บทที่ 3

การออกแบบและพัฒนา

3.1 บทนำ

การออกแบบและพัฒนาซอฟต์แวร์เป็นขั้นตอนที่วางโครงสร้างของซอฟแวร์ว่าจะมีส่วนประกอบอะไรบ้าง และแต่ละส่วนมีการทำงานอย่างไร และมีขั้นตอนการทำงานอย่างไรโดยมีการใช้เครื่องมือต่างๆ มาช่วยในการพัฒนาโดยมีรายละเอียดดังต่อไปนี้

3.2. การออกแบบซอฟต์แวร์

ระบบตรวจจับการใช้งานเครือข่ายที่ผิดปกติโดยใช้เน็ตเวิร์กโพรไฟล์ มีส่วนประกอบของการทำงานหลักๆ แบ่งเป็น 5 ส่วนหลักดังต่อไปนี้

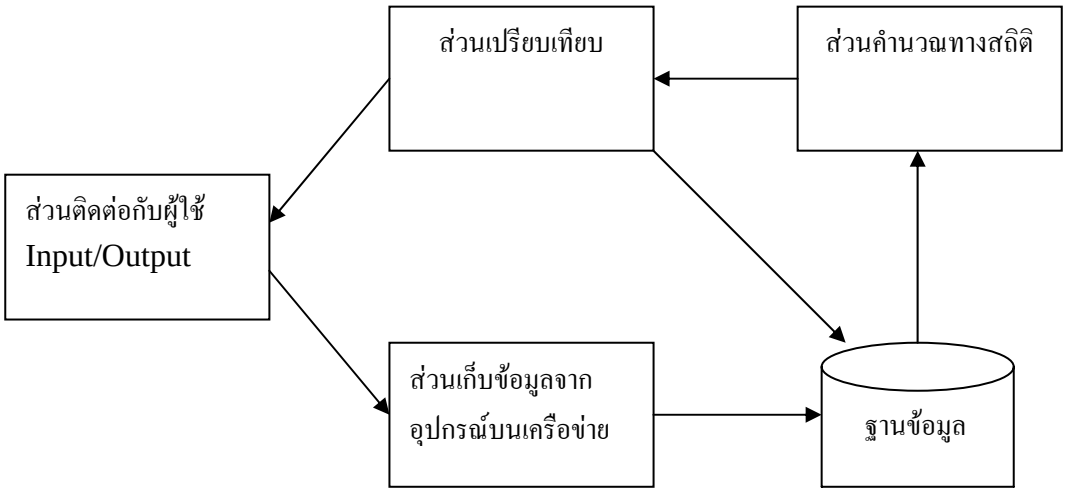
3.2.1. ส่วนเก็บข้อมูลจากอุปกรณ์บนเครือข่าย

3.2.2. ส่วนฐานข้อมูล

3.2.3. ส่วนคำนวณทางสถิติ

3.2.4. ส่วนเปรียบเทียบ

3.2.5. ส่วนติดต่อกับผู้ใช้



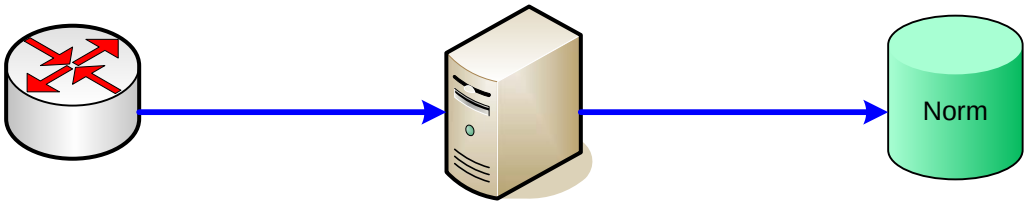
รูปที่3.1 ส่วนประกอบของซอฟต์แวร์

3.2.1. ส่วนเก็บข้อมูลจากอุปกรณ์บนเครือข่าย

ส่วนนี้มีการทำงาน โดยไปร้องขอข้อมูลของปริมาณการใช้งานเครือข่าย จากอุปกรณ์ภายในเครือข่าย เช่น เราท์เตอร์ (Router) หรืออีเธอร์เน็ตสวิตซ์ (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)

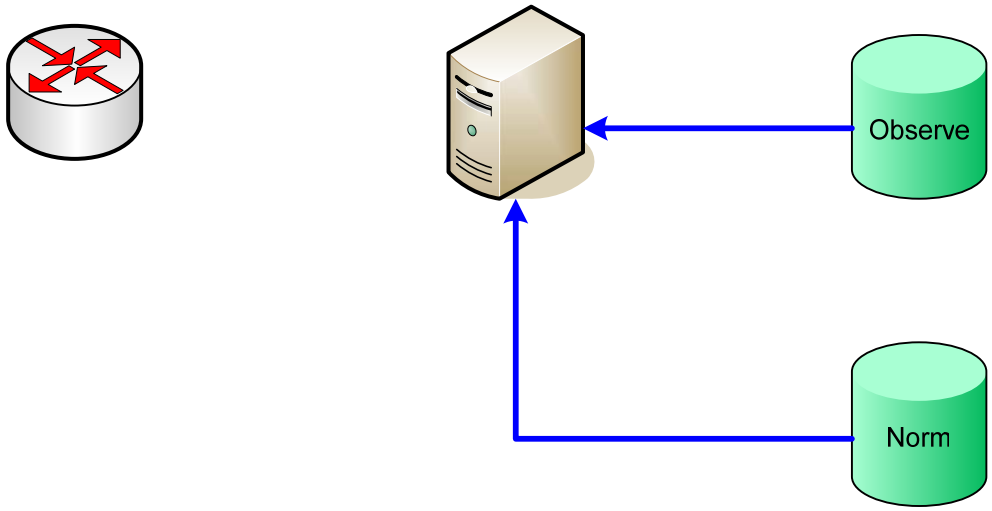
3. ifInNUcastPkts หมายถึง จำนวนแพ็กเก็ตที่ได้รับมาจากการส่งแบบไม่ใช้ยูนิคาส (non-unicast) (เช่น subnetwork-broadcast หรือ subnetwork-multicast)) จากกลุ่มเน็ตเวิร์กย่อยเพื่อถูกส่งต่อไปยังโพรโตคอลชั้นสูงกว่า (higher-layer protocol)
4. ifInDiscards หมายถึง จำนวนของแพ็กเก็ตขาเข้าซึ่งถูกเลือกให้ถูกคัดทิ้งไปถึงแม้ว่าจะไม่เกิดความผิดพลาดใดๆ 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 เพื่อหาความผิดปกติของการใช้งานโดยในส่วนการคำนวณนั้นจะทำการคำนวณในแต่ละอินเตอร์เฟสที่มีสถานะพร้อมใช้งานและแบ่งชุดข้อมูลจากตาราง 3.1 เพื่อจะทำการคำนวณออกเป็น 3 กลุ่มดังนี้

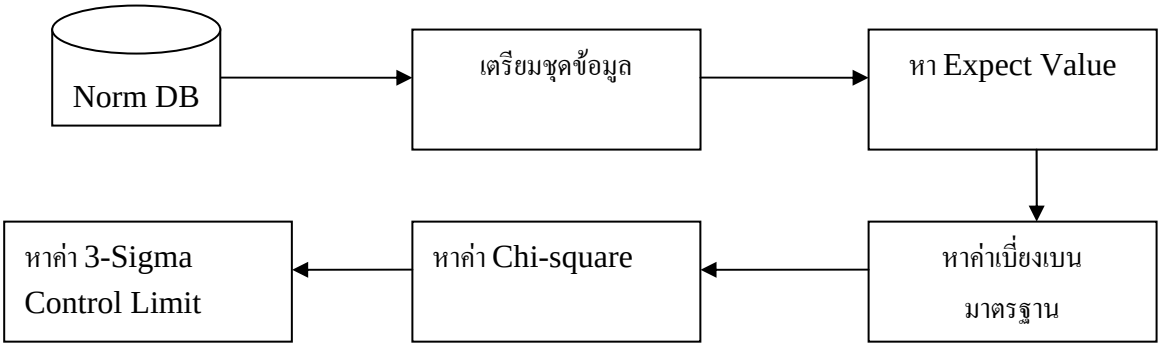
1. กลุ่มข้อมูลขาเข้าของอินเตอร์เฟส (Inbound)
2. กลุ่มข้อมูลขาออกของอินเตอร์เฟส (Outbound)
3. กลุ่มข้อมูลขนาดของแพ็กเก็ต(etherStats packets size)



รูปที่ 3.3 การเรียกข้อมูลจากฐานข้อมูลเพื่อทำการคำนวณ

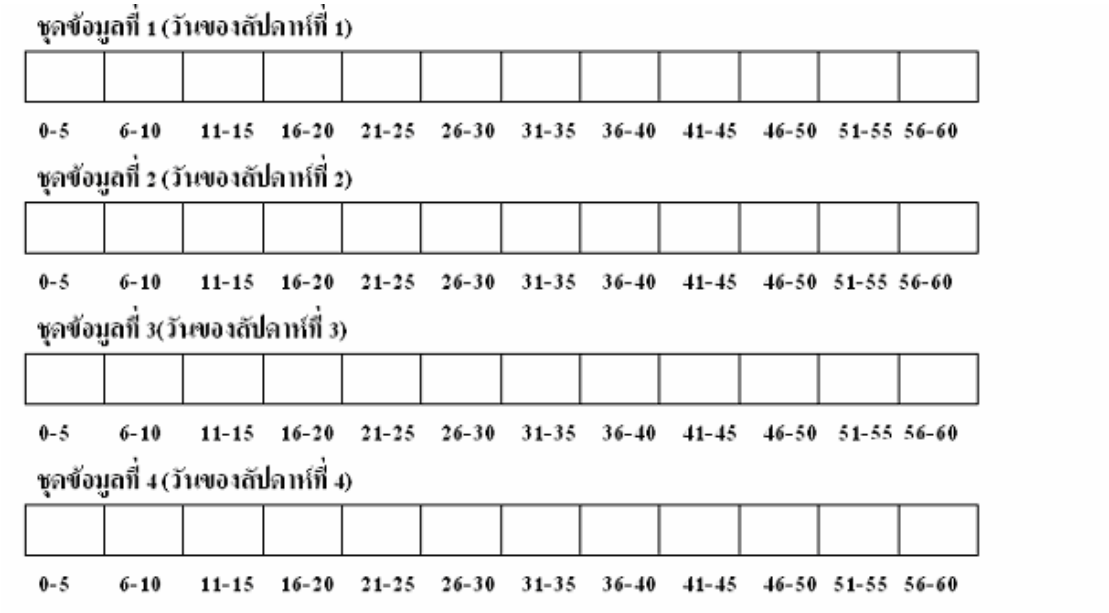
โดยส่วนคำนวณทางสถิตินั้นมีการคำนวณใน 2 ลักษณะดังนี้

3.2.3.1. ส่วนคำนวณเพื่อสร้างขอบเขตการใช้งานภาวะปกติ (การสร้าง Upper Bound)



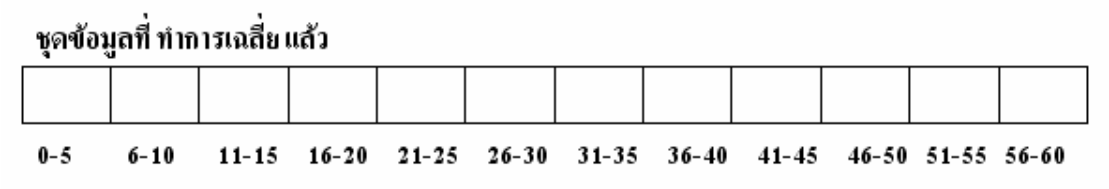
รูปที่ 3.4 ขั้นตอนการคิดคำนวณค่า Upper bound จากข้อมูลการใช้งานปกติ

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

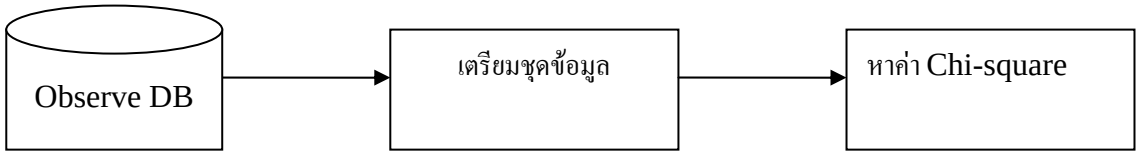


รูปที่ 3.6 ข้อมูลที่ถูกทำการเฉลี่ยแล้ว

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 ของแต่ละตัวแปรโดยที่การคำนวณ EWMA นั้นผลลัพธ์ที่ได้ เป็นข้อมูลที่มีการถ่วงน้ำหนักด้วยค่าข้อมูลในช่วงเวลาก่อนหน้าที่ผ่านๆมา เพื่อที่จะสามารถเปรียบเทียบข้อมูลที่ผ่านมาแล้วกับค่าปริมาณการใช้งานในปัจจุบันมีแนวโน้มอย่างไรโดย EWMA คำนวณโดยใช้สมการ ดังนี้โดย 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
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

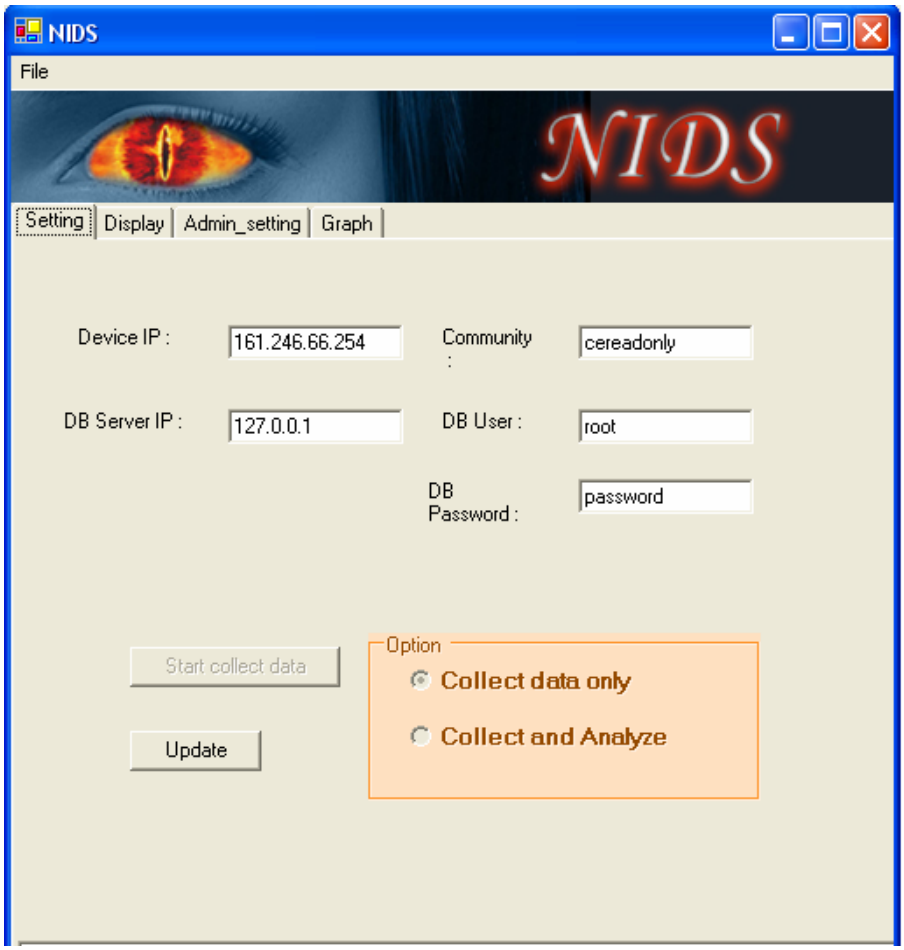
ในส่วนนี้เป็นการนำเอาผลลัพธ์จากส่วนการคำนวณทั้งค่าขอบเขตการใช้งานเครือข่ายในลักษณะที่เป็นปกติและค่าการใช้งานเครือข่ายในปัจจุบันนำมาเปรียบเทียบกันโดยเมื่อเปรียบเทียบแล้วผลที่ได้แบ่งเป็น 2 กรณี

- 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



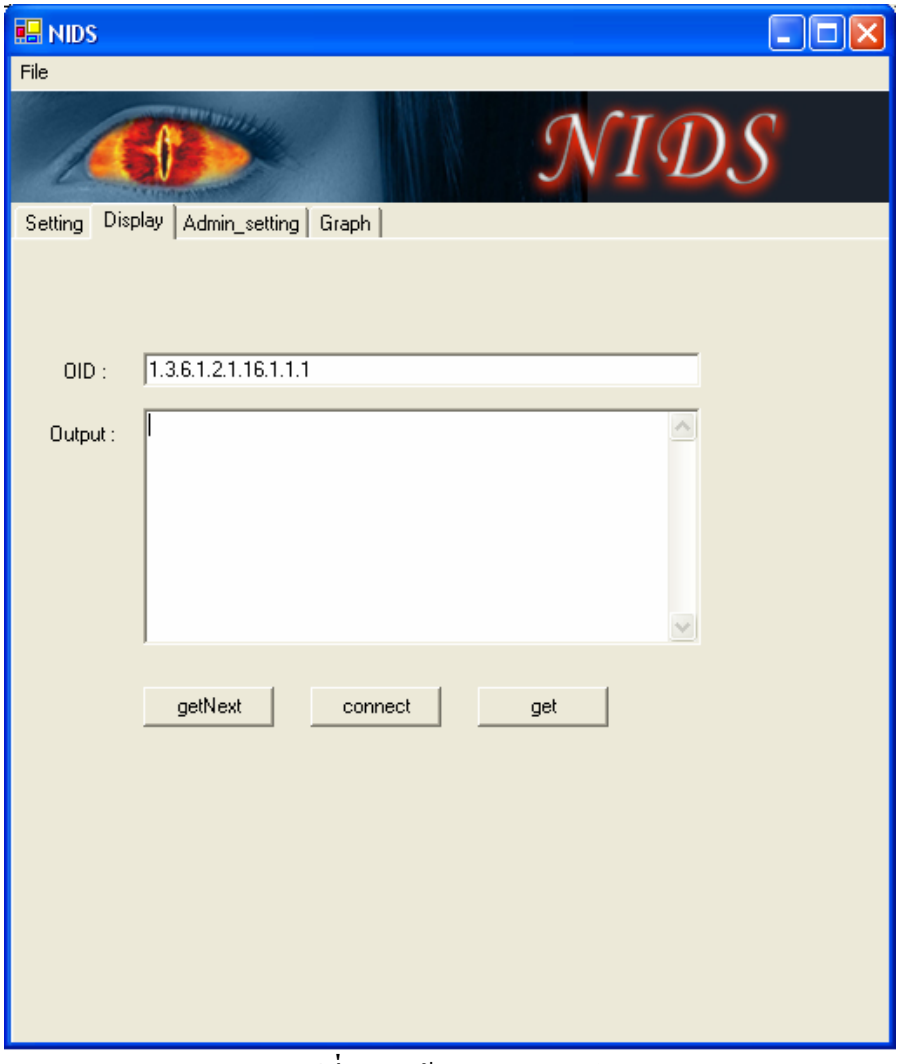
รูป 3.8 หน้า setting ของโปรแกรม

<u>Input</u>

- 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

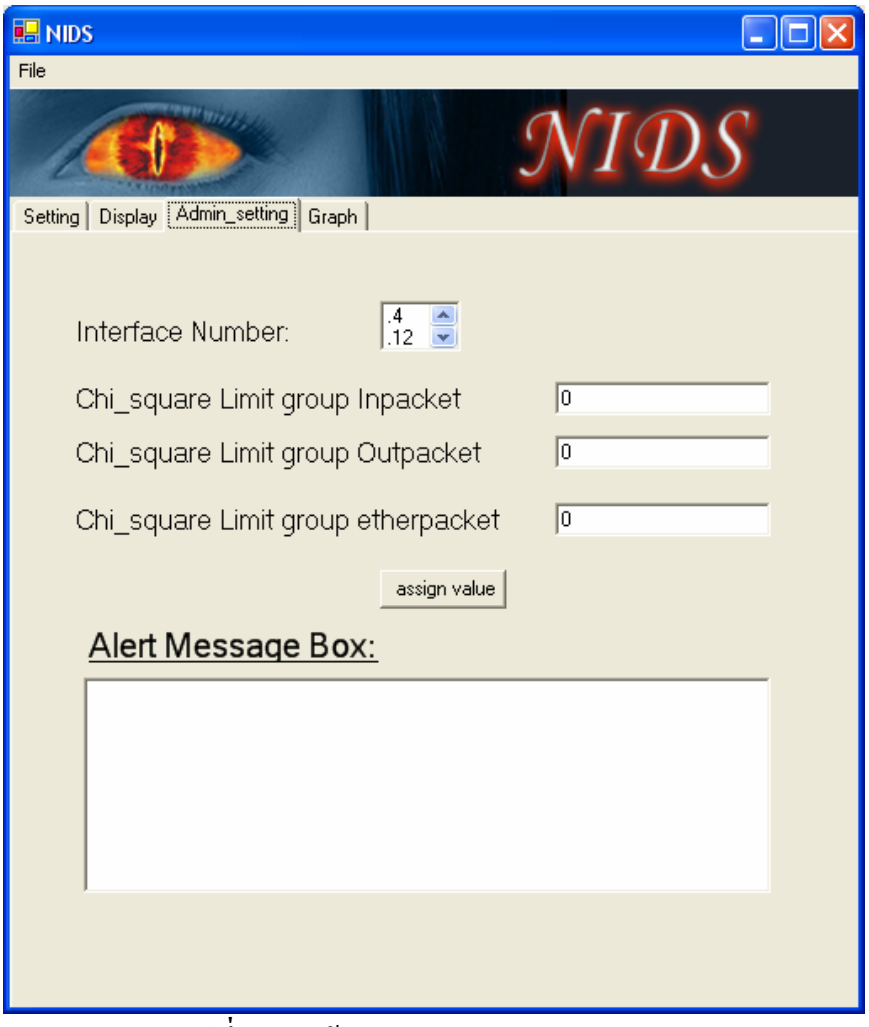
<u>Input</u>

- มีเลข OID ที่ต้องการให้โปรแกรมไปดึงข้อมูลมาแสดง

<u>Output</u>

- แสดงข้อมูลต่างๆ ที่มีอยู่ในตัวอุปกรณ์ตามค่า OID ที่ผู้ใช้ใส่เข้ามา

3.2.5.3. หน้า Admin setting มีดังต่อไปนี้



รูปที่ 3.10 หน้า Admin setting ของโปรแกรม

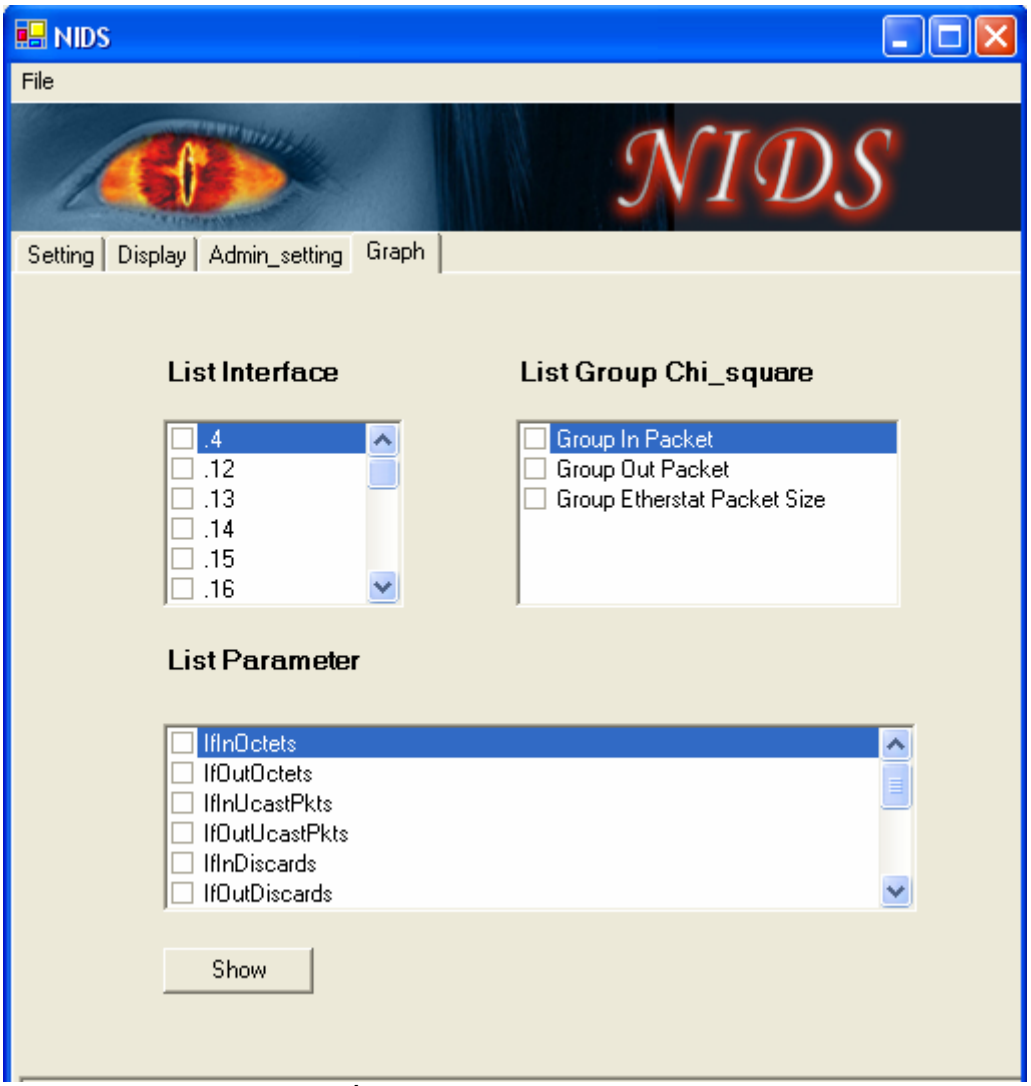
<u>Input</u>

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

<u>Output</u>

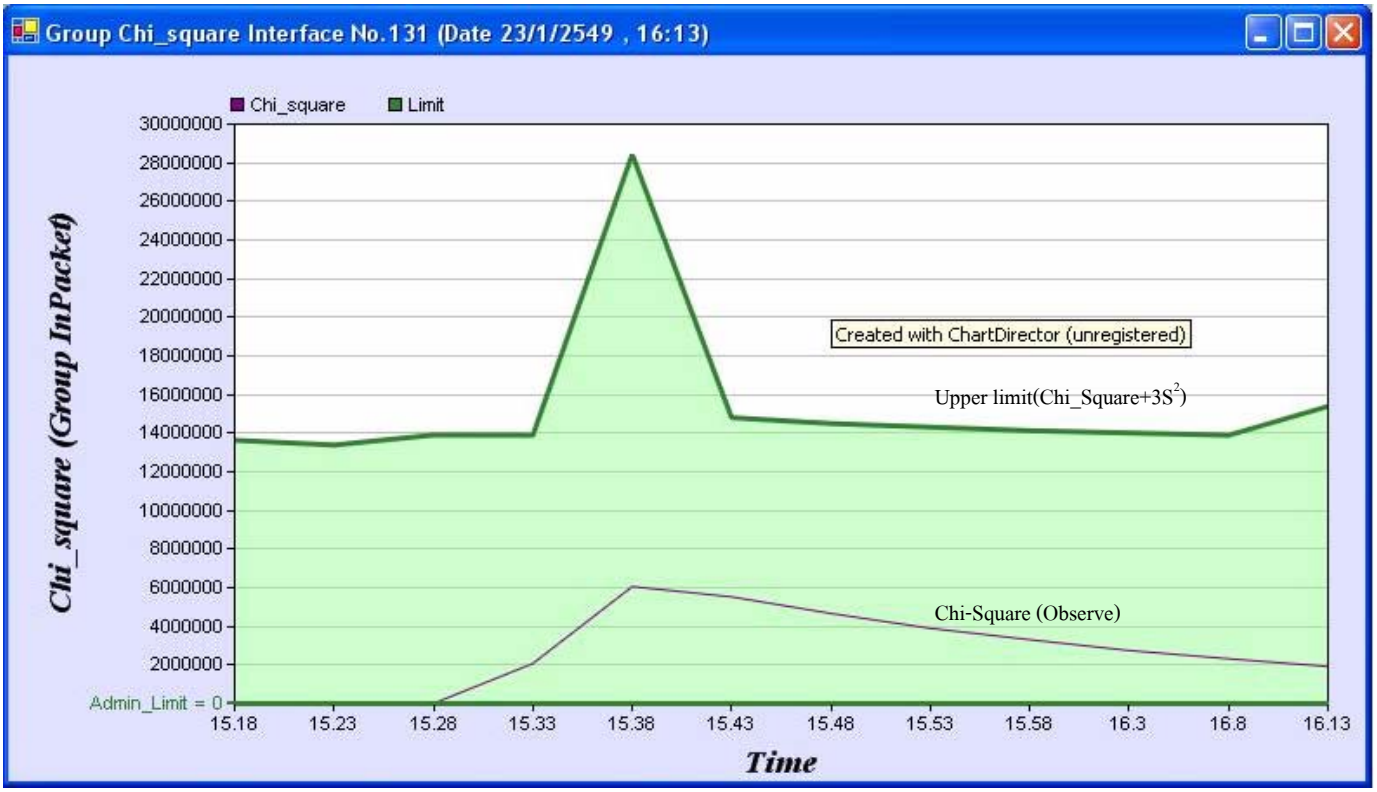
- ข้อความแจ้งเตือนความผิดปกติ

3.5.2.4. หน้า Graph มีดังต่อไปนี้

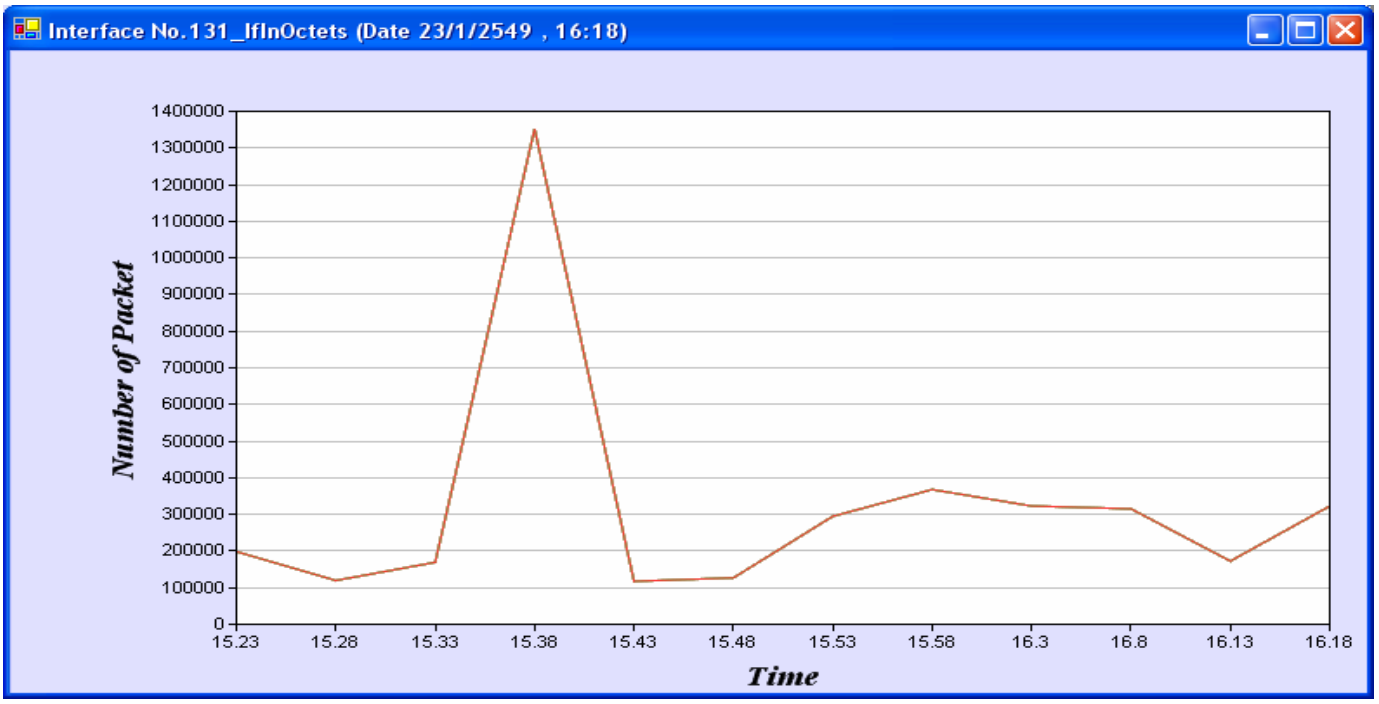


รูปที่ 3.11 หน้า Graph ของโปรแกรม

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