บทที่ 3
การออกแบบและพัฒนาโปรแกรม

3.1 รายละเอียดของการพัฒนา

ในการจัดทำโปรแกรมสำรวจเครือข่าย และระบบคอมพิวเตอร์จำเป็นต้องศึกษาทฤษฎีและข้อมูลที่ใช้ในการค้นหา และรวบรวมข้อมูลของคอมพิวเตอร์เครื่องอื่นที่อยู่ในเครือข่าย โดยในโปรแกรมของเราได้ใช้เทคนิคหลายๆอย่าง ดังนี้

- ใช้เทคนิค Port scanning (TCP connect scan) เพื่อค้นหาพอร์ตที่ต้องการบนเครื่องปลายทาง และยังนำมาใช้ในการค้นหาว่ามีเครื่องใดเปิดใช้งานอยู่บ้าง
- ใช้วิธีการของ SNMP เพื่อรวบรวมข้อมูลการใช้งานระบบเครือข่าย ซึ่งเมื่อนำมารวมกับข้อมูลของเครื่องปลายทางที่ได้รับมาจะทำให้สามารถพัฒนาโปรแกรมที่มีความสามารถในการวิเคราะห์ปริมาณการใช้งานระบบเครือข่ายในด้านต่างๆได้ในระดับนึง

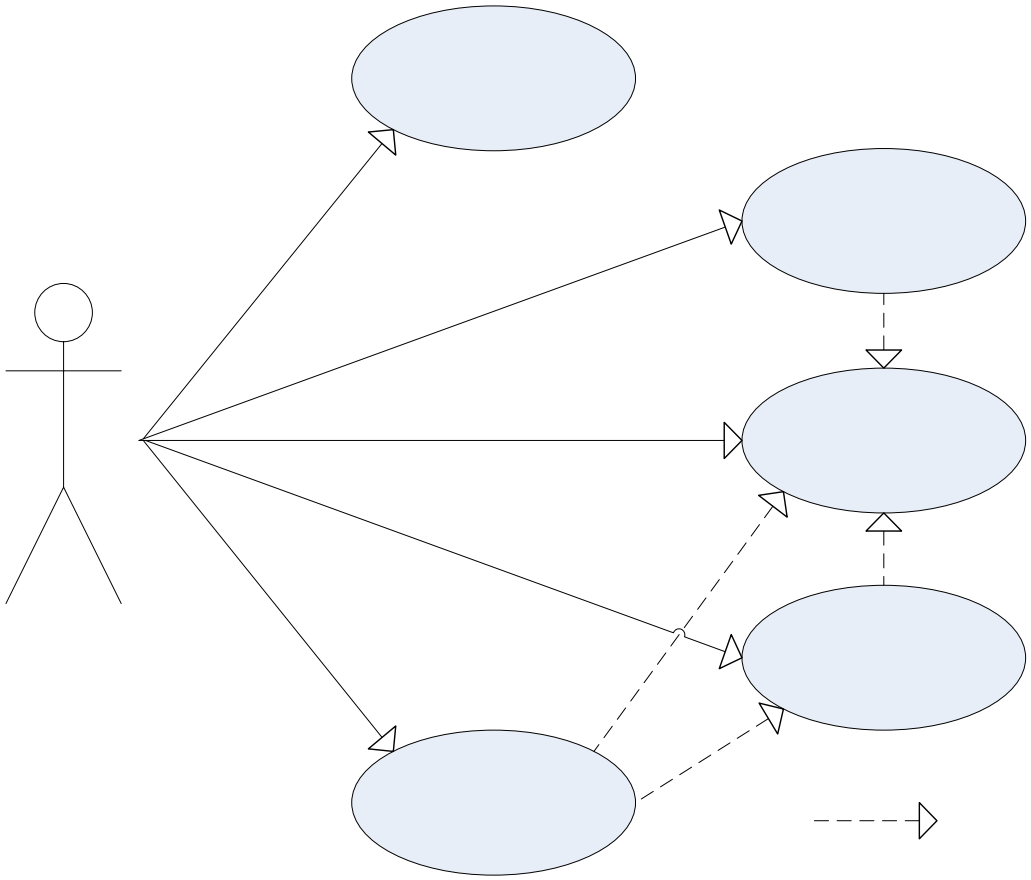
เครื่องมือต่าง ๆ ที่ใช้ในการพัฒนา

ได้แก่

- Microsoft Visual Studio .NET 2003
- Winpcap 3.1
- Nmap 3.95
- SNMP++.NET v. 1.16
- Chart Director for .NET v.4.0
- Microsoft Windows 2000 หรือ XP

3.2 การออกแบบโครงสร้างของโปรแกรม

Use case Diagram

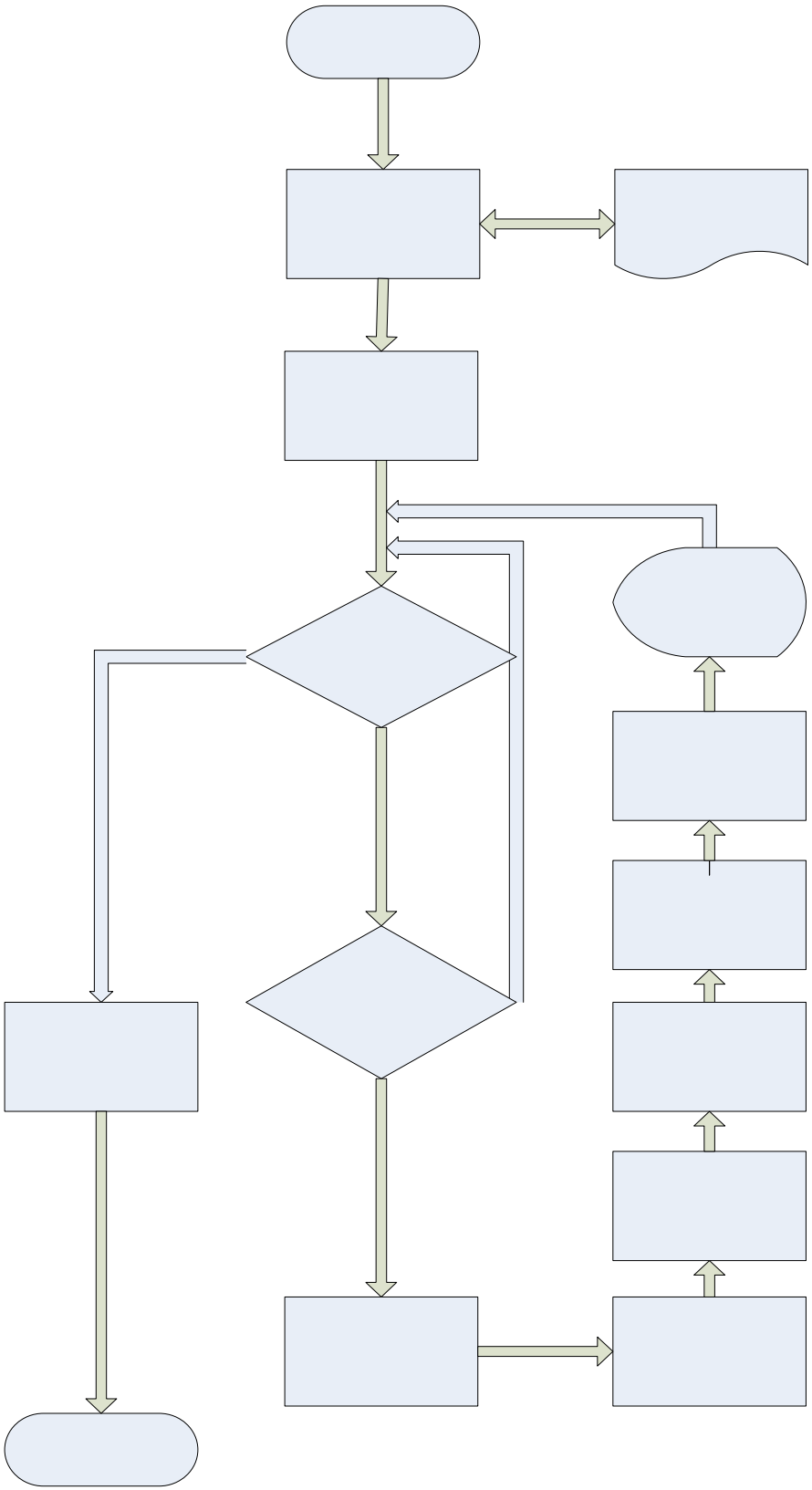


รูปที่ 3.1 Use case Diagram ของโปรแกรม

Set/Load Project File	ทำการตั้งค่า Project File ต่างๆเพื่อเป็นข้อมูลอ้างอิงการทำงาน
Enable / Disable interval scan	สั่งให้โปรแกรมเริ่มทำการแสกนแบบเป็นช่วงเวลาเพื่อเก็บข้อมูล
Scan Specific Host	สั่งให้โปรแกรมสแกนเครื่องปลายทางที่สนใจ
Select Date/Time View	เลือกวันที่และเวลาที่จะทำการเขียน Graph และ Chart
Read History Graph and Chart	อ่านข้อมูล Graph และ Chart ข้อมูลต่างๆที่ได้จากการแสกนและคำนวณ

ตารางที่ 3.1 แสดงคำอธิบาย Use case Diagram ของโปรแกรม

Flow Chart



รูปที่ 3.2 Flow Chart Diagram ของส่วนการสแกนระบบเครือข่ายโปรแกรม

Start	เริ่มต้นโปรแกรม
Set / Load Configuration File	ตั้งค่าเริ่มต้นการทำงาน หรือนำค่าเริ่มต้นที่มีอยู่แล้วมาใช้งาน
Project Configuration File	ไฟล์ซึ่งมีค่าเริ่มต้นการทำงานเก็บเอาไว้
Start Scan Network Timer	เริ่มจับเวลาในก่อนที่จะ scan
Scan Enable	สามารถทำการ scan ได้หรือไม่
Minute is Times of 10 ?	ครบ 10 นาทีแล้ว ใช่หรือไม่
Interval Network Scan	เริ่มทำการ scan
Snmp Collecting	รวบรวมข้อมูล SNMP
Internet Connection Probe	สำรวจสถานะการเชื่อมต่อระหว่างระบบเครือข่ายกับ Internet
Scan Host Online	ตรวจหาเครื่องคอมพิวเตอร์ที่เปิดใช้งานภายในเครือข่าย
Calculation of current data	ทำการคำนวณข้อมูลที่มีอยู่
Store Data	เก็บข้อมูลทีได้มา
Update Display	แสดงผลลัพธ์ออกทางหน้าจอโปรแกรม
Process Log File	จัดเก็บ Log File
End	สิ้นสุดการทำงานของโปรแกรม

ตารางที่ 3.2 แสดงคำอธิบาย Flow Chart Diagram ของโปรแกรม

3.3 โครงสร้าง และการทำงานของโปรแกรม

โครงสร้างการทำงานของโปรแกรมจะประกอบด้วยส่วนประกอบที่สำคัญ ได้แก่

ส่วนติดต่อกับผู้ใช้ โดยในขั้นตอนนี้จะได้รับ input จากผู้ใช้ถึงรายละเอียดและขอบเขตของเครือข่ายย่อยที่ผู้ใช้ต้องการให้โปรแกรมสำรวจซึ่งแบ่งออกเป็น 3 ส่วนย่อยๆ คือ

1. รายละเอียดของอุปกรณ์เครือข่ายที่จะทำการสำรวจค่าภายใต้ Protocol SNMP
2. IP Range ของ เครือข่ายย่อยแต่ละเครือข่าย
3. รายชื่อของ URL หรือ IP ที่จะใช้เป็นตำแหน่งอ้างอิงในการสำรวจสถานะของการเชื่อมต่อกับ Internet

เมื่อได้รับรายละเอียดต่างๆครบแล้วก็จะทำการบันทึกไว้เป็น Project File ซึ่งจะนำไปใช้ในการทำงาน

ส่วนสำรวจระบบเครือข่าย ซึ่งแบ่งออกเป็น 4 ส่วนย่อยๆคือ

- การสำรวจปริมาณการใช้ Bandwidth ของเครือข่ายย่อย
- การสำรวจสถานะของเครื่องคอมพิวเตอร์ภายในเครือข่ายย่อย
- การสำรวจสถานะของการเชื่อมต่อระหว่างระบบเครือข่ายกับ Internet
- การประมวลผลที่ได้จาก 3 ส่วนย่อย และส่งกลับไปให้

ส่วนแสดงผล เพื่อแสดงข้อมูลในรูปแบบต่างๆให้กับผู้ใช้นั่นเอง

นอกจากส่วนการทำงานหลักแล้วยังมีส่วนประกอบย่อยอีก 1 ส่วน คือ

ส่วนการสำรวจข้อมูลเฉพาะเครื่อง

รายละเอียดของทั้ง 4 ส่วน มีดังนี้

3.3.1 ส่วนติดต่อกับผู้ใช้ เป็นส่วนที่จะรับ Input จากผู้ใช้เพื่อนำไปใช้งานในส่วนหลักต่อไป สำหรับ Input ที่รับมาจากผู้ใช้แบ่งออกเป็น 3 ส่วนย่อยคือ

1. รายละเอียดของอุปกรณ์ในเครือข่ายที่รองรับ SNMP ที่สนใจได้แก่ IP ของ Interface ของอุปกรณ์ที่ตอบรับ Protocol SNMP และ Read Community ของอุปกรณ์นั้นๆ
2. IP Range ของเครือข่ายย่อย ซึ่งมีข้อจำกัดคือต้องสอดคล้องกับ Interface ของหนึ่งในอุปกรณ์เครือข่ายที่รองรับ SNMP ที่สนใจไม่เกิน 2 port โดย IP Range แต่ละชุดจะกลายเป็นเครือข่ายย่อย 1 เครือข่ายนั่นเอง
3. รายชื่อของ URL หรือ IP ที่จะใช้เป็นตำแหน่งอ้างอิงในการสำรวจสถานะของการเชื่อมต่อกับ Internet ซึ่งควรจะเป็น URL หรือ IP ภายนอกระบบที่มีความน่าเชื่อถือพอสมควรโดย Default แล้วจะมีมาให้ 1 URL คือ www.google.co.th

ตัวอย่างข้อมูลที่ได้รับ

เครือข่ายย่อยที่ 1 :

IP Range 161.246.5.91 - 161.246.5.130 สอดคล้องกับ Interface Fast Ethernet 0/13 และ 0/14 ของอุปกรณ์เครือข่ายที่รองรับ SNMP ที่ Interface IP 161.246.5.253 และมี Read Community เป็น cereadonly

เครือข่ายย่อยที่ 2 :

IP Range 161.246.5.131 - 161.246.5.170 สอดคล้องกับ Interface Fast Ethernet 0/6 และ 0/7 ของอุปกรณ์เครือข่ายที่รองรับ SNMP ที่ Interface IP 161.246.5.253 และมี Read Community เป็น cereadonly

3.3.2 ส่วนสำรวจระบบเครือข่าย เป็นส่วนที่นำข้อมูลจากส่วนแรกมาทำการสำรวจและหาข้อมูลต่างๆของระบบเครือข่าย และเก็บข้อมูลที่ได้นั้นประมวลผลและส่งให้กับส่วนสุดท้ายเพื่อนำไปแสดงผล ประกอบด้วย การทำงาน 4 ส่วนคือ

1. การสำรวจปริมาณการใช้ Bandwidth ของเครือข่ายย่อย โดยจะทำการดึงข้อมูลปริมาณการใช้ระบบเครือข่ายจากอุปกรณ์ SNMP และทำการบันทึกลงใน Log File แยกตามเครือข่ายย่อย
2. การสำรวจสถานะของเครื่องคอมพิวเตอร์ภายในเครือข่ายย่อย โดยจะทำการ Scan Port ของเครื่องคอมพิวเตอร์ และทำการบันทึกลง Log File แยกตามเครือข่ายย่อย
3. การสำรวจสถานะการเชื่อมต่อระหว่างระบบเครือข่ายกับ Internet โดยจะทำการ Scan Port ไปยังเครื่องเป้าหมายที่จะสุ่มออกมาจาก URL หรือ IP ที่อยู่ใน List ของตำแหน่งอ้างอิงและทำการบันทึกลงใน Log File
4. ส่วนประมวลผล ซึ่งจะนำข้อมูลที่ได้จากส่วนที่ 3.3.2.1 และ 3.3.2.2 มาประมวลผลร่วมกันได้ปริมาณการใช้งานโดยเฉลี่ยของแต่ละเครื่องแยกตามเครือข่ายย่อยและทำการบันทึกลงใน Log File

3.3.3 ส่วนแสดงผล จะทำหน้าที่นำข้อมูลที่อยู่ใน Log File มาจัดแสดงเป็น กราฟ, แผนภูมิแท่ง หรือรายงานประกอบไปด้วย 3 ส่วน คือ

1. ส่วนการแสดงผลแผนภูมิแท่งซึ่งมีหัวข้อหลักในการแสดงคือ

- ปริมาณ Bandwidth รวม
- ปริมาณ Bandwidth โดยเฉลี่ยต่อวินาที

และมีหัวข้อย่อยคือ

- Download และ Upload (รวมทั้งหมด)
- Download อย่างเดียว
- Upload อย่างเดียว

โดยทั้งหมดจะแสดง 5 ลำดับ ของเครื่องคอมพิวเตอร์ในเครือข่ายย่อยที่มีการใช้งานสูงสุด

2. ส่วนการแสดงผลกราฟ 3 มิติซึ่งมีหัวข้อหลักในการแสดงคือ

- ปริมาณ Bandwidth ในช่วงเวลาต่างๆใน 1 วัน
- จำนวนของเครื่องคอมพิวเตอร์ที่ Online ในช่วงเวลาต่างๆใน 1 วัน

ซึ่งมีหัวข้อย่อย คือ

- Download และ Upload
- Download อย่างเดียว
- Upload อย่างเดียว

โดยทั้งหมดสามารถเลือกแสดงเฉพาะเครือข่ายย่อยบางเครือข่ายเพื่อเปรียบเทียบปริมาณการใช้งานได้ชัดเจนและยังสามารถเลือกวันที่ใช้ในการแสดงผลได้ นอกจากนี้ในส่วนนี้ยังมี

หน้าต่างย่อยเพื่อตรวจสอบว่า ณ เวลาที่กำหนดนั้นมีเครื่องคอมพิวเตอร์เครื่องใดในเครือข่ายย่อย Online อยู่บ้างอีกด้วย

3. ส่วนการแสดงลำดับของเครื่องคอมพิวเตอร์ที่มีการใช้งาน Bandwidth สูงสุด 3 ส่วนย่อย คือ

- Download และ Upload
- Download อย่างเดียว
- Upload อย่างเดียว

โดยทั้งหมดจะถูกแสดงทีละเครือข่ายย่อยตามที่ได้เลือกไว้

นอกจากส่วนการทำงานหลักแล้วยังมีส่วนประกอบย่อยอีก 1 ส่วน คือ

3.3.4 ส่วนการสำรวจข้อมูลเฉพาะเครื่อง รายละเอียดจะแบ่งออกเป็น 3 ส่วน ดังนี้

1. ส่วนรับ IP และ Host Name
2. ส่วนรับของรายละเอียดที่ต้องการตรวจสอบแบ่งออกเป็น

- Service Scan : จะทำการตรวจสอบ IP/Hostname ที่กำหนดว่ามีการเปิดบริการใดอยู่บ้าง
- Trojan Scan : จะทำการตรวจสอบ IP/Hostname ที่กำหนดว่ามีการติด Trojan หรือ Worm ที่อาจเป็นอันตรายต่อระบบเครือข่ายหรือไม่
- Specific Scan : จะทำการตรวจสอบ IP/Hostname ที่กำหนดตาม Port Number ที่ผู้ใช้ได้ป้อนเข้ามา

3. ส่วนที่แสดงผลการตรวจสอบ IP / Hostname ที่กำหนด

3.4 การพัฒนาโปรแกรม

3.4.1 ศึกษาและทดลองการดึงค่า SNMP/RMON จาก อุปกรณ์เครือข่ายโดยใช้ Library SNMP++ ด้วยภาษา C#

อุปสรรค

- การ Handler Error ทำได้ยาก
- ผู้ใช้ไม่สามารถจดจำได้ว่า Object ID ใดทำหน้าที่ใด
- อุปกรณ์ทั่วไปรองรับเพียง SNMP พื้นฐานโดยการรองรับ RMON นั้นก็มีเพียงบางส่วนของ Object ID ทั้งหมด

วิธีการแก้ไข

- ทำการบังคับข้อมูลที่ผู้ใช้ป้อนเพื่อลดความผิดพลาดจาก Library และลดภาระของผู้ใช้ในการค้นหา Object ID ที่ถูกต้อง

- อาศัยการดึงข้อมูลจาก SNMP พื้นฐานเป็นหลักเพื่อลดความผิดพลาดในกรณีที่อุปกรณ์เครือข่ายที่ต้องการไม่รองรับ Object ID ที่กำหนดไว้

3.4.2 ศึกษาและทดลองการสร้าง Child Process เพื่อเรียกโปรแกรม Nmap ในการ Scan Port ที่สนใจ ด้วยภาษา C#

อุปสรรค

- Child Process ที่เรียกออกมาจะไม่ฟ้อง Error เมื่อเกิดความผิดพลาดและจะปิดตัวลง
- ในบางกรณี Child Process จะไม่ยอมปิดตัวเองทำให้ไม่สามารถสร้าง Child Process อีกครั้งเมื่อต้องการได้

วิธีการแก้ไข

- มีการตรวจสอบว่ายังคงมี Child Process เดิมอยู่หรือไม่ถ้าหากพบว่ามีก็จะทำการ Terminate ทิ้งก่อนจะมีการสร้าง Child Process ใหม่

3.4.3 ศึกษาและทดลองการแตก Thread ให้กับ Function เพื่อลดภาวะ Not Responding ของโปรแกรม ในภาษา C#

อุปสรรค

- วิธีการใช้ Thread นั้นอาศัยการเรียก Method Name ที่ต้องการแตกย่อยออกมาโดยไม่อนุญาตให้มีการ Pass หรือ Return Parameter จึงทำให้โครงสร้างของโปรแกรมเปลี่ยนไปจากเดิม
- การเรียกใช้ค่าจาก Class อื่นจากภายใน Thread ก็เป็นผลให้เกิดความผิดพลาดขึ้นได้

วิธีการแก้ไข

- รวบ Method หลักๆเข้ามาอยู่ใน Class เดียวกันเพื่อลดความผิดพลาดในการส่งผ่านค่าข้าม Class
- มีการใช้การ Locking ช่วยในกรณีที่มีการใช้ Resource ร่วมกันระหว่าง Thread
- การใช้ Thread Call Method ข้าม Class นั้นจะอาศัยการสื่อสารกับโปรแกรมหลักผ่าน File แทน

3.4.4 ศึกษาและทดลองการสร้าง Graph และแผนภูมิต่างๆ ด้วย Library Chart Director ในภาษา C#

อุปสรรค

- ลักษณะของข้อมูลที่ Chart Director รับมาสร้าง Graph และแผนภูมิต่างๆนั้นเป็นตัวแปรในรูปแบบของ Double[] ซึ่งเดิมใช้ Long
- เป็น Library ที่ไม่ได้รองรับการทำงานที่มีการ Update ข้อมูลในช่วงสั้นๆ

วิธีการแก้ไข

- สร้าง Method สำหรับการแปลงค่าที่จากเดิมเป็นลักษณะของ Double[]
- อาศัยการเขียน Graph และแผนภูมิใหม่ในกรณีที่ต้องการ Update ถึงแม้จะมีอาการกระตุกบ้างแต่ก็ยอมรับได้

3.4.5 ศึกษาและทดลองการทำงานแบบ Real-time ด้วยภาษา C#

อุปสรรค

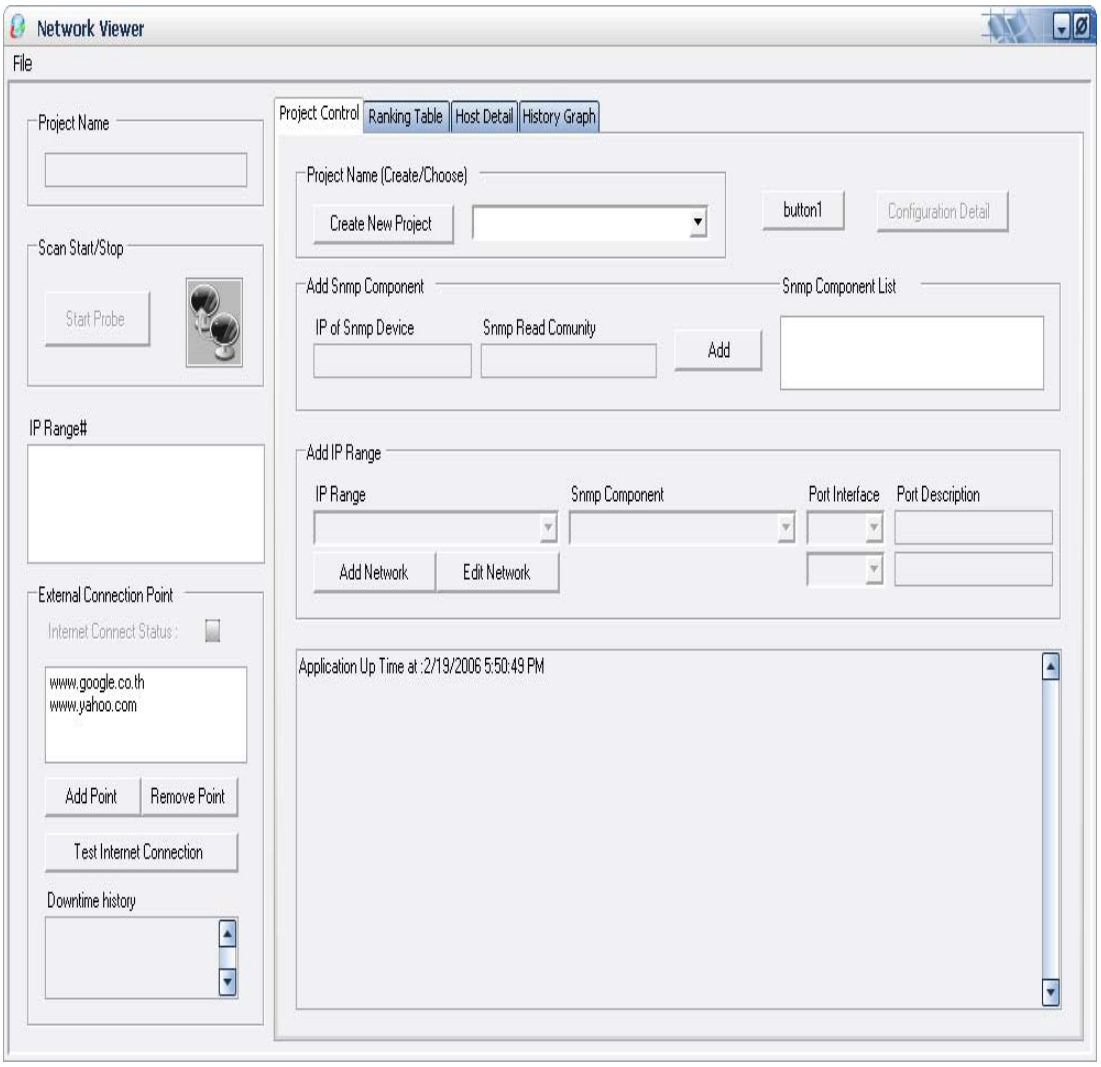
- หากมีการตั้ง Refresh Rate สั้น Library SNMP++ จะมีการใช้งาน CPU ที่สูงมากเป็นผลให้ระบบโดยรวมทำงานช้าลงอย่างเห็นได้ชัด
- หากมีการตั้ง Refresh Rate สั้น Library Chart Director จะมีการจองตัวแปรและไม่มีการลบทิ้งเป็นผลให้มีการใช้งาน Physical Memory สูงขึ้นเรื่อยๆจนถึงขีดจำกัดที่ OS กำหนดให้เป็นผลให้โปรแกรม crash ทันที
- การใช้ Nmap แสกนจำเป็นต้องใช้เวลาช่วงหนึ่งทำให้หาก Refresh Rate สั้น อาจเกิดการคาบเกี่ยวของการแสกนได้

วิธีการแก้ไข

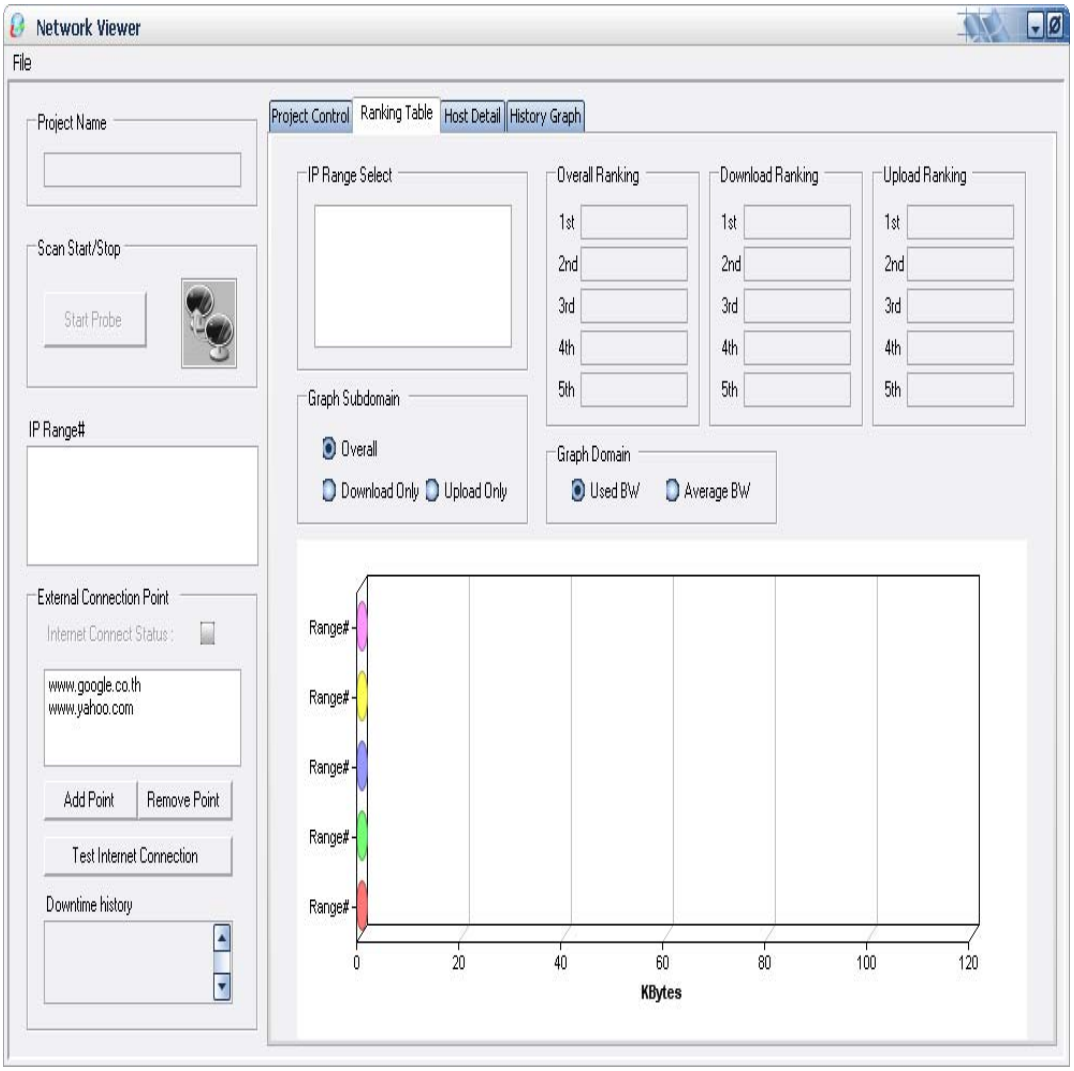
- ตั้ง Refresh Rate ให้มากขึ้นและเนื่องด้วยเหตุผลนี้จึงจำเป็นต้องไม่ให้ผู้ใช้แก้ไขค่า Refresh Rate เองได้

3.5 ตัวอย่างส่วนติดต่อกับผู้ใช้

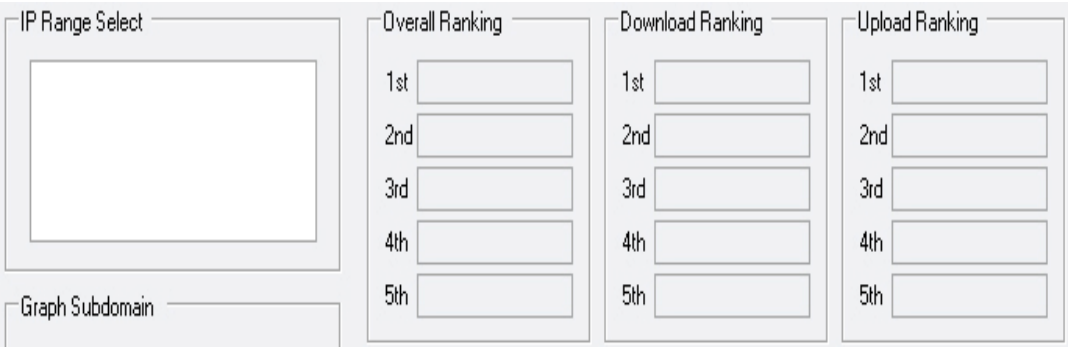
User Interface



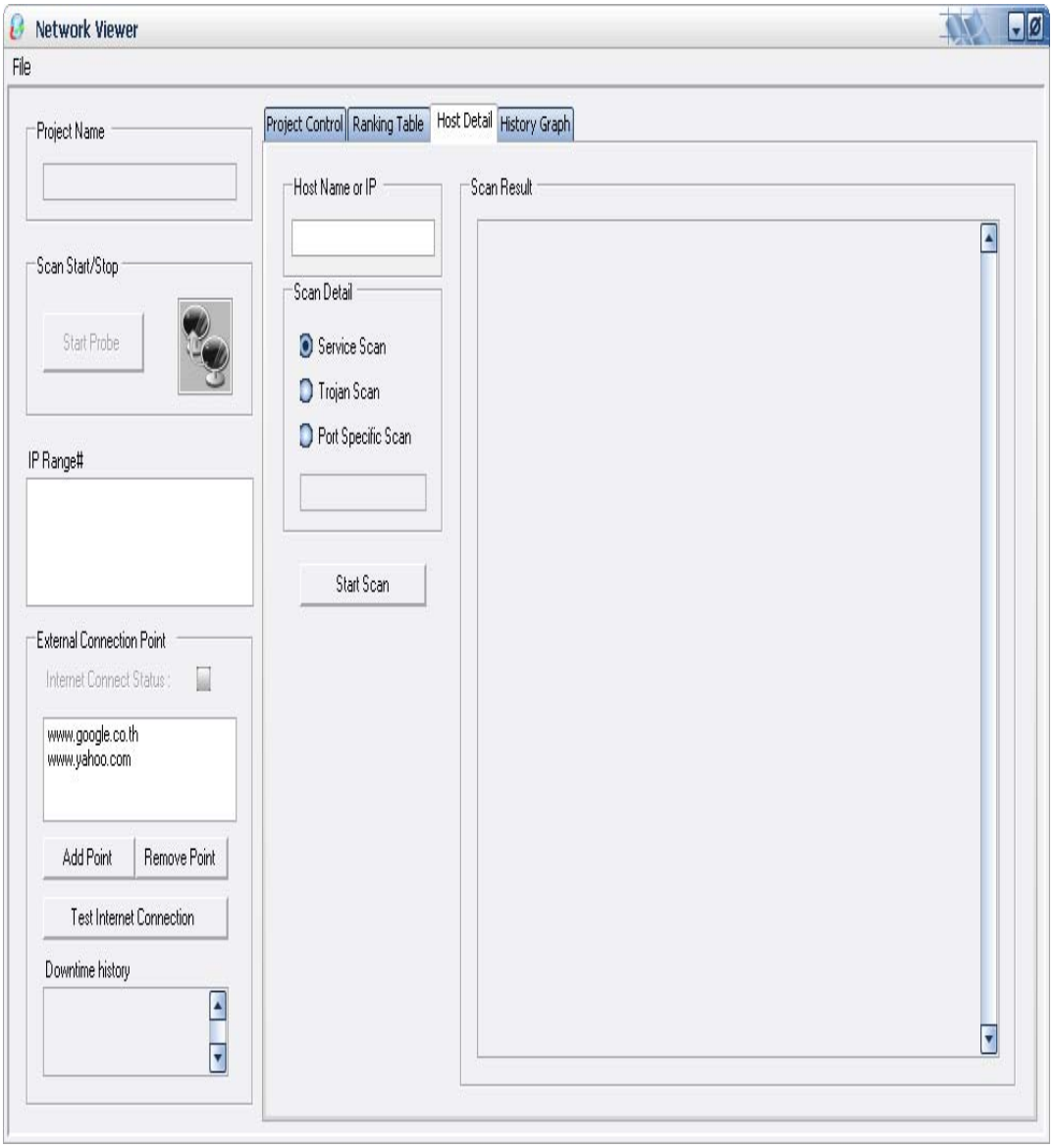
รูปที่ 3.3 User Interface ของการ Configuration ค่าเริ่มต้น



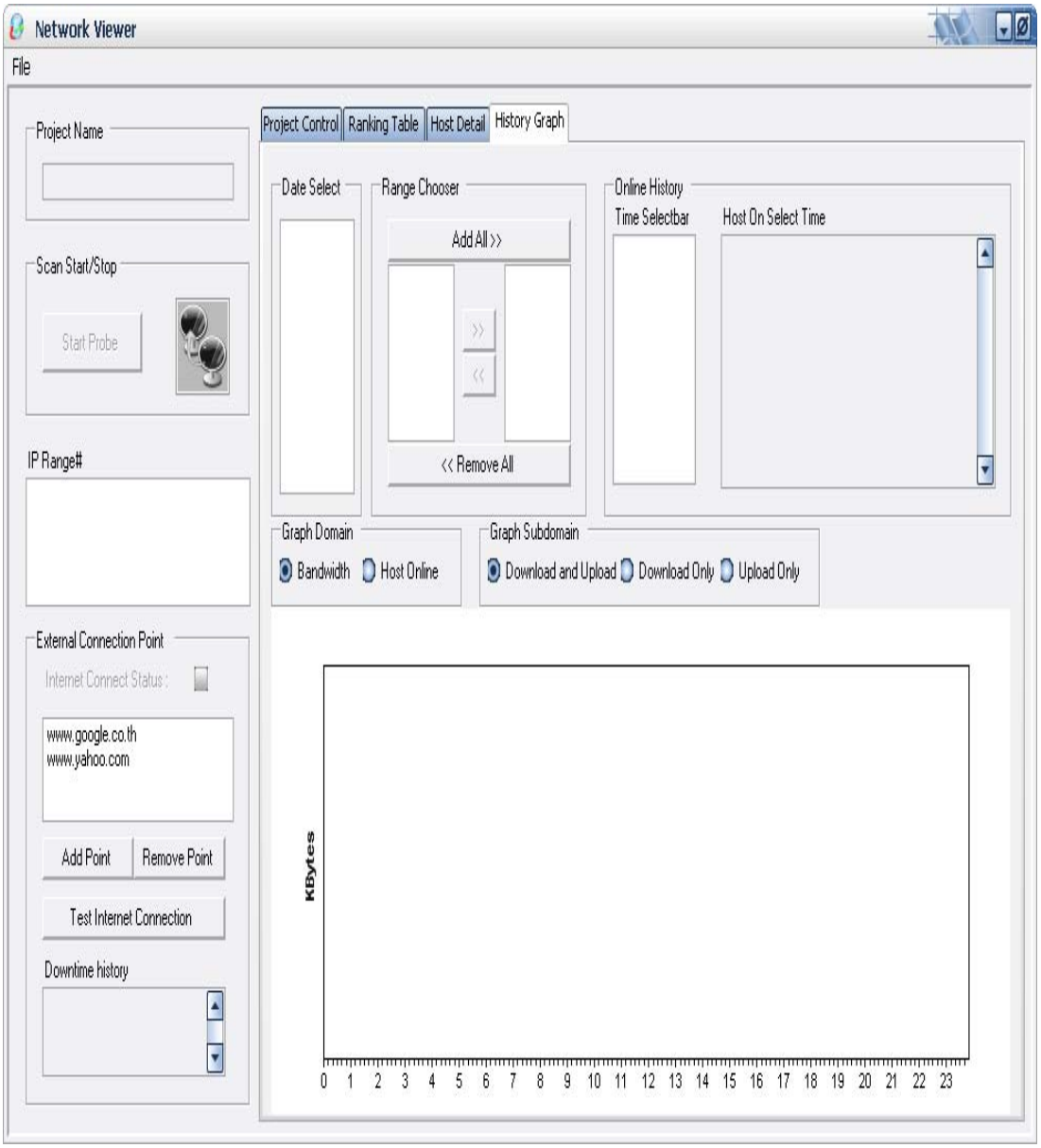
รูปที่ 3.4 User Interface ส่วนการแสดงผลแผนภูมิแท่งปริมาณ Bandwidth รวม และปริมาณ Bandwidth โดยเฉลี่ยต่อวินาที



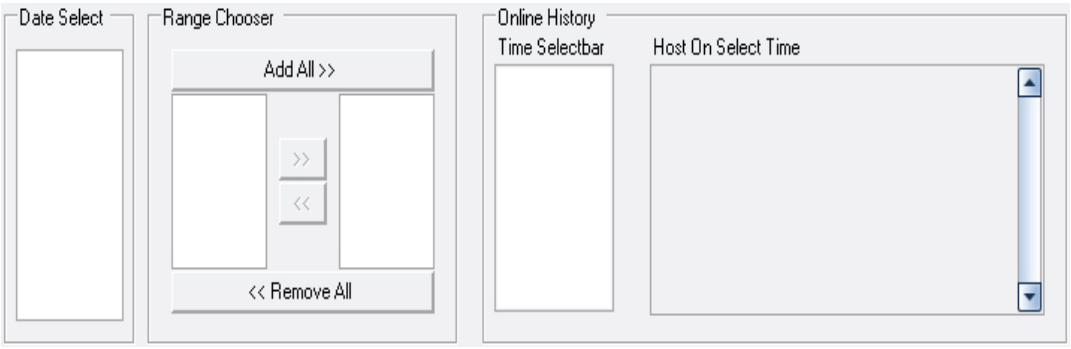
รูปที่ 3.5 User Interface แสดงลำดับของเครื่องคอมพิวเตอร์ในเครือข่ายย่อยที่มีการใช้งานสูงสุด



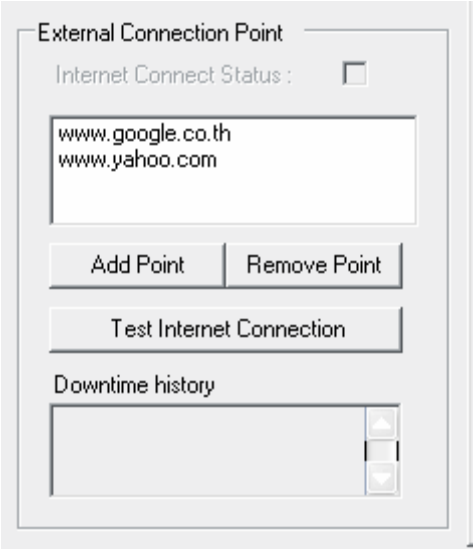
รูปที่ 3.6 User Interface ของการสำรวจข้อมูลเฉพาะเครื่อง



รูปที่ 3.7 User Interface ส่วนของการแสดงกราฟปริมาณ Bandwidth ในช่วงเวลาต่างๆใน 1 วัน และจำนวนของเครื่องคอมพิวเตอร์ที่ Online ในช่วงเวลาต่างๆใน 1 วัน



รูปที่ 3.8 User Interface ที่แสดงว่า ณ เวลาที่กำหนดมีเครื่องคอมพิวเตอร์เครื่องใดในเครือข่ายย่อย Online อยู่บ้าง



รูปที่ 3.9 User Interface ที่แสดงการสำรวจสถานะของการเชื่อมต่อระหว่างระบบเครือข่ายกับ Internet