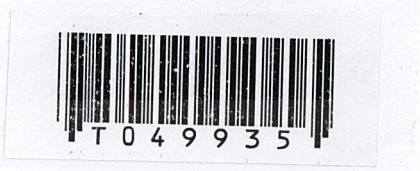
โปรแกรมสำรวจเครือข่ายและระบบคอมพิวเตอร์

Network and Computer System Viewer



โดย

นายสุภชัย กอบกิจเจริญ

นายอนรรฆพล แสนประเสริฐ

อาจารย์ที่ปรึกษา

อาจารย์ ธนา หงษ์สุวรรณ

อาจารย์ อัครเดช วัชระภูพงษ์

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2545

ปริญญานิพนธ์ปีการศึกษา 2545

ภาควิชา วิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง โปรแกรมสำรวจเครือข่ายและระบบคอมพิวเตอร์

Network and Computer System Viewer

ผู้จัดทำ

1. นายสุภชัย กอบกิจเจริญ รหัสประจำตัว 42010397

2.นายอนรรฆพล แสนประเสริฐ รหัสประจำตัว 42010425

อาจารย์ที่ปรึกษา

อาจารย์ ธนา หงษ์สุวรรณ

อาจารย์ที่ปรึกษา

อาจารย์ อัครเดช วัชระภูพงษ์

โปรแกรมสำรวจเครือข่ายและระบบคอมพิวเตอร์

นายสุภชัย	กอบกิจเจริญ	42010397
นายอนรรฆพล	แสนประเสริฐ	42010425
อาจารย์ ธนา	หงษ์สุวรรณ	อาจารย์ที่ปรึกษา
อาจารย์ อัครเดช	วัชระภูพงษ์	อาจารย์ที่ปรึกษา

ปีการศึกษา 2545

บทคัดย่อ

ในปัจจุบันนี้มีการใช้งานเครือข่ายการสื่อสารข้อมูลภายในองค์กรต่าง ๆ อย่างแพร่หลายทั้งในด้านการสื่อสารข้อมูลภายในองค์กรและการสื่อสารข้อมูลระหว่างองค์กร การใช้เครือข่ายการสื่อสารข้อมูลจึงจำเป็นที่จะต้องมีประสิทธิภาพในการทำงานที่สูงเพื่อเป็นการสนับสนุนระบบการทำงานขององค์กร

วิทยานิพนธ์นี้เป็นการนำเสนอ โครงการพัฒนาโปรแกรมสำรวจเครือข่ายและระบบคอมพิวเตอร์ (Network and Computer System Viewer) ซึ่งเป็นโปรแกรมที่ใช้สำหรับผู้ดูแลระบบเครือข่ายเพื่ออำนวยความสะดวกในการแสดงให้เห็นสถานะปัจจุบันของระบบเครือข่ายและสภาพของระบบคอมพิวเตอร์ที่ใช้งานระบบเครือข่าย โดยนำเสนอเทคนิคต่าง ๆ ที่ใช้ในการรวบรวมข้อมูลของระบบคอมพิวเตอร์บนเครือข่าย, ส่วนที่ใช้ในการจัดเก็บข้อมูล และส่วนที่ใช้ในการจัดการเพื่อนำมาแสดงผลบนโปรแกรม

รวมทั้งมีรายละเอียดในการพัฒนาโปรแกรมเพื่อให้ผู้ที่สนใจสามารถนำไปเป็นแนวทางในการพัฒนาเครื่องมือที่ใช้อำนวยความสะดวกในการจัดการเครือข่ายอื่น ๆ เพื่อลดการนำเข้าโปรแกรมต่าง ๆ จากต่างประเทศ

Network and Computer System Viewer

Mr. Supachai	Kobkijcharoen	42010397
Mr. Anakapole	Sanprasert	42010425
Mr. Thana	Hongsuwan	Advisor
Mr. Akkradach	Watcharapupong	Advisor

ABSTRACT

Presently, Communication Network is applied widely in many organizations include both internal communication and external communication. Therefore, Communication Network must have high performance to support the organization work.

This thesis describes the network and computer system viewer that is the administrator tool program for network monitoring . Including describes the use of enumeration technique for gathering network information, storing database and information processing to display. Addition developing details for developer.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้คงไม่สำเร็จลุล่วงไปด้วยดี หากปราศจากคำแนะนำและการให้คำปรึกษาจาก อาจารย์ ธนา หงษ์สุวรรณ และ อาจารย์ อัครเดช วัชระภูพงษ์ ซึ่งเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่ให้ความเอาใจใส่ แนะนำ และช่วยเหลือเสมอมา ผู้วิจัยรู้สึกซาบซึ้งในความอนุเคราะห์จากท่านและขอขอบคุณเป็นอย่างสูง

ขอขอบคุณห้องปฏิบัติการ ISAG และห้อง ESL ที่อำนวยความสะดวกเกี่ยวกับสถานที่ทำงาน และยังเป็นสถานที่พบปะเพื่อน ๆ เพื่อให้มีกำลังใจในการทำงานต่อไปด้วย

ขอขอบคุณเพื่อน ๆ พี่ ๆ น้อง ๆ จนทุก ๆ คนในครอบครัวที่ให้กำลังใจทำวิทยานิพนธ์ชิ้นนี้จนสำเร็จได้ด้วยดี

ขอขอบคุณตัวข้าพเจ้าทั้งสองที่ไม่ท้อแท้ไปเสียก่อนที่จะประสบความสำเร็จ ขอบคุณที่มีชีวิตมาถึงทุกวันนี้ และโอกาสดีๆ ที่ได้รับมา

และต้องขอขอบคุณบุคคลสำคัญที่สุดทำให้ข้าพเจ้ามีวันนี้ ก็คือ บิดา มารดา อันเป็นที่เคารพรักยิ่ง ซึ่งได้เลี้ยงดูข้าพเจ้ามาเป็นอย่างดี พร้อมทั้งให้โอกาสในการศึกษาอย่างดี และยังให้กำลังใจ เอาใจใส่เสมอมาในทุกๆ ด้านอันหาที่เปรียบมิได้ ขอกราบขอบพระคุณมา ณ ที่นี้ด้วย

สุภชัย กอบกิจเจริญ

อนรรฆพล แสนประเสริฐ

สารบัญ

สารบัญตาราง

สารบัญรูปภาพ

บทที่ 1
บทนำ

หลักการและเหตุผล

ในปัจจุบันนี้ระบบเครือข่ายคอมพิวเตอร์กำลังเป็นที่นิยมอย่างสูง ทำให้จำนวนผู้ใช้ในระบบเพิ่มขึ้นอย่างรวดเร็วและมีผลให้ระบบเครือข่ายคอมพิวเตอร์มีขนาดและมีความซับซ้อนมากขึ้น การดูแลระบบเครือข่ายก็ทำได้ยากขึ้นตามไปด้วย โดยการดูแลระบบเครือข่ายเบื้องต้นก็จำเป็นต้องทราบแผนภาพคร่าว ๆ ของชนิดและจำนวนอุปกรณ์ต่าง ๆ ที่อยู่ในเครือข่ายเสียก่อน หากระบบเครือข่ายมีความซับซ้อนมากการทำ ดังกล่าวสามารถทำได้ยาก ดังนั้นเพื่อให้การดูแลและจัดการระบบเครือข่ายทำได้อย่างมีประสิทธิภาพมากขึ้น จึงจำเป็นต้องมีเครื่องมือที่ใช้ในการช่วยสร้างรูปแผนภาพของระบบเครือข่ายจำลองขึ้น

ในการที่จะสร้างรูปแผนภาพจำลองระบบเครือข่ายคอมพิวเตอร์จำเป็นต้องทราบข้อมูลเบื้องต้นของระบบเครือข่ายที่ต้องการจะสร้างก่อน โดยเครื่องมือตัวนี้รวบรวมข้อมูลเพื่อการดูแลเครือข่ายคอมพิวเตอร์ได้โดยการ ส่ง Packet ข้อมูลไปและตรวจสอบ Packet ข้อมูลที่ได้รับกลับมา (Active SCAN) เพื่อเก็บข้อมูลเบื้องต้นต่าง ๆ เช่น มีอุปกรณ์เปิดอยู่ในเครือข่ายนี้จำนวนเท่าไร, อุปกรณ์ทำหน้าที่เป็นอะไร โดยใช้ เทคนิค การตรวจสอบแบบต่าง ๆ เช่น การ Ping Sweep , การอ่านค่าจาก SNMP Service, การตรวจสอบ port ที่เปิดบริการ และ อื่น ๆ

โดยการรวบรวมจะพยายามหาข้อมูลที่จำเป็นให้มากที่สุด เมื่อได้ข้อมูลต่าง ๆ มาแล้วก็จะนำข้อมูลเหล่านี้มาสร้างเป็นแผนภาพจำลองระบบเครือข่ายขึ้น โดยจะนำมาแสดงในรูปแบบที่ง่ายต่อการแสดงผล และมีการเปลี่ยนแปลงสถานะหากในระบบเครือข่ายเปลี่ยนแปลง เพื่อสะดวกในการดูแลระบบเครือข่ายแบบตลอดเวลา

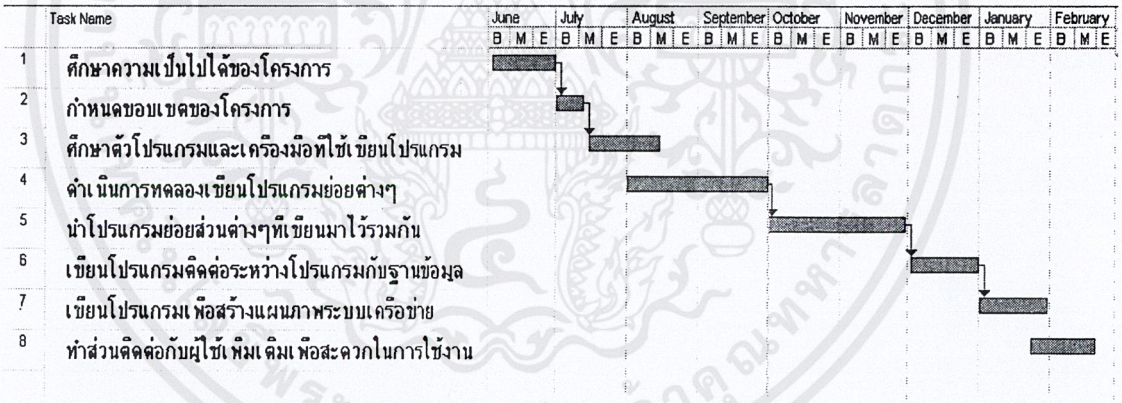
วัตถุประสงค์ของโครงการ

1. เพื่อพัฒนาต้นแบบของโปรแกรมที่ใช้ในการดูแลระบบเครือข่ายคอมพิวเตอร์ เพื่อนำไปใช้ทดแทนการนำเข้าจากต่างประเทศ
2. เพื่อพัฒนาโปรแกรมที่ใช้ในการอำนวยความสะดวกในการดูแลและตรวจสอบระบบเครือข่ายคอมพิวเตอร์

ขอบเขตของโครงการ

โดยโปรแกรมจะมีคุณสมบัติพื้นฐานดังนี้

1. สามารถหาคอมพิวเตอร์ที่เปิดใช้งานเครือข่ายอยู่ในขณะนั้นได้
2. สามารถหา OS , Service port ของคอมพิวเตอร์ในระบบเครือข่ายได้
3. สามารถอ่านค่า SNMP Service ที่สนใจในการบอกลักษณะของคอมพิวเตอร์ในระบบเครือข่ายได้
4. สามารถนำโปรแกรมที่ทำงานบน Textmode มาเพิ่มเติมความสามารถให้กับโปรแกรมและเพิ่มความสะดวกในการใช้งานได้
5. สามารถหา MAC Address และ บอก Vendor ของผู้ผลิตอุปกรณ์ Network นั้นได้
6. สามารถแสดงรายชื่อของ Shared Folder บนระบบคอมพิวเตอร์นั้น ๆ ได้
7. สามารถนำข้อมูลที่รวบรวมมาได้มาสร้างเป็น แผนภาพคอมพิวเตอร์ทาง Logical ในระบบเครือข่ายได้ โดยแสดงผลในรูปแบบกราฟฟิก
8. สามารถนำผลที่ได้มาสร้างเป็นแผนภูมิการใช้งานได้•สามารถตั้งเวลาให้ทำการสำรวจอัตโนมัติได้
9. สามารถนำผลลัพธ์แสดงออกทางรายงานได้



รูปที่ 1-1 แสดงแผนการดำเนินงาน

แผนการดำเนินงาน

ภาคการศึกษาที่ 1

1. ศึกษาความเป็นไปได้ในการที่จะสร้างและนำเครื่องมือนี้มาใช้
2. ศึกษาเทคนิคต่าง ๆ ที่จะใช้ในการรวบรวมข้อมูลเครือข่ายคอมพิวเตอร์ที่จะนำมาใช้ในการสร้างแผนภาพ
3. ทดลองเขียนโปรแกรมย่อยในการ ทำ OS-fingerprint จากการ Scan ด้วยเทคนิคต่าง ๆ
4. ทดลองเขียนโปรแกรมย่อยในการ ติดต่อ Database หาชื่อ Vendor ผู้ผลิตอุปกรณ์ จาก MAC Address

5. ทดลองเขียนโปรแกรมย่อยในการอ่านค่าจาก SNMP – Service
6. ทดลองเขียนโปรแกรมย่อยในการหา Subnet Topology

ภาคการศึกษาที่ 2

1. นำโปรแกรมย่อยส่วนต่าง ๆ ที่เขียนไว้มารวมกัน เป็นโปรแกรมเดียว
2. เขียนโปรแกรมติดต่อระหว่างโปรแกรมย่อย ต่าง ๆ กับฐานข้อมูลเพื่อเก็บข้อมูลลงไปในฐานข้อมูล
3. เขียนโปรแกรมเพื่อสร้างแผนภาพระบบเครือข่ายที่ต้องการสำรวจจาก ข้อมูลใน ฐานข้อมูลที่ได้จากโปรแกรมย่อย ต่าง ๆ
4. ทำส่วนที่ติดต่อแบบ Graphic กับผู้ใช้เพิ่มเติมเพื่อให้มีความสะดวกแก่การใช้งาน

ประโยชน์ที่ได้รับ

1. **โปรแกรมต้นแบบเพื่อใช้ในการจัดการและดูแลระบบเครือข่าย**
2. **ได้รับความรู้จากการศึกษาเกี่ยวกับเรื่องความปลอดภัย , การเดินทางของข้อมูลในระบบเครือข่ายและการเขียนโปรแกรมทางด้านเครือข่าย**
3. **ช่วยลดการนำเข้าโปรแกรมที่ใช้ในการดูแลระบบเครือข่ายจากต่างประเทศ**

บทที่ 2
ทฤษฎีการบริหารเครือข่าย

ในปัจจุบันองค์กรต่างๆ มีการตื่นตัวอย่างมากในการที่จะปรับปรุงเทคโนโลยีของระบบการทำงานและการติดต่อสื่อสารภายในองค์กร เพื่อผลของความรวดเร็วและความคล่องตัวในการดำเนินงานต่างๆ สิ่งหนึ่งที่องค์กรเหล่านั้นต้องกระทำคือ การนำเครื่องคอมพิวเตอร์ภายในองค์กรมาเชื่อมต่อกัน สร้างเป็นระบบเครือข่ายคอมพิวเตอร์ ที่ทำงานภายใต้มาตรฐานใดมาตรฐานหนึ่งตามวัตถุประสงค์ขององค์กรนั้น และมาตรฐานหนึ่งซึ่งเป็นที่นิยมในปัจจุบันคือ มาตรฐานโพรโตคอล ทีซีพี/ไอพี (TCP/IP)

เหตุผลที่มาตรฐานนี้เป็นที่นิยมสืบเนื่องมาจากการที่ระบบอินเทอร์เน็ตมีการทำงานภายใต้มาตรฐานนี้และหากองค์กรสามารถเชื่อมต่อเข้ากับระบบอินเทอร์เน็ตได้ก็จะทำให้เข้าถึงแหล่งข้อมูลทั่วโลกรวมทั้งบริการต่างๆ ที่มีอยู่มากมาย ดังนั้นเพื่อความง่ายและความสมบูรณ์แบบที่จะเข้ากันได้กับระบบอินเทอร์เน็ต หลายองค์กรจึงเลือกใช้มาตรฐานโพรโตคอลทีซีพี/ไอพีหรือเรียกเป็นระบบอินทราเน็ต

2.1 บทบาทของผู้ดูแลระบบและความจำเป็นในการดูแลระบบเครือข่าย

เมื่อมีระบบเครือข่ายก็จำเป็นจะต้องมีผู้ดูแลระบบเครือข่าย (Administrator) หมายถึงผู้ที่ทำหน้าที่ตรวจสอบดูแลและแก้ไขปัญหาอันเกิดกับการทำงานและสถานะต่างๆ ของอุปกรณ์ในระบบเครือข่าย จากหน้าที่ที่กล่าวมาจะเห็นว่า บุคคลที่จะเป็นผู้ดูแลระบบได้นั้นต้องมีความรู้ ประสบการณ์และความอดทนสูง และยังต้องเป็นผู้มีคุณธรรมด้วย ซึ่งถ้าในระบบเครือข่ายใหญ่หรือมีความซับซ้อนมากๆ อุปกรณ์ต่างๆ ภายในระบบก็มีมากขึ้นจนเกินความสามารถของผู้ดูแลระบบที่จะรับภาระได้จึงได้มีกลุ่มบุคคลที่พยายามแก้ไขและพัฒนาเทคโนโลยีด้านนี้ โดยทำการศึกษาและวิจัยพฤติกรรมการทำงานของระบบ องค์ประกอบที่จำเป็นต่อการบริหารระบบ ปัจจัยที่มีผลกระทบต่อระบบปัญหาของความหลากหลายของผลิตภัณฑ์ในระบบ รูปแบบการจัดเก็บของข้อมูลจัดการระบบ และอื่นๆ อีกมากมาย จนกระทั่งก่อกำเนิดเป็นรูปแบบของการบริหารของการบริหารงานระบบเครือข่ายอย่างง่าย (Simple Network Management) ต่อมาได้ถูกกำหนดให้เป็นมาตรฐานหนึ่งของ ISO (The International Organization for Standardization) และ CCITT (The International Telegraph and Telephone Consultative Committee) และในส่วนหนึ่งของมาตรฐานนี้ก็ได้มีการกำหนดโพรโตคอลที่ทำหน้าที่รับส่งข้อมูลการจัดการ โพรโตคอลที่ทำหน้าที่รับส่งข้อมูลการจัดการ โพรโตคอลนี้คือ โพรโตคอล เอสเอ็นเอ็มพี

2.2 ความต้องการในการจัดการระบบเครือข่ายก็เพื่อ

2.2.1 ใช้ในการควบคุมระบบเครือข่าย และทรัพยากรต่างๆ ให้มีประสิทธิภาพ

2.2.2 เพื่อควบคุมความซับซ้อนอันเนื่องมาจากการที่มีจำนวนของอุปกรณ์ในระบบเครือข่าย,ผู้ใช้งาน,โพรโตคอลที่ถูกใช้งานอยู่บนระบบเครือข่าย เพิ่มจำนวนมากขึ้น

2.2.3 เป็นการเพิ่มการบริการ(Service) ในการใช้ข้อมูลและทรัพยากรต่างๆ

2.2.4 เพื่อเพิ่มคุลยภาพการใช้ข้อมูลของโปรแกรมประยุกต์ หมายถึงว่า การที่ภายในองค์กรมีการใช้ข้อมูลและทรัพยากรสำหรับโปรแกรมประยุกต์หลายๆตัว โดยโปรแกรมประยุกต์ดังกล่าวนั้นมีการใช้ข้อมูลและทรัพยากรที่แตกต่างกัน ดังนั้นก็ต้องมีการจัดลำดับความสำคัญของโปรแกรมโดยการระบุถึงระดับความปลอดภัย (Security) รวมถึงทรัพยากรที่มีจะใช้ในโปรแกรมประยุกต์ด้วย ผู้ควบคุมระบบเครือข่ายจะต้องกำหนดและควบคุมทรัพยากร ให้สมดุลย์จากการที่มีความต้องการหลากหลายเหล่านี้

2.2.5 ช่วยลดความซับซ้อน (Redundant) ในการออกแบบและบริหารระบบเครือข่าย

2.2.6 สามารถวิเคราะห์การใช้งานของระบบเครือข่ายได้ว่าช่วงเวลาใดที่มีการใช้งานระบบเครือข่ายมากหรือน้อย

2.3 จุดประสงค์ในการทำการบริหารระบบมีดังนี้

2.3.1 จัดการกับความผิดพลาดต่างๆที่เกิดขึ้นในระบบเครือข่าย (Fault Management)

เพื่อตรวจสอบความผิดพลาดที่เกิดขึ้นกับอุปกรณ์ต่างๆ ในระบบซึ่งเมื่อเกิดความผิดพลาดในการทำงาน ขึ้นก็จะมีการปฏิบัติดังต่อไปดังนี้

2.3.1.1 ทำการตรวจสอบจุดที่เกิดความผิดพลาดหรือทำงานล้มเหลว

2.3.1.2 ทำการแยกส่วนของระบบเครือข่ายที่ทำงานผิดพลาดแล้วแยกส่วนที่ทำงานผิดพลาดนั้นออกจากระบบ เพื่อให้ระบบเครือข่ายที่เหลืออยู่สามารถทำงานต่อไปได้

2.3.1.3 ทำการรีคอนฟิกระบบใหม่ให้สามารถทำงานได้ เพื่อทดแทนการทำงานในส่วนถูกแยกไปแล้ว

2.3.1.4 ทำการซ่อมแซมหรือเปลี่ยนแปลงส่วนที่เกิดความผิดพลาดขึ้น ให้กลับมาใช้งานได้ใหม่

2.3.2 จัดการเก็บข้อมูลต่างๆ ของระบบเครือข่าย (Accounting Management)

เพื่อให้ผู้ดูแลระบบสามารถที่จะติดตามและตรวจสอบดูเหตุการณ์(Event) รวมถึงจำนวนการใช้ทรัพยากรของระบบเครือข่าย ข้อมูลที่เราติดตามจะมีประโยชน์ดังนี้

2.3.2.1 สามารถตรวจสอบจำนวนผู้ใช้งานหรือกลุ่มของที่อาจมีการเรียกใช้ข้อมูลในส่วนที่ไม่ได้รับอนุญาต รวมถึงดูความแออัดของระบบเครือข่ายในช่วงเวลาใดเวลาหนึ่ง

2.3.2.2 ผู้ใช้งานอาจจะมีการใช้ระบบเครือข่ายได้ไม่เต็มประสิทธิภาพผู้ดูแลระบบสามารถวิเคราะห์ได้ว่าควรจะมีการเพิ่มทรัพยากรใดบ้าง เพื่อจะช่วยให้ผู้ใช้งานได้ใช้ระบบเครือข่ายได้อย่างเต็มประสิทธิภาพ

2.3.2.3 ผู้ดูแลระบบสามารถที่จะวางแผนการขยายระบบเครือข่าย ถ้าทราบรายละเอียดของกิจกรรมต่างๆ ของผู้ใช้งานเพียงพอ

2.3.3 จัดการเกี่ยวกับการคอนฟิกกูเลชั่นระบบเครือข่าย (Configuration Management)

สามารถทำการคอนฟิกกูเลชั่นการทำงานของอุปกรณ์ต่างๆให้สามารถทำงานโดยอาศัยโปรแกรมประยุกต์ที่แตกต่างกันได้กับอุปกรณ์ชนิดเดียวกัน การที่เราจะเซตค่าต่างๆ หรือทำการคอนฟิกกูเลชั่นเราจะทำจากสถานีจัดการ (Network Management Station:NMS)โดยการเซตจะทำการเซตค่าของแอตทริบิวและแวรรูของอุปกรณ์แต่ละตัว

2.3.4 จัดการบริหารประสิทธิภาพระบบเครือข่าย (Performance Management)

ในการติดต่อสื่อสารในระบบเครือข่ายคอมพิวเตอร์ จะประกอบด้วยส่วนประกอบต่างๆ มากมายที่ทำการเชื่อมต่ออยู่ในระบบเครือข่ายและมีการแบ่งปันทรัพยากรซึ่งกันและกัน การบริหารเรื่องประสิทธิภาพของระบบเครือข่ายจึงแบ่งได้ 2 ประเภทด้วยกันคือ

2.3.4.1 การตรวจสอบ (Network Monitoring)

2.3.4.2 การควบคุมระบบ (Network Controlling)

การตรวจสอบก็คือการที่ผู้ดูแลระบบ Administrator จะทำการตรวจสอบ Track ดูกิจกรรมต่างๆที่เกิดขึ้นบนระบบเครือข่าย ส่วนการควบคุมระบบก็คือการที่ผู้ดูแลระบบสามารถจะควบคุมหน้าที่การทำงานและบริหารอุปกรณ์ต่างๆ โดยการปรับหรือเซตค่าพารามิเตอร์ต่างๆ ภายในตัวอุปกรณ์ที่มีอยู่ในระบบเครือข่ายให้ทำงานได้ตามต้องการ

2.3.5 การบริหารงานด้านความปลอดภัย (Security Management)

การบริหารในด้านความปลอดภัยจะยึดหลักการกระจายข้อมูล (Data Distributing) และการเก็บรหัสลับรวมถึงการเข้ารหัสข้อมูลเพื่อให้เราสามารถเข้าถึงข้อมูลต่างๆได้อย่างปลอดภัย รวมถึงการใช้ในการตรวจสอบและควบคุมระบบเครือข่าย

2.4 หลักการบริหารระบบเครือข่ายโดยใช้โพรโตคอลเอสเอ็นเอ็มพี (Simple Network Management Protocol: SNMP)

ซิมเปิลเน็ทเวิคแมเนจเม็นโพรโตคอล (Simple network management protocol: SNMP) ถูกพัฒนาโดยยึดหลักความง่ายและเป็นเครื่องมือที่ถูกสร้างมาในยุคต้นๆ โดยใช้ทำงานกับ โพรโตคอลทีซีพี/ไอพี (TCP/IP) ที่มีการใช้งานกันอย่างแพร่หลาย โดยเอสเอ็นเอ็มพี(SNMP) ได้ถูกกำหนดให้เป็นมาตรฐานหนึ่งของไอเอสโอ (The International Organization for Standardization: ISO) และซีซีไอทีที(The International Telegraph and Telephone Consulative Committee: CCITT) รายละเอียดของโพรโตคอลเอสเอ็นเอ็มพีจะได้กล่าวถึงอย่างละเอียดอีกครั้งหนึ่ง

โมเดลของการบริหารระบบเครือข่าย (Network Management) ที่ใช้สำหรับเครือข่ายทีซีพี/ไอพี (TCP/IP) ประกอบด้วยส่วนต่างๆดังต่อไปนี้

2.4.1 สถานีจัดการ (Management Station)

ตัวสถานีจัดการ (Management Station) เป็นเครื่องที่ใช้ในการบริหารระบบเครือข่าย หรืออาจจะกล่าวว่าเป็นเครื่องที่ใช้ติดต่อกับยูเซอร์ (User) นั้นเองซึ่งส่วนของสถานีจัดการ จะประกอบด้วยส่วนต่างๆดังต่อไปนี้คือ

2.4.1.1 โปรแกรมจัดการ (Management Application) สำหรับใช้วิเคราะห์ข้อมูลหรือใช้เฝ้าตรวจสอบระบบเครือข่าย

2.4.1.2 ส่วนของอินเตอร์เฟส (Interface) ทั้งที่เป็นส่วนที่ใช้ในการแสดงผล (Monitor) และส่วนที่ใช้ในการควบคุม (Control) ระบบเครือข่าย

2.4.1.3 ส่วนที่ใช้ในการดึงข้อมูลจากฐานข้อมูลการจัดการ (MIB) บนอุปกรณ์ต่างๆ ในระบบเครือข่ายมาใช้ หรือเปลี่ยนแปลงค่าได้

2.4.2 แมนเนเจเมนท์เอเจนต์ (Management Agent)

ส่วนอุปกรณ์อื่นๆที่มีซอฟต์แวร์เอเจนต์ฝังอยู่ เราจะเรียกว่าแมนเนเจอร์เจนต์ (Management Agent) เช่น โฮล (Host), บริจด์(Bridge), เราท์เตอร์(Router) และ ฮับ(Hub) เป็นต้น โดยอุปกรณ์ดังกล่าวสามารถถูกบริหารจากสถานีจัดการได้ ซึ่งอุปกรณ์แต่ละตัวจะมีโปรแกรมเอเจนต์ (Agent Software) ติดตั้งอยู่ และจะถูกมองเป็นอ๊อปเจกต์ (Object) หนึ่งของระบบการจัดการ แต่ละอ๊อปเจกต์จะมีการนิยามฟังก์ชั่นการจัดการขึ้นกับอุปกรณ์นั้นๆ ในการตรวจสอบระบบเครือข่าย สถานีจัดการจะร้องขอข้อมูลจากเอเจนต์โดยระบุตำแหน่งข้อมูลที่ต้องการในฐานข้อมูลการจัดการ ส่วนการกำหนดค่า (Setting) การทำงานต่างๆ ก็สามารถทำในลักษณะเดียวกัน โดยการกำหนดค่าอ๊อปเจกต์ไอดีแล้วตามด้วยค่าที่ต้องการให้เปลี่ยนแปลงในฐานข้อมูลการจัดการของตัวเอเจนต์ที่ต้องการ

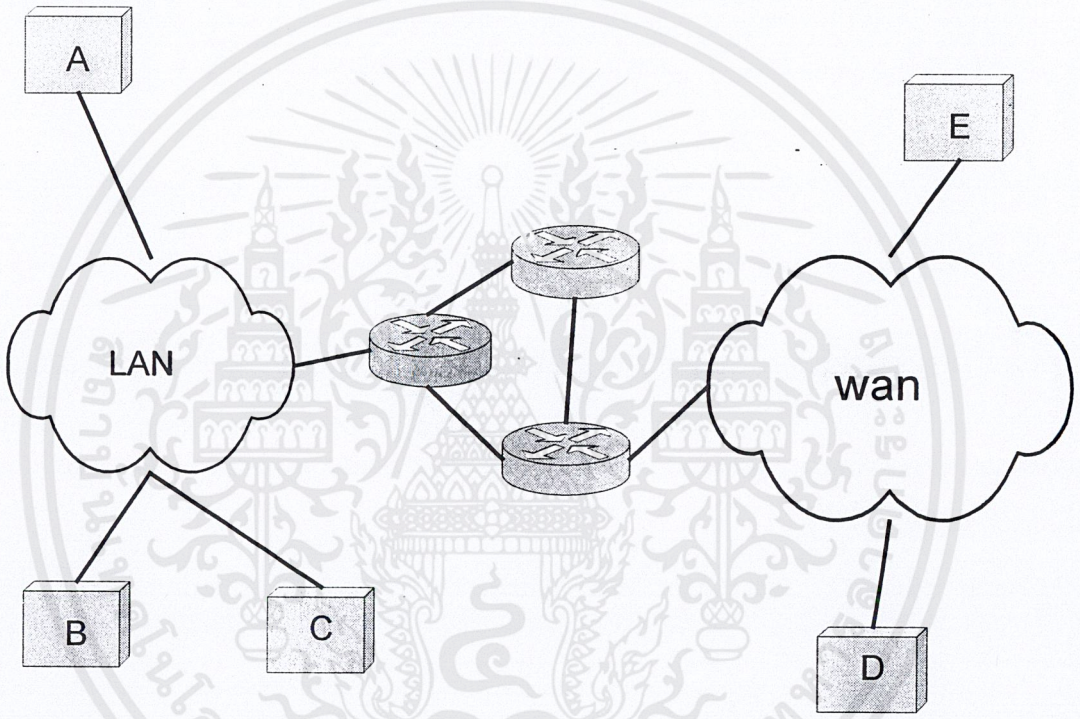
2.4.3 ฐานข้อมูลการจัดการ (Management Information Base: MIB)

ฐานข้อมูลการจัดการคือส่วนของฐานข้อมูลที่ใช้สำหรับเก็บตัวเลขที่ใช้ระบุถึงโหนดของเอเจนต์ที่เราสนใจ การอ้างถึงโหนดภายในฐานข้อมูลการจัดการ สามารถใช้วิธีการอ้างอิงได้สองแบบ คือ การอ้างอิงแบบตัวเลข (Numerical) และการอ้างอิงแบบตัวอักษร (Symbolic)

2.5 เครือข่าย ทีซีพี/ไอพี(TCP/IP Network)

เครือข่ายทีซีพี/ไอพีหรือเครือข่ายอินเตอร์เน็ทเป็นเครือข่ายที่ใช้โพรโตคอลทีซีพี/ไอพีในการสื่อสารแลกเปลี่ยนข้อมูล อินเทอร์เน็ทโพรโตคอล (IP) เป็นขั้นตอนที่ทำให้ข้อมูลไปถึงจุดหมายปลายทางที่ต้องการ ส่วน Transmission Control Protocol (TCP) เป็นขั้นตอนที่จะรับประกันความถูกต้องของข้อมูลที่ส่งซึ่งถูกนำมาใช้งานร่วมกันในการติดต่อสื่อสารเรียกว่าทีซีพี/ไอพี

โพรโตคอลทีซีพี/ไอพีถูกออกแบบมาให้ทำหน้าที่เชื่อมโยงเครือข่ายกลุ่มย่อยๆเข้าด้วยกันจนกลายเป็นเครือข่ายที่มีขนาดใหญ่ ทำให้ผู้ใช้งานมองเป็นเครือข่ายเดียว ระบบปฏิบัติการยูนิกซ์(Unix) ได้นำเอาโพรโตคอลนี้รวมเข้าไว้ระบบปฏิบัติการเพื่อใช้ทำเป็น Network Operating System และมีผู้นิยมใช้เป็นจำนวนมาก การสื่อสารบนเครือข่ายทีซีพี/ไอพี ก็ถูกแบ่งการทำงานออกเป็นลำดับชั้น (Layer) 5 ชั้นประกอบด้วย Application Layer, transport Layer, Network Layer, Data Link Layer และ Physical Layer



รูปที่ 2-1 แสดงการเชื่อมต่อของเครือข่าย ทีซีพี/ไอพี

2.5.1 Application Layer

เป็นชั้นกล่าวถึงแอพพลิเคชั่นต่างๆที่ใช้งานหรือให้บริการบนเครือข่าย ทีซีพี/ไอพี เช่น E-mail, File transfer Protocol (FTP) และ Remote login

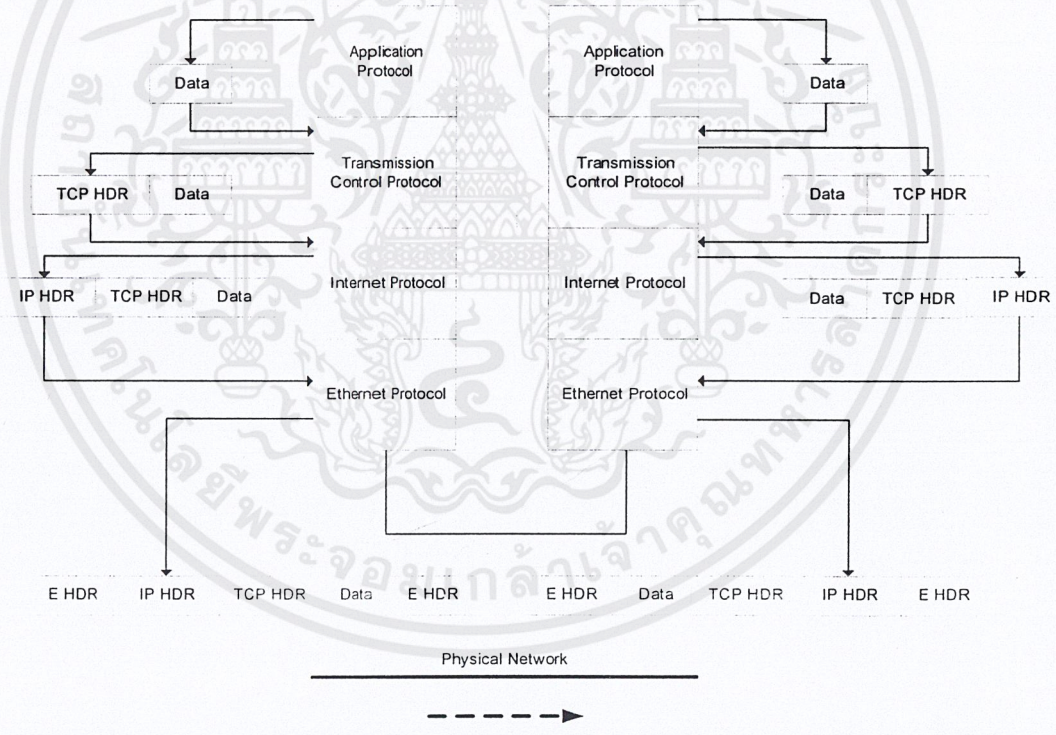
2.5.2 Transport Layer

ในชั้นนี้จะมี 2 โพรโตคอลที่ทำงานอยู่คือ Transport Control Protocol (TCP) และ User Datagram (UDP) โดยทีซีพีจะเป็นส่วนที่ทำงานในคอมพิวเตอร์มีหน้าที่ทำให้แน่ใจว่าไม่มีความผิด

พลาดของการรับส่งข้อมูลเป็นลำดับครบถ้วน โดยแอพพลิเคชั่นที่ต้องการส่งข้อมูลจะผ่านการทำงานของทีซีพี

ซึ่งในทีซีพีจะทำการแบ่งข้อมูลที่รับเข้ามาออกเป็นส่วนย่อยๆเรียกว่าการทำเซกเมนต์ (Segment) เพื่อไม่ให้มีข้อมูลที่ยาวเกินไปช่วยลดความผิดพลาดของการส่งข้อมูลขนาดใหญ่ ในขณะเดียวกันทีซีพี (ฝั่งรับ) จะทำหน้าที่ส่งข้อมูลตอบรับ (Acknowledge) แจ้งให้ผู้ส่งข้อมูลรับทราบว่าได้รับข้อมูลเรียบร้อยแล้ว แต่ถ้าฝั่งส่งข้อมูลไม่ได้รับข้อมูลตอบรับภายในเวลาที่กำหนด ฝั่งส่งก็จะทำการส่งข้อมูลซ้ำไปอีกที เนื่องจากมีการแบ่งข้อมูลออกเป็นส่วนย่อยๆแล้วส่งออกไปซึ่งอาจไปทำให้ข้อมูลไปถึงปลายทางไม่เป็นลำดับดังนั้นหน้าที่อีกอย่างของทีซีพีคือการเรียงลำดับข้อมูลให้ถูกต้องแล้วประกอบกลับให้เป็นข้อมูลที่เหมือนกับฝั่งส่งข้อมูลทุกประการ

ส่วนยูดีพี (UDP) เป็นโพรโตคอลที่ไม่จัดการเกี่ยวกับการรับรองความถูกต้องของข้อมูลว่ามีข้อผิดพลาดหรือไม่ ไม่มีการจัดเรียงข้อมูลซึ่งยูดีพีเป็นโพรโตคอลที่มีกลไกในการทำไม่ซับซ้อนทำให้ง่ายต่อการใช้งาน



รูปที่ 2-2 แสดงการเอนแคปซูเลชั่นข้อมูล และการแลกเปลี่ยนข้อมูลบนเครือข่ายทีซีพีไอพี

2.5.3 Network Layer

ขั้นตอนขอไอพี (IP) เป็นขั้นตอนการส่งข้อมูลระหว่างเครื่อง ดังนั้นจึงต้องมีการระบุถึงหมายเลขประจำเครื่อง (ตำแหน่ง) ในระบบอินเทอร์เน็ตเป็นตัวระบุว่าข้อมูลจะส่งไปยังตำแหน่งใดในเครือข่าย ลักษณะของหมายเลขประจำเครื่องมีรูปแบบดังนี้ "161.246.4.3" ส่วนของหมายเลข เครือข่ายคือ 161.246.0.0 จะถูกกำหนดโดยหน่วยงาน NIC ของกระทรวงกลาโหมสหรัฐเพื่อไม่ให้ซ้ำซ้อนกัน ส่วนตัวหลังเป็นเลขที่กำหนดโดยผู้บริหารเครือข่ายให้กับเครื่องคอมพิวเตอร์ที่อยู่ในเครือข่าย

2.5.4 Data Link Layer

เป็นชั้นกล่าวถึง ขั้นตอน รูปแบบการส่งข้อมูลไปยังปลายทาง รวมถึงการตรวจสอบข้อมูลและการชนกันของข้อมูล (Error Detection/collection) โดยมีผู้กำหนดมาตรฐานขึ้นมาใช้การสื่อสารข้อมูล เช่น X.25, IEEE ฯลฯ IEEE ได้กำหนดมาตรฐาน IEEE 802 ที่กล่าวถึง

IEEE 802.3: เป็นเครือข่าย Ethernet ที่ใช้การตรวจสอบการชนกันแบบ Carrier sense multiple accesses with collision detection: CSMA/CD

IEEE 802.4: เป็นเครือข่าย Token Bus ที่ใช้ตัว Token กำหนดสิทธิในการส่งข้อมูลอุปกรณ์ใดที่ไม่มี Token จะไม่มีสิทธิในการส่งข้อมูล เป็นการป้องกันการชนกันของข้อมูลในเครือข่าย

IEEE 802.5: เป็นเครือข่าย Token Ring ที่ใช้ตัว Token กำหนดสิทธิในการส่งข้อมูลเช่นเดียวกับ Token Bus

2.5.5 Physical Layer

เป็นส่วนที่จัดการเกี่ยวกับการเชื่อมต่อทางกายภาพของเครือข่ายโดยจะกล่าวถึงตัวกลางในการสื่อสาร (Medium) รูปแบบของสัญญาณที่ใช้ในการส่งข้อมูลและรวมไปถึงกรรมวิธีการแปลงข้อมูลเป็นสัญญาณต่างๆ ที่สามารถส่งตัวกลางต่างๆเช่นได้แก่ สายเคเบิล, ใยแก้วนำแสง, คลื่นวิทยุ ฯลฯ

บทที่ 3
โพรโตคอลทีซีพี/ไอพี

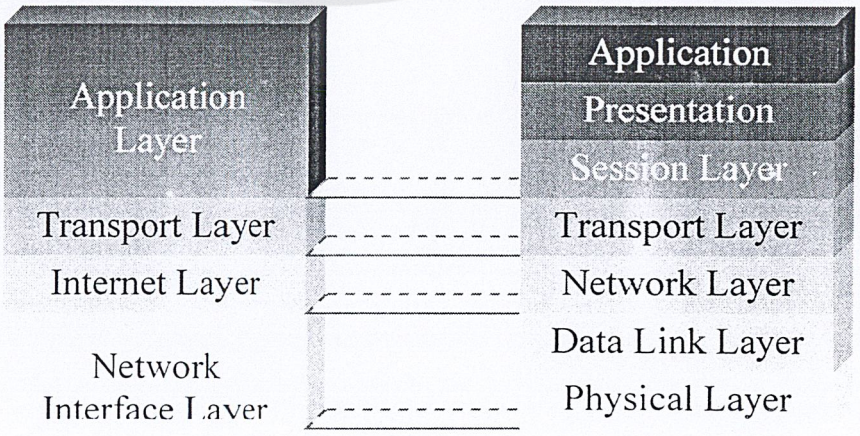
3.1 ความเป็นมาของโพรโตคอลทีซีพี/ไอพี

ทีซีพี/ไอพี เป็นโพรโตคอลมาตรฐานที่ใช้กันอยู่ในระบบปฏิบัติการแบบยูนิกซ์ เริ่มพัฒนาโดยกระทรวงกลาโหมของสหรัฐฯ ในปี ค.ศ. 1969 เพื่อเชื่อมโยงเครื่องคอมพิวเตอร์ทางทหารของแต่ละหน่วยที่อยู่ห่างไกลกัน โดยมีจุดประสงค์ คือสร้างระบบเครือข่ายให้เครื่องคอมพิวเตอร์สามารถรับส่งข้อมูลกันได้ แม้ว่าสายส่งข้อมูลบางส่วนจะถูกทำลายเสียหายไปก็ตาม เพื่อใช้งานในยามเกิดสงคราม โดยเครือข่ายที่จัดตั้งในระยะแรกชื่อว่า Advanced Research Projects Agency Network หรือ อาร์พาเน็ต (ARPANET)

ต่อมาได้พัฒนาเป็นเครือข่ายอินเทอร์เน็ต (INTERNET) โพรโตคอลนี้เหมาะสำหรับเชื่อมต่อคอมพิวเตอร์ทั้งใกล้ และไกลเข้าด้วยกัน และมีมาตรฐานรองรับทำให้ผู้ผลิตฮาร์ดแวร์ และซอฟต์แวร์สามารถสร้างอุปกรณ์ และโปรแกรมที่จะรองรับการทำงานของโพรโตคอลนี้ ทำให้เครื่องคอมพิวเตอร์สามารถรับส่งข้อมูลกันได้ไม่ว่าจะเป็นเครื่องขนาดเล็กหรือขนาดใหญ่ หรือใช้ระบบปฏิบัติการอะไรก็ตาม ทีซีพี/ไอพี (TCP/IP) เป็นชุดโพรโตคอลที่ประกอบด้วยโพรโตคอลต่างๆ หลายโพรโตคอล แต่ละโพรโตคอลมีคุณลักษณะ และมีความสามารถในการทำงานแตกต่างกัน โดยที่ในบทนี้ได้กล่าวถึงรายละเอียดและคุณสมบัติของโพรโตคอลที่สำคัญบางโพรโตคอล

3.2 การเชื่อมต่อของโพรโตคอลทีซีพี/ไอพี (TCP/IP Linking)

ทีซีพี/ไอพี (TCP/IP หรือ Transmission Control Protocol/Internet Protocol) เป็นโพรโตคอลในการสื่อสารในระบบอินเทอร์เน็ต และอินทราเน็ต มีหน้าที่ตรวจสอบการรับส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ของฝ่ายรับ และฝ่ายส่งให้ได้รับข้อมูลที่ถูกต้องครบถ้วน หากข้อมูลที่ส่งมาเกิดการสูญหายระหว่างทางจะมีการแจ้งให้ต้นทางส่งข้อมูลมาใหม่ การทำงานของทีซีพี/ไอพีสามารถเปรียบเทียบกับโมเดลอ้างอิงโอเอสไอ (Open System Interconnection Reference Model: OSI) ตามมาตรฐานไอเอสโอ (International Organization for Standardization: ISO) ได้ดังรูปที่ 2-1

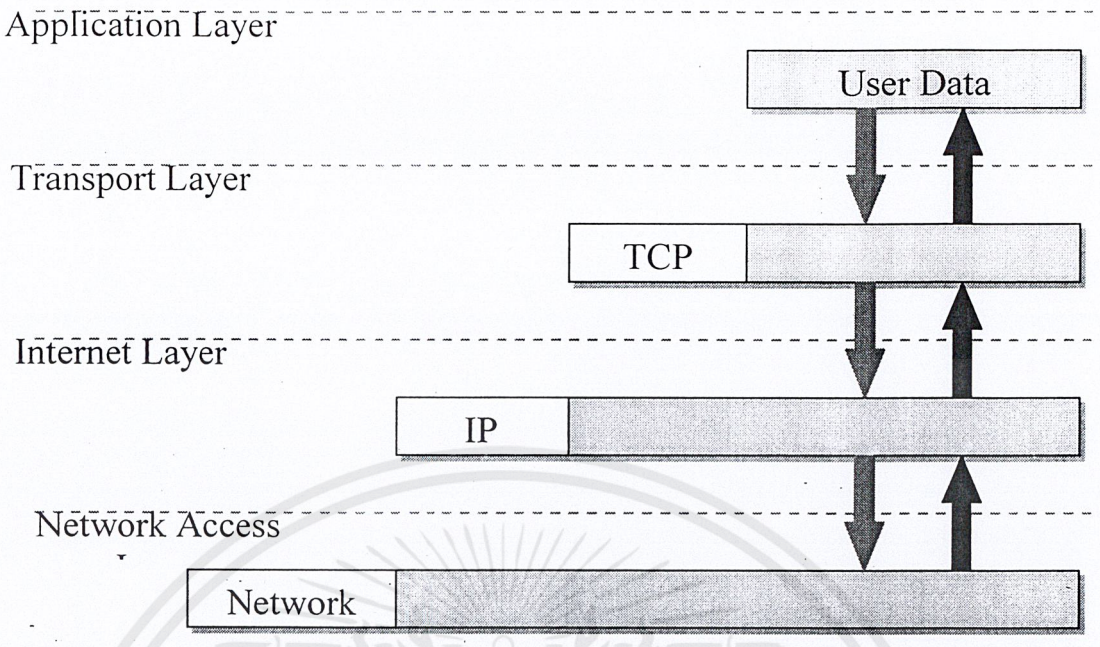


รูปที่ 3-1 แสดงการเปรียบเทียบเลเยอร์ของโอเอสไอกับเลเยอร์ของทีซีพี/ไอพี

ในแต่ละระดับชั้นของทีซีพี/ไอพีมีการทำงานที่แตกต่างกัน ตั้งแต่การติดต่อกับแอพพลิเคชันจนกระทั่งแปลงเป็นสัญญาณส่งไปตามสายสัญญาณ ซึ่งการทำงานในแต่ละระดับชั้นของทีซีพี/ไอพี มีดังตารางที่ 2-1

ชื่อระดับชั้น	หน้าที่
1. ชั้นแอพพลิเคชัน (Application Layer)	รองรับการทำงานของแอพพลิเคชันต่างๆ ที่ทำงานเป็นโพรเซสอยู่ในเครื่องต้นทางและปลายทาง โดยจัดการเชื่อมต่อระหว่างโพรเซส หรือแอพพลิเคชันที่อยู่ต่างเครื่องกัน โดยการทำงานของแอพพลิเคชันต่างๆมีการติดต่อกันตามแต่ละโพรโตคอลเฉพาะแล้วแต่แอพพลิเคชันที่ใช้งาน ซึ่งจะขอบริการจากชั้นทรานสปอร์ตอีกทีหนึ่ง
2. ชั้นทรานสปอร์ต (Transport Layer)	สร้างการเชื่อมต่อกันระหว่างแอพพลิเคชันแบบ end-to-end โดยจุดที่เชื่อมต่อกันเพื่อรับส่งข้อมูลนี้เรียกว่า พอร์ต (port) หรือซ็อกเก็ต (Socket) ในชั้นนี้มีบริการหลักอยู่ 2 แบบ คือ Connection Oriented โดยเรียกผ่านโพรโตคอลทีซีพี (TCP: Transmission Control Protocol) และ Connectionless ซึ่งเรียกผ่านโพรโตคอลยูดีพี (UDP: User Datagram Protocol) ซึ่งกล่าวถึงในหัวข้อถัดไป
3. ชั้นอินเทอร์เน็ต (Internet Layer)	ส่งผ่านข้อมูลระหว่างเครือข่าย โดยมีโพรโตคอลที่ทำงานเป็นกลไกสำคัญในการส่งผ่านข้อมูลไปยังเครือข่ายใดๆ ในอินเทอร์เน็ต คือ ไอพี (Internet Protocol: IP) ซึ่งกล่าวถึงในหัวข้อถัดไป นอกจากนี้ในชั้นนี้ยังมีโพรโตคอลทำงานอยู่ด้วยอีก 2 ชนิด คือ ไอซีเอ็มพี (Internet Control Message Protocol: ICMP) และเออาร์พี (Address Resolution Protocol: ARP)
4. ชั้นเน็ตเวิร์กอินเตอร์เฟส (Network Interface Layer)	แปลงข้อมูลให้อยู่ในรูปที่เหมาะสมกับเครือข่ายแต่ละแบบ ซึ่งแตกต่างกันออกไป และแปลงเป็นสัญญาณไฟฟ้าส่งไปยังเครือข่าย

ตารางที่ 3-1 การทำงานของแต่ละระดับชั้นของทีซีพี/ไอพี

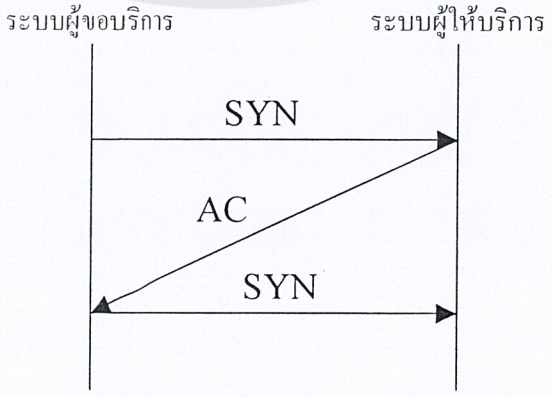


รูปที่ 3-2 แสดงการข้อมูลที่ส่งผ่านในโมเดลของทีซีพี/ไอพี

ในชุดโพรโตคอลทีซีพี/ไอพีนี้ มีโพรโตคอลหลัก ที่ขอกล่าวถึง 3 โพรโตคอล ได้แก่ โพรโตคอลทีซีพี โพรโตคอลยูดีพี ซึ่งทำงานในชั้นทรานสปอร์ต และโพรโตคอลไอพี ซึ่งทำงานในชั้นอินเทอร์เน็ต โดยมีรายละเอียดดังต่อไปนี้

3.3 โพรโตคอลทีซีพี (TCP: Transmission Control Protocol)

การทำงานที่สำคัญอย่างหนึ่งของโพรโตคอลทีซีพี คือ การทำ "3-Way Handshake" ซึ่งเป็นกระบวนการเริ่มต้นในการสร้างการเชื่อมต่อในชั้นทรานสปอร์ต กล่าวคือ ในการติดต่อกันระหว่างระบบในเครือข่ายต้องมีการสร้างการเชื่อมต่อไปยังระบบที่ให้บริการก่อน โดยผู้ขอบริการส่งสัญญาณ SYN เพื่อขอบริการ จากนั้นผู้ให้บริการจะส่งสัญญาณ ACK เพื่อตอบรับการเชื่อมต่อที่ร้องขอมา จึงสามารถรับส่งข้อมูลกันได้ ดังรูปที่ 2-3



รูปที่ 3-3 แสดงการทำ 3-Way Handshake

การเชื่อมต่อแบบ 3-Way Handshake นี้ เป็นการตรวจสอบความพร้อมของทั้งฝ่ายส่ง และฝ่ายรับ และการกำหนดค่าเริ่มต้นของพารามิเตอร์ต่างๆ ของทั้งสองฝ่ายให้ตรงกัน หลังจากกระบวนการทำ 3-Way Handshake สิ้นสุด ทั้งสองฝ่ายจึงสามารถรับ และส่งข้อมูลซึ่งกัน และกันได้

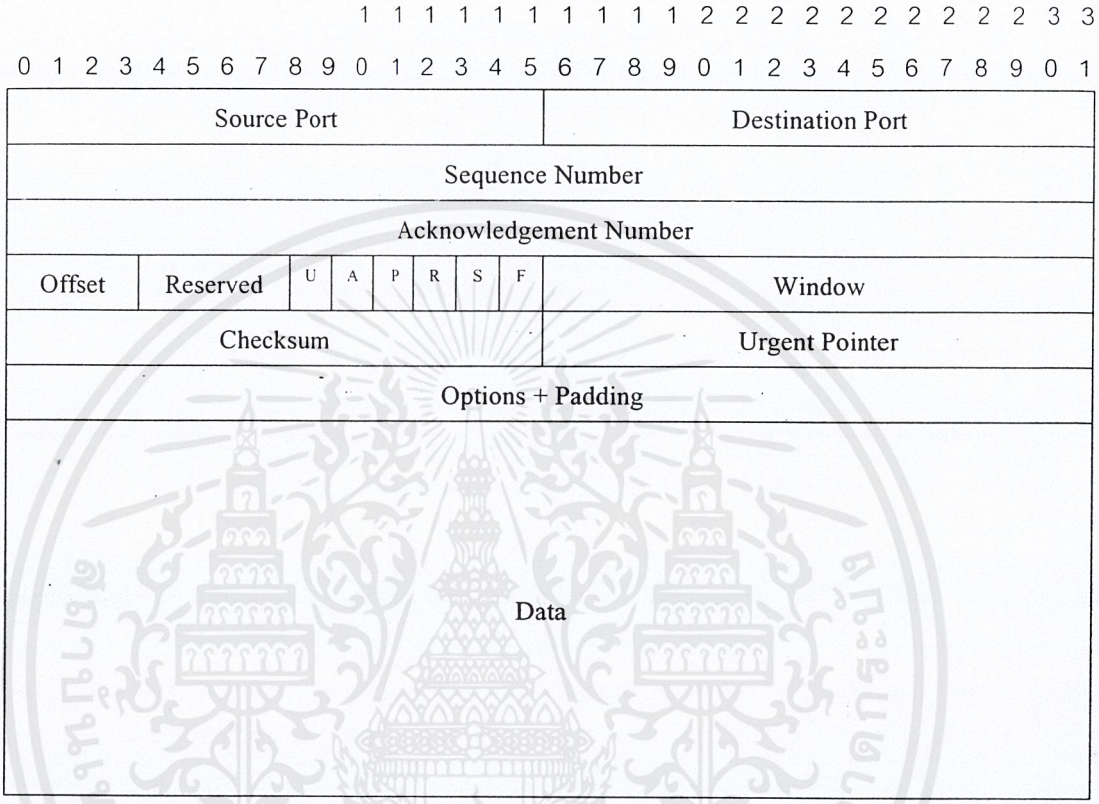
ดังนั้นโพรโตคอลทีซีพีจึงเป็นโพรโตคอลที่มีการรับส่งข้อมูลแบบ "Connection Oriented" ทำให้การทำงานของทีซีพีมีความน่าเชื่อถือมากขึ้น หน้าที่การทำงานของทีซีพีในการรับส่งข้อมูลมีหน้าที่หลัก 6 ข้อ คือ

1. ควบคุมการรับส่งข้อมูล (Basic Data Transfer)
2. ความน่าเชื่อถือในการรับส่งข้อมูล (Reliability)
3. ควบคุมการไหลของข้อมูล (Flow Control)
4. การทำมัลติเพล็ก (Multiplexing)
5. ควบคุมการเชื่อมต่อ (Connection)
6. ความปลอดภัยในการรับส่งข้อมูล (Security)

<u>ส่วนประกอบของทีซีพีเฮดเดอร์</u>

1. *Source Port* : เป็นหมายเลขพอร์ตของบริการที่เครื่องต้นทาง
2. *Destination Port* : เป็นหมายเลขพอร์ตของบริการเครื่องปลายทาง
3. *Sequence Number* : เป็นหมายเลขที่บอกลำดับของการรับส่งข้อมูลของเครื่องที่ต้องการขอส่งข้อมูล
4. *Acknowledgement Number* : เป็นหมายเลขที่บอกลำดับของการรับส่งข้อมูลที่ฝั่งรับข้อมูลปกติ ค่าของ Acknowledgement Number มีค่าเท่ากับ Sequence Number (ของอีกฝั่งหนึ่ง) + 1 เสมอ
5. *Data Offset* : เป็นตัวบอกค่าออฟเซตของข้อมูล เพราะทีซีพีนั้นไม่มีการกำหนดความยาวที่แน่นอนของข้อมูล จึงต้องมีออฟเซตเป็นตัวบอก
6. *Flag* : เป็นบิตที่บอกชนิดของข้อมูล ได้แก่
   - URG : Urgent Pointer Field Significant - แสดง Urgent Pointer
   - ACK : Acknowledgement Field Significant – แสดงการ Acknowledgement
   - PSH : Push Function
   - RST : Reset The Connection - แสดงเมื่อรีเซ็ทการเชื่อมต่อ
   - SYN : Synchronize Sequence Number - หมายเลขแพ็กเก็ตที่ส่งแบบซิงโครนัส
   - FIN : No more data from sender - แสดงว่าไม่มีข้อมูลที่ส่งจากผู้ส่งแล้ว
7. *Window* : เป็นเลขบอกจำนวนของอ็อกเต็ต (octet) ของข้อมูล จัดการในส่วนของ end-to-end flow control
8. *Checksum* : เป็นส่วนที่ตรวจสอบความถูกต้องของข้อมูล
9. *Urgent Pointer* : เป็นตัวชี้ตำแหน่งของ Urgent Data

10. *Option and Padding* : เป็นตัวบอกออปชันของโพรเซสที่ใช้ทีซีพี
11. *Data* : เนื้อข้อมูลที่ต้องการสื่อสาร มีขนาดได้ไม่ต่ำกว่า 5 32-บิตเวิร์ด (6 บิตแรกสงวนไว้และกำหนดให้เป็นศูนย์)



รูปที่ 3-4 แสดงแพ็กเก็ตทีซีพี

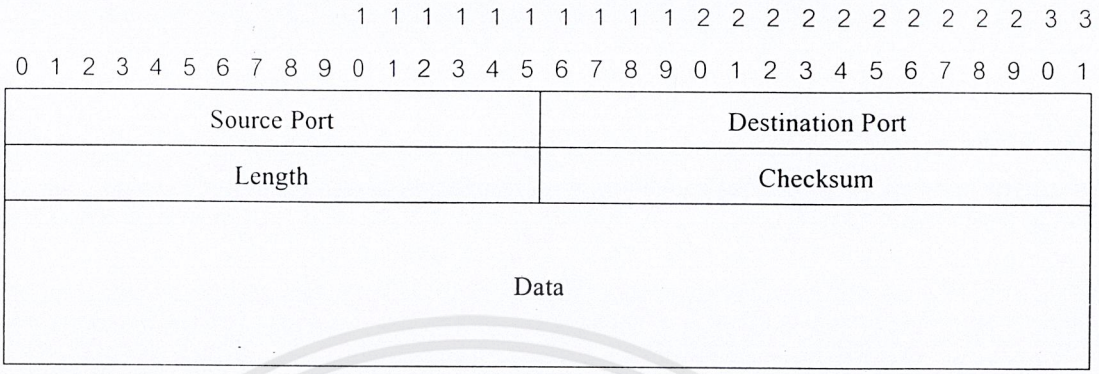
3.4 โพรโตคอลยูดีพี (UDP: User Datagram Protocol)

โพรโตคอลยูดีพีเป็นโพรโตคอลในการติดต่อสื่อสารในชั้นทรานสปอร์ต (Transport Layer) การทำงานคล้ายกับทีซีพีมาก คือจัดการเกี่ยวกับการสื่อสารระหว่างเครื่อง แต่เป็นแบบ Connectionless คือทั้งฝ่ายส่ง และฝ่ายรับไม่จำเป็นต้องอาศัยการสร้างช่องทางเชื่อมต่อกัน โดยไม่ต้องมีการแจ้งให้ฝ่ายรับข้อมูลเตรียมรับข้อมูลเหมือนโพรโตคอลทีซีพี และไม่มีการส่งสัญญาณตรวจสอบว่าข้อมูลถึงเครื่องปลายทางอย่างถูกต้องครบถ้วนในการส่งข้อมูลแต่ละครั้ง จึงไม่มีการส่งข้อมูลใหม่อีกในกรณีที่เกิดความผิดพลาดของการส่งข้อมูล

<u>ส่วนประกอบของ UDP Frame</u>

1. *Source Port* : เป็นค่าตัวเลข 16 บิต บอกพอร์ตของบริการที่เครื่องต้นทาง
2. *Destination Port* : เป็นค่าตัวเลข 16 บิต บอกพอร์ตของบริการที่เครื่องปลายทาง
3. *Length* : เป็นค่าตัวเลข 16 บิต บอกความยาวของข้อมูล

4. *Checksum* : เป็นค่าตัวเลข 16 บิต ตรวจสอบความถูกต้องของข้อมูลที่ส่ง

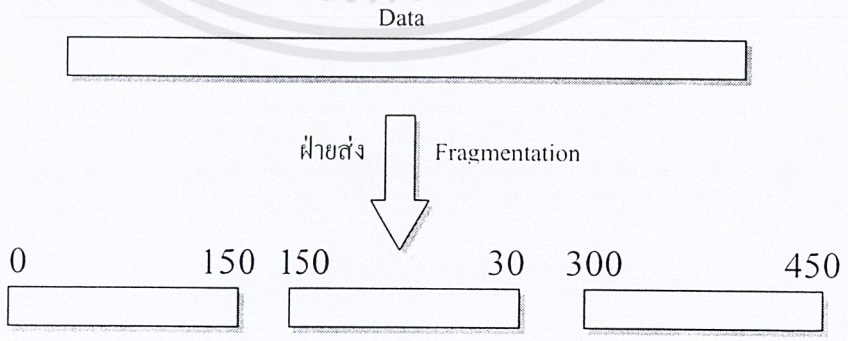


รูปที่ 3-5 แสดงแพ็กเก็ตยูดีพี

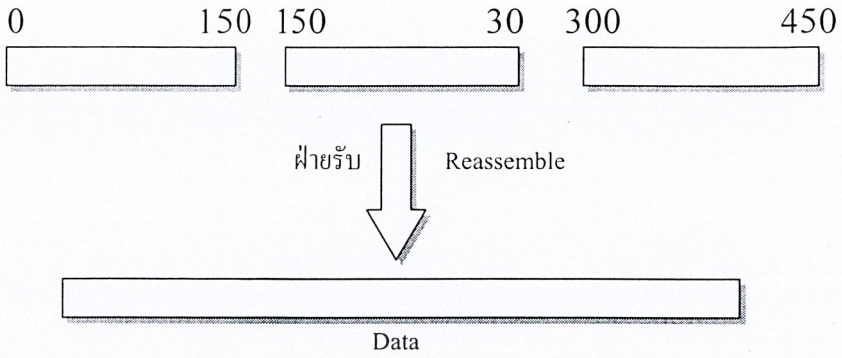
3.5 โพรโตคอลไอพี (IP: Internet Protocol)

โพรโตคอลไอพีเป็นโพรโตคอลที่จัดการเกี่ยวกับแอดเดรสของแต่ละแพ็กเก็ต เพื่อให้ส่งแพ็กเก็ตต่างๆ ไปยังเป้าหมายได้ถูกต้อง การทำงานของไอพีเป็นเพียงการส่งข้อมูลไปยังเครื่องเป้าหมายเท่านั้น ไม่มีการส่งสัญญาณขอบริการ หรือสัญญาณให้บริการระหว่างกันเหมือนทีซีพี เรียกว่าการเชื่อมต่อแบบ Connectionless ซึ่งระบบทั้งสองตั้งสมมติฐานว่าการเชื่อมต่อระหว่างกันไม่มีความผิดพลาดเกิดขึ้นแน่

เนื่องจากมาตรฐานในเครือข่ายมีหลากหลาย ขนาดของแพ็กเก็ตในแต่ละมาตรฐานจึงมีความแตกต่างกันออกไป ทำให้การส่งข้อมูลระหว่างอุปกรณ์ในเครือข่ายนั้นอาจมีการแบ่งข้อมูลออกเป็นแพ็กเก็ตย่อยๆ ในระหว่างการส่ง เรียกว่า การทำแฟร็กเมนเตชัน (Fragmentation) เช่น แพ็กเก็ตของ FDDI มีขนาด 4,500 ไบต์ หากเครื่องปลายอยู่ในเครือข่าย Ethernet ซึ่งมีขนาดของแพ็กเก็ตสูงสุดเพียง 1,500 ไบต์ ดังนั้นการส่งแพ็กเก็ตไปยังเครื่องปลายทางจึงต้องมีการแบ่งเป็นแพ็กเก็ตย่อย และเมื่อแพ็กเก็ตย่อยมาถึงเครื่องเป้าหมายก็จะมารวมกันเป็นแพ็กเก็ตเดิมที่มีขนาด 4,500 ไบต์อีกครั้ง เรียกการรวมกันนี้ว่า การรีแอสเซมเบิ้ล (Reassemble) ซึ่งทำให้ได้ข้อมูลเหมือนที่ส่งมาจากเครื่องต้นทาง



รูปที่ 3-6 แสดงการทำแฟร็กเมนเตชัน



รูปที่ 3-7 แสดงการรีแอสเซมเบิ้ล

ส่วนประกอบของแพ็กเก็ตไอพี

1. *version* : เป็นค่าตัวเลข 4 บิต บอกเวอร์ชันของมาตรฐานไอพีที่ใช้ โดยปกติมีค่าเป็น 4 ซึ่งหมายถึง IPv4
2. *Internet Header Length (IHL)* : เป็นตัวบอกความยาวเฮดเดอร์ของไอพี
3. *Type of Service* : เป็นส่วนที่บอกการทำงานของแพ็กเก็ตที่ส่งว่าทำหน้าที่อะไร มีทั้งหมด 8 บิต โดย

   Bit 0-2 : บอกรายละเอียดการทำงานของแพ็กเก็ตนั้นๆ

   111 - Network Control

   110 - Internetwork Control

   101 - CRITIC / ECP

   100 - Flash Override

   011 - Flash

   010 - Immediate

   001 - Priority

   000 - Routine

   Bit 3 : บอกถึงลักษณะของดีเลย์

   0 = Normal Delay - มีดีเลย์ปกติ

   1 = Low Delay - มีดีเลย์ต่ำ

   Bit 4 : บอกถึงประเภทของทรูพุต

   0 = Normal Throughput – มีทรูพุตปกติ

   1= High Throughput – มีทรูพุตสูง

   Bit 5 : บอกถึงประเภทของความน่าเชื่อถือ

0 = Normal Reliability - มีความน่าเชื่อถือพอประมาณ

1 = High Reliability - มีความน่าเชื่อถือสูง

Bit 6-7 : กันไว้ใช้ในอนาคต

4. *Total Length* : มีขนาด 16 บิต บอกถึงความยาวในดาต้าแกรมของไอพี
5. *Identification field* : เป็นตัวเลข 16 บิต เป็นค่าประจำตัวของไอพีนั้น โดยโฮสต์ที่ส่งเป็นผู้กำหนด และเพิ่มค่าขึ้นหนึ่งเมื่อมีการส่งดาต้าแกรมของไอพีใหม่ ซึ่งใช้ในการประกอบกลับ
6. *Flag* : เป็นตัวเลข 3 bit บอกลักษณะของแพ็กเก็ตว่ามีการแฟร็กเมนต์หรือไม่

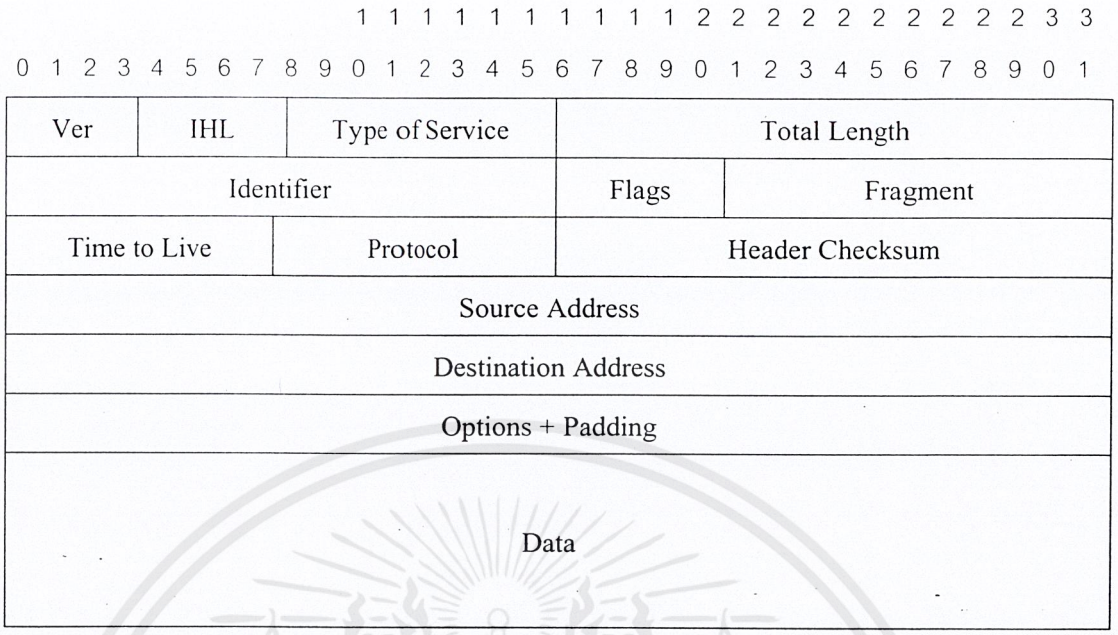
   Bit 0 : สงวนไว้ ปกติเป็น 0

   Bit 1 : 0 = บอกว่าแพ็กเก็ตมีการแตกแพ็กเก็ตย่อย

   1 = บอกว่าแพ็กเก็ตไม่มีการแตกแพ็กเก็ตย่อย

   Bit 2 : 0 = บอกว่าแพ็กเก็ตนั้นเป็นแพ็กเก็ตสุดท้ายที่ได้จากการแตกแพ็กเก็ตย่อย

   1 = บอกว่าแพ็กเก็ตนั้นยังไม่ใช่แพ็กเก็ตสุดท้ายที่ได้จากการแตกแพ็กเก็ตย่อย
7. *Fragment Offset* : เป็นค่าตัวเลข 13 บิต บอกออปเซตของแฟร็กเมนต์เมื่อเทียบในดาต้าแกรม
8. *Time To Live (TTL)* : เป็นตัวเลข 8 บิต บอกช่วงเวลาของแพ็กเก็ตที่ยังอยู่ในเครือข่ายได้ โดยกำหนดค่าเป็นจำนวนเราท์เตอร์สูงสุดที่ดาต้าแกรมผ่านได้ ซึ่งโดยทั่วไปที่ค่าระหว่าง 32 ถึง 64 และลดค่าลงเรื่อยๆ เมื่อผ่านเราเตอร์ เพื่อเป็นการป้องกันแพ็กเก็ตล้นเครือข่าย
9. *Protocol* : เป็นตัวเลข 8 bit บอกถึงโพรโตคอลที่อยู่เหนือขึ้นไป ว่าเป็นโพรโตคอลระดับสูงกว่าประเภทใด
10. *Header Checksum* : เป็นค่าตัวเลข 32 บิต ใช้ตรวจสอบความถูกต้องของเฮดเดอร์
11. *Source Address* : เป็นค่าตัวเลข 32 บิต บอกถึงไอพีแอดเดรสของเครื่องต้นทาง
12. *Destination Address* : เป็นค่าตัวเลข 32 บิต บอกถึงไอพีแอดเดรสของเครื่องปลายทาง



รูปที่ 3-8 แสดงแพ็กเก็ตไอพี

บทที่ 4

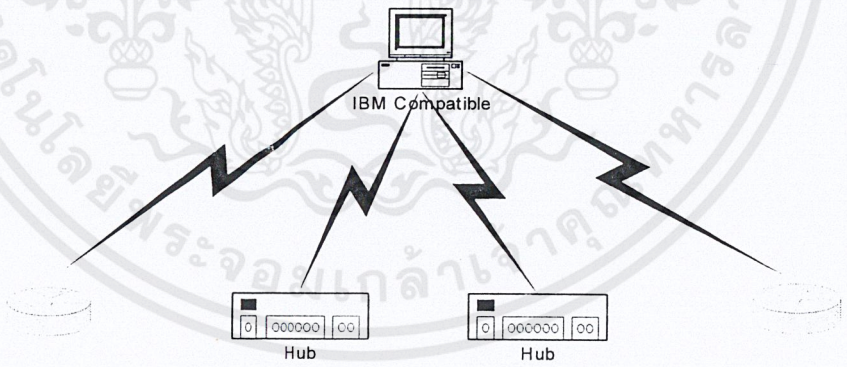
SNMP Service

การจัดการเครือข่ายใน TCP/IP อาศัยรูปแบบในการจัดการมาตรฐานตามข้อกำหนดของโพรโตคอล SNMP ซึ่งเป็นโพรโตคอลประยุกต์ที่กำหนดรูปแบบและกรรมวิธีจัดการเครือข่าย โดยมีสถานีจัดการเครือข่ายส่วนกลางทำหน้าที่ดูแล ตรวจสอบ และควบคุมการทำงานของอุปกรณ์เครือข่าย

4.1 พื้นฐานการบริหารเครือข่าย

ประโยชน์จากการใช้คอมพิวเตอร์และเครือข่ายคือประหยัดเวลาและค่าใช้จ่าย แต่ในขณะเดียวกันการใช้คอมพิวเตอร์ก็ต้องลงทุนทั้งเวลาและค่าใช้จ่ายเพื่อดูแลให้คอมพิวเตอร์และเครือข่ายทำงานได้ด้วย เครือข่ายขนาดใหญ่ที่ประกอบด้วยคอมพิวเตอร์และอุปกรณ์จำนวนมากจะทำงานได้อย่างมีประสิทธิภาพจำเป็นต้องใช้คอมพิวเตอร์ช่วยบริหารและจัดการตัวระบบเองด้วย

การบริหารเครือข่ายคือการตรวจ ควบคุม และวางแผนการใช้ทรัพยากรระบบเพื่อให้เครือข่ายทำงานได้อย่างมีประสิทธิภาพและสามารถตรวจหาจุดบกพร่องที่เกิดขึ้นเพื่อแก้ไขปัญหาได้อย่างรวดเร็ว คอมพิวเตอร์อย่างน้อยหนึ่งเครื่องในเครือข่ายทำหน้าที่เป็น แมเนเจอร์ (manager) เพื่อใช้เป็นสถานีจัดการ แมเนเจอร์อาจเรียกอีกชื่อว่า สถานีจัดการเครือข่าย (network management station) หรือ เอ็นเอ็มเอส (NMS)

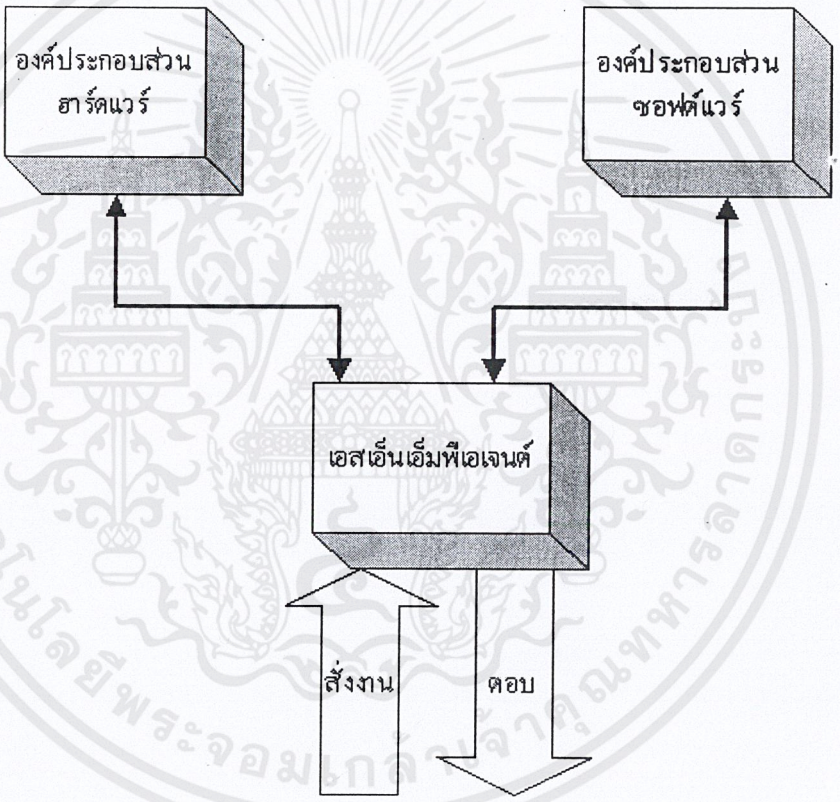


รูปที่ 4-1 องค์ประกอบในระบบจัดการเครือข่าย

4.2 เอสเอ็นเอ็มพีเอเจนต์

การจัดการเครือข่ายในทีซีพี/ไอพีอาศัยรูปแบบการจัดการมาตรฐานตามข้อกำหนดของโพรโตคอล เอสเอ็นเอ็มพี (SNMP: Simple Network Management Protocol) ซึ่งเป็นโพรโตคอลประยุกต์ที่กำหนดรูปแบบและกรรมวิธีจัดการเครือข่าย

อุปกรณ์เครือข่ายที่เป็นเอเจนต์อาจเป็นพีซี โมเด็ม ฮับ สวิตซ์ หรือเราเตอร์ อุปกรณ์เหล่านี้อาจมีส่วนทำงานที่เป็นซอฟต์แวร์และฮาร์ดแวร์และมีเอสเอ็นเอ็มพีเอเจนต์เชื่อมต่ออ เอเจนต์จะนำข้อมูลจากส่วนซอฟ์ตแวร์หรือฮาร์ดแวร์เมื่อเอ็นเอ็มเอสร้องขอข้อมูล และปรับเปลี่ยนการทำงานของซอฟ์ตแวร์หรือฮาร์ดแวร์เมื่อเอ็นเอ็มเอสสั่งงาน โดยมีการแจ้งยืนยันสิทธิในรูปรหัสผ่านว่าเอ็นเอ็มเอสมีอำนาจหน้าที่ในการร้องขอและปรับค่า



รูปที่ 4-2 เอสเอ็นเอ็มพีเอเจนต์

4.2.1 เอ็มไอบี

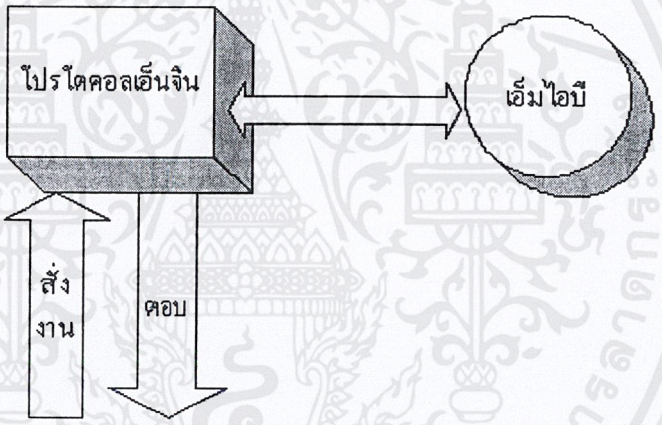
เอเจนต์ประกอบด้วยส่วนสำคัญสองส่วนคือ โพรโตคอลเอ็นจิน และฐานข้อมูลสารสนเทศการจัดการ โพรโตคอลเอ็นจินทำหน้าที่ประมวลคำสั่งที่มาจากเอ็นเอ็มเอสซึ่งได้แก่ รับคำสั่ง ถอดรหัสคำสั่ง ทำงานตามคำสั่งและส่งผลตอบกลับ ฐานสารสนเทศการจัดการหรือเรียกสั้นๆว่า เอ็มไอบี เป็นส่วนที่เก็บตัวแปรและค่ากำหนดการทำงานประจำอุปกรณ์

4.2.2 อ็อบเจ็กไอเด็นติไฟเออร์

ภายในเอ็มไอบีประกอบด้วยตัวแปรจำนวนมากที่เรียกโดยทั่วไปว่า อ็อบเจ็กจัดการ อ็อบเจ็กในความหมายนี้เป็นชื่อที่เรียกตัวแปรและลักษณะเฉพาะของตัวแปรในเอ็มไอบีโดยไม่เกี่ยวข้องกับเรื่อง เชิงวัตถุพิสัยแต่อย่างใด ขอให้พิจารณาว่าอ็อบเจ็กในเอสเอ็นเอ็มพีมีลักษณะเช่นเดียวกับคอร์ดในฐานข้อมูล

แต่ละอ็อบเจ็กจะมีชื่อเฉพาะเรียกว่า อ็อบเจ็กไอเด็นติไฟเออร์ หรือเรียกโดยย่อว่า ไอเด็นติไฟเออร์ เพื่อใช้อ้างอิงถึงอ็อบเจ็กนั้น

อ็อบเจ็กทุกตัวมีนิยามที่กำหนด ชื่อ แบบข้อมูล สิทธิ์การเข้าถึง คำอธิบายลักษณะและค่าข้อมูลการนิยามอ็อบเจ็กมีกฎเกณฑ์ตามข้อกำหนด โครงสร้างฐานข้อมูลสารสนเทศการจัดการ



รูปที่ 4-3 โครงสร้างของเอเจนต์

4.3 โพรโตคอล

การติดต่อระหว่างสถานีจัดการกับเอเจนต์มีรูปแบบในการติดต่อหลายรูปแบบด้วยกันตามวัตถุประสงค์ในการติดต่อ แบบของการติดต่อในเอสเอ็นเอ็มพีรุ่น 1 มี 5 แบบคือ

1. get-request ใช้สอบถามข้อมูลจากตัวเอเจนต์ที่อยู่บนอุปกรณ์ที่ต้องการตรวจสอบในระบบเครือข่าย
2. get-next-request ใช้สอบถามข้อมูลที่เรียงเป็นลำดับ เช่นข้อมูลที่เก็บอยู่ในรูปตาราง หรือในกรณีที่ไม่ทราบชื่อตัวแปรที่แน่ชัด
3. get-response เอเจนต์ส่งคำตอบกลับมายังผู้สอบถาม
4. set-request ใช้เปลี่ยนแปลงค่าตัวแปรที่เอเจนต์รับผิดชอบอยู่

5. trap ใช้แจ้งเหตุการณ์ที่เกิดขึ้นในระบบเครือข่าย เช่นการเริ่มต้นทำงานใหม่ของอุปกรณ์หรือเส้นทางขัดข้อง

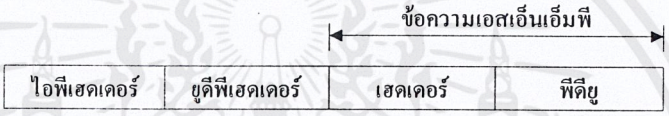
เอสเอ็นเอ็มพีอาศัยโพรโตคอลยูดีพี โดยใช้พอร์ตหมายเลข 161 สำหรับการติดต่อในแบบที่ 1 ถึง 4 และใช้พอร์ตหมายเลข 162 สำหรับแบบที่ 5

4.3.1 การเอ็นแคปซูเลต

การเอ็นแคปซูเลตคำสั่งและข้อมูลในเอสเอ็นเอ็มพีมีวิธีตามรูปที่ ----- ฟอร์แมตของเอสเอ็นเอ็มพีประกอบด้วย 2 ส่วนคือ เฮดเดอร์และพีดียู เฮดเดอร์ประกอบด้วยฟิลด์ย่อยสองฟิลด์คือ

- Version รุ่นของโพรโตคอลที่ใช้ ถ้าเป็นโพรโตคอลรุ่น 1 จะมีค่า 0 หากเป็นรุ่น 2 จะมีค่า 1

- Community รหัสผ่านในรูปสายอักขระเพื่อให้เอเจนต์ใช้ตรวจสอบว่าข้อความที่ส่งมามีสิทธิ์ในการสอบถามหรือเปลี่ยนแปลงข้อมูลหรือไม่

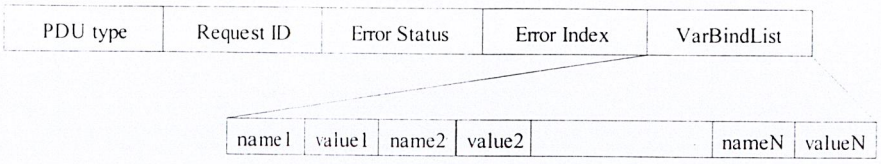


รูปที่ 4-4 การเอ็นแคปซูเลตเอสเอ็นเอ็มพี

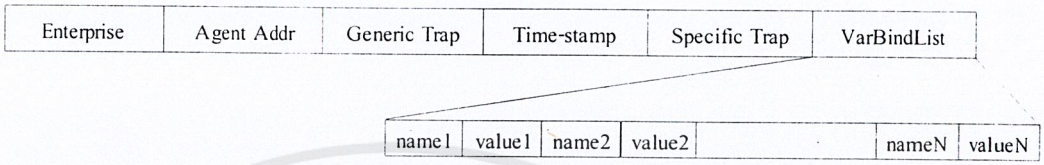
ในส่วนของพีดียูประกอบด้วยฟิลด์ย่อยตามชนิดของข้อความ หากเป็นข้อความ get, get-next และ get-response จะมีโครงสร้างเดียวกัน รูปที่---------- แสดงโครงสร้างของพีดียูโดยแต่ละฟิลด์มีความหมายดังนี้

- PDU type แบบการติดต่อ (1 ถึง 5)
- Request ID กำหนดบอกหมายเลขข้อความเพื่อใช้จับคู่เมื่อรับคำตอบกลับมา
- Error Status สถานะความผิดพลาดที่เกิดขึ้น
- Error Index ดรรชนีชี้ค่าผิดพลาดที่เกิดขึ้นเกิดจากตัวแปรตัวลำดับที่เท่าไหร่ของตัวแปรทั้งหมดที่สอบถามไป
- VarBindList ค่าผูกพันตัวแปร(variable binding) แสดงอยู่ในรูปของตัวแปรและค่าของตัวแปรต่อเนื่องกันไปเป็นรายการ

สำหรับข้อความแทร็บมีลักษณะแตกต่างกันออกไปดังรูปที่ -------- โปรดสังเกตว่าในที่นี้ไม่ได้กล่าวขนาดความยาวของแต่ละฟิลด์ เพราะทุกฟิลด์ในเอสเอ็นเอ็มพีต้องเข้ารหัสและจะได้ขนาดของแต่ละฟิลด์ที่มีความยาวแตกต่างกันไปตามชนิดข้อมูล



รูปที่ 4-5 โครงสร้างพีดียูของ get, get-next และ get-response



รูปที่ 4-6 โครงสร้างพีดียูของคำสั่ง trap

4.3.2 รหัสผิดพลาด

เอเจนต์จะตอบคำถามพร้อมทั้งแจ้งรหัสการทำงานกลับไปยังเอ็นเอ็มเอส ตารางที่ 4-1 แสดงรหัสผิดพลาดที่ใช้ในเอสเอ็นเอ็มพี

รหัสผิดพลาด	ชื่อ	คำอธิบาย
0	noError	ไม่มีข้อผิดพลาด
1	tooBig	เอเจนต์ไม่สามารถส่งคำตอบได้ในเฟรมเดียว
2	noSuchName	ไม่มีตัวแปรที่ต้องการสอบถามอยู่ในฐานข้อมูล
3	badValue	ค่าที่กำหนดให้ตัวแปรไม่ถูกต้อง
4	readOnly	เปลี่ยนค่าตัวแปรไม่ได้เพราะอ่านค่าได้เพียงอย่างเดียว
20	genErr	มีข้อผิดพลาดอื่นๆเกิดขึ้น

ตารางที่ 4-1 รหัสผิดพลาดในเอสเอ็นเอ็มพี

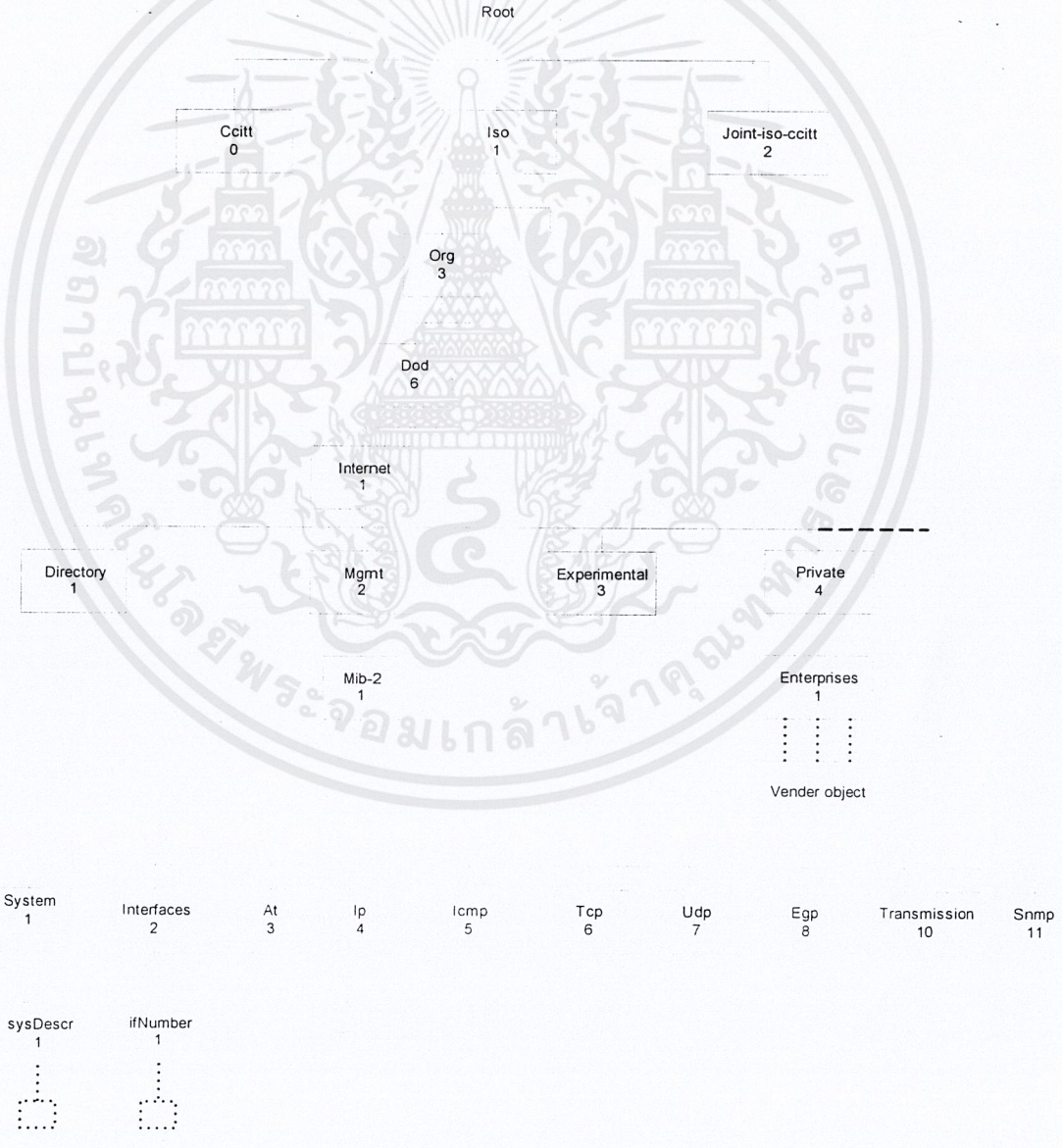
4.4 โครงสร้างเอ็มไอบี

ข้อมูลประจำอุปกรณ์เครือข่ายชิ้นหนึ่งๆมีได้อย่างหลากหลาย อีกทั้งอุปกรณ์ต่างประเภทกันย่อมมีข้อมูลประจำอุปกรณ์แตกต่างกัน ดังนั้นการสอบถาม หรือเปลี่ยนค่าฐานข้อมูลจึงต้องมีรูปแบบมาตรฐานให้กับอุปกรณ์ทุกประเภท โครงสร้างต้นไม้แบบลำดับชั้นเป็นโครงสร้างที่เหมาะสมสำหรับใช้เป็นฐานข้อมูลเพื่อจัดเก็บตัวแปรเหล่านี้

รูปนี้ แสดงข้อมูลหรืออ็อบเจ็กของเอสเอ็นเอ็มพีในโครงสร้างแบบต้นไม้ซึ่งนิยมเรียกว่า เอ็มไอบีทรี แต่ละโหนดซึ่งแทนอ็อบเจ็กหนึ่งๆมีชื่อพร้อมทั้งตัวเลขฐานสิบกำกับประจำโหนดเพื่อใช้อ้างอิง ยกเว้นรากซึ่งไม่มีชื่อกำกับ

ลำดับชั้นแรกจะมีโหนดหลักสามโหนดหลักสามโหนดซึ่งกำหนดกลุ่มองค์กรสามกลุ่มคือ ITU-T(0), ISO(1), และ Joint-ISO-ITU-T(2) ภายใต้โหนด ISO มีโหนดลำดับที่สามคือ org(3) กำหนดองค์กรนานาชาติ และส่วนหนึ่งขององค์กรนี้คือ dod(6) หรือ Department of Defense และมีโหนด internet(1) เพื่อกำหนดกลุ่มการจัดการเครือข่ายในอินเทอร์เน็ต

เมื่อต้องการอ้างอิงถึงโหนดใดในโครงสร้างให้เขียนหมายเลขจากรากไปตามเส้นทางถึงโหนดนั้นและคั่นด้วยจุด ลำดับตัวเลขนี้เรียกว่า อ็อบเจ็กไปเด็นติไฟเออร์ (object identifier) หรือ โอไอดี (OID)



รูปที่ 4-7 อ็อบเจ็กไอเด็นติไฟเออร์ในโครงสร้างฐานข้อมูลสารสนเทศ

ตัวอย่างเช่น 1.3.6.1.2.1.1 เป็นอ็อบเจ็กไอเด็นติไฟเออร์โดยมีชื่อที่สมนัยกันคือ iso.org.dod.internet.mgmt.mib-2.system โหนดที่อยู่ภายใต้ 1.3.6.1.2.1 หรือในกลุ่ม mib-2 เป็นโหนดสำหรับใช้งานเอสเอ็นเอ็มพี แต่ละโหนดจะมีโหนดย่อยเพื่ออ้างอิงถึงตัวแปรเช่น 1.3.6.1.2.1.1.1 คือตัวแปร sysDescr (System Description) ซึ่งเก็บคำอธิบายเกี่ยวกับอุปกรณ์นั้น

4.4.1 กลุ่มในเอ็มไอบี

เอ็มไอบีภายใต้ internet มีกลุ่มย่อยทั้งหมด 6 กลุ่มคือ

- directory(1) สงวนไว้สำหรับใช้งานในอนาคต
- mgmt(2) กลุ่มเอ็มไอบีที่ใช้ในการจัดการภายใต้เอสเอ็นเอ็มพีรุ่น 1
- experimental(3) ใช้สำหรับการทดลอง
- private(4) สำหรับให้ผู้ผลิตกำหนดตัวแปรเฉพาะอุปกรณ์
- security(5) ใช้ในระบบรักษาความปลอดภัย
- SNMPv2(6) ใช้ในเอสเอ็นเอ็มพีรุ่น 2

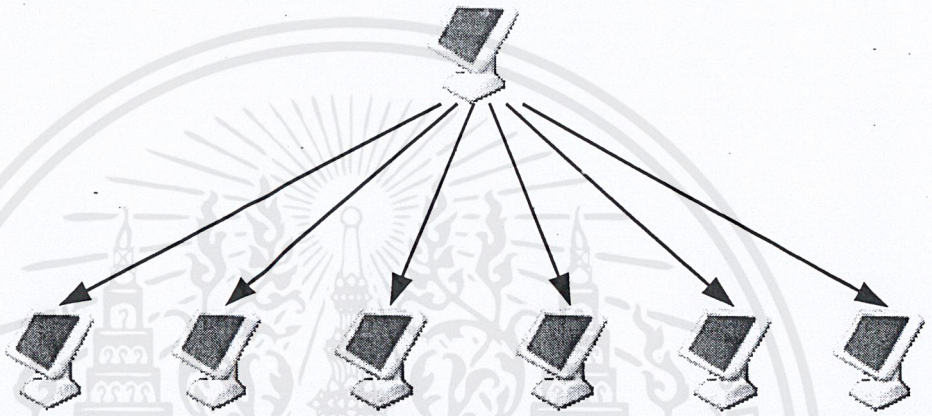
ภายให้กลุ่ม mib-2 บรรจุกลุ่มย่อยที่ใช้ในเอสเอ็นเอ็มพีซึ่งประกอบด้วย interfaces, at, ip และอื่นๆ ความหมายของแต่ละกลุ่มอธิบายไว้ในตารางที่ 22.2 แต่ละกลุ่มจะประกอบด้วยตัวแปรซึ่งมีแบบต่างๆกันไป

ลำดับ	ชื่อ	ความหมาย
1	system	ข้อมูลระบบ
2	interfaces	ข้อมูลอินเทอร์เฟสที่ใช้เชื่อมต่อ
3	at	ข้อมูลการแปลงแอดเดรส
4	ip	ข้อมูลไอพี
5	icmp	ข้อมูลไอซีเอ็มพี
6	tcp	ข้อมูลทีซีพี
7	udp	ข้อมูลยูดีพี
8	egp	ข้อมูลโพรโตคอลเกตเวย์ภายนอก
10	transmission	ข้อมูลสายสื่อสาร
11	snmp	ข้อมูลเอสเอ็นเอ็มพี

ตาราง 4-2 กลุ่มย่อยภายใต้ mgmt

บทที่ 5
การสแกนเพื่อตรวจสอบ

5.1 Network Ping Sweeps



รูปที่5-1 แสดงการทำงานของ ping sweep

หนึ่งในเทคนิคพื้นฐานที่นิยมกระทำกันก็คือ การ ping ไปยังเครื่องเป้าหมายจำนวนมากพร้อมๆ กัน ในลักษณะคล้ายกับการกวาดหรือกราดยิง ซึ่งเราเรียกว่าการทำ ping sweep เพื่อตรวจสอบว่าเครื่องปลายทางใดบ้างที่ยังเปิดทำงานอยู่ โดยปกติ ถ้าคุณใช้คำสั่ง ping ธรรมดา, ping จะมีการส่ง แพ็กเก็ต ICMP ECHO (Type 8) ออกไปยังเครื่องปลายทางและรอคอย ICMP ECHO_REPLY (Type 0) ที่ถูกส่งกลับมา ถึงแม้ ping จะมีประโยชน์สำหรับการทดสอบว่าเครื่องปลายทางเปิดอยู่หรือไม่ก็ตาม แต่มันจะเหมาะสำหรับเครื่องที่อยู่บนเน็ตเวิร์คขนาดเล็กถึงขนาดกลางเท่านั้น มันจะไม่มีประสิทธิภาพเพียงพอที่จะนำมาใช้ตรวจสอบเครื่องที่อยู่บนเน็ตเวิร์คขนาดใหญ่ได้ การตรวจสอบเครื่องที่อยู่ในเน็ตเวิร์คที่ใช้แอดเดรสในคลาส A อาจกินเวลานานหลายชั่วโมงกว่าจะทราบผล เทคนิคในการ ping sweep มีหลายเทคนิคแตกต่างกันไป เช่น ปกติแล้วการ ping จะรอคอยการตอบสนองจากเครื่องทีละเครื่อง ก่อนจะเปลี่ยนไปทดสอบเครื่องอื่นๆถัดไป มันจะใช้การส่ง แพ็กเก็ต ICMP ออกไปพร้อมๆกันแบบขนานไปยังเครื่องปลายทางหลายๆเครื่อง ในลักษณะคล้าย “Round Robin” (คือส่งแพ็กเก็ต ICMP ไปที่เครื่อง 1,2,3,.... ถึงเครื่องสุดท้าย แล้ววนกลับมาส่งแพ็กเก็ตไปที่เครื่อง 1,2,3 ใหม่ไปเรื่อยๆ แล้ววนกลับมาอีก โดยไม่จะเป็นต้องหยุดรอจากตอบสนองจากเครื่องแรก) ดังนั้น จะทำงานได้รวดเร็วกว่าคำสั่ง ping ธรรมดามาก แต่อาจทำ

ให้เกิดทราฟฟิกจำนวนมากที่เกิดขึ้นอาจเข้าไปรบกวนแบนด์วิธของ WAN Link ความเร็วอย่างต่ำเช่น 128K ISDN หรือ เฟรมรีเลย์ (Frame relay)

แต่ในบางครั้งจะทำอย่างไรถ้าที่เน็ตเวิร์คเป้าหมายได้มีการบล็อกห้ามแพ็กเก็ต ICMP ไว้ไม่ให้เข้าถึงเน็ตเวิร์คภายในได้

ถ้าแพ็กเก็ต ICMP ถูกบล็อกเอาไว้ เรามีเทคนิคและเครื่องมืออื่นที่ใช้ตรวจสอบได้ว่าเครื่องปลายทางใดบ้างที่เข้าถึงได้และเปิดทำงานอยู่ แต่อย่างไรก็ตาม มันอาจไม่ถูกต้องและรวดเร็วเท่ากับตรวจสอบด้วย ping sweep

เทคนิคที่ว่านั้นก็คือ การสแกนพอร์ต นั่นเอง ซึ่งเป็นเทคนิคแรกที่ใช้ถ้าไซต์ปลายทางบล็อกแพ็กเก็ต ICMP ไว้ โดยการสแกนพอร์ตทั่วๆไปบนแต่ละเครื่องเราจะสามารถคาดการณ์ได้ว่าเครื่องไหนเปิดอยู่บ้าง เทคนิคนี้ค่อนข้างกินเวลาและอาจไม่สามารถสรุปแน่ชัดได้ TCP Ping Scan ด้วย TCP Ping scan ไปที่พอร์ตที่ต้องการส่วนมากจะเป็นพอร์ต 80 เนื่องจากเป็นพอร์ตมาตรฐานที่เราท์เตอร์หรือไฟร์วอลล์ของไซต์ส่วนใหญ่จะเปิดไว้ให้ผ่านเข้าไปได้ยังเว็บเซิร์ฟเวอร์ที่มักตั้งอยู่ในส่วนที่เรียกว่า Demilitarized zone (DMZ) หรือยิ่งไปกว่านั้น อาจทะลุผ่านเข้าไปในอินทราเน็ตภายในด้วย โดยจะทำงานดังนี้คือสร้างแพ็กเก็ตของโพรโตคอล TCP ซึ่งได้เซตแฟลก ACK (Acknowledge) ไว้เป็น 1 ด้วย (ต่อไปเราจะเรียกแพ็กเก็ตลักษณะนี้สั้นๆว่า แพ็กเก็ต TCP ACK) แล้วส่งแพ็กเก็ตเหล่านี้ไปยังเน็ตเวิร์คเป้าหมายปลายทางหรือไม่ ถ้ามีก็แสดงว่าเครื่องปลายทางสามารถติดต่อได้และเปิดทำงานอยู่ แพ็กเก็ต TCP ACK นี้มักวิ่งทะลุผ่านไฟร์วอลล์ที่ไม่ค่อยฉลาดนักหรือคอนฟิกไว้ไม่ดีพอให้เข้าไปได้

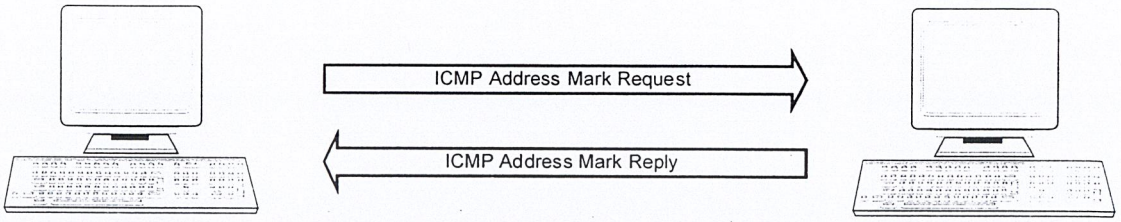
อย่างที่ได้เห็นไปแล้วว่าเทคนิคนี้ค่อนข้างใช้ได้ผลถึงแม้ไซต์ปลายทางจะบล็อกแพ็กเก็ต ICMP ไว้ ซึ่งถ้า พอร์ต 80 ใช้ไม่ได้อาจใช้เป็นพอร์ตมาตรฐานที่มักพบบ่อย อย่างเช่น พอร์ตของเซอร์วิส SMTP (หมายเลข 25), POP (110), AUTH (113), IMAP (143) หรือพอร์ตอื่นๆ ที่เป็นไปได้

ถ้าพอร์ตที่เครื่องปลายทางได้เปิดไว้แพ็กเก็ตของโพรโตคอล TCP ที่มีการเซตแฟลก SYN(S bit) ไว้และแพ็กเก็ต TCP ที่มีการเซตแฟลก ACK ไว้จะถูกส่งกลับมา

นอกจากนี้ยังมีเทคนิคอื่นในการที่จะตรวจสอบว่าเครื่องปลายทางยังเปิดทำงานอยู่หรือไม่ด้วย การส่งแพ็กเก็ต ICMP ECHO ออกไป พร้อมทั้งแพ็กเก็ตของโปรโคคอล ICMP ใน Type อื่นๆด้วย ได้แก่ ICMP Type TIME STAMP REQUEST และ ICMP INFO request เพื่อที่ว่า ถึงแม้แพ็กเก็ต ICMP ใน Type ECHO ถูกสกัดกั้นไว้ที่เราท์เตอร์ตัวที่เชื่อมต่อออกอินเทอร์เน็ตหรือที่ไฟร์วอลล์ก็ตาม แต่โอกาสที่แพ็กเก็ต ICMP ใน Type อื่นๆจะวิ่งทะลผ่านเข้าไปเพื่อตรวจสอบได้ก็ยังมีอยู่ หรืออาจจะส่งไปด้วยแพ็กเก็ตปลอม (spoofed packet) เพื่อป้องกันการตรวจสอบย้อนกลับไปว่าแพ็กเก็ตถูกส่งมาจากที่ไหน

กล่าวโดยสรุป ขั้นตอนนี้จะทำให้เราสามารถตรวจสอบได้อย่างแท้จริงว่าเครื่องปลายทางใดบ้างที่เราสามารถติดต่อได้โดยตรงผ่านอินเตอร์เน็ต ด้วยการส่งแพ็กเก็ต ICMP ใน TYPE ต่างๆ หรือใช้เทคนิคของการสแกนพอร์ตเข้าไปตรวจสอบ จากลิสต์รายการหมายเลข IP Address ที่อยู่ในคลาส C จำนวนกว่า 200 หมายเลข เราสามารถตรวจสอบได้ว่าแท้จริงแล้วมีเครื่องไหนบ้างที่อยู่ในขอบข่ายของการเป็นเครื่องเป้าหมายได้ เพื่อช่วยลดโฟกัสขอบเขตของการตรวจสอบให้แคบลงและประหยัดเวลามากขึ้น

5.2 ICMP Queries



รูปที่ 5-2 แสดงการทำงานของ ICMP QUERY

คือการส่งแพ็กเก็ตของโพรโตคอล ICMP ไปสอบถาม ตัวอย่างเช่น สอบถามเวลาของเครื่องปลายทาง (เพื่อดูว่าเครื่องๆนั้นอยู่ในโซนเวลา (time zone) แถบใด) ด้วยการส่งแพ็กเก็ต ICMP type TIMESTAMP, สอบถามค่าของ Subnet Mask ของเครื่องปลายทางด้วยการส่งแพ็กเก็ต ICMP type ADDRESS MASK REQUEST Subnet Mask เป็นค่าที่สำคัญพอสมควรเพราะมันจะทำให้คุณทราบหมายเลข Subnet Address ของเครื่องเน็ตเวิร์คเป้าหมาย การทราบค่าของ Subnet Address จะช่วยให้เราสามารถโฟกัสไปที่เน็ตเวิร์คที่ต้องการได้และหลีกเลี่ยงการส่งข้อมูลโดยระบุแอดเดรสปลายทางเป็น Broadcast Address

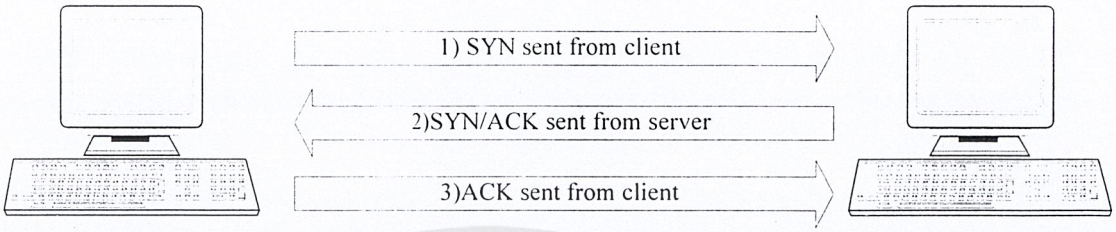
5.3 Port Scanning

การสแกนพอร์ตหรือ Port Scanning เป็นกระบวนการในการคอนเน็กเข้าไปที่ TCP Port หรือ UDP Port ของเครื่องปลายทางเพื่อค้นหาว่ามีเซอร์วิสอะไรบ้างที่ทำงานอยู่หรืออยู่ในสถานะ LISTENING

การค้นหาพอร์ตที่เปิดอยู่เป็นเรื่องสำคัญทีเดียวในการตรวจสอบประเภทของระบบปฏิบัติการและแอปพลิเคชันที่ใช้งานอยู่ในระบบ เพราะ ระบบปฏิบัติการหรือเซอร์วิสที่รันอยู่อาจมีข้อบกพร่องบางอย่างที่อนุญาตให้ผู้ใช้ที่ไม่ได้ผ่านการตรวจสอบเข้าไปในระบบได้ หรือมีข้อบกพร่องเกี่ยวกับระบบการรักษาความปลอดภัยที่เป็นที่รู้กันดี โดยเฉพาะเซอร์วิสบางเวอร์ชันที่ยังไม่สมบูรณ์ เครื่องมือและเทคนิคในการสแกนพอร์ตได้รับการพัฒนาอย่างต่อเนื่องมาหลายปี เทคนิคการสแกนพอร์ตที่เรากล่าวไปข้างต้นนั้นเป็นเพียงการสแกนพอร์ตเพื่อรู้ว่าเครื่องปลายทางเปิดอยู่และติดต่อผ่านทางอินเตอร์เน็ตหรือเครือข่ายได้หรือไม่ เท่านั้น แต่สำหรับเทคนิคการสแกนพอร์ตที่จะกล่าวถึงถัดนี้ไป เป็นการสแกนพอร์ตเพื่อค้นหาว่ามีพอร์ตหมายเลขใดเปิดอยู่ที่เครื่องปลายทางนั้นบ้าง

- TCP connect scan เป็นการคอนเน็กไปที่พอร์ตที่ต้องการบนเครื่องปลายทาง แล้วขอเปิด
- คอนเน็กชันของโพรโตคอล TCP ด้วยกลไกมาตรฐานที่เรียกว่า TCP three-way handshake

(SYN, SYN/ACK และ ACK) แต่วิธีนี้มักถูกตรวจจับได้โดยง่ายโดยไฟร์วอลล์ที่ไซต์ปลายทาง



รูปที่ 5-3 TCP 's 3-way handshake

รูปแสดงการเปิดคอนเน็กชันของโพรโตคอล TCP จะอาศัยกลไก three way handshake โดยขั้นแรกจะส่งแพ็กเก็ต TCP ที่เซตแฟลก SYN เป็น 1 ไว้ออกไปที่เครื่องปลายทาง ขั้นที่สอง เครื่องต้นทางจะได้รับ TCP SYN/ACK กลับมาและขั้นสุดท้าย จะส่งแพ็กเก็ต TCP ACK กลับไปอีกครั้งเพื่อยืนยันว่าได้รับแพ็กเก็ตในขั้นที่สองแล้ว

- TCP SYN scan เทคนิคนี้บางครั้งเรียกว่า half-open scanning สาเหตุเพราะว่า คอนเน็กชันที่สมบูรณ์ของโพรโตคอล TCP ยังไม่ได้ถูกเปิดขึ้น เพราะเมื่อแพ็กเก็ต TCP ที่เซตค่าแฟลก SYN และ ACK ไว้เป็น 1 (TCP SYN/ACK) นั่นก็เพียงพอแล้วที่จะสรุปว่า พอร์ตดังกล่าวอยู่ในสถานะ LISTENING แต่ถ้าพอร์ตดังกล่าวไม่ได้เปิดอยู่ แพ็กเก็ต TCP ที่เซตค่าแฟลก RST และ ACK ไว้เป็น 1 (TCP RST/ACK) จะถูกส่งกลับมาแทน เทคนิคค่อนข้างน่าใช้กว่าเทคนิคแรกเพราะส่วนใหญ่แล้วไฟร์วอลล์ที่ไซต์ปลายทางมักตรวจจับได้ค่อนข้างยาก
- TCP FIN scan เทคนิคนี้จะส่งแพ็กเก็ต TCP ที่เซตค่าแฟลก FIN เป็น 1 (TCP FIN) ไปยังพอร์ตที่ต้องการ ถ้าไดร์เวอร์ของโพรโตคอล TCP/IP ที่เครื่องปลายทางได้ถูกพัฒนาขึ้นมาโดยมีฟีเจอร์ตามในมาตรฐาน RFC หมายเลข 739 ครบถ้วน (http://www.ietf.org/rfc/rfc0793.txt) เครื่องปลายทางจะส่งแพ็กเก็ต TCP RST ของทุกๆพอร์ตที่ปิดอยู่กลับมาให้ (กล่าวง่ายๆก็คือ เราจะทราบหมายเลขพอร์ตที่ไม่ได้เปิดให้บริการ) โดยปกติแล้ว เทคนิคนี้มักใช้ได้กับเครื่องปลายทางที่รันยูนิกซ์
- TCP Xmas Tree scan เทคนิคนี้จะส่งแพ็กเก็ต TCP ที่เซตแฟลก FIN ,URG และ PUSH ไปยังพอร์ตเป้าหมายที่เครื่องปลายทาง และอาศัยมาตรฐาน RFC 739 อีกเช่นกัน เครื่องปลายทางจะส่งแพ็กเก็ต TCP RST ของทุกพอร์ตที่ปิดอยู่กลับมาให้

- TCP Null scan เทคนิคนี้จะส่งแพ็กเก็ต TCP ออกไปโดยเซตค่าของทุกๆแฟลกให้เป็น 0 หมด และ อาศัยมาตรฐาน RFC 793 อีกเช่นกัน เครื่องปลายทางจะส่งแพ็กเก็ต TCP RST ของทุกๆพอร์ตที่ปิดอยู่กลับมาให้
- TCP ACK scan เทคนิคนี้จะถูกใช้เพื่อค้นหา "rule" และ "policy" ต่างๆที่เซตไว้ที่ไฟร์วอลล์ เพื่อตรวจสอบดูว่าไฟร์วอลล์นั้นๆทำหน้าที่แค่เพียงกรองแพ็กเก็ตอย่างง่ายๆ หรือเป็นไฟร์วอลล์ที่มีความฉลาดพอสมควรและใช้เทคนิคการกรองแพ็กเก็ตขั้นสูง
- TCP Window scan เทคนิคนี้จะตรวจสอบพอร์ตที่เปิดอยู่ รวมทั้งตรวจดูว่า พอร์ตใดบ้างที่ถูกฟิลเตอร์เอาไว้ไม่ให้ผ่านเข้าไปถึง และพอร์ตหมายเลขใดได้รับการอนุญาตไว้บ้าง โดยอาศัยช่องโหว่จากความผิดปกติบางอย่างในการแจ้งค่าของ TCP Window Size ของโพรโตคอล TCP/IP
- TCP RPC scan เทคนิคนี้ใช้งานได้เฉพาะกับเครื่องปลายทางที่รันยูนิกซ์เท่านั้น มันถูกใช้เพื่อตรวจสอบดูว่ามีเซอร์วิสใดทำงานอยู่บนเซอร์วิส RPC บ้าง รวมทั้งตรวจดูเวอร์ชันของเซอร์วิสนั้นและโปรแกรมอื่นที่เกี่ยวข้อง
- UDP scan เทคนิคนี้จะส่งแพ็กเก็ตของโพรโตคอล UDP ไปยังพอร์ตเป้าหมาย ถ้าเครื่องปลายทางตอบกลับมาด้วยแพ็กเก็ต ICMP type PORT UNREACHABLE นั่นหมายความว่าพอร์ตนั้นปิดอยู่ในทางตรงกันข้าม ถ้าเราไม่ได้รับแพ็กเก็ต ICMP type ดังกล่าว เราสามารถสรุปได้ว่าพอร์ตนั้นเปิดอยู่ เนื่องจากโพรโตคอล UDP เป็นโพรโตคอลลักษณะ connectionless คือไม่รับรองว่าแพ็กเก็ตที่ส่งไปจะถึงเครื่องปลายทางครบถ้วนหรือไม่ ดังนั้นความถูกต้องของผลลัพธ์ที่ได้จากเทคนิคนี้ก็อาจขึ้นกับปัจจัยอื่นๆ ด้วยเช่น ปริมาณทราฟฟิกในเน็ตเวิร์คและทรัพยากรบนเครื่องปลายทาง นอกจากนั้นมันยังเป็นเทคนิคที่ค่อนข้างช้าอีกด้วยถ้าคุณกำลังสแกนเน็คเวิร์กที่ใช้งานไฟร์วอลล์หรือเราท์เตอร์ที่มีการฟิลเตอร์กรองแพ็กเก็ต จึงขอให้เตรียมใจไว้ด้วยกับผลลัพธ์ที่ไม่คาดคิดของ UDP scan

ไดร์เวอร์ของโพรโตคอล TCP/IP ของระบบปฏิบัติการบางตัวอาจส่งแพ็กเก็ต TCP RST กลับไปยังเครื่องต้นทางตลอกไม่ว่าพอร์ตๆ นั้นจะเปิดหรือปิดอยู่ ดังนั้นจึงเป็นไปได้ว่า ผลลัพธ์ที่ได้อาจแตกต่างกันไปไม่แน่นอน แต่อย่างไรก็ดี การตรวจสอบด้วยแพ็กเก็ต TCP SYN ธรรมดานั้นจะทำงานได้ดีสำหรับทุกๆ โฮสต์

5.4 การตรวจหาประเภทของระบบปฏิบัติการ

จุดประสงค์ประการแรกของการสแกนคือ การค้นหา TCP port และ UDP port ที่เปิดอยู่บนเครื่องปลายทาง ส่วนจุดประสงค์ประการที่สองคือ การค้นหาประเภทของระบบปฏิบัติการที่รันอยู่บนเครื่องหมายปลายทาง ประเภทของระบบปฏิบัติการที่เราทราบจะถูกนำไปใช้ประโยชน์ในขั้นตอนการค้นหารายละเอียดต่างๆ (enumeration) โดยอาศัยข้อบกพร่องต่างๆ ที่แต่ละระบบปฏิบัติการนั้นมี ดังนั้นเราจึงต้องมั่นใจว่า ระบบปฏิบัติการที่เราทราบนั้นเป็นข้อมูลที่ถูกต้อง

Active Stack Fingerprinting

Stack fingerprinting เป็นเทคโนโลยีที่ช่วยทำให้มั่นใจได้ว่าประเภทของระบบปฏิบัติการที่ค้นหาได้นั้นเป็นระบบปฏิบัติการที่ถูกต้อง มีเปอร์เซ็นต์ความน่าเชื่อถือสูง โดยอาศัยหลักการที่ว่า ผู้ผลิตระบบปฏิบัติการแต่ละรายมักพัฒนาไดรเวอร์ของโพรโตคอล TCP/IP และเซอร์วิสที่ทำงานบนโพรโตคอล TCP/IP ให้มีเอกลักษณ์เฉพาะตัวเป็นของตัวเอง ซึ่งมักแตกต่างกับของระบบปฏิบัติการอื่น

ดังนั้น โดยการตรวจวัดความแตกต่างเหล่านี้ เราจะสามารถเริ่มคาดเดาได้อย่างมีเหตุผล แต่เพื่อให้มีความน่าเชื่อถือสูงสุด Stack fingerprinting จำเป็นต้องอาศัยการคอนเน็กไปพอร์ตที่เปิดอยู่อย่างน้อยนึ่งพอร์ต แต่ การทำงานของโครงงานนี้ สามารถคาดเดาได้อย่างมีเหตุผล ถึงแม้ว่าจะไม่ได้คอนเน็กไปที่พอร์ตใดเลย แต่ผลที่ได้ก็อาจยังไม่น่าเชื่อถือนัก โดยให้สำรวจวิธีการตรวจวัดความแตกต่างกันทีละวิธี

- Fin probe ใช้การส่งแพ็กเก็ตของโพรโตคอล TCP โดยเซตแฟลก Fin ให้เป็น 1 ไว้ ตามมาตรฐาน RFC 793 ระบุไว้ว่า พฤติกรรมที่ถูกต้องจะต้องไม่มีการส่งแพ็กเก็ตอะไรตอบสนองกลับไป แต่ทว่า ไดรเวอร์ของโพรโตคอล TCP/IP ในระบบปฏิบัติการบางตัว อย่างเช่น วินโดว์เอ็นที จะตอบสนองกลับมาด้วยแพ็กเก็ตของโพรโตคอล TCP ที่เซตแฟลก Fin และ ACK ให้เป็น 1 ซึ่งเครื่องมือส่วนมากได้นำเทคนิคนี้ไปใช้กัน
- Bogus Flag probe ใช้การส่งแพ็กเก็ตของโพรโตคอล TCP โดยเซตแฟลก SYN ให้เป็น 1 พร้อมทั้งเซตบิตตำแหน่งที่ยังไม่ได้ใช้งานให้เป็น 1 ด้วย บางระบบปฏิบัติการเช่น ลีนุกซ์ จะตอบสนองกลับมาด้วยการเซตแฟลกบางตัวในแพ็กเก็ต ว่ามักเป็นค่าอะไร อย่างไรก็ตามบางระบบปฏิบัติการจะทำการ reset connection เมื่อได้รับแพ็กเก็ตนี้
- TCP Initial Sequence Number (ISN) sampling ใช้วิธีการตรวจหาแพทเทิร์นของ Sequence number ที่อยู่ในส่วนหัวของแพ็ตเก็ตที่ได้รับการตอบสนองต่อการร้องขอการเชื่อมต่อ ว่าเป็นค่าอะไร ซึ่งสามารถแบ่งได้หลายกลุ่มเช่น ถ้าเป็นแบบ traditional 64K จะพบใน UNIX รุ่นเก่า, แบบ Random increments จะพบใน Solaris, IRIX, FreeBSD, Digital UNIX, Cray ในเวอร์ชันใหม่, แบบ True "random" จะพบใน Linux 2.0.*, OpenVMS, AIX เวอร์ชันใหม่, ส่วน Windows จะเป็นแบบ "time dependent" model คือค่าของ ISN จะเพิ่มขึ้นจำนวนหนึ่งที่กำหนดไว้ในแต่ละช่วงเวลา, และในบางครั้งจะใช้ค่า ISN ค่าเดียวไม่เปลี่ยนเลย เช่นใน 3Com hubs จะใช้เป็น 0x803 ตลอดและใน Apple LaserWriter printers จะใช้เป็น 0xC7001
- "Don't fragment bit" monitoring บางระบบปฏิบัติการได้เซตบิต "Don't fragment bit" ไว้เพื่อเพิ่มความเร็วในการส่งข้อมูล ให้มอนิเตอร์บิตนี้เพื่อตรวจดูว่าระบบปฏิบัติการไหนเซตบิตนี้บ้าง
- TCP initial window size ใช้วิธีดูขนาดของ TCP window เพราะบางระบบปฏิบัติการจะมีการล็อคค่าไว้เลยว่าขนาดของ TCP window เป็นเท่าไหร่ (เช่น AIX เป็นเพียงระบบปฏิบัติการเดียวที่มีขนาดของ window เท่ากับ 0x3F25 ส่วน window NT มีขนาด 0x402E) ค่านี้มักเป็นค่าเฉพาะตัวของแต่ละระบบปฏิบัติการด้วย จึงยิ่งทำให้ผลที่ได้มีความถูกต้องมากขึ้น

- ACK value ระบบปฏิบัติการแต่ละระบบมักเซตค่าในฟิลด์ ACK ไม่เหมือนกัน บางระบบเซตค่าฟิลด์ ACK ให้สอดคล้องตามค่าของฟิลด์ SYN ที่เซตไว้ในฝั่งผู้ส่ง บางระบบจะเซตค่าฟิลด์ ACK ให้บวกจากค่าของฟิลด์ SYN ไปอีกหนึ่ง
- ICMP error message quenching บางระบบปฏิบัติการอาจปฏิบัติตามมาตรฐาน RFC 1812 และมีการจำกัดอัตราการส่งข้อความแจ้งข้อผิดพลาดดังนั้น (ใน Linux kernel จะจำกัดการส่งข้อความแจ้งข้อผิดพลาดไปยังปลายทางที่อัตรา 80 แพ็กเก็ตต่อ 4±0.25 วินาที) โดยการส่งแพ็กเก็ตของโพรโตคอล UDP ไปยังหมายเลขพอร์ตสูงๆ แล้วค่อยนับจำนวนของ ICMP type PORT UNREACHABLE Message ที่ตอบกลับมาภายในช่วงเวลาที่กำหนด
- ICMP message quoting เมื่อพบข้อผิดพลาดเกี่ยวกับโพรโตคอล TCP/IP ระบบปฏิบัติการแต่ละประเภทจะให้ข้อมูลและสาเหตุต่างๆมาในแพ็กเก็ตของ ICMP ไม่เท่ากัน บางระบบจะให้รายละเอียดมากบางระบบจะให้รายละเอียดน้อย (ใน Solaris จะส่งกลับมา a bit more และใน Linux จะส่งกลับมา even more than that) ดังนั้นโดยการสำรวจข้อมูลที่ได้มานี้ เราพอจะใช้ในการคาดเดาประเภทของระบบปฏิบัติการได้
- ICMP error message-echoing integrity บางระบบปฏิบัติการอาจดัดแปลงส่วนหัวของแพ็กเก็ต IP เมื่อมีการส่ง ICMP error message ด้วยการตรวจสอบลักษณะของการดัดแปลงดังกล่าวนี้คุณสามารถนำมันมาใช้ในการคาดเดาได้
- Type of service (TOS) ให้คุณสำรวจฟิลด์ที่ชื่อ Type of service ที่อยู่ในแพ็กเก็ต ICMP ประเภท port unreachable ซึ่งโดยปกติหลายๆระบบปฏิบัติการจะใช้ค่าศูนย์ แต่บางระบบอาจใช้ค่าอื่น เช่น Linux ใช้ 0xC0
- Fragmentation handling แต่ละระบบปฏิบัติการจะจัดการกับแพ็กเก็ตที่ถูกแฟรกเมนต์หรือหั่นซอยไม่เหมือนกัน เมื่อมีการประกอบแพ็กเก็ตย่อยขึ้นมาเป็นแพ็กเก็ตที่สมบูรณ์ บางระบบจะเขียนทับ

  แพ็กเก็ตย่อยอันเก่าด้วยแพ็กเก็ตย่อยอันใหม่หรือบางระบบก็ทำในทางตรงกันข้าม โดยการสังเกตพฤติกรรมตรงนี้ เราพอจะใช้ในการคาดเดาประเภทของระบบปฏิบัติการได้เช่นเดียวกัน สามารถหาข้อมูลเพิ่มเติมได้ที่ www.secnet.com
- TCP options ได้ถูกกำหนดไว้ในมาตรฐาน RFC 793 และได้รับการปรับปรุงในมาตรฐาน RFC 1323 ในปัจจุบัน ผู้ผลิตหลายรายได้มีการอิมพลีเมนต์ออปชั่นพิเศษที่อยู่ใน RFC 1323 ไว้ในระบบปฏิบัติการของตน ดังนั้น ด้วยการส่งแพ็กเก็ตที่เซตออปชั่นหลายๆออปชั่นไปทดสอบ อย่างเช่น no operation, maximum segment size, window scale factor และ timestampsมันเป็นไปได้ที่เราจะตั้งสมมติฐานเกี่ยวกับระบบปฏิบัติการที่รันที่เครื่องเป้าหมาย

ยกตัวอย่าง

Window Scale=10; NOP; Max Segment Size = 265; Timestamp; End of Ops;

บางระบบปฏิบัติการ เช่น FreeBSD จะ support ทุกออปชั่นข้างต้นขณะที่ Linux 2.0.X จะ support บางออปชั่น Linux 2.1.x support ทุกออปชั่น

แม้ว่าหลายระบบปฏิบัติการจะ support ออปชั่นเดียวกันแต่บางทีเราก็สามารถแยกแยะได้โดยจากออปชั่น the_values_of เช่น ถ้าส่งค่า MSS เล็กๆไปที่ Linux โดยทั่วไปแล้วมันจะส่ง MSS echo กลับไป ส่วนระบบปฏิบัติการอื่นจะส่งค่าที่แตกต่างกันกลับไป แต่ถ้ายังได้ผลลัพธ์เหมือนกันอีกก็สังเกตลำดับของออปชั่นที่ได้รับมา เช่น Solaris จะเป็น 'NNTNWME' ซึ่งหมายความว่า <no op><no op><timestamp><no op><window scale><echoed MSS> ขณะที่ Linux 2.1.122 จะเป็น MENNTNW ซึ่งจะเห็นได้ว่าเป็นออปชั่นเดียวกัน ส่ง MSS echo เหมือนกัน แต่ลำดับที่ส่งมาไม่เหมือนกัน

- SYN Flood Resistance บางระบบปฏิบัติการจะไม่ยอมรับการ connection ครั้งใหม่ ถ้ามีการส่งแพ็กเก็ต SYN ไปมากเกิน ซึ่งหลายระบบปฏิบัติการนั้นสามารถที่จะจัดการกับแพ็กเก็ตที่ส่งเข้ามาได้ไม่เกินครั้งละ 8 แพ็กเก็ต แต่ใน kernelของ Linux รุ่นใหม่มีวิธีในการป้องกันปัญหานี้เช่น การใช้ SYN cookies ดังนั้นเราก็สามารถรู้ได้ว่าเป็นระบบปฏิบัติการอะไรโดยการส่งแพ็กเก็ตไป 8 แพ็กเก็ตไปยังพอร์ตที่เปิดอยู่แล้วดูว่าสามารถ connect ไปยังพอร์ตนั้นได้หรือไม่

5.4 ตัวอย่างเครื่องมือที่ใช้ในการสำรวจระบบเครือข่าย

Pinger จากบริษัท Rhino9 โปรแกรมตัวนี้ทำงานโดยจะส่งแพ็กเก็ต ICMP ECHO ออกไปพร้อมๆกันแบบขนานในลักษณะของ Round robin และรอคอยการตอบสนอง นอกจากนั้น Pinger ยังอนุญาตให้คุณค้นหาชื่อโฮสต์และบันทึกผลลัพธ์ที่ได้ลงในไฟล์ด้วย ส่วนเครื่องมือที่เป็นผลิตภัณฑ์ทางการค้าอีกตัวหนึ่งซึ่งทำงานได้รวดเร็วพอๆ กับ Fping หรืออาจจะเร็วกว่าด้วย ก็คือเครื่องมือจากบริษัท SolarWinds สาเหตุที่มันทำงานได้เร็วกว่าก็เพราะว่า มันอนุญาตให้กำหนดช่วงเวลารอคอย ระหว่างการส่งแพ็กเก็ต ICMP แต่ละครั้งด้วย ถ้าระบุ delay time ให้เป็น 0 หรือ 1 คุณจะสามารถสแกน IP Address ที่อยู่ในคลาส C พร้อมทั้งแปลง IP Address เป็นชื่อโฮสต์ได้ในเวลาน้อยกว่า 7 วินาที

Network Mapper (nmap) โดย Fyodor นอกจาก NMAP จะให้ทั้งความสามารถพื้นฐานในการสแกนต่างๆที่ได้กล่าวไปข้างต้นทั้งหมด ซึ่งค่อนข้างหายากเหมือนกันสำหรับเครื่องมือตัวเดียวแต่ให้ได้ครบทุกเทคนิค

บทที่ 6
การออกแบบและพัฒนาโปรแกรม

6.1 รายละเอียดของการพัฒนา

ในการจัดทำโปรแกรมสำรวจและสังเคราะห์เครือข่ายและระบบคอมพิวเตอร์จำเป็นต้องศึกษาทฤษฎีและข้อมูลที่ใช้ในการค้นหาและรวบรวมข้อมูลของคอมพิวเตอร์เครื่องอื่นที่อยู่ในเครือข่าย โดยในโปรแกรมของเราใช้เทคนิคหลายๆอย่าง ดังนี้

- ใช้เทคนิค Ping sweep เพื่อค้นหาว่ามีเครื่องไหนอยู่ในเครือข่ายบ้าง
- ใช้เทคนิคในการอ่าน Shared Folder
- ใช้เทคนิค Trace route เพื่อสำรวจ Router
- ใช้เทคนิค การสแกนพอร์ตหรือ Port scanning เพื่อค้นหาว่ามีเซอร์วิสอะไรบ้างที่ทำงานอยู่หรืออยู่ในสถานะ listening
- ใช้เทคนิค Active Stack fingerprinting เพื่อค้นหาประเภทของระบบปฏิบัติการ
- ใช้เทคนิคในการอ่านค่า MAC Address

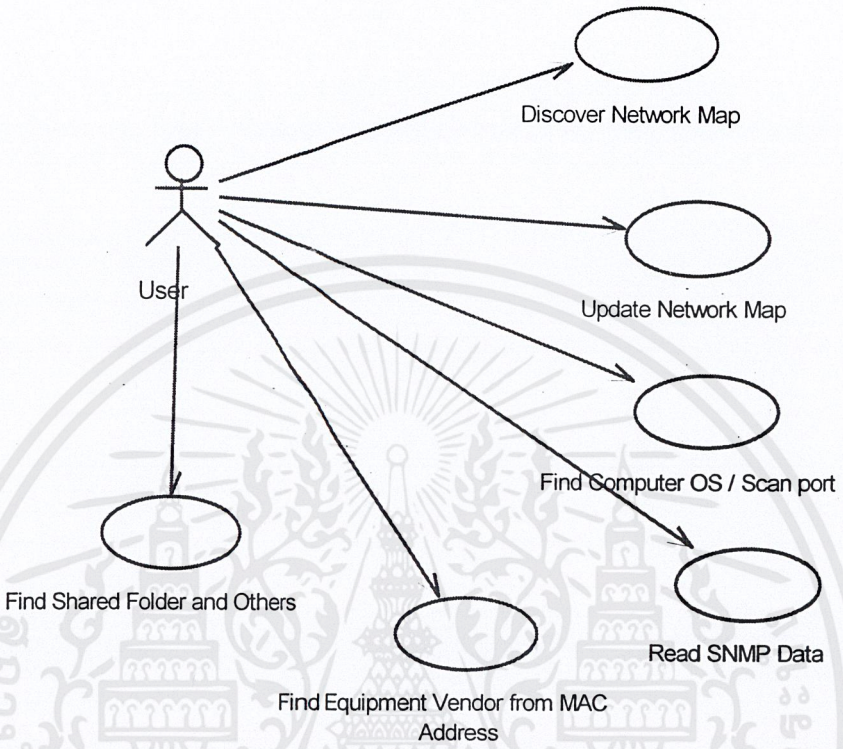
ส่วนเครื่องมือต่าง ๆ ที่ใช้ในการพัฒนาได้แก่

- Microsoft Visual C++ 6.0 MSDN Library Visual Studio 6.0
- Winpcap 2.3
- Nmap 3.00
- Nimda vesion 0.2 by Kirby Kuehl
- Microsoft Windows 2000

โดยรูปแบบของโปรแกรมจะมี Input เป็น IP address จะใส่แค่ค่าเดียวหรือ ใส่เป็นช่วงก็ได้ ผลลัพธ์ที่ได้ออกมาจะแสดงในรูปแบบ Graphic โดยจะวาดเป็นเครือข่ายแบบคร่าวๆ ไม่แสดงออกเป็น Topology แบบ Physical แต่จะวาดโดยแบ่งตามเครือข่ายที่เราทำการสำรวจโดยแสดงเครื่องคอมพิวเตอร์ทั้งหมดที่อยู่บนเครือข่ายที่ทำการสำรวจ และในแต่ละเครื่องก็จะแสดงรายละเอียดต่างๆ เช่น มี MAC Address อะไร, รายชื่อผู้ผลิตอุปกรณ์ Network ที่ใช้บนระบบเครือข่ายนั้น, มีเซอร์วิส Port อะไรบ้างที่ทำงานอยู่บ้าง, ประเภทของระบบปฏิบัติการ และหากมีการเปิด SNMP Service ก็จะอ่านรายละเอียดอื่น ๆ เพิ่มเติมได้เช่น CPU ที่ใช้เป็นรุ่นไหน มีจำนวน Interface ที่ติดต่ออยู่บนเครือข่ายเป็นเท่าไร เป็นต้น

การออกแบบโครงสร้างของโปรแกรม

Use Case Diagram

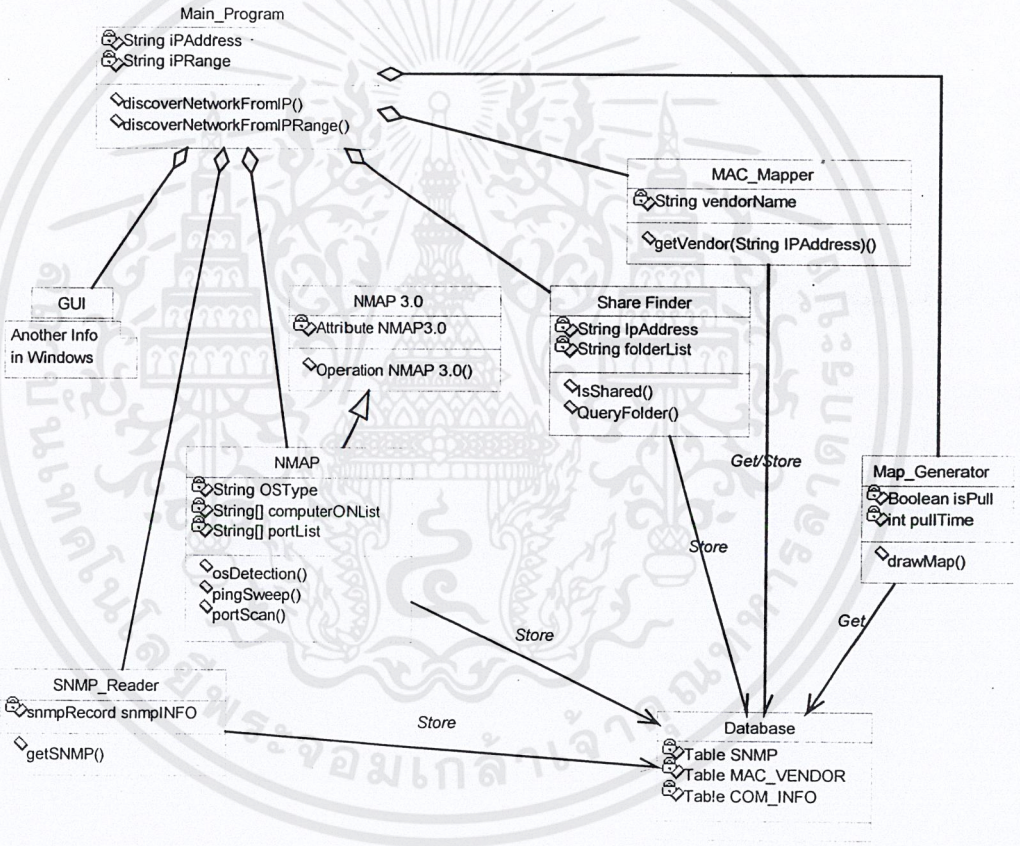


รูปที่ 6-1 แสดง Use Case ของโปรแกรม

คำศัพท์	คำอธิบาย
User	ผู้ที่ใช้โปรแกรมที่ต้องการทำการสำรวจระบบเครือข่าย เช่น ผู้ดูแลระบบ
Discover Network Map	ใช้โปรแกรมทำการสร้างแผนภาพของระบบเครือข่ายรวมโดยผู้ใช้ใส่ข้อมูลที่จำเป็นในการใช้สำรวจ
Update Network Map	สั่งให้โปรแกรมทำการสร้างแผนภาพของระบบเครือข่ายรวมอีกครั้ง โดยอาจจะใช้การกำหนดระยะเวลาในการอัพเดทเป็นระยะ ๆ
Find Computer OS/Scan port	สั่งให้โปรแกรมทำการค้นหา ระบบปฏิบัติการของคอมพิวเตอร์และport ที่เปิดบริการในระบบโดยเลือกคอมพิวเตอร์จากแผนภาพที่ได้จากการสำรวจ
Read SNMP Data	สั่งให้โปรแกรมทำการอ่านข้อมูลจาก SNMP Service

	ของคอมพิวเตอร์ในระบบโดยเลือกคอมพิวเตอร์จากแผนภาพที่ได้จากการสำรวจ
Find Equipment Vendor From MAC Address	สั่งให้โปรแกรมให้ทำการค้นหา MAC Address ของระบบคอมพิวเตอร์แล้วนำไปเทียบเพื่อบอก Equipment Vendor
Find Folder and others info	สั่งให้โปรแกรมทำการอ่าน Folder ของระบบที่มีการเปิด Shared ไว้ และทำการอ่านข้อมูลอื่น ๆ ที่สนใจเพิ่มเติม

ตารางที่ 6-1 แสดงคำอธิบาย Use Case Diagram

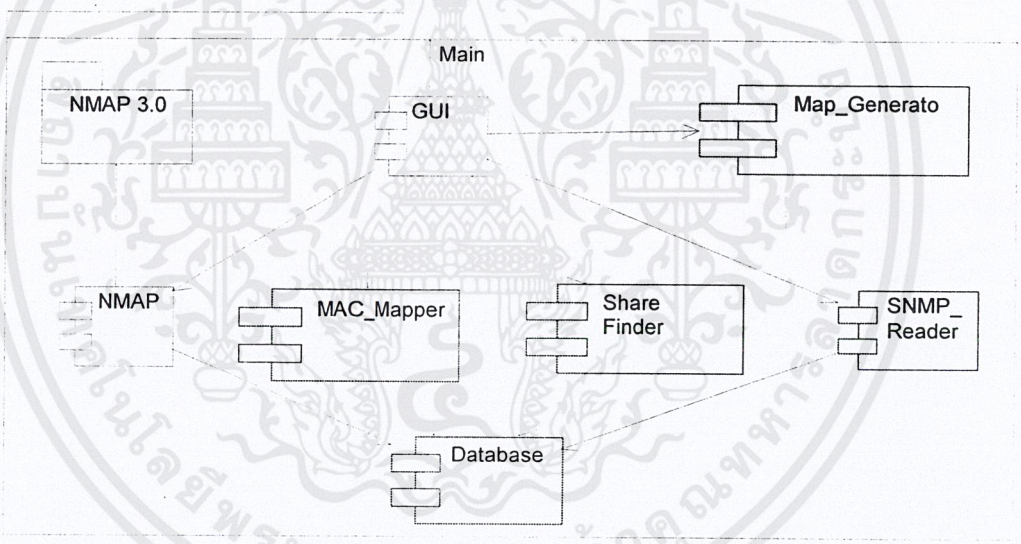


รูปที่ 6-2 แสดง Class Diagram

Class	คำอธิบาย
Main_Program	Class หลักของโปรแกรมเพื่อทำหน้าที่ติดต่อกับส่วนต่าง ๆ ของโปรแกรม
NMAP 3.0	Class ของโปรแกรม NMAP v.3.0 ที่เรานำมาใช้
NMAP	Class ของโปรแกรม NMAP ที่เราสืบทอดมาเพื่อนำมาใช้เป็นส่วนที่เราใช้

	ในการ pingsweep เครือข่าย รวมทั้งการตรวจสอบ port และใช้ในการตรวจหา OS ของคอมพิวเตอร์ในระบบ
MAC_Mapper	Class ที่ทำหน้าที่เปรียบเทียบ MAC Address กับรายชื่อ ผู้ผลิตอุปกรณ์
SNMP_Reader	Class ที่ใช้ในการอ่านค่าจาก SNMP Service ของคอมพิวเตอร์ในระบบเครือข่าย
Share Finder	Class ที่ใช้ในการสำรวจว่าระบบมีการเปิด Shared Folder ไว้หรือไม่ และทำการอ่าน Folder List ที่ Share ไว้
Map_Generator	Class ที่ใช้ในการสร้างแผนภาพของคอมพิวเตอร์ในระบบเครือข่ายจากข้อมูลใน Database
Database	Class ที่ใช้ในการติดต่อกับ Database เพื่อทำการบันทึก / อ่านข้อมูล
GUI	Class ที่ทำหน้าที่ติดต่อกับผู้ใช้ในรูปแบบ Graphic

ตารางที่ 6-2 แสดงคำอธิบาย Class Diagram

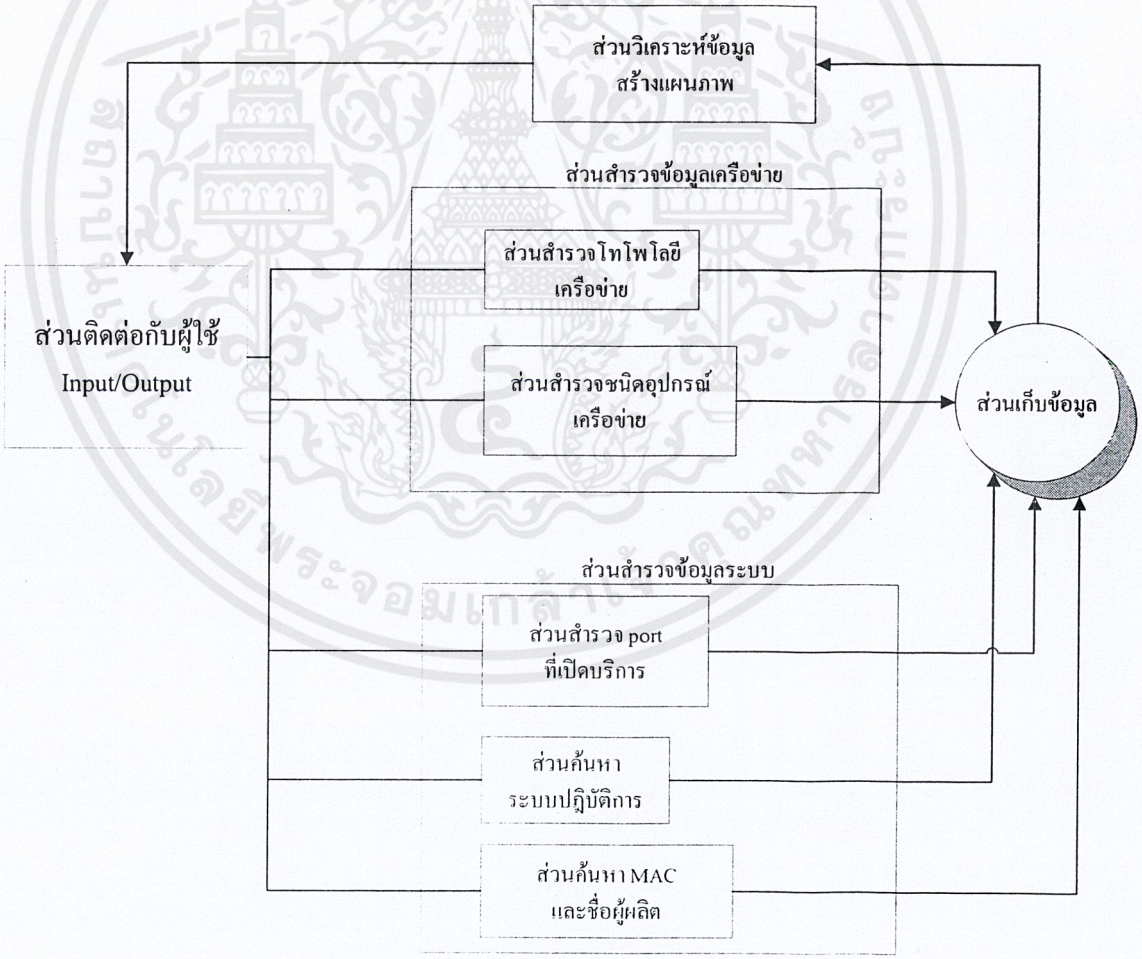


รูปที่ 6-3 แสดง Component Diagram

จากรูป Component Diagram แสดงส่วนประกอบย่อย ๆ ของโปรแกรมโดยส่วนประกอบต่าง ๆ มีหน้าที่ดังนี้

- NMAP 3.0 เป็น Package ของโปรแกรม NMAP 3.0
- NMAP เป็นส่วนที่สืบทอดมาจากโปรแกรม NMAP 3.0 มีหน้าที่ในการทำ Ping sweep , Port Scan และ การทำ OS Detection ของคอมพิวเตอร์
- Share Finder เป็นส่วนประกอบที่ใช้ในการสำรวจว่าระบบมีการเปิด Shared Folder ไว้หรือไม่
- และทำการอ่าน Folder List ที่ Share ไว้

- SNMP_Reader เป็นส่วนประกอบที่ใช้ในการติดต่อกับอุปกรณ์ในเครือข่ายด้วย SNMP Protocol เพื่ออ่านข้อมูลของอุปกรณ์นั้น
- MAC_Mapper เป็นส่วนประกอบที่ใช้ในการหา MAC Address ของอุปกรณ์ในระบบเครือข่ายและทำการค้นหา Vendor ของอุปกรณ์ในเครือข่าย
- Database เป็นส่วนประกอบที่ใช้ในการติดต่อกับฐานข้อมูลเพื่อเก็บข้อมูลที่ได้มาจากส่วนประกอบย่อยอื่น ๆ และอ่านฐานข้อมูลเพื่อนำไปสร้างแผนภาพระบบเครือข่าย
- Map_Generator เป็นส่วนประกอบที่ใช้ในการวิเคราะห์ข้อมูลที่ได้จากโปรแกรมย่อยและนำไปสร้างเป็นแผนภาพระบบเครือข่าย
- GUI เป็นส่วนประกอบที่ติดต่อกับผู้ใช้โดยมีหน้าที่รับข้อมูลและแสดงผลในรูปแบบ Graphic เพื่ออำนวยความสะดวกแก่ผู้ใช้

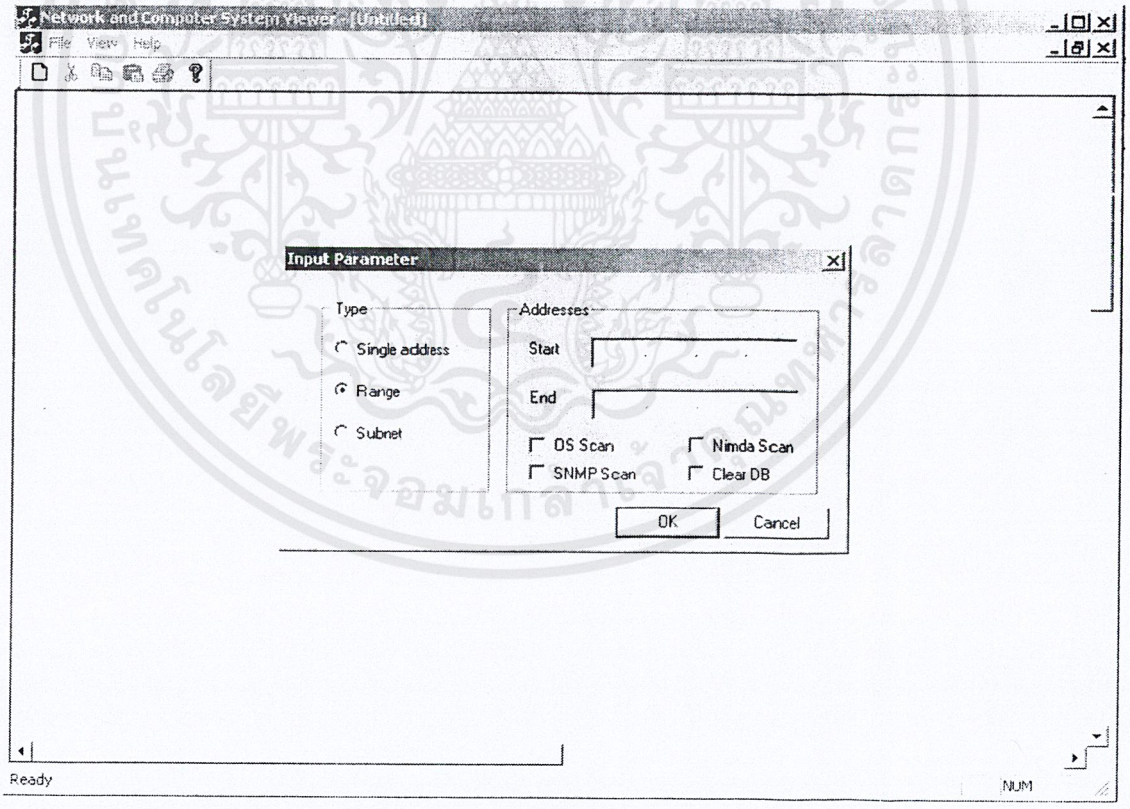


รูปที่ 6-4 แสดงโครงสร้างโปรแกรม

ส่วนหลัก ๆ ของโปรแกรมแบ่งเป็น 5 ส่วน

- ส่วนติดต่อกับผู้ใช้ ทำหน้าที่รับและแสดงผลติดต่อกับผู้ใช้
- ส่วนสำรวจข้อมูลของเครือข่าย ทำหน้าที่ค้นหาข้อมูลของระบบเครือข่าย
- ส่วนสำรวจข้อมูลระบบ ทำหน้าที่ค้นหาข้อมูลของระบบเครือข่าย
- ส่วนเก็บข้อมูล ทำหน้าที่เก็บข้อมูลที่ค้นหาได้
- ส่วนวิเคราะห์ข้อมูลและสร้างแผนภาพ ทำหน้าที่วิเคราะห์ข้อมูลที่เก็บไว้ในส่วนเก็บข้อมูลและนำมาสร้างแผนภาพของระบบเครือข่าย

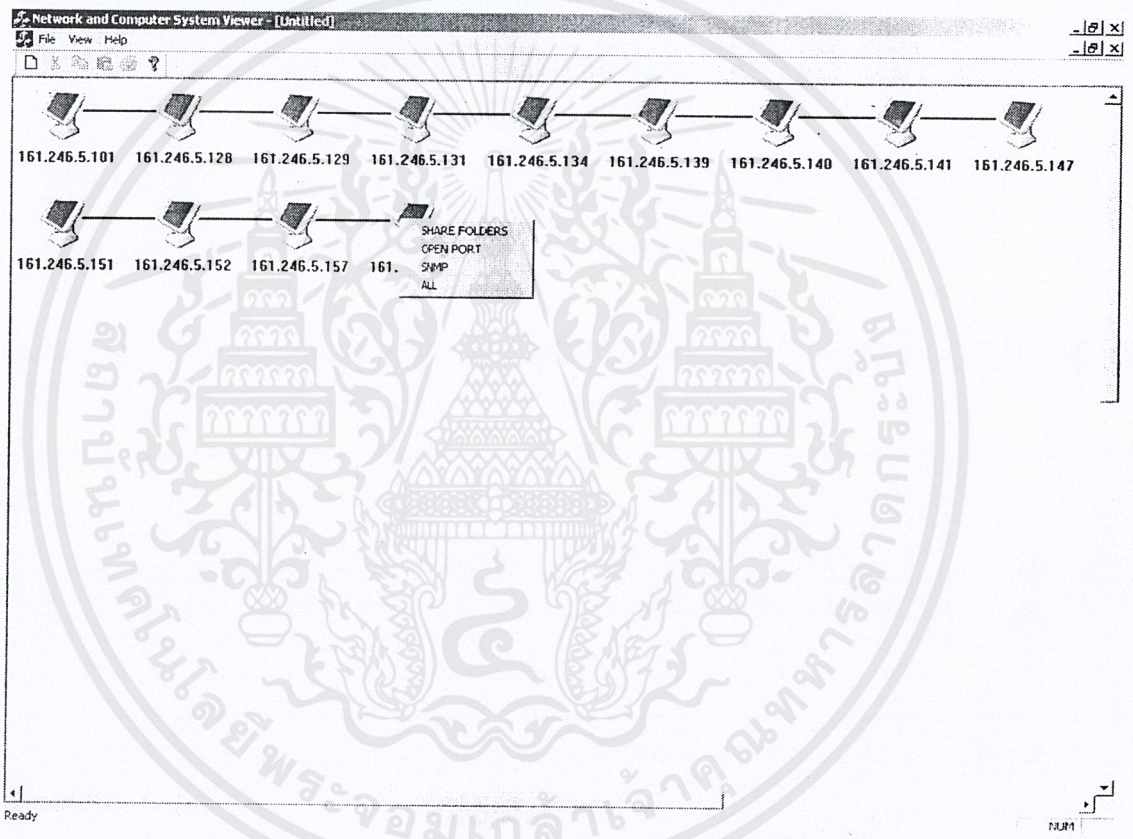
ตัวอย่างส่วนติดต่อกับผู้ใช้



รูปที่ 6-5 ตัวอย่างต้นแบบหน้าจอที่ใช้ในการใส่ Input ของโปรแกรม

Input ที่ต้องการของโปรแกรม

- Single IP Address ของคอมพิวเตอร์ที่ต้องการสำรวจกรณี ต้องการตรวจสอบหาข้อมูลเฉพาะคอมพิวเตอร์เครื่องนั้นอย่างละเอียด
- Range IP Address ของคอมพิวเตอร์กรณีต้องการสำรวจระบบเครือข่ายคอมพิวเตอร์ โดยทราบเป็นช่วงของคอมพิวเตอร์ในระบบเครือข่าย
- Subnet โดยต้องใส่ IP Address และ Subnet Mark ของกลุ่มเครือข่ายคอมพิวเตอร์ที่ต้องการทำการสำรวจ



รูปที่ 6-6 ตัวอย่างต้นแบบหน้าจอ แผนภาพที่ได้จากการสำรวจ

Output ของโปรแกรมที่ได้จากการสำรวจ

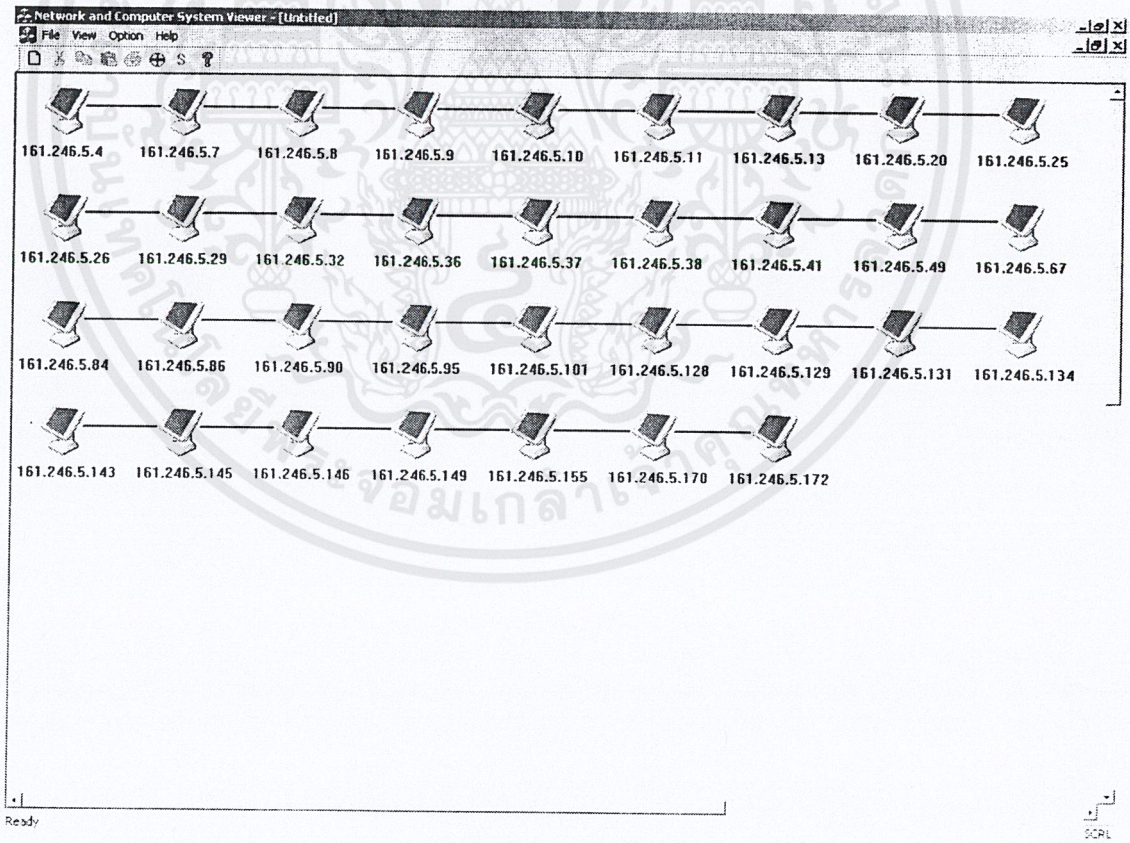
- แผนภาพทาง logical ของระบบเครือข่ายที่สำรวจมาได้
- ข้อมูลที่ได้จากการอ่าน SNMP กรณีที่เครื่องที่ต้องการมีการเปิดบริการ SNMP Service
- บอก OS ของเครื่องที่ต้องการทราบ
- บอก Service Port ของเครื่องที่ต้องการทราบ
- บอก MAC Address และเปรียบเทียบเป็นชื่อ Vendor ของอุปกรณ์เครื่องที่ต้องการทราบ
- บอก Shared Folder ของเครื่องที่ต้องการทราบ

บทที่ 7
การทำงานของโปรแกรมสำรวจเครือข่ายและระบบคอมพิวเตอร์

เป็นการทดลองใช้งานโปรแกรม โดยแบ่งเป็น การสำรวจเครื่องคอมพิวเตอร์ที่มีการใช้งานเครือข่าย, การสำรวจพอร์ตที่เครื่องคอมพิวเตอร์เปิดให้บริการ, การสำรวจ Shared Folder ที่เปิดอยู่ในระบบคอมพิวเตอร์, การนำผลที่ได้จากการสำรวจมาเก็บไว้เพื่อแสดงในรูปแผนภูมิการใช้งานเครื่องข่ายในแต่ละวัน

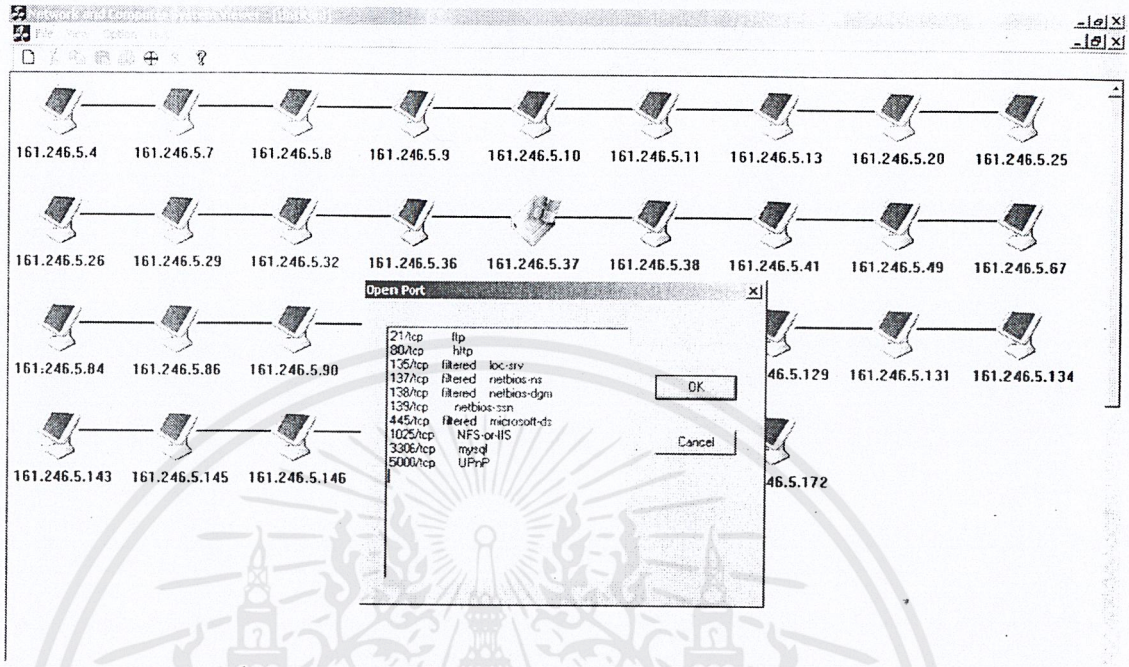
7.1 การสำรวจเครื่องคอมพิวเตอร์ที่มีการใช้งานเครือข่าย

การทำงานของโปรแกรมโดยเริ่มแรกจะให้ ผู้ใช้ทำการใส่ ช่วงหมายเลขไอพีที่ต้องการทำการสำรวจ เมื่อโปรแกรมทำการสำรวจโดยขั้นแรกหากไม่มีการเลือกตัวเลือกให้ทำการสำรวจอย่างละเอียดโปรแกรมจะทำการ Ping sweep ทำให้ได้ผลออกมาอย่างรวดเร็ว เมื่อเสร็จก็จะทำการแสดงเครื่องคอมพิวเตอร์ทั้งหมดที่มีการใช้งานเครือข่ายที่เราสนใจ



รูปที่ 7-1 แสดงรูปเครือข่ายที่ได้จากการสำรวจ

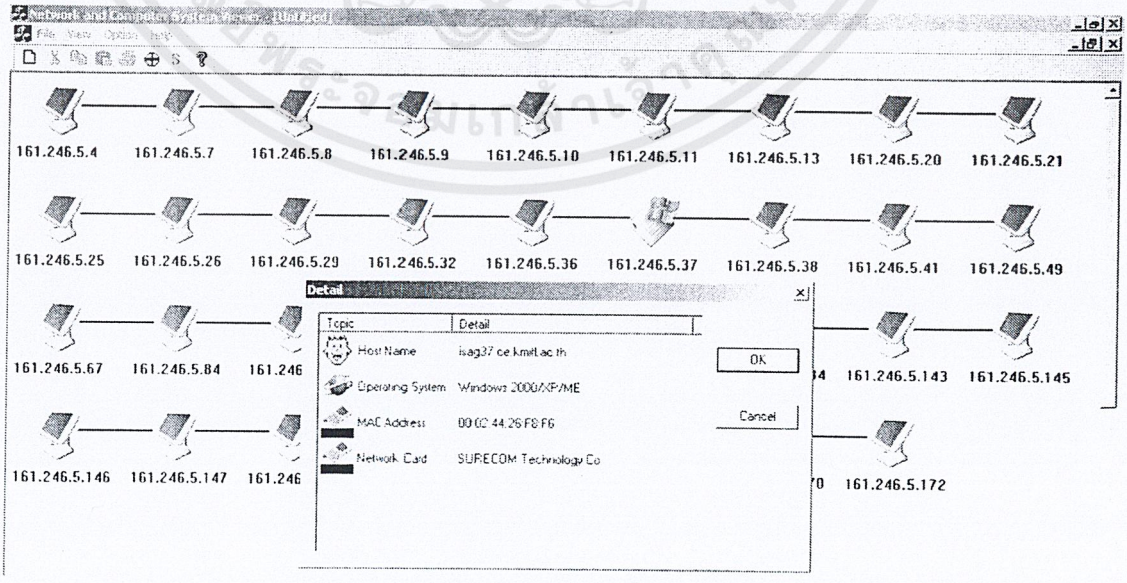
7.2 การสำรวจพอร์ตที่เครื่องคอมพิวเตอร์เปิดให้บริการ



รูปที่ 7-2 แสดงรูปผลที่ได้จากการสำรวจพอร์ตที่เปิดให้บริการ

โดยจากการรูป 7-2 นี้แสดงให้เห็นว่ามีการเปิดพอร์ต 21/tcp, 80/tcp, 135/tcp, 137/tcp, 138/tcp, 139/tcp, 445/tcp, 1025/tcp, 3306/tcp, 5000/tcp ทำให้ทราบได้ว่าเครื่องนี้มีการเปิดบริการที่สำคัญ ๆ เช่น TELNET , มีการเปิดให้บริการ WWW และ MYSQL

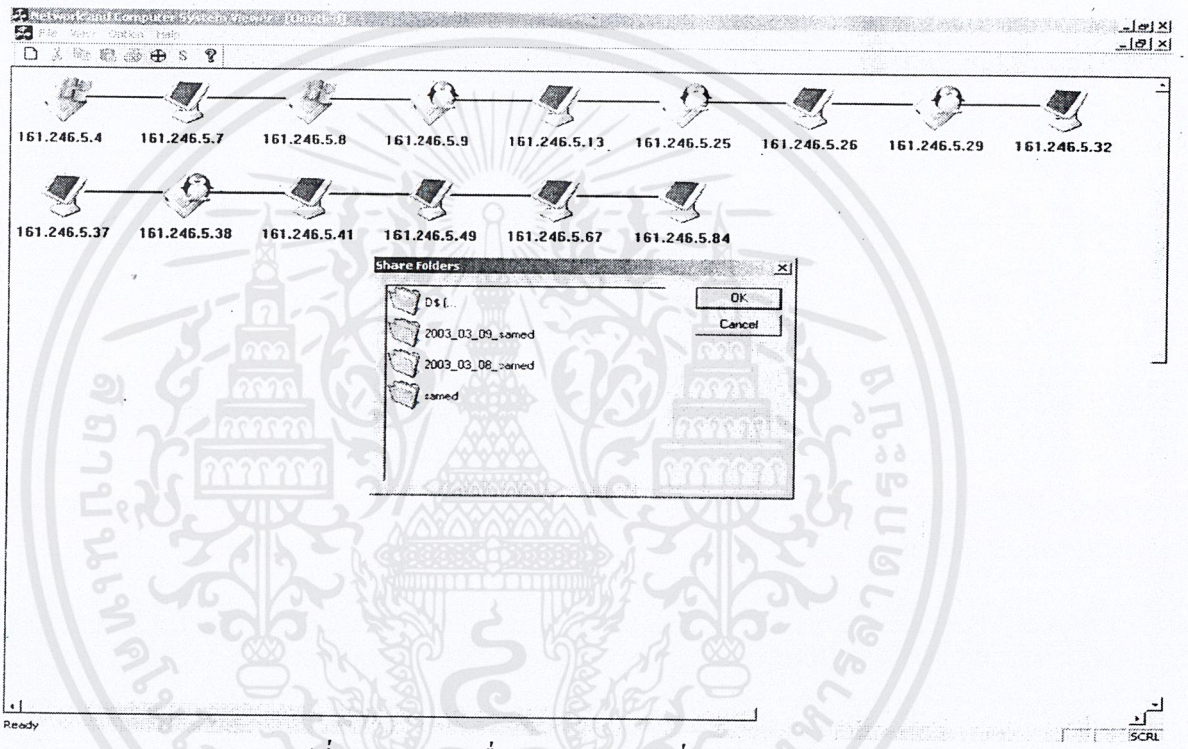
7.3 การสำรวจข้อมูลอื่น ๆ ของระบบคอมพิวเตอร์



รูปที่ 7-3 แสดงข้อมูลต่างอื่น ๆ ที่ได้จากการสำรวจ

จากรูปที่ 7-3 แสดงชื่อของโฮสต์ว่าเป็น isag37.ce.kmitl.ac.th มีการติดตั้งระบบปฏิบัติการเป็น Windows 2000/XP/ME มีหมายเลข MAC Address เป็น 00:02:44:26:F8:F6 ทำให้สามารถบอกรายชื่อผู้ผลิตเน็ตเวิร์คการ์ด ได้ว่าเป็น SURECOM Technology Co. แต่อาจมีปัญหาบางครั้งในการบอก MAC Address เนื่องจากสำหรับการอ่านค่าข้าม Subnet โปรแกรมจะทำการแสดงค่า MAC Address ที่เป็นของ Router ที่กั้นระหว่างแต่ละ Subnet มาแทนทำให้บางครั้ง Network Card อาจไม่ตรงกับความเป็นจริง

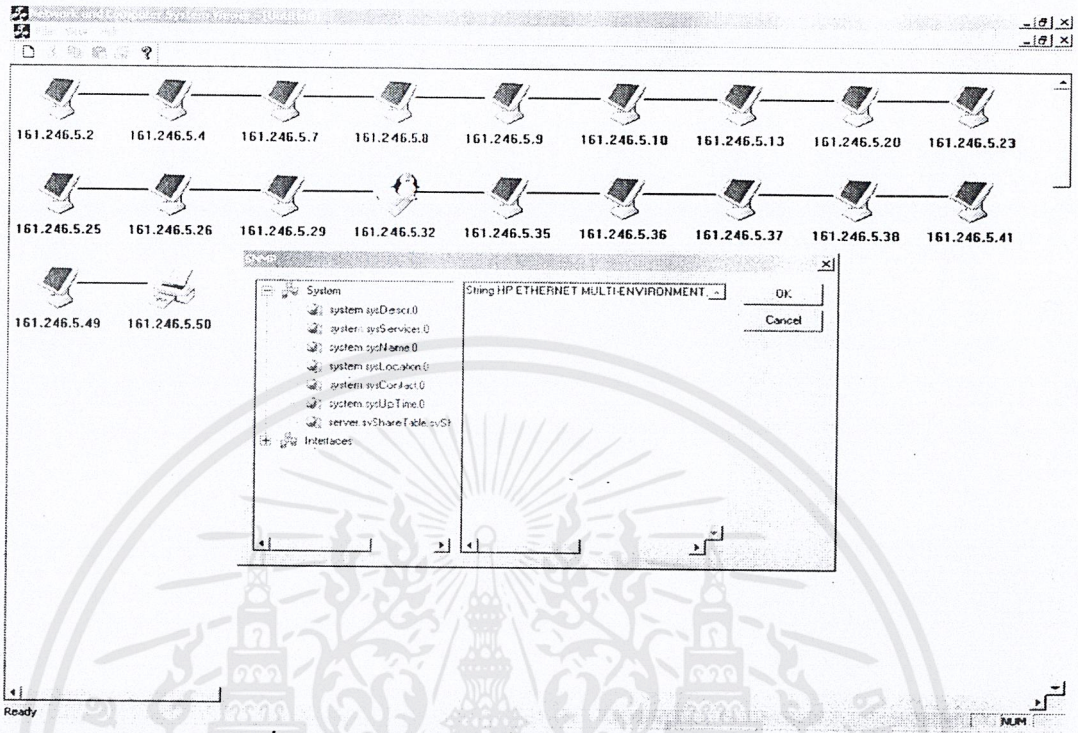
7.4 การสำรวจ Shared Folder ที่เปิดอยู่ในระบบคอมพิวเตอร์



รูปที่ 7-4 แสดงรายชื่อ Folder ต่าง ๆ ที่เปิด Share ไว้

โดยการสำรวจจะทำการแสดงรายชื่อ Folder ต่าง ๆ ของระบบคอมพิวเตอร์ที่เปิดแชร์ไว้ โดยจากการทดลองพบว่า สามารถแสดงได้ผลได้ถูกต้อง แต่อาจมีปัญหาจากการไม่พบรายชื่อ Folder บ้างเนื่องจากโปรแกรมประเภท Personal Firewall ที่มีการติดตั้งในปัจจุบันนี้มักนิยมป้องกันการเข้ามาอ่าน Folder ที่เปิดแชร์ไว้ในระบบเพื่อความปลอดภัยของระบบ

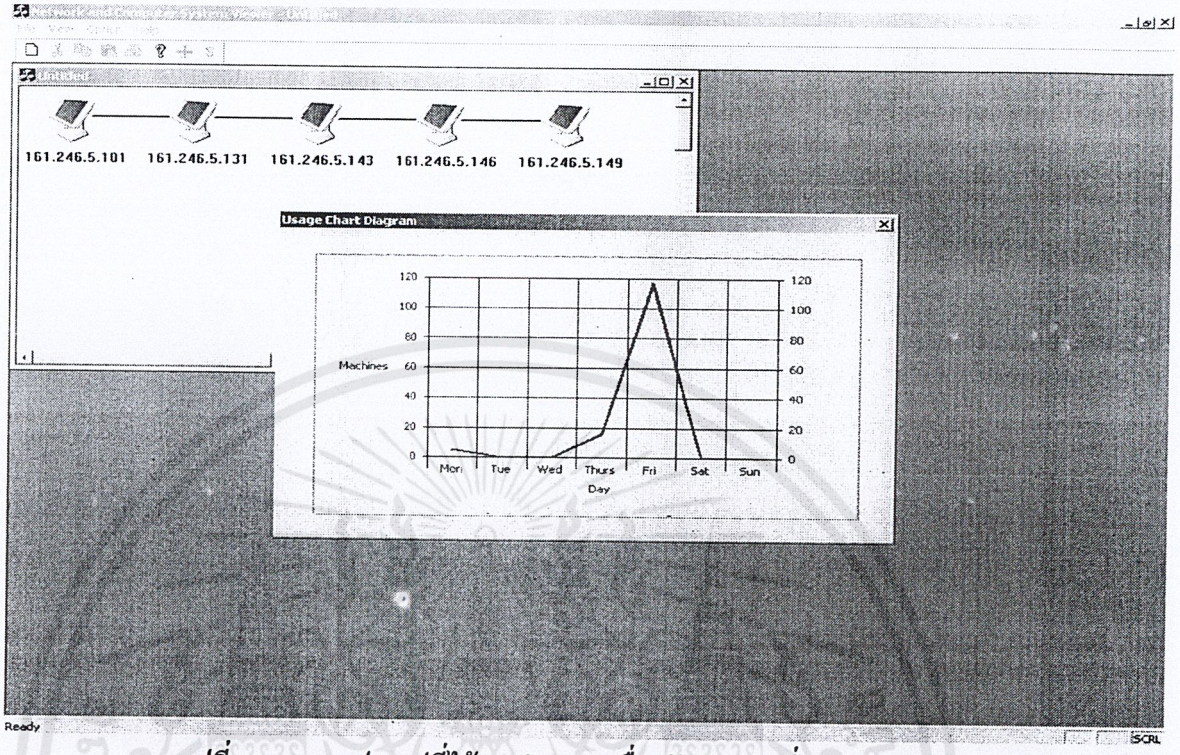
7.5 การสำรวจค่า SNMP ของระบบคอมพิวเตอร์



รูปที่ 7-5 แสดงค่า SNMP ที่ได้จากการอ่านอุปกรณ์บนเครือข่าย

โดยปกติโปรแกรมสามารถอ่านค่าจากอุปกรณ์บนเครือข่ายที่มี Community String เป็น Public และนำมาแสดงผลได้อย่างถูกต้อง แต่จากการทดลองพบว่ามีการเปิดบริการ SNMP port โดยใช้ Community String เป็น Public จำนวนไม่มากเนื่องจากเพื่อความปลอดภัยของระบบคอมพิวเตอร์หรืออุปกรณ์นั้น ๆ เอง รวมทั้งเครือข่ายส่วนใหญ่จะไม่เปิดบริการ SNMP port ไว้เนื่องจากไม่มีความจำเป็นในการจัดการเครือข่ายระยะไกล

7.6 การนำผลที่ได้จากการสำรวจมาเก็บไว้เพื่อแสดงในรูปแผนภูมิการใช้งานเครือข่ายในแต่ละวัน



รูปที่ 7-6 แสดงรูปกราฟที่ได้จากจำนวนเครื่องกับวันเวลาที่ทำการสำรวจ

การแสดงกราฟการใช้งานเครือข่าย โดยโปรแกรมสามารถนำผลที่ได้จากการสำรวจในแต่ละวันโดยสามารถนำผลมาสร้างเป็นกราฟแสดงการใช้งานเครือข่ายที่มีการใช้งานเครือข่ายในแต่ละวันได้ หากแต่ละวันทำการให้โปรแกรมทำการสำรวจโดยอัตโนมัติเป็นจำนวนครั้งที่เท่า ๆ กันในแต่ละวัน ทุก ๆ วัน แต่อาจได้รับผลที่ไม่เที่ยงตรงหากการใช้งานโปรแกรมสำรวจเครือข่ายในแต่ละวันมีจำนวนครั้งไม่เท่ากัน ก็ทำให้ผลที่นำมาเปรียบเทียบไม่ใช้ผลที่แท้จริงในการเปรียบเทียบได้

บทที่ 8
วิเคราะห์ผลการทดลองและสรุป

8.1 วิเคราะห์ผลการทดลอง

โปรแกรมสามารถทำงานได้ตามวัตถุประสงค์ดังนี้

- สามารถหาคอมพิวเตอร์ที่เปิดใช้งานเครือข่ายอยู่ในขณะนั้นได้
- สามารถหา OS , Service port ของคอมพิวเตอร์ในระบบเครือข่ายได้
- สามารถอ่านค่า SNMP Service ที่สนใจในการบอกลักษณะของคอมพิวเตอร์ในระบบเครือข่ายได้
- สามารถหา MAC Address และ บอก Vendor ของผู้ผลิตอุปกรณ์ Network นั้นได้
- สามารถนำข้อมูลที่รวบรวมมาได้มาสร้างเป็น แผนภาพคอมพิวเตอร์ทาง Logical ในระบบเครือข่ายได้ โดยแสดงผลในรูปแบบกราฟฟิก
- สามารถนำผลที่ได้มาสร้างเป็นแผนภูมิการใช้งานได้
- สามารถตั้งเวลาให้ทำการสำรวจอัตโนมัติได้
- สามารถนำผลลัพธ์แสดงออกทางรายงานได้

คุณสมบัติของโปรแกรม	NMAP 3.00	NetworkView 2.0	WhatsUp 7.0	ISAGNetView
การค้นหาระบบ OS	ได้	ไม่ได้	ไม่ได้	ได้
อ่านค่า SNMP Service	ไม่ได้	ได้	ได้	ได้
หาค่า MAC Address เทียบกับผู้ผลิต	ไม่ได้	ได้	ได้	ได้
Traceroute	ไม่ได้	ได้	ได้	ได้
สำรวจ Port	ได้	ได้	ได้	ได้
แสดงผลแบบกราฟฟิก	ไม่ได้	ได้	ได้	ได้
อ่าน Shared Folder	ไม่ได้	ได้	ได้	ได้
เพิ่มเติม Module ในการทำงานอื่น ๆ	ไม่ได้	ไม่ได้	ไม่ได้	ได้

ตาราง 8-1 แสดงคุณสมบัติเปรียบเทียบของโปรแกรม

8.2 สรุปผล

การทำงานของโปรแกรมสามารถทำงานได้เป็นที่น่าพอใจ โดยสามารถทำให้ผู้ดูแลระบบได้รับความสะดวกในการทำงานมากขึ้น

- โปรแกรมสามารถทำงานได้ ตามวัตถุประสงค์ที่วางไว้
- สามารถนำผลลัพธ์ที่ได้จากการสำรวจไปใช้ประโยชน์ได้หลากหลาย

ข้อจำกัดของโปรแกรม

- พบปัญหาในการสำรวจบ้าง เนื่องจากปัจจุบันผู้ใช้นิยมติดตั้งโปรแกรมประเภท Firewall เพื่อเพิ่มความปลอดภัยในเครื่องมากยิ่งขึ้น ข้อมูลที่ได้จึงอาจน้อยไปบ้าง
- การค้นหา MAC Address ยังสามารถทำได้ภายในเครือข่าย Subnet เดียวกันเท่านั้น
- ข้อมูลรายละเอียด SNMP ยังไม่สามารถบอกได้ทั่วทั้งหมด เนื่องจากมีเครื่องคอมพิวเตอร์ที่เปิดบริการ SNMP Service จำนวนไม่มาก
- สามารถตรวจสอบ OS จากชนิดที่มีอยู่ในรายชื่อข้อมูล OS ของ NMAP เท่านั้น เช่น Window , Linux , Unix และอุปกรณ์เช่น Router ของ CISCO, Printer ของ HP

8.3 แนวทางในการพัฒนาสำหรับผู้สนใจในอนาคต

เพื่อให้โปรแกรมมีความสามารถในการทำงานด้านการดูแลเครือข่ายและระบบคอมพิวเตอร์มากยิ่ง ๆ ขึ้น และเพื่อความสะดวกในการจัดการข้อมูลที่ได้

1. ควรจะเพิ่มเติมความสามารถในการสร้างแผนภาพที่มีความใกล้เคียงกับลักษณะเครือข่ายทางกายภาพมากยิ่งขึ้น
2. พัฒนาส่วนที่สำหรับใช้สำรวจข้อมูลเครือข่ายอื่น ๆ มาเพิ่มเติมลงไปภายในโปรแกรมทำให้โปรแกรมสามารถรู้รายละเอียดต่าง ๆ มากยิ่งขึ้น
3. ควรพัฒนาส่วนที่จะนำมาประมวลผลที่ได้จากเครื่อข่ายเพิ่มเติมเพื่อให้ข้อมูลที่ได้สามารถนำไปใช้ประโยชน์ได้โดยรวดเร็วยิ่งขึ้น

บรรณานุกรม

[1] ยุทธนา ลีลาศวัฒนกุล: "คู่มือการเขียนโปรแกรม และใช้งาน Visual C++ 6.0 ฉบับโปรแกรมเมอร์" อินโฟเพรส, 2001

[2] Gilbert Held:"LAN Management with SNMP and RMON", Jonh Wiley, 1996

[3] โรเบิร์ต ลาฟอเร่,ราบินเดอร์ ศรีกิจจาภรณ์: "การเขียนโปรแกรมแบบโอโอพี ด้วยเทอร์โบและบอร์แลนด์ C++", ซีเอ็ด, 1994

[4] สุรศักดิ์ สงวนพงษ์:"สถาปัตยกรรมและโปรโตคอลทีซีพี/ไอพี", ซีเอ็ด, 2002

[5] Joel Scambray, Stuart McClure, George Kurtz, *"Hacking Exposed Network Security & Solution"*, 2nd Edition, Mc Graw Hill

Larry J.Hughes, Jr., *"Internet Security Techniques"*, New Riders Publishing, 1961, pp. 130-144, 170-174, 192-207

[6] สุวัฒน์ ปุณณชัยยะ, ต้น ตันฑ์สุทธิวงศ์, สุพจน์ ปุณณชัยชนะ, *"เปิดโลกของ TCP/IP และโปรโตคอลของอินเตอร์เน็ต"*, โปรวิชั่น, 2543

[7] Ian Sommerville:"Software Engineering, 6th Edition, Addison-Wesley, 2001

[8] Microsoft MSDN Library, Microsoft Corporation, August 1999

[9] Gary R. Wright, W. Richard Stevens, TCP-IP illustrated Volume 2, chapter 31. Addison-Wesley professional computing series.

เว็บไซต์อ้างอิง

[1] http://www.hack.co.za

[2] http://www.insecure.org

[3] http://winpcap.polito.it/

[4] http://www.rootshell.com

[5] http://www.codeguru.com

[6] http://www.codeproject.com

[7] http://astalavista.box.sk

[8] http://neworder.box.sk

[9] http://www.technotronic.com

[10] http://www.ussrback.com

[11] http://www.nmap.org/

[12] http://www.securitybugware.org/libnetnt/

[13] http://www.laurentconstantin.com/en/lcrzoex/

[14] http://www.ff.iij4u.or.jp/~ebata/soft/winpcaparp/