บทที่ 12
เครือข่ายอินเตอร์เน็ตและเว็บ

จนถึงบทนี้การเดินทางไปตามถนนสายยาวของระบบเครือข่ายคอมพิวเตอร์ที่เริ่มจากศึกษาระบบเครือข่ายแบบ **Peer–to–Peer** ขนาดเล็ก ไปยังระบบเครือข่าย **client/server** และระบบเครือข่าย **LAN** การขยายการเชื่อมต่อ **LAN** และเทคโนโลยี **WANs** สุดท้ายก็มาถึงระบบเครือข่ายที่นับว่าใหญ่ที่สุดในบรรดาระบบเครือข่ายทั้งหมดที่มี นั่นคือเครือข่ายอินเตอร์เน็ต **(Internet)** ซึ่งส่วนใหญ่เป็นผลงานของ **Vinton Cerf** ผู้ซึ่งเรียกว่าเป็นบิดาของเครือข่ายอินเตอร์เน็ต สำหรับงานของเขาคือการพัฒนาโปรโตคอล **TCP/IP** ที่ใช้กับระบบเครือข่ายที่มีอยู่ทุกหนทุกแห่ง

อาจจะมีคำถามว่าทำไมต้องอธิบายเกี่ยวกับเครือข่ายอินเตอร์เน็ต (หรือเจาะจงไปที่เรื่องของ **World Wide Web**) ในหนังสือเกี่ยวกับระบบเครือข่าย? แล้วทำไมถึงไม่ล่ะ? ถึงแม้ว่าคนส่วนใหญ่จะมองว่าอินเตอร์เน็ต คือบางสิ่งที่เป็นสื่อที่ให้ความเพลิดเพลินและสื่อทางการค้า แต่อินเตอร์เน็ตเดียวกันนี้ก็มีสิ่งที่หล่อเลี้ยงความสนใจในด้านเทคโนโลยีต่างๆ ตั้งแต่ **Web Browsing,** การพัฒนาซอฟต์แวร์ที่สามารถใช้ข้ามแพล็ตฟอร์มที่แตกต่างกัน เป็นตัวแทนจำหน่ายอัจฉริยะ สามารถทำการ **push/pull** ข่าวสารในด้านการพาณิชย์อิเล็กทรอนิกส์ **(e-commerce)** และธุรกิจในการพัฒนาเครือข่ายอินทราเน็ต **(Intranet)** และเอ็กซ์ตร้าเน็ต **(Extranet)** นอกจากนั้นเครือข่ายอินเตอร์เน็ตยังทำได้แม้แต่การจับกระแสความสนใจของรัฐบาลต่างๆ ทั่วโลก ถึงแม้ว่าคนทั้งโลกจะค้นพบว่า การให้ความสนใจของรัฐบาลจะเป็นสิ่งที่ดี แต่ก็ยังมีคำถามที่ถกเถียงกันระหว่างผู้เชี่ยวชาญทางด้านเทคนิคกับผู้ที่ไม่ใช่ผู้เชี่ยวชาญทางด้านเทคนิคอีกมาก อย่างไรก็ตามสิ่งเหล่านี้คือสิ่งที่พูดวกวนออกไปนอกเรื่องที่เราสนใจ

12.1 ประวัติความเป็นมา

ช่วงปีคริสต์ศตวรรษ **1960** (ประมาณปี **2503**) ซึ่งเป็นยุคสงครามเย็นระหว่าง สหรัฐ กับโซเวียต มีความเสี่ยงทางการทหาร และความเป็นไปได้ที่จะถูกโจมตีด้วยอาวุธปรมาณู หรือนิวเคลียร์ การทำลายล้างศูนย์คอมพิวเตอร์ และระบบการสื่อสารข้อมูลอาจทำให้เกิดปัญหาทางการรบ และในช่วงนี้ระบบคอมพิวเตอร์มีมากมายหลากแบบ นับเป็นอุปสรรคสำคัญทำให้ไม่สามารถแลกเปลี่ยนข้อมูล ข่าวสาร และโปรแกรมระหว่างกันได้โดยสะดวก จึงมีแนวความคิดในการวิจัยระบบที่สามารถเชื่อมโยงเครื่องคอมพิวเตอร์ และแลกเปลี่ยนข้อมูลระหว่างระบบที่แตกต่างกันได้ รัฐบาลสหรัฐจึงเริ่มจัดตั้งโครงการ อาร์พาเน็ต **(ARPAnet)** เมื่อปี **2509 (1966)** ดูแลโดยหน่วยงานวิจัยชั้นสูงของสหรัฐ **(ARPA: The Advanced Research Projects Agency** ซึ่งเปลี่ยนชื่อเป็น **DARPA: Defense Advanced Research Projects Agency** ในปี **2514 (1971)** แล้วเปลี่ยนกลับเป็น **ARPA** ในปี **2536 (1993)** และล่าสุดเปลี่ยนกลับเป็น **DARPA** ในปี **2539 (1996)**) ในสังกัดกระทรวงกลาโหม เพื่อให้คอมพิวเตอร์รู้จักค้นหาเส้นทางเชื่อมโยง และส่งข้อมูลโดยอัตโนมัติ **(dynamic routing)** ในกรณีที่เครือข่ายบางจุดถูกทำลายหรือเกิดความเสียหาย เครือข่ายที่เชื่อมโยงอยู่ในระบบที่เหลือจะต้องทำงานได้สำเร็จลุล่วงต่อไปได้

อินเตอร์เน็ตถือกำเนิดขึ้นเมื่อประมาณปี ค.ศ. **1969** หรือปี พ.ศ. **2512** จากจุดประสงค์ของโครงการอาร์พาเน็ต เพื่อสร้างเครือข่ายคอมพิวเตอร์ที่คงความสามารถในการติดต่อสื่อสารถึงกันได้ แม้ว่าจะมีบางส่วนของเครือข่ายไม่

สามารถทำงานได้ก็ตาม ระบบนี้ถูกออกแบบให้ไม่มีศูนย์กลางในการติดต่อ จุดเริ่มของอาร์พาเน็ต ได้ทำการทดลองต่อเชื่อมคอมพิวเตอร์จาก 4 แห่ง ช่วงเดือนกันยายน 2512 (1969) เริ่มต้นจาก มหาวิทยาลัยลอสแองเจลิส (UCLA) กับสถาบันวิจัยสแตนฟอร์ด (SRI) ทั้งสองแห่งอยู่ในรัฐแคลิฟอร์เนียและเพิ่มอีกสองแห่ง คือ มหาวิทยาลัยซานตาบาร์บารา (UCSB) ในรัฐแคลิฟอร์เนีย และมหาวิทยาลัยแห่งรัฐยูท่าห์ (UTAH)

แนวคิดเบื้องต้นของวิธีการส่งข้อมูลบนอินเทอร์เน็ต เกิดจากพัฒนาการของ “โปรโตคอล (Protocol)” ซึ่งหมายถึง มาตรฐานกลางของการเชื่อมโยงคอมพิวเตอร์หลากหลายระบบ รวมถึงวิธีการส่งข้อมูล และแลกเปลี่ยนข้อมูลระหว่างกันให้สามารถทำงานร่วมกันได้ โปรโตคอลเหล่านี้ มีพัฒนาการมาเป็นลำดับตั้งแต่ NCP (Network Control Protocol) และล่าสุดเป็น TCP/IP (Transmission Control Protocol / Internet Protocol)

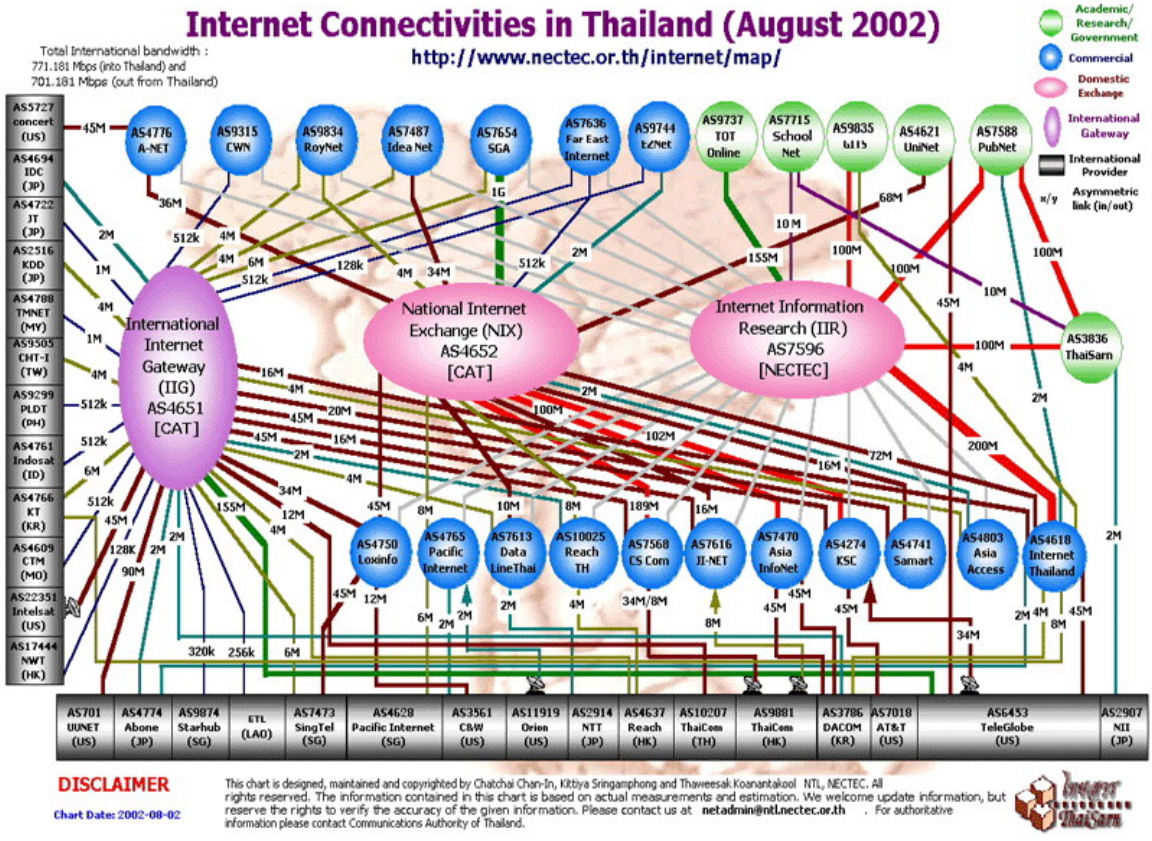
จากเครือข่าย WAN ระบบแรก ที่เกิดในปี 2508 (1965) เป็นการต่อคอมพิวเตอร์ TX-2 ในแมสซาจูเส็ทเข้าไปควบคุม เรียกใช้งาน คอมพิวเตอร์ Q-32 ในแคลิฟอร์เนีย เชื่อมต่อกันด้วยระบบเซอร์กิตสวิชชิ่ง (Circuit Switching) ผ่านสายโทรศัพท์ความเร็วต่ำ (dial-up telephone line) ซึ่งมีความเร็วไม่เพียงพอ ทำให้ต้องพัฒนาเทคโนโลยีใหม่ที่สำคัญยิ่งขึ้นมาทดแทน ช่วยให้คอมพิวเตอร์ต่างระบบคุยกันรู้เรื่อง คือ "แพ็คเก็จสวิชชิ่ง" (packet switching) หากเปรียบเทียบหลักการของแพ็คเก็จสวิชชิ่ง เหมือนกับการขนส่งจรวดสำรวจอวกาศขนาดใหญ่ (ซึ่งต้องใช้รถขนาดใหญ่ ขับเคลื่อนช้าอย่างระมัดระวัง ครอบครองถนนใหญ่ และถ้าหากกระทบกระเทือนมากๆ อาจทำให้จรวดพังต้องตั้งต้นส่งใหม่) แต่โดยวิธีการถอดแยกออกเป็นชิ้นส่วนเล็กๆ ใส่ซอง จ่าหน้าปลายทางผู้รับ ระบุต้นทาง ระบุลำดับการจัดเรียงเพื่อสะดวกในการประกอบกลับคืนแล้วส่งให้จักรยาน (ถ้าเป็นอินเตอร์เน็ตยุคสองก็เปรียบได้กับมอเตอร์ไซค์) หลายคัน ต่างวิ่งไปยังจุดหมาย ซึ่งปลายทางมีหน้าที่รวบรวม จัดลำดับ คืนรูป กลับสู่สภาพเดิม ทำให้ถนนเส้นเล็กสายเดียว สามารถใช้ส่งข้อมูลพร้อมกันได้หลายอย่างและถึงปลายทางได้หลายที่ ไม่ถูกจับจองใช้งานด้วยพาหนะใหญ่เพียงคันเดียว โปรโตคอลใหม่นี้สามารถส่งแพ็กเก็ตข้อมูล ผ่านทางสายโทรศัพท์ สายสัญญาณเช่า สัญญาณวิทยุ หรือส่งสัญญาณผ่านดาวเทียมก็ได้

ด้วยทุนสนับสนุนจากดาร์พาเน็ตให้กับบริษัทบีบีเอ็น (BBN: Bolt Beranek & Newman, Icn.) นำโดย บ็อบ คาห์น (Bob Kahn) ได้ติดต่อ วินท์ เซิร์ฟ (Vint Cerf) จากมหาวิทยาลัยสแตนฟอร์ดให้มาร่วมกันพัฒนา ได้ออกมาเป็น "รายงานของเซิร์ฟ/คาห์น" (Cerf/Kahn paper) เกี่ยวกับโปรโตคอล TCP พัฒนาต่อมาเรื่อยๆ และเปลี่ยนผู้ดูแลเป็น วินท์ เซิร์ฟ (Vint Cerf) จากสแตนฟอร์ด (Stanford) เรย์ ทอมลินสัน (Ray Tomlinson จาก BBN) และ ปีเตอร์ เคิร์ลสไตน์ (Peter Kirstein จาก UCL) จนได้มาเป็น TCP/IP (โดยถือเอาวันที่ 1 มกราคม 2526 (1983) เป็นวันสำคัญ ที่ทำการการโอนย้ายจากโปรโตคอล NCP มาเป็น TCP/IP)

ความแพร่หลายของระบบเครือข่ายท้องถิ่น หรือ LAN (Local Area Network) คอมพิวเตอร์ส่วนบุคคลและเวิร์กสเตชัน ส่งผลให้เกิดเทคโนโลยีอีเธอร์เน็ต (Ethernet technology) ในปี 2516 (1973) พัฒนาโดย บ็อบ เม็ทคาลเฟ (Bob Metcalfe) แห่ง ซีร็อกซ์ พาร์ก (Xerox PARC) ช่วยให้ระบบเครือข่ายขยายขนาดใหญ่มากขึ้น ซึ่งมีการแบ่งขนาดของระบบเป็นคลาส (Class) ต่างๆ และใช้ระบบหมายเลขไอพี (IP Address) แทนเครื่องคอมพิวเตอร์ เช่น 255.255.0.0 ซึ่งไม่เพียงพอ ทำให้เกิดการประดิษฐ์คิดค้นระบบชื่อโดเมน (DNS: Domain Name System) โดย พอล มอคคาเพทริส (Paul Mockapetris แห่ง USC/ISI) เช่น “www.cisco.com” จึงทำให้มีการพัฒนาอุปกรณ์ระบบเครือข่ายเพื่อรองรับการเติบโตของระบบอินเตอร์เน็ต

ในช่วงกลางทศวรรษ **1980** หรือประมาณปี พ.ศ.**2523** คณะวิจัยของกระทรวงกลาโหมสหรัฐอเมริกาได้เลิกสนับสนุน **ARPAnet** ระบบนี้จึงได้เปลี่ยนชื่อเป็นเอ็นเอสเอฟเน็ต **(NSFnet)** ต่อมาได้มีการรวมเอาระบบเครือข่ายอื่นเข้าด้วยกันซึ่งมีชื่อเรียกว่าระบบอินเตอร์เน็ต **(Internet)** ในระบบอินเตอร์สามารถนำระบบเครือข่ายที่มีรูปแบบต่างกันมาเชื่อมต่อเข้าด้วยกันโดยอาศัยเกตเวย์ **(Gateway)** จวบจนกระทั่งปี **2528 (1985)** ระบบอินเทอร์เน็ต ถือเป็นเทคโนโลยีที่ ฮอทฮิต สมบูรณ์พร้อมรองรับการใช้งานด้านการสื่อสาร แพร่ขยายไปในวงกว้าง ทั้งนักวิจัย นักพัฒนา และบุคคลทั่วไป ไม่จำกัดเฉพาะการทหารเท่านั้น โดยเฉพาะอย่างยิ่งการใช้งาน อีเมลล์ **(e-mail)** เวิร์ลวายด์เว็บ **(www)** แชท **(chat)** ฯลฯ ดังนั้นนับตั้งแต่ทศวรรษ **1990** ระบบอินเตอร์ได้มีการขยายการใช้งานอย่างรวดเร็ว และในปัจจุบันมีระบบเครือข่ายย่อยต่างๆในระบบอินเตอร์เน็ตประมาณ **10,000** ระบบเครือข่าย และมีผู้ใช้หลายล้านคนทั่วโลกในปัจจุบัน

สำหรับประเทศไทย อินเตอร์เน็ตเริ่มเข้ามามีบทบาทในช่วงปี พ.ศ. **2530 – 2535** ซึ่งช่วงนั้นเป็นเครือข่ายคอมพิวเตอร์ในระดับมหาวิทยาลัย **(Campus network)** ซึ่งการเชื่อมต่ออินเตอร์เน็ตทำได้สมบูรณ์ในปี พ.ศ. **2535** และได้มีการเปิดบริการอินเตอร์เน็ตเชิงพาณิชย์เป็นครั้งแรกในปี พ.ศ. **2538** ซึ่งในขณะนั้น **www** ในอเมริกากำลังได้รับความนิยมเป็นอย่างสูง คนทั่วไปเมื่อได้ยินคำว่า “อินเตอร์เน็ต” มักคิดถึงเว็บและอีเมล์เท่านั้น เนื่องจากเป็นรูปแบบที่เห็นบ่อยและใช้งานเป็นประจำ ความจริงการให้บริการที่เกี่ยวกับอินเตอร์เน็ตมีมากมาย สำหรับการจดทะเบียนและขอหมายเลข **IP** ในประเทศไทย ก็สามารถทำได้โดยตรงจาก **ISP (Internet Service Provider)** ที่ให้บริการอินเตอร์เน็ต โดย **ISP** จะกำหนดหมายเลข **IP** ให้ และมีการจัดตั้งบริษัทขึ้นมารับผิดชอบการจดทะเบียนชื่อโดเมน รูปที่ **12 – 1** แสดงให้เห็นเครือข่ายการเชื่อมโยงอินเตอร์เน็ตของประเทศไทย



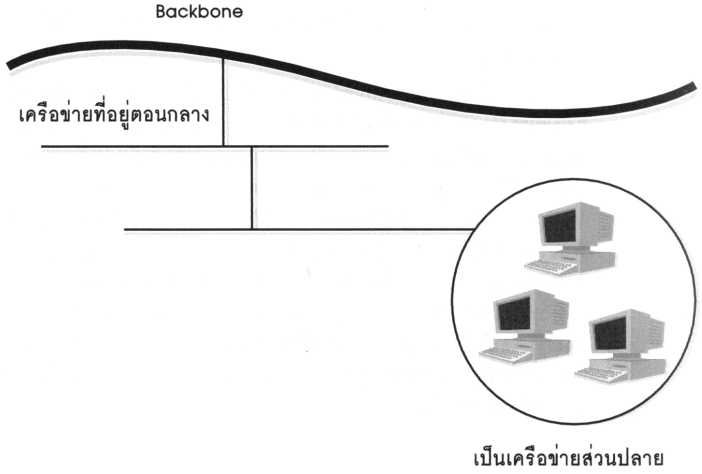
รูปที่ **12 – 1** การเชื่อมต่ออินเตอร์เน็ตในประเทศไทย

เมื่อระบบอินเตอร์เน็ตมีเครื่องคอมพิวเตอร์ต่างๆ เข้าร่วมในระบบมากขึ้น การใช้ **IP Address** ในการอ้างถึงเครื่องคอมพิวเตอร์ของแต่ละองค์กรกระทำได้ยากขึ้น เนื่องจากการกำหนดหมายเลขเครื่องคอมพิวเตอร์ในอินเตอร์เน็ตด้วยหมายเลข **IP** มีข้อเสียคือจำได้ยาก และทำให้สับสนได้ง่าย จึงได้มีการพัฒนาวิธีการอ้างอิงชื่อแทนหมายเลข **IP** เพื่อให้ใช้งานได้ง่าย ไม่สับสน ชื่อเหล่านี้เรียกว่า ชื่อโดเมน **(Domain Name)** โดยการใช้ **DNS (Domain Name Server)** หมายเลข **IP** ของ **Asia Access** เป็น **203.145.0.1** สามารถใช้โดเมนเป็น **asiaaccess.net.th** โดยที่เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็น **Domain Name Server** จะแปลงจากชื่อโดเมนเป็นหมายเลข **IP** อีกทีหนึ่ง สำหรับรูปแบบของโดเมนจะเป็นดังนี้ ชื่อโฮสต์คอมพิวเตอร์.ชื่อโดเมนย่อย[.ชื่อโดเมนย่อย].ชื่อโดเมนบนสุด เช่น **http://shop.microsoft.com** เป็นโดเมนย่อยของโดเมน **microsoft.com** เป็นต้น โดยที่ชื่อโดเมนแต่ละระดับจะคั่นด้วยเครื่องหมายจุด (.) สำหรับโดเมนบนสุดซึ่งอยู่ขวาสุดแบ่งออกเป็น 2 ประเภทคือ ชื่อโดเมนที่เป็นประเภทองค์กรในสหรัฐอเมริกา เช่น **www.midrospft.com** เป็นเว็บไซต์ของบริษัทไมโครซอฟต์ ซึ่งจะได้อธิบายรายละเอียดต่อไป

12.2 โครงสร้างของเครือข่ายอินเตอร์เน็ต (Structure of the Internet)

ดังที่ได้กล่าวถึงในตอนต้นแล้วว่าเครือข่ายอินเตอร์เน็ต คือระบบเครือข่ายสากล ที่เกิดจากการรวมระบบเครือข่ายขนาดเล็กให้สื่อสารและแลกเปลี่ยนข้อมูลซึ่งกันและกันได้ ในปัจจุบัน (ตั้งแต่ทศวรรษ **1990s**) เครือข่ายอินเตอร์เน็ตก็ยังคงเป็นเครือข่ายที่เปิดกว้างสู่สาธารณะอย่างแพร่หลายที่มีลักษณะของเทคโนโลยีระดับสูง บางทีอาจจะตั้งแต่มีเครื่อง **Apple II** และ **IBM PC** เป็นศูนย์กลางและเริ่มกระบวนการที่ทำให้ทั่วทั้งโลกมั่นใจว่าเทคโนโลยีที่เกี่ยวกับเครื่องคอมพิวเตอร์เป็นเรื่องปกติสำหรับผู้ที่ไม่ใช่ผู้เชี่ยวชาญทางด้านเทคนิคเกี่ยวกับเรื่องนี้

สำหรับคนส่วนใหญ่ เครือข่ายอินเตอร์เน็ต คือบางสิ่งที่คุณสามารถเชื่อมต่อเข้าไปได้ผ่านทางโมเด็ม และสายโทรศัพท์ หรือถ้าคุณโชคดีอาจจะติดต่อผ่านทางสาย **ISDN** หรือ **xDSL** ที่เร็วกว่า แต่อย่างไรก็ตามการเชื่อมต่อนี้ก็เป็นทุกสิ่งทุกอย่างที่ต้องการในการ **access** เข้าไปยังเครือข่ายอินเตอร์เน็ต หากไม่คำนึงถึงว่าระบบเครือข่ายได้รับการจัดตั้งอย่างซับซ้อน และถ้าคุณสามารถที่จะเห็นโครงสร้างของเครือข่ายอินเตอร์เน็ต จากจุดที่อยู่เหนือขึ้นไปบนอวกาศ คุณอาจจะเห็นว่าเครือข่ายอินเตอร์เน็ตเป็นการผสมกันของระบบเครือข่ายที่แตกต่างกันทั่วทั้งโลก ใน **network level** ดังแสดงตามรูปที่ **12 – 2**



รูปที่ **12 – 2** เครือข่ายอินเตอร์เน็ต คือการจัดเป็นลำดับชั้นของระบบเครือข่าย

ถ้าสามารถที่จะมองเข้าไปได้ใกล้ขึ้นอีก จะเห็นว่าใยแมงมุมที่สับสนนี้ประกอบด้วยเครื่องเซิร์ฟเวอร์ เกตเวย์ เราท์เตอร์ และสายสื่อสารเป็นจำนวนมากที่เชื่อมต่อสิ่งเหล่านี้เข้าด้วยกัน ซึ่งนั่นก็คือเครือข่ายอินเตอร์เน็ต ปรากฏการณ์การเติบโตของระบบเครือข่ายที่ไม่เคยเกิดขึ้นมาก่อนที่เริ่มเกิดขึ้นในกลางยุคปี **90s ...** ปรากฏการณ์ที่มีศักยภาพยิ่งใหญ่กว่าโทรทัศน์และที่ซึ่งแม้แต่ขณะนี้ก็มีการเชื่อมต่อเป็นจำนวนมาก ในความหมายของผู้ใช้ที่เข้ามามีส่วนร่วมในเครือข่ายอินเตอร์เน็ต (สร้างสำหรับใช้ทางวิชาการและทางทหาร) แต่ในปัจจุบันยังรักษาการให้บริการข่าวสารตามความต้องการของลูกข่ายที่เชื่อมต่อเข้ามาจากทุกหนทุกแห่ง

12.2.1 Regional and Other Networks

แน่นอนว่าโลกเป็นสถานที่ขนาดใหญ่ และพื้นที่ทางภูมิศาสตร์ก็มีบทบาทในการพิจารณาโครงสร้างของเครือข่ายอินเตอร์เน็ต ตัวอย่างเช่นในประเทศสหรัฐอเมริกา เครือข่ายอินเตอร์เน็ตสร้างขึ้นมาจากระบบเครือข่ายจำนวนมากตามภูมิภาคต่างๆ ที่ให้บริการในภาคตะวันออกเฉียงเหนือ ตะวันตกกลาง ตะวันตก ตะวันออก ตะวันออกเฉียงใต้ ตะวันตกเฉียงเหนือ และแคลิฟอเนียกลาง ทั้งหมดนี้คือระบบเครือข่ายตามภูมิภาค สำหรับการขนส่งข้อมูลสากลและประเทศสหรัฐอเมริกาฝั่งตะวันตก การเชื่อมต่อเข้ากับเครือข่ายอินเตอร์เน็ตขนาดใหญ่ ระบบเครือข่ายตามภูมิภาคเหล่านี้จะต่อเชื่อมเข้ากับ **backbone** ของชาติผ่านตำบลที่หลัก **4** แห่งที่เรียกว่า **network access point** หรือ **NAPs** ที่อยู่ใกล้เมืองใหญ่ๆ คือซานฟรานซิสโก วอชิงตัน ดี.ซี ชิคาโก และนิวยอร์ค

12.2.2 Internet Provider

ตอนนี้ก็มาถึงคำถามที่ว่า บุคคลทั่วไปจะเชื่อมต่อเข้าไปยังตลาดความคิดระดับจักรวาลนี้ได้อย่างไร คำตอบก็คือผ่านทางผู้ให้บริการการเชื่อมต่อเครือข่ายอินเตอร์เน็ต หรือ **ISP (Internet Service Provider)** หรือผู้จัดหาบริการในระบบออนไลน์ เช่น **Microsoft Network (MSN)** หรือ **America Online (AOL)** ซึ่งทั้ง **ISP** และการให้บริการในระบบออนไลน์เป็นเหมือนผู้จำหน่ายที่จัดให้มีเส้นทางเชื่อมต่อไปยังระบบเครือข่ายตามภูมิภาค ซึ่งเชื่อมต่ออยู่กับ **Internet backbone** เมื่อจัดตั้งเป็นกลุ่ม **Provider** เหล่านี้จึงเป็นธุรกิจที่มีอุปกรณ์และเทคโนโลยีตามความต้องการ ในการจัดให้มีการ **access** เครือข่ายอินเตอร์เน็ตด้วยความเร็วสูงผ่านทางสายสื่อสาร เช่น **T1** โดยบาง **Provider** ก็จะเป็นบริษัทในระดับนานาชาติ เช่น **MCI** และ **AOL** หรือเป็นองค์กรขนาดเล็กที่จัดให้มีการ **access** จากบางเมืองหรือครอบคลุมพื้นที่ทางภูมิศาสตร์ขนาดเล็ก

12.2.3 Internet and Web Commonality

ถึงแม้ว่าเครือข่ายอินเตอร์เน็ตจะอยู่บนพื้นฐานของการส่งข้อมูลที่เป็นข้อความ (**text**) และ **World Wide Web** จะเป็นกราฟฟิก แต่เว็บ (**Web**) ก็เป็นส่วนหนึ่งของเครือข่ายอินเตอร์เน็ต ซึ่งเป็นส่วนที่ได้รับความนิยมจากธุรกิจขนาดเล็ก ความร่วมมือระหว่างประเทศ วงการโทรทัศน์ สื่อข่าวสาร และแม้แต่จัดให้มีฮาร์ดแวร์ และซอฟต์แวร์ สำหรับ **access** เครือข่ายอินเตอร์เน็ต โดยมีเว็บเป็นส่วนหนึ่งของเครือข่ายอินเตอร์เน็ตที่กำหนดคุณสมบัติโดยการมีรูปภาพสวยๆ สัญญาณภาพ สัญญาณเสียง ภาพการ์ตูน และป้ายโฆษณาที่เรียกร้องให้ "**click me**" ที่ทำเป็นรายการให้เลือกแบบสะท้อนไปมา กระโดด บิน หรือเลื่อนไหลผ่านจอภาพ เว็บจึงเป็นที่รวบรวมของเอกสารไฮเปอร์ลิงค์ที่สร้างเป็นส่วนหนึ่งของเครือข่ายอินเตอร์เน็ตทั่วโลก สิ่งที่เว็บและอินเตอร์เน็ตจะต้องมีเหมือนกัน อย่างน้อย **2 – 3** สิ่ง คือการเริ่มต้นด้วยวิธีการจัดการและการตั้งชื่อของเครือข่ายอินเตอร์เน็ตและเว็บ

12.3 โดเมน (Domains)

นอกเหนือจากโครงสร้างทางกายภาพและการตั้งชื่อแล้ว เครือข่ายอินเตอร์เน็ตยังสร้างขึ้นจากแนวความคิดเรื่องโดเมน โดยสร้างโดเมนเหล่านี้ขึ้นอย่างมีแบบแผน และการจัดการโดเมนก็มีการออกแบบให้เป็นวิธีสำหรับรักษาการจัดลำดับเพื่อไม่ให้เกิดความสับสนในโลก และช่วยให้เครือข่ายอินเตอร์เน็ตเติบโตตามลำดับอย่างต่อเนื่อง

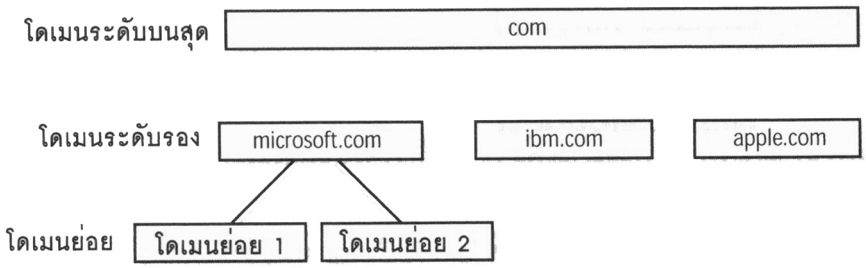
12.3.1 ระบบชื่อโดเมน (The domain name system)

ค่อนข้างจะเหมือนกับชื่อที่ใช้ในการระบุชื่อต้นไม้และสัตว์ (ตัวอย่างเช่น **mamal/big cat/lion**) โดยที่โดเมนบนเครือข่ายอินเตอร์เน็ตที่ช่วยในระบบการจัดแบ่งออกเป็นหมวดหมู่ เรียกว่า **Domain Name System (DNS)** ที่ระบุไซต์ซึ่งเป็นเอกลักษณ์ โดยพื้นฐานของการจัดลำดับชั้นแบบต้นไม้ (**Tree-like hierarchy**) ที่ประกอบด้วย **top-level domain, second-level domain,** และ **subdomains** ต่อลงไปอีก **1** ชั้นหรือมากกว่า

DNS site name จะมีลักษณะ เช่น **microsoft.com** เมื่อ

- **com** แสดงให้ทราบว่าเป็น **top-level domain**
- **microsoft** แสดงให้ทราบว่าเป็น **second-level domain** ในที่นี้คือชื่อของธุรกิจที่คุ้นเคย
- **a period** (เครื่องหมายจุด อ่านว่า **dot**) จะเป็นตัวแยก **top-level domain** และ **second-level domain** ออกจากกัน

แต่เนื่องจาก **DNS** ตั้งอยู่บนพื้นฐานการจัดในลักษณะของทรี (**Tree**) ดังนั้นโดเมนในระดับหนึ่งจะสามารถเป็น **parent** ให้กับอีกหลายโดเมนที่อยู่ในระดับต่ำลงไป ดังแสดงรูปที่ **12 – 3**

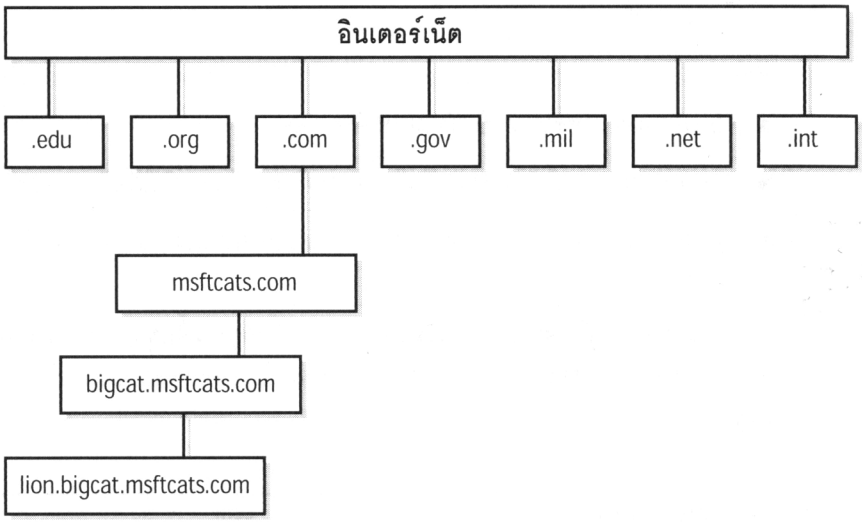


รูปที่ **12 – 3** ระบบชื่อโดเมน (**Domain Name System**)

ระบบชื่อโดเมนที่กล่าวข้างต้น อาจจะขยายออกไปเป็นโดเมนย่อย (**Subdomains**) จำนวนมากอยู่ภายในไซต์ และก็เป็นไปได้ที่จะเป็นชื่อของคอมพิวเตอร์แม่ข่ายภายในโดเมนย่อยนั้นๆ หากจินตนาการตามตัวอย่าง นี่คือ ชื่อที่เป็นตัวแทนของโดเมนย่อย **2** ชื่อที่แตกต่างกัน แสดงให้ทราบว่าเป็นเครื่องเซิร์ฟเวอร์คนละเครื่องกัน เช่น **lion.bigcat.msftcats.com** และ **tabby.smallcat.msftcats.com**

- **msftcats.com** เป็นตัวแทนของชื่อใน **second-level** และ **top-level domain**
- **bigcat** และ **smallcat** เป็นตัวแทนของโดเมนย่อยที่แตกต่างกันภายในไซต์
- **lion** และ **tabby** เป็นชื่อของเครื่องเซิร์ฟเวอร์คนละเครื่องกันภายในโดเมนย่อย

อย่างไรก็ตามให้สังเกตว่า ถึงแม้จะอ่านชื่อโดเมนจากซ้ายไปขวา แต่ชื่อจะถูกแยกออกจากขวาไปซ้าย เริ่มจากโดเมนในระดับสูงที่สุดจะอยู่ทางขวาสุด



รูปที่ 12 – 4 Internet Domain

12.3.2 Top-level Internet domains

คำว่าโดเมน อาจจะนำให้คิดไปว่าเป็นคำที่มีความหมายเหมือนกับ ราชอาณาจักร (kingdom) หรือ อาณาจักร (realm) ซึ่งที่จริงแล้วโดเมนบนเครือข่ายอินเตอร์เน็ตก็คือบางสิ่งที่มีลักษณะคล้ายกับอาณาจักรแบบเสมือน หากไม่คำนึงถึงกฎการมีผู้นำที่แตกต่างกัน ก็จะรู้สึกว่าเป็นการรวบรวมบางสิ่งที่สมาชิกทั้งหมดมีเหมือนกัน สำหรับโดเมนในระดับสูงสุด (top-level domain) คำว่าบางสิ่งนี้อาจหมายถึงพื้นที่ทางภูมิศาสตร์หรือประเภทขององค์กร

กลุ่มของโดเมนไซต์ที่จัดแบ่งตามสภาพภูมิศาสตร์ ถูกจัดตั้งขึ้นโดยแต่ละประเทศจะได้รับการระบุด้วยตัวอักษร 2 ตัวเป็นตัวย่อของชื่อประเทศ ตัวอย่างเช่น

- **.fr** สำหรับประเทศฝรั่งเศส
- **.de** สำหรับประเทศเยอรมัน
- **.ca** สำหรับประเทศแคนาดา
- **.es** สำหรับประเทศสเปน
- **.ar** สำหรับประเทศอาร์เจนตินา
- **.jp** สำหรับประเทศญี่ปุ่น
- **.za** สำหรับประเทศแอฟริกา
- **.us** สำหรับประเทศสหรัฐอเมริกา

จากรูปที่ 12 – 4 จะเห็นได้ว่าภายในโดเมนไซต์ จะมีการจัดแบ่งโดเมนย่อยตามประเภทขององค์กร โดยใช้ตัวอักษรย่อ 3 ตัว ที่คุ้นเคยสำหรับผู้ใช้เครือข่ายอินเตอร์เน็ต ดังนี้

- **.com** สำหรับบริษัททางการค้า
- **.org** สำหรับองค์กรที่ไม่ทำการค้า
- **.gov** สำหรับรัฐบาลประเทศสหรัฐอเมริกา
- **.net** สำหรับกลุ่มผู้ให้บริการเกี่ยวกับระบบเครือข่าย
- **.edu** สำหรับสถานศึกษา

- **.mil** สำหรับหน่วยงานทางทหารของสหรัฐ
- **.int** สำหรับองค์กรระหว่างประเทศ

และภายในโดเมนเหล่านี้ยังมีไซต์ย่อยต่างๆ เป็นลำดับลงไปอีกจำนวนมาก (เทียบได้กับแผงลอยในตลาดซึ่งใหญ่ที่สุดในโลก) ซึ่งถูกสร้างขึ้น เป็นเจ้าของ และบำรุงรักษาโดยบุคคลใดบุคคลหนึ่งและองค์กร ที่มีความต้องการจะประกาศตัวเอง เสนอผลิตภัณฑ์ของตนเอง บอกความสนใจของตนเอง และแม้แต่หลักปรัชญาของตนเองให้กับผู้ที่อยากจะค้นหาและเข้ามาเยี่ยมชม (บางไซต์เป็นตัวเลือกที่ผู้เข้าเยี่ยมชมอาจจะต้องสมัครเป็นสมาชิกและเป็นไปได้ที่จะต้องชำระค่าบริการ แต่โดยมากจะฟรี)

12.3.3 ฐานข้อมูล DNS และ IP Address (DNS Database and IP Address)

ในส่วนก่อนหน้านี้ได้อธิบาย **DNS** ในเรื่องเกี่ยวกับการตั้งชื่อให้กับไซต์บนเครือข่ายอินเตอร์เน็ต เนื่องจากเป็นชื่อที่พบได้บ่อยในการโฆษณา (เช่น "**come visit our Web site at www.microsoft.com**") และเป็นชื่อที่จะพิมพ์ลงไปที่ **address bar** ของโปรแกรมเบราส์เซอร์เมื่อใดก็ตามที่คุณต้องการเข้าไปเยี่ยมชมไซต์นั้นๆ

อย่างไรก็ตาม ก็เป็นสิ่งสำคัญที่จะต้องทราบว่า **DNS** ยังคงอ้างถึงฐานข้อมูลที่กระจายอยู่ท่ามกลางเครื่อง **DNS name servers** ต่างๆ เพื่อให้เข้าใจว่าทำไมเรื่องนี้ถึงเป็นสิ่งสำคัญ เริ่มจากการคิดว่าเครื่องคอมพิวเตอร์จะสามารถติดต่อซึ่งกันและกันบนเครือข่ายอินเตอร์เน็ตได้อย่างไร เมื่อคุณพิมพ์ www.microsoft.com เพื่อที่จะเข้าไปเยี่ยมชมเว็บไซต์ ของบริษัทไมโครซอฟต์ คุณคิดว่าเครื่องคอมพิวเตอร์จะส่งข้อความนี้ออกไปเพื่อหวังว่าเครื่องคอมพิวเตอร์ที่มีชื่อว่า www.microsoft.com จะตอบกลับมาหรือไม่ ความจริงไม่ได้เป็นอย่างที่คุณคิด

สิ่งที่เครื่องคอมพิวเตอร์ทำก็คือจะใช้ **IP (Internet Protocol) Address** ของ **Microsoft.com** ในการสื่อสาร โดยแอดเดรสที่กล่าวถึงนี้จะเป็นตัวเลขทั้งหมด ถึงแม้ว่าจะมีการใช้เครื่องหมายจุด (**dot**) เหมือนกับชื่อที่เป็นข้อความ แต่ก็จะมีลักษณะดังนี้ **207.46.130.149** ซึ่งแอดเดรสในลักษณะนี้จะถูกกำหนดอย่างเคร่งครัดในลักษณะไบต์ต่อไบต์ และมีชื่อเรียกทางเทคนิคว่า "**dotted octet format**" ซึ่งเป็นเพียงชื่อเดียวที่เครื่องคอมพิวเตอร์ใช้ในการจำแนกเครื่องคอมพิวเตอร์เครื่องอื่นบนเครือข่ายอินเตอร์เน็ต

อย่างไรก็ตาม จะมีเพียงไม่กี่คนที่จะสามารถจำตัวเลขที่มีความยาวขนาดนั้นได้ ซึ่งจะต้องใช้ความทรงจำเป็นอย่างมาก ดังนั้นจึงมี **DNS** และฐานข้อมูลของ **DNS** ขึ้นมาช่วยเหลือ โดยฐานข้อมูล **DNS** จะจับคู่ระหว่างชื่อที่มีความคุ้นเคยจดจำได้ง่ายเข้ากับ **IP Address** คล้ายกับสมุดโทรศัพท์ที่จับคู่ชื่อบุคคลต่างๆ กับหมายเลขโทรศัพท์ ด้วยวิธีนี้ระบบฐานข้อมูลของ **DNS** จึงทำให้มั่นใจว่ามนุษย์สามารถที่จะใช้คำที่คุ้นเคยดี ส่วนเครื่องคอมพิวเตอร์ก็สามารถใช้หมายเลขที่เครื่องคอมพิวเตอร์คุ้นเคยได้ ในขณะที่ยังรับรองว่าไซต์ที่ร้องขอจะเป็นไซต์เดียวกันกับไซต์ที่เครื่องคอมพิวเตอร์ติดต่อไป

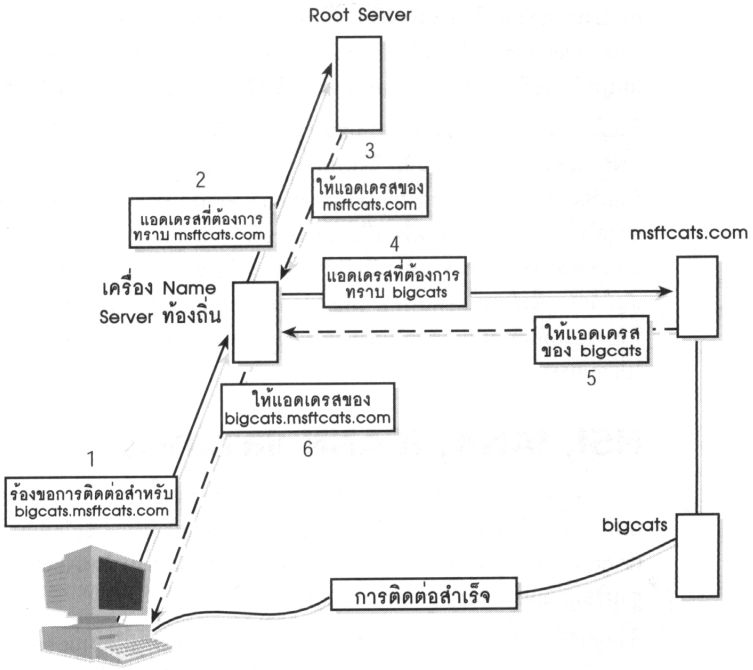
12.3.4 Root servers

ดังที่ทราบดีอยู่แล้วว่างานที่ทำโดยเครื่องโดเมนเนมเซิร์ฟเวอร์ (**domain name servers**) เป็นงานวิกฤติ นับตั้งแต่การเปลี่ยนประเภทของแอดเดรสให้เป็นหมายเลข **IP Address** อย่างไรก็ตามเครื่องเซิร์ฟเวอร์นี้ก็ไม่ใช่เครื่องที่มีขนาดใหญ่มากเพียงเครื่องเดียวที่ตั้งอยู่บางแห่งข้างนอก ที่ทำการตรวจสอบเครื่องคอมพิวเตอร์ทั้งหมดบนเครือข่ายอินเตอร์ และทำการจับคู่เครื่องไคลเอนต์ (เครื่องคอมพิวเตอร์ที่ทำการเยี่ยมเยียน) กับเครื่องเซิร์ฟเวอร์

(Internet Site) เหมือนการให้บริการจับคู่ทางดิจิตอล การจัดลำดับในเครือข่ายอินเตอร์เน็ต ประกอบด้วยโดเมนในระดับต่างๆ เครื่องโดเมนเนมเซิร์ฟเวอร์ก็จะทำการจับคู่ในแต่ละระดับด้วย และเครื่องโดเมนเนมเซิร์ฟเวอร์ในระดับที่กำหนดให้ก็จะมีอำนาจในการพิจารณาเพียงชื่อและแอดเดรสในระดับนั้น เช่น ในระดับสูงที่สุดที่มีลักษณะตรงกับ **top-level domain (com, org, net** และอื่นๆ) เครื่องโดเมนเนมเซิร์ฟเวอร์สำหรับโดเมนระดับสูงสุดเรียกว่า **"root server"** ซึ่งจะบรรจุข้อมูลที่ต้องการสำหรับการกำหนดที่อยู่ของ **microsoft.com** และนั่นคือทั้งหมดที่เครื่อง **root server** จะต้องทำ และเครื่องนี้จะไม่สนใจโดเมนย่อยในระดับที่ต่ำลงไปที่อยู่ภายใน **microsoft.com** งานที่ว่านี้จะเป็นของเครื่องเซิร์ฟเวอร์ในระดับต่ำกว่าที่บรรจุข้อมูลเกี่ยวกับโดเมนย่อย และย่อยต่อๆ ไป ด้วยความรู้สึกนี้คุณอาจจะคิดเกี่ยวกับกระบวนการในการส่งหน้าที่ต่อจากระดับหนึ่งลงไปยังระดับถัดไปยังเครื่องคอมพิวเตอร์ที่เทียบเท่ากับเป็นการลดภาระทางเศรษฐกิจอย่างช้าๆ

12.3.5 สร้างการเชื่อมต่อ (Making connections)

เมื่อมีโดเมนระดับสูงสุด โดเมนย่อย เครื่องโดเมนเนมเซิร์ฟเวอร์ และแอดเดรส ตลอดจนชื่อของไซต์จนถึง **IP address** แล้วเครื่องคอมพิวเตอร์ **A** จะติดต่อไปยังไซต์ **B (bigcat.msftcat.com)** ได้อย่างไรแน่? ในเมื่อทั้งคู่เป็นเหมือนคนแปลกหน้าต่อกันและกัน และต่อไปคือสิ่งที่จะเกิดขึ้น



รูปที่ **12 – 5** การติดต่อไซต์บนเครือข่ายอินเตอร์เน็ต

1. เริ่มแรก เครื่องคอมพิวเตอร์ **A** จะติดต่อเข้าไปยังเครื่อง **DNS name server** ในท้องถิ่น โดยบอกว่า **"ฉันต้องการที่จะติดต่อไปยัง Site B"**
2. ถ้าเครื่อง **DNS name server** ในท้องถิ่น รู้ว่าจะทำอย่างไร ก็จะโต้ตอบโดยการส่งแอดเดรสของ **Site B** กลับมายังเครื่องคอมพิวเตอร์ **A** แต่ถ้าเครื่อง **DNS name server** ในท้องถิ่น ไม่รู้แอดเดรส ก็จะทำการส่งต่อคำร้องขอนั้นไปยังเครื่อง **Root server** แต่จะรู้ได้อย่างไรว่าเครื่อง **root server** ใดที่ต้องการจะติดต่อด้วย

3. ถึงแม้ว่าเครื่อง **root server** จะไม่สามารถวิเคราะห์แอดเดรสทั้งหมดสำหรับ **Site B** ได้ แต่ก็จะให้ข้อมูลกับเครื่อง **DNS name server** ในท้องถิ่นว่าจะต้องติดต่อไปยัง **msftcats.com**
4. ด้วยข้อมูลนี้เครื่อง **DNS name server** ในท้องถิ่นก็จะติดต่อไปยัง **maftcats.com** ซึ่งสามารถที่จะให้แอดเดรสของ **bigcat.msftcats.com** ได้อย่างสมบูรณ์

กระบวนการค้นหาชื่อทั้งหมดนี้เรียกว่า **iterative query** เพราะว่าการร้องขอจะถูกส่งไปซ้ำแล้วซ้ำเล่าผ่านเครื่องเนมเซิร์ฟเวอร์ตามลำดับชั้นจนกระทั่งทราบแอดเดรสอย่างสมบูรณ์ ถึงแม้ว่ากระบวนการนี้จะฟังดูเหมือนน่าเบื่อและสิ้นเปลืองเวลา แต่ก็มีวิธีการ 2 วิธีซึ่งระบบชื่อโดเมนใช้ในการทำให้เร็วขึ้น วิธีแรกคือการทำสำเนาฐานข้อมูลของโดเมนในระดับสูงสุดไปไว้ยังเครื่อง **root server** หลายๆ เครื่องตามสถานที่ต่างๆ ทั่วโลก เพื่อที่การค้นหาโดเมนในระดับสูงที่สุดจะได้ไม่เป็นหน้าที่ของเครื่องเพียง **1 – 2** เครื่อง และวิธีที่สองคือให้เครื่องเซิร์ฟเวอร์ในทุกระดับมีการเก็บแอดเดรสที่ได้เคยค้นพบแล้วไว้ด้วย เมื่อมีคำร้องขอไปยังที่ใดๆ เครื่องเซิร์ฟเวอร์เหล่านี้ก็จะตรวจสอบกับข้อมูลที่เก็บไว้ก่อน ซึ่งถ้าพบแอดเดรสตามที่ต้องการก็จะส่งแอดเดรสนั้นกลับไปยังเครื่องคอมพิวเตอร์ที่ร้องขอในทันทีทันใด แต่ถ้าไม่สามารถหาแอดเดรสจากที่เก็บไว้ได้พบ ก็จะต้องส่งการร้องขอไปผ่านกระบวนการตามขั้นตอนต่อไป

12.3.6 NSI, IANA, ICANN และอนาคต

การที่ **DNS (Domain Name System)** ต้องเกี่ยวข้องกับการทำงานอย่างหนักในการติดตามและการเก็บบันทึกเพื่อทำให้มั่นใจว่าจะไม่มีชื่อของไซต์ที่ซ้ำกัน และรักษาให้ชื่อไซต์กับ **IP Address** เข้าคู่กันได้อย่างถูกต้อง และไซต์ที่เพิ่มเข้ามาใหม่รวมทั้ง **IP Address** จะได้รับการเพิ่มเข้าไปในฐานข้อมูลที่เหมาะสม แล้วใครจะเป็นผู้ทำสิ่งนี้? คำตอบก็คือ ... เป็นความรับผิดชอบขององค์กรเองในการเฝ้าติดตามโดเมนย่อย โฮส กลุ่มย่อยหรือโซน **(zones)** ของตนเองโดยกำหนดความรับผิดชอบในการบริหารจัดการหรือตามอำนาจหน้าที่

สำหรับโดเมนในระดับสูงสุดนั้น หน้าที่ในการจดทะเบียนชื่อใน **com, net** และ **org** จนถึงปัจจุบันเป็นหน้าที่ขององค์กรภาคธุรกิจชื่อว่า **Network Solution Inc (NSI)** สำหรับหน้าที่ในการกำหนด **IP Address** จะทำโดยกลุ่มที่เรียกว่า **IANA (Internet Assigned Numbers Authority)** ซึ่งตั้งอยู่ที่ **University of Southern California** และทั้ง 2 กลุ่มนี้ทำงานภายใต้สัญญากับรัฐบาลของประเทศสหรัฐอเมริกา

อย่างไรก็ตามในปี **1998** หลังจากที่กระทรวงพาณิชย์ของสหรัฐอเมริกาได้พิจารณาทบทวนและในบางครั้งก็มีการถกเถียง ในที่สุดจึงมีข้อตกลงในการมอบหน้าที่รับผิดชอบเหล่านี้ให้กับหน่วยงานใหม่ที่เรียกว่า **ICANN (Internet Corporation for Assigned Names and Numbers)** ดังนั้นในต้นปี **1999 ICANN** จึงอยู่ในกระบวนการพัฒนาองค์กรภายใต้การควบคุมของคณะกรรมการของผู้บริหารจำนวน **19** คน

12.4 Organizations and Standards Groups

นอกเหนือจาก **IANA** (ปัจจุบันคือ **ICANN**) ยังมีองค์กรอีกเป็นจำนวนมากที่มีส่วนเกี่ยวข้องในด้านต่างๆ ของเครือข่ายอินเตอร์เน็ต บางองค์กรก็เกี่ยวข้องกับเทคโนโลยีชั้นสูงที่คำนึงถึงการพัฒนาและรักษามาตรฐานของเครือข่ายอินเตอร์เน็ต บางองค์กรก็คำนึงถึงเรื่องที่มีความสัมพันธ์กับเครือข่ายอินเตอร์เน็ต เช่นความปลอดภัย ความเป็นส่วนตัว และในกรณีของ **EFF (Electronic Frontier Foundation)** การรักษาความเป็นอิสระและการใช้

คำพูดอย่างอิสระสำหรับผู้ใช้เครือข่ายอินเตอร์เน็ต องค์กรทางด้านเทคนิคที่ถูกกล่าวถึงในเรื่องของเครือข่ายอินเตอร์เน็ตในระดับโลกซึ่งเติบโตและมีวิวัฒนาการไปอย่างต่อเนื่อง มีดังต่อไปนี้

12.4.1 Internet Society (ISOC)

ISOC เป็นองค์กรซึ่งรวบรวมสมาชิกที่ไม่ได้ทำผลกำไร ตั้งอยู่ในเมือง **Reston** รัฐ **Virginia** และมีสมาชิกจากทั่วโลก โดยมีวัตถุประสงค์ในเรื่องมาตรฐาน การศึกษา และการกำหนดนโยบายที่มีผลกระทบต่อเครือข่ายอินเตอร์เน็ต ดังที่ได้อธิบายไว้ใน **Home Page** ขององค์กร (www.isoc.org)

12.4.2 Internet Architecture Board (IAB)

IAB เป็นกลุ่มที่ให้คำปรึกษากับ **ISOC** ที่เกี่ยวข้องในด้านต่างๆ ของเครือข่ายอินเตอร์เน็ต งานส่วนหนึ่งขององค์กรนี้ก็คือ ให้คำแนะนำทางด้านเทคนิคกับ **ISOC** และกลุ่มนี้ยังตรวจตราโครงสร้างของโปรโตคอล **IP** และวิธีการปฏิบัติ ควบคุมกระบวนการมาตรฐาน และเป็นตัวแทน **ISOC** ในการต่อรองกับองค์กรอื่นในเรื่องที่เกี่ยวข้องกับมาตรฐานของเครือข่ายอินเตอร์เน็ต

12.4.3 Internet Engineering Task Force (IETF)

IETF เป็นองค์กรเฉพาะที่สนใจในวิวัฒนาการและปฏิบัติการของเครือข่ายอินเตอร์เน็ต งานของ **IETF** คือสนับสนุนกลุ่มคณะทำงานต่างๆ ที่เกี่ยวข้องกับเรื่องต่างๆ โดยเฉพาะเช่น การกำหนดเส้นทางการขนส่งข้อมูล การปฏิบัติและการบริหารจัดการ การให้บริการผู้ใช้ และการรักษาความปลอดภัย **IETF** เปิดกว้างสำหรับสมาชิกใหม่จากทั่วโลก และได้รับการตรวจสอบโดย **IESG (Internet Engineering Steering Group)** ซึ่งส่วนหนึ่งของ **ISOC** ที่ทำหน้าที่เป็นผู้ให้คำแนะนำ

12.4.4 Internet Research Task Force (IRTF)

IRTF เป็นกลุ่มอาสาสมัครที่รวมเป็นองค์ประกอบของ **IETF** ที่มีวัตถุประสงค์ในการทำวิจัยโครงการที่เกี่ยวข้องกับเครือข่ายอินเตอร์เน็ตในระยะยาว เช่น ในเรื่องความเป็นส่วนตัวในการใช้ **e-mail** โดย **ITRF** จะได้รับการควบคุมโดย **IRSG (Internet Research Steering Group)** ซึ่งเป็นส่วนหนึ่งของ **ISOC**

12.4.5 World Wide Web Consortium (W3C)

W3C จะสนใจในเรื่อง **World Wide Web** เพียงเรื่องเดียว โดยเฉพาะอย่างยิ่งในเรื่องของมาตรฐานและโปรโตคอลที่ได้รับการออกแบบเพื่อสนับสนุนการเติบโตของเครือข่ายอินเตอร์เน็ตและความสามารถในการปฏิบัติงานร่วมกันได้ของเว็บไซต์ต่างๆ นอกจากนั้น **W3C** ยังเป็นหน่วยงานกำหนดมาตรฐานในข่าวทางด้านเทคนิคซึ่งเทคโนโลยีที่ได้รับการพัฒนาจะต้องเสนอให้พิจารณาและให้การรับรอง แม้ว่าองค์กรนี้จะมีอายุน้อย (จัดตั้งในปี **1994**) แต่ก็สามารถอวดอ้างกับสมาชิกนานาประเทศได้และมีอิทธิพลในการพัฒนา และกำหนดมาตรฐานให้กับเว็บ

12.5 การเชื่อมต่อเครือข่ายอินเตอร์เน็ต (Internet Connection)

โดยไม่คำนึงถึงขนาดของขอบเขตที่ใหญ่มาก และความเร็วของเราท์เตอร์ และส่วนประกอบอื่นของโครงสร้างพื้นฐาน เครือข่ายอินเตอร์เน็ตคือสิ่งที่มีความสำคัญ การหมุนโทรศัพท์เชื่อมต่อเข้าไปยังระบบเครือข่ายคือการที่ผู้ใช้ไม่ได้ทำการเชื่อมต่อตามปกติผ่านสายสื่อสาร **ISDN** สายเคเบิล โมเด็ม หรือเทคโนโลยีความเร็วสูงอย่างอื่น พวกเขาเหล่านั้นใช้บริการเครือข่ายระบบโทรศัพท์ที่เก่าแก่

อย่างไรก็ตามเมื่อเครือข่ายอินเตอร์เน็ตเป็นจุดสำคัญ จึงต้องการใช้บริการระบบโทรศัพท์ที่ใช้เสียงนี้ในการส่งสัญญาณข้อมูลแบบอนุกรมและทำให้เกิดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ และเครื่องคอมพิวเตอร์เองก็ต้องมีขีดความสามารถในการจัดตั้งการสนทนาและทำให้การสนทนาสิ้นสุดเมื่อเห็นพ้องกับการสร้างเฟรมข้อมูล การควบคุมความผิดพลาด และความแน่นอนในการสื่อสารอย่างอื่นที่เกิดขึ้นใน **data link layer** ทางออกที่ถูกใช้ระหว่างการสนทนาคือโปรโตคอล **IP** แบบใดแบบหนึ่งใน **3** แบบนี้ คือ **PPP, SLIP** และ **CSLIP**

12.5.1 PPP (Point-to-Point Protocol)

PPP เป็นหนึ่งในโปรโตคอลที่ถูกนำมาใช้โดย **ISPs** ส่วนมาก เนื่องจากเป็นโปรโตคอลซึ่งใหม่ที่สุดและเร็วที่สุด และเป็นมาตรฐานของเครือข่ายอินเตอร์เน็ต เนื่องจาก **PPP** สามารถสนับสนุนโปรโตคอลได้หลายแบบรวมทั้ง **TCP/IP, IPX, AppleTalk** และอื่นๆ จึงเป็นวิธีการที่มีความอ่อนตัวในการทำให้เครื่องคอมพิวเตอร์มีการสื่อสาร ซึ่ง **PPP** อยู่บนพื้นฐานขององค์ประกอบ **2** อย่าง คือ

- **Link Control Protocol (LCP)** ซึ่งใช้ในการจัดตั้ง ทดสอบ เจรจา และทำให้สิ้นสุดสำหรับการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์กับเครื่องคอมพิวเตอร์
- **Network Control Protocol (NCP)** ซึ่งใช้ในการเจรจาและจัดตั้งรายละเอียดให้กับโปรโตคอลที่จะใช้ในระหว่างการส่งสัญญาณข้อมูล

สิ่งสำคัญที่สุด คือในการเชื่อมต่อ **PPP** กับเครือข่ายอินเตอร์เน็ตนั้น ส่วนต่างๆ จะรวมกันได้อย่างพอดีได้อย่างไร? ขั้นตอนต่างๆ ต่อไปนี้จะอธิบายการทำงานในการเชื่อมต่อเครือข่ายอินเตอร์เน็ต

1. ขั้นแรก เครื่อง **PC** ใช้โมเด็มเรียกไปยัง **ISP** ของผู้ใช้
2. จากนั้นก็เป็นหน้าที่ของ **LCP** ในขั้นตอนนี้ของการเชื่อมต่อ **LCP** จะจัดตั้งการเชื่อมต่อเข้ากับอุปกรณ์ของ **ISP** ทดสอบการต่อเชื่อม เจรจาข้อตกลง เช่นประเภทของเฟรมข้อมูลและขนาดของแพ็กเก็ตที่จะใช้สำหรับการสื่อสาร
3. ต่อไป **NCP** ก็จะถูกใช้ในการตั้งค่าคุณลักษณะเฉพาะของโปรโตคอลสำหรับใช้ในขณะที่ทำการสนทนา เช่น ณ จุดนี้จะมีการเชื่อมต่อจำนวนมากที่เรียกมายังเครื่องคอมพิวเตอร์แบบ **dynamic** ผ่านทาง **NCP** โดยการกำหนด **IP Address** ชั่วคราวให้ เพื่อทำให้เครื่องคอมพิวเตอร์เรียกใช้ **TCP/IP protocol stack** (เนื่องจาก **PPP** สนับสนุน **dynamic allocation** สำหรับ **IP addresses**)
4. ถึงตอนนี้ การเตรียมการก็เสร็จสิ้นอย่างสมบูรณ์ การส่งสัญญาณข้อมูลก็จะเริ่มขึ้น
5. เมื่อถึงเวลาที่จะสิ้นสุดการสนทนา **NCP** ก็จะเริ่มทำงานอีกครั้งเพื่อถอดถอนการเชื่อมต่อใน **network layer**
6. และสุดท้าย **LCP** ก็จะรับหน้าที่ในการดำเนินการยุติการเชื่อมต่ออย่างนิ่มนวล

นอกเหนือจากทั้งหมดที่กล่าวมาแล้ว **PPP** ยังสนับสนุนวิธีในการรับรองว่าผู้ใช้เป็นของแท้ อีก **2** วิธี คือ **PAP (Password Authentication Protocol)** และ **CHAP (Challenge-Hand-shake Authentication Protocol)** ซึ่งจัดให้มีการวัดระดับของความปลอดภัยว่าเครื่องคอมพิวเตอร์ที่ติดต่อสื่อสารเข้ามาสามารถถูกตรวจสอบได้ว่าคือใคร และที่จริงแล้วใครคือผู้ที่บอกว่าคือพวกเขาเหล่านั้น

12.5.2 SLIP (Serial Line Internet Protocol)

SLIP เป็นวิธีเก่าแก่ที่ใช้ในการทำให้เครื่องคอมพิวเตอร์สื่อสารผ่านสายสื่อสารแบบอนุกรม **SLIP** เริ่มมีการใช้อย่างแพร่หลายสำหรับการเชื่อมต่อเครือข่ายอินเตอร์เน็ต **SLIP** แตกต่างจาก **PPP** ที่ว่า **SLIP** จะสนับสนุน **TCP/IP** เพียงอย่างเดียว แต่นั่นก็ไม่ใช้ข้อเสียเปรียบโดยเฉพาะเมื่อเครือข่ายอินเตอร์เน็ตใช้พื้นฐานของ **TCP/IP** อย่างไรก็ตาม **SLIP** ก็มีข้อจำกัดบางอย่างที่ทำให้เป็นที่ถูกใจน้อยกว่า **PPP** สำหรับการเชื่อมต่อเครือข่ายอินเตอร์เน็ต คือ

- **SLIP** ไม่มีวิธีในการค้นหาและแก้ไขความผิดพลาด
- **SLIP** ไม่สนับสนุน **dynamic allocation** สำหรับ **IP address** ดังนั้นผู้ที่เรียกเข้ามาจะต้องทราบและสามารถที่จะจัดให้มี **IP address** ไม่เพียงแต่เฉพาะของตัวเอง แต่ยังต้องมี **IP address** ที่กำหนดให้กับเครื่องคอมพิวเตอร์ที่ติดต่อมาจากระยะไกล ถ้า **ISP** กำหนด **IP address** ให้แบบ **dynamic** แล้ว ซอฟต์แวร์ในเครื่องของผู้ที่เรียกเข้ามาจะต้องสามารถที่จะจับ **IP address** นั้นและนำมาใช้ หรือไม่ผู้ที่เรียกเข้ามาจะต้องจัดเตรียมข้อมูลเหล่านั้นป้อนให้ด้วยมือ
- **SLIP** ไม่ใช่มาตรฐานของเครือข่ายอินเตอร์เน็ต และมี **version** ที่แตกต่างกันเป็นจำนวนมากที่ไม่สามารถใช้ร่วมกันได้
- **SLIP** ไม่มีการตรวจสอบสิทธิการใช้งานของผู้ใช้ว่าเป็นของแท้ ดังนั้นจึงไม่มีวิธีในการตรวจสอบและไม่สามารถระบุการเรียกเข้ามาของเครื่องคอมพิวเตอร์ที่เรียกเข้ามาได้

12.5.3 CSLIP (Compressed Serial Line Internet Protocol)

CSLIP เป็นการเปลี่ยนแปลงโครงสร้างของ **SLIP** โดยตัวอักษร **C** หมายถึง **Compressed** ดังนั้น **CSLIP** ก็เหมือนกับ **SLIP** ที่ได้รับการออกแบบมาสำหรับการขนส่งข้อมูลแบบอนุกรมและสนับสนุน **TCP/IP** สิ่งที่แตกต่างจาก **SLIP** ก็คือในส่วนหัวของแพ็กเก็ตข้อมูล จะถูกบีบอัดจากเดิมซึ่งใช้ใน **SLIP** ที่มีขนาด **24** ไบต์ ให้เหลือเพียง **5** ไบต์ การที่ส่วนหัวของแพ็กเก็ตถูกบีบอัดจะทำให้ **CSLIP** มีข้อได้เปรียบในความเป็นจริงที่ว่าถ้าส่วนหัวที่มีขนาดแน่นอนถูกทำซ้ำสำหรับแพ็กเก็ตต่อๆ ไป **CSLIP** จะกำจัดส่วนนั้นของแพ็กเก็ตที่ตามมาภายหลังแพ็กเก็ตที่ส่งออกไปแล้ว ดังนั้นจึงประกอบด้วยเฉพาะส่วนที่แตกต่างกันในแต่ละแพ็กเก็ต ถึงแม้ว่าการย่อเฉพาะส่วนหัวโดยปราศจากการย่อส่วนที่เป็นข้อมูลอาจจะดูเหมือนว่าไม่ค่อยจะมีความได้เปรียบมากเท่าใดนัก แต่ในความเป็นจริงแล้ว ก็เป็นการทำให้ **SLIP** เกิดประโยชน์สูงสุด โดยเฉพาะอย่างยิ่งเมื่อมีการส่งเอกสารที่มีความยาวมาก

12.6 อินเตอร์เน็ต กับเว็บ (Internet and Web)

ยังมีสิ่งต่างๆ เกี่ยวกับระบบเครือข่ายที่จะต้องเรียนรู้อีกมาก ไม่เพียงแต่เรื่องของเทคโนโลยีอีกหลายอย่าง แต่ยังต้องทราบรายละเอียดเกี่ยวกับเทคโนโลยีนั้นๆ ด้วย ซึ่งประกอบด้วย จำนวนบิต และไบต์ในส่วนหัว การสร้างเฟรมข้อมูล สัญญาณการสื่อสาร (สัญญาณการตอบรับว่าได้รับข้อมูลแล้ว หรือเกิดความสับสนให้ส่งมาใหม่ และอื่นๆ) และรายละเอียดอื่นๆ เกี่ยวกับการจัดการของซอฟต์แวร์ เพื่ออนุญาตให้ติดต่อมาจากระยะไกลได้ การ **logon** แบบอัตโนมัติ การตรวจสอบรหัสผ่าน และอื่นๆ อีกมาก ซึ่งการบรรยายในเรื่องเหล่านี้ไม่เคยเริ่มแม้แต่จะเข้าไปมีส่วนร่วมในการพัฒนาเทคโนโลยีที่ใช้อยู่ในปัจจุบัน เรื่องเหล่านี้กำลังเฝ้ารอการรับรองจากหน่วยงานกำหนดมาตรฐาน ผู้ซึ่งจะนำโลกไปสู่เครือข่ายความเร็วสูง หรืออินเตอร์เน็ต 2

จนกระทั่งจินตนาการเหล่านี้ได้ทำให้เห็นในความอัศจรรย์ของสิ่งเหล่านี้ จึงยังคงมีเครือข่ายในโลกใบนี้ หากค่อยๆ คิดอย่างช้าๆ โดยเฉพาะอย่ายิ่งในเรื่องที่เกี่ยวกับเว็บแล้วเรื่องเหล่านี้ก็ยังคงเป็นความพิศวงในด้านเทคโนโลยี หลังจากที่มีทุกสิ่งแล้วยังมีอย่างอื่นอีกหรือไม่ที่ต้องทำ ในการทำให้บุคคลใดๆ สามารถ **access** เข้ามายังแหล่งข้อมูลที่สมบูรณ์จากที่ใดๆ ผ่านทางสายโทรศัพท์ได้ในราคาไม่แพง

12.6.1 Search Engines and Services

เมื่อมีไซต์เป็นจำนวนมาก ก็ย่อมมีเอกสารจำนวนมากกว่าในเครือข่ายอินเตอร์เน็ต คำถามแรกของผู้ที่เริ่มเข้ามาใหม่ดูเหมือนว่าจะเป็น "ฉันจะค้นหาสิ่งที่ฉันต้องการได้อย่างไร?" เห็นได้อย่างชัดเจนคือมีหลายวิธี ดังนี้

- ดูที่แอดเดรสของเว็บไซต์ในโทรทัศน์ ในหนังสือพิมพ์ หรือนามบัตร
- ได้รับการบอกกล่าวจากผู้อื่น ("คุณควรจะตรวจสอบที่เว็บไซต์ www.amazon.com")

12.6.2 Web search engines

Search engines โดยทั่วไปจะมีความสัมพันธ์กับการค้นหาเว็บไซต์ ซึ่งในความเป็นจริงก็คือความจริงในวงจรชีวิตของเว็บ โดยการใช้ **search engine** คุณจะสามารถค้นหาเว็บไซต์ซึ่งมีความสัมพันธ์กับหัวเรื่องที่น่าจะเป็นไปได้ หากปราศจาก **search engine** การค้นหาไซต์บนเว็บ อาจจะเปรียบเสมือนการค้นหาสิ่งของในป่าดงโดยผู้ที่ตาบอด หรืออาจกล่าวอีกอย่างหนึ่งได้ว่า **search engine** คือสิ่งที่จำเป็น และมี **search engine** เป็นจำนวนมากซึ่งเป็นที่รู้จักกันดี ซึ่งคุณอาจจะเลือกใช้จาก **AltaVista, Infoseek, Yahoo, Lycos, Excite** และ **Google** เป็นต้น

ถึงแม้ว่า **search engine** บางตัว เช่น **AltaVista** จะให้รายการของไซต์ต่างๆ และอย่างอื่น เช่น **Yahoo** และ **Infoseek** จะจัดแบ่งประเภทสำหรับผลของการค้นหาเพื่อให้ง่ายต่อการใช้ และแม้แต่จัดลำดับผลลัพธ์ให้กับคุณ อย่างไรก็ตามหากไม่คำนึงถึงความแตกต่างในรายละเอียดเหล่านี้แล้ว **search engines** ก็มีคุณสมบัติตามปกติ คือจะใช้คำสำคัญ (**keyword**) ในการทำดรรชนีเอกสาร และต้องอาศัยฐานข้อมูลของข้อมูลในการจัดเก็บ เพื่อที่จะเรียกเว็บไซต์ ที่ตรงกับการค้นหามาดู **Search engine** ส่วนใหญ่จะจัดให้มีวิธีการใช้ให้กับผู้ใช้ ไม่ว่าจะเป็นการค้นหาอย่างง่ายที่ใช้พื้นฐานของคำสำคัญ **1** คำหรือมากกว่า หรือการค้นหาอย่างประณีตที่อนุญาตให้ใช้ **Boolean Operators** เช่น **AND, OR** และ **NOT** ได้ด้วย ในการพัฒนาการจัดเก็บคำสำคัญ และเว็บไซต์นั้น **search engine** บางตัวต้องอาศัยมนุษย์ในการทำดรรชนี บางตัวก็อาศัยดรรชนีที่มีอยู่แล้ว และบางตัวก็อาศัยเครื่องมือทางด้านซอฟต์แวร์ที่ทำให้น่าใช้ (**spiders** หรือ **robots**) ที่ท่องเที่ยวเรียงไปตามตัวอักษรของเว็บ เพื่อที่จะค้นหารายการของไซต์ และเอกสาร

12.7 บริการบนเครือข่ายอินเตอร์เน็ต (Services)

ถึงแม้ว่า **search engine** และเว็บจะช่วยให้การค้นหาเป็นไปโดยระยะเวลาอันสั้น แต่ก็ยังมีวิธีอื่นในการค้นหาและเรียกข้อมูลมาใช้ วิธีที่มีการใช้อย่างแพร่หลายอย่างหนึ่ง คือ **File Transfer Protocol** หรือ **FTP** ซึ่งใช้ในการดาวน์โหลดทั้งไฟล์ข้อความและไบนารี่ไฟล์ได้อย่างรวดเร็วและง่ายมาก **FTP** ได้รับการช่วยเหลือจากบริการที่ชื่อว่า **Archie** เพื่อช่วยในการค้นหา การให้บริการการค้นหาอีกอย่างหนึ่งซึ่งมีการใช้กันบ่อยคือ **Gopher** ซึ่งมีการทำงานเหมือน **FTP** แต่จะเพลิดเพลินน้อยกว่า โดยได้รับการช่วยเหลือจากบริการการค้นหา ชื่อ **Veronica** และ **Jughead** นอกจากนั้น การค้นหาข้อมูลสามารถที่จะแปลงไปใช้บนเครื่อง **UNIX** ได้โดยใช้บริการการค้นหาชื่อว่า **WAIS** (**Wide Area Information Services**)

12.7.1 FTP and Archie

FTP คือหัวใจสำคัญของเครือข่ายอินเตอร์เน็ตมาเป็นเวลานานแล้ว โดย **FTP** เป็นโปรโตคอลในชุด **TCP/IP suite** ที่ทำงานใน **application layer** และจัดให้มีการ **access** เข้าไปยังไฟล์จำนวนมหาศาลที่ได้รับการประกาศให้เป็นสาธารณะและจัดให้มีเพื่อการดาวน์โหลดไฟล์เหล่านี้จะได้รับการบำรุงรักษาโดยเครื่อง **FTP servers** ที่มีเป็นจำนวนมาก ซึ่งบุคคลต่างๆ สามารถ **access** เข้าไปได้โดยเป็น "**anonymous**" หรือผู้ใช้ที่เป็นแขกรับเชิญ หลังจากที่มี **e-mail address** เป็นเหมือนรหัสผ่าน การค้นหาข้อมูลที่เก็บอยู่ในเครื่อง **FTP servers** ผู้ใช้จะต้องใช้ **Archie** ซึ่งเป็นบริการการค้นหาที่ช่วยในการกำหนดตำแหน่งของไฟล์ไม่ว่าจะเป็นโดยชื่อหรือผ่านการบรรยายด้วยคำสำคัญ

12.7.2 Gopher, Judhead และ Veronica

Gopher ได้ชื่อมาจากภาษาแสลงของคำว่า "**go-fer**" สำหรับบางคน (หรือบางสิ่ง) ที่ต้องวิ่งไปๆ มาๆ เพื่อไปนำสิ่งนี้หรือสิ่งนั้นมาจากผู้อื่น **Gopher** จะเชื่อมการให้บริการข้อมูลข่าวสารผ่านการทำดรรชนีให้เป็นสถานที่ที่สามารถค้นหาได้เพียงแห่งเดียวเรียกว่าที่ **Gohherspace** จึงแตกต่างจาก **FTP** ที่สามารถ **access** เข้าไปยังเอกสารต่างๆ ที่จัดเก็บอยู่ในเครื่องเซิร์ฟเวอร์ต่างๆ ได้ ภายใน **Gopherspace** เอกสารและข้อมูลอื่นๆ จะถูกจัดเรียงตามลำดับและผู้ใช้ก็จะใช้ระบบเมนูในการทำงานผ่านระดับต่างๆ จนกระทั่งค้นพบข้อมูลที่กำลังค้นหาอยู่ ณ จุดนี้ พวกเขายังสามารถอาศัย **Gopher** ในการจัดส่งข้อมูลเหล่านั้นมายังเครื่องคอมพิวเตอร์ของพวกเขาได้ เพื่อช่วยในการค้นหาใน **Gopherspace** ผู้ใช้อาจจะอาศัยการให้บริการการค้นหาอย่างใดอย่างหนึ่งดังนี้

12.7.2.1 Veronica

ส่วนของ **Gopher** ที่คล้ายกับ **Archie** จะค้นหาเมนูในเครื่อง **Gopher servers** ทั้งหมดที่เข้าคู่กับการค้นหาของผู้ใช้ เพื่อช่วยให้การค้นหาแคบลง **Veronica** จะอนุญาตให้ใช้ข้อความย่อยและ **Boolean Operator** ในการค้นหา ถึงแม้ว่าชื่อ **Veronica** จะไม่มีความหมายและเป็นเพียงการกล่าวถึงชื่อเพื่อนของตัวการ์ตูน **Archie** แต่ชื่อนี้ก็ได้รับการพิจารณาให้เป็นคำย่อจากพยัญชนะตัวแรกของ **Very Easy Rodent-Oriented Netwide Index to Computerized Archives** ซึ่งค่อนข้างจะวกวน

12.7.2.2 Judhead

เป็นการให้บริการซึ่งจัดให้มีโดยเครื่อง **Judhead servers** พิเศษ ที่สร้างดรรชนีเมนูในระดับสูงที่สุดของเครื่อง **Gopher servers** การใช้คำสำคัญใน **Judhead** ผู้ใช้สามารถจำกัดการค้นหาไปยังเครื่อง **Gopher server** โดยเฉพาะได้แทนที่จะต้องค้นหาทั่วทั้ง **Gopherspace** และ ชื่อ **Judhead** ก็มาจากการอ้างถึงเรื่อง 2 เรื่อง คือเป็นชื่อของตัวการ์ตูนที่เป็นเพื่อนของทั้ง **Archie** และ **Veronica** และเป็นคำย่อจากพยัญชนะตัวแรกของ **Jonzy's Universal Gopher Hierarchy Excavation and Display** เช่นเดียวกับชื่อ **Veronica**

12.7.3 จดหมายอิเล็กทรอนิกส์ (E-mail)

ถึงแม้ว่าในภาคธุรกิจและบริษัทต่างๆจะจัดให้มีบริการจดหมายอิเล็กทรอนิกส์หรืออีเมลล์ (**e-mail**) ขึ้นใช้ภายในระบบเครือข่ายของตนเอง แต่ทุกคนที่ใช้เครือข่ายอินเตอร์เน็ตจะทราบดีว่า อีเมลล์นั้นจะถูกจำกัดอยู่แค่เป็นการให้บริการเฉพาะในองค์กร ในความเป็นจริงแล้วอีเมลล์คือหนึ่งในบริการของเครือข่ายอินเตอร์เน็ตที่ได้รับความนิยมสูง การให้บริการรับ/ส่ง ข่าวสารไปทั่วโลกนี้สามารถมีได้โดยใช้โปรแกรมประยุกต์ซึ่งมีอยู่เป็นจำนวนมาก ซึ่งทั้งหมดจะทำให้

ผู้ใช้เครือข่ายอินเตอร์เน็ตสามารถสื่อสารกับครอบครัว เพื่อน บุคคลแปลกหน้า และแม้แต่ไซต์ต่างๆ บนเครือข่ายอินเตอร์เน็ต ในความเป็นจริงก็คือทุกคนที่สามารถกำหนดที่อยู่ได้โดยมีรูปแบบดังนี้ username@location เมื่อ

- **username** คือชื่อของผู้รับอีเมลล์ (บางครั้งอาจจะเป็นชื่อจริงของผู้รับ หรือเป็นชื่อสมมติ)
- **@** เรียกว่า "**at" sign** ซึ่งเป็นส่วนประกอบของอีเมลล์แอดเดรส
- **location** คือสถานที่ซึ่งเป็นที่เก็บและจัดส่งจดหมายของผู้รับ

มาตรฐานการขนส่งและจัดส่งจดหมายในเครือข่ายอินเตอร์เน็ต สนับสนุนโดย **SMTP (Simple Mail Transfer Protocol)** ซึ่งทำงานใน **application layer** โดยที่ **SMTP** เป็นส่วนหนึ่งของชุดโปรโตคอล **TCP/IP suite** ที่จัดให้มีการให้บริการรับ/ส่งอีเมลล์อย่างง่าย

12.7.4 ข่าว (News)

ข่าวบนเครือข่ายอินเตอร์เน็ตมีความหมายที่แตกต่างกัน 2 ประการ คือประเภทแรก มีข่าวจากแหล่งต่างๆ หลายประเภทที่ถูกกำหนดโดยโทรทัศน์ หนังสือพิมพ์ และบทความพิเศษเฉพาะเรื่องในนิตยสาร ข่าวประเภทนี้มีอยู่อย่างแพร่หลายในเว็บ และบางเว็บก็ต้องสมัครเป็นสมาชิก แต่ส่วนใหญ่แล้วจะมีให้ฟรี เช่น **MSNBC News on MSN, CNN** และ **CNN Finance, The New York Times** และ**Fortune Magazine** เป็นต้น

ยังมีข่าวอีกประเภทหนึ่งที่ผู้คนโดยปกติ ต้องการที่จะแลกเปลี่ยนข่าวสารกันแบบออนไลน์ โดยปิดประกาศไปยังกลุ่มอภิปรายซึ่งมีการพูดคุยกันแบบ **real-time** ข้อมูลประเภทนี้จะไม่เหมือนกับข่าวที่ประกาศตามเวลา **10.00** น. แต่ส่วนมากจะเป็นที่สนใจอย่างมากสำหรับผู้ที่เกี่ยวข้อง ข่าวประเภทนี้จะได้รับการจัดการบนเครือข่ายอินเตอร์เน็ต โดยการให้บริการบนพื้นฐานของ **NNTP (Network News Transfer Protocol)** ซึ่งเป็นมาตรฐาน **de facto** ที่ใช้ในการ กระจายบทความที่รวบรวมไว้เรียกว่า **newsfeeds** ไปยัง **newsgroups**

12.7.5 NNTP

NNTP เป็นโปรโตคอลที่เร็วและมีความน่าเชื่อถือซึ่งจัดให้มีไว้สำหรับดาวน์โหลดเช่นเดียวกับ **FTP** แต่ยังเสนอให้มีความสามารถในการโต้ตอบและความสามารถในการเลือกมากกว่า ในด้านความสามารถในการโต้ตอบ **NNTP** สนับสนุนการสื่อสารระหว่างเครื่องนิวส์เซิร์ฟเวอร์ 2 เครื่อง และระหว่างเครื่องไคลเอนต์กับเครื่องเซิร์ฟเวอร์ ทำให้เครื่องไคลเอนต์สามารถที่จะดาวน์โหลด **newsfeed** และสามารถเลือก **newsgroups** ได้ โดยการข้ามสิ่งที่ไม่อยู่ในความสนใจไป นอกจากนั้น **NNTP** ยังสนับสนุนความสามารถในการสอบถามเครื่องเซิร์ฟเวอร์ และทำการปิดประกาศหัวข้อข่าวได้ การให้บริการข่าวที่จัดตั้งโดย **NNTP** ที่ได้รับความนิยมสูง มีใช้อย่างแพร่หลายและรู้จักกันดีอย่างหนึ่งคือ **USENET** ซึ่งมีขนาดใหญ่ให้บริการวันละ **24** ชั่วโมง ตลอดทุกวัน ประกอบไปด้วย กระดานปิดประกาศ **(bulletin board)** และห้องสนทนา **(chat room)** เพื่อที่จะสนับสนุน **newsgroups** จำนวนนับพัน ที่อุทิศให้กับหัวข้อข่าวทุกประเภท ในการที่จะ **access** เข้าไปยัง **USENET** ผู้ใช้จะต้องสมัครเป็นสมาชิก (ไม่คิดค่าบริการ) กับการให้บริการนี้ ทำการดาวน์โหลดโปรแกรมการเรียกดูข่าวที่เรียกว่า **newsreader** แล้วจึงเข้าเป็นสมาชิกใน **newsgroups** ที่มีเนื้อเรื่องตรงกับที่คุณสนใจ ในทันทีที่เข้าเป็นสมาชิกผู้ใช้ก็จะสามารถดาวน์โหลดบทความบางส่วนหรือทั้งหมดของ **newsfeeds** ได้ หรือจะเลือกเข้าไปมีส่วนร่วมในการอภิปรายก็สามารถส่งความคิดเห็นไปปิดประกาศไว้ใน **newsgroups** นั้น หรือโต้ตอบกับความคิดเห็นของผู้อื่นที่แสดงให้เห็นต่อเนื่องกัน

12.7.6 Telnet

Telnet เป็นโปรโตคอลในชุด **TCP/IP suit** ซึ่งทำงานใน **application layer** และมีไว้สำหรับวัตถุประสงค์เพียงอย่างเดียว คืออนุญาตให้เครื่องคอมพิวเตอร์ **logon** ไปยังเครื่องคอมพิวเตอร์เครื่องอื่นจากระยะไกล และเสแสร้งว่าเป็นเครื่องเทอร์มินัลที่ติดต่ออยู่โดยตรงกับเครื่องคอมพิวเตอร์เครื่องนั้น ต้องขอขอบคุณเครือข่ายอินเตอร์เน็ตที่ทำให้เครื่องคอมพิวเตอร์นั้นจะตั้งอยู่ในที่แห่งใดก็ได้ในขอบข่ายทางภูมิศาสตร์ของเครือข่ายอินเตอร์เน็ต ตราบเท่าที่การเชื่อมต่อของเครื่องคอมพิวเตอร์จัดให้มีความสามารถในการจำลองเป็นเครื่องเทอร์มินัล เครื่องคอมพิวเตอร์ก็จะสามารถใช้แหล่งทรัพยากรและโปรแกรมของเครื่องคอมพิวเตอร์เครื่องนั้นได้

12.7.7 MUDs, Chats, and Other Forms of Play

และสุดท้าย อะไรคือสิ่งที่น่าสนุกสำหรับผู้ที่เข้าไปร่วมในเครือข่ายอินเตอร์เน็ต? ก็มีบ้าง หากคิดอย่างใหญ่โต คำจำกัดความของคำว่าน่าสนุกจะตัดสินว่าการให้บริการอะไรที่คุณสนใจมากที่สุด ตัวอย่างเช่นบางคนอาจจะสนุก (หรืออย่างน้อยก็พึงพอใจ) ใน **newsgroups** บางเรื่อง บางคนที่เคร่งขรึมเอาจริงเอาจังส่วนใหญ่จะสนใจเทคโนโลยีในระดับสูง และน่าเศร้าที่บางคนก็สนใจแต่เรื่องที่น่ารังเกียจโดยสิ้นเชิง อย่างไรก็ตามสำหรับผู้ที่มีแนวความคิดที่เป็นจารีตประเพณี สำหรับคำว่าน่าสนุกก็ยังมีอีก 2 แหล่งที่สามารถเข้าไปได้หากมีเวลา นั่นคือ **MUDs** สำหรับผู้ที่ชอบเล่นเกม และห้องสนทนา (**chat room**) สำหรับผู้ที่ต้องการพูดคุยในแบบ **real-time**

12.7.7.1 MUDs (Multi User Dungeons)

MUD คือการเติบโตสำหรับประเภทของการโต้ตอบแบบ ป้อมปราการกับมังกรยักษ์ คือผู้เล่นหลายคนมีบทบาทในการเล่นเกม (**Multiplayer role-playing games – RPGs**) บนเครือข่ายอินเตอร์เน็ต **MUDs** จัดให้มีผู้ร่วมมือในสภาวะแวดล้อมการเล่นเกมแบบเสมือนซึ่งแต่ละคนจะสามารถเล่นเป็นส่วนหนึ่งของเกมที่มีคุณสมบัติที่แตกต่างกัน และทั้งหมดก็จะโต้ตอบกันแบบ **real-time** ในบางครั้ง **MUDs** จะถูกกล่าวถึงว่าเป็น **MUSE** (**Multi-User Simulation Environment**) บนมาตรฐานเดียวกันสำหรับผู้ที่ชอบเรื่องเกี่ยวกับเทคโนโลยีระดับสูง ถึงความเฟ้อฝัน ก็จะมีสภาวะแวดล้อมที่คล้ายกันในแบบ **real-time** เรียกว่า **MOOs** (**MUDs Object Oriented**) ซึ่งแต่ละคนสามารถทำการโต้ตอบกันได้แต่จะโน้มเอียงไปในเรื่องที่อยู่ในใจ เช่น การเขียนโปรแกรม

12.7.7.2 Chat

มีคนเป็นจำนวนมากตั้งแต่เด็กไปจนถึงคนชราชอบการให้บริการนี้ ซึ่งมีทั้งบนเครือข่ายอินเตอร์เน็ตและบน **World Wide Web** โดยที่ **Chat** จัดให้มีความร่วมมือกันด้วยวิธีการทำให้การสนทนาเป็นแบบ **real-time** บนเครือข่ายอินเตอร์เน็ต **chats** ไม่เพียงแต่จะสนับสนุนการให้บริการข่าว เช่น **USENET** แต่ยังสนับสนุนการให้บริการอื่นที่อนุญาตให้คนตั้งแต่ 2 คนขึ้นไปสามารถพูดคุยกันเล่นในแบบ **real-time** ได้ การให้บริการอย่างหนึ่งในลักษณะนี้เรียกว่า **Talk** ที่อนุญาตให้คน 2 คน ต่อเชื่อมกันและดำเนินการสนทนากัน อีกบริการหนึ่งเรียกว่า **IRC** (**Internet Relay Chat**) อนุญาตให้มีผู้เข้าร่วมเป็นจำนวนมากเพื่อที่จะพูดคุยกับผู้อื่น โดยปกติ **IRC** จะอุทิศช่องสัญญาณให้กับหัวเรื่องที่แตกต่างกันและจะออกอากาศคำอธิบายไปยังทั้งกลุ่ม

12.8 ความรู้พื้นฐานเกี่ยวกับเว็บ

เป็นที่แน่นอนว่า **World Wide Web** มีมาเป็นเวลานานตั้งแต่ **Tim Berners-Lee** คิดค้นขึ้นมา เมื่อมองย้อนกลับไปที่ห้องทดลองทางฟิสิกส์ **CERN** ในประเทศสวิสต์เซอร์แลนด์ ถึงแม้ว่าจะยังคงมีพื้นฐานในการใช้ไฮเปอร์ลิงค์สำหรับการนำทางจากเอกสารหนึ่งไปยังอีกเอกสารหนึ่ง แต่เว็บก็ใหญ่กว่า มีสีสรรมากกว่า และเต็มไปด้วยเสียงมากกว่าที่เคยมีในครั้งหนึ่ง ในปัจจุบันเว็บเติบโตออกไปนอกเหนือขอบเขตทางด้านการศึกษากลายมาเป็นพลังอันยิ่งใหญ่ในการประมาณการทั้งส่วนบุคคลและสำหรับภาคธุรกิจ และไม่เพียงเป็นตัวแทนของแหล่งเก็บข้อมูลอิเล็กทรอนิกส์ขนาดใหญ่แต่ยังเป็นตลาดอิเล็กทรอนิกส์แห่งใหม่ที่เพิ่มจำนวนของธุรกิจที่เห็นว่าเป็นสิ่งสำคัญ และเข้ามามีส่วนเกี่ยวข้องกับเวทีการค้า การตลาด การโฆษณา การซื้อ และแม้แต่การชำระเงิน อย่างรวดเร็ว

ค่อนข้างเป็นการยากที่จะบอกว่าเว็บเป็นการเพิ่มจำนวนผู้ใช้ใหม่อย่างรวดเร็ว เพื่อสนับสนุนภาคธุรกิจ เพื่อผจญภัยบนเว็บ หรือว่าเป็นการปรากฏของธุรกิจที่รู้จักกันดีที่นำผู้ใช้ใหม่นับสิบล้านคนเข้ามายังจักรวาลเสมือนนี้ และสุดท้ายไม่ว่าจะตอบคำถามที่ว่าไก่เกิดก่อนไข่หรือไข่เกิดก่อนไก่ ว่าอย่างไร ก็ไม่ใช่สิ่งที่จำเป็น เพราะว่าในปัจจุบันเว็บคือความเป็นจริงในชีวิตที่มีการใช้เครื่องคอมพิวเตอร์ และในเวลามากกว่า **2 – 3** ปีที่ผ่านมา เว็บก็จะเป็นแหล่งข้อมูลแหล่งให้ความเพลิดเพลิน แหล่งซื้อหาสินค้าที่ต้องใช้ในชีวิตประจำวัน เทคโนโลยีเว็บ และโปรโตคอลจะถูกกำหนดให้เป็นมาตรฐานสำหรับธุรกิจเกี่ยวกับคอมพิวเตอร์ จนถึงจุดที่จำเป็นต้องมีเครือข่ายอินทราเน็ตในการรวมหลายๆ บริษัทเข้าด้วยกัน และเครือข่ายเอ็กซ์ตร้าเน็ตกลายเป็นเครื่องมือที่จำเป็นสำหรับภาคธุรกิจในการโต้ตอบกับลูกค้าและหุ้นส่วนธุรกิจ และการพาณิชย์อิเล็กทรอนิกส์ (**e-commerce**) ก็จะเติบโตเป็นธุรกิจราคาหลายร้อยล้านดอลลาร์ในอีก **2 – 3** ปีข้างหน้า หากถ่ายทอดข้อความการหาเสียงของประธานาธิบดีสหรัฐอเมริกาคนปัจจุบันที่กล่าวว่า "**It's the Web, stupid**" และตั้งแต่เว็บเริ่มที่จะเป็นสิ่งสุดท้ายในระบบเครือข่าย แต่เว็บก็เป็นมากกว่าสถานที่ที่เหมาะสมในการสิ้นสุดการสำรวจระบบเครือข่ายขนาดใหญ่ที่สุดในโลก

12.8.1 The Internet and the World Wide Web

ดูเหมือนว่าในปัจจุบัน ทุกคนจะใช้เครือข่ายอินเตอร์เน็ตและเวิร์ลวายเว็บ (**World Wide Web**) ในการแลกเปลี่ยนข้อมูลข่าวสารเพิ่มมากขึ้นไม่มากก็น้อย แต่ดังเช่นที่ได้ทราบแล้วว่าทั้งคู่ไม่ใช่สิ่งเดียวกัน เครือข่ายอินเตอร์เน็ตคือการเชื่อมต่อระบบเครือข่ายระหว่างประเทศที่มีขนาดใหญ่โตมหาศาลที่รวบรวมเครื่องเซิร์ฟเวอร์จำนวนมากและเชื่อมต่อระบบเครือข่ายเข้ากับ **backbones** ที่มีอยู่ทั่วโลก ส่วนเว็บก็คือส่วนหนึ่งของเครือข่ายอินเตอร์เน็ต ที่แม้แต่ผู้ใช้เป็นจำนวนมากก็ยังคิดว่าเว็บก็คือเครือข่ายอินเตอร์เน็ต

อะไรที่สร้างเว็บ? ถ้าคุณเคยใช้เว็บแน่นอนว่าคุณทราบคำตอบอยู่แล้ว แต่ให้ลองพิจารณาเบื้องหลังว่ามีอะไรที่เกี่ยวข้องบ้างเมื่อคุณเปิดโปรแกรมเบราส์เซอร์ พิมพ์ชื่อเว็บไซต์ใน **address bar** และกดคีย์ **Enter**

12.8.2 เว็บไซต์ (Web Sites)

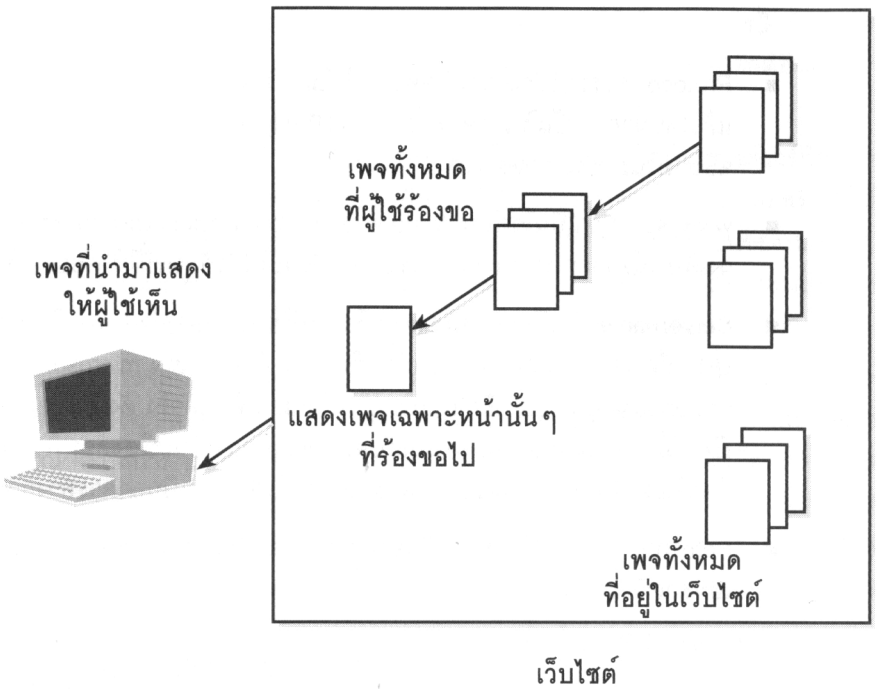
ถึงแม้จะมีคนพูดเกี่ยวกับการเล่นเว็บว่ามีการกำหนดขอบเขตทางภูมิศาสตร์เป็นอย่างดีในท้องถิ่น แต่เว็บก็ไม่ใช่แม้แต่จะเป็นสถานที่ แต่เป็นการรวบรวมเอกสาร ซึ่งเอกสารเหล่านี้เรียกว่า "เพจ (**pages**)" และการรวบรวมเพจเหล่านี้ทำให้เกิดเป็นไซต์จำนวนนับล้านที่ผู้ใดก็ตามที่ **access** เข้าไปยังเครือข่ายอินเตอร์เน็ตก็สามารถที่จะเข้าไปเยี่ยมชมได้ เว็บเพจและเว็บไซต์เหล่านี้จะร่วมกันแสดงข้อมูลในรูปแบบที่มีสีสรร ในบางครั้งถึงกับแสบตา ซึ่งไม่เพียง

ประกอบด้วยข้อความ แต่จะมีรูปภาพ เสียง ภาพการ์ตูนเคลื่อนไหว วิดีโอ และลิงค์เชื่อมโยงซึ่งมีอยู่ทุกแห่งซึ่งต้องการเพียงใช้เมาส์ ในการทำให้ผู้เยี่ยมชมเคลื่อนย้ายจากเพจหนึ่งไปยังอีกเพจหนึ่ง และจากไซต์หนึ่งไปยังอีกไซต์หนึ่งได้ ด้วยเทคโนโลยีของเว็บในระดับสูงที่มีในปัจจุบัน (ใน 2 – 3 ปีที่ผ่านมา) ทำให้เว็บเพจต่างๆ สามารถที่จะบรรจุโปรแกรมขนาดเล็ก (**script, applets, ActiveX controls**) ที่เพิ่มความสามารถในการโต้ตอบที่อนุญาตให้ผู้ใช้สามารถทำอะไรที่นอกเหนือจากการเรียกดูเพจได้ ดังแสดงตามรูปที่ **12 – 6**

รูปที่ **12 – 6** เว็บไซต์ของบริษัท **Cisco System**

บนเว็บมีเพจที่เรียงตามตัวอักษรนับล้านเพจ แต่เพจเหล่านี้จะลอยอยู่เหมือนกับใบไม้ที่ถูกลมพัดในฤดูใบไม้ร่วงหรือไม่ อมยิ้มเล็กน้อยแล้วตอบว่าแน่นอนคือไม่ใช่ เพจต่างๆ เหล่านี้จะได้รับการจัดเรียงตามลำดับชั้นอยู่ภายในเว็บไซต์ ซึ่งบางไซต์จะเป็นลักษณะ **one-stop** นั่นคือมีเนื้อหาอยู่เพียงเพจเดียว อย่างไรก็ตามส่วนมากแล้วจะเป็นการรวบรวมเพจที่มีความสัมพันธ์กันและมีวิธีในการจัดเรียงบางอย่างเช่นเดียวกับการจัดแบ่งเป็นบทของหนังสือเล่มนี้ บทต่างๆ เหล่านี้อาจจะประกอบด้วยเพจเพียง 2 – 3 เพจ ขึ้นอยู่กับไซต์นั้นๆ หรืออาจจะประกอบด้วยเพจที่มีความสัมพันธ์กันเป็นร้อยเป็นพันเพจดังเช่นในเว็บไซต์ของบริษัท **Cisco System** ที่แสดงให้เห็นในรูปที่ **12 – 6**

แต่ไม่ว่าไซต์จะมีขนาดเท่าใด ในแต่ละเพจอาจจะมีลิงค์เพื่อเชื่อมไปยังเพจอื่นๆ ได้ ไม่ว่าจะอยู่ในไซต์เดียวกัน หรือไซต์อื่นที่มีความสัมพันธ์กัน และผู้เข้าเยี่ยมชมสามารถทำงานผ่านการจัดลำดับของไซต์ โดยเริ่มจากเพจหลักที่เรียกว่า “โฮมเพจ (**Home Page**)” โดยที่โฮมเพจนี้จะจัดให้มีการเข้าถึงเพจย่อยๆ ที่รวบรวมเป็นไซต์ ตัวอย่างเช่น ในกรณีเว็บไซต์ของบริษัท **Cisco System** ที่โฮมเพจจะนำทางให้ผู้เข้าเยี่ยมชมไปยังกลุ่มย่อยๆ ของ **products, technical support** และ **events** อื่นๆ การที่จะดูเพจในเรื่องเฉพาะกลุ่มย่อย ผู้เข้าเยี่ยมชมเพียงแต่เลื่อนเมาส์ไปแล้วก็คลิกที่หัวเรื่องนั้นๆ เมื่อปรากฏเพจหลักของหัวเรื่องนั้นๆ แล้วก็ให้เลื่อนเมาส์ไปคลิกอีกเพื่อดูเพจที่ต้องการ ดังแสดงตามรูปที่ **12 – 7**



รูปที่ 12 – 7 การเรียกดูเพจต่างๆ ในเว็บไซต์

12.8.3 Web Address and URLs

การที่ผู้ใดผู้หนึ่งจะบอกเครื่องคอมพิวเตอร์ ว่าจะหาไซต์ และเพจโดยเฉพาะได้อย่างไร? โดยการบอกแอดเดรสของแต่ละไซต์ จะรวบรวมเอกสารและบำรุงรักษาโดยคนเพียงคนเดียวหรือองค์กรเดียว (รวบรวมจัดเก็บไว้ในเครื่องเซิร์ฟเวอร์เครื่องเดียวหรือมากกว่า) และเอกสารเหล่านี้จะสามารถถูก **access** ได้โดยการกำหนดแอดเดรสที่เรียกว่า "**Uniform Resource Locator**" หรือ **URL**

URLs จะดูเหมือนการรวมกันของเส้นทาง (**path**) และชื่อไฟล์ (**filename**) ซึ่งใช้ในการกำหนดตำแหน่งที่แน่นอนและชื่อของแหล่งทรัพยากรบนเว็บ ถึงแม้ว่า **URLs** จะแตกต่างจากแอดเดรสโดยทั่วไป แต่ **URL** ก็มีรูปแบบดังนี้ **Protocol://[www.]servername/path** เมื่อ

- **Protocol** จะระบุโปรโตคอลที่ต้องการใช้ในการ **access** แหล่งทรัพยากร สำหรับเว็บแล้วโดยมากจะเป็นโปรโตคอลชื่อว่า **HTTP (Hypertext Transfer Protocol)**
- **www** จะระบุว่าเป็นไซต์บน **World Wide Web** ส่วนนี้ของ **URL** แสดงอยู่ในเครื่องหมายวงเล็บก็เพราะว่าโปรแกรม **Browser** บางตัว จะใส่ตัวอักษรนี้ให้โดยอัตโนมัติ
- **Servername** เป็นชื่อของเครื่องคอมพิวเตอร์ซึ่งเป็นที่เก็บแหล่งทรัพยากร นี่เป็นส่วนของ **URL** ที่คนส่วนมากคิดว่าเป็นเว็บไซต์ที่แท้จริง เช่น **microsoft.com** หรือ **whitehouse.gov** อย่างไรก็ตามไซต์ก็ไม่ใช่สถานที่ที่แท้จริง ดังนั้นเมื่อคุณคิดเกี่ยวกับเว็บไซต์ เพื่อหลีกเลี่ยงความสับสนจะเป็นการดีถ้าคิดว่าสิ่งนี้เป็นเครื่องคอมพิวเตอร์ แทนที่จะคิดว่าเป็นหน้าร้าน หรือห้องสมุด หรืออะไรก็ตามที่เป็นอาคารทางกายภาพ
- **Path** คือเส้นทางไปยังแหล่งทรัพยากรที่แท้จริง ประกอบด้วยชื่อและประเภทของเอกสารที่จะถูกแสดง

ตัวอย่างเช่น **URL http://www.cisco.com/products/index.html** จะบอกโปรแกรมเบราส์เซอร์ให้ส่งการร้องขอและแสดงผลทางจอภาพ โดยใช้โปรโตคอล **HTTP** ในการเชื่อมต่อไปยัง **World Wide Web (www)** ที่เครื่องเซิร์ฟเวอร์ชื่อว่า **cisco.com** และแสดงเอกสารที่ชื่อว่า **product/index.html (html** คือนามสกุลของไฟล์ที่ระบุว่าเอกสารนั้นเป็น **HTML)** ซึ่งเป็นหน้าดัชนีสำหรับผลิตภัณฑ์ระบบเครือข่ายของบริษัท **Cisco System**

ดังนั้น **URL** จึงหมายถึงสิ่งที่ต้องพิมพ์ลงไปที่ **address bar** ของโปรแกรมเบราส์เซอร์ หรือในบางครั้งก็แค่คลิกที่ข่าวสารของอีเมลล์ หรือหัวเรื่องของเอกสาร ถ้าทำงานบนโปรแกรมประยุกต์ที่สามารถรันบนเว็บได้ เช่นโปรแกรม **Microsoft Word** หรือ **Microsoft Outlook** ซึ่งมีการบอกเส้นทางให้กับโปรแกรมเบราส์เซอร์ไปเปิดเอกสารที่ต้องการเมื่อใดก็ตามที่มีการคลิกที่ลิงค์บนเว็บเพจ

12.8.4 Web Browser

จนถึงตอนนี้ การเปิดโปรแกรมเบราส์เซอร์ แล้วพิมพ์ **URL** ที่คุณต้องการ หรือเลื่อนเมาส์ไปคลิกที่ลิงค์ในการเรียกดูเว็บเพจ แต่ว่าเว็บเพจเหล่านั้น ซึ่งส่วนมากจะประกอบด้วยข้อมูลหลายประเภท แต่ก็มีคำถามอยู่ว่า มีการจัดการอย่างไรในการทำให้สามารถแสดงผลทางจอภาพได้? สำหรับเรื่องนี้ จะเกิดอะไรขึ้นถ้ามีผู้หนึ่งผู้ใดคลิกที่ลิงค์และมีการขนส่งเพจทั้งหมดที่มี หรือทั้งเว็บไซต์? อะไรที่ทำให้ลิงค์เชื่อมโยงได้? และมีความแตกต่างจากข้อความและออบเจ็กต์อื่นที่เหลือบนเพจอย่างไร?

สิ่งสำคัญของทุกเรื่องที่กล่าวถึงนี้ก็คือโปรแกรมเว็บเบราส์เซอร์ **(Web Browser)** ซึ่งเป็นซอฟต์แวร์ที่ค้นหาเว็บไซต์ แล้วก็แปลงรหัสที่อธิบายเพจ เพื่อที่จะสร้างเป็นภาพให้ปรากฏบนจอภาพ ไม่ว่าจะสร้างให้เป็นโปรแกรมประยุกต์อิสระ (เช่น **Netscape Navigator)** ที่ทำงานอยู่ส่วนบนของระบบปฏิบัติการ หรือเป็นส่วนหนึ่งของระบบปฏิบัติการ (เช่น **Internet Explorer)** โดยที่โปรแกรมเบราส์เซอร์เหล่านี้ ได้รับการออกแบบเพื่อให้เข้าใจเทคโนโลยีของเว็บเพื่อให้แสดงผลลัพธ์ของเพจได้อย่างถูกต้อง โปรแกรมการจัดการเอกสาร **(Word Processor)** และโปรแกรมตารางข้อมูล **(Spreadsheet)** จะต้องเข้าใจรหัสที่ซ่อนเร้นและคำสั่งที่กำหนดว่าตัวอักษร แผนภูมิ หรือรายละเอียดงบประมาณ จะถูกนำมาแสดงได้อย่างไร โปรแกรมเบราส์เซอร์ก็เช่นเดียวกัน คือต้องเข้าใจรหัสและคำสั่งที่รวมอยู่ในเว็บเพจที่กำหนดว่า จะแสดงองค์ประกอบของเว็บเพจบนจอภาพในหน้าต่างของโปรแกรมเบราส์เซอร์อย่างไรที่ไหน ลักษณะและสีของตัวอักษรจะเป็นอย่างไร ซึ่งรหัสและคำสั่งเหล่านั้นเป็นส่วนหนึ่งของภาษามาตรฐานของเว็บที่เรียกว่า "**HTML (HyperText Markup Language)**"

12.9 ภาษาของเว็บ HTML (Hypertext Markup Language)

HTML เป็นภาษาสากลที่ใช้ในการสร้างเว็บ โดยไม่ค้นหาจุดเริ่มต้น **HTML** เป็นสิ่งที่เร้นลับเช่นเดียวกับภาษาต่างชาติ อย่างไรก็ตามเมื่อเริ่มต้นที่โปรแกรมเบราส์เซอร์ **HTML** จะอธิบายเว็บเพจ และทุกสิ่งทุกอย่างที่อยู่บนเพจอย่างหมดจด เพื่อให้เข้าใจเพิ่มมากขึ้นเกี่ยวกับ **HTML** เราจะเริ่มต้นที่การตรวจสอบจากชื่อ

- **Hypertext** ใช้อ้างถึงความจริงที่ว่า **HTML** ได้รับการออกแบบมาเพื่ออธิบายไฮเปอร์เท็กซ์ นั่นคือเอกสารเว็บ (ในความเป็นจริงแล้ว สามารถอธิบายเอกสารเว็บได้ดีกว่าว่าเป็น **hypermedia** เนื่องจากประกอบด้วยสิ่งที่เป็นมากกว่าข้อความธรรมดา อย่างไรก็ตาม **hypertext** เป็นเหมือนรากฐานของเว็บ ดังนั้นจึงใช้คำนี้ต่อไป เพื่อเป็นการสรรเสริญกับต้นกำเนิดของเว็บ)

- **Markup** ใช้อ้างถึงความจริงที่ว่า **HTML** ถูกใช้ในการทำสัญลักษณ์ให้กับเอกสาร นั่นคือจะอธิบายองค์ประกอบบนเพจ ด้วยวิธีการเดียวกับที่ผู้เรียบเรียงอธิบายวิธีในการพิมพ์เอกสารว่า ควรจะดูเมนูสคริปต์ (**menuscript**) ว่ามีรหัสพิเศษ หรือสัญลักษณ์สำหรับตัวอักษรเอียง ตัวอักษรหนา การจัดย่อหน้า และอื่นๆ
- **Language** ใช้อ้างถึงความจริงที่ว่า **HTML** ใช้พื้นฐานของรหัสและการแปลความหมายที่แน่นอน ซึ่งบุคคลใดๆ สามารถทำความคุ้นเคยได้ โดยการอ่านและทำความเข้าใจประโยคที่เขียนด้วยภาษา **HTML** เช่นเดียวกับภาษาอื่นๆ

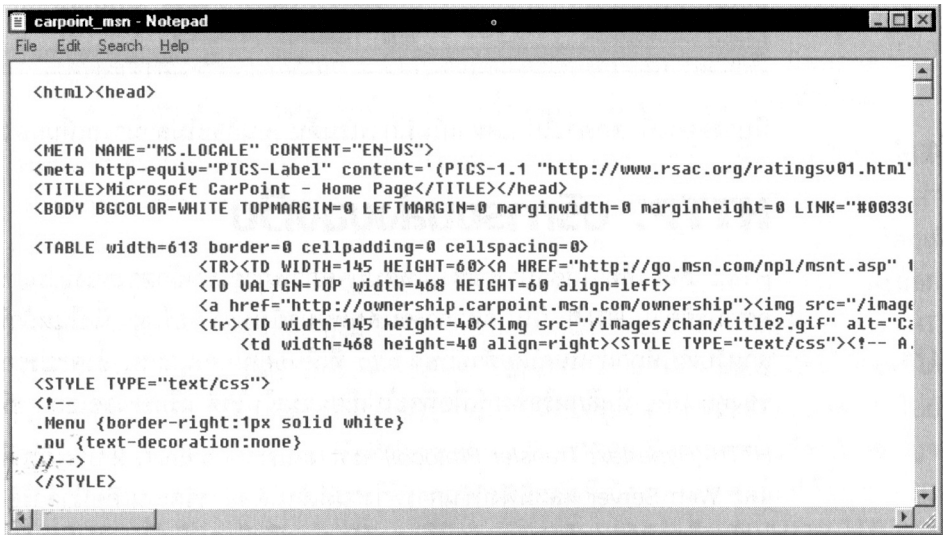
ถ้าหากหนังสือเล่มนี้ทั้งเล่มถูกเขียนด้วยภาษา **HTML** จะใช้ได้อย่างไร? คุณไม่มีความจำเป็นที่จะทราบลักษณะที่ยุ่งยากในรายละเอียดทุกอย่างของ **HTML** มากไปกว่าความแปลกใหม่ที่คุณพอใจ เว้นแต่ว่าคุณวางแผนที่จะเป็นผู้เชี่ยวชาญในด้านการออกแบบและสร้างเว็บเพจ อย่างไรก็ตามก็ไม่เป็นการเสียหายที่จะทำความเข้าใจ อย่างน้อยก็เพียงเล็กน้อยเกี่ยวกับว่า **HTML** มีการทำงานอย่างไร?

HTML ตั้งอยู่บนพื้นฐานของแนวความคิดของการใช้ **tags** ซึ่งกำหนดคุณสมบัติที่แน่นอนของเอกสาร มีคุณสมบัติประเภทใดบ้าง? คำตอบก็คือมีเป็นจำนวนมาก ประกอบด้วยคุณสมบัติประเภทที่ง่ายต่อการเข้าใจ เป็นต้นว่าคุณสมบัติที่บ่งชี้ว่าจะเริ่มย่อหน้าที่ไหน จะเริ่มทำให้ตัวอักษรหนาที่ไหนและสิ้นสุดที่ไหน และจะให้มีภาพปรากฏที่ใด **Tags** จะอยู่ภายในวงเล็บสามเหลี่ยมดังนี้ ‹**TAG**› และในบางครั้งก็จะปรากฏเป็นคู่ดังนี้ ‹**TAG**› .... ‹/**TAG**› เช่น ถ้าต้องการออกแบบเว็บ ต้องการที่เริ่มย่อหน้าใหม่ ก็จะใช้ **tag** ในการขึ้นย่อหน้าใหม่ในที่ซึ่งเป็นย่อหน้าใหม่ คือ ‹**P**›

ในกรณีที่ต้องการให้มีข้อความเป็นตัวอักษรหนา สามารถทำได้โดยใช้ **tag** เริ่มทำตัวหนา และสิ้นสุดการทำตัวหนา คือ ‹**B**› **This text is bold** ‹/**B**›

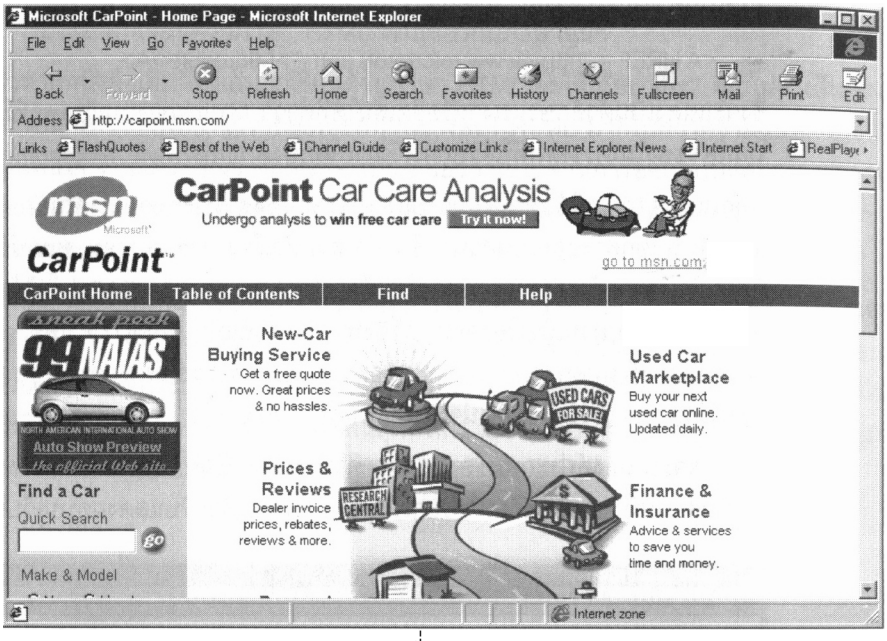
HTML ประกอบด้วย **tag** พื้นฐานเป็นจำนวนมาก และประกอบด้วย **tag** พิเศษที่เรียกว่า **anchor** ซึ่งใช้ในการบ่งชี้ว่าเป็น **link** หรือ **hypertext reference** (**HREF**) เพื่อโยงไปยัง **URL** ที่กำหนด โดยที่ **anchor** จะเริ่มด้วยตัวอักษร **A HREF** ตามด้วย **URL** และข้อความ (หรือภาพ) ที่ใช้เป็นตัวแทนของ **URL** ในเอกสาร และสิ้นสุดด้วย /**A** เช่น ‹**A HREF** = http://www.microsoft.com/›**Microsoft**‹/**A**› จะแสดงเป็นตัวอักษรแรเงาหรือขีดเส้นใต้ที่คำว่า **Microsoft** บนเว็บเพจที่มีความสัมพันธ์กับโฮมเพจของบริษัทไมโครซอฟต์ที่ได้รับการอธิบายโดยลิงค์ http://www.microsoft.com

นอกเหนือจากการใช้ **tag** โดยทั่วไปแล้ว **HTML** ยังสามารถกำหนดคุณลักษณะได้โดยวิธีการแบ่งการใช้รหัส (**code**) ในเอกสารออกเป็นส่วนๆ เรียกว่า ส่วนหัวเรื่อง (**head**) และส่วนเนื้อเรื่อง (**body**) โดยที่ส่วนหัวเรื่องจะทำเครื่องหมายโดยใช้ **tag** ‹**HEAD**› และ ‹/**HEAD**› ซึ่งใช้อธิบายหัวเรื่องของเอกสาร สำหรับส่วนเนื้อเรื่องจะทำเครื่องหมายโดยใช้ **tag** ‹**BODY**› และ ‹/**BODY**› ซึ่งจะบรรจุเนื้อหาทั้งหมดของเอกสาร เช่นข้อความ รูปภาพ ไฟล์เสียง และอื่นๆ รวมทั้ง **tag** ที่จะบอกให้ทราบว่าส่วนเนื้อเรื่องนี้จะแสดงบนจอภาพอย่างไร คุณอาจจะเห็นองค์ประกอบของ **HTML** ที่ใช้จริงเหล่านี้ได้ ตามตัวอย่างในรูปที่ **12 – 8** ซึ่งแสดงให้เห็นส่วนหนึ่งของการเขียนโปรแกรมภาษา **HTML** สำหรับเว็บเพจ



รูปที่ 12 – 8

รูปที่ 12 – 9 คือเพจที่แสดงตาม HTML Code จากรูปที่ 12 – 8



รูปที่ 12 – 9

12.10 HTTP: The Web Transport Service

HTML คือสิ่งที่ทำให้สามารถแสดงเพจบนจอภาพภายในหน้าต่างของโปรแกรมเบราส์เซอร์ได้ อย่างไรก็ตาม HTML ก็ไม่ได้ทำการขนส่งเพจมายังเบราส์เซอร์ สำหรับงานนี้เป็นหน้าที่ของ Web protocol ที่ถูกกำหนดโดยตัวอักษร http ที่เห็นอยู่ทุกหนทุกแห่ง ซึ่งจะปรากฏอยู่ที่ส่วนแรกของทุก URL ที่คลิกหรือพิมพ์เพื่อที่จะไปเยี่ยมชมเว็บไซต์ หรือร้องขอเอกสารที่อยู่ภายในไซต์นั้น

HTTP (Hypertext Transfer Protocol) จะทำงานระหว่าง **Web browsers** และ **Web server** และมีฟังก์ชันการทำงานที่เห็นได้อย่างชัดเจน คือนำคำร้องขอจากโปรแกรมเบราส์เซอร์ไปยังเครื่องเซิร์ฟเวอร์ และขนส่งเพจตามที่ร้องขอ (ถ้ามี) จากเครื่องเซิร์ฟเวอร์กลับมายังโปรแกรมเบราส์เซอร์

HTTP เป็นโปรโตคอลแบบ **object-oriented** ซึ่งหมายความว่าจะต้องอาศัยคำสั่งที่เป็นการทำงานกับเว็บเพจในลักษณะออบเจ็กต์ โดยวิธีการของ **HTTP** จะประกอบด้วยคำสั่งเป็นจำนวนมากที่ช่วยให้จัดการกับเครือข่ายอินเตอร์เน็ตได้ง่าย ตัวอย่างเช่น

- **GET** คือคำร้องขอเพื่อที่จะอ่านเพจ
- **HEAD** คือคำร้องขอเพื่อที่จะอ่านหัวเรื่องของเพจ เช่น ตัดสินใจเมื่อมีการปรับปรุงครั้งสุดท้าย
- **PUT** คือคำร้องขอเพื่อที่จะจัดเก็บเพจไว้บนเครื่องเซิร์ฟเวอร์
- **POST** คือคำร้องขอเพื่อติดประกาศ หรือเพิ่มข่าวสารให้กับแหล่งทรัพยากรที่กำหนดโดย **URL** ตัวอย่างเช่น การเพิ่มความคิดเห็นเข้าไปในกระดานปิดประกาศ

ดังนั้นการโต้ตอบโดยปกติของ **HTTP** ระหว่าง **Web browser** กับ **Web server** ควรจะมีความสัมพันธ์กับกระบวนการอย่างง่าย 2 ขั้นตอน ดังนี้

1. เบราส์เซอร์ส่งคำร้องขอไปยังเซิร์ฟเวอร์โดยใช้คำสั่งใน **HTTP** เช่น **GET** เพื่อร้องขอเว็บเพจ
2. เครื่องเซิร์ฟเวอร์ค้นหาเพจนั้น เมื่อพบก็จะส่งกลับมายังเบราส์เซอร์ และเครื่องเซิร์ฟเวอร์ก็จะส่งข่าวสารที่เป็นตัวเลขมาเพื่อทำให้เบราส์เซอร์ทราบว่าคำร้องขอนั้นจะปรากฏได้อย่างไร ถ้าเครื่องเซิร์ฟเวอร์สามารถที่จะทำตามคำร้องขอนั้นได้ ก็จะส่งสัญญาณตอบรับโดย **HTTP** กลับไปว่า "**success**" แต่ถ้าคำร้องขอนั้นล้มเหลวไม่ว่าจะด้วยเหตุผลใด เครื่องเซิร์ฟเวอร์ก็จะส่งสัญญาณกลับมาบอกให้ทราบประเภทของความผิดพลาด ตัวอย่างเช่น สัญญาณตอบรับที่เป็นตัวเลขซึ่งบอกว่า "**unable to carry out the request**"

ถึงแม้ว่า **HTTP** จะถูกนำมาใช้อย่างแพร่หลายและได้รับการพิจารณาอย่างรอบคอบให้เปิดกว้างเพื่อการปรับปรุงให้ดีขึ้นและมีวิวัฒนาการ แต่ก็ยังไม่มีการออกแบบให้มีความปลอดภัยในระดับสูง อย่างไรก็ตาม **HTTP** ก็ได้รับการเพิ่มระดับของความปลอดภัยขึ้นเรียกว่า **SHTTP (Secure HTTP)** ซึ่งเป็นการพัฒนาโดยเพิ่มการเข้ารหัสข้อมูล (**encryption**) และคุณสมบัติด้านความปลอดภัยอื่นให้กับ **HTTP** และนอกจากทำให้เกิดความสับสนแล้ว ยังมี **HTTP** อีกรูปแบบหนึ่งที่ในบางครั้งก็เรียกว่า **Secure HTTP** หรือบางครั้งก็เรียกว่า **HTTP Secure** ซึ่งใช้ตัวย่อใน **URL** ว่า **HTTPS** โดยเป็นโปรโตคอลที่ได้รับการพัฒนาโดยบริษัท **Netscapes** สำหรับการเข้ารหัสข้อมูลของเพจและ **access** เข้าไปยังเครื่อง **Web server** ผ่านทางพอร์ตที่มีความปลอดภัย **HTTPS** มีความจำเป็นที่จะต้องอนุญาตให้ **HTTP** ทำงานบนเลเยอร์รักษาความปลอดภัยที่ **Netscape** คิดค้นขึ้น ที่เรียกว่า **SSL** (จะอธิบายต่อไปในภายหลัง) โปรโตคอลที่มีการเพิ่มความปลอดภัยสำหรับ **HTTP** ได้รับการออกแบบมาเพื่อสนับสนุนความเป็นส่วนตัวและการทำธุรกรรมทางด้านการค้าบนเว็บ

<u>หมายเหตุ</u> การเข้ารหัสข้อมูล (**encryption**) และวิธีอื่นที่ทำให้มีความปลอดภัยบนเครือข่ายอินเตอร์เน็ต และ **World Wide Web** จะได้รับการอธิบายในหัวเรื่อง ความปลอดภัย (**Security**) ต่อไปในบทนี้

12.11 เว็บกับภาคธุรกิจ (Business and the Web)

เทคโนโลยีเว็บได้เข้ามาเป็นส่วนสำคัญในธุรกิจระบบเครือข่ายและดูเหมือนว่าจะถูกกำหนดให้มีความสำคัญมากยิ่งขึ้นเมื่อเครือข่ายอินเตอร์เน็ตเติบโตอย่างรวดเร็วและมีความซ่ำซองเพิ่มมากขึ้น เช่นไฮเปอร์ลิงค์ของเว็บเป็นเหมือนการเชื่อมโยงที่มีชีวิต ซึ่งต้องมีอยู่ภายในเอกสารและอีเมลล์เป็นประจำ จะจัดให้ผู้ใช้มีความสามารถในการกระโดดจากแหล่งข้อมูลหนึ่งไปยังอีกแหล่งข้อมูลหนึ่งอย่างอิสระตามต้องการ หรืออารมณ์พาไป

ในมาตราส่วนขนาดใหญ่ เทคโนโลยี **Web** ยังก่อให้เกิดขอบเขตระหว่างระบบเครือข่าย "**out there**" และระบบเครือข่าย "**within**" ให้เติบโตตามปรารถนาได้ตลอดเวลา ตัวอย่างเช่นคุณสมบัติเบื้องต้นของโปรแกรมเบราส์เซอร์ในปัจจุบัน สามารถสนับสนุนให้มีการทำงานพื้นฐานในเรื่องการจัดการไฟล์และการแสดงผลทางจอภาพ เพื่อจัดให้มีระดับของความสอดคล้องระหว่างโปรแกรมประยุกต์ และที่สำคัญมากไปกว่านั้นก็คือคุณสมบัติเหล่านี้ยังช่วยให้ซอฟต์แวร์ของผู้ใช้ลบความแตกต่างระหว่างไฟล์ท้องถิ่นกับไฟล์ที่อยู่ห่างไกลออกไป เพื่อที่จะให้ผู้ใช้มุ่งไปยังสิ่งที่พวกเขาต้องการจะดูแทนที่จะต้องวุ่นวายอยู่กับการค้นหา หากมองในมาตราส่วนที่ใหญ่ขึ้นไปอีก ในช่วง **2 – 3** ปีที่ผ่านมาเครือข่ายอินเตอร์เน็ตและเทคโนโลยีเว็บได้เจาะลึกเข้ามามีส่วนในธุรกิจด้านระบบเครือข่าย ภาคธุรกิจจำนวนมากได้จัดให้มีการปรากฏตัวของบริษัทบนเว็บ และมีหลายกรณีที่จัดให้พนักงานที่ต้องการใช้สามารถเข้าไปยังเครือข่ายอินเตอร์เน็ตและเว็บของบริษัทได้ หรืออย่างน้อยก็จัดให้สามารถใช้ทรัพยากรหลายอย่างที่พบบนระบบเครือข่ายทั่วโลกได้ นอกจากนั้นเทคโนโลยีเครือข่ายอินเตอร์เน็ตยังเข้ามาเป็นรากฐานในธุรกิจด้านการสื่อสารและโทรคมนาคม

ภายในภาคธุรกิจ บริษัทขนาดใหญ่กำลังค้นหาว่าเครือข่ายอินทราเน็ตจะจัดให้มีความง่ายต่อการใช้ ปลอดภัยและมีประสิทธิภาพทางด้านราคาในความหมายของการกระจายข้อมูลข่าวสารทุกประเภท นอกจากนั้นในธุรกิจบางอย่างยังจัดตั้งเครือข่ายอินทราเน็ตของตนเองตามข้อจำกัดที่ให้เข้าถึงได้เฉพาะผู้ใช้ภายนอกที่ได้รับความเชื่อถือ (ผู้แทนจำหน่าย หุ้นส่วนธุรกิจ ผู้จัดหา และอื่นๆ) และสุดท้าย การพาณิชย์อิเล็กทรอนิกส์ (**e-commerce**) ซึ่งเป็นการใช้เครือข่ายอินเตอร์เน็ตอย่างยิ่งใหญ่ ชนิดที่ไม่เคยมีมาก่อน ซึ่งทำให้บริษัทต่างๆ และหน่วยงานของรัฐบาล มีหูตากว้างขวางอย่างปราดเปรียว ที่เพิ่งจะมีล่าสุด เช่นเดียวกับความเจริญทางเศรษฐกิจที่มีอิทธิพลทางด้านความคิดและเป็นที่ดึงดูดใจทางด้านการตลาด แม้แต่สำหรับผู้เริ่มเล่นอินเตอร์เน็ต

12.11.1 อินทราเน็ตและเอ็กตร้าเน็ต (Intranets and Extranets)

มีความเป็นไปได้ที่การประยุกต์เทคโนโลยีที่มีความสัมพันธ์กับเว็บ ซึ่งนับว่าสำคัญที่สุดรวมกับระบบเครือข่าย จะสามารถสร้างเครือข่ายอินทราเน็ตและเอ็กซ์ตร้าเน็ต ซึ่งคล้ายคลึงกับเครือข่ายอินเตอร์เน็ตขนาดย่อ (หรือเว็บขนาดย่อ) ทั้งเครือข่ายอินทราเน็ตและเอ็กซ์ตร้าเน็ตจะต้องอาศัยโปรแกรมเว็บเบราส์เซอร์เป็นกุญแจในการเข้าไปดูและใช้โปรแกรมประยุกต์ และเอกสารจากที่สิ่งเหล่านั้นมีอยู่ โดยเครือข่ายอินทราเน็ตจะใช้ภายในบริษัท ส่วนเครือข่ายเอ็กซ์ตร้าเน็ตจะสร้างจากแนวความคิดของเครือข่ายอินทราเน็ตที่ก้าวไปอีกขั้น โดยทำให้ส่วนหนึ่งของเครือข่ายอินทราเน็ตสามารถที่จะเข้าถึงได้ โดยผู้ใช้จากภายนอกที่ได้รับความเชื่อถือ

ทั้งเครือข่ายอินทราเน็ตและเอ็กซ์ตร้าเน็ตต้องอาศัยโปรโตคอลที่ใช้บนเครือข่ายอินเตอร์เน็ต และเทคโนโลยีซึ่งประกอบด้วย **HTTP** กับ **TCP/IP** ในการขนส่งข้อมูล และ **HTML** สำหรับการอธิบายเอกสาร ในภาคธุรกิจที่กระจายอยู่ในวงกว้างอาจจะครอบคลุม **LANs** หลายวง แต่โดยพื้นฐานแล้วคุณอาจจะมองว่าเครือข่าย

อินทราเน็ตและเอ็กซ์ตร้าเน็ตเป็นการประยุกต์การจัดแบ่งประเภทที่วางอยู่เหนือการรวมระบบเครือข่ายเพื่อทำให้ได้รับความรู้สึกของ **World Wide Web** นอกจากนั้นทั้งเครือข่ายอินทราเน็ตและเอ็กซ์ตร้าเน็ตยังสามารถจัดให้มีการ **access** เข้าไปยังเครือข่ายอินเตอร์เน็ตที่อยู่ภายนอกบริษัทได้ และแน่นอนว่าในกรณีนี้การรักษาความปลอดภัยของระบบเครือข่ายภายในจากคนแปลกหน้าที่อยู่บนเครือข่ายอินเตอร์เน็ตจะต้องได้รับการพิจารณาเป็นสำคัญ โดยปกติบริษัทต่างๆ จะรักษาความปลอดภัยโดยใช้ไฟร์วอลล์ (**Firewall**) ในการแยกระบบเครือข่ายของตนเองออกจากโลกภายนอกและจัดให้มีการ **access** เครือข่ายอินเตอร์เน็ตผ่านทางเครื่องพร็อกซี่เซิร์ฟเวอร์ (**proxy servers**) ที่ทำการถ่ายทอดคำร้องขอจากเครื่องคอมพิวเตอร์ของผู้ใช้ภายในบริษัทเข้าและออกจากเครือข่ายอินเตอร์เน็ต

12.11.2 การพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce)

การพาณิชย์อิเล็กทรอนิกส์ หรือ **E-Commerce** คือ ความเร่าร้อนที่ปรากฏขึ้นบนเว็บเป็นรายล่าสุด โดยสิ่งที่ผลักดันธุรกิจทั้งขนาดใหญ่และขนาดเล็กคือการจัดตั้งร้านค้าที่สามารถทำงานได้บนเว็บ ธุรกิจส่วนใหญ่จะใช้เว็บสำหรับเป็นร้านค้าขายปลีก แต่ธุรกิจการให้บริการก็สามารถทำอย่างจริงจังได้เช่นกัน ตัวอย่างเช่นการจองตั๋วในระบบออนไลน์ที่มีใช้ทั้งในบริษัทการบินและการแสดงดนตรี ในไซต์ที่เกี่ยวกับการเดินทางจะเสนอให้มีการจองโรงแรมแบบอิเล็กทรอนิกส์ รวมทั้งการเช่ารถ และแม้แต่ธนาคาร รวมทั้งกิจการนายหน้าก็เริ่มที่จะสำรวจการใช้เว็บให้เป็นวิธีในการทำธุรกิจ ธุรกิจหลายประเภทตั้งแต่ร้านเสื้อผ้า **Eddie Bauer** จนถึง **Dell Computer** และ **amazon.com** ซึ่งเป็นอัจฉริยะทางด้านการค้าปลีกทางอิเล็กทรอนิกส์จะต้องเป็นผู้บำรุงรักษาเว็บไซต์ของตนเอง แต่ก็มีหลายธุรกิจที่ขยายมุมมองของตนเองไปอย่างกว้างไกล โดยเข้าไปเป็นหุ้นส่วนกับเจ้าของไซต์ขนาดใหญ่ซึ่งถูกใช้งานอย่างหนักที่เรียกว่า “เว็บท่า”

12.11.3 เว็บท่า (Portals)

ถ้าเคยติดตามรายงานข่าวในช่วงปีที่แล้ว อาจจะเคยอ่านเกี่ยวกับเว็บท่าในชีวิตประจำวัน เว็บท่า (**Portal**) คือทางเข้าหรือประตูไปสู่ที่แห่งอื่นในโลกของเครือข่ายอินเตอร์เน็ต เว็บท่าจะให้บริการเช่นเดียวกับวัตถุประสงค์นี้ นั่นคือจะเป็นประตูไปสู่เว็บหรือเป็นไซต์ที่ได้รับการออกแบบให้ผู้เข้าเยี่ยมชมมีความสะดวกสบายเหมือนเป็นบ้านตัวเอง ซึ่งหมายถึงเป็นสถานที่ซึ่งผู้เข้าเยี่ยมชมจะไปไหนมาไหนได้ โดยอัตโนมัติเมื่อใดก็ตามที่พวกเขาเหล่านั้น **access** เข้าไปยังเว็บนั้นๆ และเป็นสถานที่ซึ่งพวกเขาสามารถเข้าไปมีส่วนร่วมในทิศทางที่เลือกไว้ได้อย่างง่ายดาย เช่น ไปยังกระดานประกาศ ห้องสนทนา และบริการการรับ/ส่งอีเมลล์ เช่นเดียวกับการไปยังไซต์ที่อุทิศให้กับการกีฬา ข่าว รายงานอากาศ สันทนาการ การซื้อของตามร้านค้าอิเล็กทรอนิกส์ และอื่นๆ

วัตถุประสงค์หลักอย่างหนึ่งของเว็บท่า ก็คือจัดเตรียมให้มีการ **access** ไปยังไซต์ และการให้บริการอื่นที่แน่นอน ซึ่งรวมถึงร้านค้าหรือห้างสรรพสินค้าที่สามารถเลือกซื้อสินค้าแบบอิเล็กทรอนิกส์ได้ บางไซต์ และการให้บริการบางอย่างที่เสนอให้มีสิ่งเหล่านี้ ก็ถูกครอบครองโดยองค์กรที่เป็นเจ้าของเว็บท่า แต่ส่วนมากจะจัดส่งให้โดยหุ้นส่วนที่เช่าพื้นที่บนหน้าจอของเว็บท่า เช่นเดียวกับการเช่าพื้นที่ร้านค้าในห้างสรรพสินค้า เว็บท่าบางเว็บก็ได้รับความนิยมเป็นอย่างสูง บางเว็บก็ไม่ อย่างไรก็ตามเว็บท่าทั้งหมดก็พยายามที่จะให้ความรู้สึกเป็นกันเองกับผู้ใช้ของตนเอง ซึ่งโดยมากจะทำโดยการจัดแบ่งประเภทของไซต์ เพื่อช่วยคนในการค้นหาและนำทางไปยังไซต์ที่มีอย่างหลากหลายเป็นจำนวนมากบนเว็บ และถ้าใช้ภาษาที่เกี่ยวกับการตลาด เว็บท่าก็คือวิธีในการเข้ายึดหัวใจและลูกนัยตาของลูกค้า และเป็นกระบวนการที่ทำให้มีการเก็บค่าโฆษณาสำหรับผู้เป็นเจ้าของเว็บท่า

เว็บท่าไม่มีส่วนเกี่ยวข้องโดยตรงกับเรื่องของระบบเครือข่ายที่อธิบายครอบคลุมในหนังสือเล่มนี้ แต่มีส่วนเกี่ยวข้องกับการพาณิชย์อิเล็กทรอนิกส์ ซึ่งเป็นวิถีทางที่อาจจะเข้ามามีส่วนในชีวิตประจำวันสำหรับผู้บริหารระบบเครือข่าย หลังจากที่เว็บท่าได้รับการคาดว่าจะมีประชากรเติบโตต่อไปอย่างต่อเนื่อง และผู้ใช้จำนวนมากเหล่านี้ก็จะต้องเผชิญกับการพาณิชย์อิเล็กทรอนิกส์อย่างแน่นอน นอกจากนั้นเว็บท่ายังดึงดูดความสนใจสำหรับฝ่ายการเงินของบริษัทขนาดใหญ่ที่เป็นที่รู้จักดี และในปัจจุบันก็ถูกสร้างและบำรุงรักษา โดยบริษัทที่มีความเท่าเทียมกันในด้านเทคโนโลยีเว็บ ซึ่งประกอบด้วย บริษัท **Microsoft (MNS)** และบริษัท **Netscape (AOL)** และผู้จัดให้มีบริการการค้นหา เช่น **Excite, Yahoo** และ **Infoseek** หรืออาจกล่าวอย่างสั้นได้ว่า เศรษฐกิจและความสามารถในการเข้าถึง เป็นพลังผลักดันอยู่เบื้องหลังการพัฒนาและการขยายแนวความคิดของเว็บท่า และปัจจัยทั้งสองอย่างนี้ก็มีอิทธิพลต่อระบบเครือข่ายทั้งหมด ถ้าไม่โดยตรงก็จะรวมอยู่ในวิธีที่ระบบเครือข่ายได้รับการออกแบบ จัดการ และรักษาความปลอดภัย

12.12 ความปลอดภัย (Security)

ดังที่ได้กล่าวถึงในบทที่ 8 ในเรื่องของการรักษาความปลอดภัยของระบบเครือข่าย ซึ่งจะมีเนื้อหาที่แตกต่างกันเป็นอย่างมากมาก เป็นต้นว่ามีเนื้อหาของการทำให้มั่นใจโดยมีแหล่งจ่ายกำลังไฟสำรองให้กับเครื่องเซิร์ฟเวอร์มีเนื้อหาเกี่ยวกับการสำรองข้อมูลที่มีคุณค่าบนดิสก์ด้วยวิธี **mirroring** หรือ **striping** และทำให้มั่นใจว่าข้อมูลเหล่านั้นจะไม่สูญหาย สำหรับในส่วนของผู้ใช้ก็จะมีเรื่องของความต้องการให้มี ชื่อผู้ใช้และรหัสผ่านในการจำกัดการ **access** ระบบเครือข่ายให้กับผู้ที่ได้รับสิทธิในการใช้ และมีความต้องการในการควบคุมการ **access** ที่พิจารณาว่าผู้ใดสามารถที่จะเรียกดูและแก้ไขเอกสาร ฐานข้อมูลและไฟล์อื่นๆ ที่จัดเก็บข้อมูลของบริษัทไว้ ส่วนในด้านของระบบเครือข่ายก็มีเนื้อหาเกี่ยวกับความปลอดภัยเพิ่มอีก ประกอบด้วย

- การป้องกันระบบเครือข่ายภายในจากการ **access** โดยผู้ใช้ที่ไม่ได้รับสิทธิการใช้
- การป้องกันข้อมูลในขณะที่ทำการขนส่งอยู่บนเครือข่ายอินเตอร์เน็ต
- การป้องกันความเป็นส่วนตัวและการรักษาความปลอดภัยของข้อมูลส่วนตัวและข้อมูลด้านการเงินของผู้ใช้

ถึงแม้ว่าผู้สนับสนุนการเปิดกว้างของเครือข่ายอินเตอร์เน็ตในปัจจุบันได้รับสิทธิในการป้องกันและมีความภูมิใจในความสามารถในการเข้าถึงเครือข่ายอินเตอร์เน็ต แต่คุณภาพในความสามารถเหล่านั้นก็มีทั้งทางบวกและทางลบ เพื่อช่วยให้มั่นใจความเป็นส่วนตัวในการสื่อสารและข้อมูลที่เป็นส่วนตัวยังคงรักษาความเป็นส่วนตัวไว้ได้โดยปราศจากการประนีประนอมโดยเจตนาจากความเป็นอิสระของเครือข่ายอินเตอร์เน็ต บริษัทด้านเทคโนโลยีและหน่วยงานกำหนดมาตรฐานได้พัฒนา (หรือกำลังอยู่ในกระบวนการพัฒนา) วิธีการต่างๆ เพื่อจัดให้มีความปลอดภัยและเกิดความสงบในใจโดยปราศจากสิ่งที่มาขัดขวางความเป็นส่วนตัวที่ไม่จำเป็น

มีวิธีการหลายวิธีที่ทำให้มั่นใจได้ว่าผู้คน (และโปรแกรม) ทำถูกต้องตามกฎหมาย และการสื่อสารนั้นๆ ไม่สามารถถูกอ่านได้โดยผู้ลอบดักฟังทางอิเล็กทรอนิกส์ ในเรื่องเหล่านี้มีอุปกรณ์ด้านซอฟต์แวร์ เช่นลายเซ็นต์ดิจิตอล **(digital signatures)** ซึ่งสามารถใช้ในการตรวจสอบผู้ส่งข่าวสารว่าเป็นของแท้ การเข้ารหัสข้อมูล **(encryption)** ซึ่งถูกใช้ในการกวนการส่งสัญญาณข้อมูลเพื่อทำให้ข้อมูลนั้นไม่สามารถอ่านได้ และระบบเครือข่ายส่วนตัวแบบเสมือน **(virtual private network)** ซึ่งใช้เทคนิคที่เรียกว่า **tunneling** เพื่อเปลี่ยนเครือข่ายอินเตอร์เน็ตที่เป็นสาธารณะให้เป็นสื่อการสื่อสารที่ปลอดภัย วิธีต่างๆ เหล่านี้ คือ

12.12.1 Digital signatures and personal keys

ถ้าคุณใช้ **Microsoft Windows** กับ **Internet Explorer** คุณอาจจะเคยเห็นหน้าต่างการรับประกัน ปรากฏในขณะที่คุณกำลังดาวน์โหลดส่วนของซอฟต์แวร์จากเว็บ หน้าต่างนี้เป็นส่วนที่เป็นคุณสมบัติการตรวจสอบของ **Microsoft** ที่เรียกว่า **Authenticode** ซึ่งคือวิธีการรับรองกับผู้ใช้ว่าโปรแกรมที่กำลังดาวน์โหลดนั้นถูกสร้างโดยกลุ่มหรือผู้ที่มีรายชื่ออยู่ในใบประกาศนียบัตร และโปรแกรมนั้นไม่มีการเปลี่ยนแปลงนับตั้งแต่ถูกเขียนขึ้นมา ถึงแม้ว่า **Authenticode** จะไม่สามารถตรวจสอบได้ว่าโปรแกรมที่ดาวน์โหลดอยู่นั้นไม่มี **bug** หรือมีความปลอดภัยในการใช้อย่างสมบูรณ์ แต่ก็สามารถตรวจสอบได้ว่าโปรแกรมนั้นไม่ได้ถูกเปลี่ยนแปลงหลังจากที่เขียนเสร็จและลงนามโดยผู้เขียน หัวใจสำคัญของ **Authenticode** คือคุณสมบัติด้านความปลอดภัยที่เรียกว่า **digital signatures** ซึ่งเป็นรูปแบบของการเข้ารหัส ซึ่งไม่เพียงถูกใช้ในการตรวจสอบผู้สร้างว่าเป็นของแท้ แต่ยังถูกใช้ในการตรวจสอบว่าเป็นผู้ส่งข้อมูลข่าวสารที่แท้จริงอีกด้วย ในการทำงาน **digital signature** จะต้องอาศัยกุญแจที่เรียกว่า **public key** และ **private key** ซึ่งจะต้องได้รับการรับรองจากองค์กรที่เรียกว่า **Certification Authority** (เทียบเท่ากับ **locksmith**) เมื่อจำเป็น **public key** และ **private key** เหล่านี้จะทำการเปรียบเทียบกับชื่อผู้ใช้และรหัสผ่านที่ผู้ใช้ใช้ในการ **logon** อย่างเป็นทางการ **public key** คือสิ่งที่สามารถแจกให้กับผู้ใดก็ได้ เหมือนกับชื่อผู้ใช้ (**username**) ส่วน **private key** ควรจะมีผู้ที่รู้เพียงผู้เดียวคือผู้ที่เป็นเจ้าของ ซึ่งจะเหมือนกับรหัสผ่าน (**password**)

เมื่อกุญแจเหล่านี้ถูกใช้ในการทำเครื่องหมายให้กับไฟล์หรือโปรแกรม กระบวนการจะทำการคำนวณค่าที่เรียกว่า **hash number** ซึ่งอยู่บนพื้นฐานในเรื่องขนาดของไฟล์ หรือข้อมูลอย่างอื่นที่เกี่ยวกับผู้ส่ง จากนั้น **hash number** นี้จะถูกทำเป็นเครื่องหมาย (เปลี่ยนเป็นการเข้ารหัสที่เป็นชุดของบิต) กับ **private key** ของผู้ส่งเพื่อสร้างค่าที่สามารถเข้าคู่ได้กับข้อมูลที่ถูกใช้ ในการสร้าง **hash number** หรือกล่าวอีกอย่างหนึ่งได้ว่า **hash number** จะพอดีกับไฟล์ต้นกำเนิด ด้วยวิธีเดียวกันกับที่ลายนิ้วมือจะพอดีกับคนเพียงคนเดียว ดังนั้นจึงสามารถรับรองได้ว่าถ้าแม้แต่เพียง **1** บิต มีการเปลี่ยนแปลง ก็จะทำให้ไม่สามารถเข้าคู่กับ **hash number** และไฟล์ได้ และผู้รับก็จะได้รับการบอกว่าไฟล์นั้นมีการเปลี่ยนแปลงหรือถูกรบกวน ในด้านฝั่งผู้รับก็จะทำการคำนวณค่า **hash number** ใหม่และตรวจสอบกับลายเซ็นต์ที่ได้รับการช่วยเหลือจาก **public key** ของผู้ส่ง (แน่นอนว่า ผู้รับจะต้องได้รับมาแล้ว)

12.12.2 การเข้ารหัสข้อมูล (Encryption)

ถึงแม้ว่า **digital signature** จะเป็นสิ่งที่มีคุณค่าในการตรวจสอบโปรแกรมและไฟล์ว่าเป็นของแท้และถูกต้องตามกฎหมาย แต่ความปลอดภัยในระดับสูงกว่าก็จัดให้มีการเข้ารหัสไฟล์ที่มีความสำคัญก่อนที่จะทำการส่ง (จำเป็นอย่างยิ่งที่จะต้องทำให้ไฟล์นั้นเป็นอะไรที่ไร้สาระไม่สามารถอ่านได้โดยผู้อื่น ยกเว้นผู้ส่งและผู้รับ) การเข้ารหัสข้อมูลสามารถนำมาใช้เพิ่มเติมร่วมกับการใช้ **digital signature** หรือนำมาใช้แทนก็ได้

กระบวนการการเข้ารหัสข้อมูลจะแปลงข้อมูลที่สามารถอ่านได้ (**plaintext**) ให้เป็นอะไรที่ไร้สาระ (**ciphertext**) ส่วนการส่งสัญญาณข้อมูลนั้น ในตัวโปรแกรมเองจะต้องอาศัยอัลกอริทึมในการเข้ารหัสที่อยู่บนพื้นฐานของการใช้ **public key** (**asymmetric algorithm**) หรือ **private key** (**symmetric algorithm**)

- เมื่อใช้ **asymmetric algorithm** กุญแจก็จะเป็นสาธารณะและการเข้ารหัสการส่งสัญญาณข้อมูลก็สามารถดำเนินการโดยผู้ใดก็ได้ที่ได้รับกุญแจ อย่างไรก็ตามข้อมูลที่ถูกเข้ารหัสนี้ผู้ที่สามารถทำการถอดรหัสได้จะมีเพียงผู้ที่มี **private key** ที่มีลักษณะเดียวกันเท่านั้น

- เมื่อข้อมูลที่ทำการเข้ารหัสอยู่บนพื้นฐานของการใช้ **symmetric algorithm** การเข้ารหัสและถอดรหัส จะสามารถทำได้โดยการใช้กุญแจเดียวกัน หรือโดยการใช้กุญแจถอดรหัสที่ได้มาจากผู้ที่ทำการเข้ารหัสข้อมูลที่ทำการส่ง

ความแข็งแกร่งของการเข้ารหัสข้อมูลขึ้นอยู่กับจำนวนของบิตที่ใช้เป็นกุญแจ ซึ่งจำนวนที่ว่านี้อาจจะเปลี่ยนแปลงได้ แต่ในปัจจุบันได้มีการกำหนดเป็นมาตรฐานที่แน่นอน ดังนี้

- **40** บิต ซึ่งต้องใช้ความพยายามประมาณ **1** ล้านล้าน ครั้งในการที่จะเจาะเข้าไปด้วยกำลังอย่างป่าเถื่อน (หมายความว่าพยายามรวบรวมบิตที่เป็นไปได้ทั้งหมด) หากไม่คำนึงถึงจำนวนที่เหมือนการขู่ให้กลัวนี้ กุญแจที่มีความยาวขนาดนี้ก็สามารถรับรองได้ว่าไม่สามารถที่จะเจาะเข้าไปได้
- **56** บิต ซึ่งเรียกว่า **DES (Data Encryption Standard)** ซึ่งเป็นความยาวของกุญแจที่สูงที่สุดที่อนุญาตให้มีสำหรับการส่งออกไปนอกประเทศสหรัฐอเมริกา โดยที่ **DES key** นี้จะยิ่งเพิ่มความยากในการเจาะเข้าไปได้มากกว่า **40-bits key** แต่ก็สามารถถูกเจาะเข้าไปได้
- **128** บิต ซึ่งได้รับการพิจารณาว่าไม่สามารถเจาะเข้าไปได้โดยวิธีการที่มีอยู่ ในปัจจุบันกุญแจที่มีความยาวขนาดนี้มีสำหรับใช้ภายในประเทศสหรัฐอเมริกา แต่ซอฟต์แวร์ที่อยู่บนพื้นฐานของกุญแจขนาด **128** บิต จะไม่สามารถส่งออกไปยังประเทศอื่นได้

ถึงแม้ว่าการเข้ารหัสข้อมูลจะมีอยู่ตราบนานเท่าที่มนุษย์มีความต้องการในการแลกเปลี่ยนข้อมูลข่าวสาร แต่ในปัจจุบันได้เข้ามามีส่วนในเรื่องข่าวสารข้อมูลโดยเป็นปัจจัยสำคัญในการส่งสัญญาณข้อมูลบนเครือข่ายอินเตอร์เน็ตที่เติบโตออกไปนอกเหนือจากจินตนาการเรื่องเกี่ยวกับสายลับ และความลับในกล่องซีเรียล

12.12.3 ความปลอดภัยบนเครือข่ายอินเตอร์เน็ต

นอกเหนือจากการตรวจสอบว่าเป็นของแท้และการเข้ารหัสข้อมูลซึ่งมุ่งจุดสนใจไปยังข้อมูลข่าวสาร ยังมีเทคโนโลยีที่ขยายความปลอดภัยไปยังเครือข่ายอินเตอร์เน็ตอีกมาก หนึ่งในเทคโนโลยีเหล่านี้คือโปรโตคอลอีเมลล์ที่เรียกว่า **S/MIME (Secure/Multipurpose Internet Mail Extensions)** และอีก **2** อย่างเรียกว่า **SSL (Secure Socket Layer)** ที่ได้รับการออกแบบมาเพื่อจัดให้มีความเป็นส่วนตัวผ่านการตรวจสอบว่าเป็นของแท้ในระบบเครือข่ายแบบ **client/server** และ **PCT (Private Communication Technology)** ที่ใช้พื้นฐานบนแนวความคิดการจัดตั้งระบบเครือข่ายที่เรียกว่า **VPN (Virtual Private Network)**

12.12.3.1 S/MIME

ย้อนกลับไปสักนิด .... **MIME (Multipurpose Internet Mail Extensions)** คือโปรโตคอลที่รู้จักกันดีและถูกใช้อย่างแพร่หลายในการส่งอีเมลล์บนเครือข่ายอินเตอร์เน็ต ที่ได้รับการพัฒนาโดย **IETF** โดย **MIME** ได้รับการออกแบบให้อนุญาตให้ข่าวสารทางจดหมายไม่เพียงจะมีเฉพาะข้อความ แต่ยังรวมถึงเสียง รูปภาพ สัญญาณเสียง และสัญญาณภาพ การทำเช่นนี้ได้ **MIME** จะใช้ส่วนหัว เพื่อระบุเนื้อหาของข่าวสาร นั่นคือถ้าข่าวสารนั้นประกอบด้วยไฟล์เสียง ส่วนหัวก็จะบอกไว้ ที่ฝ่ายเครื่องผู้รับซอฟต์แวร์สามารถใช้ข้อมูลในส่วนหัวนี้ในการเรียกใช้โปรแกรมที่เหมาะสมเพื่อที่จะแสดงภาพ ทำให้มีเสียง หรือสื่อประเภทอื่นๆ ถึงแม้ว่า **MIME** จะกำหนด

มาตรฐานของการส่งสัญญาณข้อมูลของเอกสารแบบมัลติมีเดีย แต่ก็ไม่มีการจัดให้มีวิธีในการรักษาความปลอดภัย ดังนั้นเพื่อสนับสนุนการปฏิบัติเกี่ยวกับเรื่องนี้ **S/MIME** จึงถูกคิดค้นขึ้น **S/MIME** จึงเป็น **MIME** ที่สนับสนุนสำหรับ **digital signature** และ **encryption**

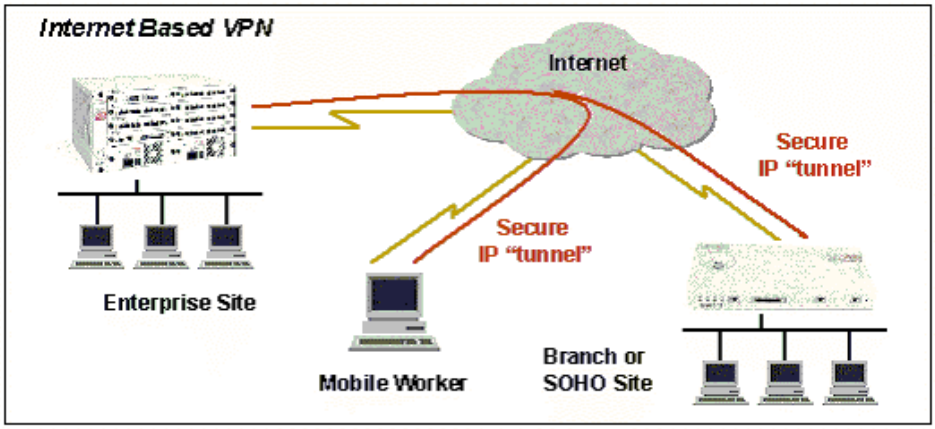
12.12.3.2 SSL และ PCT

SSL ได้รับการพัฒนาโดยบริษัท **Netscape Communication** ส่วน **PCT** ได้รับการพัฒนาเป็นฉบับร่างและเสนอให้กับ **IETF** โดยบริษัท **Microsoft** ทั้ง **SSL** และ **PCT** มีวัตถุประสงค์เดียวกัน คือ เพื่อทำให้มั่นใจในความเป็นส่วนตัวในการสื่อสารโดยการใช้วิธีตรวจสอบว่าเป็นของแท้และการเข้ารหัสข้อมูลที่ส่งผ่านระหว่างเครื่องไคลเอนต์กับเครื่องเซิร์ฟเวอร์ ถึงแม้ว่าโปรโตคอลทั้งสองจะมีประเด็นที่แน่นอนแตกต่างกัน แต่ทั้งคู่ก็อนุญาตให้โปรโตคอลที่มีความสัมพันธ์กับโปรแกรมประยุกต์ เช่น **HTTP, FTP** และ **Telnet** ทำงานบนโปรโตคอลทั้งคู่โดยปราศจากปัญหาได้ โปรโตคอลทั้งคู่จะเริ่มทำการสนทนาด้วยการสร้างข้อตกลงเบื้องต้นสำหรับการแลกเปลี่ยนข่าวสารระหว่างเครื่องไคลเอนต์และเครื่องเซิร์ฟเวอร์ เพื่อให้เครื่องคอมพิวเตอร์ที่จะทำการสื่อสารกันทำความตกลงเกี่ยวกับขั้นตอนวิธีในการเข้ารหัสข้อมูลพร้อมทั้งกุญแจที่ใช้ และตรวจสอบว่าเครื่องคอมพิวเตอร์ทั้งคู่เป็นฝ่ายเดียวกัน ในทันทีที่ทำทุกสิ่งเหล่านี้แล้วการสื่อสารระหว่างเครื่องไคลเอนต์กับเครื่องเซิร์ฟเวอร์ก็จะเกิดขึ้น และข้อมูลก็จะถูกทำการเข้ารหัสผ่านการสนทนา

12.12.3.3 ระบบเครือข่ายเสมือนส่วนตัว (Virtual private network – VPN)

VPN เป็นปรากฏการณ์ที่นับว่าใหม่ที่สุด แต่ก็เพิ่มประชากรได้อย่างรวดเร็ว เพราะเป็นวิธีที่มีประสิทธิภาพทางด้านราคาสูง ด้วยการใช้โทรคมนาคมที่เป็นสาธารณะและเครือข่ายอินเตอร์เน็ต ในการจัดให้มีความปลอดภัย ความเป็นส่วนตัว สำหรับการสื่อสารระหว่างเครื่องคอมพิวเตอร์ด้วยกันภายใน **LANs** และระหว่างเครื่องคอมพิวเตอร์กับระบบเครือข่ายของบริษัท จึงอาจเรียกได้ว่าเป็นเครือข่ายเสมือนส่วนตัว จุดสำคัญ คือ **VPNs** ใช้เครือข่ายอินเตอร์เน็ตเป็นการรวมสื่อการสื่อสารให้เป็นส่วนตัว ดังนั้นจึงไม่จำเป็นต้องคิดราคาการใช้สายสัญญาณเช่า (**Least line**) หรือทางเลือกอื่นของระบบเครือข่ายส่วนตัว ความปลอดภัยบน **VPN** เกี่ยวข้องกับการเข้ารหัสข้อมูลและวิธีการขนส่งแพ็กเก็ตข้อมูลไปบนเครือข่ายอินเตอร์เน็ตผ่านการเชื่อมต่อที่เรียกว่า **tunnel** ซึ่งก่อตั้งให้มีความเป็นเส้นทางส่วนตัวระหว่างเครื่องคอมพิวเตอร์ที่สื่อสารกันแบบชั่วคราว

สถาปัตยกรรมหลักในการทำ **tunnel** มี 2 แบบคือ **client-initiated** กับ **client-transparent** โดยการทำ **tunnel** แบบ **client-initiated** ต้องการทันแนลซอฟต์แวร์ทั้งฝั่งไคลเอ็นต์ และฝั่งเซิร์ฟเวอร์ (หรือเกตเวย์) ส่วนการทำ **tunnel** แบบ **client-transparent** โดยทั่วไปจะทำอยู่ที่ไซต์ส่วนกลางขององค์กร หรือทำให้อยู่ที่จุดเชื่อมต่อของ **ISP** ซึ่งให้บริการแก่ไซต์ส่วนกลางขององค์กรก็ได้ ด้วยการใช้ไคลเอ็นต์ซอฟต์แวร์ และทันแนลเซิร์ฟเวอร์ที่ไซต์ส่วนกลางขององค์กร ทำให้ **ISP** ไม่จำเป็นต้องสนับสนุนการทำทันแนลแต่อย่างใด โดยไคลเอ็นต์ซอฟต์แวร์ และทันแนลเซิร์ฟเวอร์จะเริ่มสร้างทันแนล ต่อจากนั้นจะตรวจสอบโดยใช้หมายเลขยูสเซอร์และรหัสผ่าน ในการติดต่อขั้นนี้ก็สามารถเข้ารหัสได้ เมื่อเชื่อมต่อเรียบร้อยแล้วการติดต่อสื่อสารสามารถทำได้โดยเสมือนว่าไม่มี **ISP** เป็นตัวเชื่อมการติดต่อ



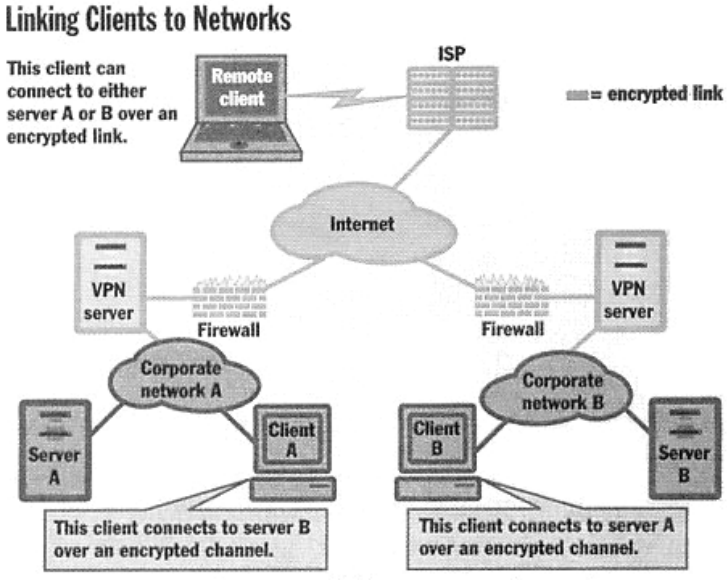
รูปที่ 12 – 10 Virtual Private Network

อีกวิธีหนึ่งหากต้องการเชื่อมต่อแบบทรานส์พาเรนต์ผ่านไปยังไคลเอ็นต์ที่จุดเชื่อมต่อของ **ISP** จำเป็นต้องมีทันแนลอีนาเบิลแอคเซสเซิร์ฟเวอร์ (**tunnel-enabled access server**) และบางทีอาจรวมไปถึงเราท์เตอร์ด้วย เริ่มจากไคลเอ็นต์หมุนโทรศัพท์ไปยังแอคเซสเซิร์ฟเวอร์ (โดยแอคเซสเซิร์ฟเวอร์สามารถแยกแยะโดยใช้หมายเลขยูสเซอร์ หรือให้ยูสเซอร์เลือกจากเมนู) เพื่อเชื่อมต่อแบบทันแนลไปยังปลายทาง หลังจากนั้นแอคเซสเซิร์ฟเวอร์จะสร้างการเชื่อมต่อแบบทันแนลกับทันแนลเซิร์ฟเวอร์แล้ว ตรวจสอบโดยใช้รหัสผ่าน แล้วไคลเอ็นต์ก็สามารถสร้างเซสชันโดยตรงกับทันแนลเซิร์ฟเวอร์ผ่านทางทันแนลดังกล่าว เสมือนว่าทั้งสองเชื่อมต่อกันโดยตรง ในขณะที่วิธีนี้มีข้อได้เปรียบตรงที่ไม่ต้องการซอฟต์แวร์พิเศษบนฝั่งไคลเอ็นต์ แต่ไคลเอ็นต์ต้องหมุนโทรศัพท์ไปยังแอคเซสเซิร์ฟเวอร์ที่กำหนดไว้เท่านั้น สำหรับโปรโตคอลที่รองรับการสร้าง **tunnel** ที่มีให้เลือกใช้คือ **PPTP (Point-to-Point Tunneling Protocol)** และ **Layer Two Forwarding (L2F)**

PPTP เป็นโปรโตคอลซึ่งได้รับการพัฒนาโดยบริษัทไมโครซอฟต์ และเพิ่มความสำคัญในการสนับสนุนระบบเครือข่ายในอุตสาหกรรม โปรโตคอลนี้เกิดจากการขยายโปรโตคอลมาตรฐาน **PPP (Point to Point Protocol)** ที่ใช้ในการจัดหีบห่อ **datagram** และส่งออกไปผ่านการเชื่อมต่อของ **TCP/IP** โดย **PPTP** จะห่อหุ้ม **PPP packet** ที่เข้ารหัสไว้ในสิ่งห่อหุ้มที่ปลอดภัย ที่เหมาะสมสำหรับการขนส่งผ่านเครือข่ายอินเตอร์เน็ต นอกจากนั้นยังจัดตั้ง รักษา และยุติการจัดตั้ง **tunnel** ระหว่างเครื่องคอมพิวเตอร์ที่สื่อสารกัน ประการสำคัญที่แตกต่างกันของสองโพรโตคอลนี้คือ **PPTP** จะสร้างทันแนลโดยห่อ **PPP** แพ็กเกตไว้ใน **IP** ซึ่งเป็นโพรโตคอลที่ทำงานในเลเยอร์ที่สาม ในขณะที่ **L2F** ทำงานในเลเยอร์ที่สอง โดยใช้เฟรมรีเลย์หรือ **ATM** ใช้ในการทำ **tunnel**

PPTP สามารถใช้เป็นแบบ **client-initiated** (ซึ่งทรานส์พาเรนต์สำหรับ **ISP**) หรือใช้เป็นแบบ **client-transparent** ก็ได้ทั้งสองแบบนี้ในปัจจุบันมีใช้เฉพาะในวินโดว์ส **NT** เท่านั้น ซึ่งต้องการทั้ง **NT** ไคลเอ็นต์และ **NT** เซิร์ฟเวอร์ ในทางตรงกันข้าม **L2F** ต้องการการสนับสนุนในแอคเซสเซิร์ฟเวอร์และในเราท์เตอร์ ดังนั้นในการใช้งาน **ISP** ต้องสนับสนุน **L2F** ด้วยระบบการป้องกันของ **L2F** มีการจัดเตรียมบางอย่างที่ **PPTP** ไม่มี ข้อได้เปรียบหลักของ **PPTP** คือสนับสนุนทั้งไคลเอ็นต์ และทันแนลเซิร์ฟเวอร์สำหรับ **PPTP** มีมาพร้อมกับ **Windows NT 4.0** และในส่วนของ **Windows 98** กำลังอยู่ในช่วงการพัฒนา ข้อได้เปรียบอื่น ๆ คือ **PPTP** สนับสนุนการทำโฟลว์คอนโทรลทำให้ทั้งไคลเอ็นต์และเซิร์ฟเวอร์ปลอดภัยจากเหตุการณ์ข้อมูลโอเวอร์โฟลว์, ช่วยเพิ่มประสิทธิภาพโดยลดการดรอปแพ็กเกตลง รวมไปถึงการส่งซ้ำด้วย อย่างไรก็ตาม **PPTP** ก็ยังคงต้องการ **IP** (แม้ว่า

จะสามารถสร้างทันแนลให้แก่ **IPX** และ **NetBEUI** ได้เช่นเดียวกับ **PPP**) และปัจจุบันใน **PPTP** ยังไม่มีความสามารถออเทนทิเคตของปลายทั้งสองด้านของทันแนลจึงจำเป็นต้องใช้ความสามารถของ **PPP** ในการตรวจสอบ



รูปที่ **12 – 11 client-initiated VPN**

การรวมข้อดีของทั้งสองโพรโตคอลเข้าด้วยกันในชื่อ **"Layer Two Tunneling Protocol (L2TP)"** ซึ่งในด้านการจัดการความปลอดภัยใช้ **Secure IP** หรือ **IPSEC** เป็นพื้นฐานในการเข้ารหัสในการเชื่อมต่อระหว่างปลายทั้งสองของ **L2TP** (มาตรฐานการเข้ารหัสยังไม่มีใน **PPTP** หรือใน **L2F**) นอกจากนั้น **L2TP** ยังสนับสนุนการทำทันแนลหลาย ๆ อันพร้อมกันบนไคลเอ็นต์เพียงตัวเดียว ซึ่งคุณสมบัตินี้ยิ่งทวีความสำคัญมากขึ้นในอนาคต เมื่อทันแนลสามารถสนับสนุนการจองแบนด์วิธและ **QoS**

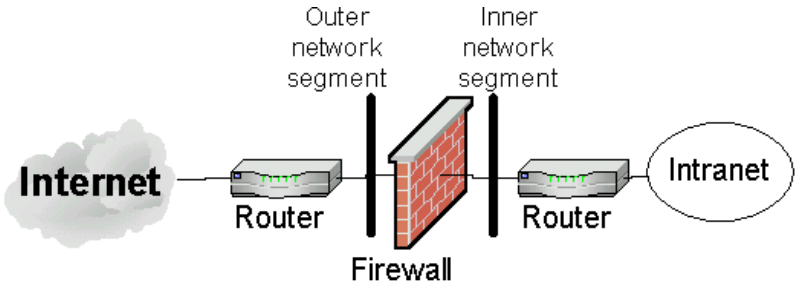
12.13 การจัดตั้งไฟร์วอลล์

จากที่อธิบายในหัวข้อที่ผ่านมาจะเห็นได้ว่าโปรโตคอลที่ปลอดภัย การเข้ารหัสข้อมูล และ **digital signature** เป็นสิ่งที่จำเป็นสำหรับคุ้มครองข้อมูลที่เดินทางอยู่บนเครือข่ายอินเตอร์เน็ต แต่ถึงแม้ว่าจะสามารถที่จะเก็บข้อมูลนั้นให้รอดพ้นจากสายตาที่คอยสอดส่องได้ แต่ในทางกายภาพแล้วก็ไม่อาจทำให้รอดพ้นจากผู้บุกรุกจากเครือข่ายอินเตอร์เน็ตได้ ซึ่งงานที่ว่านี้ไฟร์วอลล์จะสนับสนุนได้เป็นอย่างดี และสามารถทำได้โดยการขยายระบบเครือข่ายเพียงเล็กน้อย ด้วยการเพิ่มหน่วยที่เรียกว่า “พร็อกซี่” หรือเครื่องพร็อกซี่เซิร์ฟเวอร์

12.13.1 Firewall

ในความหมายทางด้านการก่อสร้างแล้ว ไฟร์วอลล์ จะหมายถึง กำแพงที่เอาไว้ป้องกันไฟไม่ให้ลุกลามไปยังส่วนอื่นๆ ส่วนทางด้านคอมพิวเตอร์นั้นก็จะมีความหมายคล้ายๆ กันก็คือ เป็นระบบที่เอาไว้ป้องกันอันตรายจากอินเตอร์เน็ตหรือเน็ตเวิร์กภายนอกนั่นเอง ไฟร์วอลล์ เป็นคอมโพเน็นต์หรือกลุ่มของคอมโพเน็นต์ที่ทำหน้าที่ในการควบคุมการเข้าถึงระหว่างเน็ตเวิร์กภายนอกหรือเน็ตเวิร์กที่เราคิดว่าไม่ปลอดภัย กับเน็ตเวิร์กภายในหรือเน็ตเวิร์กที่เราต้องการจะป้องกัน โดยที่คอมโพเน็นต์นั้นอาจจะเป็นเราท์เตอร์ คอมพิวเตอร์ หรือเน็ตเวิร์ก ประกอบกันก็ได้ ขึ้นอยู่กับวิธีการหรือโครงสร้างสถาปัตยกรรมของไฟร์วอลล์ที่ใช้

ระบบเครือข่ายที่มีไฟร์วอลล์เทียบได้กับกำแพงกันไฟภายในบ้าน คือสิ่งกีดขวางที่ได้รับการออกแบบมาเพื่อป้องกันการเกิดบางสิ่งที่ไม่ดีในบ้าน ไฟร์วอลล์คือสิ่งที่จะกันไม่ให้ไฟลุกลามไปจนไม่สามารถควบคุมได้ บนระบบเครือข่าย ไฟร์วอลล์ถูกใช้เป็นหลักในการกันผู้บุกรุกจากภายนอก และในทางตรงกันข้ามกับบทบาท ยังใช้ในการกันการขนส่งข้อมูลจากภายในไปยังไซต์ต่างๆ ที่อยู่นอกระบบเครือข่ายด้วย ตามปกติไฟร์วอลล์จะถูกตั้งให้กีดขวางที่เราท์เตอร์บริดจ์ หรือเกตเวย์ ที่อยู่ระหว่างระบบเครือข่ายกับโลกภายนอก ซึ่งไฟร์วอลล์นี้จะเป็นเหมือนประตูทางเข้าและออกจากระบบเครือข่ายและมีทหารยามเฝ้าประตู โดยจะเฝ้าดูการขนส่งข้อมูล ตรวจสอบข้อมูลแต่ละแพ็กเก็ต เพื่อตกลงใจว่าจะกีดกันแพ็กเก็ตใดและปล่อยให้แพ็กเก็ตใดผ่านเข้ามาได้ ดังแสดงตามรูปที่ 12 – 12 การควบคุมการเข้าถึงของไฟร์วอลล์นั้น สามารถทำได้ในหลายระดับและหลายรูปแบบขึ้นอยู่ชนิดหรือเทคโนโลยีของไฟร์วอลล์ที่นำมาใช้ เช่น เราสามารถกำหนดได้ว่าจะให้มีการเข้ามาใช้บริการอะไรได้บ้าง จากที่ไหน เป็นต้น



รูปที่ 12 – 12 ไฟร์วอลล์ถูกจัดตั้งขึ้นเพื่อกั้นระหว่างอินเตอร์เน็ตกับเครือข่ายภายใน

ไฟร์วอลล์สามารถช่วยเพิ่มความปลอดภัยให้กับระบบได้โดย

- บังคับใช้นโยบายด้านความปลอดภัย โดยการกำหนดกฎให้กับไฟร์วอลล์ว่าจะอนุญาตหรือไม่ให้ใช้บริการชนิดใด
- บันทึกข้อมูล กิจกรรมต่างๆ ที่ผ่านเข้าออกเน็ตเวิร์กได้อย่างมีประสิทธิภาพ
- ทำให้การพิจารณาดูแลและการตัดสินใจด้านความปลอดภัยของระบบเป็นไปได้ง่ายขึ้น เนื่องจากการติดต่อทุกชนิดกับเน็ตเวิร์กภายนอกจะต้องผ่านไฟร์วอลล์ การดูแลที่จุดนี้เป็นการดูแลความปลอดภัยในระดับของเน็ตเวิร์ก (**Network-based Security**)
- ป้องกันเน็ตเวิร์กบางส่วนจากการเข้าถึงของเน็ตเวิร์กภายนอก เช่นถ้าหากเรามีบางส่วนที่ต้องการให้ภายนอกเข้ามาใช้บริการ (เช่นถ้ามีเว็บเซิร์ฟเวอร์) แต่ส่วนที่เหลือไม่ต้องการให้ภายนอกเข้ามากรณีเช่นนี้เราสามารถใช้ไฟร์วอลล์ช่วยได้
- ไฟร์วอลล์บางชนิดสามารถป้องกันไวรัสได้ โดยจะทำการตรวจไฟล์ที่โอนย้ายผ่านทางโปรโตคอล **HTTP**, **FTP** และ **SMTP**

ถึงแม้ว่าไฟร์วอลล์จะสามารถช่วยเพิ่มความปลอดภัยให้กับเน็ตเวิร์กได้มากโดยการตรวจดูข้อมูลที่ผ่านเข้าออก แต่อย่าลืมว่าสิ่งเหล่านี้ไม่สามารถป้องกันได้จากการใช้ไฟร์วอลล์

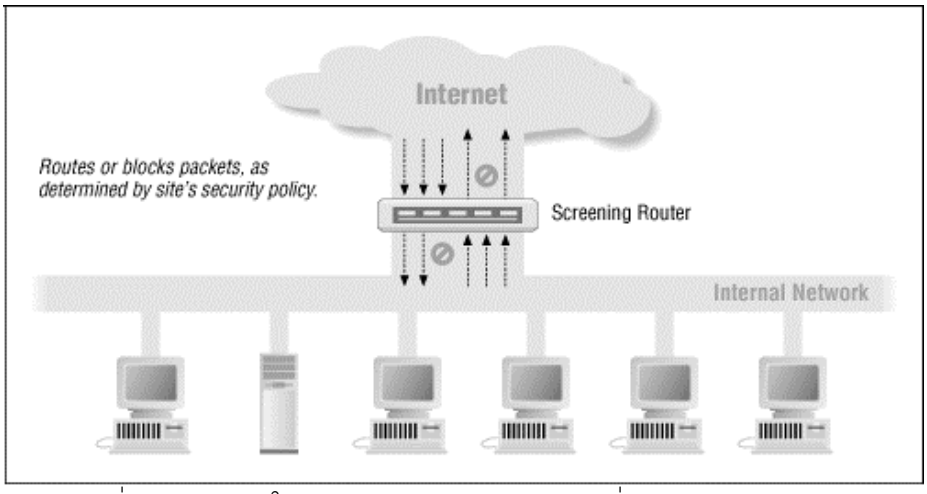
- อันตรายที่เกิดจากเน็ตเวิร์กภายใน ไม่สามารถป้องกันได้เนื่องจากอยู่ภายในเน็ตเวิร์กเองไม่ได้ผ่านไฟร์วอลล์เข้ามา

- อันตรายจากภายนอกที่ไม่ได้ผ่านเข้ามาทางไฟร์วอลล์ เช่นการ **Dial-up** เข้ามายังเน็ตเวิร์กภายในโดยตรงโดยไม่ได้ผ่านไฟร์วอลล์
- อันตรายจากวิธีใหม่ๆ ที่เกิดขึ้น ทุกวันนี้มีการพบช่องโหว่ใหม่ๆ เกิดขึ้นทุกวัน เราไม่สามารถไว้ใจไฟร์วอลล์โดยการติดตั้งเพียงครั้งเดียวแล้วก็หวังให้มันปลอดภัยตลอดไป เราต้องมีการดูแลรักษาอย่างต่อเนื่องสม่ำเสมอ
- ไวรัส ถึงแม้จะมีไฟร์วอลล์บางชนิดที่สามารถป้องกันไวรัสได้ แต่ก็ยังไม่มีไฟร์วอลล์ชนิดใดที่สามารถตรวจสอบไวรัสได้ในทุกๆ โปรโตคอล

ไฟร์วอลล์แบ่งตามเทคโนโลยีที่ใช้ในการตรวจสอบและควบคุม ได้ **3** ชนิดคือ **Packet Filtering, Proxy Service** และ **Stateful Inspection** ซึ่งจะได้อธิบายรายละเอียดของไฟร์วอลล์แต่ละชนิดในหัวข้อต่อไป

12.13.1.1 Packet Filtering

Packet Filter คือเราท์เตอร์ที่ทำการหาเส้นทางและส่งต่อออกไปอย่างมีเงื่อนไข โดยจะพิจารณาจากข้อมูลส่วนที่อยู่ในส่วนหัวของแพ็กเก็ตที่ผ่านเข้ามา เทียบกับกฎที่กำหนดไว้และตัดสินว่าควรจะทิ้งแพ็กเก็ตนั้นไปหรือว่าจะยอมให้แพ็กเก็ตนั้นผ่านไปได้ ในการพิจารณาส่วนหัว **Packet Filter** จะตรวจสอบในระดับของ **Internet Layer** และ **Transport Layer** ใน **Internet Model** ซึ่งใน **Internet Layer** จะมีแอตทริบิวต์ที่สำคัญต่อ **Packet Filtering** คือ แอดเดรสต้นทาง แอดเดรสปลายทาง และชนิดของโปรโตคอล (**TCP UDP** และ **ICMP**) และในระดับของ **Transport Layer** มีแอตทริบิวต์ที่สำคัญคือ พอร์ตต้นทาง พอร์ตปลายทาง แฟล็ก (**Flag** ซึ่งจะมีเฉพาะในเฮดเดอร์ของแพ็กเก็ต **TCP**) และชนิดของ **ICMP message** (ในแพ็กเก็ต **ICMP**) ซึ่งพอร์ต **Transport Layer** คือทั้ง **TCP** และ **UDP** นั้นจะเป็นสิ่งที่บอกถึงแอพพลิเคชันที่แพ็กเก็ตนั้นต้องการติดต่อด้วยเช่น พอร์ต **80** หมายถึง **HTTP,** พอร์ต **21** หมายถึง **FTP** เป็นต้น ดังนั้นเมื่อ **Packet Filter** พิจารณาส่วนหัวของแพ็กเก็ต จึงทำให้สามารถควบคุมแพ็กเก็ตที่มาจากที่ต่างๆ และมีลักษณะต่างๆ (ดูได้จากแฟล็กของแพ็กเก็ตหรือชนิดของ **ICMP** ในแพ็กเก็ต **ICMP**) ได้ เช่น ห้ามแพ็กเก็ตทุกชนิดจาก **crack.cracker.net** เข้ามายังเน็ตเวิร์ก **203.154.207.0/24** หรือห้ามแพ็กเก็ตที่มีไอพีต้นทางอยู่ในเน็ตเวิร์ก **203.154.207.0/24** ผ่านเราเตอร์เข้ามา



รูปที่ **12 – 13** การใช้ **Screening Router** ทำหน้าที่ **Packet Filtering**

Packet filtering สามารถอิมพลีเมนต์ได้จาก 2 แพล็ตฟอร์ม คือ

- เราท์เตอร์ซึ่งมีความสามารถในการทำ **Packet Filtering** (มีในเราท์เตอร์ส่วนใหญ่)
- คอมพิวเตอร์ที่ทำหน้าที่เป็นเราท์เตอร์

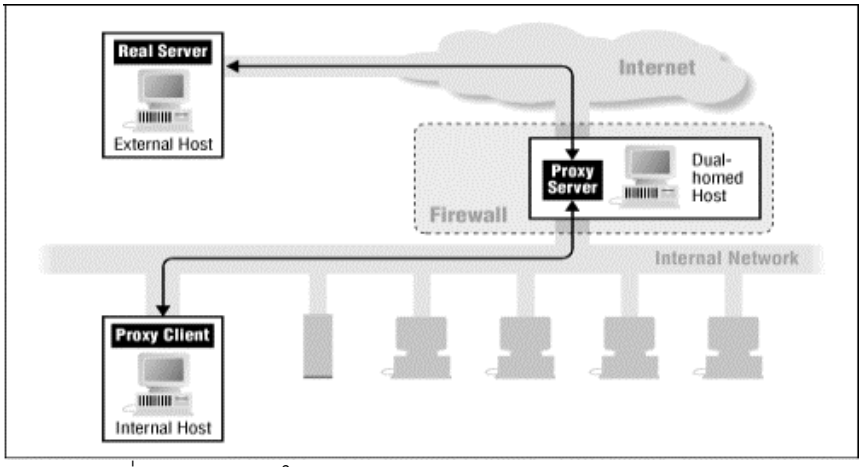
ตารางที่ **12 – 1** เปรียบเทียบข้อดีข้อเสียในการเลือกอุปกรณ์มาทำหน้าที่ **Packet Filtering**

	ข้อดี	ข้อเสีย
เราท์เตอร์	ประสิทธิภาพสูงมีจำนวนอินเตอร์เฟสมาก	เพิ่มเติมฟังก์ชันการทำงานได้ยาก, อาจต้องการหน่วยความจำมาก
คอมพิวเตอร์ที่ทำหน้าที่เป็นเราท์เตอร์	เพิ่มฟังก์ชันการทำงานได้ไม่จำกัด	ประสิทธิภาพปานกลาง,จำนวนอินเตอร์เฟสน้อย,อาจมีความเสี่ยงจากระบบปฏิบัติการที่ใช้

ในการตัดสินใจว่าแพ็กเก็ตใดๆ “ผ่านการพิจารณา” หรือ “ไม่ผ่าน” นั้น ไฟร์วอลล์จะอาศัยกลไกที่เรียกว่า **packet filter** และตารางที่มีรายการของแอดเดรสที่ “ยอมรับได้” กับ “ยอมรับไม่ได้” เมื่อมีแพ็กเก็ตผ่านเข้ามา ไฟร์วอลล์จะตรวจสอบแอดเดรสของแหล่งต้นทางและปลายทาง และ/หรือพอร์ตที่แพ็กเก็ตนั้นถูกส่งมา ถ้าแอดเดรส หรือพอร์ตของแพ็กเก็ตนั้นเข้าข่าย “ยอมรับไม่ได้” ไฟร์วอลล์ก็จะกันแพ็กเก็ตนั้นไว้ แต่ถ้าแอดเดรส หรือพอร์ตของแพ็กเก็ตนั้นเข้าข่าย “ยอมรับได้” ไฟร์วอลล์ก็จะส่งผ่านเข้ามา ด้วยวิธีนี้จึงสามารถพูดได้ว่า ไฟร์วอลล์สามารถที่จะกันทุกแพ็กเก็ตที่มีแอดเดรสไปยังปลายทาง หรือแพ็กเก็ตที่ส่งไปยังพอร์ตที่เกี่ยวกับการให้บริการโดยเฉพาะ เช่น **Telnet** ได้ ในระดับที่สูงขึ้นไป ไฟร์วอลล์อาจจะทำหน้าที่เป็นแอพพลิเคชั่นโปรแกรม ซึ่งแทนที่จะตรวจสอบข้อมูลการกำหนดแอดเดรส แต่จะตรวจสอบแพ็กเก็ตด้วยตัวเอง ทำการละทิ้งแพ็กเก็ตที่ไม่ผ่านเกณฑ์ ตัวอย่างเช่น ไฟร์วอลล์ในลักษณะนี้สามารถนำมาใช้ในการกรองข่าวสารทางอีเมลล์ซึ่งอยู่บนพื้นฐานของเนื้อหาที่ไม่เหมาะสม หรือคุณสมบัติที่สำคัญอย่างอื่นได้

12.13.1.2 พร็อกซี่ **(Proxy)**

พร็อกซี่หรือ **Application Gateway** เป็นแอพพลิเคชันโปรแกรมที่ทำงานอยู่บนไฟร์วอลล์ที่ตั้งอยู่ระหว่างเน็ตเวิร์ก 2 ระบบ ทำหน้าที่เพิ่มความปลอดภัยของระบบเน็ตเวิร์กโดยการควบคุมการเชื่อมต่อระหว่างเน็ตเวิร์กภายในและภายนอก พร็อกซี่จะช่วยเพิ่มความปลอดภัยได้มากเนื่องจากมีการตรวจสอบข้อมูลถึงในระดับของ **Application Layer** พร็อกซี่เซิร์ฟเวอร์ **(Proxy Server)** เป็นส่วนหนึ่งของไฟร์วอลล์ ในการจัดตั้งสิ่งกีดขวางระหว่างระบบเครือข่ายภายในกับโลกภายนอก อย่างไรก็ตามในกรณีนี้ พร็อกซี่จะให้บริการกับระบบเครือข่ายโดยอยู่ในเครื่องคอมพิวเตอร์เครื่องใดเครื่องหนึ่งที่ใช้ในการ **access** เครือข่ายอินเตอร์เน็ต ด้วยการแสดงเป็น **IP address** เดียวต่อโลกภายนอก จึงเป็นการซ่อนแอดเดรสของคอมพิวเตอร์เครื่องอื่นที่อยู่ในระบบเครือข่ายได้ และพร็อกซี่จะป้องกันการบุกรุกอย่างเจ้าเล่ห์ ที่เรียกว่า “**spoofing**” ซึ่งผู้บุกรุกปลอมตัวเป็นเครื่องคอมพิวเตอร์ในระบบเครือข่าย ไม่ว่าจะเป็นการโจมตีจากภายใน หรือขัดขวางข้อมูลที่ส่งไปยังเครื่องคอมพิวเตอร์ที่เสแสร้งว่าเป็น และอาจจะใช้พร็อกซี่ในการจำกัดการ **access** ไปยังเครือข่ายอินเตอร์เน็ตได้เช่นเดียวกับไฟร์วอลล์ ตัวอย่างเช่นการป้องกันไม่ให้พนักงานไปเยี่ยมชมไซต์ที่ไม่พึงปรารถนาซึ่งไม่เกี่ยวข้องกับงานที่ทำ



รูปที่ 12 – 14 การใช้ Dual-homed Host เป็น Proxy Server

เมื่อไคลเอนต์ต้องการใช้บริการภายนอก ไคลเอนต์จะทำการติดต่อไปยังพร็อกซี่ก่อน ไคลเอนต์จะเจรจา (Negotiate) กับพร็อกซี่ เพื่อให้พร็อกซี่ติดต่อไปยังเครื่องปลายทางให้ เมื่อพร็อกซี่ติดต่อไปยังเครื่องปลายทางให้แล้วจะมีการเชื่อมต่อ 2 การเชื่อมต่อ คือ ไคลเอนต์กับพร็อกซี่ และพร็อกซี่กับเครื่องปลายทาง โดยที่พร็อกซี่จะทำหน้าที่รับข้อมูลและส่งต่อข้อมูลให้ใน 2 ทิศทาง ทั้งนี้พร็อกซี่จะทำหน้าที่ในการตัดสินใจว่าจะให้มีการเชื่อมต่อกันหรือไม่ จะส่งต่อแพ็กเก็ตให้หรือไม่

12.13.1.3 Stateful Inspection Technology

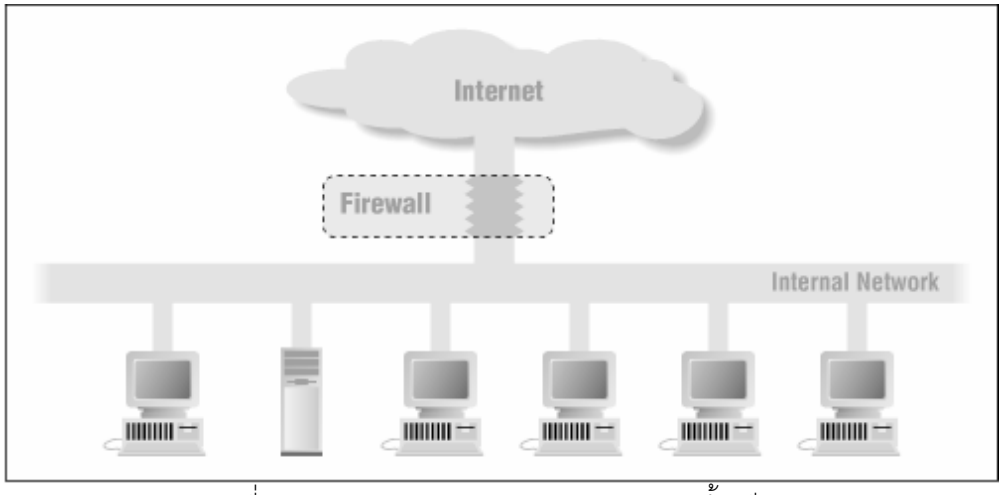
โดยปกติแล้ว **Packet filtering** แบบธรรมดา (ที่เป็น **Stateless** แบบที่มีอยู่ในเราท์เตอร์ทั่วไป) จะควบคุมการเข้าออกของแพ็กเก็ตโดยพิจารณาข้อมูลจากส่วนหัวของแต่ละแพ็กเก็ต นำมาเทียบกับกฎที่มีอยู่ ซึ่งกฎที่มีอยู่ก็จะเป็นกฎที่สร้างจากข้อมูลส่วนที่อยู่ในส่วนหัวของแพ็กเก็ตข้อมูลเท่านั้น ดังนั้น **Packet Filtering** แบบธรรมดาจึงไม่สามารถทราบได้ว่า แพ็กเก็ตนี้อยู่ส่วนใดของการเชื่อมต่อ เป็นแพ็กเก็ตที่เข้ามาติดต่อใหม่หรือเปล่า หรือว่าเป็นแพ็กเก็ตที่เป็นส่วนของการเชื่อมต่อที่เกิดขึ้นแล้ว เป็นต้น

Stateful Inspection เป็นเทคโนโลยีที่เพิ่มเข้าไปใน **Packet Filtering** โดยในการพิจารณาว่าจะยอมให้แพ็กเก็ตผ่านไปนั้น แทนที่จะดูข้อมูลจากส่วนหัวของแพ็กเก็ตข้อมูลเพียงอย่างเดียว **Stateful Inspection** จะนำเอาส่วนข้อมูลของแพ็กเก็ต (**message content**) และข้อมูลที่ได้จากแพ็กเก็ตก่อนหน้านี้ที่ได้ทำการบันทึกเอาไว้ นำมาพิจารณาด้วย จึงทำให้สามารถระบุได้ว่าแพ็กเก็ตใดเป็นแพ็กเก็ตที่ติดต่อเข้ามาใหม่ หรือว่าเป็นส่วนหนึ่งของการเชื่อมต่อที่มีอยู่แล้ว

12.13.2 โครงสร้างสถาปัตยกรรมของไฟร์วอลล์ (Firewall Architecture)

12.13.2.1 Single Box Architecture

Single Box Architecture เป็นโครงสร้างสถาปัตยกรรมแบบง่ายๆ ที่มีคอมโพเน็นต์ทำหน้าที่เป็นไฟร์วอลล์เพียงอันเดียวตั้งอยู่ระหว่างเน็ตเวิร์กภายในกับเน็ตเวิร์กภายนอก ข้อดีของวิธีนี้ก็คือการที่มีเพียงจุดเดียวที่หน้าที่ไฟร์วอลล์ทั้งหมด ควบคุมการเข้าออกของข้อมูล ทำให้ดูแลได้ง่าย เป็นจุดสนใจในการดูแลความปลอดภัยเน็ตเวิร์ก ในทางกลับกันข้อเสียของวิธีนี้ก็คือ การที่มีเพียงจุดเดียวนี้ ทำให้มีความเสี่ยงสูง หากมีการคอนฟิกูเรชันผิดพลาดหรือมีช่องโหว่เพียงเล็กน้อย การผิดพลาดเพียงจุดเดียวอาจทำให้ระบบถูกเจาะได้



รูปที่ **12 – 15 Firewall Architecture** แบบชั้นเดียว

คอมโพเน็นต์ที่ใช้ในโครงสร้างแบบนี้อาจเป็น **Screening Router, Dual-Homed Host** หรือ **Multi-purposed Firewall Box** ก็ได้

1) Screening Router

เราสามารถใช้เราท์เตอร์ทำ **Packet Filtering** ได้ วิธีนี้จะทำให้ประหยัดค่าใช้จ่ายเนื่องจากส่วนใหญ่จะใช้เราท์เตอร์ต่อกับเน็ตเวิร์กภายนอกอยู่แล้ว แต่วิธีนี้อาจไม่ยืดหยุ่นมากนักในการตั้งค่าการใช้งาน ดังนั้นโครงสร้างแบบนี้จึงเหมาะสำหรับ

- ระบบเครือข่ายที่มีการป้องกันความปลอดภัยในระดับของโฮสต์เป็นอย่างดี
- มีการใช้โปรโตคอลไม่มาก และโปรโตคอลที่ใช้ก็เป็นโปรโตคอลที่ไม่ซับซ้อน
- ต้องการไฟร์วอลล์ที่มีความเร็วสูง

2) Dual-Homed Host

เราสามารถใช้ **Dual-Homed Host** (คอมพิวเตอร์ที่มีการ์ดเชื่อมต่อระบบเครือข่ายอย่างน้อย 2 อัน) ใช้การบริการเป็นพร็อกซี่ให้กับเครื่องภายในเน็ตเวิร์ก โครงสร้างแบบนี้เหมาะสำหรับ

- ระบบเครือข่ายที่มีการใช้งานอินเตอร์เน็ตค่อนข้างน้อย
- ระบบเครือข่ายที่ไม่ได้มีข้อมูลสำคัญๆ

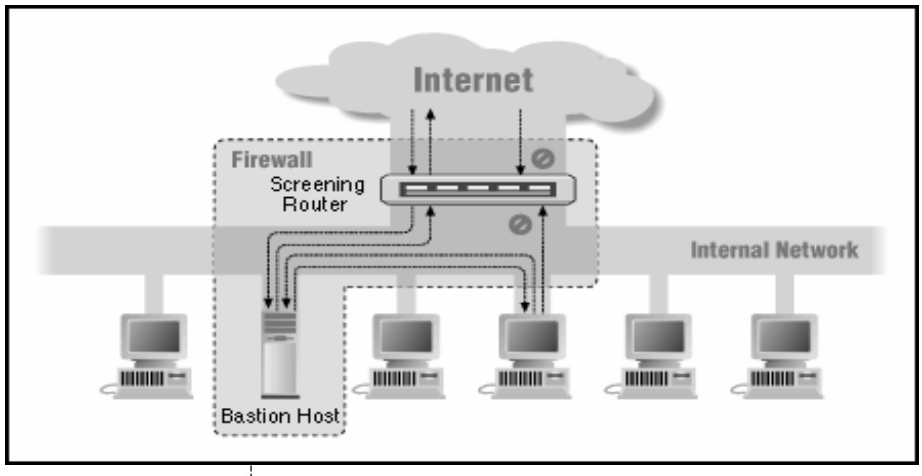
3) Multi-purposed Firewall Box

มีผลิตภัณฑ์หลายชนิดที่ผลิตออกมาเป็นกล่องๆ เดียว ซึ่งทำหน้าที่ได้หลายอย่าง ทั้ง **Packet Filtering, Proxy** แต่ก็อย่าลืมว่านี่คือ โครงสร้างแบบชั้นเดียว ซึ่งถ้าพลาดแล้วก็จะเสียหายทั้งระบบได้

12.13.2.2 Screened Host Architecture

Screened Host Architecture จะมีโฮสต์ซึ่งให้บริการพร็อกซี่เหมือนกับใน **Single Box Architecture** ที่เป็น **Dual-homed Host** แต่จะต่างกันตรงที่ว่า โฮสต์นั้นจะอยู่ภายในเน็ตเวิร์ก ไม่ต่ออยู่กับเน็ตเวิร์กภายนอกอื่นๆ (ดังนั้นก็ไม่จำเป็นที่จะต้องใช้ **Dual Homed Host**) และจะมีเราท์เตอร์ซึ่งทำหน้าที่ **Packet Filtering** ช่วยบังคับให้เครื่องภายในเน็ตเวิร์กต้องติดต่อบริการต่างๆ ผ่านพร็อกซี่ โดยไม่ยอมให้ติดต่อใช้

บริการจากภายนอกโดยตรง และก็ให้ภายนอกเข้าถึงได้เฉพาะ **Bastion host** (คือโฮสต์ที่มีความเสี่ยงสูงต่อการถูกโจมตี มักจะเป็นโฮสต์ที่เปิดให้บริการกับอินเตอร์เน็ต ดังนั้นโฮสต์นี้ต้องมีการดูแลเป็นพิเศษ) เท่านั้น



รูปที่ **12 – 16 Screened Host Architecture**

จากรูปที่ **12 – 16** ในโครงสร้างสถาปัตยกรรมแบบนี้จะประกอบไปด้วยเราท์เตอร์ทำหน้าที่ **Packet Filtering** และภายในเน็ตเวิร์กจะมี **Bastion Host** ให้บริการพร็อกซี่อยู่ โดยที่เราท์เตอร์อาจจะถูกเซ็ตดังนี้

- อาจจะอนุญาตให้เครื่องภายในใช้บริการบางอย่างได้โดยตรง
- ส่วนบริการอื่นๆ จะไม่ยอมให้เครื่องภายในติดต่อผ่านออกไปโดยตรง ยกเว้น **Bastion Host** เท่านั้นที่สามารถติดต่อกับเน็ตเวิร์กภายนอกได้ทั้งนี้เพื่อเป็นการบังคับให้ใช้บริการพร็อกซี่ผ่านทาง **Bastion Host** เท่านั้น
- เซ็ตให้เซอร์วิสส่วนใหญ่ผ่านเราเตอร์ออกไปได้โดยตรงแล้ว ให้บางส่วนต้องใช้บริการผ่านพร็อกซี่ ก็แล้วแต่นโยบายและความเหมาะสมขององค์กร

วิธีนี้ถึงแม้ว่าจะมีทั้งพร็อกซี่และเราท์เตอร์ทำหน้าที่กรองแพ็กเก็ตข้อมูล แต่ก็ยังคงอันตรายอยู่ เพราะว่าเราท์เตอร์ต้องยอมให้ภายนอกสามารถติดต่อกับ **Bastion Host** ได้อยู่แล้ว หากแฮกเกอร์สามารถเจาะเข้ามายัง **Bastion Host** ได้ก็สามารถเจาะเข้ามาได้ โครงสร้างแบบนี้เหมาะสำหรับ

- ระบบเครือข่ายที่มีการติดต่อกับเน็ตเวิร์กภายนอกน้อย
- ระบบเครือข่ายที่มีการป้องกันความปลอดภัยในระดับของโฮสต์เป็นอย่างดี

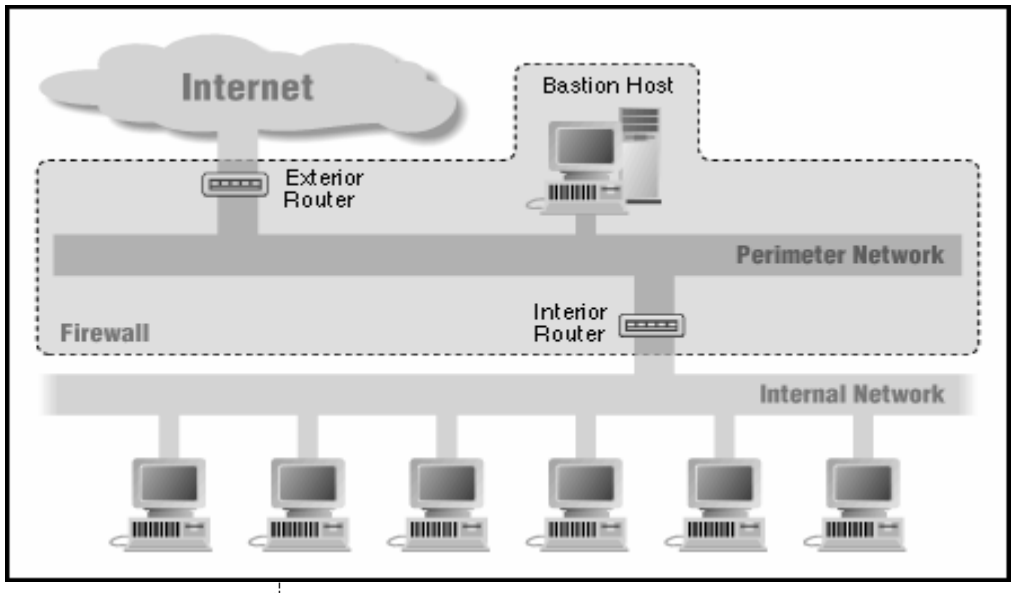
12.13.2.3 Multi Layer Architecture

ในสถาปัตยกรรมแบบหลายชั้น ไฟร์วอลล์จะเกิดขึ้นจากคอมโพเน็นต์หลายๆส่วนทำหน้าที่ประกอบกันขึ้นเป็นระบบ วิธีการนี้สามารถเพิ่มความปลอดภัยได้มาก เนื่องจากเป็นการลดความเสี่ยงต่อความผิดพลาดที่อาจเกิดขึ้น ถ้าหากมีไฟร์วอลล์เพียงจุดเดียวแล้วมีเกิดความผิดพลาดเกิดขึ้น ระบบทั้งหมดก็จะเป็นอันตราย แต่ถ้ามีการป้องกันหลายชั้น หากในชั้นแรกถูกเจาะ ก็อาจจะมีความเสียหายเพียงบางส่วน ส่วนที่เหลือระบบก็ยังคงมีชั้นอื่นๆ ในการป้องกันอันตราย และยังลดความเสี่ยงได้โดยการที่แต่ละชั้นนั้นมีการใช้เทคโนโลยีที่แตกต่างกัน เพื่อให้เกิดความหลากหลาย เป็นการหลีกเลี่ยงการโจมตีหรือช่องโหว่ที่อาจมีในเทคโนโลยีชนิดใดชนิดหนึ่ง โดยทั่วไปแล้วสถาปัตยกรรม

แบบหลายชั้นจะเป็นการต่อกันเป็นซีรี่โดยมี **Perimeter Network** (หรือบางทีเรียกว่า **DMZ Network**) อยู่ตรงกลาง เรียกว่า **Screened Subnet Architecture**

12.13.2.4 Screened Subnet Architecture

Screened Subnet Architecture เป็นสถาปัตยกรรมที่มีการเพิ่ม **Perimeter Network** เข้าไปกั้นระหว่างอินเตอร์เน็ตกับเน็ตเวิร์กภายในไม่ให้เชื่อมต่อกันโดยตรง ทำให้เน็ตเวิร์กภายในมีความปลอดภัยมากขึ้น ดังแสดงตามรูปที่ **12 – 17**



รูปที่ **12 – 17 Screened Subnet Architecture**

รูปที่ **12 – 17** แสดง **Screened Subnet Architecture** อย่างง่าย ประกอบไปด้วย เราเตอร์ 2 ตัว ตัวหนึ่งอยู่ระหว่างอินเตอร์เน็ตกับ **Perimeter Network** ส่วนอีกตัวหนึ่งอยู่ระหว่าง **Perimeter Network** กับเน็ตเวิร์กภายใน ถ้าหากแฮกเกอร์จะเจาะเน็ตเวิร์กภายในต้องผ่านเราเตอร์เข้ามาถึง 2 ตัวด้วยกัน ถึงแม้ว่าจะเจาะชั้นแรกเข้ามายัง **Bastion host** ได้ แต่ก็ยังต้องผ่านเราท์เตอร์ตัวในอีก ถึงจะเข้ามายังเน็ตเวิร์กภายในได้ คอมโพเน็นต์ของ **Screened Subnet Architecture** ในรูปที่ **12 – 17** ประกอบด้วย

- **Perimeter Network** เป็นเน็ตเวิร์กที่เพิ่มเข้ามาเพื่อความปลอดภัย อยู่ระหว่างเน็ตเวิร์กภายนอกกับเน็ตเวิร์กภายใน ประโยชน์ของ **Perimeter Network** ที่เห็นได้ชัดก็คือ การแบ่งเน็ตเวิร์กออกเป็นส่วนๆ ทำให้การไหลของกระแสข้อมูลถูกแบ่งออกเป็นส่วนๆ ตามเน็ตเวิร์กด้วย เนื่องจากโดยทั่วไปแล้ว **LAN** จะเป็นแบบอีเธอร์เน็ต ซึ่งจะมีการส่งข้อมูลแบบบรอดคาสต์ ดังนั้นถ้ามีใครคอยดักจับข้อมูลอยู่ในเน็ตเวิร์กนั้น ก็จะได้ข้อมูลต่างๆ ไปหมด ดังนั้นหากไฟร์วอลล์มีชั้นเดียวและแฮกเกอร์สามารถเข้ามาได้ โดนดักจับข้อมูลก็เสร็จหมด แต่ถ้าเรามี **Perimeter Network** ถึงจะดักจับข้อมูลได้แต่ก็จะได้เพียงที่อยู่บน **Perimeter Network** เท่านั้น

- **Bastion Host** ตั้งอยู่บน **Perimeter Network** ทำหน้าที่ให้บริการพร็อกซี่กับเน็ตเวิร์กภายใน และให้บริการต่างๆ กับผู้ใช้บนอินเตอร์เน็ต **Bastion Host** นั้นจะมีความเสี่ยงต่อการโจมตีสูง จึงต้องมีการดูแลความปลอดภัยเป็นพิเศษ
- **Interior Router** ตั้งอยู่ระหว่าง **Perimeter Network** กับเน็ตเวิร์กภายใน ทำหน้าที่กรองแพ็กเก็ตข้อมูล ป้องกันเน็ตเวิร์กภายในจาก **Perimeter Network** ในการตั้งค่าการใช้งานระหว่าง เน็ตเวิร์กภายในกับ **Perimeter Network** ควรกำหนดอย่างรอบคอบ อนุญาตเฉพาะบริการที่จำเป็นเท่านั้น อย่างเช่น **DNS, SMTP**
- **Exterior Router** ตั้งอยู่ระหว่างเน็ตเวิร์กภายนอกกับ **Perimeter Network** เนื่องจาก **Exterior Router** นี้เป็นจุดที่ต่ออยู่กับเน็ตเวิร์กภายนอก จึงมีหน้าที่ที่สำคัญอย่างหนึ่งคือ การป้องกันแพ็กเก็ตที่มีการ **Forged IP Address** เข้ามาโดยอ้างว่ามาจากเน็ตเวิร์กภายในทั้งๆ ที่จริงๆ แล้วมาจากเน็ตเวิร์กภายนอก

12.14 บทสรุป

นี่คือสิ่งที่คุณได้รับจากหนังสือเล่มนี้ การแนะนำเบื้องต้นเกี่ยวกับระบบเครือข่ายที่เริ่มจากระบบเครือข่ายแบบ **Peer-to-Peer** ของเครื่อง **PC** และสิ้นสุดที่การคุ้มครองที่ประตูทางเข้าระบบเครือข่าย ยังมีอะไรเพิ่มเติมที่ต้องทราบอีกหรือไม่? แน่นอน ไม่เพียงแต่จะมีเรื่องราวอื่นอีกมากที่ต้องเรียนรู้เกี่ยวกับระบบเครือข่ายทั้งในทางลึก (รายละเอียดเพิ่มเติม) และทางกว้าง (เนื้อหาที่ไม่มีในหนังสือเล่มนี้) ระบบเครือข่ายเองก็แทบจะไม่เป็นสภาวะแวดล้อมที่อยู่กับที่ซึ่งไม่มีการเปลี่ยนแปลง เทคโนโลยีใหม่ๆ ที่เกิดขึ้นก็เข้ามามีส่วนเกี่ยวข้องกับระบบเครือข่ายเพิ่มมากขึ้น

Throughput ของระบบเครือข่ายมีการเปลี่ยนจาก **Mbps** ไปเป็น **Gbps** อย่างกระทันหัน ฮาร์ดแวร์ที่เร็วกว่าและมีความน่าเชื่อถือมากขึ้นมีวิวัฒนาการต่อไป และอุปกรณ์ใหม่ๆ ที่มีมากเหลือคณานับ จากเพจเจอร์ (**pager**) ไปยังโทรศัพท์มือถือ และสมาร์ทการ์ด (**smart card**) ที่มี **chips** บนการ์ด พร้อมที่จะ **access** เข้าไปยังเครือข่ายอินเตอร์เน็ตเพื่อรับ/ส่งอีเมลล์ และการใช้ระบบเครือข่ายแบบอื่น วิธีการใหม่ๆ ในการจัดตั้งระบบเครือข่าย เช่น **ATM** และ **FDDI** เป็นวิถีทาง หรือการเข้าไปสู่เส้นทางสำคัญ

ดังที่ได้เห็นแล้วว่าความปลอดภัยมีเพิ่มมากขึ้น เหมือนระบบเครือข่ายมีการผจญภัยออกไปนอกเหนือการรวมผนังกั้นระบบเครือข่ายโดยการสื่อสารโทรคมนาคมและเครือข่ายอินเตอร์เน็ต การพาณิชย์อิเล็กทรอนิกส์เป็นกำลังใจในการพัฒนาการชำระเงินแบบอิเล็กทรอนิกส์และกระเป๋าเงินอิเล็กทรอนิกส์ และผลักดันมาตรฐานในการทำให้มั่นใจในระบบการเงินและความเป็นส่วนตัวของบุคคล ส่วนการทำงานบนเครือข่ายอินเตอร์เน็ตก็อยู่ในระหว่างการจัดให้มีการท่องไปทั่วโลกด้วยความเร็วที่เพิ่มมากขึ้นและเพิ่มช่องสัญญาณการสื่อสาร หรือแบนด์วิธ (**Bandwidth**)

ในการรวมโลกทั้งใบเข้าด้วยกัน เว็บจะทำงานในวิถีทางของธุรกิจระบบเครือข่ายที่จะดำเนินต่อไปเพื่อทำให้ความชัดเจนระหว่างแหล่งทรัพยากรท้องถิ่นกับแหล่งทรัพยากรระยะไกลลดลงจนพร่ามัว เทคโนโลยีเว็บเข้ามามีส่วนในหลายเรื่องที่ไม่สามารถแยกออกจากเทคโนโลยีระบบเครือข่ายได้ และก็ไม่มีแนวโน้มที่จะหยุดนิ่ง ตัวอย่างเช่น **HTML** ในปัจจุบัน มีการพัฒนา **markup language** ที่ใหม่กว่าซึ่งกำลังอยู่ในกระบวนการพัฒนา เรียกว่า **XML**

(**Extensible Markup Language**) ในขณะที่ **XML** เข้ามามีส่วนร่วมแต่ยังไม่มีการกำหนดให้เป็นมาตรฐาน ก็ได้รับการพัฒนาเพื่อทำให้ผู้สร้างเว็บไซต์ใช้ ในการอธิบายไม่เพียงแต่การมองดูเว็บเพจ แต่รวมถึงเนื้อหาบนเพจต่างๆ ด้วยวิธีการที่จะเพิ่มระดับของความอ่อนตัว และความสามารถในการโต้ตอบให้กับเว็บ

และถึงแม้ว่าจะไม่เข้มงวดว่าจะต้องเป็นพื้นฐานของระบบเครือข่าย การพัฒนาเมื่อไม่นานมานี้ เช่น **java** และสิ่งที่เรียกว่า **open source software** ก็กำลังหาวิธีของตัวเองในการเข้าไปในระบบเครือข่าย การจัดตั้งระบบเครือข่ายและเครือข่ายอินเตอร์เน็ต สำหรับ **Java** ได้รับการพัฒนาโดยบริษัท **Sun Microsystems** เป็นภาษาการเขียนโปรแกรมที่สร้างโปรแกรมให้ทำงาน บนเครื่องคอมพิวเตอร์แพล็ตฟอร์มต่างๆ ได้โดยไม่ต้องมีการปรับปรุง ตอนนี้สิ่งที่ใช้โดยทั่วไปคือเทคโนโลยี **ActiveX** ของบริษัท ไมโครซอฟต์ สำหรับสร้างโปรแกรมขนาดเล็ก (เรียกว่า **ActiveX object** หรือ **Java applets** ขึ้นอยู่กับเทคโนโลยีที่ใช้) ที่สามารถติดเข้ากับเว็บเพจ เพื่อที่จะทำให้มีความสามารถในการโต้ตอบเพิ่มมากขึ้น ดังนั้นเว็บเพจจึงสามารถโต้ตอบกับผู้ใช้ได้มากขึ้น ส่วน **Open source** ซึ่งกล่าวถึงโปรแกรมที่ผู้พัฒนาทำให้ **code** ของโปรแกรมมีไว้แจก ในลักษณะใกล้เคียงกับระบบปฏิบัติการที่แจกให้ฟรีที่ชื่อว่า **Linux** (ใช้พื้นฐานของระบบปฏิบัติการ **UNIX**) ที่ถูกชักชวนให้ใช้อย่างกว้างขวางโดยผู้ที่เลื่อมใสในความเร็ว และเป็นสภาวะแวดล้อมที่มั่นคงสำหรับเครื่อง **server** ของระบบเครือข่าย ซึ่งยังคงปรากฏว่า **open source software** จะเข้ามามีบทบาทในวิวัฒนาการของ **Java** ด้วย

<u>แบบฝึกหัดท้ายบท</u>

1. **Domain Name System** คืออะไร มีประโยชน์อย่างไรในเครือข่ายอินเตอร์เน็ต
2. จงอธิบายรูปแบบการจัดโดเมนในเครือข่ายอินเตอร์เน็ต
3. เพราะเหตุใดจึงจำเป็นต้องมี **DNS Server**
4. **IP Address** คืออะไร มีประโยชน์อย่างไรในเครือข่ายอินเตอร์เน็ต
5. โปรแกรมเว็บเบราส์เซอร์ทำหน้าที่อะไร จงยกตัวอย่างของโปรแกรมเว็บเบราส์เซอร์มา **2 – 3** โปรแกรม
6. โปรแกรมเบราส์เซอร์จะติดต่อกับเวิร์ดไวด์เว็บด้วยโปรโตคอลชื่อว่าอะไร
7. **URL** คืออะไร จงเขียนรูปแบบโดยทั่วไปของ **URL**
8. จงอธิบายความหมายของ **Public Key** และ **Private Key**
9. จงอธิบายกระบวนการในการเข้ารหัสข้อมูลมาพอสังเขป
10. สถาปัตยกรรมหลักในการทำ **tunnel** ของ **Virtual Private Network** มี **2** แบบคืออะไรบ้าง
11. **Firewall** คืออะไร มีประโยชน์อย่างไร
12. โครงสร้างสถาปัตยกรรมในการจัดตั้ง **Firewall** มีกี่แบบ อะไรบ้าง
13. จงอธิบายหลักการพื้นฐานในการทำ **Packet Filtering**
14. จงเปรียบเทียบข้อดี-ข้อเสียของการเลือกอุปกรณ์ให้ทำหน้าที่เป็น **Packet Filter**
15. **Proxy Server** คือเครื่องเซิร์ฟเวอร์ซึ่งทำหน้าที่อะไร จงอธิบาย