โปรแกรมสำหรับป้องกันการเชื่อมต่อกับเว็บไซต์ที่ไม่เหมาะสม

PROGRAM FOR PROTECTION TOAD WEBSITES

โกสิทธิ์ กรีพานิช

ทิพวรรณ เหล่าเพ็ชรรัตน์

สุภาวดี เจริญเวียงเวชกิจ

ปัญหาพิเศษนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรบัณฑิต

ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์

คณะวิทยาศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2544

PROGRAM FOR PROTECTION TOAD WEBSITES

KOSIT KREPANICH

TIPAWAN LAOPETCHARAT

SUPAWADEE CHARORNWIENGWECHAKIJ

A SPECIAL PROJECT SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIRMENT FOR THE DEGREE OF BACHELOR OF SCIENCE

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE

FACULTY OF SCIENCE

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

ACADEMIC YEAR 2001

ปัญหาพิเศษเรื่อง โปรแกรมสำหรับป้องกันการเชื่อมต่อกับเว็บไซต์ที่ไม่เหมาะสม

PROGRAM FOR PROTECTION TOAD WEBSITES

ชื่อนักศึกษา นายโกสิทธิ์ กรีพานิช 41056005

นางสาวทิพวรรณ เหล่าเพ็ชรรัตน์ 41056031

นางสาวสุภาวดี เจริญเวียงเวชกิจ 41056127

ภาควิชา คณิตศาสตร์และวิทยาการคอมพิวเตอร์

สาขาวิชา วิทยาการคอมพิวเตอร์

อาจารย์ที่ปรึกษา อาจารย์วิสันต์ ตั้งวงษ์เจริญ

ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง อนุมัติให้นับปัญหาพิเศษนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร วิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ ประจำปีการศึกษา 2544

คณะกรรมการสอบ		ลายมือชื่อ
ประธานกรรมการ	ดร.นันทิกา เบญจเทพานันท์	
กรรมการ	อาจารย์วีระศักดิ์ นิ่มขุนทด	
กรรมการและอาจารย์ที่ปรึกษา	อาจารย์วิสันต์ ตั้งวงษ์เจริญ	

(ผู้ช่วยศาสตราจารย์ไพรบูลย์ พันธรักษ์พงษ์)

หัวหน้าภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์

ลิขสิทธิ์ของภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปัญหาพิเศษเรื่อง	โปรแกรมสำหรับป้องกันการเชื่อมต่อกับเว็บไซต์ที่ไม่เหมาะสม	
ชื่อนักศึกษา	นายโกสิทธิ์ กรีพานิช	41056005
	นางสาวทิพวรรณ เหล่าเพ็ชรรัตน์	41056031
	นางสาวสุภาวดี เจริญเวียงเวชกิจ	41056127
ปริญญา	วิทยาศาสตรบัณฑิต	
ภาควิชา	คณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์	
สาขาวิชา	วิทยาการคอมพิวเตอร์	
ปีการศึกษา	2544	
อาจารย์ที่ปรึกษา	อาจารย์วิสันต์ ตั้งวงษ์เจริญ	

บทคัดย่อ

ในปัจจุบันเกิดเว็บไซต์ที่ไม่เหมาะสมขึ้นมากมาย เช่น เว็บไซต์ประเภทลามกอนาจาร การพนัน รุนแรง และ ลัทธินอกรีด เป็นต้น ซึ่งเว็บไซต์ประเภทเหล่านี้ไม่มีประโยชน์สำหรับผู้เข้าเยี่ยมชมเว็บไซต์ จึงทำให้เกิดแนวทางในการพัฒนาโปรแกรมเพื่อไม่ให้สามารถเข้าเยี่ยมชมเว็บไซต์ที่จัดอยู่ในประเภทดังกล่าวได้

โปรแกรมป้องกันการเชื่อมต่อเว็บไซต์ที่ไม่เหมาะสม สร้างขึ้นด้วยภาษาจาวาเป็นโปรแกรมที่ช่วยในการป้องการเข้าถึงเว็บไซต์ที่ไม่เหมาะสม โดยจะทำการนำ URL ที่ร้องขอซึ่งมาจากเว็บบราวเซอร์มาทำการตรวจสอบกับ URL ที่อยู่ในไฟล์รายชื่อเว็บไซต์ที่ไม่เหมาะสม ว่าเป็น URL ที่ไม่เหมาะสมหรือไม่ ถ้าเป็น URL ที่ไม่เหมาะสม โปรแกรมป้องกันการเชื่อมต่อเว็บไซต์ที่ไม่เหมาะสม จะแสดงหน้าเว็บเพจที่แสดงให้ผู้ใช้ได้รู้ว่าผู้ใช้ได้เข้าเว็บไซต์ที่ไม่เหมาะสม และมีการ Update ข้อมูลของรายชื่อเว็บไซต์ที่ไม่เหมาะสมกับโปรแกรมทางฝั่ง Server

Special Project Title	Program For Protection Toad Websites	
Students	Mister Kosit Krepanich	41056005
	Miss Tipawan Laopetcharat	41056031
	Miss Supawadee Charornwiengwechakij	41056127
Degree	Bachelor's Degree of Science	
Department	Mathematics and Computer Science, Faculty of Science	
Programme	Computer Science	
Academic Year	2001	
Special Project Advisor	Lecturer Wisan Tangwongcharoen	

ABSTRACT

Nowadays, there are enormous improper Websites such as sex, gambling, violence, and unorthodox Website etc. These Websites are useless for the visitors. Therefore, program about prohibiting people to visit these kinds of Website are developed.

The program is developed by JAVA language. It protects the visitors to access to the improper Website by comparing requested URL with name list of improper URL If the requested URL is in the list of improper URL, this program will display to the user that 'the user is accesses to prohibited Website'. Furthermore, the program always updates the improper name list with the program of server.

กิตติกรรมประกาศ

ในการทำปัญหาพิเศษเรื่องโปรแกรมสำหรับป้องกันการเชื่อมต่อกับเว็บไซต์ที่ไม่เหมาะสม สามารถสำเร็จลุล่วงไปด้วยดี คณะผู้จัดทำต้องขอขอบพระคุณ อาจารย์วิสันต์ ตั้งวงษ์เจริญ อาจารย์ผู้รับผิดชอบปัญหาพิเศษฉบับนี้ที่กรุณาให้คำแนะนำและเป็นที่ปรึกษาในการแก้ปัญหาต่างๆ รวมทั้งเป็นผู้ตรวจสอบความถูกต้องของปัญหาพิเศษฉบับนี้

นอกจากนี้คณะผู้จัดทำต้องขอขอบพระคุณ บิดา มารดา ที่ได้ให้ความสนับสนุนทางด้านกำลังใจและทุนทรัพย์ในการทำปัญหาพิเศษ รวมทั้งเพื่อนๆ และน้องๆ ทุกคนที่ให้ความช่วยเหลือในด้านต่างๆ จนปัญหาพิเศษนี้สามารถสำเร็จด้วยดีไว้ ณ ที่นี้ด้วย

คณะผู้จัดทำ

มีนาคม 2545

สารบัญ

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญภาพ

รูปที่ **หน้า**

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มาของปัญหา

อินเตอร์เน็ตเป็นระบบเครือข่ายที่เชื่อมโยงเครือข่ายมากมายหลากหลายเครือข่ายทั่วโลกเข้าด้วยกัน อินเตอร์เน็ตจึงเป็นแหล่งข้อมูลขนาดใหญ่ที่มีข้อมูลในทุกๆด้าน ซึ่งในปัจจุบันได้มีจำนวนเว็บไซต์เกิดขึ้นมากมาย วัตถุประสงค์ของแต่ละเว็บไซต์ก็แตกต่างกันไป เช่น เพื่อการศึกษา เพื่อธุรกิจ เพื่อความบันเทิง ฯลฯ แต่ก็ได้มีกลุ่มบุคคลหนึ่งได้สร้างเว็บไซต์ที่ไม่เหมาะสมขึ้นมา เช่น เว็บไซต์ลามกอนาจาร เว็บไซต์การพนัน เว็บไซต์แสดงความรุนแรง เว็บไซต์ลัทธินอกรีต เป็นต้น ซึ่งไม่ได้ให้ข้อมูลที่เป็นประโยชน์แก่ผู้ที่เข้าไปในเว็บไซต์เหล่านั้น และทำให้ผู้ที่เข้าไปชมมีสภาวะทางจิตใจที่เปลี่ยนไปในทางที่แย่ลง หรือมีความคิดในทางที่ไม่ก่อให้เกิดประโยชน์และถ้าหากดูแล้วขาดการยั้งคิด อาจจะทำให้เกิดสิ่งที่ไม่ดีตามมาได้ ดังนั้นหน่วยงานต่างๆ ควรหาทางป้องกันโดยเฉพาะอย่างยิ่งสถาบันการศึกษา ควรจะป้องกันนักศึกษาและนักเรียนไม่ให้เข้าเว็บไซต์ที่ไม่เหมาะสม

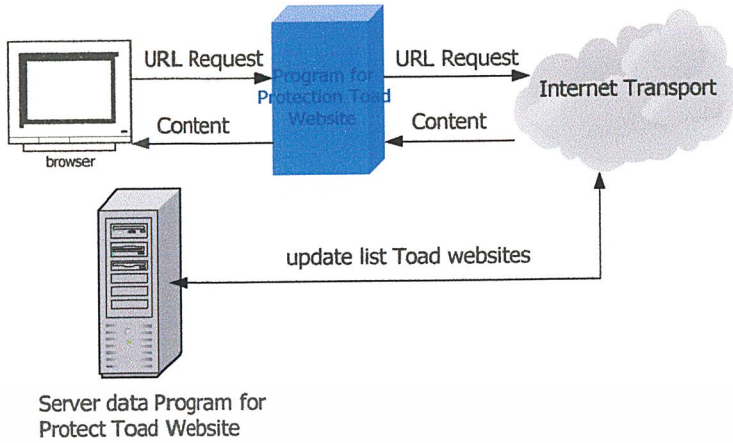
1.2 วัตถุประสงค์ของการทำปัญหาพิเศษ

1. จัดทำโปรแกรมป้องกันการติดต่อเว็บไซต์ที่ไม่เหมาะสม
2. จัดทำโปรแกรมที่มีความสามารถอัพเดตฐานข้อมูลจากเซิร์ฟเวอร์ได้โดยผ่านทางอินเตอร์เน็ต
3. จัดทำโปรแกรมที่มีความสามารถควบคุมการแสดงเว็บเพจบนเว็บบราวเซอร์ได้
4. เพื่อศึกษาการสร้างโปรแกรมทำงานร่วมกับเว็บบราวเซอร์

1.3 ขอบเขตของปัญหาพิเศษ

เป็นโปรแกรมที่ทำงานร่วมกับเว็บบราวเซอร์ โดยทำหน้าที่ป้องกันการติดต่อไปยังเว็บไซต์ที่ไม่เหมาะสมของผู้ใช้งานผ่านเว็บบราวเซอร์ ออกไปยังเว็บเซิร์ฟเวอร์ที่ให้บริการ โดยโปรแกรมนี้จะทำการตรวจสอบการร้องขอ ซึ่งจะตรวจสอบกับฐานข้อมูลที่เก็บไว้ภายในโปรแกรม โดยในฐานข้อมูลจะบรรจุรายชื่อเว็บไซต์ที่ไม่เหมาะสม

เมื่อมีการติดต่อกับอินเตอร์เน็ตไปแล้วในช่วงระยะเวลาหนึ่ง จะมีการส่งข้อความร้องขอไปยังเซิร์ฟเวอร์เพื่อถามหาฐานข้อมูลใหม่ หากมีฐานข้อมูลใหม่ เซิร์ฟเวอร์จะส่งข้อมูลมาอัพเดตฐานข้อมูลเก่าในโปรแกรม ดังแสดงในรูปที่ 1-1



รูปที่ 1-1 แสดงการทำงานของโปรแกรม

1.4 ขั้นตอนในการดำเนินงาน

1. ศึกษาปัญหาและรวบรวมข้อมูลที่เกี่ยวกับปัญหา
2. ศึกษาโปรแกรมที่เกี่ยวข้องกับการแก้ปัญหา
3. เขียนโปรแกรม ทดสอบโปรแกรม เริ่มใช้งาน
4. เข้าใจปัญหา ศึกษาสิ่งที่ต้องแก้ไข แก้ไขโปรแกรม
5. ประเมินผลงาน
6. ทำรายงาน
7. ส่งผลงานและนำเสนอผลงาน

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. โปรแกรมที่มีความสามารถป้องกันการติดต่อเว็บไซต์ที่ไม่เหมาะสม
2. นำโปรแกรมไปป้องกันการติดต่อเว็บไซต์ที่ไม่เหมาะสมให้กับหน่วยงานต่างๆ เช่น สถาบันการศึกษา
3. ได้ศึกษาการเขียนโปรแกรมทำงานร่วมกับเว็บบราวเซอร์

1.6 อุปกรณ์ที่ใช้ในการทำปัญหาพิเศษ

1. เครื่องคอมพิวเตอร์	2	เครื่อง
2. โปรแกรม Java1.2.2	1	ชุด
3. ฮาร์ดดิสก์	2	อัน
4. rack	2	อัน
5. เว็บเซิร์ฟเวอร์	1	ชุด

บทที่2
ทฤษฎีและหลักเกณฑ์ที่เกี่ยวข้อง

2.1 หลักการทำงานของเทคโนโลยีเวิลด์ไวด์เว็บ (WWW)

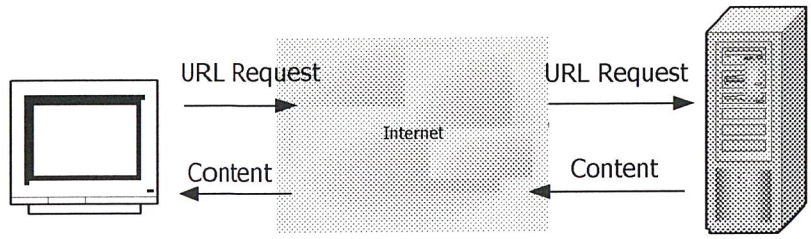
WWW (World-Wild Web) เป็นเทคโนโลยีที่ใช้บน Internet ซึ่ง WWW นี้เป็น Graphic User Interface (GUI) ทำให้ผู้ใช้งานไม่ต้องมีความรู้อะไรมากซึ่งง่ายต่อการใช้งาน WWW ใช้ภาษา Hypertext Markup Language (HTML) และใช้ HyperText Transfer Protocol (HTTP)

เมื่อกล่าวถึงการสื่อสารบน Network และการ ทำงานของโพรโตคอลระดับ Network ส่วนมากจะมีขั้นตอนการทำงานที่ประกอบไปด้วย

- Connection การเชื่อมต่อ HyperText Transfer Protocol (HTTP)
- Request การร้องขอ
- Response การตอบสนอง
- Close การยกเลิกการเชื่อมต่อ

2.2 หลักการทำงานของClient / Server

การทำงานแบบ ไคลเอนต์/เซิร์ฟเวอร์ จะเป็นการแบ่ง Process วิ่งบนส่วนต่างๆ คือ แบ่งโปรแกรมแบ่งเป็น 2 ส่วน ส่วนหนึ่งอยู่ที่ ไคลเอนต์ อีกส่วนหนึ่งอยู่ที่ เซิร์ฟเวอร์



หน้าที่

1. จัดการด้านการแสดงผล
2. จัดการด้านการตอบโต้กับผู้ใช้
3. จัดการร้องขอไปยัง web server
4. จัดการด้านการตรวจสอบข้อมูล

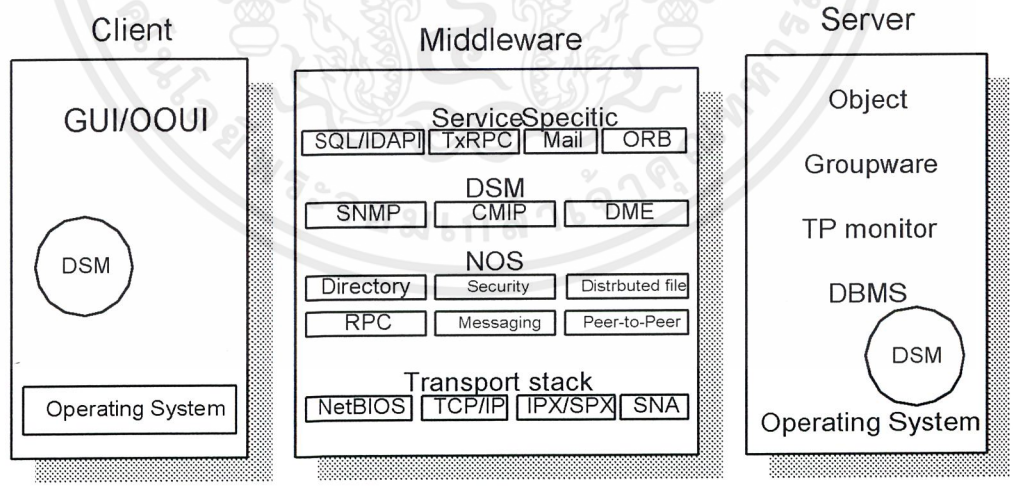
หน้าที่

1. จัดการด้านการร้องขอจากหลาย Client
2. จัดการด้านการเชื่อมต่อ
3. จัดการด้านการเรียกใช้โปรแกรม
4. จัดการด้านความปลอดภัย
5. จัดการด้านการตอบสนองการร้องขอ
6. จัดการความถูกต้องและแน่นอนในกรณีที่ Client ร้องขอมาพร้อมๆ กัน

รูปที่ 2-1 แสดงการทำงานของ Client/Server

2.3 โครงสร้างพื้นฐานของ Client /Server

ประกอบไปด้วย Client Middleware Server



รูปที่ 2-2 แสดงโครงสร้างพื้นฐานของ Client/Server

2.3.1 หลักการทำงานของ Client

เป็นส่วนที่จะรันแอพพลิเคชั่นบนไคลเอนต์ โดยใช้ระบบ GUI (Graphical User Interface) หรือ OOUI (Object Oriented User Interface) หรือ DSM (Distributed System Management) เป็นการติดต่อกับUser ผ่านระบบกราฟฟิก ซึ่งทำงานแบบเชิงวัตถุ (object) จะเห็นว่าโครงสร้างพื้นฐานของ ไคลเอนต์ /เซิร์ฟเวอร์ ถูกแบ่งออกเป็น 3 ส่วนคือ Client, Middleware และ Server

2.3.2 หลักการทำงานของ Middleware

เป็นส่วนที่ทำงานอยู่ระหว่าง ไคลเอนต์ /เซิร์ฟเวอร์ เป็นเสมือนสะพานเชื่อมการทำงาน สามารถแบ่งออกเป็น 4 แบบ คือ Service, Specific, DSM, NOS และ Transport stack

2.3.2.1 Service Specific

Service Specific หรือ การบริการโดยเฉพาะ จะขึ้นอยู่กับการใช้ แอพพลิเคชั่นในการทำงาน เช่น แอพพลิเคชั่นของ object แบบกระจายจะใช้ middleware ORB (Object Reguest Broker) Application group จะใช้ middleware Mail และ TP monitor จะใช้ middleware TxRPC (Transactional Remote Procedure call) ส่วนระบบฐานข้อมูล SQL จะใช้ ODBC (Open Database Connectivity) DRDA (Distribute Relational Database Architecture) ของ IBM , RDA (Remote Database Access) , Oracle Glue , CLI (Call-level Interface)

2.3.2.2 DSM (Distribute System Management)

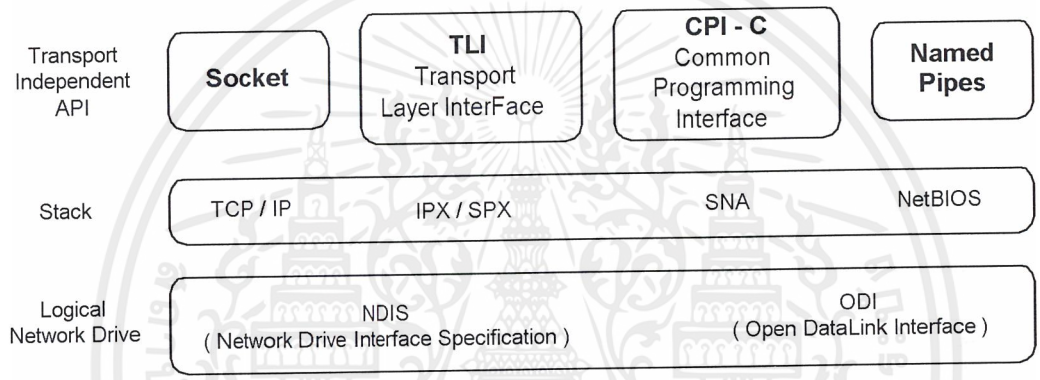
จะรันบนทุกโหนดของระบบ network ที่เป็น ไคลเอนต์ /เซิร์ฟเวอร์ จะมี middleware SNMP (Simple Network Management Protocol), CMLP (Common Management Information Protocol) และ DME

- NOS (Network Operation System) เป็นระบบปฏิบัติการ Network ซึ่งให้บริการทั่วๆ ไปโดยจะมีทั้ง Directory Services , Naming Service , Security/Authentication Service , Message Service
- Distributed file ,RPC , Peer to Peer ฯลฯ ระบบปฏิบัติการเหล่านี้ เช่น Windows NT Server , Netware , Banyan Vines , OSF DCE
- NOS จะช่วยให้การใช้ชื่อ (namespace) เพียงชื่อเดียวสามารถเข้าถึงทรัพยากรต่าง ๆ บนระบบ network ร่วมได้
- NOS จะทำให้ผู้ใช้งาน (user) ไม่ต้องรับรู้เกี่ยวกับความผิดพลาดที่เกิดขึ้น เช่น การรับ-ส่งข้อมูลผิดพลาด ระบบ netware มีปัญหาหรือมีการเคลื่อนย้ายทรัพยากรจาก directory ไปยังเซิร์ฟเวอร์ NOS จะแก้ไขและ update ข้อมูลต่าง ๆ ให้เป็นหนึ่งเดียวทั้งระบบ

- NOS ทำให้สามารถใช้รหัสผ่านเพียง 1 ชุด เข้าสู่ระบบnetwork จากเครื่องใด ที่ไหนก็ได้ โดยจะใช้ระบบรักษาความปลอดภัยแบบ DCE (Distributed Computing Environment) ในการตรวจสอบ
- NOS จะมีระบบ directory แบบ Global directory ซึ่งจะนำคน แอพพลิเคชั่น โปรแกรม สิ่งต่างๆ เข้ามาทำงานร่วมกัน ทำให้ไม่ต้องขึ้นกับสถานที่ สามารถจะเปลี่ยนสถานที่ในการเข้าใช้ทรัพยากรได้
- NOS จะจัดการในเรื่อง Distribute time ให้ทั้งระบบคือจะมีการ Synchronize ในเรื่องเวลาระหว่าง เซิร์ฟเวอร์ และ ไคลเอนต์ ทุกตัว
- NOS จะจัดการในเรื่อง Distributed Security อย่างต่ำจะอยู่ในระดับ C2 ซึ่งจะต้องมีการแสดงตน (Authentication) มีการเข้ารหัสผ่าน (Encrypt) ใช้มาตรฐาน Kerboros และ Application server จะมีอำนาจ (Authorization) ในการใช้ ACLs(Access Control Lists) เพื่อควบคุมการเข้าใช้ทรัพยากรจาก User
- NOS สามารถจะใช้ middleware MOM (Message Oriented Middleware) ในการช่วยจัดคิวข้อความ (Message queue) เพื่อให้ทั้ง ไคลเอนต์ และ เซิร์ฟเวอร์ ยังคงทำงานได้อย่างต่อเนื่องแม้จะมีปัญหาทางระบบสื่อสาร ลักษณะนี้อาจเรียกว่า Loosely-Coupled queue based และอีกรูปแบบ คือการใช้ RPCs (Remote Procedure Calls) ซึ่ง NOS เหล่านี้คือ OSF/DCE , ONC/SUN , Netware 4. Xx / Novell
- Transport stack เป็นบริการพื้นฐานในการสื่อสารระหว่าง ไคลเอนต์ และ เซิร์ฟเวอร์ บนระบบ LAN และ WAN Protocol หลักในส่วนของ Transport stack มีอยู่ 4 ตัว ด้วยกันคือ NetBIOS, TCP/IP, IPX/SPX และ SNA
- NetBIOS เป็นโพรโตคอล ที่ออกแบบโดย บ.ไอบีเอ็มให้ใช้งานกับเครือข่ายขนาดเล็ก ต่อมาพัฒนาเห็น NetBEUI (NetBIOS Extended User Interface) สามารถจะใช้งานกับระบบเครือข่ายที่มีเครื่องคอมพิวเตอร์ตั้งแต่ 20-200 เครื่องไม่สามารถใช้งานกับเครือข่ายขนาดใหญ่ได้และไม่สามารถค้นหาเส้นทางได้ จะเห็นว่าใช้กับงาน Work group เช่น Windows for workgroups Microsoft LAN Management protocol NetBIOS จะทำงานอยู่ในชั้นของ Session Layer ตามมาตรฐาน OSI-7 Layer
- TCP/IP (Transmission Control Protocol / Internet Protocol) เป็นโพรโตคอลที่ใช้งานบนระบบ UNIX พัฒนาขึ้นในปี 2512 โดยกระทรวงกลาโหมของสหรัฐอเมริกามีเครือข่ายชื่อ ARPANET (Advanced Research Project Agency Network) สำหรับ

ใช้งานกับเครือข่ายขนาดใหญ่อย่าง WANs มีความสามารถในการค้นหาเส้นทาง และมีความยืดหยุ่นในการทำงานสูง

- IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) เป็นโพรโตคอลหลักของระบบปฏิบัติการ network Netware มีความฉลาดในการทำงานกว่า NetBIOS คือสามารถค้นหาเส้นทางได้ ทำให้โพรโตคอล IPX/SPX สามารถจะทำงานบนระบบ LAN และ WAN ได้ (แต่การทำงานบนระบบ WAN เช่น internet ยังสู้โพรโตคอล TCP/IP ไม่ได้)
- SNA (Systems Network Architecture) เป็นโพรโตคอลที่ออกแบบโดย บ.ไอบีเอ็ม เพื่อใช้งานบนระบบเครือข่ายเครื่องเมนเฟรมของไอบีเอ็ม



รูปที่ 2-3 แสดงโครงสร้างระดับล่างของ transport stack

2.3.3 หลักการทำงานของ Server

เป็นส่วนที่จะรัน Application ในการจัดการทรัพยากรต่างๆ สำหรับระบบไคลเอนต์ /เซิร์ฟเวอร์ สามารถแบ่งออกได้ 4 แบบ ด้วยกันคือ

- ระบบฐานข้อมูล SQL (DBMS)
- ระบบจัดการ transaction (TP monitor)
- ระบบกรุ๊ปแวร์ (Groupware)
- ระบบออบเจ็กต์แบบกระจาย (Distributes objects)

2.4 หลักการทำงานของเว็บบราวเซอร์ (Web Browser)

เว็บเพจแต่ละหน้าเป็นเอกสารข้อมูลที่ถูกเขียนขึ้นด้วยภาษา HTML ดังนั้นที่เครื่องของเราจะอ่านและแสดงผลเว็บเพจเหล่านี้ได้จะต้องมีโปรแกรมพิเศษสำหรับทำหน้าที่นี้โดยเฉพาะโปรแกรม

เหล่านี้ เรียกว่าเว็บบราวเซอร์ (Web Browser) ซึ่งมีอยู่มากมายในปัจจุบัน แต่ที่รู้จักกันดี ได้แก่ Internet Explorer ของบริษัทไมโครซอฟท์ และ Netscape Navigator ของเน็ตสเคป

2.5 หลักการทำงานของเว็บเซิร์ฟเวอร์(Web Server)

เว็บเซิร์ฟเวอร์ หมายถึง แอพพลิเคชั่นที่ทำหน้าที่รับ และประมวลผลเอกสาร ที่ถูกร้องขอจากผู้ใช้บริการอินเตอร์เน็ต ซึ่งเว็บเซิร์ฟเวอร์จะส่งเอกสารกลับไปแสดงผลให้ผู้ใช้บริการผ่านบราวเซอร์ นอกจากเว็บเซิร์ฟเวอร์จะถูกนำมาให้บริการในอินเตอร์เน็ตแล้ว อาจจะมีการประยุกต์ให้นำมาใช้กับเครือข่ายภายในองค์กรหรืออินทราเน็ตได้เช่นกัน

เดิมทีนั้นเว็บเซิร์ฟเวอร์มักจะอยู่ในเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ UNIX ที่มีประสิทธิภาพสูงและราคาแพง ต่อมาเมื่ออินเตอร์เน็ตขยายความนิยมมาสู่ผู้ใช้ PC ทำให้มีการพัฒนาซอฟต์แวร์ที่ทำหน้าที่เป็นเว็บเซิร์ฟเวอร์บน PC ซึ่งสามารถทำงานได้ทั้ง Windows 95/98 และ Windows NT Server/Workstation ตัวอย่าง เช่น

- NCSA Web Server จาก NCSA เป็นเว็บเซิร์ฟเวอร์ที่สามารถดาวน์โหลดได้ฟรีจากเว็บไซต์ที่ให้บริการดาวน์โหลดฟรีทั่วไป
- Net Server จาก NetScape เป็น WWW Server ที่มีความสามารถรองรับ Java ได้อย่างเต็มรูปแบบ
- Oracle Web Server จาก Oracle เป็นเว็บเซิร์ฟเวอร์จาก Oracle ที่เน้นความสามารถด้านการติดต่อกับ Database Server โดยเฉพาะการใช้งานร่วมกับระบบจัดการฐานข้อมูลของ Oracle ปัจจุบันเราอาจจะได้ยินชื่อที่ตั้งขึ้นใหม่เป็น Application Server (ซึ่งก็คือ Oracle Web Server ตัวเดิมที่ถูกพัฒนาขึ้น)
- Personal Web Server ของ Microsoft เป็นเว็บเซิร์ฟเวอร์ที่สามารถใช้งานได้กับ Windows 95/98 หรือ Windows NT Workstation และรองรับการใช้งานร่วมกับ Active Server Pages โดยเราสามารถดาวน์โหลดมาใช้ได้ฟรีจากเว็บไซต์ของไมโครซอฟต์
- Internet Information Server ของ Microsoft เป็น Internet Server ที่แถมมากับ Windows NT Server มีความสามารถให้บริการได้ ทั้ง WWW, FTP และ Gopher

2.6 หลักการทำงานของ Proxy Server

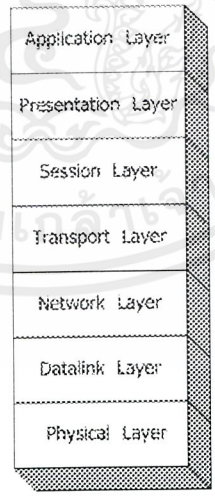
Proxy Server เป็นอุปกรณ์อีกประเภทหนึ่งที่ช่วยให้การใช้งานบนอินเตอร์เน็ตมีประสิทธิภาพมากขึ้น หรือได้รับความสะดวกมากขึ้น โดยทำงานเป็นเซิร์ฟเวอร์อีกตัวหนึ่งอยู่ในเน็ตเวิร์ก ซึ่งไคลเอนต์ต่างๆ ที่ต้องการติดต่อเข้าไปใช้งานเว็บเซิร์ฟเวอร์บนอินเตอร์เน็ตก็จะต้องติดต่อผ่าน

Proxy เข้าไป เสมือนว่า Proxy เป็นตัวกลางระหว่างไคลเอนต์ของเน็ตเวิร์ก และเครือข่ายอินเตอร์เน็ตนั่นเอง นอกจากนั้น Proxy บางตัวยังสามารถทำงานเป็น Firewall ได้ด้วย

การทำงานของ Proxy จะทำตามมาตรฐานที่กำหนดไว้โดย CERN (Center European pour la Research Nucleaire หรือชื่อเต็มในภาษาอังกฤษคือ European Laboratory for Particle Physics) เมื่อไคลเอนต์ต้องการใช้ข้อมูลจากเซิร์ฟเวอร์ ก็จะส่งคำร้องขอผ่านไปยัง Proxy จากนั้นก็เป็นหน้าที่ของ Proxy ที่จะติดต่อไปยังเว็บเซิร์ฟเวอร์บนอินเตอร์เน็ตอีกทีหนึ่ง ซึ่งโพรโตคอลที่ Proxy รองรับได้ก็จะมีโพรโตคอลมาตรฐานของอินเตอร์เน็ตทั่วๆ ไปเช่น HTTP, FTP, Gopher และอื่นๆ ซึ่งเมื่อ Proxy ได้ข้อมูลจากเว็บเซิร์ฟเวอร์แล้ว ก็จะนำข้อมูลที่ได้นั้นแจกจ่ายกลับไปยังเครื่องที่เป็นไคลเอนต์ต่อไป ดังนั้นจะเห็นได้ว่าข้อมูลบางส่วนที่ไคลเอนต์เรียกใช้งานผ่าน Proxy จะถูกเก็บไว้ที่ Proxy ด้วย ช่วยให้ไม่ต้องไปดึงรายละเอียดที่ต้องการจากเว็บเซิร์ฟเวอร์ใหม่ทุกครั้งที่ไคลเอนต์เรียกใช้งาน

2.7 รูปแบบระบบเครือข่ายมาตรฐานสากล

องค์การ International Standards Organization (ISO) ได้กำหนดให้การสื่อสารข้อมูลจากระบบคอมพิวเตอร์ หนึ่งไปยังอีกระบบหนึ่งแบ่งออกเป็น 7 ขั้นตอนย่อยๆ ซึ่งคอมพิวเตอร์ทั้งสองระบบจะมีขั้นตอนทั้ง 7 นี้เหมือนกันทั้งสองฝั่ง จะเรียกการสื่อสารข้อมูลนี้ว่า OSI 7-Layer Reference Model ดังแสดงใน รูปที่2.4 โดยโครงสร้างการสื่อสารข้อมูลที่กำหนดขึ้นมีคุณสมบัติดังนี้ คือ

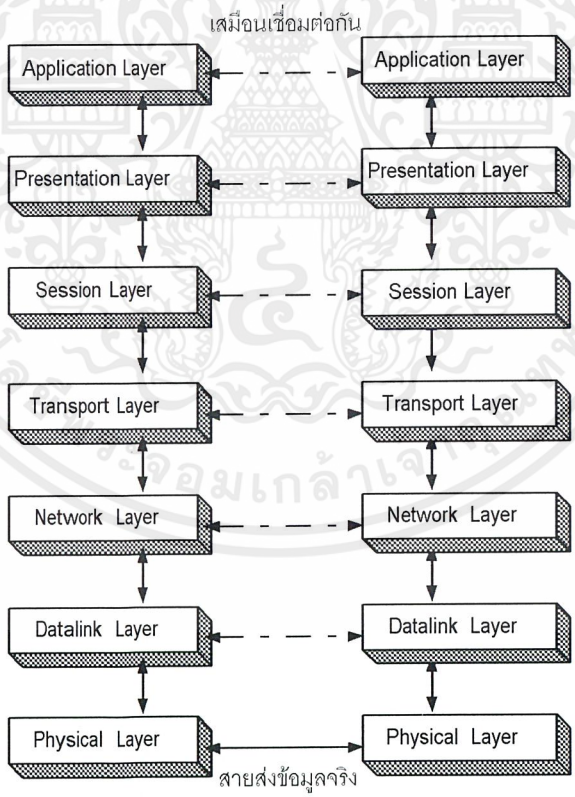


รูปที่ 2-4 โครงสร้างของ OSI 7 – Layer Model

แต่ละขั้นของการสื่อสารข้อมูลจะเรียกว่า Layer ในการสื่อสารข้อมูลจะประกอบด้วยชั้นย่อยๆ 7 ชั้น ในแต่ละชั้น หรือแต่ละ Layer จะเสมือนเชื่อมต่ออยู่กับชั้นที่เทียบเท่าของคอมพิวเตอร์อีก

ด้านหนึ่ง ส่วนการเชื่อมต่อกันจริงๆจะมีเพียงชั้น Physical Layer ซึ่งเป็นชั้นล่างสุดเท่านั้นที่มีการรับส่งข้อมูลเกิดขึ้นผ่านสายส่งข้อมูลระหว่างคอมพิวเตอร์ทั้งสองระบบ ส่วนชั้นอื่นๆจะไม่ได้เชื่อมต่อกันจริง เพียงแต่ทำงานเสมือนกับว่ามีการติดต่อรับส่งข้อมูลกับกลไกในชั้นเดียวกันของคอมพิวเตอร์อีกด้านหนึ่งเท่านั้น

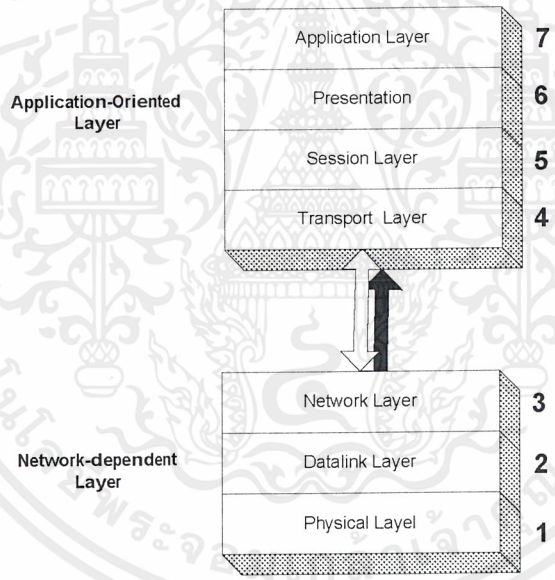
คุณสมบัติข้อที่สองของ OSI 7-Layer Model ก็คือ แต่ละขั้นที่ทำหน้าที่รับส่งข้อมูลจะมีการติดต่อรับส่งข้อมูลกับชั้นที่อยู่ติดกับตัวเองเท่านั้น จะติดต่อรับส่งข้อมูลข้ามกระโดดไปชั้นอื่นๆในคอมพิวเตอร์ของตัวเองไม่ได้ เช่น คอมพิวเตอร์ด้านที่ส่งข้อมูลออกไปให้ผู้รับ ชั้น Application Layer ซึ่งอยู่บนสุดของด้านส่งข้อมูล จะมีการเชื่อมต่อเข้ากับชั้น Presentation Layer เท่านั้น ซึ่งชั้น Presentation Layer นี้ก็จะมีการเชื่อมต่อรับส่งข้อมูลกับชั้น Application Layer และชั้น Transport Layer ของคอมพิวเตอร์ด้านส่งข้อมูลเท่านั้น ส่วนชั้น Application Layer จะกระโดดไปทำการรับส่งข้อมูลกับชั้น Transport Layer หรือ Session Layer ไม่ได้ คอมพิวเตอร์ด้านรับข้อมูลผ่านสายส่งข้อมูล และจะทำการรับข้อมูลจากชั้นที่ 1 ไล่ขึ้นไปจนถึงชั้น Application Layer ตามลำดับ ลำดับชั้นของการส่งข้อมูลชั้น Application Layer จะเสมือนเชื่อมต่อเข้ากับลำดับชั้นการรับข้อมูลในชั้น Application Layer ของคอมพิวเตอร์อีกด้านหนึ่ง ดังแสดงในรูปที่ 2.5



รูปที่ 2-5 การรับส่งข้อมูลของ OSI 7-Layer Model

ผู้ใช้ หรือ User จะติดต่อข้อมูลผ่านทางชั้น 7 ซึ่งอยู่ด้านบนสุดของ OSI 7- Layer Model เท่านั้น ในทางทฤษฎีแล้วแต่ละชั้นของการรับส่งข้อมูลจะมีฟังก์ชั่นการทำงานที่แน่นอน และแยกเด็ดขาดออกจากกัน สามารถที่จะนำแต่ละชั้นของแต่ละบริษัทมาเชื่อมต่อกันได้อย่างไม่มีขีดจำกัด แต่ในทางปฏิบัตินั้น OSI 7 – Layer Model จะแบ่งออกเป็น 2 กลุ่มใหญ่ๆ คือ กลุ่มแรกได้แก่ 4 ชั้นด้านบน คือชั้นที่ 7,6,5 และ 4 ทำหน้าที่เชื่อมต่อรับส่งข้อมูลระหว่างผู้ใช้กับซอฟต์แวร์โปรแกรมประยุกต์ ให้รับส่งข้อมูลกับฮาร์ดแวร์ที่อยู่ชั้นล่างได้ถูกต้อง เรียกว่า Application-oriented layers ซึ่งจะเกี่ยวข้องกับซอฟต์แวร์เป็นหลัก โดย 4 ชั้นด้านบนนี้จะเป็นซอฟต์แวร์ของบริษัทใดบริษัทหนึ่งรวมอยู่อย่างเบ็ดเสร็จในโปรแกรมเดียว จะแยกออกจากกันเป็นชั้นๆ เพื่อใช้โปรแกรมของบริษัทอื่นได้ลำบาก หรือในบางกรณีก็อาจทำไม่ได้เลย

กลุ่มที่สองจะเป็นชั้นล่าง ได้แก่ ชั้นที่ 3, 2 และ 1 ทำหน้าที่เกี่ยวกับการรับส่งข้อมูลผ่านสายส่ง และควบคุมการรับส่งข้อมูล ตรวจสอบข้อผิดพลาด รวมทั้งเลือกเส้นทางที่ใช้ในการรับส่งข้อมูล ซึ่งจะเกี่ยวข้องกับฮาร์ดแวร์เป็นหลัก เรียกว่า Network dependent layers ดังแสดงในรูปที่ 2-6



รูปที่ 2-6 การแบ่งกลุ่มของ OSI 7-Layer Model

ซึ่งในส่วนของ 3 ชั้นล่างสุด หรือชั้นที่ 1 , 2 และ 3 นั้น เนื่องจากเกี่ยวข้องกับฮาร์ดแวร์และโปรแกรมควบคุมฮาร์ดแวร์เป็นหลัก ทำให้สามารถแยกแต่ละชั้นออกจากกันได้ง่าย และใช้ผลิตภัณฑ์ของต่างบริษัทกันในแต่ละชั้นได้อย่างไม่มีปัญหา

OSI 7-Layer Model ที่แบ่งการรับส่งข้อมูลระหว่างคอมพิวเตอร์สองระบบออกเป็น 7 ชั้นนั้น แต่ละชั้นมีชื่อเรียกและหน้าที่การทำงานดังนี้ คือ

ชั้นที่ 7 Application Layer

เป็นชั้นที่อยู่บนสุดของขบวนการรับส่งข้อมูล ทำหน้าที่เชื่อมต่อผู้ใช้เข้าระบบคอมพิวเตอร์ โดยรับคำสั่งต่างๆ จากผู้ใช้ให้ระบบคอมพิวเตอร์แปลความหมาย และทำงานตามคำสั่งที่ได้รับในระดับโปรแกรมประยุกต์ เช่น แปลความหมายของการกดปุ่มบนเมาส์ให้เป็นคำสั่งในการก๊อปปี้ไฟล์ หรือดึงข้อมูลมาแสดงผลบนจอภาพ เป็นต้น ซึ่งการแปลคำสั่งจากผู้ใช้ส่งให้กับคอมพิวเตอร์รับไปทำงานนี้ จะต้องแปลออกมาถูกต้องตามกฎ (Syntax) ที่ใช้ในระบบปฏิบัติการของคอมพิวเตอร์นั้นๆ ตัวอย่างเช่น ถ้ามีการก๊อปปี้ไฟล์เกิดขึ้นในระบบ คำสั่งที่ใช้จะต้องสร้างไฟล์ได้ถูกต้อง มีชื่อไฟล์ยาวไม่เกินจำนวนที่ระบบปฏิบัติการใช้อยู่ และชื่อไฟล์ต้องประกอบด้วยตัวอักษรตามที่กำหนด ไม่มีตัวอักษรต้องห้ามมาตั้งเป็นชื่อไฟล์ เป็นต้น สิ่งต่างๆเหล่านี้จะเกิดขึ้นในชั้นที่ 7 ของการสื่อสารข้อมูล รวมทั้งฟังก์ชันในการเชื่อมต่อรับส่งข้อมูลระหว่างชั้นที่ 7 กับชั้นที่ 6 ด้วย

ชั้นที่ 6 Presentation Layer

เป็นชั้นที่ทำหน้าที่ตกลงกับคอมพิวเตอร์อีกด้านหนึ่งว่า การรับส่งข้อมูลในระดับโปรแกรมประยุกต์จะมีขั้นตอนและข้อบังคับอย่างไร ข้อมูลที่ทำการรับส่งกันในชั้นที่ 6 นี้จะอยู่ในรูปแบบของข้อมูลชั้นสูง ซึ่งอยู่ในรูปแบบของคำสั่งที่มีกฎ (Syntax) บังคับอย่างแน่นอน เช่น ในการก๊อปปี้ไฟล์ก็จะมีขั้นตอนย่อยประกอบกัน คือสร้างไฟล์ที่กำหนดขึ้นมาเสียก่อน จากนั้นจึงเปิดไฟล์ แล้วทำการรับข้อมูลจากปลายทางมาเก็บลงในไฟล์ที่สร้างขึ้นใหม่นี้ โดยเนื้อหาของข้อมูลที่ทำการรับส่งระหว่างกัน ก็คือคำสั่งของขั้นตอนย่อย ๆข้างต้นนั่นเอง คำสั่งเหล่านี้จะต้องหมายถึงว่าจะให้ทำอะไรบ้างและถูกต้องตามกฎด้วย นอกจากนี้ในชั้นที่ 6 ยังทำหน้าที่แปลความหมายของคำสั่งที่ได้รับจากชั้นที่7 ให้เป็นคำสั่งระดับปฏิบัติการส่งให้ชั้นที่ 5 ต่อไปอีกด้วย

ชั้นที่ 5 Session Layer

ทำหน้าที่ควบคุม “จังหวะ” ในการรับส่งข้อมูลของคอมพิวเตอร์ทั้งสองด้านที่รับส่งแลกเปลี่ยนข้อมูลกันให้มีความสอดคล้องกัน (Synchronization) และกำหนดวิธีที่ใช้รับส่งข้อมูล เช่น อาจจะเป็นในลักษณะสลับกันส่ง (Half Duplex) หรือรับส่งข้อมูลพร้อมกันทั้งสองด้าน (Full Duplex) ซึ่งในชั้นที่ 5 นี้จะเป็นชั้นที่ใช้ควบคุมการรับส่งข้อมูลในลักษณะดังกล่าว ข้อมูลที่รับส่งกันในชั้นที่ 5 นี้จะอยู่ในรูปของ dialog หรือประโยคของข้อมูลที่สนทนาโต้ตอบกันระหว่างด้านรับและด้านที่ส่งข้อมูล ไม่ได้มองเป็นคำสั่งอย่างในชั้นที่ 6 เช่น เมื่อผู้รับได้รับข้อมูลส่วนแรกเรียบร้อยแล้ว และพร้อมที่จะรับข้อมูลส่วนที่สองต่อไป คล้ายกับการสนทนาโต้ตอบกันระหว่างผู้รับและผู้ส่งนั่นเอง

ชั้นที่ 4 Transport Layer

ทำหน้าที่เชื่อมต่อการรับส่งข้อมูลระดับสูงของชั้นที่ 5 (ซึ่งมองข้อมูลอยู่ในรูปที่เรียกว่า dialog หรือประโยคของข้อมูลที่โต้ตอบกัน) มาเป็นข้อมูลที่รับส่งในระดับฮาร์ดแวร์ เช่น แปลงค่าหรือชื่อของคอมพิวเตอร์ในเครือข่ายให้เป็น network address พร้อมทั้งเป็นชั้นที่ควบคุมการรับส่งข้อมูลจากปลายด้านส่งถึงปลายด้านรับข้อมูล ให้ข้อมูลมีการไหลลื่นตลอดเส้นทางตามจังหวะที่ควบคุม

จากชั้นที่ 5 โดยในชั้นที่ 4 นี้จะเป็นรอยต่อระหว่างการรับส่งข้อมูลของซอฟต์แวร์กับฮาร์ดแวร์ การรับส่งข้อมูลของระดับสูงจะถูกแยกจากฮาร์ดแวร์ที่ใช้รับส่งข้อมูลที่ชั้นที่ 4 นี้ และจะไม่มีส่วนใดผูกติดกับฮาร์ดแวร์ที่ใช้รับส่งข้อมูลในระดับล่าง ดังนั้นฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ควบคุมการรับส่งข้อมูลในระดับล่างลงไปจากชั้นที่ 4 จึงสามารถสับเปลี่ยนและใช้ข้ามไปมากับซอฟต์แวร์รับส่งที่อยู่ข้างบน (ตั้งแต่ชั้นที่ 4 ขึ้นไปถึงชั้นที่ 7) ได้ง่าย หน้าที่อีกประการหนึ่งของชั้นที่ 4 คือการควบคุมคุณภาพของการรับส่งข้อมูลให้มีมาตรฐานในระดับที่ตกลงกันของทั้งสองฝ่าย และการตัดข้อมูลออกเป็นส่วนย่อยๆให้เหมาะกับลักษณะการทำงานของฮาร์ดแวร์ที่ใช้ในเน็ตเวิร์ก เช่น หากชั้นที่ 5 ต้องการส่งข้อมูลที่มีความยาวมากเกินกว่าที่ระบบเครือข่ายจะส่งได้ ชั้นที่ 4 ก็จะทำหน้าที่ตัดข้อมูลออกเป็นส่วนย่อยๆ แล้วส่งไปให้ผู้รับ ข้อมูลที่ได้รับปลายทางก็จะถูกนำมาต่อกันที่ชั้นที่ 4 ของด้านผู้รับ และส่งให้ชั้นที่ 5 ต่อไป

ชั้นที่ 3 Network Layer

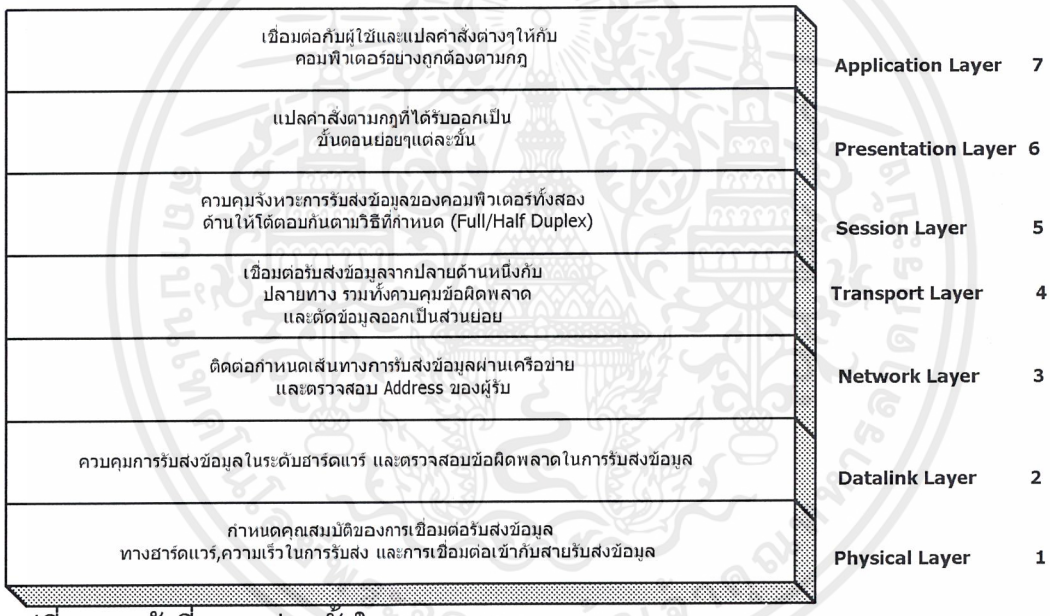
ทำหน้าที่เชื่อมต่อคอมพิวเตอร์ของด้านรับและด้านส่งเข้าหากันผ่านระบบเครือข่าย พร้อมทั้งเลือกหรือกำหนดเส้นทางที่จะใช้ในการรับส่งข้อมูลระหว่างกัน และส่งผ่านข้อมูลที่ได้รับยังอุปกรณ์ในเครือข่ายต่างๆ จนกระทั่งถึงปลายทาง ในชั้นที่ 3 นี้ข้อมูลที่รับส่งกันจะอยู่ในรูปแบบของกลุ่มข้อมูลที่เรียกว่า Packet หรือ Frame ข้อมูลที่ชั้น 4,5,6 และ 7 มองเห็นเป็นคำสั่งและ Dialog ต่างๆ นั้น จะถูกแปลงและผนึกรวมอยู่ในรูปของ Packet หรือ Frame ที่มีเพียงแอดเดรสของผู้รับ, ผู้ส่ง, ลำดับการรับส่งและส่วนของข้อมูลเท่านั้น ตัวเนื้อหาของข้อมูลจะไม่มีผลใดๆ ในการรับส่งข้อมูลเลย ไม่ว่าข้อมูลในระดับสูงจะเป็น วิดีโอ, ภาพ, เสียง หรือข้อมูลอื่นใดก็ตาม แต่ในชั้นที่ 3 จะมองข้อมูลทั้งหมดเป็น Packet หรือ Frame เท่านั้น หน้าที่อีกประการหนึ่งของชั้นที่ 3 นี้คือการทำ Call Setup หรือเรียกติดต่อคอมพิวเตอร์ปลายทางก่อนการรับส่งข้อมูล และการทำ Call Clearing หรือยกเลิกการติดต่อเมื่อการรับส่งข้อมูลจบลงแล้ว ในกรณีที่การรับส่งข้อมูลนั้นต้องมีการติดต่อกันก่อน

ชั้นที่ 2 Datalink Layer

เป็นชั้นที่ทำหน้าที่เชื่อมต่อการรับส่งข้อมูลในระดับฮาร์ดแวร์ โดยเมื่อมีการสั่งให้รับข้อมูลจากในชั้นที่ 3 ลงมา ชั้นที่ 2 จะทำหน้าที่แปลคำสั่งนั้นให้เป็นคำสั่งควบคุมฮาร์ดแวร์ที่ใช้รับส่งข้อมูล ทำการตรวจสอบข้อผิดพลาดในการรับส่งข้อมูลของระดับฮาร์ดแวร์ และแก้ไขข้อผิดพลาดที่ตรวจพบนั้น ข้อมูลที่อยู่ในชั้นที่ 2 นี้จะอยู่ในรูปของ Frame คือกลุ่มของข้อมูลที่มีรูปร่างตามข้อบังคับของฮาร์ดแวร์ที่ใช้ในการรับส่งข้อมูล เช่น ถ้าฮาร์ดแวร์ที่ใช้เป็น Ethernet LAN ข้อมูลก็จะมีรูปร่างของ Frame ตามที่ระบุไว้ในมาตรฐานของ Ethernet หากว่าฮาร์ดแวร์ที่ใช้รับส่งข้อมูลเป็นชนิดอื่น เช่น Token Ring LAN Fiber Distributed Data Interface (FDDI)รูปร่างของ Frame ที่ใช้ในการรับส่งข้อมูลก็จะเปลี่ยนไปตามมาตรฐานนั้นๆ

ชั้นที่ 1 Physical Layer

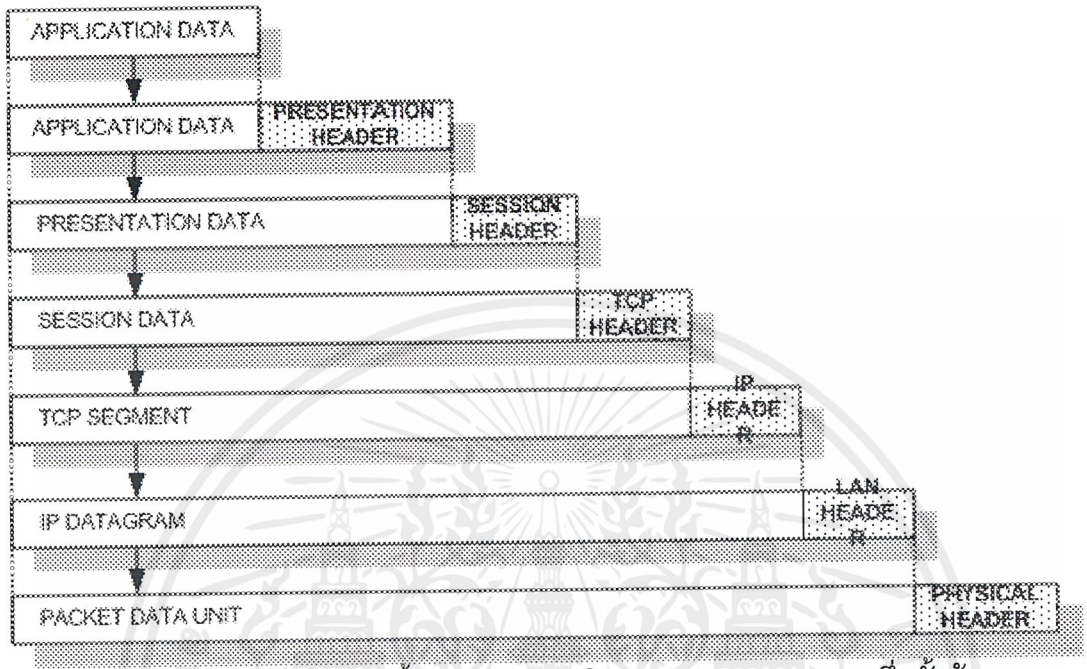
เป็นชั้นล่างสุดของขั้นตอนในการรับส่งข้อมูลของ OSI 7-Layer Reference Model ซึ่งเป็นชั้นเดียวที่มีการเชื่อมต่อกันทางกายภาพระหว่างคอมพิวเตอร์สองระบบที่ทำการรับส่งข้อมูลกัน ในชั้นที่ 1 นี้จะกำหนดคุณสมบัติทางกายภาพของฮาร์ดแวร์ที่ใช้เชื่อมต่อระหว่างคอมพิวเตอร์ทั้งสองระบบ เช่น สายที่ใช้รับส่งข้อมูลจะเป็นแบบไหน, ข้อต่อหรือปลั๊กที่ใช้ในการรับส่งข้อมูลมีมาตรฐานอย่างไร, ใช้ไฟกี่โวลต์, ความเร็วในการรับส่งข้อมูลเป็นเท่าใด, สัญญาณที่ใช้รับส่งข้อมูลในสายมีรูปร่างอย่างไร ข้อมูลในชั้นที่ 1 นี้จะมองเห็นเป็นการรับส่งข้อมูลทีละบิตเรียงต่อกันไป โดยไม่มีการพิจารณาเรื่องความหมายของข้อมูลเลย การรับส่งข้อมูล “0” หรือ “1” ไปให้คอมพิวเตอร์ด้านรับข้อมูลในระดับฮาร์ดแวร์เท่านั้น หากการรับส่งข้อมูลมีปัญหาเนื่องจากฮาร์ดแวร์ เช่น สายสัญญาณที่ใช้รับส่งข้อมูลขาด, อุปกรณ์เสียหาย ก็จะเป็นหน้าที่ของชั้นที่ 1 นี้เช่นกันที่จะตรวจสอบและแจ้งข้อผิดพลาดนั้นให้ชั้นอื่นๆ ที่อยู่เหนือขึ้นไปทราบ



รูปที่ 2-7 หน้าที่ของแต่ละชั้นใน OSI 7- Layer Model

ในการรับส่งข้อมูลใน OSI 7-Layer Model นั้น ข้อมูลจากชั้นบนสุด คือชั้นที่ 7 เมื่อถูกส่งลงไปในชั้นถัดลงไป ข้อมูลเดิมก็จะถูกผนึกรวมกับข้อมูลที่ใช้ควบคุมของแต่ละชั้นซ้อนๆ กันเป็นลำดับเท่ากับจำนวนชั้นที่ผ่านลงไป ตัวอย่างเช่น Application Data เมื่อถูกส่งลงไปยังชั้นถัดไปก็จะถูกผนึกด้วย Application Header และทั้ง Application Header และ Application Data จะรวมกันเป็นข้อมูลของชั้นที่อยู่ถัดลงไปอีก ซึ่งชั้นที่อยู่ถัดลงไปอีกก็จะผนึกข้อมูลนี้ด้วย Header ของมันเองอีกครั้งหนึ่ง และทั้ง Header และข้อมูลเดิมนี้ก็จะกลายเป็นข้อมูลในชั้นถัดลงไปอีกเรื่อยๆ เป็นเช่นนี้จนกระทั่งถึงชั้นล่างสุด ซึ่งเป็น Physical Layer ซึ่งเมื่อข้อมูลถูกส่งไปถึงปลายทาง ข้อมูลที่

ได้รับจะถูกแยก Header ที่เพิ่มเข้ามาเนื้อออกทีละชั้น ซึ่งเป็นขบวนการย้อนกลับกับด้านส่ง จนกระทั่งถึงชั้นบนสุด จึงจะเป็นข้อมูลของ Application Data ให้ผู้รับตามต้องการ ดังแสดงในรูปที่ 2-8



รูปที่ 2-8 การรับส่งข้อมูลแต่ละชั้นของ TCP/IP ใน OSI 7-Layer Model ซึ่งทั้งข้อมูลและ TCP Header จะถูกผนึกรวมกันเป็นข้อมูลเรียกว่า IP Datagram

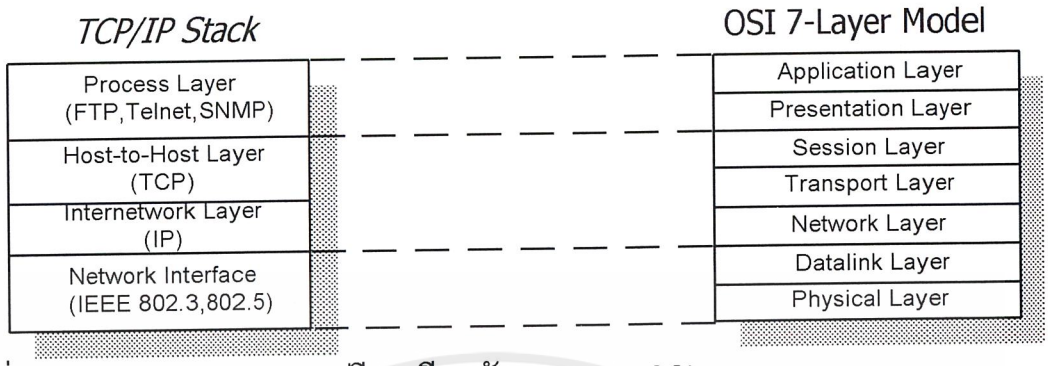
2.8 โครงสร้างของโพรโตคอลTCP/IP

โพรโตคอล TCP/IP มีการจัดกลไกการทำงานเป็นชั้นหรือ layer เรียงต่อกัน โดยในแต่ละ layer จะมีการทำงานเทียบได้กับ OSI model มาตรฐาน แต่บาง layer ของโพรโตคอล TCP/IP จะทำงานเทียบกับ OSI หลาย layer ปนกัน ซึ่งในแต่ละ layer ของโพรโตคอล TCP/IP จะประกอบด้วย

- Process layer
- Host-to-Host layer
- Internetwork layer
- Network Interface layer

โดยเมื่อเทียบกับมาตรฐาน OSI model แล้วจะเป็นดังรูปที่ 2.9 ซึ่งจะเห็นว่าบางกลไกของโพรโตคอล TCP/IP เทียบได้กับมาตรฐาน OSI model สองชั้น หรือบางกลไกก็ทำงานคาบเกี่ยวกันระหว่างสองชั้นของ OSI model ตัวอย่างเช่น กลไกการทำงานของโพรโตคอล TCP/IP ในส่วน Network Interface layer เมื่อเทียบกับมาตรฐาน OSI model จะเทียบได้กับ Data Link layer

และ Physical layer 2 ชั้นรวมกัน เป็นต้น ในแต่ละกลไกของโพรโตคอล TCP/IP จะมีโพรโตคอลอื่นๆในชุดของ TCP/IP ร่วมทำงานอยู่ด้วย



รูปที่ 2-9 แสดง TCP/IP stack เปรียบเทียบกับมาตรฐาน OSI

2.8.1 หลักการทำงานของ Process layer

จากรูปที่ 2-9 แสดงลำดับชั้นการทำงานของโพรโตคอล TCP/IP เทียบกับมาตรฐาน OSI model นั้นในชั้นบนสุดเรียกว่า Process layer ทำงาน 2 หน้าที่เทียบได้กับ Application layer และ Presentation layerในชั้นนี้จะรองรับการทำงานของแอพพลิเคชั่นต่างๆ ที่ทำงานเป็นโปรเซสอยู่ในเครื่องเซิร์ฟเวอร์ให้บริการและเครื่องที่ขอใช้บริการ หรือไคลเอนต์ (client) ซึ่งจะติดต่อกันผ่านแอพพลิเคชั่นเฉพาะแอพพลิเคชั่นอีกทีหนึ่ง ตัวอย่างเช่น เมื่อผู้ใช้งานอินเตอร์เน็ตต้องการโอนถ่ายไฟล์หรือ download ข้อมูลจากเครื่องเซิร์ฟเวอร์ที่ให้บริการ โดยอาจจะเรียกใช้โปรแกรม ftp client ทั่วไป เช่น โปรแกรม WS_ftp ติดต่อกับโปรเซส ftp ที่กำลังให้บริการอยู่ที่เครื่องเซิร์ฟเวอร์ จากนั้นตัวโปรเซส ftp ก็จะเรียกใช้โพรโตคอล FTP (File Transfer Protocol) เพื่อทำการโอนถ่ายไฟล์นี้ หรือถ้าผู้ใช้ต้องการเรียกใช้งานคอมพิวเตอร์เครื่องที่อยู่ห่างไกลออกไปด้วยการใช้โปรแกรม telnet เพื่อติดต่อกัน หรือในกรณีที่มีการเรียกใช้โปรแกรม web browser เช่น Netscape Navigator เพื่อเรียกดูเว็บเพจในเว็บไซต์ CNN ที่เครื่องซึ่งให้บริการเว็บของ CNN ก็จะมีโปรเซส HTTP (HyperText Transfer Protocol) ทำงานอยู่และจะติดต่อกับผู้ใช้ผ่านโพรโตคอล HTTP เป็นต้น

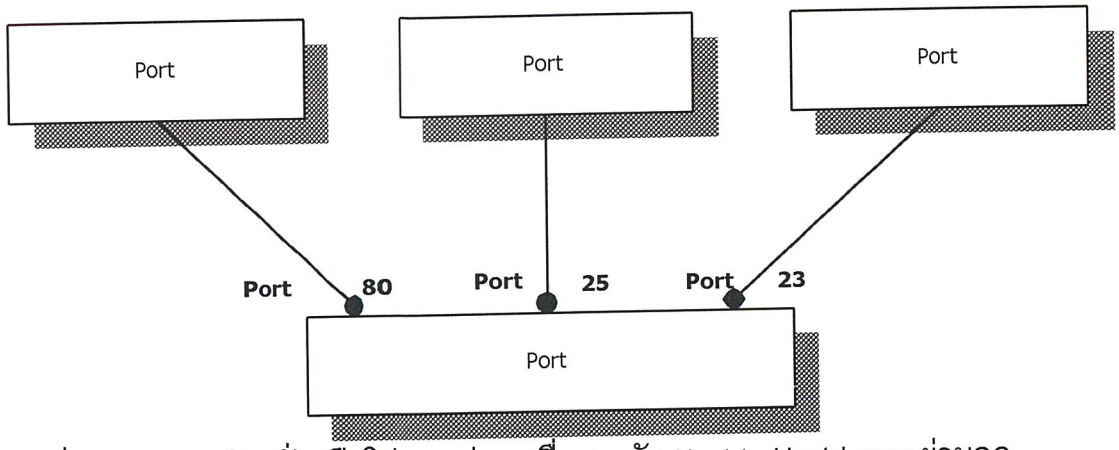
การทำงานของแอพพลิเคชั่นต่างๆจะอยู่ที่ Process layer นี้ และมีการติดต่อกันตามแต่ละโพรโตคอลเฉพาะแล้วแต่แอพพลิเคชั่นที่ใช้งาน จากการที่ Process layer ของ TCP/IP รองรับให้โพรโตคอลอื่นทำงานได้หลายๆอย่างพร้อมกัน เช่น เปิดโปรแกรม Internet Explorer เพื่อเรียกดูเว็บเพจ พร้อมกับใช้งานโปรแกรม Outlook Express เพื่อรับส่งอีเมล์ไปพร้อมกันได้โดยไม่ต้องรอให้ทำงานอย่างหนึ่งอย่างใดเสร็จก่อนหรือในปัจจุบันมีการพัฒนาโปรแกรม web browser ให้สามารถเรียกใช้งานโพรโตคอลอื่นๆ ได้มากขึ้น ทำให้สามารถใช้โปรแกรม web browser โอนถ่ายไฟล์ข้อมูลที่ใช้โพรโตคอล FTP ได้โดยไม่ต้องไปหาโปรแกรมอื่นมาใช้

โพรโตคอลหลักๆ ที่ทำงานใน Process layer ได้แก่ FTP (File Transfer Protocol) , Telnet , HTTP (HyperText Transfer Protocol) และ SMTP (Simple Mai Transfer protocol) นอกจากนี้ยังมีโพรโตคอลอื่นที่อยู่เบื้องหลัง เช่น

- โพรโตคอล DNS (Domain Name System) ที่ทำหน้าที่แปลงข้อมูลชื่อ domain name หรือชื่อเว็บไซต์ทั้งหลายให้เป็นหมายเลข IP address
- โพรโตคอล SNMP (Simple Network Management Protocol) ใช้ในการควบคุมและตรวจสอบอุปกรณ์ที่อยู่ในเครือข่าย
- โพรโตคอล DHCP (Dynamic Host Configuration Protocol) ทำหน้าที่แจกจ่ายข้อมูลพารามิเตอร์ของเครือข่ายให้กับเครื่องลูกข่ายที่เชื่อมต่ออยู่

2.8.2 หลักการทำงานของ Host-to-Host layer

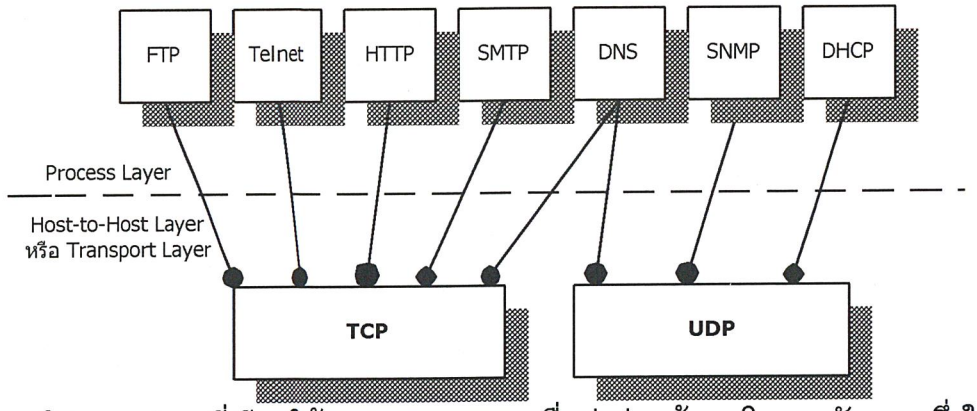
การทำงานที่ชั้นของ Host-to-Host layer นี้จะมีบทบาทในการจัดการต่อจาก Process layer บางครั้งมักเรียกชั้น Host-to-Host ว่า Transport layer ซึ่งไม่ใช่ชั้นของ Transport layer ในมาตรฐาน OSI model การทำงานของ Host-to-Host layer นี้จะมีการสร้าง connection หรือการเชื่อมต่อกันระหว่างแอพพลิเคชั่นกับ Host-to-Host layer โดยจุดที่เชื่อมกันเพื่อรับส่งข้อมูลนี้เรียกว่า port หรือ socket (คำว่า port ในที่นี้ไม่ได้หมายถึงฮาร์ดแวร์) และในแต่ละแอพพลิเคชั่นก็จะสร้างการเชื่อมต่อผ่าน port ได้พร้อมกันหลายแอพพลิเคชั่น ซึ่งการใช้งาน port ของแต่ละแอพพลิเคชั่นที่อยู่ในชั้น Process layer จะแตกต่างกันตามหมายเลขที่กำหนดไว้ และแต่ละโพรโตคอลจะมีการใช้งาน port หมายเลขต่างๆไม่ซ้ำกัน ดังรูปที่ 2-10



รูปที่ 2-10 แอพพลิเคชั่นหรือโปรเซสต่าง ๆ สื่อสารกับ Host-to-Host Layer ผ่านจุดเชื่อมต่อหรือ port ส่วนหมายเลขในรูปคือหมายเลข port ที่โปรเซสใช้งาน เช่น เว็บหรือโปรเซส http ใช้งาน port 80 ในการส่งผ่านข้อมูล เป็นต้น

เมื่อแอพพลิเคชั่นทำงานผ่านโพรโตคอลในชั้น Process layer จะมีการส่งผ่านข้อมูลไปยัง Host-to-Host layer ที่ชั้นนี้จะมีการเชื่อมต่อผ่าน port ที่กำหนด ทำให้การรับส่งข้อมูลในแต่ละโพรโตคอลทำได้ถูกต้อง ถึงแม้ว่าในเครื่องเซิร์ฟเวอร์ที่ให้บริการจะมีการทำงานอยู่หลายโปรเซสที่แตกต่างกันก็ตาม ในชั้น Host-to-Host หรือ Transport layer ของ TCP/IP นี้ จะมีโพรโตคอลทำงานอยู่ 2 โพรโตคอลที่แตกต่างกัน คือ โพรโตคอล TCP และ โพรโตคอล UDP (User Datagram Protocol) ในการส่งผ่านข้อมูลลงไปที่ชั้นถัดๆไป จะเห็นว่าโพรโตคอล TCP และ UDP จะถูกผนึกเข้าไปในโพรโตคอล IP อีกทีหนึ่งและส่งต่อไปยังเครือข่ายอินเตอร์เน็ตต่อไป

ตัวโพรโตคอล TCP และโพรโตคอล UDP จะมีแอพพลิเคชั่นเฉพาะเพื่อเรียกใช้งานแยกกันคือ แอพพลิเคชั่นที่ใช้โพรโตคอล FTP, Telnet, HTTP และ SMTP จะมีการส่งผ่านข้อมูลโดยเรียกใช้โพรโตคอล TCP ส่วนแอพพลิเคชั่นที่ใช้โพรโตคอล SNMP และ DHCP จะส่งผ่านข้อมูลโดยเรียกใช้โพรโตคอล UDP และสำหรับโพรโตคอล DNS นั้น จะสามารถเรียกใช้งานได้ทั้ง TCP และ UDP ดังรูป ซึ่งเหตุผลที่มีการเรียกใช้โพรโตคอล TCP และ UDP แตกต่างกัน ก็เนื่องจากวิธีการทำงานของทั้งสองโพรโตคอลต่างกันนั่นเอง



รูปที่ 2-11 โปรเซสต่าง ๆที่เรียกใช้ Transport layer เพื่อส่งผ่านข้อมูลโดยอาศัย port ซึ่งในแต่ละโปรเซสจะเรียกใช้งาน port เฉพาะแตกต่างกัน ยกเว้น DNS ที่สามารถใช้งานได้ทั้ง TCP และUDP

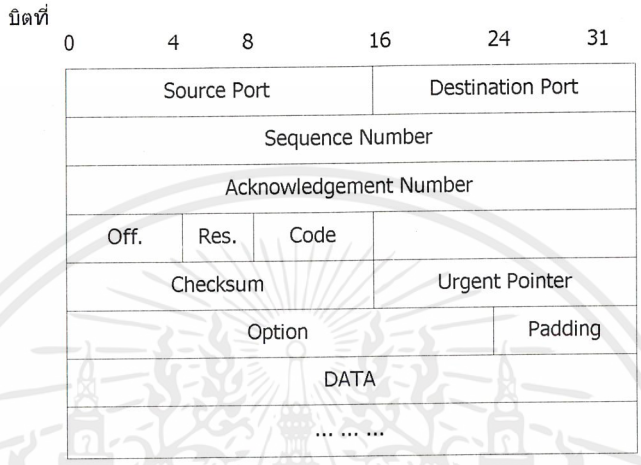
2.8.2.1 โพรโตคอล TCP

โพรโตคอล TCP (Transmission Control Protocol) เป็นโพรโตคอลที่มีการรับส่งข้อมูลแบบ stream oriented protocol หมายความว่า การรับส่งข้อมูลจะไม่คำนึงถึงปริมาณข้อมูลที่จะส่งไป แต่จะแบ่งข้อมูลเป็นส่วนย่อยๆก่อน แล้วจึงจะส่งไปยังปลายทางอย่างต่อเนื่องเป็นลำดับข้อมูล ในกรณีที่ข้อมูลส่วนใดส่วนหนึ่งสูญหายไป ก็จะส่งข้อมูลส่วนนั้นใหม่อีกครั้ง สำหรับปลายทางก็จะทำหน้าที่จัดเรียงส่วนของข้อมูล datagram ใหม่ให้ต่อเนื่องกันและประกอบกลับเป็นข้อมูลทั้งหมดได้ ซึ่งจะแยกข้อมูลที่ไม่ถูกต้องออกดังนั้นแอพพลิเคชั่นหรือโปรเซสใดที่อาศัยการส่งผ่านข้อมูลด้วย โพรโตคอล TCP จะต้องใช้หน่วยความจำและขนาดของช่องสัญญาณ (bandwidth) มากกว่า UDP

การติดต่อระหว่างกันจะต้องเป็นแบบ connection – oriented คือต้องมีการสร้างการติดต่อกันเป็น session ทั้ง 2 ด้าน เสียก่อน แล้วจึงจะรับส่งข้อมูลไปได้พร้อมกัน (full duplex) เหมือนกับการใช้โทรศัพท์ติดต่อกัน เมื่อผู้ติดต่อต้นทางเรียกให้ฝ่ายตรงข้ามรับสายแล้ว จึงเริ่มการสนทนา เช่น พูดคำว่า “สวัสดี” หรือ “ฮัลโหล” กันก่อนเพื่อให้แน่ใจว่าฝ่ายตรงข้ามพร้อมจะติดต่อด้วย จากนั้นจึงเริ่มต้นติดต่อกัน และเมื่อต้องการจะเลิกการติดต่อก็จะมีการพูดคำว่า “สวัสดี” ให้ฝ่ายตรงข้ามทราบว่าจะเลิกการติดต่อและวางสายไป ซึ่งในระหว่างการติดต่อกันนั้น แม้ว่าฝ่ายใดฝ่ายหนึ่งหรือทั้งสองฝ่ายจะเงียบไป คือไม่พูดอะไรเป็นเวลานาน ๆ แต่การเชื่อมโยงระหว่างทั้งสองด้านยังคงมีอยู่ไม่ขาดไปจนกว่าฝ่ายใดฝ่ายหนึ่งจะวางสาย เช่นเดียวกับการติดต่อกันด้วยกลไกโพรโตคอล TCP เมื่อแอพพลิเคชั่นต้องการส่งผ่านข้อมูลจะใช้โพรโตคอลที่เหมาะสมในชั้น Process layer ติดต่อไปและมีการสร้างช่องส่งข้อมูลผ่าน port ที่กำหนดเพื่อส่งผ่านข้อมูลไปยังโพรโตคอล TCP

ในระหว่างการรับส่งข้อมูลนี้โพรโตคอล TCP จะเพิ่มขบวนการสอบทานข้อมูลเพื่อให้ข้อมูลมีความถูกต้องไม่ผิดพลาดไปจากเดิม โดยการส่งสัญญาณสอบทานข้อมูล (acknowledgement) และส่งข้อมูลให้ใหม่อีกครั้ง ถ้าปลายทางไม่ได้รับหรือเกิดความผิดพลาดขึ้น

ความน่าเชื่อถือของการส่งผ่านข้อมูลโดยโพรโตคอล TCP จะมีมากกว่า แต่ก็ต้องอาศัยทรัพยากรของระบบมากกว่าในการทำงานเช่นกัน



รูปที่ 2-12 รูปแบบของ TCP packet จะเห็นว่ามีฟิลด์ Acknowledgement Number และข้อมูล Checksum เพื่อใช้ตรวจสอบการเดินทางของข้อมูล ส่วน header มีข้อมูลมากทำให้ต้องอาศัยทรัพยากรของระบบทำงานมาก

2.8.2.2 โพรโตคอล UDP

ใน Host-to-Host layer นอกจากจะมีโพรโตคอล TCP ทำงานแล้ว ก็ยังมีโพรโตคอล UDP (User Datagram Protocol) ที่มีคุณสมบัติแตกต่างกันอยู่ด้วย ในการรับส่งข้อมูลผ่านโพรโตคอล UDP จะเป็นแบบที่ทั้งสองด้านไม่จำเป็นต้องอาศัยช่องทางเชื่อมต่อกัน (connectionless) ระหว่างเครื่องเซิร์ฟเวอร์ให้บริการกับเครื่องที่ขอใช้บริการ โดยไม่ต้องแจ้งให้ฝ่ายรับข้อมูลเตรียมรับข้อมูลเหมือนโพรโตคอล TCP และไม่มีการตรวจสอบความถูกต้องครบถ้วนในการรับส่งข้อมูลนั้นๆด้วย เนื่องจากโพรโตคอล UDP ไม่มีสัญญาณสอบทานข้อมูล (acknowledgement) ในการส่งข้อมูลแต่ละครั้งและไม่มีการส่งข้อมูลใหม่อีกในกรณีที่เกิดความผิดพลาดของการส่งข้อมูล เมื่อเป็นเช่นนี้ แอพพลิเคชั่น หรือ โปรเซสใดที่ต้องอาศัยโพรโตคอล UDP ในการส่งผ่านข้อมูลก็อาจจะต้องสร้างขบวนการตรวจสอบข้อมูลขึ้นมาเอง

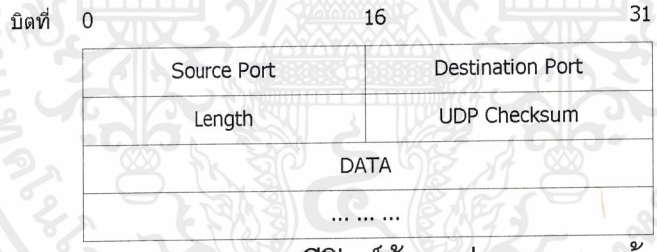
ตามรูปที่ 2.11 จะเห็นว่าโพรโตคอลชั้นบนขึ้นไป ที่ใช้การส่งผ่านข้อมูลโดยโพรโตคอล UDP เช่น โพรโตคอล SNMP (ใช้ควบคุมและจัดการอุปกรณ์ในเครือข่าย) หรือโพรโตคอล DHCP (ใช้ส่งข้อมูลพารามิเตอร์ของเครือข่ายให้กับเครื่องลูกข่ายได้ใช้งาน) การส่งข้อมูลเหล่านั้นไม่ต้อง

รับทราบหรือตรวจสอบว่าข้อมูลไปถึงปลายทางถูกต้องหรือไม่ แต่กลไกการตรวจสอบข้อมูลที่มีการรับส่งจะไปทำในขั้นตอนของโพรโตคอลชั้นที่สูงกว่าแทน

ตัวอย่างขั้นตอนกลไกการทำงานโดยใช้โพรโตคอล UDP มีดังต่อไปนี้

1. ในชั้นของ Process layer เมื่อโปรแกรมควบคุมอุปกรณ์เครือข่ายเช่น โปรแกรม Network management ต้องการส่งข้อมูลไปยังอุปกรณ์ที่ต้องการ แอพพลิเคชั่นนั้นจะติดต่อผ่านโพรโตคอล SNMP ในชั้น Process layer
2. โพรโตคอล SNMP จะติดต่อกับโพรโตคอล UDP ในชั้นถัดไป เพื่อขอติดต่อผ่าน port ที่กำหนด
3. โพรโตคอล SNMP เตรียมข้อมูลที่จะส่ง รวมทั้งที่อยู่ปลายทาง
4. โพรโตคอล SNMP ส่งผ่านข้อมูลให้โพรโตคอล UDP ที่อยู่ในชั้น Host-to-Host layer
5. โพรโตคอล UDP ทำหน้าที่ผนึกข้อมูลหรือ datagram นั้น ไปกับโพรโตคอล IP ในชั้นถัดลงไป เพื่อส่งข้อมูลออกจากเครื่อง

ซึ่งจะเห็นว่ามีกลไกที่ต่างจากการส่งข้อมูลด้วยโพรโตคอล TCP ซึ่งจะต้องมีการติดต่อกันก่อนและทั้งสองฝ่ายรับทราบการรับส่งข้อมูลของช่องการส่งข้อมูลนั้น



รูปที่ 2-13 รูปแบบของ UDP packet จะมีฟิลด์ข้อมูลส่วน header น้อยมากและไม่มีข้อมูลส่วนกลางตรวจสอบข้อมูล ทำให้ UDP packet มีขนาดเล็ก และใช้หน่วยความจำ หรือทรัพยากรของระบบ

2.8.3 หลักการทำงานของ Internetwork Layer

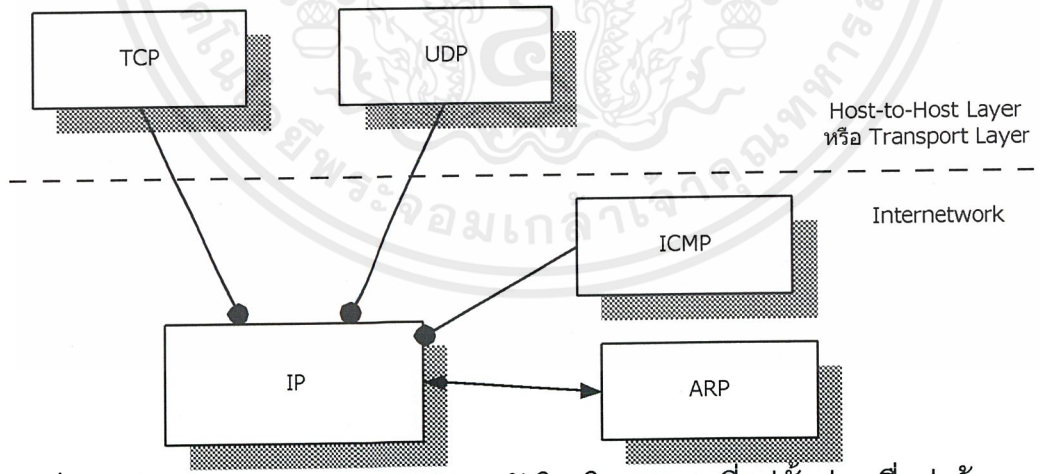
ในระดับล่างต่อมาในชั้น Internetwork Layer มีหน้าที่ส่งผ่านข้อมูลในระหว่างเครือข่าย โดยมีโพรโตคอลที่ทำงานเป็นกลไกสำคัญในการส่งผ่านข้อมูลไปยังเครือข่ายใดๆบนอินเตอร์เน็ต คือ โพรโตคอล IP (Internet Protocol) นอกจากนี้ในชั้น Internetwork Layer ยังมีโพรโตคอลทำงานอยู่ด้วยอีก 2 ชนิด คือ โพรโตคอล Internet Control Message Protocol (ICMP) และโพรโตคอล Address Resolution Protocol (ARP)

2.8.3.1 โพรโตคอล IP

โพรโตคอล IP ทำหน้าที่ให้บริการส่งผ่านข้อมูลที่มาจาก Host-to-Host layer เพื่อส่งข้ามไปยังเครือข่ายใดๆได้อย่างถูกต้อง แม้ว่าจะมีเครือข่ายเชื่อมต่อกันอยู่ในอินเตอร์เน็ตเป็นล้านๆเครือข่ายก็ตาม เนื่องจากโพรโตคอล IP มีข้อมูลตำแหน่ง IP ปลายทางที่จะส่งข้อมูลที่จะส่งข้อมูลไปให้ โดยทำงานร่วมกับอุปกรณ์ Router เพื่อส่งข้อมูลข้ามเครือข่ายออกไปได้ ตัวโพรโตคอล IP จะทำงานแบบ packet switching คือมีการส่งข้อมูลผ่าน switch ไปยังปลายทาง โดยข้อมูลจะเดินทางไปยังเครือข่ายต่างๆผ่าน switch นี้ไปเรื่อยๆจนกว่าจะถึงปลาย ตัววงจรผ่านหรือ switch นี้อาจ เป็น Gateway หรือ Router ในระบบเครือข่ายก็ได้ ซึ่งในข้อมูลของโพรโตคอล IP จะมีข้อมูลของหมายเลข IP ปลายทางที่จะส่งข้อมูลไปและเมื่อถึงเครือข่ายปลายทางแล้ว จะมีกลไกแปลงหมายเลข IP ให้เป็นหมายเลขฮาร์ดแวร์ประจำเครื่องที่ถูกต้องอีกทีหนึ่งด้วยโพรโตคอล ARP ตามรูปที่2.14 ที่จะแสดงที่จะแสดงการติดต่อกันระหว่างโพรโตคอลในชั้นของ Host-to-Host layer และ Internetwork layer

2.8.3.2 โพรโตคอล ICMP

หน้าที่หลักของโพรโตคอล ICMP (Internet Control Message Protocol) คือ การแจ้งหรือแสดงข้อความจากระบบ เพื่อบอกให้ผู้ใช้ทราบว่าเกิดอะไรขึ้นในการส่งผ่านข้อมูลนั้น ซึ่งปัญหาส่วนมากที่พบคือส่งไปไม่ได้ หรือปลายทางรับข้อมูลไม่ได้ เป็นต้น นอกจากนี้โพรโตคอล ICMP ยังถูกเรียกใช้งานจากเครื่องเซิร์ฟเวอร์และ Router อีกด้วย เพื่อแลกเปลี่ยนข้อมูลที่ใช้ควบคุม ส่วนรูปแบบการทำงานของโพรโตคอล ICMP นั้นจะทำควบคู่กับโพรโตคอล IP ในระดับเดียวกัน และข้อความต่างๆที่แจ้งให้ทราบจะถูกผนึกอยู่ภายในข้อมูลของ IP(IP datagram) อีกทีหนึ่ง



รูปที่ 2-14 โพรโตคอล TCPและ UDP อาศัยโพรโตคอล IP ที่อยู่ชั้นล่างเพื่อส่งข้อมูลระหว่างเครือข่ายและในชั้น Internetwork Protocol ยังมีโพรโตคอล ICMP ทำหน้าที่ส่งข้อความแจ้งเตือนโพรโตคอล ARP ทำหน้าที่แปลงเลขหมาย IP ไปเป็นเลขหมายของฮาร์ดแวร์จริง

ข้อความที่โพรโตคอล ICMP ส่งนั้นแบ่งออกได้ 2 แบบ คือ ICMP error message หรือข้อความแจ้งข้อผิดพลาดและ ICMP query หรือข้อความเรียกขอข้อมูลเพิ่ม ตัวอย่างกลไกการทำงานของโพรโตคอล ICMP เช่น เมื่อมีการส่งผ่านข้อมูลจากผู้ใช้ไปยังปลายทางที่ไม่ถูกต้อง หรือขณะนั้นเครื่องปลายทางเกิดปัญหาจนไม่สามารถรับข้อมูลได้ที่ Router จะส่งข้อความแจ้งเป็น ICMP Message ที่ชื่อ destination unreachable ให้กับผู้ส่งข้อมูล นอกจากนี้ตัวข้อมูลที่แจ้งเป็น ICMP message ที่ชื่อ destination unreachable ให้กับผู้ส่งข้อมูล นอกจากนี้ตัวข้อมูลที่แจ้งข้อความก็จะมีส่วนของข้อมูล IP datagram ที่เกิดปัญหาด้วย ดังนั้นเมื่อผู้ส่งข้อมูลได้รับข้อความแจ้งแล้วก็จะทราบได้ว่าจุดที่เกิดปัญหานั้นอยู่ที่ใด

ดังนั้นโพรโตคอล ICMP จึงกลายมาเป็นเครื่องมืออย่างหนึ่งในการช่วยทดสอบเครือข่าย เช่น คำสั่ง ping ที่มักใช้ทดสอบว่าเครื่องเซิร์ฟเวอร์ที่ให้บริการหรืออุปกรณ์ที่ต่ออยู่ในเครือข่ายอินเตอร์เน็ตนั้นยังทำงานเป็นปกติหรือไม่ แล้วคำสั่ง ping มีการเรียกใช้งานโพรโตคอล ICMP แจ้งเป็นข้อความให้ทราบอีกต่อหนึ่ง

2.8.3.3 โพรโตคอล ARP

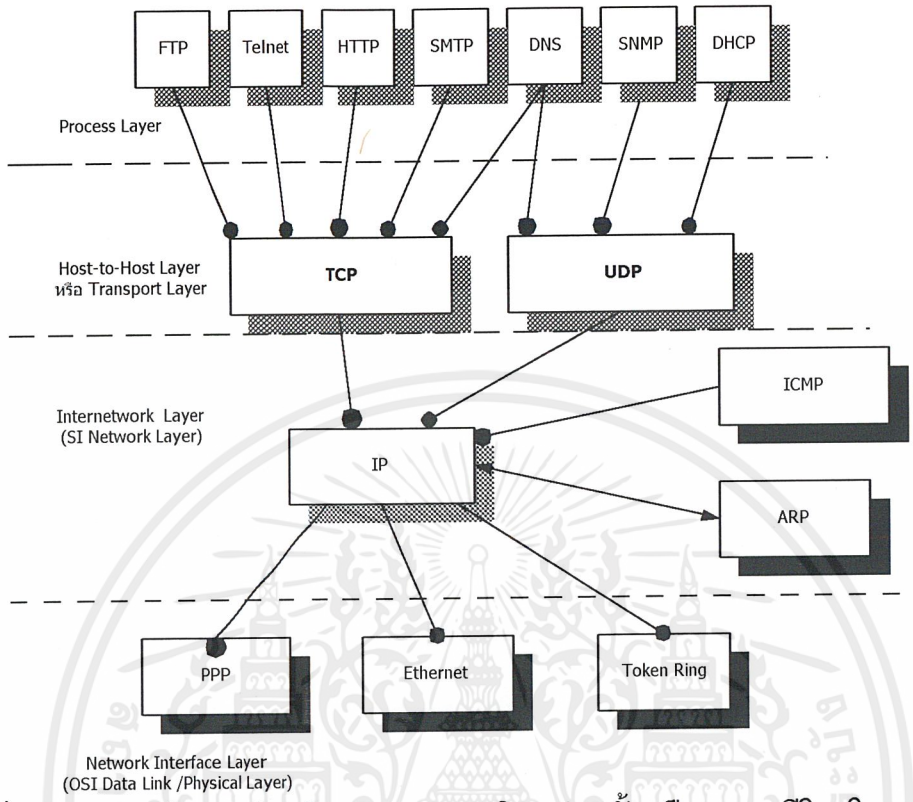
โพรโตคอล ARP (Address Resolution Protocol) ถูกเรียกใช้งานโดยโพรโตคอล IP เพื่อช่วยแปลงหมายเลข IP ไปเป็นหมายเลขฮาร์ดแวร์ปลายทาง ตัวอย่างเช่น เว็บเซิร์ฟเวอร์เครื่องหนึ่งเชื่อมต่ออยู่ในเครือข่ายอินเตอร์เน็ตและในการเชื่อมต่อนี้ต้องอาศัย Network Interface Card (NIC) หรือ LAN card ติดตั้งอยู่ที่ LAN card นี้เองจะมีหมายเลขเฉพาะประจำฮาร์ดแวร์ที่ไม่ซ้ำกับใคร เพื่อใช้อ้างอิงการส่งข้อมูลในเครือข่าย แต่เมื่อมาใช้งานในโพรโตคอล TCP/IP ก็จะต้องมีการกำหนดหมายเลข IP address ประจำตัวเพื่อใช้อ้างอิงกัน และโพรโตคอล ARPจะทำหน้าที่แปลงค่าหมายเลข IP ให้เป็นหมายเลขฮาร์ดแวร์จริงให้ในระดับการทำงานที่ Internetwork layer นี้ ซึ่งกลไกการแปลงนี้เรียกว่า address resolution

2.8.4 หลักการทำงานของ Network Interface Layer

เนื่องจากในด้านกายภาพของเครือข่ายนั้น มีหลายวิธีการและหลายรูปแบบในการเชื่อมต่อระบบให้เป็นเครือข่าย แต่อย่างไรก็ตามในเครือข่ายอินเตอร์เน็ตนี้ ข้อมูลหรือ IP datagram จะถูกถ่ายทอดและส่งผ่านไปยังปลายทางโดยไม่คำนึงถึงรูปแบบการเชื่อมต่อทางกายภาพ ไม่ว่าจะเป็นการใช้เครือข่ายใยแก้วนำแสงหรือเครือข่าย สาย Unshielded Twist Pair (UTP) เชื่อมต่อเป็นแบบเครือข่าย Ethernet ธรรมดาหรือเครือข่าย Token Ring, ATM, ISDN ฯลฯ ก็ตาม

การทำงานระดับล่างสุดต่อจาก Internetwork layer จะเป็นการแปลงข้อมูล IP datagram ให้อยู่ในรูปที่เหมาะสม และแปลงเป็นสัญญาณไฟฟ้าส่งไปยังเครือข่ายต่อไป ซึ่งในชั้น Network Interface Layer นี้เมื่อเทียบกับมาตรฐาน OSI model แล้วจะเป็นการรวม 2 layer เข้าด้วยกันคือ

Data link layer และ Physical layer กล่าวโดยสรุปคือการทำงานในชั้นต่างๆ ตามโครงสร้างของโพรโตคอล TCP/IP จะมีลักษณะดังรูปที่2.15



รูปที่ 2-15 โครงสร้างของโพรโตคอล TCP/IP ในแต่ละชั้นหรือ layer มีโพรโตคอลหลักทำหน้าที่ต่าง ๆและส่งผ่านข้อมูลไปยังเครือข่ายและออกสู่อินเตอร์เน็ต

ตารางที่ 2-1 สรุปหมายเลขบางส่วนของ port ที่ใช้งานโดย TCP และ UDP

โปรโตคอล ที่ใช้งาน	Port หรือ socket เชื่อมต่อ (เลขฐาน 10)	โปรโตคอลใน ระดับ Host-to Host	รายละเอียด
BootP	67	UDP	BOOTstrap Protocol ด้านเซิร์ฟเวอร์
BootP	68	UDP	BOOTstrap Protocol ด้านไคลเอนต์
DHCP	67	UDP	Dynamic Host Configuration Protocol ด้านเซิร์ฟเวอร์
DHCP	68	UDP	Dynamic Host Configuration Protocol ด้านไคลเอนต์
DNS	53	UDP/TCP	Domain Name System
FTP	21	TCP	File Transfer Protocol ด้านเซิร์ฟเวอร์ ที่ควบคุม
FTP	20	TCP	File Transfer Protocol ด้านเซิร์ฟเวอร์ ที่ส่งข้อมูล
HTTP	80	TCP/UDP	Hyper text Transfer Protocol ด้านเซิร์ฟเวอร์
NeTBT	138	UDP	NetBIO datagram service
NetBT	139	TCP	NetBIO session service
SMTP	25	TCP	Simple Mail Transfer Protocol ด้านเซิร์ฟเวอร์
SNMP	161	UDP	Simple network Management Protocol ด้าน agent
SNMP	162	UDP	SNMP trap manager
Telnet	23	TCP	Teletype Network Protocol
TFTP	69	UDP	Trivial File Transfer Protocol
WINS	137	UDP	Windows Internet Name Service

กล่าวโดยสรุปก็คือ โพรโตคอล TCP/IP ทำงานโดยแบ่งเป็นชั้นเทียบกับ OSI model ได้ กลไกในการทำงานของโพรโตคอล TCP/IP มี 4 ชั้น ซึ่งในชั้นแรก คือ Process layer ทำหน้าที่ติดต่อกับแอพพลิเคชั่นและโพรโตคอลที่แอพพลิเคชั่นนั้นๆใช้งาน และส่งต่อมาให้ชั้น Host-to-Host layer เพื่อติดต่อกันระหว่างเครื่องเซิร์ฟเวอร์ให้บริการกับผู้ขอใช้บริการ ในชั้นนี้จะมีการสร้าง session หรือการเชื่อมต่อระหว่างระบบขึ้นตามแต่ละโพรโตคอลที่ต้องการ ต่อมาเป็นการผนึกข้อมูลไปเป็น IP datagram ที่ชั้น Internetwork layer โดยอาศัยโพรโตคอล IP เพื่อให้สามารถติดต่อส่งข้อมูลข้ามเครือข่ายไปยังเครือข่ายและเครื่องที่ถูกต้องได้ และสุดท้ายการส่งข้อมูลออกสู่โลกภายนอก

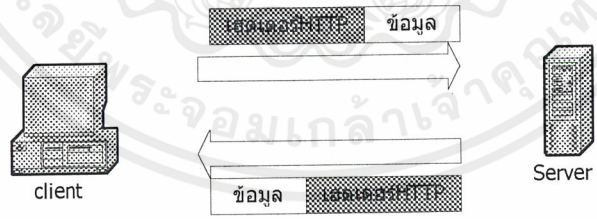
ต้องอาศัยกลไกในชั้น Network Interface Layer เพื่อแปลงข้อมูลใหม่ เพิ่มข้อมูลที่จำเป็นในการอ้างอิงตำแหน่งและแปลงข้อมูลเป็นสัญญาณไฟฟ้าส่งออกไปยังเครือข่าย และอาจจะออกไปยัง Gateway หรือ Router เพื่อข้ามเครือข่ายออกไปยังเส้นทางที่กำหนดไว้ในอินเตอร์เน็ตต่อไป

ในแต่ละชั้นของโครงสร้าง TCP/IP Stack มีการใช้งานโพรโตคอลต่างๆอยู่หนึ่งโพรโตคอลหรือมากกว่า ในแต่ละโพรโตคอลเหล่านี้ก็จะรับผิดชอบทำหน้าที่ของตน เพื่อส่งผ่านข้อมูลลงไปยังระดับล่าง และออกสู่เครือข่ายอินเตอร์เน็ตในที่สุด

2.9 โครงสร้างโพรโตคอล HTTP

โพรโตคอล HTTP อยู่บนพื้นฐานของไคลเอนต์ / เซิร์ฟเวอร์ ที่ต้องมีการร้องขอ (request) และการตอบสนอง (response) โพรโตคอลนี้อาศัยการเชื่อมต่อผ่านทางโพรโตคอล TCP/IP อีกทีหนึ่ง โดยใช้พอร์ตหมายเลข 80 เป็นช่องทางมาตรฐานในการติดต่อ ในทางปฏิบัติจะใช้พอร์ตหมายเลขอื่นก็ได้ แต่จะทำให้เกิดความลำบากต่อผู้ใช้ที่ต้องระบุหมายเลขพอร์ตลงใน URL ด้วย เช่น ถ้ากำหนดให้เว็บเซิร์ฟเวอร์ ใช้พอร์ตหมายเลข 82 เวลาผู้ใช้จะเปิดเว็บเพจหรือร้องขอใดๆ จะต้องระบุหมายเลขพอร์ตต่อท้าย UPL เช่น http:// ventura.lanna.com:82

ในการร้องขอจาก ไคลเอนต์ และการตอบสนองจาก เซิร์ฟเวอร์ ย่อมต้องมีการรับส่งข้อมูลระหว่างกัน แต่ข้อมูลที่รับส่งให้กันในแต่ละครั้งไม่ได้มีเฉพาะข้อมูลเพียงอย่างเดียว แต่ละฝ่ายจะต้องเพิ่มส่วนที่เรียกว่า HTTP Header เข้าไปในส่วนหัวของข้อมูลด้วย header HTTP จะใช้เป็นตัวบอกว่าข้อมูลที่ส่งหลังจากนี้เป็นอะไร เป็นข้อมูลการร้องขอจาก ไคลเอนต์ หรือเป็นข้อมูลตอบสนองจาก เซิร์ฟเวอร์ ดังรูปที่ 2-16

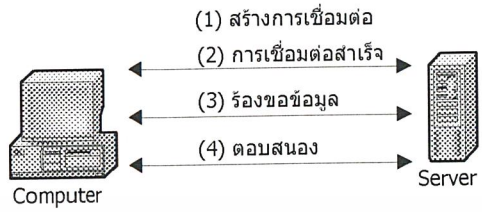


รูปที่ 2-16 แสดงลักษณะข้อมูลที่รับส่งระหว่าง client กับ server

เนื่องจากข้อมูลใน header HTTP เป็นตัวควบคุมหรือบอกว่าให้ฝ่ายรับควรทำอย่างไรกับข้อมูลที่ส่งมาให้ ในบางครั้งจึงมีคนเรียกข้อมูลส่วนนี้ว่า Meta Information

2.10 วิธีการติดต่อของโพรโตคอล HTTP

ด้วยเหตุที่การทำงานของโพรโตคอล HTTP เป็นแบบ ไคลเอนต์ และ เซิร์ฟเวอร์ ดังนั้นการติดต่อสื่อสารใด ๆ ผ่าน โพรโตคอล นี้จำเป็นต้องมีเครื่องคอมพิวเตอร์ตัวลูกกับตัวแม่ การสื่อสารจึงจะสมบูรณ์ได้ การติดต่อจะมีขั้นตอนดังรูปที่ 2-17



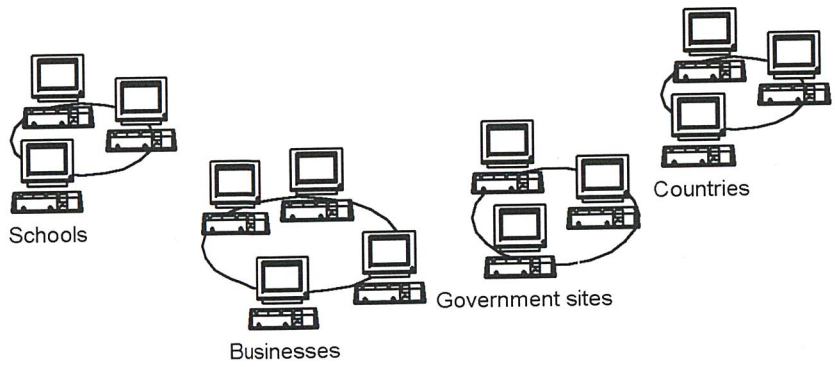
รูปที่ 2-17 การติดต่อระหว่างไคลเอนต์กับเซิร์ฟเวอร์

จากรูปที่ 2-17 ขั้นแรกคือ ไคลเอนต์ (ในตอนนี้คือ web browser) จะสร้าง การติดต่อ (connection) กับ เซิร์ฟเวอร์ ผ่านสิ่งที่เรียกว่า “Socket” (Socket) เมื่อ Socket ทั้งสองฝั่งเสียบเชื่อมต่อกันได้สำเร็จ ไคลเอนต์ จะส่งคำร้องขอข้อมูล (request) ไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์จะไปหาข้อมูลที่ ไคลเอนต์ ต้องการ ซึ่งไม่ว่าจะมีหรือไม่มีข้อมูลตามที่ไคลเอนต์ร้องขอเซิร์ฟเวอร์ก็จะต้องส่งข้อมูลตอบสนอง (response) กลับมายัง ไคลเอนต์ เสมอ สุดท้ายการเชื่อมต่อจะถูกตัดขาดหรือปลดการเชื่อมต่อของ Socket ทั้งสองฝั่งออกนั่นเอง

2.11 หลักการทำงานของ DNS (Domain Name System)

ชื่อโดเมนในอินเตอร์เน็ตนั้นจะเป็นไปตามรูปแบบของ DNS (Domain Name System หรือบางครั้งก็ใช้คำว่า Service) ซึ่งเป็นระบบที่ได้รับการออกแบบมาเพื่อให้แบ่งลำดับชั้นของสิ่งต่างๆ และรองรับการเพิ่มจำนวนประชากรเครื่องที่ต่อกับอินเตอร์เน็ตในโลกให้เป็นไปอย่างมีระเบียบเรียบร้อย ในแง่หนึ่งนั้น DNS จะทำการแบ่งไซต์ต่างๆในอินเตอร์เน็ตออกเป็นกลุ่ม โดยแยกตามประเภท ส่วนในอีกแง่หนึ่ง DNS เป็นส่วนที่กระจายฐานข้อมูลไปยังหลายๆ เครื่องเพื่อให้บริการหาที่ตั้งของอินเตอร์เน็ตไซต์ตามที่ต่างๆ

DNS จะแยกหมวดหมู่ของไซต์ต่างๆ ออกตามประเภทหรือตามชื่อของประเทศที่ขอจดทะเบียนไซต์เหล่านี้



รูปที่ 2-18 แสดงการแยกหมวดหมู่ของ DNS

ลักษณะโครงสร้างแบบนี้จะมีการแบ่งเป็นลำดับชั้น เพื่อรองรับชื่อที่มีเพิ่มมากขึ้นเรื่อยๆ โดยจะมีหน่วยงานหรือองค์กรที่คอยกำกับดูแลชื่อต่างๆ ในแต่ละชั้นนั้น ในลำดับชั้นที่สูงที่สุดคือ top-level domain นั้นจะอยู่ภายใต้การกำกับดูแลขององค์กรที่ชื่อว่า Internet Assigned Numbers Authority หรือ IANA (www.iana.org) ซึ่งปัจจุบัน IANA คอยดูแลการจดทะเบียน TLD ที่เป็นประเภทของหน่วยงานหรือองค์กร ซึ่งมีอยู่ 7 ประเภทด้วยกัน และ TLD ที่เป็นชื่อย่อตัวอักษรของประเทศต่างๆ นั้นพอจะยกตัวอย่างได้ดังต่อไปนี้

ตารางที่ 2-2 แสดงชื่อโดเมนแยกตามประเภทองค์กร

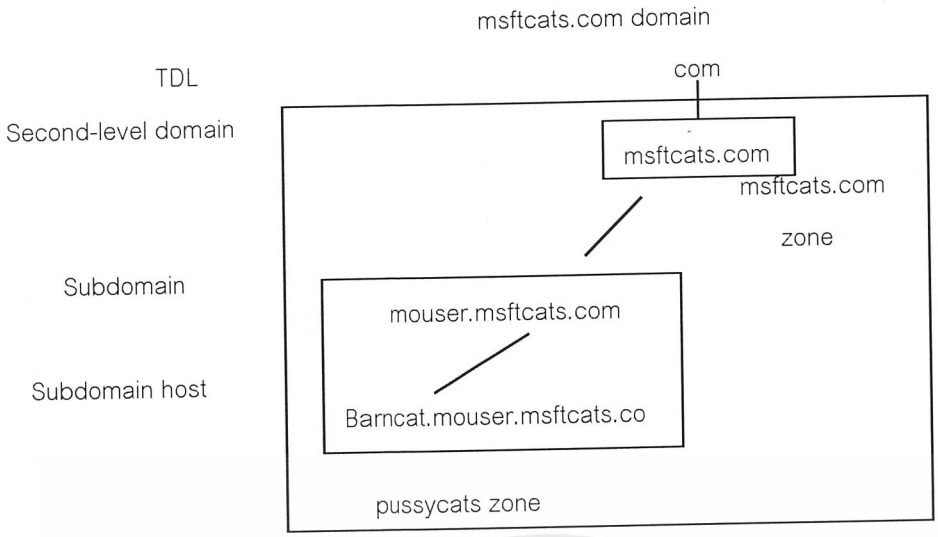
ชื่อโดเมนแยกตามประเภทองค์กร	
.com	องค์กรเพื่อการค้า ธุรกิจ บริษัทต่างๆ
.edu	สถาบันการศึกษา
.gov	หน่วยงานของรัฐบาลสหรัฐฯ
.int	องค์กรระหว่างประเทศ
.mil	หน่วยงานทางทหาร
.net	หน่วยงานที่ให้บริการด้านเน็ตเวิร์ก
.org	องค์กรที่ไม่หวังผลกำไร

ตารางที่ 2-3 แสดงชื่อโดเมนแยกตามประเทศ

ชื่อโดเมนแยกตามประเทศ					
Ar	Argentina	fr	France	nz	New Zealand
at	Austria	gr	Greece	pl	Poland
au	Australia	il	Israel	pt	Portugal
be	Belgium	in	India	se	Sweden
br	Brazil	is	Iceland	sg	Singapore
ca	Canada	it	Italy	th	Thailand
cn	China	jp	Japan	tw	Taiwan
de	Germany	kr	South Korea	uk	United Kingdom
dk	Denmark	mx	Mexico	ve	Venezuela
eg	Egypt	my	Malaysia	za	South Africa
es	Spain	nl	Netherlands		
fi	Finland	no	Norway		

การใช้ TLD เพียงอย่างเดียวอาจทำให้ปริมาณชื่อที่ตั้งให้กับไซต์ต่างๆ ไม่เพียงพอ ด้วยเหตุนี้จึงต้องแบ่งชื่อย่อยลงไปเป็นส่วนประกอบที่สองของชื่อ ที่เรียกว่าโดเมนระดับที่สอง (second-level domain name หรือ SLD) ซึ่งชื่อที่ตั้งในระดับนี้จะต้องมีการจดทะเบียนเพื่อไม่ให้มีโอกาสที่ซ้ำกับชื่ออื่น เมื่อนำชื่อในระดับ SLD และ TLD มาต่อกัน ก็จะได้เป็นชื่อที่พบกันบ่อยๆ

สำหรับ second-level domain นี้อาจถูกแบ่งออกเป็น subdomain หรือ โดเมนย่อยหลาย ๆ อัน ซึ่งในแต่ละโดเมนย่อยนี้ก็อาจประกอบไปด้วยโฮสต์ต่างๆหลายๆตัวด้วยกัน นอกจากนี้โดเมนและโดเมนย่อยยังอาจถูกจัดกลุ่มใหม่เรียกว่า zone หรือ โซน เพื่อแยกให้เห็นหน่วยงานต่างๆ ที่กำกับดูแลหรือรับผิดชอบ ในขณะที่โดเมนย่อยจะถูกกำหนดด้วยโฮสต์ แต่สำหรับโซนจะถูกกำหนดโดยไฟล์ๆ หนึ่งที่อยู่บนดิสก์ ซึ่งเก็บชื่อโดเมนและโดเมนย่อยที่อยู่ในโซนนั้น จะเห็นภาพได้ดีขึ้นโดยดูบริษัทตัวอย่าง ชื่อ Microsoft Cats (โปรดสังเกตว่าการตีความจากชื่อนั้นจะทำโดยเริ่มอ่านจากขวาไปซ้าย คือ ส่วนของโดเมนใหญ่ที่สุดจะอยู่ทางขวามือ แล้วไล่ไปหาที่เล็กลงตามลำดับ)



รูปที่ 2-19 แสดง second-level ของบริษัท Microsoft Cats

2.12 หลักการทำงานของ Data Packet

เมื่อมีการรับหรือส่งข้อมูลกันในระบบเครือข่ายอินเตอร์เน็ตนั้น ตัวข้อมูล (เช่นข้อความในอีเมล์หรือไฟล์ HTML ที่เป็นในโปรแกรมบราวเซอร์) จะถูกทำให้มีขนาดเล็กลงโดยแบ่งออกเป็นส่วนย่อย ๆ เรียกว่า Data Packet หรือ Datagram ซึ่งการจัดแบ่งให้เป็นส่วนย่อยลงนี้มีประโยชน์คือ ทำให้เครือข่ายนั้นสามารถรองรับการติดต่อและรับส่งข้อมูลกันได้อย่างราบรื่นไม่ติดขัด หรือพบปัญหาเครือข่ายทำงานช้าเมื่อมีการรับส่งข้อมูลขนาดใหญ่ เนื่องจากสายสัญญาณเชื่อมโยงเป็นสื่อที่ต้องแบ่งกันใช้งาน นอกจากนี้การแบ่งข้อมูลออกเป็นส่วนย่อยๆ ยังทำให้สามารถเพิ่มกระบวนการตรวจทานความถูกต้องของข้อมูลที่ปลายทาง และแก้ไขเมื่อข้อมูลผิดพลาดหรือตกหล่นได้โดยง่ายอีกด้วย

สายสัญญาณเชื่อมโยงอุปกรณ์ในเครือข่ายนั้น เป็นสิ่งที่ต้องใช้งานร่วมกัน เมื่อมีอุปกรณ์ใดต้องการส่งข้อมูล อุปกรณ์อื่นก็ต้องรอให้การส่งข้อมูลนั้นเสร็จสิ้นเสียก่อนจึงจะสามารถส่งข้อมูลของตนเองได้ โดยเฉพาะอย่างยิ่งในกรณีที่มีการส่งข้อมูลขนาดใหญ่ ถ้าไม่มีการแบ่งข้อมูลให้เป็นส่วนเล็กลงเพื่อทยอยส่งไปยังปลายทางโดยเป็นการแบ่งเวลาให้กับอุปกรณ์อื่นๆได้ใช้สายสัญญาณด้วยแล้ว เครือข่ายนั้นก็อาจจะเกิดปัญหาติดขัดได้ ทั้งนี้เมื่อ datagram ถูกส่งไปยังปลายทางแล้ว ก็จะมีกระบวนการรวมข้อมูลย่อยเหล่านี้ให้กลับคืนสู่สภาพเดิมได้ต่อไป

ประโยชน์อีกประการหนึ่งในการแยกข้อมูลให้เป็นส่วนย่อยๆ คือ การแก้ไขและตรวจสอบข้อมูลที่เสียหายในการส่งข้อมูล จะสามารถทำได้อย่างมีประสิทธิภาพ ซึ่งการส่งข้อมูลผ่านสายสัญญาณต่างๆ มักจะพบปัญหาสัญญาณรบกวนหรือสัญญาณขาดหายระหว่างการส่งอยู่บ่อยๆ ทำให้ข้อมูลที่ส่งไปยังผู้รับไม่ถูกต้องครบถ้วน ซึ่งปัญหานี้สามารถแก้ไขได้ เนื่องจากข้อมูลที่

ถูกแบ่งเป็น datagram จะมีขนาดเล็กลง ทำให้สามารถเพิ่มการตรวจสอบการรับส่งข้อมูลนั้นได้ดีขึ้น เช่น เทคนิคการคำนวณ (check sum)จะคำนวณค่าของข้อมูลที่ส่งไปและได้รับ ถ้าตรงกันก็แสดงว่าการรับส่ง datagram นั้นถูกต้อง แต่ถ้าผลการคำนวณไม่ตรงกัน ด้านผู้รับข้อมูลก็จะส่งสัญญาณมาให้เพื่อส่งเฉพาะ datagram นั้นใหม่อีกครั้ง โดยไม่ต้องส่งข้อมูลทั้งหมดมาอีก ทำให้สามารถแก้ไขข้อมูลที่ผิดพลาดทำได้อย่างรวดเร็ว

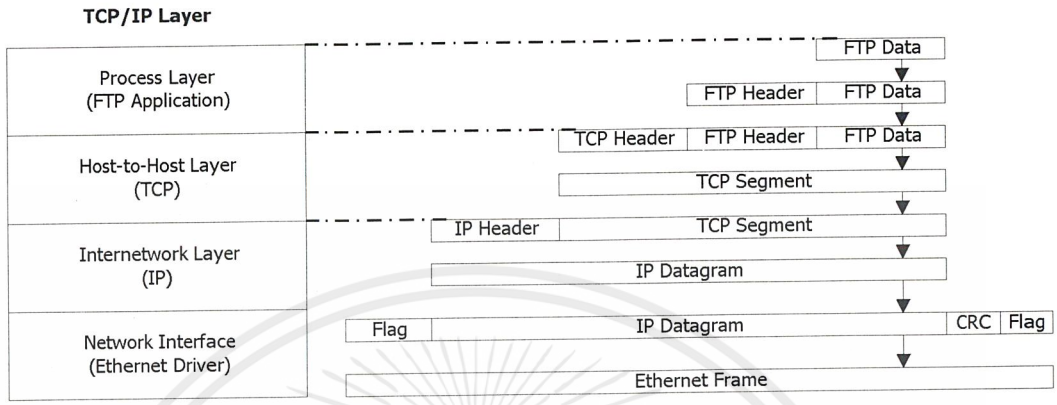
ตัวข้อมูลที่ถูกแยกออกเป็น data packet หรือ datagram นี้จะมีลักษณะเป็นข้อมูลแบบต่อเนื่อง (stream byte) คือมีการกำหนดลำดับก่อนหลังของข้อมูล เพื่อให้ประกอบข้อมูลย่อยคืนสู่สภาพเดิมได้อย่างถูกต้อง และมีรูปแบบหรือฟอร์แมต (format) ที่แน่นอนคือ datagram จะประกอบด้วยส่วนของ header และส่วนของตัวข้อมูล (body) โดยในส่วนของ header จะมีข้อมูลต่างๆระบุที่อยู่ปลายทางที่ต้องส่งข้อมูลไปเลขหมายต้นทางที่ส่งข้อมูลมา ค่าบอกขนาดความยาวของ datagram นี้ และข้อมูลอื่นๆ สำหรับในส่วนของ body อาจจะเป็นเนื้อหาข้อมูลใดๆ เช่น ข้อความในอีเมล์,ไฟล์ข้อมูลบางส่วน หรืออาจจะเป็น datagram ของข้อมูลในรูปแบบอื่นๆที่ถูกผนึก (encapsulation) มาด้วย เป็นต้น ซึ่ง datagram ที่ใช้ในเครือข่ายอินเตอร์เน็ตนี้จะเรียกว่า IP datagram

2.13 การ Encapsulation

ก่อนที่ข้อมูลใดจะถูกส่งผ่านไปในเครือข่ายอินเตอร์เน็ตได้ ก็จะต้องถูกแยกเป็นส่วนย่อยๆ เรียกว่า datagram และถูกผนึกหรือทำ encapsulation เข้าไปกับโพรโตคอล IP หรือ เรียกว่าเป็น IP datagram ก่อนจึงจะส่งผ่านไปในเครือข่ายอินเตอร์เน็ตได้ เนื่องจากโพรโตคอล IP มีข้อมูลในการระบุเส้นทางการส่งผ่านข้อมูลไปยังปลายทางได้นั่นเอง การผนึกข้อมูลหนึ่งไปเป็นข้อมูลในอีกรูปแบบหนึ่งนี้ เป็นกลไกที่สำคัญของการใช้งานโพรโตคอล TCP/IP มาก โดยขบวนการที่ใช้จะมีขั้นตอนคร่าวๆ ดังรูปที่ 2.20

ตามรูป เริ่มต้นมีการใช้งานโปรแกรมรับส่งข้อมูล เช่น เมื่อเรียกใช้โปรแกรม FTP โปรแกรมแอพพลิเคชั่นจะเตรียมข้อมูลเพื่อส่งผ่านไปในเครือข่ายอินเตอร์เน็ตหลังจากโปรเซส FTP เตรียมข้อมูลและแยกส่วนเป็น FTP header เพิ่มเข้าไปในส่วนของข้อมูล เมื่อมาถึงชั้น Transport หรือ host-to-host layer ซึ่งโพรโตคอล TCP เป็นผู้รับผิดชอบจะมีการสร้าง TCP segment รวมกัน จากนั้น TCP segment นี้จะถูกส่งต่อไปยัง layer ระดับล่างลงไปคือ Internetwork layer ในชั้นนี้โพรโตคอล IP จะทำงานโดยการเพิ่มส่วน IP head รวมกันกับ TCP segment เข้าไป เรียกว่าเป็น IP datagram ก็เป็นอันเสร็จสิ้นขั้นตอนการผนึกหรือ encapsulation ข้อมูลจากระดับบนสุดลงมาเพื่อให้ส่งผ่าน IP datagram ออกไปยังสายสัญญาณ ในชั้น Network Interface จะมีการแปลงข้อมูลและเพิ่มส่วน error correction และ flag เพื่อให้การส่งข้อมูลนั้นไม่ผิดพลาด จากนั้นก็แปลง

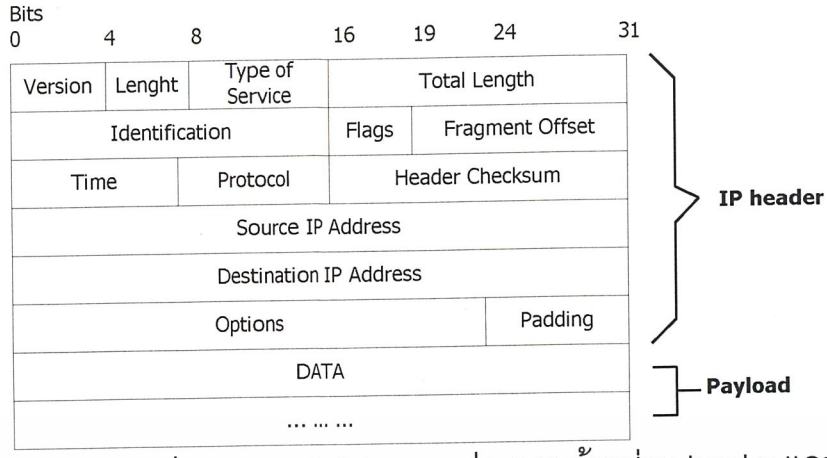
ข้อมูลเป็นสัญญาณไฟฟ้าส่งผ่านสายสัญญาณที่เชื่อมโยงอยู่ต่อไป ซึ่งจากตัวอย่างนี้มีการส่งผ่านข้อมูลไปในเครือข่ายแบบ Ethernet ดังนั้นในชั้นสุดท้ายข้อมูลก็จะต้องถูกแปลงเป็น Ethernet Frame เสียก่อน



รูปที่ 2-20 ตัวอย่างการ Encapsulation ของข้อมูล FTP เทียบกับ TCP/IP layer

2.14 รูปแบบของ IP Datagram

จากขบวนการ encapsulation นั้น ข้อมูลในการติดต่อกันไม่ว่าจะเป็นเนื้อความในอีเมล์หรือไฟล์ที่ส่งไปมา จะถูกผนึกข้อมูลหรือ encapsulate ไปเป็นรูปของ IP datagram และสุดท้ายก็จะถูกแปลงเป็น Ethernet frame หรือเฟรมข้อมูลในรูปแบบอื่นๆตามลักษณะการเชื่อมต่อทางกายภาพ เช่น Ethernet หรือ Token-Ring เป็นต้น เพื่อให้สามารถส่งข้อมูลออกสู่เครือข่ายและข้ามเครือข่ายไปสู่อินเตอร์เน็ตได้ ตัวข้อมูลที่ถูกแปลงมาเป็น IP datagram นี้จะประกอบด้วย 2 ส่วน คือ ส่วน IP header ที่มีขนาด 32 ไบต์ และส่วนเนื้อข้อมูลที่เรียกว่า payload ขนาดของ IP datagram มีขนาดไม่แน่นอน และมีลักษณะดังรูปที่ 2-21



รูปที่ 2-21 แสดงรูปแบบของ IP datagram ประกอบด้วยส่วน header และ payload

ส่วนของ IP header มีการแบ่งย่อยเพื่อระบุพารามิเตอร์ในการใช้งานต่างๆ ดังนี้

- ส่วน Version มีขนาด 4 บิต ถูกกำหนดค่าเป็น 4 ในกรณีที่ใช้หมายเลข IP เป็น Ipv4 และในอนาคตเมื่อหมายเลข IP มีการใช้งานเป็น IPv6 หรือ IP เวอร์ชัน 6 ค่าของ Version ก็จะมีค่าเป็น 6
- ส่วน Length มีขนาด 4 บิต ซึ่งเป็นค่าความยาวของ IP header นี้
- ส่วน Type of Service เป็นฟิลด์ข้อมูลขนาด 8 บิต เพื่อบอกให้ทราบว่าจะดำเนินการกับข้อมูลนี้อย่างไร เช่น low delay, high throughput เป็นต้น แต่ในการใช้งานจริง อุปกรณ์ Router ที่ส่งผ่านข้อมูลจะไม่สนใจข้อมูลนี้

- ส่วน Total Length มีขนาด 16 บิต เก็บข้อมูลแสดงค่าความยาวสุทธิของ IP datagram นี้เป็นจำนวนไบต์ ดังนั้นขนาดของ IP datagramจะมีความยาวไม่เกิน 2^{16} หรือ 65,535 ไบต์ ซึ่งในส่วนของ IP header จะมีขนาดอย่างน้อย 20 ไบต์ ดังนั้นเนื้อข้อมูลหรือ payload ของ IP datagram ใดๆ จะมีขนาดไม่เกิน 65,515 ไบต์ และในการส่งผ่านข้อมูลกันในอินเตอร์เน็ตตัว IP datagram จะมีขนาดเล็กสุดที่ 576 ไบต์ (IP header 20 ไบต์, payload 512 ไบต์ และสำหรับข้อมูล option หรือ โพรโตคอล header อีก 44 ไบต์) ดังนั้นในการส่งผ่านข้อมูล IP datagram ขนาด 576 ไบต์จึงเป็นขนาดเล็กที่สุดซึ่งไม่สามารถแยกย่อยลงไปกว่านี้ได้อีก
- ส่วน Identification เป็นข้อมูลที่บอกให้ทราบว่า IP datagram นั้นมาจากที่ใด โดยเฉพาะกรณีที่ข้อมูลที่ถูกแยกออกเป็นส่วนย่อยๆแล้ว

- ส่วน Flags และ Fragment offset เป็นส่วนข้อมูลที่ใช้ระบุการแยกและรวมข้อมูล เพื่อให้ข้อมูลที่ถูกแยกออกเป็นข้อมูลย่อย (fragment) สามารถกลับมารวมกันใหม่ตามลำดับได้ถูกต้อง
- ส่วน Time หรือ Time to Live เป็นข้อมูลแสดงจำนวนเวลามากที่สุดของ IP datagram นี้ ซึ่งสามารถจะส่งผ่านเครือข่ายไปยังปลายทางได้ โดยมีหน่วยเป็นวินาที และตามปกติจะมีค่าเป็น32 โดยในระหว่างที่ข้อมูล IP datagram ถูกส่งผ่าน Router ตัว Router ก็จะลดค่า Time to Live ลง1ค่าเสมอ ทำให้สามารถนำค่า time นี้ไปใช้นับจำนวนเครือข่ายที่ IP datagram นี้ถูกส่งผ่านไปยังปลายทางได้ ซึ่งเรียกว่า hop count
- ส่วนโพรโตคอล เป็นข้อมูลการระบุโพรโตคอลที่ทำงานใน layer ข้างบนซึ่งผนึกลงมาใน IP datagram ซึ่งตัวอย่างของโพรโตคอล ในชั้นบนที่ถูกผนึกมาให้ IP นี้ก็ได้แก่ โพรโตคอล ICMP , โพรโตคอล TCP และโพรโตคอล UDP เป็นต้น ส่วนค่าที่อยู่ในฟิลด์นี้จะเป็นตัวเลขตามตารางที่ 2-4

ตารางที่ 2-4 แสดงค่าที่ระบุโพรโตคอลที่ใช้บ่อยๆ

โปรโตคอล	ค่าที่กำหนดในฟิลด์	คำอธิบาย
ICMP	1	Internet Control Message Protocol
TCP	6	Transmission Control Protocol
BGP	8	Border Gateway Protocol
UDP	17	User Datagram ProtocOl
OSPF	89	Open Shortest Path First

- ส่วน Header Checksum เป็นส่วนของข้อมูลที่ใช้ตรวจสอบความถูกต้องของข้อมูลเฉพาะในส่วนของ IP header โดยไม่เกี่ยวกับส่วนของ payload ซึ่งการตรวจสอบความถูกต้องของข้อมูลนี้ โพรโตคอล IP จะทำหน้าที่ในการคำนวณและตรวจสอบ โดยกรณีที่เกิดความผิดพลาดของข้อมูล IP datagram นั้นจะถูกยกเลิกหรือไม่รับข้อมูลมาใช้งาน
- ส่วน Source IP address เป็นส่วนเก็บข้อมูลของหมายเลข IP ต้นทางที่ IP datagram นี้ถูกส่งมา
- ส่วน Destination IP address เป็นส่วนเก็บข้อมูลของหมายเลข IP ปลายทางที่เป็นผู้รับข้อมูล IP datagram นี้

- ส่วน Option เป็นฟิลด์เก็บข้อมูลที่มีขนาดไม่แน่นอน ใช้สำหรับกำหนดค่าพารามิเตอร์ส่วนประกอบปลีกย่อย ซึ่งส่วนใหญ่ไม่มีการนำไปใช้งาน
- และส่วนสุดท้าย คือ Padding ทำหน้าที่เป็นส่วนข้อมูลเติมเต็มเพื่อให้ IP header เต็มครบ 32 ไบต์ ซึ่งเป็นผลมาจาก Option ที่มีขนาดไม่แน่นอนนั่นเอง

2.15 หลักการทำงานของ Socket

Socket ถูกกำหนดหรือนิยามไว้ว่า เป็นคู่ของการสื่อสาร หรือคู่ของ process (หรือThread) โดยที่การสื่อสารบน Network ใช้คู่ของ Socket สำหรับแต่ละ process

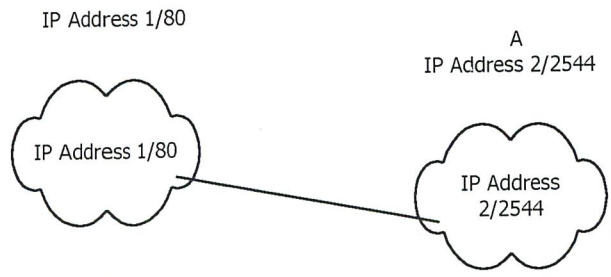
สำหรับ Socket ประกอบไปด้วย IP Address กับหมายเลข Port (Port Number)

โดยทั่วๆไป Socket ใช้สถาปัตยกรรมไคลเอนต์/เซิร์ฟเวอร์ จะรอการเข้ามาตามการขอร้องของไคลเอนต์ โดยการฟังที่port เฉพาะ เมื่อการขอร้องได้รับเซิร์ฟเวอร์ก็จะยอมรับการเชื่อมต่อจาก Socket client เพื่อให้สมบูรณ์ในการเชื่อมต่อ

เซิร์ฟเวอร์ ที่สร้างการบริการเฉพาะ เช่น telnet, ftp, mail และ http จะฟัง (listen) ที่พอร์ตมีชื่อ เช่น เซิร์ฟเวอร์ telnet จะฟังที่พอร์ต 23, เซิร์ฟเวอร์ ftp จะฟังที่พอร์ต 21 หรือ เซิร์ฟเวอร์ http จะฟังที่พอร์ต 80 เป็นต้น

หมายเลขพอร์ตทั้งหมดที่ต่ำกว่า 1,024 จะถูกพิจารณาว่าเป็นพอร์ตที่มีชื่อเสียง สามารถใช้พอร์ตเหล่านี้เพื่อสร้างการบริการมาตรฐานได้

ตัวอย่างการสื่อสารด้วย Socket เมื่อ thread client เริ่มต้นการขอร้องสำหรับการเชื่อมต่อ จะถูกกำหนดพอร์ตโดย host คอมพิวเตอร์ (Host Computer) พอร์ตนี้เป็นหมายเลขใดๆก็ได้ที่มากกว่า 1,024 ตัวอย่างเช่น ถ้าไคลเอนต์บน host A มี IP Address 2 ต้องการที่สร้างการเชื่อมต่อกับ เซิร์ฟเวอร์ http (ซึ่งฟังที่พอร์ต 80) ที่มี IP Address 1 host A จะถูกกำหนดพอร์ต 2,544 และที่ฝั่ง เซิร์ฟเวอร์ จะเป็นพอร์ต 80 สถานการณ์นั้นสามารถแสดงได้ดังรูปที่ 2-22 package ไปมาระหว่าง host ทั้งสองจะถูกส่งไปยัง thread ที่เหมาะสม ซึ่งขึ้นอยู่กับหมายเลขพอร์ตปลายทาง



รูปที่ 2-22 แสดงการสื่อสารโดยใช้ Socket

การเชื่อมต่อทั้งหมดเป็นคุณสมบัติเฉพาะ ดังนั้นถ้า process อื่นๆ บน host A ต้องการสร้างการเชื่อมต่ออื่นๆ กับ เซิร์ฟเวอร์ http เดียวกัน เซิร์ฟเวอร์ จะกำหนดหมายเลขพอร์ตที่มากกว่า 1,024 และต้องไม่เท่ากับพอร์ต 2,544 (เนื่องจากถูกใช้ไปแล้ว) การทำอย่างนี้เพื่อให้แน่ใจว่าการเชื่อมต่อทั้งหมดประกอบด้วยคู่ที่เป็นยูนิค (Unique) ของ Socket หรือเป็นสิ่งที่ไม่ซ้ำกับการเชื่อมต่ออื่น ๆ ของ Socket

โดยปกติแล้วเซิร์ฟเวอร์จะมีหลายๆการขอร้องที่พร้อมกัน จะต้องใช้ระยะเวลาหนึ่งที่ไคลเอนต์ต้องรอคอยเพื่อที่จะถูกบริการโดย server thread เดียว ซึ่งจะไม่สามารถรับได้

เพื่อแก้ไขสถานการณ์นี้เซิร์ฟเวอร์ ต้องจัดการการขอร้องที่พร้อมๆ กัน โดยการกำหนด thread แยกออกมาเพื่อบริการแต่ละการขอร้องที่เข้ามา ตัวอย่างเช่น เซิร์ฟเวอร์ http ที่ไม่ว่างจะกำหนด thread แยกออกมาเพื่อบริการแต่ละการขอร้องสำหรับเว็บเพจ

IP Address จะเป็น 32 บิต ซึ่งทำหน้าที่ระบุ host บนอินเตอร์เน็ตและขณะที่หมายเลขพอร์ตจะเป็น 16 บิต ซึ่งทำหน้าที่ระบุ process บน host นั้นๆ

2.16 ชนิดของ Socket

ชนิดของ Socket มีอยู่สามชนิด คือ

1. Connection-Oriented Socket
2. Connectionless Socket
3. Raw Socket

2.16.1 หลักการทำงานของ Connection-Oriented Socket

เป็น Socket การเชื่อมต่อแบบต่อเนื่องที่อนุญาตให้ process เชื่อมต่อกับ process ระยะไกล (Remote) ซึ่งใช้โพรโตคอล TCP (Transmission Control Protocol) ดังนั้นด้วยวิธีการนี้ทำให้ข้อมูลเชื่อถือได้ เมื่อการเชื่อมต่อได้เกิดขึ้นโพรเซสก็จะมีการส่งข้อมูลกลับไปจนกระทั่งฝั่งใดฝั่งหนึ่งหรืออื่นๆ มีการปิดการเชื่อมต่อ ชนิดของ Socket นี้ บางครั้งเรียกว่า Stream Socket ทั้ง ftp และ http ใช้ Socket แบบนี้ในการสื่อสาร

2.16.2 หลักการทำงานของ Connectionless Socket

หรือเรียกอีกอย่างว่า datagram เป็น Socket แบบไม่ต่อเนื่อง และนำมาใช้เป็นประโยชน์ในการส่งmessage สั้นๆ ซึ่งไม่สามารถสนับสนุนส่วนหัว ดังนั้นจึงพิจารณาการเชื่อมต่อประเภทนี้เป็นแบบเชื่อถือไม่ได้ ซึ่งก็คือ การไม่รับประกันข้อมูลที่ถูกส่งออกไป ไม่เหมือนกับ Socket ปลายทางถูกตรวจสอบเมื่อ package ถูกส่งออกไป

Socket แบบไม่ต่อเนื่อง เปรียบเสมือนกับการบริการของไปรษณีย์ที่ผู้ส่งจดหมายไปตามที่อยู่แล้วใส่ในกล่องรับจดหมาย ผู้ส่งจะไม่ทราบว่าผู้รับได้รับจดหมายหรือไม่ Socket แบบนี้นิยมใช้กัน

ในเซิร์ฟเวอร์ DNS (Domain Name System) ที่ใช้ Socket datagram ในการตอบสนองต่อการขอร้องที่เข้ามามากๆ

นอกจากนี้จะใช้ datagram Socket ในการกระจาย (Broadcast) message หรือ Multicast เพื่อไปยังปลายทางหลายๆ แห่งพร้อมกัน ซึ่งเหมือนกับการกระจายเสียงวิทยุ หรือ โทรทัศน์

2.16.3 หลักการทำงานของ Raw Socket

เป็น Socket ที่อนุญาตให้การเข้าถึง protocol Transport Raw Socket ยังสามารถนำมาใช้เพื่อจัดการ (IP Header) นอกจากนี้แล้วการใช้ Socket ชนิดนี้ ต้องการความรู้อย่างมากของโครงสร้างโพรโตคอลพื้นฐาน

ยังมีอีก Socket หนึ่งเป็น Infrared Socket หรือ Irsock ซึ่งเป็นเทคโนโลยีตัวใหม่ที่แนะนำใน Windows CE โดยที่ Infrared Socket อนุญาตให้เครื่องคอมพิวเตอร์สองเครื่องติดต่อสื่อสารซึ่งกันและกันตลอดโดย พอร์ตอนุกรม Socket Infrared ใช้โพรโตคอลแบบต่อเนื่อง (Connection Oriented) ซึ่งเป็น ที่เชื่อถือได้

บทที่ 3
การออกแบบและการพัฒนาโปรแกรม

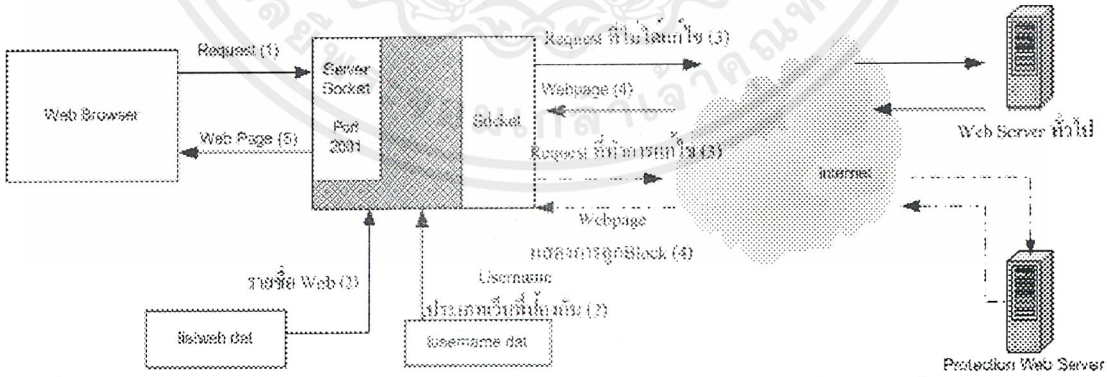
หลักการทำงานของโปรแกรมจะแบ่งออกเป็น 2 ส่วนคือ

- ส่วนโปรแกรมที่ทำการตรวจสอบการร้องขอเว็บเพจ
- ส่วนที่ทำการเพิ่มเติมรายชื่อเว็บเพจที่ส่วนกลาง

โดยจะมีการทำงานโดยรวมดังนี้

3.1 ส่วนโปรแกรมที่ทำการตรวจสอบการร้องขอเว็บเพจ

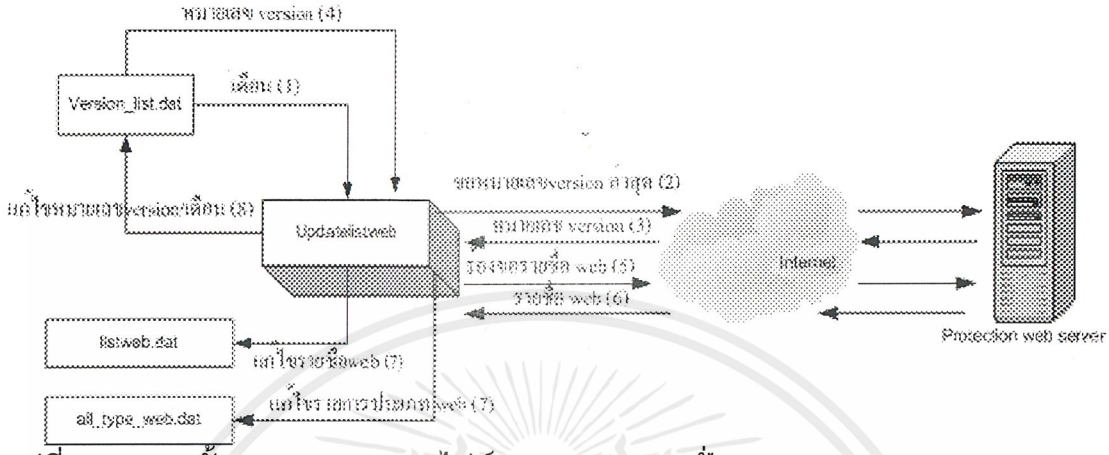
ส่วนนี้จะทำการตรวจสอบการร้องขอเว็บเพจจากเว็บบราวเซอร์ เมื่อเปิดเครื่องโปรแกรมจะทำการถาม Username แล้วจะนำ Username ที่ได้ไปตรวจสอบกับ รายชื่อ User ใน ไฟล์ lusername.dat ถ้าพบ Username โปรแกรมจะดึงประเภทการป้องกันมาใช้งาน แล้วทำการสร้าง Server Socket ไว้ที่ Port 2001 เพื่อรอการร้องขอจากเว็บบราวเซอร์ เมื่อมีการร้องขอโปรแกรมจะทำการนำการร้องขอนั้นไปตรวจสอบกับรายชื่อเว็บเพจที่ไม่เหมาะสมที่อยู่ในไฟล์ listweb.dat แล้วทำการสร้าง Socket โดยจะเลือก Port ที่ว่างในเครื่องนั้นเพื่อทำการร้องขอเว็บเพจ หากการร้องขอนั้นเป็นการร้องขอเว็บเพจที่มีรายชื่ออยู่ใน listweb.dat และ เป็นเว็บเพจนั้นประเภทที่ User นั้นถูกป้องกัน ก็จะทำการเปลี่ยนการร้องขอนั้นให้ไปดึงเว็บเพจที่ทำการแจ้งว่าการร้องขอนั้นเป็นการร้องขอที่ไม่เหมาะสม และหากการร้องขอนั้นเป็นเว็บเพจที่เหมาะสมก็จะทำการร้องขอเว็บเพจนั้นให้ดังรูปที่ 3-1



รูปที่ 3-1 แสดงการทำงานของโปรแกรมในส่วนตรวจสอบและการร้องขอเว็บเพจ

นอกจากนี้ยังมีProgram Updatelistweb ที่ทำการตรวจสอบ version ของ listweb.dat โดยจะตรวจสอบทุกเดือน โดยโปรแกรมจะร้องขอเลข version ล่าสุดจาก Server และนำมาตรวจกับ

version ที่เก็บไว้ใน Version.dat ว่าเท่ากันหรือไม่ หากไม่เท่ากัน ก็ส่งการร้องขอไฟล์ listweb.dat และ list_all_type.dat ตัวใหม่ไปยัง Server แล้ว นำไฟล์ listweb.dat และ list_all_type.dat มาเขียนทับของเก่า แล้วทำการเปลี่ยนเลข version ดังรูปที่ 3-2



รูปที่ 3-2 แสดงขั้นตอนการ update ไฟล์ listweb.dat ทางฝั่ง Client

3.2 ส่วนที่ทำการเพิ่มเติมรายชื่อเว็บเพจที่ส่วนกลาง

การทำงานของโปรแกรมทางฝั่ง Server จะมีการให้บริการไฟล์ listweb_server.dat ซึ่งเป็นไฟล์ที่เก็บรายชื่อเว็บไซต์ที่ไม่เหมาะสม เพื่อให้โปรแกรมทางฝั่ง Client ได้ Download ไปใช้งาน ถ้าโปรแกรมทางฝั่ง Server ทำการ update ไฟล์ listweb_server.dat เมื่อไหร่ โปรแกรมทางฝั่ง Server ก็จะทำการเก็บ วันที่ เวลา และ version ล่าสุดในไฟล์ filedate_version.dat เอาไว้สำหรับให้โปรแกรมทางฝั่ง Client ทำการตรวจสอบว่า version ไฟล์ listweb_server.dat ที่โปรแกรมทางฝั่ง Client มีอยู่เป็น version ล่าสุดหรือเปล่า ถ้าไม่ใช่โปรแกรมทางฝั่ง Client ก็จะทำการ Download ไฟล์ listweb_server.dat จากโปรแกรมทางฝั่ง Server

3.3 การออกแบบไฟล์ในตรวจสอบการร้องขอเว็บเพจ

ประกอบด้วย 4 ไฟล์คือ

1. ไฟล์ lusername.dat เก็บ username,ประเภทเว็บที่ต้องการป้องกันโดยลักษณะการจัดเก็บดังรูปที่ 3-3

Username	Web Type	Username	Web Type	.....

รูปที่ 3-3 ลักษณะการจัดเก็บไฟล์ lusername.dat

ตัวอย่าง เช่น

boripat เป็น Username

13 เป็นประเภทเว็บที่ต้องการป้องกันโดย

หมายเลข 1 หมายถึงเป็นเว็บประเภทลามกอนาจาร

หมายเลข 2 หมายถึงเป็นเว็บประเภทรุนแรง

หมายเลข 3 หมายถึงเป็นเว็บประเภทการพนัน

หมายเลข 4 หมายถึงเป็นเว็บประเภทลัทธินอกรีต

ดังนั้นถ้าเก็บเป็น 13 หมายถึงต้องการจะป้องกันเว็บประเภทลามกอนาจารและเว็บการพนัน จะถูกจัดเก็บในไฟล์เป็นดังนี้

boripat :13/

2. ไฟล์ listweb.dat เก็บรายชื่อเว็บไซต์ที่ไม่เหมาะสม ซึ่งไฟล์นี้ต้องมีการ update version จากทาง server โดยลักษณะการจัดเก็บดังรูปที่ 3-4

URL	status	URL	status	.....

รูปที่ 3-4 ลักษณะการจัดเก็บไฟล์ listweb.dat

status คือจะบอกว่า URL นั้นจัดอยู่ในประเภทอะไรบ้างแทนด้วย

หมายเลข 1 หมายถึงเป็นเว็บประเภทลามกอนาจาร

หมายเลข 2 หมายถึงเป็นเว็บประเภทรุนแรง

หมายเลข 3 หมายถึงเป็นเว็บประเภทการพนัน

หมายเลข 4 หมายถึงเป็นเว็บประเภทลัทธินอกรีต

ตัวอย่าง เช่น

xxx.com จัดอยู่ในประเภท ลามกอนาจาร

casino.com จัดอยู่ในประเภท การพนัน

haha.com จัดอยู่ในประเภท รุนแรง และ ลัทธินอกรีต

จะถูกจัดเก็บใน file เป็นดังนี้

xxx.com:1*casino.com:3*haha.com:24*

3. ไฟล์ version_list.dat เก็บ version ของ listweb.dat และเก็บวันที่ของการ update ไฟล์ครั้งหลังสุดดังรูปที่ 3-5

month	version

รูปที่ 3-5 ลักษณะการจัดเก็บของไฟล์ version.dat

4. ไฟล์ all_type_web.dat โดยจะเก็บรายการประเภทเว็บที่จะป้องกัน โดยจะแสดงดังรูปที่ 3-6

ชื่อประเภท	ตัวเลขที่ใช้แทน	ชื่อประเภท	ตัวเลขที่ใช้แทน	.....

รูปที่ 3-6 ลักษณะการจัดเก็บของไฟล์ all_type_web.dat

3.4 การออกแบบไฟล์ทางเครื่อง Server ที่ทำการเพิ่มเติมรายชื่อเว็บเพจที่ส่วนกลาง

ประกอบด้วย 2 ไฟล์ คือ

1. ไฟล์ usepass.dat เก็บ Password และ Username โดยลักษณะการจัดเก็บดังรูปที่ 3-7

Username	Passwordd

รูปที่ 3-7 ลักษณะการจัดเก็บของไฟล์ usepass.dat

ตัวอย่าง เช่น

ksskss เป็น username

41056005 เป็น Password

จะถูกจัดเก็บในfile เป็นดังนี้

ksskss/41056005

2. ไฟล์ listweb_server.dat เก็บ URL ที่ต้องการป้องกันการเชื่อมต่อ
   - ลักษณะการจัดเก็บจะเหมือนกับไฟล์ listweb.dat ทางฝั่ง client
3. ไฟล์ filedate_version.dat เก็บ version ของ ไฟล์ listweb_server.dat โดยลักษณะการจัดเก็บดังรูปที่ 3-8

date	time	version

รูปที่ 3-8 ลักษณะการจัดเก็บของไฟล์ version_server.dat

ตัวอย่าง เช่น

14 March 2002 12:15:27 PM/v.4

4. ไฟล์ type_web.dat เก็บประเภทของเว็บไซต์ที่ไม่เหมาะสมโดยลักษณะการจัดเก็บดังรูปที่ 3-9

ชื่อประเภท	แทนด้วยตัวเลขหรือตัวอักษร	ชื่อประเภท	.....

รูปที่ 3-9 ลักษณะการจัดเก็บประเภทของเว็บไซต์ที่ไม่เหมาะสม

การแทนประเภทด้วยตัวเลขจะแทนประเภทตั้งแต่ 1-9

การแทนประเภทด้วยตัวอักษรจะแทนประเภทตั้งแต่ 10 ขึ้นไป จะใช้ตัวอักษรภาษาอังกฤษในการแทนประเภท ดังนี้ ประเภทที่ 10 แทนด้วย a , ประเภทที่ 11 แทนด้วย b ....

ตัวอย่าง เช่น ลามก:1/รุนแรง:2/การพนัน:3/ลัทธินอกรีด:4/aaaa:5/bbbb:6/cccc:7/

5. ไฟล์ listweb_server.dat เก็บรายชื่อเว็บไซต์ที่ไม่เหมาะสม โดยลักษณะการจัดเก็บดังรูปที่ 3-10

URL	status	URL	status	.....

รูปที่ 3-10 ลักษณะการจัดเก็บไฟล์ listweb_server.dat

status คือจะบอกว่า URL นั้นจัดอยู่ในประเภทอะไรบ้างแทนด้วย

เช่น หมายเลข 1 หมายถึงเป็นเว็บประเภทลามกอนาจาร

หมายเลข 2 หมายถึงเป็นเว็บประเภทรุนแรง

ตัวอย่าง เช่น

xxx.com จัดอยู่ในประเภท ลามกอนาจาร

haha.com จัดอยู่ในประเภท รุนแรง และ ลัทธินอกรีต

จะถูกจัดเก็บใน file เป็นดังนี้

xxx.com:1*haha.com:24*

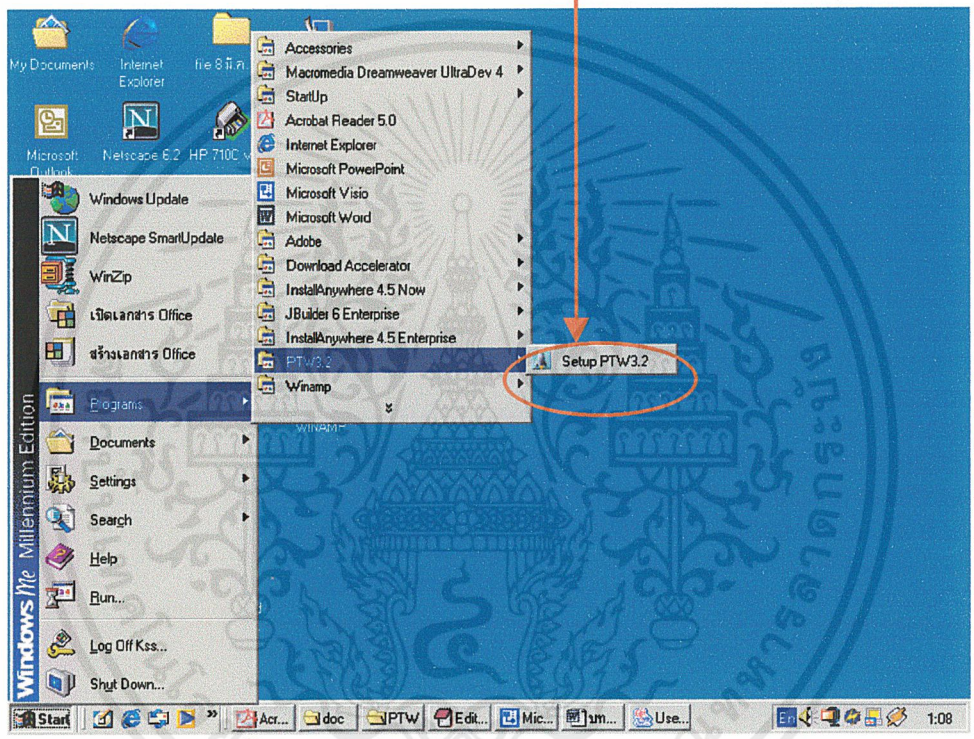
บทที่ 4
การใช้งานโปรแกรม

4.1 การทำงานของโปรแกรมทางฝั่งไคลเอนต์

โปรแกรมทางฝั่งไคลเอนต์จะที่การทำงานอยู่ 2 ส่วนคือ

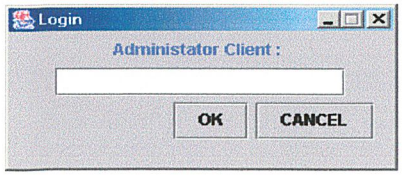
4.1.1 การทำงานในส่วนของการจัดการระบบของผู้ดูแลระบบทางฝั่ง Client

ในการเรียกใช้ให้เลือก Start → Programs → PTW3.2 และเลือก Setup PTW3.2 ดังรูปที่ 4-1



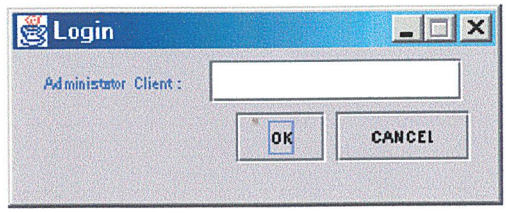
รูปที่ 4-1 แสดงการเรียกใช้ Setup PTW3.2

เมื่อเลือกSetup PTW3.2 แล้ว จะแสดงหน้า Login ขึ้นมาให้กรอก Password ของ Administrator Client แล้ว กดปุ่ม OK หรือ กดปุ่ม Cancel ถ้าต้องการออกจากโปรแกรม ดังรูปที่ 4-2



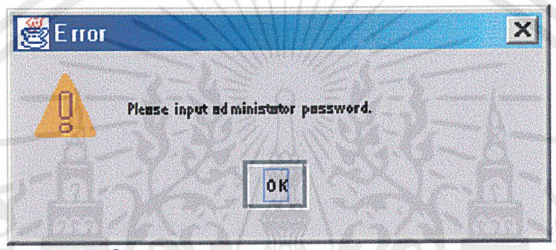
รูปที่ 4-2 แสดงหน้าจอ Login

เมื่อเลือก Setup PTW3.2 แล้ว จะแสดงหน้า Login ขึ้นมาให้กรอก password ของ administrator client แล้ว กดปุ่ม OK หรือ กดปุ่ม Cancel ถ้าต้องการออกจากโปรแกรม ดังรูปที่ 4-2



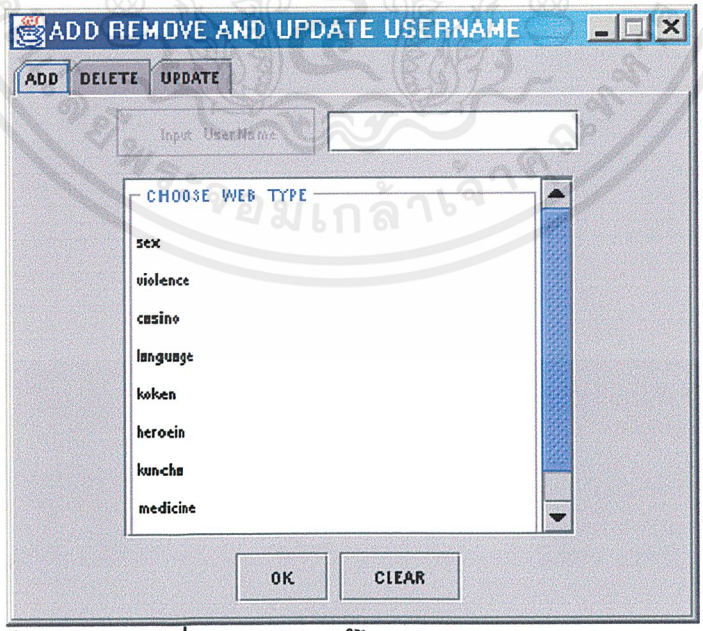
รูปที่ 4-2 แสดงหน้าจอ Login

หากยังไม่ได้กรอก password แล้วกด OK จะแสดงหน้าจอเตือนให้ใส่ username ดังรูปที่ 4-3



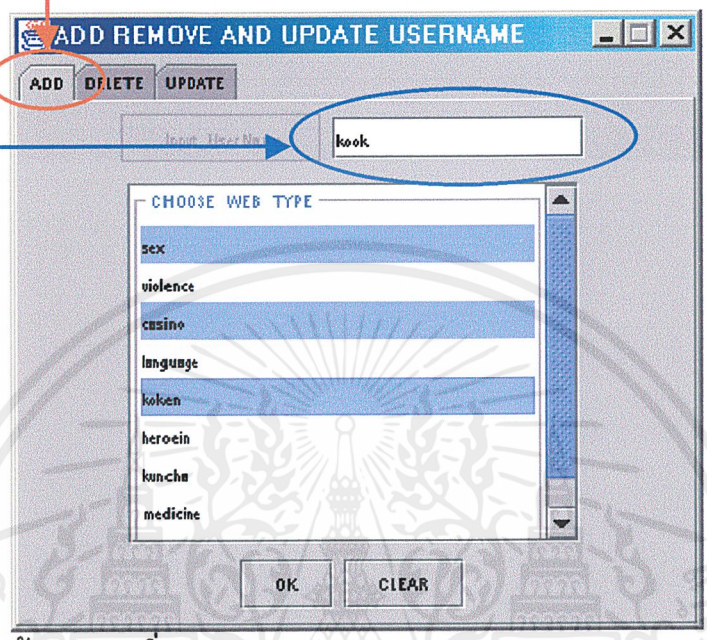
รูปที่ 4-3 แสดงหน้าจอเตือนให้ใส่ password

ถ้ากรอกข้อมูลในรูปที่ 4-2 แล้วคลิก OK ก็จะแสดงหน้าจอให้ administrator client สามารถ เพิ่ม ลบ และแก้ไขข้อมูลของผู้ใช้แต่ละคนได้ แสดงดังรูปที่ 4-4



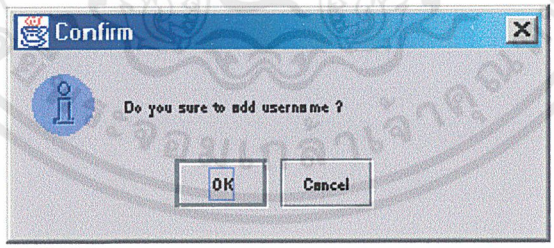
รูปที่ 4-4 แสดงหน้าจอในการเพิ่ม ลบ และแก้ไข username

หากต้องการเพิ่ม username ให้เลือกที่ Tab ADD แล้วทำการกรอก username ที่ต้องการเพิ่มลงในช่องว่าง แล้ว เลือกประเภทเว็บที่ต้องการป้องกัน หากต้องการเลือกมากกว่าหนึ่งประเภท ให้กด Ctrl ค้างไว้แล้วหรือประเภทเว็บที่ต้องการป้องกัน เมื่อเลือกเสร็จแล้วให้กดปุ่ม OK หรือหากต้องการเลือกใหม่ให้กดปุ่ม CLEAR ดังรูปที่ 4-5



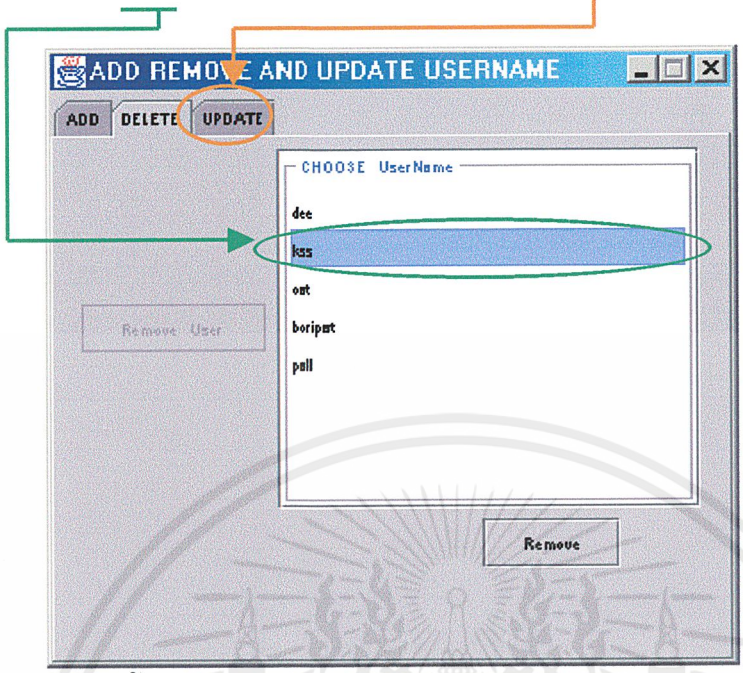
รูปที่ 4-5 แสดงหน้าจอการเพิ่ม username

เมื่อคลิกปุ่ม OK จะแสดงหน้าจอดังรูปที่ 4-6 ซึ่งเป็นหน้าจอที่ทำการถามว่าต้องการเพิ่มรายชื่อนี้ใช่หรือไม่ คลิก OK ถ้าต้องการเพิ่ม คลิก Cancel ถ้าต้องการยกเลิก



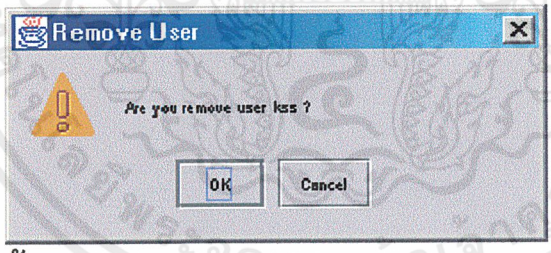
รูปที่ 4-6 แสดงหน้าจอการ Confirm

หากต้องการลบ username ที่มีอยู่แล้วให้เลือกที่ Tab DELETE แล้วเลือก username ที่ต้องการลบจากใน List โดยสามารถเลือกลบได้เพียงครั้งละ 1 username ดังรูปที่ 4-7



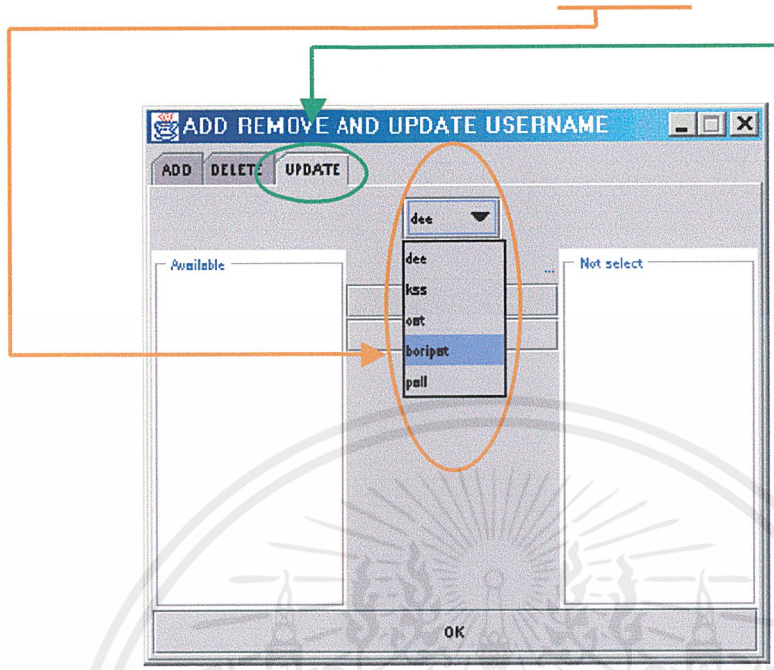
รูปที่ 4-7 แสดงหน้าจอการลบ username

เมื่อกดปุ่ม Remove โปรแกรมจะทำการแสดงหน้าจอ Remove User หากต้องการลบ Username ที่เลือกไว้ให้กดปุ่ม OK แต่หากไม่ต้องลบให้กดปุ่ม Cancel ดังรูปที่ 4-8



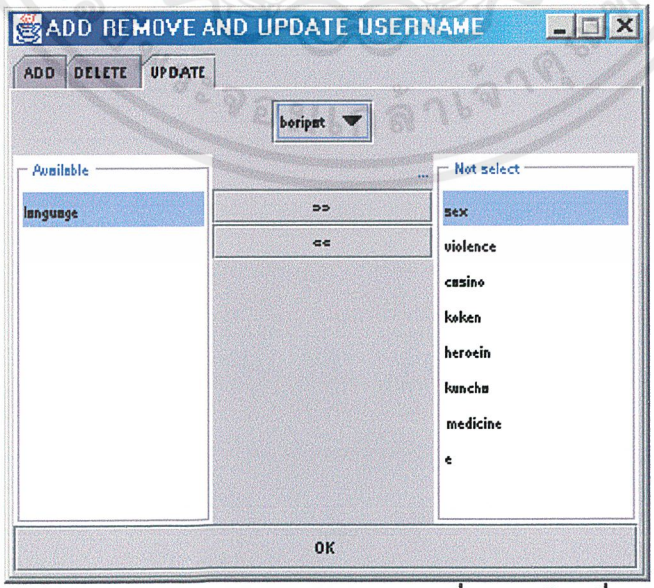
รูปที่ 4-8 แสดงหน้าจอการ Remove User

หากต้องการแก้ไขประเภทที่ต้องการป้องกันของแต่ละ username ให้เลือกที่ Tab UPDATE แล้วทำการเลือก username ที่ต้องการแก้ไขข้อมูลจาก combobox ดังรูปที่ 4-9



รูปที่ 4-9 แสดงหน้าจอการเลือก username เพื่อทำการ update

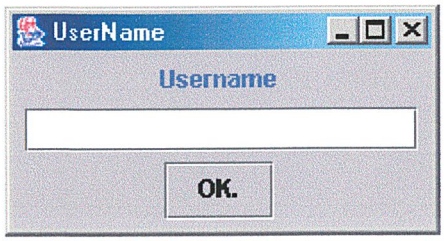
เมื่อเลือก username ได้แล้ว หากต้องการเพิ่มประเภทเว็บไซต์ที่ต้องการป้องกัน ให้เลือกจาก List Not select แล้วคลิกที่ปุ่ม << และหากต้องการลดประเภทเว็บไซต์ที่ต้องการป้องกัน ให้เลือกจาก List Available แล้วคลิกที่ปุ่ม >> โดยการเลือกจะเลือกได้เพียงทีละรายการเดียว เมื่อเลือกเสร็จแล้วว่าต้องการจะเพิ่มหรือลดประเภทเว็บไซต์ใดบ้างก็ให้คลิกที่ปุ่ม OK



รูปที่ 4-10 แสดงหน้าจอการเลือกรายการจาก List เพื่อลบหรือเพิ่มประเภทเว็บไซต์

4.1.2 การทำงานในส่วนของผู้ใช้

เมื่อทำการเปิดเครื่องโปรแกรมจะทำการแสดงหน้าจอ Username เพื่อให้ผู้ใช้กรอก Username เพื่อจะเลือกประเภทการป้องกัน แล้วกดปุ่มOK ดังรูปที่ 4-11

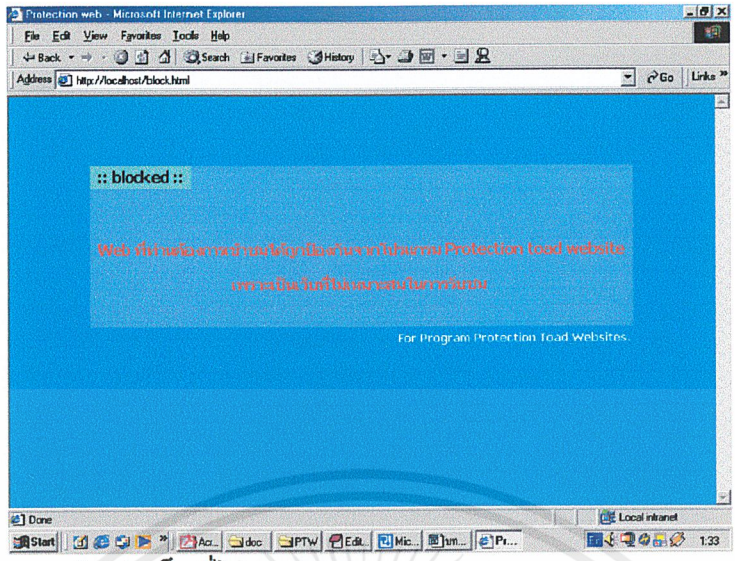


รูปที่ 4-11 แสดงหน้าจอ Username

เมื่อผู้ใช้ เรียกหน้าเว็บเพจที่ต้องการจากเว็บเบราเซอร์ เว็บเบราเซอร์จะทำการส่ง request ไปยังโปรแกรม Cheackrequest แล้วโปรแกรมก็จะตรวจสอบว่าเป็นเว็บไซต์ที่เหมาะสมหรือไม่ หากเป็นเว็บไซต์ที่เหมาะสมจะทำการสร้าง request แล้วส่งไปยัง Host ที่เว็บเบราเซอร์นั้น request มา จากนั้น Host จะส่ง response กลับมายังโปรแกรม แล้วโปรแกรมก็ทำการส่งเข้าเว็บเบราเซอร์อีกทีหนึ่ง แล้วจะแสดงข้อมูลออกทางเว็บเบราเซอร์ เช่นถ้าร้องขอเว็บ www.kmitl.ac.th ซึ่งเป็นเว็บที่เหมาะสม จะแสดงดังรูป 4-12

รูปที่ 4-12 แสดงการติดต่อเว็บที่เหมาะสม

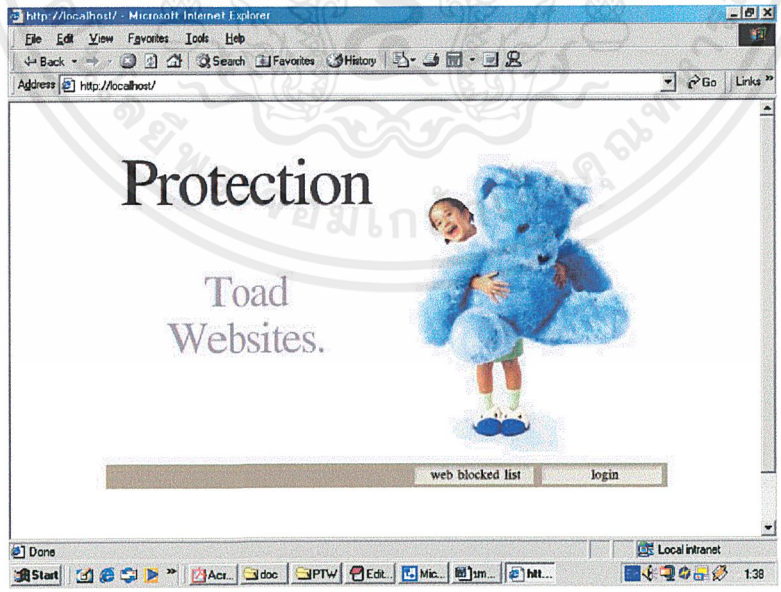
แต่ถ้าเป็นเว็บที่ไม่เหมาะสม โปรแกรมจะทำการเปลี่ยนข้อมูลใน request เป็นร้องขอหน้าเว็บเพจที่แสดงให้เห็นว่าการร้องขอนั้นเป็นการร้องขอเว็บเพจที่ไม่เหมาะสมในการรับชมดังรูปที่ 4-13



รูปที่ 4-13 แสดงการติดต่อเว็บที่ไม่เหมาะสม

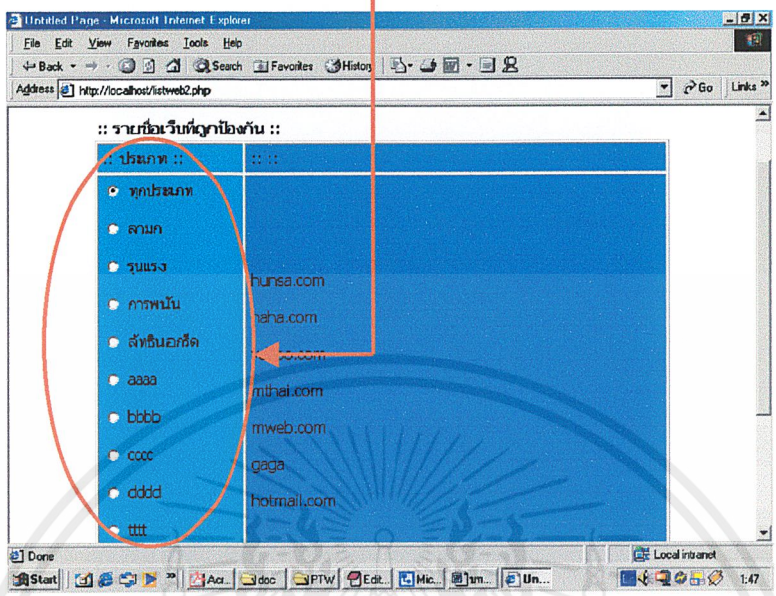
4.2 การทำงานของโปรแกรมทางฝั่งเซิร์ฟเวอร์

Administrator ทางฝั่ง Server สามารถที่จะ update file URL ที่ไหนก็ได้ โดยการ update file URL นี้จะทำการ update ผ่านทาง internet โดยใช้เว็บเบราเซอร์ ติดต่อเข้ามายังเครื่องเซิร์ฟเวอร์ โดยจะแสดงหน้าจอหลักโดยหากจะดูรายละเอียดเว็บที่ทำการป้องกันให้เลือก web blocked list หรือหากต้องการทำการการเพิ่มเติมลบหรือแก้ไขรายการเว็บก็ให้เข้า login ดังรูปที่ 4-14



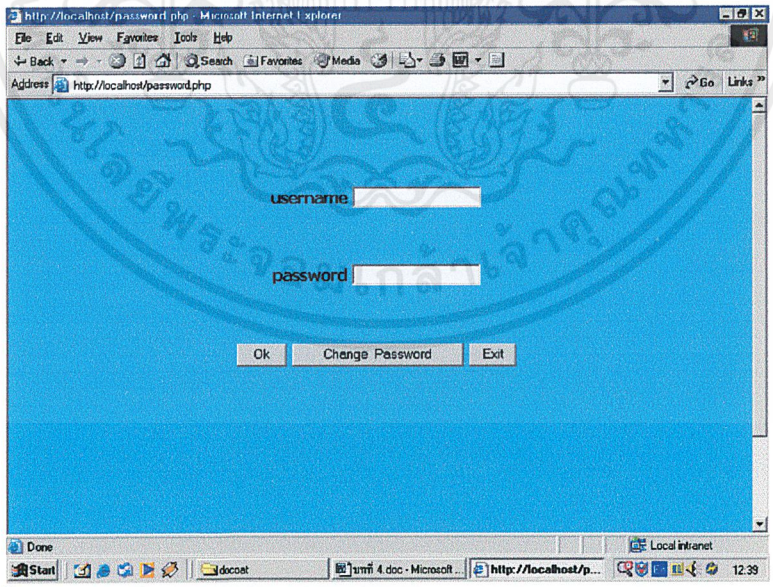
รูปที่ 4-14 หน้า Home Page ของ Web Protection Toad Websites

ถ้าเลือก web blocked list จะแสดงรายละเอียดของรายการเว็บที่โปรแกรมได้ทำการป้องกันไว้โดยจะแสดงตามประเภทเว็บ ที่ระบุไว้ทางฝั่งซ้ายของหน้าจอ ดังรูปที่ 4-15



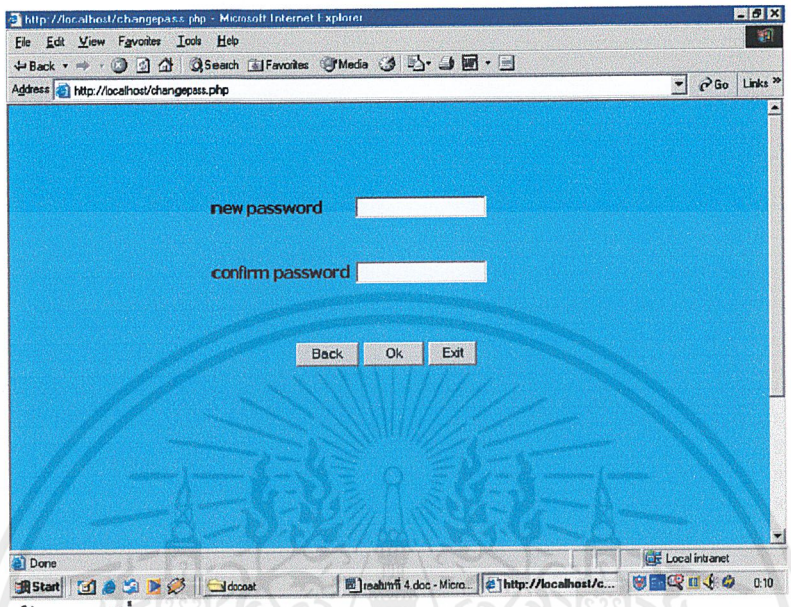
รูปที่ 4-15 หน้าจอแสดงรายชื่อเว็บที่ทำการป้องกัน

จากหน้า Homepage หาก เลือก login จะต้องทำการกรอก username และ password ของ Administrator Server ถ้า username และ password ถูกต้องจะทำการ update file และสามารถที่จะทำการเปลี่ยนแปลง password ได้ ดังรูปที่ 4-16



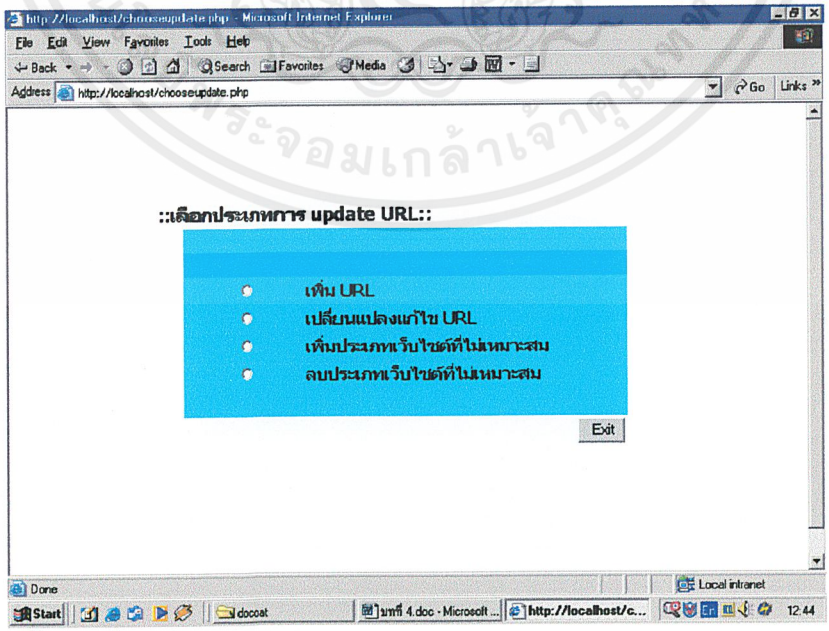
รูปที่ 4-16 หน้าจอ username และ password

ถ้าทำการกดปุ่ม change password หน้าจอ username และ password ก็จะมาหน้าเปลี่ยน password ดังรูปที่ 4-17 หรือ ถ้ากดปุ่ม Ok ก็จะมาหน้าให้เลือกว่าจะทำการ update file แบบไหน จะเพิ่ม URL จะเปลี่ยนแปลงแก้ไข URL หรือเพิ่มประเภทเว็บไซต์ที่ไม่เหมาะสม ดังรูปที่ 4-17



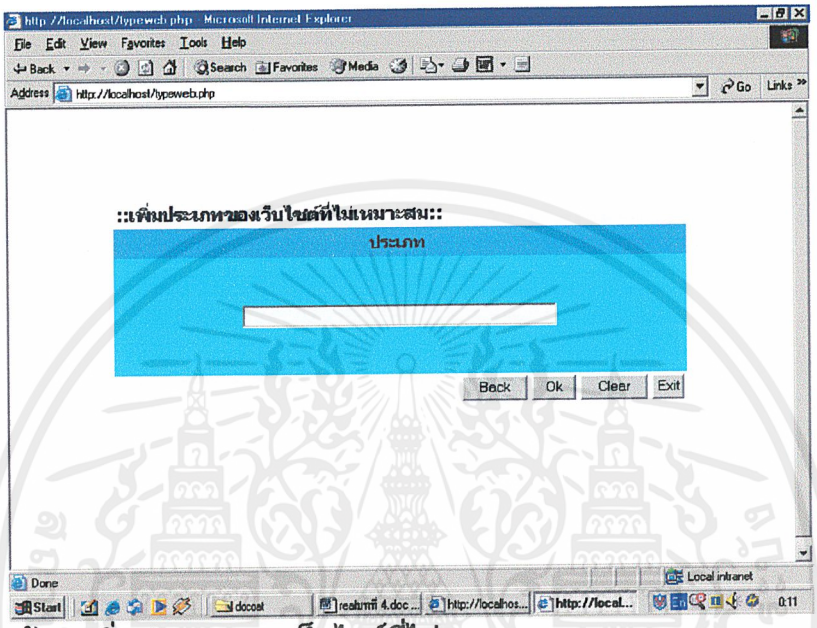
รูปที่ 4-17 หน้าจอเปลี่ยน password

ถ้าทำการกดปุ่ม Ok หน้าจอ username และ password และหน้าจอเปลี่ยน password ก็จะมาหน้าเลือกประเภทการ update URL ว่าเป็นแบบไหน จะเพิ่ม URL จะเปลี่ยนแปลงแก้ไข URL หรือเพิ่มประเภทเว็บไซต์ที่ไม่เหมาะสม เมื่อเลือกเสร็จแล้วให้ทำการกดปุ่ม Ok ดังรูปที่ 4-18



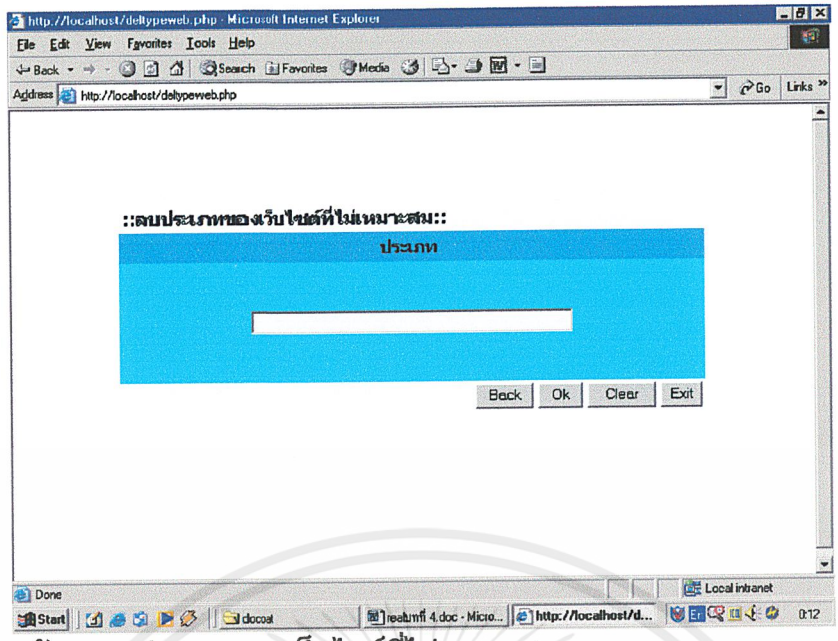
รูปที่ 4-18 หน้าจอเลือกประเภทการ update URL

ถ้าเลือกว่าจะเพิ่มประเภทเว็บไซต์ที่ไม่เหมาะสม จะแสดงหน้าจอเพิ่มประเภทของเว็บไซต์ที่ไม่เหมาะสม ดังรูปที่ 4-19 ซึ่งหน้าจอนี้จะให้ทำการกรอกประเภทของเว็บไซต์ที่ไม่เหมาะสมที่ต้องการเพิ่ม แล้วกดปุ่ม Ok



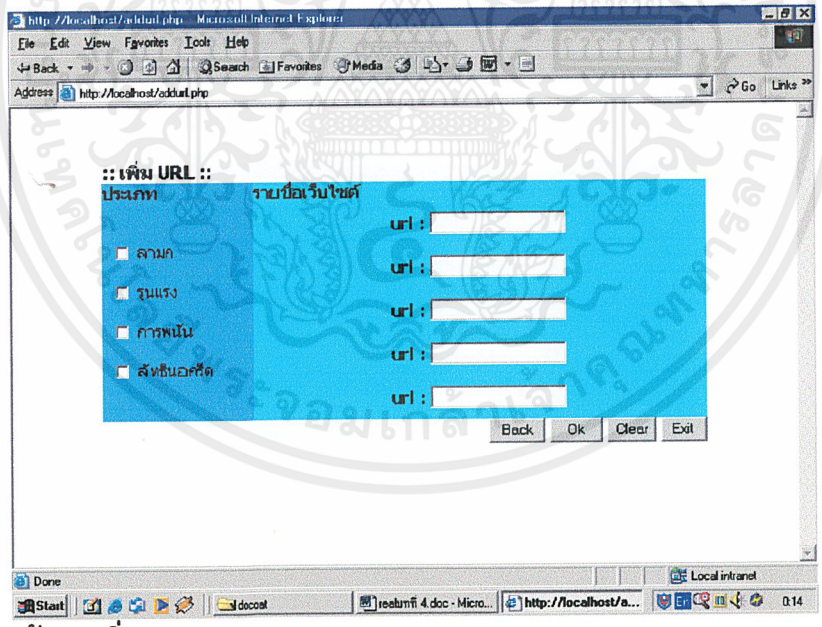
รูปที่ 4-19 หน้าจอเพิ่มประเภทของเว็บไซต์ที่ไม่เหมาะสม

ถ้าเลือกว่าจะลบประเภทเว็บไซต์ที่ไม่เหมาะสม จะแสดงหน้าจอลบประเภทของเว็บไซต์ที่ไม่เหมาะสม ดังรูปที่ 4-20 ซึ่งหน้าจอนี้จะให้ทำการกรอกประเภทของเว็บไซต์ที่ไม่เหมาะสมที่ต้องการลบ แล้วกดปุ่ม Ok



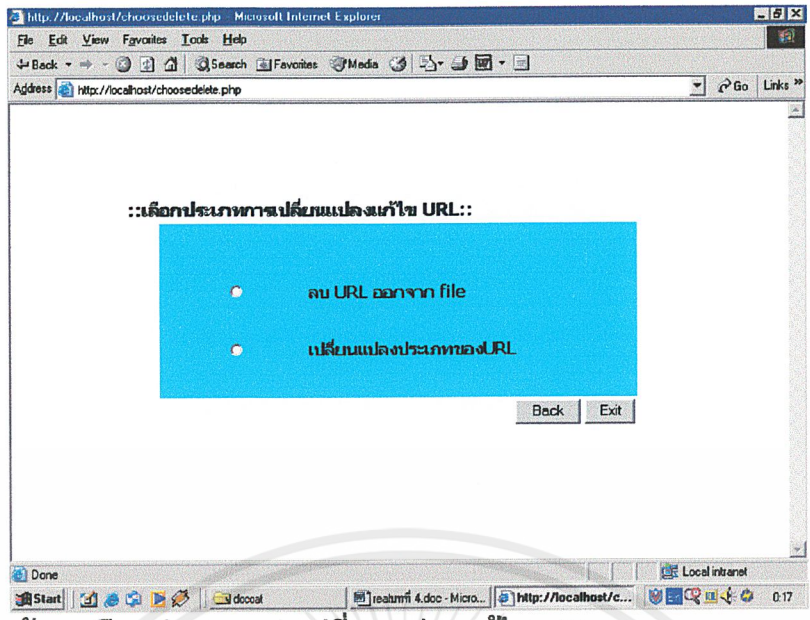
รูปที่ 4-20 หน้าจอลบประเภทของเว็บไซต์ที่ไม่เหมาะสม

ถ้าเลือกว่าจะเพิ่ม URL จะแสดงหน้าจอเพิ่ม URL ดังรูปที่ 4-21 ซึ่งหน้าจอนี้จะให้กรอก URL ที่ต้องการเพิ่มและจะต้องเลือกด้วยว่าจะให้URL นี้จัดอยู่ในประเภทไหน แล้วกดปุ่ม Ok



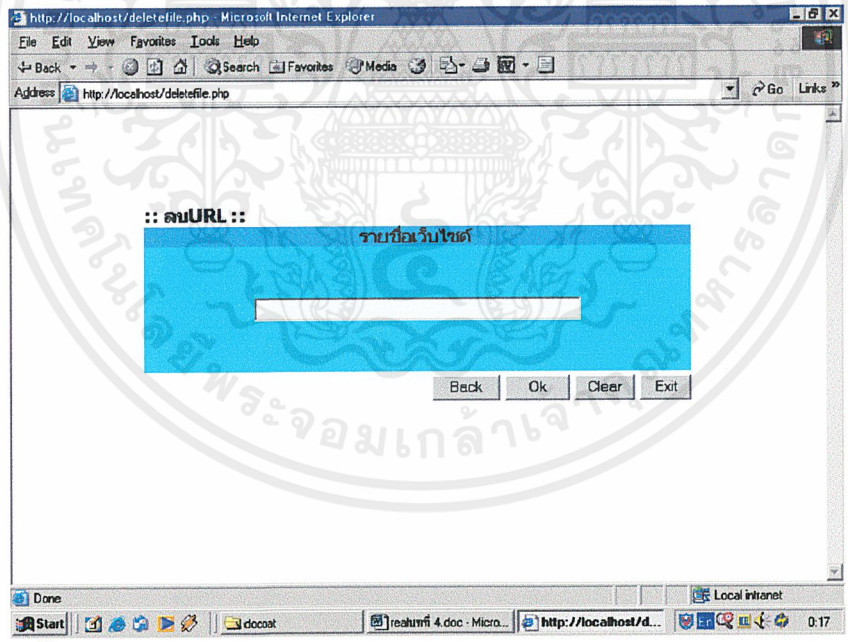
รูปที่ 4-21 หน้าจอเพิ่ม URL

ถ้าเลือกว่าจะเปลี่ยนแปลงแก้ไข URL จะแสดงหน้าจอดังรูปที่ 4-22 ซึ่งให้เลือกอีกว่าจะทำการลบURLออกจากfile หรือ ว่าจะทำการเปลี่ยนแปลงประเภทของURL เลือกเสร็จแล้วให้ทำการกดปุ่ม Ok



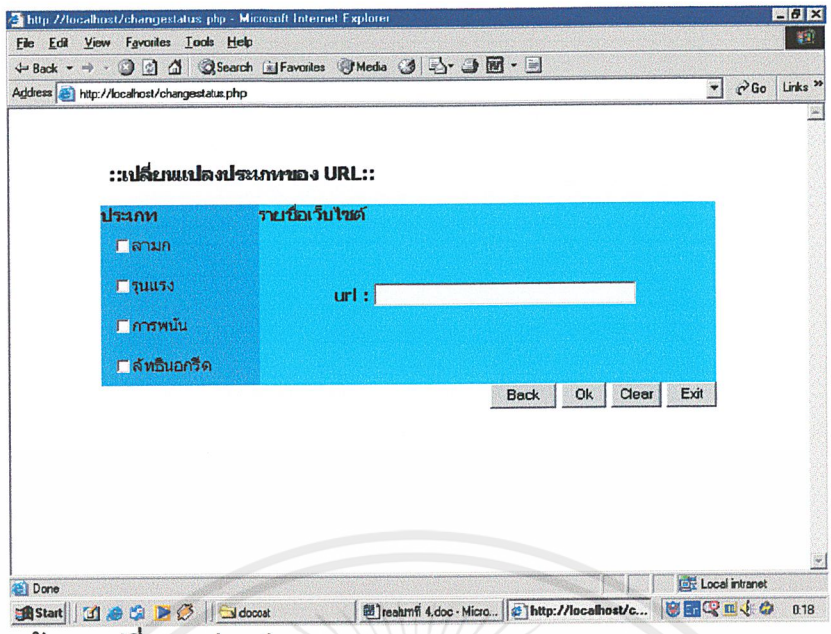
รูปที่ 4-22 หน้าจอเลือกประเภทการเปลี่ยนแปลงแก้ไข URL

ถ้าเลือกลบ URL ออกจาก file จะแสดงหน้าจอดังรูปที่ 4-23 ซึ่งจะให้กรอกURLที่ต้องการให้ลบออกจาก file แล้วกดปุ่ม Ok



รูปที่ 4-23 หน้าจอลบ URLออกจาก flie

ถ้าเลือกทำการเปลี่ยนแปลงประเภทของURL จะแสดงหน้าจอดังรูปที่ 4-24 ซึ่งจะให้กรอก URLที่ต้องการเปลี่ยนประเภท และจะให้ทำการเลือกใหม่ว่าURLนั้น ควรจัดอยู่ในประเภทใดบ้าง เสร็จแล้วกดปุ่ม Ok



รูปที่ 4-24 หน้าจอเปลี่ยนแปลงประเภทของ URL

บทที่ 5
สรุปผลปัญหาพิเศษและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

จากการทดสอบการทำงานของโปรแกรม โปรแกรมสามารถทำงานได้ดังนี้

5.1.1 ทางฝั่ง client

- สามารถกำหนดประเภทของเว็บไซต์ที่ต้องการป้องกันได้ โดยเลือกจาก 4 ประเภทซึ่งประกอบด้วย ลามก อนาจาร รุนแรง การพนัน และลัทธินอกรีต ซึ่งประเภทของเว็บไซต์ที่ต้องการป้องกันสามารถเปลี่ยนแปลงได้ โดยต้องใส่ username และ password ให้ตรงกับที่ได้กรอกข้อมูลในการเรียกใช้โปรแกรมในครั้งแรก
- สามารถทำการตรวจสอบ request จากเว็บเบราเซอร์ได้ ซึ่งหากเป็นเว็บไซต์ที่ไม่เหมาะสมแล้ว จะทำการแสดงหน้าเว็บแจ้งเตือนแก่ผู้ใช้ว่าผู้ใช้ได้เข้าเว็บไซต์ที่ไม่เหมาะสม
- สามารถทำการ update version ไฟล์รายชื่อเว็บไซต์ที่ไม่เหมาะสมได้ โดยจะทำการ update ไฟล์รายชื่อเว็บไซต์ที่ไม่เหมาะสมแบบอัตโนมัติทุกๆ 1 เดือน

5.1.2 ทางฝั่ง server

- สามารถให้บริการ update ไฟล์รายชื่อเว็บไซต์ที่ไม่เหมาะสม โดยส่งไฟล์ version ใหม่ไปให้แก่ โปรแกรมที่ทำการ request มาทุก ๆ 1 เดือน
- สามารถกำหนด username และ password ได้โดยป้องกันการเข้าถึงแก่บุคคลภายนอก และสามารถเปลี่ยน password ใหม่ได้
- สามารถทำการเพิ่มและลบรายชื่อเว็บไซต์ที่ไม่เหมาะสม และแก้ไขประเภทของรายชื่อเว็บไซต์ที่ไม่เหมาะสมจากเครื่องคอมพิวเตอร์ที่ไหนก็ได้

5.2 ข้อเสนอแนะ

- หากไม่ได้ config properties เกี่ยวกับ connections ในเว็บเบราเซอร์ โปรแกรมจะไม่สามารถทำงานได้ ดังนั้นหากเป็นโปรแกรมที่ไม่ต้องมีการ config properties แล้วสามารถตรวจสอบ request ได้ จะเป็นโปรแกรมที่มีความสะดวกในการใช้งานมากขึ้น
- ควรมีการเข้ารหัสไฟล์รายชื่อเว็บไซต์ที่ไม่เหมาะสม เพื่อป้องกันบุคคลอื่นเปลี่ยนแปลงข้อมูลในไฟล์

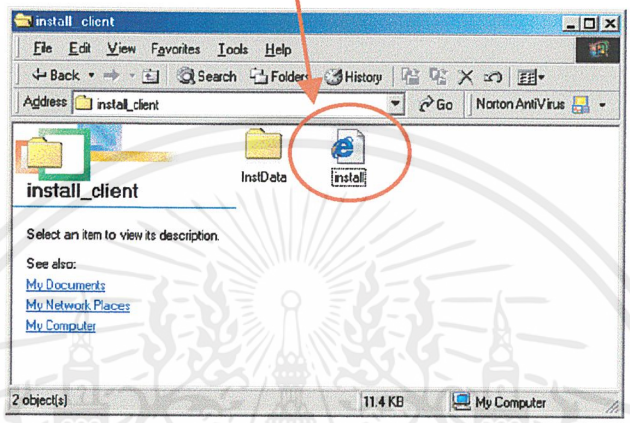
- การทำงานของโปรแกรมยังไม่ยืดหยุ่นในการกำหนดค่าต่างๆในโปรแกรมที่ทำการตรวจสอบการร้องขอ ดังนั้นควรจะทำเป็น icon ใน taskbar เพื่อทำการกำหนดค่าต่างๆได้สะดวกยิ่งขึ้น
- การเก็บรายการเว็บเพจที่ไม่เหมาะสมในรูปแบบไฟล์ นั้นทำให้การค้นหาข้อมูลนั้นต้องใช้เวลามาก ดังนั้นควรทำเป็นการเก็บข้อมูลที่ลดเวลาในการค้นหา โดยอาจจะทำเป็น Database
- การสืบค้นว่าเว็บไซต์ใดควรจะเป็นเว็บไซต์ที่ป้องกันนั้นทำได้ยาก ดังนั้นควรมี Function ช่วยAdministrator Server ในการสืบค้นเพื่อลดปริมาณเว็บไซต์ที่ Administrator Server ต้องตรวจสอบ
- Java Runtime นั้นมีการทำงานที่ช้าทำให้โปรแกรมนั้นช้าไปด้วย ดังนั้นอาจจะเปลี่ยนไปใช้การทำงานอื่นแทน

ภาคผนวก

ภาคผนวก ก.
การติดตั้งโปรแกรม

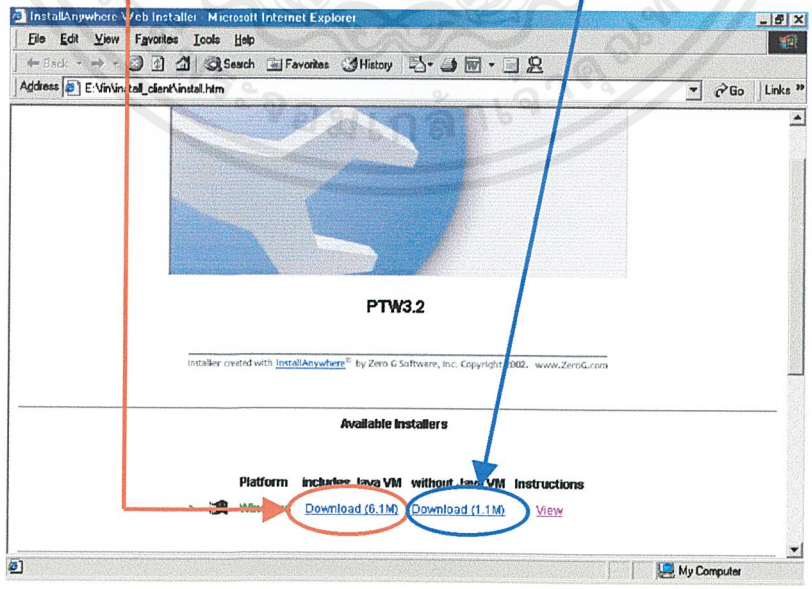
การติดตั้งโปรแกรมจะแบ่งออกเป็น 2 ส่วน

1. **โปรแกรมทางฝั่ง Client** ซึ่งเป็นส่วนที่ทำการกำหนดประเภทของเว็บไซต์ที่ไม่เหมาะสม ในการติดตั้งโปรแกรมให้ Run install.htm ใน Folder install_client ดังรูปที่ ก-1



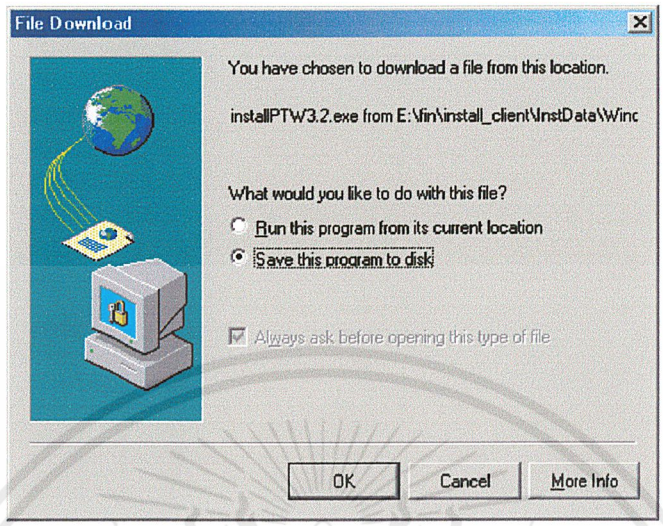
รูปที่ ก-1 แสดงการ Run install.htm

เมื่อ Run install.htm แล้วจะแสดง Web page ให้ download โปรแกรม PTW3.2 โดยถ้าเครื่องที่ต้องการลงโปรแกรมมี Java VM อยู่แล้วให้เลือก Download (1.1M) แต่ถ้าเครื่องไม่มี Java VM ให้เลือก Download (6.1M)ดังรูปที่ ก-2



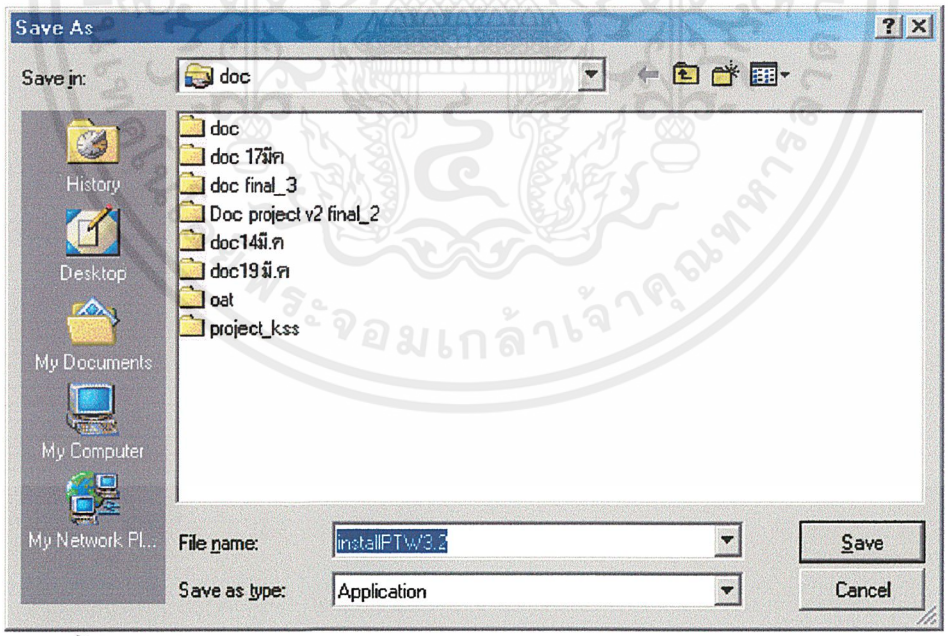
รูปที่ ก-2 หน้าจอการ Download Program PTW3.2

เมื่อเลือกแล้วจะแสดงหน้าจอ File Download ดังรูปที่ ก-3 ให้เลือก Save this Program to disk เพื่อทำการ Save File installPTW3.2.exe แล้วกดปุ่ม OK



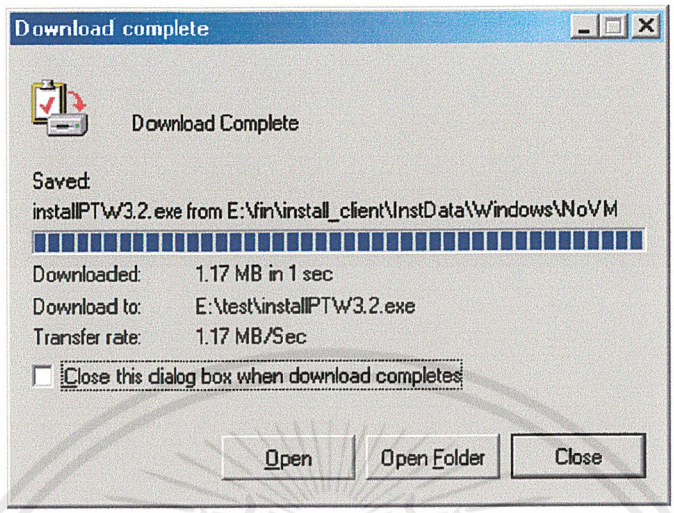
รูปที่ ก-3 หน้าจอ File Download

หลังจากกดปุ่ม OK แล้วโปรแกรมจะแสดงหน้าจอ Save As เพื่อให้เลือกตำแหน่งที่จะ Save File installPTW3.2 เมื่อเลือกแล้วให้ กดปุ่ม Save ดังรูปที่ ก-4



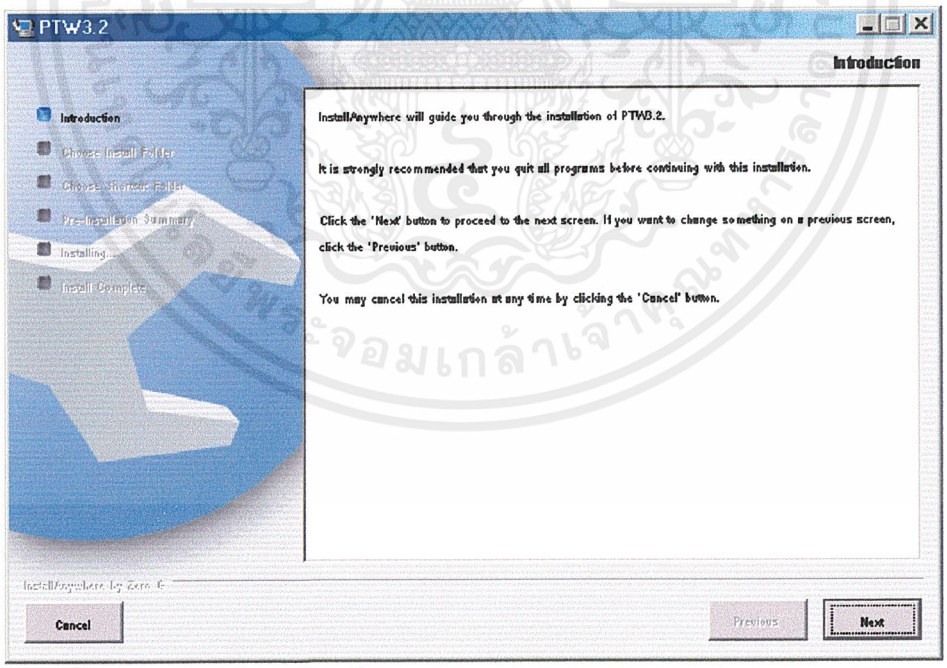
รูปที่ ก-4 หน้าจอ Save As

เมื่อกดปุ่ม Save As โปรแกรมจะทำการ Save File installPTW3.2 แล้วแสดงหน้าจอ Downloa complete ดังรูปที่ ก-4 ให้เลือก Open เพื่อ Run InstallPTW3.2



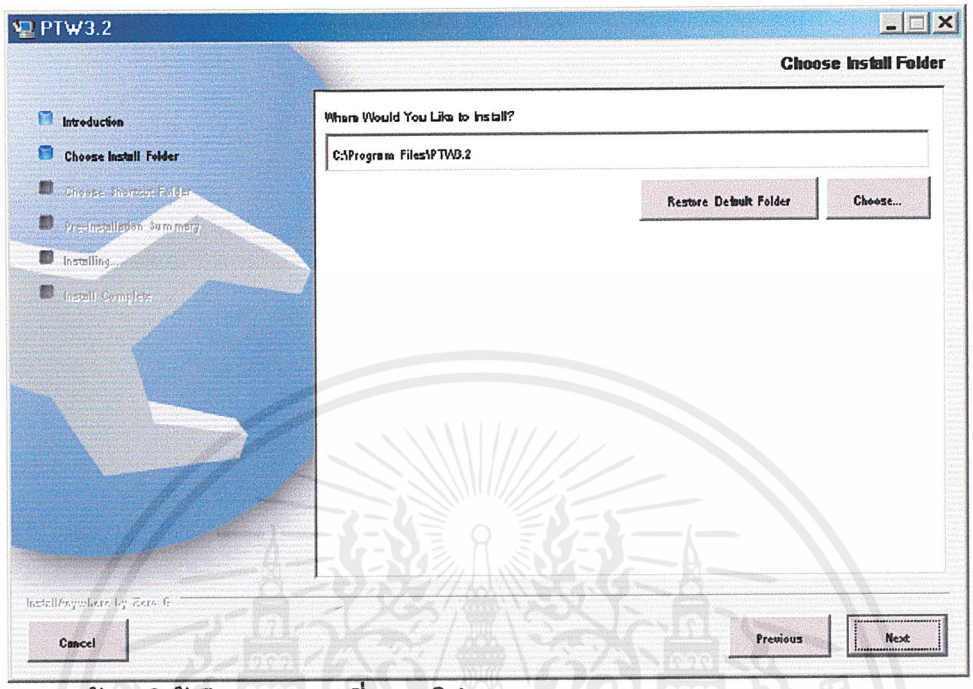
รูปที่ ก-4 หน้าจอ Download complete

เมื่อกดปุ่ม Open โปรแกรมจะทำการแสดงรายละเอียดของ โปรแกรม PTW3.2 ดังรูปที่ ก-5 จากนั้นให้กดปุ่ม Next



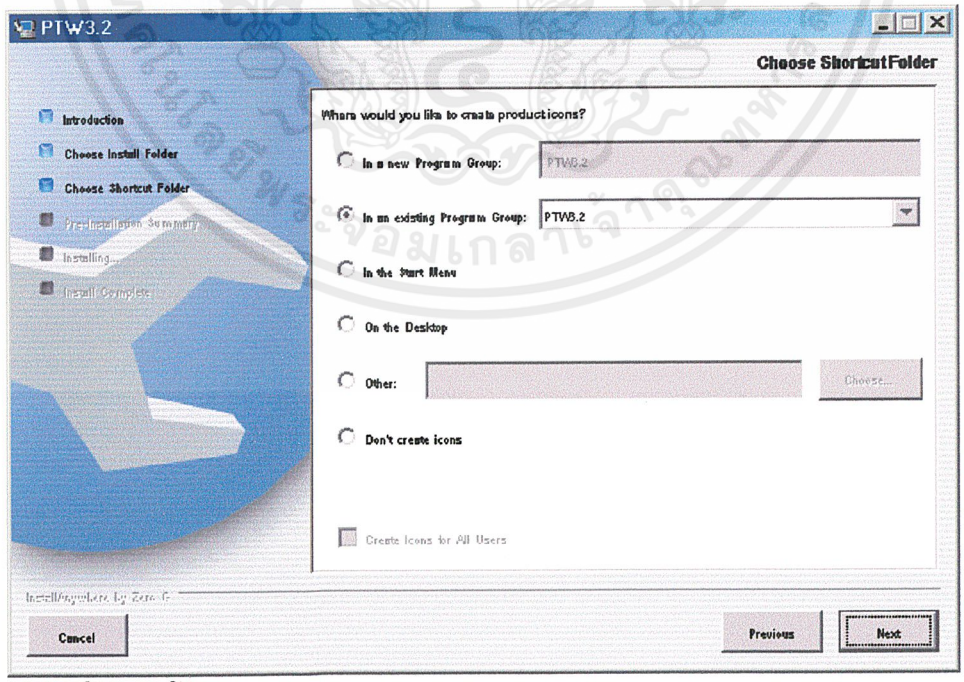
รูปที่ ก-5 หน้าจอแสดงรายละเอียดโปรแกรม PTW3.2

หลังจากกดปุ่ม Next แล้วโปรแกรมจะทำการแสดงหน้าจอให้เลือก Folder ที่จะลงโปรแกรม PTW3.2 ดังรูปที่ ก-6 แล้วให้กดปุ่มNext



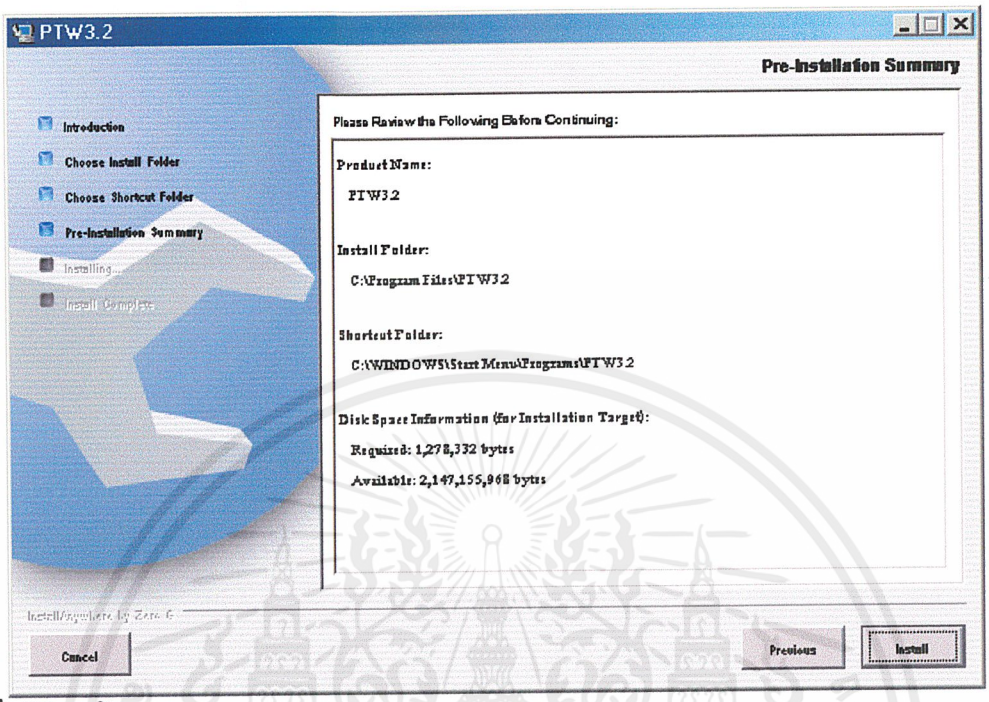
รูปที่ ก-6 หน้าจอให้เลือก Folder ที่จะลงโปรแกรม PTW3.2

หลังจากกดปุ่ม Next แล้วโปรแกรม แสดงตำแหน่งที่จะลง Shortcut ดังรูปที่ ก-7



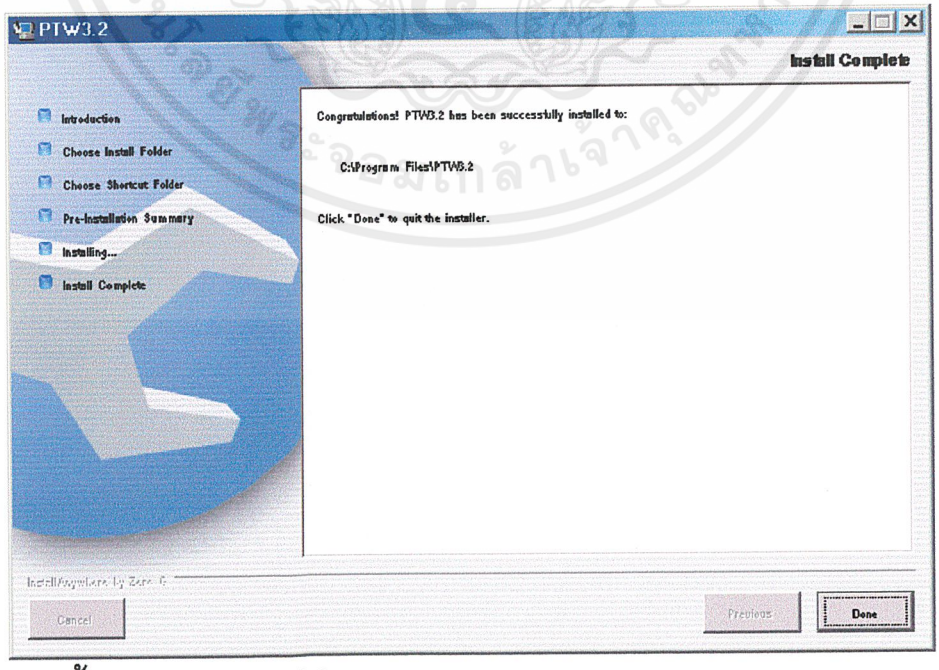
รูปที่ ก-7 หน้าจอให้เลือกการลง Shortcut

หลังจากกดปุ่ม Next แล้วโปรแกรมจะแสดงสรุปค่าที่เลือกไว้ ดังรูปที่ ก-8 แล้วกดปุ่ม Install



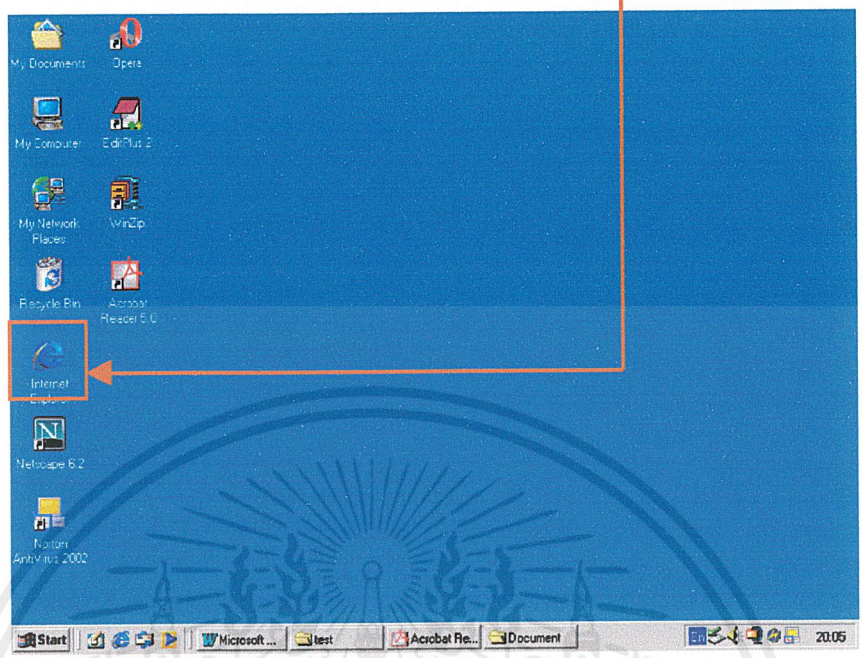
รูปที่ ก-8 หน้าจอแสดงสรุปค่าการ Install

เมื่อกดปุ่ม Next แล้ว โปรแกรมจะทำการ Install แล้วจะแสดงหน้าจอ Install Complete ดังรูปที่ ก-9



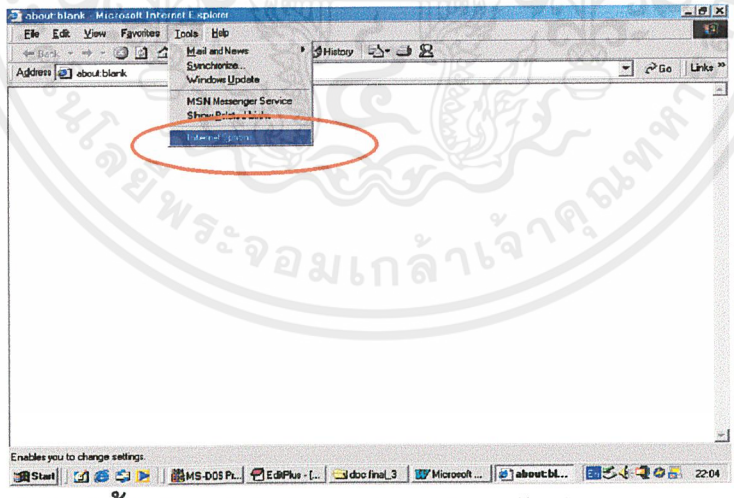
รูปที่ ก-9 หน้าจอ Install Complete

หลังจากลงโปรแกรม PTW3.2 เสร็จให้เรียกโปรแกรม Internet Explorer ดังรูปที่ ก-10



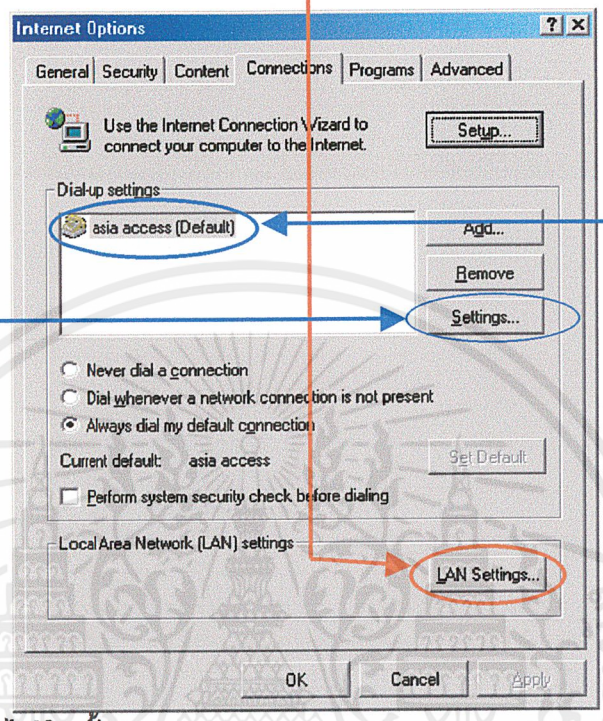
รูปที่ ก-10 แสดงการเรียก Internet Explorer

หลังจากเข้าโปรแกรม Internet Explorer แล้วให้เลือก หัวข้อ Internet Options ในหัวข้อ Tools ใน Tools Bar ดังรูปที่ ก-11



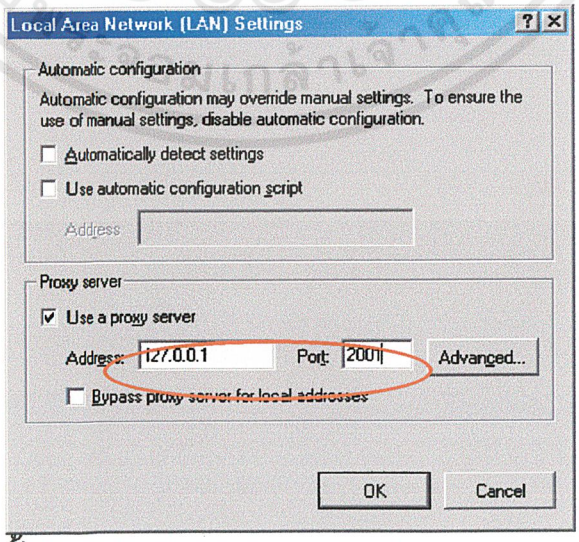
รูปที่ ก-11 แสดงการเข้า Internet Options ของ Internet Explorer

ถ้าเครื่องใช้ในระบบ LAN ให้เลือก LAN Settings... ในหัวข้อ Connections ดังรูปที่ ก-12 แต่ถ้าถ้าเครื่องคอมพิวเตอร์ใช้ระบบ modem ในการเชื่อมต่อ ให้เลือก Dial-up Package ที่ต้องการ แล้วกด Settings...



รูปที่ ก-11 แสดงการเข้าไปติดตั้ง IE

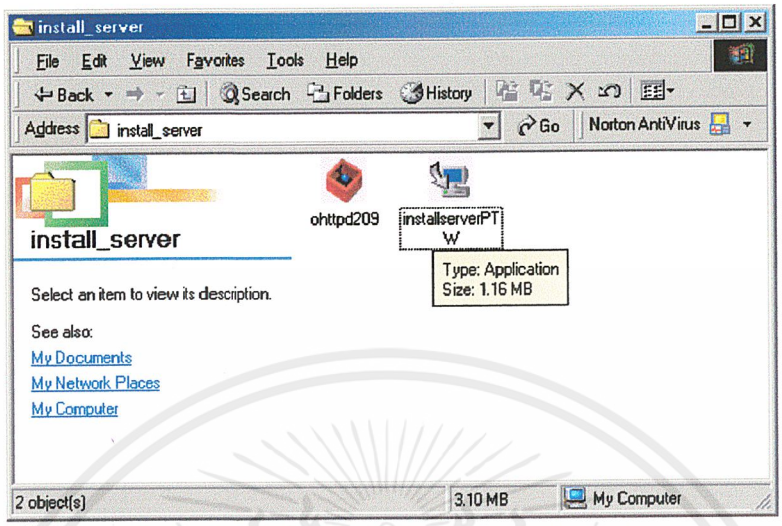
ทำการกำหนดหมายเลข address ให้เป็น 127.0.0.1 และ Port 2001 ในหัวข้อ Proxy server ดังรูปที่ ก-12



รูปที่ ก-12 แสดงการติดตั้ง หมายเลข address และ port

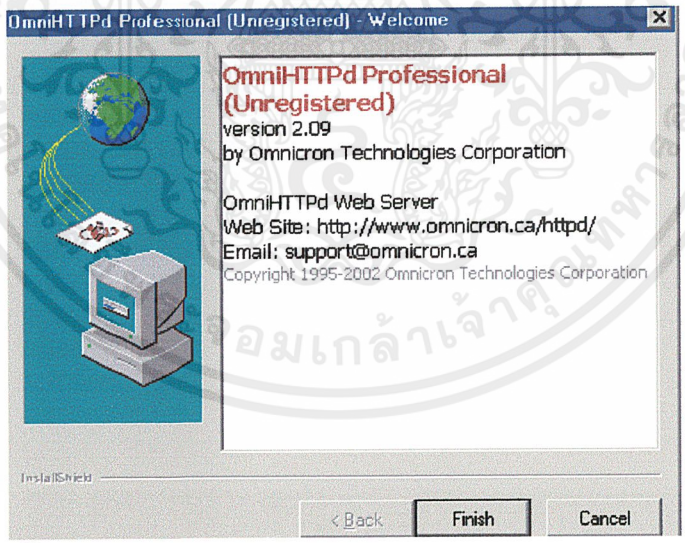
2. **โปรแกรมทางฝั่ง Server** เป็นส่วนที่ install Web server

ให้ Run file ohttpd209.exe ใน Folder ดังรูปที่ ก-13



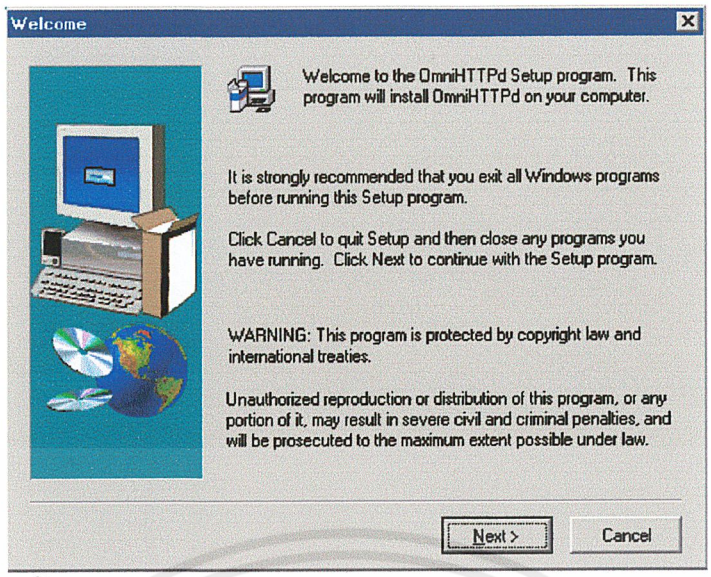
รูปที่ ก-13 แสดงการเรียก ohttpd209

เมื่อทำการ double click ที่ file ohttpd209.exe ก็จะแสดงหน้าจอบอกรายละเอียดเกี่ยวกับ OmniHTTPd Web Server และ Email ดังรูปที่ ก-14 ให้คลิกที่ Finish



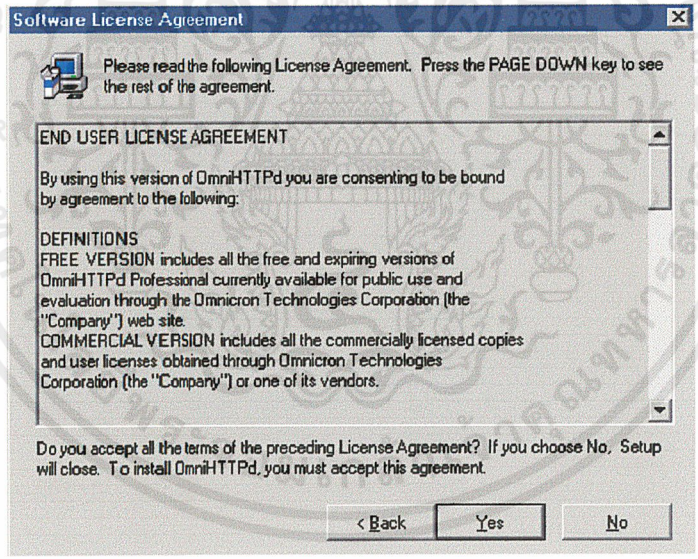
รูปที่ ก-14 เป็นหน้าจอ OmniHTTPd Professional

เมื่อทำการคลิก Finish ที่หน้าจอ OmniHTTPd Professional ก็จะเข้าสู่การติดตั้งให้คลิกNext ดังรูปที่ ก-15



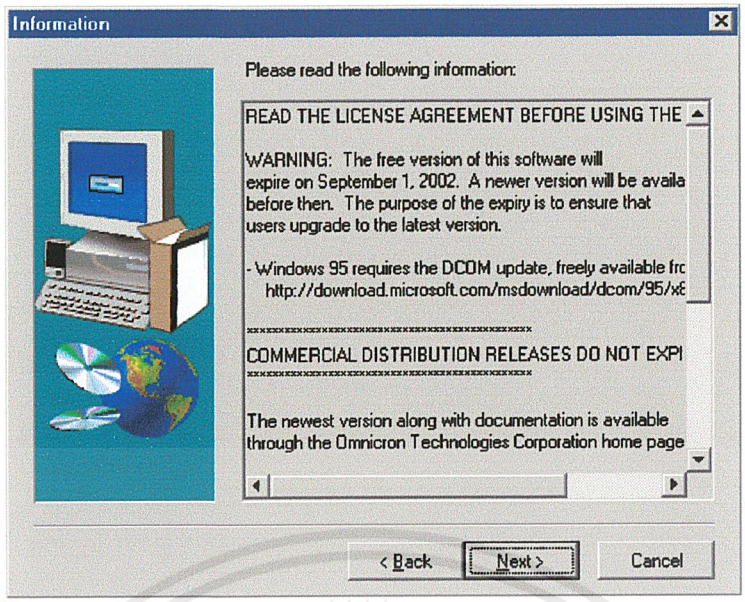
รูปที่ ก-15 เป็นหน้าจอ Welcome

เมื่อคลิก Next ที่หน้าจอ Welcome ก็จะเข้าสู่หน้าจอ Software License Agreement เพื่อให้เรายอมรับ ดังรูปที่ ก-16



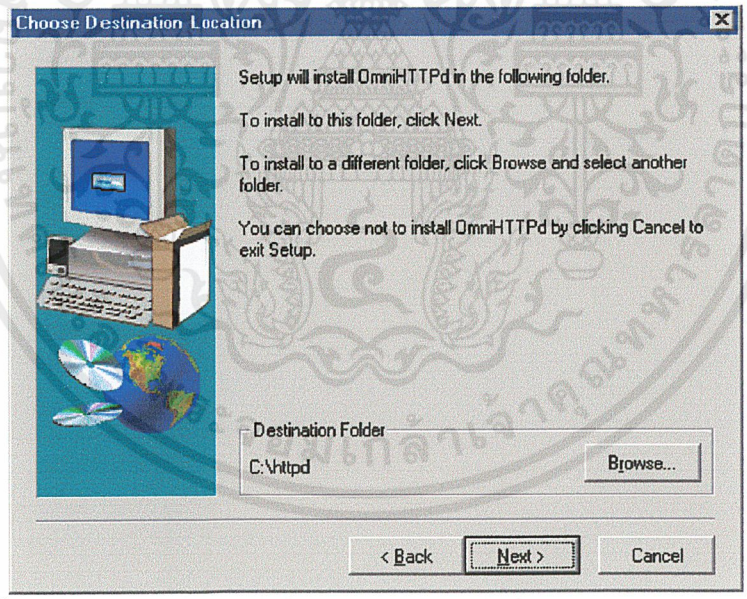
รูปที่ ก-16 หน้าจอ Software License Agreement

เมื่อคลิก yes หน้าจอ Software License Agreement ก็จะเข้าสู่หน้าจอ Information ดังรูปที่ ก-17



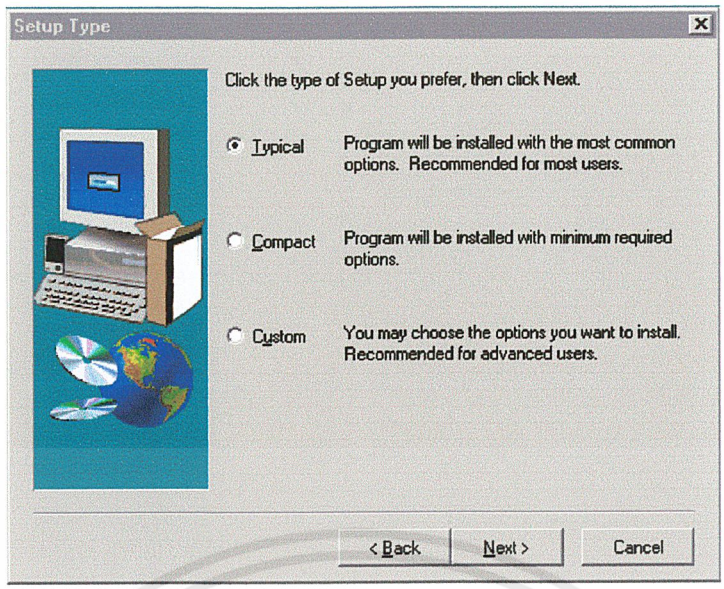
รูปที่ ก-17 หน้าจอ Information

เมื่อคลิก Nextหน้าจอ Information ก็จะเข้าสู่หน้าจอ Choose Destination Location ดังรูปที่ ก-18



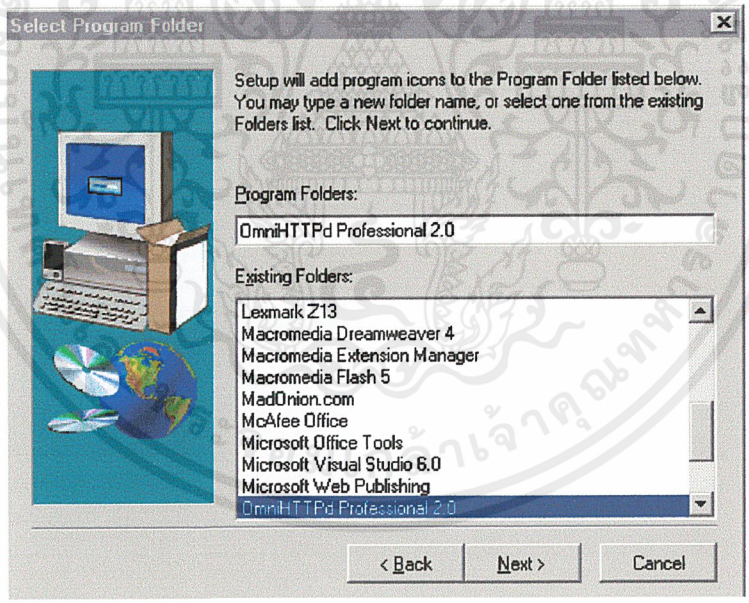
รูปที่ ก-18 หน้าจอ Choose Destination Location

เมื่อคลิก Nextหน้าจอ Choose Destination Location ก็จะเข้าสู่หน้าจอ Setup Type ดังรูปที่ ก-19



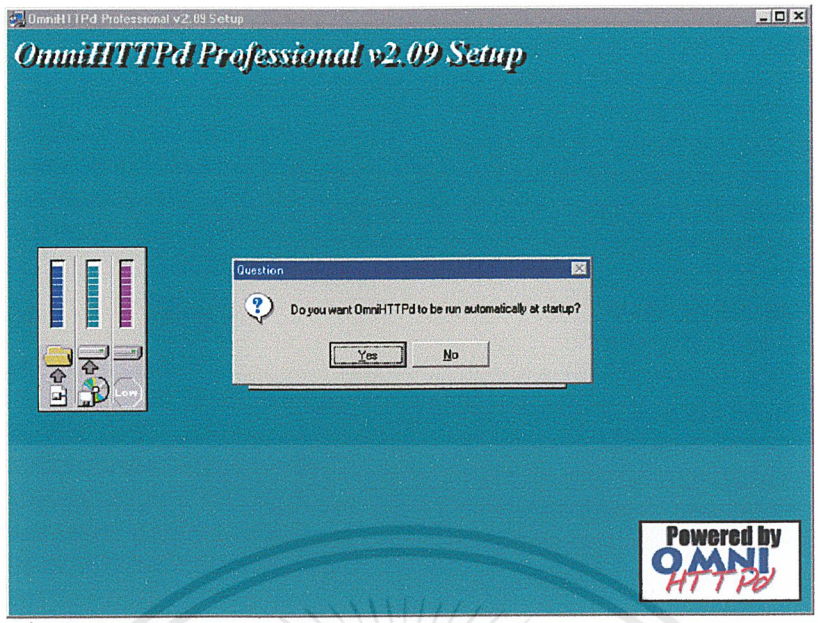
รูปที่ ก-19 หน้าจอ Setup Type

เมื่อเลือกและคลิก Next หน้าจอ Setup Type ก็จะเข้าสู่หน้าจอ Select Program Folder ดังรูปที่ ก-20



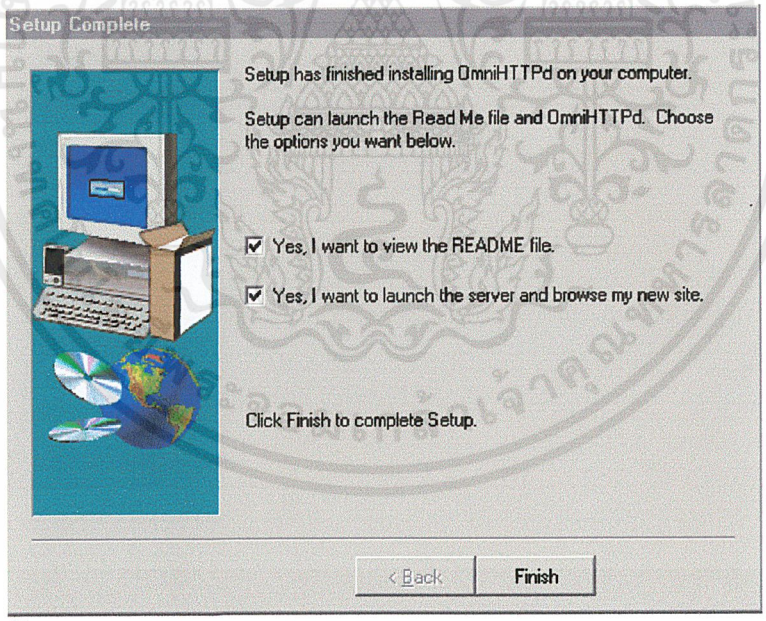
รูปที่ ก-20 หน้าจอ Select Program Folder

เมื่อคลิก Next ที่หน้าจอ Select Program Folder ก็จะเข้าสู่หน้าจอ การติดตั้งและทำการถามว่าต้องการ Run โปรแกรม OmniHTTd ทุกครั้งที่เปิดเครื่องหรือไม่ให้เลือก Yes ดังรูปที่ ก-21



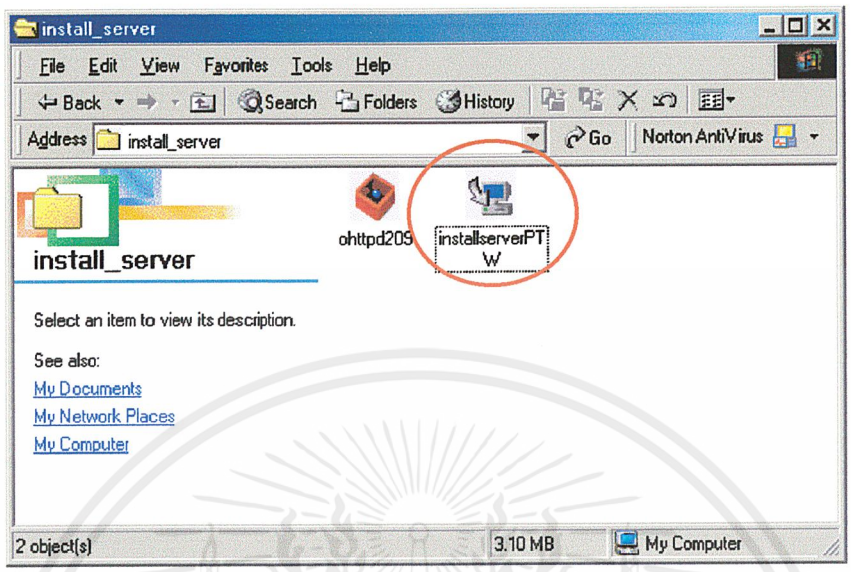
รูปที่ ก-21 หน้าจอQuestion

เมื่อกดปุ่ม Yes ที่ Question ก็จะเข้าสู่หน้าจอ Setup Complete ดังรูปที่ ก-22 เมื่อกดปุ่ม Finish เป็นอันว่าการsetup โปรแกรม OmniHTTPd เสร็จสมบูรณ์



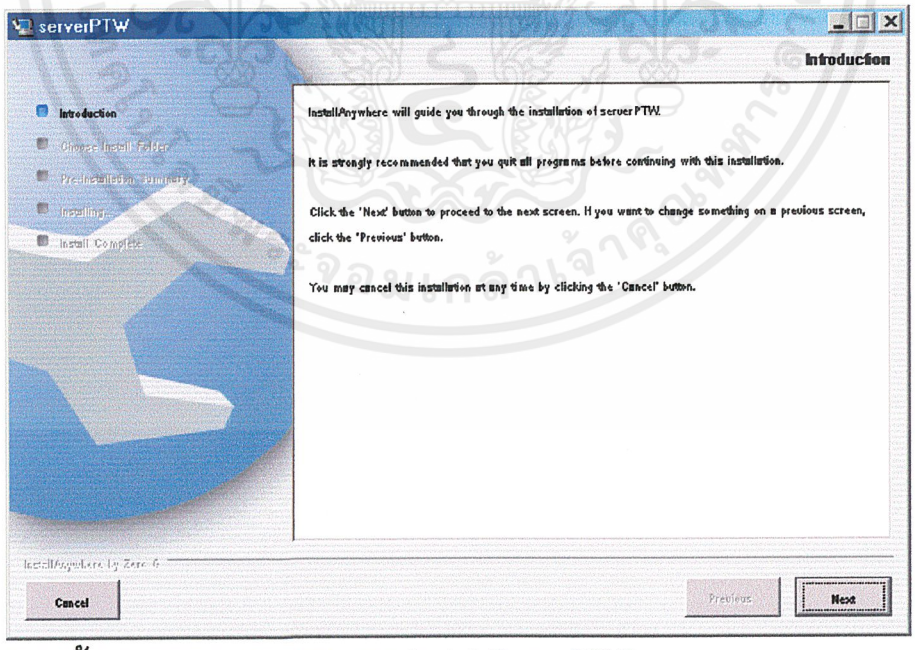
รูปที่ ก-22 หน้าจอ Setup Complete

เมื่อลงโปรแกรม OmniHTTPd เสร็จให้เลือก installserverPTW ใน Folder install_server เพื่อทำการลง Web Protection Toad Websites ดังรูปที่ ก-23



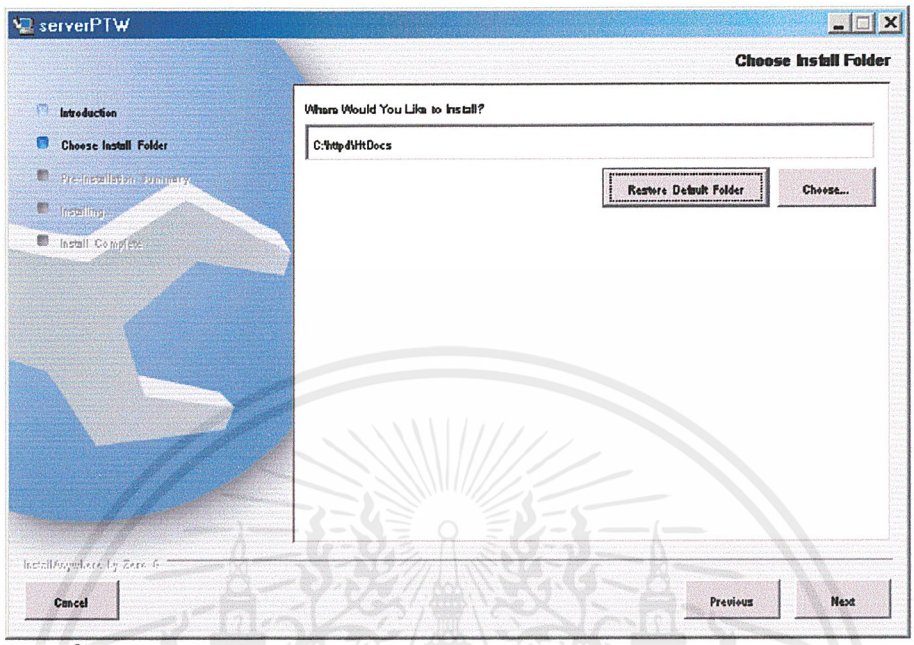
รูปที่ ก-23 แสดงการเรียก installserverPTW

หลังจากนั้นโปรแกรมจะทำการแสดงหน้าจอ แสดงละเอียดโปรแกรม ดังรูปที่ ก-24 แล้วให้กด Next



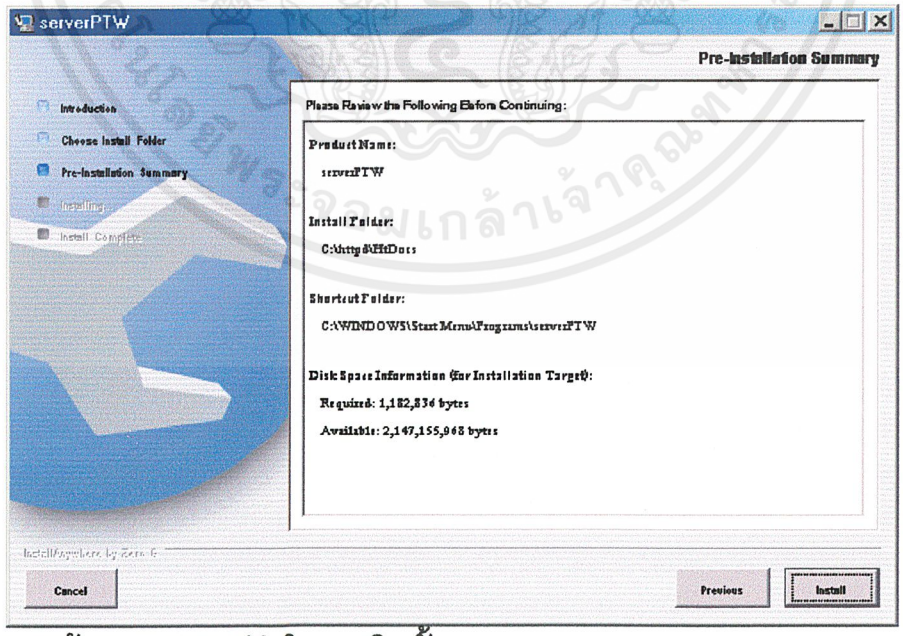
รูปที่ ก-24 หน้าจอ Introduction ของการ Install ServerPTW

หลังจากนั้นโปรแกรมจะแสดงหน้าจอให้เลือก Folder ที่จะ Install ให้เลือกไปยัง Folder ที่ต้องการสร้างเป็น Web Protection Toad Websites ดังรูปที่ ก-25



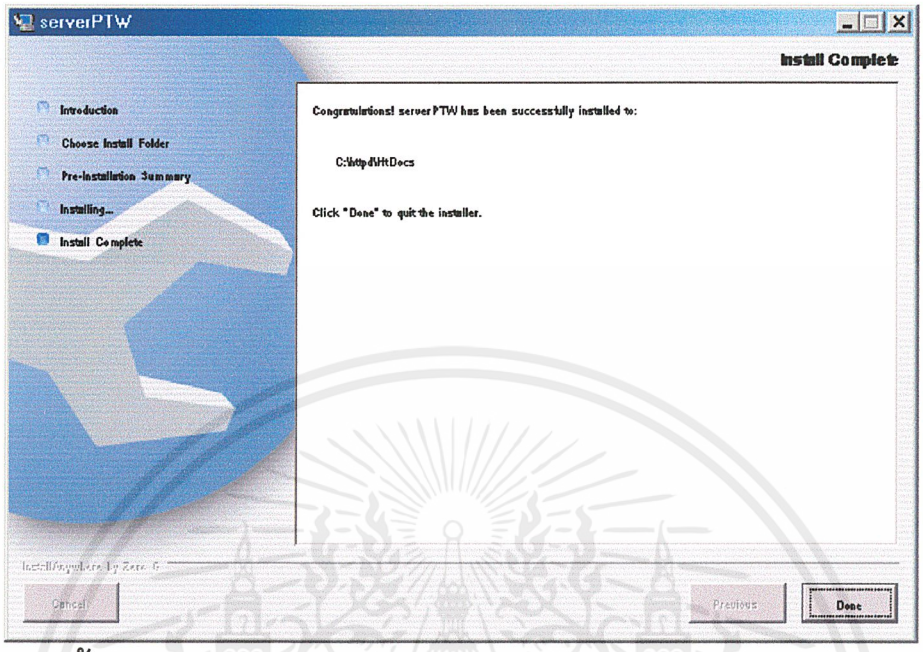
รูปที่ ก-25 หน้าจอ Choose Install Folder ของการ Install serverPTW

หลังจากนั้นโปรแกรมจะแสดงสรุปค่าที่ได้กำหนดมาตั้งแต่ต้นในการ Install ครั้งนี้ ดังรูปที่ ก-26 แล้วให้กดปุ่ม Install



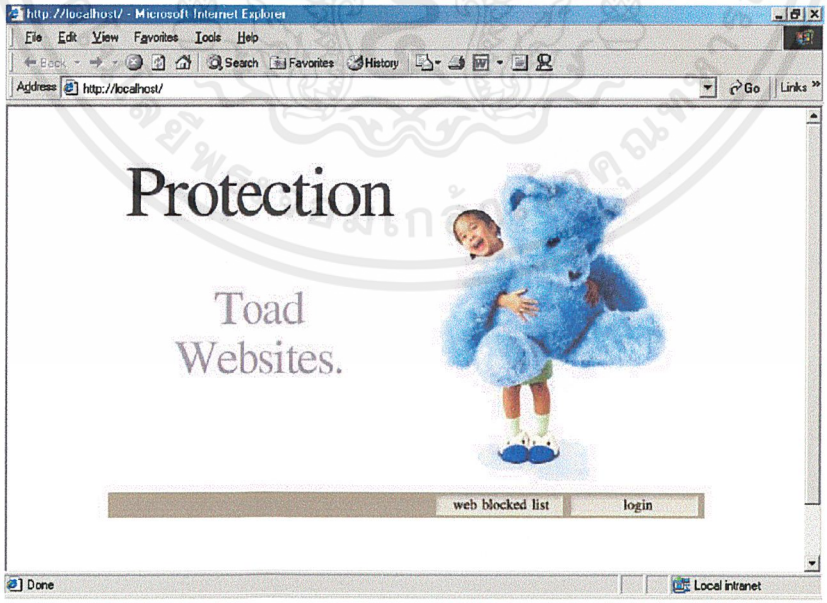
รูปที่ ก-26 หน้าจอแสดงสรุปค่าในการติดตั้ง

เมื่อกดปุ่ม Install โปรแกรมจะทำการติดตั้งโปรแกรม เมื่อติดตั้งเสร็จโปรแกรมจะแสดงหน้าจอ ว่าติดตั้งเสร็จสิ้นแล้ว ดังรูปที่ ก-27



รูปที่ ก-27 หน้าจอ Install Complete ของการ Install serverPTW

จะทำการเรียกโปรแกรมโดยใช้ Web browser เรียก Http://161.246.60.10 แล้วจะแสดงหน้าเว็บเพจดังรูป ก-28



รูปที่ ก-28 Home page ของ Protection Toad Websites.