บทที่ ๒
เรื่องไม่ลึกแต่ควรรู้กับเครือข่ายคอมพิวเตอร์

ถ้าเราเป็นผู้ที่ต้องดูแลระบบเครือข่ายคอมพิวเตอร์ในองค์กรของเรา ซึ่งก็คือโรงเรียนที่เรารับผิดชอบอยู่ จะด้วยเพราะหน้าที่ที่ตรงกับความสามารถของเรา หรือเพราะไม่มีใครทำก็ตาม เมื่อมีความจำเป็นจะต้องทำ เราก็ควรจะรู้เรื่องที่จะกล่าวต่อไปนี้บ้างเพื่อรู้จักกับเครือข่ายคอมพิวเตอร์บ้าง แต่ถ้ารู้แล้วจะข้ามเนื้อหานี้ไปก็ได้

ประเภทของระบบเครือข่ายคอมพิวเตอร์

โดยทั่วไปแล้วนิยมจำแนกระบบเครือข่ายคอมพิวเตอร์ เป็น ๓ ประเภท ดังนี้

๑. **เครือข่ายระดับประเทศ** (Wide Area Network หรือเรียกย่อๆ ว่า WAN) เป็นระบบเครือข่ายที่เชื่อมต่อกันระหว่างประเทศ หรือทั้งโลก

๒. **เครือข่ายระดับเมือง** (Metropolitan Area Network หรือเรียกย่อๆ ว่า MAN) เป็นระบบเครือข่ายที่เชื่อมระหว่างเมือง หรือจังหวัด ในประเทศไทยก็ต้องอาศัยการเชื่อมต่อผ่านเครือข่ายของ บ.ทีโอที จำกัด (มหาชน) หรือ บ. กสท โทรคมนาคม จำกัด (มหาชน)

๓. **เครือข่ายท้องถิ่น** (Local Area Network หรือเรียกย่อๆ ว่า LAN) เป็นระบบเครือข่ายที่ติดตั้งและใช้งานภายในองค์กร มิได้ออกไปนอกบริเวณขององค์กร

ชนิดของระบบเครือข่ายคอมพิวเตอร์

แบ่งได้เป็น ๓ ชนิด คือ

๑. เครือข่ายแบบ Host-Terminal เป็นระบบเครือข่ายขนาดใหญ่ โดยเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เราจะเรียกว่า โฮส (Host) และมีเครื่องคอมพิวเตอร์ลูกข่ายที่มาขอใช้บริการเรียกว่า เทอร์มินอล (Terminal)

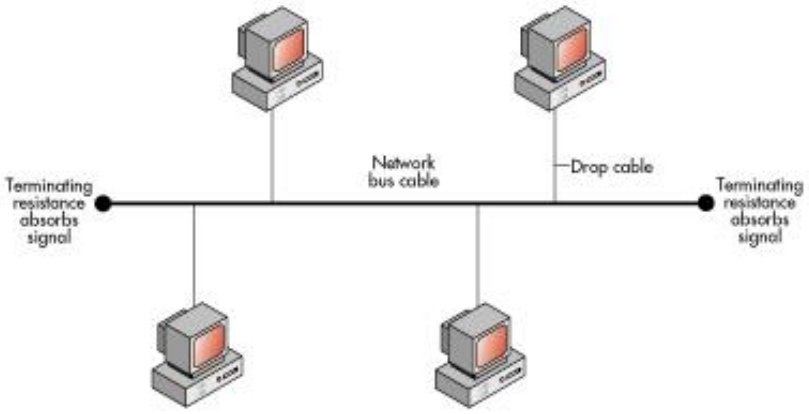
๒. เครือข่ายแบบ Client/Server เป็นระบบเครือข่ายที่มีเครื่องคอมพิวเตอร์ที่ให้บริการแก่เครื่องคอมพิวเตอร์ภายในเครือข่าย ซึ่งเรียกว่า เซิร์ฟเวอร์ (Server) ส่วนเครื่องคอมพิวเตอร์ลูกข่ายที่ใช้บริการเรียกว่า ไคล์เอน (Client) มีความปลอดภัยสูง ซึ่งเป็นระบบที่เราจะกล่าวถึงและนำมาใช้ในหนังสือเล่มนี้

๓. เครือข่ายแบบ Peer-to-Peer เป็นระบบเครือข่ายขนาดเล็ก ใช้งานง่าย ทุกเครื่องในระบบเครือข่ายมีสิทธิเท่าเทียมกัน ทำให้การควบคุมดูแลการใช้งานยาก

รูปแบบของการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ (Network Topology)

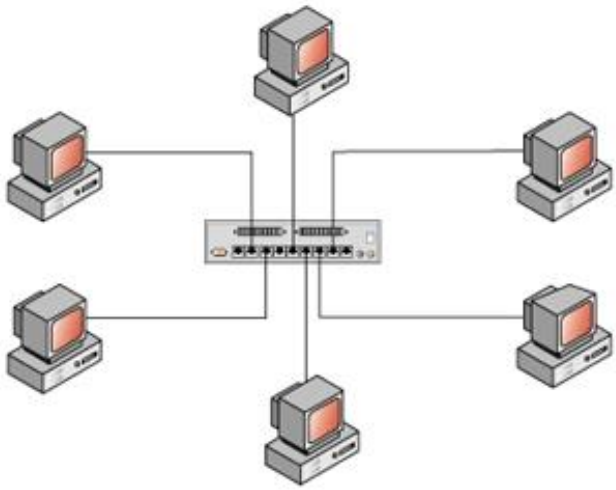
เราคงจะไม่กล่าวถึงอย่างละเอียดลึกซึ้งของรูปแบบการเชื่อมต่อในรูปแบบต่างๆ ว่าเป็นไปตามมาตรฐานอะไร สายต้องเป็นแบบไหน มีความยาวได้เท่าไร จะกล่าวเฉพาะ Topology เบื้องต้นเท่าที่จำเป็น และรูปแบบที่จะสามารถนำไปใช้งานจริงในปัจจุบัน

๑. การเชื่อมต่อแบบบัส (Bus Topology) เป็นการเชื่อมต่อโดยมีสายนำสัญญาณเส้นเดียวเป็นแกน (สาย Coaxial) การจะเชื่อมต่อกับคอมพิวเตอร์จะมีหัวต่อเหมือนสามทางแบบในการต่อท่อประปา มีชื่อเรียกว่า T-connector และต่อกับการ์ดแลน ด้วยหัวต่อ BNC ส่วนด้านหัวและท้ายของสายจะต้องปิดด้วย เทอร์มินอล ดังรูป ๒.๑ ซึ่งปัจจุบันยังพอมีใช้งานอยู่ แต่น่าจะหาได้ยากแล้ว



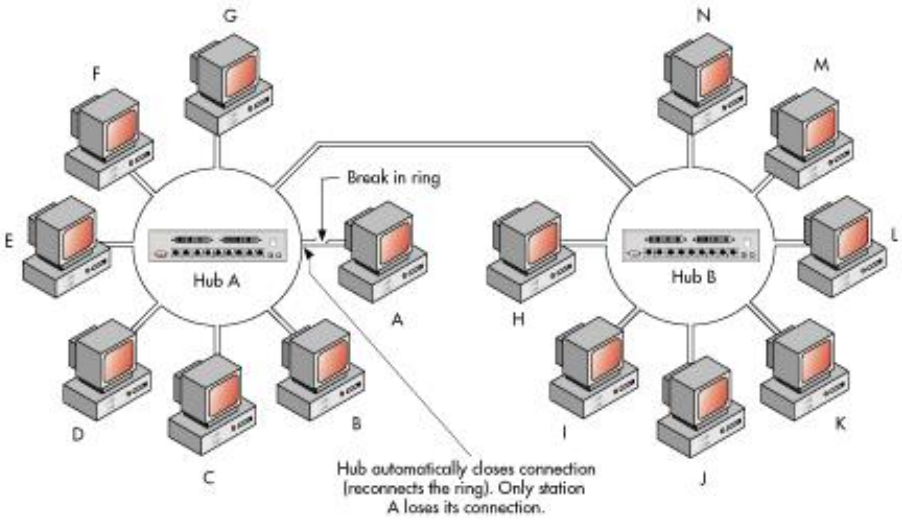
รูป ๒.๑ การเชื่อมต่อแบบบัส
(ภาพจากเว็บไซด์ www.novell.com)

๒. การเชื่อมต่อแบบสตาร์ (Star Topology) รูป ๒.๒ เป็นการเชื่อมต่อที่จะต้องมีอุปกรณ์ฮับ(Hub) หรือ สวิทช์ (Switch) เป็นตัวที่จะเชื่อมไปยังคอมพิวเตอร์เครื่องต่างๆ หรืออาจกล่าวได้ว่า มี ฮับ หรือ สวิทช์ เป็นศูนย์กลาง (ปัจจุบันใช้สวิทช์มากกว่า เนื่องจากราคาถูกมาก และมีความฉลาดและเร็วกว่าฮับ) เป็นรูปแบบการเชื่อมต่อที่มีการใช้งานกันในปัจจุบันเป็นจำนวนมาก รวมทั้งในโรงเรียนทั่วไปด้วย



รูป ๒.๒ การเชื่อมต่อแบบสตาร์
(ภาพจากเว็บไซด์ www.novell.com)

๓. การเชื่อมต่อแบบวงแหวน (Ring Topology) รูป ๒.๓ เป็นการเชื่อมต่อคอมพิวเตอร์เข้าด้วยกันเป็นลักษณะวงกลม ค่อนข้างยุ่งยากแต่ก็ยังมีใช้กันอยู่



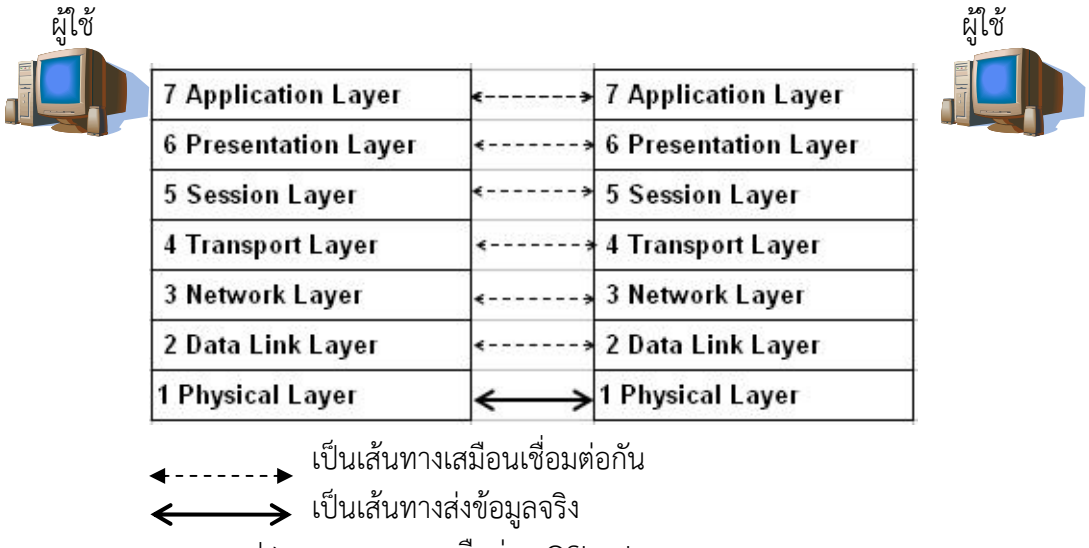
รูป ๒.๓ การเชื่อมต่อแบบวงแหวน
(ภาพจากเว็บไซต์ www.novell.com)

นอกจากนี้ยังมีรูปแบบการเชื่อมต่ออื่นอีก เช่น Mesh Topology และ Hybrid Topology เป็นต้น

*(**หมายเหตุ:** ในส่วนของการเชื่อมต่อระบบเครือข่ายแบบ LAN นั้น ในปัจจุบันนิยมใช้แบบสตาร์ และใช้เทคโนโลยีเครือข่ายสำหรับ LAN แบบ Ethernet)*

ระบบเครือข่าย กับมาตรฐานเครือข่าย OSI

International Organization for Standardization หรือ ISO หรือ องค์กรมาตรฐานสากล ได้กำหนดมาตรฐานด้านเครือข่ายเพื่อให้เครือข่ายที่ถูกสร้างที่แตกต่างกันสามารถเชื่อมโยงและติดต่อสื่อสารกันได้อย่างไม่มีปัญหา ด้วยมาตรฐานเครือข่าย OSI (Open System Interconnection) ๗ Layer



รูป ๒.๔ มาตรฐานเครือข่าย OSI ๗ Layer

Application Layer หรือ Layer ๗ เป็นชั้นที่จัดการแปลความหมาย และทำงานตามคำสั่งที่ได้รับในระดับโปรแกรมประยุกต์

Presentation Layer หรือ Layer ๖ เป็นชั้นที่ดูแลและทำหน้าที่ตกลงกับคอมพิวเตอร์อีกด้านหนึ่งในชั้นเดียวกันว่าการรับส่งข้อมูลในระดับโปรแกรมประยุกต์จะมีขั้นตอนและข้อบังคับอย่างไร

Session Layer หรือ Layer ๕ เป็นชั้นที่ควบคุมการรับส่งข้อมูลของคอมพิวเตอร์ทั้งสองด้านให้สอดคล้องกัน

Transport Layer หรือ Layer ๔ เป็นชั้นที่ควบคุมความผิดพลาดในการรับส่งข้อมูลที่เป็นรอยต่อระหว่างการรับส่งข้อมูลของซอฟต์แวร์กับฮาร์ดแวร์

Network Layer หรือ Layer ๓ เป็นชั้นติดต่อกำหนดเส้นทางของการรับส่งข้อมูลผ่านระบบเครือข่าย และตรวจสอบ Address ของผู้รับ

Data Link Layer หรือ Layer ๒ เป็นชั้นควบคุมการรับส่งข้อมูลในระดับฮาร์ดแวร์ และตรวจสอบความผิดพลาดในการรับส่งข้อมูล

Physical Layer หรือ Layer ๑ เป็นชั้นล่างสุดที่ควบคุมการเชื่อมต่อข้อมูลระหว่างกันทางฮาร์ดแวร์ ควบคุมความเร็วในการรับส่งข้อมูล ควบคุมการเชื่อมต่อเข้ากับสายรับส่งข้อมูล

โปรโตคอล TCP/IP

โปรโตคอล TCP/IP (Transmission Control Protocol/Internet Protocol) เป็นโปรโตคอลที่นิยมใช้ในระบบเครือข่ายอินเทอร์เน็ตมากที่สุด และเป็นโปรโตคอลระบบเปิด ที่ไม่มีบริษัทใดบริษัทหนึ่งเป็นเจ้าของลิขสิทธิ์ บริษัทใดพัฒนาระบบของตนเองขึ้นมาก็เพียงแต่ให้รองรับ TCP/IP เท่านั้นก็สื่อสารกันได้

โปรโตคอล TCP/IP จะประกอบด้วย

๑. Application Layer หรือ Process Layer
๒. Host to Host Layer หรือ Transport Layer
๓. Internet work Layer
๔. Network interface Layer

หลักการทำงานของโปรโตคอล TCP/IP คือการสื่อสารจะเริ่มจาก Application ของผู้ใช้ ส่งข้อมูลให้กับโปรโตคอลในชั้น Application ซึ่งจะเพิ่มข้อมูลส่วนหัวที่มีชื่อเครื่องที่ต้องการสื่อสารด้วยและหมายเลขพอร์ตของเครื่องนั้น หลังจากนั้นข้อมูลก็จะถูกส่งไปยังชั้นเชื่อมต่อโฮสต์ ข้อมูลในชั้นนี้จะเรียกว่า เซกเมนต์ (Segment) เมื่อชั้นนี้ได้รับข้อมูลก็จะแบ่งข้อมูลออกเป็นส่วนย่อยๆ *(ส่วนย่อยๆ ก็จะมีส่วนหัวเพิ่มเข้าไปด้วย)* หลังจากนั้นก็จะถูกส่งต่อไปยังชั้นอินเทอร์เน็ต ซึ่งก็จะถูกเพิ่มข้อมูลส่วนหัวเข้าไปอีกเช่นกัน (เช่น หมายเลข IP) ข้อมูลในชั้นนี้จะเรียกว่า แพ็คเก็ต (packet) แล้วถูกส่งต่อเข้าไปในเครือข่ายจนถึงเครื่องปลายทาง และเครื่องปลายทางก็จะทำตามขั้นตอนที่ตรงกันข้ามกับเครื่องส่ง และข้อมูลก็จะถูกส่งต่อไปให้ Application เพื่อนำข้อมูลไปดำเนินการต่อไป (**<u>ข้อเสนอแนะ</u>**: อ่านไว้เพื่อความรู้ก็พอ ในการใช้งานจริงนั้นก็คงไม่มาอธิบายกันหรอก)

ไอพีแอดเดรส (IP Address)

เป็นหมายเลขอ้างอิงประจำตัวของอุปกรณ์ต่างๆ ที่เชื่อมต่ออยู่ในเครือข่ายอินเทอร์เน็ต โดยการกำหนด IP Address ***(ถ้ากล่าวว่า ไอพี ก็ขอให้เข้าใจว่าก็คือ IP Address เช่นเดียวกัน)*** ให้แต่ละเครื่องหรือแต่ละอุปกรณ์นั้นจะต้องไม่ซ้ำกัน หน่วยงานกลางที่ทำหน้าที่จัดสรร IP Address คือ InterNIC (Internet Network Information Center) โดยเขียนเป็นรูปเลขฐานสิบ ๔ ชุด คั่นด้วยเครื่องหมายจุด แต่ละชุดมีค่าตั้งแต่ ๐-๒๕๕ เช่น ๒๐๓.๑๑๓.๑๒๗.๙๙ (ของ บ.ทีโอที จำกัด) เป็นต้น

ไอพีแอดเดรส สามารถแบ่งได้ทั้งหมด ๕ Class คือ A,B,C,D,E ที่ใช้งานจริงในปัจจุบันมี ๓ Class คือ Class A,B และ C

Class A	เริ่มต้นที่ค่า	๐.๐.๐.๐	ถึง	๑๒๗.๒๕๕.๒๕๕.๒๕๕
Class B	เริ่มต้นที่ค่า	๑๒๘.๐.๐.๐	ถึง	๑๙๑.๒๕๕.๒๕๕.๒๕๕
Class C	เริ่มต้นที่ค่า	๑๙๒.๐.๐.๐	ถึง	๒๒๓.๒๕๕.๒๕๕.๒๕๕
Class D	เริ่มต้นที่ค่า	๒๒๔.๐.๐.๐	ถึง	๒๓๙.๒๕๕.๒๕๕.๒๕๕
Class E	เริ่มต้นที่ค่า	๒๔๐.๐.๐.๐	ถึง	๒๕๕.๒๕๕.๒๕๕.๒๕๕

Class D ไว้ใช้ในเครือข่าย Multicast

Class E ยังไม่ถูกนำมาใช้งาน

Private และ Public IP

การเชื่อมต่อคอมพิวเตอร์เข้ากับอินเทอร์เน็ตนั้น จำเป็นที่ต้องขอหมายเลขไอพี จาก InterNIC ซึ่งรับผิดชอบเกี่ยวกับการแจกจ่ายหมายเลขไอพี ซึ่งไอพีจำพวกนี้คือ Public IP Address จะต้องเสียค่าใช้จ่ายต่อปีด้วย แต่สภาพการใช้งานปัจจุบันในองค์กรเล็กๆ หรือ โรงเรียนนั้น เราไม่จำเป็นต้องขอ Public IP Address เนื่องจากในปัจจุบันเรานิยมใช้ ADSL จากหน่วยงานที่ให้บริการ เช่น True , TOT , CAT เหล่านี้ เราเพียงแต่มีเครือข่ายภายในองค์กรของเรา แล้วเชื่อมต่อกับหน่วยงานดังกล่าว ก็สามารถใช้งานอินเทอร์เน็ตได้แล้ว แต่เครือข่ายภายในของเราก็จะใช้ Private IP Address (ไอพีพวกนี้ออกสู่อินเทอร์เน็ตด้วยสถานะจริงไม่ได้) แล้ว เชื่อมต่อผ่านหน่วยงานที่ให้บริการดังกล่าว ซึ่งค่า Private IP Address ที่ใช้มีดังนี้

Class A	เริ่มต้นที่ค่า	๑๐.๐.๐.๐	ถึง	๑๐.๒๕๕.๒๕๕.๒๕๕
Class B	เริ่มต้นที่ค่า	๑๗๒.๑๖.๐.๐	ถึง	๑๗๒.๓๑.๒๕๕.๒๕๕
Class C	เริ่มต้นที่ค่า	๑๙๒.๑๖๘.๐.๐	ถึง	๑๙๒.๑๖๘.๒๕๕.๒๕๕ (นิยมใช้ส่วนนี้ และที่นิยมกันมากก็คือ ๑๙๒.๑๖๘.๐.๑-๒๕๕ และ ๑๙๒.๑๖๘.๑.๑-๒๕๕)

ส่วนค่า Default Subnet Mask ที่จะใช้คู่กับค่า IP Address จะเป็นดังนี้

Class A ใช้ค่า ๒๕๕.๐.๐.๐

Class B ใช้ค่า ๒๕๕.๒๕๕.๐.๐

Class C ใช้ค่า ๒๕๕.๒๕๕.๒๕๕.๐

ตั้งแต่ปี ๒๕๕๖ นี้เป็นต้นไปโรงเรียนต่างๆ ส่วนใหญ่จะได้รับการเชื่อมต่อเข้ากับ Uninet ด้วยเครือข่ายใยแก้วนำแสงซึ่งก็จะมี Public IP ให้เราด้วย

(**ข้อความพิเศษ**: ในเรื่องไอพีนั้น คอมพิวเตอร์ยังสามารถรับค่าไอพีอัตโนมัติจากเครื่องที่ให้บริการที่เป็นเครื่องแม่ข่ายก็ได้ หรือรับค่าจาก Router หรือ จาก ADSL Router ก็ได้ แต่ก็ไม่แนะนำเพราะ

เจตนาของหนังสือเล่มนี้ส่วนหนึ่งก็คือเรื่องความปลอดภัยในเครือข่ายและดูแลการใช้งานของเครื่องลูกข่าย)

รายละเอียดของ IP Address และ Subnet Mask ยังมีปลีกย่อยอีกมาก ซึ่งเห็นว่าเกินความจำเป็นที่จะนำไปใช้งานจริง เพราะถ้ากล่าวต่อไปอีกจะเหมาะสำหรับการดูแลระบบเครือข่ายคอมพิวเตอร์ในองค์กรใหญ่ๆ เสียมากกว่า ดังนั้นจึงขอไว้แต่เพียงเท่านี้

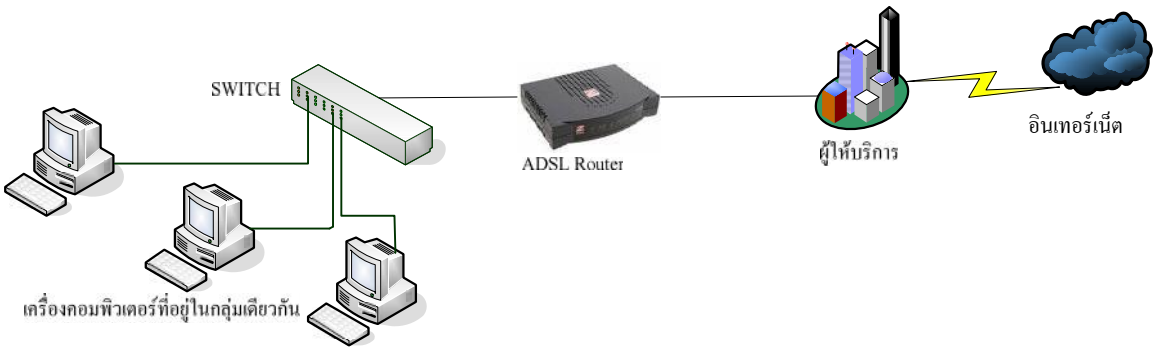
การเชื่อมต่อเครือข่ายคอมพิวเตอร์กับอินเทอร์เน็ต

ในโครงการที่โรงเรียนได้รับเครื่อง Server ไปนั้น โรงเรียนจะมีการเชื่อมต่อกับอินเทอร์เน็ตอยู่ ๒ ลักษณะ คือ การเชื่อมต่อกับ ADSL และการเชื่อมต่อกับ เราเตอร์ (Router)

การเชื่อมต่อเครือข่ายคอมพิวเตอร์ด้วย ADSL

การเชื่อมต่อด้วยวิธีนี้อาศัยประสิทธิภาพของอินเทอร์เน็ตความเร็วสูง ทำให้เครือข่ายมีความเร็วขึ้น และใช้งานได้สะดวกขึ้น โดยมีรูปแบบการเชื่อมต่อเครือข่ายดังนี้

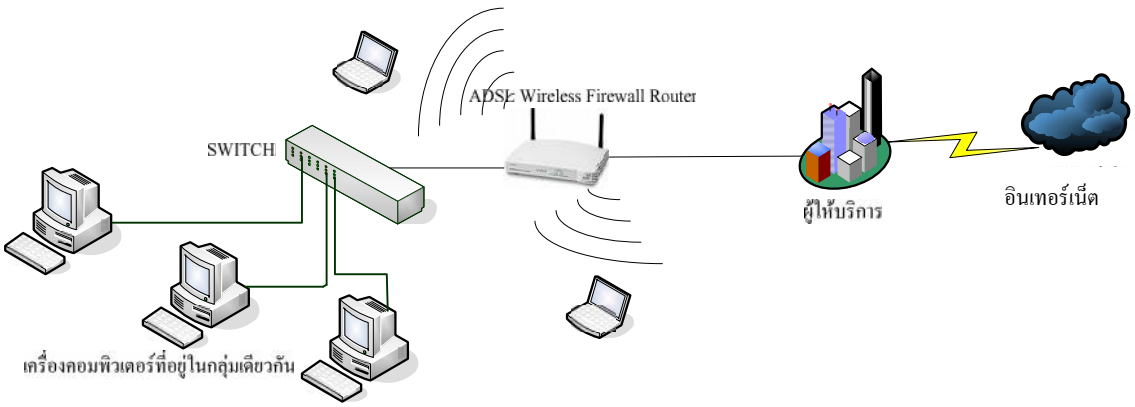
๑. ADSL Router



รูป ๒.๕ การต่อเครือข่ายคอมพิวเตอร์ด้วย ADSL Router

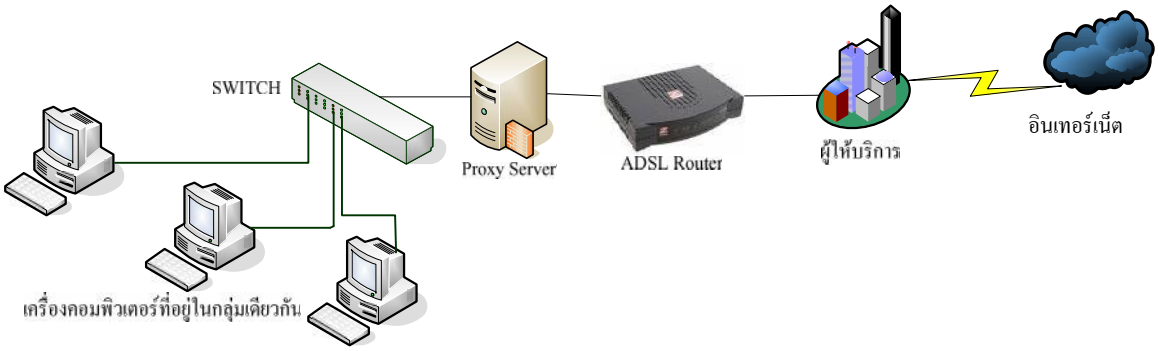
การต่อแบบ ADSL Router นี้ จะแจกค่า IP Address มายังเครื่องลูกข่าย โดยเครื่องลูกข่ายสามารถออกสู่อินเทอร์เน็ตได้เลย

๒. ADSL Wireless Firewall Router



รูป ๒.๖ การต่อเครือข่ายคอมพิวเตอร์ด้วย ADSL Wireless Firewall Router

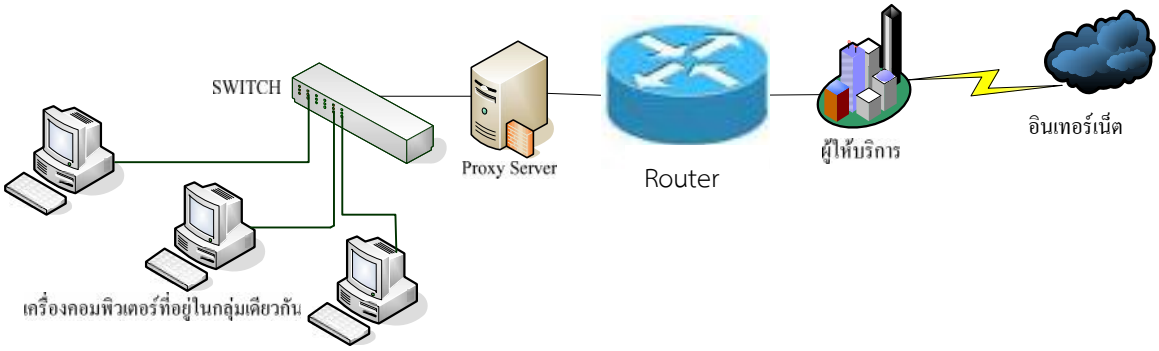
จะเห็นได้ว่าทั้ง ๒ แบบ ที่ใช้ ADSL ในปัจจุบันต่อเข้ากับ Switch โดยตรง เราไม่สามารถควบคุมและดูแลความปลอดภัยใดๆ ได้ ทุกเครื่องสามารถออกสู่อินเทอร์เน็ตได้อย่างอิสระ ซึ่งถ้าเราต้องการควบคุมดูแลก็ต้องนำคอมพิวเตอร์ มาทำเป็นเครื่องแม่ข่าย (Computer Server)ให้ส่วนเครื่องลูกข่าย การจะออกสู่อินเทอร์เน็ตจะต้องผ่านเครื่องแม่ข่ายเท่านั้น โดยนำเครื่อง Server มากั้นระหว่าง Switch กับ ADSL Router ดังรูป ๒.๗ การต่อแบบนี้จำเป็นต้องมีการ์ดแลน ๒ อันบนตัวที่เป็น Proxy Server



รูป ๒.๗ การนำเครื่อง Server มากั้นระหว่าง Switch กับ ADSL Router

การเชื่อมต่อเครือข่ายคอมพิวเตอร์ด้วยเราเตอร์

เป็นระบบเครือข่ายที่มีความยุ่งยากมากพอสมควร จะต้องใช้อุปกรณ์ เราเตอร์ ***(ซึ่งจำเป็นต้องมีการคอนฟิกค่าที่ค่อนข้างยุ่งยากและสลับซับซ้อน)*** แต่โครงการ Uninet ที่มีการเชื่อมสายสัญญาณใยแก้วนำแสง (Fiber Optic) ไปยังโรงเรียนต่างๆ ทั่วประเทศในขณะนี้ (ปี ๒๕๕๖) ได้มีการติดตั้งเราเตอร์แทนการใช้ ADSL Router โดยโรงเรียนไม่ต้องคอนฟิกค่าใดๆ (ทางบริษัทที่ได้รับสัมปทานจะดำเนินการให้) ซึ่งรูปแบบก็เหมือนกันเพียงแต่เปลี่ยนจาก ADSL Router เป็น Router แทน



รูป ๒.๘ การนำเครื่อง Server มากั้นระหว่างเครือข่ายภายในกับเครือข่ายภายนอก (อินเทอร์เน็ต)

Windows Server ๒๐๐๘

เป็นระบบปฏิบัติการที่ออกแบบมาเพื่อใช้งานในระบบเครือข่าย ซึ่งสามารถนำมาบริหารให้บริการและการจัดการด้านเครือข่ายได้เป็นอย่างดี นอกจากนั้น Windows Server ๒๐๐๘ ยังมีระบบโครงสร้างพื้นฐานทางด้านเครือข่ายที่มีความปลอดภัยสูง และช่วยเพิ่มประสิทธิภาพในการใช้

งานเครือข่ายภายในโรงเรียนได้เป็นอย่างดี อีกทั้งช่วยสร้างความมั่นคงให้กับระบบโครงสร้างพื้นฐานด้านคอมพิวเตอร์ของโรงเรียนด้วย Windows Server ๒๐๐๘ ถูกออกแบบมาหลายรุ่น แล้วแต่ภาระงาน ซึ่งสามารถหาข้อมูลได้ในอินเทอร์เน็ต ดังนั้นคงไม่กล่าวในที่นี้ให้ยุ่งยาก ***เพราะเจตนาของหนังสือเล่มนี้คือต้องการให้นำไปใช้ได้ และทำได้จริง***

Forefront Threat Management Gateway ๒๐๑๐

หรือบางทีเรียกสั้นๆ ว่า TMG ๒๐๑๐ นั้น เป็นซอฟต์แวร์ประเภท Security Gateway เพราะว่าไม่ได้เป็นแค่พร็อกซี่ (Proxy) อย่างเดียว แต่มีความสามารถทั้งเป็น

๑. Firewall
๒. VPN
๓. IPS
๔. Anti-Spam
๕. Content Inspection
๖. URL Filtering
๗. Load Balance

และอื่นๆ อีกมากมาย ด้วยความสามารถต่างๆ นี้เอง จึงจัดว่า TMG ๒๐๑๐ เป็น Security Gateway ลองมาทำความเข้าใจง่ายๆ กับความสามารถของ TMG ๒๐๑๐ ดูดังนี้

Firewall (ไฟร์วอลล์)

คือระบบที่ช่วยป้องกันเครือข่ายจากบุคคลภายนอก ทำหน้าที่เสมือนเป็นป้อมปราการป้องกันการบุกรุก ในขณะเดียวกันจะยอมให้ผู้ที่ระบบรู้จักสามารถเข้าออกได้ ซึ่งรูปแบบของไฟร์วอลล์มีทั้งแบบที่เป็นฮาร์ดแวร์ และซอฟท์แวร์ ส่วน TMG ๒๐๑๐ เป็นซอฟต์แวร์ไฟร์วอลล์ที่มีความสามารถสูงตัวหนึ่ง

VPN

ย่อมาจาก Virtual Private Network เป็นเทคโนโลยีการเชื่อมต่อเครือข่ายนอกอาคาร เป็นระบบเครือข่ายในองค์กร ซึ่งเชื่อมเครือข่ายในแต่ละแห่งเข้าด้วยกัน โดยอาศัยอินเทอร์เน็ตเป็นตัวกลาง มีการสร้างอุโมงค์เสมือนไว้รับส่งข้อมูล มีระบบเข้ารหัสป้องกันการลักลอบใช้ข้อมูล เหมาะสำหรับองค์กรขนาดใหญ่ ซึ่งต้องการความคล่องตัวในการติดต่อรับส่งข้อมูลระหว่างกัน

IPS

ย่อมาจาก Instrusion Prevension System คือระบบที่คอยตรวจจับการบุกรุกของผู้ที่ไม่ประสงค์ดี รวมไปถึงข้อมูลจำพวกไวรัสด้วย โดยสามารถทำการวิเคราะห์ข้อมูลทั้งหมดที่ผ่านเข้าออกภายในเครือข่ายว่า มีลักษณะการทำงานที่เป็นความเสี่ยงที่ก่อให้เกิดความเสียหายต่อระบบเครือข่ายคอมพิวเตอร์หรือไม่ เมื่อตรวจพบข้อมูลที่มีลักษณะการทำงานที่เป็นความเสี่ยงต่อระบบเครือข่ายคอมพิวเตอร์ก็จะทำการป้องกันข้อมูลดังกล่าวนั้น ไม่ให้เข้ามาภายในเครือข่ายได้

Anti-Spam

คือการป้องกัน E-mail ที่เราท่านไม่พึงประสงค์ เช่น เชิญชวนให้ซื้อสินค้าหรือแนะนำเว็บทางการค้า หรืออาจเกิดจากนักเจาะระบบสมัครเล่นที่ชอบทดลอง

Content Inspection

คือระบบการตรวจสอบเนื้อหาของเว็บไซต์ว่ามีความเหมาะสมหรือไม่

URL Filtering

คือการบล็อกเว็บไซต์ต่างๆ ที่ไม่ต้องการให้ใช้ เพื่อให้การทำงานขององค์กรมีประสิทธิภาพขึ้น และเพื่อไม่ให้เสียเวลาไปใช้เว็บไซต์ที่ไม่สมควรหรือผิดวัตถุประสงค์

Load Balance

การแบ่งและกระจายงานภายในกลุ่มของ server ให้ทำงานไปได้พร้อมๆ กัน เพื่อให้ได้งานมากขึ้นและเร็วขึ้น

ก่อนจะไปดำเนินการติดตั้ง Windows Server ๒๐๐๘ และ Forefront Threat Management Gateway ๒๐๑๐ ในบทต่อไป จะขอกล่าวถึงความรู้เกี่ยวกับไฟร์วอลล์ (firewall) และ Cache Proxy ซึ่งเราจะใช้ประโยชน์จากเรื่องดังกล่าวจากการใช้ Windows Server ๒๐๐๘ และ Forefront Threat Management Gateway ๒๐๑๐ (TMG ๒๐๑๐) สำหรับเครือข่ายในโรงเรียนเพื่อเพิ่มทักษะความรู้ทางด้านเครือข่ายคอมพิวเตอร์ แก่ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ แต่ถ้ามีความรู้อยู่แล้วจะละเว้นข้ามไปเลยก็ได้

ความรู้เกี่ยวกับไฟร์วอลล์เพิ่มเติม

ไฟร์วอลล์ คือ เครื่องมือที่ใช้ป้องกันระบบเครือข่ายจากการติดต่อสื่อสารของระบบเครือขายคอมพิวเตอร์ทั่วไปที่ไม่ได้รับอนุญาต ซึ่งปัญหาพื้นฐานที่สุดในระบบเครือข่ายคอมพิวเตอร์ก็คือในเรื่องความปลอดภัย เช่น การเข้าถึงระบบหรือข้อมูลภายใน ผ่านทางระบบเครือข่ายคอมพิวเตอร์ หรือที่เรียกว่า ลอจิคัลแอคเซส (Logical Access) ซึ่งมักเกิดขึ้นได้ง่ายกว่าการเข้าถึงทางตัวเครื่องจริง (Physical) เพราะการที่เรานำเครือข่ายคอมพิวเตอร์ของเราต่อเข้าระบบเครือข่ายคอมพิวเตอร์อื่นๆ ผ่านทางอินเทอร์เน็ตนั้น ทำให้เราสามารถถูกเข้าถึงได้จากทุกๆ ที่ในโลกนี้ได้

หลักการทำงานของไฟร์วอลล์ ซึ่งมีใน TMG ๒๐๑๐ นั้น TMG ๒๐๑๐ จะกำหนดในการเข้ามาภายในระบบเครือข่ายคอมพิวเตอร์ เมื่อบุคคลภายนอกที่ต้องการใช้งานอินเทอร์เน็ตที่ผ่านการตรวจสอบสิทธิจะสามารถเข้าใช้งานได้ตามปกติ ส่วนคนที่ไม่หวังดีก็ไม่สามารถเข้าใช้งานอินเทอร์เน็ตได้

ไฟร์วอลล์เป็นเครื่องมือรักษาความปลอดภัยที่ทำงานในเชิงป้องกัน ซึ่งจะทำหน้าที่ควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ โดยอาศัยกฎ (Rule) เป็นพื้นฐาน ดังนั้นการที่ข้อมูลหรือแพ็คเก็ตใดๆ จะสามารถผ่านเข้าออกไฟร์วอลล์ได้หรือไม่นั้น จึงขึ้นอยู่กับกฎเป็นสำคัญ เพราะไฟร์วอลล์ โดยตัวเองแล้วนั้นจะไม่รู้ว่าแพ็คเก็ตใดเป็นแพ็คเก็ตที่ปลอดภัย หรือไม่ปลอดภัย ไฟร์วอลล์จะรู้จักเฉพาะแพ็คเก็ตที่ได้รับอนุญาตหรือไม่ได้รับอนุญาตตามกฎที่ระบุไว้เท่านั้น

Cache Proxy

คือ การที่มีไฟล์ที่ผู้ใช้คนใดคนหนึ่งเคยเรียกมา ควรมีที่เก็บไว้เพื่อให้คนอื่นๆ ที่ต้องการไฟล์เดียวกันสามารถนำไปใช้ได้ทันที ช่วยให้การดึงไฟล์ผ่านช่องทางการสื่อสารเกิดขึ้นเพียงครั้งเดียว และ

ผู้ใช้รายอื่นๆ สามารถดึงไฟล์ได้ด้วยความเร็วที่สูงมากขึ้น ไฟล์เหล่านั้นถูกเก็บไว้ในเครื่องแม่ข่ายที่ทำหน้าที่ ซึ่งเรียกว่า Proxy Cache Server

ดังนั้น Proxy Cache เปรียบเสมือนเป็นตัวกลางระหว่างเครื่องลูกข่ายกับอินเทอร์เน็ต โดยที่ตัวเครื่องลูกข่ายไม่ได้ติดต่อโดยตรงกับอินเทอร์เน็ต เช่นกรณีที่เครื่องลูกข่ายต้องการจะเรียกดูข้อมูลในเว็บไซต์ใดๆ Proxy Cache จะค้นหาข้อมูลในฮาร์ดดิสก์ว่ามีข้อมูลนั้นหรือไม่ ถ้ามีก็จะส่งไปให้เครื่องลูกข่าย และทำการสำเนาข้อมูลเก็บไว้ ซึ่งเรียกว่า แคช (Cache) และในครั้งต่อไป ถ้าหากมีเครื่องลูกข่ายเครื่องใดต้องการข้อมูลซ้ำอีก Proxy Cache จะส่งข้อมูลจากแคช (Cache) ไปได้ทันทีโดยไม่ต้องเสียเวลาไปนำมาจากอินเทอร์เน็ตอีก ทำให้ผู้ใช้ในเครื่องลูกข่ายนั้นจะรู้สึกว่ามีความเร็วในการทำงานมาก เราเรียกการทำงานในลักษณะนี้ว่า การทำ Web Caching