หน่วยที่ 3

แบบจำลองเครือข่ายและโพรโทคอล

สาระสำคัญ

การออกแบบระบบเครือข่ายนั้นจะทำการแบ่งหน้าที่ของการทำงานต่าง ๆ ออกเป็นลำดับชั้น (Layer) โดยที่แต่ละ Layer จะทำการรับข้อมูลจาก Layer ที่สูงกว่าลงมาและส่งผ่านไป Layer ที่ต่ำกว่าลงไปเรื่อย ๆ จนถึง Layer ลำดับล่างสุด ซึ่งจะเป็นตัวกลางทางกายภาพ (Physical Medium) หรือสายสัญญาณที่ใช้ทำการส่งข้อมูลกันจริง ๆ มักจะมองว่า เกิดการสื่อสารกันระหว่าง Layer ที่มีลำดับตรงกัน กับคอมพิวเตอร์ทั้งสองฝั่งขึ้น ซึ่งจะเรียกว่าการสื่อสารเสมือน (Virtual Communication) ซึ่งการสื่อสารที่เกิดขึ้นจริงจะถูกส่งผ่านตาม Layer บนลงมาจนถึง Layer ลำดับล่างสุด ซึ่งเป็นตัวกลางการสื่อสารและส่งผ่านไปให้คอมพิวเตอร์อีกด้านหนึ่งและผ่าน Layer จากชั้นล่างสุดไปจนถึง Layer ชั้นบนสุดวิธีการที่ Layer ในลำดับที่ตรงกันของเครื่องที่ทำการสื่อสารกัน จะถูกเรียกว่าโพรโทคอล (Protocol) เช่น การคุยผ่านอินเทอร์เน็ต (Internet Relay Chat : IRC) หรือเรียกว่าการแชท (Chat) ซึ่งเหมือนเกิดการสื่อสารขึ้นจริง ระหว่างคู่สนทนาที่อยู่ห่างไกลออกไป แต่ในความเป็นจริงเมื่อเราทำการพิมพ์ข้อความ ข้อความนั้นจะถูกดัดแปลงสัญญาณทางไฟฟ้าและถูกส่งลงไปใน Layer ของการสื่อสารตามตั้งแต่ลำดับล่างสุดไปจนถึงระดับบนสุด ในกรณีนี้โปรแกรม Chat ที่ใช้งานจะต้องมีวิธีการสื่อสาร มีข้อตกลงหรือ Protocol เดียวกัน จึงจะสามารถสื่อสารกันได้และต้องใช้งานผ่านเครื่องบริการ (Server) เพื่อจัดการเกี่ยวกับข้อมูลการคุยผ่านอินเทอร์เน็ต

สาระการเรียนรู้

1. แบบจำลอง OSI สำหรับระบบเครือข่าย
2. แบบจำลอง TCP/IP
3. โพรโทคอล (Protocol) สำหรับเครือข่าย
4. ไอพีแอดเดรส (IP Address) และดีเอ็นเอส (DNS)
5. ใบงานที่ 3 ตั้งค่า IP Address และ Subnet
6. ใบงานที่ 4 การแชร์ทรัพยากรบนเครือข่าย (Network Sharing)

จุดประสงค์การเรียนรู้

จุดประสงค์ทั่วไป

1. เพื่อให้มีความเข้าใจหลักการของแบบจำลอง OSI แบบจำลอง TCP/IP และโพรโทคอล (Protocol) ในระบบเครือข่ายคอมพิวเตอร์

2. เพื่อให้มีคุณธรรม จริยธรรมในงานอาชีพและตระหนักถึงคุณค่าของปรัชญาเศรษฐกิจพอเพียง

จุดประสงค์เชิงพฤติกรรม

ด้านความรู้ (ทฤษฎี)

1. อธิบายหลักการของแบบจำลอง OSI ได้ถูกต้อง
2. อธิบายหลักการของแบบจำลอง TCP/IP ได้ถูกต้อง
3. อธิบายหลักการของโพรโทคอล (Protocol) ได้ถูกต้อง
4. อธิบายหลักการไอพีแอดเดรส (IP Address) และดีเอ็นเอส (DNS) ได้ถูกต้อง

แบบทดสอบก่อนเรียน
หน่วยที่ 3 แบบจำลองเครือข่ายและโพรโทคอล

คำชี้แจง

1. ให้ทำเครื่องหมายกากบาท (×) ลงบนกระดาษคำตอบข้อที่ถูกที่สุดเพียง 1 ข้อ
2. แบบทดสอบมีจำนวน 12 ข้อ ให้ทำทุกข้อ
3. เวลา 12 นาที

---

1. Layer ระดับบนของ OSI Model คือข้อใด
   - ก. Network Layer
   - ข. Data Link Layer
   - ค. Application Layer
   - ง. Presentation layer
   - จ. Session Layer
2. Layer ใดที่เกี่ยวกับแรงดันไฟฟ้า มีการเชื่อมต่อสายและมีระยะเวลาในการส่งข้อมูลแต่ละ Bit
   - ก. Presentation layer
   - ข. Transport Layer
   - ค. Session Layer
   - ง. Data Link Layer
   - จ. Physical Layer
3. ข้อใดหมายถึง Presentation Layer
   - ก. เกี่ยวกับรูปแบบของข้อมูลการเข้ารหัส ถอดรหัส เพื่อให้คอมพิวเตอร์สามารถสื่อสารกันได้
   - ข. การควบคุมเทอร์มินอล ชนิดต่าง ๆ รูปแบบการแสดงผลทางจอภาพอาจมีความแตกต่างกัน
   - ค. การหาเส้นทางเพื่อพิจารณาว่า Packet จะถูกส่งจากต้นทางไปยังปลายทางได้อย่างไร
   - ง. ทำการควบคุม การส่งข้อมูลดิบให้เหมือนกับว่าไม่มีข้อผิดพลาดเกิดขึ้น
   - จ. ทำการถ่ายโอนไฟล์ระหว่างเครื่องและยังทำหน้าที่เกี่ยวกับการซิงโครไนซ์เซชั่น

4. TCP/IP พัฒนาขึ้นมาเพื่อจุดประสงค์ในข้อใด
   ก. สำหรับใช้งานจดหมายอิเล็กทรอนิกส์
   ข. ตรวจสอบความถูกต้อง ของข้อมูล
   ค. สามารถหาเส้นทางที่จะส่งข้อมูลไปได้เองโดยอัตโนมัติ
   ง. ติดต่อสื่อสารระหว่างระบบที่มีความแตกต่างกัน
   จ. เพื่อคอยแยกข้อมูล ให้มีขนาดพอเหมาะ
5. Internet Protocol (IP) ทำหน้าที่เกี่ยวกับอะไร
   ก. ใช้เป็นข้อมูลสำหรับอุปกรณ์จัดเส้นทาง (Router)
   ข. จัดการเกี่ยวกับ Address, Data และควบคุมการส่งข้อมูล
   ค. การรับข้อมูลจากชั้นสื่อสาร IP มาแล้วส่งไปยัง Node
   ง. จัดการเกี่ยวกับ Packet
   จ. เข้ารหัสข้อมูล
6. ขนาด Header ของ IP คือข้อใด
   ก. 10 Bytes
   ข. 20 Bytes
   ค. 32 Bytes
   ง. 64 Bytes
   จ. 128 Bytes
7. Protocol ที่ทำหน้าที่แปลงข้อมูลชื่อเว็บไซต์หลายให้เป็นหมายเลข IP Address คือข้อใด
   ก. DNS
   ข. SNMP
   ค. DHCP
   ง. Packet
   จ. FTP
8. File Transfer Protocol (FTP) ด้านServer ใช้ Port ใดในการสื่อสาร
   ก. 67
   ข. 161
   ค. 21
   ง. 80
   จ. 53

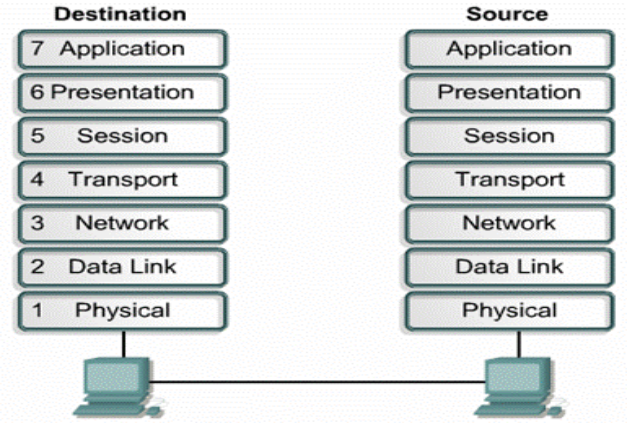
9. โพรโทคอลที่ใช้สำหรับการบริการด้าน Web คือข้อใด
   ก. DNS
   ข. HTTP
   ค. SNMP
   ง. DHCP
   จ. FTP
10. IP หมายเลข 10.0.5.130 อยู่ในกลุ่ม IP Class ใด
   ก. Class E
   ข. Class C
   ค. Class D
   ง. Class A
   จ. Class B
11. ข้อใด หมายถึง IP Address
   ก. หมายเลข ประจำเครื่องคอมพิวเตอร์
   ข. เครือข่ายของผู้ให้บริการอินเตอร์เน็ต
   ค. โพรโตคอลสำหรับโอนย้ายข้อมูล
   ง. การตั้งชื่อเป็นตัวอักษรเพื่อใช้แทน IP
   จ. www.technicphrae.ac.th
12. โดเมนเมนนี้ www.electronic.ac.th เป็นโดเมนประเภทใด
   ก. เครือข่ายของเอกชน
   ข. เครือข่ายของผู้ให้บริการอินเตอร์เน็ต
   ค. เครือข่ายของหน่วยงานรัฐบาล
   ง. เครือข่ายขององค์กรที่ไม่มุ่งหวังกำไร
   จ. เครือข่ายของหน่วยงานการศึกษา

เนื้อหาสาระ

1. แบบจำลองของ OSI (OSI Model)

การสื่อสารระหว่างคอมพิวเตอร์เครื่องหนึ่งจะส่งข้อมูลไปยังคอมพิวเตอร์อีกเครื่องหนึ่งได้นั้นจะต้องอาศัยกลไกหลาย ๆ อย่างร่วมกัน ทำงานต่างหน้าที่กันและเชื่อมต่อเป็น Network เข้า ด้วยกัน ปัญหาที่เกิดขึ้นคือการเชื่อมต่อมีความแตกต่าง ระหว่างระบบและอุปกรณ์หรือเป็นบริษัทผู้ผลิตต่างกัน ซึ่งเป็นสิ่งที่ทำให้การสร้าง Network เป็นเรื่องที่ยุ่งยาก เนื่องจากขาดมาตรฐานกลางที่จำเป็นในการเชื่อมต่อจึงได้เกิดหน่วยงานกำหนดมาตรฐานสากลขึ้นคือ International Standards Organization (ISO) ขึ้นและทำการกำหนดโครงสร้างทั้งหมดที่จำเป็นต้องใช้ ในการสื่อสารข้อมูลและเป็นระบบเปิดเพื่อให้ผู้ผลิตต่าง ๆ สามารถแยกผลิตในส่วนตามความสามารถและนำไปใช้ร่วมกันได้ ระบบ Network คอมพิวเตอร์ที่ใช้ปัจจุบัน จะถูกออกแบบให้มีโครงสร้างที่แน่นอน และเพื่อเป็นการลดความซับซ้อนเครือข่ายส่วนมากจึงแยกการทำงานออกเป็นชั้น ๆ (Layer) กำหนดหน้าที่ในแต่ละชั้นไว้อย่างชัดเจน แบบจำลองสำหรับอ้างอิงแบบ Open System Interconnection Reference Model (OSI) หรือที่นิยมเรียกกันทั่วไปว่า OSI Reference Model ของ ISO เป็นแบบจำลองที่ถูกเสนอและพัฒนาโดยองค์กร ISO โดยบรรยายถึงโครงสร้างของสถาปัตยกรรม เครือข่ายในอุดมคติ ซึ่งระบบเครือข่ายที่เป็นไปตามสถาปัตยกรรมนี้จะเป็นระบบเครือข่ายแบบเปิดและอุปกรณ์ทางเครือข่ายจะสามารถติดต่อกันได้ โดยไม่ขึ้นกับว่าเป็นอุปกรณ์ของผู้ขายรายใด แบบ จำลองสำหรับอ้างอิงแบบ OSI แสดงดังภาพที่ 3.1 และภาพที่ 3.2

ภาพที่ 3.1 แบบจำลองสำหรับอ้างอิง OSI
ที่มา : เอกชัย ไก่แก้ว (2556)



ภาพที่ 3.2 การสื่อสารระหว่างคอมพิวเตอร์ผ่าน OSI Model
ที่มา : เอกชัย ไก่แก้ว (2556)

1.1 การส่งผ่านข้อมูลระหว่างชั้น

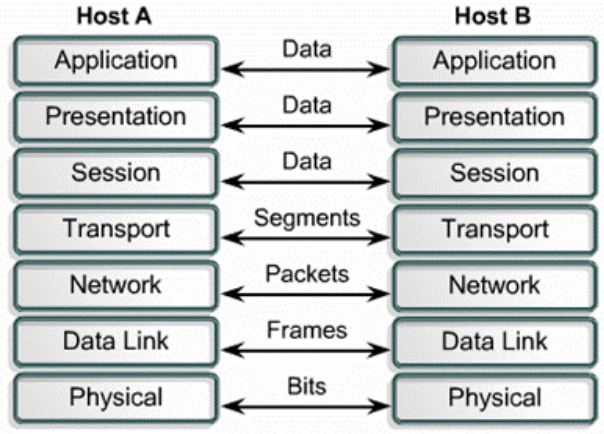
เมื่อ Computer A ต้องการส่งข้อมูลไปยัง Computer B จะมีกระบวนการทำงานต่าง ๆ ตามลำดับดังนี้

1.1.1 ข้อมูลจาก Layer 7, 6, 5 จะถูกนำมาแยกเป็นส่วน ๆ แล้วใส่ข้อมูลเพิ่มเข้าไปในส่วนหัว เรียกว่า Header เพื่อใช้ในการบันทึกข้อมูลที่จำเป็นเช่น หมายเลข Port ต้นทางและหมายเลข Port ปลายทางรวมมาเป็นกลุ่มข้อมูล (Data Segment) ใน Layer 4 ซึ่งเรียกว่า TCP Segment

1.1.2 จากนั้นข้อมูล Layer 4 จะถูกส่งผ่านลงไปยัง Layer 3 และจะถูกใส่ Header อีกซึ่งเป็นการเพิ่ม Header เป็นชั้น ๆ เรียกว่าการ Encapsulate ซึ่งในส่วนนี้จะเหมือนกับการเอาเอกสารใส่ซองจดหมายแล้วจ่าหน้าซองระบุผู้ส่งและผู้รับ คือเป็นการบันทึกหมายเลข IP Address ของ Host ต้นทางและ Host ปลายทางไว้ด้วย เมื่อการ Encapsulate เสร็จสิ้นจะได้ Data Segment ที่เรียกว่า Packet

1.1.3 ข้อมูล Packet จะถูกส่งผ่านไปยังระดับล่างอีก คือส่งไปให้ Layer 2 ในชั้นนี้ข้อมูลจะถูกใส่ Header เพิ่มเข้าไปที่ส่วนหัวเพื่อเก็บ MAC Address ของต้นทางและปลายทางและยังมีการใส่ข้อมูลต่อเพิ่มเข้าไปในส่วนท้ายด้วย ข้อมูลที่ต่อเพิ่มไปในส่วนท้ายนี้เรียกว่า Trailer จึงรวมกันกลายเป็น Data Segment ของ Layer 2 ที่เรียกว่า Frame

1.1.4 ข้อมูล Frame จะถูกแปลงให้เป็น Bit ของข้อมูลเพื่อส่งไปตามสื่อเช่น สาย UTP, Fiber Optic ต่อไป การส่งสัญญาณทางไฟฟ้าไปตามสื่อต่าง ๆ นี้ เป็นการทำงานในระดับ Layer 1 เรียกว่า Physical Layer แสดงดังภาพที่ 3.3

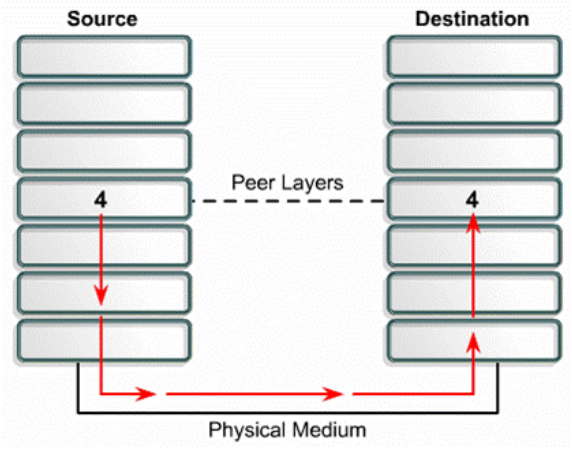


ภาพที่ 3.3 การส่งผ่านข้อมูลระหว่างชั้น
ที่มา : เอกชัย ไก่แก้ว (2556)

1.2 OSI Model ได้แบ่ง ตามลักษณะของการทำงานออกเป็น 2 กลุ่มใหญ่ ได้แก่

1.2.1 Application Oriented Layers เป็น 4 Layer ด้านบนคือ Layer ที่ 7, 6, 5, 4 ทำหน้าที่เชื่อมต่อรับ ส่งข้อมูลระหว่างผู้ใช้กับโปรแกรมประยุกต์ เพื่อให้รับส่งข้อมูลกับ Hard ware ที่อยู่ชั้นล่างได้อย่างถูกต้อง ซึ่งจะเกี่ยวข้องกับ Soft ware เป็นหลัก

1.2.2 Network Dependent Layers เป็น 3 Layers ด้านล่าง ทำหน้าที่เกี่ยวกับการรับส่งข้อมูลผ่านสายส่งและควบคุมการรับส่งข้อมูลตรวจสอบข้อผิดพลาด รวมทั้งเลือกเส้นทางที่ใช้ในการรับส่ง ซึ่งจะเกี่ยวข้องกับ Hard ware เป็นหลัก ทำให้ใช้ผลิตภัณฑ์ต่างบริษัทกันได้อย่างไม่มีปัญหา แสดงดังภาพที่ 3.4



ภาพที่ 3.4 แบ่ง OSI Model ออกเป็น 2 กลุ่ม
ที่มา : เอกชัย ไก่แก้ว (2556)

1.3 แบบจำลองสำหรับอ้างอิงแบบ OSI (Open System Interconnection Reference Model) หรือที่นิยมเรียกกันทั่วไปว่า OSI Reference Model โดยจะบรรยายถึงโครงสร้างของสถาปัตยกรรมเครือข่ายในอุดมคติ สถาปัตยกรรมนี้จะเป็นระบบเครือข่ายแบบเปิดและอุปกรณ์ทางเครือข่ายยังสามารถติดต่อกันได้โดยไม่ขึ้นกับว่าเป็นอุปกรณ์ของผู้ขายรายใด แบบจำลองสำหรับอ้างอิงแบบ OSI แบ่งการทำงานออกเป็น Layer ดังนี้

1.3.1 Layer 1 : Physical Layer ชั้นนี้จะเกี่ยวข้องกับการส่งข้อมูลระดับ Bit ผ่าน ช่องสื่อสารข้อมูล โดยการออกแบบจะต้องแน่ใจว่าจะสามารถส่งข้อมูลออกไป และปลายทางจะต้องรับข้อมูลนั้นได้อย่างถูกต้อง โดยส่วนใหญ่จะเป็นข้อกำหนดเกี่ยวกับเรื่องของแรงดันไฟฟ้า ว่าจะต้องใช้แรงดันเท่าไรสำหรับแทนเลข "1" และเท่าใดสำหรับแทนเลข "0" ระยะเวลาในการส่งแต่ละ Bit จะต้องห่างกันเท่าใด รวมถึงรูปแบบของ Connector วิศวกรไฟฟ้าจะเกี่ยวข้องโดยตรงกับ Layer ในลำดับชั้นนี้

1.3.2 Layer 2 : Data Link Layer จุดประสงค์หลักของ Layer นี้คือ จะทำการควบคุม การส่งข้อมูลดิบให้เหมือนกับว่าไม่มีข้อผิดพลาดเกิดขึ้น ทำให้ Layer ในลำดับถัดไปไม่ต้องสนใจในเรื่องนี้ วิธีการคือจะต้อง ทำการแตกข้อมูลออกเป็นก้อนๆเรียกว่า เฟรมข้อมูล (Data Frame) แล้วทำการส่งออกไปทีละชุดและรอการตอบรับ (Acknowledge Frame) กลับมาในกรณีที่มีสัญญาณรบกวนทำให้สัญญาณขาดหายไป จะต้องมีการบอกให้เครื่องต้นทางทำการส่งข้อมูลที่หายไปนั้นกลับมาให้ใหม่ นอกจากนี้จะต้องมีการพักข้อมูลไว้ใน Buffer หากความเร็วในการส่งข้อมูลของทั้งสองฝ่ายไม่เท่ากัน

1.3.3 Layer 3 : Network Layer หน้าที่หลักของ Layer นี้จะเกี่ยวข้องกับการหาเส้นทาง (Route) เพื่อพิจารณาว่า Packet จะถูกส่งจากต้นทางไปยังปลายทางได้อย่างไร การกำหนดเส้นทางอาจจะ กำหนดตั้งแต่เริ่มต้นการติดต่อหรือสามารถเปลี่ยนแปลงได้ตลอดเวลา (Dynamic) นอกจากหากมีการส่งข้อมูลข้ามเครือข่าย Network Layer จะต้องทำการจัดการปัญหาเกี่ยวกับ ความแตกต่างระหว่างเครือข่ายหรือใช้ Protocol แตกต่างกัน เพื่อให้แต่ละเครือข่ายสามารถเชื่อมต่อกันได้ เสมือนเป็นเครือข่ายเดียวกัน

1.3.4 Layer 4 : Transport Layer ใน Layer นี้จะคอยทำการติดต่อกับ Layer ถัดไป (Session Layer) เพื่อคอยแยกข้อมูล ให้มีขนาดพอเหมาะและส่งต่อให้กับ Network Layer พร้อมทั้งตรวจสอบว่าข้อมูลได้ถูกส่งไปถึงยังปลายทางได้อย่างเรียบร้อยหรือไม่ โดย Layer นี้จะต้องจัดการได้อย่างมีประสิทธิภาพเพื่อเป็นการแยกให้ Session Layer เป็นอิสระจากการเปลี่ยนแปลงทางด้าน Hardware

1.3.5 Layer 5 : Session Layer นอกจากจะทำการส่งข้อมูลแบบเดียวกับ Transport - Layer แล้ว ยังมีการให้บริการอื่น ๆ เช่น การยอมให้ผู้ใช้งานเข้าไปใช้งานยังเครื่องที่อยู่ห่างไกลออกไป (Remote Login) หรือทำการถ่ายโอนไฟล์ระหว่างเครื่องและยังทำหน้าที่เกี่ยวกับการซิงโครไนซ์เซชั่น (Synchronization) หรือทำให้สองระบบทำงานอย่างสัมพันธ์กัน

1.3.6 Layer 6 : Presentation layer สำหรับ Layer นี้จะสนใจในเรื่องของรูปแบบของข้อมูล เช่นการเปลี่ยนรหัสข้ามจาก ASCII เป็นรหัส EBCDIC เพื่อทำให้คอมพิวเตอร์ที่มีการเข้ารหัสต่างกันสามารถสื่อสารกันได้ นอกจากนี้ก็อาจทำการลดขนาดของข้อมูล (Data Compression) หรือทำการเข้ารหัสของข้อมูล (Data Encryption) เพื่อป้องกันการโจรกรรมข้อมูลได้ด้วย

1.3.7 Layer 7 : Application layer ในส่วน Layer บนสุดจะเกี่ยวข้องกับ Protocol มากมาย ซึ่งจะมีการใช้งานที่แตกต่างกันโดยเฉพาะ ตัวอย่างเช่นการควบคุมเทอร์มินอล (Terminal) ชนิดต่าง ๆ รูปแบบการแสดงผลทางจอภาพอาจมีความแตกต่างกัน ก็อาจมีการกำหนด Terminal เสมือนเพื่อเป็นตัวกลาง ในการควบคุมการทำงานของ Terminal

ARPANET : Advanced Research Project Agency Network เกิดจากโครงการวิจัยทางการทหารของกระทรวงกลาโหมของสหรัฐอเมริกาโดยเริ่มต้นจากมหาวิทยาลัยบางแห่ง และเพิ่มจำนวนขึ้นมากเรื่อย ๆ (ปัจจุบันเป็นระบบ Internet) ARPANET ไม่ได้มีการแบ่งรูปแบบตามแบบของ OSI เนื่องจากมีการใช้งานก่อนกำหนดมาตรฐาน OSI เกือบ 10 ปี Protocol การสื่อสารระหว่าง IMP จะเป็นการผสมผสานระหว่าง Layer 2 และ Layer 3 นอกจากนี้ยังมีกระบวนการตรวจสอบความถูกต้องของข้อมูลที่ฝั่งรับของ IMP ด้วย ARPANET มี Protocol ที่ทำงานคล้ายในแบบจำลองของ OSI ที่ Network Layer และ Transport Layer เรียกว่า IP (Internet Protocol) มีลักษณะแบบ Connectionless และถูกออกแบบมาให้ต่อกับ LAN และ WAN ที่ต่อกับ ARPA Internet Protocol ของ ARPANET ที่ Transport Layer ทำงานแบบ Connection Oriented เรียกว่า TCP (Transmission Control Protocol) ซึ่งจะคล้าย ๆ กับ Protocol ของ OSI ที่ Transport Layer แต่มีความแตกต่างกันในด้านรายละเอียด และ TCP ถูกใช้งานอย่างแพร่หลายมากในระบบปฏิบัติการตระกูล UNIX ARPANET ในระยะแรกไม่มี Session และ Application Protocol แต่ภายหลังก็มี Application Protocol ต่าง ๆ ซึ่งไม่ได้มีโครงสร้างแบบเดียวกับ OSI บริการที่มีเช่น FTP (File Transfer Protocol) หรือการถ่ายโอนไฟล์ SMTP (Simple Mail Transfer Protocol) สำหรับใช้งานจดหมายอิเล็กทรอนิกส์ และ TELNET สำหรับการขอใช้งานจากระยะไกล ในระยะหลัง ๆ เมื่อ ARPANET ได้กลายเป็น Internet แล้ว ได้มีการพัฒนา Application Protocol ขึ้นมามากตามมาภายหลัง เช่น HTTP, NNTP เป็นต้น

2. แบบจำลอง TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) เป็นชุดของ Protocol ที่ถูกใช้ในการสื่อสารผ่าน Internet โดยมีวัตถุประสงค์เพื่อให้สามารถใช้สื่อสารจากต้นทางข้ามเครือข่าย ไปยังปลายทางได้ และสามารถหาเส้นทางที่จะส่งข้อมูลไปได้เองโดยอัตโนมัติ ถึงแม้ว่าในระหว่างทางอาจจะผ่านเครือข่ายที่มีปัญหา Protocol ก็ยังคงหาเส้นทางอื่นในการส่งผ่านข้อมูลไปให้ถึงปลายทางได้ ชุด Protocol นี้ได้รับการพัฒนามาตั้งแต่ปี 1960 ซึ่งใช้เป็นครั้งแรกในเครือข่าย ARPANET ซึ่งต่อมาได้ขยายการเชื่อมต่อไปทั่วโลกเป็น Internet ทำให้ TCP/IP เป็นที่ยอมรับจนถึงปัจจุบัน

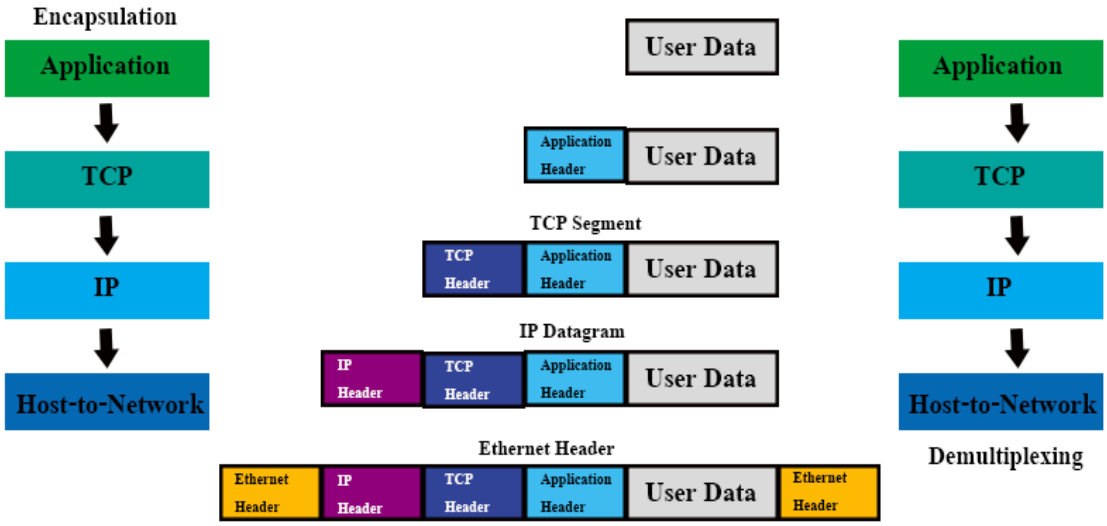
จุดประสงค์ของ TCP/IP ในการสื่อสารคือ

1) เพื่อใช้ติดต่อสื่อสารระหว่างระบบที่มีความแตกต่างกัน

2) ความสามารถในการแก้ไขปัญหาที่เกิดขึ้นในระบบเครือข่ายเช่นในกรณีที่ผู้ส่งและผู้รับยังคงมีการติดต่อกันอยู่แต่ Node กลางที่ใช้เป็นผู้ช่วยในการรับส่งเกิดเสียหายใช้การไม่ได้หรือสายนำสัญญาณบางช่วงถูกตัดขาด กฎการสื่อสารนี้จะต้องสามารถจัดหาทางเลือกอื่นเพื่อทำให้การสื่อสารดำเนินต่อไปได้โดยอัตโนมัติ

3) มีความคล่องตัวต่อการสื่อสารข้อมูลได้หลายชนิดทั้งแบบที่ไม่มีความเร่งด่วน เช่น การจัดส่งแฟ้มข้อมูล และแบบที่ต้องการรับประกันความเร่งด่วนของข้อมูล เช่น การสื่อสารแบบ Real Time และทั้งการสื่อสารแบบเสียง (Voice) และข้อมูล (Data)

การสื่อสารข้อมูลในแต่ละ Layer ผ่าน TCP/IP เริ่มต้นตั้งแต่การ Encapsulation ไปจนถึงขั้นตอนสุดท้าย Demultiplexing แสดงดังภาพที่ 3.5



ภาพที่ 3.5 ขั้นตอนการ Encapsulation และ Demultiplexing

ที่มา : เอกชัย ไก่แก้ว (2556)

การส่งข้อมูลผ่านในแต่ละ Layer โดยแต่ละ Layer จะทำการประกอบข้อมูลที่ได้รับมากับข้อมูลส่วนควบคุมซึ่งถูกนำมาไว้ในส่วนหัวของข้อมูลเรียกว่า Header ภายใน Header จะบรรจุข้อมูลที่สำคัญของ Protocol ที่ทำการ Encapsulate เมื่อผู้รับได้รับข้อมูล ก็จะเกิดกระบวนการทำงานย้อนกลับคือ Protocol เดียวกัน ทางฝั่งผู้รับก็จะได้รับข้อมูลส่วนที่เป็น Header ก่อนและนำไปประมวลและได้ข้อมูลว่ามีลักษณะอย่างไร ซึ่งกระบวนการย้อนกลับนี้เรียกว่า Demultiplexing

ข้อมูลที่ผ่านการ Encapsulate ในแต่ละ Layer มีชื่อเรียกแตกต่างกัน ดังนี้

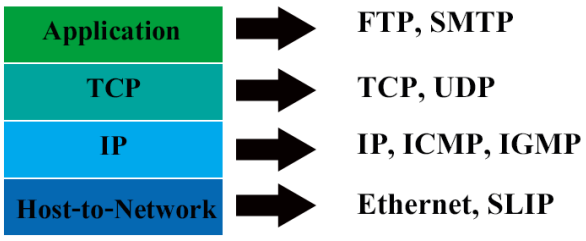
1) ข้อมูลที่มาจาก User หรือก็คือข้อมูลที่ User เป็นผู้ป้อนให้กับ Application เรียกว่า User Data

2) เมื่อ Application ได้รับข้อมูลจาก User จะนำมาประกอบกับส่วนหัวของ Application เรียกว่า Application Data และส่งต่อไปยัง Protocol TCP

3) เมื่อ Protocol TCP ได้รับ Application Data ก็จะนำมารวมกับ Header ของ Protocol TCP เรียกว่า TCP Segment และส่งต่อไปยังProtocol IP

4) เมื่อ Protocol IP ได้รับ TCP Segment ก็จะนำมารวมกับ Header ของ Protocol IP เรียกว่า IP Datagram และส่งต่อไปยัง Layer Host to Network Layer

5) ในระดับ Host to Network จะนำ IP Datagram มาเพิ่มส่วน Error Correction และ Flag เรียกว่า Ethernet Frame ก่อนจะแปลงข้อมูลเป็นสัญญาณไฟฟ้าส่งผ่านสายสัญญาณที่เชื่อมโยงอยู่ต่อไปในแต่ละ Layer ของโครงสร้าง TCP/IP แสดงดังภาพที่ 3.6



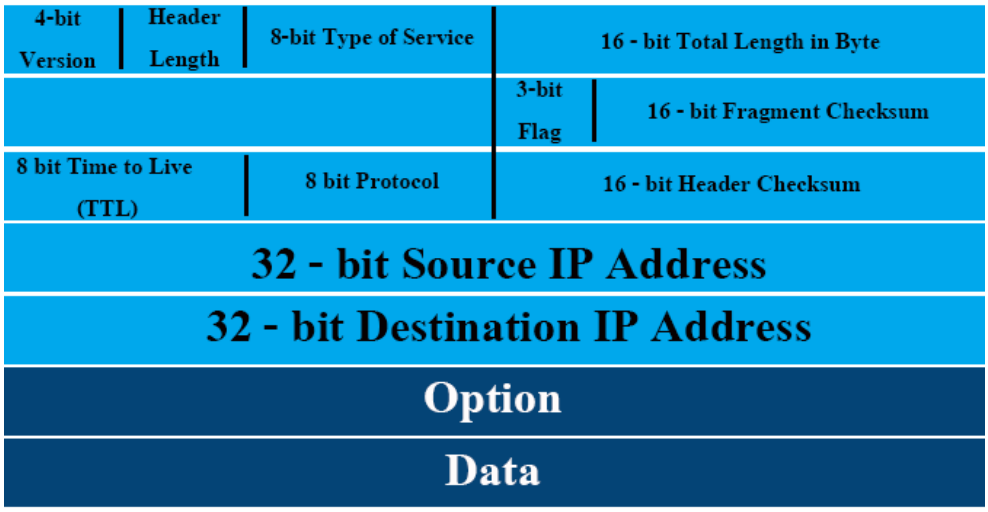
ภาพที่ 3.6 โครงสร้าง TCP/IP
ที่มา : เอกชัย ไก่แก้ว (2556)

หลักการทำงานตามโครงสร้าง TCP/IP มีดังนี้

2.1 ชั้น Host Network (Host to Network Layer) Protocol สำหรับการควบคุมการสื่อสาร ในชั้นนี้ ไม่มีการกำหนดรายละเอียดอย่างเป็นทางการ หน้าที่หลักคือการรับข้อมูลจากชั้นสื่อสาร IP มาแล้วส่งไปยัง Node ที่ระบุไว้ในเส้นทางเดินข้อมูลทางด้านผู้รับก็จะทำงานในทางกลับกัน คือรับข้อมูลจากสายนำสัญญาณแล้วนำส่งให้กับโปรแกรมในชั้นสื่อสาร

2.2 ชั้นสื่อสารอินเทอร์เน็ต (The Internet Layer) ใช้ประเภทของระบบการสื่อสารที่เรียกว่าระบบเครือข่ายแบบสลับช่องสื่อสารระดับ Packet (Packet Switching Network) ซึ่งเป็นการติดต่อแบบไม่ต่อเนื่อง (Connectionless) หลักการทำงานคือการปล่อยให้ข้อมูลขนาดเล็กเรียกว่า แพ็กเกจ (Packet) สามารถส่งจาก Node ของผู้ส่งไปตาม Node ต่าง ๆ ในระบบจนถึงจุดหมายปลายทางได้โดยอิสระ หากว่ามีการส่ง Packet ออกมาเป็นชุดโดยมีจุดหมายปลายทางเดียวกันในระหว่างการเดินทางในเครือข่าย Packet แต่ละตัวในชุดนี้ก็จะเป็นอิสระแก่กันและกัน ดังนั้น Packet ที่ส่งไปถึงปลายทางอาจจะไม่เป็นไปตามลำดับก็ได้

2.2.1 ไอพี (Internet Protocol : IP) IP เป็น Protocolในระดับ Network Layer ทำหน้าที่จัดการเกี่ยวกับ Address, Data และควบคุมการส่งข้อมูลบางอย่างที่ใช้ในการหาเส้นทางของ Packet กลไกในการหาเส้นทางของ IP จะมีความสามารถในการหาเส้นทางที่ดีที่สุดและสามารถเปลี่ยนแปลงเส้นทางได้ในระหว่างการส่งข้อมูลและมีระบบการแยกและประกอบดาต้าแกรม (Datagram) เพื่อรองรับการส่งข้อมูลระดับ Data Link ที่มีขนาด MTU (Maximum Transmission Unit) ที่แตกต่างกัน ทำให้สามารถนำ IP ไปใช้บน Protocol อื่นได้หลากหลาย เช่น Ethernet, Token Ring หรือ Apple-Talk การเชื่อมต่อของ IP เพื่อทำการส่งข้อมูลจะเป็นแบบ Connectionless หรือเกิดเส้นทางการเชื่อมต่อในทุก ๆ ครั้งของการส่งข้อมูล 1 Datagram โดยจะไม่ทราบถึงข้อมูล Datagram ที่ส่งก่อนหน้าหรือส่งตามมา แต่การส่งข้อมูลใน 1 Datagram อาจจะเกิดการส่งได้หลายครั้งในกรณีที่มีการแบ่งข้อมูลออกเป็นส่วนย่อย ๆ (Fragmentation) และถูกนำไปรวมเป็น Datagram เดิมเมื่อถึงปลายทาง แสดงดังภาพที่ 3.7



ภาพที่ 3.7 แสดงโครงสร้าง IP Header
ที่มา : เอกชัย ไก่แก้ว (2556)

Header ของ IP โดยปกติจะมีขนาด 20 Bytes ยกเว้นในกรณีที่มีการเพิ่ม Option บางอย่าง Field ของ Header IP จะมีความหมายดังนี้

1) Version : หมายเลขเวอร์ชันของ Protocol ที่ใช้งานในปัจจุบันคือ เวอร์ชัน 4 (IPv4) และเวอร์ชัน 6 (IPv6)

2) Header Length : ความยาวของ Header โดยทั่วไปถ้าไม่มีส่วน Option จะมีค่าเป็น 5 (5*32 Bit)

3) Type of Service (TOS) : ใช้เป็นข้อมูลสำหรับอุปกรณ์จัดเส้นทาง (Router) ในการตัดสินใจเลือกเส้นทาง (Route) ของข้อมูลในแต่ละ Datagram แต่ปัจจุบันไม่ได้นำไปใช้งานแล้ว

4) Length : ความยาวทั้งหมดเป็นจำนวน Byte ของ Datagram ซึ่งมีขนาด 16 Bit ของฟิลด์ (Field) จะหมายถึงความยาวสูงสุดของ Datagram คือ 65535 Byte (64 Kbyte) แต่ในการส่งข้อมูล จริง ข้อมูลจะถูกแยกเป็นส่วน ๆ ตามขนาดของ MTU ที่กำหนดในลิงค์ Layer และนำมารวมกันอีกครั้ง เมื่อส่งถึงปลายทาง Application ส่วนใหญ่จะมีขนาดของ Datagram ไม่เกิน 512 byte

5) Identification : เป็นหมายเลขของ Datagram ในกรณีที่มีการแยก Datagram เมื่อข้อมูลส่งถึงปลายทางจะนำข้อมูลที่มี Identification เดียวกันมารวมกัน

6) Flag : ใช้ในกรณีที่มีการแยก Datagram

7) Fragment Offset : ใช้ในการกำหนดตำแหน่งข้อมูลใน Datagram ที่มีการแยกส่วน เพื่อให้สามารถนำกลับมาเรียงต่อกันได้อย่างถูกต้อง

8) Time to Live (TTL) : กำหนดจำนวนครั้งที่มากที่สุดที่ Datagram จะถูกส่งระหว่าง Hop (การส่งผ่านข้อมูลระหว่างเน็ตเวิร์ก) เพื่อป้องกันไม่ให้เกิดการส่งข้อมูลโดยไม่สิ้นสุด โดยเมื่อข้อมูลถูกส่งไป 1 Hop จะทำการลดค่า TTL ลง 1 เมื่อค่าของ TTL เป็น 0 และข้อมูลยังไม่ถึงปลายทาง ข้อมูล นั้นจะถูกยกเลิกและ Router สุดท้ายจะส่งข้อมูล ICMP แจ้งกลับมายังต้นทางว่าเกิด Time Out ในระหว่างการส่งข้อมูล

9) Protocol : ระบุ Protocol ที่ส่งใน Datagram เช่น TCP ,UDP หรือ ICMP

10) Header Checksum : ใช้ในการตรวจสอบความถูกต้องของข้อมูลใน Header

11) Source IP Address : หมายเลข IP ของผู้ส่งข้อมูล

12) Destination IP Address : หมายเลข IP ของผู้รับข้อมูล

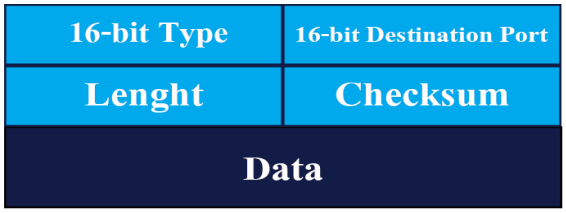
13) Data : ข้อมูลจาก Protocol ระดับบน

2.2.2 ไอซีเอ็มพี (Internet Control Message Protocol : ICMP) ICMP เป็น Protocol ที่ใช้ในการตรวจสอบและรายงานสถานภาพของ Datagram ในกรณีที่เกิดปัญหากับ Datagram เช่น Router ไม่สามารถส่ง Datagram ไปถึงปลายทางได้ ICMP ถูกส่งออกไปยัง Host ต้นทางเพื่อรายงานข้อผิดพลาด ที่เกิดขึ้น อย่างไรก็ดี ไม่มีอะไรรับประกันได้ว่า ICMP Message ที่ส่งไปจะถึงผู้รับจริงหรือไม่ หากมีการส่ง Router ออกไปแล้วไม่มี ICMP Message ฟ้อง Error กลับมา ก็แปลความหมายได้สองกรณีคือ ข้อมูลถูกส่งไปถึงปลายทางเรียบร้อยหรืออาจจะมีปัญหา ในการสื่อสารทั้งการส่ง Router และ ICMP Message ที่ส่งกลับมาก็มีปัญหาระหว่างทางได้ ICMP จึงเป็น Protocol ที่ไม่มีความน่าเชื่อถือ (Unreliable) จะเป็นหน้าที่ของ Protocol ในระดับสูงกว่า Network Layer ในการจัดการให้การสื่อสาร นั้นๆ มีความน่าเชื่อถือ ในส่วนของ ICMP Message จะประกอบด้วย Type ขนาด 8 Bit Checksum ขนาด 16 Bit และส่วนของ Content จะมีขนาดแตกต่างกันตาม Type และ Code แสดงดังภาพที่ 3.8

ภาพที่ 3.8 แสดงโครงสร้าง ICMP Message
ที่มา : เอกชัย ไก่แก้ว (2556)

2.3 ชั้นสื่อสารนำส่งข้อมูล (Transport Layer) แบ่งเป็น Protocol 2 ชนิดคือ ชนิดแรกเรียกว่า Transmission Control Protocol (TCP) เป็นแบบที่มีการกำหนดช่วงการสื่อสารตลอดระยะเวลาการสื่อสาร (Connection Oriented) ซึ่งจะยอมให้มีการส่งข้อมูลเป็นแบบ Byte Stream ที่ไว้ใจได้โดยไม่มีข้อผิดพลาด ข้อมูลที่มีปริมาณมากจะถูกแบ่งออกเป็นส่วนเล็ก ๆ เรียกว่า Message ซึ่งจะถูกส่งไปยังผู้รับผ่านทางชั้นสื่อสารของ Internet ทางฝ่ายผู้รับจะนำ Message มาเรียงต่อกันตามลำดับเป็นข้อมูลตัวเดิม TCP ยังมีความสามารถในการ ควบคุมการไหลของข้อมูลเพื่อป้องกันไม่ให้ผู้ส่ง ส่งข้อมูลเร็วเกินกว่าที่ผู้รับจะทำงานได้ทันอีกด้วย Protocol การนำส่งข้อมูล ชนิดที่สองเรียกว่า UDP (User - Datagram Protocol) เป็นการติดต่อแบบไม่ต่อเนื่อง (Connectionless) มีการตรวจสอบความถูกต้องของข้อมูลแต่จะไม่มีการแจ้งกลับไปยังผู้ส่ง จึงถือได้ว่าไม่มีการตรวจสอบความถูกต้องของข้อมูล อย่างไรก็ตาม วิธีการนี้มีข้อดีในด้านความรวดเร็วในการส่งข้อมูล จึงนิยมใช้ในระบบผู้ให้และผู้ใช้บริการ (Client/Server System) ซึ่งมีการสื่อสารแบบ ถาม ตอบ (Request/Reply) นอกจากนั้นยังใช้ในการส่งข้อมูลประเภทภาพเคลื่อนไหวหรือการส่งเสียง (Voice) Internet

2.3.1 ยูดีพี (User Datagram Protocol : UDP) เป็น Protocol ที่อยู่ในชั้น Transport Layer เมื่อเทียบกับโมเดล OSI โดยการส่งข้อมูลของ UDP นั้นจะเป็นการส่งครั้งละ 1 ชุดข้อมูล เรียกว่า UDP Datagram ซึ่งจะไม่มีความสัมพันธ์กันระหว่าง Datagram และจะไม่มีกลไกการตรวจสอบความสำเร็จ ในการรับส่งข้อมูล กลไกการตรวจสอบโดย Checksum ของ UDP นั้นเพื่อป้องกันข้อมูลที่อาจจะ ถูกแก้ไขหรือมีความผิดพลาดระหว่างการส่งและหากเกิดเหตุการณ์ดังกล่าว ปลายทางจะได้รู้ว่ามีข้อ ผิดพลาดเกิดขึ้น แต่มันจะเป็นการตรวจสอบเพียงฝ่ายเดียวเท่านั้น โดยในข้อกำหนดของ UDP หากพบว่า Checksum Error ก็ให้ผู้รับปลายทางทำการทิ้งข้อมูลนั้น แต่จะไม่มีการแจ้งกลับไปยังผู้ส่งแต่อย่างใด การรับส่งข้อมูลแต่ละครั้งหากเกิดข้อผิดพลาดในระดับ IP เช่น ส่งไม่ถึงหมดเวลา ผู้ส่งจะได้รับ Error Message จากระดับ IP เป็น ICMP Error Message เมื่อข้อมูลส่งถึงปลายทางถูกต้อง แต่เกิดข้อผิดพลาดในส่วนของ UDP จะไม่มีการยืนยันหรือแจ้งให้ผู้ส่งทราบ แสดงดังภาพที่ 3.9



ภาพที่ 3.9 แสดงโครงสร้าง UDP Header
ที่มา : เอกชัย ไก่แก้ว (2556)

จากภาพที่ 3.9 โครงสร้าง UDP Header มีรายละเอียดดังนี้

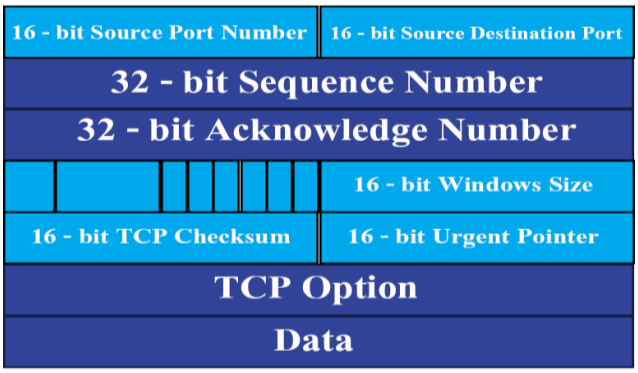
1) Source Port Number : หมายเลข Port ต้นทางที่ส่ง Datagram นี้

2) Destination Port Number : หมายเลข Port ปลายทางที่จะเป็นผู้รับ Datagram

3) UDP Length : ความยาวของ Datagram ทั้งส่วน Header และ Data หมายความว่า ค่าที่น้อยที่สุดใน Field นี้คือ 8 ซึ่งเป็นขนาดของ Header

4) Checksum : เป็นตัวตรวจสอบความถูกต้องของ UDP Datagram และจะนำข้อมูลบางส่วนใน IP Header มาคำนวณด้วย

2.3.2 ทีซีพี (Transmission Control Protocol: TCP) อยู่ใน Transport Layer เช่นเดียวกับ UDP ทำหน้าที่จัดการและควบคุมการรับส่งข้อมูลซึ่งมีความสามารถและรายละเอียดมากกว่า UDP โดย Datagram ของ TCP จะมีความสัมพันธ์ต่อเนื่องกัน มีกลไกควบคุมการรับส่งข้อมูลให้มีความถูกต้อง (Reliable) และมีการสื่อสารอย่างเป็นกระบวนการ (Connection Oriented) แสดงดังภาพที่ 3.10



ภาพที่ 3.10 TCP Header

ที่มา : เอกชัย ไก่แก้ว (2556)

จากภาพที่ 3.10 แสดงรายละเอียดของ TCP Header ดังต่อไปนี้

1) Source Port Number : หมายเลขพอร์ตต้นทางที่ส่ง Datagram นี้

2) Destination Port Number : หมายเลขพอร์ตปลายทางที่จะเป็นผู้รับ Datagram

3) Sequence Number : Field ที่ระบุหมายเลขลำดับอ้างอิงในการสื่อสารข้อมูลแต่ละครั้ง เพื่อใช้ในการแยกแยะว่าเป็นข้อมูลของชุดใดและนำมาจัดลำดับได้ถูกต้อง

4) Acknowledgment Number : หน้าที่เหมือนกับ Sequence Number แต่ใช้ในการตอบรับ

5) Header Length : โดยปกติความยาวของ Header TCP จะมีความยาว 20 ไบต์ แต่อาจจะมากกว่านั้น ถ้ามีข้อมูลใน Field Option แต่ต้องไม่เกิน 60 ไบต์

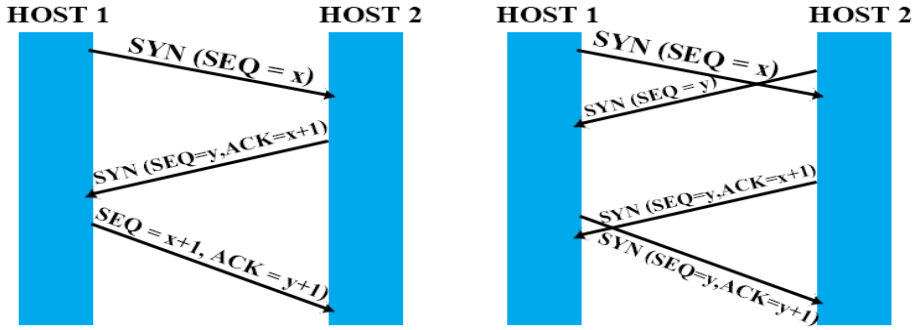
6) Flag : เป็นข้อมูลระดับ Bit ที่อยู่ใน Header TCP ใช้เป็นตัวบอกคุณสมบัติของ Packet TCP ขณะนั้นและเป็นตัวควบคุมจังหวะการรับส่งข้อมูลด้วย ซึ่ง Flag มีอยู่ทั้งหมด 6 Bit แบ่งได้ตามตารางที่ 3.1 ดังนี้

ตารางที่ 3.1 แสดงการแบ่ง Flag ขนาด 6 Bit

Type	Description
URG	บอกความหมายว่าเป็นข้อมูลด่วนและมีข้อมูลพิเศษมาด้วย (อยู่ใน Urgent Pointer)
ACK	แสดงว่าข้อมูลในField Acknowledge Number นำมาใช้งานได้
DSH	แจ้งให้ผู้รับข้อมูลว่าควรจะส่งข้อมูล Segment นี้ไปยัง Application ที่กำลังรออยู่โดยเร็ว
RST	ยกเลิกการติดต่อ (Reset) เนื่องจากในกรณีที่เกิดผิดพลาดจากการส่งข้อมูลขึ้นด้วยเหตุผลต่าง ๆ เช่น Host มีปัญหาให้เริ่มสื่อสารใหม่
SYN	ใช้ในการเริ่มต้นเพื่อติดต่อกับปลายทาง
FIN	ใช้ส่งเพื่อแจ้งให้ปลายทางทราบว่าสิ้นสุดการติดต่อ

Flag Header ของ TCP มีความสำคัญในการกำหนดการทำงานของ TCP Segment เนื่องจากข้อมูลใน Header ของ TCP จะมีข้อมูลครบถ้วนทั้งการรับและการส่งข้อมูล ซึ่งในการทำงานแต่ละอย่างจะมีการใช้งาน Field ไม่เหมือนกัน Flag จะเป็นตัวกำหนดว่าให้ใช้งาน Field ไหน เช่น Filed Acknowledgment Number จะไม่ถูกใช้ในขั้นตอนการเริ่มต้นการเชื่อมต่อ แต่จะมีข้อมูลใน Filed ซึ่งเป็นข้อมูลที่ไม่มีความหมายใด ๆ ซึ่งถ้าไม่มี Flag เป็นตัวกำหนดก็อาจจะมีการนำข้อมูลมาใช้และทำให้เกิดความผิดพลาดได้

เมื่อ Segment Connect (SYN = “1” และ ACK = “0”) เดินทางมาถึง Entity TCP ที่ Host ปลายทางจะค้นหาโพรเซส (Process) ตามหมายเลขพอร์ต (Port) ที่กำหนดในเขตข้อมูล Destination Port ซึ่งถ้าหากไม่พบก็จะตอบปฏิเสธด้วย Segment ที่มี RST = “1” กลับไปยังผู้ส่ง Segment Connect ของผู้ส่งจะถูกส่งต่อไปยัง Process ตาม Port ที่ระบุซึ่งอาจจะตอบรับหรือตอบปฏิเสธก็ได้ถ้า Process ต้องการสื่อสารด้วยก็จะส่ง Segment ตอบรับกลับไป แสดดังภาพที่ 3.11 (ก) จะแสดงลำดับขั้นตอนการส่ง TCP Segment ในการสร้างการเชื่อมต่อในสภาวะปกติระหว่างผู้ส่งและผู้รับ ในกรณีที่ Host ทั้งสองแห่งพยายามสร้างการเชื่อมต่อระหว่างซ็อคเก็ต (Socket) คู่เดียวกันจะเกิดเป็นลำดับขั้นตอนแสดงดังภาพที่ 3.11 (ข)



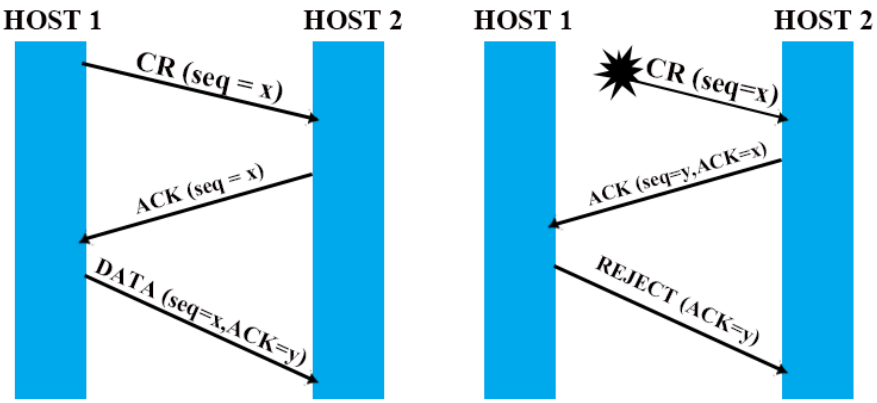
(ก) การส่ง TCP Segment (ข) การเชื่อมต่อระหว่างซ็อคเก็ต (Socket)

ภาพที่ 3.11 แสดงการสื่อสารบน TCP

ที่มา : เอกชัย ไก่แก้ว (2556)

สุดท้ายจะมีการเชื่อมต่อเกิดขึ้นเพียงหนึ่งช่องทางเท่านั้นเนื่องจากการเชื่อมต่อในแต่ละช่องทางจะถูกกำหนดขึ้นโดยใช้หมายเลข Socket ผู้ส่งและผู้รับ ถ้าการเชื่อมต่อลำดับแรกสำเร็จก็จะถูกบันทึกไว้ในตารางการสื่อสาร เช่น (x, y) ถ้าการเชื่อมต่อลำดับที่สองสำเร็จในเวลาต่อมา ข้อมูลนี้ก็จะถูกบันทึกไว้ที่เดียวกันคือ (x, y) ขั้นตอนในการสร้างการเชื่อมต่อและการยกเลิก สามารถเขียนอธิบายด้วยไฟไนท์สเตทแมชชีน (Finite state machines) คือการตรวจสอบข้อความที่ตามหลังตัวแปรในคำสั่ง "Integer" ซึ่งเป็นคำสั่งที่ใช้ประกาศตัวแปรที่เป็น Integer ตัวแปรนั้นอาจเป็นตัวแปรเดี่ยวหรือ ตัวแปร Array ก็ได้

การเริ่มต้นการสื่อสารของ TCP โดยใช้การบันทึกเวลาแบบ Three Way Handshake เป็นวิธีการส่ง Packet ที่สามารถช่วยแก้ปัญหาในเรื่อง Packet ซ้ำซ้อนได้ดี แต่วิธีนี้จำเป็นจะต้องสร้างช่องสื่อสารให้ได้ก่อนที่จะเริ่มรับ ส่งข้อมูล อย่างไรก็ตาม Packet ควบคุมที่ใช้ในการต่อรองค่าตัวแปรสำหรับการสื่อสารต่าง ๆ อาจเกิดการตกค้างอยู่ในระบบได้ ทำให้การกำหนดค่าหมายเลขลำดับมีปัญหาไปด้วย เช่นการสร้างช่องสื่อสารระหว่าง Host 1 และ Host 2 เริ่มจาก Host 1 ขอการเชื่อมต่อด้วยการส่ง Packet CR (Connection Request) ไปยัง Host 2 ซึ่งจะมีค่าตัวแปรต่าง ๆ สำหรับการสื่อสารรวมทั้งหมายเลขลำดับและหมายเลขช่องสื่อสารไปด้วย ผู้รับคือ Host 2 ก็จะส่ง ACK (Acknowledge) กลับมายัง Host 1 แต่ถ้า Packet จากผู้ส่งเกิดสูญหายระหว่างทางและสำเนา Packet ที่ยังตกค้างอยู่ระบบเกิดเดินทางไปถึงผู้รับในภายหลังก็จะทำให้การสร้างช่องสื่อสารใช้การไม่ได้ เนื่องจากมีค่าตัวแปรต่าง ๆ ไม่ตรงกันการใช้ Three Way Handshake เป็นการไม่บังคับให้ผู้ส่งและผู้รับข้อมูลจะต้องกำหนดค่าเริ่มต้นของหมายเลขลำดับเป็นเลขเดียวกัน ทำให้สามารถนำวิธีนี้มาใช้ร่วมกับวิธีการจัดจังหวะ (Synchronization) การทำงานให้พร้อมกันได้ แทนที่จะเป็นการใช้วิธีการบันทึกเวลา แสดงดังภาพที่ 3.12 (ก) แสดงขั้นตอนการเริ่มต้นการทำงานจาก Host 1 ไปยัง Host 2 สมมุติให้ Host 1 เลือกหมายเลขลำดับเป็น “x” และส่ง Packet Connection Request ไปยัง Host 2 Host 2 ตอบรับด้วย Packet Connection Accepted ซึ่งจะยอมรับหมายเลขลำดับ “x” พร้อมกับประกาศหมายเลขลำดับ “y” ที่เป็นของตนเอง จากนั้น Host 1 ก็จะตอบรับค่าตัวเลือกของ Host 2 ผ่านทางเขตข้อมูลสำหรับการควบคุมใน Packet ข้อมูลแรกที่ส่งมา



(ก) การทำงานจาก Host 1 ไปยัง Host 2 (ข) แสดงเหตุการณ์ที่ Packet TPDU

ภาพที่ 3.12 แสดงการสื่อสารบน TCP

ที่มา : เอกชัย ไก่แก้ว (2556)

ถ้าหากได้เกิดปัญหาการสูญหายของ Packet ในขณะที่สำเนา Packet ที่ค้างในระบบเดินทางไปถึงผู้รับแทน ภาพที่ 3.12 (ข) แสดงเหตุการณ์ที่ Packet TPDU (ตัวแรกในภาพ) เป็นสำเนา Packet เก่าที่พึ่งจะเดินทางไปถึง Host 2 โดยที่ Host 1 ไม่ทราบ Host 2 ก็จะทำงานตามปกติคือจะตอบรับด้วยการส่ง Packet Connection Accepted TPDU กลับมา ที่ Host 1 ซึ่ง Host 1 จะสามารถตรวจสอบได้ว่าหมายเลขลำดับ Host 2 ตอบกลับมานั้นเป็นหมายเลขลำดับที่เลิกใช้ไปแล้ว จึงมีการส่ง Packet - Reject กลับมายัง Host 2 เพื่อบอกยกเลิกการทำงาน จะเห็นว่าวิธีการนี้อาศัยการสื่อสารผ่าน Packet3 ตัวซึ่งเป็นที่มาของคำว่า “การจับมือร่วมสามขั้นตอน” ผลสุดท้าย ทั้ง Host 1 และ Host 2 ก็จะไม่มีการสร้างช่องสื่อสารขึ้นมาจากข้อมูลในสำเนา Packet เดิมแต่อย่างใด

2.4 ชั้นสื่อสารการประยุกต์ (Application Layer) Protocol ที่ใช้สำหรับการจัดการแฟ้มข้อมูลเรียกว่า FTP และ Protocol สำหรับการให้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) เรียกว่า SMTP โดย Protocol สำหรับสร้างจอเทอร์มินัลเสมือน (Telnet) ช่วยให้ผู้ใช้สามารถติดต่อกับเครื่อง Host ที่อยู่ไกลออกไปโดยผ่านอินเทอร์เน็ต และสามารถทำงานได้เสมือนกับว่ากำลังนั่งทำงานอยู่ที่เครื่อง Host นั้น Protocol สำหรับการจัดการแฟ้มข้อมูลช่วยในการคัดลอกแฟ้มข้อมูลมาจากเครื่องอื่นที่อยู่ในระบบเครือข่าย หรือส่งสำเนาแฟ้มข้อมูลไปยังเครื่องใด ๆ ก็ได้ Protocol สำหรับให้บริการจดหมายอิเล็กทรอนิกส์ ช่วยในการจัดส่งข้อความไปยังผู้ใช้ในระบบหรือรับข้อความที่มีผู้ส่งเข้ามา

3. โพรโทคอลสำหรับเครือข่าย

การทำงานของ Protocol TCP/IP เทียบกับมาตรฐาน OSI Model นั้น ในชั้นบนสุดเรียกว่า Process Layer ทำงาน 2 หน้าที่เทียบได้กับ Application และ Presentation Layer ในชั้นนี้จะรองรับการทำงานของ Application ต่าง ๆ ที่ทำงานเป็น Process แต่อยู่ในเครื่องเซิร์ฟเวอร์ (Server) และเครื่องที่ขอใช้บริการหรือไคลเอนต์ (Client) ซึ่งจะติดต่อกันผ่าน Protocol เฉพาะ Application อีกที เช่น เมื่อผู้ใช้งาน Internet ต้องการโอนถ่ายไฟล์หรือ Download ข้อมูลจากเครื่อง Server โดยอาจจะเรียกใช้โปรแกรม FTP Client ทั่วไป เช่น โปรแกรม WS FTP ติดต่อกับ Process FTP ที่กำลังให้บริการอยู่ที่เครื่อง Server จากนั้นตัว Process FTP ก็จะเรียกใช้ Protocol FTP (File Transfer Protocol) เพื่อทำการถ่ายโอนไฟล์นี้ หรือถ้าผู้ใช้ต้องการเรียกใช้งานคอมพิวเตอร์เครื่องที่อยู่ห่างไกลออกไปด้วยการใช้โปรแกรม Telnet เพื่อติดต่อกันหรือในกรณีที่มีการเรียกใช้โปรแกรม Web Browser เพื่อเรียกดู Web Page ใน Website ก็จะมี Process HTTP (Hyper Text Transfer Protocol) ทำงานอยู่และจะติดต่อกับผู้ใช้ผ่าน Protocol HTTP เป็นต้น

การทำงานของ Application ต่าง ๆ จะอยู่ที่ Process Layer นี้และมีการติดต่อกันตามแต่ละ Protocol เฉพาะแล้วแต่ Application ที่ใช้งาน จากการที่ Process layer ของ TCP/IP รองรับให้ Protocol อื่นที่ทำงานได้หลาย Process และหลาย Protocol ได้พร้อมกันนั้น ทำให้ผู้ใช้สามารถเปิดโปรแกรมใช้งานได้หลายโปรแกรมพร้อมกัน เช่น เปิดโปรแกรม Internet Explorer เพื่อเรียกดู Web Page พร้อมกับใช้งานโปรแกรม Outlook Express เพื่อส่ง E-mail ไปพร้อมกันได้ โดยไม่ต้องรอให้ทำงานอย่างใดอย่างหนึ่งเสร็จก่อนหรือในปัจจุบันมีการพัฒนาโปรแกรม Web Browser ทำให้สามารถเรียกใช้งาน Protocol อื่น ๆ ได้มากขึ้น ทำให้สามารถใช้โปรแกรม Web Browser โอนถ่ายข้อมูลที่ใช้ Protocol FTP ได้โดยไม่ต้องไปหาโปรแกรมอื่นมาใช้ Protocol หลักที่ทำงานใน Process Layer ที่ผู้ใช้งานจะรู้จักกันได้แก่

1) FTP (File Transfer Protocol),

2) Telnet

3) HTTP (Hypertext Transfer Protocol)

4) SMTP (Simple Mail Transfer Protocol)

นอกจากนี้ยังมี Protocol อื่นซึ่งทำงานโดยที่ผู้ใช้งานไม่สามารถมอง เห็นได้จากโปรแกรมหรือไม่ได้มีการใช้งานโดยตรง เช่น

1) Protocol DNS (Domain Name System) ทำหน้าที่แปลงข้อมูลชื่อ Domain Name หรือชื่อเว็บไซต์ทั้งหลายให้เป็น IP Address

2) Protocol SNMP (Simple Network Management Protocol) ใช้ในการควบคุมและตรวจสอบอุปกรณ์ที่อยู่ในเครือข่าย

3) Protocol DHCP (Dynamic Host Configuration Protocol) มีหน้าที่แจกจ่ายข้อมูลพารามิเตอร์ของเครือข่ายให้กับเครื่องลูกข่ายที่เชื่อมต่ออยู่

Network Interface Layer เป็นการเชื่อมต่อทางด้านกายภาพของเครือข่าย มีหลายวิธีการและหลายรูปแบบในการเชื่อมต่อ แต่อย่างไรก็ตามในเครือข่าย Internet นี้ ข้อมูลหรือ IP Datagram จะถูกถ่ายทอดและส่งผ่านไปยังปลายทางโดยไม่คำนึงถึงรูปแบบการเชื่อมต่อทางกายภาพ ไม่ว่าจะเป็นการใช้เครือข่ายใยแก้วนำแสงหรือเครือข่ายสาย Unshielded Twist Pair (UTP) เชื่อมต่อเป็นแบบเครือข่าย Ethernet ธรรมดาหรือเครือข่าย Token Ring, ATM, ISDN หรืออื่น ๆ การทำงานเริ่มจากระดับล่างสุดต่อจาก Internet Layer จะเป็นการแปลงข้อมูล IP Datagram ให้อยู่ในรูปที่เหมาะสมแล้วแปลงเป็นสัญญาณไฟฟ้าส่งไปยังเครือข่ายต่อไป ซึ่งในชั้น Network Interface Layer นี้เทียบกับมาตรฐาน OSI Model แล้วจะเป็นการรวมเอา Layer 2 Layer เข้าด้วยกันคือ Data Link Layer และ Physical Layer กล่าวโดยสรุปคือ การทำงานตามโครงสร้างของ Protocol TCP/IP จะมีลักษณะใช้งานของ Protocol และ Port การสื่อสารแสดงดังตารางที่ 3.2 จะสรุปหมายเลขบางส่วนของ Port ที่ใช้งานโดย TCP และ UDP

ตารางที่ 3.2 สรุปหมายเลขบางส่วนของ Port ที่ใช้งานโดย TCP และ UDP

Protocol	Port หรือ Socket เชื่อมต่อ	Protocol ในระดับ Host to Host	รายละเอียด
BootP	67	UDP	BOOT Strap Protocol ด้านServer
BootP	68	UDP	BOOT Strap Protocol ด้านไคลเอนต์
DHCP	67	UDP	Dynamic Host Configuration Protocol ด้าน Server
DHCP	68	UDP	Dynamic Host Configuration Protocol ด้าน Client
DNS	53	UDP/TCP	Domain Name System
FTP	21	TCP	File Transfer Protocol ด้านServer ที่ควบคุม
FTP	20	TCP	File Transfer Protocol ด้านServer ที่ส่งข้อมูล
HTTP	80	TCP/UDP	Hyper Text Transfer Protocol ด้านServer
NetBT	138	UDP	NetBIOS Datagram Service
NetBT	139	TCP	NetBIOS Session Service
SNMP	161	UDP	Simple Network Management Protocol ด้าน agent
SNMP	162	UDP	SNMP Trap Manager
Telnet	23	TCP	Teletype Network Protocol
TFTP	69	UDP	Trivial File Transfer Protocol
WINS	137	UDP	Windows Internet Name Service

4. ไอพี แอดเดรสและดีเอ็นเอส (IP Address และ DNS)

4.1 ไอพี แอดเดรส หรือ IP Address ย่อมาจากคำว่า Internet Protocol Address คือหมายเลขประจำเครื่องคอมพิวเตอร์แต่ละเครื่องในระบบเครือข่ายที่ใช้โปรโตคอลแบบ TCP/IP เปรียบเทียบก็คือบ้านเลขที่นั่นเอง ในระบบเครือข่ายจำเป็นจะต้องมีหมายเลข IP กำหนดไว้ให้กับคอมพิวเตอร์และอุปกรณ์อื่น ๆ ที่ต้องการ IP ทั้งนี้เวลามีการโอนย้ายข้อมูล หรือสั่งงานใด ๆ จะสามารถทราบตำแหน่งของเครื่องที่ต้องการส่งข้อมูลไปจะได้ไม่ผิดพลาดในส่งข้อมูล ซึ่งประกอบ ด้วยตัวเลข 4 ชุดมีเครื่องหมายจุดขั้นระหว่างชุด เช่น 192.168.100.1 หรือ 172.16.10.1 เป็นต้น โดยหมายเลข IP Address ของเครื่องคอมพิวเตอร์แต่ละเครื่องจะมีค่าไม่ซ้ำกันสิ่งตัวเลข 4 ชุดนี้บอก คือ Network ID กับ Host ID ซึ่งจะบอกให้รู้ว่า เครื่องคอมพิวเตอร์ ว่าอยู่ในเครือข่ายไหนและเป็นเครื่องไหนในเครือข่ายนั้นเราจะรู้ได้อย่างไรว่า Network ID และ Host ID มีค่าเท่าไหร่ ก็ขึ้นอยู่กับว่า IP Address นั้น อยู่ใน Class อะไร

การแบ่ง Class ของ IP เพื่อให้เกิดความเป็นระเบียบ เป็นการแบ่ง IP Address ออกเป็นหมวดหมู่ สิ่งที่จะเป็นตัวจำแนก Class ของ Network คือ Bit ทางซ้ายมือสุดของตัวเลขตัวแรกของ IP Address (ที่แปลงเป็นเลขฐาน 2 แล้ว) โดยที่ถ้า Bit ทางซ้ายมือสุดเป็น 0 ก็จะเป็น Class A ถ้าเป็น 10 ก็จะเป็น Class B ถ้าเป็น 110 ก็จะเป็น Class C ดังนั้น IP Address จะอยู่ใน Class A ถ้าตัวเลขตัวแรกมีค่าได้ตั้งแต่ 0 ถึง 127 (00000000 ถึง 01111111) จะอยู่ใน Class B ถ้าเลขตัวแรกมีค่าตั้งแต่ 128 ถึง 191 (10000000 ถึง 10111111) และ จะอยู่ใน Class C ถ้าเลขตัวแรกมีค่าตั้งแต่ 192 ถึง 223 (11000000 ถึง 11011111) แต่ข้อยกเว้นอยู่ก็คือตัวเลข 0 และ 127 ใช้เป็นหมายเลขพิเศษ จะไม่ใช้เป็น Address ของ Network ดังนั้น Network ใน Class A จะมีค่าตัวเลขตัวแรก ในช่วง 1 ถึง 126 สำหรับตัวเลขตั้งแต่ 224 ขึ้นไป จะเป็น Class พิเศษ เช่น Class D ซึ่งถูกใช้สำหรับการส่งข้อมูลแบบ Multicast ของบาง Application และ Class E ซึ่ง Class นี้เป็น Address ที่ถูกสงวนไว้ก่อน ยังไม่ถูกใช้งานจริง โดย Class D และ Class E นี้เป็น Class พิเศษ ซึ่งไม่ได้ถูกนำมาใช้งานในภาวะปกติ

Class ของ หมายเลข IP Address

Class A ตั้งแต่ 10.xxx.xxx.xxx

Class B ตั้งแต่ 172.16.xxx.xxx ถึง 172.31.xxx.xxx

Class C ตั้งแต่ 192.168.0.xxx ถึง 192.168.255.xxx

Class D เป็นการสำรองหมายเลข IP Address ตั้งแต่ 224.0.0.0 ถึง 239.255.255 .255 สำหรับการส่งข้อมูลแบบ Multicast ซึ่งจะไม่มีการแจกจ่ายใช้งานทั่วไปสำหรับบุคคลทั่วไป

Class E เป็นการสำรองหมายเลข IP Address ช่วง 240.0.0.0 ถึง 255.255.255.255 สำหรับการทดลองและพัฒนา

จาก IP Address สามารถที่จะบอกได้ว่า Computer 2 เครื่องอยู่ใน Network วงเดียวกันหรือไม่โดยการเปรียบเทียบว่าถ้ามี Network ID ของ IP Address ตรงกันแสดงว่าอยู่ใน Network วงเดียวกัน เช่น Computer เครื่องหนึ่งมี IP Address 1.2.3.4 จะอยู่ใน network วงเดียวกับอีกเครื่องหนึ่งซึ่งมี IP Address 1.100.150.200 เนื่องจากมี Network ID ตรงกันคือ 1 (Class A ใช้ Network ID 1 Byte)

4.2 ระบบโดเมนเนม (Domain Name System)

ระบบโดเมนเนม (Domain Name System) เป็นการตั้งชื่อเป็นตัวอักษรเพื่อใช้แทน IP Address เพื่อง่ายต่อการจดจำ เช่นหมายเลข IP Address 113.53.238.196 แทนที่ด้วย Domain Name ชื่อ technicphrae.ac.th ซึ่งเรียกการแทนที่ IP ด้วย Domain Name ว่า Name to IP Address Mapping ซึ่งช่วยให้สามารถเรียกชื่อเว็บไซต์ได้สะดวกขึ้นโดยไม่ต้องจำตัวเลข กลไก Name to IP Address มีการกำหนดฐานข้อมูลส่วนกลางในการจัดการแก้ไขฐานข้อมูลให้เพื่อป้องกันการตั้งชื่อซ้ำกัน

การตั้งชื่อ Domain Name แบบเดิมเป็น แบบไม่มีลำดับชั้น คือไม่สามารถแยกย่อยเป็นส่วน รียกว่า Name Space ทำให้มีปัญหามากเนื่องจากฐานข้อมูลมีขนาดใหญ่ขึ้นเรื่อย ๆ ทำให้การค้นหายาก จึงได้มีการพัฒนาข้อมูลแบบ Name Space ใหม่ให้เป็นแบบลำดับชั้น (Hierarchical Structure) ที่เรียกว่า Domain Name System (DNS) ซึ่งเป็นโครงสร้างที่มีการบอกประเภทขององค์กร หรือชื่อประเทศที่เครือข่ายตั้งอยู่

Domain Name System (DNS) จึงหมายถึงระบบจัดการแปลงชื่อไปเป็นหมายเลข IP โดยมีโครงสร้างฐานข้อมูลแบบลำดับชั้น กลไกหลักของระบบ DNS ทำหน้าที่แปลงชื่อและหมายเลข IP Address หรือทำกลับกันได้ โดยระบบ DNS จะมีการกำหนด Name Space ที่มีกฎเกณฑ์อย่างชัดเจน มีการเก็บข้อมูลเป็นฐานข้อมูลแบบกระจายและทำงานในลักษณะ Client Server โดยมี DNS Server ทำหน้าที่ให้บริการค้นชื่อและแปลงข้อมูลตามที่เครื่องลูกข่าย (DNS Client) ร้องขอมา การทำงานแบบ Client Server นี้ทำให้เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็น DNS สามารถเป็นได้ทั้งเครื่อง Server และ Client ของ DNS ในเครื่องเดียวกัน

4.2.1 Domain Name ระดับบนสุด (Top Level Domain) เป็นการกำหนดชื่อ Domain Name ให้มีความหมายในการบอกประเภทขององค์กร หรือชื่อของประเทศแบ่งออกเป็น 2 ประเภท คือ

4.2.1.1 Organization Domains เป็น Domain Name ระดับสูงสุดซึ่งแสดงถึงองค์กรหรือหน่วยงาน ดังแสดงในตารางที่ 3.3

ตารางที่ 3.3 แสดง Domain Name ระดับสูงสุดขององค์กรหรือหน่วยงาน

Domain Name	**ความหมาย**
com	เครือข่ายของเอกชน
edu	เครือข่ายของหน่วยงานการศึกษา
gov	เครือข่ายของหน่วยงานรัฐบาล
mil	เครือข่ายของหน่วยงานทหาร
net	เครือข่ายของผู้ให้บริการอินเตอร์เน็ต
org	เครือข่ายขององค์กรที่ไม่มุ่งหวังกำไร

4.2.1.2 Geographical Domains เป็น Domain Name ระดับสูงสุดซึ่งแบ่งตามลักษณะภูมิศาสตร์หรือประเทศ ดังแสดงในตารางที่ 3.4

ตารางที่ 3.4 แสดง Domain Name ระดับสูงสุด แบ่งตามลักษณะภูมิศาสตร์หรือประเทศ

Domain Name	ความหมาย
at	ออสเตรีย
au	ออสเตรเลีย
ca	แคนาดา
ch	สวิตเซอร์แลนด์
cn	สาธารณรัฐประชาชนจีน
de	เยอรมัน
dk	เดนมาร์ก
fr	ฝรั่งเศส
jp	ญี่ปุ่น
nz	นิวซีแลนด์
th	ไทย
uk	สหราชอาณาจักร (อังกฤษ)
us	สหรัฐอเมริกา

นามสกุลนั้นมีไว้เพื่อบ่งบอกกิจกรรมของเว็บไซต์นั้น ๆ ว่าเกี่ยวข้องกับอะไรซึ่งบางทีก็ไม่สามารถบ่งบอกได้ชัดเจนมากนัก เนื่องจากบางนามสกุล เช่น .com, .net ไม่ได้มีข้อบังคับชัดเจน ว่าจะนามสกุลใด ๆ จะต้องใช้เพื่อกิจกรรมนั้น ๆ เพียงเท่านั้น แต่โดยทั่วไปของการจดตามนามสกุลต่าง ๆ นั้นจะสามารถแบ่งได้คร่าว ๆ ดังนี้

.com ใช้สำหรับเว็บไซต์ที่เกี่ยวกับธุรกิจการค้า (.com = Company)

.net (Network) ใช้กับเว็บไซต์ขององค์กรใดหรือบริษัทใด ที่ทำงานเกี่ยวข้องกับ Internet หรือ Network

.org (Organization) ใช้สำหรับเว็บไซต์องค์กรที่ไม่หวังผลกำไร เช่น สมาคมหรือมูลนิธิ

.biz ใช้สำหรับเว็บไซต์ขององค์กรที่เกี่ยวกับธุรกิจการค้า

.infoใช้สำหรับเว็บไซต์ที่นำเสนอข้อมูลเป็นหลัก

.co.th สำหรับบริษัทที่จดทะเบียนในไทย

.in.th สำหรับหน่วยงานทุกประเภทและบุคคลทั่วไป

.ac.th สำหรับสถาบันการศึกษา

.go.th สำหรับการใช้ของภาครัฐบาล

.net.th สำหรับนิติบุคคลผู้ได้รับใบอนุญาตประกอบกิจการโทรคมนาคมทั้ง 3 แบบตาม

.or.th สำหรับองค์กรที่ไม่แสวงผลกำไร

.mi.th สำหรับหน่วยงานทางทหาร

ในปัจจุบัน ได้มีนามสกุลต่าง ๆ ออกมามากมาย เช่น .it, .ws, .tv แต่ความนิยมการในการจดทะเบียนยังคงเป็น .com, .net, .org, .co.th, .in.th เป็นส่วนใหญ่

Domain Name ในประเทศไทยใช้ .th เป็นโดเมนประจำประเทศ โดยมีโดเมนย่อย (Sub - Domain) 5 โดเมน ได้แก่ .or, .ac, .go, .co และ .net ดังแสดงตารางที่ 3.5

ตารางที่ 3.5 แสดงโดเมนย่อย หรือ Sub Domain

Domain Name	ความหมาย
or	องค์กรไม่แสวงผลกำไร
ac	สถาบันการศึกษา
go	หน่วยงานราชการ
co	หน่วยงานเอกชน
net	องค์กรที่ให้บริการเครือข่าย

4.2.3 การลงทะเบียนขอชื่อ Domain Name สำหรับการลงทะเบียนขอชื่อ Domain Name ในประเทศไทยทำได้ 2 ทางเลือกคือ

4.2.3.1 จดทะเบียนที่ใช้ชื่อแบบ xxx.xx.th สามารถจดทะเบียนได้ที่ Thailand Network Information Center หรือ Th NIC หรือที่เว็บไซต์ www.thnic.net และต้องแนบเอกสารหลักฐานการจดทะเบียนบริษัทในการขอจดทะเบียน

4.2.3.2 จดทะเบียนที่ใช้ชื่อเป็น .com หรือ .net หรือแบบอื่น ๆ ที่ไม่ใช่ของประเทศไทย ต้องขอจดทะเบียนโดยตรงที่หน่วยงานที่เป็นตัวแทนของ Inter NIC (Internet Network Information-Center) หรือที่เว็บไซต์ www.internic.net ซึ่งการจดทะเบียนแบบนี้ต้องแจ้งให้ผู้รับจดทะเบียนทั้ง Th NIC และ Inter NIC ทราบด้วยว่าใครเป็นผู้ดูแลเซิร์ฟเวอร์

4.2.4 MAC Address (Media Access Control Address) คือหมายเลขของ Network Card ซึ่งหมายเลขจะไม่ซ้ำกัน โดยค่าหมายเลขนี้จะถูกกำหนดมาจากโรงงานที่ผลิต Network Card รูปแบบของค่า MAC Address จะอยู่ในรูปแบบของเลขฐานสิบหก ดังนี้ 01-23-45-67-89-ab หรือ 01:23:45:67:89:ab

สรุป

การสื่อสารระหว่างคอมพิวเตอร์จำเป็นต้องใช้ Protocol เดียวกันเท่านั้นจึงสามารถสื่อสารกันได้ Protocol มาตรฐานหลายชุดของ Protocol ที่พัฒนาขึ้นใช้งานและบาง Protocol ก็ไม่ได้ถูกนำมาใช้งานปัจจุบันที่นิยมใช้กันมากคือ Protocol TCP/IP ชุด Protocol นี้ทำงานโดยแบ่งชั้นเทียบกับ OSI Model ได้กลไกในการทำงานของ Protocol TCP/IP มี 4 ชั้น ในชั้นแรก คือ Process Layer ทำหน้าที่ ติดต่อกับ Application และ Protocol ที่ Application นั้น ๆใช้งานและส่งต่อมาให้ชั้น Host to Host Layer เพื่อติดต่อกันระหว่างเครื่อง Server ให้บริการกับเครื่อง Client ในชั้นนี้จะมีการสร้าง Session หรือการเชื่อมต่อระหว่างระบบตามแต่ละ Protocol ที่ต้องการ ต่อมาเป็นการผนึกข้อมูลไปเป็น IP Datagram ที่ชั้น Internet Layer โดยอาศัย Protocol IP เพื่อให้สามารถติดต่อส่งข้อมูลข้ามเครือข่ายไปยังเครือข่ายและเครื่องที่ถูกต้องได้ และสุดท้ายการส่งข้อมูลออกสู่ภายนอกต้องอาศัยกลไกในชั้น Network Interface Layer โดยอาศัย Protocol IP เพื่อให้สามารถติดต่อส่งข้อมูลออกสู่ภายนอกต้องอาศัยกลไกในชั้น Network Interface Layer เพื่อแปลงข้อมูลใหม่ เพิ่มข้อมูลที่จำเป็นในการอ้างอิง ตำแหน่งและแปลงข้อมูลเป็นสัญญาณไฟฟ้าส่งออกไปยังเครือข่ายและอาจจะออกไปยัง Gateway หรือ Router เพื่อข้ามเครือข่ายออกไปยังเส้นทางที่กำหนดไว้ใน Internet ต่อไป

แบบฝึกหัด
หน่วยที่ 3 แบบจำลองเครือข่ายและโพรโทคอล

คำชี้แจง

1. ให้ให้ตอบคำถามพร้อมทั้งอธิบาย ลงบนกระดาษคำตอบ
2. แบบฝึกหัดมีจำนวน 6 ข้อ ให้ทำทุกข้อ
3. เวลา 15 นาที (จำนวน 12 คะแนน)

---

1. แบบจำลองเครือข่าย OSI มีกี่ Layer อะไรบ้าง
2. OSI Model แบ่ง ตามลักษณะของการทำงานออกเป็น 2 กลุ่มใหญ่ ได้แก่อะไรบ้าง
3. ให้อธิบายถึงวิธีการ Encapsulation ของข้อมูล
4. จงบอกถึง Protocol ที่ใช้งานตามโครงสร้างของ TCP/IP
5. ให้นักศึกษาเปรียบเทียบการทำหน้าที่ของ TCP/IP กับ OSI Model
6. IP Address แบ่งกี่ Class อะไร บ้างพร้อมยกตัวอย่าง IP แต่ละ Class

แบบทดสอบหลังเรียน
หน่วยที่ 3 แบบจำลองเครือข่ายและโพรโทคอล

คำชี้แจง

1. ให้ทำเครื่องหมายกากบาท (×) ลงบนกระดาษคำตอบข้อที่ถูกที่สุดเพียง 1 ข้อ
2. แบบทดสอบมีจำนวน 12 ข้อ ให้ทำทุกข้อ
3. เวลา 12 นาที

---

1. Layer ระดับบนของ OSI Model คือข้อใด
   - ก. Network Layer
   - ข. Data Link Layer
   - ค. Application Layer
   - ง. Session Layer
   - จ. Presentation layer
2. Layer ใดที่เกี่ยวกับแรงดันไฟฟ้า มีการเชื่อมต่อสายและมีระยะเวลาในการส่งข้อมูลแต่ละ Bit
   - ก. Presentation layer
   - ข. Physical Layer
   - ค. Transport Layer
   - ง. Session Layer
   - จ. Data Link Layer
3. ข้อใดหมายถึง Presentation Layer
   - ก. เกี่ยวกับรูปแบบของข้อมูลการเข้ารหัส ถอดรหัส เพื่อให้คอมพิวเตอร์สามารถสื่อสารกันได้
   - ข. การควบคุมเทอร์มินอล ชนิดต่าง ๆ รูปแบบการแสดงผลทางจอภาพอาจมีความแตกต่างกัน
   - ค. การหาเส้นทางเพื่อพิจารณาว่า Packet จะถูกส่งจากต้นทางไปยังปลายทางได้อย่างไร
   - ง. ทำการควบคุม การส่งข้อมูลดิบให้เหมือนกับว่าไม่มีข้อผิดพลาดเกิดขึ้น
   - จ. ทำการถ่ายโอนไฟล์ระหว่างเครื่องและยังทำหน้าที่เกี่ยวกับการซิงโครไนซ์เซชั่น

4. TCP/IP พัฒนาขึ้นมาเพื่อจุดประสงค์ในข้อใด
   ก. สำหรับใช้งานจดหมายอิเล็กทรอนิกส์
   ข. ตรวจสอบความถูกต้อง ของข้อมูล
   ค. ติดต่อสื่อสารระหว่างระบบที่มีความแตกต่างกัน
   ง. สามารถหาเส้นทางที่จะส่งข้อมูลไปได้เองโดยอัตโนมัติ
   จ. เพื่อคอยแยกข้อมูล ให้มีขนาดพอเหมาะ
5. Internet Protocol (IP) ทำหน้าที่เกี่ยวกับอะไร
   ก. จัดการเกี่ยวกับ Address, Data และควบคุมการส่งข้อมูล
   ข. ใช้เป็นข้อมูลสำหรับอุปกรณ์จัดเส้นทาง (Router)
   ค. การรับข้อมูลจากชั้นสื่อสาร IP มาแล้วส่งไปยัง Node
   ง. จัดการเกี่ยวกับ Packet
   จ. เข้ารหัสข้อมูล
6. Header ของ IP มีขนาดกี่ Byte
   ก. 10 bytes
   ข. 20 bytes
   ค. 32 bytes
   ง. 64 bytes
   จ. 128 bytes
7. Protocol ที่ทำหน้าที่แปลงข้อมูลชื่อเว็บไซต์หลายให้เป็นหมายเลข IP Address คือข้อใด
   ก. SNMP
   ข. DHCP
   ค. Packet
   ง. DNS
   จ. FTP
8. File Transfer Protocol (FTP) ด้าน Server ใช้ Port ใดในการสื่อสาร
   ก. 21
   ข. 53
   ค. 67
   ง. 80
   จ. 161

9. โพรโทคอลที่ใช้สำหรับการบริการด้าน Web คือข้อใด
   ก. DNS
   ข. SNMP
   ค. HTTP
   ง. DHCP
   จ. FTP
10. IP หมายเลข 10.0.5.130 อยู่ในกลุ่ม IP Class ใด
   ก. Class E
   ข. Class C
   ค. Class D
   ง. Class A
   จ. Class B
11. ข้อใด หมายถึง IP Address
   ก. www.technicphrae.ac.th
   ข. เครือข่ายของผู้ให้บริการอินเตอร์เน็ต
   ค. โพรโตคอลสำหรับโอนย้ายข้อมูล
   ง. การตั้งชื่อเป็นตัวอักษรเพื่อใช้แทน IP
   จ. หมายเลข ประจำเครื่องคอมพิวเตอร์
12. โดเมนเมนนี้ www.electronic.ac.th เป็นโดเมนประเภทใด
   ก. เครือข่ายของเอกชน
   ข. เครือข่ายของหน่วยงานการศึกษา
   ค. เครือข่ายของผู้ให้บริการอินเตอร์เน็ต
   ง. เครือข่ายของหน่วยงานรัฐบาล
   จ. เครือข่ายขององค์กรที่ไม่มุ่งหวังกำไร

ใบงานที่ 3

หน่วยที่ 3

ชื่อหน่วย แบบจำลองเครือข่าย และโพรโทคอล **เวลา** 2 **ชั่วโมง**

ชื่อใบงาน ตั้งค่า IP Address และ Subnet **สอนครั้งที่ 3**

จุดประสงค์การเรียนรู้

ด้านทักษะ (ปฏิบัติ)

1.สามารถตั้งค่า IP Address และทดสอบการทำงานได้อย่างถูกต้อง

เครื่องมือและอุปกรณ์

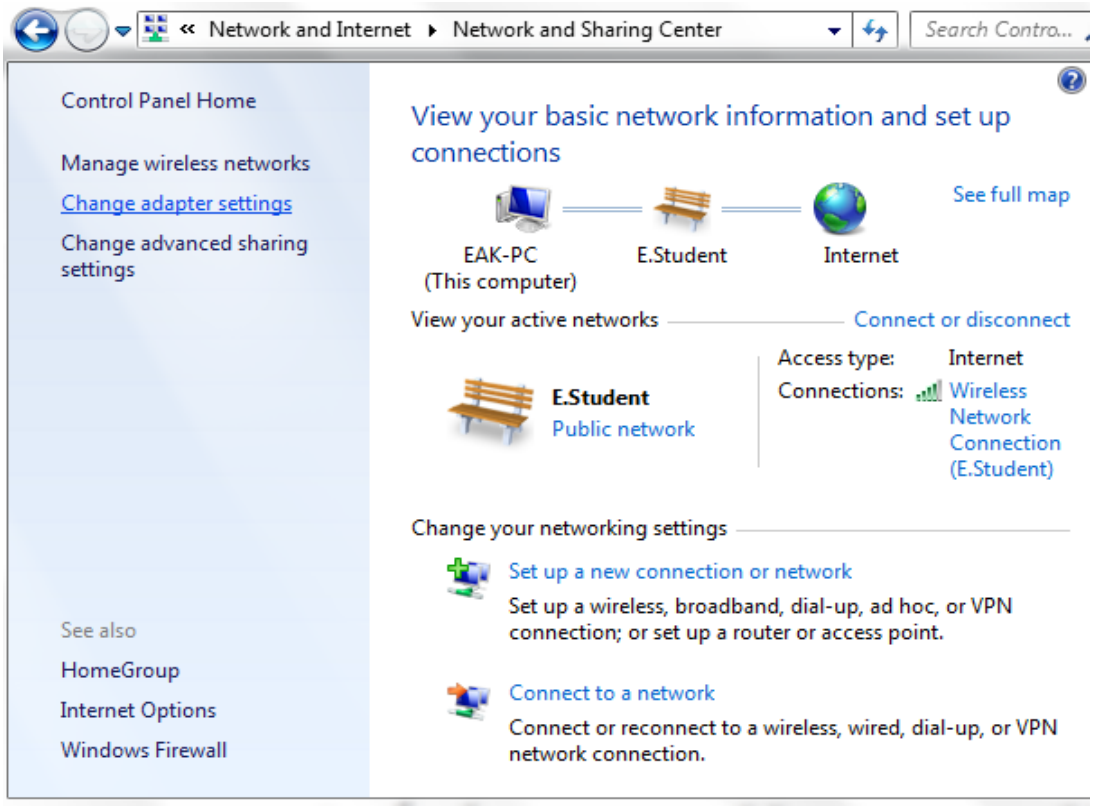
1. เครื่องคอมพิวเตอร์พร้อมโปรแกรมระบบปฏิบัติการ Windows 1 ชุด
2. ระบบเครือข่าย 1 ชุด

ขั้นตอนการปฏิบัติงาน

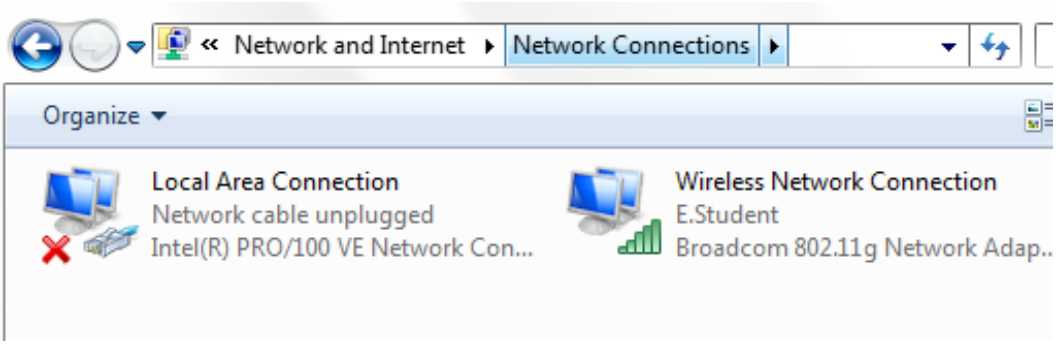
การตั้งค่า IP Address ของ Windows 7 มีวิธีการตั้งค่าดังนี้

1.คลิ๊กที่ปุ่ม Start > Control Panel จากนั้นทำการเลือก View by : Category จากนั้นทำการคลิ๊ก View Network status and tasks

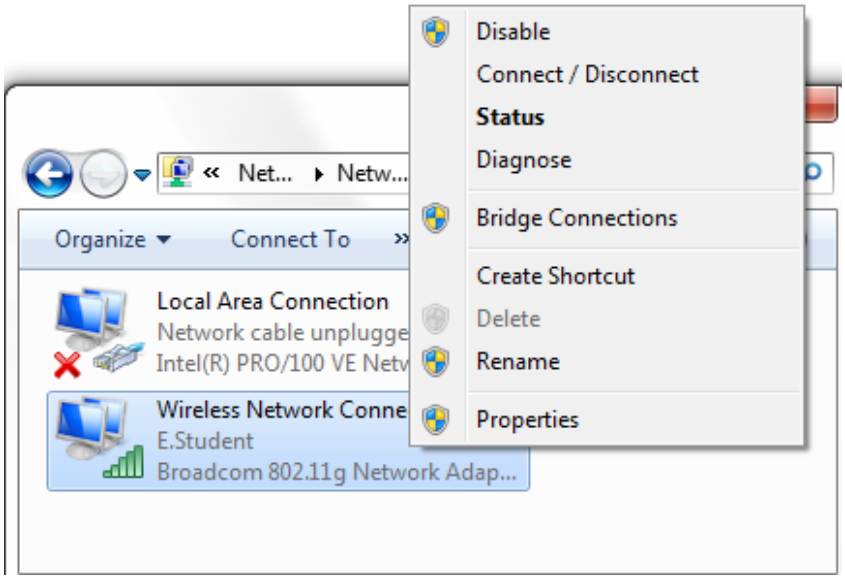
2. คลิ๊กที่ Change adapter settings



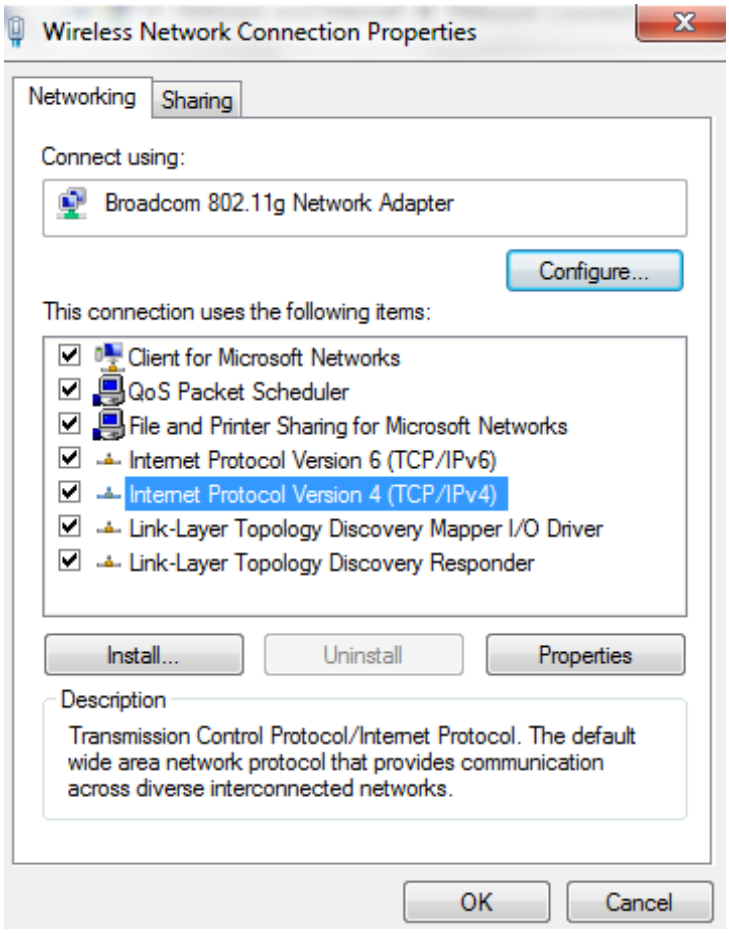
3. ทำการคลิ๊กขวาที่ Local Area Connection ถ้าเป็นการต่อแบบสาย LAN แต่ถ้าเป็น Wireless ก็ให้เลือก Wireless Area Connection



4. คลิ๊กขวาที่ Local Area Connection แล้วเลือก Properties



5. ทำการคลิ้ก Internet Protocol Version 4 (TCP/IPv4) -> จากนั้น คลิ้ก Properties



6. ทำการตั้งค่า IP Address

- ทำการเลือก Use the following IP address (เป็นการกำหนดค่า IP Address เอง)

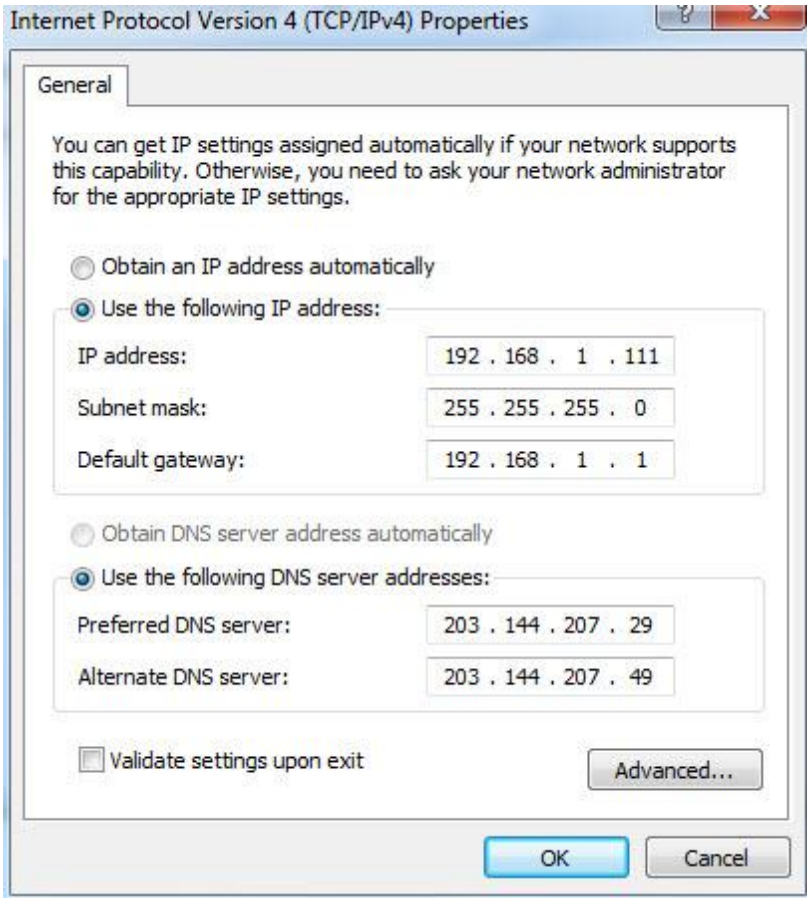
IP Address : เป็นการใส่ค่า IP ในการเชื่อมต่อการสื่อสาร เช่น 192.168.1.1

Subnet mark : เป็นการแบ่ง Class ในการแบ่ง Subnet ของ Network ออกจากกัน เช่น 255.255.255.0

Default Gateway : เป็นการใส่ทางออกของ Internet โดยส่วนมากก็จะใส่ IP Address ของ Router

- เลือก Use the Following DNS :

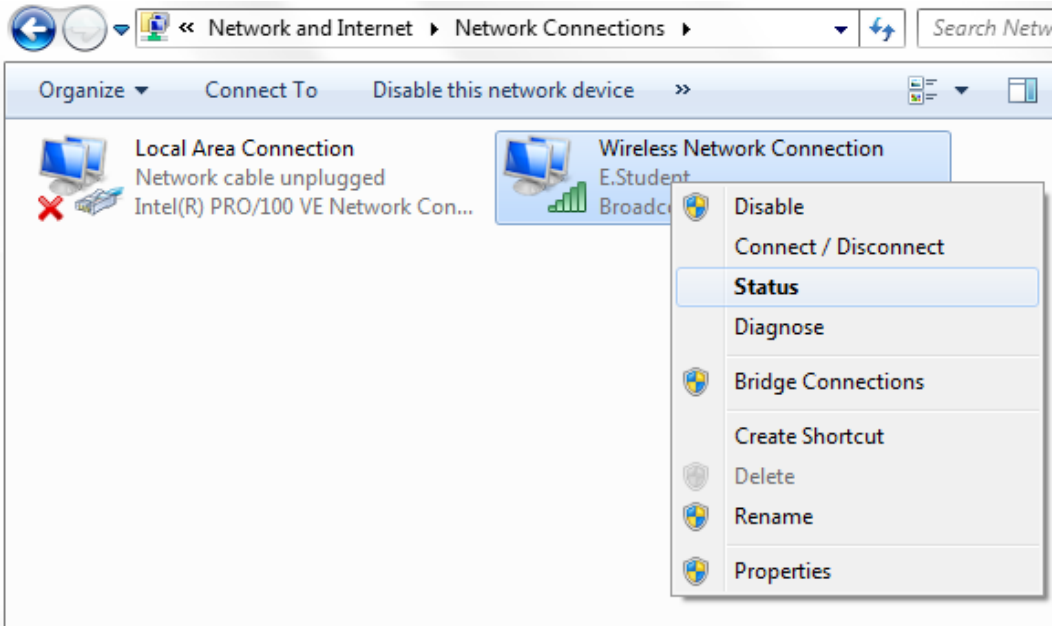
Preferred DNS Sever : ทำการใส่ DNS ของ Router หรือจะใส่ DNS ของ ISP ที่เช่าวงจรใช้งาน



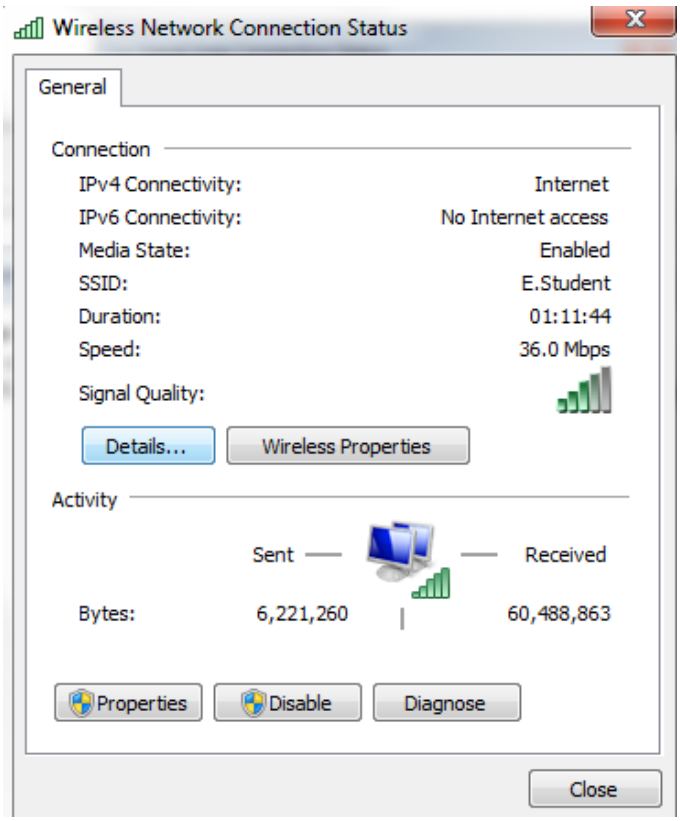
จากนั้นก็ทำการกด OK เพื่อเป็นการบันทึกค่า IP Address โดยถ้าในบ้านมีเครื่องคอมพิวเตอร์หลายเครื่องและต้องการ Fix IP Address ก็ให้ใส่ IP Address เรียงลำดับกันไป เช่น 192.168.100.1, 192.168.100.2, 192.168.100.x

การตรวจสอบหมายเลขไอพีของเครื่อง สำหรับ Windows 7

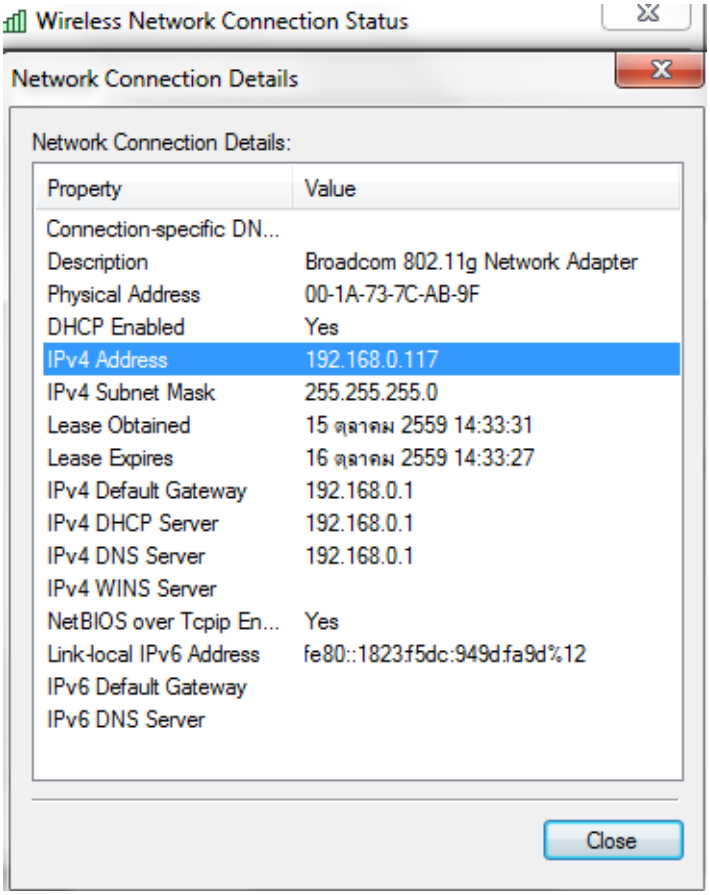
1. คลิ้กขวาที่ Connection ที่ต้องการ เลือก Status



2. ในหน้าต่างของ Connection Status กดปุ่ม Details



3. จากนั้นจะมีหน้าต่างแสดงข้อมูลต่างๆ เช่น IP Address, Subnet Mask, Default Gateway เป็นต้น



บันทึกค่าที่ได้จาก Network Connection Details

IP Address.....

Subnet Mask.....

Default Gateway.....

ทดสอบ IP Address windows 7

วิธีการรวบรวมคำสั่งและตรวจสอบการเชื่อมต่อ Internet ด้วยตัวคุณเองบน Windows 7 ถ้าต้องการตรวจสอบการเชื่อมต่อ Internet สามารถทำได้ไม่กี่ขั้นตอน ซึ่งในกรณีที่ต้องการตรวจสอบว่าการเชื่อมต่อ Internet นั้นมีปัญหาตรงไหน เพื่อที่จะได้แก้ไขปัญหาได้อย่างตรงจุดและรวดเร็ว

ขั้นตอนแรกให้ตรวจสอบพารามิเตอร์ที่จำเป็นในการเชื่อมต่อ Internet ของ Windows 7 ก่อน โดยทำตามขั้นตอนดังนี้

1. สำหรับพารามิเตอร์ที่จำเป็นในการเชื่อมต่อ Internet ประกอบไปด้วย IP Address, Subnet Mask, Gateway และ DNS Server

2. เปิด Start -> Run -> cmd พิมพ์คำสั่ง ipconfig/all จากนั้น ทำการตรวจสอบว่า IP Address / Subnet Mask / Gateway / DNS ถูกต้องหรือไม่

ผลที่ได้.....

.....

.....

.....

.....

3. ทดลองใช้คำสั่ง ping ไปยัง Gateway ที่ได้รับ

ผลที่ได้.....

.....

.....

.....

.....

4. จากนั้นทดลองใช้คำสั่ง ping ไปยัง DNS Server ที่ได้รับ (* ในกรณีที่ DNS Server ของผู้ใช้บริการใช้งานอยู่ ไม่อนุญาตให้ ping ได้นั้น สามารถทดสอบกับ DNS Server ของผู้ใช้บริการรายอื่น เช่น True = 203.144.207.29, 203.144.207.49 เป็นต้น)

ผลที่ได้.....

.....

.....

.....

.....

5. ทดลองใช้คำสั่ง nsloookp เพื่อทดสอบว่า DNS Server ที่ กำหนดอยู่นั้น สามารถตอบสนองการทำงานหรือไม่

ผลที่ได้.....

.....

.....

.....

.....

6. จากนั้นทดลองค้นหา yahoo.com เพื่อทดสอบว่า DNS Server ที่กำหนดอยู่นั้น สามารถ Resolved ชื่อโดเมนเนมให้กลายเป็น IP Address ได้หรือไม่

ผลที่ได้.....

.....

.....

.....

7. เมื่อค้นหาเว็บไซต์ที่ต้องการและสามารถแปลงกลับมาเป็น IP Address ได้แล้วนั้น ให้ทดสอบโดยใช้คำสั่ง ping ไปยัง yahoo.com เพื่อทดสอบว่า Router สามารถ forward packet ไปยังปลายทางที่ต้องการได้หรือไม่ โดยใช้คำสั่ง exit เพื่อออกมาจาก DNS Query Mode จากนั้นจึงสามารถใช้คำสั่ง ping ได้

```
C:\Users\Kru_eak>ping www.yahoo.com

Pinging fd-fp3.wg1.b.yahoo.com [106.10.138.240] with 32 bytes of data:
Reply from 106.10.138.240: bytes=32 time=92ms TTL=51
Reply from 106.10.138.240: bytes=32 time=75ms TTL=51
Reply from 106.10.138.240: bytes=32 time=90ms TTL=51
Reply from 106.10.138.240: bytes=32 time=94ms TTL=51

Ping statistics for 106.10.138.240:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 75ms, Maximum = 94ms, Average = 87ms
```

8. ในกรณีที่ไม่สามารถเชื่อมต่อ Internet โดยไม่สามารถ ping ไปยังเว็บไซต์ปลายทางที่ต้องการได้ (ในกรณีที่เว็บไซต์อนุญาตให้ใช้คำสั่ง ping ได้เท่านั้น) ให้ทดลองใช้คำสั่ง tracert http://www.yahoo.com เพื่อทดสอบว่าเส้นทาง หรือ hop ตรงจุดไหนที่มีปัญหา ทำให้ไม่สามารถ forward packet ออกไปได้ โดยคำสั่ง tracert -> TRACE ROUTE จะเป็นคำสั่งที่ใช้ในการตรวจสอบเส้นทางจากเครื่อง PC/Notebook ไปยังเว็บไซต์ปลายทางที่ต้องการเชื่อมต่อ

```
E:\Documents and Settings\suppasit>tracert www.sys2u.com

Tracing route to www.sys2u.com [203.150.231.71]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.10.10
  2    28 ms    28 ms    29 ms  ppp-124-120-130-1.revip2.asianet.co.th [124.120.
130.1]
  3    29 ms    28 ms    29 ms  ppp-210-86-189-43.revip.asianet.co.th [210.86.18
9.43]
  4    32 ms    30 ms    30 ms  10.169.43.1
  5    30 ms    30 ms    30 ms  58-97-25-102.static.asianet.co.th [58.97.25.102]

  6    30 ms    29 ms    29 ms  61-90-132-85.static.asianet.co.th [61.90.132.85]

  7    29 ms    30 ms    29 ms  203-144-193-65.static.asianet.co.th [203.144.193
.65]
  8    29 ms    32 ms    29 ms  TIG-Net31-137.trueinternetgateway.com [122.144.3
1.137]
  9    32 ms    31 ms    32 ms  TIG-Net31-98.trueinternetgateway.com [122.144.31
.98]
 10    32 ms    32 ms    32 ms  xge-333-cleopatra.inter.net.th [203.150.222.43]

 11    33 ms    31 ms    31 ms  host71.porar.com [203.150.231.71]

Trace complete.
```

สรุปผลการปฏิบัติงาน

.....

.....

.....

.....

.....

.....

.....

ตอบคำถาม

.....

.....

.....

.....

.....

.....

.....

ใบงานที่ 4

หน่วยที่ 3

ชื่อหน่วย แบบจำลองเครือข่ายและโพรโทคอล **เวลา** 2 **ชั่วโมง**

ชื่อใบงาน การแชร์ทรัพยากรบนเครือข่าย **สอนครั้งที่ 4**

จุดประสงค์การเรียนรู้

ด้านทักษะ (ปฏิบัติ)

1.สามารถตั้งค่าการใช้งานทรัพยากรร่วมกันบนเครือข่ายได้

เครื่องมือและอุปกรณ์

1. เครื่องคอมพิวเตอร์ พร้อมโปรแกรมระบบปฏิบัติการ Windows 1 ชุด
2. ระบบเครือข่าย LAN

ขั้นตอนการปฏิบัติงาน

สิ่งที่ต้องเตรียมก่อนการแชร์ไฟล์ระหว่าง Windows

ในการแชร์ File, Printer, Hard disk การแชร์ไฟล์ระหว่าง Windows 7 กับ Windows 7 โดยวิธีเหมาะสมสำหรับคอมพิวเตอร์ที่แชร์ไฟล์ที่ทำงานหรือสถานศึกษา

1. คอมพิวเตอร์ 2 เครื่องที่ลง Windows 7 แล้ว เช่น

- คอมพิวเตอร์เครื่องแรก (Computer Name = A) เครื่อง A เป็นเครื่องแม่ข่าย ที่เอาไว้แชร์ไฟล์
- คอมพิวเตอร์เครื่องสอง (Computer Name = B)

2. เชื่อมต่อสายแลน หรือรับสัญญาณมาจาก Wireless ทั้งคู่ (โดยได้รับ ip address แล้ว)

1. ตั้งค่าการแชร์ไฟล์ใน Windows 7

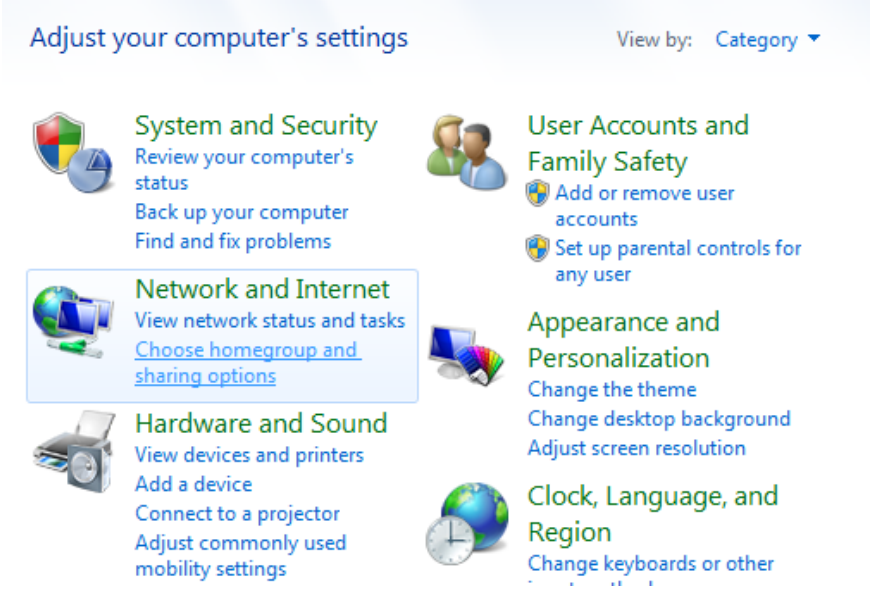
1.1 ขั้นตอนนี้จะเป็นการแชร์ไฟล์ระหว่างคอมพิวเตอร์ 2 เครื่อง

หมายเหตุ ถ้าต้องการจะแชร์ไฟล์เครื่องเดียว ให้ตั้งค่าเฉพาะเครื่องแม่ข่ายที่จะทำการแชร์ไฟล์

1.1.1 ไปที่ Start > Control Panel >

1.1.2 ปรับมุมมองเป็น Category

1.1.3 คลิ๊กที่ Choose Home group and Sharing options ดังภาพ



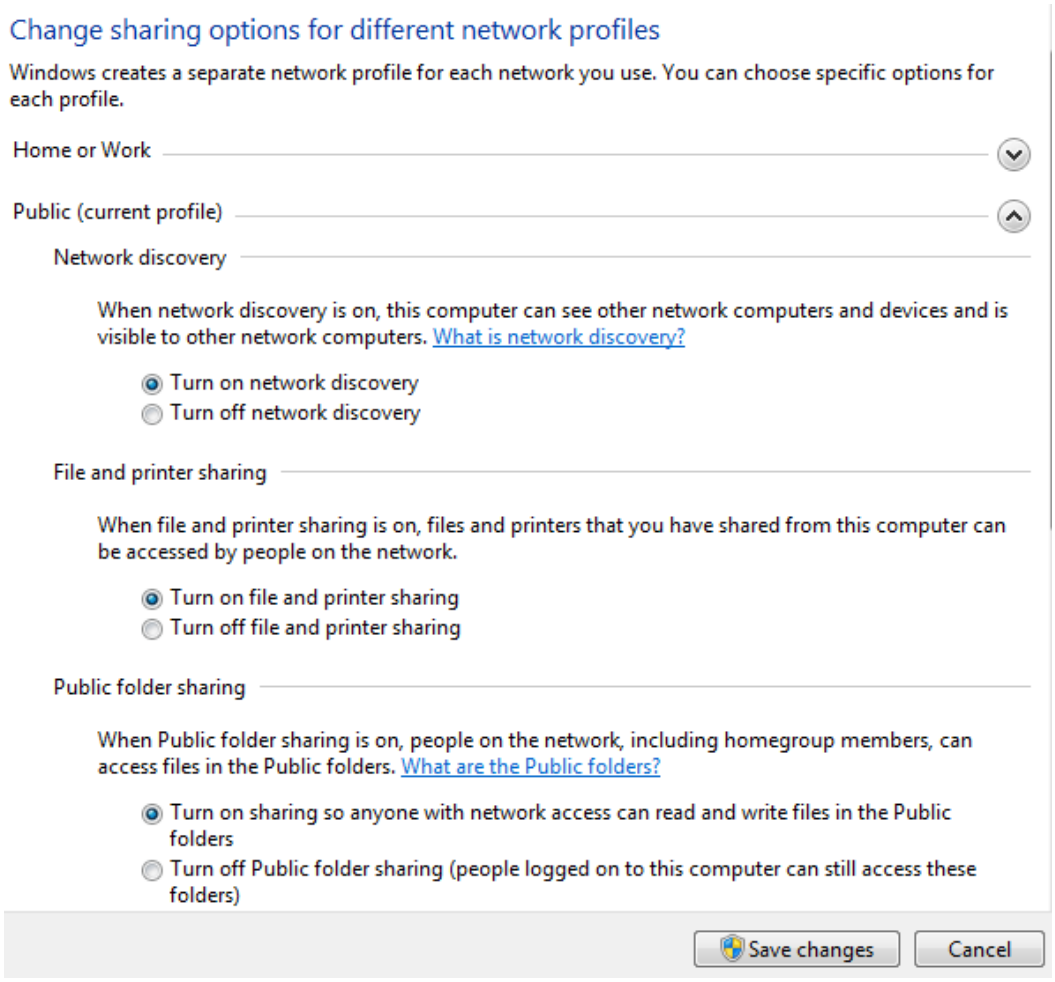
1.2 คลิ้ก Change advanced sharing settings.

1.3 ทำการเลือก Publish (Current Profile)

1.3.1 Network Discovery: เลือก.....

1.3.2 File and Printer sharing: เลือก.....

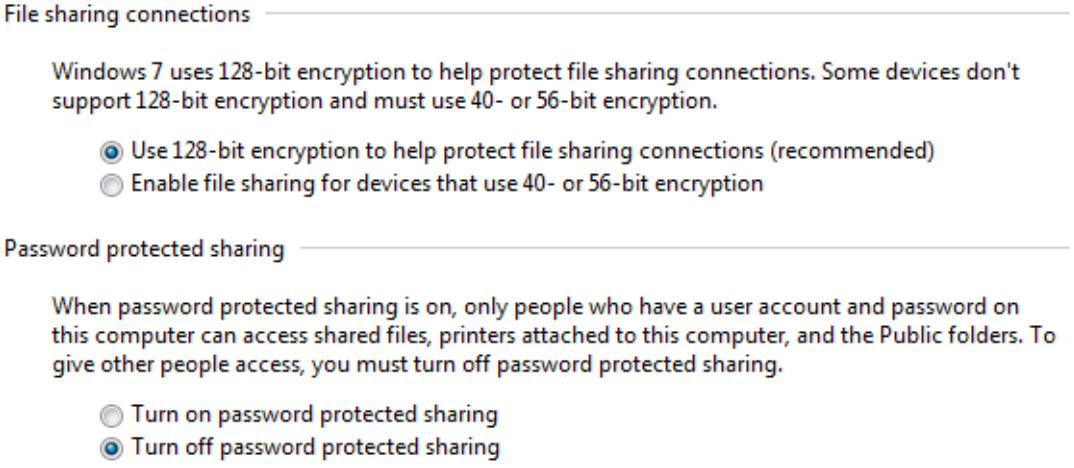
1.3.3 Publish folder sharing: เลือก.....



1.3.4 File Sharing connection: เลือก.....

1.3.5 Password protected sharing: เลือก.....

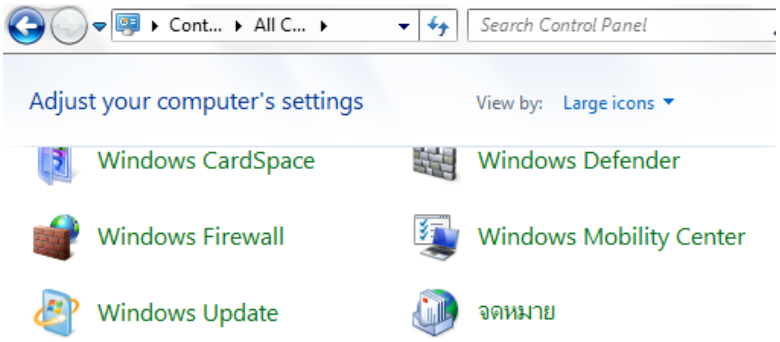
1.3.6 กด Save Change เพื่อเป็นการบันทึก



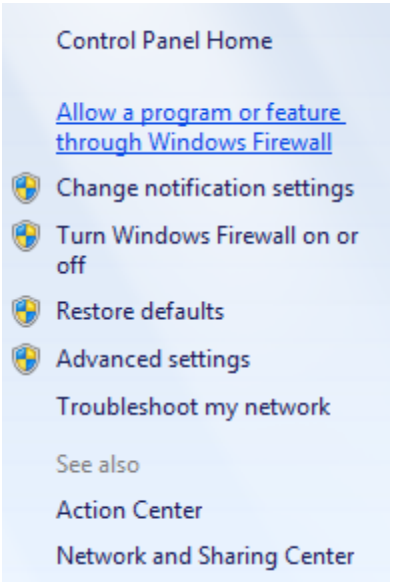
1.4 เลือก Control Panel

1.4.1 ปรับมุมมองเป็น Small icon

1.4.2 คลิ๊ก Windows Firewall



1.4.3 คลิ๊ก Allow a program or feature through Windows Firewall.

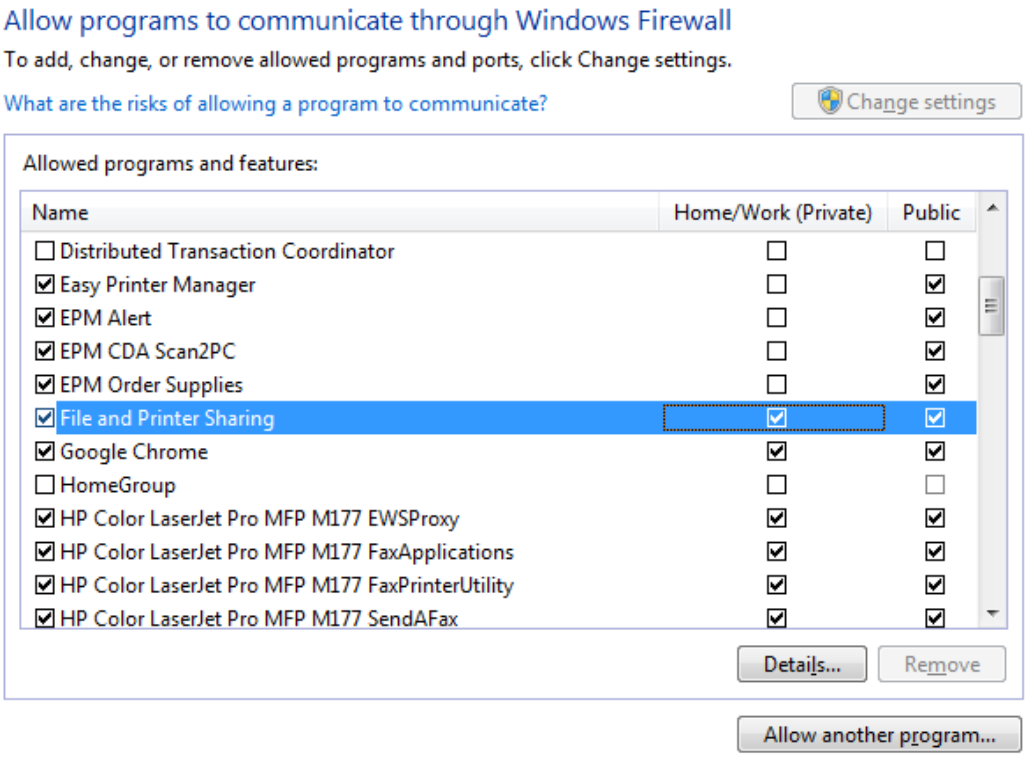


1.4.4 คลิ๊ก File and Printer sharing

1) เลือก Home/Work (Private)

2) เลือก Public

1.4.5 กด ok



2. ทดสอบการทำงาน

2.1 ทำการทดสอบการ Ping จากเครื่อง B ไปยังเครื่อง A ว่าสามารถ ping ได้หรือเปล่าไปที่คอมพิวเตอร์ B

2.2 ทำการ ping ไปยังเครื่อง A หรือ ping เครื่องปลายทางนั่นเอง โดยใช้ Command Ping Computer Name หรือ ping IP Address

ผลที่ได้.....

.....

.....

.....

.....

.....

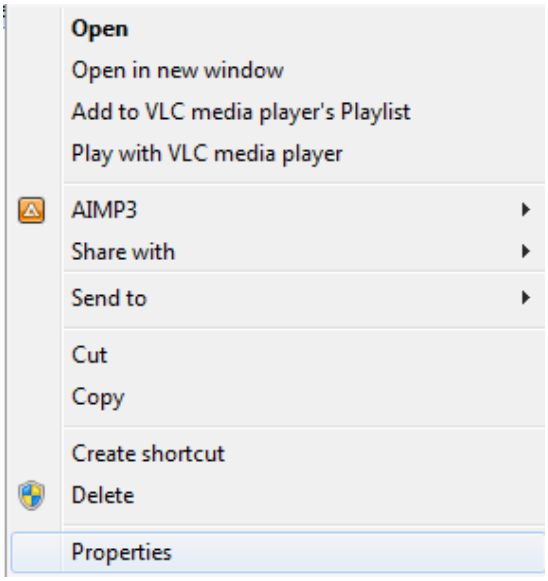
.....

3. แชร์ Folders ที่ต้องการแชร์ บนเครื่องหลักหรือเครื่องแม่

3.1 Folder ชื่อ Share A

3.1.1 คลิ้กขวาที่ folder

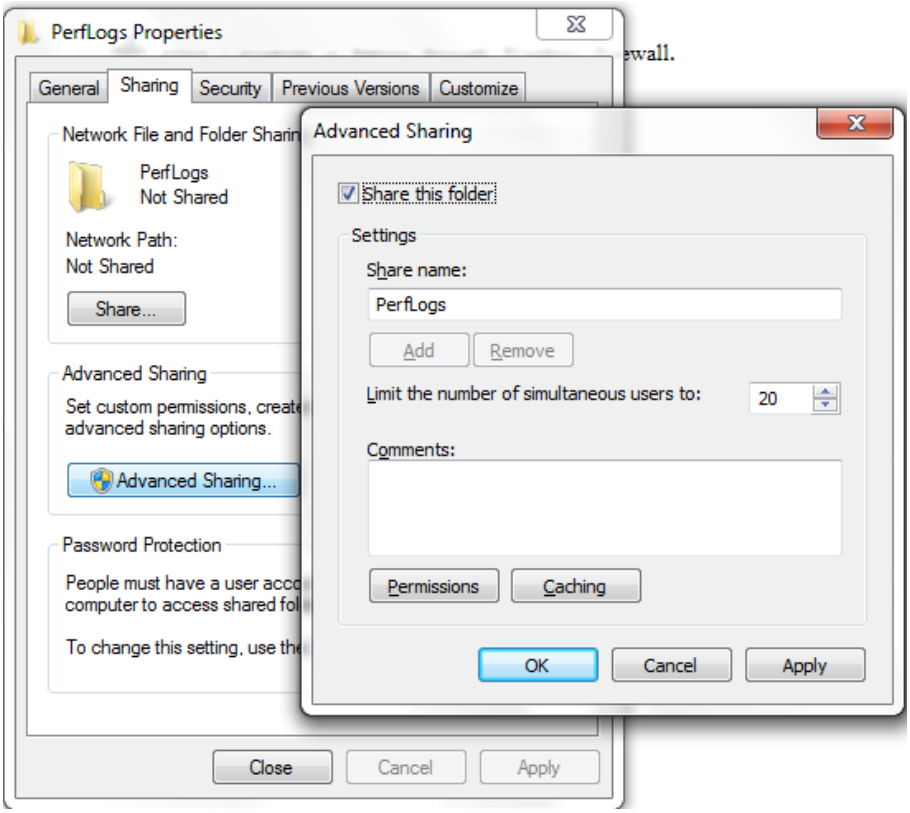
3.1.2 เลือก Properties



3.2 เลือก Tab: Sharing

3.2.1 คลิ๊ก.....

3.2.2 เลือก (/).....

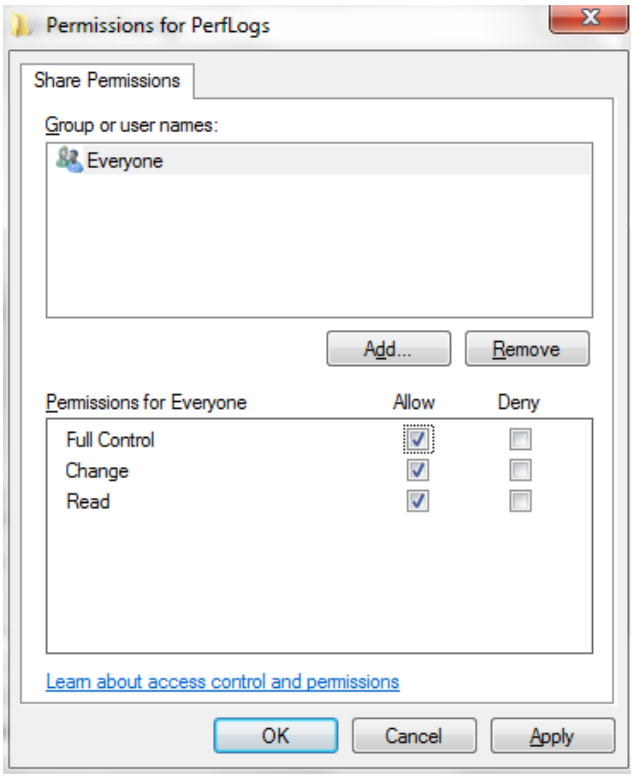


3.3 จากนั้นทำการกด Permission

3.3.1 คลิ้ก Everyone

3.3.2 ทำการปรับตามภาพ

3.3.3 กด OK เพื่อทำการบันทึกค่า



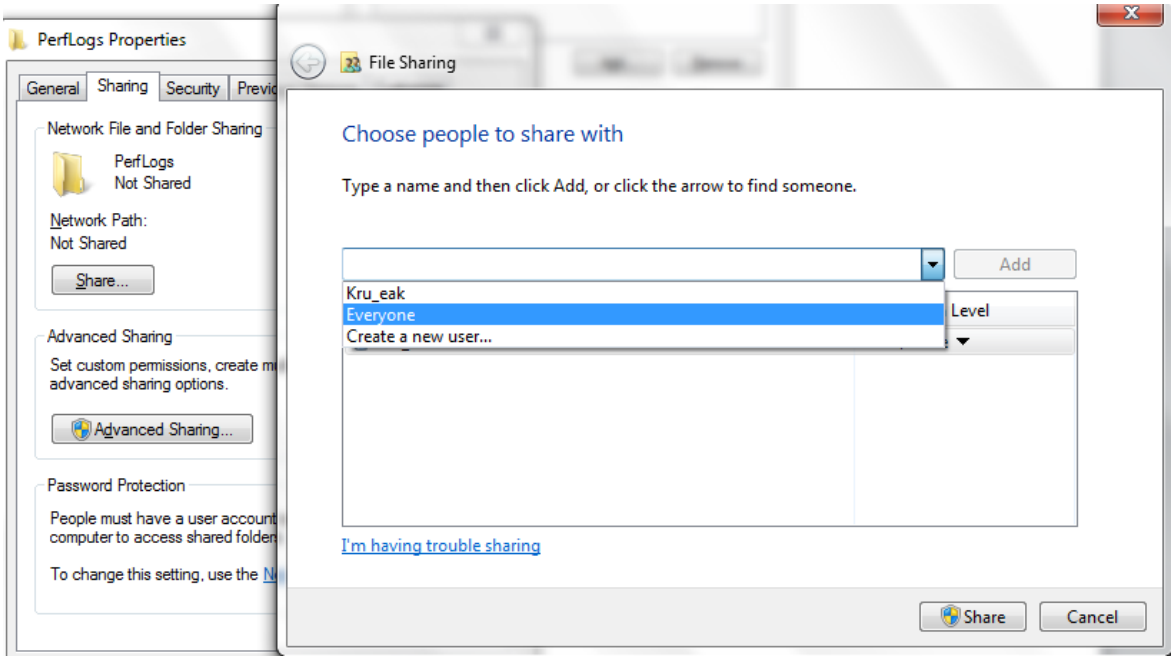
3.4. เลือก Tab: Sharing

3.4.1 เลือก Share จากนั้นการ

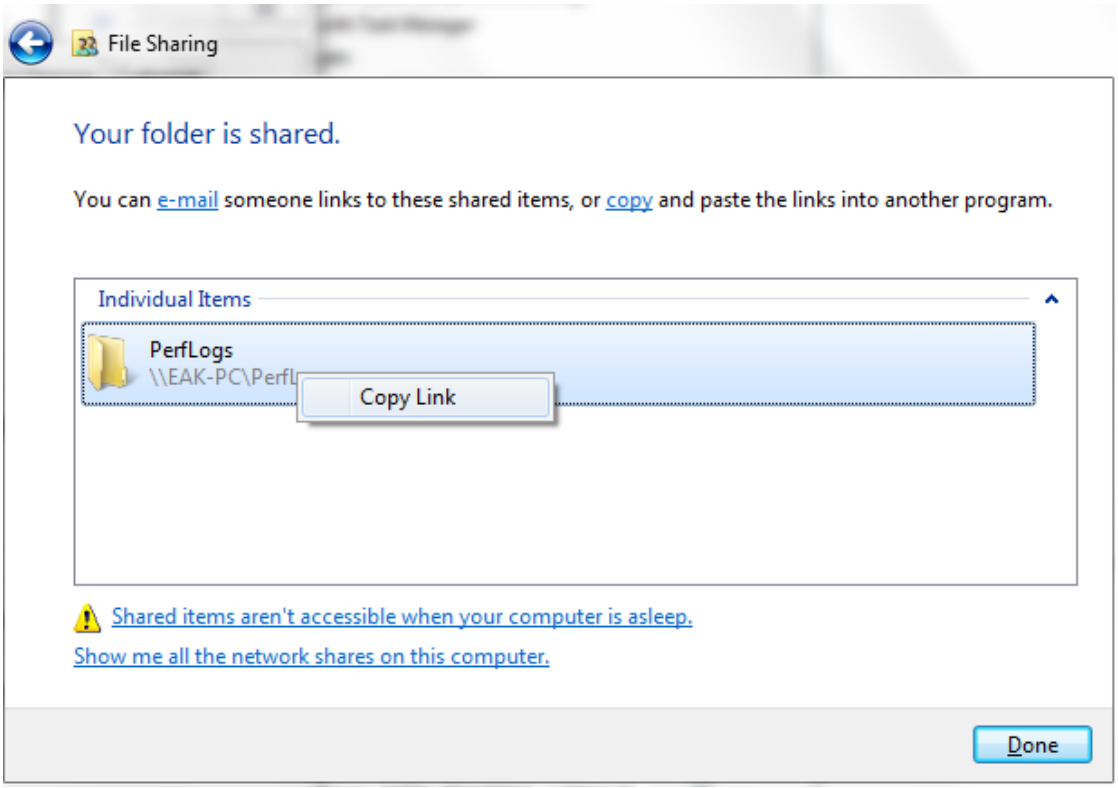
3.4.2 พิมพ์ลงไป Everyone และกด Add

3.4.3 เลือก Read/Chang

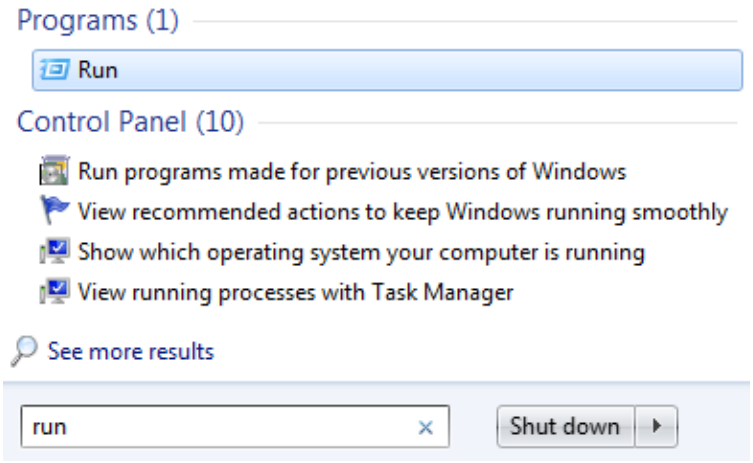
3.4.4 ทำการกด Share และ กด ok



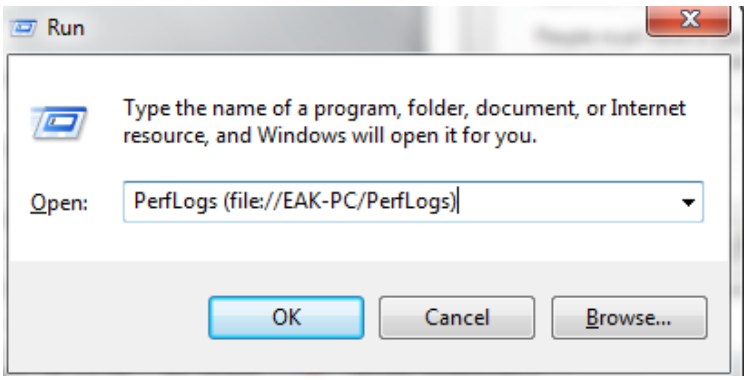
3.5 เมื่อเครื่องแม่ทำการแชร์ไฟล์เรียบร้อย จะมี Network Path ขึ้นมา ให้เอา URL ตรงนี้ไปใส่ที่เครื่องลูกเพื่อเข้ามาเอาไฟล์ในเครื่องแม่



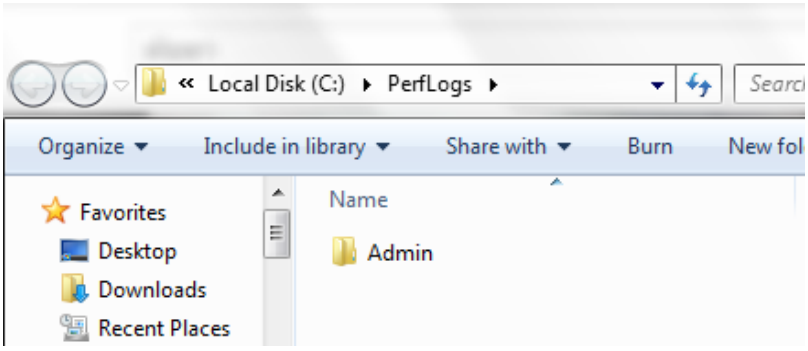
3.6 จากนั้นไปยังเครื่องลูกที่ต้องการเข้ามาดึงไฟล์จากเครื่องแม่กดปุ่ม Windows + R บน Keyboard หรือ Search แล้วพิมพ์คำว่า Run



3.7 แล้วพิมพ์ .....เพื่อที่จะทำการแชร์ไฟล์



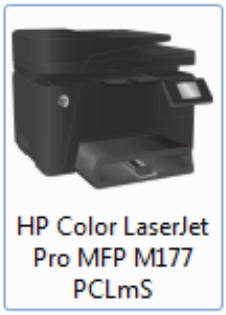
3.8 จะเห็น Folders ต่าง ๆ ที่อยู่ภายใต้ Folders ที่ ทำการแชร์บนเครื่องแม่ข่าย



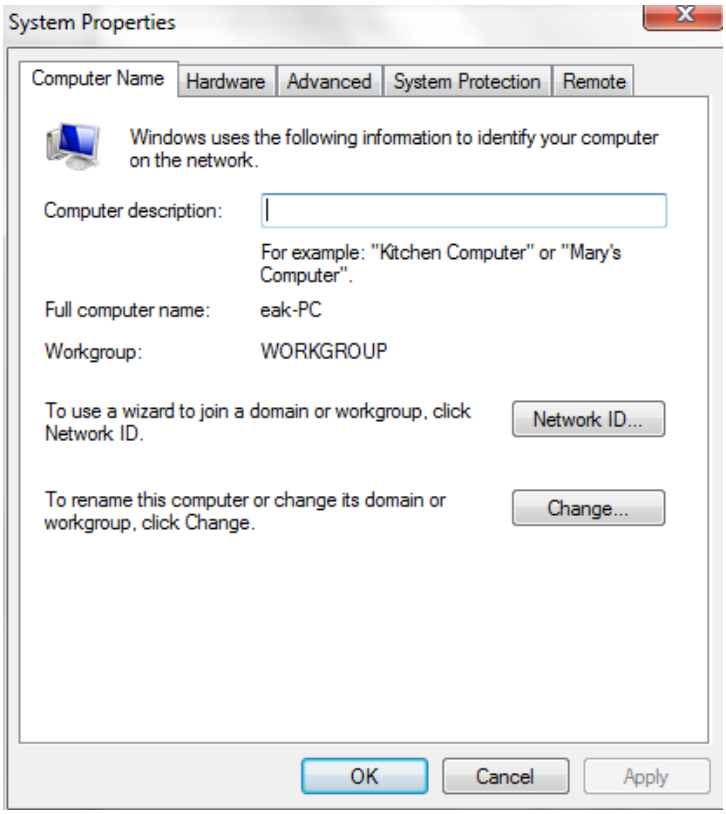
และขั้นตอนสุดท้ายก็สามารถเข้าใช้งานข้อมูลใน Folder ชื่อ Admin ได้

4. การแชร์ Printer

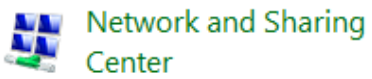
4.1 ทำการติดตั้งเครื่องพิมพ์ให้เรียบร้อย



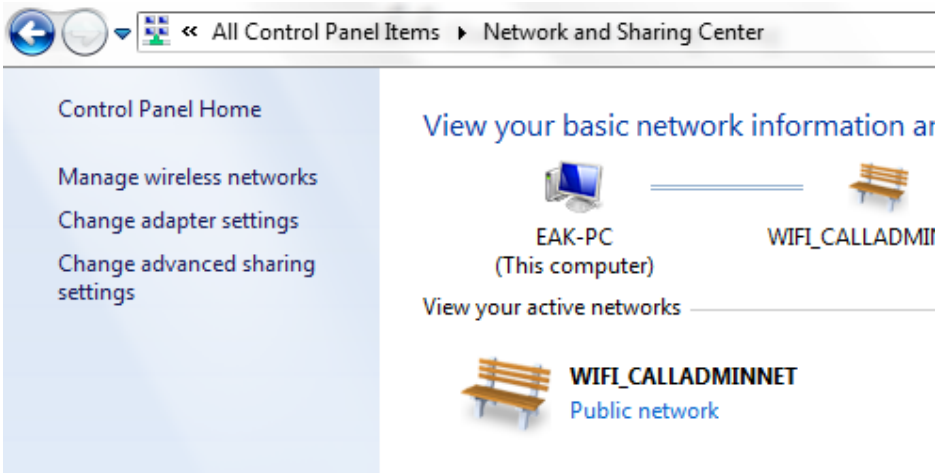
4.2 กำหนด Work group ให้เป็น group เดียวกัน



4.3 บน Windows 7 คลิ้กที่ Control Panel เลือก Network and Sharing Center



4.4 คลิ้กที่ Change advance sharing setting



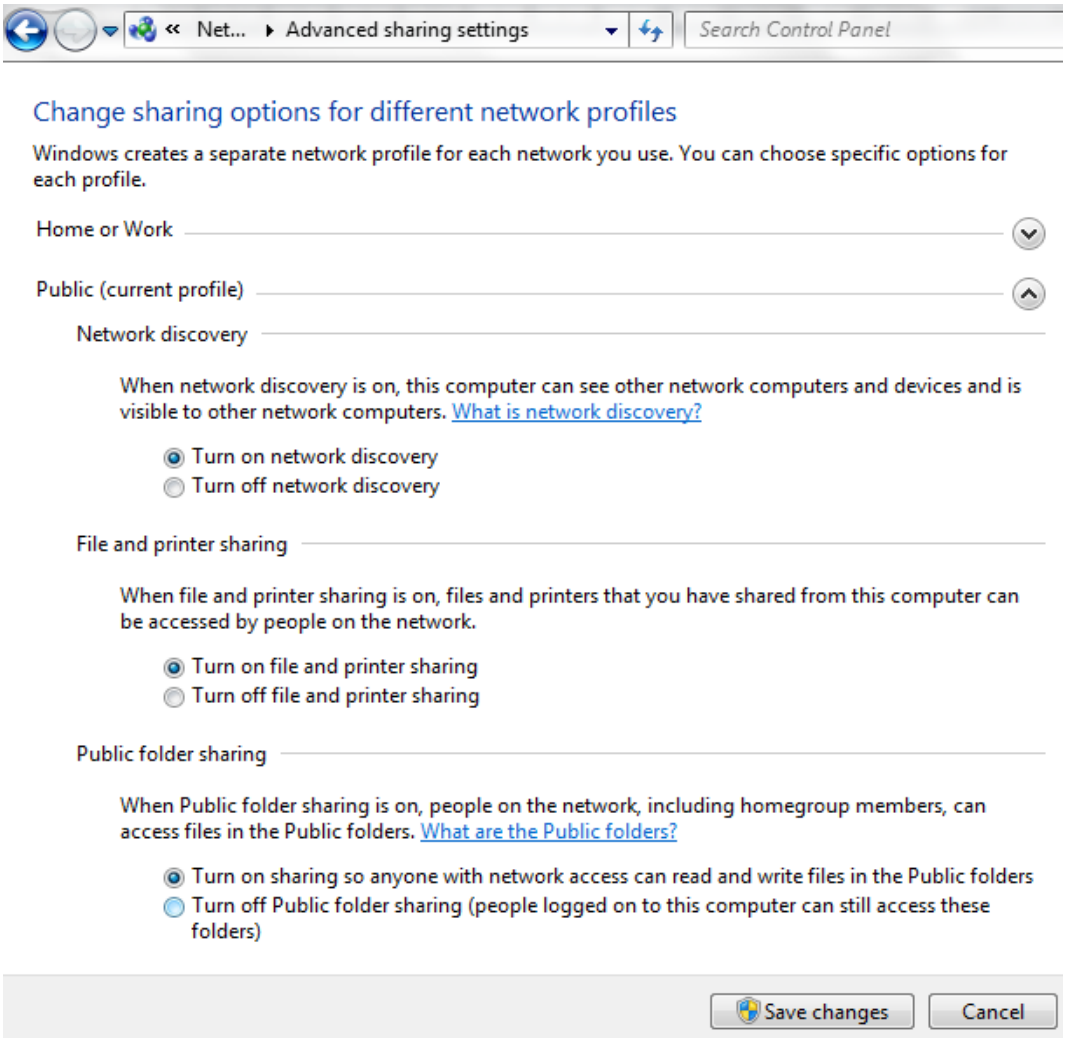
4.5 กำหนดให้

4.5.1 Turn on network discovery

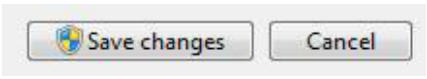
4.5.2 Turn on file and printer sharing

4.5.3 Turn on sharing so anyone with network access can read and write file in the public folder

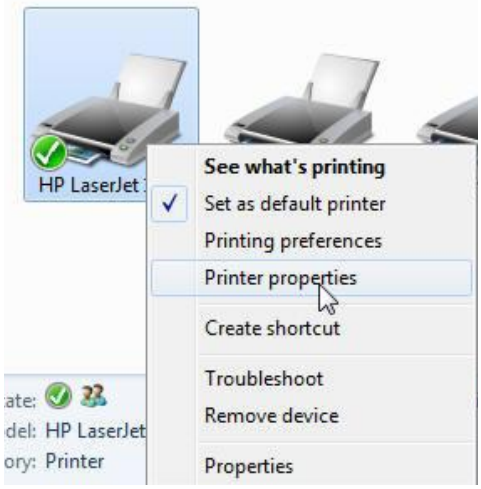
4.5.4 Turn off password protected sharing (หากไม่ Turn off password protected sharing แล้ว Windows จะไม่ให้ connect และต้องกรอกรหัสผ่าน)



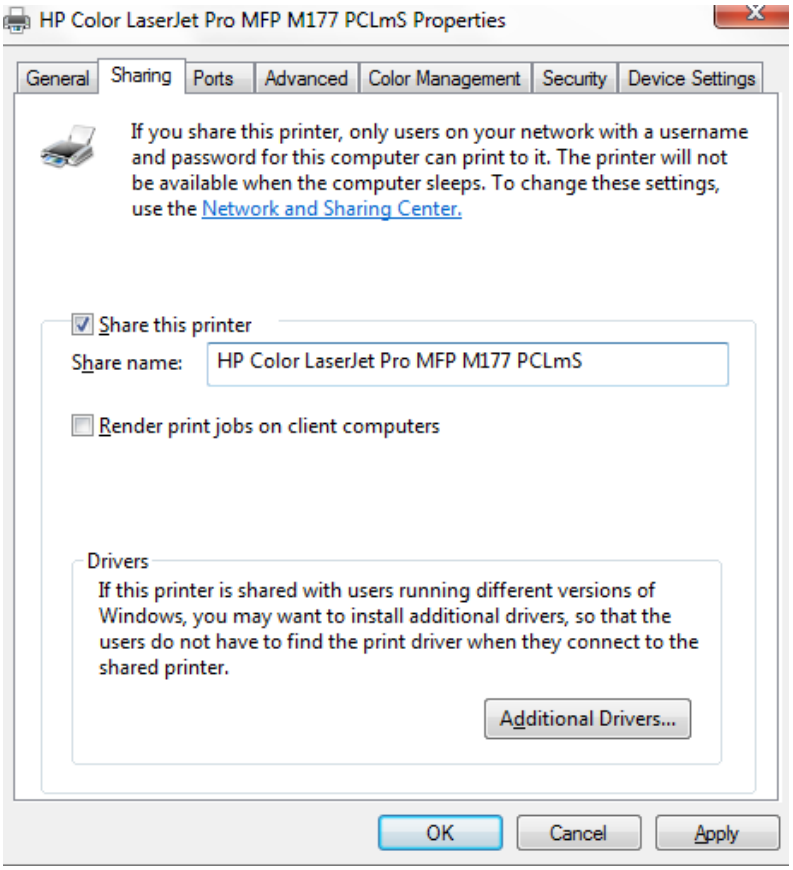
4.6 คลิ๊กปุ่ม Save changes



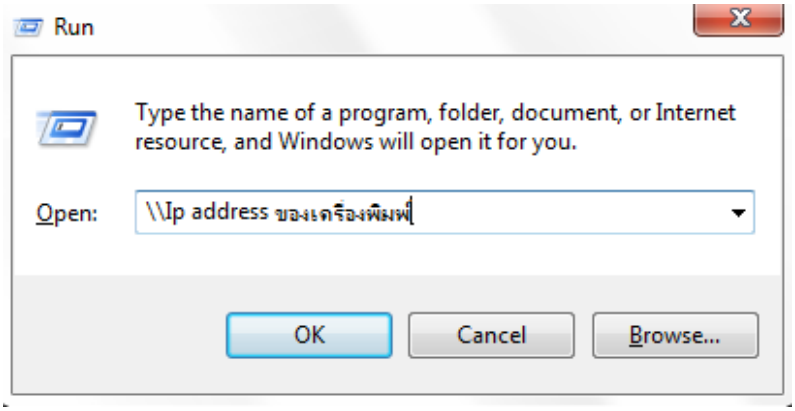
4.7 คลิ๊กขวาที่เครื่องพิมพ์เลือก Printer properties



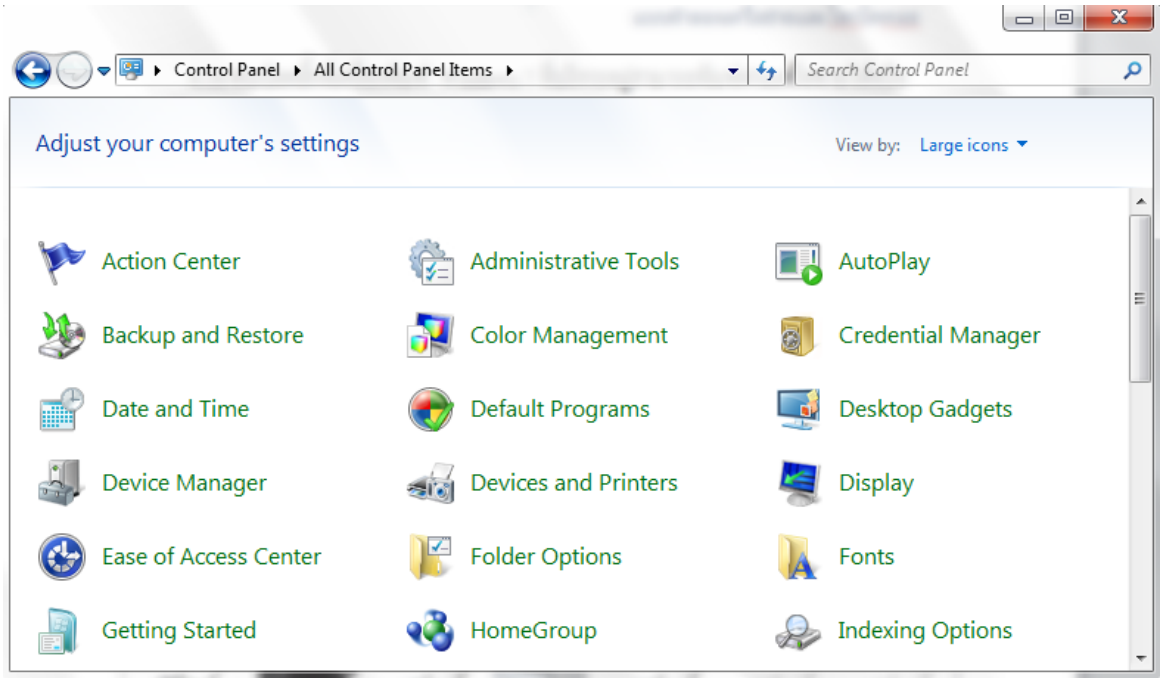
4.8 ใส่เครื่องหมายถูกหน้า ..... และ ..... แล้วคลิ้กปุ่ม OK



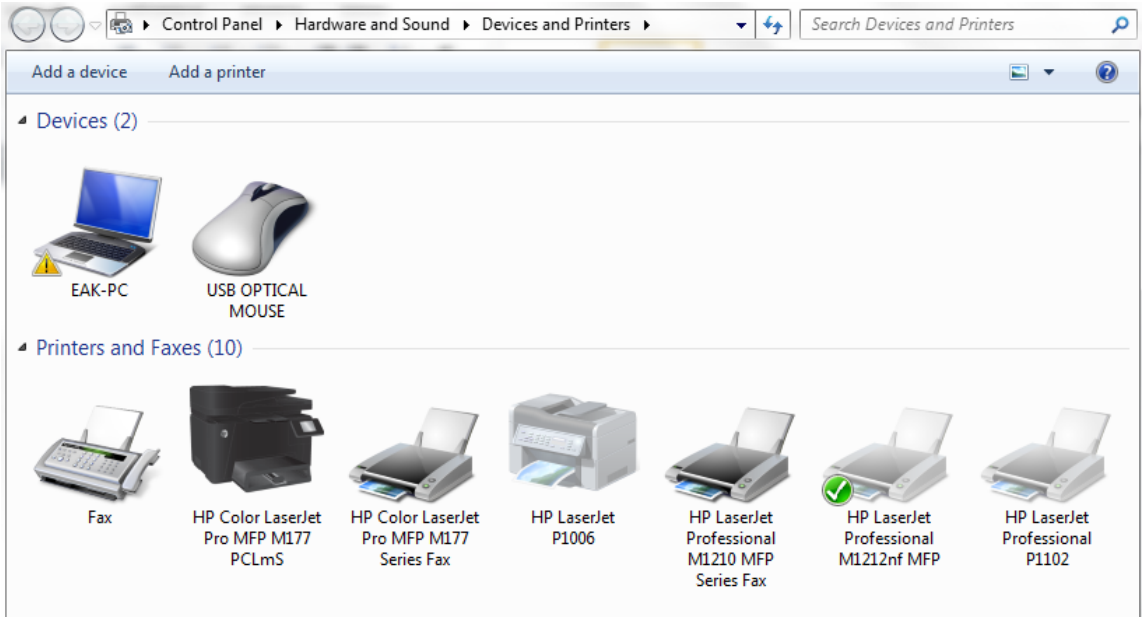
4.9 ให้คลิกที่ปุ่ม Start และ Run พิมพ์ \\ หมายเลข Ip Address ของเครื่องพิมพ์ที่ให้บริการบน Windows 7



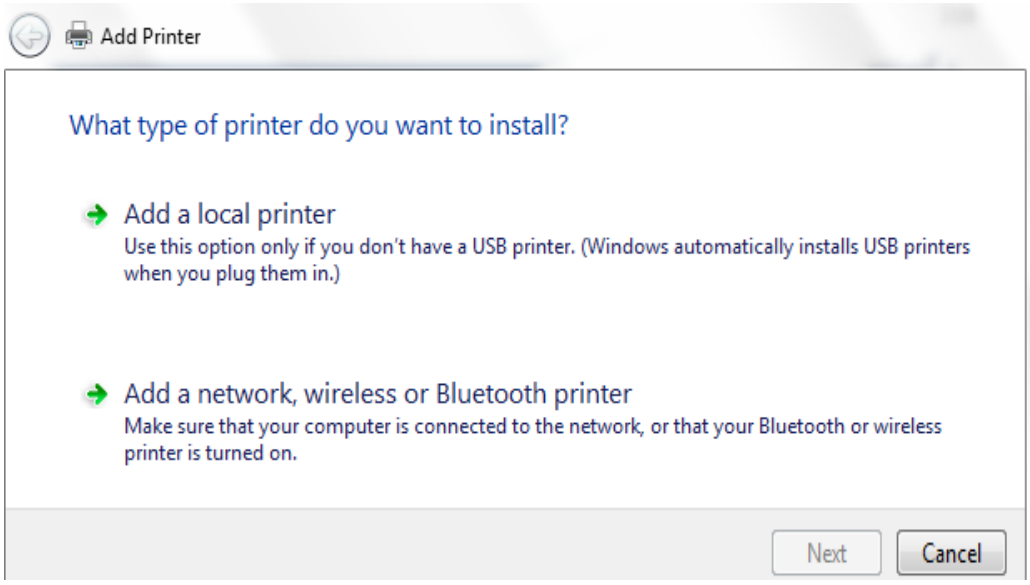
4.10 ดับเบิลคลิ๊กที่เครื่องพิมพ์ Windows 7 ที่บริการอยู่สามารถพิมพ์ผ่านเครือข่ายได้หรือเข้าไปที่ Control Panel เลือก Device and Printers



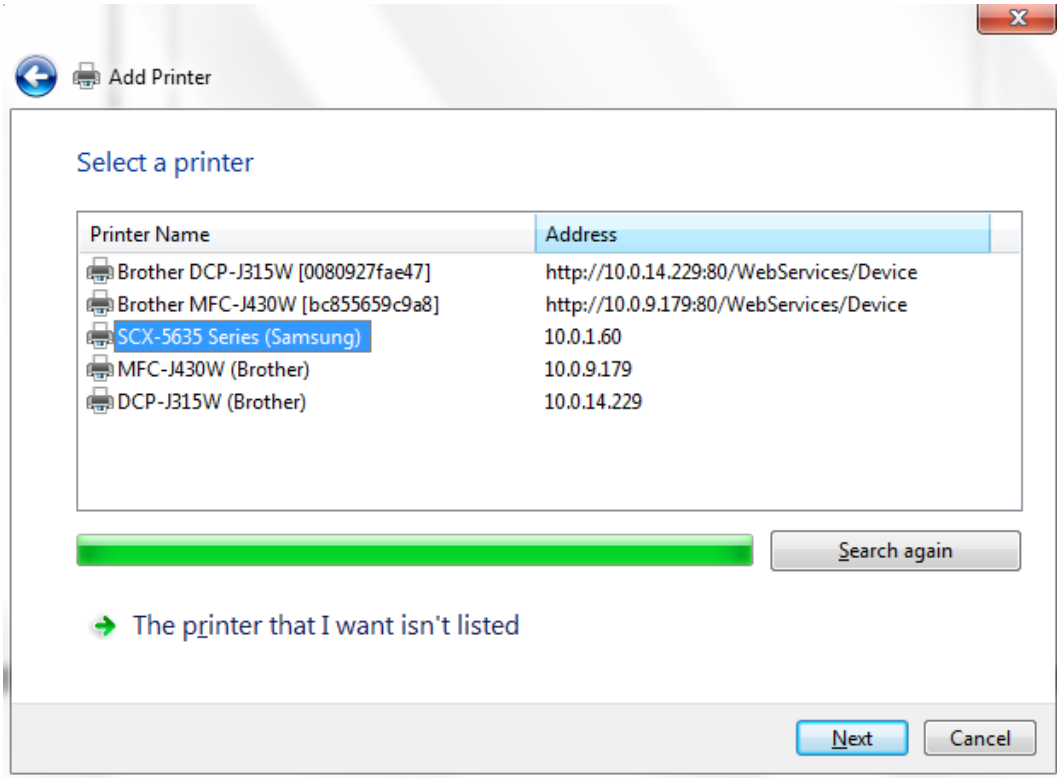
4.11 ทำการคลิ๊กเลือก Add a printer



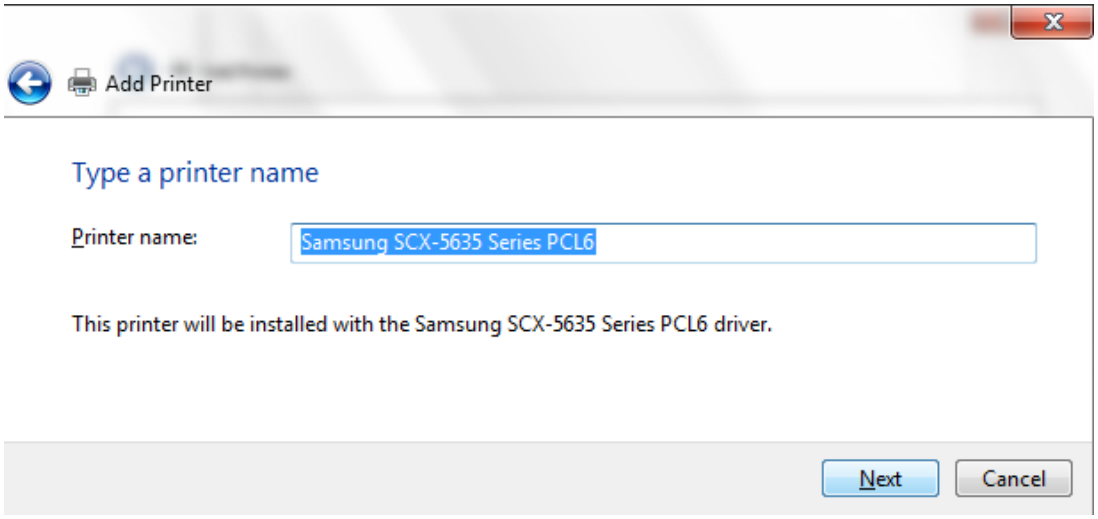
4.12 ทำการขั้นตอนการ Add a printer จนถึงหน้าต่างนี้ให้เลือก A network printer. or a printer attached computer แล้วกด Next



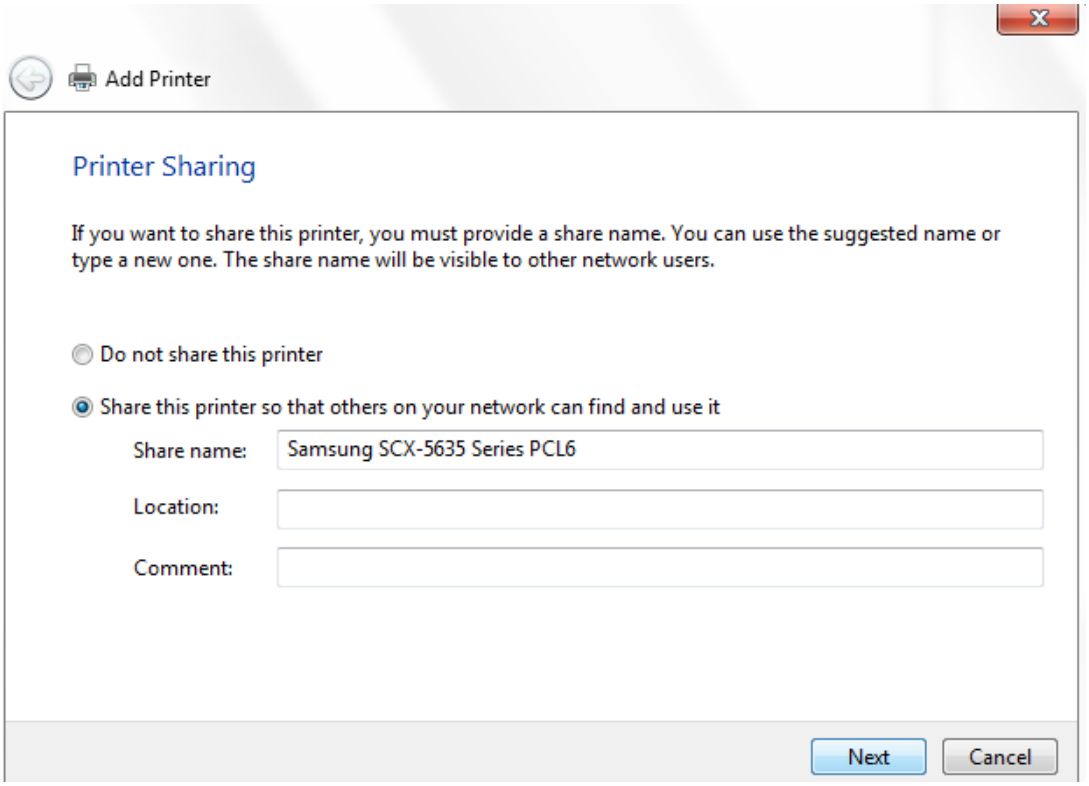
4.13 เลือก Add a network wireless or Bluetooth printer แล้วกด Next



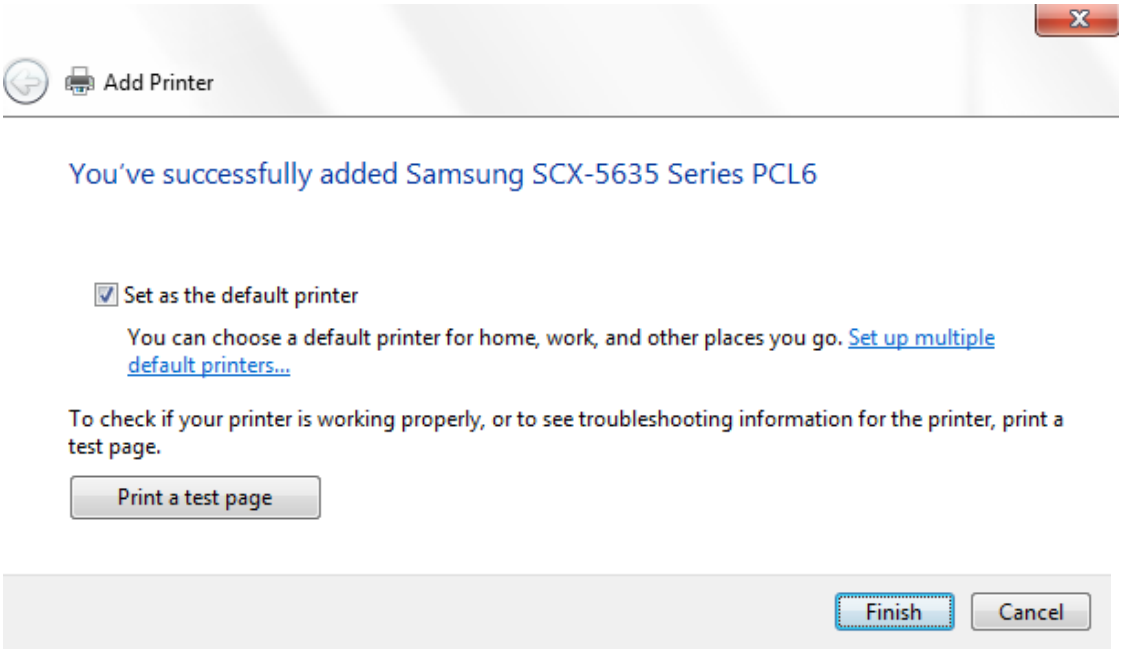
4.14 กดที่ Group เดียวกันเช่นข้างบน Windows 7 เลือกเป็น Work group ก็เลือกที่กลุ่ม Work group เหมือนกันและเลือกชื่อเครื่อง Print ที่ต้องการ



4.15 ทำตามขั้นตอนต่อไปจนเห็นว่า status: จะขึ้นว่า Ready แล้วกด Next เป็นอันเสร็จสิ้น



4.16 เลือก Share this printer so that on your network can find and use it แล้วคลิ้ก Next



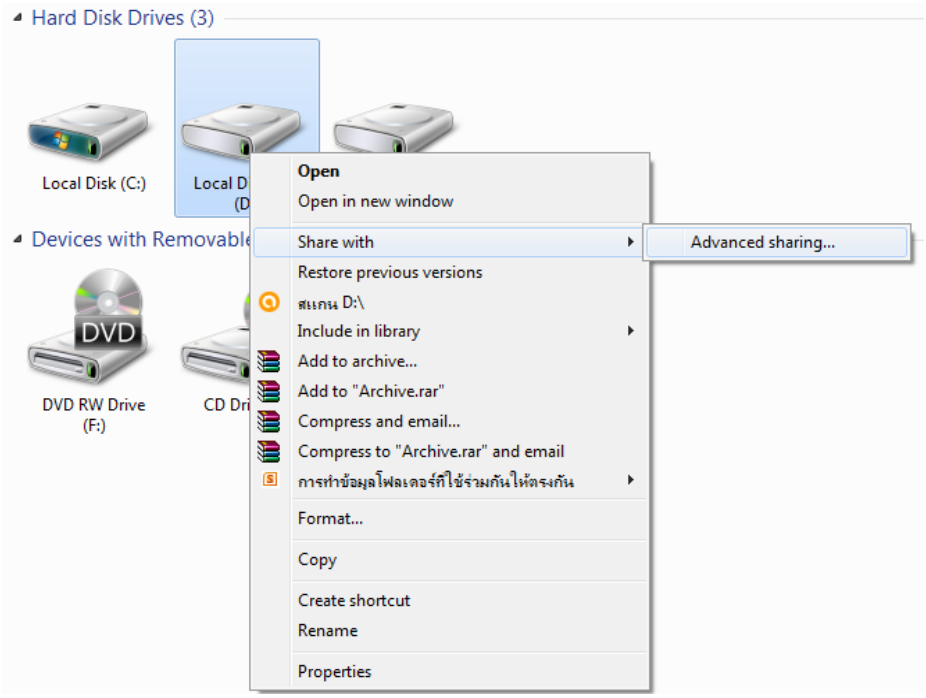
4.17 ขั้นตอนสุดท้ายเป็นการแจ้ง ติดตั้งเรียบร้อยแล้ว จะขึ้นว่า Ready แล้วกด next เป็นอันเสร็จสิ้น

5. การแชร์ Hard disk

5.1 เปิดโฟลเดอร์ Computer

5.1.1 คลิ้กขวาที่ไดร์ฟที่ต้องแชร์

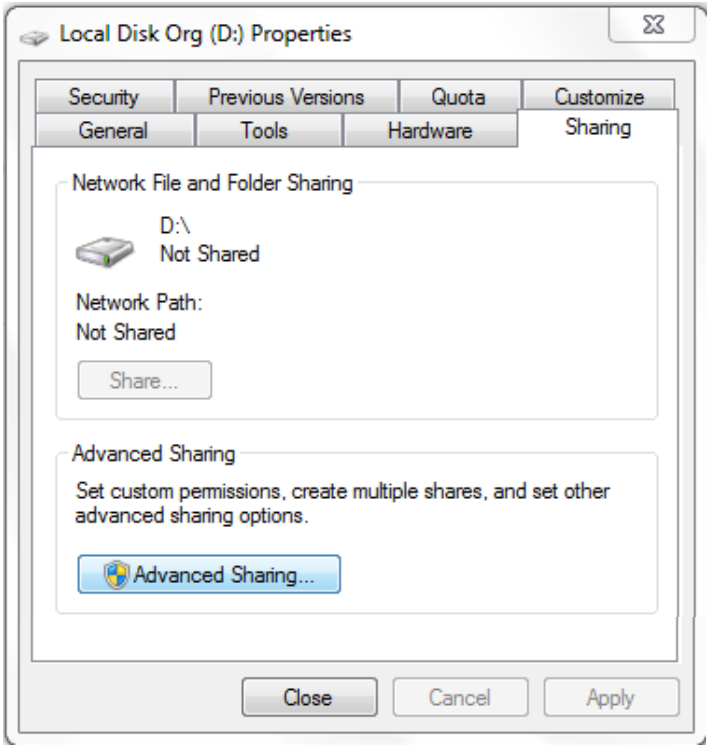
5.1.2 เลือกคำสั่ง Share with > Advanced sharing



5.2 หน้าต่าง System Properties ของไดร์ฟที่ต้องการแชร์แสดงออกมา

5.2.1 ไปที่ แท็บ Sharing

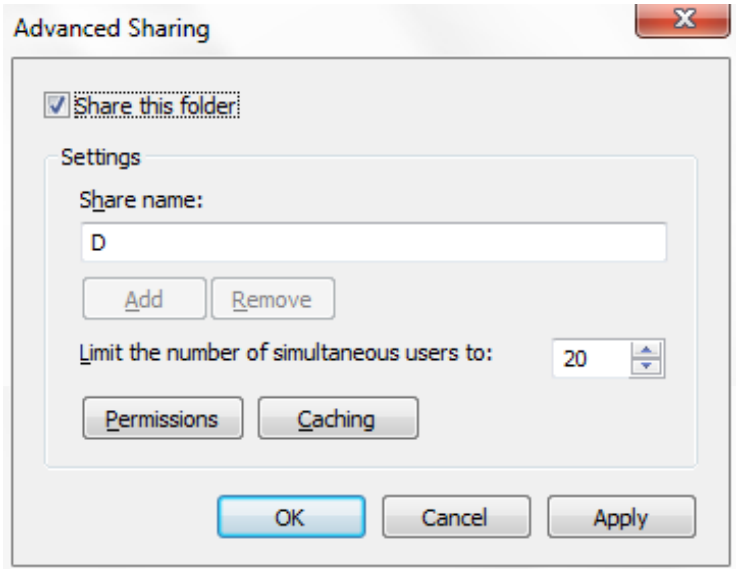
5.2.2 คลิ้ก Advanced Sharing



5.3 ต่อมาให้คลิ๊กทำเครื่องหมายถูกที่ Share this folder

5.3.1 ให้สังเกตที่ Share name: จะมีชื่อไดร์ฟ.....ที่ต้องการแชร์แสดงออกมา

5.3.2 คลิ๊กที่ OK เสร็จสิ้นขั้นตอนการแชร์ Hard disk



สรุปผลการปฏิบัติงาน

.....

.....

.....

.....

.....

ตอบคำถาม

.....

.....

.....

.....

.....

.....

เอกสารอ้างอิง

ก่อกิจ วีระอาชากุล . **Guide & Practice Network Administration**. นนทบุรี:
ไอดีซี พรีเมียร์ จำกัด. 2553

ฝ่ายผลิตหนังสือตำราวิชาการคอมพิวเตอร์.**การสื่อสารข้อมูลและเครือข่าย.**กรุงเทพฯ:
บริษัทซีเอ็ดยูเคชั่น จำกัด วี.พริ้นท์ (1991). 2551

พิศาล พิทยาธุรวิวัฒน์.**ติดตั้งระบบเครือข่ายคอมพิวเตอร์ Intranet/Internet ฉบับผู้เริ่มต้น**.
กรุงเทพฯ:บริษัทซีเอ็ดยูเคชั่น จำกัด วี.พริ้นท์ (1991). 2551

วิรินทร์ เมฆประดิษฐสิน.**คัมภีร์ระบบเครือข่ายแบบฉบับอาจารย์วิรินทร์ เล่ม 1** .กรุงเทพฯ:
บริษัทซีเอ็ดยูเคชั่น จำกัด เอช.เอ็น.กรุ๊ป .2547

จตุชัย แพงจันทร์.**เจาะระบบ Network ฉบับสมบูรณ์**.นนทบุรี:
บริษัทไอดีซี อินโฟ ดิสทริบิวเตอร์ เซ็นเตอร์ จำกัด.2546

เรืองไกร รังสิพล. **เจาะระบบ TCP/IP: จุดอ่อนของ Protocol และวิธีป้องกัน**. กรุงเทพฯ:
บริษัท โปรวิชั่น จำกัด. 2544

Cisco Systems, Inc. **Cisco Networking Academy Program CCNA 1 and 2 Companion Guide**. Indiana USA: Cisco Press. 2005

Cisco Systems, Inc. **Cisco Networking Academy Program CCNA 3 and 4 Companion Guide**. Indiana USA: Cisco Press. 2004

สืบค้นจาก http://www.tnetsecurity.com/content_basic/tcp_ip_knowledge.php
(สืบค้นเมื่อวันที่ 8 มีนาคม 2556)