้ได้ โดยเลือกที่ <dl> ดังรูปที่

ก.21



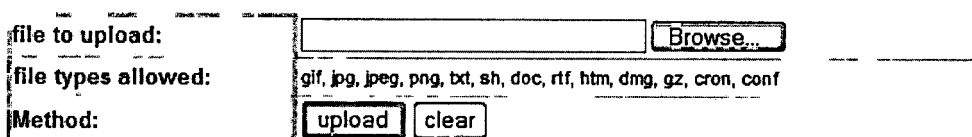
รูปที่ ก.21 ขั้นตอนการดาวน์โหลดไฟล์คอนฟิกูเรชัน

ผู้ดูแลระบบกำหนดสามารถลบไฟล์คอนฟิกูเรชันทิ้งได้โดยการเลือกที่ <delete> ซึ่งระบบจะแจ้งเตือนให้ผู้ดูแลระบบทำการยืนยันการทำงานก่อนทุกครั้งดังรูปที่ ก.22



รูปที่ ก.22 ขั้นตอนการลบไฟล์คอนฟิกูเรชัน

ระบบนี้สามารถรองรับการอัปโหลดไฟล์จากเครื่องส่วนตัวได้โดยกดที่ Browse เพื่อเลือกไฟล์ และกดที่ปุ่ม upload ดังรูปที่ ก.23



รูปที่ ก.23 ขั้นตอนการอัปโหลดไฟล์ไฟล์คอนฟิกูเรชัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## การจัดการเครื่องให้บริการปลายทางและบริการที่ติดตั้งในเครื่องนั้นๆ (Machine and Service Management)

ผู้ดูแลระบบสามารถใช้งานฟังก์ชันนี้ด้วยการใช้งานในส่วนของ Remote Management แล้วเลือก Machine and Service ซึ่งระบบจะแสดงเครื่องให้บริการปลายทางทั้งหมดที่ผู้ดูแลระบบทำการบันทึกไว้ ดังรูปที่ ค.24

| Machine_id | Machine_ip  | Machine_name |
|------------|-------------|--------------|
| 1030       | 192.168.0.1 | Proxy Server |
| 1040       | 192.168.1.1 | Web Server   |
| 1041       | 192.168.3.1 | firewall     |

รูปที่ ค.24 การทำงานในส่วนของการจัดการเครื่องให้บริการและบริการต่างๆ

ผู้ดูแลระบบทำการเลือกเครื่องให้บริการปลายทางที่ต้องการจัดการ จากนั้นเลือกชนิดของบริการที่ติดตั้งบนเครื่องนั้นๆ ซึ่งมี 2 แบบคือ บริการที่ผู้ดูแลระบบติดตั้งเอง และบริการที่มีอยู่แล้วในระบบปฏิบัติการ ดังรูปที่ ค.25

รูปที่ ค.25 ชนิดของบริการต่างๆ

เมื่อเลือกชนิดของบริการแล้วระบบจะแสดงดังรูปที่ ค.26

**Service Management**

Machine IP: 192.168.0.1  
Machine Name : newFreeBSD for testing

>>All services which are installed on this machines

| Machine_ip  | Machine_name           | service_name |
|-------------|------------------------|--------------|
| 192.168.0.1 | newFreeBSD for testing | squid        |

Please select service you want to manage.

| Service                                   | Method                    |
|-------------------------------------------|---------------------------|
| squid <input checked="" type="checkbox"/> | status start stop restart |

output: squid is running as pid 1112 1114.

รูปที่ ค.26 การทำงานในส่วนของการจัดการบริการ

ในส่วนนี้ระบบจะแสดงรายละเอียดของเครื่องให้บริการ และบริการที่เครื่องดังกล่าวติดตั้งอยู่ ผู้ดูแลระบบสามารถทำการจัดการกับบริการเหล่านี้ได้ โดยการกดปุ่ม status, start, stop หรือ restart เพื่อควบคุมบริการนั้นๆตามความต้องการ ตัวอย่างเช่นเมื่อผู้ดูแลระบบกดปุ่ม stop บริการที่ชื่อว่า squid จะหยุดทำงานดังรูปที่ ค.27

>>All services which are installed on this machines

| Machine_ip  | Machine_name           | service_name |
|-------------|------------------------|--------------|
| 192.168.0.1 | newFreeBSD for testing | squid        |

Please select service you want to manage.

| Service                                   | Method                    |
|-------------------------------------------|---------------------------|
| squid <input checked="" type="checkbox"/> | status start stop restart |

output: squid is not running.

รูปที่ ค.27 ผลการทำงานเมื่อผู้ดูแลระบบกดปุ่ม stop

นอกจากการจัดการบริการที่ติดตั้งอยู่บนเครื่องให้บริการปลายทางแล้วระบบยังสามารถ ส่งคำสั่งไปยังเครื่องให้บริการปลายทางเพื่อให้เริ่มการทำงานใหม่ (restart machine) หรือรีสตาร์ทเน็ตเวิร์คอินเตอร์เฟซได้ โดยการเลือกที่ Restart Machine หรือ Restart Network Interface ดังรูปที่ ค.28 ซึ่งเมื่อหากไม่มีข้อผิดพลาดระบบจะแสดงข้อความยืนยันให้ทราบ

รูปที่ ค.28 ฟังก์ชันการทำงานที่ระบบสามารถทำได้

การส่งไฟล์คอนฟิกูเรชันไปยังเครื่องให้บริการปลายทาง (Configuration File Sending)

ผู้ดูแลระบบสามารถใช้งานฟังก์ชันนี้ด้วยการใช้งานในส่วนของ Remote Management แล้วเลือก Configuration File Sending ซึ่งระบบจะแสดง ดังรูปที่ ค.29

รูปที่ ค.29 การทำงานในส่วนของการส่งไฟล์คอนฟิกูเรชันไปยังเครื่องให้บริการปลายทาง

ผู้ดูแลระบบเลือกเครื่องให้บริการปลายทางที่ต้องการ จากนั้นระบบจะแสดงบริการทั้งหมดที่เครื่องให้บริการมี ดังรูปที่ ค.30

**Configuration file sending**

Machine IP: 192.168.1.1

Service Name: apach22 <= select service name that you want.

| Service_name | ConfigFile_name |
|--------------|-----------------|
| apach22      |                 |
| mysql-server |                 |
| -other-      |                 |

---

**Please select configuration file you want to manage.**

Configuration File : ▼

Edit Configuration File: Edit

Send Configuration File: Send

รูปที่ ค.30 ขั้นตอนการทำงานในการส่งไฟล์คอนฟิกูเรชันไปยังปลายทาง 1

ระบบจะแสดงไฟล์คอนฟิกูเรชันทั้งหมดที่บริการนั้นมี ผู้ดูแลระบบทำการเลือกไฟล์ที่ต้องการ ดังรูปที่ ค.31

Machine IP: 192.168.1.1

Service Name: apach22

| Service_name | ConfigFile_name |
|--------------|-----------------|
| apach22      | httpd.conf      |
| apach22      | php.ini         |
| apach22      | php.conf        |

---

**Please select configuration file you want to manage.**

Configuration File : ▼ <= select configuration file that you want.

Edit Configuration File: httpd.conf

Send Configuration File: php.conf

รูปที่ ค.31 ขั้นตอนการทำงานในการส่งไฟล์คอนฟิกูเรชันไปยังปลายทาง 2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เมื่อเลือกไฟล์ที่ต้องการแล้วเพื่อความยืดหยุ่นในการใช้งาน ผู้ดูแลระบบต้องทำการกำหนดตำแหน่งปลายทาง รวมถึงชื่อของไฟล์ที่จะส่งด้วย จากนั้นจึงกดปุ่ม Send ดังรูปที่ ค.32

**Please select configuration file you want to manage.**

Configuration File :  <= select configuration file that you want.

Edit Configuration File:

Send Configuration File:

Enter destination path here. (use '/', not '\ or '\\, no trailing '/')

Enter destination file name here.

รูปที่ ค.32 ขั้นตอนการทำงานในการส่งไฟล์คอนฟิกูเรชันไปยังเครื่องให้บริการปลายทาง

ก่อนทำการส่งไฟล์ ผู้ดูแลระบบสามารถตรวจสอบความถูกต้องของไฟล์ได้ โดยกดที่ปุ่ม Edit ระบบจะทำการเปิดไฟล์ดังกล่าวขึ้นมาเพื่อให้ผู้ดูแลระบบทำการแก้ไขได้ดังรูปที่ ค.33

**Edit Configuration File**

`/usr/local/www/apache22/data/test/config_file/httpd.conf`

```
#
# This is the main Apache HTTP server configuration file. It contains the
# configuration directives that give the server its instructions.
# See <URL:http://httpd.apache.org/docs/2.2> for detailed information.
# In particular, see
# <URL:http://httpd.apache.org/docs/2.2/mod/directives.html>
# for a discussion of each configuration directive

# with ServerRoot set to "/usr/local" will be interpreted by the
# server as "/usr/local/var/log/foo.log".

#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
```

รูปที่ ค.33 การตรวจสอบความถูกต้องของไฟล์คอนฟิกูเรชัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## การสำรองไฟล์ระบบของเครื่องให้บริการปลายทาง (Backup)

ผู้ดูแลระบบสามารถใช้งานฟังก์ชันนี้ด้วยการใช้งานในส่วนของ Backup and Recovery แล้วเลือก Backup ซึ่งระบบจะแสดง ดังรูปที่ ค.34

The screenshot shows the 'Web-based Remote Service Management System' interface. At the top, it says 'Power by FreeBSD'. On the left is a 'MENU' with options: Global Configuration (Information Management, Config File Management, User Management), Remote Management (Machine and Service, Configuration file sending), and Backup and Recovery (Backup, Backup Schedule, Recovery). The main area is titled 'Backup' and contains the following fields and options:

- Machine IP: 192.168.0.1
- Backup time: 12:00
- Please select backup schedule that you want.
  - Every Day: daily backup
  - Every week: day of week
  - On Demand: date / month
  - Immediately: backup file system now
- A 'backup' button is located at the bottom right of the configuration area.

รูปที่ ค.34 การทำงานในส่วนของการสำรองไฟล์ระบบ

ผู้ดูแลระบบกำหนดเวลาที่ต้องการ จากนั้นกำหนดช่วงเวลาที่ต้องการให้เครื่องให้บริการปลายทางทำการสำรองไฟล์ระบบของตัวเองช่วงไหน เช่น ทุกวัน ทุกสัปดาห์ ตามเวลาที่กำหนด หรือต้องการให้ทำการสำรองไฟล์ระบบทันที เมื่อกำหนดตารางเวลาเสร็จแล้ว กดปุ่ม backup ระบบจะทำการสร้างตารางเวลาตามที่ผู้ดูแลระบบกำหนด ซึ่งจากตัวอย่างเป็นการกำหนดให้เครื่องให้บริการปลายทางทำการสำรองไฟล์ระบบในเวลา 23.39 น. ทุกวันอาทิตย์เป็นต้น ดังรูปที่ ค.35

**Backup Schedule**

Machine IP : 192.168.0.1

Backup time : 23 : 59

Please select backup schedule that you want.

Every Day      daily backup

Every week      sunday

On Demand      date / month

Immediately      backup file system now!

backup

รูปที่ ค.35 ขั้นตอนการการสำรองไฟล์ระบบ

### การกู้คืนระบบของเครื่องให้บริการปลายทาง (Recovery)

ผู้ดูแลระบบสามารถใช้งานฟังก์ชันนี้ด้วยการใช้งานในส่วนของ Backup and Recovery แล้วเลือก Recovery ซึ่งระบบจะแสดงอิมเมจของ ไฟล์ระบบทั้งหมดที่เก็บไว้ที่เครื่องตัวกลาง ดังรูปที่ ค.36

**MENU**

- Global Configuration
  - Information Management
  - Config File Management
  - User Management
- Remote Management
  - Machine and Service
  - Configuration file sending
- Backup and Recovery
  - Backup
  - Backup Schedule
  - Recovery

**Recovery File System**

Select Machine : 192.168.0.1

>> All Image Files

| Image file name               | Size      |       |
|-------------------------------|-----------|-------|
| 192.168.0.1@23-08-2007.tar.gz | 169.93 MB | <del> |
| 192.168.0.1@27-08-2007.tar.gz | 270.50 KB | <del> |
| 192.168.1.1@03-08-2007.tar.gz | 284.42 KB | <del> |

Select image file to recovery.

Image file name: select Recovery

รูปที่ ค.36 การทำงานในส่วนของการกู้คืนระบบ

ผู้ดูแลทำการเลือกการเครื่องให้บริการปลายทาง และอิมเมจของ ไฟล์ระบบที่ต้องการ จากนั้นกดปุ่ม Recovery ระบบจะทำการส่งอิมเมจของ ไฟล์ระบบที่เลือกไว้ไปยังเครื่องให้บริการปลายทางที่เลือกไว้และทำการส่งคำสั่งให้เครื่องดังกล่าวทำการกู้คืน ไฟล์ระบบของตัวเอง โดยใช้ อิมเมจของ ไฟล์ระบบที่ได้รับ ซึ่งในส่วนนี้จะใช้เวลาานพอสมควร อย่าปิดหน้าเว็บเพื่งนี้จนกว่า ระบบจะแสดงข้อความยืนยันความถูกต้อง ดังรูปที่ ค.37 และรูปที่ ค.38

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

**Recovery File System**

Select Machine :

>>All Image Files

| Image file name               | Size      |       |
|-------------------------------|-----------|-------|
| 192.168.0.1@23-08-2007.tar.gz | 169.93 MB | <del> |
| 192.168.0.1@27-08-2007.tar.gz | 270.50 KB | <del> |
| 192.168.1.1@03-08-2007.tar.gz | 284.42 KB | <del> |

Select Image file to recovery.

Image file name:

รูปที่ ค.37 ขั้นตอนการการกู้คืนระบบ

**The recovery process was successful.**

Click ok to close this this page.

รูปที่ ค.38 ข้อความยืนยันจากระบบ

## ประวัติผู้เขียน

|                     |                                                               |
|---------------------|---------------------------------------------------------------|
| ชื่อ-สกุล           | นายพิทักษ์ วงศ์อินทร์                                         |
| วัน-เดือน-ปีเกิด    | 26 กุมภาพันธ์ พ.ศ.2524                                        |
| ที่อยู่ปัจจุบัน     | 155/1 ถ.แม่ตำสาขายใน ต.แม่ตำ อ.เมือง จ.พะเยา                  |
| อีเมลทหรอนิกส์เมล์  | bee_sodaice@hotmail.com                                       |
| ประวัติการศึกษา     | วิทยาศาสตรบัณฑิต สาขาฟิสิกส์ คณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร |
| ปีที่สำเร็จการศึกษา | 2547                                                          |
| ประวัติการทำงาน     | -                                                             |



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้