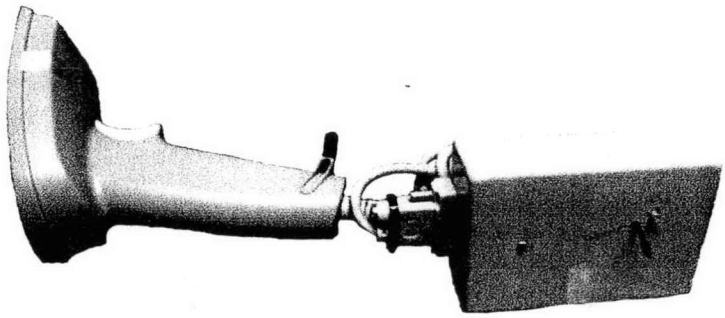
โครงการวิจัย

เครื่องอ่านบาร์โค้ดแบบไร้สายและผ่านระบบอินเตอร์เน็ต

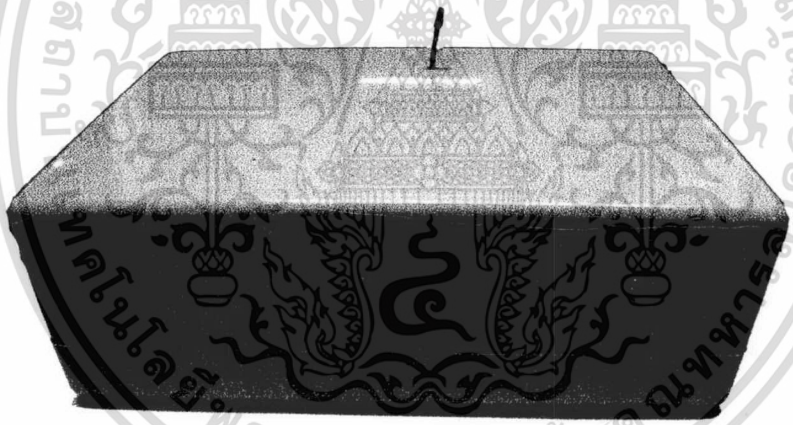
Wireless and Internet System Barcode Reader

ปราโมทย์ วาดเขียน
ศักดา สงดวง
ธนันท์ คณะเจริญ
ภัคภูมิ สมภพกุลเวช

ภาควิชาวิศวกรรมโทรคมนาคม
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง



ระบบส่งข้อมูล



ระบบรับข้อมูล

บทที่ 1
บทนำ

1.1 ความเป็นมา

เนื่องจากคลังสินค้าส่วนใหญ่จะประสบกับปัญหายุ่งยากในการบริหารและตรวจสอบสินค้าภายในคลังสินค้า ซึ่งปริมาณมาก ทำให้คลังสินค้าจำเป็นที่จะต้องมีระบบการบริหารจัดการที่ดี และมีประสิทธิภาพ ซึ่งในปัจจุบันก็ได้มีการนำเทคโนโลยีการระบุตัวตน(RFID) มาประยุกต์ใช้งานกับระบบคลังสินค้า เพื่อให้การบริหารและจัดการสามารถทำได้ง่ายขึ้น แต่ข้อเสียของการนำเทคโนโลยี RFID มาใช้คือ มีความจำเป็นที่จะต้องใช้เงินลงทุนค่อนข้างสูง ทั้งในส่วนของหัวอ่าน การวางระบบ และชิพ ที่ใช้ระบุตัวตนของสินค้า ทางคณะผู้วิจัย จึงได้ทำการนำเสนอ ระบบคลังสินค้าที่ใช้เทคโนโลยีของบาร์โค้ด มาใช้ในการบริหารและจัดการ ซึ่งหากทำการเปรียบเทียบระหว่างเทคโนโลยีของบาร์โค้ด กับเทคโนโลยี RFID จะเห็นได้ว่า เทคโนโลยีของบาร์โค้ดจะมีต้นทุนที่น้อยกว่า ทั้งในส่วนของหัวอ่าน และในส่วนของชิพ นอกจากนี้ทางคณะผู้วิจัย ยังได้มีแนวคิดที่จะทำการลดต้นทุน ในการวางระบบบริหารจัดการคลังสินค้า ด้วยการนำเทคโนโลยีไร้สายมาใช้งานร่วมกับเทคโนโลยีบาร์โค้ดอีกด้วย

1.2 วัตถุประสงค์ของโครงการวิจัย

๑. เพื่อนำความรู้ที่ได้ออกเผยแพร่ให้ผู้ที่สนใจทราบ
๒. เพื่อลดค่าใช้จ่ายในการติดตั้งระบบดังกล่าว
๓. เพื่อศึกษาการรับ-ส่งข้อมูลแบบไร้สาย
๔. เพื่อความสะดวกในการเช็คระบบคลังสินค้า

1.3 ขอบเขตของโครงการวิจัย

๑. สามารถออกแบบระบบบาร์โค้ดไร้สาย
๒. ออกแบบระบบบาร์โค้ดแบบไร้สายและแบบเข้าระบบอินเตอร์เน็ต
๓. ออกแบบการส่งสัญญาณแบบไร้สายที่ใช้ ระบบ อาร์เอฟไอดี(RFID)

บทที่ 2
ทฤษฎีและหลักการ

2.1 บาร์โค้ด

บาร์โค้ดคือสัญลักษณ์รหัสแท่งที่ใช้แทนข้อมูลตัวเลขมีลักษณะเป็นแถบมีความหนาบางแตกต่างกันขึ้นอยู่กับตัวเลขที่กำกับอยู่ข้างล่าง การอ่านข้อมูลจะอาศัยหลักการสะท้อนแสง เพื่ออ่านข้อมูลเข้าเก็บในคอมพิวเตอร์โดยตรงไม่ต้องผ่านการกดปุ่มที่แป้นพิมพ์ ระบบนี้เป็นมาตรฐานสากลที่นิยมใช้กันทั่วโลก ลักษณะที่เป็นลายเส้นสีขาว – ดำ จะมีขนาดความกว้างลายเส้นตามมาตรฐานแต่ละชนิดของบาร์โค้ดและมีข้อมูลตัวอักษรเป็นส่วนที่แสดงความหมายของข้อมูลลายเส้นสำหรับให้อ่านเข้าใจได้ และมีแถบว่าง (Quiet Zone) ใช้เป็นส่วนที่เครื่องอ่านบาร์โค้ดกำหนดขอบเขตของบาร์โค้ดและกำหนดค่าให้กับสีขาว (ความเข้มของการสะท้อนแสงในสีของพื้นผิวแต่ละชนิดที่ใช้แทนสีขาว) โดยแต่ละเส้นจะมีความยาวเท่ากันเรียงตามลำดับในแนวนอนจากซ้ายไปขวา ซึ่งจะเป็นประโยชน์ต่อเครื่องอ่านบาร์โค้ด (Barcode Scanner) ในการอ่านข้อมูลที่บันทึกไว้

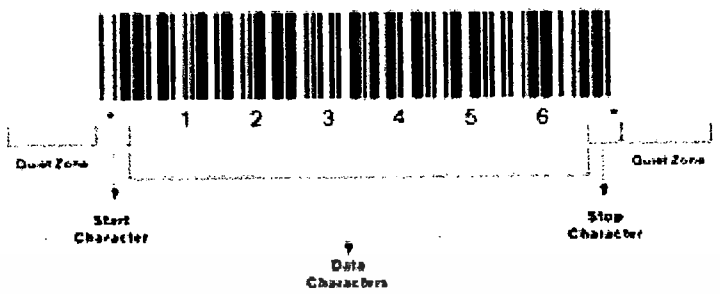
2.1.1 ส่วนประกอบของบาร์โค้ด

บาร์โค้ดจะมีส่วนประกอบต่างๆ ดังต่อไปนี้

- Quiet Zone เป็นบริเวณที่ว่างเปล่าไม่มีการพิมพ์ข้อความใดๆ โดยจะอยู่ก่อนและหลังบาร์โค้ด
- Start/Stop Character เป็นบริเวณแถบแท่งหรือช่องว่าง เพื่อเตรียมสั่งให้เซนเซอร์เริ่มต้นหรือหยุดบาร์โค้ด
- Data เป็นบริเวณแถบแท่งหรือช่องว่างที่แทนข้อมูลต่างๆ ที่เราต้องการ
- Check Digit เป็นบริเวณแถบแท่งที่ไว้สำหรับเก็บค่าตัวเลข เพื่อตรวจสอบในข้อมูลส่วน Data เพื่อให้มั่นใจว่าถูกต้องแม่นยำ

2.1.2 โครงสร้างของบาร์โค้ด

บาร์โค้ดประกอบด้วยแถบสีดำและสีขาว โดยความกว้างของแถบสีดำสลับขาวเป็นรหัสแทนข้อมูลเรียงจากซ้ายไปขวา การถอดรหัสจำเป็นต้องทาบความกว้างของแถบดำและแถบขาวนำไปเทียบกับมาตรฐานเครื่องอ่านบาร์โค้ด ประกอบด้วยหัวอ่านอินฟาเรด แบบปากกาและแบบวงจรถอดรหัส การใช้งานเริ่มต้นด้วยการกวาดหัวอ่านผ่านบาร์โค้ด ซึ่งหัวอ่านจะมีตัวตรวจจับแสงสะท้อนไปจุดชนวนวงจรอิเล็กทรอนิกส์ ทำให้เกิดคลื่นสัญญาณไฟฟ้าแบบพัลส์โดยความกว้างของรูปคลื่นจะเป็นสัดส่วนกับความกว้างของแถบโค้ด ต่อจากนั้นวงจรถอดรหัสจะตรวจสอบความกว้างของรูปคลื่นแล้วนำไปเปรียบเทียบกับแถบขาวดำทั้งหมดที่แทนข้อมูลตัวเลขหรือตัวอักษร โดยปกติเครื่องอ่านจะต่อเข้ากับคอมพิวเตอร์ ดังนั้นวงจรภายในเครื่องอ่านจะส่งข้อมูลตัวเลขที่ถอดรหัสได้ไปยังคอมพิวเตอร์เพื่อประมวลผลต่อไป ดังรูปที่ 1



รูปที่ 2.1 โครงสร้างของบาร์โค้ด

2.1.3 การอ่านบาร์โค้ด

ในการอ่านบาร์โค้ดใช้หลักการเปลี่ยนรหัสแถบใช้เป็นรหัสแอสกี้ โดยอาศัยความแตกต่างกันระหว่างแถบเข้มและพื้นที่ว่าง โดยพื้นที่ว่าง (ปกติจะเป็นสีขาวหรือสีอ่อน) จะมีการสะท้อนกลับของแสงได้มากกว่าบริเวณที่เป็นแถบเข้ม (ซึ่งใช้สีดำหรืออื่นที่มีความเข้มมากกว่า) ตัวอ่าน (Barcode reader) จะประกอบด้วย ตัวกำเนิดแสงผ่านเลเซอร์ออกมาโดยถูกบังคับทิศทางให้มีจุดรวมแสงที่เล็กที่สุด กับตัวรับที่มีความไวสูง ทั้ง 2 อย่างนี้จะบรรจุไว้ที่ตัวอ่านเดียวกันที่มีหลายรูปแบบ แต่แบบที่เป็นพื้นฐานที่สุดอยู่ในรูปคล้ายปากกาขนาดใหญ่ (Wand type) ตัวอ่านจะถูกแสกนผ่านบาร์โค้ด ในขณะที่ตัวกำเนิดแสงจะทำให้เกิดแสงส่งผ่านเลนส์ไปกระทบบนบาร์โค้ดและสะท้อนกลับจากแถบ (แถบและช่องว่าง) กลับไปยังตัวรับแสง (Photosensor) ที่เกิดค่าความแตกต่างขึ้นตามหลักการสะท้อนกลับในแต่ละแถบทำให้เกิดสภาวะลอจิก "0" และลอจิก "1" ขึ้นตามที่กล่าวมาแล้วข้างต้นซึ่งเมื่อรวมสภาวะลอจิก "0" และ "1" ทั้งหมดตลอดความกว้างของทุกแถบแล้วจะตรงกับแบบที่ได้กำหนดไว้แล้ว ในตัวอ่านบาร์โค้ดจะใช้ตัวกำเนิดแสงสีแดงหรือสีขาว แต่ส่วนใหญ่จะใช้แสงสีแดงเนื่องจากแสงสีขาวต้องการพลังงานและความเข้มของแสงสูงมากกว่าแสงสีแดง แสงสีแดงสามารถอ่านรหัสที่พิมพ์ด้วยสีต่างๆ ได้ยกเว้นรหัสที่พิมพ์ด้วยสีแดง องค์ประกอบที่สำคัญ 2 ประการที่จำเป็นอย่างมากในการอ่านบาร์โค้ดได้ถูกต้อง ประการแรกคือ พื้นที่ภายในแถบและช่องว่างจะต้องทำให้เกิดความแตกต่างของการสะท้อนกลับอย่างมาก (Contrast) เช่น แถบสีดำและช่องว่างสีขาว เป็นต้น ซึ่งปกกติความแตกต่างนี้ต้องอยู่ในช่วงระหว่างอัตรา 30-90 เปอร์เซ็นต์ขึ้นไป ประการที่สองคือ ความกว้างระหว่างแถบกว้างหรือช่องว่างกว้างต่อแถบแคบ หรือ ช่องว่างแคบจะเป็นอัตราส่วน 2:0.5 , 2:1 และ 3:1

2.1.4 เซนเซอร์อ่านบาร์โค้ด

เซนเซอร์อ่านบาร์โค้ดส่วนใหญ่แล้วแบ่งออกเป็น 2 ชนิดคือ

1. **แบบ Laser** จะใช้อ่านบาร์โค้ดที่ติดในสายการผลิต ซุปเปอร์มาเก็ต และคลังสินค้า หลักการทำงานคือ ลำแสงเลเซอร์ถูกปล่อยออกจากเลเซอร์ไดโอดมากระทบกับกระจกแบบหลายเหลี่ยมเพื่อที่จะแสกนบาร์โค้ด เมื่อลำแสงเลเซอร์กระทบบาร์โค้ดจะกระจายออก และถูกส่งมาที่โฟโต้ไดโอด ลักษณะของลำแสงที่กระจายตามบาร์โค้ดจะถูกแปลงให้เป็นสัญญาณอนาลอก จากนั้นทำการแปลงสัญญาณเป็นดิจิตอล ลักษณะ

ของสัญญาณดิจิตอลจะขึ้นอยู่กับขนาดของแท่ง และที่ว่างในแถบบาร์โค้ด จากนั้นก็จะแปลงรหัสเป็นข้อมูลผ่านพอร์ทคอมพิวเตอร์ เพื่อให้คอมพิวเตอร์ไปประมวลผลหรือเก็บข้อมูลไว้ใช้

2. แบบ CCD จะใช้อ่านบาร์โค้ดที่ติดชิ้นงานที่มีขนาดเล็ก เช่น หลอดทดลอง แผงวงจร ที่ชิ้นงานกับตัวอ่านใกล้กัน หลักการทำงานคือ หลอด LED จะเปล่งแสงมากระทบบาร์โค้ดแล้วสะท้อนมาที่เซนเซอร์ CCD Image เพื่อจับภาพของบาร์โค้ดขึ้นมาเป็นข้อมูลเก็บไว้ใช้งานต่อไป การแสกนของเซนเซอร์อ่านบาร์โค้ดจะมี 2 แบบคือ แบบ Singer Scan จะปล่อยลำแสงขวางในการแสกน 1 แถว ซึ่งเหมาะแก่การเคลื่อนที่ของบาร์โค้ดแบบ Picket Fence Direction และแบบ Raster Scan จะปล่อยลำแสงขวางในการแสกนหลายแถว แม้บาร์โค้ดที่พิมพ์จะคุณภาพไม่ดีก็สามารถอ่านค่าได้ถูกต้อง การแสกนแบบนี้เหมาะสำหรับการเคลื่อนที่ของบาร์โค้ดแบบ Ladder Direction

ตารางที่ 2.1 ตารางเปรียบเทียบเซนเซอร์อ่านบาร์โค้ดแบบ Laser และแบบ CCD

เปรียบเทียบ	แบบ Laser	แบบ CCD
ข้อดี	อ่านได้ในระยะไกล มุมในการอ่านกว้าง สามารถอ่านวัตถุเคลื่อนที่ได้	ขนาดเล็ก ราคาไม่แพง อายุการใช้งานยาวนานกว่า
ข้อเสีย	ราคาแพง	ไม่เหมาะกับชิ้นงานเคลื่อนที่

2.1.5 ประเภทของเครื่องอ่านบาร์โค้ด

เครื่องอ่านบาร์โค้ดสามารถแบ่งตามลักษณะการใช้งานได้ดังนี้

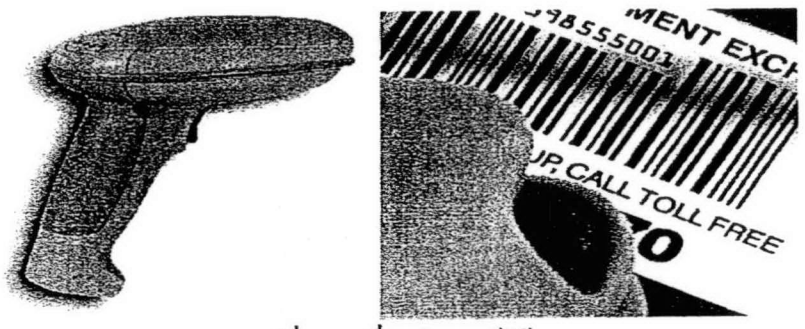
1. Moving Bean Scanner เครื่องอ่านอยู่กับที่ แต่แสงฉายกวาดไปที่สินค้า เพื่อหาบาร์โค้ดที่กำกับบนสินค้านั้น

2. Fixed Bean Scanner เครื่องอ่านอยู่กับที่ลำแสงไม่เคลื่อนที่สินค้าเคลื่อนที่ผ่านจุดที่แสงฉาย

3. Hand Held Scanner เครื่องอ่านที่ต้องใช้คนควบคุมและถือได้ เหมาะสำหรับการอ่านบาร์โค้ดของสินค้าที่มีขนาดใหญ่เคลื่อนที่ยาก เช่น ม้วนกระดาษใหญ่ที่ผลิตจากโรงงาน

4. Wand Scanner เครื่องอ่านที่ให้แสงสีแดงอินฟาเรดในการอ่านต้องใช้เครื่องอ่านสัมผัสกัลแถบบาร์โค้ด

5. Hand Held Laser Scanner เครื่องอ่านที่มีหลักการทำงานแบบ Moving Bean Scanner ที่ให้แสงเลซอร์



รูปที่ 2.2 เครื่องอ่านบาร์โค้ด

2.1.6 มาตรฐานบาร์โค้ด

บาร์โค้ดสามารถแบ่งออกตามชนิดของข้อมูลได้ดังนี้

- ตัวเลขเพียงอย่างเดียว (Numeric-only barcodes)
- ตัวอักษรและตัวเลข (Alphanumeric barcodes)
- 2 มิติ (2-Dimensional barcodes)

บาร์โค้ดมาตรฐานที่ใช้กันอยู่ปัจจุบันมีประมาณ 12 ระบบดังนี้

1. UPC – Uniform Product Code

บาร์โค้ดระบบแรกของโลกพัฒนาและทดลองใช้ครั้งแรกในปี ค.ศ. 1949 โดยชาวอเมริกันชื่อ Mr. Norm Woodland และ Mr. Barnard Silvers และสามารถใช้ได้อย่างสมบูรณ์เมื่อปี ค.ศ. 1973 โดย Uniform Code Council ตั้งอยู่ที่เมือง Daytor รัฐโอไฮโอ สหรัฐอเมริกา ระบบนี้นิยมใช้กันมากในประเทศแคนาดาและสหรัฐอเมริกา

รูปที่ 2.3 ตัวอย่างบาร์โค้ดระบบ UPC

จากรหัสของ UPC รหัสทางซ้ายมือจะใช้กับรหัสแถบแบบ UPC ในทางโซนซ้าย ส่วนรหัสทางขวาจะใช้ได้กับโซนทางขวาของรหัสแถบชนิด UPC เท่านั้น จะใช้สลับกันไม่ได้ ในส่วนของรหัสทางซ้ายจะขึ้นต้นด้วยบิต 0 และลงท้ายด้วยบิต 1 เสมอ จะมีการตรวจสอบเป็นแบบบิตคี่ (Odd parity) ส่วนรหัสทางขวาจะกลับด้านกับรหัสทางซ้าย คือ มีบิต 1 เป็นบิตเริ่มต้น และ 0 เป็นบิตสิ้นสุด การตรวจสอบบิตเป็นแบบคู่ (Even parity) นอกจากนี้ตารางเลขรหัสทางซ้ายและทางขวาเป็นเลขแบบ 1's complement ซึ่งกันและกัน

2. EAN – European Article Number

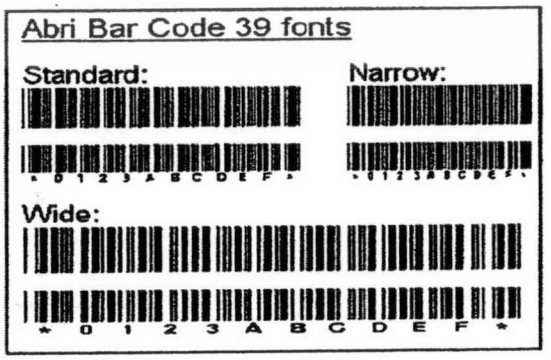
เป็นรหัสที่นิยมกับสินค้าที่มาจากต่างประเทศหลายประเภท หรือสินค้าที่ส่งออกไปขายต่างประเทศ ผู้อ่านหลายๆ คนคงได้เคยเห็นรหัสชนิดนี้ปรากฏบนสินค้าที่ซื้อ โครงสร้างของรหัสชนิดนี้ต่างจากรหัสแถบประเภทอื่นๆ โดยสิ้นเชิง

จากรูปที่ 4 จะเห็นได้ว่ารหัสแถบชนิดนี้แบ่งเป็น 2 ส่วน ซึ่งถูกแบ่งด้วยแถบสีดำเล็กๆ แต่ยาวกว่าแถบอื่น 2 แถบคั่นอยู่ตรงกลาง (เลขฐาน 2 ของแถบคั่นกลางนี้เป็น 01010) และยังมีแถบลักษณะเดียวกัน 2 ชุด อยู่ทางซ้าย—ขวาสุด (เลขฐาน 2 ของแถบนี้คือ 101) แถบทึบ 3 ชุดนี้เรียกว่า Guide bar ซึ่งปกติจะมีความยาวกว่าแถบอื่นๆ เป็นข้อสังเกตทำให้แบ่งรหัสแถบเป็น 2 ส่วน คือ โซนทางซ้ายและโซนทางขวา หลักสุดท้ายของทางซ้ายทางขวาสุด เป็นตัวกลางตรวจสอบความถูกต้อง (Check digit) ซึ่งคำนวณมาจากหลักที่เหลือ โดยตัวตรวจสอบทางซ้ายสุดมาจากเลข 5 หลักที่อยู่ทางด้านขวา ซึ่งแถบสำหรับตรวจสอบนี้บางครั้งก็พิมพ์ยาวเท่ากับส่วนที่เป็นข้อมูล

รูปที่ 2.4 ตัวอย่างบาร์โค้ดระบบ EAN

3. CODE 39

รหัส 3 ใน 9 เป็นรหัสที่ใช้แทนตัวอักขระทั้งหมด 44 อักขระเป็นอักษรตัวใหญ่ 26 รหัส เลข 0-9 10 รหัส และอักขระพิเศษอีก 3 รหัส เป็นการประยุกต์ ใช้รหัส 2 ใน 5 โดยการนำเอาส่วนที่เป็นแถบดำ 5 แถบและแถบว่าง 4 แถบ รวมเป็น 9 แถบแทน 1 รหัส ในแถบดำ 5 แถบนั้น ประกอบก้วยแถบกว้างที่เป็นบิต 1 อยู่ 2 แถบ และแถบแคบที่เป็นบิต 0 อีก 3 แถบ ดังนั้นเมื่อรวมทั้ง 9 แถบจะเป็นบิต 1 อยู่ 3 แถบ และบิต 0 อยู่ 6 แถบ รหัส 3 ใน 9 มีส่วนเริ่มต้น (Start code) และสิ้นสุด (Stop code) ด้วยรหัวเดียวกันคือ (Asterisk) ซึ่งมีรหัสฐาน 2 เป็นแถบ 00110 และช่องว่าง 1000 ข้อดีของรหัสชนิดนี้คือ ใช้งานได้กว้างขวางมากขึ้น เพราะสามารถใช้ตัวเลขปนกับตัวอักษรและเครื่องหมายต่างๆ ได้



รูปที่ 2.5 ตัวอย่างบาร์โค้ดระบบ CODE 39

4. ชนิดรหัส 2 ใน 5 (2 of 5 code)

เป็นรหัสที่มีใช้ตั้งแต่ ค.ศ. 1960 เป็นแบบที่ง่ายที่สุดในการใช้งาน การที่ชื่อเรียกว่า 2 ใน 5 เพราะใน 1 รหัส จะประกอบไปด้วยแถบ 5 แถบ (5 บิต) แต่จะมีแถบกว้างที่มีค่า (แถบกว้าง) เพียง 2 แถบ (2 บิต) เท่านั้น ส่วนบิตที่เหลือเป็น 0 ทั้งหมดคือ การแทนด้วยแถบแคบ (Narrow bar) 3 แถบโดยไม่นำส่วนที่เป็นช่องว่าง (Space bar) มาใช้เลย 2 ใน 5 นี้เป็นรหัสที่ใช้แทนข้อมูลได้เฉพาะตัวเลข 0-9 เพียงแค่ 10 รหัสเท่านั้น เริ่มต้นจาก Start code 3 บิต คือ 110 (แถบกว้าง 2 และแถบแคบ 1 กับปิดท้ายด้วย stop code 3 บิต คือ 101 ส่วนรหัสทั้ง 5 บิตที่แทนเลข 0-9 ดูได้ในตารางในรหัส Interleaved 2 of 5)

ตารางที่ 2.2 รหัสเลขฐาน 2 ของรหัส 2 ใน 5

ตัวเลข	เลขฐาน 2 ทั้ง 6 แบบ				
0	0	0	1	1	0
1	1	0	0	0	1
2	0	1	0	0	1
3	1	1	0	0	0
4	0	0	0	0	1
5	1	0	0	0	0
6	0	1	0	0	0
7	0	0	1	1	1
8	1	0	1	1	0
9	0	1	1	1	0

5. ITF – INTERLEAVE 2 of 5

รหัสแบบนี้พัฒนามาจากแบบ 2 ใน 5 เนื่องจากรหัส 2 ใน 5 ไม่ได้นำส่วนที่เป็นช่องว่างกว้างและช่องว่างแคบมาใช้ ใช้แต่เพียงแถบกว้างและแถบแคบจึงทำให้ความหนาแน่นของข้อมูลน้อยลงนั่นคือ เมื่อต้องการบรรจุข้อมูลต่อเนื่องหลายตัวเลข จะต้องใช้แถบกว้างมากขึ้น รหัส 2 ใน 5 แบบสอดแทรกได้ดัดแปลงนำส่วนที่เป็นช่องว่างทั้ง 2 ชนิด มาใช้งานด้วยโดยการสอดแทรกรหัสลงไปอีก 1 รหัสทุกๆ ช่อง 5 แถบของรหัสปกติที่เป็นแถบสีดำแต่ก็ยังแทนรหัสตัวเลข 0-9 ได้เพียง 10 รหัสเท่านั้น ดังรูปที่ 6

รูปที่ 2.6 ตัวอย่างบาร์โค้ดระบบ IFT 2 of 5

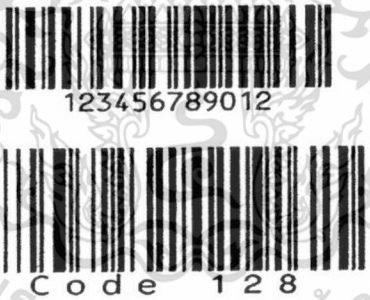
6. CODABAR

รหัส Codabar ประกอบด้วย 7 บิตโดย 4 บิตเป็นแถบดำและ 3 บิตเป็นช่องว่าง ใช้แทนตัวเลข 0-9 เครื่องหมาย - $: / . +A B C และ D รหัส Codabar ที่สมบูรณ์จะต้องมีรหัสที่ใช้แทนตัวอักษร A B C หรือ D (เช่น A = 00110010) เป็นส่วนเริ่มต้นและสิ้นสุด ภายในประกอบด้วยรหัสของ Codabar ที่เป็นตัวเลขและเครื่องหมายซึ่งทำให้มีความยาวที่ไม่แน่นอนเพราะ 12 รหัสแรกมีบิตที่เป็น 1 อยู่ 2 บิต 4 รหัส ต่อมามีบิต 1 อยู่ 3 บิต (Cocabar ใช้ทั้งแถบดำและขาวแทนข้อมูลใน 1 รหัส) และ 4 รหัสสุดท้ายเป็นรหัส A, B, C, D กำหนดขึ้นมาเพื่อใช้เป็นรหัสเริ่มต้นและสิ้นสุด (Start/Stop code) ดังตัวอย่างรูปที่ 7

รูปที่ 2.7 ตัวอย่างบาร์โค้ดระบบ Codabar

7. CODE 128

ได้ถูกพัฒนาขึ้นและยอมรับว่าได้ใช้เป็นทางการในสหรัฐอเมริกา เมื่อปี ค.ศ. 1981 นิยมใช้ในวงการดีไซน์เนอร์และแฟชั่น ปัจจุบันกำลังเริ่มนิยมใช้ในสหรัฐอเมริกา ดังตัวอย่างรูปที่ 8



รูปที่ 2.8 ตัวอย่างบาร์โค้ดระบบ CODE 128

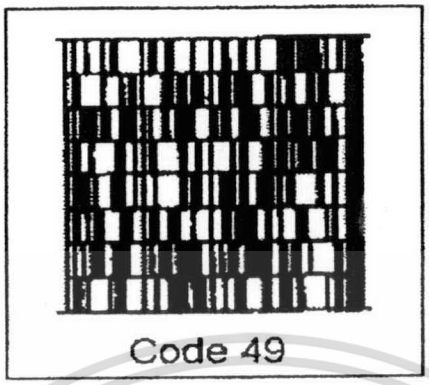
8. CODE 39

ได้เริ่มพัฒนาขึ้นในปี ค.ศ. 1982 ปัจจุบันเริ่มนิยมใช้ในสหรัฐอเมริกา ดังตัวอย่างรูปที่ 9

รูปที่ 2.9 ตัวอย่างบาร์โค้ดระบบ CODE 39

9. CODE 49

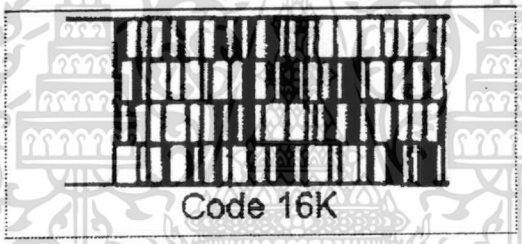
ได้เริ่มพัฒนาขึ้นในปี ค.ศ. 1987 โดย Dr. Davis Allais ผู้คิดค้น CODE 39 ได้ปรับปรุงพัฒนาให้บรรจุข้อมูลได้มากขึ้นด้วยพื้นที่เท่าเดิม ดังตัวอย่างรูปที่ 10



รูปที่ 2.10 ตัวอย่างบาร์โค้ดระบบ CODE 49

10. CODE 16K

เหมาะสำหรับอุตสาหกรรมผลิตสินค้าที่มีขนาดเล็กมาก พื้นที่ในการใส่บาร์โค้ดน้อย เช่น อุปกรณ์อะไหล่เครื่องไฟฟ้า ดังตัวอย่างรูปที่ 11



รูปที่ 2.11 ตัวอย่างบาร์โค้ดระบบ CODE 16K

11. ISBN/ISSN – International Standard Book Number / International Standard Serial Number

ใช้สำหรับหนังสือและนิตยสาร ดังตัวอย่างรูปที่ 12

รูปที่ 2.12 ตัวอย่างบาร์โค้ดระบบ ISBN/ISSN

12. EAN/UCC 128 (shipping container code)

เป็นระบบใหม่ ซึ่งเป็นการร่วมมือกันระหว่าง EAN ของยุโรป และ UCC ของสหรัฐอเมริกา โดยนำเอาระบบ EAN มาใช้ร่วมกับ CODE 128 เพื่อบอกรายละเอียดของสินค้ามากขึ้น เช่น วันเดือนปีที่ผลิต ครั้งที่ผลิต วันที่สั่งซื้อ มีกี่สี กี่ขนาด เป็นต้น ดังตัวอย่างรูปที่ 13

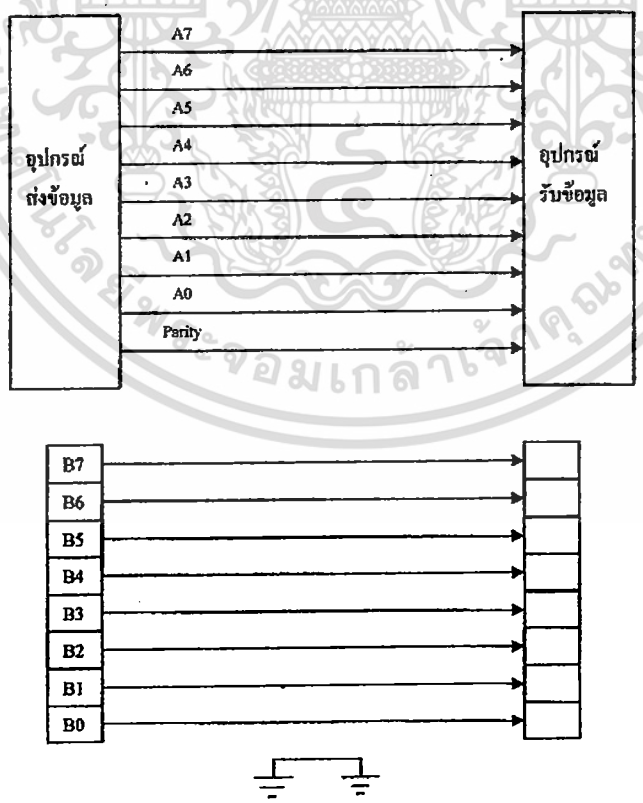
รูปที่ 2.13 ตัวอย่างบาร์โค้ดระบบ EAN/UCC 128

2.2 การสื่อสารผ่านพอร์อนุกรม RS-232

2.2.1 การสื่อสารข้อมูล

การสื่อสารข้อมูลแบบขนาน (Parallel Communication)

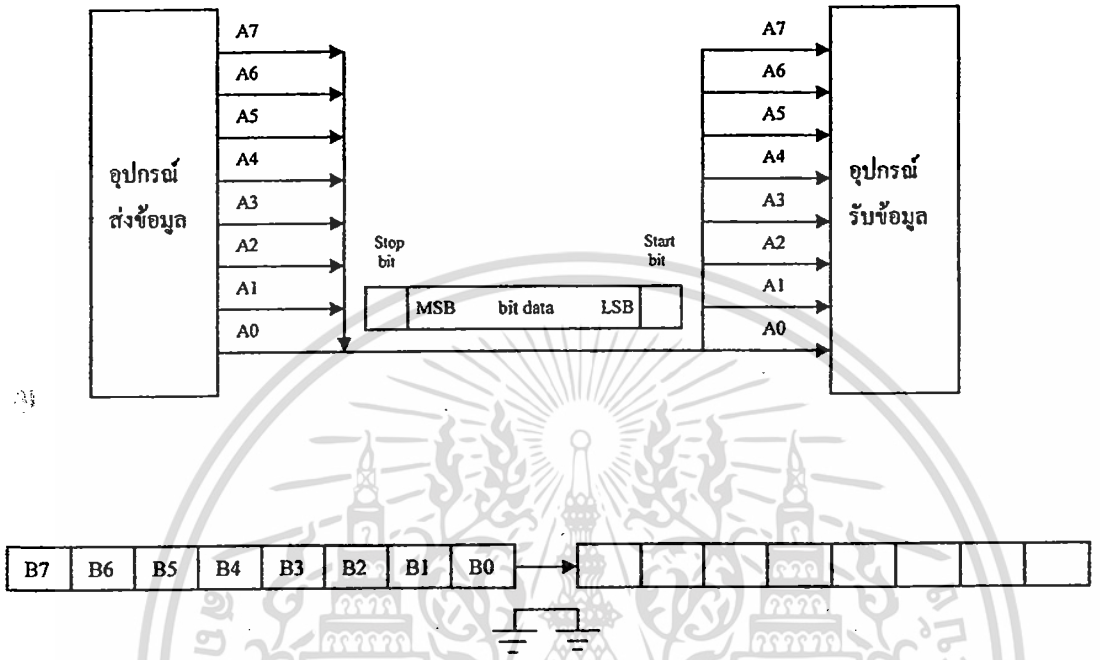
การสื่อสารข้อมูลแบบขนานคือ การสื่อสารแบบที่ส่งข้อมูลพร้อมๆ กัน n บิตผ่านสายสัญญาณ n เส้น สามารถแสดงรูปการสื่อสารข้อมูลแบบขนานได้ดังรูป 1



รูปที่ 2.14 แสดงบล็อกไดอะแกรมรูปแบบการสื่อสารแบบขนาน

การสื่อสารข้อมูลแบบอนุกรม (Serial Communication)

การสื่อสารข้อมูลแบบอนุกรมคือ การสื่อสารแบบที่ส่งข้อมูลทีละบิตผ่านสายสัญญาณเส้นเดียวกันจนครบจำนวนข้อมูลที่ต้องการ โดยเฟรมของการสื่อสาร้อมูลแบบอนุกรมประกอบด้วยสตาร์ทบิต (start bit), อสต็อปบิต (stop bit) และบิตข้อมูล (data bit) สามารถแสดงรูปแบบการสื่อสารข้อมูลแบบอนุกรมได้ดังรูปที่ 2

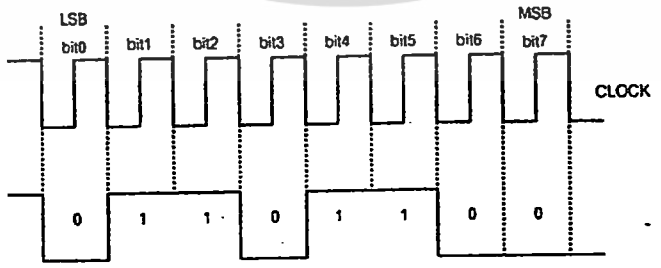


รูปที่ 2.15 แสดงบล็อกไดอะแกรมรูปแบบการสื่อสารแบบอนุกรม

การสื่อสารแบบอนุกรมนั้นจะแบ่งออกได้เป็น 2 แบบคือ การสื่อสารอนุกรมแบบซิงโครนัสและการสื่อสารอนุกรมแบบอะซิงโครนัส

1. การสื่อสารข้อมูลแบบซิงโครนัส

การสื่อสารข้อมูลแบบซิงโครนัสจะมีสัญญาณนาฬิการ่วมอยู่กับการรับและส่งสัญญาณด้วย ตัวอย่างการส่งข้อมูลแบบซิงโครนัสคือ คีย์บอร์ดของคอมพิวเตอร์ ซึ่งสายเส้นหนึ่งจะเป็นสายของสัญญาณนาฬิกา ส่วนสายอีกเส้นหนึ่งจะเป็นสายของข้อมูล ดังนั้นการติดต่อแบบซิงโครนัสนี้จะต้องใช้สายในการเชื่อมต่ออย่างน้อยที่สุด 3 เส้น คือ สัญญาณนาฬิกา, ข้อมูล และกราวด์ ดังรูปที่ 3



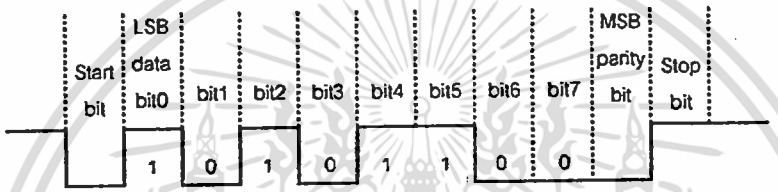
รูปที่ 2.16 รูปแบบอย่างง่ายที่สุดของข้อมูลอนุกรม

2. การสื่อสารข้อมูลแบบอะซิงโครนัส

การสื่อสารข้อมูลแบบอะซิงโครนัส คือ การรับส่งข้อมูลไปในสายสัญญาณ โดยไม่จำเป็นต้องส่งสัญญาณนาฬิการ่วมด้วยเหมือนกับการรับส่งข้อมูลแบบซิงโครนัส แต่จะใช้การกำหนดค่าสัญญาณนาฬิกาทั้งภาครับและภาคส่งให้มีค่าเท่ากัน ซึ่งเรียกสัญญาณนาฬิกาที่ใช้ในการกำหนดค่าให้ภาครับและภาคส่งนี้ว่า อัตราการถ่ายเทข้อมูล หรือ อัตราบอด (baud rate) ที่มีหน่วยเป็น บิตต่อวินาที (bit per second : bps)

รูปแบบของข้อมูลที่ใช้ในการรับส่งแบบอะซิงโครนัสประกอบด้วย 4 ส่วนด้วยกันคือ

1. บิตเริ่มต้น (Start Bit) ซึ่งจะมีขนาด 1 บิต
2. บิตข้อมูลอนุกรมจะมีขนาด 5, 6, 7 หรือ 8 บิต
3. บิตตรวจสอบพาริตี้ (Parity Bit) จะมีขนาด 1 บิตหรือไม่มี
4. บิตปิดท้าย (Stop Bit) จะมีขนาด 1, 1.5 หรือ 2 บิต



รูปที่ 2.17 รูปแบบอย่างง่ายที่สุดของข้อมูลอนุกรมแบบอะซิงโครนัส

รูปที่ 4 แสดงรูปแบบของข้อมูลอนุกรมแบบอะซิงโครนัส ซึ่งเมื่อไม่มีข้อมูลที่จะส่ง ขาคาต้าจะมีสถานะลอจิก "1" ซึ่งจะเรียกสถานะนี้ว่าสถานะว่าง (Idle stage) การเริ่มต้นส่งข้อมูลจะเริ่มจากการให้ขาคาต้ามีลอจิก "0" ด้วยช่วงระยะเวลา 1 บิต ซึ่งจะเรียกบิตนี้ว่าบิตเริ่มต้น จากนั้นบิตข้อมูลจะถูกส่งออกไปโดยเริ่มจากบิตที่มีนัยสำคัญต่ำที่สุด (LSB) ก่อน ซึ่งข้อมูลในไบต์ที่จะส่งอาจจะมีจำนวนบิต 5, 6, 7 หรือ 8 บิตก็ได้ จากนั้นจะตามด้วยบิตพาริตี้ ซึ่งใช้เพื่อตรวจสอบความผิดพลาดที่เกิดขึ้นจากการส่งข้อมูลบิตสุดท้ายที่จะส่งคือบิตปิดท้าย ซึ่งจะให้ขาคาต้ามีสถานะลอจิก 1 อีกครั้งด้วยระยะเวลาอย่างน้อย 1 บิต, 1.5 บิต หรือ 2 บิต เพื่อเป็นการแสดงว่าสิ้นสุดข้อมูลแล้ว

อุปกรณ์พิเศษที่ได้รับการออกแบบมาสำหรับการรับและการส่งข้อมูลแบบอะซิงโครนัส เรียกว่า Universal Asynchronous Receiver / Transmitter หรือ UART อัตราความเร็วในการรับและการส่งข้อมูลของการรับส่งข้อมูลแบบอะซิงโครนัส คือ ค่าอัตราบอด ซึ่งก็คือค่าอัตราการเข้ารหัสที่ใช้ในการรับและส่งข้อมูล อัตราบอดมาตรฐานที่ใช้สำหรับพอร์ทอนุกรม RS-232 ได้แก่ 110, 150, 300, 600, 1200, 2400, 4800, 9600 และ 19200 บิตต่อวินาที และมีค่าเพิ่มมากขึ้นตามเทคโนโลยีของคอมพิวเตอร์ ซึ่งการรับส่งแบบอนุกรมโดยไม่ผ่านโมเด็มอาจจะสามารถกำหนดค่าอัตราบอดได้สูงถึง 115,200 บิตต่อวินาที เนื่องจากอัตราบอดคือ จำนวนบิตของข้อมูลที่สามารถถ่ายทอดได้ภายใน 1 วินาที ยกตัวอย่าง ข้อมูลอนุกรมถูกส่งในลักษณะ 8 บิต ไม่มีการตรวจสอบพาริตี้ มีบิตเริ่มต้น 1 บิตและบิตปิดท้าย 1 บิต ความยาวของข้อมูลที่รับส่งนี้เท่ากับ 10 บิต ถ้าใช้อัตราบอดในการส่งข้อมูลเท่ากับ 9600 บิตต่อวินาที ก็จะสามารถรับส่งข้อมูลได้ด้วยความเร็ว 960 ไบต์ต่อวินาที และถ้ามีการใช้พาริตี้ความเร็วในการรับส่งข้อมูลจะเหลือเป็น 872 ไบต์ต่อวินาที

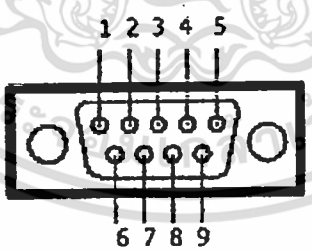
MAX-232 เป็น IC ในวงจรที่ทำหน้าที่เปลี่ยนแรงดันที่เข้ามาจาก Serial Port ซึ่งเป็นแรงดันตามมาตรฐานของ RS-232 โดยเปลี่ยนเป็นระดับแรงดัน TTL เพื่อให้ใช้ได้กับไมโครคอนโทรลเลอร์

ลักษณะของการส่งข้อมูลแบบอนุกรมนั้น ข้อมูลจะส่งออกมาทีละบิตจากตัวส่งไปตัวรับข้อมูล ช่องสัญญาณในการส่งข้อมูลอาจใช้เพียง 1 หรือ 2 ช่องสัญญาณเท่านั้น ทำให้ค่าใช้จ่ายในการสื่อสารจะถูกกว่าแบบขนาน แต่อัตราการรับ-ส่งข้อมูลจะช้ากว่าแบบขนาน ในการส่งข้อมูลแบบอนุกรมข้อมูลที่ต้องการส่งจะอยู่ในลักษณะเป็นไบต์จะทยอยส่งทีละบิต และทางตัวรับจะต้องรับข้อมูงเข้ามาทีละบิตแล้วมารวมกันเป็นไบต์ ซึ่งทางตัวรับต้องคอยตรวจสอบว่าบิตใดเป็นบิตเริ่มต้นหรือบิตสุดท้ายของข้อมูล การตรวจสอบนั้นจะขึ้นอยู่กับรูปแบบของรหัสของบิตข้อมูลที่ใช้ ซึ่งในการรับส่งข้อมูลแบบอนุกรมระหว่างไมโครคอมพิวเตอร์กับอุปกรณ์ภายนอกนั้นจำเป็นจะต้องมีมาตรฐานในการรับส่งข้อมูล ซึ่งมาตรฐานที่นิยมมากที่สุดก็คือมาตรฐาน RS-232

2.2.2 มาตรฐาน RS-232

เพื่อที่จะทำให้อุปกรณ์จากผู้ผลิตต่างกันทำงานร่วมกันได้ มาตรฐานหลายชนิดจึงได้รับการออกแบบขึ้น มาตรฐานที่ใช้กันอย่างกว้างขวางที่สุดคือ RS-232 ซึ่งปกติไมโครคอมพิเตอร์จะมีพอร์ทที่เป็นแบบอนุกรมอยู่ในตัวแล้ว และจะทำหน้าที่รับส่งข้อมูลในแบบอนุกรม

ตามจุดประสงค์ของมาตรฐาน RS-232 นั้นเพื่อจะสามารถเชื่อมต่อกันระหว่างอุปกรณ์รับส่งปลายทาง (Data Terminal Equipment : DTE) เช่น พอร์ทของคอมพิวเตอร์หลักหรืออุปกรณ์ปลายทางกับอุปกรณ์สื่อสาร RS-232 เป็นข้อกำหนดของการอินเตอร์เฟสมาตรฐาน และสามารถใช้เพื่อจุดประสงค์อื่นต่างกันไป เช่น การสื่อสารแบบซิงโครนัส (synchronous communication) และรูปแบบการสื่อสารที่ต้องการสัญญาณนาฬิกา และสัญญาณกำหนดจังหวะเพิ่มเติมขึ้นมา ในความเป็นจริงแล้วเราสามารถทำให้มีการสนทนากันระหว่าง DTE และ DCE โดยการใช้สายสัญญาณเพียง 3 เส้นเท่านั้น คือใช้สาย Tx สาย Rx และสายกราวด์เท่านั้น มีลักษณะของคอนเน็คเตอร์ดังรูปที่ 5



รูปที่ 2.18 ลักษณะของคอนเน็คเตอร์แบบ DB-9

2.2.3 ระบบเครือข่าย Ethernet

ระบบเครือข่าย Ethernet เป็นระบบเครือข่ายท้องถิ่นหรือ LAN (Local Area Network) ประกอบด้วยส่วนที่เป็นฮาร์ดแวร์ที่ทำงานร่วมกันเพื่อการส่งถ่ายข้อมูลในระบบดิจิตอลระหว่างคอมพิวเตอร์ระบบเครือข่าย Ethernet มีลักษณะดังนี้

1. เป็นระบบเครือข่ายที่มีความเร็วในการส่งข้อมูลในรูปแบบดิจิตอลที่มีความเร็วตั้งแต่ 10 Mbps จนถึง 1,000 Mbps (1 Gbps)

2. เป็นเครือข่ายที่มีขนาด Diameter ตั้งแต่ 205 เมตรจนถึง 4,000 เมตร

3. ใช้โปรโตคอลการทำงานที่เรียกว่า CSMA/CD (Carrier Sense Multiple Access with Collision Detect) ซึ่งเป็นมาตรฐานของ IEEE802.3 นอกจากนี้ก็ยังมีมาตรฐาน IEEE802.3a สำหรับ Gigabit Ethernet ที่ใช้สายทองแดง

4. หนึ่งเครือข่าย Ethernet สามารถมีอุปกรณ์เชื่อมต่อ เช่น คอมพิเตอร์ลูกข่าย อุปกรณ์ Repeater เป็นต้น ได้มากมายถึง 1,024 รายการหรือเรียกว่า Node

5. เป็นเครือข่ายที่สามารถใช้สายสัญญาณได้หลายแบบ เช่น สาย coaxial ทั้งแบบหนาแบบบาง สาย Twisted Pair ทั้งแบบ Shield และ Unshield รวมทั้งสาย Optical Fiber แบบขนาดต่างๆ นอกจากนี้ยังสามารถใช้สื่อที่ใช้รับส่งข้อมูลแบบไร้สายเช่น คลื่นวิทยุที่มีความถี่ Spread Spectrum รวมทั้งไมโครเวฟ (Microwave) ที่ใช้ความถี่ในช่วง 14 GHz. และอินฟาเรด (infrared) เป็นต้น

6. เป็นระบบเครือขายที่มีการเชื่อมต่อในรูปแบบ Bus และ Star Topology

7. อุปกรณ์ราคาประหยัด

8. มีความน่าเชื่อถือสูง โดยเฉพาะหากใช้สื่อที่เป็นสาย Optic Fiber

9. มีเครื่องมือในรูปแบบของซอฟแวร์ที่ให้บริการจัดการเครือข่ายมากมายที่ทำงานภายใต้ SNMP (Simple Network Management Protocol)

2.2.4 ส่วนประกอบหลักที่สำคัญของเครือข่าย Ethernet

ระบบเครือข่าย Ethernet มีส่วนประกอบหลักซึ่งเมื่อทำงานด้วยกันแล้วจะเป็นเครือข่ายที่มีประสิทธิภาพการทำงานสูงดังนี้

1. ตัวเฟรมเป็นชุดรูปแบบของบิตข้อมูลข่าวสารที่ใช่ส่งผ่านมาบนระบบ หากไม่มีเฟรมจะไม่สามารถสื่อสารข้อมูลบนเครือข่ายได้เด็ดขาด การรับส่งข้อมูลข่าวสารบนเครือข่าย Ethernet จะต้องเป็นรูปแบบเฟรมมาตรฐาน 2 แบบ และเป็นแบบใดแบบหนึ่งเท่านั้น (การ์ด LAN เป็นผู้สร้างเฟรมนี้ขึ้นมา)

2. ชุดโปรโตคอลที่ใช้ในการควบคุมการแอกเซสเข้าไปเครือข่าย (Media Access Control Protocol) ซึ่งประกอบด้วยชุดของกฎกติกาที่อยู่ใน Ethernet Interface (เช่น การ์ด LAN เป็นต้น) ซึ่งเป็นกฎกติกามาตรฐานที่จะยอมให้คอมพิวเตอร์ต่างๆ สามารถเข้ามในเครือข่ายและแบ่งใช้ทรัพยากรต่างๆ บนเครือข่ายได้อย่างมีประสิทธิภาพ

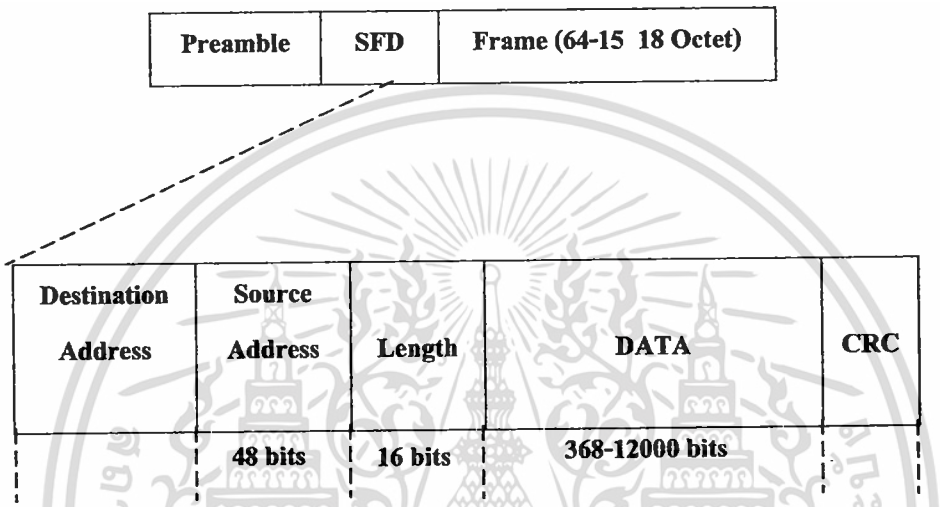
3. อุปกรณ์ที่ใช้รับส่งสัญญาณบนเครือข่าย (Signaling Components) ประกอบด้วยชุดของอุปกรณ์ที่ใช้เชื่อมต่อและส่งสัญญาณเพื่อการรับส่งข้อมูลในเครือข่าย

4. สื่อที่ใช้ในการรับส่งสัญญาณข้อมูลบนเครือข่าย (Physical Medium) ประกอบด้วยสายสัญญาณรวมทั้งอุปกรณ์ทางฮาร์ดแวร์อื่นๆ ที่จะช่วยในการนำพาข้อมูลข่าวสารต่างๆ ในรูปแบบดิจิตอลวิ่งไปมาบนเครื่อง

2.2.5 เฟรมบนระบบ Ethernet

หัวใจสำคัญของระบบ Ethernet ได้แก่ เฟรมข้อมูลทางข่าวสารและอุปกรณ์ทางฮาร์ดแวร์ที่ใช้เชื่อมต่อสื่อสารบนเครือข่าย ซึ่งได้แก่ การ์ด Ethernet LAN สายสัญญาณและอุปกรณ์เสริมอื่นๆ ที่จะช่วยนำพาข้อมูลในรูปแบบของบิตทางดิจิตอล ที่เรียกว่าเฟรมวิ่งไปวิ่งมาระหว่างคอมพิวเตอร์บนเครือข่าย

เฟรมข้อมูลสำหรับระบบ Ethernet ประกอบขึ้นด้วยกลุ่มของบิตที่เป็นข้อมูลและข่าวสารสำคัญแบ่งออกเป็นขนาดสัดส่วนที่แน่นอนที่เรียกว่า ช่อง Field



รูปที่ 2.19 ลักษณะโครงสร้างของเฟรมข้อมูล

จากรูปที่ 6 ทั้งสองเฟรมจะมีความแตกต่างกันเล็กน้อย ทำให้เครือข่ายที่ใช้เฟรมแตกต่างกันนี้อาจไม่สามารถเข้ากันได้ หมายความว่าระบบเครือข่าย Ethernet ของท่านจะต้องเลือกใช้อุปกรณ์เครือข่ายที่คอยสนับสนุนเฟรมอย่างใดอย่างหนึ่งเท่านั้น แต่ก็เป็นเรื่องที่ดีที่ผู้ผลิตอุปกรณ์สนับสนุนเฟรมทั้งสองแบบในตัวเดียวกันดังรูปที่ 7

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

รูปที่ 2.20 ลักษณะของ Ethernet II Frame

ข้อกำหนดเกี่ยวกับขนาดของ Data Frame

ขนาดของ Data Frame มีมาตรฐานดังต่อไปนี้

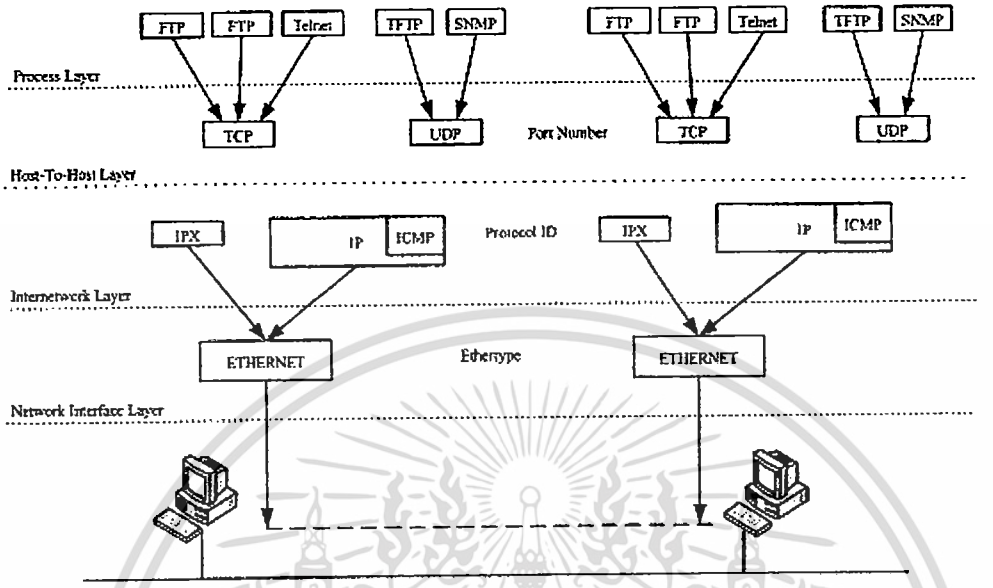
1. ขนาดเล็กที่สุด ต้องไม่น้อยกว่า 64 byte โดยมี 12 byte สำหรับแอดเดรส 2 byte สำหรับช่อง length 46 byte สำหรับเก็บข้อมูล และ 4 byte สำหรับตรวจสอบความผิดพลาดข้อมูล หรือ Frame Check Sequence

2. ขนาดใหญ่ที่สุดต้องไม่เกิน 1,518 byte โดยแบ่งออกเป็น 12 byte สำหรับแอดเดรส 2 byte สำหรับ Length 1,500 byte สำหรับข้อมูล และ 4 byte สำหรับช่องตรวจสอบความผิดพลาดข้อมูล

3. เฟรมที่มีขนาดเล็กที่สุด 64 byte จะต้องใช้เวลาอยู่ที่ 51.2 ไมโครวินาที

2.2.6 โครงสร้างของสถาปัตยกรรมรูปแบบของ Protocol TCP/IP

สามารถแบ่งออกเป็น 4 เลเยอร์ และในแต่ละเลเยอร์ได้มีการกำหนดหน้าที่การทำงานไว้ดังรูปที่ 8



รูปที่ 2.21 แสดงการรับส่งข้อมูลผ่านโปรโตคอล TCP/IP

Process Layer

เป็นลำดับชั้นการทำงานของโปรโตคอล TCP/IP มาตรฐาน DoD-Reference Model ซึ่งเมื่อนำมาเปรียบเทียบกับมาจรฐาน OSI-Reference Model นั้น ในชั้นบนสุดที่เรียกว่า Process Layer ของ DoD Model จะทำงาน 2 หน้าที่เทียบได้กับ Application Layer และ Presentation Layer ของ OSI-Reference Model ในชั้นนี้จะรองรับการทำงานของ Application ต่างๆ อย่างเช่น เมื่อเครื่อง Client ทั่วไป ขอใช้บริการเพื่อจะติดต่อขอ Download File ผ่านทาง Internet โดยอาจจะเรียกใช้โปรแกรม FTP Client ทั่วไป อย่างเช่นโปรแกรม WS_ftp เพื่อติดต่อกับโปรเซส FTP ที่กำลังให้บริการอยู่ที่เครื่อง Server จากนั้นตัวโปรเซส FTP ก็จะเรียกใช้โปรโตคอล FTP (File Transfer Protocol) เพื่อทำการโอนถ่ายไฟล์นี้ไปให้เครื่อง Client เป็นต้น หรือถ้าผู้ใช้ต้องการเรียกใช้งานคอมพิวเตอร์จากเครื่องที่อยู่ห่างไกลออกไปด้วยการใช้โปรแกรม Telnet ที่เครื่อง Server ให้บริการตัวโปรเซส Telnet ที่ทำงานอยู่ก็จะเรียกใช้โปรโตคอล Telnet เพื่อติดต่อกัน

การทำงานของ Application ต่างๆ จะอยู่ที่ Process Layer นี้ และมีการติดต่อกันตามแต่ละโปรโตคอลเฉพาะแล้วแต่ Application ที่ใช้งานจากการที่ Process Layer ของ TCP/IP รองรับให้โปรโตคอลอื่นทำงานได้หลายโปรเซส และหลายโปรโตคอลได้พร้อมกัน นั้นทำให้ผู้ใช้สามารถเปิดโปรแกรมใช้งานได้หลายอย่างพร้อมกัน เช่น เปิดโปรแกรม Internet Explorer เพื่อเรียกดูเว็บเพจพร้อมกับใช้งานโปรแกรม Outlook Explorer เพื่อรับส่ง E-mail ไปพร้อมกันได้โดยไม่ต้องรอให้การทำงานอย่างใดอย่างหนึ่งเสร็จไปก่อน หรือในปัจจุบันมีการพัฒนาโปรแกรม Web Browser โดยถ่ายโอนไฟล์ข้อมูลที่ใช้โปรโตคอล FTP ได้โดยไม่ต้องไปหาโปรแกรมอื่นมาใช้เพิ่มเติมอีก

โปรโตคอลหลักที่ทำงานและให้บริการในชั้น Process Layer

1. FTP (File Transfer Protocol)

FTP ที่ใช้ในการรับ-ส่งแฟ้มข้อมูลระหว่างเครื่องลูกข่ายและเครื่อง Server จะต้องมีโปรแกรมให้บริการ FTP (FTP Server) ติดตั้งและทำงานอยู่ เพื่อให้ลูกข่ายที่รันโปรแกรม FTP Client สามารถเข้ามาใช้บริการได้

2. Telnet

Telnet เป็นบริดารที่ให้ลูกข่ายสามารถเข้าไปใช้เครื่อง Server โดยจำลองตัวเองให้ทำงานในเทอร์มินอล ผู้ใช้งานจะต้องใส่รหัสผู้ใช้งานและรหัสผ่านเพื่อแจ้งการเข้าใช้เครื่อง เมื่อเข้าไปใช้ได้แล้ว การทำงานจะเหมือนกับการเข้าไปทำงานที่หหน้าจอของเครื่อง Server การทำงานแบบนี้เครื่อง Server จะติดตั้งโปรแกรมการให้บริการ Telnet ซึ่งโดยปกติในระบบปฏิบัติการยูนิกส์ จะมีบริการนี้ติดตั้งไว้แล้วเป็นมาตรฐาน มีศัพท์เรียกโปรแกรมให้บริการบนเครื่องยูนิกส์ว่า daemon เช่น FTP daemon, Telnet daemon เป็นต้น

3. HTTP (Hypertext Transfer Protocol)

HTTP ใช้ในการติดตั้งรับส่งข้อมูลชนิดไฮเปอร์เท็กซ์ (Hypertext) ระหว่างเครื่องลูกข่ายกับ WWW Server (World Wide Web) โดยเอกสารนี้จะอยู่ในรูปแบบที่เขียนในภาษา HTML (Hypertext Markup Language) เอกสารแต่ละชิ้นจะสามารถเชื่อมโยงไปยังเอกสารอื่นได้ ซึ่งเอกสารที่ถูกเชื่อมโยงนี้อาจจะอยู่บนเครื่องคอมพิวเตอร์เดียวกันหรือต่างเครื่องกันก็ได้

4. SMTP (Sample Mail Transfer Protocol)

SMTP เป็นการให้บริการอินเตอร์เน็ตเพื่อรับส่งจดหมายอิเล็กทรอนิกส์ (E-mail) โดยที่ SMTP จะมีตู้ไปรษณีย์เพื่อทำหน้าที่รับจดหมายจากผู้อื่นที่ต้องการส่งให้และการเก็บจดหมายของผู้ใช้ที่ต้องการส่งไปยังผู้ใช้อื่น เมื่อถึงกำหนดเวลาที่ตั้งไว้โปรแกรมจะทำการส่งจดหมายออกและรับจดหมายเข้า ผู้ใช้ก็สามาระจะเปิดอ่านได้เมื่อต้องการ

นอกจากนี้โปรโตคอลที่อยู่เบื้องหลัง ซึ่งทำงานโดยที่ผู้ใช้สามารถมองเห็นได้จากโปรแกรมหรือไม่ได้มีการใช้งานโยตรง เช่น

- Protocol DNS (Domain Name System) ที่ทำหน้าที่แปลงข้อมูลชื่อ Domain Name หรือชื่อเว็บไซท์ทั้งหลายให้เป็นหมายเลข IP Address

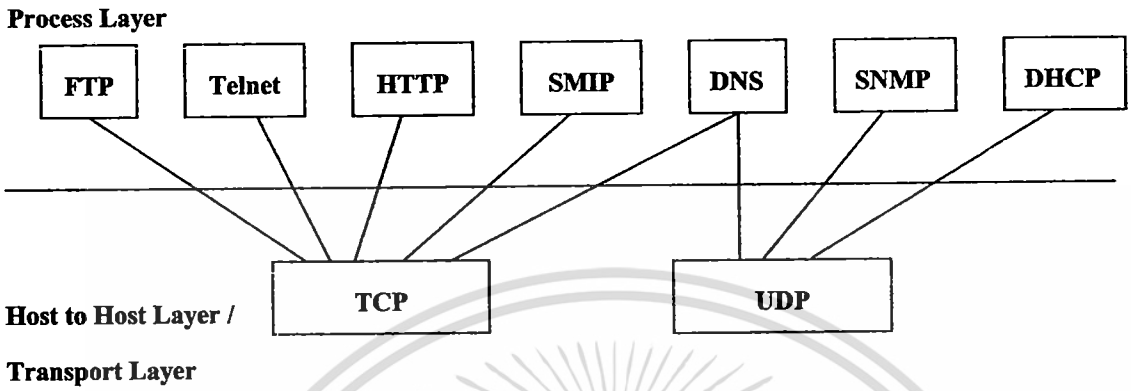
- Protocol SNMP (Simple Network Management Protocol) ใช้ในการควบคุมและตรวจสอบอุปกรณ์ที่อยู่ในเครือข่าย

- Protocol DHCP (Dynamic Configuration Protocol) ทำหน้าที่แจกจ่ายข้อมูล พารามิเตอร์ของโครงข่ายให้กับเครื่องลูกข่ายที่เชื่อมต่ออยู่

Host-to-Host Layer

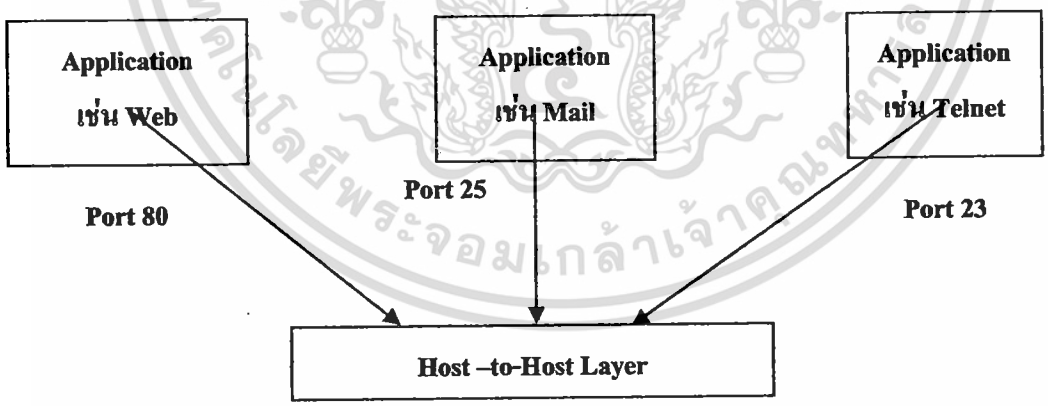
การทำงานที่ชั้นของ Host-to-Host Layer จะมีบทบาทในการจัดการต่อจากชั้นของ Process Layer บางครั้งเรามักเรียกชั้น Host-to-Host Layer ว่าเป็น Transport Layer ซึ่งไม่ใช่ชั้นของ Transport Layer ในมาตรฐาน OSI-Reference Model การทำงานของ Host-to-Host Layer นี้จะมีการสร้าง Connection หรือการเชื่อมต่อกันระหว่างแอพพลิเคชัน Host-to-Host Layer โดยจุดที่เชื่อมกันเพื่อรับส่งข้อมูลนี้เรียกว่า Port หรือ

Socket (คำว่า Port ในที่นี้ไม่ได้หมายถึง Port ทาง Hardware) และในแต่ละแอพพลิเคชันก็จะสร้างการเชื่อมต่อผ่าน Port ได้พร้อมกันหลายแอพพลิเคชัน ซึ่งการใช้งาน Port ของแต่ละแอพพลิเคชันที่อยู่ในชั้น Process Layer จะแตกต่างกันตามหมายเลขที่กำหนดไว้และแต่ละโปรโตคอลจะมีการใช้งาน Port หมายเลขไม่ซ้ำกันดังรูปที่ 9



รูปที่ 2.22 แสดงการใช้งาน port ตองแต่ละโปรโตคอล

เมื่อแอพพลิเคชันทำงานผ่านโปรโตคอลในชั้น Process Layer จะมีการส่งผ่านข้อมูลไปยัง Host-to-Host Layer ที่ชั้นนี้จะมีการเชื่อมต่อผ่าน port ที่กำหนดดังรูปที่ 9 ทำให้การรับส่งข้อมูลในแต่ละโปรโตคอลทำได้ถูกต้อง ถึงแม้ว่าในเครื่องเซิร์ฟเวอร์ที่ให้บริการจะมีการทำงานอยู่หลายโปรเซสที่แตกต่างกันก็ตามหรือมีผู้ใช้บริการเข้ามาใช้งานพร้อมกันจำนวนมากและหลายแอพพลิเคชันในเวลาเดียวกัน ในชั้น Host-to-Host หรือ Transport layer ของ TCP/IP นี้ จะมีโปรโตคอลทำงานอยู่ 2 โปรโตคอลที่แตกต่างกัน คือ โปรโตคอล TCP และโปรโตคอล UDP (User Datagram Protocol) ในการส่งผ่านข้อมูลลงไปที่ชั้นถัดไป จะเห็นว่าโปรโตคอล TCP และ UDP จะถูกผนึกเข้าไปในโปรโตคอล IP อีกทีหนึ่งและส่งต่อไปยังเครือข่ายอินเตอร์เน็ตต่อไป



รูปที่ 2.23 แสดงการส่งข้อมูลจาก Application ไปยัง Host-to-Host Layer

ตัวโปรโตคอล TCP และโปรโตคอล UDP จะมีแอพพลิเคชันเฉพาะเพื่อเรียกใช้งานแยกกันคือ แอพพลิเคชันที่ใช้โปรโตคอล FTP, Telnet, HTTP และ SMTP จะมีการส่งผ่านข้อมูลโดยเรียกใช้โปรโตคอล TCP ส่วนแอพพลิเคชัน SNMP และ DHCP จะส่งผ่านข้อมูลโดยเรียกใช้โปรคอล UDP และสำหรับโปรโตคอล DNS นั้นจะสามารถเรียกใช้งานได้ทั้ง TCP และ UDP ดังรูป ซึ่งเหตุผลที่มีการเรียกใช้โปรโตคอล TCP และ UDP แตกต่างกัน เนื่องจากวิธีการทำงานของทั้งสองโปรโตคอลต่างกัน

โปรโตคอล TCP

โปรโตคอล TCP (Transmission Control Protocol) เป็นโปรโตคอลที่มรการรับส่งข้อมูลแบบ stream oriented protocol หมายความว่า การรับส่งข้อมูลจะไม่คำนึงถึงปริมาณข้อมูลที่จะส่งไป แต่จะแบ่งข้อมูลเป็นส่วนย่อยๆ ก่อนแล้วจึงจะส่งไปยังปลายทางอย่างต่อเนื่องเป็นลำดับข้อมูล ในกรณีที่ข้อมูลส่วนใดส่วนหนึ่งสูญหายไป จะส่งข้อมูลส่วนนั้นใหม่อีกครั้ง สำหรับปลายทางจะทำหน้าที่จัดเรียงส่วนของข้อมูล datagram ใหม่ให้ต่อเนื่องกันและประกอบกับเป็นข้อมูลทั้งหมดได้ ซึ่งจะแยกข้อมูลที่ไม่ถูกต้องออก ดังนั้นแอพพลิเคชันหรือโปรเซสใดที่อาศัยการส่งผ่านข้อมูลด้วยโปรโตคอล TCP จะต้องใช้หน่วยความจำและขนาดของช่องสัญญาณ (bandwidth) มากกว่า UDP การติดต่อระหว่างกันจะต้องเป็นแบบ connection-oriented คือ ต้องมีการสร้างการติดต่อกันเป็น session ทั้ง 2 ด้านเสียก่อน แล้วจึงจะรับส่งข้อมูลไปได้พร้อมกัน (full duplex) เหมือนกับการใช้โทรศัพท์ติดต่อกัน เมื่อผู้ติดต่อต้องการเรียกให้ฝ่ายตรงข้ามรับสายแล้วจึงเริ่มการสนทนา เช่น พูดคำว่า “สวัสดี” หรือ “ฮัลโหล” กันก่อนเพื่อให้แน่ใจว่าอีกฝ่ายตรงข้ามพร้อมที่จะติดต่อด้วย จากนั้นจึงเริ่มที่จะติดต่อกันและเมื่อต้องการจะเลิกการติดต่อก็จะมีการพูดคำว่า “สวัสดี” ให้ฝ่ายตรงข้ามทราบว่าจะเลิกการติดต่อและวางสายไป ซึ่งในระหว่างการติดต่อกันนั้น แม้ว่าฝ่ายใดฝ่ายหนึ่งหรือทั้งสองฝ่ายจะเงียบไป คือ ไม่พูดอะไรกันเป็นเวลานานๆ แต่การเชื่อมโยงระหว่างทั้งสองด้านยังคงมีอยู่ไม่ขาดไปจนกว่าฝ่ายใดฝ่ายหนึ่งจะวางสาย เช่นเดียวกับการติดต่อกันด้วยกลไกโปรโตคอล TCP เมื่อแอพพลิเคชันต้องการผ่านข้อมูลจะใช้โปรโตคอลที่เหมาะสมในชั้น Process Layer ติดต่อไปและมีการสร้างช่องส่งข้อมูลผ่าน port ที่กำหนดเพื่อส่งผ่านข้อมูลไปยังโปรโตคอล TCP

ในระหว่างการรับส่งข้อมูลนี้ โปรโตคอล TCP จะเพิ่มกระบวนการสอบทานข้อมูลเพื่อให้ข้อมูลมีความถูกต้องไม่ผิดพลาดไปจากเดิม โดยการส่งสัญญาณสอบทานข้อมูล (acknowledgement) และส่งข้อมูลให้ใหม่อีกครั้งถ้าปลายทางไม่ได้รับหรือเกิดความผิดพลาดขึ้น ความน่าเชื่อถือของการส่งผ่านข้อมูลโดยโปรโตคอล TCP จะมีมากกว่า แต่ก็ต้องอาศัยทรัพยากรของระบบมากกว่าในการทำงานเช่นกัน

โปรโตคอล UDP

ใน Host-to-Host Layer นอกจากนี้จะมีโปรโตอคล TCP ทำงานแล้ว ก็ยังมีโปรโตคอล UDP (User Datagram Protocol) ที่มีคุณสมบัติแตกต่างกันอยู่ด้วย ในการรับส่งข้อมูลผ่านโปรโตคอล UDP จะเป็นแบบที่ทั้งสองด้านไม่จำเป็นต้องอาศัยการสร้างช่องทางเชื่อมต่อกัน (connectionless) ระหว่างเครื่องเซิร์ฟเวอร์ให้บริการกับเครื่องที่ขอใช้บริการ โดยไม่ต้องแจ้งให้ฝ่ายรับข้อมูลเตรียมรับข้อมูลเหมือนโปรโตคอล TCP และไม่มีการตรวจสอบความถูกต้องครบถ้วนในการรับส่งข้อมูล เนื่องจากโปรโตคอล UDP ไม่มัญญาณสอบทานข้อมูล (acknowledgement) ในการส่งข้อมูแต่ละครั้งและไม่มีการส่งข้อมูลใหม่อีกในกรณีที่เกิดความผิดพลาด

ของการส่งข้อมูล เมื่อเป็นเช่นนี้แอพพลิเคชันหรือโปรเซสใดที่ต้องอาศัยโปรโตคอล UDP ในการส่งผ่านข้อมูล ก็อาจจะต้องสร้างขบวนการตรวจสอบข้อมูลขึ้นมาเอง

ตัวอย่างขั้นตอนกลไกการทำงานโดยใช้โปรโตคอล UDP มีดังต่อไปนี้

1. ในชั้นของ Process Layer เมื่อโปรแกรมควบคุมอุปกรณ์เครือข่าย เช่น โปรแกรม Network Management ต้องการส่งข้อมูลไปยังอุปกรณ์ที่ต้องการแอพพลิเคชันนั้นจะติดต่อผ่านโปรโตคอล SNMP ในชั้น Process Layer

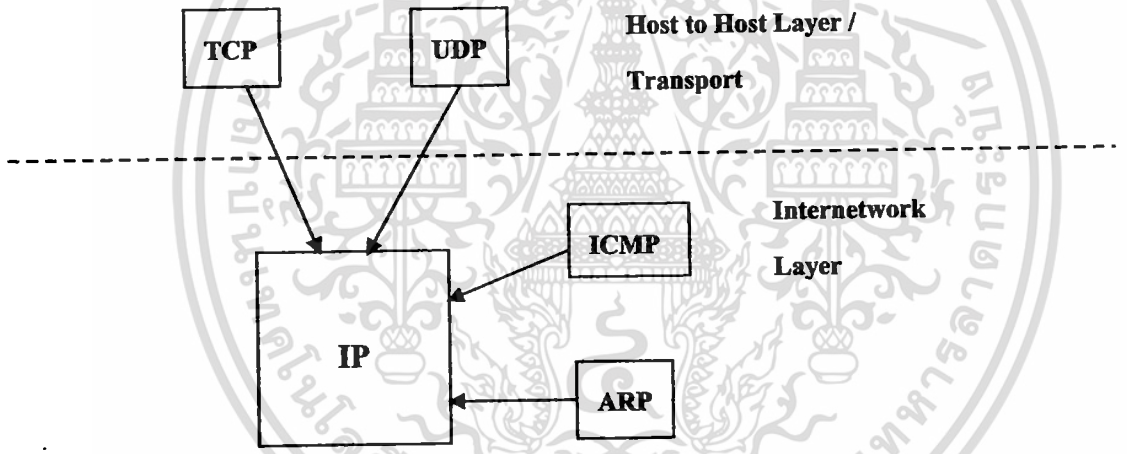
2. โปรโตคอล SNMP จะติดต่อกับโปรโตคอล UDP ในชั้นถัดไปเพื่อขอติดต่อผ่าน port ที่กำหนด

3. โปรโตคอล SNMP เตรียมข้อมูลที่จะส่งรวมทั้งที่อยู่ปลายทาง

4. โปรโตคอล SNMP ส่งผ่านข้อมูลให้โปรโตคอล UDP ที่อยู่ในชั้น Host-to-Host Layer

5. โปรโตคอล UDP ทำหน้าที่ผนึกข้อมูลหรือ datagram นั้น ให้กับโปรโตคอล IP ในชั้นถัดลงไปเพื่อส่งข้อมูลออกจากเครื่อง

ซึ่งจะเห็นว่ามีกลไกที่ต่างจากการส่งข้อมูลด้วยโปรโตคอล TCP ซึ่งจะต้องมีการติดต่อกันก่อนและทั้งสองฝ่ายรับทราบการรับส่งข้อมูลของช่องการส่งข้อมูล



รูปที่ 2.24 แสดงกลไกการส่งข้อมูลด้วยโปรโตคอล UDP

จากรูปที่ 11 จะเห็นว่าโปรโตคอลชั้นบนขึ้นไปที่ใช้การส่งข้อมูลโดยโปรโตคอล UDP เช่น โปรโตคอล SNMP (ใช้ควบคุมและจัดการอุปกรณ์ในเครือข่าย) หรือโปรโตคอล DHCP (ใช้ส่งข้อมูลพารามิเตอร์ของเครือข่ายให้กับเครื่องลูกข่ายได้ใช้งาน) การส่งข้อมูลเหล่านั้นไม่ต้องทราบหรือตรวจสอบว่าข้อมูลไปถึงปลายทางถูกต้องหรือไม่ แต่กลไกการตรวจสอบข้อมูลที่มีการรับส่งจะไปทำให้ขั้นของโปรโตคอลชั้นที่สูงกว่าแทน

UDP Header

มีขนาด 8 ไบต์ โดยประกอบด้วย 4 ส่วน ดังรูปที่ 12

Source Port	Destination Port	Length	Checksum
2 ไบต์	2 ไบต์	2 ไบต์	2 ไบต์

รูปที่ 2.25 แสดงโครงสร้างของ UDP Header

- **Source Port** มี 2 ไบต์ใช้ระบุเป็น Source Application Layer Protocol ทำการส่ง UDP Message โดย Source Port เป็น port ที่ใช้ในการเลือก เมื่อใดที่ไม่ได้ใช้มัน มันจีค่าเป็น 0×00-00 IP multicast traffic เปรียบเสมือน videocasts ใช้ส่ง UDP สามารถใช้ค่า 0×00-00 เพราะจะไม่ตอบรับ video traffic เป็นเพียงการสมมุติ Application Layer ใช้ Source Port ในการนำ UDP Message เข้ามา Destination Port สำหรับการตอบรับ

- **Destination Port** มี 2 ไบต์ใช้ระบุเป็น Destination Application Layer Protocol การรวม Destination IP Address ของ IP Header และ Destination Port ของ UDP Header จะไม่เหมือนใครสำหรับกระบวนการที่จะส่งข้อมูล

- **Length** มี 2 ไบต์ที่ใช้ในการแสดงความยาวใน UDP Message มีความยาวน้อยที่สุด 8 ไบต์ (ขนาดของ UDP Header) และมากที่สุด 65,515 ไบต์ (ค่าสูงสุด IP Datagram 65,535 ไบต์น้อยกว่าค่าน้อยที่สุด IP Header 20 ไบต์) ความยาวมากที่สุดที่แท้จริงถูกจำกัดโดย MTU ซึ่งจะทำการเชื่อมโยงโดย UDP Message เป็นตัวส่งความยาว UDP สามารถคำนวณได้จากความยาวทั้งหมดและความยาวของ IP Header field ใน IP Header

- **Checksum** มี 2 ไบต์โดยจะทำการตรวจระดับของบิตอย่างสมบูรณ์สำหรับ UDP Message โดยที่ UDP Checksum คำนวณโดยใช้วิธีเดียวกันกับ IP Header Checksum

ตารางที่ 2.3 UDP Checksum คำนวณโดยใช้วิธีเดียวกันกับ IP Header Checksum

ตำแหน่ง	ชื่อ	อธิบาย
บิต 0-15	Source port number	หมายเลขโทรศัพท์ที่ส่งดาต้าแกรมนี้ มีความยาว 16 บิต
บิต 16-31	Destination port number	หมายเลขพอร์ทปลายทางที่จะเป็นผู้รับดาต้าแกรม มีความยาว 16 บิต เช่นกัน
บิต 32-47	UDP Length	ความยาวของดาต้าแกรมทั้งส่วน Header และ data นั่นหมายความว่า ค่าที่น้อยที่สุดในฟิลด์นี้คือ 8 ซึ่งเป็นขนาดของ Header
บิต 48-63	Checksum	เป็นตัวตรวจสอบความถูกต้องของ UDP datagram และจะนำข้อมูลบางส่วนใน IP Address มาคำนวณด้วย

UDP Port

UDP Port จะแสดงที่ตั้งหรือแถวของ message ที่ชัดเจนสำหรับการส่ง message ถึง Application Layer Protocol โดยใช้ UDP services รวมถึงในแต่ละตัวของ UDP message เป็น Source Port และ Destination Port ซึ่ง Internet Assigned Number Authority (IANA) จะเป็นตัวกำหนดหมายเลข Port

ตารางที่ 2.4 UDP Port Numbers

Port Number	Application Layer Protocol
53	Domain Name System (DNS)
67	BOOTP client (Dynamic Host Configuration Protocol [DHCP])
68	BOOTP server (DHCP)
69	Trivial File Transfer Protocol (TFTP)
137	NetBIOS Name Service
138	NetBIOS Datagram Service
161	Simple Network Management Protocol (SNMP)
520	Routing Information Protocol (RIP)
445	Direct hosting of serve Message Block (SMB) datagram over TCP/IP
1812, 1813	Remote Authentication Dial-In User Service (RADIUS)

UDP Checksum

Checksum เป็นเลข 16 บิตถูกคำนวณด้วยวิธี one's complement โดยนำ Pseudo Header และข้อมูลทั้งหมดใน UDP Datagram มาคำนวณ Pseudo Header เป็นข้อมูลที่อยู่ในส่วนของ IP Header) ประกอบด้วยฟิลด์ source IP address destination IP address, zero, protocol, UDP length ดังแสดงในรูปที่ 13

16-bit Source IP address		
16-bit Source IP address		
zero	8-bit Protocol (17 for UDP)	16-bit length

รูปที่ 2.26 Pseudo Header

หาค่า Checksum ที่คำนวณออกมาเป็น 0 ค่า Checksum จะถูกเซ็ตเป็น 1 ทั้งหมดแทน (มีค่าเท่ากันในระบบ 1's complement) ทั้งนี้เพราะในบางแอพพลิเคชันที่ไม่ต้องการตรวจสอบค่า checksum ในระดับ UDP จะเซ็ตค่านี้เป็น 0 (disable checksum)

Internetwork Layer

ในระดับล่างต่อมาในชั้น Internetwork Layer มีหน้าที่ส่งผ่านข้อมูลในระหว่างเครือข่ายโดยมีโปรโตคอลที่ทำงานเป็นกลไกสำคัญในการส่งผ่านข้อมูลไปยังเครือข่ายต่างๆ บนอินเตอร์เน็ต คือ โปรโตคอล IP (Internet Protocol) นอกจากนี้ในชั้น Internetwork Layer ยังมีโปรโตคอลที่ทำงานอยู่ด้วยอีก 2 ชนิด คือ โปรโตคอล Internet Control Message Protocol (ICMP) และโปรโตคอล Address Resolution Protocol (ARP)

โปรโตคอล IP (Internet Protocol)

โปรโตคอล IP นี้ทำหน้าที่บริการส่งผ่านข้อมูลที่มาจาก Host-to-Host Layer เพื่อส่งเข้าไปยังเครือข่ายใดๆ ได้อย่างถูกต้อง แม้ว่าจะมีเครือข่ายเชื่อมต่ออยู่ในอินเตอร์เน็ตเป็นล้านๆ เครือข่ายก็ตาม เนื่องจากโปรโตคอล IP มีข้อมูลตำแหน่ง IP ปลายทางที่จะส่งข้อมูลไปให้โดยทำงานกับอุปกรณ์ Router เพื่อส่งข้อมูลข้ามเครือข่ายออกไปได้ ตัวโปรโตคอล IP จะทำงานแบบ Packet Switching คือ มีการส่งผ่านข้อมูลสวิทช์ (Switch) ไปยังปลายทาง โดยข้อมูลจะเดินทางไปยังเครือข่ายต่างๆ ผ่านสวิทช์นี้ไปเรื่อยๆ จนกว่าจะถึงปลายทาง ตัววงจรผ่านหรือสวิทช์นี้เป็น Gateway หรือ Router ในระบบเครือข่ายก็ได้ ซึ่งในข้อมูลของโปรโตคอล IP จะมีข้อมูลของหมายเลข IP ปลายทางที่จะส่งข้อมูลไปให้และเมื่อถึงเครือข่ายปลายทางแล้วจะมีกลไกแปลงหมายเลข IP ให้เป็นหมายเลขฮาร์ดแวร์ประจำเครื่องที่ถูกต้องอีกทีหนึ่งด้วยโปรโตคอล ARP

กลไกของโปรโตคอล IP

ในการส่งผ่านข้อมูลหรือ IP datagram ไปยังเครือข่ายอินเตอร์เน็ตนั้น โปรโตคอล IP จะทำหน้าที่พิจารณาว่าปลายทางในการส่ง IP datagram นั้นเป็นภายในเครือข่ายตนเองหรือจะต้องส่งข้อมูลข้ามเครือข่ายไปอีก โดยการพิจารณานี้โปรโตคอล IP Address ปลายทางว่าส่วนที่เป็นค่าหมายเลขเครือข่าย (network address) จะเหมือนกับค่าเลขหมายเครือข่าย IP Address ต้นทางหรือไม่ ถ้าค่าตรงกันแสดงว่าการส่งข้อมูลภายในเครือข่ายเดียวกัน แต่ถ้าค่าต่างกัน แสดงว่าต้องส่งข้อมูลไปยังปลายทางที่อยู่คนละเครือข่ายกัน

การส่งข้อมูลภายในเครือข่ายเดียวกันมีกลไก ดังนี้

1. โปรโตคอล IP จะเรียกใช้บริการโปรโตคอล ARP (Address Resolution Protocol) เพื่อแปลงหมายเลข IP ปลายทางให้เป็นค่าหมายเลขฮาร์ดแวร์ เช่น MAC Address
2. เมื่อโปรโตคอล IP ได้รับค่าหมายเลขฮาร์ดแวร์แล้วก็จะส่งข้อมูลไปยังฮาร์ดแวร์ที่ระบุไว้

การส่งข้อมูลข้ามเครือข่ายมีกลไก ดังนี้

1. โปรโตคอล IP ตรวจสอบพบว่าหมายเลข IP Address ที่ปลายทางอยู่คนละเครือข่ายโดยโปรโตคอล IP จะอ่าน IP Address ของ Router เพื่อเตรียมส่งข้อมูลไปที่ Router แทนซึ่งในที่นี้จะมีการกำหนดเป็น default router
2. โปรโตคอล IP จะเรียกใช้บริการโปรโตคอล ARP เพื่อแปลงค่า IP Address ของ Router ให้เป็นค่าหมายเลขฮาร์ดแวร์
3. โปรโตคอล IP ส่งข้อมูล IP datagram ไปยัง Router ส่งข้อมูลข้ามเครือข่ายไปตามขั้นตอน

IP Datagram

IP Datagram ประกอบด้วย IP Header และ IP Payload

IP Header	IP Payload

-IP Header เป็นขนาดที่เปลี่ยนแปลงได้ระหว่าง 20 และ 60 ไบต์ ในการเพิ่มขึ้น 4 ไบต์ มันจะจัดเตรียมการสนับสนุน routing, การแสดงตัว payload, การชี้ให้เห็นถึงขนาด IP Header และ Datagram, การสนับสนุน fragmentation โดยมีโครงสร้างดังรูปที่ 14

Vision	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

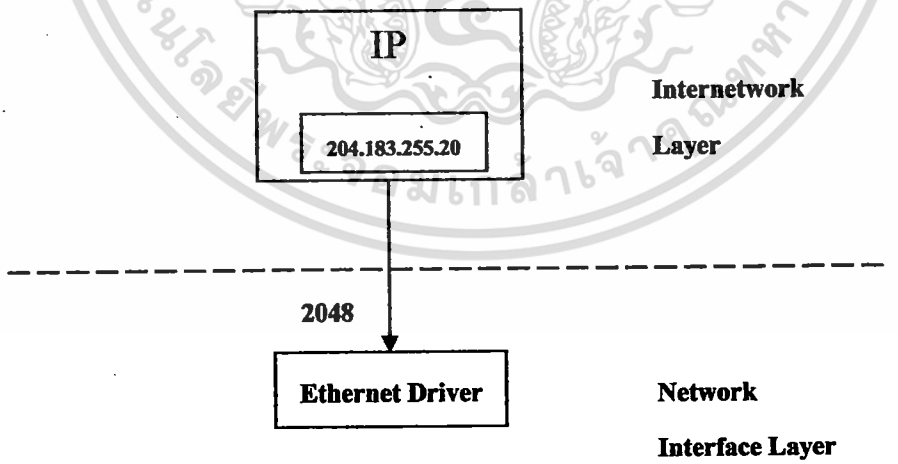
รูปที่ 2.27 แสดงโครงสร้าง IP Header

กำหนดการ IP address ให้กับอุปกรณ์

ต้องกำหนดหมายเลข IP address ให้กับจุดเชื่อมต่อเข้ากับเครือข่ายทุกจุด จุดเชื่อมต่อหรือ Interface อาจจะหมายถึง Network Interface Card (LAN การ์ด) ที่ติดตั้งในเซิร์ฟเวอร์หรือ WAN port, Ethernet port ที่ Router ใช้เชื่อมต่อเข้ากับเครือข่าย เป็นต้น การกำหนดหมายเลข IP address ให้กับจุดเชื่อมต่อนี้ทำให้เราเข้าใจได้ว่า ในบางอุปกรณ์ที่มีจุดเชื่อมต่อเข้ากับเครือข่ายมากกว่าหนึ่งจุดต้องกำหนดหมายเลข IP address ให้ครบ

การ Bind IP address

เมื่อได้กำหนดหมายเลข IP address ให้กับจุดเชื่อมต่อเช่น LAN card แล้วที่เครื่องเซิร์ฟเวอร์จะต้องมีการ bind หรือผนวกค่า IP address ดังกล่าวเท่ากับ Ethernet driver เพื่ออ้างอิงหมายเลข IP กับฮาร์ดแวร์ให้ทำหน้าที่ติดต่อส่งข้อมูลในระดับ Network Interface ได้ต่อไป ดังตัวอย่างรูปที่ 15



รูปที่ 2.28 แสดงการ Bind IP address

จากรูปที่ 15 จะแสดงค่า bind IP address 204.183.255.20 เข้ากับ Ethernet driver โปรโตคอล IP จะให้ค่า IP address นี้ในการติดต่อกันและผ่านฮาร์ดแวร์ที่ถูก bind ไว้อีกต่อหนึ่งค่าหมายเลขฮาร์ดแวร์ ได้แก่ MAC address ที่มีประจำอยู่บน LAN card ซึ่งจะไม่ได้ใช้งานอ้างอิงโดยตรงแต่จะผ่านหมายเลข IP address แทน

- **IP Payload** เป็นขนาดที่เปลี่ยนแปลงโดยมีลำดับจาก 8 ไบต์ (68 ไบต์ IP Datagram กับ 60 ไบต์ IP Header) ถึง 65,535 ไบต์ (65,535 ไบต์ IP Datagram กับ 20 ไบต์ IP Header)

Protocol

Protocol Field มีขนาดยาว 1 ไบต์และใช้เป็นตัวบ่งบอกในการบรรจุข้อมูลไปยัง Layer ที่สูงขึ้นกับใน IP Payload และยังเป็นตัวบ่งบอกลูกข่ายโปรโตคอลที่ชัดเจน โดยปกติค่าของ IP Protocol Field จะเป็น 1 สำหรับ ICMP6 สำหรับ TCP และ 17 (0×11) สำหรับ UDP Protocol field จะแสดงตัวได้อย่างมากมาย ดังนั้น payload สามารถที่จะผ่านไปยัง Layer ที่สูงขึ้นไปได้ถูกต้องโดยจะได้รับที่ destination

โปรโตคอล ICMP (Internet Control Message Protocol)

หน้าที่หลักของโปรโตคอล ICMP (Internet Control Message Protocol) คือการแจ้ง หรือแสดงข้อความจากระบบเพื่อบอกให้ผู้ใช้ทราบว่าเกิดอะไรขึ้นในการส่งผ่านข้อมูลนั้น ซึ่งปัญหาส่วนมากที่พบคือส่งไปไม่ได้หรือปลายทางรับข้อมูลไม่ได้ เป็นต้น นอกจากนี้ โปรโตคอล ICMP ยังถูกเรียกใช้งานจากเครื่อง Server และ Router อีกด้วย เพื่อแลกเปลี่ยนข้อมูลที่ใช้ควบคุม ส่วนรูปแบบการทำงานของโปรโตคอล ICMP นั้นจะทำควบคู่กับโปรโตคอล IP ในระบบเดียวกันและข้อความที่แจ้งให้ทราบจะถูกผนึกอยู่ภายในข้อมูล IP (IP datagram)

ข้อความที่โปรโตคอล ICMP ส่งนั้น แบ่งออกได้เป็น 2 แบบ คือ ICMP Error Message หรือข้อความแจ้งข้อความผิดพลาดและ ICMP Query หรือข้อความเรียกขอข้อมูลเพิ่ม ตัวอย่างกลไกการทำงานของโปรโตคอล ICMP เช่น เมื่อมีการส่งผ่านข้อมูลจากผู้ใช้ไปยังปลายทางที่ไม่ถูกต้อง หรือขณะนั้นเครื่องปลายทางเกิดปัญหาจนไม่สามารถรับข้อมูลได้ที่ Router จะส่งข้อความแจ้งเตือนเป็น ICMP Message ที่ชื่อ Destination Unreachable ให้กับผู้ส่งข้อมูลนั้น นอกจากนี้ตัวข้อมูลที่แจ้งข้อความ ก็จะมีส่วนของข้อมูล IP datagram ที่เกิดปัญหาด้วย ดังนั้น เมื่อผู้ส่งข้อมูลได้รับข้อความแจ้งแล้วก็จะทราบได้ว่า จุดที่เกิดปัญหานั้นอยู่ที่ใด ดังนั้นโปรโตคอล ICMP จึงกลายมาเป็นเครื่องมืออย่างใดอย่างหนึ่งในการช่วยทดสอบเครือข่าย เช่น คำสั่ง Ping ที่เรามักใช้ทดสอบว่าเครื่อง Server ที่ให้บริการหรืออุปกรณ์ที่ต่ออยู่ในเครือข่ายอินเตอร์เน็ตนั้นยังทำงานเป็นปกติหรือไม่ แล้วคำสั่ง Ping มีการเรียกใช้งานโปรโตคอล ICMP แจ้งเป็นข้อความให้ทราบอีกด้วยต่อหนึ่ง

ตารางที่ 2.5 ค่าต่างๆ ของ IP Protocol Field

Value	Protocol
0	Reserved
1	Internet Control Message Protocol (ICMP)
2	Internet Group Management Protocol (IGMP)
4	IP and IP encapsulation
6	Transmission Control Protocol (TCP)
8	Exterior Gateway Protocol (EGP)
17	User Datagram Protocol (UDP)
46	Resource Reservation Protocol (RSVP)

47	Generic Routing Protocol (GRE)
50	IP Security Encapsulation Security Payload (ESP)
51	IP Security Authentication Header (AH)
89	Open Shortest Path First (OSPF)

โปรโตคอล ARP (Addressable Resolution Protocol)

โปรโตคอล ARP ถูกเรียกใช้งานโดยโปรโตคอล IP เพื่อช่วยแปลหมายเลข IP ไปเป็นหมายเลขฮาร์ดแวร์ปลายทาง ตัวอย่างเช่น เว็บเซิร์ฟเวอร์เครื่องหนึ่งเชื่อมต่ออยู่ในเครือข่ายอินเตอร์เน็ตและในการเชื่อมต่อนี้ต้องอาศัย LAN card ที่ติดตั้งอยู่นี่เอง จะมีหมายเลขเฉพาะประจำฮาร์ดแวร์ที่ไม่ซ้ำใครเพื่อใช้อ้างอิงการส่งข้อมูลในเครือข่าย แต่มาใช้งานโปรโตคอล TCP/IP ก็ต้องมีการกำหนดหมายเลข IP Address ประจำตัวเพื่อใช้อ้างอิงกัน และโปรโตคอล ARP จะทำหน้าที่แปลงค่าหมายเลข IP ให้เป็นหมายเลขฮาร์ดแวร์จริงให้ในระดับการทำงานที่ Internetwork Layer นี้ ซึ่งกลไกการแปลงนี้เรียกว่า Address Resolution

โปรโตคอล ARP ย้อนกลับ หรือ RARP (Reserve Addressable Protocol)

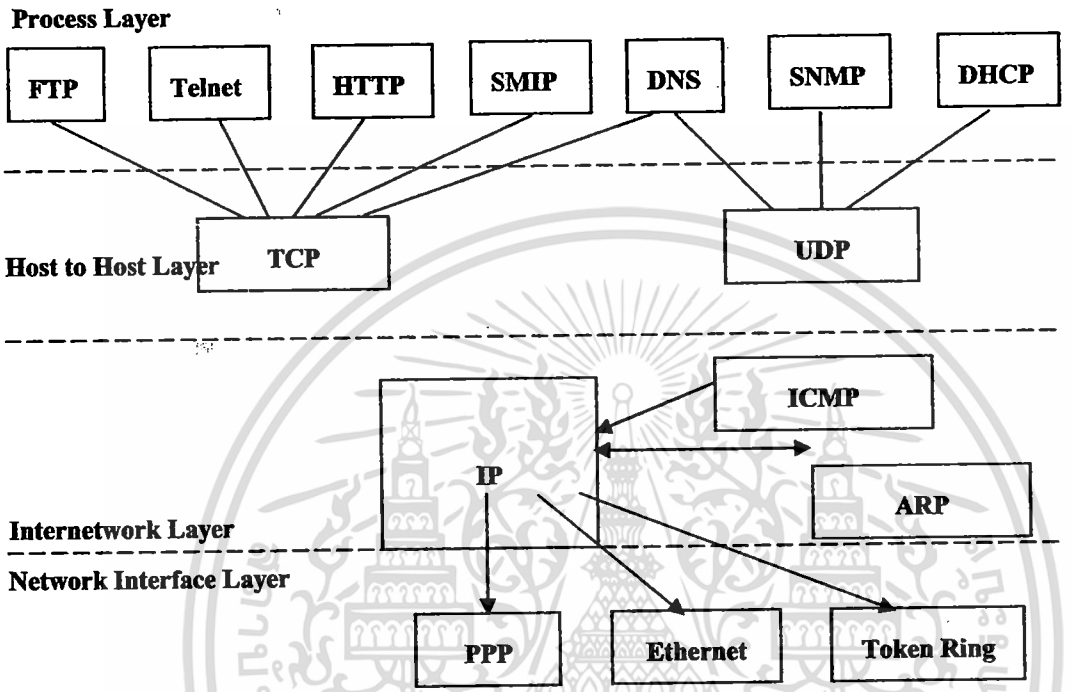
วิธีการ ARP ช่วยแก้ปัญหาในการค้นหาที่อยู่ของข้อมูลที่ใช้ในการกำหนดที่อยู่ฮาร์ดแวร์แบบ IP แต่ถ้าทราบที่อยู่แบบฮาร์แวร์แล้วต้องการแปลงที่อยู่เป็น IP จะทำอย่างไร ปัญหานี้มักเกิดขึ้นกับเครื่อง Computer ที่เริ่มทำงานด้วยการอ่านข้อมูลทั้งหมดจากเครื่อง Host เครื่องประเภทนี้จะทราบเพียงที่อยู่ของตนเองจากอุปกรณ์สื่อสารเครือข่ายเท่านั้น การค้นหาคำตอบสามารถทำได้โดยวิธีควบคุมการสื่อสารแบบ ARP ย้อนกลับหรือ RARP (Reserve Addressable Protocol) วิธีการนี้ Computer ที่เพิ่งจะเริ่มทำงาน (หรือเครื่องใดก็แล้วแต่) จะส่งคำถามออกไปในทำนอง "ที่อยู่ขนาด 48 Bits แบบฮาร์ดแวร์ของฉัน คือ 14.04.05.18.01.25 มีใครทราบที่อยู่ IP ของฉันบ้าง" เครื่องที่ให้บริการ RARP จะถูกตรวจดูข้อมูลในตารางข้อมูลของตนเองแล้วจึงส่งหมายเลข IP กลับไปให้ วิธีการนี้ช่วยให้เกิดความอ่อนตัวหรือเพิ่มประสิทธิภาพในการใช้หมายเลข IP เนื่องจากผู้ใช้ไม่มีหมายเลข IP เป็นของตัวเอง ผู้ควบคุมระบบสามารถกำหนดหมายเลข IP ที่ไม่มีผู้ใช้งานในขณะนั้นให้ใช้ได้ หมายเลข IP ในที่นี้จึงเป็นเสมือนสมบัติส่วนกลางที่ทุกคนใช้ร่วมกัน

ข้อด้อยของวิธี RARP คือ การที่ผู้ใช้จะส่งคำถามโดยใช้หมายเลข 1 จำนวน 48 ตัว เป็นที่อยู่ของผู้ให้บริการหมายเลขนี้เป็นหมายเลขพิเศษที่ Router จะไม่ยอมส่ง Packet ผ่านไปยังเครือข่ายอื่นเลย ฉะนั้นผู้ให้บริการ RARP จะต้องมีอยู่ประจำทุกเครือข่าย อย่างไรก็ตาม Protocol แบบ BOOTP ได้รับการพัฒนาขึ้นมาเพื่อแก้ปัญหานี้โดยการใช้ Packet UDP แทน Packet ชนิดนี้ สามารถส่งไปได้ทั่วทุกเครือข่ายและยังให้ข้อมูลอื่นเพิ่มเติม เช่น หมายเลข IP ของผู้ให้บริการแฟ้มข้อมูล หมายเลข IP ของ Router อัตโนมัติและตารางข้อมูลเครือข่ายย่อย เป็นต้น

Network Interface Layer

เนื่องจากในด้านกายภาพของเครือข่ายนั้น มีหลายวิธีการและหลายรูปแบบในการเชื่อมต่อระบบให้เป็นเครือข่าย แต่อย่างไรก็ตามในเครือข่ายอินเตอร์เน็ตนี้ ข้อมูลใน IP datagram จะถูกถ่ายทอดและส่งผ่านไปยังปลายทางโดนไม่คำนึงถึงรูปแบบการเชื่อมต่อทางกายภาพไม่ว่าจะเป็นการใช้เครือข่ายใยแก้วนำแสงหรือเครือข่ายสาย Unshielded Twist Pair (UDP) เชื่อมต่อเป็นแบบเครือข่าย Ethernet ธรรมดาหรือเครือข่าย Token

ring, ATM, ISDN ฯลฯ ก็ตาม การทำงานระดับล่างสุดต่อจาก Internetwork Layer จะเป็นการแปลงข้อมูล IP datagram ให้อยู่ในรูปที่เหมาะสมปละแปลงสัญญาณไฟฟ้าส่งไปยังเครือข่ายต่อไป ซึ่งในชั้น Network Interface Layer นี้เมื่อเทียบกับมาตรฐาน OSI Model แล้วจะเป็นการรวม 2 layer เข้าด้วยกันคือ Data link layer และ Physical layer กล่าวโดยสรุป คือ การทำงานในชั้นต่างๆ ตามโครงสร้างโปรโตคอล TCP/IP จะมีลักษณะดังรูปที่ 16



รูปที่ 2.29 โครงสร้างของโปรโตคอล TCP/IP

ในแต่ละชั้นหรือ layer จะมีโปรโตคอลหลักทำหน้าที่ต่างๆ และส่งข้อมูลไปยังเครือข่ายและออกสู่อินเตอร์เน็ต

MAC Address

เนื่องจากคอมพิวเตอร์แต่ละเครื่องสามารถแลกเปลี่ยนข้อมูลกันได้ในระบบเครือข่ายเดียวกัน ดังนั้นแต่ละเครื่องควรมีสิ่งที่ชี้ลักษณะเฉพาะตัวของมัน เช่น เราต้องมีบัตรประจำตัวประชาชน ซึ่งในทางคอมพิวเตอร์นี้เราจะใช้เลขฐาน 16 จำนวน 12 digits เป็นตัวบ่งชี้ลักษณะเฉพาะ ซึ่งเราเรียกว่า MAC Address เนื่องจาก MAC Address เป็นตัวบ่งชี้ลักษณะเฉพาะของแต่ละเครื่อง ดังนั้นจึงต้องเป็นค่าที่ไม่ซ้ำกัน (unique) MAC Address เป็นเลข 48 digits โดยแบ่งออกเป็น 2 ส่วน โดย 24 bits แรกเป็นค่าที่แสดงถึงบริษัทที่ผลิตการ์ด ส่วน 24 bits หลังเป็น serial number ที่ทางบริษัทกำหนดให้ ซึ่งแต่ละตัวต้องไม่ซ้ำกัน เราเรียก 24 bit นี้ว่า OUI (Organization Unique Identifier) ซึ่ง OUI จะใช้เพียง 22 bits เท่านั้น ส่วนอีก 2 bits ที่เหลือจะถูกใช้เพื่อวัตถุประสงค์อื่น โดย bit หนึ่งจะใช้เพื่อแสดงว่า address นั้นเป็น broadcast/multicast address ส่วนอีก bit หนึ่งนั้นไว้แสดงว่า adapter นั้นถูกกำหนด locally administered address ซึ่ง admin ของระบบจะทำการกำหนด MAC Address เพื่อความเหมาะสมของนโยบายระบบ เช่น MAC Address = 03 00 00 00 00 00 01 ซึ่งจะเห็นว่า

byte แรก = 03 = 00000011 นั่นคือ ทั้ง 2 bits ถูก set (reset = 0) ซึ่งเอาไว้กรณี multicast ให้ทุกเครื่องที่ run บนโปรโตคอล NetBEUI

กล่าวโดยสรุป คือ โปรโตคอล TCP/IP ทำงานโดยแบ่งชั้นเทียบกัน OSI Model ได้กลไกในการทำงานของโปรโตคอล TCP/IP มี 4 ชั้น ซึ่งในชั้นแรก คือ Process layer ทำหน้าที่ติดต่อกับแอพพลิเคชันและโปรโตคอลที่แอพพลิเคชันนั้นๆ ใช้งานและส่งมาให้ชั้น Host-to-Host Layer เพื่อติดต่อกันระหว่างเครื่องเซิร์ฟเวอร์ให้บริการกับเครื่องผู้ขอใช้บริการ ในชั้นนี้จะมีการสร้าง Session หรือการเชื่อมต่อระหว่างระบบขึ้นตามแต่ละโปรโตคอลที่ต้องการ ต่อมาเป็นการผนึกข้อมูลไปเป็น IP datagram ที่ชั้น Internetwork Layer โดยอาศัยโปรโตคอล IP เพื่อให้สามารถติดต่อข้อมูลข้ามเครือข่ายและเครื่องที่ถูกต้องได้ และสุดท้ายการส่งข้อมูลออกสู่โลกภายนอกต้องอาศัยกลไกในชั้น Network Interface Layer เพื่อแปลงข้อมูลใหม่ให้เป็นสัญญาณไฟฟ้าส่งออกไปเครือข่ายและอาจจะออกไปยัง Gateway หรือ Router เพื่อข้ามเครือข่ายออกไปยังเส้นทางที่กำหนดไว้ในอินเตอร์เน็ตโปรโตคอล ในแต่ละโปรโตคอลเหล่านี้ก็จะรับผิดชอบหน้าที่ของตนเพื่อผ่านข้อมูลลงไปยังระดับล่างและออกสู่เครือข่ายอินเตอร์เน็ตในที่สุด

2.3 MANET Applications

เนื่องจากว่า ad hoc network เป็นเครือข่ายที่ค่อนข้างที่จะมีความยืดหยุ่นสามารถที่จะ set up ได้จากทุกที่และทุกเวลาโดยปราศจากโครงสร้างพื้นฐานที่จำเป็นสำหรับการพัฒนา รวมทั้งการ configure ก่อน และการบริหารจัดการ ผู้คนที่เข้าใจถึงศักยภาพในการติดต่อและข้อดีของ mobile ad hoc network จึงเริ่มให้ความสนใจในเทคโนโลยีนี้ ต่อไปเราจะศึกษาในส่วนของการประยุกต์ใช้ mobile ad hoc network ว่ามีการเปลี่ยนแปลงในอดีตอย่างไร และในอนาคตจะมีการเปลี่ยนแปลงอย่างไร

ในอดีต mobile ad hoc network มีความสำคัญอย่างยิ่งในการแก้ปัญหาการติดต่อสื่อสารกันในสมรภูมิธรรมชาติที่มีการเปลี่ยนแปลงแปลงอยู่ตลอดเวลาของการปฏิบัติการทางทหารนั้นมันทำให้ความน่าเชื่อถือในการติดต่อสื่อสารระหว่างฐานที่มั่นคงกับกลางสมรภูมิที่มีการคาดไว้ล่วงหน้าเปลี่ยนแปลงไป เนื่องจากว่าการติดต่อแบบไร้สายนั้นมีข้อจำกัดโดยสัญญาณวิทยุ(radio) จะมีปัญหาคลื่นรบกวน ซึ่ง mobile ad hoc network จำเข้ามาแก้ปัญหาในจุดนี้ได้

สำหรับยุคเริ่มต้น mobile ad hoc network สามารถเดินตามเส้นทางกลับไปยัง DARPA Packet Radio Network (PRNet) ที่มีการวางแผนไว้ ใน ค.ศ.1972 และนี่ถูกกระตุ้นโดยประสิทธิภาพของเทคโนโลยี packet switching ดังเช่น การแชร์แบนวิธ และ store-and-forward routing ในค.ศ. 1983 Survivable Radio Network (SURANs) ถูกพัฒนามาจาก DARPA โดยมีวัตถุประสงค์หลักคือพยายามที่จะพัฒนา network algorithms ให้รองรับเครือข่ายที่มีถึง 10,000 node , ป้องการการถูกโจมตี, ราคาถูก , ลดกำลังส่งสัญญาณวิทยุ ในช่วงปลายทศวรรษ 1980 ถึงต้นทศวรรษ 1990 ความเจริญเติบโตทางด้าน อินเทอร์เน็ตและไมโครคอมพิวเตอร์เพิ่มมากขึ้นทำให้ปัจจัยในการลงมือเริ่มต้นทำโครงการ initial packet radio network เริ่มมีความเป็นไปได้ ที่ U.S. Department of Defense initiated the DARPA Global Mobile (GloMo) ได้จัดทำขึ้นโดยมีวัตถุประสงค์ที่จะรองรับ Ethernet-Type multimedia connectivity ให้ได้ทุกที่ทุกเวลาระหว่างอุปกรณ์ในเครือข่ายด้วยกันหลากหลายการออกแบบถูกค้นพบ ยกตัวอย่างเช่น Wireless Internet Gateway (WINGs) ที่ใช้หลักการ flat peer-to-peer network และ Multimedia Mobile Wireless Network (MMWN) ที่ใช้เทคนิคการ cluster

แม้ว่าในช่วงเริ่มต้นการประยุกต์ใช้และการขยายงานของ MANET ส่วนใหญ่แล้วจะถูกใช้ทางทหาร แต่ต่อมาก็ถูกนำมาใช้กันภายนอกจนกระทั่งกลายมาเป็นสิ่งที่ควรจับตามองในปัจจุบัน โดยเฉพาะอย่างยิ่งในช่วง 2-3 ปีที่ผ่านมาการเจริญเติบโตอย่างรวดเร็วของงานวิจัย mobile ad hoc network ทำให้กลายมาเป็นสิ่งที่น่าสนใจและถูกนำมาใช้ในภาคธุรกิจ ยกตัวอย่างเทคโนโลยีใหม่ๆที่ได้จากการประยุกต์ใช้ mobile ad hoc network ที่นอกเหนือมาจากงานทหาร ได้แก่ Buletooth, IEEE.802.11, ZigBee เป็นต้น

2.4 ZigBee

ZIGBEE เป็นเทคโนโลยีไร้สายที่ร่วมกันสื่อสารข้อมูลผ่านเซ็นเซอร์ขนาดเล็ก จำนวนเป็นพันๆ หมื่นๆ ชิ้นที่ฝังอยู่ตามส่วนต่างๆ ในอาคาร สำนักงาน โรงงาน หรือแม้แต่ในบ้าน ชื่อ ZIGBEE ได้มาจากพฤติกรรมการสื่อสารของผึ้ง โดยผึ้งจะบินแบบซิกแซ็ก และจำให้ข้อมูลข่าวสารระหว่างผึ้งด้วยกัน ที่เกี่ยวกับตำแหน่ง ระยะทาง และทิศทางของอาหารที่พวกมันกำลังหาอยู่ ZIGBEE ถูกสร้างขึ้นในการทำระบบเครือข่ายไร้สายส่วนบุคคล (Wireless personnal Area networks ;WPANs) มีทั้งความเร็วในการรับส่งข้อมูลสูง IEEE ได้วิจัยและพัฒนาออกมามี2 มาตราฐาน คือ มาตราฐาน IEEE 802.15.3a สำหรับ WPAN ความเร็วสูง และอีกมาตราฐานหนึ่งที่เราใช้คือ มาตรฐาน IEEE 802.15.4 โดยมาตรฐานนี้ใช้งานสำหรับการสื่อสารความเร็วต่ำซึ่งนิยมใช้กันเนื่องจากมีราคาถูก ขนาดเล็ก และมีช่วงการใช้งานจากแบตเตอรี่ หลายเดือนหรือหลายปีและมีความซับซ้อนน้อยมากการทำงานของ ZIGBEE จะเป็นการรับ-ส่งคลื่นสัญญาณข้อมูล ผ่านชิปเล็กจิ๋วนี้จุดต่อจุดไปเรื่อยๆ จนถึงปลายทางที่ต้องการดาวน์โหลดข้อมูลลงในเครื่องคอมพิวเตอร์เพื่อใช้ในการวิเคราะห์ข้อมูล ข้อมูลที่ได้อาจจะเป็นการวัดอุณหภูมิ การเคลื่อนไหวของสิ่งมีชีวิต จับปริมาณมลพิษในอากาศ ปริมาณน้ำ ท่อแก๊ส โดยใช้พลังงานแสงอาทิตย์หรือแบตเตอรี่ขนาดเล็กที่กินไฟน้อยมาก

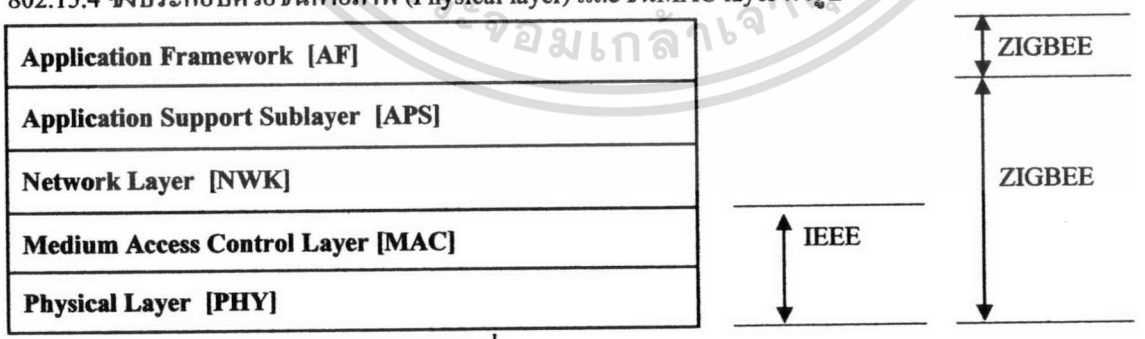
สำหรับมาตราฐาน IEEE 802.15.4 จะใช้ได้กับมาตราฐานการสื่อสารไร้สายอื่นๆ เช่น Wi-Fi และ UWB (Ultra Wideband) อย่างไรก็ตามมาตราฐาน IEEE 802.15.4 จะแตกต่างจากมาตราฐานอื่น ที่คุณลักษณะต่างๆ คือ การรับส่งข้อมูลเทคโนโลยีเครือข่ายความเร็วต่ำ ใช้กำลังไฟฟ้าน้อย อุปกรณ์ราคาถูก นอกจากนี้ยังสามารถประยุกต์ใช้กับอ0E38กรณ์พื้นฐานที่หลากหลายในชีวิตประจำวัน หากนำมาตราฐานเครือข่ายไร้สาย IEEE 802.15.4 มาประยุกต์ใช้งานโดยเป็นการสื่อสารระหว่างอุปกรณ์กับอุปกรณ์ หรือ อุปกรณ์กับมนุษย์ ที่ผ่านระบบเครือข่ายไร้สาย เช่นระบบการควบคุมอัตโนมัติที่บ้าน (Remote Control) ,ระบบการติดตามสำหรับรักษาความปลอดภัย สำหรับมาตราฐาน IEEE 802.15.4 ถูกกำหนดไว้ในชั้นของ Physical Layer และ Medium Access Control ที่มีการสื่อสาร ที่มีการสื่อสารด้วยอัตราข้อมูลต่ำ ส่วนโครงสร้างของโครงข่าย (Topology) ที่รองรับนั้นจะมี 2 แบบ คือ One-hop star เมื่อรัศมีการสื่อสารน้อยกว่า 10 เมตร และ multi-hop สำหรับโครงข่าย peer-to-peer ทั้งนี้อุปกรณ์แต่ละตัวจะมีแอดเดรสของตัวเอง

ลักษณะของ ZIGBEE คือมีการเข้าช่องสัญญาณโดยการใช้ Carrier Sense Multiple Accesswith Collision Avoidance (CSMA – CA) หรือมีทางเข้าช่องสัญญาณหลายๆ ทางเพื่อหลีกเลี่ยงการชนกันระยะทางโดยทั่วไปประมาณ 50 เมตร มี topology แบบ star , peer-to-peer , mesh5

รูปที่ 2.30 ZIGBEE

2.4.1 มาตรฐานโปรโตคอล ZIGBEE

โปรโตคอลแสตค IEEE 802.15.4 ซึ่งถูกออกแบบมาสำหรับเครื่อข่ายแบบ Low – Rate Wireless Private Area Networks (LR - WPAN) ตัวรับรู้เป็นอุปกรณ์เชื่อมต่อทำให้เครื่องคอมพิวเตอร์ที่เราใช้งานกันในปัจจุบัน สามารถรับรู้ที่เกี่ยวกับสภาพแวดล้อมของโลกเราโดยตัวรับรู้มีหลายชนิดตามการใช้งานดังนี้ เช่น ตัววัดอุณหภูมิ ความชื้น การเคลื่อนไหวของวัตถุและตัวรับรู้ก็ได้มีการพัฒนาให้มีขีดความสามารถสูงขึ้นเรื่อยๆ จากระบบวัดคุมส่วนใหญ่จะเป็นแบบจุดต่อจุดไม่มีการสื่อสารระหว่างกัน จึงเป็นข้อจำกัด ดังนั้น ZIGBEE Alliance เป็นสมาคมบริษัทที่ทำงานร่วมกันเพื่อสร้างผลิตภัณฑ์ด้านการควบคุมและสังเกตที่มีการเชื่อมต่อบนเครือข่ายไร้สายที่เชื่อถือได้ คุ้มค่า ใช้ไฟต่ำ ซึ่งทำงานบนมาตรฐานโลกแบบเปิด โดย ZIGBEE Alliance เป็นกลุ่มอุตสาหกรรมที่ไม่แสวงผลกำไรและมีการเติบโตอย่างรวดเร็ว ซึ่งประกอบด้วยกลุ่มผู้ผลิตเซมิคอนดักเตอร์ระดับชั้นนำ ผู้ให้บริการเทคโนโลยี OEM (Original Equipment Manufacturing) และผู้ใช้โดยตรงทั่วโลก การสมัครสมาชิกเปิดกว้างสำหรับทุกหน่วยงาน เครื่อข่ายตัวรับรู้ Zigbee ถูกออกแบบภายใต้มาตรฐาน IEEE 802.15.4 ซึ่งประกอบด้วยชั้นกายภาพ (Physical layer) และชั้นMAC layer ดังรูป

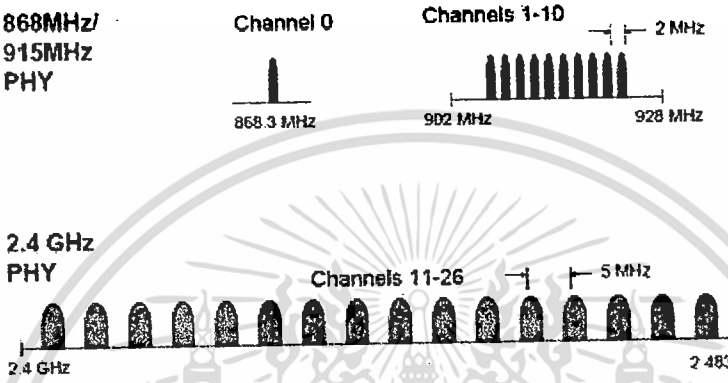


รูปที่ 2.31 ZIGBEE Protocol

ชั้น Physical Layer ของมาตราฐาน IEEE 802.15.4 ของ ZIGBEE ได้แบ่งย่านความถี่ออกเป็น 3 ย่าน คือ 2.4 GHz 898 MHz 915 MHzดังรูป ย่านความถี่ใช้งานได้ทั่วโลก ISM 2.4 GHz จะมีช่องสัญญาณทั้งหมด 16 ช่อง ช่องที่อัตราเร็วของข้อมูล 250 kb/s คลื่นวิทยุที่ใช้อยู่ในย่านความถี่ ISM (Industrial Scientific and Medical) ซึ่ง

เป็นย่านความถี่ที่อนุญาตให้ใช้ต่างกัน สำหรับประเทศไทย กระทรวงเทคโนโลยีสารสนเทศอนุญาตให้ใช้โดยไม่ต้องขอย่านความถี่ใช้ในอเมริกาและออสเตรเลีย

สำหรับความถี่ 868 MHz มี 1 ช่องสัญญาณสื่อสาร ด้วยอัตราข้อมูล 40 kb/s และสำหรับความถี่ 915 MHz จำนวน 10 ช่อง สัญญาณสื่อสาร อัตรารับส่งข้อมูล 20 kb/s สำหรับชั้น network/security และชั้น application framework จะอยู่บนพื้นฐานของระบบ IEEE 802.15.4 ซึ่งในชั้น network นี้สามารถรองรับได้ 3 แบบ คือ star , mesh และ Cluster tree



รูปที่ 2.32 ความถี่มาตราฐานของ ZIGBEE

จำนวนช่องของย่านความถี่ 868 MHz มี 1 ช่องคือช่องหมายเลข 0 ช่องหมายเลข 1 ถึง 10 ย่านความถี่ 915 MHz และ ช่องหมายเลข 11 ถึง 26 ย่านความถี่ 2.4 GHz อัตรการรับส่งข้อมูลที่กล่าวไปแล้วนั้นเป็นเชิงอุดมคติ การใช้งานจริงจะสูญเสียไปกับโปรโตคอลของระบบเครือข่ายค่าจริงจึงมีค่าต่ำกว่า IEEE 802.15.4 และมีความยาวของแพคเกท 127 ไบท์ ประกอบด้วย header และ 16-bit checksum(CRC), play load มีได้ถึง 104 byte บางช่องสัญญาณถูกกำหนดช่วงติดต่อนั้นต้องเสร็จภายในเวลาเพื่อป้องกันปัญหาของการติดต่อกันภายในเครือข่ายอื่น IEEE 802.15.4 ได้ถูกออกแบบกลไกการตอบรับ (Acknowledgement) เพื่อส่งกลับถ้าต้องการอย่างไรก็ตามจะมีอยู่ในชั้นของ MAC Layer เท่านั้น ZIGBEE stack หรือ application จะคอยดูแลทุกข้อมูลซ้ำ เนื่องจาก ถ้าไม่ได้รับการตอบกลับในเวลาที่กำหนด หรือถ้าข้อมูลหายไปบางส่วน checksum ควบคุมและตรวจสอบว่าข้อมูลนั้นถูกต้องหรือไม่ สถาปัตยกรรมทางด้านฮาร์ดแวร์ Zigbee จะแบ่งออกเป็น 2 ชนิด ตารางที่ 2.5 คือ RFD(Reduce Function Device) และ FFD(Full Function Device) FFD มีฟังก์ชันการ ทำงานที่ครบถ้วนสามารถเป็น Coordinator ได้ แต่ RFD ถูกจำกัดเรื่องการกินพลังงานและต้องมีราคาถูกดังนั้นจึงถูกตัดฟังก์ชันที่ไม่จำเป็นออกเช่นการ Router เป็นต้น ส่วนโนดของ ZIGBEE แบบ Logical Device มี 3 ประเภท คือ ZIGBEE coordinators , ZIGBEE Routers และ ZIGBEE End Device โดย ZIGBEE coordinators ทำหน้าที่ initializes โครงข่ายจัดการโนดในโครงข่าย ส่วนของ ZIGBEE Routers ทำหน้าที่จัดการเส้นทางของข้อมูลที่ส่งผ่านภายในโครงข่ายระหว่างโนด และ โนดประเภท ZIGBEE End Device เป็นโนดที่อยู่ในส่วนของผู้ใช้งาน โดยสามารถเป็นได้ทั้งแบบ RFD และ FFD

ตารางแสดงหน้าที่ของZIGBEE ในเครือข่าย ZIGBEE จะกำหนดให้ FFD เป็น Coordinator ทำหน้าที่เป็น Adiminstrator ควบคุมและจัดการ เครื่อข่าย Coordinator จะมี Neighbor table ของ device ที่พบอยู่ในบริเวณใกล้เคียง ซึ่งเป็นสาเหตุ ทำให้ Coordinator จำเป็นต้องมีหน่วยความจำสูงและต้องใช้พลังงานสูง

เพราะจะต้องติดต่อกับลูก ข่ายตลอดเวลา โดยทั่วไปจะมีหน่วยความจำชั่วคราว 2 - 4 kB และมีหน่วยความจำของส่วนโปรแกรม FLASH ขยายได้ถึง 64 kB ปริมาณที่ใช้ในหน่วยความจำชั่วคราวขึ้นอยู่กับว่า Coordinator ต่ออยู่กับจำนวนโหนดมากหรือน้อยเพียงใด จากการประมาณจำนวนหน่วยความจำชั่วคราวขนาด 4 kB สามารถต่อ device ได้อย่างน้อย 30 ตัว

ตารางที่ 2.6 ตารางแสดงชนิดของ ZIGBEE

Device Type	Services Offered	Typical Power Source	Typical Receiver Configuration
Full Function Device (FFD)	Most or All	Mains (Power line)	On when Idle
Reduced Function Device (RFD)	Limited	Battery	Off when Idle

ตารางที่ 2.7 ตารางแสดง หน้าที่ของ ZIGBEE

ZIGBEE Protocol Device	IEEE Device Type	Typical Function
Coordina.tor	FED	One per network Forms the network ,allocates network addresses , hold binding table
Router	FED	Optional. Extends the physical range of the network. Allows more nodes to join the network. May also perform monitoring and/or control function
End	FFD or RED	Performs monitoring and/or control functions

Zigbee เมื่อเปรียบเทียบกับมาตรฐานระบบสื่อสารไร้สายต่างๆ แสดงในตารางที่ 2.7 จะเห็นได้ว่าเทคโนโลยีของ Bluetooth และ Wi – Fi นั้นกินพลังงานสูงมากจึงไม่เหมาะนำมาใช้งานกับเครือข่ายตัวรับรู้ ซึ่งอัตราการส่งข้อมูลไม่จำเป็นต้องเร็วมากนักเพราะว่าจะมีการเรียกข้อมูลเป็นคาบเวลา

ตารางที่ 2.8 การเปรียบเทียบในมาตรฐานเทคโนโลยีการสื่อสารไร้สาย

	ZIGBEE	**Bluetooth**	**Wi-Fi**	**TRW**
Standard	802.15.4	802.15.1	802.11b	
Memory requirements	4 – 32 kB	250 kB+	1 MB+	-
Battery life	Years	Days	hours	Month
Nodes per master	65,000 +	7	32	-
Data rate	250 kb/s	1 Mb/s	11 Mb/s	280m (250Kbps) 150m (1Mbps)

Range	300 m	10 m	100 m	150 – 280 m
Power output	0 dBm	18 dBm max	16 dBm	4 dBm+

2.4.2 การเชื่อมต่อพื้นฐานของระบบ IEEE 802.15.4

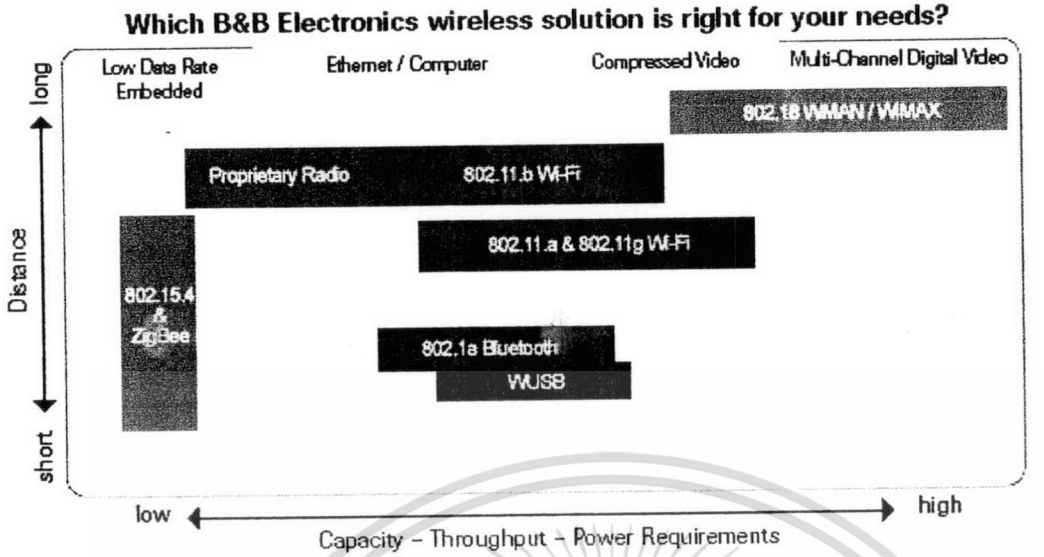
มาตรฐาน IEEE 802.15.4 เป็นมาตรฐานสำหรับเครือข่ายแบบไร้สายระยะใกล้ความเร็วต่ำหรือ low-rate WPAN (LR-WPAN) โดยมีคุณลักษณะ คือ อัตราการรับ-ส่งข้อมูล ต่ำกว่าหรือเท่ากับ 250 กิโลบิตต่อวินาที ใช้กำลังไฟฟ้าน้อย อุปกรณ์มีราคาถูก นอกจากนี้ยังสามารถประยุกต์ใช้กับอุปกรณ์พื้นฐานที่หลากหลายในชีวิตประจำวันและโดยมากการนำมาประยุกต์ใช้ของ WPAN มักจะเกี่ยวข้องกับ wireless sensor networks (WSNs)

IEEE 802.15.4 Physical Layer

ชั้นฟิสิคัลเลเยอร์มาตรฐาน IEEE 802.15.4 มีการใช้ 3 ความถี่ คือ 868/868.6 เมกะเฮิรตซ์ ใช้ดีเอสเอสเอส(DSSS: Direct-Sequence Spread Spectrum) โดยอัตราความเร็วของข้อมูล 20กิโลบิตต่อวินาที สำหรับความถี่ 902/928 เมกะเฮิรตซ์ ใช้DSS โดยอัตราความเร็วของข้อมูล 40 กิโลบิตต่อวินาทีและความถี่ 2.4 กิกะเฮิร์ต ใช้DSSSโดยอัตราเร็วของข้อมูล 250 กิโลบิตต่อวินาที สำหรับความถี่ 868 เมกะเฮิร์ต จะมี 1 ช่องสัญญาณสื่อสาร, 10 ช่องสัญญาณใน 915 เมกะเฮิร์ต และ16 ช่องสัญญาณ ใน 2.4 กิกะเฮิร์ต โดยย่านความถี่เหล่านี้ไม่ใช่ความถี่สากล โดย 868 เมกะเฮิรตซ์ ใช้ในยุโรป, 915 เมกะเฮิรตซ์ ใช้ในอเมริกา และ 2.4 กิกะเฮิรตซ์ถือว่าเป็นความถี่ที่ใช้กันมากที่สุดในโลก ดังตารางที่ 2.8

ตารางที่ 2.9 IEEE 802.15.4 frequency bands and data transfer rates

Band (เมกะเฮิรตซ์)	Frequency Band	Bit Rate (kbps)	Symbol Rate (kbps)	DSS Spreading Parameter	
				Modulation Technique	Chip Rate
868	868-868.6 เมกะเฮิรตซ์	20	20	BPSK	300 kcps
915	902-928 เมกะเฮิรตซ์	40	40	BPSK	600 kcps
2400	2400-2483.5 เมกะเฮิรตซ์	250	62.5	O-QPSK	2 mcps



รูปที่ 2.33 ปริมาณการใช้ทรูพุตของมาตราฐานการสื่อสารไร้สายแบบต่างๆ

คุณสมบัติทั่วไปของโมดูลไร้สายซิกบี Feature Summary ของ Xbee โดยรวมที่เหมือนกัน

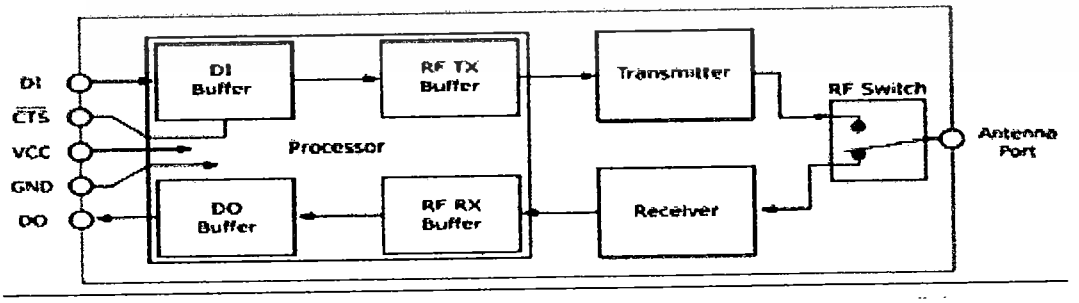
1. Operating Frequency ISM Band 2.4 Ghz (ISM Band หมายถึง ย่านความถี่ใช้งานเพื่อการวิจัย ซึ่งจะอนุญาตให้ใช้กับ อุตสาหกรรม (Industrial) วิทยาศาสตร์ (Scientific) และ ทางการแพทย์ (Medical) รวมเป็น ISM)
2. มีสายอากาศให้เลือกใช้หลายแบบ คือ แบบ Chip Ant , Whip Ant , UFL con , RPSMA con โดย 2 แบบหลัง เราต้องไปหาเสาอากาศย่าน 2.4 Ghz ที่เป็น connector แบบ UFL หรือ SMA ครับ
3. Supply Voltage อยู่ที่ 2.8-3.4 V
4. Power Down Current < 10uA
5. มี RF data rate อยู่ที่ 250 Kbps (เป็นส่วนของ สัญญาณที่ส่งผ่านอากาศ)
6. มี Serial interface data rate อยู่ระหว่าง 1200 – 115200 Bps (เป็นส่วนที่ติดต่อสื่อสารกับไมโครคอนโทรเลอร์)
7. เป็น Spread Spectrum ชนิด DSSS (Direct Sequence)
8. การกำหนด addressing มีลำดับลักษณะคือ กำหนด PAN ID สำหรับเครือข่ายหนึ่ง ๆ , กำหนด Channel และ กำหนด address ของแต่ละตัว

ตารางที่ 2.10 ตารางแสดงพอร์ตและหน้าที่ ของซิกบี

ขาที่	ชื่อขา	การทำงาน
1	Vcc	ขาต่อไฟเลี้ยง +3.3 โวลต์
2	DOUT	ขาเอาต์พุตส่งข้อมูลอนุกรม
3	DIN	ขาอินพุตรับข้อมูลอนุกรม
4	D08	ขาเอาท์พุตดิจิตอล ช่อง 8
5	RESET	ขารีเซ็ตหลัก (Active “0”)

6	PWM0/RSSI	ขาเอาต์พุต PWM ช่อง 0 และขาเอาต์พุตแสดงความความแรงของการรับสัญญาณ
7	PWM1	ขาเอาต์พุต PWM ช่อง 1
8	ไม่ใช้งาน	
9	DTR/SLEEP_RQ/DI8	ขาอินพุตรับสัญญาณให้หยุดการทำงานเข้าสู่โหมดสลีป หรือ ขาอินพุตดิจิตอล ช่อง 8
10	GND	ขาต่อกราวน์
11	AD4/DI07	ขาอินพุตอะนาล็อก 4 หรือ ขาอินพุตเอาต์พุตดิจิตอล 4
12	CTS/DIO7	อินพุตรับสัญญาณแจ้งการส่งข้อมูลจากโฮสต์ (Clear-To-Send)ใช้ในการควบคุมจังหวะการรับส่งข้อมูล หรือ ขาอินพุตเอาต์พุตดิจิตอล
13	ON/SLEEP	ขาแสดงสถานะการทำงาน “0” อยู่ในโหมดทำงานปกติ “1” อยู่ในโหมดสลีป
14	VREF	ขาต่อแรงดันอ้างอิงสำหรับโมดูลแปลงสัญญาณแอนะล็อกเป็นดิจิตอล ภายใน XBee-Pro
15	Associated/AD5/DIO5	ขาแสดงสถานะการเชื่อมต่อ หรือ ขาอินพุตแอนะล็อก 5 หรือ ขาอินพุตเอาต์พุตดิจิตอล 5
16	RTS/AD6/DIO6	ขาเอาต์พุตแจ้งความพร้อมในการส่งข้อมูล หรือ ขาอินพุตแอนะล็อก 6 หรือขาอินพุตดิจิตอล 6
17	AD3/DIO3	ขาอินพุตแอนะล็อก 3 หรือ ขาเอาต์พุตดิจิตอล 3
18	AD2/DIO2	ขาอินพุตแอนะล็อก 2 หรือ ขาเอาต์พุตดิจิตอล 2
19	AD1/DIO1	ขาอินพุตแอนะล็อก 1 หรือ ขาเอาต์พุตดิจิตอล 1
20	AD0/DIO0	ขาอินพุตแอนะล็อก 0 หรือ ขาเอาต์พุตดิจิตอล 0

Figure 2-03. Internal Data Flow Diagram



รูปที่ 2.34 การส่งข้อมูลภายในโมดูลไร้สายซิกบี

คุณสมบัติด้านการสื่อสารข้อมูลของโมดูลไร้สายซิกบี มีดังนี้

1. สามารถทำงานเป็นอปกรณ์มาสเตอร์และสเลฟได้
2. อัตราบิต 250 กิโลบิตต่อวินาที
3. อัตราบอด 1.2 – 115.2 กิโลบิตต่อวินาที
4. รูปแบบโครงข่ายข้อมูลที่รองรับเป็นแบบจุดต่อจุด (Point-to-Point) จุดต่อหลายจุด (Point-to-multipoint) และความเข้ากันได้กับอุปกรณ์ตามมาตรฐาน 802.15.4
5. มีการเข้าถึงช่องสัญญาณแบบ Channel access using Carrier Sense Multiple Access with Collision Avoidance (CSMA - CA) หรือมีทางเข้าช่วงสัญญาณหลาย ๆ ทาง เพื่อหลีกเลี่ยงการชนกัน
6. มีโทโปโลยีแบบสตาร์ แบบจุดต่อจุด และแบบเมส
7. สามารถรองรับแอดเดรส (Address) ได้ถึง 64 bit IEEE แอดเดรส (65535 โครงข่าย)
8. รองรับการทำงานทั้งแบบ API และ AT command
9. เทคโนโลยีในการกระจายคลื่นแบบDSSS
10. ใช้พลังงานต่ำ (สามารถใช้ได้หลายเดือนจนถึงปี)

2.4.3 โครงสร้างของโมดูลไร้สายซิกบี

มาตรฐานของซิกบี มีการแบ่งเป็นเลเยอร์ (Layer) ซึ่งเลเยอร์เหล่านี้จะทำให้การใช้งานมีประสิทธิภาพมากขึ้น ราคาถูก ติดตั้งง่าย การส่งข้อมูลที่น่าเชื่อถือ ใช้พลังงานน้อย แบ่งเป็นเลเยอร์ต่างๆ ดังนี้

2.4.3.1 เน็ตเวิร์คเลเยอร์ (Network layer)

- เลเยอร์นี้ถูกออกแบบมาเพื่อทำให้การส่งข้อมูลในเน็ตเวิร์ค ใช้พลังงานไม่มาก สามารถจัดการกับเน็ตเวิร์คที่มีจำนวนโหนดมากๆ ทำหน้าที่ดังนี้
- สามารถสร้างเน็ตเวิร์คขึ้นใหม่ได้
- สามารถเข้าร่วมและออกจากเน็ตเวิร์คได้
- สามารถกำหนดค่าของสแตก (Stack) ได้
- กำหนดแอดเดรสให้กับอุปกรณ์แต่ละตัวได้
- สามารติดต่อกับอุปกรณ์อื่นๆแบบซิงโครไนเซชันได้
- ทำให้เฟรมรับส่งมีความปลอดภัย
- จัดหาเส้นทางของเฟรมปลายทาง

2.4.3.2 แอพพลิเคชั่นเลเยอร์(Application Layer)

เลเยอร์นี้ของซิกบี ประกอบด้วย ตัวอุปกรณ์ซิกบีเชิงวัตถุ (ZDO: Zigbee Device Object), user defined application profile(s) และ Application Support (APS) sub-layer

แอพพลิเคชั่นซัพพอร์ตเลเยอร์ (APS : Application Support Layer) ทำหน้าที่ดังนี้

- Discovery สามารถค้นหาและระบุได้ว่าอุปกรณ์ตัวใดติดต่ออยู่กับอุปกรณ์ตัวใดอยู่

- Binding สามารถจับคู่อุปกรณ์ไว้ด้วยกันได้โดยใช้ table of binding และ forward message ระหว่างอุปกรณ์

ตัวอุปกรณ์ซิกบีเชิงวัตถุ (ZDO: Zigbee Device Object) ทำหน้าที่ดังนี้

- กำหนดหน้าที่ของอุปกรณ์แต่ละตัวภายในโครงข่าย เช่น โคออดิเนตซิกบีหรือเอนดิไวซ์
- สร้างหรือตอบสนองการร้องขอ
- สร้างระบบรักษาความปลอดภัยระหว่างอุปกรณ์ในโครงข่าย โดยเลือกจากซิกบีซีเคียวริตีเมตอด(Zigbee's security methods) เช่น public key, symmetric key

ยูเซอร์ ดีไฟน์แอพพลิเคชั่น (User-defined application) หมายถึง เอนดีไวซ์ (end device) ซึ่งเป็นไปตามมาตรฐานของซิกบี

ฟิสิคัลเลเยอร์ (Physical Layer)

IEEE 802.15.4 ถูกออกแบบมาเพื่อลดต้นทุนของความต้องการโดยการใช้วิธีไดเรกซีเควน (Direct sequence) ซึ่งทำให้วงจรไฟฟ้ามีความง่ายมากขึ้น ทำให้ราคาของการติดตั้งลดลง ฟิสิคัลไทป์ดีไวซ์ (Physical type device) ที่จะช่วยลดต้นทุนของระบบมี 2 อย่างคือ ฟลูฟังก์ชันดิไวซ์ (FFD: full function devices) และรีดิวฟังก์ชันดิไวซ์ (RFD: reduced function devices)

Full function device (FFD)

- สามารถฟังก์ชันได้ในทุกๆโทโปโลยี
- สามารถทำเป็นอุปกรณ์เชื่อมต่อระหว่างเครือข่ายได้
- สามารถทำเป็นอุปกรณ์เชื่อมต่อได้
- สามารถติดต่อได้กับทุกๆอุปกรณ์

Reduced function device (RFD)

- ทำได้เฉพาะในโทโปโลยีแบบสตาร์
- ไม่สามารถเป็นสามารถเป็นอุปกรณ์เชื่อมต่อระหว่างเครือข่ายได้
- สามารถสื่อสารได้กับอุปกรณ์เชื่อมต่อระหว่างเครือข่ายเท่านั้น
- สะดวกในการติดตั้ง

IEEE 802.15.4 โครงข่ายซิกบี ต้องการฟูลฟังก์ชั่นดิไวซ์ ที่เป็นอุปกรณ์เชื่อมต่อระหว่างเครือข่ายอย่างน้อยหนึ่งตัว แต่ตัว End point device จะต้องเป็นรีดิวซ์ฟังก์ชันดิไวซ์ เพื่อที่จะลดต้นทุน

2.4.3.3 Media access control (MAC) layer

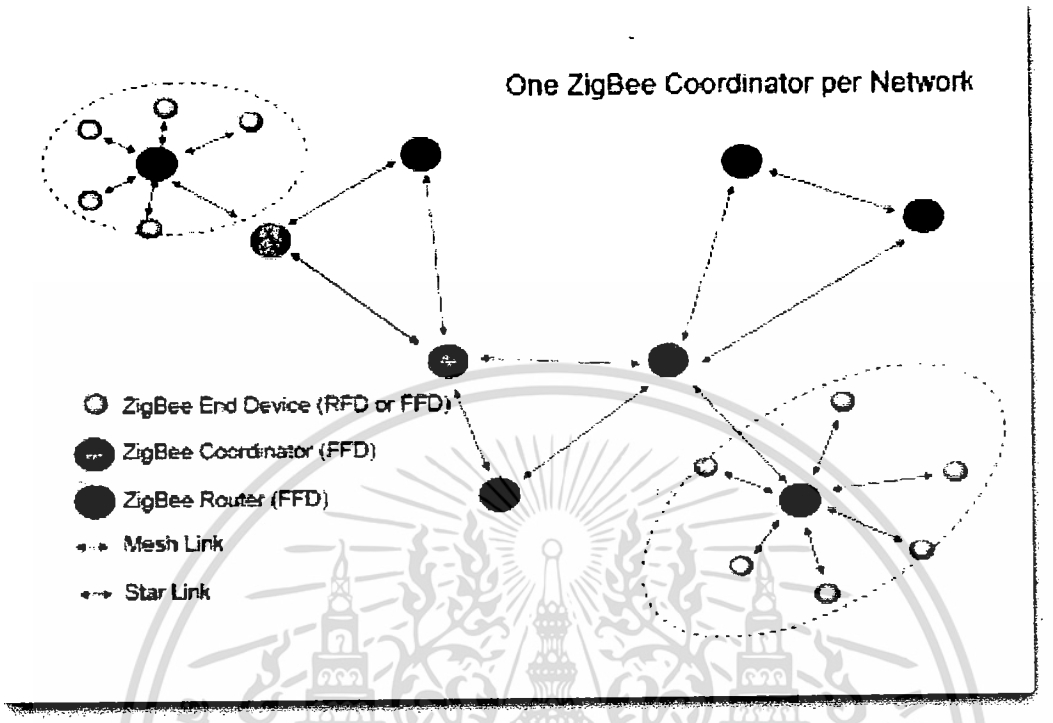
เลเยอร์นี้ถูกออกแบบมาเพื่อให้สามารถใช้โทโปโลยีได้หลายแบบโดยไม่ซับซ้อน ซึ่งทำให้สามารถใช้งานได้กับอุปกรณ์จำนวนมากๆ

อุปกรณ์ซิกบี ดังรูปที่ แบ่งออกเป็น 3 ส่วน คือ

ซิกบีโคออดิเนต (Zigbee Coordinator) ทำหน้าที่สร้างโครงข่าย จัดการโหนดในโครงข่ายและเก็บข่าวสารของโหนดในโครงข่าย

ซิกบีเราเตอร์ (Zigbee Router) ทำหน้าที่จัดการเส้นทางของข้อมูลที่ส่งผ่านภายในโครงข่ายระหว่างโหนดที่ส่งผ่านภายในโครงข่ายระหว่างโหนด

ซิกบีเอนดิไวซ์ (Zigbee end Device) เป็นจุดปลายของโครงสร้างเครือข่าย อยู่ในส่วนของผู้ใช้งานโดย สามารถเป็นไปได้ทั้งแบบรีดิวซ์ฟังก์ชันดีไวซ์ และแบบฟูลฟังก์ชันดิไวซ์



รูปที่ 2.35 ตัวอย่างการสร้างเครือข่ายของอุปกรณ์ ซิกบี

2.4.4 การส่งข้อมูลของโมดูลไร้สายซิกบี

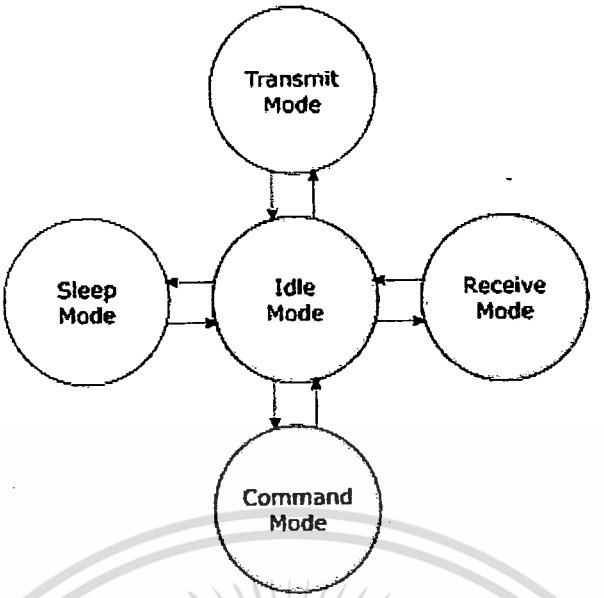
การส่งข้อมูลแบบอาร์เอฟ (RF) ของแต่ละแพ็คเกจในส่วนของเฮดเดอร์ จะประกอบไปด้วยแอดเดรสต้นทางและแอดเดรสปลายทาง โดยที่ IEEE 802.15.4 จะมีโครงสร้าง 2 แบบ นั่นคือแบบสั้น 16 บิตแอดเดรส (short 16-bits address) และแบบยาว 64 บิตแอดเดรส (long 64-bit address) ซึ่ง 64 บิตแอดเดรสจะสามารถอ่านคำสั่ง SL (Serial Number Low) และ SH (Serial Number High) และการส่งข้อมูลแบบอาร์เอฟ จะส่งได้ 2 โหมด คือ โหมดยูนิแคส (Unicast Mode) และโหมดบรอดแคส (Broadcast Mode)

การส่งแพ็คเกจโดยใช้โครงสร้าง 16 บิตแอดเดรส ให้ตั้งค่าแปร DL (Destination Address Low) .ให้เท่ากับตัวแปร MY และตั้งค่าตัวแปร DH (Destination Address High) เป็น '0'

การส่งแพ็คเกจโดยใช้โครงสร้าง 64 บิตแอดเดรส ให้ตั้งค่าแอดเดรสปลายทาง (DL + DH) ให้เข้ากับแอดเดรสต้นทาง (SL+SH) ของปลายทางที่จะส่งแพ็คเกจไป

2.4.5 การทำงานของซิกบี

การทำงานของซิกบี แบ่งออกได้เป็น 5 โหมด ดังรูปที่ 2.20



รูปที่ 2.36 แผนภาพแสดงโหมดการทำงานของซิกบี

Idle Mode เป็นโหมดที่ไม่มีการรับส่งข้อมูล และเป็นโหมดกลางที่สามารถเปลี่ยนไปยงโหมดต่างๆ ได้

Transmit Mode มีการส่งข้อมูลได้สองวิธี

1. Direct Transmission – ข้อมูลทั้งหมดจะถูกส่งไปยัง Destination Address ทันที

2. Indirect Transmission – ข้อมูลจะถูกเก็บไว้จนกว่าจะถึงเวลาส่งเท่านั้น และจะส่งไปยังที่มีการตอบรับมา (Source Address = Destination Address)

Receive Mode ข้อมูล RF จะถูกรับทางสายอากาศ

Sleep Mode RF อยู่ในสถานะที่มีการใช้กำลังไฟฟ้าต่ำหรือไม่มีการใช้ การเข้ามาอยู่ในโหมดนี้นั้นจะต้องเป็นไปตามเงื่อนไขต่อไปนี้อย่างน้อยหนึ่งอย่าง (ค่าของตัวแปร SM ต้องไม่เป็น 0)

1. มีการใช้งานที่ Sleep_RQ (pin 9)

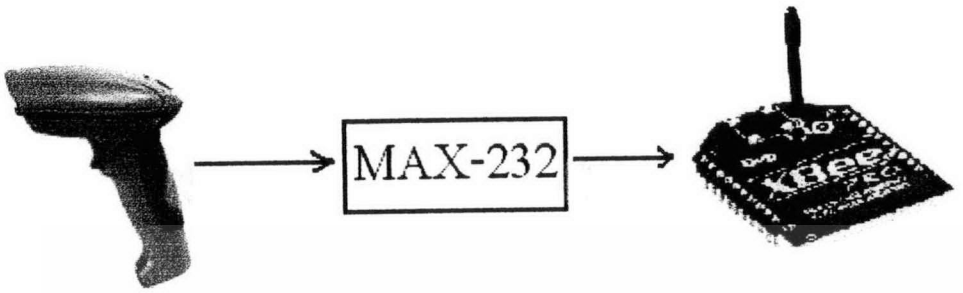
2. อยู่โหมด idle (ไม่มีการรับส่งข้อมูล) เป็นเวลานานมากกว่าที่กำหนดไว้ที่ตัวแปร ST (Time before Sleep)

Command Mode เป็นโหมดคำสั่งโดยจะใช้ลำดับเป็นสำคัญ

บทที่ 3

การออกแบบและคำนวณ

3.1 บล็อกไดอะแกรม



รูปที่ 3.1 บล็อกไดอะแกรมการส่งข้อมูล

รูปที่ 3.2 บล็อกไดอะแกรมการรับข้อมูล

3.2 การคำนวณอัตราการส่งผ่านข้อมูล

$$Baud \quad Rate = \frac{f\,CK}{16(UBR+1)}$$

f CK = Crystal clock frequency

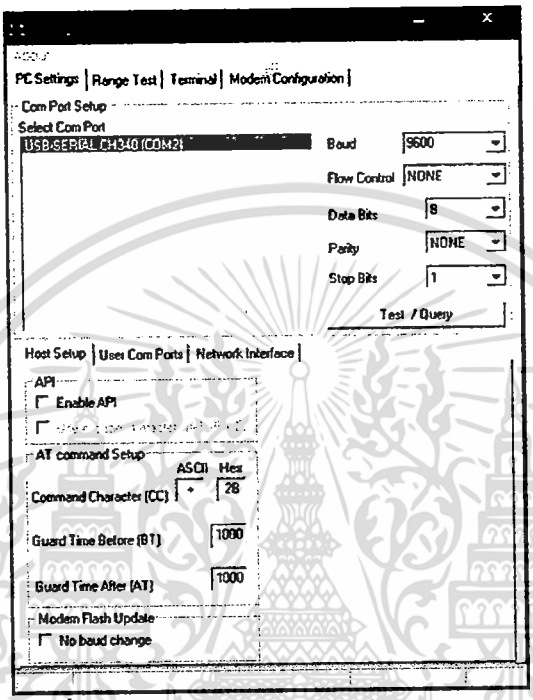
UBR = Contents of the UBRRH and UBRR Registers

3.3 การกำหนดค่าของ ZigBee

ก่อนที่จะมีการใช้ซิกบีจะต้องมีการเซ็ตค่าต่างของซิกบีซึ่งในงานวิจัยนี้ได้ใช้ซิกบีมาเป็นส่วนหนึ่งของการรับส่งข้อมูลและจะมีการเซ็ตค่าดังต่อไปนี้

การเซ็ตอัตราการส่งข้อมูล(Broadrate)

จากรูปที่ 3.3 เป็นการเซ็ตค่าอัตราการส่งข้อมูลของซิกบีเพื่อให้อุปกรณ์ดังกล่าวสามารถที่จะรับส่งข้อมูลได้



รูปที่ 3.3 การเซ็ตค่าอัตราการส่งข้อมูลของซิกบี

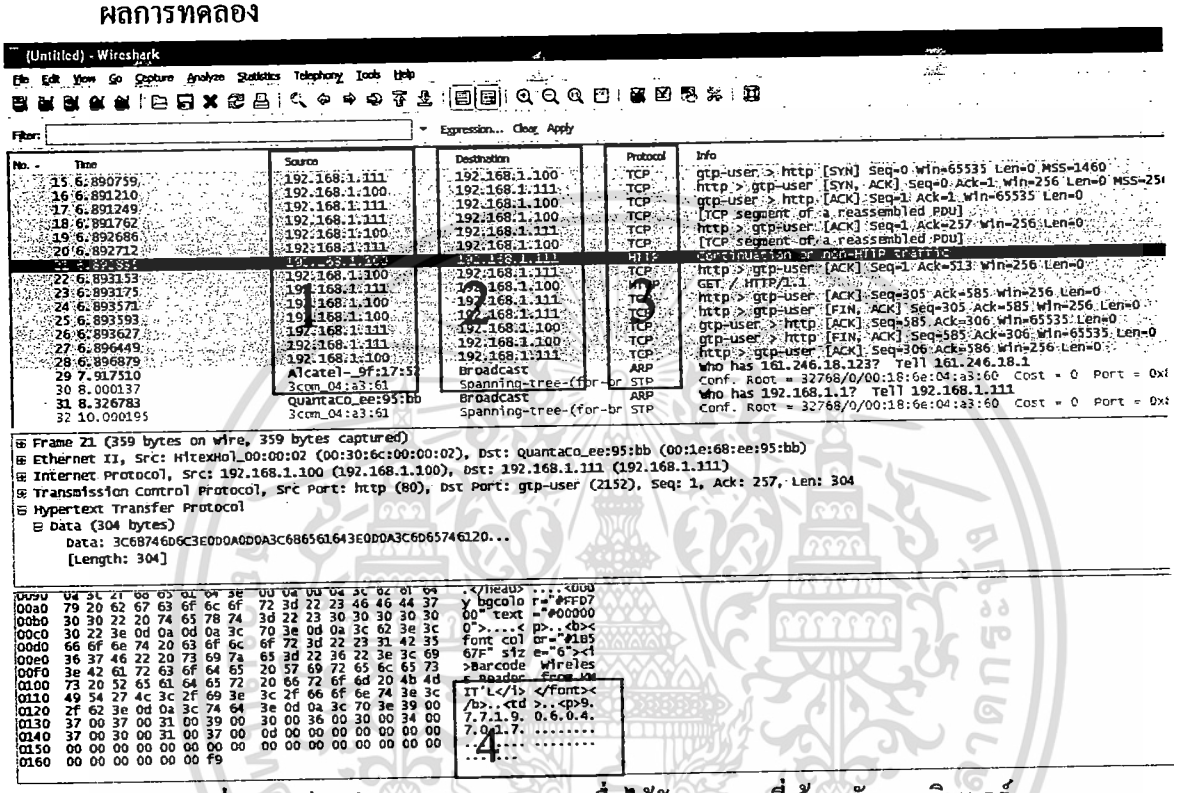
จากนั้นทำการเซ็ตค่าที่อุปกรณ์ซิกบีให้เป็นตัวรับหรือตัวส่ง จากรูปที่ 3.4 เป็นการเซ็ตให้ซิกบีเป็นอุปกรณ์รับสัญญาณ

4.5 การทดลองแสดงผลข้อมูลที่เข้ามาในคอมพิวเตอร์โดยใช้โปรแกรม wireshark

ขั้นตอนการทดลอง

1. ทำการเชื่อมต่อระบบรับข้อมูลกับคอมพิวเตอร์โดยใช้พอร์ต RJ45
2. จ่ายไฟเลี้ยงให้กับเครื่องอ่านบาร์โค้ดและทำการกดเพื่อแสกนบาร์โค้ด
3. เปิดโปรแกรม wireshark เพื่อตรวจจับ Packet ที่เข้ามาในคอมพิวเตอร์ทางด้านรับ

ผลการทดลอง



รูปที่ 4.7 หน้าจอโปรแกรม wireshark เมื่อได้รับ Packet ที่เข้ามายังคอมพิวเตอร์

จากรูปที่ 4.7 สามารถอธิบายได้ดังนี้

หมายเลข 1 : IP Address ของต้นทางซึ่งเป็น IP จาก ARM 7 คือ 192.168.1.100

หมายเลข 2 : IP Address ของปลายทางซึ่งเป็น IP จาก คอมพิวเตอร์ คือ 192.168.1.111

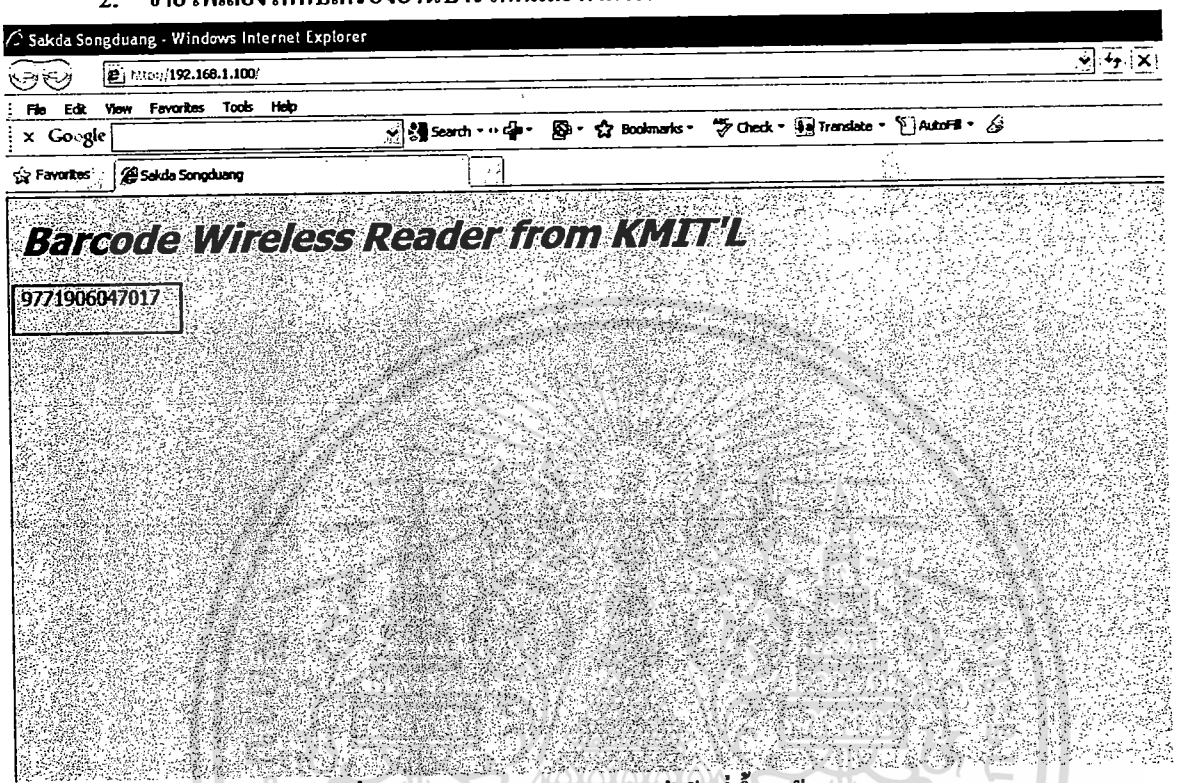
หมายเลข 3 : ต้นทางและปลายทางมีการติดต่อโดยใช้โปรโตคอล TCP

หมายเลข 4 : แสดงข้อมูลที่อยู่ใน Packet ซึ่งเป็นข้อมูลที่ได้จากการอ่านบาร์โค้ด

4.6 การทดลองแสดงข้อมูลทางหน้า Web

ขั้นตอนการทดลอง

1. เปิดหน้า Web http\\:192.168.1.100
2. จ่ายไฟเลี้ยงให้กับเครื่องอ่านบาร์โค้ดและทำการกดเพื่อแสกนบาร์โค้ด



รูปที่ 4.8 ข้อมูลจากการแสกนบาร์โค้ดที่ขึ้นหน้า Web

จากรูปที่ 4.8 เมื่อทำการแสกนบาร์โค้ดผ่านระบบอินเตอร์เน็ตโดยเปิดหน้าเว็ปดังกล่าวจะพบว่าโค้ดที่ได้ทำการแสกนนั้นตรงกับโค้ดที่ขึ้นหน้าเว็ป

บทที่ 4

ผลการทดลอง

4.1 การทดลองวัดค่าสัญญาณจากเครื่องอ่านบาร์โค้ด

ขั้นตอนการทดลอง

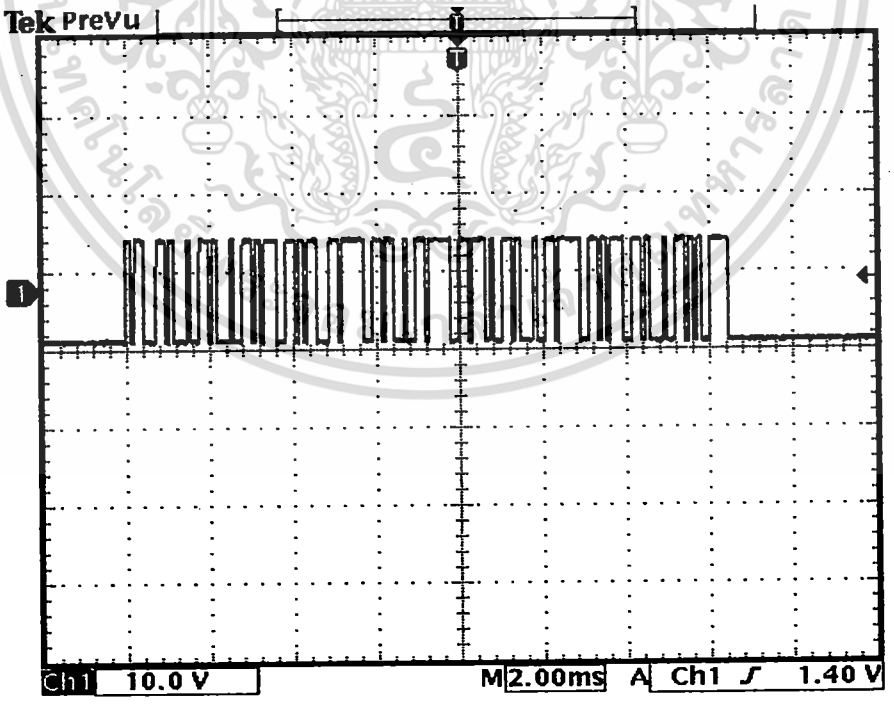
1. จ่ายไฟเลี้ยงให้กับเครื่องอ่านบาร์โค้ดและทำการกดเพื่อแสกนบาร์โค้ด
2. ทำการวัดค่าสัญญาณข้อมูลที่ขา 2 ของพอร์ตอนุกรม
3. วัดค่าสัญญาณเมื่อผ่าน IC MAX-232

ผลการทดลอง

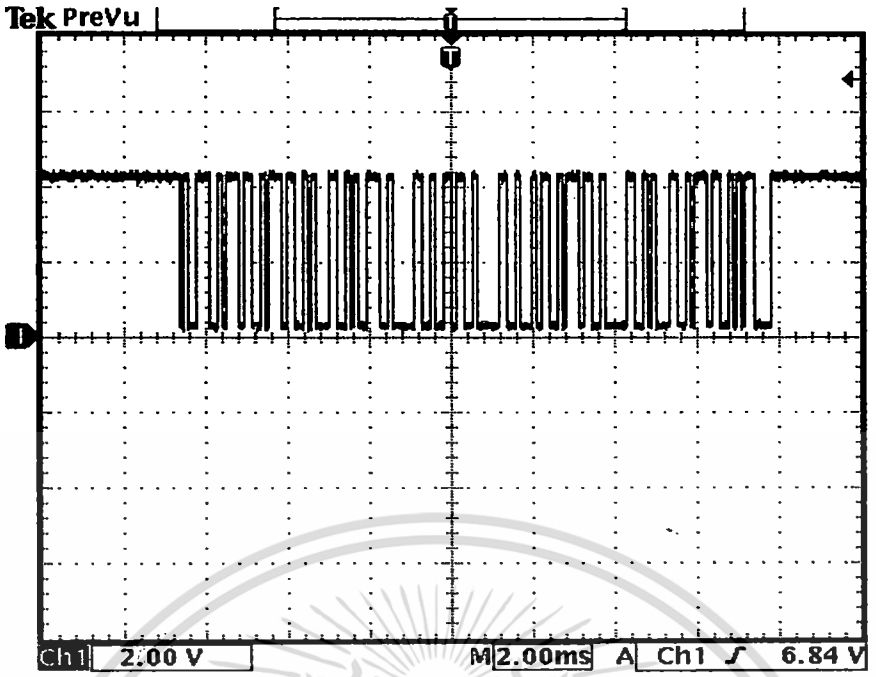
ISSN 1906-0475 09

9 771906 047017

รูปที่ 4.1 ตัวอย่างบาร์โค้ดที่เลือกมาเพื่อใช้แสกน



รูปที่ 4.2 สัญญาณข้อมูลที่อ่านได้จากการแสกนบาร์โค้ด



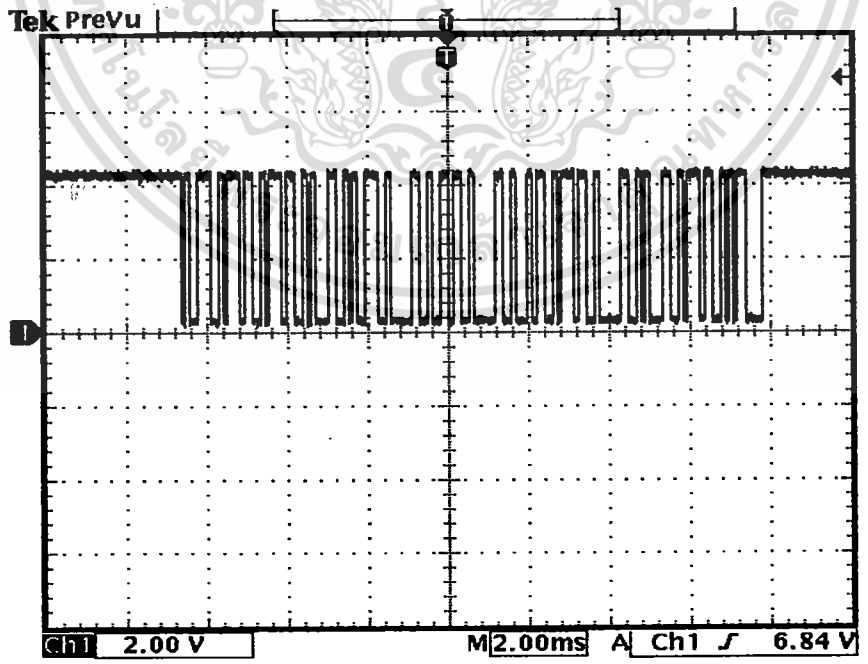
รูปที่ 4.3 วัดค่าสัญญาณข้อมูลแบบ TTL ที่ได้จากขา 9 จาก IC MAX-232

4.2 การทดลองวัดค่าสัญญาณที่ซิกบีฝั่งส่ง

ขั้นตอนการทดลอง

1. Set ซิกบีให้มีอัตราการส่งข้อมูลที่ 9600 และ Set ให้เป็นตัวส่งข้อมูล
2. จ่ายไฟเลี้ยงให้กับเครื่องอ่านบาร์โค้ดและทำการกดเพื่อแสกนบาร์โค้ด
3. วัดสัญญาณที่ขา 3 ของซิกบี

ผลการทดลอง



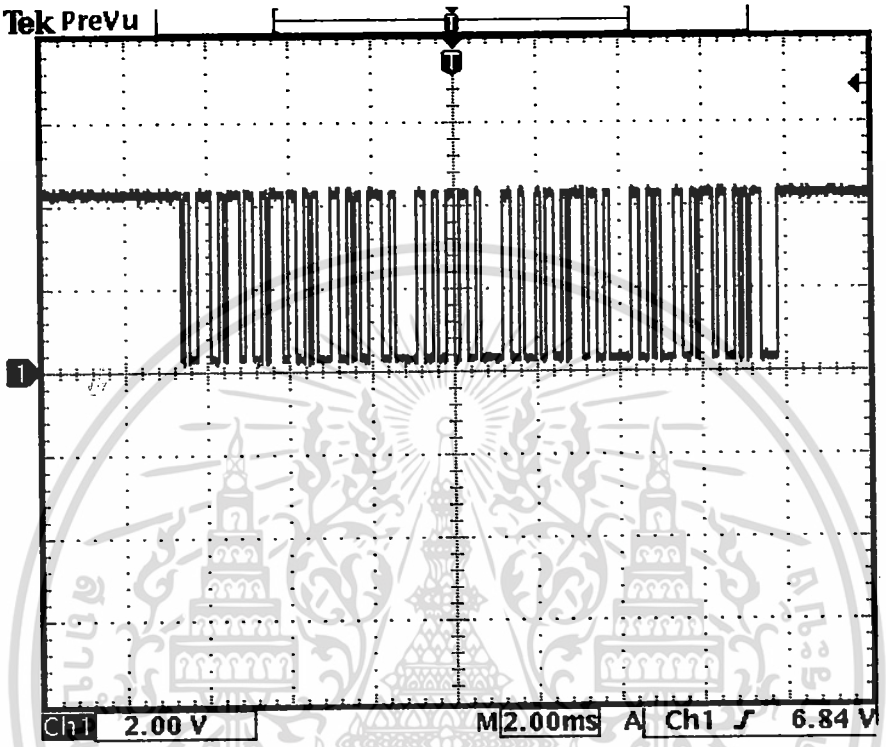
รูปที่ 4.4 วัดค่าสัญญาณข้อมูลที่ได้จากขา 3 ของซิกบี

4.3 การทดลองวัดค่าสัญญาณที่ซิกบีฝั่งส่ง

ขั้นตอนการทดลอง

1. Set ซิกบีให้มีอัตราการส่งข้อมูลที่ 9600 และ Set ให้เป็นตัวรับข้อมูล
2. จ่ายไฟเลี้ยงให้กับเครื่องอ่านบาร์โค้ดและทำการกดเพื่อแสกนบาร์โค้ด
3. วัดสัญญาณที่ขา 2 ของซิกบี

ผลการทดลอง



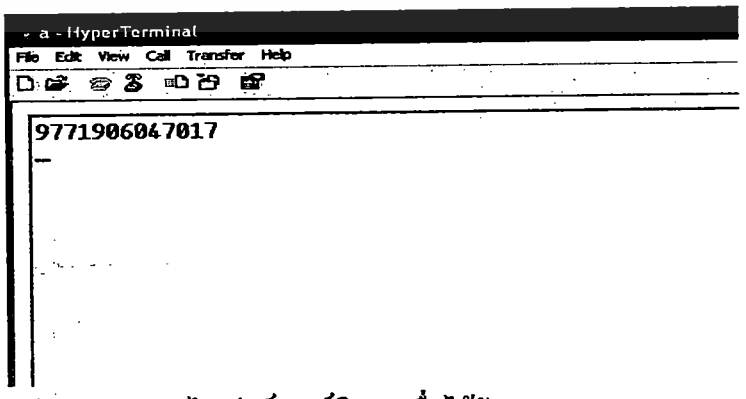
รูปที่ 4.5 วัดค่าสัญญาณข้อมูลที่ได้จากขา 2 ของซิกบี

4.4 การทดลองแสดงผลเป็นหมายเลขบาร์โค้ดบนไฮเปอร์เทอร์มินอล

ขั้นตอนการทดลอง

1. ทำการเชื่อมต่อระบบรับข้อมูลกับคอมพิวเตอร์โดยใช้พอร์ตอนุกรม
2. จ่ายไฟเลี้ยงให้กับเครื่องอ่านบาร์โค้ดและทำการกดเพื่อแสกนบาร์โค้ด
3. เปิดโปรแกรมไฮเปอร์เทอร์มินอลเพื่อรับค่าจากพอร์ต COM 1

ผลการทดลอง



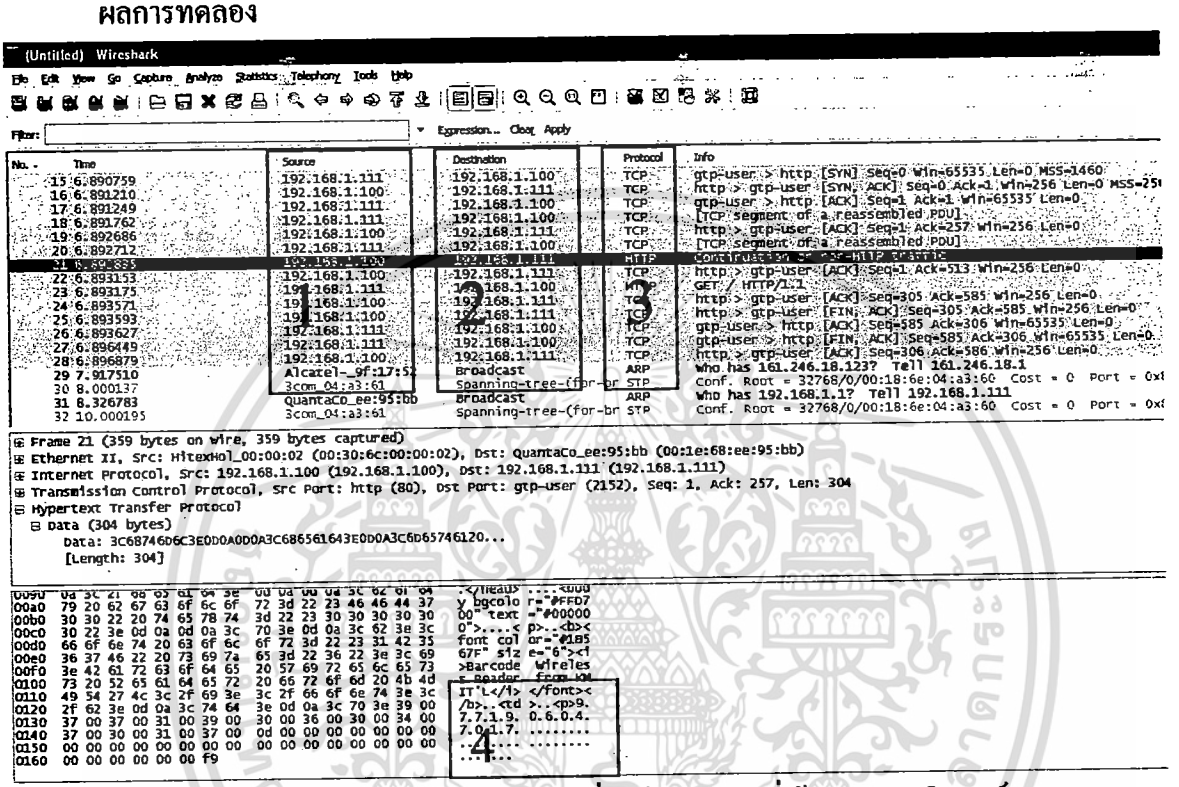
รูปที่ 4.6 หน้าจอโปรแกรมไฮเปอร์เทอร์มินอลเมื่อได้รับหมายเลขจากการแสกนบาร์โค้ด

4.5 การทดลองแสดงผลข้อมูลที่เข้ามาในคอมพิวเตอร์โดยใช้โปรแกรม wireshark

ขั้นตอนการทดลอง

1. ทำการเชื่อมต่อระบบรับข้อมูลกับคอมพิวเตอร์โดยใช้พอร์ต RJ45
2. จ่ายไฟเลี้ยงให้กับเครื่องอ่านบาร์โค้ดและทำการกดเพื่อแสกนบาร์โค้ด
3. เปิดโปรแกรม wireshark เพื่อตรวจจับ Packet ที่เข้ามาในคอมพิวเตอร์ทางด้านรับ

ผลการทดลอง



รูปที่ 4.7 หน้าจอโปรแกรม wireshark เมื่อได้รับ Packet ที่เข้ามายังคอมพิวเตอร์

จากรูปที่ 4.7 สามารถอธิบายได้ดังนี้

หมายเลข 1 : IP Address ของต้นทางซึ่งเป็น IP จาก ARM 7 คือ 192.168.1.100

หมายเลข 2 : IP Address ของปลายทางซึ่งเป็น IP จาก คอมพิวเตอร์ คือ 192.168.1.111

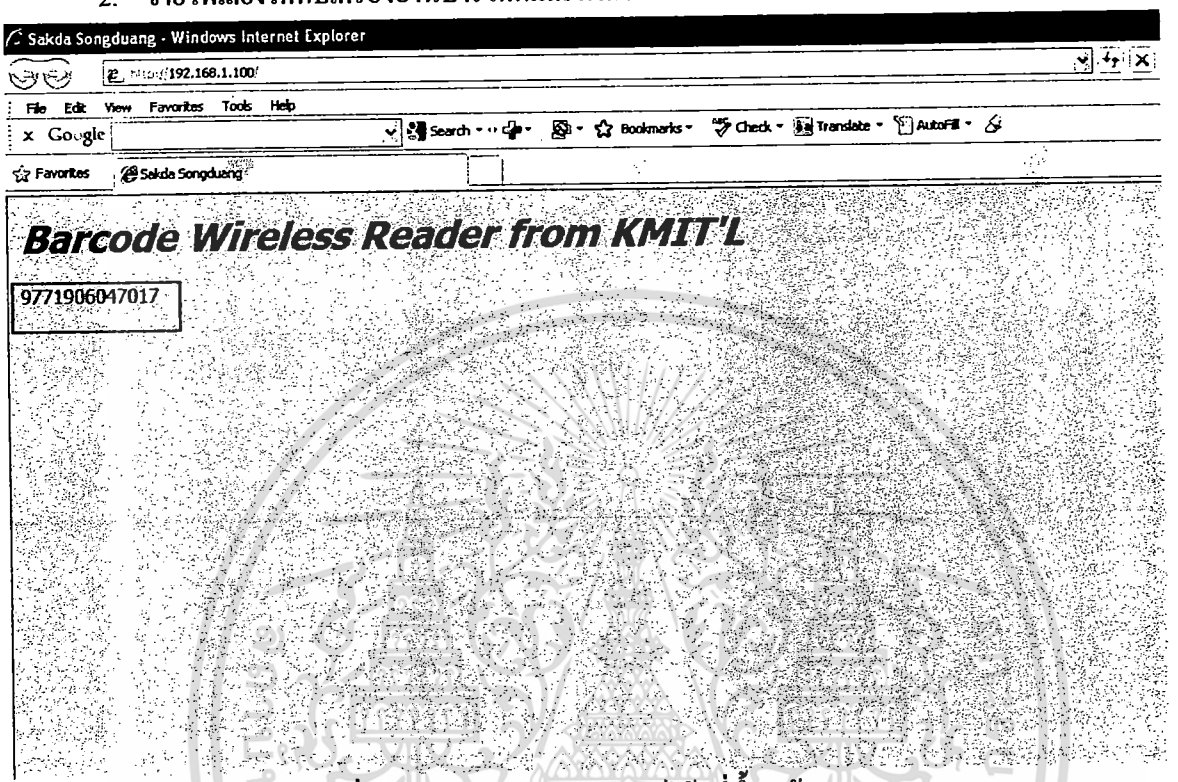
หมายเลข 3 : ต้นทางและปลายทางมีการติดต่อโดยใช้โปรโตคอล TCP

หมายเลข 4 : แสดงข้อมูลที่อยู่ใน Packet ซึ่งเป็นข้อมูลที่ได้จากการอ่านบาร์โค้ด

4.6 การทดลองแสดงข้อมูลทางหน้า Web

ขั้นตอนการทดลอง

1. เปิดหน้า Web http\\:192.168.1.100
2. จ่ายไฟเลี้ยงให้กับเครื่องอ่านบาร์โค้ดและทำการกดเพื่อแสกนบาร์โค้ด



รูปที่ 4.8 ข้อมูลจากการแสกนบาร์โค้ดที่ขึ้นหน้า Web

จากรูปที่ 4.8 เมื่อทำการแสกนบาร์โค้ดผ่านระบบอินเตอร์เน็ต โดยเปิดหน้าเว็ปดังกล่าวจะพบว่าโค้ดที่ได้ทำการแสกนนั้นตรงกับโค้ดที่ขึ้นหน้าเว็ป ก็คือ 9771906047017

บทที่ 5
บทวิจารณ์และสรุปผล

บทสรุป

จากการศึกษาระบบบาร์โค้ดที่ใช้กันในปัจจุบันพบว่ายังมีการใช้แบบที่เป็นสายกันอยู่และถ้ามีการนำระบบระบุตัวตนเข้ามาใช้ก็จะทำให้มีการสิ้นเปลืองมากขึ้น จากการออกแบบระบบบาร์โค้ดแบบไร้สายโดยผ่านระบบอีเทอร์เน็ต ซึ่งมีการใช้อุปกรณ์ซิกบี (ZigBee) และ ARM 7 เข้ามาช่วยในการส่งข้อมูลที่ได้จากการแสกน และเมื่อทำการออกแบบให้ซิกบีเป็นอุปกรณ์ที่ใช้ในการส่งข้อมูลแบบไร้สายนั้นพบว่าจะต้องมีการเซ็ตอุปกรณ์ซิกบีให้เป็นตัวรับและเป็นตัวส่งข้อมูลหลังจากนั้นต้องเซ็ตอัตราการส่งข้อมูลของซิกบี ซึ่งจะเห็นได้ว่าถ้านำอุปกรณ์ซิกบีมาใช้ก็จะง่ายขึ้น ส่วน ARM 7 นั้นจะใช้เป็นตัวประมวลผลส่งผ่านไปยังระบบอีเทอร์เน็ตและทางพอรต์อนุกรม และเมื่อออกแบบให้รับข้อมูลมาจากซิกบีจะส่งข้อมูลที่ได้ไปยังเว็ปและพอรต์อนุกรมพร้อมๆ กันในเวลาเดียวกัน จากการทดลองแสกนตัวอย่างสินค้าพบว่าสามารถที่จะส่งรหัสหรือโค้ดของสินค้าผ่านระบบไร้สายได้ และในเรื่องของระยะทางในการส่งข้อมูลนั้นอยู่ที่ 150 เมตรในที่มีสิ่งกีดขว้าง นอกจากนั้นแล้วยังมีการต่อผ่านระบบอีเทอร์เน็ตที่ใช้แลนด์ พบว่าสามารถที่จะต่อผ่านได้หลาย ๆ เครื่องในเวลาเดียวกันของการแสกน ซึ่งถ้าหากนำไปใช้ในอุตสาหกรรมของระบบคลังสินค้าก็สามารถที่นำไปใช้ได้

บทวิจารณ์

สำหรับปัญหาที่พบจากการออกแบบระบบดังกล่าวไม่สามารถที่จะนำไปแสกนในคลังสินค้าที่มีรัศมีกว้างเกิน 200 เมตรไม่ได้หากจะนำไปใช้ต้องทำให้เป็นระบบทวนสัญญาณของซิกบี และการแสกนจะไม่มีตัวบ่งบอกว่าข้อมูลที่ได้แสกนนั้นไปถึงคอมพิวเตอร์หรือเปล่าและจะต้องใช้พลังงานในด้านส่งมากพอสมควร