ระบบควบคุมการจ่ายกระแสไฟฟ้าอัตโนมัติผ่านเครือข่ายท้องถิ่นแบบไร้สาย โดยใช้อุปกรณ์แอ็กเซสพอยต์

Electrical Power Automatic Control System Via Access Point

โดย

นางสาวกมลทิพย์ ฤทธิพัฒน์

นายทศพร วัฒนะพันธ์ศักดิ์

นายศักดา แกล้วกล้า

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2549

ผ่านการตรวจชิ้นงานแล้ว

(ลงชื่อ).....ผู้ตรวจ

ผ่านการตรวจรูปเล่มแล้ว

(ลงชื่อ).....ผู้ตรวจ

ระบบควบคุมการจ่ายกระแสไฟฟ้าอัตโนมัติผ่านเครือข่ายท้องถิ่นแบบไร้สาย โดยใช้อุปกรณ์แอ็กเซสพอยต์

Electrical Power Automatic Control System Via Access Point

โดย

นางสาวกมลทิพย์ ฤทธิพัฒน์ 47015001

นายทศพร วัฒนะพันธ์ศักดิ์ 47015050

นายศักดา แกล้วกล้า 47015066

อาจารย์ที่ปรึกษา

ศ.ดร. วิวัฒน์ กิรานนท์

รศ.ดร.ปราโมทย์ วาดเขียน

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2549

ปริญญานิพนธ์ปีการศึกษา 2549

ภาควิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง ระบบควบคุมการจ่ายกระแสไฟฟ้าอัตโนมัติผ่านเครือข่ายท้องถิ่นแบบไร้สาย
โดยใช้อุปกรณ์แอ็กเซสพอยต์

Electrical Power Automatic Control System Via Access Point

ผู้จัดทำ

1. นางสาวกมลทิพย์ ฤทธิพัฒน์ 47015001
2. นายทศพร วัฒนะพันธ์ศักดิ์ 47015050
3. นายศักดา แกล้วกล้า 47015066

..... อาจารย์ที่ปรึกษา

(ศ.ดร. วิวัฒน์ กิรานนท์)

..... อาจารย์ที่ปรึกษา

(รศ.ดร.ปราโมทย์ วาดเขียน)

ระบบควบคุมการจ่ายกระแสไฟฟ้าอัตโนมัติผ่านเครือข่ายท้องถิ่นแบบไร้สาย โดยใช้อุปกรณ์แอ็กเซสพอยต์

Electrical Power Automatic Control System Via Access Point

โดย นางสาวกมลทิพย์ ฤทธิพัฒน์ 47015001

นายทศพร วัฒนะพันธ์ศักดิ์ 47015050

นายศักดา แกล้วกล้า 47015066

อาจารย์ที่ปรึกษา ศ.ดร. วิวัฒน์ กิรานนท์

รศ.ดร.ปราโมทย์ วาดเขียน

บทคัดย่อ

โครงงานนี้นำเสนอระบบควบคุมการจ่ายกำลังไฟฟ้าอัตโนมัติให้กับห้องพักโดยผ่านระบบเครือข่ายท้องถิ่นแบบไร้สายโดยใช้อุปกรณ์แอ็กเซสพอยต์โดยระบบประกอบด้วย ตัวบริการหลักซึ่งอยู่ที่ศูนย์กลางและตัวลูกข่ายซึ่งใช้อีเทอร์เน็ตแบบฝังตัวนอกจากนี้จะมีไมโครคอนโทลเลอร์ทำหน้าที่ในการรับส่งข้อมูลกับตัวบริการและทำการควบคุมการจ่ายกระแสไฟฟ้าให้กับห้องพัก

Abstract

The project presents an electrical power automatic control system for lodging's room via access point .The proposed system is composed of a central server and users with employ embedded Ethernet. In addition, the microcontroller is used for transmitting/receiving data to/from the server and control the power line outlet.

สารบัญ

สารบัญ (ต่อ)

หน้าที่

สารบัญรูปภาพ

สารบัญรูปภาพ (ต่อ)

สารบัญรูปภาพ (ต่อ)

สารบัญตาราง

หน้าที่

บทที่ 1
บทนำ

1.1.ความเป็นมาของโครงงาน

ปัจจุบันการใช้งานทางเน็ตเวิร์คหรือเครือข่ายท้องถิ่นได้รับการนิยมอย่างแพร่หลายและมีการประยุกต์ใช้งานหลากหลายตามไปด้วย เช่น การติดต่อโทรศัพท์ผ่านเครือข่าย หรือการติดต่อสื่อสารโดยใช้มัลติมีเดีย ดังนั้นโครงงานนี้จึงนำเครือข่ายแบบไร้สายมาประยุกต์ใช้ในการจ่ายกระแสไฟฟ้าให้กับโรงแรมหรือห้องพักที่ใช้ชุดควบคุมแบบฝังตัว (Embedded) อันประกอบด้วยวงจรควบคุมการรับ-ส่งข้อมูลผ่านอีเทอร์เน็ตและไมโครคอนโทรลเลอร์ และใช้การเชื่อมต่อเครือข่ายท้องถิ่นแบบไร้สาย (Wireless LAN)โดยใช้แอ็กเซสพอยต์(Access Point)เป็นตัวส่งผ่านข้อมูลเพื่อใช้ในการจ่ายกระแสไฟฟ้าภายในห้องพัก

1.2.วัตถุประสงค์ของโครงงาน

เพื่อสามารถควบคุมการจ่ายกระแสไฟฟ้าให้กับโรงแรมหรือห้องพักโดยใช้คอมพิวเตอร์ศูนย์กลาง (Server) เป็นตัวสั่งการทำงานผ่านเครือข่ายท้องถิ่นแบบไร้สายโดยใช้อุปกรณ์แอ็กเซสพอยต์ทำให้การควบคุมทำได้สะดวกรวดเร็วและลดการเชื่อมระบบต่างๆด้วยสายไฟ

1.3.ประโยชน์ที่ได้รับ

ทำให้ระบบเครือข่ายซึ่งโดยทั่วไปตามโรงแรมหรือห้องพักต่างๆมักจะมีระบบเครือข่ายท้องถิ่นแบบไร้สายให้บริการกับลูกค้าได้ถูกใช้ประโยชน์มากยิ่งขึ้นนอกจากนี้ยังเป็นการอำนวยความสะดวกแก่เจ้าของกิจการและพนักงานที่ต้องทำหน้าที่ตรวจสอบความเรียบร้อยอีกด้วย

1.4 .ขั้นตอนการดำเนินงาน

โครงงานนี้แบ่งเป็น 2 ส่วนใหญ่ๆคือ

1. ส่วนของซอฟต์แวร์ ประกอบด้วย
   - 1.1 โปรแกรมเชื่อมต่อระหว่างคอมพิวเตอร์ศูนย์กลางกับ เอ็มเบสเด็ส
   - 1.2 โปรแกรมควบคุมอีเทอร์เน็ตคอนโทรลเลอร์
   - 1.3 โปรแกรมควบคุมการจ่ายกระแสไฟฟ้า
2. ส่วนของฮาร์ดแวร์ ประกอบด้วย
   - 2.1 ส่วนของการเชื่อมต่อระหว่าง อีเทอร์เน็ตคอนโทรลเลอร์และเครือข่ายท้องถิ่นแบบไร้สาย
   - 2.2 ส่วนของตัวควบคุม อีเทอร์เน็ตคอนโทรลเลอร์
   - 2.3 ส่วนของวงจรควบคุมการจ่ายกระแสไฟฟ้า และตรวจสอบความผิดพลาด

ขั้นตอนการดำเนินงาน

- รวบรวมข้อมูลการทำงานของอีเทอร์เน็ต,การควบคุมแบบฝังตัว และวงจรต่างๆที่เกี่ยวข้อง
- สร้างฮาร์ดแวร์ที่ใช้ในการรับและส่งข้อมูลผ่านเครือข่ายท้องถิ่น ซึ่งประกอบด้วย วงจรควบคุมการรับส่งข้อมูลผ่านอีเทอร์เน็ต และไมโครคอนโทรลเลอร์
- เขียนโปรแกรมทางด้านเครื่องคอมพิวเตอร์ศูนย์กลางเพื่อใช้ในการรับและส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์กับฮาร์ดแวร์ที่ได้กล่าวมาในข้อที่แล้ว
- สร้างฮาร์ดแวร์ส่วนของวงจรควบคุมการจ่ายกระแสไฟฟ้า
- ส่วนของ ฮาร์ดแวร์กับการเชื่อมต่อกับระบบ เครือข่ายท้องถิ่นแบบไร้สายที่สามารถรับข้อมูลจากเครื่องคอมพิวเตอร์ศูนย์กลาง
- ทำการเชื่อมต่อระบบทั้งหมดเข้าด้วยกัน
- เก็บผลการทดลอง
- วิเคราะห์และสรุปผล

บทที่ 2
ทฤษฎีและหลักการ

2.1 ระบบเครือข่ายเบื้องต้น

2.1.1. ความหมายของระบบเครือข่าย

ระบบเครือข่าย คือ ระบบที่มีคอมพิวเตอร์อย่างน้อย 2 เครื่องเชื่อมต่อกันโดยมีสื่อกลางในการเชื่อมต่อ และสามารถสื่อสารข้อมูลระหว่างกันได้โดยที่เครื่องคอมพิวเตอร์ทั้งสองเครื่องนั้นสามารถที่จะแลกเปลี่ยนข้อมูลระหว่างกันได้รวมถึงสามารถใช้ทรัพยากรที่มีอยู่ร่วมกันได้เช่นการถ่ายโอนข้อมูลงานเอกสารหรือการใช้งานเครื่องพิมพ์ร่วมกัน

2.1.2 .วัตถุประสงค์ของการใช้ระบบเครือข่าย

1. สามารถใช้โปรแกรมและข้อมูลร่วมกันได้

คือเครื่องลูก (Client) สามารถเข้ามาใช้โปรแกรมข้อมูลร่วมกันได้จากเครื่องแม่ (Server) หรือระหว่างเครื่องลูกกับเครื่องลูกก็ได้เป็นการประหยัดเนื้อที่ในการจัดเก็บโปรแกรมไม่จำเป็นว่าทุกเครื่องต้องมีโปรแกรมเดียวกันนี้ในเครื่องของตนเอง

2. เพื่อความประหยัด

เพราะว่าเป็นการลงทุนที่คุ้มค่าอย่างเช่นในสำนักงานหนึ่งมีเครื่องอยู่จำนวน30 เครื่องหรือมากกว่านี้ ถ้าไม่มีการนำระบบเครือข่ายคอมพิวเตอร์มาใช้จะเห็นว่าต้องใช้เครื่องพิมพ์อย่างน้อย 5-10 เครื่องมาใช้งาน แต่ถ้ามีระบบเครือข่ายคอมพิวเตอร์มาใช้แล้วก็สามารถใช้อุปกรณ์หรือเครื่องพิมพ์ประมาณ 2-3เครื่องก็พอต่อการใช้งานแล้วเพราะว่าทุกเครื่องสามารถเข้าใช้เครื่องพิมพ์เครื่องไหนก็ได้เครื่องอื่นๆที่ในระบบเครือข่ายเดียวกัน

3. เพื่อความเชื่อถือได้ของระบบงาน

นับเป็นสิ่งที่สำคัญสำหรับการดำเนินธุรกิจเมื่อนำระบบเครือข่ายคอมพิวเตอร์มาใช้งานทำให้ระบบงานมีประสิทธิภาพ มีความน่าเชื่อถือของข้อมูล เพราะจะมีการสำรองข้อมูลไว้เมื่อเครื่องที่ใช้งานเกิดมีปัญหาก็สามารถนำข้อมูลที่มีการสำรองมาใช้ได้อย่างทันที

4. ประหยัดเวลา ค่าเดินทาง

เมื่อต้องการแลกเปลี่ยนข้อมูลกัน ในที่ที่อยู่ห่างไกลกันเช่น บริษัทแม่อยู่ที่ กรุงเทพ ส่วนบริษัทลูกอาจจะอยู่ตามต่างจังหวัด แต่ละที่ก็มีการเก็บข้อมูล การเงิน ประวัติลูกค้าและอื่นๆ แต่ถ้าต้องการใช้ข้อมูลของอีกที่หนึ่งจะเกิดความลำบาก ล่าช้าและไม่สะดวกจึงมีการนำหลักการของเครือข่ายคอมพิวเตอร์ (Computer Network) มาใช้งานเช่น มีการใช้ทรัพยากรร่วมกันหรือโปรแกรมข้อมูลร่วมกัน

2.1.3. โครงสร้างของระบบเครือข่าย

โครงสร้างที่จะประกอบกันเป็นส่วนของระบบเครือข่ายคอมพิวเตอร์นั้น จะประกอบไปด้วย เครื่องคอมพิวเตอร์หลัก เครื่องคอมพิวเตอร์ลูกข่าย และอุปกรณ์ในการเชื่อมต่อ

- เครื่องคอมพิวเตอร์หลักหรือเครื่องเซิร์ฟเวอร์ก็คือเครื่องคอมพิวเตอร์ที่ทำหน้าที่ให้บริการข้อมูลและทรัพยากรของระบบเครื่องเซิร์ฟเวอร์นั้นจะต้องเป็นเครื่องที่มีประสิทธิภาพสูง ไม่ว่าจะเป็นเรื่องของความเร็วของซีพียู ขนาดของหน่วยความจำขนาดความจุข้อมูลของฮาร์ดดิสก์เครื่องเซิร์ฟเวอร์ นั้นสามารถแบ่งออกได้เป็นหลายประเภทตามความเหมาะสมกับการใช้งานเพื่อให้ได้มาซึ่งประสิทธิภาพในการให้บริการอย่างเช่น Web Server , FTP Server , File Server , Mail Server , Printer Server เป็นต้น

- เครื่องคอมพิวเตอร์ลูกข่ายก็คือเครื่องคอมพิวเตอร์ที่มีหน้าที่ขอใช้ทรัพยากรของระบบจากเครื่องคอมพิวเตอร์หลักหรือจากเครื่องคอมพิวเตอร์ลูกข่าย ด้วยกันก็ได้

- อุปกรณ์ในการเชื่อมการติดต่อสื่อสารเป็นอุปกรณ์ที่ทำให้เครื่องคอมพิวเตอร์ในระบบเครือข่ายสามารถติดต่อสื่อสารกันได้ ก็มีอุปกรณ์หลายอย่างเช่น สายสัญญาณข้อมูล (Network Cable) แผงวงจรรับส่งสัญญาณจากสายสัญญาณ (Network Adapter) ซึ่งเป็นอุปกรณ์ที่ใช้เป็นช่องทางเดินของข้อมูล

2.1.4.ประเภทของระบบเครือข่ายคอมพิวเตอร์ตามระยะการเชื่อมต่อ

1.ระบบเครือข่ายคอมพิวเตอร์ระยะใกล้ (Local Area Network หรือ LAN)

เป็นระบบเครือข่ายระดับท้องถิ่น มีขนาดเล็ก ครอบคลุมพื้นที่จำกัด เชื่อมโยงกันในรัศมีใกล้ๆในเขตพื้นที่เดียวกัน เช่นในอาคารเดียวกันห้องเดียวกันภายในตึกเดียวกันหรือหลายๆ ตึกใกล้ๆกันระบบเครือข่ายท้องถิ่น มีประโยชน์ตรงที่สามารถทำให้เครื่องคอมพิวเตอร์หลาย ๆ เครื่องที่เชื่อมต่อกันสามารถส่งข้อมูลแลกเปลี่ยนกันได้อย่างสะดวกรวดเร็วและยังสามารถใช้ทรัพยากรร่วมกันได้อีกด้วย เทคโนโลยีของระบบเครือข่ายท้องถิ่นมีหลายรูปแบบอย่างเช่นเครือข่ายท้องถิ่นแบบ อีเทอร์เน็ต ฟาสอีเทอร์เน็ต โทเคนริง เป็นต้นแต่เทคโนโลยีที่ได้รับความนิยมมากที่สุดในปัจจุบันก็คือ อีเทอร์เน็ต และฟาสอีเทอร์เน็ต ระบบเครือข่ายโดยทั่วไปที่ใช้กันอยู่นี้จะเป็นการนำเครือข่ายระบบเครือข่ายท้องถิ่นมาประยุกต์ใช้ให้เหมาะสม

2.ระบบเครือข่ายคอมพิวเตอร์ระยะกลาง (Metropolitan Area Network หรือ MAN)

เป็นระบบเครือข่ายระดับเมือง คือมีการเชื่อมโยงกันในพื้นที่ที่กว้างไกลกว่าระบบเครือข่ายท้องถิ่นคืออาจจะเชื่อมโยงกันภายในจังหวัดโดยจะต้องมีการใช้ระบบเครือข่ายของโทรศัพท์เข้ามาช่วยในการติดต่อสื่อสาร

3.ระบบเครือข่ายคอมพิวเตอร์ระยะไกล (Wide Area Network หรือ WAN)

เป็นระบบเครือข่ายระดับไกลคือจะเป็นเครือข่ายที่เชื่อมต่อคอมพิวเตอร์หรืออุปกรณ์ที่อยู่ห่างไกลกันเข้าด้วยกันอาจจะต้องเป็นการติดต่อสื่อสารกันในระดับประเทศข้ามทวีปหรือทั่วโลกก็ได้ในการเชื่อมการติดต่อกันนั้นจะต้องมีการต่อเข้ากับระบบสื่อสารต่างๆที่ช่วยเอื้ออำนวยต่อการสื่อสารได้อย่างดี เช่น ระบบไอพีสตาร์ ใยแก้วนำแสง (Fiber Optic) จานดาวเทียม

2.1.5.รูปแบบของการเชื่อมโยงเครือข่าย หรือโทโปโลยี (LAN Topology)

โทโปโลยี คือ ลักษณะทางกายภาพ (ภายนอก) ของระบบเครือข่าย ซึ่งหมายถึง ลักษณะของการเชื่อมโยงสายสื่อสารเข้ากับอุปกรณ์ อิเล็กทรอนิกส์และเครื่องคอมพิวเตอร์ ภายในเครือข่ายด้วยกันนั่นเอง โทโปโลยีของเครือข่ายท้องถิ่นแต่ละแบบมีความเหมาะสมในการใช้งาน แตกต่างกันออกไป การนำไปใช้จึงมีความจำเป็นที่เราจะต้องทำการศึกษาลักษณะและคุณสมบัติ ข้อดีและข้อเสียของโทโปโลยีแต่ละแบบเพื่อนำไปใช้ในการออกแบบพิจารณาระบบเครือข่ายให้เหมาะสมกับการใช้งานรูปแบบของโทโปโลยีของเครือข่ายหลักๆ มีดังต่อไปนี้

1.โทโปโลยีแบบบัส (Bus)

เป็นรูปแบบที่ เครื่องคอมพิวเตอร์จะถูกเชื่อมต่อกันโดยผ่านสายสัญญาณแกนหลักที่เรียกว่าบัส หรือแบ็คโบน คือ สายรับส่งสัญญาณข้อมูลหลักใช้เป็นทางเดินข้อมูลของทุกเครื่องภายในระบบเครือข่ายและจะมีสายแยกย่อยออกไปในแต่ละจุด เพื่อเชื่อมต่อเข้ากับคอมพิวเตอร์เครื่องอื่นๆซึ่งเรียกว่าโหนด ข้ อมูลจากโหนดผู้ส่งจะถูกส่งเข้าสู่สายบัสในรูปของแพ็กเก็ต ซึ่งแต่ละแพ็กเก็ตจะประกอบไปด้วยข้อมูลของผู้ส่ง, ผู้รับ และข้อมูลที่จะส่ง การสื่อสารภายในสายบัสจะเป็นแบบ 2 ทิศทางแยกไปยังปลายทั้ง 2 ด้านของบัส โดยตรงปลายทั้ง 2 ด้านของบัส จะมีเทอร์มิเนเตอร์ ทำหน้าที่ลบล้างสัญญาณที่ส่งมาถึง เพื่อป้องกันไม่ให้สัญญาณข้อมูลนั้นสะท้อนกลับ เข้ามายังบัสอีก เพื่อเป็นการป้องกันการชนกันของข้อมูลอื่นๆ ที่เดินทางอยู่บนบัสในขณะนั้น สัญญาณข้อมูลจากโหนดผู้ส่งเมื่อเข้าสู่บัส ข้อมูลจะไหลผ่านไปยังปลายทั้ง 2 ด้านของบัส แต่ละโหนดที่เชื่อมต่อเข้ากับบัส จะคอยตรวจดูว่า ตำแหน่งปลายทางที่มากับแพ็กเก็ตข้อมูลนั้นตรงกับตำแหน่งของตนหรือไม่ถ้าตรง ก็จะรับข้อมูลนั้นเข้ามาสู่โหนด ตน แต่ถ้าไม่ใช่ ก็จะปล่อยให้สัญญาณข้อมูลนั้นผ่านไป จะเห็นว่าทุกๆโหนดภายในเครือข่ายแบบ บัส นั้นสามารถรับรู้สัญญาณข้อมูลได้ แต่จะมีเพียงโหนดปลายทางเพียงโหนดเดียวเท่านั้นที่จะรับข้อมูลนั้นไปได้

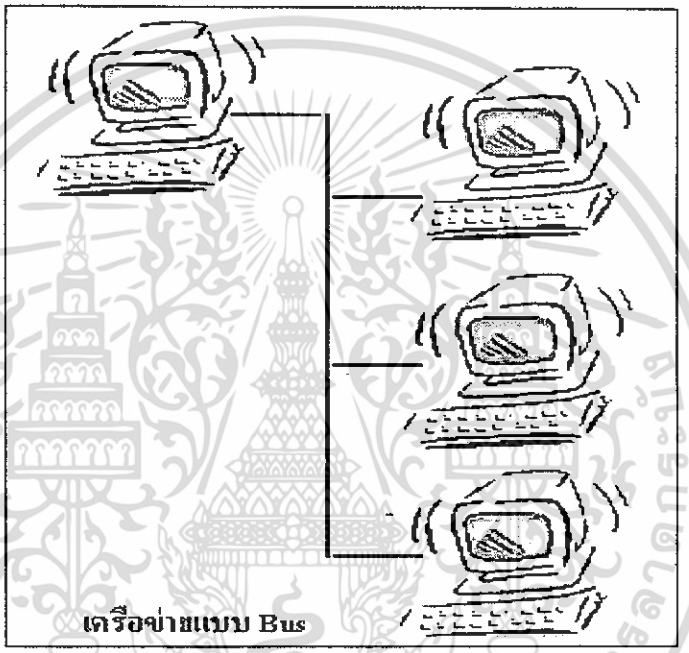
- ข้อดี

- ไม่ต้องเสียค่าใช้จ่ายในการวางสายสัญญาณมากนักสามารถขยายระบบได้ง่ายเสียค่าใช้จ่ายน้อย ซึ่งถือว่าระบบบัสนี้เป็นแบบโทโปโลยีที่ได้รับความนิยมใช้กันมากที่สุดมา ตั้งแต่อดีตจนถึงปัจจุบัน เหตุผลอย่างหนึ่งก็คือสามารถติดตั้งระบบ ดูแลรักษา และติดตั้งอุปกรณ์เพิ่มเติมได้ง่ายไม่ต้องใช้เทคนิคที่ยุ่งยากซับซ้อนมากนัก

- ข้อเสีย

- อาจเกิดข้อผิดพลาดง่าย เนื่องจากทุกเครื่องคอมพิวเตอร์ต่ออยู่บนสายสัญญาณเพียงเส้นเดียว ดังนั้นหากมีสายสัญญาณขาดที่ตำแหน่งใดตำแหน่งหนึ่งก็จะทำให้เครื่องบางเครื่อง หรือทั้งหมดในระบบไม่สามารถใช้งานได้ตามไปด้วย

- การตรวจหาโหนดเสียทำได้ยากเนื่องจากขณะใดขณะหนึ่งจะมีคอมพิวเตอร์เพียงเครื่องเดียวเท่านั้นที่สามารถส่งข้อความออกมาบนสายสัญญาณดังนั้นถ้ามีเครื่องคอมพิวเตอร์จำนวนมากๆอาจทำให้เกิดการคับคั่งของเครือข่ายซึ่งจะทำให้ระบบช้าลงได้



รูปที่ 2.1 แสดงเครือข่ายแบบบัส

2.โทโปโลยีแบบวงแหวน (Ring)

เป็นรูปแบบที่เครื่องคอมพิวเตอร์ทุกเครื่องในระบบเครือข่ายทั้งเครื่องที่เป็นผู้ให้บริการและ เครื่องที่เป็นผู้ขอใช้บริการทุกเครื่องถูกเชื่อมต่อกันเป็นวงกลม ข้อมูลข่าวสารที่ส่งระหว่างกันจะไหลวนอยู่ในเครือข่ายไปในทิศทางเดียวกันโดยไม่มีจุดปลายหรือเทอร์มิเนเตอร์เช่นเดียวกับเครือข่ายแบบบัส ในแต่ละโหนดหรือแต่ละเครื่องจะมีรีพีตเตอร์ ประจำแต่ละเครื่อง 1 ตัวซึ่งจะทำหน้าที่เพิ่มเติมข้อมูลที่จำเป็นต่อการติดต่อสื่อสารเข้าในส่วนหัวของแพ็กเก็ตที่ส่งและตรวจสอบข้อมูลจากส่วนหัวของแพ็กเก็ต ที่ส่งมาถึงว่าเป็นข้อมูลของตนหรือไม่แต่ถ้าไม่ใช่ก็จะปล่อยข้อมูลนั้นไปยังรีพีตเตอร์ของเครื่องถัดไป

- ข้อดี

- ผู้ส่งสามารถส่งข้อมูลไปยังผู้รับได้หลายๆเครื่องพร้อมๆกันโดยกำหนดตำแหน่งปลายทางเหล่านั้นลงในส่วนหัวของแพ็กเก็ตข้อมูลรีพีตเตอร์ของแต่ละเครื่องจะทำการตรวจสอบเองว่าข้อมูลที่ส่งมาให้นั้นเป็นตนเองหรือไม่

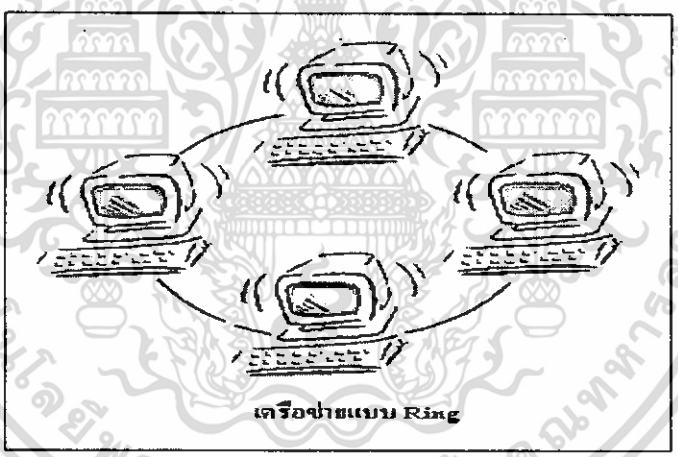
- การส่งผ่านข้อมูลในเครือข่ายแบบวงแหวนจะเป็นไปในทิศทางเดียวจากเครื่องสู่เครื่องจึงไม่มีการชนกันของสัญญาณข้อมูลที่ส่งออกไป

- คอมพิวเตอร์ทุกเครื่องในเครือข่ายมีโอกาสที่จะส่งข้อมูลได้อย่างทัดเทียมกัน

- ข้อเสีย

- ถ้ามีเครื่องใดเครื่องหนึ่งในเครือข่ายเสียหายข้อมูลจะไม่สามารถส่งผ่านไปยังเครื่องต่อๆไปได้และจะทำให้เครือข่ายทั้งเครือข่ายหยุดชะงักได้

- ขณะที่ข้อมูลถูกส่งผ่านแต่ละเครื่องเวลาส่วนหนึ่งจะสูญเสียไปกับการที่ทุกๆรีพีตเตอร์ จะต้องทำการตรวจสอบตำแหน่งปลายทางของข้อมูลนั้นๆ ทุกข้อมูลที่ส่งผ่านมาถึง



รูปที่ 2.2 แสดงเครือข่ายแบบวงแหวน

3.โทโปโลยีแบบดาว (Star)

เป็นรูปแบบที่เครื่องคอมพิวเตอร์ทุกเครื่องที่เชื่อมต่อเข้าด้วยกันในเครือข่ายจะต้องเชื่อมต่อกับอุปกรณ์ตัวกลางตัวหนึ่งที่เรียกว่า ฮับ หรือเครื่องๆหนึ่งซึ่งทำหน้าที่เป็นศูนย์กลางของการเชื่อมต่อสายสัญญาณที่มาจากเครื่องต่างๆในเครือข่ายและควบคุมเส้นทางการสื่อสารทั้งหมดเมื่อมีเครื่องที่ต้องการส่งข้อมูลไปยังเครื่องอื่นๆที่ต้องการในเครือข่ายเครื่องนั้นก็จะต้องส่งข้อมูลมายังฮับหรือเครื่องศูนย์กลางก่อนแล้วฮับก็จะทำหน้าที่กระจายข้อมูลนั้นไปในเครือข่ายต่อไป

- ข้อดี

- การติดตั้งเครือข่ายและการดูแลรักษาทำได้ง่ายหากมีเครื่องใดเกิดความเสียหายก็สามารถตรวจสอบได้ง่ายและศูนย์กลางสามารถตัดเครื่องที่เสียหายนั้นออกจากการสื่อสารในเครือข่ายได้เลยโดยไม่มีผลกระทบกับระบบเครือข่าย

-ข้อเสีย

-เสียค่าใช้จ่ายมากทั้งในด้านของเครื่องที่จะใช้เป็นเครื่องศูนย์กลางหรือตัวฮับเองและค่าใช้จ่ายในการติดตั้งสายเคเบิลในเครื่องอื่นๆทุกเครื่องการขยายระบบให้ใหญ่ขึ้นทำได้ยากเพราะการขยายแต่ละครั้งจะต้องเกี่ยวเนื่องกับเครื่องอื่นๆทั้งระบบ

รูปที่ 2.3 แสดงเครือข่ายแบบดาว

4.โทโปโลยีแบบผสม (Hybrid)

เป็นรูปแบบใหม่ที่เกิดจากการผสมผสานกันของโทโปโลยีแบบ ดาว บัส วงแหวนเข้าด้วยกันเพื่อเป็นการลดข้อเสียของรูปแบบที่กล่าวมาและเพิ่มข้อดีขึ้นมามักจะนำมาใช้กับระบบเครือข่ายระยะไกลมากซึ่งการเชื่อมต่อกันของแต่ละรูปแบบนั้นต้องใช้ตัวเชื่อมสัญญาณเข้ามาเป็นตัวเชื่อมก็คือเราท์เตอร์เป็นตัวเชื่อมการติดต่อกัน

5.โทโปโลยีแบบ MESH

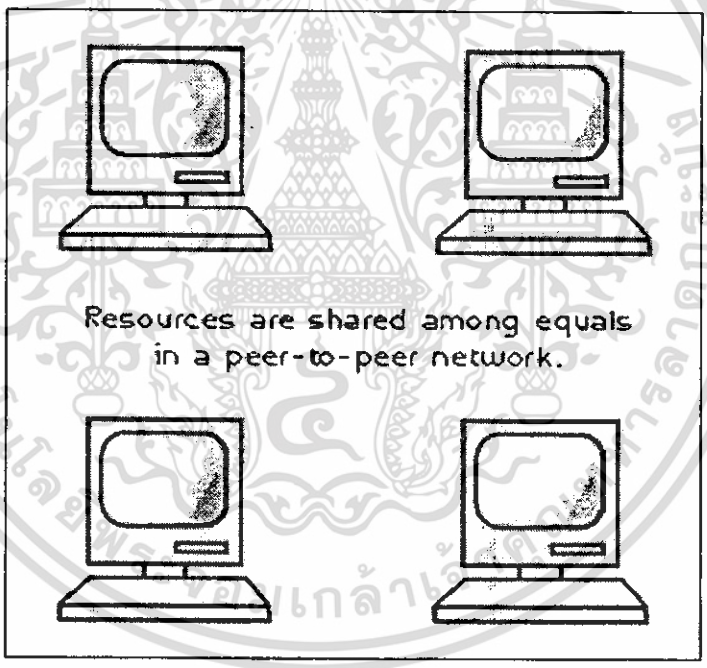
เป็นรูปแบบที่ถือว่าสามารถป้องกันการผิดพลาดที่อาจจะเกิดขึ้นกับระบบได้ดีที่สุดเป็นรูปแบบที่ใช้วิธีการเดินสายของแต่ละเครื่องไปเชื่อมการติดต่อกับทุกเครื่องในระบบเครือข่าย คือเครื่องทุกเครื่องในระบบเครือข่ายนี้ต้องมีสายไปเชื่อมกับทุกๆ เครื่องระบบนี้ยากต่อการเดินสายและมีราคาแพงจึงไม่ค่อยนิยมมากนัก

2.1.6. ประเภทของระบบเครือข่ายท้องถิ่น ซึ่งแบ่งตามลักษณะการทำงาน

ในการแบ่งรูปแบบการเชื่อมต่อระบบเครือข่ายท้องถิ่นนั้น สามารถแบ่งออกเป็น 2 ประเภทใหญ่ๆ ได้แก่การเชื่อมต่อแบบเพียร์-ทู-เพียร์ (Peer-To–Peer) และแบบไคลเอนท์/เซิร์ฟเวอร์ (Client / Server)

1. แบบเพียร์-ทู-เพียร์

เป็นการเชื่อมต่อเครื่องคอมพิวเตอร์เข้าด้วยกันโดยเครื่องคอมพิวเตอร์แต่ละเครื่องจะสามารถแบ่งทรัพยากรต่างๆไม่ว่าจะเป็นไฟล์หรือเครื่องพิมพ์ซึ่งกันและกันภายในเครือข่ายได้เครื่องแต่ละเครื่องจะทำงานในลักษณะที่ทัดเทียมกันไม่มีเครื่องใดเครื่องหนึ่งเป็นเครื่องหลักเหมือนแบบไคลเอนท์/เซิร์ฟเวอร์ แต่ก็ยังคงคุณสมบัติพื้นฐานของระบบเครือข่ายไว้เหมือนเดิมการเชื่อมต่อแบบนี้มักทำในระบบที่มีขนาดเล็กๆเช่น หน่วยงานขนาดเล็กที่มีเครื่องใช้ไม่เกิน 10เครื่องการเชื่อมต่อแบบนี้มีจุดอ่อนในเรื่องของระบบรักษาความปลอดภัย แต่ถ้าเป็นเครือข่ายขนาดเล็กและเป็นงานที่ไม่มีข้อมูลที่เป็นความลับมากนักเครือข่ายแบบนี้ก็เป็นรูปแบบที่น่าเลือกนำมาใช้ได้เป็นอย่างดี

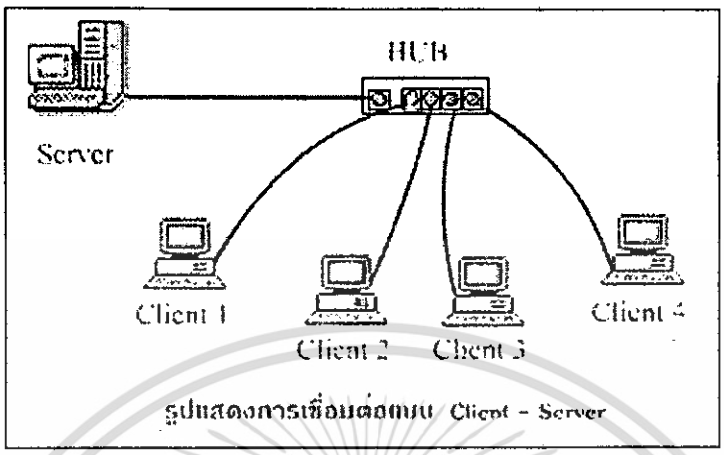


รูปที่ 2.4 แสดงการเชื่อมต่อแบบ เพียร์-ทู-เพียร์

2. แบบไคลเอนท์ / เซิร์ฟเวอร์

เป็นระบบที่มีเครื่องคอมพิวเตอร์ทุกเครื่องมีฐานะการทำงานที่เหมือนๆกันเท่าเทียมกันภายในระบบเครือข่าย แต่จะมีเครื่องคอมพิวเตอร์เครื่องหนึ่งที่ทำหน้าที่เป็นเครื่องเซิร์ฟเวอร์ที่ทำหน้าที่ให้บริการทรัพยากรต่างๆให้กับเครื่องที่ขอใช้บริการซึ่งอาจจะต้องเป็นเครื่องที่มีประสิทธิภาพที่ค่อนข้างสูงถึงจะทำให้การให้บริการมีประสิทธิภาพตามไปด้วยข้อดีของระบบเครือข่ายไคลเอนท์/เซิร์ฟเวอร์เป็นระบบที่มีการรักษาความปลอดภัยสูงกว่าระบบแบบ เพียร์-ทู-เพียร์เพราะว่าการจัดการในด้านรักษาความปลอดภัยนั้น

จะทำกันบนเครื่องเซิร์ฟเวอร์เพียงเครื่องเดียวทำให้ดูแลรักษาง่ายและสะดวก มีการกำหนดสิทธิการเข้าใช้ทรัพยากรต่างๆให้กับเครื่องผู้ขอใช้บริการหรือเครื่องไคลเอนท์

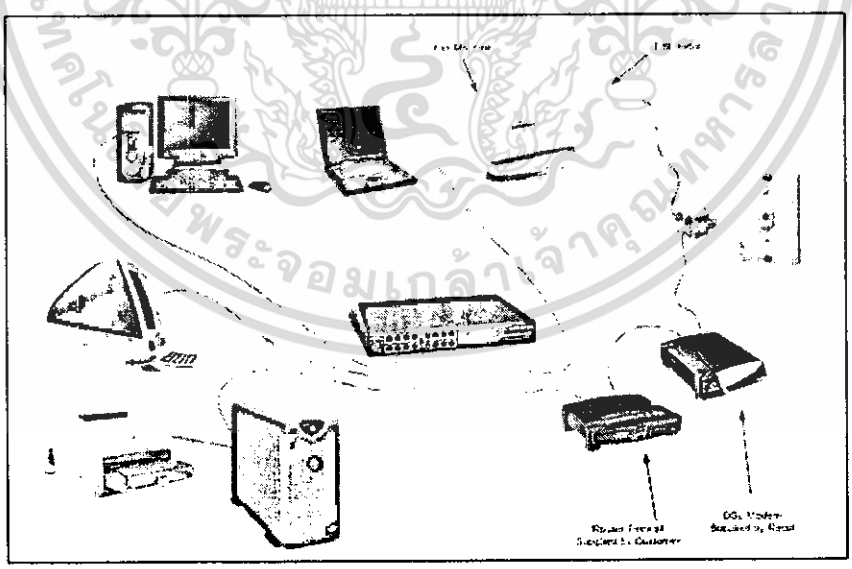


รูปที่ 2.5 แสดงการเชื่อมต่อแบบไคลเอนท์/เซิร์ฟเวอร์

2.1.7. อุปกรณ์ในการเชื่อมต่อ

1. ฮับ และสวิตช์ฮับ

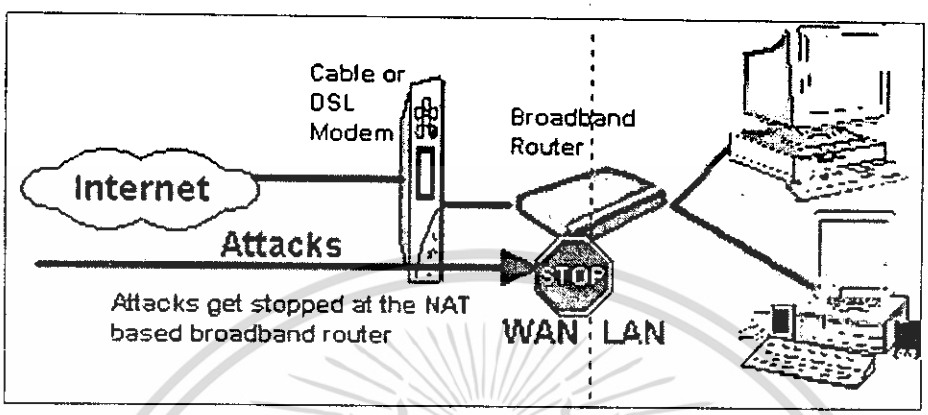
ทำหน้าที่ในการเชื่อมต่อคอมพิวเตอร์หลายๆเครื่องให้สามารถเชื่อมต่อกันและทำงานร่วมกันได้ ส่วนมากจะนำมาใช้ในการต่อในระบบเครือข่ายแบบดาวโดยอุปกรณ์ชนิดนี้จะคอยส่งข้อมูลจากเครื่องต้นทางไปยังเครื่องคอมพิวเตอร์ปลายทางตามพอร์ตหรือช่องทางที่ถูกเลือกไว้



รูปที่2.6 แสดงอุปกรณ์แบบฮับ และ สวิตช์ฮับ

2. เราท์เตอร์

เป็นอุปกรณ์ที่ใช้เชื่อมต่อระหว่างเครือข่ายระหว่างระบบเครือข่ายภายในกับระบบเครือข่ายอินเตอร์เน็ต หรือระหว่างเครือข่ายสำนักงานใหญ่กับสำนักงานสาขา เช่น ระหว่างตู้เอทีเอ็ม กับ ธนาคาร



รูปที่ 2.7 แสดงอุปกรณ์แบบ เราท์เตอร์

2.1.8. เครือข่ายท้องถิ่นแบบไร้สาย (Wireless LAN)

ประเภทของระบบเครือข่ายมีอีกรูปแบบหนึ่งที่กำลังเป็นที่นิยมใช้กันในปัจจุบันก็คือการเชื่อมต่อเครือข่ายแบบไร้สาย เป็นเทคโนโลยีที่นำมาใช้ได้อย่างกว้างขวางเหมาะที่จะใช้ได้ทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพาซึ่งการส่งสัญญาณติดต่อกันนั้นจะใช้สัญญาณวิทยุเป็นพาหะ ดังนั้นความเร็วในการส่งข้อมูลก็จำเป็นต้องขึ้นอยู่กับระยะทางระยะทางยิ่งไกลความเร็วในการส่งข้อมูลก็ทำให้ช้าลงไปด้วยเครือข่ายไร้สายจึงเหมาะที่จะนำมาใช้กับงานที่ต้องการความคล่องตัวในการปฏิบัติงานที่สามารถเคลื่อนที่ไปที่ใดก็ได้ภายในขอบเขตของระยะทางที่กำหนด จุดเด่นๆ ของเครือข่ายแบบไร้สาย มีดังนี้

- การเคลื่อนที่ทำได้สะดวกสามารถใช้ระบบเครือข่ายท้องถิ่นจากที่ใดก็ได้และสามารถเข้าถึงข้อมูลได้แบบเรียลไทม์ ได้อีกด้วย
- การติดตั้งใช้งานง่าย และรวดเร็วไม่ต้องเดินสายสัญญาณให้ยุ่งยาก
- การติดตั้งและการขยายระบบทำได้อย่างกว้างขวางเพราะสามารถขยายไปติดตั้งใช้งานในพื้นที่ที่สายสัญญาณเข้าไม่ถึง
- เสียค่าใช้จ่ายลดน้อยลงเพราะว่าในปัจจุบันการส่งสัญญาณของเครือข่ายแบบไร้สายทำได้ไกลมากยิ่งขึ้นสามารถส่งได้ไกลกว่า10 กิโลเมตรทำให้ลดค่าใช้จ่ายในส่วนของการเช่าสายสัญญาณลงไปได้เป็นอย่างมาก
- มีความยืดหยุ่นในการใช้งานและการติดตั้งสามารถปรับแต่งระบบให้ใช้ได้กับทุกโทโปโลยี เลยทีเดียวการปรับปรุงเครือข่ายทำได้ง่าย

2.1.9. มาตรฐานของ เครือข่ายแบบไร้สายตามมาตรฐานสากล 802.11

IEEE802.11a

เป็นมาตรฐานที่ได้รับการตีพิมพ์และเผยแพร่เมื่อปี พ.ศ.2542โดยใช้เทคโนโลยี OFDM (Orthogonal Frequency Division Multiplexing) เพื่อพัฒนาให้ผลิตภัณฑ์ไร้สายมีความสามารถในการรับส่งข้อมูลด้วยอัตราความเร็วสูงสุด 54 เมกะบิตต่อวินาทีโดยใช้คลื่นวิทยุย่านความถี่ 5 กิกะเฮิรตซ์ ซึ่งเป็นย่านความถี่ที่ไม่ได้รับอนุญาตให้ใช้งานโดยทั่วไปในประเทศไทยเนื่องจากสงวนไว้สำหรับกิจการทางด้านดาวเทียม ข้อเสียของผลิตภัณฑ์มาตรฐาน IEEE 802.11a ก็คือมีรัศมีการใช้งานในระยะสั้นและมีราคาแพง ดังนั้นผลิตภัณฑ์ไร้สายมาตรฐาน IEEE 802.11a จึงได้รับความนิยมน้อย

IEEE802.11b

เป็นมาตรฐานที่ถูกตีพิมพ์และเผยแพร่ออกมาพร้อมกับมาตรฐาน IEEE 802.11a เมื่อปี พ.ศ. 2542 ซึ่งเป็นที่รู้จักกันดีและได้รับความนิยมในการใช้งานกันอย่างแพร่หลายมากที่สุดผลิตภัณฑ์ที่ออกแบบมาให้รองรับมาตรฐาน IEEE 802.11b ใช้เทคโนโลยีที่เรียกว่า CCK (Complimentary Code Keying) ร่วมกับเทคโนโลยี DSSS (Direct Sequence Spread Spectrum) เพื่อให้สามารถรับส่งข้อมูลได้ด้วยอัตราความเร็วสูงสุดที่ 11 เมกะบิตต่อวินาที โดยใช้คลื่นสัญญาณวิทยุย่านความถี่ 2.4 กิกะเฮิรตซ์ ซึ่งเป็นย่านความถี่ที่อนุญาตให้ใช้งานในแบบสาธารณะทางด้านวิทยาศาสตร์ อุตสาหกรรม และการแพทย์ โดยผลิตภัณฑ์ที่ใช้ความถี่ย่านนี้มีทั้งผลิตภัณฑ์ที่รองรับเทคโนโลยี บลูทูธ โทรศัพท์ไร้สายและไมโครเวฟ จึงทำให้การใช้งานนั้นมีปัญหาในเรื่องของสัญญาณรบกวนของผลิตภัณฑ์เหล่านี้ ข้อดีของมาตรฐาน IEEE 802.11b ก็คือสนับสนุนการใช้งานเป็นบริเวณกว้างกว่ามาตรฐาน IEEE 802.11a ผลิตภัณฑ์มาตรฐาน IEEE 802.11b เป็นที่รู้จักในเครื่องหมายการค้า Wi-Fi ซึ่งกำหนดขึ้นโดย WECA (Wireless Ethernet Compatability Alliance) โดยผลิตภัณฑ์ที่ได้รับเครื่องหมาย Wi-Fi ได้ผ่านการตรวจสอบและรับรองว่าเป็นไปตามข้อกำหนดของมาตรฐาน IEEE 802.11b ซึ่งสามารถใช้งานร่วมกันกับผลิตภัณฑ์ของผู้ผลิตรายอื่นๆได้

IEEE 802.11g

เป็นมาตรฐานที่นิยมใช้งานกันมากในปัจจุบันและได้เข้ามาทดแทนผลิตภัณฑ์ที่รองรับมาตรฐาน IEEE 802.11b เนื่องจากสนับสนุนอัตราความเร็วของการรับส่งข้อมูลในระดับ 54 เมกะบิตต่อวินาทีโดยใช้เทคโนโลยี OFDM บนคลื่นสัญญาณวิทยุย่านความถี่ 2.4 กิกะเฮิรตซ์และให้รัศมีการทำงานที่มากกว่า IEEE 802.11a พร้อมความสามารถในการใช้งานร่วมกันกับมาตรฐาน IEEE 802.11b ได้

IEEE 802.11e

เป็นมาตรฐานที่ออกแบบมาสำหรับการใช้งานแอพพลิเคชันทางด้านมัลติมีเดียอย่างVoIP (Voice over IP) เพื่อควบคุมและรับประกันคุณภาพของการใช้งานตามหลักการ QoS (Quality of Service) โดยการปรับปรุง ชั้นแม็ค (MAC Layer) ให้มีคุณสมบัติในการรับรองการใช้งานให้มีประสิทธิภาพ

IEEE 802.11f

มาตรฐานนี้เป็นที่รู้จักกันในนาม IAPP (Inter Access Point Protocol) ซึ่งเป็นมาตรฐานที่ออกแบบมาสำหรับจัดการกับผู้ใช้งานที่เคลื่อนที่ข้ามเขตการให้บริการของ แอ็กเซสพอยต์ ตัวหนึ่งไปยัง แอ็กเซสพอยต์เพื่อให้บริการในแบบโรมมิงสัญญาณระหว่างกัน

IEEE 802.11h

มาตรฐานที่ออกแบบมาสำหรับผลิตภัณฑ์เครือข่ายไร้สายที่ใช้งานย่านความถี่ 5 กิกะเฮิรตซ์ให้ทำงานถูกต้องตามข้อกำหนดการใช้ความถี่ของประเทศในทวีปยุโรป

IEEE802.11i

เป็นมาตรฐานในด้านการรักษาความปลอดภัยของผลิตภัณฑ์เครือข่ายไร้สาย โดยการปรับปรุงชั้นแม็ค เนื่องจากระบบเครือข่ายไร้สายมักมีปัญหาในการใช้งานโดยเฉพาะฟังก์ชันการเข้ารหัสแบบ WEP 64/128-bit ซึ่งใช้คีย์ที่ไม่มีการเปลี่ยนแปลง ซึ่งไม่เพียงพอสำหรับสภาพการใช้งานที่ต้องการความมั่นใจในการรักษาความปลอดภัยของการสื่อสารระดับสูง มาตรฐาน IEEE 802.11i จึงกำหนดเทคนิคการเข้ารหัสที่ใช้คีย์ชั่วคราวด้วย WPA (Wi-Fi Protected Privacy), WPA2 และการเข้ารหัสในแบบ AES (Advanced Encryption Standard) ซึ่งมีความน่าเชื่อถือสูง

IEEE802.11k

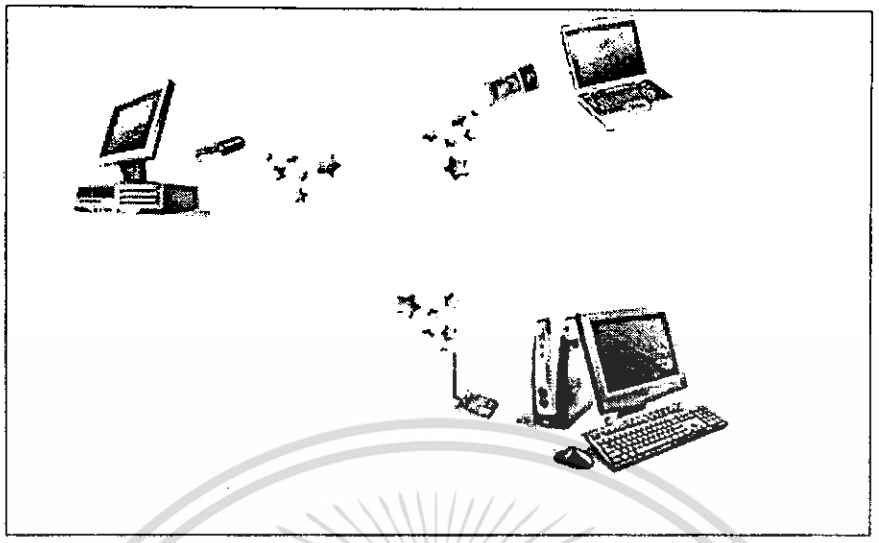
เป็นมาตรฐานที่ใช้จัดการการทำงานของระบบเครือข่ายไร้สาย ทั้งจัดการการใช้งานคลื่นวิทยุให้มีประสิทธิภาพ มีฟังก์ชันการเลือกช่องสัญญาณ, การโรมมิงและการควบคุมกำลังส่ง นอกจากนั้นก็ยังมีการร้องขอและ ปรับแต่งค่าให้เหมาะสมกับการทำงาน การหารัสมีการใช้งานสำหรับเครื่องไคลเอนท์ที่เหมาะสมที่สุดเพื่อให้ระบบจัดการสามารถทำงานจากศูนย์กลางได้

IEEE802.11n

เป็นมาตรฐานของผลิตภัณฑ์เครือข่ายไร้สายที่คาดหมายกันว่าจะเข้ามาแทนที่มาตรฐาน IEEE 802.11a, IEEE 802.11b และ IEEE 802.11g ที่ใช้งานกันอยู่ในปัจจุบัน โดยให้อัตราความเร็วในการรับส่งข้อมูลในระดับ 100 เมกะบิตต่อวินาที

IEEE 802.1x

เป็นมาตรฐานที่ใช้งานกับระบบรักษาความปลอดภัย ซึ่งก่อนเข้าใช้งานระบบเครือข่ายไร้สายจะต้องตรวจสอบสิทธิ์ในการใช้งานก่อน โดย IEEE 802.1x จะใช้โปรโตคอลอย่าง LEAP, PEAP, EAP-TLS, EAP-FAST ซึ่งรองรับการตรวจสอบผ่านเซิร์ฟเวอร์ เช่น RADIUS, Kerberos เป็นต้น

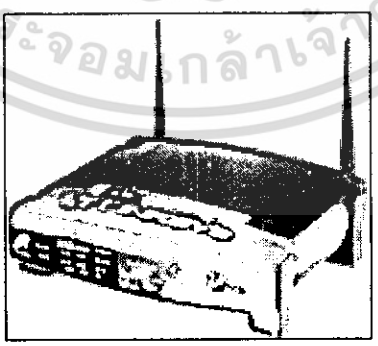


รูปที่ 2.8 แสดงการเชื่อมต่อแบบเครือข่ายไร้สาย

2.1.10. อุปกรณ์เครือข่ายไร้สาย (Wireless Device)

1. แอ็กเซสพอยต์ (Access Point)

เป็นอุปกรณ์กระจายสัญญาณไปยังอุปกรณ์รับ-ส่งสัญญาณในเครือข่ายโดยที่ตัวแอ็กเซสพอยต์ทำหน้าที่เหมือนกับสวิตช์ ในระบบเครือข่ายใช้สายซึ่งมีอุปกรณ์บางรุ่นที่ทำหน้าที่เป็นสวิตท์ให้กับระบบเครือข่ายใช้สายปกติโดยจะมี พอร์ต RJ45 รวมอยู่ด้วย 4-8 พอร์ตดังแสดงในรูปที่ 2.9 นอกจากนี้ยังอาจเพิ่มความสามารถในการเป็นปริ้นเซิร์ฟเวอร์ หรือเราท์เตอร์ เข้าไปด้วย



รูปที่ 2.9 แสดงแอ็กเซสพอยต์แบบไร้สาย

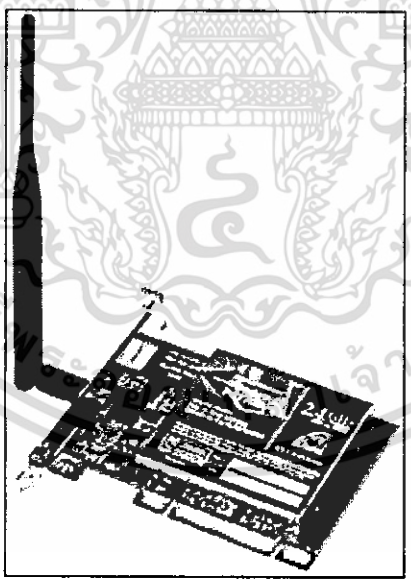
2. การ์ดเอ็มซีไอเอ (MCIA)

เป็นอุปกรณ์รับ-ส่งสัญญาณที่ใช้ติดตั้งกับคอมพิวเตอร์แบบพกพา เพื่อให้สามารถ เชื่อมต่อรับสัญญาณจากแอ็กเซสพอยต์ หรืออุปกรณ์ไร้สายอื่นๆซึ่งทำหน้าที่เหมือนกับการ์ดแลนแบบ PCMCIA ทั่วไปดังแสดงในรูปที่2.10

รูปที่ 2.10 แสดงการ์ดแบบเอ็มซีไอเอ

3. การ์ดพีซีไอ (PCI Card)

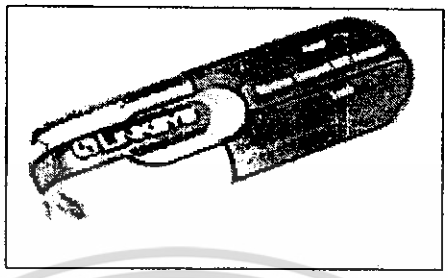
ใช้ติดตั้งลงบนช่องซีไอบนเครื่องคอมพิวเตอร์ลักษณะเดียวกับการ์ดแลนแต่ส่งสัญญาณผ่านเสาอากาศที่ติดตั้งมาด้วยแทนการส่งสัญญาณผ่านสายทองแดงดังแสดงในรูปที่ 2.11



รูปที่ 2.11 แสดงการ์ดแบบพีซีไอ

4. ยูเอสบี (USB)

ใช้ติดตั้ง กับพอร์ตยูเอสบีทำงานในลักษณะเดียวกับการ์ดแลนแต่ส่งสัญญาณผ่านเสาอากาศที่ติดตั้งมาด้วยแทนการส่งสัญญาณผ่านสายทองแดงดังแสดงในรูปที่ 2.12



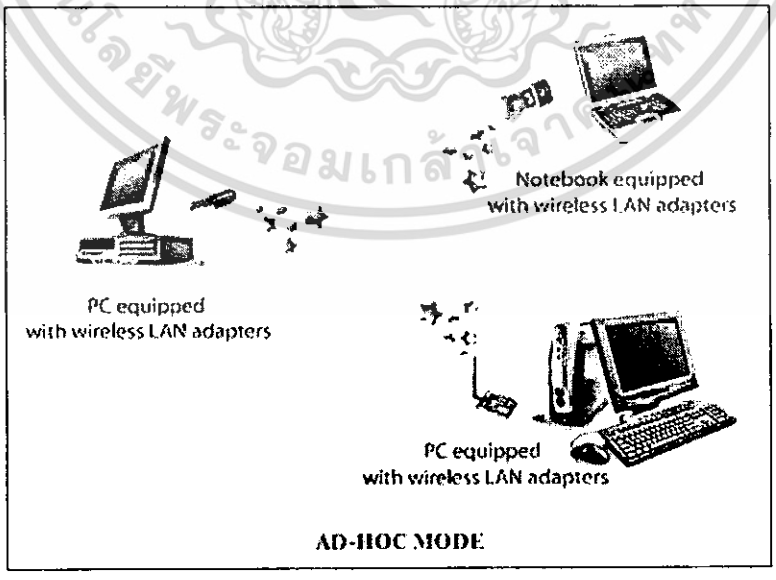
รูปที่ 2.12 แสดงยูเอสบีแบบไร้สาย

2.1.11. รูปแบบการติดตั้ง/ออกแบบเครือข่ายไร้สาย

เครือข่ายไร้สายแบ่งการทำงานออกเป็นสองลักษณะ คือ

1.โหมดแอดฮอค (Ad-Hoc Mode)

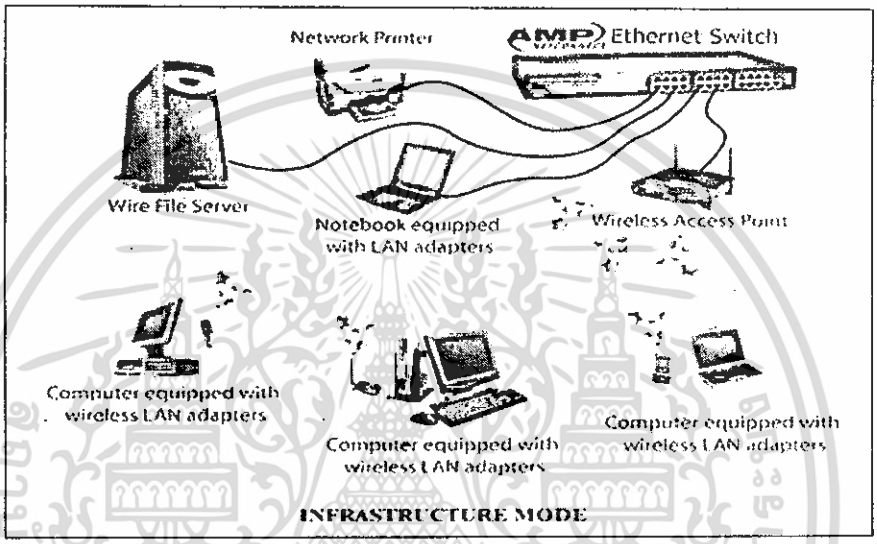
เป็นการทำงานในลักษณะที่ มีการติดตั้งแอ็กเซสพอยต์ เข้าไปในระบบเครือข่ายสายทองแดงเพื่อกระจายสัญญาณไปยังเครื่องคอมพิวเตอร์ที่ติดตั้ง อุปกรณ์ไร้สายอยู่การทำงานในลักษณะนี้เป็นที่นิยมแพร่หลายเนื่องจากสามารถใช้งานร่วมกับระบบ สายทองแดงและยังดัดแปลงใช้งานร่วมกับอุปกรณ์ที่มีอยู่เดิมโดยไม่ต้อง ติดตั้งอุปกรณ์ไร้สายอื่นเพิ่มเติม มากเกินความจำเป็น ดังแสดงในรูปที่ 2.13



รูปที่ 2.13 แสดงแอ็กเซสพอยต์แบบโหมดแอดฮอค

2.โหมดอินฟราสซัคเจอร์ (Infrastructure Mode)

เป็นการทำงานในลักษณะที่มีการติดตั้ง แอ็กเซสพอยต์ เข้าไปในระบบเครือข่ายสายทองแดงเพื่อกระจายสัญญาณไปยัง เครื่องคอมพิวเตอร์ที่ติดตั้งอุปกรณ์ไร้สายอยู่การทำงานในลักษณะนี้เป็นที่นิยมแพร่หลายเนื่องจาก สามารถใช้งานร่วมกับระบบสายทองแดงและยังดัดแปลงใช้งานร่วมกับอุปกรณ์ที่มีอยู่เดิมโดยไม่ต้องติดตั้งอุปกรณ์ไร้สายอื่นเพิ่มเติม มากเกิน ความจำเป็นดังแสดงในรูปที่ 2.14

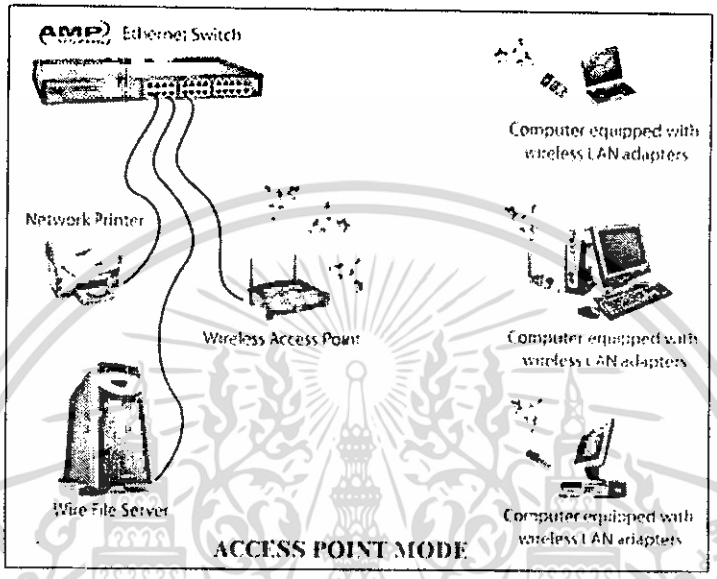


รูปที่ 2.14 แสดงแอ็กเซสพอยต์แบบโหมดอินฟราสซัคเจอร์

2.1.12.รูปแบบการใช้งาน

1.โหมดแอ็กเซสพอยต์ (Access Point Mode)

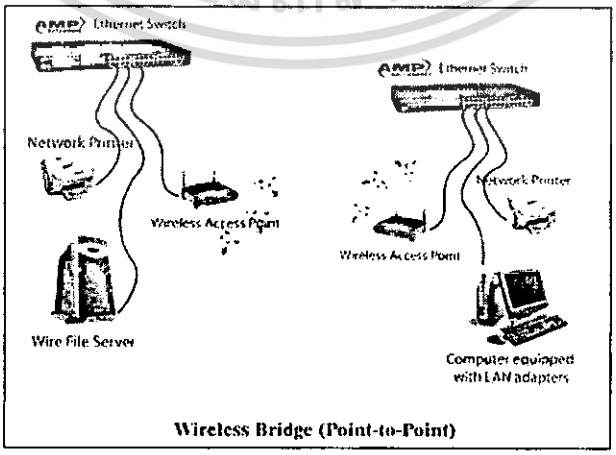
คือการใช้งานโดยมีแอ็กเซสพอยต์เชื่อมต่อระหว่างเครือข่ายไร้สายกับเครือข่ายสายทองแดงเป็นลักษณะการทำงานที่นิยมใช้กันมากที่สุดดังแสดงในรูปที่ 2.15



รูปที่ 2.15 แสดงการต่อใช้งานแบบโหมดแอ็กเซสพอยต์

2. บริดจ์ไร้สาย (Wireless Bridge)

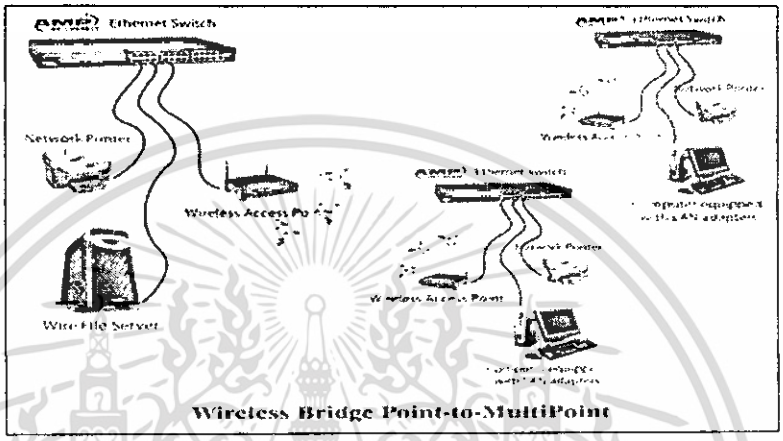
เป็นการทำงานในลักษณะที่มีการติดตั้งแอ็กเซสพอยต์เข้าไปในระบบเครือข่ายสายทองแดงเพื่อกระจายสัญญาณไปยังเครื่องคอมพิวเตอร์ที่ติดตั้งอุปกรณ์ไร้สายอยู่ การทำงานในลักษณะนี้เป็นที่นิยมแพร่หลายเนื่องจากสามารถใช้งานร่วมกับระบบสายทองแดง และยังดัดแปลงใช้งานร่วมกับอุปกรณ์ที่มีอยู่เดิมโดยไม่ต้องติดตั้งอุปกรณ์ไร้สายอื่นเพิ่มเติม มากเกินความจำเป็นดังแสดงในรูปที่ 2.16



รูปที่ 2.16 แสดงการต่อใช้งานแบบบริดจ์ไร้สาย

3. แบบบริดจ์ไร้สายจุดต่อหลายจุด (Wireles Bridge Point-to-Multipoint)

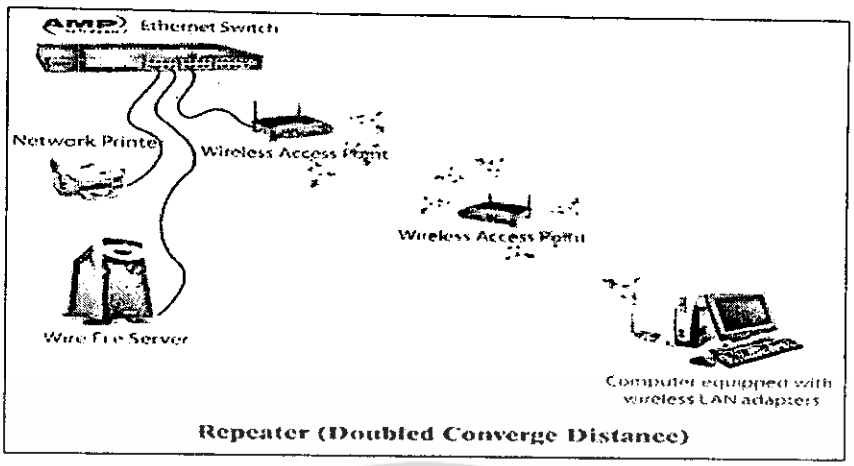
แอ็กเซสพอยต์ แบบไร้สายทำงานในลักษณะเดียวกับแบบจุดต่อจุด คือเชื่อมต่อเครือข่ายสายทองแดงเข้าด้วยกันแต่มีการทำงานร่วมกันมากกว่าสองเครือข่ายดังนั้นแอ็กเซสพอยต์ แบบไร้สายแต่ละตัวจะมีการรับส่งสัญญาณถึงกันโดยตรงดังแสดงในรูปที่ 2.17



รูปที่ 2.17 แสดงการต่อใช้งานแบบบริดจ์ไร้สายจุดต่อหลายจุด

4.โหมดรีพีตเตอร์ (Repeater Mode)

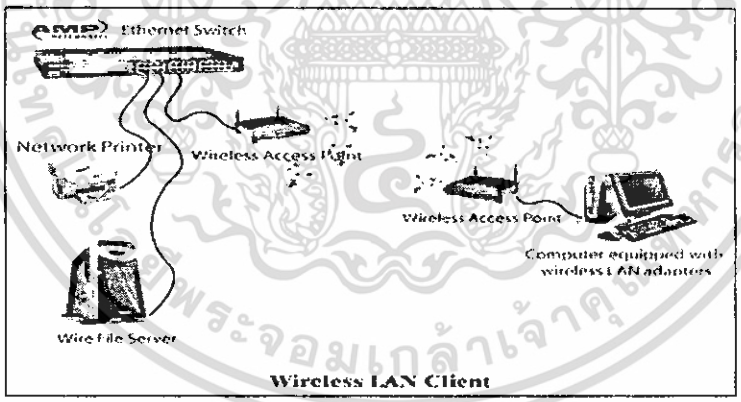
เนื่องจากการทำงานด้วยอุปกรณ์ไร้สายปัจจุบัน แอ็กเซสพอยต์ แบบไร้สายปกติ ที่มีขายในท้องตลาดมีรัศมีการส่งสัญญาณภายในอาคารอยู่ที่ 90-120 เมตร และภายนอกอาคาร 300-400 เมตร ถ้าหากมีความต้องการใช้งานที่เกินกว่าข้อจำกัดนี้ จึงจำเป็นต้องมีการเพิ่ม แอ็กเซสพอยต์เข้าไปเพื่อทำการทวนสัญญาณให้ได้ระยะทางการส่งข้อมูลที่ไกลกว่าเดิมแต่การทำงานในลักษณะนี้ทำให้เครือข่ายทั้งสองติดต่อกันด้วยความเร็วไม่แน่นอนและประสิทธิภาพการทำงานลดลงจึงมีการผลิตอุปกรณ์ไร้สายที่ส่งสัญญาณได้ไกลกว่าปกติขึ้นหรืออาจมีการติดตั้งเสาอากาศชนิดพิเศษเข้าไปเพื่อเพิ่มระยะทางได้อีกทางเลือกหนึ่งดังแสดงในรูปที่ 2.18



รูปที่ 2.18 แสดงการต่อใช้งานแบบรีพีตเตอร์โหมด

5. เครือข่ายไร้สายของเครื่องลูกข่าย (Wireless LAN Client)

ในโมเดลการทำงานนี้เป็นการส่งสัญญาณจากเครือข่ายโดย แอ็กเซสพอยต์แบบไร้สายไปยังแอ็กเซสพอยต์แบบไร้สายอีกตัวหนึ่งที่ติดตั้งอยู่กับเครื่องคอมพิวเตอร์เสมือนกับว่าแอ็กเซสพอยต์ตัวนั้นทำงานเป็นอุปกรณ์ไร้สายพีซีไอ การ์ดพีซี ยูเอสบีอาจใช้ในช่วงเริ่มต้น เพื่อขยายจำนวนผู้ใช้งานแบบไร้สายในอนาคตดังแสดงในรูปที่ 2.19



รูปที่ 2.19 แสดงการต่อใช้งานแบบเครือข่ายไร้สายของเครื่องลูกข่าย

2.2. อีเทอร์เน็ต (Ethernet)

อีเทอร์เน็ตนั้นเป็นมาตรฐานการส่งข้อมูลที่อนุญาตให้เครื่องคอมพิวเตอร์ใช้ช่องสัญญาณร่วมกัน โดยผลัดกันใช้อุปกรณ์ที่ใช้ในการส่งสัญญาณของอีเทอร์เน็ตนั้นก็คือ การ์ดแลน สายแลน และ อุปกรณ์รวมสัญญาณถ้าเป็นการเชื่อมต่อแบบบัสจะใช้สายสัญญาณกลางหรือแบ็คโบนเป็นตัวรวมสัญญาณ แต่ถ้าเป็นการเชื่อมต่อแบบดาวจะใช้ฮับเป็นอุปกรณ์รวมสัญญาณในปัจจุบันนิยมใช้การเชื่อมต่ออีเทอร์เน็ตแบบดาวมากเนื่องจากความเร็วในการส่งข้อมูลและความสะดวกในการดูแลรักษา

ระบบเครือข่ายอีเทอร์เน็ต หมายถึง มาตรฐานในการเชื่อมคอมพิวเตอร์หลายเครื่อง (ตั้งแต่สองเครื่องขึ้นไป) เข้าด้วยกันเป็นระบบเครือข่ายสำหรับปฏิบัติการในแต่ละจุด (เช่นตามบ้าน หรือ สำนักงานต่างๆ) รวมทั้งระบบการสื่อสารที่ช่วยให้คอมพิวเตอร์เหล่านั้นสามารถใช้ข้อมูลและโปรแกรมต่างๆ ร่วมกันได้ด้วย

ในกรณีที่ คอมพิวเตอร์หลายเครื่องในห้องหรืออาคารเดียวกันระบบเครือข่ายอีเทอร์เน็ตจะสามารถช่วยเพิ่มประสิทธิภาพการทำงานของคอมพิวเตอร์เหล่านั้นได้เพราะหลังจากการสร้างระบบเครือข่ายอีเทอร์เน็ตขึ้นมาแล้วข้อมูลจะสามารถถ่ายโอนระหว่างคอมพิวเตอร์และเครื่องเซิร์ฟเวอร์ได้รวดเร็วขึ้นมาก อีกทั้งยังสามารถสั่งพิมพ์งานผ่านเครื่องพิมพ์หรือใช้โปรแกรมต่างๆรวมทั้งระบบต่อเชื่อมอินเตอร์เน็ตร่วมกันระหว่าง คอมพิวเตอร์ทุกเครื่องในเครือข่ายนั้นด้วย

จนถึงบัดนี้ระบบเครือข่ายนี้ก็ยังนับเป็นระบบยอดนิยมสำหรับธุรกิจน้อยใหญ่ทำให้เครือข่ายอีเทอร์เน็ตกลายเป็นระบบมาตรฐานอย่างหนึ่งในการสร้างระบบเครือข่ายคอมพิวเตอร์ในปัจจุบันแต่ระบบเครือข่ายอีเทอร์เน็ตก็เป็นอะไรที่มากกว่าแค่อุปกรณ์ฮาร์ดแวร์เพราะยังรวมถึงรูปแบบในการสื่อสาร และการถ่ายโอนข้อมูลต่างๆของคอมพิวเตอร์ที่เชื่อมโยงกันนั้นด้วยทั้งนี้คอมพิวเตอร์ที่ต่อเชื่อมด้วยระบบอีเทอร์เน็ตนี้จะส่งข้อมูลไปตามสายในรูปแบบของกลุ่มข้อมูลขนาดเล็กที่เรียกว่าแพ็กเก็ต (Packet) โดยในแพ็กเก็ตนั้นนอกจากมีข้อมูลต่างๆแล้วยังมีข้อมูลเกี่ยวกับที่อยู่ของคอมพิวเตอร์ที่เกี่ยวข้องกับการรับ-ส่งข้อมูลต่างๆ ด้วย

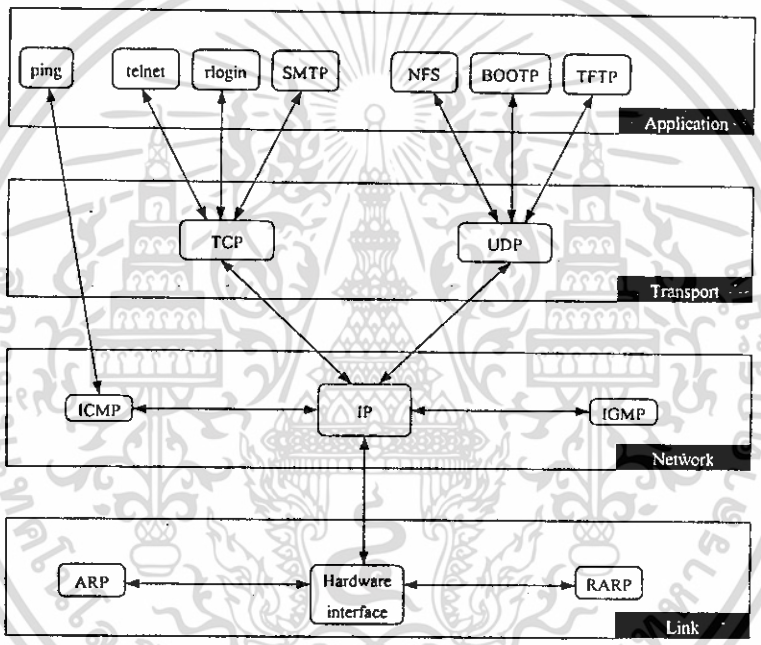
ในช่วงแรกที่พัฒนาเทคโนโลยีนี้อีเทอร์เน็ตจะทำงานที่ความเร็ว 10 เมกะบิตต่อวินาทีเท่านั้นซึ่งก็ถือว่าเป็นแบนด์วิดท์ที่สูงสุดในขณะนั้นอีเทอร์เน็ตจะแบ่งตามประเภทของสายสัญญาณที่ใช้อยู่มี 3 ประเภทคือ สายโคแอ็กเชียล สายคู่ตีเกลียว และสายไฟเบอร์

ในการสร้างเครือข่ายจริงๆนั้นไม่จำเป็นต้องใช้สายสัญญาณประเภทเดียวกันทั้งเครือข่าย เพราะสายสัญญาณแต่ละประเภทเหมาะกับประเภทงานที่ต่างกันและมีข้อดีและข้อเสียที่ต่างกันการเลือกใช้สายสัญญาณหรือประเภทของอีเทอร์เน็ตควรให้เหมาะสมกับสิ่งแวดล้อมเครือข่ายอีเทอร์เน็ตทุกประเภทสามารถทำงานร่วมกันได้ไม่ว่าอุปกรณ์หรือสายสัญญาณนั้นจะผลิตด้วยบริษัทใดก็ตามโดยทั่วไปแล้วการเลือกใช้สายสัญญาณควรจะให้เหมาะสมกับลักษณะงานส่วนใหญ่จะแบ่งประเภทการใช้งานออกเป็น 3 ส่วนคือการเชื่อมต่อคอมพิวเตอร์ทั่วไปการเชื่อมต่อกับเครื่องเซิร์ฟเวอร์ และการเชื่อมต่อระหว่างฮับหรือสวิตช์ การเชื่อมต่อทั้งสามประเภทที่กล่าวมานี้มีความต้องการเกี่ยวกับประสิทธิภาพที่ต่างกัน เช่น การเชื่อมต่อเครื่องคอมพิวเตอร์ทั่วไป ส่วนใหญ่จะใช้สายสัญญาณค่อนข้างสั้น ทางเลือกที่ดีควรเป็น 10Base2, 10 Base5 ,10 Base-T, 10 Base-FL แต่ส่วนใหญ่จะใช้ 10 Base-T

การเชื่อมต่อกับเซิร์ฟเวอร์จะมีลักษณะคล้ายกับการเชื่อมต่อกับเครื่องลูกข่ายทั่วๆไปข้อแตกต่างก็คือ อัตราข้อมูลที่ไหลเข้าออกเซิร์ฟเวอร์จะมีปริมาณที่มากกว่าเครื่องลูกข่ายทั่วไปดังนั้นสายที่เชื่อมต่อควรมีประสิทธิภาพดี ทางที่ดีคือ10 Base-T หรือ 10 Base-FL

การเชื่อมต่อระหว่างฮับหรือสวิตช์หรือว่าบางทีเรียกว่า แบ็คโบนของเครือข่ายเหมือนกับการเชื่อมต่อกับเซิร์ฟเวอร์ อัตราข้อมูลที่ไหลผ่านแบ็คโบนนี้ค่อนข้างสูง และอีกอย่างระยะทางระหว่างฮับส่วนใหญ่จะไกลกว่าการเชื่อมต่อกับคอมพิวเตอร์ทั่วไปดังนั้นสายสัญญาณที่ใช้ควรสามารถส่งข้อมูลได้ไกลพอ จึงควรเลือกเป็น10 Base-FLหรือ 10Base-FOIRL

2.3. โปรโตคอล TCP/IP

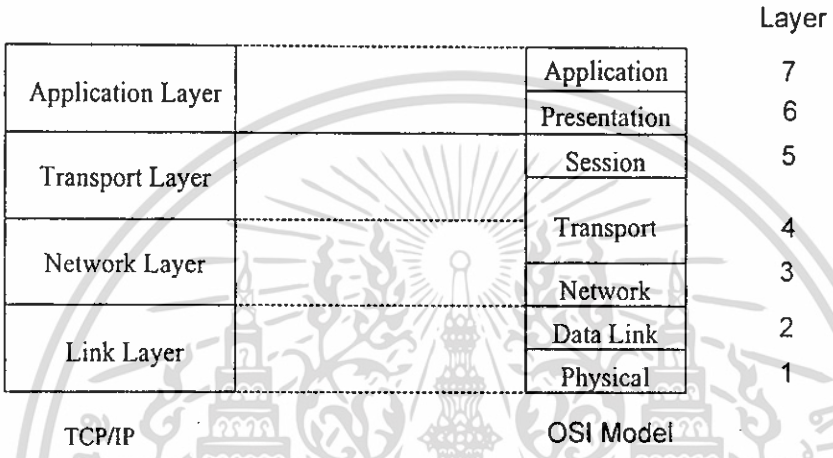


รูปที่ 2.20 โครงสร้างของโปรโตคอล TCP/IP

โดยปกติในการออกแบบระบบสื่อสารคอมพิวเตอร์ ผู้พัฒนาระบบมักจะจัดแบ่งกระบวนการทำงานออกเป็นส่วนๆอย่างเป็นลำดับขั้นเพื่อลดความซับซ้อน การแบ่งแยกงานในแต่ละชั้นจะกำหนดให้มีขอบเขตหน้าที่ชัดเจน ไม่ทับซ้อน และมีความเป็นความอิสระจากกันมากที่สุด การต่อของชั้นโปรโตคอลที่ติดกันจะมีรายละเอียดขั้นตอนและรูปแบบที่เหมาะสมเพื่อให้ได้ระบบที่มีประสิทธิภาพ สำหรับมาตรฐานโปรโตคอล TCP/IP ก็เช่นกัน ได้มีการจัดแบ่งการทำงานของระบบออกเป็นชั้นโปรโตคอลจำนวน 4 ชั้น ดังนี้

1.ชั้นแอพพลิเคชัน (Application Layer)
2.ชั้นทรานสปอร์ต (Transport Layer)
3.ชั้นเน็ตเวิร์ก (Network Layer)
4.ชั้นลิงก์ (Link Layer)

โดยเมื่อเทียบกับมาตรฐาน OSI model ดังรูปที่ 2.21 ซึ่งเราจะเห็นว่าบางกลไกของโปรโตคอล TCP/IP เทียบได้กับมาตรฐาน OSI model สองชั้น หรือบางกลไกก็จะทำงานคาบเกี่ยวกันระหว่างบางชั้นของ OSI model ตัวอย่างเช่น กลไกการทำงานของโปรโตคอล TCP/IP ในส่วน ชั้นลิงค์ เมื่อเทียบกับมาตรฐาน OSI model จะเทียบได้กับชั้นดาต้าลิงค์ (Data Link Layer) และชั้นฟิสิคอล (Physical Layer) 2 ชั้นรวมกันเป็นต้น ในแต่ละกลไกของโปรโตคอล TCP/IP และโปรโตคอลอื่นๆในชุดของ TCP/IPร่วมทำงานอยู่ด้วย



รูปที่ 2.21 แสดงกลไกของโปรโตคอลมาตรฐาน OSI model

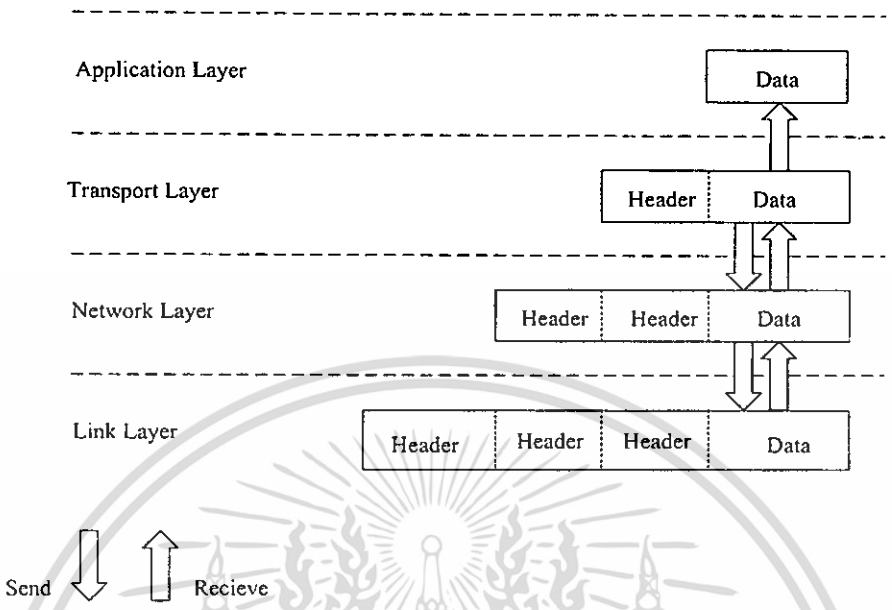
สำหรับการศึกษาโปรโตคอล TCP/IP นั้นเราจะไม่อ้างอิง OSI Reference Model นี้เพราะจะเข้าใจได้ยาก ดังนั้นเราจึงจะสร้างโมเดลขึ้นมาใหม่โดยแบ่งออกเป็น 4 ชั้นดังตารางที่ 2.1นี้

ตารางที่ 2.1แสดงชั้นโปรโตคอล TCP / IP

4	Application Layer
3	Transport Layer
2	Network Layer
1	Link Layer

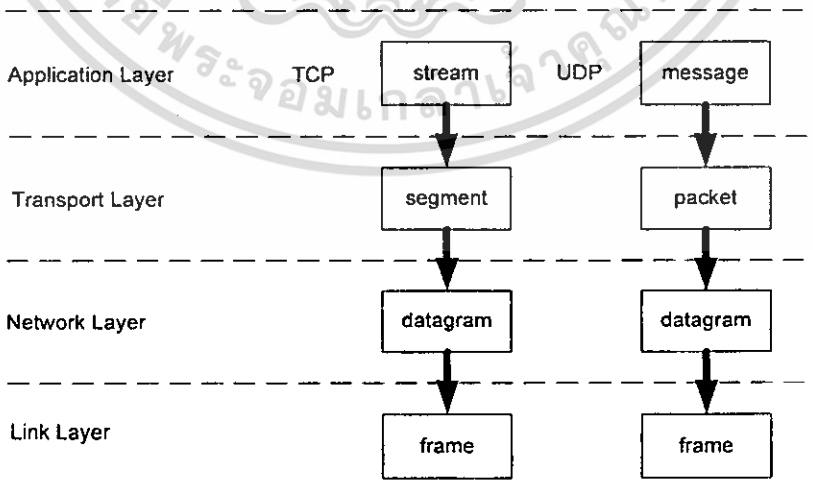
ลักษณะการทำงานของโมเดลในลักษณะนี้คือ ข้อมูลจะถูกส่งลงมาจากชั้นข้างบนลงมายังชั้นข้างล่างสุดซึ่งมีหน้าที่จัดการเกี่ยวกับการส่งข้อมูลผ่านสายสัญญาณไปยังจุดหมายปลายทาง เมื่อข้อมูลไปถึงจุดหมายแล้วก็จะกลับย้อนจากชั้นล่างขึ้นไปชั้นบนสุด ซึ่งเป็นชั้นที่โปรแกรมใช้งานต่างๆ ทำงานอยู่

ขณะที่ข้อมูลถูกส่งผ่านจากชั้นบนลงมายังชั้นล่าง แต่ละชั้นจะทำการเพิ่มข้อมูลควบคุมเข้าไปเพื่อให้การส่งข้อมูลถูกต้อง และเป็นการส่งพารามิเตอร์ที่จำเป็นไปให้กับชั้นนั้นๆในเครื่องปลายทาง ข้อมูลควบคุมเหล่านี้เราเรียกว่าเฮดเดอร์ (Header) แต่ละชั้นจะมีเฮดเดอร์ ที่มีรูปแบบเป็นของตัวเอง การเพิ่มเฮดเดอร์เข้าไปกับข้อมูลนั้นเราเรียกว่า Data Encapsulation ซึ่งได้แสดงไว้ในรูปที่ 2.22



รูปที่ 2.22 Data Encapsulation

หน่วยของข้อมูลที่จะทำการส่งนั้นจะมีชื่อเรียกต่างกันเมื่อเดินทางผ่านแต่ละชั้น ดังแสดงไว้ในรูปที่ 2.23 ซึ่งจะเห็นว่าการส่งใน TCP/IP นั้นมีอยู่ 2 โปรโตคอล ย่อยคือ TCP กับ UDP ชื่อของข้อมูลที่ผ่านโปรโตคอลทั้งสองนั้นแตกต่างกันในชั้นบนๆ เท่านั้น ชื่อสำคัญๆ ที่เราจะต้องพบและใช้ต่อไปบ่อยๆ ได้แก่ Datagram และเฟรม



รูปที่ 2.23 โครงสร้างของข้อมูล

2.3.1 Link Layer

เป็นชั้นล่างสุดมีชื่อเรียกได้แตกต่างกันเช่นชั้นดาต้าลิงก์ หรือชั้นเน็ตเวิร์คอินเทอร์เฟส (Network Interface Layer)หน้าที่ของโปรโตคอลในชั้นนี้ได้แก่ การกำหนดชนิดของฮาร์ดแวร์อินเทอร์เฟสที่ใช้ เช่น เป็นสายคู่ตีเกลียว (Twisted Pairs) หรือสายโคแอ็กเชียล (Coaxial Cable) กำหนดรูปแบบการส่งสัญญาณที่ส่งและโปรโตคอลที่ใช้ในการติดต่อกับระบบปฏิบัติการ (Operating System) ของเครื่องคอมพิวเตอร์ สำหรับชุดโปรโตคอล TCP/IP มิได้มีข้อจำกัดของโปรโตคอลในชั้นดาต้าลิงก์ไว้โดยเฉพาะเป็นของมันเอง หากแต่กลับได้รับการออกแบบเพื่อให้สามารถรองรับเทคโนโลยีโครงข่ายคอมพิวเตอร์ชนิดใดก็ได้ ซึ่งเป็นคุณลักษณะที่สำคัญของโปรโตคอล TCP/IP คือสามารถใช้ในการเชื่อมต่อโครงข่ายหลากหลายประเภทและอาศัยเทคโนโลยีแตกต่างกันให้สามารถติดต่อสื่อสารกันได้อย่างถูกต้องและมีประสิทธิภาพ

เนื่องจากในด้านกายภาพของเครือข่ายนั้น มีหลายวิธีการและหลายรูปแบบในการเชื่อมต่อระบบให้เป็นเครือข่ายแต่อย่างไรก็ตามในเครือข่ายอีเทอร์เน็ตนี้ ข้อมูลหรือ IPdatagram จะถูกถ่ายทอดและส่งผ่านไปยังปลายทางโดยไม่คำนึงถึงรูปแบบการเชื่อมต่อทางกายภาพไม่ว่าจะเป็นการใช้เครือข่ายใยแก้วนำแสงหรือเครือข่ายสายยูทีพี (Unshielded Twist Pair ,UTP) เชื่อมต่อเป็นแบบเครือข่ายอีเทอร์เน็ตธรรมดาหรือเครือข่าย โทเคนริง เอทีเอ็ม ไอเอสดีเอ็น ฯลฯ ก็ตาม

1. อีเทอร์เน็ต

อีเทอร์เน็ตเป็นการใช้สายโคแอ็กเชียลแบบบัสเชื่อมต่อระบบเข้าด้วยกันเพื่อทำการส่งถ่ายข้อมูลในระบบดิจิตอลระหว่างคอมพิวเตอร์โดยบริษัทอุปกรณ์ดิจิตอล บริษัทอินเทล (Intel) และบริษัทซีรีอก (Xerox) ได้ใช้ระบบนี้อ้างอิงเรื่อยมา ซึ่งอีเทอร์เน็ตจะใช้เทคนิคการส่งเบสแบนด์ในการเข้าถึงข้อมูล และยังสามารถใช้บนสายโคแอ็กเชียลที่มี 2 ขนาดคือสายอีเทอร์เน็ตแบบหนา (Thick Ethernet) และสายอีเทอร์เน็ตแบบบาง (Thin Ethernet) โดยสายเคเบิลทั้งสองนี้เป็นที่ใช้กันอย่างกว้างขวางในปัจจุบัน

ส่วนประกอบหลักที่สำคัญของเครือข่ายอีเทอร์เน็ต

ระบบเครือข่ายอีเทอร์เน็ต มีส่วนประกอบหลักซึ่งเมื่อทำงานด้วยกันแล้วก็จะเป็นเครือข่ายที่มีประสิทธิภาพการทำงานสูงดังนี้

- ตัวเฟรมเป็นชุดรูปแบบของบิตข้อมูลข่าวสารที่ใช้ส่งผ่านมาบนระบบหากไม่มีเฟรมเราจะไม่สามารถสื่อสารข้อมูลบนเครือข่ายได้โดยเด็ดขาดการรับส่งข้อมูลข่าวสารบนเครือข่าย อีเทอร์เน็ตจะต้องเป็นไปในรูปแบบเฟรมมาตรฐาน 2 แบบและเป็นแบบใดแบบหนึ่งเท่านั้น (การ์ดแลนเป็นผู้สร้างเฟรมนี้ขึ้นมา)

- ชุดโปรโตคอลที่ใช้ในการควบคุมการเข้าถึงเครือข่าย (Media Access Control Protocol) ซึ่งประกอบด้วยชุดของกฎกติกาที่อยู่ในการเชื่อมต่ออีเทอร์เน็ต (Ethernet Interface) เช่น การ์ดแลนเป็นต้น ซึ่งเป็นกฎมาตรฐานที่จะยอมให้คอมพิวเตอร์ต่างๆสามารถเข้ามาที่เครือข่ายและแบ่งใช้ทรัพยากรต่างๆบนเครือข่ายได้อย่างมีประสิทธิภาพ

- อุปกรณ์ที่ใช้รับส่งสัญญาณบนเครือข่าย (Signaling Components) ประกอบด้วยชุดของอุปกรณ์ที่ใช้เชื่อมต่อและส่งสัญญาณเพื่อการรับส่งข้อมูลภายในเครือข่าย

- สื่อที่ใช้ในการรับส่งสัญญาณข้อมูลบนเครือข่าย (Physical Medium) ประกอบด้วยสายสัญญาณ รวมทั้งอุปกรณ์ทางฮาร์ดแวร์อื่นๆ ที่จะช่วยในการนำพาข้อมูลข่าวสารต่างๆในรูปแบบดิจิตอลวิ่งไปมาบนเครือข่าย

2. เฟรมอีเทอร์เน็ต

อีเทอร์เน็ตได้ถูกระบุไว้อย่างแน่นอนไว้ในชั้นฟิสิคอล โดยจะแสดงรายละเอียดของรูปแบบเป็นแพ็กเก็ต ซึ่งโดยส่วนมากจะเรียกว่าเฟรมซึ่งเป็นหัวใจสำคัญของระบบอีเทอร์เน็ต จากรูปที่ 2.24 ได้แสดงรูปแบบของเฟรมอีเทอร์เน็ตโดยเฟรมนี้จะ Encapsulates TCP/IP โปรโตคอลและสามารถทำการตอบสนองสำหรับส่งข้อมูลข้ามเข้าระบบที่เชื่อมต่อไปยังอีกชั้นได้โดยเกตเวย์ (Gateway) หรือโหนดปลายทาง (End Node)

Preamble	Destination MAC Address (6 Byte)	Source MAC Address (6 Byte)	Type (2 Byte)	Data Field (1500 Byte Max)	Cyclic Redundancy Check (4 Byte)

รูปที่ 2.24 ลักษณะของเฟรมอีเทอร์เน็ต

โครงสร้างหรือรูปแบบของเฟรมอีเทอร์เน็ต (Ethernet Frame Format) มีลักษณะดังในรูป 2.24 ซึ่งประกอบด้วยส่วนต่างๆดังนี้คือ

1. ฟิลด์นำ (Preamble) (8ไบต์) มีไว้สำหรับใช้ในการบ่งบอกถึงจุดเริ่มต้นของเฟรมเพื่อให้ภาครับสามารถเข้าจังหวะเฟรมได้โดยกำหนดให้มีค่าเป็น 1 และ 0 สลับกันไปตลอด

2. ฟิลด์ ที่อยู่ปลายทาง(Destination Address) (6ไบต์) เป็นหมายเลขที่ระบุถึงที่อยู่ของสถานีจุดหมายปลายทางของเฟรม

3. ฟิลด์ที่ต้นทาง (Source Address) (6ไบต์) เป็นหมายเลขที่บอกถึงที่อยู่ของสถานีที่ให้กำเนิดเฟรมดังกล่าว

4. ฟิลด์ชนิด (Type) (2ไบต์) เป็นค่าที่ระบุชนิดของโปรโตคอลชั้นที่สูงกว่าอีเทอร์เน็ตที่บรรจุอยู่ในฟิลด์ ข้อมูล เพื่อให้ภาครับสามารถตีความหมายของข้อมูลที่บรรจุอยู่ในส่วนของข้อมูลได้ถูกต้อง เช่น หากมีข้อมูลเท่ากับ 0x0800 แสดงว่าข้อมูลที่ตามมาเป็นแพ็กเกตของโปรโตคอล IP หรือหากมีค่าเป็น 0x0806 แสดงว่าเป็นโปรโตคอล ARP

5. ฟิลด์ข้อมูล (Data) (46-1500 ไบต์) เป็นส่วนที่บรรจุข้อมูลจากโปรโตคอลชั้นสูงกว่าซึ่งกำหนดให้ต้องมีขนาดไม่เล็กกว่า 46ไบต์ ทั้งนี้เพื่อให้เฟรมของอีเทอร์เน็ตมีขนาดไม่เล็กกว่า 64ไบต์เสมอ ทั้งนี้ไม่นับรวมฟิลด์นำ

6. ฟิลด์ CRC (4ไบต์) เป็นส่วนที่ใช้สำหรับตรวจจับความผิดพลาดที่อาจเกิดขึ้นกับเฟรมของอีเทอร์เน็ตระหว่างการรับส่งสัญญาณ

หมายเลขที่อยู่ของอีเทอร์เน็ต กำหนดให้มีขนาดเท่ากับ 6 ไบต์ หรือ 48 บิต โดยการ์ดอีเทอร์เน็ตทุกการ์ดที่ผลิตออกจากโรงงานจะมีหมายเลขอีเทอร์เน็ตที่แตกต่างกันทั่วโลกซึ่งบรรจุอยู่ในหน่วยความจำรอม (ROM) ของแผ่นการ์ดในระหว่างกระบวนการผลิตเพื่อป้องกันมิให้มีการใช้หมายเลขซ้ำกันของผู้ผลิตต่างโรงงาน สมาคมวิศวกรรม IEEE ได้กำหนดช่วงของหมายเลขที่ต่างกันสำหรับโรงงานผู้ผลิตแต่ละแห่ง

3. MAC Address

เนื่องจากคอมพิวเตอร์แต่ละเครื่องสามารถแบ่งข้อมูลกันใช้ได้ในระบบเครือข่ายเดียวกันดังนั้นแต่ละเครื่องควรมีสิ่งที่ชี้ลักษณะเฉพาะตัวเสมือนการมีบัตรประจำตัวประชาชน ซึ่งในทางคอมพิวเตอร์นี้เราจะใช้เลขฐาน 16 จำนวน 12 ดิจิต (Digits) เป็นตัวบ่งชี้ลักษณะเฉพาะนั้นๆซึ่งเราเรียกว่า MAC Address เนื่องจาก MAC Address เป็นตัวบ่งชี้ลักษณะเฉพาะของแต่ละเครื่องดังนั้นจึงต้องเป็นค่าที่ไม่ซ้ำกัน MAC Address เป็นเลข 48 บิตโดยแบ่งออกเป็น 2 ส่วนโดย 24 บิตแรกเป็นค่าที่แสดงถึงบริษัทที่ผลิตการ์ดนั้นๆ ส่วน 24 บิต หลังเป็น Serial Number ที่ทางบริษัทกำหนดให้ ซึ่งแต่ละตัวจะไม่ซ้ำกัน เราเรียกเลข 24 บิต นี้ว่า OUI (Organizationally Unique Identifier) ซึ่ง OUI จะใช้เพียง 22 บิตเท่านั้น ส่วนอีก 2 บิตที่เหลือจะถูกใช้เพื่อวัตถุประสงค์อื่น โดยบิตหนึ่งจะใช้เพื่อแสดงว่าที่อยู่นั้นเป็น Broadcast/Multicast Address ส่วนอีกบิตหนึ่งนั้นไว้แสดงว่า Adapter นั้นถูกกำหนด Locally Administered Address ซึ่งผู้ดูแล ของระบบจะทำการกำหนด MAC Address เพื่อความเหมาะสมของนโยบายระบบ เช่น MAC Address = 03 00 00 00 00 01 ซึ่งจะเห็นว่าไบต์แรก = 03 = 00000011 นั่นคือ ทั้ง 2 bits ถูก set (Reset = 0) ซึ่งเอาไว้กรณี Multicast ให้ทุกเครื่องที่รันบนโปรโตคอล NetBEUI

4. Type field

ประเภทของฟิลด์จะใช้ระบุความแตกต่างของโปรโตคอลคอมพิวเตอร์จะดำเนินการให้โปรโตคอลหลายๆตัว สามารถเห็นความแตกต่างของโปรโตคอลแต่ละตัวได้ง่ายและผ่านการยินยอมของเฟรมที่เกี่ยวเนื่องกับเครือข่าย

ระบบ TCP/IP โดยทั่วไปจะใช้อีเทอร์เน็ต 3 ฟิลด์ ซึ่งมีค่าดังตารางที่ 2.2 ประเภทของหมายเลขอีเทอร์เน็ตเป็นรีจีสเตอร์กับ IEEE โดยจะใช้หมายเลขที่เฉพาะเจาะจงไม่เหมือนใคร

ตารางที่ 2.2 Ethernet Type Fields

Type	Protocol
0x0800	IP
0x0806	ARP
0x0835	RARP

5. Cyclic Redundancy Check (CRC)

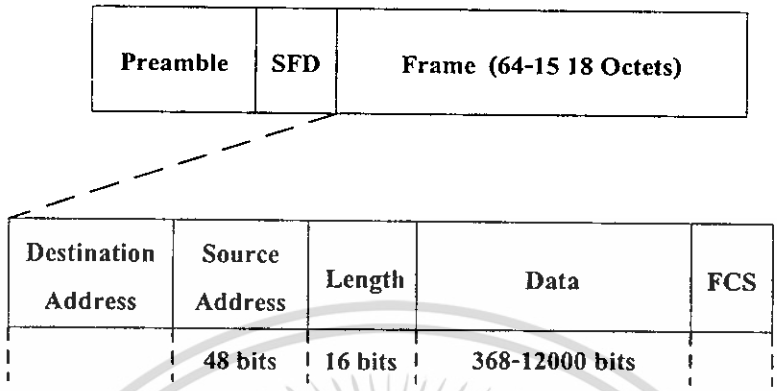
ที่ปลายสุดของเฟรม คือ Cyclic Redundancy Check (CRC) มีขนาด 32 บิต ที่คำนวณได้จากบิตทั้งหมดของอีเทอร์เน็ตเฟรม แต่จะไม่สนใจ Preamble ถ้าในเฟรมมีความผิดพลาดเกิดขึ้น ค่าที่คำนวณได้จะแตกต่างไปจากเฟรมเดิม ทำให้ข้อมูลไม่สามารถที่จะผ่านเฟรมไปยังชั้นเน็ตเวิร์ค (Network Layer) ได้

6. IEEE 802.3 เฟรม

IEEE 802.3 หรือ อีเทอร์เน็ต (Ethernet) เป็นเครือข่ายที่มีความเร็วสูงการส่งข้อมูล 10 เมกะบิตต่อวินาที สถานีในเครือข่ายอาจมีโทโปโลยีแบบบัสหรือแบบดาว IEEE ได้กำหนดมาตรฐานอีเทอร์เน็ตซึ่งทำงานที่ความเร็ว 10 เมกะบิตต่อวินาทีไว้หลายประเภทตามชนิดสายสัญญาณเช่น

1. 10Base5 อีเทอร์เน็ตโทโปโลยีแบบบัสซึ่งใช้สายโคแอ็กเชียลแบบหนา ความยาวของสายในเซกเมนต์หนึ่งๆไม่เกิน 500 เมตร
2. 10Base2 อีเทอร์เน็ตโทโปโลยีแบบบัสซึ่งใช้สายโคแอ็กเชียลแบบบาง ความยาวของสายในเซกเมนต์หนึ่งๆไม่เกิน 185 เมตร
3. 10BaseT อีเทอร์เน็ตโทโปโลยีแบบดาวซึ่งใช้ฮับเป็นศูนย์กลางสถานีและฮับเชื่อมด้วยสายยูทีพีด้วยความยาวไม่เกิน 100 เมตร

เฟรมข้อมูลสำหรับระบบอีเทอร์เน็ตประกอบขึ้นด้วยกลุ่มของบิตที่เป็นข้อมูลและข่าวสารสำคัญ แบ่งออกเป็นขนาดสัดส่วนที่แน่นอนที่เรียกว่าช่องฟิลด์ (Field) ดังรูปที่ 2.25



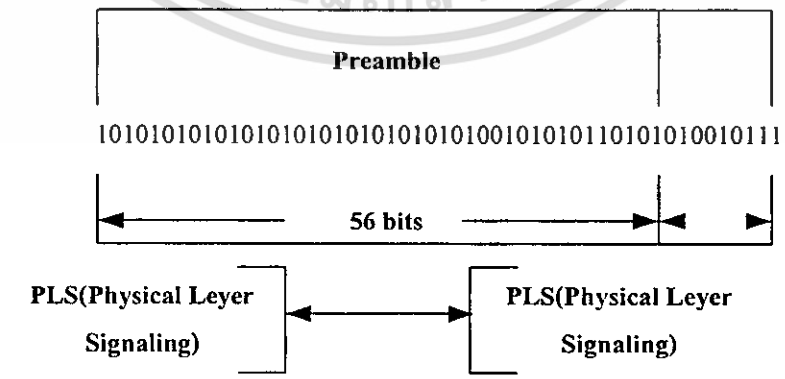
รูปที่ 2.25 ลักษณะโครงสร้างของเฟรมข้อมูลตามมาตรฐาน IEEE802.3

เฟรมมาตรฐานของ IEEE802.3 สามารถอธิบายได้ดังนี้

ช่อง Preamble

ช่อง Preamble ประกอบด้วยบิตข่าวสารที่เป็นเลข 1 และ 0 สลับกันและสิ้นสุดที่ 11 ซึ่งเป็นบิตที่ 63 และ 64 เป็นบิตข่าวสารที่ยังไม่ใช่ข้อมูลจริงของผู้ส่ง Preamble ประกอบด้วยข่าวสารที่มีขนาด 7 หรือ 8 ไบต์ จุดประสงค์ของข่าวสารนี้ก็เพื่อใช้สร้างจังหวะการรับข้อมูลให้แก่ผู้รับโดยที่ส่วนนี้จะไปถึงตัวผู้รับก่อนทำให้เครื่องคอมพิวเตอร์ของผู้รับสามารถปรับจังหวะความเร็วให้เข้ากับผู้ส่งได้ (Synchronize) สำหรับเฟรมแบบ อีเทอร์เน็ตทู (Ethernet II) จะมีขนาด 8ไบต์ และถ้าเป็นมาตรฐาน IEEE802.3 แล้วช่องนี้จะถูกแบ่งออกเป็น 2 ส่วน ดังรูปที่ 2.26 ได้แก่

1. Preamble
2. Start of Frame Delimiter

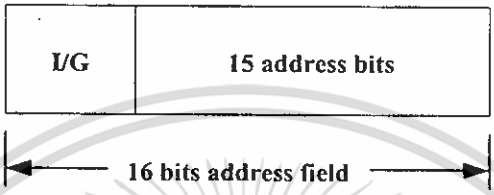


รูปที่ 2.26 ลักษณะส่วนการทำงานภายในของ Preamble

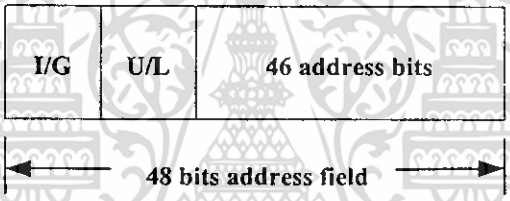
ช่อง Destination Address

ในช่อง Destination Address ประกอบด้วยข้อมูลข่าวสารเกี่ยวกับแอดเดรสหรือที่อยู่ของผู้รับปลายทาง ช่องนี้ถูกแบ่งออกเป็นช่องย่อยๆที่เรียกว่าฟิลด์ย่อย (Sub-Fields) ซึ่งเก็บข้อมูลข่าวสารที่ใช้ดูแลการทำงานของเครือข่าย ทั้งนี้ขึ้นอยู่กับที่อยู่ที่ปรากฏอยู่ในช่องนี้ไม่ว่าช่องแอดเดรสนี้จะมีที่อยู่ที่ถูกเจาะจงเป็นรายบุคคลหรือเป็นกลุ่มของผู้รับก็ตาม

1. ช่องข่าวสารขนาด 2 ไบต์



2. ช่องข่าวสารขนาด 6 ไบต์



ช่อง I/G

มีการจัดตั้งค่าบิตขึ้นในช่องนี้โดยการ์ดแลน ซึ่งหากค่านี้ถูกตั้งค่าไว้ที่ "0" ก็แสดงว่าตัวที่อยู่ที่ระบุอยู่ในช่อง Destination Address นั้นเป็นที่อยู่ที่ระบุตัวคอมพิวเตอร์ผู้รับแบบเฉพาะเจาะจง แต่ถ้าถูกตั้งค่าเป็น "1" ก็แสดงว่าที่อยู่ในช่อง Destination Address นี้เป็นที่อยู่ที่ใช้ติดต่อผู้รับที่เป็นกลุ่มคอมพิวเตอร์ทั้งหลาย เราเรียกกลุ่มที่อยู่ ตัวอย่างของกลุ่มที่อยู่ได้แก่ "FFFFFFFFFFFF" ซึ่งถือว่าเป็น Broadcasting Address หรือที่อยู่ที่ไม่เจาะจงผู้รับ โดยผู้รับเป็นกลุ่มหรือทั้งหมดก็สามารถรับข้อมูลข่าวสารนี้ได้

ช่องย่อย U/L

ช่องย่อย U/L มีไว้สำหรับช่องขนาด 6ไบต์เท่านั้นค่าที่ถูกตั้งไว้ในช่องย่อยนี้เป็นการบ่งบอกให้ทราบว่าที่อยู่ที่ปรากฏอยู่ในช่อง ที่อยู่ปลายทาง นี้เป็นที่อยู่ที่ถูกกำหนดมาตรฐานโดย IEEE

ช่อง Source Address

สำหรับช่อง Source Address นี้มีไว้เพื่อแสดงตัวสถานีเครือข่ายต้นทางที่เป็นต้นทางส่งข้อมูลข่าวสารเข้ามาและเช่นเดียวกับช่อง Destination Address กล่าวคือ ช่อง Source Address สามารถมีช่องย่อยได้ทั้งแบบ 2ไบต์หรือ 6ไบต์อย่างใดอย่างหนึ่ง

ตารางที่ 2.3 เป็นตัวอย่างของ Source Address ที่แสดงรหัสแอดเดรสของผู้ผลิตดังนี้คือ

ผู้ผลิตการ์ด แลน	รหัสผู้ผลิตขนาด 3 ไบต์
Cisco	00-00-0C
Cabletron	00-00-1D
Intel	00-AA-00
3 Com	02-60-8C
Hewlett Packard	08-00-09
Sun	08-00-20
DEC	08-00-2B
Shiva	00-80-D3
Xerox	00-00-AA
IBM	08-00-5A

ช่องแสดง Type

ช่องแสดง Type มีขนาด 2ไบต์ใช้กับอีเทอร์เน็ตเฟรมเท่านั้นโดยช่องนี้ใช้เพื่อแสดงว่าโปรโตคอลการทำงานของเฟรมนี้เป็นแบบใด จุดประสงค์คือเพื่อต้องการให้ทราบว่าข้อมูลที่อยู่ในเฟรมนี้ จะทำงานภายใต้โปรโตคอลใด ซึ่งผู้รับจะได้เตรียมการแปลความหมายที่อยู่ในช่องข้อมูล (Data Field) ได้ถูกต้อง

ภายใต้ระบบเครือข่ายอีเทอร์เน็ตเราสามารถใช้โปรโตคอลได้หลายตัวพร้อมกันบนเครือข่ายท้องถิ่นและบริษัทซีร็อก ทำหน้าที่เป็นผู้ให้บริการ กำหนดพิกัดระยะของแอดเดรสที่เป็นลิขสิทธิ์ให้แก่ผู้ผลิตการ์ดแลน ต่างๆรวมทั้งการกำหนดค่าที่ใช้แสดงแทนโปรโตคอลที่ใช้ในช่อง Type แห่งนี้

ตารางที่ 2.4 เป็นตัวอย่างของรหัสที่ใช้แสดงแทนโปรโตคอลที่ใช้ในช่อง Type 18 รายการดังนี้

โปรโตคอลที่ใช้	ค่าที่เป็นรหัสแบบเลขฐาน 16
IP	0800
X.75 Internet	0801
X.25 Level 3	0805
Address Resolution Protocol (ARP)	0806
Banyan Systems	0BAD
BBN Simnet	5208
DEC MOP Dump/Load	6001
DEC MOP Remote Console	6002
DEC DECNET Phase IV Route	6003
DEC LAT	6004
DEC Diagnostic Protocol	6005
DEC LANBridge	8038
DEC Ethernet Encryption	803D
Apple Talk	809B
IBM SNA Service on Ethernet	80D5
Apple Talk ARP	80F3
NetWare IPX/SPX	8137
SNMP	814C

ช่อง Length

ช่องนี้มีขนาดความยาวเพียง 2 ไบต์ใช้ได้กับเฟรมมาตรฐาน IEEE802.3 เท่านั้นเป็นช่องที่ใช้แสดงขนาดจำนวนของไบต์ที่มีปรากฏอยู่ในช่องข้อมูล

ช่อง ข้อมูล (Data Field)

ดังที่ได้กล่าวมาแล้วว่าช่องของข้อมูลอย่างน้อยต้องมีขนาดไม่เล็กกว่า 46ไบต์เพื่อให้แน่ใจว่าเฟรมมีขนาดไม่ต่ำกว่า 64ไบต์ซึ่งหมายความว่าการแพร่ข้อมูลขนาดหนึ่งไม่ว่า 1หรือ 10ไบต์ก็ตามต้องมาจาก 46 ไบต์นี้แต่ถ้าข้อมูลในช่องนี้เล็กกว่า 46ไบต์แน่นอนว่าต้องมีการเพิ่มไบต์ลงไปอีกเพื่อให้ได้ขนาด 46ไบต์ ขนาดของข้อมูลที่อยู่ในข้อมูลจะต้องมีขนาดสูงสุดไม่เกิน 1,500ไบต์

ช่องตรวจสอบความผิดพลาดของข้อมูลในเฟรม (Frame Check Sequence)

ช่อง Frame Check Sequence นี้ใช้ได้ ทั้งเฟรมมาตรฐาน ทั้งอีเทอร์เน็ตและ IEEE802.3 เป็นช่องที่ประกอบด้วยข้อมูลที่ใช้เป็นกลไกในการตรวจสอบความผิดพลาดของข้อมูลภายในเฟรม

หลักการทำงานก็คือว่าก่อนที่เครื่องผู้ส่งจะส่งข้อมูลออกไปที่เครือข่าย การ์ดแลนของมันจะคำนวณค่าต่างๆในช่องต่างๆซึ่งครอบคลุมตั้งแต่ช่องที่อยู่ ต่างๆของ Type และช่อง Lengthรวมทั้งช่อง ข้อมูล การคำนวณค่าแบบนี้เรียกว่า Cyclic Redundancy Check (CRC) ซึ่งหลังจากที่ได้คำนวณค่าเสร็จสิ้นแล้ว ผลลัพธ์ที่คำนวณได้มีขนาด 4 ไบต์จะถูกนำไปใส่ไว้ในช่อง Frame Check Sequence แห่งนี้

2.3.2. Network Layer

มีบทบาทสำคัญในการส่งผ่านข้อมูลของผู้ใช้ในรูปแบบของ IPdatagram จากอุปกรณ์ต้นทางผ่านเราท์เตอร์ในระบบ และนำส่งไปให้อุปกรณ์ปลายทาง การเลือกเส้นทางในการส่ง IPdatagram จึงเป็นปัญหาหลักที่ต้องการได้รับการพิจารณาและการออกแบบอย่างถูกต้องต้องมีประสิทธิภาพเพื่อให้การรับส่ง Datagram มีความรวดเร็วและถึงมือผู้ใช้ปลายทางโดยมีความผิดพลาดน้อยที่สุดโปรโตคอลที่สำคัญในชั้นนี้ได้แก่

-โปรโตคอล IP (Internet Protocol)

-โปรโตคอล ICMP (Internet Control Message Protocol)

-โปรโตคอล IGMP (Internet Group Management Protocol)

1. โปรโตคอลIP (Internet Protocol)

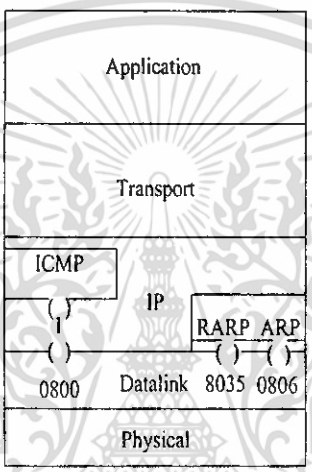
โปรโตคอล IP ทำหน้าที่ให้บริการส่งผ่านข้อมูลที่มาจากชั้นทรานสปอร์ตเพื่อส่งข้ามไปยังเครือข่ายใดๆได้อย่างถูกต้องแม้ว่าจะมีเครือข่ายเชื่อมต่อกันอยู่ในอินเตอร์เน็ตเป็นล้านๆเครือข่ายก็ตามเนื่องจากโปรโตคอล IP มีข้อมูลตำแหน่ง IP ปลายทางที่จะส่งข้อมูลไปให้โดยทำงานร่วมกับอุปกรณ์เราท์เตอร์เพื่อส่งข้อมูลข้ามเครือข่ายออกไปได้ ตัวโปรโตคอล IP จะทำงานแบบ แพ็กเก็ตสวิทช์ (Packet Switching) คือมีการส่งข้อมูลผ่านสวิทช์ (Switch)ไปยังปลายทางโดยข้อมูลจะเดินทางไปยังเครือข่ายต่างๆ ผ่านสวิทช์นี้ไปเรื่อยๆ จนกว่าจะถึงปลายทาง ตัววงจรผ่านหรือสวิทช์นี้อาจเป็น เกตเวย์หรือเราท์เตอร์ในระบบเครือข่ายก็ได้ ซึ่งในข้อมูลของโปรโตคอล IP จะมีข้อมูลของหมายเลข IP ที่จะส่งข้อมูลไปและเมื่อถึงเครือข่ายปลายทางแล้วจะมีกลไกแปลงหมายเลข IPให้เป็นหมายเลขฮาร์ดแวร์ประจำเครื่องที่ถูกต้องอีกทีหนึ่งด้วยโปรโตคอล ARP

IP จะให้บริการชนิด คอลเนกชันเลส สำหรับผู้ใช้ ดังนั้นข้อมูลที่ถูกส่งผ่าน IP โดยกระบวนการส่งยังไม่แน่ว่าจะสามารถส่งถึงข้อมูลของ IP หน่วยต่างๆที่ถูกส่งเรียกว่า IPdatagram ซึ่งผ่านการ Encapsulation ข้อมูลที่ถูกส่งมาจากชั้น ที่สูงกว่าด้วย IP Header ถ้า IPdatagram ไม่ได้ถูกนำส่งภายในเวลาที่กำหนด Datagram นั้นก็จะไม่ถูกส่งอีกเลยสำหรับช่วงเวลาที่กำหนดนั้นสามารถกำหนดไว้ในกระบวนการส่ง

ส่วนประกอบของ IP

IPaddress จะต้องมีค่าเฉพาะเจาะจงไม่เหมือนใครเพื่อที่จะใช้เชื่อมต่อเข้ากับเครือข่ายที่หมายเลขของเครือข่ายที่เฉพาะเจาะจงเช่นกันโดยในรูปที่ 2.27 แสดงให้เห็นว่าในชั้น IP จะประกอบไปด้วย 3โปรโตคอล ได้แก่

1. The Address Resolution Protocol (ARP)
2. The Reverse Address Resolution Protocol (RARP)
3. The Internet Control Message Protocol (ICMP)



รูปที่ 2.27 ส่วนประกอบของ IP

ARP และ RARP จะอยู่ที่ส่วนปลายสุดของชั้น IP เพราะทั้งสองโปรโตคอลไม่ใช้ IP และจะถูกแยกโปรโตคอลโดยดาต้าลิงค์ ที่สนับสนุนตัวมันอยู่ ส่วน ICMP จะอยู่ในส่วนบนสุดของชั้น IP ซึ่งจะข้ามเข้าไปในเครือข่ายใน IPdatagram

IP Datagram

Datagram เป็นหน่วยพื้นฐาน ของข้อมูลที่ IP จะทำการส่ง ซึ่งถูกออกแบบมาให้ทำงานกับเครือข่ายแบบแพ็กเก็ตสวิทช์ ซึ่งข้อมูลของผู้ใช้มักถูกแบ่งออกเป็นหลาย Datagram โดยแต่ละตัวจะมีเฮดเดอร์ที่เก็บรายละเอียดเกี่ยวกับตัวเองไว้และปลายทางที่จะส่งไป Datagram แต่ละตัวจะเดินทางโดยไม่เกี่ยวข้องกัน นั่นคือ Datagram แต่ละตัวอาจจะเดินทางไปยังปลายทางโดยใช้เส้นทางคนละเส้นและลำดับที่ของการไปถึงจุดหมายปลายทางก็ไม่แน่นอน เป็นหน้าที่ของ อินเตอร์เน็ตโปรโตคอล (Internet Protocol) ในเครื่องปลายทางที่จะต้องประกอบ Datagram เหล่านี้ให้กลายเป็นข้อมูลของผู้ใช้ที่สมบูรณ์อีกครั้ง

IP Datagram ประกอบด้วย IP Header และ IP Payload

IP Header	IP Payload

IP Header เป็นขนาดที่เปลี่ยนแปลงได้ระหว่าง 20 และ 60ไบต์ในการเพิ่มขึ้น 4ไบต์ จะมีการจัดเตรียมการสนับสนุนการจัดเส้นทาง (Routing) การแสดงตัว Payload การชี้ให้เห็นถึงขนาด IP Header และ Datagram การสนับสนุน Fragmentation โดยมีโครงสร้างดังรูปที่ 2.28

Version	IP Header Length	Type of Service	Total Length	Identifier	Flags	Fragment Offset
4 bit	4 bit	8 bit	16 bit	16 bit	3 bit	13 bit

Time – to – Live	Protocol	Header Checksum	Source IP Address	Destination IP Address	IP Option and Padding
8 bit	8 bit	16 bit	32 bit	32 bit	32 bit

รูปที่ 2.28 แสดงโครงสร้าง IP Header

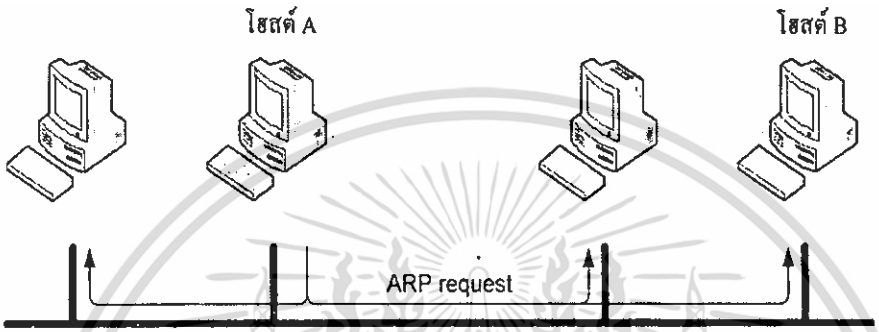
IP Payload เป็นขนาดที่เปลี่ยนแปลงโดยมีลำดับจาก 8ไบต์ (68ไบต์ IP datagram กับ 60ไบต์ IP Header) ถึง 65,515ไบต์ (65,535 ไบต์ IP datagram กับ 20ไบต์ IP)

Address Resolution Protocol (ARP)

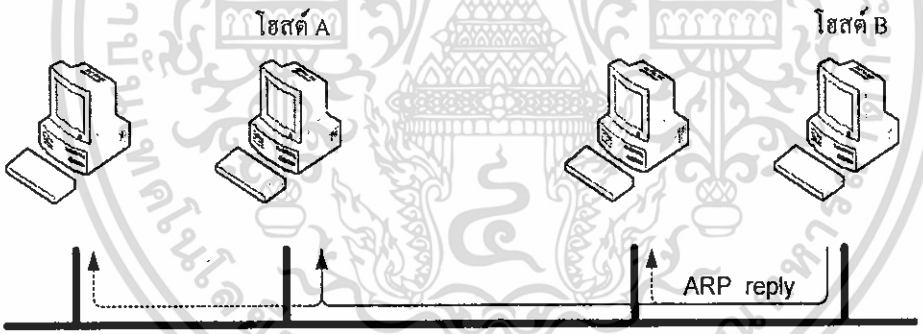
การทำงาน ARP กับระบบอีเทอร์เน็ต

ระบบอีเทอร์เน็ตเป็นรูปแบบของโครงข่ายที่มีสถาปัตยกรรมเป็นแบบบรอดคาสต์นั่นคือหากโฮสต์หนึ่งส่งเฟรมข้อมูลออกโฮสต์อื่นๆทั้งหมดภายในระบบจะรับทราบและเห็นเฟรมดังกล่าวเฟรมแต่ละเฟรมที่ส่งออกจะมีการระบุหมายเลขประจำตัวของอินเทอร์เฟสการ์ดหรือหมายเลขฮาร์ดแวร์แอดเดรสที่ให้กำเนิดเฟรมกำกับอยู่ที่เฮดเดอร์พร้อมทั้งกันนั้นก็จะมีการระบุหมายเลขฮาร์ดแวร์แอดเดรสของอินเทอร์เฟสการ์ดของโฮสต์ปลายทาง สำหรับโปรโตคอลอีเทอร์เน็ต หมายเลขดังกล่าวมีขนาด 48 บิตซึ่งโดยทั่วไปเรียกว่าอีเทอร์เน็ตแอดเดรส หมายเลขนี้เป็นหมายเลขเฉพาะที่กำหนดจากโรงงานผู้ผลิตซึ่งจะไม่มีการซ้ำกันกับอีเทอร์เน็ตการ์ดอื่นๆสำหรับระบบที่มีโครงสร้างการทำงานคล้ายคลึงกับอีเทอร์เน็ต แนวทางในการแปลงหมายเลข IPaddress ให้เป็นหมายเลขฮาร์ดแวร์แอดเดรสมีขั้นตอนดังนี้คือขั้นแรกให้อุปกรณ์สื่อสารหรือโฮสต์ต้นทาง A ส่งเฟรมที่มีหน้าที่เฉพาะกิจ ARP request ในการสืบหาหมายเลขฮาร์ดแวร์ของโฮสต์ปลายทาง B ที่ต้องการติดต่อ ดูรูปที่ 2.29 ประกอบ สังเกตว่าเฟรมที่ส่งออกในขั้นตอน

นี้จะต้องเป็นเฟรมประเภทบรอดคาสต์เพราะว่าในจังหวะที่ A ยังไม่ทราบหมายเลขฮาร์ดแวร์แอดเดรสของ B ดังนั้นโฮสต์ต่างๆในระบบจะต้องอ่านและตรวจสอบเฟรมดังกล่าวว่าหมายเลข IPaddress ที่บรรจุอยู่เป็นของตนหรือไม่ แน่นอนว่าจะมีเพียง B เท่านั้นที่จะตอบรับกลับโดยการส่งเฟรมที่บรรจุหมายเลขฮาร์ดแวร์ของตนลงไป ARP reply ในขั้นตอนนี้เฟรมที่ส่งออกไม่จำเป็นต้องเป็นเฟรมบรอดคาสต์อีกต่อไป B สามารถกำหนดหมายเลขฮาร์ดแวร์แอดเดรสปลายทางเป็นแอดเดรสของ A ได้เลยและทันทีที่สถานี A ได้รับเฟรมตอบรับดังกล่าวก็สามารถทราบถึงหมายเลขฮาร์ดแวร์ของ B ดังรูป



1.โฮสต์ A ประกาศผ่านเฟรมชนิดบรอดคาสต์เพื่อถามหาโฮสต์ที่เป็นเจ้าของ IPaddress ที่ระบุ



2.โฮสต์ B ตอบกลับไปโดยใช้เฟรมที่ระบุหมายเลขปลายทางแบบเจาะจงเฉพาะกับ A

รูปที่ 2.29 ขั้นตอนการทำงานของโปรโตคอล ARP

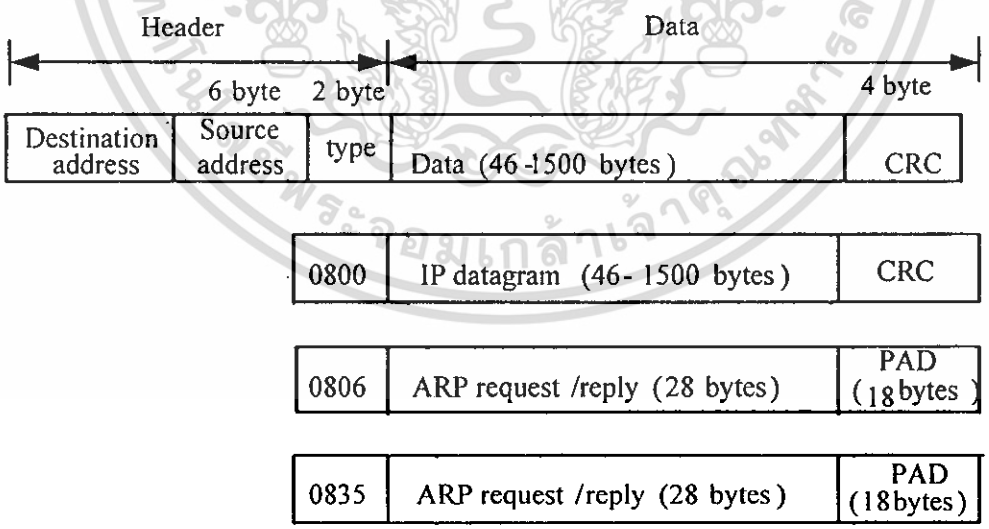
จากที่กล่าวมาจะเห็นว่ากระบวนการ ARP ต้องมีการใช้แบนด์วิดท์ของช่องสัญญาณไปส่วนหนึ่ง ดังนั้นเพื่อให้การสูญเสียแบนด์วิดท์ในส่วนนี้มีปริมาณน้อยที่สุดโฮสต์แต่ละตัวมักจะมีการเก็บคู่ IPaddress กับฮาร์ดแวร์แอดเดรสที่ทราบแล้วไว้ในแคชของตนเอง ดังนั้นเมื่อโฮสต์มี ARP แคชแล้วการส่งข้อมูลของผู้ใช้บริการแต่ละครั้งก็ไม่ต้องทำกระบวนการ ARP ใหม่อีกอย่างไรก็ตามข้อมูลที่เก็บในแคชจะถูกลบออกหลังจากได้เก็บไว้ใช้งานระยะหนึ่ง ทั้งนี้เพราะในบางสถานการณ์คู่ IPaddress กับฮาร์ดแวร์

แอดเดรสอาจเกิดการเปลี่ยนแปลงได้ เช่น กรณีอีเทอร์เน็ตการ์ดเสียหายและได้รับการเปลี่ยนใหม่ซึ่งหมายเลขอีเทอร์เน็ตแอดเดรสหรือฮาร์ดแวร์แอดเดรสย่อมเปลี่ยนไปด้วย โดยทั่วไปข้อมูลแต่ละข้อมูล

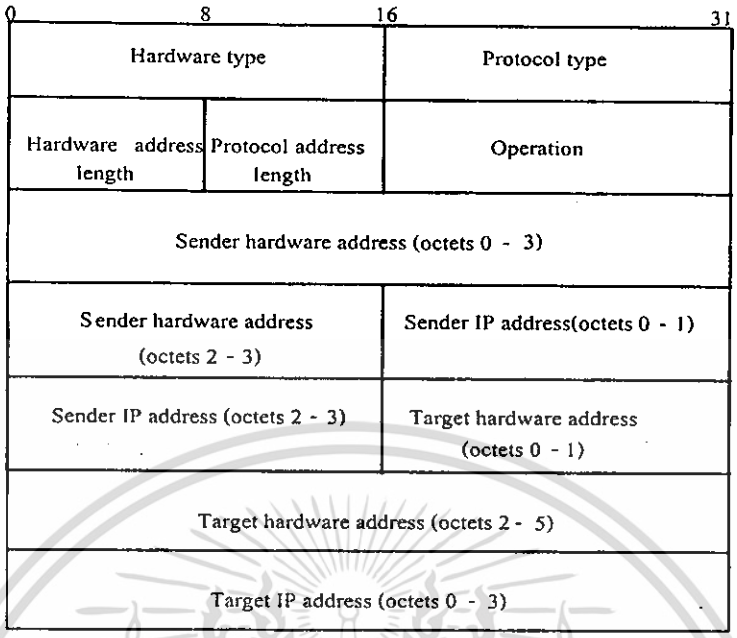
แต่ละคู่ในแคชจะกำหนดให้มีการใช้งานประมาณ 15-20 นาทีสังเกตว่ากระบวนการ ARP ที่ทำงานในลักษณะนี้เกิดขึ้นได้โดยอัตโนมัติผู้ใช้งานหรือผู้ดูแลระบบไม่จำเป็นต้องเข้ามายุ่งเกี่ยวในการตั้งค่าพารามิเตอร์ใดๆจึงสะดวกในการใช้งาน

รูปแบบหรือโครงสร้างของโปรโตคอล ARP

การส่งผ่านข่าวสารของโปรโตคอล ARP จากอุปกรณ์สื่อสารหนึ่งไปสู่อีกอุปกรณ์หนึ่งจะกระทำโดยอาศัยเฟรมของชั้นโปรโตคอลดาต้าลิงก์ในลักษณะเดียวกับการส่งผ่าน IPdatagram ดังนั้นในเฮดเดอร์ของเฟรมจะต้องมีฟิลด์ที่บ่งบอกให้ทราบว่าข้อมูลที่บรรจุในเฟรมเป็นโปรโตคอลชนิดใดสำหรับโปรโตคอลอีเทอร์เน็ตมีโครงสร้างเฟรมดังในรูป2.30 เมื่อพิจารณาจากรูปจะเห็นว่าเฟรมอีเทอร์เน็ตแบ่งออกเป็น 2 ส่วน คือ เฮดเดอร์และข้อมูล ส่วนของเฮดเดอร์ประกอบด้วยแอดเดรสปลายทาง (Destination Address) แอดเดรสต้นทาง (Source Address) และฟิลด์ชนิดข้อมูล (Type) แอดเดรสทั้งคู่มีขนาด 6ไบต์ หรือ 48 บิตซึ่งคืออาร์ดแวร์แอดเดรสหรืออีเทอร์เน็ตแอดเดรสที่ได้กล่าวไว้ในส่วนที่แล้วนั่นเอง สำหรับฟิลด์ Type เป็นส่วนที่บ่งบอกให้ทราบว่าข้อมูลที่บรรจุอยู่ในเฟรมเป็นข้อมูลชนิดใดตามมาตรฐานโปรโตคอลอีเทอร์เน็ตกำหนดให้ Type =0800 แทน IPdatagram 0806 แทน Datagram ARP และ 0835 แทน Datagram RARP สำหรับมาตรฐานโปรโตคอลของโครงข่ายประเภทอื่นๆก็อาจจะมีการกำหนดค่า Type ที่แตกต่างออกไป



รูปที่ 2.30 โครงสร้างเฟรมของโปรโตคอลอีเทอร์เน็ต



รูปที่ 2.31 ตัวอย่างรูปแบบและโครงสร้างโปรโตคอล ARP

เมื่อมาพิจารณาส่วนของโปรโตคอล ARP ที่ใช้กับโครงข่ายอีเทอร์เน็ต โครงสร้างของ Datagram ARP มีขนาด 28 ไบต์ ดูรูปที่ 2.31 ประกอบรูปแบบองค์ประกอบของฟิลด์ใน Datagram ARP ได้รับการออกแบบให้ยืดหยุ่นสามารถทำงานร่วมกับฮาร์ดแวร์หรือโครงข่ายได้หลากหลายประเภทซึ่งแต่ละส่วนมีความหมายดังนี้

1.ฟิลด์ Hardware Type ขนาด 16 บิตเป็นฟิลด์ที่บ่งบอกถึงประเภทหรือชนิดของฮาร์ดแวร์อินเทอร์เฟสที่โปรโตคอล ARP ทำงานร่วมอยู่ เช่น Hardware Type จะกำหนดให้มีค่าเป็น 1 สำหรับฮาร์ดแวร์อีเทอร์เน็ต และกำหนดให้เป็น 4 สำหรับฮาร์ดแวร์โทเคนริงเป็นต้น

2. ฟิลด์ Protocol Type ขนาด 16 บิต มีไว้สำหรับบอกชนิดของโปรโตคอลชั้นสูงของต้นทางที่ประสงค์จะทำกระบวนการ ARP ด้วยกรณีที่ใช้งานร่วมกับอีเทอร์เน็ตค่านี้ได้กำหนดให้เท่ากับ 0800 สำหรับบ่งบอกให้ทราบว่า IPaddress สังเกตว่าค่านี้ได้กำหนดให้ตรงกันกับค่าของฟิลด์ Type ใน เฮดเดอร์ของเฟรมอีเทอร์เน็ตที่แทน IPdatagram ดูได้จากรูป 2.31

3. ฟิลด์ Hardware Address Length ขนาด 16 บิต มีไว้เพื่อให้สามารถรองรับฮาร์ดแวร์หลายประเภทที่มักจะมีขนาดของแอดเดรสแตกต่างกันไป สำหรับอีเทอร์เน็ตฟิลด์นี้มีค่าเท่ากับ 6 ซึ่งตรงกับขนาดแอดเดรสของอีเทอร์เน็ตที่มีขนาดเท่ากับ 6ไบต์ หรือ 48 บิต

4. ฟิลด์ Protocol Address Length ขนาด16 บิต กำหนดขึ้นเพื่อให้สามารถรองรับโปรโตคอลชั้นสูงได้หลายประเภทที่อาจจะมีขนาดของแอดเดรสแตกต่างกันไปสำหรับโปรโตคอล IP ฟิลด์นี้กำหนดให้มีค่าเท่ากับ 4 ไบต์ซึ่งตรงกับขนาด IPaddress ที่มีขนาดเท่ากับ 4ไบต์ หรือ 32 บิตนั่นเอง

5. ฟิลด์ Operation ขนาด 16 บิตมีหน้าที่แยกแยะชนิดของโปรโตคอล ARP/RARP ย่อยลงเป็น 4รูปแบบ

ตารางที่ 2.5 รายละเอียดของ ฟิลด์ Operation

ประเภทของโปรโตคอล	ค่าของฟิลด์ Operation
ARP request	1
ARP reply	2
RARP request	3
RARP reply	4

6. ฟิลด์ Address ประกอบด้วยฮาร์ดแวร์แอดเดรสและ IPaddress ของทั้งต้นทางและปลายทาง ขนาดของฟิลด์เหล่านี้ได้รับการกำหนดให้สอดคล้องกับขนาดของอีเทอร์เน็ตแอดเดรสและ IPaddress สำหรับการส่ง ARP request จะไม่มีการบรรจุค่าลงในฟิลด์ Target Hardware Address เพราะเป็นค่าที่โฮสต์ทางต้องการทราบนั่นเอง ค่าดังกล่าวนี้จะใช้รับการบรรจุใน ARP reply โดยโฮสต์ปลายทางและจะส่งในฟิลด์ Send Hardware

Reverse Address Resolution Protocol (RARP)

วิธีการ ARP ช่วยแก้ปัญหาในการค้นหาที่อยู่ของข้อมูลที่ใช้การกำหนดที่อยู่แบบฮาร์ดแวร์ แต่ถ้าทราบที่อยู่แบบฮาร์ดแวร์แล้วต้องการแปลงที่อยู่เป็น IP จะทำอย่างไรปัญหานี้มักเกิดขึ้นกับเครื่องคอมพิวเตอร์ ที่เริ่มทำงานด้วยการอ่านข้อมูลทั้งหมดจากเครื่องฮอส (Host) เครื่องประเภทนี้จะทราบเพียงที่อยู่ ของตนเองจากอุปกรณ์สื่อสารเครือข่ายเท่านั้น

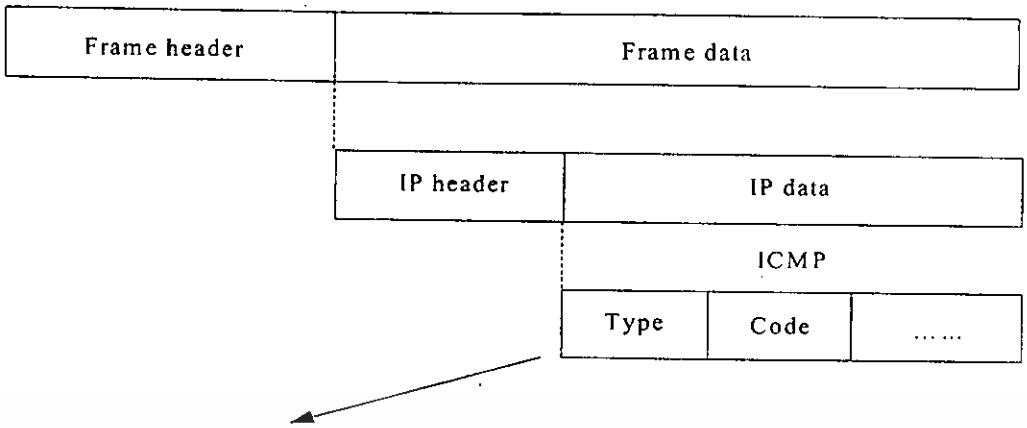
การค้นหาคำตอบสามารถทำได้โดยวิธีควบคุมการสื่อสารแบบ ARP ย้อนกลับ หรือ RARP (Reverse Address Resolution Protocol) วิธีการนี้คอมพิวเตอร์ที่เพิ่งจะเริ่มทำงาน(หรือเครื่องใดก็แล้วแต่) จะส่งคำถามออกไปในทำนอง "ที่อยู่ขนาด 48 บิตแบบฮาร์ดแวร์ของฉันคือ 14.04.05.18.01.25 มีใครทราบที่อยู่IP ของฉันบ้าง" เครื่องที่ให้บริการ RARP จะตรวจดูข้อมูลในตารางข้อมูลของตนเองแล้วจึงส่งหมายเลข IP กลับไปให้วิธีการนี้ช่วยให้เกิดความอ่อนตัวและเพิ่มประสิทธิภาพในการใช้หมายเลข IP เนื่องจากผู้ใช้ไม่มีหมายเลข IP เป็นของตนเองผู้ควบคุมระบบสามารถกำหนดหมายเลข IP ใดๆที่ไม่มีผู้ใช้งานในขณะนั้นให้ใช้ได้หมายเลข IP ในที่นี้จึงเป็นเสมือนสมบัติส่วนกลางที่ทุกคนใช้ร่วมกัน

2. Internet Control Message Protocol (ICMP)

ถึงแม้ว่า IP จะเป็น Datagram Service และไม่มีการรับประกันรูปแบบการส่ง โดย Internet Control Message Protocol (ICMP) จะถูกจัดเตรียมไว้ภายใน IP ทำให้เกิด Error Messages ให้เข้าไปช่วยชั้น IP ให้มีความสามารถในการส่งที่ดีที่สุดโดยหน้าที่หลักของโปรโตคอล ICMP คือการแจ้งหรือแสดงข้อความจากระบบ เพื่อบอกให้ผู้ใช้ทราบว่าเกิดอะไรขึ้นในการส่งผ่านข้อมูลนั้นซึ่งปัญหาส่วนมากที่พบคือส่งไปไม่ได้หรือปลายทางรับข้อมูลไม่ได้ เป็นต้นนอกจากนี้โปรโตคอล ICMP ยังถูกเรียกใช้งานจากเครื่องเซิร์ฟเวอร์และ เราท์เตอร์อีกด้วยเพื่อแลกเปลี่ยนข้อมูลที่ใช้ควบคุม ส่วนรูปแบบการทำงานของโปรโตคอล ICMP นั้นจะทำควบคู่กับโปรโตคอล IP ในระบบเดียวกันและข้อความต่างๆที่แจ้งให้ทราบจะถูกผนึกอยู่ภายใน IPdatagram อีกที

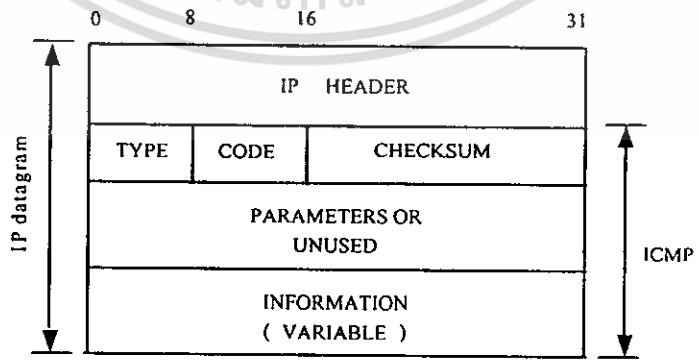
รูปที่ 2.32 แสดงรูปแบบพื้นฐานของ ICMP Message Encapsulated ใน IPdatagram ใน ICMP มีหมายเลข IP โปรโตคอลของตัวเอง ดังนั้นชั้น IP รู้ว่ารับ ICMP แม้ว่า ICMP ใช้ ชั้น IP ที่เป็นตัวพิจารณาว่า IP ภายในเป็นของใครเพราะว่าไม่สามารถจัดเตรียมให้กับ ชั้นที่สูงกว่าได้นับตั้งแต่ IP Message ที่ถูกขนย้ายใน IPจะถูกทิ้งไปเหมือนกับ IPdatagramโดยมันจะไม่สามารถรักษาสถานภาพไว้ได้ ICMP Message จะไม่ถูกทำให้เกิดขึ้นในกรณีที่ ICMP Message เกิดความผิดพลาดเกิดขึ้น

รูปแบบพื้นฐานของ ICMP Datagram แสดงไว้ในรูปที่ 2.33โดยจะประกอบไปด้วยการแบ่งประเภทของ ICMP Message และ Code ที่ต้องจัดเตรียมรายละเอียด Checksum ต้องถูกนำมาใช้ เพราะ IP ไม่สามารถที่จะป้องกันข้อมูลของมันได้ เมื่อทำการดำเนินการมาอยู่เหนือ Physical Network ที่มี Frame Check Sequence ICMP Checksum ต้องเป็น 0 นั่นหมายความว่าจะไม่มีการคำนวณเกิดขึ้น



Type field	Message type
0	Echo reply
3	Destination unreachable
4	Source quench
5	Redirect (change route)
8	Echo request
11	Time exceeded for datagram
12	Parameter problem on datagram
13	Time stamp request
14	Time stamp reply
15	Information request
16	Information reply
17	Address mask request
18	Address mask response

รูปที่ 2.32 ICMP encapsulated ใน IP และประเภทของ ICMP



รูปที่ 2.33 รูปแบบของ ICMP Datagram

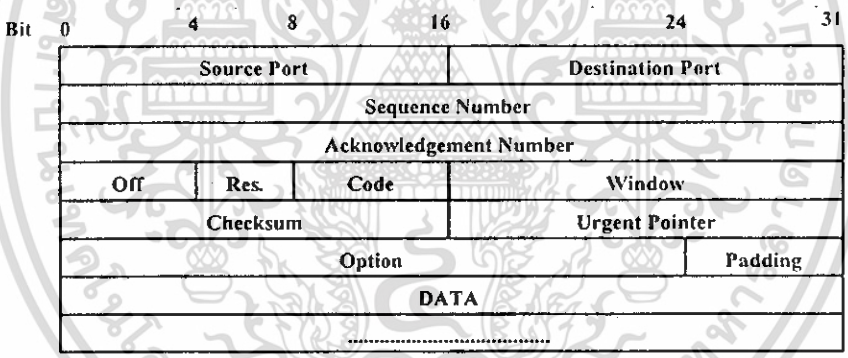
2.3.3.Transport Layer

เป็นชั้นที่ถัดจากชั้นแอพพลิเคชัน ทำหน้าที่เชื่อมต่อระหว่างความต้องการของโปรแกรมแอพพลิเคชันกับบริการที่ทางโครงข่ายจัดเตรียมไว้ให้ในการรับส่งข้อมูลระหว่างโฮสต์ที่อยู่ห่างไกลกันโปรโตคอลในชั้นทรานสปอร์ตประกอบด้วย

- โปรโตคอล TCP (Transmission Control Protocol)
- โปรโตคอล UDP (User Datagram Protocol)

1.โปรโตคอล TCP

โปรโตคอล TCP เป็นโปรโตคอลที่มีการรับส่งข้อมูลแบบ Stream Oriented Protocol หมายความว่าการรับส่งข้อมูลจะไม่คำนึงถึงปริมาณข้อมูลที่จะส่งไปแต่จะแบ่งข้อมูลเป็นส่วนย่อยๆก่อนแล้วจึงส่งไปยังปลายทางอย่างต่อเนื่องเป็นลำดับข้อมูลในกรณีที่ข้อมูลส่วนใดส่วนหนึ่งสูญหายไปก็จะส่งข้อมูลส่วนนั้นใหม่อีกครั้ง สำหรับปลายทางก็จะทำหน้าที่จัดเรียงส่วนของข้อมูล Datagram ดังนั้นแอพพลิเคชันหรือกระบวนการใดที่อาศัยการส่งผ่านข้อมูลด้วยโปรโตคอล TCP จะต้องใช้หน่วยความจำและขนาดของช่องสัญญาณ (Bandwidth) มากกว่า UDP ดังรูปที่ 2.34



รูปที่ 2.34 แสดงโครงสร้างของโปรโตคอล TCP

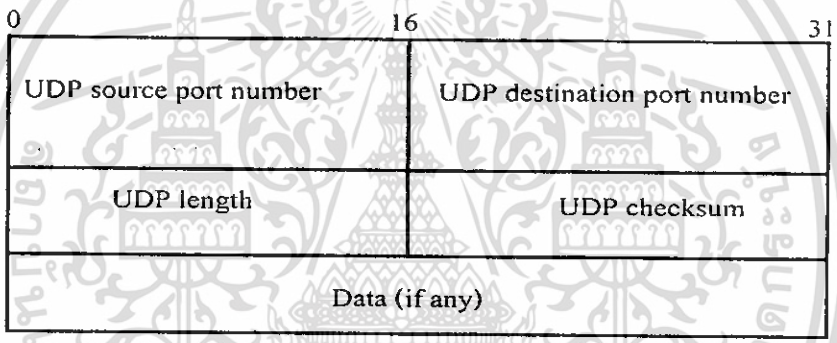
2.โปรโตคอล UDP

ในชั้นทรานสปอร์ตนอกจากจะมีโปรโตคอล TCP ทำงานแล้วก็ยังมีโปรโตคอล UDP ในการส่งข้อมูลแต่ละครั้งและไม่มีการส่งข้อมูลใหม่อีกในกรณีที่เกิดความผิดพลาดของการส่งข้อมูล เมื่อเป็นเช่นนี้แอพพลิเคชันหรือกระบวนการใดที่ต้องอาศัยโปรโตคอล UDP จะเป็นแบบที่ทั้งสองด้านไม่จำเป็นต้องอาศัยการสร้างช่องทางเชื่อมต่อกัน ระหว่างเครื่องเซิร์ฟเวอร์ให้บริการกับเครื่องที่ขอใช้บริการ โดยไม่ต้องแจ้งให้ฝ่ายรับข้อมูลเตรียมรับข้อมูลเหมือนโปรโตคอล TCP และไม่มีการตรวจสอบความถูกต้องครบถ้วนในการรับส่งข้อมูลนั้นๆ ด้วยเนื่องจากโปรโตคอล UDP ไม่มีสัญญาณตรวจทานข้อมูล ในการส่งข้อมูลแต่ละครั้งและไม่มีการส่งข้อมูลใหม่อีกในกรณีที่เกิดความผิดพลาดของการส่งข้อมูลเมื่อเป็นเช่นนี้แอพพลิเคชัน

หรือกระบวนการใดที่ต้องอาศัยโปรโตคอล UDP ในการส่งผ่านข้อมูลก็อาจจะต้องสร้างขบวนการตรวจสอบข้อมูลขึ้นมาเอง

โครงสร้างDatagram UDP

โครงสร้าง Datagram UDP มีลักษณะดังรูปที่2.35 พิจารณาดูสองฟิลด์แรกได้แก่หมายเลขพอร์ตต้นทาง (UDP Source port number) และหมายเลขพอร์ตปลายทาง (UDP Destination port number) ลักษณะการใช้งานหมายเลขพอร์ตในโปรโตคอล UDP เป็นดังนี้คือ เมื่อโปรแกรมแอพพลิเคชันหนึ่งมีการใช้งานสื่อสารของ UDP โปรแกรมดังกล่าวจะต้องกำหนดหมายเลขพอร์ตของโฮสต์ต้นทางและโฮสต์ปลายทาง หมายเลขพอร์ตของโฮสต์ปลายทางเป็นส่วนสำคัญและเป็นค่าที่ระบุชนิดของโปรแกรมแอพพลิเคชันที่โฮสต์ต้นทางต้องการติดต่อกับโฮสต์ปลายทาง ส่วนหมายเลขพอร์ตต้นทางระบุเพื่อให้โปรแกรมแอพพลิเคชันปลายทางสามารถตอบกลับให้ถูกต้องตรงกันสังเกตว่าการเลือกหมายเลขพอร์ตต้นทางไม่สัมพันธ์กับชนิดของโปรแกรมแอพพลิเคชัน



รูปที่ 2.35โครงสร้างDatagramของโปรโตคอล UDP

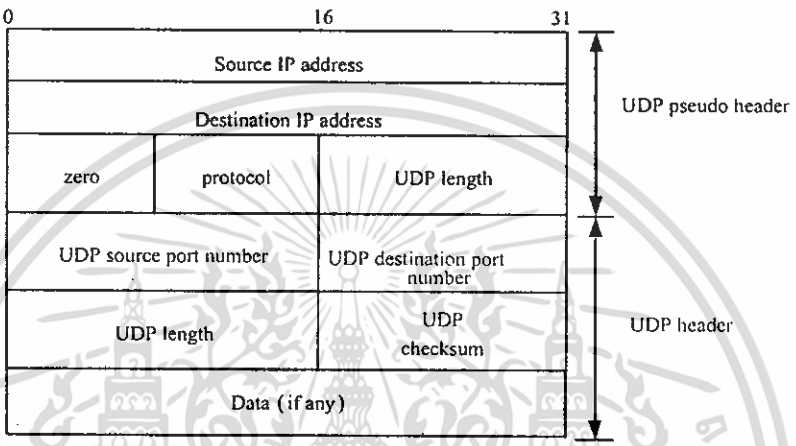
1.ฟิลด์ UDP Length มีขนาด 8 บิตกำหนดเพื่อบ่งบอกจำนวนไบต์หรืออ็อกเตทของ Datagram UDP ซึ่งนับรวมทั้งส่วนเฮดเดอร์และส่วนข้อมูลรวมกัน ฉะนั้นฟิลด์นี้ย่อมมีค่าอย่างต่ำเท่ากับ8บิตซึ่งคือขนาดของเฮดเดอร์นั่นเอง สังเกตว่าข่าวสารส่วนนี้มีความซับซ้อนกับฟิลด์ Length ที่กำกับอยู่ที่ เฮดเดอร์ของ IPdatagram

2.ฟิลด์ UDP Checksum ขนาด 8 บิต มีไว้สำหรับตรวจสอบความผิดพลาดของDatagram UDPการคำนวณฟิลด์ UDP Checksum มีการนำองค์ประกอบของข้อมูลถึง 3 ส่วนร่วมในการคำนวณเพื่อตรวจสอบความถูกต้องได้แก่

1. เฮดเดอร์ UDP (UDP Header)
2. ข้อมูล UDP (UDP Data)
3. เฮดเดอร์เทียม UDP (UDP Pseudo Header)

เมื่อเทียบกับการคำนวณ Checksum ของโปรโตคอล IP จะพบจุดแตกต่างที่น่าสนใจคือในกรณีโปรโตคอล IP การคำนวณ Checksum จะกระทำเฉพาะกับส่วนเฮดเดอร์ของ IPdatagram เท่านั้น

ส่วนข้อมูลของ IPdatagram จะถูกส่งผ่านโครงข่ายโดยไม่มีการตรวจสอบความผิดพลาดเลย ในขณะที่ Datagram UDP จะตรวจสอบ Checksum ทั้งกับเฮดเดอร์และข้อมูล สังเกตว่าเวลาใช้จริง Datagram UDP จะถูกบรรจุในส่วนข้อมูลของ IPdatagram ฉะนั้นข่าวสารจากโปรแกรมแอพพลิเคชันจึงได้รับการตรวจสอบความถูกต้องเมื่อมีการใช้งานผ่านโปรโตคอล UDP อย่างไรก็ตามโปรโตคอล UDP ไม่มีการแก้ปัญหาความผิดพลาดที่อาจเกิดขึ้นอีกทั้งการคำนวณ Checksum ของโปรโตคอล UDP ก็ไม่ได้กำหนดเป็นข้อบังคับว่าต้องทำ ผู้พัฒนาซอฟต์แวร์สามารถเลือกจะคำนวณหรือไม่ทำก็ได้



รูปที่ 2.36 องค์ประกอบที่ใช้ในการคำนวณ Checksum ของโปรโตคอล UDP

ในการคำนวณ Checksum ของโปรโตคอล UDP นอกจากจะพิจารณาจากเฮดเดอร์และข้อมูลของ Datagram UDP แล้วยังนำฟิลด์บางฟิลด์ในเฮดเดอร์ของ IPdatagram มาคำนวณด้วยและเรียกส่วนเพิ่มเติมนี้ว่า เฮดเดอร์เทียม UDP จากรูปที่ 2.36จะเห็นว่ามีการนำหมายเลข IPaddress ของอุปกรณ์ต้นทางและปลายทาง ฟิลด์ Protocol และ ฟิลด์ UDP Length มาร่วมในการคำนวณ สังเกตว่า ฟิลด์ UDP Length ในเฮดเดอร์เทียมเป็นข้อมูลที่ซ้ำซ้อนกับเฮดเดอร์ UDP การคำนวณหมายเลข IPaddress มาร่วมในการตรวจสอบพร้อมกับหมายเลขพอร์ตมีวัตถุประสงค์เพื่อให้เกิดความแน่ใจว่า คู่ซอกเก็ต (Socket pair) ของการเชื่อมต่อหรือคอนเนกชันของโปรแกรมแอพพลิเคชันมีความถูกต้องและแน่นอน (หมายเลข ระบุจะไม่มีการส่งเฮดเดอร์เทียมออกไปกับ Datagram UDP แต่อย่างใด เฮดเดอร์เทียมใช้เฉพาะกับการคำนวณค่า Checksum เท่านั้น)

วิธีการคำนวณค่า Checksum ของ Datagram UDP มีขั้นตอนดังนี้คือนำฟิลด์ต่างๆที่เกี่ยวข้องทั้งหมดมาบวกกันครั้งละ 16บิตแบบ One 's complementในกรณีที่จำนวนบิตของส่วนท้ายสุดมีค่าไม่ลงตัวที่ 16 บิตให้เติมศูนย์ (Padding) ต่อท้ายจนครบ 16 บิต เพื่อให้คำนวณได้ทั้งนี้ระบบจะไม่ส่งบิตศูนย์เหล่านี้ผ่านโครงข่ายไปกับ Datagram UDP แต่อย่างใด ผลการบวกที่ได้มาทำการ One 's complement ซึ่งคือการสลับค่าบิตจากศูนย์เป็นหนึ่งและจากบิตหนึ่งเป็นศูนย์นั่นเอง ผลลัพธ์ที่ได้เป็นค่าที่บรรจุลงในฟิลด์ Checksum สำหรับกระบวนการตรวจสอบความถูกต้องของ Datagram UDP ที่โฮสต์ปลายทางมีขั้นตอนการทำงาน

ดังนี้ นำฟิลด์ต่างๆที่ใช้ในการคำนวณ Checksum ทั้งหมดบวกกับค่าในฟิลด์ Checksum ครั้งละ 16 บิต แบบ One 's complement หากผลการบวกมีค่าเป็นหนึ่งทั้ง 16 บิต ก็แสดงว่าไม่มีความผิดพลาดเกิดขึ้นกับ Datagram UDP ดังกล่าว แต่ถ้าได้ค่าที่ต่างไปก็แสดงความผิดพลาดเกิดขึ้นกับ Datagram UDP

เนื่องจากการตรวจสอบความผิดพลาดของฟิลด์ Checksum ในโปรโตคอล UDP มิได้กำหนดเป็นข้อบังคับว่าต้องทำเสมอ ดังนั้นหากผู้พัฒนาโปรแกรมเลือกที่จะไม่ตรวจสอบความผิดพลาด ก็ตั้งค่าในฟิลด์ Checksum ทั้ง 16 บิตให้เป็นศูนย์ทั้งหมด ฉะนั้นเมื่อโฮสต์ปลายทางตรวจพบว่าฟิลด์ Checksum มีค่าเป็นศูนย์จะทราบทันทีว่าไม่มีการใช้งานฟิลด์ดังกล่าว การตกลงกันระหว่างโฮสต์ต้นทางและปลายทางในลักษณะนี้มักทำให้เกิดคำถามขึ้นว่าหากระบบมีการคำนวณ Checksum และเผอิญผลการคำนวณที่ได้มีค่าเป็นศูนย์จะก่อให้เกิดความเข้าใจผิดหรือไม่คำตอบคือไม่เนื่องจากในระบบการบวกแบบ One 's complement ตัวเลขศูนย์สามารถแสดงได้ 2 รูปแบบคือ แบบที่ทุกบิตมีค่าเป็นศูนย์ และแบบที่ทุกบิตมีค่าเป็นหนึ่ง ในกรณีที่ผลการคำนวณ Checksum มีค่าเป็นศูนย์ระบบจะบรรจุค่าลงในฟิลด์ Checksum ด้วยบิตที่มีค่าเป็นหนึ่งทั้งหมด

2.3.4. Application Layer

การแสดงลำดับชั้นการทำงานของโปรโตคอล TCP/IP เทียบกับมาตรฐาน OSI model นั้นในชั้นบนสุดเรียกว่าชั้นแอพพลิเคชัน (Application Layer)ในชั้นนี้จะรองรับการทำงานของแอพพลิเคชันต่างๆ ที่ทำงานเป็นกระบวนการอยู่ในเครื่องเซิร์ฟเวอร์ที่ให้บริการและเครื่องที่ขอใช้บริการ หรือลูกข่าย ซึ่งจะติดต่อกันผ่านโปรโตคอลเฉพาะแอพพลิเคชันอีกทีหนึ่ง ตัวอย่างเช่น เมื่อผู้ใช้งานอินเตอร์เน็ตต้องการโอนถ่ายไฟล์หรือ ดาวโหลด (Download) ข้อมูลจากเครื่องเซิร์ฟเวอร์ที่ให้บริการโดยอาจจะเรียกใช้โปรแกรม FTP Client ทั่วไป เช่น โปรแกรม WS_FTP ติดต่อกับกระบวนการ FTP ที่กำลังให้บริการอยู่ที่เครื่องเซิร์ฟเวอร์ จากนั้นตัวกระบวนการ FTP ก็จะเรียกใช้โปรโตคอล FTP (File Transfer Protocol) เพื่อทำการโอนถ่ายไฟล์นี้ หรือถ้าผู้ใช้ต้องการเรียกใช้งานคอมพิวเตอร์ที่อยู่ห่างไกลออกไปด้วยการใช้โปรแกรมเทลเน็ต (Telnet) ที่เครื่องเซิร์ฟเวอร์ให้บริการ ตัวกระบวนการ เทลเน็ต ที่ทำงานอยู่ก็จะเรียกใช้โปรโตคอลเทลเน็ตเพื่อติดต่อกัน หรือในกรณีที่มีการเรียกใช้โปรแกรม Web Browser เช่น Netscape Navigator เพื่อเรียกดูเว็บไซท์ CNN ที่เครื่องซึ่งให้บริการเว็บของ CNN ก็จะมีกระบวนการ HTTP (Hypertext Transfer Protocol) ทำงานอยู่และจะติดต่อกับผู้ใช้ผ่านโปรโตคอล HTTP เป็นต้น

การทำงานของแอพพลิเคชันต่างๆ จะอยู่ที่ ชั้นแอพพลิเคชันนี้ และมีการติดต่อกันตามแต่ละโปรโตคอลเฉพาะแล้วแต่แอพพลิเคชันที่ใช้งานจากการที่ชั้นแอพพลิเคชันของ TCP/IP รองรับให้โปรโตคอลอื่นทำงานได้หลายกระบวนการและหลายโปรโตคอลได้พร้อมกันนั้น ทำให้ผู้ใช้สามารถเปิดโปรแกรมใช้งานได้หลายๆ โปรแกรมพร้อมกัน เช่น เปิดโปรแกรม Internet Explorer เพื่อเรียกดูเว็บเพจพร้อมกับใช้งานโปรแกรม Outlook Express เพื่อรับส่งอีเมล์ไปพร้อมกันได้โดยไม่ต้องรอให้ทำงานอย่างหนึ่งอย่างใดเสร็จก่อน หรือในปัจจุบันมีการพัฒนาโปรแกรม Web Browser ให้สามารถเรียกใช้งานโปรโตคอลอื่นๆ ได้มากขึ้นทำให้เราสามารถใช้โปรแกรม Web Browser โอนถ่ายไฟล์ข้อมูลที่ใช้โปรโตคอล FTP ได้โดยไม่ต้องไปหาโปรแกรมอื่นมาใช้

โปรโตคอลหลักๆ ที่ทำงานใน ชั้นแอพพลิเคชันซึ่งผู้ใช้มักจะคุ้นเคยกันดีได้แก่

FTP (File Transfer Protocol), Telnet, HTTP (Hyper Text Transfer Protocol), SMT (Simple Mail Transfer Protocol) นอกจากนี้ยังมีโปรโตคอลอื่นที่อยู่เบื้องหลัง ซึ่งทำงานโดยที่ผู้ใช้ไม่ได้มีการใช้งานโดยตรง เช่น

- โปรโตคอล DNS (Domain Name System) ที่ทำหน้าที่แปลงข้อมูลชื่อ Domain Name หรือชื่อเว็บไซท์ ทั้งหลายให้เป็นหมายเลข IPaddress

- โปรโตคอล DHCP (Dynamic Host Configuration Protocol) ทำหน้าที่แจกจ่ายข้อมูลพารามิเตอร์ของเครือข่ายให้กับเครื่องลูกข่ายที่เชื่อมต่ออยู่

บทที่ 3
การคำนวณและการสร้างวงจร

หลังจากที่ทราบถึงทฤษฎีและหลักการในบทที่ 2 แล้วเราก็สามารถทำการคำนวณและทำการสร้างวงจรโดยในโครงงานนี้จะแบ่งส่วนประกอบหลักของระบบออกเป็น 4 ส่วนด้วยกันคือ

1.โปรแกรมที่ทำหน้าที่ติดต่อรับ-ส่งข้อมูลกับฮาร์ดแวร์

2. ฮาร์ดแวร์ของระบบที่ใช้ในการรับ-ส่งข้อมูล ผ่านเครือข่ายท้องถิ่นโดยมีคอมพิวเตอร์ศูนย์กลางที่รอรับข้อมูลแล้วส่งคำสั่งมายังฮาร์ดแวร์

3. ฮาร์ดแวร์ที่ใช้ในการควบคุมการจ่ายกระแสไฟฟ้าภายในห้องพัก

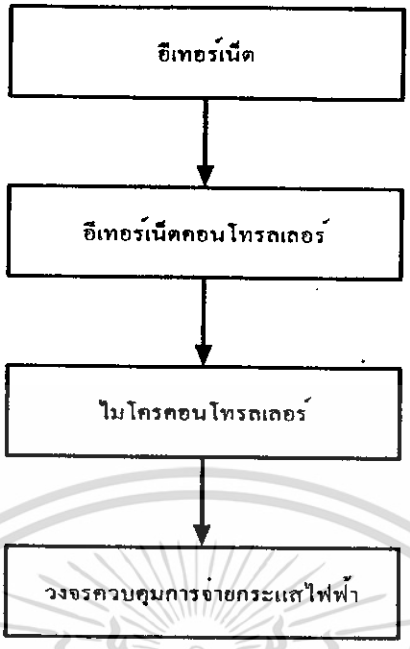
4. ส่วนของการเชื่อมต่อระหว่างฮาร์ดแวร์กับเครือข่ายไร้สายโดยใช้แอ็กเซสพอยต์

3.1.ฮาร์ดแวร์ของระบบที่ใช้ในการรับ–ส่งข้อมูล ผ่านเครือข่ายท้องถิ่น

ในส่วนฮาร์ดแวร์ของระบบควบคุมนั้นจะใช้การควบคุมแบบฝังตัวซึ่งจะประกอบด้วย วงจรควบคุมการรับ-ส่งข้อมูลผ่านอีเทอร์เน็ต ไมโครคอนโทรลเลอร์ และหลอดไฟ LED แสดงผลของข้อมูลที่ประมวลผลได้จากเครื่องคอมพิวเตอร์ศูนย์กลาง รายละเอียดการออกแบบฮาร์ดแวร์ที่จะกล่าวถึงในที่นี้จึงประกอบด้วย การเชื่อมต่อฮาร์ดแวร์เข้ากับระบบเครือข่าย โดยอาศัยอุปกรณ์ควบคุมการเชื่อมต่อกับเครือข่ายท้องถิ่น (Embedded Ethernet Controller) และอธิบายถึงการควบคุม I/O พอร์ต ซึ่งถูกควบคุมด้วยไมโครคอนโทรลเลอร์ และกระบวนการรับ-ส่งข้อมูลของฮาร์ดแวร์

3.1.1. ส่วนประกอบของฮาร์ดแวร์ในการเชื่อมต่อกับอีเทอร์เน็ต

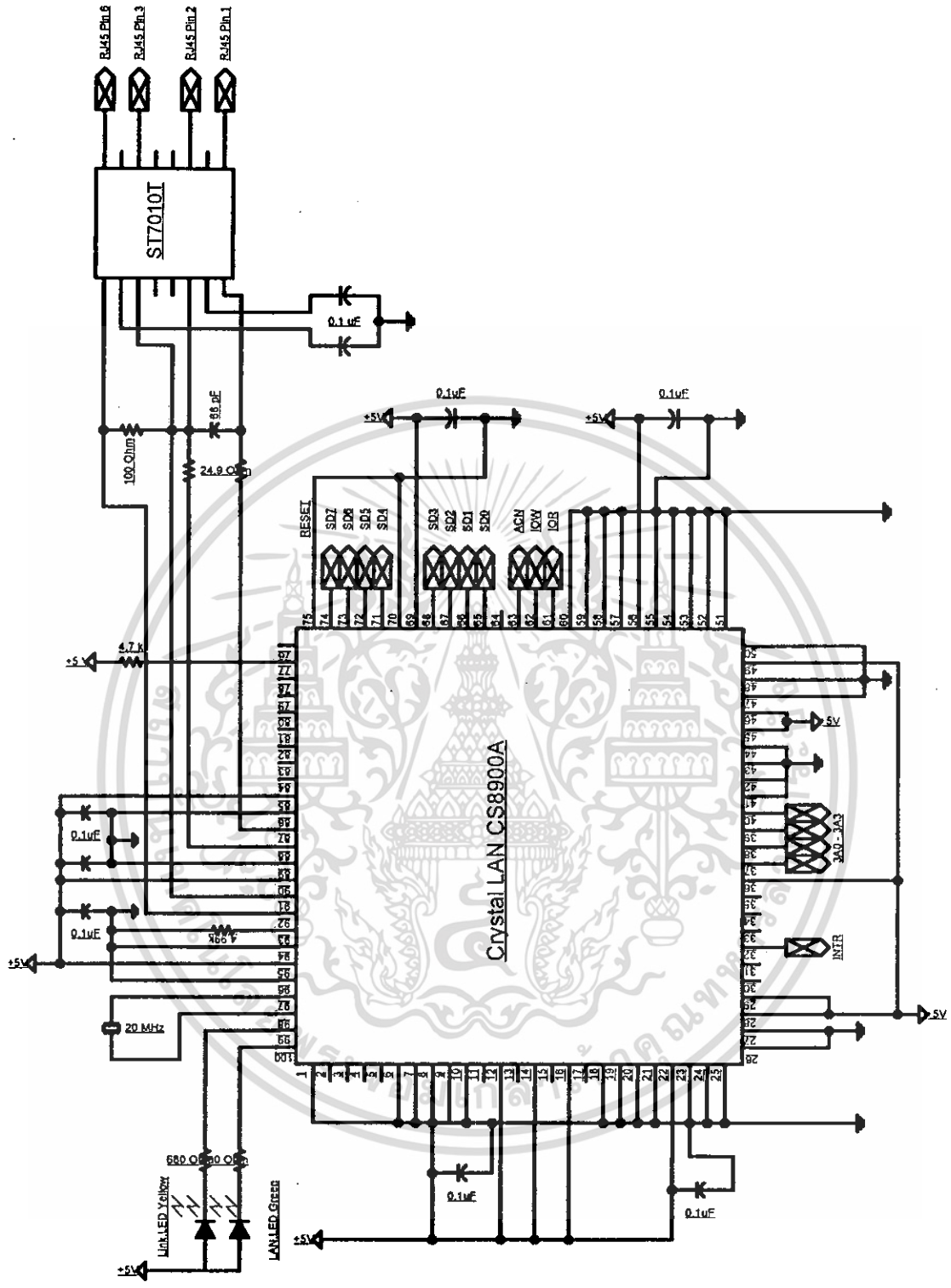
ส่วนประกอบหลักของฮาร์ดแวร์ทั้งหมดประกอบด้วย วงจรเชื่อมต่อกับระบบเครือข่ายโดยในส่วนนี้จะเชื่อมต่อกับอีเทอร์เน็ตและไมโครคอนโทรลเลอร์ โดยที่ไมโครคอนโทรลเลอร์จะไปควบคุมการทำงานจาก I/O พอร์ต ของอีเทอร์เน็ตคอนโทรลเลอร์ ดังรูปที่ 3.1 เป็นการแสดงขั้นตอนทำงานของระบบ



รูปที่ 3.1 แสดงส่วนประกอบหลักของฮาร์ดแวร์ที่ส่งข้อมูลผ่านเครือข่ายท้องถิ่น

3.1.2. ส่วนเชื่อมต่อระบบเครือข่าย

จะใช้อุปกรณ์ควบคุมการเชื่อมต่อระบบเครือข่าย (Ethernet Controller) แสดงดังรูปที่ 3.2 โดยภายในวงจรจะประกอบไปด้วยส่วนประกอบหลักกับชิปควบคุมอีเทอร์เน็ต ในที่นี้จะทำการเลือกใช้ CS8900A-CQ, Isolator Transformer (ST7010T) และ RJ-45 Connector และ วงจรควบคุมการเชื่อมต่อระบบเครือข่ายจะมี PIN OUT 18 ขา ดังรูปที่ 3.3



รูปที่ 3.2 แสดงส่วนเชื่อมต่อระบบเครือข่าย

PIN 1	PIN 2	PIN 3	PIN 4	PIN 5	PIN 6	PIN 7	PIN 8	PIN 9
GND	VCC	INTR	SA0	SA1	SA2	SA3	/IOR	/IOW

PIN 10	PIN 11	PIN 12	PIN 13	PIN 14	PIN 15	PIN 16	PIN 17	PIN 18
/AEN	SD0	SD1	SD2	SD3	SD4	SD5	SD6	SD7

รูปที่ 3.3 PIN OUT

VCC - แหล่งจ่ายไฟตรง +5 V

GND - กราวด์อ้างอิง 0 V

INTR - สำหรับใช้งานในโหมดอินเตอร์รัปต์

SA0 – SA3 - Address Bus เชื่อมต่อกับไมโครคอนโทรลเลอร์

/IOR - I/O Port Read (Active low)

/IOW - I/O Port Write (Active low)

/AEN - Chip Enable (Active low)

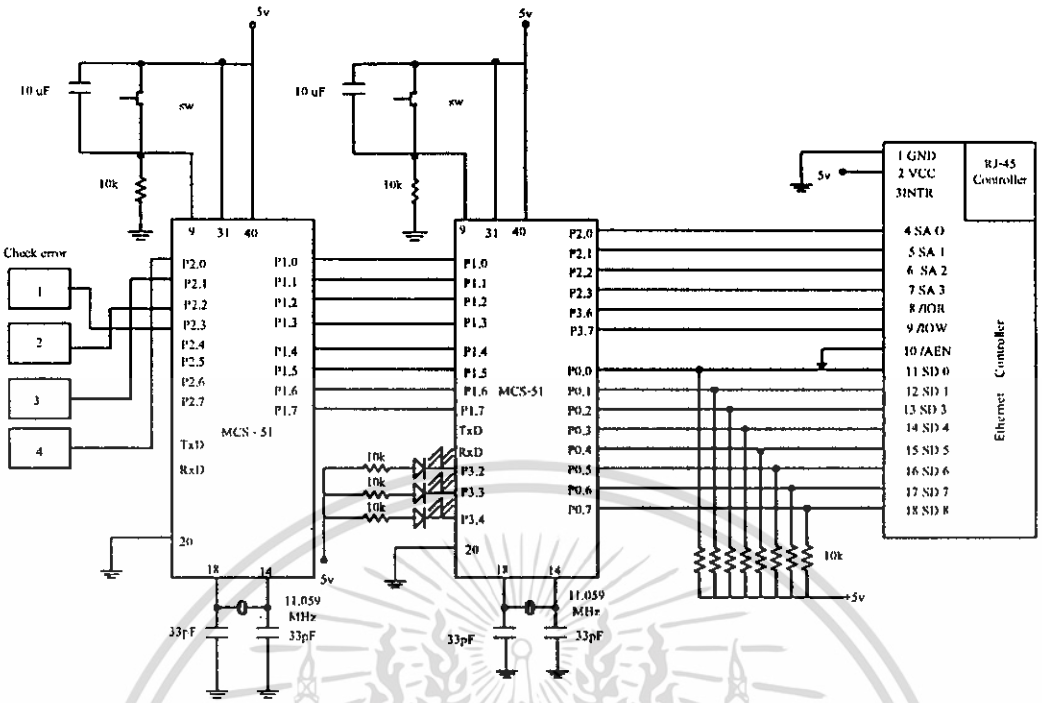
SD0 – SD7 - Data Bus เชื่อมต่อกับไมโครคอนโทรลเลอร์

และมี LED แสดงผลคือ

- Link LED (Yellow) จะกระพริบเมื่อมีเฟรมข้อมูลส่งออกอีเทอร์เน็ตคอนโทรลเลอร์
- LAN LED (Green) จะกระพริบเมื่อมีเฟรมข้อมูลเข้ามายังอีเทอร์เน็ตคอนโทรลเลอร์

3.1.3 การติดต่อกับอุปกรณ์ต่างๆ

ในการใช้ไมโครคอนโทรลเลอร์ในที่นี้จะใช้ MCS-51 เบอร์AT89C52 เป็นไมโครคอนโทรลเลอร์ที่ส่งข้อมูลทีละ 8 บิต ไปควบคุมอุปกรณ์ควบคุมการเชื่อมต่อระบบเครือข่ายโดย SD0–SD7 จะเป็นดาต้าบัสเชื่อมต่อกับ P0.0–P0.7, SA0–SA3 จะเป็น Address Bus เชื่อมต่อกับ P2.0 – P2.3, /IOW ต่อกับ P3.7, /IOR ต่อกับ P3.6, /AEN จะต่อลงกราวด์ ขา INTR ปล่อยลอย เพราะไม่ใช้อินเตอร์รัปต์ ดังรูปที่ 3.4



รูปที่ 3.4 แสดงการติดต่อกับอุปกรณ์ต่างๆ

3.1.4. การเข้าถึงหน่วยความจำของระบบ

ในอุปกรณ์ควบคุมการเชื่อมต่อระบบเครือข่ายจะมีชิปประมวลผลที่สำคัญคือ CS8900A-CQ โดยชิปนี้มีรูปแบบการทำงาน 3 โหมด คือ Memory Mode, I/O Mode และ DMA Mode แต่ในที่นี้จะใช้เพียง I/O Mode เพียงอย่างเดียว ใน I/O Mode จะประกอบด้วย I/O พอร์ต อยู่ 8 พอร์ต แต่ละพอร์ตจะมีความยาว 16 บิต แต่เนื่องจากไมโครคอนโทรลเลอร์ทำงานทีละ 8 บิต จึงจำเป็นต้องส่งข้อมูล 2 รอบ จึงจะเข้าถึง I/O พอร์ต ได้ คำสั่งต่างๆใน I/O Mode จะประกอบด้วย

- Receive / Transmit Data (พอร์ต 0, พอร์ต 1)
  ใช้ในการรับส่งข้อมูลจากอีเทอร์เน็ต ส่วนมากจะใช้พอร์ต 0
- TxCMD (Transmit Command) ใช้ในการสั่งให้อุปกรณ์ควบคุมการเชื่อมต่อระบบเครือข่ายเตรียมตัวส่งข้อมูล
- Tx Length (Transmit Length)
  ใช้ในการระบุความยาวของข้อมูลที่จะส่งเป็นไบต์
- Interrupt Status Queue
  ใช้ในการอินเตอร์รัปต์
- Packet Page Pointer
  ใช้ในการระบุรีจีสเตอร์ภายในของ CS8900A-CQ สามารถหาดูได้จาก Datasheet

- Packet Page Data (พอร์ต 0, พอร์ต 1)ใช้ในการอ่านหรือเขียนรีจีสเตอร์ภายในที่ถูกระบุโดย Packet Page Pointer

ในการระบุคำสั่งต่างๆของ I/O พอร์ต ทำได้โดยการจ่ายไฟไปยัง Address Bus (SA0 – SA4) ดังตารางที่ 3.1

ตารางที่ 3.1 I/O พอร์ตของชิป CS8900A-CQ

Offset	Type	Description
0000h	Read/Write	Receive/Transmit Data (Port 0)
0002h	Read/Write	Receive/Transmit Data (Port 1)
0004h	Write-only	TxCMD (Transmit Command)
0006h	Write-only	TxLength(Transmit Length)
0008h	Read/Write	Interrupt Status Queue
000Ah	Read/Write	PacketPage Pointer
000Ch	Read/Write	PacketPage Data (Port 0)
000Eh	Read/Write	PacketPage Data (Port 1)

ตัวอย่างการเข้าถึงรีจีสเตอร์ภายในของ I/O Mode

ถ้าต้องการเข้าถึงรีจีสเตอร์ Receiver Event (Rx Event) ที่มี Address อยู่ที่ 0x0124 สามารถทำได้โดย

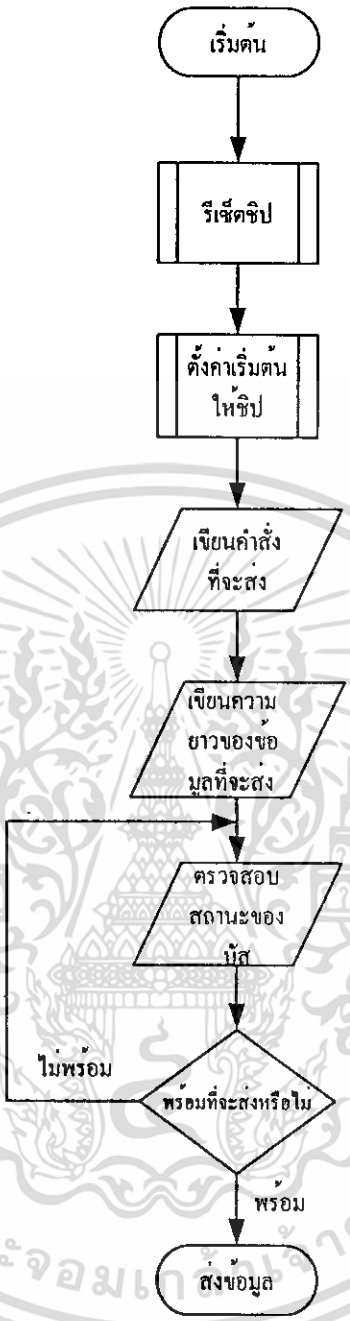
1. Write 0x24 (Least Significant 8 bit) to Packet Page Pointer นั่นคือ Address Bus = 0xa และ Data Bus = 0x24
2. Write 0x01 (Most Significant 8 bit) to Packet Page Pointer + 1 นั่นคือ Address Bus = 0xa + 1 = 0xb และ Data Bus = 0x01
3. เมื่อระบุรีจีสเตอร์แล้วก็จะสามารถ อ่าน(Read) หรือเขียน (Write) รีจีสเตอร์ได้โดยใช้ Packet Page Data พอร์ต 0 ทำได้โดย

- Read / Write to Packet Page Data จะได้ Least Significant 8 บิต นั่นคือ Address Bus = 0xc และ Data Bus = Data Least Significant 8 บิต ที่ต้องการจะ อ่าน หรือ เขียน
- Read / Write to Packet Page Data จะได้ Most Significant 8 บิต นั่นคือ Address Bus = 0xc + 1 = 0xd และ Data Bus = Data Most Significant 8 บิต ที่ต้องการจะ อ่าน หรือ เขียน

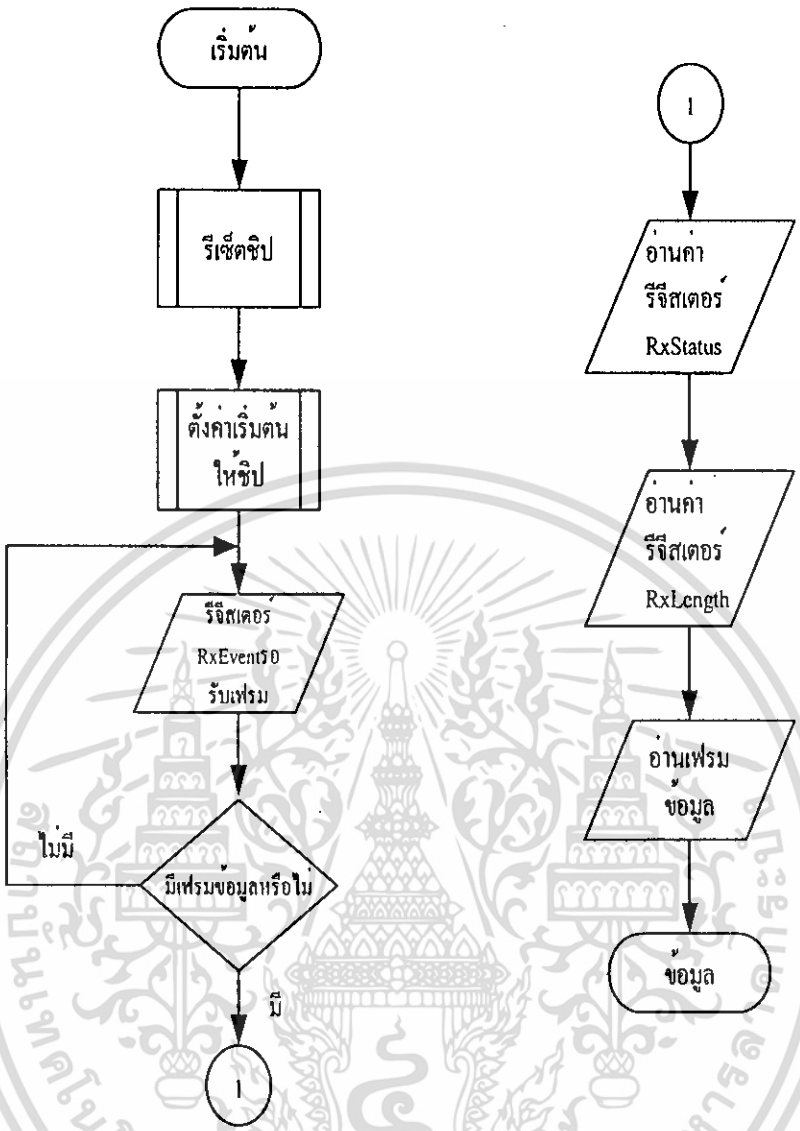
3.1.5. กระบวนการส่งและรับข้อมูลของอีเทอร์เน็ตคอนโทรลเลอร์

ในกระบวนการส่งข้อมูลในอีเทอร์เน็ตคอนโทรลเลอร์เริ่มต้นด้วยการรีเซ็ตเพื่อลบค่าเก่าออกจากอุปกรณ์ควบคุมการเชื่อมต่อระบบเครือข่ายก่อน จากนั้นทำการตั้งค่าเริ่มต้นของอุปกรณ์ควบคุมการเชื่อมต่อระบบเครือข่าย โดยใช้รีจีสเตอร์ RxCTL, LineCTL และค่า MAC Address ต่อมาตามด้วยการเขียนคำสั่งที่ต้องการที่จะส่ง (TxCMD) และ เขียนความยาวของข้อมูล (TxLength) จากนั้นตรวจดูว่าบัสที่ต้องการส่งว่างหรือไม่ โดยตรวจดูจากรีจีสเตอร์ BusST เมื่อบัสว่างก็จะสามารถส่งข้อมูลโดยเข้า I/O พอร์ต คือ Transmit Data (พอร์ต 0) ที่ Address 0x00 ดังในโฟลว์ชาร์ตในการส่งข้อมูลของอีเทอร์เน็ตคอนโทรลเลอร์ ในรูปที่ 3.5

ส่วนกระบวนการรับข้อมูลใน ฮาร์ดแวร์ เริ่มต้นทำการรีเซ็ตและตั้งค่าเริ่มต้นของอุปกรณ์ควบคุมการเชื่อมต่อระบบเครือข่าย และใช้รีจีสเตอร์ RxEvent รอรับ เฟรมเมื่อมีเฟรมเข้ามาให้ทำการอ่านค่า RxStatus และค่า RxLength จาก Receive Data พอร์ต 0 แต่มีข้อต้องระวังคือ RxStatus และ RxLength จะต้องอ่านจาก Most Significant bit ก่อนแล้วจึงค่อยอ่านจาก Least Significant bit คือ Set Address = 0x01 แล้วจึง Set Address = 0x00 จากนั้นก็ทำการอ่านค่าตามปกติจาก I/O Receive Data พอร์ต 0 คือ อ่าน Address = 0x00 แล้วจึงอ่านค่า 0x01 วนไปเรื่อยจนข้อมูลที่ส่งมาครบหมด ดังในโฟลว์ชาร์ตในการรับข้อมูลของอีเทอร์เน็ตคอนโทรลเลอร์ ในรูปที่ 3.6



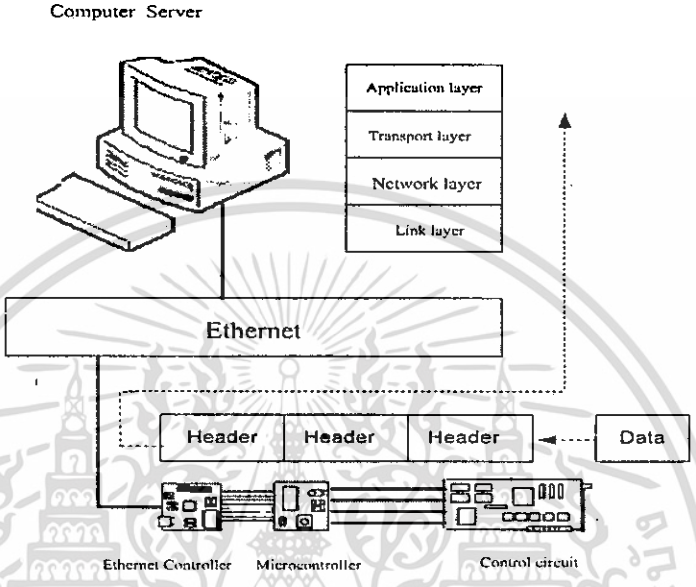
รูปที่ 3.5 แสดงโฟลว์ชาร์ตในการส่งข้อมูลของอีเทอร์เน็ตคอนโทรลเลอร์



รูปที่ 3.6 แสดงโฟลว์ชาร์ตในการรับข้อมูลของอีเทอร์เน็ตคอนโทรลเลอร์

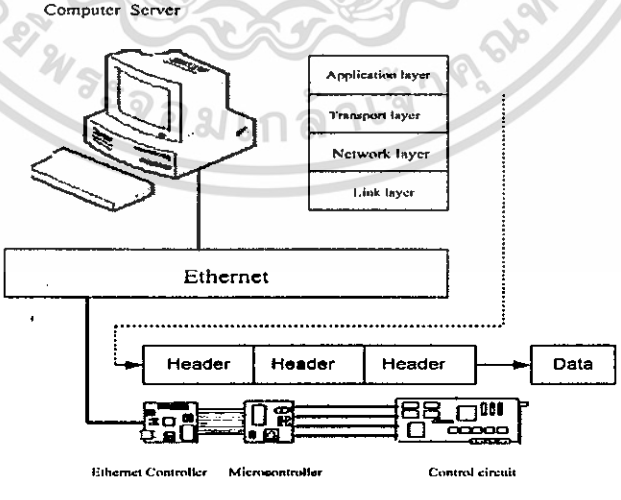
3.1.6. กระบวนการส่งและรับข้อมูลของระบบ

ในการส่งข้อมูลฮาร์ดแวร์จะควบคุมการเชื่อมต่อโดยทำการส่งข้อมูลที่ประกอบไปด้วยข้อมูลที่ทำการส่งและเฮดเดอร์ของแต่ละชั้นโปรโตคอลไปยังเครื่องคอมพิวเตอร์ศูนย์กลางเพื่อประมวลผล การเชื่อมต่อดังแสดงในรูปที่ 3.7



รูปที่ 3.7 แสดงการส่งข้อมูลของระบบ

ส่วนการรับข้อมูล ฮาร์ดแวร์จะรับข้อมูลที่ประกอบไปด้วยเฮดเดอร์และข้อมูลที่มาจากคอมพิวเตอร์ศูนย์กลาง ดังแสดงในรูปที่ 3.8



รูปที่ 3.8 กระบวนการรับข้อมูลของระบบ

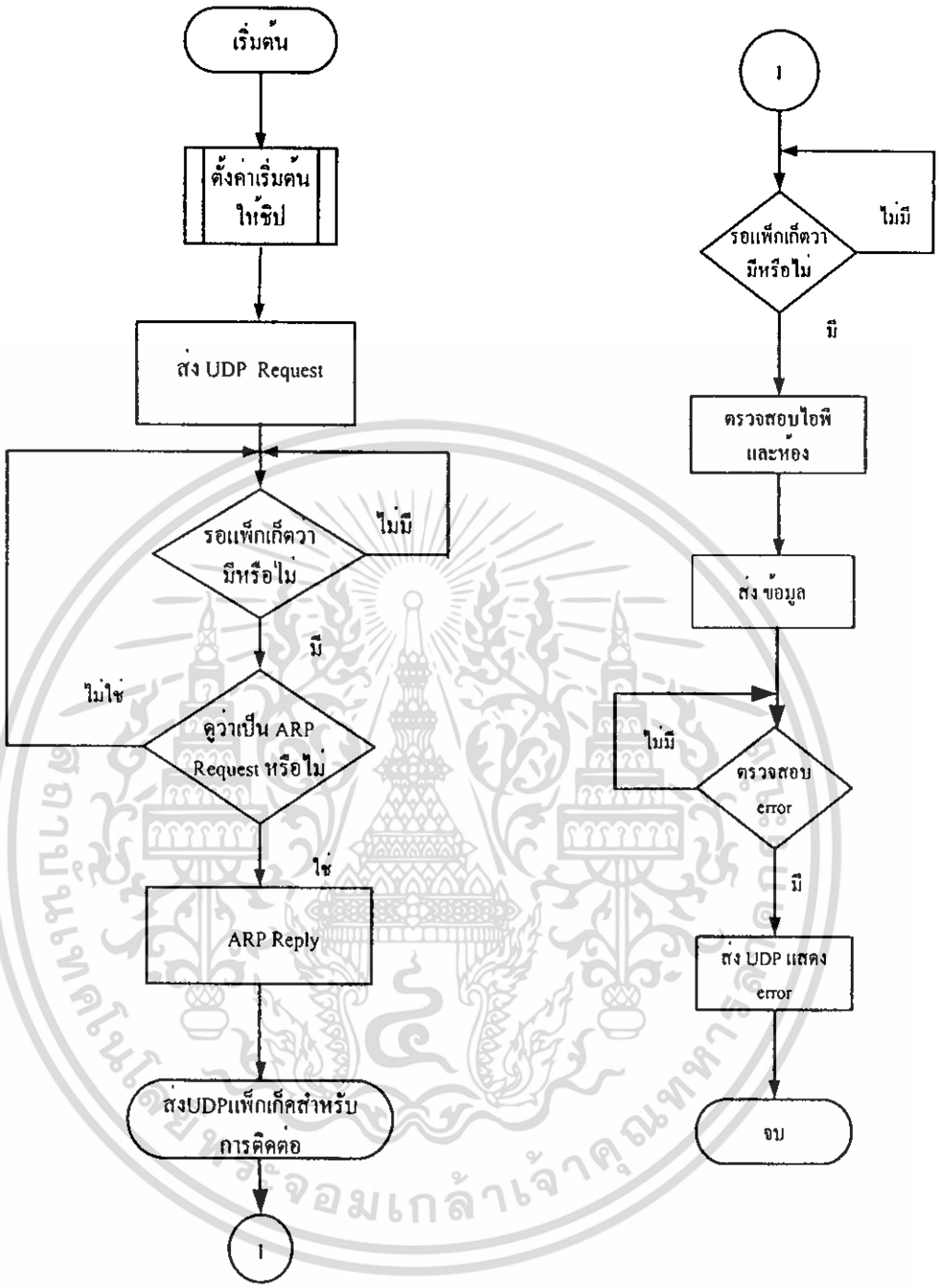
3.1.7. กระบวนการทำงานของฮาร์ดแวร์ และเครื่องคอมพิวเตอร์ศูนย์กลาง

ในการควบคุมอีเทอร์เน็ตคอนโทรลเลอร์โดยการใช้ไมโครคอนโทรลเลอร์ เพื่อแสดงถึงการเชื่อมต่อการรับ-ส่งข้อมูล และการแสดงผลของข้อมูลที่เครื่องคอมพิวเตอร์ศูนย์กลางโดยมีขั้นตอนดังนี้

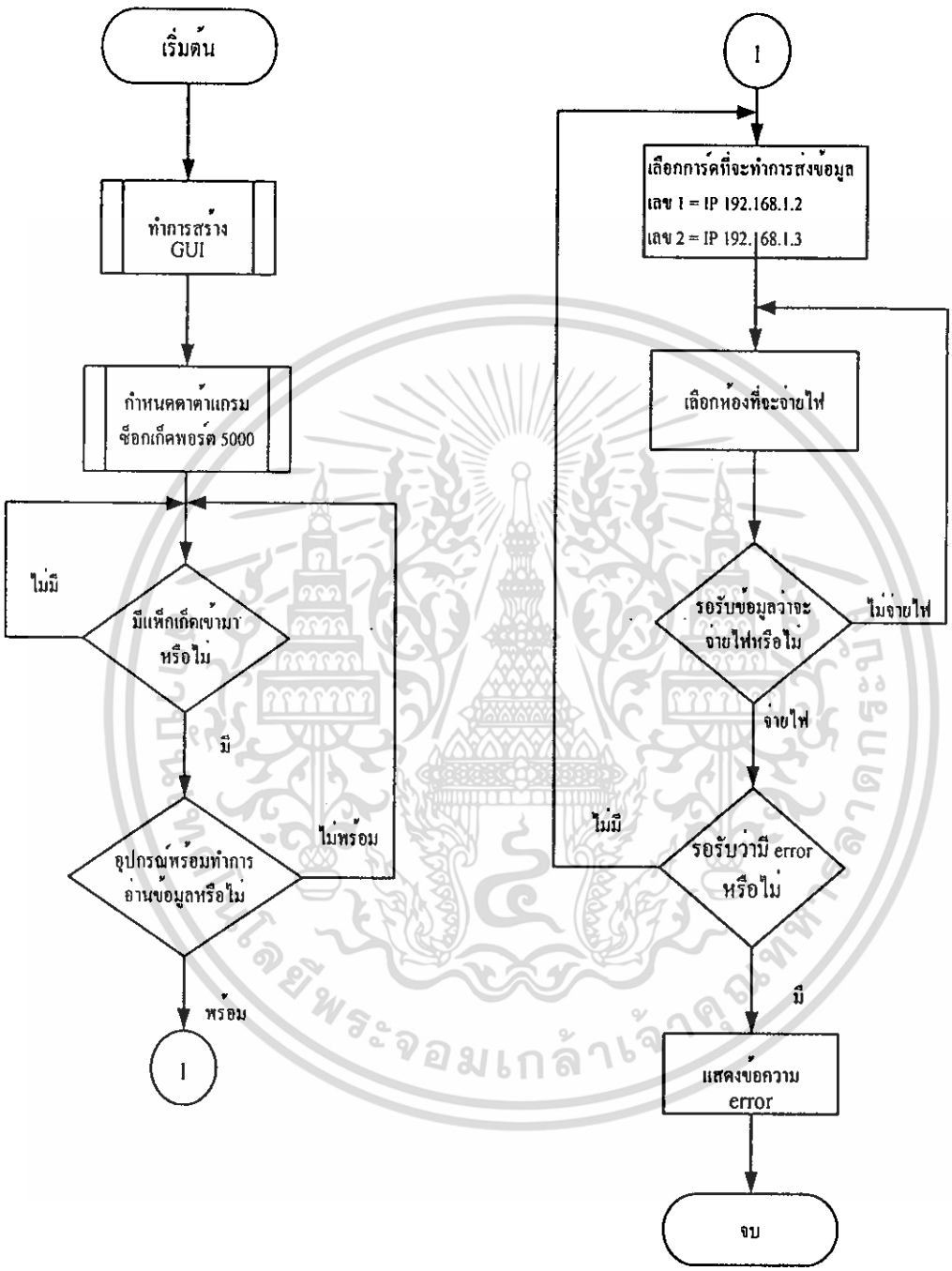
1. ทำการรีเซ็ตชิปและตั้งค่าให้กับอีเทอร์เน็ตคอนโทรลเลอร์
2. ส่งเฟรมข้อมูล Ping Request ซึ่งมี IP ปลายทางเป็นหมายเลข IP ของเครื่องคอมพิวเตอร์ศูนย์กลาง
3. ทำการรอรับเฟรมที่เครื่องคอมพิวเตอร์ศูนย์กลางส่งกลับมา ถ้าเฟรมที่ส่งกลับมาเป็น ARP Request ที่เป็น IP ของตน ฮาร์ดแวร์จะทำการส่ง ARP Reply ส่งกลับไปยังเครื่องคอมพิวเตอร์ศูนย์กลาง เมื่อเครื่องคอมพิวเตอร์ศูนย์กลางทราบ MAC Address ของฮาร์ดแวร์แล้วให้ทำการส่งเฟรม UDP ให้กับเครื่องคอมพิวเตอร์ศูนย์กลางเพื่อแสดงว่าการเชื่อมต่อเรียบร้อย ในขณะนี้ไฟ LED สีเขียวและสีเหลืองจะสว่าง
4. จากนั้นฮาร์ดแวร์จะทำการรอรับเฟรมข้อมูลที่ใช้ในการควบคุมการจ่ายกระแสไฟฟ้าแล้วเช็คว่าเฟรมข้อมูลที่ได้รับเข้ามาเป็นข้อมูลที่ให้ทำการควบคุมการจ่ายกระแสไฟฟ้าที่ฮาร์ดแวร์ตัวไหนและห้องไหน
5. เมื่อได้รับเฟรมข้อมูลจากเครื่องคอมพิวเตอร์ศูนย์กลางแล้ว ก็ทำการจ่ายกระแสไฟบวก 5 โวลต์เพื่อให้จ่ายกระแสไฟฟ้า หรือ จ่ายกระแสไฟฟ้า 0 โวลต์เพื่อทำการตัดกระแสไฟฟ้า
6. ถ้ามีการจ่ายกระแสไฟฟ้าไปยังอุปกรณ์ควบคุมการจ่ายกระแสไฟฟ้าแล้ว ฮาร์ดแวร์ก็จะทำการรอรับข้อมูลจากอุปกรณ์ควบคุมการจ่ายกระแสไฟฟ้าว่ามีความผิดพลาดเกิดขึ้นกับห้องที่จ่ายกระแสไฟฟ้าหรือไม่ ถ้ามีความผิดพลาดก็ให้ทำการส่งเฟรมข้อมูลไปแจ้งที่เครื่องคอมพิวเตอร์ศูนย์กลาง ดังแสดงในโฟลว์ชาร์ตรูปที่ 3.9

และในส่วนของเครื่องคอมพิวเตอร์ศูนย์กลาง จะเขียนโปรแกรมโดยใช้ JAVA เพื่อทำการรับข้อมูลการเชื่อมต่อและส่งข้อมูลควบคุมการจ่ายกระแสไฟฟ้าไปยังฮาร์ดแวร์ โดยมีขั้นตอนการทำงานดังนี้

1. ทำการสร้าง GUI (Graphic User Interface) ชนิด เจ เฟรม แล้วเปิด UDP Socket ซึ่งมีค่าของพอร์ตเท่ากับ 5000 แล้วทำการรอรับเฟรมข้อมูลชนิด UDP จากฮาร์ดแวร์ (ในส่วนของเฟรม Ping และ ARP นั้นการ์ดแลนจะเป็นตัวจัดการในการส่งเฟรม ไม่เกี่ยวข้องกับตัวโปรแกรม)
2. รอรับเฟรม UDP ที่ฮาร์ดแวร์ส่งมาเพื่อแสดงถึงการเชื่อมต่อ ถ้ายังไม่ได้รับเฟรมนี้ตัวโปรแกรมจะไม่ยอมให้ทำการส่งข้อมูลใดๆไปยังฮาร์ดแวร์ได้ เมื่อได้รับเฟรมนี้แล้วก็จะแสดงข้อความว่าพร้อมทำการส่งข้อมูล แล้วจึงจะทำการส่งข้อมูลได้
3. เมื่อส่งข้อมูลเสร็จแล้วก็รอรับข้อมูลว่ามีข้อมูลที่แสดงความผิดพลาดในการจ่ายกระแสไฟฟ้าส่งกลับมาหรือไม่ ถ้ามีก็ทำการแสดงข้อความแจ้งความผิดพลาดที่หน้าจอเครื่องคอมพิวเตอร์ศูนย์กลาง ดังโฟลว์ชาร์ตรูปที่ 3.10

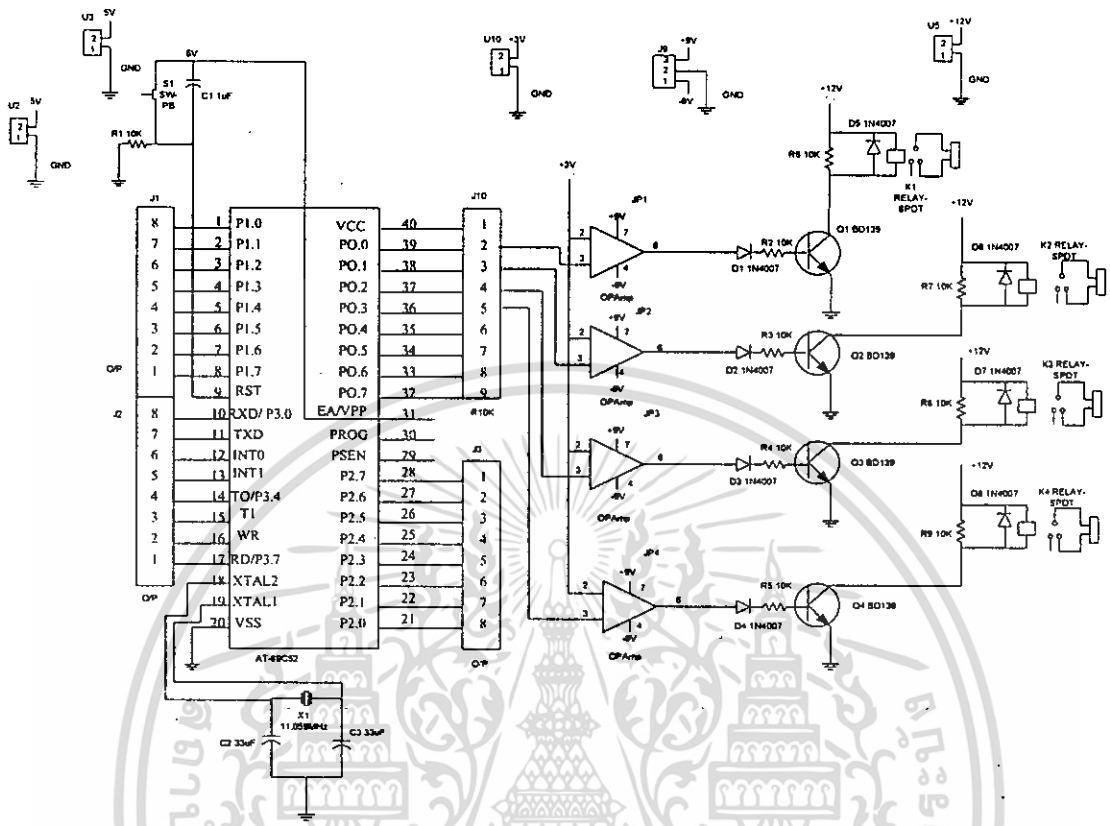


รูปที่ 3.9 แสดงโฟลว์ชาร์ตของการทำงานของฮาร์ดแวร์



รูปที่ 3.10โฟลว์ชาร์ตแสดงการทำงานที่เครื่องคอมพิวเตอร์ศูนย์กลาง

3.1.8.วงจรควบคุมการจ่ายกระแสไฟฟ้า

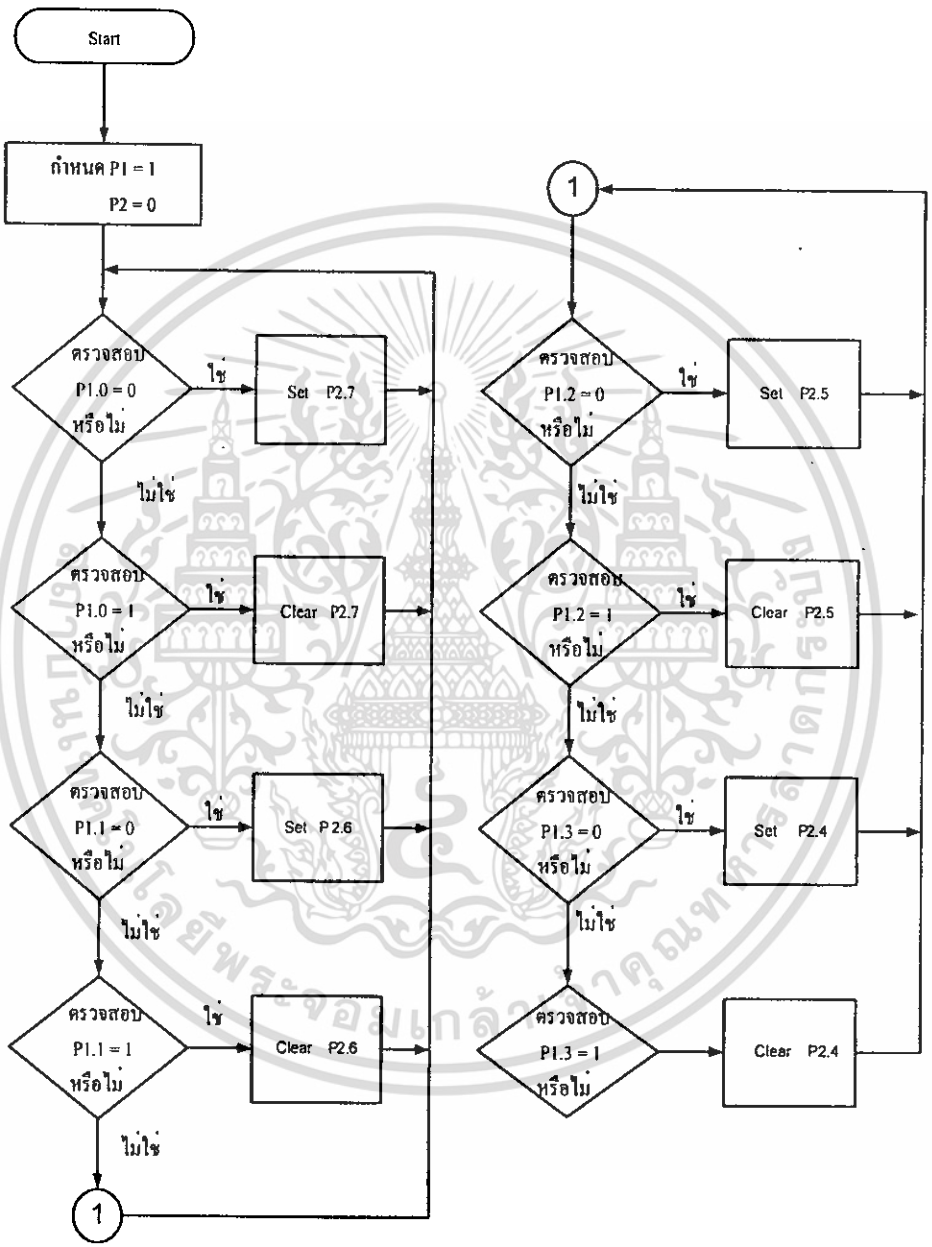


รูปที่ 3.11 แสดงวงจรควบคุมการจ่ายกระแสไฟฟ้า

การทำงาน

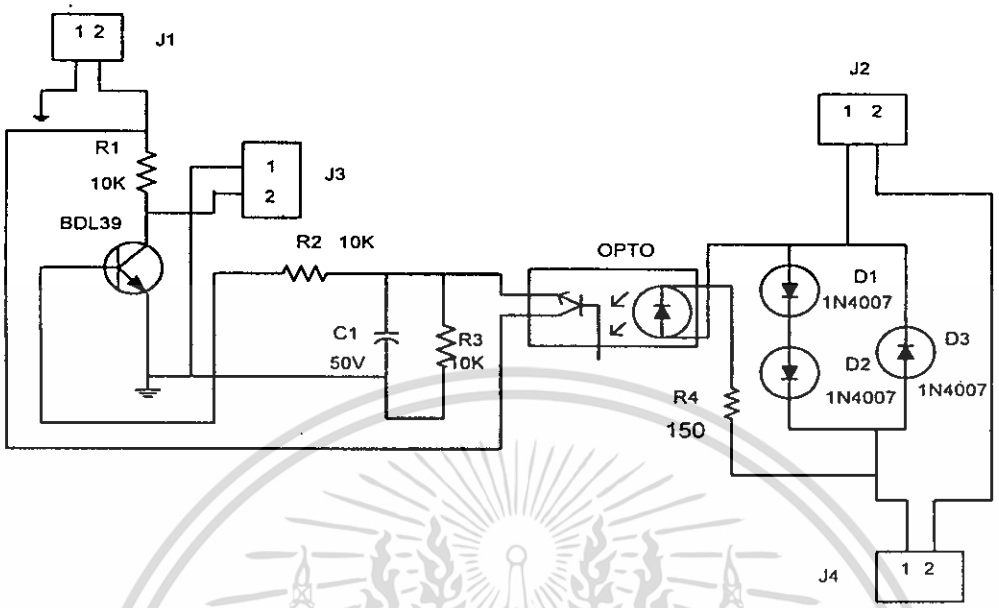
1. ที่พอร์ต 1 ของ MCS-51 คือ P1.0 - P1.3 จะคอยรับคำสั่งที่มาจากชุดควบคุมเอ็มเบสเด็ส
2. เมื่อทำการตรวจสอบแล้วว่ามีสัญญาณที่พอร์ต 1 ก็จะทำคำสั่งและส่งสัญญาณออกที่พอร์ต 0 คือ P0.0 - P0.3 (โดย P1.0 จะควบคุม P0.0 ,P1.1 จะควบคุม P0.1 ,P1.2 จะควบคุม P0.2 ,P1.3จะควบคุม P0.3)
3. สัญญาณที่ออกมาจากพอร์ต 0 ก็จะเข้าสู่วงจรเปรียบเทียบแรงดันโดยใช้ ออปแอม เบอร์ 741 เป็นตัวเปรียบเทียบโดยที่ขา 2 จะทำการต่อแรงดันอ้างอิง 3.3 โวลต์ เพื่อให้มั่นใจว่าวงจรควบคุมรีเลย์จะไม่ทำงานก่อนที่จะมีสัญญาณออกมาจาก MCS-51
4. เมื่อผ่านวงจรเปรียบเทียบและจะถูกส่งผ่านไปยังไดโอดก่อนที่จะถูกส่ง ไปที่ขาเบสของทรานซิสเตอร์เพื่อให้ทรานซิสเตอร์จะได้รับไฟบวกในการไบอัส หลังจากได้รับการไบอัสที่ขาเบสแล้วก็จะทำให้ทรานซิสเตอร์ทำงานส่งผลให้รีเลย์ทำงานเพื่อทำการควบคุมการจ่ายกระแสไฟฟ้า

5. หากมีความผิดพลาดเกิดขึ้น ตัวตรวจสอบความผิดพลาดก็จะส่งสัญญาณเข้ามาทาง P0.4- P0.7 จากนั้นก็จะส่งสัญญาณออกทาง P1.4 - P1.7 เพื่อส่งให้ชุดควบคุมเอ็มเบสเด็สรายงานความผิดพลาดที่หน้าจอเครื่องคอมพิวเตอร์ศูนย์กลางต่อไป



รูปที่3.12 โฟลว์ชาร์ตแสดงวงจรควบคุมการจ่ายกระแสไฟฟ้า

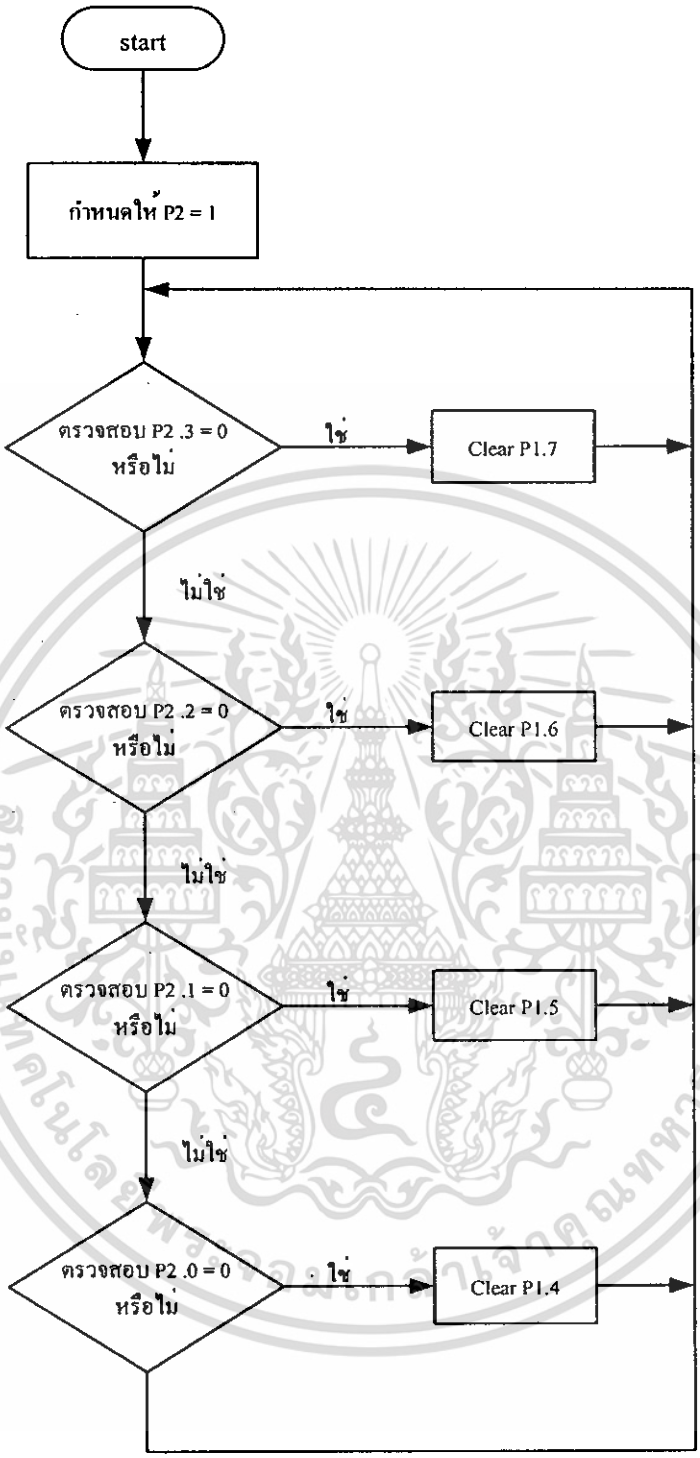
3.1.9. วงจรตรวจสอบความผิดพลาดของอุปกรณ์ไฟฟ้า



รูปที่ 3.13 แสดงวงจรตรวจสอบความผิดพลาดอุปกรณ์ไฟฟ้า

การทำงาน

ในขณะที่มีอุปกรณ์ไฟฟ้าต่ออยู่จะมีกระแสไหลผ่านออปโต้ ทำให้ออปโต้ทำงานจึงทำให้มีสัญญาณแรงดันทางด้านขาเบสของทรานซิสเตอร์ส่งผลให้ค่าที่จุด Detect Appliance มีค่าเป็น 0 (GND) แต่ในขณะที่ไม่มีอุปกรณ์ไฟฟ้าต่ออยู่จะไม่มีกระแสผ่านออปโต้ดังนั้นค่าที่จุดมีค่าเป็น Detect Appliance 1 (5 V) ดังแสดงในรูปที่ 3.13



รูปที่ 3. 14 โฟลว์ชาร์ตแสดงการทำงานของวงจรตรวจสอบอุปกรณ์ไฟฟ้า

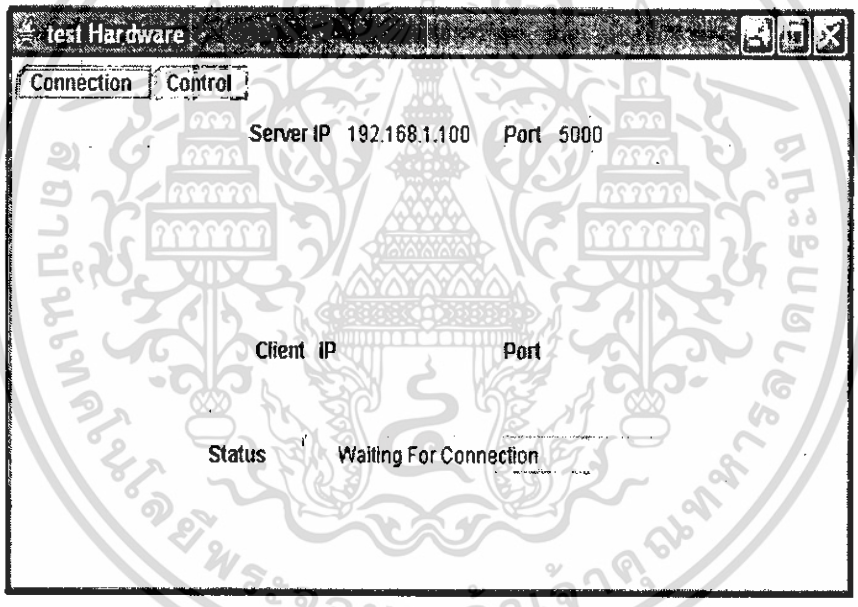
บทที่ 4

การทดลองและผลการทดลอง

เมื่อเราทราบทฤษฎีหรือหลักการและการคำนวณการสร้างวงจรแล้ว เราสามารถนำความรู้ข้างต้นมาทำการทดลอง การเชื่อมต่อระบบและทำการรับ-ส่ง ข้อมูลระหว่างเครื่องคอมพิวเตอร์ศูนย์กลางกับฮาร์ดแวร์ได้

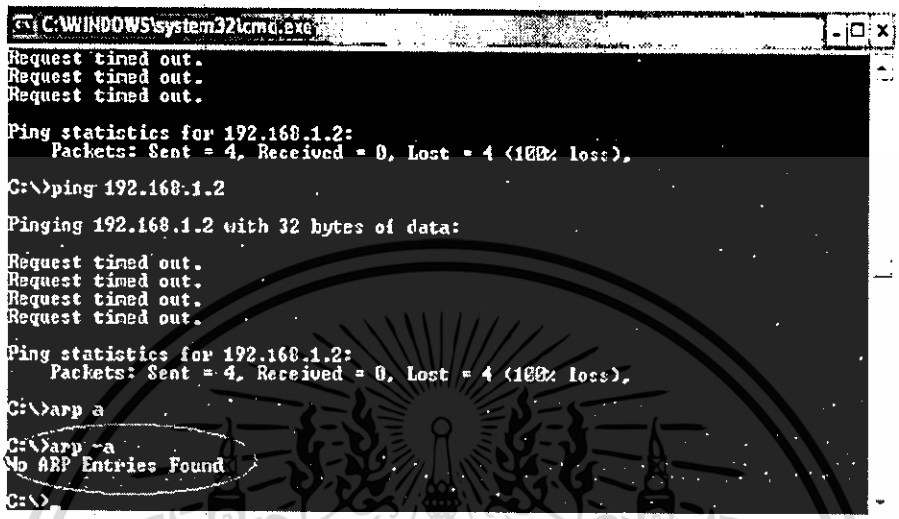
4.1. การทำงานโปรแกรมที่พร้อมใช้งานบนหน้าจอเครื่องคอมพิวเตอร์ศูนย์กลาง

โปรแกรมที่ใช้บนเครื่องคอมพิวเตอร์ศูนย์กลางนั้นจะใช้ภาษา Java ดังรูป 4.1 เมื่อเปิดโปรแกรม จะแสดงหมายเลข IP ของเครื่องคอมพิวเตอร์ศูนย์กลาง และหมายเลขพอร์ตที่กำหนดไว้เพื่อที่จะติดต่อกับฮาร์ดแวร์ และแสดงข้อความรอการเชื่อมต่อ



รูปที่ 4.1 แสดงโปรแกรมที่ใช้งานบนเครื่องคอมพิวเตอร์ศูนย์กลางที่ยังไม่ได้ทำการเชื่อมต่อกับฮาร์ดแวร์

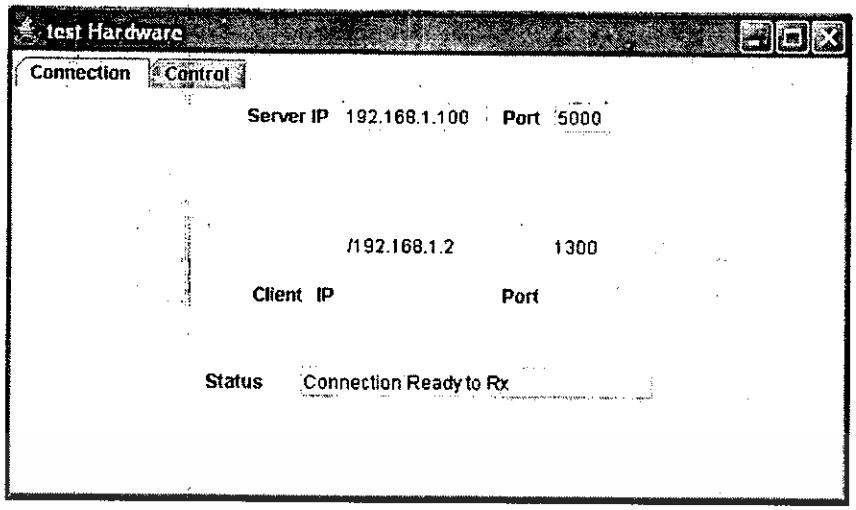
และถ้าทำการเข้าไปที่โปรแกรม MS- DOS แล้วใช้คำสั่ง arp–a ก็จะได้ผลดังในรูปที่ 4.2 ซึ่งในตอนนี้เครื่องคอมพิวเตอร์ศูนย์กลางจะยังไม่สามารถทำการส่งข้อมูลใดๆไปยังฮาร์ดแวร์ได้



รูปที่ 4.2 แสดงผลการรันที่โปรแกรม MS-DOS ขณะที่ยังไม่มีการเชื่อมต่อ

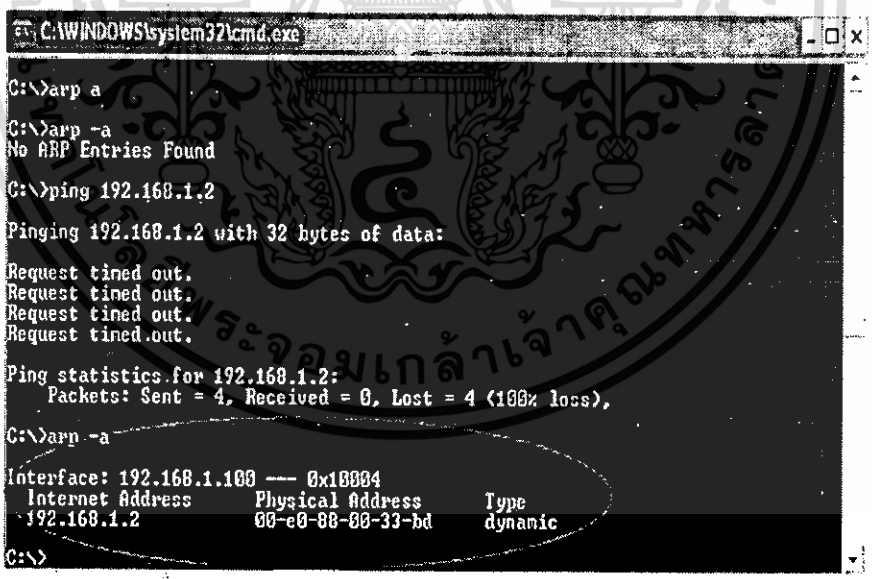
4.2. การเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ศูนย์กลางกับฮาร์ดแวร์

เมื่อฮาร์ดแวร์เปิดเครื่องแล้วจะทำการส่งสัญญาณ ping ให้กับเครื่องคอมพิวเตอร์ศูนย์กลาง ถ้าเครื่องคอมพิวเตอร์ศูนย์กลางยังไม่รู้ค่า MAC Address ของฮาร์ดแวร์จะทำการส่ง ARP Request ไปก่อนแล้วรอรับ ARP Reply จากฮาร์ดแวร์ จากนั้นจึงส่งสัญญาณ ping กลับไปยังฮาร์ดแวร์ เมื่อฮาร์ดแวร์ได้รับสัญญาณ ping แล้ว จะทำการส่งเฟรม UDP เพื่อยืนยันการเชื่อมต่อกับเครื่องคอมพิวเตอร์ศูนย์กลางเมื่อเครื่องคอมพิวเตอร์ศูนย์กลางได้รับเฟรม UDP ที่ยืนยันการเชื่อมต่อแล้วจะแสดงหมายเลข IP และพอร์ตที่มาเชื่อมต่อกัน ของฮาร์ดแวร์ ดังรูปที่ 4.3 ในตอนนี้เครื่องคอมพิวเตอร์ศูนย์กลางจะยอมให้ทำการส่งเฟรมข้อมูลไปยังฮาร์ดแวร์ได้แล้ว

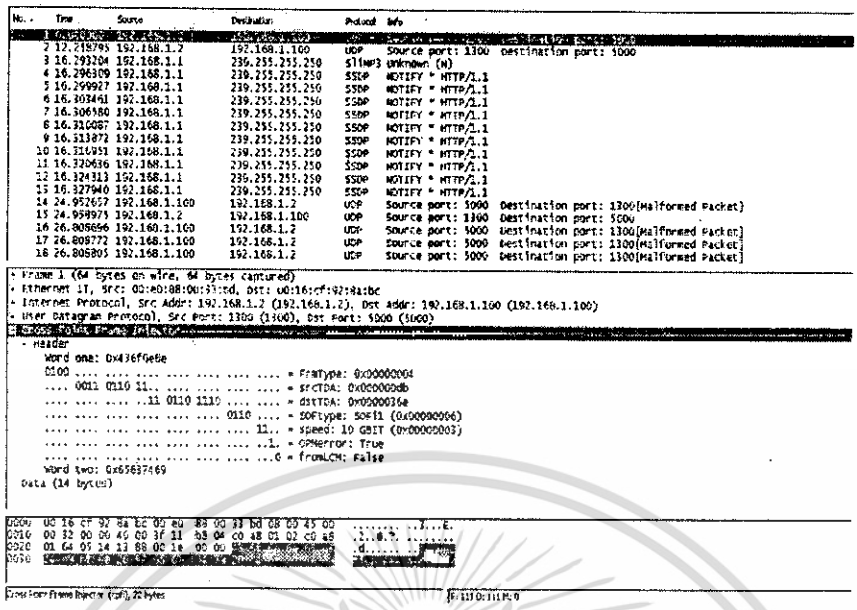


รูปที่ 4.3 แสดงโปรแกรมที่ใช้งานบนเครื่องคอมพิวเตอร์ศูนย์กลางที่ทำการเชื่อมต่อกับฮาร์ดแวร์

และถ้าทำการเข้าไปที่โปรแกรม MS- DOS แล้วใช้คำสั่ง arp–a ก็จะแสดงค่าMAC Address ของฮาร์ดแวร์ที่เชื่อมต่อได้ดังในรูปที่ 4.4 และดูผลของการตรวจจับเฟรมข้อมูลที่เชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ศูนย์กลางกับฮาร์ดแวร์จะได้ดังรูปที่ 4.5 ในตอนนี้เครื่องคอมพิวเตอร์ศูนย์กลางสามารถทำการส่งข้อมูลไปยังฮาร์ดแวร์ได้แล้ว



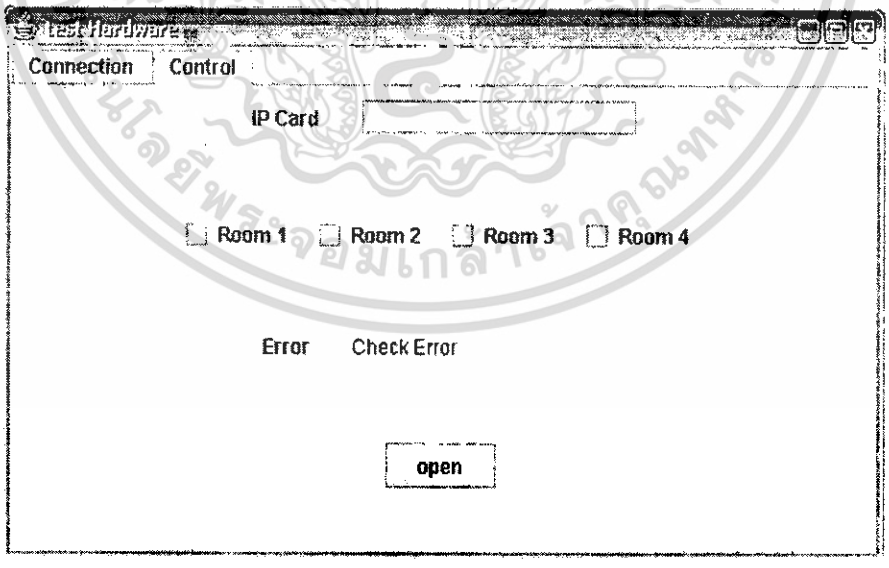
รูปที่ 4.4 แสดงผลการรันที่โปรแกรม MS-DOS ขณะที่มีการเชื่อมต่อ



รูปที่ 4.5 แสดงการตรวจจับเฟรมข้อมูลที่มีการเชื่อมต่อแล้ว

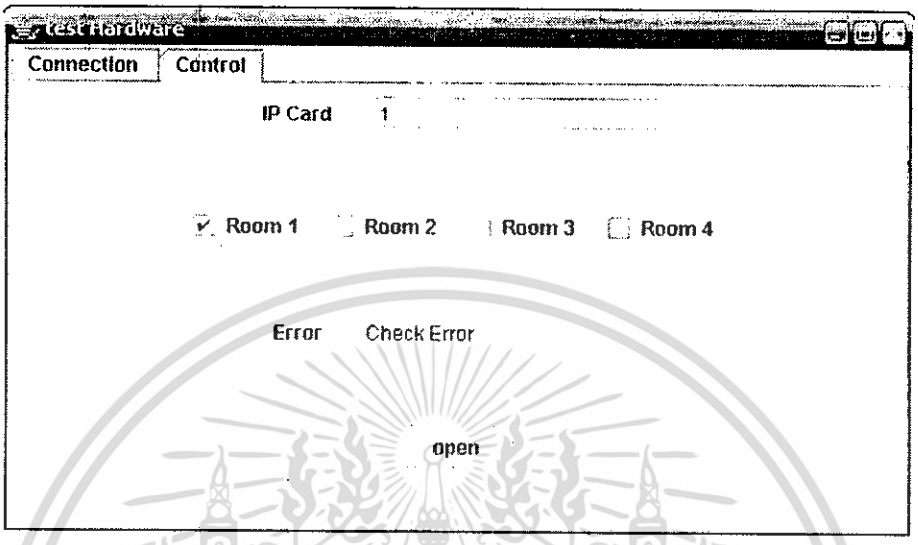
4.3. การทำงานโปรแกรมที่พร้อมทำการควบคุมการจ่ายกระแสไฟฟ้า

เมื่อเครื่องคอมพิวเตอร์ศูนย์กลางเชื่อมต่อกับฮาร์ดแวร์เรียบร้อยแล้วเครื่องคอมพิวเตอร์ศูนย์กลางก็จะเข้าสู่หน้าโปรแกรมควบคุมการจ่ายกระแสไฟฟ้า ดังที่แสดงในรูปที่ 4.6



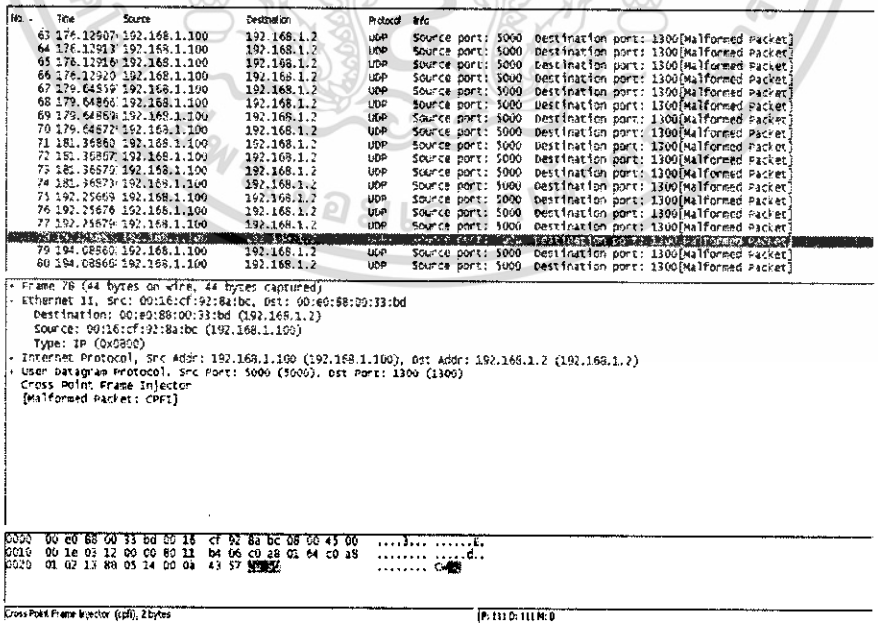
รูปที่ 4.6 แสดงโปรแกรมที่พร้อมจะทำการสั่งให้จ่ายกระแสไฟฟ้าไปยังห้องพัก

เมื่อจะสั่งให้จ่ายกระแสไฟฟ้าจะต้องใส่หมายเลขของการ์ดที่จะส่งข้อมูลในที่นี่ใช้การ์ดแผ่นที่ 1 แล้วจากนั้นคลิกที่ห้องพักที่ต้องการจะจ่ายกระแสไฟฟ้า ในรูปที่ 4.7 เมื่อคลิกที่ "Room 1" ก็จะทำการส่งเฟรมข้อมูลให้จ่ายกระแสไฟฟ้าไปยังห้องพักที่ 1



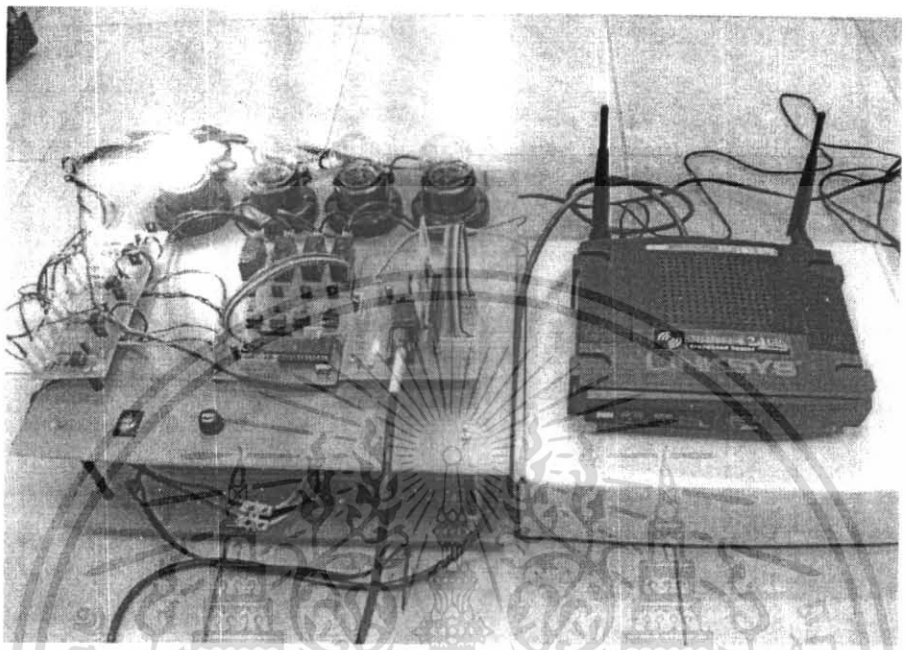
รูปที่ 4. 7 แสดงการสั่งงานให้จ่ายกระแสไฟฟ้าไปยังห้องพักที่ 1

เมื่อเฟรมข้อมูลถูกส่งจากเครื่องคอมพิวเตอร์ศูนย์กลางแล้วสามารถทำการตรวจจับเฟรมข้อมูลที่ส่งมาได้ดังที่แสดงในรูปที่ 4.8



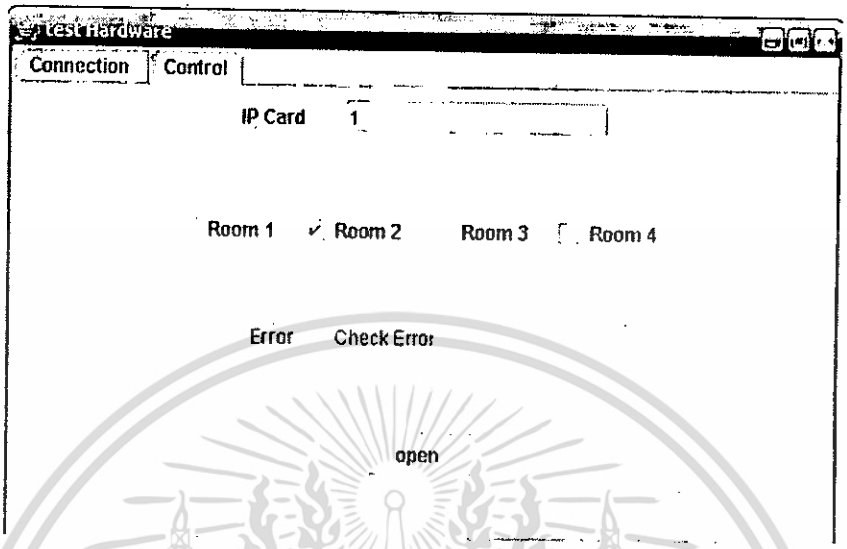
รูปที่ 4.8 แสดงการตรวจจับเฟรมข้อมูลที่ส่งมาให้ฮาร์ดแวร์จ่ายกระแสไฟฟ้าไปยังห้องพักที่ 1

เมื่อฮาร์ดแวร์ได้รับเฟรมข้อมูลที่สั่งให้จ่ายกระแสไฟฟ้าแล้วก็จะส่งข้อมูลไปควบคุมอุปกรณ์ให้อุปกรณ์ทำงาน ดังที่แสดงในรูปที่ 4.9 ที่เป็นผลที่แสดงออกหลอดไฟหลอดที่หนึ่งแทนการจ่ายกระแสไฟฟ้าไปยังห้องพักที่ 1



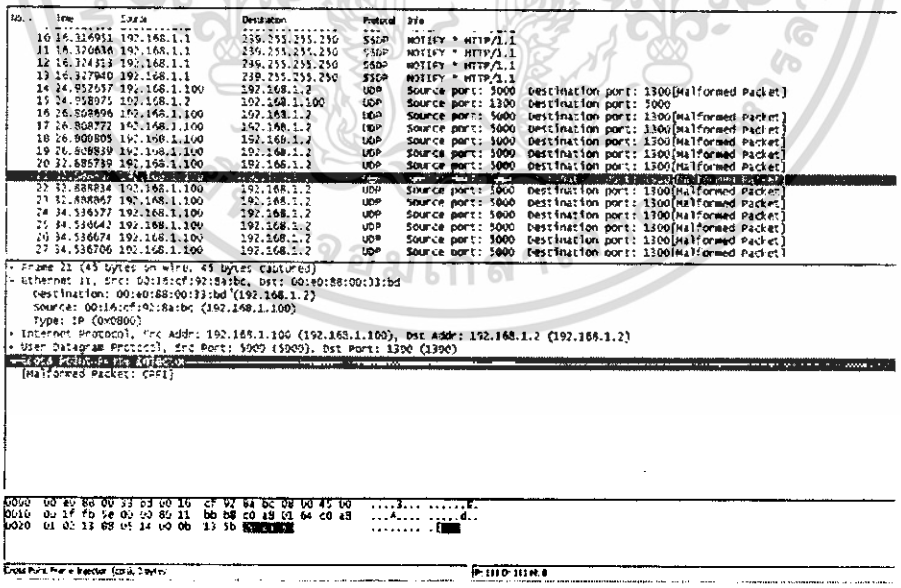
รูปที่ 4.9 ผลการควบคุมการจ่ายกระแสไฟฟ้าไปยังห้องพักที่ 1

เมื่อต้องการควบคุมการจ่ายกระแสไฟฟ้าที่ห้องพักที่ 2 ก็คลิกที่ “Room 2” จากนั้นเครื่องคอมพิวเตอร์ศูนย์กลางก็จะส่งเฟรมข้อมูลให้ทำการจ่ายกระแสไฟฟ้าไปยังห้องพักที่ 2 ดังแสดงในรูปที่ 4.10



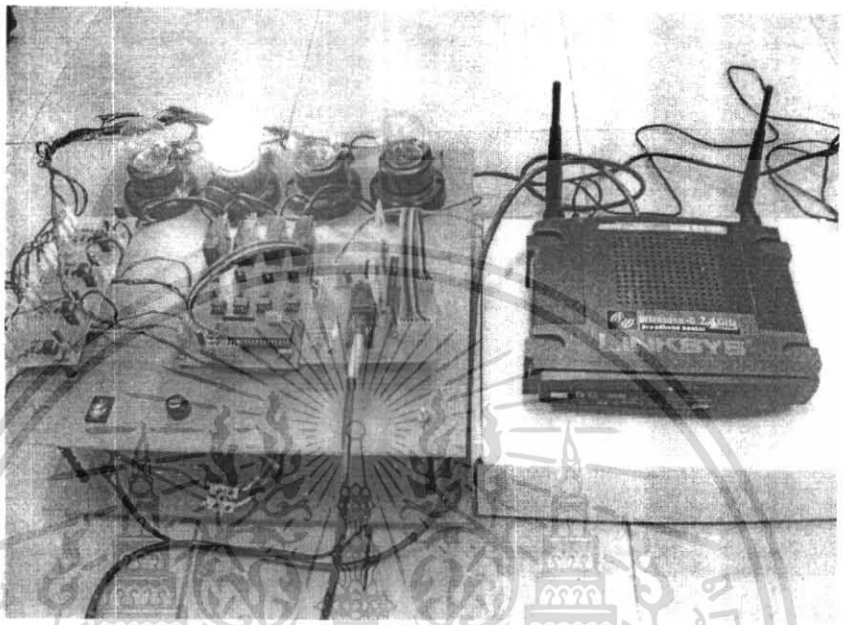
รูปที่ 4.10 แสดงการสั่งงานให้จ่ายกระแสไฟฟ้าไปยังห้องพักที่ 2

เมื่อเฟรมข้อมูลถูกส่งจากเครื่องคอมพิวเตอร์ศูนย์กลางแล้วสามารถทำการตรวจจับเฟรมข้อมูลที่ส่งมาได้ดังที่แสดงในรูปที่ 4.11



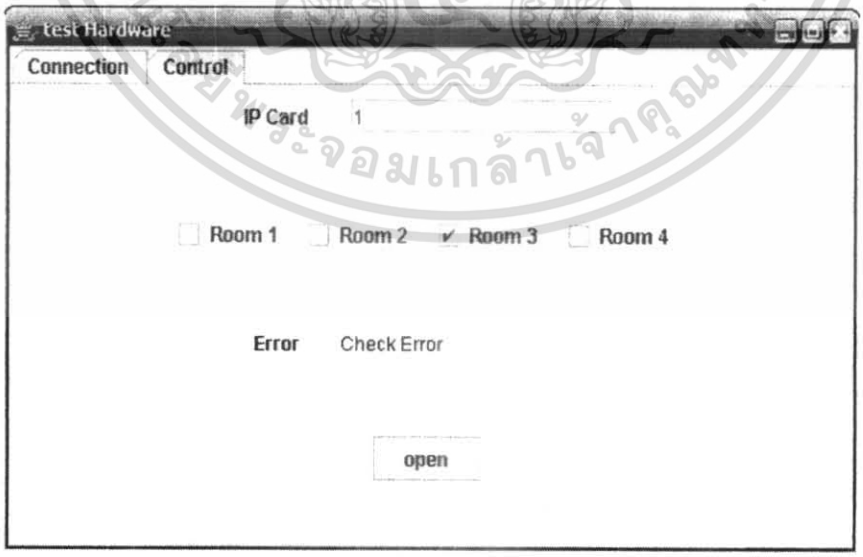
รูปที่ 4.11 แสดงการตรวจจับเฟรมข้อมูลที่ส่งมาให้ฮาร์ดแวร์จ่ายกระแสไฟฟ้าไปยังห้องพักที่ 2

เมื่อฮาร์ดแวร์ได้รับเฟรมข้อมูลที่สั่งให้จ่ายกระแสไฟฟ้าจากโปรแกรมที่สั่งงานแล้วก็จะส่งข้อมูลไปควบคุมอุปกรณ์ให้อุปกรณ์ทำงาน ดังที่แสดงในรูปที่ 4.12 ซึ่งเป็นผลที่แสดงออกหลอดไฟหลอดที่สองแทนการจ่ายกระแสไฟฟ้าไปยังห้องพักที่ 2



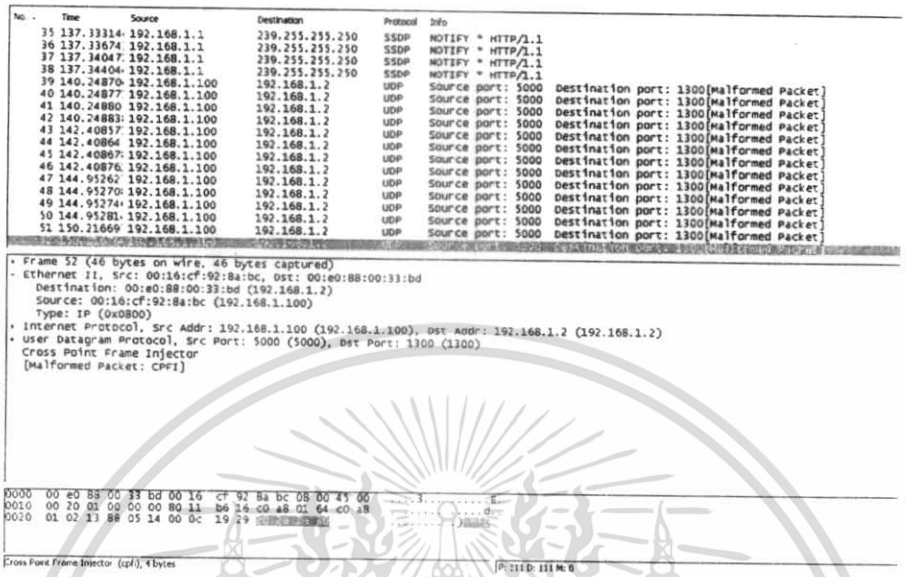
รูปที่ 4.12 ผลการควบคุมการจ่ายกระแสไฟฟ้าไปยังห้องพักที่ 2

เมื่อต้องการควบคุมการจ่ายกระแสไฟฟ้าที่ห้องพักที่ 3 ก็คลิกที่ "Room 3" จากนั้นเครื่องคอมพิวเตอร์ศูนย์กลางก็จะส่งเฟรมข้อมูลให้ทำการจ่ายกระแสไฟฟ้าไปยังห้องพักที่ 3 ดังแสดงในรูปที่ 4.13



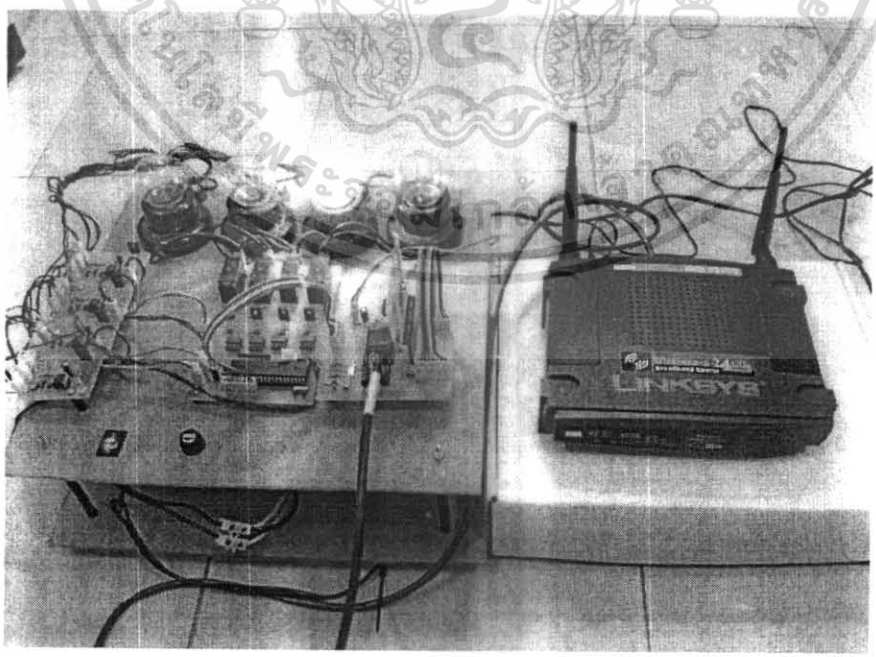
รูปที่ 4. 13 แสดงการสั่งงานให้จ่ายกระแสไฟฟ้าไปยังห้องพักที่ 3

เมื่อเฟรมข้อมูลถูกส่งจากเครื่องคอมพิวเตอร์ศูนย์กลางแล้วสามารถทำการตรวจจับเฟรมข้อมูลที่ส่งมาได้ดังที่แสดงในรูปที่ 4.14



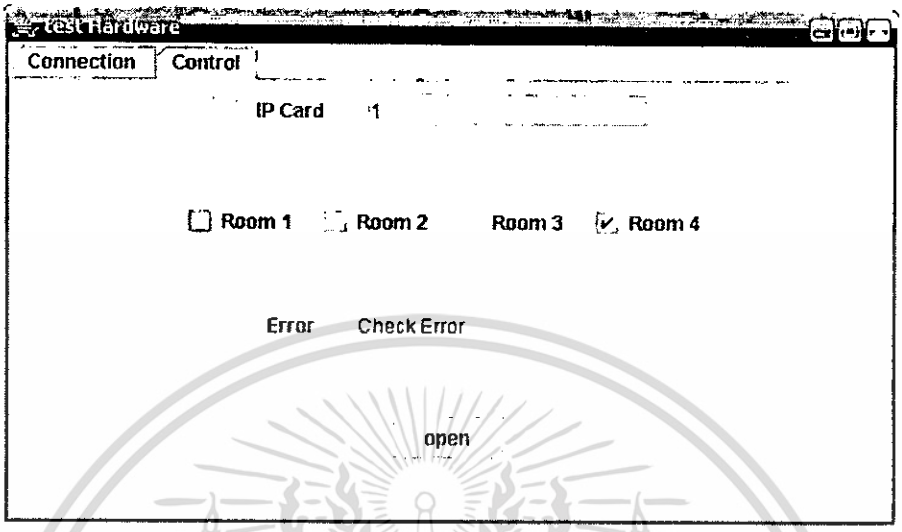
รูปที่ 4.14 แสดงการตรวจจับเฟรมข้อมูลที่ส่งมาให้ฮาร์ดแวร์จ่ายกระแสไฟฟ้าไปยังห้องพักที่ 3

เมื่อฮาร์ดแวร์ได้รับเฟรมข้อมูลที่สั่งให้จ่ายกระแสไฟฟ้าจากโปรแกรมที่สั่งงานแล้วก็จะส่งข้อมูลไปควบคุมอุปกรณ์ให้อุปกรณ์ทำงาน ดังที่แสดงในรูปที่ 4.15 ที่เป็นผลที่แสดงออกหลอดไฟหลอดที่สามแทนการจ่ายกระแสไฟฟ้าไปยังห้องพักที่ 3



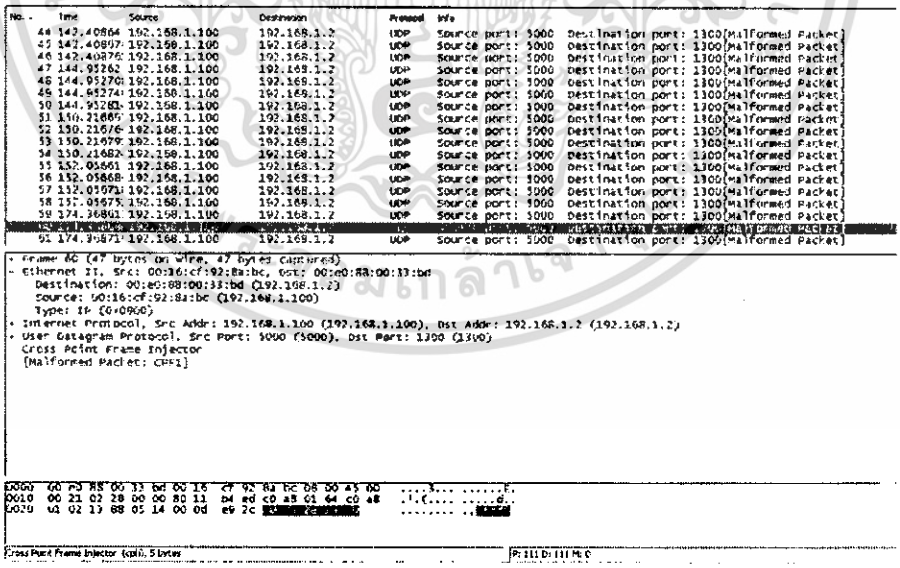
รูปที่ 4.15 ผลการควบคุมการจ่ายกระแสไฟฟ้าไปยังห้องพักที่ 3

เมื่อต้องการควบคุมการจ่ายกระแสไฟฟ้าที่ห้องพักที่ 4 ก็คลิกที่ “Room 4” จากนั้นเครื่องคอมพิวเตอร์ศูนย์กลางก็จะส่งเฟรมข้อมูลให้ทำการจ่ายกระแสไฟฟ้าไปยังห้องพักที่ 4 ดังแสดงในรูปที่ 4.16



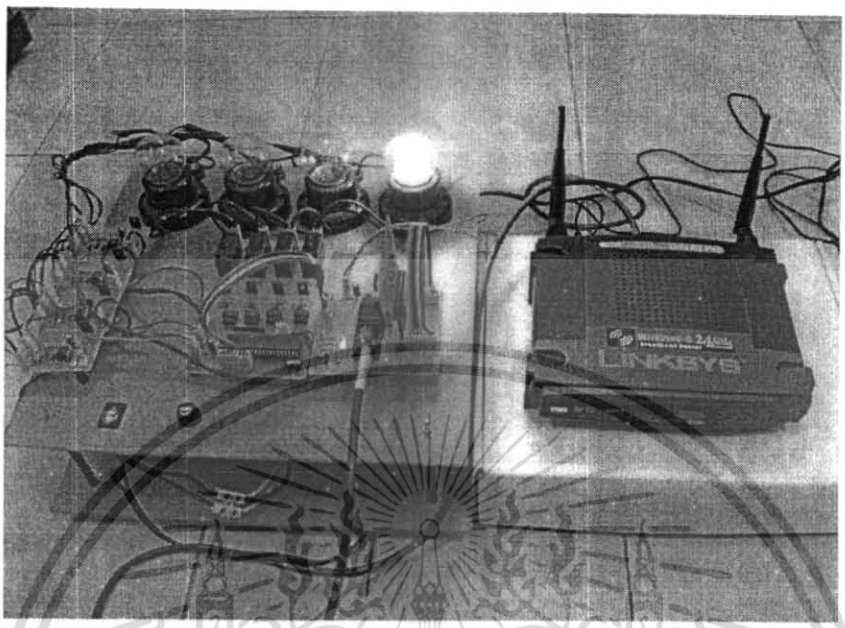
รูปที่ 4. 16 แสดงการสั่งงานให้จ่ายกระแสไฟฟ้าไปยังห้องพักที่ 4

เมื่อเฟรมข้อมูลถูกส่งจากเครื่องคอมพิวเตอร์ศูนย์กลางแล้วสามารถทำการตรวจจับเฟรมข้อมูลที่ส่งมาได้ดังที่แสดงในรูปที่ 4.17



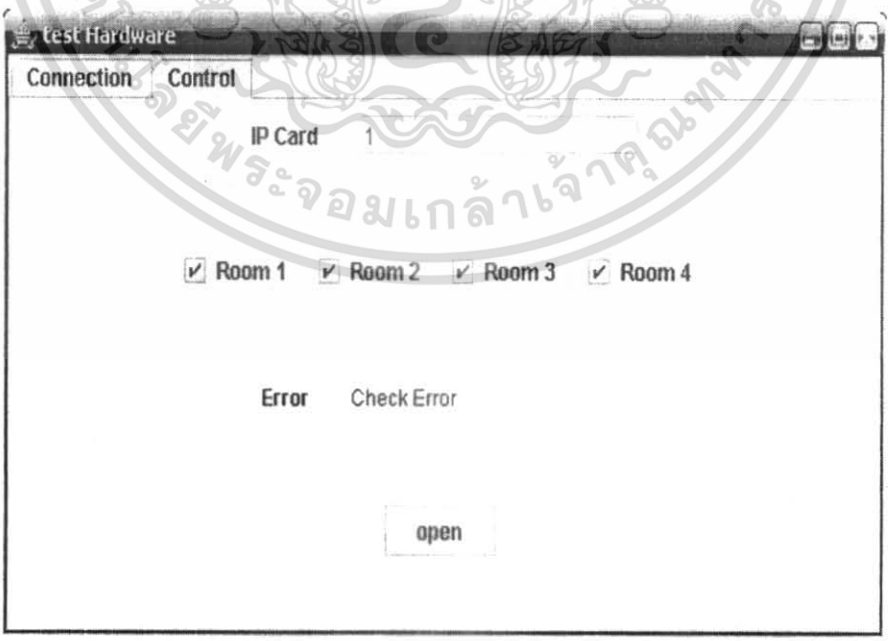
รูปที่ 4.17 แสดงการตรวจจับเฟรมข้อมูลที่ส่งมาให้ฮาร์ดแวร์จ่ายกระแสไฟฟ้าไปยังห้องพักที่ 4

เมื่อฮาร์ดแวร์ได้รับการสั่งงานจากเครื่องคอมพิวเตอร์ศูนย์กลางที่ทำการเลือกห้องหมายเลข 4 หลอดไฟหลอดที่ 4 ก็จะแสดงผลดังในรูปที่ 4.18



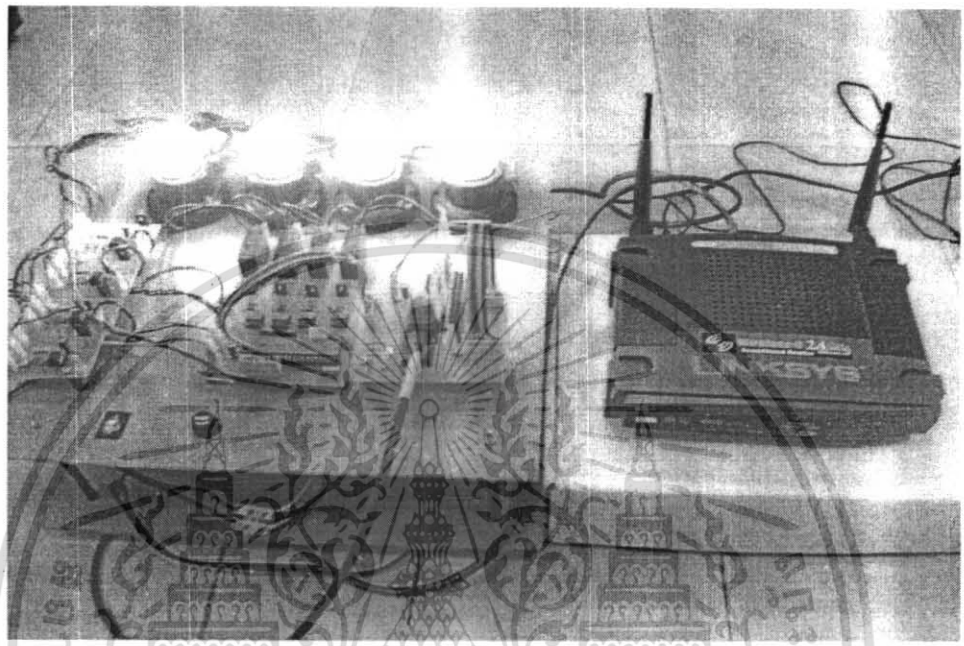
รูปที่ 4.18 ผลการควบคุมการจ่ายกระแสไฟฟ้าไปยังห้องพักที่ 4

โปรแกรมที่แสดงการสั่งงานโดยคลิกที่ห้องพักทั้งหมดที่ต้องการจะจ่ายกระแสไฟฟ้าให้ ดังที่แสดงไว้ในรูปที่ 4.19 เป็นการสั่งงานให้ทำการจ่ายกระไฟฟ้าให้กับห้องพักทั้ง 4 ห้อง



รูปที่ 4.19 แสดงการสั่งงานให้จ่ายกระแสไฟฟ้าไปยังห้องพักทั้ง 4

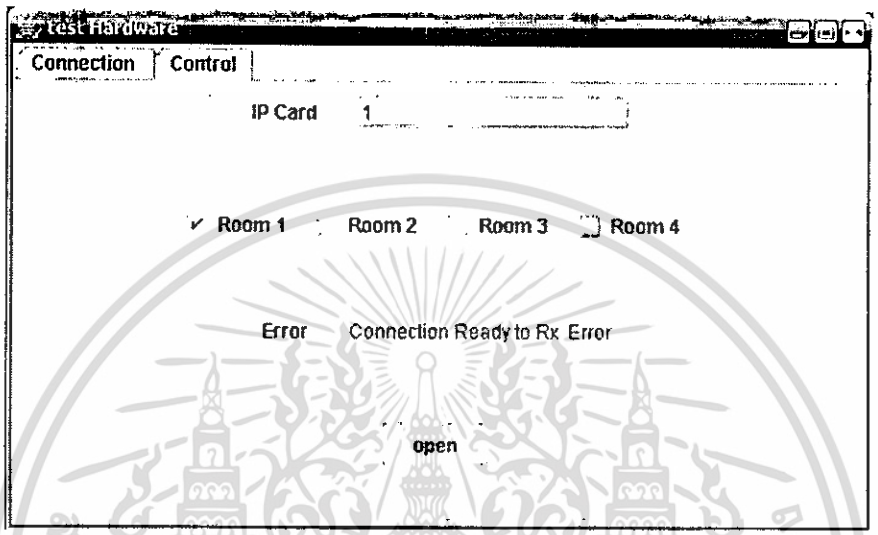
เมื่อฮาร์ดแวร์ได้รับการสั่งงานจากคอมพิวเตอร์ศูนย์กลางที่ทำการเลือกห้องพักทั้งสี่ห้องหลอดไฟทั้ง4 หลอดก็จะแสดงผลดังในรูปที่ 4.20 หลอดไฟทุกหลอดก็จะทำงานเสมือนว่าได้ทำการจ่ายกระแสไฟฟ้าให้กับอุปกรณ์ครบทุกชิ้น



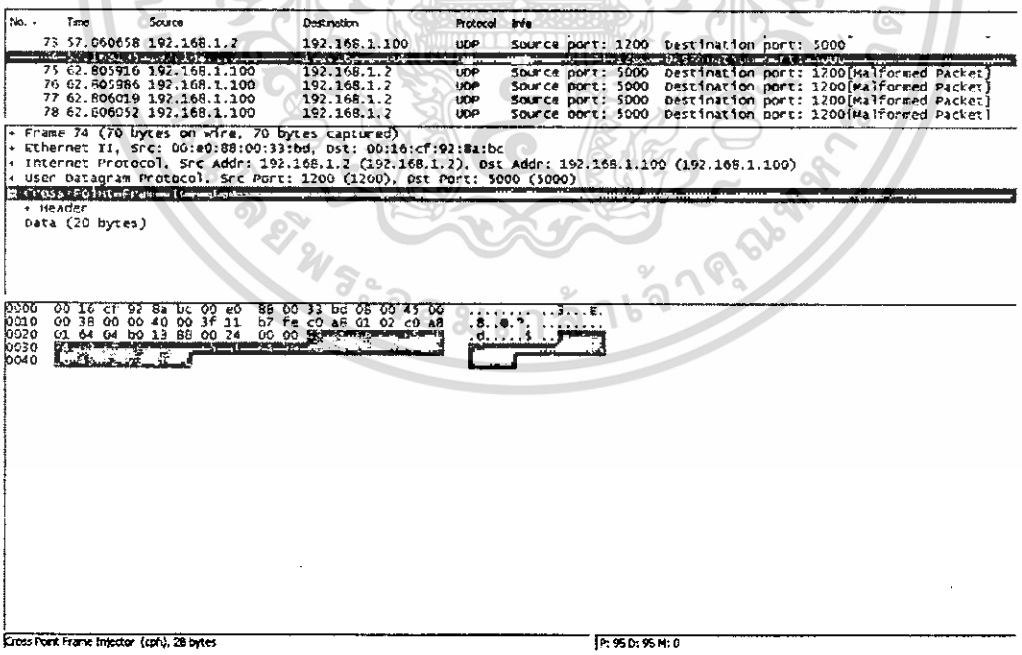
รูปที่ 4.20 ผลการควบคุมการจ่ายกระแสไฟฟ้าไปยังห้องพักทั้ง 4

4.4. การทำงานโปรแกรมที่ได้รับเฟรมข้อมูลแสดงความผิดพลาด

เมื่อเราทำการส่งเฟรมข้อมูลเพื่อควบคุมการจ่ายกระแสไฟฟ้าไปยังฮาร์ดแวร์แล้ว ดังในรูปที่ 4.7 , 4.10,4.13 และ 4.16 แล้วมีห้องพักห้องใดห้องหนึ่งไม่สามารถใช้ไฟฟ้าได้ ฮาร์ดแวร์ก็จะส่งเฟรมข้อมูลที่แสดงข้อความความผิดพลาดกลับมายังเครื่องคอมพิวเตอร์ศูนย์กลาง ดังแสดงในรูปที่ 4.21 และสามารถทำการจับเฟรมข้อมูลที่แสดงค่าความผิดพลาด



รูปที่ 4. 21 แสดงค่าผิดพลาดที่ส่งมาจากฮาร์ดแวร์



รูปที่ 4.22 แสดงการตรวจจับเฟรมข้อมูลที่ฮาร์ดแวร์แจ้งมายังเครื่องคอมพิวเตอร์ศูนย์กลาง

บทที่ 5
บทสรุปและวิจารณ์

ปริญญานิพนธ์ฉบับนี้เป็นการสร้างฮาร์ดแวร์เชื่อมต่อกับเครื่องคอมพิวเตอร์ศูนย์กลางเพื่อใช้ควบคุมการจ่ายกระแสไฟฟ้าให้กับห้องพักด้วยโครงข่ายอีเทอร์เน็ตโดยอาศัยโครงสร้างของโปรโตคอล TCP/IP เป็นโครงข่ายหลักในการรับส่งข้อมูล

สรุปผลการทดลอง

จากการทดลองทำการทดลองส่งเฟรมข้อมูลจากเครื่องคอมพิวเตอร์ศูนย์กลางไปยังฮาร์ดแวร์เป็นจำนวนหลายครั้งจะเห็นว่าสามารถทำการส่งข้อมูลได้อย่างถูกต้องและถ้าทำการทดลองสมมุติให้มีข้อมูลการจ่ายกระแสไฟฟ้าจากเครื่องคอมพิวเตอร์ศูนย์กลางมายังห้องพัก แล้วเกิดห้องพักไม่สามารถใช้ไฟฟ้าได้ ก็ให้ทำการแสดงข้อความความผิดพลาดที่เครื่องคอมพิวเตอร์ศูนย์กลาง และเครื่องคอมพิวเตอร์ศูนย์ก็สามารถแสดงค่าได้อย่างถูกต้อง แต่ปัญหาที่เจอในการทดลองพบว่าในการเริ่มต้นของระบบเมื่อทำการเปิดสวิตช์ในครั้งแรก จะเกิดการกระชากของกระแสไฟฟ้าทำให้ระบบมีปัญหาบ้าง แต่ก็ได้ทำการแก้ปัญหาโดยการนำตัวเก็บประจุมาต่อคร่อมตัวสวิตช์ไว้เพื่อลดปัญหาดังกล่าว

แนวทางการพัฒนาโครงงาน

ในการทำโครงงานชิ้นนี้มีการแบ่งส่วนในการทำงานหลัก ๆ ของฮาร์ดแวร์ออกเป็น 2 ส่วน คือ

- ส่วนที่เชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ศูนย์กลางกับฮาร์ดแวร์
- ส่วนควบคุมการจ่ายกระแสไฟฟ้า

ทำให้สามารถนำส่วนที่เชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ศูนย์กลางกับฮาร์ดแวร์ไปใช้ในการควบคุมอุปกรณ์อื่น ๆ ที่ต้องการได้ เช่นนำไปควบคุมอุปกรณ์ที่ต้องการให้ทำงานต่างเวลากันแต่ต้องติดตั้งไว้ในพื้นที่เดียวกัน หรือควบคุมอุปกรณ์ที่ไม่ต้องการให้คนเข้าไปใกล้กับบริเวณนั้นเป็นต้น

บรรณานุกรม

[1] วรรณิกา เนตรงาม **คู่มือการเขียนโปรแกรมภาษา JAVA ฉบับผู้เริ่มต้น** นนทบุรี : อินโนเพรส,2545

[2] ธีรบูลย์ หล่อวิเชียนรุ่ง , นคร ภักดีชาติ , ชัยวัฒน์ ลิ้มพรจิตรวิไล **ปฏิบัติการไมโครคอนโทรลเลอร์ MCS-51 ด้วยโปรแกรมภาษาซี** กรุงเทพ : บริษัท อินโนเวตีฟ เอ็กเพอร์เมนต์ จำกัด , 2537

[3] สัญฉกร วุฒิสิทธิกุลกิจ **โครงข่ายอินเตอร์เน็ตและ โพรโทคอลทีซีพี/ไอพี** กรุงเทพ : จุฬาลงกรณ์มหาวิทยาลัย ,2545

[4] จตุพล แพงจันทร์ , อนุโชต วุฒิพรพงษ์ **เจาะระบบ Network ฉบับสมบูรณ์** นนทบุรี : บริษัทไอดีซี อินโฟ ดิสทริบิวเตอร์ เซ็นเตอร์ จำกัด , 2547

[5] http://www.rabc.ac.th/ Wireless LAN