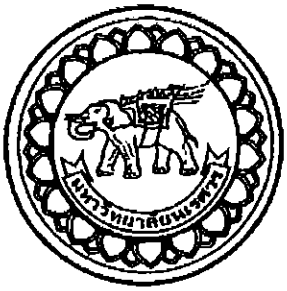


ระบบจัดการแบนด์วิดท์โดยใช้ลินุกซ์เราท์เตอร์

BANDWIDTH MANAGEMENT SYSTEM BY USING LINUX ROUTER

นายอิษณัย วงศ์สิทธิกร รหัส 49362604

นายอนุชา ประภาสนิรัติศัย รหัส 49362857

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร

ปีการศึกษา 2552

ใบรับรองโครงงานวิศวกรรม

หัวข้อโครงงาน	ระบบจัดการแบนด์วิดท์โดยใช้ Linux Router		
ผู้ดำเนินโครงงาน	**นายอิษณัย**	**วงศ์สิทธิกร**	**รหัส 49362604**
	นายอนุชา	**ประภาสนิรัติศัย**	**รหัส 49362857**
อาจารย์ที่ปรึกษา	อาจารย์ภาณุพงศ์ สอนคม		
สาขาวิชา	วิศวกรรมคอมพิวเตอร์		
ภาควิชา	วิศวกรรมไฟฟ้าและคอมพิวเตอร์		
ปีการศึกษา	2552		

.....

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร อนุมัติให้โครงงานฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์

คณะกรรมการสอบโครงงานวิศวกรรม

..... ประธานกรรมการ
(อาจารย์ภาณุพงศ์ สอนคม)

..... กรรมการ
(อาจารย์เศรษฐา ตั้งค้าวานิช)

..... กรรมการ
(ดร.สุรเดช จิตประไพกุลศาล)

หัวข้อโครงงาน	ระบบจัดการแบนด์วิดท์โดยใช้ Linux Router		
ผู้ดำเนินโครงงาน	นายอิษณัย	วงศ์สิทธิกร	รหัส 49362604
	นายอนุชา	ประภาสนิรัดิศัย	รหัส 49362857
อาจารย์ที่ปรึกษา	อาจารย์ภาณุพงศ์ สอนคม		
สาขาวิชา	วิศวกรรมคอมพิวเตอร์		
ภาควิชา	วิศวกรรมไฟฟ้าและคอมพิวเตอร์		
ปีการศึกษา	2552		

บทคัดย่อ

โครงงานนี้มีวัตถุประสงค์เพื่อศึกษาเกี่ยวกับการทำงานของซอฟต์แวร์เราท์เตอร์ที่ใช้ในการจัดการแบนด์วิดท์ ได้แก่ IPCop, NetLimiter, PFSense การศึกษาในครั้งนี้ได้ทดลองใช้งานซอฟต์แวร์เราท์เตอร์ ทั้ง 3 ซอฟต์แวร์ จากการทำงานทั้ง 2 รูปแบบ คือ Block Port และ Bandwidth Shaping โดยเปรียบเทียบกับแบบที่ไม่ได้ทำการ Block Port และ Bandwidth Shaping และ นำผลการทดลองมาวิเคราะห์เปรียบเทียบประสิทธิภาพการทำงานของแต่ละซอฟแวร์จากอัตราการดาวน์โหลด อัพโหลด เฉลี่ย และ เวลาเฉลี่ยที่ใช้ในการเข้าเว็บไซต์ โดยมีวัตถุประสงค์เพื่อแก้ปัญหาแบนด์วิดท์โดยเน้นการแก้ปัญหาแบนด์วิดท์ในสภาพแวดล้อมของหอพักเป็นหลัก เช่น ผู้จัดการหอพักไม่มีความรู้เกี่ยวกับการจัดการแบนด์วิดท์ มีปัญหาเกี่ยวกับผู้ใช้ทำการดาวน์โหลดไฟล์ชนิด P2P (Peer-to-Peer) ต้องการประหยัดค่าใช้จ่าย ต้องการกำหนดชื่อ และ รหัสผ่านของผู้ใช้ เพื่อเข้าใช้งานอินเทอร์เน็ต และ ต้องการเก็บข้อมูล Log เพื่อรองรับพ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จากผลการทดลองพบว่า ประสิทธิภาพในการทำงานของซอฟต์แวร์ 3 ซอฟต์แวร์ไม่มีความแตกต่างกันอย่างมีนัยสำคัญทางสถิติ และพบว่า NetLimiter สามารถใช้งานในรูปแบบ Bandwidth Shaping ได้ แต่ไม่สามารถใช้งานในรูปแบบ Block Port ได้

ผลที่ได้จากการทำโครงงานนี้ ทำให้ได้เรียนรู้ถึงการทำงานของซอฟต์แวร์เราท์เตอร์ และพบว่าซอฟแวร์เราท์เตอร์สามารถนำไปใช้ในการจัดการแบนด์วิดท์ได้จริง และ การนำไปช่วยในการแก้ไขในสถานการณ์ต่างๆ ตามความต้องการของผู้จัดการหอพักได้จริง

Project Title	Bandwidth Management System by using Linux Router		
Name	Mr.Isanai	Wongsittigom	ID. 49362604
	Mr.Anucha	Prapadnirattisai	ID. 49362857
Project Advisor	Mr.Panupong	Sornkhom	
Major	Computer Engineering		
Department	Electrical and Computer Engineering		
Academic Year	2552		

ABSTRACT

In this study, we aim to learn that how software router can manage bandwidth. We choose 3 software routers in our experiment, IPCop, NetLimiter , and PFSense. We run this experiment in 2 ways, port blocking and bandwidth shaping, compare with unconditional status. Study result is analyzed by comparing upload and download rate that each software router can do and average time use accessing website.

We hope that our study can help internet provider especially in organization and dormitory that have to share internet publicly. In that places, there a lot of problem such as, client secretly use peer-to-peer file transfer that can caused another clients faced bandwidth lacking, risk of violent in code of computer crime.

Our study suggests that each software router can function equally in all process of study without statistically significant and the outcome can be further applied in larger scale organization.

กิตติกรรมประกาศ

โครงงานวิศวกรรมคอมพิวเตอร์นี้สำเร็จลุล่วงได้ด้วยดี เนื่องมาจากได้รับความอนุเคราะห์จาก อาจารย์ที่ปรึกษาโครงงาน คือ อาจารย์ภาณุพงศ์ สอนคม คณะกรรมการคือ ดร.สุรเดช จิตประไพกุลศาล และ อาจารย์เศรษฐา ตั้งค้าวานิช ที่ได้เสียสละเวลาให้คำแนะนำติชมและให้ความช่วยเหลือในด้านต่างๆ

ในโอกาสนี้ทางคณะผู้จัดทำโครงงานขอขอบพระคุณทุกๆ ท่านที่มีส่วนร่วมในการทำโครงงานนี้ ตลอดจนผู้เขียน ผู้คิดค้นทฤษฎีต่างๆ ที่โครงงานฉบับนี้ได้นำความรู้ที่ได้มาศึกษาและทำการทดลองจนทำให้โครงงานสำเร็จลุลวงไปด้วยดี

นายอิษณัย วงศ์สิทธิกร

นายอนุชา ประภาสนิรัติศัย

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ **หน้า**

สารบัญรูป (ต่อ)

รูปที่ **หน้า**

สารบัญรูป (ต่อ)

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญตาราง (ต่อ)

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญ

การใช้งานระบบอินเทอร์เน็ต (Internet) ในปัจจุบันนั้น มักเกิดปัญหาเกี่ยวกับปริมาณการใช้งานเส้นทางในการส่งข้อมูล หรือ ที่เรียกว่า "แบนด์วิดท์" (Bandwidth) ในการเชื่อมต่อกับระบบอินเทอร์เน็ตมีไม่เพียงพอ ทำให้เกิดความล่าช้าในการใช้งานอินเทอร์เน็ตของผู้ใช้บริการภายในหน่วยงานหรือสถานที่ต่าง ๆ ซึ่งสาเหตุที่ทำให้แบนด์วิดท์ไม่เพียงพอต่อการใช้งานมักเกิดจากการที่ผู้ใช้หลายคนใช้งานแบนด์วิดท์มากเกินความจำเป็น เช่น การดาวน์โหลด (Download) การอัพโหลด (Upload) ไฟล์ผ่านระบบเครือข่ายแบบ P2P (Peer-to-Peer) ที่มีการรับส่งข้อมูลเป็นจำนวนมาก อยู่ตลอดเวลา จนส่งผลกระทบต่อผู้ใช้บริการคนอื่น ๆ ในระบบ

เพื่อแก้ไขปัญหาดังกล่าว จึงควรมีการควบคุมการใช้แบนด์วิดท์ของระบบ หรือ ของผู้ใช้แต่ละคน เพื่อไม่ให้มีการใช้งานที่ไม่เหมาะสม นอกจากนี้ผู้ดูแลระบบควรจะทราบข้อมูลรายงานการใช้แบนด์วิดท์ของผู้ใช้แต่ละคน เพื่อนำไปปรับปรุงนโยบายในการให้บริการได้ ซึ่งจะทำให้คุณภาพการให้บริการเครือข่ายอยู่ในระดับที่น่าพอใจกับผู้ใช้ทุกคน

แต่เนื่องจากอุปกรณ์เครือข่ายที่สามารถควบคุมการใช้งานแบนด์วิดท์นั้นมีราคาแพง ทำให้หน่วยงานเล็ก ๆ เช่น โรงเรียน หรือ หอพักต่าง ๆ ไม่สามารถซื้อมาใช้งานได้ ผู้จัดทำโครงงานจึงมีแนวคิดในการประยุกต์ใช้ซอฟต์แวร์ (Software) ในการจัดการปริมาณข้อมูลเข้าออก (Traffic) เพื่อแก้ปัญหาดังกล่าว โดยเน้นการแก้ปัญหาแบนด์วิดท์ในสภาพแวดล้อมของหอพักเป็นหลัก ซึ่งระบบอินเทอร์เน็ตในหอพักนั้น มีการใช้งานอินเทอร์เน็ตผ่านทางระบบ ADSL (Asymmetric digital subscriber line) และมีการแชร์อินเทอร์เน็ตไปยังห้องต่างๆ โดยผู้จัดทำโครงงานได้ทำการศึกษาและ ทดลองระบบเพื่อแก้ไขปัญหาด้วยค่าใช้จ่ายที่ไม่สูงมาก และ ง่ายต่อการบริหารจัดการ โดยไม่ต้องมีผู้ดูแลระบบที่มีความรู้สูงตามหอพักต่างๆ จากนั้นผู้จัดทำโครงงานจะทำการทดลองเพื่อหาระบบและการปรับแต่งที่เหมาะสมกับการแก้ปัญหาดังกล่าว เพื่อใช้เป็นข้อมูลประกอบการเลือกซอฟต์แวร์ไปประยุกต์ใช้งานจริงต่อไป

1.2 วัตถุประสงค์ของโครงงาน

1.2.1 เพื่อแก้ไขปัญหาการใช้งานแบนด์วิดท์อินเทอร์เน็ตตามหอพักได้ ซึ่งระบบที่นำมาใช้จะต้องมีคุณสมบัติดังต่อไปนี้

- สามารถบล็อกพอร์ต (Block Port) หรือ จำกัดแบนด์วิดท์ (Bandwidth Shaping) ได้
- สามารถรายงานการใช้งาน (Log) ได้
- ใช้งานง่ายและประหยัดค่าใช้จ่าย

1.2.2 เพื่อศึกษาและเปรียบเทียบคุณสมบัติของซอฟต์แวร์เราเตอร์ จำนวน 3 ซอฟต์แวร์ ได้แก่ IPCop, NetLimiter และ PFSense

1.3 ขอบข่ายของโครงงาน

1.3.1 ศึกษาซอฟต์แวร์ที่เกี่ยวกับระบบจัดการแบนด์วิดท์ ทั้ง 3 ซอฟต์แวร์ คือ IPCop, NetLimiter, PFSense และ ทำการทดลองเปรียบเทียบการทำงานของซอฟต์แวร์

1.3.2 ระบบสามารถรายงานการใช้ แบนด์วิดท์โดยจำแนกตามแอปพลิเคชั่น (Application)

1.3.3 ผู้ดูแลระบบสามารถควบคุมการใช้งานแบนด์วิดท์โดยใช้ซอฟต์แวร์ที่มีคุณสมบัติที่ตรงตามจุดประสงค์ได้ตามที่กำหนด

1.4 ขั้นตอนการดำเนินงาน

1.4.1 ศึกษาและรวบรวมข้อมูลที่เกี่ยวข้องกับหัวข้อโครงงาน

1.4.2 ศึกษาขั้นตอนการทำงานของซอฟต์แวร์ที่ใช้ในการจัดการแบนด์วิดท์

1.4.3 ทำการศึกษาและทดสอบซอฟต์แวร์ที่ใช้ในการจัดการแบนด์วิดท์

1.4.4 สรุปและวิเคราะห์ผลการทดสอบ

1.4.5 จัดทำคู่มือโครงงาน

1.5 แผนการดำเนินงาน

กิจกรรม	พ.ศ. 2552							พ.ศ. 2553	
	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.
1. ศึกษาและรวบรวมข้อมูลที่เกี่ยวข้องกับหัวข้อโครงงาน									
2. ศึกษาขั้นตอนการทำงานของซอฟต์แวร์									
3. ทำการทดลองซอฟต์แวร์									
4. สรุปและวิเคราะห์ผลการทดสอบซอฟต์แวร์									
5. จัดทำคู่มือโครงงาน									

1.6 ผลที่คาดว่าจะได้รับ

1.6.1 มีความรู้เกี่ยวกับการจัดการแบนด์วิดท์เบื้องต้น

1.6.2 สามารถนำผลไปประยุกต์ใช้ในการแก้ปัญหาอินเทอร์เน็ตตามหน่วยงาน หรือ หอพัก ได้จริง

1.6.3 สามารถเลือกซอฟต์แวร์ และ ทำการปรับตั้งค่าที่เหมาะสมกับปัญหาและสภาพแวดล้อม ได้

1.7 งบประมาณของโครงงาน

1.7.1 ค่าพิมพ์โครงงานและถ่ายเอกสาร	700	บาท
1.7.2 ค่าเข้าเล่มโครงงาน	600	บาท
1.7.3 อุปกรณ์ทางด้านคอมพิวเตอร์	400	บาท
1.7.4 อื่นๆ	300	บาท
รวมเป็นเงินทั้งสิ้น	2,000	บาท (สองพันบาทถ้วน)

หมายเหตุ ขออนุมัติถัวเฉลี่ยทุกรายการมัติถัวเฉลี่ยทุกรายการ

บทที่ 2
หลักการและทฤษฎีที่เกี่ยวข้อง

แบนด์วิดท์ (Bandwidth) หรือช่องสัญญาณ เป็นคำที่ใช้วัดความเร็วในการส่งข้อมูลของอินเทอร์เน็ต (Internet) โดยมากมักวัดความเร็วของการส่งข้อมูลเป็น bps (bit per second) ซึ่งในโครงงานนี้ทางผู้จัดทำได้ให้ความสำคัญเกี่ยวกับแนวคิดวิธีการในการจัดการแบนด์วิดท์ โดยมีวัตถุประสงค์เพื่อการควบคุมความเร็วในการส่งข้อมูล และ เพิ่มประสิทธิภาพในการทำงานบนระบบปฏิบัติการลีนุกซ์ เราเตอร์ ซึ่งทางผู้จัดทำได้ศึกษาถึงหลักการและทฤษฎีที่เกี่ยวข้องในการจัดทำโครงงาน โดยมีรายละเอียดดังนี้

2.1 หลักการและวิธีบริหารจัดการกับแบนด์วิดท์

โครงข่ายคอมพิวเตอร์เพื่อใช้งานภายในอินเทอร์เน็ต (LAN) ก็เป็นอีกช่องทางในการรับ-ส่งข้อมูลที่ใช้หลักการเกี่ยวกับแบนด์วิดท์เช่นกัน โดยทั่วไปแล้ว LAN มีความเร็วในการรับ หรือ ส่งข้อมูลด้วยความเร็วราวๆ 100 Mbps ซึ่งหมายความว่ามีช่องสัญญาณเพื่อรองรับการใช้งานเท่ากับ 100 Mbps สำหรับการถ่ายโอนข้อมูลภายในโครงข่าย แต่ถ้ากรณีความเร็วในการเชื่อมต่ออินเทอร์เน็ตที่ใช้งานอยู่นั้นมีความเร็วที่ 512/256 Kbps นั่นหมายความว่า แบนด์วิดท์สำหรับการดาวน์โหลด (Download) อยู่ที่ 512 Kbps และ แบนด์วิดท์สำหรับอัพโหลด (Upload) อยู่ที่ 256 Kbps

ในการพิจารณาการรับ-ส่งข้อมูลบนระบบบัสแบนด์วิดท์ (Bus Bandwidth) เปรียบได้กับความกว้างของเส้นทางในการส่งข้อมูลยิ่งเส้นทางในการส่งข้อมูลกว้างเท่าไรข้อมูลก็จะสามารถรับส่งได้สะดวกมากขึ้นเท่านั้น โดยที่ใช้ปริมาณจำนวนข้อมูลของเลข Single Number (0 หรือ 1) มาใช้พิจารณาข้อมูลที่รับ-ส่งบนระบบบัส โดยปริมาณข้อมูลของเลข Single Number สามารถแปรผันได้ตามเวลา ดังนั้นจึงควรพิจารณาการรับ-ส่งข้อมูลผ่านทางระบบบัสด้วย ความกว้างสูงสุดในการรับ-ส่งข้อมูลของบัส (Peak Bandwidth Bus) โดยสามารถวัดได้จากจำนวนข้อมูลที่ถูกรับ-ส่ง ระหว่างหน่วยประมวลผลกลาง (CPU) กับ หน่วยความจำ (Ram) ภายในหนึ่งคาบเวลา ซึ่งเรียกว่า ความเร็วของสัญญาณนาฬิกา

<u>ตัวอย่างการคำนวณ แบนด์วิดท์จากความเร็วของสัญญาณนาฬิกา</u>

กำหนดความเร็วของสัญญาณนาฬิการะหว่างหน่วยประมวลผลกลางและหน่วยความจำมีค่าเท่ากับ 100 เมกะเฮิรตซ์ (MHz) โดยมีการรับ-ส่งข้อมูลจำนวน 8 ไบต์ (Byte) ในแต่ละหนึ่งรอบของสัญญาณนาฬิกา สามารถคำนวณแบนด์วิดท์ได้ดังนี้

8 Byte X 100 MHz = 800 MB/s

ซึ่งตัวเลขของ แบนด์วิดท์ ที่ได้จากการคำนวณข้างต้นนั้นเป็นเพียงตัวเลขทางทฤษฎีที่บอกถึงปริมาณของข้อมูลที่เข้าสู่ หน่วยประมวลผลกลาง ในแต่ละ 1 วินาที ซึ่งในความเป็นจริง ในการรับส่งข้อมูลของแบนด์วิดท์ดังกล่าวของระบบอาจมีค่าต่ำกว่าค่าที่ได้จากการคำนวณข้างต้น

2.1.1 หลักการบริหารจัดการแบนด์วิดท์

การจัดการแบนด์วิดท์ คือ เครื่องมือที่ช่วยบริการในการบริหารการจัดการกับแบนด์วิดท์ในแต่ละแอปพลิเคชั่น (Application) เช่น อินเทอร์เน็ต, จดหมายอิเล็กทรอนิกส์ (E-mail), เว็บไซต์ (Web Site) เป็นต้น ซึ่งสามารถกำหนดหรือเปลี่ยนแปลงค่าแบนด์วิดท์ได้ตามต้องการ และ ความเหมาะสม และ สามารถช่วยให้แอปพลิเคชั่นดังกล่าวสามารถทำงานกับระบบปฏิบัติการได้อย่างรวดเร็ว และ เต็มประสิทธิภาพ รวมทั้งยังสามารถจำกัดการใช้งานในแอปพลิเคชั่นที่ไม่เป็นประโยชน์ได้อีกด้วย

ในการใช้งานโครงข่ายในการรับส่งข้อมูลของแต่ละบริษัทนั้นจำเป็นต้องมีการบริหารจัดการกับแบนด์วิดท์ ซึ่งถ้าหากไม่มีการบริหารจัดการแบนด์วิดท์บนโครงข่ายที่ใช้งานอยู่ จะส่งผลให้ผู้ใช้งานจะแย่งการใช้งานของแบนด์วิดท์ที่มีอยู่ในเวลาเดียวกัน ทำให้เกิดการล่าช้า และ ปัญหาติดขัดในการรับส่งข้อมูลเพราะไม่มีการวางแผนการจัดระเบียบกับแบนด์วิดท์ในโครงข่ายดังกล่าว

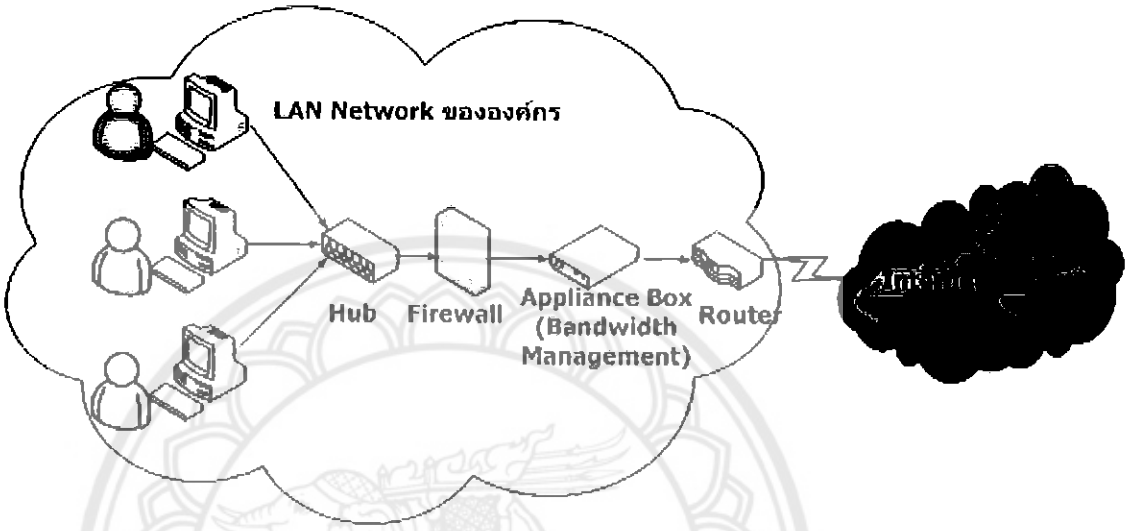
ตารางที่ 2.1 ตัวอย่างการบริหารจัดการแบนด์วิดท์ เพื่อใช้งานในสำนักงาน

ผู้ใช้งาน	Bandwidth Management				
	Priority	Bandwidth		Application	
		Intranet	Internet	E-mail	Google
ผู้จัดการ	ต่ำ	100 Kbps	50 Kbps	✓	✓
พนักงานสั่งสินค้าและทำบัญชี	สูง	200 Kbps	100 Kbps	✓	-
พนักงานขาย	สูง	200 Kbps	100 Kbps	✓	✓

2.1.2 รูปแบบการทำงานในการบริหารจัดการแบนด์วิดท์

โดยปกติผู้ใช้งานสามารถควบคุมปริมาณการใช้งานของแบนด์วิดท์ ในแต่ละแอปพลิเคชั่น ให้เป็นไปตามนโยบาย และ ความต้องการของหน่วยงานโดยผ่านทางเว็บเบส (Web Base) โดยที่รูปแบบของการบริหารจัดการแบนด์วิดท์ที่ช่วยในการจัดการแบนด์วิดท์ สำหรับแอปพลิเคชั่น แต่ละประเภทให้เป็นไปตามต้องการนั้นสามารถทำได้โดยการติดตั้งชุดอุปกรณ์ Box Appliance ซึ่ง สำนักงานบริการเทคโนโลยีสารสนเทศภาครัฐ (สบทร.) เป็นผู้พัฒนาขึ้น

โดยที่อุปกรณ์ดังกล่าวสามารถวิเคราะห์แบนด์วิดท์ของแอปพลิเคชั่น ใหม่ๆได้ หากมีการใช้งานแอปพลิเคชั่น ทั้งปกติ และ ไม่ปกติ และยังสามารถรองรับประเภทแอปพลิเคชั่น ที่มีอยู่ทั่วไปได้ถึง 122 ประเภท โดยมีรูปแบบการติดตั้งการทำงานดังแสดงในรูปที่ 2.1



รูปที่ 2.1 แสดงการเชื่อมต่อภายในองค์กรลูกค้าเมื่อติดตั้งอุปกรณ์บริหารจัดการแบนด์วิดท์

รูปที่ 2.1 แสดงตำแหน่งการติดตั้งอุปกรณ์เพื่อให้บริการบริหารจัดการแบนด์วิดท์โดยติดตั้งอยู่ระหว่างไฟร์วอลล์ (Firewall) กับเราท์เตอร์ (Router) ขององค์กร เมื่อมีการใช้งานแอปพลิเคชั่นต่างๆของผู้ใช้งานก่อนที่จะออกไปเครือข่ายภายนอก ระบบจะทำหน้าที่จัดแยกประเภทแอปพลิเคชั่น และ ควบคุมปริมาณแบนด์วิดท์ในแต่ละแอปพลิเคชั่น ที่ใช้งานให้เป็นไปตามนโยบายการบริหารจัดการแบนด์วิดท์ของหน่วยงาน

2.2 การจัดสรรช่องสัญญาณสำหรับข้อมูล (Traffic Shaping)

การจัดสรรช่องสัญญาณสำหรับข้อมูลคือการนำการบริหารจัดการแบนด์วิดท์ ไปใช้งานจริงในทางปฏิบัติ โดยที่ผู้ใช้งานโครงข่ายสามารถเลือกใช้งานซอฟต์แวร์ (Software) หรือ ฮาร์ดแวร์ (Hardware) ที่ได้ถูกจัดทำ Traffic Shaping มาใช้ควบคุมการทำงานของแบนด์วิดท์ได้

256 Kbps	พนักงานสั่งสินค้าและบัญชี	100 Kbps
	พนักงานขาย	100 Kbps
	ผู้จัดการ	50 Kbps

รูปที่ 2.2 แสดงการใช้งานช่องสัญญาณที่มีการทำ Traffic Shaping แล้ว

จากรูปที่ 2.2 แสดงการใช้งานช่องสัญญาณในการรับส่งข้อมูลที่มีการทำ Traffic Shaping เพื่อให้ผู้ใช้งานไม่ต้องแย่งกันเพื่อใช้งานแบนด์วิดท์ที่มีอยู่ แต่ผู้ใช้งานจะถูกแยกให้ใช้งานแบนด์วิดท์โดยการกำหนดอนุญาติให้ใช้งานในความเร็วที่ถูกจัดสรร โดยไม่ต้องกังวลว่าจะไม่ได้ใช้งานแบนด์วิดท์ในกรณีเร่งด่วน

2.2.1 วิธีการจัดสรรช่องสัญญาณสำหรับข้อมูล (Traffic Shaping Management)

การทำ Traffic Shaping ด้วยซอฟต์แวร์ นั้น จำเป็นต้องมีการติดตั้งซอฟต์แวร์ ที่ทำหน้าที่ควบคุมแบนด์วิดท์ บนโครงข่าย ที่เรียกว่า "ซอฟต์แวร์ สำหรับการบริหารจัดการแบนด์วิดท์" เช่น Traffic shaper, Bandwidth shaper, Bandwidth controller และ Bandwidth Management เป็นต้น โดยที่การใช้ฮาร์ดแวร์ หรือ อุปกรณ์ที่ทำหน้าที่ควบคุมการใช้งานช่องสัญญาณบนโครงข่าย จะเรียกว่า "Bandwidth Manageable Switch"

โดยที่ตำแหน่งที่เหมาะสมสำหรับติดตั้ง Bandwidth Manageable Switch คือ ตำแหน่งเดียวกับที่วางคอมพิวเตอร์ที่เป็นเกตเวย์ (Gateway) เพื่อควบคุมการใช้งานของช่องสัญญาณทั้งโครงข่าย โดยอุปกรณ์ประเภทนี้มีความสามารถในการบริหารจัดการแบนด์วิดท์สูงมากซึ่งผู้ใช้งานเพียงแต่ทำการกำหนดค่าพารามิเตอร์ต่างๆให้อุปกรณ์เท่านั้น ซึ่งได้แก่พวก ขนาดแบนด์วิดท์ ของผู้ใช้งานที่จะต้องเชื่อมต่อกับพอร์ต (Port) ของสวิทซ์นั้น, ระดับความสำคัญ (Priority) ของการถ่ายโอนข้อมูลผ่านพอร์ตนั้นๆ เป็นต้น ซึ่งในปัจจุบันการกำหนดพารามิเตอร์ ต่างๆสามารถทำได้โดยอาศัยซอฟต์แวร์ ประเภท Web Base Application

2.2.2 ประโยชน์ของการทำ Traffic Shaping ด้วยซอฟต์แวร์

การทำ Traffic Shaping ด้วยซอฟต์แวร์นั้นนอกจากทำให้สูญเสียค่าใช้จ่ายน้อยแล้ว ยังช่วยให้เกิดความสะดวกในการใช้งานฮาร์ดแวร์ด้วยเหตุผลต่าง ๆ ดังนี้

1. ไม่จำเป็นต้องใช้ผู้ดูแลระบบโครงข่ายที่มีประสบการณ์สูง

2. สามารถแสดงรายงานได้อย่างละเอียด (ขึ้นอยู่กับความสามารถของซอฟต์แวร์นั้นๆ)

3. สามารถดูการใช้งาน Bandwidth บนโครงข่ายจริงได้ตลอดเวลา

4. สามารถควบคุมการใช้งานได้ลึกถึงระดับโพรโตคอล (Protocol)

5. สามารถตั้งเงื่อนไขสำหรับการใช้งานได้อย่างมากมาย

6. สามารถติดตั้งได้ทั้งบนคอมพิวเตอร์แม่ข่าย (Server) และ เครื่องลูกข่าย (Client) เพื่อทำหน้าที่ควบคุมโครงข่ายที่แตกต่างกัน

2.3 คำจำกัดความที่เกี่ยวข้องกับการจัดการกับแบนด์วิดท์

ในการศึกษาถึงวิธีการจัดการเกี่ยวกับแบนด์วิดท์นั้นจำเป็นต้องมีความรู้ถึงคำจำกัดความของข้อมูลที่เกี่ยวข้องในการจัดการกับแบนด์วิดท์ ซึ่งมีรายละเอียดดังนี้

2.3.1 โพรโตคอล (Protocol)

โพรโตคอล เปรียบเหมือนภาษาที่ใช้เพื่อติดต่อสื่อสารระหว่างผู้ส่งสาร และ ผู้รับสาร ยกตัวอย่างการสื่อสารกันในโครงข่ายคอมพิวเตอร์สำหรับผู้ส่งสารและผู้รับสาร ซึ่งเครื่องคอมพิวเตอร์ที่ใช้งานอาจอยู่บนโครงข่ายเดียวกัน หรือ ต่างโครงข่ายกัน โดยผู้ส่งสารและผู้รับจะสามารถสื่อสารกันได้อย่างถูกต้องนั้น หมายถึงจำเป็นต้องใช้ภาษาเดียวกันในการสื่อสารด้วย หรืออาจจะกล่าวได้คือ จำเป็นต้องมีการใช้โพรโตคอล เดียวกันนั้นเอง

1. ชนิดของโพรโตคอล

โพรโตคอล ที่ถูกใช้เพื่อส่ง หรือ รับข้อมูลบนโครงข่ายคอมพิวเตอร์ มีหลากหลายชนิด แต่ที่นิยมในการใช้งาน และ จัดเป็นซอฟต์แวร์ที่จัดการแบนด์วิดท์ ต้องใช้งานนั้น มีดังนี้

ตารางที่ 2.2 แสดงชนิดโพรโตคอลที่ใช้งานอยู่ในปัจจุบัน

Protocol	การนำไปใช้งาน
Transmission Control Protocol (TCP)	นำส่งข้อมูลจาก Application Layer ไปยังจุดหมายปลายทาง โดยปัจจุบันเป็นโพรโตคอล หลักที่ถูกใช้ในการนำส่งข้อมูลต่างๆบนโครงข่ายอินเทอร์เน็ต นอกจากนั้นยังเหมาะสำหรับการเชื่อมต่อที่ความมั่งคงต่ำ (Non Reliable Link) อย่าง
User Datagram Protocol (UDP)	ทำงานเหมือนกับ TCP แต่มักพบถูกใช้กับโครงข่ายการเชื่อมต่อที่มั่นคงสูง นอกจากนั้นขนาดของ Header ของ UDP ยังเล็กกว่า TCP ค่อนข้างมาก และไม่ต้องรอรับสัญญาณตอบกลับ จังทำให้ส่งข้อมูลแบบ UDP สำหรับถ่ายโอนข้อมูลระหว่างต้นทางและปลายทางในโครงข่ายแบบอินทราเน็ตมากกว่าอินเทอร์เน็ต
Internet Control Message protocol (ICMP)	ถูกใช้เพื่อแจ้ง Routerให้ทราบว่าแม่ข่าย (Host) ต้องการรับข้อความแบบ Multi Cast จากผู้ส่งหลายแหล่ง

ตารางที่ 2.2 แสดงชนิดโพรโตคอลที่ใช้งานอยู่ในปัจจุบัน (ต่อ)

Protocol	การนำไปใช้งาน
Generic Router Encapsulation protocol (GRE)	เป็นโพรโตคอล ที่ถูกใช้เพื่อทำการเข้ารหัสข้อมูลทั้งแพ็คเกต ก่อนนำส่งออก สู่โครงข่ายคอมพิวเตอร์ มักถูกใช้ทำงานร่วมกับ PPTP Protocol (Point to Point Tunneling Protocol) ทำหน้าที่สร้างอุโมงค์ส่ง หรือ รับข้อมูลส่วนบุคคลโดยเชื่อมโยงเครื่องคอมพิวเตอร์ต้นทางและปลายทางเข้าด้วยกัน

2. การกำหนดหมายเลขโพรโตคอล

สำหรับการส่ง หรือ รับข้อมูลโดยทั่วไปบนโครงข่ายอินเทอร์เน็ต และ อินทราเน็ตที่เราใช้งานกันอยู่ทุกวันนี้ อาศัยโพรโตคอล ที่มีชื่อว่า TCP หรือ UDP เป็นหลัก โดยข้อมูลที่ถูกสร้างขึ้นเพื่อติดต่อสื่อสารจากทั้ง 2 โพรโตคอลนี้ จะประกอบไปด้วย 2 ส่วนหลักคือ ส่วนหัวข้อ (Header) และ ข้อมูล โดยส่วนหัวข้อ คือส่วนหัวข้อของข้อมูลซึ่งจะบรรจุข้อมูลที่สำคัญต่างๆ เช่น ความยาวของข้อมูลที่จะถูกส่งมา หมายเลขพอร์ต และ การเช็คข้อผิดพลาด (Error Checking) เป็นต้น

2.3.2 พอร์ต (Port)

พอร์ต คือ หมายเลขที่มีไว้สำหรับระบุความแตกต่างระหว่างข้อมูลออกจากกัน เมื่อใช้งานโพรโตคอลเดียวกันในการรับ หรือ ส่งข้อมูล นอกจากนั้นหมายเลขพอร์ต ยังถูกนำไปใช้เพื่อบอกเครื่องคอมพิวเตอร์ปลายทางว่า ข้อมูลที่รับเข้ามานั้นต้องใช้แอปพลิเคชั่นใดจัดการต่อไป ยกตัวอย่างเช่น การค้นหาข้อมูลบน Google หรือ การเข้าไปเยี่ยมชมเว็บไซต์ต่างๆ ข้อมูลที่ถูกรับหรือ ส่งระหว่างต้นทาง และ ปลายทางนั้น จะอาศัยโพรโตคอล ที่ชื่อ TCP (Transmission Control Protocol) นอกจากนั้นยังจำเป็นต้องมีหมายเลขพอร์ต กำกับอยู่ด้วยเสมอ ซึ่งหมายเลขพอร์ต ที่ต้องถูกใช้ได้แก่หมายเลข 80 หรือ 8080 โดยทั้งสองหมายเลขนี้ จะเป็นตัวบอกเลขคอมพิวเตอร์ปลายทางว่า ข้อมูลที่รับมาจะต้องนำไปประมวลผลต่อ โดยใช้โปรแกรม Internet Explore หรือ Firefox เป็นต้น

1. พอร์ตและการจัดการแบนด์วิดท์บนโครงข่าย

ความสัมพันธ์ของพอร์ต และ การจัดการแบนด์วิดท์บนโครงข่ายเกี่ยวกันอย่างหลีกเลี่ยงไม่ได้ เนื่องจากเครื่องคอมพิวเตอร์ที่ทำหน้าที่ดูแลการใช้งานแบนด์วิดท์ต้องอาศัยการตรวจดูตำแหน่งของพอร์ต และ ชนิดของโพรโตคอล จากข้อมูลที่ไหลผ่านเครื่องคอมพิวเตอร์ เพื่อกำหนดความเร็วสำหรับการถ่ายโอนข้อมูลระหว่างเครื่องคอมพิวเตอร์ หรือ ปิดการติดต่อสื่อสารตามแต่ละข้อกำหนดที่ผู้ดูแลระบบโครงข่ายได้กำหนดขึ้นมา เพื่อจำกัดสิทธิการใช้งานสำหรับเครื่องนั้นๆไว้ ซึ่งคอมพิวเตอร์จะไม่ทำงานหนัก เนื่องจากการจัดการแบนด์วิดท์ จะเลือกดู่แค่ตำแหน่งของพอร์ต ที่เก็บอยู่ในส่วนหัวข้อของแพ็คเกต เท่านั้น ไม่จำเป็นต้องดูทั้งแพ็คเกตจึงไม่ทำให้คอมพิวเตอร์ทำงานหนักมากเท่าไร

2.3.3 ไฟร์วอลล์ (Firewall)

ไฟร์วอลล์ ทำหน้าที่ป้องกันอันตรายจากโลกภายนอกที่อาจเข้ามาทำร้ายเครื่องคอมพิวเตอร์ หรือ โครงข่าย ซึ่งอาจเป็นโครงข่ายอินเทอร์เน็ต หรือ อินทราเน็ตได้ ซึ่งจะพบว่า ไฟร์วอลล์นั้นมีการทำงานอยู่ตรงกลางระหว่างโครงข่ายภายนอก และ โครงข่ายภายใน ซึ่งปัจจุบันเครื่องคอมพิวเตอร์ที่ติดตั้ง Windows XP Service Pack 2 จะมีไฟร์วอลล์ให้โดยอัตโนมัติด้วย หลักการทำงานของไฟร์วอลล์นั้น คือ ทุกข้อมูลที่ต้องผ่านเข้าหรือออกจากเครื่องต้องถูกตรวจ เพื่อดูว่าข้อมูลเหล่านั้นมาจากพอร์ทใด โดยถ้าตรวจพบว่าไม่ได้มาจากพอร์ทที่ได้รับอนุญาตไว้ในไฟร์วอลล์ข้อมูลเหล่านั้นจะไม่สามารถผ่านเข้าไปยังเครื่องคอมพิวเตอร์ปลายทางได้

1. ประเภทของไฟร์วอลล์

ไฟร์วอลล์ที่นิยมติดตั้งมากที่สุดมี 2 ประเภท คือไฟร์วอลล์ประเภทฮาร์ดแวร์และไฟร์วอลล์ประเภทซอฟแวร์ โดยการติดตั้งและการใช้งานแตกต่างกันตามระดับความเหมาะสม โดยมีรายละเอียดดังนี้

- ไฟร์วอลล์ประเภทฮาร์ดแวร์ มีความสามารถสูงในการตรวจสอบแพ็คเกต ที่ไหลเข้า หรือ ออกจากโครงข่าย ที่เรียกว่า "Packet Filtering" เป็นวิธีการเพิ่มความปลอดภัยในระบบไฟร์วอลล์ที่คัดแยกข้อมูลบางอย่างออก นอกจากนี้ไฟร์วอลล์ประเภทฮาร์ดแวร์ยังเหมาะที่จะทำหน้าที่ป้องกันโครงข่ายขนาดใหญ่ เนื่องจากอุปกรณ์ประเภทนี้มีเสถียรภาพสูงกว่าเครื่องคอมพิวเตอร์ที่ติดตั้งไฟร์วอลล์มาก ในด้านการกำหนดเงื่อนไขนั้น จะไม่มีอะไรยุ่งยากเหมือนไฟร์วอลล์ประเภทซอฟต์แวร์ ซึ่งมีหลากหลายแบบให้เลือก ซึ่งสรุปได้ว่า ไฟร์วอลล์ประเภทนี้เหมาะกับโครงข่ายขนาดใหญ่

- ไฟร์วอลล์ประเภทซอฟต์แวร์ ความสามารถของไฟร์วอลล์ประเภทซอฟต์แวร์ นี้จะช่วยกำหนดสิทธิในการติดต่อสื่อสารระหว่างแอปพลิเคชั่นที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ และโลกภายนอกได้ ข้อดีของไฟล์วอลล์ประเภทนี้ คือ ยอมให้เรากำหนดกฎต่างๆได้มากกว่าประเภทฮาร์ดแวร์ นอกจากนั้น ไฟร์วอลล์บางตัวยังมีความยืดหยุ่นสูงขนาดที่สามารถทำงานร่วมกับโปรแกรมป้องกันไวรัสได้อย่างดี ซึ่งสรุปได้ว่า ไฟร์วอลล์ประเภทนี้เหมาะกับโครงข่ายขนาดเล็กถึงขนาดกลาง

2.3.4 บิต ทอร์เรนต์ (Bit Torrent)

บิต ทอร์เรนต์เป็นวิธีการส่งข้อมูลในอินเทอร์เน็ตที่จะแตกไฟล์ออกเป็นชิ้นเล็กๆ แล้วสุ่มไฟล์ย่อยทีละชิ้นไปยังเครื่องรับปลายทาง และ จะส่งข้อมูลที่ได้รับต่อไปยังเครื่องรับอื่นๆ ที่มีการขอไฟล์เดียวกันด้วย ทำให้เครื่องคอมพิวเตอร์แต่ละเครื่องเป็นทั้งผู้รับ และ ผู้ส่งในเวลาเดียวกัน ทำให้มีการส่งทอดไฟล์นี้ให้กับผู้ใช้คนต่อๆไปที่ร้องขอการดาวน์โหลด จึงทำให้ไฟล์ถูกแพร่กระจายไปได้อย่างรวดเร็ว

ในการดาวน์โหลดโดยการใช้ Bit Torrent นั้น จะต้องมีผู้ที่มีไฟล์สมบูรณ์ และ ปล่อยให้ ดาวน์โหลดอยู่ด้วย ยิ่งไฟล์นั้นมีการดาวน์โหลดมากเท่าไร จะทำให้การดาวน์โหลดง่าย และ มีประสิทธิภาพมากยิ่งขึ้น ด้วยเหตุนี้จึงทำให้ Bit Torrent สามารถรองรับการดาวน์โหลดข้อมูลจำนวนมากๆ ได้สูงกว่าการดาวน์โหลดแบบทั่วไป และ เป็นที่นิยมมากในปัจจุบัน

1. หลักการทำงานของ Bit Torrent

Bit Torrent มีการทำงานแบบ P2P (Peer to Peer) คือเป็นการส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ภายในระบบเครือข่าย โดยจะทำหน้าที่เป็นทั้งผู้รับ และ ผู้ส่งในเครื่องเดียวกัน เมื่อมีการเริ่มการส่ง หรือ ดาวน์โหลดไฟล์เกิดขึ้น โปรแกรมจะทำหน้าที่แตกไฟล์ออกเป็นส่วนๆ แล้วส่งต่อไปให้กับผู้ที่เข้ามาดาวน์โหลดต่อทีละส่วน โดยไม่จำเป็นต้องรอให้ดาวน์โหลดครบ 100% ก่อน ซึ่งจะเป็นการดาวน์โหลดในลักษณะที่มีการแบ่งไฟล์ให้แก่กัน การทำงานของโปรแกรมแบ่งออกเป็น 3 ส่วน ดังนี้

- Torrent Client หรือ ที่เรียกว่าโปรแกรม Torrent ซึ่งจะติดตั้งที่เครื่องของเรามีให้เลือกใช้หลายโปรแกรมด้วยกัน เช่น BitTorrent, BitComet, Vuze, BitTornado และ TorrentStorm เป็นต้น โดยโปรแกรมแต่ละตัวมีข้อดีแตกต่างกัน แต่ทำงานอยู่บนโพรโตคอล Bit Torrent

- Tracker Server หรือ เรียกสั้นๆ ว่า Tracker ซึ่งเป็นเว็บไซต์ หรือ Server ที่เป็นแม่ข่าย ทำหน้าที่เป็นตัวกลางระหว่างโปรแกรม Torrent โดยก่อนที่จะเริ่มดาวน์โหลดโปรแกรม Torrent ในเครื่องของผู้ใช้จะติดต่อกับ Tracker ก่อน จากนั้น จะทำการติดต่อเป็นระยะๆ เพื่อปรับ (Update) สถานะ

- Torrent File (นามสกุล .torrent) เป็นไฟล์ที่ใช้เก็บข้อมูลต่างๆ ของไฟล์ที่จะให้ดาวน์โหลด เช่น ที่อยู่ของไฟล์ ขนาดของไฟล์ และ ชื่อไฟล์ เป็นต้น โดยไฟล์นี้จะถูกนำไปใช้โดยโปรแกรม Torrent เพื่ออ่านข้อมูลที่อยู่ในไฟล์ Torrent

2.3.5 Software Router

ซอฟแวร์เราเตอร์ คือโปรแกรมสำหรับควบคุมการทำงานของเราเตอร์ ซึ่งในปัจจุบันมีอยู่หลายโปรแกรมด้วยกัน โดยในโครงงานนี้ได้เลือกศึกษาซอฟแวร์เราเตอร์อันได้แก่ IPCop, NetLimiter และ PFSense โดยมีรายละเอียดการทำงานดังนี้

1. IPCop

IPCop เป็น Opensource สำหรับระบบปฏิบัติการลินุกซ์ (Linux Operating System) ที่พัฒนาขึ้นมาเพื่อมีเป้าหมายเน้นทางด้านระบบความปลอดภัยของเครือข่ายจึงเหมาะสมที่จะนำมาพัฒนาเป็นไฟร์วอลล์โดยมีคุณสมบัติที่เด่นๆ ของ Smootwall (เป็น Software ที่ IPCop นำมาพัฒนาต่อ ทำงานคล้ายๆกัน) โดย IPCop นั้นได้มีการนำเอา Smootwall มาพัฒนาเพื่อให้ใช้งานฟังก์ชันต่างๆ ได้ฟรี โดยไม่ต้องเสียค่าใช้จ่าย และ สามารถใช้งานฟังก์ชั่นเหล่านั้นได้อย่างมีประสิทธิภาพ นอกจากนี้ยังมีโปรแกรมเสริม (Add-on) ที่สามารถใช้กับ IPCop ได้เป็นจำนวนมาก

นอกจากนี้โปรแกรมที่ติดตั้งมากับ IPCop เพื่อใช้งานในเรื่องของการแชร์อินเทอร์เน็ต และ ไฟร์วอลล์แล้ว ยังมีโปรแกรมที่สามารถตั้งเข้าไปได้อีก เพื่อช่วยให้สามารถทำงานได้อย่างมีประสิทธิภาพ หรือ Add-on โดยมีรายละเอียดดังนี้

- Advproxy (Advanced Proxy) ช่วยให้สามารถกำหนดค่าของ Proxy ได้อย่างมีประสิทธิภาพ ซึ่งโดยปกติแล้วหน้าเว็บเพจ (Web Page) สำหรับการกำหนดค่าของ Proxy ที่มากับ IPCop เอง จะมีตัวเลือกในการกำหนดค่าของ Proxy ไม่มาก ทำให้ไม่สามารถที่จะใช้งาน Proxy ได้อย่างเต็มที่ เช่น กำหนดผู้ใช้งาน Proxy ได้ จำกัดความเร็วในการดาวน์โหลด เป็นต้น

- I7Filter เป็น Add-on พื้นฐานในการติดตั้งแพ็คเกต ของ p2pblock และ Qos_ng

- p2pblock มีไว้สำหรับบล็อกการทำงานของ Bit Torrent หรือ ทำการ Block port

- Qos_ng ทำหน้าที่เกี่ยวกับการจัดการแบนด์วิดท์ หรือ ทำการ Bandwidth shaping

- URL Filter ช่วยนำมาใช้ในการควบคุมการเข้าใช้งานอินเทอร์เน็ตของเครื่องลูกข่าย ที่เข้า เว็บไซต์ หรือ ดาวน์โหลดโปรแกรมที่ไม่เหมาะสม จำกัดเวลาในการใช้อินเทอร์เน็ต จำกัดช่วงเวลาที่จะสามารถใช้อินเทอร์เน็ตได้ ซึ่งจะทำงานร่วมกับ Advproxy

- BlockOfTraffic (BOT) ทำหน้าที่เป็น Firewall Configure สำหรับกำหนดกฎที่จะใช้กับเครื่องลูกข่ายที่จะออกไปสู่อินเทอร์เน็ตข้างนอก (บล็อกการออกไปสู่อินเทอร์เน็ตของเครื่องลูกข่าย ไม่เกี่ยวกับการบล็อกจากด้านนอกเข้ามาข้างในเครือข่าย)

ข้อดีของ IPCop

1. ง่ายในการบริหารจัดการผ่านเว็บ
2. มีความสามารถในการทำงานร่วมกับการ์ดแลน (Network Interface Card) ได้ 4 ชนิด ดังนี้

ตารางที่ 2.3 แสดงประเภทอินเตอร์เฟส ของ IPCop

ชื่ออินเตอร์เฟส	คุณสมบัติ
RED	เป็นอินเตอร์เฟส ที่เชื่อมต่อกับระบบอินเทอร์เน็ตหรือเครือข่ายข้างนอก
GREEN	เป็นอินเตอร์เฟส ที่เชื่อมต่อกับระบบ LAN (เครือข่ายในสำนักงาน)
BLUE	เป็นอินเตอร์เฟสพิเศษสำหรับเชื่อมต่อกับ Access Point หรืออุปกรณ์ที่ใช้สำหรับแชร์อินเทอร์เน็ตอื่น
ORANGE	เป็นอินเตอร์เฟส สำหรับไว้เชื่อมต่อกับ Server ในกรณีที่เรามี Server ในระบบเครือข่ายของเรา ซึ่งข้างนอกจะเข้าถึง Server นี้ได้โดยผ่านทางระบบ DMZ โดยจะมีการ Forward Port ไปยัง Server ต่างๆ

2. NetLimiter

NetLimiter เป็นซอฟต์แวร์พื้นฐานในการทำการควบคุมปริมาณการใช้งานอินเตอร์เน็ต และ เป็นเครื่องมือที่ใช้ในการตรวจสอบปริมาณการใช้งานของอินเทอร์เน็ตซึ่งถูกออกแบบมาสำหรับระบบปฏิบัติการวินโดว์ (Windows Operating System) NetLimiter สามารถทำการควบคุมปริมาณการใช้งานอินเทอร์เน็ตโดยการจำกัดอัตราการถ่ายโอนสำหรับแอปพลิเคชั่น และ ตรวจสอบปริมาณการใช้งานอินเทอร์เน็ตที่ขาเข้า และ ขาออก

NetLimiter สามารถจำกัดอัตราการดาวน์โหลด และอัพโหลด สำหรับแอปพลิเคชั่นการเชื่อมต่อ ซึ่งง่ายในการจำกัด หรือ บริหารจัดการแบนด์วิดท์ การเชื่อมต่ออินเทอร์เน็ต ให้กับแอปพลิเคชั่นที่ทำงานบนคอมพิวเตอร์โดยมีรายละเอียดการทำงานดังนี้

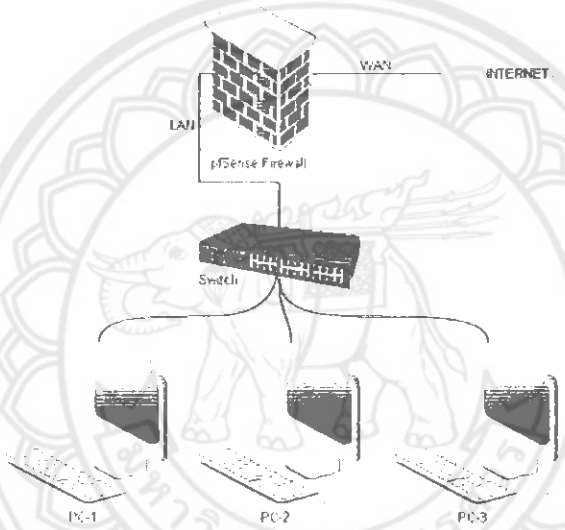
1. สามารถแสดงรายการช่องทางสื่อสารที่มีการเชื่อมต่อ และ อัตราการรับ-ส่งของแอปพลิเคชั่น
2. มีไฟร์วอลล์ช่วยในการควบคุมการเชื่อมต่อทั้งขาเข้า และ ขาออกของแอปพลิเคชั่น
3. สามารถเฝ้าสังเกต (Monitor) และ ควบคุมปริมาณการใช้งานแบ่งเป็น 3 Predefined Zone ได้แก่ My Computer, Local Network และ Internet
4. สามารถกำหนดกลุ่มการเชื่อมต่อ หรือ แอปพลิเคชั่นเพื่อง่ายในการจำกัดปริมาณการใช้งาน
5. สามารถทำการปรับแต่ง แก้ไข และ ตั้งเวลาการทำงานของกฎ
6. มีการบันทึก (Log) เหตุการณ์ต่างๆของเครือข่าย
7. สามารถแสดงกิจกรรมของรายการแอปพลิเคชั่น หรือ การเชื่อมต่อแบบ Real Time สามารถบริหารจัดการเกี่ยวกับการอนุญาต (Permission) ในการเฝ้าสังเกต หรือ ควบคุมปริมาณข้อมูลเข้าออก (Traffic)

3. PFSense

PFSense เป็น Open Source firewall ที่ไม่ได้ต้องการฮาร์ดแวร์สูงมากนัก จะทำหน้าที่เป็นทั้งไฟร์วอลล์ และ เกตเวย์ไปพร้อมๆ กัน สิ่งที่จำเป็นคือ NIC (Network Interface Card) จำนวน 2 ใบ สำหรับข่ายงานบริเวณเฉพาะที่ (LAN) และ ข่ายงานบริเวณกว้าง (WAN)

LAN : จะทำการเชื่อต่อกับ Switch เพื่อกระจายไปยังคอมพิวเตอร์อื่นๆ ในเครือข่าย

WAN : เชื่อต่อไปยัง ADSL Modem เพื่อทำการเชื่อมต่อกับอินเทอร์เน็ต



รูปที่ 2.3 แสดงการทำงานของ PFSense

[ที่มา : http://www.laontalk.com/2009/01/15/365]

บทที่ 3
ขั้นตอนและการดำเนินงาน

3.1 วิเคราะห์ระบบ

จากปัญหาเกี่ยวกับปริมาณการใช้งานแบนด์วิดท์ (Bandwidth) ที่เชื่อมต่อกับระบบอินเทอร์เน็ต (Internet) ทำให้เกิดความล่าช้าในการใช้งานอินเทอร์เน็ตของผู้ใช้บริการภายในหอพัก ซึ่งเมื่อมีการใช้งานอินเทอร์เน็ตมากขึ้น โดยไม่มีการจำกัดการใช้งาน ปัญหาการใช้อินเทอร์เน็ตที่เกิดจากการใช้แบนด์วิดท์ของอินเทอร์เน็ตไม่เพียงพอต่อความต้องการของผู้ใช้งานจึงเกิดขึ้น

ด้วยเหตุนี้การแก้ไขปัญหาดังกล่าวจึงเป็นเรื่องของการติดตั้งซอฟต์แวร์เราเตอร์ ซึ่งเป็นซอฟต์แวร์ที่เกี่ยวข้องกับการจัดการแบนด์วิดท์ให้บริการแก่ผู้ใช้งานอินเทอร์เน็ต เพื่อช่วยแก้ปัญหาดังกล่าว

3.1.1 ความต้องการของระบบ (System Requirement)

- ความต้องการของผู้ใช้งานอินเทอร์เน็ต

ต้องการแบนด์วิดท์ที่เพียงพอต่อการใช้งานอินเทอร์เน็ต เพื่อไม่ให้เกิดความล่าช้าในการใช้งาน

- ความต้องการของผู้ดูแลระบบ

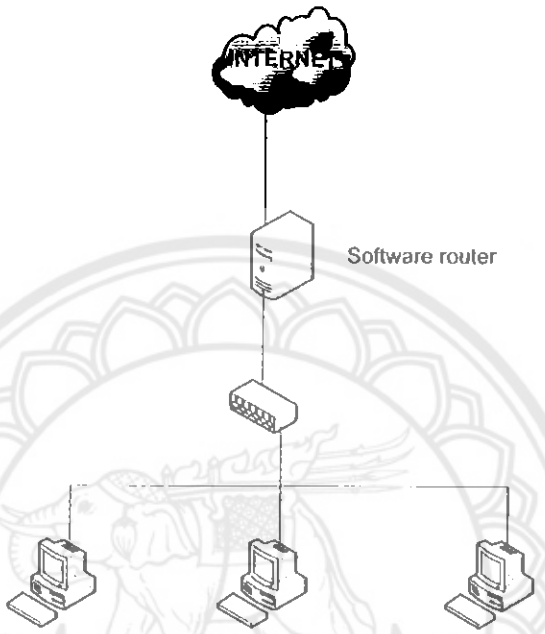
สามารถติดตั้ง และ จัดการระบบบริหารการใช้งานแบนด์วิดท์โดยใช้ ซอฟต์แวร์เราเตอร์ที่นำมาทำการทดลองได้อย่างมีประสิทธิภาพ

- นำ ซอฟต์แวร์เราเตอร์ มาใช้ในการจัดการแบนด์วิดท์
- จัดสรรแบนด์วิดท์ได้พอดีกับความต้องการของผู้ใช้งานอินเทอร์เน็ต

3.2 ออกแบบระบบ

จากการศึกษาเรื่องการบริหารจัดการแบนด์วิดท์ (Bandwidth Management) หนึ่งในวิธีที่น่าสนใจคือการใช้ซอฟต์แวร์เราเตอร์ ในการจำกัดแบนด์วิดท์ซึ่งซอฟต์แวร์เราเตอร์ ที่นำมาใช้มีจำนวน 3 ซอฟต์แวร์ (Software) ได้แก่

1. IPCop
2. NetLimiter
3. PFSense



รูปที่ 3.2 แผนภาพการทำงานของซอฟต์แวร์เราเตอร์

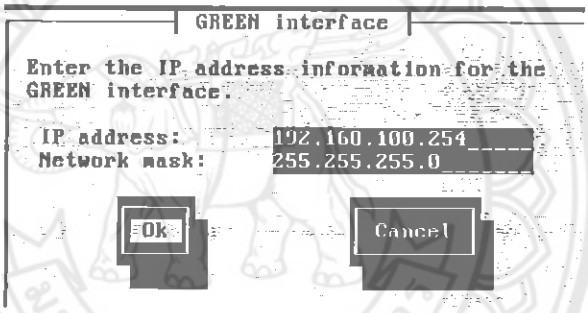
จากรูปซอฟต์แวร์เราเตอร์ จะสามารถต่อกับอินเตอร์เน็ตได้โดยใช้การ์ดแลน (LAN Card) ใบที่หนึ่ง ซึ่งจะเรียกว่าระบบ WAN (Wide Area Network) แล้ว ซอฟต์แวร์เราเตอร์จะทำการส่งอินเตอร์เน็ตไปยังเครื่องลูกข่าย (Client) โดยใช้การ์ดแลนใบที่สอง ซึ่งจะเรียกว่าระบบ LAN (Local Area Network)

โดย IPCop จะใช้การ์ดแลนใบที่ 1 เป็นแบบ Red Interface ส่วนการ์ดแลนใบที่ 2 เป็นแบบ Green Interface

3.3 การเชื่อมต่ออินเตอร์เน็ตกับซอฟต์แวร์เราเตอร์

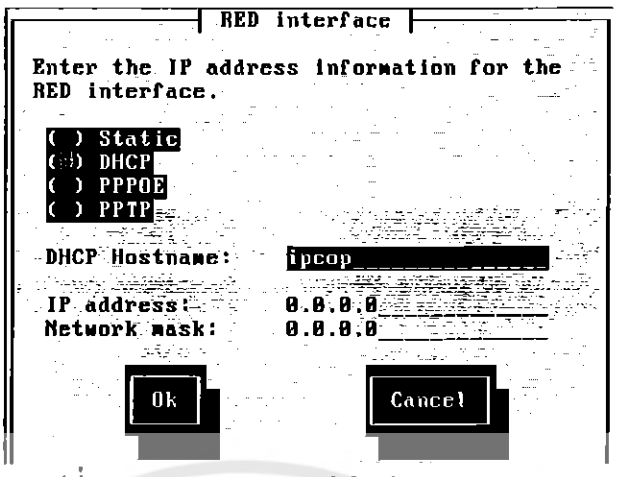
ในการทดลองเชื่อมต่ออินเตอร์เน็ตกับซอฟต์แวร์เราเตอร์ จำนวน 3 ซอฟต์แวร์ได้แก่ IPCop, NetLimiter และ PFSense โดยใช้โปรแกรม VMware ในการจำลองซอฟต์แวร์ทั้ง 3 ตัวนี้โดยกำหนดให้ซอฟต์แวร์แต่ละตัวมีการ์ดแลนจำนวน 2 ใบซึ่งใบที่หนึ่งไว้เชื่อมต่อกับอินเตอร์เน็ตเป็นชนิด NAT (Network Address Translation) ส่วนใบที่สองไว้เชื่อมต่อกับระบบแลน เป็นชนิด NAT เช่นเดียวกัน ซึ่งทำการทดลองโดยการจำลอง Windows XP ขึ้นมาเพื่อเป็นเครื่องลูกข่าย ซึ่งในแต่ละซอฟต์แวร์จะต้องกำหนดค่าต่างๆดังนี้

1. IPCop ในส่วน Green Interface จะกำหนด IP Address เป็น 192.168.100.254 เพื่อเป็น Default Gateway และ DNS Server ให้กับเครื่องลูกดังรูปที่ 3.3



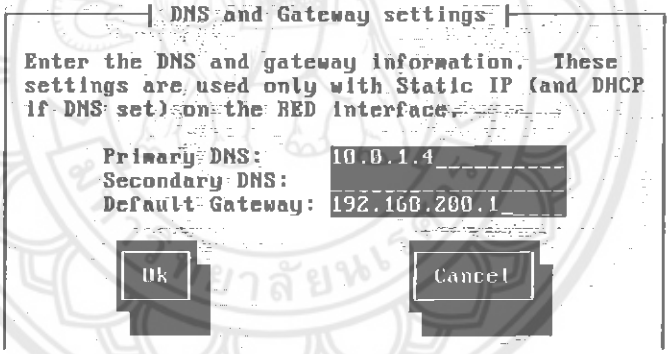
รูปที่ 3.3 แสดงการกำหนดค่าในส่วน Green Interface

ส่วน Red Interface จะกำหนดให้เป็นแบบ DHCP เพื่อให้ระบบส่ง IP Address มาทำให้สามารถเล่นอินเตอร์เน็ตได้ดังรูปที่ 3.4



รูปที่ 3.4 แสดงการกำหนดค่าในส่วน Red Interface

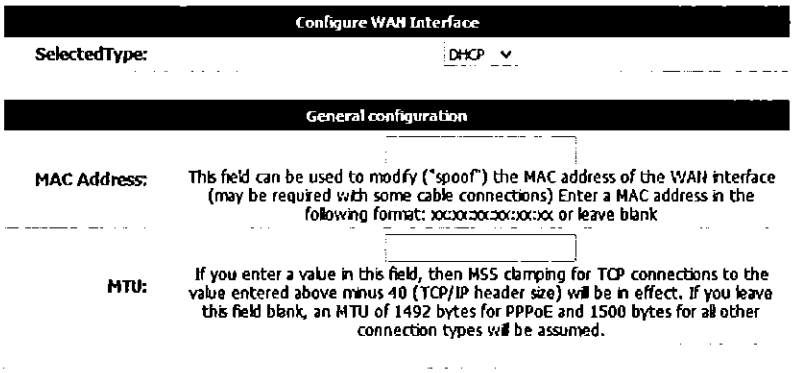
ในส่วนของ Default Gateway และ DNS Server ให้กำหนดตามแต่ละหอพักที่ใช้โดยในที่นี้ใช้ Default Gateway เป็น 192.168.200.1 และ DNS Server เป็น 10.0.1.4 ดังรูปที่ 3.5



รูปที่ 3.5 แสดงการกำหนดค่าในส่วน DNS Server และ Default Gateway

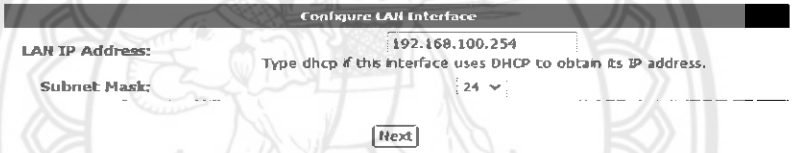
2. Netlimiter ซอฟต์แวร์ตัวนี้จะต้องทำการติดตั้งที่เครื่องลูกข่าย มีไว้เพื่อจัดการแบนด์วิดท์ภายในเครื่อง

3. PFSense จะทำการกำหนดการ์ดแลนใบที่หนึ่ง ที่เรียกว่าระบบ WAN ให้เป็นแบบ DHCP เพื่อให้ระบบส่ง IP Address มาทำให้สามารถเล่นอินเตอร์เน็ตได้ ดังรูปที่ 3.6



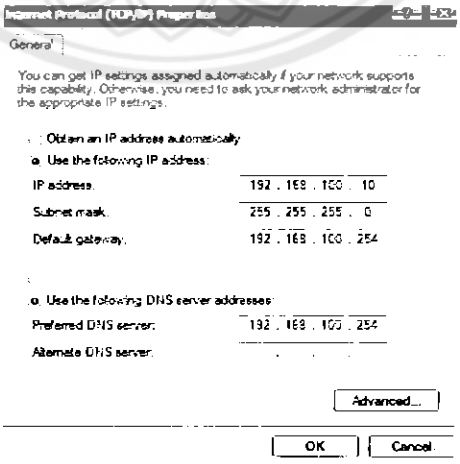
รูปที่ 3.6 แสดงการกำหนดค่าในส่วน WAN Interface

ส่วนการ์ดแลนใบที่สอง ที่เรียกว่าระบบ LAN กำหนด IP Address เป็น 192.168.100.254 เพื่อเป็น Default Gateway และ DNS Server ให้กับเครื่องลูกข่าย ดังรูปที่ 3.7



รูปที่ 3.7 แสดงการกำหนดค่าในส่วน LAN Interface

ในเครื่องลูกข่ายจะกำหนด IP Address อยู่ในช่วง 192.168.100.10 – 192.168.100.250 ในส่วน Default Gateway เป็น 192.168.100.254 และ DNS Server เป็น 10.0.1.4 ดังรูปที่ 3.8



รูปที่ 3.8 แสดงการกำหนดค่าต่างๆในเครื่องลูกข่าย

3.4 ออกแบบสำรวจการใช้งานอินเทอร์เน็ตของผู้จัดการหอพัก

แบบสอบถามการใช้อินเทอร์เน็ตของผู้จัดการหอพัก

ชื่อหอพัก .....

1. ชนิดของอินเทอร์เน็ตที่ใช้ภายในหอพัก

O Router ADSL O Software สำเร็จ

O Wireless LAN O อื่นๆ โปรดระบุ .....

2. จำนวนคอมพิวเตอร์ที่ต้องการใช้งานอินเทอร์เน็ตภายในหอพัก

O มี ..... เครื่อง O ไม่ทราบ

3. ต้นทุนในการติดตั้งการใช้งานอินเทอร์เน็ต

O ต่ำ O สูง

4. มีความรู้เกี่ยวกับระบบ Network

O มาก O น้อย

5. ความต้องการในการจัดการ Bandwidth (ความกว้างในการรับ-ส่งข้อมูล)

O ไม่จำกัด O จำกัด

6. มีปัญหาเกี่ยวกับการดาวน์โหลดไฟล์ชนิด P2P (Peer-to-Peer) เช่น Bit Torrent

O ไม่มี O มี

7. เก็บบันทึกข้อมูลในการใช้อินเทอร์เน็ต (Log)

O ไม่ต้องการ O ต้องการ

8. เข้าระบบโดยการใช้ User name และ Password

O ไม่ต้องการ O ต้องการ

ความต้องการของผู้จัดการหอ :

.....

.....

3.5 ออกแบบตารางเก็บผลการทดลอง

เก็บข้อมูลค่าดาวน์โหลด (Download) อัพโหลด (Upload) และ เวลาที่ใช้ในการเข้าเว็บไซต์ของทั้ง 3 ซอฟต์แวร์ โดยจะทำงานใน 2 รูปแบบ คือ

1. Block Port คือ การทดลองที่ใช้ซอฟต์แวร์เราเตอร์ ป้องกันการใช้โปรแกรมรับส่งข้อมูลผ่านระบบเครือข่ายแบบ P2P (Peer-To-Peer) เช่น บิต ทอร์เรนต์ ซึ่งจะทำการ Block Port ที่อยู่ในช่วง 1024 – 65535 เพื่อไม่ให้เกิดการรับส่งข้อมูลขณะทำการทดลอง

2. Bandwidth Shaping คือ การทดลองที่ใช้ซอฟต์แวร์เราเตอร์ กำหนดแบนด์วิดท์ในการรับส่งข้อมูล เช่น กำหนดความเร็วในการรับส่งข้อมูลผ่านระบบเครือข่ายแบบ P2P เพื่อไม่ให้รบกวนการทำงานของแอปพลิเคชั่น (Application) อื่นๆ

โดยนำ Block Port และ Bandwidth Shaping มาเปรียบเทียบกับ Uncondition

Uncondition คือ การทดลองการใช้อินเทอร์เน็ต ทั่วไปซึ่งไม่มีการใช้งาน โปรแกรมซอฟต์แวร์ในการจำกัดแบนด์วิดท์ (Bandwidth Shaping) และ ไม่มีการ Bock Port โดยปล่อยให้มีอิสระในการดาวน์โหลด (Download) และ อัพโหลด (Upload) จึงทำให้โปรแกรมบิต ทอร์เรนต์ (Bit Torrent) สามารถดาวน์โหลดได้เต็มที่

โดยได้ทำการทดลองกับ เว็บไซต์ (Web Site) จำนวน 10 เว็บไซต์ ได้แก่

1. http://www.youtube.com
2. http://www.hotmail.com
3. http://www.yahoo.com
4. http://www.teenee.com
5. http://www.kapook.com
6. http://www.facebook.com
7. http://www.nu.ac.th
8. http://www.hi5.com
9. http://www.sanook.com
10. http://www.thaitv3.com

และใช้ซอฟต์แวร์เราเตอร์ ในการทดลองจำนวน 3 ซอฟต์แวร์คือ IPCop, NetLimiter และ PFSense โดยทำการทดลองในแต่ละซอฟต์แวร์เป็นจำนวน 10 ครั้งต่อ 1 เว็บไซต์ แล้วรายงานผลเป็นค่าเฉลี่ยเปรียบเทียบค่าดาวน์โหลด และ ค่าอัพโหลดที่จำกัดโดยซอฟต์แวร์ และ เวลาที่ใช้ในการเข้าเว็บไซต์

ตารางที่ 3.1 ตารางบันทึกผลการทดลอง

ครั้งที่	Web Site	Download/Upload (Kb/s)			Time (Second)		
		Unconditon	Block Port	Bandwidth Shaping	Unconditon	Block Port	Bandwidth Shaping
1	www.youtube.com						
	www.hotmail.com						
	www.yahoo.com						
	www.teenee.com						
	www.kapook.com						
	www.facebook.com						
	www.nu.ac.th						
	www.hi5.com						
	www.sanook.com						
	www.thaitv3.com						
เฉลี่ย							

บทที่ 4
ผลการทดลองและวิเคราะห์ผลการทดลอง

4.1 ผลการทดลอง

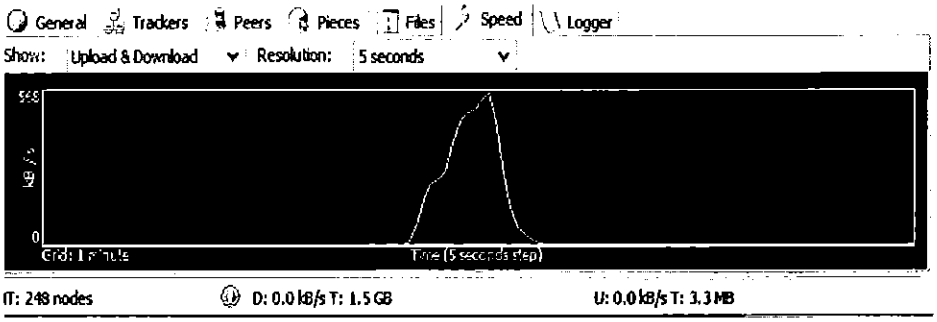
- **Uncondition**

รูปที่ 4.3 แสดงอัตราการดาวน์โหลดของโปรแกรม Bit Torrent (Uncondition)

Uncondition คือ การทดลองการใช้อินเทอร์เน็ตทั่วไป ซึ่งไม่มีการใช้งานโปรแกรมซอฟต์แวร์ในการจำกัดแบนด์วิดท์ และ ไม่มีการ Block Port โดยปล่อยให้มีอิสระในการดาวน์โหลด และ อัพโหลด จึงทำให้โปรแกรม Bit Torrent สามารถดาวน์โหลดได้เต็มที่ จากรูปแสดงค่าดาวน์โหลด และค่าอัพโหลด จะมีค่าที่สูงเพราะว่าปล่อยให้ดาวน์โหลดเต็มที่ ซึ่งจะรบกวนแอปพลิเคชั่นต่างๆ

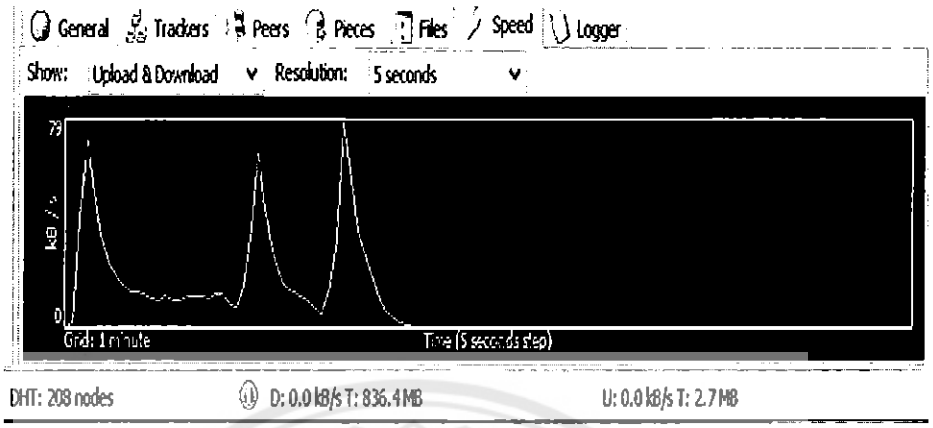
- **Block Port**

1. **IPCop**



รูปที่ 4.4 แสดงอัตราการดาวน์โหลดของโปรแกรม Bit Torrent โดยใช้ IPCop (Block Port)

2. PFSense

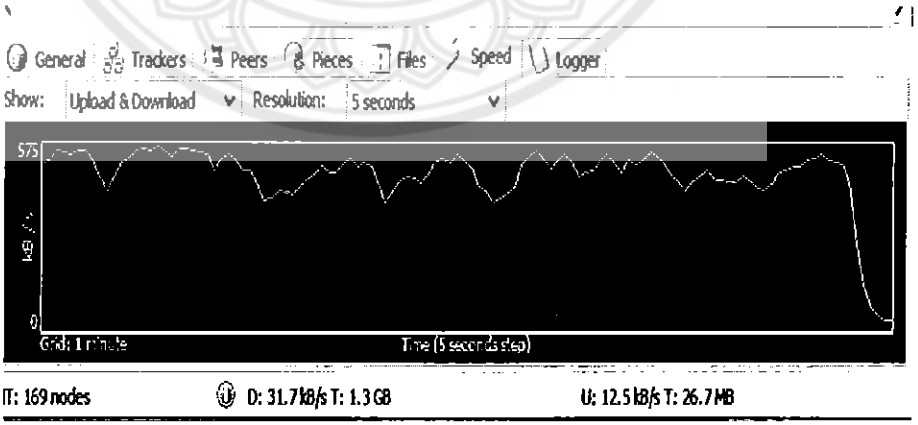


รูปที่ 4.5 แสดงอัตราการดาวน์โหลดของโปรแกรม Bit Torrent โดยใช้ PFSense **(Block Port)**

Block port คือ การทดลองที่ใช้ Software Router ในการ Block Port **ของไฟล์ประเภท P2P เช่น** Bit Torrent (จะไม่สามารถดาวน์โหลดไฟล์ได้) ซึ่งจะเห็นได้ว่าค่าดาวน์**โหลด และ ค่าอัพโหลด**จะมีค่าเป็นศูนย์ ดังภาพของ IPCop และ PFSense ส่วน NetLimiter จะไม่มี**คุณสมบัติในข้อนี้ จึงทำให้**ไม่สามารถที่จะทำการ Block Port ได้

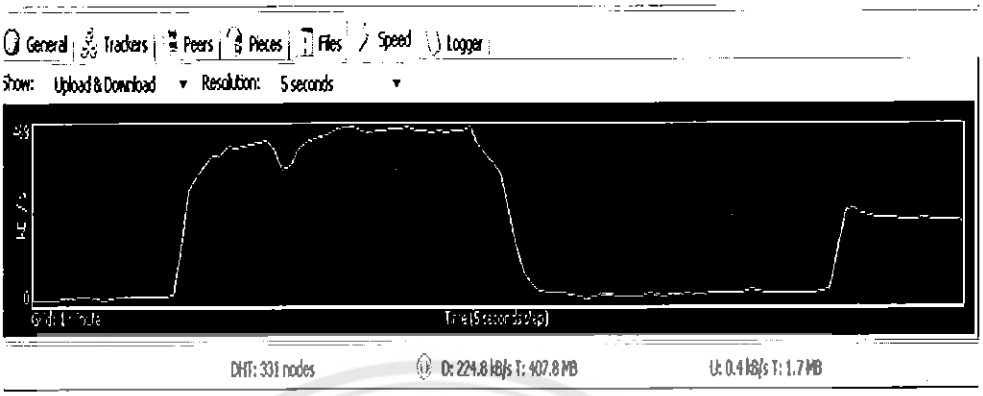
- **Bandwidth Shaping**

1. IPCop



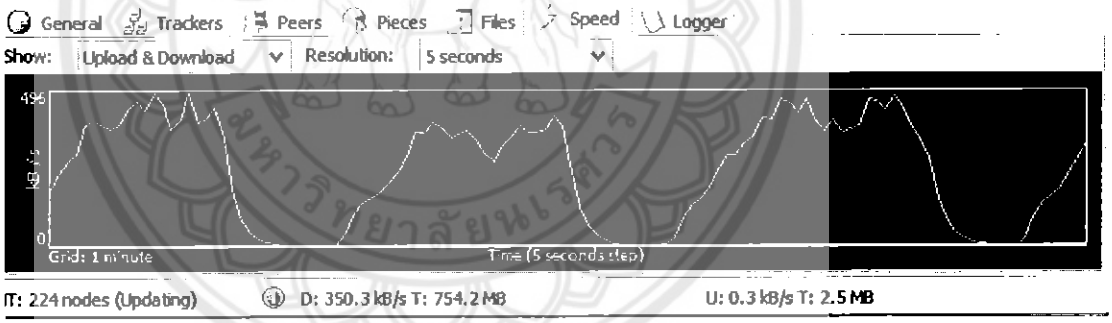
รูปที่ 4.6 แสดงอัตราการดาวน์โหลดของโปรแกรม Bit Torrent โดยใช้ IPCop (Bandwidth Shaping)

2. NetLimiter



รูปที่ 4.7 แสดงอัตราการดาวน์โหลดของโปรแกรม Bit Torrent โดยใช้ NetLimiter (Bandwidth Shaping)

3. PFSense

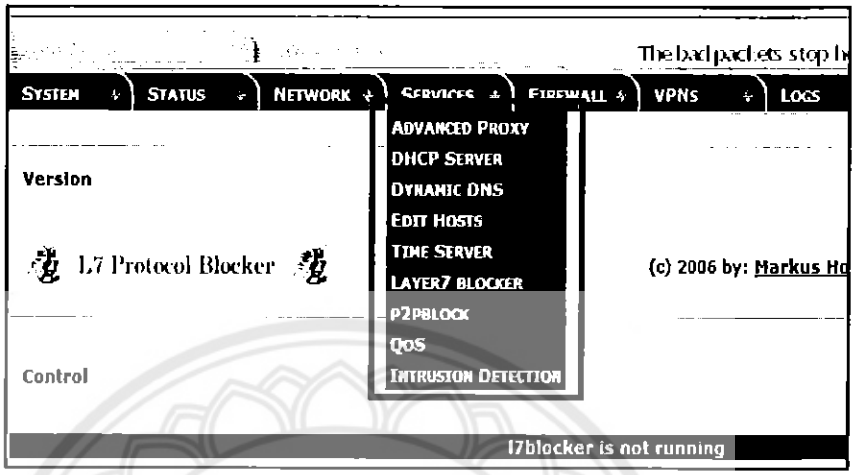


รูปที่ 4.8 แสดงอัตราการดาวน์โหลดของโปรแกรม Bit Torrent โดยใช้ PFSense (Bandwidth Shaping)

Bandwidth Shaping คือ การทดลองที่ใช้ Software Router กำหนดแบนด์วิดท์ในการรับส่งข้อมูล เช่น กำหนดความเร็วในการรับส่งข้อมูลผ่านระบบเครือข่ายแบบ P2P เพื่อไม่ให้รบกวนการทำงานของแอปพลิเคชั่นอื่นๆ ดังภาพ ทั้ง 3 ซอฟต์แวร์มีคุณสมบัติการ Bandwidth Shaping จะเห็นได้ว่า เมื่อเราใช้ วิธีนี้แล้ว ค่าดาวน์โหลด และ ค่าอัพโหลดจะไม่เกินค่าดาวน์โหลดที่กำหนด ซึ่งเป็นคุณสมบัติที่ใช้ในการจัดการแบนด์วิดท์ได้ดีในระดับหนึ่ง

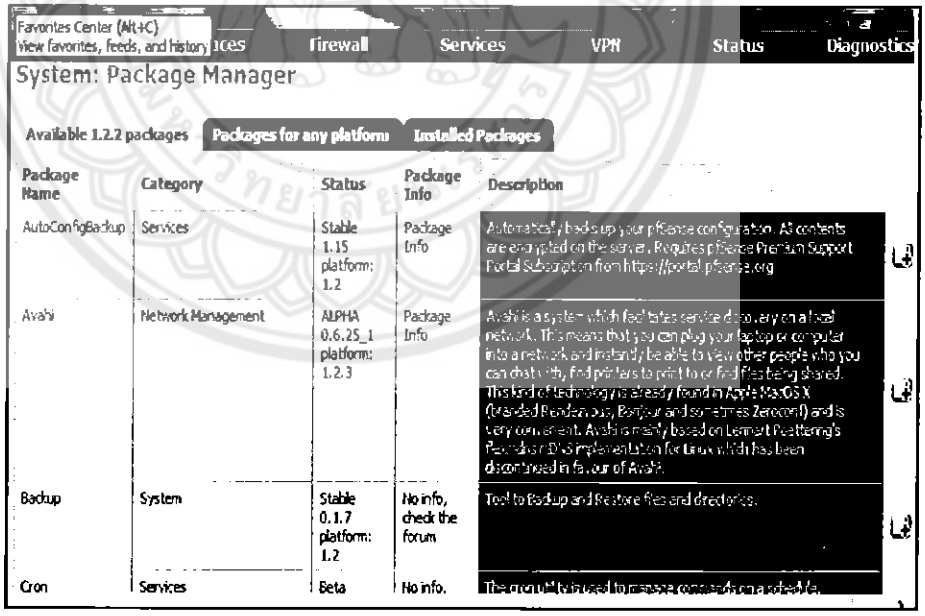
- **Application Support**

1. IPCop



รูปที่ 4.9 แสดง Application Support ของซอฟต์แวร์ IPCop (Add-on)

2. PFSense

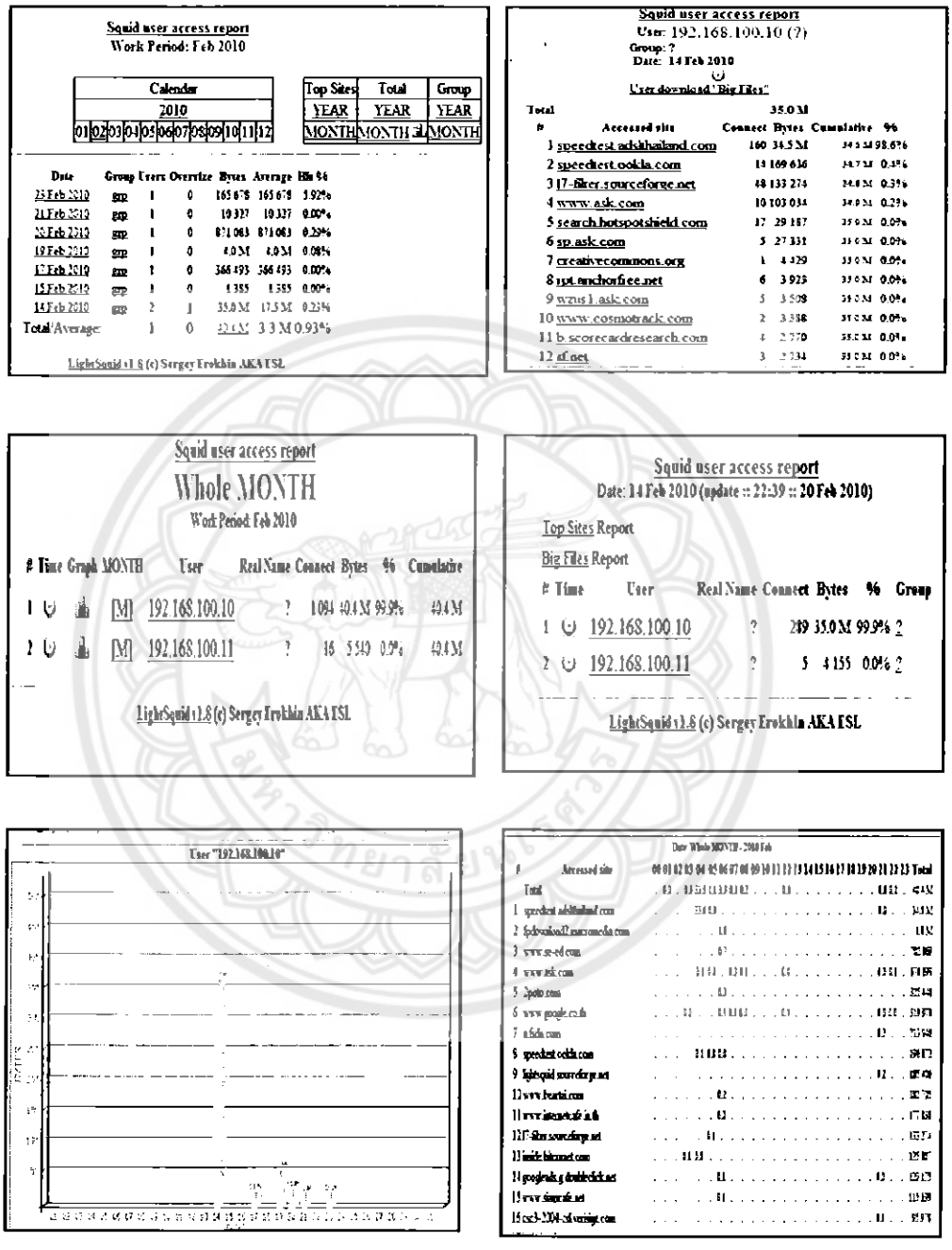


รูปที่ 4.10 แสดง Application Support ของซอฟต์แวร์ PFSense (Package)

IPCop และ PFSense มี Application Support ที่ใช้ในการทำงาน ซึ่งใน IPCop เรียกว่า Add-on ส่วนใน PFSense เรียกว่า Package ซึ่งใน NetLimiter นี้จะไม่มี Application Support

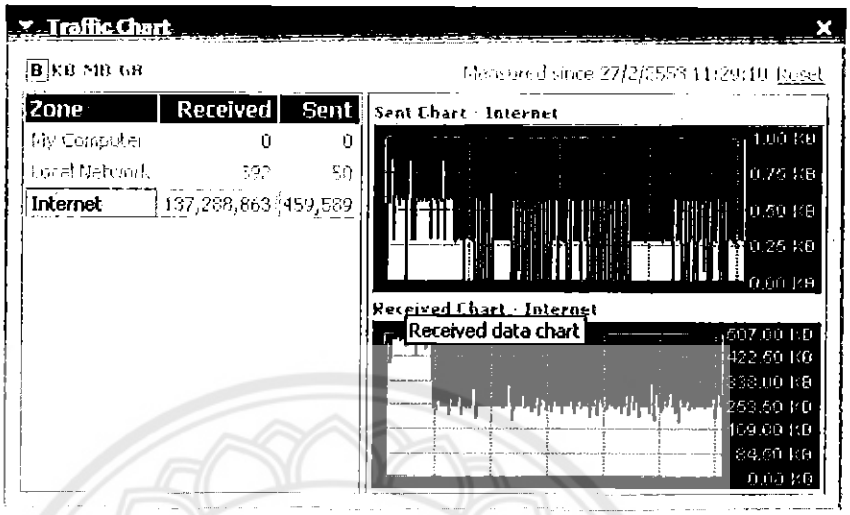
- **History Log**

1. IPCop



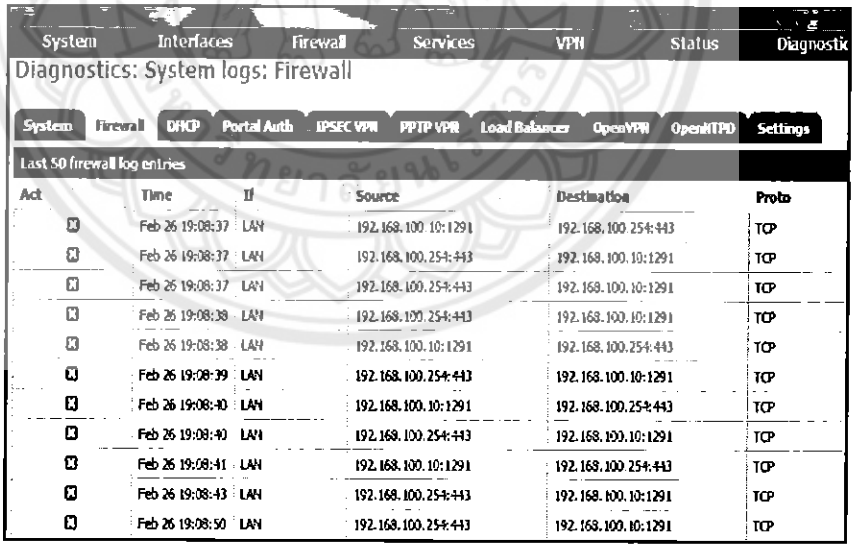
รูปที่ 4.11 แสดง History Log ของซอฟต์แวร์ IPCop

2. NetLimiter



รูปที่ 4.12 แสดง History Log ของซอฟต์แวร์ NetLimiter

3. PFSense



รูปที่ 4.13 แสดง History Log ของซอฟต์แวร์ PFSense

การเก็บ Log ซึ่งแต่ละซอฟต์แวร์มีคุณสมบัติการเก็บ Log ทั้งหมดโดย

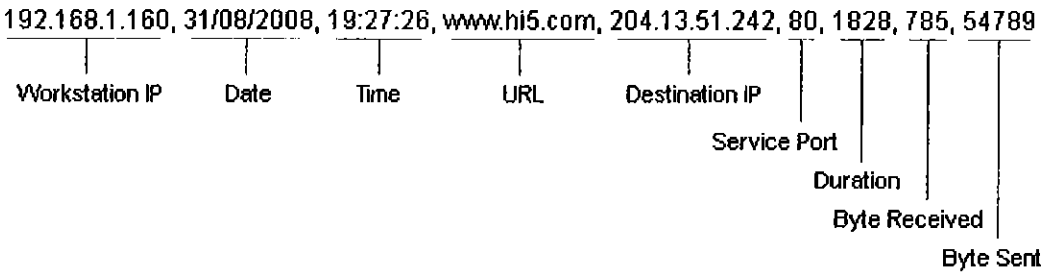
- IPCop มีคุณสมบัติที่เกี่ยวกับการเก็บ Log มาให้กับซอฟต์แวร์อยู่แล้ว แต่ยังไม่มีความละเอียดในการรายงานผลการใช้งานเพียงพอ แต่จะมี Add-on ชื่อ LightSquid ซึ่งทำหน้าที่เก็บ Log ทำให้ IPCop สามารถเก็บ Log ที่มีความละเอียดมากขึ้น

- NetLitmiter สามารถเก็บ Log ได้แต่ไม่มีความละเอียดพอ และ ไม่สามารถที่จะเพิ่มคุณสมบัติการเก็บ Log ที่ละเอียดได้มากกว่านี้ ซึ่งจะรายงานผลการใช้งานออกมาในลักษณะของกราฟ

- PFSense มีคุณสมบัติที่เกี่ยวกับการเก็บ Log มาให้กับซอฟต์แวร์อยู่แล้วแต่ยังไม่มีความละเอียดในการรายงานผลการใช้งานเพียงพอ แต่จะมี Package ชื่อ LightSquid ให้ดาวน์โหลดเพิ่มทำให้ประสิทธิภาพในการเก็บ Log ดีขึ้น

ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 บัญญัติให้ผู้ให้บริการต้องเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ไม่ต่ำกว่า 90 วัน "หากผู้ใดไม่ปฏิบัติ ต้องระวางโทษปรับไม่เกิน 500,000 บาท และ หากผู้ใดไม่ให้ความร่วมมือในการปฏิบัติตามต้องระวางโทษปรับไม่เกิน 200,000 บาท และ ต้องโทษปรับรายวันอีกไม่เกินวันละ 5,000 บาท จนกว่าจะปฏิบัติให้ถูกต้อง"

ระบบการจัดเก็บข้อมูล Log ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2550 สำหรับโรงเรียน หรือ หอพัก ที่มีการให้บริการอินเตอร์เน็ต ตามหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ ประเภท ข. ที่เป็นผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ต้องเก็บข้อมูลตามประกาศข้อ 5(1) ข. ถึง ค. ที่ต้องมีการอ้างถึงเวลาสากลรวมถึงการเก็บ Log file จากเครื่อง Server และ อุปกรณ์เครือข่าย (Network Device) ตามเจตนารมณ์ของกฎหมายเพียงแค่ให้สามารถระบุตัวตนที่แท้จริงของผู้กระทำผิดเท่านั้น



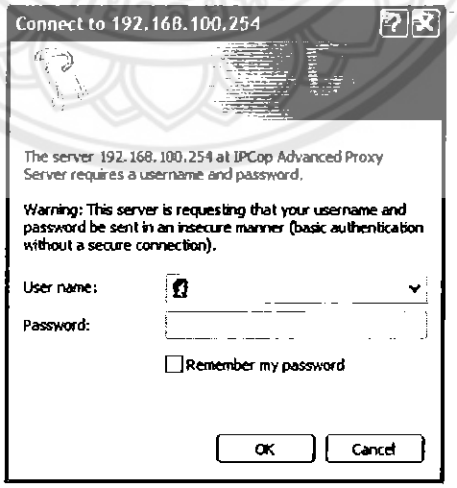
รูปที่ 4.14 ตัวอย่างการเก็บข้อมูล Log

สำหรับข้อมูล Log ที่ต้องจัดเก็บนั้นจะแตกต่างกันไปตาม Protocol ที่ใช้ในแต่ละบริการของหอพักนั้นๆ เช่น การใช้บริการอินเทอร์เน็ต หรือ การดาวน์โหลดไฟล์ผ่านระบบเครือข่ายแบบ P2P ก็จะเก็บเวลา และ วันที่ เป็นต้น โดยข้อมูล Log ที่ต้องมีการจัดเก็บจะประกอบไปด้วย

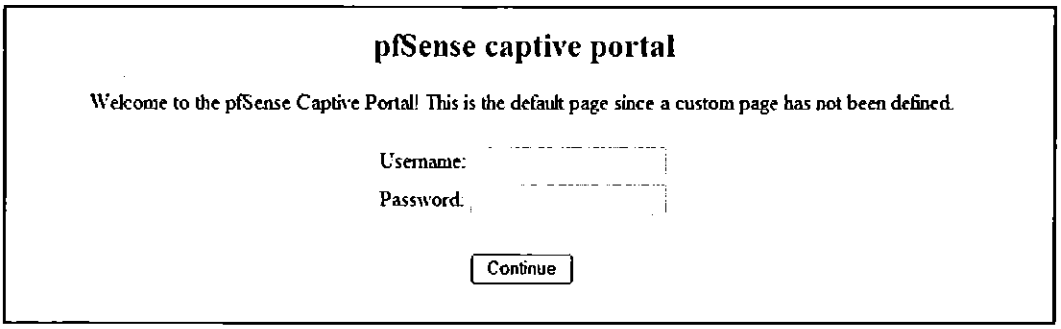
- แหล่งกำเนิด
- ต้นทาง ปลายทาง
- เส้นทาง
- เวลาและวันที่
- ปริมาณ
- ระยะเวลา
- ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์

จึงมีความจำเป็นที่ทุก ๆ หอพักที่อยู่ในฐานะของผู้ให้บริการจำเป็นต้องจัดหาอุปกรณ์ หรือเครื่องมือเพื่อให้รองรับกับ พรบ. ดังกล่าว ซึ่งเงื่อนไขสำคัญคือการจัดหาอุปกรณ์ที่มีราคาเหมาะสมกับขนาดของหอพัก

- Authentication



รูปที่ 4.15 แสดงหน้าต่างสำหรับ Login ของซอฟต์แวร์ IPCop



รูปที่ 4.16 แสดงหน้าต่างสำหรับ Login ของซอฟต์แวร์ PFSense

Authentication เป็นการกำหนดรูปแบบการตรวจสอบตัวเองของผู้ใช้งานในเครือข่ายโดยผู้ที่ต้องการจะเข้าอินเทอร์เน็ตจะต้องระบุชื่อผู้ใช้ และ รหัสผ่านของตัวเองจึงจะสามารถเข้าอินเทอร์เน็ตได้ ซึ่ง IPCop และ PFSense สามารถทำการ Authentication ได้ โดยชื่อผู้ใช้ และรหัสผ่านเดียวกันสามารถล็อกอิน (Login) ได้เพียงหนึ่ง IP Address ซึ่งถ้าหากนำชื่อผู้ใช้ไปใช้ใน IP Address อื่น IPCop จะไม่สามารถเข้าอินเทอร์เน็ตได้ ส่วน PFSense จะเข้าอินเทอร์เน็ตได้ แต่ IP Addressเดิมจะถูกตัดออกจากระบบอัตโนมัติ

4.2 วิเคราะห์ผลการทดลอง

หลังจากที่ได้ทดลองซอฟต์แวร์กับเว็บไซต์จำนวน 10 เว็บไซต์ โดยจำกัดแบนด์วิดท์สำหรับการดาวน์โหลดที่ 80% , 50% , 30% และ 10% และ รายงานผลเป็นค่าเฉลี่ย โดยการทดลองจะกำหนดเงื่อนไขในการใช้งานที่แตกต่างกันออกไปคือ มีการ Block Port, Bandwidth Shaping และ Uncondition (ไม่ได้ทำการ Block Port และ Bandwidth Shaping) โดยทั้ง 3 Software Router ให้ผลดังนี้

ตารางที่ 4.1 แสดงสรุปอัตราการ Download/Upload (Kb/s) และเวลาที่ใช้ในการเข้าเว็บไซต์ (Second) ของแต่ละซอฟต์แวร์

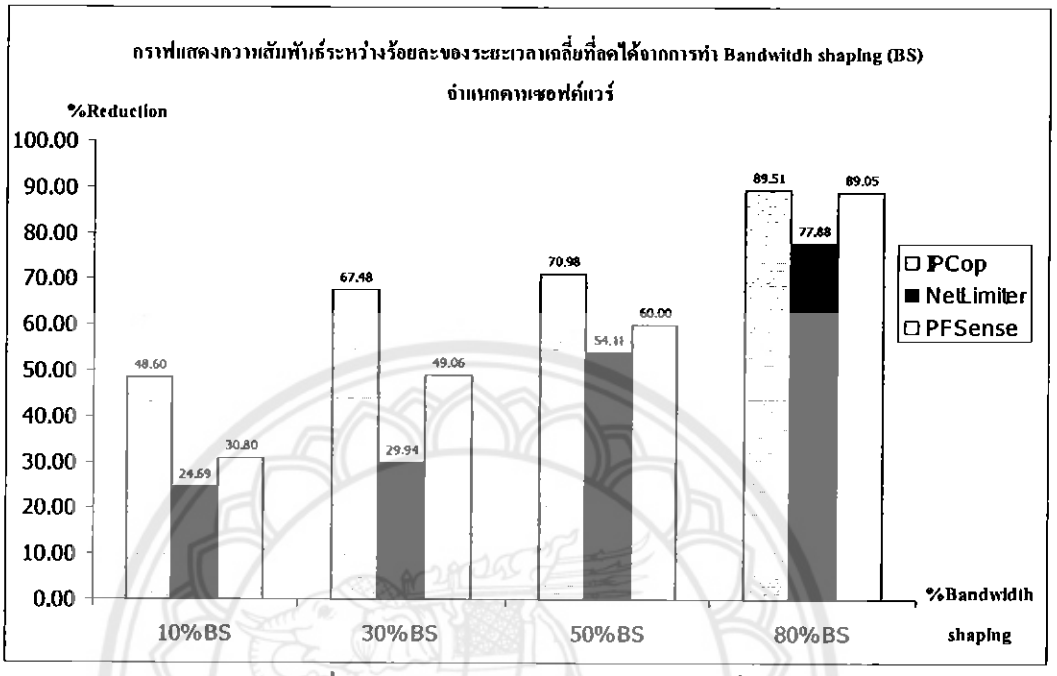
Sofeware Router	Download/Upload (Kb/s)			Time (second)		
	Uncondition	Block Port	Bandwidth Shaping	Uncondition	Block Port	Bandwidth Shaping
IPCop 80	516.26	0.00	42.99	9.5699	4.32	8.29
IPCop 50	473.23	0.00	28.45	6.7119	3.27	4.48
IPCop 30	519.22	0.00	14.19	5.2965	1.98	3.74
IPCop 10	473.23	0.00	5.61	4.573	1.89	2.44
NetLimiter 80	473.24	0.00	373.36	10.00	0.00	7.79
NetLimiter 50	491.99	0.00	258.11	10.12	0.00	5.48
NetLimiter 30	487.95	0.00	142.31	10.03	0.00	3.00
NetLimiter 10	488.13	0.00	47.36	10.11	0.00	2.50
PFSense 80	450.25	0.00	353.20	10.02	2.74	8.85
PFSense 50	447.04	0.00	241.55	10.37	1.95	6.22
PFSense 30	467.97	0.00	50.37	10.21	1.77	4.77
PFSense 10	443.60	0.00	22.88	9.85	1.54	2.83

ตารางที่ 4.2 แสดงร้อยละเฉลี่ยของอัตราการ Download/Upload (Kb/s) เฉลี่ย และเวลาที่ใช้ในการเข้าเว็บไซต์ (Second) เฉลี่ย

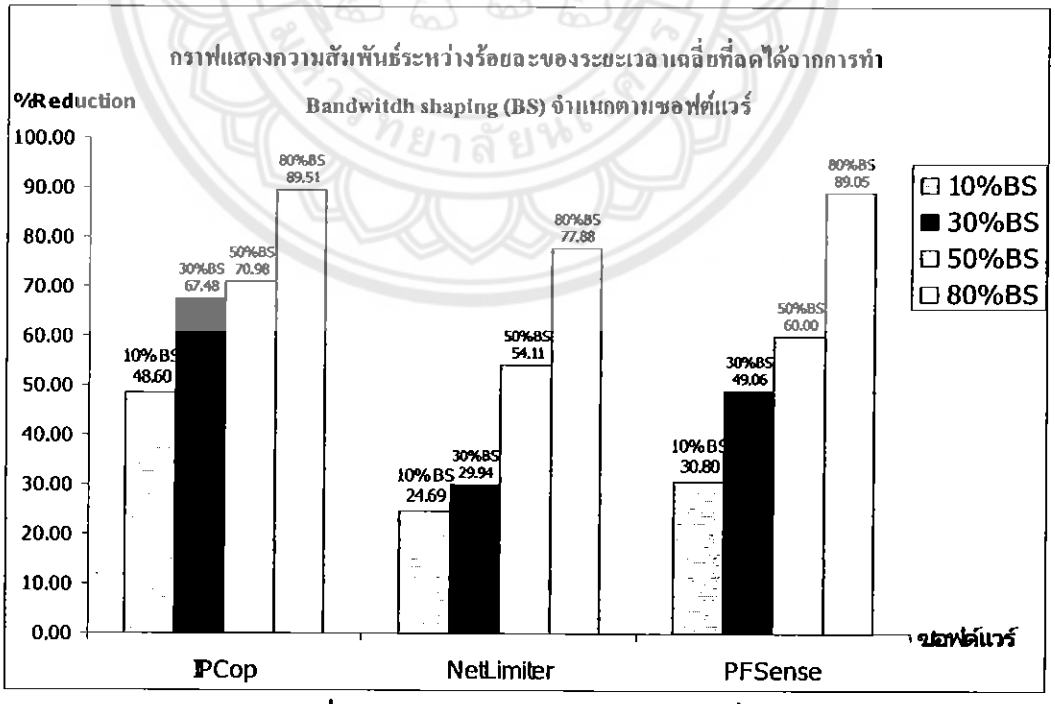
Software Router	อัตราเวลาเฉลี่ยคิดเป็นร้อยละ
	Bandwidth Shaping
IPCop 80%	89.51
IPCop 50%	70.98
IPCop 30%	67.48
IPCop 10%	48.60
NetLimiter 80%	77.88
NetLimiter 50%	54.11
NetLimiter 30%	29.94
NetLimiter 10%	24.69
PFSense 80%	89.05
PFSense 50%	60.00
PFSense 30%	49.06
PFSense 10%	30.80

จากตารางจะพบว่าเมื่อจำกัดแบนด์วิดท์สำหรับการดาวน์โหลดที่ 80%, 50%, 30% และ 10% ความเร็วในการเข้าถึงเว็บไซต์โดยวิธีการ Block Port จะสามารถเข้าถึงเว็บไซต์ได้ไวที่สุด (ยกเว้น NetLimiter ซึ่งไม่สามารถทำการ Block Port ได้) รองลงมาคือการจำกัดแบนด์วิดท์โดยเมื่อจำกัดแบนด์วิดท์ที่ 80% จะส่งผลให้ความเร็วในการเข้าเว็บไซต์ประมาณ 80% และ เมื่อจำกัดแบนด์วิดท์ที่ 50%, 30% และ 10% จะส่งผลให้ความเร็วในการเข้าเว็บไซต์ลดลงตามลำดับ ส่วนถ้าไม่ได้ทำการ Block Port และจำกัดแบนด์วิดท์จะมีความเร็วในการเข้าถึงเว็บไซต์ช้าที่สุด

จากผลการทดลองข้างต้น สามารถนำมาทำกราฟได้ดังนี้



รูปที่ 4.17 กราฟแสดงความสัมพันธ์แบบที่ 1



รูปที่ 4.18 กราฟแสดงความสัมพันธ์แบบที่ 2

บทที่ 5
สรุปและข้อเสนอแนะ

5.1 สรุปผลการทดลอง

จากการทดลอง และ สรุปผลการทดลอง สามารถที่จะแสดงข้อเปรียบเทียบของแต่ละซอฟต์แวร์เราท์เตอร์ (Software Router) ได้ดังตารางต่อไปนี้

ตารางที่ 5.1 เปรียบเทียบคุณสมบัติการทำงานของแต่ละซอฟต์แวร์เราท์เตอร์

No.	Feature	IPCop	NetLimiter	PFSense
1	File Size	45.9 MB	2.8 MB	49.1 MB
2	OS Platforms	Linux	Windows 2000, XP, Vista	FreeBSD
3	User Friendly	✓	✓	✓
4	Block Port	✓	✗	✓
5	Bandwidth Shaping	✓	✓	✓
6	Application Support	Add-on	✗	Package
7	History Log	✓	✓	✓
8	Authentication	✓	✗	✓
9	License	Free	- NetLimiter 2 Monitor (Shareware) - NetLimiter 2 Lite - NetLimiter 2 Pro	Free

จากตารางสามารถอธิบายแต่ละ Feature ได้ดังนี้

1. File Size คือ ขนาดของไฟล์ที่ใช้ในการติดตั้ง ซึ่งจะเห็นว่า ซอฟต์แวร์ทั้ง 3 ตัวนี้มีขนาดไฟล์ที่ไม่ใหญ่มากนัก

2. OS Platforms คือ ซอฟต์แวร์ (Software) ทั้ง 3 สามารถทำงานได้บนระบบปฏิบัติการใดได้บ้าง

3. User Friendly คือ ผู้ใช้สามารถกำหนดค่าต่างๆได้ง่าย ซึ่งซอฟต์แวร์ IPCop และ PFSense จะกำหนดค่าต่างๆผ่านทางเว็บไซต์ ส่วน NetLimiter จะกำหนดค่าต่างๆบน GUI (Graphical User Interface)

4. Block Port คือ ผู้ใช้สามารถปิดพอร์ต (Port) ที่ไม่ต้องการให้ใช้งาน ซึ่งซอฟต์แวร์ IPCop สามารถ Block Port ได้โดยการใช้ Add-on เรียกว่า p2pblock ส่วน PFSense สามารถ Block Port ได้โดยการตั้งกฎของไฟร์วอลล์ (Firewall) เพื่อปิดพอร์ตที่ไม่ต้องการใช้งานส่วน NetLimiter ไม่มีคุณสมบัติในการ Block Port

5. Bandwidth Shaping คือ ผู้ใช้สามารถจำกัดแบนด์วิดท์ในการดาวน์โหลด (Download) ได้ ซึ่ง IPCop สามารถจำกัดแบนด์วิดท์ ได้โดยการใช้ Add-on เรียกว่า QoS ส่วน NetLimiter และ PFSense สามารถจำกัดแบนด์วิดท์ได้โดยการกำหนดกฎ

6. Application Support คือ คุณสมบัติเพิ่มเติมที่ทำให้แต่ละซอฟต์แวร์ทำงานได้มีประสิทธิภาพมากขึ้น เช่น ใน IPCop เรียกว่า Add-on และ ใน PFSense เรียกว่า Package

7. History Log รายงานผลการใช้งานในแต่ละครั้งของแต่ละซอฟต์แวร์

8. Authentication เป็นการกำหนดรูปแบบการตรวจสอบตัวเองของผู้ใช้งานในเครือข่าย โดยผู้ที่ต้องการจะเข้าสู่เว็บไซต์จะต้องระบุ ชื่อผู้ใช้ (Username) และ รหัสผ่าน (Password) ของตัวเอง จึงจะสามารถเข้าสู่เว็บไซต์ได้ ใน IPCop และ PFSense สามารถทำ Authentication ได้ ส่วนใน NetLimiter ไม่สามารถทำได้

9. License ใน IPCop และ PFSense ทำงานบนระบบปฏิบัติการลินุกซ์ (Linux Operating System)ซึ่ง เป็น Opensource จึงสามารถใช้งานได้ฟรี ส่วนใน NetLimiter มีอยู่ 3 เวอร์ชั่น ซึ่งเวอร์ชั่นที่ใช้ในการทดลอง คือ NetLimiter 2 Pro ซึ่งเป็น Shareware ส่วน NetLimiter 2 Monitor และ NetLimiter 2 Lite ต้องเสียค่า License จึงจะใช้งานได้

ตารางที่ 5.2 เปรียบเทียบการเก็บ Log ของแต่ละซอฟต์แวร์เพื่อให้สอดคล้องกับ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2550

ข้อมูล Log	Software Router		
	IPCop	NetLimiter	PFSense
- แหล่งกำเนิด	✗	✗	✗
- ต้นทาง ปลายทาง	✓	✗	✓
- เส้นทาง	✓	✗	✓
- เวลาและวันที่	✓	✓	✓
- ปริมาณ	✓	✓	✗
- ระยะเวลา	✓	✗	✗
- ชนิดของบริการอื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์	✗	✗	✗

จากตารางสามารถอธิบายข้อมูล Log ได้ดังนี้

1. แหล่งกำเนิด คือ ข้อมูลที่ระบุตัวตนของผู้ใช้ โดยผู้จัดการหอพักควรทำการจดชื่อผู้ใช้ และ IP Address ของผู้ใช้เพื่อให้รองรับ พ.ร.บ. ฉบับนี้
2. ต้นทาง ปลายทาง คือ หมายเลข IP Address หรือ MAC Address
3. เส้นทาง คือ การใช้งานผ่าน Services เช่น www
4. เวลาและวันที่ คือ เวลาและวันที่ในการเข้าใช้งานอินเทอร์เน็ต (Internet)
5. ปริมาณ คือ ปริมาณในการเข้าใช้งานอินเทอร์เน็ต
6. ระยะเวลา คือ ระยะเวลาในการเข้าใช้งานอินเทอร์เน็ต
7. ชนิดของบริการอื่นๆที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ คือ การใช้แอปพลิเคชั่นอื่นๆ

จากการทดลองการใช้งานของซอฟต์แวร์เราท์เตอร์ จำนวน 3 ซอฟต์แวร์โดยวิธีการเปรียบเทียบวิเคราะห์จากค่าดาวน์โหลด อัพโหลด (Upload) และ เวลาเฉลี่ยที่ใช้ในการเข้าเว็บไซต์ (Web Site) จากการทำงานทั้ง 3 รูปแบบ และ ติดตามผลที่ได้จากการตั้งค่าการดาวน์โหลด อัพโหลด ที่ส่งผลต่อเวลาในการเข้าเว็บไซต์ หลังจากทำการทดลองของทั้ง 3 ซอฟต์แวร์ ใน 3 วิธีการทดลองแล้ว พบว่า ผู้ใช้สามารถที่จะกำหนดแบนด์วิดท์ได้ และ ช่วยลดปัญหา เมื่อมีการรับส่งไฟล์ประเภท

บิต ทอร์เรนต์ (Bit Torent) ได้ดี ซึ่งข้อผิดพลาดที่เกิดขึ้นจากการดาวน์โหลด อัพโหลดที่คลาดเคลื่อน เมื่อพิจารณาจากค่าดาวน์โหลด อัพโหลด และ อัตราเวลาเฉลี่ยที่ใช้ในการเข้าเว็บไซต์ขณะทำการดาวน์โหลด อัพโหลด แล้ว สาเหตุที่ทำให้เกิดข้อผิดได้หลายประการเช่น ขณะทำการทดลองมีการใช้อินเทอร์เน็ตในการเล่นเกมส์ หรือ ขณะทำการทดลองความเร็วของอินเทอร์เน็ตวิ่งไม่สม่ำเสมอ ทำให้เกิดการคลาดเคลื่อนของผลการทดลองได้

โดยสามารถสรุปผลการทดลองออกมาได้ดังตารางที่ 5.5

ตารางที่ 5.3 แสดงค่าเฉลี่ยอัตราการ Download/Upload (Kb/s) และ เวลาที่ใช้ในการเข้าเว็บไซต์ (Second) ของ IPCop

Sofeware Router	Download/Upload (Kb/s)			Time (second)		
	Uncondition	Block Port	Bandwidth Shaping	Uncondition	Block Port	Bandwidth Shaping
IPCop 80%	516.26	0.00	42.99	9.5699	4.32	8.29
IPCop 50%	473.23	0.00	28.45	6.7119	3.27	4.48
IPCop 30%	519.22	0.00	14.19	5.2965	1.98	3.74
IPCop 10%	473.23	0.00	5.61	4.573	1.89	2.44

ตารางที่ 5.4 แสดงค่าเฉลี่ยอัตราการ Download/Upload (Kb/s) และ เวลาที่ใช้ในการเข้าเว็บไซต์ (Second) ของ NetLimiter

Sofeware Router	Download/Upload (Kb/s)			Time (second)		
	Uncondition	Block Port	Bandwidth Shaping	Uncondition	Block Port	Bandwidth Shaping
NetLimiter 80%	473.24	0.00	373.36	10.00	0.00	7.79
NetLimiter 50%	491.99	0.00	258.11	10.12	0.00	5.48
NetLimiter 30%	487.95	0.00	142.31	10.03	0.00	3.00
NetLimiter 10%	488.13	0.00	47.36	10.11	0.00	2.50

ตารางที่ 5.5 แสดงค่าเฉลี่ยอัตราการ Download/Upload (Kb/s) และ เวลาที่ใช้ในการเข้าเว็บไซต์ (Second) ของ PFSense

Sofeware Router	Download/Upload (Kb/s)			Time (second)		
	Uncondition	Block Port	Bandwidth Shaping	Uncondition	Block Port	Bandwidth Shaping
PFSense 80%	450.25	0.00	353.20	10.02	2.74	8.85
PFSense 50%	447.04	0.00	241.55	10.37	1.95	6.22
PFSense 30%	467.97	0.00	50.37	10.21	1.77	4.77
PFSense 10%	443.60	0.00	22.88	9.85	1.54	2.83

ตารางที่ 5.6 แสดงร้อยละของเปรียบเทียบการใช้เวลาเฉลี่ยที่ใช้ในการเข้าเว็บไซต์

Software Router	Uncondition เทียบกับ Bandwidth Shaping
IPCop 80%	86.3
IPCop 50%	70.56
IPCop 30%	66.77
IPCop 10%	53.41
NetLimiter 80%	77.88
NetLimiter 50%	54.11
NetLimiter 30%	29.44
NetLimiter 10%	24.69
PFSense 80%	88.39
PFSense 50%	60.00
PFSense 30%	44.69
PFSense 10%	28.73

สรุป

จากการทดลองนี้สามารถแก้ปัญหาตามหอพักได้โดยวิธีดังต่อไปนี้

1. **ใช้วิธี** Block Port **จะสามารถเข้าถึงเว็บไซต์ได้ไวที่สุด (ยกเว้น** NetLimiter **ซึ่งไม่สามารถทำการ** Block Port **ได้)**

2. **ใช้วิธี** Bandwidth Shaping **โดยแยกตามแต่ละ** Software Router **ได้ดังนี้**

- IPCop **จำกัดความเร็วในการดาวน์โหลดที่ 80% ทำให้สามารถเข้าเว็บไซต์ได้ไวขึ้นคิดเป็น 86.3%**

- IPCop **จำกัดความเร็วในการดาวน์โหลดที่ 50% ทำให้สามารถเข้าเว็บไซต์ได้ไวขึ้นคิดเป็น** 70.56%

- IPCop **จำกัดความเร็วในการดาวน์โหลดที่** 30% **ทำให้สามารถเข้าเว็บไซต์ได้ไวขึ้นคิดเป็น** 66.77%

- IPCop **จำกัดความเร็วในการดาวน์โหลดที่** 10% **ทำให้สามารถเข้าเว็บไซต์ได้ไวขึ้นคิดเป็น** 53.41%

- NetLimiter **จำกัดความเร็วในการดาวน์โหลดที่** 80% **ทำให้สามารถเข้าเว็บไซต์ได้ไวขึ้นคิดเป็น** 77.88%

- NetLimiter **จำกัดความเร็วในการดาวน์โหลดที่** 50% **ทำให้สามารถเข้าเว็บไซต์ได้ไวขึ้นคิดเป็น** 54.11%

- NetLimiter **จำกัดความเร็วในการดาวน์โหลดที่** 30% **ทำให้สามารถเข้าเว็บไซต์ได้ไวขึ้นคิดเป็น** 29.44%

- NetLimiter **จำกัดความเร็วในการดาวน์โหลดที่** 10% **ทำให้สามารถเข้าเว็บไซต์ได้ไวขึ้นคิดเป็น** 24.69%

- PFSense **จำกัดความเร็วในการดาวน์โหลดที่** 80% **ทำให้สามารถเข้าเว็บไซต์ได้ไวขึ้นคิดเป็น** 88.39%

- PFSense **จำกัดความเร็วในการดาวน์โหลดที่** 50% **ทำให้สามารถเข้าเว็บไซต์ได้ไวขึ้นคิดเป็น** 60.00%

- PFSense **จำกัดความเร็วในการดาวน์โหลดที่** 30% **ทำให้สามารถเข้าเว็บไซต์ได้ไวขึ้นคิดเป็น** 44.69%

- PFSense **จำกัดความเร็วในการดาวน์โหลดที่** 10% **ทำให้สามารถเข้าเว็บไซต์ได้ไวขึ้นคิดเป็น** 28.73%

5.2 สถานการณ์และความต้องการของผู้จัดการหอพัก

จากผลการทดลอง และ การวิเคราะห์ผลการทดลอง สามารถแนะนำให้ผู้จัดการหอพักเลือกใช้ซอฟต์แวร์ได้ดังนี้

1. สถานการณ์ : ผู้จัดการหอพักต้องการประหยัดค่าใช้จ่าย ไม่มีความรู้เกี่ยวกับการจัดการแบนด์วิดท์ และ มีปัญหาเกี่ยวกับผู้ใช้ทำการดาวน์โหลดไฟล์ชนิด P2P (Peer-to-Peer)

เลือกใช้ซอฟต์แวร์ : ได้ทั้ง IPCop และ PFSense เนื่องจากทั้งสองซอฟต์แวร์ทำงานบนระบบปฏิบัติการลินุกต์ ซึ่งเป็น Opensource และ มีการกำหนดค่าผ่านเว็บไซต์ทำให้ง่ายต่อการใช้งาน ซึ่งโปรแกรมทั้งสองตัวนี้สามารถแก้ปัญหาในเรื่องการดาวน์โหลดไฟล์ชนิด P2P โดยมีให้เลือก 2 วิธีคือ

- สามารถที่จะทำการ Block Port ของการดาวน์โหลดไฟล์ชนิด P2P ซึ่งวิธีนี้จะทำให้ผู้ใช้ไม่สามารถดาวน์โหลดไฟล์ชนิด P2P ได้ แต่จะมีข้อเสียคือผู้ใช้จะรู้สึกอึดอัด
- สามารถที่จะทำการจำกัดความเร็วในการใช้งานของแต่ละเครื่อง วิธีนี้จะทำให้ผู้ใช้สามารถดาวน์โหลดไฟล์ชนิด P2P ได้ โดยจะดาวน์โหลดได้ไม่เกินความเร็วที่จำกัดไว้ในแต่ละเครื่องซึ่งจะทำให้ไม่รบกวนการเข้าเว็บไซต์ของผู้ใช้คนอื่นๆ แต่ถ้าผู้จัดการหอพักต้องการที่จะจำกัดความเร็วของแต่ละแอปพลิเคชั่น (Application) ควรเลือกใช้ซอฟต์แวร์ IPCop เนื่องจาก มี Add-on ที่สามารถจำกัดความเร็วในการใช้งานของแอปพลิเคชั่นต่างๆได้

2. สถานการณ์ : ผู้จัดการหอต้องการกำหนดชื่อ และ รหัสผ่านของผู้ใช้ เพื่อเข้าใช้งานอินเทอร์เน็ต

เลือกใช้ซอฟต์แวร์ : ได้ทั้ง IPCop และ PFSense เนื่องจากสามารถทำการ Authentication ได้โดยชื่อผู้ใช้ และ รหัสผ่านเดียวกันสามารถล็อกอิน (Login) ได้เพียงหนึ่ง IP Address ซึ่งถ้าหากนำชื่อผู้ใช้ไปใช้ใน IP Address อื่น IPCop จะไม่สามารถเข้าอินเทอร์เน็ตได้ ส่วน PFSense จะเข้าอินเทอร์เน็ตได้ แต่ IP Address เดิมจะถูกตัดออกจากระบบอัตโนมัติ

3. สถานการณ์ : ผู้จัดการหอต้องการเก็บข้อมูล Log เพื่อรองรับพ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

เลือกใช้ซอฟต์แวร์ : IPCop เนื่องจากมีคุณสมบัติที่เกี่ยวกับการเก็บ Log มาให้กับซอฟต์แวร์อยู่แล้ว แต่ยังไม่มีความละเอียดในการรายงานผลการใช้งานเพียงพอ แต่จะมี Add-on ชื่อ LightSquid ซึ่งทำหน้าที่เก็บ Log ทำให้ IPCop สามารถเก็บ Log ได้ตรงตามพ.ร.บ. ว่าด้วยการกระทำความผิด

เกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ทั้งนี้ IPCop ยังไม่มีคุณสมบัติในการระบุตัวตนของผู้ใช้ ดังนั้น ผู้จัดการหอพักควรทำการจดชื่อผู้ใช้ และ IP Address ของผู้ใช้เพื่อให้รองรับกับพ.ร.บ.ฉบับนี้

5.3 ปัญหาและแนวทางแก้ไข

1. คณะผู้ทดลองมีความรู้เกี่ยวกับระบบปฏิบัติการลีนุกซ์ ไม่เพียงพอจึงทำให้เสียเวลาในการศึกษาเป็นเวลานาน สามารถแก้ได้โดยทำการศึกษาเกี่ยวกับระบบปฏิบัติการลินุกซ์ให้เข้าใจ

2. คณะผู้ทดลองมีความรู้เกี่ยวกับระบบโครงข่าย (Network) ไม่เพียงพอจึงทำให้เสียเวลาในการศึกษาเป็นเวลานาน สามารถแก้ได้โดยทำการศึกษาเกี่ยวกับระบบ Network ให้เข้าใจ

3. มีปัญหาเกี่ยวกับไฟร์วอลล์ของ โปรแกรมป้องกันไวรัส NOD32 จึงทำให้เสียเวลาในการตั้งค่า สามารถแก้ได้โดยปิดไฟร์วอลล์ (Firewall) ของโปรแกรมป้องกันไวรัส NOD32 ก่อน

4. ปัญหาเกี่ยวกับอินเทอร์เน็ตของหอพัก เนื่องจากมีการแบ่งสัญญาณอินเทอร์เน็ตกับผู้ใช้อื่น ทำให้สัญญาณอินเทอร์เน็ตที่ใช้ในการทดลองจึงไม่เสถียรเท่ากันตลอดการทดลอง ทำให้การทดลองไม่สามารถเปรียบเทียบระหว่างกลุ่มเพื่อระบุข้อดี ข้อเสียของแต่ละซอฟต์แวร์ได้

5.4 แนวทางการพัฒนาในอนาคต

1. สามารถนำเอาข้อมูลการใช้งานอินเทอร์เน็ตมาวิเคราะห์ถึงความต้องการใช้งานของลูกข่ายได้ และ ประยุกต์ใช้ซอฟต์แวร์ให้มีความเหมาะสมกับรูปแบบการใช้งาน

2. สามารถศึกษา และ พัฒนาซอฟต์แวร์อื่นๆ ที่ทำงานคล้ายกับ Software Router ที่ใช้ในการทดลองเพื่อนำผลมาวิเคราะห์เปรียบเทียบ และ หาซอฟต์แวร์ที่เหมาะสม

3. มีการศึกษาเปรียบเทียบในระบบที่ควบคุมที่มีความเสถียรกว่าอินเทอร์เน็ตหอพัก เพื่อให้ผลที่ได้มีความน่าเชื่อถือ และ ความคลาดเคลื่อนระหว่างกลุ่มน้อยลง

เอกสารอ้างอิง

[1] เอกชัย ศรีปทุมภรณ์ . **Bandwidth Management บริหารโครงข่ายอย่างมีประสิทธิภาพด้วยตัวเอง. กรุงเทพมหานคร: บริษัท** Provision จำกัด

[2] **พันจันทร์ ธนวัฒนเสถียร .โหลดมันส์...ไม่ยั้งกับ Bit Torrent. กรุงเทพมหานคร : บริษัท** Successmedia จำกัด

[3] **สถิต เรียนพิศ .ติดตั้งและใช้งาน IPCop . กรุงเทพมหานคร : บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน)**

[4] ผศ.พ.ต.ต.ดร. ดนุวศิน เจริญ. "**Management Information Systems.**" [Online].Available : http://y28.wikidot.com/term- paper-group1-50

[5] "**เทคนิคการใช้ Proxy Log เพื่อทำการแสดงชื่อ User.**" [Online]. Available : http://www.linuxthai.org/ forum/index.php?topic=940.0

[6] "**Squid คืออะไร.**" [Online]. Available : http://www.cpe.rmuti.ac.th/ webbroad2/ index.php?topic=976.0

[7] "**LightSquid.**" [Online]. Available : http://lightsquid.sourceforge.net/

[8] "**L7-filter Supported Protocols.**" [Online]. Available : http://www.bcoms.net/ dictionnary/detail.asp?id=416. 2009.

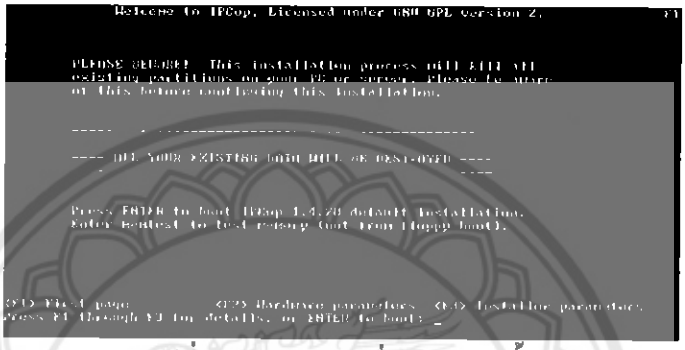
[9] "**การติดตั้ง PFSense Firewall.**" [Online]. Available : http://www.laontalk.com/2009/01/15/

[10] "**คู่มือ Ubuntu Server.**" [Online]. Available : http://linux.sothorn.org/node/356.

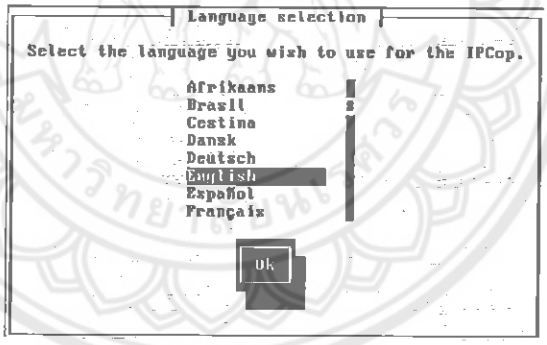
ภาคผนวก ก.

การติดตั้งโปรแกรม Software Router

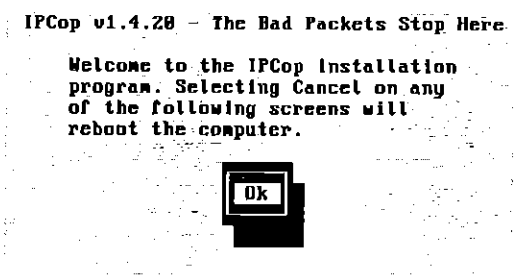
1. การติดตั้งโปรแกรม IPCop



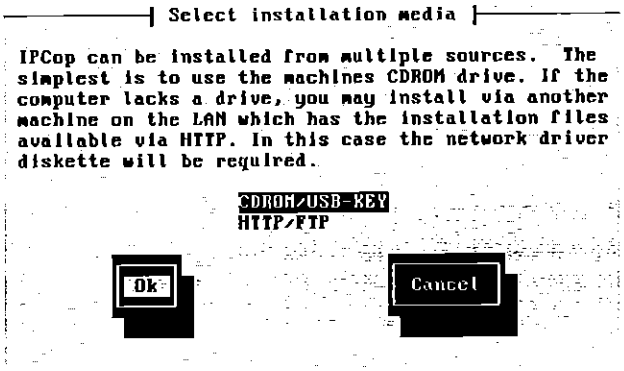
รูปที่ ก-1 กด Enter เพื่อทำการติดตั้ง



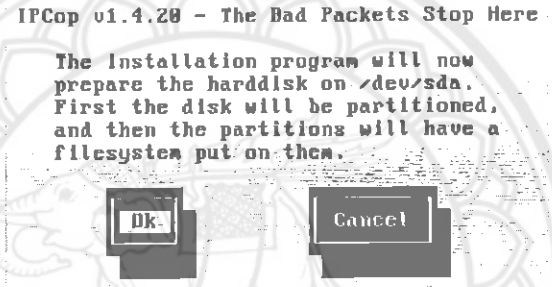
รูปที่ ก-2 เลือกภาษาที่ต้องการ คือ English



รูปที่ ก-3 แสดงข้อความยืนยัน และ แจ้งเตือนในการติดตั้ง

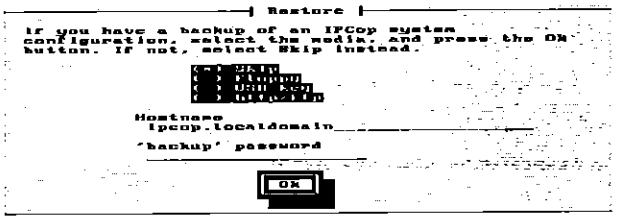


รูปที่ ก-4 เลือกรูปแบบการติดตั้ง ให้เลือก CDROM/USB-Key

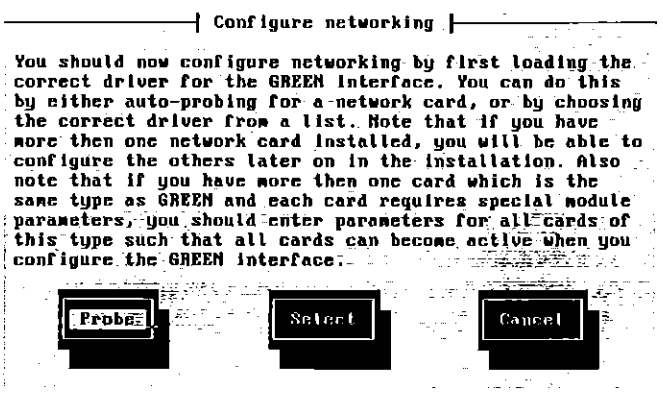


รูปที่ ก-5 ยืนยันการลบข้อมูลในฮาร์ดดิสก์

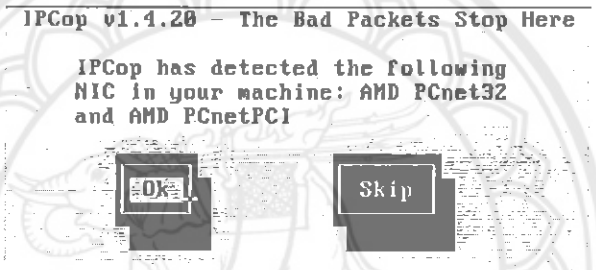
รูปที่ ก-6 โปรแกรมเริ่มการติดตั้ง



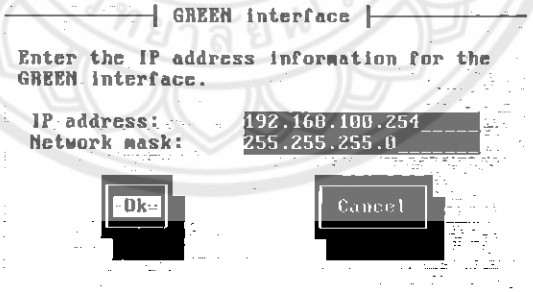
รูปที่ ก-7 เรียกข้อมูลสำรองไว้กลับคืนมา ให้เลือก Skip



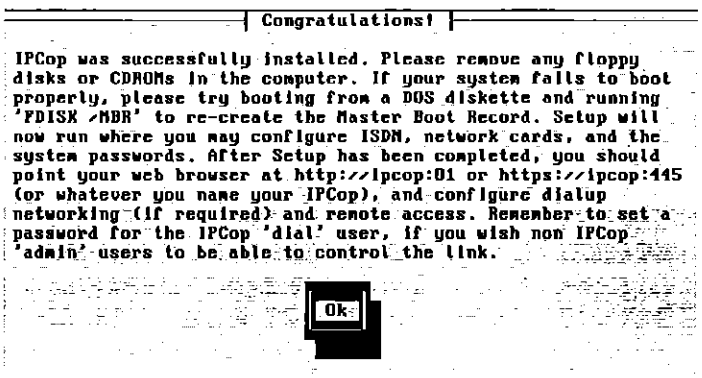
รูปที่ ก-8 หน้าต่างแสดงการกำหนดค่า Network ให้เลือก Probe



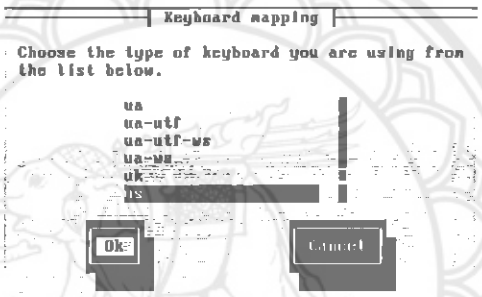
รูปที่ ก-9 กำหนดไดรเวอร์ให้กับการ์ดแลนที่เป็น Greeb Interface



รูปที่ ก-10 กำหนดค่า IP Address ให้กับ Green Interface

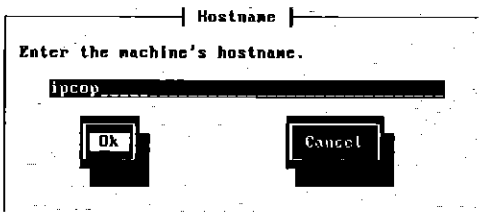


รูปที่ ก-11 สิ้นสุดการติดตั้ง

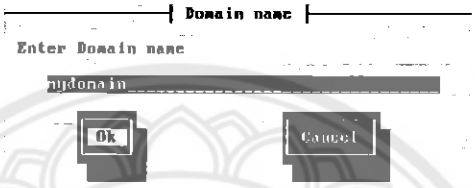


รูปที่ ก-12 เลือกประเภทคีย์บอร์ดที่จะใช้งาน

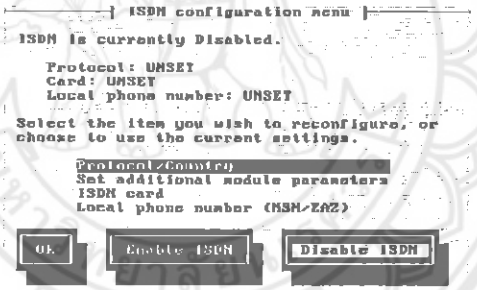
รูปที่ ก-13 เลือก Time zone



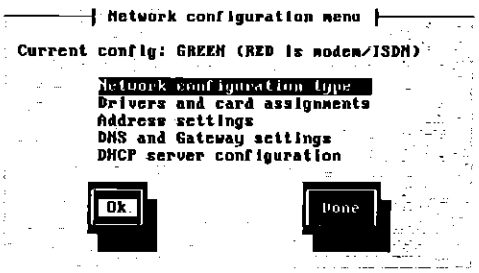
รูปที่ ก-14 กำหนดชื่อ Host ให้กับเครื่อง



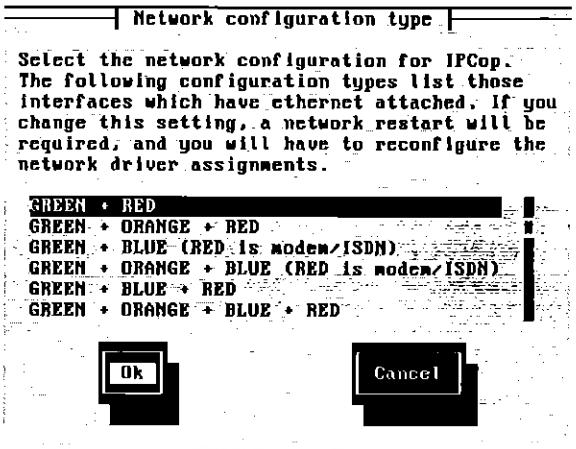
รูปที่ ก-15 กำหนดค่า Domain



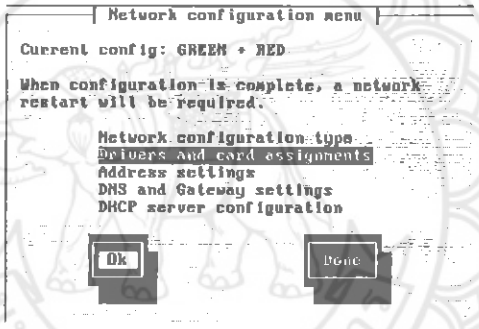
รูปที่ ก-16 ยกเลิกการใช้งาน ISDN



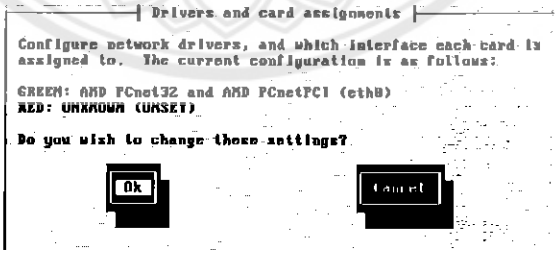
รูปที่ ก-17 กำหนดค่ารูปแบบการเชื่อมต่อ



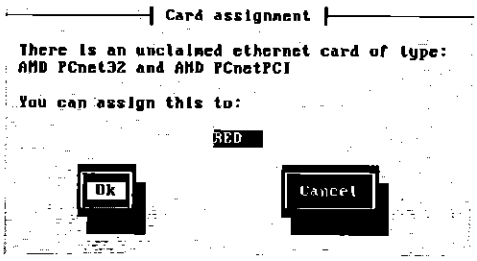
รูปที่ ก-18 เลือกรูปแบบของ Network Configuration Type ของ IPCop



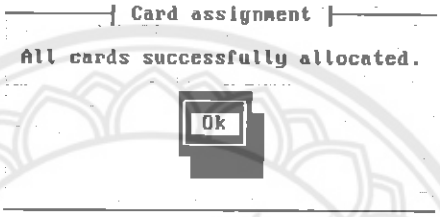
รูปที่ ก-19 เลือกเมนูเพื่อกำหนดไดรเวอร์ให้กับการ์ดแลนแต่ละใบ



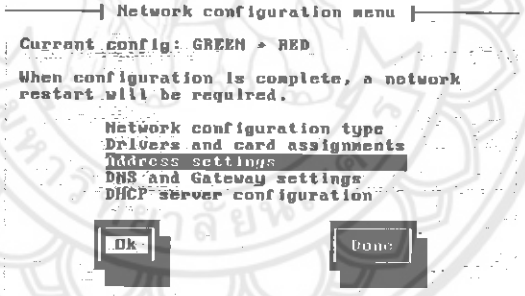
รูปที่ ก-20 กำหนดไดรเวอร์ให้กับ Red Interface



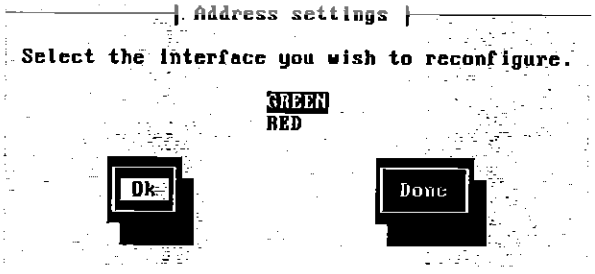
รูปที่ ก-21 กำหนดไดร์เวอร์ให้กับ Red Interface



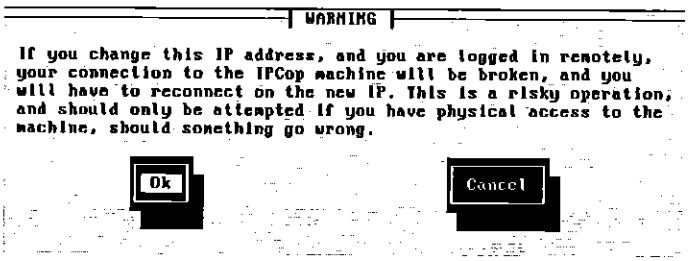
รูปที่ ก-22 ติดตั้งไดร์เวอร์สมบูรณ์



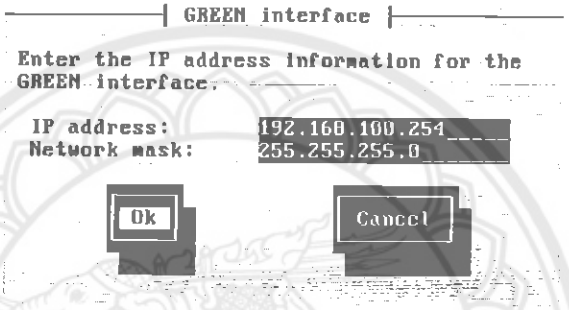
รูปที่ ก-23 เมนูการกำหนดค่า IP Address



รูปที่ ก-24 เมนูการกำหนดค่า IP Address ให้กับ Green Interface

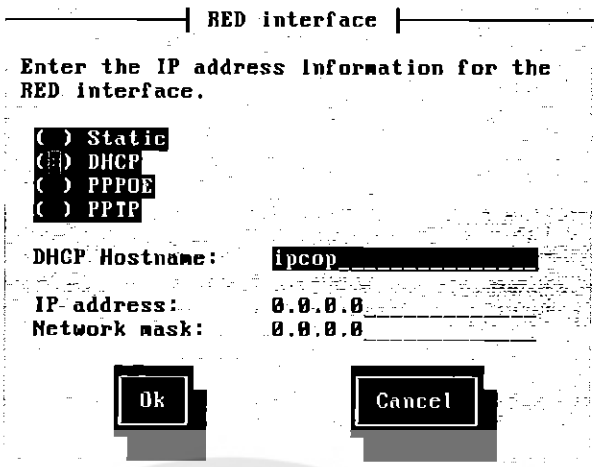


รูปที่ ก-25 โปรแกรมแสดงข้อความเตือนการกำหนด IP Address

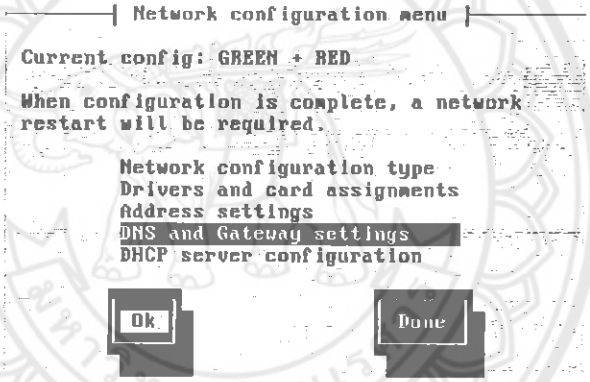


รูปที่ ก-26 แสดงการกำหนดค่า IP Address ให้กับ Green Interface

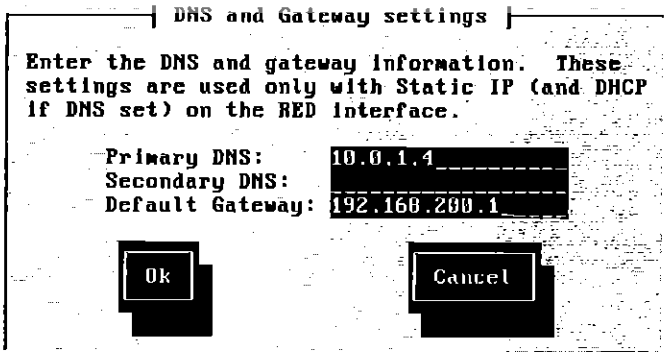
รูปที่ ก-27 เมนูการกำหนดค่า IP address ให้กับ Red Interface



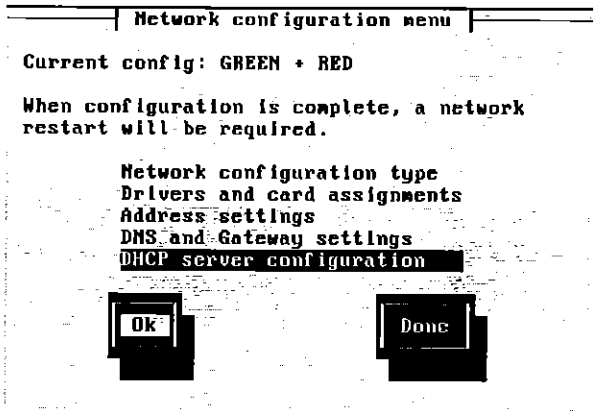
รูปที่ ก-28 แสดงการกำหนดค่า IP Address ให้กับ Red Interface



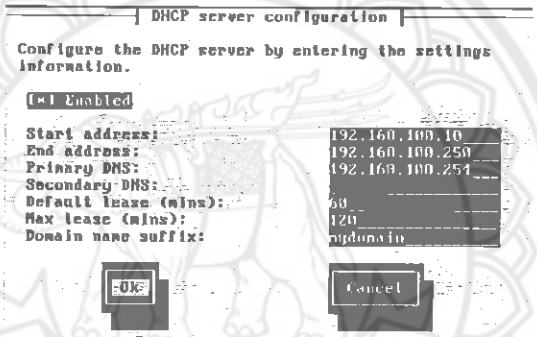
รูปที่ ก-29 เลือกเมนูการกำหนดค่า DNS and Gateway settings



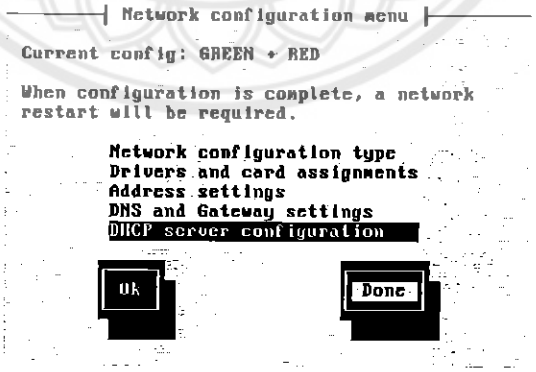
รูปที่ ก-30 กำหนดค่า DNS และ Gateway ให้กับ IPCop



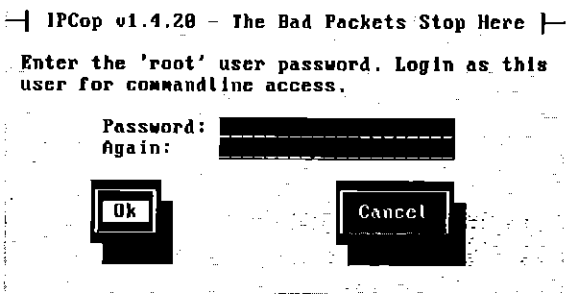
รูปที่ ก-31 เมนูเพื่อการกำหนดค่า DHCP Server



รูปที่ ก-32 กำหนดค่า DHCP Server

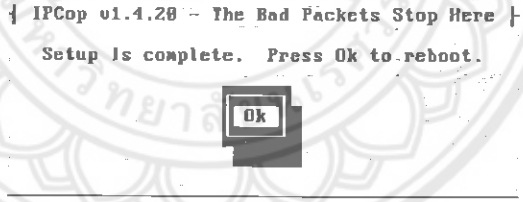


รูปที่ ก-33 เสร็จสิ้นการกำหนดค่า Network

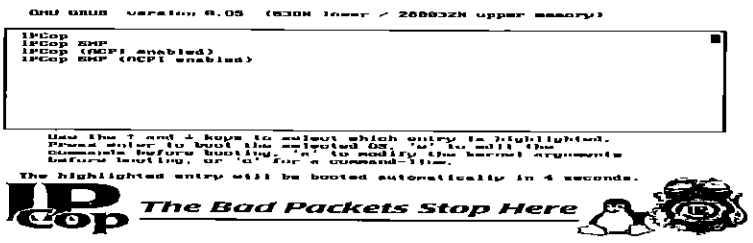


รูปที่ ก-34 กำหนดรหัสผ่านให้กับ Root

รูปที่ ก-35 กำหนดรหัสผ่านให้กับ Admin



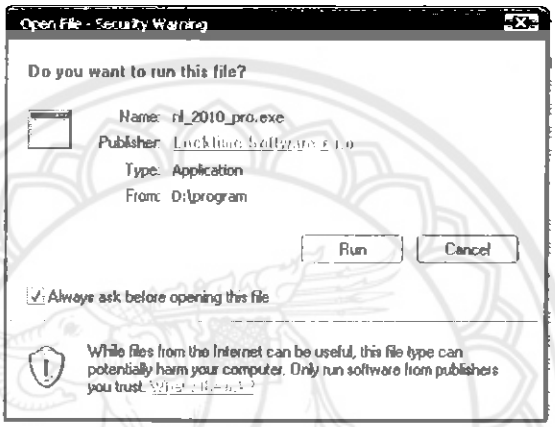
รูปที่ ก-36 ติดตั้งเสร็จสมบูรณ์



รูปที่ ก-37 GRUB Loader

รูปที่ ก-38 แสดงการล็อกอินเข้าใช้งานของระบบ

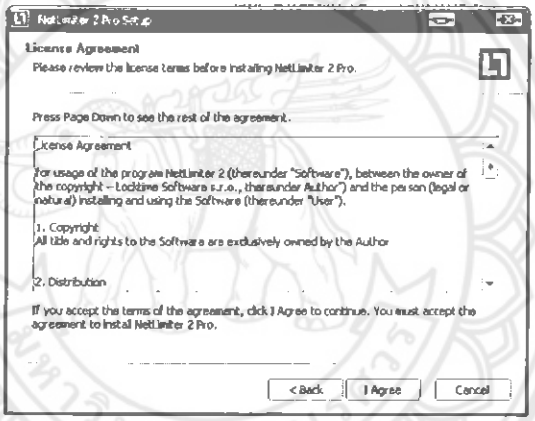
2. การติดตั้งโปรแกรม NetLimiter



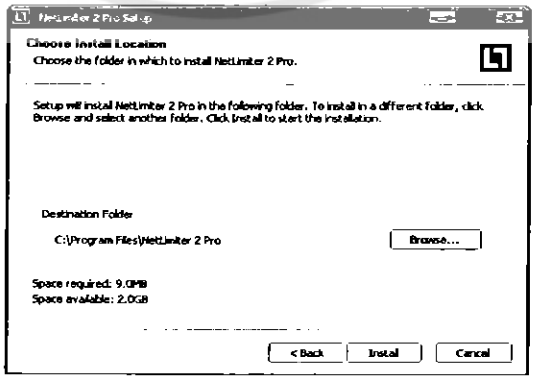
รูปที่ ก-39 เลือกการติดตั้งโปรแกรม

รูปที่ ก-40 เลือกภาษาในการทำงาน

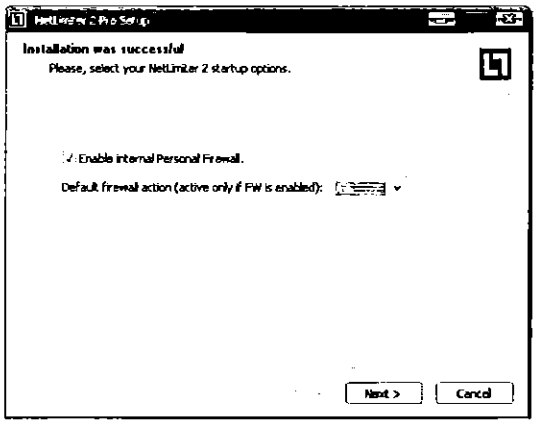
รูปที่ ก-41 เลือก Next เพื่อทำการงานต่อไป



รูปที่ ก-42 License Agreement เมื่ออ่านจบแล้วให้เลือก I Agree



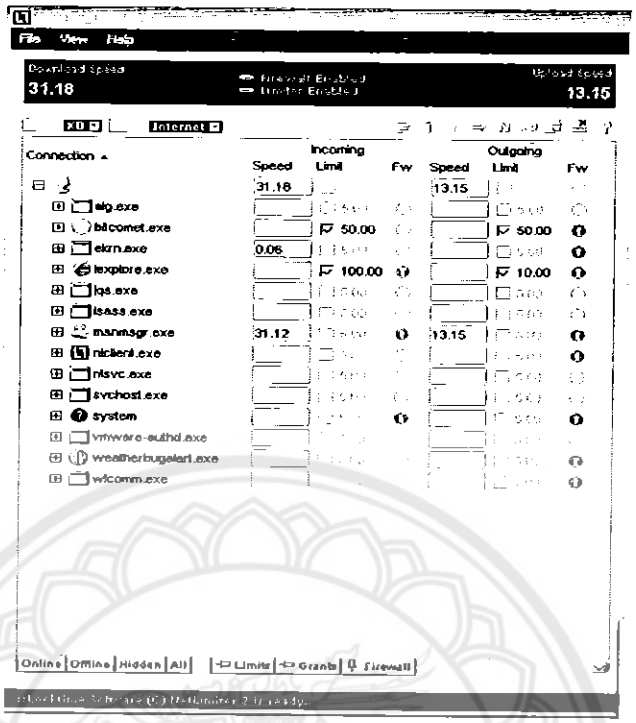
รูปที่ ก-43 เลือกที่อยู่ของโปรแกรมที่จะติดตั้ง



รูปที่ ก-44 เลือก Next เพื่อเสร็จสิ้นการติดตั้งโปรแกรม

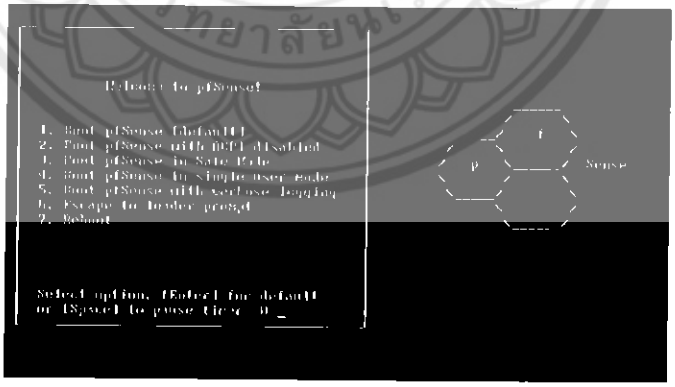
รูปที่ ก-45 เลือก Reboot Now เพื่อรีสตาร์ทคอมพิวเตอร์สำหรับเริ่มต้นการใช้งานของโปรแกรม

รูปที่ ก-46 เลือก Continue เพื่อเริ่มต้นการใช้งาน

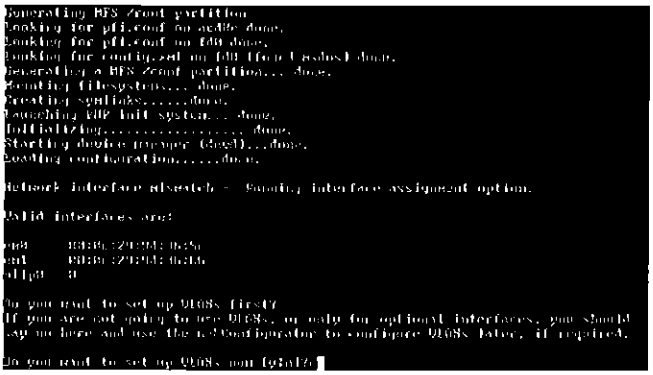


รูปที่ ก-47 หน้าโปรแกรม NetLimiter

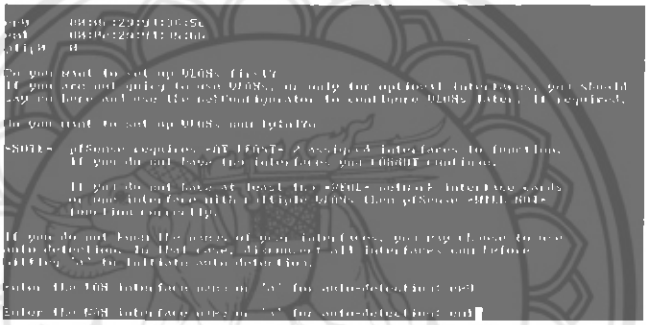
3. การติดตั้งโปรแกรม PFSense



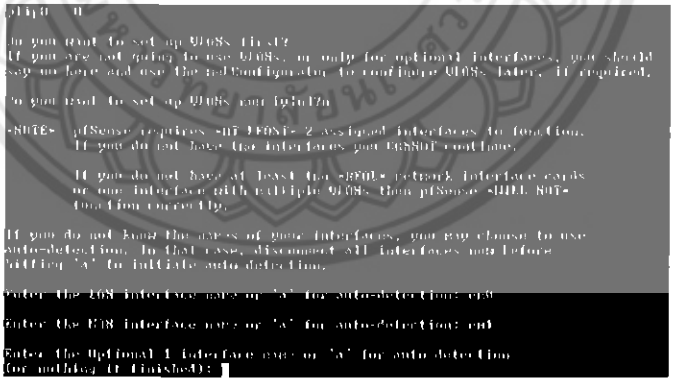
รูปที่ ก-48 หน้าหลักการ Install เลือก Enter เพื่อทำการติดตั้ง



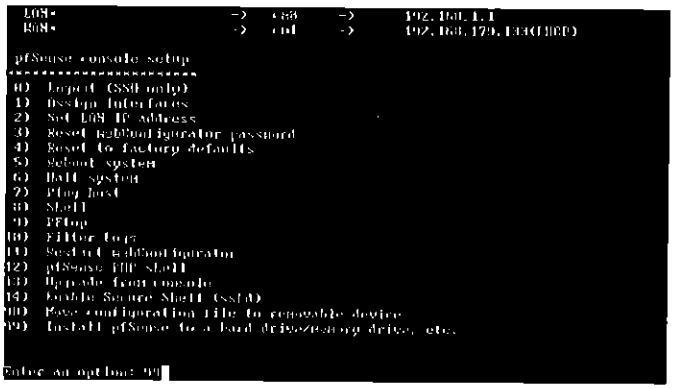
รูปที่ ก-49 แสดงการติดตั้ง VLANs ในที่นี้ไม่ต้องการติดตั้ง



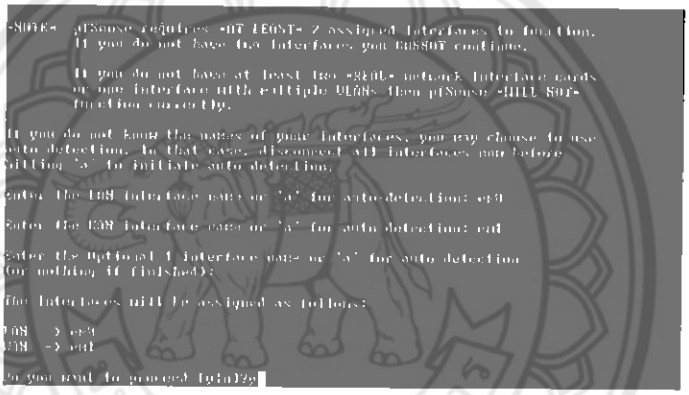
รูปที่ ก-50 กำหนดให้ LAN เป็น em0 และ WAN เป็น em1



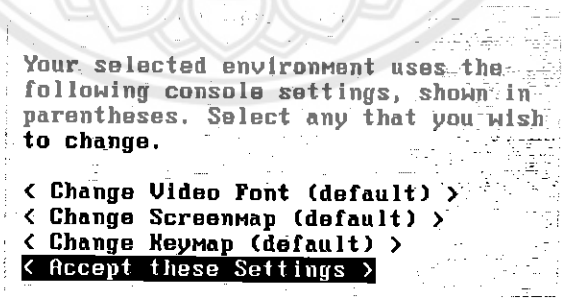
รูปที่ ก-51 พิมพ์ a หรือ enter เพื่อทำขั้นต่อไป



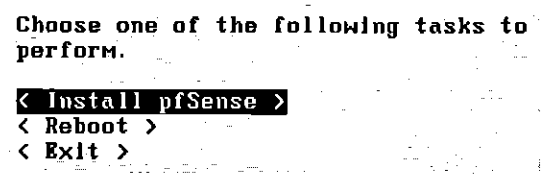
รูปที่ ก-52 พิมพ์เลข 99 เพื่อทำการติดตั้ง



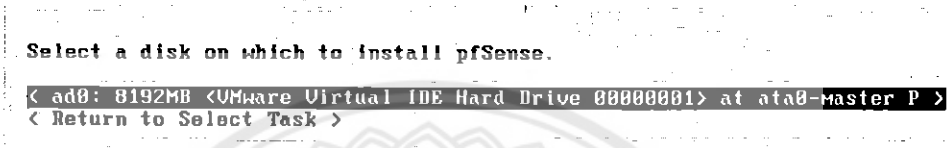
รูปที่ ก-53 พิมพ์ y เพื่อทำงานต่อไป



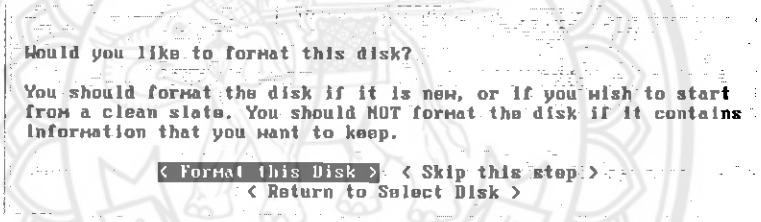
รูปที่ ก-54 เลือก Accept these Settings



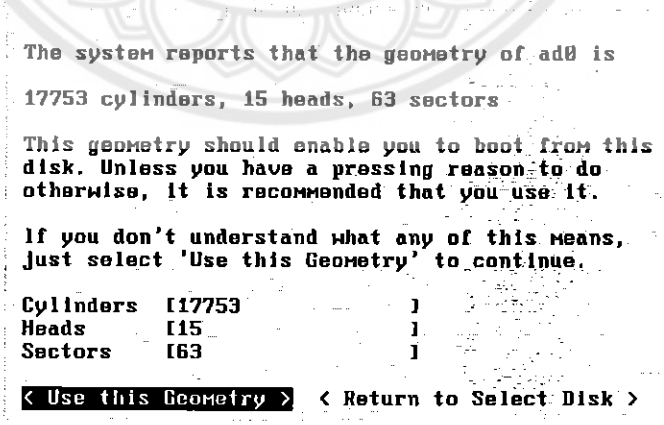
รูปที่ ก-55 เลือก Install pfSense เพื่อเริ่มการติดตั้งโปรแกรม



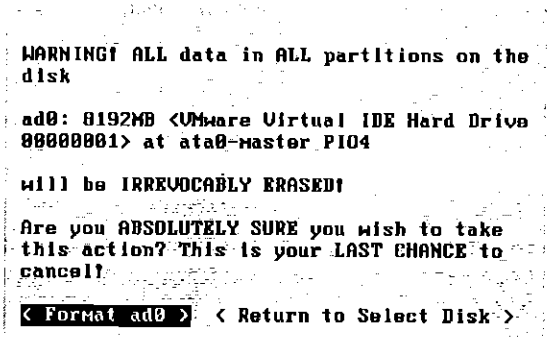
รูปที่ ก-56 เลือก Disk เพื่อทำการติดตั้ง



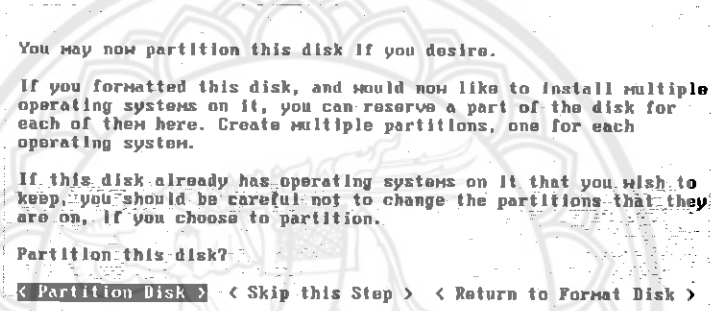
รูปที่ ก-57 เลือก Format Disk



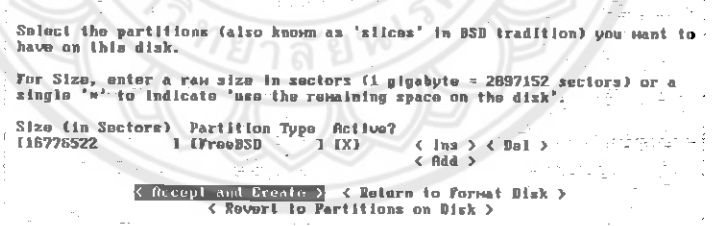
รูปที่ ก-58 เลือก Use this Geometry



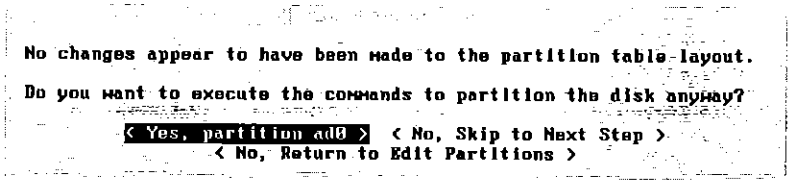
รูปที่ ก-59 เลือก Format ad0



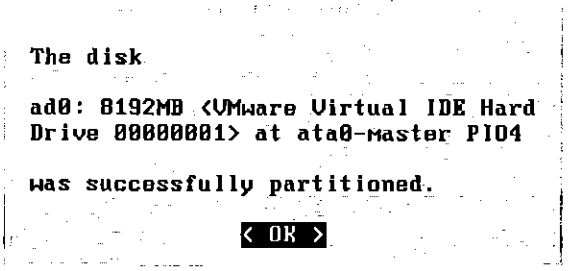
รูปที่ ก-60 เลือก Partition Disk สำหรับการแบ่ง Partition



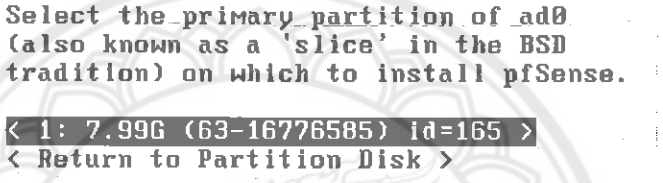
รูปที่ ก-61 เลือก Accept and Create



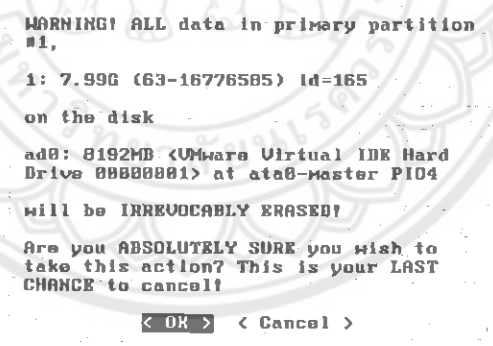
รูปที่ ก-62 เลือก Yes partition ad0 เพื่อเริ่มการแบ่ง Partition



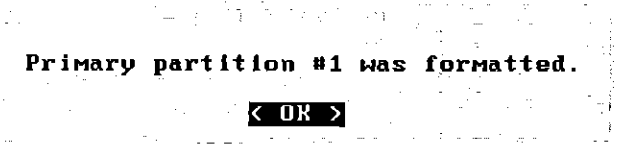
รูปที่ ก-63 การแบ่ง Partition เสร็จสมบูรณ์



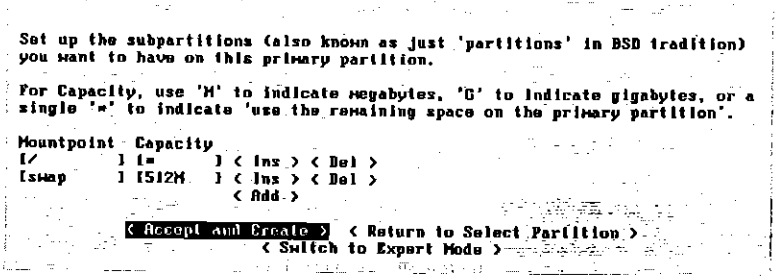
รูปที่ ก-64 เลือก Partition



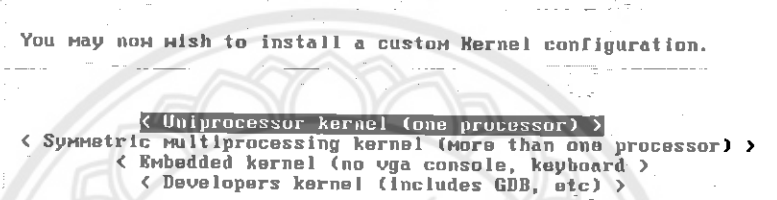
รูปที่ ก-65 เลือก OK



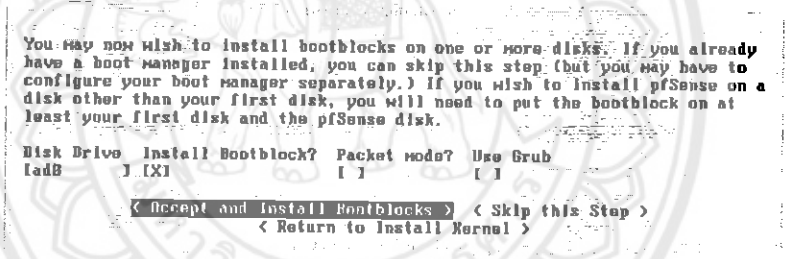
รูปที่ ก-66 เลือก OK



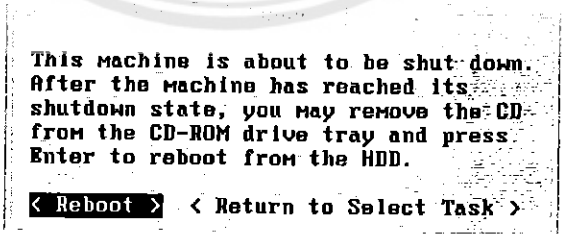
รูปที่ ก-67 เลือก Accept and Create



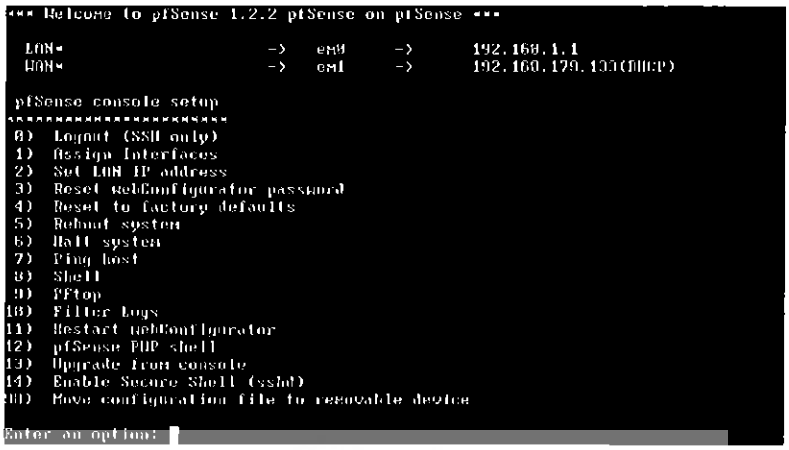
รูปที่ ก-68 เลือก Uniprocessor Kernel



รูปที่ ก-69 เลือก Accept and Install Bootblock เพื่อยอมรับและทำการติดตั้ง Bootblock



รูปที่ ก-70 เลือก Reboot เพื่อรีสตาร์ทคอมพิวเตอร์สำหรับเริ่มต้นการใช้งานโปรแกรม



รูปที่ ก-71 หน้าหลักโปรแกรม PFSense

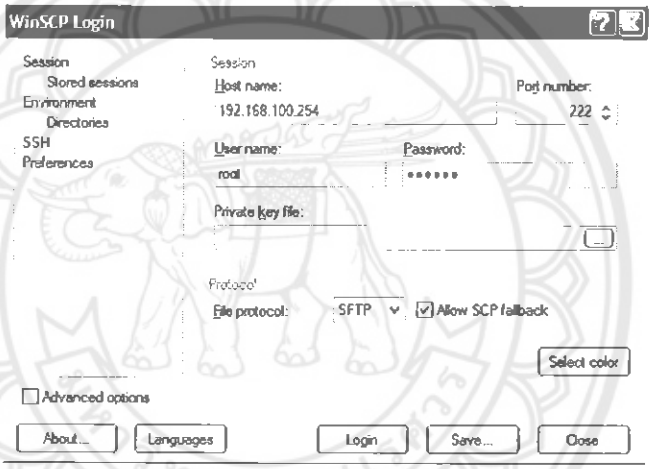
ภาคผนวก ข.

ขั้นตอนการคอนฟิก (Config)

1. การ Config IPCop

- Advproxy

1. ดาวน์โหลดโปรแกรม Advproxy จากเว็บไซต์ http://www.advproxy.com
2. คัดลอกไฟล์ที่ได้ไปไว้ใน IPCop โดยใช้โปรแกรม WinSCP โดยกำหนดค่าดังรูปที่ ข-1



รูปที่ ข-1 การกำหนดค่าโปรแกรม WinSCP

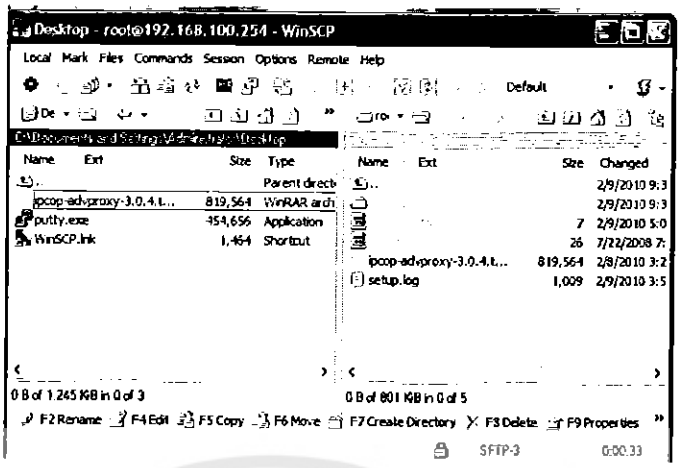
- Host name : ใส่หมายเลขไอพีของ IPCop

- Port number : ใส่ 222 เพราะ IPCop จะให้บริการ SFTP และ SSH ผ่านทางพอร์ต 222

- User name : ใส่ root

- Password : ใส่รหัสผ่านของ root

จากนั้นกดปุ่ม Login เพื่อเชื่อมต่อกับเครื่อง IPCop



รูปที่ ข-2 อัพโหลดไฟล์ไปไว้ที่ IPCop Server ด้วย WinSCP

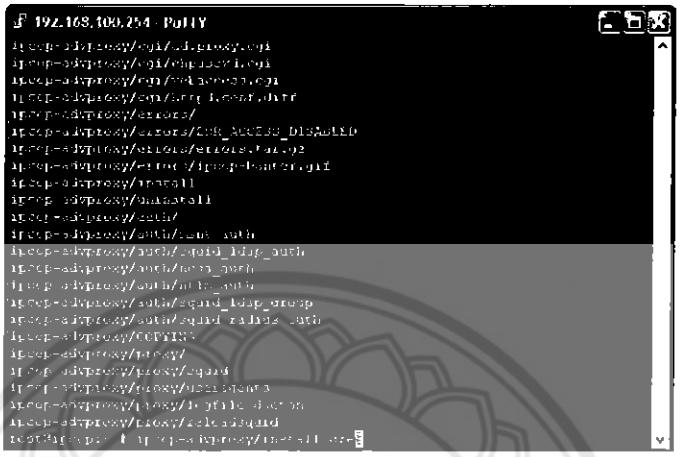
3. ใช้เมาส์ลากไฟล์ ipcop-advproxy จากด้านซ้ายมือไปไว้ที่โฟล์เดอร์ root ทางฝั่งของ IPCop ด้านขวามือ

4. เปิดโปรแกรม PuTTY เพื่อล็อกอินเข้าไปที่เครื่องของ IPCop

5. แตกไฟล์โดยใช้คำสั่งดังรูปที่ ข-3

รูปที่ ข-3 แตกไฟล์ โดยพิมพ์คำสั่ง tar xvzf ipcop-advproxy-3.0.4.tar.tar

6. ติดตั้ง Advproxy โดยใช้คำสั่งตามรูปที่ ข-4



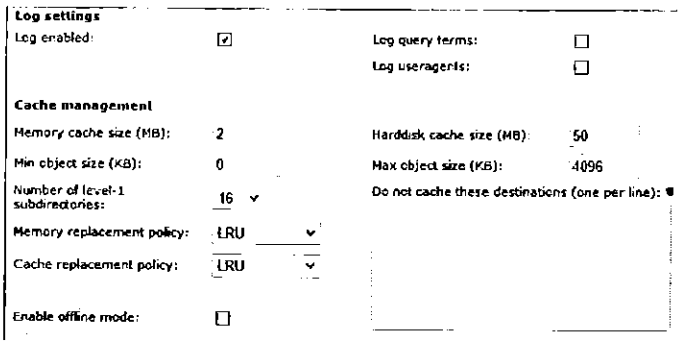
รูปที่ ข-4 ติดตั้ง Advproxy โดยพิมพ์คำสั่ง ipcop-advproxy/insatall cre

รูปที่ ข-5 หน้าจอหลัก Advproxy

- Enabled on Green : เป็นการเปิดให้บริการ Proxy ในส่วนของอินเตอร์เฟซ

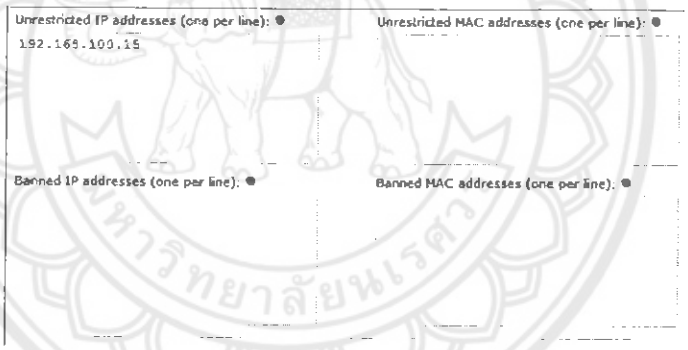
- Transparent on Green : เปิดให้บริการ Proxy แบบ Transparent ซึ่งจะทำการฟอร์เวิร์ดการร้องขอที่จะไปยังพอร์ตปลายทางที่เป็นพอร์ต 80 ไปยัง Proxy โดยอัตโนมัติโดยที่ไม่ต้องทำการกำหนดค่าที่เบราเซอร์ของเครื่องลูกข่าย

- Proxy Port : กำหนดพอร์ตที่ใช้งานของ Proxy ซึ่งจะตอบสนองการร้องขอของเครื่องลูกข่าย ซึ่งโดยปกติแล้วจะใช้พอร์ต 800



รูปที่ ข-6 แสดง Log settings และ Cache management

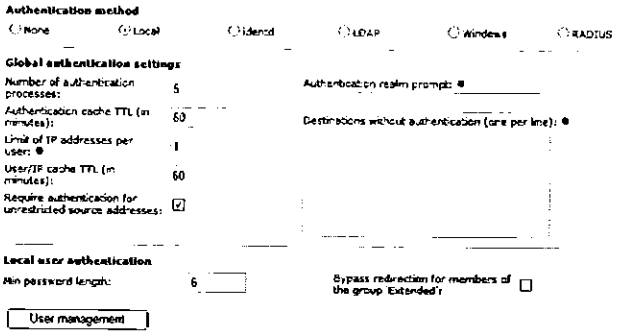
- Log settings : ใช้สำหรับการเปิดใช้การเก็บข้อมูล Log
- Cache management : ใช้สำหรับกำหนดค่าการจัดเก็บ Cache สำหรับ Proxy



รูปที่ ข-7 แสดง Network based access control

- Network based access control : ใช้สำหรับการกำหนดลูกข่ายที่จะใช้งาน Proxy
- Authentication method : สำหรับกำหนดรูปแบบการตรวจสอบตัวเองของผู้ใช้งานในเครือข่าย โดยผู้ที่ต้องการจะเข้าเว็บไซต์จะต้องระบุ ชื่อผู้ใช้ และ รหัสผ่านของตัวเองจึงจะสามารถเข้าเว็บไซต์ได้

การทำระบบ Authentication นั้นจะต้องปิดการให้บริการแบบ Transparent ของ Proxy Server ก่อน เพราะการทำ Authentication นั้นจะไม่สนับสนุนการทำงานแบบ Transparent



รูปที่ ข-8 แสดง Authentication method

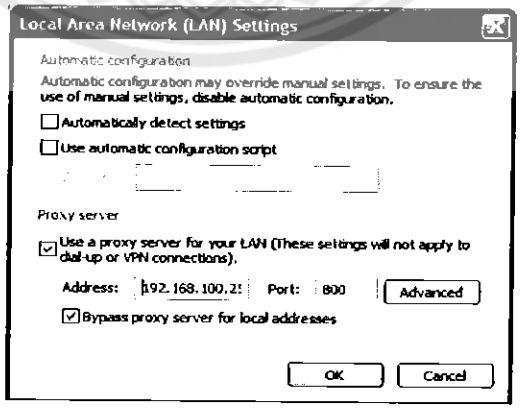
- None : ปิดการใช้งานระบบตรวจสอบผู้ใช้งาน ซึ่งจะเป็นค่าเริ่มต้นของ Advproxy

- Local : เครื่องลูกข่ายถ้าต้องการจะเข้าเว็บไซต์ จะต้องระบุชื่อ และ รหัสผ่าน จึงจะเข้าเว็บไซต์ได้ โดยชื่อ และ รหัสผ่านจะถูกเก็บไว้ที่ IPCop Proxy Server

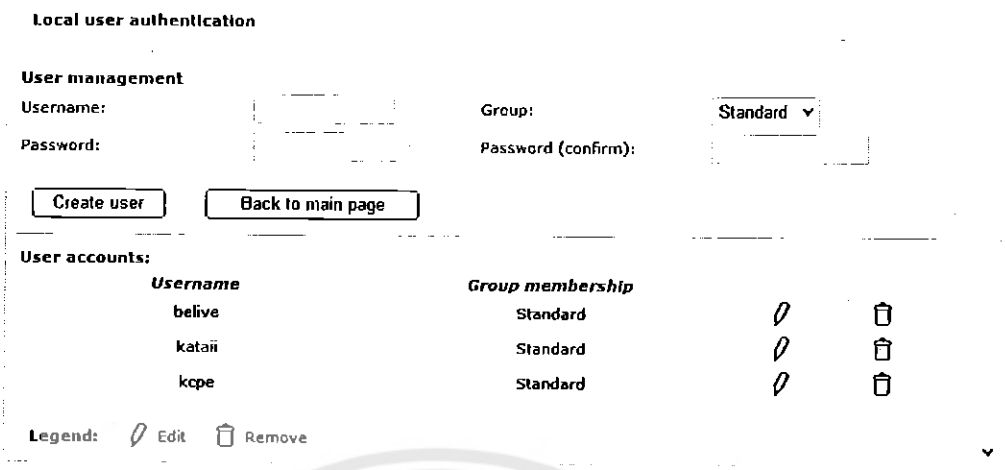
- Limit of IP Address per user : ระบุจำนวน IP Address ที่จะสามารถล็อกอินโดยใช้ชื่อผู้ใช้ และ รหัสผ่านเดียวกัน

- User/IP cache TTL : กำหนดระยะเวลาที่ใช้ในการเข้าใช้งานของแต่ละ User หรือ IP ซึ่งเมื่อครบตามที่กำหนด ต้องทำการล็อกอินใหม่อีกครั้ง ค่าปกติคือ 0 หมายถึงปิดการใช้งาน

- Min password length : รหัสผ่านขั้นต่ำสุดที่สามารถใช้ได้



รูปที่ ข-9 กำหนดค่า Proxy ใน Internet Explorer

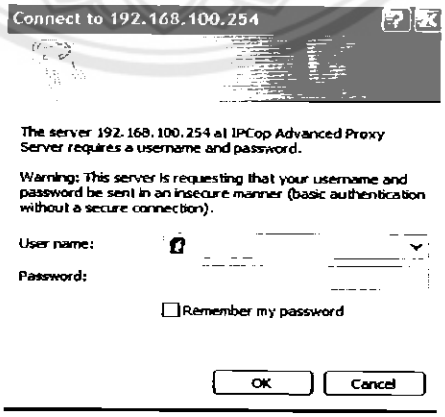


รูปที่ ข-10 การสร้างบัญชีรายชื่อใหม่

- Username : ระบุชื่อที่ต้องการ
- Password : กำหนดรหัสผ่านจำนวนตามที่กำหนดไว้ในส่วนของ Min password length
- Password (confirm) : ระบุรหัสผ่านอีกครั้ง

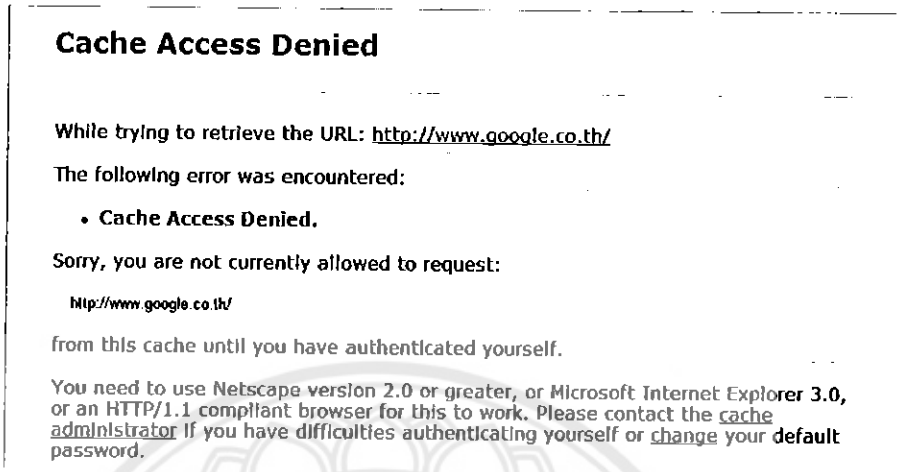
ทดสอบการทำงาน

เปิดโปรแกรมเว็บเบราเซอร์แล้วทดลองเข้าเว็บไซต์ จะปรากฏหน้าต่างสำหรับระบุชื่อผู้ใช้งาน และ รหัสผ่าน เพื่อให้กรอกก่อนที่จะเข้าเว็บไซต์ดังรูปที่ ข-11



รูปที่ ข-11 หน้าต่างสำหรับล็อกอิน

หากคลิกที่ปุ่ม Cancel โปรแกรมเบราเซอร์จะแสดงหน้าเว็บเพจดังรูปที่ ข-12



Cache Access Denied

While trying to retrieve the URL: http://www.google.co.th/

The following error was encountered:

- **Cache Access Denied.**

Sorry, you are not currently allowed to request:

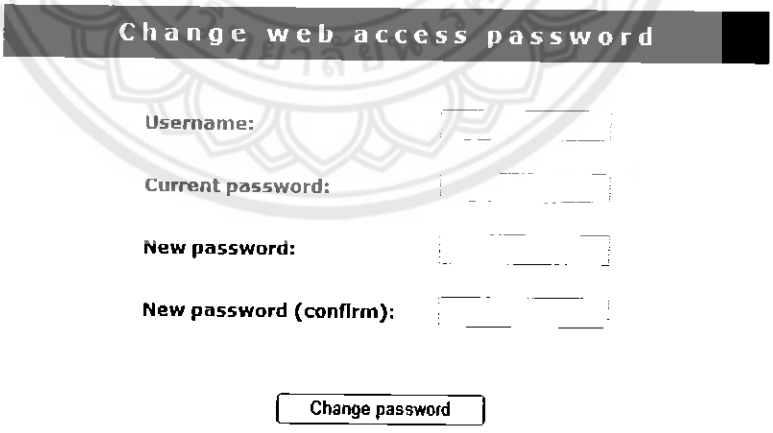
http://www.google.co.th/

from this cache until you have authenticated yourself.

You need to use Netscape version 2.0 or greater, or Microsoft Internet Explorer 3.0, or an HTTP/1.1 compliant browser for this to work. Please contact the cache administrator if you have difficulties authenticating yourself or change your default password.

รูปที่ ข-12 แสดงรูปเมื่อคลิก Cancel

หากผู้ใช้งานต้องการจะเปลี่ยนรหัสผ่านของตัวเอง สามารถทำได้โดยเข้าไปที่ http://192.168.100.254:81/cgi-bin/chpasswd.cgi จากนั้นจะปรากฏหน้าเว็บเพจสำหรับเปลี่ยนรหัสผ่าน ดังรูปที่ ข-13



Change web access password

Username:

Current password:

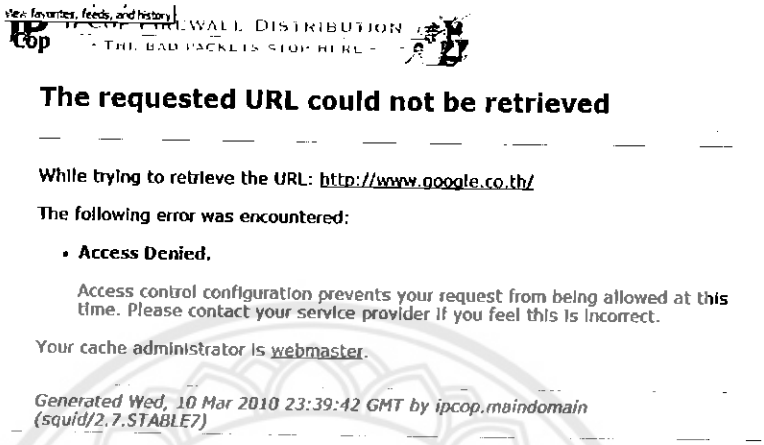
New password:

New password (confirm):

Change password

รูปที่ ข-13 แสดงหน้าเว็บเพจสำหรับเปลี่ยนรหัสผ่าน

หากผู้ใช้ทำการล็อกอินโดยใช้ชื่อผู้ใช้ และ รหัสผ่านเดียวกัน จะปรากฏหน้าเว็บเพจดังรูปที่ ข-14

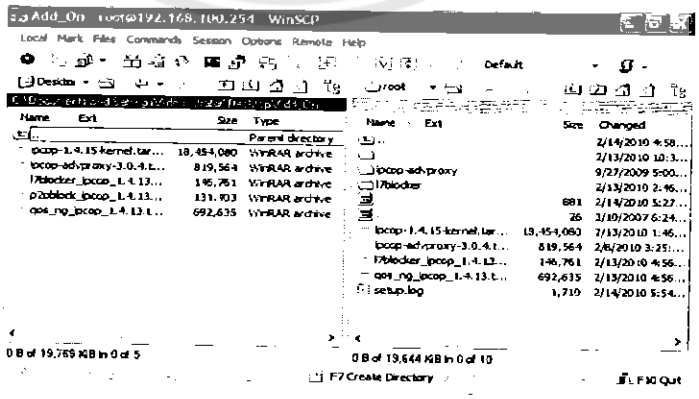


รูปที่ ข-14 แสดงรูปเมื่อล็อกอินโดยใช้ชื่อผู้ใช้ และ รหัสผ่านเดียวกัน

- I7Filter

I7Filter เป็น Add-on ที่สำคัญเนื่องจากการติดตั้ง P2PBlock และ QoS_ng จำเป็นต้องลง I7Filter ก่อน

1. ดาวน์โหลดโปรแกรม I7Filter จากเว็บไซต์ http://mh-lantech.css-hamburg.de/ipcop/download.php?list.24
2. ก๊อบปี้ไฟล์ที่ได้ไปไว้ใน IPCop โดยใช้โปรแกรม WinSCP



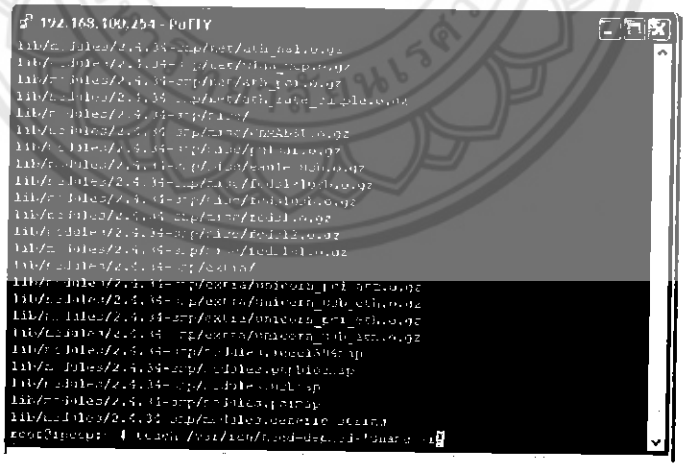
รูปที่ ข-15 อัพโหลดไฟล์ไปไว้ที่ IPCop Server ด้วย WinSCP

3. ใช้เมาส์ลากไฟล์ ipcop-1.4.15-kernel.tar.bz2 จากด้านซ้ายมือไปไว้ที่โฟล์เดอร์ root ทางฝั่งของ IPCop ด้านขวามือ

4. เปิดโปรแกรม PuTTY เพื่อล็อกอินเข้าไปที่เครื่องของ IPCop

5. แตกไฟล์โดยใช้คำสั่งตามรูปที่ ข-16

รูปที่ ข-16 แตกไฟล์ โดยใช้คำสั่ง tar xvfj ipcop-1.4.15-kernel.tar.bz2 –C /

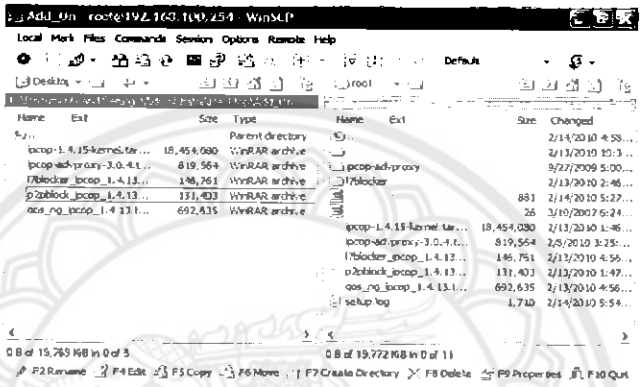


รูปที่ ข-17 พิมพ์คำสั่ง touch /var/run/need-depmod-'uname –r'

- P2PBlock

1. ดาวน์โหลดโปรแกรม P2PBlock จากเว็บไซต์ http://mh-lantech.css-hamburg.de/ipcop/download.php?list.24

2. ก๊อบปี้ไฟล์ที่ได้ไปไว้ใน IPCop โดยใช้โปรแกรม WinSCP

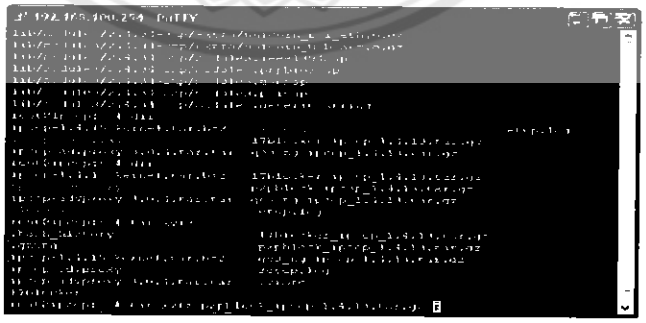


รูปที่ ข-18 อัพโหลดไฟล์ไปไว้ที่ IPCop Server ด้วย WinSCP

3. ใช้เมาส์ลากไฟล์ p2pblock_Ipcop_1.4.13 จากด้านซ้ายมือไปไว้ที่โฟล์เดอร์ root ทางฝั่งของ IPCop ด้านขวามือ

4. เปิดโปรแกรม PuTTY เพื่อล็อกอินเข้าไปที่เครื่องของ IPCop

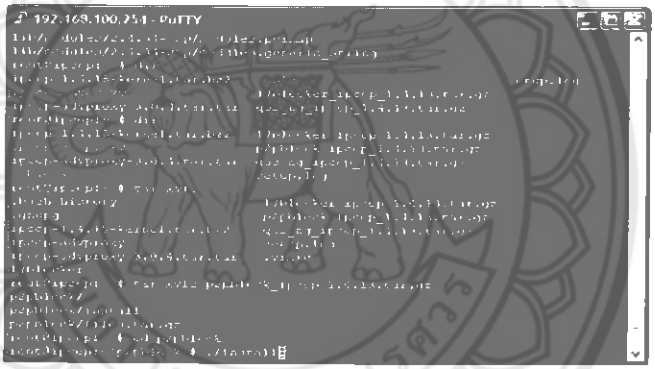
5. แตกไฟล์โดยใช้คำสั่งตามรูปที่ ข-19



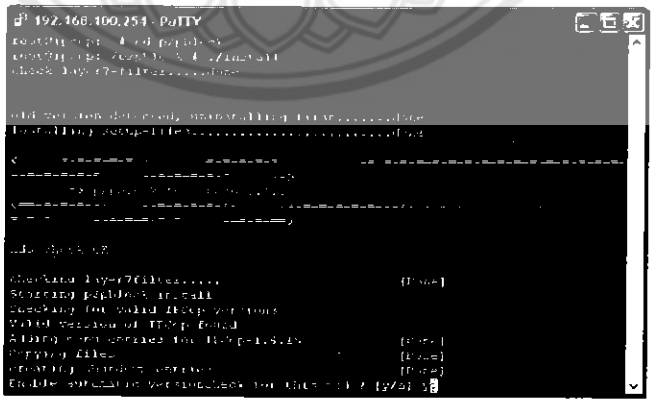
รูปที่ ข-19 แตกไฟล์ โดยใช้คำสั่ง tar xvfz pspblock_ipcop_1.4.13.tar.gz

6. ติดตั้ง P2PBlock โดยใช้คำสั่งตามรูปข้างล่าง

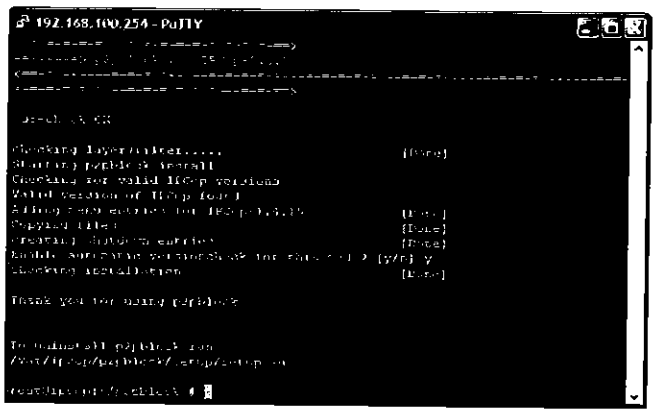
รูปที่ ข-20 เข้าไปยังไดเร็กทอรี่ p2pblock โดยใช้คำสั่ง cd p2pblock



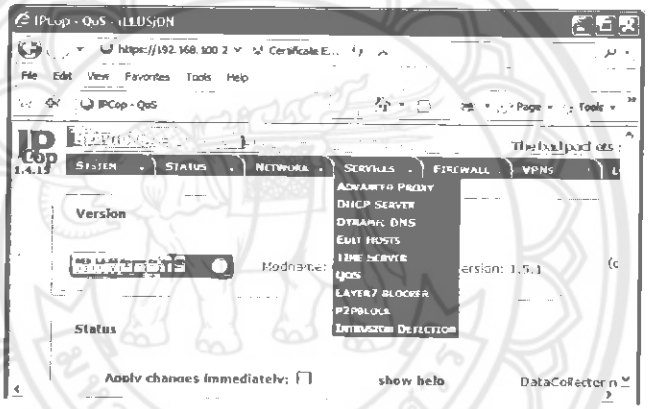
รูปที่ ข-21 ติดตั้งโปรแกรมด้วยคำสั่ง ./install



รูปที่ ข-22 พิมพ์ y เพื่อทำการ update โปรแกรม layer7-filter

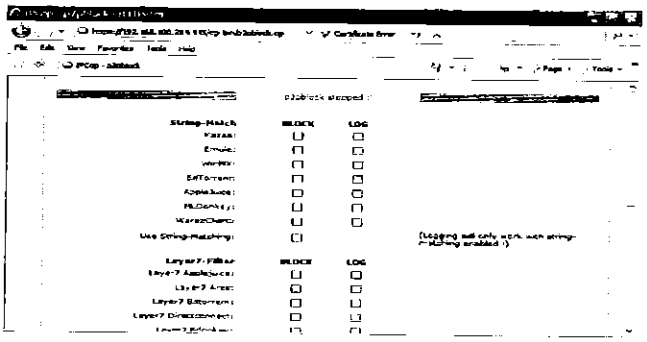


รูปที่ ข-23 uninstall โดยใช้คำสั่ง /var/ipcop/p2pblock/setup/setup –u



รูปที่ ข-24 เมนูการใช้งาน P2Pblock

7. เลือก Protocol ที่ต้องการที่จะ Block ดังรูปที่ ข-25

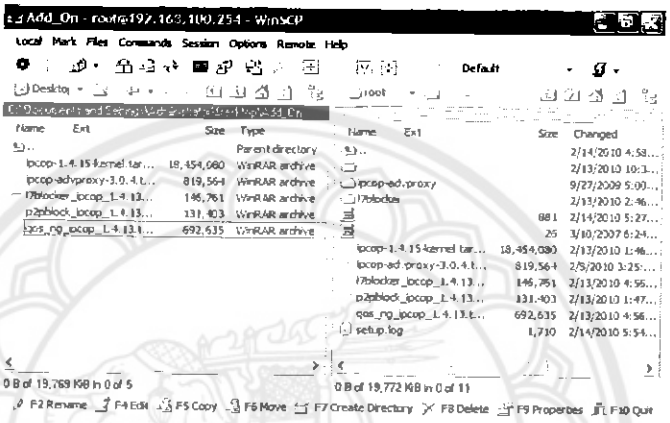


รูปที่ ข-25 เลือก Protocol ที่ต้องการ Block

- QoS_ng

1. ดาวน์โหลดโปรแกรม QoS_ng จากเว็บไซต์ http://mh-lantech.css-hamburg.de/ipcop/download.php?list.24

2. ก๊อบปี้ไฟล์ที่ได้ไปไว้ใน IPCop โดยใช้โปรแกรม WinSCP



รูปที่ ข-26 อัพโหลดไฟล์ไปไว้ที่ IPCop Server ด้วย WinSCP

3. ใช้เมาส์ลากไฟล์ qos_ng_ipcop_1.4.13 จากด้านซ้ายมือไปไว้ที่โฟล์เดอร์ root ทางฝั่งของ IPCop ด้านขวามือ

4. เปิดโปรแกรม PuTTY เพื่อล็อกอินเข้าไปที่เครื่องของ IPCop

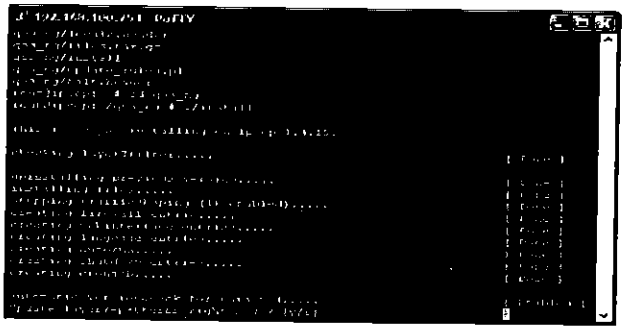
5. แตกไฟล์โดยใช้คำสั่งตามรูปที่ ข-27

รูปที่ ข-27 แตกไฟล์ โดยใช้คำสั่ง tar xvfz qos_ng_ipcop_1.4.13.tar.gz

6. ติดตั้ง QoS_ng โดยใช้คำสั่งตามรูปที่ ข-28

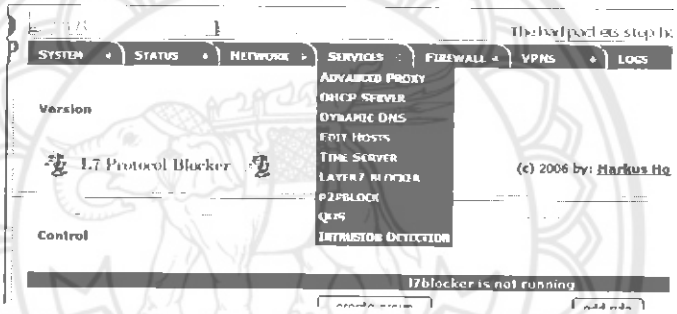
รูปที่ ข-28 เข้าไปยังไดเร็กทอรี่ QoS_ng โดยใช้คำสั่ง cd qos_ng

รูปที่ ข-29 ติดตั้งโปรแกรมด้วยคำสั่ง ./install



รูปที่ ข-30 พิมพ์ y เพื่อทำการ Update โปรแกรม layer7-filter

รูปที่ ข-31 ติดตั้งเสร็จสมบูรณ์

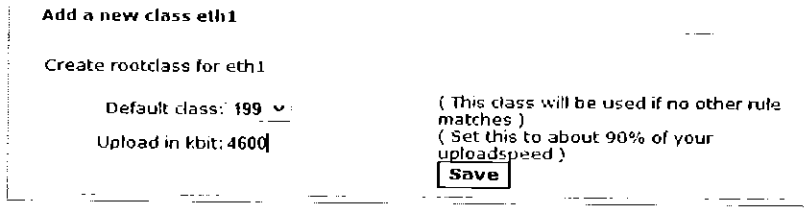


รูปที่ ข-32 เมนูการใช้งาน QoS

การตั้งค่าของ QoS_ng

1. สร้าง Root Class ขึ้นมา 2 Class ได้แก่

- Class 199 (eth1-Red) เป็น Class ที่ใช้ในการอัพโหลดซึ่งในที่นี้ได้ใช้อินเทอร์เน็ตความเร็ว 4 Mb/512 Kb ซึ่งจะได้ค่า upload คือ 512 Kb และจะใช้ความเร็ว 90%



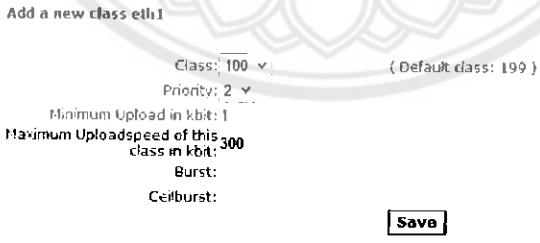
รูปที่ ข-33 แสดงการสร้าง Root Class

- Class 399 (eth0-Green) เป็น Class ที่ใช้ในการดาวน์โหลดซึ่งในที่นี้ความเร็วของการ์ดแลนคือ 100 Mb และจะใช้ความเร็ว 90%

รูปที่ ข-34 แสดงการสร้าง Root Class

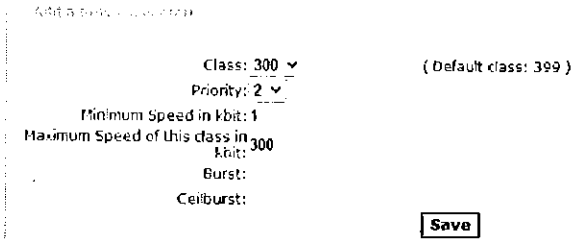
2. สร้าง Child Class ขึ้นมา 2 Class ได้แก่

- Class 100 มาจาก Root Class = 199 เป็น Class ที่กำหนดความเร็วในการอัพโหลดของ HTTP และ FTP (Priority = 2) โดยให้ความเร็วในการอัพโหลดไม่เกิน 300 Kb



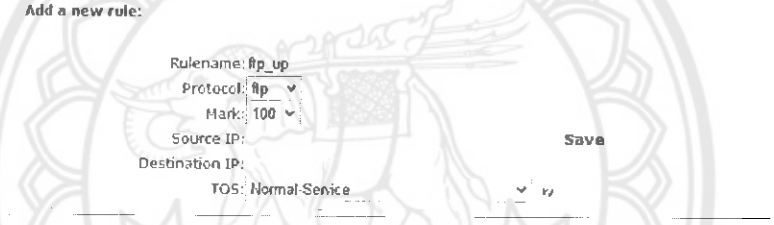
รูปที่ ข-35 แสดงการสร้าง Child Class

- Class 300 มาจาก Root Class = 399 เป็น Class ที่กำหนดความเร็วในการดาวน์โหลดของ FTP และ HTTP (Priority = 2) โดยให้ความเร็วในการอัพโหลดไม่เกิน 300 Kb

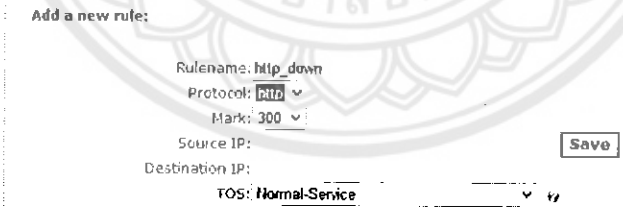


รูปที่ ข-36 แสดงการสร้าง Child Class

3. ใช้ layer7 ในการสร้างกฎบังคับให้ HTTP และ FTP ใช้งานได้ไม่เกิน 300 Kb โดยสามารถดาวน์โหลด Protocol ได้จากเว็บ http://l7-filter.sourceforge.net/protocols แล้วนำไปไว้ที่ /etc/l7-protocols/protocols



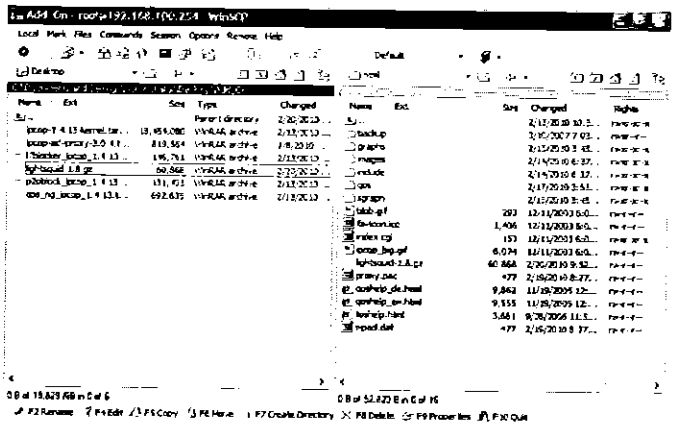
รูปที่ ข-37 แสดงการสร้างกฎ



รูปที่ ข-38 แสดงการสร้างกฎ

- Lightsquid

1. ดาวน์โหลดโปรแกรม Lightsquid จากเว็บไซต์ http://lightsquid.sourceforge.net/
2. ก๊อบปี้ไฟล์ที่ได้ไปไว้ใน IPCop โดยใช้โปรแกรม WinSCP

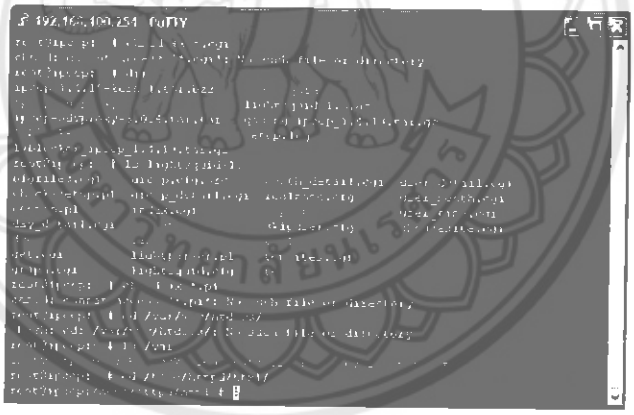


รูปที่ ข-39 อัพโหลดไฟล์ไปไว้ที่ IPCop Server ด้วย WinSCP

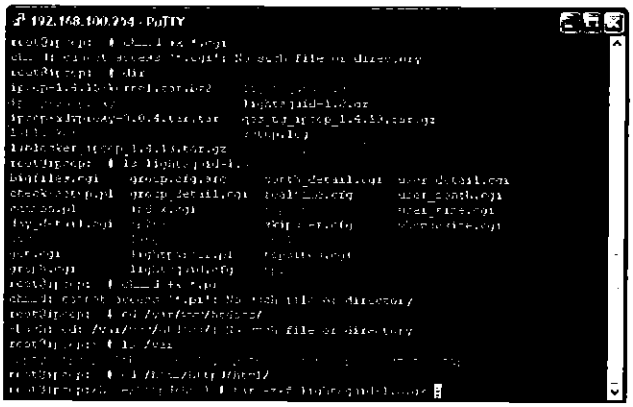
3. ใช้เมาส์ลากไฟล์ lightsquid-1.8.gz จากด้านซ้ายมือไปไว้ที่โฟล์เดอร์ /home/httpd/html ทางฝั่งของ IPCop ด้านขวามือ

4. เปิดโปรแกรม PuTTY เพื่อล็อกอินเข้าไปที่เครื่องของ IPCop

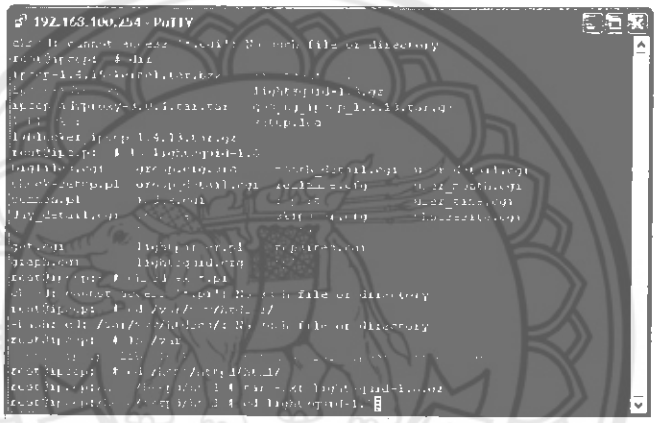
5. แตกไฟล์โดยใช้คำสั่งตามรูปข้างล่าง



รูปที่ ข-40 เข้าไปในไดเรกทอรี่ /home/httpd/html



รูปที่ ข-41 แตกไฟล์ โดยใช้คำสั่ง tar -zxf loghtsquid-1.8.gz

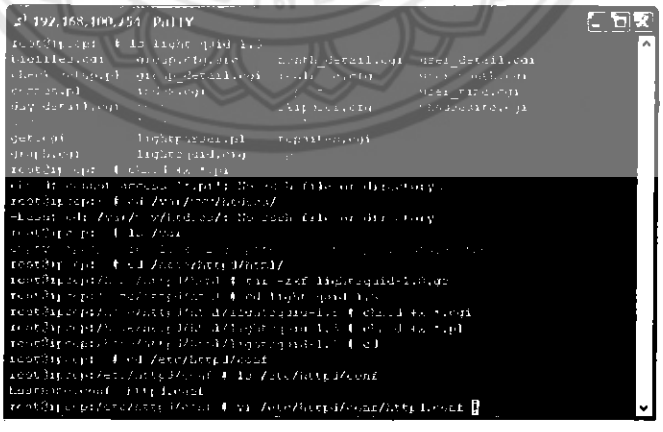


รูปที่ ข-42 เข้าไปในไดเรกทอรี่ของ lightsquid โดยใช้คำสั่ง cd lightsquid-1.8

รูปที่ ข-43 ใช้คำสั่ง chmod +x *.cgi

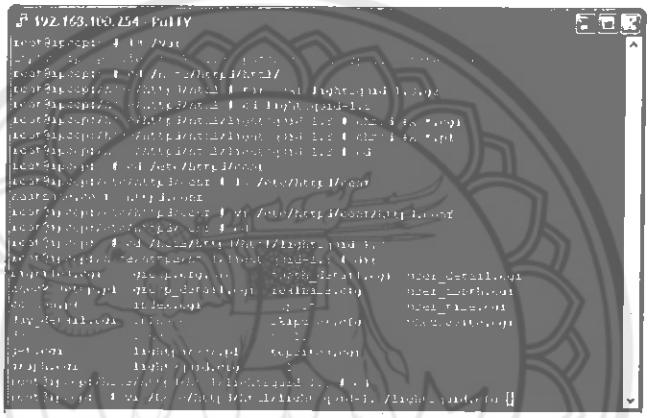
รูปที่ ข-44 ใช้คำสั่ง chmod +x *.pl

รูปที่ ข-45 ใช้คำสั่ง cd /etc/httpd/conf

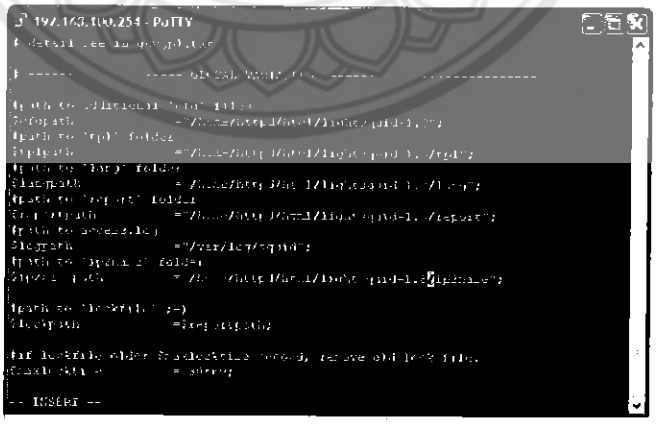


รูปที่ ข-46 ใช้คำสั่ง vi / etc/httpd/conf/httpd.conf

รูปที่ ข-47 เข้าไปยัง httpd.conf แก้ข้อความตามนี้



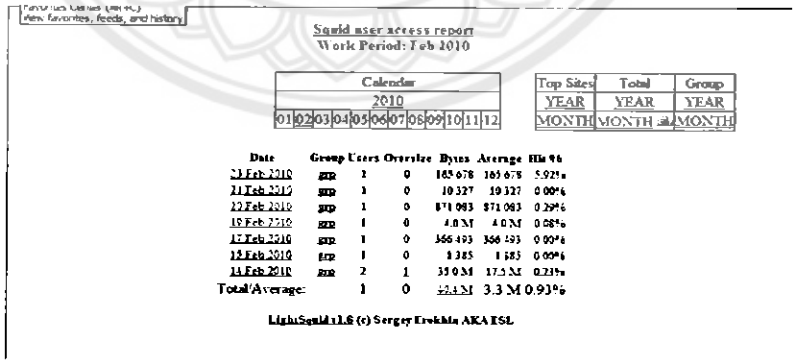
รูปที่ ข-48 พิมพ์ vi /home/httpd/html/lightsquiid-1.8/lightsquid.cfg



รูปที่ ข-49 เข้าไปยัง lightsquid.cfg แก้ข้อความตามนี้

รูปที่ ข-50 ทดสอบโดยการพิมพ์ ./check-setup.pl

รูปที่ ข-51 ใช้คำสั่ง ./lightparser.pl



Squid user access report
Work Period: Feb 2010

Calendar											
2010											
01	02	03	04	05	06	07	08	09	10	11	12

Top Sites	Total	Group
YEAR	YEAR	YEAR
MONTH	MONTH	MONTH

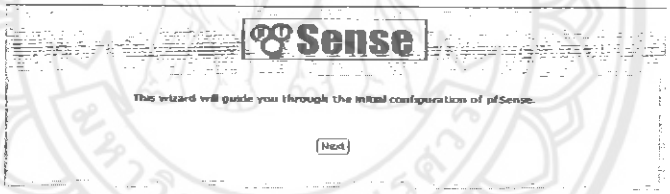
Date	Group	Users	Overvize	Bytes	Average	Hit %
3 Feb 2010	grp	1	0	165 678	165 678	5.92%
11 Feb 2010	grp	1	0	10 327	10 327	0.00%
12 Feb 2010	grp	1	0	871 083	871 083	0.29%
16 Feb 2010	grp	1	0	4.0 M	4.0 M	0.08%
17 Feb 2010	grp	1	0	366 493	366 493	0.00%
18 Feb 2010	grp	1	0	1 385	1 385	0.00%
14 Feb 2010	grp	2	1	35.0 M	17.5 M	0.23%
Total/Average:		1	0	43.4 M	3.3 M	0.93%

LightSquid v1.8 (c) Sergey Erokhin AKA ESL

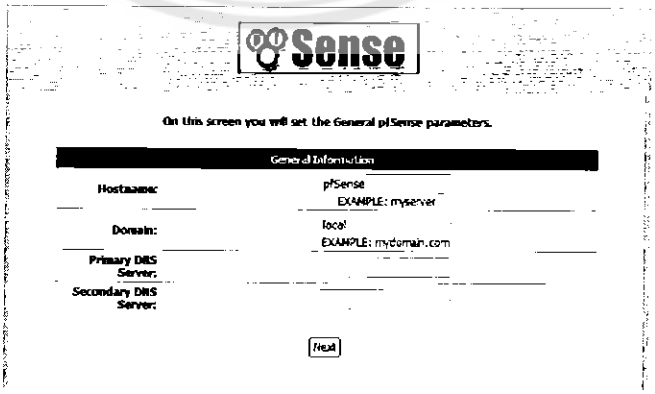
รูปที่ ข-52 แสดงหน้าหลัก Lightsquid

2. การ Config PFSense

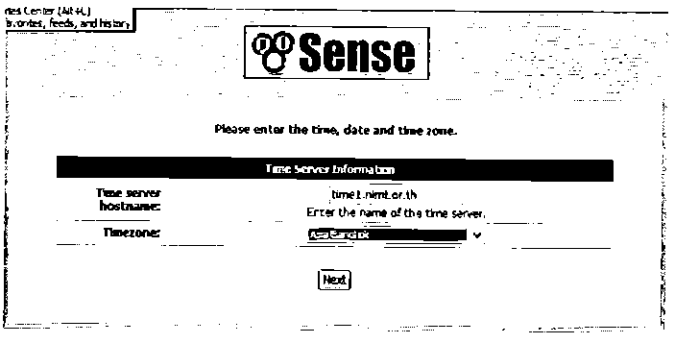
รูปที่ ข-53 แสดงการเข้าสู่ระบบ



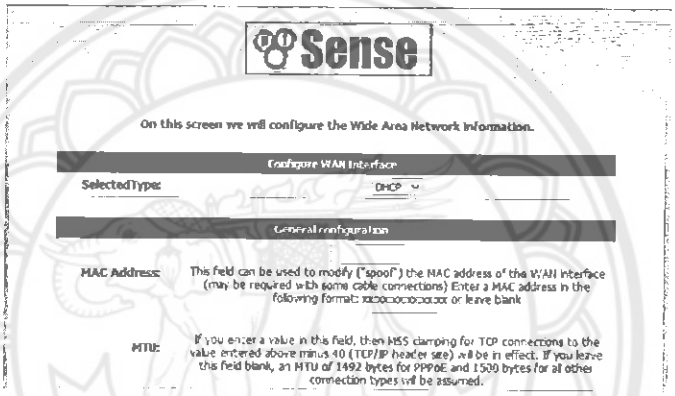
รูปที่ ข-54 กด Next เพื่อทำขั้นตอนต่อไป



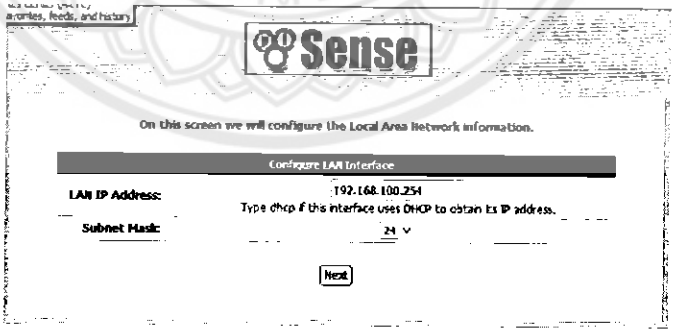
รูปที่ ข-55 การกำหนดค่า Hostname และ Domain



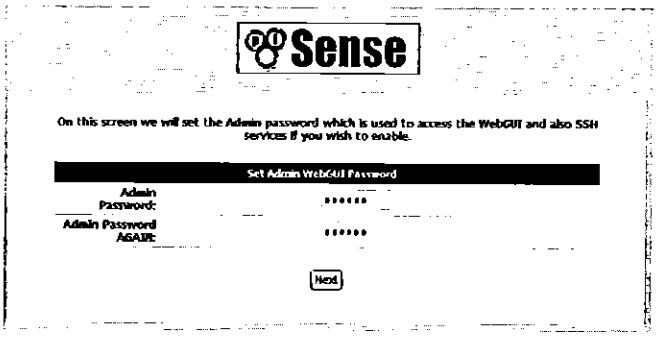
รูปที่ ข-56 ตั้งค่า Time Server Information



รูปที่ ข-57 ตั้งค่า Config WAN Interface

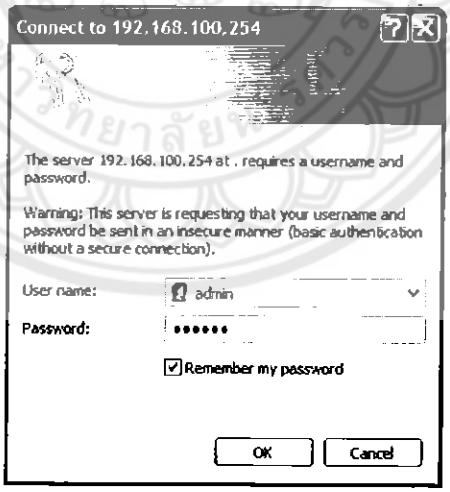


รูปที่ ข-58 ตั้งค่า Configure LAN Interface



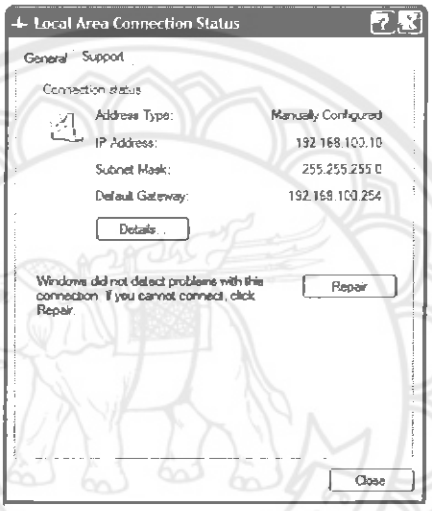
รูปที่ ข-59 กำหนดรหัสผ่านของ Admin

รูปที่ ข-60 กด Reload เสร็จสิ้นการ Config

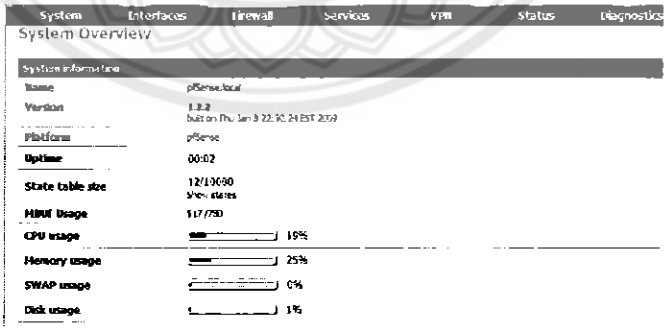


รูปที่ ข-61 แสดงการเข้าสู่ระบบ

รูปที่ ข-62 ระบบทำการ Reload

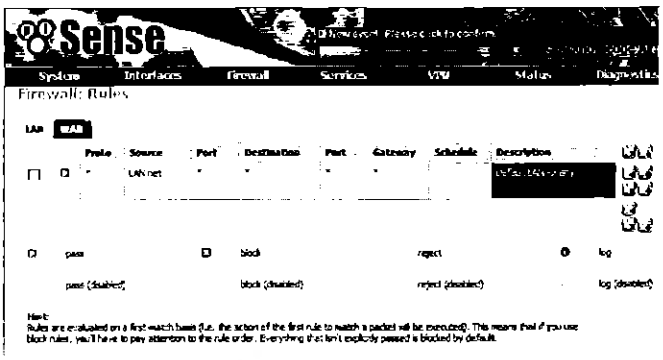


รูปที่ ข-63 ตั้งค่า IP Address ของเครื่องลูกข่าย

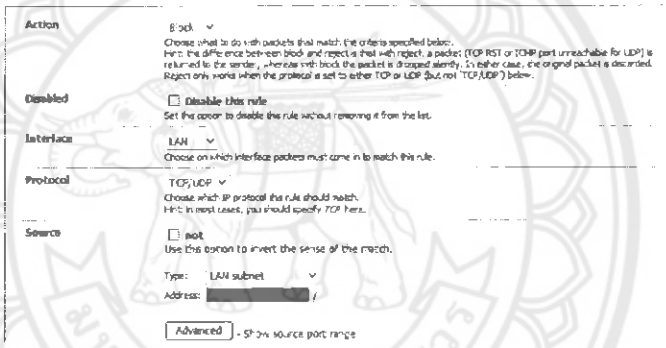


รูปที่ ข-64 แสดงหน้าหลักของ PFSense

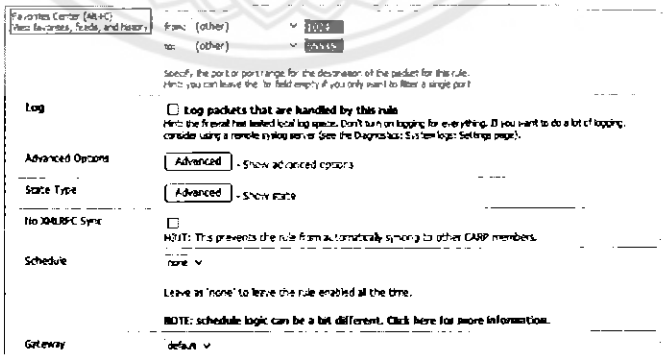
การ Block Port ทำได้โดยใช้เมนู Firewall -> Rules



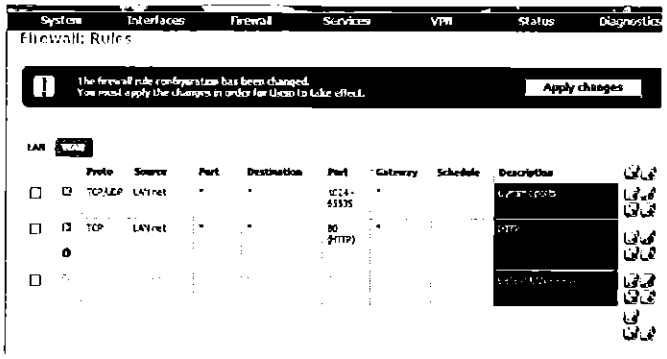
รูปที่ ข-65 แสดงหน้าหลักของ Firewall Rules ในส่วน LAN



รูปที่ ข-66 กำหนดกฎในการ Block Port (1024-65535)

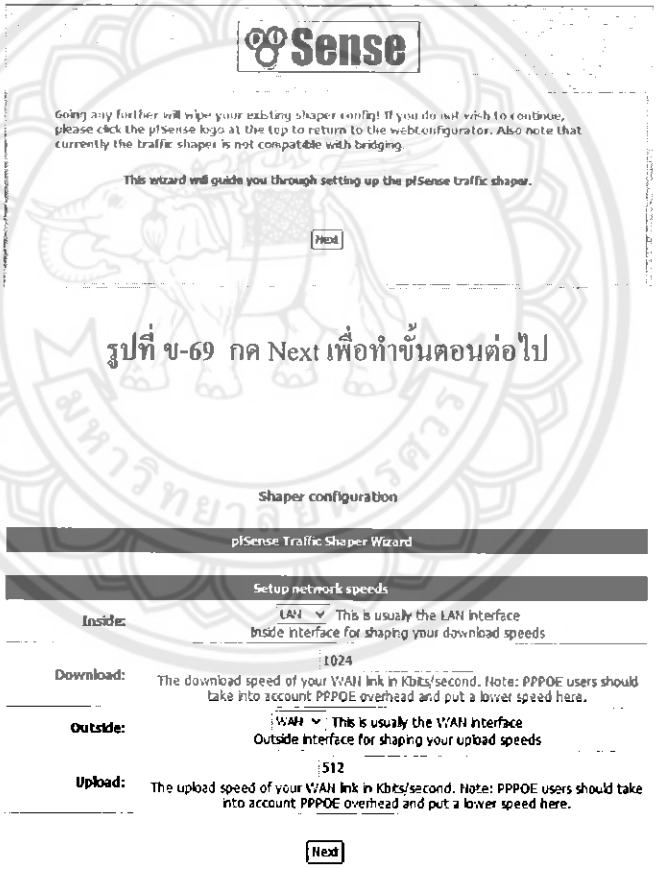


รูปที่ ข-67 กำหนดกฎในการ Block Port (1024-65535)



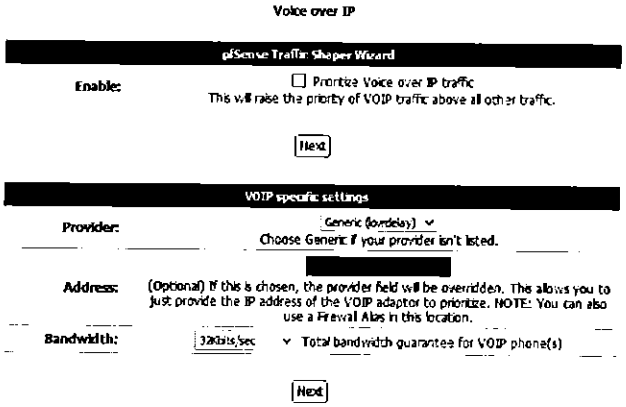
รูปที่ ข-68 แสดงการเปิด Port เกี่ยวกับการเข้าเว็บไซต์ และ Block Port (1024-65535)

การทำ Bandwidth Shaping ทำได้โดยใช้เมนู Firewall -> Traffic Shaper

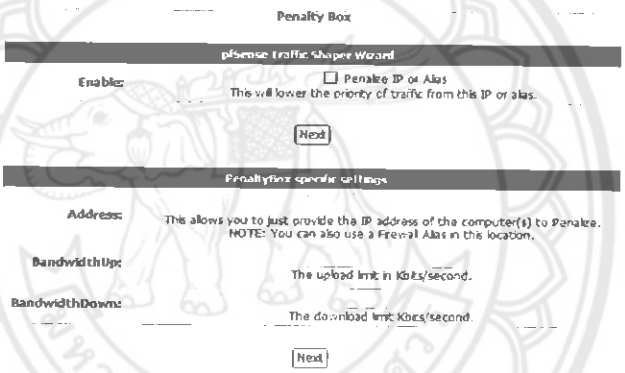


รูปที่ ข-69 กด Next เพื่อทำขั้นตอนต่อไป

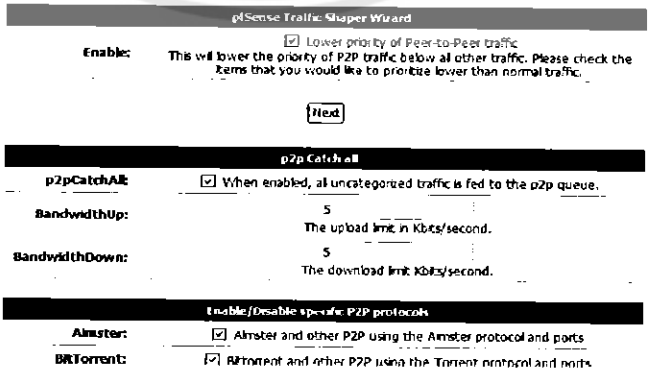
รูปที่ ข-70 กำหนดความเร็วให้กับ LAN และ WAN Interface กด Next เพื่อทำขั้นตอนต่อไป



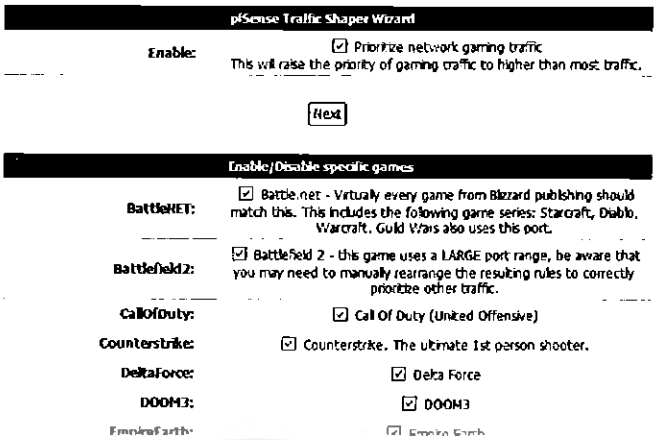
รูปที่ ข-71 กำหนด Voice over IP กด Next เพื่อทำขั้นตอนต่อไป



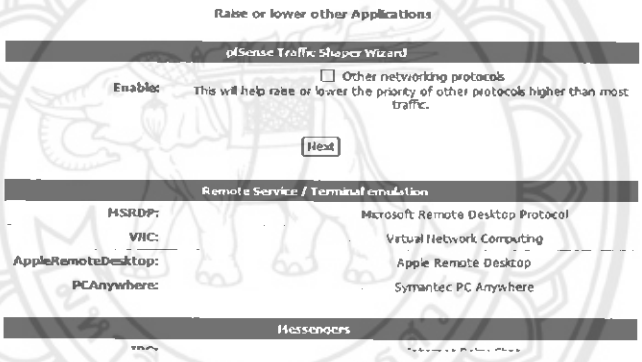
รูปที่ ข-72 กำหนด Penalty Box กด Next เพื่อทำขั้นตอนต่อไป



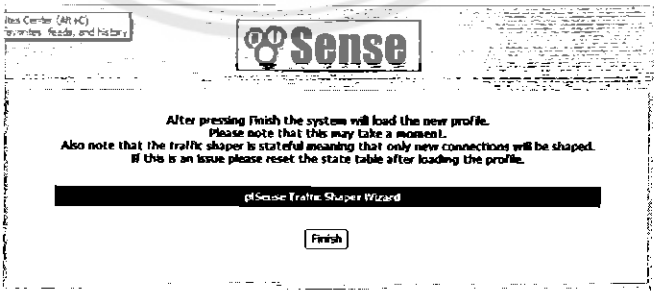
รูปที่ ข-73 กำหนดความเร็วในการดาวน์โหลดไฟล์ P2P กด Next เพื่อทำขั้นตอนต่อไป



รูปที่ ข-74 กำหนดความเร็วในการดาวน์โหลด path games กด Next เพื่อทำขั้นตอนต่อไป

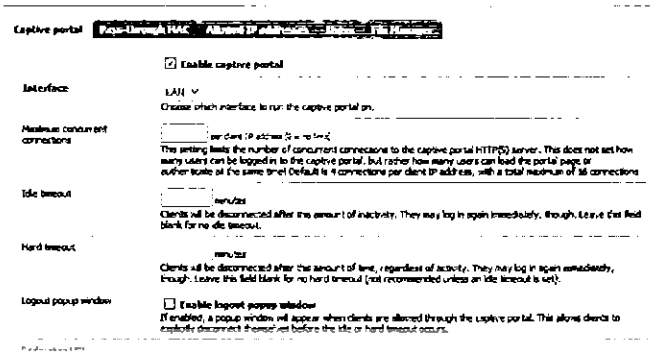


รูปที่ ข-75 กำหนดความสำคัญการดาวน์โหลด กด Next เพื่อทำขั้นตอนต่อไป



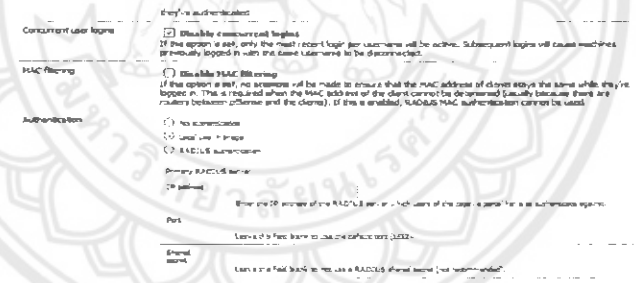
รูปที่ ข-76 กด Finish เพื่อสิ้นสุดการตั้งค่า

การทำ Authentication ทำได้โดยใช้เมนู Services -> Captive portal



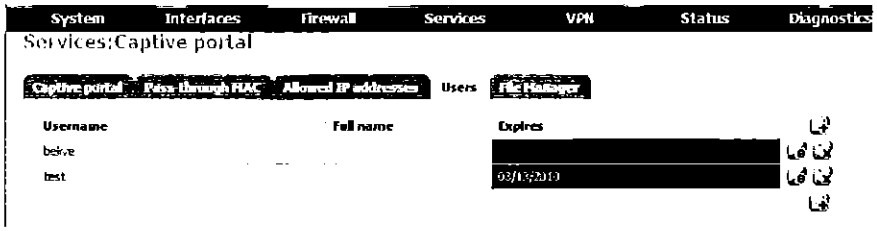
รูปที่ ข-77 แสดงหน้าหลักของ Captive portal

- TAB Captive portal : เลือก Enable captive portal
- Interface : เลือก Interface เป็น LAN



รูปที่ ข-78 แสดงหน้าหลักของ Captive portal

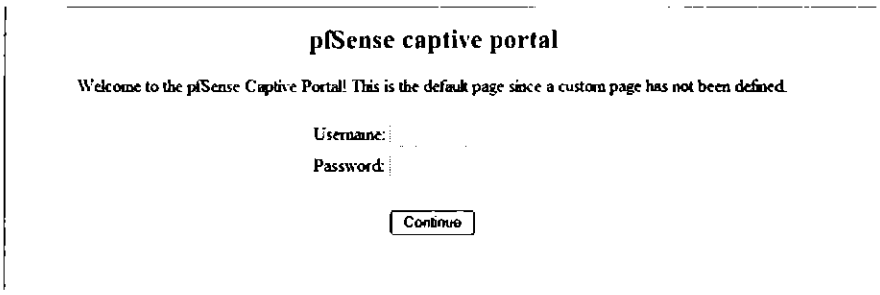
- Disable concurrent logins : ไม่สามารถใช้ชื่อผู้ใช้ล็อกอินพร้อมกันสองเครื่องขึ้นไปไม่ได้ เครื่องที่ล็อกอินก่อนจะหลุด
- Local user manager : ต้องการให้ระบบสอบถามชื่อผู้ใช้ และ รหัสผ่าน จาก PFSense



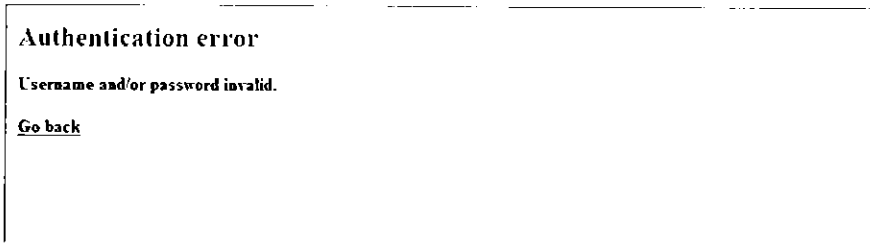
รูปที่ ข-79 แสดงชื่อของผู้ใช้ในโปรแกรม PFSense

รูปที่ ข-80 กำหนดชื่อของผู้ใช้ในโปรแกรม PFSense

- Username : ระบุชื่อที่ต้องการ
- Password : กำหนดรหัสผ่าน
- Full name : ชื่อเจ้าของ Username
- Expiration date : กำหนดวันหมดอายุของ Username



รูปที่ ข-81 หน้าต่างสำหรับล็อกอิน



รูปที่ ข-82 แสดงรูปเมื่อกรอกชื่อผู้ใช้ และ รหัสผ่านผิด

ภาคผนวก ค.

พอร์ต (Port)

1. Port ต่างๆ ที่จำเป็นที่ต้องใช้ในการสื่อสาร

ตารางที่ ค-1 ชนิดโปรโตคอลและหมายเลขพอร์ตสำหรับใช้โปรแกรมแชร์ (Share) ข้อมูลประเภท P2P

Application's Protocol	Port	Protocol		ลักษณะการใช้งาน
		TCP	UDP	
Azureus	6881 to 6889	✓	✓	✓
DC++	411,1025-32000	✓	✓	✓
Gnutella	6346	✓	✓	✓
Limewire	6346 to 6347	✓	✓	✓
Bit Torrent	-	-	-	✓

** โปรแกรมแชร์ (Share) ข้อมูลประเภท P2P

ตารางที่ ค-2 ชนิดโปรโตคอลและหมายเลขพอร์ตสำหรับการใช้งานโปรแกรมรับชมวิดีโอผ่านโครงข่ายอินเทอร์เน็ต

Application's Protocol	Port	Protocol		ลักษณะการใช้งาน
		TCP	UDP	
WebcamXP	8080,8090	✓		แชร์ VDO
QuickTime	6970-7000	✓	✓	แชร์ VDO
YouTube	80	✓		แชร์ VDO

** รับชมวีดีโอผ่านโครงข่ายอินเทอร์เน็ต (VDO Streaming)

ตารางที่ ค-3 ชนิดโปรโตคอลและหมายเลขพอร์ตสำหรับการใช้งานรับฟังเพลง Online

Application's Protocol	Port	Protocol		ลักษณะการใช้งาน
		TCP	UDP	
Winamp Streamming	8000-8001	✓		ฟังเพลง online
iTunes	3689	✓	✓	แชร์ไฟล์ ดนตรี
Windows Media Streaming	1755,7007	✓	✓	ฟังเพลง,ดูหนัง ตัวอย่าง Online

** รับฟังดนตรีผ่านโครงข่ายอินเทอร์เน็ต (VDO Streaming)

ตารางที่ ค-4 ชนิดโปรโตคอลและหมายเลขพอร์ตสำหรับการใช้งานสนทนา

Application's Protocol	Port	Protocol		ลักษณะการใช้งาน	
		TCP	UDP	ภาพ	เสียง
AOL Instant Messenger	5190	✓	✓	✓	✓
ICQ	4000		✓	✓	✓
MSN Messenger	1863,5190 6891-6901	✓	✓	✓	✓
Yahoo Messenger	5010	✓		✓	✓
TeamSpeak	8767,14534 51234	✓	✓		✓
Skype	80,443	✓			✓

** สนทนาผ่านโครงข่ายอินเทอร์เน็ต (Chat)

ตารางที่ ค-5 ชนิดโปรโตคอลและหมายเลขพอร์ตสำหรับการใช้งานโทรศัพท์ผ่านเครื่องคอมพิวเตอร์ (VoIP)

Application's Protocol	Port	Protocol		ลักษณะการใช้งาน
		TCP	UDP	
Net2Phone	6801		✓	✓
NetFone	10200	✓		✓
PhoneFree	1034-1035, 2644,8000, 9900-9901	✓	✓	✓
Speak Freely	2074-2076		✓	✓
Vonage	5061, 10000-20000		✓	✓
VPhone	11675	✓	✓	✓

** สามารถโทรศัพท์ผ่านโครงข่าย VoIP ได้

ตารางที่ ค-6 ชนิดโปรโตคอลและหมายเลขพอร์ตสำหรับการใช้งานเกมส์

Application's Protocol	Port	Protocol		ลักษณะการใช้งาน
		TCP	UDP	
Xbox	80,1900,3390,3074, 3776,3932,5555, 7777	✓	✓	เล่นเกมส์ออนไลน์
Gamespy Arcade	3783,6515,6500, 6667,13139,27900, 28900,29900,29901	✓	✓	เข้าไปดูเกมส์ต่างๆ
Age of Empires	2300-2400,6073, 47624	✓	✓	
Call of Duty	20500,20510,28960	✓	✓	✓
Counter-Strike	1200,27000-27015, 27020-27039	✓	✓	✓

Doom 3	27650,27666	✓	✓	✓
Everquest	1024,6000,7000	✓	✓	✓
Far Cry	49001-49002,49124	✓	✓	✓
FIFA	3658,10400-10499	✓	✓	✓
GTA 2	2300-2400,47624	✓	✓	✓
Half Life 2	1200,27000-27015, 27020-27039	✓	✓	✓
Microsoft Flight Simulator	2300-2400, 6073,23456,47624	✓	✓	✓
NBA Live	3658,9570, 18699-28600		✓	✓
Need For Speed	80,1030,3658,3659, 9442,13505,18210, 18215,30900-30999	✓	✓	✓
Neverwinter Nights	5120-5300,6500, 6667,27900,28900		✓	✓
NHL	3658,10300,13505	✓	✓	✓
No One Lives Forever	2300-2400, 7000-10000,27888	✓	✓	✓
Quake	27650,27910,27950, 27952,27960,27965	✓	✓	✓
Rainbow Six	80,2346-2348, 6667,7777-7787, 8777-8787, 40000-42999, 44000,45000	✓	✓	✓
Soldier of Fortune	28910-28915,20100-20112	✓	✓	✓
Starcraft	6112	✓	✓	✓

Tiger Woods PGA tour	80,443,9570,13505, 20803,20809,32768-65535	✓	✓	✓
Tribes	28000,28001	✓	✓	✓
Ultima Online	5001-5010,7775-7777,7575,8800-8900,9999	✓		✓
Unreal Tournament	7777-7788,8080,8777,9777,27900,42292	✓	✓	✓
Warcraft	6112-6119	✓	✓	✓
World of Warcraft	3724,6112,6881-6999	✓		✓
Worms Armageddon	80,6667,17010-17012	✓		✓

** เกมส์ออนไลน์

✓ เล่นเกมส์ออนไลน์ในห้องที่สร้างขึ้น

ตารางที่ ค-7 ชนิดโปรโตคอลและหมายเลขพอร์ตสำหรับการใช้งานโปรแกรมฐานข้อมูล

Application's Protocol	Port	Protocol		ลักษณะการใช้งาน
		TCP	UDP	
Microsoft SQL Server	1433-1434	✓	✓	ฐานข้อมูล
MySQL	3306	✓	✓	ฐานข้อมูล
Oracle SQL	1521,1522,1525,1529	✓		ฐานข้อมูล

ตารางที่ ค-8 ชนิดโปรโตคอลและหมายเลขพอร์ตสำหรับการใช้งาน

Application's Protocol	Port	Protocol		ลักษณะการใช้งาน
		TCP	UDP	
DNS	53	✓	✓	Domain Name System (DNS) protocol สำหรับเปลี่ยน Domain name เป็นเลข IP
IMAP	143	✓		สำหรับเชื่อมต่อโปรแกรม Outlook,Outlook express,Eudora และ Thunderbird เข้ากับ Mail Server
Remote Desktop	3389	✓	✓	ควบคุมเครื่องคอมพิวเตอร์จากตำแหน่งห่างไกล
HTTP	80,8080	✓		แสดงหน้า Web page ผ่านทางโปรแกรม Internet Explorer,Firefox และ Opera
LDAP	389	✓	✓	ถูกใช้เพื่อติดต่อไปยังฐานข้อมูลส่วนกลางเพื่อขอใช้บริการข้อมูลต่างๆจากเครื่องในโครงข่าย
NETBIOS	137-139	✓	✓	ใช้สำหรับส่งไฟล์ระหว่างเครื่องคอมพิวเตอร์ที่ใช้งานในระบบปฏิบัติการ windows
NNTP	119	✓		รับส่งข้อมูลกลับกลุ่มข่าว (Newsgroup) ผ่านโครงข่ายอินเทอร์เน็ต
Microsoft PPTP	1723	✓		สร้าง Vitual Private Network (VPN) ที่ใช้การเข้ารหัสซ่อนข้อมูลไม่ให้คนที่ไม่เกี่ยวข้องอ่านได้
POP3	110	✓		ดึงอีเมลล์จาก Mail Server
Microsoft Terminal Server/Citrix ICA	1494,1604		✓	ควบคุมเครื่องคอมพิวเตอร์จากระยะทางไกล
PCAnywhere	5632	✓	✓	ควบคุมเครื่องคอมพิวเตอร์จากระยะทางไกล
Real VNC	5900	✓	✓	ควบคุมเครื่องคอมพิวเตอร์จากระยะ

				ทางไกล
Tight VNC	5800,5500,5900	✓		ควบคุมเครื่องคอมพิวเตอร์จากระยะทางไกล
RIP	520		✓	Routing Information Protocol โปรโตคอลที่เป็นส่วนประกอบหลักอันหนึ่งข้างในอินเทอร์เน็ต
SSH	22	✓		สำหรับเพิ่มความปลอดภัยในการรับหรือส่งข้อมูลผ่านโครงข่ายอินเทอร์เน็ต
SMTP	25	✓		สำหรับส่งอีเมลล์จากเครื่องคอมพิวเตอร์ต้นทางไปยังปลายทาง
SNMP	161-162		✓	ถูกใช้โดยผู้ดูแลโครงข่ายเพื่อเก็บข้อมูลจากเครื่องคอมพิวเตอร์ต่างๆบนโครงข่าย
Shiva VPN	2233	✓	✓	สร้าง Vitual Private Network (VPN)
Wingate VPN	809	✓	✓	สร้าง Vitual Private Network (VPN)
Telnet	23	✓		ถูกใช้โดยผู้ดูแลโครงข่าย เพื่อเข้าไปล็อกออนยังหน้าจอของเครื่องเซิร์ฟเวอร์
HTTPS	443	✓	✓	ใช้การเข้ารหัสเพื่อปกปิดข้อมูลและสร้างความปลอดภัยในการใช้งาน Web รับส่งข้อมูลสำคัญ เช่น เลขที่บัญชีบัตรเครดิต
Kerberos	88	✓	✓	สร้างสิทธิการใช้งาน ใช้บนระบบปฏิบัติการ Window เท่านั้น
VNC	5800,5900	✓		ควบคุมเครื่องคอมพิวเตอร์จากระยะไกล

ภาคผนวก ง.

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๑๐ มิถุนายน พ.ศ. ๒๕๕๐

เป็นปีที่ ๖๒ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐"

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวัน นับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชบัญญัตินี้

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ นั้น

"ผู้ให้บริการ" หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

"ผู้ใช้บริการ" หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

"พนักงานเจ้าหน้าที่" หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

"รัฐมนตรี" หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

หมวด ๑
ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้ สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหาย แก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่ง ข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐

(๑) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลัง และไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(๒) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

มาตรา ๑๓ ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมา ตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

มาตรา ๑๕ ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือ

ปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักร และ

(๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ

จะต้องรับโทษภายในราชอาณาจักร

หมวด ๒

พนักงานเจ้าหน้าที่

มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการ ให้แก่พนักงานเจ้าหน้าที่

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อ ประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้

มาตรา ๑๙ การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจ เพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตาม พระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วยในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อ ที่ทำให้ต้องใช้อำนาจตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้ เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ

(๘) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา ๑๘ (๔) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา ๑๘ (๘) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้วพนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัด ไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้นให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึด หรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง

มาตรา ๒๐ ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสองลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้

มาตรา ๒๑ ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจ เพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์ นั้นระงับการใช้ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง

หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่ง ที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวงทั้งนี้เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้นตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

มาตรา ๒๒ ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ให้แก่บุคคลใดความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษ จำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๓ พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๔ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการ ที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๕ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจมีคำมั่น สัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้า สู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกิน เก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษ

เฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

มาตรา ๒๗ ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ ที่สั่งตามมาตรา ๑๘ หรือมาตรา ๒๐ หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา ๒๑ ต้องระวางโทษปรับไม่เกินสองแสนบาทและปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

มาตรา ๒๘ การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีกำหนด

มาตรา ๒๙ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้

ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้น ผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป

ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับ แนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง

มาตรา ๓๐ ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลซึ่งเกี่ยวข้อง

บัตรประจำตัวของพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้รับสนองพระบรมราชโองการ

พลเอก สุรยุทธ์ จุลานนท์

นายกรัฐมนตรี

<u>หมายเหตุ</u> :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญ ของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใดๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใดๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐรวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้

ประวัติผู้เขียนโครงงาน

ชื่อ นายอิษณัย วงศ์สิทธิกร

ภูมิลำเนา 46 ตำบล ปากน้ำโพธิ์ อำเภอเมือง
จังหวัด นครสวรรค์ 60000

ประวัติการศึกษา

- จบระดับมัธยมศึกษาจากโรงเรียนนครสวรรค์
- ปัจจุบันกำลังศึกษาอยู่ในระดับปริญญาตรีชั้นปีที่ 4
  สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
  มหาวิทยาลัยนเรศวร

E-mail : isanai20@hotmail.com

ชื่อ นายอนุชา ประภาสนิรัดิศัย

ภูมิลำเนา 137 หมู่ 13 ตำบล ออย อำเภอ ปง
จังหวัด พะเยา 56140

ประวัติการศึกษา

- จบระดับมัธยมศึกษาจากโรงเรียนปงพัฒนาวิทยาคม
- ปัจจุบันกำลังศึกษาอยู่ในระดับปริญญาตรีชั้นปีที่ 4
  สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
  มหาวิทยาลัยนเรศวร

E-mail : no_cpe@hotmail.com