บทที่ 2

แนวคิดและทฤษฎีที่เกี่ยวข้อง

2.1 โอเอสไอโมเดล (OSI Model)

ในปี ค.ศ.1977 องค์กรมาตรฐานไอเอสโอ (International Organization for Standardization) หรือไอเอสโอ (ISO) ได้มีการศึกษาและหาแนวทางในการกำหนดมาตรฐานของระบบเครือข่าย เพื่อช่วยแก้ไขปัญหาในการเชื่อมต่อระหว่างเครือข่าย ไอเอสโอ พบว่าระบบเครือข่ายจะมีกิจกรรมพื้นฐานที่คล้ายคลึงกัน เช่น การรับส่งข้อมูล การเข้าใช้งานเครื่องแม่ข่าย การสั่งพิมพ์ที่เครื่องพิมพ์ในเครือข่าย ฯลฯ ดังนั้น ไอเอสโอได้จัดแบ่งกิจกรรมต่าง ๆ ที่ได้มีการใช้งานในระบบเครือข่ายออกเป็นงานย่อย และกำหนดเป็นโมเดลมาตรฐาน โดยแบ่งเป็นชั้น ๆ ตามลำดับ 7 เลเยอร์ ซึ่งเรียกว่าการเชื่อมต่อระหว่างระบบเปิด (Open System Interconnection) หรือ โอเอสไอโมเดล (OSI Model) ด้วยวิธีการแบ่งกิจกรรมที่ซับซ้อนในเครือข่ายออกเป็นงานย่อย ๆ จะช่วยทำให้การออกแบบและ การใช้งานเครือข่ายรวมถึงการเชื่อมโยงกันเป็นไปได้ด้วยความสะดวกและมีวิธีการทำงานอยู่ในกรอบเดียวกัน โอเอสไอโมเดลนี้เป็นต้นแบบแนวคิดในการสร้างเครือข่ายและเป็นมาตรฐานให้กับผู้ที่ต้องการสร้างระบบเครือข่ายอุปกรณ์และซอฟต์แวร์ที่เกี่ยวข้อง

ในการจัดแบ่งชั้นต่าง ๆ ของโอเอสไอโมเดลเราสามารถที่จะแบ่งกลุ่มการใช้งานในแต่ละเลเยอร์ได้เป็นสองกลุ่ม คือ กลุ่มแรก ประกอบด้วย แอพพลิเคชั่นเลเยอร์ พรีเซ็นเตชั่นเลเยอร์ และเซสชั่นเลเยอร์ โดยในกลุ่มแรกนี้จะมีหน้าที่หลัก ในการจัดการเรื่องราวเกี่ยวกับงานของโปรแกรมประยุกต์ ในกลุ่มที่สองจะประกอบด้วย ทรานสปอตร์เลเยอร์ เน็ตเวิร์คเลเยอร์ ดาต้าลิงค์เลเยอร์ และฟิสิคอลเลเยอร์ จะทำหน้าที่ในจัดการเรื่องราวของการส่งข้อมูลในเครือข่ายเดียวกันและระหว่างเครือข่าย รายละเอียดของแต่ละชั้นเป็นไปตามตารางที่ 2.1 ดังนี้

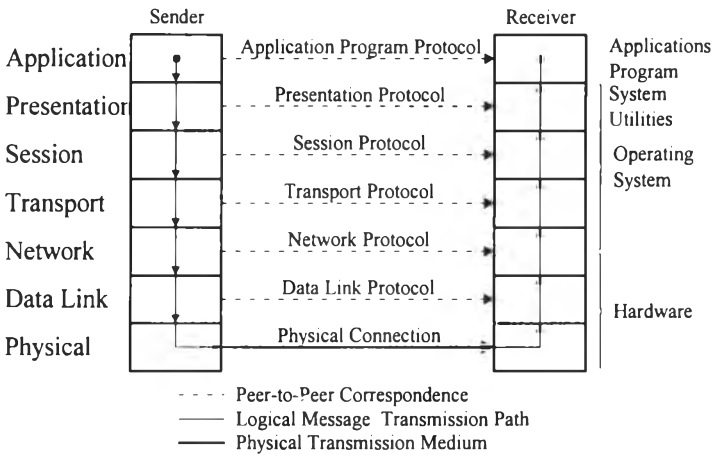
เลเยอร์ที่	รายละเอียด
7 แอพพลิเคชั่น (Application)	เป็นเลเยอร์บนสุดของโมเดล มีหน้าที่ในการดูแลเครือข่ายกับ ผู้ใช้เป็นไปได้ตามต้องการ เช่น ระบบไปรษณีย์อิเล็กทรอนิกส์ (E-mail) การถ่ายโอนแฟ้มข้มูล (File Transfer) การขอเข้าใช้ระบบคอมพิวเตอร์ในเครือข่าย (Host terminal) เป็นต้น แอพพลิเคชั่นของ เครือข่ายจะทำหน้าที่จัดการเรื่องต่าง ๆ ของเครือข่ายตามที่ผู้ใช้ต้องการ โดยจะอยู่ระดับบนที่ใกล้ชิดกับผู้ใช้ที่มากสุด

ตารางที่ 2.1 : แสดงหน้าที่และการทำงานของโอเอสไอ 7 เลเยอร์

เลเยอร์ที่	รายละเอียด
6 พรีเซ็นเตชั่น (Presentation)	เป็นเลเยอร์ที่มีหน้าที่หลักคือเป็นส่วนที่จัดรูปแบบ และนำเสนอข้อมูลให้เป็นไปตามต้องการ รวมไปถึงการจัดแปลงข้อมูลใน รูปมาตรฐานแอสกี (ASCII) การลดขนาดข้อมูล (Data Compression) การเข้ารหัสหรือถอดรหัสของข้อมูลเพื่อความ ปลอดภัยในการสื่อสาร แต่ส่วนใหญ่แล้วแอพพลิเคชั่นจะเป็นตัวจัดการแทนให้
5 เซสชั่น (Session)	เป็นเลเยอร์ที่เป็นตัวจัดการในเรื่องของการสร้าง "การติดต่อแต่ละครั้ง" หรือ เซสชั่น ให้ระบบคอมพิวเตอร์ทั้งสองฝั่ง โดยทำหน้าที่ตั้งแต่เริ่มการติดต่อ ดูแลให้การส่งผ่านข้อมูลในการติดต่อครั้งนั้น ๆ เป็นไปได้โดยไม่มีปัญหา จนถึงการเลิกการติดต่อเมื่อเสร็จงาน
4 ทรานสปอตร์ (Transport)	เป็นเลเยอร์ที่มีหน้าที่ในการควบคุมปริมาณและรายละเอียดเกี่ยวกับวิธีการรับส่งข้อมูล ให้เป็นไปตามที่ได้กำหนดไว้ ตลอดจนจัดการให้การเชื่อมโยงเครือข่ายเป็นไปอย่างราบรื่น ในเลเยอร์นี้เป็นเลเยอร์สุดท้ายที่จัดการเรื่องของเส้นทางในการส่งข้อมูลและจัดการตรวจสอบความผิดพลาดของข้อมูล
3 เน็ตเวิร์ค (Network)	เป็นเลเยอร์ที่มีหน้าที่ในการควบคุมวิธีการส่งผ่านข้อมูล ระหว่างเครือข่ายให้ถูกต้องและเป็นไปตามเส้นทางที่กำหนดไว้ นอกจากนี้ยังจะทำหน้าที่ในการจัดการดูแล เส้นทางในการส่งข้อมูล และกั้นหรือกรองข้อมูลที่ส่งไปยังที่หมายภายในเครือข่ายเดียวกัน ไม่ให้ข้ามไปยังเครือข่ายย่อยอื่น ซึ่งจะช่วยลดปริมาณข้อมูลที่จะวิ่งบนเครือข่ายได้ส่วนหนึ่ง
2 ดาต้าลิงค์ (Data Link)	เป็นเลเยอร์ที่มีหน้าที่ในการกำหนดวิธีในการเรียกใช้ช่องทางในการส่งข้อมูล (Access Method) ให้ถูกต้อง เช่น อีเธอร์เน็ต ฯลฯ ตลอดจนรวมถึงการควบคุมลำดับอัตราการรับส่งข้อมูล ที่อยู่ปลายทางที่จะส่งข้อมูลไป ในเลเยอร์นี้จะเป็นเลเยอร์แรกที่จัดการแปลงข้อมูลจากบิตให้อยู่ในรูปของ แพ็กเก็ต โดยจะมีการเพิ่มข้อมูลเพื่อใช้ในการตรวจสอบความถูกต้อง ในกรณีที่ต้องการส่งข้อมูลออกไป หรือ ในกรณีอ่านข้อมูลเข้ามาก็จะมีการตรวจสอบความถูกต้อง เพื่อดูว่าข้อมูลที่ได้รับมาถูกต้องครบถ้วนหรือไม่ ถ้าถูกต้องข้อมูลนั้นก็สามารถที่จะนำไปใช้งานได้ แต่ถ้าไม่ถูกต้องก็จะไม่มีการนำข้อมูลนั้นมาใช้และบอกไปยังต้นทางให้ส่งมาใหม่
1 ฟิสิคอล (Physical)	เป็นเลเยอร์ที่มีหน้าทำหน้าที่ในการรับผิดชอบดูแลในรายละเอียดการส่งข้อมูลในด้านฮาร์ดแวร์จริง เช่น การส่งสัญญาณผ่านสายสัญญาณแบบต่าง ๆ การเชื่อมต่อเข้าเครือข่ายแบบต่าง ๆ ในเลเยอร์นี้จะจัดการในเรื่องของสัญญาณทางไฟฟ้า สัญญาณเสียง สัญญาณแสงที่จำเป็นในการสื่อสารโดยตรง

ตารางที่ 2.1 : แสดงหน้าที่และการทำงานของ โอเอสไอ 7 เลเยอร์ (ต่อ)

การติดต่อสื่อสารแต่ละชั้นของ โอเอสไอโมเดล จะมีการแบ่งองค์ประกอบที่เกี่ยวข้องออกเป็นสองประเภทคือ ผู้ส่งข้อมูล (Sender) และผู้รับข้อมูล (Receiver) โดยจะมีการรับส่งข้อมูลกันตามลำดับชั้น โดยเริ่มจากผู้ส่งข้อมูลจะมีการส่งข้อมูลจาก แอพพลิเคชั่นเลเยอร์มายังฟิสิคอลเลเยอร์ ในทางกลับกัน ผู้รับข้อมูลก็จะมีการรับข้อมูลจาก ฟิสิคอลเลเยอร์แล้วส่งไปยังแอพพลิเคชั่นเลเยอร์ ดังแสดงในรูปที่ 2.1



รูปที่ 2.1 แสดงการรับ-ส่งข้อมูลบนโอเอสไอ 7 เลเยอร์

(Uyless Black, 1994.)

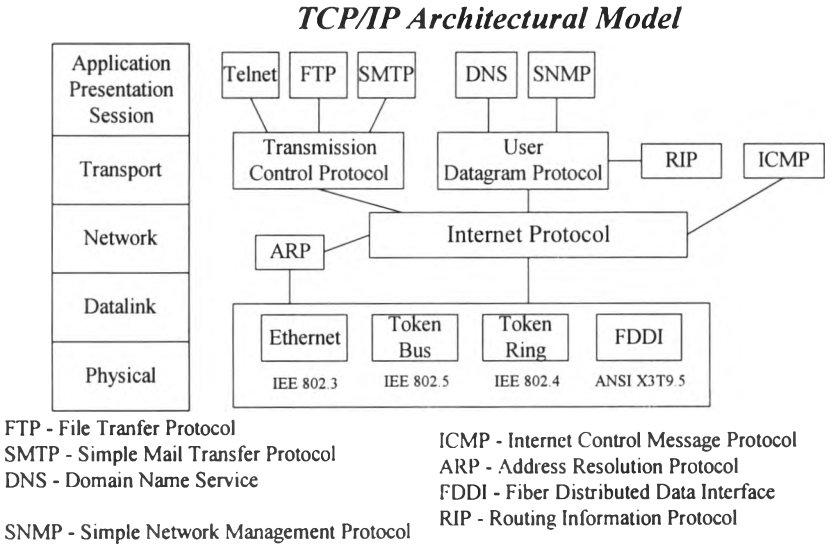
2.2 โพรโทคอลทีซีพี/ไอพี (TCP/IP Protocol)

โพรโทคอลทีซีพี/ไอพี (TCP/IP) หรือ ทรานสมิทชั่นคอนโทรโพรโทคอลอินเตอร์เน็ตโพรโทคอล (Transmission Control Protocol/Internet Protocol) เป็นข้อกำหนดหรือวิธีการในการสื่อสารระหว่างคอมพิวเตอร์ที่ใช้กันอย่างกว้างขวางและถือเป็นมาตรฐานในปัจจุบันนี้ จุดกำเนิดของโพรโทคอลทีซีพี/ไอพีเริ่มขึ้นประมาณปี พ.ศ. 2512 โดยกระทรวงกลาโหมของสหรัฐ พบปัญหาในการเชื่อมโยงเครือข่ายคอมพิวเตอร์ที่ใช้ในหน่วยงานต่าง ๆ ที่มีอยู่ ซึ่งจะต้องมีการส่งข้อมูลไปยังหน่วยงานภายนอกอื่น ๆ เช่น มหาวิทยาลัย ห้องทดลองต่าง ๆ ซึ่งแต่ละแห่งก็มีระบบคอมพิวเตอร์ที่แตกต่างกันไป และการเชื่อมต่อระบบเครือข่ายภายในของแต่ละที่ก็ต่างกัน จึงทำให้ข่าวสารข้อมูลทั้งหลายจึงไม่สามารถที่จะถ่ายเทกันไปมาได้ ดังนั้นกระทรวงกลาโหมสหรัฐได้จัดตั้งหน่วยงาน แอดวานซ์รีเสิร์ทโปรเจคส์เอเยนซี่ (Advanced Research Projects Agencies) หรือ อาร์พา (ARPA) ขึ้นมา เพื่อกำหนดมาตรฐานในการสื่อสารข้อมูลและได้จัดตั้งเครือข่ายอาร์พาเน็ต (ARPANET) ขึ้นโดยใช้โพรโทคอล ทีซีพี/ไอพี ซึ่งได้รับการยอมรับและเป็นมาตรฐานต่อมาในปี พ.ศ. 2525

ความสัมพันธ์ระหว่างโพรโทคอลทีซีพี/ไอพีกับระบบปฏิบัติการยูนิกซ์เกิดขึ้นเนื่องจากมหาวิทยาลัยแคลิฟอร์เนียที่เบอร์คเลย์ ได้พัฒนาระบบปฏิบัติการยูนิกซ์ ซึ่งมีการผนวกเข้ากับโพรโทคอลทีซีพี/ไอพี สำหรับใช้ในการสื่อสารระหว่างระบบ และเผยแพร่ต่อไปยังหน่วยงานต่าง ๆ ทำให้การสื่อสารกันของเครื่องที่ใช้ระบบปฏิบัติการส่วนใหญ่มักจะต้องใช้โพรโทคอลทีซีพี/ไอพีมาถึงปัจจุบัน

2.3 โพรโทคอลทีซีพี/ไอพี (TCP/IP Protocol) กับโอเอสไอโมเดล (OSI Model)

ลักษณะในการเปรียบเทียบในแง่การทำงานของโพรโทคอลทีซีพี/ไอพี กับโอเอสไอโมเดล จะเปรียบเทียบกันได้ดังรูปที่ 2.2



รูปที่ 2.2 แสดงการเปรียบเทียบการทำงานของโพรโทคอลทีซีพี/ไอพีกับโอเอสไอ 7 เลเยอร์
(Uyless Black , 1994)

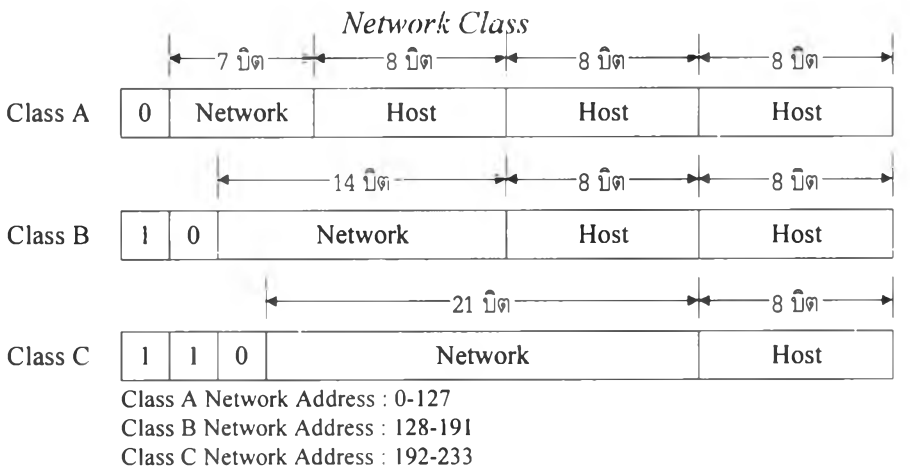
จากรูปที่ 2.2 โพรโทคอลทีซีพี/ไอพีจะแบ่งการทำงานกันเป็น 2 ส่วนคือ โพรโทคอลทีซีพีจะทำงานอยู่ในเลเยอร์ที่ 3 หรืออยู่ในเลเยอร์ของเน็ตเวอร์คเลเยอร์และโพรโทคอลไอพีจะทำงานอยู่ในเลเยอร์ที่ 4 หรืออยู่ในเลเยอร์ของ ทรานสปอร์ตเลเยอร์

2.4 หมายเลขไอพี (IP Address)

การสื่อสารในระบบเครือข่ายอินเตอร์เน็ตที่มีโพรโทคอลทีซีพี/ไอพี เป็นมาตรฐานเครื่องคอมพิวเตอร์ทุกเครื่องที่เชื่อมต่อกันอยู่จะต้องมีหมายเลขประจำตัวเอาไว้อ้างอิงให้คอมพิวเตอร์อื่น ๆ ได้ทราบเหมือนกับคนทุกคนต้องมีชื่อให้คนอื่นเรียก หมายเลขอ้างอิงดังกล่าวเราเรียกว่า ไอพีแอดเดรส (IP Address) หรือหมายเลขไอพี ซึ่งถูกจัดเป็นตัวเลขชุดหนึ่งขนาด 32 บิต ใน 1 ชุดนี้จะมีตัวเลขถูกแบ่งออกเป็น 4 ส่วน ส่วนละ 8 บิตเท่า ๆ กัน ลักษณะการเขียนจะแปลงให้เป็นเลขฐานสิบก่อนเพื่อความง่ายโดยคั่นแต่ละส่วนด้วยจุด ดังนั้นในตัวเลขแต่ละส่วนนี้จึงมีค่าได้ตั้งแต่ 0 จนถึง 2^8-1 หรือ 255 เท่านั้นตัวอย่างหมายเลขเช่น 192.10.1.101 เป็นต้น

หมายเลขไอพีชุดนี้จะเป็นสิ่งที่สำคัญคล้ายเบอร์โทรศัพท์ ที่เราใช้อยู่โดยจะต้องกำหนดให้ไม่ซ้ำกัน ซึ่ง สามารถกำหนดเป็นตัวเลขได้ทั้งสิ้นกว่า 4 พันล้านเลขหมายไอพี แต่การกำหนดให้คอมพิวเตอร์มีเลขหมายไอพีแอดเดรส นี้ไม่ได้เริ่มต้นจากหมายเลข 1 และนับขึ้นไปเรื่อย ๆ หากแต่จะมีการจัดแบ่งออกเป็น 2 ส่วน คือส่วนแรกเป็นหมายเลขของเครือข่าย (Network Number) ส่วนที่สองเรียกว่า หมายเลขของคอมพิวเตอร์ที่อยู่ในเครือข่ายนั้น (Host Number) เพราะในเครือข่ายใด ๆ อาจจะมีเครื่องคอมพิวเตอร์เชื่อมต่อได้อยู่มากมาย ในเครือข่ายที่อยู่คนละระบบอาจมีหมายเลขโฮสซ้ำกันได้ แต่เมื่อรวมกับหมายเลขของเครือข่ายแล้วจะได้เป็น ไอพีแอดเดรสที่ไม่ซ้ำกัน

ไอพีแอดเดรสนี้มีการจัดแบ่งออกเป็นทั้งหมด 3 ระดับ (3 Class) คือ คลาสเอ (Class A) คลาสบี (Class B) และคลาสซี (Class C) ซึ่งก็แบ่งตามขนาดความใหญ่ของเครือข่ายนั่นเอง ถ้าเครือข่ายใดมีจำนวนเครื่องคอมพิวเตอร์เชื่อมต่ออยู่มาก ก็จะมีหมายเลขอยู่ในคลาสเอ ถ้ามีเครื่องต่ออยู่ลดหลั่นกันลงมาก็จะอยู่ในคลาสบีและคลาสซี ตามลำดับดังรูปที่ 2.3



รูปที่ 2.3 แสดงโครงสร้างของแอดเดรสในคลาสต่างๆ
(Dougess E. Comer, 1990)

จากรูปที่ 2.3 จะเห็นว่าหมายเลขไอพีของคลาสเอมีตัวแรกเป็น 0 และหมายเลขของเครือข่าย มีขนาด 7 บิตและมีหมายเลขของเครื่องคอมพิวเตอร์ มีขนาด 24 บิต ทำให้ในหนึ่งเครือข่ายของคลาสเอสามารถมีคอมพิวเตอร์เชื่อมต่ออยู่ในเครือข่ายได้ถึง 2^{24} หรือ 16 ล้านเครื่อง เหมาะสำหรับองค์กรขนาดใหญ่ แต่ในคลาสเอนี้จะมีหมายเลขเครือข่ายได้ 128 ตัวทั่วโลกเท่านั้น ซึ่งหมายความว่าจะมีเครือข่ายขนาดใหญ่แบบนี้ได้เพียง 128 เครือข่ายเท่านั้น สำหรับคลาสบีจะมีหมายเลขเครือข่าย 14 บิต และหมายเลขเครื่องคอมพิวเตอร์แบบ 16 บิต (ส่วนอีก 2 บิตที่เหลือบังคับว่าต้องขึ้นต้นด้วย 10_2) ดังนั้นจึงสามารถมีจำนวนเครือข่ายที่อยู่ในคลาสบีได้มากกว่าคลาสเอ คือมีถึง 2^{14} หรือประมาณกว่า 16,000 เครือข่าย และสามารถมีเครื่องคลาสซี จะมีหมายเลขเครื่องคอมพิวเตอร์แบบ 8 บิต และมีหมายเลขเครือข่ายแบบ 21 บิต ส่วนสามบิตแรก

บังคับว่าต้องเป็น 110_2 ดังนั้นในแต่ละเครือข่ายคลาสซีจะมีจำนวนเครื่องต่อเชื่อมได้ไม่เกิน 254 เครื่องในแต่ไอพีแอดเดรสในส่วนหน้า (ดูในส่วนของหมายเลขเครือข่าย) โดย

Class A จะมี เน็ตเวิร์คแอดเดรส ตั้งแต่ 0 ถึง 127

Class B จะมี เน็ตเวิร์คแอดเดรส ตั้งแต่ 128 ถึง 191 (เพราะขึ้นต้นด้วย 10_2 เท่านั้น)

Class C จะมี เน็ตเวิร์คแอดเดรส ตั้งแต่ 192 ถึง 223 (เพราะขึ้นต้นด้วย 110_2 เท่านั้น)

เช่น ถ้าเครื่องคอมพิวเตอร์ในอินเตอร์เน็ตมีหมายเลขไอพีเป็น 181.11.82.22 ตัวเลข 181.11 แสดงว่าเป็นเครือข่ายในคลาสบีซึ่งหมายเลขเครือข่ายเต็ม ๆ จะใช้ 2 ส่วนแรก คือ 181.11 และมีหมายเลขคอมพิวเตอร์คือ 82.22 หรือ ถ้ามีหมายเลขไอพีเป็นเป็น 192.131.10.101 ทำให้ทราบว่าเครื่องคอมพิวเตอร์นั้นเชื่อมต่ออยู่บนเครือข่ายคลาสซี มีหมายเลขเครือข่ายคือสามซึ่งส่วนแรกได้แก่ 192.131.10 และหมายเลขประจำเครื่องคือ 101 เป็นต้น

2.5 เร้าเตอร์ (Router)

เร้าเตอร์ เป็นอุปกรณ์ที่ทำงานอยู่ในชั้นของเน็ตเวิร์คเลเยอร์ มีหน้าที่หลักในการค้นหาเส้นทางที่เหมาะสมเพื่อใช้ในการส่งแพ็กเก็ต โดยเร้าเตอร์จะทำการส่งแพ็กเก็ตจากเน็ตเวิร์คหนึ่งไปยังอีกเน็ตเวิร์คหนึ่ง นอกจากนี้เร้าเตอร์ยังทำหน้าที่สำคัญในการกำหนดระบบรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ตในรูปของแพ็กเก็ตฟิวเตอร์ โดยมีการทำงานในลักษณะของแอคเซสคอนโทรลลิซส์

2.6 ระบบไฟร์วอลล์ (Firewall System)

ระบบไฟร์วอลล์ (Firewall System) หมายถึง ระบบหรืออุปกรณ์ที่มีผลบังคับใช้ให้เป็นไปตามแบบแผนปฏิบัติในการป้องกัน โดยจะเป็นตัวเชื่อมระหว่างเน็ตเวิร์คที่ใช้ภายในองค์กรและอินเตอร์เน็ต สำหรับหน้าที่ของระบบไฟร์วอลล์จะเป็นตัวกำหนดระดับการเข้าถึงระบบของผู้ใช้ว่าจะให้มีการเข้าถึงการใช้งานจากผู้ใช้ภายนอกที่ได้รับสิทธิในการเข้าถึงระบบได้หรือไม่ ถ้าได้จะได้ใช้งานในระดับใด

2.7 พีไอเอ็กซ์ไฟร์วอลล์ (PIX Firewall)

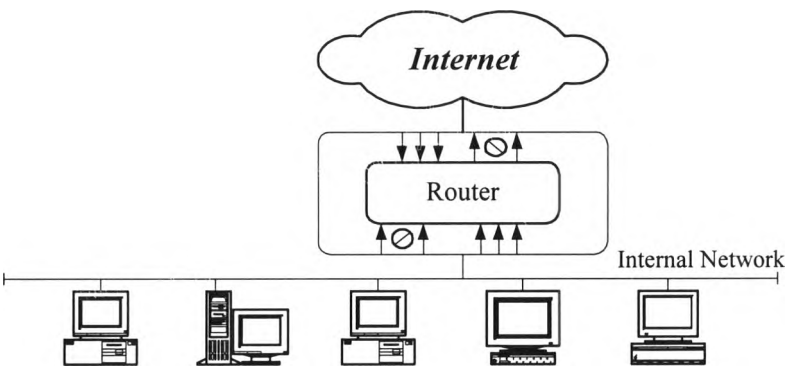
พีไอเอ็กซ์ไฟร์วอลล์ (PIX Firewall) เป็นอุปกรณ์ไฟร์วอลล์ที่ทำหน้าที่รักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ต โดยจะทำการป้องกันการรุกรานจากผู้ที่ไม่ได้รับการอนุญาตจากภายนอกไม่ให้เข้าสู่ระบบ โดยปกติแล้วพีไอเอ็กซ์ไฟร์วอลล์จะถูกออกแบบให้ใช้งานควบคู่ไปกับเร้าเตอร์ เพื่อเพิ่มความสามารถให้ระบบเครือข่ายอินเตอร์เน็ตให้มีความปลอดภัยมากยิ่งขึ้น ทั้งนี้เนื่องมาจากพีไอเอ็กซ์ไฟร์วอลล์มีการทำงานโดยใช้ขั้นตอนวิธีในการเข้ารหัสของข้อมูลที่เรียกว่า "เอเอสเอ" ซึ่งมีลักษณะเด่นคือมีการทำงานเป็นแบบ สเตทฟูล โดยลักษณะในการทำงานของเอเอสเอจะทำการเก็บแอดเดรสต้นทาง แอดเดรสปลายทาง ทีซีพีซีเควนซ์นัมเบอร์ พอร์ตนัมเบอร์ และทีซีพีแฟลก ของ แพ็กเก็ต ซึ่งรายละเอียดและส่วนต่าง ๆ ของแพ็กเก็ตนี้จะถูกเก็บ

ไว้เป็นตารางเพื่อใช้เป็นตัวเปรียบเทียบความถูกต้องกับแพ็กเก็ตต่อไป เมื่อมีแพ็กเก็ตเข้ามาจากภายนอก แพ็กเก็ตทั้งหมดก็จะถูกตรวจสอบกับตาราง ที่ได้ทำการเก็บรายละเอียดของแต่ละแพ็กเก็ตไว้แล้ว ถ้าเป็นแพ็กเก็ตที่ถูกต้องกับมาตรการรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ต ที่ได้มีการกำหนดไว้พีไอเอ็กซ์ ไฟร์วอลล์ ก็จะยอมให้แพ็กเก็ตนั้นผ่านไปได้

2.8 การทำงานของระบบไฟร์วอลล์ (Firewall System)

การทำงานของระบบไฟร์วอลล์ แบ่งได้เป็น 2 ประเภท

2.8.1 แพ็กเก็ตฟิวเตอร์ (Packet Filtering)

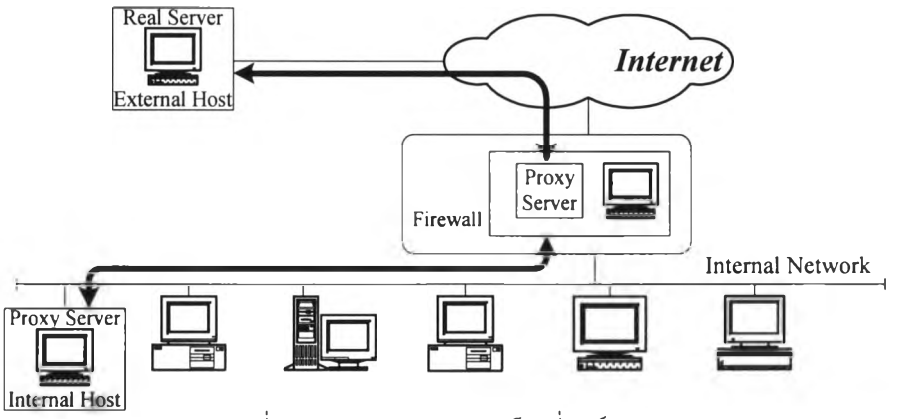


รูปที่ 2.4 แสดงการทำงานของแพ็กเก็ตฟิวเตอร์
(D.Brent Chapman , 1995)

รูปที่ 2.4 แพ็กเก็ตฟิวเตอร์จะมีหน้าที่ในการกลั่นกรองแพ็กเก็ตจากระบบอินเตอร์เน็ตภายนอก นอกจากนี้ยังมีหน้าที่ในการจัดเส้นทางเดินของแพ็กเก็ต ระหว่างโฮสภายในและโฮสภายนอกและขบวนการกลั่นกรองแพ็กเก็ตนี้เองก็จะมีการบันทึกรายชื่อผู้มีสิทธิ์ในการผ่านเข้า-ออก แล้วจะทำการตรวจสอบแพ็กเก็ตที่ได้มีการบันทึกรายชื่อที่มีการผ่านเข้า-ออกนั้นว่าตรงกับเกณฑ์ของแพ็กเก็ตฟิวเตอร์ หรือไม่ถ้าตรงกันก็สามารถผ่านได้ โดยที่เกณฑ์ของแพ็กเก็ตฟิวเตอร์ จะขึ้นอยู่กับรายละเอียดของแพ็กเก็ตเฮดเดอร์ ซึ่งปกติแพ็กเก็ตฟิวเตอร์จะอยู่บนเร้าเตอร์ บริดจ์ หรือโฮส ต่าง ๆ

แพ็กเก็ตเฮดเดอร์ จะประกอบไปด้วยหมายเลขไอพีของผู้ส่ง หมายเลขไอพีของผู้รับ โพรโทคอลต่าง ๆ ทีซีพี/ยูดีพีของผู้ส่ง ทีซีพี/ยูดีพีของผู้รับ ซึ่งรายละเอียดเหล่านี้จะนำไปตรวจสอบกับที่เกณฑ์ของแพ็กเก็ตฟิวเตอร์ เพื่อใช้ในการตัดสินว่าแพ็กเก็ตนั้นสามารถที่จะผ่านไปได้หรือไม่ ดังการทำงานของแพ็กเก็ตฟิวเตอร์

2.8.2 พร็อกซี่เซอร์วิส (Proxy Services)



รูปที่ 2.5 แสดงการทำงานของพร็อกซี่เซอร์วิส

(D.Brent Chapman, 1995)

พร็อกซี่จะทำงานในลักษณะของโปรแกรมประยุกต์ โดยจะทำงานอยู่บนไฟร์วอลล์โฮส จากรูปที่ 2.5 การทำงานของพร็อกซี่เซิฟเวอร์ จะประกอบไปด้วยองค์ประกอบ 2 ส่วนคือ พร็อกซี่เซิฟเวอร์และพร็อกซี่ไคลแอน ของ พร็อกซี่ไคลแอนจะเป็นส่วนของโปรแกรมประยุกต์ต่าง ๆ เช่น โปรแกรมประยุกต์เทลเน็ต โปรแกรมประยุกต์เอฟทีพี โปรแกรมประยุกต์เอชทีทีพี ฯลฯ เมื่อพร็อกซี่ไคลแอนต้องการติดต่อกับโฮส ที่อยู่ภายนอกจะต้องผ่าน พร็อกซี่เซิฟเวอร์ ถ้าพร็อกซี่เซิฟเวอร์ มีโปรแกรมประยุกต์ที่ พร็อกซี่ไคลแอนต้องการก็สามารถที่จะใช้ โปรแกรมประยุกต์นั้นได้เลย แต่ถ้าไม่มีก็จะขึ้นอยู่กับว่า พร็อกซี่เซิฟเวอร์นั้นได้ถูกกำหนดโครงแบบ ให้สามารถที่จะติดต่อกับโฮสที่อยู่ภายนอกเพื่อที่จะไปนำโปรแกรมประยุกต์ มาให้กับพร็อกซี่ไคลแอนได้หรือไม่ ซึ่งก็ขึ้นอยู่กับ แบบแผนปฏิบัติในการป้องกันขององค์กรที่ได้มีการกำหนดไว้