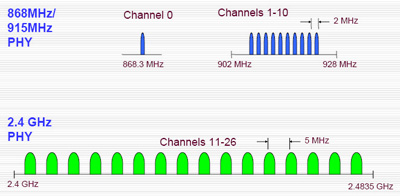


Zigbee and Xbee BASIC ตอน Zigbee คืออะไร

[ZigBee](http://en.wikipedia.org/wiki/ZigBee" \t "_blank) มาตรฐานสากล กำหนดโดย [ZigBee Alliance](http://www.zigbee.org/) เป็น การสื่อสารแบบไร้สาย ที่มีอัตราการรับส่งข้อมูลต่ำ ใช้พลังงานต่ำ ราคาถูก จุดประสงค์ก็เพื่อให้สามารถสร้างระบบที่เรียกว่า Wireless Sensor Network ได้ ซึ่งระบบนี้จะสามารถทำงาน ในร่ม กลางแจ้ง ทนแดด ทนฝน และอยู่ได้ด้วยแบตเตอรี่ก้อนเล็ก (เช่นถ่าน AA 2 ก้อน) นานเป็นเดือน เป็นปี เหมาะสมใช้งานกับพวก Monitoring ต่าง ๆ หากยังมีความไม่เข้าใจอยู่ อาจหาความรู้เพิ่มเติมจาก Clip Video ที่บรรยายเรื่อง ระบบเซ็นเซอร์ในการตรวจวัดทางด้านสิ่งแวดล้อม

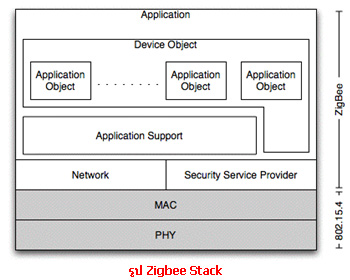
[ZigBee](http://en.wikipedia.org/wiki/ZigBee" \t "_blank) กำหนดย่านความถี่ใช้งานตามมาตรฐานไว้ 3 ย่านความถี่คือ ย่าน 2.4 GHz, ย่าน 915 MHz และย่าน 868 MHz โดยแต่ละย่านจะมีช่องสัญญาณ 16 ช่อง, 10 ช่อง และ 1 ช่อง ตามลำดับ ส่วน อัตรารับส่งข้อมูล (ทางอากาศ) จะอยู่ที่ 250 Kbps, 40 Kbps, 20 Kbps ตามลำดับเช่นกัน



สรุป  
1. ย่านความถี่ 2.4 Ghz มี 16 ช่องสัญญาณ อัตรารับส่งข้อมูล 250 Kbps  
2. ย่านความถี่ 915 Ghz มี 10 ช่องสัญญาณ อัตรารับส่งข้อมูล 40 Kbps  
3. ย่านความถี่ 868 Ghz มี 1 ช่องสัญญาณ อัตรารับส่งข้อมูล 20 Kbps

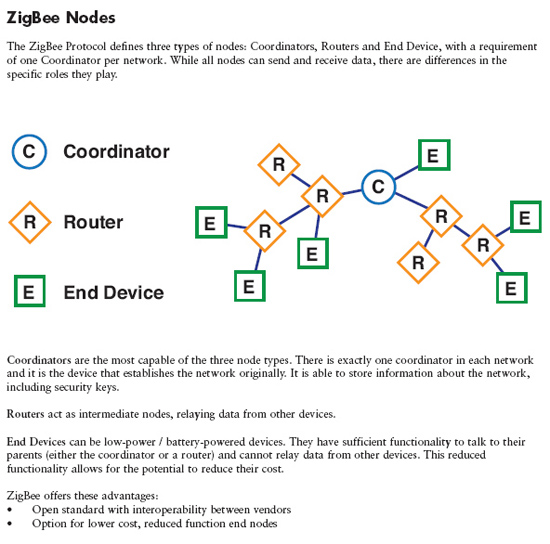
โดยมากมักสับสน ระหว่าง Zigbee กับ Wifi โดยผู้ที่เริ่มศึกษาจะมีคำถามว่า Zigbee กับ Wifi (หรือ โมดูล 2.4 Ghz) นั้น ย่านความถี่เหมือนกัน จะสามารถสื่อสารกันได้หรือไม่ คำตอบคือ สื่อสารกันไม่ได้ เพราะทางกายภาพ ถึงแม้จะเป็นย่านความถี่เดียวกัน แต่ Protocol ที่ใช้สื่อสารกันนั้นไม่เหมือนกัน

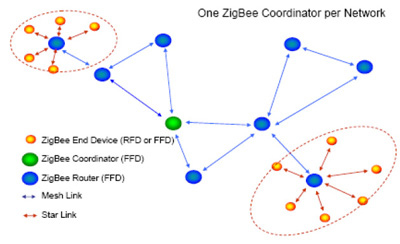
ZigBee นำ Physical Layer และ MAC Layer ของ [IEEE 802.15.4](http://www.ieee802.org/15/pub/TG4.html) ซึ่งเป็นมาตรฐานการกำหนดการสื่อสารไร้สายแบบ WPAN (Wireless Personal Area Network) มาทำงานใน Layer ที่ต่ำกว่า (2 Layer ล่างสุด) เช่น เรื่องของ ระดับกำลังสัญญาณ, Link Quality, Access control, Security ฯลฯ แต่ใน Layer ถัดไปจะเป็นรูปแบบของ Zigbee



จากที่กล่าวมา ZigBee จะสามารถสร้างเป็นเครือข่ายได้เพราะอิงมาตรฐานตาม IEEE 802.15.4 และมีการจัดการในแบบของ Zigbee ใน Layer ถัดไป ทั้งนี้ IEEE 802.15.4 แบ่งชนิดอุปกรณ์ในเครือข่ายออกเป็น 2 ประเภท คือ FFD ( Full Function Device )ซึ่งหมายถึงอุปกรณ์ที่สามารถทำงานได้ทุกอย่างในเครือข่าย และ RFD (Reduce Function Device) ซึ่งหมายถึงอุปกรณ์ที่ถูกลดความสามารถการทำงานในเครือข่าย

 \*\* ZigBee ได้แบ่งตามลักษณะการทำงาน 3 แบบ คือ   
1. Coordinator  มีหน้าที่สร้างการสื่อสาร เชื่อมโยงเครือข่าย ระหว่าง End Device กับ Router หรือ Coordinator กับ Coordinatorด้วยกัน หรือ Coordinator กับ Router กำหนด address ให้กับ device ที่อยู่ในวงเครือข่าย ไม่ให้ซ้ำกัน ดูแลจัดการเรื่องการRouting เส้นทาง ซึ่งเทียบได้กับ FFD  
2. End Device  เป็นอุปกรณ์ปลายทางสุด ซึ่งจะใช้รับสัญญาณจาก Sensor ที่ปลายทาง โดยที่ใช้พลังงานต่ำในการทำงาน เทียบได้กับ RFD หรือ FFD บางกรณี ขึ้นอยู่กับ sensor ที่ใช้  
3. Router มีหน้าที่ รับส่งข้อมูล ในเส้นทางต่าง ๆ ของเครือข่าย  ซึ่งเทียบได้กับ FFD





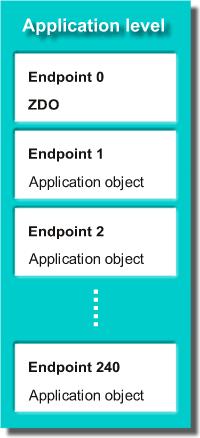
**โครงสร้างซอฟท์แวร์**

จากรูปแสดง 3 ชั้นหลัก ชั้นล่าง PHY+MAC ว่าตาม 802.15.4 (รับผิดชอบการรับส่งข้อมูลและ addressing) แล้วกลุ่มพันธมิตร ZigBee หยิบมาต่อเติมชั้นบนเป็น ZigBee Stack ซึ่งจัดเตรียมสมบัติหรือฟังก์ชั่น โครงสร้างเน็ตเวิร์ก เส้นทางการส่งข้อมูล และการรักษาความปลอดภัย (คุณมองว่ามันคือ network layer ได้เลยครับ) กับ Application level ซึ่งเป็นตัวปฏิบัติการตาม app ที่ทำงานของแต่ละโหนด

|  |  |  |
| --- | --- | --- |
| http://www.bloggang.com/data/z/zol/picture/1297744315.jpg | http://www.bloggang.com/data/z/zol/picture/1297744520.jpg | http://www.bloggang.com/data/z/zol/picture/1297744355.gif |

เมื่อแจกแจงให้ละเอียดกว่าเดิมอีกนิดโครงสร้างซอฟท์แวร์ของ ZigBee จะเป็นดังรูปขวามือ โดยทั่วไปโหนดอาจะมีได้หลาย app และเราเรียก app instance บนโหนดว่า endpoint (มันเป็น jargon ที่ถ้าคุณได้ใช้ก็น่าจดจำนะครับ) ซึ่งพูดง่าย ๆ endpoint เป็นที่ที่ข้อความ (message) ถูกสร้างขึ้นหรือเป็นที่ปลายทางของข้อความ หนึ่งโหนดสามารถมีได้สูงสุด 240 endpoints แต่ละ endpoint ต้องมีหมายเลขกำกับ (address) ตั้งแต่ 1 ถึง 240 (ถ้าคุณอ้างอิงหมายเลขที่อยู่ 255 มันจะตีความว่าเป็นการ broadcast) และที่อยู่หมายเลข 0 สงวนไว้สำหรับ app พิเศษตัวหนึ่งซึ่งเรียกว่า ZDO (ZigBee Device Objects)

ZDO มีหน้าที่   
     1. กำหนดชนิดของโหนด   
     2. เริ่มการทำงานของโหนด   
     3. มีส่วนในการสร้างเน็ตเวิร์ก (กรณีที่โหนดนั้นคือตัวแม่)  
ด้วยบทบาทพิเศษของ ZDO ที่ต้องเข้าไปเจรจาข้องเกี่ยวกับ layer เน็ตเวิร์ก มันจึงมี ZDO Management Plane ที่แผ่ครอบคลุมชั้น APS (Application Support Sub-layer) กับ NWK (Network layer) ซึ่งยินยอมให้ ZDO ติดต่อสื่อสารกับสองชั้นนี้ตอนที่มันทำงานประเภท internal task และยินยอมให้ ZDO รับมือกับ request จาก application สำหรับการ access เน็ตเวิร์กและฟังก์ชั่นด้านความปลอดภัยด้วยการใช้ ZDP

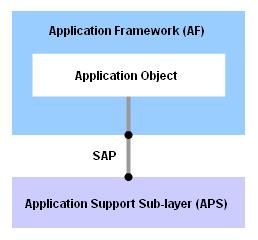
(ZigBee Device Profile) message  
SAP จะจัดเตรียมกลุ่มของ operation สำหรับส่ง information และ command ระหว่างชั้น มี 4 operation หลักได้แก่

1. request ซึ่ง layer บนต้องการใช้ service บางอย่างจาก layer ล่างก็จะส่งคำสั่ง request ไปยัง layer ล่าง

2. confirm เป็นการตอบสนองกลับของ layer ล่างว่ามัน accept หรือ reject ต่อ request นั้น

3. response เป็นการตอบสนองผลลัพธ์ของ request จาก layer ล่างในแบบใดแบบหนึ่ง ซึ่งคุณ response นี้อาจจะ reponse ทันทีทันใดหรือไม่ทันทีทันใด หน่วงเวลาออกไปก็ได้นะครับ ทั้งนี้ทั้งนั้นขึ้นอยู่กับว่าสิ่งที่ layer บน request มานั้นเป็นอะไร และ

4. indication จะถูกสร้างขึ้นมาเมื่อ layer ล่างมีอะไรอยากแจ้ง layer บน พูดง่าย ๆ ว่ามันเป็น unsolicited information หรืออาจจะเป็น command ที่ต้องส่งต่อให้กับ layer บน (เช่น layer ล่างอาจ indicate ให้ layer บนรับทราบว่ามีข้อมูลบางอย่างส่งมานะ)

  
ต่ำลงมา APS หรือ Application Support Sub-layer มีหน้าที่สำคัญ 2 ประการ  
     1. เป็นช่องทางสื่อสารของ app โดยข้อความจะถูกส่งผ่าน SAP (Service Access Point) ที่อยู่ระหว่าง APS กับแต่ละ endpoint  
     2. จัดการดูแลตาราง binding (เดี๋ยว concept ของการ binding เราจะพูดถึงอีกที) และส่งข้อความระหว่างโหนดที่เชื่อมพันธะถึงกัน  
บริเวณนี้มี jargon อีก 2 คำ คือ Application Framework (AF) กับ SAP คำว่า AF นั้นได้แก่ส่วนที่ประกอบด้วย endpoint (ในรูปเขียน Application object) กับ ส่วนสนับสนุนการติดต่อสื่อสารระหว่าง app กับ APS โดย app จะติดต่อกับ APS ผ่าน interface ที่เรียกว่า SAP

ถัดลงมาจาก APS คือ NWK (Network layer) จัดการเกี่ยวกับ network addressing กับ routing โดยไป invoke ให้เกิดการกระทำใน MAC layer

สรุปหน้าที่สำคัญ

1. สำหรับตัวแม่ ฟังก์ชันของ layer นี้คือการเริ่มต้นเน็ตเวิร์ก จากนั้น

2. กำหนด network address

3. เพิ่มหรือลดอุปกรณ์จากเน็ตเวิร์ก

4. routing ข้อมูลไปยังจุดหมายปลายทาง 5. ใส่มาตรการรักษาความปลอดภัยให้กับข้อมูลที่จะส่งออก และ

5. implementing route discovery

**Applications**

Stack profile เป็นตัวกำหนด ชนิด รูปร่าง และลักษณะของเน็ตเวิร์กขึ้นอยู่กับประเภทของ application เช่น Home Controls profile ภายใต้ stack profile ก็จะมี application profile เช่นกลุ่มพันธมิตร ZigBee ได้นิยาม Home Controls-Lighting (HCL) application profile สำหรับใช้ควบคุมไฟภายในบ้าน ตัว application profile นี้จะกำหนดจำนวนอุปกรณ์และฟังก์ชั่นที่จะเป็นสำหรับควบคุมไฟ เช่น switch, dimmer, occupancy sensors และ ตัวควบคุมโหลด 

|  |  |  |
| --- | --- | --- |
| http://www.bloggang.com/data/z/zol/picture/1297758840.jpg |  | Application profile ก็แบ่งออกเป็น 2 ประเภท คือ public profile กับ private profile กรณีใช้ public profile อุปกรณ์ก็จะมีสมบัติ interoperability (ใช้ข้ามยี่ห้อ)  http://www.bloggang.com/data/z/zol/picture/1297759074.jpg  Device Description จะถูกบรรยายไว้ในแต่ละ application profile พูดถึงชนิดของอุปกรณ์ที่ profile ดังกล่าวสนับสนุน เช่นใน HCL profile ก็จะมีอุปกรณ์พวก Switch Remote Control, Light Sensor Monochromatic, Dimmer Remote Control ให้ใช้ และแต่ละ device ใน application profile ก็จะมีตัว device identifier เฉพาะเจาะจงของมัน |

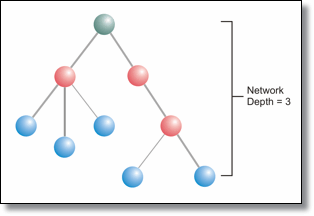
ลองดูตัวอย่าง device ที่ชื่อ Switch Remote Control (SRC) ตัวมันเองก็คือ endpoint ตัวหนึ่ง ซึ่งเราบรรยายข้อมูลที่ส่งถึงกันได้ดังรูปด้านล่าง ใน ZigBee เราเรียกข้อมูลที่ส่งระหว่าง device ว่า attribute แต่ละ attribute ก็มี identifier เฉพาะ และกลุ่มของ attribute ที่จับรวมกันเราเรียกว่า cluster ซึ่งก็ต้องมี identifier เช่นกัน จากรูป ProgramSRC คือ identifier ของคลัสเตอร์ที่ประกอบด้วย 3 attribute ที่มีชื่อ (identifier) ว่า Auto, Override, FactoryDefault อันเป็นข้อมูลที่จะส่งเข้าหรือออกจาก endpoint นี้

|  |  |
| --- | --- |
| http://www.bloggang.com/data/z/zol/picture/1297759943.jpg | http://www.bloggang.com/data/z/zol/picture/1297767463.jpg |

concept ที่น่ารู้อีกอย่างของ ZigBee คือการ binding กล่าวคือ binding เป็นกระบวนการสร้างความสัมพันธ์ (establishing a relationship) ระหว่างโหนดให้สามารถสื่อสารรู้ความกัน binding นี่เป็นการดำเนินการในระดับ endpoint คือ endpoint ไหน request ที่จะ bind กับ endpoint ไหน เช่น โหนดแรกเป็น switch unit มี 2 endpoints แต่ละ endpoints แทนสวิตช์ 1 อัน โหนดที่สองเป็น lamp unit มี 4 endpoints แต่ละ endpoint คือหลอดไฟ 1 หลอด จากรูป switch 1 บายด์กับหลอดไฟ 4 แบบ 1 ต่อ 1 ส่วน switch 2 บายด์กับหลอดไฟ 1 2 3 สร้างความสัมพันธ์แบบ one to many ซึ่งรูปแบบความสัมพันธ์ของการ bind นี้อาจเป็น 1-1, 1-many, many-1 หรือ many-many ก็ได้ทั้งนั้น  
เกี่ยวกับ reliability และ security นั้น ZigBee เตรียมไว้ให้พอสมควร เทคนิคที่ใช้สร้างความมั่นใจเกี่ยวกับ reliable ของการสื่อสารมี 3 เทคนิค

1. ตรวจสอบว่า channel ถูกใช้งานอยู่รึเปล่า ถ้ามีใครใช้อยู่มันก็ไม่ส่ง (อาจหน่วงเวลาด้วยเวลาสุ่ม) จากนั้นก็ตรวจสอบการใช้งานช่องสื่อสารอีกที มันจะส่งเมื่อช่องสื่อสารว่างครับ

2. การใช้ acknowledgement เพื่อยืนยันว่าข้อมูลที่ส่งไปถึงปลายทางแล้ว

3. alternative route กรณีพวก intermediate node ล่ม เน็ตเวิร์กสามารถ "discover" และกำหนดเส้นทางใหม่ได้ ด้านความปลอดภัยก็มี 3 มาตรการ 1. การเข้ารหัส (AES) ข้อมูลที่ต้นทางและถอดรหัสข้อมูลที่ปลายทาง การถอดและเข้ารหัสใช้คีย์เดียวกัน 2. message timeout มีการใส่ frame counter เข้าไปใน message เพื่อให้ตัวรับรู้ message นั้นอายุเท่าไร เก่าใหม่ timeout ไปรึยัง และ 3. access control list ก็คือการทำบัญชีของ MAC address ที่อนุญาตให้เข้ามา join ในเครือข่ายนั่นแหละครับ  
ใน ZigBee นั้น เน็ตเวิร์กถูกเริ่มต้นด้วยตัวแม่ (coordinator) และมีสมบัติหลายอย่างที่สามารถ pre-configure ก่อน initialize ได้ เช่น maximum network depth หมายถึงจำนวน hop สูงสุดจากตัวแม่ไปยังลูกที่อยู่ไกลที่สุด (ดูรูป), จำนวนลูก, จำนวน routers  
  
  
  
การ form เน็ตเวิร์กของตัวแม่ มี 3 ขั้นตอนหลัก

1. ค้นหาช่องสัญญาณวิทยุที่เหมาะสม ถ้าเราไม่ได้กำหนดเอาไว้ว่าช่องไหน มันจะเลือกช่องที่มี activity น้อยที่สุด

2. กำหนด PAN ID ซึ่ง PAN ID นี้เราจะกำหนดไว้ก่อนล่วงหน้าเองก็ได้ หรือตรวจจับเน็ตเวิร์กใกล้เคียงเพื่อไม่ให้เกิดปัญหา PAN ID ซ้ำกัน จากนั้นตัวเองจะกำหนด short address ให้กับตัวเอง (address ใน ZigBee มีแบบยาว 64 บิต คือ MAC address กับแบบสั้น short address 16 บิต ซึ่งตัวแม่เป็นตัวกำหนดให้กับตัวลูกแต่ละตัว) โดยทั่วไปตัวแม่จะมี address ที่ 0x000 สุดท้าย

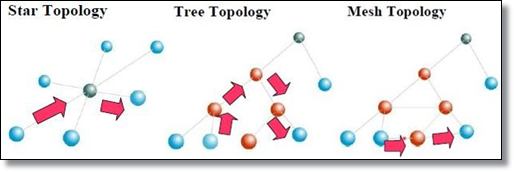
3. เริ่มเน็ตเวิร์ก หมายถึงสภาวะที่พร้อมสำหรับรับการ join จากลูก ๆ

ตัวลูกนั้น ในการ join เน็ตเวิร์ก มี 4 ขั้นตอนหลัก

1. หลังจากเปิดทำงานมันจะหาค้นหาเน็ตเวิร์ก ถ้าเราไม่กำหนดช่องสัญญาณ มันจะหาช่องที่สัญญาณดีที่สุด ถึงแม้เรากำหนดช่องสัญญาณ แต่ช่องสัญญาณเดียวกันอาจมีหลายเน็ตเวิร์กก็ได้ ลูกก็จะเลือกแม่ที่แรงที่สุด ฉะนั้นหลังจากค้นหาสัญญาณมันก็ทำการ

2. เลือกตัวแม่

3. ส่งสัญญาณขอเข้าร่วมเน็ตเวิร์กไปยังตัวแม่

4. ถ้าตัวแม่พร้อมทำงาน แม่จะกำหนด short address ให้มันเพื่อให้อุปกรณ์ในเครือข่ายใช้สื่อสาร ถ้าแม่ไม่พร้อม ตัวลูกจะได้รับ reject join request  
  
เมื่อเราได้เน็ตเวิร์กแล้ว ลักษณะของการส่งข้อมูล หรือ message propagation ก็สอดคล้องกับ topology และ 802.15.4 คือ RFD คุยกับ FFD ได้เพียงตัวเดียว ส่วน FFD คุยกันเองกี่ตัวก็ไม่เป็นปัญหาแต่ประการใด  
  


**การ Routing ของ Zigbee ที่ต่อแบบ Mash**

Protocol ที่ใช้ในการ Route คือ Ad hoc On-Demand Distance Vector (AODV) Routing

การ Route ของ AODV จะทำที่ชั้น Network Layer

ขั้นตอนคือ

1. Source Node (โหนดต้นทาง) จะส่ง RREQ (Route Request packet) แบบ broadcast ไปยังโหนดทุกโหนดที่อยู่ใกล้เคียง แล้วโหนดที่ได้รับ RREQ ก็จะทำการเก็บ Address ของโหนดต้นทางและโหนดอันก่อนหน้า ที่ส่ง RREQ มาหามันไว้ใน Routing Table ทุกๆโหนดก็จะทำแบบนี้เช่นกันจนกว่าจะถึง Destination Node

(โหนดปลายทาง) ในแต่ละครั้งที่เปลี่ยน โหนด จะมีการเก็บ Hop Count ไว้ปลายทางจะเลือกทางที่มี Hop Count น้อยที่สุดแล้วส่ง RREP (Route Reply packet) กลับไปที่เส้นทางนั้น

\*\*\*ถ้าหากระหว่างทางมีการเกิด Circle ตรวจสอบได้จาก Boradcast id ถ้าหาก Boradcast id ซ้ำ มันจะทำการตัดทิ้งไม่เก็บลงใน Routing Table เก็บเพียงอันเดียว

1. เมื่อถึง Destination Node จะส่ง RREP แบบ unicast กลับไปในเส้นทางที่มี Hop Count น้อยที่สุด แต่ถ้ามี Hop Count เท่ากันจะดูที่ broadcast ที่น้อยที่สุด จากนั้น Routing Table ก็จะเก็บ Address ของ Destination Node และ โหนดก่อนหน้ามันเอาไว้ ทำแบบนี้ไปเรื่อยๆจนถึง Source Node ที่ส่ง RREQ
2. เมื่อ Source Node ได้รับ RREP แล้วถึงจะทำการส่ง Data ออกไป