บทที่ 1
ระบบเครื่อข่ายคอมพิวเตอร์

การที่ระบบเครือข่ายมีบทบาทและความสำคัญเพิ่มขึ้น เพราะไมโครคอมพิวเตอร์ได้รับการใช้งานอย่างแพร่หลาย จึงเกิดความต้องการที่จะเชื่อมต่อคอมพิวเตอร์เหล่านั้นถึงกับเพื่อเพิ่มขีดความสามารถของระบบให้สูงขึ้น เพิ่มการใช้งานด้านต่าง ๆ และลดต้นทุนระบบโดยรวมลง มีการแบ่งใช้งานอุปกรณ์และข้อมูลต่าง ๆ ตลอดจนสามารถทำงานร่วมกันได้ สิ่งสำคัญที่ทำให้ระบบข้อมูลมีขีดความสามารถเพิ่มขึ้น คือ การโอนย้ายข้อมูลระหว่างกัน และการเชื่อมต่อหรือการสื่อสาร การโอนย้ายข้อมูลหมายถึงการนำข้อมูลมาแบ่งกันใช้งาน หรือการนำข้อมูลไปใช้ประมวลผลในลักษณะแบ่งกันใช้ทรัพยากร เช่น แบ่งกันใช้ซีพียู แบ่งกันใช้ฮาร์ดดิสก์ แบ่งกันใช้โปรแกรม และแบ่งกันใช้อุปกรณ์อื่น ๆ ที่มีราคาแพงหรือไม่สามารถจัดหาให้ทุกคนได้ การเชื่อมต่อคอมพิวเตอร์เป็นเครือข่ายจึงเป็นการเพิ่มประสิทธิภาพการใช้งานให้กว้างขวางและมากขึ้นจากเดิม

การเชื่อมต่อในความหมายของระบบเครือข่ายท้องถิ่น ไม่ได้จำกัดอยู่ที่การเชื่อมต่อระหว่างเครื่องไมโครคอมพิวเตอร์ แต่ยังรวมไปถึงการเชื่อมต่ออุปกรณ์รอบข้าง เทคโนโลยีที่ก้าวหน้าทำให้การทำงานเฉพาะมีขอบเขตกว้างขวางยิ่งขึ้น มีการใช้เครื่องบริการแฟ้มข้อมูลเป็นที่เก็บรวบควมแฟ้มข้อมูลต่างๆ มีการทำฐานข้อมูลกลาง มีหน่วยจัดการระบบสื่อสารหน่วยบริการใช้เครื่องพิมพ์ หน่วยบริการการใช้ซีดี หน่วยบริการปลายทาง และอุปกรณ์ประกอบสำหรับต่อเข้าในระบบเครือข่ายเพื่อจะทำงานเฉพาะเจาะจงอย่างใดอย่างหนึ่ง ในรูป เป็นตัวอย่างเครือข่ายคอมพิวเตอร์ที่จัดกลุ่มเชื่อมโยงเป็นระบบ

ตัวอย่างเครือข่ายคอมพิวเตอร์ที่จัดกลุ่มอุปกรณ์รอบข้างเชื่อมโยงเป็นระบบ

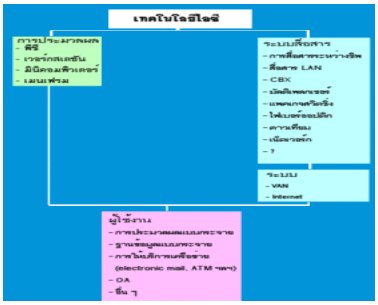
เครือข่ายคอมพิวเตอร์ก่อให้เกิดความสามารถในการปฏิบัติการร่วมกัน ซึ่งหมายถึงการให้อุปกรณ์ทุกชิ้นที่ต่ออยู่บนเครือข่ายทำงานร่วมกันได้ทั้งหมดในลักษณะที่ประสานรวมกัน โดยผู้ใช้เห็นเสมือนใช้งานในอุปกรณ์เดียวกัน จึงเป็นวิธีการในการนำเอาอุปกรณ์ต่างชนิดจำนวนมาก มารวมกันเป็นเสมือนระบบเดียวกัน ทั้ง ๆ ที่อุปกรณ์เหล่านั้นอาจจะมาจากต่างยี่ห้อ ต่างบริษัทก็ได้

ปัจจุบัน ที่ไมโครคอมพิวเตอร์เริ่มแพร่หลาย ความคิดเกี่ยวกับการใช้คอมพิวเตอร์โครคอมพิวเตอร์กำลังจะเข้ามามีบทบาทมียอดการจำหน่ายสูงมากจนมีผู้ทำเลียนแบบกันมากมาย เพียงระยะเวลาผ่านไปไม่กี่ปีไมโครคอมพิวเตอร์ก็ก้าวหน้าขึ้นอย่างรวดเร็ว ในปี ค.ศ. 1979 สตีฟ จ๊อบ หนึ่งในสองของผู้ก่อตั้งบริษัทแอปเปิ้ลคอมพิวเตอร์มีโอกาสไปเยี่ยมบริษัทซีร็อกซ์ที่ศูนย์วิจัย Palo Alto มีมลรัฐแคลิฟอร์เนียมีความประทับใจกับระบบคอมพิวเตอร์ ซึ่งในขณะนั้นเป็นคอมพิวเตอร์ขนาดใหญ่ แต่มีการแสดงกราฟิกและการใช้งานที่ง่าย สตีฟ จ๊อบ จึงเริ่มความคิดที่จะสร้างคอมพิวเตอร์ขนาดเล็กที่มีระบบการใช้ หรือที่เรียกว่ายูสเซอร์อินเตอร์เฟสเหมือนกับเครื่องคอมพิวเตอร์ของบริษัทซีร๊อกซ์ และในที่สุดก็พัฒนาเป็นคอมพิวเตอร์ชื่อลิซ่า แต่ลิซ่าไม่ประสบผลสำเร็จเท่าที่ควร บริษัทแอปเปิ้ลจึงพัฒนาย่อส่วนลงและเพิ่มขีดความสามารถขึ้นจนกลายเป็นเครื่องแมคอินทอชในปัจจุบัน ความคิดของไมโครคอมพิวเตอร์ขณะนั้นคือเพิ่มขีดความสามารถของการทำงานโดยเน้นการใช้งานง่ายเป็นสำคัญ แนวความคิด "หั่นเป็นชิ้นแยกส่วนการทำงาน" เริ่มต้นแล้ว ทำอย่างไรจึงให้คอมพิวเตอร์ขนาดใหญ่ ซึ่งมีบทบาทและความจำเป็นมาก ถูกจำลองลงด้วยเครื่องขนาดเล็ก การใช้งานไมโครคอมพิวเตอร์จึงยังไม่สามารถทดแทนระบบขนาดใหญ่ได้ ศูนย์วิจัยของบริษัทซีร๊อกซ์ได้พัฒนาและสร้างระบบต้นแบบไว้หลายอย่าง ความรู้แล้วต้นตำรับของเครือข่ายคอมพิวเตอร์ก็เริ่มขึ้นที่นี่ด้วย ซีร๊อกซ์ได้พัฒนาระบบคอมพิวเตอร์แยกส่วน และเชื่อมโยงต่อกันเป็นเน็ตเวอร์ก และในที่สุดอีเธอร์เนต หรือ IEEE 802.3 ก็ได้รับการยอมรับ นับว่าจุดเริ่มต้นของแนวความคิดได้รับการยอมรับ และกลายเป็นมาตรฐานโลกไปในที่สุด หากย้อนรอยตั้งแต่ไอบีเอ็มประกาศไอบีเอ็มพีซีครั้งแรก ถนนการค้าไมโครคอมพิวเตอร์ก็ได้รับการขานรับและพัฒนาต่อเนื่องอย่างไม่หยุดยั้ง จาก 286 มาเป็น 386 และกลายเป็น 486 ปัจจุบันมีหลายบริษัทได้พัฒนาระบบบัสที่เป็นแบบความเร็วสูง เช่น MCA, EISA หรือนำบัสที่เคยใช้บนมินิคอมพิวเตอร์ เช่น VME, Q bus หรือแม้แต่มัลติบัสมาใช้กับไมโครคอมพิวเตอร์ที่ใช้ซีพียู 68000, 68020, 68030 เป็นต้น ช่วงสามสี่ปีที่ผ่านมา ระบบเวอร์กสเตชันก็ขานรับต่อมา มีเครื่องระดับเวอร์กสเตชันออกมามากมาย เช่น ของบริษัทซันไมโครซิสเต็ม ฮิวเล็ตต์แพคการ์ด หรือแม้แต่ไอบีเอ็มก็พัฒนาระบบ R6000 ขึ้นเช่นกัน สิ่งที่น่าสังเกตคือ ระบบคอมพิวเตอร์ยุคหลังนี้มาบนเส้นทางที่ให้ระบบการเชื่อมต่อถึงกันทั้งสิ้น การสร้างเครือข่ายคอมพิวเตอร์จึงดูจริงจังและเป็นงานเป็นการขึ้นกว่าเดิมมาก

หากย้อนไปเมื่อยี่สิบปีที่แล้วคอมพิวเตอร์มีราคาแพง การใช้งานจะอยู่ที่หน่วยงานใหญ่ ๆ ต้องมีห้อง มีศูนย์คอมพิวเตอร์ ระบบคอมพิวเตอร์เป็นระบบรวมศูนย์ ถึงแม้แยกออกมาเป็นเทอร์มินัลก็แตกกระจาย จากศูนย์กลางออกไปแต่ แต่ในปัจจุบันการใช้คอมพิวเตอร์เริ่มแปรเปลี่ยนไป หน่วยงานต่าง ๆ พยายามมีคอมพิวเตอร์ของตนเอง ไมโครคอมพิวเตอร์หรือพีซีก็กระจายแพร่หลายไปทุกหน่วยงาน การพัฒนาซอฟต์แวร์เป็นไปอย่างกว้างขวาง มีโปรแกรมสำเร็จรูปออกมามากมาย สาเหตุสำคัญที่ทำให้ระบบเครือข่ายคอมพิวเตอร์มีความจำเป็น และมีบทบาทที่สำคัญต่อมาเพราะ การใช้งานในหน่วยงานยิ่งแพร่หลาย ความต้องการที่จะเชื่อมโยงข้อมูลข่าวสารก็มีมากขึ้น ไมโครคอมพิวเตอร์มีราคาถูกเมื่อเทียบกับมินิคอมพิวเตอร์หรือเมนเฟรม ประจวบกับการใช้งานไมโครคอมพิวเตอร์ทำได้ง่ายกว่ามาก มีซอฟต์แวร์มาก แต่จุดอ่อนของไมโครคอมพิวเตอร์ก็อยู่ที่ระบบงานที่อาจต้องมีการเชื่อมโยงถึงกัน ดังนั้นการเพิ่มคุณค่าของระบบจึง

ต้องพัฒนาในเรื่องเครือข่ายคอมพิวเตอร์เป็นประการสำคัญ พัฒนาการของไมโครโปรเซสเซอร์ไปเร็วมาก เหตุผลประการสำคัญอีกประการหนึ่งคือ ไมโครโปรเซสเซอร์และพัฒนาการทางด้านชิพได้ก้าวล้ำไปมาก ขีดความสามารถของซีพียูสูงขึ้น การคำนวณหรือระบบงานไมโครคอมพิวเตอร์ทำได้มาก ประกอบกับอุปกรณ์สื่อสารโทรคมนาคมได้มีการพัฒนาไปพร้อมกับระบบเครือข่ายสื่อสารโทรคมนาคมรองรับได้มาก ส่วนนี้เองเป็นแรงกระตุ้นการเชื่อมโยงระบบให้มีการผูกยึดเป็นระบบเครือข่าย

เทคโนโลยีหลายด้านได้พัฒนาก้าวหน้าขึ้นเป็นอันมาก เช่น เทคโนโลยีไฟเบอร์ออปติก ไมโครเวฟ หรือแม้แต่สายโคแอกเชียล ก็สามารถทำให้มีแบนด์วิดธ์สูงมาก ในขณะที่ราคาต้นทุนลดลง การทำให้จำนวนกิโลบิตที่ว่งได้ต่อวินาทีสูงขึ้น โอกาสของถนนสายข้อมูลก็มีรถซึ่งเป็นข้อมูลวิ่งได้มากขึ้น นอกจากนี้พัฒนาการทางเทคนิคทางซอฟต์แวร์โดยเฉพาะอย่างยิ่งระบบสื่อสารที่เรียกว่า โปรโตคอล ก็ได้พัฒนาไปมาก มีการกำหนดมาตรฐานระหว่างประเทศขึ้น เพื่อตอบสนองการเชื่อมโยงเป็นระบบมากในระยะสองสามปีที่ผ่านมา ความต้องการการเชื่อมโยงระบบคอมพิวเตอร์เข้าหากันมีจุดมุ่งหมายหลาย อย่างเช่น



รูปที่ 1 โครงสร้างการพัฒนา

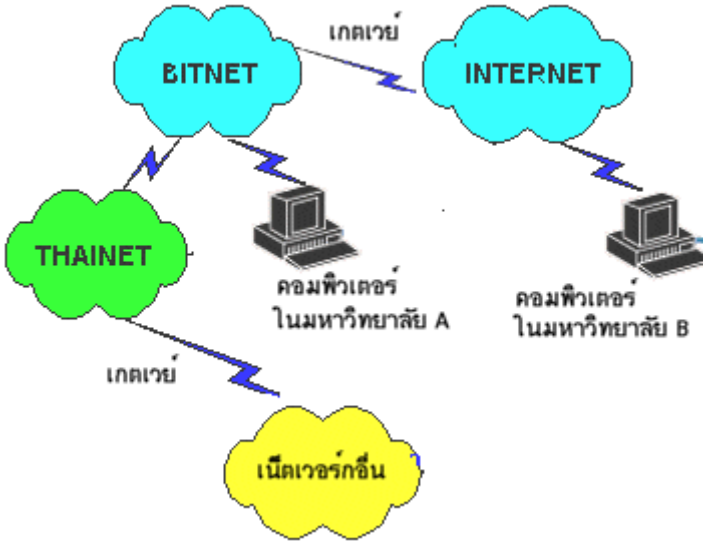
การใช้ทรัพยากรที่มีราคาแพงเช่นเครื่องพิมพ์คุณภาพใช้ซีพียูร่วมกัน ใช้ข้อมูลร่วมกัน การใช้ทรัพยากรร่วมกันนี้เป็นระบบที่จำเป็น เพราะเครือข่ายการทำงานขององค์กรจะต้องรวมกันเป็นน้ำหนึ่งใจเดียวกันให้ได้มากที่สุด

การใช้ไมโครคอมพิวเตอร์ในการประมวลผลมีค่าใช้จ่ายถูกใช้งานง่าย หาบุคลากรได้ การที่ให้บริษัทลงทุนกับเครื่องคอมพิวเตอร์ราคาแพง เช่น มินิ หรือเมนเฟรม อาจเป็นปัญหาในเรื่องการลงทุน และการหาบุคลากร การขยายตัวของระบบจะค่อยเป็นค่อยไป การลงทุนด้วยระบบคอมพิวเตอร์ขนาดเล็กจึงเป็นระบบขยายต่อได้ ถ้าหากระบบมีการเชื่อมโยงเครือข่าย

การทำงานหลายอย่างมีขอบเขตจำกัดมาก เช่น การเรียกค้นข้อมูลระหว่างเครื่องการทำรายงานเมื่อข้อมูล เช่น การเรียกค้นข้อมูลระหว่างเครื่อง การทำรายงานเมื่อข้อมูลกระจาย ระบบข่าวสารแบบกระจายนี้จำเป็นต้องอาศัยการเชื่อมโยง การเพิ่มประสิทธิภาพของระบบเป็นไปได้มาก เพราะจะทำให้ระบบเล็กกลายเป็นระบบที่ทำงานได้ โดยมีขีดความสามารถเพิ่มขึ้น การประยุกต์ในระบบเครือข่ายมีได้หลายรูปแบบ เช่น ระบบสำนักงานอัตโนมัติ ระบบอีเมล์ ระบบการเข้าถึงข้อมูลแบบออนไลน์ เป็นต้น หากพิจารณาโครงสร้างการทำงานของเมนเฟรม คอมพิวเตอร์เหล่านั้นมีระบบการทำงานรวมศูนย์ ดังนั้นโครงสร้างจะต้องทำให้มีประสิทธิภาพสูง ใช้เทคโนโลยีที่สลับซับซ้อน ระบบเมนเฟรมจึงมีราคาแพง

อย่างไรก็ตามการที่ให้เมนเฟรมมีทุกฟังก์ชันจึงเท่ากับว่าเป็นการเพิ่มโหลดให้กับซีพียูมาก ต้นทุนของเมนเฟรมจึงสูง ระยะหลังจึงมีการพูดกันถึงเรื่องดาวน์ไซซิ่งกันมาก กล่าวคือใช้ไมโครคอมพิวเตอร์หลาย ๆ ตัวต่อเป็นเน็ตเวอร์ก โดยใช้ปรัชญาในเรื่องการทำงานร่วมกันให้ซีพียูแต่ละตัวรับผิดชอบ หรือสร้างให้มีขีดความสามารถพิเศษในรูปแบบเซอร์ฟเวอร์ เช่น ซีพียูหลักตัวหนึ่งทำหน้าที่เป็นไฟล์เซอร์ฟเวอร์ ดูแลที่เก็บข้อมูลขนาดใหญ่มาก มีซอฟต์แวร์สนับสนุนในเรื่องการเข้าถึงฐานข้อมูล การจัดข้อมูล การทำดัชนี การค้นหา ฯลฯ การให้ซีพียูบางตัว เช่น ซีพียู พวก RISC ที่มีโปรเซสเซอร์พิเศาทางคณิตศาสตร์ร่วมทำงานในแง่การคำนวณได้ดีเป็นพิเศษ อาจมีขีดความสามารถเชิงความเร็วได้สูงกว่า 50 MIPS ซีพียูส่วนนี้ทำหน้าที่เป็นคอมพิวเตอร์เซอร์ฟเวอร์ ใช้สำหรับงานกราฟิก งาน CAD เป็นต้น ปรัชญาของเครือข่ายจึงใช้หลักการที่กระจายขีดความสามารถในจุดเด่นแต่ละตัว แล้วนำมารวมเป็นระบบเดียวกัน ผู้ใช้ที่อยู่ที่ต่าง ๆ ก็สามารถเรียกใช้เข้าหาในส่วนที่ตนเองต้องการใช้น เช่น ต้องการใช้ฐานข้อมูลก็เรียกใช้ได้ ต้องการผ่านไปในระบบสื่อสารข้อมูลอื่นก็ย่อมทำได้เช่นกัน ทุกบริษัทหันเข้าหาหลักการเซอร์ฟเวอร์มากขึ้นด้วยปรัชญาดังกล่าวนี้ เกือบทุกบริษัทที่ผลิตคอมพิวเตอร์จึงต้องลดขนาดของเครื่องให้เล็กลง และทำเป็นเซอร์ฟเวอร์ที่สามารถต่อร่วมกับหลายซีพียูได้ หากดูระบบไมโครคอมพิวเตอร์ของบางบริษัท เช่น คอมแพค บริษัทคอมแพคได้สร้างระบบ System Pro เพื่อสนับสนุนหลักการนี้ โดยมีระบบปฏิบัติงานเป็นยูนิกซ์ คอมแพคใช้ซีพียู 80486 ทำหน้าที่เป็นเซอร์ฟเวอร์ให้กับเครือข่าย ไอบีเอ็มเองประสบผลสำเร็จอย่างมากในเรื่องพีซี ปัจจุบันไอบีเอ็มได้พัฒนาพีเอสทูออกมาอีกหลายโมเดล แต่ละโมเดลก็เพิ่มขีดความสามารถในเรื่องการแสดงผล เช่น โมเดล 95 ใช้ 486 เป็นซีพียู มีขีดความสามารถในการประมวลผลได้สูงมาก และทำเป็นไฟล์เซอร์ฟเวอร์ในระบบเครือข่ายได้ทั้งอีเธอร์เน็ตและโทเก้นริง นอกจากนี้ไอบีเอ็มยังได้พัฒนาระบบเวอร์กสเตชัน และยูนิกซ์ขึ้นเช่นกัน ระบบที่ไอบีเอ็มพัฒนาคือ R6000 ซึ่งมีหลายโมเดลทำตัวเป็นไฟล์เซอร์ฟเวอร์ที่ดูแลข้อมูลได้หลายสิบกิกะไบต์

ระบบเครือข่ายเชื่อมโยงได้ขยายวงอย่างกว้างขวาง เริ่มจากการมีเครือข่ายระหว่างมหาวิทยาลัยในสหรัฐอเมริกา ได้แก่ ARPANET หลังจากนั้นก็ขยายการเชื่อมโยงมากขึ้น ปัจจุบันยังมีเครือข่ายระหว่างประเทศที่แพร่หลายมาก ซึ่งได้แก่ BITNET การเชื่อมโยงนี้ทำให้การติดต่อทางด้านข้อมูลข่าวสารระหว่างนักวิจัยทำได้สะดวกขึ้น ผู้ใช้สามารถเชื่อมโยงระบบของตนเข้ากับเครือข่ายและสามารถส่ง EMAIL ถึงกันได้หมาด



รูปที่ 2 การเชื่อมโยงเน็ตเวอร์กต่าง ๆ เข้าหากัน

การสร้างเครือข่ายจะเป็นลักษณะการเชื่อมโยงเข้าหากันเป็นระบบ จากระบบเล็กเข้าสู่ระบบใหญ่ จากระบบหนึ่งเกตเวย์เข้าสู่อีกระบบหนึ่ง ในที่สุดจะมีคอมพิวเตอร์ในโลกที่เชื่อมโยงถึงกันเป็นล้าน ๆ เครื่อง ด้วยหลักวิธีการนี้ทำให้การสร้างเน็ตเวอร์กภายใน เริ่มจากหน่วยงาน เช่นภายในเริ่มจากหน่วยงานเช่นในมหาวิทยาลัยจะสร้าง Backbone Network หรือเครือข่ายหลักของตนเอง จากนั้นเชื่อมโยงต่อกับเน็ตเวอร์กระดับสูงขึ้น

ระบบเน็ตเวอร์กให้ข้อดีในหลาย ๆ ประการ จึงมีบริษัทใหญ่หลายบริษัทในสหรัฐอเมริกาได้ดำเนินการด้านหลักการดาวน์ไซซิ่ง คือ แทนเมนเฟรมด้วยเน็ตเวอร์ก แต่หลังจากพัฒนาระบบภายในพบว่าการดูแลรักษาข้อมูลทำได้ยากกว่ามาก ระบบซอฟต์แวร์ที่สร้างความปลอดภัยของข้อมูลยังมีจุดอ่อนต่อการใช้งาน นอกจากนี้หากพัฒนาในระดับลึกของการประยุกต์ที่ยุ่งยากซับซ้อนจำเป็นต้องมีซอฟต์แวร์รองรับอีกมากพอควร ยังต้องรอและให้ผู้พัฒนาระบบกระจายเพิ่มขึ้น การแก้ปัญหาในเรื่องความปลอดภัยของข้อมูลเป็นเรื่องที่น่าเป็นห่วง

จากการคาดคะเนว่า ในปี ค.ศ. 1995 ไมโครคอมพิวเตอร์ที่มีขายทั่วไป จะมีระบบเชื่อมต่อเป็นฮาร์ดแวร์พื้นฐานติดมาด้วย หลายคนคาดไว้ว่า 70 เปอร์เซ็นต์ของเครื่องไมโครคอมพิวเตอร์ในอนาคตอีกสี่ห้าปีนี้จะมีการเชื่อมโยงกัน การเชื่อมโยงจึงเป็นเทคโนโลยีที่พวกเราเตรียมตัวกันได้แล้ว ถึงแม้วันนี้จะยังมีใช้ไม่หมด แต่อีกไม่นานก็คงจะต้องใช้อย่างแน่นอน

การสื่อสารข้อมูล: ความจำเป็นของธุรกิจในปัจจุบัน

หากลองวาดภาพถึงสำนักงานแห่งหนึ่งที่พนักงานทุกคนทำงานอย่างเต็มประสิทธิภาพ ผู้จัดการฝ่ายขายต้องการรู้ข้อมูลข่าวสารของการขายสินค้าแต่ละตัวว่ามีแนวโน้มการขายเป็นอย่างไร มียอดการขายแต่ละเดือนเพิ่มขึ้นเท่าไร ผู้จัดการฝ่ายขายต้องส่งข้อมูลการสั่งสินค้าให้กับฝ่ายผลิตเพื่อเตรียมการผลิตให้ตรงกับความ

ต้องการ การติดต่อสื่อสารทางด้านข้อมูลจึงเกิดขึ้นในกลไกขององค์กร ทั้งแนวราบและแนวระดับ เพื่อให้การดำเนินการขององค์กรเป็นไปอย่างดี

ภายในสำนักงานต้องมีอุปกรณ์สื่อสารหลายอย่างประกอบกัน เริ่มต้นไปที่ระบบโทรศัพท์การสื่อสารด้วยเสียงผ่านชุมสายโทรศัพท์กลาง หรือภายในสำนักงานมีตู้ชุมสายโทรศัพท์ขนาดเล็กที่เรียกว่า PABX การสื่อสารด้านสายโทรศัพท์ยังรวมไปถึงการใช้กับเครื่องโทรสาร หรือสื่อสารข้อมูลผ่านโมเด็ม มีเทเล็กซ์ไว้ส่งข้อมูลตัวอักษรระหว่างกัน มีระบบเชื่อมโยงคอมพิวเตอร์เป็นเครือข่ายใน

ระบบสำนักงานอัตโนมัติกับเครือข่ายคอมพิวเตอร์

เครือข่ายคอมพิวเตอร์ คือการนำเอาคอมพิวเตอร์หลาย ๆ เครื่องต่อเชื่อมโยงให้มีการสื่อสารข้อมูลระหว่างกัน การเชื่อมโยงเครือข่ายคอมพิวเตอร์เข้าหากันก็ด้วยเหตุผลที่ราคาของคอมพิวเตอร์ถูกลง และต้องการเพิ่มขีดความสามารถของระบบโดยรวม หรือที่เรียกว่าการสร้างมูลค่าเพิ่ม เพราะอุปกรณ์คอมพิวเตอร์เพียงอย่างเดียวก็ทำงานได้ในตัวเองอย่างหนึ่ง แต่เมื่อต่อรวมกันจะทำงานได้เพิ่มขึ้น มีการใช้ทรัพยากรร่วมกันแลกเปลี่ยนข้อมูลข่าวสารระหว่างกัน ทำให้เกิดความสะดวกสบายในการใช้งาน มีความรวดเร็วเพิ่มขึ้น

การทำงานในสำนักงานก็เช่นเดียวกัน ที่จำเป็นต้องมีการแลกเปลี่ยนข้อมูลข่าวสารระหว่างกันภายในโต๊ะทำงานตัวหนึ่งเสมือนจุดการประมวลผล การวิเคราะห์ การแยกแยะข้อมูลข่าวสาร แล้วส่งต่อให้โต๊ะอื่น ๆ หรือหน่วยอื่น ๆ ต่อไป การเชื่อมโยงเครือข่ายเป็นระบบก็เช่นเดียวกัน เป็นการเชื่อมโยงระบบประมวลผลหรือคอมพิวเตอร์หลาย ๆ ระบบเข้าด้วยกัน ระบบสำนักงานอัตโนมัติจึงเป็นเรื่องของการประมวลผลในจุดต่าง ๆ แล้วส่งข้อมูลเข้าหากันผ่านทางเครือข่าย

อุปกรณ์สำนักงานที่เชื่อมต่อเป็นเครือข่าย

ภายในสำนักงานย่อมมีเครื่องใช้สำนักงานต่าง ๆ ประกอบกันอยู่มาก ในอดีตต้องมีตู้เก็บเอกสาร เก็บแฟ้มข้อมูล มีเครื่องคิดเลข กระดาษ ดินสอ การทำงานก็มีแบบฟอร์มต่าง ๆ ที่ต้องกรอก ต้องประมวลผลหรือคิดคำนวณ การส่งเอกสารกระทำโดยเด็กส่งหนังสือ การสรุปผลหรือทำรายงานยุ่งยากเสียเวลา เช่น การสรุปยอดขายหรือทำบัญชีต้องมีการกรอกข้อมูล คิดคำนวณตัวเลขเป็นจำนวนมาก

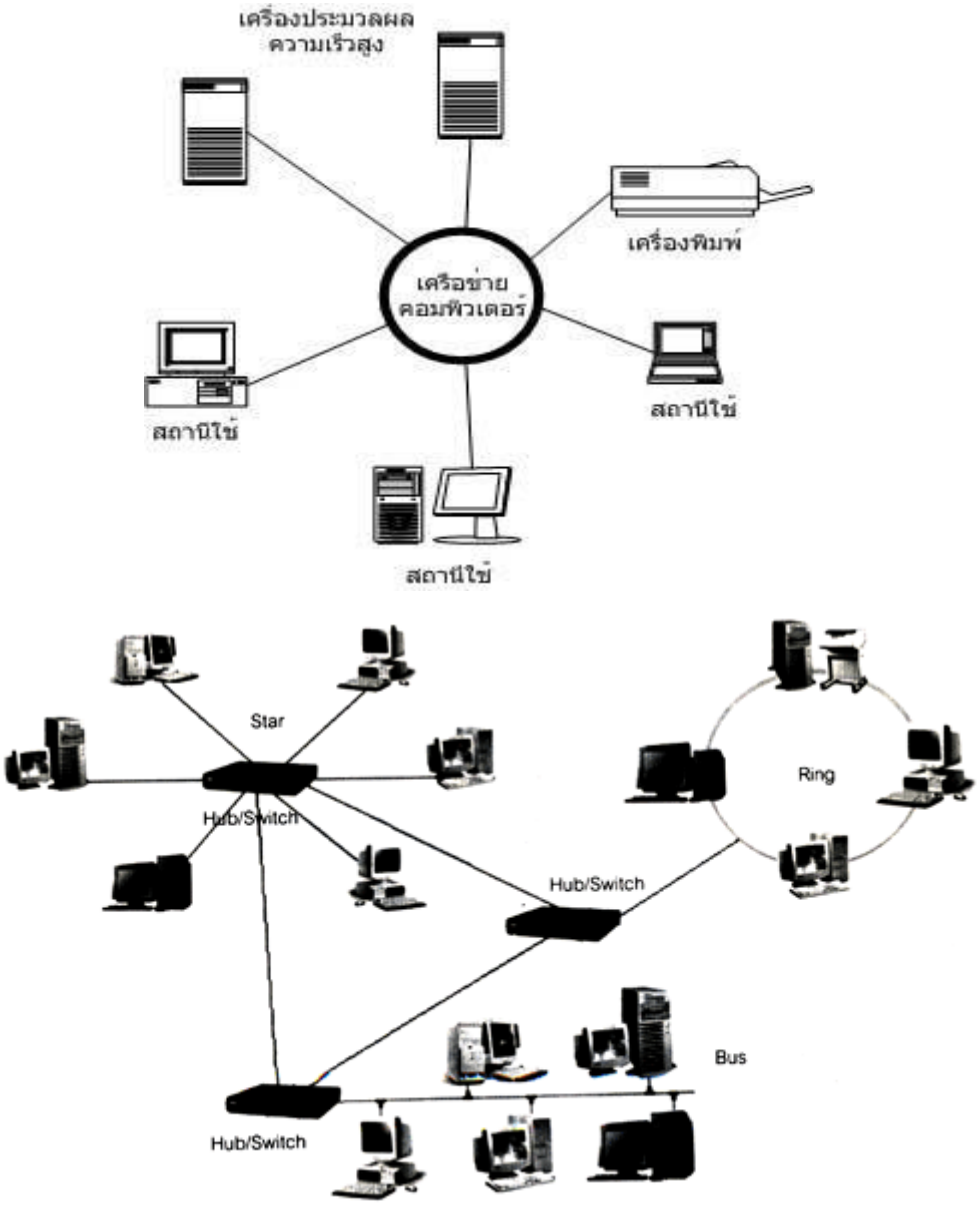
ในปัจจุบันมีอุปกรณ์สำนักงานช่วยอำนวยความสะดวกมากมาย มีเครื่องพิมพ์ที่ใช้คอมพิวเตอร์ช่วย เรียกว่าเวิร์ดโปรเซสเซอร์ ส่วนที่ก้าวหน้าขึ้นไปก็เรียกว่าเดสท็อปพับปลิชเชอร์มีการใช้คอมพิวเตอร์ช่วยในการคิดคำนวณและประมวลผลเก็บข้อ เช่น ฟลอปปี้ดิสก์ ฮาร์ดดิสก์ ข้อมูลที่จัดเก็บสามารถเรียกมาใช้สรุปผล สร้างรายงาน ทำกราฟ การส่งข้อมูลข่าวสารระหว่างกันก็ทำในรูปการสื่อสารข้อมูล ระบบการทำงานจึงเกี่ยวข้องกับอุปกรณ์อิเล็กทรอนิกส์หลายอย่าง ซึ่งสามารถผนวกเข้าหากันเป็นระบบเดียวกันได้ อุปกรณ์สำนักงานเหล่านี้ได้แก่ โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องพิมพ์ หรือเชื่อมโยงเข้ากับระบบตรวจสอบต่าง ๆ เช่น ตรวจวัดอุณหภูมิความชื้น ระบบรักษาความปลอดภัย ระบบการนับจำนวน เป็นต้น การเชื่อมโยงเหล่านี้ก็เพื่อให้มีการส่งถ่าย หรือรับข้อมูลได้อย่างอัตโนมัติ

โครงข่ายของระบบในสำนักงาน

หลักการของคอมพิวเตอร์หรืออุปกรณ์รับ-ส่งข้อมูลที่ประกอบเป็นเครือข่าย ที่มีการเชื่อมโยง ต้องเชื่อมต่อถึงกัน รูปแบบหลายอย่างตามความเหมาะสมซึ่งขึ้นกับเทคโนโลยี โครงข่ายการเชื่อมโยงนี้เรียกว่าโทโปโลยี เช่น ถ้าหากพิจารณาว่าภายในสำนักงานมีอุปกรณ์สำนักงานที่ใช้งานอยู่กระจัดกระจาย และต้องการเชื่อมโยงต่อถึงกัน หากต้องการเชื่อมต่อโดยตรงจะต้องใช้สายเชื่อมโยงมาก ดังรูปที่ 1

ปัญหาของการเชื่อมต่อคอมพิวเตอร์ หรืออุปกรณ์เทอร์มินัลหลาย ๆ ครั้ง เห็นจะได้แก่ สายเชื่อมโยงระหว่างสถานีที่เพิ่มขึ้นเป็นจำนวนมาก และระบบการสวิตซ์เพื่อใช้เชื่อมโยงข้อมูลในการสื่อสารระหว่างสถานี หากใช้สถานีมากขึ้นการเชื่อมโยงต้องใช้สายมากขึ้นอีกมาก และขณะที่สถานีหนึ่งทำงานก็จะใช้เส้นทางตรงไปยังอีกสถานี ทำให้การใช้สายสัญญาณไม่เต็มประสิทธิภาพ

จึงมีความพยายามที่จะหารูปแบบการลดจำนวนสายสัญญาณเพิ่มประสิทธิภาพ ลดค่าใช้จ่าย ซึ่งก็มีโทโปโลยีในการใช้สื่อสารหลายรูปแบบ ดังรูป



รูปโครงข่าย

รูปแบบดาวมีรูปแบบการต่อโดยการนำสถานีต่าง ๆ หลายสถานีต่อรวมกันเป็นหน่วยสวิตชิงกลาง การติดต่อสื่อสารระหว่างสถานีจะกระทำได้ด้วยการติดต่อผ่านทางวงจรสวิตชิง การทำงานของหน่วยสวิตชิงกลางจึงคล้ายกับศูนย์กลางของการตัดต่อวงจรเชื่อมโยงระหว่างสถานีต่าง ๆ ที่ต้องการติดต่อกัน

รูปแบบวงแหวนประกอบด้วยสัญญาณข้อมูลจากสถานีต่าง ๆ ที่เรียกว่า รีพีตเตอร์ (repeter) ทำหน้าที่รับข้อมูลจากสถานีแล้วต่อไปยังรีพีตเตอร์ตัวถัดไปเรื่อย ๆ เป็นรูปวงกลม หากข้อมูลที่ส่งเป็นสถานีใด รีพีตเตอร์ของสถานีนั้นก็รับและส่งให้กับสถานี รีพีตเตอร์จึงมีหน้าที่รับข้อมูลและตรวจสอบว่าเป็นของตนเองหรือไม่ ถ้าใช่ก็รับไว้ ถ้าไม่ใช่ก็ส่งต่อไป

รูปแบบบัสและทรีเป็นรูปแบบที่มีผู้นิยมใช้มากแบบหนึ่ง เพราะมีโครงสร้างไม่ยุ่งยาก และไม่ต้องใช้รีพีตเตอร์หรืออุปกรณ์สวิตชิ่งเหมือนแบบวงแหวน หรือรูปดาว ทุก ๆ สถานีจะเชื่อมต่อเข้าหาบัสโดยผ่านทางอุปกรณ์อินเตอร์เฟสที่เป็นฮาร์ดแวร์ การจัดส่งข้อมูลลงบนบัสจึงสามารถทำให้ข้อมูลไปถึงอุปกรณ์ทุกสถานีได้ การจัดส่งในวิธีนี้จึงต้องมีการกำหนดวิธีการที่จะไม่ให้ทุกสถานีส่งข้อมูลพร้อมกัน เพราะจะทำให้ข้อมูลชนกัน วิธีการจัดแบ่งอาจแบ่งช่วงเวลา หรือให้แต่ละสถานีใช้ความถี่สัญญาณแตกต่างกัน

ความสำคัญอยู่ที่วิธีการทำให้ทุกสถานีสื่อสารถึงกันได้

หากพิจารณาว่าภายในองค์กรหนึ่งเสมือนมีโครงข่ายข้อมูลอยู่โครงข่ายหนึ่ง ดังนั้นทุก ๆ สถานีจะต่อร่วมเข้าหาโครงข่ายนี้ หรือหากมองภาพที่กว้างออกไป เช่น ธนาคารแห่งหนึ่งมีสาขาอยู่ทั่วประเทศ คอมพิวเตอร์หรืออุปกรณ์ประมวลผลข้อมูลอื่น เช่น เอทีเอ็มทุกตัวก็เชื่อมเข้ากับเครือข่ายสื่อสารข้อมูลเช่นกัน โครงข่ายสื่อสารข้อมูลที่อยู่ในพื้นที่จำกัด ก็เรียกว่าระบบโครงข่ายท้องถิ่น (แลน-LAN - Local Area Network) หากอยู่ระหว่างห่างไกลกันมาก ๆ ก็เรียกว่า แวน (WAN - Wide Area Network) ไม่ว่าจะเป็นโครงข่ายอย่างไรอาจเขียนแทนได้

การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์

การสื่อสารข้อมูล (Data communication) หมายถึง การส่งข้อมูลหรือข่าวสาร จากผู้ส่งต้นทางไปยังผู้รับปลายทางที่อยู่ห่างไกล โดยผ่านช่องทางการสื่อสารเพื่อเป็นสื่อกลางในการส่งข้อมูล ซึ่งอาจจะเป็นแบบใช้สายหรือไม่ใช้สายก็ได้ ส่วนข้อมูลหรือข่าวสารนั้นอาจจะเป็นข้อความ เสียง ภาพเคลื่อนไหว หรือข้อมูลที่เป็นมัลติมีเดียก็ได้ ดังนั้นการสื่อสารข้อมูลจึงเป็นส่วนหนึ่งของการสื่อสารโทรคมนาคม โดยเน้นการส่งผ่านข้อมูล โดยใช้ระบบคอมพิวเตอร์และเครือข่ายเป็นหลัก

เครือข่ายคอมพิวเตอร์ หมายถึง การนำคอมพิวเตอร์และอุปกรณ์ต่าง ๆ มาเชื่อมต่อถึงกันโดยใช้สายเคเบิ้ลเป็นสื่อกลางในการแลกเปลี่ยนชุดข้อมูล ชุดคำสั่ง และข่าวสารต่าง ๆ ระหว่างคอมพิวเตอร์ กับ 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

องค์ประกอบของการสื่อสาร

ปี 1960 แบบจำลอง SMCR ของเบอร์โล (Berlo) ได้ให้ความสำคัญกับสิ่งต่าง ๆ คือ

1. ผู้ส่งสาร (Source) ต้องเป็นผู้ที่มีความสามารถเข้ารหัส(Encode) เนื้อหาข่าวสารได้มีความรู้อย่างดีในข้อมูลที่จะส่งสามารถปรับระดับให้เหมาะสมสอดคล้องกับผู้รับ
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)

การใช้เทคโนโลยีในการสื่อสาร

เทคโนโลยี เป็นการนำเอาแนวความคิด หลักการ เทคนิค ความรู้ ระเบียบวิธี กระบวนการ ตลอดจนผลผลิตทางวิทยาศาสตร์ทั้งในด้านสิ่งประดิษฐ์และวิธีปฏิบัติมาประยุกต์ใช้ในระบบงานเพื่อช่วยให้เกิดการเปลี่ยนแปลงในการทำงานให้ดียิ่งขึ้นและเพื่อเพิ่มประสิทธิภาพและประสิทธิผลของงานให้มีมากยิ่งขึ้น

การสื่อสาร หมายถึง การนำสื่อหรือข้อความของฝ่ายหนึ่งส่งให้อีกฝ่ายหนึ่ง ประกอบด้วยผู้ส่งข่าวสารหรือแหล่งกำเนิดข่าวสาร ช่องทางการส่งข้อมูลซึ่งเป็นสื่อกลางหรือตัวกลางอาจเป็นสายสัญญาณ และหน่วยรับข้อมูลหรือผู้รับสาร

ดังนั้น **เทคโนโลยีในการสื่อสาร** คือ การเอาแนวคิด หลักการ เทคนิค ระเบียบวิธี กระบวนการ ผ่านช่องทางการส่งข้อมูล ซึ่งทำให้ผู้รับ ได้รับและเข้าถึงข้อมูลได้เร็วขึ้น เทคโนโลยีที่ใช้ในการสื่อสารที่พบเห็น เช่น E-mail, Voice Mail, Video Conferencing เป็นต้น

ชนิดของสัญญาณข้อมูล

ชนิดของสัญญาณแบ่งได้เป็น 2 ชนิดคือ

1.Analog signalเป็นสัญญาณต่อเนื่อง ลักษณะของคลื่นไซน์ sine wave ตัวอย่างการส่งข้อมูลที่เป็น analog คือการส่งข้อมูลผ่านระบบโทรศัพท์

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

Bit rate เป็นอัตราความเร็วในการส่งข้อมูล โดยนับจำนวน bit ที่ส่งได้ในช่วง 1 วินาที เช่น ส่งข้อมูลได้ 14,400 bps (bit per seconds)

ทิศทางการส่งข้อมูล

ทิศทางการส่งข้อมูล สามารถจำแนกทิศทางการส่งข้อมูลได้ 3 รูปแบบ ดังนี้

1. **การส่งข้อมูลแบบทิศทางเดียว** (Simplex transmission) เป็นการสื่อสารข้อมูลที่มีผู้ส่งข้อมูลทำหน้าที่ส่งข้อมูลแต่เพียงอย่างเดียว และผู้รับข้อมูลก็ทำหน้าที่รับข้อมูลแต่เพียงอย่างเดียวเช่นกัน การส่งข้อมูลในลักษณะนี้เช่น การส่งข้อมูลของสถานีโทรทัศน์

2. **การส่งข้อมูลแบบสองทิศทางสลับกัน** (Half-duplex transmission) เป็นการสื่อสารข้อมูลที่มีการแลกเปลี่ยนข้อมูลทั้งผู้รับและผู้ส่ง โดยแต่ละฝ่ายสามารถเป็นทั้งผู้รับและผู้ส่งข้อมูลได้ แต่จะต้องสลับกันทำหน้าที่จะเป็นผู้ส่งและผู้รับข้อมูลพร้อมกันทั้งสองฝ่ายไม่ได้ เช่น การสื่อสารโดยวิทยุ

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

ตัวกลางการสื่อสาร

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

1. สื่อกลางประเภทมีสาย
2. สื่อกลางประเภทไร้สาย

1.1สายคู่บิดเกลียว (twisted pair) ประกอบด้วยเส้นลวดทองแดงที่หุ้มด้วยฉนวนพลาสติก 2 เส้นพันบิดเป็นเกลียว เพื่อลดการรบกวนจากคลื่นแม่เหล็กไฟฟ้าจากคู่สายข้างเคียงภายในเคเบิลเดียวกันหรือจากภายนอก เนื่องจากสายคู่บิดเกลียวนี้ยอมให้สัญญาณไฟฟ้าความถี่สูงผ่านได้ สำหรับอัตราการส่งข้อมูลผ่านสายคู่บิดเกลียวจะขึ้นอยู่กับความหนาของสาย คือ สายทองแดงที่มีเส้นผ่านศูนย์กลางกว้าง จะสามารถส่งสัญญาณไฟฟ้ากำลังแรงได้ ทำให้สามารถส่งข้อมูลด้วยอัตราส่งสูง โดยทั่วไปแล้วสำหรับการส่งข้อมูลแบบดิจิทัลสัญญาณที่ส่งเป็นลักษณะคลื่นสี่เหลี่ยม สายคู่บิดเกลียวสามารถใช้ส่งข้อมูลได้ถึงร้อยเมกะบิตต่อวินาที ในระยะทางไม่เกินร้อยเมตร เนื่องจากสายคู่บิดเกลียว มีราคาไม่แพงมาก ใช้ส่งข้อมูลได้ดี จึงมีการใช้งานอย่างกว้างขวาง ตัวอย่างเช่น

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

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

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

1.3 เส้นใยนำแสง (fiber optic) มีแกนกลางของสายซึ่งประกอบด้วยเส้นใยแก้วหรือพลาสติกขนาดเล็กหลายๆ เส้นอยู่รวมกัน เส้นใยแต่ละเส้นมีขนาดเล็ดเท่าเส้นผมและภายในกลวง และเส้นใยเหล่านั้นได้รับการห่อหุ้มด้วยเส้นใยอีกชนิดหนึ่งก่อนจะหุ้มชั้นนอกสุดด้วยฉนวน การส่งข้อมูลผ่านทางสื่อกลางชนิดนี้จะแตกต่างจากชนิดอื่นๆ ซึ่งใช้สัญญาณไฟฟ้าในการส่ง แต่การทำงานของสื่อกลางชนิดนี้จะใช้เลเซอร์วิ่งผ่านช่องกลวงของเส้นใยแต่ละเส้นและอาศัยหลักการหักเหของแสงโดยใช้ใยแก้วชั้นนอกเป็นกระจกสะท้อนแสง การให้แสงเคลื่อนที่ไปในท่อแก้วสามารถส่งข้อมูลด้วยอัตราความหนาแน่นของสัญญาณข้อมูลสูงมากและไม่มีการก่อกวนของคลื่นแม่เหล็กไฟฟ้า ปัจจุบันถ้าใช้เส้นใยนำแสงกับระบบอีเทอร์เน็ตจะใช้ได้ด้วยความเร็วหลายร้อยเมกะบิต และเนื่องจากความสามรถในการส่งข้อมูลด้วยอัตราความหนาแน่นสูง ทำให้สามารถส่งข้อมูลทั้งตัวอักษร เสียง ภาพกราฟิก หรือวีดิทัศน์ได้ในเวลาเดียวกัน อีกทั้งยังมีความปลอดภัยในการส่งสูง แต่อย่างไรก็มีข้อเสียเนื่องจากการบิดงอสายสัญญาณจะทำให้เส้นใยหัก จึงไม่สามารถใช้สื่อกลางนี้ในการเดินทางตามมุมตึกได้ เส้นใยนำแสงมีลักษณะพิเศษที่ใช้สำหรับเชื่อมโยงแบบจุดไปจุด จึงเหมาะที่จะใช้กับการเชื่อมโยงระหว่างอาคารกับอาคารหรือระหว่างเมืองกับเมือง เส้นใยนำแสงจึงถูกนำไปใช้เป็นสายแกนหลัก

2.1 **สัญญาณไมโครเวฟ** (Microwave) เป็นสื่อกลางในการสื่อสารที่มีความเร็วสูง ส่งข้อมูลโดยอาศัยสัญญาณไมโครเวฟซึ่งเป็นสัญญาณคลื่นแม่เหล็กไฟฟ้าไปในอากาศพร้อมกับข้อมูลที่ต้องการส่ง และจะต้องมีสถานีที่ทำหน้าที่ส่งและรับข้อมูล และเนื่องจากสัญญาณไมโครเวฟจะเดินทางเป็นเส้นตรงไม่สามารถเลี้ยวหรือโค้งตามขอบโลกที่มีความโค้งได้ จึงต้องมีการตั้งสถานีรับ-ส่งข้อมูลเป็นระยะๆ และส่งข้อมูลต่อกันเป็นทอดๆ ระหว่างสถานีต่อสถานีจนกว่าจะถึงสถานีปลายทาง และแต่ละสถานีจะตั้งอยู่ในที่สูงเช่นดาดฟ้าตึกสูงหรือยอดดอยเพื่อหลีกเลี่ยงการชนหากมีสิ่งกีดขวางเนื่องจากแนวการเดินทางที่เป็นเส้นตรงของสัญญาณดังที่กล่าว

มาแล้ว การส่งข้อมูลด้วยสื่อกลางชนิดนี้เหมาะกับการส่งข้อมูลในพื้นที่ห่างไกลมากๆ และทุรกันดาร

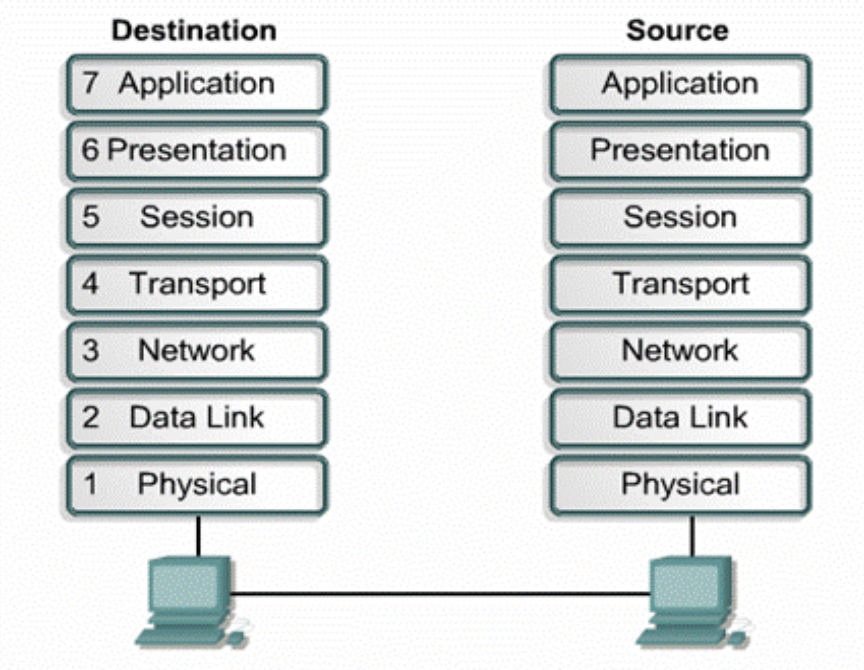
2.2 ดาวเทียม (satilite) ได้รับการพัฒนาขึ้นมาเพื่อหลีกเลี่ยงข้อจำกัดของสถานีรับ-ส่งไมโครเวฟบนผิวโลก วัตถุประสงค์ในการสร้างดาวเทียมเพื่อเป็นสถานีรับ-ส่งสัญญาณไมโครเวฟบนอวกาศและทวนสัญญาณในแนวโคจรของโลก ในการส่งสัญญาณดาวเทียมจะต้องมีสถานีภาคพื้นดินคอยทำหน้าที่รับและส่งสัญญาณขึ้นไปบนดาวเทียมที่โคจรอยู่สูงจากพื้นโลก 22,300 ไมล์ โดยดาวเทียมเหล่านั้นจะเคลื่อนที่ด้วยความเร็วที่เท่ากับการหมุนของโลก จึงเสมือนกับดาวเทียมนั้นอยู่นิ่งอยู่กับที่ขณะที่โลกหมุนรอบตัวเอง ทำให้การส่งสัญญาณไมโครเวฟจากสถานีหนึ่งขึ้นไปบนดาวเทียมและการกระจายสัญญาณจากดาวเทียมลงมายังสถานีตามจุดต่างๆ บนผิวโลกเป็นไปอย่างแม่นยำ ดาวเทียมสามารถโคจรอยู่ได้โดยอาศัยพลังงานที่ได้มาจากการเปลี่ยนพลังงานแสงอาทิตยด้วยแผงโซลาร์ (solar panel)

ความรู้เกี่ยวกับ OSI Model

ISO (International Standards Organization) เป็นหน่วยงาน ที่มีหน้าที่พัฒนา มาตรฐานสำหรับ การสื่อสารข้อมูล ในประเทศ และระหว่างประเทศ ในช่วงต้นทศวรรษ 1970 ISO ได้พัฒนาแบบจำลอง OSI (Open Systems Interconnection) ขึ้นเพื่อใช้เป็นมาตรฐาน สำหรับการออกแบบอุปกรณ์ ของผู้ผลิตเพื่อที่อุปกรณ์ จากต่างผู้ผลิตสามารถสื่อสารกันได้ แบบจำลอง OSI ประกอบด้วย 7 เลเยอร์ (layer) อธิบายถึงสิ่งที่เกิดขึ้น เมื่ออุปกรณ์ที่เชื่อมโยงกันสนทนากัน Layer ทั้ง 7 จะสนับสนุนในส่วนฮาร์ดแวร์ และซอฟท์แวร์ รวมทั้งการติดต่อถึงกัน ของทั้งสองข้างที่ต้องการสื่อสารเข้าด้วยกัน คือ ด้านส่ง และด้านรับจึงได้เกิดหน่วยงานกำหนดมาตรฐานสากลขึ้นคือ International Standards Organization ขึ้นและทำการกำหนดโครงสร้างทั้งหมดที่จำเป็นต้องใช้ในการสื่อสารข้อมูล และเป็นระบบเปิด เพื่อให้ผู้ผลิตต่างๆสามารถแยกผลิตในส่วนที่ตัวเองถนัดแต่สามารถนำไปใช้ร่วม กันได้ระบบเครือข่ายคอมพิวเตอร์สมัยใหม่จะถูกออกแบบให้มีโครงสร้างทีแน่นอน และเพื่อเป็นการลดความซับซ้อน ระบบเครือข่ายส่วนมากจึงแยกการทำงานออกเป็นชั้นๆ (layer) โดยกำหนดหน้าที่ในแต่ละชั้นไว้อย่างชัดเจน แบบจำลองสำหรับอ้างอิงแบบ OSI (Open System Interconnection Reference Model) หรือที่นิยมเรียกกันทั่วไปว่า OSI Reference Model ของ ISO เป็นแบบจำลองที่ถูกเสนอและพัฒนาโดยองค์กร International Standard Organization (ISO) โดยจะบรรยายถึงโครงสร้างของสถาปัตยกรรมเครือข่ายในอุดมคติซึ่งระบบเครือข่าย ที่เป็นไปตามสถาปัตยกรรมนี้จะเป็นระบบเครือข่ายแบบเปิดและอุปกรณ์ทางเครือ ข่ายจะสามารถติดต่อกันได้โดยไม่ขึ้นกับว่าเป็นอุปกรณ์ของผู้ขายรายใด

แบบจำลอง OSI 7 Layer Reference Model

แบบจำลอง OSI จะแบ่งการทำงานของระบบเครือข่ายออกเป็น 7 ชั้น คือ



รูปแสดงแบบจำลอง OSI 7 Layer Reference Model

แต่ละชั้น ของแบบการสื่อสารข้อมูลเรียกว่า Layer ประกอบด้วย Layer ย่อยๆทั้งหมด7 Layerแต่ละชั้นทำหน้าที่รับส่งข้อมูลกับชั้นที่อยู่ติดกับตัวเองเท่านั้นจะ ไม่
ติดต่อกระโดดข้ามไปยังชั้นอื่นๆเช่น Layer 6จะติดต่อกับ Layer5 และ Layer7 เท่านั้นและการส่งข้อมูลจะทำไล่จาก Layer7 ลงมาจนถึง Layer1 ซึ่งเป็นชั้นที่มีการเชื่อมต่อทางกายภาพ จากนั้นข้อมูลจะถูกส่งไปยังเครื่องผู้รับปลายทางโดยเริ่มจาก Layer1 ข้อมูลก็จะถูกถอดรหัส และส่งขึ้นไปตาม Layer จนถึง Layer7 ก็จะประกอบกลับมาเป็นข้อมูล นำไปส่งให้ application นำไปใช้แสดงผลต่อไป

มาตรฐานเครือข่ายไร้สาย (Wireless Networking Protocols)

ด้วยความเจริญเติบโตอย่างรวดเร็วของเทคโนโลยีเครือข่ายไร้สายได้ส่งผลให้อุปกรณ์อิเล็กทรอนิกส์ เช่น พีดีเอ โทรศัพท์มือถือ ตลอดจนโรงงานอุตสาหกรรมโทรคมนาคมมีความต้องการมาตรฐานเพื่อการสื่อสารไร้สาย ในที่นี้กล่าวถึงการสื่อสารไร้สายดังนี้ (ศรีไพร ศักดิ์รุ่งพงศากุล และ เจษฎาพร ยุทธนวิบูลย์ชัย. 2549 : 106-108)

บลูทูธ (Bluetooth) บลูทธเป็นชื่อที่เรียกสำหรับมาตรฐานเรือข่ายแบบ 802.15 บลูทูธเป้นเทคโนโลยีไร้สายที่ใช้การส่งข้อมูลทางคลื่นวิทยุ (Universal Radio Interface) เริ่มใช้ในปี ค.ศ. 1998 สำหรับการเชื่อมโยงสื่อสารไร้สายในแถบความถี่ 2.45 GHz ซึ่งเป็นอุปการณ์อิเล็กทรอนิกส์ที่ถือเคลื่อนย้ายได้ สามารถติดต่อเชื่อมโยงสื่อสารแบบไร้สายระหว่างกันในช่วงระยะห่างสั้น ๆ ได้

ไว-ไฟ (Wi-Fi) ไว-ไฟ ย่อมาจากคำว่า Wireless Fidelity คือมาตรฐานที่รับรองว่าอุปกาณ์ไวร์เลว (Wireless LAN) สามารถทำงานร่วมกันได้ และสนับสนุนมาตรฐาน IEEE802.11b

ไว-ไฟ เป็นเทคโนโลยีอินเทอร์เน็ตไร้สายความเร็วสูงที่นิยมใช้ที่สุดในโลก ใช้สัญญาณวิทยุในการรับส่งข้อมูลความเร็วสูงผ่านเครือข่ายไร้สายจากบริเวณที่มีการติดตั้ง Access Point ไปยังอุปกรณ์ที่ใช้เชื่อมต่อ เช่น โทรศัพท์มือถือ พีดีเอ และโนตบุคเป็นต้น

ไว- แมกซ์ (Wi-MAX) เป็นชื่อเรียกเทคโนโลยีไร้สายรุ่นใหม่ล่าสุดที่คาดหมายกันว่าจะถูกนำมาใช้งานที่ประเทศไทยอย่างเป็นทางการ ในอนาคตอันใกล้นี้ (ตอนนี้มีแอบทดสอบ WiMAX กันหลายที่ในต่างจังหวัดแล้ว เช่น ที่เชียงใหม่) ซึ่งเป็นเทคโนโลยีบรอดแบนด์ไร้สายความเร็วสูงรุ่นใหม่ตัวนี้ ได้รับการพัฒนาขึ้นมาบนมาตรฐานที่เรียกเป็นทางการว่า IEEE 802.16

ซึ่งต่อมาก็ได้พัฒนามาตรฐาน IEEE 802.16a (เหมือนกับมาตรฐานสากลตัวแรก แต่มี a ต่อท้าย) ขึ้น โดยได้อนุมัติโดย IEEE มาเมื่อเดือนมกราคม 2004 ซึ่ง IEEE ที่ว่า ก็คือสถาบันวิศวกรรมไฟฟ้าและอิเล็กทรอนิกส์ หรือชื่อเต็มๆก็คือ Institute of Electrical and Electronics Engineers โดยเจ้าระบบ WiMAX นี้มีซึ่งมีรัศมีทำการไกลสูงสุดที่ 30 ไมล์ หรือเป็นระยะทางประมาณ 48 กิโลเมตร (คนล่ะโลกกับ WiFi ที่เรารู้จักกันเลยทีเดียว)

ซึ่งนั่นหมายความว่า WiMAX สามารถให้บริการครอบคลุมพื้นที่กว้างกว่าระบบโครงข่ายโทรศัพท์เคลื่อนที่ระบบ 3G (ซึ่งก็เป็นระบบมือถือในอนาคตของประเทศไทยเราอีกนั้นแหละ เพียงแต่ตอนนี้เราใช้ 2.5G กันอยู่) มากถึง 10 เท่า ยิ่งกว่านั้นก็ยังมีอัตราความเร็วในการส่งผ่านข้อมูลสูงสุดถึง 75 เมกะบิตต่อวินาที (Mbps) ซึ่งเร็วกว่า 3G ถึง 30 เท่าทีเดียว และแน่นอนว่าเร็วกว่าระบบ WiFi ด้วย

เครือข่ายคอมพิวเตอร์

เครือข่ายคอมพิวเตอร์ คือ ระบบการสื่อสารระหว่างคอมพิวเตอร์จำนวนตั้งแต่สองเครื่องขึ้นไปการที่ระบบเครือข่ายมีบทบาทสำคัญมากขึ้นในปัจจุบัน เพราะมีการใช้งานคอมพิวเตอร์อย่างแพร่หลาย จึงเกิดความ

ต้องการที่จะเชื่อมต่อคอมพิวเตอร์เหล่านั้นถึงกัน เพื่อเพิ่มความสามารถของระบบให้สูงขึ้น และลดต้นทุนของระบบโดยรวมลง

การโอนย้ายข้อมูลระหว่างกันในเครือข่าย ทำให้ระบบมีขีดความสามารถเพิ่มมากขึ้น การแบ่งการใช้ทรัพยากร เช่น หน่วยประมวลผล, หน่วยความจำ, หน่วยจัดเก็บข้อมูล, โปรแกรมคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ที่มีราคาแพงและไม่สามารถจัดหามาให้ทุกคนได้ เช่น เครื่องพิมพ์ เครื่องกราดภาพ (scanner) ทำให้ลดต้นทุนของระบบลงได้

องค์ประกอบพื้นฐานของเครือข่าย

การที่คอมพิวเตอร์จะเชื่อมต่อกันเป็นเครือข่ายได้ ต้องมีองค์ประกอบพื้นฐานดังต่อไปนี้

- คอมพิวเตอร์ อย่างน้อย 2 เครื่อง
- เน็ตเวิร์คการ์ด หรือ NIC (Network Interface Card) เป็นการ์ดที่เสียบเข้ากับช่องเมนบอร์ดของคอมพิวเตอร์ ซึ่งเป็นจุดเชื่อมต่อระหว่างคอมพิวเตอร์และเครือข่าย
- สื่อกลางและอุปกรณ์สำหรับการรับส่งข้อมูล เช่น สายสัญญาณ สายสัญญาณที่เป็นที่นิยมในเครือข่าย เช่น สายโคแอ็กเชียล สายคู่เกลียวบิด และสายใยแก้วนำแสง เป็นต้น ส่วนอุปกรณ์เครือข่าย เช่น ฮับ สวิตซ์ เราท์เตอร์ เกตเวย์ เป็นต้น
- โปรโตคอล (Protocol) โปรโตคอลเป็นภาษาที่คอมพิวเตอร์ใช้สื่อสารกันผ่านเครือข่ายคอมพิวเตอร์ที่สามารถสื่อสารกันได้นั้นจำเป็นที่ต้องใช้ “ภาษา” หรือโปรโตคอลเดียวกัน เช่น OSI, TCP/IP, IPX/SPX เป็นต้น
- ระบบปฏิบัติการเครือข่าย หรือ NOS (Network Operating System) ระบบปฏิบัติการเครือข่ายจะเป็นตัวที่คอยจัดการเกี่ยวกับการใช้งานเครือข่ายของผู้ใช้แต่ละคน หรือเป็นตัวจัดการและควบคุมการใช้ทรัพยากรต่างๆ ของเครือข่าย ระบบปฏิบัติการเครือข่ายที่เป็นที่นิยม เช่น Windows Server 2003, Novell NetWare, Sun Solaris และ Red Hat Linux เป็นต้น

โครงสร้างเครือข่ายคอมพิวเตอร์ (Topology)

การนำเครื่องคอมพิวเตอร์มาเชื่อมต่อกันเพื่อประโยชน์ของการสื่อสารนั้น สามารถกระทำได้หลายรูปแบบ ซึ่งแต่ละแบบก็มีจุดเด่นต่างกันไป โดยทั่วไปแล้วโครงสร้างของเครือข่ายคอมพิวเตอร์สามารถจำแนกตามลักษณะการเชื่อมต่อได้ดังนี้

1. **เครือข่ายแบบบัส** (Bus Network)

เป็นเครือข่ายที่เชื่อมต่อคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ด้วยสายเคเบิ้ลยาวต่อเนื่องไปเรื่อย ๆ โดยมีตัวเชื่อมต่อคอมพิวเตอร์ และอุปกรณ์เข้ากับสายเคเบิ้ลในการส่งข้อมูลจะมีคอมพิวเตอร์เพียงตัวเดียวเท่านั้นที่สามารถส่งข้อมูลได้ในช่วงเวลาหนึ่ง ๆ การจัดส่งข้อมูลวิธีนี้มีวิธีการที่จะไม่ให้ทุกสถานี ส่งข้อมูลพร้อมกันเพราะจะทำให้ข้อมูลชนกัน การติดตั้งเครือข่ายแบบนี้ทำได้ไม่ยาก เพราะคอมพิวเตอร์และอุปกรณ์

แต่ละชนิดถูกเชื่อมต่อด้วยสายเคเบิ้ลเพียงเส้นเดียว โดยส่วนใหญ่เครือข่ายแบบบัสมักจะใช้ในเครือข่ายขนาดเล็ก ซึ่งอยู่ในองค์กรที่มีเครื่อง คอมพิวเตอร์ใช้ไม่มากนัก

ข้อดี ประหยัดสายสัญญาณ เครื่องหนึ่งเสียก็ไม่กระทบกับเครือข่าย
ข้อเสีย อาจเกิดการชนกันของ ข้อมูลได้ ต้องมีการส่งใหม่ ถ้าสายหลักเสีย เครือข่ายล่ม

2. **เครือข่ายแบบดาว** (Star Network)

เป็นเครือข่ายที่เชื่อมต่อคอมพิวเตอร์ เข้ากับอุปกรณ์ที่เป็นจุดศูนย์กลางของเครือข่าย โดยการนำสถานีต่าง ๆ มาต่อร่วมกันกับหน่วยสลับสายกลาง การติดต่อสื่อสารระหว่างสถานีจะกระทำได้ด้วยการติดต่อผ่านทางวงจรของ หน่วยสลับสายกลางการทำงานของหน่วยสลับสายกลางจึงเป็นศูนย์กลาง ของการติดต่อวงจรเชื่อมโยงระหว่างสถานีต่าง ๆ ที่ต้องการติดต่อกัน

ข้อดี ติดตั้งและดูแลง่าย ถ้าเครื่องลูกข่ายเสียก็ตรวจสอบได้ง่าย เครื่องอื่นยังติดต่อกันได้
ข้อเสีย ถ้าฮับเสีย เครือข่ายล่ม ใช้สัญญาณมากกว่าแบบอื่น

3. **เครือข่ายแบบวงแหวน** (Ring Network)

เป็นเครือข่ายที่เชื่อมต่อเครื่อง คอมพิวเตอร์ด้วยสายเคเบิ้ลเพียงเส้นเดียวในลักษณะวงแหวน การรับส่งข้อมูลในเครือข่ายวงแหวนจะใช้ทิศทางเดียวเท่านั้นเมื่อคอมพิวเตอร์เครื่องหนึ่งส่งข้อมูล จะส่งไปยังคอมพิวเตอร์เครื่องถัดไปถ้าข้อมูลที่รับมาไม่ตรงตามที่เครื่องคอมพิวเตอร์ ต้นทางระบุ จะส่งผ่านไปยังเครื่องคอมพิวเตอร์เครื่องถัดไปซึ่งจะเป็นขั้นตอนอย่างนี้ไป เรื่อย ๆ จนกว่าจะถึงเครื่องคอมพิวเตอร์ที่อยู่ปลายทางที่ถูกระบุตามที่อยู่จากเครื่องต้นทาง

ข้อดี ส่งข้อมูลไปยังผู้รับหลายเครื่อง ๆ พร้อมกันได้ ไม่เกิดการชนกันของข้อมูล
ข้อเสีย ถ้าเครื่องใดมีปัญหา เครือข่ายล่มการติดตั้งทำได้ยาก และใช้สายสัญญาณมากกว่าแบบบัส

4. **เครือข่ายแบบตาข่าย** (Mesh Network)

โครงสร้างแบบเมชมีการทำงานโดยเครื่องคอมพิวเตอร์แต่ละเครื่องจะต้องมีช่อง ส่งสัญญาณจำนวนมากเพื่อที่จะเชื่อมต่อกับเครื่องคอมพิวเตอร์เครื่องอื่นๆ ทุกเครื่อง โครงสร้างนี้เครื่องคอมพิวเตอร์แต่ละเครื่องจะส่งข้อมูลได้อิสระไม่ต้องรอ การส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์เครื่องอื่นๆ ทำให้การส่งข้อมูลมีความรวดเร็ว แต่ค่าใช้จ่ายสายเคเบิ้ลก็สูงด้วยเช่นกัน

ข้อดี – การสื่อสารข้อมูลเร็ว เพราะคอมพิวเตอร์แต่ละคู่สามารถสื่อสารกันได้โดยไม่ต้องรอ เส้นทางการ

เชื่อมต่อใดๆ ขาด ไม่มีผลต่อการสื่อสารของเครื่องอื่นๆ

ข้อเสีย – สิ้นเปลืองค่าใช้จ่าย จากจำนวนสายสัญญาณและช่องต่อสาย ตามจำนวนเครื่องในระบบ

5. **เครือข่ายแบบผสม** (Hybrid Network)

เป็นเครือข่ายที่ผสมผสานโครงสร้าง เครือข่ายแบบต่าง ๆ เข้าด้วยกันเป็นเครือข่ายขนาดใหญ่เพียงเครือข่ายเดียว เช่น การเชื่อม ต่อเครือข่ายแบบวงแหวน แบบดาว และแบบบัสเข้าเป็นเครือข่ายเดียว

การประยุกต์ใช้

การเชื่อมต่อคอมพิวเตอร์เครือข่ายขนาดเล็ก ที่มีจำนวนเครื่องจำกัด หรืออยู่ในบริเวณไม่กว้าง มักเลือกใช้โทโพโลยีอย่างใดอย่างหนึ่ง ขึ้นกับวัตถุประสงค์ อุปกรณ์ที่มี และสภาพพื้นที่ เช่น การต่อภายในห้อง อาจจะใช้แบบดาว การต่อระหว่างหลายๆ อาคาร อาจเป็นแบบบัส แต่เมื่อมีการขยายขนาดเครือข่ายให้ใหญ่ขึ้น อาจจะเป็นการต่อหลายๆ เครือข่ายเข้าด้วยกัน ลักษณะของโทโพโลยีโดยรวม คือการเชื่อมต่อหลายๆ โทโพโลยีเข้าด้วยกัน

ประเภทเครื่องคอมพิวเตอร์ในเครือข่ายคอมพิวเตอร์

1.**เซิร์ฟเวอร์** เป็นเครื่องคอมพิวเตอร์ที่ทำหน้าที่ให้บริการต่าง ๆ โดยเครือข่ายต่าง ๆ สามารถมีเครื่องเซิร์ฟเวอร์กี่เครื่องก็ได้ตามต้องการ

ชนิดของเครื่องคอมพิวเตอร์เซิร์ฟเวอร์

ไฟล์เซิร์ฟเวอร์ (File Server)

เป็นเซิร์ฟเวอร์ที่ทำหน้าที่ในการจัดเก็บไฟล์ จะเสมือนฮาร์ดดิสก์รวมศูนย์ (Centerized disk storage) เสมือนว่าผู้ใช้งานทุกคนมีที่เก็บข้อมูลอยู่ที่เดียว เพราะควบคุม-บริหารง่าย การสำรองข้อมูลโดยการ Restore ง่าย

พรินต์เซิร์ฟเวอร์ Print Server

หนึ่งเหตุผลที่จะต้องมี Print Server ก็คือ เพื่อแบ่งให้พรินเตอร์ราคาแพงบางรุ่นที่ออกแบบมาใช้สำหรับการทำงานมาก ๆ เช่น HP Laser 5000 พิมพ์ได้ถึง 10 – 24 แผ่นต่อนาที พรินเตอร์สำหรับประเภทนี้ความสามารถในการทำงานที่จะสูง

แอพพลิเคชันเซิร์ฟเวอร์ (Application Server)

Application Server คือ เซิร์ฟเวอร์ที่รันโปรแกรมประยุกต์ได้ โดยการทำงานสอดคล้องกับไคลเอ็นต์ เช่น Mail Server (รัน MS Exchange Server) Proxy Server (รัน Proxy Server) หรือ Web Server (รัน Web

Server Program เช่น Xitami , Apache')

อินเตอร์เน็ตเซิร์ฟเวอร์ (Internet Server)

ปัจจุบันอินเตอร์เน็ตนั้น มีผลกระทบกับเครือข่ายในปัจจุบันเป็นอย่างมาก อินเตอร์เน็ตเป็นเครือข่ายที่มีขนาดใหญ่มากและมีผู้ใช้งานมากที่สุดในโลก เทคโนโลยีที่ทำให้อินเตอร์เน็ตเป็นที่นิยมก็คือ เว็บ และอีเมล เพราะทั้งสองแอพพลิเคชันทำให้ผู้ใช้สามารถแลกเปลี่ยนข้อมูลและสื่อสารกันได้ง่ายและมีรวดเร็ว

เว็บเซิร์ฟเวอร์ (Web Server) คือ เซิร์ฟเวอร์ที่ให้บริการข้อมูลในรูปแบบ HTML (Hyper text Markup Language)

เมลเซิร์ฟเวอร์ (Mail Server) คือ เซิร์ฟเวอร์ที่ให้บริการรับ – ส่ง จัดเก็บ และจัดการเกี่ยวกับอีเมลของผู้ใช้

2. **เวิร์กสเตชั่น** (Workstation) เป็นเครื่องคอมพิวเตอร์ทั่ว ๆ ไปที่สามารถทำการประมวลผลข้อมูลต่าง ๆ ได้
3. **ไคลเอนต์** (Client) เป็นเครื่องคอมพิวเตอร์ที่มีการเรียกใช้ข้อมูลจากเซิร์ฟเวอร์
4. **เทอร์มินัล** (Terminal) เป็นอุปกรณ์ที่ประกอบไปด้วยจอภาพ แป้นพิมพ์ และอื่น ๆ เทอร์มินัลไม่สารถประมวลผลข้อมูลได้ด้วยตัวเองแต่ใช้การสื่อสารข้อมูลกับเซิร์ฟเวอร์เพื่อให้เซิร์ฟเวอร์ประมวลผลพร้อมทั้งแสดงผลที่จอเทอร์มินอล

รูปแบบการประมวลผลข้อมูลในเครือข่ายคอมพิวเตอร์ (Computing Architecture)

การประมวลผลข้อมูลที่ส่วนกลาง (Centrallized Processing)

เป็นการประมวลผลข้อมูลที่เซิร์ฟเวอร์ เครื่องลูกข่ายคอมพิวเตอร์จะเป็นเทอร์มินัลไม่สามารถประมวลผลได้เอง การประมวลผลแบบนี้ เซิร์ฟเวอร์จะต้องเป็นเครื่องที่ประมวลผลได้ เซิร์ฟเวอร์ต้องเป็นเครื่องที่มีความเร็วสูง สามารถประมวลผลข้อมูลได้เป็นจำนวนมาก

การประมวลผลข้อมูลแบบไคลเอนต์/เซิร์ฟเวอร์

เป็นรูปแบบหนึ่งของเครือข่ายแบบ server-based โดยจะมีคอมพิวเตอร์หลักเครื่องหนึ่งเป็นเซิร์ฟเวอร์ ซึ่งจะไม่ได้ทำหน้าที่ประมวลผลทั้งหมดให้เครื่องลูกข่าย หรือไคลเอนต์ (client) เซิร์ฟเวอร์ทำหน้าที่เสมือนเป็นที่เก็บข้อมูลระยะไกล (remote disk) และประมวลผลบางอย่างให้กับไคลเอนต์เท่านั้น เช่น ประมวลผลคำสั่งในการดึงข้อมูลจากเซิร์ฟเวอร์ฐานข้อมูล (database server) เป็นต้น

ชนิดของเครือข่ายคอมพิวเตอร์

เครือข่ายคอมพิวเตอร์ สามารถจำแนกตามระยะทางของการเชื่อมต่อระหว่างการสื่อสารได้เป็น 4

ประเภทดังนี้

1. **แพน (PAN)** หรือเครือข่ายส่วนบุคคล เป็นเครือข่ายสำหรับการแลกเปลี่ยนสารสนเทศและบริการตลอดจนการใช้งานอุปกรณ์ร่วมกัน

2. **ระบบแวน** (wide area networks : WAN) ระบบเครือข่ายบริเวณกว้างที่เชื่อมโยงคอมพิวเตอร์ที่อยู่ห่าง ไกลกันข้ามจังหวัดหรือประเทศ ดังนั้น จึงต้องใช้ระบบสื่อสารโทรคมนาคมที่มีประสิทธิภาพสูงในระดับประเทศ เช่น ขององค์การ โทรศัพท์แห่งประเทศไทย สำหรับตัวกลางอาจเป็นคู่สายโทรศัพท์ธรรมดา สายเช่า วงจรไมโครเวฟ เส้นใยแก้วนำแสง สายเคเบิล แบบโคแอกเชียล หรือใช้ระบบ ดาวเทียมก็ได้ โดยพื้นฐานแล้ว ระบบเครือข่ายบริเวณกว้างเป็นระบบเครือข่ายสื่อสาร ที่สามารถใช้ส่ง สัญญาณ เสียง ภาพ และข้อมูลข้ามอาณาบริเวณไกล ๆ ได้

3.**ระบบแมน** (**20**etropolitan area network : MAN) ระบบเครือข่ายบริเวณมหานครเป็นระบบ ที่เชื่อมโยงคอมพิวเตอร์ซึ่ง อาจตั้งอยู่ห่างไกลกันในช่วง 5 ถึง 50 กิโลเมตร ปกติมักใช้สำหรับสื่อสารข้อมูล เสียง และภาพผ่านสาย โคแอกเชียลหรือเส้นใยแก้วนำแสง ผู้ใช้ระบบแมนมักเป็นบริษัทขนาดใหญ่ที่จำเป็น จะต้องติดต่อสื่อสารข้อมูลผ่าน ระบบ คอมพิวเตอร์ด้วยความเร็วสูงมาก โดยที่การสื่อสารนั้นจำกัดภายในบริเวณเมือง หรือมหานคร

4. **ระบบแลน** (local area networks : LAN) เป็นระบบเครือข่ายเฉพาะบริเวณที่เชื่อมโยง คอมพิวเตอร์ที่ติดตั้งภายในตัวอาคารหลังเดียว หรือที่อยู่ในละแวกเดียวกัน การเชื่อมโยงมักใช้ตัวกลางสื่อสารของตัวเอง เป็นระบบที่เจ้าของ ควบคุมการปฏิบัติงานได้อย่างสมบูรณ์แบบด้วย

ในระบบเครือข่ายทั้งสามระบบนี้ระบบ LAN ได้รับความนิยมใช้กันมากที่สุดทั้งในภาครัฐและเอกชนเพราะเทคโนโลยีระบบ LAN มีราคาไม่สูงมากอีกทั้ง คอมพิวเตอร์ที่ต่อกับระบบเครือข่ายนี้ก็เป็นไมโครคอมพิวเตอร์ ซึ่งมีราคาถูก ละหน่วยงานต่าง ๆ มีใช้อยู่แล้วหลายเครื่อง การลงทุนซื้ออุปกรณ์สำหรับเครือข่าย LAN มาติดตั้งจึงกระทำได้ง่ายที่สำคัญคือระบบ LAN หลายระบบสามารถเชื่อมต่อกับคอมพิวเตอร์ขนาดใหญ่ ทั้งมินิคอมพิวเตอร์และระดับเมนเฟรมได้ แต่แท้ที่จริงแล้วระบบ LAN ก็คือ เครือข่ายขนาดเล็กใช้เชื่อมโยงเครื่องคอมพิวเตอร์ภายในบริเวณสำนักงานที่อยู่อาคารเดียวกันหรือบริเวณเดียวกันเท่านั้น

บทที่ 2
การสื่อสารไร้สายของเครื่อข่ายคอมพิวเตอร์

การเชื่อมต่อระบบเครือข่ายด้วย wireless LAN

เครือข่ายไร้สาย (Wireless Network)

มาทำความรู้จักกับมาตรฐานของ การสื่อสารระบบเครือข่ายไร้สายกัน

คือ มาตรฐาน การส่งผ่านข้อมูลแบบไร้สาย โดยที่มี มาตรฐาน IEEE 802.11 (IEEE คือ Institute of Electrical Electronic Engineers)
ที่ใช้สัญญาณคลื่นความถี่ 2,400 เมกะเฮิรตซ์ รับส่งสัญญาณหรือข้อมูล แบบ DSSS (Direct-Sequence Spread Spectrum)
เป็นการแบ่งส่งข้อมูลส่งไปแต่ละคลื่นความถี่ภายในช่วงระยะเวลาที่สั้นมากตามมาตรฐาน ของระบบแลนไร้สาย ระดับสากล

Retail Wireless Market Standard

ผลิตภัณฑ์ที่มีวางจำหน่ายอยู่ในตลาด ขณะนี้ แบ่งออกตามมาตรฐานเทคโนโลยีที่ใช้เป็นสามกลุ่มหลัก ๆ คือ

IEEE802.11b

เข้าถึงข้อมูลได้ด้วยความเร็วสูงสุด 11 เมกะบิตต่อวินาที (Mbps) / 2.4 GHz

(มีผลิตภัณฑ์บางรุ่นที่ ระบุว่าเป็น IEEE802.11b+ ที่เข้าถึงข้อมูลได้ด้วยความเร็วสูงสุด 22 เมกะบิตต่อวินาที (Mbps) อยู่ด้วย)

IEEE802.11g

เข้าถึงข้อมูลได้ด้วยความเร็วสูงสุด 54 เมกะบิตต่อวินาที (Mbps) / 2.4 GHz

IEEE802.11a

เข้าถึงข้อมูลได้ด้วยความเร็วสูงสุด 54 เมกะบิตต่อวินาที (Mbps) / 5 GHz

โดยที่มีข้อแตกต่างกันดังตารางนี้

Benefits of A vs B vs G

802.11b Wireless-B	802.11a Wireless-A	802.11g Wireless-G
• Lowest price • Excellent signal range • Coverage penetrates most walls • Works with public hotspots	• Supports more users per room • Unaffected by interference from 2.4GHz devices • Can co-exist with B and G networks • Coverage limited To one room	• Best value - only 10% premium for 5 times the speed of Wireless-B • Compatible with Wireless-B networks and hotspots • Excellent signal range • Coverage penetrates most walls

Wireless Product / ผลิตภัณฑ์เครือข่ายไร้สาย

ผลิตภัณฑ์เครือข่ายไร้สายมีหลายชนิดต่าง ๆ

Access Point

เป็นอุปกรณ์กระจายสัญญาณไปยัง อุปกรณ์รับ-ส่งสัญญาณในเครือข่าย โดยที่ตัว Access Point ทำหน้าที่เหมือนกับ Switch

ในระบบเครือข่ายใช้สาย ซึ่งมีผลิตภัณฑ์บางรุ่นที่ ทำหน้าที่เป็น Switch ให้กับระบบเครือข่ายใช้สายปกติ โดยจะมี Port RJ45 รวมอยู่ด้วย 4 - 8 Port นอกจากนี้ยังอาจเพิ่มความสามารถในการเป็น Print Server หรือ Router เข้าไปด้วย

PC Card (PCMCIA)

เป็นอุปกรณ์รับ-ส่งสัญญาณที่ใช้ติดตั้งกับ Notebook เพื่อให้สามารถเชื่อมต่อรับสัญญาณจาก Access Point หรืออุปกรณ์ไร้สายอื่น ๆ
ซึ่งทำหน้าที่เหมือนกับ Lan Card แบบ PCMCIA ทั่วไป

PCI Card

ใช้ติดตั้ง ลงบน PCI-Slot บนเครื่อง PC ลักษณะเดียวกับ NIC-Card (Lan Card) แต่ส่งสัญญาณผ่านเสาอากาศที่ติดตั้งมาด้วย
แทนการส่งสัญญาณผ่านสายทองแดง

USB

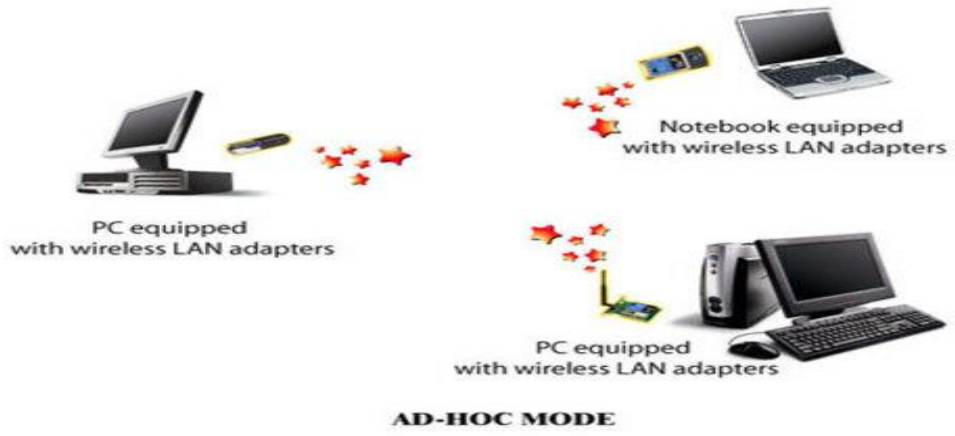
ใช้ติดตั้ง กับพอร์ต USB ทำงานในลักษณะเดียวกับ NIC-Card (Lan Card) แต่ส่งสัญญาณผ่านเสาอากาศที่ติดตั้งมาด้วย
แทนการส่งสัญญาณผ่านสายทองแดง

รูปแบบการติดตั้ง/ออกแบบเครือข่ายไร้สาย

เครือข่ายไร้สายแบ่งการทำงานออกเป็นสองลักษณะ คือ

1. Ad-Hoc Mode (also known as “peer-to-peer” mode)

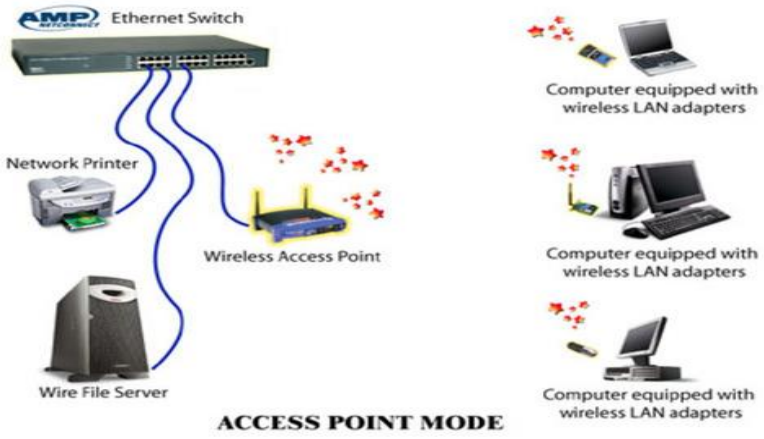
คือการทำงานที่ปราศจาก AccessPoint โดยที่เครื่องคอมพิวเตอร์ ทุกตัว ติดตั้งอุปกรณ์ PC card หรือ PCMCIA ไว้
แล้วส่งสัญญาณหากัน ในลักษณะเดียวกับเครือข่ายสายทองแดง แบบ peer-to-peer



AD-HOC MODE

2. Infrastructure Mode

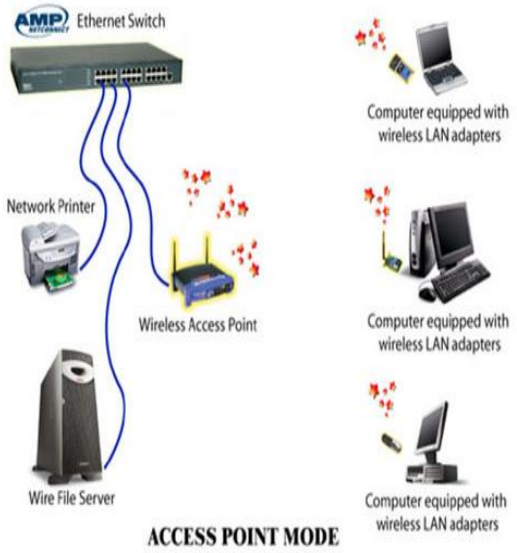
เป็นการทำงานในลักษณะที่ มีการติดตั้ง Access Point เข้าไปในระบบเครือข่ายสายทองแดง เพื่อกระจายสัญญาณไปยัง
เครื่องคอมพิวเตอร์ที่ติดตั้งอุปกรณ์ไร้สายอยู่ การทำงานในลักษณะนี้ เป็นที่นิยมแพร่หลายเนื่องจากสามารถใช้งานร่วมกับระบบสายทองแดง
และยังดัดแปลงใช้งานร่วมกับอุปกรณ์ที่มีอยู่เดิม โดยไม่ต้องติดตั้งอุปกรณ์ไร้สายอื่นเพิ่มเติมมากเกินความจำเป็น



รูปแบบการใช้งาน

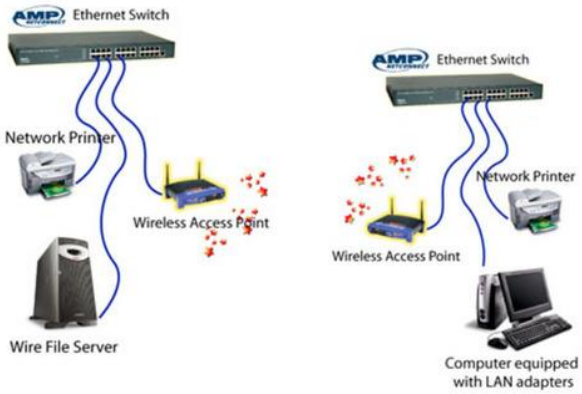
1. Access Point Mode

คือ การใช้งานโดยมี Access Point เชื่อมต่อระหว่าง เครือข่ายไร้สาย กับเครือข่ายสายทองแดง เป็นลักษณะการทำงานที่นิยมใช้กันมากที่สุด



2. Wireless Bridge (Point-to-Point)

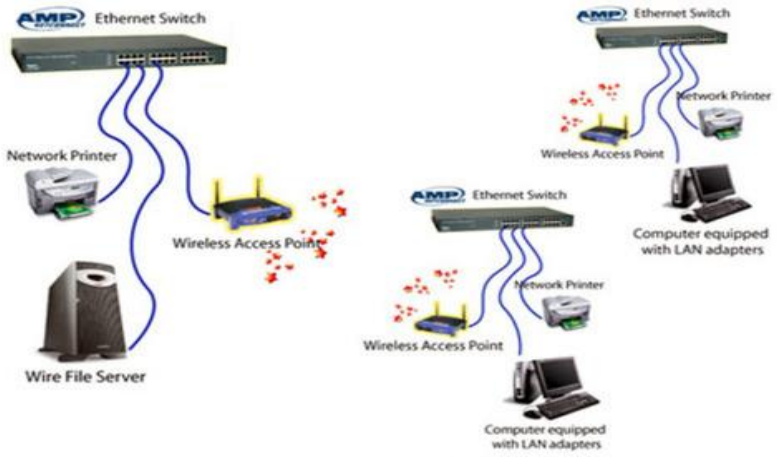
เป็นการทำงานในลักษณะที่ มีการติดตั้ง Access Point เข้าไปในระบบเครือข่ายสายทองแดง เพื่อกระจายสัญญาณไปยัง
เครื่องคอมพิวเตอร์ที่ติดตั้งอุปกรณ์ไร้สายอยู่ การทำงานในลักษณะนี้ เป็นที่นิยมแพร่หลายเนื่องจากสามารถใช้งานร่วมกับระบบสายทองแดง
และยังดัดแปลงใช้งานร่วมกับอุปกรณ์ที่มีอยู่เดิม โดยไม่ต้องติดตั้งอุปกรณ์ไร้สายอื่นเพิ่มเติมมากเกินความจำเป็น



Wireless Bridge (Point-to-Point)

3. Wireles Bridge Point-to-Multipoint

Wireless Access Point ทำงานในลักษณะเดียวกับ แบบ Point-to-Point คือ เชื่อมต่อเครือข่ายสายทองแดงเข้าด้วยกัน
แต่มีการทำงานร่วมกันมากกว่าสองเครือข่าย ดังนั้น Wireless Access Point แต่ละตัว จะมีการรับส่งสัญญาณถึงกันโดยตรง

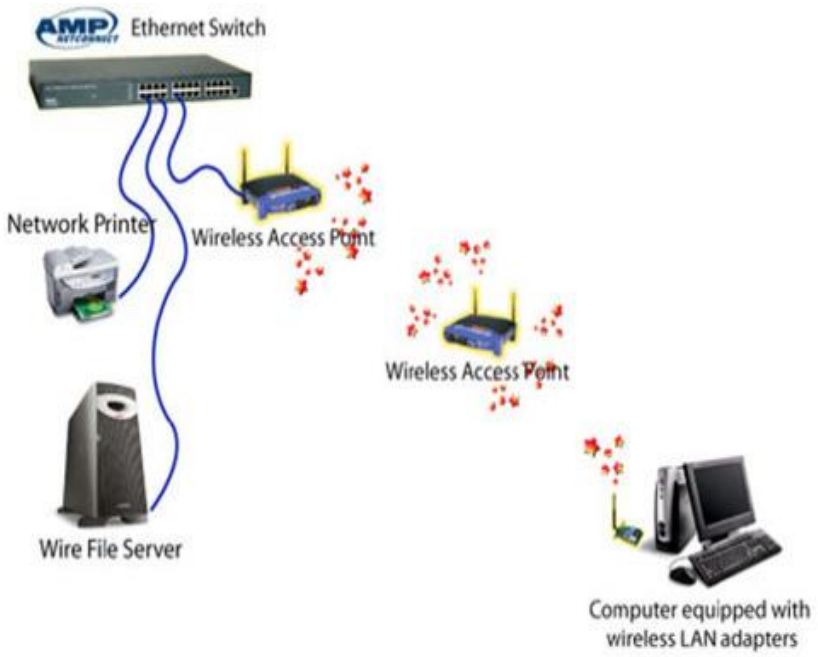


Wireless Bridge Point-to-MultiPoint

4. Repeater Mode

เนื่องจากการทำงานด้วยอุปกรณ์ไร้สาย ปัจจุบัน Wireless Access Point ปกติที่มีขายในท้องตลาด มีรัศมีการส่งสัญญาณ
ภายในอาคารอยู่ที่ 90-120 เมตร และภายนอกอาคาร 300-400 เมตร ถ้าหากมีความต้องการใช้งานที่เกินกว่าข้อจำกัดนี้
จึงจำเป็นต้องมีการเพิ่ม Access Point เข้าไปเพื่อทำการทวนสัญญาณ ให้ได้ระยะทางการส่งข้อมูลที่ไกลกว่าเดิม แต่การทำงานในลักษณะนี้
ทำให้เครือข่ายทั้งสองติดต่อกันด้วยความเร็วไม่แน่นอนและประสิทธิภาพการทำงานลดลง จึงมีการผลิต อุปกรณ์ไร้

สายที่ส่งสัญญาณได้ไกลกว่าปกติขึ้น
หรืออาจมีการติดตั้ง เสาอากาศชนิดพิเศษเข้าไปเพื่อเพิ่มระยะทาง ได้อีกทางเลือกหนึ่ง



Repeater (Doubled Converge Distance)

5. Wireless LAN Client

ในโมเดลการทำงานนี้ เป็นการส่งสัญญาณจากเครือข่ายโดย Wireless Access Point ไปยัง Wireless Access Point
อีกตัวหนึ่งที่ติดตั้งอยู่กับเครื่องคอมพิวเตอร์ เสมือนกับว่า Access Point ตัวนั้น ทำงานเป็น อุปกรณ์ไร้สาย (PCI, PCMCIA, USB)
อาจใช้ในช่วงเริ่มต้น เพื่อขยายจำนวนผู้ใช้งานไร้สาย ในอนาคต

บทที่ 3
การรักษาความปลอดภัย

การรักษาความปลอดภัยในอีกทางหนึ่งไม่เพียงต้องการระบบการป้องกันเท่านั้น แต่ควรพิจารณาปัจจัยภายนอกที่เกี่ยวข้องกับระบบการทำงานด้วย ระบบการป้องกันจะเป็นโมฆะ หากผู้ใช้รับรองความถูกต้อง หรือใช้งานโปรแกรมที่ไม่ได้รับอนุญาต ทรัพยากรคอมพิวเตอร์ต้องได้รับการระมัดระวังการเข้าถึงที่ไม่ได้รับอนุญาต,การทำลาย หรือการเปลี่ยนแปลงที่เป็นอันตราย และความไม่แน่นอนที่นำไปสู่อุบัติเหตุ ทรัพยากรเหล่านี้รวมถึงข้อมูลที่เก็บไว้ในระบบ (ทั้งข้อมูลและรหัส) ตลอดจนซีพียู,หน่วยความจำ,ดิสก์, เทป และเครือข่ายคอมพิวเตอร์ ในบทเรียนนี้ เราจะเริ่มต้นโดยการตรวจสอบวิธีที่อาจจะนำทรัพยากรไปใช้ในทางที่ผิดด้วยความบังเอิญ หรือความตั้งใจ จากนั้นเราจะวินิจฉัยหัวใจสำคัญของความปลอดภัย ที่ทำให้สามารถอ่านรหัสได้ ในที่สุดเราค้นหาวิธีการเพื่อป้องกันหรือตรวจสอบการโจมตี

ปัญหาการรักษาความปลอดภัย

ในหลายแอปพลิเคชัน การตรวจสอบการรักษาความปลอดภัยของระบบคอมพิวเตอร์ที่มีมูลค่าเป็นกอบเป็นกำ ระบบเชิงพาณิชย์ขนาดใหญ่ที่มีบัญชีเงินเดือน หรือข้อมูลทางการเงินอื่นๆที่ดึงดูดใจให้ขโมย ระบบที่มีข้อมูลเกี่ยวข้องกับองค์กร การดำเนินงานอาจจะได้รับผลประโยชน์ ไม่มีหลักการคู่แข่ง นอกจากนี้การสูญเสียข้อมูลดังกล่าว ไม่ว่าจะโดยอุบัติเหตุหรือการฉ้อโกง สามารถทำให้เสียศักยภาพอย่างจริงจังขององค์กรได้

การละเมิดการรักษาความปลอดภัย (หรือการนำไปใช้ในทางที่ผิด) ของระบบสามารถจัดประเภทเป็นโดยตั้งใจ (อันตราย) หรือเป็นเหตุบังเอิญ การป้องกันการนำไปใช้ในทางที่ผิดโดยเหตุบังเอิญทำได้ง่ายกว่าการนำไปใช้ในทางที่ผิดโดยตั้งใจ โดยส่วนใหญ่วิธีการป้องกันจะใช้การป้องกันจากเหตุบังเอิญเป็นหลัก รายการต่อไปนี้ประกอบด้วยรูปแบบของการละเมิดการรักษาความปลอดภัยโดยเหตุบังเอิญและอันตราย เราควรจะบันทึกในการพิจารณาการรักษาความปลอดภัย นอกจากนี้ การคุกคามเป็นการละเมิดการรักษาความปลอดภัยที่มีศักยภาพ เช่น การค้นพบความเสี่ยง ในขณะที่การโจมตีพยายามที่จะหยุดการรักษาความปลอดภัย

•**การละเมิดความลับ** การละเมิดรูปแบบนี้เกี่ยวกับการอ่านข้อมูลโดยไม่ได้รับอนุญาต (หรือโจรกรรมข้อมูล) โดยทั่วไป การละเมิดความลับเป็นเป้าหมายของผู้บุกรุก จับข้อมูลความลับจากระบบหรือเส้นทางการลำเลียงข้อมูล เช่น ข้อมูลเครดิตการ์ด หรือข้อมูลเฉพาะตัวจากการโจรกรรมเฉพาะตัว อาจส่งผลโดยตรงกับเงินจากผู้บุกรุก
•**การละเมิดความซื่อสัตย์** การละเมิดเกี่ยวกับการดัดแปลงข้อมูลโดยไม่ได้รับอนุญาต การโจมตีดังกล่าวมีความสามารถ ตัวอย่างเช่น ผลลัพธ์ที่ผ่านไปเกี่ยวกับความรับผิดชอบของผู้บริสุทธิ์ หรือการเปลี่ยนแปลงรหัสแหล่งที่มาที่สำคัญในการใช้ประโยชน์เชิงพาณิชย์

•**การละเมิดการหามาได้** การละเมิดเกี่ยวกับการทำลายข้อมูล เคร็กเกอร์บางคนจะปล่อยความเสียหาย และสถานภาพที่ได้รับ หรือสิทธิที่พูดโอ้อวดมากกว่าได้รับทางด้านการเงิน เว็บไซต์ถูกทำให้เสียโฉม คือปกติทั่วไปของการละเมิดการรักษาความปลอดภัยประเภทนี้

•**การโจรกรรมการบริการ** การละเมิดเกี่ยวกับการใช้ทรัพยากร ตัวอย่างเช่น ผู้บุกรุก (หรือโปรแกรมการบุกรุก) จะติดตั้งไว้บนระบบจะแสดงที่ไฟล์เซิร์ฟเวอร์

•**การปฏิเสธการบริการ** การละเมิดเกี่ยวกับการป้องกันการใช้อย่างถูกต้องตามกฎหมายของระบบ การปฏิเสธการบริการ หรือ DOS จะโจมตีเหตุบังเอิญในบางครั้ง ไวรัสอินเทอร์เน็ตแบบเก่าจะเปลี่ยนเป็น DOS จะโจมตีบักให้ล้มเหลวล่าช้าและกระจายตัวอย่างรวดเร็ว เราจะพูดถึงการโจมตีของ DOS ให้มากขึ้นในข้อที่ 18.3.3.

นักโจมตีใช้วิธีการหลายมาตรฐานในการพยายามละเมิดความปลอดภัย โดยทั่วไปส่วนมากคือ การปลอมแปลง ซึ่งเป็นหนึ่งที่มีส่วนร่วมในการติดต่อสื่อสารที่อวดอ้างจากผู้อื่น (โฮสต์อื่นหรือบุคคลอื่น) โดยการปลอมแปลง นักโจมตีจะละเมิดการตรวจสอบ, บัตรประจำตัวที่ถูกต้อง; พวกเขาสามารถเข้าใช้งานที่พวกเขาไม่ได้รับอนุญาตตามปกติ หรือเพิ่มสิทธิ-ขอรับสิทธิจากสิ่งใดสิ่งหนึ่งที่พวกเขาได้รับสิทธิแบบผิดปกติ การโจมตีแบบธรรมดาอย่างอื่นคือการถูกเข้ายึดแลกเปลี่ยนข้อมูลใหม่ การรีเพลย์โจมตีประกอบด้วยอันตราย หรือการฉ้อโกงข้อมูลที่ถูกต้องมาถ่ายทอดซ้ำ บางครั้งการรีเพลย์ประกอบด้วยการโจมตีทั้งหมด ตัวอย่างเช่น ในการร้องขอการโอนเงินซ้ำ แต่บ่อยครั้งที่การทำตามข้อความดัดแปลงอีกครั้งเพื่อเพิ่มสิทธิ พิจารณาความเสียหายที่อาจกระทำ หากมีการร้องขอให้มีการตรวจสอบสิทธิ์ของผู้ใช้ข้อมูลที่ถูกต้องตามกฎหมายแทนที่ผู้ใช้ที่ไม่ได้รับอนุญาต กระนั้นประเภทของการโจมตีอย่างอื่น เรียกว่า แมน-อิน-เดอะ-มิดเดิล แอทแทค, ที่ผู้โจมตีเข้าถึงสายข้อมูลของการสื่อสาร, ปลอมแปลงจากผู้ส่งไปยังผู้รับ และในทำนองเดียวกันในเครือข่ายการสื่อสาร แมน-อิน-เดอะ-มิดเดิล แอทแทคอาจจะล่วงจากการถูกปล้น ในการสื่อสารที่ถูกขัดขวาง

ในบางกรณี เช่น การปฏิเสธการบริการโจมตีจะดีกว่าเพื่อการป้องกันการโจมตี แต่การตรวจสอบการโจมตีเพียงพอ เพื่อที่จะตอบโต้มาตรการที่จะสามารถยึดไปได้

เพื่อป้องกันระบบเราจะต้องใช้มาตรการรักษาความปลอดภัย 4 ระดับ

1.กายภาพ เว็บไซต์ หรือเว็บไซต์ที่มีระบบคอมพิวเตอร์ต้องปลอดภัยต่อร่างกาย ต่อต้านการติดอาวุธ หรือปิดบังสิทธิในการเข้าโดยผู้บุกรุก ทั้งห้องเครื่องและขั้วปลายสาย หรือสถานที่ทำงานที่มีการเข้าถึงเครื่องก็จะต้องมีความปลอดภัย

2.มนุษย์ อนุญาตให้ผู้ใช้ต้องดำเนินการอย่างรอบคอบ เพื่อผู้ใช้มั่นใจในการเข้าถึงระบบได้อย่างเหมาะสม แม้แต่ผู้ใช้ที่ได้รับอนุญาต อย่างไรก็ตาม อาจจะ "แนะนำให้" เพื่ออนุญาตให้บุคคลอื่นใช้เข้าถึง (ในการแลกเปลี่ยนสำหรับสินบน จากตัวอย่าง) พวกเขายังอาจจะหลงกลอนุญาตให้เข้าถึงผ่านทางสังคมวิศวกรรม ชนิดหนึ่งของสังคม-สังคมวิศวกรรมโจมตีเป็นการหลอกลวง ณ ที่นี้ ดูอีเมลล์ที่ถูกกฎหมายลทำให้เข้าใจผิดหรือหน้าเว็บที่ผู้ใช้เข้าป้อนข้อมูลที่เป็นความลับ อีกเทคนิค คือ ดัมส์เตอร์ ไดฟ์วิง โดยทั่วไปสำหรับการพยายามที่จะรวบรวมข้อมูลจากคำสั่งที่จะได้รับโดยไม่ได้รับอนุญาตการเข้าถึงคอมพิวเตอร์ (โดยดูผ่านถังขยะ,หนังสือค้นหาเบอร์โทรศัพท์ หรือบันทึกการ

ค้นหาที่มีรหัสผ่าน จากตัวอย่าง) ปัญหาการรักษาความปลอดภัยเหล่านี้เป็นปัญหาการจัดการและบุคลากร ไม่มีปัญหาเกี่ยวกับระบบปฏิบัติการ

3.ระบบปฏิบัติการ ระบบจะต้องป้องกันตัวเองจากเหตุบังเอิญ หรือความตั้งใจละเมิดความปลอดภัย กระบวนการหลบหนีเป็นเหตุบังเอิญการปฏิเสธการบริการโจมตี การค้นหาบริการอาจเปิดเผยรหัสผ่าน การสุมล้นาจทำให้การเริ่มดำเนินการโดยไม่ได้รับอนุญาตของกระบวนการ รายการละเมิดที่เป็นไปได้เกือบจะไม่มีที่สิ้นสุด

4.เครือข่าย ข้อมูลในคอมพิวเตอร์ส่วนใหญ่ระบบเดินทางที่ทันสมัยมากกว่าสายไปรเวต, สายที่ใช้อินเทอร์เน็ตร่วมกัน, การเชื่อมต่อไร้สาย หรือสายแบบเดล-อัพ การขัดขวางข้อมูลเหล่านี้อาจเป็นอันตรายเช่นเดียวกับการทำลายลงในคอมพิวเตอร์; และการขัดขวางการสื่อสารสามารถเป็นการปฏิเสธการบริการโจมตีระยะไกล, จำนวนผู้ใช้น้อยลงและความเชื่อมั่นในระบบ

การรักษาความปลอดภัยที่สองระดับแรกจะต้องรักษา ถ้าปฏิบัติการระบบรักษาความปลอดภัยมั่นใจจุดอ่อนที่ระดับสูงของการรักษาความปลอดภัย (กายภาพหรือมนุษย์) ยอมรับการใช้อุบายกำจัดเข้มงวดระดับต่ำ (ระบบปฏิบัติการ) มาตรการรักษาความปลอดภัย ดังนั้นคำกล่าวโบราณที่เป็นเครื่องผูกมัดเป็นจุดอ่อนเช่นเดียวกับการเชื่อมโยงที่อ่อนที่สุด โดยเฉพาะอย่างยิ่งระบบรักษาความปลอดภัยที่เคร่งครัด ทั้งหมดนี้จะต้องเป็นลักษณะสำหรับการรักษาความปลอดภัยที่จะรักษา

นอกจากนี้ระบบจะต้องให้การป้องกัน (บทที่17) เพื่อให้ดำเนินการคุณสมบัติการรักษาความปลอดภัย โดยสามารถอนุญาตผู้ใช้และการควบคุมการเข้าถึง, เข้าสู่ระบบและกิจกรรมของพวกเขา เป็นไปไม่ได้สำหรับระบบปฏิบัติการในการปรับใช้มาตรการรักษาความปลอดภัยหรือเพื่อรันอย่างปลอดภัย คุณลักษณะการป้องกันมีฮาร์ดแวร์ที่จำเป็นในการสนับสนุนการรวมป้องกันแบบแผน ตัวอย่างเช่น, ระบบการป้องกันแบบมีหน่วยความจำจะไม่มีความปลอดภัย ฮาร์ดแวร์ใหม่มีคุณสมบัติที่ทำให้มีความปลอดภัยมากขึ้น ตามที่เราจะสนทนา

โชคไม่ดีเล็กน้อยที่การรักษาความปลอดภัยคือความซื่อตรง เนื่องจากผู้บุกรุกเอาเปรียบช่องโหว่การรักษาความปลอดภัย การรักษาความปลอดภัย เคาน์เตอร์มีเชอร์ส มีการสร้างและการปรับใช้ ทำให้ผู้บุกรุกมีความซับซ้อนมากขึ้นในการโจมตี ตัวอย่างเช่น ล่าสุดเหตุการณ์การรักษาความปลอดภัยรวมถึงการใช้สปายแวร์ให้สำหรับสแปมบริสุทธิ์ผ่านระบบ (เราจะพูดถึงหลักปฏิบัติในข้อที่18.2) เกมส์แมวและหนูจะดำเนินการต่อด้วยเครื่องมือการรักษาความปลอดภัยเพิ่มเติมที่จำเป็นเพื่อป้องกันเทคนิคการบุกรุกเพิ่มมากขึ้นและกิจกรรม

ในส่วนที่เหลือของบทนี้ เราพูดต่อเกี่ยวกับเครือข่ายการรักษาความปลอดภัยและระดับของระบบปฏิบัติการกายภาพของการรักษาความปลอดภัยและระดับของมนุษย์ แต่ที่สำคัญสำหรับส่วนใหญ่นอกจากขอบเขตของข้อความนี้ การรักษาความปลอดภัยภายในระบบปฏิบัติการ และระหว่างระบบปฏิบัติการดำเนินการได้หลายวิธี จัดระเบียบรหัสผ่านสำหรับการตรวจสอบผ่านการป้องกันต่อต้านไวรัสเพื่อตรวจจับการบุกรุก เราได้เริ่มต้นด้วยการสำรวจภัยคุกคามความปลอดภัย กระบวนการพร้อมกับแก่นแท้เป็นเพียงวิธีการบันทึกการทำงานกับคอมพิวเตอร์ ดังนั้นการเขียนโปรแกรมที่สร้างมีการฝ่าฝืนระบบรักษาความปลอดภัย หรือก่อให้เกิดกระบวนการตามปกติเพื่อเปลี่ยนการทำงานและก่อให้เกิดการฝ่าฝืนกฎหมาย เป็นเป้าหมายของเคร็กเกอร์ ในความเป็นจริงแม้กระทั่งการรักษาความปลอดภัยส่วนใหญ่ไม่ใช่โปรแกรมกิจกรรมที่มีเป้าหมายเป็นสาเหตุการคุกคามโปรแกรม ตัวอย่างเช่น

ในขณะที่เป็นประโยชน์เพื่อเข้าสู่ระบบโดยไม่ได้รับอนุญาต มันเป็นประโยชน์ค่อนข้างมากหลังออกจากเบ็ค-ดอร์เดมอนที่ให้ข้อมูล หรือช่วยให้สะดวกแม้ว่าการเอารัดเอาเปรียบเดิมจะถูกบล็อก ในหัวข้อนี้เราอธิบายถึงวิธีทั่วไปที่โปรแกรมทำให้เกิดการละเมิดความปลอดภัย โปรดทราบว่ามีการพิจารณารูปแบบในการตั้งชื่อการรักษาความปลอดภัย ที่เราใช้ส่วนใหญ่หรือคำอธิบาย

ม้าโทรจัน

หลายระบบมีวิธีการเพื่อให้โปรแกรมที่เขียนโดยผู้ใช้ที่ดำเนินการโดยผู้ใช้อื่น หากโปรแกรมเหล่านี้ดำเนินการในขอบเขตที่มีสิทธิ์การเข้าถึงของผู้ใช้ดำเนินการ ผู้ใช้อื่นอาจนำสิทธิไปใช้ในทางที่ผิด ข้อความ-แก้ไขโปรแกรมตัวอย่างเช่น อาจรวมถึงรหัสเพื่อค้นหาแฟ้มที่ได้รับการแก้ไขบางคำหลัก และผู้ใดถูกพบ แฟ้มข้อมูลทั้งหมดอาจถูกคัดลอกไปยังพื้นที่พิเศษที่สามารถเข้าถึงได้โดยผู้ออกแบบโปรแกรมแก้ไขข้อความ ส่วนหลักเกณฑ์ที่การนำไปใช้ในทางที่ผิดสภาพแวดล้อมของหลักเกณฑ์เรียกว่า ม้าโทรจัน การค้นหาที่ยาวนาน เช่น ระบบยูนิกซ์ทั่วไป ปัญหาม้าโทรจันทำให้รุนแรง การค้นหารายการชุดของไดเรกทอรีจะได้รับเมื่อค้นหาชื่อโปรแกรมที่คลุมเครือ เส้นทางคือค้นหาจากชื่อแฟ้มข้อมูล และข้อมูลที่ดำเนินการ ไดเรกทอรีทั้งหมดในการค้นหาเส้นทางดังกล่าวจะต้องมีความปลอดภัย หรือม้าโทรจันอาจลักลอบเข้าเส้นทางของผู้ใช้และดำเนินการโดยบังเอิญ

เป็นต้นว่าพิจารณาการใช้ "." อักขระในค้นหาเส้นทาง "." แจ้งที่เชลล์เพื่อรวมไดเรกทอรีปัจจุบันในการค้นหา ดังนั้นหากผู้ใช้ "." ในการค้นหาเส้นทางของเธอ ปัจจุบันเธอได้กำหนดไดเรกทอรีให้ไดเรกทอรีของเพื่อนและป้อนชื่อของปกติระบบคำสั่ง คำสั่งอาจจะดำเนินการจากไดเรกทอรีของเพื่อนแทน โปรแกรมจะทำงานภายในขอบเขตของผู้ใช้ อนุญาตให้โปรแกรมทำอะไรก็ตามที่ผู้ใช้สามารถทำ รวมทั้งการลบแฟ้มข้อมูลของผู้ใช้ด้วย เป็นต้น

รูปแบบที่หลากหลายของม้าโทรจันเป็นโปรแกรมที่มีการเลียนแบบการเข้าสู่ระบบโปรแกรม ไม่สงสัยเลยที่ผู้ใช้เริ่มต้นเข้าสู่ระบบที่ปลายทาง และประกาศที่เขาไม่ปรากฏชนิดรหัสผ่าน เขาพยายามอีกครั้งและประสบความสำเร็จ เกิดอะไรขึ้นการตรวจสอบความถูกต้องของหัวใจสำคัญ และรหัสผ่านที่ถูกขโมยโดยการเข้าสู่ระบบของผู้ลอกเลียนแบบ ซึ่งออกจากการทำงานบนปลายทางโดยการขโมย ผู้ลอกเลียนแบบจัดเก็บรหัสผ่านให้ห่างจากตัว พิมพ์ข้อความการเข้าสู่ระบบที่ผิดพลาดออกมา และออก ผู้ใช้มีการเข้าสู่ระบบพรอมต์ของแท้ การโจมตีประเภทนี้สามารถจำกัดโดยมีระบบปฏิบัติการที่มีการใช้งานพิมพ์ข้อความที่ท้ายของชุดการโต้ตอบ หรือโดยลำดับหัวใจสำคัญที่ไม่ใช่สิ่งล่อลวง เช่นคอนโทรล-อัลติเน็ต-ดีลีดชุดค่าผสมทั้งหมดที่ใช้งานโดยระบบปฏิบัติการที่วินโดว์สที่ทันสมัย

อีกรูปแบบในม้าโทรจันคือสปายแวร์ สปายแวร์บางครั้งมากับโปรแกรมที่ผู้ใช้เลือกที่จะติดตั้ง บ่อยที่สุดมาพร้อมกับโปรแกรมฟรีแวร์หรือแชร์แวร์ แต่บางครั้งจะรวมอยู่กับซอฟต์แวร์เชิงพาณิชย์ เป้าหมายของสปายแวร์คือการดาวน์โหลดที่จะแสดงบนระบบของผู้ใช้ สร้างป๊อปอัพเบราว์เซอร์วินโดว์ส เมื่อมีการเข้าชมบางเว็บไซต์ หรือเข้ายึดข้อมูลจากระบบของผู้ใช้และส่งข้อมูลกลับไปยังศูนย์กลางเว็บไซต์ โหมดหลังนี้เป็นตัวอย่างทั่วไปของการโจมตีประเภทที่เรียกว่าช่องแอบแฝง ที่เกิดการซ่อนเร้นการสื่อสารขึ้น ในปัจจุบัน เช่น การติดตั้งที่ไม่มีอันตรายตามที่ปรากฏโปรแกรมในระบบวินโดว์สได้ผลในการโหลดของสปายแวร์ผี สปายแวร์ที่สามารถติดต่อ

ศูนย์กลางเว็บไซต์ จะได้รับข้อความและรายการที่อยู่ผู้รับ และส่งข้อความสแปมแก่บรรดาผู้ใช้จากเครื่องวินโดว์ส กระบวนการนี้ทำงานต่อเนื่องจนกว่าผู้ใช้จะพบสปายแวร์ หลายครั้งที่ไม่พบสปายแวร์ ในปีคริสตศักราช 2004 ประมาณ 80 เปอร์เซ็นต์ของสแปมเป็นการจัดส่งด้วยวิธีการนี้ การขโมยการบริการนี้ไม่ได้แม้แต่ถือว่าเป็นอาชญากรรมในประเทศส่วนใหญ่

สปายแวร์เป็นไมโครตัวอย่างของแมโครปัญหา การละเมิดหลักการของสิทธิ์น้อยที่สุด ภายใต้สถานการณ์ส่วนใหญ่ผู้ใช้ของระบบปฏิบัติการไม่จำเป็นต้องติดตั้งเครือข่ายผี นั่นเครือข่ายผีมีการติดตั้งผ่านทางสองข้อผิดพลาดอันดับแรก,ผู้ใช้อาจดำเนินการเพิ่มเติมสิทธิ์เกินจำเป็น (เช่นเป็นผู้ดูแลระบบ) โปรแกรมที่ช่วยให้เธอดำเนินการมีหลายวิธีการที่เข้าถึงระบบมากกว่าสิ่งที่จำเป็น นี่เป็นกรณีของมนุษย์ที่มีข้อผิดพลาดทั่วไปของความปลอดภัยที่อ่อนแอ อันดับที่สอง,ระบบปฏิบัติการอาจเพิ่มเติมโดยค่าเริ่มต้นมากกว่าสิทธิ์ทั่วไปที่ผู้ใช้ต้องการ นี่เป็นกรณีการออกแบบตัดสินใจระบบปฏิบัติการที่ไม่ดี ระบบปฏิบัติการ(และแน่นอนซอฟต์แวร์ทั่วไป)ควรอนุญาตให้ปรับการควบคุมการเข้าถึงให้เล็กลงและการรักษาความปลอดภัย แต่ต้องมีความสะดวกในการจัดการและความเข้าใจมาตรการการรักษาความปลอดภัยที่ไม่สะดวก หรือไม่เพียงพอมีความเกี่ยวพันกับการใช้อุบายในการกำจัด สาเหตุที่ทำให้การรักษาความปลอดภัยโดยรวมอ่อนลงพวกเขาถูกออกแบบมาเพื่อใช้สอย

หน่วยความจำ หรือ ที่พักข้อมูลล้น

หน่วยความจำ หรือ ที่พักข้อมูลล้น เป็นวิธีการโจมตีทั่วไปสำหรับผู้โจมตีจากภายนอกระบบ ในเครือข่ายหรือการเชื่อมต่อเพื่อเข้าถึงระบบเป้าหมายโดยไม่ได้รับอนุญาต หรือเพิ่มสิทธิ์ของผู้ใช้ที่ได้รับอนุญาตแล้ว

เป็นหลักการโจมตีที่หาประโยชน์จากข้อบกพร่องในโปรแกรม บั๊กเกิดขึ้นได้ง่ายจากโปรแกรมที่แย่ ที่โปรแกรมเมอร์ละเลยการตรวจสอบขอบเขตของอินพุตฟิลด์ ในกรณีนี้การโจมตีจะส่งข้อมูลมากกว่าที่โปรแกรมคาดไว้ การแก้ไขใช้การแกะรอยและข้อผิดพลาด หรือด้วยการตรวจสอบซอร์สโค้ดที่โจมตีโปรแกรมในกรณีที่มี การกำหนดความเสี่ยงของการโจมตีและเขียนโปรแกรมเพื่อดำเนินการต่อไปนี้

1. การล้นของอินพุตฟิลด์, คอมมาน-ไลน์ หรือ ที่พักข้อมูลอินพุต ตัวอย่างเช่นในเครือข่ายภูตจนถึงการเขียนลง stack
2. การเขียนทับข้อมูลปัจจุบันลงใน stack กับข้อมูลที่เป็นประโยชน์ต่อการโหลดรหัสในขั้นที่ 3
3. การเขียนชุดโค้ดอย่างง่ายสำหรับช่องว่างถัดไปใน stack ซึ่งการโจมตีต้องการที่จะเข้าถึง ตัวอย่างเช่นไข่ที่มีเปลือก

ผลของโจมตีนี้ การทำงานของโปรแกรมจะทำให้รากเซลล์อื่น ๆ มีสิทธิพิเศษในคำสั่งหรือการกระทำ

Viruses

สายการทำงานของโปรแกรมถูกเรียกอีกอย่างหนึ่งคือ ไวรัส ไวรัสมีการจำลองตัวเองและมีการออกแบบให้ไปฝังตัวกับโปรแกรมอื่นๆได้ พวกมันสามารถทำให้เกิดความเสียหายแก่ระบบได้โดยการปรับแต่งหรือทำลายไฟล์และเป็นสาเหตุที่ทำให้เกิดการแคชและโปรแกรมไม่สามารถทำงานได้ตามปกติได้ ไวรัสเป็นหนึ่งของโค้ดที่นำไปติดไว้กับโปรแกรม โดยส่วนใหญ่การโจมตี ไวรัสจะมีปัญหาสำหรับผู้ใช้คอมพิวเตอร์ส่วนบุคคล ยูนิกซ์และระบบปฏิบัติการอื่นๆจะไม่ค่อยมีการติดไวรัสเพราะโปรแกรมได้มีการป้องกันการเขียนจากระบบปฏิบัติการเอง ถ้าเกิดว่าไวรัสได้ติดกับโปรแกรมแล้วมันจะมีความสามารถจำกัดเพราะ ระบบที่มีการคาดการณ์ไว้แล้วจะมีการป้องกัน

ไวรัสโดยส่วนใหญ่จะเกิดมาจากอีเมล์ สแปมเป็นส่วนมากแล้ว มันจะทำการกระจายตัวไปตามผู้ที่มาโหลดโปรแกรมนั้นจากอินเตอร์เน็ต โดยบริการไฟล์แชร์ริ่ง

อีกทางหนึ่งที่ไวรัสจะมาจากการขนส่งคือการใช้ ไมโครซอฟต์ออฟฟิตไฟล์และเอกสานไมโครซอฟต์เวิร์ด เอกสารพวกนี้จะมีส่วนใหญ่หลักคือมาโครซึ่งเป็นโปรแกรมมาจากออฟฟิตสูทมันจะมีการทำงานอย่างอัตโนมัติ เพราะโปแกรมมันจะทำงานภายใต้บัญชีผู้ใช้อื่น มาโครสามารถรันงานใหญ่ ๆ ได้ โดยไม่ต้องมีเงื่อนไข เช่นสามารถลบไฟล์ผู้ใช้ได้ ทั่วๆไปแล้วไวรัสจะมีการติดกับอีเมล์ตนเองหรือติดกับผู้ใช้ที่มีการติดต่อสื่อสารกัน โดยต่อไปนี้จะแสดงโค้ดตัวอย่างของการเขียน มาโครซึ่งไวรัสสามารถใช้รูปแบบนี้ในการลบฮาร์ดดิสก์ของวินโดวส์คอมพิวเตอร์ได้ และไฟล์มาโครก็จะถูกเปิดออกมา

ไวรัสจะทำงานได้อย่างไร เมื่อไวรัสไปถึงยังเครื่องเป้าหมายโปรแกรมจะรู้ว่าไวรัสได้ตกลงมาแล้วไวรัสจะถูกนำเข้าไปในระบบ ไวรัสที่ตกลงมาโดยทั่วไปคือ ม้าโทรจัน การทำงานสำหรับการที่มันจะติดตั้งตัวเองลงไปยัง

แกนกลางของกิจกรรม เมื่อการติดตั้งเสร็จสิ้น ไวรัสอาจจะมีจำนวนมากมายที่เราไม่สามารถคิดเอาไว้ได้ ไวรัสพัน ๆ ตัว ได้มีการจัดแบ่งประเภทไว้หลายกลุ่ม บางทีไวรัสหนึ่งตัวอาจจะจัดได้มากกว่าหนึ่งกลุ่ม

File มาตรฐานไฟล์ไวรัสในระบบจะกำหนดโดยตัวมันเอง มันสามารถเปลี่ยนแปลงการเริ่มต้นของโปรแกรม ดังนั้นการทำงานจะกระโดดไปยังโค้ดที่ต้องการ หลังจากทำงานแล้ว มันจะคืนค่าควบคุมไปยังโปรแกรมดังนั้นการทำงานจะไม่เป็นที่สังเกตไฟล์ไวรัส บางตัวจะรู้ว่าเป็นคล้ายพยาธิ ที่จะออกจากจากสิ่งที่ไม่มีไฟล์แล้วและออกจากโปรแกรมที่ไมสามารถทำงานได้อีก

Boot ไวรัสที่เกิดจากการบูทเซกเตอร์ในระบบ มันจะทำงานทุกๆเวลาที่ระบบมีการบูทและก่อนที่ระบบปฏิบัติการจะมีการโหลดขึ้นมา มันสามารถดูว่าสื่อไหนสามารถบูทได้เช่น แผ่นดิสเกต และไวรัสก็สามารถบูทได้ทางนี้เช่นกัน ไวรัสมันจะรู้ว่ามีหน่วยความจำของไวรัสเพราะมันจะไม่ปรากฏในระบบไฟล์

Encrypted การเข้ารหัสไวรัสจะรวมถึงการถอดรหัสด้วย ไวรัสที่ถูกเข้ารหัสจะสามารถรอดจากการตรวจจับได้ โดยอย่างแรกไวรัสจะทำการถอดรหัสตัวมันเองและจะทำงานต่อไป

Stealth ไวรัสชนิดนี้จะพยายามไม่ให้ตรวจจับได้โดยการปรับแต่งส่วนของระบบโดยทำให้ไม่สามารถตรวจจับได้ ตัวอย่างเช่น มันสามารถปรับแต่งการอ่าน system callได้ดังนั้น ถ้าไฟล์ที่ถูกปรับแต่งถูกอ่านขึ้น รูปแบบเดิมของโค้ดจะถูกส่งค่ากลับไปและสุดท้ายก็จะเป็นไวรัสโค้ด

Tunneling ไวรัสชนิดนี้จะพยายาม หาทางลัดไม่ให้ตรวจจับไดโดยแอนตี้ไวรัสสแกนเนอร์โดยการติดตั้งตัวมันเองลงใน interrupt-handler chain ทั่วไปแล้วไวรัสมักจะติดตั้งตัวมันเองไปกับอุปกรณ์ไดเวอร์

Multipartite ไวรัสชนิดนี้เป็นประเภทที่สามารถติดไปกับส่วนหนึ่งของระบบซึ่งรวมถึงบูทเซกเตอร์ หน่วยความจำและไฟล์เป็นสิ่งที่ยากในการตรวจสอบสิ่งที่เก็บไว้ในนั้น

Armored ไวรัสอาร์เมอร์คือ สร้างโค้ดด้วยตัวมันเองซึ่งยากสำหรับนักวิจัยไวรัสหาทางแก้ไขได้และทำความเข้าใจ มันสารถบีบตัวเองเพื่อให้รอดจากการตรวจสอบและไม่ติดเชื้อ ส่วนเพิ่มเติม ไวรัสที่ตกลงมากับไฟล์ที่เต็มเปี่ยม มันจะมีส่วนหนึ่งของไวรัสที่ไม่ดีจำนวนมากที่ซ่อนอยู่ในไฟล์คุณลักษณะหรือไฟล์ที่ไม่ทราบชื่อ

นี้ก็เป็นส่วนหนึ่งของไวรัสซึ่งมีแนวโน้มที่จะมากขึ้นเรื่อยๆ ในความจริงปี 2004 ได้พบกระจายอย่างกว้างขว้างและก็ถูกตรวจจับได้ มีการกระจายตัวของแมงสำหรับระบบปฏิบัติการ ไวรัสจะเริ่มโดยการติดเชื่อนับร้อยของวินโดวส์เซิร์ฟเวอร์ การทำงานของไมโครซอฟต์อินเตอร์เน็ต การใช้งานอินเตอร์เน็ตบราวเซอร์ที่ไปเยี่ยมชมเว็บที่มีการติดไวรัสหรือการดาวโหลดต่าง ๆ ที่มีการติดไวรัส ไวรัสบราวเซอร์จะทำการติดตั้งตัวมันเองลงประตูหลังของโปรแกรมพร้อมทั้งรวม keystroke logger กับทุก ๆ สิ่งที่มาทางคีย์บรอดซึ่งรวมถึงรหัสลับ รหัสเครดิตการ์ด มันจะมีการจำลองที่ยอมรับการเข้าถึงทางรีโมทได้อย่างไม่จำกัดทางผู้ที่สร้างมันขึ้นมาหรือยอมให้คนอื่น ๆสามารถเข้ามาใช้การได้กับเครื่องคอมพิวเตอร์ที่ติดไวรัส

ทั่ว ๆ ไปแล้วไวรัสส่วนใหญ่จะโจมตีระบบป้องกันให้แตกแยก เพราะมันจะส่งผลในการทำงานอย่างต่อเนื่องในการเขียนและกระจาย เมื่อมีกิจกรรมการล่อล่วงเกิดขึ้นจากการคำนวณโดยคอมพิวเตอร์เกิดขึ้นใน

หลายๆระบบที่ทำงานในระบบฮาร์ดแวร์เดียวกัน ระบบปฏิบัติการณ์เดียวกัน และแอบพลิเคชันซอฟแวร์เดียวกัน มันจะเพิ่มการกระจายและผลกระทบถึงระบบป้องกันอย่างมาก

ระบบภัยคุกคาม

ระบบปฏิบัติการโดยส่วนใหญ่ให้หมายความว่ากระบวนการเพื่อวางไข่อื่นๆกระบวนการ.
ในดังกล่าวมีสภาพแวดล้อมที่เป็นไปได้ที่จะสร้างสถานการณ์ที่ ปฏิบัติการ-ทรัพยากรระบบและผู้ใช้แฟ้ม misused. ทั้งสองส่วนใหญ่ วิธีการนี้ achieving ด่าว่ามีไวรัสและเวิร์ม

หนอน

มีหนอนเป็นกระบวนการที่ใช้วางไข่กลไกเพื่อข่มขี่ประสิทธิภาพระบบ. ที่หนอน spawns สำเนาเองขึ้นใช้ทรัพยากรระบบและ บางทีล็อกออกจากระบบอื่นๆทั้งหมดโดยใช้กระบวนการ. คอมพิวเตอร์ในเครือข่าย เวิร์มมีเฉพาะชะงัดเนื่องจากอาจทำซ้ำในหมู่พวกเขาเอง ระบบจึงปิดการ entirer network. เมื่อในสถานที่หลักที่หนอน undertook ระบบพยายามค้นพบ รหัสผ่านผู้ใช้ มันเริ่มโดยพยายามง่ายๆกรณีที่ไม่มีรหัสผ่านหรือรหัสผ่าน การสร้างบัญชีผู้ใช้ชื่อชุดแล้วใช้เปรียบเทียบ กับพจนานุกรมภายในของ 432 รหัสผ่านโปรดเลือกจากนั้นไปที่ ขั้นตอนสุดท้ายของพยายามแต่ละคำในมาตรฐานยูนิกซ์ในบรรทัดพจนานุกรม เป็น รหัสผ่านเป็นไปได้และมีประสิทธิภาพสามขั้นรหัสผ่านกรอบ กลไกเปิดได้รับเพิ่มเติมเข้าสู่บัญชีผู้ใช้อื่นๆที่ ระบบที่ติดไวรัส ที่หนอนแล้วค้นหาแฟ้มข้อมูลใน rsh เหล่านี้ใหม่ เสียบัญชี. Rsh รายการใดๆที่ถูกทดสอบและตามที่ได้อธิบายไว้ก่อนหน้านี้ที่ แล้วหนอนสามารถเข้าสู่บัญชีผู้ใช้ในระบบระยะไกล ด้วยการเข้าถึงแต่ละใหม่ที่หนอนโปรแกรมค้นหาใช้งานแล้ว สำเนาตัวเอง. หากพบหนึ่งใหม่ที่คัดลอกออกยกเว้นทุกเจ็ด ตัวอย่าง. มีหนอนออกซ้ำในทุก sightings มันอาจมีอยู่ไม่ยอมให้ทุกเจ็ดซ้ำเพื่อดำเนินการ (อาจจะเป็น เอาไปปนกันเพื่อความพยายามหยุดการแพร่กระจายโดย baiting ด้วย เวิร์ม) สร้างขายส่งรังควาญของ Sun และ VAX ระบบในอินเทอร์เน็ต.

Firewall เพื่อปกป้องระบบและเครือข่าย

จากคำถามของวิธีการที่เชื่อถือได้ที่สามารถเชื่อมต่อคอมพิวเตอร์อย่างปลอดภัยไปยังเครือข่ายไว้ใจไม่ได้. วิธีการแก้ปัญหาหนึ่งคือการใช้ไฟร์วอลล์เพื่อแยกว่าระบบ น่าเชื่อถือ และไม่น่าเชื่อถือ ไฟร์วอลล์เป็นคอมพิวเตอร์โปรแกรมหรือเราเตอร์ที่ แยกระหว่างเชื่อถือและ ไม่น่าเชื่อถือ. เครือข่ายไฟร์วอลล์ จำกัดการเข้าถึงเครือข่ายระหว่างสองความปลอดภัยโดเมนและจอภาพและบันทึกการเชื่อมต่อทั้งหมด. มันยังสามารถจำกัดการเชื่อมต่อจากแหล่งที่มาหรือปลายทางที่อยู่หรือแหล่งปลายทางพอร์ตหรือทิศทางของการเชื่อมต่อ. ตัวอย่างเช่น เว็บเซิร์ฟเวอร์ใช้ HTTP ในการสื่อสารกับเว็บเบราเซอร์. ไฟร์วอลล์จึงอาจอนุญาต HTTP เท่านั้นที่จะผ่าน host ทั้งหมด นอกไฟร์วอลล์ไปที่เว็บเซิร์ฟเวอร์ภายในไฟร์วอลล์. ที่ Morris Internet worm ใช้ fingerโปรโตคอลที่จะผ่านเข้าไปในคอมพิวเตอร์ดังนั้น fingerโปรโตคอลจะไม่อนุญาตให้ผ่านเช่น. ในความเป็นจริง, เครือข่ายไฟร์วอลล์ที่สามารถเข้ามาในเครือข่ายที่แยกจากกันหลายโดเมน. ดำเนินการทั่วไปมีอินเทอร์เน็ตเป็นโดเมนที่ไม่น่าเชื่อถือ มีกึ่งเชื่อถือและกึ่งปลอดภัยเครือข่ายเรียก เขตปลอดทหาร (DMZ), เป็นโดเมนอื่นและบริษัทของ

คอมพิวเตอร์เป็นสามโดเมน สามารถเชื่อมต่อจากอินเทอร์เน็ตเพื่อ DMZ คอมพิวเตอร์และจากบริษัทคอมพิวเตอร์ไปยังอินเทอร์เน็ตแต่ไม่อนุญาตให้มีการติดต่อจากอินเทอร์เน็ตหรือ DMZ คอมพิวเตอร์บริษัทคอมพิวเตอร์. ทางเลือกคือควบคุมการสื่อสารอาจอนุญาตระหว่าง DMZ และบริษัทหนึ่งหรือมากกว่าคอมพิวเตอร์. ตัวอย่างเช่น เว็บเซิร์ฟเวอร์ใน DMZ อาจต้องสืบค้นฐานข้อมูลเซิร์ฟเวอร์ในเครือข่ายขององค์กรด้วยไฟร์วอลล์อย่างไรก็ตามการเข้าถึง DMZ ระบบที่เสียหายยังคงไม่สามารถเข้าถึงหน่วยงาน แน่นอนไฟร์วอลล์เองจะต้องมีความปลอดภัยและโจมตี-หลักฐาน มีความสามารถในการรักษาความปลอดภัยการเชื่อมต่อสามารถอะลุ้มอล่วย นอกจากนี้ไฟร์วอลล์ไม่ได้ป้องกันการโจมตีที่อุโมงค์หรือเดินทางภายในโปรโตคอลหรือการเชื่อมต่อที่ไฟร์วอลล์ช่วยให้เป็นบัฟเฟอร์-ล้นโจมตีไปยังเว็บเซิร์ฟเวอร์จะไม่หยุดโดย ไฟร์วอลล์ เช่นเนื่องจาก HTTP ในการเชื่อมต่อที่อนุญาตให้ เป็นเนื้อหาของ HTTP ในการเชื่อมต่อที่อยู่ที่โจมตี. เช่นเดียวกับการปฏิเสธของเนื้อหาของบริการอาจส่งผลกระทบต่อการโจมตีไฟร์วอลล์ที่เครื่องอื่นๆ อีกหนึ่งความเสี่ยงของไฟร์วอลล์คือหลอกลวงซึ่งในที่ไม่ได้รับอนุญาตโฮสต์หลอกลวง ก้ออนุญาตเป็นโฮสต์โดยประชุมบางอนุมัติเกณฑ์. ตัวอย่างเช่นหากกฎไฟร์วอลล์ช่วยให้การเชื่อมต่อจากโฮสต์และระบุว่าโฮสต์โดยที่อยู่ IP จากนั้นอื่นโฮสต์สามารถส่งแพ็คเก็ตที่ใช้ที่อยู่เดียวกันและสามารถผ่านไฟร์วอลล์. นอกเหนือจากส่วนใหญ่ไฟร์วอลล์เครือข่ายมีอื่นๆใหม่กว่าชนิดไฟร์วอลล์แต่ละด้วย pros และ cons. ส่วนตัวไฟร์วอลล์คือซอฟต์แวร์เลเยอร์ใดรวมอยู่กับระบบปฏิบัติการหรือเพิ่มเป็นแอปพลิเคชัน. แทนที่จะจำกัดการสื่อสารระหว่างความปลอดภัยโดเมนมันวงเงินเพื่อการสื่อสาร (และอาจจาก) ที่ระบุโฮสต์. ผู้ใช้สามารถเพิ่มไฟร์วอลล์ส่วนบุคคลเพื่อที่เธอพีซีเพื่อที่ Trojan ม้าจะถูกปฏิเสธการเข้าถึงไปยังเครือข่ายที่มีการเชื่อมต่อพีซี. แอปพลิเคชันมอบฉันทะไฟร์วอลล์เข้าใจโปรโตคอลที่ใช้งานพูดข้ามเครือข่าย ตัวอย่างเช่น SMTP ใช้สำหรับจดหมายโอน แอปพลิเคชันมอบฉันทะเพียงยอมรับการเชื่อมต่อเป็นเซิร์ฟเวอร์ SMTP จะและจะเริ่มต้นการเชื่อมต่อกับปลายทางเดิมเซิร์ฟเวอร์ SMTP. สามารถติดตามการเข้าชมตามที่ล้ำหน้าข้อความการดูและการปิดใช้งานที่ผิดกฎหมายคำสั่งพยายามเอาเปรียบโรคจิต, เป็นต้น ไฟร์วอลล์บางคนได้รับการออกแบบเฉพาะสำหรับหนึ่งโปรโตคอล XML ที่ไฟร์วอลล์เช่นมีเฉพาะวัตถุประสงค์ของการเข้าชมและวิเคราะห์ XML ที่ไม่สามารถบล็อคหรือ XML ที่ไม่ถูกต้อง ระบบโทรติดต่อไฟร์วอลล์นั่งระหว่างโปรแกรมประยุกต์และ เคอร์เนลการติดตาม system call ตัวอย่างเช่นใน Solaris 10, ที่ "อย่างสิทธิ์" คุณสมบัติ วิธีการทำรายการกว่าห้าสิบระบบสายกระบวนการที่อาจจะหรืออาจจะไม่ได้รับอนุญาตให้ทำการ. กระบวนการที่ไม่จำเป็นต้องวางไข่อื่นๆสามารถมีกระบวนการที่สามารถนำห่างตัวอย่าง.

<u>การรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ของกรมสนับสนุนบริการสุขภาพ</u>

<u>(Network and Server Policy)</u>

ข้อ ๑ กรมสนับสนุน กำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

ข้อ ๒ ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากกรมสนับสนุน และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

ข้อ ๓ การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อกรมสนับสนุน และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้บริการอื่นๆ

ข้อ ๔ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

ข้อ ๕ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(๑) ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๒) ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๓) ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

(๕) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

(๖) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

(๗) เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

(๘) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๙) การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ (System Administrator) และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ข้อ ๖ ผู้ดูแลระบบ (System Administrator) ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ ๗ กรมสนับสนุน กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

(๑) ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

(๒) ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

(๓) ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

(๔) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ข้อ ๘ กรมสนับสนุน กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

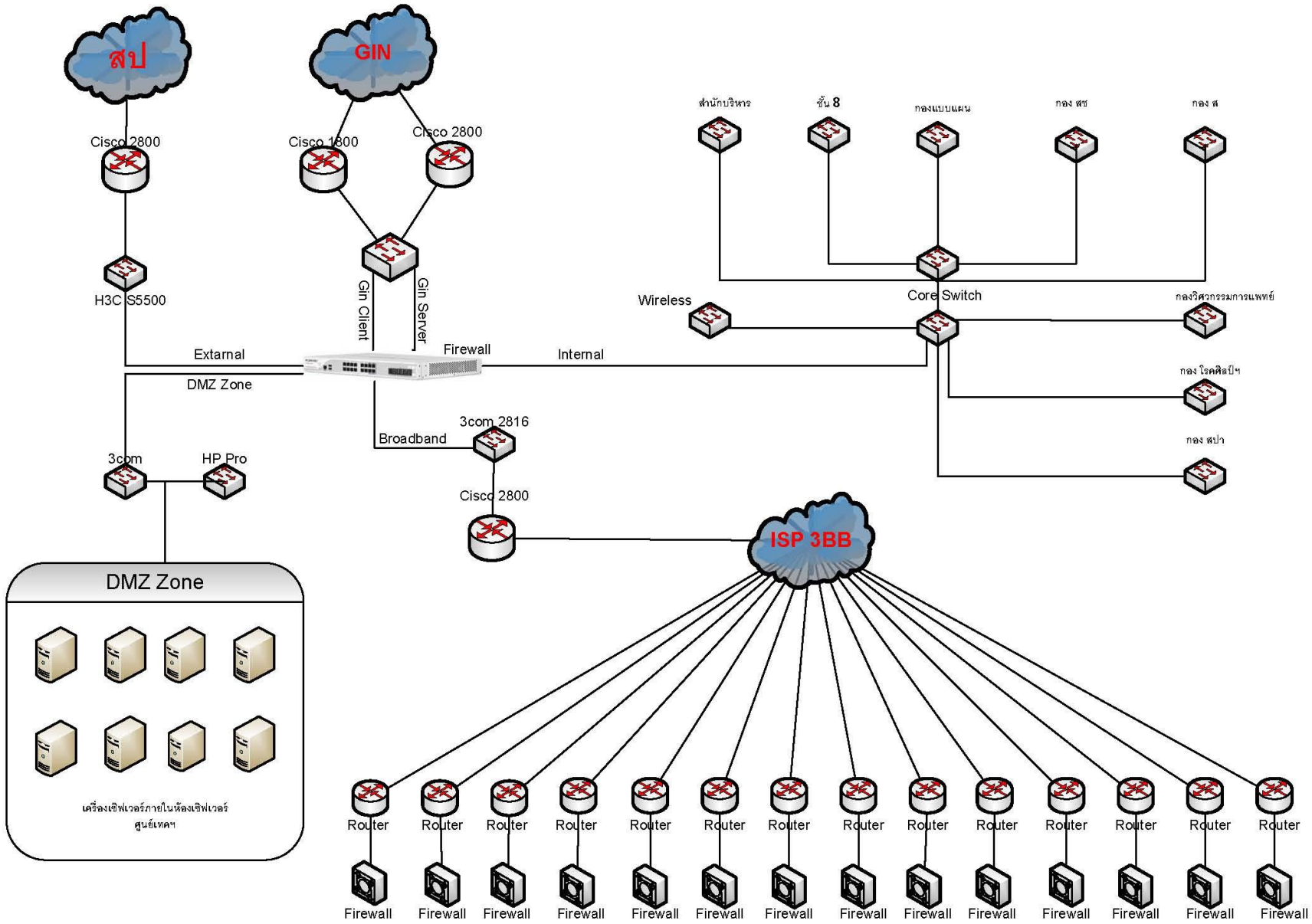
(๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้บัญชาการกรมสนับสนุน

(๒) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(๓) วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้บัญชาการกรมสนับสนุน

(๔) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

(๕) การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน


สป
GIN
Cisco 2800
Cisco 1800
Cisco 2800
H3C S5500
Gin Client
Gin Server
Extarnal
Firewall
Internal
DMZ Zone
สำนักบริหาร
ชั้น 8
กองแบบแผน
กอง ศช
กอง ส
Wireless
Core Switch
กองวิศวกรรมการแพทย์
กอง โรคศิลป์ฯ
กอง สป้า
3com 2816
Broadband
3com
HP Pro
Cisco 2800
ISP 3BB
DMZ Zone
เครื่องเซิฟเวอร์ภายในห้องเซิฟเวอร์
ศูนย์เทคฯ
Router
Firewall

นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำ อุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ควรเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

ข้อ ๕ ผู้ดูแลระบบ (System Administrator) ควรมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ ๖ ผู้ดูแลระบบ (System Administrator) ควรกำหนดให้ผู้ใช้บริการในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

ข้อ ๗ ผู้ดูแลระบบ (System Administrator) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ (System Administrator) รายงานต่อผู้บัญชาการสำนักงานตำรวจแห่งชาติทราบทันที

ข้อ ๘ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

ความมั่นคงปลอดภัยของการตรวจจับการบุกรุก

(Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS Policy)

ข้อ ๑ IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในกรมสนับสนุนให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

ข้อ ๒ IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของกรมสนับสนุน และเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

ข้อ ๓ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

ข้อ ๔ ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ ๕ โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

ข้อ ๖ มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

ข้อ ๗ มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ ๘ IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

ข้อ ๙ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๐ กรมสนับสนุนมีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งาน ล่วงหน้า

ข้อ ๑๑ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของกรมสนับสนุนการพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของกรมสนับสนุนจะต้องถูกดาเนินคดีตามขั้นตอนของกฎหมาย

การกำหนด IPS Policy ของกรมสนับสนุนจะกำหนดผ่านการใช้งาน Firewall ซึ่ง Policy จะถูกกำหนดเป็นเกณฑ์มาตรฐานในการใช้งาน โดยแบ่งตามประเภทการใช้งานของงานแต่ละประเภท ดังต่อไปนี้

1. all_default – การตรวจสอบและป้องกันอยู่ในระดับสูงสุด ซึ่ง IPS/IDS จะทำการตรวจสอบและป้องกันในระดับสูงสุด โดยจะทำการตรวจสอบและป้องกันในทุกระดับของการโจมตี
2. protect_http_server – การตรวจสอบและป้องกันจะมุ่งเน้นไปในการป้องกันการโจมตีผ่าน HTTP โปรโตคอล ซึ่ง IPS/IDS จะทำการตรวจสอบและป้องกันการใช้งาน HTTP เป็นหลัก โดยจะทำการตรวจสอบผู้ที่เข้าใช้งาน Web Server ของกรม และผู้ที่ออกไปใช้งาน Internet
3. protect_client – การตรวจสอบและป้องกันจะมุ่งเน้นไปในการป้องกันการโจมตีเครื่องลูกข่าย ซึ่ง IPS/IDS จะทำการตรวจสอบและป้องกันการใช้งานเครือข่ายของ Client ซึ่งอาจถูกโจมตีจากการใช้งานเครือข่าย Internet เช่น Worm หรือ Trojan ต่างๆ

<u>นโยบายความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)</u>

ข้อ ๑ ศูนย์เทคโนโลยีสารสนเทศ มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด

ข้อ ๒ การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

ข้อ ๓ ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบายจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

ข้อ ๔ ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Login account ก่อนการใช้งานทุกครั้ง

ข้อ ๕ ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

ข้อ ๖ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๗ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๘ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางกรมสนับสนุนอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความความยินยอมจากกรมสนับสนุนก่อน

ข้อ ๙ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จาเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบาย

จะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

ข้อ ๑๐ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

ข้อ ๑๑ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๒ กรมสนับสนุนมีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มี ความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ ๑๓ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจาก กรมสนับสนุนก่อน

ข้อ ๑๔ ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

<u>นโยบายความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access control Policy)</u>

หมวด ๑ การควบคุมการเข้าถึงระบบสารสนเทศ

ข้อ ๑ สำนักงานตำรวจแห่งชาติ กำหนดมาตรการควบคุมการเข้าใช้งาน ระบบสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บัญชาการสำนักงานสำนักงานตำรวจแห่งชาติ

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

หมวด ๒ การบริหารจัดการการเข้าถึงระบบสารสนเทศ

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของสำนักงานตำรวจแห่งชาติ ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

(๓) ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

(๔) ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๕) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๖) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหนง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

(๕) ควรกำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

บทที่ 4
การพัฒนาระบบของกองวิศวกรรมการแพทย์

การพัฒนาระบบเครือข่ายคอมพิวเตอร์ของกองวิศวกรรมการแพทย์ คือ การดำเนินการปรับปรุงระบบการเชื่อมโยงต่าง ๆ ของกองวิศวกรรมการแพทย์ เชื่อมต่อระหว่างกรมสนับสนุนบริการสุขภาพ กับ กองวิศวกรรมการแพทย์รวมทั้งเขต บริการของกรม จำนวน 12 เขต ปรับปรุงเครือข่ายคอมพิวเตอร์ของกองวิศวกรรมการแพทย์ให้รองรับและสนับสนุนการปฏิบัติงานด้านต่าง ๆ โดยมีรายละเอียดอุปกรณ์ดังนี้

1. **อุปกรณ์เครือข่าย Access Switch จำนวน 10 ตัว โดยมีคุณลักษณะต่อชุดอย่างน้อยดังต่อไปนี้**
    1. ทำงานได้ในระดับ Layer 2 Switching และ Layer 3 Routing
    2. มีขนาดของ Switching Capacity ไม่น้อยกว่า 56 Gbps และ Switching Throughput ไม่น้อยกว่า 41 Mpps ตามลำดับ
    3. มีพอร์ตแบบ 10/100/1000BASE-T จำนวน 24 พอร์ต
    4. มีพอร์ตแบบ SFP ไม่น้อยกว่า 4 พอร์ต
    5. เป็นอุปกรณ์สวิตช์ที่สามารถทำการจัดลำดับความสำคัญของข้อมูลตามมาตราฐาน IEEE 802.1p
    6. สนับสนุน Routing แบบ Static ได้ไม่น้อยกว่า 32 routes
    7. สามารถทำงานได้ตามมาตรฐานการจัดแบ่ง VLAN และ Tagging ตามมาตรฐาน IEEE 802.1Q
    8. สนับสนุนการทำงานแบบ Rate Limiting แล ะสนับสนุนการจัดลำดับความสำคัญตาม TCP/UDP พอร์ตได้เป็นอย่างน้อย
    9. สนับสนุนการทำงานแบบ Port mirroring , Network Time Protocol และ IEEE802.1AB Link Layer Discovery Protocol (LLDP) , LLDP-MED ได้
    10. มีระบบรักษาความปลอดภัยสำหรับเครื่องลูกข่ายแบบ IEEE 802.1x และ auto-voice VLAN ได้
    11. สามารถกำหนด Access Control List และการควบคุมข้อมูลแบบ Broadcast Control ได้

12. สามารถทำงานได้ตามมาตรฐาน Link Aggregation IEEE 802.3ad
13. สนับสนุนมาตรฐาน RMON และ SNMP ได้เป็นอย่างน้อย และรองรับการจัดการผ่านทาง CLI และ HTTPS ได้

2. **อุปกรณ์ Wireless Access Point จำนวน 14 ตัว โดยแต่ละชุดมีคุณลักษณะเฉพาะอย่างน้อยดังนี้**
    1. มีแลนพอร์ต 10/100/1000 Base-T แบบ Full Duplex ที่รองรับระบบ auto MDI/MDIX อย่างน้อย 1 พอร์ต
    2. รองรับการจ่ายไฟผ่านสายแลนแบบ Power over Ethernet ตามมาตรฐาน 802.3af ได้
    3. มีสายอากาศภายนอกขนาด 3dBi ไม่น้อยกว่า 2 ชุด
    4. รองรับการทำงานตามมาตรฐานดังต่อไปนี้
    5. รองรับมาตรฐาน IEEE 802.11b, IEEE 802.11g และ IEEE 802.11n
    6. รองรับมาตรฐาน IEEE 802.11i
    7. รองรับมาตรฐาน IEEE 802.1q
    8. รองรับมาตรฐาน IEEE 802.1x
    9. รองรับมาตรฐาน IEEE 802.11az
    10. รองรับย่านความถี่ที่ตั้งแต่ 2.412 GHz ถึง 2.472 GHz
    11. รองรับการรับส่งข้อมูลที่ความเร็วสูงสุด 300 Mbps
    12. รองรับการทำงานแบบ Multiple SSIDs ได้ และใช้งาน SSID ที่แตกต่างกัน ได้สูงถึง 4 SSIDs พร้อมกัน
    13. รองรับระบบรักษาความปลอดภัยของ Wireless LAN ดังต่อไปนี้
    14. รองรับระบบรักษาความปลอดภัยแบบ WEP 64/128/152
    15. รองรับระบบรักษาความปลอดภัยแบบ WPA-PSK, WPA2-PSK
    16. รองรับระบบรักษาความปลอดภัยแบบ WPA-Enterprise, WPA2-Enterprise
    17. รองรับระบบรักษาความปลอดภัยแบบ 802.1x (EAP-TLS, TTLS, PEAP, SIM)
    18. รองรับการทำ QoS แบบ WMM และ DiffServ Marking ได้
    19. รองรับการทำ MAC Filtering ได้ไม่น้อยกว่า 128 รายการ

20. รองรับทำการ Authentication User ผ่าน Radius Server ได้
21. สามารถเลือกโหมดการทำงานเป็น AP, Repeater, Bridge, Wireless Client ได้
22. รองรับการบริหารจัดการผ่านทาง HTTP , Telnet, FTP, SNMP v2C, v3 ได้
23. รองรับการทำงานที่อุณหภูมิ 0 ถึง 50 องศาเซลเซียส ความชื้นสัมพัทธ์ 20% ถึง 95 %
24. รองรับมาตรฐาน FCC Part 15C, ETSI EN 300 328, DGT LP000, FCC Part 15/107, EN 60950-1, IEC 60950-1

3. **เครื่องสำรองไฟฟ้าขนาด 1000 VA จำนวน 7 ตัว โดยแต่ละชุดมีคุณลักษณะเฉพาะอย่างน้อย ดังนี้**
    1. เป็นเครื่องสำรองไฟชนิด On Line Protection หรือ Line Interactive with Stabilizer
    2. มีขนาดไม่ต่ำกว่า 1000 VA. / 400 Watts หรือดีกว่า
    3. สามารถรับแรงดันไฟฟ้าขาเข้าได้ที่ 220 Volts +/- 25 %, Frequency 50 Hz .
    4. สามารถจ่ายแรงดันไฟฟ้าขาออกได้ที่ 220 Volt +/- 10 %, Frequency 50 Hz +/- 0.1 % หรือดีกว่า
    5. ใช้แบตเตอรี่ชนิด Sealed Lead Acid Maintenance Free
    6. มี Surge Protection For Telephone Line
    7. มี LED แสดงสถานะ On line และ On battery
    8. มี Switch ทดสอบแบตเตอรี่และตัดสัญญาณเสียงเตือนในตัวเดียวกัน
    9. มีระบบปิดเครื่องอัตโนมัติ (No load shutdown system) เมื่อไม่มีการใช้งาน (Option)
    10. สามารถเปิดเครื่องได้โดยใช้ไฟจากแบตเตอรี่
    11. สามารถเปลี่ยนแบตเตอรี่ได้โดยไม่ต้องปิดเครื่องและเปลี่ยนแบตเตอรี่ด้วยมือเปล่า (Hot Swap)
    12. มีเต้ารับด้านOutput เป็นแบบ Universal รับปลั๊กเสียบได้ทั้งขากลมและ ขาแบนไม่น้อยกว่า 4 ช่อง

13. ต้องได้รับมาตรฐานผลิตภัณฑ์อุตสาหกรรม (มอก.1291-2545) พร้อมแนบเอกสารแสดง
14. ต้องได้รับมาตรฐาน ISO 14001: 2004 และ ISO 9001: 2008 จากคณะกรรมการแห่งชาติว่าด้วยการรับรองระบบงาน(NAC)ที่ครอบคลุมถึง การผลิต การออกแบบ, โรงงาน, ขาย และ การบริการ (service) ที่ระบุในเอกสารอย่างชัดเจน พร้อมเอกสารยืนยัน
15. มีโรงงานผลิตในประเทศไทยไม่น้อยกว่า 18 ปี (พร้อมแสดงเอกสาร)
16. รับประกันคุณภาพ 1 ปีเต็มฟรีค่าอะไหล่และค่าบริการและศูนย์บริการไม่น้อยกว่า 40 ศูนย์ทั่วประเทศ(พร้อมแสดงเอกสาร)

4. **ตู้สำหรับจัดเก็บเครื่องคอมพิวเตอร์และอุปกรณ์ ชนิดแขวนผนัง (ขนาด 12U) จำนวน 7 ตัว โดยมีรายละเอียดอย่างน้อย**

ออกแบบและผลิตแบ่งออกเป็น 3 ส่วน คือ ส่วนหน้า กลางและหลัง

1. ต้องเป็นอุปกรณ์ที่ได้มาตรฐานที่มีความกว้าง x ลึก ของฐาน ไม่น้อยกว่า 600 x 500 มม.
2. ผลิตจากเหล็ก Electro galvanized sheet steel หนา1.2mm. แข็งแรงและกันสนิมได้ 100%
3. เสาสำหรับติดตั้งอุปกรณ์ผลิตจากเหล็ก Electro galvanized sheet steel หนา 2mm. มีความ แข็งแรงและป้องกันสนิม 100% สามารถปรับระยะการติดตั้งตามแนวลึกของ Rack ได้ตามความต้องการ
4. ฝาหน้าบริเวณส่วนกลางเป็น Plastic acrylic สีชาหนา 5mm. น้ำหนักเบาพร้อมยางกันฝุ่นรอบขอบประตู พร้อมบานพับที่อลูมิเนียมแข็งแรงพร้อมกุญแจล็อค (Turn lock)
5. ด้านข้างเจาะรูระบายอากาศโดยรอบ (Perforated slot) พร้อมกุญแจล็อค (Turn lock)
6. มีพัดลมสำหรับระบายความร้อน อย่างน้อย 1 ชุด
7. มีรางไฟฟ้าอย่างน้อย 6 ช่อง จำนวน 1 ชุด
8. เป็นสีทูโทน (สีขาวและสีเทาดำ) แบบ powder epoxy โดยใช้ระบบ Electro – Static เพื่อความแข็งแรงทนทาน

9. ได้รับมาตรฐาน ANIS/EIA-310D-1992(Rev.EIA-310-C), IEC 60297-1, IEC 60297-2, BS 5954: Part 2, DIN 41494. หรือเทียบเท่า

5. **งานติดตั้ง และงานเดินสายสัญญาณ (Cabling)**

1. เป็นสายสัญญาณชนิด Category 5e หรือดีกว่า

2. ชนิดสายสัญญาณ 4-Pairs, Unshielded Twisted Pair (UTP) Cables หรือดีกว่า

3. การติดตั้งสายสัญญาณสาย UTP ต่อเชื่อมกับหัวต่อ RJ-45 พร้อมยางกันฝุ่น (การเข้าหัวสายตามมาตรฐาน EIA/TIA 568B

เตรียมการก่อนการการพัฒนาระบบ

1) การทำ Site-Survey อย่างละเอียด

- ทำการ Site Survey โดยละเอียดเพื่อกำหนดตำแหน่งของ LAN outlet, Rack และ ชนิดวัสดุที่จะใช้ในบริเวณต่างๆ

2) กำหนดจุดติดตั้งต่างๆ หรือ Layout ต่างๆ ให้แล้วเสร็จก่อนเริ่มการติดตั้ง

3) จัดเตรียมสายสัญญาณต่างๆ

- จัดเตรียมสายสัญญาณต่างๆ สำหรับการเชื่อมต่อที่จำเป็นต่อการเชื่อมต่อระบบ

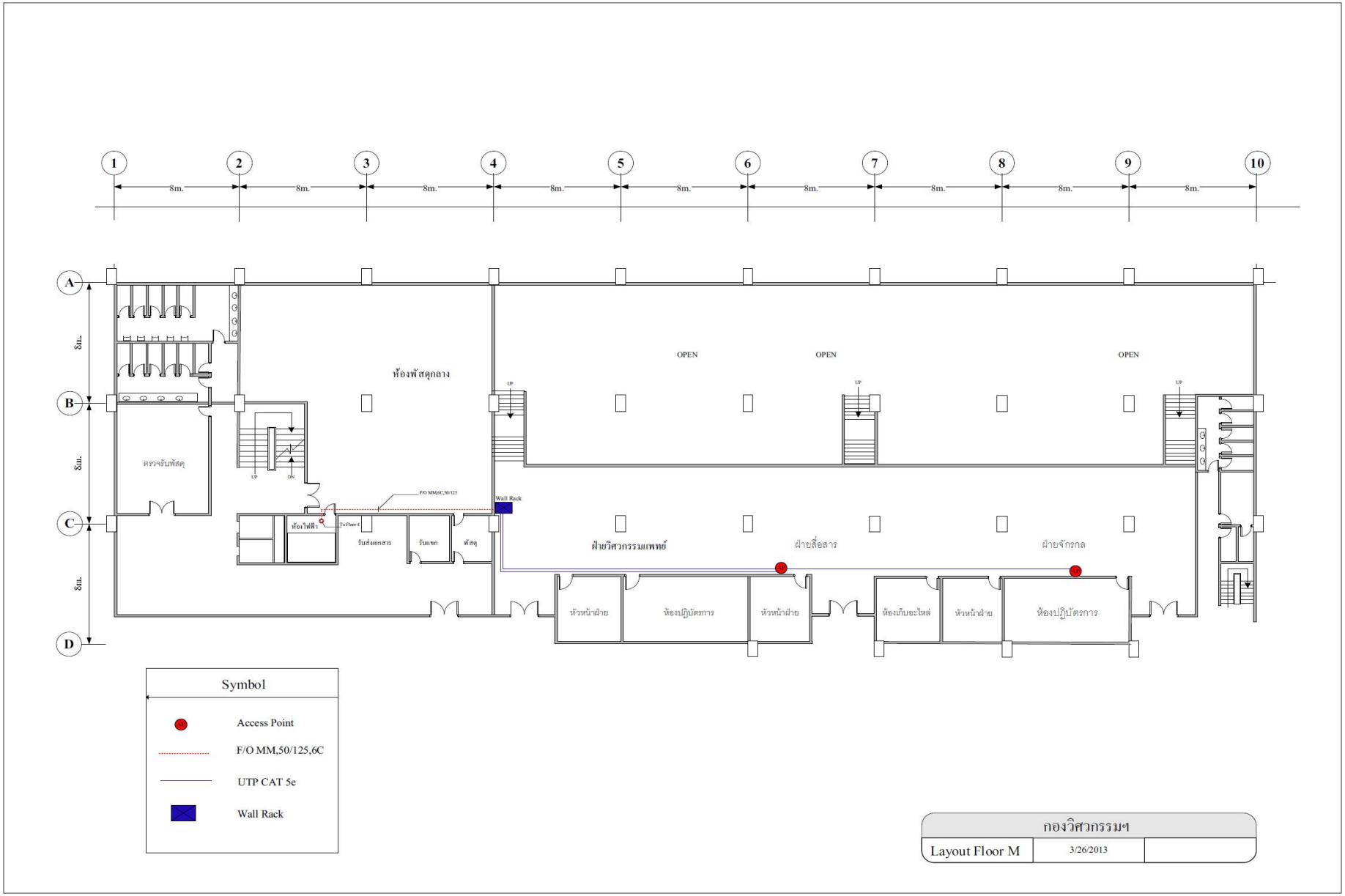
4) ติดตั้งอุปกรณ์เครื่องแม่ข่ายและอุปกรณ์เครือข่าย

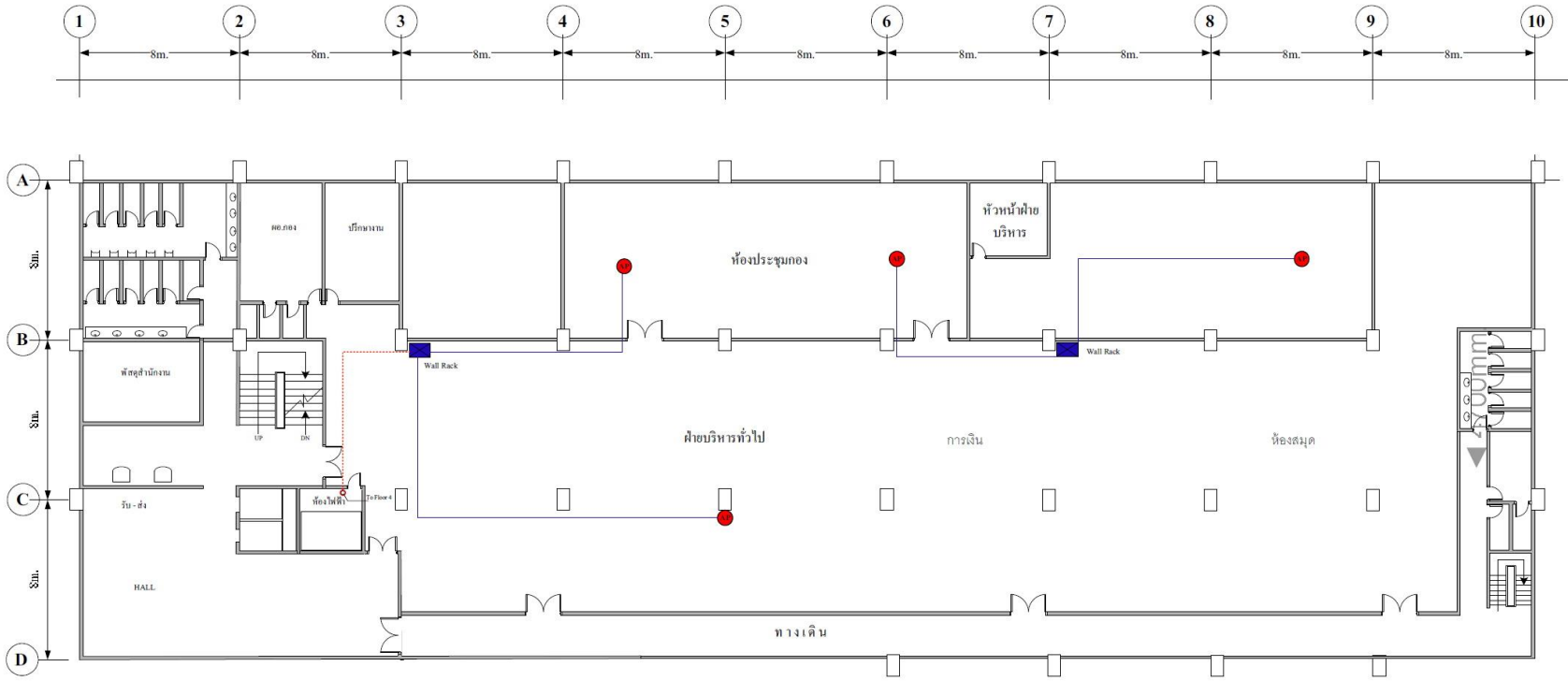
- ติดตั้งอุปกรณ์ตามข้อกำหนดและเงื่อนไขการติดตั้ง
- ทำการ Commissioning ระบบ และ Simulated Test

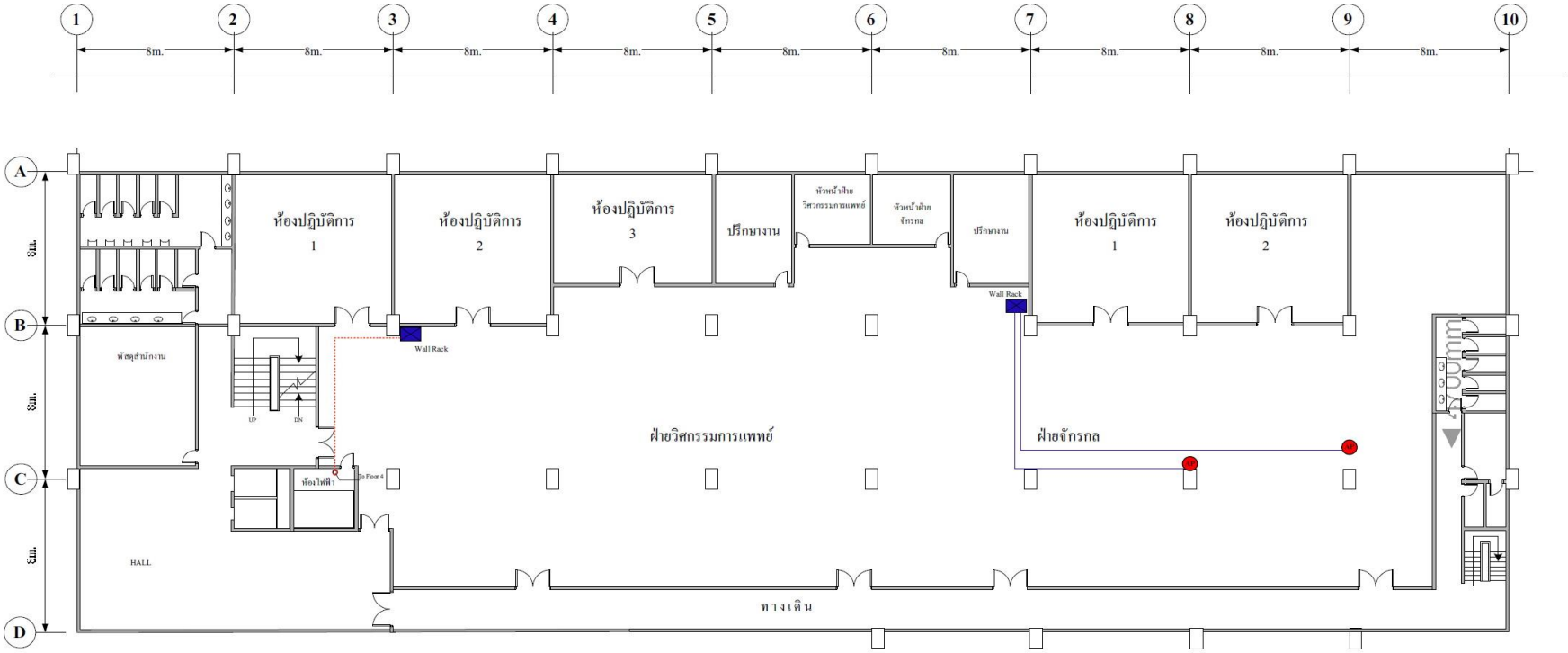
5) เชื่อมระบบเก่าและใหม่

- เพื่อให้การย้าย จากระบบเก่ามาระบบใหม่มีความต่อเนื่อง (less downtime) และเพื่อให้เกิดผลกระทบกับผู้ใช้งานน้อยที่สุด จึงต้องทำการเชื่อมต่อระบบใหม่และเก่าเข้าหากันก่อนย้ายระบบ
- ทดสอบการทำงานอุปกรณ์ระบบในแต่ละส่วนเพื่อให้แน่ใจว่าอุปกรณ์ที่ติดตั้งทำงานได้อย่างมีประสิทธิภาพ

แผนผังการติดตั้งระบบ




1
2
3
4
5
6
7
8
9
10
8m.
A
B
C
D
8m.
ห้องประชุมกอง
หัวหน้าฝ่าย
บริหาร
Wall Rack
Wall Rack
ฝ่ายบริหารทั่วไป
การเงิน
ห้องสมุด
พัสดุสำนักงาน
รับ - ส่ง
HALL
ห้องไฟฟ้า
To Floor 4
UP
DN
ท า ง เ ดิ น
Symbol
Access Point
F/O MM,50/125,6C
UTP CAT 5e
Wall Rack
กองวิศวกรรมฯ
Layout Floor 2
3/26/2013

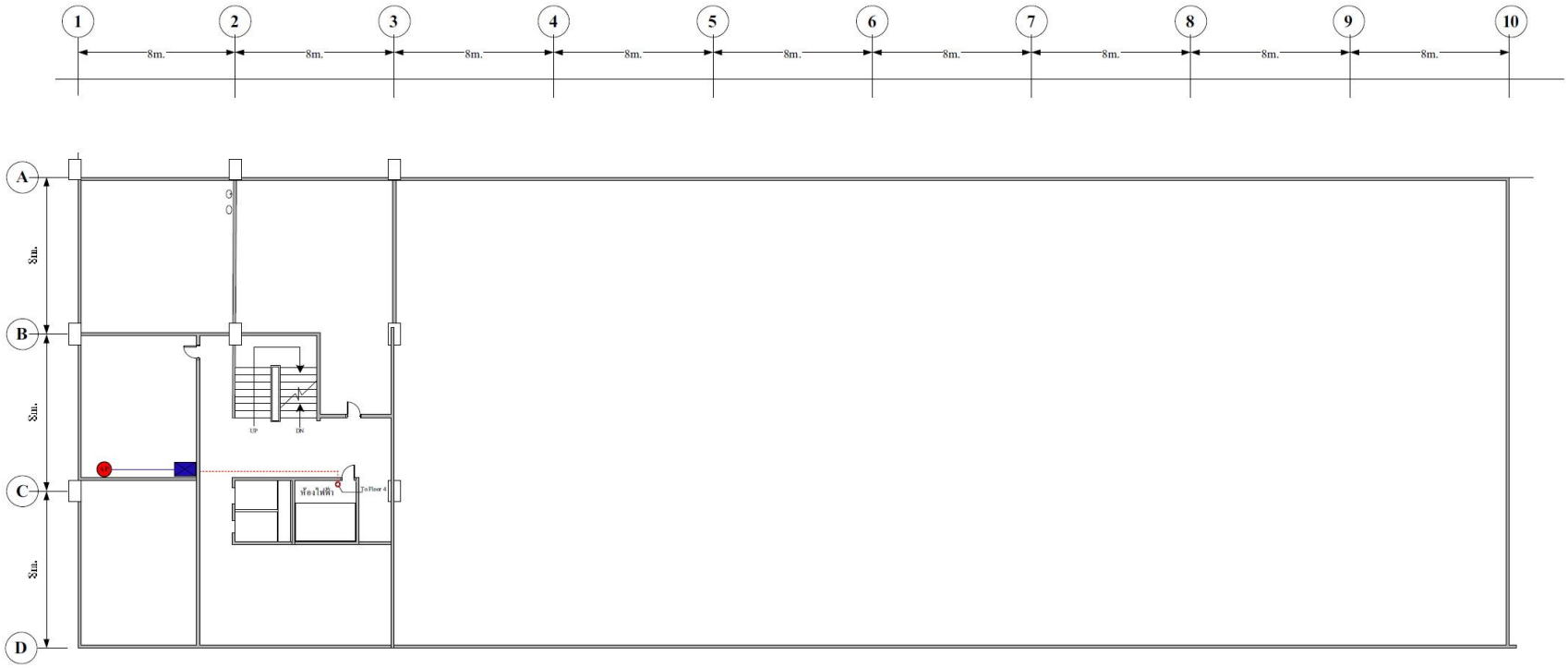


Symbol

- Access Point
- F/O MM,50/125,6C
- UTP CAT 5e
- Wall Rack

กองวิศวกรรมฯ		
Layout Floor 3	3/26/2013	

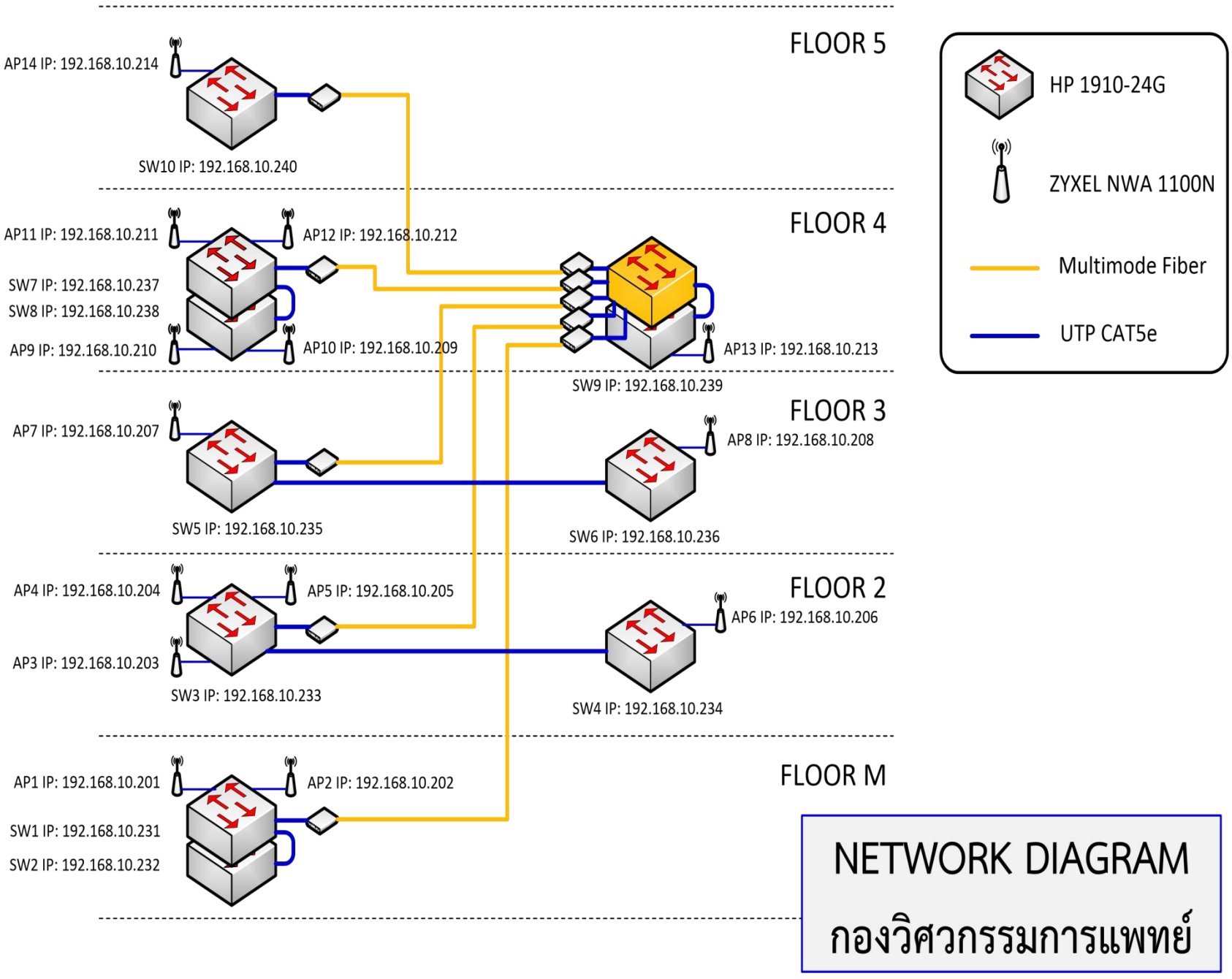

1
2
3
4
5
6
7
8
9
10
8m.
A
B
C
D
8m.
402
403
404
405
406
Server Room
408
409
410
UP
DN
ห้องไฟฟ้า
To Floor 4
ทางเดิน
Symbol
Access Point
F/O MM,50/125,6C
UTP CAT 5e
Wall Rack
กองวิศวกรรมฯ
Layout Floor 4
3/26/2013



Symbol

- Access Point
- F/O MM,50/125,6C
- UTP CAT 5e
- Wall Rack

กองวิศวกรรมฯ		
Layout Floor 5	3/26/2013	


FLOOR 5
AP14 IP: 192.168.10.214
SW10 IP: 192.168.10.240
FLOOR 4
AP11 IP: 192.168.10.211
AP12 IP: 192.168.10.212
SW7 IP: 192.168.10.237
SW8 IP: 192.168.10.238
AP9 IP: 192.168.10.210
AP10 IP: 192.168.10.209
AP13 IP: 192.168.10.213
SW9 IP: 192.168.10.239
FLOOR 3
AP7 IP: 192.168.10.207
AP8 IP: 192.168.10.208
SW5 IP: 192.168.10.235
SW6 IP: 192.168.10.236
FLOOR 2
AP4 IP: 192.168.10.204
AP5 IP: 192.168.10.205
AP6 IP: 192.168.10.206
AP3 IP: 192.168.10.203
SW3 IP: 192.168.10.233
SW4 IP: 192.168.10.234
FLOOR M
AP1 IP: 192.168.10.201
AP2 IP: 192.168.10.202
SW1 IP: 192.168.10.231
SW2 IP: 192.168.10.232
HP 1910-24G
ZYXEL NWA 1100N
Multimode Fiber
UTP CAT5e
NETWORK DIAGRAM
กองวิศวกรรมการแพทย์

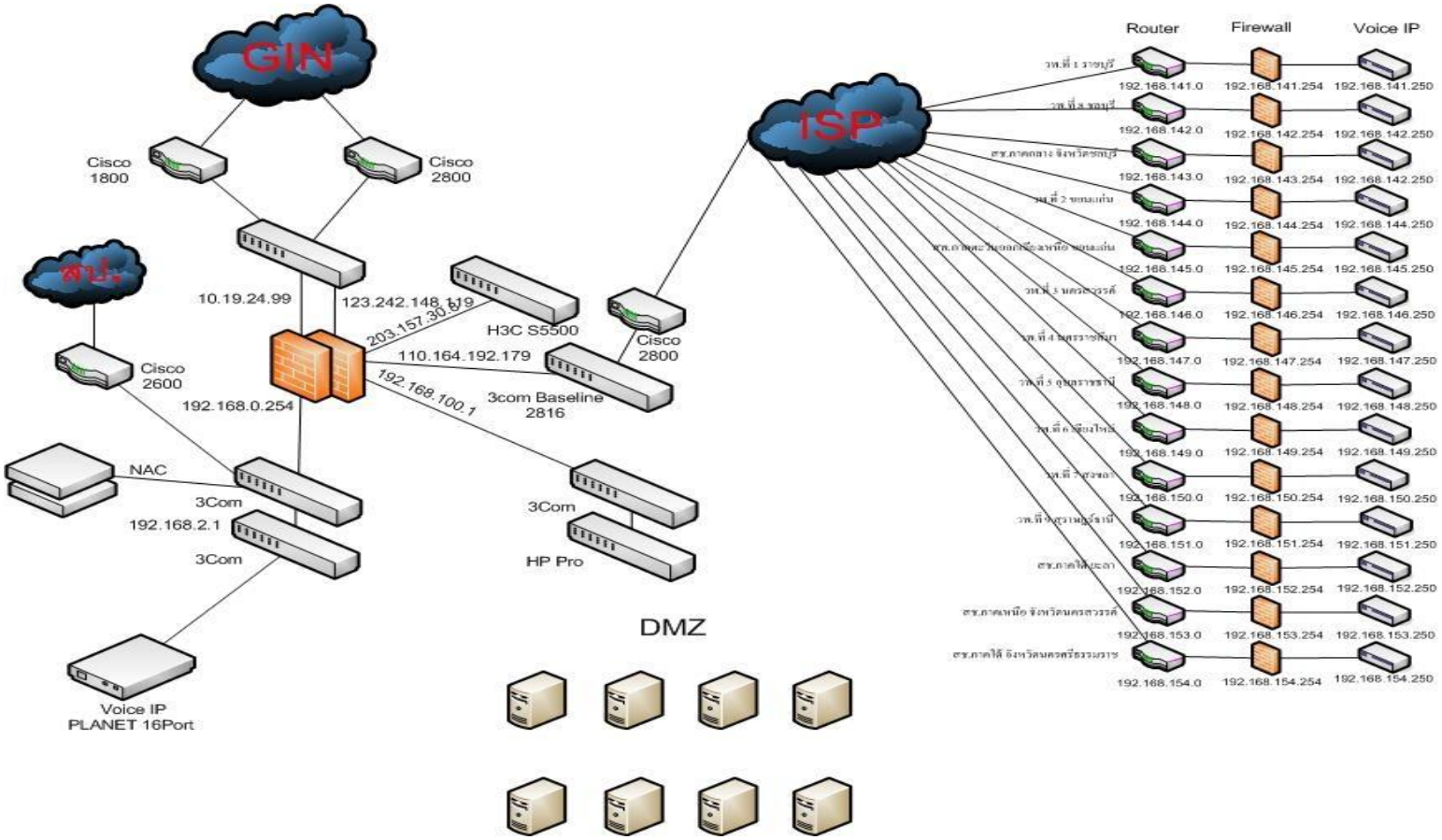
SUMMARY FIBER OPTIC 50/125 MM,6C Site กองวิศวกรรมการแพทย์							
Cable		Wavelength		Location		Length (m.)	Remark
Fiber Optic	Core	1300	Loss dB	From	To		
Fiber Optic 6 Core 50/125	1	●	0.47	FL M	SIRMER ROOM FL4	95	
Fiber Optic 6 Core 50/125	2	●	0.51	FL M	SIRMER ROOM FL4	95	
Fiber Optic 6 Core 50/125	3	●	0.50	FL M	SIRMER ROOM FL4	95	
Fiber Optic 6 Core 50/125	4	●	0.49	FL M	SIRMER ROOM FL4	95	
Fiber Optic 6 Core 50/125	5	●	0.44	FL M	SIRMER ROOM FL4	95	
Fiber Optic 6 Core 50/125	6	●	0.40	FL M	SIRMER ROOM FL4	95	
Fiber Optic 6 Core 50/125	7	●	0.46	FL 2	SIRMER ROOM FL4	75	
Fiber Optic 6 Core 50/125	8	●	0.51	FL 2	SIRMER ROOM FL4	75	
Fiber Optic 6 Core 50/125	9	●	0.46	FL 2	SIRMER ROOM FL4	75	
Fiber Optic 6 Core 50/125	10	●	0.50	FL 2	SIRMER ROOM FL4	75	
Fiber Optic 6 Core 50/125	11	●	0.48	FL 2	SIRMER ROOM FL4	75	
Fiber Optic 6 Core 50/125	12	●	0.44	FL 2	SIRMER ROOM FL4	75	
Fiber Optic 6 Core 50/125	13	●	0.50	FL 3	SIRMER ROOM FL4	83	
Fiber Optic 6 Core 50/125	14	●	0.46	FL 3	SIRMER ROOM FL4	83	
Fiber Optic 6 Core 50/125	15	●	0.47	FL 3	SIRMER ROOM FL4	83	
Fiber Optic 6 Core 50/125	16	●	0.43	FL 3	SIRMER ROOM FL4	83	
Fiber Optic 6 Core 50/125	17	●	0.46	FL 3	SIRMER ROOM FL4	83	
Fiber Optic 6 Core 50/125	18	●	0.40	FL 3	SIRMER ROOM FL4	83	
Fiber Optic 6 Core 50/125	19	●	0.50	FL 4	SIRMER ROOM FL4	49	
Fiber Optic 6 Core 50/125	20	●	0.44	FL 4	SIRMER ROOM FL4	49	
Fiber Optic 6 Core 50/125	21	●	0.43	FL 4	SIRMER ROOM FL4	49	
Fiber Optic 6 Core 50/125	22	●	0.48	FL 4	SIRMER ROOM FL4	49	
Fiber Optic 6 Core 50/125	23	●	0.39	FL 4	SIRMER ROOM FL4	49	
Fiber Optic 6 Core 50/125	24	●	0.43	FL 4	SIRMER ROOM FL4	49	
Fiber Optic 6 Core 50/125	25	●	0.45	FL 5	SIRMER ROOM FL4	78	
Fiber Optic 6 Core 50/125	26	●	0.50	FL 5	SIRMER ROOM FL4	78	
Fiber Optic 6 Core 50/125	27	●	0.45	FL 5	SIRMER ROOM FL4	78	
Fiber Optic 6 Core 50/125	28	●	0.48	FL 5	SIRMER ROOM FL4	78	
Fiber Optic 6 Core 50/125	29	●	0.49	FL 5	SIRMER ROOM FL4	78	
Fiber Optic 6 Core 50/125	30	●	0.47	FL 5	SIRMER ROOM FL4	78	
Fiber Optic 6 Core 50/125	31	●	0.33	SIRMER ROOM FL4	FL M	95	
Fiber Optic 6 Core 50/125	32	●	0.49	SIRMER ROOM FL4	FL M	95	
Fiber Optic 6 Core 50/125	33	●	0.50	SIRMER ROOM FL4	FL M	95	
Fiber Optic 6 Core 50/125	34	●	0.42	SIRMER ROOM FL4	FL M	95	
Fiber Optic 6 Core 50/125	35	●	0.44	SIRMER ROOM FL4	FL M	95	
Fiber Optic 6 Core 50/125	36	●	0.46	SIRMER ROOM FL4	FL M	95	
Fiber Optic 6 Core 50/125	37	●	0.49	SIRMER ROOM FL4	FL 2	75	
Fiber Optic 6 Core 50/125	38	●	0.43	SIRMER ROOM FL4	FL 2	75	
Fiber Optic 6 Core 50/125	39	●	0.50	SIRMER ROOM FL4	FL 2	75	
Fiber Optic 6 Core 50/125	40	●	0.45	SIRMER ROOM FL4	FL 2	75	
Fiber Optic 6 Core 50/125	41	●	0.50	SIRMER ROOM FL4	FL 2	75	
Fiber Optic 6 Core 50/125	42	●	0.46	SIRMER ROOM FL4	FL 2	75	
Fiber Optic 6 Core 50/125	43	●	0.47	SIRMER ROOM FL4	FL 3	83	
Fiber Optic 6 Core 50/125	44	●	0.32	SIRMER ROOM FL4	FL 3	83	
Fiber Optic 6 Core 50/125	45	●	0.47	SIRMER ROOM FL4	FL 3	83	
Fiber Optic 6 Core 50/125	46	●	0.39	SIRMER ROOM FL4	FL 3	83	
Fiber Optic 6 Core 50/125	47	●	0.34	SIRMER ROOM FL4	FL 3	83	
Fiber Optic 6 Core 50/125	48	●	0.37	SIRMER ROOM FL4	FL 3	83	
Fiber Optic 6 Core 50/125	49	●	0.45	SIRMER ROOM FL4	FL 4	49	
Fiber Optic 6 Core 50/125	50	●		SIRMER ROOM FL4	FL 4	49	

ระบบสามารถใช้ครอบคลุมทั้งกองวิศวกรรมการแพทย์ โดยสามารถระบุ IP ของแต่ละเครื่องที่ต่ออยู่กับระบบได้อย่างสะดวก และระบบเครือข่ายไร้สายสามารถติดต่อได้โดยใช้เพียงการ LOGIN เพียงครั้งเดียว โดยระบบที่ใช้ในระบบแบบใช้สาย จะใช้ IP ทั้ง IP จริง และ Private IP Class C วง 192.168.9.0 – 192.168.9.255 ใช้ได้ไม่น้อยกว่า 250 เครื่อง และ ระบบไร้สายใช้ Private IP Class C วง 192.168.10.0 – 192.168.10.255 ใช้กับคอมพิวเตอร์ไร้สายไม่น้อยกว่า 250 เครื่อง สามารถใช้ได้ทุกจุดครอบคลุมพื้นที่ให้บริการของกองวิศวกรรมการแพทย์

โดยทั้งระบบสามารถเชื่อมต่อกับเครื่องพิมพ์ผ่านเครือข่าย เชื่อมต่ออินเตอร์เน็ต เชื่อมต่อกับกรมสนับสนุนบริการสุขภาพและสำนักเขตบริการสุขภาพ โดยผ่านโครงข่าย Vlan ใช้ได้เสมือนเป็นเครือข่ายเดียวกันทั้งหมด รวมทั้งการรักษาความปลอดภัยในการเข้าระบบเครือข่าย ทั้งไร้สายและใช้สาย โดยต้องมีการระบุตัวตนก่อนเข้าใช้งานทุกคน

บทที่ 5
สรุปผล

ในการพัฒนาและบูรณาการระบบเทคโนโลยีสารสนเทศ เพื่อเป็นการสนับสนุนหน่วยงานภายใต้สังกัด โดยจัดทำระบบเชื่อมโยงเครือข่ายของกองวิศวกรรมการแพทย์ และ ระบบเทคโนโลยีสารสนเทศเพื่อเชื่อมโยงระบบเข้ากับระบบของกรมสนับสนุนสุขภาพ จากแนวทางการพัฒนาดังกล่าว ซึ่งมีการดำเนินการไปบางส่วนในบทที่ 4 แล้วนั้น ระบบดังกล่าวจะต้องมีการพัฒนาปรับปรุงและแก้ไขปัญหาระบบ เพื่อสามารถนำไปปรับปรุงแก้ไขระบบ และวางแผนงานในระยะยาวได้ การติดต่อสื่อสารแลกเปลี่ยนข้อมูลระหว่างเครือข่ายของกองวิศวกรรมการแพทย์การติดต่อทางระบบเครือข่าย Internet ทั้งระบบใช้สายและระบบไร้สาย ของหน่วยงานเป็นไปอย่างสะดวกและรวดเร็ว ซึ่งการติดต่อสื่อสารจะผ่านอุปกรณ์ป้องกันเครือข่ายที่มีการบริหารจัดการความปลอดภัยการเชื่อมโยงข้อมูลกับระบบ VPN (Virtual private Network) ซึ่งเป็นการเชื่อมต่อระหว่างกรมสนับสนุนบริการสุขภาพส่วนกลางและหน่วยงานในสังกัดจะใช้ประโยชน์จากการเชื่อมต่อกันเดิมที่ใช้บริการทาง Internet ในการส่งข้อมูลถึงกัน โดยเพิ่มขีดความสามารถของระบบรักษาความปลอดภัยในการส่งข้อมูลในรูปแบบของ VPN และทางศูนย์ได้ทำการเชื่อมต่อระบบโทรศัพท์ VOIP เพื่อใช้งานร่วมกับระบบเครือข่ายที่จัดทำขึ้นอีกด้วย ซึ่งการเชื่อมต่อเครือข่ายของกรมสนับสนุนบริการสุขภาพส่วนกลาง และส่วนภูมิภาค มีการเชื่อมต่อเครือข่ายผ่านระบบ Internet โดยใช้ระบบการเข้ารหัสแบบ VPN (Virtual Private Network) ผ่านอุปกรณ์ป้องกันเครือข่าย Firewall ดังรูป


GIN
ISP
Cisco 1800
Cisco 2800
10.19.24.99
123.242.148.119
203.157.30.67
H3C S5500
Cisco 2800
Cisco 2600
110.164.192.179
192.168.0.254
192.168.100.1
3com Baseline 2816
NAC
3Com
192.168.2.1
3Com
3Com
HP Pro
Voice IP PLANET 16Port
DMZ
Router
Firewall
Voice IP
192.168.141.0
192.168.141.254
192.168.141.250
192.168.142.0
192.168.142.254
192.168.142.250
192.168.143.0
192.168.143.254
192.168.142.250
192.168.144.0
192.168.144.254
192.168.144.250
192.168.145.0
192.168.145.254
192.168.145.250
192.168.146.0
192.168.146.254
192.168.146.250
192.168.147.0
192.168.147.254
192.168.147.250
192.168.148.0
192.168.148.254
192.168.148.250
192.168.149.0
192.168.149.254
192.168.149.250
192.168.150.0
192.168.150.254
192.168.150.250
192.168.151.0
192.168.151.254
192.168.151.250
192.168.152.0
192.168.152.254
192.168.152.250
192.168.153.0
192.168.153.254
192.168.153.250
192.168.154.0
192.168.154.254
192.168.154.250

จากโครงสร้างเครือข่าย จะพบว่า มีอุปกรณ์หลายชนิดที่เกี่ยวข้องกับระบบงานเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการสุขภาพ และกองวิศวกรรมการแพทย์

ประโยชน์ของเครือข่ายไร้สาย

1. **Mobility** เพิ่มความสะดวกในการเคลื่อนย้าน ทำให้การใช้งานเครือข่ายไร้สายไม่ได้จำกัดอยู่ ณ จุดที่มีสายเคเบิลเดินถึงเท่านั้น แต่เครือข่ายไร้สาย สามารถช่วยให้ผู้ใช้สามารถเข้าถึงข้อมูลจากทุกๆ ที่ ที่สัญญาณครอบคลุมถึง

2. **Installation Simplicity** การติดตั้งเพื่อใช้งานนั้น สามารถทำได้ง่ายและรวดเร็ว เพราะมไม่ต้องเสียเวลาติดตั้งสายเคเบิล และไม่รกรุงรัง

3. **Installation Flexibility** มีความยืดหยุ่นในการติดตั้งระบบเครือข่าย เพราะในบางครั้ง บางเวลาจำเป็นต้องมีการเคลื่อนย้ายจุดปล่อยสัญญาณ เพื่อนให้สัญญาณครอบคลุมพื้นที่ที่ต้องการ ซึ่งเครือข่ายไร้สายทำได้ง่ายไม่ยุ่งยาก

4. **Reduce cost-of-ownership** การลงทุนในระยะยาวนั้นจะมีต้นทุนที่ต่ำกว่า ถึงแม้ราคาอุปกรณ์ของเครือข่ายไร้สายจะมีราคาที่สูงกว่าอุปกรณ์เครือข่ายใช้ สาย แต่ระบบเครือข่ายไร้สายนั้นจะลดต้นทุนในการติดตั้งในเรื่องคน และเวลา รวมถึงการบำรุงรักษาระบบเครือข่าย เพราะไม่ต้องคอยดูแลสายเคเบิลซึ่งอาจจะเป็นส่วนที่ทำให้เกิดปัญหาในอนาคต

5. **Scalability** เครือข่ายไร้สายทำให้องค์กรสามารถปรับขนาด และความเหมาะสมได้ง่าย ไม่ยุ่งยาก เพราะสามารถโยกย้าย หรือปรับเปลี่ยนตำแหน่งการใช้งาน โดยเฉพาะระบบที่มีกาเชื่อมต่อระหว่างอาคาร

แนวทางการพัฒนาระบบเทคโนโลยีสารสนเทศของกองวิศวกรรมการแพทย์

จากการวิเคราะห์และสรุปปัญหา และอุปสรรคต่อการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารของกองวิศวกรรมการแพทย์ ได้ ดังนี้

- การปฏิบัติงานยังขาดแคลนอุปกรณ์ทางด้านเทคโนโลยีสารสนเทศและ การสื่อสารมาสนับสนุน โดยเฉพาะในการเพิ่มประสิทธิภาพการปฏิบัติงานและการจัดเก็บ การรายงานข้อมูลต่างๆ ที่จำเป็นต่อการบริหารจัดการ
- ระบบเทคโนโลยีสารสนเทศที่พัฒนาขึ้นมานั้น ยังเป็นลักษณะแยกส่วน ยังไม่ได้เชื่อมโยงให้เกิดความสามารถในการบูรณาการ แลกเปลี่ยนข้อมูล และส่งต่อกิจกรรมระหว่างกัน
- การจัดเก็บ รวบรวมข้อมูลภายใน ยังเป็นลักษณะที่แยกส่วน ยังไม่มีหน่วยงานหลักใดที่จะรับผิดชอบในการบูรณาการ เพื่อเชื่อมโยงข้อมูลและเพิ่มคุณค่าของข้อมูลระหว่างกัน จึงส่งผลให้ข้อมูลที่มีอยู่ติดอยู่กับบุคลากรที่รับผิดชอบในส่วนงานนั้นๆ และทำให้มีความซ้ำซ้อนในการรายงานหรือรวบรวมข้อมูล

- ขาดแคลนบุคลากรที่มีองค์ความรู้และทักษะด้านเทคโนโลยีชั้นสูงในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร
- พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ ตลอดจนระบบรักษาความปลอดภัย การบริหารความเสี่ยง
- สร้างและปรับปรุง โครงสร้างพื้นฐาน ด้านเทคโนโลยี สารสนเทศ เพื่อรองรับการขยายการให้บริการได้ ทั่วถึงมีประสิทธิภาพและ เสถียรภาพ แผนเพิ่มความ มั่นคงปลอดภัยให้ ระบบเทคโนโลยีสารสนเทศ
- การบำรุงรักษาอุปกรณ์ที่เกี่ยวข้อง กับการพัฒนาระบบ โครงสร้างพื้นฐาน ICT
- การขยาย ช่องทางการสื่อสาร ทางอินเทอร์เน็ต
- การจัดหาเพิ่มเติม อุปกรณ์กระจายสัญญาณแบบมีสาย และไร้สาย
- การจัดหา ทดแทน และปรับปรุงการใช้งานเครื่องคอมพิวเตอร Server และขยายระบบ
- งการจัดหาระบบสำรองข้อมูล และศูนย์สำรองระบบสารสนเทศ จากภัยพิบัติ (Disaster Recovery System)
- การจัดหาและทดแทนอุปกรณ์คอมพิวเตอร์ลูกข่ายและอุปกรณ์ต่อพ่วง
- การเสริมสร้างขีดความสามารถของบุคลากรทางด้านสารสนเทศ เพื่อใช้ในงานด้านวิศวกรรม การแพทย์

บรรณานุกรม

แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ. 2557 -2560 กรมสนับสนุนบริการสุขภาพ

การศึกษาเชิงประเมินมาตรฐานความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และระบบเครือข่าย ของหน่วยราชการในกรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข :พ.ศ. 2555

เรืองไกร รังสิพล. (2544): เจาะระบบ TCP/IP จุดอ่อนของโปรโตคอลและวิธีป้องกัน: กรุงเทพ ฯ บ.โปรวิชั่น จำกัด

ผศ.ดร.สัลยุทธ สว่างวรรณ (2542):COMPUTER NETWORTS. กรุงเทพ ฯ : ซีเอ็ดยูเคชั่น

จตุชัย แพงจันทร์. (2547). **เจาะระบบเน็ตเวิร์ค ฉบับสมบูรณ์.** พิมพ์ครั้งที่ 2. นนทบุรี : ไอดีซีฯ

วรินทร์ เมฆประดิษฐ์สิน. (2547). **คัมภีร์ระบบเครือข่ายฉบับอาจารย์วรินทร์เล่ม 1**.

ศรีไพร ศักดิ์รุ่งพงศากุล และเจษฎาพร ยุทธนวิบูลย์ชัย. (2549). **ระบบสารสนเทศและเทคโนโลยีการจัดการความรู้.** พิมพ์ครั้งที่ 6. กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

http://mymint.tripod.com/