ระบบตรวจจับความผิดปกติในระบบเครือข่าย
โดยอาศัยการเปลี่ยนแปลงเอนโทรปี

ENTROPY BASED NETWORK ANOMALY DETECTION SYSTEM

วิศรา ทาตุจนาภิชย์

วิทิตพรรค์ ชัยวิเชียร

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2556

ระบบตรวจจับความผิดปกติในระบบเครือข่าย
โดยอาศัยการเปลี่ยนแปลงเอนโทรปี
ENTROPY BASED NETWORK ANOMALY DETECTION SYSTEM

วริศรา กาญจนวณิชย์
วิทิตพงศ์ ชัยวิเชียร

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปีการศึกษา 2556

ปริญญานิพนธ์ปีการศึกษา 2556

สาขาวิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง ระบบตรวจจับความผิดปกติในระบบเครือข่ายโดยอาศัยการเปลี่ยนแปลงเอนโทรปี
ENTROPY BASED NETWORK ANOMALY DETECTION SYSTEM

ผู้จัดทำ

1. นางสาววริศรา กาญจนวณิชย์ รหัสนักศึกษา 53011431
2. นายวิทิตพงศ์ ชัยวิเชียร รหัสนักศึกษา 53011481

.....อาจารย์ที่ปรึกษา

(ดร. ธนัญชัย ตรีภาค)

ระบบตรวจจับความผิดปกติในระบบเครือข่าย โดยอาศัยการเปลี่ยนแปลงเอนโทรปี

นางสาววริศรา กาญจนวณิชย์ 53011431
นายวิทิตพงศ์ ชัยวิเชียร 53011481
ดร. ธนัญชัย ตรีภาค อาจารย์ที่ปรึกษา
ปีการศึกษา 2556

บทคัดย่อ

ในปัจจุบันมีการใช้งานระบบเครือข่ายในองค์กรต่างๆ อย่างแพร่หลาย การรักษาความปลอดภัยบนระบบเครือข่ายจึงมีความสำคัญอย่างมาก ดังนั้นในระบบเครือข่ายจึงควรมีเครื่องมือที่ช่วยในการรักษาความปลอดภัยให้กับระบบเครือข่าย และสามารถตรวจสอบการทำงานของระบบเครือข่ายได้

โครงงานระบบตรวจจับความผิดปกติในระบบเครือข่ายโดยอาศัยการเปลี่ยนแปลงเอนโทรปี เป็นเครื่องมือสำหรับผู้ดูแลระบบเครือข่ายที่ใช้งานบนระบบปฏิบัติการวินโดว์ โดยมีความสามารถในการตรวจตราการทำงานของระบบเครือข่าย จากนั้นทำการวิเคราะห์การทำงานของระบบเครือข่ายโดยอาศัยเทคนิคการเปลี่ยนแปลงเอนโทรปีของข้อมูล และแสดงผลที่ได้จากการวิเคราะห์เครือข่ายในลักษณะกราฟ ทำให้ผู้ดูแลระบบเครือข่ายสามารถทำการตรวจสอบระบบ เพื่อตรวจหาสิ่งผิดปกติที่เกิดขึ้นและสามารถแก้ไขปัญหาต่างๆ ส่งผลให้ระบบเครือข่ายสามารถทำงานได้อย่างมีประสิทธิภาพสูงสุด

ENTROPY BASED NETWORK ANOMALY DETECTION SYSTEM

Ms. Warissara	Kanchanawanich	53011431
Mr. Wititpong	Chaiwichean	53011481
Dr. Thanunchai	Threepak	Advisor

Academic Year 2013

ABSTRACT

As many organizations are widely and increasingly depending on network system, so security protection on the network becomes unavoidably vital. Therefore, security tools in network system that are capable in securing and monitoring network performance is greatly required.

This project applies Entropy Based Network Anomaly Detection System as a tool for network system administrators to monitoring network that is based on Windows operating system. The system has the ability to monitor the performance of the network, then analyze the performance of the network by using entropy based techniques and can graphically display the results of network analysis. Thus, the Network Administrator can detect any anomalies while monitoring the network and thus can quickly rectify the problems. By this way, the network system can achieve the maximum service efficiency with the least downtime.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้ได้รับคำแนะนำ และคำปรึกษาเกี่ยวกับการวิจัยและค้นคว้าเป็นอย่างดีจากอาจารย์ ดร. ธนัญชัย ตรีภาค อาจารย์ที่ปรึกษาในการจัดทำปริญญานิพนธ์ คณะผู้จัดทำรู้สึกซาบซึ้งเป็นอย่างมากในความอนุเคราะห์จากอาจารย์ที่คอยให้การสนับสนุนในการทำปริญญานิพนธ์นี้เสมอมา อีกทั้งอาจารย์อัครเดช วัชระภูพงษ์ ที่ช่วยเหลือ ให้ความรู้ที่เป็นประโยชน์ในการทำงานให้สำเร็จ รวมไปถึงห้องวิจัย ISAG ของสาขาวิชาวิศวกรรมคอมพิวเตอร์ ที่ได้อำนวยความสะดวก เป็นทั้งสถานที่ทำงาน ที่ศึกษาหาความรู้ประกอบการทำวิจัย และสนับสนุนอุปกรณ์การทำวิจัยในครั้งนี้

คณะผู้จัดทำขอขอบพระคุณเป็นอย่างสูง และหวังเป็นอย่างยิ่งว่าปริญญานิพนธ์ฉบับนี้จะเป็นประโยชน์ต่อทุกท่าน และสามารถให้คำแนะนำแก่นักศึกษารุ่นต่อไปในอนาคตได้

วริศรา กาญจนวณิชย์
วิทิตพงศ์ ชัยวิเชียร

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญรูป

รูปที่ **หน้า**

สารบัญรูป (ต่อ)

รูปที่ **หน้า**

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มาของโครงงาน

ปัจจุบันการรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์มีความสำคัญอย่างมาก เนื่องจากมีการใช้งานเครือข่ายอินเทอร์เน็ตในชีวิตประจำวันมากขึ้น สำหรับองค์กรต่างๆ ยิ่งต้องให้ความสำคัญกับการปกป้องรักษาความปลอดภัยของข้อมูลหรือต้องสามารถบริหารจัดการให้ระบบเครือข่ายสามารถใช้งานได้อย่างเป็นปกติ ดังนั้นในระบบเครือข่ายจึงควรมีอุปกรณ์ที่ช่วยในการรักษาความปลอดภัยให้กับเครือข่าย เช่น ระบบตรวจจับความผิดปกติในระบบเครือข่าย ซึ่งโครงการนี้มีจุดประสงค์ในการพัฒนาโปรแกรมให้สามารถคอยตรวจตราและทำการวิเคราะห์เครือข่ายจากการเปลี่ยนแปลงเอนโทรปี เพื่อที่จะใช้เป็นเครื่องมือที่ช่วยให้ผู้ใช้งานหรือผู้ดูแลระบบสามารถตรวจสอบความผิดปกติที่เกิดขึ้นในระบบเครือข่ายได้ (Network Anomaly Detection)

1.2 วัตถุประสงค์ของโครงงาน

1) เพื่อศึกษาหลักการทำงานของระบบตรวจจับความผิดปกติในระบบเครือข่ายโดยอาศัยการเปลี่ยนแปลงเอนโทรปี
2) เพื่อช่วยเหลือผู้ดูแลระบบในการวิเคราะห์ระบบเครือข่าย
3) เพื่อพัฒนาโปรแกรมต้นแบบที่ตรวจจับความผิดปกติของเครือข่าย โดยอาศัยการเปลี่ยนแปลงเอนโทรปี
4) เพื่อนำไปประยุกต์ใช้กับงานด้านอื่นๆ ทั้งในด้านการศึกษาและเชิงพาณิชย์

1.3 ขอบเขตของโครงงาน

ระบบตรวจจับความผิดปกติในระบบเครือข่ายจะใช้เทคนิคการวัดค่าความเปลี่ยนแปลงเอนโทรปีของข้อมูลในอุปกรณ์เครือข่าย ซึ่งการทำงานหลักของโปรแกรม คือ การดึงข้อมูลของอุปกรณ์เครือข่าย เช่น เราท์เตอร์ หรือ สวิตช์ โดยใช้โพรโทคอลเอสเอ็นเอ็มพี (Simple Network Management Protocol - SNMP) จากนั้นนำข้อมูลที่ได้มาคำนวณและวิเคราะห์การเปลี่ยนแปลงของค่าเอนโทรปีในระบบ เพื่อตรวจจับความผิดปกติบนเครือข่าย สามารถนำมาใช้ในการวิเคราะห์ความเปลี่ยนแปลงของค่าต่างๆบนเครือข่ายได้ ทำให้ผู้ใช้งานสามารถทราบได้ว่ามีความผิดปกติเกิดขึ้นหรือไม่ สามารถแบ่งการทำงานออกได้เป็น 4 ส่วน ดังต่อไปนี้

1) ส่วนการเก็บข้อมูลจากอุปกรณ์บนเครือข่าย
2) ส่วนติดต่อฐานข้อมูล
3) ส่วนการคำนวณเอนโทรปี
4) ส่วนการติดต่อกับผู้ใช้งาน

1.4 วิธีการดำเนินการ

1) ศึกษาความรู้ขั้นพื้นฐาน รูปแบบของโปรแกรมที่เกี่ยวข้อง ภาษาที่ใช้เขียนโปรแกรม การติดต่อฐานข้อมูล ไลบรารี่ที่ใช้ในการดึงข้อมูลจากอุปกรณ์เครือข่าย เพื่อนำมาใช้พัฒนาโปรแกรม
2) ศึกษารายละเอียดเกี่ยวกับโพรโทคอลเอสเอ็นเอ็มพี เพื่อหาตัวแปรที่จะนำมาใช้
3) ศึกษาความรู้เรื่องเอนโทรปี เทคนิคการวัดค่าความเปลี่ยนแปลงเอนโทรปีของข้อมูล และศึกษาสมการของเอนโทรปีเพื่อใช้ในการวิเคราะห์ข้อมูลการใช้งาน
4) ศึกษาความเป็นไปได้ในการดำเนินโครงการและทดสอบฟังก์ชันต่างๆ
5) ออกแบบส่วนต่างๆ ของโปรแกรม
6) พัฒนาโปรแกรมตามที่ได้ออกแบบไว้
7) เก็บชุดข้อมูลของการใช้งานเครือข่าย
8) ทดสอบระบบโดยใช้เอนโทรปีมาวิเคราะห์ความผิดปกติของข้อมูลในเครือข่าย
9) สรุปผลการทดลองและจัดทำเอกสาร

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1) ได้พัฒนาทักษะการเขียนโปรแกรมตรวจจับความผิดปกติในระบบเครือข่าย ทั้งในส่วนการติดต่อกับอุปกรณ์เครือข่าย การเก็บข้อมูล การวิเคราะห์ และการแสดงผลข้อมูล
2) ได้รับความรู้ในการวิเคราะห์ข้อมูลในเครือข่าย โดยใช้การเปลี่ยนแปลงเอนโทรปีของข้อมูล
3) สามารถตรวจจับความผิดปกติในระบบเครือข่ายได้
4) สามารถอำนวยความสะดวกให้กับผู้ใช้งานในการตรวจตราความเปลี่ยนแปลงของระบบเครือข่าย

1.6 ส่วนประกอบของปริญญานิพนธ์

ปริญญานิพนธ์ฉบับนี้ได้แบ่งเนื้อหาออกเป็น 5 บท โดยมีรายละเอียดดังต่อไปนี้

บทที่ 1 บทนำ กล่าวถึง ความสำคัญและที่มาของโครงงาน วัตถุประสงค์ของโครงงาน ขอบเขตของโครงงาน วิธีการดำเนินการ ประโยชน์ที่คาดว่าจะได้รับ และส่วนประกอบของปริญญานิพนธ์

บทที่ 2 ทฤษฎีที่เกี่ยวข้อง กล่าวถึง ทฤษฎีพื้นฐาน หลักการ ความรู้ต่างๆ ที่ใช้ในโครงงาน ซึ่งประกอบด้วย รายละเอียดของโพรโทคอลเอสเอ็นเอ็มพี และรายละเอียดของเอนโทรปี ซึ่งเป็นเทคนิคที่ใช้วัดค่าความเปลี่ยนแปลงของข้อมูล

บทที่ 3 การออกแบบและการพัฒนา กล่าวถึง วัตถุประสงค์ของโปรแกรม รายละเอียดการออกแบบและพัฒนาโปรแกรม บรรยายส่วนของการทำงานของระบบและโครงสร้างของระบบ

บทที่ 4 การทดลองและผลการทดลอง กล่าวถึง การตั้งค่าโปรแกรม การทดสอบกับระบบและผลลัพธ์ที่ได้จากการทดสอบ

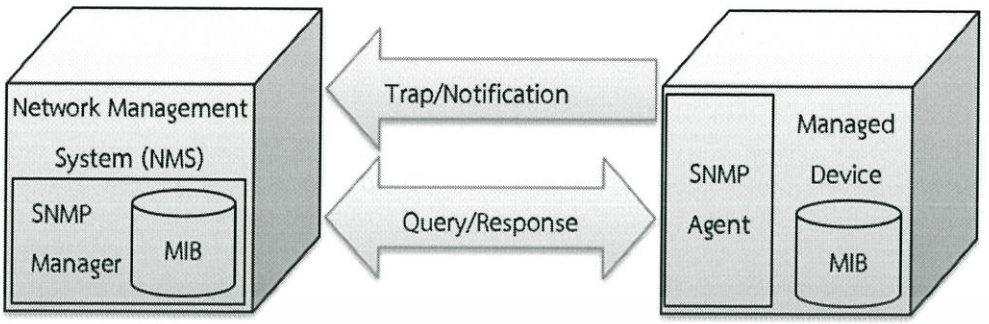
บทที่ 5 บทสรุปและข้อเสนอแนะ กล่าวถึง บทสรุปของโครงงาน วิจารณ์สิ่งที่ได้รับจากโครงงาน ข้อจำกัด รวมถึงปัญหาอุปสรรคต่างๆ ของโครงงาน และข้อเสนอแนะสำหรับเป็นแนวทางในการพัฒนาต่อ

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

การบริหารและจัดการเครือข่ายทีซีพี/ไอพี คือ การตรวจตรา ควบคุม และวางแผนการใช้งานทรัพยากรของระบบ เพื่อให้เครือข่ายสามารถทำงานได้อย่างมีประสิทธิภาพ สามารถตรวจหาจุดบกพร่องของเครือข่ายเมื่อเกิดปัญหา และแก้ไขปัญหาได้อย่างรวดเร็ว ดังนั้น ในเครือข่ายจึงจำเป็นต้องมีคอมพิวเตอร์ (Computer) อย่างน้อยหนึ่งเครื่อง เพื่อใช้ในการทำหน้าที่เป็นสถานีจัดการเครือข่าย เรียกว่า แมนเนเจอร์ (Manager) หรือ เอ็นเอ็มเอส (NMS : Network Management Station) และภายในแต่ละเครือข่ายจะมีเอเจนต์ (Agent) หรืออุปกรณ์เครือข่ายที่มีฟังก์ชัน (Function) ให้ตรวจสอบหรือปรับเปลี่ยนการทำงานได้โดยในเครือข่ายจะมีเอเจนต์เพียงหนึ่งตัวหรือหลายตัวก็ได้ ในการบริหารและจัดการเครือข่ายทีซีพี/ไอพีนั้น ผู้ที่มีหน้าที่รับผิดชอบในการบริหารจัดการจะต้องทำการบริหารจัดการเครือข่าย โดยอาศัยรูปแบบการจัดการมาตรฐานตามข้อกำหนดของโพรโทคอลเอสเอ็นเอ็มพี (SNMP Protocol) เป็นหลัก เพื่อการบริหารและจัดการเครือข่ายอย่างมีประสิทธิภาพ ดังนั้นผู้บริหารจัดการเครือข่ายควรจะต้องทำความเข้าใจในตัวโพรโทคอลเอสเอ็นเอ็มพี อีกทั้งโครงงานนี้ได้นำเทคนิคการคำนวณเอนโทรปีมาทำหน้าที่ในการตรวจจับ และวิเคราะห์ความเปลี่ยนแปลงของระบบเครือข่าย ซึ่งเนื้อหาในบทที่ 2 นี้ จะกล่าวถึงรายละเอียดของโพรโทคอลเอสเอ็นเอ็มพี และรายละเอียดของเอนโทรปีดังนี้

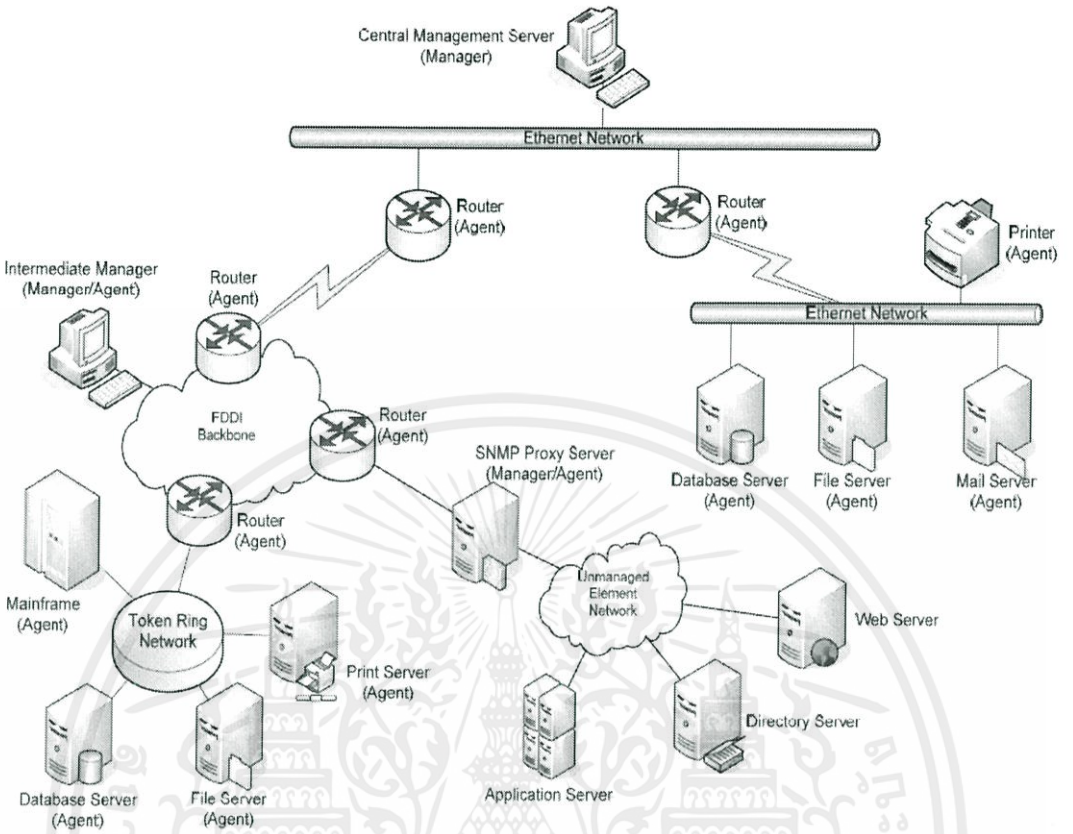
2.1 โพรโทคอลเอสเอ็นเอ็มพี

เอสเอ็นเอ็มพี (SNMP : Simple Network Management Protocol) เป็นโพรโทคอลประยุกต์ที่กำหนดรูปแบบ และกรรมวิธีในการบริหารจัดการเครือข่าย โดยที่โพรโทคอลเอสเอ็นเอ็มพีจะประกอบด้วยองค์ประกอบหลักอยู่ 4 อย่าง คือ แมนเนเจอร์ (Manager), เอเจนต์ (Agent), ชุดคำสั่งที่ใช้สำหรับแลกเปลี่ยนข้อมูล และฐานข้อมูลสารสนเทศ (Management Information Base) หรือ มิบ (MIB) ดังที่แสดงในรูปที่ 2.1



รูปที่ 2.1 องค์ประกอบของการจัดการเครือข่ายด้วยโพรโทคอลเอสเอ็นเอ็มพี

โพรโทคอลเอสเอ็นเอ็มพีได้รับความนิยมและใช้งานกันอย่างแพร่หลายในการจัดการอุปกรณ์ต่างๆ เช่น พีซี (PC : Personal Computer) โมเดม (Modem) ฮับ (Hub) สวิตช์ (Switch) เราเตอร์ (Router) เป็นต้น ในเครือข่ายอินเทอร์เน็ต โพรโทคอลเอสเอ็นเอ็มพีจะช่วยให้สามารถรวบรวมข้อมูลเพื่อนำไปวิเคราะห์ค้นหาปัญหาและแก้ปัญหาความผิดพลาดของระบบเครือข่ายที่เกิดขึ้น รวมทั้งใช้ในการจัดการประสิทธิภาพและการวางแผนการเจริญเติบโตของเครือข่ายขององค์กรในอนาคตได้ง่ายขึ้น โดยที่ภายในระบบจัดการเครือข่ายจะมีซอฟต์แวร์แมนเนเจอร์ ทำหน้าที่ในการเฝ้าติดตามและควบคุมการทำงานของอุปกรณ์ต่างๆ ในเครือข่าย ซึ่งในแต่ละอุปกรณ์ที่จะถูกจัดการเหล่านี้จะต้องมีส่วนของซอฟต์แวร์เอเจนต์ทำงานอยู่ เพื่อทำหน้าที่รอรับคำสั่งการปรับค่าการทำงานอุปกรณ์จากแมนเนเจอร์ และรอรับคำสั่งการสอบถามจากแมนเนเจอร์มาแปลผล เพื่อดึงเอาข้อมูลที่ต้องการในฐานข้อมูล MIB ส่งกลับไปให้กับแมนเนเจอร์ นอกจากนี้ยังทำหน้าที่ในการแจ้งเตือนเหตุการณ์บางอย่างที่เกิดขึ้นภายในอุปกรณ์ให้กับแมนเนเจอร์ โดยไม่ต้องมีการร้องขอจากแมนเนเจอร์ เช่น อินเทอร์เฟสการ์ดของอุปกรณ์ไม่ทำงาน, การใช้พื้นที่ของฮาร์ดดิสก์เกินค่าที่ได้กำหนดไว้ เป็นต้น ส่วนฐานข้อมูล MIB จะมีอยู่ทั้งในแมนเนเจอร์และเอเจนต์ ซึ่งภายในฐานข้อมูลนี้จะเก็บตัวแปรของอ็อบเจ็คต่างๆ เพื่อใช้อ้างถึงข้อมูลของอุปกรณ์ เช่น ชื่อของอุปกรณ์ (sysName), จำนวนเวลาทั้งหมดที่อุปกรณ์ทำงานอย่างต่อเนื่อง (sysUpTime), จำนวนของแพ็คเก็ตขาเข้าทั้งหมด (ifInOctets) ซึ่งมิบจะถูกอธิบายและกำหนดขึ้นตามโครงสร้างการจัดการอ็อบเจ็คในฐานข้อมูลมิบ (SMI) และผู้ผลิตอุปกรณ์แต่ละรายสามารถที่จะนำ SMI มาใช้ในการกำหนดและอธิบายกลุ่มของอ็อบเจ็คสำหรับใช้จัดการอุปกรณ์ของตนเองได้ รูปที่ 2.2 จะแสดงตัวอย่างของการจัดวางระบบจัดการเครือข่ายของโพรโทคอลเอสเอ็นเอ็มพี โดยการจัดการเครือข่ายด้วยโพรโทคอลเอสเอ็นเอ็มพี สามารถมีแมนเนเจอร์ได้มากกว่าหนึ่งแมนเนเจอร์ โดยมี 1 แมนเนเจอร์ทำหน้าที่เป็นตัวบริหารจัดการหลัก และแมนเนเจอร์ที่เหลือจะทำหน้าที่เป็นตัวบริหารจัดการรอง ซึ่งตัวบริหารจัดการรองจะถูกจัดการโดยแมนเนเจอร์หลักได้ด้วย และกลุ่มของอุปกรณ์ที่ไม่สนับสนุนโพรโทคอลเอสเอ็นเอ็มพี จะสามารถถูกจัดการได้โดยผ่านทางบริการของพร็อกซี



รูปที่ 2.2 ตัวอย่างการจัดวางองค์ประกอบของระบบจัดการเครือข่ายด้วยโพรโทคอลเอสเอ็นเอ็มพี

โพรโทคอลเอสเอ็นเอ็มพีมีการพัฒนามาอย่างต่อเนื่องตั้งแต่เอสเอ็นเอ็มพีเวอร์ชัน 1 จนถึงปัจจุบันคือเอสเอ็นเอ็มพีเวอร์ชัน 3 โดยในเวอร์ชัน 1 และ 2 นั้นมีลักษณะของสถาปัตยกรรมและการทำงานที่คล้ายคลึงกัน ซึ่งในเวอร์ชัน 2 ได้พัฒนา เพื่อยกระดับความสามารถและประสิทธิภาพของการทำงานจากเวอร์ชัน 1 เช่น เพิ่มคำสั่งสำหรับใช้ในการจัดการเครือข่าย, เพิ่มกลุ่มของอ็อบเจ็คภายในฐานข้อมูลมิบ เป็นต้น แต่วัตถุประสงค์หลักอันหนึ่งในการพัฒนาเอสเอ็นเอ็มพีเวอร์ชัน 2 ที่ยังไม่ประสบความสำเร็จ คือ การยกระดับในด้านความปลอดภัย ต่อมาจึงได้มีการพัฒนากลายมาเป็นเอสเอ็นเอ็มพีเวอร์ชัน 3 ที่ได้มีการแก้ไขปัญหาความไม่ปลอดภัยของโพรโทคอลเอสเอ็นเอ็มพีทั้งสองเวอร์ชันก่อนหน้านี้ โดยจะอธิบายรายละเอียดของโพรโทคอลเอสเอ็นเอ็มพีดังนี้

2.2 โพรโทคอลเอสเอ็นเอ็มพีเวอร์ชัน 2

โพรโทคอลเอสเอ็นเอ็มพีเวอร์ชัน 2 ได้ปรับปรุงแก้ไขข้อจำกัดของเวอร์ชัน 1 ซึ่งเป้าหมายในการแก้ไขเรื่องการขาดความปลอดภัยของเวอร์ชัน 1 ยังไม่สามารถปรับปรุงแก้ไขได้ในเวอร์ชันนี้ โดยที่ยังใช้ชื่อ community เป็นหลักเหมือนกับเวอร์ชัน 1 ซึ่งเรียกกันในชื่อว่า SNMPv2C โดยกำหนดรายละเอียดใน RFC 1901

การติดต่อระหว่างแมนเนเจอร์กับเอเจนต์มีรูปแบบในการติดต่อมากมายขึ้นอยู่กับวัตถุประสงค์ในการติดต่อแต่สำหรับเอสเอ็นเอ็มพีรุ่น 1 (SNMP Version 1) มีรูปแบบในการติดต่อกัน 5 คำสั่ง ดังนี้

1) Get-Request : ใช้สอบถามข้อมูลเอเจนต์ที่อยู่บนอุปกรณ์ที่ต้องการตรวจสอบในเครือข่าย
2) Get-Next-Request : ใช้สอบถามข้อมูลเรียงลำดับ เช่น ข้อมูลที่เก็บอยู่ในรูปแบบตารางหรือในกรณีที่ไม่ทราบตัวแปรที่แน่ชัด
3) Set-Request : ใช้เปลี่ยนแปลงค่าตัวแปรที่เอเจนต์รับผิดชอบอยู่
4) Get-Response : เอเจนต์ส่งคำตอบกลับยังผู้สอบถาม
5) Trap : ใช้แจ้งเหตุการณ์ที่เกิดขึ้นในระบบเครือข่าย เช่น การเริ่มต้นทำงานใหม่ของอุปกรณ์หรือเส้นทางที่ขัดข้อง

การเปลี่ยนแปลงแก้ไขอื่นๆ ของเวอร์ชันสองนี้ได้กำหนดรายละเอียดอยู่ในเอกสารตั้งแต่ RFC 1902 ไปถึง RFC 1907 โดยการเปลี่ยนแปลงหลักๆ ในโพรโทคอลเอสเอ็นเอ็มพีเวอร์ชัน 2 มีดังนี้

- เพิ่มคำสั่งพื้นฐานสำหรับใช้ในการจัดการเครือข่ายขึ้นอีก 2 คำสั่ง คือ คำสั่ง Get-Bulk-Request เพื่อใช้สำหรับการสอบถามข้อมูลครั้งละปริมาณมากๆ ซึ่งจะทำงานได้เร็วกว่าการใช้ Get-Next-Request ซึ่งจะทำให้การสอบถามข้อมูลจากตารางทำได้ง่ายและมีประสิทธิภาพมากขึ้น และอีกคำสั่ง คือ คำสั่ง Inform-Request ที่ใช้สำหรับติดต่อสื่อสารกันระหว่าง 2 ระบบจัดการเครือข่าย (Manager-to-Manager) นอกจากนี้ยังมีอีกหนึ่งคำสั่งที่ได้กำหนดขึ้นในเวอร์ชันนี้ แต่ยังไม่ได้นำมาใช้งาน คือ คำสั่ง Report โดยรายละเอียดของคำสั่งจะถูกกำหนดอยู่ในเอกสาร RFC 1905
- ข้อกำหนดของ SMI และ Trap ที่ใช้ในโพรโทคอลเอสเอ็นเอ็มพีเวอร์ชัน 1 ถูกนำมารวมกันและแก้ไขปรับปรุงเป็น SMIv2
- Textual Conventions ซึ่งเกี่ยวกับการกำหนดชนิดข้อมูลแบบใหม่ โดยใช้โครงสร้างตามที่กำหนดใน SMIv2 เพื่อทำให้ชนิดข้อมูลนั้นมีความหมายที่ชัดเจน สามารถเข้าใจได้ง่ายขึ้น
- Conformance Statements ซึ่งเกี่ยวกับข้อกำหนดที่ผู้ผลิตอุปกรณ์แต่ละรายนั้นจะต้องทำตามข้อกำหนดนี้เป็นอย่างน้อยในการผลิตอุปกรณ์ เพื่อให้ผลิตภัณฑ์ของตนสามารถใช้งานร่วมกับมาตรฐานของโพรโทคอลเอสเอ็นเอ็มพีได้ และนอกจากนี้ผู้ผลิตนั้นสามารถเพิ่มเติมส่วนต่างๆ เฉพาะของตนเข้าไปได้
- การเพิ่มความสามารถในการทำงานกับตาราง โดยสามารถต่อเติมคอลัมน์ของตารางที่มีอยู่ก่อนได้ รวมทั้งการสร้างและลบแถวของข้อมูลในตารางได้

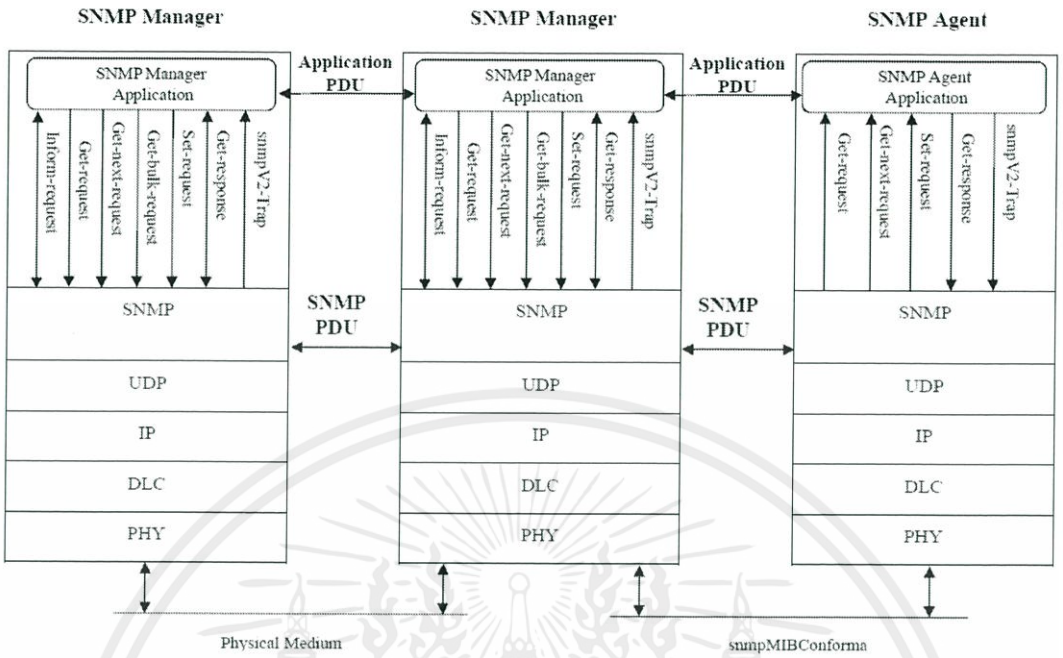
- ปรับปรุงอ็อบเจ็คในฐานข้อมูล MIB โดยการเพิ่มกลุ่มอ็อบเจ็คภายใต้โหนด internet, การเปลี่ยนแปลงกลุ่มอ็อบเจ็ค system และ snmp และเพิ่มกลุ่มอ็อบเจ็คภายใต้โหนด mib-2
- Transport Mappings ซึ่งเกี่ยวกับข้อกำหนดและรายละเอียดของโพรโทคอลในระดับชั้นทรานสปอร์ตเลเยอร์ ที่นอกเหนือจากการใช้โพรโทคอลยูดีพี (UDP) ของทีซีพี/ไอพี (TCP/IP) ที่สามารถใช้งานร่วมกับโพรโทคอลเอสเอ็นเอ็มพี ได้ เช่น OSI, IPX, DDP

และเนื่องจากการเปลี่ยนแปลงที่เกิดขึ้นในโพรโทคอลเอสเอ็นเอ็มพีเวอร์ชัน 2 นี้ไม่สามารถนำกลับมาใช้ร่วมกับเวอร์ชัน 1 ที่ใช้งานอยู่ก่อนหน้านี้ได้ จึงได้มีการนำเสนอวิธีการใช้งานร่วมกันของโพรโทคอลเอสเอ็นเอ็มพี ทั้งสองเวอร์ชันซึ่งถูกกำหนดรายละเอียดอยู่ในเอกสาร RFC 1908

2.2.1 สถาปัตยกรรม

องค์ประกอบพื้นฐานของโพรโทคอลเอสเอ็นเอ็มพีเวอร์ชัน 2 จะเหมือนกันกับในเวอร์ชัน 1 คือ ประกอบด้วยแมนเนเจอร์และเอเจนต์ ดังรูปที่ 2.3 แต่มีส่วนการยกระดับความสามารถและประสิทธิภาพของการทำงานให้ดีขึ้นจากโพรโทคอลเอสเอ็นเอ็มพีเวอร์ชัน 1 คือ

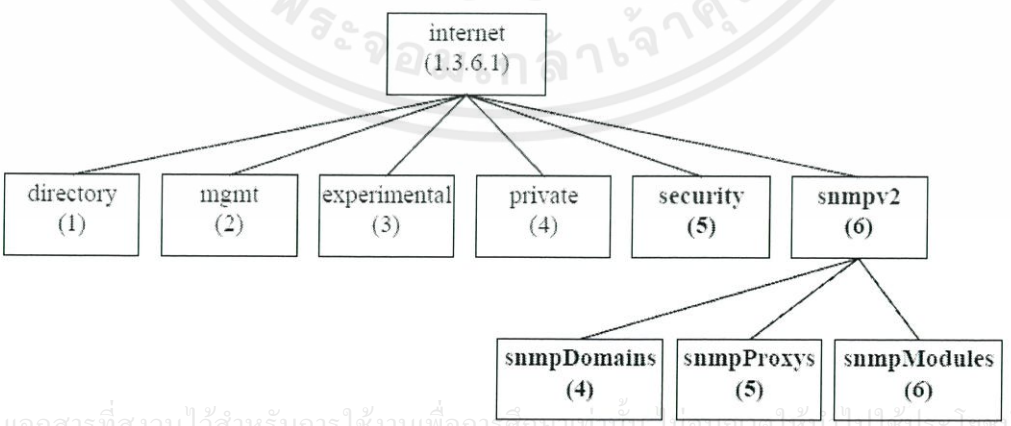
- มีการยกระดับเพื่อให้สามารถเลือกใช้โพรโทคอลสำหรับการขนส่งข้อมูลในระดับชั้นทรานสปอร์ตเลเยอร์ได้หลายแบบ เช่น ที่เอเจนต์สามารถเลือกใช้โพรโทคอล CLNS (Connectionless-Mode Network Service) ของ OSI ติดต่อสื่อสารกับแมนเนเจอร์ที่ใช้ UDP
- มีคำสั่งสำหรับใช้ในการทำงานเพิ่มขึ้นจากเดิม 2 คำสั่ง รวมเป็น 7 คำสั่ง โดยมีคำสั่ง Inform-Request สำหรับให้แมนเนเจอร์หนึ่งติดต่อสื่อสารกับแมนเนเจอร์อื่นๆ ได้ และคำสั่ง Get-Bulk-Request สำหรับใช้ในการสอบถามข้อมูลได้เป็นกลุ่มก้อน เช่น ข้อมูลที่เป็นตาราง
- คำสั่งอื่นที่เหลือคือ get-request, get-next-request และ set-request ยังคงมีรูปแบบและการทำงาน เหมือนกับเวอร์ชัน 1 ส่วนคำสั่ง get-response ยังคงมีรูปแบบเหมือนเดิมแต่ในเวอร์ชันนี้สามารถ สร้างขึ้นได้ทั้งจากเอเจนต์เพื่อตอบสนองต่อคำสั่งกลุ่ม get กับ set และสร้างขึ้นจากแมนเนเจอร์เพื่อ ใช้สำหรับการตอบสนองต่อคำสั่ง inform-request จากแมนเนเจอร์อื่น และคำสั่ง SNMPv2-trap ยังคงมีรูปแบบการทำงานเหมือนกับเวอร์ชัน 1 แต่ได้ยกเลิกการใช้รูปแบบ PDU ของ trap ใน เวอร์ชัน 1 แล้วปรับมาใช้โครงสร้างของ PDU ที่เหมือนกับคำสั่งอื่น



รูปที่ 2.3 สถาปัตยกรรมของโพรโทคอลเอสเอ็นเอ็มพีเวอร์ชัน 2

2.2.2 โครงสร้างการจัดการอ็อบเจ็คในฐานข้อมูลมิบ

โครงสร้างการจัดการอ็อบเจ็คในฐานข้อมูลมิบ (Structure of Management Information) เรียกสั้นๆ ว่า SMI สำหรับใน SNMPv2 ได้ยกระดับเป็น SMIv2 จาก SMIv1 ซึ่งกำหนดในรายละเอียดอยู่ ใน RFC 1902 โดยได้เพิ่ม 2 กลุ่มอ็อบเจ็คใหม่ขึ้นภายใต้โหนด internet คือ อ็อบเจ็ค security {1.3.6.1.5} และ snmpv2 {1.3.6.1.6} และอ็อบเจ็ค snmpDomains, snmpProxys และ snmpModules ภายใต้โหนด snmpv2 ดังรูปที่ 2.4



รูปที่ 2.4 กลุ่มของอ็อบเจ็คในโพรโทคอลเอสเอ็นเอ็มพีเวอร์ชัน 2

SMIv2 ถูกแบ่งออกเป็น 3 ส่วน คือ Module definitions เป็นส่วนที่ใช้อธิบายเกี่ยวกับความหมายของข้อมูล (Information modules) เช่นส่วนของฐานข้อมูล MIB, Object definitions เป็นส่วนที่ใช้อธิบายเกี่ยวกับ อ็อบเจ็ค (Managed Objects) และ Notification definitions เป็นส่วนที่ใช้อธิบายเกี่ยวกับการส่งข้อมูลที่ไม่ได้มีการร้องขอ เช่น Trap นอกจากนี้ยังมีอีกสองเอกสารที่เกี่ยวข้องกับ SMI คือ RFC 1903 เรื่อง Textual Conventions ที่เกี่ยวกับการกำหนดชนิดข้อมูลใหม่เพื่อให้สามารถอ่านเข้าใจได้ง่ายขึ้น

2.2.3 Management Information Base (MIB)

ฐานข้อมูล MIB สำหรับ SNMPv2 นี้ได้ปรับปรุงแก้ไขกลุ่มของอ็อบเจ็ค system และ snmp ภายใต้โหนด mib-2 ที่ใช้ในโพรโทคอลเอสเอ็นเอ็มพีเวอร์ชัน 1 และได้เพิ่มกลุ่มของอ็อบเจ็คใหม่ขึ้นมาสองกลุ่มภายใต้โหนด internet คือ security และ snmpv2 โดยที่โหนด security ยังไม่ได้มีการนำมาใช้งานในเวอร์ชันนี้ และภายใต้โหนด snmpv2 จะมีอีกสามโหนดย่อย คือ snmpDomains, snmpProxys และ snmpModules

กลุ่มของ MIB ที่อยู่ในโลกอินเทอร์เน็ตถูกแบ่งออกเป็น 6 กลุ่มย่อย ดังนี้

1) directory : เป็นกลุ่มที่สงวนไว้สำหรับการใช้งานในอนาคต
2) mgmt : เป็นกลุ่มของเอ็มไอบีที่ใช้ในการจัดการภายใต้โพรโทคอลเอสเอ็นเอ็มพีรุ่น 1
3) experimental : ใช้สำหรับการทดลอง
4) private : ใช้สำหรับผู้ผลิตกำหนดตัวแปรเฉพาะอุปกรณ์
5) security : ใช้ในระบบความปลอดภัย
6) SNMPv2 : ใช้ในโพรโทคอลเอสเอ็นเอ็มพีรุ่น 2

ภายใต้กลุ่ม mib-2 จะบรรจุกลุ่มย่อยที่ใช้เอสเอ็นเอ็มพี ซึ่งประกอบด้วนส่วนต่างๆ ซึ่งแต่ละกลุ่ม จะประกอบด้วยตัวแปรรูปแบบต่างกันไป ความหมายของกลุ่มได้แสดงไว้ดังตารางที่ 2.1

ตารางที่ 2.1 ความหมายของกลุ่มภายใต้เอ็มไอบี-2

ลำดับ	ชื่อกลุ่ม	ความหมาย
1	System	ข้อมูลระบบ
2	Interface	ข้อมูลอินเตอร์เฟสที่ใช้เชื่อมต่อ
3	At	ข้อมูลการแปลงที่อยู่ (Address)
4	Ip	ข้อมูลไอพี

5	Icmp	ข้อมูลไอซีเอ็มพี
6	Tcp	ข้อมูลทีซีพี
7	Udp	ข้อมูลยูดีพี
8	Egp	ข้อมูลโพรโทคอลเกตเวย์ภายนอก
9	Transmission	ข้อมูลบนสายสื่อสาร
10	snmp	ข้อมูลเอสเอ็นเอ็มพี

ชนิดของตัวแปรในเอ็มไอบี ซึ่งตัวแปรแต่ละชนิดของเอสเอ็นเอ็มพีจะมีแบบข้อมูลประจำของตัวเอง ซึ่งแบบข้อมูลต่างๆ ที่ใช้ในโพรโทคอลเอสเอ็นเอ็มพีก็คือ ตัวแปรชนิดต่างๆ ในเอ็มไอบีนั่นเอง และชนิดของตัวแปรต่างๆ ในเอ็มไอบีแสดงได้ดังตาราง 2.2

ตารางที่ 2.2 ชนิดของตัวแปรเอ็มไอบี

แบบข้อมูล	คำอธิบาย
Integer	ข้อมูลที่เป็นจำนวนเต็มมีค่าได้ตั้งแต่ 0 ถึง 65,535 หมายเลขพอร์ตของโพรโทคอลทีซีพี/ไอพี หรือยูดีพี
OctetString	ข้อมูลที่เก็บเป็นอักขระตั้งแต่ 0 อ็อคเต็ต (Octet) แต่ละออคเต็ตมีค่าตั้งแต่ 0 ถึง 255 ตัวอย่างของข้อมูลประเภทนี้ ได้แก่ รหัสผ่าน
DisplayString	ข้อมูลที่เก็บเป็นสายอักขระตั้งแต่ 0 อ็อคเต็ต แต่ละอ็อคเต็ตต้องเป็นรหัสแบบแอสกี้เอ็นวีที (ASCII NVT) มีความยาวตั้งแต่ 0 ถึง 255 ตัวอักษร
Null	ใช้เพื่อระบุว่าตัวแปรนั้นไม่มีค่าข้อมูลใดอยู่เลย เช่น เมื่อมีการสอบถามข้อมูลด้วยคำสั่ง get, get-next-request จะทำการกำหนดรูปแบบตัวแปรเป็น Null
ObjectIdentifier	เป็นชื่อตัวแปรในรูปการอ้างถึงแบบตัวเลขตามโครงสร้างเอ็มไอบี
IpAddress	เป็นสายอักขระ 4 อ็อคเต็ตแต่ละอ็อคเต็ตแทนไอพีแอดเดรสในแต่ละตำแหน่ง
PhysicalAddress	เป็นอักขระกำหนดหมายเลขของฮาร์ดแวร์ (Hardware Address) เช่นในอีเทอร์เน็ตแอดเดรส (Ethernet Address) ใช้สายอักขระ 6 อ็อคเต็ต
Counter	เป็นเลขจำนวนเต็มที่ไม่มีเครื่องหมาย มีค่าตั้งแต่ 0 ถึง 2^{32} (4,294,267,296) ค่าของข้อมูลชนิดนี้จะเพิ่มขึ้นเรื่อยๆ

	(เพิ่มอย่างเดียว) จนถึงค่าสูงสุดก็จะกลับมาเริ่มที่ 0 ใหม่อีกครั้ง
Gauge	เป็นเลขจำนวนเต็มที่ไม่คิดเครื่องหมายมีค่าตั้งแต่ 0 ถึง 2^{32} (4,294,267,296) เหมือน Counter แต่ค่าของข้อมูลชนิดนี้สามารถเพิ่มหรือลดค่าได้ เมื่อค่าเพิ่มไปถึงค่าสูงสุดก็จะคงไว้ค่าตามเดิม จนกว่าจะมีการปรับค่าให้กลับมาเป็น 0 อีกครั้ง ตัวอย่างตัวแปรที่ใช้ค่านี้ เช่น จำนวนการเชื่อมโยงทีซีพีที่อนุญาตให้มีได้
TimeTicks	เป็นเลขจำนวนเต็มที่ใช้นับเวลาในหน่วยเศษหนึ่งส่วนร้อยของวินาที เช่น เวลาตั้งแต่ระบบทำงาน (system uptime)
Sequence	เป็นโครงสร้างแบบเรคคอร์ด (Record) มีลักษณะคล้ายกับข้อมูลสตรัค (Struc) ในภาษาซี
Sequence of	เป็นโครงสร้างแบบตาราง หรืออาจมองเป็นรูปของอาร์เรย์ (Array) เช่น ตารางการเลือกเส้นทางของไอพี

2.2.4 คำสั่งพื้นฐานของโพรโทคอลเอสเอ็นเอ็มพีเวอร์ชัน 2

การติดต่อสื่อสารกันของโพรโทคอลเอสเอ็นเอ็มพี เวอร์ชันนี้ยังคงใช้ชื่อ community เป็นหลักสำหรับการกำหนดสิทธิในการเข้าถึงข้อมูลในแต่ละอุปกรณ์ โดยมีคำสั่งเพื่อใช้ในการจัดการเครือข่ายเพิ่มขึ้นอีก 2 คำสั่ง คือ คำสั่ง get-bulk-request เพื่อใช้สอบถามข้อมูลเป็นกลุ่ม และคำสั่ง inform-request เพื่อใช้ในการติดต่อสื่อสารกันระหว่างแมนเนเจอร์กับแมนเนเจอร์ และเปลี่ยน PDU ของคำสั่ง Trap ในเวอร์ชัน 1 ให้มาใช้รูปแบบเดียวกันกับ PDU ของคำสั่งอื่น ยกเว้น PDU ของคำสั่ง get-bulk-request ดังรูปที่ 2.5 แต่ยังคงหน้าที่เหมือนกับในเวอร์ชัน 1 และเรียกชื่อใหม่ว่า snmpv2-trap และนอกจากนี้ยังได้มีการกำหนดสถานะข้อผิดพลาด (Error Status) เพิ่มจากเดิมด้วย

PDU Type	RequestID	Error Status	Error Index	VarBind 1 Name	VarBind 1 Value	...	VarBind n Name	VarBind n Value

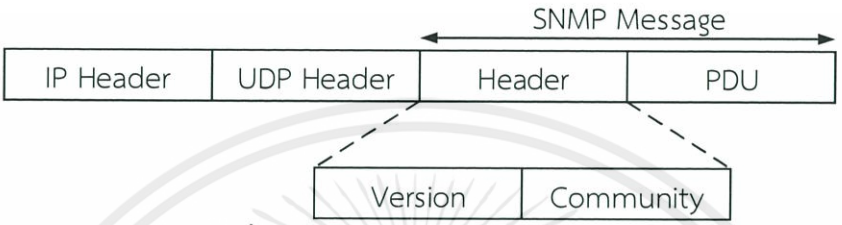
รูปที่ 2.5 PDU สำหรับคำสั่งทั้งหมดใน SNMPv2 ยกเว้นคำสั่ง get-bulk-request

PDU Type	RequestID	Non-Repeaters	Max-Repetitions	VarBind 1 Name	VarBind 1 Value	...	VarBind n Name	VarBind n Value

รูปที่ 2.6 PDU สำหรับคำสั่ง get-bulk-request

2.2.5 การเข้ารหัสข้อมูลเอสเอ็นเอ็มพี

การเข้ารหัสหรือการเอ็นแคบซูเลต (Encapsulate) คำสั่งและข้อมูลต่างๆในเอสเอ็นเอ็มพี จะเห็นว่าข้อความเอสเอ็นเอ็มพี (SNMP Message) จะประกอบด้วยข้อมูล 2 ส่วนคือเฮดเดอร์ (Header) และ พีดียู (PDU)

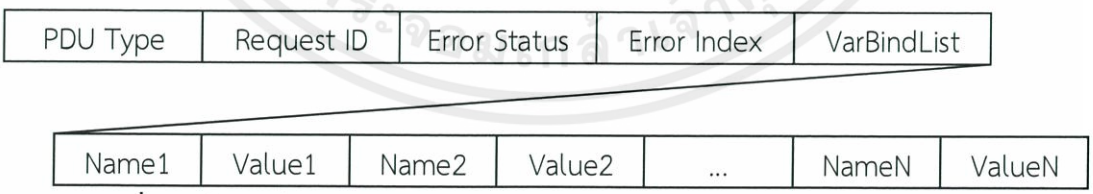


รูปที่ 2.7 โครงสร้างข้อมูลเอสเอ็นเอ็มพี

จากรูปที่ 2.7 จะเห็นว่าในส่วนเฮดเดอร์ของข้อความเอสเอ็นเอ็มพี จะประกอบด้วยข้อมูลอีก 2 ฟิลด์ ดังนี้

1) เวอร์ชั่น (Version) เป็นฟิลด์ที่ใช้ระบุรุ่นของโพรโทคอลเอสเอ็นเอ็มพีที่ใช้ หากใช้เอสเอ็นเอ็มพีรุ่น 1 ค่าในฟิลด์นี้จะถูกระบุเป็น 0 หากใช้เอสเอ็นเอ็มพีรุ่น 2 ในฟิลด์นี้จะถูกระบุเป็น 1
2) คอมมิวนิตี้ (Community) เป็นฟิลด์ที่ใช้ระบุรหัสผ่านในรูปสายอักขระ เพื่อให้เอเจนต์ใช้ในการตรวจสอบข้อความที่ส่งมาว่ามีสิทธิ์ในการสอบถามหรือเปลี่ยนแปลงข้อมูลหรือไม่

จากรูปที่ 2.8 จะเห็นว่าในส่วนของ PDU ของข้อความเอสเอ็นเอ็มพี ก็จะประกอบด้วยฟิลด์ย่อยเช่นกัน แต่จะมีลักษณะของฟิลด์ที่แตกต่างออกไปตามชนิดข้อความ หากเป็นข้อความชนิด get, get-next และ get-response จะมีโครงสร้างดังรูป 2.8



รูปที่ 2.8 โครงสร้างพีดียูของข้อความชนิด get, get-next และ get-response

จากตารางที่ 2.3 จะอธิบายถึงโครงสร้าง PDU ของข้อความชนิด get, get-next และ get-response ส่วนตารางที่ 2.4 จะแสดงรหัสความผิดพลาดของโพรโทคอลเอสเอ็นเอ็มพี

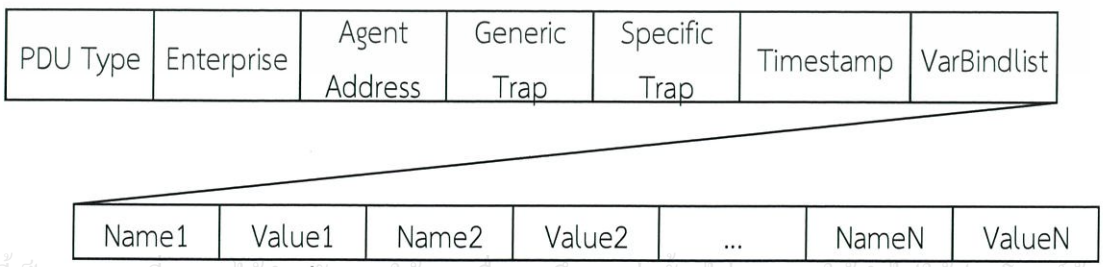
ตารางที่ 2.3 คำอธิบายโครงสร้าง PDU ของข้อความชนิด get, get-next และ get-response

คำศัพท์	คำอธิบาย
PDU Type	ระบุรูปแบบการติดต่อตั้งแต่รูปแบบที่ 1 - 5
Request ID	กำหนดหมายเลขข้อความเพื่อใช้จับคู่เมื่อได้รับคำตอบกลับมา
Error Status	ระบุรหัสผิดพลาดที่เกิดขึ้น ซึ่งรหัสผิดพลาดดูได้จากตาราง 2.4
Error Index	ดัชนีค่าผิดพลาดที่เกิดจากตัวแปรลำดับที่เท่าไหร่ของตัวแปรทั้งหมดที่ได้สอบถามไป
VarBindList	แสดงในรูปของตัวแปรและค่าของตัวแปรต่อเนื่องกับไปเป็นรายการ

ตารางที่ 2.4 รหัสผิดพลาดในเอสเอ็นเอ็มพี

รหัสผิดพลาด	ชื่อความผิดพลาด	คำอธิบาย
0	noError	ไม่มีข้อผิดพลาด
1	tooBig	เอเจนต์ไม่สามารถส่งคำตอบได้ในเฟรมเดียว
2	noSuchName	ไม่มีตัวแปรที่ต้องการในฐานข้อมูล
3	badValue	ค่าที่กำหนดให้ตัวแปรไม่ถูกต้อง
4	readOnly	เปลี่ยนค่าตัวแปรไม่ได้ เพราะอ่านค่าได้เพียงอย่างเดียว
25	genErr	มีข้อผิดพลาดอื่น ๆ อีก

ส่วนข้อความชนิดที่ trap จะมีลักษณะดังรูปที่ 2.9 และคำอธิบายโครงสร้าง PDU ของข้อความชนิด trap แสดงดังตารางที่ 2.5



รูปที่ 2.9 โครงสร้าง PDU ของข้อความชนิด Trap

ตารางที่ 2.5 คำอธิบายโครงสร้าง PDU ของข้อความชนิด trap

คำศัพท์	คำอธิบาย
PDU Type	ระบุรูปแบบการติดต่อตั้งแต่รูปแบบที่ 1 - 5
Enterprise	ระบุชนิดของเอเจนต์ที่สร้าง trap
Agent Address	ระบุที่อยู่ของเอเจนต์ที่สร้าง trap
Generic trap type	ระบุชนิดของ Generic trap
Specific trap code	ระบุหมายเลขของ Specific trap
Time stamp	ระยะเวลาตั้งแต่เริ่มเชื่อมต่อเครือข่ายจนกระทั่งสร้าง trap
VarBindList	แสดงในรูปของตัวแปรและค่าของตัวแปรต่อเนื่องกันไปเป็นรายการ

จะเห็นได้ว่าขนาดในแต่ละฟิลด์ของข้อความเอสเอ็นเอ็มพีจะไม่ได้กำหนดตายตัวไว้เพราะทุกฟิลด์ของข้อความเอสเอ็นเอ็มพีจะต้องเข้ารหัสก่อนส่งจึงมีขนาดแตกต่างกันไปตามชนิดของข้อมูล

2.2.6 การใช้งานร่วมกันกับโพรโทคอลเอสเอ็นเอ็มพีเวอร์ชัน 1

เนื่องจากการปรับเปลี่ยนแก้ไขหลายๆ อย่างใน SNMPv2 ทั้งส่วนของ SMI และฐานข้อมูล MIB จึงทำให้ไม่สามารถนำไปใช้งานร่วมกับเวอร์ชัน 1 ดังนั้นกลุ่มผู้ดูแลรับผิดชอบในการพัฒนา SNMP ของ IETF ได้กำหนดมาตรฐานของการใช้งานร่วมกันทั้งสองเวอร์ชัน ซึ่งได้กำหนดรายละเอียดไว้ในเอกสาร RFC 1908 โดยได้นำเสนอรูปแบบของการใช้งานร่วมกันไว้ 2 รูปแบบ คือ Bilingual Manager และ SNMP Proxy Server

2.3 เอนโทรปี

Entropy ในความหมายทั่วๆไปที่ไม่ใช่ความหมายในเชิงข้อมูลเครือข่าย คือ ปริมาณที่แสดงความไม่เป็นระเบียบของระบบ ซึ่งตามทฤษฎีอุณหพลศาสตร์นั้น เมื่อใดที่มีสิ่งต่างๆ เกิดการเปลี่ยนแปลงไปจากเดิม เอนโทรปีรวมของสิ่งต่างๆ ที่เกี่ยวข้องกับการเปลี่ยนแปลงดังกล่าวจะเพิ่มขึ้นเสมอ เช่น ห้องที่มีการจัดระเบียบไว้ดีแล้ว จะมีเอนโทรปีของห้องสูงขึ้นเมื่อเกิดความไม่เป็นระเบียบขึ้นภายในห้อง และหากเราพยายามจัดให้ห้องมีระเบียบเหมือนเดิม เราจะต้องใช้แรงงานของเราทำให้ร่างกายรู้สึกเหน็ดเหนื่อยจากการทำงาน เมื่อจัดระเบียบห้องเรียบร้อยแล้วจะเห็นได้ว่าเอนโทรปีของห้องจะลดลงเนื่องจากห้องมีความเป็นระเบียบมากขึ้น แต่ร่างกายของเราที่มีการใช้งานเพื่อจัดระเบียบห้องจะมีเอนโทรปีเพิ่มสูงขึ้น ส่งผลให้เอนโทรปีรวมของห้องและของเราเองสูงขึ้นด้วย

หากเป็นในเชิงข้อมูลเครือข่ายเอนโทรปีจะสามารถบอกได้ถึงความไม่เป็นระเบียบของข้อมูล โดยจะใช้ข้อมูลเป็นชุดๆ ในการวิเคราะห์ความเปลี่ยนแปลงของข้อมูล ถ้าหากข้อมูลในช่วงใดมีความผิดปกติไปจากข้อมูลที่เกิดขึ้นแบบสม่ำเสมอแล้ว เอนโทรปีจะสามารถบ่งบอกได้ว่าช่วงนั้นเกิดความผิดปกติบางอย่างขึ้น แต่เอนโทรปีจะไม่สามารถบอกได้ว่าความผิดปกติที่เกิดขึ้นนั้นคืออะไร ทั้งนี้ขึ้นอยู่กับการนำข้อมูลที่นำมาใช้คำนวณเอนโทรปีมาวิเคราะห์ในภายหลังว่าสิ่งที่เกิดขึ้นนั้นเกิดจากสาเหตุใด โดยในการคำนวณค่าเอนโทรปีของข้อมูลแต่ละชุดจะได้ผลลัพธ์เป็นค่าเอนโทรปีค่าเดียว

2.3.1 เทคนิคการคำนวณเอนโทรปีของข้อมูล

ก่อนที่จะทำการพัฒนาโปรแกรมจะต้องทำการพิสูจน์เทคนิคการคำนวณเอนโทรปีข้อมูลว่าสามารถนำหลักการนี้มาใช้งานได้จริงหรือไม่โดยหลักการคำนวณเอนโทรปีของข้อมูล ขั้นแรกจะต้องมีข้อมูลเป็นตัวแปรสำคัญในการคำนวณ ข้อมูลจะถูกแบ่งออกเป็นชุดตามความสัมพันธ์กันของข้อมูล ข้อมูลใดที่ส่งผลไปในทิศทางเดียวกันจะจัดเป็นข้อมูลชุดเดียวกัน เมื่อนำมาพิจารณาหาค่าเอนโทรปีข้อมูลจะต้องนำข้อมูลที่สัมพันธ์กันนั้นมาคำนวณทั้งชุด ขั้นที่สองการคำนวณเอนโทรปีมีสมการคณิตศาสตร์ [3] คือ

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log P(x_i)$$

โดย $P(x_i)$ คือค่าอัตราส่วนระหว่างข้อมูลแต่ละ attribute หารด้วยผลรวมทั้งหมดของจำนวนข้อมูลในข้อมูลชุดที่มีความสัมพันธ์กันในหนึ่งช่วงเวลา กล่าวคือ

$$P(x_i) = \frac{Number\ of\ packets\ with\ certain\ attribute}{Total\ number\ of\ packets}$$

เมื่อคำนวณตามสมการข้างต้น จะได้ค่าเอนโทรปีของข้อมูลในแต่ละชุด ข้อมูลเอนโทรปีจะสามารถบอกความแตกต่างของลักษณะข้อมูลที่มีการเปลี่ยนแปลงได้ ตัวอย่างการคำนวณเพื่อพิสูจน์ว่าเอนโทรปีสามารถบอกความแตกต่างของข้อมูลได้ จึงได้ทดลองนำฟังก์ชันทางคณิตศาสตร์ คือ sin(x), cos(x) และ tan(x) มาคำนวณบน Microsoft Excel ซึ่งจะทดลองโดยใช้ค่าของ sin(x), cos(x) และ tan(x) ซึ่งมีค่าปกติดังตารางที่ 2.6

ตารางที่ 2.6 ตารางแสดงค่าฟังก์ชัน sin(x), cos(x) และ tan(x)

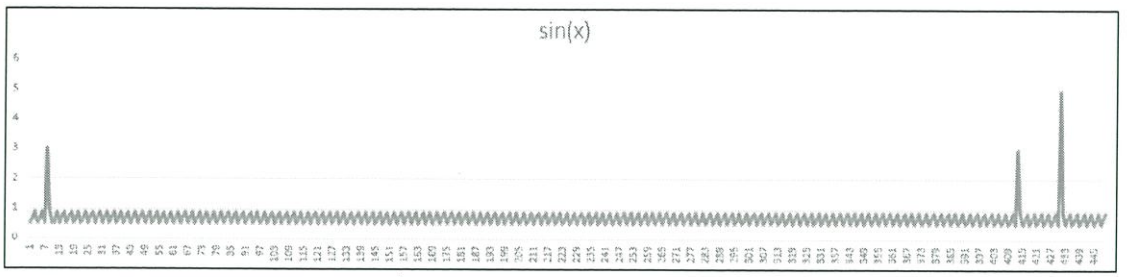
	sin(x)	cos(x)	tan(x)
30°	0.5	0.866	0.577
45 °	0.707	0.707	1
60 °	0.866	0.5	1.732

การทดลองเพื่อทดสอบค่าเอนโทรปีของข้อมูลว่าสามารถบอกความแตกต่างข้อมูลได้จริงหรือไม่ จึงได้ทดลองเปลี่ยนแปลงค่าของข้อมูลบางตัวให้มีค่าที่ผิดไปจากค่าจริง ดังแสดงในรูปที่ 2.10

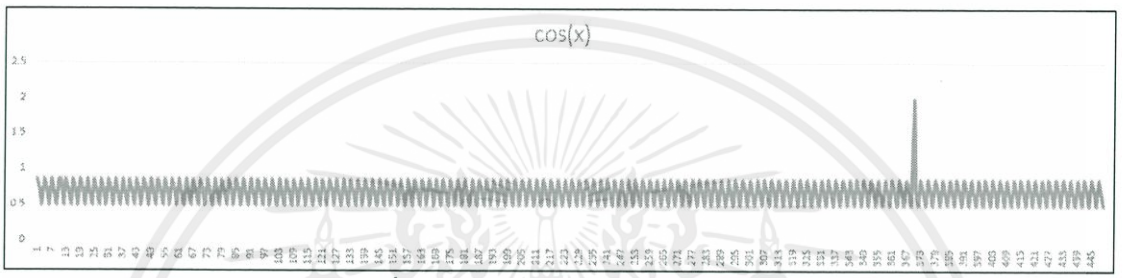
	A	B	C	D	E	F	G	H	I	J	K
1	sin(x)	cos(x)	tan(x)	sum	P sin(x)	PlogP sin(x)	P cos(x)	PlogP cos(x)	P tan(x)	PlogP tan(x)	Entropy
2	0.5	0.866	0.577	1.943	0.25733402	-0.151699124	0.445702522	-0.156421488	0.296963459	-0.156587937	0.464708549
3	0.707	0.707	1	2.414	0.292874896	-0.156195411	0.292874896	-0.156195411	0.414250207	-0.158548992	0.470939813
4	0.866	0.5	1.732	3.098	0.279535184	-0.154740481	0.161394448	-0.127842384	0.559070368	-0.141184011	0.423766876
5	0.5	0.866	0.577	1.943	0.25733402	-0.151699124	0.445702522	-0.156421488	0.296963459	-0.156587937	0.464708549
6	0.707	0.707	1	2.414	0.292874896	-0.156195411	0.292874896	-0.156195411	0.414250207	-0.158548992	0.470939813
7	0.866	0.5	1.732	3.098	0.279535184	-0.154740481	0.161394448	-0.127842384	0.559070368	-0.141184011	0.423766876
8	0.5	0.866	0.577	1.943	0.25733402	-0.151699124	0.445702522	-0.156421488	0.296963459	-0.156587937	0.464708549
9	3	0.707	1	4.707	0.63734863	-0.124680015	0.150201827	-0.123664887	0.212449543	-0.142924198	0.3912691
10	0.866	0.5	1.732	3.098	0.279535184	-0.154740481	0.161394448	-0.127842384	0.559070368	-0.141184011	0.423766876
11	0.5	0.866	0.577	1.943	0.25733402	-0.151699124	0.445702522	-0.156421488	0.296963459	-0.156587937	0.464708549
12	0.5	0.866	5	6.366	0.078542256	-0.086781074	0.136035187	-0.117853913	0.785422557	-0.082388179	0.287023166
13	0.866	0.5	1.732	3.098	0.279535184	-0.154740481	0.161394448	-0.127842384	0.559070368	-0.141184011	0.423766876
14	0.5	0.866	0.577	1.943	0.25733402	-0.151699124	0.445702522	-0.156421488	0.296963459	-0.156587937	0.464708549
15	0.707	0.707	1	2.414	0.292874896	-0.156195411	0.292874896	-0.156195411	0.414250207	-0.158548992	0.470939813

รูปที่ 2.10 ตัวอย่างตารางทดสอบค่าเอนโทรปีของข้อมูล

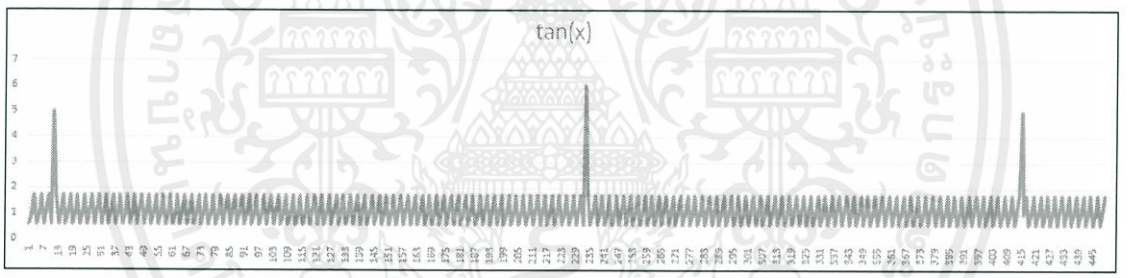
จากรูป 2.10 เป็นเพียงบางส่วนของตารางเท่านั้น เพราะจำนวนข้อมูลที่ใช้ทดสอบจริงมีจำนวน 450 แถว ซึ่งมากเกินไป จึงยกตัวอย่างตารางมาแค่บางส่วน จะเห็นได้ว่าค่าของฟังก์ชัน sin(x), cos(x) และ tan(x) ถูกแทนค่าลงไปอย่างถูกต้องตามค่าของฟังก์ชันที่เลือกมารูปที่ 2.10 แต่มีการเปลี่ยนแปลงค่าที่ถูกต้องในบางส่วนของตารางตามรูปในส่วนที่วงกลม คือ เปลี่ยนค่า sin(45°) จาก 0.707 เป็น 3 และค่า tan(30°) จาก 0.577 เป็น 5 (ในแถวที่ 9 และ 11 ตามรูปที่ 2.18) จะเห็นได้ว่าจากค่าที่ได้ทำการเปลี่ยนแปลง จะส่งผลให้ค่าเอนโทรปีเปลี่ยนแปลงไปจากปกติด้วย สามารถแสดงผลในรูปแบบกราฟได้ดังนี้



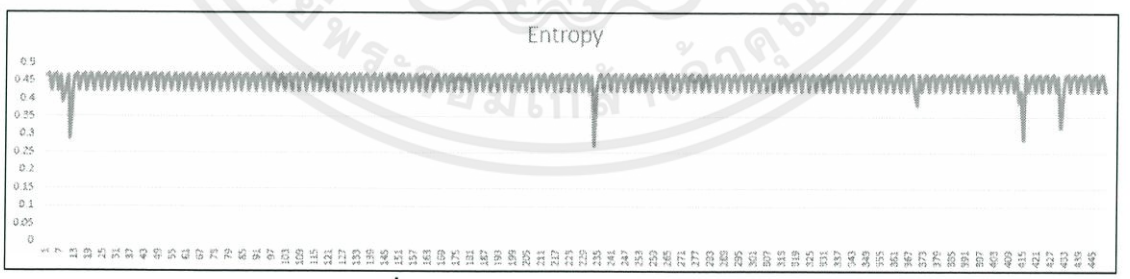
รูปที่ 2.11 กราฟของฟังก์ชัน sin(x)



รูปที่ 2.12 กราฟของฟังก์ชัน cos(x)



รูปที่ 2.13 กราฟของฟังก์ชัน tan(x)



รูปที่ 2.14 กราฟของเอนโทรปีข้อมูล

จะเห็นได้ว่าเมื่อเปรียบเทียบกราฟ sin(x), cos(x) และ tan(x) กับกราฟ entropy เมื่อกราฟของฟังก์ชันทั้งสามมีการเปลี่ยนแปลงค่าทำให้ค่าผิดปกติไปจากเดิม จะทำให้กราฟเอนโทรปีมีการเปลี่ยนแปลงไปด้วย โดยกราฟเอนโทรปีจะเปลี่ยนแปลงไปตามตัวแปรหรือ attribute ที่เปลี่ยนแปลงไปในช่วงเวลานั้นๆ

ดังนั้น เทคนิคการคำนวณเอนโทรปีข้อมูลจะสามารถแสดงให้เห็นถึงความแตกต่าง หรือความผิดปกติของข้อมูลที่เกิดขึ้นได้ จึงได้มีการนำเทคนิคการคำนวณเอนโทรปีข้อมูลมาใช้กับข้อมูลที่ได้จากระบบเครือข่าย เพื่อให้สามารถตรวจจับความผิดปกติที่เกิดขึ้นในระบบเครือข่ายได้เช่นกัน

2.3.2 งานวิจัยเอนโทรปีที่เกี่ยวข้อง

จากข้อมูลที่ได้ศึกษามาในทางเครือข่ายจะมีการนำเอนโทรปีมาใช้วิเคราะห์ตรวจจับความผิดปกติของเครือข่ายอยู่บ้างแต่ยังไม่เป็นที่แพร่หลาย โดยผู้วิจัยจะยกตัวอย่างจากงานวิจัยของเอนโทรปีในเชิงเครือข่ายเพื่อให้ได้เห็นตัวอย่างที่ชัดเจนขึ้นและเพื่อเป็นการยืนยันได้ว่าเอนโทรปีสามารถใช้ในเชิงเครือข่ายได้จริง [3]

งานชิ้นนี้เป็นการวิเคราะห์ข้อมูลจาก Carnegie Mellon University ในเดือนกุมภาพันธ์ปี 2005 ข้อมูลทั้งหมดมาจากการจราจรภายในเน็ตเวิร์คซึ่งมีไอพีแอดเดรสกว่า 10,000 ไอพีและข้อมูลที่ผ่านเข้าออกเน็ตเวิร์คมากกว่า 92 เทราไบต์ (TB) จากสองพันห้าร้อยล้าน (2,500,000,000) แพ็คเก็ตไอพีแอดเดรสในข้อมูลชุดนี้จะเก็บข้อมูลทุกๆ 5 นาทีที่ไม่มีการซ้อนทับกันและจะต้องจบการเชื่อมต่อกันภายในเวลา 5 นาทีนี้ด้วย เช่น การเก็บข้อมูลทั้งต้นทางและปลายทางของไอพีแอดเดรส (IP Address), พอร์ต (Port), ลำดับแพ็คเก็ต (Packet count) และลำดับของไบต์ (byte count) เมื่อมีการเก็บข้อมูลเหล่านี้จะทำให้เราทราบได้ถึง เวลาในการเชื่อมต่อ (connection time), โพรโตคอลที่ใช้ (protocol use), สถานะภาพการเชื่อมต่อ (connection state) และ ทิศทางของการส่งข้อมูล (flow direction) อย่างไรก็ตามในบางกรณีก็ไม่สามารถเห็นได้ชัดเจนจากข้อมูลที่เก็บไว้ เช่น ยูดีพีโฟลว์ (UDP flows), ทีซีพีโฟลว์ (TCP flows) ซึ่งจะต้องรอให้หมดเวลาที่กำหนด (time out) จึงจะสามารถทราบค่าเหล่านี้ได้

สูตรการคำนวณค่าเอนโทรปีที่นำมาใช้ในงานวิจัยนี้จะเริ่มต้นจากกำหนดให้ X เป็นค่าสุ่มซึ่งเป็นตัวแทนค่าของการกระจายในส่วนของลักษณะการใช้งานในเครือข่าย เช่น พอร์ตต้นทางและพอร์ตปลายทางที่ผ่านเข้าออกเน็ตเวิร์คเรากำหนดค่า $x_1 \dots x_n$ เป็นช่วงของค่า x ที่เป็นไปได้และ x_i กำหนดให้ $p(x_i)$ เป็นค่าของการสุ่มค่าที่ X จะถูกแทนด้วยค่า x_i ดังนี้ $p(x_i) = \Pr[X = x_i]$. เอนโทรปีของการสุ่มค่า X ถูกกำหนดให้เป็นลอการิทึมฐาน 2 ทั้งหมดโดยกำหนดให้ $0\log 0 = 0$ เราจะคำนวณค่าปกติของเอนโทรปี (ค่าจะอยู่ระหว่าง 0 กับ 1) จาก $\frac{H}{\log N_0}$ เมื่อ N_0 เป็นค่าที่แตกต่างจาก x_i ที่กำหนดดังสมการ

$$H(X) = -\sum_{i=1}^{N} p(x_i) \log p(x_i)$$

เราจะทำการศึกษาและทดลองการจาราจรในเครือข่ายทั้งหมด 7 ส่วนด้วยกันโดย 5 จากทั้งหมดนี้เราได้ข้อมูลที่จะนำมาใช้ศึกษาจาก ไอพีเฮดเดอร์ (IP header) คือ ที่อยู่ต้นทาง (source address), ที่อยู่ปลายทาง (destination address), พอร์ตต้นทาง (source port), พอร์ตปลายทาง (destination port) และ การกระจายของโฟลว์ไซส์ (FSD) โดยใช้หน่วยเป็นแพ็คเก็ตต่อโฟลว์ ก่อนที่เราจะใช้คุณสมบัติของโฟลว์เฮดเดอร์ในการวิเคราะห์ตามหลักของเอนโทรปีเราต้องใช้ข้อมูลในแบบการไหลของข้อมูลทิศทางเดียว (uni-directional) แต่ข้อมูลที่เราทำการบันทึกมาได้ในตอนแรกนั้นเป็นการไหลในแบบสองทิศทาง (bi-directional) เราจึงต้องทำการแปลงให้มาเป็นแบบทิศทางเดียวก่อนจึงจะสามารถนำข้อมูลมาใช้ได้โดยเราจะแปลงให้อยู่ในรูปของการไหลทิศทางเดียวสองครั้ง เพื่อคำนวณการกระจายได้มากกว่าคุณสมบัติของโฟลว์เฮดเดอร์ และสำหรับแหล่งที่อยู่ปลายทาง (destination address) และพอร์ต x_i เราสามารถคำนวณได้ดังนี้

$$p(x_i) = \frac{Number\ of\ pkts\ with\ x_i\ as\ src\ (dest)\ address\ (port)}{Total\ number\ of\ pkts}$$

อีกสองกรณีที่ต้องทำการนวณในงานวิจัยนี้ซึ่งอยู่ในพฤติกรรมการเชื่อมต่อสื่อสารกับโฮสภายนอกเราพิจารณาทั้งขาเข้าและขาออกของไอพีแอดเดรสภายใต้เครือข่ายเดียวกัน สำหรับโฮส X ขาออกถือข้อมูลไอพีแอดเดรสที่ทำการติดต่อไปยัง X และโฮส X ขาเข้าถือเป็นไอพีแอดเดรสที่ X ทำการติดต่อเข้ามาสำหรับ 2 กรณีนี้เราจะใช้การเชื่อมต่อแบบสองทิศทางทั้งโฮสขาเข้าและขาออกทั้งหมดคือค่า x_i และเราสามารถคำนวณได้ดังสมการต่อไปนี้

$$p(x_i) = \frac{Number\ of\ host\ with\ out - degree\ x_i}{Total\ number\ of\ host}$$

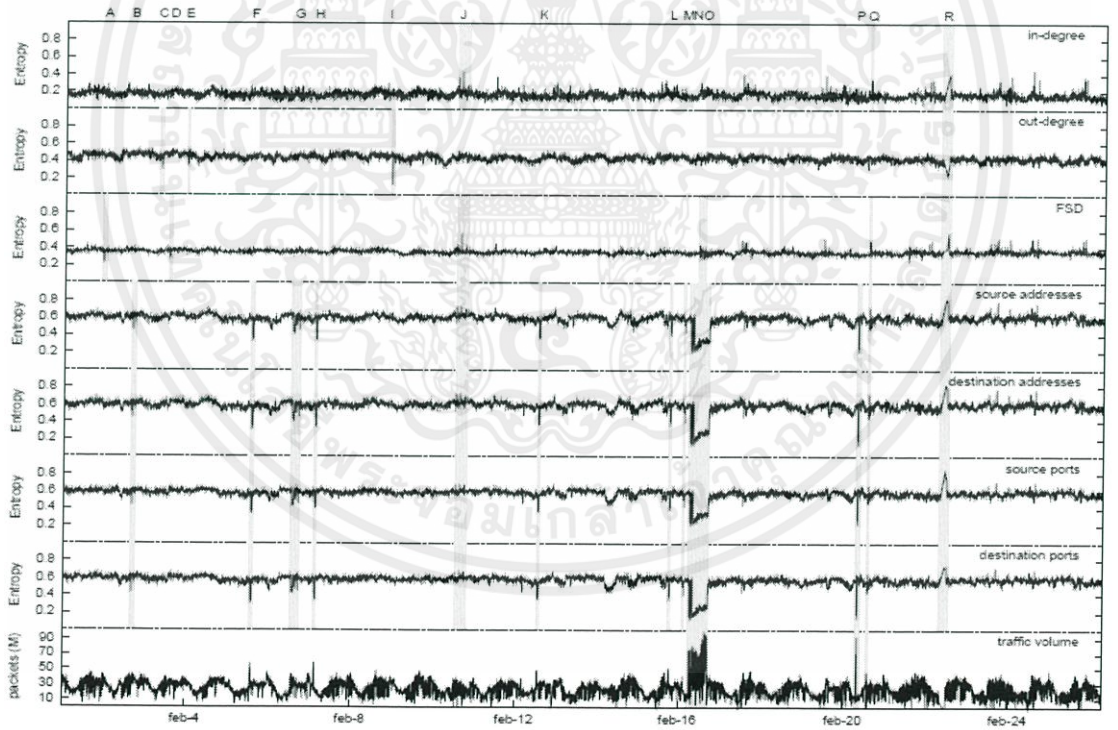
ตัวประกอบมาตรฐานของสมการนี้คือ $\log(D)$ เมื่อ D คือค่าของการเข้าและออกของโฮสในระยะเวลาที่กำหนด

ความสัมพันธ์ของอนุกรมเวลากับเอนโทรปีในรูปที่ 2.14 แสดงถึงค่าของความสัมพันธ์ระหว่างอนุกรมเวลากับเอนโทรปีของการกระจายที่ต่างกันออกไป เราพบความสัมพันธ์ของค่าเอนโทรปีในระดับสูง (>0.95) ซึ่งเกิดขึ้นระหว่างแอดเดรสกับพอร์ตส่วนตัวชี้วัดที่เหลือแสดงให้เห็นถึงความสัมพันธ์ในระดับที่ต่ำมาก

	Out Deg	Src Addr	Dst Addr	Src Port	Dst Port	FSD
InDeg	0.102	0.100	0.097	0.000	0.007	0.414
OutDeg	-	-0.034	-0.033	-0.054	-0.015	-0.018
SrcAddr	-	-	0.994	0.962	0.956	0.307
DstAddr	-	-	-	0.966	0.969	0.286
SrcPort	-	-	-	-	0.989	0.171
DstPort	-	-	-	-	-	0.181

รูปที่ 2.15 ความสัมพันธ์ระหว่างเอนโทรปีกับอนุกรมเวลาในชุดข้อมูลของ CMU-2005

ในรูปที่ 2.16 แสดงค่าอนุกรมเวลากับเอนโทรปีของทั้งเดือนจากรูปสามารถยืนยันได้ว่าความสัมพันธ์เป็นค่าที่มีเพียงหนึ่งเดียวโดยเป็นไปตามแกนเวลา นอกจากที่เราจะเห็นได้ว่าจะมีค่าที่เปลี่ยนแปลงอย่างรวดเร็วคล้ายๆกันหมด แสดงให้เห็นถึงความผิดปกติที่เกิดขึ้นในเวลาเดียวกันได้อย่างชัดเจน



รูปที่ 2.16 ความสัมพันธ์ระหว่างเอนโทรปีกับอนุกรมเวลาในเดือนกุมภาพันธ์

บทที่ 3
การออกแบบและการพัฒนา

การออกแบบและพัฒนาโปรแกรมเป็นขั้นตอนที่วางโครงสร้างของโปรแกรมว่าจะมีส่วนประกอบอะไรบ้าง และแต่ละส่วนมีการทำงานอย่างไร และมีขั้นตอนการทำงานอย่างไร โดยมีการใช้เครื่องมือต่างๆ มาช่วยในการพัฒนาโดยมีรายละเอียดดังต่อไปนี้

3.1 รายละเอียดของระบบ

การออกแบบและการพัฒนาระบบ จะต้องพิจารณาถึงรายละเอียดของระบบ ขั้นตอนการทำงานต่างๆ ของโปรแกรม รวมไปถึงการแสดงผลลัพธ์ของการวิเคราะห์ของโปรแกรมจะต้องมีความใกล้เคียงกับปัญหาที่เกิดขึ้นจริงของระบบในขณะนั้นด้วย

3.1.1 รายละเอียดการนำเข้าข้อมูล (Input Specification)

ข้อมูลที่นำเข้าสู่ระบบเพื่อนำมาใช้ในการวิเคราะห์ได้จากการดึงข้อมูลเครือข่ายผ่านโพรโทคอลเอสเอ็นเอ็มพีจากอุปกรณ์ในเครือข่ายโดยตรง

3.1.2 รายละเอียดผลลัพธ์ของระบบ (Output Specification)

ส่วนแสดงผลข้อมูลจะสามารถแสดงกราฟของข้อมูลที่ผ่านการวิเคราะห์ด้วยเอนโทรปี โดยผู้ใช้จะสามารถกำหนดอุปกรณ์เครือข่ายที่ต้องการแสดงผล กำหนดโปรไฟล์และช่วงเวลาของการแสดงผลได้เอง ทำให้ผู้ใช้สามารถวิเคราะห์ความผิดปกติของการใช้งานบนระบบเครือข่ายจากกราฟเอนโทรปีของข้อมูลนี้ได้ อีกทั้งยังสามารถแสดงผลกราฟของข้อมูลจริงที่นำมาวิเคราะห์ได้อีกด้วย

3.1.3 ขอบเขตของระบบที่พัฒนา

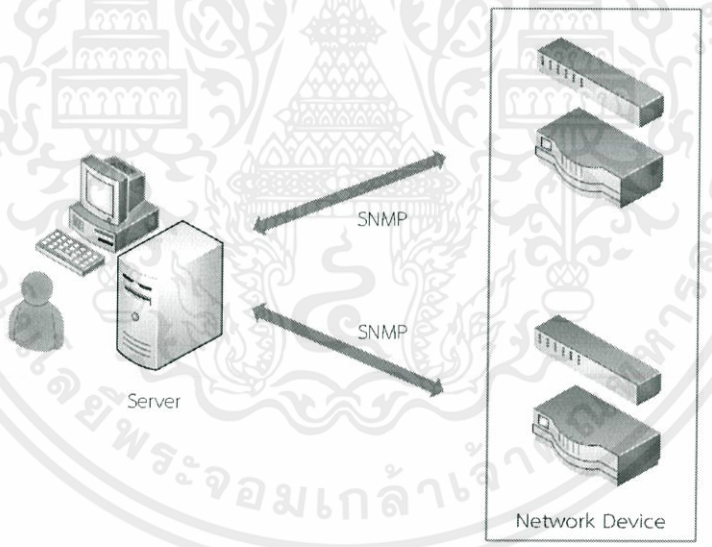
1) โปรแกรมนี้ถูกพัฒนาขึ้นบนระบบปฏิบัติการวินโดว์ จึงสามารถทำงานให้มีประสิทธิภาพสูงสุดสำหรับบนระบบปฏิบัติการวินโดว์เท่านั้น
2) การนำเข้าข้อมูลจากอุปกรณ์เครือข่าย จะต้องอาศัยการดึงข้อมูลผ่านโพรโทคอลเอสเอ็นเอ็มพีเท่านั้น ดังนั้นอุปกรณ์เครือข่ายที่ต้องการมอนิเตอร์จะต้องสนับสนุนการทำงานของโพรโทคอลเอสเอ็นเอ็มพีด้วย

3.1.4 เครื่องมือที่ใช้ในการพัฒนา

1) ระบบปฏิบัติการที่ใช้ คือ ระบบปฏิบัติการวินโดว์ เนื่องจากเป็นระบบปฏิบัติการที่มีการใช้งานอย่างแพร่หลาย และง่ายต่อการใช้งานและพัฒนา
2) ภาษาที่ใช้ในการพัฒนา คือ ภาษาจาวา
3) ระบบฐานข้อมูลที่ใช้ คือ มายเอสคิวแอล (MySQL)
4) อุปกรณ์เครือข่ายของสาขาวิชา ได้แก่ Cisco Catalyst 4006

3.2 โครงสร้างของระบบ

โครงสร้างของระบบจะประกอบไปด้วยเครื่องเซิร์ฟเวอร์ซึ่งทำหน้าที่คอยรับข้อมูลเครือข่ายจากอุปกรณ์เครือข่ายที่เป็นแกนหลักของระบบเครือข่ายโดยตรงผ่านโพรโทคอลเอสเอ็นเอ็มพี จากนั้นระบบจะนำข้อมูลที่ได้มาวิเคราะห์คำนวณหาค่าเอนโทรปีและแสดงผลเอนโทรปีของข้อมูลให้ผู้ใช้สามารถตรวจสอบหาความผิดปกติที่เกิดขึ้นบนระบบเครือข่ายได้



รูปที่ 3.1 โครงสร้างของระบบ

ระบบตรวจจับความผิดปกติในระบบเครือข่ายโดยอาศัยการเปลี่ยนแปลงเอนโทรปี มีส่วนประกอบหลักของการทำงาน แบ่งออกเป็น 4 ส่วนหลักดังต่อไปนี้

1) ส่วนการเก็บข้อมูลจากอุปกรณ์บนเครือข่าย
2) ส่วนติดต่อฐานข้อมูล
3) ส่วนการคำนวณเอนโทรปี
4) ส่วนการติดต่อกับผู้ใช้งาน

รูปที่ 3.2 การทำงานของระบบ

3.2.1 ส่วนการเก็บข้อมูลจากอุปกรณ์บนเครือข่าย

ส่วนการเก็บข้อมูลจากอุปกรณ์เครือข่าย จะมีการร้องขอข้อมูลของปริมาณการใช้งานเครือข่ายจากอุปกรณ์เครือข่ายที่เป็นแกนหลักของระบบ เช่น เราท์เตอร์ หรือ สวิตช์ ซึ่งข้อมูลเหล่านี้เป็นข้อมูลที่มีเก็บอยู่ในตัวอุปกรณ์เครือข่ายอยู่แล้ว การเก็บข้อมูลจากอุปกรณ์เครือข่ายจึงทำได้โดยใช้โพรโทคอลเอสเอ็นเอ็มพีดึงข้อมูลเหล่านั้นมา และข้อมูลเหล่านั้นจะถูกเก็บลงในฐานข้อมูลต่อไป

ตัวอย่างอุปกรณ์เครือข่ายที่จะนำมาใช้ในการมอนิเตอร์ตรวจตราดูปริมาณการใช้งานเครือข่าย จะแสดงในตารางที่ 3.1

ตารางที่ 3.1 รายชื่ออุปกรณ์ที่ใช้

ชื่ออุปกรณ์	ไอพีแอดเดรส	ประเภทอุปกรณ์
CE-Switch	161.246.66.254/24	Switch
emerald	161.246.4.254/24	Multi-Layer Switch
emerald	161.246.5.254/24	Multi-Layer Switch
emerald	161.246.6.254/24	Multi-Layer Switch

ตัวแปรหลักที่นำมาใช้ในการดึงข้อมูลจากอุปกรณ์เครือข่าย จะแสดงในตารางที่ 3.2

ตารางที่ 3.2 Object Descriptor และ OID

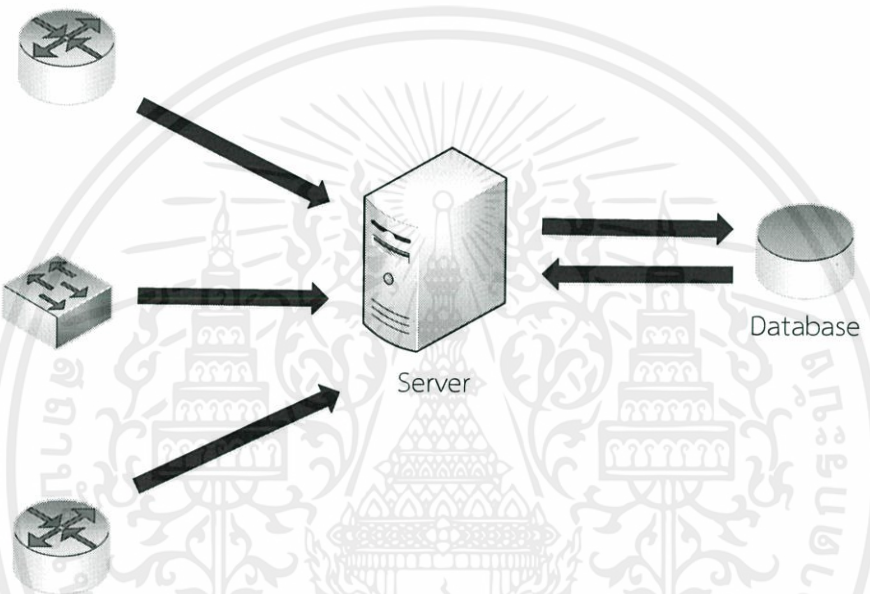
Object Descriptor	OID
sysDescr	1.3.6.1.2.1.1.1
sysName	1.3.6.1.2.1.1.5
ifNumber	1.3.6.1.2.1.2.1
ifIndex	1.3.6.1.2.1.2.2.1.1
ifInOctets	1.3.6.1.2.1.2.2.1.10
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11
ifOutOctets	1.3.6.1.2.1.2.2.1.16
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17
ifOutQLen	1.3.6.1.2.1.2.2.1.21

ความหมายของตัวแปรหลักที่นำมาใช้ในการดึงข้อมูลจากอุปกรณ์เครือข่าย

1) sysDescr หมายถึง รายละเอียดของอุปกรณ์
2) sysName หมายถึง ชื่อของอุปกรณ์
3) ifNumber หมายถึง จำนวนอินเทอร์เฟสทั้งหมดในระบบ
4) ifIndex หมายถึง หมายเลขที่ไม่ซ้ำกันของแต่ละอินเทอร์เฟส
5) ifInOctets หมายถึง จำนวนข้อมูลทั้งหมดในหน่วยไบต์ ที่รับเข้ามาในอินเทอร์เฟสนี้ ข้อมูลนั้นจะรวมส่วนประกอบของเฟรมด้วย
6) ifInUcastPkts หมายถึง จำนวนของแพ็คเก็ตขาเข้าทั้งหมดที่ได้รับมาจากการส่งข้อมูลแบบยูนิแคส (unicast) เช่น subnetwork-unicast จากกลุ่มเน็ตเวิร์กย่อย เพื่อถูกส่งต่อไปยังโพรโทคอลชั้นสูงกว่า (higher-level protocol)
7) ifOutOctets หมายถึง จำนวนข้อมูลทั้งหมดในหน่วยไบต์ ที่ส่งออกไปจากอินเทอร์เฟสนี้ ข้อมูลนั้นจะรวมส่วนประกอบของเฟรมด้วย
8) ifOutUcastPkts หมายถึง จำนวนของแพ็คเก็ตขาออกทั้งหมดที่โพรโทคอลในชั้นสูงกว่า (higher-level protocol) ถูกร้องขอให้ส่งออกไปยังเครือข่ายย่อยแบบยูนิแคส (unicast) เช่น subnetwork-unicast address รวมไปถึงแพ็คเก็ตที่ถูกคัดทิ้งหรือไม่ได้ส่งด้วย
9) ifOutQLen หมายถึง ความยาวของแถวคอย (queue) ที่ใช้ส่งแพ็คเก็ตออก

3.2.2 ส่วนติดต่อฐานข้อมูล

ส่วนติดต่อฐานข้อมูลเป็นส่วนที่มีการบันทึกค่าการใช้งานระบบเครือข่ายที่ได้มาจากอุปกรณ์บนเครือข่ายโดยตรง การเก็บข้อมูลในฐานข้อมูลนี้จึงเป็นข้อมูลจริงที่ไม่ได้ผ่านการคำนวณหรือมีการตัดทอนข้อมูลใดๆ ล่วงหน้า เนื่องจากฐานข้อมูลจะต้องมีการติดต่อกับส่วนผู้ใช้งานโดยตรงในภายหลัง กล่าวคือ เมื่อผู้ใช้ต้องการแสดงผลลัพธ์ของข้อมูลในช่วงเวลาใดก็ตาม ระบบจะต้องสามารถดึงข้อมูลในช่วงเวลาที่ต้องการนั้นมาทำการวิเคราะห์และคำนวณเอนโทรปีให้แก่ผู้ใช้งานได้ทุกช่วงเวลานั่นเอง



รูปที่ 3.3 โครงสร้างการติดต่อฐานข้อมูล

การออกแบบฐานข้อมูลของระบบ ถูกออกแบบมาเพื่อให้สามารถเก็บข้อมูลโดยเกิดความซ้ำซ้อนกันของข้อมูลน้อยที่สุด สามารถแบ่งออกได้เป็น 4 ตาราง ดังนี้

1) ตาราง Raw_Data ประกอบด้วย 7 attributes ดังนี้
   - RouterID คือ หมายเลขเฉพาะของอุปกรณ์แต่ละตัว โดยจะมีค่าไม่ซ้ำกัน
   - ProfileID คือ หมายเลขเฉพาะของแต่ละโปรไฟล์ บนอุปกรณ์แต่ละตัวอาจมีได้หลากหลายโปรไฟล์ ซึ่งแต่ละโปรไฟล์ของอุปกรณ์นั้นๆ จะมีค่าไม่ซ้ำกัน
   - OID คือ ชุดของตัวเลขจำนวนเต็มฐานสิบที่คั่นด้วยจุด ซึ่งจะใช้แทนตำแหน่งของอ็อบเจ็คในฐานข้อมูลมิบ
   - Value คือ ผลลัพธ์ที่ได้
   - Type คือ ชนิดของข้อมูลซึ่งกำหนดรายละเอียดของแต่ละอ็อบเจ็ค
   - WalkingGroup คือ หมายเลขแสดงครั้งที่มีการบันทึกข้อมูลลงในฐานข้อมูล

- TimeStamp คือ เวลาขณะที่มีการบันทึกข้อมูลลงในฐานข้อมูล

2) ตาราง Router ประกอบด้วย 4 attributes ดังนี้
   - RouterID คือ หมายเลขเฉพาะของอุปกรณ์แต่ละตัว โดยจะมีค่าไม่ซ้ำกัน
   - RouterIP คือ IP Address ของอุปกรณ์ที่นำมาใช้มอนิเตอร์
   - RouterName คือ ชื่อของอุปกรณ์ที่นำมาใช้มอนิเตอร์
   - Community คือ Community String ของแต่ละอุปกรณ์
3) ตาราง Profile ประกอบด้วย 3 attributes ดังนี้
   - RouterID คือ หมายเลขเฉพาะของอุปกรณ์แต่ละตัว โดยจะมีค่าไม่ซ้ำกัน
   - ProfileID คือ หมายเลขเฉพาะของแต่ละโปรไฟล์ บนอุปกรณ์แต่ละตัวอาจมีได้หลากหลายโปรไฟล์ ซึ่งแต่ละโปรไฟล์ของอุปกรณ์นั้นๆ จะมีค่าไม่ซ้ำกัน
   - ProfileName คือ ชื่อของแต่ละโปรไฟล์
4) ตาราง OID ประกอบด้วย 4 attributes ดังนี้
   - RouterID คือ หมายเลขเฉพาะของอุปกรณ์แต่ละตัว โดยจะมีค่าไม่ซ้ำกัน
   - ProfileID คือ หมายเลขเฉพาะของแต่ละโปรไฟล์ บนอุปกรณ์แต่ละตัวอาจมีได้หลากหลายโปรไฟล์ ซึ่งแต่ละโปรไฟล์ของอุปกรณ์นั้นๆ จะมีค่าไม่ซ้ำกัน
   - OID คือ ชุดของตัวเลขจำนวนเต็มฐานสิบที่คั่นด้วยจุด ซึ่งจะใช้แทนตำแหน่งของอ็อบเจ็คในฐานข้อมูลมิบ
   - Type คือ ชนิดของข้อมูลซึ่งกำหนดรายละเอียดของแต่ละอ็อบเจ็ค

3.2.3 ส่วนการคำนวณเอนโทรปี

ส่วนการคำนวณเอนโทรปีเป็นส่วนที่ดึงข้อมูลจากฐานข้อมูล ซึ่งมีการเก็บข้อมูลมาจากอุปกรณ์เครือข่ายมาก่อน โดยนำข้อมูลที่ได้จากฐานข้อมูลมาคำนวณหาค่าเอนโทรปีของข้อมูลแต่ละชุด

การคำนวณเอนโทรปีของข้อมูลจะเป็นไปตามสมการหลัก คือ

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log P(x_i)$$

การคำนวณเอนโทรปีจะอาศัยค่าที่ได้จากโพรโทคอลเอสเอ็นเอ็มพีซึ่งมีข้อมูลหลากหลายชนิด และเนื่องจากข้อมูลชนิดเคาท์เตอร์ (Counter) เป็นตัวเลขจำนวนเต็มบวกซึ่งมีขนาด 32 บิต ทำให้มีค่า

อยู่ระหว่าง 0 - 2^{32} (4,294,967,295) โดยจะมีค่าที่เพิ่มขึ้นเรื่อยๆ ไม่มีการลดค่า และเมื่อค่าเพิ่มขึ้นจนถึงค่าสูงสุดหรือเมื่อมีการเริ่มต้นระบบใหม่ (reboot) ข้อมูลชนิดนี้จะกลับมาเริ่มต้นที่ศูนย์ใหม่อีกครั้ง เช่น ใช้ในการนับจำนวนแพ็คเก็ตขาข้าวของการ์ดอินเทอร์เฟส ดังนั้นการนำข้อมูลชนิดเคาท์เตอร์มาใช้ในการคำนวณเอนโทรปีจึงแตกต่างไปจากข้อมูลชนิดอื่นๆ ระบบจึงแบ่งลักษณะการคำนวณเอนโทรปีออกเป็น 2 ประเภท คือ ส่วนการคำนวณเอนโทรปีของข้อมูลชนิดทั่วไป และ ส่วนการคำนวณเอนโทรปีของข้อมูลชนิดเคาท์เตอร์

3.2.3.1 ส่วนการคำนวณเอนโทรปีของข้อมูลชนิดทั่วไป

การคำนวณเอนโทรปีของข้อมูลชนิดทั่วไปมีขั้นตอนดังนี้

1) ดึงข้อมูลของโปรไฟล์ที่อยู่ในช่วงเวลาที่ต้องการมาจากฐานข้อมูล ซึ่งข้อมูลแต่ละโปรไฟล์อาจมีตัวแปร OID ได้หลายค่าและหลายชนิดได้
2) นำข้อมูลของโปรไฟล์นั้นมาทีละ WalkingGroup ซึ่งคือครั้งที่มีการบันทึกข้อมูลตามที่กำหนดไว้ในฐานข้อมูล โดยเริ่มจาก WalkingGroup ที่มีค่าน้อยที่สุดไล่ไปค่ามากที่สุดตามลำดับ
3) นำข้อมูลแต่ละ OID ของ WalkingGroup นั้นๆ มาคำนวณหาค่าเฉลี่ยแบบถ่วงน้ำหนัก ทั้งนี้เนื่องจากการคำนวณเอนโทรปีต้องการให้ความสำคัญกับข้อมูลที่ผ่านมาในอดีตให้เป็นตัวแปรหนึ่งในการวิเคราะห์ลักษณะการเปลี่ยนแปลงของข้อมูล ทำให้การวิเคราะห์ข้อมูลไม่ยึดติดเฉพาะกับข้อมูลปัจจุบันเพียงอย่างเดียว การคำนวณหาค่าเฉลี่ยแบบถ่วงน้ำหนักเป็นไปตามสมการคือ

$$\overline{X_t} = (\alpha \times X_t) + \left(\beta \times \overline{X_{t-1}}\right) \text{ โดยที่ } \alpha + \beta = 1$$

โดย $\overline{X_t}$ คือ ค่าเฉลี่ยแบบถ่วงน้ำหนักของข้อมูลปัจจุบัน

α คือ น้ำหนักที่ให้ความสำคัญกับข้อมูลปัจจุบัน

β คือ น้ำหนักที่ให้ความสำคัญกับค่าเฉลี่ยแบบถ่วงน้ำหนักของข้อมูลที่ผ่านมาในอดีต

X_t คือ ข้อมูลปัจจุบัน

$\overline{X_{t-1}}$ คือ ค่าเฉลี่ยแบบถ่วงน้ำหนักของข้อมูลที่ผ่านมาในอดีต

4) ทำสมูทติ้ง (Smoothing) เพื่อลดการแกว่งของข้อมูล เป็นการจัดระเบียบข้อมูลให้ข้อมูลที่ใกล้เคียงกันอยู่ในระดับเดียวกันมากขึ้น ช่วยให้สามารถสังเกตบางข้อมูลที่มีค่าแตกต่างจากข้อมูลอื่นๆได้ง่ายมากยิ่งขึ้น โดยนำค่าข้อมูลจริงของแต่ละ OID ในแต่ละ WalkingGroup ที่ได้จากข้อ 2) มาหารด้วยค่าเฉลี่ยแบบถ่วงน้ำหนักของข้อมูลที่มี OID และ WalkingGroup

เดียวกันที่ได้จากข้อ 3) จะได้ผลลัพธ์เป็นค่าที่ผ่านการทำสมูทติ้งของแต่ละ OID ในแต่ละ WalkingGroup สำหรับโปรไฟล์นั้นๆ

5) คำนวณผลรวมที่ได้จากข้อ 4) จะได้ผลลัพธ์คือผลรวมของค่าที่ผ่านการทำสมูทติ้งทั้งหมดทุก OID ที่เป็นองค์ประกอบในโปร์ไฟล์นั้นๆ ของแต่ละ WalkingGroup

6) คำนวณหาค่าเอนโทรปีของข้อมูลตามสมการหลัก คือ

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log P(x_i)$$

โดย $P(x_i)$ คือ ค่าที่ผ่านการทำสมูทติ้งของแต่ละ OID ในแต่ละ WalkingGroup ที่ได้จากข้อ 4) หารด้วยผลรวมของค่าที่ผ่านการทำสมูทติ้งทั้งหมดทุก OID ที่เป็นองค์ประกอบในโปร์ไฟล์นั้นๆ ของ WalkingGroup เดียวกันที่ได้จากข้อ 5)

3.2.3.2 ส่วนการคำนวณเอนโทรปีของข้อมูลชนิดเคาท์เตอร์

เนื่องจากข้อมูลชนิดเคาท์เตอร์มีค่าอยู่ระหว่าง 0 - 2^{32} โดยจะมีค่าที่เพิ่มขึ้นเรื่อยๆ ไม่มีการลดค่า และเมื่อค่าเพิ่มขึ้นจนถึงค่าสูงสุดหรือเมื่อมีการเริ่มต้นระบบใหม่ (reboot) ข้อมูลชนิดนี้จะกลับมาเริ่มต้นที่ศูนย์ใหม่อีกครั้ง ทำให้การคำนวณเอนโทรปีของข้อมูลชนิดเคาท์เตอร์แตกต่างจากข้อมูลชนิดทั่วไป โดยการคำนวณเอนโทรปีของข้อมูลชนิดเคาท์เตอร์มีขั้นตอนดังนี้

1) ดึงข้อมูลของโปรไฟล์ที่อยู่ในช่วงเวลาที่ต้องการมาจากฐานข้อมูล ซึ่งข้อมูลแต่ละโปรไฟล์อาจมีตัวแปร OID ได้หลายค่าและหลายชนิดได้

2) นำข้อมูลของโปรไฟล์นั้นมาทีละ WalkingGroup ซึ่งคือครั้งที่มีการบันทึกข้อมูลตามที่กำหนดไว้ในฐานข้อมูล โดยเริ่มจาก WalkingGroup ที่มีค่าน้อยที่สุดไล่ไปค่ามากที่สุดตามลำดับ

3) คำนวณหาผลต่างของข้อมูล โดยการนำค่าข้อมูลจริงของแต่ละ OID ของ WalkingGroup ที่พิจารณาอยู่ในปัจจุบัน ลบด้วยค่าข้อมูลจริงของ OID เดียวกันของ WalkingGroup ที่ผ่านมา แต่ถ้าข้อมูลในปัจจุบันมีค่าน้อยกว่าข้อมูลที่ผ่านมา การคำนวณหาผลต่างของข้อมูลจะมีค่าเท่ากับ 2^{32} – ข้อมูลที่ผ่านมา + ข้อมูลในปัจจุบัน

4) นำค่าผลต่างของแต่ละ OID สำหรับ WalkingGroup ที่พิจารณาอยู่ที่ได้จากข้อ 3) มาทำการคำนวณหาค่าเฉลี่ยแบบถ่วงน้ำหนัก เนื่องจากการคำนวณเอนโทรปีต้องการให้ความสำคัญกับข้อมูลที่ผ่านมาในอดีตให้เป็นตัวแปรหนึ่งในการวิเคราะห์ลักษณะการเปลี่ยนแปลงของข้อมูล

ทำให้การวิเคราะห์ข้อมูลไม่ยึดติดเฉพาะกับข้อมูลปัจจุบันเพียงอย่างเดียว การคำนวณหาค่าเฉลี่ยแบบถ่วงน้ำหนักเป็นไปตามสมการคือ

$$\overline{X_t} = (\alpha \times X_t) + \left(\beta \times \overline{X_{t-1}}\right) \text{ โดยที่ } \alpha + \beta = 1$$

โดย $\overline{X_t}$ คือ ค่าเฉลี่ยแบบถ่วงน้ำหนักของผลต่างของข้อมูลที่พิจารณาในปัจจุบัน

α คือ น้ำหนักที่ให้ความสำคัญกับผลต่างของข้อมูลที่พิจารณาในปัจจุบัน

β คือ น้ำหนักที่ให้ความสำคัญกับค่าเฉลี่ยแบบถ่วงน้ำหนักของผลต่างข้อมูลที่ผ่านมา

X_t คือ ผลต่างของข้อมูลที่พิจารณาในปัจจุบัน

$\overline{X_{t-1}}$ คือ ค่าเฉลี่ยแบบถ่วงน้ำหนักของผลต่างของข้อมูลที่ผ่านมา

5) ทำสมูทติ้ง (Smoothing) เพื่อลดการแกว่งของข้อมูล เป็นการจัดระเบียบข้อมูลให้ข้อมูลที่ใกล้เคียงกันอยู่ในระดับเดียวกันมากขึ้น ช่วยให้สามารถสังเกตบางข้อมูลที่มีค่าแตกต่างจากข้อมูลอื่นๆ ได้ง่ายมากยิ่งขึ้น โดยนำค่าผลต่างข้อมูลของแต่ละ OID ในแต่ละ WalkingGroup ที่ได้จากข้อ 3) มาหารด้วยค่าเฉลี่ยแบบถ่วงน้ำหนักของผลต่างของข้อมูลที่มี OID และ WalkingGroup เดียวกันที่ได้จากข้อ 4) จะได้ผลลัพธ์เป็นค่าผลต่างที่ผ่านการทำสมูทติ้งของแต่ละ OID ในแต่ละ WalkingGroup สำหรับโปรไฟล์นั้นๆ
6) คำนวณผลรวมที่ได้จากข้อ 5) จะได้ผลลัพธ์คือผลรวมของค่าผลต่างที่ผ่านการทำสมูทติ้งทั้งหมดทุก OID ที่เป็นองค์ประกอบในโปร์ไฟล์นั้นๆ ของแต่ละ WalkingGroup
7) คำนวณหาค่าเอนโทรปีของข้อมูลตามสมการหลัก คือ

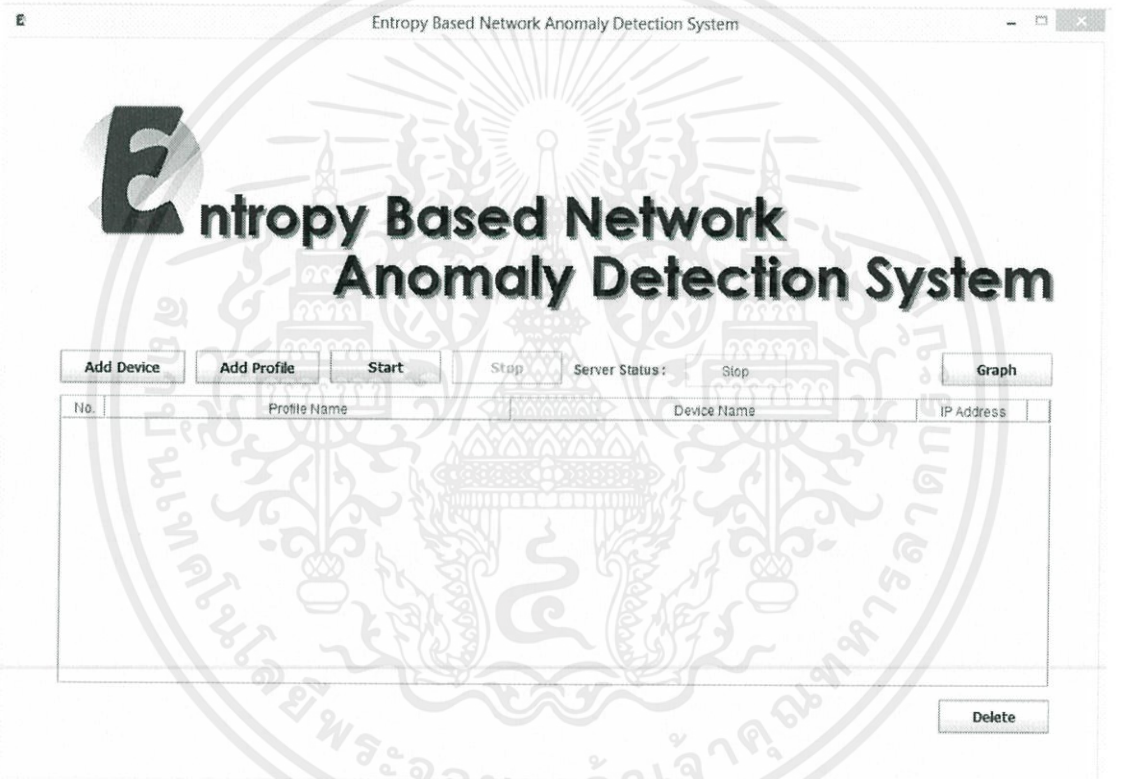
$$\mathrm{H(X)} = -\sum_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{P(x_i)\,logP(x_i)}$$

โดย $\mathrm{P(x_i)}$ คือ ค่าผลต่างที่ผ่านการทำสมูทติ้งของแต่ละ OID ในแต่ละ WalkingGroup ที่ได้จากข้อ 5) หารด้วยผลรวมของค่าผลต่างที่ผ่านการทำสมูทติ้งทั้งหมดทุก OID ที่เป็นองค์ประกอบในโปร์ไฟล์นั้นๆ ของ WalkingGroup เดียวกันที่ได้จากข้อ 6)

3.2.4 ส่วนการติดต่อกับผู้ใช้งาน

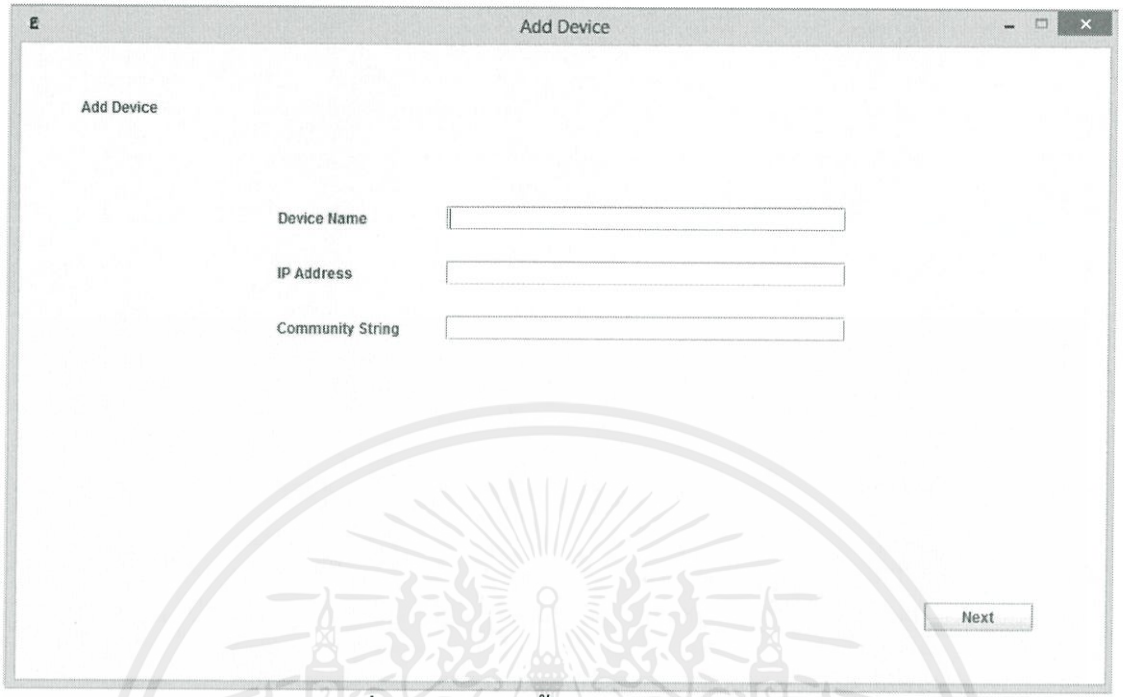
ส่วนการติดต่อกับผู้ใช้งานเป็นส่วนแสดงผลกับผู้ใช้งานโปรแกรม จะแสดงผลการใช้งานอุปกรณ์เครือข่าย โดยมีหน้าตาของโปรแกรมดังต่อไปนี้

1) ส่วนหน้าโปรแกรมหลัก เป็นส่วนที่ผู้ใช้จะเริ่มต้นการใช้งานโปรแกรม ผู้ใช้งานจะสามารถเพิ่มอุปกรณ์เครือข่ายที่ต้องการมอนิเตอร์ได้เอง สามารถเริ่มหรือหยุดการทำงานของอุปกรณ์เครือข่ายได้ สามารถแสดงผลการตรวจตราการใช้งานเครือข่ายได้ และแสดงรายละเอียดของอุปกรณ์และโปรไฟล์ทั้งหมดที่โปรแกรมถูกตั้งค่าเพื่อให้ทำการมอนิเตอร์ได้



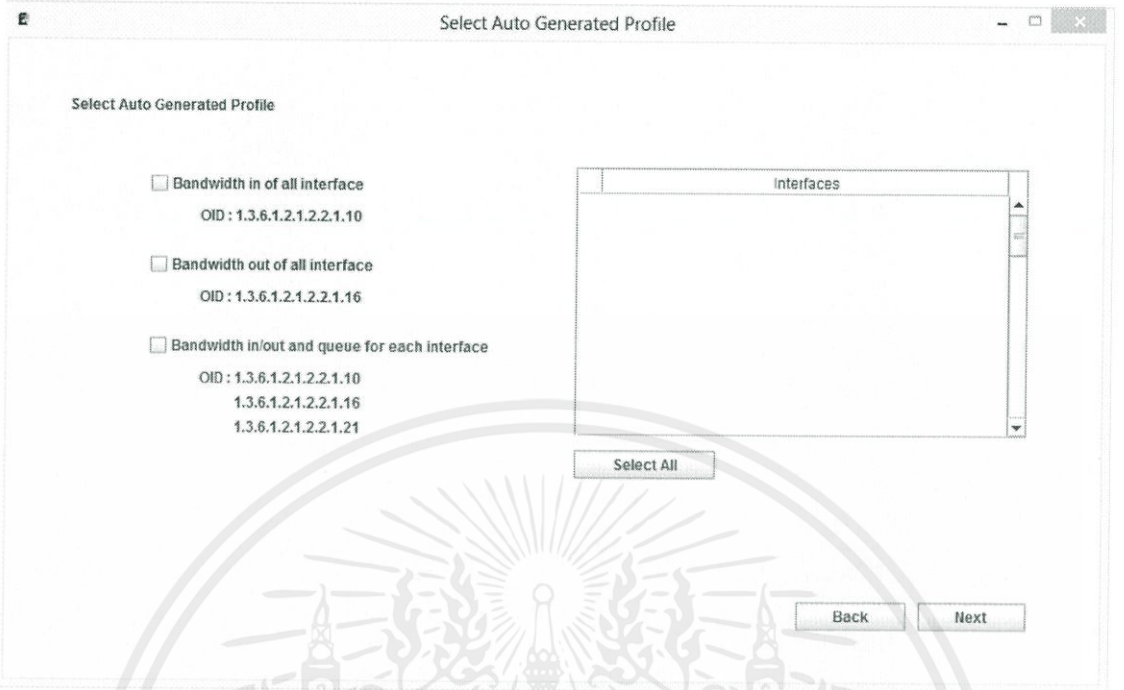
รูปที่ 3.4 หน้าโปรแกรมหลัก

2) ส่วนหน้าการตั้งค่าอุปกรณ์เครือข่าย เมื่อผู้ใช้งานต้องการเพิ่มอุปกรณ์เครือข่ายให้โปรแกรมทำการมอนิเตอร์ หน้าการตั้งค่าอุปกรณ์เครือข่ายนี้จะมีไว้ให้ผู้ใช้ตั้งค่าต่างๆ เกี่ยวกับอุปกรณ์เครือข่ายนั้นๆ ประกอบด้วย ชื่อของอุปกรณ์ (Device Name) ไอพีแอดเดรส (IP Address) และคอมมิวนิตี้สตริง (Community String)



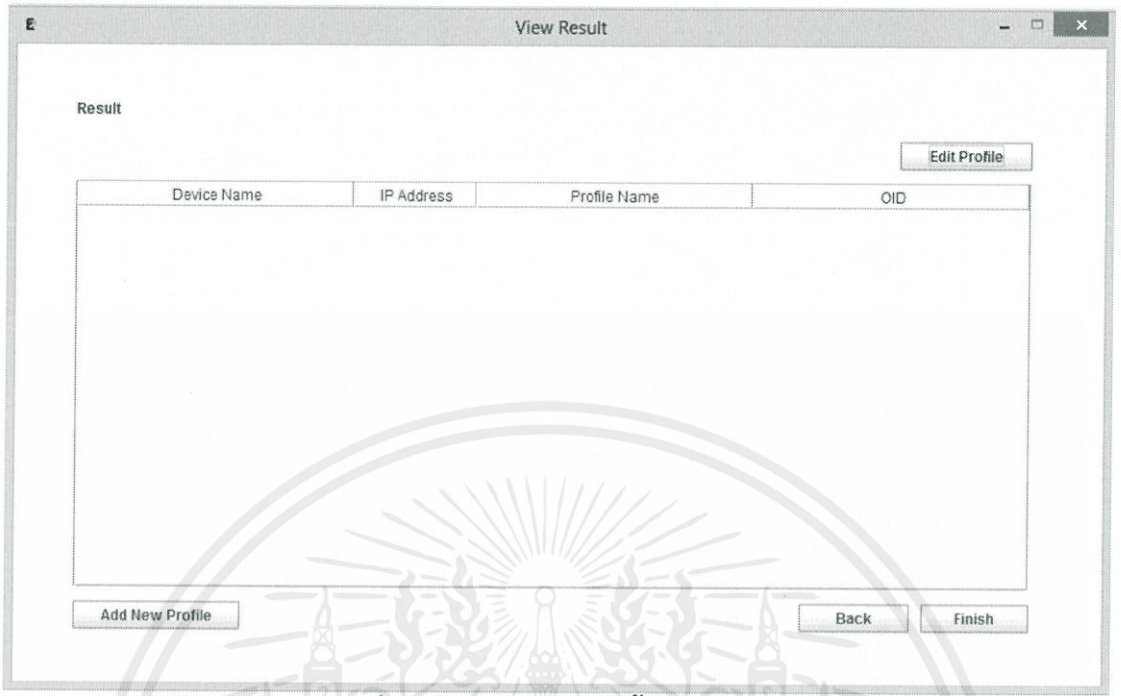
รูปที่ 3.5 หน้าการตั้งค่าอุปกรณ์เครือข่าย

3) ส่วนหน้าการกำหนดโปรไฟล์อัตโนมัติ (Auto Generated Profile) เป็นโปรไฟล์อัตโนมัติที่ผู้ใช้สามารถกำหนดให้อุปกรณ์ทำการมอนิเตอร์ได้ โดยที่ผู้ใช้ไม่จำเป็นต้องกำหนดโปรไฟล์เอง ในส่วนนี้จะประกอบด้วยชื่อของโปรไฟล์ (Profile Name)และหมายเลข OID ที่กำหนดไว้สำหรับโปรไฟล์นั้นๆ ผู้ใช้งานสามารถคลิกปุ่มหน้าชื่อของโปรไฟล์ได้ทันที สำหรับโปรไฟล์ Bandwidth in/out and queue for each interface เมื่อคลิกเลือกจะปรากฏหมายเลขอินเทอร์เฟสทั้งหมดของอุปกรณ์นั้นๆ ที่บริเวณพื้นที่ว่างสี่เหลี่ยมด้านขวา ดังรูปที่ 3.7 จากนั้นผู้ใช้งานจะสามารถเลือกอินเทอร์เฟสที่ต้องการมอนิเตอร์ได้



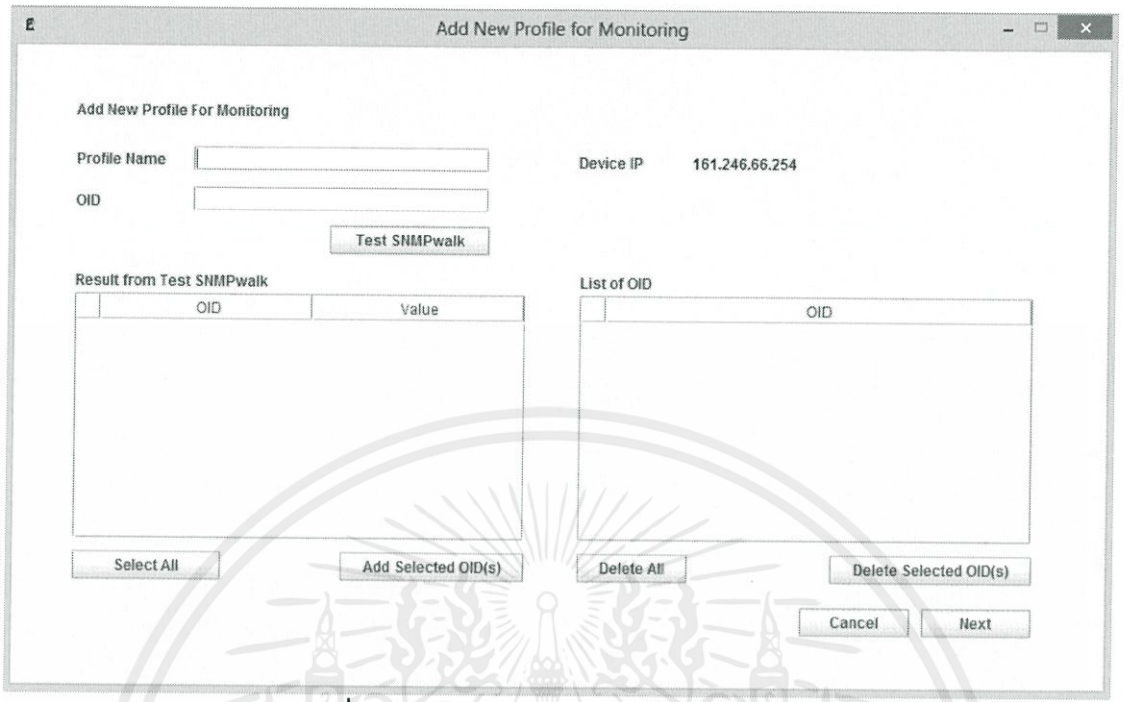
รูปที่ 3.6 หน้าการกำหนดโปรไฟล์อัตโนมัติ

4) ส่วนหน้าสรุปผลการตั้งค่าอุปกรณ์ จะแสดงผลการตั้งค่าทั้งหมดที่ผู้ใช้งานกำหนดให้อุปกรณ์นั้นใช้ในการมอนิเตอร์ ประกอบด้วย ชื่อของอุปกรณ์ (Device Name), ไอพีแอดเดรส (IP Address), ชื่อของโปรไฟล์ (Profile Name) และหมายเลข OID หากผู้ใช้งานต้องการกลับไปแก้ไขการกำหนดโปรไฟล์อัตโนมัติ จะสามารถคลิกปุ่ม Back เพื่อกลับไปตั้งค่าในส่วนหน้าการกำหนดโปรไฟล์อัตโนมัติได้ และหากผู้ใช้งานต้องการเพิ่มโปรไฟล์อื่นๆ ด้วยตนเอง ซึ่งอยู่นอกเหนือจากโปรไฟล์อัตโนมัติ จะสามารถคลิกปุ่ม Add New Profile



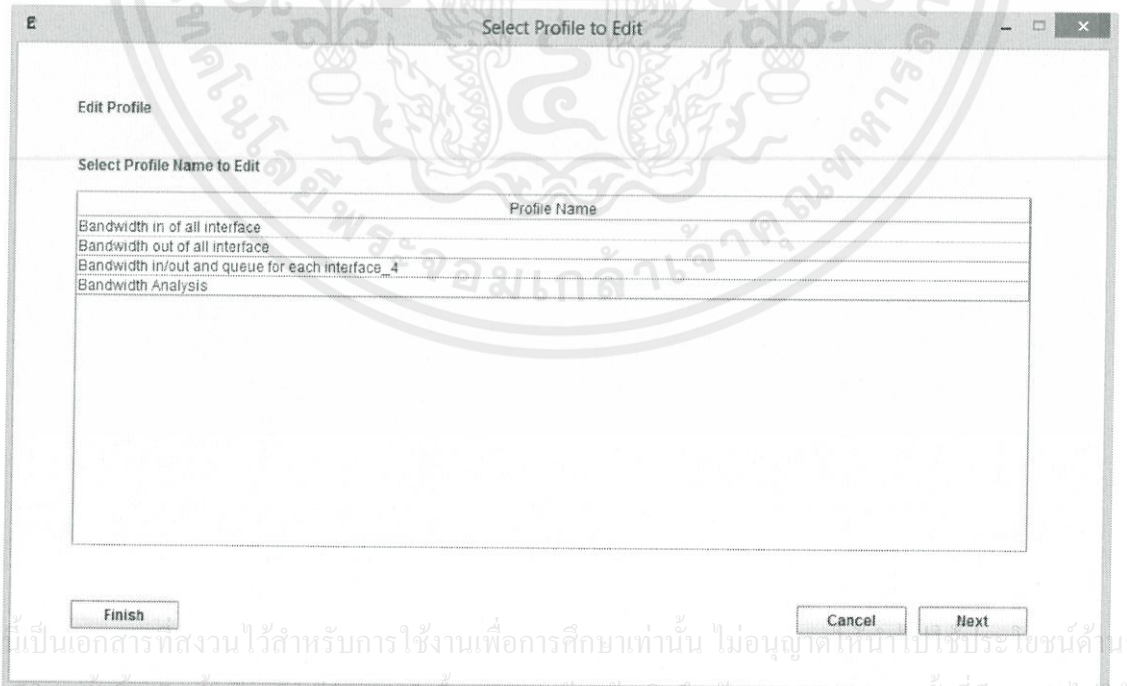
รูปที่ 3.7 หน้าสรุปผลการตั้งค่าอุปกรณ์

5) ส่วนหน้าการกำหนดโปรไฟล์ด้วยตนเอง ผู้ใช้งานสามารถกำหนดชื่อโปรไฟล์ (Profile Name) และหมายเลข OID สำหรับโปรไฟล์นั้นๆ ได้ตามต้องการ โดยผู้ใช้จะต้องกรอกหมายเลข OID ที่ต้องการลงในช่อง OID แล้วคลิกปุ่ม Test SNMPwalk เพื่อทดสอบว่าหมายเลข OID นั้นๆ สามารถนำมาใช้งานได้หรือไม่ ถ้าหมายเลข OID นั้นสามารถนำมาใช้งานได้ โปรแกรมจะแสดงหมายเลข OID ที่ผู้ใช้งานกรอกลงไปลงในตาราง Result from Test SNMPwalk ดังรูปที่ 3.9 หากผู้ใช้งานต้องการหมายเลข OID นี้ ผู้ใช้งานจะต้องคลิกเลือกหน้าหมายเลข OID ที่ต้องการ แล้วคลิกปุ่ม Add Selected OID(s) จะปรากฏหมายเลข OID ที่เลือกในตารางทางด้านขวา คือ ตาราง List of OID ผู้ใช้งานสามารถกรอกหมายเลข OID และทำการ Test SNMPwalk ได้หลายครั้ง จนกระทั่งกำหนดหมายเลข OID สำหรับโปรไฟล์นั้นๆ ได้ครบตามต้องการ จากนั้นคลิกปุ่ม Next เป็นการยืนยันการเพิ่มโปรไฟล์นั้นๆ โดยรายละเอียดจะแสดงในหน้าสรุปผลการตั้งค่าอุปกรณ์



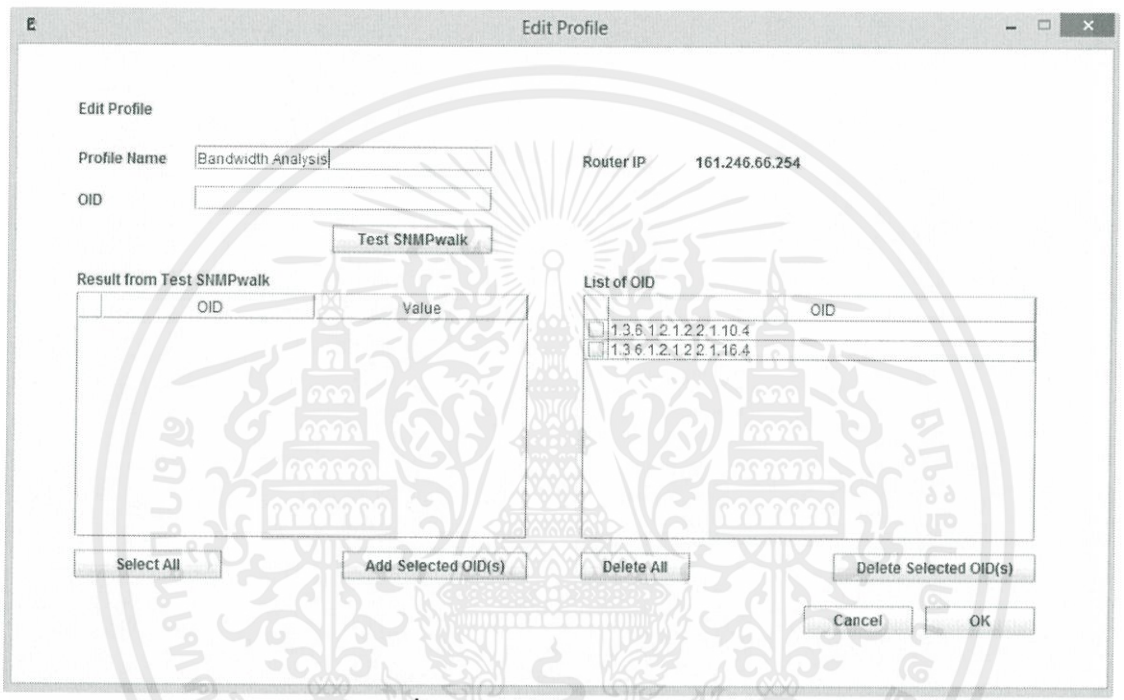
รูปที่ 3.8 หน้าการกำหนดโปรไฟล์ด้วยตนเอง

6) ส่วนหน้าการเลือกโปรไฟล์สำหรับแก้ไข ผู้ใช้งานสามารถแก้ไขโปรไฟล์ได้ โดยเลือกชื่อโปรไฟล์ (Profile Name) ที่ต้องการแก้ไข แล้วคลิกปุ่ม Next เพื่อเข้าสู่หน้าการแก้ไขโปรไฟล์



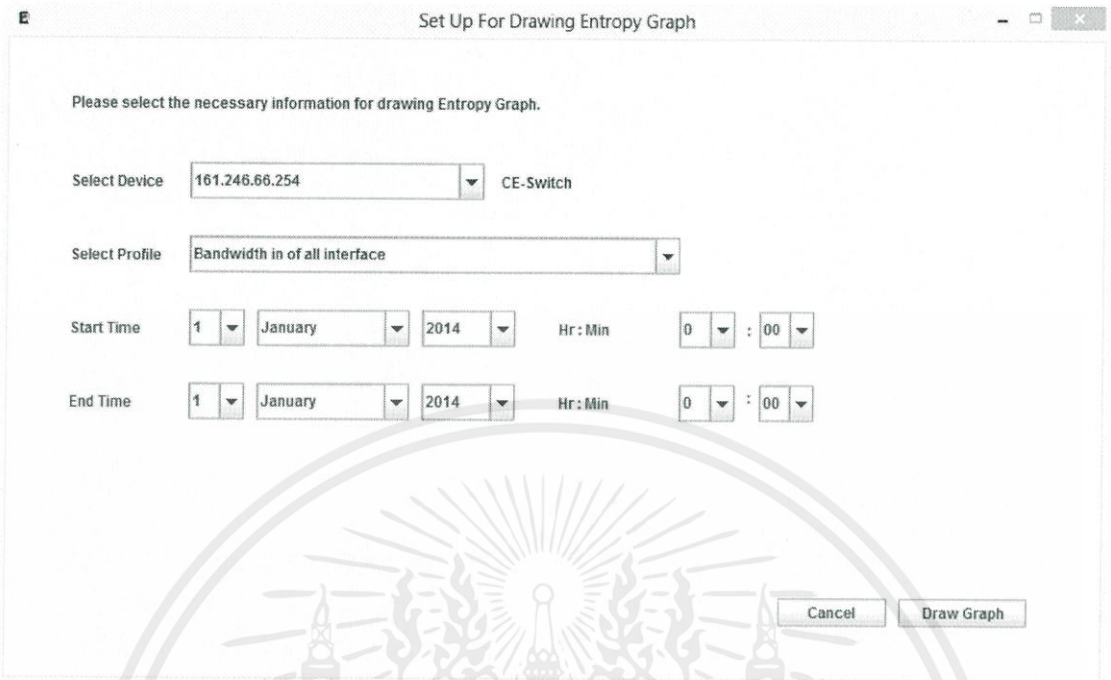
รูปที่ 3.9 หน้าการเลือกโปรไฟล์สำหรับแก้ไข

7) ส่วนหน้าการแก้ไขโปรไฟล์ เมื่อเข้าสู่หน้าแก้ไขโปรไฟล์ โปรแกรมจะแสดงชื่อโปรไฟล์ และหมายเลข OID ที่ผู้ใช้งานได้ทำการตั้งค่าไว้ครั้งล่าสุด ผู้ใช้งานสามารถแก้ไขชื่อของโปรไฟล์ รวมถึงเพิ่มหรือลบหมายเลข OID ได้ โดยมีหลักการทำงานคล้ายกับส่วนหน้าการกำหนดโปรไฟล์ด้วยตนเอง เมื่อแก้ไขโปรไฟล์นั้นเสร็จเรียบร้อยแล้วทำการคลิกปุ่ม OK โปรแกรมจะย้อนกลับมาส่วนหน้าการเลือกโปรไฟล์สำหรับแก้ไขอีกครั้ง หากผู้ใช้งานไม่ต้องการแก้ไข



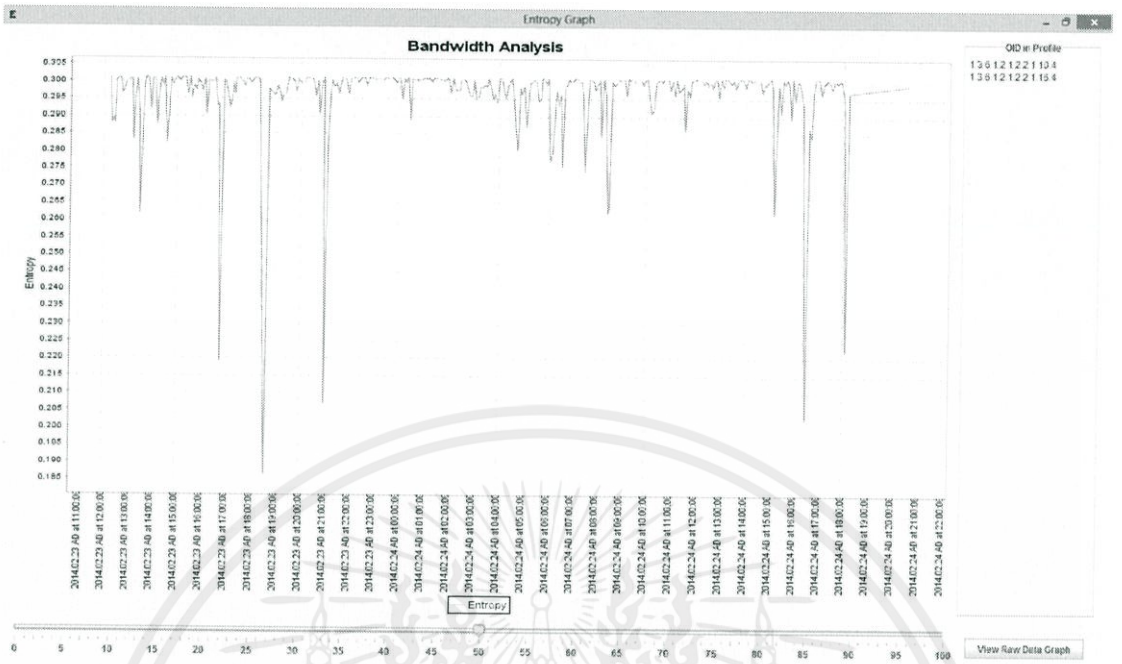
รูปที่ 3.10 หน้าการแก้ไขโปรไฟล์

8) ส่วนหน้าการตั้งค่าการแสดงผลกราฟเอนโทรปี ผู้ใช้สามารถกำหนดอุปกรณ์เครือข่ายที่ต้องการ, กำหนดโปรไฟล์ของอุปกรณ์นั้นๆ รวมถึงกำหนดช่วงเวลาที่ต้องการแสดงผลได้เอง เมื่อคลิกปุ่ม Draw Graph โปรแกรมจะทำการคำนวณเอนโทรปีของข้อมูลตามช่วงเวลาที่กำหนด และแสดงผลออกมาในรูปของกราฟเอนโทรปีของข้อมูล



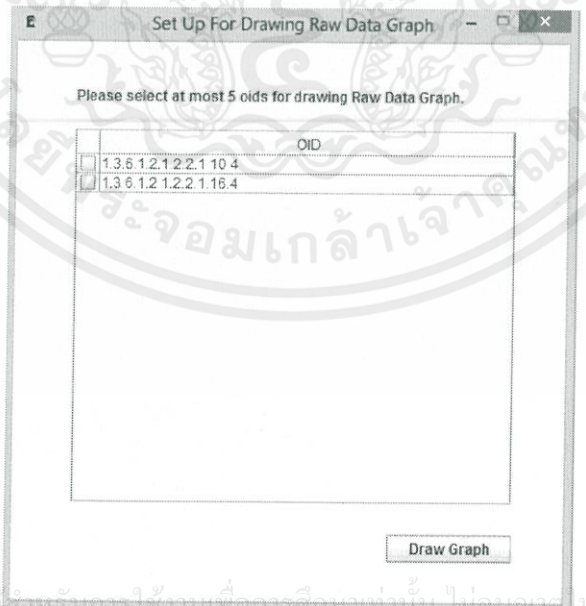
รูปที่ 3.11 หน้าการตั้งค่าการแสดงผลกราฟเอนโทรปี

9) ส่วนหน้าการแสดงผลกราฟเอนโทรปี ผู้ใช้งานสามารถสังเกตลักษณะความผิดปกติของกราฟเอนโทรปีเพื่อพิจารณาถึงความผิดปกติของการใช้งานในระบบเครือข่ายได้ อีกทั้งสามารถคลิกปุ่ม View Raw Data Graph เพื่อให้โปรแกรมแสดงผลกราฟของข้อมูลจริงของหมายเลข OID ที่เป็นองค์ประกอบของโปรไฟล์นั้นๆ ซึ่งเป็นข้อมูลที่ได้มาจากอุปกรณ์เครือข่ายโดยตรง ผู้ใช้งานจะสามารถนำกราฟของข้อมูลจริงเหล่านั้นมาประกอบการพิจารณาร่วมกับกราฟเอนโทรปี ทำให้สามารถวิเคราะห์ความผิดปกติของการใช้งานในระบบเครือข่ายได้ง่ายยิ่งขึ้น นอกจากนี้ ผู้ใช้งานยังสามารถปรับสเกลที่อยู่ด้านล่างของกราฟ ซึ่งสเกลนี้เป็นการปรับค่าที่กำหนดอัตราส่วนของการให้ความสำคัญกับข้อมูลในปัจจุบันกับข้อมูลที่ผ่านมาในอดีต โดยหลักการของสเกลนี้คือ เมื่อปรับสเกลให้มีค่าสูงขึ้น หมายความว่า มีการกำหนดอัตราส่วนของข้อมูลโดยให้ความสำคัญกับข้อมูลที่เกิดขึ้นในปัจจุบันมากกว่าข้อมูลที่ผ่านมาในอดีต ในทางกลับกัน เมื่อปรับสเกลให้มีค่าลดต่ำลง หมายความว่า มีการกำหนดอัตราส่วนของข้อมูลโดยให้ความสำคัญกับข้อมูลที่เกิดขึ้นในปัจจุบันน้อยกว่าข้อมูลที่ผ่านมาในอดีตนั่นเอง



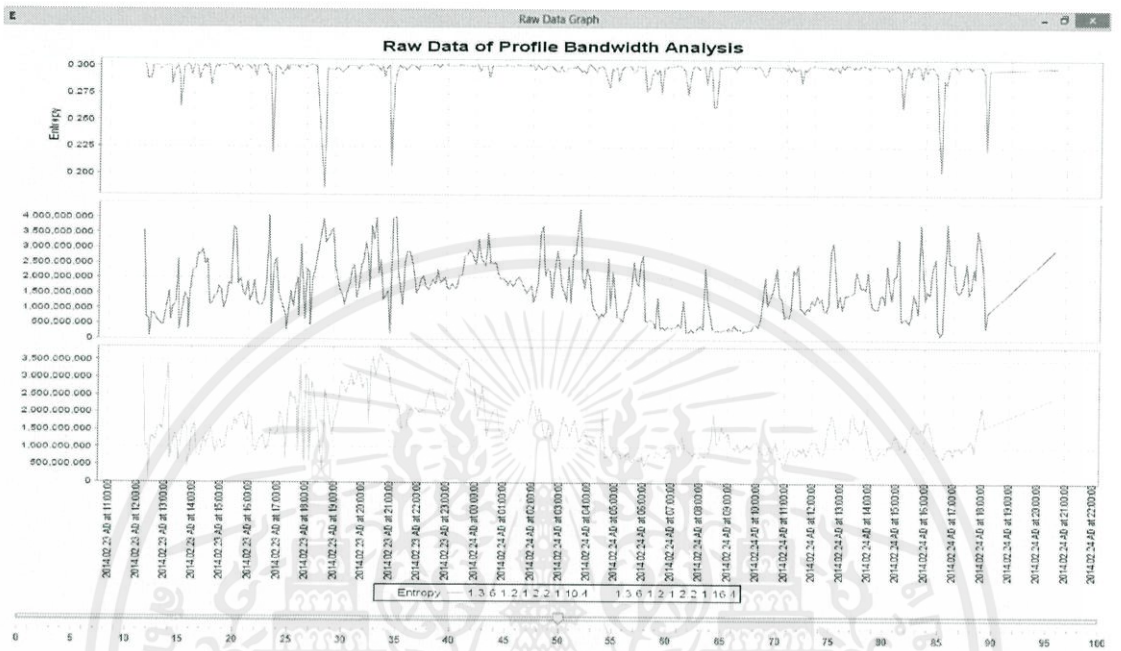
รูปที่ 3.12 หน้าการแสดงผลกราฟเอนโทรปี

10) ส่วนหน้าการตั้งค่าการแสดงผลกราฟข้อมูลจริง ผู้ใช้สามารถกำหนดหมายเลข OID ที่ต้องการให้แสดงผลกราฟข้อมูลจริงได้ตามต้องการ โดยสามารถเลือกหมายเลข OID เพื่อแสดงผลได้พร้อมกันสูงสุด 5 หมายเลข OID



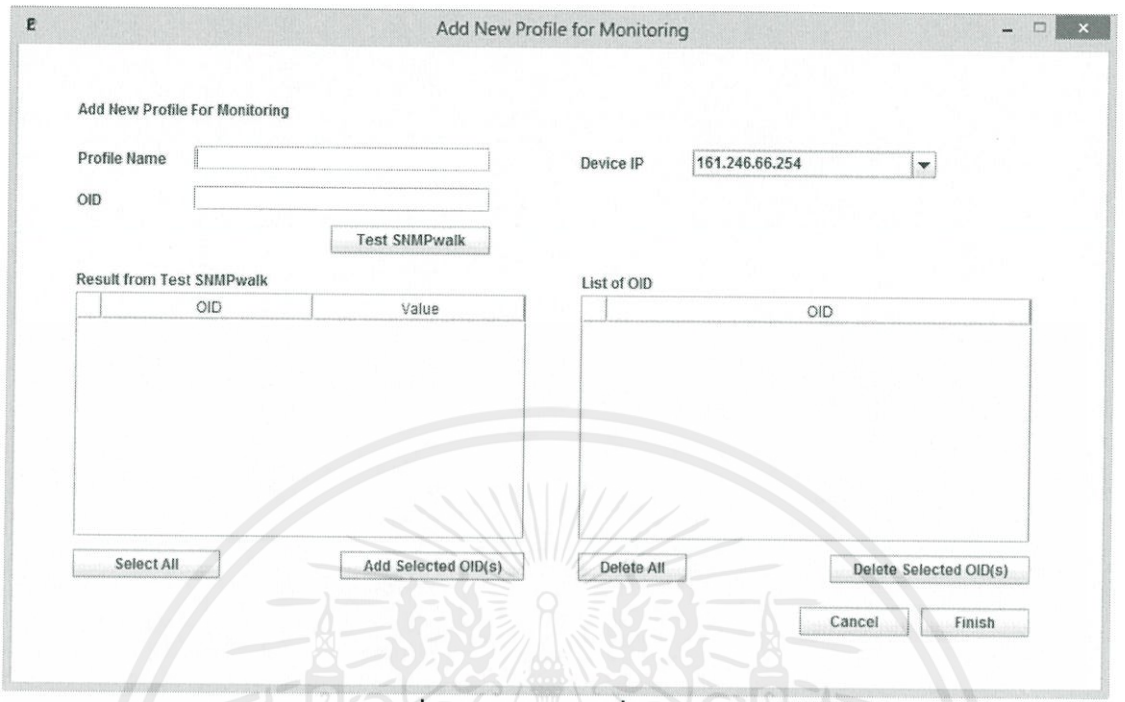
รูปที่ 3.13 หน้าการตั้งค่าการแสดงผลกราฟข้อมูลจริง

11) ส่วนหน้าการแสดงผลกราฟข้อมูลจริง จะแสดงผลกราฟบนสุดเป็นกราฟเอนโทรปี ถัดมาจะแสดงผลกราฟข้อมูลจริงที่ตามที่ผู้ใช้งานกำหนด



รูปที่ 3.14 หน้าการแสดงผลกราฟข้อมูลจริง

12) ส่วนหน้าการเพิ่มโปรไฟล์ ผู้ใช้งานสามารถเพิ่มเติมโปรไฟล์สำหรับอุปกรณ์เครือข่ายที่มีการตั้งค่าให้ทำการมอนิเตอร์เครือข่ายอยู่ก่อนหน้าแล้ว ทั้งนี้เนื่องจากผู้ใช้งานจะไม่สามารถเพิ่มอุปกรณ์เครือข่ายที่มีอยู่แล้วซ้ำได้อีกนั่นเอง ในส่วนนี้โปรแกรมจะแสดงอุปกรณ์เครือข่ายที่มีการทำงานอยู่ทั้งหมดในระบบ ให้ผู้ใช้งานเลือกอุปกรณ์เครือข่ายที่ต้องการ หลังจากนั้นผู้ใช้จะสามารถเพิ่มรายละเอียดของโปรไฟล์สำหรับมอนิเตอร์ได้ตามปกติ



รูปที่ 3.15 หน้าการเพิ่มโปรไฟล์

3.3 การออกแบบและผังการทำงานของระบบ

ระบบตรวจจับความผิดปกติในระบบเครือข่ายโดยอาศัยการเปลี่ยนแปลงเอนโทรปี จะต้องมีการออกแบบการทำงานที่ทำให้สามารถตรวจจับความผิดปกติโดยอาศัยการคำนวณเอนโทรปีของข้อมูลได้จริง เมื่อเทียบกับข้อมูลความผิดปกติที่เกิดขึ้นจริงที่ไม่ได้ผ่านการพิจารณาด้วยปัจจัยอื่นๆ การคำนวณเอนโทรปีนั้นเป็นการทำงานในส่วนแบ็กเอนด์ (backend) ของระบบจะสามารถแสดงผลในลักษณะของกราฟให้ผู้ใช้งานสังเกตเห็นได้ว่ามีข้อมูลในช่วงใดที่มีความผิดปกติที่จะทำให้กราฟแสดงผลเอนโทรปีมีความเปลี่ยนแปลง ส่วนการทำงาน ฟรอนท์เอนด์ (frontend) จะต้องออกแบบการทำงานให้ง่ายต่อการใช้งานที่สุด และผลจากการทำงานของระบบจะต้องสามารถแสดงผลลัพธ์ที่มีความน่าเชื่อถือได้ สามารถสังเกตความเปลี่ยนแปลงของระบบเครือข่ายจากกราฟเอนโทรปีได้ ดังนั้นจึงควรออกแบบการทำงานและวางผังการทำงานระบบให้เข้าใจง่ายแต่มีประสิทธิภาพในการทำงานสูงสุด

โปรแกรมได้ออกแบบการตั้งค่าโปรไฟล์ที่ต้องการมอนิเตอร์ให้กับโปรแกรม โดยจะแบ่งออกเป็น 2 รูปแบบ ดังนี้

1) การตั้งค่าโปรไฟล์อัตโนมัติ

ผู้ใช้งานสามารถเลือกโปรไฟล์ที่ระบบกำหนดไว้ให้แก่อุปกรณ์สำหรับทำการมอนิเตอร์ได้ โดยที่ผู้ใช้ไม่จำเป็นต้องกรอกรายละเอียดของโปรไฟล์นั้นๆ ด้วยตนเอง ซึ่งโปรไฟล์อัตโนมัติประกอบด้วย 3 โปรไฟล์ ได้แก่

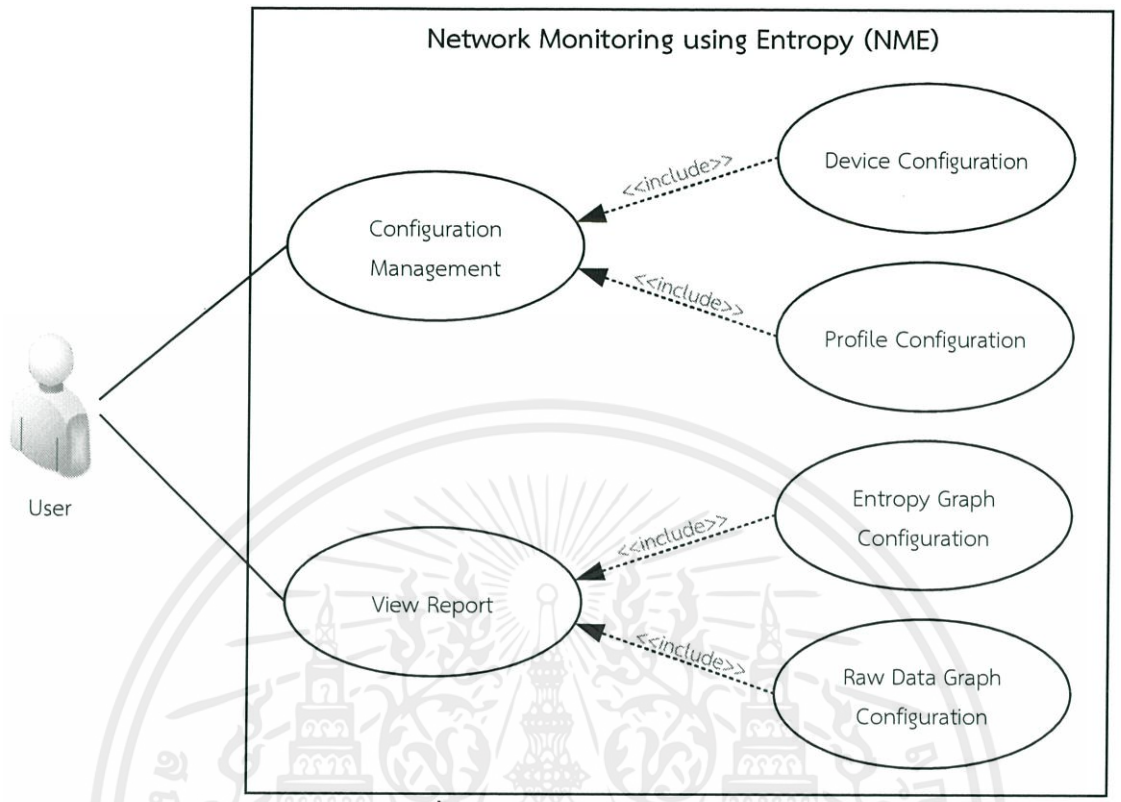
- Bandwidth in of all interface
  - โปรไฟล์นี้จะมอนิเตอร์ดูปริมาณการใช้งานแบนด์วิทธ์ขาเข้าในทุกอินเทอร์เฟสของอุปกรณ์เครือข่ายนั้นๆ
  - หมายเลข OID ที่ใช้ คือ 1.3.6.1.2.1.2.2.1.10
- Bandwidth out of all interface
  - โปรไฟล์นี้จะมอนิเตอร์ดูปริมาณการใช้งานแบนด์วิทธ์ขาออกในทุกอินเทอร์เฟสของอุปกรณ์เครือข่ายนั้นๆ
  - หมายเลข OID ที่ใช้ คือ 1.3.6.1.2.1.2.2.1.16
- Bandwidth in/out and queue of each interface
  - โปรไฟล์นี้ผู้ใช้งานสามารถเลือกอินเทอร์เฟสที่ต้องการมอนิเตอร์เพื่อดูปริมาณการใช้งานแบนด์วิทธ์เฉพาะของอินเทอร์เฟสนั้นๆ ได้
  - หมายเลข OID ที่ใช้ คือ 1.3.6.1.2.1.2.2.1.10, 1.3.6.1.2.1.2.2.1.16 และ 1.3.6.1.2.1.2.2.1.21

2) การตั้งค่าโปรไฟล์ด้วยตนเอง

ผู้ใช้งานสามารถสร้างโปรไฟล์ที่ต้องการใช้มอนิเตอร์ได้เอง โดยสามารถกำหนดชื่อโปรไฟล์ (Profile Name) และหมายเลข OID สำหรับโปรไฟล์นั้นๆ ได้ตามต้องการ

3.3.1 ยูสเคสไดอะแกรม (Use Case Diagram)

ผู้ใช้งานจะสามารถตั้งค่าอุปกรณ์เครือข่ายและกำหนดโปรไฟล์ที่จะใช้ในการมอนิเตอร์ตรวจตราปริมาณการใช้งานในระบบเครือข่ายได้เอง โดยการทำงานระบบจะวิเคราะห์โดยอาศัยเทคนิคการคำนวณเอนโทรปีของข้อมูล อีกทั้งยังสามารถเรียกดูหน้าต่างแสดงผลการตรวจตราอุปกรณ์เครือข่ายในลักษณะกราฟได้อีกด้วย



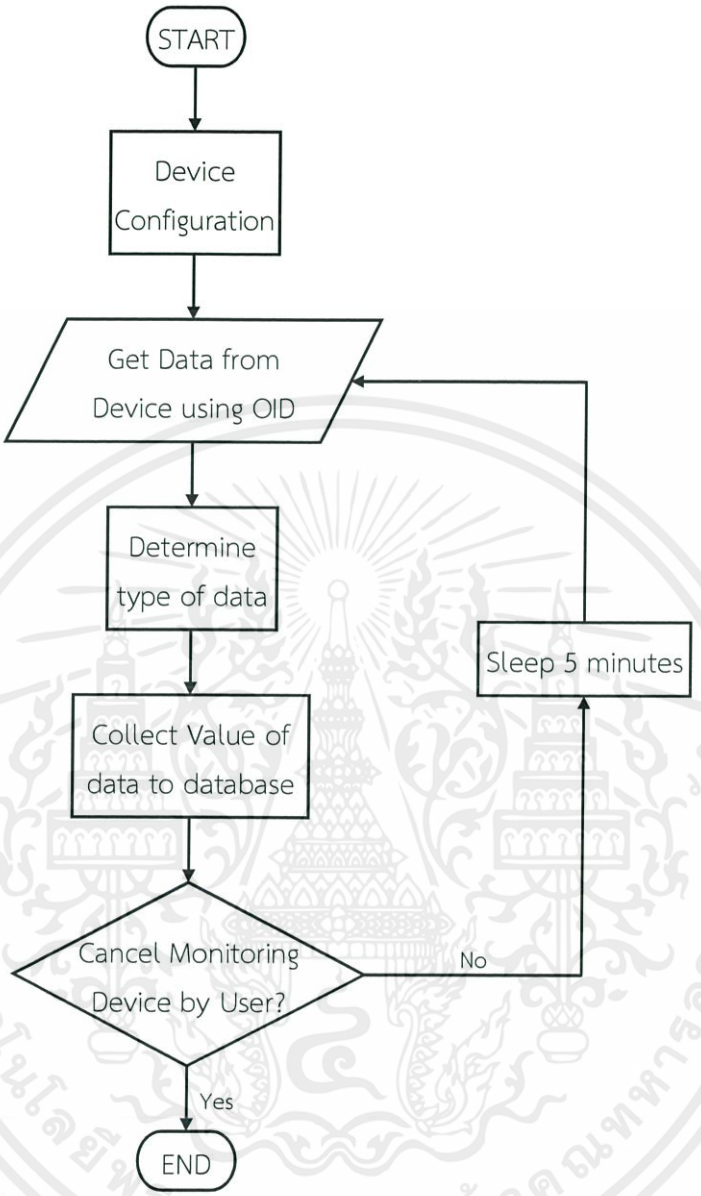
รูปที่ 3.16 ยูสเคสไดอะแกรม

3.3.2 ผังการทำงานของโปรแกรม (Flow Chart)

ระบบตรวจจับความผิดปกติในระบบเครือข่ายโดยอาศัยการเปลี่ยนแปลงเอนโทรปี สามารถแบ่งการทำงานได้ดังนี้

1) ส่วนการเก็บข้อมูลจากอุปกรณ์บนเครือข่าย

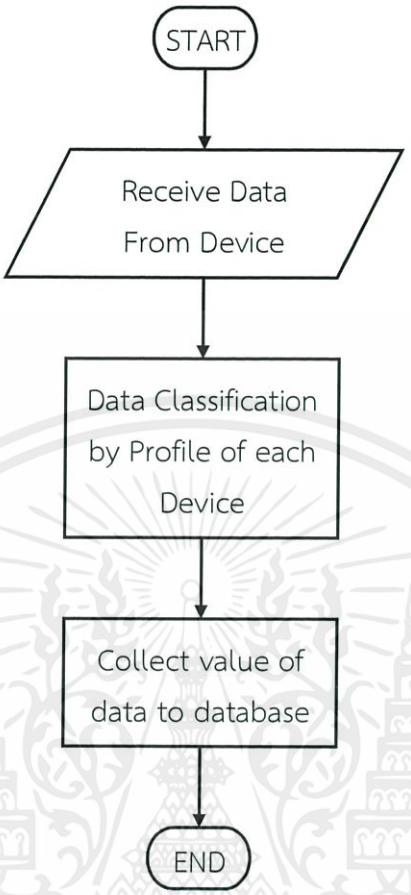
การเก็บข้อมูลจากอุปกรณ์บนเครือข่าย โดยอาศัยการทำงานของโพรโทคอลเอสเอ็นเอ็มพีในการดึงข้อมูลจากอุปกรณ์เครือข่ายมาเก็บในฐานข้อมูล โดยจะทำการเก็บข้อมูลจากอุปกรณ์เครือข่ายตามช่วงเวลาที่กำหนด คือ จะทำการเก็บข้อมูลทุก 5 นาที



รูปที่ 3.17 ผังการทำงานส่วนการเก็บข้อมูลจากอุปกรณ์บนเครือข่าย

2) ส่วนติดต่อฐานข้อมูล

ระบบมีการติดต่อฐานข้อมูลโดยมีการบันทึกค่าการใช้งานระบบเครือข่ายที่ได้มาจากการดึงข้อมูลจากอุปกรณ์เครือข่ายโดยตรงผ่านโพรโทคอลเอสเอ็นเอ็มพี

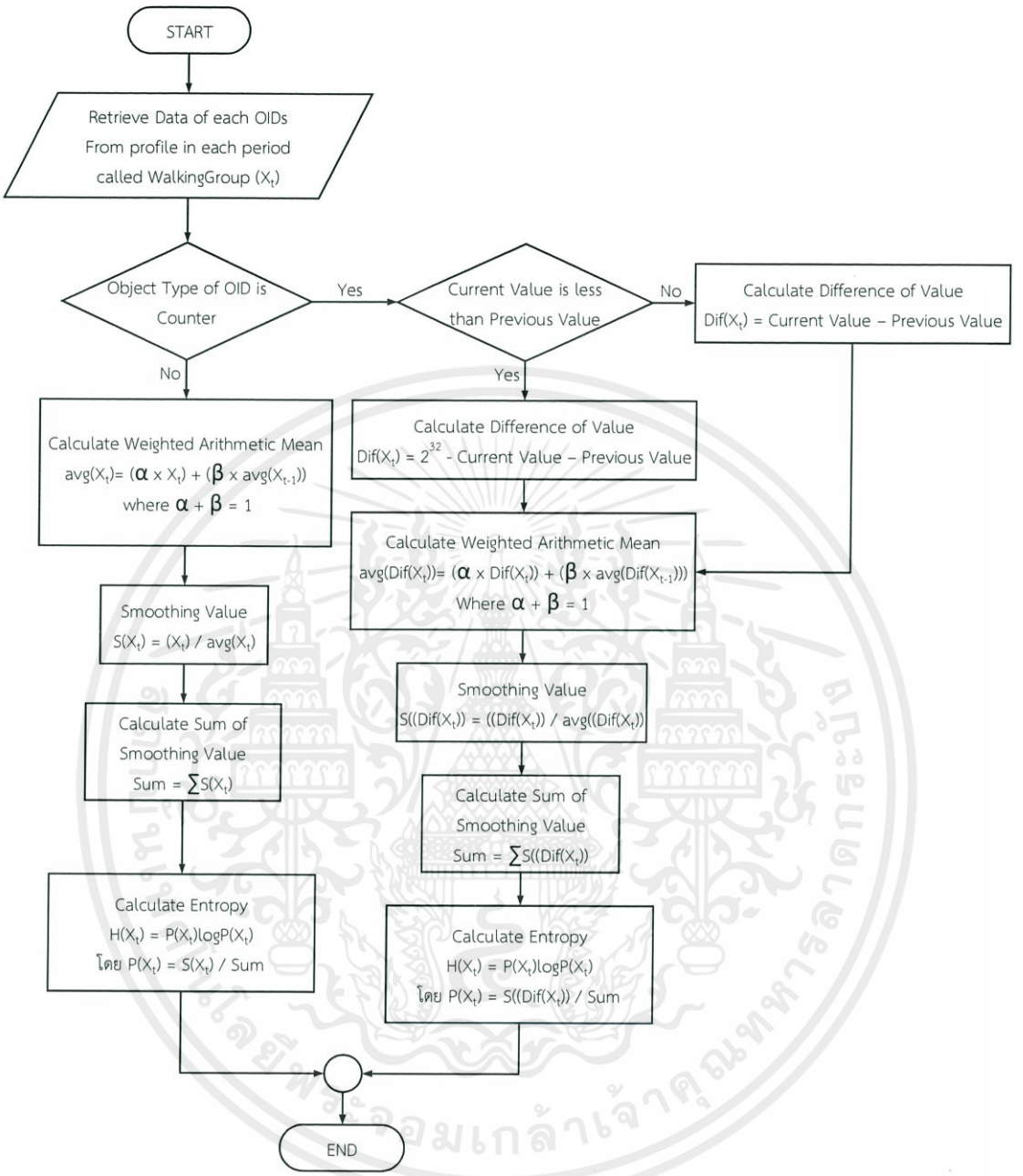


รูปที่ 3.18 ผังการทำงานส่วนติดต่อฐานข้อมูล

3) ส่วนการคำนวณเอนโทรปี

ส่วนการคำนวณเอนโทรปีจะนำข้อมูลจากฐานข้อมูลที่เก็บข้อมูลจริงที่ได้จากอุปกรณ์เครือข่ายไปคำนวณหาค่าเอนโทรปีของข้อมูลตามสมการหลัก คือ

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log P(x_i)$$



รูปที่ 3.19 ผังการทำงานส่วนการคำนวณเอนโทรปี

บทที่ 4
การทดลองและผลการทดลอง

ในส่วนของบทนี้จะมีเนื้อหาเกี่ยวกับการทำงานของโปรแกรม การเก็บข้อมูลจากอุปกรณ์เครือข่ายผ่านโพรโทคอลเอสเอ็นเอ็มพีแล้วนำมาวิเคราะห์ข้อมูลด้วยเทคนิคการคำนวณเอนโทรปีของข้อมูล รวมถึงการแสดงผลลัพธ์ที่ได้จากการคำนวณเอนโทรปีของข้อมูลในลักษณะกราฟด้วย

4.1 การตั้งค่าการใช้งานโปรแกรม

การคำนวณเอนโทรปีของข้อมูลในครั้งนี้ ผู้วิจัยได้ทดสอบโปรแกรม Network Monitoring using Entropy (NME) กับอุปกรณ์เครือข่ายของสาขาวิชาวิศวกรรมคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง รายชื่อของอุปกรณ์เครือข่ายที่ผู้วิจัยสามารถนำมาทดสอบได้จะแสดงในตารางที่ 4.1

ตารางที่ 4.1 รายชื่ออุปกรณ์ที่นำมาทดสอบ

ชื่ออุปกรณ์	ไอพีแอดเดรส	ซับเน็ต
CE-Switch	161.246.66.254	255.255.255.0
emerald	161.246.4.254	255.255.255.0
emerald	161.246.5.254	255.255.255.0
emerald	161.246.6.254	255.255.255.0

ผู้วิจัยได้เลือกอุปกรณ์ CE-Switch ซึ่งมีไอพีแอดเดรส 161.246.66.254/24 มาใช้ในการทดสอบ โดยผู้วิจัยได้กำหนดโปรไฟล์ให้แก่อุปกรณ์เครือข่ายเพื่อทำการมอนิเตอร์ แสดงในตารางที่ 4.2

ตารางที่ 4.2 ชื่อโปรไฟล์และหมายเลข OID ที่ใช้ในการทดสอบ

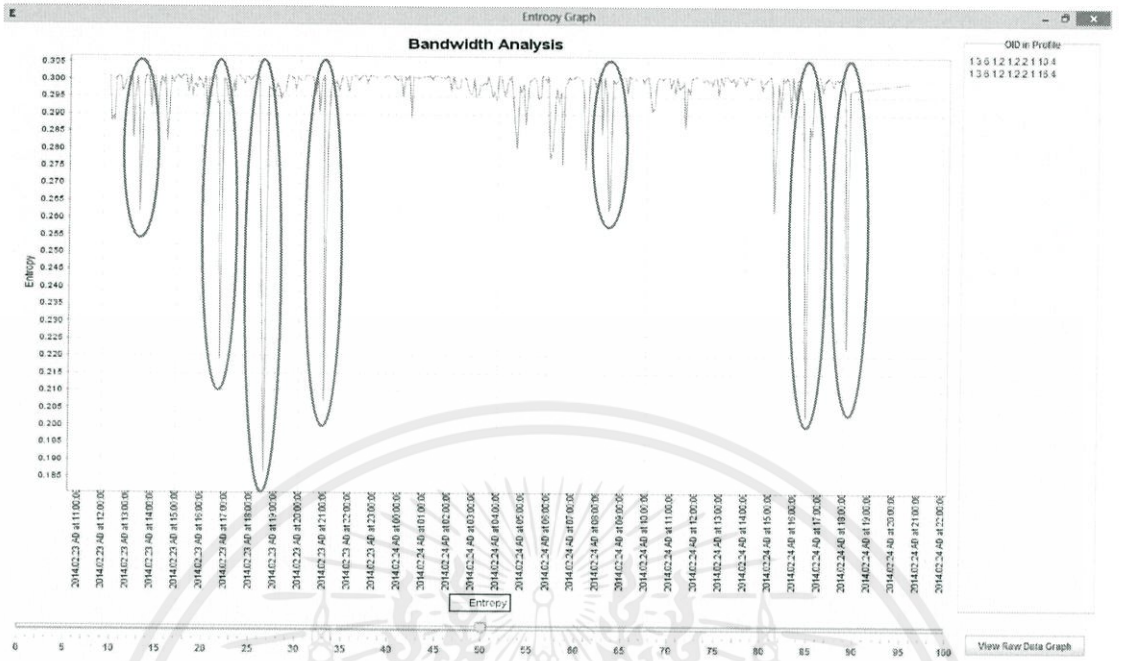
ลำดับที่	ชื่อโปรไฟล์	หมายเลข OID	ชนิดของข้อมูล
1	Bandwidth in of all interface	1.3.6.1.2.1.2.2.1.10	Counter
2	Bandwidth out of all interface	1.3.6.1.2.1.2.2.1.16	Counter
3	Bandwidth in/out and queue for each interface_4	1.3.6.1.2.1.2.2.1.10.4	Counter
		1.3.6.1.2.1.2.2.1.16.4	Counter

		1.3.6.1.2.1.2.2.1.21.4	Gauge
4	Bandwidth Analysis	1.3.6.1.2.1.2.2.1.10.4	Counter
		1.3.6.1.2.1.2.2.1.16.4	Counter
5	Packet Analysis	1.3.6.1.2.1.2.2.1.11.4	Counter
		1.3.6.1.2.1.2.2.1.17.4	Counter
6	CPU Utilization	1.3.6.1.4.1.9.9.109.1.1.1.1.3	Gauge
		1.3.6.1.4.1.9.9.109.1.1.1.1.4	Gauge
		1.3.6.1.4.1.9.9.109.1.1.1.1.5	Gauge
7	Memory Usage	1.3.6.1.4.1.9.9.48.1.1.1.5.1	Gauge
		1.3.6.1.4.1.9.9.48.1.1.1.6.1	Gauge

หลังจากทำการตั้งค่าอุปกรณ์เครือข่าย และตั้งค่าโปรไฟล์ต่างๆ ตามตารางที่ 4.1 และ 4.2 เสร็จเรียบร้อย โปรแกรมจะเริ่มเก็บข้อมูลจากอุปกรณ์เครือข่ายโดยตรงตามโปรไฟล์ที่ได้กำหนดไว้ โดยจะบันทึกค่าต่างๆ ลงในฐานข้อมูล เพื่อจะได้นำค่าต่างๆ เหล่านี้ใช้ในการวิเคราะห์หาความผิดปกติของการใช้งานระบบเครือข่ายในภายหลังได้

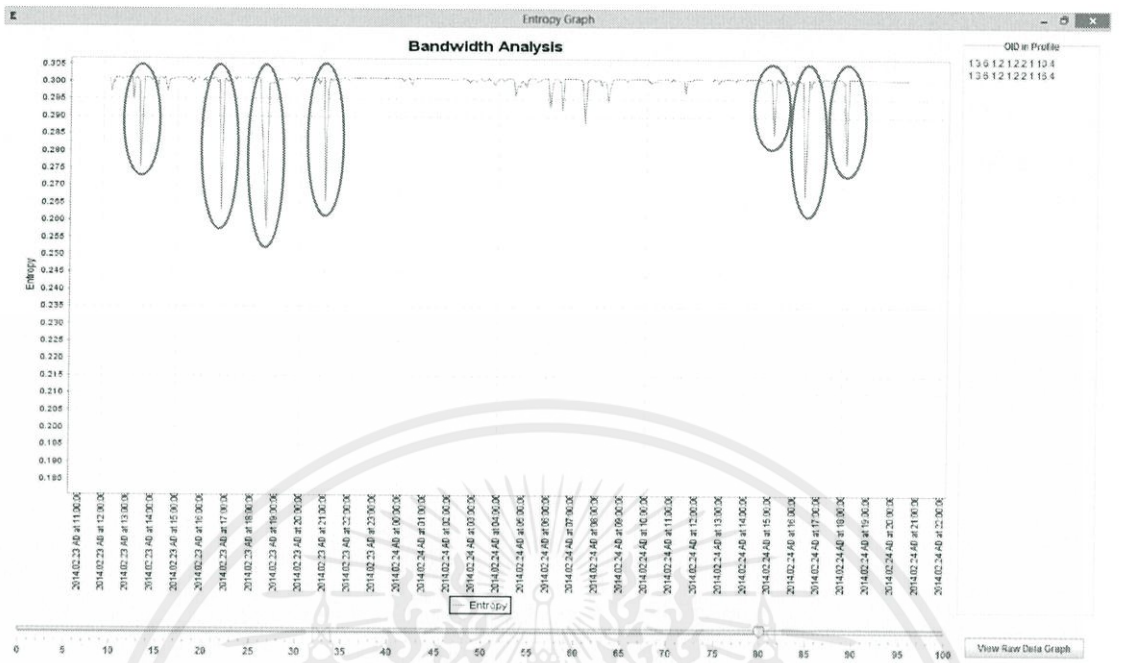
4.2 ผลการทดลอง

จากการทดลองในหัวข้อที่ 4.1 สามารถแสดงผลที่ได้จากการทำงานของโปรแกรมซึ่งได้จากการนำค่าต่างๆ มาจากฐานข้อมูล แล้วทำการคำนวณเอนโทรปีของข้อมูล การแสดงผลจะสร้างกราฟเอนโทรปีของข้อมูลในรูปแบบของกราฟเส้นได้ เพื่อให้ง่ายต่อการพิจารณาหาความผิดปกติของข้อมูล ตัวอย่างเช่น การแสดงผลกราฟเอนโทรปีของโปรไฟล์ Bandwidth Analysis ดังรูปที่ 4.12



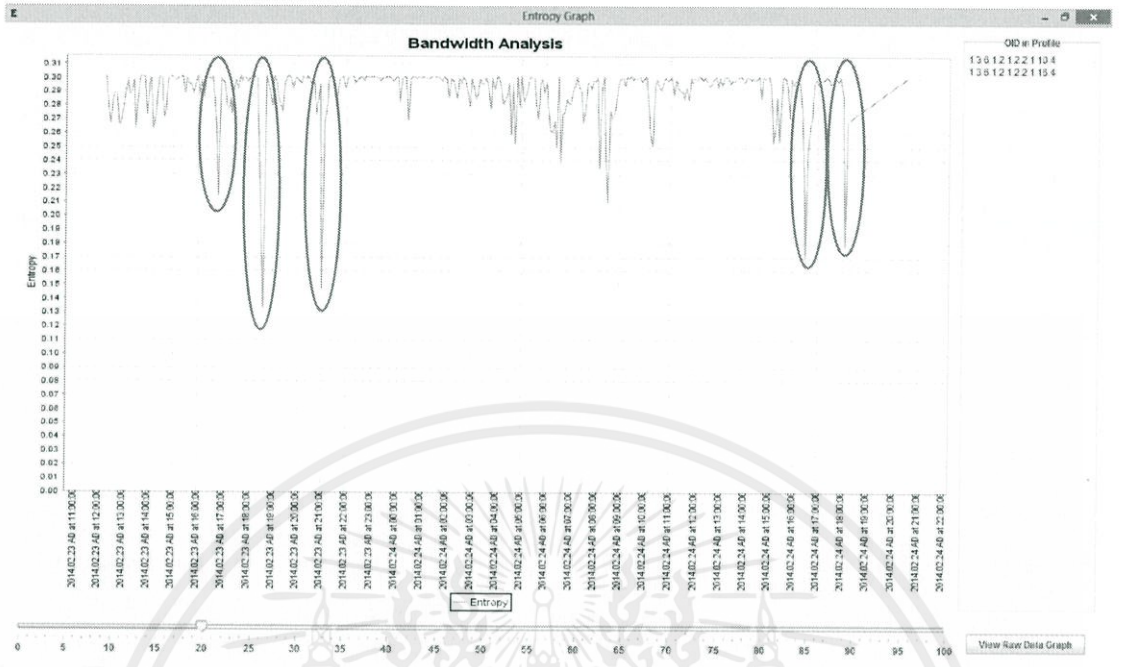
รูปที่ 4.1 กราฟเอนโทรปีของโปรไฟล์ Bandwidth Analysis โดยกำหนดอัตราส่วนของการให้ความสำคัญกับข้อมูลในปัจจุบันเท่ากับข้อมูลที่ผ่านมาในอดีต

จากรูปที่ 4.1 จะสังเกตได้ว่าค่าเอนโทรปีของโปรไฟล์ชุดนี้มีข้อมูลเอนโทรปีบางค่าที่มีการเปลี่ยนแปลงไปอย่างรวดเร็วแตกต่างจากค่าเอนโทรปีของข้อมูลข้างเคียง เมื่อทำการพิจารณากราฟเบื้องต้น อาจสรุปได้ว่าข้อมูลในกลุ่มที่วงกลมไว้ในรูปที่ 4.1 มีความผิดปกติเกิดขึ้นในระบบเครือข่ายอย่างแน่นอน



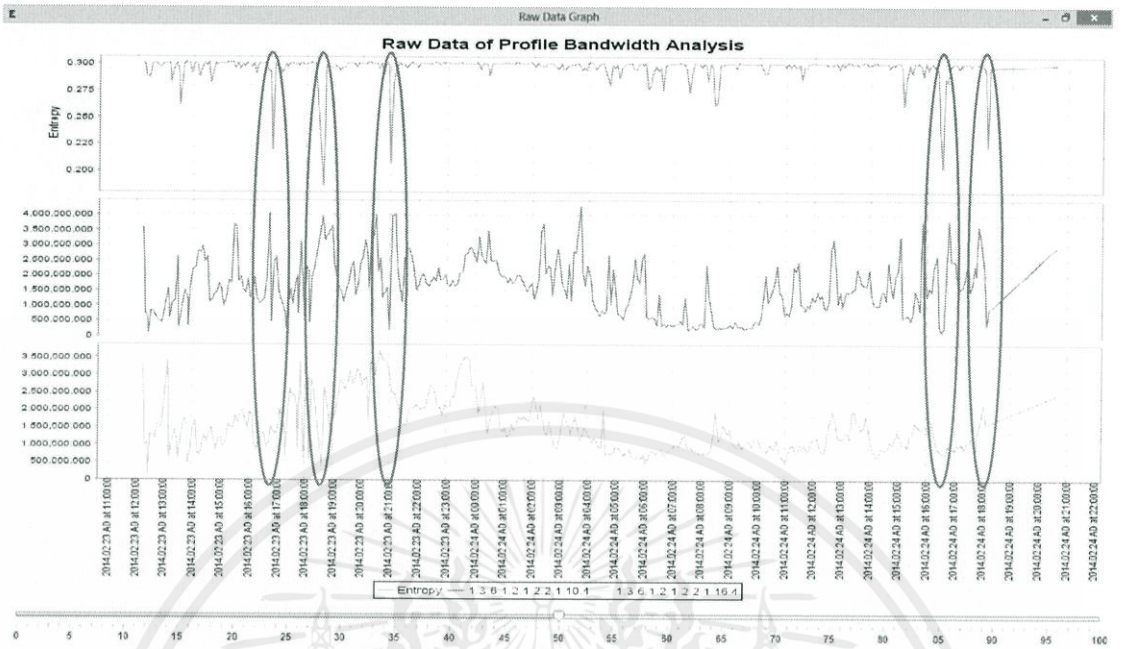
รูปที่ 4.2 กราฟเอนโทรปีของโปรไฟล์ Bandwidth Analysis โดยกำหนดอัตราส่วนของการให้ความสำคัญกับข้อมูลในปัจจุบันมากกว่าข้อมูลที่ผ่านมาในอดีต

จากรูปที่ 4.2 จะสามารถสังเกตได้ว่าเมื่อมีการปรับสเกลที่ส่วนด้านล่างของกราฟ โดยมีการกำหนดอัตราส่วนของข้อมูลโดยให้ความสำคัญกับข้อมูลที่เกิดขึ้นในปัจจุบันมากกว่าข้อมูลที่ผ่านมาในอดีต จะได้กราฟเอนโทรปีใหม่ซึ่งมีลักษณะราบเรียบมากขึ้น ข้อมูลแกว่งน้อยลง นั่นหมายความว่า ตัวแปรของโปรไฟล์นี้มีความสัมพันธ์กัน แต่หากกราฟมีการแกว่งมากขึ้น มีลักษณะของกราฟฟันเลื่อยมากขึ้น แสดงว่าตัวแปรของโปรไฟล์ที่นำมาใช้ไม่ค่อยมีความสัมพันธ์กัน ในกรณีที่กราฟนิ่งและราบเรียบมากขึ้น ค่าเอนโทรปีในช่วงใดที่เปลี่ยนแปลงไปจากค่าอื่นมากๆ จะสามารถทราบได้ทันทีว่าเครือข่ายเกิดความผิดปกติขึ้นในช่วงเวลาดังกล่าว



รูปที่ 4.3 กราฟเอนโทรปีของโปรไฟล์ Bandwidth Analysis โดยกำหนดอัตราส่วนของการให้ความสำคัญกับข้อมูลในปัจจุบันน้อยกว่าข้อมูลที่ผ่านมาในอดีต

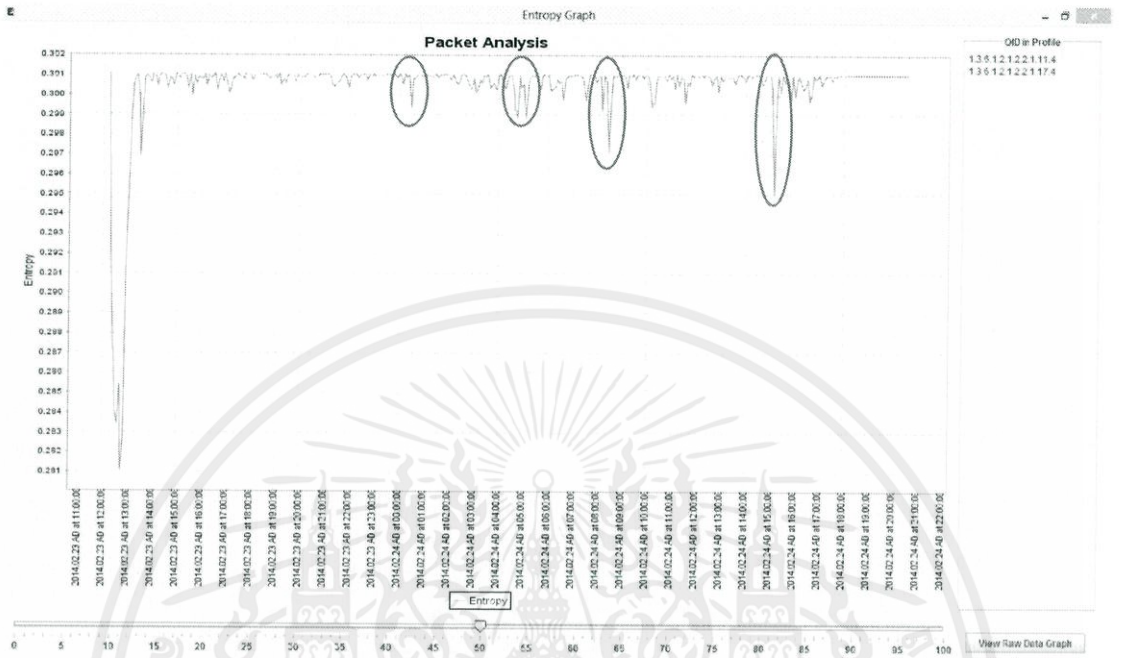
จากรูปที่ 4.3 จะสามารถสังเกตได้ว่าเมื่อมีการปรับสเกลที่ส่วนด้านล่างของกราฟ โดยมีการกำหนดอัตราส่วนของข้อมูลโดยให้ความสำคัญกับข้อมูลที่เกิดขึ้นในปัจจุบันน้อยกว่าข้อมูลที่ผ่านมาในอดีต จะได้กราฟเอนโทรปีใหม่ซึ่งมีลักษณะเป็นฟันเลื่อย ข้อมูลที่ได้มีการแกว่งมากขึ้น แต่ก็ยังมีข้อมูลบางส่วนที่เปลี่ยนแปลงไปค่อนข้างน้อย ไม่แตกต่างจากเดิม นั่นหมายความว่า ตัวแปรของโปรไฟล์นี้มีความสัมพันธ์กันดี ค่าเอนโทรปีในช่วงใดที่เปลี่ยนแปลงไปจากค่าอื่นมากๆ จะสามารถทราบได้ทันทีว่าเครือข่ายเกิดความผิดปกติขึ้นในช่วงเวลาดังกล่าวเช่นกัน



รูปที่ 4.4 กราฟข้อมูลจริงของโปรไฟล์ Bandwidth Analysis

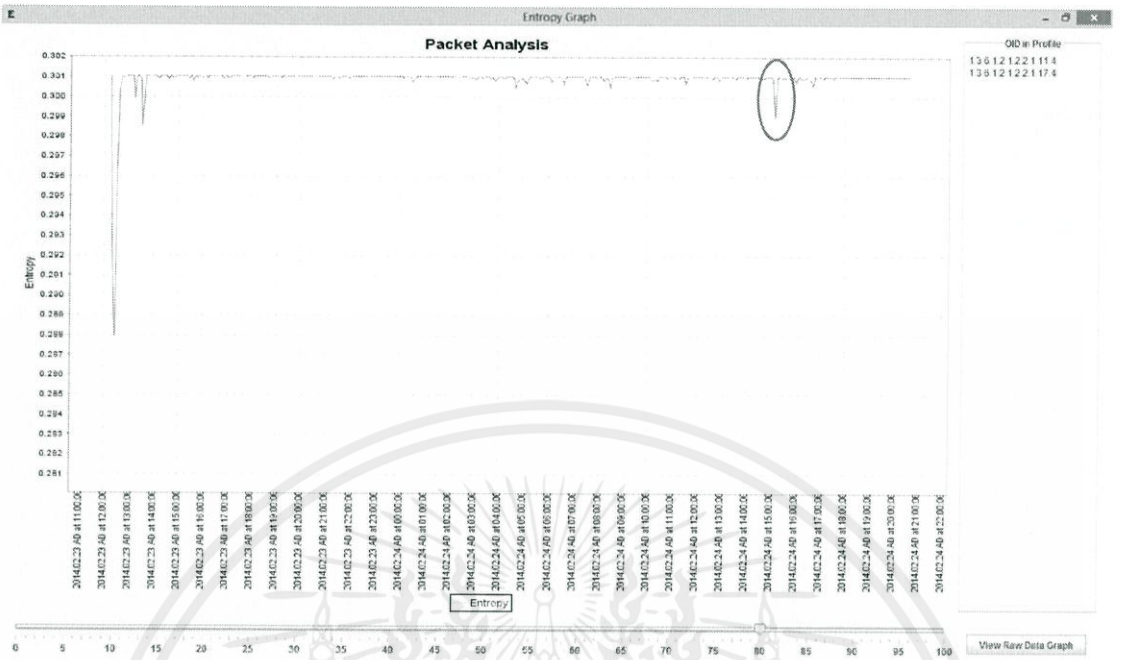
จากรูปที่ 4.4 เมื่อแสดงผลกราฟข้อมูลจริงของโปรไฟล์ร่วมกับกราฟเอนโทรปีของข้อมูล โดยแสดงผลกราฟทั้งหมดในช่วงเวลาเดียวกัน ทำให้ง่ายต่อการพิจารณาเพื่อหาความผิดปกติที่เกิดขึ้นในระบบเครือข่าย จากกราฟจะสามารถสังเกตเห็นได้อย่างเด่นชัดอยู่แล้วว่ามีเอนโทรปีของข้อมูลบางช่วงที่มีการเปลี่ยนแปลงไปจากเอนโทรปีของข้อมูลปกติเป็นอย่างมาก เพียงเท่านี้อาจจะทราบได้ว่าน่าจะมีความผิดปกติของการใช้งานเครือข่ายในช่วงเวลาใดบ้าง เมื่อมีกราฟข้อมูลจริงมาประกอบการพิจารณาร่วมกับเอนโทรปีด้วย ทำให้มั่นใจได้มากยิ่งขึ้นว่าเกิดความผิดปกติขึ้นในแต่ละช่วงเวลานั้นๆ จริงหรือไม่ เนื่องจากกราฟข้อมูลจริงก็จะมีลักษณะของข้อมูลที่ผิดปกติร่วมด้วย และการปรับสเกลของกราฟ เพื่อการทำสมูทติ้งกราฟ โดยเป็นการหาตำแหน่งของจุดที่เกิดความผิดปกติขึ้นจริง ซึ่งเกิดขึ้นในตำแหน่งที่ค่อนข้างจะคงที่ไม่ว่าจะปรับสเกลไปอย่างไรก็ตาม ประโยชน์ของการทำสมูทติ้งคือ สามารถตัดรายละเอียดของการเปลี่ยนแปลงข้อมูลย่อยๆ บางส่วนได้ ทำให้ผู้ใช้งานสามารถเห็นความแตกต่างของความผิดปกติที่เกิดขึ้นในเครือข่ายได้ชัดเจนยิ่งขึ้น

ตัวอย่างถัดมาเป็นการแสดงผลกราฟเอนโทรปีของโปรไฟล์ Packet Analysis ดังรูปที่ 4.16



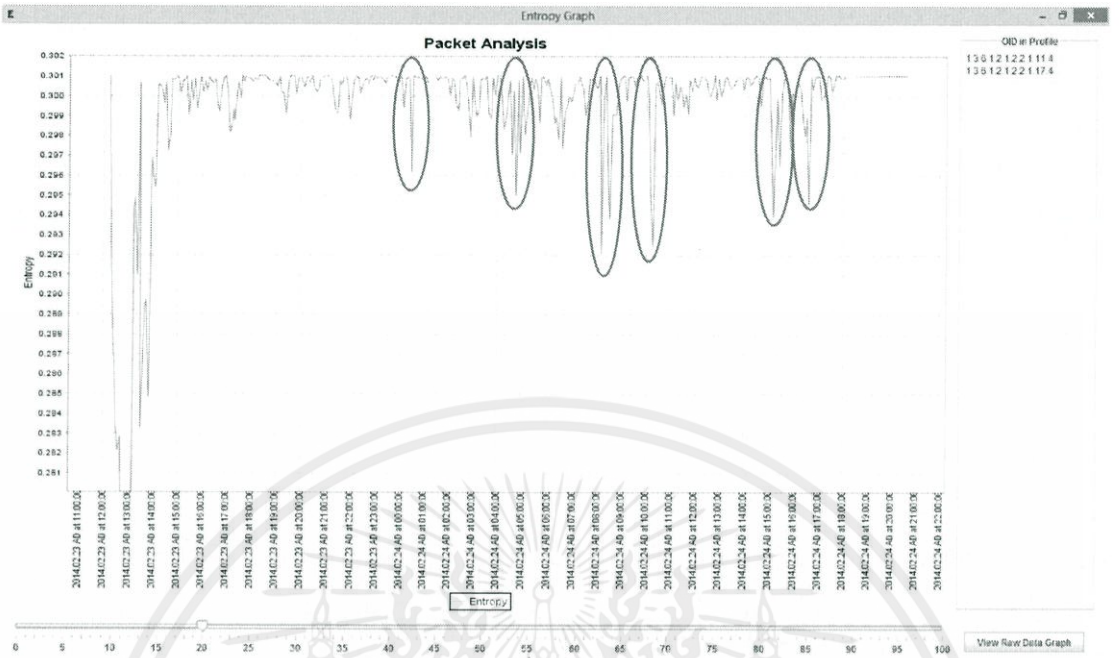
รูปที่ 4.5 กราฟเอนโทรปีของโปรไฟล์ Packet Analysis โดยกำหนดอัตราส่วนของการให้ความสำคัญกับข้อมูลในปัจจุบันเท่ากับข้อมูลที่ผ่านมาในอดีต

จากรูปที่ 4.5 จะสามารถสรุปผลได้คล้ายกับโปรไฟล์ Bandwidth Analysis เช่นกัน โดยจะสังเกตได้ว่าค่าเอนโทรปีของโปรไฟล์ชุดนี้มีข้อมูลเอนโทรปีบางค่าที่เปลี่ยนแปลงไปอย่างรวดเร็ว แตกต่างจากค่าเอนโทรปีของข้อมูลข้างเคียง เมื่อทำการพิจารณากราฟเบื้องต้น อาจสรุปได้ว่าข้อมูลในกลุ่มที่วงกลมไว้ในรูปที่ 4.5 มีความผิดปกติเกิดขึ้นในระบบเครือข่ายอย่างแน่นอน แต่สำหรับข้อมูลของกราฟในช่วงแรกๆ อาจจะสังเกตได้ว่ากราฟมีค่าลดต่ำลงจนผิดปกติ แต่ทั้งนี้เนื่องจากกราฟในช่วงแรกเป็นช่วงที่เริ่มต้นการคำนวณเอนโทรปีของข้อมูล ซึ่งจะต้องผ่านขั้นตอนการหาค่าเฉลี่ยแบบถ่วงน้ำหนักมาก่อน ช่วงที่เริ่มต้นการคำนวณนั้นจะยังไม่ค่อยมีข้อมูลเพื่อนำมาคำนวณ ผลลัพธ์ที่ได้จึงมีค่าเปลี่ยนแปลงไปได้ง่ายกว่าการคำนวณเมื่อมีปริมาณข้อมูลจำนวนมากกว่า ทำให้ในช่วงแรกค่าเฉลี่ยแบบถ่วงน้ำหนักที่ได้อาจไม่ใช่ค่าที่เสถียรแล้ว การได้มาของค่าเฉลี่ยแบบถ่วงน้ำหนักที่เสถียรแล้วอาจจะต้องอาศัยเวลาชักระยะหนึ่ง เมื่อข้อมูลเข้าสู่สภาวะคงที่ระบบจะสามารถแสดงผลเอนโทรปีของข้อมูลได้ถูกต้องตามปกติ



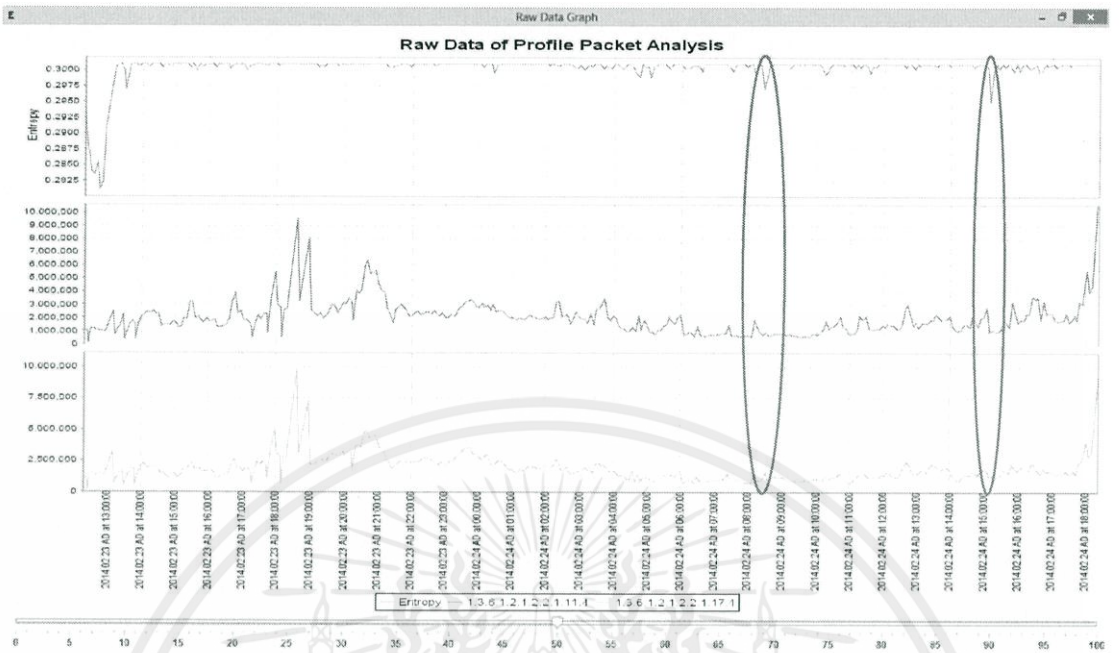
รูปที่ 4.6 กราฟเอนโทรปีของโปรไฟล์ Packet Analysis โดยกำหนดอัตราส่วนของการให้ความสำคัญกับข้อมูลในปัจจุบันมากกว่าข้อมูลที่ผ่านมาในอดีต

จากรูปที่ 4.6 จะสามารถสังเกตได้ว่าเมื่อมีการปรับสเกลที่ส่วนด้านล่างของกราฟ โดยมีการกำหนดอัตราส่วนของข้อมูลโดยให้ความสำคัญกับข้อมูลที่เกิดขึ้นในปัจจุบันมากกว่าข้อมูลที่ผ่านมาในอดีต จะได้กราฟเอนโทรปีใหม่ซึ่งมีลักษณะราบเรียบมากขึ้น ข้อมูลแกว่งน้อยลง นั่นหมายความว่า ตัวแปรของโปรไฟล์นี้มีความสัมพันธ์กัน แต่หากกราฟมีการแกว่งมากขึ้น มีลักษณะของกราฟฟันเลื่อยมากขึ้น แสดงว่าตัวแปรของโปรไฟล์ที่นำมาใช้ไม่ค่อยมีความสัมพันธ์กัน ในกรณีที่กราฟนิ่งและราบเรียบมากขึ้น ค่าเอนโทรปีในช่วงใดที่เปลี่ยนแปลงไปจากค่าอื่นมากๆ จะสามารถทราบได้ทันทีว่าเครือข่ายเกิดความผิดปกติขึ้นในช่วงเวลาดังกล่าว



รูปที่ 4.7 กราฟเอนโทรปีของโปรไฟล์ Packet Analysis โดยกำหนดอัตราส่วนของการให้ความสำคัญกับข้อมูลในปัจจุบันน้อยกว่าข้อมูลที่ผ่านมาในอดีต

จากรูปที่ 4.7 จะสามารถสังเกตได้ว่าเมื่อมีการปรับสเกลที่ส่วนด้านล่างของกราฟ โดยมีการกำหนดอัตราส่วนของข้อมูลโดยให้ความสำคัญกับข้อมูลที่เกิดขึ้นในปัจจุบันน้อยกว่าข้อมูลที่ผ่านมาในอดีต จะได้กราฟเอนโทรปีใหม่ซึ่งมีลักษณะเป็นฟันเลื่อย ข้อมูลที่ได้มีการแกว่งมากขึ้นอย่างเห็นได้ชัด แต่ก็ยังมีข้อมูลบางส่วนที่เปลี่ยนแปลงไปค่อนข้างน้อย ไม่แตกต่างจากเดิมมากนัก นั่นหมายความว่าตัวแปรของโปรไฟล์นี้มีความสัมพันธ์กันดี ค่าเอนโทรปีในช่วงใดที่เปลี่ยนแปลงไปจากค่าอื่นมากๆ จะสามารถทราบได้ทันทีว่าเครือข่ายเกิดความผิดปกติขึ้นในช่วงเวลาดังกล่าวเช่นกัน



รูปที่ 4.8 กราฟข้อมูลจริงของโปรไฟล์ Packet Analysis

จากรูปที่ 4.8 เมื่อแสดงผลกราฟข้อมูลจริงของโปรไฟล์ร่วมกับกราฟเอนโทรปีของข้อมูล โดยแสดงผลกราฟทั้งหมดในช่วงเวลาเดียวกัน จะสามารถสังเกตเห็นได้อย่างเด่นชัดอยู่แล้วว่ามีเอนโทรปีของข้อมูลบางช่วงที่มีการเปลี่ยนแปลงไปจากเอนโทรปีของข้อมูลปกติเป็นอย่างมาก และเมื่อพิจารณากราฟข้อมูลจริงร่วมด้วย จะทำให้มั่นใจได้มากยิ่งขึ้นว่าเกิดความผิดปกติขึ้นในแต่ละช่วงเวลานั้นๆ จริงหรือไม่ เนื่องจากกราฟข้อมูลจริงก็จะมีลักษณะของข้อมูลที่ผิดปกติร่วมด้วยนั่นเอง

จากผลการทดลองสามารถสรุปได้ดังนี้

- ตัวแปรที่นำมาใช้สร้างเป็นโปรไฟล์สำหรับมอนิเตอร์ควรมีความสัมพันธ์กันจึงจะสามารถให้ผลลัพธ์ที่น่าเชื่อถือและสามารถบอกได้ว่าเกิดความผิดปกติของการใช้งานในระบบเครือข่ายขึ้นในช่วงเวลาใด
- หากข้อมูลในโปรไฟล์นั้นมีความสัมพันธ์กัน เมื่อปรับสเกลหรือปรับอัตราส่วนของการให้ความสำคัญกับข้อมูลในปัจจุบันมากกว่าข้อมูลในอดีต จะได้กราฟที่มีลักษณะราบเรียบขึ้น กราฟจะนิ่งมากขึ้น หากค่อยๆลดอัตราส่วนความสำคัญของข้อมูลในปัจจุบันลง ใช้ข้อมูลในอดีตมาเกี่ยวข้องให้มากขึ้น ค่าเอนโทรปีที่ได้จะมีความแกว่งมากขึ้น กราฟจะมีลักษณะเป็นฟันเลื่อยมากขึ้น
- ในกรณีที่มีตัวแปรหลายตัวที่ไม่มีความสัมพันธ์กันเลย กราฟจะแกว่งมากถึงแม้ว่าเราจะกำหนดอัตราส่วนความสำคัญของข้อมูลในปัจจุบันมากเพียงใดก็ตาม

- หากชุดข้อมูลมีความสัมพันธ์กันดี ไม่ว่าจะกำหนดอัตราส่วนความสำคัญให้ข้อมูลปัจจุบันหรือข้อมูลที่ผ่านมาในอดีตมาก ข้อมูลเครือข่ายที่ปกติจะทำให้กราฟนิ่ง หรือแกว่งน้อยเสมอ หากกราฟแกว่งมากแสดงว่าชุดข้อมูลที่นำมาใช้ไม่มีความสัมพันธ์กัน
- ในขั้นตอนการคำนวณเอนโทรปี การแกว่งที่ตัวหารมีค่าอดีตต่ำ (กำหนดอัตราส่วนความสำคัญให้ข้อมูลปัจจุบันมากกว่าข้อมูลที่ผ่านมาในอดีต) จะบ่งบอกความผิดปกติมากกว่าการแกว่งที่ตัวหารมีค่าอดีตสูง (กำหนดอัตราส่วนความสำคัญให้ข้อมูลในอดีตมากกว่าข้อมูลปัจจุบัน) เนื่องจากถ้าให้ค่าปัจจุบันมีค่ามาก ตัวหารที่มีค่าอดีตต่ำจะมีค่าใกล้เคียงกับตัวตั้งมาก ผลหารที่ได้จึงเปลี่ยนไม่มาก ส่งผลให้กราฟควรจะมีการแกว่งน้อย แต่ในกรณีที่มีความผิดปกติของสัดส่วนข้อมูลเกิดขึ้น ก็จะยังคงมีการเปลี่ยนแปลงของข้อมูลที่สูง ถึงแม้ว่าจะใช้ค่าอดีตต่ำก็ตาม
- การพิจารณาความผิดปกติของข้อมูลเครือข่าย คือ พิจารณาจากลักษณะสัดส่วนของข้อมูลในปัจจุบันที่ไม่สอดคล้องกับข้อมูลที่ผ่านมาในอดีต โดยจะเกิดใน 2 ลักษณะ คือ ประการแรก จะเกิดข้อมูลที่ผิดปกติขึ้นมาซึ่งที่ผ่านมาในอดีตไม่เคยเกิดความผิดปกติขึ้นกับข้อมูลนี้ และประการที่สอง จะเกิดความผิดปกติหรือเกิดการเปลี่ยนแปลงของข้อมูลมากในช่วงเวลาสั้นๆ ซึ่งที่ผ่านมาในอดีตไม่เคยเกิดขึ้นในลักษณะนี้
- การปรับอัตราส่วนความสำคัญของข้อมูลมีผลต่อการทำสมูทติ้งเพื่อลดการแกว่งของข้อมูล

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 สรุปและบทวิจารณ์

ระบบเครือข่ายในปัจจุบันควรมีเครื่องมือที่ช่วยในการตรวจจับความผิดปกติที่เกิดขึ้นบนระบบเครือข่าย เพื่อให้ผู้ดูแลระบบสามารถทำการวิเคราะห์และแก้ไขปัญหาต่างๆ ที่เกิดขึ้นได้ ซึ่งส่งผลให้สามารถใช้งานระบบเครือข่ายได้อย่างมีประสิทธิภาพสูงสุด ระบบตรวจจับความผิดปกติในระบบเครือข่ายโดยอาศัยการเปลี่ยนแปลงเอนโทรปีสามารถที่จะทำการตรวจจับความผิดปกติที่เกิดขึ้นในระบบเครือข่าย และสามารถแสดงผลในรูปแบบกราฟของเอนโทรปีให้ผู้ดูแลระบบสามารถทำการตรวจสอบปริมาณการใช้งานเครือข่ายได้

5.2 ปัญหาและอุปสรรค

1) ผู้พัฒนายังขาดความรู้และประสบการณ์ในการพัฒนาโปรแกรม และการวางแผนบริหารจัดการเครือข่าย ทำให้การออกแบบการวิเคราะห์ระบบอาจมีประสิทธิภาพไม่ดีเท่าที่ควร
2) มีปัญหาเกี่ยวกับการเขียนโปรแกรมบางช่วง เพราะต้องใช้เวลาศึกษาและค้นหาอัลกอริทึมที่สามารถทำให้โปรแกรมทำงานได้อย่างสมบูรณ์
3) ปัญหาการนำข้อมูลมาสร้างโปรไฟล์ไม่สัมพันธ์กัน เนื่องจากโปรแกรมที่พัฒนาขึ้นมีการเปิดให้ผู้ใช้สามารถกำหนดข้อมูลที่ต้องการสร้างโปรไฟล์ได้เอง โดยข้อมูลของโปรไฟล์เดียวกันจะต้องมีความสัมพันธ์กัน ถ้าหากข้อมูลไม่มีความสัมพันธ์กัน การคำนวณเอนโทรปีอาจไม่สามารถบอกถึงความผิดปกติที่เกิดขึ้นได้ดีเท่าที่ควร
4) ปัญหาการแสดงผลกราฟ ผู้วิจัยยังขาดทักษะการเขียนโปรแกรม และการใช้งานไลบรารี่ต่างๆ ทำให้การแสดงผลกราฟอาจไม่สวยงามและไม่รองรับความต้องการการแสดงผลในอีกหลายๆ รูปแบบ
5) ผู้พัฒนายังขาดประสบการณ์ในการวิเคราะห์ข้อมูลเครือข่ายและการตีความจากกราฟ อาจทำให้วิเคราะห์ผลผิดพลาดไปบ้าง

5.3 แนวทางแก้ไข

1) ขอคำปรึกษาจากผู้มีประสบการณ์ในการพัฒนาโปรแกรม และผู้ที่มีประสบการณ์ในการบริหารจัดการเครือข่ายในเรื่องการออกแบบการวิเคราะห์ระบบ

2) เพิ่มตัวแปรเอสเอ็นเอ็มพีเพื่อให้ได้รับข้อมูลมาใช้ในการวิเคราะห์ปัญหามากขึ้น
3) สอบถามหรือขอความช่วยเหลือจากผู้ที่มีประสบการณ์ในการเขียนโปรแกรมเพื่อให้โปรแกรมทำงานได้ผิดพลาดน้อยที่สุด
4) ก่อนจะกำหนดข้อมูลเพื่อสร้างโปรไฟล์สำหรับมอนิเตอร์ต้องมีการศึกษาความสัมพันธ์ของข้อมูลก่อนว่ามีความสัมพันธ์กันหรือไม่เพื่อประสิทธิภาพสูงสุดในการวิเคราะห์หาความผิดปกติของเครือข่ายด้วยการคำนวณเอนโทรปี
5) เพิ่มฟังก์ชันการแสดงผลของกราฟให้มีรูปแบบที่หลากหลายมากยิ่งขึ้น

5.4 แนวทางการพัฒนาต่อ

1) พัฒนาความสามารถของโปรแกรมให้ใช้งานได้กับระบบเครือข่ายที่มีลักษณะการใช้งานหลากหลายประเภท
2) เพิ่มเติมตัวแปรเอสเอ็นเอ็มพี เพื่อให้ได้ข้อมูลมาใช้ในการวิเคราะห์มากขึ้น
3) พัฒนาโปรแกรมใช้ทรัพยากรของระบบน้อยลง
4) พัฒนาโปรแกรมให้สามารถแจ้งเตือนผู้ดูแลระบบเมื่อเกิดปัญหาการใช้งานในเครือข่าย
5) ศึกษาหาแนวทางที่สามารถวิเคราะห์ได้ว่าความผิดปกติที่เกิดขึ้นบนระบบเครือข่ายมีสาเหตุมาจากอะไร

บรรณานุกรม

[1] ชมภูนุช สันธนะผล, ชาญกฤษณ์ มากมี, ชาญวิทย์ พิณพาทย์. **"โปรแกรมวิเคราะห์เครือข่ายอัตโนมัติ"** ปริญญานิพนธ์วิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง. 2553.

[2] สาขาวิชาวิศวกรรมคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง. **"Multi Router Traffic Grapher."** [Online]. Available : http://www.ce.kmitl.ac.th/download.php?DOWNLOAD_ID=76&database=pj_download.

[3] G. Nychis, V. Sekar, D. G. Andersen, etc. **"An Empirical of Entropy-based Anomaly Detection."** Thesis of Information Networking Institute Carnegie Mellon University. 2007.

[4] Qian Quan, Che Hong-Yi, Zhang Rui. **"Entropy Based Method for Network Anomaly Detection."** Shanghai University. 15th IEEE Pacific Rim International Symposium on Dependable Computing. 2009.

[5] Cisco Systems, Inc. **"SNMP Object Navigator."** [Online]. Available : http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do. 2013.