ระบบตรวจจับการใช้งานเครือข่ายที่ผิดปกติโดยใช้เน็ตเวิร์กโพรไฟล์

NETWORK TRAFFIC ANOMALY DETECTION USING NETWORK PROFILES

นายพลสุธี ธเนศนิรัตศัย
นายภาสกร สิริสรรพสาร

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ.2548

ระบบตรวจจับการใช้งานเครือข่ายที่ผิดปกติโดยใช้เน็ตเวิร์กโพรไฟล์

NETWORK TRAFFIC ANOMALY DETECTION USING NETWORK PROFILES

นายพลสุธี ธเนศนิรัตศัย

นายภาสกร สิริสรรพสาร

อาจารย์ที่ปรึกษา

อาจารย์ ธนัญชัย ตรีภาค

อาจารย์ อัครเดช วัชระภูพงษ์

ผศ. ธนา หงษ์สุวรรณ

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2548

ปริญญานิพนธ์ปีการศึกษา 2548

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง ระบบตรวจจับการใช้งานเครือข่ายที่ผิดปกติโดยใช้เน็ตเวิร์กโพรไฟล์

NETWORK TRAFFIC ANOMALY DETECTION USING NETWORK PROFILES

ผู้จัดทำ

1. นายพลสุธี ธเนศนิรัตศัย รหัสประจำตัว 45010517
2. นายภาสกร สิริสรรพสาร รหัสประจำตัว 45010590

_____ อาจารย์ที่ปรึกษา

(อาจารย์ ธนัญชัย ตรีภาค)

_____ อาจารย์ที่ปรึกษา

(อาจารย์ อัครเดช วัชระภูพงษ์)

_____ อาจารย์ที่ปรึกษา

(ผศ. ธนา หงษ์สุวรรณ)

ระบบตรวจจับการใช้งานเครือข่ายที่ผิดปกติโดยใช้โดยใช้เน็ตเวิร์คโพรไฟล์

นายพลสุธี ธเนศนิรัตศัย	45010517
นายภาสกร สิริสรรพสาร	45010590
อาจารย์ ธนัญชัย ตรีภาค	อาจารย์ที่ปรึกษา
อาจารย์ อัครเดช วัชระภูพงษ์	อาจารย์ที่ปรึกษาร่วม
ผศ. ธนา หงษ์สุวรรณ	อาจารย์ที่ปรึกษาร่วม
ปีการศึกษา 2548	

บทคัดย่อ

ในปัจจุบันนี้มีการใช้งานเครือข่ายการสื่อสารข้อมูลภายในองค์กรต่างๆ อย่างแพร่หลายทั้งในด้านการสื่อสารข้อมูลภายในองค์กรและการสื่อสารข้อมูลระหว่างองค์กร ดังนั้นองค์กรจึงจำเป็นต้องมีการตรวจระวังการบุกรุกจากบุคคลที่ไม่หวังดี เพื่อให้เครือข่ายสามารถใช้งานได้อย่างเป็นปกติ

โครงงานนี้เป็นการนำเสนอ เครื่องมือสำหรับผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ในด้านการรักษาความปลอดภัยนั้น ต้องสามารถตรวจจับความผิดปกติของการใช้งานภายในเครือข่าย โดยการตรวจสอบข้อมูลสถิติการใช้งานของอุปกรณ์บนระบบเครือข่าย นำมาเก็บสถิติไว้และใช้เปรียบเทียบโดยใช้ทฤษฎีทางสถิติเพื่อคำนวณ และหาลักษณะความผิดปกติของการใช้งานภายในเครือข่าย เพื่อเป็นเครื่องมือให้ผู้ดูแลระบบช่วยในการตัดสินใจในการรักษาความปลอดภัยบนระบบเครือข่าย และเพื่อเพิ่มความปลอดภัยให้กับระบบเครือข่ายให้มากขึ้น โดยแสดงผลในรูปแบบกราฟ

NETWORK TRAFFIC ANOMALY DETECTION USING NETWORK PROFILES

Mr. Polnsutee Thanesniratsai

Mr. Passakorn Sirisuppasarn

Mr. Thanunchai Threepak Advisor

Mr. Akkradach Watcharapupong Co-Advisor

Asst. Prof. Thana Hongsuwan Co-Advisor

Academic Year 2004

ABSTRACT

Presently,Communication Network is applied widely in many organizations including both internal communication and external communication. So organizations must be to keep safe from intrusion for netwok work probably.

This project study statistics theory for classifying amount of data on computer network and detect abnormal network traffic characteristics. Program request traffic data from network device and make sample spaces of norm then compared with current data to identifies current network traffic characteristics and display graph output by Windows based

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้สำเร็จได้ด้วยดี เนื่องจากได้รับการแนะนำ สนับสนุน และให้คำปรึกษาเป็นอย่างดีจากอาจารย์ ธนัญชัย ตรีภาค อาจารย์อัครเดช วัชระภูพงษ์ และ ผศ. ธนา หงษ์สุวรรณ อาจารย์ที่ปรึกษาปริญญานิพนธ์ ซึ่งต้องขอขอบพระคุณเป็นอย่างสูง รวมทั้งอาจารย์ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุกท่าน ที่ให้การอบรมสั่งสอนวิชาความรู้แก่คณะผู้จัดทำมาโดยตลอด

ขอขอบคุณห้องวิจัย ISAG ที่อำนวยความสะดวกเกี่ยวกับสถานที่ทำงาน ที่ศึกษาหาความรู้ และที่พบปะเพื่อน ๆ พี่ ๆ น้อง ๆ เพื่อแลกเปลี่ยนความคิดเห็นแก่กันและกัน

และขอขอบพระคุณเป็นอย่างสูงสำหรับบุคคลที่สำคัญที่สุดที่ทำให้คณะผู้จัดทำมีวันนี้ คือ บิดา มารดา ผู้เป็นที่เคารพรักยิ่งของคณะผู้จัดทำ ซึ่งท่านให้การอบรมสั่งสอน เลี้ยงดู และให้โอกาสในการศึกษาอย่างเต็มที่จึงขอกราบขอบพระคุณมา ณ ที่นี้

พลสุธี ธเนศนิรัตศัย

ภาสกร สิริสรรพสาร

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญรูป

สารบัญรูป (ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

1.1. ความสำคัญและที่มาของโครงงาน

การรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์มีความสำคัญอย่างมาก สำหรับองค์กรต่างๆ ยิ่งต้องให้ความสำคัญกับการปกป้องรักษาความปลอดภัยของข้อมูลหรือบริหารจัดการให้ระบบเครือข่ายใช้งานได้อย่างเป็นปกติ เพราะฉะนั้นในระบบเครือข่ายนั้นก็จำเป็นจะต้องมีอุปกรณ์ช่วยในการรักษาความปลอดภัย ตัวอย่างเช่น ระบบตรวจจับการบุกรุกทางเครือข่าย ซึ่งสามารถสร้างจากโปรแกรมแล้วนำไปใช้ปฏิบัติการที่เครื่องเซิร์ฟเวอร์บนเครือข่ายท้องถิ่นในแต่ละหน่วยงาน ทั้งนี้เพื่อให้ระบบมีประสิทธิผลตรงตามความต้องการของผู้ใช้งานโปรแกรม และยังเหมาะสมกับสภาพแวดล้อมของปริมาณการใช้งานเครือข่ายในแต่ละองค์กรมากขึ้น จากเหตุผลข้างต้นจึงได้ทำการพัฒนาโปรแกรมซึ่งเหมาะสมกับการตรวจจับความผิดปกติของข้อมูลการใช้งานระบบเครือข่ายคอมพิวเตอร์แบบตรวจจับเมื่อเกิดความผิดปกติ (Anomaly detection) เพื่อเป็นอีกเครื่องมือหนึ่งให้ผู้ดูแลระบบใช้ช่วยในการตัดสินใจดำเนินการเพื่อเพิ่มความปลอดภัยของระบบเครือข่ายมากยิ่งขึ้น

1.2. วัตถุประสงค์ของโครงงาน

1. เพื่อศึกษาหลักการทำงานของระบบตรวจจับผู้บุกรุกทางเครือข่ายโดยใช้เน็ตเวิร์กโพรไฟล์
2. เพื่อพัฒนาโปรแกรมต้นแบบที่ตรวจจับความผิดปกติของปริมาณข้อมูลของการใช้งานเครือข่ายคอมพิวเตอร์
3. เพื่อเพิ่มเครื่องมือตรวจสอบด้านความปลอดภัยให้กับผู้ดูแลระบบเครือข่ายคอมพิวเตอร์

1.3. ขอบเขตของโครงงาน

โปรแกรมระบบตรวจจับการใช้งานเครือข่ายที่ผิดปกติโดยใช้เน็ตเวิร์กโพรไฟล์นั้น ใช้วิธีการตรวจสอบปริมาณข้อมูลของการใช้งานเครือข่าย โปรแกรมจะทำการดึงข้อมูลโดยใช้โปรโตคอล Simple Network Management Protocol (SNMP) จากอุปกรณ์บนเครือข่าย (เช่น เราท์เตอร์ หรือ อีเธอร์เน็ตสวิตช์) ซึ่งค่าปริมาณข้อมูลของการใช้งานเครือข่ายนั้นได้ถูกเก็บเอาไว้ในอุปกรณ์อยู่แล้ว โปรแกรมจะนำค่าที่ดึงมาจากอุปกรณ์มาเก็บและวิเคราะห์ในเชิงสถิติ เพื่อวิเคราะห์ว่าปริมาณการใช้งานเครือข่ายในช่วงเวลาขณะนั้นๆ ว่าเกิดความผิดปกติขึ้นจากสถิติการใช้งานปกติ

เดิมที่เก็บไว้เป็นโพรไฟล์หรือไม่ ถ้าหากเกิดความผิดปกติก็จะแจ้งให้ผู้ดูแลระบบทราบว่าปริมาณการใช้งานเครือข่ายมีลักษณะผิดปกติจนอาจจะเกิดการบุกรุกเข้ามาในเครือข่าย หรือเกิดการแพร่กระจายตัวของไวรัสคอมพิวเตอร์ภายในระบบเครือข่าย

1.4. วิธีการดำเนินการ

1. ศึกษารายละเอียดเกี่ยวกับโปรโตคอลเอสเอ็นเอ็มพี(SNMP)และอาร์เอ็มโอเอ็น (RMON) เพื่อหาตัวแปรที่จะนำมาใช้งานในโครงงาน
2. ศึกษาสมการทางสถิติเพื่อใช้ในการวิเคราะห์ข้อมูลการใช้งาน
3. ศึกษาการเขียนโปรแกรมภาษาซีชาร์ปด็อตเน็ต (C#.NET)
4. ศึกษา Library SNMP++ เพื่อใช้ในการดึงข้อมูลจากอุปกรณ์บนเครือข่าย
5. ศึกษาการเขียนโปรแกรมเพื่อติดต่อฐานข้อมูลโดยใช้ MySQL
6. ศึกษาเครื่องมือ Chartdirector เพื่อใช้ในการสร้างกราฟเพื่อแสดงผล
7. พัฒนาโปรแกรมที่ตรวจจับความผิดปกติของปริมาณข้อมูลของการใช้งานเครือข่ายคอมพิวเตอร์
8. รวบรวมชุดข้อมูลการใช้งานของเครือข่ายปกติ
9. ทำการทดสอบโปรแกรมในการตรวจจับความผิดปกติของปริมาณการใช้งานเครือข่าย
10. ทำการแก้ไขข้อผิดพลาดต่าง ๆ ที่เกิดขึ้น
11. สรุปผลการทดลอง

1.5. ประโยชน์ที่คาดว่าจะได้รับ

1. ได้รับความรู้ในกระบวนการตรวจจับผู้บุกรุกในลักษณะตรวจจับความผิดปกติ
2. ได้ทักษะในการเขียนโปรแกรมที่มีการติดต่อกับอุปกรณ์บนเครือข่าย
3. ได้รับความรู้ ความเข้าใจลักษณะในการวิเคราะห์ข้อมูลเชิงสถิติ
4. ได้โปรแกรมตรวจสอบความผิดปกติการใช้งานเครือข่ายที่อำนวยความสะดวกแก่ผู้ดูแลระบบ

1.6. ส่วนประกอบของปริญญานิพนธ์

ปริญญานิพนธ์นี้ได้มีการแบ่งออกเป็น 6 บท โดยมีรายละเอียดดังต่อไปนี้

บทที่ 1เป็นบทที่อธิบายถึงวัตถุประสงค์ ขอบเขต ของโครงงานว่ามีลักษณะอย่างไร

บทที่ 2 เป็นบทที่อธิบายถึงรายละเอียดของทฤษฎีและโปรโตคอลต่างๆ ที่เกี่ยวข้องกับโครงงานและได้นำมาใช้กับโครงงาน เช่น ทฤษฎีทางสถิติ ต่างๆ

บทที่ 3 เป็นบทที่อธิบายถึงรายละเอียดของการออกแบบโปรแกรมภายในโครงงาน โดยบอกถึงขั้นตอนการทำงานของโปรแกรมในส่วนต่างๆ ภายในโปรแกรม รวมทั้งเครื่องมือที่ใช้ในการพัฒนา

บทที่ 4 เป็นบทที่อธิบายถึงการทำงานหลัก ๆ ของโปรแกรมว่ามีอะไรและทำงานอย่างไรบ้างรวมถึงรายละเอียดในแต่ละขั้นตอน

บทที่ 5 เป็นบทที่ทำการทดลองโปรแกรมเพื่อทำการตรวจจับความผิดปกติ

บทที่ 6 เป็นบทวิจารณ์และสรุป ซึ่งกล่าวถึงบทสรุปของโครงงาน วิจารณ์สิ่งที่ได้รับจากโครงงาน และข้อเสนอแนะสำหรับเป็นแนวทางในการพัฒนาต่อ

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

2.1.บทนำ

SNMP เป็นโปรโตคอลในระดับประยุกต์ (Application Layer) ที่กำหนดรูปแบบ และ กรรมวิธีการจัดการเครือข่าย โดยมีสถานีจัดการเครือข่ายส่วนกลางทำหน้าที่ดูแล ตรวจสอบ และควบคุมการทำงานของอุปกรณ์เครือข่าย

2.2. SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

2.2.1. พื้นฐานการบริหารเครือข่าย

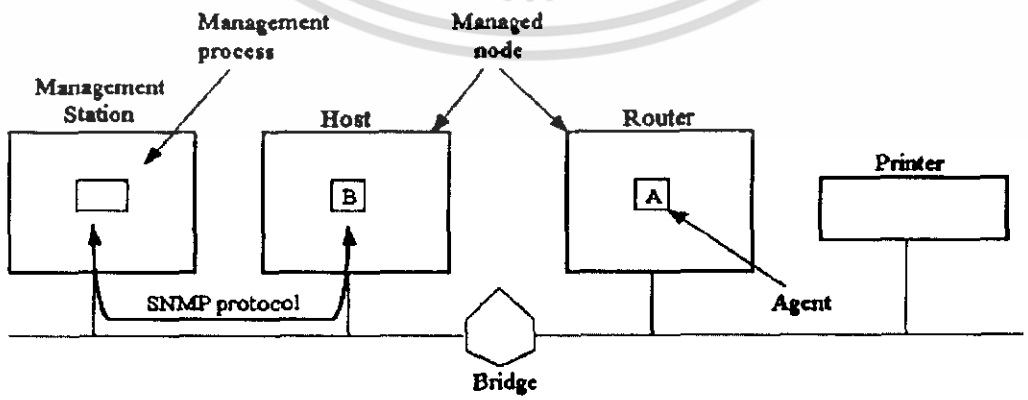
การบริหารเครือข่าย คือ การตรวจ ควบคุม และวางแผนการใช้ทรัพยากรระบบเพื่อให้เครือข่ายทำงานได้อย่างมีประสิทธิภาพ และ สามารถตรวจหาจุดบกพร่องที่เกิดขึ้นเพื่อแก้ไขปัญหาได้อย่างรวดเร็วในระบบเครือข่ายใดๆที่ เอสเอ็นเอ็มพี จัดการ จะต้องประกอบด้วย เอสเอ็นเอ็มพี โมเดล (SNMP Model) 4 ส่วนคือ

2.1.1.1. Managed nodes: อาจจะเป็น โฮสต์, เราท์เตอร์, ปรินท์เตอร์ หรืออุปกรณ์อื่นๆก็ได้ที่สามารถส่งข้อมูลสถานะของมันออกไปยังระบบได้ จะเป็นอุปกรณ์ ฮาร์ดแวร์ หรือ ซอฟท์แวร์ ก็ได้ แต่ต้องมี เอสเอ็นเอ็มพีเอเจนต์ อยู่ในตัวด้วย

2.1.1.2. Management stations: คือ อุปกรณ์ใดๆที่มีฟังก์ชั่น ให้ตรวจสอบและปรับเปลี่ยนการทำงานได้ ซึ่งทำหน้าที่ ตรวจตรา และ ควบคุม Managed nodes

2.1.1.3. Management information.

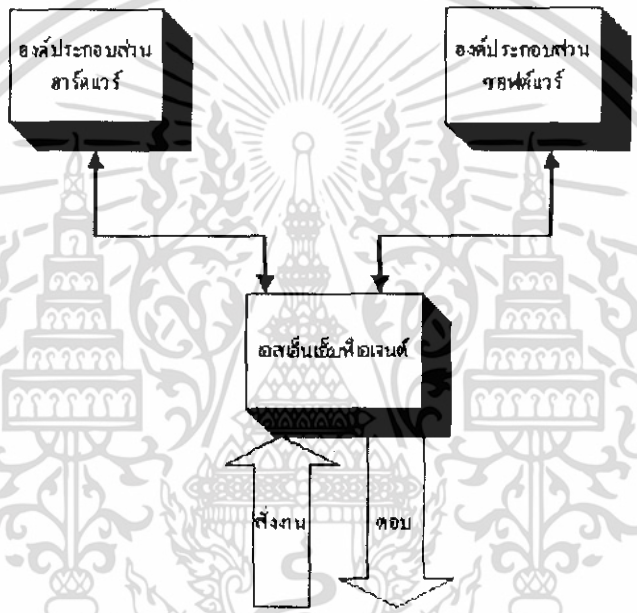
2.1.1.4. A management protocol.



รูปที่ 2.1 โมเดลส่วนประกอบในการจัดการของเอสเอ็นเอ็มพี

2.2.2. เอสเอ็นเอ็มพีเอเจนต์

การจัดการเครือข่าย TCP/IP อาศัยรูปแบบการจัดการมาตรฐานตามข้อกำหนดของโปรโตคอล SNMP ซึ่งเป็นโปรโตคอลประยุกต์ที่กำหนดรูปแบบและกรรมวิธีการจัดการเครือข่าย โดยการทำงานagent จะนำข้อมูลจากส่วน ซอฟท์แวร์ หรือ ฮาร์ดแวร์ เมื่อ Management stations ร้องขอข้อมูล และปรับเปลี่ยนการทำงานของ ซอฟท์แวร์ หรือ ฮาร์ดแวร์ เมื่อ Management stations สั่งงาน โดยมีการแจ้งยืนยันสิทธิในรูปในรหัสผ่านว่าManagement stations มีอำนาจหน้าที่ในการร้องขอและปรับค่า



รูปที่ 2.2 เอสเอ็นเอ็มพีเอเจนต์

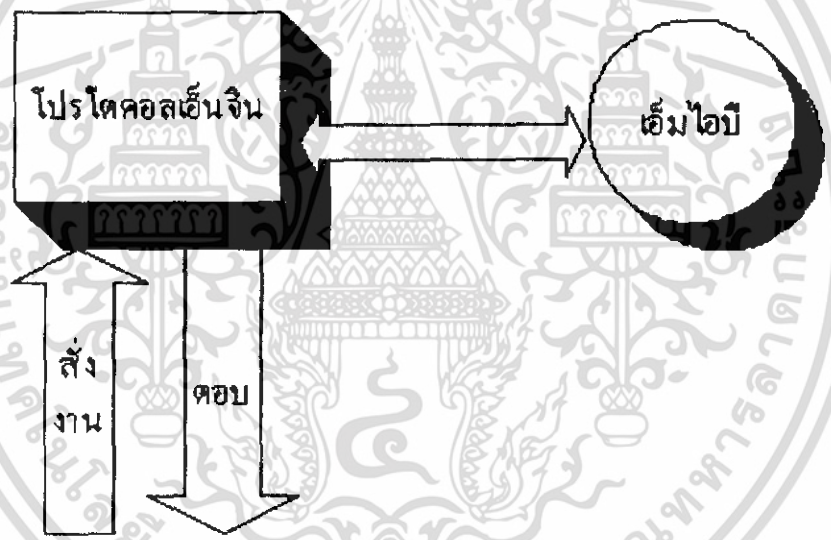
2.2.3. เอ็มไอบี (MIB: Management Information Base)

เอเจนต์จะประกอบด้วยส่วนสำคัญ 2 ส่วนคือ โปรโตคอลเอ็นจิน (Protocol engine) และฐานข้อมูลสารสนเทศการจัดการ (Management Information Base: MIB) โปรโตคอลเอ็นจินทำหน้าที่ประมวลคำสั่งที่มาจากNMS (Network Management Station) ซึ่งได้แก่ รับคำสั่ง ถอดรหัสคำสั่ง ทำงานตามคำสั่งและส่งผลตอบกลับ MIB เป็นส่วนที่เก็บตัวแปรและค่ากำหนดการทำงานประจำอุปกรณ์ภายใน MIB ประกอบด้วยตัวแปรจำนวนมากที่เรียกโดยทั่วไปว่า อ๊อบเจ็คจัดการ (managed object) อ๊อบเจ็คในความหมายนี้เป็นชื่อที่ใช้เรียกตัวแปรและลักษณะเฉพาะของตัวแปรในMIBโดยไม่เกี่ยวข้องกับ เชิงวัตถุพิสัย (object oriented) แต่อย่างใด โดยจะพิจารณาอ๊อบเจ็คใน SNMP มีลักษณะเช่นเดียวกับเรคอร์ดในฐานข้อมูลแต่ละอ๊อบเจ็ค จะมีชื่อเรียกเฉพาะเรียกว่า อ๊อบ

เจ็คไอเด็นติไฟเออร์ (Object Identifier) หรือเรียกโดยย่อว่า ไอเด็นติไฟเออร์ (Identifier) เพื่อใช้อ้างอิงถึงอ๊อบเจ็คนั้นอ๊อบเจ็คทุกตัวมีนิยามที่กำหนด ชื่อ แบบข้อมูล สิทธิ์การเข้าถึง คำอธิบายลักษณะ และค่าข้อมูลการนิยามอ๊อบเจ็คมีกฎเกณฑ์ตามข้อกำหนด โครงสร้างฐานข้อมูลสารสนเทศ (Structure of Management Information: SMI)[RFC 1155]

2.2.3.1. ตัวระบุอ๊อบเจ็ค (Object identifier)

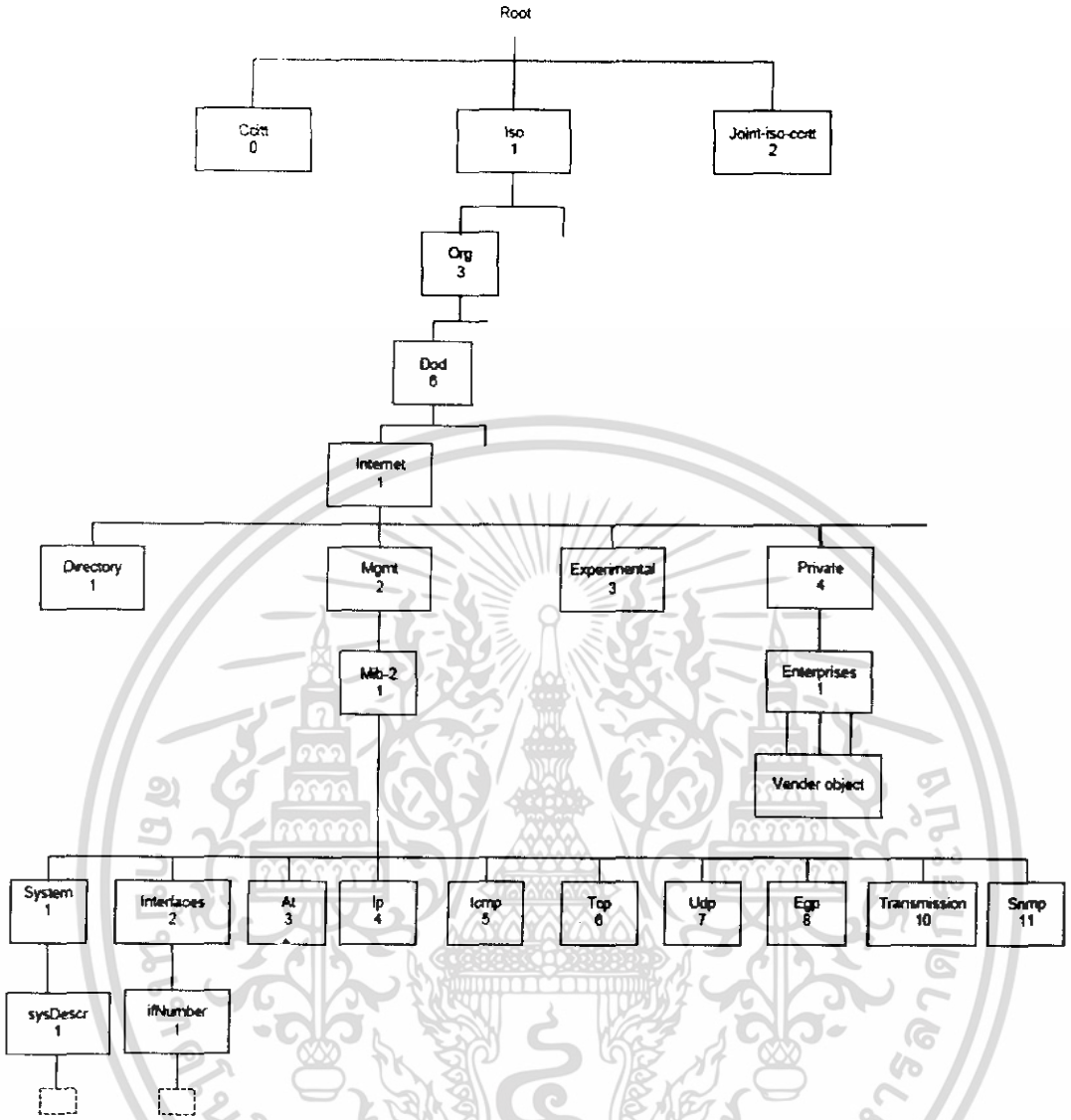
OID (Object Identifier) คือตัวระบุอ๊อบเจ็คใน Management Information Base ซึ่งเป็นข้อมูลเพื่อการจัดการข้อมูลและกระบวนการทำงานของอุปกรณ์บนระบบเครือข่ายที่สนับสนุนโปรโตคอล SNMP (Simple Network Management Protocol) โดยแต่ละอ๊อบเจ็คจะมีนิยามที่กำหนด ชื่อ แบบข้อมูล สิทธิ์การเข้าถึง คำอธิบายลักษณะและค่าของข้อมูลโดยการนิยามอ๊อบเจ็คมีกฎเกณฑ์ตามข้อกำหนด โครงสร้างฐานข้อมูลสารสนเทศการจัดการ (MIB)



รูปที่ 2.3 โครงสร้างของเอเจนต์

2.2.3.2. โครงสร้างเอ็มไอบี

ข้อมูลประจำของในแต่ละอุปกรณ์เครือข่ายชนิดหนึ่งๆนั้นมีได้อย่างหลากหลาย และด้วยความแตกต่างกันของผู้ผลิตก็ย่อมมีการวางข้อมูลประของอุปกรณ์ที่แตกต่างกัน ดังนั้นการร้องขอค่าต่างๆ หรือการเปลี่ยนแปลงค่าต่างๆ นั้นต้องทำให้เป็นรูปแบบมาตรฐานกลางเดียวกันให้กับทุกอุปกรณ์และทุกผู้ผลิต ซึ่งโครงสร้างรูปแบบต้นไม้แบลำดับชั้นนั้นเป็นโครงสร้างที่เหมาะสำหรับใช้เป็นโครงสร้างที่จัดเก็บตัวแปร และข้อมูลเหล่านี้



รูปที่ 2.4 โครงสร้างอ๊อบเจ็คไอเด็นติไฟเออร์ ในโครงสร้างฐานข้อมูลสารสนเทศการจัดการ

ดังรูปที่ 2.4 แสดงโครงสร้างอ๊อบเจ็คของเอสเอ็นเอ็มพีในรูปแบบโครงสร้างต้นไม้ซึ่งเรียกกันว่า มิบทรี (MIB tree) ซึ่งแต่ละโหนดแทนด้วยอ๊อบเจ็คหนึ่งๆ มีชื่อพร้อมทั้งตัวเลขฐานสิบกำกับตำแหน่งเพื่อใช้ในการอ้างอิง ยกเว้นโหนดราก จะไม่มีชื่อกำกับ

เมื่อต้องการอ้างอิงถึงโหนดในโครงสร้างใดๆ ในโครงสร้างให้เขียนหมายเลขกำกับโหนดตั้งแต่รากไปตามเส้นทางโหนดที่ต้องการโดยแต่ละโหนดคั่นด้วยจุดโดยตัวเลขเหล่านี้ คือ อ๊อบเจ็คไอเด็นติไฟเออร์ (OID)

ตัวอย่างการอ้างชื่อของโหนดอ๊อบเจ็คไอเด็นติไฟเออร์ 1.3.6.1.2.1.1 เป็น อ๊อบเจ็คไอเด็นติไฟเออร์ที่มีชื่อ iso.org.internet.mgmt.mib-2.system โหนดที่อยู่ภายใต้ 1.3.6.1.2.1 หรือในกลุ่ม mib-

2 เป็นโหนดสำหรับใช้งานเอสเอ็นเอ็มพี แต่ละโหนดจะมีโหนดย่อยเพื่ออ้างอิงถึงตัวแปรเช่น 1.3.6.1.2.1.1.1 คือตัวแปร sysDesc (System Description) ซึ่งเก็บคำอธิบายของอุปกรณ์นั้น

2.2.3.3. กลุ่มของมิบ

มิบภายใต้ internet มีกลุ่มย่อย 6 กลุ่ม คือ

1. directory (1) สงวนไว้ใช้งานสำหรับในอนาคต
2. mgmt (2) กลุ่มมิบที่ใช้ในการจัดการภายใต้
3. experiment (3) ใช้สำหรับการทดลอง
4. private (4) ใช้สำหรับให้ผู้ผลิตกำหนดตัวแปรเฉพาะอุปกรณ์
5. security (5) ใช้ในระบบรักษาความปลอดภัย
5. SNMPv2 (6) ใช้ในเอสเอ็นอีมพี รุ่น 2

ภายใต้กลุ่ม mib-2 บรรจุกลุ่มย่อยที่ใช้ในเอสเอ็นเอ็มพีซึ่งประกอบด้วย interfaces, at และ ip และที่อื่นๆ ความหมายของแต่ละกลุ่มอธิบายไว้ในตารางที่ 2.1 แต่ละกลุ่มจะประกอบด้วยตัวแปรซึ่งมีแบบต่างๆ กันไป

ตารางที่ 2.1 กลุ่มย่อยภายใต้โหนด mgmt

ลำดับ	ชื่อ	ความหมาย
1	system	ข้อมูลระบบ
2	interfaces	ข้อมูลอินเตอร์เฟสที่ใช้เชื่อต่อ
3	at	ข้อมูลการแปลงแอดเดรส
4	ip	ข้อมูลไอพี
5	icmp	ข้อมูลไอซีเอ็มพี
6	Tcp	ข้อมูลทีซีพี
7	Udp	ข้อมูลยูดีพี
8	Egp	ข้อมูลโพรโตคอลเกตเวย์ภายนอก
10	Tranmission	ข้อมูลสายสื่อสาร
10	Snmp	ข้อมูลเอสเอ็นเอ็มพี
16	rmon	ข้อมูลเครือข่าย

2.2.3.4. ชนิดของตัวแปรมิบ

แต่ละตัวแปรในเอสเอ็นเอ็มพีมีข้อมูลประจำ แบบข้อมูลที่ใช้อยู่ในเอสเอ็นเอ็มพีมีดังนี้

• Integer: จำนวนเต็มเช่นหมายเลขพอร์ตของโปรโตคอลทีซีพีหรือยูดีพี มีค่าได้ตั้งแต่ 0 ถึง 65535

• OctetString: สายอักขระขนาดตั้งแต่ 0 อ๊อกเท็ต แต่ละอ๊อกเท็ตมีค่าตั้งแต่ 0 ถึง 255 ตัวอย่างแบบข้อมูลสายอักขระได้แก่ รหัสผ่าน

• DisplayString: สายอักขระตั้งแต่ 0 อ๊อกเท็ตแต่ละอ๊อกเท็ตต้องเป็นรหัสแอสกีเอ็นวีที ข้อมูลประเภทนี้มีความยาวตั้งแต่ 0 ถึง 255 ตัวอักษร

• Null: ใช้บอกว่าตัวแปรนั้นไม่มีค่าข้อมูลใดอยู่ เช่นเมื่อสอบถามข้อมูลด้วยคำสั่ง get หรือ get-next-request จะกำหนดแบบข้อมูลตัวแปรเท่ากับ null

• ObjectIdentifier: ชื่อตัวแปรในรูปแบบของการอ้างถึงแบบตัวเลขตามโครงสร้างมิบ

• IpAddress: สายอักขระ 4 อ๊อกเท็ต แต่ละอ๊อกเท็ตแทนไอพีแอดเดรสแต่ละตำแหน่ง

• PhysicalAddress: สายอักขระกำหนดฮาร์ดแวร์แอดเดรสเช่น อีเทอเน็ตแอดเดรสใช้สายอักขระ 6 อ๊อกเท็ต

• Counter: เลขจำนวนเต็มไม่คิดเครื่องหมาย มีค่าตั้งแต่ 0 ถึง 2 – 1 (4,294,967,295) การใช้ข้อมูล counter เป็นแบบเพิ่มค่าขึ้นอย่างเดียว เมื่อเพิ่มถึงค่ามากสุดจะกลับเป็น 0 ใหม่

• Gauge: เลขจำนวนเต็มไม่คิดเครื่องหมาย มีค่าตั้งแต่ 0 ถึง 2 -1 โดยสามารถเพิ่มหรือลดค่าได้ แต่เมื่อเพิ่มไปสูงสุดแล้วจะคงค่าไว้จนกว่าจะถูกปรับค่ากลับมาเป็น 0 อีกครั้ง ตัวอย่างตัวแปรที่ใช้ค่านี้ เช่น จำนวนการเชื่อมโยงทีซีพีที่อนุญาตให้มีได้

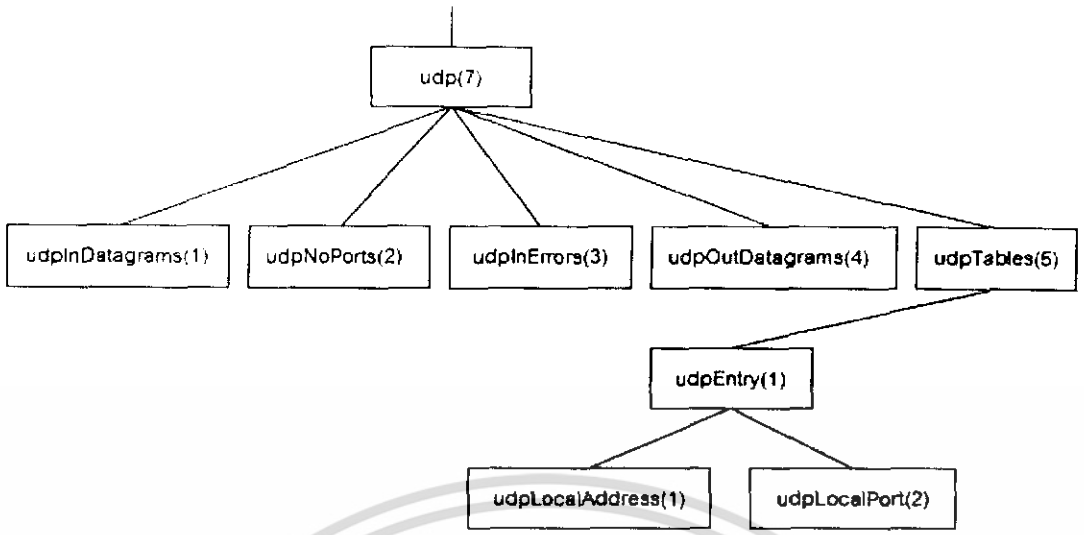
• TimeTicks: เลขจำนวนเต็มใช้นับเวลาให้หน่วยเศษหนึ่งส่วนร้อยของวินาที เช่น เวลานับตั้งที่ระบบเริ่มทำงาน

• Sequence: โครงสร้างแบบเร็คคอร์ด หรือคล้ายกับแบบข้อมูล struct ในภาษาซี

• Sequence of: โครงสร้างแบบตารางหรือมองในรูปของอาร์เรย์ เช่นตารางเลือกเส้นทางของไอพี

2.2.3.5. ตัวอย่างแบบข้อมูลอาร์เรย์

แบบข้อมูล sequence of ใช้กำหนดข้อมูลแบบเวกเตอร์ซึ่งสมาชิกทั้งหมดภายในมีข้อมูลแบบเดียวกัน หากสมาชิกมีแบบข้อมูลเบื้องต้น เช่น แบบจำนวนเต็มก็จะได้เวกเตอร์แบบมิติเดียว หรือหากสมาชิกมีข้อมูลแบบ sequence ก็จะได้อาร์เรย์ 2 มิติ ตัวอย่างของตัวแปรโครงสร้างอาร์เรย์ในมิบมีอยู่หลายตัวแปร แต่จะยกตัวอย่างเฉพาะตัวแปรที่มีขนาดเล็กเพื่อที่จะทำความเข้าใจได้ง่าย ได้แก่ udpTable ซึ่งสังกัดอยู่ภายใต้กลุ่ม udp ตามโครงสร้างข้อมูลดังรูปที่ 2.5



รูปที่ 2.5 udpTable ในรูปอาร์เรย์สองมิติ (ตาราง)

udpTable มีแบบข้อมูล sequence of และภายใต้ udpTable มี udpEntry ซึ่งมีแบบข้อมูล sequenceโดยประกอบด้วย udpLocalAddress และ udpLocalPort

udpLocalAddress มีแบบข้อมูล IpAddress ใช้กำหนดไอพีแอดเดรสที่รอให้บริการส่วนของudpLocalPort กำหนดหมายเลขพอร์ตดังนั้น udpTable จึงมีโครงสร้างเป็นอาร์เรย์ 2 มิติหรือเขียนด้วยตารางดังรูปที่ 2.6

	udpLocalAddress	udpLocalPort
udpEntry	(IpAddress)	(Integer)
udpEntry	...	...
udpEntry	...	...
udpEntry	...	...
udpEntry	...	...

รูปที่ 2.6 udpTable ในรูปอาร์เรย์สองมิติ (ตาราง)

2.2.3.6. ชื่อคอมมูนิตี้ (Communities and Community Names)

การบริหารเครือข่ายจะถือได้ว่าเป็นการทำงานในลักษณะระบบกระจาย (Distributed application)รูปแบบหนึ่ง ซึ่งจะเห็นได้ว่าความสัมพันธ์ระหว่างสถานีจัดการเครือข่าย (Network Management Station :NMS) กับเอเจนต์ (Agent) จะเป็นในรูปแบบ many-to-many คือ สถานีจัดการเครือข่ายจะบริหารจัดเอเจนต์ได้หลายเครื่อง และในขณะเดียวกันเอเจนต์ก็สามารถถูกบริหาร

ควบคุมจากสถานีจัดการเครือข่ายหลายเครื่องเช่นกัน จากความสัมพันธ์ดังกล่าวจึงจำเป็นที่เอเจนต์แต่ละเครื่องจำเป็นที่จะต้องมีมาตรการควบคุมความปลอดภัยในการใช้งานฐานข้อมูลสารสนเทศการจัดการ (Management Information Base : MIB) ของตนเองโดยจะมีมุมมองทางด้านความปลอดภัย 3 ประการได้แก่

- การพิสูจน์ตัวตน (Authentication service) จะเป็นการจำกัดให้เฉพาะสถานีจัดการเครือข่ายที่จะเข้ามาบริการควบคุม
- นโยบายการเข้าถึง (Access policy) จะมีการกำหนดระดับการอนุญาตการเข้าถึงฐานข้อมูล
- สารสนเทศการจัดการให้แต่ละสถานีจัดการเครือข่ายไม่เท่ากันในแต่ละเครื่อง การให้บริการ Proxy (Proxy service) เอเจนต์อาจทำหน้าที่เป็น Proxy ให้กับเอเจนต์เครื่องอื่นซึ่งจะรวมถึงการพิสูจน์ตัวตนและนโยบายการเข้าถึงของเอเจนต์ตัวอื่นที่อยู่ในระบบ Proxy

เอสเอ็นเอ็มพี (SNMP) ได้มีการกำหนดการทำงานเพื่อสนับสนุนมุมมองทางด้านทางปลอดภัยดังกล่าวในรูปแบบของ SNMP Community โดยการทำงานคือ เอเจนต์แต่ละเครื่องจะมีการสร้างCommunity name เพื่อกำหนดให้กับสถานีจัดการเครือข่าย โดนในหนึ่ง Community name จะสามารถมีสถานีจัดการเครือข่ายมากกว่าหนึ่งตัว

เนื่องจาก Community name จะถูกกำหนดในแต่ละเอเจนต์จึงอาจเป็นไปได้ว่ามีการตั้งชื่อ Community name ซ้ำกันในแต่ละเอเจนต์ แต่สถานีจัดการเครือข่ายจะสามารถแยกความแต่ต่างของ Community ที่มีชื่อซ้ำกันเหล่า นี้เองได้ถ้าอยู่ในคนละเอเจนต์กัน ดังนั้นจึงจำเป็นที่ว่าสถานีจัดการเครือข่ายจะต้องเก็บข้อมูลของ Community name และข้อมูลที่เกี่ยวข้องของแต่ละเอเจนต์เพื่อใช้ในการบริหารควบคุม

2.2.3.7. นโยบายการเข้าถึง (Access policy)

การควบคุมการเข้าถึงในเอสเอ็นเอ็มพีจะประกอบด้วย 2 องค์ประกอบหลักที่เกี่ยวข้องคือ

- SNMP MIB view: คือกลุ่มของอ็อบเจ็กในฐานข้อมูลสารสนเทศการจัดการที่ตั้งขึ้นโดยในแต่ละกลุ่มอาจจะประกอบด้วยหลาย Sub tree ในฐานข้อมูลสารสนเทศการจัดการได้
- SNMP access mode: คือรูปแบบของการเข้าถึงได้แก่ READ-ONLY และ READWRITE

ในเอเจนต์จะมีการกำหนด Access mode ให้แต่ละ MIB view ซึ่ง Access mode จะมีผลกับทุกๆObject ที่อยู่ในกลุ่มของ MIB view โดยทั้ง Access mode และ MIB view จะถูกเรียกรวมกันว่า SNMP community profile ซึ่งจะถูกกำหนดในแต่ละ Community

ใน Access mode ของเอสเอ็นเอ็มพีจะมีการประนีประนอมต่อรองระดับการเข้าถึงกับระดับของการเข้าถึงของฐานข้อมูลสารสนเทศการจัดการ (MIB Access Category) ดังตารางที่ 2.2

(Access mode ของเอสเอ็นเอ็มพีกับระดับของการเข้าถึงของฐานข้อมูลสารสนเทศการจัดการเป็นคนละส่วนกัน) และจะเรียกรวม SNMP community และ SNMP community profile ว่า SNMP access policy

ตารางที่ 2.2 ความสัมพันธ์ระหว่าง MIB Access Category และ SNMP Access Mode

MIB Access	SNMP Access Mode	
Category	READ-ONLY	READ-WRITE
read-only	สามารถใช้คำสั่ง get และ trap ได้	
read-write	สามารถใช้คำสั่ง get และ trap ได้	สามารถใช้คำสั่ง get, set และ trap ได้
write-only	สามารถใช้คำสั่ง get และ trap แต่ต้องเป็นค่าที่เป็น implementation-specific	สามารถใช้คำสั่ง get, set และ trap ได้แต่ต้องเป็นค่าที่เป็น implementation-specific สำหรับคำสั่ง get และ trap
not accessible	ไม่สามารถเข้าถึงได้	

2.2.3.8. การอ้างอิงถึงค่าในอ็อบเจ็ก (Instance Identification)

ในการอ้างอิงถึงค่าของอ็อบเจ็กในฐานข้อมูลสารสนเทศการจัดการของเอสเอ็นเอ็มพีนั้นจะอาศัยการอ้างอิงของอินสแตนท์ไอเด็นติไฟเออร์ (Instance Identifier) สำหรับการอ้างถึงค่าของอ็อบเจ็คแบบปกติ (Simple Object Value) โดยทั่วไปจะใช้อินสแตนท์ไอเด็นติไฟเออร์ที่ประกอบไปด้วยค่าของ อ็อบเจ็คไอเด็นติไฟเออร์ (Object Identifier) แล้วปิดท้ายด้วย 0 คือจะอยู่ในรูปแบบของ

Instance Identifier = Object Identifier.0

เช่นการอ้างถึงค่าในอ็อบเจ็คsysDescrด้วยค่าอินสแตนท์ไอเด็นติไฟเออร์คือ 1.3.6.1.2.1.1.1.0 ซึ่งก็คือจะประกอบด้วยค่าอ็อบเจ็คไอเด็นติไฟเออร์ของอ็อบเจ็ค sysDescr คือ 1.3.6.1.2.1.1.1 แล้วต่อท้ายด้วย0 นอกจากนั้นยังอาจเขียนในรูปของชื่อได้คือ iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0 หรือ เขียนสั้นๆเพียง sysDescr.0 ก็ได้ สำหรับการอ้างถึงค่าของอ็อบเจ็คในรูปแบบตาราง (Sequence of Object Value) นั้น เอสเอ็นเอ็มพีไม่อนุญาตให้อ้างอิงทั้งตารางได้ในคราวเดียว การอ้างอิงจะต้องทำที่อ็อบเจ็คที่เป็นโหนดปลายเท่านั้น (Leaf object)

2.3. Exponential Weight Moving Average (EWMA)

Exponentially Weighted Moving Average (EWMA) เป็นสถิติที่ใช้สำหรับตรวจสอบสิ่งต่างๆ ที่มีการเฉลี่ยข้อมูลซึ่งเป็นการคาดคะเนว่าข้อมูลที่ได้นั้นมีลักษณะอย่างไร เมื่อเทียบกับข้อมูลในอดีตที่ผ่านมา ถ่วงน้ำหนักข้อมูลใหม่และข้อมูลเก่าให้มีความเหมาะสมกับสัดส่วน ทำให้ค่าเฉลี่ยไม่แปรผันตามข้อมูลใหม่จนเกิดความแปรปรวนมากจนเกินไป โดยมีรูปแบบสมการดังนี้

$$X_{i(t)} = \lambda * X + (1-\lambda) * X_{(t-1)} \qquad (2.1)$$

โดย

1. λ เป็นค่าคงที่ที่กำหนดอัตราว่าข้อมูลที่ผ่านมานั้นมีผลเท่าไหร่กับการคิดค่าใน EWMA โดยมาค่าอยู่ในช่วง 0 ถึง1
   - ถ้า λ มีค่าเป็น 1 แสดงว่าข้อมูลที่ผ่านมานั้นมีผลมากที่สุดกับการคิด EWMA
   - ถ้า λ มีค่าเป็น 0 คือ ค่าข้อมูลที่ผ่านมาไม่มีค่าใดกับกับการคิด EWMA
2. X เป็นค่าที่แตกต่างกันระหว่างของค่า $Y_{(t)} - Y_{(t-1)}$ (ค่าข้อมูลดิบที่ได้มาจาก SNMP ที่ดึงมาจาก Router)
3. $X_{(t-1)}$ เป็นค่า EWMA ณ เวลาที่ t-1 (เวลาที่ผ่านมา)
4. $X_{i(t)}$ เป็นค่า EWMA ณ เวลา t (ช่วงที่สังเกต)

โดยค่าข้อมูลเมื่อผ่าน EWMA นั้นจะถูกถ่วงน้ำหนักด้วยค่าของช่วงที่ผ่านมาซึ่งมีความสัมพันธ์กับค่าที่ผ่านมาในอดีต

2.4. Chi-Square Test

เป็นวิธีการทางสถิติในลักษณะ Bivariate tabular analysis เพื่อแยกรูปแบบระดับของการทดสอบว่าค่าที่ทดสอบนั้นมีความเบี่ยงเบนไปจากค่าที่ควรจะเป็นขนาดใด

ข้อกำหนดของ Chi-Square มีดังนี้

1. โดยค่าที่สังเกตในแต่ละตัวแปรนั้นจะต้องเป็นอิสระจากกัน
2. ความถี่ของค่าที่สังเกตต้องมีขนาดไม่เล็กจนเกินไป

$$X^2 = \sum_{i=1}^{n} \frac{(X_i - E_i)^2}{E_i} \qquad (2.2)$$

โดย

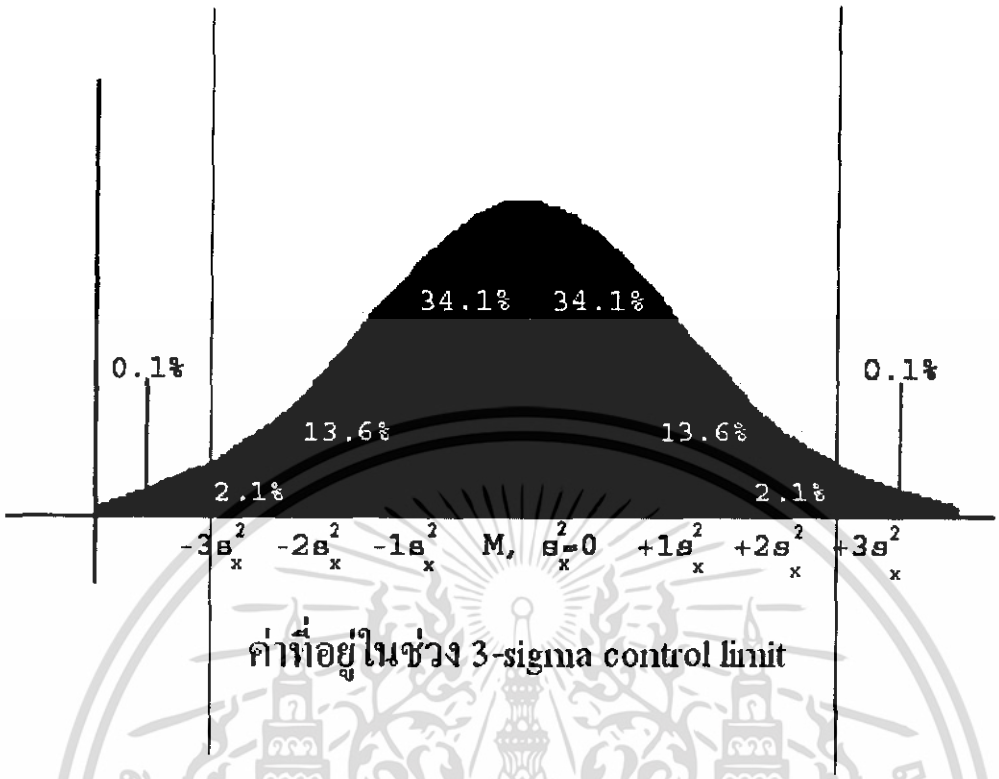
1. Xi เป็นค่าของข้อมูลการใช้งานเครือข่าย ณ เวลาที่สังเกต
2. Ei เป็นค่าปริมาณการใช้งานที่ควรจะเป็นของข้อมูลการใช้งานเครือข่ายในเครือข่ายปกติ (Expect value) โดยในโครงงานนี้ ใช้ค่านี้เป็น ค่าเฉลี่ยของข้อมูลในเครือข่ายปกติ

โดยเมื่อค่าในการสังเกตกับค่าในระบบปกติมีความใกล้เคียงกัน ผลที่ได้จากการคำนวณ Chi-Square Test นั้นจะมีค่าอยู่ภายในขอบเขตค่า 3-Sigma Control Limit เป็น control limit ซึ่งเป็นตัวกำหนดว่า ค่าที่ได้จากการคำนวณ Chi-Square test นั้น อยู่ในเกณฑ์ที่ยอมรับได้ยังอยู่ในสถานการณ์การใช้งานเครือข่ายที่ปกติหรือไม่

$$\text{Control Limit} = \overline{X}^2 + 3S^2 \qquad (2.3)$$

โดย

1. $\overline{X}^2$ เป็นค่า Chi-Square ของ ปริมาณข้อมูลการใช้งานเครือข่ายปกติ
2. $3S^2$ เป็นค่าเบี่ยงเบนมาตรฐานของข้อมูลการใช้งานปกติ



รูปที่2.7 ขอบเขตของค่า 3-sigma control limit

2.5. ค่าเบี่ยงเบนมาตรฐาน (Standard Deviation)

ค่าเบี่ยงเบนมาตรฐาน เป็นค่าที่ใช้วัดการกระจายตัวของข้อมูลว่ามีการกระจายตัวขนาดมากน้อยมากเพียงใด

$$SD. = \sqrt{\frac{\sum (X - \bar{X})^2}{N}} \qquad (2.4)$$

โดย

SD คือ ค่าเบี่ยงเบนมาตรฐาน

X คือ ค่าของตัวแปรที่นำมาคิดค่าเบี่ยงเบนมาตรฐาน

$\bar{X}$ คือ ค่าเฉลี่ยเลขคณิต

2.6 ค่าเฉลี่ยเลขคณิต

ค่าเฉลี่ยเลขคณิต เป็นค่าที่ใช้ในการหาค่าเฉลี่ยของชุดข้อมูลที่ได้นำมาทำการคิดคำนวณ

$$\bar{X} = \sum_{i=0}^{N} \frac{X_i}{N} \qquad (2.5)$$

โดย

$\bar{X}$ คือ ค่าเฉลี่ยเลขคณิต

X คือ ค่าตัวแปรที่นำมาคิดค่าเฉลี่ยเลขคณิต

N คือ จำนวนตัวแปรที่นำมาคิดค่าเฉลี่ยเลขคณิต

2.7. ระบบตรวจจับการบุกรุก (Intrusion Detection System, IDS)

ระบบตรวจจับการบุกรุกเป็น ส่วนหนึ่งของการรักษาความปลอดภัยภายในระบบเครือข่ายคอมพิวเตอร์ซึ่งเป็นระบบที่ใช้ในการตรวจจับการใช้งานและความพยายามในการใช้งานคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ซึ่งขัดกับข้อบังคับและเจตจำนงการใช้งาน ซึ่งส่งผลต่อความปลอดภัยของระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ 3 ประการคือ Confidentiality, Integrity และ Availability

ระบบตรวจจับการบุกรุกสามารถเข้ามาช่วยตรวจสอบการละเมิดการใช้งานดังกล่าวได้โดยจะสามารถแจ้งเตือน หรือกระทำเหตุการณ์ที่ผู้ดูแลระบบกำหนดเพื่อป้องกันความเสียหายที่จะเกิดขึ้นดังนี้

- Confidentiality: การป้องกันข้อมูลจากผู้ที่ไม่ได้สิทธิในการเข้าถึง
- Integrity: การป้องกันไม่ให้ผู้ที่ไม่มีสิทธิแก้ไขข้อมูล
- Availability: การป้องกันไม่ให้ผู้ที่ไม่มีสิทธิทำข้อมูลเสียหายจนไม่สามารถให้บริการข้อมูลเหล่านั้นได้และทำให้ผู้ใช้งานที่มีสิทธิ์เข้าถึงข้อมูลได้เมื่อต้องการ

บทที่ 3
การออกแบบและพัฒนา

3.1 บทนำ

การออกแบบและพัฒนาซอฟต์แวร์เป็นขั้นตอนที่วางโครงสร้างของซอฟแวร์ว่าจะมีส่วนประกอบอะไรบ้าง และแต่ละส่วนมีการทำงานอย่างไร และมีขั้นตอนการทำงานอย่างไรโดยมีการใช้เครื่องมือต่างๆ มาช่วยในการพัฒนาโดยมีรายละเอียดดังต่อไปนี้

3.2. การออกแบบซอฟต์แวร์

ระบบตรวจจับการใช้งานเครือข่ายที่ผิดปกติโดยใช้เน็ตเวิร์กโพรไฟล์ มีส่วนประกอบของการทำงานหลักๆ แบ่งเป็น 5 ส่วนหลักดังต่อไปนี้

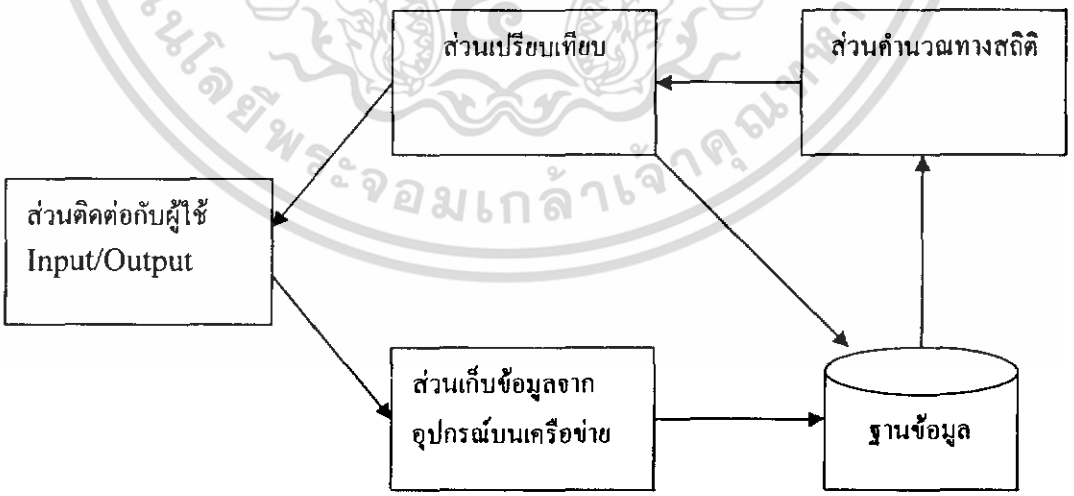
3.2.1. ส่วนเก็บข้อมูลจากอุปกรณ์บนเครือข่าย

3.2.2. ส่วนฐานข้อมูล

3.2.3. ส่วนคำนวณทางสถิติ

3.2.4. ส่วนเปรียบเทียบ

3.2.5. ส่วนติดต่อกับผู้ใช้



รูปที่3.1 ส่วนประกอบของซอฟต์แวร์

3.2.1. ส่วนเก็บข้อมูลจากอุปกรณ์บนเครือข่าย

ส่วนนี้มีการทำงาน โดยไปร้องขอข้อมูลของปริมาณการใช้งานเครือข่าย จากอุปกรณ์ภายในเครือข่าย เช่น เราท์เตอร์ (Router) หรืออีเธอร์เน็ตสวิตช์ (Ethernet Switch) ซึ่งเป็นข้อมูลที่มีเก็บอยู่ในตัวอุปกรณ์เครือข่ายอยู่แล้วโดยใช้โพรโตคอลเอสเอ็นเอ็มพีเพื่อนำข้อมูลเหล่านั้นมาใช้งานในส่วนอื่นๆ โดยในส่วนนี้แบ่งการทำงานเป็น 2 ลักษณะ

3.2.1.1. สร้างชุดข้อมูลการใช้งานในภาวะปกติ

โดยลักษณะนี้เป็นการเก็บข้อมูลเพื่อนำไปสร้างชุดข้อมูลการใช้งานปกติเพื่อใช้ในการใช้เป็นข้อมูลอ้างอิงของการใช้งานในภาวะปกติ

รูปที่ 3.2 โครงสร้างการทำงานของส่วนเก็บข้อมูลทางสถิติ

จากรูปที่ 3.2 โปรแกรมจะทำการร้องขอข้อมูลจากอุปกรณ์เครือข่าย จากนั้นจะมาทำการพักไว้ที่หน่วยความจำ พอถึงช่วงเวลาถัดไป (5 นาที) โปรแกรมก็จะทำการร้องขอข้อมูลจากอุปกรณ์เครือข่ายอีกครั้ง จากนั้นนำมาคำนวณหาผลต่างของปริมาณข้อมูล ก่อนที่จะนำไปเก็บไว้ในฐานข้อมูล วนทำเช่นนี้ไปเรื่อยๆ ที่ต้องทำเช่นนี้เพราะว่าสถิติการใช้งานที่อุปกรณ์เก็บไว้ จะเก็บในรูปแบบตัวเลขนับขึ้นไปเรื่อยๆ โดยมีจุดจำกัดที่ 2^{32} จึงต้องนำมาคิดหาผลต่างเช่นนี้เพื่อป้องกันความผิดพลาดที่อาจเกิดขึ้นถ้าหากนำข้อมูลจากอุปกรณ์ไปใช้งานโดยตรง

โปรแกรมจะนำข้อมูลที่สะสมเก็บไว้นี้ เป็นกลุ่มตัวอย่างในการคำนวณเพื่อเป็นฐานในการนำไปเปรียบเทียบหาความผิดปกติของการใช้งานต่อไป โดยในในขั้นตอนนี้จะยังไม่มีการคำนวณทางสถิติ (โดยระยะเวลาในการเก็บข้อมูลชุดปกติคือ 1 เดือน)

3.2.1.2. การเก็บข้อมูลการใช้งานเครือข่ายเพื่อตรวจสอบการใช้งาน

โดยลักษณะการทำงานนี้เป็นการเก็บข้อมูลการใช้งาน ณ. เวลานั้นเพื่อจะนำไปวิเคราะห์การใช้งานว่ามีลักษณะที่ผิดปกติหรือไม่ โดยค่าที่ทำการเก็บได้จะถูกส่งไปให้กับส่วนการคำนวณเพื่อทำการคำนวณปริมาณการใช้งานต่อไป

3.2.2. ส่วนฐานข้อมูล

เป็นส่วนที่ทำการบันทึกค่าของการใช้งานของระบบเครือข่ายที่อยู่ในสภาวะปกติที่ดึงมาจากอุปกรณ์ภายในเครือข่ายเพื่อเก็บสถิติ และเป็นข้อมูลเพื่อทำการเปรียบเทียบหาความผิดปกติ ที่เกิดขึ้น โดยตัวแปรที่นำมาใช้ แสดงในตารางที่ 3.1 ซึ่งเป็นค่าที่โปรแกรมจะไปดึงมาเก็บในฐานข้อมูลและจะนำมาพิจารณาเพื่อตรวจจับความผิดปกติของปริมาณข้อมูลการใช้ระบบเครือข่าย

ตารางที่ 3.1 ชื่อของตัวแปรและหมายเลข OID

ชื่อของตัวแปร	หมายเลข OID
ifInOctets	1.3.6.1.2.1.2.2.1.10
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11
ifInNUcastPkts	1.3.6.1.2.1.2.2.1.12
ifInDiscards	1.3.6.1.2.1.2.2.1.13
ifOutOctets	1.3.6.1.2.1.2.2.1.16
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17
ifOutNUcastPkts	1.3.6.1.2.1.2.2.1.18
ifOutDiscards	1.3.6.1.2.1.2.2.1.19
etherStatsPkts64Octets	1.3.6.1.2.1.16.1.1.1.14.17
etherStatsPkts65to127Octets	1.3.6.1.2.1.16.1.1.1.15.17
etherStatsPkts128to255Octets	1.3.6.1.2.1.16.1.1.1.16.17
etherStatsPkts256to511Octets	1.3.6.1.2.1.16.1.1.1.17.17
etherStatsPkts512to1023Octets	1.3.6.1.2.1.16.1.1.1.18.17
etherStatsPkts1024to1518Octets	1.3.6.1.2.1.16.1.1.1.19.17

ความหมายของตัวแปรที่โปรแกรมนำมาใช้ในการวิเคราะห์

1. ifInOctets หมายถึง จำนวนข้อมูลในหน่วยไบต์ ที่รับเข้ามาในอินเตอร์เฟสนี้ ข้อมูลนั้นรวมส่วนประกอบของเฟรมด้วย
2. ifInUcastPkts หมายถึง จำนวนของแพ็กเก็ตที่ได้รับมาจากการส่งแบบยูนิคาส (subnetwork-unicast) จากกลุ่มเน็ตเวิร์กย่อยเพื่อถูกส่งต่อไปยังโพรโตคอลชั้นสูงกว่า (higher-layer protocol)

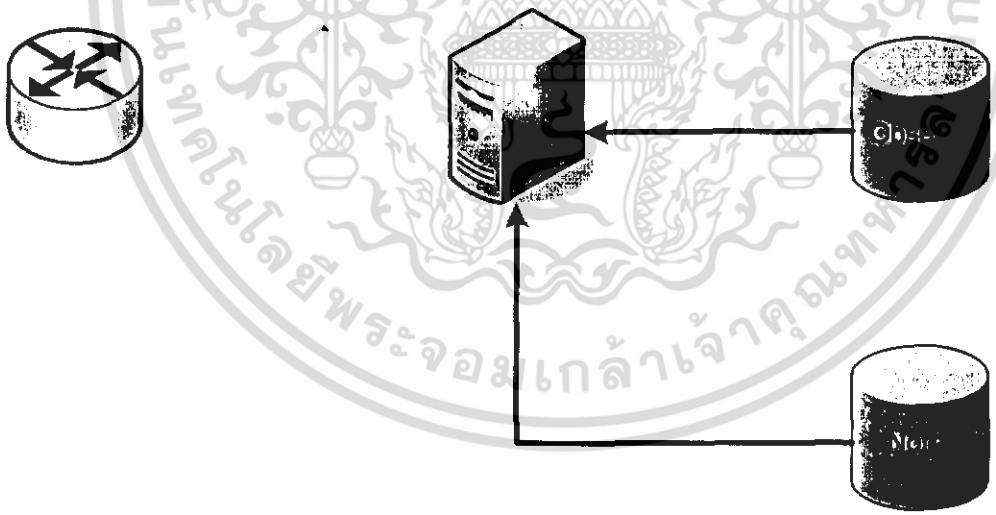
3. ifInNUcastPkts หมายถึง จำนวนแพ็กเก็ตที่ได้รับมาจากการส่งแบบไม่ใช้ยูนิคาส (non-unicast) (เช่น subnetwork-broadcast หรือ subnetwork-multicast)) จากกลุ่มเน็ตเวิร์กย่อยเพื่อถูกส่งต่อไปยังโพรโตคอลชั้นสูงกว่า (higher-layer protocol)
4. ifInDiscards หมายถึง จำนวนของแพ็กเก็ตขาเข้าซึ่งถูกเลือกให้ถูกคัดทิ้งไปถึงแม้ว่าจะไม่เกิดความผิดพลาดใดๆ แต่ทำเพื่อป้องกันความสามารถในการส่งข้อมูลไปยังโพรโตคอลชั้นสูงกว่า(higher-layer protocol) โดยเหตุผลที่ทำการคัดทิ้งแพ็กเก็ตอาจเป็นการทำให้บัฟเฟอร์ของอุปกรณ์ว่างขึ้น
5. ifOutOctets หมายถึง จำนวนข้อมูลในหน่วยไบต์ ที่ส่งออกไปจากอินเตอร์เฟสนี้ ข้อมูลนั้นรวมส่วนประกอบของเฟรมด้วย
6. ifOutUcastPkts หมายถึง จำนวนของแพ็กเก็ตที่โพรโตคอลในชั้นสูงกว่า (higher-layer protocol) ถูกร้องขอให้ส่งออกไปยังเครือข่ายย่อยแบบยูนิคาส (subnetwork-unicast address) (รวมไปถึงแพ็กเก็ตที่ถูกคัดทิ้งหรือไม่ได้ส่งด้วย)
7. ifOutNUcastPkts หมายถึง จำนวนของแพ็กเก็ตที่โพรโตคอลในชั้นสูงกว่า (higher-level protocol) ถูกร้องขอให้ส่งออกไปยังเครือข่ายย่อยโดยไม่ใช้การส่งแบบยูนิคาส (non-unicast address) (เช่น subnetwork-broadcast หรือ subnetwork-multicast) (รวมไปถึงแพ็กเก็ตที่ถูกคัดทิ้งหรือไม่ได้ส่งด้วย)
8. ifOutDiscards หมายถึง จำนวนของแพ็กเก็ตขาออกซึ่งถูกเลือกให้ถูกคัดทิ้งไปถึงแม้ว่าจะไม่เกิดความผิดพลาดใดๆ แต่ทำเพื่อป้องกันความสามารถในการส่งข้อมูลไปยังโพรโตคอลชั้นสูงกว่า(higher-layer protocol) โดยเหตุผลที่ทำการคัดทิ้งแพ็กเก็ตอาจเป็นการทำให้บัฟเฟอร์ของอุปกรณ์ว่างขึ้น
9. etherStatsPkts64Octets หมายถึง จำนวนแพ็กเก็ตทั้งหมดที่ได้รับเข้ามาแล้วมีขนาด 64 อ็อกเต็ต (octet) โดยรับรวมแพ็กเก็ตที่มีข้อผิดพลาดด้วย (ขนาดนั้นนับรวม Frame Check Sequence ด้วยแต่ไม่รวมส่วนของ framing bit)
10. etherStatsPkts65to127Octets หมายถึง จำนวนแพ็กเก็ตทั้งหมดที่ได้รับเข้ามาแล้วมีขนาดระหว่าง 65 ถึง 127 อ็อกเต็ต (octet) โดยรับรวมแพ็กเก็ตที่มีข้อผิดพลาดด้วย (ขนาดนั้นนับรวม Frame Check Sequence ด้วยแต่ไม่รวมส่วนของ framing bit)
11. etherStatsPkts128to255Octets หมายถึง จำนวนแพ็กเก็ตทั้งหมดที่ได้รับเข้ามาแล้วมีขนาดระหว่าง 128 ถึง 255 อ็อกเต็ต (octet) โดยรับรวมแพ็กเก็ตที่มีข้อผิดพลาดด้วย (ขนาดนั้นนับรวม Frame Check Sequence ด้วยแต่ไม่รวมส่วนของ framing bit)
12. etherStatsPkts256to511Octets หมายถึง จำนวนแพ็กเก็ตทั้งหมดที่ได้รับเข้ามาแล้วมีขนาดระหว่าง 256 ถึง 511 อ็อกเต็ต (octet) โดยรับรวมแพ็กเก็ตที่มีข้อผิดพลาดด้วย (ขนาดนั้นนับรวม Frame Check Sequence ด้วยแต่ไม่รวมส่วนของ framing bit)

13. etherStatsPkts512to1023Octets หมายถึง จำนวนแพ็กเก็ตทั้งหมดที่ได้รับเข้ามาแล้วมีขนาดระหว่าง 512 ถึง 1023 อ็อกเต็ต (octet) โดยรับรวมแพ็กเก็ตที่มีข้อผิดพลาดด้วย (ขนาดนั้นนับรวม Frame Check Sequence ด้วยแต่ไม่รวมส่วนของ framing bit)
14. etherStatsPkts1024to1518Octets หมายถึง จำนวนแพ็กเก็ตทั้งหมดที่ได้รับเข้ามาแล้วมีขนาดระหว่าง 1024 ถึง 1518 อ็อกเต็ต (octet) โดยรับรวมแพ็กเก็ตที่มีข้อผิดพลาดด้วย (ขนาดนั้นนับรวม Frame Check Sequence ด้วยแต่ไม่รวมส่วนของ framing bit)

3.2.3. ส่วนคำนวณทางสถิติ (Statistical Computing)

เป็นส่วนที่ทำการคำนวณโดยใช้ทฤษฎีทางสถิติเพื่อหาโพรไฟล์ของการใช้ระบบเครือข่ายในสถานการณ์ปกติเพื่อใช้เปรียบเทียบอ้างอิงกับสถานการณ์ปัจจุบัน เพื่อหาความผิดปกติของการใช้งาน โดยในส่วนการคำนวณนั้นจะทำการคำนวณในแต่ละอินเตอร์เฟสที่มีสถานะพร้อมใช้งาน และแบ่งชุดข้อมูลจากตาราง 3.1 เพื่อจะทำการคำนวณออกเป็น 3 กลุ่มดังนี้

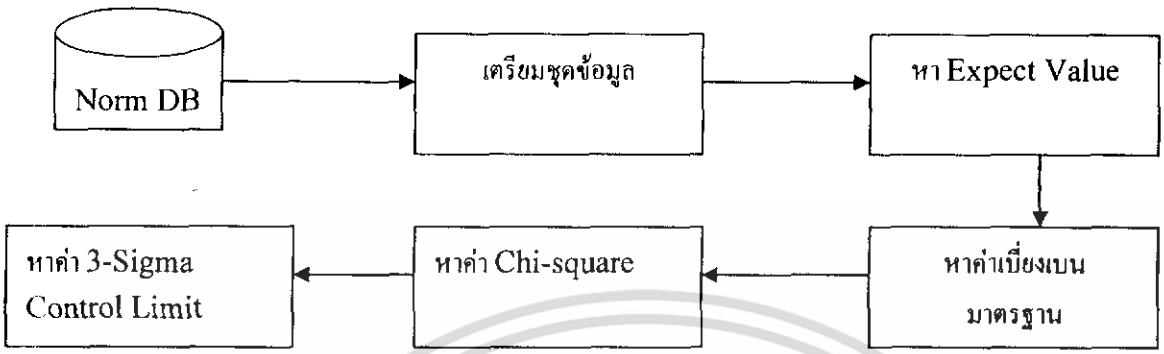
1. กลุ่มข้อมูลขาเข้าของอินเตอร์เฟส (Inbound)
2. กลุ่มข้อมูลขาออกของอินเตอร์เฟส (Outbound)
3. กลุ่มข้อมูลขนาดของแพ็กเก็ต(etherStats packets size)



รูปที่ 3.3 การเรียกข้อมูลจากฐานข้อมูลเพื่อทำการคำนวณ

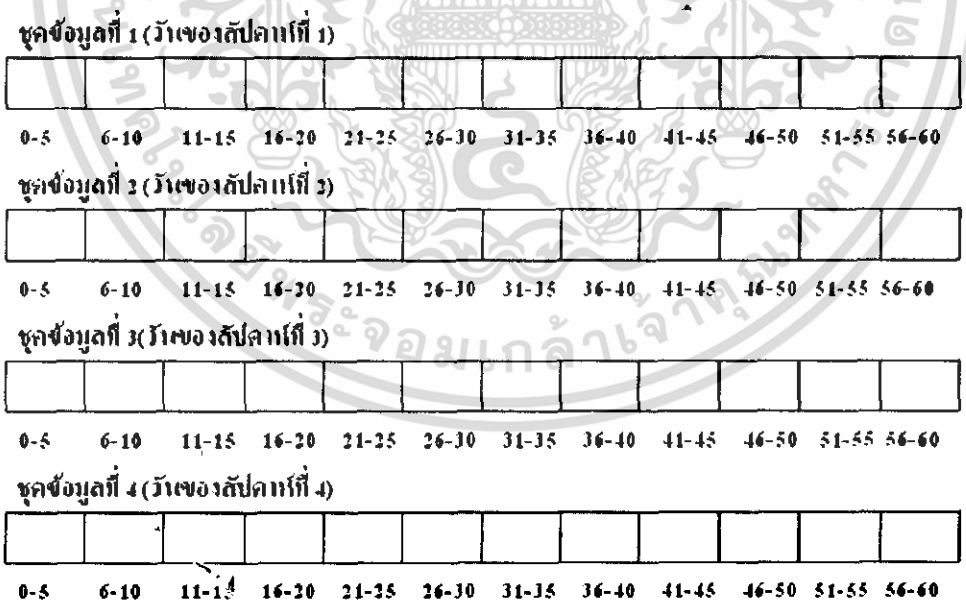
โดยส่วนคำนวณทางสถิตินั้นมีการคำนวณใน 2 ลักษณะดังนี้

3.2.3.1. ส่วนคำนวณเพื่อสร้างขอบเขตการใช้งานภาวะปกติ (การสร้าง Upper Bound)



รูปที่ 3.4 ขั้นตอนการคิดคำนวณค่า Upper bound จากข้อมูลการใช้งานปกติ

เพื่อเป็นค่าขอบบนของการใช้งานเครือข่ายในลักษณะปกติมีขั้นตอนการทำงานดังต่อไปนี้



รูปที่ 3.5 ลักษณะข้อมูลการใช้งานปกติที่ได้ดึงมาจากฐานข้อมูล

1. ดึงข้อมูลการใช้งานเครือข่ายที่มีลักษณะการใช้งานปกติจากฐานข้อมูล (Norm DB) โดยเรียกข้อมูลจากกลุ่มตัวอย่างที่เก็บไว้เป็นฐานในการเปรียบเทียบ ณ วันและเวลาตรงกับวันและเวลาในปัจจุบัน ตลอดจนย้อนหลังไป 1 ชั่วโมง โดยข้อมูลการใช้งานปกติ ที่ทำการดึงมาจากฐานข้อมูลจะมีลักษณะดังรูปที่ 3.5 ซึ่งข้อมูลจะมีทั้งหมด 48 ค่า เนื่องจากโครงงานนี้ใช้ระยะเวลาของข้อมูล 1 เดือนโดยแบ่งเป็น 4 กลุ่มคือชุดข้อมูลละ 12 ค่า (ณ. ชั่วโมงนั้นของวันของแต่ละสัปดาห์)
2. จากนั้นทำการเฉลี่ยปริมาณการใช้งานในแต่ละช่วงเวลา 5 นาที โดยใช้วิธีการคำนวนค่าเฉลี่ยเลขคณิต ก็จะได้ผลลัพธ์เหลือเป็นข้อมูล 1 ชุดดังรูปที่ 3.6

รูปที่ 3.6 ข้อมูลที่ถูกทำการเฉลี่ยแล้ว

3. นำผลลัพธ์ที่ได้จากข้อ 2 มาคำนวณโดยใช้ทฤษฎี EWMA โดยที่การคำนวณ EWMA นั้นผลลัพธ์ที่ได้ เป็นข้อมูลที่มีการถ่วงน้ำหนักด้วยค่าข้อมูลในช่วงเวลาก่อนหน้าที่ผ่านๆ มา เพื่อที่จะสามารถเปรียบเทียบข้อมูลที่ผ่านมาแล้วกับค่าปริมาณการใช้งานในปัจจุบันมีแนวโน้มอย่างไร โดย EWMA คำนวณโดยใช้สมการ ดังสมการ
$X_{i(t)} = \lambda * X + (1- \lambda) * X_{(t-1)}$ โดยกำหนดให้ค่า X ซึ่งจะนำไปถ่วงน้ำหนักกับค่า ณ เวลาปัจจุบัน ให้เท่ากับ 1/12 และกำหนดให้ค่า $X_{(t-1)}$ ซึ่งจะนำไปถ่วงน้ำหนักกับค่าของการใช้งานก่อนหน้าให้เท่ากับ 11/12 ที่ทำการกำหนดค่าทั้งสองให้เป็นเช่นนี้เพราะชุดข้อมูลที่นำเข้ามาใช้ในการเปรียบเทียบมีจำนวน 12 ตัว โดยผลลัพธ์ที่ได้จะมีจำนวนข้อมูล 11 ค่า (เพราะการคำนวณ EWMA) จากนั้นทำการ ถ่วงค่าโดยหาค่าที่มากที่สุด และนำไปหารและคูณด้วย 100 เพื่อทำเป็นเปอร์เซ็นต์ว่าค่านั้นมีการเปลี่ยนแปลงเป็นเปอร์เซ็นต์เท่าไหร่
4. นำข้อมูลที่ได้ข้อ 3 ในแต่ละตัวแปรมาทำการรวมเป็นเวกเตอร์ของกลุ่มชุดข้อมูลที่ทำการคำนวณ (โดยโครงงานนี้มีการแบ่งตัวแปรเป็น 3 กลุ่ม คือ Inbound, Outbound และ Etherstats) ด้วยสูตร $V_{(i)} = \sqrt{A^2_{(i)} + B^2_{(i)} + C^2_{(i)} + D^2_{(i)}}$ ... ก็จะได้ ชุดข้อมูล มา 3 กลุ่ม

5. นำเอาผลลัพธ์ที่ได้จากข้อที่ 4 มาทำการคำนวณเพื่อหาค่าเบี่ยงเบนมาตรฐานเพื่อจะนำไปใช้หาค่า 3 – Sigma Control Limit ต่อไป
6. เอาผลลัพธ์ที่ได้จากข้อที่ 4 มาทำการคิดค่า Chi-square เพื่อจะนำไปใช้หาค่า 3 – Sigma Control Limit ต่อไป
7. เอาผลลัพธ์ที่ได้จากข้อที่ 4 มาทำการคิดค่า Expect Value โดยใช้วิธี EWMA และนำค่าสุดท้ายของการคำนวณมาเป็น Expect Value เพื่อจะนำไปใช้หาค่า 3 – Sigma Control Limit ต่อไป
8. นำค่าผลลัพธ์ที่ได้จากข้อที่ 5 , 6 และ 7 มาทำการหาคำนวณ 3-Sigma Control Limit
9. ได้ผลลัพธ์ เป็น ค่า upper bound

3.2.3.2. ส่วนคำนวณเพื่อตรวจสอบความผิดปกติ

รูปที่ 3.7 ขั้นตอนการคิดคำนวณค่าของการใช้งานเครือข่าย ณ เวลา ใดๆ

1. ดึงข้อมูลการใช้งานเครือข่ายจากฐานข้อมูล (Observe DB) โดยเรียกข้อมูลปริมาณการใช้งานเครือข่ายตั้งแต่ปัจจุบันย้อนหลังไป 1 ชั่วโมง จากนั้นทำการคำนวณ EWMA ของแต่ละตัวแปร โดยที่การคำนวณ EWMA นั้นผลลัพธ์ที่ได้ เป็นข้อมูลที่มีการถ่วงน้ำหนักด้วยค่าข้อมูลในช่วงเวลาก่อนหน้าที่ผ่านๆมา เพื่อที่จะสามารถเปรียบเทียบข้อมูลที่ผ่านมาแล้วกับค่าปริมาณการใช้งานในปัจจุบันมีแนวโน้มอย่างไร โดย EWMA คำนวณโดยใช้สมการ ดังนี้โดย EWMA คำนวณโดยใช้สมการ ดังสมการ

   $X_{i(i)} = \lambda * X + (1-\lambda) * X_{(i-1)}$ โดยกำหนดให้ค่า X ซึ่งจะนำไปถ่วงน้ำหนักกับค่า ณ เวลาปัจจุบัน ให้เท่ากับ 1/12 และกำหนดให้ค่า $X_{(i-1)}$ ซึ่งจะนำไปถ่วงน้ำหนักกับค่าของการใช้งานก่อนหน้าให้เท่ากับ 11/12 ที่ทำการกำหนดค่าทั้งสองให้เป็นเช่นนี้เพราะชุดข้อมูลที่นำเข้ามาใช้ในการเปรียบเทียบมีจำนวน 12 ตัว
2. นำข้อมูลที่ได้ข้อ 1 ในแต่ละตัวแปรมาทำการรวมเป็นเวกเตอร์ของกลุ่มชุดข้อมูลที่ทำการคำนวณ (โดยโครงงานนี้มีการแบ่งตัวแปรเป็น 3 กลุ่ม คือ Inbound, Outbound และ Etherstat) ด้วยสูตร $V_{(i)} = \sqrt{A^2_{(i)} + B^2_{(i)} + C^2_{(i)} + D^2_{(i)}}$ ... ก็จะได้ ชุดข้อมูล มา 3 กลุ่ม

3. ได้ผลลัพธ์ที่ได้จากข้อ 2 และนำค่า Expect Value มาจากชุดข้อมูลการใช้งานปกติเพื่อทำการคำนวณโดยใช้ Chi-Square ของการใช้งานเครือข่าย ณ เวลาที่สังเกต
4. ได้ผลลัพธ์ เป็น ค่า Chi-Square ของชุดข้อมูลปกติ

3.2.4. ส่วนการเปรียบเทียบ

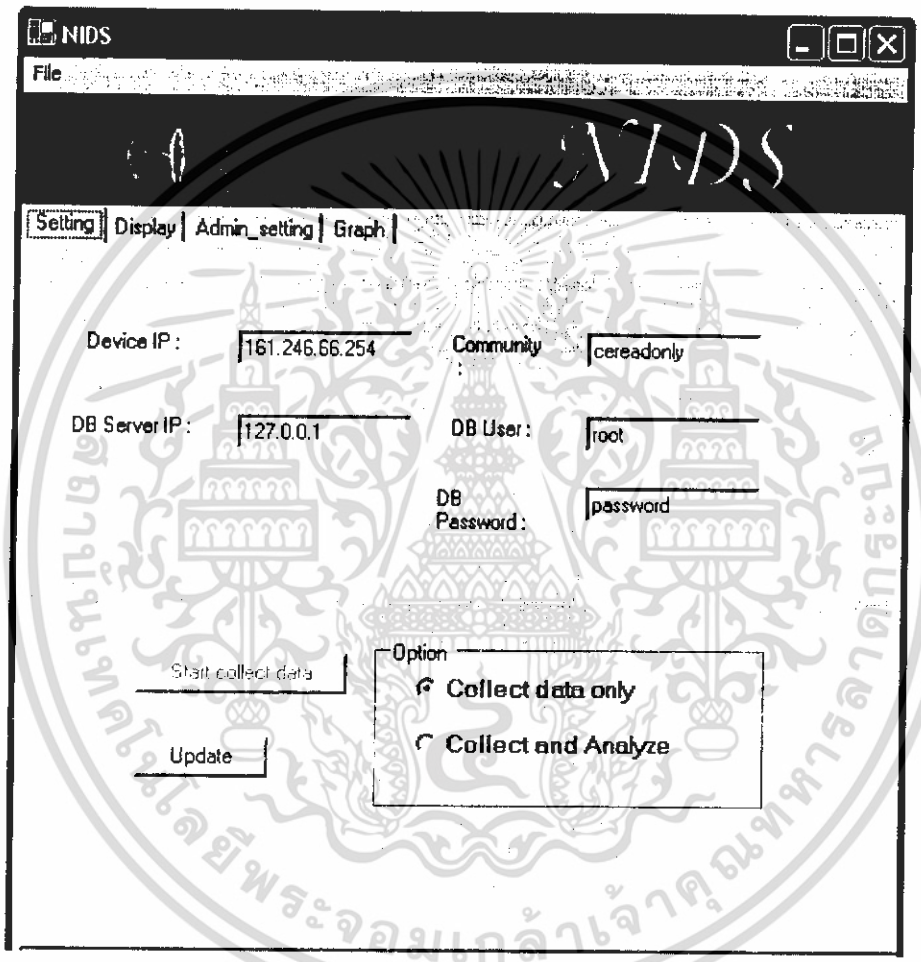
ในส่วนนี้เป็นการนำเอาผลลัพธ์จากส่วนการคำนวณทั้งค่าขอบเขตการใช้งานเครือข่ายในลักษณะที่เป็นปกติและค่าการใช้งานเครือข่ายในปัจจุบันนำมาเปรียบเทียบกัน โดยเมื่อเปรียบเทียบแล้วผลที่ได้แบ่งเป็น 2 กรณี

- มีการใช้งานเครือข่ายที่เป็นปกติ (Chi –Square ณ ปัจจุบัน < Upper bound) ระบบจะมีการนำข้อมูลการใช้งาน ณ. เวลานั้นไปทำการเก็บลงในฐานข้อมูลในส่วนของชุดข้อมูลการใช้งานปกติ (norm profile) เพื่อทำให้ชุดข้อมูลการใช้งานปกติมีความทันสมัยกับการใช้งานในเครือข่ายอยู่เสมอ
- มีการใช้งานเครือข่ายที่ผิดปกติ (Chi –Square ณ ปัจจุบัน > Upper bound) ระบบจะทำการแจ้งเตือนไปยังผู้ดูแลระบบผ่านทางส่วนติดต่อกับผู้ใช้งาน โดยระบบจะไม่มีการเก็บข้อมูล ณ. เวลานั้นที่เกิดความผิดปกติลงฐานข้อมูลในชุดข้อมูลที่เป็นปกติ (norm profile)

3.2.5. ส่วนติดต่อกับผู้ใช้

เป็นส่วนแสดงผลกับผู้ใช้งานโปรแกรม เพื่อแจ้งเตือนเมื่อเกิดเหตุการณ์ผิดปกติจากการใช้งานเครือข่าย รวมถึงแสดงสถิติการใช้งานของอุปกรณ์บนเครือข่ายโดยมีหน้าของโปรแกรมดังต่อไปนี้

3.2.5.1. ในหน้า Setting มีดังต่อไปนี้



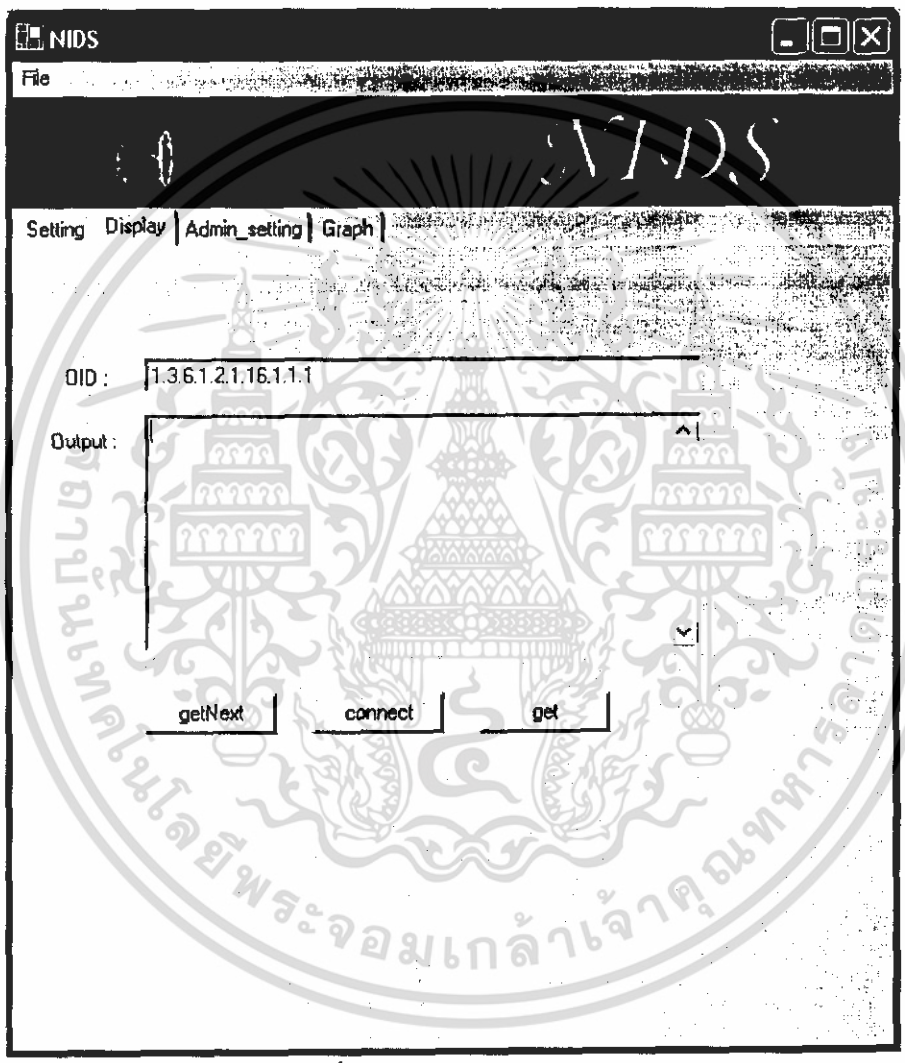
รูป 3.8 หน้า setting ของโปรแกรม

Input

- หมายเลข IP ของอุปกรณ์เครือข่ายที่จะทำการดึงข้อมูล
- รหัสคอมมูนิตี้ของอุปกรณ์เครือข่าย
- หมายเลข IP ของเครื่องฐานข้อมูล

- User name ของ ฐานข้อมูล
- Password ของฐานข้อมูล

3.2.5.2. ในหน้า Display มีดังต่อไปนี้



รูปที่ 3.9 หน้า Display ของโปรแกรม

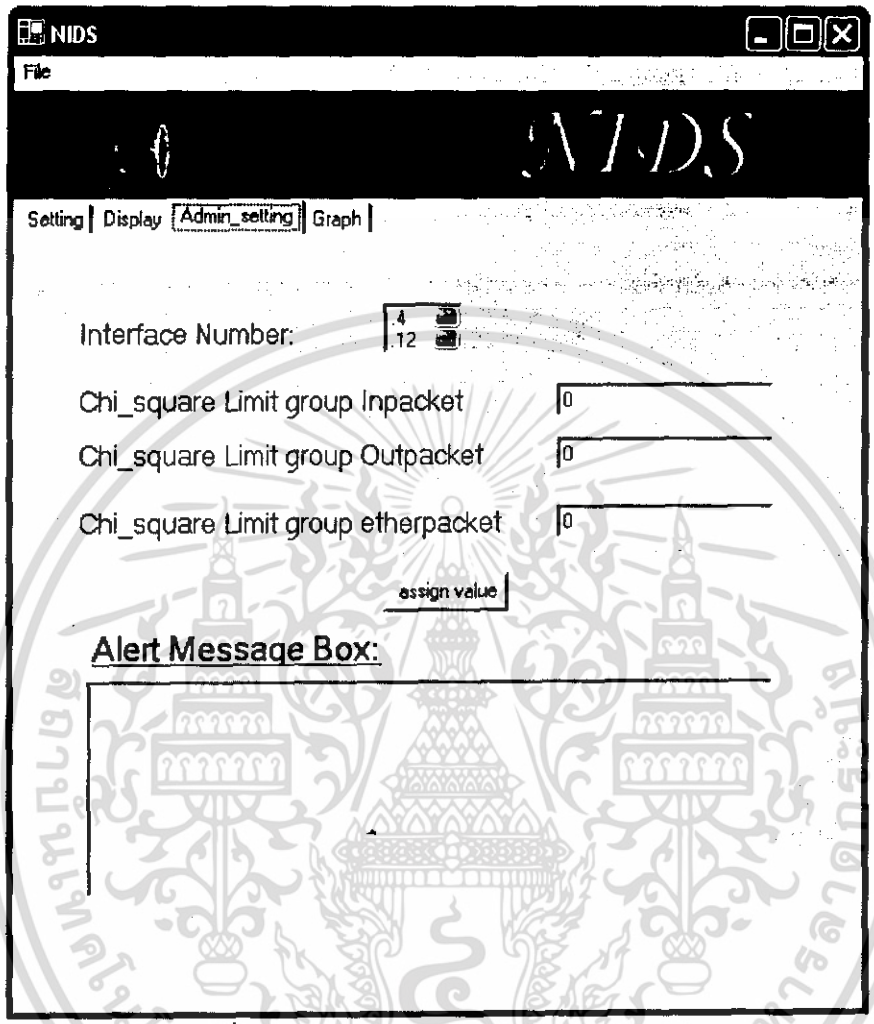
Input

- มีเลข OID ที่ต้องการให้โปรแกรมไปดึงข้อมูลมาแสดง

Output

- แสดงข้อมูลต่างๆ ที่มีอยู่ในตัวอุปกรณ์ตามค่า OID ที่ผู้ใช้ใส่เข้ามา

3.2.5.3. หน้า Admin setting มีดังต่อไปนี้



รูปที่ 3.10 หน้า Admin setting ของโปรแกรม

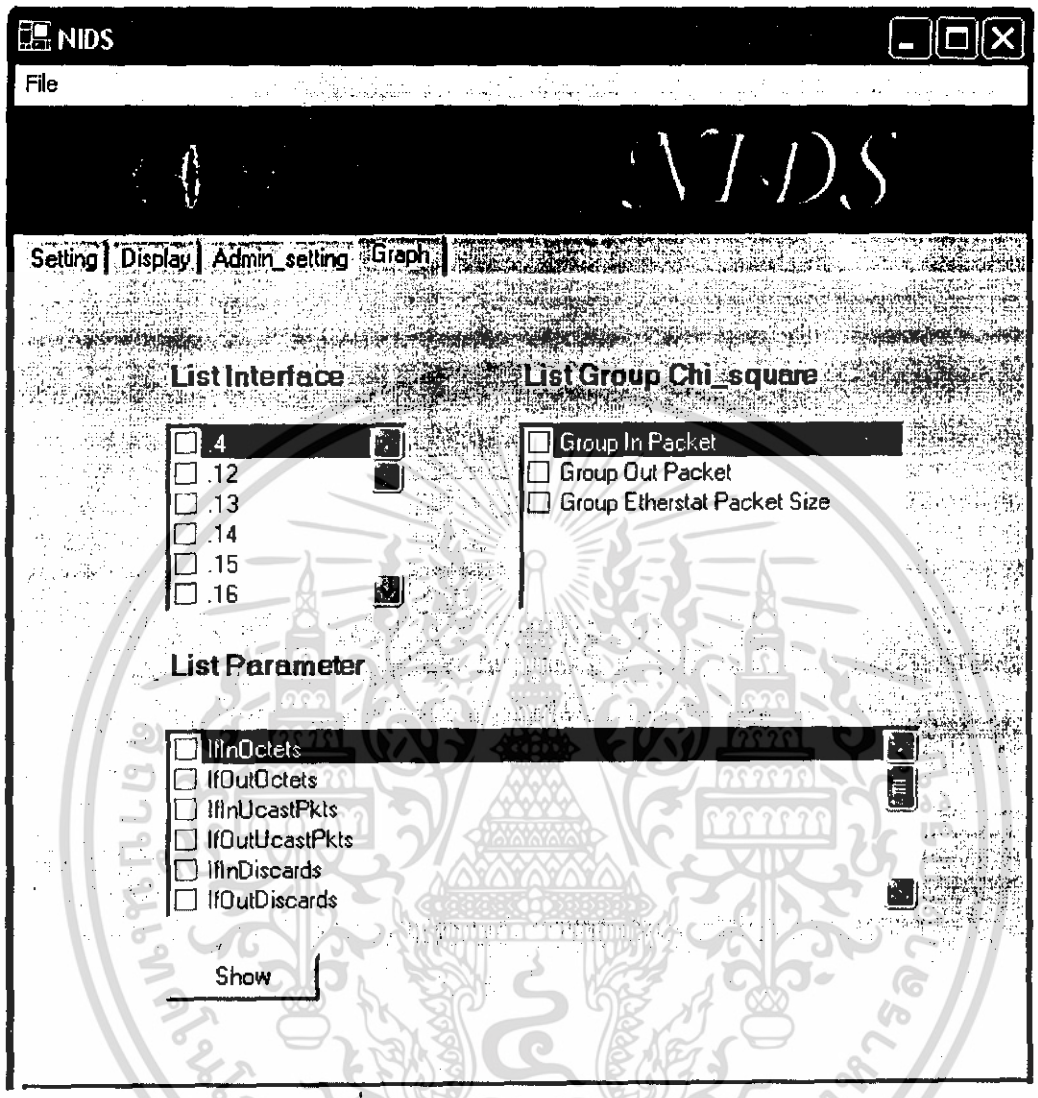
Input

- ค่า upper bound ที่ผู้ดูแลระบบสามารถยอมรับได้ของกลุ่มการใช้งานขาเข้าแต่ละอินเตอร์เฟส
- ค่า upper bound ที่ผู้ดูแลระบบสามารถยอมรับได้ของกลุ่มการใช้งานขาออกแต่ละอินเตอร์เฟส
- ค่า upper bound ที่ผู้ดูแลระบบสามารถยอมรับได้ของกลุ่มขนาดของแพ็กเก็ตแต่ละอินเตอร์เฟส

Output

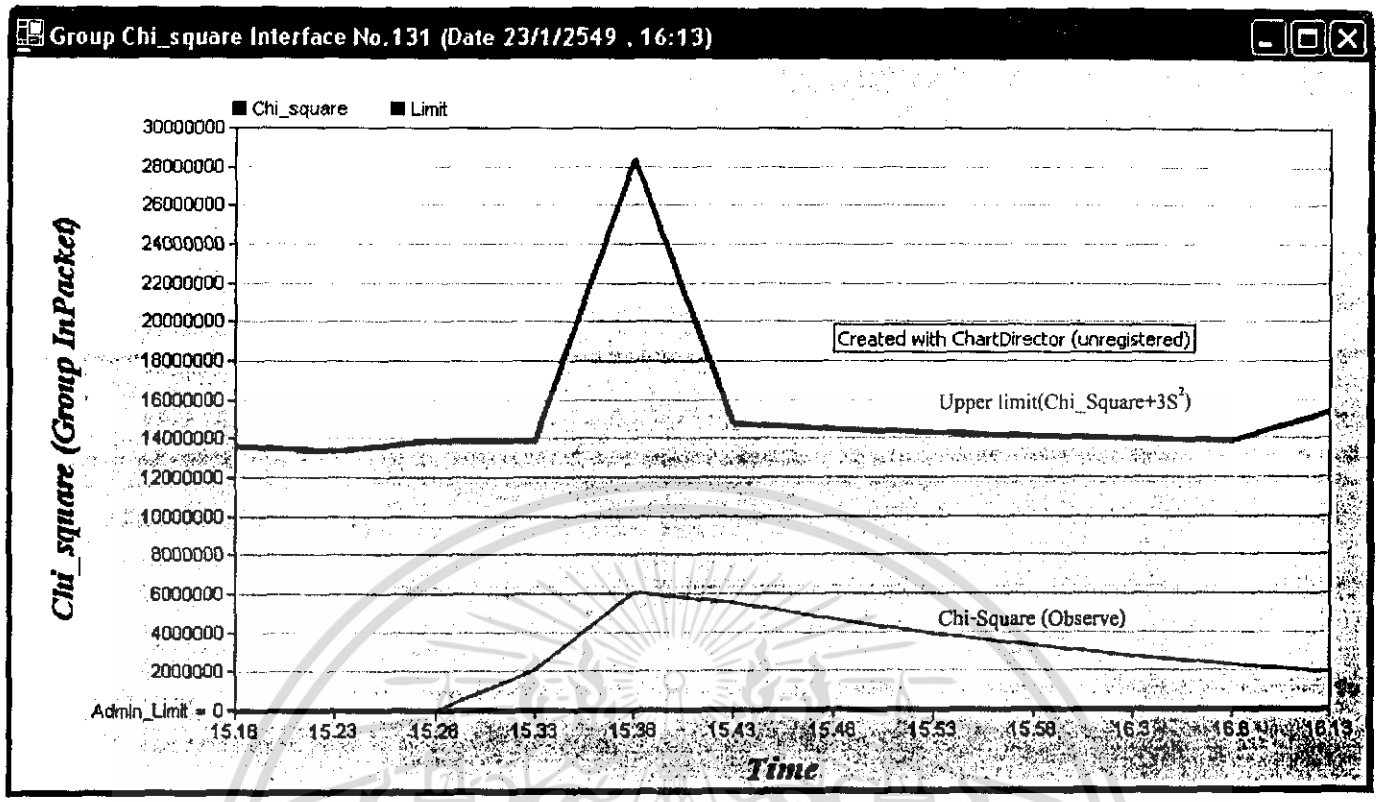
- ข้อความแจ้งเตือนความผิดปกติ

3.5.2.4. หน้า Graph มีดังต่อไปนี้

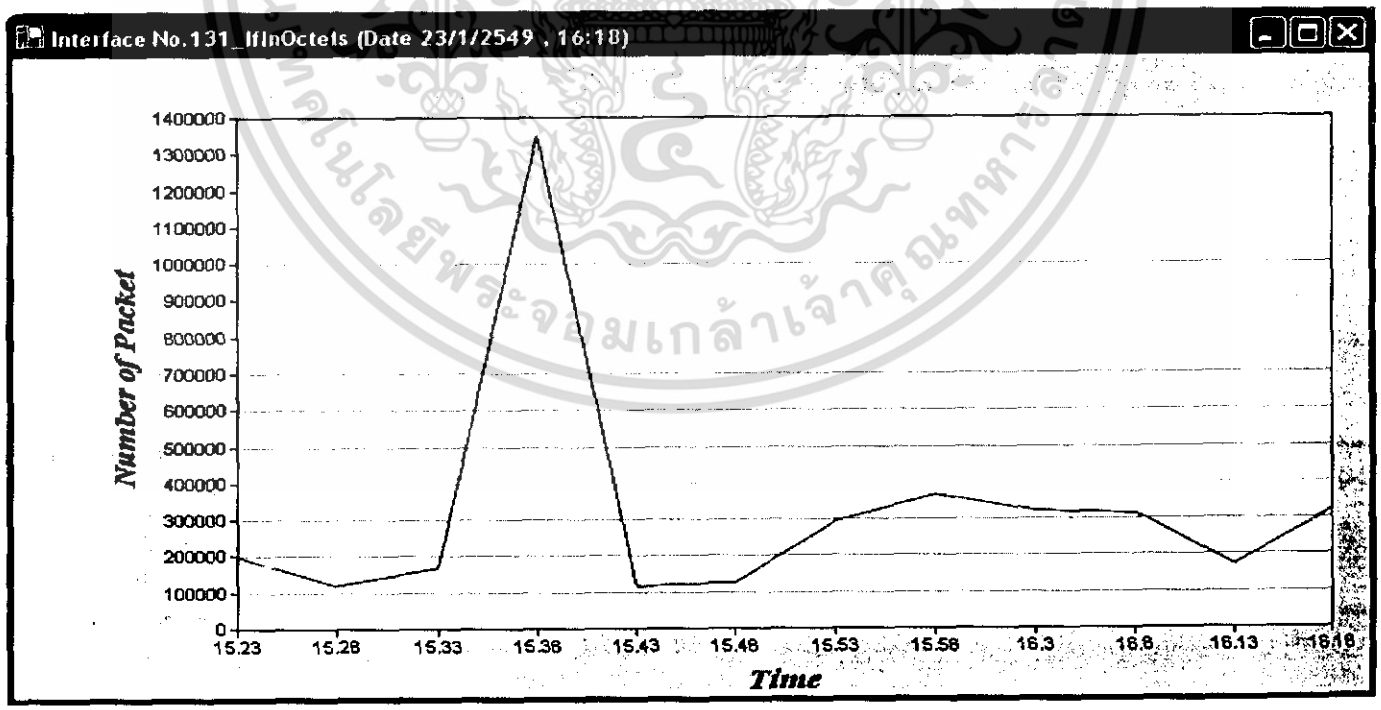


รูปที่ 3.11 หน้า Graph ของโปรแกรม

โดยส่วนนี้เป็นส่วนที่ระบบแสดงผลของระบบให้กับผู้ใช้งานได้รับรู้รับทราบถึงข้อมูลต่างๆ ที่เกิดขึ้น



รูปที่ 3.12 ตัวอย่างกราฟแสดงค่าของ Chi_square ในกลุ่มขาเข้าอินเตอร์เฟส *131*



รูปที่ 3.13 ตัวอย่างกราฟแสดงปริมาณการใช้งานของตัวแปร ifInOctets อินเตอร์เฟส 131

3.3. เครื่องมือที่ใช้ในการพัฒนา

3.3.1. Microsoft Visual Studio .NET 2003 (C#)

3.3.2. Library SNMP++

3.3.3. Microsoft Windows XP

3.3.4. Chartdirector Tool

3.3.5. MySQL Server

3.3.6. MySQL-Administrator

3.3.7. MySQL-Query-browser

บทที่ 4
การทำงานของโปรแกรม

ลักษณะในการทำงานของระบบนั้นมีอยู่ 2 รูปแบบ

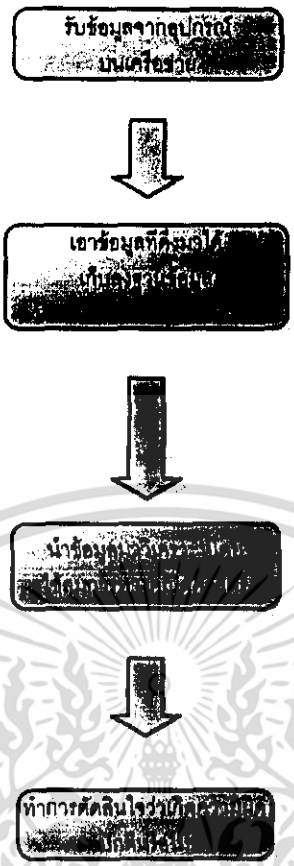
4.1. การทำงานในขณะเริ่มต้นการทำงานของระบบ(ยังไม่มี Norm Profile)

เริ่มแรกต้องมีการเตรียมระบบเพื่อสร้าง Norm Profile (ทำตอนเริ่มระบบครั้งแรกเท่านั้น) มีการรับข้อมูลแล้วเก็บลงฐานข้อมูลในส่วนของ Norm Profile Database (โดยในส่วนการสร้าง Norm Profile นี้ ต้องสร้างในเวลาการใช้งานที่ทำการตั้งสมมติฐานว่าระบบมีการใช้งานที่มีความปกติ) เพื่อให้ได้ช่วงข้อมูลมากพอตามที่ต้องการ (ในโครงงานนี้ใช้ 1 เดือนเป็นอย่างน้อย) เพื่อใช้เป็นข้อมูลเพื่อใช้ในการสร้าง Upper bound limit

รูปที่ 4.1 การทำงานของโปรแกรมขณะอยู่ในภาวะเริ่มต้น

4.2. การทำงานในขณะทำการวิเคราะห์ความผิดปกติ(กรณีที่มี Norm Profile)

ทำการร้องขอข้อมูลของปริมาณข้อมูลการใช้งานเครือข่ายจากอุปกรณ์บนเครือข่ายมาทำการเก็บไว้ที่ฐานข้อมูลเพื่อนำข้อมูลมาวิเคราะห์โดยใช้สมการทางคณิตศาสตร์ จากนั้นนำข้อมูลไปวิเคราะห์เพื่อหาความผิดปกติของปริมาณข้อมูลการใช้งานเครือข่ายโดยมีขั้นตอนการทำงานย่อยต่างๆ ดังรูปที่ 4.2



รูปที่ 4.2 การทำงานของโปรแกรมขณะทำการวิเคราะห์ความผิดปกติ

4.2.1. รับข้อมูลจากอุปกรณ์บนเครือข่าย

ในส่วนนี้โปรแกรมจะทำการติดต่อกับโดยใช้โพรโตคอลเอสเอ็นเอ็มพีเพื่อร้องขอข้อมูลที่โปรแกรมต้องการจากอุปกรณ์เครือข่ายโดยส่วนนี้จะทำการร้องขอข้อมูลจากอุปกรณ์บนเครือข่ายทุก ๆ 5 นาทีจากนั้นนำข้อมูลที่ได้มาคิดค่าปริมาณการใช้งานที่เกิดขึ้นในช่วง 5 นาทีที่ผ่านมา

4.2.2. นำข้อมูลที่ได้มาเก็บลงฐานข้อมูล

ในส่วนนี้โปรแกรมจะทำการนำข้อมูลที่ได้มาจากขั้นตอนที่ผ่านมาทำการเก็บลงฐานข้อมูลทุกๆ ตัวแปรที่ได้มาในแต่ละอินเตอร์เฟส เพื่อใช้เป็นข้อมูลในการนำไปคำนวณทางคณิตศาสตร์

4.2.3. นำข้อมูลมาวิเคราะห์โดยใช้สมการทางคณิตศาสตร์

ในส่วนนี้โปรแกรมจะทำการนำข้อมูลชุดการใช้งานปกติจากฐานข้อมูลที่ได้เก็บไว้ เพื่อคำนวณ Upper bound ข้อมูลการใช้งานโดยมีขั้นตอนการทำงานต่างๆ ดังในรูปที่ 3.4 และคำนวณ Chi-square การใช้งานปัจจุบันเพื่อส่งข้อมูลทั้ง 2 นำไปเปรียบเทียบการใช้งานระหว่างค่า Chi-square ที่เวลาที่ ณ ปัจจุบันและค่า Upper bound ของชุดข้อมูลการใช้งานปกติ ดังรูปที่ 3.5

4.2.4. การตัดสินใจว่ามีความผิดปกติของการปริมาณข้อมูลของการใช้งานเครือข่าย

ทำการเปรียบเทียบค่า ของ Chi –Square ของเครือข่าย ณ เวลาปัจจุบัน กับ Upper bound เพื่อทำการตัดสินใจว่าจะทำการแจ้งเตือนไปยังผู้ดูแลระบบหรือไม่

1. ถ้าเกิดความผิดปกติ (Chi –Square ณ ปัจจุบัน > Upper bound) จะ ทำการแจ้งเตือนไปยังผู้ดูแลระบบ และไม่ทำการ Update ข้อมูลนั้นเข้าสู่ Norm Profile Table
2. ถ้าไม่เกิดความผิดปกติ (Chi –Square ณ ปัจจุบัน < Upper bound) จะไม่ทำการแจ้งเตือนไปยังผู้ดูแลระบบ และทำการ Update ข้อมูลนั้นเข้าสู่ Norm Profile Table

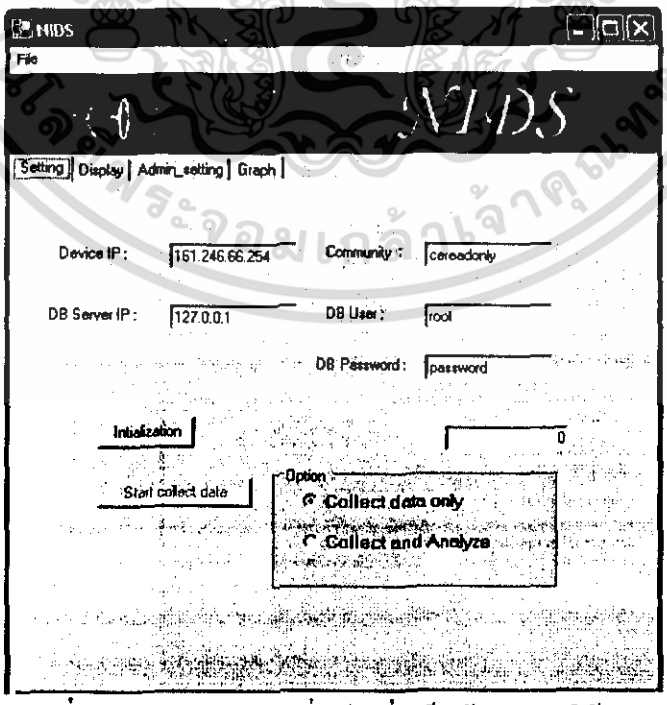
บทที่ 5
ผลการทดลอง

เป็นการแสดงขั้นตอนการใช้งานของโปรแกรมในส่วนต่างๆ โดยแบ่งเป็นการทำงานของการในส่วนของการเริ่มต้นระบบด้วยการสร้างฐานข้อมูล , การวิเคราะห์ , การตั้งค่าการใช้งานของผู้ใช้งาน และการเรียกดูปริมาณการใช้งานในรูปแบบกราฟ

5.1. ระบบเครือข่ายคอมพิวเตอร์ที่ใช้ทดสอบ

ระบบเครือข่ายคอมพิวเตอร์ที่ใช้ทดสอบคือระบบเครือข่ายของภาควิชาคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง โดยทำการปรับตั้งค่าที่โปรแกรมเพื่อให้ทำการติดต่อไปยังอุปกรณ์สวิตซ์หลักของเครือข่ายแล้วทำการร้องขอข้อมูลปริมาณการใช้งานเครือข่ายที่อุปกรณ์ โดยในช่วงแรกของการทำงานโปรแกรมนั้น จะต้องทำการเก็บข้อมูลเพื่อเป็นโพรไฟล์ ซึ่งโพรไฟล์นั้นทำการเก็บสะสมไว้ในฐานข้อมูลในเครื่องเดียวกันกับเครื่องที่รันโปรแกรม จากนั้นเมื่อมีโพรไฟล์มากพอโปรแกรมจะนำข้อมูลที่ร้องขอมาจากอุปกรณ์เพื่อวิเคราะห์ปริมาณการใช้งานเครือข่ายจริงนั้น แล้วแสดงผลการทำงานในรูปแบบกราฟ

5.2. การทำงานงานโปรแกรมในหน้า Setting

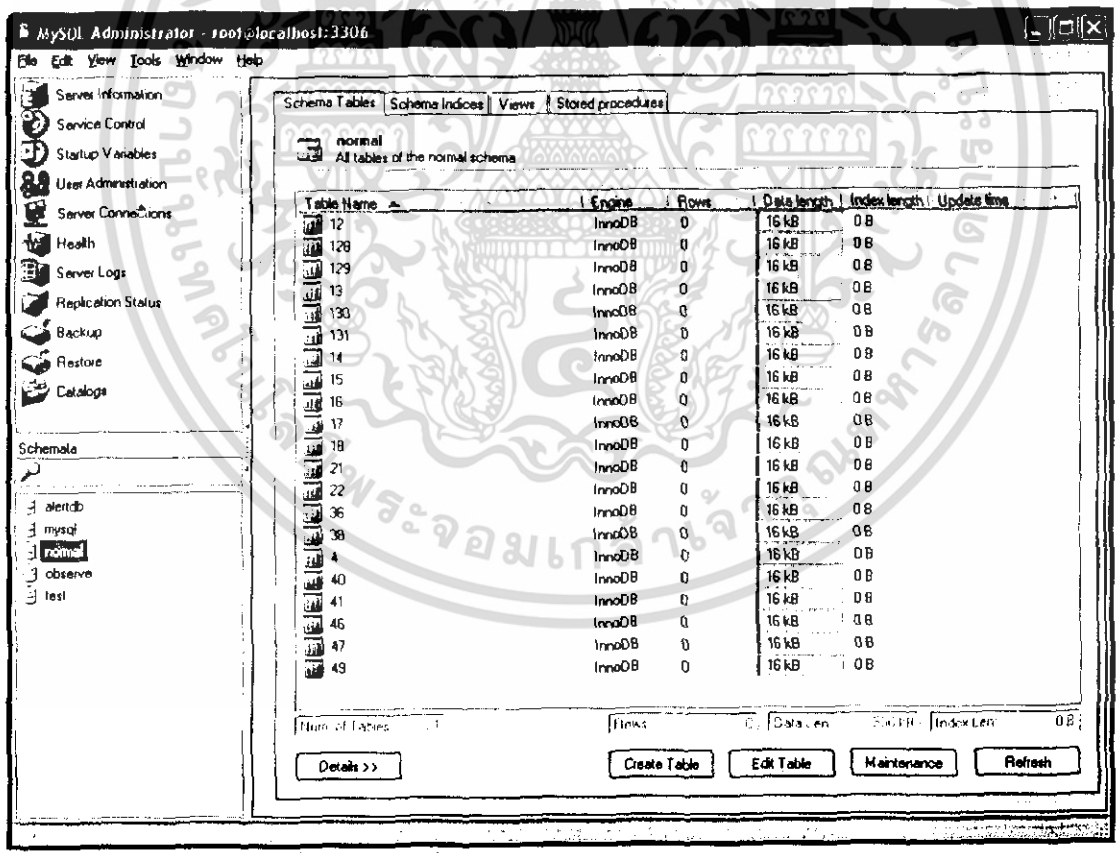


รูปที่ 5.1 โปรแกรมขณะเริ่มต้นเพื่อเก็บข้อมูลการใช้งาน

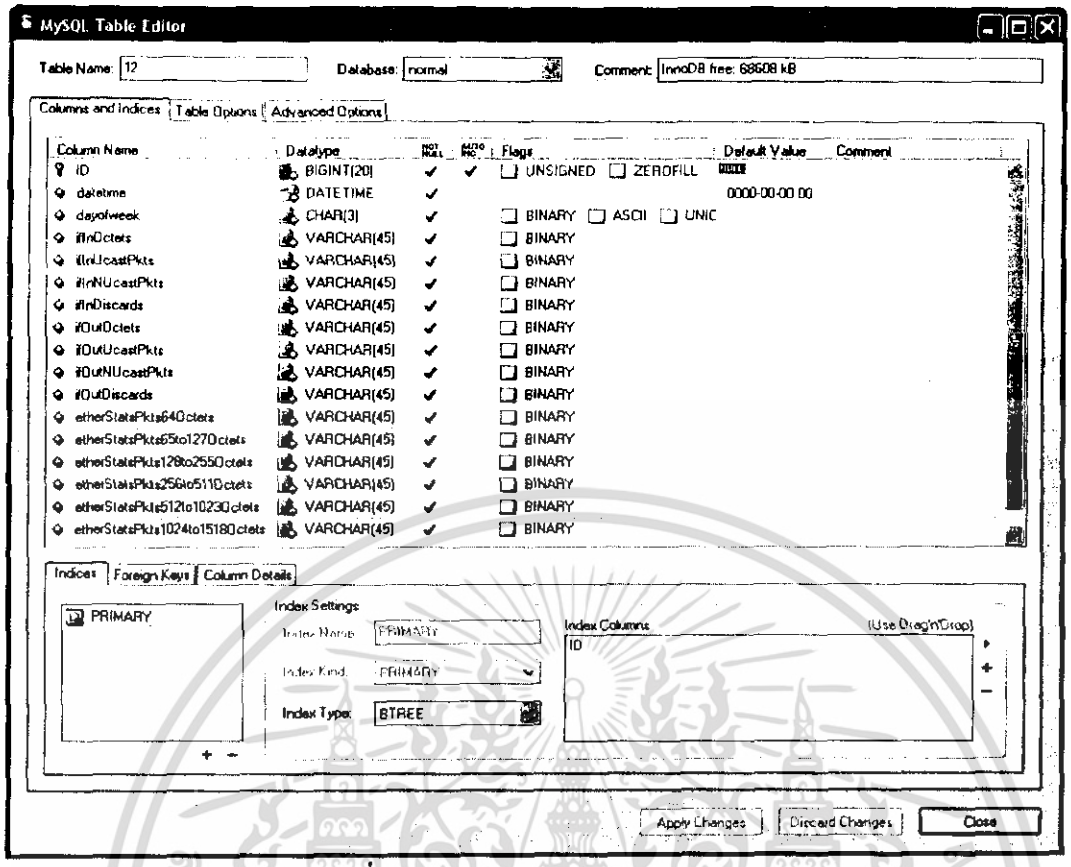
โดยเมื่อเริ่มรันโปรแกรมแล้วจะมีโปรแกรมขึ้นมาดังรูปที่ 5.1 ซึ่งจะมีข้อมูลให้ผู้ใช้งานป้อนข้อมูลดังต่อไปนี้

- Device IP คือ หมายเลข IP Address ของอุปกรณ์เครือข่ายที่จะทำการดึงข้อมูล
- Community คือ ค่าคอมมูนิตี้เพื่ออ่านข้อมูลจากอุปกรณ์เครือข่าย
- IP DB Server คือ หมายเลข IP Address ของเครื่องที่เป็นฐานข้อมูล
- DB User คือ ชื่อ User ของโปรแกรมจัดการฐานข้อมูล
- DB Password คือ Password ของโปรแกรมจัดการฐานข้อมูล

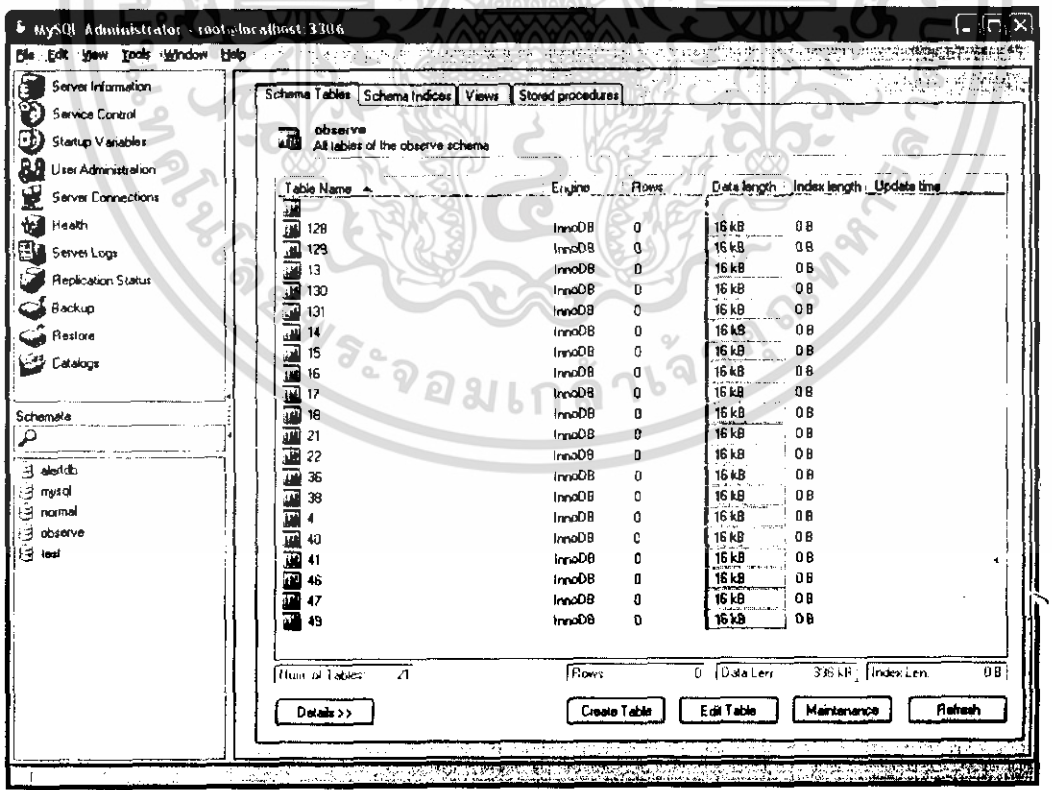
หลังจากป้อนเสร็จแล้วจะมีปุ่มให้กด (ซึ่งถ้าเป็นการใช้งานครั้งแรก)ซึ่งถ้ายังไม่มีการใช้งานมาก่อนจะมีปุ่ม initialization ซึ่งเมื่อกดปุ่ม initialization แล้วโปรแกรมจะเข้าไปทำการดึงข้อมูลว่ามีอินเตอร์เฟสใดบ้างที่เปิดใช้งานอยู่และสร้างตารางในฐานข้อมูลให้อย่างอัตโนมัติโดยมีชื่อ Schema ว่า normal, observe และ alertdb ซึ่งมีข้อมูลในแต่ละตารางดังรูปที่ 5.2, 5.4 และ 5.6 ตามลำดับ



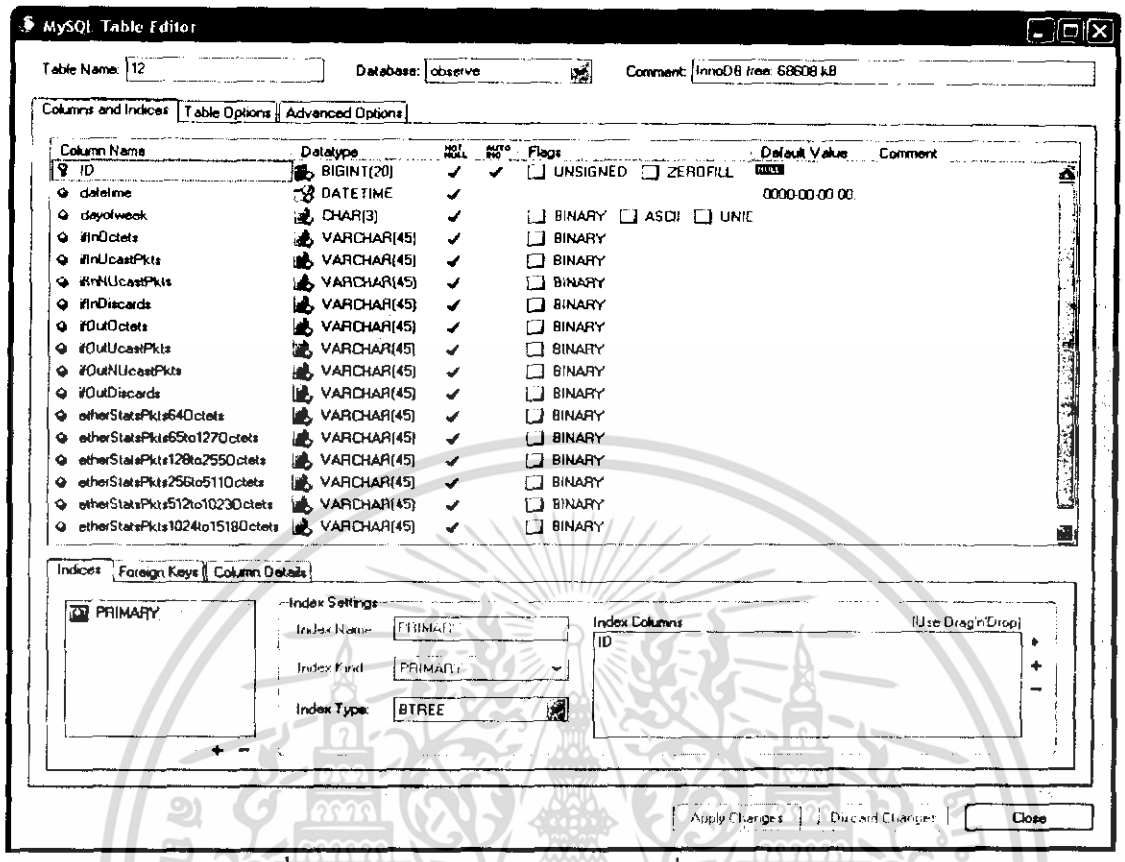
รูปที่ 5.2 ตารางที่อยู่ใน Schema normal (ชุดข้อมูลปกติ)



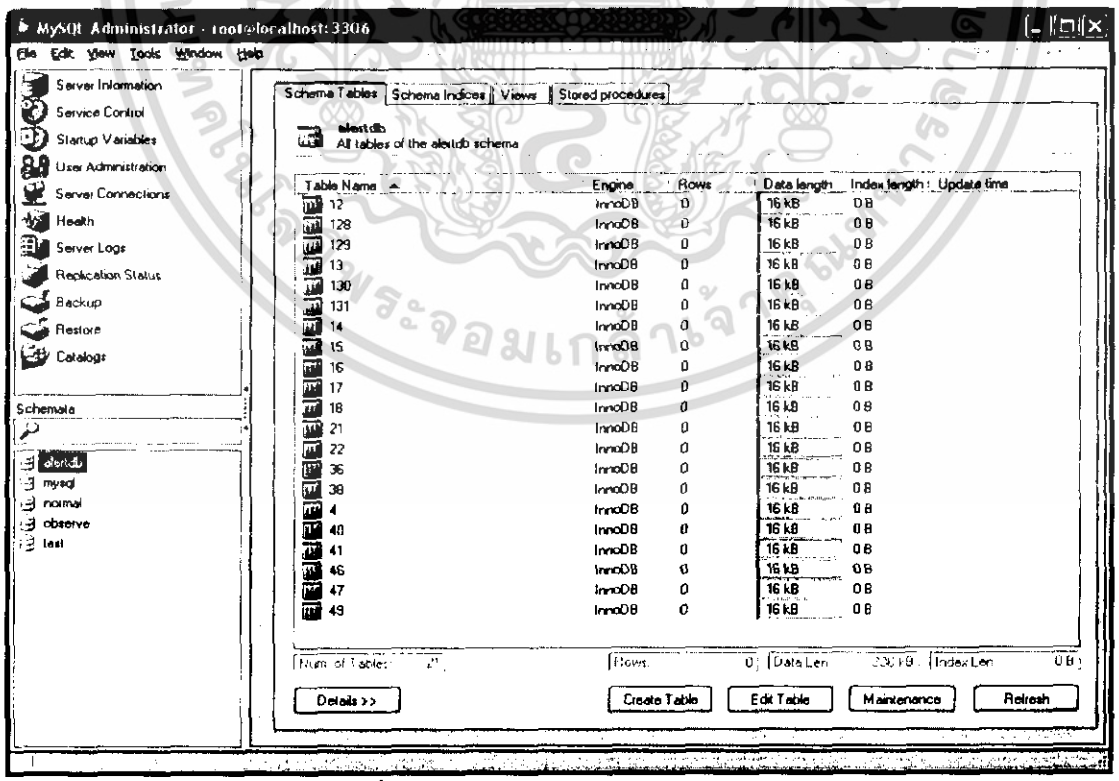
รูปที่ 5.3 ข้อมูลในตารางของชุดข้อมูลปกติ



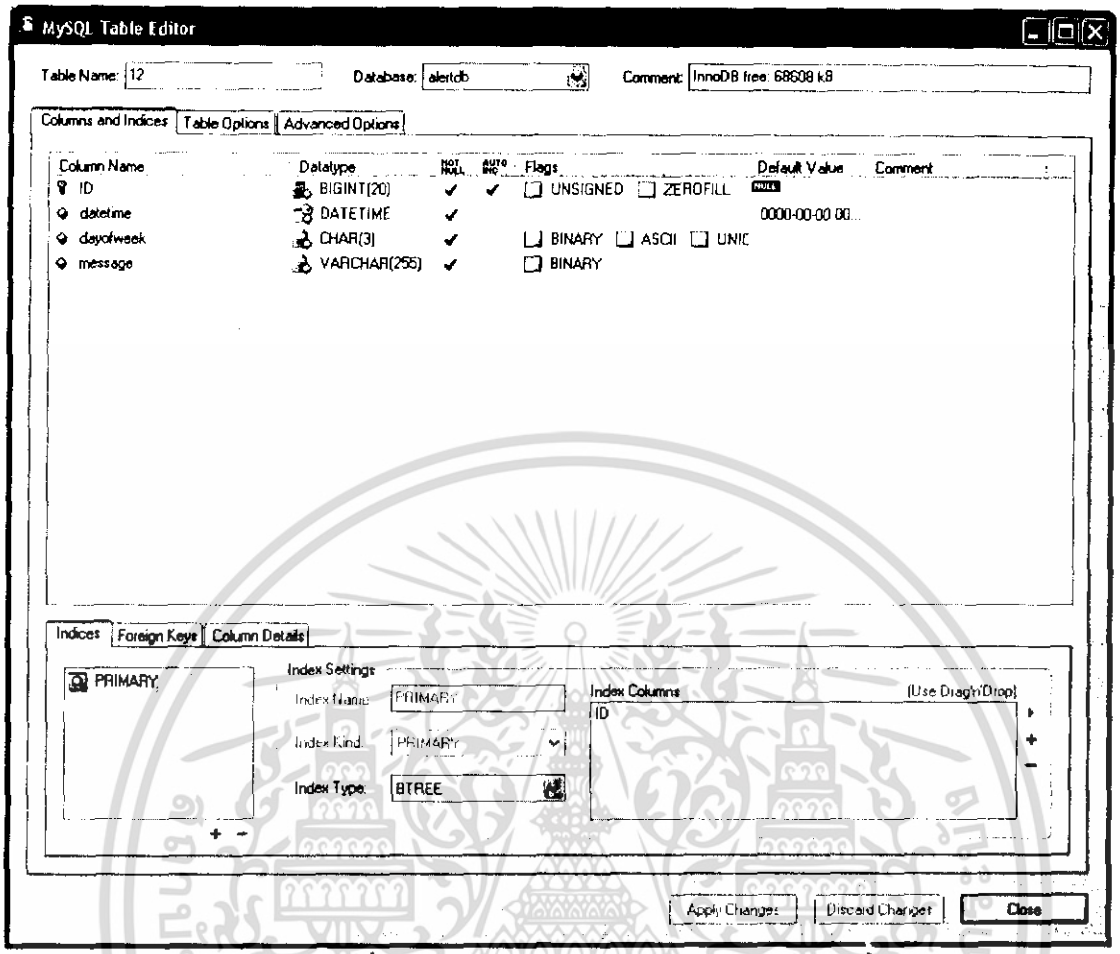
รูปที่ 5.4 ที่อยู่ใน Schema observe (ชุดข้อมูลที่สังเกต ณ ปัจจุบัน)



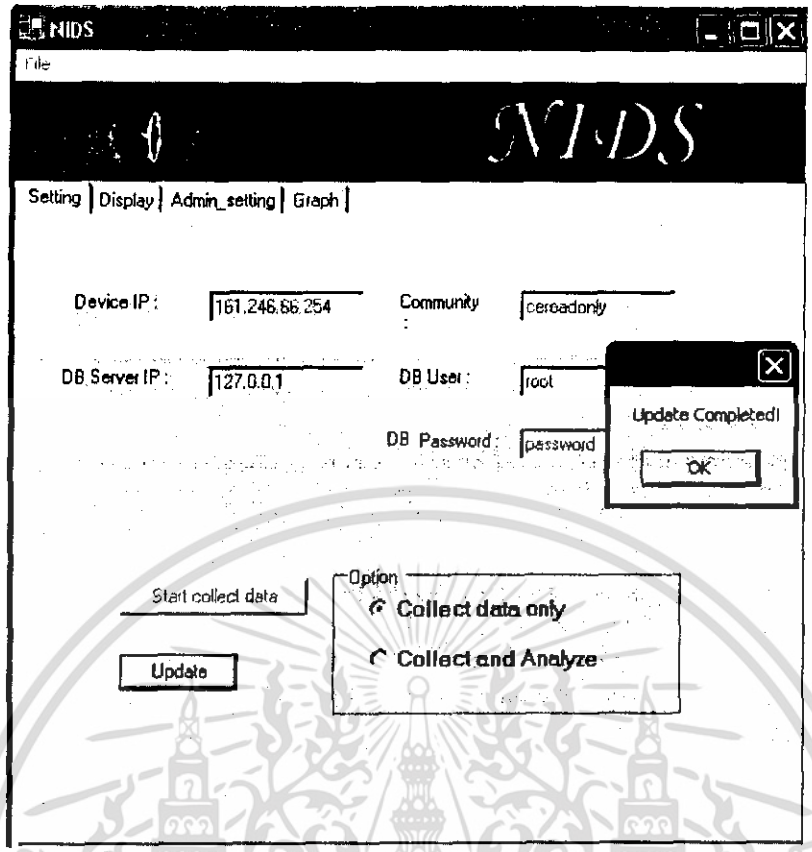
รูปที่ 5.5 ข้อมูลในตารางของชุดข้อมูลที่สังเกต ณ ปัจจุบัน



รูปที่ 5.6 ข้อมูลตารางใน Schema alertdb

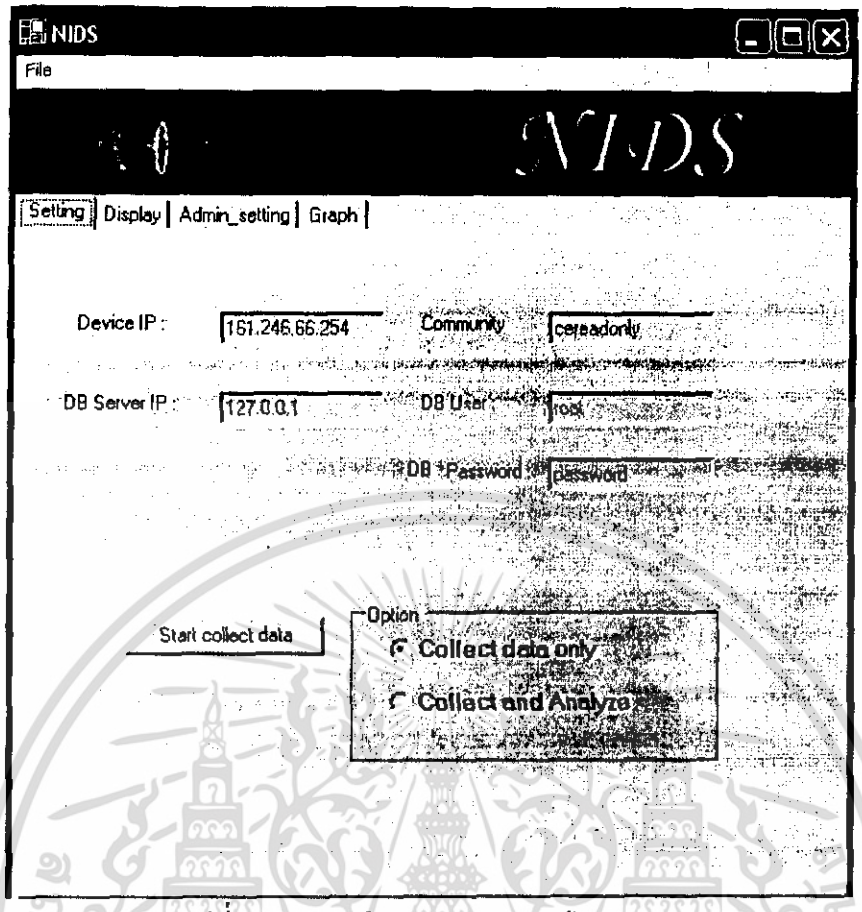


รูปที่ 5.7 ข้อมูลตารางของ Schema alertdb



รูปที่ 5.8 การทำงานของโปรแกรมหลังการกดปุ่ม Initialization

จากนั้นก็จะมีปุ่ม update ปรากฏขึ้นซึ่งปุ่มอัพเดทนี้เป็นการเตรียมตัวแปรต่างๆ ในโปรแกรม (ถ้ามีการสร้างฐานข้อมูลมาก่อนแล้วเมื่อเปิดโปรแกรมใหม่อีกครั้งจะขึ้นหน้านี้เลย) เมื่อกดปุ่มupdate แล้วจะปรากฏดังรูปที่ 5.8

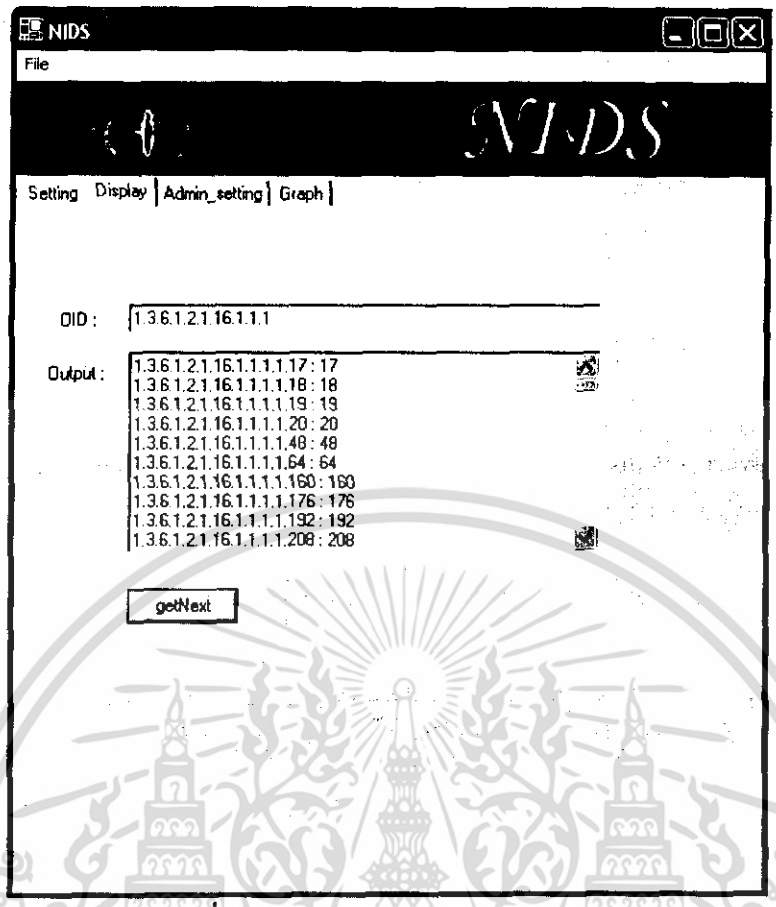


รูปที่ 5.9 รูปของโปรแกรมหลังกดปุ่ม update

จากนั้นทำการเลือก Option ที่ Collect data only เพื่อสั่งให้โปรแกรมทำการเก็บข้อมูลเท่านั้นยังไม่มีการคำนวณและวิเคราะห์ความผิดปกติโปรแกรมจะทำการแบ่ง thread ไปทำการเก็บข้อมูลทุกๆ 5 นาที แต่ถ้าเป็นการสั่งงานให้ทำการวิเคราะห์ให้เลือก option ที่ Collect and Analyze โปรแกรมจะทำการแบ่ง thread จากนั้นกดปุ่ม Start collect data โปรแกรมจะเริ่มทำการวิเคราะห์ข้อมูล

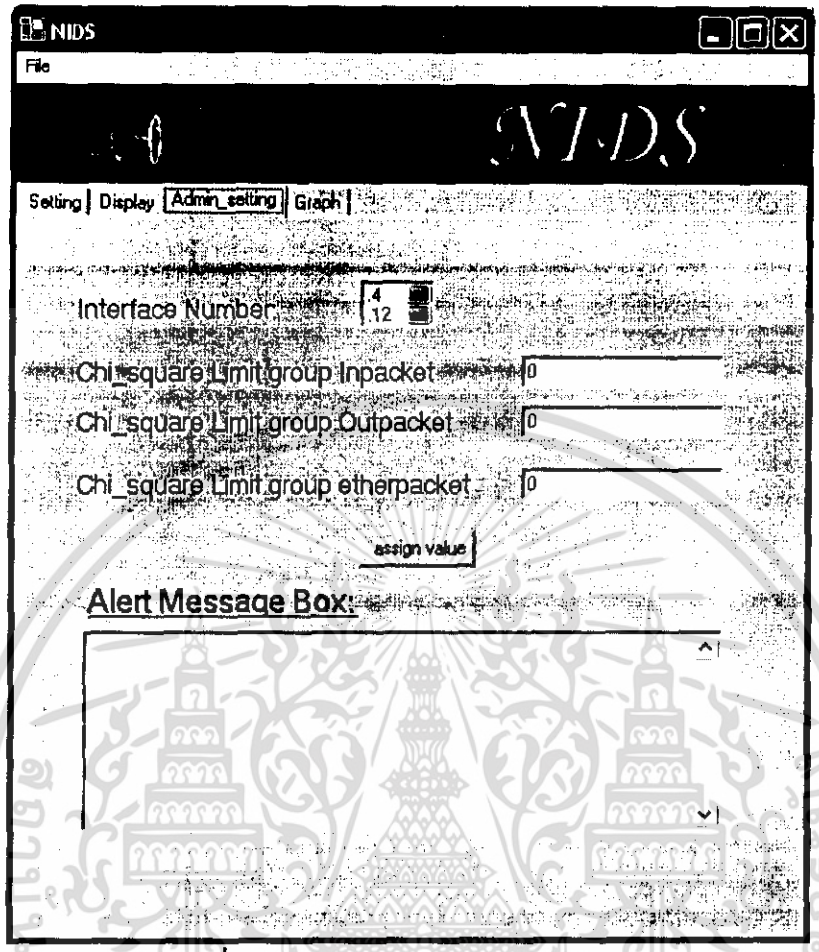
5.3. การทำงานในหน้า Display

ในหน้า Display มีข้อมูลที่ผู้ใช้ต้องกรอกในช่อง OID คือค่าอ๊อบเจ็คไอเด็นติไฟเออร์ ที่ต้องการให้โปรแกรมไปทำการดึงข้อมูลออกมาแสดงโดยเมื่อทำการป้อนข้อมูลในช่อง OID เสร็จเรียบร้อยแล้ว กดปุ่ม get โปรแกรมจะแบ่ง thread ไปทำการดึงข้อมูลตั้งแต่โหนดของค่าที่กรอกในช่อง OID ลงไปและแสดงผลออกมาในช่อง Output ดังแสดงในรูปที่ 5.10



รูปที่ 5.10 ผลการทำงานในหน้า display

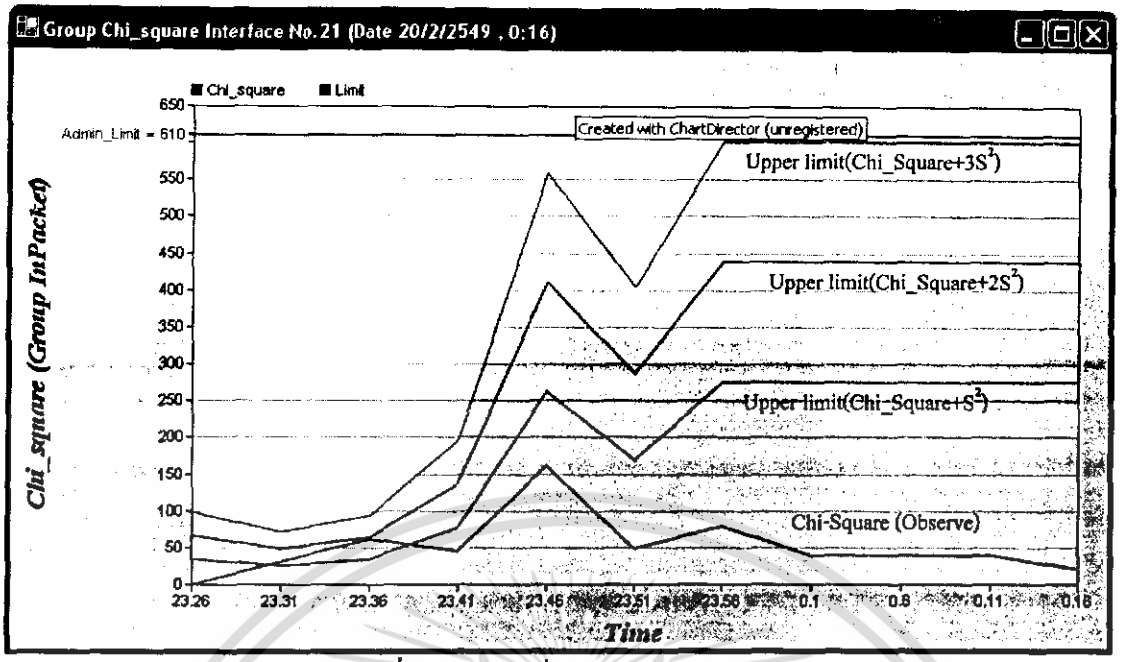
5.4. การทำงานในหน้า Admin_setting



รูปที่ 5.11 การใช้งานหน้า Admin_setting

โดยหน้า Admin_setting นี้มีการทำงานแบ่งออกเป็น 2 ส่วน

- ผู้ใช้งานสามารถกำหนดขอบเขตของการใช้งานปกติโดยป้อนค่าที่ต้องการเข้าไปในช่อง Chi-square Limit ต่างๆ ของในแต่ละอินเตอร์เฟสเพื่อใช้ในในเหตุการณ์ปกติแต่มีการใช้งานเครือข่ายแบบผิดปกติ เช่น มีการจัดงานขึ้นภายในองค์กรซึ่งมีการใช้งานเครือข่ายมากขึ้นกว่าปกติจนเกินขอบเขต upper bound ที่โปรแกรมคำนวณได้ โปรแกรมก็จะทำการแจ้งเตือน ซึ่งเป็นเหตุการณ์ที่ไม่มีความผิดปกติ ดังนั้นในส่วนนี้เป็นส่วนที่เอาไว้ใช้ป้องกันในเรื่อง False positive (การแจ้งเตือนโดยที่ไม่มีความผิดปกติเกิดขึ้นจริง) โดยเมื่อเรากำหนดค่า Admin_chi_square แล้วค่านั้นจะไปปรากฏอยู่บนกราฟนั้น(หากไม่มีการกำหนดจะมีค่าเป็น 0) เพื่อแสดงขอบเขตที่ผู้ใช้กำหนดขึ้นดังรูปที่ 5.12



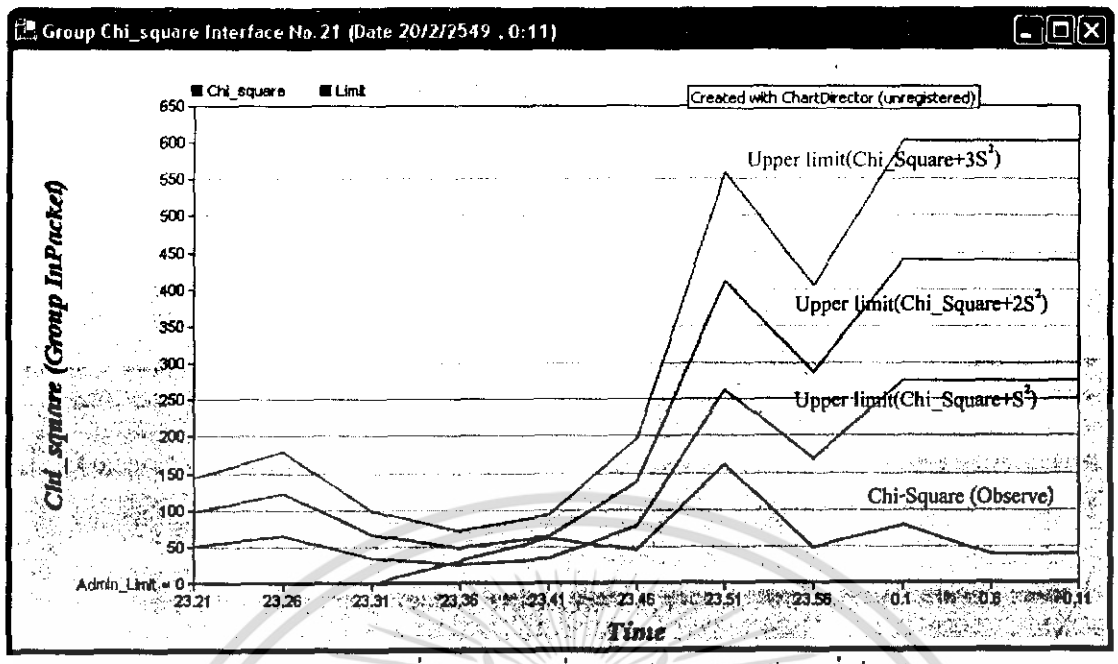
รูปที่ 5.12 กราฟที่มีการกำหนดค่า Admin_Chi_square

- โปรแกรมจะทำการแจ้งเตือนไปยังผู้ดูแลระบบในกรณีที่เกิดความผิดปกติไว้ที่ช่อง Alert Message Box (โดยเหตุการณ์ที่เกิดความผิดปกติผู้ใช้งานสามารถตรวจสอบข้อมูลเหล่านี้ในฐานข้อมูล alertdb ได้ด้วยอีกทางหนึ่ง)

5.5. การทำงานในหน้า Graph

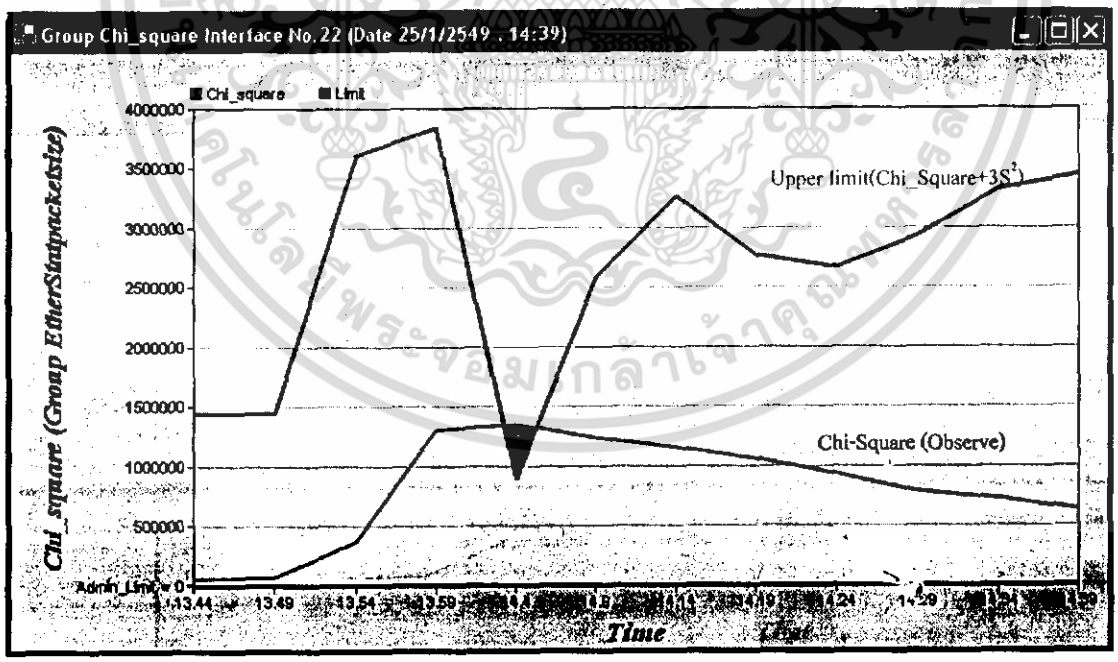
โดยหน้านี้มีการทำงานหลักคือการสร้างกราฟต่างๆ โดยกราฟจะทำการแสดงข้อมูลใหม่โดยอัตโนมัติเมื่อมีข้อมูลใหม่ที่เกิดจากการวิเคราะห์ตามที่ผู้ใช้งานเลือกมาให้แสดง โดยกราฟที่ได้นั้นมี 2 ลักษณะคือ

- กราฟที่มีการใช้งานปกติอยู่ตลอด คือปริมาณการใช้งานอยู่ใต้เส้นขอบเขตการใช้งานปกติเสมอดังแสดงในรูปที่ 5.13



รูปที่ 5.13 กราฟที่แสดงข้อมูลการใช้งานที่เป็นปกติ

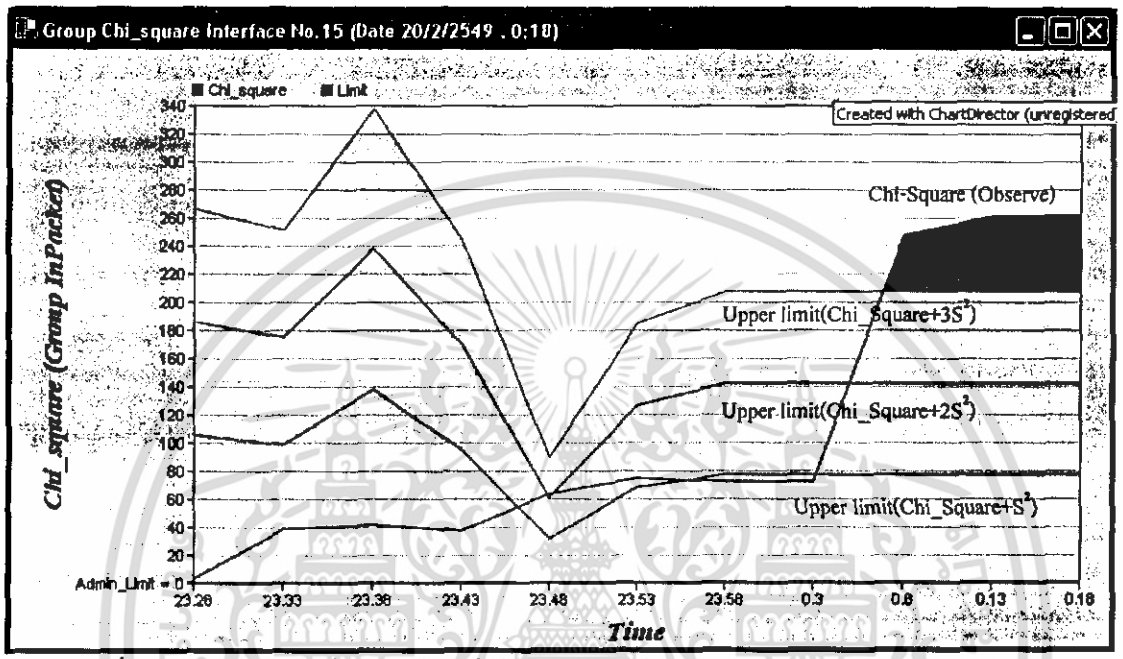
- กราฟที่มีการใช้งานผิดปกติ คือปริมาณการใช้งานอยู่เหนือเส้นขอบเขตการใช้งานปกติ จะมีลักษณะเป็นเส้นสีแดงเพื่อบ่งบอกลักษณะสิ่งที่ผิดปกติอย่างชัดเจนดังแสดงในรูปที่ 5.14



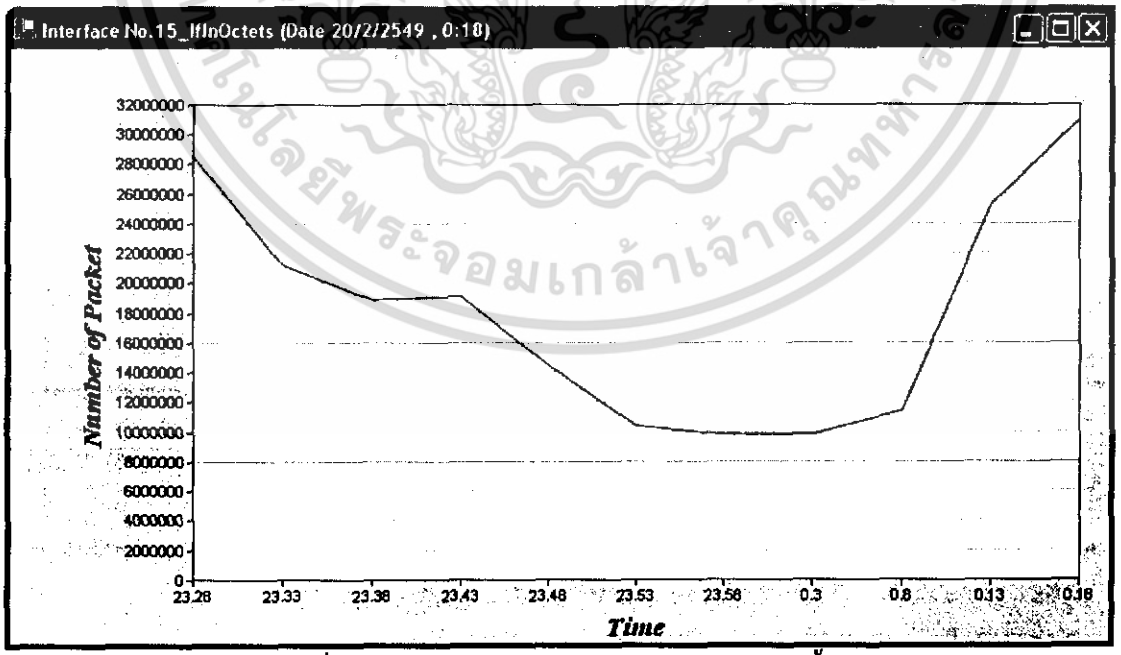
รูปที่ 5.14 กราฟที่แสดงข้อมูลการใช้งานที่ผิดปกติในช่วงเวลา 14.4 น.

5.6 ตัวอย่างผลการทำงานของโปรแกรม

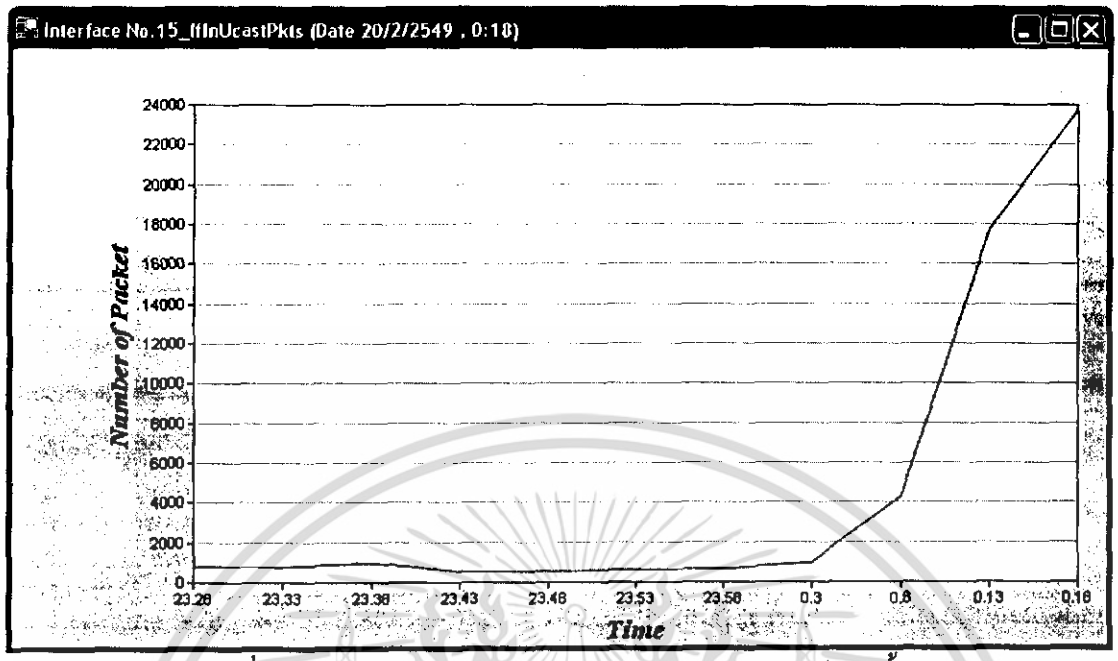
รูปแสดงการทำงานของโปรแกรมโดย ขณะที่โปรแกรมทำงานนั้นตรวจพบปริมาณการใช้งานที่ผิดปกติของอินเตอร์เฟสหนึ่ง ซึ่งเมื่อปริมาณข้อมูลขาเข้าของอินเตอร์เฟส (IfInOctets) เพิ่มขึ้นมากกว่าโพรไฟล์แล้วค่าทางสถิติที่คำนวณออกมาจะเกินค่าขอบเขตบน ดังรูป 5.15



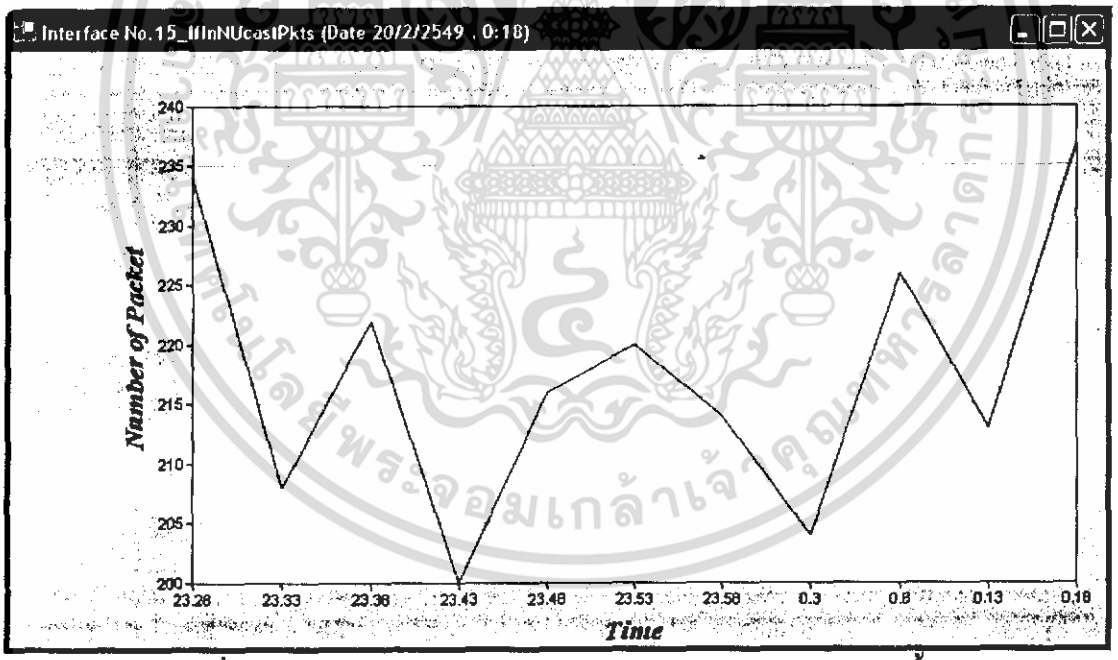
รูปที่ 5.15 ค่าทางสถิติที่คำนวณได้เมื่อปริมาณการใช้งานขาเข้าของอินเตอร์เฟสผิดปกติ



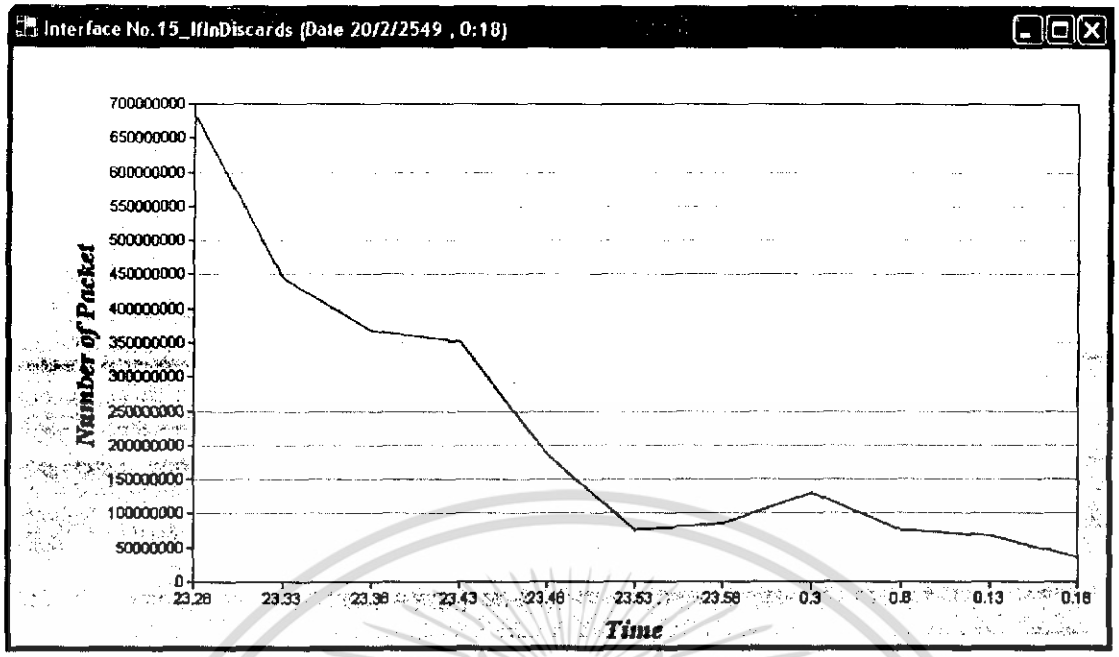
รูปที่ 5.16 ปริมาณข้อมูลขาเข้าของอินเตอร์เฟสนั้น



รูปที่ 5.17 ปริมาณข้อมูลขาเข้าแบบ-ยูนิคาสของอินเตอร์เฟสนั้น



รูปที่ 5.18 ปริมาณข้อมูลขาเข้าแบบนอน-ยูนิคาสของอินเตอร์เฟสนั้น



รูปที่ 5.19 ปริมาณข้อมูลที่อุปกรณ์ละทิ้งไปของอินเตอร์เฟสนั้น

บทที่ 6
บทสรุปและวิจารณ์

6.1. บทสรุปและวิจารณ์

ระบบเครือข่ายในปัจจุบันมีความเสี่ยงต่อการถูกโจมตีทั้งจากแฮกเกอร์และไวรัสคอมพิวเตอร์ที่อาศัยช่องโหว่ทางความปลอดภัยของเครื่องคอมพิวเตอร์ โดยลักษณะของปริมาณการใช้งานเครือข่ายที่มีลักษณะผิดปกติไป ก็บ่งชี้ได้ว่าเครือข่ายนั้นอาจจะถูกโจมตีเช่น โจมตีเพื่อปิดบริการ, ติดไวรัสคอมพิวเตอร์ หรืออาจเกิดลักษณะการทำงานที่เพิ่มมากขึ้นอันเนื่องมาจากความจำเป็นของผู้ใช้ในสถานการณ์ที่ต่างออกไปมาก ดังนั้นโปรแกรมนี้สามารถเป็นเครื่องชี้วัดถึงลักษณะการใช้งานที่ผิดปกติไปจากโพรไฟล์ และเป็นเครื่องมือช่วยตัดสินใจให้กับผู้ดูแลระบบว่าระบบเครือข่ายมีปริมาณการใช้งานมากผิดปกติเกินไปจนอาจเกิดการโจมตี เพื่อให้ผู้ดูแลระบบทำการตรวจสอบและแก้ไขต่อไป

6.2. วิจารณ์สิ่งที่ได้จากโครงงาน

1. โปรแกรมต้องทำการเก็บชุดข้อมูลการใช้งานในภาวะปกติเป็นระยะเวลาหนึ่งก่อนที่จะสามารถตรวจสอบความผิดปกติได้จริง
2. อุปกรณ์เครือข่ายที่โปรแกรมจะติดต่อขอข้อมูลนั้นต้องสนับสนุนเอสเอ็นเอ็มพีโปรโตคอล
3. โปรแกรมไม่สามารถวิเคราะห์เครือข่ายที่มีความผันผวนในการใช้งานสูงเนื่องจากค่าปริมาณการใช้งานจะมีความแตกต่างกันมากจนทำให้ค่า upper bound นั้นสูงมากจนเกิดไม่สามารถตรวจสอบความผิดปกติได้
4. โปรแกรมสามารถตรวจสอบความผิดปกติได้ว่าเกิดที่อินเตอร์เฟสใด แต่โปรแกรมไม่สามารถระบุความผิดปกติได้ว่าเกิดจากสาเหตุใด
5. โปรแกรมนี้เหมาะสมกับระบบเครือข่าย ที่มีการใช้งานในรูปแบบซ้ำๆ ซึ่งไม่มีเหตุการณ์ที่ทำให้มีการใช้เครือข่ายสูงในช่วงเวลาสั้นๆ คล้ายกับไวรัส หรือ หนอนคอมพิวเตอร์ เช่น การดาวโหลดไฟล์

6.3. ปัญหาและอุปสรรค

1. อุปสรรคในการเก็บข้อมูลโพรไฟล์ของการใช้งานปกติ เนื่องจากข้อมูลที่ใช้เป็นของสถาบันการศึกษาจึงเปิดกว้างให้นักศึกษาคนใดก็ได้ใช้งาน ซึ่งส่งผลให้ในขณะเก็บข้อมูลนั้นอาจมีเครื่องคอมพิวเตอร์ ภายในระบบเกิดการติดไวรัส , หนอนคอมพิวเตอร์ ซึ่งไม่สามารถไปควบคุมเครื่องคอมพิวเตอร์ภายในระบบได้ทุกเครื่องเพราะเป็นคอมพิวเตอร์ส่วนบุคคล ทำให้ข้อมูลโพรไฟล์ที่ได้ไม่เป็นข้อมูลที่เป็นการใช้งานปกติจริง
2. อุปสรรคในการเก็บข้อมูลโพรไฟล์ของการใช้งานปกติ โดยถ้าเกิดกรณีไฟฟ้าดับเกิดขึ้นจะทำให้ข้อมูลช่วงเวลานั้นขาดหายไปและเมื่อไฟฟ้ากลับมาปกติแล้วอุปกรณ์เครือข่ายจะมีการทำงานที่มีค่าโพรไฟล์สูงมาก ทำให้ค่าโพรไฟล์ที่ได้นั้นไม่ใช่ค่าที่เป็นการใช้งานปกติจริง
3. เนื่องจากโปรแกรมได้ทำการพัฒนาโดยทำการเก็บข้อมูลทุกๆ ช่วง 5 นาทีซึ่งเป็นช่วงเวลาที่กว้างพอสมควร จึงทำให้ปริมาณการใช้งานบางครั้งมีค่ามากน้อยแตกต่างกันค่อนข้างมากจนอาจก่อให้เกิดความผิดพลาดในการตรวจจับได้

6.4. แนวทางการพัฒนาต่อ

1. เพิ่มเติมในส่วนของตัวแปรต่างๆ ที่นำมาวิเคราะห์
2. เพิ่มเติมในส่วนทฤษฎีในการหา upper bound เพื่อใช้เปรียบเทียบกันทั้งแบบเดิมและแบบใหม่เพื่อเพิ่มความถูกต้องให้มากขึ้น
3. พัฒนาในส่วนของโปรแกรมให้ใช้ทรัพยากรน้อยลง
4. พัฒนาในส่วนของติดต่อกับผู้ใช้ให้มีรายละเอียดมากขึ้น เช่น แสดงปริมาณการใช้งานในชุดข้อมูลปกติของแต่ละตัวแปร
5. พัฒนาส่วนที่ระบุว่าความผิดปกติเกิดจากสาเหตุใด
6. พัฒนาโดยลดช่วงเวลาของการทำงานจากเดิม 5 นาทีให้น้อยลงกว่าเดิมเพื่อลดความผันผวนปริมาณการใช้งานที่เกิดขึ้น

บรรณานุกรม

หนังสืออ้างอิง

[1] "Chi Square Tutorial."[Online]. Available http://www.georgetown.edu/faculty/ballc/webtools/web_chi_tut.html

[2] N.Ye, and Q Chen. "An anomaly detection technique based on a chi-square statistic for detecting intrusions into information systems." Quality and Reliability Engineering International , Vol 17,NO. 2,2001,pp. 105 -112

[3] Montgomery DC. Introduction to Statistic Quality Control. John Wiley & Sons: Newyork,1989.

[4] William Stallings:"SNMP,SNMPv2,SNMPv3,and RMON1 and 2 ,Addison-Wesley,1999

[5] น.ท. ไพศาล โมลิสกุลมงคล :"Microsoft Visual C#.NET

เว็บไซต์อ้างอิง

1. http://www.advsofteng.com/
2. http://www.georgetown.edu/faculty/ballc/webtools/web_chi_tut.html
3. http://www.gcseguide.co.uk/standard_deviation.htm
4. http://www.thaicert.nectec.or.th/paper/ids/ids.php
5. http://www.thaicert.nectec.or.th/paper/basic/paniwat1.5_r1.pdf
6. http://republika.pl/maom_onet/snmp/snmp_ppnet/