การบริหารระบบเครือข่ายโดยใช้วิธีการตรวจจับแพ็กเก็ต

NETWORK MANAGEMENT SYSTEM USING PACKET DETECTION

โดย

นายยศวัฒน์ ลีลาแสงสาย

นายวรนิตย์ มีทิพย์กิจ

นายสราวุธ มลกระวิ

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2553

การบริหารระบบเครือข่ายโดยใช้วิธีการตรวจจับแพ็กเก็ต

NETWORK MANAGEMENT SYSTEM USING PACKET DETECTION

โดย

นายยศวัฒน์	ลีลาแสงสาย	50011249
นายวรนิตย์	มีทิพย์กิจ	50011360
นายสราวุธ	มลกระวิ	50011651

อาจารย์ที่ปรึกษา

ดร.สมปอง วิเศษพาณิชกิจ

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2553

ผ่านการตรวจชิ้นงานแล้ว

(ลงชื่อ).....

ผ่านการตรวจรูปเล่มแล้ว

(ลงชื่อ).....

ปริญญานิพนธ์ปีการศึกษา 2553

สาขาวิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง การบริหารระบบเครือข่ายโดยใช้วิธีการตรวจจับแพ็กเก็ต

NETWORK MANAGEMENT SYSTEM USING PACKET DETECTION

ผู้จัดทำ

1. นายยศวัฒน์ ลีลาแสงสาย 50011249
2. นายวรนิตย์ มีทิพย์กิจ 50011360
3. นายสราวุธ มลกระวิ 50011651

..... อาจารย์ที่ปรึกษา

(ดร. สมปอง วิเศษพาณิชกิจ)

กิตติกรรมประกาศ

รายงานฉบับนี้จะสำเร็จลุล่วงไปได้ด้วยดีเนื่องจากได้รับความอนุเคราะห์จากอาจารย์ ดร.สมปอง วิเศษพาณิชกิจ ที่ให้คำปรึกษาที่ดีตลอดเวลาในการทำโครงงานนี้ อีกทั้งยังคอยช่วยเหลือในด้านต่างๆ เป็นอย่างดีและขอบคุณบิดา มารดา ผู้ปกครอง ที่คอยดูแลเลี้ยงดูและส่งเสียค่าเล่าเรียนตลอดจนขอขอบพระคุณภาควิชาโทรคมนาคมที่ให้โอกาสคณะผู้จัดทำได้ทำโครงงานนี้และขอขอบคุณ เพื่อนๆ ที่คอยแนะนำให้ความช่วยเหลือเป็นอย่างดี

นายยศวัฒน์ ลีลาแสงสาย
นายวรนิตย์ มีทิพย์กิจ
นายสราวุธ มลกระวิ
ผู้จัดทำ

การบริหารระบบเครือข่ายโดยใช้วิธีการตรวจจับแพ็กเก็ต

NETWORK MANAGEMENT SYSTEM USING PACKET DETECTION

โดย นายยศวัฒน์ ลีลาแสงสาย 50011249
นายวรนิตย์ มีทิพย์กิจ 50011360
นายสราวุธ มลกระวิ 50011651

อาจารย์ที่ปรึกษา ดร.สมปอง วิเศษพาณิชกิจ

บทคัดย่อ

โครงงานนี้นำเสนอการตรวจสอบและจัดการระบบเครือข่ายโดยอิงกรณีศึกษา จากเครือข่ายของสาขาวิชาวิศวกรรมโทรคมนาคม โดยใช้โปรโตคอล SNMP ตรวจสอบข้อมูล จัดเก็บข้อมูลที่ได้ แจ้งเตือนเมื่อค่าที่สนใจมีค่ามากกว่าที่กำหนดไว้ เช่น ปริมาณข้อมูลขาเข้ามีค่ามากกว่าที่กำหนด หรือ ปริมาณข้อมูลขาออกมีค่ามากกว่าที่กำหนด และนำข้อมูลที่เก็บไว้มาแสดงผล โครงงานมีขอบเขตงาน 3 ส่วน คือ 1) ส่วนตรวจสอบ 2) ส่วนการเก็บบันทึกและแจ้งเตือนให้ผู้ดูแลระบบทราบ 3) ส่วนแสดงผลบนหน้าเว็บ เพื่อช่วยผู้ดูแลเครือข่ายในการบริหารจัดการเครือข่าย

ABSTRACT

This project presents the inspection and management network based on case study from network of major telecommunication Engineering. By used protocol SNMP check information and store data and notification when the value of interest is greater than the amount of input, For example the input traffic is higher than set value or the output traffic is higher than set value and show stored data to display. The first part is inspection and analysis based on condition. The second part is storage, record, and warning to the administrator. The other part is displayed on the Web applications. The system reduces the overwork of the network administrators.

สารบัญ

สารบัญ (ต่อ)

สารบัญรูป

สารบัญรูป (ต่อ)

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันเครือข่ายอินเทอร์เน็ตได้เข้ามามีบทบาทในชีวิตประจำวันมากขึ้น หน่วยงานต่างๆ ทั้งภาครัฐและเอกชนต่างมีเครือข่ายคอมพิวเตอร์เป็นของตนเองและเชื่อมโยงเข้าสู่เครือข่ายอินเทอร์เน็ต การบริหารจัดการเครือข่ายและการใช้ทรัพยากรที่มีในเครือข่ายอย่างมีประสิทธิภาพ ซึ่งเป็นปัญหาที่พบบ่อยในหน่วยงานขนาดกลางและขนาดเล็ก เช่น โรงเรียนและหน่วยงานราชการส่วนใหญ่จะขาดบุคลากรที่มีความรู้ความสามารถในการดูแลจัดการเครือข่าย ระบบช่วยบริหารจัดการเครือข่ายนี้จึงมีบทบาทที่สำคัญและเป็นที่ต้องการ โดยที่จะพัฒนาระบบให้เป็นระบบอัตโนมัติที่จะช่วยดูแลการใช้งานเครือข่ายให้มีความมั่นคงปลอดภัย จัดการให้มีการใช้งานทรัพยากรภายในเครือข่ายอย่างเต็มประสิทธิภาพ และแจ้งเตือนถึงสาเหตุ เมื่อมีความผิดปกติเกิดขึ้นในเครือข่าย โดยเน้นในเรื่องของระบบที่ใช้งานง่ายดังนั้นจึงได้แนวคิดเพื่อที่จะพัฒนาระบบการตรวจสอบและจัดการระบบเครือข่ายโดยอิงกรณีศึกษาจากเครือข่ายของสาขาวิชาโทรคมนาคมโดยใช้หลักการดังนี้ ใช้โปรโตคอล SNMP ตรวจสอบข้อมูล จัดเก็บข้อมูลที่ได้ และทำการแจ้งเตือนเมื่อค่าที่สนใจมีค่ามากกว่าที่กำหนดไว้ เช่น ปริมาณข้อมูลขาเข้ามีค่ามากกว่าที่กำหนด หรือ ปริมาณข้อมูลขาออกมีค่ามากกว่าที่กำหนด และนำข้อมูลที่เก็บไว้มาแสดงผล

โครงงานมีขอบเขตงาน 3 ส่วน คือ

1) ส่วนตรวจสอบ

2) ส่วนการเก็บบันทึกและแจ้งเตือนให้ผู้ดูแลระบบทราบ

3) ส่วนแสดงผลบนหน้าเว็บ

เพื่อให้ระบบสามารถทำการจัดการบริหารเครือข่ายได้ด้วยตัวเองและช่วยลดภาระงานของผู้ดูแลเครือข่ายได้

1.2 วัตถุประสงค์

1) เพื่อพัฒนาระบบบริหารจัดการเครือข่ายที่มีประสิทธิภาพ สำหรับองค์กรทั่วไปที่ขาดแคลนผู้เชี่ยวชาญด้านเครือข่าย
2) เพื่อตอบสนองความต้องการของหน่วยงานต่างๆที่ต้องการใช้ระบบบริหารจัดการเครือข่ายในการลดเวลาการจัดการกับปัญหาและข้อผิดพลาดบนเครือข่าย ซึ่งเป็นการลดภาระของผู้ดูแลระบบ

1.3 ขอบเขตของปริญญานิพนธ์

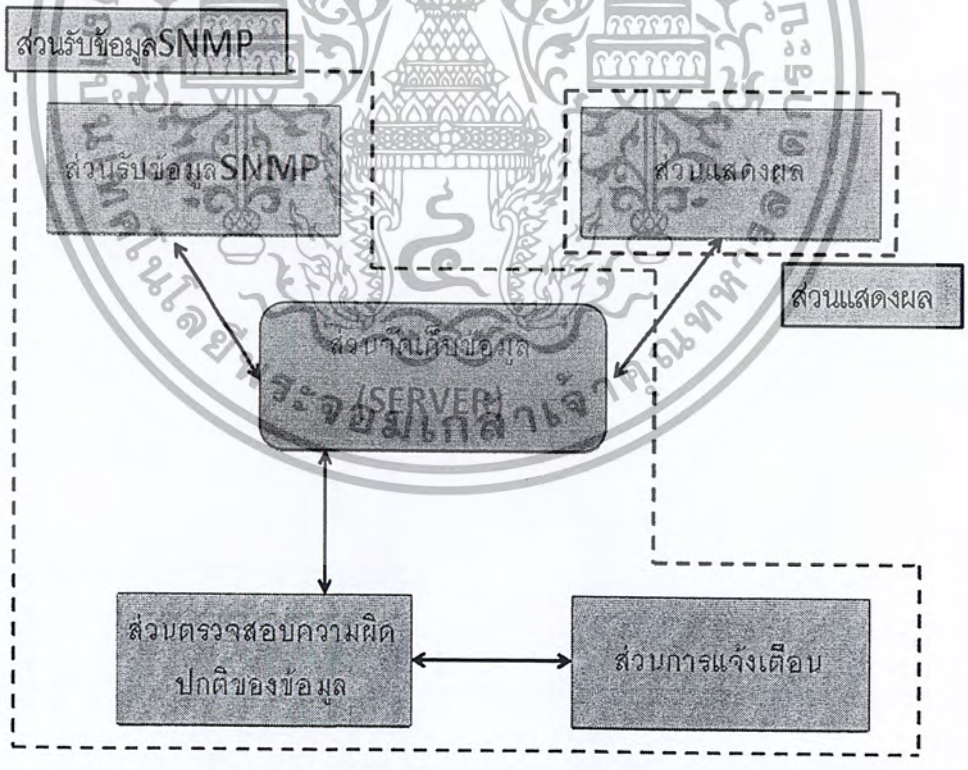
ตรวจจับปริมาณข้อมูลที่วิ่งภายในเครือข่ายจากการทำ MIRROR PORT และ Simple Network Management Protocol (SNMP) จัดเก็บข้อมูลที่ได้และทำการแจ้งเตือนเมื่อค่าที่สนใจมีค่ามากกว่าที่กำหนดไว้ และนำข้อมูลที่เก็บไว้มาแสดงผลบนหน้าเว็บเพจ

โดยภายในหน้าเว็บเพจสามารถทำการเพิ่ม ลบ แก้ไขอุปกรณ์ ตั้งค่าจัดการ OID ต่างๆ และสามารถแสดงข้อมูลปริมาณข้อมูลขาเข้า, ปริมาณข้อมูลขาออกในรูปแบบกราฟ, ปริมาณข้อมูลโดยรวมและ ปริมาณข้อมูลโพรโทคอลของแต่ละห้องภายในตึกภาควิชาโทรคมนาคม ชั้น 3 และสามารถดูปริมาณข้อมูลในเครือข่ายย้อนหลังได้

บทที่ 2

ทฤษฎีและหลักการที่เกี่ยวข้อง

การจัดทำโครงงานนี้มีวัตถุประสงค์เพื่อพัฒนาระบบเครือข่ายโดยใช้วิธีการตรวจจับแพ็กเก็ต จากรูปที่ 2.1 ส่วนรับข้อมูลจะมีส่วนย่อยๆแบ่งลงไปดังนี้คือ ส่วนรับข้อมูลซึ่งทำหน้าที่ส่งคำร้องขอข้อมูลจากโพรโทคอล SNMP หลังจากนั้นทำการรับและจัดเก็บข้อมูลที่ได้ลงไปในฐานข้อมูล และมีส่วนที่ทำการตรวจสอบว่าข้อมูลที่ทำการจัดเก็บมีความผิดปกติหรือไม่ หากมีจะทำการแจ้งเตือนและอีกส่วนคือส่วนแสดงผลสำหรับในส่วนนี้จะเป็นการแสดงผลข้อมูลที่ได้จากการเก็บชุดข้อมูลต่างๆลงในฐานข้อมูลโดยจะนำเอาข้อมูลที่เก็บอยู่ในฐานข้อมูลขึ้นมาแสดงผลในรูปแบบของของข้อมูลที่เก็บได้



รูปที่ 2.1 บล็อกไดอะแกรมแสดงการทำงานการบริหารระบบเครือข่ายโดยใช้วิธีการตรวจจับแพ็กเก็ต

ดังนั้นเพื่อให้เกิดองค์ความรู้ในการพัฒนาระบบดังกล่าวผู้จัดทำจึงได้ศึกษาทฤษฎี โดยครอบคลุมหัวข้อต่างๆดังนี้

1) พื้นฐานการบริหารเครือข่าย (ส่วนดึงข้อมูล SNMP)
2) เอสเอ็นเอ็มพี (ส่วนดึงข้อมูล SNMP)
3) ฐานข้อมูลสารสนเทศการจัดการ (ส่วนดึงข้อมูล SNMP)
4) หลักการทำงานของ SNMP (ส่วนดึงข้อมูล SNMP)
5) ระบบปฏิบัติการอูบุนตู (ระบบปฏิบัติการที่ใช้อยู่บนเครื่อง Server โดยอยู่ในส่วนจัดเก็บข้อมูล)
6) พีเอชพี (ภาษาที่ใช้ในการเขียนโปรแกรมติดต่อเพื่อพัฒนาโปรแกรมในส่วนดึงข้อมูล SNMP)
7) มายเอสคิวแอล (ฐานข้อมูลที่ใช้เก็บข้อมูล ในส่วนของการจัดเก็บข้อมูล)
8) อาปาเช่ (โปรแกรมที่ทำให้เครื่อง Server สามารถติดต่อกับเครื่องลูกข่ายและฐานข้อมูลผ่านเว็บเพจได้)
9) มิรเรอร์พอร์ท (Mirror Port)
10) ลิบพีแคบ (Libpcap) เพื่อใช้ดักจับแพ็กเกต (Packet capture library)
11) เจพีกราฟ (Jpgraph) เป็นโมดูลที่ใช้ในการสร้างกราฟโดยใช้ภาษา PHP

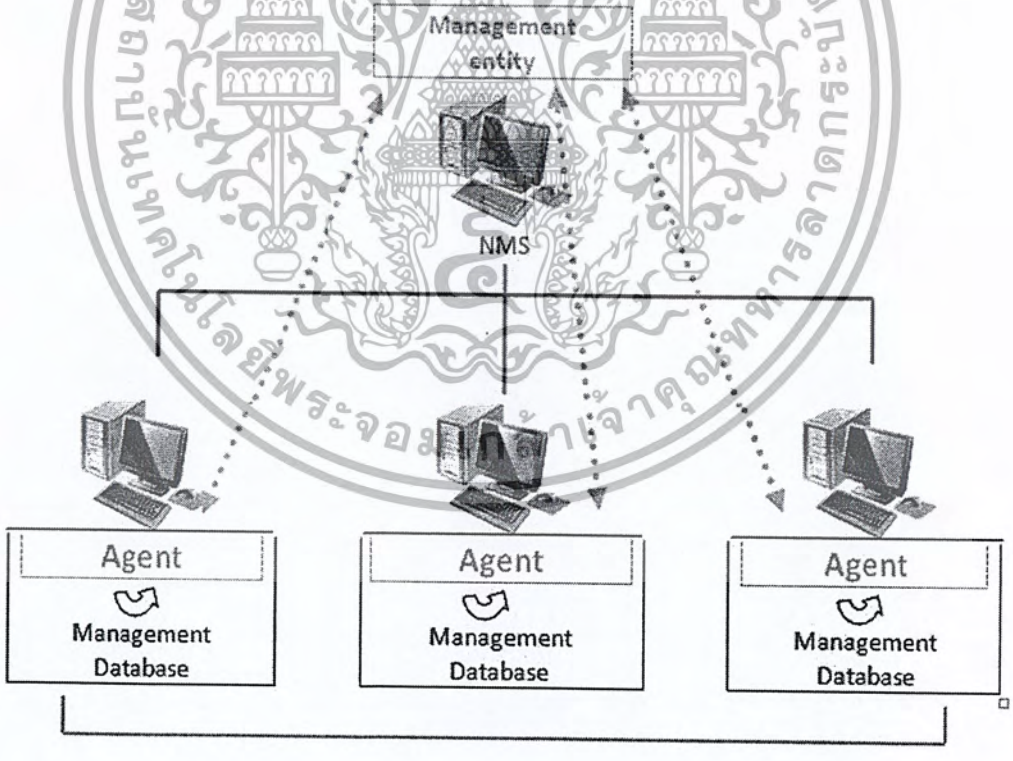
2.1 พื้นฐานการบริหารเครือข่าย

การบริหารจัดการระบบเครือข่ายจัดเป็นสิ่งสำคัญยิ่งสำหรับองค์กรที่มีการใช้งานคอมพิวเตอร์เป็นแบบเครือข่าย แต่มักจะถูกสนใจเป็นอันดับท้าย ๆ หรือจนกว่าจะมีปัญหาเกิดขึ้น ในระบบเครือข่ายการบริหารจัดการเครือข่ายมีความสำคัญและความจำเป็นตั้งแต่เริ่มออกแบบระบบเครือข่ายจนถึงขั้นตอนการติดตั้งการใช้งานและมีการขยายเครือข่ายล้วนต้องการเทคนิคและเครื่องมือในการบริหารจัดการเครือข่ายที่ดี

ประโยชน์จากการใช้คอมพิวเตอร์และเครือข่ายคือช่วยประหยัดเวลาและค่าใช้จ่าย แต่ในขณะเดียวกันการใช้คอมพิวเตอร์ก็ต้องลงทุนทั้งเวลา และค่าใช้จ่ายเพื่อดูแลให้คอมพิวเตอร์และเครือข่ายทำงานได้ด้วย เครือข่ายขนาดใหญ่ที่ประกอบด้วยคอมพิวเตอร์และอุปกรณ์จำนวน

มาก จะทำงานได้อย่างมีประสิทธิภาพจำเป็นต้องใช้คอมพิวเตอร์ช่วยบริหารและจัดการตัวระบบเครือข่ายด้วยตัวเองด้วย

การบริหารเครือข่ายดังรูปที่ 2.2 คือการตรวจสอบ ควบคุม และวางแผนการใช้ทรัพยากรระบบเพื่อให้เครือข่ายทำงานได้อย่างมีประสิทธิภาพและสามารถตรวจหาจุดบกพร่องที่เกิดขึ้น เพื่อแก้ปัญหาได้อย่างรวดเร็ว โดยทั่วไปจะมีการกำหนดให้คอมพิวเตอร์อย่างน้อยหนึ่งเครื่องในเครือข่าย ทำหน้าที่เป็นตัวจัดการหรือเรียกว่า Manager เพื่อใช้เป็นสถานีจัดการอาจเรียกอีกชื่อว่า สถานีจัดการเครือข่าย (Network management station) หรือ NMS โดยมีการแลกเปลี่ยนข้อมูลระหว่างเครื่องที่ใช้จัดการ และเครื่องลูกข่ายจะส่งผ่านข้อมูลโดยอาศัยโพรโทคอลที่เป็นมาตรฐานกลางคือ โพรโทคอล SNMP



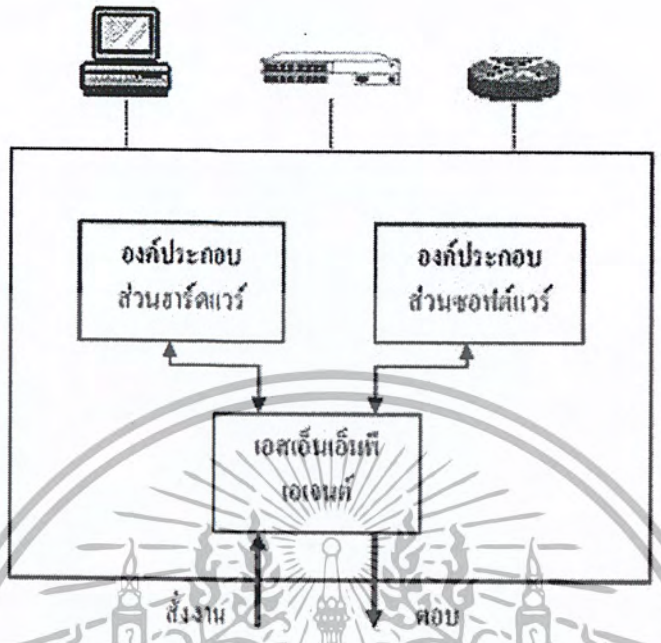
รูปที่ 2.2 องค์ประกอบในการจัดการเครือข่าย [1]

2.2 เอสเอ็นเอ็มพี (Simple Network Management Protocol: SNMP)

SNMP ย่อมาจาก Simple Network Management Protocol (SNMP) เป็นโพรโทคอลที่ทำงานอยู่ในชั้นโปรแกรมประยุกต์(Application Layer) และเป็นส่วนหนึ่งของชุดโพรโทคอลทีซีพี/ไอพี(TCP/IP) โดยมีรูปแบบในการส่งผ่านข้อมูลแบบ UDP ที่ Port 161 โดยอาศัยสถานีจัดการเครือข่ายส่วนกลางทำหน้าที่ดูแล ตรวจสอบ และควบคุมการทำงานของอุปกรณ์เครือข่าย ทำให้ผู้ดูแลเครือข่าย(Network Manager) สามารถตรวจสอบการทำงานของเครือข่ายได้อย่างต่อเนื่องและสามารถใช้งานกับเครื่องมือบริหารจัดการเครือข่ายของหลายค่าย และยังสามารถใช้กับอุปกรณ์เครือข่ายหลายชนิด ไม่ว่าจะเป็น File Server, Network Interface Card (NIC), Router, Repeater, Bridge และ Hub เป็นต้น การทำงานของ SNMP นั้นจะทำงานเป็นอิสระจากเครือข่าย หมายความว่าการทำงานจะไม่ขึ้นอยู่กับ โพรโทคอล(Protocol) ที่ใช้ในการเชื่อมต่อระหว่างเครือข่ายทำให้ SNMP สามารถวิเคราะห์การทำงานของเครือข่ายเช่น แพ็กเก็ตที่ไม่สมบูรณ์ หรือการ Broadcast โดยไม่จำเป็นต้องรู้ข้อมูลของแต่ละสถานีเชื่อมโยงที่ติดต่อสื่อสารกัน นอกจากนี้การทำงานของ SNMP ยังใช้หน่วยความจำ (Memory) ไม่มากนัก การที่จะใช้โพรโทคอล SNMP ในการติดต่อจากเครื่องที่ใช้จัดการ ไปยังเครื่องลูกข่ายได้นั้น เครื่องลูกข่ายจะต้องทำการติดตั้งโปรแกรม SNMP Agent ก่อนเพื่อให้เครื่องลูกข่ายมีความสามารถเป็น Agent ที่มีความสามารถในการตอบกลับข้อมูลทางโพรโทคอล SNMP

2.2.1 SNMP AGENT

การจัดการเครือข่าย ใน ทีซีพี/ไอพี(TCP/IP) อาศัยรูปแบบการจัดการมาตรฐานตามข้อกำหนดของโพรโทคอล SNMP (Simple Network Management Protocol) ซึ่งเป็นโพรโทคอลประยุกต์ที่กำหนดรูปแบบและกรรมวิธีจัดการเครือข่าย อุปกรณ์เครือข่ายที่สามารถตอบสนองคำร้องขอจากเครื่องที่ใช้จัดการเครือข่ายเรียกอีกอย่างนึงว่า Agent อาจเป็น PC, Modem, Hub, Switch หรือ Router อุปกรณ์เหล่านี้อาจมีส่วนทำงานที่เป็นซอฟต์แวร์และฮาร์ดแวร์ และมี SNMP Agent เชื่อมต่ออยู่ด้วย ดังรูปที่ 2.3



รูปที่ 2.3 องค์ประกอบภายในของ SNMP Agent [2]

โดยเมื่อ เครื่องที่ใช้จัดการ ร้องขอข้อมูลและปรับเปลี่ยนการทำงานของซอฟต์แวร์และฮาร์ดแวร์ของ Agent แล้ว Agent ก็จะทำการตอบสนอง ซึ่งข้อมูลที่ Agent จะทำการตอบกลับคำร้องขอจากเครื่องจัดการ โดย Agent จะทำการดึงข้อมูลจากฐานข้อมูลสารสนเทศ (MIB) การจัดการในตัวเองส่งกลับไปให้เครื่องจัดการ

2.3 ฐานข้อมูลสารสนเทศการจัดการ (Management Information Base: MIB)

Agent ประกอบด้วยส่วนสำคัญสองส่วนคือ Protocol Engine และฐานข้อมูลสารสนเทศการจัดการ (Management Information Base: MIB) โดย Protocol Engine ทำหน้าที่ประมวลคำสั่งที่มาจาก NMS ซึ่งได้แก่ รับคำสั่ง ถอดรหัสคำสั่ง ทำงานตามคำสั่งและส่งผลกลับ ส่วนฐานข้อมูลสารสนเทศการจัดการหรือเรียกสั้นๆว่า MIB เป็นส่วนที่เก็บตัวแปรและค่าที่กำหนดการทำงานประจำของอุปกรณ์ ซึ่ง MIB มีองค์ส่วนประกอบดังนี้

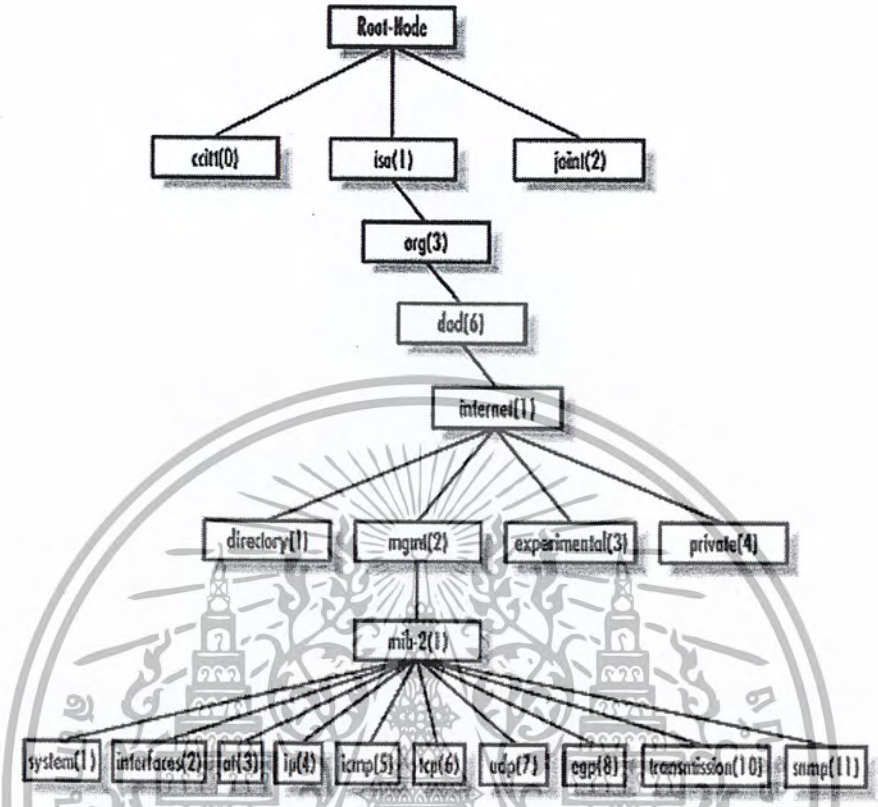
2.3.1 OBJECT IDENTIFIER (OID)

ภายใน MIB ประกอบด้วยตัวแปรจำนวนมากที่เรียกโดยทั่วไปว่า Managed Object ในความหมายนี้เป็นชื่อที่ใช้เรียกตัวแปร และลักษณะเฉพาะของตัวแปรใน MIB ซึ่งไม่เกี่ยวข้องกับเรื่องของการเขียนโปรแกรมเชิงวัตถุ(Object Oriented Programming) Object ใน SNMP มีลักษณะเช่นเดียวกับเรคคอร์ดในฐานข้อมูล แต่ละ Object จะมีชื่อเฉพาะเรียกว่า OBJECT IDENTIFIER หรือเรียกโดยย่อว่า OID เพื่อใช้อ้างอิงถึง Object นั้น Object ทุกตัวมีนิยามที่กำหนดชื่อ แบบข้อมูล สิทธิ์การเข้าถึง คำอธิบาย ลักษณะและค่าข้อมูล

2.3.2 โครงสร้าง MIB

ข้อมูลประจำอุปกรณ์เครือข่ายชิ้นหนึ่งๆมีได้หลายอย่าง อีกทั้งอุปกรณ์ต่างประเภทกันย่อมมีข้อมูลประจำอุปกรณ์แตกต่างกัน ดังนั้นการสอบถาม(อ่าน) หรือเปลี่ยนค่า(เขียน)ในฐานข้อมูลจึงต้องมีรูปแบบมาตรฐานให้กับอุปกรณ์ทุกประเภท โครงสร้างต้นไม้แบบลำดับชั้นเป็นโครงสร้างที่เหมาะสมสำหรับเพื่อใช้จัดการตัวแปรเหล่านี้ จากรูปที่ 2.4 เป็นภาพที่แสดงข้อมูล หรือ Object ของ SNMP ในโครงสร้างแบบต้นไม้ซึ่งนิยมเรียกว่า MIB Tree แต่ละโหนดซึ่งแทน Object หนึ่งๆ มีชื่อพร้อมทั้งเลขฐานสิบกำกับประจำโหนดเพื่อใช้อ้างอิง ยกเว้นรากซึ่งไม่มีชื่อกำกับลำดับชั้นแรกจะมีโหนดหลักสามโหนดซึ่งกำหนดองค์กรสามกลุ่มคือ iso,ccit,joint-iso-ccit ภายใน iso มีโหนดลำดับที่สามคือ org กำหนดองค์กรนานาชาติ และส่วนหนึ่งขององค์กรนี้คือ dod หรือ Department of Defend และมีโหนด Internet เพื่อกำหนดกลุ่มการจัดการเครือข่ายในอินเทอร์เน็ต เมื่อต้องการอ้างอิงถึงโหนดใดในโครงสร้างให้เขียนหมายเลขจากรากไปตามเส้นทางถึงโหนดนั้นและคั่นด้วยจุด ลำดับตัวเลขนี้เรียกว่า OBJECT IDENTIFIER จากรูปที่ 2.4

ตัวอย่างเช่น 1.3.6.1.2.1.1 เป็น OBJECT IDENTIFIER โดยที่มีชื่อสมนัยกันคือ iso.org.dod.internet.mgmt.mib-2.system ที่อยู่ภายในกลุ่ม mib-2 หรือ 1.3.6.1.2.1



รูปที่ 2.4 Object ของ SNMP ในโครงสร้างแบบต้นไม้ [3]

2.4 หลักการทำงานของ SNMP

SNMP เป็นโพรโทคอลที่ช่วยในการจัดการและบริหาร Network ได้จากศูนย์กลาง SNMP เป็นที่นิยมใช้กันมากในระบบบริหารเครือข่าย โดยทำหน้าที่ในการสื่อสารระหว่างเครื่องที่ใช้ในการจัดการเครือข่าย Management Station (MS) กับ เครื่องลูกข่าย Management Agent (MA) ภายในระบบบริหารเครือข่าย

SNMP เป็นโพรโทคอลในชั้นโปรแกรมประยุกต์ของ TCP/IP Stack ทำงานกับ User Datagram Protocol (UDP) ทั้งนี้เนื่องจากการทำงานของ UDP เป็นแบบ connectionless คือไม่ต้องมีการสร้างการเชื่อมต่อก่อนการส่งข้อมูล

2.4.1 การทำงานของโพรโทคอล SNMP

การติดต่อระหว่างสถานีจัดการกับ เครื่องลูกข่าย มีรูปแบบในการติดต่อหลายรูปแบบด้วยกัน ตามวัตถุประสงค์ในการติดต่อซึ่งตาม SNMP รุ่นที่ 1 มีด้วยกัน 5 แบบคือ

2.4.1.1 GetRequest

ใช้สอบถามข้อมูลจากเครื่องลูกข่าย ที่อยู่บนเครือข่ายที่ต้องการตรวจสอบในระบบเครือข่าย GetRequest เป็น Message ที่เครื่องจัดการเครือข่ายส่งไปยังเครื่องลูกข่าย เพื่อบอกว่าเครื่องจัดการเครือข่าย ต้องการทราบข้อมูลอะไรจากเครื่องลูกข่าย ซึ่งกำหนดสิ่งที่ต้องการด้วย OID ที่ส่งไปพร้อมกับ Message เช่น เครื่องจัดการเครือข่าย ระบุ OID เป็น 1.3.6.1.2.1.1 ซึ่งเป็นการระบุว่าต้องการทราบข้อมูล System ซึ่งเครื่องจัดการเครือข่ายก็จะตอบข้อมูลกลับมาด้วย GetRespone

2.4.1.2 GetNextRequest

ใช้สอบถามข้อมูลที่เรียงเป็นลำดับ เช่นข้อมูลที่เก็บอยู่ในรูป ตารางหรือในกรณีที่ไม่ทราบชื่อตัวแปรที่แน่ชัด GetNextRequest Message ชนิดนี้จะต่างจาก GetRequest ตรงที่ข้อมูลที่ส่งกลับมาจากเครื่องลูกข่าย จะไม่ใช่ข้อมูลของ OID ที่เครื่องที่ใช้จัดการส่งไปให้แต่จะเป็นข้อมูลของ OID ของตัวถัดไป ซึ่งจะใช้ใน กรณีตัวที่ใช้จัดการไม่สามารถที่จะระบุ OID ได้ โดยจะใช้ Message GetNextRequest นี้ไปในลักษณะของการ ท่องเข้าไปใน tree ตัวอย่าง เช่น เครื่องที่ใช้จัดการส่ง Message GetNextRequest ที่ให้ OBJECT IDENTIFIER เป็น 1.3.6.1.2.1 เป็นการเข้าถึง mib-2 ใน MIB tree โดยที่ไม่ได้ระบุว่าต้องการทราบข้อมูลในกลุ่ม mib-2 ดังนั้น เมื่อเครื่องลูกข่ายส่ง Message GetResponse กลับมาให้มันก็จะส่งค่าของ OID เป็น 1.2.6.1.2.1.1 ซึ่งเป็นค่าของ system ที่อยู่ในกลุ่ม mib-2 ซึ่งเป็นค่าของ OBJECT IDENTIFIER ตัวถัดไปใน tree นั่นเอง

2.4.1.3 GetResponse

เครื่องลูกข่ายส่งคำตอบกลับมายังผู้สอบถามด้วย GetResponse เป็น Message ที่เครื่องลูกข่ายใช้ในการส่งผลลัพธ์กลับมาให้เครื่องที่ใช้จัดการ เนื่องจากที่ เครื่องที่ใช้จัดการได้ทำการส่ง Message GetRequest, GetNextRequest, SetRequest ไปให้

2.4.1.4 SetRequest

ใช้เปลี่ยนแปลงค่าตัวแปรที่เครื่องลูกข่าย รับผิดชอบอยู่ SetRequest เป็น Message ที่เครื่องที่ใช้จัดการใช้บอกให้เครื่องลูกข่าย เปลี่ยนแปลงค่า Configuration ต่างๆของข้อมูลใน MIB ของอุปกรณ์นั้นๆ

2.4.1.5 Trap

ใช้แจ้งเหตุการณ์ที่เกิดขึ้นในระบบเครือข่าย เช่น การเริ่มต้นทำงานใหม่ของอุปกรณ์ หรือ เส้นทางขัดข้อง Trap เป็น Message ที่เครื่องลูกข่ายส่งไปให้เครื่องที่ใช้จัดการเพื่อรายงานเหตุการณ์หรือปัญหาที่เกิดขึ้น จากเครื่องลูกข่ายโดยตรง ไม่ได้มีการร้องขอข้อมูลจากเครื่องแม่ข่ายใดๆทั้งสิ้น

2.5 ระบบปฏิบัติการอูบุนตู (Ubuntu)

ระบบปฏิบัติการอูบุนตู (Ubuntu) เป็นชุดแจกจ่ายลินุกซ์ (Linux Distribution) ซึ่งใช้งานได้ฟรีๆโดยฟรีในความหมายนี้มีสองประการ

1)ใช้ฟรี (FreeBeer) คือสามารถใช้งานได้โดยไม่เสียค่าใช้จ่ายใดๆ

2) เสรีภาพ (Freedom) คือมีอิสระในการใช้งานสามารถใช้งานแก้ไขดัดแปลงแต่งเติมแจกจ่ายคัดลอกได้ตามต้องการ

โดยอูบุนตู นี้เองจะประกอบด้วยซอฟต์แวร์โอเพนซอร์ส คุณภาพดีหลายๆ ตัว (ยกเว้นบางตัวอาจไม่ใช่โอเพนซอร์ส เช่น driver อุปกรณ์ต่างๆ ที่จำเป็นต้องใช้ให้ระบบทำงานได้เต็มประสิทธิภาพ โดย อูบุนตู เองจะไม่แถมพวกนี้ลงในแผ่นติดตั้งให้มากจะต้องติดตั้งภายหลังผ่าน

อินเทอร์เน็ต) อูบุนตูนี้พัฒนาโดยชุมชนโดยมีบริษัท Canonical ให้การสนับสนุน ดังนั้นใครๆก็ตาม สามารถมีส่วนร่วมในการพัฒนาอูบุนตูได้เช่นเดียวกันอูบุนตู มีการออกรุ่นใหม่ทุกๆ 6 เดือน โดยในแต่ละรุ่นจะมีการสนับสนุน(มีอัพเดตต่างๆ ให้ และสามารถติดตั้งโปรแกรมจากคลังแพคเกจ) ยาว 18 เดือน และรุ่นที่ต่อท้ายด้วย LTS (ปัจจุบันนี้คือ 10.04) จะมีการสนับสนุนนานเป็นพิเศษถึง 3 ปีบนเดสก์ท็อป และ 5 ปีบนเซิร์ฟเวอร์ และสามารถอัพเกรดระหว่างรุ่นต่างๆได้ (แต่อาจไม่ค่อยดีในบางรุ่นควรจะติดตั้งใหม่) ข้อดีอย่างหนึ่ง ในการใช้ อูบุนตู คือซอฟต์แวร์ของอูบุนตู รุ่นล่าสุดนั้นจะสดใหม่อยู่เสมอ ทำให้เราทราบถึงการพัฒนาการของลินุกซ์ได้แต่ขณะเดียวกันระบบก็ยังมีเสถียรภาพ

2.6 พีเอชพี (PHP)

พีเอชพี (PHP) คือ ภาษาคอมพิวเตอร์ในลักษณะเซิร์ฟเวอร์-ไซด์ สคริปต์ โดยลิขสิทธิ์อยู่ในลักษณะโอเพนซอร์ส ภาษาพีเอชพีใช้สำหรับจัดทำเว็บไซต์ โดยมีรากฐานโครงสร้างคำสั่งมาจากภาษา ภาษาซี ภาษาจาวา และ ภาษาเพิร์ล ซึ่ง ภาษาพีเอชพี นั้นง่ายต่อการเรียนรู้ ซึ่งเป้าหมายหลักของภาษานี้ คือให้นักพัฒนาเว็บไซต์สามารถเขียนเว็บเพจที่มีความตอบโต้ได้อย่างรวดเร็ว

2.6.1 คุณสมบัติ

พีเอชพีเป็นภาษาที่เรียนรู้และเริ่มต้นได้ไม่ยาก โดยมีเครื่องมือช่วยเหลือและคู่มือที่สามารถหาอ่านได้ฟรีบนอินเทอร์เน็ต ความสามารถการประมวลผลหลักของพีเอชพี ได้แก่ การสร้างเนื้อหาอัตโนมัติจัดการคำสั่ง การอ่านข้อมูลจากผู้ใช้และประมวลผล การอ่านข้อมูลจากฐานข้อมูล ความสามารถจัดการกับคุกกี้ ซึ่งทำงานเช่นเดียวกับโปรแกรมในลักษณะซีจีไอ(CGI) คุณสมบัติอื่นเช่น การประมวลผลตามบรรทัดคำสั่ง (command line scripting) ทำให้ผู้เขียนโปรแกรมสร้างสคริปต์พีเอชพี ทำงานผ่านพีเอชพีพาร์เซอร์ (PHP parser) โดยไม่ต้องผ่านเซิร์ฟเวอร์หรือเบราว์เซอร์

2.6.2 การรองรับพีเอชพี

คำสั่งของพีเอชพี สามารถสร้างผ่านทางโปรแกรมแก้ไขข้อความทั่วไป เช่น Notepad หรือ vi ซึ่งทำให้การทำงานพีเอชพี สามารถทำงานได้ในระบบปฏิบัติการหลักเกือบ

ทั้งหมด โดยเมื่อเขียนคำสั่งแล้วนำมาประมวลผลด้วย Apache, Apache Tomcat, Microsoft Internet Information Services (IIS) สำหรับส่วนหลักของ พีเอชพี ยังมี Module ในการรองรับซีจีไอมาตรฐาน ซึ่งพีเอชพี สามารถทำงานเป็นตัวประมวลผลซีจีไอด้วย และมีอิสรภาพในการเลือกระบบปฏิบัติการ และ เครื่องบริการเว็บ นอกจากนี้ยังสามารถใช้สร้างโปรแกรมโครงสร้าง สร้างโปรแกรมเชิงวัตถุ (OOP) หรือสร้างโปรแกรมที่รวมทั้งสองอย่างเข้าด้วยกัน แม้ว่าความสามารถของคำสั่ง OOP มาตรฐานในเวอร์ชันนี้ยังไม่สมบูรณ์ แต่ตัวไลบรารีทั้งหลายของโปรแกรม และตัวโปรแกรมประยุกต์ (รวมถึง PEAR library) ได้ถูกเขียนขึ้นโดยใช้รูปแบบการเขียนแบบ OOP เท่านั้น

พีเอชพีสามารถทำงานร่วมกับฐานข้อมูลได้หลายชนิด ซึ่งฐานข้อมูลส่วนหนึ่งที่รองรับได้แก่ Oracle, PostgreSQL, MySQL, ODBC โครงสร้างของฐานข้อมูลแบบ DBX ซึ่งทำให้พีเอชพีใช้กับฐานข้อมูลอะไรก็ได้ที่รองรับรูปแบบนี้ และพีเอชพียังรองรับ ODBC (Open Database Connection) ซึ่งเป็นมาตรฐานการเชื่อมต่อฐานข้อมูลที่ใช้กันแพร่หลายอีกด้วย คุณสามารถเชื่อมต่อกับฐานข้อมูลต่างๆ ที่รองรับมาตรฐานโลกนี้ได้

พีเอชพียังสามารถรองรับการสื่อสารกับการบริการในโพรโทคอลต่างๆ เช่น LDAP IMAP SNMP NNTP POP3 HTTP COM (บนวินโดวส์) และอื่นๆ อีกมากมาย คุณสามารถเปิด Socket บนเครื่องข่ายโดยตรง และ ตอบโต้โดยใช้ โพรโทคอลใดๆ ก็ได้

2.7 มายเอสคิวแอล (MySQL)

เป็นระบบจัดการฐานข้อมูลโดยใช้ภาษาเอสคิวแอล(SQL) แม้ว่า มายเอสคิวแอล เป็นซอฟต์แวร์โอเพนซอร์ส โดยมีการพัฒนาภายใต้บริษัท มายเอสคิวแอล AB ในประเทศสวีเดน โดยจัดการ มายเอสคิวแอล ทั้งในแบบที่ให้ใช้ฟรี และแบบที่ใช้ในเชิงธุรกิจมายเอสคิวแอล สร้างขึ้นโดยชาวสวีเดน 2 คน และชาวฟินแลนด์ ชื่อ David Axmark, Allan Larsson และ Michael "Monty" Widenius ปัจจุบันบริษัทออเรเคิล(Oracle) เข้าซื้อกิจการของ มายเอสคิวแอล AB เรียบร้อยแล้ว ฉะนั้นผลิตภัณฑ์ภายใต้ มายเอสคิวแอล AB ทั้งหมดจะตกเป็นของออเรเคิล

2.7.1 รุ่นของผลิตภัณฑ์

รุ่นของผลิตภัณฑ์นั้นแบ่งออกมาได้สามสายการผลิต ได้แก่ เวอร์ชันใช้ฟรี เวอร์ชันการค้า และเวอร์ชันที่สนับสนุนกับผลิตภัณฑ์ SAP (MAX DB) ความแตกต่างคือเวอร์ชันคอมมิวนิตี้นั้นสามารถนำไปใช้งานได้ฟรีแต่ขาดการสนับ สนุนหรือการช่วยเหลือเมื่อมีปัญหาเกิดขึ้น, เวอร์ชันที่เป็นคอมเมอร์เชียลนั้นให้บริการด้านความสนับสนุนเมื่อมีปัญหา (ซื้อบริการ) สรุปคร่าวๆ ประเภทดาต้าเบสให้เลือกใช้ดังนี้

- มายเอสคิวแอล เอนเทอร์ไพรส์ Enterprise
- มายเอสคิวแอล คลัสเตอร์ Cluster
- มายเอสคิวแอล Embedded
- มายเอสคิวแอล Community (โอเพนซอร์สเวอร์ชัน)

2.7.2 การใช้งาน

มายเอสคิวแอล เป็นที่นิยมใช้กันมากสำหรับฐานข้อมูลสำหรับเว็บไซต์ เช่น มีเดียวิกิ และ phpBB และนิยมใช้งานร่วมกับภาษาโปรแกรมพีเอชพี ซึ่งมักจะได้ชื่อว่าเป็นคู่ จะเห็นได้จากคู่มือคอมพิวเตอร์ต่างๆ ที่จะสอนการใช้งานมายเอสคิวแอล และพีเอชพี ควบคู่กันไป นอกจากนี้ หลายภาษาโปรแกรมที่สามารถทำงานร่วมกับฐานข้อมูลมายเอสคิวแอล ซึ่งรวมถึง ภาษาซี ซีพลัสพลัส ปาสคาล ซีชาร์ป ภาษาจาวา ภาษาเพิร์ล พีเอชพี ไพทอน รูบี และภาษาอื่น ใช้งานผ่าน API สำหรับโปรแกรมที่ติดต่อผ่าน ODBC หรือ ส่วนเชื่อมต่อกับภาษาอื่น (database connector) เช่น เอเอสพี สามารถเรียกใช้ มายเอสคิวแอล ผ่านทาง MyODBC,ADO,ADO.NET เป็นต้น

2.7.3 โปรแกรมช่วยในการจัดการฐานข้อมูล และ ทำงานกับฐานข้อมูล

ในการจัดการฐานข้อมูล มายเอสคิวแอล คุณสามารถใช้โปรแกรมแบบ Command-line เพื่อจัดการฐานข้อมูล (โดยใช้คำสั่ง: มายเอสคิวแอล และ มายเอสคิวแอลแอดมิน เป็นต้น) หรือจะดาวน์โหลดโปรแกรมจัดการฐานข้อมูลแบบ GUI จากเว็บไซต์ของ มายเอสคิวแอล ซึ่งคือโปรแกรม: มายเอสคิวแอล Administrator และ มายเอสคิวแอล Query Browser. เป็นต้น

2.7.4 ส่วนเชื่อมต่อกับภาษาการพัฒนาอื่น (database connector)

มีส่วนติดต่อ (interface) เพื่อเชื่อมต่อกับภาษาในการพัฒนา อื่นๆ เพื่อให้เข้าถึงฟังก์ชันการทำงานกับฐานข้อมูล มายเอสคิวแอล ได้เช่น ODBC (Open Database Connector) อันเป็นมาตรฐานกลางที่กำหนดมาเพื่อให้ใช้เป็นสะพานในการเชื่อมต่อกับโปรแกรม หรือระบบอื่นๆ เช่น MyODBC อันเป็นไดรเวอร์เพื่อใช้สำหรับการเชื่อมต่อในระบบปฏิบัติการวินโดว์, JDBC คลาสส่วนเชื่อมต่อสำหรับจาวา เพื่อใช้ในการติดต่อกับ มายเอสคิวแอล และมี API (Application Programming Interface) ต่างๆมีให้เลือกใช้มากมายในการที่เข้าถึง มายเอสคิวแอล โดยไม่ขึ้นอยู่กับภาษาการพัฒนาใดภาษาหนึ่ง

นอกเหนือจาก ตัวเชื่อมต่อกับภาษาอื่น (Connector) ที่ได้กล่าวมาแล้ว ยังมี API ที่สนับสนุนในขณะนี้คือ

- DBI สำหรับการเชื่อมต่อกับ ภาษา perl
- Ruby สำหรับการเชื่อมต่อกับ ภาษา ruby
- ไพธอน สำหรับการเชื่อมต่อกับภาษาไพธอน
- .NET สำหรับการเชื่อมกับภาษา .NET framework
- MySQL++ สำหรับเชื่อมต่อกับภาษา C++
- Ch สำหรับการเชื่อมต่อกับ Ch (C/C++ interpreter)
- พีเอชพี สำหรับการเชื่อมต่อกับภาษาพีเอชพี

2.8 อาปาเช่ (Apache web server)

อาปาเช่พัฒนามาจาก HTTPD Web Server ที่มีกลุ่มผู้พัฒนาอยู่ก่อนแล้วโดย ร็อบ แม็คคูล (Rob McCool) ที่ NCSA (National Center for Supercomputing Applications) มหาวิทยาลัยอิลลินอยส์ เออร์แบนา-แชมเปญจน์ สหรัฐอเมริกา แต่หลังจากที่ แม็คคูล ออกจาก NCS และหันไปให้ความสนใจกับโครงการอื่นๆ มากกว่าทำให้ HTTPD เว็บเซิร์ฟเวอร์ ถูกปล่อยทิ้งไม่มีผู้พัฒนาต่อ แต่เนื่องจากเป็นซอฟต์แวร์ที่อยู่ภายใต้ลิขสิทธิ์ กนู คือ ทุกคนมีสิทธิ์ที่จะนำเอาซอร์สโค้ดไปพัฒนาต่อได้ ทำให้มีผู้ใช้กลุ่มหนึ่งได้พัฒนาโปรแกรมขึ้นมาเพื่ออุดช่องโหว่ ที่มีอยู่เดิม และยังได้รวบรวมเอาข้อมูลการพัฒนา และการแก้ไขต่างๆ แต่ข้อมูลเหล่านี้อยู่ตามที่ต่างๆ ไม่ได้รวมอยู่ในที่ที่เดียวกัน จนในที่สุด ไบอัน บีเลนดอร์ฟ (Brian Behlendorf) ได้สร้างจดหมายกลุ่ม

(mailing list) ขึ้นมาเพื่อนำเอาข้อมูลเหล่านี้เข้าไว้เป็นกลุ่มเดียวกัน เพื่อให้สามารถเข้าถึงข้อมูลเหล่านี้ได้ง่ายยิ่งขึ้น และในที่สุดกลุ่มผู้พัฒนาได้เรียกตัวเองว่า กลุ่มอาปาเช่ (Apache Group) และได้ปล่อยซอฟต์แวร์ HTTPD เว็บเซิร์ฟเวอร์ ที่พัฒนาโดยการนำเอาแพทช์หลายๆ ตัวที่ผู้ใช้ได้พัฒนาขึ้นเพื่อปรับปรุงการทำงานของซอต์ฟแวร์ตัวเดิมให้มีประสิทธิภาพมากยิ่งขึ้น ตั้งแต่ ปี พ.ศ. 2539 อาปาเช่ได้รับความนิยมขึ้นเรื่อยๆ จนปัจจุบันได้รับความนิยมเป็นอันดับหนึ่ง มีผู้ใช้งาน อยู่ประมาณ 50% ของเว็บเซิร์ฟเวอร์ที่ให้บริการอยู่ทั้งหมด

2.8.1 ความสามารถ

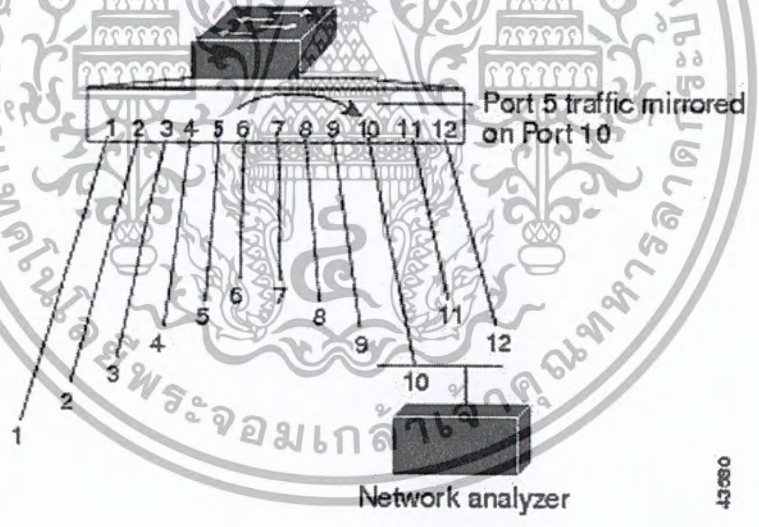
การที่อาปาเช่เป็นซอฟต์แวร์ที่อยู่ในลักษณะของโอเพ่นซอร์สที่เปิดให้บุคคลทั่วไปสามารถเข้ามาร่วมพัฒนาส่วนต่างๆของอาปาเช่ได้ ซึ่งทำให้เกิดเป็น โมดูล ที่เกิดประโยชน์มากมาย เช่น mod_perl, mod_python หรือ mod_php ซึ่งเป็นโมดูลที่ทำให้อาปาเช่สามารถใช้ประโยชน์ และทำงานร่วมกับภาษาอื่นได้ แทนที่จะเป็นเพียงเซิร์ฟเวอร์ที่ให้บริการเพียงแค่เอชทีเอ็มแอล อย่างเดียว นอกจากนี้อาปาเช่เองยังมีความสามารถอื่นๆ ด้วย เช่น การยืนยันตัวบุคคล (mod_auth, mod_access, mod_digest) หรือเพิ่มความปลอดภัยในการสื่อสารผ่านโพรโทคอล https (mod_ssl) นอกจากนี้ ก็ยังมีโมดูลอื่นๆ ที่ได้รับความนิยมใช้ เช่น mod_vhost ทำให้สามารถสร้างโฮสท์เสมือน www.sample.com, wiki.sample.com, mail.sample.com หรือ www.ilovewiki.org ภายในเครื่องเดียวกันได้ หรือ mod_rewrite เป็นเครื่องมือที่จะช่วยให้ url ของเว็บนั้นอ่านง่ายขึ้น ยกตัวอย่างเช่น จากเดิมต้องอ้างถึงเว็บไซต์แห่งหนึ่งด้วยการพิมพ์ http://www.yourdomain.com/board/quiestion.php?action=viewtopic&qid=2xDffw แต่หลังจากใช้ mod_rewrite จะทำให้สั้นลง กลายเป็น http://www.yourdomain.com/board/question/2xDffw ซึ่งที่อยู่หลังนี้จะขึ้นอยู่กับว่าผู้ดูแลเว็บไซต์ต้องการให้อยู่ในลักษณะใด

2.9 มิรเรอร์พอร์ท (Mirror Port)

Switch เป็นอุปกรณ์สำหรับเชื่อมต่อ เครือข่ายท้องถิ่น หรือ แลน (LAN)ประเภทเดียวกัน ใช้โพรโตคอลเดียวกัน สองวงเข้าด้วยกัน เช่น ใช้เชื่อมต่อ อีเธอร์เน็ตแลน (Ethernet LAN)หรือโทเคนริงก์แลน (Token Ring LAN) ทั้งนี้ สวิตช์ จะมีความสามารถในการเชื่อมต่อ ฮาร์ดแวร์และ

Switchg ถ้าต้องการที่จะตรวจข้อมูลที่วิ่งผ่าน Switch สามารถที่จะทำมิรเรอร์พอร์ท(Mirror port) คือ มันจะเป็นพอร์ตที่สะท้อนทุกๆอย่างที่วิ่งผ่านเข้ามาใน Switch แล้วเมื่อวิ่งเข้ามาแล้วพอร์ตนี้ก็จะเห็นว่ามีอะไรจากที่ไหนจะไปไหนสามารถใช้โปรแกรมหรืออุปกรณ์ Hardware ตรวจจับได้

Mirror Port ใช้บนเครือข่ายสวิตช์เพื่อส่งสำเนาของแพ็คเก็ตเครือข่ายที่เห็นในพอร์ตสวิทช์หนึ่ง (หรือ VLAN ทั้งหมด) เพื่อตรวจสอบเครือข่ายการเชื่อมต่อบนพอร์ตสวิทช์อื่น หรือบางครั้งก็จะเรียก ว่าSPAN port (Switch port Analyzer) มันจะสำเนาข้อมูลพอร์ทต้นทาง มายังพอร์ทปลายทาง ดังรูปที่ 2.5 จะทำการสำเนาข้อมูลที่พอร์ท 5 มายังพอร์ทที่ 10 ที่ทำการต่อกับโปรแกรมประเภทวิเคราะห์เครือข่าย ซึ่งพอร์ทต้นทาง เช่น Physical Port หรือ VLAN หรือ PortChannal การใช้งานก็จะเป็นประเภทการวิเคราะห์เครือข่ายโดยใช้โปรแกรม sniffer เป็นต้น



รูปที่ 2.5 ลักษณะการทำ Mirror Port [4]

2.10 ลิบพีแคบ (Libpcap)

Libpcap เป็นชุดคำสั่งแบบ Opensource ที่ให้การเชื่อมต่อทางเครือข่ายกับระบบตรวจจับแพคเก็จถูกสร้างในปี 1994 โดย Mccane, Leres และ Jacobson นักวิจัยที่ Lawrence Berkeley National National Laboratory จาก university of california ที่ Berkeley ซึ่งเป็นส่วนหนึ่งของงานวิจัย สืบหาและเพิ่มประสิทธิภาพให้แก่ TCP และ internet gateway เป้าหมายของผู้สร้าง Libpcap คือเพื่อสร้าง platform independent API เพื่อขจัดความต้องการของ platform dependent ของโมดูลที่ใช้จับแพคเก็จในแต่ละ application เพราะในแต่ละระบบปฏิบัติการจะมีกระบวนการในการจับที่ต่างกัน Libpcap API ถูกออกแบบมาจากภาษา C และ C++ ยังไงก็ตามมันก็ยังนำไปใช้กับภาษาต่างๆได้เช่น Perl, PHP, JAVA, C#, Ruby Libpcap ทำงานในระบบปฏิบัติการที่คล้าย Unix(Linux, Solaris, HPUX, BSD) ถ้าทำงานในระบบปฏิบัติการ Windows จะใช้ชื่อว่า Winpcap ปัจจุบัน Libpcap ถูกจัดการโดย Tcpdump Group ข้อมูลและ Source Code สามารถหาอ่านได้ TCPDUMP/LIBPCAP public repository และ WinPcap - Home สำหรับ windows ติดตั้ง libpcap บน ubuntu สำหรับเขียนโปรแกรมใช้คำสั่ง sudo apt-get install libpcap-dev ติดตั้งเสร็จแล้วให้เข้าไปเช็คที่ /usr/include/ ดูว่ามีไฟล์ชื่อ pcap.h ถ้ามีแสดงว่าติดตั้งสมบูรณ์ วิธีการคอมไพล์ไฟล์ให้ใช้คำสั่ง gcc -o ชื่อไฟล์ output ชื่อไฟล์ sourcecode –l pcap

ในปัจจุบันมีซอฟทแวรสำเร็จรูปมากมายที่พัฒนาด้วย Libpcap ที่รู้จักกันดี ไดแก Wireshartk, tcpdump, Snort, NMap, Ntop ฯลฯ

2.11 เจพีกราฟ (Jpgraph)

JpGraph คือ library ตัวหนึ่ง ที่ถูกเขียนขึ้นเพื่อทำให้สร้างกราฟในเว็บเพจรูปแบบต่างๆ ได้ง่ายและรวดเร็วขึ้น โดยเขียนโค้ดไม่ยาวมากนักและวิธีการใช้งานไม่ยากจนเกินไป จึงทำให้ชื่อเสียงของ JpGraph โด่งดังมาก และมีคนใช้งานกันมากมายJpGraph มีเว็บไซต์อย่างเป็นทางการอยู่ที่ http://www.aditus.nu/jpgraph/ เขียนขึ้นโดย Johan Persson โดยเริ่มเวอชัน 1.0 เมื่อ 16 เดือนกันยายน 2002 ซึ่งภายในเว็บไซต์จะมีตัวอย่างและเอกสารบทเรียนให้ดาวน์โหลดมากมาย โดยเขียนโดยที่ JpGraph ถูกเขียนขึ้น ตามแนวทางการเขียนโปรแกรมแบบ Object-Oriented-ProGramming สามารถรันด้วย php ในโหมดต่างๆ ไม่ว่าจะเป็น CGI/APXS/CLI?

นอกจากนี้แล้วยังสามารถเอา JpGraph มาพัฒนาต่อได้ง่ายๆ เพราะโครงสร้างโปรแกรมที่เขียน มาแบบ OOP สำหรับ Font ของ JpGraph ก็สามารถใช้ TTF Font ได้ ซึ่งทำให้สามารถใช้งานภาษาไทยได้อย่างไม่มีปัญหา

ในตอนแรก JpGraph เป็น ฟรีซอฟต์แวร์แบบ Donation Ware คือสามารถใช้ได้โดยไม่ต้องเสียเงินแต่สามารถบริจาคเงินให้ทีหลังได้เพื่อเป็นกองทุนในการพัฒนาซอฟต์แวร์ในปัจจุบัน JpGraph ได้แบ่งสายการพัฒนาออกเป็น สอง เวอร์ชันตามเวอร์ชันของ PHP คือ

1) เวอร์ชัน 1.X ใช้งานกับ PHP4 โดยล่าสุดจะเป็นเวอร์ชัน 1.20.5
2) เวอร์ชัน 2.X ใช้งานกับ PHP5 โดยล่าสุดจะเป็นเวอร์ชัน 2.1.4

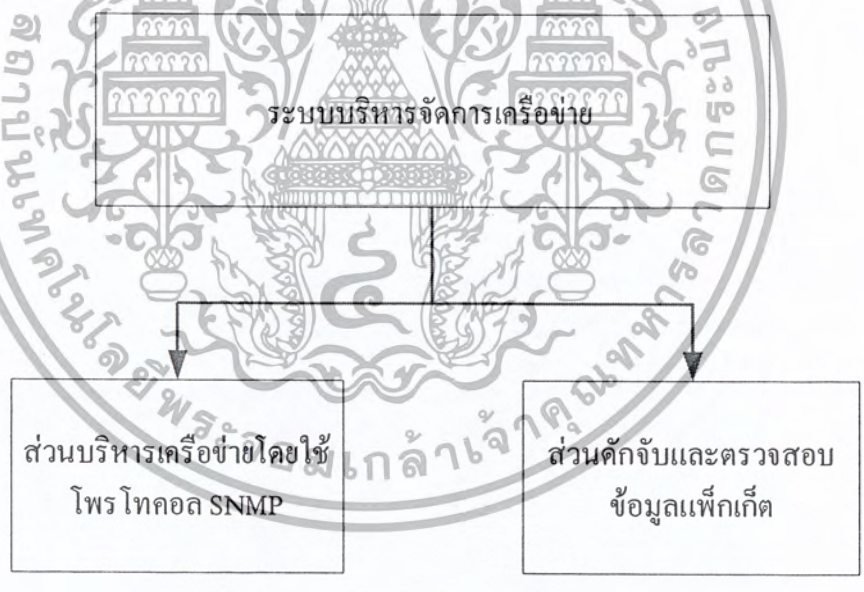
เหตุที่ต้องแบ่งออกเป็น สอง เวอร์ชันเพราะว่า PHP ได้ปรับเปลี่ยนและพัฒนาฟีเจอร์ในการเขียนโปรแกรมเชิงออบเจ็กต์ใน PHP5 ใหม่ และเป็นผลให้ JpGraph 1.X ซึ่งเขียนโปรแกรมด้วยวิธีนี้จะทำงานร่วมกับ PHP5 ไม่ได้ ดังนั้น JpGraph จึงออก เวอร์ชัน 2.X มาเพื่อให้ใช้ได้กับ PHP

บทที่ 3

การออกแบบและการจัดทำปริญญานิพนธ์

3.1 การออกแบบ

ระบบบริหารการจัดการเครือข่ายโดยใช้วิธีการตรวจจับแพ็กเก็ตแบ่งออกเป็น 2 ส่วน ประกอบไปด้วย 1. ส่วนบริหารเครือข่ายโดยใช้โพรโทคอล SNMP 2. ส่วนเก็บข้อมูลแพ็คเก็ต แสดงผลดังรูปที่ 3.1



รูปที่ 3.1 องค์ประกอบของระบบเครือข่ายโดยใช้วิธีการตรวจจับแพ็คเก็ต

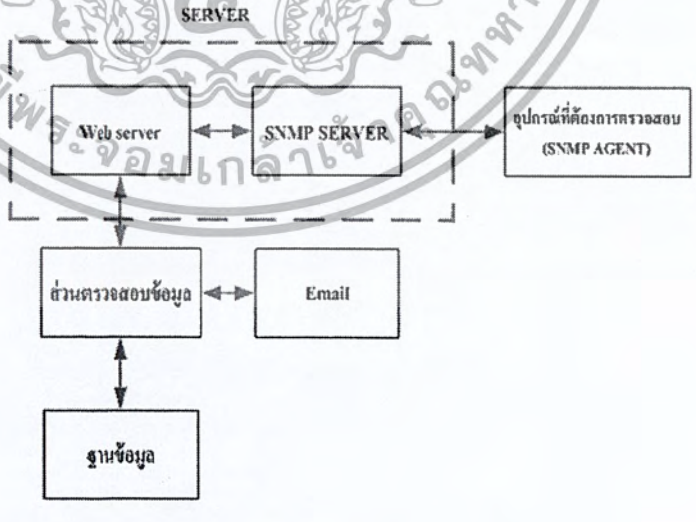
ส่วนบริหารเครือข่ายโดยใช้โพรโทคอล SNMP มีหน้าที่ในการดึงข้อมูลสิ่งที่ผู้ดูแลระบบสนใจจากอุปกรณ์นั้นๆ มาเก็บไว้ในฐานข้อมูลโดยอาศัยโพรโทคอล SNMP จะมีส่วนย่อยๆแบ่งลงไปดังนี้คือ ส่วนรับข้อมูลซึ่งทำหน้าที่ส่งคำร้องขอข้อมูลจากโพรโทคอล SNMP หลังจากนั้นทำ

การรับและจัดเก็บข้อมูลที่ได้ลงไปในฐานข้อมูล และมีส่วนที่ทำการตรวจสอบว่าข้อมูลที่ทำการจัดเก็บมีความผิดปกติหรือไม่ หากมีจะทำการแจ้งเตือน และอีกส่วนคือ ส่วนแสดงผลจะเป็นการแสดงผลข้อมูลจากฐานข้อมูล

ส่วนดักจับและตรวจสอบข้อมูลแพ็กเก็ตทำหน้าที่เก็บข้อมูลของแพ็กเก็ตที่วิ่งอยู่บนเครือข่ายมาจัดเก็บลงในฐานข้อมูลและแสดงผลข้อมูลจากฐานข้อมูล

3.1.1 ส่วนบริหารเครือข่ายโดยใช้โพรโทคอล SNMP

ในส่วนบริหารเครือข่าย โดยใช้โพรโทคอล SNMP โปรแกรมจะทำงานที่ server อยู่ตลอดเวลาเพื่อเข้าไปตรวจสอบการทำงานของอุปกรณ์ทุกๆ 60 วินาที โดยเริ่มจากเข้าไปดึงข้อมูลจากฐานข้อมูลจากแต่ละอุปกรณ์ที่ต้องการตรวจสอบข้อมูล หลังจากนั้นจะติดต่อไปยัง SNMP SERVER เพื่อส่งคำร้องขอไปยังอุปกรณ์ที่ต้องการตรวจสอบ หลังจากนั้นอุปกรณ์จะตอบกลับมาและนำค่าที่อุปกรณ์ตอบกลับมาเข้าไปเก็บยังฐานข้อมูลและนำข้อมูลเดียวกันเข้าไปยังส่วนตรวจสอบข้อมูล หากมีความผิดปกติจะทำการแจ้งเตือนความผิดปกตินี้ไปยังผู้ดูแลระบบด้วยการส่ง Email ดังรูปที่ 3.2



รูปที่ 3.2 บล็อกไดอะแกรมส่วนรับข้อมูล

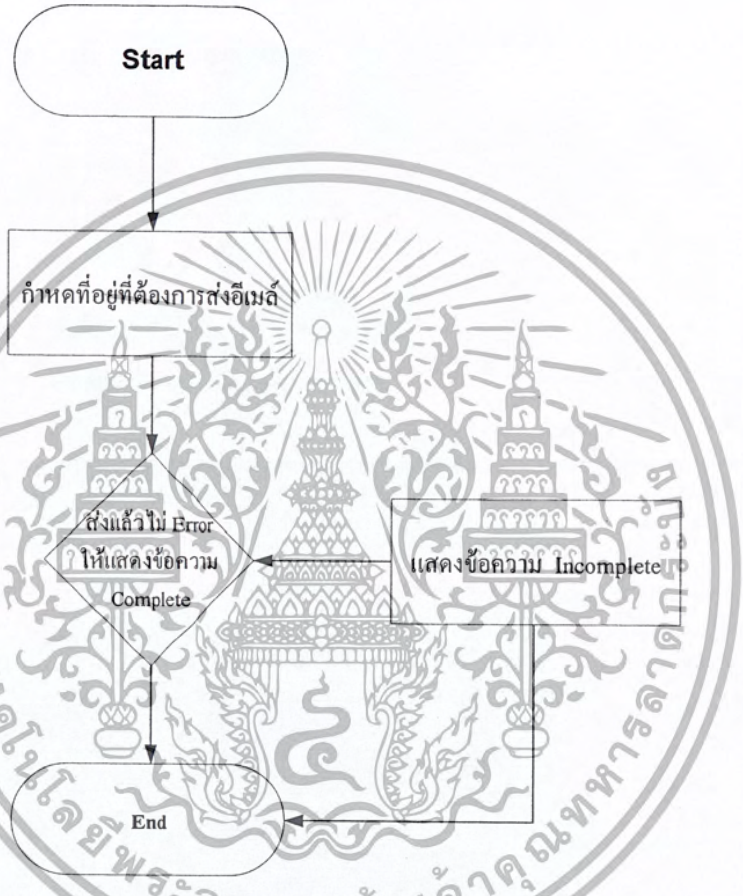
3.1.1.1 การรับข้อมูล SNMP

ในส่วนการรับข้อมูลโปรแกรมจะทำการรับข้อมูลตลอดเวลา โดยจากแผนผังการทำงานเริ่มจากเข้าไปดึงข้อมูล OID จากแต่ละอุปกรณ์ที่สนใจและทำการส่งคำร้องขอไปยังอุปกรณ์โดยผ่านทาง SNMP SERVER และเมื่ออุปกรณ์ตอบกลับจะนำผลการตอบกลับเก็บลงในฐานข้อมูล แล้วทำการดึงข้อมูลมาเก็บทุกๆ 60 วินาที ดังรูปที่ 3.3

รูปที่ 3.3 แผนผังการรับข้อมูล SNMP

3.1.1.2 การออกแบบการแจ้งเตือนโดยการส่งอีเมล์

โดยเมื่อเกิดความผิดปกติจากค่าที่ตั้งไว้จะทำการส่งอีเมล์ไปยังอีเมล์ที่ตั้งไว้ ดังรูปที่ 3.4



รูปที่ 3.4 แผนผังการส่งอีเมล์

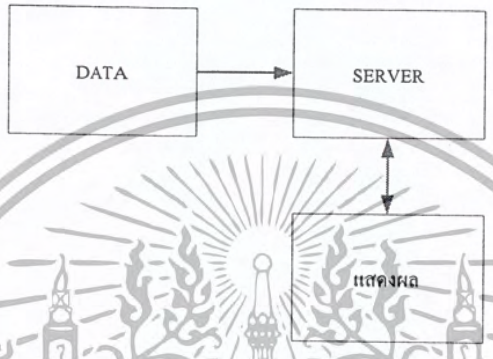
3.1.2 ส่วนแสดงผล

โดยส่วนนี้ได้มีการแสดงผลเป็นเว็บเพจให้นำข้อมูลที่เก็บไว้ในฐานข้อมูลมาแสดงผลโดยให้ทำการเลือกค่าของอุปกรณ์ที่สนใจ โปรแกรมจะไปทำการดึงข้อมูลมาทำการแสดงผลเป็นกราฟในระยะเวลา 24 ชั่วโมง ดังรูปที่ 3.5

รูปที่ 3.5 แผนผังการแสดงผล

3.1.3 ส่วนดักจับและตรวจสอบข้อมูลแพ็กเก็ต

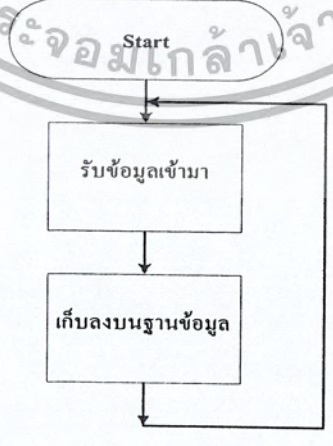
ในส่วนนี้จะมีการทำงานโดยข้อมูลส่งเข้ามาที่ SERVER และนำข้อมูลที่ได้มาเก็บไว้ในฐานข้อมูลและสามารถแสดงผลข้อมูลจากฐานข้อมูลได้ ดังรูปที่ 3.6



รูปที่ 3.6 บล็อกไดอะแกรมส่วนดักจับและตรวจสอบข้อมูลแพ็กเก็ต

3.2.1 แผนผังการทำงานของส่วนดักจับและตรวจสอบข้อมูลแพ็กเก็ต

โดยส่วนนี้ได้มีการรับข้อมูลแพ็กเก็ตแล้วนำข้อมูลแพ็กเก็ตที่ได้มาเก็บไว้ลงบนฐานข้อมูลและจะทำการรับค่าข้อมูลตลอดเวลา ดังรูปที่ 3.7



รูปที่ 3.7 แผนผังการดักจับและตรวจสอบข้อมูลแพ็กเก็ต

3.2 เครื่องมือที่ใช้ในการทดลอง

1) PHP คือ ภาษาที่ใช้ในการเขียนโปรแกรมเพื่อติดต่อระหว่างจัดการข้อมูลกับส่วนต่างๆ
2) SNMP สำหรับ PHP เป็นโมดูลของภาษา PHP ทำให้ PHP สามารถเขียนโปรแกร ติดต่อกับโพรโทคอล SNMP
3) MySQL Server เป็นโปรแกรมที่ใช้เก็บข้อมูลลงในฐานข้อมูลและสามารถจัดการฐานข้อมูลนั้นๆได้
4) Ubuntu Server เป็นระบบปฏิบัติการที่ติดตั้งลงในส่วนจัดการข้อมูลที่เครื่อง Server
5) Apache Webserver โปรแกรมที่ทำให้เครื่อง Server สามารถติดต่อกับเครื่องลูกข่ายและฐานข้อมูลผ่านเว็บเพจได้
6) Libpcab เป็น library ของภาษา C ที่ใช้ในการรับ packet ต่างๆเข้ามา
7) ภาษา C ใช้ในการเขียนโปรแกรมติดต่อกับ Libpcap เพื่อรับข้อมูลมาเก็บลงในฐานข้อมูล

บทที่ 4

ผลการทดลอง

ถ้าต้องการให้เครื่องลูกข่ายใดสามารถรับและส่งผ่านข้อมูลผ่านโพรโทคอล SNMP ได้ ต้องทำให้เครื่องนั้นๆเป็น Agent เสียก่อนโดยทำการติดตั้งโปรแกรม SNMP Agent และทำการตั้งค่า Community string ให้ตรงกันระหว่าง เครื่องที่ใช้ในการจัดการเครือข่าย กับ เครื่องลูกข่าย

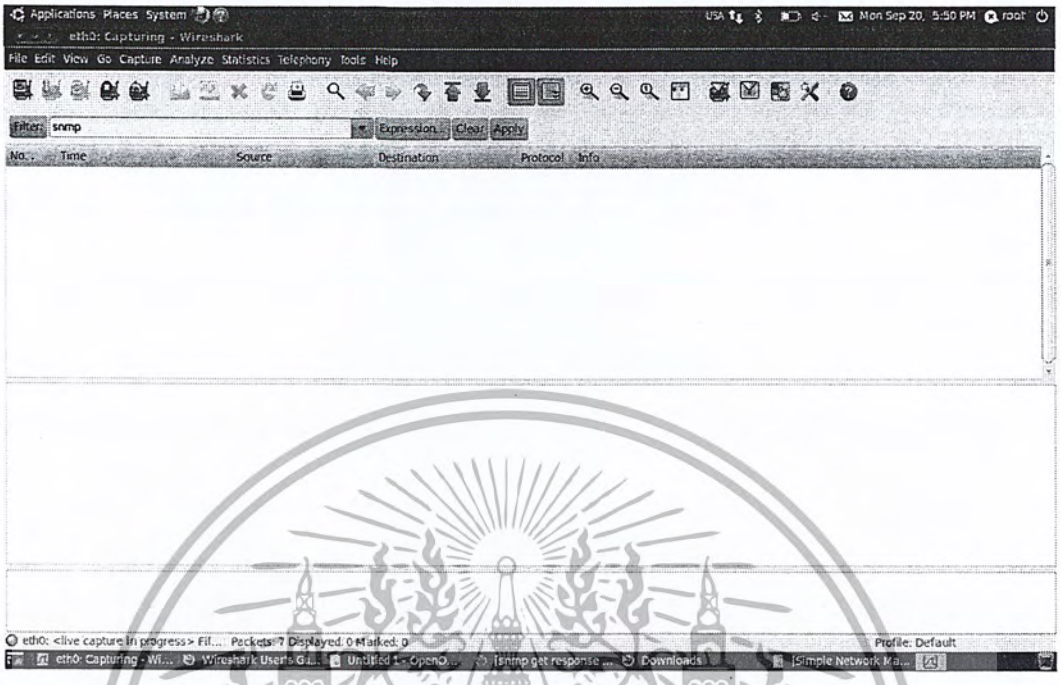
4.1 ผลการทดสอบการส่งคำร้องขอไปยัง SNMP AGENT

การส่งคำร้องของไปยัง SNMP AGENT และรับผลตอบกลับมาแสดงผลลักษณะข้อมูลเป็นแบบค่าเดียว

1.ทำการเชื่อมต่ออุปกรณ์ดังรูปที่ 4.1 โดยเครื่องคอมพิวเตอร์ทำการเชื่อมต่อผ่านสายแลนกับเราท์เตอร์โดยคอมพิวเตอร์มีไอพี 192.168.1.107 และ เราท์เตอร์มีไอพี 192.168.1.1

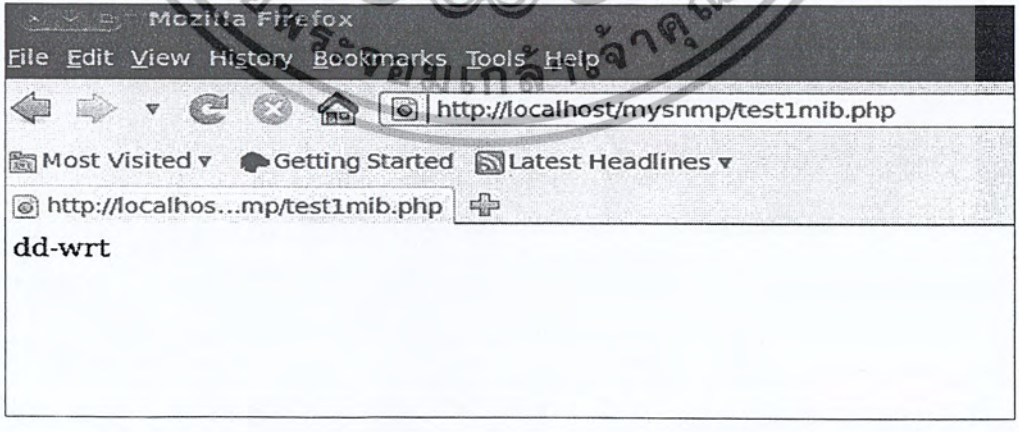
รูปที่ 4.1 ลักษณะการเชื่อมต่ออุปกรณ์

2. เปิดโปรแกรม WireShark เพื่อทำการจับข้อมูลที่วิ่งอยู่บนเครือข่าย โดยทำการจับค่าที่พอร์ต Ethernet ผลเป็นดังรูปที่ 4.2



รูปที่ 4.2 เริ่มต้นการดักจับข้อมูลที่โพรโทคอล SNMP ด้วย Wireshark แบบค่าเดียว

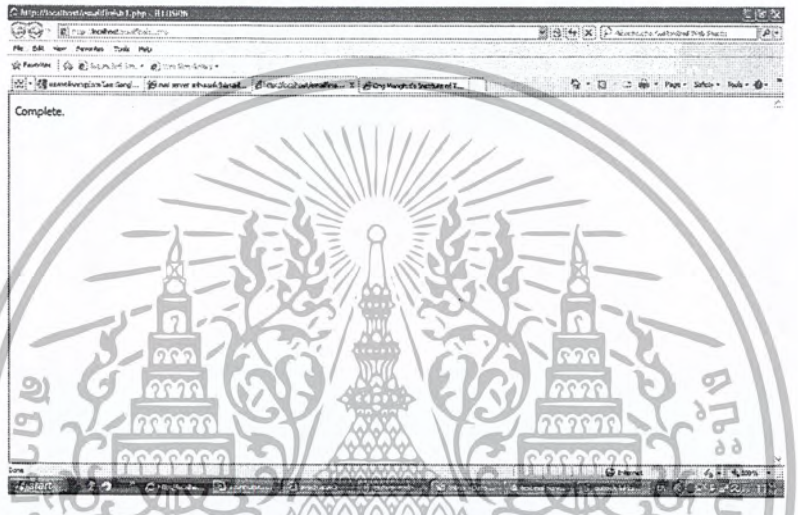
3. ทำการเปิด Browser แล้ว กรอกที่อยู่ของไฟล์ลงไป โปรแกรมจะทำการเข้าไปยังOID 1.3.6.1.2.1.1.5.0 ที่ชื่อว่า sysName (sysName คือชื่อของอุปกรณ์ที่ผู้ดูแลระบบเป็นคนตั้งไว้) กลับมาแล้วแสดงผลตอบกลับมาเป็นดังรูปที่ 4.3



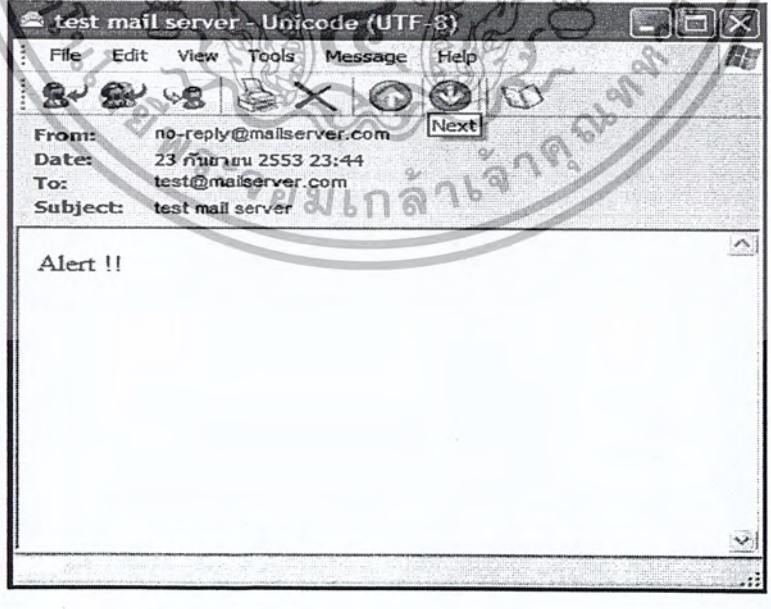
รูปที่ 4.3 ผลตอบกลับที่จากการติดต่อไปยัง OID ที่ชื่อว่า sysName

4.2 ผลการทดสอบการส่งอีเมล์

ทำการส่งอีเมล์ โดยส่วนนี้จะทำการส่งข้อความสั้นๆไปยังอีเมล์เพื่อทำการแจ้งเตือน ได้ผลการทดลองดังรูปที่ 4.4 จะแสดงข้อความขึ้นอีเมล์ถูกส่งออกไปได้และจะดูรายละเอียดของข้อมูลที่ส่งมาได้จากโปรแกรม Outlook Express ดังรูปที่ 4.5



รูปที่ 4.4 ทำการส่งอีเมล์ออกไปได้

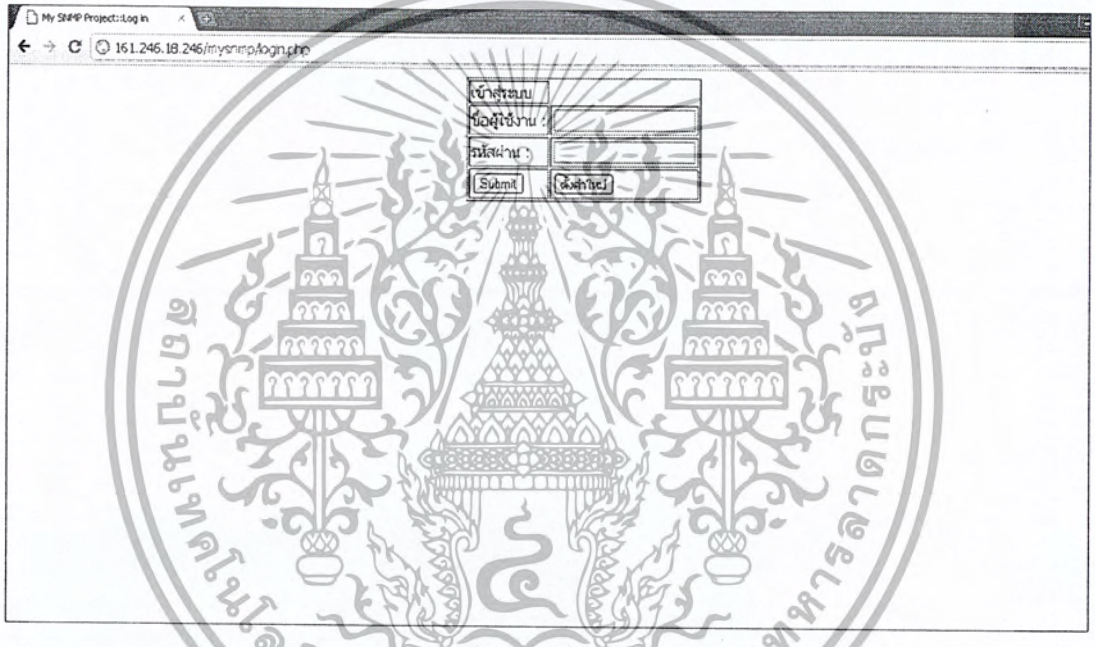


รูปที่ 4.5 อ่านอีเมล์โดยโปรแกรม Outlook Express

4.3 ผลการทดสอบการทำงานของเว็บไซต์

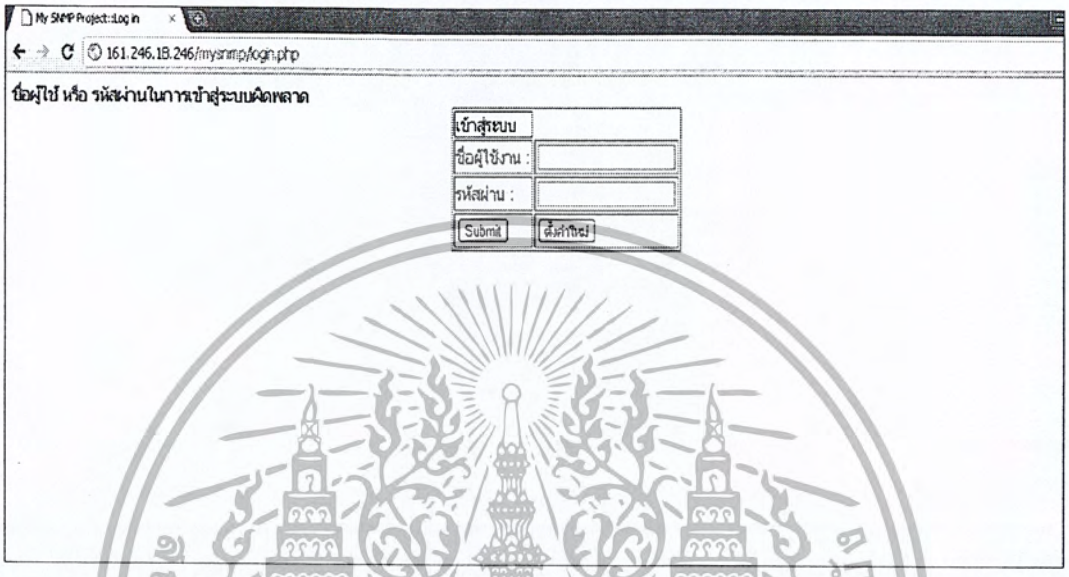
แสดงการทำงานของหน้าเว็บไซต์ที่ได้จัดทำขึ้นเพื่อช่วยอำนวยความสะดวกในการจัดการข้อมูลของผู้ดูแลระบบ

1.เมื่อเปิดหน้า Browser แล้วใส่ http://161.246.18.246/mysnmp/login.php จะได้ผลดังรูปที่ 4.6 เป็นหน้าตาของหน้าพิสูจน์ตัวตนเพื่อให้ผู้ดูแลระบบและผู้ได้รับมอบหมายเข้าใช้งานได้เท่านั้น



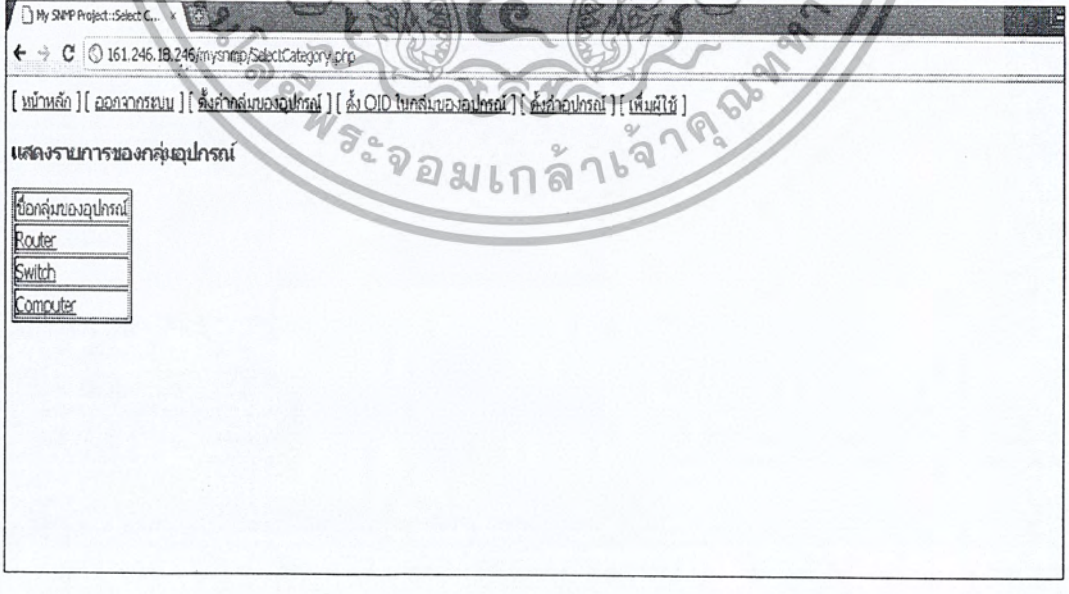
รูปที่ 4.6 หน้าพิสูจน์ตัวตนของเว็บเพจ

2. เมื่อทำการใส่ชื่อผู้ใช้งาน และรหัสผ่านผิดพลาด จะแสดงข้อความว่าชื่อผู้ใช้ หรือรหัสผ่านในการเข้าสู่ระบบผิดพลาด ดังรูปที่ 4.7



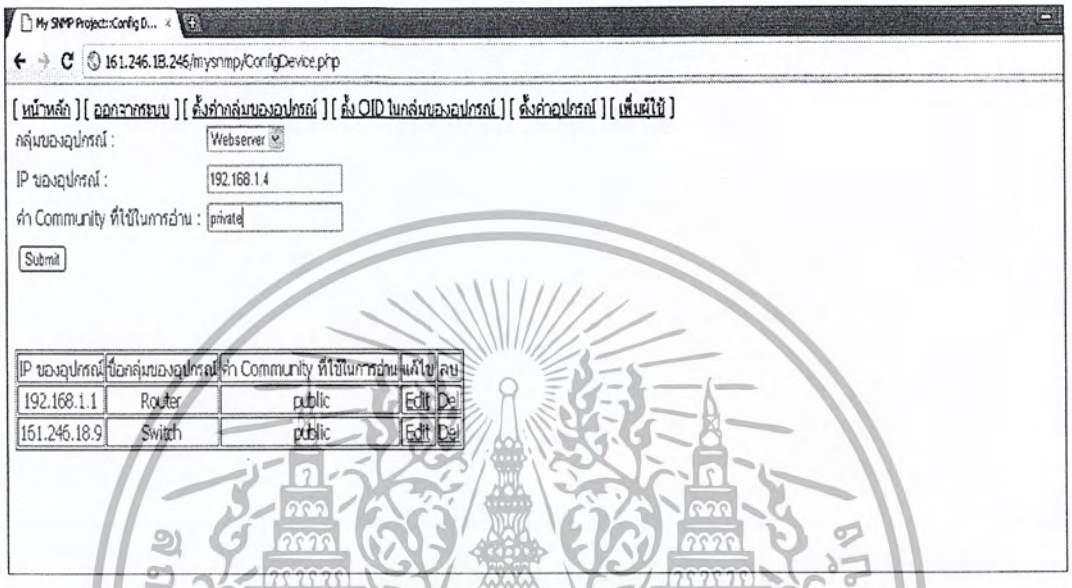
รูปที่ 4.7 หน้าล็อกอินของเว็บเพจผิดพลาด

3. เมื่อทำการใส่ ชื่อผู้ใช้งาน และรหัสผ่านถูกต้องจะ ได้หน้าเว็บเพจดังรูปที่ 4.8



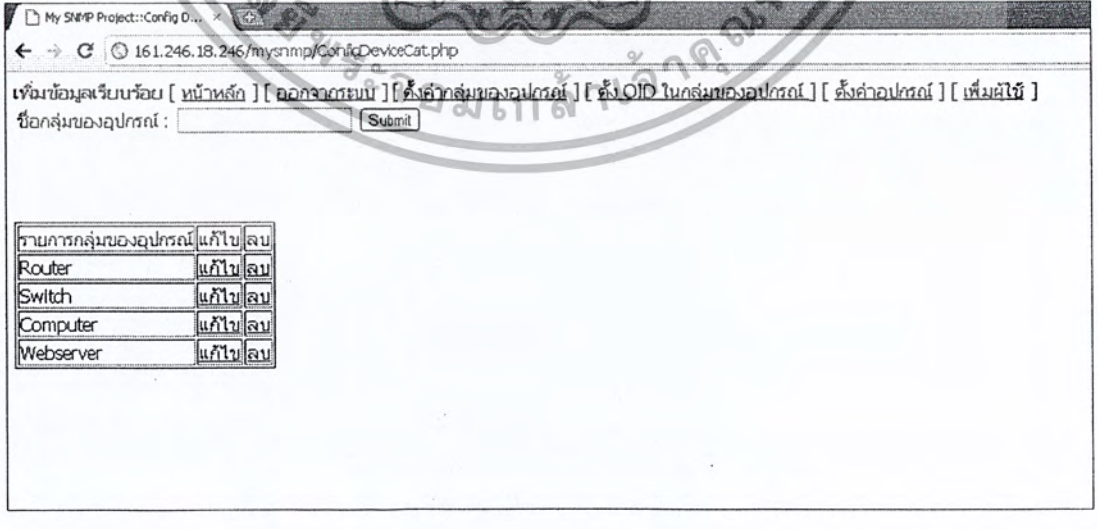
รูปที่ 4.8 ทำการ Login ถูกต้อง

4. เมื่อทำการกดเข้าไปที่ ตั้งค่ากลุ่มของอุปกรณ์ก็จะสามารถทำการเพิ่มอุปกรณ์ได้ดังรูปที่ 4.9



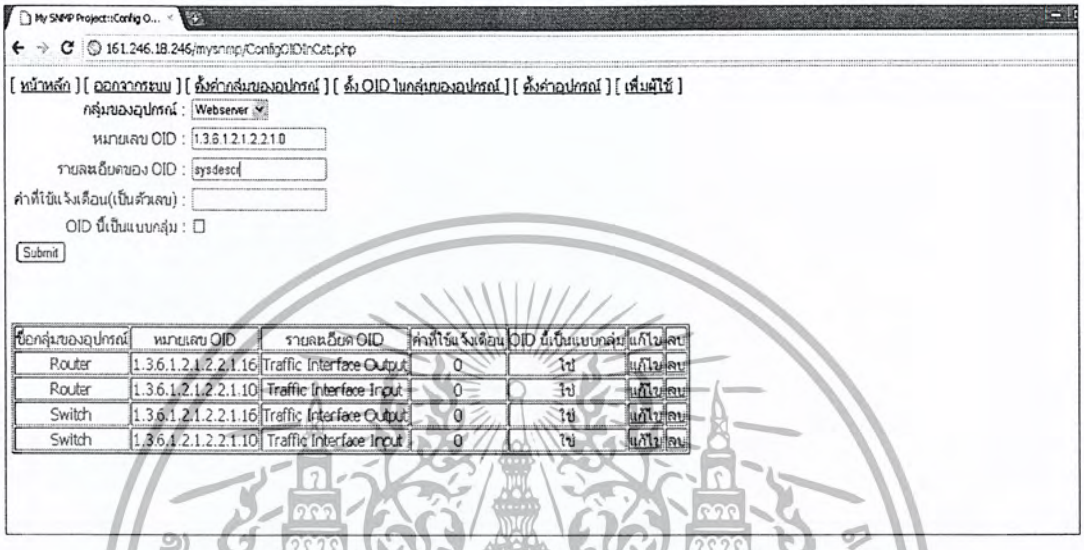
รูปที่ 4.9 ทำการเพิ่มอุปกรณ์

5. เมื่อทำการเพิ่มอุปกรณ์เรียบร้อยโดยในรูปทำการเพิ่ม อุปกรณ์ที่ชื่อ Webserver ดังรูปที่ 4.10 โดยหากเพิ่มสำเร็จจะแสดงข้อความว่า เพิ่มข้อมูลเรียบร้อย



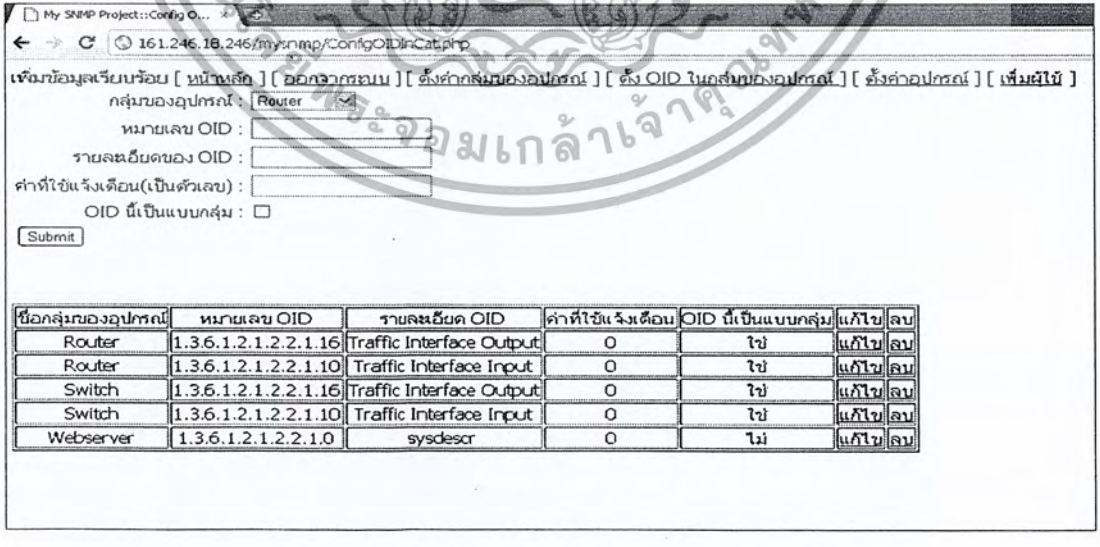
รูปที่ 4.10 ทำการเพิ่มอุปกรณ์สำเร็จ

6. เมื่อทำการกดเข้าไปที่ ตั้งค่ากลุ่มของอุปกรณ์เพื่อกำหนดค่า OID ของแต่ละกลุ่ม ก็จะแสดงหน้าเว็บเพจดังรูปที่ 4.11 และทำการใส่หมายเลขOID, รายละเอียดของOID, ที่ต้องการลงไป



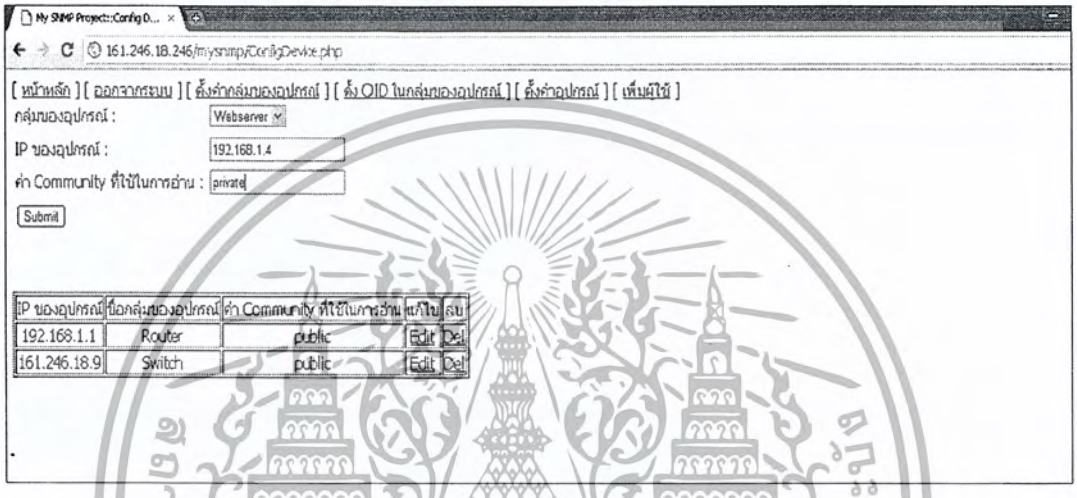
รูปที่ 4.11 ป้อนค่า OID ของแต่ละกลุ่มอุปกรณ์ที่ต้องการติดตามข้อมูล

7. กดปุ่ม Submit จะได้ผลดังรูปที่ 4.12 ถ้าข้อมูลถูกเพิ่มได้ จะแสดงข้อความว่า เพิ่มข้อมูลเรียบร้อย



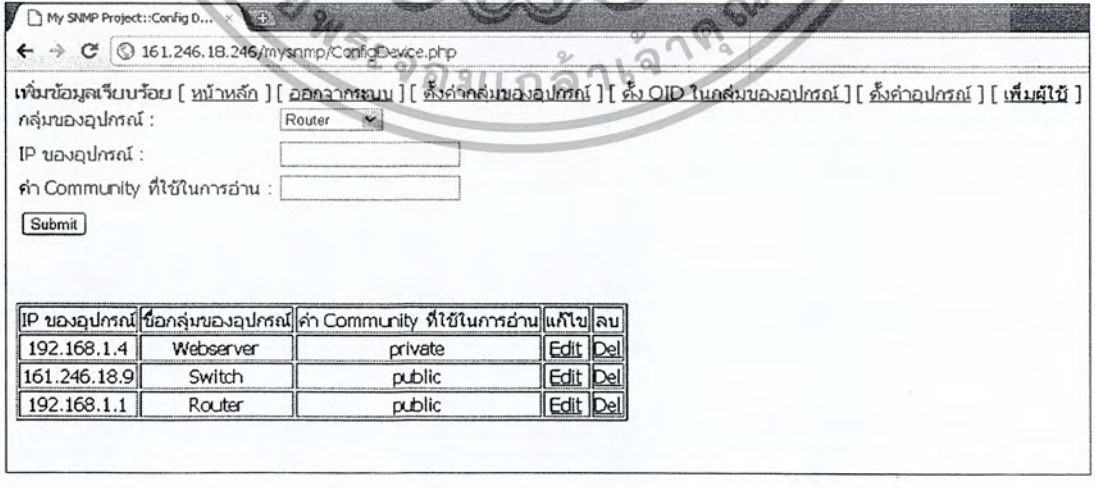
รูปที่ 4.12 เพิ่มค่า OID แต่ละกลุ่มที่ต้องการติดตามเรียบร้อย

8. เมื่อทำการกดที่ตั้งค่าอุปกรณ์เพื่อจัดการข้อมูลของอุปกรณ์ เช่น เพิ่ม เปลี่ยน ลบ อุปกรณ์ ก็จะแสดงหน้าต่างเว็บเพจจะแสดงหน้าจอของการกรอก IP ของอุปกรณ์ และค่า Community ที่ใช้ในการอ่านค่าของอุปกรณ์ ทำการใส่ค่า IP ของอุปกรณ์, ค่าCommunity ที่ใช้ในการอ่านที่ต้องการ ดังรูปที่ 4.13



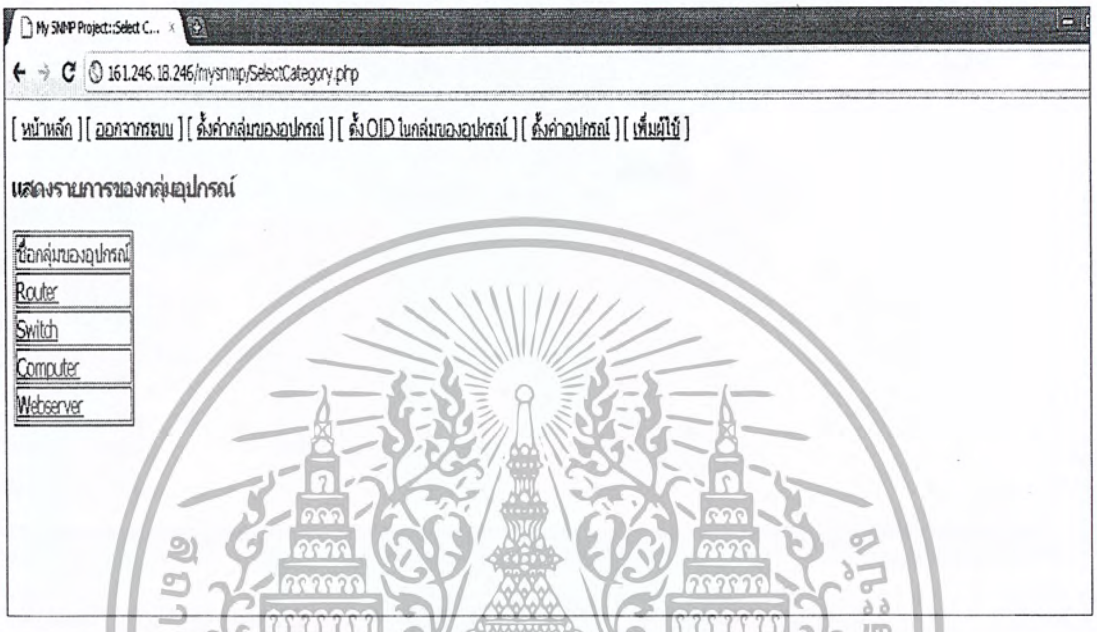
รูปที่ 4.13 เพิ่มอุปกรณ์ที่ต้องการติดตามข้อมูล

9. เมื่อเพิ่มอุปกรณ์สำเร็จจะแสดงผลดังรูปที่โดยมีข้อความ เพิ่มข้อมูลเรียบร้อยดังรูปที่ 4.14 เมื่อข้อมูลถูกเพิ่ม



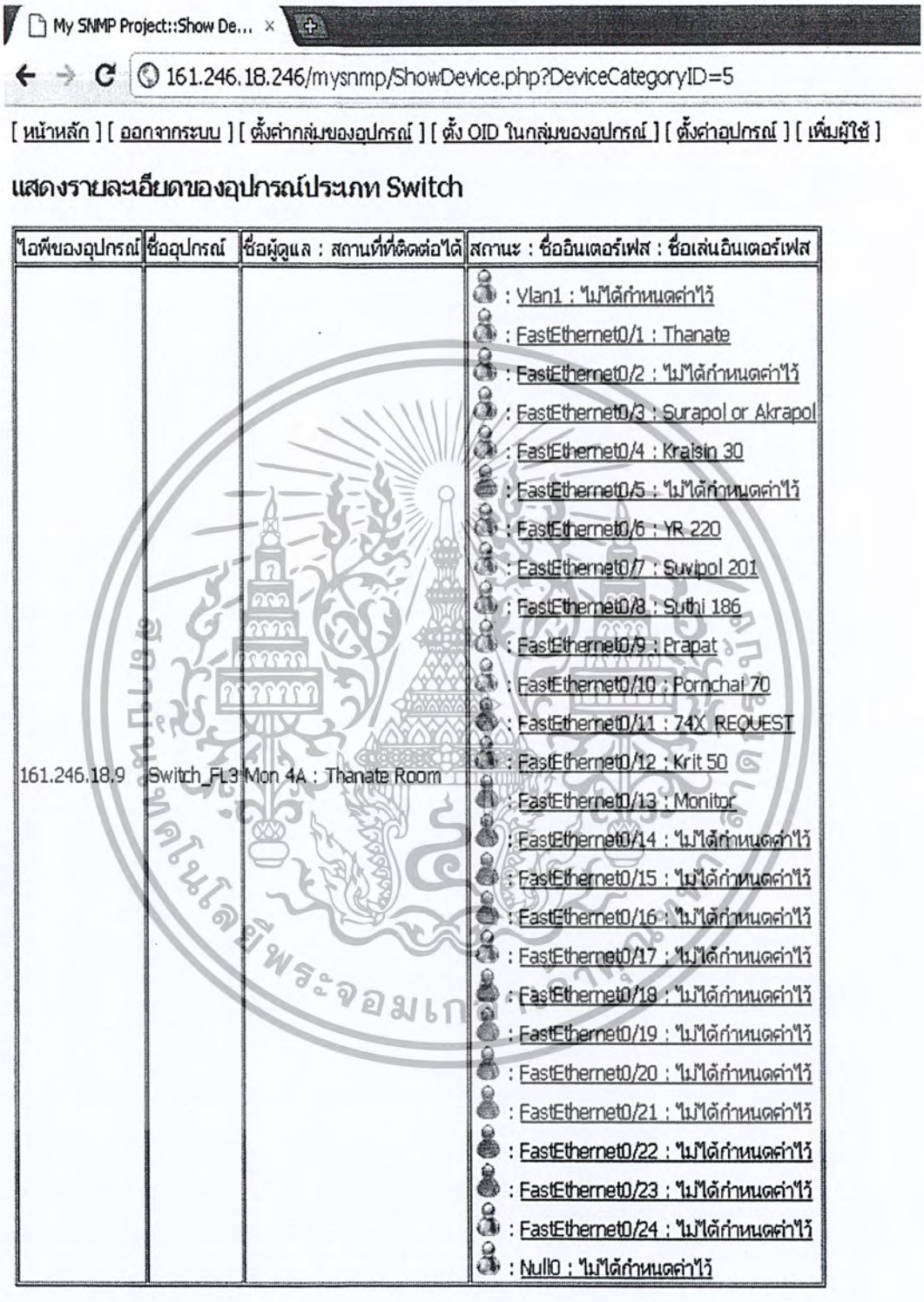
รูปที่ 4.14 เพิ่มอุปกรณ์ที่ต้องการติดตามข้อมูลเรียบร้อย

10. เมื่อทำการกดไปที่ หน้าแรก ก็จะแสดงหน้าเว็บเพจดังรูปโดยจะมีกลุ่มอุปกรณ์ต่างๆ ดังรูปที่ 4.15

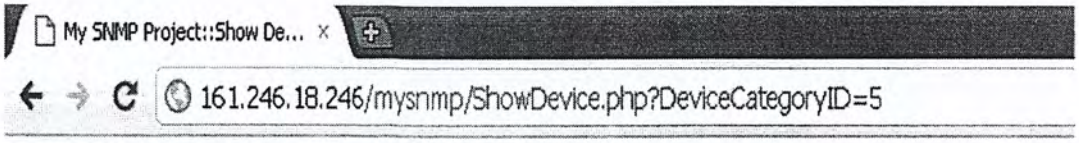


รูปที่ 4.15 หน้าจอหลักแสดงกลุ่มของอุปกรณ์

11. เลือกกดเข้าไปที่กลุ่มอุปกรณ์ที่เราต้องการดู (ในที่นี้เลือก Switch) ก็จะแสดงรายละเอียดของอุปกรณ์ประเภท Switch ที่มีทั้งหมดและแสดงค่าไอพีของอุปกรณ์ ชื่ออุปกรณ์ ชื่อผู้ดูแล สถานที่ที่ติดต่อได้ สถานะ ชื่ออินเตอร์เฟส ชื่อเล่นอินเตอร์เฟส ภายในไอพีที่กำหนดทั้งหมด ดังรูปที่ 4.16 และแสดงสถานะปริมาณข้อมูลขาเข้าทั้งหมด ปริมาณข้อมูลขาออกทั้งหมด ณ เวลาในขณะนั้นดังรูปที่ 4.17 พร้อมทั้งแสดงผลออกมาเป็นกราฟ ดังรูปที่ 4.18



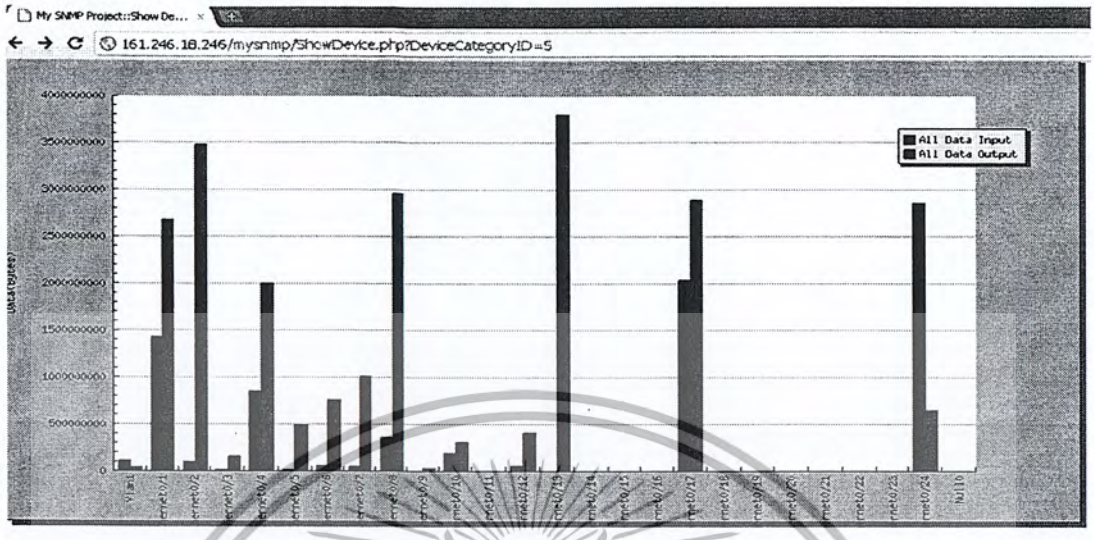
รูปที่ 4.16 รายละเอียดของอุปกรณ์ภายในกลุ่มอุปกรณ์ Switch



รายละเอียดของ Switch_FL3

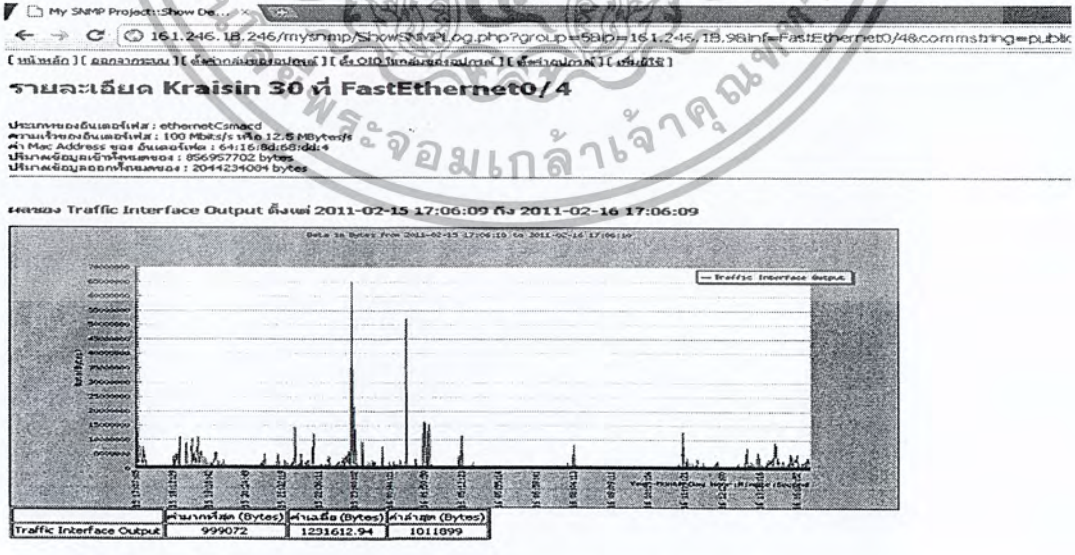
ชื่ออินเตอร์เฟส : ชื่อเล่นอินเตอร์เฟส	ปริมาณข้อมูลเข้าทั้งหมด(bytes)	ปริมาณข้อมูลออกทั้งหมด(bytes)
Vlan1 : ไม่ได้กำหนดค่าไว้	116559884	38075158
FastEthernet0/1 : Thanate	1527284530	4135593091
FastEthernet0/2 : ไม่ได้กำหนดค่าไว้	98069868	3483928967
FastEthernet0/3 : Surapol or Akrapol	6820881	170101775
FastEthernet0/4 : Kraisin 30	928116595	2822985510
FastEthernet0/5 : ไม่ได้กำหนดค่าไว้	14297750	489835535
FastEthernet0/6 : YR 220	66122533	847002991
FastEthernet0/7 : Suvipol 201	48467816	1013181043
FastEthernet0/8 : Suthi 186	384825822	3129084994
FastEthernet0/9 : Prapat	1012136	31232538
FastEthernet0/10 : Pornchai 70	224633493	337698507
FastEthernet0/11 : 74X_REQUEST	0	0
FastEthernet0/12 : Krit 50	60466108	439066871
FastEthernet0/13 : Monitor	0	1917083283
FastEthernet0/14 : ไม่ได้กำหนดค่าไว้	0	0
FastEthernet0/15 : ไม่ได้กำหนดค่าไว้	0	0
FastEthernet0/16 : ไม่ได้กำหนดค่าไว้	0	0
FastEthernet0/17 : ไม่ได้กำหนดค่าไว้	2097013414	3564567527
FastEthernet0/18 : ไม่ได้กำหนดค่าไว้	0	0
FastEthernet0/19 : ไม่ได้กำหนดค่าไว้	0	0
FastEthernet0/20 : ไม่ได้กำหนดค่าไว้	0	0
FastEthernet0/21 : ไม่ได้กำหนดค่าไว้	0	0
FastEthernet0/22 : ไม่ได้กำหนดค่าไว้	0	0
FastEthernet0/23 : ไม่ได้กำหนดค่าไว้	0	0
FastEthernet0/24 : ไม่ได้กำหนดค่าไว้	1733705775	899588103
Null0 : ไม่ได้กำหนดค่าไว้	0	0

รูปที่ 4.17 ปริมาณข้อมูลขาเข้าทั้งหมด ปริมาณข้อมูลขาออกทั้งหมด

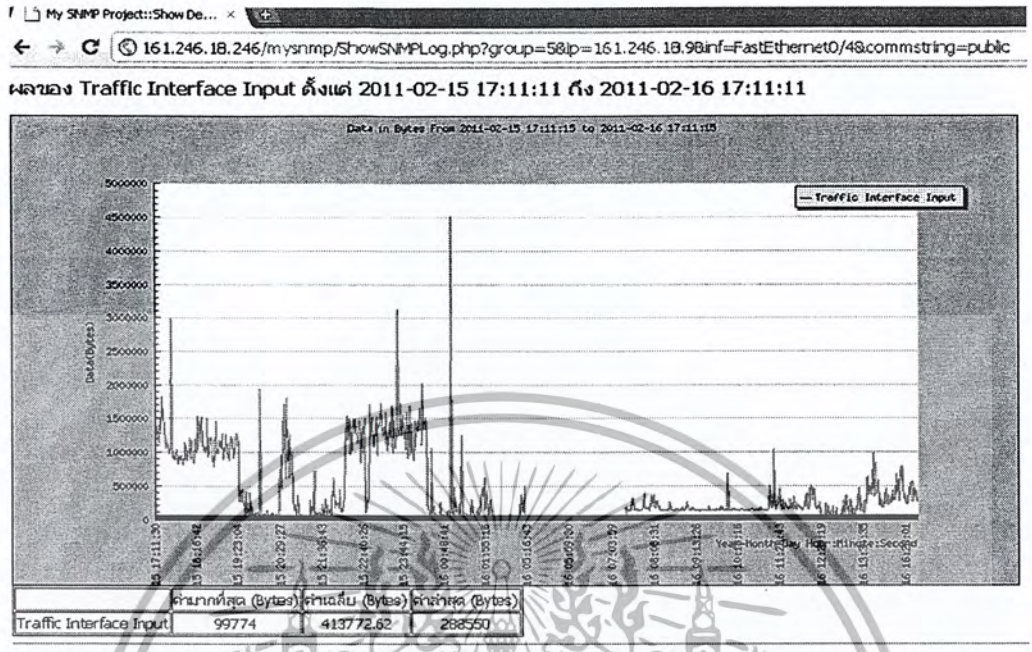


รูปที่ 4.18 ปริมาณข้อมูลขาเข้าทั้งหมด และปริมาณข้อมูลขาออก

12. เมื่อทำการเข้าไปดูในชื่ออินเตอร์เฟสที่เราสนใจก็จะแสดงหน้าต่างเว็บเพจซึ่งแสดงรายละเอียดของอินเตอร์เฟสที่สนใจ ซึ่งเป็นค่าปริมาณข้อมูลขาเข้าของอินเตอร์เฟส ดังรูปที่ 4.19 และปริมาณข้อมูลขาออกของอินเตอร์เฟสดังรูปที่ 4.20 รวมทั้งแสดงค่าข้อมูลปัจจุบันภายใน 24 ชั่วโมงออกมาในรูปกราฟ

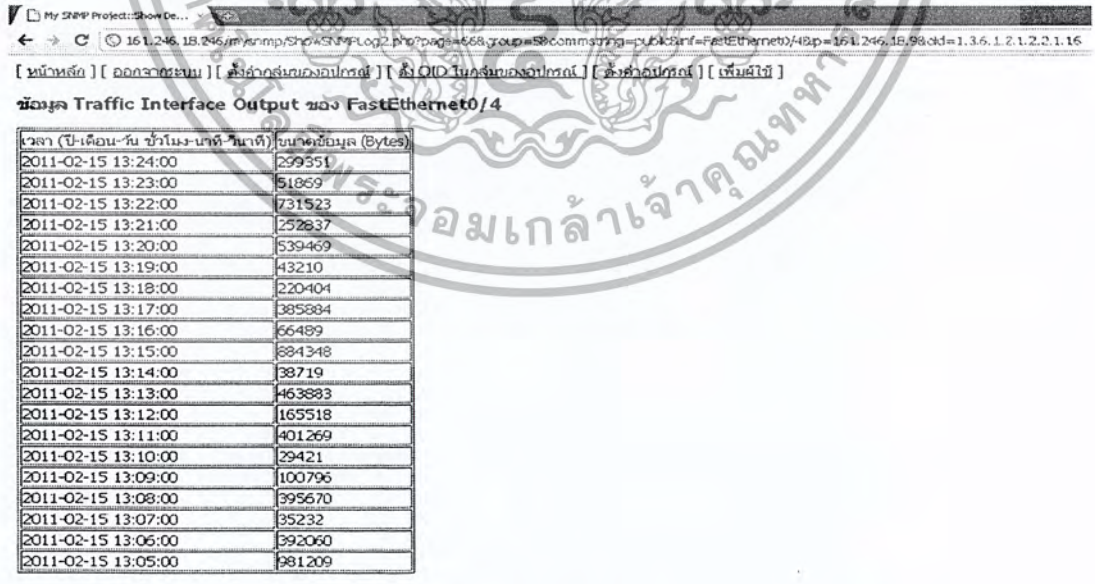


รูปที่ 4.19 ปริมาณข้อมูลขาเข้าของอินเตอร์เฟส



รูปที่ 4.20 ปริมาณข้อมูลขาออกของอินเตอร์เฟส

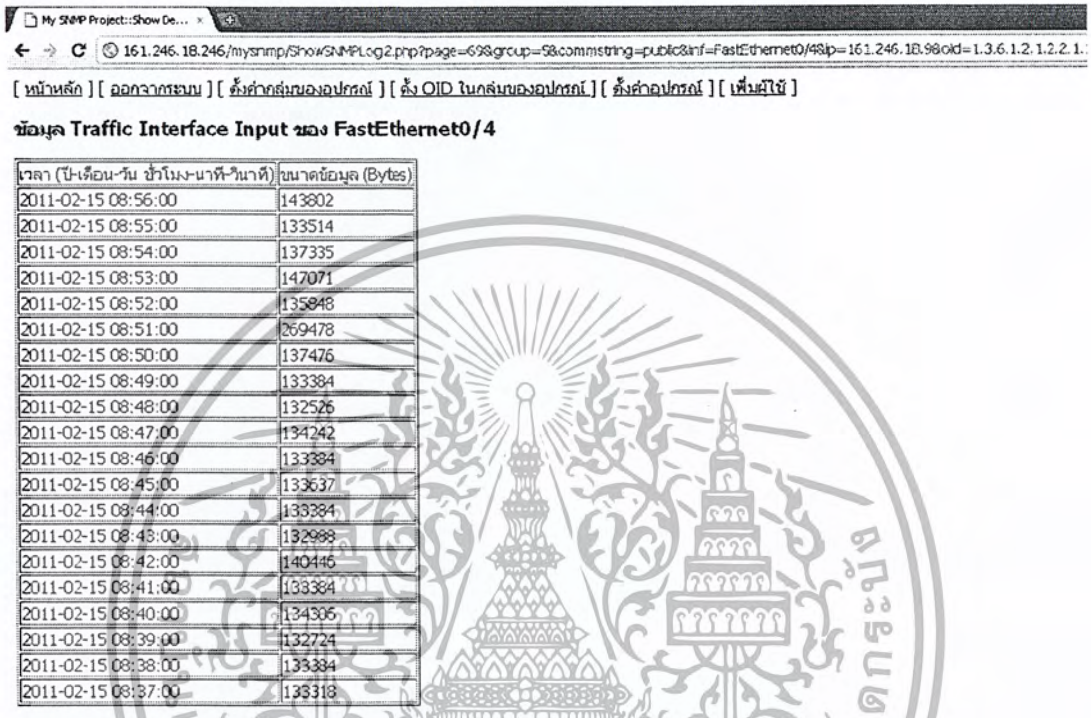
13. เมื่อทำการกดเข้าไปดูในกราฟ Trafffic Interface Output ก็จะแสดงปริมาณข้อมูลขาออกทั้งหมดที่ทำการเก็บข้อมูล ดังรูปที่ 4.21



เวลา (ปี-เดือน-วัน ชั่วโมง-นาที-วินาที)	ขนาดข้อมูล (Bytes)
2011-02-15 13:24:00	299351
2011-02-15 13:23:00	51869
2011-02-15 13:22:00	731523
2011-02-15 13:21:00	252837
2011-02-15 13:20:00	539469
2011-02-15 13:19:00	43210
2011-02-15 13:18:00	220404
2011-02-15 13:17:00	385884
2011-02-15 13:16:00	66489
2011-02-15 13:15:00	884348
2011-02-15 13:14:00	38719
2011-02-15 13:13:00	463883
2011-02-15 13:12:00	165518
2011-02-15 13:11:00	401269
2011-02-15 13:10:00	29421
2011-02-15 13:09:00	100796
2011-02-15 13:08:00	395670
2011-02-15 13:07:00	35232
2011-02-15 13:06:00	392060
2011-02-15 13:05:00	981209

รูปที่ 4.21 ปริมาณข้อมูลขาออกทั้งหมดที่ทำการเก็บข้อมูล

14. เมื่อทำการกดเข้าไปดูในกราฟ Traffic Interface Input ก็จะแสดงปริมาณข้อมูลขาออกทั้งหมดที่ทำการเก็บข้อมูล ดังรูปที่ 4.22


My SNMP Project::Show De...

161.246.18.246/mysnmp/Show/SNMPLog2.php?page=6%&group=5&commstring=public&inf=FastEthernet0/4&ip=161.246.18.98&oid=1.3.6.1.2.1.2.2.1.

[หน้าหลัก] [ออกจากระบบ] [ตั้งค่ากลุ่มของอุปกรณ์] [ตั้ง OID ในกลุ่มของอุปกรณ์] [ตั้งค่าอุปกรณ์] [เพิ่มผู้ใช้]

ข้อมูล Traffic Interface Input ของ FastEthernet0/4

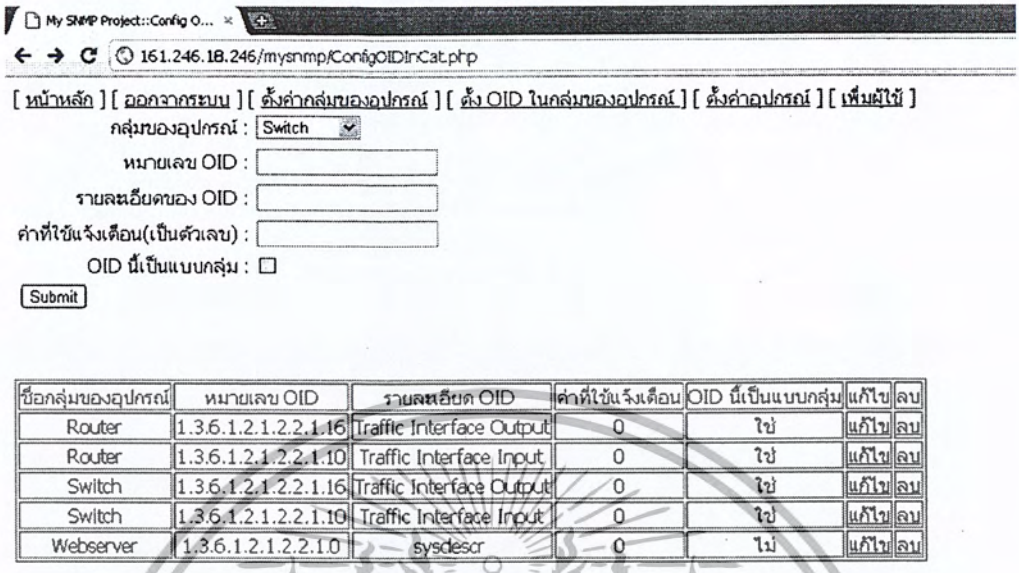
เวลา (ปี-เดือน-วัน ชั่วโมง-นาที-วินาที)	ขนาดข้อมูล (Bytes)
2011-02-15 08:56:00	143802
2011-02-15 08:55:00	133514
2011-02-15 08:54:00	137335
2011-02-15 08:53:00	147071
2011-02-15 08:52:00	135848
2011-02-15 08:51:00	269478
2011-02-15 08:50:00	137476
2011-02-15 08:49:00	133384
2011-02-15 08:48:00	132526
2011-02-15 08:47:00	134242
2011-02-15 08:46:00	133384
2011-02-15 08:45:00	133637
2011-02-15 08:44:00	133384
2011-02-15 08:43:00	132988
2011-02-15 08:42:00	140446
2011-02-15 08:41:00	133384
2011-02-15 08:40:00	134306
2011-02-15 08:39:00	132724
2011-02-15 08:38:00	133384
2011-02-15 08:37:00	133318

รูปที่ 4.22 ปริมาณข้อมูลขาออกทั้งหมดที่ทำการเก็บข้อมูล

4.4 ผลการทดสอบส่วนการแจ้งเตือน

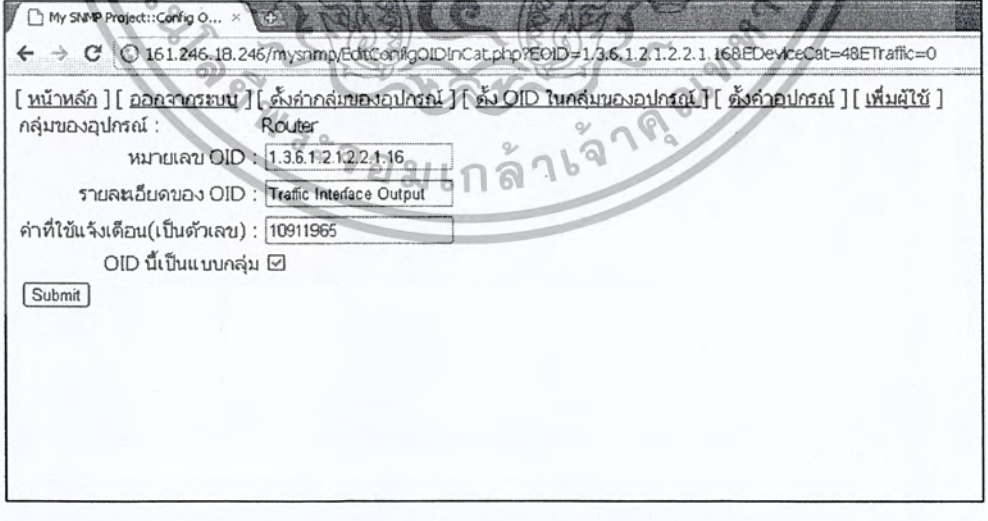
ในการแจ้งเตือนข้อมูลที่มีความผิดพลาดเกิดขึ้นจะทำการแจ้งเตือนผู้ดูแลระบบโดยผ่านทางอีเมล์ เมื่อผู้ดูแลทำการตรวจสอบอีเมล์ก็จะทราบถึงข้อผิดพลาดที่เกิดขึ้น

1. ในส่วนการแจ้งเตือนเมื่อทำการกดเข้าไปที่ ตั้งค่า OID ในกลุ่มของอุปกรณ์ และทำการแก้ไข ดังรูปที่ 4.23



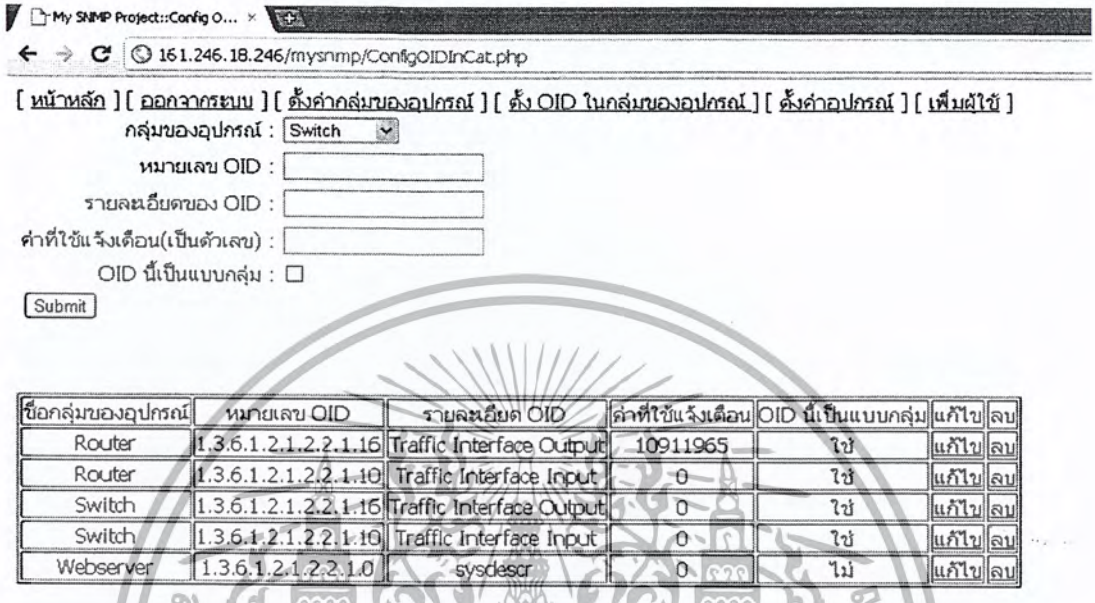
รูปที่ 4.23 หน้าจอการตั้งค่า OID ในกลุ่มของอุปกรณ์

2. ทำการแก้ไขโดยใส่ค่าที่ใช้แจ้งเตือน (เป็นตัวเลข) ใส่ค่าที่ต้องการลงไปในช่องดังรูปที่ 4.24 ในที่นี้ยกตัวอย่างการกำหนดค่าที่ใช้แจ้งเตือนเป็น 10911965



รูปที่ 4.24 การตั้งค่าการแจ้งเตือน

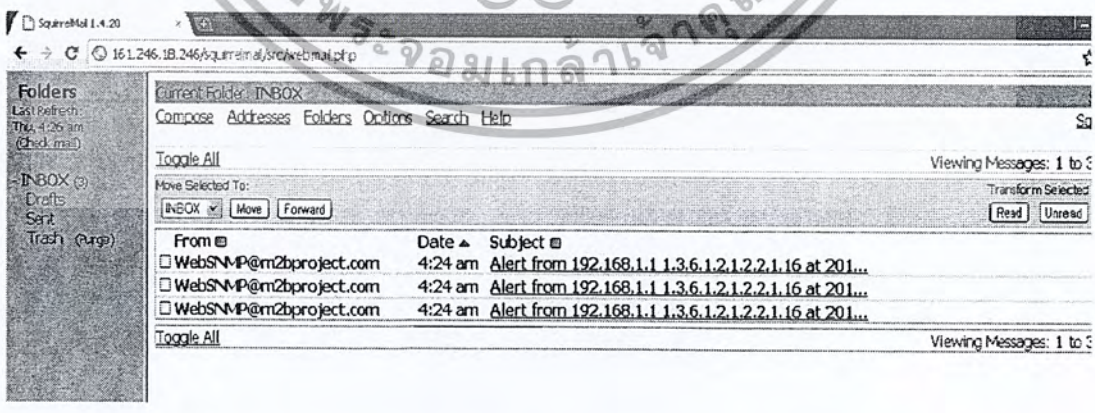
3. เมื่อกำหนดค่าที่ใช้แจ้งเตือนเรียบร้อยแล้วจะแสดงผลดังรูปที่ 4.25



ชื่อกลุ่มของอุปกรณ์	หมายเลข OID	รายละเอียด OID	ค่าที่ใช้แจ้งเตือน	OID นี้เป็นแบบกลุ่ม	แก้ไข	ลบ
Router	1.3.6.1.2.1.2.2.1.16	Traffic Interface Output	10911965	ใช่	แก้ไข	ลบ
Router	1.3.6.1.2.1.2.2.1.10	Traffic Interface Input	0	ใช่	แก้ไข	ลบ
Switch	1.3.6.1.2.1.2.2.1.16	Traffic Interface Output	0	ใช่	แก้ไข	ลบ
Switch	1.3.6.1.2.1.2.2.1.10	Traffic Interface Input	0	ใช่	แก้ไข	ลบ
Webserver	1.3.6.1.2.1.2.2.1.0	sysdescr	0	ไม่	แก้ไข	ลบ

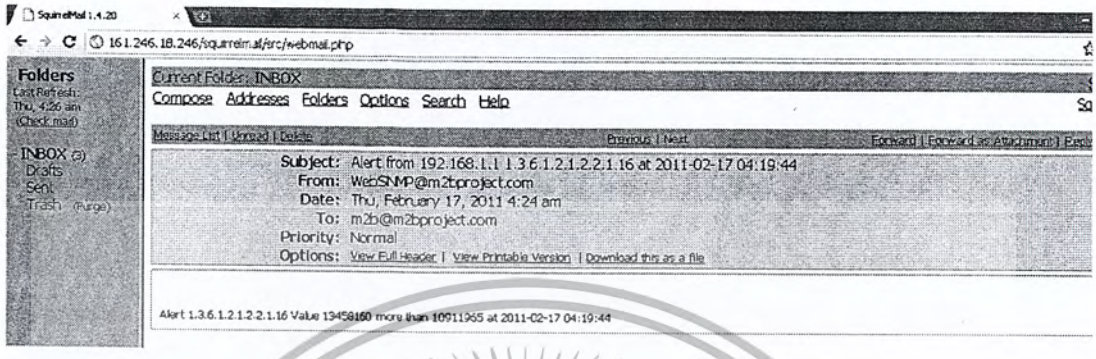
รูปที่ 4.25 กำหนดค่าที่ใช้แจ้งเตือนเรียบร้อย

4. เมื่อเปิดหน้า Browser แล้วใส่ http://161.246.18.246/squirrelmail.php ซึ่งเป็นหน้าเว็บเมล์ที่ใช้ในการอ่านและเขียนอีเมล์ จากนั้นทำการใส่ผู้ชื่อใช้งาน และรหัสผ่านจะได้ผลดังรูปที่ 4.26



รูปที่ 4.26 เข้าถึงอีเมล์ที่ใช้รับค่าการแจ้งเตือน

5. เมื่อกดเข้าไปเพื่ออ่านอีเมล์ จะพบเนื้อหาอีเมล์ที่มีข้อความแจ้งเตือน ดังรูปที่ 4.27

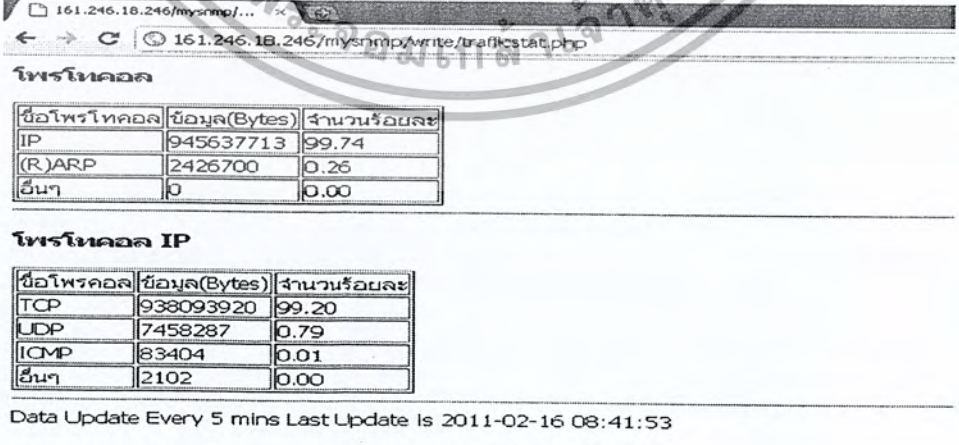


รูปที่ 4.27 เนื้อหาอีเมล์ที่ส่งมาจากระบบแจ้งเตือน

4.5 ผลการทดสอบส่วนดักจับและตรวจสอบข้อมูลแพ็กเก็ต

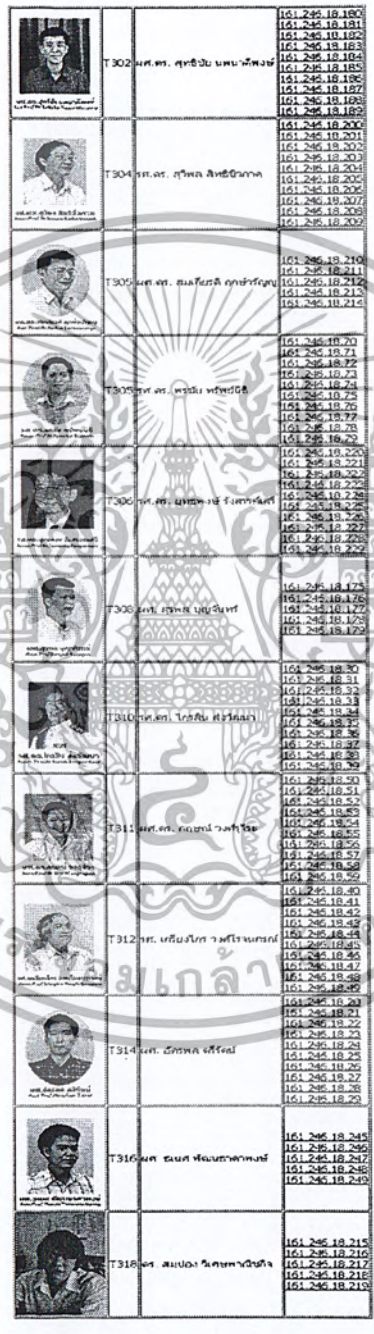
ในส่วนนี้ทำการทดสอบส่วนดักจับและตรวจสอบข้อมูลแพ็กเก็ตโปรแกรมจะทำการรับข้อมูลเข้ามาและนำข้อมูลมาแสดงผลบนเว็บเพจ

1. เมื่อทำการเข้าไปดูในไฟล์ชื่อ trafficstat.php ก็จะแสดงปริมาณข้อมูลการใช้งานโพรโทรคอลประเภท IP, ARP และอื่นๆ ดังรูปที่ 4.28



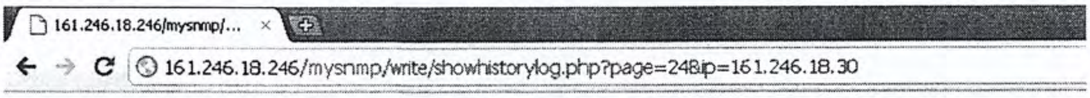
รูปที่ 4.28 ปริมาณข้อมูลการใช้โพรโทรคอล IP, ARP และ อื่นๆ

2. เมื่อทำการเข้าไปดูในไฟล์ชื่อ Showroom.php แสดงข้อมูลของ IP Address ภายในห้องแต่ละห้อง ดังรูปที่ 4.29



รูปที่ 4.29 ข้อมูลของ IP Address ภายในห้องแต่ละห้อง

3. เมื่อทำการกดเข้าไปดูใน IP Address ก็จะแสดงข้อมูลภายใน IP Address นั้นๆ ว่าใช้ไอพีต้นทาง ไอพีปลายทาง โพรโทคอล ทีซีพี ยูดีพี พอร์ตต้นทาง พอร์ตปลายทาง ดังรูปที่ 4.30



วันที่	เวลา	ไอพีต้นทาง	ไอพีปลายทาง	โพรโตคอล	ทีซีพี/ยูดีพี	พอร์ตต้นทาง	พอร์ตปลายทาง
2011-02-16	03:06:08	209.85.231.100	161.246.18.30	IP	TCP	2835	34379
2011-02-16	03:06:08	209.85.231.100	161.246.18.30	IP	TCP	2835	34379
2011-02-16	03:06:08	209.85.231.100	161.246.18.30	IP	TCP	2832	33921
2011-02-16	03:06:08	209.85.231.100	161.246.18.30	IP	TCP	2832	33921
2011-02-16	03:06:08	209.85.231.100	161.246.18.30	IP	TCP	2835	34379
2011-02-16	03:06:08	209.85.231.100	161.246.18.30	IP	TCP	2835	34379
2011-02-16	03:06:08	209.85.231.100	161.246.18.30	IP	TCP	2835	34379
2011-02-16	03:06:08	209.85.231.100	161.246.18.30	IP	TCP	2835	34379
2011-02-16	03:06:08	209.85.231.100	161.246.18.30	IP	TCP	2835	34379
2011-02-16	03:06:08	209.85.231.100	161.246.18.30	IP	TCP	2835	34379
2011-02-16	03:06:08	209.85.231.100	161.246.18.30	IP	TCP	2835	34379
2011-02-16	03:06:08	209.85.231.100	161.246.18.30	IP	TCP	2835	34379
2011-02-16	03:06:08	209.85.231.100	161.246.18.30	IP	TCP	2835	34379
2011-02-16	03:06:08	209.85.231.100	161.246.18.30	IP	TCP	2835	34379
2011-02-16	03:06:08	209.85.231.100	161.246.18.30	IP	TCP	2835	34379
2011-02-16	03:06:08	209.85.231.100	161.246.18.30	IP	TCP	2835	34379
2011-02-16	03:06:08	161.246.18.30	209.85.231.100	IP	TCP	80	46820
2011-02-16	03:06:08	161.246.18.30	209.85.231.100	IP	TCP	80	46820
2011-02-16	03:06:08	161.246.18.30	209.85.231.100	IP	TCP	80	46820
2011-02-16	03:06:08	161.246.18.30	209.85.231.100	IP	TCP	80	46820

รูปที่ 4.30 ข้อมูล ไอพีต้นทาง, ไอพีปลายทาง, โพรโทคอล, ทีซีพี, ยูดีพี

พอร์ตต้นทาง และพอร์ตปลายทาง

บทที่ 5

สรุปผลและข้อเสนอแนะ

5.1 สรุปผล

การพัฒนาโครงงานเรื่องระบบการบริหารระบบเครือข่ายโดยใช้วิธีการตรวจจับแพ็กเก็ต ได้มีการพัฒนาโดยนำทฤษฎีของการบริหารจัดการเครือข่าย(NMS) ซึ่งมีสองส่วนคือ 1.ส่วนบริหารเครือข่ายโดยใช้โพรโทคอล SNMP 2.ส่วนจัดเก็บข้อมูลแพ็กเก็ต

ส่วนบริหารเครือข่ายโดยใช้โพรโทรคอลนั้นอาศัยโพรโทคอลเอสเอ็นเอ็มพี (SNMP) โดยใช้ภาษาพีเอชพี (PHP) และฐานข้อมูล (MySQL) เข้ามาประยุกต์ใช้ร่วมกันเพื่อช่วยให้การพัฒนาระบบ ซึ่งความสามารถของส่วนนี้มีดังนี้ สามารถดูข้อมูลที่สนใจภายในอุปกรณ์ต่างๆได้ สามารถตั้งค่าเพื่อกำหนดไว้เมื่อค่าที่เกิดขึ้นมีค่ามากกว่าที่กำหนดก็จะทำการแจ้งเตือนไปยังอีเมล์ที่กำหนดไว้ สามารถแสดงผลข้อมูลภายใน 1 วันล่าสุดในรูปของกราฟได้ สามารถแสดงข้อมูลที่เก็บไว้ย้อนหลังได้ แบ่งผู้ใช้งานออกเป็น 2 กลุ่ม คือ ผู้ดูแลระบบและผู้ใช้งานระบบ โดยมีการทำงานดังนี้ ผู้ดูแลระบบมีสิทธิ์ในการดูข้อมูลต่างๆในระบบทั้งหมด และสามารถจัดการระบบได้ เช่น เพิ่ม แก้ไข ลบ อุปกรณ์ และจัดการกับ OID ต่างๆ ได้

ส่วนจัดเก็บข้อมูลแพ็คเกตนั้นเขียนขึ้นด้วยภาษา C ติดต่อกับ libpcap ซึ่งเป็น library ของภาษา C ที่ใช้ในการรับแพ็กเก็ต ซึ่งความสามารถของส่วนนี้มีดังนี้ สามารถรับข้อมูลประเภทแพ็กเก็ตมาได้ สามารถแสดงผลโพรโทคอลที่มีการใช้งานมากได้

โครงงานนี้ทำสำเร็จตามขอบเขตของงานที่ทางกลุ่มของข้าพเจ้าได้ตั้งไว้

5.2 ปัญหาและอุปสรรค

1) ในตอนเริ่มต้นมีความคิดที่จะใช้ภาษาไพธอนในการเขียนโปรแกรมติดต่อกับ SNMPแต่มีปัญหาเรื่องในการติดตั้งโมดูลที่ใช้กับ SNMP ทั้ง NET-SNMP และ PySNMP

2) ในส่วนการแจ้งเตือนทางอีเมล์ มีปัญหาตรงที่การจะส่งอีเมล์ออกไปได้นั้นต้องมีการติดตั้ง mail server ก่อนซึ่งมีขั้นตอนยุ่งยาก

3) ในการออกแบบฐานข้อมูลจำเป็นจะต้องมีความเชื่อมโยงกันในแต่ละตารางเพื่อให้สามารถใช้งานแต่ละตารางร่วมกันได้

4) การจัดเก็บข้อมูลที่มีขนาดใหญ่ มีผลทำให้ระบบทำงานช้าลง

5) ข้อมูลที่เก็บจะไม่ต่อเนื่อง ถ้าไฟฟ้าดับ

5.3 ข้อเสนอแนะ

1) ประยุกต์ใช้กับการเก็บบันทึกข้อมูลตาม พรบ.คอมพิวเตอร์ 2550

2) สามารถดูรายละเอียดของโพรโทคอลชนิด IPv6

บรรณานุกรม

[1] http://www.netbright.co.th/?name=knowledge&file=readknowledge&id=10.

[2] www.cs.psu.ac.th.

[3] http://oreilly.com/catalog/esnmp/chapter/ch02.html.

[4] http://www.compspot.net/index.php?option=com_content&task=view&id=347&Itemid=46.

[5] คุณพร้อมเลิศ หล่อวิจิตร. *คู่มือเรียน PHP และ MySQL สำหรับผู้เริ่มต้น*.กรุงเทพฯ : โปรวิชั่น 2550.

[6] บัญชา ปะสีละเตสัง. *คู่มือการพัฒนาเว็บด้วย PHP 5 และ MySQL 5*. กรุงเทพฯ : ซีเอ็ดยูเคชั่น, 2550.

[7] อ.บัณฑิต จามรภูติ. *คัมภีร์ Ubuntu Linux Server เล่ม 1*. กรุงเทพฯ : บัณฑิต, 2552.

[8] อ.บัณฑิต จามรภูติ. *คัมภีร์ Ubuntu Linux Server เล่ม 2*. กรุงเทพฯ: บัณฑิต, 2553.

[9] จักรกฤษณ์ แสงแก้ว. *การเขียนโปรแกรมภาษาไพธอนด้วยตนเอง*. กรุงเทพฯ : ส.ส.ท, 2549.

[10] พุฑฒิ วงศ์สว่าง "การพัฒนาระบบสังเกตการณ์การทำงานของเว็บแอพพลิเคชั่นเซิร์ฟเวอร์เพื่อใช้ในโรงพยาบาลกรุงธน." วิทยานิพนธ์ปริญญาวิทยาศาสตร์มหาบัณฑิต, สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ, สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ, 2549.

[11] นิรุธ อำนวยศิลป์. *PHP how-to and web-based application techniques*. กรุงเทพฯ : Thaidev.com, 169 หน้า : ภาพประกอบ, 2548.

[12] นิรุธ อำนวยศิลป์. PHP how-to and web-based application techniques .กรุงเทพฯ : Thaidev.com, 159 หน้า : ภาพประกอบ,2548.

[13] ธวัชชัย ชมศิริ. *Computer&Network Security*. กรุงเทพฯ : โปรวิชั่น, 2553.

[14] Naba Barkakati.The Waite Group's Turbo C Bible.USA : SAMS, 1990.

[15] http://php.net/manual/en/book.snmp.php.

[16] http://bc425.212cafe.com/archive/2007-12-14/network-devices/.

[17] http://202.28.94.55/web/322461/2550/report/g14/snmpIndex.htm.

[18] http://wiki.nectec.or.th/ngiwiki/pub/Project/IntelligentNMS/ng-libpcap1.pdf.

[19].http://citecclub.org/forum/blogs/misslily-13664/%E0%B9%81%E0%B8%9B%E0%B8%A5-programming-libpcap-sniffing-network-our-own-application-%E0%B8%95%E0%B8%AD%E0%B8%99%E0%B8%97%E0%B8%B5%E0%B9%88-1-91/.

[20] http://www.csram.com/board/index.php?topic=121.0.

[21]http://www.google.co.th/url?sa=t&source=web&cd=1&ved=0CCUQFjAA&url=http%3A%2F%2Fcsn.cs.psu.ac.th%2Fkui%2Fdoc%2Fsnmpdoc.pdf&rct=j&q=snmp%20pdf&ei=VNcTI6BoOrceiatPQJ&usg=AFQjCNG7KSIZ3bkMYVwcI95Zf_wpW_6P4w&cad=rja.

[22] http://www.netbright.co.th/?name=knowledge&file=readknowledge&id=10.