บทที่ 8
การออกแบบและพัฒนาโปรแกรม

8.1 รายละเอียดของการพัฒนา

ในการจัดทำโปรแกรมสำรวจและสังเคราะห์เครือข่ายและระบบคอมพิวเตอร์จำเป็นต้องศึกษาทฤษฎีและข้อมูลที่ใช้ในการค้นหาและรวบรวมข้อมูลของคอมพิวเตอร์เครื่องอื่นที่อยู่ในเครือข่าย โดยในโปรแกรมของเราใช้เทคนิคหลายๆอย่าง ดังนี้

- ใช้เทคนิค Ping sweep เพื่อค้นหาว่ามีเครื่องไหนอยู่ในเครือข่ายบ้าง
- ใช้เทคนิค Trace route เพื่อสำรวจ Router
- ใช้เทคนิค Netstat โดยอาศัยการเปิด Service RIP Listener เพื่อหา Routing Table
- ใช้เทคนิค SNMP เพื่อ Query ข้อมูลของ Router
- ใช้ Whois เพื่อหา Network Address

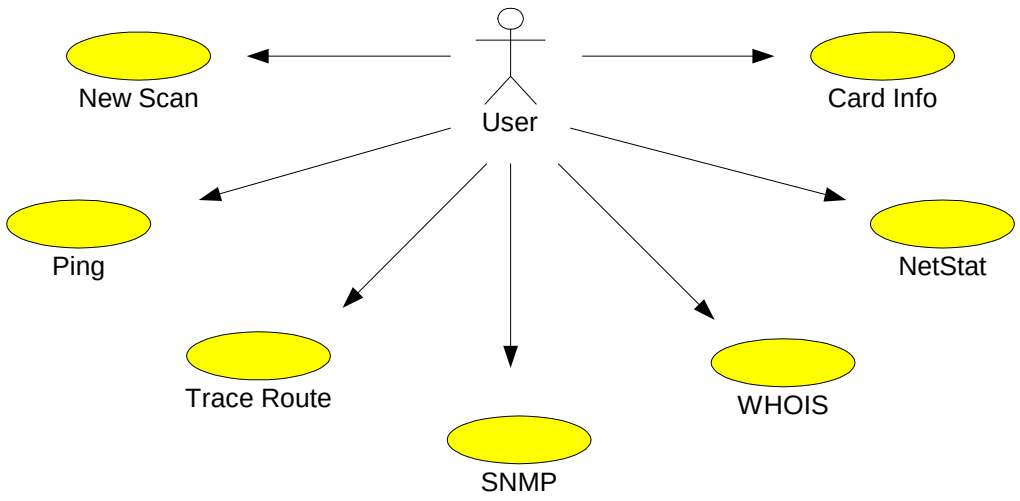
ส่วนเครื่องมือต่าง ๆ ที่ใช้ในการพัฒนาได้แก่

- Microsoft Visual C++ 6.0 MSDN Library Visual Studio 6.0
- Winpcap 3.0
- Nmap 3.00
- Microsoft Windows XP

โดยรูปแบบของโปรแกรมจะมี Input เป็น IP address จะใส่แค่ค่าเดียวหรือ ใส่เป็นช่วงก็ได้ หรือจะใส่เป็นจำนวน Hop ผลลัพธ์ที่ได้ออกมาจะแสดงในรูปแบบ Graphic โดยจะวาดเป็นการเชื่อมต่อ ว่ามีการเชื่อมต่อจากเครือข่ายใดไปยังเครือข่ายใด และเครือข่ายใดอยู่กลุ่มเดียวกัน แต่จะวาดโดยแบ่งตามเครือข่ายที่เราทำการสำรวจ โดยสามารถแสดงเครื่องคอมพิวเตอร์ทั้งหมดที่สำรวจได้ที่อยู่บนเครือข่ายที่ทำการสำรวจ และหากมีการเปิด SNMP Service ก็จะอ่านรายละเอียดอื่น ๆ เพิ่มเติมได้เช่น CPU ที่ใช้เป็นรุ่นไหน มีจำนวน Interface ที่ติดต่ออยู่บนเครือข่ายเป็นเท่าไร เป็นต้น

8.2 การออกแบบโครงสร้างของโปรแกรม

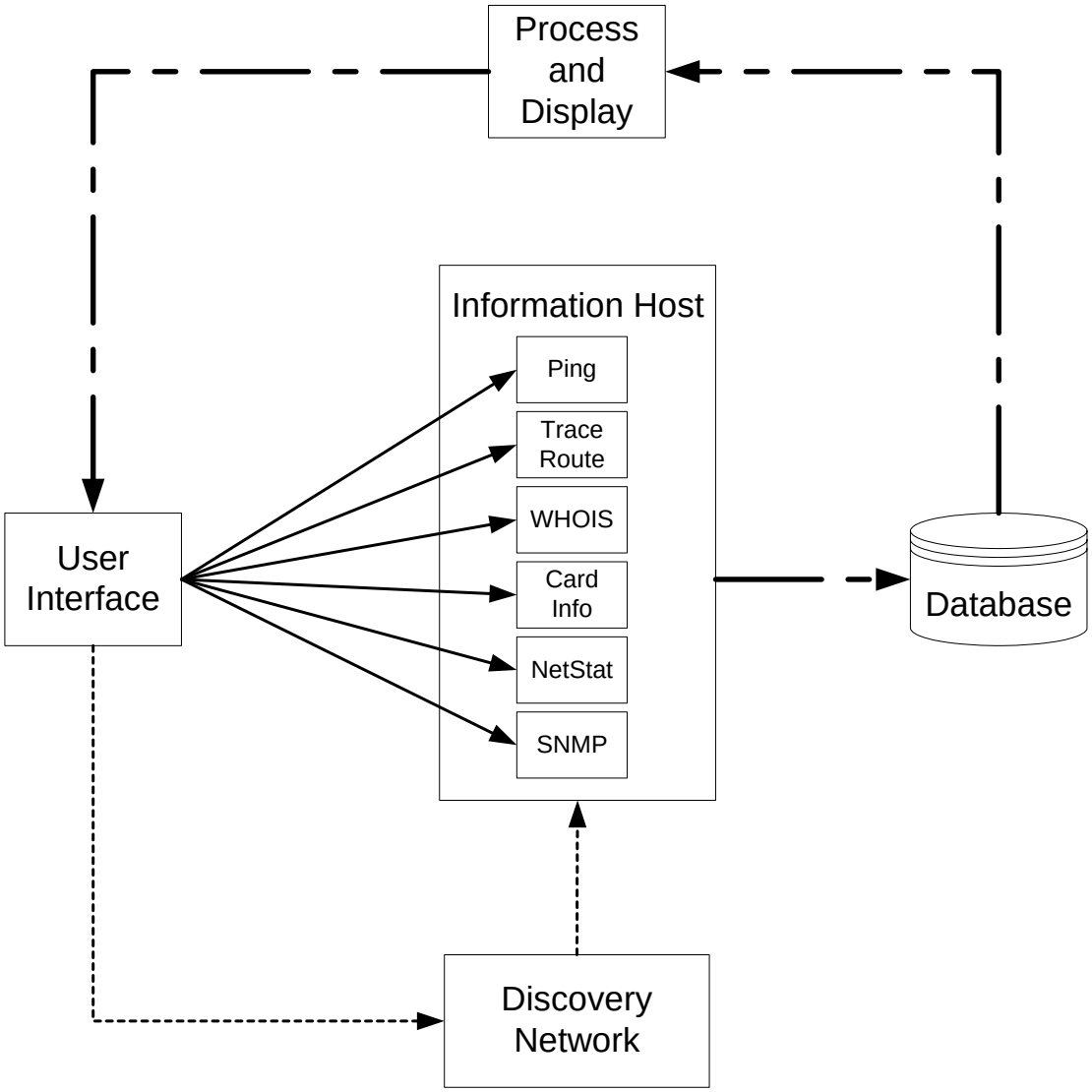
Use Case Diagram



รูปที่ 8-1 แสดง Use Case ของโปรแกรม

คำศัพท์	คำอธิบาย
User	ผู้ที่ใช้โปรแกรมที่ต้องการทำการสำรวจระบบเครือข่าย เช่น ผู้ดูแลระบบ
New Scan	ใช้โปรแกรมทำการสร้างแผนภาพของระบบเครือข่ายรวมโดยผู้ใช้ใส่ข้อมูลที่จำเป็นในการใช้สำรวจ
Ping	สั่งให้โปรแกรม Ping ไปยัง IP ที่สนใจ
Trace Route	สั่งให้โปรแกรมทำการค้นหาเส้นทางไปยัง IP ที่สนใจ
SNMP	สั่งให้โปรแกรมทำการอ่านข้อมูลจาก SNMP Service ของคอมพิวเตอร์ในระบบ จาก IP ที่สนใจ
WHOIS	สั่งให้โปรแกรมให้ทำการค้นหา Network Address ของ IP ที่สนใจ
NetStat	สั่งให้โปรแกรมทำการอ่านค่า Connection ต่างๆ หรือ อ่านค่า Routing Table ของตนเอง
Card Info	สั่งให้โปรแกรมทำการอ่านรายละเอียดจาก Network Card ตนเอง

ตารางที่ 8-1 แสดงคำอธิบาย Use Case Diagram



รูปที่ 8-2 แสดงโครงสร้างโปรแกรม

ส่วนหลัก ๆ ของโปรแกรมแบ่งเป็น 5 ส่วนหลักๆ

- User Interface ทำหน้าที่รับและแสดงผลติดต่อกับผู้ใช้
- Information Host ทำหน้าที่ค้นหาข้อมูลของเครื่องที่ผู้ใช้สนใจ
- Discovery Network ทำหน้าที่ค้นหาเครือข่าย
- Database ทำหน้าที่เก็บข้อมูลที่ค้นหาได้
- Process and Display ทำหน้าที่วิเคราะห์ข้อมูลที่เก็บไว้ในส่วนเก็บข้อมูลและ นำมาสร้างแผนภาพของระบบเครือข่าย

ความสามารถการทำงานของโปรแกรมแบ่งเป็น 2 ส่วนหลักๆ

1. Information Host (โดยมีฟังก์ชั่นภายในดังนี้)

- Ping
- Trace Route
- WHOIS
- Card Info
- NetStat
- SNMP

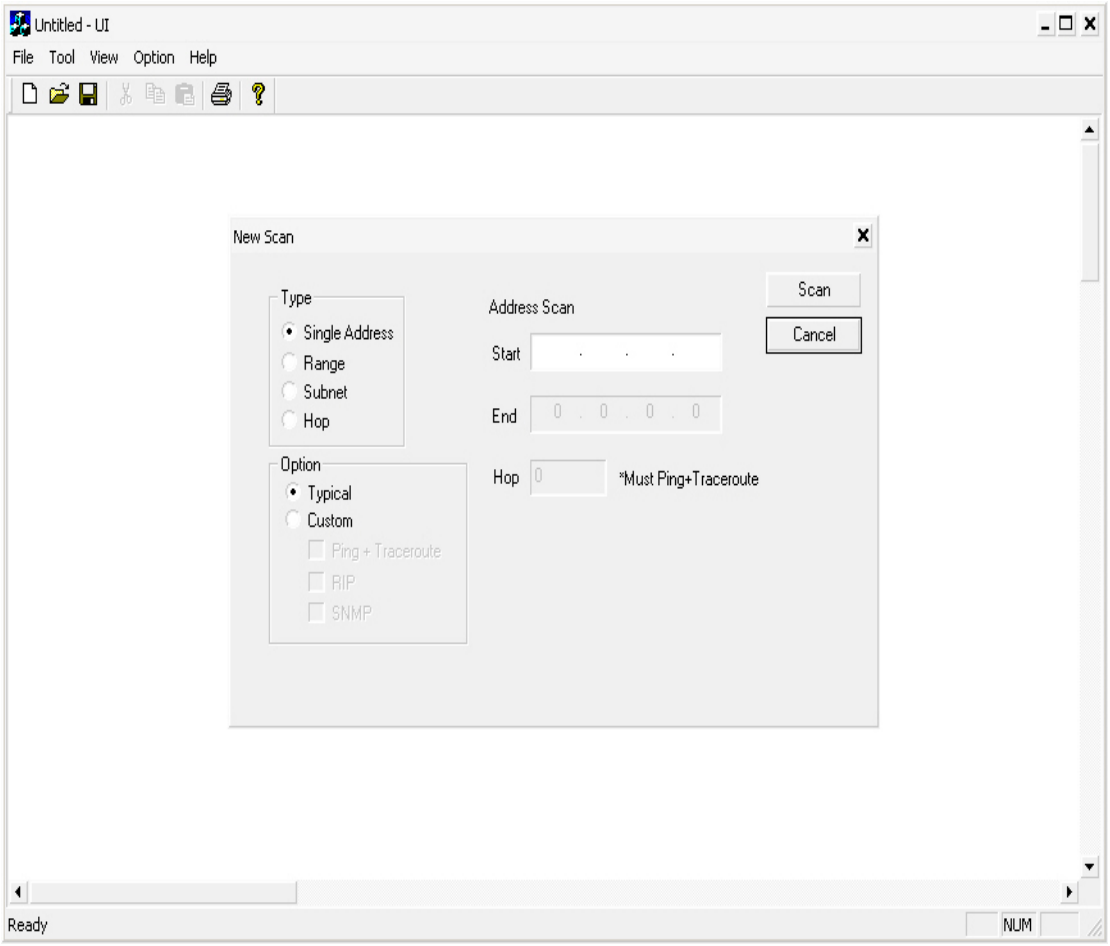
ทั้งหมดนี้จะทำการค้นหาข้อมูลที่ของเครื่องที่ผู้ใช้สนใจและนำข้อมูลนั้นมาแสดงผล โดยไม่ได้มีการเก็บข้อมูลลงฐานข้อมูลแต่อย่างใด

2. Discovery Network จะทำงานโดยเรียกใช้ฟังก์ชั่นต่างๆบนส่วน Information Host และเมื่อเรียกใช้ฟังก์ชั่นใดฟังก์ชั่นหนึ่งเสร็จก็จะเก็บลงฐานข้อมูล และเรียกใช้ฟังก์ชั่นอื่นต่อไป (ตามแต่ผู้ใช้งานจะเลือกใช้งานฟังก์ชั่นใดบ้าง โดยค่าเริ่มต้นจะเรียกทุกฟังก์ชั่น) หลังจากเก็บข้อมูลทั้งหมดที่หามาได้ ก็จะนำข้อมูลเหล่านั้นไปผ่านส่วนวิเคราะห์ข้อมูลและนำมาสร้างแผนภาพ เพื่อแสดงผลให้กับผู้ใช้งาน

โดยมีขั้นตอนการทำงานดังนี้

- Ping Sweep ไปยัง IP ที่สนใจและเก็บสถานะของ IP เหล่านั้นลงฐานข้อมูล
- Trace Route ไปยัง IP ที่มีสถานะ ON อยู่ในขณะนั้น โดยตรวจสอบจากฐานข้อมูล ถ้าไม่มีข้อมูลก็จะ Trace Routeไปทุก IP ที่ป้อนเข้ามา และเก็บลงฐานข้อมูล
- Query SNMP ไปยัง IP ที่มีสถานะ ON อยู่ในขณะนั้น โดยตรวจสอบจากฐานข้อมูล ถ้าไม่มีข้อมูลก็จะ Query SNMP ไปทุก IP ที่ป้อนเข้ามา และเก็บลงฐานข้อมูล
- Query NetStat จากเครื่องที่ผู้ใช้งาน
- นำข้อมูลที่เก็บลงฐานข้อมูลมาประมวลผลเป็นภาพ

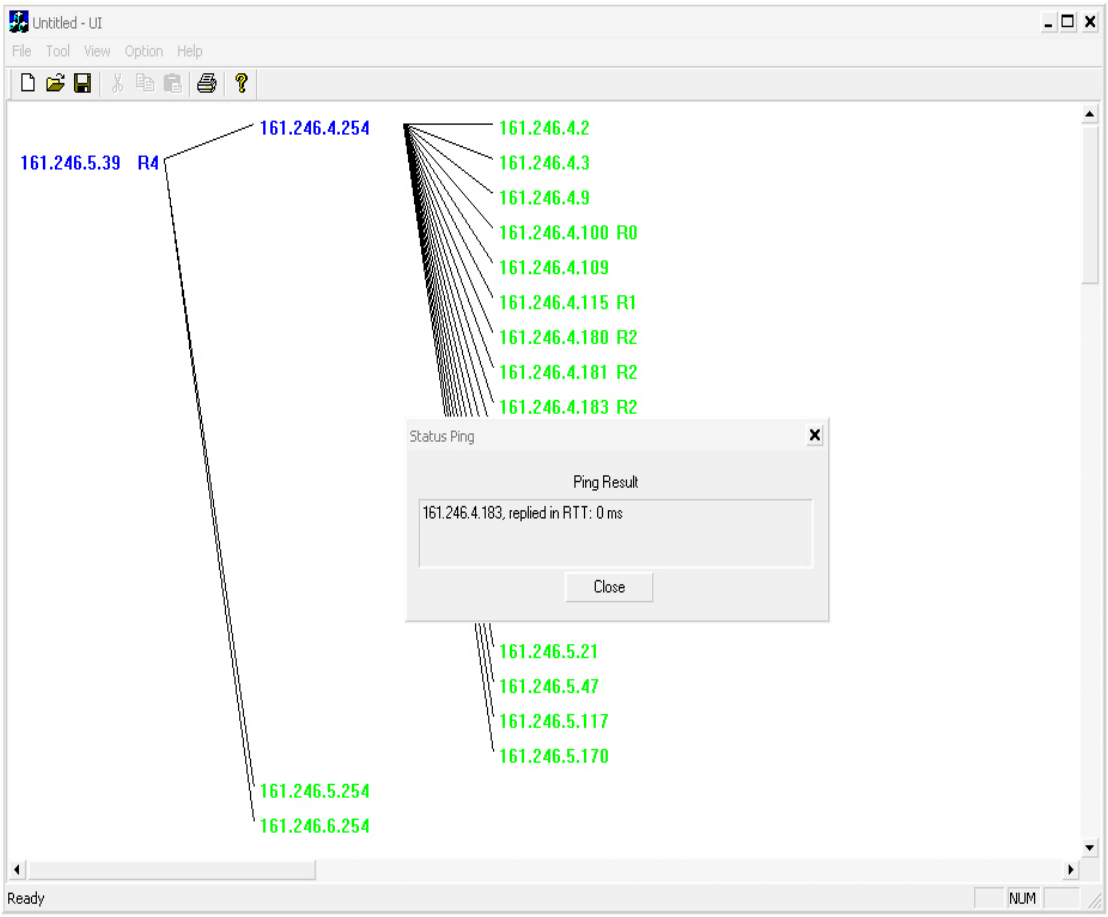
8.3 ตัวอย่างส่วนติดต่อกับผู้ใช้



รูปที่ 8-3 ตัวอย่างต้นแบบหน้าจอที่ใช้ในการใส่ Input ของโปรแกรม

Input ที่ต้องการของโปรแกรม

- Single Address ของคอมพิวเตอร์ที่ต้องการสำรวจกรณี โดยรู้เพียง IP ของเครื่องนั้น
- Range ของคอมพิวเตอร์กรณีต้องการสำรวจระบบเครือข่ายคอมพิวเตอร์ โดยทราบเป็นช่วงของคอมพิวเตอร์ในระบบเครือข่าย
- Subnet โดยต้องใส่ IP Address และ Subnet Mark ของกลุ่มเครือข่ายคอมพิวเตอร์ที่ต้องการทำการสำรวจ
- Hop โดยใส่เป็นจำนวนของ Hop Count ที่ต้องการสำรวจระบบเครือข่าย ว่ารูปแบบของเครือข่ายภายในจำนวนที่ป้อนไว้เป็นอย่างไร



รูปที่ 8-4 ตัวอย่างต้นแบบหน้าจอ แผนภาพที่ได้จากการสำรวจ

Output ของโปรแกรมที่ได้จากการสำรวจ

- แผนภาพทางกายภาพของระบบเครือข่ายที่สำรวจมาได้ จากเครือข่ายตัวอย่างที่สนใจ (161.246.4.0 - 161.246.6.0) โดยจะแสดงเป็นโนดหรือรายชื่อเครื่องที่ยังมีชีวิตภายในโนดนั้นก็ได้
- ถ้าเครื่องหรือโนดใด มีการเปิด SNMP Service ก็จะมีการแสดงตัวอักษรท้าย IP Address นั้น
- โดยสามารถตรวจสอบสถานะของเครื่องที่แสดงได้ ว่ายังมีชีวิตอยู่หรือหายไปแล้ว