บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ตมีการขยายตัวและเติบโตเป็นอย่างมากอันเป็นผลมาจากพัฒนาการด้านความเร็วของคอมพิวเตอร์ส่วนบุคคล ความเร็วของหน่วยประมวลผลกลาง ขนาดของหน่วยความจำและความเร็วของสัญญาณอินเทอร์เน็ตที่ได้รับจากผู้ให้บริการซึ่งมีระดับความเร็วที่เพิ่มขึ้นอย่างต่อเนื่องทำให้จำนวนผู้ใช้มีมากขึ้นตามไปด้วย โดยอินเทอร์เน็ต [1] จัดเป็นเครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เชื่อมโยงเครือข่ายคอมพิวเตอร์ทั่วโลกเข้าด้วยกัน เรียกอีกอย่างหนึ่งว่า ไซเบอร์สเปซ (Cyberspace) อินเทอร์เน็ต [2] มีบริการหลากหลายชนิด เช่น ไปรษณีย์อิเล็กทรอนิกส์ (e-mail) , Gopher, Internet Relay Chat: IRC เป็นต้น แต่บริการที่ได้รับความนิยมและเป็นที่ยอมรับกันอย่างกว้างขวางก็คือ เวิลด์ไวด์เว็บ (World Wide Web: WWW) ซึ่งได้รับการพัฒนาจากนักวิจัยของห้องทดลองฟิสิกส์ในประเทศสวิตเซอร์แลนด์ที่มีชื่อว่า CERN โดยบริการ WWW นี้ ได้รวมความสามารถในการแลกเปลี่ยนข้อมูลข่าวสารบนอินเทอร์เน็ต โดยการใช้ Hypertext ซึ่งช่วยให้ง่ายต่อการใช้งาน สามารถใช้เพียงการคลิ๊กเมาส์ ที่จุดที่กำหนดในเอกสาร ก็สามารถจะเชื่อมโยงนำไปยังอีกเอกสารหนึ่งที่เกี่ยวข้องได้ในเวลาอันรวดเร็ว นอกจากนี้เหตุผลอีกประการหนึ่งที่ WWW ได้รับความนิยมมากก็คือ ความสามารถในการนำเสนอรูปภาพ เสียง วีดีโอ และภาพเคลื่อนไหว ควบคู่กับตัวอักษรในเอกสารเว็บได้ ซึ่งถูกเรียกว่าเอกสาร HTML (Hypertext markup language) หรือ Web Pages โดยการเรียกดูเอกสารเหล่านี้ จะกระทำผ่านโปรแกรมที่เรียกว่าบราวเซอร์ (web browser) ความสวยงามและความง่ายในการใช้งานนี้ ทำให้อินเทอร์เน็ต [3] เป็นช่องทางที่ถูกใช้ประโยชน์ทางธุรกิจ ทางการศึกษา การแสดงความคิดเห็น การรายงานเหตุการณ์ตลอดจนเป็นช่องทางการสื่อสารระหว่างกันของบุคคลต่างๆทั่วโลก อินเทอร์เน็ตทำให้การเคลื่อนย้ายและส่งผ่านข่าวสารข้อมูลจากที่หนึ่งไปอีกที่หนึ่งกระทำได้โดยง่าย โดยไม่จำกัดเรื่องระยะทางและเวลา สามารถส่งข้อมูลได้หลากหลายรูปแบบ เช่น ส่งเป็นแบบข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เสียง โดยอาศัยเครือข่ายโทรคมนาคมเป็นตัวเชื่อมต่อเครือข่าย การเชื่อมโยงเครือข่ายจะใช้เครือข่ายสื่อสารโทรคมนาคม เช่น สายสัญญาณโทรศัพท์ สายใยแก้วนำแสง (Fiber Optic) สัญญาณไมโครเวฟ สัญญาณจากดาวเทียม เป็นต้น ทำให้การส่งผ่านข้อมูลจากที่หนึ่งไปยังอีกที่หนึ่งสามารถกระทำให้เป็นไปด้วยความรวดเร็ว อินเทอร์เน็ตเป็นแหล่งรวบรวมข้อมูลแหล่งใหญ่ที่สุดของโลก และเป็นที่รวมทั้งบริการและเครื่องมือสืบค้นข้อมูลหลายประเภท จนกระทั่งกล่าวได้ว่าอินเทอร์เน็ตเป็นเครื่องมือสำคัญอย่างหนึ่งในการประยุกต์ใช้เทคโนโลยีสารสนเทศทั้งในระดับบุคคลและองค์กร

การเติบโตดังกล่าวทั้งเรื่องจำนวนเครื่องคอมพิวเตอร์ที่มากขึ้นนั้น ขนาดของข้อมูลที่ส่งผ่านเข้าออกในระบบอินเทอร์เน็ตจากที่หนึ่งไปสู่อีกที่หนึ่งก็มีขนาดใหญ่มากขึ้นด้วย [4] โดยข้อมูลที่ผู้ใช้เข้าถึงในแต่ละวันแต่ละช่วงเวลามักเป็นข้อมูลเดิมจากเว็บไซต์ที่เดียวกัน ทำให้เกิดการกระทำกับข้อมูลเดิมที่มีการเรียกใช้ซ้ำๆ ดังนั้นในทางการบริหารเครือข่ายเมื่อรับรู้ถึงลักษณะการใช้งานของผู้ใช้ในลักษณะนี้ และเพื่อใช้ประโยชน์จากการกระทำนี้ จึงพบว่ามีการนำเอาระบบพรอกซี่หรือระบบแคชซึ่งเข้ามาใช้เพื่อช่วยลดปริมาณของข้อมูลที่วิ่งผ่านเข้าออกระหว่างเครือข่ายภายในองค์กรกับ

อินเทอร์เน็ตภายนอก เพื่อช่วยลดระยะเวลาในการดึงข้อมูลจากภายนอกด้วยการดึงข้อมูลบางอย่างจากจากเครื่องแม่ข่ายพรอกซี่เซิร์ฟเวอร์ภายในเพื่อให้ใช้งานได้ทันทีโดยไม่ต้องร้องขอข้อมูลจากภายนอกทุกครั้ง ซึ่งเป็นต้นเหตุของการเกิดความหนาแน่นของข้อมูลในระบบอินเทอร์เน็ต และส่งผลให้ประสิทธิภาพการใช้งานอินเทอร์เน็ตตกลงในที่สุดเนื่องจากช่องสัญญาณหรือที่เรียกว่าแบนด์วิดท์มีน้อย

สำหรับความหมายของคำว่าแบนด์วิดท์ (Bandwidth) เป็นคำที่ใช้วัดความเร็วในการส่งข้อมูลของอินเทอร์เน็ต หรือจะเรียกอีกอย่างว่าเป็นความกว้างของช่องสัญญาณที่ใช้ในการสื่อสารผ่านตัวกลางซึ่งก็คือระยะห่างระหว่างคลื่นสัญญาณความถี่สูงสุดและความถี่ต่ำสุดที่ใช้เป็นช่องทางของการสื่อสารโดยแบนด์วิดท์ของระบบการสื่อสารบนเครือข่ายนั้นมี 2 รูปแบบ คือ แบบ Bandwidth in Hertz และแบบ Bandwidth in Bits per seconds สำหรับความสัมพันธ์ระหว่างแบนด์วิดท์ในเฮิร์ทและในบิตต่อวินาทีนั้น โดยพื้นฐานก็คือเมื่อมีการเพิ่มประสิทธิภาพของเครือข่ายโดยการเพิ่มแบนด์วิดท์ในเฮิร์ท ก็จะหมายถึงการเพิ่มประสิทธิภาพของแบนด์วิดท์ในบิตต่อวินาทีด้วย ในความหมายทั่วไปแบนด์วิดท์เป็นสัดส่วนโดยตรงของจำนวนข้อมูลทั้งหมดที่ส่งผ่านหรือรับต่อหน่วยเวลา ในความหมายเชิงคุณภาพ แบนด์วิดท์เป็นสัดส่วนของความซับซ้อนของข้อมูลสำหรับการทำงานของระบบที่รองรับได้เช่น การดาวน์โหลดไฟล์ทุกประเภทรูปภาพในหนึ่งวินาทีใช้แบนด์วิดท์มากกว่าการดาวน์โหลดข้อความในเวลาหนึ่งวินาที ส่วนไฟล์ประเภทเสียงขนาดใหญ่ในโปรแกรมคอมพิวเตอร์และภาพเคลื่อนไหวต้องใช้แบนด์วิดท์มาก การนำเสนอแบบ Virtual reality (VR) และ ภาพแบบ 3 มิติชนิด Full-length ใช้ แบนด์วิดท์มากที่สุด

กระบวนการนำเอาระบบพรอกซี่หรือระบบแคชชิ่งเซิร์ฟเวอร์มาใช้ในอดีตที่ผ่านมาเน้นในเรื่องของการลดเวลาการเข้าถึงข้อมูลหรือเหมือนว่าทำให้ผู้ใช้เข้าถึงข้อมูลได้เร็วซึ่งมีประโยชน์มากกับเครือข่ายที่มีความเร็วสัญญาณอินเทอร์เน็ตแบบจำกัด โดยระบบของพรอกซี่จะทำงานเหมือนเป็นตัวกั้นกลางระหว่างผู้ใช้งานภายในองค์กรกับเครือข่ายอินเทอร์เน็ตภายนอกผ่านพอร์ต 80 หรือ 8080 เมื่อผู้ใช้เปิดโปรแกรมเว็บเบราว์เซอร์เพื่อใช้งานอินเทอร์เน็ตสัญญาณจะถูกบังคับให้วิ่งผ่านพอร์ตนี้เสมอ แต่ในความเป็นจริงสำหรับการใช้งานของผู้ใช้ยังมีลักษณะงานอีกประเภทหนึ่งที่สร้างปัญหาทำให้ความเร็วของอินเทอร์เน็ตตกลงก็คือบริการที่เรียกว่าการดาวน์โหลดซึ่งทำงานอยู่บนพอร์ต 21 การดาวน์โหลดเป็นรูปแบบการรับส่งไฟล์ระหว่างเครื่องคอมพิวเตอร์ลูกข่ายกับเครื่องคอมพิวเตอร์แม่ข่ายโดยทำการติดต่อกันทางโปรโตคอล FTP (File Transfer Protocol) การกระทำในลักษณะนี้จะใช้เวลาในการครองครองช่องสัญญาณเป็นเวลานานเนื่องมาจากขนาดของไฟล์ข้อมูลที่ทำการดาวน์โหลดมีขนาดใหญ่และเล็กไม่เท่ากันซึ่งรวมแล้วมักมีขนาดใหญ่ เมื่อมีผู้ใช้ทำการดาวน์โหลดข้อมูลพร้อมๆกันยิ่งจะทำให้ช่องสัญญาณเกิดความหนาแน่นทำให้ความเร็วของการใช้งานอินเทอร์เน็ตโดยรวมตกลงไปจนเป็นอุปสรรคให้กับผู้ใช้อินเทอร์เน็ตรายอื่นที่มีความต้องการในเรื่องอื่นๆ เช่นการสืบค้นข้อมูล การส่งไฟล์งานให้กันและกัน ซึ่งปัญหาจากการดาวน์โหลดข้อมูลนั้นระบบพรอกซี่ที่มีอยู่ไม่สามารถจัดการกับเรื่องนี้ได้ ดังนั้นการพัฒนาระบบเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยระบบปฏิบัติการลินุกซ์จึงเป็นเรื่องที่จัดทำขึ้นเพื่อทำให้ปัญหาดังกล่าวมีทางออกและทำให้เกิดประโยชน์ต่อการใช้งานระบบอินเทอร์เน็ต ต่อไป

1.2 วัตถุประสงค์ของการวิจัย

เพื่อศึกษาระบบการทำงานพื้นฐานของอินเทอร์เน็ต โครงสร้างสถาปัตยกรรมและองค์ประกอบ บริการที่มีในระบบอินเทอร์เน็ต ความเกี่ยวข้องของระบบปฏิบัติการ ปัญหาการเข้าถึงข้อมูลอินเทอร์เน็ต ข้อมูลอันก่อให้เกิดปัญหาที่นำมาซึ่งประสิทธิภาพที่ลดลงของการใช้งานอินเทอร์เน็ต แลเพื่อพัฒนาระบบที่สามารถเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยระบบปฏิบัติการลินุกซ์

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1.3.1 ทราบปัญหาที่ทำให้เกิดความล่าช้าในการเข้าถึงข้อมูลในระบบเครือข่ายอินเทอร์เน็ตของหน่วยงาน

1.3.2 มีระบบที่สามารถเพิ่มประสิทธิภาพการทำงานของระบบอินเทอร์เน็ตเดิมให้ดีขึ้นโดยใช้ซอฟท์แวร์ที่มีต้นทุนต่ำ

1.3.3 สามารถนำระบบที่จัดทำขึ้นโดยใช้ซอฟต์แวร์โอเพ่นซอร์สที่มีราคาการลงทุนต่ำมาประยุกต์ใช้ในหน่วยงานที่ต้องการได้

1.3.4 สามารถนำระบบที่จัดทำขึ้นไปประยุกต์ใช้ในหน่วยงานอื่นๆได้

1.4 ขอบเขตของการวิจัย

ระบบเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยระบบปฏิบัติการลินุกซ์มีขั้นตอนการพัฒนาโดยแบ่งขั้นตอน ดังนี้

1.4.1 ส่วนบริหารจัดการข้อมูลที่เกิดจากการใช้งานของผู้ใช้ในรูปแบบของการดาวน์โหลด

1.4.2 ส่วนรายงานข้อมูลที่เกิดจากการใช้งานของผู้ใช้

1.4.3 ส่วนตรวจสอบและแสดงผลที่สามารถรายงานความเร็วที่ได้จากการเปิดให้บริการของระบบที่พัฒนาขึ้น

1.5 ข้อตกลงเบื้องต้น

ระบบเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยระบบปฏิบัติการลินุกซ์ เป็นระบบที่พัฒนาขึ้นโดยมีพื้นฐานการทำงานทั้งหมดบนระบบปฏิบัติการ (Operating System) ลินุกซ์ (Linux) เวอร์ชั่น CentOs เป็นหลักโดยปรับแต่งไฟล์ที่มีอยู่แล้วในระบบซึ่งประกอบไปด้วยการปรับแต่งระบบพรอกซี่ ระบบไฟร์วอลล์ (Firewall) การปรับแต่งไฟล์สำหรับระบบ FTP ซึ่งทั้งหมดไม่ได้ทำการทดสอบบนระบบปฏิบัติการวินโดวส์

ในการทำงานของระบบจะใช้ระบบพรอกซี่ที่ได้รับความนิยมกันอย่างกว้างขวางอยู่แล้วคือโปรแกรมสควิด (Squid) โปรแกรมนี้มีอยู่แล้วในระบบปฏิบัติการลินุกซ์ทุกเวอร์ชั่น ทำหน้าที่ในการให้บริการเข้าถึงเว็บไซต์ผ่านโปรโตคอล HTTP บนพอร์ต 80 เช่นเดิมและเพิ่มเติมส่วนบริหารจัดการการใช้งานประเภทดาวน์โหลดที่ผ่านโปรโตคอล FTP บนพอร์ต 21 โดยปรับแต่งให้ทั้งสองส่วนทำงานร่วมกันและแยกหน้าที่การทำงานตามวัตถุประสงค์ที่ตั้งไว้

1.6 ข้อจำกัดการวิจัย

ระบบเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยระบบปฏิบัติการลินุกซ์ ติดตั้งและทดสอบการทำงานบนเครื่องแม่ข่ายที่ติดตั้งระบบปฏิบัติการลินุกซ์เท่านั้น และใช้การทดสอบผลการทดลองด้วยการเก็บผลจากการทดสอบทั้งในส่วนของระบบเดิมแบบที่มีพรอกซี่เพียงอย่างเดียว และทดสอบระบบในสภาวะที่มีการเพิ่มระบบใหม่ โดยวัดผลจากความเร็วที่ทำได้ทั้งสองรูปแบบ พร้อมนำมาเปรียบเทียบ วิเคราะห์ผลทดสอบ และใช้โปรแกรมวัดความเร็วในการเข้าถึงข้อมูลอินเทอร์เน็ตพร้อมแสดงผลด้วยกราฟเส้น

1.7 กรอบแนวคิดในการวิจัย

จากข้อมูลความต้องการและขอบเขตการทำงานข้างตน ทำให้กรอบแนวคิดในการวิจัยที่จะสร้างระบบ มีดังต่อไปนี้

1.7.1 ศึกษารวบรวมข้อมูล

1.7.1.1 ศึกษากระบวนการส่งผ่านและเข้าถึงข้อมูลของระบบอินเทอร์เน็ต

1.7.1.2 ศึกษาการทำงานของโปรโตคอล TCP/IP

1.7.1.3 ศึกษาการทำงานของโปรโตคอล HTTP

1.7.1.4 ศึกษาการทำงานของโปรโตคอล FTP

1.7.1.5 ศึกษาการทำงานของไอพีเทเบิ้ล

1.7.1.6 ศึกษาการทำงานของความสัมพันธ์ของเครือข่ายกับระบบพรอกซี่

1.7.2 พัฒนาระบบ

1.7.2.1 ติดตั้งและปรับแต่งเครื่องแม่ข่ายลินุกซ์

1.7.2.2 ติดตั้งและปรับแต่งส่วนการทำงานของสควิดพรอกซี่

1.7.2.3 ติดตั้งและปรับแต่งส่วนการทำงานของเอฟทีพีพรอกซี่

1.7.2.4 ติดตั้งและปรับแต่งส่วนการทำงานของไอพีเทเบิ้ล

1.7.3 ทดสอบการทำงานของระบบ

1.7.3.1 ทดสอบการทำงานระบบในรูปแบบการเปิดเว็บไซต์ทั่วไป

1.7.3.2 ทดสอบการทำงานระบบในรูปแบบการดาวน์โหลดข้อมูล

1.7.3.3 วัดประสิทธิภาพการใช้งานอินเทอร์เน็ตโดยรวมด้วยการวัดความเร็วก่อนเปิดระบบที่พัฒนาขึ้น

1.7.3.4 ทดลองเปิดระบบที่พัฒนาขึ้นและทำการตรวจวัดประสิทธิภาพการใช้งานอินเทอร์เน็ตโดยรวมด้วยการวัดความเร็วอีกครั้ง

1.7.3.5 ตรวจสอบความถูกต้องจากร่องรอยระบบ

1.7.3.6 ทดสอบความเที่ยงตรงของระบบ

1.7.3.7 แก้ไขและปรับปรุงระบบ

1.8 นิยามศัพท์เฉพาะ

ระบบปฏิบัติการ, ลินุกซ์, สควิดพรอกซี่, พรอกซี่เซิร์ฟเวอร์, แคชชิ่ง, อินเทอร์เน็ต, ไอพี, โปรโตคอล, ดาวน์โหลด, เน็ตเวิร์ค, HTTP, FTP

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

การดำเนินงานวิจัยเรื่อง เพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยระบบปฏิบัติการลินุกซ์ ผู้จัดทำได้ดำเนินการศึกษาค้นคว้าข้อมูลเพื่อให้ได้ขั้นตอน วิธีการ ในการจัดทำระบบตามที่ออกแบบไว้ โดยแบ่งขั้นตอนรายละเอียดการศึกษา ดังนี้

2.1 พื้นฐานอินเทอร์เน็ต และสถาปัตยกรรมโปรโตคอลทีซีพีไอพี (TCP/IP)

2.2 ระบบปฏิบัติการลินุกซ์ (Linux Operating System)

2.3 โปรโตคอล HTTP (Hypertext Transfer Protocol)

2.4 โปรโตคอล FTP (File Transfer Protocol)

2.5 พรอกซี่เซิร์ฟเวอร์ (Proxy Server)

2.6 ไฟร์วอลล์ (Firewall)

2.1 พื้นฐานอินเทอร์เน็ต และสถาปัตยกรรมโปรโตคอลทีซีพีไอพี (TCP/IP)

อินเทอร์เน็ต คือ ระบบเครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่มีเครื่องคอมพิวเตอร์เชื่อมต่อกันทั่วโลกโดยใช้มาตรฐานเดียวกันในการรับส่งข้อมูล เรียกว่าโปรโตคอล (Protocol) [5] ซึ่งโปรโตคอลที่ใช้บนระบบเครือข่ายอินเทอร์เน็ตมีชื่อว่าทีซีพีไอพี (TCP/IP: Transmission Control Protocol/Internet Protocol) [6] อินเทอร์เน็ตเปรียบเสมือนห้องสมุดสาธารณะขนาดใหญ่ที่มีข้อมูลต่างๆมากมายให้เราสามารถค้นหา [7] เพื่อนำไปใช้ประโยชน์ในด้านต่างๆ อาทิเช่น การศึกษาการวิจัย การโฆษณาขายสินค้า หรือความบันเทิงก็สามารถหาได้จากอินเทอร์เน็ต [8]

ระบบอินเทอร์เน็ตนั้น มีหลักการทำงานโดยอาศัยโปรโตคอลที่ชื่อว่าทีซีพีไอพีเป็นหลัก สิ่งสำคัญที่ควรทราบเกี่ยวกับโปรโตคอลทีซีพีไอพี [9] คือ การเชื่อมต่อของเครื่องคอมพิวเตอร์หรืออุปกรณ์ใดๆเข้าสู่ระบบเครือข่ายที่อาศัยการทำงานบนโปรโตคอลทีซีพีไอพีนั้น ทุกเครื่องทุกอุปกรณ์จะต้องมีหมายเลขอ้างอิงกำกับไว้ด้วยเสมอ เพื่อระบุตัวตนและข้อมูลแหล่งที่ โดยหมายเลขที่ใช้กำกับอุปกรณ์คอมพิวเตอร์นี้มีชื่อเรียกว่า ไอพี (IP) หมายเลขไอพีเหล่านี้จะมีลักษณะหรือรูปแบบเป็นชุดของตัวเลขฐานสอง ขนาด 32 บิต แบ่งออกเป็น 4 ชุด แต่ละชุดมีค่าตั้งแต่ 0-255 หากพิจารณาแบบง่ายๆอินเทอร์เน็ตก็มีความคล้ายคลึงกับเครือข่ายหนึ่งที่มีการเชื่อมต่อกับคอมพิวเตอร์ชนิดต่างๆ กันเข้าหากัน แต่แท้จริงแล้วอินเทอร์เน็ตเป็นเครือข่ายขนาดมหึมาที่มีจำนวนมาก มากกว่าสิบล้านโฮสต์และมีมากกว่าพันเครือข่ายที่เชื่อมต่อเข้าด้วยกัน และด้วยเครือข่ายที่มีขนาดใหญ่มหึมาขนาดนี้จึงทำให้คอมพิวเตอร์ที่เชื่อมต่อเข้ากับเครือข่ายอินเทอร์เน็ตนั้นมีหลายระดับ หลายประเภทด้วยกัน ไม่ว่าจะเป็นคอมพิวเตอร์ในระดับพีซี คอมพิวเตอร์พกพา เมนเฟรมคอมพิวเตอร์ รวมไปถึงโทโปโลยีหรือรูปแบบการเชื่อมต่อเครือข่ายที่มีความซับซ้อนตามไปด้วยตามความเหมาะสม ซึ่งรูปแบบที่รู้จักกันและนิยมกันทั่วไปอาจเป็นแบบที่เรียกว่า อีเทอร์เน็ต (Ethernet) โทเค็นริง (Token ring) หรือ FDDI (Fiber Distributed Data Interface) เป็นต้น สำหรับมุมมองของทีซีพีไอพีนั้น จะมองเครือข่ายที่ประกอบไปด้วยฟิสิคัลเน็ตเวิร์กเหล่านั้นเป็นเสมือนหนึ่งเครือข่ายขนาดใหญ่ กล่าวคือแต่ละโฮสต์ที่

เชื่อมต่อเข้ากับเครือข่าย ทีซีพีไอพีจะถูกมองในรูปแบบลอจิคัลเน็ตเวิร์ก (Logical Network) ที่เสมือนเป็นหนึ่งเครือข่ายมากกว่าจะมองเครือข่ายเหล่านั้นเป็นฟิสิคัลเน็ตเวิร์ก (Physical Network) ที่ประกอบไปด้วยกลุ่มเครือข่ายเฉพาะต่างๆ

2.1.1 สถาปัตยกรรมชุดโปรโตคอล TCP/IP

จากรายละเอียดข้างต้นจะเห็นได้ว่าอินเทอร์เน็ตทำงานโดยอาศัยการส่งผ่านข้อมูลในรูปแบบที่เรียกว่าโปรโตคอล แท้ที่จริงโปรโตคอลก็คือ ข้อกำหนดหรือข้อตกลงที่ใช้ควบคุมการสื่อสารข้อมูลในเครือข่าย ไม่ว่าจะเป็นการสื่อสารข้อมูลระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์อื่นๆ เครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายที่ใช้โปรโตคอลชนิดเดียวกันเท่านั้น จึงจะสามารถติดต่อและส่งข้อมูลระหว่างกันได้ โปรโตคอลจึงมีลักษณะเช่นเดียวกับภาษาภาษาที่ใช้ในการสื่อสารของมนุษย์ที่ต้องใช้ภาษาเดียวกันจึงจะสามารถสื่อสารกันได้เข้าใจ สำหรับในเครือข่าย โปรโตคอลจะเป็นตัวกำหนดลักษณะหรือองค์ประกอบต่างๆที่ใช้ในการสื่อสารไม่ว่าจะเป็นรูปแบบการแทนข้อมูล วิธีการในการรับ-ส่งข้อมูล รูปแบบสัญญาณรับ-ส่ง อุปกรณ์หรือสื่อกลางในการส่งข้อมูล การกำหนดหรือการอ้างอิงตำแหน่ง การตรวจสอบความผิดพลาดของข้อมูล รวมถึงความเร็วในการรับ-ส่งข้อมูล โดยมาตรฐานกลางที่ใช้ในการส่งข้อมูลระหว่างคอมพิวเตอร์ในระบบเครือข่าย คือ มาตรฐาน OSI (Open Systems Interconnection Model) โดยในปี ค.ศ.1977 องค์กร ISO (International Organization for Standard) ได้จัดตั้งคณะกรรมการขึ้นกลุ่มหนึ่งเพื่อทำการศึกษา จัดรูปแบบมาตรฐาน และพัฒนาสถาปัตยกรรมเครือข่าย และในปี ค.ศ.1983 องค์กร ISO ก็ได้ออกประกาศรูปแบบของสถาปัตยกรรมเครือข่ายมาตรฐานในชื่อของ "รูปแบบ OSI" เพื่อใช้เป็นรูปแบบมาตรฐานในการเชื่อมต่อระบบคอมพิวเตอร์ จุดมุ่งหมายของการกำหนดมาตรฐาน OSI นี้ขึ้นมาก็เพื่อจัดแบ่งการดำเนินงานพื้นฐานของเครือข่ายและกำหนดหน้าที่การทำงานในแต่ละชั้น ซึ่งแบ่งออกได้เป็น 7 ชั้น ประกอบไปด้วยชั้นต่างๆดังต่อไปนี้

1) ชั้นฟิสิคัล (Physical Layer)
2) ชั้นดาต้าลิงค์ (Data Link Layer)
3) ชั้นเน็ตเวิร์ค (Network Layer)
4) ชั้นทรานสปอร์ต (Transport Layer)
5) ชั้นเซสชั่น (Session Layer)
6) ชั้นพรีเซนเทชัน (Presentation Layer)
7) ชั้นแอพพลิเคชั่น (Application Layer)

รายละเอียดของแต่ละชั้นมีดังต่อไปนี้

1) ชั้นฟิสิคัล (Physical Layer) เป็นชั้นล่างสุดและเป็นชั้นทางกายภาพ ในชั้นนี้จะกล่าวถึงอุปกรณ์ที่ใช้ในการเชื่อมต่อ จะมีการกำหนดคุณสมบัติทางกายภาพของฮาร์ดแวร์ที่ใช้เชื่อมต่อระหว่างคอมพิวเตอร์ทั้งสองระบบ เช่น สายเคเบิ้ลที่ใช้รับส่งข้อมูลจะเป็นแบบไหน ข้อต่อหรือปลั๊กที่ใช้ในการรับส่งข้อมูลมีมาตรฐานอย่างไร ความเร็วในการรับส่งข้อมูลเท่าใด สัญญาณที่ใช้ในการรับส่งข้อมูลมีรูปร่างอย่างไร ใช้แรงดันไฟฟ้าเท่าไหร่ เป็นต้น ซึ่งข้อมูลในชั้นฟิสิคัลนี้ จะมองเห็นเป็นการรับส่งข้อมูลทีละบิตเรียงต่อกันไป

2) ชั้นดาต้าลิงค์ (Data Link Layer) หรือเรียกชั้น สื่อกลางของการส่งข้อมูล เพราะจะต้องมีการ ระบุหมายเลข address ของอุปกรณ์ต่างๆ ที่เรียกว่า MAC Address เป็นชั้นที่ทำหน้ากำหนดรูปแบบของการส่งข้อมูลข้าม Physical Network โดยใช้ Physical Address อ้างอิงที่อยู่ต้นทางและปลายทาง ซึ่งก็คือ MAC Address นั่นเอง รวมถึงทำการตรวจสอบและจัดการกับ error ในการรับส่งข้อมูล ข้อมูลที่ถูกส่งบน Layer 2 เราจะเรียกว่า Frame ตัวอย่างของ protocol ในชั้นนี้คือ Ethernet , Token Ring , IEEE 802.3/202.2 , Frame Relay, FDDI,HDLC, ATM , MPLS เป็นต้น ซึ่งบน Layer 2 ก็จะแบ่งเป็น LAN และ WAN ปัจจุบัน บน Layer 2 LAN เรานิยมใช้เทคโนโลยีแบบ Ethernet มากที่สุด ส่วน WAN ก็จะมีหลายแบบแตกต่างกันไป เช่น Lease Line (HDLC , PPP) , MPLS , 3G และอื่นๆ สำหรับ LAN ยังมีการแบ่งย่อยออกเป็น 2 sub layers คือ

2.1) Logical Link Control (LLC) IEEE 802.2 ซึ่งจะให้บริการกับ Layer ด้านบนในการเข้าใช้สัญญาณใน การรับ-ส่งข้อมูล ตามมาตรฐาน IEEE802 แล้ว จะอนุญาตให้สถาปัตยกรรมของ LAN ที่ต่างกันสามารถทำงานร่วมกันได้ หมายความว่า Layer ด้านบนไม่จำเป็นต้องทราบว่า Physical Layer ใช้สายสัญญาณประเภทใดในการรับ-ส่งข้อมูล เพราะ LLC จะรับผิดชอบในการปรับ Frame ข้อมูลให้สามารถส่งไปได้ในสายสัญญาณประเภทนั้นได้ และไม่จำเป็นต้องสนใจว่าข้อมูลจะส่งผ่านเครือข่ายแบบไหน เช่น Ethernet , Token Ring บลาๆๆ และไม่จำเป็นต้องรู้ว่าการส่งผ่านข้อมูลใน Physical Layer จะใช้การรับส่งข้อมูล แบบใด LLC จะเป็นผู้จัดการเรื่องเหล่านี้ได้ทั้งหมด

2.2) Media Access Control (MAC) IEEE 802.3 ใช้ควบคุมการติดต่อสื่อสารกับ Layer 1 และรับผิดชอบในการรับ-ส่งข้อมูลให้สำเร็จและถูกต้อง โดยมีการระบุ MAC Address ของอุปกรณ์เครือข่าย ซึ่งใช้อ้างอิงในการส่งข้อมูลจากต้นทางไปยังปลายทาง เช่น จากต้นทางส่งมาจาก MAC Address หมายเลข AAAA:AAAA:AAAA ส่งไปหาปลายทางหมายเลข BBBB:BBBB:BBBB เมื่อปลายทางได้รับข้อมูลก็จะรู้ว่าใครส่งมา เพื่อจะได้ตอบกลับไปถูกต้องนั่นเอง และบน Ethernet (IEEE802.3) เมื่อมันมีหน้าที่ในการรับผิดชอบการรับ-ส่งข้อมูลให้สำเร็จและถูกต้อง มันจึงมีการตรวจสอบข้อผิดพลาดในการส่งข้อมูลด้วย ที่เราเรียกว่า Frame Check Sequence (FCS) และยังตรวจสอบกับ Physical ด้วยว่าช่องสัญญาณพร้อมสำหรับส่งข้อมูลไหม ถ้าว่างก็ส่งได้ ถ้าไม่ว่างก็ต้องรอ กลไลนี่เรารู้จักกันในชื่อ CSMA/CD นั่นเอง ในส่วนของ CSMA/CD มันก็คือกลไกการตรวจสอบการชนกันของข้อมูลบน Ethernet ถ้าเกิดมีการชนกันเกิดขึ้น มันก็จะส่งสัญญาณ (jam signal) ออกไปเพื่อให้ทุกคนหยุดส่งข้อมูล แล้วสุ่มรอเวลา (back off) เพื่อส่งใหม่อีกครั้ง

ในชั้น Data Link Layer นี้จะมีคำศัพท์ที่เกี่ยวข้องคือคำว่า encapsulation โดยทั่วไป encapsulation คือการรวมของสิ่งหนึ่งภายในอีกสิ่ง ดังนั้นสิ่งที่รวมไม่ปรากฏ decapsulation คือขจัดหรือทำให้สิ่งของปรากฏเหมือนก่อนการทำ encapsulation ซึ่งแปลแล้วค่อนข้างเข้าใจยาก เอาเป็นว่า encapsulation คือรูปแบบการจัดส่งข้อมูลในรูปแบบเฟรมแบบต่างๆ จะแบ่งการพิจารณาออกเป็น 2 ส่วนคือ ในส่วนของ LAN และ WAN

ในส่วนของ LAN จะเกี่ยวกับอุปกรณ์ Switch จะสนใจเกี่ยวกับ เรื่อง Mac Address Table, การทำ VLAN และมีในส่วนของค่า encapsulation เหมือนกันกับ Switch และมีการแบ่ง VLAN ด้วย Port ที่เชื่อมต่อระหว่าง Switch กับ Switch จะเรียกว่า Trunk port ต้องทำ

การคอนฟิกค่า encapsulation ให้ถูกต้องและตรงกันทั้ง 2 ฝั่ง โดยค่า encapsulation ของ Trunk port ค่ามาตรฐานจะเป็น IEEE 802.1Q ส่วน ISL จะเป็นค่า encapsulation ของทางบริษัทซิสโก้ ในส่วนของ WAN ค่า encapsulation จะขึ้นอยู่กับประเภทของมีเดียที่เช่ากับ Media Provider ต่างๆ เช่น ถ้าเราเช่ามีเดียเป็นวงจรเช่า หรือ Leased line ค่า encapsulation ที่สามารถเซตได้ที่ Router Cisco นั้นคือ encapsulation แบบ HDLC (ค่า encapsulation default ของ Router Cisco) และ encapsulation แบบ ppp (ค่า encapsulation มาตรฐานสำหรับ Router ต่างยี่ห้อกัน) กรณีเช่ามีเดียเป็น Frame-Relay ค่า encapsulation ที่สามารถเซตได้ที่ Router Cisco นั้นคือ encapsulation frame-relay (กรณีที่ router ทั้ง 2 ฝั่งเป็น cisco ทั้งคู่) และค่า encapsulation frame-relay ietf (frame-relay แบบ ietf จะเป็นค่า encapsulation มาตรฐาน สำหรับ Router ต่างยี่ห้อกัน) กรณีเช่ามีเดียเป็น xDSL ค่า encapsulation หรือ WAN Protocol ที่สามารถเซตได้ เช่น PPPoE, PPPoE, RFC 1483 Routed เป็นต้น ขึ้นอยู่กับประเภทของ xDSL ที่เช่าซื้อต้องเซตค่า encapsulation ให้ตรงกับของ xDSL Provider จะเห็นว่าค่า encapsulation นั้นมีหลายประเภท และอยู่ใน Data Link Layer ทั้งสิ้น

3) ชั้นเน็ตเวิร์ค (Network Layer) ในชั้นนี้จะกล่าวถึงโปรโตคอลต่างๆ เช่น IP, Novell's IPX , IBM's APPN, Appletalk เป็นต้น การทำงานในชั้นนี้จะเป็นการเชื่อมต่อและการเลือกเส้นทาง การนำพาข้อมูลระหว่างเครื่องสองเครื่องในเครือข่าย หน่วยของ layer นี้คือ packet ทำหน้าที่ส่งข้อมูลข้ามเครือข่าย หรือ ข้าม network โดยส่งข้อมูลผ่าน Internet Protocol (IP) โดยมีการสร้างที่อยู่ขึ้นมา (Logical Address) เพื่อใช้อ้างอิงเวลาส่งข้อมูล เราเรียกว่า IP address ข้อมูลที่ถูกส่งมาจากต้นทาง เพื่อไปยังปลายทาง ที่ไม่ได้อยู่บนเครือข่ายเดียวกัน จำเป็นจะต้องพึ่งพาอุปกรณ์ที่ทำงานบน Layer 3 นั่นก็คือ Router หรือ Switch Layer 3 โดยใช้ Routing Protocol (OSPF , EIGRP) เพื่อหาเส้นทางและส่งข้อมูลนั้น (IP) ข้ามเครือข่ายไป โดยการทำงานของ Internet Protocol (IP) เป็นการทำงานแบบ Connection-less หมายความว่า IP ไม่มีการตรวจสอบข้อมูลว่าส่งไปถึงปลายทางไหม แต่มันจะพยายามส่งข้อมูลออกไปด้วยความพยายามที่ดีที่สุด (Best-Effort) เพราะฉะนั้น ข้อมูลที่ส่งออกไปแล้วไม่ถึงปลายทาง ต้นทางก็จะไม่รู้เลย ถ้าส่งไปแล้วข้อมูลไม่ถึงปลายทาง ฝั่งต้นทางจะต้องทำการส่งไปใหม่ บน Layer 3 จึงมี Protocol เพื่อใช้ตรวจสอบว่าปลายทางยังดำเนินอยู่ไหมก่อนที่จะส่งข้อมูล นั่นคือ ICMP แต่ผู้ใช้งานจะต้องเป็นคนเรียกใช้ protocol ตัวนี้เอง

4) ชั้นทรานสปอร์ต (Transport Layer) ในชั้นนี้จะเป็นการแบ่งข้อมูลใน Layer ต่างๆ ให้พอเหมาะกับการใช้งานเช่นอาจจะแบ่งข้อมูลในส่วนของ Layer บนให้พอเหมาะกับการจัดส่งลงไปใน Layer ล่าง ซึ่งเรียกว่า Segmentation ส่วนโปรโตคอลในชั้นนี้คือ TCP,UDP,SPX ทำหน้าที่เชื่อมต่อกับ Upper Layer ในการใช้งาน network services ต่างๆ หรือ Application ต่าง จากต้นทางไปยังปลายทาง (end-to-end connection) ในแต่ละ services ได้ โดยใช้ port number ในการส่งข้อมูลของ Layer 4 จะใช้งานผ่าน protocol 2 ตัว คือ TCP และ UDP

เมื่อข้อมูลถูกส่งมาใช้งานผ่านบริการ Telnet ไปยังปลายทางถูกส่งลงมาที่ Layer 4 ก็จะทำการแยกว่า telnet คือ port number 23 เป็น port number ที่ใช้ติดต่อไปหาปลายทาง แล้วฝั่งต้นทางก็จะสุ่ม port number ขึ้นมาเพื่อให้ปลายทางสามารถตอบกลับมาได้เช่นเดียวกัน

โปรโตคอลที่สำคัญ 2 ตัว ใน Layer 4 มีรายละเอียดดังนี้

4.1) Transmission Control Protocol (TCP) มีคุณลักษณะที่สำคัญ ดังนี้

4.1.1) จัดแบ่งข้อมูลจากระดับ Application ให้มีขนาดพอเหมาะที่จะส่งไปบนเครือข่าย (Segment)

4.1.2) มีการสร้างการเชื่อมต่อ (Connection) กันก่อนที่จะมีการรับส่งข้อมูลกัน (Connection-oriented)

4.1.3) มีการใช้ Sequence Number เพื่อจัดลำดับการส่งข้อมูล

4.1.4) มีการตรวจสอบว่าข้อมูลที่ส่งไปถึงปลายทางหรือไม่ (Recovery)

การทำงานบน TCP ก่อนจะส่งข้อมูลนั้นจะต้องทำการตรวจสอบก่อนว่า ปลายทางสามารถติดต่อได้ โดยจะทำการสร้างการเชื่อมต่อระหว่างผู้ส่งและผู้รับก่อน โดยใช้กลไก Three-Way Handshake เพื่อให้แน่ใจว่าข้อมูลที่ส่งจะสามารถส่งถึงผู้รับแน่นอน นอกจาก Three-Way Handshake แล้ว TCP ยังมีกลไก Flow Control เพื่อควบคุมการส่งข้อมูลเมื่อเกิดปัญหาบนเครือข่ายระหว่างที่ส่งข้อมูลอยู่ หรือกลไก Error Recovery ในกรณีที่มีข้อมูลบางส่วนหายไปขณะส่งก็ให้ทำการส่งมาใหม่ (Retransmission) นอกจากนั้นยังสามารถทำการจัดสรรหรือแบ่งส่วนของข้อมูลออกเป็นส่วนๆ (Segmentation) ก่อนที่จะส่งลงไปที่ Layer 3 อีกด้วย และข้อมูลที่ถูกแบ่งออกก็จะใส่ลำดับหมายเลขเข้าไป (Sequence number) เพื่อให้ปลายทางนำข้อมูลไปประกอบกันได้อย่างถูกต้อง

4.2) User Datagram Protocol (UDP) มีคุณลักษณะที่สำคัญ ดังนี้

4.2.1) ไม่มีการสร้างการเชื่อมต่อ (Connection) กันก่อนที่จะมีการรับส่งข้อมูลกัน (Connectionless)

4.2.2) ส่งข้อมูลด้วยความพยายามที่ดีที่สุด (Best-Effort)

4.2.3) จะไม่มีการตรวจสอบว่าข้อมูลที่ส่งไปนั้น ถึงปลายทางหรือไม่ (No Recovery)

บน UDP จะตรงข้ามกับ TCP เพราะไม่มีการสร้างการเชื่อมต่อกันก่อน หมายความว่าถ้าบริการใดๆ ใช้งานผ่าน UDP ก็จะถูกส่งออกไปทันทีด้วยความพยายามที่ดีที่สุด (Best-Effort) และไม่มีการส่งใหม่เมื่อข้อมูลสูญหาย (No Recovery) หรือส่งไม่ถึงปลายทางอีกด้วย ข้อดีของมันก็คือ มีความรวดเร็วในการส่งข้อมูล เพราะฉะนั้นบริการที่ใช้งานผ่าน UDP ก็มีมากมาย เช่น TFTP, DHCP, VoIP และอื่นๆ เป็นต้น

5) ชั้นเซสชั่น (Session Layer) ชั้นนี้จะเป็นตัวควบคุมการส่งผ่านข้อมูลการสื่อสารจากต้นทางไปยังปลายทาง ให้มีความสอดคล้องกัน โดยไม่เกิดผลกระทบต่ออินเตอร์เฟสต่างๆ protocol ในชั้นนี้คือ RPC, SQL, Netbios, Windows socket, NFS เป็นต้น ทำหน้าที่ควบคุมการเชื่อมต่อ session เพื่อติดต่อจากต้นทาง กับ ปลายทาง เมื่อฝั่งต้นทางต้องการติดต่อไปยังปลายทางด้วย port 80 (เปิด Internet Explorer) ฝั่งต้นทางก็จะทำการติดต่อไปยังปลายทาง โดยการสร้าง session ขึ้นมา เป็น session ที่ 1 ส่งผ่าน Layer 4 โดย random port ต้นทางขึ้นมาเป็น 1025 ส่งไปหาปลายทางด้วย port 80 ระหว่าง ที่ session ที่ 1 ใช้งานอยู่ เราติดต่อไปยังปลายทางอีกครั้งด้วย port 80 (เปิด Google Chrome) ฝั่งต้นทางก็จะทำการสร้าง session ที่ 2 ขึ้นมา ส่งผ่าน

Layer 4 โดยสุ่ม port ต้นทางขึ้นมาเป็น 1026 ส่งไปหาปลายทางด้วย port 80 แล้วแต่ละ session ฝั่งปลายทาง ก็จะตอบกลับมาด้วย port ที่ฝั่งต้นทางส่งมา ทำให้สามารถแยก session ออกได้ เมื่อเราส่งข้อมูลบนเครือข่ายนั่นเอง สำหรับ Session Layer นี้จะเปรียบเหมือนชั้นแห่งการเข้าถึง Application ต่างๆ ยกตัวอย่าง ที่เห็นได้ชัด กรณีเราเข้า Program เกี่ยวกับ Network ที่เห็นได้ชัดสุด เช่นmsn messenger ช่วงที่connecting อยู่นั้น จะเป็นช่วงของsession layer จะเป็นชั้นที่บอกว่าจะเข้าสูแอพพลิเคชั่นได้หรือไม่

6) ชั้นพรีเซนเทชัน (Presentation Layer) ทำหน้าที่ในการแปล หรือ นำเสนอ structure , format , coding ต่างๆของข้อมูลบน application ที่จะส่งจากต้นทางไปยังปลายทาง ให้อยู่ในรูปแบบที่ฝั่งต้นทางและปลายทาง สามารถเข้าใจได้ทั้ง 2 ฝั่ง เป็นชั้นที่จะแสดงผลออกมาในรูปของ ภาพต่างๆที่เรามองเห็น เช่น รูปภาพ ที่ปรากฏบนจอคอมพิวเตอร์ และอาจจะรวมไปถึง การส่งผ่าน ข้อมูลต่างๆในรูปแบบของตัวโปรแกรม ที่มีการเข้ารหัส ว่ามีผลเป็นอย่างไร protocol ที่ใช้งานในชั้นนี้คือ JPEG, ASCII, Binary, EBCDICTIFF, GIF,MPEG, Encription เป็นต้น ต่อจาก Session Layer ยกตัวอย่าง msn messenger ช่วงที่connecting ถ้า network ปกติ user และ password ถูกต้อง จะสามารถเข้าสู่ msn messenger ได้และจะมีหน้าตาของ Application ขึ้นมา ซึ่งก็คือไฟล์รูปภาพ ต่างๆนั่นเอง อาจจะเป็น JPEG , BMP เป็นต้น

7) ชั้นแอพพลิเคชั่น (Application Layer) ทำหน้าที่ติดต่อระหว่างผู้ใช้ (user) กับ application ที่ใช้งานบนเครือข่าย เช่น Web Browser (HTTP), FTP, Telnet เป็นต้น สรุปแล้วมันก็คือพวก application ที่ใช้งานผ่าน network นั่นเอง ในชั้นนี้จะเป็นการแสดงผลจากตัวโปรแกรมต่างๆ ที่มีการส่งผ่านข้อมูลทางอินเตอร์เน็ต หรือเป็นโปรแกรมที่ใช้ในการโอนถ่ายข้อมูล ระหว่างเครือข่ายของเรา protocol ที่ใช้งานในชั้นนี้คือ Web Browser, HTTP, FTP, Telnet, WWW , SMTP, SNMP, NFS, MSN, Yahoo Messenger, Skye เป็นต้น ซึ่ง Application ต่างๆยังต้องอ้างอิง port ที่ใช้งานด้วยว่าเป็น tcp หรือ udp และในปัจจุบันแอพพลิเคชั่นใหม่ๆจะใช้ทั้ง tcp และ udp ในการส่งข้อมูล ดังนั้นในการทำ ACL หรือ Config Firewall ควรตรวจสอบให้ครบถ้วน

จากรายละเอียดของมาตรฐานการสื่อสารข้อมูลในระบบคอมพิวเตอร์ทำให้เราทราบว่าการที่คอมพิวเตอร์และอุปกรณ์ต่างๆจะสื่อสารกันได้ต้องมีมาตรฐานการสื่อสารหรือที่เรียกว่าโปรโตคอล สำหรับอินเทอร์เน็ตนั้น ก็มีมาตรฐานที่ใช้งานบนระบบเครือข่ายสากลหรือเครือข่ายอินเทอร์เน็ตคือโปรโตคอลทีซีพีไอพี ซึ่งสถาปัตยกรรมชุดโปรโตคอลทีซีพีไอพีได้มีการพัฒนาขึ้นมาก่อนแบบจำลอง OSI ดังนั้น ลำดับชั้นต่างๆในโปรโตคอลทีซีพีไอพี จึงไม่ตรงกับแบบจำลอง OSI แต่ก็นับได้ว่าเป็นความโชคดีที่แบบจำลองทั้งสองมีหลักการทำงานที่คล้ายคลึงกันมาก โดยทีซีพีไอพีจะมีเพียง 5 ลำดับชั้น ซึ่งประกอบด้วยลำดับชั้นฟิสิคัล ดาต้าลิงค์ เน็ตเวิร์ก ทรานสปอร์ต และชั้นแอปพลิเคชั่น โดยลำดับชั้นแอปพลิเคชั่นในทีซีพีไอพีก็คือการรวมกันของลำดับชั้นเซสชั่น พรีเซนเทชัน และชั้นแอปพลิเคชั่นของแบบจำลอง OSI นั่นเอง

พิจารณาจากตารางที่ 2.1 ที่ใช้เปรียบเทียบระหว่างแบบจำลอง OSI และสถาปัตยกรรมชุดโปรโตคอลทีซีพีไอพี มีรายละเอียด ดังนี้

ตารางที่ 2-1 เปรียบเทียบระหว่างแบบจำลอง OSI และสถาปัตยกรรมชุดโปรโตคอล TCP/IP

OSI
Application
Presentation
Session
Transport
Network
Data Link
Physical

TCP/IP
Application
Transport
Network
Data Link
Physical

จากตารางที่ 2-1 แสดงถึงการห่อหุ้มของหน่วยข้อมูลในแต่ละลำดับชั้นของชุดโปรโตคอลทีซีพีไอพี โดยที่หน่วยข้อมูลนี้จะถูกสร้างขึ้นจากผู้ใช้เริ่มจากลำดับชั้นแอปพลิเคชั่น และเรียกข้อมูลนี้ว่า เมสเสจ (message) จากนั้นเมื่อทีซีพีรับข้อมูลจากลำดับชั้นบนมาแล้ว ก็จะทำการเตรียมข้อมูลก่อนที่จะส่งต่อไปยังไอพี โดยหน้าที่ของหน่วยข้อมูลที่จัดเตรียมในลำดับชั้นทรานสปอร์ตข้อมูลตรงนี้จะเรียกว่า เซกเมนต์ หรือยูสเซอร์ดาต้าแกรม เพื่อส่งผ่านลงไปยังส่วนของลำดับชั้นเครือข่าย โดยไอพีก็จะสร้างหน่วยข้อมูลที่เรียกว่า ดาต้าแกรม และไอพีก็จะมีหน้าที่ในการนำส่งข้อมูลนี้ไปให้ถึงปลายทาง โดยข้อมูลที่นำไปส่งนั้นจะมีการแบ่งส่วนออกเป็นส่วนย่อยๆที่เรียกว่า แพ็กเก็ต และแพ็กเก็ตเหล่านี้ก็จะเดินทางผ่านเครือข่ายต่างๆมากมาย บางแพ็กเก็ตก็อาจหลงทางอยู่บนเครือข่ายทำให้ไปถึงปลายทางล่าช้ากว่าแพ็กเก็ตอื่นๆ ในขณะที่บางแพ็กเก็ตอาจสูญหายระหว่างเดินทางก็เป็นได้ ดังนั้นทีซีพีของฝั่งปลายทางจึงต้องทำหน้าที่ในการจัดเลขลำดับข้อมูลของแพ็กเก็ตให้เรียงลำดับกันอย่างถูกต้อง และด้วยเลขลำดับนี้เองจึงทำให้สามารถตรวจสอบได้ว่ามีแพ็กเก็ตใดที่หายไปหรือยังมาไม่ถึงรวมถึงข้อมูลใดที่มีการส่งมาซ้ำ ซึ่งหากข้อมูลมีการส่งมาซ้ำก็สามารถดำเนินการกำจัดแพ็กเก็ตซ้ำซ้อนนี้ออกไป นอกจากนี้ทีซีพียังต้องมีกลไกในการควบคุมการไหลของข้อมูล (Flow Control) เพื่อใช้ควบคุมจังหวะการรับส่งระหว่างฝ่ายส่งกับฝ่ายรับ ไม่ให้มีการส่งข้อมูลจนท่วมล้นจนทำให้ปลายทางรับข้อมูลไม่ทัน และเมื่อข้อมูลถูกส่งมายังลำดับชั้นดาต้าลิงค์ ในลำดับชั้นดาต้าลิงค์ก็จะทำการเอ็นแคปซูเลตข้อมูลให้อยู่ในรูปแบบของเฟรม และท้ายสุดก็จะส่งเป็นสัญญาณข้อมูลผ่านตัวกลางส่งข้อมูลในลำดับชั้นฟิสิคัล สำหรับหน้าที่ต่างๆของแต่ละลำดับชั้นในสถาปัตยกรรมชุดโปรโตคอลทีซีพีไอพี สามารถอธิบายในรายละเอียดได้ดังนี้

1) ชั้นฟิสิคัลและดาต้าลิงค์ (Physical and Data Link Layer) สำหรับในชั้นนี้ได้มีการรวมลำดับชั้นทั้งสองคือชั้นฟิสิคัลกับชั้นดาต้าลิงค์เข้าอยู่ในลำดับชั้นเดียวกัน โดยลำดับชั้นทั้งสองมีหน้าที่ในการควบคุมฮาร์ดแวร์และการรับส่งข้อมูลผ่านเครือข่าย ลำดับชั้นฟิสิคัลและดาต้าลิงค์นั้น ทีซีพีมิได้มีการระบุโปรโตคอลเฉพาะเจาะจงลงไป กล่าวคือจะสนับสนุนมาตรฐานโปรโตคอลทั้งหมดบนระดับดาต้าลิงค์ไม่ว่าจะเป็นอีเทอร์เน็ต หรือโทเค็นริง และด้วยเหตุดังกล่าวจึงมีเครือข่ายหลายประเภทที่สามารถสื่อสารกับโปรโตคอลทีซีพีได้ อย่างไรก็ตามเครือข่ายทีซีพีที่ใช้งานบนเครือข่าย

ระดับสากล ยังสามารถนำมาใช้งานเพื่อเชื่อมต่อเป็นเครือข่ายท้องถิ่น (LAN) เครือข่ายระดับเมือง (MAN) หรือเครือข่ายระดับประเทศ (WAN) ได้ด้วย

2) ชั้นเน็ตเวิร์ค (Network Layer) ทำหน้าที่ในการเลือกเส้นทางเพื่อจัดส่งข้อมูลในรูปแบบของแพ็กเก็ต โดยจะมีการใช้อัลกอลิทึ่มในการกำหนดเส้นทาง (Routing Algorithms) เพื่อให้ข้อมูลเดินทางไปถึงปลายทาง ซึ่งโปรโตคอลที่รับผิดชอบในลำดับชั้นเน็ตเวิร์คนี้เรียกว่าไอพี (IP: Internetworking Protocol) แต่การทำงานของลำดับชั้นนี้จะเป็นเพียงการตัดสินใจว่าจะส่งข้อมูลไปยังเส้นทางใดเพื่อไปถึงปลายทางเท่านั้น ไม่ได้รับประกันว่าข้อมูลที่ส่งไปจะถึงปลายทางหรือไม่ ซึ่งการรับประกันการส่งข้อมูลจะเป็นหน้าที่ของลำดับชั้นทรานสปอร์ตหรือโปรโตคอลทีซีพี

3) ชั้นทรานสปอร์ต (Transport Layer) ในลำดับชั้นทรานสปอร์ต จะทำหน้าที่จัดเตรียมข้อมูลเพื่อส่งจากต้นทางไปยังปลายทางหรือรับส่งข้อมูลระหว่างโฮสต์ที่อยู่ห่างไกลกันในลักษณะแบบ End-to-End โดยลำดับชั้นทรานสปอร์ตจะประกอบด้วยโปรโตคอลสองชุดไว้คอยบริการคือ โปรโตคอลทีซีพี ซึ่งเป็นโปรโตคอลแบบคอนเน็กชันโอเรียนเต็ด (Connection-Oriented) โดยมีการรับประกันการส่งข้อมูลถึงปลายทาง กล่าวคือจะมีการตรวจสอบข้อมูลที่ส่งไปว่าถึงผู้รับหรือไม่ โดยมีการรับรองว่าข้อมูลที่ส่งไปจะส่งถึงมือผู้รับอย่างแน่นอน นอกจากนี้ยังมีโปรโตคอลแบบ UDP (User Datagram Protocol) ซึ่งเป็นโปรโตคอลแบบคอนเน็กชันเลส (Connectionless) ที่ทำงานตรงกันข้ามกับโปรโตคอล TCP กล่าวคือจะไม่สร้างคอนเน็กชันเพื่อการเชื่อมต่อระหว่างโฮสต์โดยจะส่งข้อมูลทันทีที่ต้องการ โดยเมื่อมีข้อมูลที่จะส่งก็จะดำเนินการส่งทันที จะคาดหวังเพียงว่าข้อมูลที่ส่งไปนี้ฝั่งปลายทางคงจะได้รับในขณะที่โปรโตคอลแบบทีซีพีที่มีการทำงานแบบคอนเน็กชันโอเรียนเต็ดจะมีการสร้างคอนเน็กชันเพื่อการเชื่อมต่อระหว่างโฮสต์ต้นทางกับปลายทางก่อนที่จะมีการส่งข้อมูลจริง อีกทั้งจะมีการรับประกันถึงข้อมูลที่ส่งไปด้วยว่าถึงมือผู้รับอย่างแน่นอน

4) ชั้นแอพพลิเคชั่น (Application Layer) เป็นลำดับชั้นประยุกต์ซึ่งเป็นส่วนของผู้ใช้ที่ใช้ติดต่อกับระบบ อนุญาตให้ยูสเซอร์ที่ใช้งานซอฟต์แวร์แอพพลิเคชั่นต่างๆที่อาจมีหลายรูปแบบด้วยกัน โดยมุ่งเน้นการอินเตอร์เฟสกับผู้ใช้งานเป็นสำคัญ กล่าวคือในลำดับชั้นแอพพลิเคชั่นนี้ จะมีโปรแกรมประยุกต์ต่างๆมากมายที่จัดเตรียมไว้เพื่อความสะดวกในการอินเตอร์เฟสระหว่างยูสเซอร์กับคอมพิวเตอร์ และสนับสนุนการบริการต่างๆโดยตัวอย่างโปรโตคอลในลำดับชั้นนี้ได้แก่ Telnet, FTP, SMTP, HTTP เป็นต้น

2.1.2 โปรโตคอลไอพี (IP: Internet Protocol)

ไอพี (IP) เป็นกลไกการส่งข้อมูลที่ใช้โปรโตคอลทีซีพีไอพี ในลักษณะคอนเน็กชันเลส โดยจะไม่รับประกันการส่งข้อมูลว่าจะไปถึงผู้รับหรือไม่ ไม่มีการตรวจสอบข้อผิดพลาด และด้วยการปราศจากกลไกการรับประกันข้อมูลที่ส่งไปถึงปลายทาง การไม่มีการตรวจสอบข้อผิดพลาด และไม่ต้องสร้างคอนเน็กชันกับโฮสต์ปลายทางนี้เอง จึงทำให้หลักการทำงานของโปรโตคอลไอพีนี้ ไม่มีความซับซ้อน โดยมีหน้าที่เพียงนำส่งข้อมูลไปถึงปลายทางได้ด้วยหมายเลข IP ซึ่งเป็นหมายเลขที่ใช้ระบุตำแหน่งเครื่องและเป็นหมายเลขที่ไม่ซ้ำกัน

อย่างไรก็ตาม หากความน่าเชื่อถือในการส่งข้อมูลไปยังปลายทางเป็นสิ่งจำเป็น โปรโตคอลไอพี ก็จะทำงานควบคู่ไปกับโปรโตคอลที่มีเครื่องมือในการตรวจสอบข้อมูลว่าส่งไปถึงปลายทางหรือไม่ นั่นก็คือโปรโตคอลทีซีพี ซึ่งสามารถอธิบายเพื่อให้เห็นภาพได้ชัดเจนด้วยการ

เปรียบเทียบกับการส่งจดหมายไปรษณีย์ โดยการส่งจดหมายแบบปกติ ผู้ส่งจะนำจดหมายมาใส่ซอง ติดแสตมป์และนำไปหยอดลงในตู้ส่งจดหมาย จากนั้นเมื่อถึงเวลาบุรุษไปรษณีย์ก็จะเปิดตู้จดหมาย เพื่อนำจดหมายนี้ส่งไปถึงผู้รับปลายทางตามที่อยู่ที่ได้จ่าหน้าซองไว้ ซึ่งการส่งจดหมายในลักษณะนี้ จะไม่มีการรับประกันการส่งว่าจดหมายนี้จะถึงผู้รับปลายทางหรือไม่ จดหมายอาจมีการตกหล่นหรือสูญหายระหว่างทางก็ได้ ดังนั้น หากผู้ส่งต้องการความน่าเชื่อถือด้วยวิธีรับประกันว่าจดหมายฉบับนี้จะถึงมือผู้รับอย่างแน่นอนหรือหากไม่ถึงผู้รับ ก็จะต้องได้รับแจ้งข่าวสารกลับมาให้ทราบ การส่งจดหมายในลักษณะนี้จึงจำเป็นต้องมีการลงทะเบียน โดยผู้รับจะต้องมีการเซ็นรับจดหมายเพื่อยืนยันว่าได้รับจดหมายฉบับนี้จริง จึงถือเป็นกระบวนการส่งจดหมายถึงผู้รับเสร็จสมบูรณ์ ดังนั้นไอพีก็เปรียบเสมือนกับการส่งจดหมายธรรมดา ในขณะที่ทีซีพีก็คือการส่งจดหมายแบบลงทะเบียนที่มีการรับประกันการส่งถึงมือผู้รับนั่นเอง สำหรับแพ็กเก็ตในลำดับชั้นไอพีจะ เรียกว่าดาต้าแกรม (Datagram) โดยดาต้าแกรมเป็นแพ็กเก็ตในลักษณะ Variable-Length ซึ่งสามารถบรรจุข้อมูลได้สูงถึง 65,536 ไบต์ โดยประกอบไปด้วยสองส่วนหลักๆ ด้วยกันคือ ส่วนของเฮดเดอร์ (Header) และส่วนข้อมูล (Data) โดยเฮดเดอร์นั้นเริ่มจากตำแหน่งไบต์ที่ 20 จนถึงไบต์ที่ 60 และบรรจุด้วยข้อมูลสำคัญที่ใช้สำหรับเลือกเส้นทาง (Routing) และการส่งมอบข้อมูล โดยรายละเอียดของไอพีดาต้าแกรมมีดังนี้

2.1.2.1 Version

สำหรับฟิลด์แรกนี้คือหมายเลขเวอร์ชันของไอพี ซึ่งปัจจุบันที่ใช้งานคือเวอร์ชัน 4 (IPV4) โดยมีค่าไบนารีที่กำหนดไว้เท่ากับ 0100 (สำหรับแนวโน้มอนาคตอันใกล้นี้ จะมีการนำ IPv6 มาใช้งาน เพื่อรองรับอัตราการเจริญเติบโตของผู้ใช้อินเทอร์เน็ต ที่นับวันจะเพิ่มขึ้นและเติบโตอย่างต่อเนื่อง)

2.1.2.2 Header Length

เป็นฟิลด์ที่ใช้ระบุความกว้างของเฮดเดอร์ ซึ่งมีขนาด 4 บิต ทำให้สามารถแทนค่าตัวเลขระหว่าง 0 ถึง 15 และเนื่องจากหน่วยนับความยาวจะเป็น 4 เท่าของไบต์ ดังนั้น เมื่อมีการนำมาคูณด้วย 4 จึงทำให้มีค่าสูงสุดเท่ากับ 60 ไบต์

2.1.2.3 Service Type

เป็นฟิลด์ขนาด 8 บิต ที่ใช้กำหนดรูปแบบการบริการให้กับฝ่ายส่ง เช่น ระดับของทรูพุต ความน่าเชื่อถือ และค่าหน่วงเวลา

2.1.2.4 Total Length

เป็นฟิลด์ขนาด 16 บิต หรือ 2 ไบต์ ที่ใช้ระบุความยาวทั้งหมด(รวมเฮดเอดร์)ของไอพีดาต้าแกรม ซึ่งสามารถระบุความยาวได้สูงสุด 64 กิโลไบต์ หรือ 65,535 ไบต์

2.1.2.5 Identification

สำหรับฟิลด์นี้ จะใช้สำหรับการแฟร็กเมนต์ (Fragmentation) โดยในขณะที่ดาต้าแกรมได้มีการส่งผ่านไปยังเครือข่ายต่างชนิดกัน อาจจำเป็นต้องมีการแบ่งเป็นแฟร็กเมนต์เพื่อให้เข้ากับขนาดเฟรมของเครือข่ายนั้นๆ โดยแต่ละแฟร็กเมนต์จะถูกระบุด้วยหมายเลขลำดับในฟิลด์

2.1.2.6 Flags

ในส่วนของแฟล็กขนาด 3 บิตนี้ จะใช้สำหรับกำหนดดาต้าแกรมว่า สามารถที่จะทำการแฟร็กเมนต์ได้หรือไม่ รวมถึงเป็นตัวที่ระบุว่าแฟร็กเมนต์นั้นเป็นแฟร็กเมนต์แรก กลาง หรือเป็นแฟร็กเมนต์สุดท้าย

2.1.2.7 Fragmentation Offset

เป็นส่วนที่ใช้สำหรับเป็นพอยเตอร์หรือตัวชี้ตำแหน่งออฟเซตของข้อมูล ในส่วนของข้อมูลในดาต้าแกรมนี้มีขนาดความกว้างเท่ากับ 960 ไบต์ โดยสมมุติว่าดาต้าแกรมจะต้องเดินทางผ่านไปยังเครือข่ายต่างๆ ซึ่งมีข้อจำกัดเกี่ยวกับชิ้นส่วนของดาต้าแกรม ที่ต้องมีขนาดไม่เกิน 400 ไบต์ ดังนั้น จึงจำเป็นต้องมีการแบ่งดาต้าแกรมออกเป็น 3 ส่วนด้วยกัน คือ 400, 400 และ 16 ไบต์ โดยแต่ละแฟร็กเมนต์เหล่านั้นจะต้องมีเฮดเดอร์ปะรวมอยู่ด้วย และจะมีระยะวัดหรือที่เรียกว่าออฟเซต (Offset) ซึ่งเป็นตัววัดระยะของหน่วยนับเป็น 8 ไบต์ต่อยูนิต จะเห็นได้ว่าแฟร็กเมนต์แรกจะไม่มีระยะวัด จึงมีค่าออฟเซตเป็นศูนย์ โดยออฟเซตแรกนี้มีขนาด 400 ไบต์ สำหรับในแฟร็กเมนต์ที่สองก็จะเริ่มต้นถัดไปอีก 400 ไบต์นับจากแฟร็กเมนต์แรก และด้วยหน่วยนับเท่ากับ 8 ไบต์ต่อยูนิต ดังนั้นค่าออฟเซตที่ใช้เป็นตัววัดระยะของแฟร็กเมนต์ที่สองก็จะมีค่าเท่ากับ 50 (ได้มาจาก 400 หารด้วย 8) ในขณะที่แฟร็กเมนต์ที่สาม ซึ่งเป็นแฟร็กเมนต์สุดท้าย จะเริ่มถัดไปจาก 800 ไบต์เป็นต้นไป ดังนั้นแฟร็กเมนต์ที่สามนี้ จึงมีค่าออฟเซตเป็น 100 นั่นเอง

2.1.2.8 Time To Live (TTL)

เป็นฟิลด์ที่ใช้สำหรับกำหนดอายุขัยของดาต้าแกรม โดยโฮสต์ฝ่ายส่งจะมีการกำหนดค่าเริ่มต้นของอายุขัยให้กับดาต้าแกรม และเมื่อดาต้าแกรมนี้ได้เดินทางผ่านเครือข่ายอินเทอร์เน็ตจากเร้าเตอร์ไปยังเร้าเตอร์ตัวถัดไป เร้าเตอร์แต่ละตัวก็จะทำการลดค่านี้ลงทีละหน่วย และหากค่าดังกล่าวได้ถูกลดค่าลง จนกระทั่งมีค่าเป็นศูนย์ก่อนที่ดาต้าแกรมเหล่านั้นจะเดินทางไปถึงปลายทางสุดท้าย ดาต้าแกรมที่หมดอายุขัยนี้ก็จะถูกละทิ้งไป ซึ่งกระบวนการดังกล่าวจะเป็นการป้องกันมิให้ดาต้าแกรมที่มีปัญหาส่งข้อมูลวนเวียนอยู่ภายในเครือข่ายนั่นเอง

2.1.2.9 Protocol

เป็นฟิลด์ที่ใช้ระบุชนิดของโปรโตคอลในลำดับชั้นส่วนบน (Upper-Layer) เพื่อจะได้เป็นตัวกำหนดว่าจะส่งให้กับ TCP หรือ UDP

2.1.2.10 Header Checksum

เป็นฟิลด์ขนาด 16 บิต ที่ใช้สำหรับตรวจสอบความถูกต้องสมบูรณ์ของเฮดเดอร์ โดยการตรวจสอบในที่นี้จะทำเฉพาะในส่วนของเฮดเดอร์เท่านั้น ไม่ได้รวมแพ็กเก็ตข้อมูล

2.1.2.11 Source Address

คือหมายเลข IP ของโฮสต์ต้นทาง

2.1.2.12 Destination Address

คือหมายเลขไอพีของโฮสต์ปลายทาง

2.1.2.13 Options

เป็นส่วนเพิ่มเติมในกรณีที่ต้องการให้กำหนดหน้าที่เพิ่มเติมให้กับไอพีดาต้าแกรม โดยมีหน้าที่เกี่ยวกับการควบคุมเส้นทาง เวลา การจัดการ และวางแนวทาง เป็นต้น

2.1.3 การกำหนดตำแหน่งที่อยู่ (Addressing)

สำหรับฟิสิคัลแอดเดรสที่ได้บรรจุไว้ในอุปกรณ์ฮาร์ดแวร์ เช่น การ์ดเครือข่าย หรือที่เรียกว่า “แมคแอดเดรส (MAC Address)” จะใช้เป็นหมายเลขอ้างอิงถึงโหนดนั้นๆบนเครือข่าย ในขณะที่เครือข่ายอินเทอร์เน็ตจะมีการอ้างอิงหมายเลขโฮสต์เช่นกัน แต่จะอ้างอิงด้วยหมายเลขไอพี หรือไอพีแอดเดรส ทุกๆโฮสต์และรวมถึงอุปกรณ์อย่างเร้าเตอร์ที่ใช้งานบนเครือข่ายอินเทอร์เน็ตจำเป็นต้องมีไอพีแอดเดรสและจะไม่มีเครื่องใดบนอินเทอร์เน็ตที่จะมีไอพีแอดเดรสซ้ำกัน ขนาดความยาวของไอพีแอดเดรสที่ใช้งานอยู่ในปัจจุบันมีความยาวที่ 32 บิต ซึ่งใช้สำหรับกำหนดตำแหน่งที่อยู่ต้นทาง (Source Address) และตำแหน่งที่อยู่ปลายทาง (Destination Address) ของแพ็กเก็ตไอพีนั้นๆ แต่สิ่งสำคัญประการหนึ่งที่จำเป็นต้องรับรู้ว่าไอพีแอดเดรสนั้นไม่ใช่เป็นหมายเลขที่ใช้สำหรับอ้างอิงโฮสต์หนึ่งโฮสต์ใดจริงๆแต่การอ้างอิงถึงตำแหน่งจริงๆของโฮสต์นั้นจะใช้หมายเลขการ์ดเครือข่าย หรือแมคแอดเดรส

ในไอพีแอดเดรสจะประกอบไปด้วย 4 ไบต์ (32 บิต) โดยปกติจะประกอบด้วย 2 ส่วนหลักๆด้วยกันคือ ส่วนของหมายเลขเครือข่าย (NetID) และส่วนของหมายเลขโฮสต์ (HostID) แต่ภายในส่วนของหมายเลขเครือข่ายนี้ยังรวมถึงบิตที่ใช้สำหรับระบุคลาสของไอพีแอดเดรส ดังนั้นภายในไอพีแอดเดรสจึงประกอบด้วย 3 ฟิลด์หลักๆด้วยกัน คือ

1) ประเภทของคลาส (Class Type) เป็นประเภทของคลาสที่ใช้ระบุไอพีแอดเดรสเพื่อให้ทราบว่าไอพีแอดเดรสนี้จัดอยู่ในคลาสใด

2) หมายเลขเครือข่าย (Network Identifier: NetID) เป็นส่วนที่ใช้สำหรับการวางเส้นทางแพ็กเก็ตระหว่างเครือข่าย

3) หมายเลขโฮสต์ (Host Identifier: HostID) เป็นส่วนที่ใช้ระบุตำแหน่งเฉพาะเจาะจงของอุปกรณ์หรือโฮสต์บนเครือข่าย

2.1.4 คลาส (Classes)

ปัจจุบันมีรูปแบบของคลาสที่ใช้งานอยู่ 5 ชนิดด้วยกัน ซึ่งแต่ละคลาสได้ออกแบบมาเพื่อรองรับความต้องการที่แตกต่างกันตามแต่ละองค์กร โดยคลาส A และคลาส B ได้ถูกนำมาใช้งานเต็มหมดแล้ว ดังนั้นในปัจจุบันจึงมีเพียงแต่คลาส C ที่ใช้งานอยู่ทั่วไปเพียงเดียว ในขณะที่คลาส D และคลาส E ได้ถูกสงวนการใช้งานไว้ โดยคลาส D สงวนไว้สำหรับมัลติคาสต์แอดเดรส ส่วนคลาส E สงวนไว้เพื่อใช้งานในอนาคต

2.1.5 ซับเน็ตมาสก์ (Subnet Mask)

ในการแบ่งซับเน็ตจะทำให้เราสามารถใช้งานไอพีแอดเดรสได้อย่างมีประสิทธิภาพ และการทำซับเน็ตมากส์ก็จะทำควบคู่ไปกับการทำซับเน็ต ซับเน็ตมากส์หรือการทำมาสกิ้ง เป็นกระบวนการที่บอกให้รู้ว่าเครือข่ายของเราได้มีการแบ่งเป็นซับเน็ต จำนวนบิตที่ใช้แบ่งเครือข่ายนั้นมีกี่บิต และใช้ตำแหน่งใดเพื่อระบุเป็นหมายเลขเครือข่ายย่อย ดังนั้นในการออกแบบเครือข่ายจึงจำเป็นต้องมีการระบุซับเน็ตมากส์ด้วย เพื่อให้รู้ว่าแอดเดรสนี้มีการแบ่งส่วนหมายเลขเครือข่ายและส่วนของหมายเลขโฮสต์อย่างไร

2.1.6 เครือข่ายไอพีภายใน (Private IP Network)

จากรายละเอียดเกี่ยวกับหมายเลขไอพีแอดเดรสในแต่ละคลาสนั้น มุ่งเน้นถึงการเชื่อมต่อเข้ากับเครือข่ายระดับสากลหรืออินเทอร์เน็ตเป็นสำคัญ อย่างไรก็ตามหมายเลขไอพีแอดเดรส

ทั้งสามคลาสนั้นยังมีช่วงของหมายเลขช่วงหนึ่งที่ได้ถูกสงวนไว้เพื่อใช้งานภายใน โดยไม่ยุ่งเกี่ยวกับเครือข่ายภายนอกซึ่งเรียกว่า ไพรเวทไอพีเน็ตเวิร์ค (Private IP Network) หรือเครือข่ายไอพีภายใน ไพรเวทไอพีเน็ตเวิร์คปกติจะใช้งานภายในบริษัท หรือหน่วยงานที่ต้องการใช้เครือข่ายเฉพาะบุคคล โดยระบบจะต้องไม่มีการเชื่อมต่อไปยังเครือข่ายอินเทอร์เน็ต ซึ่งในการเข้าถึงเครือข่ายอินเทอร์เน็ต อุปกรณ์อย่างเร้าเตอร์หรือเกตเวย์จะมีการกันหมายเลขไพรเวทไอพีของเครือข่ายส่วนบุคคลเหล่านี้ ไม่ให้เชื่อมโยงไปยังเครือข่ายสาธารณะอย่างอินเทอร์เน็ตได้ เราสามารถใช้ไพรเวทไอพีเน็ตเวิร์คคลาสต่างๆ ไปใช้งานบนเครือข่ายท้องถิ่นที่มีการเชื่อมต่อด้วยโปรโตคอลทีซีพีไอพี โดยไม่ต้องขอจดทะเบียนกับทางไอเอสพี โดยแอดเดรสของไพรเวทไอพีเน็ตเวิร์คแต่ละคลาสมีรายละเอียด ดังนี้

คลาส A : หมายเลข 10.0.0.0 ถึง 10.255.255.255

คลาส B : หมายเลข 172.16.0.0 ถึง 172.31.255.255

คลาส C : หมายเลข 192.168.0.0 ถึง 192.168.255.255

นอกจากไอพีซึ่งจัดเป็นโปรโตคอลสำคัญในลำดับชั้นเน็ตเวิร์คในลำดับชั้นนี้ยังสนับสนุนโปรโตคอลอื่นๆอีกมากมาย เช่น ARP, RARP, ICMP เป็นต้น [10]

2.2 การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์

การสื่อสารข้อมูล (Data communication) [11] หมายถึง การส่งข้อมูลหรือข่าวสาร จากผู้ส่งต้นทางไปยังผู้รับปลายทางที่อยู่ห่างไกล โดยผ่านช่องทางการสื่อสารเพื่อเป็นสื่อกลางในการส่งข้อมูล ซึ่งอาจจะเป็นแบบใช้สาย หรือไม่ใช้สายก็ได้ ส่วนข้อมูลหรือข่าวสารนั้นอาจจะเป็นข้อความ เสียง ภาพเคลื่อนไหว หรือข้อมูลที่เป็นมัลติมีเดียก็ได้ ดังนั้นการสื่อสารข้อมูลจึงเป็นส่วนหนึ่งของการสื่อสารโทรคมนาคม โดยเน้นการส่งผ่านข้อมูล โดยใช้ระบบคอมพิวเตอร์และเครือข่ายเป็นหลัก ส่วนเครือข่ายคอมพิวเตอร์ หมายถึง การนำคอมพิวเตอร์และอุปกรณ์ต่าง ๆ มาเชื่อมต่อถึงกันโดยใช้สายเคเบิ้ลเป็นสื่อกลางในการแลกเปลี่ยนชุดข้อมูล ชุดคำสั่ง และข่าวสารต่าง ๆ ระหว่างคอมพิวเตอร์กับ คอมพิวเตอร์และระหว่างคอมพิวเตอร์กับอุปกรณ์ต่าง ๆ การที่ระบบเครือข่ายมีบทบาทและความสำคัญเพิ่มขึ้น เพราะไมโครคอมพิวเตอร์ได้รับการใช้งานอย่างแพร่หลาย จึงเกิดความต้องการที่จะเชื่อมต่อคอมพิวเตอร์เหล่านั้นถึงกับเพื่อเพิ่มขีดความสามารถของระบบให้สูงขึ้น เพิ่มการใช้งานด้านต่าง ๆ และลดต้นทุนระบบโดยรวมลง มีการแบ่งใช้งานอุปกรณ์และข้อมูลต่าง ๆ ตลอดจนสามารถทำงานร่วมกันได้ สิ่งสำคัญที่ทำให้ระบบข้อมูลมีขีดความสามารถเพิ่มขึ้น คือ การโอนย้ายข้อมูลระหว่างกัน และการเชื่อมต่อหรือการสื่อสาร การโอนย้ายข้อมูลหมายถึงการนำข้อมูลมาแบ่งกันใช้งาน หรือการนำข้อมูลไปใช้ประมวลผลในลักษณะแบ่งกันใช้ทรัพยากร เช่น แบ่งกันใช้ซีพียู แบ่งกันใช้ฮาร์ดดิสก์ แบ่งกันใช้โปรแกรม และแบ่งกันใช้อุปกรณ์อื่น ๆ ที่มีราคาแพงหรือไม่สามารถจัดหาให้ทุกคนได้ การเชื่อมต่อคอมพิวเตอร์เป็นเครือข่าย จึงเป็นการเพิ่มประสิทธิภาพการใช้งานให้กว้างขวางและมากขึ้นจากเดิม (จตุชัย แพงจันทร์. 2547 : 6)

2.2.1 องค์ประกอบของการสื่อสาร

ปี 1960 แบบจำลอง SMCR ของเบอร์โล (Berlo) ได้ให้ความสำคัญกับสิ่งต่าง ๆซึ่งเกี่ยวข้องกับการสื่อสาร คือ

1) ผู้ส่งสาร (Source) ต้องเป็นผู้ที่มีความสามารถเป็นอย่างมากในการเข้ารหัส (Encode) เนื้อหาข่าวสารได้ มีความรู้อย่างดีในข้อมูลที่จะส่ง สามารถปรับระดับให้เหมาะสมสอดคล้องกับผู้รับ

2) ข่าวสาร (Message) คือเนื้อหา สัญลักษณ์ และวิธีการส่ง

3) ช่องทางการสื่อสาร (Channel) ให้ผู้รับได้ด้วยประสาทสัมผัสทั้ง 5

4) ผู้รับสาร (Receiver) ผู้ที่มีความมารถในการถอดรหัส (Decode) สารที่รับมาได้อย่างถูกต้อง

แบบจำลอง SMCR ของเบอร์โล จะให้ความสำคัญในปัจจัยต่าง ๆ ที่มีผลทำให้การสื่อสารประสบผลสำเร็จได้แก่ ทักษะในการสื่อสาร ทัศนคติ ระดับความรู้ ระบบสังคมและวัฒนธรรม ซึ่งผู้รับละผู้ส่งต้องมีตรงกันเสมอ (ศุภรัศมิ์ ฐิติกุลเจริญ. 2540)

2.2.2 การใช้เทคโนโลยีในการสื่อสาร

เทคโนโลยี เป็นการนำเอาแนวความคิด หลักการ เทคนิค ความรู้ ระเบียบวิธีการ และกระบวนการ ตลอดจนผลผลิตทางวิทยาศาสตร์ทั้งในด้านสิ่งประดิษฐ์และวิธีปฏิบัติมาประยุกต์ใช้ในระบบงานเพื่อช่วยให้เกิดการเปลี่ยนแปลงในการทำงานให้ดียิ่งขึ้นและเพื่อเพิ่มประสิทธิภาพและประสิทธิผลของงานให้มีมากยิ่งขึ้น ส่วนการสื่อสาร หมายถึง การนำสื่อหรือข้อความของฝ่ายหนึ่งส่งให้อีกฝ่ายหนึ่ง ประกอบด้วยผู้ส่งข่าวสารหรือแหล่งกำเนิดข่าวสาร ช่องทางการส่งข้อมูลซึ่งเป็นสื่อกลางหรือตัวกลางอาจเป็นสายสัญญาณ และหน่วยรับข้อมูลหรือผู้รับสาร ดังนั้น เทคโนโลยีในการสื่อสาร คือการเอาแนวคิด หลักการ เทคนิค ระเบียบวิธี กระบวนการ ผ่านช่องทางการส่งข้อมูล ซึ่งทำให้ผู้รับ ได้รับและเข้าถึงข้อมูลได้เร็วขึ้น เทคโนโลยีที่ใช้ในการสื่อสารที่พบเห็น เช่น E-mail, Voice Mail, Video Conferencing เป็นต้น

2.2.3 ชนิดของสัญญาณข้อมูล

ชนิดของสัญญาณแบ่งได้เป็น 2 ชนิดคือ

1) Analog signalเป็นสัญญาณต่อเนื่อง ลักษณะของคลื่นไซน์ sine wave ตัวอย่างการส่งข้อมูลที่เป็น analog คือการส่งข้อมูลผ่านระบบโทรศัพท์ ส่วน Hertz คือหน่วยวัดความถี่ของสัญญาณ โดยนับความถี่ที่เกิดขึ้นใน 1 วินาที เช่น 1 วินาทีมีการเปลี่ยนแปลงของระดับสัญญาณ 60 รอบแสดงว่ามีความถี่ 60 Hz

2) Digital สัญญาณไม่ต่อเนื่อง ข้อมูลในเครื่องคอมพิวเตอร์ที่เป็นเลขฐาน 2 จะถูกแทนด้วยสัญญาณ digital คือเป็น 0 และ 1 โดยการแทนข้อมูลสัญญาณแบบ Unipolar จะแทน 0 ด้วยสัญญาณไฟฟ้าที่เป็นกลาง และ 1 ด้วยสัญญาณไฟฟ้าที่เป็นบวก และ Bit rate เป็นอัตราความเร็วในการส่งข้อมูล โดยนับจำนวน bit ที่ส่งได้ในช่วง 1 วินาที เช่น ส่งข้อมูลได้ 14,400 bps (bit per seconds)

2.2.4 ทิศทางการส่งข้อมูล

ทิศทางการส่งข้อมูล สามารถจำแนกทิศทางการส่งข้อมูลได้ 3 รูปแบบ ดังนี้ (ศรีไพร ศักดิ์พงศากุล และ เจษฎาพร ยุทธวิบูลย์ชัย. 2549: 100-101)

1) การส่งข้อมูลแบบทิศทางเดียว (Simplex transmission) เป็นการสื่อสารข้อมูลที่มีผู้ส่งข้อมูลทำหน้าที่ส่งข้อมูลแต่เพียงอย่างเดียว และผู้รับข้อมูลก็ทำหน้าที่รับข้อมูลแต่เพียงอย่างเดียวเช่นกัน การส่งข้อมูลในลักษณะนี้เช่น การส่งข้อมูลของสถานีโทรทัศน์

2) การส่งข้อมูลแบบสองทิศทางสลับกัน (Half-duplex transmission) เป็นการสื่อสารข้อมูลที่มีการแลกเปลี่ยนข้อมูลทั้งผู้รับและผู้ส่ง โดยแต่ละฝ่ายสามารถเป็นทั้งผู้รับและผู้ส่งข้อมูลได้ แต่จะต้องสลับกันทำหน้าที่ จะเป็นผู้ส่งและผู้รับข้อมูลพร้อมกันทั้งสองฝ่ายไม่ได้ เช่น การสื่อสารโดยวิทยุ

3) การส่งข้อมูลแบบสองทิศทางพร้อมกัน (Full-duplex transmission) เป็นการสื่อสารข้อมูลที่มีการแลกเปลี่ยนข้อมูลของทั้งผู้ส่งและผู้รับข้อมูล โดยทั้งสองฝ่ายสามารถเป็นทั้งผู้ส่งข้อมูลและผู้รับข้อมูลได้ในเวลาเดียวกัน และสามารถส่งข้อมูลได้พร้อม กัน เช่น การสื่อสารโดยใช้สายโทรศัพท์

2.2.5 ตัวกลางการสื่อสาร

สื่อกลางหรือตัวกลางในการนำส่งข้อมูล เป็นสื่อหรือช่องทางที่ใช้ในการนำข้อมูลจากต้นทางไปยังปลายทาง สื่อกลางในการเชื่อมต่ออุปกรณ์ต่าง ๆ (จตุชัย แพงจันทร์. 2547: 10-11) สามารถแบ่งออกได้เป็น 2 ชนิดใหญ่ ๆ ได้แก่

1) สายคู่บิดเกลียว (twisted pair) ประกอบด้วยเส้นลวดทองแดงที่หุ้มด้วยฉนวนพลาสติก 2 เส้นพันบิดเป็นเกลียว เพื่อลดการรบกวนจากคลื่นแม่เหล็กไฟฟ้าจากคู่สายข้างเคียงภายในเคเบิลเดียวกันหรือจากภายนอก เนื่องจากสายคู่บิดเกลียวนี้ยอมให้สัญญาณไฟฟ้าความถี่สูงผ่านได้ สำหรับอัตราการส่งข้อมูลผ่านสายคู่บิดเกลียวจะขึ้นอยู่กับความหนาของสาย คือ สายทองแดงที่มีเส้นผ่านศูนย์กลางกว้าง จะสามารถส่งสัญญาณไฟฟ้ากำลังแรงได้ ทำให้สามารถส่งข้อมูลด้วยอัตราส่งสูง โดยทั่วไปแล้วสำหรับการส่งข้อมูลแบบดิจิทัล สัญญาณที่ส่งเป็นลักษณะคลื่นสี่เหลี่ยม สายคู่บิดเกลียวสามารถใช้ส่งข้อมูลได้ถึงร้อยเมกะบิตต่อวินาที ในระยะทางไม่เกินร้อยเมตร เนื่องจากสายคู่บิดเกลียวมีราคาไม่แพงมาก ใช้ส่งข้อมูลได้ดี จึงมีการใช้งานอย่างกว้างขวาง ตัวอย่างเช่น

(ก) สายคู่บิดเกลียวชนิดหุ้มฉนวน (Shielded Twisted Pair : STP) เป็นสายคู่บิดเกลียวที่หุ้มด้วยลวดถักชั้นนอกที่หนาอีกชั้นเพื่อป้องกันการรบกวนของคลื่นแม่เหล็กไฟฟ้า

(ข) สายคู่บิดเกลียวชนิดไม่หุ้มฉนวน (Unshielded Twisted Pair: UTP) เป็นสายคู่บิดเกลียวมีฉนวนชั้นนอกที่บางอีกชั้นทำให้สะดวกในการโค้งงอแต่สามารถป้องกันการรบกวนของคลื่นแม่เหล็กไฟฟ้าได้น้อยกว่าชนิดแรก แต่ก็มีราคาต่ำกว่า จึงนิยมใช้ในการเชื่อมต่ออุปกรณ์ในเครือข่าย ตัวอย่างของสายสายคู่บิดเกลียวชนิดไม่หุ้มฉนวนที่เห็นในชีวิตประจำวันคือ สายโทรศัพท์ที่ใช้อยู่ในบ้าน

2) สายโคแอกเชียล (coaxial) เป็นตัวกลางเชื่อมโยงที่มีลักษณะเช่นเดียวกับสายที่ต่อจากเสาอากาศ สายโคแอกเชียลที่ใช้ทั่วไปมี 2 ชนิด คือ 50 โอห์มซึ่งใช้ส่งข้อมูลแบบดิจิทัล และชนิด 75 โอห์มซึ่งใช้ส่งข้อมูลสัญญาณแอนะล็อก สายประกอบด้วยลวดทองแดงที่เป็นแกนหลักหนึ่งเส้นที่หุ้มด้วยฉนวนชั้นหนึ่งเพื่อป้องกันกระแสไฟรั่ว จากนั้นจะหุ้มด้วยตัวนำซึ่งทำจากลวดทองแดงถักเป็นเปียเพื่อป้องกันการรบกวนของคลื่นแม่เหล็กไฟฟ้าและสัญญาณรบกวนอื่นๆ ก่อนจะหุ้มชั้นนอกสุดด้วยฉนวนพลาสติก ลวดทองแดงที่ถักเป็นเปียนี้เองเป็นส่วนหนึ่งที่ทำให้สายแบบนี้มีช่วงความถี่

สัญญาณไฟฟ้าสามารถผ่านได้สูงมาก และนิยมใช้เป็นช่องสื่อสารสัญญาณอนาล็อกเชื่องโยงผ่านใต้ทะเลและใต้ดิน

3) เส้นใยนำแสง (fiber optic) มีแกนกลางของสายซึ่งประกอบด้วยเส้นใยแก้วหรือพลาสติกขนาดเล็กหลายๆ เส้นอยู่รวมกัน เส้นใยแต่ละเส้นมีขนาดเล็ดเท่าเส้นผมและภายในกลวง และเส้นใยเหล่านั้นได้รับการห่อหุ้มด้วยเส้นใยอีกชนิดหนึ่งก่อนจะหุ้มชั้นนอกสุดด้วยฉนวน การส่งข้อมูลผ่านทางสื่อกลางชนิดนี้จะแตกต่างจากชนิดอื่นๆ ซึ่งใช้สัญญาณไฟฟ้าในการส่ง แต่การทำงานของสื่อกลางชนิดนี้จะใช้เลเซอร์วิ่งผ่านช่องกลวงของเส้นใยแต่ละเส้นและอาศัยหลักการหักเหของแสงโดยใช้ใยแก้วชั้นนอกเป็นกระจกสะท้อนแสง การให้แสงเคลื่อนที่ไปในท่อแก้วสามารถส่งข้อมูลด้วยอัตราความหนาแน่นของสัญญาณข้อมูลสูงมากและไม่มีการก่อกวนของคลื่นแม่เหล็กไฟฟ้า ปัจจุบันถ้าใช้เส้นใยนำแสงกับระบบอีเทอร์เน็ตจะใช้ได้ด้วยความเร็วหลายร้อยเมกะบิต และเนื่องจากความสามารถในการส่งข้อมูลด้วยอัตราความหนาแน่นสูง ทำให้สามารถส่งข้อมูลทั้งตัวอักษร เสียง ภาพกราฟิกหรือวีดิทัศน์ได้ในเวลาเดียวกัน อีกทั้งยังมีความปลอดภัยในการส่งสูง แต่อย่างไรก็มีข้อเสียเนื่องจากการบิดงอสายสัญญาณจะทำให้เส้นใยหัก จึงไม่สามารถใช้สื่อกลางนี้ในการเดินทางตามมุมตีกได้ เส้นใยนำแสงมีลักษณะพิเศษที่ใช้สำหรับเชื่อมโยงแบบจุดไปจุด จึงเหมาะที่จะใช้กับการเชื่อมโยงระหว่างอาคารกับอาคารหรือระหว่างเมืองกับเมือง เส้นใยนำแสงจึงถูกนำไปใช้เป็นสายแกนหลัก

4) สัญญาณไมโครเวฟ (Microwave) เป็นสื่อกลางในการสื่อสารที่มีความเร็วสูง ส่งข้อมูลโดยอาศัยสัญญาณไมโครเวฟซึ่งเป็นสัญญาณคลื่นแม่เหล็กไฟฟ้าไปในอากาศพร้อมกับข้อมูลที่ต้องการส่ง และจะต้องมีสถานีที่ทำหน้าที่ส่งและรับข้อมูล และเนื่องจากสัญญาณไมโครเวฟจะเดินทางเป็นเส้นตรงไม่สามารถเลี้ยวหรือโค้งตามขอบโลกที่มีความโค้งได้ จึงต้องมีการตั้งสถานีรับ-ส่งข้อมูลเป็นระยะๆ และส่งข้อมูลต่อกันเป็นทอดๆ ระหว่างสถานีต่อสถานีจนกว่าจะถึงสถานีปลายทาง และแต่ละสถานีจะตั้งอยู่ในที่สูงเช่นดาดฟ้าตึกสูงหรือยอดดอยเพื่อหลีกเลี่ยงการชนหากมีสิ่งกีดขวาง เนื่องจากแนวการเดินทางที่เป็นเส้นตรงของสัญญาณดังที่กล่าวมาแล้ว การส่งข้อมูลด้วยสื่อกลางชนิดนี้เหมาะกับการส่งข้อมูลในพื้นที่ห่างไกลมากๆ และทุรกันดาร

5) ดาวเทียม (satellite) ได้รับการพัฒนาขึ้นมาเพื่อหลีกเลี่ยงข้อจำกัดของสถานีรับส่งไมโครเวฟบนผิวโลก วัตถุประสงค์ในการสร้างดาวเทียมเพื่อเป็นสถานีรับ-ส่งสัญญาณไมโครเวฟบนอวกาศและทวนสัญญาณในแนวโคจรของโลก ในการส่งสัญญาณดาวเทียมจะต้องมีสถานีภาคพื้นดินคอยทำหน้าที่รับและส่งสัญญาณขึ้นไปบนดาวเทียมที่โคจรอยู่สูงจากพื้นโลก 22,300 ไมล์ โดยดาวเทียมเหล่านั้นจะเคลื่อนที่ด้วยความเร็วที่เท่ากับการหมุนของโลก จึงเสมือนกับดาวเทียมนั้นอยู่นิ่งอยู่กับที่ขณะที่โลกหมุนรอบตัวเอง ทำให้การส่งสัญญาณไมโครเวฟจากสถานีหนึ่งขึ้นไปบนดาวเทียมและการกระจายสัญญาณจากดาวเทียมลงมายังสถานีตามจุดต่างๆ บนผิวโลกเป็นไปอย่างแม่นยำ ดาวเทียมสามารถโคจรอยู่ได้โดยอาศัยพลังงานที่ได้มาจากการเปลี่ยนพลังงานแสงอาทิตย์ด้วยแผงโซลา (solar panel)

2.2.6 มาตรฐานเครือข่ายไร้สาย (Wireless Networking Protocols)

ด้วยความเจริญเติบโตอย่างรวดเร็วของเทคโนโลยีเครือข่ายไร้สายได้ส่งผลให้อุปกรณ์อิเล็กทรอนิกส์ เช่น พีดีเอ โทรศัพท์มือถือ ตลอดจนโรงงานอุตสาหกรรมโทรคมนาคมมีความต้องการ

มาตรฐานเพื่อการสื่อสารไร้สาย ในที่นี้กล่าวถึงการสื่อสารไร้สายดังนี้ (ศรีไพร ศักดิ์รุ่งพงศากุล และเจษฎาพร ยุทธนวิบูลย์ชัย. 2549 : 106-108)

1) บลูทูธ (Bluetooth) บลูทูธเป็นชื่อที่เรียกสำหรับมาตรฐานเรือข่ายแบบ 802.15 บลูทูธเป็นเทคโนโลยีไร้สายที่ใช้การส่งข้อมูลทางคลื่นวิทยุ (Universal Radio Interface) เริ่มใช้ในปี ค.ศ. 1998 สำหรับการเชื่อมโยงสื่อสารไร้สายในแถบความถี่ 2.45 GHz ซึ่งเป็นอุปกรณ์อิเล็กทรอนิกส์ที่ถือเคลื่อนย้ายได้ สามารถติดต่อเชื่อมโยงสื่อสารแบบไร้สายระหว่างกันในช่วงระยะห่างสั้น ๆ ได้

2) ไว-ไฟ (Wi-Fi) ไว-ไฟ ย่อมาจากคำว่า Wireless Fidelity คือมาตรฐานที่รับรองว่าอุปกรณ์ไร้สาย (Wireless LAN) สามารถทำงานร่วมกันได้ และสนับสนุนมาตรฐาน IEEE802.11b ไว-ไฟ เป็นเทคโนโลยีอินเทอร์เน็ตไร้สายความเร็วสูงที่นิยมใช้ที่สุดในโลก ใช้สัญญาณวิทยุในการรับส่งข้อมูลความเร็วสูงผ่านเครือข่ายไร้สายจากบริเวณที่มีการติดตั้ง Access Point ไปยังอุปกรณ์ที่ใช้เชื่อมต่อ เช่นโทรศัพท์มือถือ พีดีเอ เป็นต้น

3) ไว-แมกซ์ (Wi-MAX) เป็นชื่อเรียกเทคโนโลยีไร้สายรุ่นใหม่ล่าสุดที่คาดหมายกันว่าจะถูกนำมาใช้งานที่ประเทศไทยอย่างเป็นทางการ ในอนาคตอันใกล้นี้ ซึ่งเป็นเทคโนโลยีไร้สายความเร็วสูงรุ่นใหม่ตัวนี้ ได้รับการพัฒนาขึ้นมาบนมาตรฐานที่เรียกเป็นทางการว่า IEEE 802.16 ซึ่งต่อมาก็ได้พัฒนามาตรฐาน IEEE 802.16a (เหมือนกับมาตรฐานสากลตัวแรก แต่มี a ต่อท้าย) ขึ้นโดยได้อนุมัติโดย IEEE มาเมื่อเดือนมกราคม 2004 ซึ่ง IEEE ที่ว่า ก็คือสถาบันวิศวกรรมไฟฟ้าและอิเล็กทรอนิกส์ หรือชื่อเต็มๆก็คือ Institute of Electrical and Electronics Engineers โดยเจ้าระบบ Wi-MAX นี้มีรัศมีทำการไกลสูงสุดที่ 30 ไมล์ หรือเป็นระยะทางประมาณ 48 กิโลเมตร ซึ่งนั่นหมายความว่า Wi-MAX สามารถให้บริการครอบคลุมพื้นที่กว้างกว่าระบบโครงข่ายโทรศัพท์เคลื่อนที่ระบบ 3G มากถึง 10 เท่า ยิ่งกว่านั้นก็ยังมีอัตราความเร็วในการส่งผ่านข้อมูลสูงสุดถึง 75 เมกะบิตต่อวินาที (Mbps) ซึ่งเร็วกว่า 3G ถึง 30 เท่าทีเดียว และแน่นอนว่าเร็วกว่าระบบ Wi-Fi ด้วย

2.3 ระบบปฏิบัติการลินุกซ์

ลินุกซ์ (Linux) เป็นชื่อของระบบปฏิบัติการ (Operating System) แบบยูนิกซ์ (Unix-Compatible) [12] ตัวหนึ่งที่ทำงานบนเครื่องคอมพิวเตอร์ที่ใช้ตัวประมวลผล (CPU) ตระกูล Intel-x86 Compatible, Motorola 68k, Compaq (ในอดีต Digital) Alpha, Sparc, Mips และ Motorola PowerPC โดยมีการพัฒนาตามมาตรฐาน POSIX (Portable Operating System Interface) เช่นเดียวกับระบบปฏิบัติการแบบยูนิกซ์อื่นๆ (ปัจจุบัน POSIX ได้ถูกรวมเป็นส่วนประกอบของ X/Open Programming Guide) ลินุกซ์ได้ถูกพัฒนาขึ้นโดยมีความตั้งใจเริ่มต้นที่จะให้เป็นระบบปฏิบัติการแบบคล้ายยูนิกซ์ที่สามารถทำงานได้บนเครื่องพีซีธรรมดาที่ใช้ซีพียู ตระกูล Intel-x86 Compatible ซึ่งก็คือที่เราใช้กันตามบ้านนั่นเอง เป็นการพลิกผันโลกของระบบ ยูนิกซ์แทนที่จะอยู่เฉพาะในเครื่องใหญ่ๆ ตามศูนย์คอมพิวเตอร์เหมือนแต่ก่อน ลินุกซ์เป็นระบบปฏิบัติการแบบคล้ายระบบยูนิกซ์ที่มีประสิทธิภาพสูงตัวหนึ่งจุดเด่นคือลินุกซ์เป็นซอฟต์แวร์ภายใต้ลิขสิทธิ์GNU GPL (GNU General Public License, บางทีเรียกว่า GPL) สามารถใช้งานโดยที่ไม่ต้องเสียค่าใช้จ่ายใดๆ เราสามารถหาซอฟต์แวร์ลินุกซ์ได้จากเครื่องให้บริการดาวน์โหลด (FTP) หลายแห่งบนอินเทอร์เน็ต หรืออาจจะต้องจ่ายเงินเล็กน้อยเพื่อสั่งซื้อแผ่นซีดีจากบริษัทจำหน่ายซอฟต์แวร์ต่างๆ ถ้า

ไม่มีอินเทอร์เน็ตใช้งาน หรือไม่อยากจะรอดาวน์โหลดนานๆ ชนิดข้ามวันข้ามคืน เนื่องจากตัวซอฟต์แวร์ทั้งชุดจะมีขนาดหลายร้อยเมกะไบต์ เราสามารถใช้งานลินุกซ์ ได้โดยไม่ต้องเสียค่าใช้จ่ายในส่วนลิขสิทธิ์ แต่ลินุกซ์ไม่ใช่ฟรีแวร์ (Freeware) หรือแชร์แวร์ (Shareware) ตัวเคอร์เนลนั้นสงวนลิขสิทธิ์โดย Linus Torvalds ส่วนโปรแกรมประกอบอื่นๆที่เขียนขึ้นโดยผู้ใดก็จะเป็นสงวนลิขสิทธิ์เป็นของเจ้าของคนนั้นและจะอยู่ภายใต้ข้อกำหนดของ GPL เราสามารถใช้งานลินุกซ์โดยไม่เสียค่าใช้จ่ายใดๆ โดยต้องปฏิบัติตามเงื่อนไขของ GPL ซึ่งสนับสนุนให้เรามีสิทธิ์ที่จะใช้ซอฟต์แวร์ใดๆได้ และมีสิทธิ์ที่จะได้รับ Source Code เพื่อแก้ไข รวมถึงมีสิทธิ์ที่จะเผยแพร่ฉบับที่เราแก้ไขภายใต้ GPL

ลินุกซ์ถูกพัฒนาขึ้นเป็นครั้งแรกในปี ค.ศ. 1991 (พ.ศ. 2534) ที่ University of Helsinki ประเทศ Finland โดยนักศึกษาในขณะนั้นที่ชื่อ Linus B. Torvalds และถูกแจกจ่ายให้ทดลองใช้งานบนอินเทอร์เน็ต ตัวเคอร์เนลของลินุกซ์ไม่ได้ใช้ส่วนใดๆ จากระบบยูนิกซ์ของบริษัท AT&T หรือระบบปฏิบัติการยูนิกซ์อื่นใด ซอฟต์แวร์หลักที่ใช้งานบนลินุกซ์ส่วนใหญ่พัฒนามาจากโครงการ GNU (http://www.gnu.org) ที่ Free Software Foundation (FSF) (http://www.fsf.org) อย่างไรก็ตามในปัจจุบันเริ่มมีนักพัฒนาโปรแกรมหันมาพัฒนาโปรแกรมเพื่อใช้งานบนลินุกซ์เพิ่มมากขึ้นเรื่อยๆ

ในระยะแรกลินุกซ์ถูกพัฒนาเพื่อเป็นงานอดิเรกเท่านั้น โดยผู้เริ่มพัฒนาได้แรงบันดาลใจมาจากระบบมินิกซ์ (Minix) ซึ่งเป็นระบบปฏิบัติการแบบคล้ายยูนิกซ์เล็กๆ ตัวหนึ่งที่พัฒนาขึ้น โดย Andy Tanenbaum เพื่อประกอบการเรียนรู้ในหนังสือเกี่ยวกับการออกแบบระบบปฏิบัติการคอมพิวเตอร์ของเขา ลินุกซ์ถูกพูดถึงเป็นครั้งแรกในกลุ่มข่าว comp.os.minix ว่าเป็นระบบปฏิบัติการแบบคล้ายยูนิกซ์เพื่อการศึกษาขนาดเล็ก สำหรับผู้ใช้งานมินิกซ์ที่ต้องการความสามารถมากกว่าที่มินิกซ์จะทำได้ การพัฒนาในระยะแรกจะมุ่งไปที่ความสามารถในการสลับการทำงานระหว่างโปรเซส(Task-Switching) ของหน่วยประมวลผลกลาง 80386 ในProtected Mode โดยโปรแกรมทั้งหมดถูกเขียนขึ้นด้วยภาษาแอสเซมบลีภายหลังได้เริ่มเปลี่ยนมาใช้ภาษาซี ซึ่งช่วยให้การพัฒนาเป็นไปได้เร็วขึ้นกว่าเดิมมาก และในที่สุด Linux เวอร์ชัน 0.01 (ราวๆ ปลายเดือนสิงหาคม 1991) ก็ถูกแจกจ่ายให้ทดลองใช้ในเวอร์ชันนี้มีเพียงฮาร์ดดิสก์ไดรเวอร์ และระบบไฟล์ขนาดเล็กให้ใช้งานเท่านั้น ไม่มีแม้แต่ฟลอปปี้ดิสก์ไดรเวอร์ เราจะต้องมีระบบมินิกซ์อยู่แล้วจึงจะสามารถทำการคอมไพล์และทดลองใช้งานได้

2.3.1 ลีนุกซ์ดิสทริบิวชัน (Linux Distribution)

ในช่วงแรกของการนำลินุกซ์มาใช้งาน กลุ่มผู้ใช้มักจะเป็นโปรแกรมเมอร์ผู้มีความชำนาญมาก โดยจะดาวน์โหลดในส่วนของเคอร์เนล คอมไพลเลอร์ และเครื่องมือต่างๆ มาสร้างเป็นระบบปฏิบัติการของตนเองทีละส่วน จนกระทั่งเป็นระบบที่สมบูรณ์ หากติดขัดปัญหาขึ้นมาจะสอบถามและแลกเปลี่ยนความรู้กันผ่านระบบอินเทอร์เน็ต ซึ่งเป็นเรื่องยุ่งยากและใช้เวลามาก ในระยะต่อมาจึงมีการจัดตั้งกลุ่มผู้ใช้ขึ้น เพื่อรวบรวมส่วนประกอบต่างๆ ที่จำเป็นเหล่านี้เข้าด้วยกัน พร้อมทั้งจัดสร้างซอฟต์แวร์ช่วยอำนวยความสะดวกในการติดตั้งระบบปฏิบัติการนี้ขึ้น ซึ่งช่วยให้มีการติดตั้ง และใช้งานที่ง่ายขึ้น กลุ่มผู้พัฒนากรรมวิธีการติดตั้ง และรวบรวมชุดของโปรแกรมต่างๆ เหล่านี้จะเรียกว่า ลีนุกซ์ดิสทริบิวชั่น (Linux Distribution) โดยบรรดาดิสทริบิวชั่นจะเปิดเว็บไซต์ หรือ เอฟทีพีเซิร์ฟเวอร์ (FTP Server) เพื่อให้บุคคลอื่นที่สนใจสามารถดาวน์โหลดชุดโปรแกรมนี้ไปใช้ได้ฟรี แต่ยังคงมีอุปสรรคในเรื่องขนาดของไฟล์ที่มีขนาดใหญ่มาก จึงทำให้เกิดบริษัทที่จัดจำหน่ายซีดีรอมชุด

ติดตั้งโปรแกรมลีนุกซ์ขึ้น และจัดเตรียมซอฟต์แวร์แอพพลิเคชั่นที่น่าใช้งานต่างๆ ทั้งที่เป็นของฟรีและไม่ฟรี (มักจะเป็นชุดสาธิตเพื่อทดลองใช้งาน) ให้มากมาย ลีนุกซ์จึงกลายเป็นสินค้าที่มีเครื่องหมายการค้าเป็นยี่ห้อหรือค่ายต่างๆ เกิดขึ้นมากมายในปัจจุบัน เช่น Red Hat, Mandrake, Caldera Linux, Debian, Slackware และค่ายอื่นๆ อีกเป็นจำนวนมาก

ลีนุกซ์ดิสทริบิวชั่นแต่ละรายจะมีความแตกต่างกันออกไป ไม่ว่าจะเป็นขั้นตอนการติดตั้งซอฟต์แวร์ที่ให้มา ด้วยโครงสร้างไดเรคทอรี่ภายใน เครื่องมือช่วยเหลือในการคอนฟิกระบบ แต่จะมีส่วนที่เหมือนกันอย่างแน่นอน คือ จะใช้เคอร์เนลของลีนุกซ์เหมือนกัน ด้วยเหตุนี้จึงทำให้รูปแบบการคอนฟิกและใช้งานลีนุกซ์แต่ละค่ายนั้น ยังไม่มีความเป็นมาตรฐานที่แน่นอน ปัญหาดังกล่าวอาจจะสร้างความสับสนให้แก่ผู้ใช้งานได้

2.3.2 เรดแฮดลีนุกซ์ (Red Hat Linux)

เรดแฮด เป็นดิสทริบิวชั่นที่ได้รับความนิยมสูงมากทั้งในประเทศไทยและต่างประเทศ ซึ่งปัจจุบันได้ออกเวอร์ชั่นล่าสุดคือ เรดแฮด 9 โดยใช้เคอร์เนลเวอร์ชั่น 2.4.7-10 ซึ่งมีโค้ดเนมว่าอีนิกม่า (Enigma) หากนำมาเปรียบเทียบกับในรุ่นก่อนๆแล้วจะสังเกตเห็นได้ว่ามีคุณสมบัติเพิ่มขึ้นหลายอย่าง

มีเหตุผลมากมายที่ทำให้เรดแฮดได้รับความนิยมมากเช่นนี้ ทั้งนี้เนื่องมาจากมีผู้ใช้ลีนุกซ์เป็นจำนวนมากที่ใช้งานเรดแฮดอยู่ทำให้มีผู้ที่รู้เกี่ยวกับเรดแฮดมากกว่าลีนุกซ์ค่ายอื่นๆ ดังนั้นเมื่อเกิดปัญหาขึ้นสามารถขอคำปรึกษาจากผู้รู้ได้ง่าย นอกจากนี้ยังมีหนังสือ ตำรา เว็บไซต์ที่มีเนื้อหาอ้างอิงเป็นจำนวนมากกว่าลีนุกซ์ค่ายอื่นๆ ซึ่งช่วยให้ผู้ที่เริ่มต้นใหม่สามารถค้นคว้าหาข้อมูลได้ด้วยตนเอง บางครั้งอาจจะเคยได้รับทราบมาว่าผู้ดูแลระบบเครือข่ายที่ใช้ลีนุกซ์เป็นเซิร์ฟเวอร์อย่างจริงจังมักจะไม่สนใจที่จะใช้เรดแฮดแต่มักจะเลือกใช้ลีนุกซ์ดิสทริบิวชั่นอื่นๆ เช่น แสลคแวร์ (Slack Ware) โดยให้เหตุผลว่าเรดแฮดมีการติดตั้งและคอนฟิกระบบที่ง่ายเกินไป ทำให้ผู้คอนฟิกใช้ความรู้ความสามารถน้อย ไม่เหมาะสมกับหน้าที่ผู้ดูแลระบบ แต่อันที่จริงแล้ว ถ้าหากจะมีระบบปฏิบัติการอะไรซักตัวหนึ่งที่จะประสบความสำเร็จขึ้นจริงมาได้ ระบบปฏิบัติการนั้นควรจะต้องมีการติดตั้งที่สะดวกรวดเร็ว มีความรวดเร็วในการคอนฟิก และสามารถค้นหาแก้ไขข้อผิดพลาดได้ง่าย ที่สำคัญจะต้องเป็นระบบปฏิบัติการที่ถูกสร้างขึ้นมาเพื่อผู้ใช้ทุกๆ ระดับตั้งแต่มือใหม่ไปจนถึงมืออาชีพสามารถที่จะเรียนรู้ และใช้งานได้เหมือนกัน ในขณะเดียวกันยังยินยอมให้ผู้ใช้งานในระดับสูงสามารถที่จะแก้ไขปรับแต่งระบบได้โดยวิธีการแบบแมนนวลได้ตามต้องการ ซึ่งเรดแฮดเป็นดิสทริบิวชั่นหนึ่งที่มีรูปแบบของการใช้งานเช่นนั้น คือ มีรูปแบบการติดตั้งที่ให้เลือกในแบบง่ายมากไปจนถึงในแบบขั้นสูง ภายหลังจากการติดตั้งยังสามารถเลือกได้ว่าจะใช้การคอนฟิกด้วยโปรแกรมยูทิลิตี้แบบกราฟิก หรือโปรแกรมเมนูแบบเท็กซ์โหมด หรือจะคอนฟิกด้วยโปรแกรมอิดิทเตอร์แบบดั่งเดิมได้ตามต้องการ

ในด้านการจัดการแพ็คเกจ (ซอฟต์แวร์ส่วนประกอบย่อยๆ ของลีนุกซ์) เป็นอีกสิ่งหนึ่งที่มีความสำคัญมาก ไม่ว่าจะเป็นการติดตั้ง การอัพเกรด หรือยกเลิกการติดตั้งซอฟต์แวร์ต่างๆในลีนุกซ์ จะต้องมีเครื่องมือที่ช่วยอำนวยความสะดวกสำหรับงานเหล่านี้ เรดแฮดได้สร้างระบบการจัดการแพ็คเกจเป็นของตนเอง คือ อาร์พีเอ็ม (Red Hat Package Management) ซึ่งเป็นที่นิยมใช้งานกันอย่างแพร่หลายดังจะเห็นได้ว่า ดิสทริบิวชั่นอื่นๆ จะสนับสนุนอาร์พีเอ็มนี้เช่นกันรวมทั้งซอฟต์แวร์ใช้

งานต่างๆ ที่ผลิตขึ้นมาเพื่อติดตั้งใช้งานกับลีนุกซ์จะมีแพ็คเกจ อาร์พีเอ็มเป็นส่วนใหญ่ จนเรียกได้ว่าเป็นรูปแบบมาตรฐานในการติดตั้งซอฟต์แวร์บนลีนุกซ์

จากความสำเร็จของเรดแฮดในด้านความง่ายในการติดตั้งระบบ การคอนฟิก และมีการสนับสนุนทางเทคนิคสำหรับองค์กรขนาดใหญ่ จึงทำให้ เรดแฮดเป็นดิสทริบิวชั่นอันดับต้นๆ ที่ถูกเลือกเพื่อนำมาใช้งานในทุกๆ ระดับ รวมไปถึงเป็นต้นแบบของดิสทริบิวชั่นอื่นๆ ที่ได้รับการพัฒนาขึ้นในเวลาต่อมา จึงทำให้โครงสร้างหลักๆ ของลีนุกซ์ค่ายอื่นๆ ทั้งที่เป็นของคนไทย และของประเทศอื่นๆ มีความคล้ายคลึงกันกับเรดแฮดเป็นอย่างมากด้วยจำนวนผู้ใช้เรดแฮดที่มีจำนวนมากขึ้นนี้เอง เรดแฮดจึงมีพัฒนาการในการให้บริการต่างๆ เพิ่มมากขึ้น โดยมีเว็บไซต์ http://www.redhat.com เป็นแหล่งข่าวสารเกี่ยวกับลีนุกซ์ที่สำคัญแห่งหนึ่ง ซึ่งมีจำนวนสมาชิกนับล้านคนจากทั่วโลก นอกจากนี้ยังมีสำนักงานสาขาต่างๆอยู่ทั่วทุกมุมโลก และเมื่อไม่นานมานี้ ยังได้มีการรวมเป็นพันธมิตรทางธุรกิจ และการพัฒนาผลิตภัณฑ์ร่วมกันกับบริษัทคอมพิวเตอร์รายใหญ่ๆ เช่น ไอบีเอ็ม (IBM), อินเทล (Intel), เอชพี(HP), คอมแพค (Compaq) อีกด้วย

2.3.3 เรดแฮดลีนุกซ์ในฐานะเซิร์ฟเวอร์

ลีนุกซ์ เป็นระบบปฏิบัติการแบบ 32 บิต ที่มีลักษณะคล้ายยูนิกซ์ จึงมีคุณสมบัติที่พร้อมสำหรับการทำหน้าที่เป็นเซิร์ฟเวอร์ของระบบเครือข่ายได้ทันที การนำลีนุกซ์เข้ามาใช้งานในระยะแรกๆ จึงเป็นในฐานะเครื่องเซิร์ฟเวอร์มากกว่าจะใช้งานเป็นเครื่องเดสก์ทอปธรรมดา สำหรับลีนุกซ์ดิสทริบิวชั่นต่างๆ มักจะออกแบบผลิตภัณฑ์ของตนเองให้ผู้ใช้สามารถนำไปใช้งานได้ทุกลักษณะตามต้องการ จึงได้รวบรวมเอาซอฟต์แวร์ต่างๆ เอาไว้ให้เป็นจำนวนมาก เรดแฮดเองเช่นกัน สามารถนำเรดแฮดมาใช้งานในฐานะเซิร์ฟเวอร์ต่างๆ ได้มากมาย

2.3.4 ไฟล์เซิร์ฟเวอร์ (File Server)

งานด้านการให้บริการของไฟล์เซิร์ฟเวอร์ เป็นงานที่สำคัญในอันดับต้นๆ ที่ในองค์กรจำเป็นต้องใช้งาน เรดแฮดจะมีซอฟต์แวร์ที่ทำหน้าที่นี้ให้มาพร้อมด้วยแล้วหลายโปรแกรมเช่นแซมบ้า (Samba) ซึ่งจะทำหน้าที่เป็นตัวจำลองการทำงานให้ลีนุกซ์ทำหน้าที่เป็นไฟล์เซิร์ฟเวอร์ของไมโครซอฟต์วินโดวส์ (Microsoft Window) เมื่อคอนฟิกแซมบ้าสำเร็จแล้ว จะสามารถเห็นเครื่องลีนุกซ์นี้ได้โดยผ่าน เน็ทเวิร์กเนเบอร์ฮู้ด (Network Neighborhood) และเข้าใช้งานแชร์โฟลเดอร์ของแซมบ้าได้เช่นเดียวกันกับคอมพิวเตอร์ที่เป็นวินโดวส์ที่เราคุ้นเคยกัน โดยสามารถที่จะกำหนดสิทธิ์ให้แก่ผู้ใช้งานแต่ละคน หรือจัดผู้ใช้เป็นกรุ๊ป สามารถทำงานร่วมกับฐานข้อมูลเดิมที่ใช้อยู่ในระบบวินโดวส์เอ็นที หรือ วินโดวส์ 2000 (Windows NT/2000) ได้ นอกจากนี้ยังสามารถจำลองแซมบ้าเป็น ไพรมารี่โดเมนคอนโทรเลอร์ (Primary Domain Controller) และวินส์เซิร์ฟเวอร์ (WINS Server) ได้อีกด้วย และเอ็นเอฟเอส (Network File System) เป็นไฟล์แชร์ลิ่งเซอร์วิส ที่มีการใช้งานในระบบยูนิกซ์ ซึ่งลีนุกซ์สามารถทำหน้าที่นี้ได้เช่นกัน นอกจากนี้ยังมีไฟล์เซิร์ฟเวอร์ชนิดอื่นๆ ให้มาอีก เช่นไฟล์เซิร์ฟเวอร์ในแบบของเน็ทแวร์ (Netware)

2.3.5 เครื่องพิมพ์บนระบบเครือข่าย (Print Server)

งานบริการเครื่องพิมพ์บนระบบเครือข่าย เป็นงานหนึ่งซึ่งทุกๆ องค์กรจำเป็นต้องใช้งาน เรดแฮดสามารถจะทำหน้าที่นี้ได้อย่างดีเช่นกัน โดยอาจจะคอนฟิกแซมบ้าเพื่อแชร์เครื่องพิมพ์

จากลีนุกซ์เพื่อให้บริการแก่เครื่องลูกข่ายที่เป็นวินโดวส์ หรืออาจจะใช้บริการในรูปแบบของยูนิกซ์ อย่าง แอลพีดี (lpd) สำหรับเครื่องลูกข่ายที่เป็นลีนุกซ์หรือยูนิกซ์ด้วยกันได้

2.3.6 เว็บเซิร์ฟเวอร์ (Web Server)

ในยุคอินเทอร์เน็ตอย่างทุกวันนี้ เว็บเซิร์ฟเวอร์เป็นกลไกสำคัญต่อองค์กรต่างๆ และช่วยสนับสนุนแอพพลิเคชั่นใหม่ๆ ในลักษณะของเว็บเบสแอพพลิเคชั่น (Web based Application) ซึ่งเรดแฮดได้รวมเอา อาปาร์เช่เว็บเซิร์ฟเวอร์ (Apache Web Server) อันเป็นเว็บเซิร์ฟเวอร์ที่มีประสิทธิภาพสูงและนิยมใช้มากที่สุดในโลกไว้แล้ว โดยพร้อมที่จะทำงานทันทีที่คอนฟิกอีกเพียงเล็กน้อย นอกจากตัวอาปาร์เช่เองแล้ว เรดแฮดยังมีส่วนประกอบอื่นๆ ที่เกี่ยวข้องกับการพัฒนาบริการต่างๆ บนเว็บให้มาพร้อมกันด้วย เช่น เพิล (Perl), พีเอชพี(PHP), ไพทัน(Python) และเอสเอสไอ (SSI) เป็นต้น

2.3.7 ดีเอ็นเอสเซิร์ฟเวอร์ (DNS Server)

ดีเอ็นเอส หรือโดเมนเนมเซิร์ฟเวอร์ (Domain Name Server) เป็นงานบริการพื้นฐานในเครือข่ายที่ใช้โปรโตคอล ทีซีพี/ไอพี (TCP/IP) ซึ่งงานบริการต่างๆ เช่นเว็บหรือเมล์ จะไม่สามารถทำงานได้ หากเครื่องให้บริการปราศจากดีเอ็นเอส เรดแฮดมีซอฟต์แวร์ชื่อว่า บายด์ (BIND : Berkeley Internet Name Domain) แม้ว่าเรดแฮดจะเป็นซอฟต์แวร์ฟรี แต่บายด์มีความเป็นมาตรฐานที่ทำงานอยู่ในเซิร์ฟเวอร์ยูนิกซ์ทั่วโลก

2.3.8 เมล์เซิร์ฟเวอร์ (Mail Server)

หากจะนำเรดแฮดมาใช้งานด้านเมล์เซอร์วิสแล้ว นับได้ว่าเป็นสิ่งที่คุ้มค่าที่สุด เพราะว่าเรดแฮด จะมีโมดูลที่ชื่อว่า เซนเมล์ (Sendmail) ซึ่งเป็น อินเทอร์เน็ตเมล์เซิร์ฟเวอร์ (Internet Mail Server) ที่มีใช้งานมากที่สุด เมื่อประกอบเข้ากับซอฟต์แวร์เล็กๆ อีก 2-3 โปรแกรม (ซึ่งมีมาพร้อมกันแล้ว) จะทำให้ได้เมล์เซิร์ฟเวอร์ที่สนับสนุนทั้ง เอสเอ็มทีพี (SMTP), ป๊อปทรี(POP3) และ ไอแมพ (IMAP) และยังสามารถนำไปประยุกต์ทำออฟไลน์เมล์เซิร์ฟเวอร์ (Off-line Mail Server) ได้อีกด้วย

2.3.9 อินเทอร์เน็ตเกตเวย์ (Internet Gateway)

การเชื่อมต่อระบบเครือข่ายภายในองค์กรเข้ากับอินเทอร์เน็ตโดยผ่านอินเทอร์เน็ตเกตเวย์เป็นสิ่งที่นิยมกันอย่างแพร่หลายในทุกๆ องค์กร โดยเราสามารถที่จะใช้คุณสมบัติของไอพีเราท์ติ้ง (IP Routing) และการทำแนท (Network Address Translation) ด้วยโปรแกรมประเภทแพ็คเกจฟิลเตอร์ริ่ง (Packet Filtering) ที่มีมาพร้อมกันแล้วในลีนุกซ์ เพียงเท่านี้ สามารถที่จะให้คอมพิวเตอร์ลูกข่ายใช้งานอินเทอร์เน็ตได้

2.3.10 ดาต้าเบสเซิร์ฟเวอร์ (Database Server)

เราคงจะไม่สามารถปฏิเสธได้ว่า ข้อมูล คือสิ่งที่มีความสำคัญที่สุดทางธุรกิจ ดาต้าเบสเซิร์ฟเวอร์ที่ดิสทริบิวชั่นต่างๆ รวมทั้งเรดแฮด ได้ผนวกรวมมาในชุดมาตรฐานแล้ว และจะเป็นซอฟต์แวร์ฟรีเช่นกัน ซึ่งได้แก่ โพสเกรทเอสคิวแอล (PostgreSQL) และ มายเอสคิวแอล(MySQL) ซึ่งในช่วงเวลาที่ผ่านมายังไม่มีการนำคุณสมบัติส่วนนี้มาใช้มากเท่าไรนัก แต่สำหรับ
ในอนาคตแล้ว มีแนวโน้มที่จะพัฒนาในด้านนี้เพิ่มขึ้นอย่างแน่นอน โดยเฉพาะในด้านเว็บแอพพลิเคชั่น

2.3.11 เซอร์วิสอื่นๆในด้านของเซิร์ฟเวอร์

นอกจากหน้าที่สำคัญๆ ที่ได้กล่าวไปแล้ว ลีนุกซ์ยังมีบริการขั้นพื้นฐานของโปรแกรมในชุดโปรโตคอลทีซีพี/ไอพีอยู่อีกมากมาย ไม่ว่าจะเป็น เอฟทีพี (FTP) ที่ให้บริการอัพโหลดหรือดาวน์โหลดไฟล์ เทลเน็ท (Telnet) ที่ใช้เพื่อการติดต่อเข้าสู่เซิร์ฟเวอร์จากเครื่องอื่นๆ ในเครือข่าย ดีเอชซีพี (DHCP) ซึ่งให้บริการในด้านการแจกไอพีแอดเดรสแบบไดนามิค แก่เครื่องลูกข่ายในระบบ รวมทั้งยังมีบริการอื่นๆ อีกหลายอย่างที่ลีนุกซ์ทุกๆ ดิสทริบิวชั่นรวมทั้งเรดแฮดได้รวบรวมไว้ให้แล้วในซีดีชุดติดตั้ง

2.3.12 เรดแฮดกับงานด้านเดสก์ทอป

จะเห็นได้ว่าลีนุกซ์ สามารถที่จะทำหน้าที่ของเซิร์ฟเวอร์ได้มากมายและคุ้มค่า ส่วนงานในด้านเดสก์ทอปในประเทศไทยยังถือว่าอยู่ในช่วงเริ่มต้นเท่านั้น แต่ก็มีพัฒนาการที่รวดเร็ว มีข่าวคราวเกี่ยวกับการพัฒนาระบบภาษาไทยและแอพพลิเคชั่นต่างๆ เกิดขึ้นอยู่เสมอ มีผู้ใช้งานบางกลุ่มเริ่มที่จะนำลีนุกซ์ดิสทริบิวชั่นต่างๆ ที่มีความสามารถด้านภาษาไทยมาใช้งาน ในระดับเครื่องเดสก์ทอปกันมากขึ้น แต่ในปัจจุบัน ลีนุกซ์ยังไม่สามารถที่จะนำมาแทนที่ไมโครซอฟต์วินโดวส์ได้ทั้งหมดการกำหนดการทำงานของลีนุกซ์จะมีความยุ่งยากซับซ้อนกว่าวินโดวส์ เนื่องจากลีนุกซ์มีสภาพแวดล้อมแบบผู้ใช้งานหลายคน มีระบบรักษาความปลอดภัยและการกำหนดสิทธิ์ โดยที่ผู้ใช้จะต้องมีการเรียนรู้และปรับตัวกันใหม่ ลีนุกซ์มีระบบจียูไอ (Graphics User Interface) ที่มีหน้าจอเดสก์ทอปเป็นแบบกราฟิกและสนับสนุนการใช้งานด้วยเมาส์ มีหน้าจอที่สวยงามน่าใช้และมีให้เลือกใช้งานหลายโปรแกรม ได่แก่ จีโนม (GNOME) และเคดีอี (KDE) โดยที่เดสก์ทอปทุกตัวจะทำงานบนระบบ เอกซ์วินโดวส์ (X Window) อีกชั้นหนึ่ง เดสก์ทอปแบบกราฟิกนี้เองที่ช่วยให้ผู้ใช้ทั่วไปสามารถที่จะใช้งานลีนุกซ์ได้สะดวกมากยิ่งขึ้น

โปรแกรมเดสก์ทอปจีโนม เป็นโปรแกรมที่ใช้ในการจัดการลีนุกซ์แบบกราฟิกที่สวยงามช่วยให้ใช้งานได้สะดวกมากยิ่งขึ้นกว่าเดิม ส่วนเดสก์ทอปแบบเคดีอี จะมีการติดตั้งซอฟต์แวร์ที่ชื่อว่าคอนคิวเรอร์ (Konqueror) ซึ่งมีคุณสมบัติที่ดี ทั้งการแสดงผลแบบทรีหรือแบบวิวเวอร์และสามารถเป็นเว็บบราวเซอร์ได้ในตัว ทำให้เรียนรู้เพียงแค่อินเตอร์เฟสเดียว แต่สามารถที่จะใช้งานได้เอนกประสงค์และยังมีแอพพลิเคชั่นอีกจำนวนมากมายทั้งเกมส์ ชุดโปรแกรมออฟฟิศ เครื่องมือพัฒนาโปรแกรม ยูทิลิตี้ด้านการคอนฟิก เน็ทเวิร์ก และอินเทอร์เน็ต มีให้เลือกใช้ทั้งในส่วนของจีโนมและเคดีอี ถ้ายังไม่ตรงตามความต้องการใช้งานสามารถค้นหาฟรีซอฟต์แวร์มาติดตั้งเพิ่มเติมได้อีก

2.3.13 ลีนุกซ์กับงานด้านการศึกษาและพัฒนาระบบคอมพิวเตอร์

จากที่ได้กล่าวถึงความเป็นมาของลีนุกซ์ซึ่ง ถูกพัฒนามาในฐานะส่วนหนึ่งของการเรียนการสอนวิชาทางด้านคอมพิวเตอร์ ลีนุกซ์จึงเป็นระบบปฏิบัติการที่เหมาะสมกับนักศึกษาและผู้สนใจในด้านคอมพิวเตอร์เป็นอย่างยิ่ง เนื่องจาก ลีนุกซ์เป็นระบบปฏิบัติการแบบโอเพ่นซอสและเป็นฟรีซอฟต์แวร์อีกทั้งยังมีโปรแกรมตัวแปลภาษาต่างๆ ให้เลือกใช้อย่างมากมาย ดังนั้นจึงสามารถที่จะนำไปใช้ในการศึกษาเรียนรู้ได้อย่างกว้างขวาง ไม่ว่าจะใช้เพื่อศึกษาการทำงานของระบบปฏิบัติการ การเขียนโปรแกรมตั้งแต่ระดับซอฟต์แวร์ทั่วๆ ไป จนถึงแอพพลิเคชั่นระดับสูงศึกษาระบบเครือข่ายโปรโตคอล และระบบรักษาความปลอดภัย หรือจะใช้เป็นเครื่องมือเพื่อพัฒนาเว็บไซต์ ระบบปฏิบัติการลีนุกซ์ จึงไม่เป็นเพียงแค่ระบบปฏิบัติการสำหรับผู้บริหารระบบเครือข่ายเท่านั้น แต่ยังสามารถใช้เป็นตัวสร้างโอกาสทางการศึกษาและพัฒนาระบบคอมพิวเตอร์ที่นักคอมพิวเตอร์ทุก

ระดับควรนำมาใช้ให้เกิดประโยชน์สูงสุด โดยเฉพาะองค์กรที่มีข้อจำกัดเรื่องงบประมาณในการลงทุนเกี่ยวกับเครือข่าย เนื่องจากอุปกรณ์ฮาร์ดแวร์ที่มีราคาสูงแล้ว ซอฟต์แวร์ระบบปฏิบัติการก็มีค่าลิขสิทธิ์ที่แพงเช่นกัน การนำลินุกซ์มาใช้ถือว่าเป็นทางเลือกที่ดี

2.3.14 ลินุกซ์ CentOS

CentOS ย่อมาจาก Community ENTerprise Operating System เป็นลีนุกซ์ที่พัฒนามาจากต้นฉบับ RedHat Enterprise Linux (RHEL) โดยที่ CentOS ได้นำเอาซอร์สโค้ดต้นฉบับของ RedHat มาทำการคอมไพล์ใหม่โดยการพัฒนายังเน้นพัฒนาเป็นซอฟต์แวร์ Open Source ที่ถือลิขสิทธิ์แบบ GNU General Public License ในปัจจุบัน CentOS Linux ถูกนำมาใช้ในการทำ Web Hosting กันอย่างกว้างขวางเนื่องจากเป็นระบบปฏิบัติการที่มีต้นแบบจาก RedHat ที่มีความแข็งแกร่งสูง (ปัจจุบันเน้นพัฒนาในเชิงการค้า) การติดตั้งแพ็กเกจย่อยภายในสามารถใช้ได้ทั้ง RPM, TAR, APT หรือใช้คำสั่ง YUM ในการอัพเดทซอฟต์แวร์แบบอัตโนมัติ สามารถอ่านรายละเอียดเพิ่มเติมได้ที่เว็บไซต์หลักของ CentOS

เหตุผลหลักที่องค์กรจะเลือกใช้ระบบ CentOS เพราะว่า สำหรับองค์กรธุรกิจเหมาะสมอย่างมากที่จะนำระบบตัวลีนุกซ์ตัวนี้มาทำเป็น เซิร์ฟเวอร์ใช้งานภายในองค์กร โดยพอสรุปเหตุผลหลักในการนำระบบนี้มาใช้งานได้ดังนี้

1) เพื่อประหยัดงบประมาณขององค์กร เนื่องจาก CentOS เป็นซอฟต์แวร์โอเพ่นซอสองค์กรไม่จำเป็นต้องจ่ายค่าลิขสิทธ์ซอฟต์แวร์ (เพียงแต่ผู้ดูแลระบบต้องลงทุนเรียนรู้ระบบก่อนการใช้งาน ในปัจจุบันสามารถเรียนรู้ได้ง่ายดายผ่านทางหน้าเว็บ Google.com)

2) เพื่อนำมาทำเซิร์ฟเวอร์บริการงานต่างๆ ในองค์กร ซึ่งภายใน CentOS มีแพ็กเกจย่อยที่นำมาใช้ทำเซิร์ฟเวอร์สำหรับใช้งานในองค์กรจำนวนมาก อาทิ เช่น Web Server (Apache), FTP Server (ProFTPd/VSFTPd), Mail Server (Sendmail/Postfix/Dovecot), Database Server (MySQL/PostgreSQL), File and Printer Server (Samba), Proxy Server (Squid), DNS Server (BIND), DHCP Server (DHCPd), Antivirus Server (ClamAV), Streaming Server, RADIUS Server (FreeRADIUS), Control Panel (ISPConfig) เป็นต้น

3) เพื่อนำมาทำเป็นระบบเซิร์ฟเวอร์สำหรับจ่ายไอพีปลอม (Private IP Address) ไปเลี้ยงเครื่องลูกข่ายในองค์กร รวมทั้งตั้งเป็นระบบเก็บ Log Files ผู้ใช้งาน เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ปี 2550

แพ็กเกจยอดนิยมสำหรับใช้งานบนระบบ CentOS สำหรับในแผ่น CD ของ CentOS มีแพ็กเกจที่สามารถนำมาติดตั้งใช้งานได้ทันทีจำนวนมาก โดยสามารถนำมาติดตั้งใช้งานได้ทันที สำหรับแพ็กเกจที่ไม่มีอยู่ในแผ่น CD สามารถเข้าไปดาวน์โหลดได้ที่เว็บไซต์ http://www.rpmfind.net หรือ http://www.freshrpms.net ซึ่งมีเพียงพอต่อการใช้งาน สำหรับ

2.4 โปรโตคอลเอชทีทีพี (HTTP)

ปีพ.ศ.2533 นักวิทยาศาสตร์จากห้องทดลองของสถาบันเซิร์น (CERN) ซึ่งเป็นห้องปฏิบัติการฟิสิกส์แห่งยุโรปในนครเจนีวา ประเทศสวิตเซอร์แลนด์ คือ ทิม เบิร์นเนอร์ส-ลี (Tim Berners-Lee)

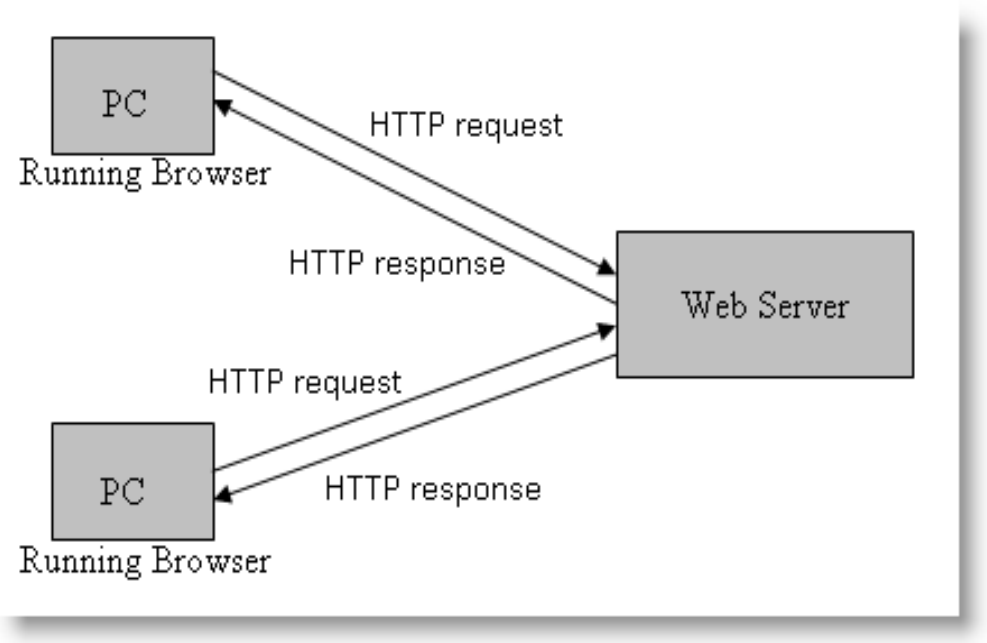
ได้สร้างระบบการสื่อสารข้อมูลผ่านเครือข่ายคอมพิวเตอร์ในรูปแบบใหม่ที่เรียกว่า ไฮเพอร์เท็กซ์ (Hypertext) ซึ่งผลที่ได้ทำให้มีการสร้างโปรโตคอลแบบ HTTP (Hypertext Transport Protocol) [13] ขึ้นเพื่อใช้ในการส่งสารสนเทศต่างๆ โดยจะถูกจัดอยู่ในรูปแบบใหม่ที่เรียกว่า HTML (Hypertext Markup Language) ซึ่งการสื่อสารและการสืบค้นสารสนเทศในรูปแบบใหม่นี้ทำให้มนุษย์สามารถติดต่อสื่อสารกันได้อย่างรวดเร็วในทุกรูปแบบ ไม่ว่าจะเป็นข้อความ ภาพ หรือเสียง

การทำงานของไฮเปอร์เท็กซ์ นั้นมีหน้าที่ที่จะต้องกำหนดว่าข้อมูลจะเป็นไปในรูปแบบใดและข้อมูลจะส่งไปอย่างไร อีกทั้งยังต้องกำหนดด้วยว่าเว็บที่ให้บริการ (Web Server) และเครื่องมือที่ช่วยเรียกดูเว็บ (Browser) [14] มีหน้าที่รับผิดชอบคำสั่งทั้งหมดอย่างไร ตัวอย่างเช่น เมื่อเราใส่รหัสที่ตั้งทรัพยากร (Uniform Resource Locator : URL) ลงในเบราว์เซอร์เพื่อสั่งค้นหาข้อมูลจากอินเทอร์เน็ตตามรหัสค้นหาที่เรากำหนด ซึ่งเมื่อทำดังนี้เบราว์เซอร์ก็จะส่งคำร้องขอตามกฎเกณฑ์การส่งไฮเปอร์เท็กซ์นั้นไปยังเว็บที่ทำหน้าที่ให้บริการ (Web Server) [15] เมื่อเว็บให้บริการรับการร้องขอนั้นมา ก็จะทำการประมวลผลและส่งข้อมูลกลับมาในรูปแบบของเอกสารเว็บเพจ (Web Page) เมื่อเบราว์เซอร์ได้รับข้อมูลกลับมาก็จะนำมาสร้างเป็นรูปแบบเอกสารนำเสนอต่อผู้ใช้ ซึ่งมาตรฐานในการกำหนดและควบคุมว่าเอกสารเป็นรูปแบบใดก็คือ รูปแบบที่ใช้แสดงผลแบบเอกสารเว็บ (HTML) ซึ่งจะควบคุมทั้งหมดว่าเอกสารนั้นเป็นไปในรูปแบบไหน และจะถูกจัดแสดงอย่างไร

กฎเกณฑ์การส่งไฮเปอร์เท็กซ์นั้นเป็นแบบที่ไม่มีการเก็บสถานะของเก่าไว้เลย แต่ละคำร้องที่ถูกจัดส่งโดยกฎเกณฑ์การส่งแบบกฎเกณฑ์การส่งไฮเปอร์เท็กซ์นั้นถูกนำไปใช้งานอย่างอิสระ นั่นจึงเป็นเหตุผลหนึ่งที่ทำให้เกิดความยากในการนำมาปรับใช้กับระบบคอมพิวเตอร์ที่ทำหน้าที่เก็บเอกสารเว็บเพื่อให้ผู้อื่นนำไปใช้ เพราะเป็นการยุ่งยากที่จะปรับปรุงให้สามารถที่จะตอบสนองความต้องการที่ผู้ใช้ร้องขอเข้ามาได้อย่างชาญฉลาดเพราะข้อจำกัดของกฎเกณฑ์การส่งไฮเปอร์เท็กซ์นี้จึงทำให้เกิดเทคโนโลยีมากมายตามมาเพื่อขจัดปัญหาเหล่านี้ให้หมดไป หากจะเปรียบเทียบกฎเกณฑ์การส่งไฮเปอร์เท็กซ์กับกฎเกณฑ์การถ่ายข้อมูล (FTP) ความแตกต่างก็คือกฎเกณฑ์การส่งไฮเปอร์เท็กซ์เป็นการสื่อสารทางเดียว เพียงแค่ถ่ายโอนเนื้อหาของเอกสารเว็บมายังเครื่องมือช่วยเรียกดู เช่น Internet Explorer เพื่อที่จะนำมาแสดงผล ซึ่งต่างกับกฎเกณฑ์การถ่ายโอนข้อมูล ที่เป็นแบบสื่อสารสองทางระหว่างเครื่องคอมพิวเตอร์เครื่องหนึ่งกับเครื่องคอมพิวเตอร์และจัดเก็บข้อมูลลงในสื่อบันทึกข้อมูล

กฎเกณฑ์การส่งไฮเปอร์เท็กซ์ (Hypertext Transport Protocol : HTTP) [16] เป็นมาตรฐานอินเทอร์เน็ตที่กำหนดขึ้นมาไว้ใช้สนับสนุนการแลกเปลี่ยนข้อมูลบนเวิลด์ไวด์เว็บ (www) โดยการกำหนดที่ตั้งทรัพยากรที่สอดคล้องกัน (Uniform Resource Locators : URLs) และวิธีการใช้ในการสืบค้นข้อมูลที่ใดก็ได้ในอินเทอร์เน็ต โดยไม่เพียงแต่เอกสารในเว็บเท่านั้น แต่รวมถึงแฟ้มที่เข้าถึงได้ในกฎเกณฑ์การถ่ายโอนแฟ้ม (File Transfer Protocol : FTP) นอกจากนี้กฎเกณฑ์การส่งไฮเปอร์เท็กซ์ยังให้ผู้เขียนในเว็บสามารถฝังจุดเชื่อมโยงหลายมิติ (Hyperlink) ในเอกสารเว็บได้อีกด้วย เมื่อมีการคลิกที่จุดเชื่อมโยงจะเริ่มกระบวนการถ่ายโอนข้อมูลซึ่งเข้าถึงและค้นคืนเอกสารให้โดยที่ผู้ใช้ไม่ต้องทำสิ่งใดให้ยุ่งยาก กล่าวอย่างสั้นๆก็คือ กฎเกณฑ์การส่งไฮเปอร์เท็กซ์ได้วางรากฐานสำหรับการเข้าถึงอินเทอร์เน็ตอย่างโปร่งใสเข้าใจง่าย นั่นเอง

2.4.1 หลักการทำงานของ HTTP



ภาพที่ 2-1 หลักการทำงานของ HTTP

1) สร้างการเชื่อมต่อ (TCP connection) ไปยังเว็บเซิร์ฟเวอร์ โดยถ้าไม่มีการระบุพอร์ต (port) จะใช้เป็นพอร์ต 80 เป็นดีฟอล์ต จากนั้นทำการร้องขอ (Request) ขอให้เครื่องเว็บเซิร์ฟเวอร์ส่งสำเนาของวัตถุนั้นมาให้เครื่องลูกข่าย ซึ่งเครื่องเว็บเซิร์ฟเวอร์จะทำการตอบกลับ (Responses) โดยบ่งบอกรุ่น (Version) ของ HTTP ที่เครื่องให้บริการใช้อยู่ พร้อมกับรหัสผลลัพธ์และข้อความอื่นๆ ตามด้วยเฮดเดอร์วัตถุ (Optional Object Headers) ต่อเนื่องเป็นลำดับ

2) ส่ง HTTP Request ผ่าน socket ที่สร้างผ่านการเชื่อมต่อ TCP ในข้อ 1

3) Web server ค้นหาไฟล์ที่ได้รับการร้องขอมา แล้วส่งไปใน packet ตอบกลับไปยังเครื่อง client

4) Web Server คงสถานภาพการเชื่อมต่อไว้ เพื่อรอรับการร้องขอถัดไป

5) เมื่อ client ได้รับการตอบกลับ จะทำการอ่านไฟล์เว็บเพ็จที่ได้มาและอ่านURL ของไฟล์รูปภาพที่อยู่ในเว็บเพ็จแล้วส่งการร้องขอผ่านการเชื่อมต่อ

2.5 โปรโตคอลเอฟทีพี (FTP)

เอฟทีพี (File Transfer Protocol) [17] หรือเกณฑ์วิธีถ่ายโอนแฟ้ม เป็นโปรโตคอลเครือข่ายชนิดหนึ่ง ใช้สำหรับแลกเปลี่ยนและจัดการไฟล์บนเครือข่ายทีซีพี/ไอพีเช่นอินเทอร์เน็ต เอฟทีพีถูกสร้างขึ้นด้วยสถาปัตยกรรมแบบระบบรับ-ให้บริการ (client-server) และใช้การเชื่อมต่อสำหรับส่วนข้อมูลและส่วนควบคุมแยกกันระหว่างเครื่องลูกข่ายกับเครื่องแม่ข่าย โปรแกรมประยุกต์เอฟทีพีเริ่มแรกโต้ตอบกันด้วยเครื่องมือรายคำสั่ง สั่งการด้วยไวยากรณ์ที่เป็นมาตรฐาน แต่ก็มีการพัฒนาส่วน

ต่อประสานกราฟิกกับผู้ใช้ขึ้นมาสำหรับระบบปฏิบัติการเดสก์ท็อปที่ใช้กันทุกวันนี้ เอฟทีพียังถูกใช้เป็นส่วนประกอบของโปรแกรมประยุกต์อื่นเพื่อส่งผ่านไฟล์โดยอัตโนมัติสำหรับการทำงานภายในโปรแกรม เราสามารถใช้เอฟทีพีผ่านทางการพิสูจน์ตัวจริงด้วยชื่อผู้ใช้และรหัสผ่าน หรือเข้าถึงด้วยผู้ใช้นิรนาม นอกจากนี้ยังมีทีเอฟทีพี (Trivial File Transfer Protocol) ซึ่งมีลักษณะคล้ายกับเอฟทีพีที่ลดความซับซ้อนลง แต่ไม่สามารถควบคุมให้ทำงานประสานกันได้ และไม่มีการพิสูจน์ตัวจริง

ประวัติของเอฟทีพี [18] นั้น มีการกำหนดลักษณะเฉพาะครั้งแรกใน RFC 114 เมื่อ 16 เมษายน พ.ศ. 2514 จากนั้นถูกเปลี่ยนโดย RFC 765 เมื่อเดือนมิถุนายน พ.ศ. 2523 และต่อมาก็ถูกเปลี่ยนอีกครั้งหนึ่งโดย RFC 959 เมื่อเดือนตุลาคม พ.ศ. 2528 ซึ่งเป็นรุ่นที่ใช้กันอยู่ในปัจจุบัน มีมาตรฐานอีกจำนวนหนึ่งที่พยายามเสริมคุณลักษณะเข้าไปในเอกสารขอความเห็นรุ่นดังกล่าว ตัวอย่างเช่น RFC 2228 เมื่อเดือนมิถุนายน พ.ศ. 2540 เสนอให้เพิ่มส่วนขยายสำหรับความปลอดภัย และ RFC 2428 เมื่อเดือนกันยายน พ.ศ. 2541 เพิ่มการรองรับสำหรับไอพีวี6 และกำหนดวิธีการส่งผ่านไฟล์แบบวิธีรับการร้องขอชนิดใหม่

กระบวนการการทำงานของเอฟทีพีเริ่มจากเครื่องลูกข่ายเริ่มต้นสร้างการเชื่อมต่อไปยังเครื่องแม่ข่ายโดยใช้ทีซีพีบนพอร์ตหมายเลข 21 การเชื่อมต่อนี้คือ การเชื่อมต่อส่วนควบคุม ซึ่งจะเปิดอยู่ตลอดเวลาขณะที่มีการใช้งาน หลังจากนั้น การเชื่อมต่อส่วนข้อมูล บนพอร์ตหมายเลข 20 จะถูกสร้างขึ้นตามความจำเป็นเพื่อส่งผ่านข้อมูลไฟล์ คำสั่งที่ส่งโดยเครื่องลูกข่ายไปยังส่วนควบคุมมีรูปแบบเป็นข้อความแอสกี และจบคำสั่งด้วย CRLF (อักขระปัดแคร่ตามด้วยอักขระป้อนบรรทัด) ตัวอย่างเช่น RETR filename เป็นคำสั่งรับข้อมูลไฟล์ที่ต้องการจากเครื่องแม่ข่ายมายังเครื่องลูกข่าย หลังจากเครื่องแม่ข่ายได้รับคำสั่งแล้ว จะตอบกลับด้วยรหัสสถานภาพเป็นตัวเลขสามหลักพร้อมกับข้อความแอสกีถ้ามี บนการเชื่อมต่อส่วนควบคุม ตัวอย่างเช่น 200 หรือ 200 OK หมายความว่าคำสั่งล่าสุดสำเร็จผล การส่งผ่านไฟล์บนการเชื่อมต่อส่วนข้อมูลที่กำลังดำเนินอยู่สามารถยุติลงได้ด้วยการส่งคำสั่งให้หยุดไปบนการเชื่อมต่อส่วนควบคุม เอฟทีพีสามารถทำงานได้ใน วิธีส่งการร้องขอ (active mode) และ วิธีรับการร้องขอ (passive mode) ซึ่งเป็นการเลือกว่าให้จัดการการเชื่อมต่อที่สองอย่างไร ด้วยวิธีส่งการร้องขอ เครื่องลูกข่ายจะส่งหมายเลขไอพีและพอร์ตที่ต้องการใช้ส่งผ่านข้อมูลให้กับเครื่องแม่ข่าย จากนั้นเครื่องแม่ข่ายจะเปิดการเชื่อมต่อนั้นกลับมา ในขณะที่วิธีรับการร้องขอ เครื่องแม่ข่ายจะส่งหมายเลขไอพีและพอร์ตให้กับเครื่องลูกข่ายก่อน จากนั้นเครื่องลูกข่ายจะสร้างการเชื่อมต่อดังกล่าว (แนวคิดตรงข้ามกับวิธีส่งการร้องขอ) วิธีรับการร้องขอถูกคิดค้นขึ้นมาเพื่อใช้ในกรณีเครื่องลูกข่ายตั้งอยู่หลังไฟร์วอลล์ และไม่สามารถรับการเชื่อมต่อทีซีพีที่ไม่รู้จักจากภายนอกได้ วิธีการทั้งคู่ได้รับการปรับปรุงเมื่อเดือนกันยายน พ.ศ. 2541 เพื่อให้รองรับไอพีวี6 [19] และปรับแต่งวิธีรับการร้องขอทำให้เกิดเป็น วิธีรับการร้องขอแบบเสริม (extended passive mode) ขึ้นมาขณะที่ส่งผ่านข้อมูลไปบนเครือข่าย การแสดงออกของข้อมูลสามารถใช้ได้สี่อย่าง ซึ่งมีเพียงสองชนิดที่ใช้กันโดยทั่วไป วิธีข้อมูลแอสกี ใช้สำหรับข้อมูลชนิดข้อความล้วนเท่านั้น (หากใช้กับข้อมูลชนิดอื่นจะทำให้ไฟล์เสีย) วิธีข้อมูลไบนารี เครื่องที่ส่งข้อมูลจะส่งไปทีละไบต์ และเครื่องที่รับข้อมูลจะรับเป็นกระแสข้อมูลไบต์ (bytestream) มาตรฐานเอฟทีพีเรียกวิธีนี้ว่า วิธีข้อมูลอิมเมจ ส่วนที่เหลืออีกสองชนิดคือ วิธีข้อมูลเอบซีดิก และ วิธีข้อมูลไฟล์เฉพาะที่ ถูกยกเลิกการใช้งานไปแล้ว สำหรับไฟล์ข้อความล้วน เราสามารถเลือกการควบคุมรูปแบบและโครงสร้างการบันทึกที่แตกต่างกันได้ แม้ว่าคุณลักษณะเหล่านี้

แทบจะไม่ได้ใช้ในปัจจุบัน วิธีการส่งผ่านข้อมูลต่าง ๆ เหล่านี้สามารถเลือกใช้ได้ตามต้องการ แต่วิธีการปริยายที่ใช้กันในปัจจุบันจะเป็นการส่งกระแสข้อมูลเสมอ

ด้านความปลอดภัยของเอฟทีพี ลักษณะเฉพาะเริ่มแรกของเอฟทีพีใช้วิธีการส่งผ่านไฟล์ที่ไม่มีการรักษาความปลอดภัย เพราะไม่มีวิธีการใดที่ระบุการส่งผ่านแบบเข้ารหัสข้อมูล หมายความว่าภายใต้การกำหนดค่าเครือข่ายส่วนใหญ่ ชื่อผู้ใช้ รหัสผ่าน คำสั่งเอฟทีพี และไฟล์ที่ส่งผ่าน สามารถถูกดักจับได้โดยใครก็ตามที่อยู่บนเครือข่ายเดียวกันด้วยตัวดักจับกลุ่มข้อมูล (packet sniffer) สิ่งนี้เป็นปัญหาหนึ่งของโพรโทคอลอินเทอร์เน็ตโดยทั่วไปเช่น เอชทีทีพี เอสเอ็มทีพี เทลเน็ต เป็นต้น จึงเกิดการคิดค้นเอสเอสแอลเพื่อการเข้ารหัสขึ้นมาใช้ การแก้ปัญหาความปลอดภัยนี้คือใช้ เอสเอฟทีพี (SSH File Transfer Protocol) [20] หรือ เอฟทีพีเอส (FTP over SSL) ซึ่งเพิ่มการเข้ารหัสด้วยเอสเอสแอล (หรือทีแอลเอส) ไปบนเอฟทีพีธรรมดา ตามที่ระบุไว้ใน RFC 4217

เครื่องแม่ข่ายที่ให้บริการเอฟทีพีอาจมีการเพิ่มระดับการเข้าถึงโดยผู้ใช้นิรนาม(anonymous FTP) นั่นคือไม่ต้องระบุตัวตนกับเครื่องแม่ข่าย โดยทั่วไปผู้ใช้ต้องล็อกอินเข้าสู่บริการด้วยชื่อบัญชี anonymous และเครื่องแม่ข่ายมักจะร้องขอให้ใส่รหัสผ่านเป็นที่อยู่อีเมล์แทน ถึงกระนั้นก็ตามบริการเอฟทีพีไม่สามารถตรวจสอบว่าที่อยู่อีเมล์นั้นมีตัวตนอยู่จริงหรือเป็นของผู้ใช้จริงหรือไม่ โปรแกรมลูกข่ายเอฟทีพีสมัยใหม่มักจะซ่อนกระบวนการล็อกอินแบบนิรนามจากผู้ใช้ และป้อนข้อมูลหลอก ๆ เป็นรหัสผ่าน (เนื่องจากโปรแกรมอาจไม่สามารถรับรู้ที่อยู่อีเมล์ของผู้ใช้ได้) โพรโทคอลโกเฟอร์ (Gopher) เป็นทางเลือกอีกทางหนึ่งเพื่อการเข้าถึงเอฟทีพีของผู้ใช้นิรนาม เช่นเดียวกับทีเอฟทีพีและเอฟเอสพี (File Service Protocol)

เมื่อการเข้าถึงเอฟทีพีถูกจำกัด บริการเอฟทีพีระยะไกล (เอฟทีพีเมล) สามารถใช้งานแทนได้ เพื่อแก้ปัญหานี้ อีเมล์ที่บรรจุคำสั่งเอฟทีพีที่สร้างขึ้นจะถูกส่งไปยังเครื่องให้บริการเอฟทีพีระยะไกล ซึ่งเครื่องนั้นเป็นเมล์เซิร์ฟเวอร์ที่สามารถแจงส่วนอีเมล์ที่รับมาแล้วดำเนินการคำสั่งเอฟทีพีได้ และส่งกลับข้อมูลใด ๆ ที่ดาวน์โหลดไปทางอีเมล์เป็นไฟล์แนบ วิธีนี้มีความยืดหยุ่นน้อยกว่าการใช้โปรแกรมลูกข่ายเอฟทีพี เพราะไม่สามารถแสดงรายการไดเรกทอรีหรือปรับแต่งคำสั่งได้อย่างทันใจ และอาจเกิดปัญหาไฟล์แนบที่มีขนาดใหญ่ไม่สามารถส่งผ่านไปถึงผู้รับ เนื่องจากผู้ใช้อินเทอร์เน็ตทุกวันนี้สามารถเข้าถึงเอฟทีพีได้โดยตรงอยู่แล้ว กระบวนการเหล่านี้จึงไม่มีการใช้อีกต่อไป เว็บเบราว์เซอร์และตัวจัดการไฟล์รุ่นใหม่ ๆ ส่วนใหญ่สามารถติดต่อกับเครื่องให้บริการเอฟทีพีได้ แม้ว่าอาจไม่มีการรองรับส่วนขยายโปรโตคอลเช่นเอฟทีพีเอส การใช้เว็บเบราว์เซอร์และตัวจัดการไฟล์สามารถจัดดำเนินการไฟล์ระยะไกลบนเอฟทีพี ด้วยส่วนติดต่อที่คล้ายกับระบบไฟล์แบบเฉพาะที่ และยังสามารถกระทำได้โดยป้อนยูอาร์แอลของเอฟทีพีในรูปแบบนี้

2.6 พรอกซี่เซิร์ฟเวอร์ (Proxy Server)

ในเครือข่ายคอมพิวเตอร์ พรอกซี่เซิร์ฟเวอร์ (Proxy Server) [21-23] หรือเรียกโดยย่อว่าพรอกซี่ คือเครื่องเซิร์ฟเวอร์หรือเครื่องแม่ข่าย (ระบบคอมพิวเตอร์หรือโปรแกรมประยุกต์) ที่ทำงานโดยการเป็นตัวกลางในการหาข้อมูลตามคำขอของเครื่องลูกข่ายจากเซิร์ฟเวอร์อื่นๆ กล่าวคือเครื่องลูกข่ายเชื่อมต่อไปที่ พรอกซี่เซิร์ฟเวอร์เพื่อขอใช้งานบางบริการ เช่น ไฟล์ การเชื่อมต่อ เว็บเพ็จ หรือทรัพยากรต่าง ๆ จากเซิร์ฟเวอร์อื่น จากนั้น พรอกซี่เซิร์ฟเวอร์จะทำการคัดกรองด้วยกฎที่ตั้ง

ตัวอย่างเช่น คัดกรองจาก หมายเลขไอพี, Protocol หลังจากนั้นถ้าการขอผ่านการคัดกรอง พรอกซี่เซิร์ฟเวอร์จะจัดหาข้อมูลตามคำร้องขอจากเซิร์ฟเวอร์อื่นแทนเครื่องลูกข่าย พรอกซี่เซิร์ฟเวอร์มีสองจุดประสงค์คือ เพื่อให้เครื่องลูกข่ายซ่อนตัว (โดยส่วนใหญ่ เพื่อความปอดภัย) เพื่อความเร็วของการใช้บริการที่เพิ่มขึ้น โดยการเก็บเว็บเพ็จจากเว็บเซิร์ฟเวอร์ พรอกซี่เซิร์ฟเวอร์ที่ไม่มีการเปลี่ยนแปลงการขอและการตอบกลับเรียกว่า Gateway หรือในบางครั้ง tunneling proxy โดยพรอกซี่เซิร์ฟเวอร์ถูกตั้งค่าให้ใช้งานได้ตั้งแต่ 1 อย่างหรือมากกว่า ดังนี้

2.6.1 Caching proxy server [24] ใช้เร่งความเร็วโดยการเก็บข้อมูลจากการเรียกใช้งานครั้งครั้งก่อนจากเครื่องลูกข่าย Caching proxy เก็บสำรองสำรองข้อมูลที่ถูกร้องขอบ่อย ๆ ทำให้องค์กรขนาดใหญ่ลด upstream bandwidth และค่าใช้จ่าย ในขณะเดียวกันเพิ่มความสามารถขององค์กร โดยส่วนมากหน่วย ISP ธุรกิจขนาดใหญ่ และมหาวิทยาลัยจะมี Caching Proxy

ข้อสำคัญของพรอกซี่เซิร์ฟเวอร์อีกประการหนึ่งคือทำให้ประหยัดค่าใช้จ่าย ในหนึ่งองค์กรอาจมีหลายระบบในเครือข่าย หรือในความควบคุม บนเครื่องเซิร์ฟเวอร์เพียงตัวเดียวสามารถแบ่งแยกการเชื่อมต่อสู่อินเทอร์เน็ตของผู้ใช้ในแต่ละระบบ กล่าวคือ ผู้ใช้ในระบบสามารถเชื่อมต่อไปที่ พรอกซี่เซิร์ฟเวอร์และพรอกซี่เซิร์ฟเวอร์เชื่อมต่อไปที่เซิร์ฟเวอร์หลัก

2.6.2 Web proxy เป็นพรอกซี่เซิร์ฟเวอร์ที่สนใจแต่การเชื่อมโยงบนเวิลด์ไวด์เว็บ เรียกว่า web proxy การทำงานหลักของมันคือการเป็น web cache, proxy โปรแกรมส่วนใหญ่ปฏิเสธบาง URL ใน Blacklist ภายใต้เงื่อนไขการคัดกรอง นิยมใช้ในบริษัท สถานศึกษา ห้องสมุด หรือที่ใดก็ตามที่ทำการคัดกรอง

2.6.3 Hostile proxy บางครั้งพรอกซี่เซิร์ฟเวอร์อาจถูกใช้ในจุดประสงค์ที่ไม่ดี เพื่อดักเก็บข้อมูลที่ส่งผ่านระหว่างเครื่องลูกข่ายกับเว็บเซิร์ฟเวอร์ สามารถเก็บข้อมูลในการกรอกแบบฟอร์มต่าง ๆ บนเว็บ เช่น รหัสผ่านสำหรับอีเมล์หรือธนาคารออนไลน์ ทั้งนี้สามารถใช้ SSL เพื่อความปลอดภัย

2.7 ไฟร์วอลล์ (Firewall)

Firewall [25] นั้นหากจะแปลตรงตัวจะแปลว่ากำแพงไฟ แต่ที่จริงแล้ว firewall เป็นกำแพงที่มีไว้เพื่อป้องกันไฟโดยที่ตัวมันเองนั้นไม่ใช่ไฟตามคำแปล firewall ในสิ่งปลูกสร้างต่างๆนั้นจะทำด้วยอิฐเพื่อแยกส่วนต่างๆของสิ่งปลูกสร้างออกจากกันเพื่อที่ว่าในเวลาไฟไหม้ไฟจะได้ไม่ลามไปทั่วสิ่งปลูกสร้างนั้นๆ หรือ Firewall ในรถยนต์ก็จะเป็นแผ่นโลหะใช้แยกส่วนของเครื่องยนต์และส่วนของที่นั่งของผู้โดยสารออกจากกันในเครือข่าย Internet นั้น firewall อาจถูกใช้สำหรับป้องกันไม่ให้ “ไฟ” จากเครือข่าย Internet ภายนอกลามเข้ามาภายในเครือข่ายภายในส่วนตัวได้หรืออาจถูกใช้เพื่อป้องกันไม่ให้ผู้ใช้ในเครือข่ายออกไปโดน “ไฟ” ในเครือข่ายอินเทอร์เน็ตภายนอกได้

ตามคำจำกัดความแล้ว firewall หมายความถึง ระบบหนึ่งหรือกลุ่มของระบบที่บังคับใช้นโยบายการควบคุมการเข้าถึงของระหว่างเครือข่ายสองเครือข่าย โดยที่วิธีการกระทำนั้นก็จะแตกต่างกันไปแล้วแต่ระบบ แต่โดยหลักการแล้วเราสามารถมอง firewall ได้ว่าประกอบด้วยกลไกสองส่วน โดยส่วนแรกมีหน้าที่ในการกั้น traffic และส่วนที่สองมีหน้าที่ในการปล่อย traffic ให้ผ่านไปได้

Firewall โดยทั่วไปจะถูกแบ่งออกเป็น 2 ประเภท คือ firewall ระดับ network (network level firewall) และ firewall ระดับ application (application level firewall) [26] ก่อนที่

firewall ระดับ network จะตัดสินใจยอมให้ traffic ใดผ่านนั้นจะดูที่ address ผู้ส่งและผู้รับ และ port ในแต่ละ IP packet เมื่อพิจารณาแล้วเห็นว่า traffic สามารถผ่านไปได้ก็จะ route traffic ผ่านตัวมันไปโดยตรง router โดยทั่วไปแล้วก็จะถือว่าเป็น firewall ระดับ network ชนิดหนึ่ง firewall ประเภทนี้จะมีความเร็วสูงและจะ transparent ต่อผู้ใช้ (คือผู้ใช้มองไม่เห็นความแตกต่างระหว่างระบบที่ไม่มี firewall กับระบบที่มี firewall ระดับ network อยู่) การที่จะใช้ firewall ประเภทนี้โดยมากผู้ใช้จะต้องมี IP block (ของจริง) ของตนเอง

Firewall ระดับ application นั้นโดยทั่วไปก็คือ host ที่ run proxy server อยู่ firewall ประเภทนี้สามารถให้รายงานการ audit ได้อย่างละเอียดและสามารถบังคับใช้นโยบายความปลอดภัยได้มากกว่า firewall ระดับ network แต่ firewall ประเภทนี้ก็จะมีความ transparent น้อยกว่า firewall ระดับ network โดยที่ผู้ใช้จะต้องตั้งเครื่องของตนให้ใช้กับ firewall ประเภทนี้ได้นอกจากนี้ firewall ประเภทนี้จะมีความเร็วน้อยกว่า firewall ระดับ network บางแหล่งจะกล่าวถึง firewall ประเภทที่สามคือประเภท stateful inspection filtering ซึ่งใช้การพิจารณาเนื้อหาของ packets ก่อนๆในการที่จะตัดสินใจให้ packet ที่กำลังพิจารณาอยู่เข้ามา

2.7.1 ขีดความสามารถของ firewall ทั่วๆไปนั้นมีดังต่อไปนี้

1) ป้องกันการล็อกอินที่ไม่ได้รับอนุญาตที่มาจากภายนอกเครือข่าย

2) ปิดกั้นไม่ให้ traffic จากนอกเครือข่ายเข้ามาภายในเครือข่ายแต่ก็ยอมให้ผู้ที่อยู่ภายในเครือข่ายสามารถติดต่อกับโลกภายนอกได้

3) เป็นจุดรวมสำหรับการรักษาความปลอดภัยและการทำ audit (เปรียบเสมือนจุดรับแรงกระแทกหรือ “choke” ของเครือข่าย)

2.7.2 ข้อจำกัดของ firewall มีดังนี้

1) firewall ไม่สามารถป้องกันการโจมตีที่ไม่ได้กระทำผ่าน firewall (เช่น การโจมตีจากภายในเครือข่ายเอง)

2) ไม่สามารถป้องกันการโจมตีที่เข้ามากับ application protocols ต่างๆ (เรียกว่าการ tunneling) หรือกับโปรแกรมไคลเอนต์ที่มีความล่อแหลมและถูกดัดแปลงให้กระทำการโจมตีได้ (โปรแกรมที่ถูกทำให้เป็น Trojan horse)

3) ไม่สามารถป้องกัน virus ได้อย่างมีประสิทธิภาพเนื่องจากจำนวน virus มีอยู่มากมาย จึงจะเป็นการยากมากที่ firewall จะสามารถตรวจจับ pattern ของ virus ทั้งหมดได้

ถึงแม้ว่า firewall จะเป็นเครื่องมือที่สามารถนำมาใช้ป้องกันการโจมตีจากภายนอกเครือข่ายได้อย่างมีประสิทธิภาพ การที่จะใช้ firewall ให้ได้ประโยชน์สูงสุดนั้นจะขึ้นอยู่กับนโยบายความปลอดภัยโดยรวมขององค์กรด้วย

2.8 แบนด์วิดท์ (Bandwidth)

สำหรับความหมายของคำว่าแบนด์วิดท์ (Bandwidth) เป็นคำที่ใช้วัดความเร็วในการส่งข้อมูลของอินเทอร์เน็ต หรือจะเรียกอีกอย่างว่าเป็นความกว้างของช่องสัญญาณที่ใช้ในการสื่อสารผ่านตัวกลางซึ่งก็คือระยะห่างระหว่างคลื่นสัญญาณความถี่สูงสุดและความถี่ต่ำสุดที่ใช้เป็นช่องทางของการสื่อสารโดยแบนด์วิดท์ของระบบการสื่อสารบนเครือข่ายนั้นมี 2 รูปแบบ คือ

1) Bandwidth in Hertz เป็นช่วงความถี่ที่สารมารถผ่านช่องสื่อสารได้โดยมีหน่วยการนับที่เรียกว่า Hertz (Hz) ซึ่ง 1 Hz คือสัญญาณที่เกิดขึ้น 1 ครั้ง ในเวลา 1 วินาที และในระบบการสื่อสารจะมีทั้ง KHz (KiloHertz), MHz (MegaHertz) และ GHz (GigaHertz) เช่น แบนด์วิดท์ของการใช้บริการสายโทรศัพท์มีขนาดเป็น 4 KHz เป็นต้น

2) Bandwidth in Bits per seconds เป็นส่วนของ Bandwidth ที่สามารถใช้ค่าอ้างอิงเป็นจำนวนบิตต่อวินาทีในช่องทางการสื่อสารหรือเป็นความสามารถในการส่งข้อมูลบนเครือข่ายเช่น แบนด์วิดท์ของเครือข่าย Gigabit Ethernet มีค่าสูงถึง 1000 Mbps ซึ่งความหมายก็คือระบบเครือข่ายนั้นสามารถมีอัตราการส่งข้อมูลได้ถึง 1000 Mbps

สำหรับความสัมพันธ์ระหว่างแบนด์วิดท์ในเฮิร์ทและในบิตต่อวินาทีนั้น โดยพื้นฐานก็คือเมื่อมีการเพิ่มประสิทธิภาพของเครือข่ายโดยการเพิ่มแบนด์วิดท์ในเฮิร์ท ก็จะหมายถึงการเพิ่มประสิทธิภาพของแบนด์วิดท์ในบิตต่อวินาทีด้วย ในความหมายทั่วไปแบนด์วิดท์เป็นสัดส่วนโดยตรงของจำนวนข้อมูลทั้งหมดที่ส่งผ่านหรือรับต่อหน่วยเวลา ในความหมายเชิงคุณภาพ แบนด์วิดท์เป็นสัดส่วนของความซับซ้อนของข้อมูลสำหรับการทำงานของระบบที่รองรับได้เช่น การดาวน์โหลดไฟล์ทุกประเภท รูปภาพในหนึ่งวินาทีใช้แบนด์วิดท์มากกว่าการดาวน์โหลดข้อความในเวลาหนึ่งวินาที ส่วนไฟล์ประเภทเสียงขนาดใหญ่ในโปรแกรมคอมพิวเตอร์และภาพเคลื่อนไหวต้องใช้แบนด์วิดท์มาก การนำเสนอแบบ Virtual reality (VR) และ ภาพแบบ 3 มิติ ชนิด Full-length ใช้ แบนด์วิดท์มากที่สุด

2.8.1 การจัดการ (Bandwidth Management)

Bandwidth Management คือ บริการที่ช่วยในการบริหารจัดการแบนด์วิดท์ของแต่ละแอพพลิเคชั่น (application) เช่น Internet, mail, web, และ application ประเภทอื่นๆ เป็นต้น ให้เป็นไปตามนโยบายของแต่ละหน่วยงานซึ่งสามารถกำหนดหรือเปลี่ยนแปลงได้ตามความเหมาะสม และช่วยให้แอพพลิเคชั่นที่มีความสำคัญต่อการปฏิบัติงานขององค์กรสามารถใช้งานได้อย่างรวดเร็วและเต็มประสิทธิภาพ รวมทั้งเป็นการจำกัดการใช้งานในแอพพลิเคชั่นที่ไม่เป็นประโยชน์อีกด้วย สำหรับลักษณะเด่นของ Bandwidth Control ผู้ใช้งานสามารถควบคุมปริมาณการใช้งานแบนด์วิดท์ของแต่ละแอพพลิเคชั่นให้เป็นไปตามนโยบายของแต่ละหน่วยงาน เช่น การกำหนดปริมาณการใช้งานแบนด์วิดท์ของแอพพลิเคชั่นในบางช่วงเวลาตามองค์กรได้การกำหนดเพื่อให้ใช้ประโยชน์ของการใช้แบนด์วิดท์ได้คุ้มค่ามากที่สุด

2.8.2 สาเหตุของการจัดการ Bandwidth

2.8.2.1 เนื่องจากการเชื่อมต่อไปนอกองค์กรมีต้นทุนสูง จึงต้องมีการดำเนินการบริหารจัดการเพื่อให้เกิดความคุ้มค่ามากที่สุด

2.8.2.2 เพื่อจัดลำดับความสำคัญของข้อมูล (Priority)

2.8.2.3 เพื่อลดความรุนแรงจากการโจมตีเครือข่ายแบบ DoS

2.8.2.4 เพื่อนำมาซึ่งการจัดตั้งนโยบายการใช้เครือข่ายอย่างมีประสิทธิภาพ

(Web. การจัดการแบนด์วิดท์. [ออนไลน์]. เข้าถึงได้จาก : http://web.bsru.ac.th/~jumpot/Article/Bandwidth.htm (วันที่ค้นหาข้อมูล: 23 กรกฎาคม 2554).

2.8.3 SoftPerfect Bandwidth Manager

เป็นเครื่องมือบริหารจัดการปริมาณการใช้แบนด์วิดท์สำหรับระบบปฏิบัติการวินโดวส์ 2000, วินโดวส์ XP, วินโดวส์ 2000 Server และวินโดวส์ 2003 ทำหน้าที่ในการครบคุมแบนด์วิดท์และคุณภาพการบริการโดยจะยึดกฎการจัดลำดับ ซึ่งการกำหนดกฎจะถูกสร้างโดยระบุการทำงานถึงไอพี, โพรโตคอล,พอร์ต โดยไม่กระทบต่อโครงสร้างเครือข่าย สามารถกำหนดหรือ ระบุกฎโดยใช้กับ IP และ MAC Address, Protocols, Port (สำหรับ TCP และ UDP) และ Network Interfaces และมีหน้าต่างที่ใช้สำหรับตรวจดูปริมาณการใช้เครือข่ายสำหรับกฎนั้น ๆ(SB. SoftPerfect Bandwidth Manager. [ออนไลน์].เข้าถึงได้จาก:
http://www.easyfp.com/bandwidth-manager/index.html (วันที่ค้นหาข้อมูล: 23 กรกฎาคม 2554).

2.9 งานวิจัยที่เกี่ยวข้อง

2.9.1 ชัยวัฒน์ นิลวรรณ (2549) [4] พัฒนาระบบจัดการสควิดพรอกซี่โดยผ่านเว็บอินเตอร์เฟส ซึ่งใช้วิธีบริหารจัดการ การทำงานของผู้ดูแลระบบผ่านทางหน้าเว็บเพจ ซึ่งพัฒนาด้วยภาษาพีเอชพี การทำงานของสควิดพรอกซี่ติดตั้งอยู่บนระบบปฏิบัติการลินุกซ์เซิร์ฟเวอร์ การพัฒนาระบบจัดการสควิดพรอกซี่โพลีซีโดยผ่านเว็บอินเตอร์เฟส แบ่งออกเป็น 2 ส่วนหลักคือ ส่วนของการจัดการกับแฟ้มข้อมูลหลักของสควิดพรอกซี่ และส่วนของการจัดการกับกลุ่มของข้อมูลที่เป็นเงื่อนไข โดยกลุ่มของข้อมูลแต่ละกลุ่มจะถูกมองเหมือนกับเป็นอ็อพเจ็ค แต่ละอ็อพเจ็คจะแยกออกจากกันอย่างอิสระ อ็อพเจ็คแต่ละอ็อพเจ็คจะนำมาประกอบกันตามเงื่อนไขที่ต้องการ เพื่อที่จะให้สควิดพรอกซี่นำไปเป็นส่วนของการฟิลเตอร์ข้อมูลต่างๆ ที่วิ่งผ่านสควิดพรอกซี่ ผลการทดลองเมื่อนำระบบงานที่ได้พัฒนา ไปทำการทดสอบเพื่อหาระดับความพึงพอใจของระบบจากผู้เชี่ยวชาญด้านการดูแลระบบและผู้ดูแลระบบ สามารถสรุปผลการประเมินหาประสิทธิภาพได้ว่าเป็นระบบที่พัฒนาโดยมีประสิทธิภาพอยู่ในระดับดี

ผลการทำงานสรุปได้ว่าการใช้สควิดพรอกซี่มีประสิทธิภาพใช้งานได้ดี แต่มีปัญหาว่าการจัดเก็บข้อมูลของระบบนั้นเป็นการเก็บข้อมูลของเว็บซึ่งเกิดจากการใช้งานเว็บไซต์ทั่วไปเท่านั้นยังไม่มีส่วนที่ช่วยจัดการปัญหาข้อมูลที่เกิดจากการดาวน์โหลดข้อมูลแต่อย่างใด

2.9.2 กลุ่มนักวิจัยหน่วยปฏิบัติการเทคโนโลยีเครือข่ายศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติหรือเนคเทค นำเสนองานวิจัยการบริหารจัดการแบนด์วิท์ (Bandwidth Management) รายงานว่าเมื่ออินเทอร์เน็ตเข้ามามีบทบาทในชีวิตประจำวันมากขึ้นส่งผลให้บริการอินเทอร์เน็ตความเร็วสูง(ADSL) เริ่มเข้าถึงประชาชนในพื้นที่ต่างๆ ง่ายขึ้น เพราะการให้บริการอินเทอร์เน็ตความเร็วสูง หรือบรอดแบนด์ ตัวผู้ให้บริการอินเทอร์เน็ตหรือไอเอสพีแต่ละรายต่างต้องแข่งขันกันสูง เพื่อทำให้ค่าบริการถูกอันเป็นประโยชน์กับผู้รับโภคที่จะได้ใช้ของดีราคาถูก และทำให้ใครๆก็สามารถใช้ได้ไม่ว่าจะเป็นหน่วยงานภาครัฐ รัฐวิสาหกิจ บริษัทเอกชนขนาดใหญ่ หรือบริษัทขนาดกลางและขนาดย่อม สถาบันการศึกษาและศูนย์การเรียนรู้ชุมชนต่างๆ ก็มีเครือข่ายคอมพิวเตอร์หรือระบบเป็นของตัวเองได้ แต่ทว่าความท้าทายที่ตามมาจากการมีเครือข่ายใช้งานตามหน่วยงานและชุมชนทั่วไป คือ ทำอย่างไรจึงจะบริหารจัดการทรัพยากรในเครือข่ายที่มีอยู่ ให้ใช้งานได้อย่างเต็มประสิทธิภาพ ทั้งเรื่องของระบบความปลอดภัย การบริหารจัดการแบนด์วิท์ และการบำรุงรักษา

เนื่องจากปัญหาที่พบบ่อยคือ หน่วยงานขนาดกลางและขนาดเล็กเช่น โรงเรียนและชุมชน มักขาดบุคลากรที่มีความรู้ความสามารถในการดูแลจัดการเครือข่ายและเมื่อมีปัญหาเกิดขึ้นก็ไม่ทราบสาเหตุและไม่สามารถแก้ไขเองได้ ต้องรอผู้เชี่ยวชาญ หรือวิศวกรไอทีมาแก้ไขให้ ทำให้เครือข่ายที่มีใช้งานได้ไม่เต็มที่หรือถูกปล่อยทิ้งไว้ไม่ได้นำมาใช้งาน

กลุ่มนักวิจัยหน่วยปฏิบัติการเทคโนโลยีเครือข่ายศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติหรือเนคเทคเห็นว่าปัญหานี้มีความสำคัญมาก เพราะเครือข่ายขนาดกลางและขนาดเล็กในประเทศมีแนวโน้มเพิ่มมากขึ้นเนื่องด้วยนโยบายรัฐบาลอิเล็กทรอนิกส์ หรือ E-Government ที่บังคับให้ทุกหน่วยงานราชการ มีเครือข่ายคอมพิวเตอร์เชื่อมต่อถึงกันรวมถึงต้องมีระบบอีเมล์ภายในเป็นของตัวเอง อีกทั้งนโยบายกระทรวงศึกษาธิการ ที่ให้งบประมาณสนับสนุนการเชื่อมต่อบรอดแบนด์ไปทุกโรงเรียน รวมถึงนโยบายกระจายอำนาจสู่ท้องถิ่น ที่จัดสรรงบประมาณให้องค์การบริหารส่วนจังหวัด ส่วนอำเภอ และส่วนตำบลไสร้างสาธารณูปโภคขั้นพื้นฐานเองและเครือข่ายอินเทอร์เน็ตชุมชน ก็เป็นหนึ่งในโครงสร้างพื้นฐานสำคัญ

ดร.พนิตา พงษ์ไพบูลย์ นักวิจัยหน่วยปฏิบัติการการวิจัยเทคโนโลยีเครือข่าย NTL เนคเทคกล่าวว่า จากที่ทีมงานวิจัยของเนคเทคได้สำรวจสถานภาพความพร้อมในการใช้งานคอมพิวเตอร์ และอินเทอร์เน็ตของโรงเรียน จากบุคลากรของโรงเรียนจากภูมิภาคต่างๆ ทั่วประเทศ 112 คน จาก 105 โรง เมื่อช่วงเดือน มิ.ย.-ส.ค. 2550 โดยส่วนมากเป็นโรงเรียนของรัฐบาล ที่เคยเข้าร่วมโครงการอบรมใช้งานโอเพ่นซอร์สของเนคเทค เพื่อสำรวจความต้องการของผู้ใช้รวมถึงศึกษาปัญหาด้านเครือข่ายอุปกรณ์ไอที ความพร้อมของโรงเรียนในการรับบริการ หรือแอพพลิเคชั่น ต่างๆ ทั้งนี้เพื่อนำผลการศึกษาที่ได้ไปใช้ในการพัฒนาโปรแกรมที่เหมาะสม และตรงต่อความต้องการของผู้ใช้ นอกจากนี้ยังใช้ข้อมูลที่ได้เป็นข้อมูลพื้นฐานในการพัฒนาเทคโนโลยีของโรงเรียน

รายงานวิจัยครั้งนี้ระบุว่า จากกลุ่มตัวอย่างทั้งหมด 105 โรงเรียน ส่วนมากมีความพร้อมขั้นพื้นฐานทางด้านคอมพิวเตอร์คือ มีพีซีโดยเฉลี่ย 72 เครื่องต่อโรงเรียน และอัตราส่วนพีซี 1 เครื่องต่อนักเรียน 15 คน มีบุคลากรที่มีความรู้และประสบการณ์ในการเรียนการสอนคอมพิวเตอร์โดยเฉลี่ย 1-3 คนต่อโรงเรียน มีการเรียนการสอนวิชาคอมพิวเตอร์ มีการใช้คอมพิวเตอร์ประกอบการเรียนในวิชาอื่นๆ ในทุกระดับชั้น อย่างไรก็ตามโปรแกรมที่ทำการสอนส่วนมากยังคงเป็นโปรแกรมพื้นฐาน เช่น ไมโครซอฟท์ออฟฟิศ อะโดบีโฟโต้ช็อป และการเสิร์ชข้อมูลทางอินเทอร์เน็ต ขณะที่พีซีของโรงเรียนใช้ระบบปฏิบัติการตระกูลไมโครซอฟท์ วินโดวส์ ถึง 90%

ส่วนความพร้อมด้านเครือข่ายของโรงเรียนพบว่า ทุกโรงเรียนที่ตอบแบบสำรวจมีการติดตั้งระบบอินเทอร์เน็ต โดยส่วนมากจะเชื่อมต่อผ่านระบบอินเทอร์เน็ตความเร็วสูง (ADSL) จานดาวเทียมไอพีสตาร์ (IP Star) และวงจรเช่า (Leased line) ด้านความเร็วในการเชื่อมต่ออินเทอร์เน็ตหรือแบนดวิท์อยู่ที่ระดับ 512 kbps – 1 Mbps เป็นหลัก นอกจากนี้กว่า 60% ของผู้ตอบแบบสำรวจรายงานว่ามีการติดตั้งและใช้งานเซิร์ฟเวอร์ภายใน โรงเรียน เพื่อให้บริการ Web DHCP และ FTP เป็นต้น ส่วนการใช้งานเครือข่าย พบว่าโรงเรียนส่วนใหญ่มีนโยบายจำกัดช่วงเวลาการใช้งานของนักเรียน จำกัดการเข้าถึงเว็บไซต์ที่ไม่เหมาะสม และห้ามเล่นเกมส์ อย่างไรก็ตามยังมีโรงเรียนบางส่วนที่อนุญาตให้นักเรียนใช้งานได้ตามอิสระ ปัญหาที่ตามมาจากการใช้งานเครือข่ายที่โรงเรียนเห็นว่าสำคัญที่สุด คือปัญหาการติดไวรัสคอมพิวเตอร์รองลงมาเป็นปัญหาอินเทอร์เน็ตช้า ปัญหาอุปกรณ์เสีย

บ่อย และปัญหาแบนด์วิทไม่เพียงพอต่อการใช้งานของครูและนักเรียน เมื่อถามถึงความต้องการใช้งานซอฟต์แวร์ เพื่อช่วยควบคุมและดูแลระบบคอมพิวเตอร์และเครือข่าย สิ่งที่โรงเรียนต้องการมากที่สุดคือระบบป้องกันไวรัสคอมพิวเตอร์รองลงมาเป็น ระบบควบคุมการเข้าถึงเว็บไซต์ที่ไม่เหมาะสม ระบบแจ้งเตือนปัญหาพร้อมขั้นตอนการแก้ไขปัญหาและ ระบบรายงานประเภทของเว็บไซต์และโปรแกรมที่ใช้งานอินเทอร์เน็ต นักวิจัยของเนคเทคเล่าให้ฟังว่าจากประเด็นปัญหาที่สำรวจพบ “โครงการวิจัยระบบบริหารจัดการ เครือข่ายอัจฉริยะ” จึงเกิดขึ้นเพื่อช่วยแก้ปัญหาดังกล่าวข้างต้น โดยการวิจัยและพัฒนาระบบที่บริหารจัด การเครือข่ายได้อย่างอัตโนมัติ จุดมุ่งหมายสำคัญของโครงการนี้คือการลดภาระของผู้ดูแลระบบ โดย ลดขั้นตอนการจัดการเครือข่ายบางส่วนที่ต้องทำเป็นประจำ เช่น การตรวจสอบสถานะขอเซิร์ฟเวอร์ให้เกิดขึ้นโดยอัตโนมัติ และลดขั้นตอนที่ยุ่งยากซับซ้อนลง นอกจากนี้ระบบบริหารจัดการเครือข่ายดังกล่าว ควรเป็นเสมือนผู้เชี่ยวชาญที่แจ้งเตือนและแนะนำวิธีแก้ปัญหาแก่ผู้ดูแลระบบ

ดร.พนิตา อธิบายว่าสาหรับระบบบริหารจัดการเครือข่ายอัจฉริยะนี้จะพัฒนาขึ้นบนพื้นฐานของซอฟต์แวร์โอเพ่นซอร์ส โดยมีส่วนประกอบหลักสามส่วน คือ 1.ระบบดูแลตรวจสอบสถานะของเครือข่ายและบริการ โดยพัฒนาต่อยอดจากซอฟต์แวร์โอเพ่นซอร์สที่ชื่อโปรแกรม Nagios มีความสามารถในการตรวจวิเคราะห์สถานะการทำงาน และทรัพยากรบน อุปกรณ์เครือข่ายต่างๆ และยังสามารถแจ้งเตือนผู้ดูแลระบบ ในกรณีที่เกิดความผิดพลาดขึ้นกับอุปกรณ์ เหล่านั้น 2.ระบบตรวจวัดและวิเคราะห์การใช้งานบนเครือข่าย(Traffic monitoring and classification)โดยพัฒนาต่อยอดจากซอฟต์แวร์โอเพ่นซอร์สที่ชื่อโปรแกรม ntop ใช้ในการตรวจสอบพฤติกรรมการใช้งานเครือข่ายจำแนกตามชนิดของแอพพลิเคชั่นที่ใช้งานของผู้ใช้แต่ละคน รวมถึงรายงานความผิดปกติที่อาจ เกิดจากการจู่โจมบนเครือข่าย 3.ระบบบริหารจัดการแบนด์วิท์ (Bandwidth manager) พัฒนาบนพื้นฐานของระบบปฏิบัติการใน Linux มีความสามารถควบคุมปริมาณการใช้งานแบนด์วิท์ เข้า-ออก เครือข่าย โดยสามารถควบคุมแบนด์วิท์ และจำกัดการใช้งานอินเทอร์เน็ต จำแนกตามผู้ใช้และตามประเภทของแอพพลิเคชั่น นักวิจัยฯเนคเทค อธิบายเสริมว่าในช่วงแรกของโครงการทีมผู้วิจัยต้องการพัฒนาทั้ง 3 ระบบย่อยในลักษณะ stand-alone ที่เมื่อพัฒนาเสร็จระบบทั้ง 3 จะสามารถไปใช้งานได้จริง โดยไม่จำเป็นต้องพึ่งกัน เหมาะสมสำหรับผู้ดูแลเครือข่ายระดับเล็กที่มีความต้องการเฉพาะทาง ในช่วงที่ 2 ทีมผู้วิจัยจะนำ เอาระบบทั้ง 3 มาประกอบกันเป็นระบบใหญ่ที่ฉลาดมากขึ้นและเพิ่มมูลค่าให้กับทั้งสามระบบย่อย เช่นระบบตรวจวิเคราะห์การใช้งาน สามารถจำแนกชนิดของแอพพลิเคชั่นที่แม่นยำ เพื่อให้ระบบจัดการแบนด์วิท์ ได้ตัดสินใจที่จะควบคุมลำดับเวลาการส่งข้อมูลที่เหมาะสม และข้อมูลการใช้งานเครือข่าย ช่วยให้ระบบตรวจสอบสถานะเครือข่ายเข้าใจถึงสาเหตุความผิดปกติในเครือข่ายและแนะนำวิธีการแก้ปัญหาที่เหมาะสมได้ ทั้งหมดนี้คือความตั้งใจของนักวิจัยคนไทย ที่ต้องการสร้างเทคโนโลยีที่มาจากการพึ่งพาตัวเอง โดยเฉพาะโซลูชั่นด้านเครือข่ายและระบบรักษาความปลอดภัย ที่หากใช้ของต่างประเทศ อุปกรณ์เหล่านี้ก็มีราคาที่ค่อนข้างสูง และต้องการการดูแลรักษาโดยผู้เชี่ยวชาญอยู่เสมอ อีกทั้งยังสอดคล้องกับการใช้งานบรอดแบนด์ในปัจจุบันที่มีผู้ใช้งานกันกว้างขวาง แต่ยังขาดการบริหารจัดการบนเครือข่ายที่ดี ดังนั้นจึงนับเป็นอีกเรื่องที่ควรสนับสนุน และติดตามการพัฒนาเทคโนโลยีด้านเครือข่ายของคนไทย ต่อไป

บทที่ 3
วิธีการดำเนินการวิจัย

ขั้นตอนการพัฒนาระบบเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยระบบปฏิบัติการลินุกซ์ เป็นการทำงานโดยใช้ซอฟท์แวร์หลายชนิดที่มีอยู่แล้วในระบบปฏิบัติการลินุกซ์ รวมถึงระบบเครือข่ายเน็ตเวิร์คพื้นฐานของหน่วยงานซึ่งไม่จำเป็นต้องเพิ่มเติมในเรื่องของฮาร์ดแวร์พิเศษแต่อย่างใด เพียงแต่ต้องมีการศึกษาเอาข้อดีหรือข้อเด่นของซอฟท์แวร์ชนิดต่างๆมาทำการศึกษาและดัดแปลงให้สามารถทำงานร่วมกันได้ โดยแบ่งขั้นตอนการดำเนินงานออกเป็น 4 ขั้นตอน ดังนี้

3.1 ศึกษาและรวบรวมข้อมูลที่จำเป็นในการพัฒนาระบบ

3.2 การวิเคราะห์และออกแบบระบบ

3.3 พัฒนาระบบ

3.4 ทดสอบการทำงาน แก้ไข และปรับปรุงระบบ

3.5 ทดสอบการทำงานด้วยซอฟท์แวร์เฉพาะทาง

3.1 ศึกษาและรวบรวมข้อมูลที่จำเป็นในการพัฒนาระบบ

การศึกษาและรวมรวมข้อมูลสำหรับนำมาใช้ในการพัฒนาระบบเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยการใช้ระบบปฏิบัติการลินุกซ์ นั้น ประกอบด้วยการนำเอาระบบปฏิบัติการลินุกซ์มาใช้เป็นระบบปฏิบัติการหลัก ซึ่งมีความคงทนต่อการใช้งานกับเครือข่ายขนาดใหญ่ได้เป็นอย่างดี มีการใช้ทรัพยากรระบบน้อย และที่สำคัญเป็นโอเพ่นซอร์ส ไม่มีค่าลิขสิทธิ์ใดๆ จึงใช้ได้กับผู้ใช้ในทุกระดับ นอกจากนี้ยังมีการนำเอาซอฟท์แวร์สควิดพรอกซี่ที่มีอยู่แล้วในระบบปฏิบัติการลินุกซ์ซึ่งทำหน้าที่ให้บริการด้านการเข้าถึงอินเทอร์เน็ตให้เกิดความรวดเร็วและลื่นไหลทำหน้าที่เป็นเว็บแคชอยู่แล้วในระดับหนึ่ง นอกจากนั้นยังมีการทำงานของซอฟท์แวร์และไฟล์วอลล์สคริปต์บางส่วนที่ต้องศึกษาเพื่อใช้งานประสานกับสควิดพรอกซี่ในการลดปริมาณข้อมูลการใช้งานอินเทอร์เน็ตจากเดิมที่จัดการโดยสควิดพรอกซี่อย่างเดียวซึ่งยังไม่เป็นที่พึงพอใจ ยังไม่สามารถลดปริมาณข้อมูลและเพิ่มความเร็วการเข้าถึงอินเทอร์เน็ตได้ดีนัก เนื่องจากมีปัจจัยอื่นเข้ามาเกี่ยวข้อง โดยมีส่วนที่ต้องศึกษา ดังนี้

3.1.1 การทำงานของระบบปฏิบัติการลินุกซ์

เนื่องจากลินุกซ์นั้นมีอยู่ด้วยกันหลายตระกูล การทำงานและการคอนฟิกค่าบางอย่างไม่เหมือนกัน ซึ่งผู้ใช้สามารถเลือกใช้ได้ตามความถนัด ในระบบเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยระบบปฏิบัติการลินุกซ์ในครั้งนี้ใช้ระบบปฏิบัติการลินุกซ์ CentOS 5.0 เป็นตระกูลที่มีสภาวะแวดล้อมรวมถึงเครื่องมือติดตั้งที่ใช้งานง่าย ติดตั้งได้อย่างรวดเร็ว ใช้ทรัพยากรของระบบน้อย เหมาะกับหน่วยงานที่มีงบประมาณไม่มาก ซึ่งในการติดตั้งระบบปฏิบัติการลินุกซ์ CentOS นั้นจำเป็นต้องศึกษาการติดตั้งแพ็คเกจที่จำเป็นต้องใช้ เพื่อให้สามารถทำงานร่วมกับระบบสควิดพรอกซี่ และระบบไฟล์วอลล์ที่เป็นส่วนหนึ่งขององค์ประกอบในระบบนี้ และต้องมีการกำหนดค่าการทำงานบางอย่าง

ด้วย เนื่องจากในการติดตั้งลินุกซ์ในเบื้องต้นนั้นจะได้แพ็คเกจต่างๆจำนวนหนึ่งซึ่งอาจไม่เพียงพอหรือแพ็คเกจนั้นอาจเก่าเกินไปไม่ทันสมัยอันเนื่องมาจากช่วงเวลาปัจจุบันอาจมีการออกเวอร์ชั่นของแพ็คเกจบางอย่างที่ใหม่กว่าในแผ่นติดตั้ง จึงต้องมีการกำหนดค่าบางอย่างเพื่อจะทำให้ระบบได้แพ็คเกจที่ดีขึ้น อีกทั้งยังมีเรื่องของความปลอดภัยเนื่องจากเป็นการให้บริการเกี่ยวกับอินเทอร์เน็ต หากระบบหรือแพ็คเกจใดเก่าเกินไปอาจก่อให้ระบบเกิดช่องโหว่ถูกโจมตีจากภายนอกหรือถูกโจมตีด้วยไวรัสได้ รวมไปถึงสควิดพรอกซี่และไฟล์วอลล์ที่อาจทำงานไม่ได้หากไม่มีแพ็คเกจที่ถูกต้องหรือทันสมัยอยู่เสมอ และจากที่ปัญหาที่กล่าวมานั้นสามารถทำการแก้ไขโดยสั่งอัพเดทแพ็คเกจผ่านช่องทางการดาวน์โหลดจากเว็บไซต์ผู้พัฒนาระบบปฏิบัติการลินุกซ์ซึ่งในขั้นตอนการติดตั้งจึงจำเป็นต้องมีการเชื่อมต่ออินเทอร์เน็ตไว้ด้วยเสมอ(ขั้นตอนติดตั้งระบบปฏิบัติการลินุกซ์ในภาคผนวก)

3.1.2 การคอนฟิกค่าที่จำเป็นและการกำหนดโพลิซีของสควิดพรอกซี่

การคอนฟิกค่าการทำงานและกำหนดโพลิซีของสควิดพรอกซีถือเป็นเรื่องสำคัญประการหนึ่งของการศึกษาระบบนี้ ซึ่งการคอนฟิกและกำหนดโพลิซีในสควิดพรอกซี่จะมีรูปแบบหรือมาตรฐานที่ต้องเข้าใจเป็นมาตรฐานที่สควิดพรอกซี่กำหนดไว้ เราสามารถเพิ่มเติม แก้ไข ปรับเปลี่ยนได้ตามต้องการแต่ต้องมีความเข้าใจและถูกต้อง หากกระทำโดยไม่มีความเข้าใจ นอกจากจะไม่ได้ระบบที่ดีมีประสิทธิภาพสูงขึ้นแต่กลับจะทำให้ระบบเกิดความสับสนและทำให้ประสิทธิภาพของระบบโดยรวมตกลงอีกด้วย และหากมีความเข้าใจที่ดีในการกำหนดโพลีซีแล้วแล้วก็เพียงนำมาปรับเปลี่ยนเงื่อนไขตามที่ผู้ใช้ต้องการ โดยส่วนหลักๆของโพลีซีมีดังนี้

ทำการติดตั้งโปรแกรมสควิดพรอกซี่ การติดตั้งใช้ไฟล์ติดตั้งที่มีอยู่แล้วในแผ่นติดตั้งของลินุกซ์ หลังจากติดตั้งโปรแกรมแล้วให้เปิดไฟล์คอนฟิกของสควิด โดยไฟล์นี้จะถูกจัดเก็บไว้ในไดเร็คทอรี /etc/squid/squid.conf เพื่อตั้งค่าการใช้งานต่างๆตามความเหมาะสม โดยรายละเอียดภายในไฟล์คอนฟิกมีดังนี้

ตัวอย่างไฟล์คอนฟิกของสควิดพรอกซี่ (squid.conf)

```
http_port 8080
icp_port 3130
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin ?

no_cache deny QUERY
cache_mem 32 MB
cache_replacement_policy heap GDSF
memory_replacement_policy heap GDSF
cache_dir diskd /cache 1000 16 256
acl localnet src 192.168.0.0/255.255.255.0
acl localhost src 127.0.0.1/255.255.255.255
acl Safe_ports port 80 443 210 70 21 1025-65535
```

acl CONNECT method CONNECT
acl all src 0.0.0.0/0.0.0.0
http_access allow localnet
http_access allow localhost
deny !Safe_ports
http_access deny CONNECT http_access deny all
cache_mgr admin@abcdef.com
cache_effective_user squid
cache_effective_group squid
logfile_rotate 0
log_icp_queries off
cachemgr_passwd my-secret-pass all
buffered_logs on
visible_hostname http://www.abcdef.com

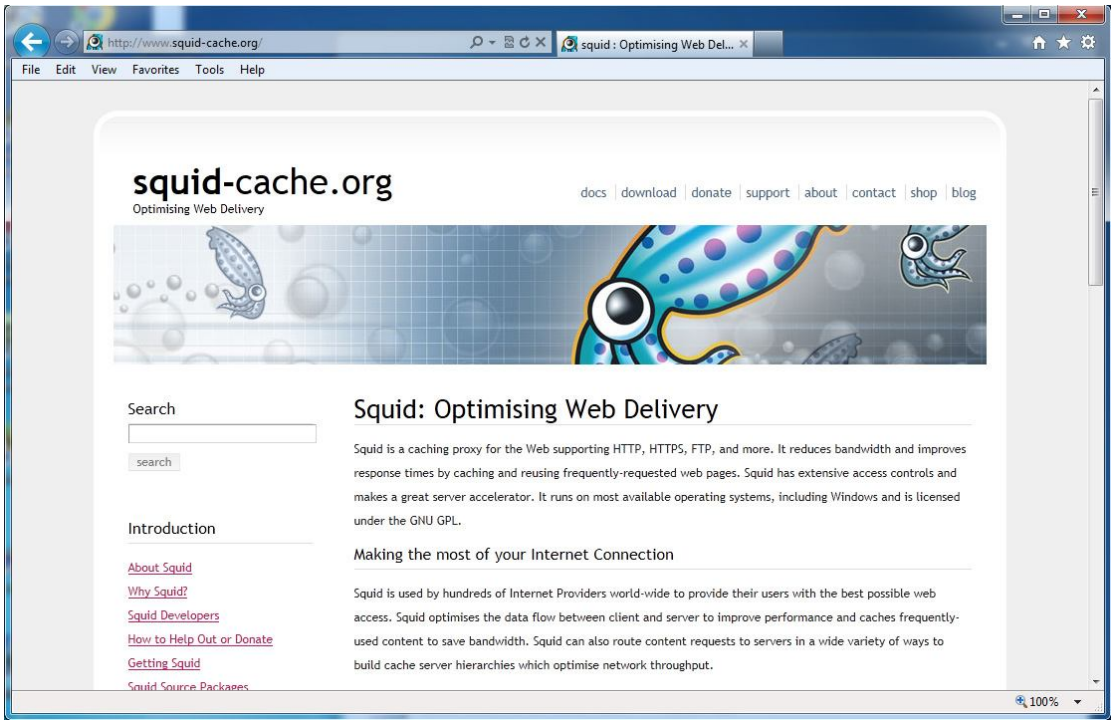
ตารางที่ 3-1 ความหมายของคำสั่งที่ปรากฏในไฟล์ squid.conf

http_port 8080	port ที่ให้บริการเชื่อมต่อระหว่างเครื่องแม่ข่ายกับเครื่องลูกข่ายส่วนใหญ่จะใช้ port 8080
icp_port 3130	port ที่ใช้สื่อสารระหว่าง Web cache ใช้เพื่อหา Web objectใน cache ค่า 3130 เป็นค่ามาตรฐาน
hierarchy_stoplist cgi-bin acl QUERY urlpath_regex cgi-bin \? asp php no_cache deny QUERY	กำหนดค่าให้เก็บหรือไม่เก็บอะไรบ้าง โดยเขียนต่อท้ายบรรทัด เช่น เว็บที่เป็น asp หรือ php เป็นเว็บที่มีการเปลี่ยนแปลงเร็ว ดังนั้นจึงสั่งว่าไม่ต้องเก็บค่าไว้
cache_mem 8 MB	กำหนดขนาด Memory ของ cache ถ้าไม่กำหนด ค่าเริ่มต้นที่มีมาจะมีค่าเท่ากับ 8 MB
cache_replacement_policy heap GDSF memory_replacement_policy heap GDSF	เป็นการกำหนด Policy รูปแบบการจัดการ cache และ Memory ในที่นี้ใช้ heap (sort) แบบ GDSF
cache_dir diskd /cache 1000 16 256	เป็นการกำหนดขนาดและไดเรกทอรีที่จะใช้เก็บ cache ข้อมูล มีรูปแบบดังนี้ cache เป็นชื่อไดเรคทอรีที่ใช้เก็บแคชข้อมูล 1000 ขนาดไดเรกทอรีที่ใช้เก็บข้อมูล 16 คือจำนวนไดเรกทอรีย่อยภายใน 256 คือจำนวนไดเรกทอรีย่อยภายในแต่ละ

	ไดเรคทอรีหลัก
acl localnet src 192.168.0.0/255.255.255.0	กำหนด IP ของ Network ภายในว่าช่วง IP เท่าใดและ Subnet ใดบ้างที่สามารถใช้ Proxy นี้ได้
acl localhost src 127.0.0.1/255.255.255.255	กำหนด IP ของ Localhost ของเครื่องแม่ข่าย
acl Safe_ports port 80 443 210 70 21	อนุญาติให้ใช้ port ตามที่กำหนด ในที่นี้ประกอบด้วย port 80 # http port 443 # https port 210 # wais port 70 # gopher port 21 # ftp เป็นต้น
acl CONNECT method CONNECT	ค่า Method พื้นฐานของ Access List
acl all src 0.0.0.0/0.0.0.0	ต้นทางทุกเครื่องสามารถใช้งานได้หมด
http_access allow localnet	อนุญาตให้ IP ของ Network ที่ชื่อ localnet ใช้งาน Proxy ได้
http_access allow localhost	อนุญาตให้ IP ของ Localhost ภายในใช้งาน Proxy ได้
deny !Safe_ports	port ที่นอกเหนือจากที่กำหนดไว้ ไม่สามารถใช้งานได้
http_access deny CONNECT http_access deny all	ไม่สามารถเข้าถึง url เป้าหมายได้ ต้องผ่าน proxy เท่านั้น
cache_mgr admin@abcdef.com	ผู้สามารถสั่งงานได้ในการเปลี่ยนแปลงคือ admin เท่านั้น
cache_effective_user squid cache_effective_group squid	สามารถทำงานได้ด้วยการสั่งงานของ User หรือ Group Squid
logfile_rotate 0	กำหนดเลขของ logfile โดยDefault = 0
log_icp_queries off	ไม่อนุญาตให้ Queries logs ของ icp
cachemgr_passwd my-secret-pass all	สามารถใช้ my-secret-pass ทำ valid actions ได้ทั้งหมด (all)
buffered_logs on	เปิดสถานะของ Buffer ของ Logs ในที่นี้คือ on
visible_hostname http://www.abcdef.com	กำหนดชื่อ Hostname

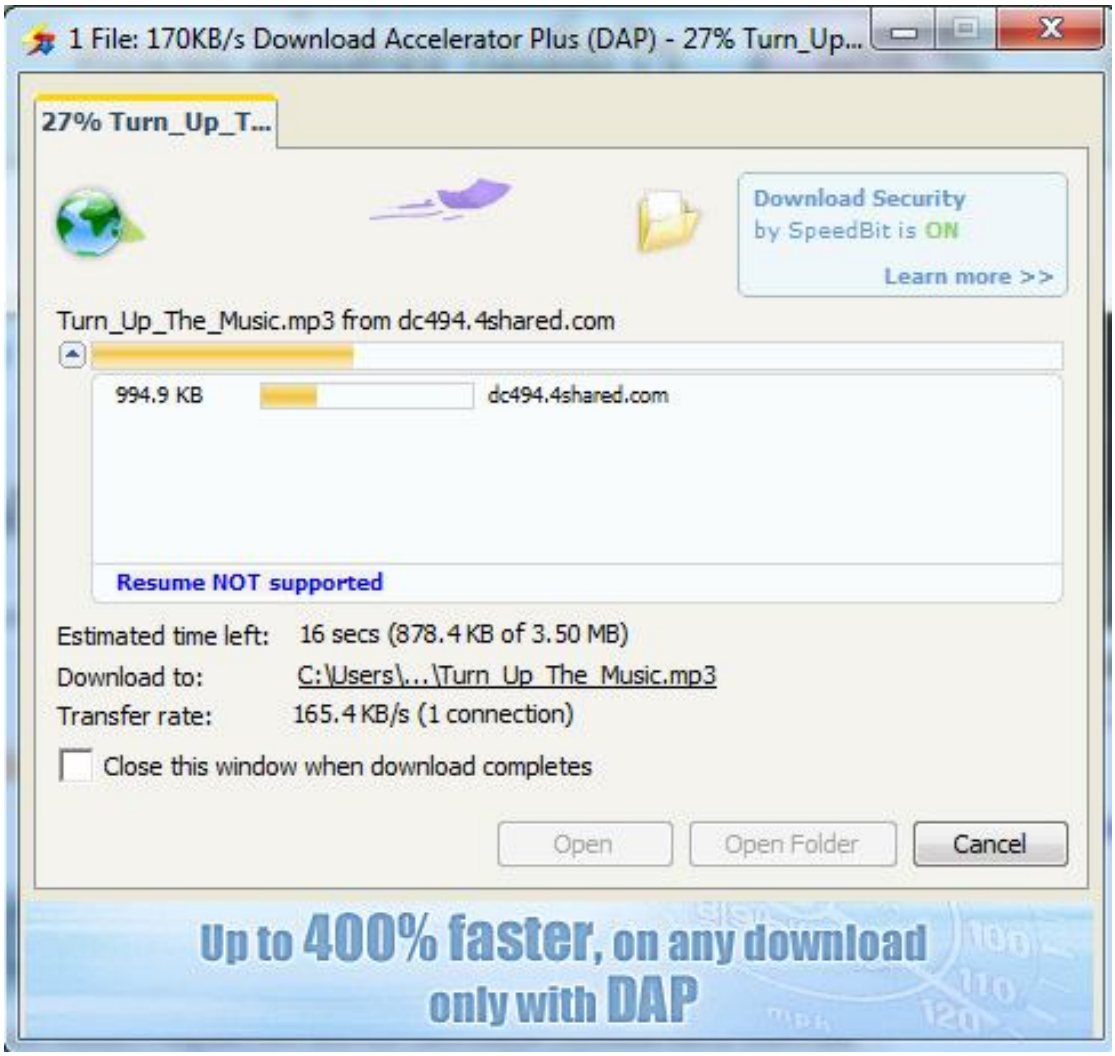
3.1.3 กระบวนการทำงานของการดาวน์โหลด

การทำงานของสควิดพรอกซี่นั้นจะทำการเก็บข้อมูลเว็บด้วยโปรโตคอล HTTP ข้อมูลใดก็ตามที่มีการส่งผ่านหน้าโปรแกรมเว็บเบราว์เซอร์จะต้องผ่านตัวกลางคือสควิดพรอกซี่เสมอโดยใช้พอร์ท 80 (Port 80) และสควิดพรอกซี่จะทำการเก็บข้อมูลที่ผู้ใช้เคยเรียกใช้ไปแล้วมาเก็บไว้ในแคช (Web Cache) จะทำให้การเข้าถึงข้อมูลในอินเทอร์เน็ตเร็วขึ้นกว่าเดิมเป็นอย่างมาก แต่ยังมีข้อมูลจากผู้ใช้อีกประเภทที่ไม่ได้วิ่งผ่านโปรโตคอล HTTP หรือพอร์ท 80 นั่นคือข้อมูลที่เกิดจากการดาวน์โหลด กระบวนการนี้จะใช้โปรโตคอล FTP และผ่านพอร์ท 21 (Port 21) ดังนั้นหากจะทำให้ระบบเกิดการเก็บข้อมูลหรือแคชข้อมูลทั้งสองแบบจำเป็นต้องมีการศึกษากระบวนการทำงานของโปรโตคอล FTP เพื่อให้ระบบปฏิบัติการลินุกซ์และสควิดพรอกซี่สามารถทำงานและแยกแยะการเก็บข้อมูลระหว่างข้อมูลที่วิ่งผ่านพอร์ท 80 กับพอร์ท 21 เก็บไว้ในระบบโดยแยกเนื้อที่การจัดเก็บออกเป็นสองส่วน ตัวอย่างการทำงานของ http และ ftp มีดังนี้



ภาพที่ 3-1 การทำงานของ http (port 8080)

ภาพที่ 3-1 แสดงการทำงานของโปรโตคอล http ซึ่งจะเป็นลักษณะการเปิดดูเว็บทั่วไป และข้อมูลเว็บที่เคยถูกเปิดแล้วจะถูกเก็บเป็นแคชข้อมูลไว้ในสควิดพรอกซี่ เมื่อมีการเรียกเปิดเว็บนี้ซ้ำจะทำให้การเข้าถึงเร็วกว่าเดิมเนื่องจากข้อมูลนี้ถูกเก็บอยู่ในเครื่องแม่ข่าย



ภาพที่ 3-2 การดาวน์โหลดไฟล์ของ ftp (port 21)

ภาพที่ 3-2 แสดงการดาวน์โหลดไฟล์ต่างๆในแบบที่ใช้โปรโตคอล ftp ซึ่งใช้ port 21 และการดาวน์โหลดแบบนี้ระบบเครือข่ายที่ใช้พรอกซี่ปกติ โดยทั่วไปยังไม่มีการเก็บข้อมูลที่เรียกว่าแคช ทำให้การทำงานของระบบตกลงเมื่อมีผู้ใช้โหลดพร้อมกันจำนวนมากๆ

3.1.4 การเขียนสคริปต์และโพลีซีของไฟล์วอลล์

การทำงานที่สำคัญที่สุดของระบบนี้คือการบังคับการทำงานให้เป็นไปอย่างถูกต้องและแม่นยำจำเป็นต้องมีการกำหนดสิทธิ์ในด้านความปลอดภัยให้กับระบบ ซึ่งโดยปกติระบบปฏิบัติการลินุกซ์จะมีระบบรักษาความปลอดภัย (Security)ที่สูงอยู่แล้ว ข้อมูลใดที่วิ่งเข้าออกในระบบสามารถถูกบังคับให้เป็นไปตามที่ต้องการได้โดยใช้แพ็คเกจของไอพีเทเบิ้ล (iptables) ซึ่งการจะเขียนกฎ (Chain) หรือโพลิซีใดได้นั้นจำเป็นต้องรู้รูปแบบของกฎต่างๆที่จำเป็นเพื่อให้ข้อมูลจากพอร์ท 80 กับ ข้อมูลจากพอร์ท 21 ถูกบังคับให้จัดเก็บลงในไดเรคทอรีของการเก็บแคชแยกกันได้อย่างถูกต้อง ซึ่งรูปแบบและกฎของไอพีเทเบิ้ลที่สำคัญมีดังนี้

ตัวอย่างรูปแบบของไอพีเทเบิ้ล(iptables)

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -A INPUT -i eth0 -s 192.168.1.0/24 -d 192.168.1.11 -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -i eth0 -s 192.168.1.0/24 -d 192.168.1.11 -p tcp --dport 8080 -j
ACCEPT
iptables -A INPUT -i eth0 -m iprange --src-range 192.168.1.100-192.168.1.254 -d
192.168.1.11 -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -i eth0 -m iprange --src-range 192.168.1.100-192.168.1.254 -d
192.168.1.11 -p tcp --dport 10000 -j ACCEPT
iptables -A INPUT -i eth0 -s 192.168.1.0/24 -d 192.168.1.11 -p icmp -j ACCEPT
iptables -A OUTPUT -o eth0 -j ACCEPT
```

ความหมายของกฎในแต่ละบรรทัด

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -A INPUT -i eth0 -s 192.168.1.0/24 -d 192.168.1.11 -p tcp --dport 80 -j ACCEPT
(สามารถเชื่อมต่อมายัง Server ต้นทาง IP 192.168.1.0/24 ด้วย Protocol TCP Port 80 (Proxy
Server))
iptables -A INPUT -i eth0 -s 192.168.1.0/24 -d 192.168.1.11 -p tcp --dport 8080 -j
ACCEPT
(สามารถเชื่อมต่อมายัง Server ต้นทาง IP 192.168.1.0/24 ด้วย Protocol TCP Port 8080
(Proxy Server))
iptables -A INPUT -i eth0 -m iprange --src-range 192.168.1.100-192.168.1.254 -d
192.168.1.11 -p tcp --dport 22 -j ACCEPT
(สามารถเชื่อมต่อมายัง Server ได้เฉพาะกลุ่ม IP 192.168.1.100-254 ด้วย Protocol TCP Port 22
(SSH Server))
iptables -A INPUT -i eth0 -m iprange --src-range 192.168.1.100-192.168.1.254 -d
192.168.1.11 -p tcp --dport 10000 -j ACCEPT
(สามารถเชื่อมต่อมายัง Server ได้เฉพาะกลุ่ม IP 192.168.1.100-254 ด้วย Protocol TCP Port
1000 (Webmin))
iptables -A INPUT -i eth0 -s 192.168.1.0/24 -d 192.168.1.11 -p icmp -j ACCEPT
(สามารถปิงเข้ามายัง Server ได้ ต้นทาง IP 192.168.1.0/24)
```

iptables -A OUTPUT -o eth0 -j ACCEPT
(กำหนดข้อมูลที่วิ่งออกจาก Server)

เมื่อทำความเข้าใจโดยการศึกษาและรวบรวมข้อมูลที่จำเป็นในการพัฒนาระบบ ทำให้ทราบว่าส่วนที่เกี่ยวข้องนั้น ประกอบไปด้วยองค์ความรู้ของการทำงานในการส่งผ่านข้อมูลของระบบเครือข่าย นั่นก็คือทุกครั้งที่มีการเรียกใช้งานอินเทอร์เน็ต จำเป็นต้องใช้โปรแกรมเว็บเบราว์เซอร์ ผ่านพอร์ทที่ชื่อว่า 80 กระบวนการนี้ระบบปฏิบัติการจะคอยดูแลและให้บริการ ในที่นี้คือระบบปฏิบัติการลินุกซ์ซึ่งมีแพ็คเก็จสำหรับดูแลการใช้งานอินเทอร์เน็ตผ่านพอร์ท 80 คือ สควิดพรอกซี่ทำหน้าที่เป็นเว็บแคช มีไอพีเทเบิ้ลเป็นกลไกในการบังคับการทำงานของแพ็คเก็จ ทำให้สามารถระบบมีศักยภาพในการกำหนดรูปแบบของการดาวน์โหลดในรูปแบบต่างๆดังที่กล่าวไปแล้วได้ และสามารถนำมากำหนดการทำงานเพื่อเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลในขั้นตอนการวิเคราะห์และออกแบบระบบต่อไป

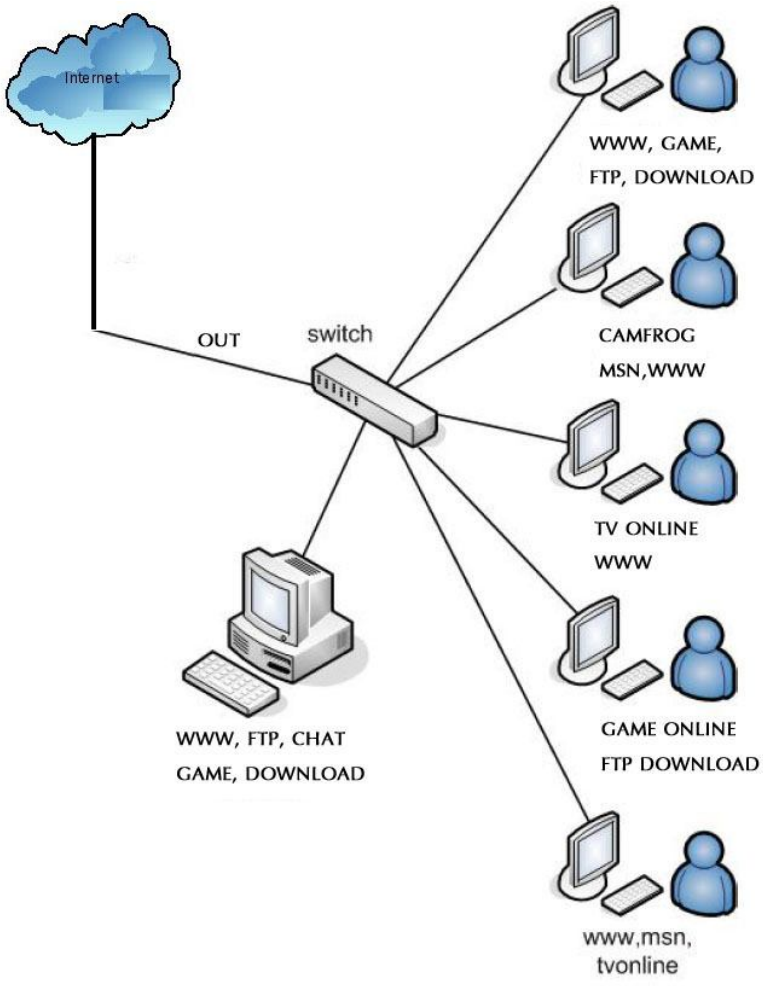
3.2 การวิเคราะห์และออกแบบระบบ

3.2.1 กำหนดขอบเขตของปัญหา

จากการศึกษาพบว่าเมื่อผู้ใช้ทำการเปิดโปรแกรมเบราว์เซอร์ใช้งานอินเทอร์เน็ต ผู้ใช้ทำการพิมพ์ที่อยู่ของเว็บปลายทาง(URL)ที่ต้องการ สัญญาณการร้องขอจากผู้ใช้จะวิ่งผ่านสควิดพรอกซี่ก่อนเป็นอันดับแรก จากนั้นสควิดพรอกซี่ทำการตรวจสอบข้อมูลที่ผู้ใช้ต้องการในแคช หากในแคชมีข้อมูลอยู่สควิดจะทำการตอบกลับคำร้องขอให้ผู้ใช้รายนั้นด้วยข้อมูลที่มีอยู่ในแคช และในทางกลับกันหากสควิดไม่พบข้อมูลในแคชจึงทำการร้องขอข้อมูลออกไปนอกเครือข่ายผ่านอุปกรณ์เครือข่ายต่างๆจนได้ข้อมูลที่ต้องการกลับมา กระบวนการนี้ใช้โปรโตคอล HTTP และพอร์ท 80 ส่วนการทำงานอีกรูปแบบหนึ่งซึ่งเรียกว่าการดาวน์โหลดเกิดจากกระบวนการที่ผู้ใช้ ใช้โปรแกรมเฉพาะทางที่ไม่ใช่เบราว์เซอร์ (โปรแกรมช่วยดาวน์โหลด) เช่น File Zilla ฯ ทำการติดต่อไปยังเครื่องแม่ข่ายที่ให้บริการดาวน์โหลด (FTP Server) การทำงานอาจมีการตรวจสอบสิทธิ์ในการเข้าถึงหรือไม่มีก็ได้ เมื่อการเชื่อมต่อเป็นผลสำเร็จข้อมูลจะถูกส่งมายังเครื่องผู้ใช้(Download)จนครบ ซึ่งก้อนข้อมูลของการดาวน์โหลดแต่ละครั้งมักมีขนาดใหญ่และใช้เวลาในการดาวน์โหลดข้อมูลนานมาก ในกระบวนการทำงานตรงนี้ใช้โปรโตคอลชื่อ FTP และทำงานผ่านพอร์ท 21 และสควิดพรอกซี่ไม่รู้จักการทำงานในรูปแบบที่เกิดขึ้น เนื่องจากต่างโปรโตคอลจึงไม่มีการเก็บแคชข้อมูลไว้ในระบบของสควิดพรอกซี่ ทำให้เกิดปัญหาว่าในครั้งหน้าเมื่อมีผู้ใช้ทำการดาวน์โหลดข้อมูลหรือไฟล์ข้อมูลเดิมอีกครั้งก็จะต้องเริ่มกระบวนการใหม่เหมือนในครั้งก่อนและใช้เวลาดาวน์โหลดนานเช่นเดิมหรืออาจมากกว่าหากช่วงเวลานั้นมีผู้ใช้ ใช้งานอินเทอร์เน็ตจำนวนมาก(Traffic) ปัญหานี้จะทำให้ความเร็วในการใช้งานอินเทอร์เน็ตตกลงจนถึงช้ามากหากในช่วงเวลานั้นมีผู้ใช้ดาวน์โหลดพร้อมๆกัน และในความเป็นจริงนั้นพบว่าแนวโน้มการใช้อินเทอร์เน็ตสำหรับดาวน์โหลดข้อมูลมีจำนวนเพิ่มมากขึ้นทุกวันอันเนื่องมาจากความต้องการของผู้ใช้และความเร็วของระบบเครือข่ายที่มีการพัฒนาไปอย่างรวดเร็วและความเร็วอินเทอร์เน็ตปัจจุบันดูเหมือนว่าไม่ใช่ปัญหาของผู้ใช้อีกต่อไปแล้ว ปัญหาของผู้ดูแลระบบจึงอยู่ที่จะทำอย่างไรให้ความเร็วของอินเทอร์เน็ตที่มีอยู่สามารถตอบสนองผู้ใช้ได้อย่างมีประสิทธิภาพไม่เกิดสภาวะการอัดแน่นของปริมาณความต้องการข้อมูล และนั่นคือปัญหาที่นำมาสู่การออกแบบระบบ

3.2.2 การออกแบบระบบ

การออกแบบระบบเพื่อให้การทำงานเป็นไปอย่างถูกต้อง ได้มีการจัดระบบการทำงานออกเป็นส่วนๆ ดังนี้

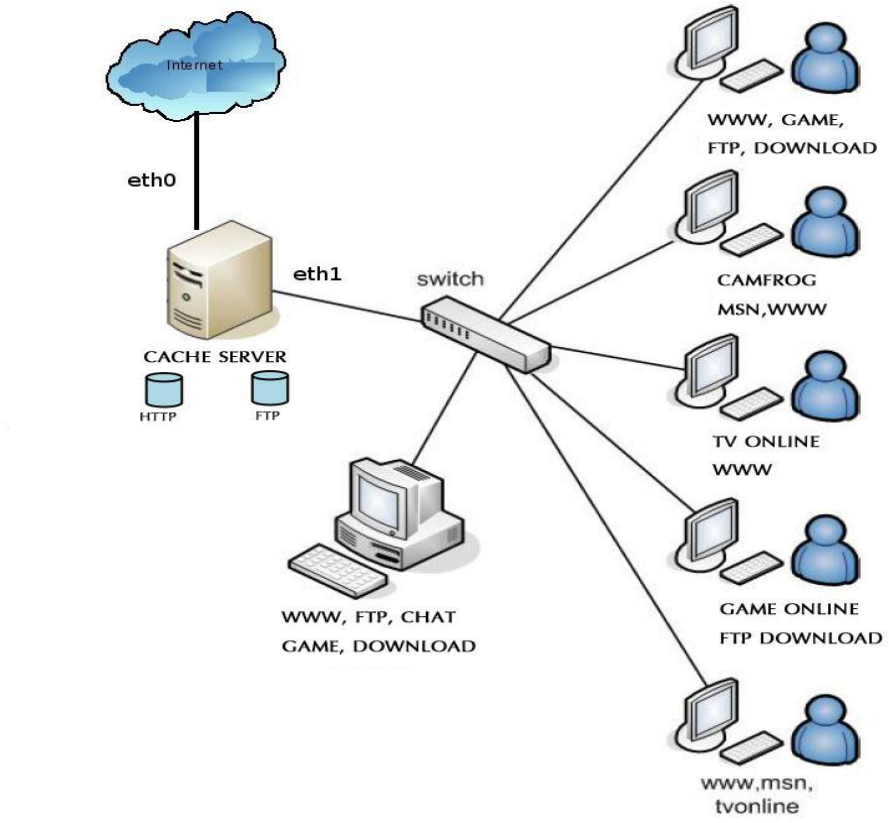


ภาพที่ 3-3 การทำงานของระบบ

จากภาพการทำงานของระบบ จะพบว่ากลุ่มเครื่องผู้ใช้ (Client) ที่เชื่อมต่ออยู่กับระบบนั้น หากเครื่องใดเครื่องหนึ่งต้องการเข้าถึงระบบอินเทอร์เน็ตด้วยบริการอะไรก็ตาม อาทิเช่น การเปิดเว็บไซต์ทั่วไป (www) ซึ่งใช้โปรโตคอล HTTP หรือการดาวน์โหลดข้อมูล (ftp download) สัญญาณการร้องขอบริการจะต้องไหลผ่านอุปกรณ์กระจายสัญญาณ (Switch) ก่อนเสมอและการทำงานไม่ว่าการอัพโหลดหรือดาวน์โหลดจะเข้าออกด้านเดียว (out) ร่วมกันเพียงทางเดียว นั่นหมายความว่าทุกเครื่องที่อยู่ด้านหลังอุปกรณ์กระจายสัญญาณจะออกใช้งานอินเทอร์เน็ตด้วยเส้นทางเดียวกันเสมอ ไม่ว่าจะใช้บริการประเภทใด อาจเป็นการเปิดเว็บไซต์หรือการดาวน์โหลดข้อมูลจากนั้นจึงเข้าสู่ระบบอินเทอร์เน็ตได้โดยตรง การทำงานในลักษณะดังกล่าวทำให้เกิดปัญหาการอัด

แน่นของข้อมูล (Traffic) ทำให้เกิดความล่าช้าในการเข้าถึงอินเทอร์เน็ตประสิทธิภาพด้วยรวมของระบบตกลงด้วยปริมาณข้อมูลจำนวนมาก(เกิดปัญหาคอขวดตามมา)

การออกแบบระบบเพื่อแก้ไขปัญหาและลดปริมาณข้อมูลดังกล่าวจึงจำเป็นต้องมีระบบและอุปกรณ์บางอย่างทำหน้าที่ลดภาระงาน ซึ่งระบบที่เป็นที่นิยมทั่วไป มักใช้ระบบเก็บแคชข้อมูล เพื่อลดปริมาณในระดับหนึ่ง(proxy server) ผู้วิจัยจึงออกแบบโดยเพิ่มระบบใหม่ ดังภาพ



ภาพที่ 3-4 ระบบที่มีการจัดเก็บแคช

จากภาพของระบบที่ออกแบบใหม่จะพบว่ามีการเพิ่มเครื่องแม่ข่ายซึ่งประกอบด้วยแลนการ์ด(เน็ตเวิร์คการ์ด) 2 การ์ด (eth0, eth1) ระบบปฏิบัติการลินุกซ์, ซอฟท์แวร์พร้อมแพ็คเก็จที่จำเป็น เช่น สควิดพรอกซี่, ไอพีเทเบิ้ล เป็นต้น

3.2.2.1 ติดตั้งเครื่องแม่ข่าย (Cache Server) เพื่อให้บริการการเข้าถึงอินเทอร์เน็ต ในที่นี้ใช้ระบบปฏิบัติการ Linux CentOS 5.0

3.2.2.2 ติดตั้งการ์ดแลนจำนวน 2 การ์ดลงในเครื่องแม่ข่าย โดยการ์ดที่ 1 ใช้เป็นการ์ดภายนอก (eth0) ติดต่อกับสัญญาณอินเทอร์เน็ต การ์ดที่ 2 ใช้สำหรับเชื่อมต่อกับเครือข่ายภายใน (eth1)

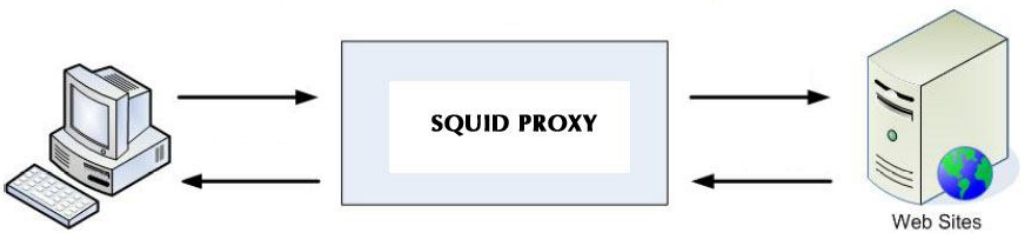
3.2.2.3 ติดตั้งโปรแกรมพรอกซี่ (Proxy) ในที่ใช้โปรแกรมสควิดพรอกซี่ ซึ่งมีอยู่แล้วในแผ่นติดตั้งของ Linux CentOS 5.0 เพื่อใช้เก็บแคชข้อมูลประเภทเว็บไซต์ทั่วไปที่ใช้หรือวิ่งผ่านโปรโตคอล HTTP

3.2.2.4 ติดตั้งโปรแกรมเอฟทีพีพรอกซี่ (Ftp Proxy) ในที่นี้ใช้โปรแกรม Frox สามารถหาดาวน์โหลดได้ทั่วไปเนื่องจากเป็น Open Source ใช้ได้ไม่มีลิขสิทธิ์

3.2.2.5 ติดตั้งโปรแกรมไฟล์วอลล์ ในที่นี้ใช้ไฟล์วอลล์ที่มีมากับระบบปฏิบัติการ Linux CentOS 5.0 คือ Iptables Firewall โดยไฟล์วอลล์นี้จะเป็นส่วนสำคัญที่ช่วยให้การแยกเก็บแคชข้อมูลเป็นไปอย่างถูกต้อง

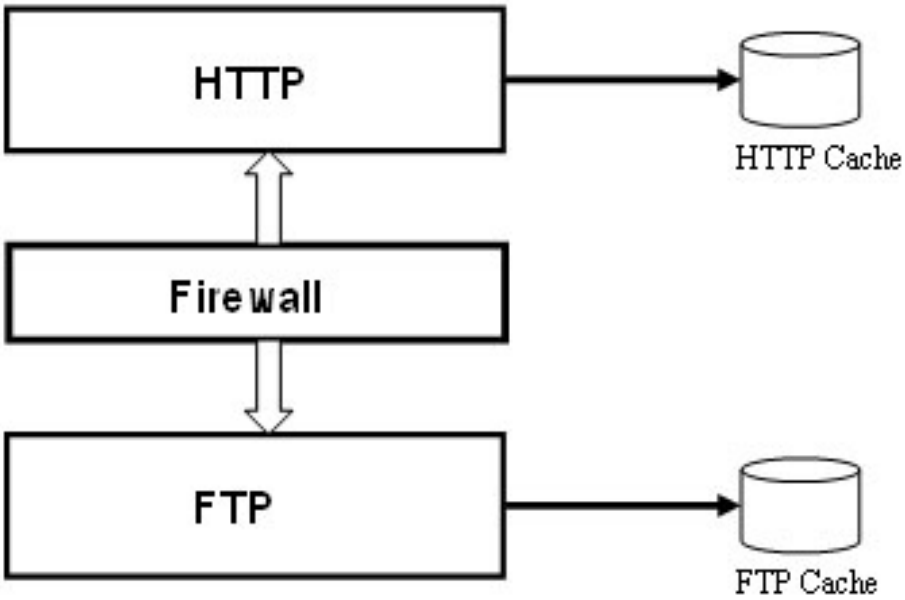
3.3 การพัฒนาระบบ

การดำเนินการพัฒนาระบบเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยระบบปฏิบัติการลินุกซ์ ได้เลือกใช้ระบบปฏิบัติการลินุกซ์เป็นหลัก เนื่องจากเป็นระบบปฏิบัติการที่มีผู้นำมาใช้เป็นระบบหลักของเครื่องแม่ข่ายเป็นจำนวนมากเนื่องจากได้รับการยอมรับว่ามีความคงทนและมีความเสถียรสูงมาก สามารถรองรับการทำงานได้ทั้งระบบทั่วไปและระบบที่มีขนาดใหญ่และซับซ้อน และที่สำคัญเป็นระบบปฏิบัติการที่เป็นโอเพ่นซอร์สไม่มีค่าลิขสิทธิ์ มีการเปิดเผยโค้ดให้สามารถดัดแปลงเพิ่มเติมได้ง่าย รวมถึงโปรแกรมหรือแพ็คเกจทั้งหมดที่ใช้ในการทำงานครั้งนี้ก็มีมากับระบบปฏิบัตการลินุกซ์ทั้งสิ้น ทำให้ง่ายต่อการดำเนินงาน โดยการพัฒนาระบบมีดังนี้



ภาพที่ 3-5 การเข้าถึงอินเทอร์เน็ตโดยผ่าน Squid Proxy

ในการเข้าถึงข้อมูลอินเทอร์เน็ตจากเดิมสามารถเข้าถึงได้โดยตรง ในที่นี้มีการบังคับให้เครื่องลูกข่ายจะต้องมีการวิ่งผ่าน Squid Proxy สำหรับข้อมูลที่เป็นเว็บ และบังคับให้ข้อมูลที่เป็นการดาวน์โหลดแยกไปเก็บอีกที่ด้วยโปรแกรม Frox เสียก่อน ดังแผนภาพการทำงาน ต่อไปนี้



ภาพที่ 3-6 ภาพการทำงานของระบบแยกแคช

สำหรับวิธีการบังคับเครื่องลูกข่ายนั้นทำได้โดยการกำหนดโพลีซีในไฟล์คอนฟิกของสควิดพรอกซี่ ในไดเรคทอรี /etc/squid/squid.conf มีรูปแบบและส่วนสำคัญ ดังนี้

cache_dir ufs /var/spool/squid 20480 16 256

คำสั่งสำหรับการระบุสถานที่และขนาดในการเก็บแคชข้อมูล โดยให้ปรับตัวเลข 20480 ตามความเหมาะสมของระบบ โดยตัวเลขนี้มีหน่วยเป็น MB ในที่นี้จึงมีค่าเท่ากับ 20 GB ไดเรคทอรีที่เก็บอยู่ที่ /var/spool/squid นั่นเอง

cache_mem 128 MB

หน่วยความจำของระบบสำหรับให้สควิดใช้ทำงานหากมีหน่วยความจำหลัก (Main Memory) อยู่ในระบบมากๆยิ่งดีและควรตั้งไว้ประมาณ 1/2 ของหน่วยความจำที่มี เช่น หน่วยความจำขนาด 1 GB ก็ควรกำหนดตัวเลขในส่วนนี้เป็น 512 MB

acl webconfig_lan src 192.168.2.0/24

acl webconfig_to_lan dst 192.168.2.0/24

ส่วนคำสั่งที่ระบุอนุญาตให้หรือไม่ให้เครือข่ายใดใช้งานอินเทอร์เน็ตได้ โดยให้ทำการแก้หมายเลขให้ตรงกับเครือข่ายที่ใช้งานอยู่จริง ตัวอย่างเช่น 192.168.2.0/24 เป็นต้น

http_port 192.168.2.254:3128 transparent

http_port 127.0.0.1:3128 transparent

ส่วนคำสั่งระบุหมายเลขเครื่องแม่ข่ายที่ให้บริการเป็น Proxy Server โดยให้แก้หมายเลขไอพีจาก 192.168.2.254 แก้เป็นไอพีที่ใช้งานตามจริง และให้ ใส่คำว่า transparent ต่อท้ายด้วยเพื่อเป็นการ

สั่งให้ระบบทำงานเป็น Transparent Proxy ส่วนหมายเลข 3128 เป็นหมายเลขพอร์ตที่สควิดให้บริการ

เมื่อกำหนดค่าในสควิดพรอกซี่เรียบร้อยแล้วต่อไปคือการกำหนดค่าเพื่อให้เก็บแคชข้อมูลที่เกิดจากการดาวน์โหลดที่ใช้โปรโตคอลประเภท FTP โดยกำหนดในไฟล์คอนฟิกของโปรแกรม Frox ซึ่งเก็บอยู่ในไดเรคทอรี /etc/frox.conf ดังนี้

HTTPProxy 127.0.0.1:3128

HTTPProxy 192.168.2.254:3128

แก้หมายเลขให้ตรงกับหมายเลขไอพีเครื่องแม่ข่ายที่ให้บริการตามจริง

#ForceHTTP yes

#CacheModule HTTP

###################################

CacheModule local

CacheSize 4000

กำหนดขนาดเนื้อที่สำหรับทำแคช ในที่นี้มีค่าเท่ากับ 4 GB

เมื่อทำการคอนฟิกค่าที่จำเป็นใน Squid และ Frox แล้ว จะต้องกำหนดคำสั่งให้ระบบรู้กระบวนการทำงานที่สัญญาณอินเทอร์เน็ตวิ่งเข้าออกระบบผ่าน Squidและ Frox รวมถึงการ์ดแลน โดยต้องกำหนดคำสั่งให้ไฟล์วอลล์ (Iptables) ดังนี้

iptables -t nat -A PREROUTING -m multiport -p tcp -i eth1 --dport 88,80,9898 -j REDIRECT --to 3128

คำสั่งนี้จะสั่งให้ Iptables ทำการ redirect port http ทุกอย่างที่ผู้ใช้มีการใช้งานผ่านโปรโตคอล HTTP ให้เก็บเข้าสู่สควิดพรอกซี่หรือให้ผ่านได้ ตัวอย่างเช่น เมื่อเครื่องลูกข่ายเข้าใช้งาน port 88,80,9898 ระบบจะทำให้มีการผ่านเข้าสควิดพรอกซี่โดยอัตโนมัติเสมอ และให้แก้ตรงคำว่า eth1 ให้ตรงกับการใช้งานจริงซึ่งเป็นการ์ดแลนด้านที่ต่ออยู่กับเครือข่ายภายในนั่นเอง

คำสั่งต่อมา

iptables -t nat -A PREROUTING -m multiport -p tcp -i eth1 --dport 6001,21,8021 -j REDIRECT --to 2121

คำสั่งนี้จะสั่งให้ Iptables ทำการ redirect port ftp ทุกอย่างที่ผู้ใช้มีการใช้งานผ่านโปรโตคอล FTP ให้เก็บเข้าสู่สควิดพรอกซี่หรือให้ผ่านได้เสมอ ตัวอย่างเช่น เมื่อเครื่องลูกข่ายเข้าใช้งาน port 6001,21,8021 ระบบจะทำให้มีการผ่านเข้าสควิดพรอกซี่โดยอัตโนมัติ และให้แก้ตรงคำว่า eth1 ให้ตรงกับการใช้งานจริงซึ่งเป็นการ์ดแลนด้านที่ต่ออยู่กับเครือข่ายภายในเหมือนในการทำงานที่ผ่านมา

เมื่อเสร็จสิ้นการคอนฟิกค่าต่างๆแล้ว ให้ทำการเริ่มการทำงานของ Squid และ Frox ใหม่อีกครั้ง (Restart) ระบบก็จะสามารถให้บริการเก็บแคชข้อมูลดังที่ต้องการได้แล้ว

คำสั่ง # service frox restart

เมื่อรีสตาร์ทเสร็จแล้วค่าคอนฟิกใหม่จะเริ่มทำงานทันที

3.4 ทดสอบการทำงาน แก้ไข และปรับปรุงระบบ

3.4.1 หลังการพัฒนาระบบเรียบร้อยผู้วิจัยจะทำการทดสอบการทำงาน โดยเชื่อมต่อเครื่องลูกข่ายผ่านอุปกรณ์ Switch ไปยังเครื่องแม่ข่ายดังภาพที่ 3-4 ในครั้งแรกจะทดสอบโดยเปิดเครื่องแม่ข่ายแต่ไม่เปิดระบบสควิดพรอกซี่ ทดลองเปิดเว็บเพจและทดลองดาวน์โหลดข้อมูลไฟล์เดียวกัน ขนาดเท่ากัน จากเว็บไซต์ที่เดียวกันแล้ววัดประสิทธิภาพการทำงานที่ได้ด้วยการดูรายงานจากล็อกไฟล์ที่รายงานโดยระบบปฏิบัติการลินุกซ์

3.4.2 ครั้งที่สองทำเหมือนเดิม โดยครั้งนี้เปิดระบบให้บริการสควิดพรอกซี่ ทดลองเปิดเว็บเพจและทดลองดาวน์โหลดข้อมูลไฟล์เดียวกัน ขนาดเท่ากัน จากเว็บไซต์ที่เดียวกัน แล้ววัดประสิทธิภาพการทำงานที่ได้ด้วยการดูรายงานจากล็อกไฟล์ที่รายงานโดยระบบปฏิบัติการลินุกซ์

3.4.3 ครั้งที่สามทำเหมือนครั้งที่สอง แต่ครั้งนี้เปิดระบบการทำงานทั้งหมดโดยทำการสตาร์ทแพ็คเก็จ (Frox) และรีสตาร์ทไอพีเทเบิ้ลด้วย ทดลองเปิดเว็บเพจและทดลองดาวน์โหลดข้อมูลไฟล์เดียวกัน ขนาดเท่ากัน จากเว็บไซต์ที่เดียวกัน แล้ววัดประสิทธิภาพการทำงานที่ได้ด้วยการดูรายงานจากล็อกไฟล์ที่รายงานโดยระบบปฏิบัติการลินุกซ์

3.4.4 บันทึกผลการทำงานของระบบ แก้ไขส่วนแสดงผลให้ตรงความต้องการ ตรวจสอบค่าคอนฟิกให้ถูกต้องและปรับส่วนที่ต้องการเพื่อนำผลไปวิเคราะห์ ต่อไป

3.5 ทดสอบการทำงานด้วยซอฟท์แวร์เฉพาะทาง

การวิจัยในครั้งนี้ใช้การทดสอบความถูกต้องของการทำงานโดยใช้ซอฟท์แวร์วัดความเร็วการเข้าถึงอินเทอร์เน็ต ทั้งในส่วนของระบบเดิม และระบบใหม่ที่พัฒนาขึ้น โดยเก็บสถิติแล้วแสดงผลเป็นค่าเฉลี่ย พร้อมทั้งเปรียบเทียบประสิทธิภาพระหว่างระบบเดิมกับระบบใหม่ และเพิ่มความน่าเชื่อถือของการนำระบบใหม่ไปใช้ด้วยการทดสอบระบบใหม่ซ้ำๆและคิดเปอร์เซนต์ความถูกต้องเป็นร้อยละ สุดท้ายแสดงผลให้เห็นความเปลี่ยนแปลงอย่างชัดเจนระหว่างความเร็วของระบบเดิมกับระบบใหม่ด้วยกราฟเส้น ร่วมกับกราฟแสดงความหนาแน่นของระบบเครือข่ายผ่านทางโปรแกรมตรวจวัดประสิทธิภาพของระบบเครือข่าย คือโปรแกรม MRTGซึ่งเป็นโปรแกรมที่ได้รับการยอมรับในการนำไปใช้วิเคราะห์ระบบเครือข่าย และเป็นโปรแกรมที่สามารถติดตั้งใช้งานได้ง่าย มีมากับระบบปฏิบัติการลินุกซ์ทุกเวอร์ชั่น

สำหรับการเข้าตรวจดูร่องรอย (log) หรือข้อมูลการใช้งานของผู้ใช้ สามารถกระทำได้ง่ายๆด้วยคำสั่งที่มีอยู่แล้วในระบบปฏิบัติการลินุกซ์ผ่านทางคอมมานด์ไลน์

ตัวอย่าง เช่น ใช้คำสั่งดูร่องรอยการทำงานของ Frox ดังนี้

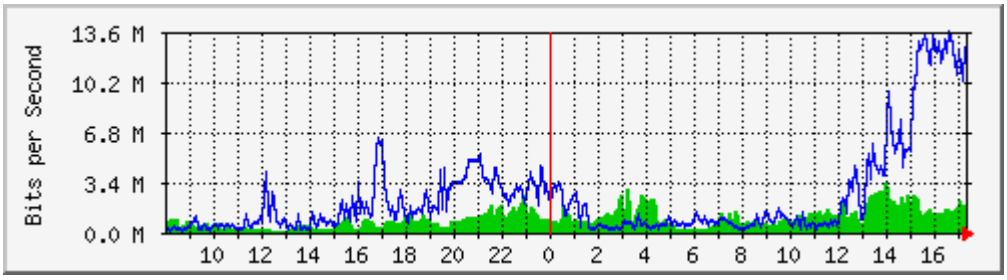
tail –f /var/log/frox - log คำสั่งนี้มีผลเพื่อดูล็อกการทำงานของ Frox จะได้ผลลัพธ์ดังภาพที่ 3-7

```
1223120444.683     4 192.168.1.38 TCP_HIT/200 21186 GET http://patch.pangya.in.          th/patch_lv1/updatelist - NONE/- application/octet-stream
1223120446.437   759 192.168.1.39 TCP_MISS/200 395 GET http://www.google-analyt          ics.com/__utm.gif? - DIRECT/209.85.143.127 image/gif
1223120458.310   970 192.168.1.33 TCP_MISS/200 146611 GET http://61.47.40.207/U          pdateFile/BannerFile.7z - DIRECT/61.47.40.207 7-Zip
1223120465.627  1024 192.168.1.39 TCP_MISS/200 395 GET http://www.google-analyt          ics.com/__utm.gif? - DIRECT/209.85.143.127 image/gif
1223120473.477   242 192.168.1.42 TCP_MISS/200 395 GET http://www.google-analyt          ics.com/__utm.gif? - DIRECT/209.85.143.127 image/gif
1223120477.268  1022 192.168.1.39 TCP_MISS/200 395 GET http://www.google-analyt          ics.com/__utm.gif? - DIRECT/209.85.143.127 image/gif
1223120483.148  1166 192.168.1.39 TCP_MISS/200 395 GET http://www.google-analyt          ics.com/__utm.gif? - DIRECT/209.85.143.127 image/gif
1223120490.470   330 192.168.1.39 TCP_MISS/200 395 GET http://www.google-analyt          ics.com/__utm.gif? - DIRECT/209.85.143.127 image/gif
1223120499.018     8 192.168.1.39 TCP_MISS/503 791 GET http://www.google-analyt        ics.com/__utm.gif? - NONE/- text/html
1223120527.574 114590 192.168.1.33 TCP_MISS/000 0 POST http://www.silvergang.com       /Account/Register.aspx - DIRECT/61.47.40.214 -
```

```
frox_addons_clarkconnect-1.5/
frox_addons_clarkconnect-1.5/install
frox_addons_clarkconnect-1.5/files/
frox_addons_clarkconnect-1.5/files/frox.conf
frox_addons_clarkconnect-1.5/files/frox
frox_addons_clarkconnect-1.5/files/frox-service
frox_addons_clarkconnect-1.5/files/rule
frox_addons_clarkconnect-1.5/uninstall
[root@volknet home]# cd frox_addons_clarkconnect-1.5
[root@volknet frox_addons_clarkconnect-1.5]# ./install
==================================
```

ภาพที่ 3-7 แสดงรายการร่องรอยที่เก็บอยู่ในระบบ

นอกจากนั้นยังสามารถดูความหนาแน่นของระบบเครือข่าย ซึ่งเกิดจากการใช้งานของผู้ใช้ในแต่ละช่วงเวลาที่ต้องการได้ด้วยกราฟซึ่งเกิดจากการติดตั้งไฟล์เครื่องมือกราฟ โดยมีอยู่แล้วในแผ่นติดตั้งของลินุกซ์ ตัวอย่างดังภาพที่ 3-8 แสดงผลการทำงานด้วยโปรแกรมตรวจประสิทธิภาพเครือข่าย MRTG ด้วยการเรียกผ่านเว็บ



ภาพที่ 3-8 ภาพการทำงานของโปรแกรม MRTG

บทที่ 4
ผลการดำเนินงาน

หลังจากได้พัฒนาระบบเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยระบบปฏิบัติการลินุกซ์เรียบร้อยแล้ว ขั้นตอนสำคัญลำดับต่อไปคือการนำระบบที่พัฒนาไปทดสอบผลการดำเนินงาน โดยแบ่งเป็นขั้นตอนต่างๆ ดังต่อไปนี้

4.1 ภาพรวมของระบบการทำงานที่เกี่ยวข้องในงานวิจัยนี้

4.2 จัดวางระบบเพื่อใช้ในการทดลองให้เหมือนสภาพใช้งานจริง

4.3 ทดสอบการเข้าใช้งานอินเทอร์เน็ตโดยใช้ระบบทดสอบแบบเดิมก่อนพัฒนาระบบใหม่ (ระบบที่มีเพียงพรอกซี่อย่างเดียว)

4.4 ทดสอบการเข้าใช้งานอินเทอร์เน็ตด้วยระบบใหม่ที่พัฒนาขึ้น

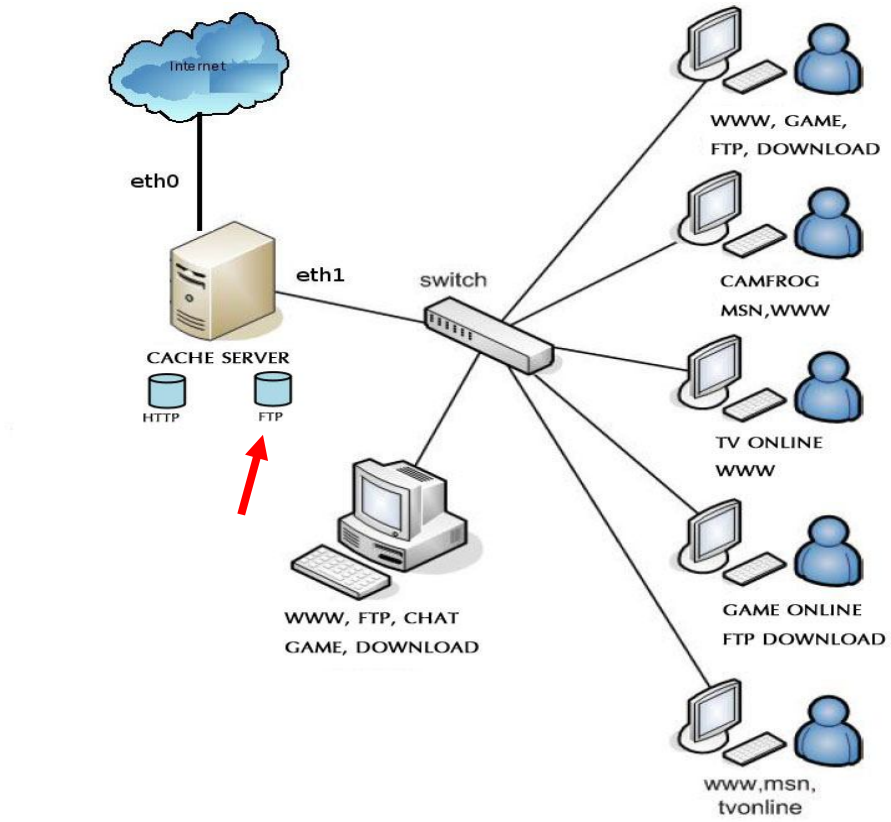
4.5 เปรียบเทียบการใช้งานระบบเก่ากับระบบที่พัฒนาขึ้นใหม่

เพื่อให้บรรลุวัตถุประสงค์ของงานวิจัยในครั้งนี้ การวัดประสิทธิภาพของระบบใหม่ที่พัฒนาขึ้นจะใช้การวัดความเร็วของการเข้าถึงข้อมูล นั่นคือการดาวน์โหลดข้อมูลเปรียบเทียบระหว่างระบบเดิมกับระบบใหม่ คำว่าระบบเดิมหมายถึงระบบที่มีเครื่องแม่ข่ายช่วยการใช้งานอินเทอร์เน็ตในการเข้าถึงเว็บไซต์โดยใช้ระบบพรอกซี่ (Proxy Server) ส่วนคำว่าระบบใหม่หมายถึงระบบที่มีเครื่องแม่ข่ายช่วยการใช้งานอินเทอร์เน็ตในการเข้าถึงเว็บไซต์โดยใช้ระบบพรอกซี่และเพิ่มระบบการดาวน์โหลดข้อมูลและการลดความหนาแน่นของข้อมูลในเครือข่าย หมายถึง การที่ในระบบมีข้อมูลส่งผ่านเข้าออกน้อย เมื่อใดที่มีผู้ใช้เข้าใช้อินเทอร์เน็ตพร้อมกันจำนวนมากการร้องขอข้อมูลจากภายในออกไปภายนอกย่อมมีมาก ปริมาณความหนาแน่นของข้อมูลก็มีมากตามไปด้วย หากในระบบมีผู้ใช้งานอยู่น้อยหมายถึงการร้องขอข้อมูลจากภายในออกไปภายนอกย่อมมีน้อย ดังนั้นถ้าช่วงเวลาใดมีผู้ใช้งานน้อยหรือใช้งานเสร็จได้เร็วย่อมหมายถึงความหนาแน่นของข้อมูลก็จะมีน้อยตามไปด้วย ระบบที่พัฒนาขึ้นจึงใช้ตัวชี้วัดความสำเร็จที่เรื่องของความเร็วในการใช้งานของผู้ใช้ นั่นคือหากผู้ใช้ทำการดาวน์โหลดข้อมูลซึ่งมีขนาดไฟล์ที่ใหญ่แตกต่างกันไป การดาวน์โหลดนั้นก็จะใช้เวลานานไม่เท่ากันตามไปด้วย แต่หากผู้ใช้สามารถดาวน์โหลดข้อมูลเสร็จได้เร็วเท่าไรหมายความว่าช่วงเวลานั้นก็จะไม่เกิดความหนาแน่นของข้อมูลหรือมีน้อยลงซึ่งเป็นที่มาของการลดปริมาณข้อมูล รายละเอียดต่อไปนี้จะแสดงให้เห็นการทำงานและความเร็วที่ได้จากระบบใหม่ที่พัฒนาขึ้น

4.1 ภาพรวมของระบบการทำงานที่เกี่ยวข้องในงานวิจัยนี้

เพื่อให้เห็นภาพการทำงานของระบบการเข้าใช้งานอินเทอร์เน็ตทั้งระบบก่อนพัฒนากับระบบหลังมีการพัฒนาใหม่ และเพื่อให้ง่ายต่อการเข้าใจและเห็นผลสรุปที่ได้จากงานวิจัยฉบับนี้ได้อย่างชัดเจน ในเบื้องต้นผู้วิจัยได้ใช้แผนภาพเครือข่ายที่ 4-1 จำลองการทำงานจากระบบจริงโดยจากภาพจะพบว่าเป็นเครือข่ายที่ผู้วิจัยได้จัดทำขึ้นใหม่จากระบบเดิม (ระบบที่มีแต่พรอกซี่) ที่นิยมใช้งานกันทั่วไป หากดูจากรูปภาพให้สังเกตว่าระบบเดิมคือระบบที่ไม่มีลูกศรสีแดงกำกับอยู่ ส่วนระบบใหม่ที่พัฒนาขึ้นคือระบบที่มีการเพิ่มส่วนความสามารถของการดาวน์โหลด (ftp) ตรงทีมีลูกศรสีแดงชี้กำกับ

อยู่เข้าในระบบเพื่อเพิ่มความสามารถที่จะใช้ในการลดปริมาณข้อมูลที่มีความหนาแน่นอันเกิดมาจากระบบเดิมที่ไม่สามารถให้บริการที่ครอบคลุมบริการดาวน์โหลดข้อมูล และไม่สามารถจัดการกับปริมาณข้อมูลจำนวนมากที่เกิดจากการใช้ของผู้ใช้อินเทอร์เน็ตได้ จากภาพที่ 4-1 นั้น เป็นระบบที่จำลองขึ้นโดยใช้เครื่องพีซีธรรมดามิใช่เครื่องให้บริการพิเศษเฉพาะทาง (server) เพื่อให้เห็นว่าระบบใหม่สามารถทำงานได้อย่างมีประสิทธิภาพจริงโดยไม่ขึ้นต่อศักยภาพของเครื่องมือหรือฮาร์ดแวร์พิเศษ



ภาพที่ 4-1 ระบบแม่ข่ายลดปริมาณข้อมูล

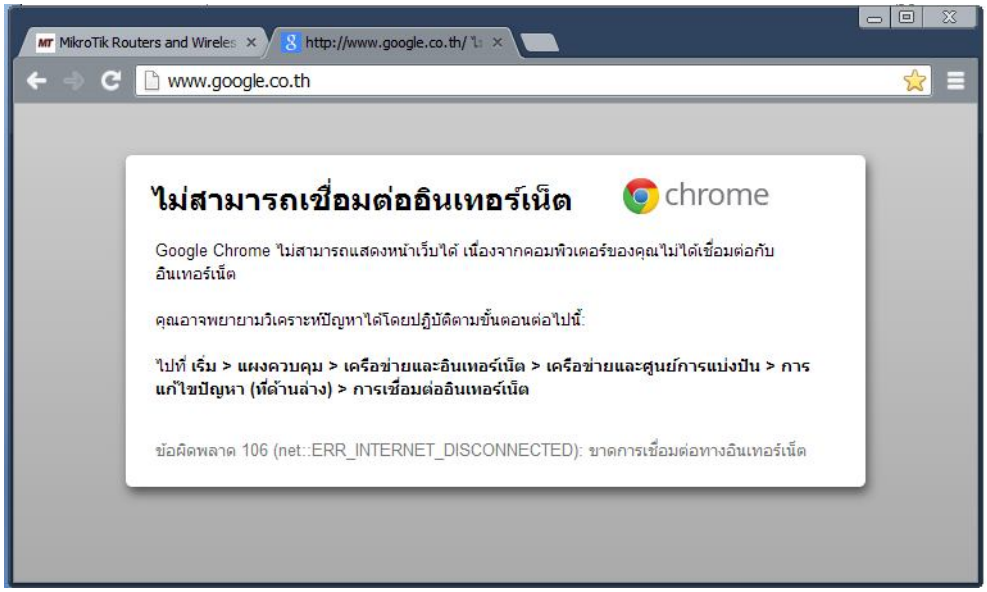
4.2 จัดวางระบบเพื่อใช้ในการทดลองให้เหมือนสภาพใช้งานจริง

จากภาพ 4-1 จะพบว่าระบบที่จำลองขึ้นมานั้นมีสภาพโดยรวมที่เหมือนกันทุกประการ ทั้งเรื่องของฮาร์ดแวร์และซอฟต์แวร์ โดยฮาร์ดแวร์ที่เห็นตามภาพประกอบไปด้วยเครื่องพีซีที่ทำหน้าที่เป็นเครื่องแม่ข่ายจำลองในระบบหลัก ภายในตัวเครื่องแม่ข่ายจำลองประกอบไปด้วยเน็ตเวริค์การ์ด 2 การ์ด คือ eth0 กับ eth1 โดยคอนฟิกค่าไอพีแอดเดรสของการ์ด eth0 เป็นแบบพลวัตร (Dynamic DHCP) และ eth0 นี้เป็นส่วนที่ใช้ในการติดต่อกับอินเทอร์เน็ตภายนอก (outside network) eth1 เป็นส่วนที่ใช้ติดต่อกับเครือข่ายภายใน (inside network) ค่าไอพีแอดเดรสเป็นแบบคงที่ (static) คอนฟิกให้เป็นหมายเลขเครือข่ายภายในเฉพาะ (private ip) เชื่อมต่อเข้ากับอุปกรณ์กระจายสัญญาณ (switch) หลังอุปกรณ์กระจายสัญญาณคือบริเวณที่สามารถนำอุปกรณ์ที่ต้องการใช้งานอินเทอร์เน็ตมาเชื่อมต่อ อาทิเช่น เครื่องพีซี เครื่องคอมพิวเตอร์พกพา เครื่องกระจายสัญญาณอินเทอร์เน็ตแบบไร้สาย (WI-FI) เป็นต้น

4.3 ทดสอบการเข้าใช้งานโดยใช้ระบบทดสอบแบบเดิมก่อนพัฒนาระบบใหม่

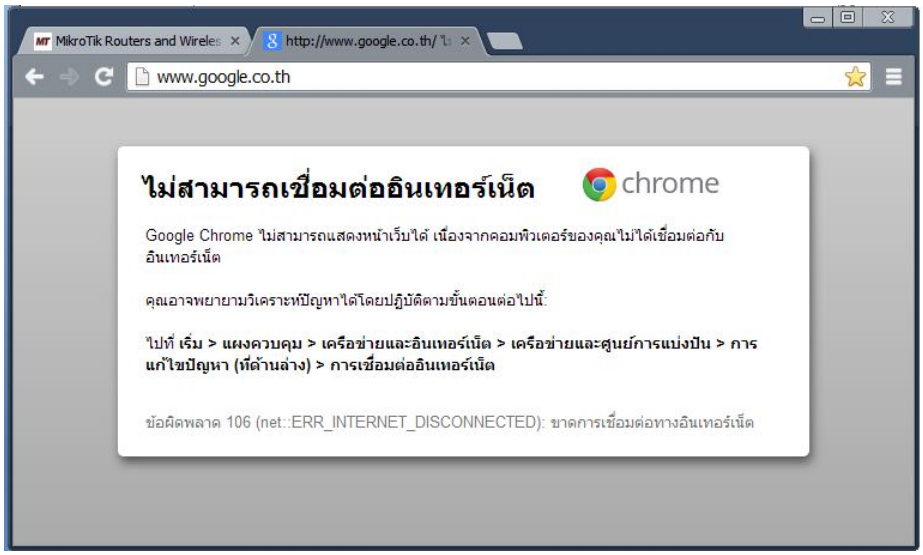
สำหรับการทดลองการใช้งานอินเทอร์เน็ตด้วยระบบเดิม (พรอกซี่) กระทำโดยแบ่งการทดสอบเป็นสองลักษณะคือ ใช้เครื่องพีซีต่อเข้ากับอุปกรณ์กระจายสัญญาณและเรียกใช้งานอินเทอร์เน็ตโดยการเปิดเว็บทั่วไป ผลการใช้งานเป็นไปด้วยดีการเข้าถึงเว็บไซต์มีความรวดเร็วตามรายละเอียดเนื้อหาและความสามารถของระบบที่มีพรอกซี่ที่ได้อธิบายไว้ในบทที่ 2 ทุกประการ โดยรายละเอียดขั้นตอนมีดังนี้

4.3.1 เชื่อมต่อเครื่องคอมพิวเตอร์ผ่านอุปกรณ์กระจายสัญญาณ (Switch) จากนั้นเปิดเครื่องแม่ข่ายแต่ไม่เปิดระบบพรอกซี่และเซอร์วิสอื่นๆที่ระบบนี้สร้างขึ้น ทดลองใช้เครื่องพีซีคอมพิวเตอร์เปิดเว็บเพ็จของ http://google.co.th ได้ผลดังนี้



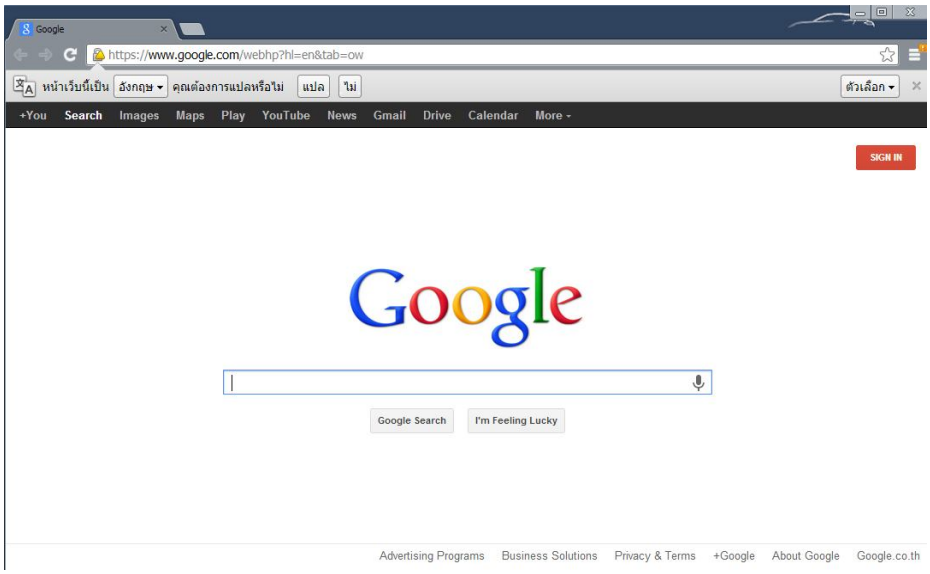
ภาพที่ 4-2 การทำงานของเว็บเพ็จ

ภาพที่ 4-2 แสดงผลการทำงานให้เห็นว่าระบบพรอกซี่ได้มีการทำงานถูกต้องแล้ว นั่นคือเมื่อทำการเปิดระบบที่สร้างขึ้นเพื่อให้บริการ แต่ไม่เปิดพรอกซี่ จะไม่สามารถเข้าถึงอินเทอร์เน็ตได้ดังภาพที่ 4-2 เหตุเพราะว่าตัวระบบเองได้มีการคอนฟิกค่าไว้แล้วว่าหากเครื่องคอมพิวเตอร์ใดเปิดเบราว์เซอร์เรียกเว็บเพ็จใดๆก็ตาม ระบบจะบังคับให้สัญญาณวิ่งมาถามหรือมาผ่านที่พรอกซี่ก่อนเสมอ จากนั้นพรอกซี่จึงจะส่งต่อการทำงานให้ทำงานได้สมบูรณ์ต่อไป แต่เมื่อระบบไม่ได้เปิดจึงทำให้เกิดอาการที่เรียกว่าเพ็จผิดพลาดหรือ error page ไม่สามารถเชื่อมต่อระบบอินเทอร์เน็ตได้ ผลจากการทำงานที่ได้จึงมีผลต่อการทดสอบการดาวน์โหลดโปรแกรมผ่านหน้าเว็บไปโดยปริยาย เพราะเมื่อไม่สามารถเข้าถึงหน้าเว็บเพ็จใดๆได้ การดาวน์โหลดก็ไม่สามารถกระทำได้ไปโดยอัตโนมัติ ดังนั้นผลการดาวน์โหลดในขั้นตอนนี้จึงไม่มีผลใดๆ และสามารถเข้าดูรายงานสภาวะจากล็อกไฟล์ที่รายงานโดยระบบปฏิบัติการลินุกซ์ด้วยคำสั่ง # tail –f /var/log/squid/access.log ระบบจะรายงานผลว่าไม่สามารถเชื่อมต่ออินเทอร์เน็ตได้ ดังภาพ



ภาพที่ 4- 3 รายงานที่ได้จากระบบปฏิบัติการลินุกซ์

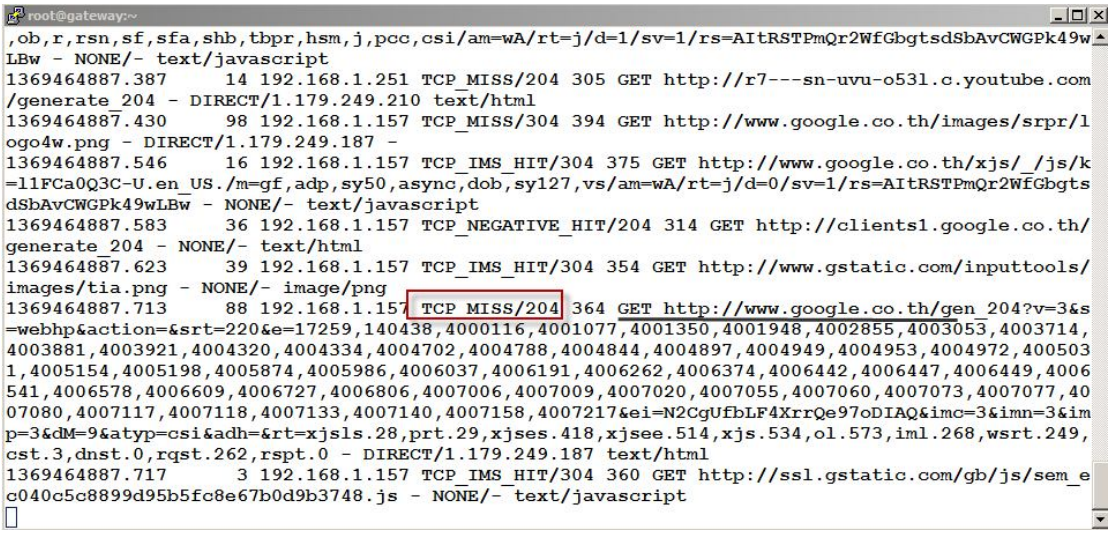
4.3.2 ครั้งที่สองทำเหมือนเดิม โดยครั้งนี้เปิดระบบให้บริการเฉพาะพรอกซี่แต่ยังคงปิดเซอร์วิสในส่วนอื่นไว้ ทดลองใช้โปรแกรมเว็บเบราว์เซอร์เปิดเว็บเพ็จ ผลที่ได้แสดงดังภาพ



ภาพที่ 4-4 การแสดงผลเมื่อเปิดบริการสควิดพรอกซี่

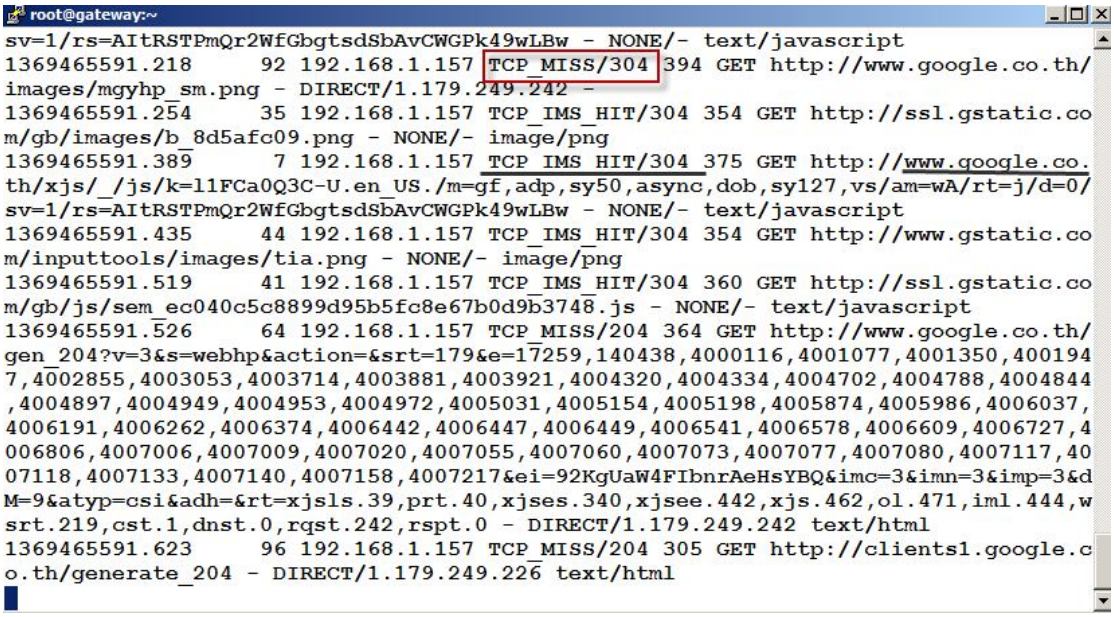
จากภาพที่ 4-4 เว็บเบราว์เซอร์สามารถแสดงผลหน้าเว็บเพ็จที่เรียกไปได้ครบสมบูรณ์ ไม่มีข้อความแสดงความผิดพลาดใดๆ นั่นก็เป็นการแสดงให้เห็นว่าการทำงานของพรอกซี่มีผลทำให้เว็บเพจแสดงผลได้หรือแสดงผลไม่ได้ ดังผลการทดลองในข้อที่ 4.3.1 เว็บเพจไม่แสดงผลเนื่องจากปิดบริการของพรอกซี่ และเมื่อเข้าดูเข้าดูรายงานสภาวะจากล็อกไฟล์ที่รายงานโดยระบบปฏิบัติการลิ

นุกซ์ด้วยคำสั่ง # tail –F /var/log/squid/access.log ระบบจะรายงานผลการเชื่อมต่ออินเทอร์เน็ตได้ ดังภาพที่ 4-5



ภาพที่ 4-5 รายงานแสดงการเชื่อมต่ออินเทอร์เน็ต

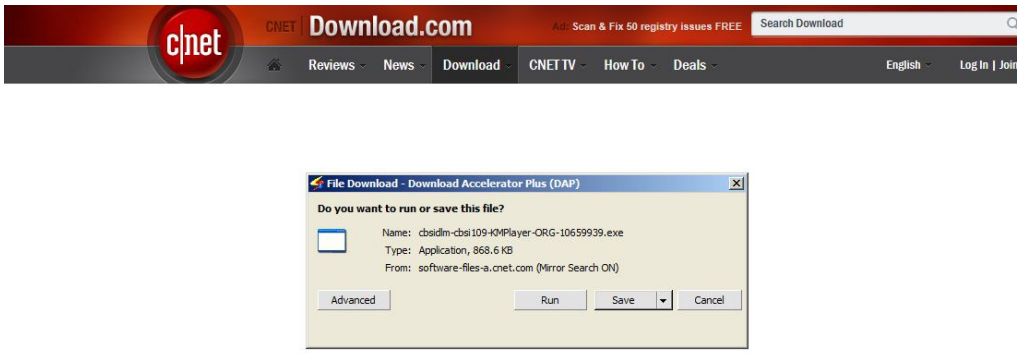
จากภาพที่ 4-5 จะพบว่ารายงานแสดงข้อความการเชื่อมต่อกับเว็บไซต์ปลายทาง http://www.google.co.th (ขีดเส้นใต้สีดำ)ได้สำเร็จ โดยแสดงเป็นชื่อของเว็บไซต์และไอพีแอดเดรสของเครื่องพีซีที่ติดต่อไปยังเว็บไซต์ จุดที่ควรสังเกตคือ บรรทัดนี้จะมีคำว่า TCP_IMS_MISS อยู่ท้ายบรรทัด หมายความว่าถ้ามีการเข้าถึงเว็บไซต์นี้เป็นครั้งแรกระบบจะยังไม่มีการเก็บแคชของเว็บเนื่องจากเพิ่งเข้ามาเป็นครั้งแรก การเข้าถึงเว็บจึงต้องมีการส่งคำร้องขอออกไปยังภายนอก หากมีการเรียกไปแล้วหนึ่งครั้งระบบจะทำการแคชเก็บไว้ในเครื่องแม่ข่าย ในครั้งหน้าหากมีเครื่องพีซีใดเรียกเว็บ google อีกระบบจะสามารถเข้าถึงได้เร็วขึ้นโดยไม่ต้องร้องขอที่อยู่เว็บออกไปข้างนอกเครือข่าย ผลจากการกระทำนี้หากมีแคชอยู่แล้วในระบบค่าในบรรทัดนี้จะแสดงสถานะเป็นคำว่า TCP_IMS_HIT สรุปก็คือ ถ้าไม่มีแคชอยู่ในเครื่องแม่ข่ายระบบจะแจ้งว่า TCP_IMS_MISS แต่ถ้าพบหรือมีแคชระบบจะแจ้งว่า TCP_MIS_HIT ดังนั้นเพื่อให้เห็นภาพการทำงานและการเปลี่ยนแปลงที่มีผลมาจากการเปิดบริการของพรอกซี่ การทดสอบเพื่อให้เห็นผลกระทำโดยพิมพ์ชื่อเว็บไซต์หลายๆที่ต่างๆกัน สลับกับการเรียกไปยังเว็บไซต์เดิมที่เคยเปิดไปแล้วโดยจะกี่ครั้งก็ได้ ซึ่งจำนวนครั้งจะไม่ได้เป็นตัวแปรในเรื่องความถี่ เพียงแต่ขอให้มีการเรียกซ้ำไปที่เว็บไซต์เดิมที่เคยเปิดไปแล้วเพื่อดูว่ามีการเก็บแคชไว้หรือไม่ ซึ่งหลังจากทำการเปิดเว็บเรียบร้อยแล้วให้เข้าดูรายงานสภาวะจากล็อกไฟล์ที่รายงานโดยระบบปฏิบัติการอีกครั้งด้วยคำสั่ง # tail –F /var/log/squid/access.log ระบบจะรายงานผลการเชื่อมในครั้งใหม่ ดังภาพที่ 4-6



ภาพที่ 4-6 ภาพแสดงผลการเชื่อมต่อครั้งใหม่

สังเกตว่าในการทดลองครั้งนี้จะพบว่าบริเวณท้ายบรรทัดของรายงานจะแสดงทั้งคำว่า TCP_MISS (กรอบสี่เหลี่ยมสีแดง) และคำว่า TCP_IMS_HIT (ขีดเส้นใต้สีดำ) ซึ่งคำว่า HIT หมายถึงเว็บที่เคยไปมาแล้วจะมีการเก็บแคชไว้เมื่อมีการเรียกซ้ำระบบจะจัดส่งที่อยู่ให้โดยไม่ต้องร้องขอออกไปยังนอกระบบซึ่งจะทำให้การเชื่อมต่อไปยังเว็บปลายทางมีความเร็วในการเข้าถึงเร็วกว่าในครั้งแรก

4.3.3 สำหรับการทดลองถัดมานั้น ทำการทดลองเปิดเว็บไซต์ที่ให้บริการดาวน์โหลด เพื่อทำการดาวน์โหลดผ่านหน้าเว็บไซต์ ผลการทดลองแสดงได้ดังภาพที่ 4-7 ผลการทดลองดาวน์โหลดแสดงให้เห็นว่ากระบวนการดาวน์โหลดทำงานได้เป็นปกติไม่ติดปัญหาใดๆ เช่นเดียวกับการเปิดเว็บเพจทุกประการ



ภาพที่ 4-7 การดาวน์โหลดผ่านหน้าเว็บไซต์

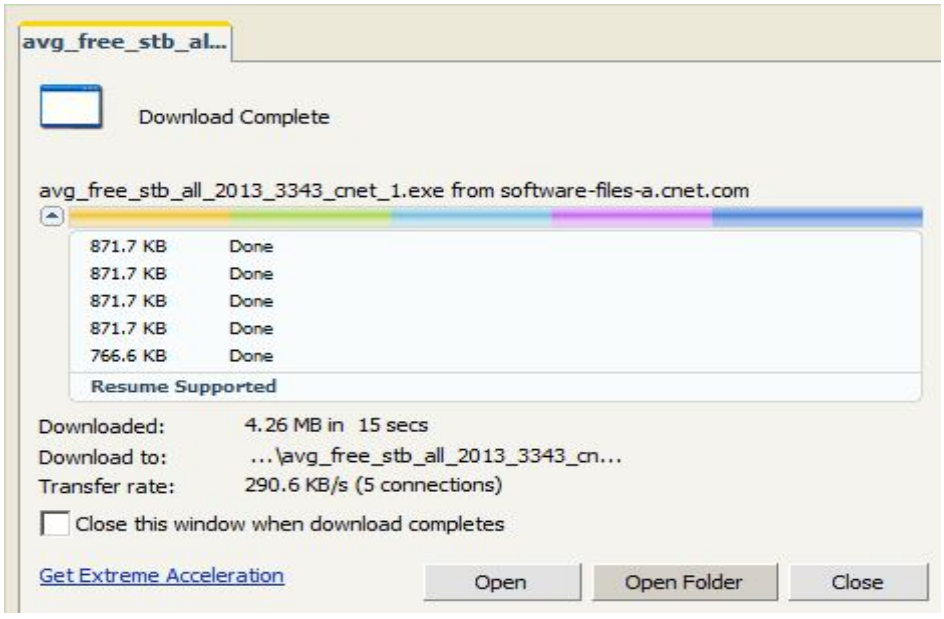
4.4 ทดสอบการเข้าใช้งานด้วยระบบใหม่ที่พัฒนาขึ้น

สำหรับการทดสอบระบบด้วยระบบใหม่ที่พัฒนาขึ้น มีความแตกต่างจากระบบเดิมในเรื่องของการบริการเก็บแคชไฟล์สำหรับการดาวน์โหลดไว้ในเครื่องแม่ข่าย ดังนั้นผลการทดลองจะให้ผลในเรื่องความเร็วในการเข้าถึงเว็บไซต์ได้เช่นเดียวกันกับระบบเดิม รวมถึงวิธีการตรวจสอบก็ใช้แบบเดียวกัน ยกเว้นเรื่องของการดาวน์โหลดจะให้ผลลัพธ์ที่แตกต่างจากระบบเดิมโดยสรุปผลภาพรวม ได้ดังนี้

4.4.1 ทำการเปิดเซอร์วิสของระบบใหม่ที่พัฒนาขึ้น

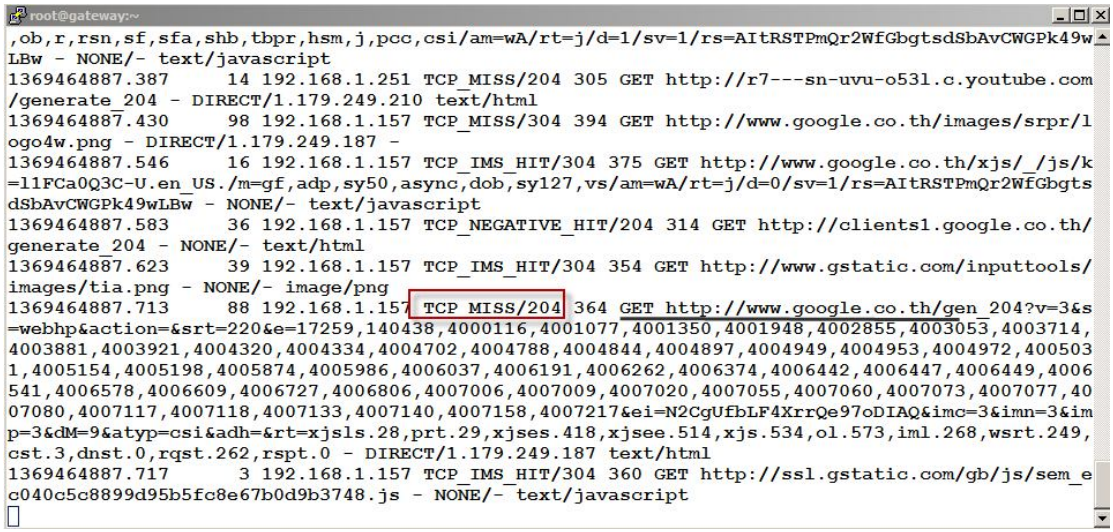
4.4.2 ทดสอบใช้อินเทอร์เน็ตโดยการเปิดเว็บไซต์เหมือนการทดลองที่ผ่านมา ผลการเข้าถึงเว็บไซต์ยังคงให้ผลเหมือนกับระบบเดิมทุกประการ นั่นคือหากเปิดเว็บไซต์ใดๆในครั้งแรก ระบบจะยังไม่มีการแคชไว้ ดังนั้นหากดูผลและร่องรอยก็จะได้ผลลัพธ์คือ TCP_MISS เหมือนกับการทดลองในครั้งต้น หากมีแคชอยู่แล้วผลลัพธ์ของร่องรอยก็จะได้เป็น TCP_MIS_HIT เช่นกัน ซึ่งผลการทดลองในขั้นนี้จะไม่ขอแสดงรูปภาพการทำงานเนื่องจากจะซ้ำซ้อนกับในส่วนที่ผ่านมา

4.4.3 ผลการทดสอบที่สำคัญในขั้นนี้ดังที่บอกไปแล้วคือ จะมีการเปิดเซอร์วิสแคชของการดาวน์โหลดเพิ่มเข้ามา ผลการเปิดเซอร์วิสนี้ทำให้ระบบมีการเปลี่ยนแปลง โดยทดลองดาวน์โหลดไฟล์จากหน้าเว็บไซต์ที่มีบริการให้ดาวน์โหลดไฟล์ฟรี ซึ่งเว็บไซต์เหล่านี้จะให้บริการไฟล์หรือแอปพลิเคชั่นต่างๆที่ขนาดไฟล์แตกต่างกันออกไปทั้งไฟล์ขนาดเล็กและขนาดใหญ่ โดยความเร็วในการให้บริการดาวน์โหลดก็ต่างกันออกไปด้วย ส่งผลให้ความอัดแน่นของเครือข่ายมีสะสมเป็นอย่างมากหากในหน่วยงานมีผู้ใช้ดาวน์โหลดพร้อมๆกันจำนวนมาก ทำให้ประสิทธิภาพของระบบอินเทอร์เน็ตตกลงหรือที่เราเรียกกันว่า อินเทอร์เน็ตช้า การทดลองเริ่มโดยการดาวน์โหลดไฟล์โดยไม่คำนึงถึงข้อจำกัดเรื่องความเร็วของการให้บริการ ดังภาพที่ 4-8



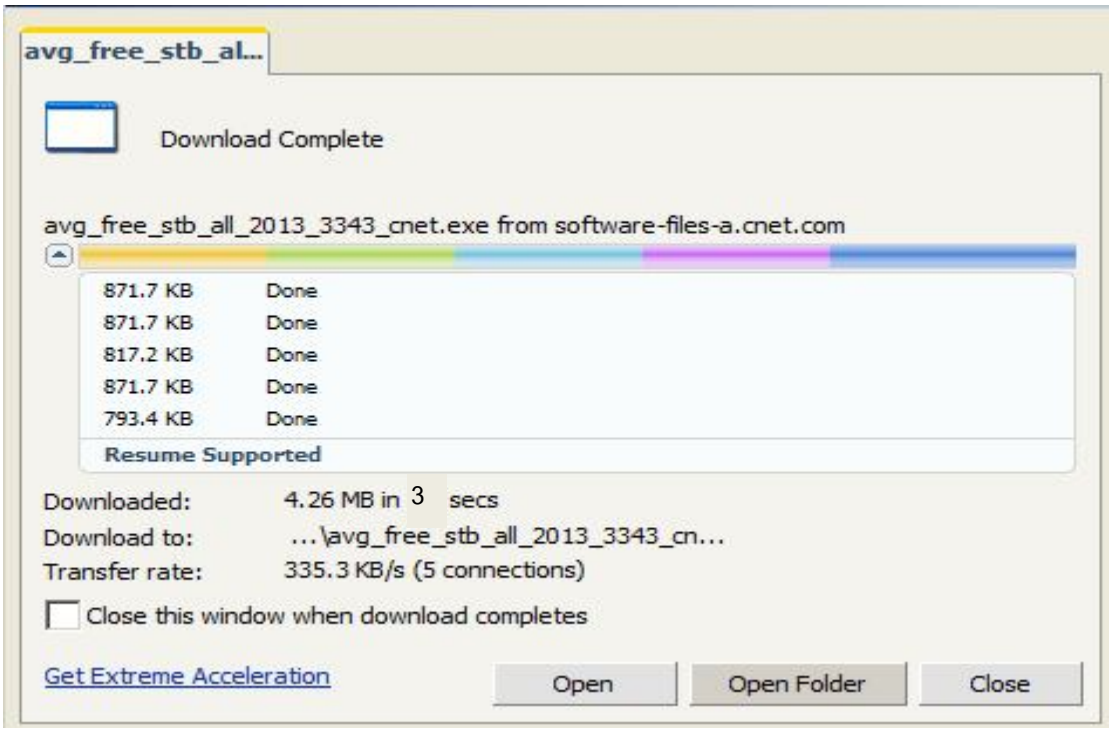
ภาพที่ 4-8 การดาวน์โหลดผ่านหน้าเว็บไซต์กรณีไม่มีแคช

ผลการทดลองจากภาพที่ 4-8 แสดงให้เห็นว่าการดาวน์โหลดไฟล์ขนาด 4.26 MB ทำงานได้เสร็จสมบูรณ์โดยไม่มีการเก็บแคช ใช้เวลาทั้งสิ้น 15 วินาที (15 secs) โดยหากเข้าดูร่องรอยการทำงานด้วยคำสั่งเดียวกันกับระบบเดิมคือ # tail –f /var/log/squid/access.log ก็จะพบข้อมูลการเข้าถึงแบบไม่มีแคชว่า TCP_MISS ดังภาพที่ 4-9



ภาพที่ 4-9 ร่องรอยการดาวน์โหลดผ่านหน้าเว็บไซต์กรณีไม่มีแคช

จากนั้นทำการดาวน์โหลดไฟล์เดิม ขนาดเท่าเดิม จากเว็บเดิม อีกครั้ง ผลลัพธ์ที่ได้คือความเร็วในการดาวน์โหลดครั้งนี้ใช้เวลาเพียง 3 วินาที ซึ่งแสดงให้เห็นว่ามีความเร็วกว่าครั้งแรกมาก เนื่องมาจากมีการเก็บแคชไว้แล้วในเครื่องแม่ข่ายเพราะเฉพาะนั้นในการดาวน์โหลดครั้งถัดมาจึงไม่ต้องดาวน์โหลดนอกเครือข่ายแต่จะดึงเอาจากเครื่องแม่ข่ายภายใน ซึ่งจะมีความเร็วกว่าเดิมส่วนจะมากน้อยในแต่ละครั้งอาจไม่เท่ากันเนื่องมาจากปัจจัยภายใน เช่น ความหนาแน่นของเครือข่ายภายในเอง แต่อย่างไรก็จะเร็วกว่าการดาวน์โหลดจากภายนอกเป็นอย่างมาก และผลการดูร่องรอยครั้งนี้ด้วยคำสั่ง # tail –f /var/log/squid/access.log ก็จะพบข้อมูลการเข้าถึงแบบมีการเก็บแคชว่า TCP_MIS_HIT ซึ่งความหมายของ HIT คือพบไฟล์ในแคชดังอธิบายความหมายไปแล้วในเบื้องต้น ผลการดาวน์โหลด ดังภาพที่ 4-10



ภาพที่ 4-10 การดาวน์โหลดผ่านหน้าเว็บไซต์กรณีมีแคช

ภาพที่ 4-10 แสดงให้เห็นว่าการดาวน์โหลดในครั้งที่สองทำได้เร็วกว่าเดิม นั่นหมายความว่าเมื่อการดาวน์โหลดทำเสร็จได้เร็วเท่าใดความหนาแน่นในระบบเครือข่ายภายในก็จะลดลงมากเท่านั้น

4.5 เปรียบเทียบการใช้งานระบบเก่ากับระบบที่พัฒนาขึ้นใหม่

เพื่อให้เปรียบเทียบให้เห็นความแตกต่างของระบบใหม่ที่พัฒนาขึ้นกับระบบแบบเดิม การทดลองทำโดยใช้ระบบเดิมและระบบใหม่ทำการดาวน์โหลดไฟล์ขนาดต่างๆกัน จำนวน 10 ไฟล์ จากเว็บไซต์เดียวกัน เพื่อป้องกันความแตกต่างทางด้านความเร็วของเว็บที่ให้บริการซึ่งมีความเร็วในการให้บริการที่แตกต่างกัน รายละเอียดดังแสดงไว้ในตารางที่ 4-1

ตารางที่ 4-1 รายละเอียดไฟล์ที่ใช้ดาวน์โหลด

ลำดับที่	ขนาดไฟล์ (เมกกะไบต์)
1	34
2	12
3	16
4	59

ลำดับที่	ขนาดไฟล์ (เมกกะไบต์)
5	15
6	18
7	55
8	62
9	56
10	12.67

จากนั้นใช้ข้อมูลในตารางที่ 4-1 ทำการทดสอบระบบ โดยเปิดระบบแบบเดิมคือมีพรอกซี่อย่างเดียว แต่ปิดเซอร์วิสของการดาวน์โหลดที่มีอยู่ในระบบใหม่ แล้วทำการทดสอบดาวน์โหลดไฟล์ตั้งแต่ไฟล์ที่ 1 ถึง ไฟล์ที่ 10 ผลการดาวน์โหลดด้วยระบบเดิม (ใช้พรอกซี่เพียงอย่างเดียว) แสดงในตารางที่ 4-2

ตารางที่ 4-2 ผลการดาวน์โหลดด้วยระบบเดิม

ลำดับที่	ขนาดไฟล์ (เมกกะไบต์)	เวลาที่ใช้ดาวน์โหลด (นาที)
1	34	4
2	12	2.10
3	16	2.15
4	59	4.40
5	15	1.30
6	18	1.20
7	55	5.10
8	62	5.40
9	56	5.25
10	12.67	1.15

ขั้นตอนต่อมาใช้ข้อมูลในตารางที่ 4-1 เช่นเดียวกัน ทำการทดสอบระบบ โดยเปิดระบบแบบเดิมคือมีพรอกซี่อย่างเดียว และเปิดเซอร์วิสของการดาวน์โหลดที่มีอยู่ในระบบใหม่ด้วย แล้วทำการทดสอบดาวน์โหลดไฟล์ตั้งแต่ไฟล์ที่ 1 ถึง ไฟล์ที่ 10 ผลการดาวน์โหลดด้วยระบบเดิมพร้อมเปิดเซอร์วิสของระบบใหม่ (มีพรอกซี่และเซอร์วิสของการดาวน์โหลด) ดังที่ได้แสดงให้ดูไปแล้วในขั้นตอนการเปิดระบบใหม่ว่า เมื่อจะใช้ระบบใหม่ต้องใช้คำสั่ง ดังนี้

หากต้องการหยุดการทำงานใช้คำสั่ง # service Frox stop

หากต้องการเริ่มการทำงานใช้คำสั่ง # service Frox start

ผลการทดสอบดังแสดงในตารางที่ 4-3

ตารางที่ 4-3 ผลการดาวน์โหลดด้วยระบบใหม่

ลำดับที่	ขนาดไฟล์ (เมกกะไบต์)	เวลาที่ใช้ดาวน์โหลด (นาที)
1	34	0.08
2	12	0.05
3	16	0.05
4	59	0.11
5	15	0.06
6	18	0.06
7	55	0.33
8	62	0.46
9	56	0.36
10	12.67	0.05

ผลการทดสอบในตารางที่ 4-3 เห็นได้อย่างชัดเจนว่า เมื่อมีการเปิดเซอร์วิสของระบบใหม่ การดาวน์โหลดไฟล์ทั้ง 10 ไฟล์ สามารถกระทำได้เสร็จสิ้นโดยใช้เวลาสั้นกว่าระบบเดิมเป็นอย่างมาก ตัวอย่างเช่น ไฟล์ที่ 8 ซึ่งมีขนาดใหญ่ที่สุด ใช้เวลาในการดาวน์โหลดเพียง 0.46 นาที เท่านั้น ขณะที่ระบบเดิมใช้เวลาดาวน์โหลดนานถึง 5.40 นาที

และเพื่อให้เห็นความแตกต่างของทั้งสองระบบอย่างชัดเจน ผู้วิจัยจึงทำการสร้างตารางเปรียบเทียบความเร็วในการดาวน์โหลดระหว่างระบบเดิมกับระบบใหม่ โดยแสดงไว้ในตารางที่ 4-4

ตารางที่ 4-4 ผลการดาวน์โหลดเปรียบเทียบระบบเดิมกับระบบใหม่

ลำดับที่	**ขนาดไฟล์ (เมกกะไบต์)**	**เวลาที่ใช้ดาวน์โหลด (นาที)**	
		ระบบเดิม	ระบบใหม่
1	34	4	0.08
2	12	2.10	0.05
3	16	2.15	0.05
4	59	4.40	0.11
5	15	1.30	0.06
6	18	1.20	0.06
7	55	5.10	0.33
8	62	5.40	0.46
9	56	5.25	0.36
10	12.67	1.15	0.05
ค่าเฉลี่ย (Average)	33.96	3.20	0.16

ในกระบวนการทดสอบในขั้นสุดท้าย เพื่อทดสอบความเสถียรของระบบในการใช้งานของระบบใหม่ที่พัฒนาขึ้น ตารางที่ 4-5 แสดงการดาวน์โหลดข้อมูลโดยใช้ไฟล์ขนาด 34 เมกกะไบต์ ทดสอบดาวน์โหลดซ้ำ จำนวน 20 ครั้ง และทำการบันทึกความเร็วในการทำงาน ค่าเฉลี่ย รวมถึงค่าความสำเร็จที่เรียกว่า TCP_MIS_HIT ผลที่ได้ดังแสดงในตารางที่ 4-5

ตารางที่ 4-5 ผลการดาวน์โหลดด้วยระบบใหม่จำนวน 20 ครั้ง

ลำดับที่	**ขนาดไฟล์ (เมกกะไบต์)**	**เวลาที่ใช้ดาวน์โหลด (นาที)**	**TCP_MIS_HIT**
1	34	0.08	1
2	34	0.08	1
3	34	0.08	1

ลำดับที่	ขนาดไฟล์ (เมกกะไบต์)	เวลาที่ใช้ดาวน์โหลด (นาที)	TCP_MIS_HIT
4	34	0.08	1
5	34	0.08	1
6	34	0.08	1
7	34	0.08	1
8	34	0.08	1
9	34	0.08	1
10	34	0.09	1
11	34	0.08	1
12	34	0.08	1
13	34	0.08	1
14	34	0.09	1
15	34	0.08	1
16	34	0.08	1
17	34	0.08	1
18	34	0.08	1
19	34	0.08	1
20	34	0.08	1
ค่าเฉลี่ย (Average)		0.081	
เปอร์เซ็นต์ความถูกต้อง			100

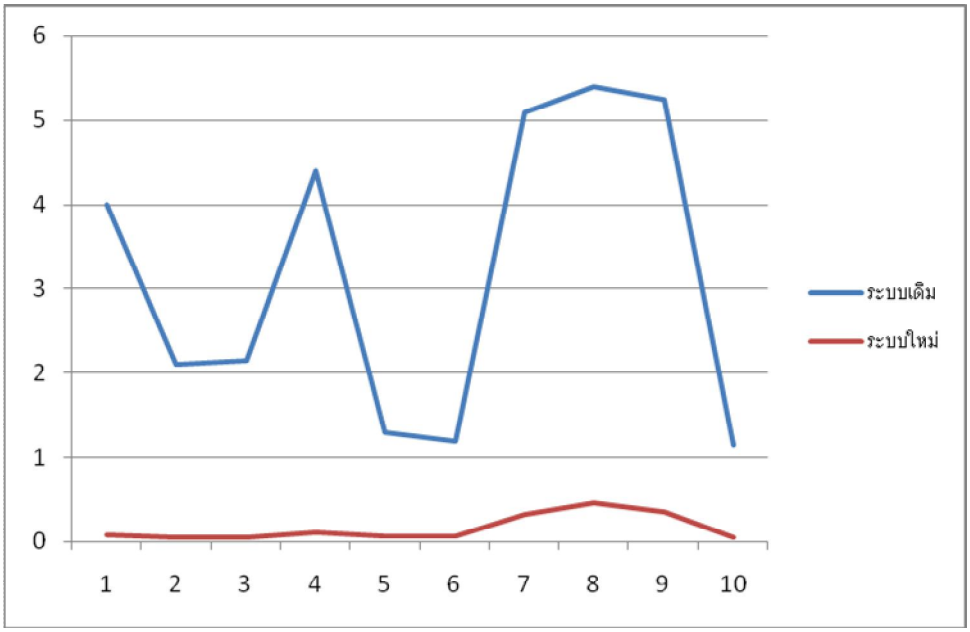
ผลลัพธ์ที่ได้จากการทดสอบดังแสดงไว้ในตารางที่ 4-5 พบว่าความเร็วในการดาวน์โหลดทั้ง 20 ครั้ง มีค่าค่อนข้างไม่เปลี่ยนแปลง นั่นคือมีค่าเท่ากับ 0.08 นาที มีเพียงบางค่าคือลำดับที่ 10 และ 14 เท่านั้นที่มีค่าเวลาที่ใช้ในการดาวน์โหลดเท่ากับ 0.09 ซึ่งใช้เวลามากกว่าการดาวน์โหลดในลำดับอื่นๆ ซึ่งค่าที่มากกว่านี้เกิดขึ้นจากความหนาแน่นของเครือข่ายภายในระบบเอง บางเวลาอาจมีการหน่วง (Relay) หรือติดขัดภายในตัวอุปกรณ์เอง แต่โดยเฉลี่ยแล้วความเร็วก็ยังคงไม่แตกต่างจากการดาวน์โหลดโดยรวมซึ่งมีค่าเฉลี่ยเท่ากับ 0.081 และจากการทดลองนี้ยังแสดงให้เห็นถึงความน่าเชื่อถือของระบบที่พัฒนาขึ้นว่าสามารถใช้งานได้อย่างแม่นยำถูกต้องในทุกๆครั้งของการใช้งานโดยดูจากค่าของ HIT RATE ในคอลัมน์ขวาสุดของตารางที่ 5 ค่า TCP_MISS_HIT หรือค่าที่บ่งบอกว่ามีการพบข้อมูลอยู่ภายในแคชของเครื่องแม่ข่าย (พบ มีค่าเท่ากับ 1 ไม่พบมีค่าเท่ากับ 0) สังเกตว่าค่าตั้งแต่ลำดับที่ 1 ถึง 20 มีค่าเท่ากับ 1ทั้งหมด ซึ่งหมายความว่าการดาวน์โหลดพบข้อมูลในแคชทุกครั้ง คิดเป็นเปอร์เซ็นต์ได้ดังนี้

กำหนดให้ค่า (TCP_MISS_HIT) = TMH
จำนวนครั้งของการทดลองดาวน์โหลด = N

$$\text{HIT RATE} = \frac{\sum_{1}^{N} TMH}{N} \times 100$$

$$\text{ดังนั้นเปอร์เซ็นต์ของ HIT RATE} = \frac{20}{20} \times 100 = 100$$

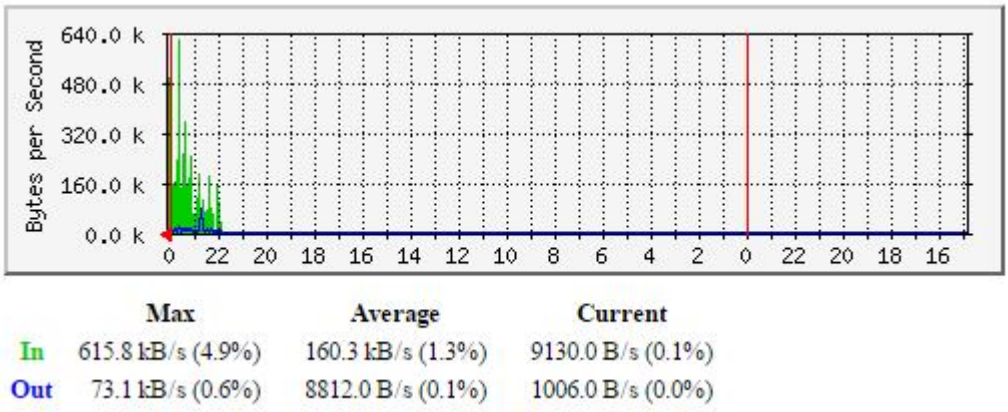
จากผลลัพธ์ของ HIT RATE ที่มีค่าเท่ากับ 100 เปอร์เซ็นต์แสดงให้เห็นว่าความเสถียรจากการใช้งานระบบใหม่มีความน่าเชื่อถือมากซึ่งรวมไปถึงระบบมีความเที่ยงตรงสม่ำเสมอต่อการให้บริการอีกด้วย



ภาพที่ 4-11 กราฟแสดงความเร็วที่ใช้ในการดาวน์โหลดระหว่างระบบเดิมกับระบบใหม่

นอกจากนั้นกราฟภาพที่ 4-11 ยังแสดงให้เห็นได้อย่างชัดเจนว่าความเร็วในการโหลดข้อมูลของระบบใหม่ที่พัฒนาขึ้นนั้นเร็วกว่าระบบเดิม โดยรายละเอียดของภาพที่ 4-6 นั้นใช้ข้อมูลการดาวน์โหลดข้อมูลของระบบเดิมกับระบบใหม่ในสองคอลัมน์สุดท้ายของตารางที่ 4-4 มาทำการสร้างกราฟเพื่อเปรียบเทียบให้เห็นความเร็วที่แตกต่างกันได้อย่างชัดเจน เส้นกราฟสีน้ำเงินหมายถึงระบบเดิม เส้นกราฟสีแดงหมายถึงระบบใหม่ ตัวเลขในแกนแนวนอน เช่น 1, 2, 3, 4, ...,10 คือจำนวนครั้งหรือครั้งที่ที่ทำการดาวน์โหลด ส่วนตัวเลขในแกนแนวตั้งของกราฟ เช่น 1, 2, 3, 4, ...,6 เป็นค่าของเวลา (นาที) ตัวอย่างเช่น เลข 1 หมายถึงการดาวน์โหลในครั้งนั้นใช้เวลาไป 1 นาที และถ้าดูจากในกราฟครั้งที่ 1 การดาวน์โหลดของระบบเดิม (สีน้ำเงิน) ใช้เวลาไปทั้งสิ้น 4 นาที ส่วนการดาวน์โหลดด้วยระบบใหม่ (สีแดง) ใช้เวลาไปทั้งสิ้น 0.08 นาที จากรายละเอียดของกราฟในภาพที่4-6 นั้นสามารถบอกได้ว่าระบบใหม่ที่พัฒนาขึ้นสามารถให้ผลลัพธ์การทำงาน คือการดาวน์โหลดข้อมูลได้เร็วกว่าระบบเดิมในทุกๆครั้งของการทดสอบ (10 ครั้ง)

ผลจากการทำงานของระบบที่พัฒนาขึ้นยังสามารถแสดงให้เห็นถึงประสิทธิภาพได้ชัดเจนว่าสามารถลดปริมาณข้อมูลที่มีอยู่ในระบบเครือข่ายได้ดี โดยดูจากกราฟ (MRTG) แสดงปริมาณข้อมูลของการเข้าใช้อินเทอร์เน็ตในภาพที่ 4-12



ภาพที่ 4-12 กราฟ MRTG

สำหรับภาพที่ 4-12 เป็นกราฟที่เกิดจากการสร้างด้วยโปรแกรมที่เรียกว่า MRTG ซึ่งมีอยู่แล้วในระบบปฏิบัติการลินุกซ์ สีเขียวที่ปรากฏในกราฟหมายถึงปริมาณข้อมูลที่มีการวิ่งเข้ามาในเครือข่าย ส่วนสีน้ำเงินหมายถึงข้อมูลที่มีการร้องขอออกไปภายนอก ถ้าสีน้ำเงินมีมากแสดงว่าความหนาแน่นของข้อมูลภายในมีมากหรือที่เรียกว่าช่องสัญญาณแน่น ทำให้อินเทอร์เน็ตมีอาการช้าลง ดังนั้นถ้าดูจากภาพที่ 4-12 จะพบว่าสีน้ำเงินมีอยู่เล็กน้อยโดยจะสูงในช่วงสั้นๆซึ่งหมายถึงตอนที่มีการดาวน์โหลดครั้งแรกจำเป็นต้องร้องขอข้อมูลออกไปภายนอกเครือข่าย แต่พอครั้งต่อๆมาสีน้ำเงินจะลดลงจนแถบไม่มีการสูงขึ้นอีกเลย นั่นหมายความว่าการร้องขอข้อมูลออกไปภายนอกมีน้อยเพราะระบบที่พัฒนาขึ้นได้ทำการเก็บแคชไว้แล้วภายในเครือข่ายเอง จึงไม่ต้องร้องขอออกไปภายนอกและทำให้ช่องสัญญาณของเครือข่ายภายในไม่มีความหนาแน่นหรือช่องสัญญาณว่างมากขึ้น

จากการเปรียบเทียบผลลัพธ์ของการทดสอบระบบทั้งหมดในบทนี้ ซึ่งแสดงไว้เป็นตารางตัวเลขโดยแบ่งเป็นรายละเอียดของไฟล์ทั้งหมดที่ใช้ในการทดสอบดังแสดงไว้ในตารางที่ 4-1 ผลการทดสอบด้วยระบบเก่าในตารางที่ 4-2 ผลการทดสอบด้วยระบบใหม่ในตารางที่ 4-3 ผลการเปรียบเทียบระหว่างระบบเก่ากับระบบใหม่แสดงไว้ในตารางที่ 4-4 รวมถึงผลการทดสอบเพื่อให้เห็นความเที่ยงตรงของระบบใหม่ที่พัฒนาขึ้น โดยรายละเอียดแสดงไว้ในตารางที่ 4-5 นอกจากนั้นเพื่อให้เห็นภาพความแตกต่างของผลลัพธ์ที่ได้จากระบบเก่าและระบบใหม่ การทดสอบนี้ได้แสดงความแตกต่างด้วยกราฟเส้น โดยรายละเอียดแสดงไว้ในภาพที่ 4-11 ซึ่งผลการทดสอบทั้งหมดสามารถสรุปได้ว่าระบบใหม่ที่พัฒนาขึ้น คือ ระบบเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยระบบปฏิบัติการลินุกซ์ นั้นสามารถให้ผลลัพธ์การทำงานที่ดีกว่าระบบเดิม คือระบบที่มีเพียงพรอกซี่อย่างเดียวทุกประการรวมถึงมีความแม่นยำสามารถนำไปใช้บริหารจัดการระบบอินเทอร์เน็ตเพื่อลดความหนาแน่นของข้อมูลได้ดังสมมุติฐานงานวิจัยที่ตั้งไว้

บทที่ 5
สรุป อภิปรายผล และข้อเสนอแนะ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อนำเสนอแนวทางในการจัดทำระบบเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยระบบปฏิบัติการลินุกซ์ ที่สามารถใช้งานได้จริงและสอดคล้องกับสมมุติฐานที่ตั้งไว้ ซึ่งระบบที่จัดทำขึ้นในครั้งนี้ใช้แนวทางเพื่อให้ได้ระบบที่มีประสิทธิภาพแต่มีความประหยัด เพราะลงทุนน้อยแต่สามารถทำให้ได้ระบบที่มีความรวดเร็ว เนื่องมาจากใช้ซอฟต์แวร์ที่สามารถหาได้ง่าย โดยเฉพาะใช้ระบบปฏิบัติการที่เป็นซอฟต์แวร์รหัสเปิดหรือที่รู้จักกันในนามโอเพ่นซอร์ส (Open Source) ที่ชื่อลินุกซ์ (Linux) ลินุกซ์เป็นซอฟท์แวร์ที่ได้รับความนิยมอย่างสูงในปัจจุบันและที่สำคัญนั้น ลักษณะของโอเพ่นซอร์สเป็นซอร์ฟแวร์ที่ทางผู้พัฒนาทำการแจกจ่ายให้ใช้ได้ฟรี ไม่มีค่าลิขสิทธิ์ใดๆ แต่มีประสิทธิภาพสูงเนื่องจากมีลักษณะของการเปิดเผยซอร์สโค้ดที่เขียน หากผู้ใดต้องการแก้ไขหรือพัฒนาให้มีความสามารถมากขึ้นก็สามารถทำได้เพียงแต่เมื่อมีการแก้ไขแล้วต้องมีการบอกต่อและแจกจ่ายให้คนอื่นได้ใช้ร่วมกันห้ามนำไปเพื่อทำการค้าหรือแอบอ้างเป็นเจ้าของโดยเด็ดขาด

จากการทดสอบระบบในบทที่ 4 แสดงให้เห็นว่าระบบใหม่ที่พัฒนาขึ้นภายใต้ชื่อระบบเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยระบบปฏิบัติการลินุกซ์นั้น ให้ผลการทำงานจากการวัดประสิทธิภาพในเรื่องความเร็วโดยวัดจากการทดลองดาวน์โหลดข้อมูลที่มีขนาดไฟล์ต่างกัน ให้ผลลัพธ์ที่ดีหรือเร็วกว่าการทำงานของระบบเดิมซึ่งมีเพียงระบบพรอกซี่เพียงอย่างเดียว ซึ่งปัจจัยที่ทำให้ระบบใหม่ดีกว่าระบบเดิมก็คือการที่ระบบใหม่มีการเพิ่มบริการด้านการทำแคชซึ่งระบบดาวน์โหลดของผู้ใช้ เมื่อผู้ใช้เข้าใช้อินเทอร์เน็ตโดยการสืบค้นข้อมูลบนหน้าเว็บผ่านโปรโตคอล HTTP ระบบจะถูกแคชไว้ในเครื่องแม่ข่ายพรอกซี่ (Proxy Server) นั่นคือความเร็วในการเข้าถึงเว็บไซต์จะมีความเร็วสูงในครั้งต่อๆไป แต่ไม่ครอบคลุมถึงเรื่องการดาวน์โหลด ความหมายก็คือหากผู้ใช้มีการดาวน์โหลดไฟล์ซึ่งส่วนใหญ่แล้วขนาดของการดาวน์โหลดไฟล์แต่ละครั้งไฟล์มักมีขนาดใหญ่กว่าการเข้าถึงเว็บไซต์ปกติ และเมื่อมีผู้ใช้จำนวนมากทำการดาวน์โหลดก็จะทำให้การครองครองช่องสัญญาณในระบบโดยใช้ระยะเวลาอยู่ในระบบนาน ทำให้ระบบเครือข่ายเกิดความหนาแน่นและประสิทธิภาพของอินเทอร์เน็ตตกลงในที่สุด ดังนั้นเมื่อนำระบบใหม่ที่พัฒนาเข้ามาใช้ ระบบใหม่จะทำการเก็บทั้งแคชของเว็บไซต์และเก็บแคชของการดาวน์โหลดเพิ่มเข้าไปด้วยจึงทำให้การทำงานของระบบใหม่มีประสิทธิภาพสามารถให้ความเร็วในการดาวน์โหลดเร็วมากส่งผลให้เวลาในการครอบครองช่องสัญญาณสื่อสารของผู้ใช้สั้นลง ความหมายก็คือหากผู้ใช้ทำงานใดในระบบอินเทอร์เน็ตนานเท่ากับว่าช่องสัญญาณจะถูกครอบครอง ประกอบกับเมื่อมีผู้ใช้เพิ่มมากขึ้นการครองครองช่องสัญญาณก็จะยิ่งมากขึ้น นานขึ้น หรือหนาแน่นขึ้น แต่เมื่อมีระบบใหม่การทำงานจะสั้นลงเนื่องจากระบบใหม่ทำให้งานนั้นๆเสร็จเร็วขึ้น ทำให้ปริมาณข้อมูลในระบบเครือข่ายลดลง ทำให้การวิจัยครั้งนี้เป็นไปตามวัตถุประสงค์ของงานวิจัยระบบเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยระบบปฏิบัติการลินุกซ์ทุกประการ

5.1 สรุปผลการวิจัย

ผลการวิจัยในครั้งนี้เป็นไปตามเป้าหมายและการออกแบบที่ออกแบบไว้ทุกประการ สามารถทำงานได้อย่างถูกต้องแม่นยำ สามารถจัดเก็บร่องรอยการใช้งานของผู้ใช้ได้ครบถ้วนตามวัตถุประสงค์ที่ตั้งไว้ และให้ความเร็วของระบบเพิ่มขึ้น ซึ่งสรุปผลการทำงานได้ดังนี้

ในระบบเครือข่ายเดิมก่อนติดตั้งระบบระบบเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยระบบปฏิบัติการลินุกซ์ นั้น ผู้ใช้งานสามารถเข้าใช้งานเครือข่ายอินเทอร์เน็ตได้ทันทีจากที่ใดก็ได้เพียงผู้ใช้มีอุปกรณ์ที่ใช้เชื่อมต่อ เช่น เครื่องพีซี หรือเครื่องคอมพิวเตอร์พกพา เชื่อมต่อด้วยสายหรือไร้สายก็ได้ โดยผู้ใช้สามารถเข้าถึงเว็บไซต์ใดๆด้วยความเร็วระดับหนึ่งโดยรู้สึกว่าการเข้าเว็บนั้นมีความเร็วค่อนข้างน่าพอใจ แต่เมื่อใดที่ทำการดาวน์โหลดจะรู้สึกว่าต้องรอนาน

เมื่อทำการติดตั้งระบบที่จัดทำขึ้นเพิ่มเข้าไปในระบบเดิมที่มีอยู่โดยทำการเพิ่มเครื่องคอมพิวเตอร์แม่ข่ายที่ได้ติดตั้งซอฟท์แวร์ที่จำเป็นต่างๆ ไว้ภายใน ทำให้ระบบมีการทำงานเปลี่ยนไปจากเดิม ดังนี้

เมื่อผู้ใช้เข้าใช้งานเครือข่ายอินเทอร์เน็ต ผู้ใช้จะรู้สึกว่าสามารถเข้าใช้งานอินเทอร์เน็ตได้อย่างรวดเร็วมากขึ้นกว่าเดิม ซึ่งเบื้องหลังของส่วนการทำงานตรงนี้ใช้ความสามารถของซอร์ฟแวร์ที่ชื่อ Squid Proxy ทำการให้บริการ มากกว่านั้นเมื่อผู้ใช้ดาวน์โหลดไฟล์ผู้ใช้จะรู้สึกได้ทันทีว่ามีความแตกต่างเพราะสามารถกระทำได้อย่างรวดเร็วต่างจากการใช้งานด้วยระบบ ซึ่งในส่วนการให้บริการตรงนี้เกิดจากการทำงานของซอฟต์แวร์และการคอนฟิกระบบเพิ่มเข้ามานั้นคือใช้ระบบ Squid Proxy ร่วมกับ Frox เพื่อช่วยการดาวน์โหลด ผลจากการนำระบบไปทดสอบและปรากฏว่าสามารถทำงานได้เป็นอย่างดีโดยเฉพาะเมื่อเปรียบเทียบกับระบบเดิมรวมไปถึงงานวิจัยอื่นที่มีเพียงระบบพรอกซี่เพียงอย่างเดียวทุกประการ

5.2 อภิปรายผล

ในการพัฒนาระบบเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยระบบปฏิบัติการลินุกซ์ สามารถสรุปสิ่งที่ได้จากการพัฒนาระบบ ดังนี้

5.2.1 ระบบที่พัฒนาขึ้นสามารถจัดทำขึ้นได้โดยง่ายด้วยการใช้ซอฟต์แวร์จากระบบเดิมที่มีอยู่แล้วร่วมกับการเพิ่มไฟล์คอนฟิกเล็กน้อยตามการจัดทำระบบภายในงานวิจัยที่เสนอนี้

5.2.2 มีระบบจัดเก็บแคชข้อมูลของผู้ใช้เพื่อทำให้ระบบเกิดความรวดเร็วด้วยการใช้ซอฟต์แวร์แบบโอเพ่นซอร์สที่มีความประหยัดในการจัดทำ

5.2.3 มีระบบตรวจสอบการเข้าใช้เครือข่ายอินเทอร์เน็ตของผู้ใช้ โดยสามารถเช็คความถูกต้องและความแม่นยำของระบบได้ผ่านทางคอมมานด์ไลน์ง่ายๆของระบบปฏิบัติการลินุกซ์ รวมถึงมีการตรวจสถานะของเครือข่ายด้วยเครื่องมือผลิตกราฟซึ่งมีอยู่แล้วในซอฟต์แวร์ระบบปฏิบัติการลินุกซ์

5.2.4 มีระบบตรวจเช็คหมายเลขไอพีแอดเดรสของเครื่องคอมพิวเตอร์ผู้ใช้รวมถึงรายละเอียดที่จำเป็น เช่น ชื่อเครื่อง (Computer Name) และชื่อเว็บไซต์ปลายทางที่ผู้ใช้ร้องขอ เป็นต้น

5.2.5 มีระบบจัดเก็บข้อมูลที่เป็นมาตรฐาน คงทน และน่าเชื่อถือ ในรูปแบบ Centralized Log Server ในการบริหารจัดการ Log File รวมถึงความสามารถในการย้ายโอนข้อมูล การสำรองข้อมูล การกู้คืนข้อมูล โดยจัดเก็บอยู่ในรูปฐานข้อมูล

5.2.6 มีความสามารถในการเก็บข้อมูลเพื่อใช้ในการค้นหาข้อมูลในช่วงเวลาต่างๆ เช่นข้อมูลปัจจุบัน ข้อมูลย้อนหลังรายวัน รายสัปดาห์ หรือรายเดือน เพื่อให้ข้อมูลกรณีผู้ดูแลระบบต้องการตรวจสอบประสิทธิภาพของระบบเครือข่าย ซึ่งจากการทดสอบพบว่าสามารถจัดเก็บได้อย่างครบถ้วนและถูกต้อง แม่นยำ

5.3 ข้อเสนอแนะ

จากการพัฒนาระบบเพิ่มประสิทธิภาพการให้บริการอินเทอร์เน็ตของหน่วยงานด้วยการลดปริมาณข้อมูลโดยใช้ระบบแม่ข่ายพักข้อมูลด้วยระบบปฏิบัติการลินุกซ์ มีข้อจำกัดบางประการที่เป็นปัญหาและอุปสรรคในการนำไปใช้งานที่ผู้จัดทำพบและจะต้องหาทางแก้ไขให้เหมาะสมกับสภาพแวดล้อมในการใช้งานของแต่ละเครือข่าย ดังนี้

5.3.1 ระบบที่จัดทำขึ้นอาศัยหลักการทำงานของพรอกซี่เซิรฟ์เวอร์ ซึ่งจำเป็นต้องตั้งใช้เครื่องเซิร์ฟเวอร์ที่มีประสิทธิภาพพอสมควรหากต้องการความมั่นคง ทนทาน เนื่องจากเป็นเสมือนทางผ่านของทุกเครื่องที่จะต้องผ่านเข้ามายังเครื่องแม่ข่ายนี้ หากเครื่องแม่ข่ายนี้ไม่สามารถให้บริการได้ เครื่องคอมพิวเตอร์ลูกข่ายทุกเครื่องก็ไม่สามารถใช้งานอินเทอร์เน็ตได้

5.3.2 ควรแก้ปัญหาของระบบพรอกซี่เซิร์ฟเวอร์ให้สามารถทำงานได้ตลอดเวลาด้วยการจัดหาเครื่องสำรองเพื่อรับมือกรณีเครื่องหลักเกิดความเสียหายโดยไม่ขาดฝัน หรือจะใช้วิธีจัดตั้งเครื่องแม่ข่ายมากกว่าหนึ่งตัวก็ได้ในลักษณะเป็นโหลดบาลานซ์ (Load Balance)

5.3.3 เพื่อให้การทำงานของระบบสามารถทำงานได้อย่างรวดเร็ว ควรจัดให้เครื่องคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่เป็นพรอกซี่เซิร์ฟเวอร์มีหน่วยความจำสูงๆ จะทำให้การสนองตอบต่อเครื่องผู้ใช้เป็นไปอย่างรวดเร็ว

5.3.4 ควรจัดหาระบบแอนตี้ไวรัสและไฟร์วอลล์ที่มั่งคงเพื่อป้องกันมิให้เครื่องแม่ข่ายเกิดความเสียหาย

บรรณานุกรม

1. วนิดา, จ., อินเทอร์เน็ตมิติใหม่แห่งการสื่อสาร. กรุงเทพฯ : บริษัซีเอ็ดยูเคชั่นจำกัด (มหาชน). 2537.
2. และคณะ., พ.พ., การแสวงหาข่าวสารเกี่ยวกับประเด็นทางเพศของวัยรุ่นไทยที่นำเสนอผ่านทางอินเทอร์เน็ต. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิเทศศาสตร์. กรุงเทพฯ: จุฬาลงกรณ์มหาวิทยาลัย, (2544).
3. กัลยาศิริ, จ.โ., *LINUX* อินเทอร์เน็ตเซิร์ฟเวอร์. กรุงเทพฯ : บริษัทซีเอ็ดยูเคชั่น จำกัด (มหาชน). 2542.
4. นิลวรรณ, ช., ระบบจัดการสวิคพร็อกซี่โพลีซีโดยผ่านเว็บอินเตอร์เฟส. กรุงเทพฯ : สำนักหอสมุดกลาง. สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ. . 2549.
5. Qinyun, L., Z. Jinguo, and C. Min. *Research of TCP/IP protocol stack based on embedded system*. in *Computer Research and Development (ICCRD),* 2011 3*rd International Conference on*. 2011.
6. *Sripitakieat, A.,* 1997, *"TCPIP Networking,"* เอกสารประกอบวิชา *Computer Network, Chiangmai University.*
7. บุญศิริ, ส., อินเทอร์เน็ต : นานาสาระแห่งบริการ. กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย. สำนักวิทยบริการ. 2538.
8. เพชรไม้, ณ., เรียนลัด หัดใช้อินเทอร์เน็ต. กรุงเทพฯ : สำนักพิมพ์ สวัสดี ไอที. 2550.
9. เอี่ยมสิริวงศ์, โ., การวิเคราะห์และออกแบบระบบ. กรุงเทพฯ:ซีเอ็ดยูเคชั่น. 2548.
10. โอภาสเอี่ยมสิริวงศ์, การวิเคราะห์และออกแบบระบบ. 2548, กรุงเทพฯ:ซีเอ็ดยูเคชั่น.
11. สว่างวรรณ, ส., *Computer Networks.* กรุงเทพฯ : เพียร์สัน เอ็ดดูเคชั่น อินโดไชน่า. 2542.
12. ภัทระเกียรติเสวี, สร้างอินเทอร์เน็ตเซิร์ฟเวอร์ด้วย *Linux*. 2542, ซีเอ็ดยูเคชั่น จำกัด (มหาชน).
13. รังสิพล, เ., เจาะระบบ *TCP/IP* จุดอ่อนของโปรโตคอล และวิธีป้องกัน. โปรวิชั่น. 2544.
14. เกษพานิช, ว., การเขียนเว็บเพจด้วยภาษา *HTML*. สำนักพิมพ์แม็ค 2547.
15. จามรภูมิ, บ., คัมภีร์ *Ubuntu Linux Server* เล่ม 2. ซีเอ็ดยูเคชั่น จำกัด (มหาชน). 2553.
16. (*http://wiki.nectec.or.th/ngiwiki/pub/Main/GroupProject/HTTP.ppt#257,1,HTTP*, สืบค้นวันที่ 4 กรกฎาคม 2554).
17. Gien, M., *A File Transfer Protocol (FTP).* Computer Networks (1976), 1978. 2(4): p. 312-319.
18. (*http:// http://th.wikipedia.org/wiki/*เอฟทีพี, สืบค้นวันที่ 4 กรกฎาคม 2554).
19. *IPv6 Protocols A2 - Loshin, Pete*, in *IPv6* (*Second Edition)*. 2004, Morgan Kaufmann: San Francisco. p. 85-87.

20. *Chapter 7 - The SSH Server Basics*, in *Next Generation SSH2 Implementation*. 2009, Syngress: Burlington. p. 137-172.
21. พาลพ่าย, ว., การจำกัดการใช้งานแบนวิดธ์ของพรอกซีเซิร์ฟเวอร์ในระดับผู้ใช้. วิทยานิพนธ์วิศวกรรมศาสตรมหาบัณฑิต บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยี พระจอมเกล้าธนบุรี, 2545.
22. Katalinic, B., M. Sysel, and O. Doležal, 24*th DAAAM International Symposium on Intelligent Manufacturing and Automation,* 2013*An Educational HTTP Proxy Server.* Procedia Engineering, 2014. 69: p. 128-132.
23. *Saetae, W.,* 1999*, User Authentication Program Development for Cache Server,*

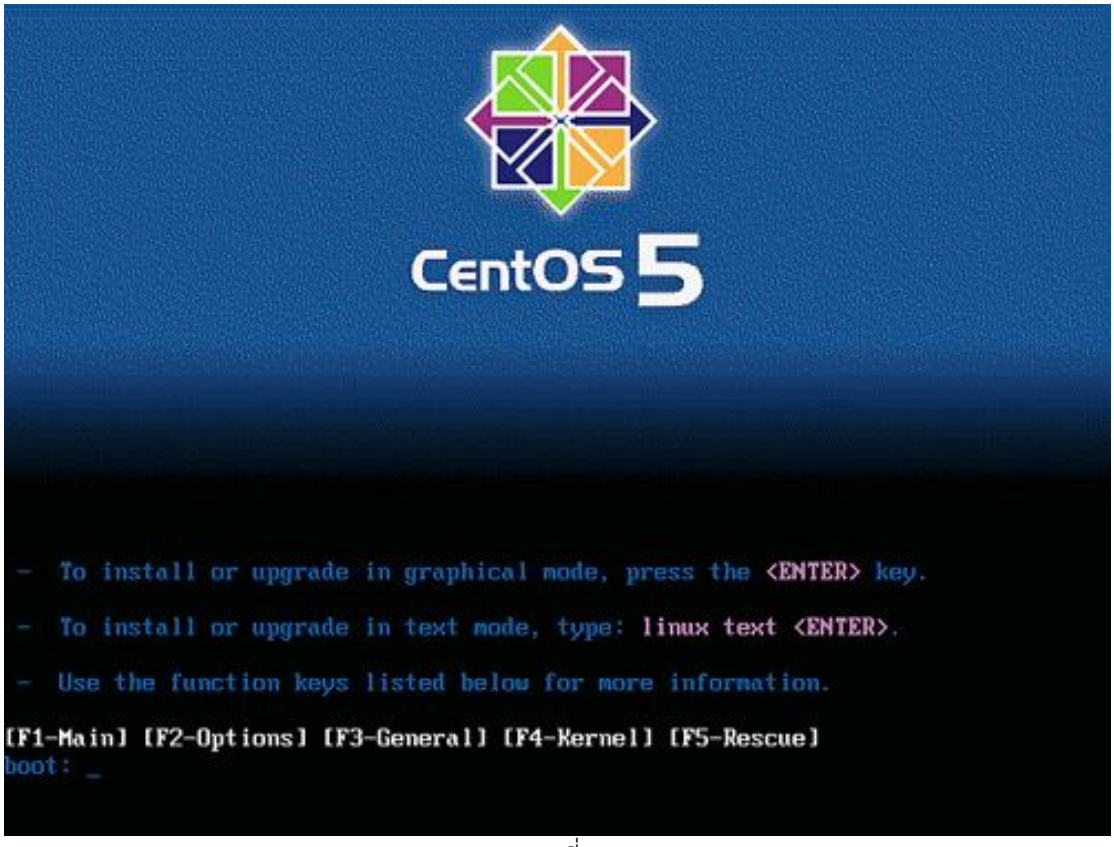
Bechelor of Information Technology Project, Information Technology Program, King Monkut's University of Technology Thonburi.

24. (*http:// http://th.wikipedia.org/wiki/*พร็อกซี่เซิร์ฟเวอร์*,* สืบค้นวันที่ 4 กรกฎาคม 2554).
25. Fulp, E.W., *Chapter 6 - Firewalls A2 - Vacca, John R*, in *Managing Information Security (Second Edition)*. 2014, Syngress: Boston. p. 143-175.
26. (*http://thaicert.nectec.or.th/paper/firewall/firewall.pdf,* สืบค้นวันที่ 4 กรกฎาคม 2554).

ภาคผนวก

ขั้นตอนการติดตั้งระบบปฏิบัติการลินุกซ์ (Linux CentOS)

เริ่มติดตั้ง CentOS ดังนี้



ภาพที่ 1

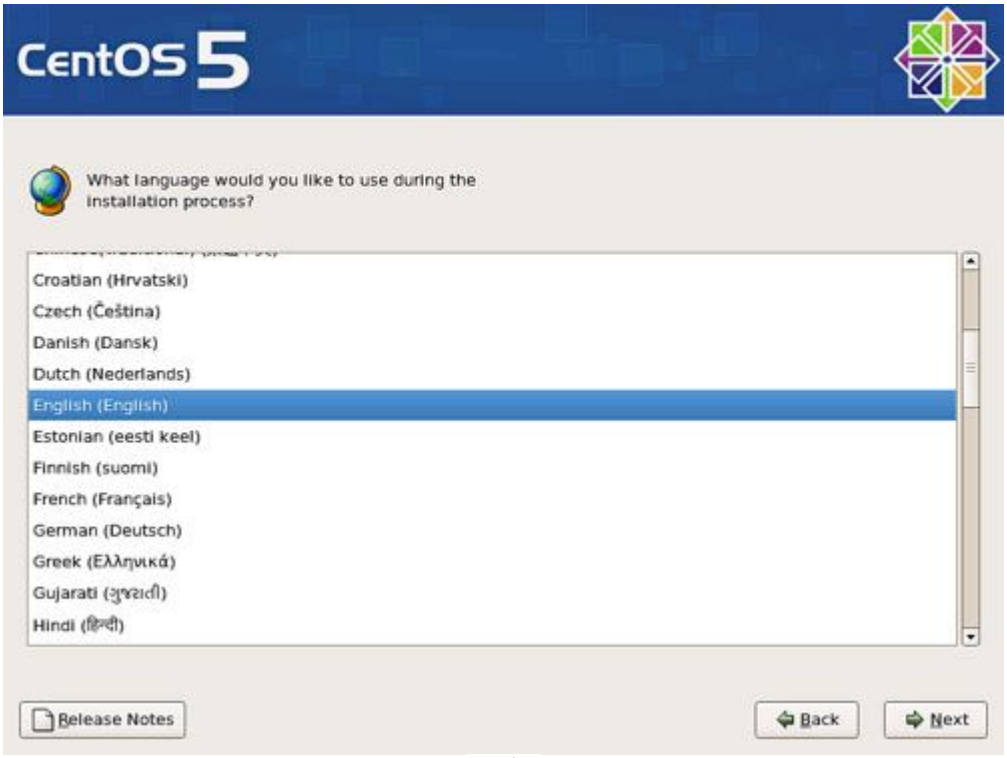
1. ทำการบูทผ่าน CD ROM หรือ DVD ROM โดยระบบบูทขึ้นมาจะปรากฏหน้าจอดังภาพที่ 1 จากนั้นให้กดปุ่ม <ENTER> เพื่อเข้าสู่การติดตั้งในขั้นต่อไป

ภาพที่ 2

2. เมื่อบูทเข้ามาแล้วจะขึ้นหน้าจอสีฟ้าก่อนเข้าสู่โหมดการติดตั้งแบบ GUI โดยในขั้นตอนนี้จะเป็นการตรวจเช็คสภาพของแผ่นติดตั้งทั้ง CD และ DVD แต่ถ้าแน่ใจในคุณภาพของแผ่นก็สามารถ Skip ผ่านขั้นตอนนี้เพื่อเข้าสู่หน้าจอติดตั้งแบบ GUI ได้เลย

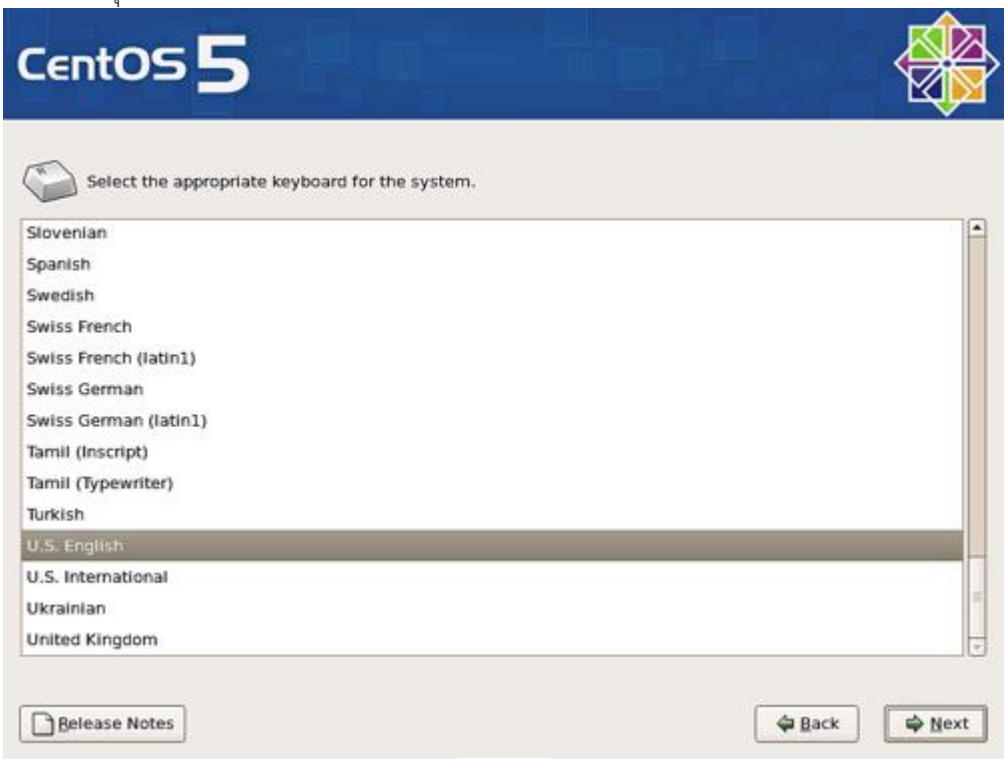
ภาพที่ 3

3. หลังจากที่ Skip ไม่ตรวจสอบแผ่นแล้ว เครื่องจะทำการ run โปรแกรมติดตั้ง Anaconda GUI ซึ่งเป็นโปรแกรมติดตัง CentOS 5.2 โดยหน้าจอแรกจะเป็นหน้าจอ Welcome Screen ให้คลิ๊กที่ปุ่ม Next เพื่อไปสู่ขั้นตอนการตัดตั้งหน้าจอการติดตั้งถัดไป



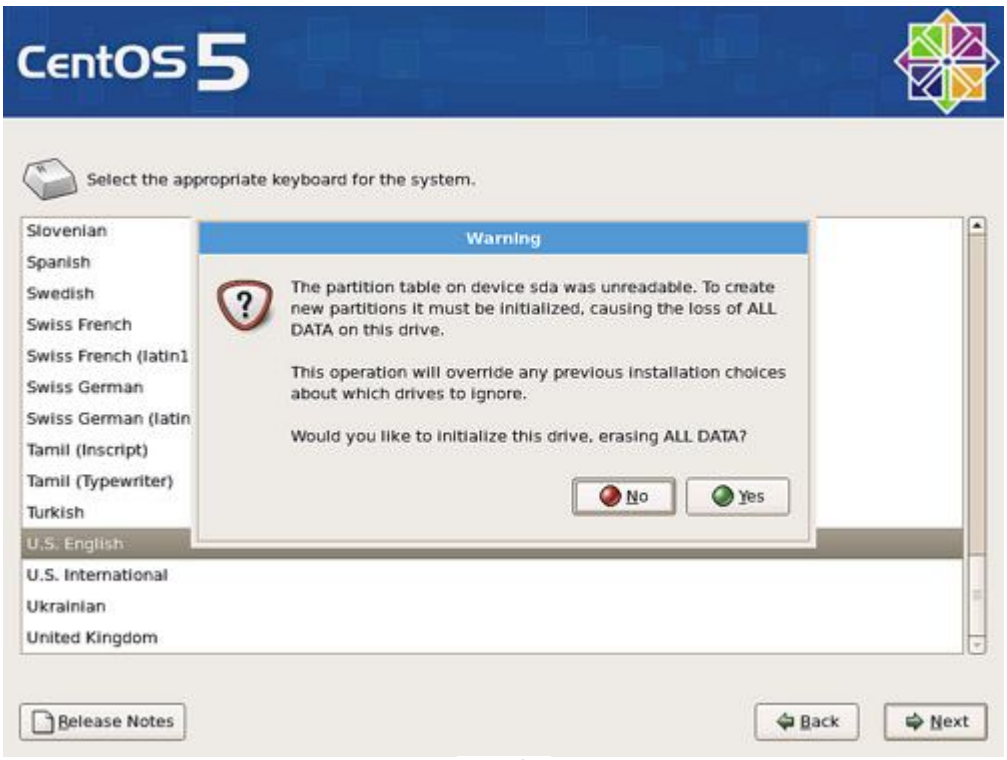
รูปที่ 4

4. หน้าจอถัดไปจะเป็นการเลือกภาษาในการติดตั้ง ในที่นี้เลือกใช้ภาษาอังกฤษสำหรับการติดตั้ง (เนื่องจากไม่มีชุดติดตั้งภาษาไทย)



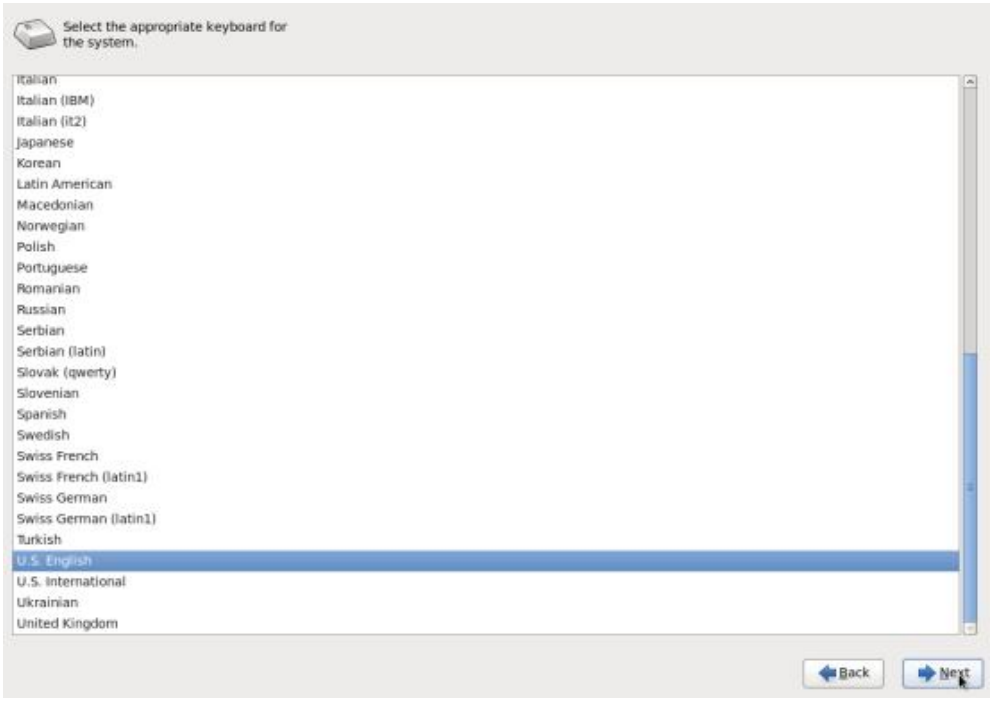
ภาพที่ 5

5. เป็นการกำหนดค่าของ Keyboard Layout ในที่นี้ให้เลือกเป็น English



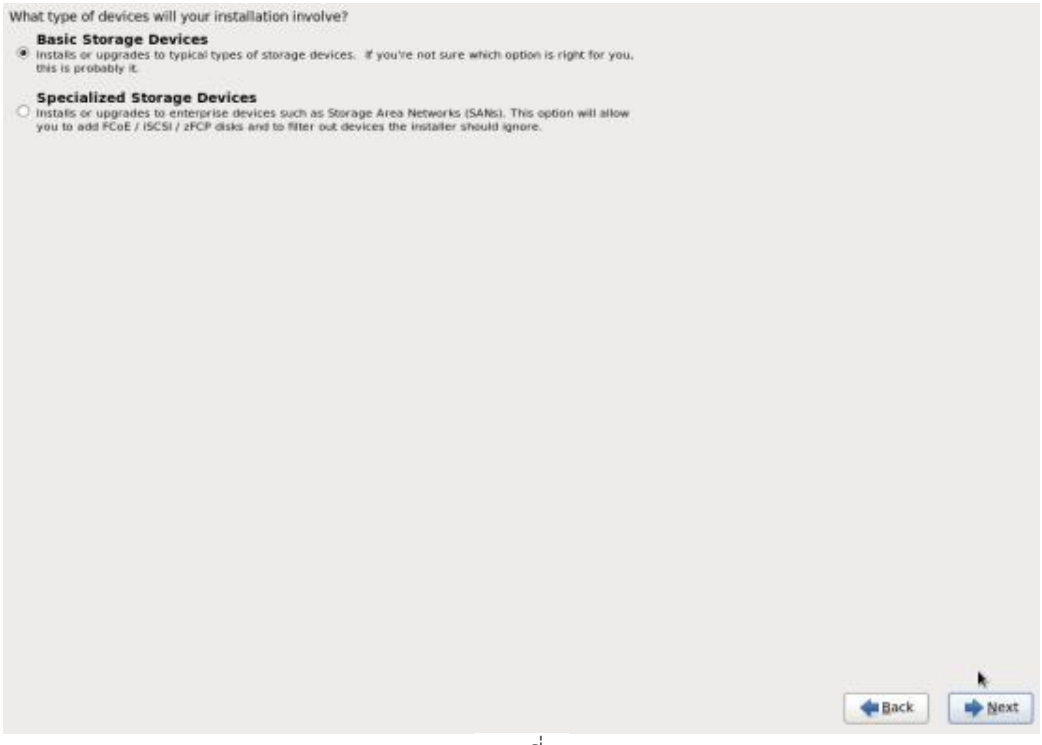
ภาพที่ 6

6. เมื่อทำการคลิ๊กตอบตกลงเลือกภาษาที่ต้องการแล้ว ชุดติดตั้งจะขึ้นข้อความเกี่ยวกับการแบ่ง Partition Hard disk ในที่นี้ให้ตอบ No เนื่องจากเราจะไม่ให้ชุดติดตั้งทำการแบ่ง Partition และลบข้อมูลต่าง ๆ ใน Hard disk เราอัตโนมัติ



ภาพที่ 7

7. จากนั้นเลือก Keyboard Layout (US English)

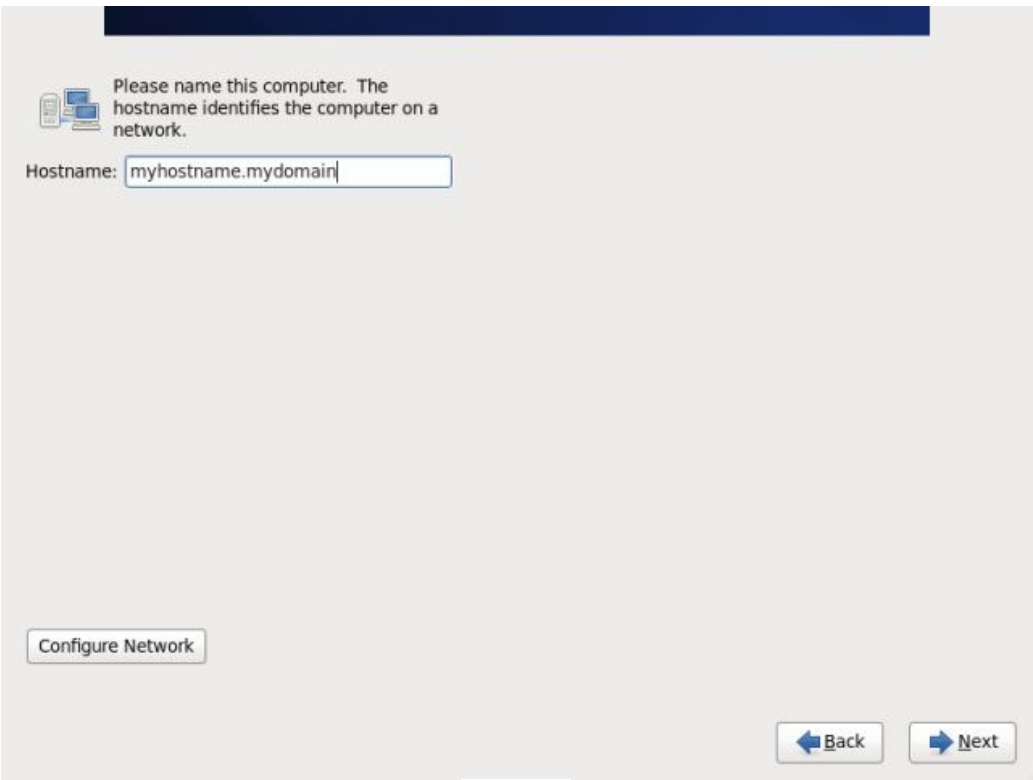


ภาพที่ 8

8. ทำการเลือก Basic Storage Device เพราะว่าเราใช้ Hard Disk ธรรมดาๆ

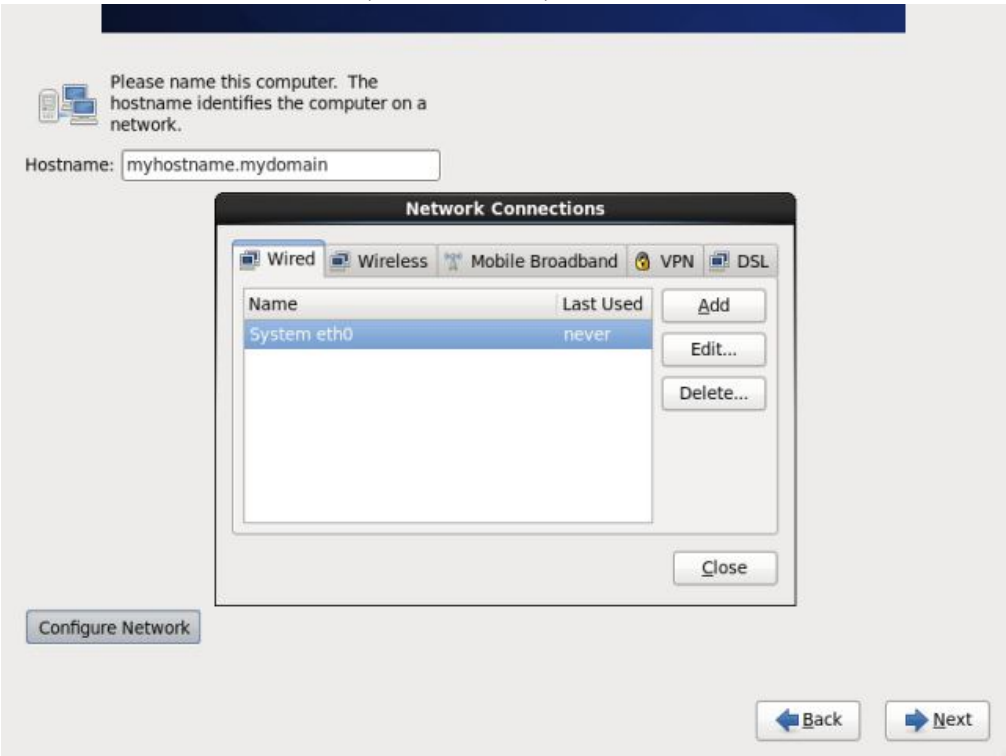
ภาพที่ 9

9. กด Yes, discard any data เพื่อยืนยันว่าถ้ามีข้อมูลอยู่ใน Hard Disk ตัวนี้เราไม่เอามันแล้วและยอมให้ลบได้เลย



ภาพที่ 10

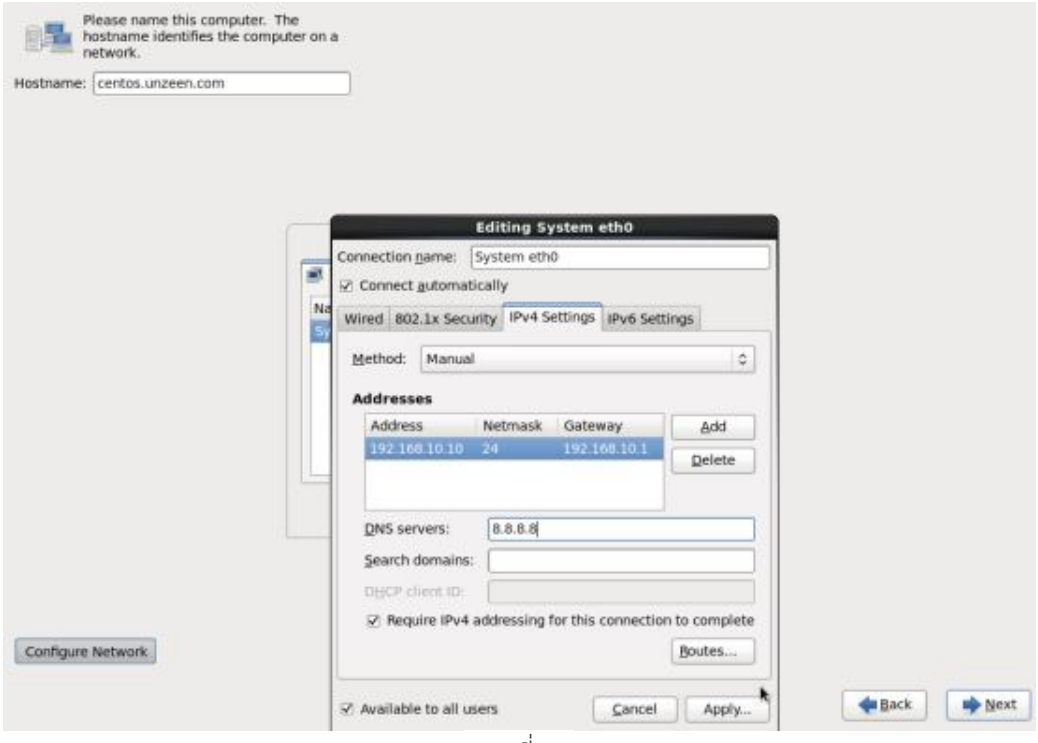
10. ทำการตั้งชื่อเครื่อง ในที่นี้ตั้งว่า myhostname.mydomain



ภาพที่ 11

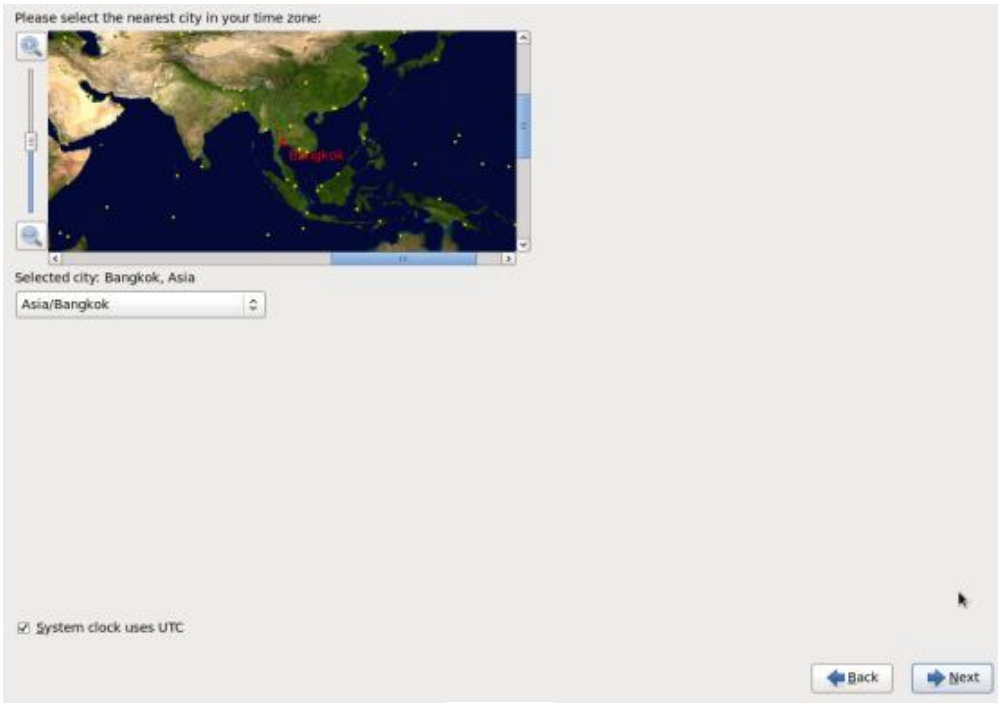
11. จากนั้นคลิกที่ Configure Network เพื่อทำการกำหนด IP Address โดยเลือกไปที่ Wired และ

คลิก Edit ที่ eth0 ซึ่งเป็นการ์ดแลน



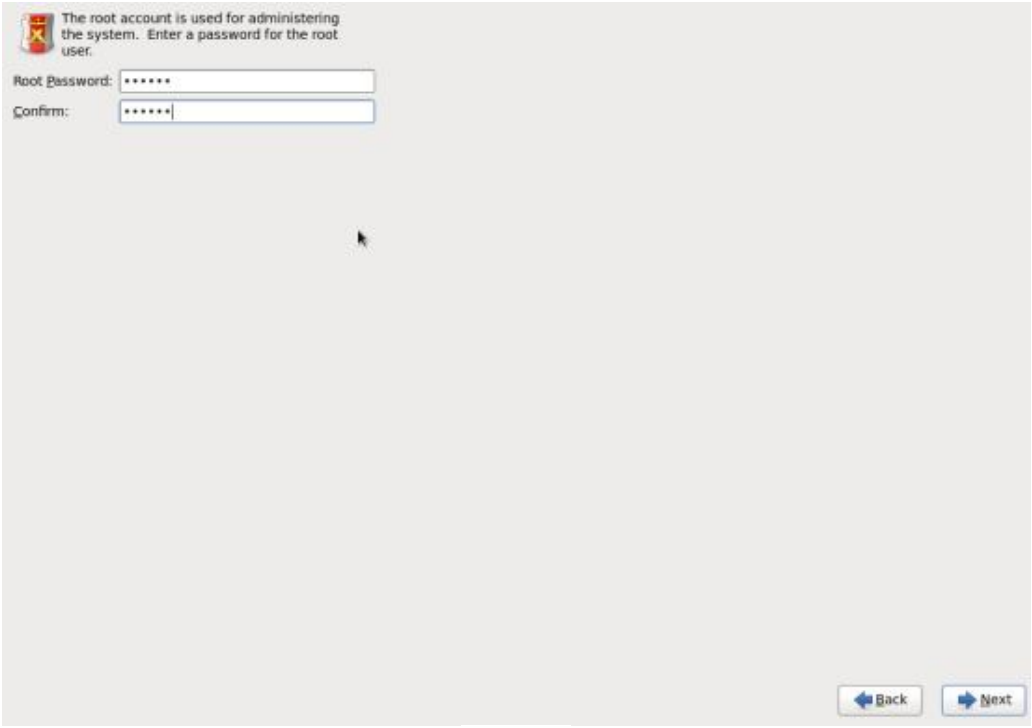
ภาพที่ 12

12. ทำการคลิ๊กถูกที่ Connect automatically จากนั้นเลือกไปที่แท็บ IPv4 Setting กำหนดข้อมูลในช่อง Method เป็น Manual และทำการเพิ่ม IP Address, Netmask, Gateway, DNS Server โดยกำหนดดังนี้ IP Address : 192.168.10.10 Netmask : 24 Gateway : 192.168.10.1 DNS Server : 8.8.8.8



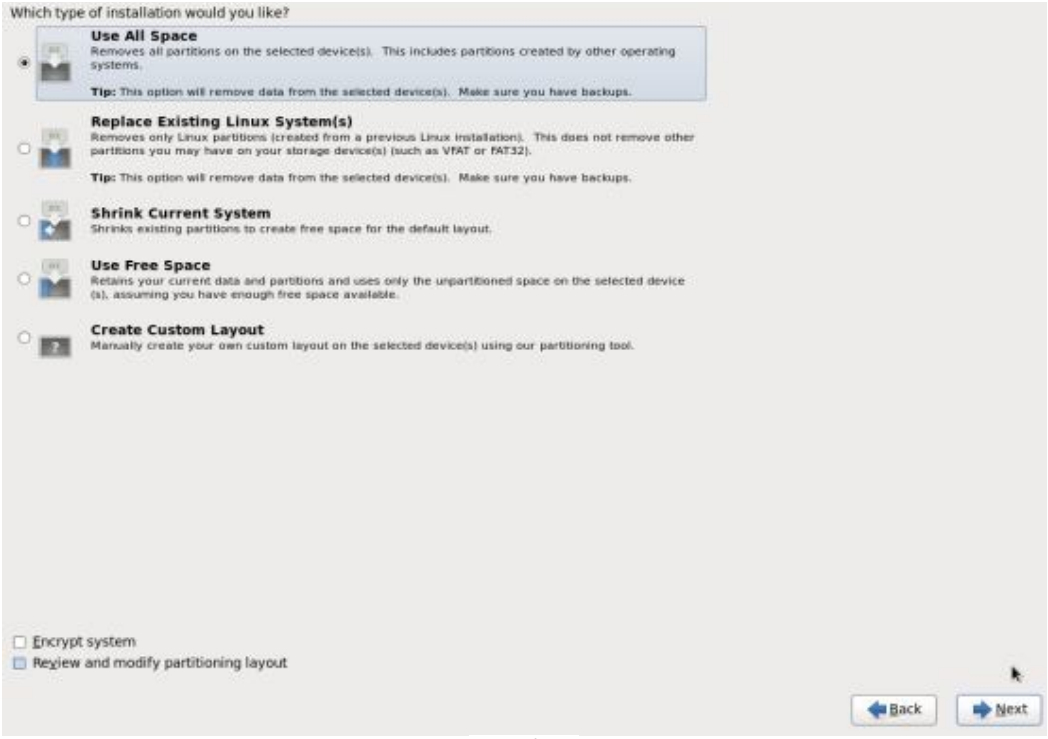
ภาพที่ 13

13. ต่อไปทำการเลือกประเทศ



ภาพที่ 14

14. กำหนดรหัสผ่านสำหรับ root

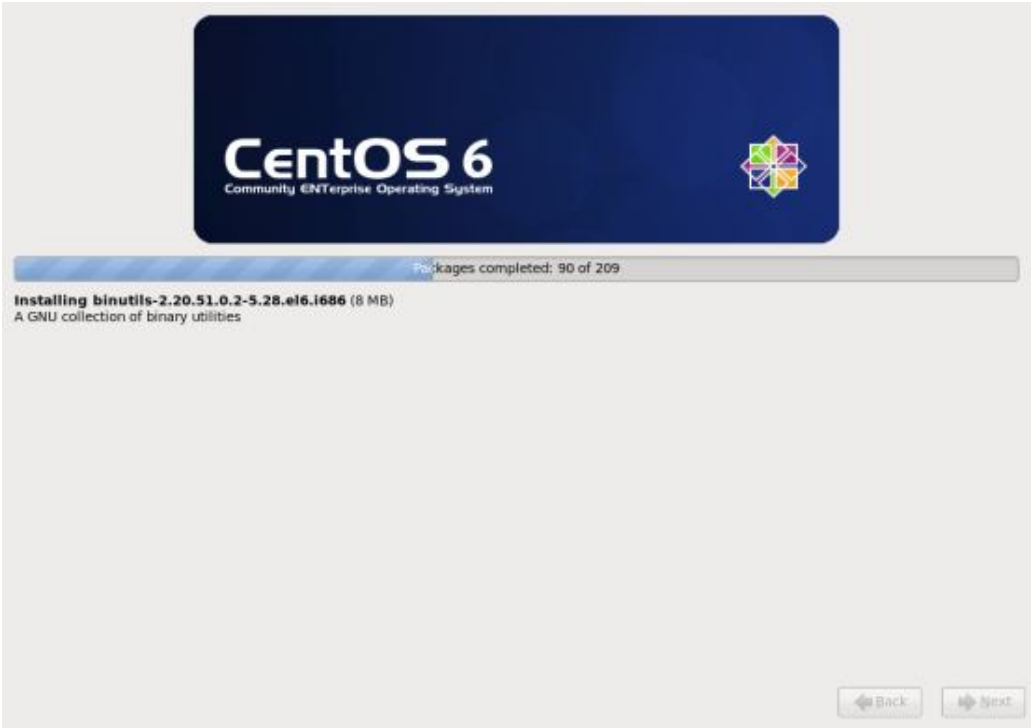


ภาพที่ 15

15. เลือก Use All Space เพราะว่าเราต้องการติดตั้งโดยไม่แบ่ง partition แต่ถ้าใครเชียวชาญมากแล้วก็เลือก Create Custom Layout ได้

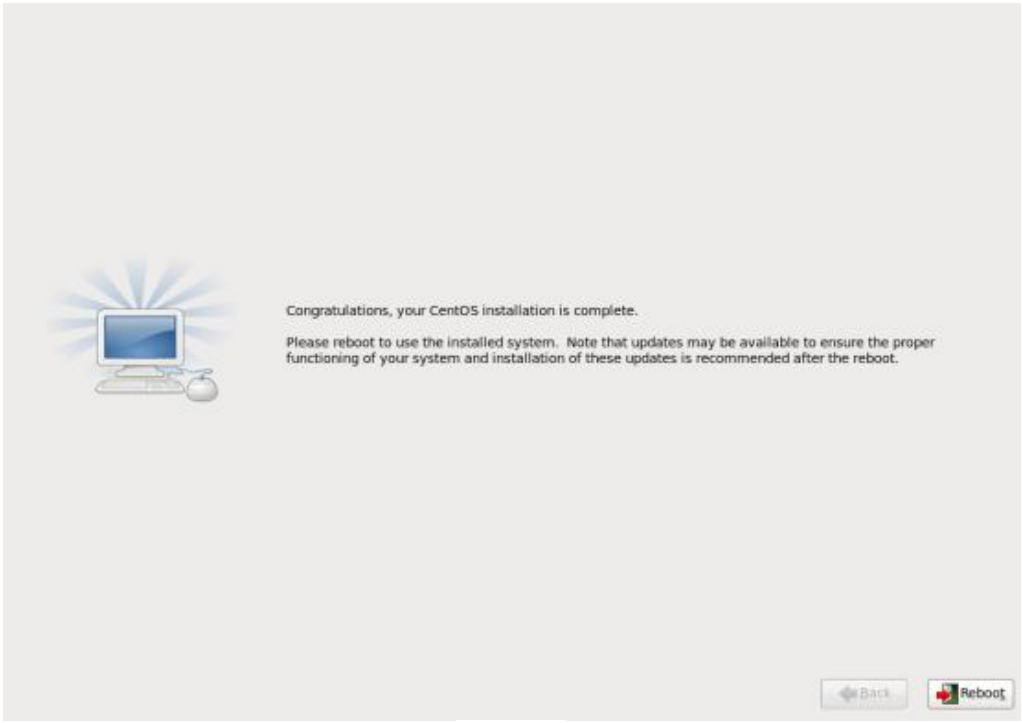
ภาพที่ 16

16. คลิ๊ก Write changes to disk



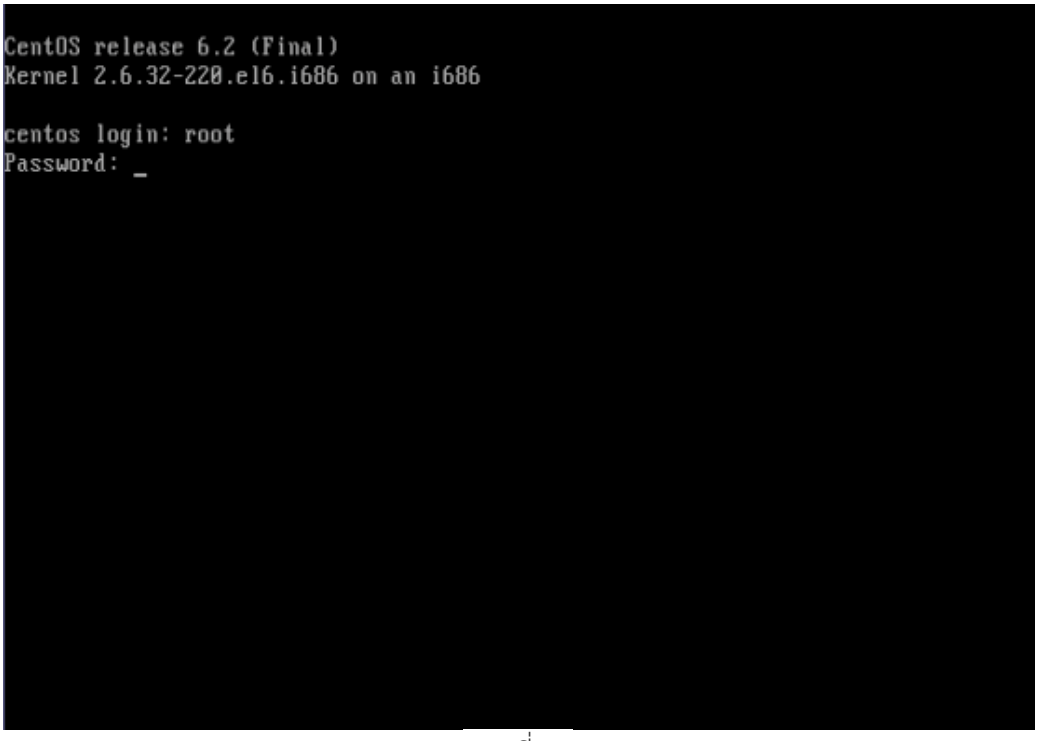
ภาพที่ 17

17. ระบบเริ่มทำการติดตั้ง CentOS ลงบน Hard Disk



ภาพที่ 18

18. เมื่อติดตั้งเรียบร้อยแล้วคลิ๊ก Reboot



ภาพที่ 19

19. เมื่อ Reboot เรียบร้อยแล้วเราจะเห็นหน้าจอให้ใส่ Username และ Password หากไม่มีอะไรผิดพลาดไปจากนี้ถือว่าขั้นตอนการติดตั้งเสร็จเรียบร้อย