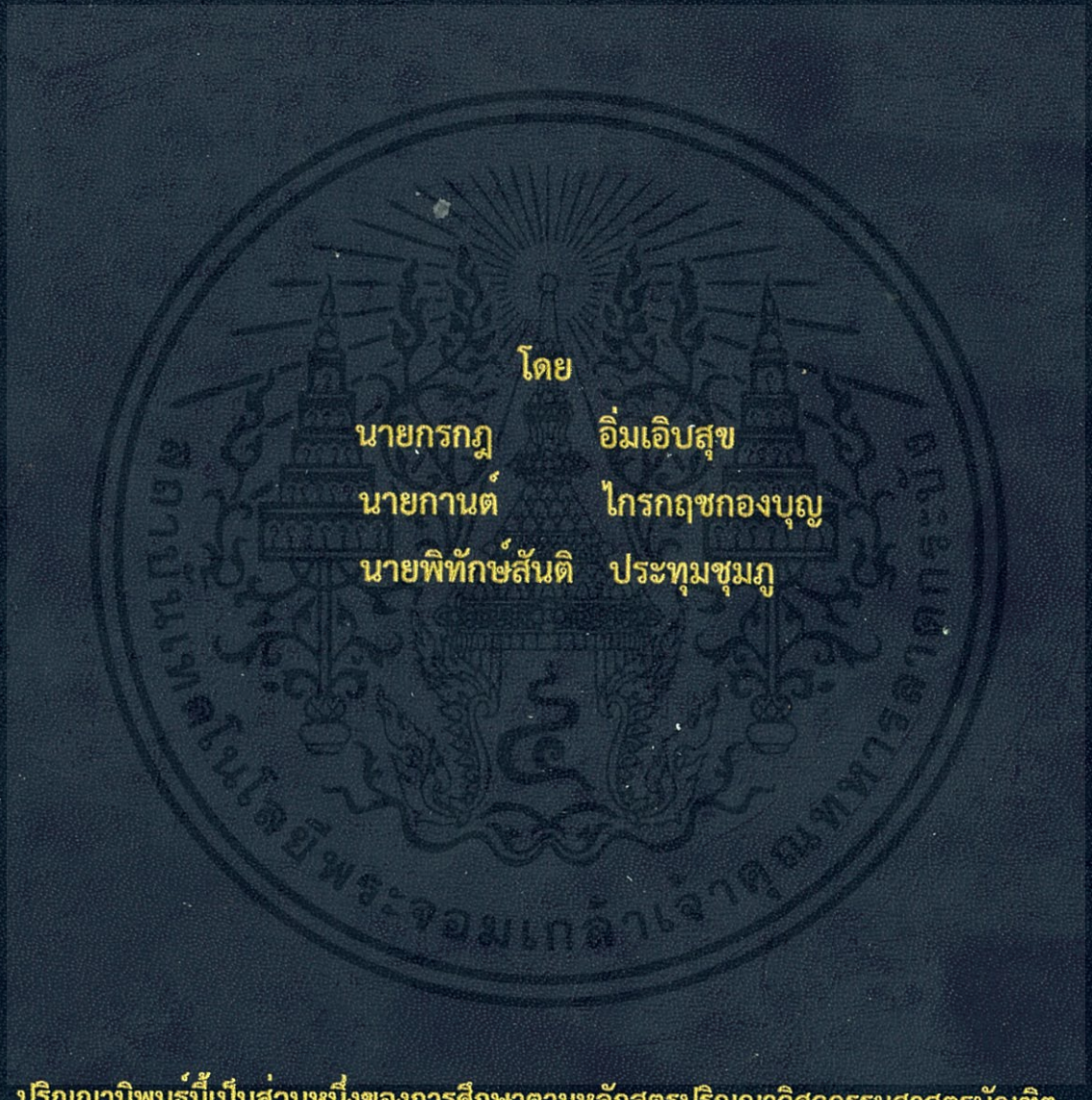
ระบบบริหารจัดการในการเข้าถึงข้อมูลอินเตอร์เน็ต

INTERNET ACCESS MANAGEMENT



โดย

นายกรกฎ อิ่มเอิบสุข

นายกานต์ ไกรกฤชกองบุญ

นายพิทักษ์สันติ ประทุมชุมภู

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2557

ระบบบริหารจัดการในการเข้าถึงข้อมูลอินเตอร์เน็ต
Internet Access Management

โดย

นายกรกฎ	อิ่มเอิบสุข	54010019
นายกานต์	ไกรกฤชกองบุญ	54010096
นายพิทักษ์สันติ	ประทุมชุมภู	54010921

อาจารย์ที่ปรึกษา

รศ.ดร. สุวิพล สิทธิชีวภาค

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2557

ปริญญานิพนธ์ปีการศึกษา 2557
ภาควิชาวิศวกรรมโทรคมนาคม
คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
เรื่อง ระบบบริหารจัดการในการเข้าถึงข้อมูลอินเตอร์เน็ต
INTERNET ACCESS MANAGEMENT

ผู้จัดทำ

1.	นายกรกฎ	อิ่มเอิบสุข	54010019
2.	นายกานต์	ไกรกฤชกองบุญ	54010096
3.	นายพิทักษ์สันติ	ประทุมชุมภู	54010921

..... **อาจารย์ที่ปรึกษา**
(รศ.ดร. สุวิพส สิทธิชีวภาค)

กิตติกรรมประกาศ

โครงงานนี้สำเร็จลุล่วงไปด้วยดีด้วยคำแนะนำที่มีประโยชน์และมีคุณค่าพร้อมทั้งการให้คำปรึกษาที่ดียิ่งโดยเฉพาะ รศ.ดร.สุวิพล สิทธิชีวภาค อาจารย์ที่ปรึกษาโครงงานที่ให้การสนับสนุนช่วยเหลือในด้านเครื่องมือ ค่าใช้จ่ายเพิ่มเติมและอุปกรณ์ต่างๆเป็นอย่างดีมาโดยตลอด ขอขอบคุณสำนักบริการคอมพิวเตอร์โดยเฉพาะอย่างยิ่ง คุณกฤษฎิ์ธนิก ศรีธนสาร สำหรับคำแนะนำ แง่คิดและคาปรึกษาในเรื่องต่างๆ จนสามารถแก้ไขปัญหาได้อย่างสำเร็จลุล่วงเรื่อยมาตลอดจนเพื่อนในห้องโปรเจค T 304 ที่คอยให้คำปรึกษาอย่างเป็นกันเอง ทำให้โครงงานสำเร็จตามที่คาดหวัง

ทั้งนี้ขอขอบพระคุณคณาจารย์ที่ปรึกษาโครงงานและคณาจารย์ท่านอื่นที่ได้สละเวลาอันมีค่ามาให้คำแนะนำและคำปรึกษาแก่กลุ่มของข้าพเจ้า ตลอดจนเพื่อนๆ พี่ๆทุกคนผู้ซึ่งได้ให้ความรู้ รวมทั้งบิดา มารดา ที่ได้อบรม เลี้ยงดูและให้กำลังใจแก่ข้าพเจ้าเป็นอย่างดี จนทำให้คณะผู้จัดทำมีคุณภาพชีวิตที่ดีมาจนถึงทุกวันนี้

นายกรกฎ อิ่มเอิบสุข
นายกานต์ ไกรกฤชกองบุญ
นายพิทักษ์สันติ ประทุมชุมภู
ผู้จัดทำ

ระบบบริหารจัดการในการเข้าถึงข้อมูลอินเตอร์เน็ต
INTERNET ACCESS MANAGEMENT

โดย นายกรกฎ อิ่มเอิบสุข 54010019
นายกานต์ ไกรกฤชกองบุญ 54010096
นายพิทักษ์สันติ ประทุมชุมภู 54010921

อาจารย์ที่ปรึกษา รศ.ดร. สุวิพล สิทธิชีวภาค

บทคัดย่อ

โครงงานนี้เป็นการสร้างระบบบริหารจัดการในการเข้าถึงข้อมูลอินเตอร์เน็ตโดยมีฟังก์ชั่น (Function) ที่ใช้ควบคุมการทำงานซึ่งประกอบด้วยฟังก์ชั่น Multiple–Gateways ฟังก์ชั่น Authentication System ฟังก์ชั่น Web–Caching (Proxy) ฟังก์ชั่น Network Security (Firewall) และฟังก์ชั่น Graphical User Interface Management ในการบริหารจัดการเพื่อควบคุมและจำกัดการเข้าถึงข้อมูลอินเตอร์เน็ตของผู้ใช้บริการ ตรวจสอบสิทธิ์ในการใช้งานของผู้ใช้บริการ ดูแลรักษาความปลอดภัยเครือข่ายและข้อมูลของผู้ใช้บริการ ตรวจสอบสถานะของระบบสำหรับบริหารจัดการระบบโดยนำฟังก์ชั่นดังกล่าวมาทำการโปรแกรมไปยังอุปกรณ์ Hardware เพื่อทำหน้าที่เป็น เซิร์ฟเวอร์(Server)ในการให้บริการและจัดการในการเข้าถึงข้อมูลอินเตอร์เน็ตของผู้ใช้งาน

ABSTRACT

The creation of management system is studied in this project. Many Function are used in control system such as Function Multiple–Gateways, Function Authentication System, Function Web-Caching (Proxy), Function Network Security (Firewall) and Function Graphical User Interface Management. The functions are programmed into the hardware to perform as a server in providing data access and management of Internet applications.

สารบัญ

		หน้า
กิตติกรรมประกาศ		I
บทคัดย่อ		II
สารบัญ		III
สารบัญรูป		VI
สารบัญตาราง		VIII
บทที่ 1	**บทนำ**	1
	1.1 ความเป็นมาและความสำคัญของปัญหา	1
	1.2 วัตถุประสงค์	1
	1.3 ขอบเขตของโครงงาน	1
บทที่ 2	**ทฤษฎีและหลักการที่เกี่ยวข้อง**	2
	2.1 อินเตอร์เน็ต (INTERNET)	2
	2.1.1 หน้าที่และความสำคัญของอินเตอร์เน็ต	2
	2.2 เครือข่าย (NETWORK)	2
	2.2.1 ประเภทของเครือข่าย	3
	2.2.1.1 เครือข่ายส่วนบุคคล (PERSONAL AREA NETWORK : PAN)	3
	2.2.1.2 เครือข่ายภายใน (LOCAL AREA NETWORK : LAN)	3
	2.2.1.3 เครือข่ายระดับเมือง (METROPOLITAN AREA NETWORK : MAN)	4
	2.2.1.4 เครือขายระยะไกล (WIDE AREA NETWORK:WAN)	5
	2.2.2 รูปแบบการเชื่อมต่อของระบบเครือข่าย	5
	2.2.2.1 โครงข่ายแบบเส้นตรง (BUS TOPOLOGY)	5
	2.2.2.2 โครงข่ายแบบดาว (STAR TOPOLOGY)	6

สารบัญ (ต่อ)

	หน้า
2.2.2.3 โครงข่ายแบบวงแหวง (RING TOPOLOGY)	6
2.2.2.4 โครงข่ายแบบต้นไม้ (TREE TOPOLOGY)	7
2.2.2.5 โครงข่ายแบบเมช (MESH TOPOLOGY)	7
2.2.2.6 โครงข่ายแบบไฮบริด (HYBRID TOPOLOGY)	8
2.3 LINUX OPERATING SYSTEM	9
2.4 ภาษา PHP	10
2.5 TCP/IP	10
2.6 ROUTING PROTOCOL	11
2.7 WEB CACHING	11
2.7.1 ประเภทของ WEB-CACHE	12
2.7.1.1 BROWSER CACHE	12
2.7.1.2 PROXY CACHE	13
2.7.2 DNS (DOMAIN NAME SERVICE)	13
2.8 AUTHENTICATION	14
2.9 FIREWALL	15
2.9.1 การป้องกันการเข้าถึงระบบ	16
2.9.2 คุณสมบัติของ FIREWALL	16
2.9.3 ประเภทของ FIREWALL	17
2.9.4 ขีดความสามารถของ FIREWALL	18
2.9.5 ข้อจำกัดFIREWALL	18
2.10 GRAPHICAL USER INTERFACE	19
2.11 การสร้างฟอร์มHTML	20

สารบัญ (ต่อ)

		หน้า
	2.11.1 การออกแบบฟอร์มให้มีลักษณะต่าง ๆ	20
	2.11.1.1 รูปแบบการสร้าง FORM	20
	2.11.2. ตัวอย่างการสร้าง FORM แบบต่าง ๆ	21
	2.11.2.1 การสร้างที่ใส่ชื่อ	21
	2.11.2.2 การสร้าง PASSWORD	21
	2.11.2.3 แปลความหมาย	21
	2.11.2.4 การสร้างปุ่ม BUTTON	21
	2.12 โหลดบาลานซ์ (LOAD BALANCE)	22
	2.12.1 โหลดบาลานซิ่ง (LOAD BALANCING)	22
	2.12.2 ระบบโหลดบาลานซ์ (LOAD BALANCE SYSTEM)	23
	2.12.3 วิธีการกระจายภาระงานของโหลดบาลานซ์ (LOAD BALANCE)	23
	2.12.3.1 แบบ ROUND ROBIN	23
	2.12.3..2 แบบ WEIGHTED ROUND ROBIN	23
	2.12.3.3 แบบ FAST RESPONSE	24
	2.12.3.4 แบบ LEAST CONNECTION	24
	2.12.3.5 แบบ POLICY ROUTING	25
	2.12.3.6 แบบ LINK BACKUP	25
บทที่ 3	**การออกแบบและการจัดทำปริญญานิพนธ์**	26
	3.1 การออกแบบ	26
	3.1.1 การแจก DHCP	28
	3.1.2 ฟังก์ชั่นตรวจสอบสิทธิ์ของผู้ใช้ (AUTHENTICATION)	28
	3.1.2.1 กระบวนการ MARK PACKET	28
	3.1.2.2 กระบวนการตรวจสอบสิทธิ์ของผู้ใช้ (AUTHENTICATION)	29

สารบัญ (ต่อ)

		หน้า
	3.1.3 ระบบกำหนดเวลาในการใช้งานอินเตอร์เน็ต	30
	3.1.4 ฟังก์ชั่นพรอกซี (PROXY)	30
	3.1.5 ฟังก์ชั่น MULTIPLE-GATEWAYS (GATEWAY BALANCER)	30
	3.1.6 การกำหนดเส้นทางผ่านเกตเวย์ (ACCESS GATEWAY)	32
	3.1.7 ฟังก์ชั่น NETWORK SECURITY	32
	3.1.8 ฟังก์ชัน GRAPHICAL USER INTERFACE (GUI)	35
	3.1.8.1ส่วนแสดงผล	35
	3.1.8.2 ส่วนควบคุม	35
	3.2 เครื่องมือที่ใช้ในการทดลอง	41
	3.2.1 HARDWARE	41
	3.2.2 SOFTWARE	41
	3.3 การจัดเก็บผลการทดลอง	42
	3.3.1 การออกแบบการทดลองของฟังก์ชัน AUTHENTICATION	42
	3.3.2 การออกแบบการทดลองของฟังก์ชัน WEB CACHING (PROXY)	43
	3.3.2.1 ทำการทดลอง TCP_MISS และ TCP_ HIT	43
	3.3.2.2 ทำการทดลองวัดเวลาในการเข้าถึงหน้าเว็บไซต์ที่ต้องการ	43
	3.3.3 การออกแบบการทดลองของฟังก์ชัน MULTIPLE-GATEWAYS	43
	3.3.4 การออกแบบการทดลองของฟังก์ชัน GRAPHICAL USER INTERFACE (GUI)	43
บทที่ 4	**ผลการทดลอง**	44
	4.1 การทดลองของฟังก์ชัน AUTHENTICATION	44
	4.1.1ทำการทดลองการสร้างแอคเคาท์ (ACCOUNT)	44
	4.1.2 ทำการทดลองการทำงานของฟังก์ชั่นการยืนยันตัวตน	47
	4.2 การทดลองของฟังก์ชัน WEB CACHING (PROXY)	52

สารบัญ (ต่อ)

		หน้า
	4.2.1ทำการทดลองหาTCP_MISS และTCP_HIT	52
	4.2.2ทำการทดลอง BLACK LIST DOMAIN	59
	4.3 การทดลองของฟังก์ชัน (MULTIPLE – GATEWAYS)	61
	4.3.1 การทดลองของฟังก์ชัน (MULTIPLE – GATEWAYS) แบบ WEIGHTED ROUND ROBIN	61
บทที่ 5	**สรุปผลและข้อเสนอแนะ**	
	5.1 สรุปผล	67
	5.2 ข้อเสนอแนะ	67
	บรรณานุกรม	68

สารบัญรูป

รูปที่		หน้า
2.1	เครือข่ายส่วนบุคคล (PAN)	3
2.2	เครือข่ายภายใน (LAN)	4
2.3	เครือข่ายระดับเมือง (MAN)	4
2.4	เครือข่ายระยะไกล (WAN)	5
2.5	โครงข่ายแบบเส้นตรง (BUS TOPOLOGY)	6
2.6	โครงข่ายแบบดาว (STAR TOPOLOGY)	6
2.7	โครงข่ายแบบวงแหวน (RING TOPOLOGY)	7
2.8	โครงข่ายแบบต้นไม้ (TREE TOPOLOGY)	7
2.9	โครงข่ายแบบเมช (MESH TOPOLOGY)	8
2.10	โครงข่ายแบบไฮบริด (HYBRID TOPOLOGY)	8
2.11	LINUX OPERATING SYSTEM	9
2.12	ROOT ของ DOMAIN NAME SYSTEM	14
2.13	หน้าต่าง AUTHENTICATION	15
2.14	การจำกัดการเข้าถึงเครือข่ายจากภายนอกโดย FIREWALL	16
2.15	ลักษณะของ NETWORK LEVEL FIREWALL	17
2.16	ลักษณะของ APPLICATION LAYER FIREWALL	18
2.17	ภาพส่วนของ FIREWALL	19
2.18	ตัวอย่าง ICONS ในโปรแกรม AUTOCAD	20
2.19	ส่วนของ USERNAME	21
2.20	ส่วนของ PASSWORD	22
2.21	ตัวอย่างการสร้างหน้าเว็ปด้วยภาษาHTML	22
3.1	บริการที่มีอยู่ในเซิร์ฟเวอร์ของระบบ	26
3.2	โฟลว์ชาร์ต (FLOWCHART) การทำงานของระบบโดยรวม	27
3.3	คำสั่งที่ใช้กำหนดจำนวนผู้ใช้ทั้งหมดที่สามารถใช้งานในเวลาเดียวกัน	28
3.4	คำสั่งสำหรับการทำเครื่องหมายให้กับแพ็กเก็ต	28

สารบัญรูป(ต่อ)

หน้า

รูปที่		
3.5	โฟลว์ชาร์ตกระบวนการตรวจสอบสิทธิ์ของผู้ใช้บริการ	29
3.6	คำสั่งกำหนดระยะเวลาในการล็อกอินเข้าใช้งานอินเตอร์เน็ตในหนึ่งครั้ง	30
3.7	คำสั่งในการแบ่งหน่วยความจำสำหรับเก็บอ็อบเจกต์ของเว็บไซต์	30
3.8	ช่องทางในการรับส่งข้อมูลของเซิร์ฟเวอร์	31
3.9	คำสั่งสำหรับการสุ่มทำเครื่องหมายให้กับแพ็กเก็ตเพื่อกระจายเส้นทาง	31
3.10	คำสั่งการกำหนดเส้นทางของแพ็กเก็ตที่ถูกทำเครื่องหมาย	32
3.11	คำสั่งกำหนดค่า WEIGHT ในการส่งแพ็กเก็ต	32
3.12	คำสั่งการกำหนดเส้นทางผ่านเกตเวย์	32
3.13	IP TABLE PACKET FLOW	34
3.14	คำสั่งในการกำหนดพอร์ตการใช้งาน	34
3.15	แผนภูมิค่าเปอร์เซ็นต์การใช้หน่วยความจำและหน่วยประมวลผล	36
3.16	แผนภูมิค่าความเร็วของข้อมูลที่ผ่านแต่ละอินเตอร์เฟส	36
3.17	แผนภูมิค่าเปอร์เซ็นต์การใช้โปรโตคอลและพอร์ตต่างๆ	36
3.18	แผนภูมิบอกจำนวนผู้ใช้ที่ได้ล็อกอินเข้าใช้งานอินเตอร์เน็ต	37
3.19	IP ADDRESS และ NETWORK MASK ของแต่ละอินเตอร์เฟส	37
3.20	LOGIN USERS ที่กำลังใช้งานอินเตอร์เน็ตผ่านบริการของระบบ	37
3.21	กราฟค่าความเร็วของข้อมูลที่ผ่านแต่ละอินเตอร์เฟสใน 60 นาทีก่อนหน้า	38
3.22	กราฟค่าความเร็วของข้อมูลที่ผ่านแต่ละอินเตอร์เฟสใน 30 วันก่อนหน้า	38
3.23	กราฟความเร็วของข้อมูลที่ผ่านแต่ละอินเตอร์เฟสใน 24 ชั่วโมงก่อนหน้า	38
3.24	กราฟค่าความเร็วของข้อมูลที่ผ่านแต่ละอินเตอร์เฟสใน 12 เดือนก่อนหน้า	39
3.25	หน้าต่างสำหรับการสั่งปิดเครื่อง (SHUTDOWN) รีสตาร์ท(RESTART) หรือไปสู่หน้าแอ็คเคาน์(ACCOUNT)	39
3.26	หน้าต่างสำหรับกำหนดสถานะการทำงานของฟังก์ชัน	39
3.27	หน้าต่างสำหรับการกำหนดค่า WEIGHT ในการส่งข้อมูล	40
3.28	หน้าต่างสำหรับการกีดกันเว็บไซต์ที่ไม่ต้องการให้ผู้ใช้เข้าถึง	40
3.29	หน้าต่างสำหรับกำหนดค่า IP ADDRESS ที่จะทำการบายพาส	40

สารบัญรูป(ต่อ)

รูปที่		หน้า
4.1	หน้าต่างรับข้อมูลของผู้ใช้	44
4.2	ตัวอย่างการสร้างแอคเคาท์ผู้ใช้รายบุคคล	44
4.3	ข้อมูลของผู้ใช้งานถูกนำไปเก็บในดาต้าเบส (DATABASE)	45
4.4	หน้าต่างรับข้อมูลของผู้ใช้แบบกลุ่ม	45
4.5	ตัวอย่างการสร้างแอคเคาท์ผู้ใช้แบบกลุ่ม	46
4.6	ข้อมูลของผู้ใช้งานแบบกลุ่มถูกนำไปเก็บในดาต้าเบส	46
4.7	การทดลองการยืนยันตัวตนครั้งที่ 1	47
4.8	ผลการทดลองการยืนยันตัวตนครั้งที่ 1	48
4.9	การทดลองการยืนยันตัวตนครั้งที่ 2	48
4.10	ผลการทดลองการยืนยันตัวตนครั้งที่ 2	49
4.11	การทดลองการยืนยันตัวตนครั้งที่ 3	49
4.12	ผลการทดลองการยืนยันตัวตนครั้งที่ 3	50
4.13	การทดลองการยืนยันตัวตนครั้งที่ 4	50
4.14	ผลการทดลองการยืนยันตัวตนครั้งที่ 4	51
4.15	สถานะ TCP_MISS	52
4.16	เว็บไซต์ที่เป็น TCP_MISS	53
4.17	สถานะ TCP_HIT	53
4.18	เว็บไซต์ HTTP://WWW.TEE-PAK.NET/DOOLAKORN ที่เป็น TCP_HIT	54
4.19	สถานะ TCP_MISS	54
4.20	เว็บไซต์ HTTP://WWW.WATCHLAKORN.IN/TAG/อายุน้อยร้อยล้าน ที่เป็น TCP_MISS	55
4.21	สถานะ TCP_HIT	55
4.22	เว็บไซต์ HTTP://WWW.WATCHLAKORN.IN/TAG/อายุน้อยร้อยล้าน ที่เป็นTCP_HIT	56
4.23	สถานะ TCP_MIS	56
4.24	เว็บไซต์ HTTP://FO3.GARENA.IN.TH/MAIN ที่เป็น TCP_MISS	57

สารบัญรูป(ต่อ)

รูปที่		หน้า
4.25	สถานะ TCP_HIT	57
4.26	เว็บไซต์ HTTP://FO3.GARENA.IN.TH/MAIN/ ที่เป็นTCP_HIT	58
4.27	รายชื่อเว็บไซต์ที่ระบบได้ทำการ BLACK LIST DOMAIN	59
4.28	หน้า URL ที่อันตรายหรือไม่เหมาะสม	59
4.29	REMOVE BLACK LIST ในลำดับที่4	60
4.30	หลังที่ได้ทำการ REMOVE	60
4.31	หน้า URL ของเว็ปไซต์ WWW.LAZADA.CO.TH	61
4.32	กำหนดค่า GATEWAYS RATIO WEIGHTING เป็น GW1:GW2 เท่ากับ 4:1	62
4.33	เซิร์ฟเวอร์กระจายงานไปยัง GATEWAY1 ที่ PORT : P1P1	62
4.34	เซิร์ฟเวอร์กระจายงานไปยัง GATEWAY2 ที่ PORT : P2P1	63
4.35	กำหนดค่า GATEWAYS RATIO WEIGHTING เป็น GW1:GW2 เท่ากับ 1:1	63
4.36	เซิร์ฟเวอร์กระจายงานไปยัง GATEWAY1 ที่ PORT : P1P1	64
4.37	เซิร์ฟเวอร์กระจายงานไปยัง GATEWAY2 ที่ PORT : P2P1	64
4.38	กำหนดค่า GATEWAYS RATIO WEIGHTING เป็น GW1:GW2 เท่ากับ 1:4	65
4.39	เซิร์ฟเวอร์กระจายงานไปยัง GATEWAY1 ที่ PORT : P1P1	65
4.40	เซิร์ฟเวอร์กระจายงานไปยัง GATEWAY2 ที่ PORT : P2P1	66

สารบัญตาราง

ตารางที่		หน้า
3.1	พอร์ตที่ใช้ในการสื่อสารข้อมูลระหว่างเซิร์ฟเวอร์ของระบบกับคอมพิวเตอร์ภายนอก	33
3.2	ฐานข้อมูลยูสเซอร์เนมและพาสเวิร์ดของระบบ	42
4.1	การทดลองการกระจายงานของเซิร์ฟเวอร์ กรณีที่ 1	63
4.2	การทดลองการกระจายงานของเซิร์ฟเวอร์ กรณีที่ 2	64
4.3	การทดลองการกระจายงานของเซิร์ฟเวอร์ กรณีที่ 3	66

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

เครือข่ายอินเตอร์เน็ตเป็นเครือข่ายที่นิยมใช้กันอย่างแพร่หลายทั้งภายในองค์กรและอาคารสถานที่ต่างๆ จึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการสร้างระบบบริหารจัดการในการเข้าถึงข้อมูลอินเตอร์เน็ตของผู้ใช้ภายในอาคารอย่างเหมาะสม เพื่อให้ผู้ใช้สามารถเข้าถึงข้อมูลอินเตอร์เน็ตได้อย่างสะดวก รวดเร็ว และปลอดภัย คณะผู้จัดทำจึงได้ทำการสร้างระบบบริหารจัดการในการเข้าถึงข้อมูลอินเตอร์เน็ตโดยระบบดังกล่าวประกอบด้วย เซิร์ฟเวอร์ (server) และฟังก์ชั่น(Function)การทำงานต่างๆที่บรรจุอยู่ในเซิร์ฟเวอร์ ได้แก่ฟังก์ชั่น Multiple – Gateways , ฟังก์ชั่น Authentication System , ฟังก์ชั่น Web – Caching (Proxy) , ฟังก์ชั่นNetwork Security (Firewall) และฟังก์ชั่น Graphic User Interface Management

1.2 วัตถุประสงค์

1. สามารถตรวจสอบสิทธิ์ในการใช้งานของผู้ใช้บริการ
2. ดูแลรักษาความปลอดภัยเครือข่ายและข้อมูลของผู้ใช้บริการ
3. สามารถตรวจสอบสถานะของระบบสำหรับบริหารจัดการระบบได้อย่างเหมาะสม
4. ควบคุมและจำกัดการเข้าถึงข้อมูลอินเตอร์เน็ตของผู้ใช้บริการได้อย่างมีประสิทธิภาพ

1.3 ขอบเขตปริญญานิพนธ์

เขียนโปรแกรมสร้างระบบบริหารจัดการในการเข้าถึงข้อมูลอินเตอร์เน็ตโดยมีฟังก์ชั่นควบคุมการทำงานดังต่อไปนี้

1. Multiple – gateways
2. Authentication System
3. Web – caching (Proxy)
4. Network Security (Firewall)
5. Graphic User Interface Management

บทที่ 2

ทฤษฎีและหลักการที่เกี่ยวข้อง

2.1 Internet

อินเตอร์เน็ต (Internet) มาจากคำว่า International Network เป็นเครือข่ายของการสื่อสารข้อมูลขนาดใหญ่อันประกอบด้วยเครือข่ายคอมพิวเตอร์จำนวนมาก เชื่อมโยงแหล่งข้อมูลจากองค์กรต่างๆ ทั่วโลกเข้าด้วยกัน ส่วนคำว่า “เครือข่าย” หมายถึง การที่มีคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไป เชื่อมต่อเข้าด้วยกันด้วยสายเคเบิลหรือสายโทรศัพท์ มีผู้ใช้คอมพิวเตอร์และมีการถ่ายเทข้อมูลระหว่างกัน

2.1.1 หน้าที่และความสำคัญของอินเตอร์เน็ต

การสื่อสารในยุคปัจจุบันที่กล่าวขานกันว่าเป็นยุคไร้พรมแดนนั้น การเข้าถึงกลุ่มเป้าหมายจำนวนมากๆ ได้ในเวลาอันรวดเร็วและใช้ต้นทุนในการลงทุนต่ำ เป็นสิ่งที่พึงปรารถนาของทุกหน่วยงาน และอินเทอร์เน็ตเป็นสื่อที่สามารถตอบสนองต่อความต้องการดังกล่าวได้ จึงเป็นความจำเป็นที่ทุกคนต้องให้ความสนใจและปรับตัวให้เข้ากับเทคโนโลยีใหม่นี้ เพื่อจะได้ใช้ประโยชน์จากเทคโนโลยีดังกล่าวอย่างเต็มที่

อินเทอร์เน็ต ถือเป็นระบบเครือข่ายคอมพิวเตอร์สากลที่เชื่อมต่อเข้าด้วยกัน ภายใต้มาตรฐานการสื่อสารเดียวกัน เพื่อใช้เป็นเครื่องมือสื่อสารและสืบค้นสารสนเทศจากเครือข่ายต่างๆ ทั่วโลก ดังนั้น อินเทอร์เน็ตจึงเป็นแหล่งรวมสารสนเทศจากทุกมุมโลก ทุกสาขาวิชา ทุกด้าน ทั้งบันเทิงและวิชาการ ตลอดจนการประกอบธุรกิจต่างๆ

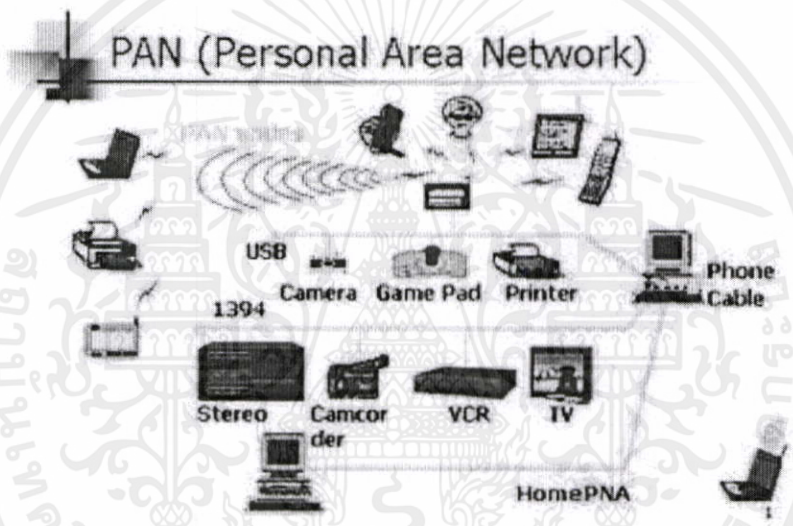
2.2 เครือข่าย (Network)

เครือข่ายคอมพิวเตอร์หมายถึง วิธีการเชื่อมต่อคอมพิวเตอร์เข้าด้วยกันผ่านสื่อกลางต่างๆ เช่นสายสัญญาณหรือคลื่นวิทยุ เป็นต้น เพื่อทำให้สามารถสื่อสารแลกเปลี่ยนข้อมูล และใช้ทรัพยากรร่วมกันได้ เครือข่ายนั้นมีหลายขนาดตั้งแต่ขนาดเล็กที่เชื่อมต่อกันด้วยคอมพิวเตอร์ สองสามเครื่องเพื่อใช้งานในบ้านหรือในบริษัทเล็กๆจนถึงเครือข่ายขนาดใหญ่ที่เชื่อมกันทั้งโลก

2.2.1 ประเภทของเครือข่าย

2.2.1.1 เครือข่ายส่วนบุคคล (Personal Area Network ; PAN)

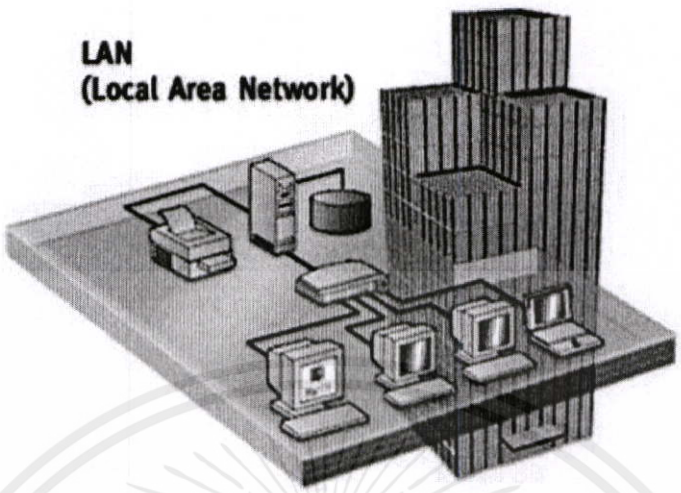
เครือข่ายส่วนบุคคลเป็นการเชื่อมต่ออุปกรณ์พกพา เช่น PDA หรือ โทรศัพท์มือถือเข้าด้วนกัน โดยมีขอบเขตของเครือข่ายเพียงระยะทางสั้นๆ และมีลักษณะเป็นเครือข่ายไร้สายสามารถเชื่อมต่ออุปกรณ์ที่อยู่ในระยะไม่เกิน 10 เมตร ตัวอย่างของ PAN เช่น Bluetooth ซึ่งเป็นการเชื่อมอุปกรณ์สองชิ้นด้วยความถี่ของ ISM Band ที่ 2.45 GHz มีอัตรารับส่งข้อมูลที่ 3Mbps



รูปที่ 2.1 เครือข่ายส่วนบุคคล (PAN) [1]

2.2.1.2 เครือข่ายภายใน (Local Area Network : LAN)

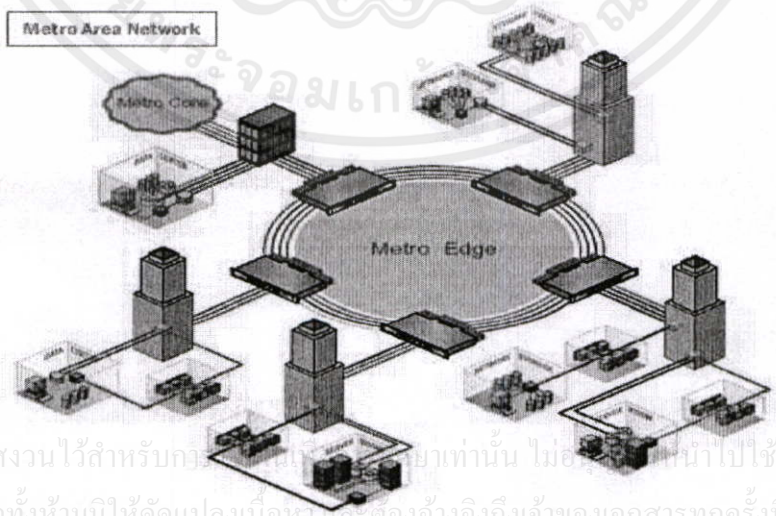
เครือข่ายภายในหรือ LAN เป็นเครือข่ายขนาดเล็กที่เชื่อมโยงอุปกรณ์ต่างๆ ที่อยู่ในพื้นที่ใกล้เคียงมีขอบเขตครอบคลุมบริเวณห้อง อาคาร หรือ สำนักงานเดียวกัน โดยเครือข่ายประเภทนี้จะประกอบไปด้วยคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงตั้งแต่ 2 ชิ้นขึ้นไป



รูปที่ 2.2 เครือข่ายภายใน (LAN) [2]

2.2.1.3 เครือข่ายระดับเมือง (Metropolitan Area Network : MAN)

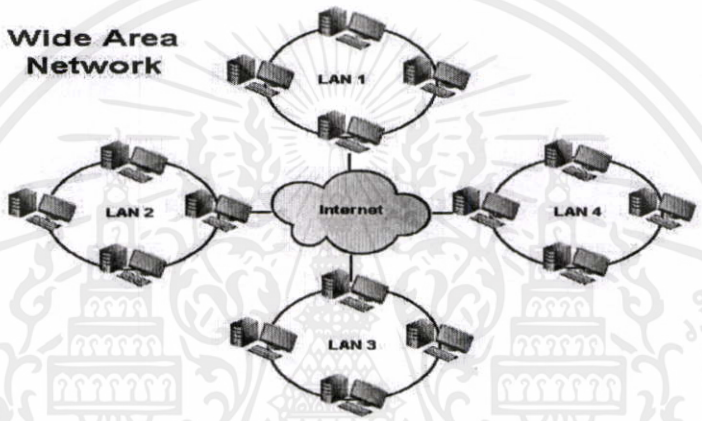
เครือข่ายระดับเมืองเป็นเครือข่ายที่มีขนาดใหญ่ครอบคลุมระดับเมือง ซึ่งอาจเป็นเครือข่ายเดียวที่มีการเชื่อมโยงภายในเมืองเดียวกัน เช่น การให้บริการของเคเบิลทีวีในระดับท้องถิ่น เป็นต้น หรือ อาจประกอบด้วยเครือข่ายระดับเมืองหลายเครือข่ายเชื่อมโยงกันผ่านเครือข่ายสาธารณะระดับเมืองก็ได้ เช่น การเชื่อมโยงเครือข่ายระดับเมือง ของบริษัทแห่งหนึ่งซึ่งมีหลายสาขาอยู่ภายในเมืองเดียวกัน เป็นต้น



รูปที่ 2.3 เครือข่ายระดับเมือง (MAN) [3]

2.2.1.4 เครือขายระยะไกล (Wide Area Network : WAN)

เครือข่ายระยะไกล WAN เป็นเครือข่ายที่ครอบคลุมทั่วโลก สามารถเชื่อมต่อเครือข่ายระดับเมือง ที่ห่างไกลกว่าระดับเมืองได้ผ่านเครือข่ายสาธารณะขนาดใหญ่หรือผู้ให้บริการเชื่อมโยงต่างๆ เช่น เครือข่ายอินเตอร์เน็ตที่สามารถเชื่อมโยงผู้ใช้ได้จากทุกมุมโลกผ่านผู้ให้บริการที่เรียกว่า ISP (Internet Service Provider) เป็นต้น

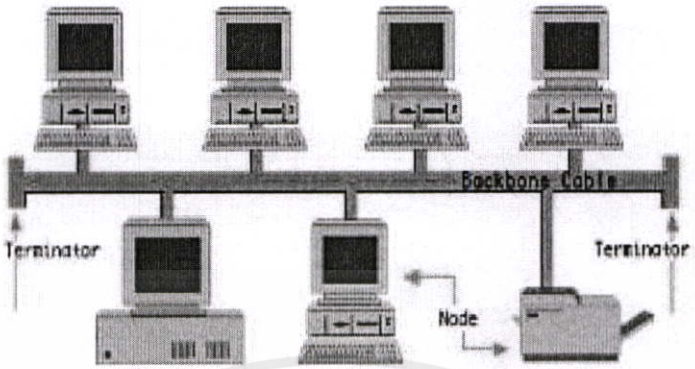


รูปที่ 2.4 เครือข่ายระยะไกล (WAN) [4]

2.2.2 รูปแบบการเชื่อมต่อของระบบเครือข่าย

2.2.2.1 โครงข่ายแบบเส้นตรง (Bus Topology)

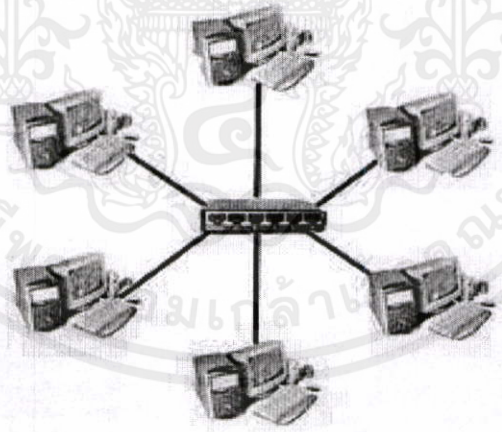
การเชื่อมต่อแบบเส้นตรงเป็นการเชื่อมต่อโดยใช้สายเคเบิลอย่างเดียว ไม่มีอุปกรณ์เน็ตเวิร์คอื่นเชื่อมต่อ ซึ่งในการส่งข้อมูลจากคอมพิวเตอร์เครื่องใดเครื่องหนึ่ง ข้อมูลนั้นจะไปถึงเครื่องคอมพิวเตอร์อื่นทุกเครื่องที่ต่ออยู่ด้วย แต่จะมีเพียงเครื่องปลายทางที่เป็นเป้าหมายเท่านั้นที่สามารถนำข้อมูลไปใช้งานได้



รูปที่ 2.5 โครงข่ายแบบเส้นตรง (Bus Topology) [5]

2.2.2.2 โครงข่ายแบบดาว (Star Topology)

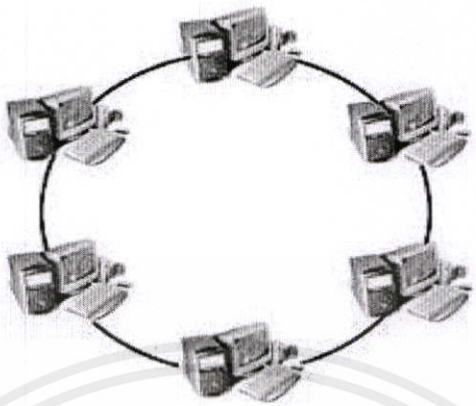
การเชื่อมต่อสำหรับโครงข่ายนี้ โหนดต่างๆจะถูกเชื่อมเข้ากับอุปกรณ์เน็ตเวิร์คตัวหนึ่งที่เป็นศูนย์กลาง โดยทั่วไปจะใช้ ฮับ (Hub) หรือ สวิตช์ (Switch) เมื่อต้องการส่งข้อมูลไปยังเครื่องปลายทางข้อมูลจะถูกส่งมาที่ฮับก่อน จากนั้นตัวอุปกรณ์จะส่งต่อไปยังเครื่องปลายทาง



รูปที่ 2.6 โครงข่ายแบบดาว (Star Topology) [6]

2.2.2.3 โครงข่ายแบบวงแหวน (Ring Topology)

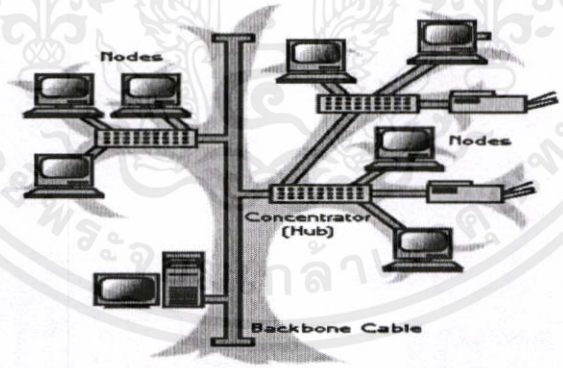
สำหรับโครงข่ายแบบวงแหวนโหนดแต่ละโหนดจะเชื่อมต่อกันเป็นวงลูป การส่งข้อมูลจะสามารถส่งได้เฉพาะกับโหนดที่ต่อด้วยกันเท่านั้น ถ้าต้องการติดต่อกับโหนดที่ไม่ได้ต่อก็ต้องใช้วิธีส่งผ่านจากโหนดที่ต่ออยู่เป็นทอดๆจนถึงปลายทางที่มีแอดเดรสตรงกับข้อมูล



รูปที่ 2.7 โครงข่ายแบบวงแหวน (Ring Topology) [7]

2.2.2.4 โครงข่ายแบบต้นไม้ (Tree Topology)

เป็นโครงข่ายที่เกิดจากการผสมผสาน ระหว่างโครงข่ายแบบเส้นตรงและโครงข่ายแบบดาว ลักษณะการเชื่อมต่อจะใช้สายเคเบิลเป็นสื่อกลาง เหมือนโครงข่ายแบบเส้นตรงทำหน้าที่เป็น “แบ็คโบน” โดยมีกลุ่มของโหนดต่างๆที่เชื่อมต่อกันแบบดาว เข้ามาเชื่อมต่อกับแบ็คโบนอีกที

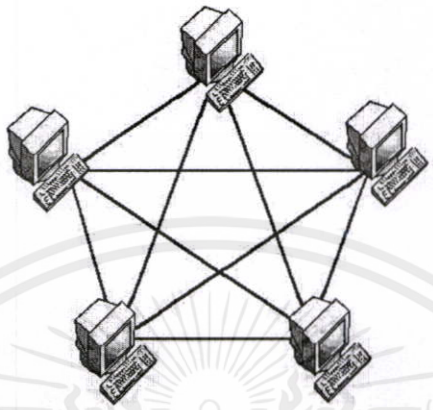


รูปที่ 2.8 โครงข่ายแบบต้นไม้ (Tree Topology) [8]

2.2.2.5 โครงข่ายแบบเมช (Mesh Topology)

โหนดทุกโหนดในโครงข่ายนี้จะเชื่อมต่อกันมากกว่าหนึ่งทาง เปรียบเสมือนมีเส้นทางสำรองไว้ สำหรับโครงข่ายแบบเมชแบ่งเป็น 2 แบบคือ ฟลูเมช (Full Mesh) และพาร์เชียล (Partial Mesh) ทั้งสองแบบต่างกันตรงที่การเชื่อมต่อของโหนดในโครงข่ายโดยแบบฟลูเมชนั้น

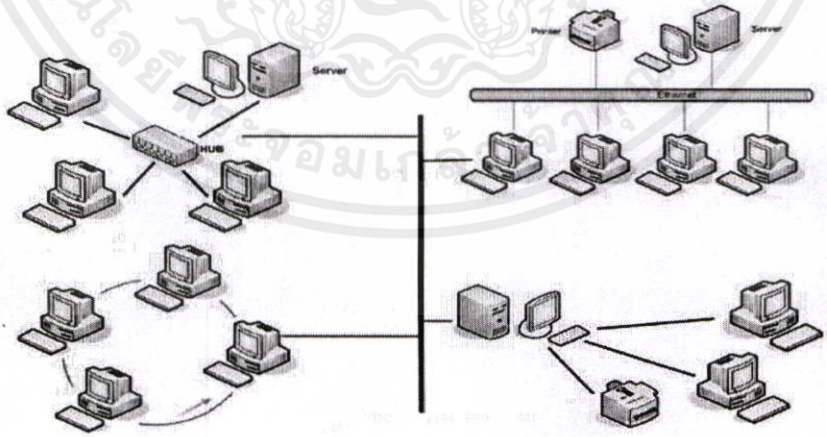
โหนดทุกโหนดจะเชื่อมต่อกันหมด ดังรูปด้านล่าง แต่ถ้าเป็นแบบพาร์เชียลเมช บางโหนดอาจจะเชื่อมกับโหนดที่มีการติดต่อบ่อยๆเท่านั้น



รูปที่ 2.9 โครงข่ายแบบเมช (Mesh Topology) [9]

2.2.2.6 โครงข่ายแบบไฮบริด (Hybrid Topology)

เป็นการเชื่อมต่อที่ผสมผสานเครือข่ายย่อยๆหลายส่วนมารวมเข้าด้วยกัน เช่น นำเอาโครงข่ายแบบบัส โครงข่ายแบบวงแหวน และ โครงข่ายแบบดาวมาเชื่อมต่อเข้าด้วยกัน เหมาะสำหรับบางหน่วยงานที่มีเครือข่ายเก่าและใหม่ให้สามารถทำงานร่วมกันได้

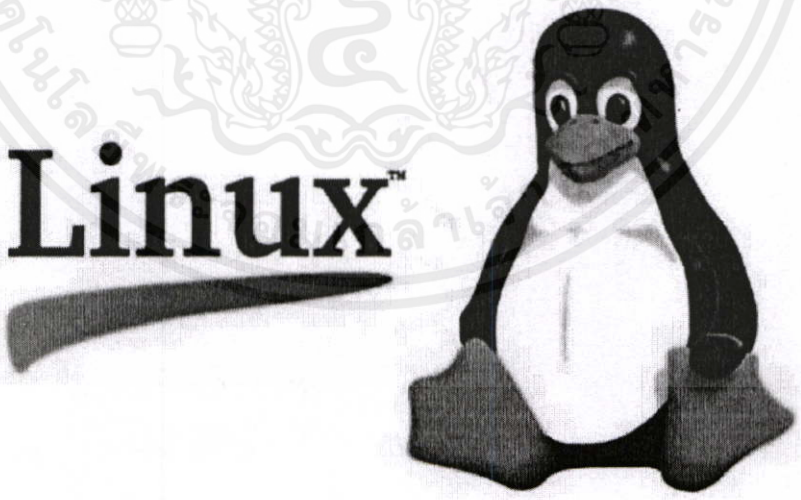


รูปที่ 2.10 โครงข่ายแบบไฮบริด (Hybrid Topology) [10]

2.3 Linux operating system

ลีนุกซ์ (Linux) คือโปรแกรมเคอร์เนล (Kernel) ซึ่งทำหน้าที่เป็นศูนย์กลางของระบบปฏิบัติการ (Operating System) ซึ่งก็จะเหมือนกับระบบปฏิบัติการ อื่นๆ เช่น Window , ยูนิกซ์ (Unix) โดยที่ ลีนุกซ์ ได้รับการพัฒนามาจากระบบปฏิบัติการยูนิกซ์ ซึ่งลีนุกซ์มีระบบปฏิบัติการแบบ 32บิต และ 64บิต มีระบบ X วินโดวส์ซึ่งเป็นระบบการติดต่อผู้ใช้แบบกราฟฟิก และเป็นระบบปฏิบัติการที่อยู่ภายใต้เงื่อนไขของ GPL (General Public Licence) หมายความว่าสามารถเปลี่ยนแปลงแก้ไขพัฒนา และแจกจ่ายให้ใช้ฟรี

ส่วนประกอบที่สำคัญที่สุดภายในระบบปฏิบัติการก็คือตัวโปรแกรมเคอร์เนลนี้เอง โดยภายในเคอร์เนลจะมีส่วนโปรแกรมย่อยๆ เรียกว่า โมดูล รวมกันไว้ภายใน แต่ละโมดูลทำหน้าที่ และช่วยให้ระบบปฏิบัติการมีความสามารถต่างๆ จะมากหรือน้อยก็ขึ้นอยู่กับความสามารถ และจำนวนของโมดูลภายในเคอร์เนล เพราะฉะนั้นระบบปฏิบัติการทุกระบบที่นิยมใช้งานกันในปัจจุบัน จึงล้วนมีเคอร์เนลเป็นศูนย์กลางของระบบ แต่อาจมีความแตกต่างกันได้เนื่องจากมีผู้พัฒนาขึ้นหลายรายนั้นเอง ได้แก่ ระบบปฏิบัติการวินโดวส์ก็มีเคอร์เนลของตนเอง แตกต่างจากระบบปฏิบัติการอื่นๆ เช่น FreeBSD ซึ่งเป็นระบบปฏิบัติการยูนิกซ์ชนิดหนึ่งก็มีเคอร์เนลเป็นของตัวเองเช่นกัน ดังนั้นหากพิจารณาภายในระบบปฏิบัติการลีนุกซ์ย่อมพบเคอร์เนลลีนุกซ์อย่างแน่นอน



รูปที่ 2.11 Linux operating system [11]

2.4 ภาษา PHP

พีเอชพี (PHP) คือภาษาสคริปต์ (Script) อย่างหนึ่งที่เรียกว่า Server-Side Script ซึ่งจะทำงาน ในฝั่งเซิร์ฟเวอร์ แล้วส่งการแสดงผลมายัง Browser ของตัวผู้ใช้ และนอกจากนี้ยังสามารถเป็นสคริปต์ ที่ทำงานร่วมกับ HTML ได้อีกด้วย

พีเอชพี เป็นภาษาจำพวก Scripting Language คำสั่งต่างๆจะเก็บอยู่ในไฟล์ที่เรียกว่าสคริปต์ และเวลาใช้งานต้องอาศัยตัวแปรชุดคำสั่ง ตัวอย่างของภาษาสคริปก็เช่น JavaScript, Perl เป็นต้น

ลักษณะของพีเอชพีที่แตกต่างจากภาษาสคริปต์แบบอื่นๆ คือพีเอชพีได้รับการพัฒนาและออกแบบมา เพื่อใช้งานในการสร้างเอกสารแบบ HTML โดยสามารถสอดแทรกหรือแก้ไขเนื้อหาได้โดยอัตโนมัติ ดังนั้นจึงกล่าวว่าพีเอชพี เป็นภาษาที่เรียกว่า server-side หรือ HTML-Embedded Scripting Language เป็นเครื่องมือที่สำคัญชนิดหนึ่งที่ช่วยให้เราสามารถสร้างเอกสารแบบ Dynamic HTML ได้อย่างมีประสิทธิภาพและมีลูกเล่นมากขึ้น

เนื่องจากพีเอชพี ไม่ได้เป็นส่วนหนึ่งของตัว Web Server ดังนั้นถ้าจะใช้พีเอชพีก็จะต้องดูก่อนว่า Web Server นั้นสามารถใช้สคริปต์พีเอชพี ได้หรือไม่ ยกตัวอย่างเช่นพีเอชพีสามารถใช้ได้กับ Apache Web Server และ Personal Web Server (PWS) สำหรับระบบปฏิบัติการ Windows 95/98/NT

ในกรณีของ Apache เราสามารถใช้พีเอชพีได้สองรูปแบบคือ ในลักษณะของ CGI และ Apache Module ความแตกต่างอยู่ตรงที่ว่า ถ้าใช้ พีเอชพีเป็นแบบโมดูล พีเอชพีจะเป็นส่วนหนึ่งของ Apache หรือเป็นส่วนขยายในการทำงาน ซึ่งจะทำงานได้เร็วกว่าแบบที่เป็น CGI เนื่องจากถ้าเป็น CGI แล้ว ตัวแปรชุดคำสั่งของพีเอชพีถือว่าเป็นแค่โปรแกรมภายนอก ซึ่ง Apache จะต้องเรียกขึ้น มาทำงานทุกครั้งที่ต้องการใช้พีเอชพีดังนั้น ถ้ามองในเรื่องของประสิทธิภาพในการทำงาน การใช้พีเอชพีแบบที่เป็นโมดูลหนึ่งของ Apache จะทำงานได้มีประสิทธิภาพมากกว่า

2.5 TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) เป็นโปรโตคอล (protocol) การสื่อสารพื้นฐานของระบบอินเตอร์เน็ต มันสามารถใช้เป็นโปรโตคอลในการสื่อสารภายในเครือข่ายส่วนบุคคล เรียกว่า Intranet และ Extranet เมื่อมีการติดต่อโดยตรงกับ internet เครื่องคอมพิวเตอร์จะได้รับการคัดลอกโปรแกรม TCP/IP เช่นเดียวกับคอมพิวเตอร์อื่น ๆ เพื่อทำให้ส่งข้อความขอรับสารสนเทศ

TCP/IP เป็นโปรแกรม 2 เลเยอร์ TCP (Transmission Control Protocol) เป็นเลเยอร์ที่สูงกว่า ทำหน้าที่จัดการแยกข้อความหรือไฟล์แลปรกอบให้เหมือนเดิม IP (Internet Protocol) เป็นเลเยอร์ที่ต่ำกว่า ทำหน้าที่จัดการส่วนของที่อยู่ของแต่ละชุดข้อมูล เพื่อทำให้มีปลายทางที่ถูกต้อง เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็น Gateway บนเครือข่ายจะตรวจที่อยู่นี้เพื่อหาจุดหมายในการส่งข้อความ ชุดข้อมูลอาจจะใช้เส้นทางไปยังปลายทางต่างกัน แต่ทั้งหมดจะได้รับการประกอบใหม่ที่ปลายทาง

2.6 Routing Protocol

Routing Protocol คือโพรโทคอลที่ใช้ในการแลกเปลี่ยน Routing Table ระหว่างอุปกรณ์เครือข่ายต่างๆที่ทำงานในระดับ Network Layer (Layer 3) เช่น Router เพื่อให้อุปกรณ์เหล่านี้สามารถส่งข้อมูล (IP packet) ไปยังคอมพิวเตอร์ปลายทางได้อย่างถูกต้อง โดยที่ผู้ดูแลเครือข่ายไม่ต้องแก้ไขข้อมูล Routing Table ของอุปกรณ์ต่างๆตลอดเวลา เรียกว่าการทำงานของ Routing Protocol ทำให้เกิดการใช้งาน Dynamic Routing ต่อระบบเครือข่าย

2.7 Web Caching

Web Caching เป็นพื้นที่สำหรับเก็บออบเจ็กต์ของเว็บชั่วคราว เช่น เอกสาร HTML สำหรับการเรียกใช้ในภายหลัง ซึ่งทำให้มีข้อดีในการใช้ที่สำคัญอยู่ 3 ประการคือ

1. ลดการใช้แบนวิดท์ (Bandwidth) เพราะการเรียกใช้และการตอบสนองเพียงที่ต้องออกไปนอกเครือข่ายน้อยลง

2. ลดการทำงานของเซิร์ฟเวอร์ เพราะการเรียกใช้บางครั้งเท่านั้นที่ตัวเซิร์ฟเวอร์ต้องจัดการ

3. ลด Latency เพราะ การตอบสนองของในการเรียกใช้ข้อมูลที่อยู่ แคช (Cache) จะทำได้ทันที และอยู่ใกล้กับตัวผู้ใช้

Caching จะถูกใช้งานโดย Client Application และ ถูก Built-In ไว้ในโปรแกรม Web Browser ต่าง ๆ นอกจากนี้ก็ยังมีผลิตภัณฑ์จำนวนมากที่ได้ขยาย (Extend) หรือแทนที่ (Replace) Built-In Cache ไว้กับระบบ ซึ่งมี Storage ขนาดใหญ่ มี Feature มากขึ้น และมีประสิทธิภาพสูงขึ้น

Caching สามารถที่จะถูกนำมาใช้เป็นตัวกลางระหว่างผู้ใช้ และ เซิร์ฟเวอร์ ในรูปของการเป็นส่วนหนึ่งของ พร็อกซี่ (Proxy) ดังรูปที่ 2.13 ซึ่ง พร็อกซี่แคช (Proxy Cache) ส่วนมากจะติดตั้งอยู่ใกล้กับ Network Gateway เพื่อเป็นการลดแบนวิดท์ในการที่จะต้องไปดึงข้อมูลที่อยู่ใน

อินเตอร์เน็ต ซึ่งตัวระบบจะให้บริการผู้ใช้ ด้วยการเก็บแคชออบเจ็กต์ของเว็บจากเซิร์ฟเวอร์หลาย ๆ แห่งซึ่งตามความเป็นจริง จะมีประโยชน์มากเพราะโอกาสถึง 80% ที่ออบเจ็กต์ที่อยู่ในแคช ซึ่งถูกต้องการโดย ผู้ใช้หนึ่งๆ มักจะถูกเรียกใช้จากผู้ใช้อื่นๆ อีกในภายหลัง และเพื่อให้ประสิทธิภาพที่สูงขึ้นไปอีกพร็อกซี่แคชหลายๆตัว จะถูกประกอบกันเป็นส่วนหนึ่งของ Cache Hierarchy เพื่อที่จะได้ทำการสอบถาม (Inquiry) เอกสารที่ต้องการได้จาก Neighboring Cache โดยไม่ได้ไปโหลดออบเจ็กต์ต่าง ๆ โดยตรง

แคชสามารถที่จะถูกติดตั้งไว้ที่ส่วนหน้าของเซิร์ฟเวอร์เพื่อลดจำนวนครั้งในการร้องขอ (Request) ที่ เซิร์ฟเวอร์ ต้องจัดการ ซึ่ง พร็อกซี่แคชโดยส่วนมากก็จะถูกใช้งานในลักษณะนี้ แต่จะมีชื่อเรียกที่แตกต่างกัน เช่น Reserve Cache, Inverse Cache บางครั้งเรียกว่า HTTP Accelerator เพื่อที่จะสะท้อนให้เห็นความจริงที่ว่าแคช เหล่านี้ ได้ทำการจัดเก็บข้อมูลของหลาย ๆ ผู้ใช้ แต่ (โดยปกติ) ข้อมูลเหล่านั้นเป็นของ เซิร์ฟเวอร์อันเดียว

Web Cache จะอยู่ระหว่าง Web Server และผู้ใช้จะคอยตรวจสอบการเรียกใช้ HTML, รูปภาพ และไฟล์ที่มีการเรียกใช้จาก ผู้ใช้ แล้วทำการคัดลอกไว้สำหรับตัวมันเอง หากมีการร้องขอมาที่ออบเจ็กต์เดิม Web Cache ก็จะให้ออบเจ็กต์ ตัวที่มันคัดลอกไว้ไปแทน ดังนั้นจึงมี 2 เหตุผลหลักที่ควรนำ Web Cacheมาใช้ นั่นคือ

1. Reduce Latency เพราะว่าการร้องขอจะถูกเรียกใช้จากแคช (ซึ่งอยู่ใกล้กับผู้ใช้) แทนที่จะไปที่ เซิร์ฟเวอร์ ทำให้ใช้เวลาน้อยลง เมื่อผู้ใช้จะไปดึงออบเจ็กต์มาและแสดง
2. Reduce Traffic เพราะว่าแต่ละออบเจ็กต์จะถูกดึงมาจาก เซิร์ฟเวอร์เพียงครั้งเดียว ทำให้เป็นการลดจำนวนการใช้แบนวิดท์ ของผู้ใช้จะเป็นการประหยัดหากผู้ใช้ ต้องเสียค่าใช้จ่ายเรื่อง Traffic และจะทำให้การจัดการแบนวิดท์ จัดการได้ง่าย

2.7.1 ประเภทของ web-cache

2.7.1.1 Browser Cache

หากลองเปิด Dialogue ที่ชื่อ Preference ของ Browser สมัยใหม่ จะมีหัวข้อ Cache Setting ที่ผู้ใช้สามารถกำหนดพื้นที่บนฮาร์ดดิสก์ เพื่อใช้ในการเก็บออบเจ็กต์ที่เคยเข้าไปดูมาแล้ว Browser Cache จะทำงานโดยใช้หลักการเบื้องต้นของแคช และจะมีประโยชน์ เมื่อมีการกดปุ่ม Back ซึ่งจะเป็นการกลับไปดูหน้าจอที่เคยดูมาแล้ว

2.7.1.2 Proxy Cache

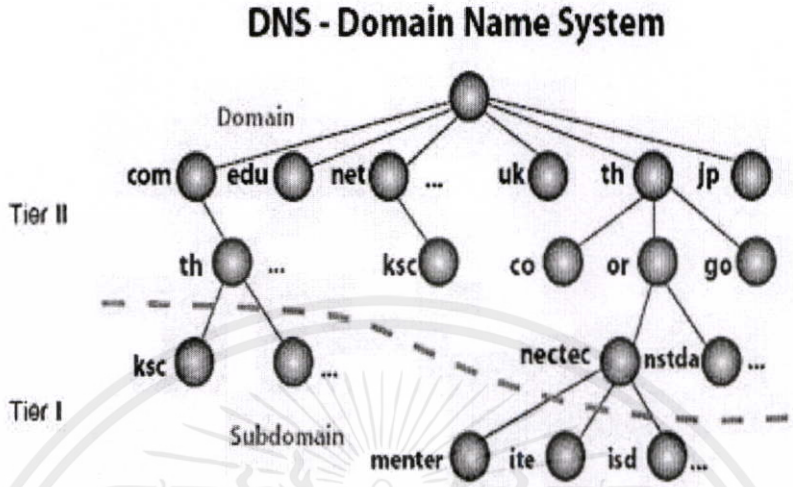
แคชประเภทนี้จะทำงานบนหลักการเดิมแต่จะมีขนาดที่ใหญ่กว่า พร็อกซี่แคชจะให้บริการกับผู้ใช้งานจำนวนมากกว่า, ถูกใช้ในองค์กรขนาดใหญ่ และ ISP มักจะติดตั้งแคชประเภทนี้บนไฟร์วอลของพวกเขา เพราะว่าพร็อกซี่แคชจะมีผู้ใช้จำนวนมากที่ใช้งาน มันจึงเป็นสิ่งที่ดีในเรื่องของการลด Latency และ Traffic ลง ส่วนใหญ่แล้วพร็อกซี่แคชได้ถูกนำมาใช้ในองค์กรขนาดใหญ่ และ ISP ที่ต้องการลดจำนวนการใช้แบนวิดท์ของอินเตอร์เน็ตเพราะว่าแคชจะช่วยบริการผู้ใช้จำนวนมาก พร็อกซี่แคชจะเป็นประเภท Shared Cache

2.7.2 DNS (Domain Name Service)

ระบบ ดีเอ็นเอส มาจากคำว่า Domain Name Service (DNS) นี้เป็นระบบจัดการแปลงชื่อไปเป็นหมายเลข ไอพีแอดเดรส (IP address) โดยมีโครงสร้างฐานข้อมูลแบบลำดับชั้นเพื่อใช้เก็บข้อมูลที่เรียกค้นได้อย่างรวดเร็ว กลไกหลักของระบบดีเอ็นเอส คือ ทำหน้าที่แปลงข้อมูลชื่อและหมายเลข ไอพีแอดเดรสหรือทำกลับกันได้ นอกจากนี้ยังมีฟังก์ชันเพิ่มเติมอื่นๆ อีก เช่น แจ้งชื่อของอีเมลเซิร์ฟเวอร์ใน domain ที่รับผิดชอบด้วยในระบบดีเอ็นเอส จะมีการกำหนด Name Space ที่มีกฎเกณฑ์อย่างชัดเจน มีกลไกการเก็บข้อมูลเป็นฐานข้อมูลแบบกระจาย ทำงานในลักษณะของผู้ใช้และเซิร์ฟเวอร์

ดีเอ็นเอส คือสิ่งที่นำมาอ้างถึงหมายเลขเครื่อง หรือ หมายเลข ไอพีแอดเดรส เพื่อให้ง่ายต่อการจดจำ ดีเอ็นเอส จะทำหน้าที่คล้ายกับสมุดโทรศัพท์ คือ เมื่อมีคนต้องการจะโทรศัพท์หาใคร คน ๆ นั้นก็จะต้องเปิดสมุดโทรศัพท์เพื่อค้นหาเบอร์โทรศัพท์ของคนที่ต้องการจะติดต่อ คอมพิวเตอร์ก็เช่นกัน เมื่อต้องการจะสื่อสารกับคอมพิวเตอร์เครื่องอื่น เครื่องนั้นก็จะทำการสอบถามหมายเลข IP ของเครื่องที่ต้องการจะสื่อสาร กับ DNS Server ซึ่งจะทำการค้นหาหมายเลขดังกล่าวในฐานข้อมูลแล้วแจ้งให้ Host ดังกล่าวทราบ ระบบดีเอ็นเอส แบ่งออกได้เป็น 3 ส่วน คือName Resolvers โดยเครื่องผู้ใช้ ที่ต้องการสอบถามหมายเลขไอพีเรียกว่า Resolver ซึ่งซอฟต์แวร์ที่ทำหน้าที่เป็น Resolvers นั้นจะถูกสร้างมากับแอพพลิเคชันหรือเป็น Library ที่มีอยู่ในผู้ใช้

Domain Name Space เป็นฐานข้อมูลของดีเอ็นเอส ซึ่งมีโครงสร้างเป็น Tree หรือเป็นลำดับชั้น แต่ละโหนดคือ โดเมนโดยสามารถมีโดเมนย่อย (Sub Domain) ซึ่งจะใช้จุดในการแบ่งแยก Name Servers เป็นคอมพิวเตอร์ที่รันโปรแกรมจัดการฐานข้อมูลบางส่วนของดีเอ็นเอส โดย เนมเซิร์ฟเวอร์ (Name Server) จะตอบการร้องขอทันที โดยการหาข้อมูลตัวเอง หรือส่งต่อการร้องขอไปยังเนมเซิร์ฟเวอร์ อื่น ซึ่งถ้า มีข้อมูลของส่วนโดเมนแสดงว่าเซิร์ฟเวอร์นั้นเป็นเจ้าของโดเมนเรียกว่า Authoritative แต่ถ้าไม่มีเรียกว่า Non-Authoritative



รูปที่ 2.12 root ของ Domain Name System [12]

2.8 Authentication

การระบุตัวตน (Authentication) เป็นวิธีการที่ใช้ในการตรวจสอบผู้ที่มาใช้งานระบบเครือข่ายอินเทอร์เน็ต โดยระบบจะตรวจสอบว่า Username และ Password ที่ใช้ในการเข้าสู่ระบบนั้น ถูกต้องหรือไม่ มีตัวตนของผู้ใช้งานอยู่จริงหรือไม่ ดังรูปที่ 2.15

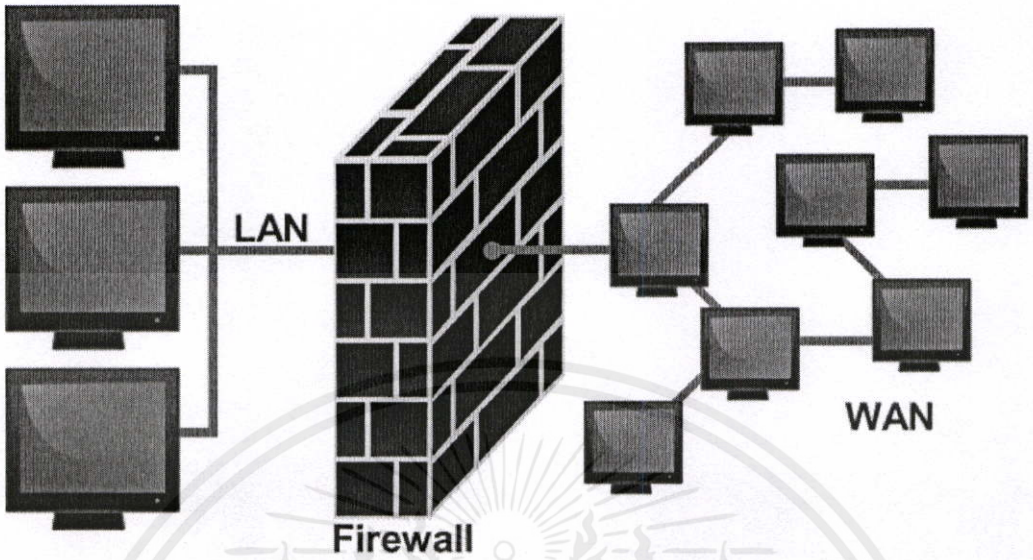
จุดประสงค์หลักของการระบุตัวตน คือพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต คือใคร พร้อมทั้งทำการตรวจสอบสิทธิ์ว่าผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตของท่านนั้นมีสิทธิ์ใช้ได้นานเท่าไหร่และสามารถ Upload หรือ Downloadได้ด้วยความเร็วเท่าไหร่ซึ่งระบบนั้นจะทำการตัดผู้ใช้ออกไปจากการให้บริการทันทีที่เวลาหมด อีกทั้งยังสามารถกำหนดเวลาและความเร็วได้ตามความเหมาะสมด้วย ต่อจากนั้นจะทำการบันทึกข้อมูลการใช้งานระบบเครือข่ายอินเทอร์เน็ตซึ่งจุดประสงค์หลักของขบวนการนี้ เพื่อทำรายงานการใช้ระบบเครือข่ายอินเทอร์เน็ตจะทำการยืนยันบันทึกข้อมูลในการใช้งานระบบเครือข่ายอินเทอร์เน็ตไว้อย่างละเอียดโดยสามารถทำรายงานสรุปและสถิติต่างๆ ได้ตามความต้องการ

จากเหตุผลดังกล่าวข้างต้นทำให้รู้ว่าการระบุตัวตน เป็นส่วนที่สำคัญและขาดไม่ได้ ถ้าต้องการใช้งานระบบเครือข่ายอินเทอร์เน็ตในปัจจุบัน จะต้องมีการยืนยันตัวตน เนื่องจากต้องการรู้ว่าผู้ใช้คือบุคคลใด

รูปที่ 2.13 หน้าต่างการระบุตัวตน

2.9 ไฟร์วอลล์

ไฟร์วอลล์ เป็นเครื่องมือที่ใช้สำหรับป้องกันระบบเครือข่าย จากการสื่อสารทั่วไปที่ถูกบุกรุก จากผู้ที่ไม่ได้รับอนุญาต เป็นเรื่องเกี่ยวกับการรักษาความปลอดภัยในระบบเครือข่าย หรือระบบเครือข่าย การป้องกันโดยใช้ระบบไฟร์วอลล์ นี้จะเป็นการกำหนดกฎเกณฑ์ หรือนโยบายในการควบคุมการเข้าออก หรือการควบคุมการรับส่งข้อมูลในระบบเครือข่าย สรุปคือไฟร์วอลล์ เป็นเสมือน Network Filter ทำหน้าที่จำกัดการเข้าถึงระบบเครือข่ายจากภายนอกนั้นเอง



รูปที่ 2.14 การจำกัดการเข้าถึงเครือข่ายจากภายนอกโดยไฟร์วอลล์ [13]

2.9.1 การป้องกันการเข้าถึงระบบ สามารถแบ่งออกได้เป็น 2 ประเภท

1. Logical Access คือการเข้าถึงผ่านระบบเครือข่าย เช่น ผ่านระบบเครือข่ายอินเตอร์เน็ต เป็นต้น

2. Physical Access คือ การเข้าถึงในลักษณะถึงตัวเครื่องจริงๆ เช่น การเข้าถึงในลักษณะเดินเข้ามาใช้งาน หรือลักลอบเข้ามาใช้ถึงตัวเครื่องคอม ในระบบเครือข่าย นั้นๆ

2.9.2 คุณสมบัติของ ไฟร์วอลล์

1. Protect โดยไฟร์วอลล์ เป็นเครื่องมือที่ใช้ในการป้องกัน โดยข้อมูลที่มีการรับหรือส่งผ่านระบบเครือข่าย โดยจะถูกกำหนดเป็นกฎเกณฑ์ หรือ Rule เพื่อบังคับใช้ในการสื่อสารภายในเครือข่าย

2 .Rule Base ข้อกำหนดในการควบคุมการรับส่งข้อมูลภายในระบบเครือข่าย ดังนั้นการติดตั้ง firewall จะต้องมีการกำหนดกฎเกณฑ์ในการควบคุมการทำงานในระบบเครือข่าย

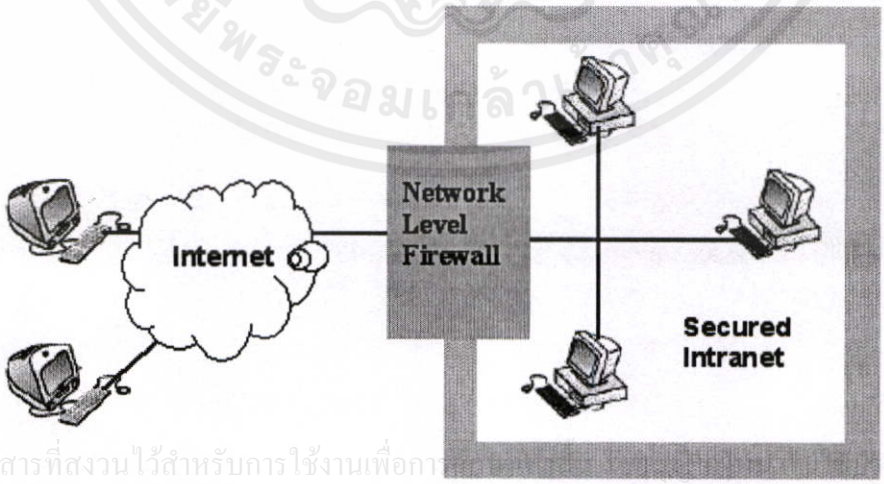
3. Access Control คือ การควบคุมระดับการเข้าถึง การรับส่ง ข้อมูล

2.9.3 ประเภทของ Firewall

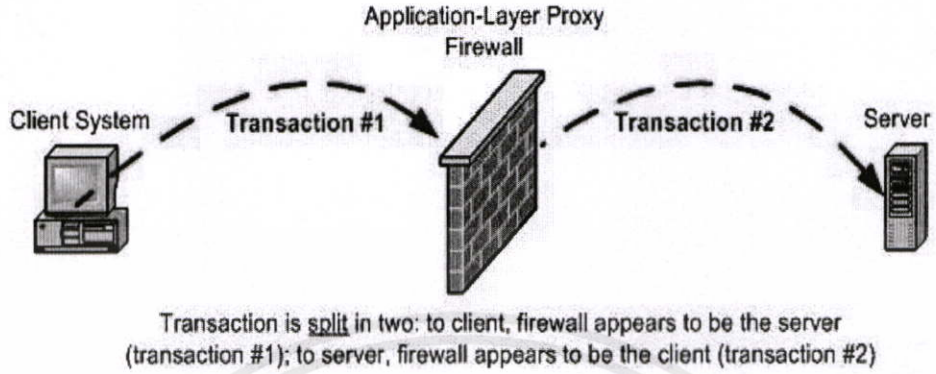
ไฟร์วอลล์ โดยทั่วไปจะถูกแบ่งออกเป็น 2 ประเภทคือ ไฟร์วอลล์ ระดับเครือข่าย (Network Level Firewall) และ Firewall Network จะตัดสินใจยอมให้ Traffic ใดผ่านนั้นจะดูที่ Address ผู้ส่งและผู้รับ และ Port ในแต่ละ IP packet ระดับ Application (Application Level Firewall)

ก่อนที่ไฟร์วอลล์ ระดับ เมื่อพิจารณาแล้วเห็นว่าทราฟฟิค สามารถผ่านไปได้ก็จะ Route Traffic ผ่านตัวมันไปโดยตรง Router โดยทั่วไปแล้วก็จะถือว่าเป็นไฟร์วอลล์ ระดับเครือข่าย ชนิดหนึ่งไฟร์วอลล์ ประเภทนี้จะมีความเร็วสูงและจะ Transparent ต่อผู้ใช้ (คือผู้ใช้มองไม่เห็น ความแตกต่างระหว่างระบบที่ไม่มีไฟร์วอลล์ กับระบบที่มีไฟร์วอลล์ระดับเครือข่าย การที่จะใช้ไฟร์ วอลล์ ประเภทนี้โดยมากผู้ใช้จะต้องมี IP block (ของจริง) ของตนเอง

ไฟร์วอลล์ ระดับ Application นั้นโดยทั่วไปก็คือ Host ที่ Run พร็อกซี่เซิร์ฟเวอร์ อยู่ ประเภทไฟร์วอลล์ นี้สามารถให้รายงานการ Audit ได้อย่างละเอียดและสามารถบังคับใช้นโยบาย ความปลอดภัยได้มากกว่าไฟร์วอลล์ระดับเครือข่าย แต่ไฟร์วอลล์ประเภทนี้ก็จะมีความ Transparent น้อยกว่าไฟร์วอลล์ ระดับเครือข่าย โดยที่ผู้ใช้จะต้องตั้งเครื่องของตนให้ใช้กับไฟร์ วอลล์ ประเภทนี้ได้ นอกจากนี้ไฟร์วอลล์ ประเภทนี้จะมีความเร็วน้อยกว่าไฟร์วอลล์ระดับเครือข่าย บางแหล่งจะกล่าวถึงไฟร์วอลล์ ประเภทที่สามคือประเภท Stateful Inspection Filtering ซึ่งใช้ การพิจารณาเนื้อหาของ แพ็คเก็ต (Packets) ก่อนๆในการที่จะตัดสินใจให้แพ็คเก็ต ที่กำลังพิจารณา อยู่เข้ามา



รูปที่ 2.15 ลักษณะของ Network Level Firewall [14]



รูปที่ 2.16 ลักษณะของ Application Layer Firewall [15]

2.9.4 ขีดความสามารถของ Firewall

1. ป้องกันการ Login ที่ไม่ได้รับอนุญาตที่มาจากภายนอกเครือข่าย

2. ปิดกั้นไม่ให้ทราฟฟิค จากภายนอกเครือข่ายเข้ามาภายในเครือข่ายแต่ก็ยอมให้ผู้ที่อยู่ภายในเครือข่ายสามารถติดต่อกับโลกภายนอกได้

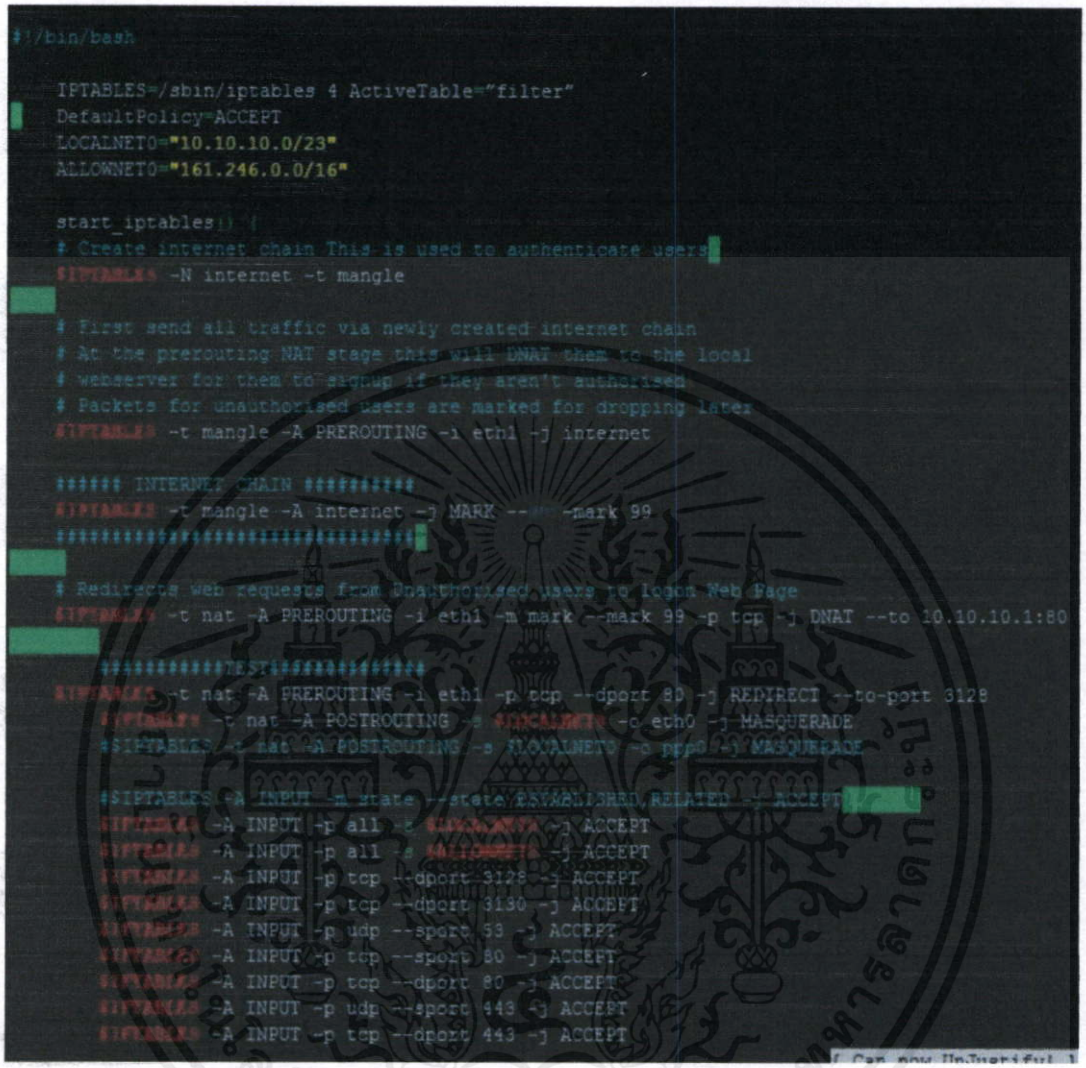
3. เป็นจุดรวมสำหรับการรักษาความปลอดภัยและการทำ Audit (เปรียบเสมือนจุดรับแรงกระแทกหรือ \"choke\" ของเครือข่าย)

2.9.5 ข้อจำกัดของ ไฟร์วอลล์

1. ไฟร์วอลล์ ไม่สามารถป้องกันการโจมตีที่ไม่ได้กระทำผ่านไฟร์วอลล์ (เช่น การโจมตีจากภายในเครือข่ายเอง)

2. ไม่สามารถป้องกันการโจมตีที่เข้ามากับ Application Protocols ต่างๆ (เรียกว่า การ Tunneling) หรือกับโปรแกรมผู้ใช้ ที่มีความล่อแหลมและถูกดัดแปลงให้กระทำการโจมตีได้ (โปรแกรมที่ถูกทำให้เป็น Trojan Horse)

3. ไม่สามารถป้องกัน ไวรัส (Virus) ได้อย่างมีประสิทธิภาพเนื่องจากจำนวน ไวรัสมีอยู่มากมาย จึงจะเป็นการยากมากที่ไฟร์วอลล์จะสามารถตรวจจับ Pattern ของ ไวรัสทั้งหมดได้

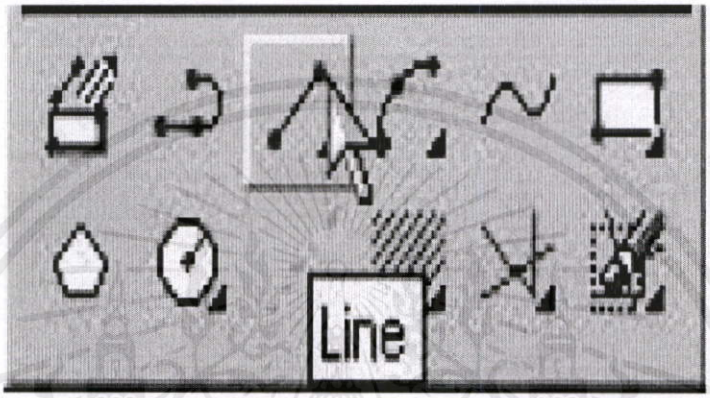


รูปที่ 2.17 ภาพส่วนของไฟล์วอลล์

2.10 Graphical user interface

จียูไอ(GUI) ย่อมาจาก Graphical User Interface คือการติดต่อกับผู้ใช้โดยใช้ภาพสัญลักษณ์ เป็นการออกแบบส่วนของโปรแกรมคอมพิวเตอร์ให้มีการโต้ตอบกับผู้ใช้ โดยการใช้ไอคอน (Icon) ,รูปภาพ และสัญลักษณ์อื่นๆ เพื่อแทนลักษณะต่างๆ ของโปรแกรม แทนที่ผู้ใช้จะพิมพ์คำสั่งต่างๆในการทำงาน ช่วยทำให้ผู้ใช้งานสามารถทำงานได้ง่าย และรวดเร็วขึ้น ไม่จำเป็นต้องจดจำคำสั่งต่างๆ ของโปรแกรมมากนัก ถือเป็นวิธีการให้ความสะดวกแก่ผู้ใช้คอมพิวเตอร์ ให้ติดต่อสื่อสารกับระบบโดยผ่านทางภาพ เช่น ใช้เมาส์กดเลือก ไอคอนแทนการพิมพ์คำสั่งดังแต่ก่อน โดยเฉพาะในบางโปรแกรมที่มีคำสั่งมากๆ เช่น โปรแกรม Autocad ที่ใช้ในการวาดแบบ ซึ่งจะมี คำสั่งต่างๆ ที่ใช้ในการสร้างรูปมากมาย ผู้ใช้สามารถใช้เม้าซ์ (Mouse) เลือกคำสั่งที่ต้องการจะวาดจากไอคอนที่ปรากฏ

ในโปรแกรมและใช้งานได้เลย โดยไม่ต้องพิมพ์คำสั่งต่างๆ ทางแป้นพิมพ์ ช่วยทำให้เกิดความรวดเร็วในการทำงาน และไม่ต้องเสียเวลาในการเรียนรู้และจดจำคำสั่งที่ต้องการมากนัก เพียงดูจากไอคอนที่ปรากฏในโปรแกรมก็สามารถใช้งานได้ทันที ตัวอย่างโปรแกรมที่ช่วยออกแบบโปรแกรมที่ใช้จียูไอ เช่น Microsoft Visual Basic เป็นต้น



รูปที่ 2.18 ตัวอย่างไอคอน ในโปรแกรม Autocad

2.11 การสร้างฟอร์มHTML

การสร้างแบบฟอร์ม (Form) เพื่อใช้ในการรับข้อมูลเป็นวิธีการหนึ่งที่นิยมทำกันในเว็บไซต์ทั่วไป เพราะการสร้างแบบฟอร์มจะทำให้กรอกข้อมูลได้ง่ายเป็นระเบียบสวยงาม และเป็นสัดส่วน ตัวอย่างแบบฟอร์มที่ใช้กันทั่วไปเช่นการกรอกข้อมูลในการสมัครสมาชิกต่าง ๆ การแสดงความคิดเห็น การกรอกแบบสอบถาม สิ่งเหล่านี้ถือได้ว่าเป็นการรับข้อมูลผ่านฟอร์มทั้งสิ้น

2.11.1 การออกแบบฟอร์มให้มีลักษณะต่าง ๆ ขึ้นอยู่กับประโยชน์ในการใช้งาน

2.11.1.1. รูปแบบการสร้าง Form

การสร้างแบบฟอร์ม (Form) ควบคุมด้วยแท็ก FORM และ INPUT โดยมีรูปแบบดังนี้

<FORM พารามิเตอร์>

<INPUT TYPE="TEXT" NAME="ชื่อของเท็กซ์บอกซ์" VALUE="ค่าเริ่มต้น"SIZE=ขนาดของเท็กซ์บอกซ์ MAXLENGTH=จำนวนตัวอักษรที่สามารถบันทึกได้>

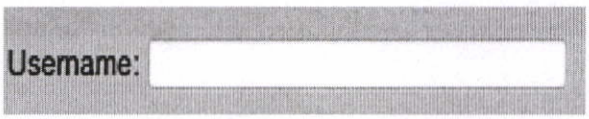
</FORM>

2.11.2. ตัวอย่างการสร้าง Form แบบต่าง ๆ

2.11.2.1 การสร้างที่ใส่ชื่อ

Username : <Input Type="text" size="15" maxlength="20">

จะได้เป็น

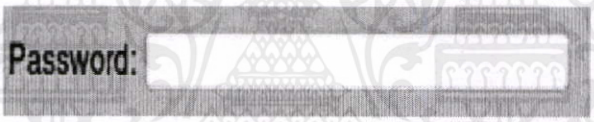


รูปที่ 2.19 ส่วนของ USERNAME

2.11.2.2 การสร้าง Password

Password : <Input Type="Password" Size="15" Maxlength="25">

จะได้เป็น



รูปที่ 2.20 ส่วนของ PASSWORD

2.11.2.3 แปลความหมาย

<Input Type="....."> คือการใส่ค่า Form ที่ต้องการเช่นต้องการ Form ใส่ชื่อ ก็ให้ใส่ Type ไว้ว่า Text

หรือจะใส่ Password ก็ให้ใส่ Type ไว้ว่า Password

<Input Size="....">ใส่ขนาดความกว้างของ Form ค่าเป็นตัวเลข เช่น 15

<Input Maxlength="...."> ขนาดความจุของตัวอักษรซึ่งถ้าเกินจำนวนที่ระบุจะไม่กรอกเข้าไปใน Input มีค่าเป็นตัวเลข เช่น 25

2.11.2.4 การสร้างปุ่ม Button

การสร้างปุ่ม Button ใน Form สามารถทำได้ทั้งปุ่มส่งหรือรับข้อมูล (Submit) และปุ่มยกเลิกการทำงานหรือ Reset

<Input Type="Submit" Value="ส่งข้อมูล" Name="Data"> จะได้รูปแบบเป็น

รูปที่ 2.21 ส่วนของ PASSWORD

แปลความหมายไทป์ (Type) ของการส่งคือ Submit และไทป์ของการรีเซ็ตคือ Reset ส่วน Name เป็นการกำหนดชื่อข้อมูลเพื่อส่งไปประมวลผล

รูปที่ 2.22 ตัวอย่างการสร้างหน้าเว็ปด้วยภาษาHTML [17]

2.12 โหลดบาลานซ์ (Load Balance)

2.12.1 โหลดบาลานซิ่ง (Load balancing)

โหลดบาลานซิ่ง (Load Balancing) คือการจัดกลุ่มของคอมพิวเตอร์หลายๆตัวเพื่อแบ่งงานกันหรือกระจายโหลดการใช้งานของผู้ใช้งาน ไปยังคอมพิวเตอร์ภายในกลุ่ม เพื่อให้สามารถรับจำนวนผู้ใช้งาน ที่เข้ามาใช้งานได้มากขึ้น หรือสามารถรับงานที่เข้ามาได้มากขึ้น นอกจากนั้นยังมีคุณสมบัติของ Fail Over คือหากมีคอมพิวเตอร์ภายในกลุ่มไม่สามารถทำงานได้เช่น Down อยู่หรือไม่สามารถรับโหลดเพิ่มได้เนื่องจาก Resource ที่ใช้ทำงานไม่พอ โหลดบาลานซ์เซิร์ฟเวอร์ที่เป็นตัวแจกโหลดให้คอมพิวเตอร์ภายในกลุ่มก็จะส่งโหลดไปยังคอมพิวเตอร์เครื่องอื่นๆแทนจนกว่าคอมพิวเตอร์เครื่องนั้นจะกลับมาใช้งานได้ใหม่

2.12.2 ระบบโหลดบาลานซ์ (Load Balance System)

ระบบโหลดบาลานซ์ (Load Balance System) เป็นระบบที่จะช่วยแก้ไขปัญหาการทำงานของระบบที่มีการใช้งานหนักได้เป็นอย่างดี โดยการทำโหลดบาลานซ์ คือการจัดกลุ่มของเซิร์ฟเวอร์หลายๆเครื่องเพื่อแบ่งงานกันทำหรือกระจายโหลดการใช้งานของผู้ใช้ ไปยังเซิร์ฟเวอร์เครื่องต่างๆภายในกลุ่มเพื่อรองรับการทำงาน เช่น เว็บไซต์ที่มีผู้เข้าชมจำนวนมากจะมีการเรียกใช้งาน Web Server, Database Server สูงจนทำให้เซิร์ฟเวอร์ เครื่องเดียวไม่สามารถรองรับการทำงานได้ทั้งหมด โหลดบาลานซ์สามารถรองรับกับจำนวนผู้ใช้งาน ที่เข้ามาใช้งานได้มากขึ้น ซึ่งปัญหาหลักๆของคนทำเว็บไซต์คือ จะทำอย่างไรให้ระบบสามารถรองรับการใช้งานของผู้ใช้งานจำนวนมากๆได้ และเทคนิคหนึ่งที่มีการใช้กันอย่างแพร่หลายก็คือการทำโหลดบาลานซ์

2.12.3 วิธีการกระจายภาระงานของโหลดบาลานซ์ (Load Balance)

2.12.3.1 แบบ Round Robin

วิธีการวนรอบ (Round robin) วิธีการนี้จะสลับการทำงานของแต่ละโหนดของเรียลเซิร์ฟเวอร์ (Real Server) แบบวนไปเรื่อยๆ เช่น ครั้งแรกใช้งานเครื่องที่ 1 ครั้งที่ 2 จะใช้งานเครื่องที่ 2 เมื่อครบรอบจะกลับมาเริ่มต้นใหม่อีกครั้ง ข้อดีของวิธีนี้คือง่ายที่สุดและใช้งบประมาณน้อยที่สุด แต่เป็นวิธีที่มีข้อเสียค่อนข้างมาก ข้อเสียที่สำคัญคือไม่สามารถควบคุมการทำงานได้ เนื่องจากการทำงานด้วยวิธีนี้จะมีแต่การทำวิธีการวนรอบเท่านั้น ไม่สามารถปิดการแบ่งโหลดการทำงานแบบเรียลไทม์ (Real-time) ได้และหากต้องการ Register Server เข้าไปในโหลดจะต้องใช้เวลานาน เพราะการทำ Mapping DNS นั้นจะมีการแคช ข้อมูลไว้ตามที่ต่างๆ ซึ่งเราไม่สามารถควบคุมได้

2.12.3..2 แบบ Weighted Round Robin

วิธีการวนรอบแบบถ่วงน้ำหนัก (Weighted Round Robin) วิธีการทำงานของวิธีนี้คือจะทำงานคล้ายกับวิธีการวนรอบ แต่เราสามารถที่จะทำการกระจายงานโดยคำนึงถึงประสิทธิภาพในการทำงานที่แตกต่างกันของเซิร์ฟเวอร์ต่างๆที่อยู่ในระบบโดยวิธีการนี้จะทำการกำหนดค่าตัวแบ่งน้ำหนักที่บ่งบอกถึงประสิทธิภาพในการทำงานของเซิร์ฟเวอร์แต่ละเครื่องที่อยู่ในระบบคลัสเตอร์โดยวิธีการนี้ไม่ได้คำนึงถึงจำนวนการติดต่อของแต่ละเซิร์ฟเวอร์ที่อยู่ในระบบ ซึ่งทำให้มี Overhead น้อย และส่งผลให้ระบบสามารถมีจำนวนเซิร์ฟเวอร์ภายในระบบคลัสเตอร์ได้มาก แต่วิธีการนี้อาจจะนำไปสู่การกระจายงานอย่างไม่สมดุลภายในระบบคลัสเตอร์ได้ถ้ามีภาระงานของการร้องขอบริการมีความแตกต่างกันมาก กล่าวคือภาระการร้องขอบริการจำนวนมากที่มีการทำงานมากอาจจะถูกส่งไปให้กับเซิร์ฟเวอร์เครื่องที่อยู่ภายในระบบว่าเครื่องอื่นได้การวนรอบแบบถ่วงน้ำหนัก เพื่อให้เครื่องกระจายงานในปริมาณที่เหมาะสมกับขีดความสามารถของเครื่องแต่ละเครื่องในระบบ เป็นต้น ใน

ส่วนนี้ถ้าเราออกแบบหรือใช้อัลกอริทึมที่เหมาะกับประเภทของงาน จะทำให้สามารถใช้ประสิทธิภาพของระบบได้เพิ่มมากขึ้น

2.12.3.3 แบบ Fast Response

ฟาสต์ เรสปอนส์(Fast Response) การกระจายโหลดแบบนี้จะพิจารณาถึงการตอบสนองทางเวลา (Response Time) ของระบบว่าเรียลเซิร์ฟเวอร์ ตัวใดมีเวลาในการตอบสนองที่เร็วที่สุด โหลดบาลานซ์เซิร์ฟเวอร์ก็จะทำการกระจายโหลดไปให้เรียลเซิร์ฟเวอร์ตัวนั้นก่อนที่จะกระจายโหลดไปให้ตัวต่อๆไปที่มีการตอบสนองทางเวลามากกว่า (การตอบสนองทางเวลา ที่มีค่าน้อยแสดงว่าใช้เวลาในการตอบสนองต่อระบบได้เร็ว) ซึ่งจากการกระจายโหลดแบบวิธีฟาสต์ เรสปอนส์ จะให้ระบบสามารถกระจายโหลดได้อย่างมีประสิทธิภาพมากขึ้น ทำให้เกิดความรวดเร็วในการส่งข้อมูล โดยการกระจายโหลดแบบนี้ เงื่อนไขที่พิจารณาได้ในระบบคือพิจารณาได้จากการทำโพลลิ้ง(Polling) ที่ได้ทำไปก่อนหน้านี้ ซึ่งการทำโพลลิ้งได้แสดงถึงการตอบสนองทางเวลา ของเรียลเซิร์ฟเวอร์แต่ละตัวทำให้การกระจายโหลดแบบ ฟาสต์ เรสปอนส์ นำเงื่อนไขนี้ไปใช้ได้

2.12.3.4 แบบ Least Connection

การเชื่อมต่อน้อยที่สุด (Least Connection) การกระจายโหลดแบบนี้พิจารณาถึงจำนวนภาระงานที่ เรียลเซิร์ฟเวอร์แต่ละตัวได้รับซึ่งในการกระจายโหลดของโหลดบาลานซ์เซิร์ฟเวอร์จะกระจายโหลดไปให้ เรียลเซิร์ฟเวอร์ตัวที่มีภาระงานน้อยที่สุดก่อน ส่วนตัวที่รับภาระงานเยอะก็หยุดกระจายโหลดชั่วคราวซึ่งโหลดบาลานซ์เซิร์ฟเวอร์จะพยายามกระจายโหลดไปให้แก่ เรียลเซิร์ฟเวอร์ในอัตราส่วนที่เหมาะสมตามประสิทธิภาพเครื่องของ เรียลเซิร์ฟเวอร์แต่ละตัว (ในกรณีที่เรียลเซิร์ฟเวอร์แต่ละตัวมีประสิทธิภาพในการทำงานต่างกัน) ในการกระจายโหลดแบบนี้จะทำให้การกระจายโหลดมีความสมดุลไม่ต้องรอว่า เรียลเซิร์ฟเวอร์ตัวใดตัวหนึ่งทำงานหนักอยู่แต่จะกระจายโหลดไปให้ตัวที่ทำงานน้อยๆ เรียลเซิร์ฟเวอร์ประสิทธิภาพสูงกว่าทำแทนซึ่งเป็น

การบริหารประสิทธิภาพของเครื่องเรียลเซิร์ฟเวอร์ แต่ละเครื่องให้ทำงานกับระบบได้สมดุลทำให้การส่งข้อมูลมีความเสถียรและรวดเร็วขึ้น ซึ่งจะสังเกตว่าการกระจายโหลดแบบนี้จะมีความคล้ายคลึงกับวิธีการกระจายโหลดแบบ Ratio (Weighted Round Robin) แต่แบบ Ratio จะเป็นแบบที่ผู้ดูแลระบบทำการประเมินประสิทธิภาพเองและเลือกอัตราส่วนการกระจายโหลดเอง แต่การกระจายโหลดแบบ การเชื่อมต่อน้อยที่สุด ระบบจะทำการวิเคราะห์ระบบเองและเลือกอัตราส่วนในการกระจายโหลดเองซึ่งจุดประสงค์ในการใช้งานของแต่ละระบบก็มีความแตกต่างกันไปขึ้นอยู่กับว่าการกระจายโหลดแบบไหนที่เหมาะสมกับระบบมากกว่าและให้ผลลัพธ์ตามที่ต้องการ

2.12.3.5 แบบ Policy Routing

โพลิซี เร้าติ้ง (Policy Routing) เป็นเทคนิคที่ใช้เพื่อการกำหนดเส้นทางและการตัดสินใจในการส่งข้อมูลหรือโหลดจากต้นทางไปยังปลายทางโดยผู้ดูแลระบบเป็นผู้กำหนดโพลิซี เร้าติ้ง โดยทั่วไปแล้วการหาเส้นทางในการส่งข้อมูลของอุปกรณ์ Layer 3 นั้นจะใช้ปลายทางของทราฟฟิคนั้นเป็นตัวตัดสินใจในการเลือกเส้นทางว่าจะส่งไปในเส้นทางใด เช่น ต้องการส่งข้อมูลไปยังเซิร์ฟเวอร์ ที่อยู่ต่างประเทศ เมื่อทราฟฟิคนั้นเดินทางมาถึงเราเตอร์ เราเตอร์ก็จะดูว่าปลายทางของทราฟฟิคนั้นสามารถส่งไปยังเส้นทางใดบนตัวมันได้บ้าง จากนั้นมันจึงจะทำการส่งทราฟฟิคไปยังเส้นทางที่ดีที่สุดเพื่อไปยังปลายทางที่ต้องการ แต่ด้วยการใช้งาน โพลิซี เร้าติ้ง เราจะสามารถใช้ต้นทาง (Source) หรือชนิดของทราฟฟิค ในการเลือกเส้นทางที่จะใช้ในการส่งข้อมูลได้ เช่น เราสามารถเลือกได้ว่าให้ ทราฟฟิคที่มีต้นทางเป็น 192.168.1.10 ถึง 192.168.1.20 ให้ไปใช้งานเส้นทางหนึ่ง ส่วนทราฟฟิค ชนิดอื่นๆก็ให้ใช้งานอีกเส้นทางหนึ่งได้

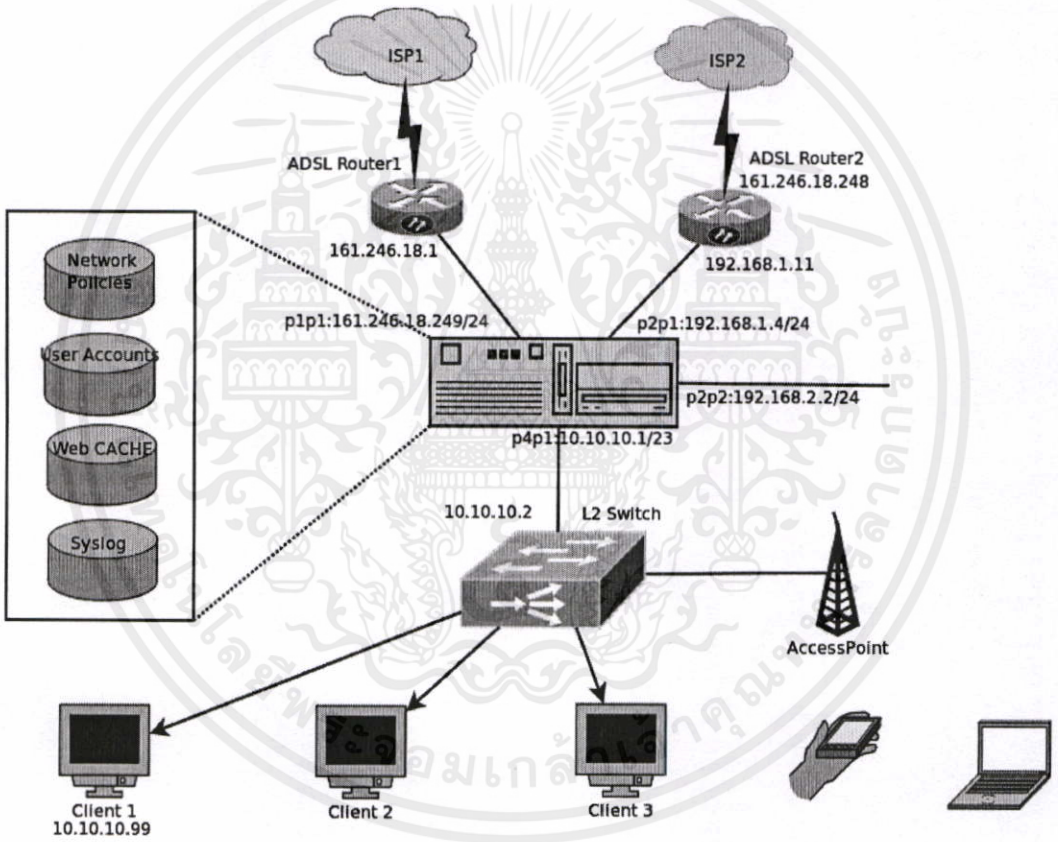
2.12.3.6 แบบ Link Backup

Link Backup เป็นรูปแบบการใช้งานอินเตอร์เน็ตโดยลิงค์สำรองจะทำงานก็ต่อเมื่อลิงค์หลักไม่สามารถใช้งานได้ โดยสามารถกำหนดแบนด์วิดท์ หรือความเร็วในการใช้งานอินเตอร์เน็ต (Internet Bandwidth) และรูปแบบการใช้งาน (Internet Application) ให้กับกลุ่มของผู้ใช้งานที่อยู่ในระบบเครือข่ายได้ เช่น กำหนดให้การใช้งานเว็บดาวน์โหลดข้อมูล ใช้งานที่ลิงค์ WAN1 เท่านั้น และ กำหนดให้การใช้งานรับ-ส่งอีเมลล์ ใช้งานที่ลิงค์ที่ WAN2 เท่านั้นหรือสามารถกำหนดความเร็วที่ต้องการให้ใช้งานได้ เช่น กำหนดให้ผู้ใช้งานไอพีแอดเดรสในช่วง 192.168.1.10 -192.168.1.20 ใช้งานเว็บที่ลิงค์ที่ 1 โดยสามารถใช้ความเร็วได้ในช่วง 512-1024 Kbps และผู้ใช้งานไอพีแอดเดรสในช่วง 192.168.1.21 - 192.168.1.100 ใช้งานเว็บที่ลิงค์ที่ 2 โดยสามารถใช้ความเร็วได้ในช่วง 512]– 2048 Kbps เป็นต้น

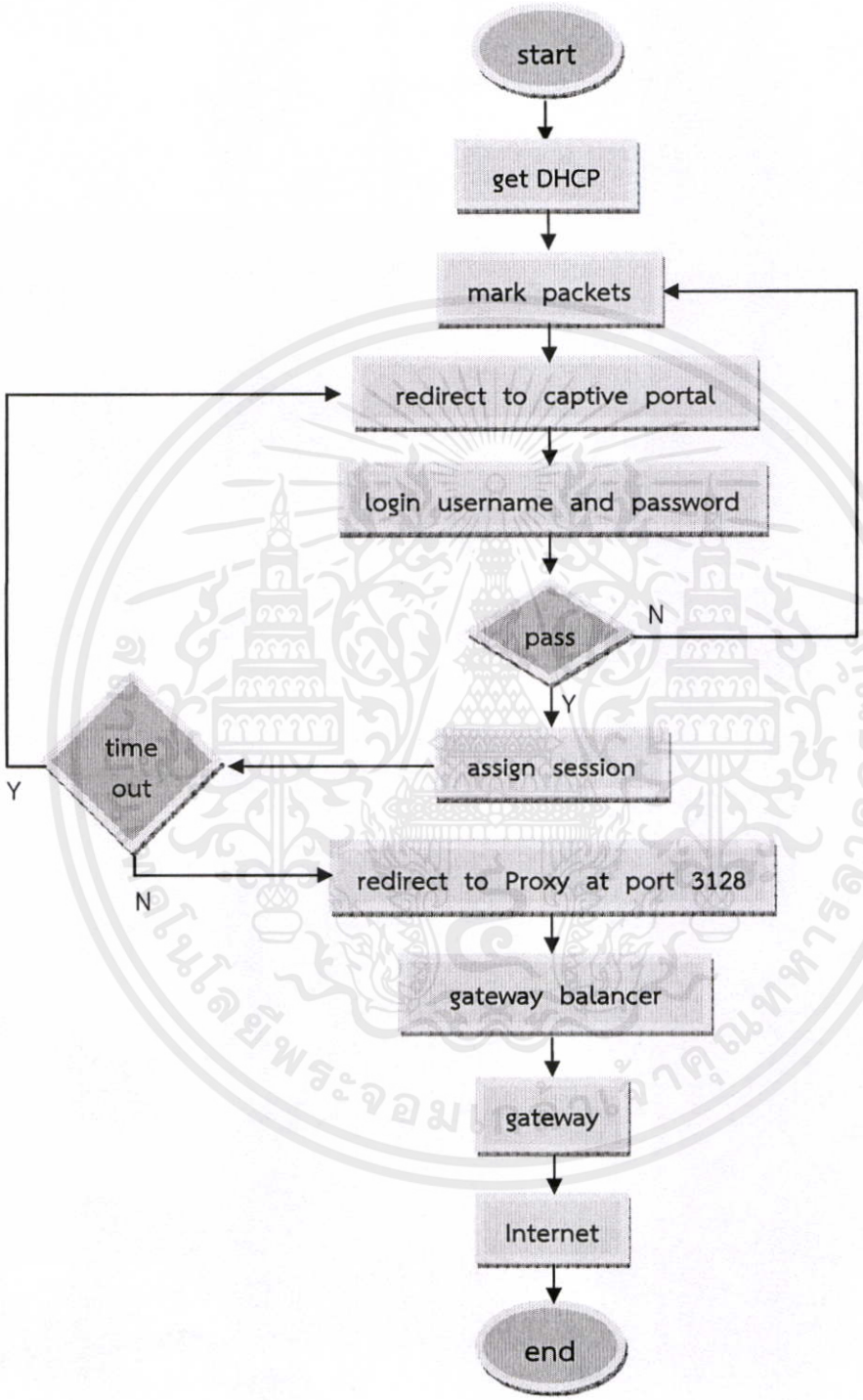
บทที่ 3
การออกแบบและการจัดทำปริญญานิพนธ์

3.1 การออกแบบ

ระบบบริหารจัดการในการเข้าถึงอินเตอร์เน็ตเป็นระบบที่ทำงานผ่านเซิร์ฟเวอร์โดยแบ่งออกเป็นฟังก์ชั่นและบริการต่างๆที่จำเป็นต่อการใช้งาน ดังรูปที่ 3.1 ซึ่งในการเข้าถึงอินเตอร์เน็ตจะต้องผ่านกระบวนการตามขั้นตอน ดังรูปที่ 3.2



รูปที่ 3.1 บริการที่มีอยู่ในเซิร์ฟเวอร์ของระบบ



รูปที่ 3.2 โฟลว์ชาร์ต (flowchart) การทำงานของระบบโดยรวม

3.1.1 การแจก DHCP

เมื่อผู้ใช้ทำการเข้าสู่เครือข่ายอินเตอร์เน็ต เซิร์ฟเวอร์จะทำการแจก DHCP ให้กับผู้ใช้บริการ ซึ่งได้แก่ IP address, Subnet mark, หมายเลข DNS และ Default gateway โดยมีคำสั่งในการแจก DHCP ดังรูปที่ 3.3

```
subnet 10.10.10.0 netmask 255.255.254.0 {
                range 10.10.10.11 10.10.11.250;
                option subnet-mask 255.255.254.0;
                option broadcast-address 10.10.11.255;
                option routers 10.10.10.1;
                option domain-name-servers 8.8.8.8;
}
```

รูปที่ 3.3 คำสั่งที่ใช้กำหนดจำนวนผู้ใช้ทั้งหมดที่สามารถใช้งานในเวลาเดียวกัน

3.1.2 ฟังก์ชั่นตรวจสอบสิทธิ์ของผู้ใช้ (Authentication)

ฟังก์ชันตรวจสอบสิทธิ์ของผู้ใช้ (Authentication) เป็นฟังก์ชันที่ใช้ในการระบุตัวตนของผู้ใช้ที่เข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต โดยระบบจะตรวจสอบว่ายูสเซอร์เนม (Username) และพาสเวิร์ด (Password) ที่ใช้ในการเข้าสู่ระบบนั้นถูกต้องหรือไม่ สิทธิ์ในการใช้อินเตอร์เน็ตหมดอายุแล้วหรือไม่ เพื่อยืนยันสิทธิ์และตัวตนของผู้ใช้ที่แท้จริง โดยจะมีขั้นตอนการทำงาน 2 ขั้นตอนดังนี้

3.1.2.1 กระบวนการทำเครื่องหมายแพ็กเก็ต (Mark Packet)

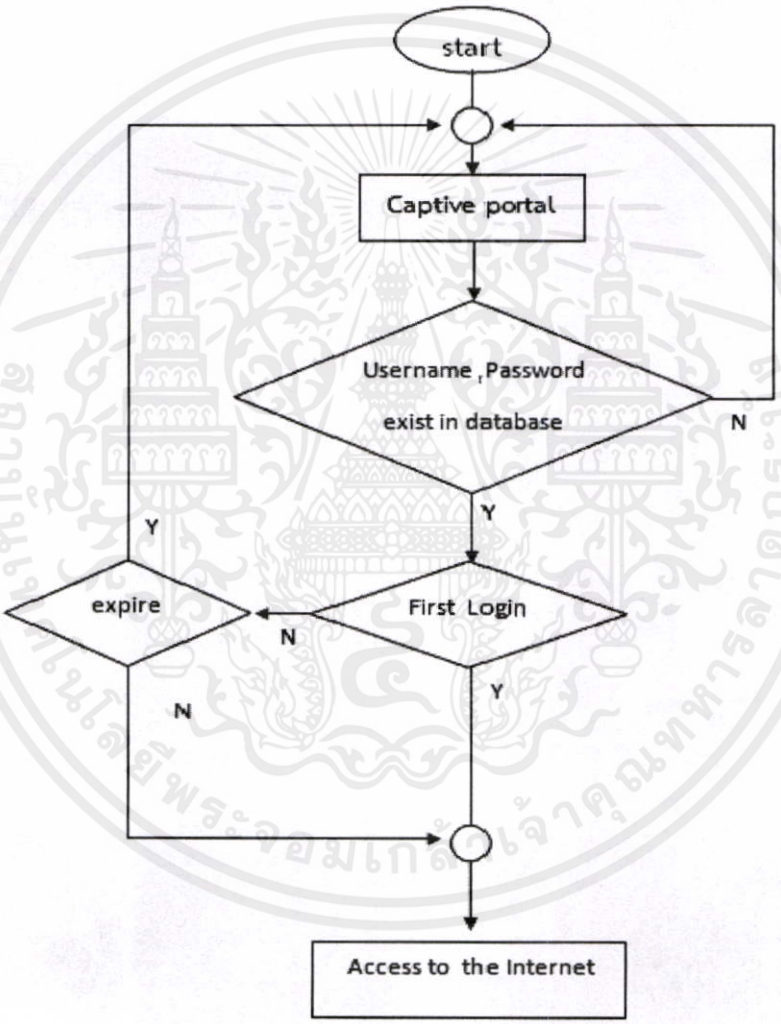
เมื่อมี IP Address ของผู้ใช้ผ่านเข้ามาในระบบ จะมีการทำเครื่องหมายให้กับแพ็กเก็ตของผู้ใช้เพื่อที่จะทำให้ผู้ใช้ถูกเปลี่ยนเส้นทางไปที่หน้าต่างสำหรับระบุตัวตน ซึ่งก็คือหน้าต่างล็อกอิน โดยมีคำสั่งของกระบวนการทำเครื่องหมายแพ็กเก็ตไว้ดังรูปที่ 3.4

```
$IPTABLES -t mangle -A internet -j MARK --set-mark 99
```

รูปที่ 3.4 คำสั่งสำหรับการทำเครื่องหมายให้กับแพ็กเก็ต

3.1.2.2 กระบวนการตรวจสอบสิทธิ์ของผู้ใช้บริการ

เมื่อเข้าสู่หน้าต่างสำหรับระบุตัวตน ผู้ใช้จะต้องทำการกรอกยูสเซอร์เนมและพาสเวิร์ด เพื่อตรวจสอบสิทธิ์ของผู้ใช้ ระบบจะทำการตรวจสอบยูสเซอร์เนมและพาสเวิร์ดว่าถูกต้องหรือไม่ รวมทั้งตรวจสอบสิทธิ์การใช้งานอินเตอร์เน็ตว่าหมดอายุแล้วหรือไม่ โดยมีกระบวนการตรวจสอบสิทธิ์ของผู้ใช้ดังรูปที่ 3.5



รูปที่ 3.5 โฟลว์ชาร์ตกระบวนการตรวจสอบสิทธิ์ของผู้ใช้บริการ

3.1.3 ระบบกำหนดเวลาในการล็อกอินเข้าใช้งานอินเตอร์เน็ตในหนึ่งครั้ง

การเข้าถึงอินเตอร์เน็ตของผู้ใช้จะต้องมีการกำหนดเวลาในการใช้งานเพื่อให้ผู้อื่นสามารถเข้าใช้งานอินเตอร์เน็ตได้เมื่อเวลาในการใช้งานของผู้ใช้รายเดิมหมดลง โดยมีคำสั่งของระบบกำหนดเวลาในการใช้งานอินเตอร์เน็ตไว้ดังรูปที่ 3.6

```
$min=300;
//$atime = strtotime(" 0 days 0 hours $min minutes 0 seconds");
```

รูปที่ 3.6 คำสั่งกำหนดระยะเวลาในการล็อกอินเข้าใช้งานอินเตอร์เน็ตในหนึ่งครั้ง

3.1.4 ฟังก์ชั่นพรอกซี (Proxy)

เป็นฟังก์ชันที่มีพื้นที่สำหรับเก็บออบเจ็กต์ของเว็บชั่วคราว เช่น เอกสาร HTML สำหรับการเรียกใช้ในภายหลัง จะใช้พอร์ต 3128 ในการเรียกใช้งานพรอกซี ซึ่งสามารถลดการใช้แบนด์วิดท์ของระบบ และลดความแออัดในการสื่อสารข้อมูลในเครือข่ายเพราะการตอบสนองของในการเรียกใช้ข้อมูลที่ถูกเก็บไว้โดยฟังก์ชันพรอกซีจะทำได้ทันที และอยู่ใกล้กับตัวไคลเอนต์ (Client) โดยมีคำสั่งการแบ่งหน่วยความจำสำหรับเก็บอ็อบเจกต์ของเว็บไซต์ของฟังก์ชันพรอกซีดังรูปที่ 3.7

```
cache_dir diskd /webcache 737280 720 2048
cache_mem 1056 MB
```

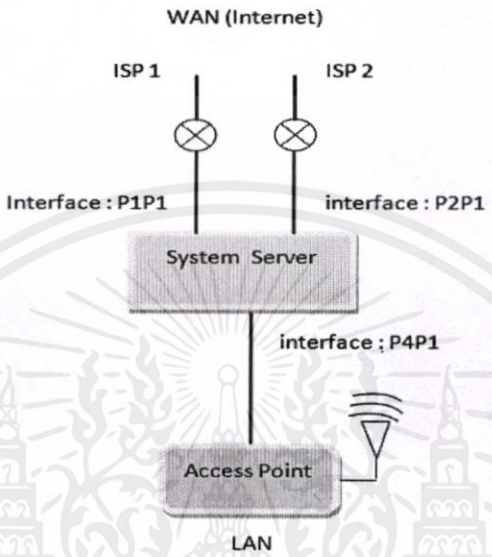
รูปที่ 3.7 คำสั่งในการแบ่งหน่วยความจำสำหรับเก็บอ็อบเจกต์ของเว็บไซต์

3.1.5 ฟังก์ชั่น Multiple-gateways (Gateway balancer)

การเข้าถึงข้อมูลอินเตอร์เน็ตของผู้ใช้โดยปกติจะทำการสื่อสารข้อมูลระหว่างโครงข่าย LAN กับโครงข่าย WAN ผ่านทางอินเตอร์เฟส (Interface) p4p1 และ p1p1 แต่สำหรับการสร้างฟังก์ชัน Multiple-gateway ในที่นี้จะใช้ช่องทางในการสื่อสารข้อมูลในด้านโครงข่าย WAN เพิ่มเป็น 2 ช่องทางคือ p1p1 และ p2p1 ดังรูปที่ 3.8

การใช้สองช่องทางในการสื่อสารข้อมูลฝั่งโครงข่าย WAN มีจุดประสงค์เพื่อใช้สำหรับรับส่งแพ็กเก็ตของข้อมูลในสองช่องทางอย่างเหมาะสม เป็นการใช้แบนด์วิดท์อย่างมีประสิทธิภาพและช่วยลดความเสี่ยงเมื่อเกิดการชำรุดของสาย ซึ่งถ้าเกิดการชำรุดของสายใดสายหนึ่งในฝั่ง

โครงข่าย WAN ระบบก็ยังคงสามารถทำงานต่อไปได้ ในที่นี้ได้ใช้รูปแบบการกระจายแพ็กเก็ตแบบ Weighted Round Robin



รูปที่ 3.8 ช่องทางในการรับส่งข้อมูลของเซิร์ฟเวอร์

การสื่อสารข้อมูลทางโครงข่าย WAN หรืออินเตอร์เน็ตเป็นการสื่อสารผ่าน 2 อินเตอร์เฟสคือ p1p1 และ p2p1 ซึ่งได้ทำเครื่องหมาย “1” และ “2” ให้กับแพ็กเก็ตตัวแรกของแต่ละคอนเน็คชั่น (connection) ที่เข้ามายังเซิร์ฟเวอร์ ทำในลักษณะแบบสุ่มด้วยค่าความน่าจะเป็นเท่ากับ 0.5 ดังคำสั่งในรูปที่ 3.9

```
SIPTABLES -t mangle -A FORWARD -m state --state new -j MARK --set-mark 2
SIPTABLES -t mangle -A FORWARD -m state --state new -m statistic --mode random
--probability 0.5 -j MARK --set-mark 1
```

รูปที่ 3.9 คำสั่งสำหรับการสุ่มทำเครื่องหมายให้กับแพ็กเก็ตเพื่อกระจายเส้นทาง

หลังจากที่แพ็กเก็ตถูกทำเครื่องหมายแล้วก็จะถูกส่งออกไปยังอินเตอร์เน็ต โดยแพ็กเก็ตที่ถูกทำเครื่องหมาย “1” จะถูกส่งออกทางอินเตอร์เฟส p1p1 ส่วนแพ็กเก็ตที่ถูกทำเครื่องหมาย “2” จะถูกส่งออกทางอินเตอร์เฟส p2p1 กำหนดด้วยคำสั่งดังรูปที่ 3.10

```
${RUN_IP} rule add fwmark 1 table ${TA1}
${RUN_IP} rule add fwmark 2 table ${TA2}
```

รูปที่ 3.10 คำสั่งการกำหนดเส้นทางของแพ็กเก็ตที่ถูกทำเครื่องหมาย

การส่งข้อมูลแพ็กเก็ตผ่านอินเตอร์เฟส p1p1 และ p2p1 สามารถกำหนดค่า weight ในการส่งข้อมูลของแต่ละอินเตอร์เฟสดังรูปที่ 3.11 ในที่นี้ได้กำหนดค่า weight ของแต่ละอินเตอร์เฟสเท่ากับ 1 กล่าวคือ จะมีการส่งข้อมูลผ่านแต่ละอินเตอร์เฟสในปริมาณของคอนเน็คชั่นที่เท่ากัน โดยค่า weight สามารถกำหนดเองได้

```
${RUN_IP} route add default scope global nexthop via ${GW1} dev
${POT1} weight 1 nexthop via ${GW2} dev ${POT2} weight 1
```

รูปที่ 3.11 คำสั่งกำหนดค่า weight ในการส่งแพ็กเก็ต

3.1.6 การกำหนดเส้นทางผ่านเกตเวย์ (Access Gateway)

เป็นการกำหนดตารางไอพีที่ใช้ NAT (Network Address Translation) ทำหน้าที่กำหนดเส้นทางของข้อมูล เป็นเสมือนไฟร์วอลล์ทางอ้อมของระบบ โดยมีคำสั่งการกำหนดเส้นทางผ่านเกตเวย์ดังรูปที่ 3.12

```
$IPTABLES -t nat -A POSTROUTING -s $LOCALNET0 -o p1p1 -j SNAT --to $WanIP1
$IPTABLES -t nat -A POSTROUTING -s $LOCALNET0 -o p2p1 -j SNAT --to $WanIP2
```

รูปที่ 3.12 คำสั่งการกำหนดเส้นทางผ่านเกตเวย์

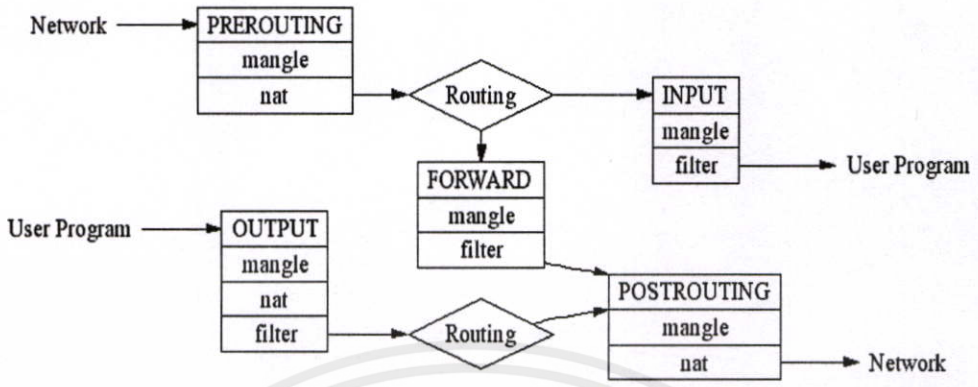
3.1.7 ฟังก์ชั่น Network Security

ระบบบริหารจัดการในการเข้าถึงข้อมูลอินเตอร์เน็ตจำเป็นต้องมีการป้องกันการถูกคุกคามจากภายนอกเข้าสู่เซิร์ฟเวอร์ของระบบ ซึ่งทำได้โดยการกำหนดพอร์ต (port) การทำงานต่างๆที่สำคัญในการสื่อสารระหว่างเซิร์ฟเวอร์ของระบบกับคอมพิวเตอร์ภายนอก ดังตารางที่ 3.1

ตารางที่ 3.1 พอร์ตที่ใช้ในการสื่อสารข้อมูลระหว่างเซิร์ฟเวอร์ของระบบกับคอมพิวเตอร์ภายนอก

พอร์ต	โพรโตคอล	หน้าที่
22	TCP	เป็นพอร์ตมาตรฐานของโปรโตคอล SSH
389	TCP	เป็นพอร์ตที่ใช้เชื่อมต่อไปหา Active Directory
3128	TCP	เป็นพอร์ตการทำงานของ Proxy
3130	TCP	เป็นพอร์ตการทำงานของ Proxy
1812	TCP/UDP	เป็นพอร์ตการทำงานของ RADIUS โดยใช้สำหรับ RADIUS authentication
1813	TCP/UDP	เป็นพอร์ตการทำงานของ RADIUS โดยใช้สำหรับ RADIUS accounting
53	UDP	เป็นพอร์ตการทำงานของ DNS
80	TCP	เป็นพอร์ตมาตรฐานของโปรโตคอล http
443	TCP/UDP	เป็นพอร์ตมาตรฐานของโปรโตคอล https
-	ICMP	เป็นโปรโตคอลควบคุมและรายงานความผิดพลาดระหว่าง host server กับ gateway บนอินเตอร์เน็ต

การทำงานของฟังก์ชั่นไฟร์วอลล์จะมีการจัดการแพ็กเก็ตตามลำดับดังรูปที่ 3.13 ซึ่งเซิร์ฟเวอร์ของระบบเทียบได้กับตำแหน่ง User Program โดยมีคำสั่งการทำงานดังรูปที่ 3.14



รูปที่ 3.13 IP Table Packet Flow

$IPTABLES -A INPUT -p tcp --dport 22 -j ACCEPT	$IPTABLES -A OUTPUT -p tcp --sport 22 -j ACCEPT
$IPTABLES -A INPUT -p tcp --sport 389 -j ACCEPT	$IPTABLES -A OUTPUT -p tcp --dport 389 -j ACCEPT
$IPTABLES -A INPUT -p tcp --dport 3128 -j ACCEPT	$IPTABLES -A OUTPUT -p tcp --sport 3128 -j ACCEPT
$IPTABLES -A INPUT -p tcp --dport 3130 -j ACCEPT	$IPTABLES -A OUTPUT -p tcp --sport 3130 -j ACCEPT
$IPTABLES -A INPUT -p tcp --dport 1812 -j ACCEPT	$IPTABLES -A OUTPUT -p tcp --sport 1812 -j ACCEPT
$IPTABLES -A INPUT -p tcp --dport 1813 -j ACCEPT	$IPTABLES -A OUTPUT -p tcp --sport 1813 -j ACCEPT
$IPTABLES -A INPUT -p udp --dport 1812 -j ACCEPT	$IPTABLES -A OUTPUT -p udp --sport 1812 -j ACCEPT
$IPTABLES -A INPUT -p udp --dport 1813 -j ACCEPT	$IPTABLES -A OUTPUT -p udp --sport 1813 -j ACCEPT
$IPTABLES -A INPUT -p udp --sport 53 -j ACCEPT	$IPTABLES -A OUTPUT -p udp --dport 53 -j ACCEPT
$IPTABLES -A INPUT -p tcp --sport 80 -j ACCEPT	$IPTABLES -A OUTPUT -p tcp --dport 80 -j ACCEPT
$IPTABLES -A INPUT -p tcp --dport 80 -j ACCEPT	$IPTABLES -A OUTPUT -p tcp --sport 80 -j ACCEPT
$IPTABLES -A INPUT -p udp --sport 443 -j ACCEPT	$IPTABLES -A OUTPUT -p tcp --dport 443 -j ACCEPT
$IPTABLES -A INPUT -p tcp --dport 443 -j ACCEPT	$IPTABLES -A OUTPUT -p tcp --sport 443 -j ACCEPT
$IPTABLES -A INPUT -p icmp -j ACCEPT	$IPTABLES -A OUTPUT -p icmp -j ACCEPT
	$IPTABLES -A OUTPUT -p all -j DROP

รูปที่ 3.14 คำสั่งในการกำหนดพอร์ตการใช้งาน

3.1.8 ฟังก์ชัน Graphical User Interface (GUI)

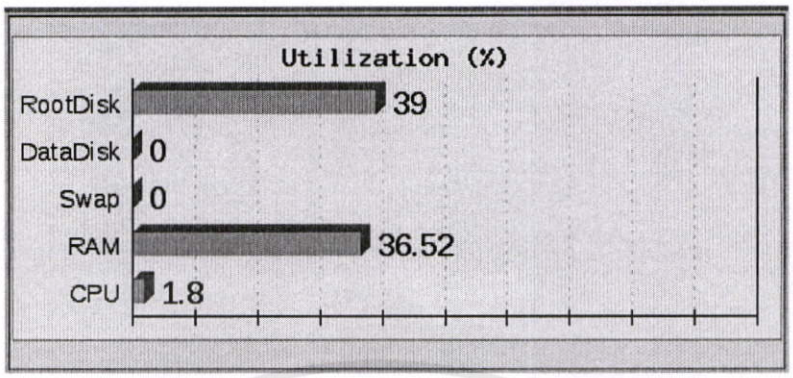
ในหัวข้อนี้จะแบ่งการทำงานของฟังก์ชันออกเป็นสองส่วนคือส่วนแสดงผลและส่วนควบคุม ซึ่งส่วนแสดงผลจะให้ข้อมูลในรูปของแผนภูมิ กราฟและตาราง โดยส่วนของแผนภูมิและกราฟจะแสดงผลแบบเรียลไทม์

3.1.8.1 ส่วนแสดงผล

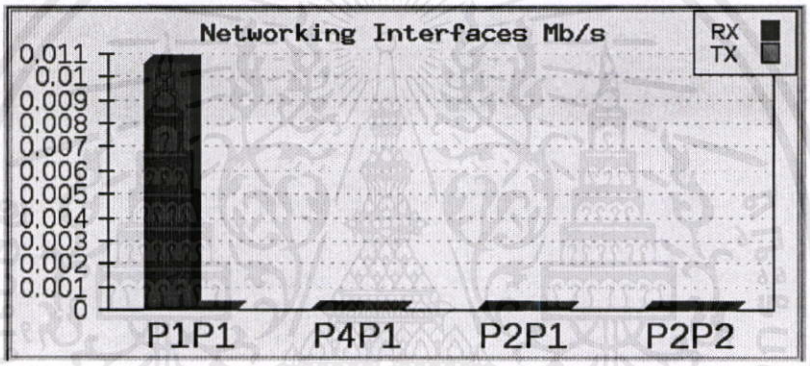
1. แผนภูมิแสดงค่าเปอร์เซ็นต์การใช้หน่วยความจำและหน่วยประมวลผล ดังรูปที่ 3.15
2. แผนภูมิแสดงค่าความเร็วของข้อมูลที่ผ่านแต่ละอินเตอร์เฟส ดังรูปที่ 3.16
3. แผนภูมิแสดงค่าเปอร์เซ็นต์การใช้โปรโตคอลและพอร์ตต่างๆ ดังรูปที่ 3.17
4. แผนภูมิบอกจำนวนผู้ใช้ที่ล็อกอินเข้าใช้งานอินเตอร์เน็ต ดังรูปที่ 3.18
5. แสดง IP Address และ Network Mask ของแต่ละอินเตอร์เฟส ดังรูปที่ 3.19
6. แสดง login users ที่กำลังใช้งานอินเตอร์เน็ตผ่านบริการของระบบ ดังรูปที่ 3.20
7. กราฟค่าความเร็วของข้อมูลที่ผ่านแต่ละอินเตอร์เฟสใน 60 นาทีก่อนหน้า ดังรูปที่ 3.21
8. กราฟค่าความเร็วของข้อมูลที่ผ่านแต่ละอินเตอร์เฟสใน 30 วันก่อนหน้า ดังรูปที่ 3.22
9. กราฟค่าความเร็วของข้อมูลที่ผ่านแต่ละอินเตอร์เฟสใน 24 ชั่วโมงก่อนหน้า ดังรูปที่ 3.23
10. กราฟค่าความเร็วของข้อมูลที่ผ่านแต่ละอินเตอร์เฟสใน 12 เดือนก่อนหน้า ดังรูปที่ 3.24

3.1.8.2 ส่วนควบคุม

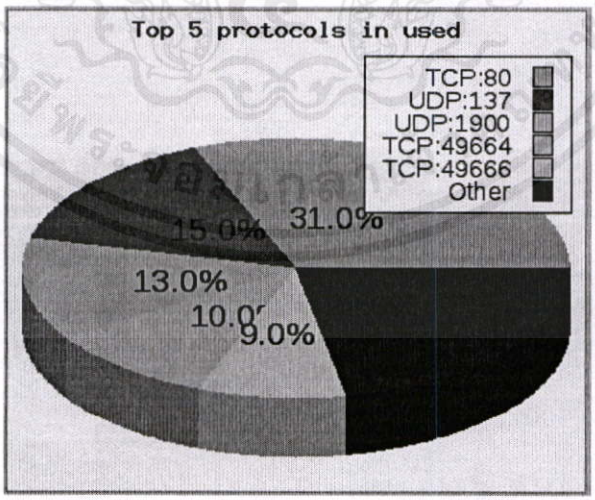
1. หน้าต่างสำหรับการสั่งปิดเครื่อง(shutdown) รีสตาร์ท(restart) หรือไปสู่หน้าแอคเคานท์ (account) ดังรูปที่ 3.25
2. หน้าต่างสำหรับกำหนดสถานะการทำงานของฟังก์ชัน ดังรูปที่ 3.26
3. หน้าต่างสำหรับการกำหนดค่า weight ในการส่งข้อมูล ดังรูปที่ 3.27
4. หน้าต่างสำหรับการกีดกันเว็บไซต์ที่ไม่ต้องการให้ผู้ใช้เข้าถึง ดังรูปที่ 3.28
5. หน้าต่างสำหรับกำหนดค่า IP Address ที่จะทำการบายพาส (bypass) ดังรูปที่ 3.29



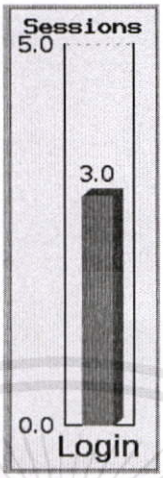
รูปที่ 3.15 แผนภูมิค่าเปอร์เซ็นต์การใช้หน่วยความจำและหน่วยประมวลผล



รูปที่ 3.16 แผนภูมิค่าความเร็วของข้อมูลที่ผ่านแต่ละอินเตอร์เฟส



รูปที่ 3.17 แผนภูมิค่าเปอร์เซ็นต์การใช้โปรโตคอลและพอร์ตต่างๆ



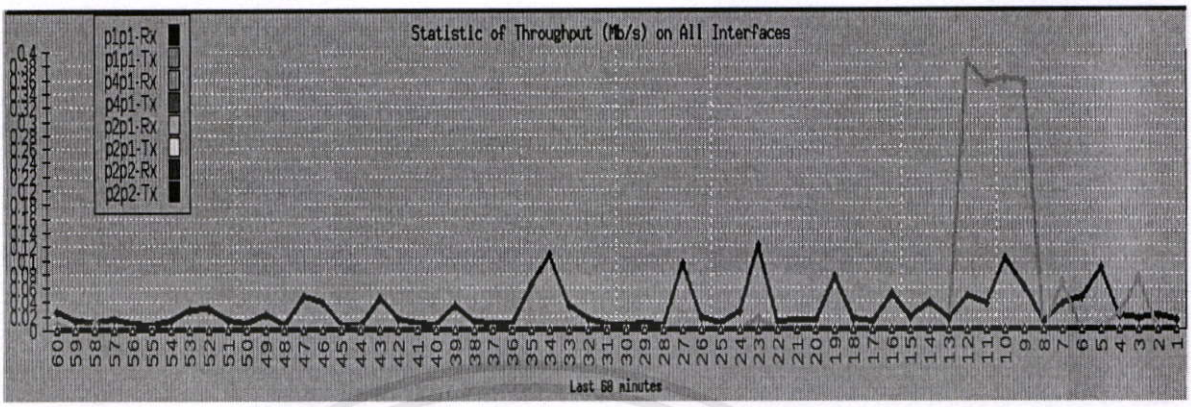
รูปที่ 3.18 แผนภูมิบอกจำนวนผู้ใช้ที่ได้ล็อกอินเข้าใช้งานอินเตอร์เน็ต

Interfaces Information		
Interface	IP Address	Network Mask
p1p1	161.246.18.249	255.255.255.0
p4p1	10.10.10.1	255.255.254.0
p2p1	192.168.1.2	255.255.255.0
p2p2	192.168.2.2	255.255.255.0

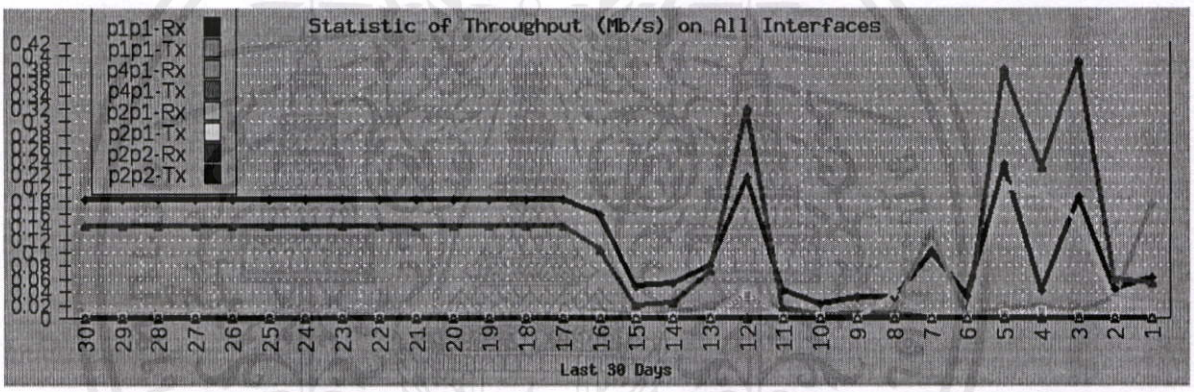
รูปที่ 3.19 IP Address และ Network Mask ของแต่ละอินเตอร์เฟส

Concurrent Login Users				
No.	Login	From	Exp	etc
1	user4	10.10.10.17	20150412160044	End
2	user4	10.10.10.17	20150412180033	End
3	user4	10.10.10.17	20150412181735	End
4	user2	10.10.10.19	20150412182433	End
5	user3	10.10.10.18	20150412190352	End

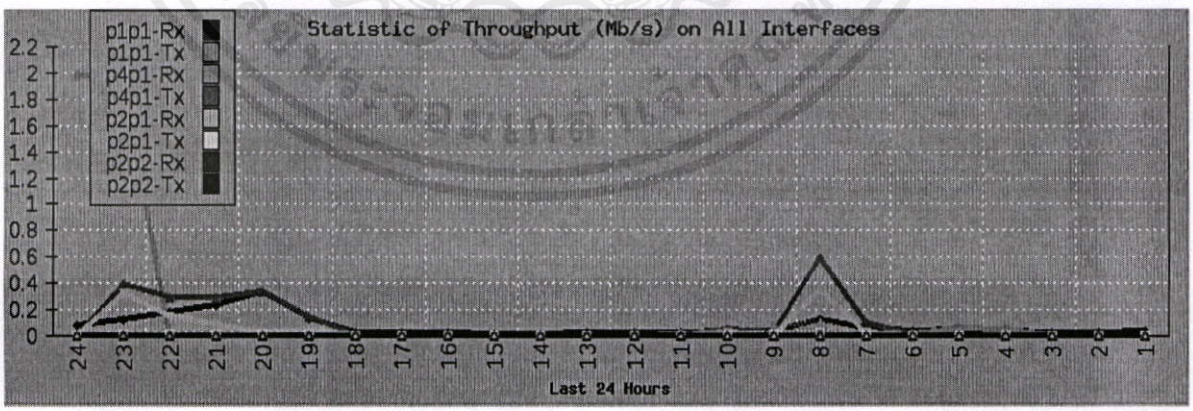
รูปที่ 3.20 login users ที่กำลังใช้งานอินเตอร์เน็ตผ่านบริการของระบบ



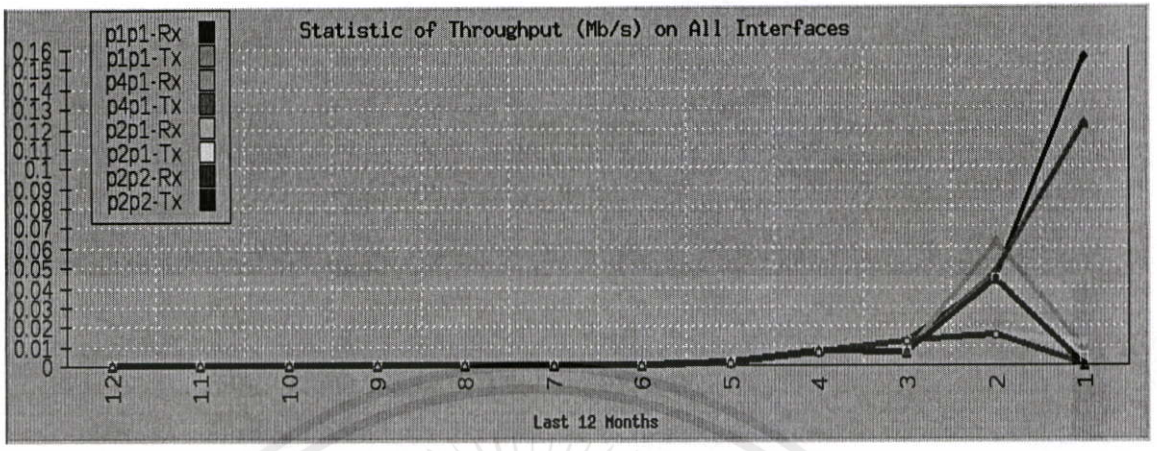
รูปที่ 3.21 กราฟค่าความเร็วของข้อมูลที่ผ่านแต่ละอินเตอร์เฟสใน 60 นาทีก่อนหน้า



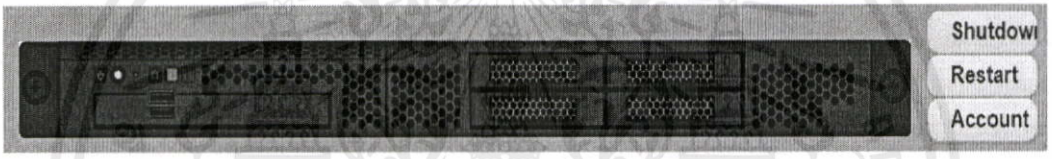
รูปที่ 3.22 กราฟค่าความเร็วของข้อมูลที่ผ่านแต่ละอินเตอร์เฟสใน 30 วันก่อนหน้า



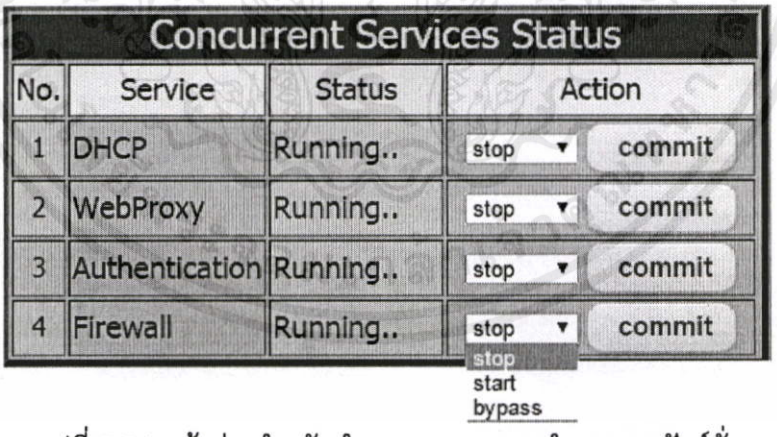
รูปที่ 3.23 กราฟค่าความเร็วของข้อมูลที่ผ่านแต่ละอินเตอร์เฟสใน 24 ชั่วโมงก่อนหน้า



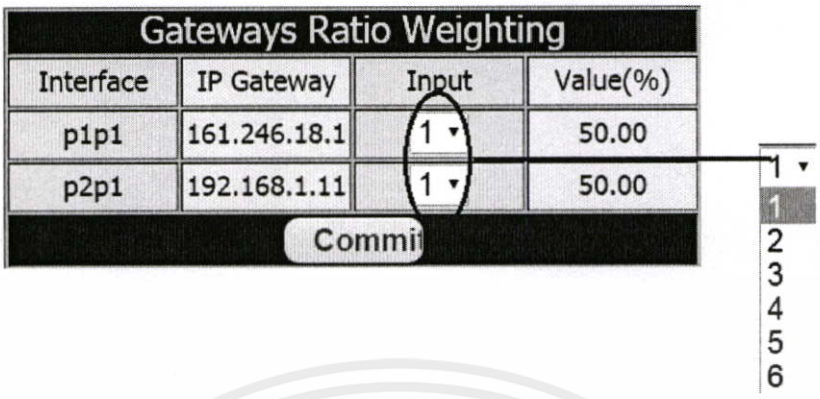
รูปที่ 3.24 กราฟค่าความเร็วของข้อมูลที่ผ่านแต่ละอินเตอร์เฟสใน 12 เดือนก่อนหน้า



รูปที่ 3.25 หน้าต่างสำหรับการสั่งปิดเครื่อง (shutdown) รีสตาร์ท(restart) หรือไปสู่หน้าแอ็คเคาน์ (account)

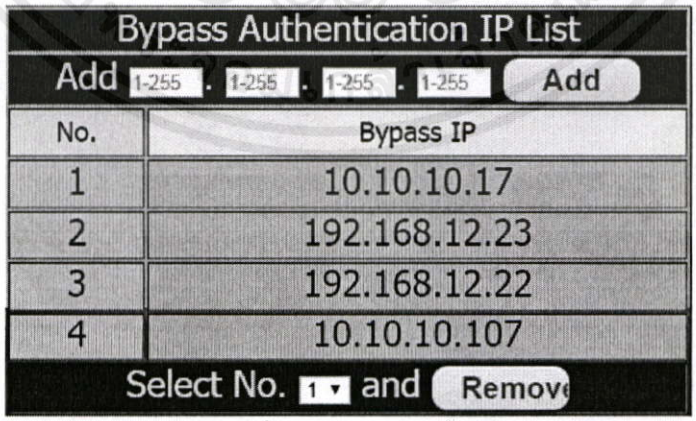


รูปที่ 3.26 หน้าต่างสำหรับกำหนดสถานะการทำงานของฟังก์ชั่น



รูปที่ 3.27 หน้าต่างสำหรับการกำหนดค่า weight ในการส่งข้อมูล

รูปที่ 3.28 หน้าต่างสำหรับการกีดกันเว็บไซต์ที่ไม่ต้องการให้ผู้ใช้เข้าถึง



รูปที่ 3.29 หน้าต่างสำหรับกำหนดค่า IP Address ที่จะทำการบายพาส

3.2 เครื่องมือที่ใช้ในการทดลอง

3.2.1 ฮาร์ดแวร์ (Hardware)

1.) เครื่องแม่ข่าย (server) จำนวน 1 เครื่อง
   - 1.1) บอร์ด (sever) dual interface USB 3.0 จำนวน 1 เครื่อง
   - 1.2) power supply จำนวน 1 ตัว
   - 1.3) Harddisk จำนวน 1 ตัว
   - 1.4) 32bit PCI Riser Card จำนวน 1 ตัว

2.) คอมพิวเตอร์โน้ตบุ๊ก (notebook) จำนวน 1 เครื่อง
3.) switch 10/100 จำนวน 1 เครื่อง
4.) สายสัญญาณ UTP จำนวน 3 เส้น
5.) wifi – router จำนวน 1 เครื่อง

3.2.2 ซอร์ฟแวร์ (Software)

1.) โปรแกรม Putty
2.) โปรแกรม FileZilla
3.) ระบบปฏิบัติการ Linux Ubuntu Server
4.) ระบบปฏิบัติการ window 7
5.) โปรแกรม Squid 3.7
6.) โปรแกรม Apache

3.3 การจัดเก็บผลการทดลอง

3.3.1 การออกแบบการทดลองของฟังก์ชั่น Authentication

ทำการทดลองสร้างแอคเคานท์เข้าไปในระบบโดยแบ่งออกเป็น 2 ส่วนได้แก่ ส่วนสำหรับลงทะเบียนผู้ใช้งานอินเตอร์เน็ตรายบุคคลและส่วนสำหรับลงทะเบียนเพื่อสร้างแอคเคานท์แบบกลุ่ม จากนั้นทำการกรอกยูสเซอร์เนมและพาสเวิร์ดโดยอาศัยข้อมูลตามตารางที่ 3.2

ตารางที่ 3.2 ฐานข้อมูลยูเซอร์เนมและพาสเวิร์ดของระบบ

Use / Password	User1	User2	User3	User4
Pin1				
Pin2				
Pin3				
Pin4				

ผู้ใช้ต้องกรอกยูสเซอร์เนมและพาสเวิร์ดที่ตรงตามสีเขียวจึงจะสามารถเข้าใช้งานระบบได้ แต่ถ้าผู้ใช้กรอกยูสเซอร์เนมและพาสเวิร์ดไม่ตรงตามข้อมูลในช่องสีเขียวหรือเป็นข้อมูลที่ไม่อยู่ในตาราง ผู้ใช้จะไม่สามารถเข้าใช้งานระบบได้

3.3.2 การออกแบบการทดลองของฟังก์ชั่น Web Caching (Proxy)

3.3.2.1 ทำการทดลอง TCP_MISS และ TCP_ HIT

ถ้าเซิร์ฟเวอร์ของระบบเก็บออบเจ็กต์ของเว็บไซต์ที่กำลังเข้าถึงจะแสดงผลเป็น TCP_HIT แต่ถ้าออบเจ็กต์ของเว็บไซต์ที่ทำการเข้าถึงไม่ได้อยู่ในเซิร์ฟเวอร์ของระบบจะแสดงผลเป็น TCP_MISS

3.3.2.2 ทำการทดลองวัดเวลาในการเข้าถึงหน้าเว็บไซต์ที่ต้องการ

ทำการทดลองเข้าเว็บไซต์ที่เป็น TCP_MISS แล้วทำการจับเวลา ต่อมาทำการเข้าเว็บไซต์เดิมที่เป็น TCP_HIT แล้วทำการจับเวลา จากนั้นทำการทดลองในลักษณะเดิมกับเว็บไซต์อื่นๆรวมทั้งหมด 4 เว็บไซต์

3.3.3 การออกแบบการทดลองของฟังก์ชั่น Multiple-Gateways

ทำการกำหนดค่า weight จากหน้าต่างสำหรับการกำหนดค่า weight ในการส่งข้อมูลที่ส่วนของจียูไอ จากนั้นทำการเข้าสู่อินเตอร์เน็ต บันทึกผลการทดลองโดยสังเกตผลจากส่วนของจียูไอ

3.3.4 การออกแบบการทดลองของฟังก์ชั่น Graphical User Interface (GUI)

เข้าไปที่หน้าจียูไอแล้วทำการทดสอบการทำงานของส่วนควบคุมต่างๆ จากนั้นทำการสังเกตผลที่เกิดขึ้นพร้อมทั้งบันทึกผลการทดลอง

บทที่ 4

ผลการทดลอง

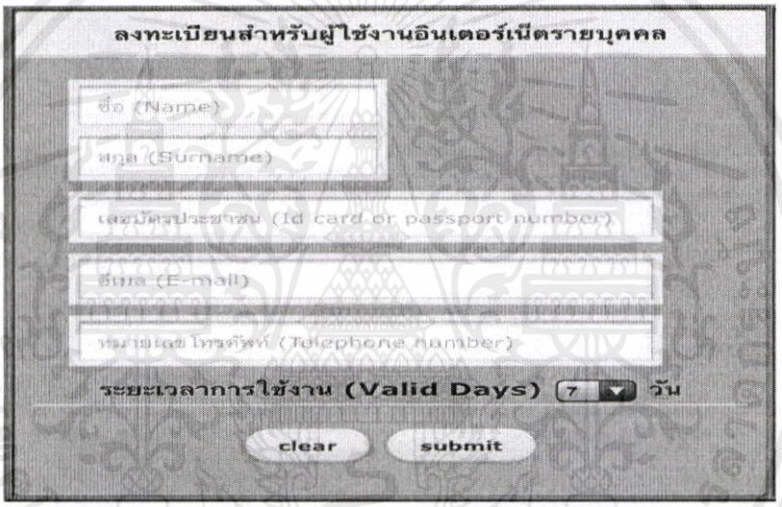
ผลการทดลอง

4.1. การทดลองของฟังก์ชัน Authentication

4.1.1ทำการทดลองการสร้างแอคเคาท์ (Account)

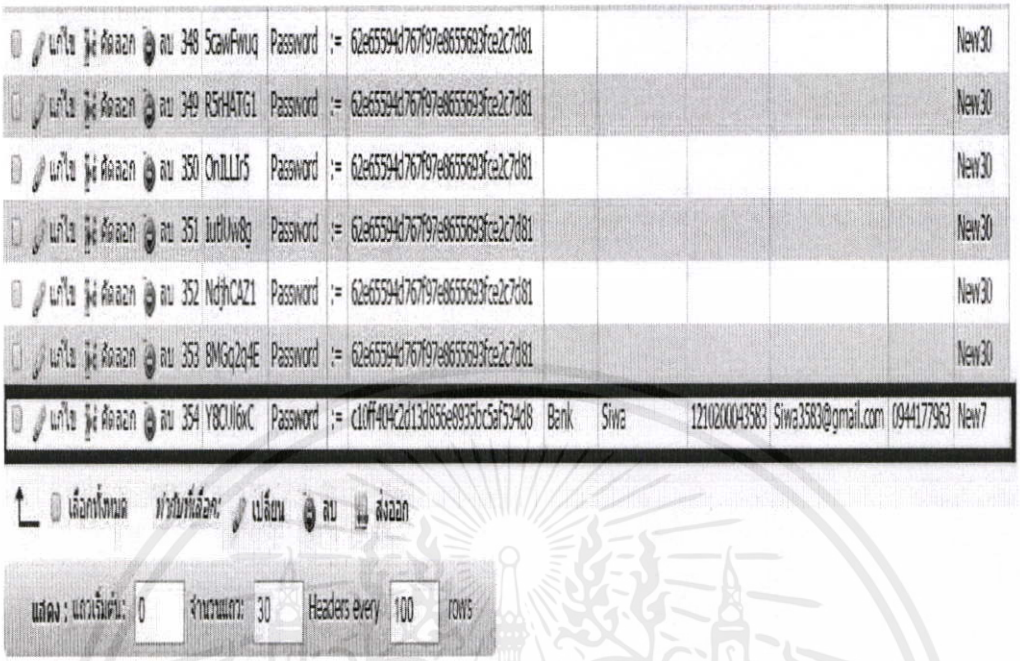
เข้าไปในระบบ โดยแบ่งออกเป็น 2 ส่วนดังนี้ ส่วนที่1 ลงทะเบียนสำหรับผู้ใช้งานอินเตอร์เน็ตรายบุคคล ส่วนที่2 ลงทะเบียนสำหรับสร้างแอคเคาท์แบบกลุ่ม

ทำการสร้างแอคเคาท์ลงทะเบียนสำหรับผู้ใช้รายบุคคล



รูปที่ 4.1 หน้าต่างรับข้อมูลของผู้ใช้

รูปที่ 4.2 ตัวอย่างการสร้างแอคเคาท์ผู้ใช้รายบุคคล



รูปที่ 4.3 ข้อมูลของผู้ใช้งานถูกนำไปเก็บในดาต้าเบส (Database)

ลงทะเบียนสำหรับสร้างแอคเคาท์แบบกลุ่ม

รูปที่ 4.4 หน้าต่างรับข้อมูลของผู้ใช้แบบกลุ่ม

รูปที่ 4.5 ตัวอย่างการสร้างแอคเคาท์ผู้ใช้แบบกลุ่ม

โดยการสร้างแอคเคาท์ใหม่เข้าไปในระบบจะกำหนดให้ผู้ใช้กลุ่มนี้จะมีจำนวณผู้ใช้เท่ากับ 15 ผู้ใช้ สามารถอยู่ในระบบใช้งานได้นาน 30 วัน

แก้ไข คัดลอก ลบ	337	6defHlA	Password	:=	01d656e8c5ce36ee530484bc3da0b4f2	MyGuest	6Desa	1123581321	kas@hotmail.com	122112	20150415
แก้ไข คัดลอก ลบ	338	NYeiuPfK	Password	:=	06ab4e7051429af7fcccd0f8d8e7f025	Siwa	pathumchumpu	3312	siwa@google.co.th	1122112	New30
แก้ไข คัดลอก ลบ	339	QAKzrPJ7	Password	:=	62e65594d767f97e8655693fce2c7d81						New30
แก้ไข คัดลอก ลบ	340	CvSHpWDV	Password	:=	62e65594d767f97e8655693fce2c7d81						New30
แก้ไข คัดลอก ลบ	341	RZQptmaB	Password	:=	62e65594d767f97e8655693fce2c7d81						New30
แก้ไข คัดลอก ลบ	342	TjB70343	Password	:=	62e65594d767f97e8655693fce2c7d81						New30
แก้ไข คัดลอก ลบ	343	8krUJfK5	Password	:=	62e65594d767f97e8655693fce2c7d81						New30
แก้ไข คัดลอก ลบ	344	2unY0jew	Password	:=	62e65594d767f97e8655693fce2c7d81						New30
แก้ไข คัดลอก ลบ	345	A0kr3mS3	Password	:=	62e65594d767f97e8655693fce2c7d81						New30
แก้ไข คัดลอก ลบ	346	JrURJNJW	Password	:=	62e65594d767f97e8655693fce2c7d81						New30
แก้ไข คัดลอก ลบ	347	TV20LrV4	Password	:=	62e65594d767f97e8655693fce2c7d81						New30
แก้ไข คัดลอก ลบ	348	5cawFwuq	Password	:=	62e65594d767f97e8655693fce2c7d81						New30
แก้ไข คัดลอก ลบ	349	R5rHATG1	Password	:=	62e65594d767f97e8655693fce2c7d81						New30
แก้ไข คัดลอก ลบ	350	OnILLJr5	Password	:=	62e65594d767f97e8655693fce2c7d81						New30
แก้ไข คัดลอก ลบ	351	IutIUw8g	Password	:=	62e65594d767f97e8655693fce2c7d81						New30
แก้ไข คัดลอก ลบ	352	NdjhCAZ1	Password	:=	62e65594d767f97e8655693fce2c7d81						New30
แก้ไข คัดลอก ลบ	353	8MGq2q4E	Password	:=	62e65594d767f97e8655693fce2c7d81						New30

เลือกทั้งหมด ทำกับที่เลือก: เปลี่ยน ลบ ส่งออก

รูปที่ 4.6 ข้อมูลของผู้ใช้งานแบบกลุ่มถูกนำไปเก็บในดาต้าเบส

4.1.2 ทำการทดลองการทำงานของฟังก์ชั่นการยืนยันตัวตน

โดยใช้ข้อมูลจากดาต้าเบส (Database) ซึ่งเป็นข้อมูลของ username และ password ของระบบนำมาทดสอบเพื่อตรวจสอบสิทธ์ของผู้ใช้งาน ซึ่งจะมีการทดสอบการกรอก username และ password เป็นจำนวน 4 ครั้ง ดังต่อไปนี้

ครั้งที่1 username = user2 , password = pin2

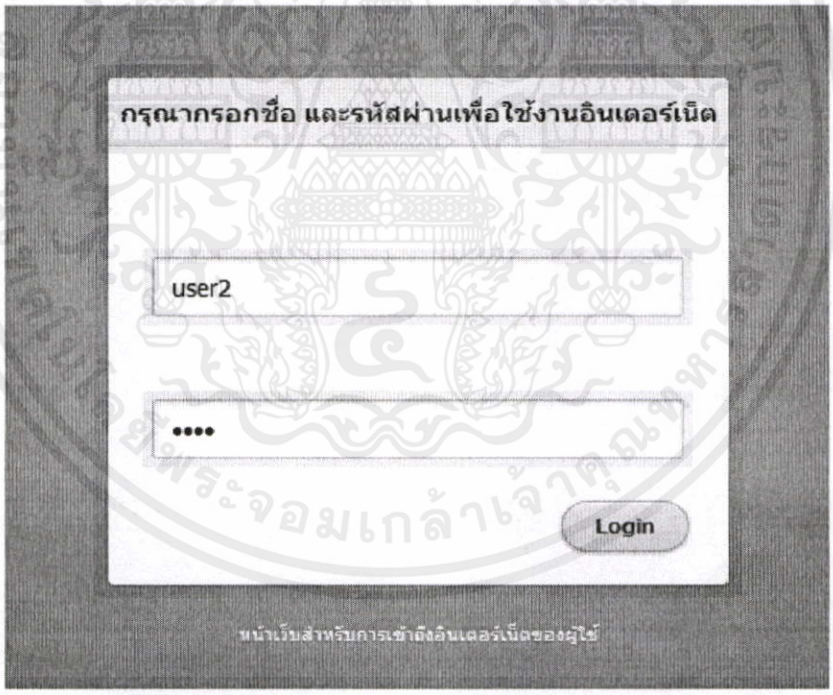
ครั้งที่2 username = user3 , password = pin2

ครั้งที่3 username = user4 , password = pin3

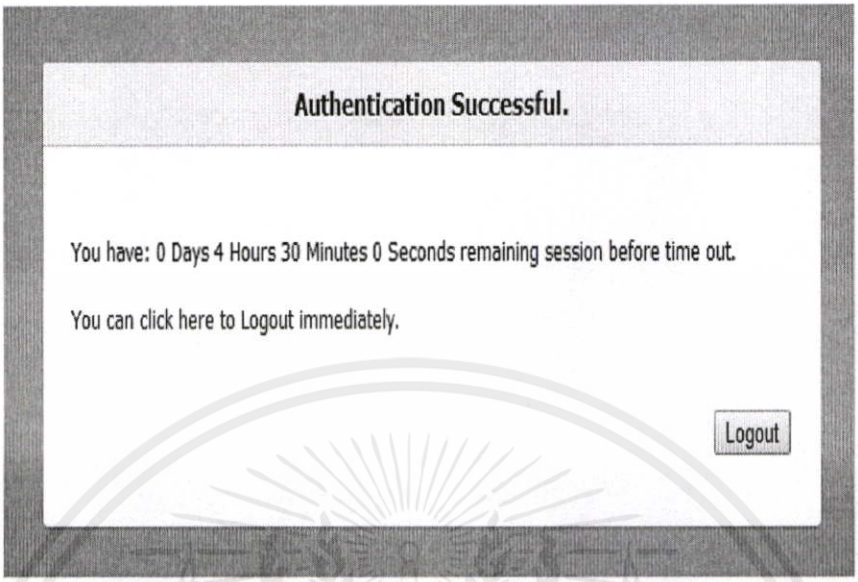
ครั้งที่4 username = kmitl , password = telecom

หลังจากการทำการป้อน username password ในแต่ละครั้ง จะทำการ logout ระบบก่อนแล้วเริ่มการ login ในแต่ละครั้งต่อไป

ทำการทดลองครั้งที่ 1 โดยกรอก username = user2 และ password = pin2



รูปที่ 4.7 การทดลองการยืนยันตัวตน ครั้งที่ 1

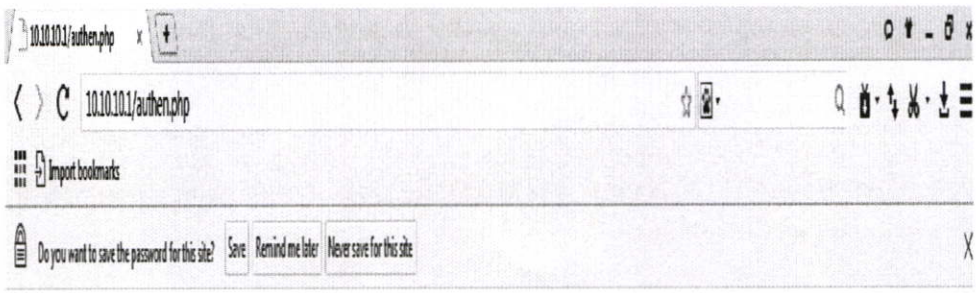


รูปที่ 4.8 ผลการทดลองการยืนยันตัวตน ครั้งที่ 1

จากรูปที่ 4.6 และ 4.7 เมื่อทำการกรอก user name กับ password ที่ตรงกับฐานข้อมูลของระบบ จะเห็นได้ว่าผลที่ได้คือระบบจะอนุญาติให้ผู้ใช้เข้าใช้งานอินเตอร์เน็ตได้

ทำการทดลองครั้งที่ 2 โดยกรอก username = user3 และ password = pin2

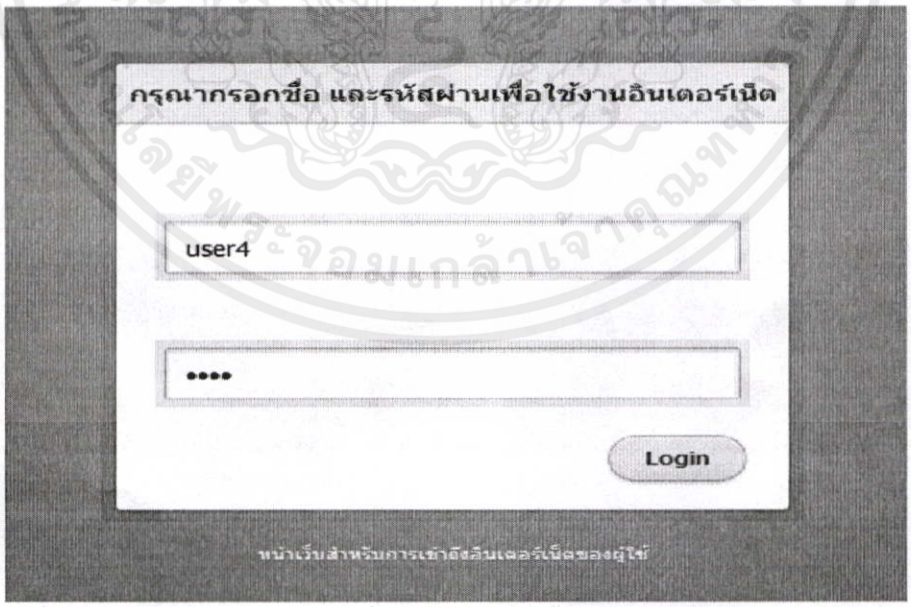
รูปที่ 4.9 การทดลองการยืนยันตัวตน ครั้งที่ 2



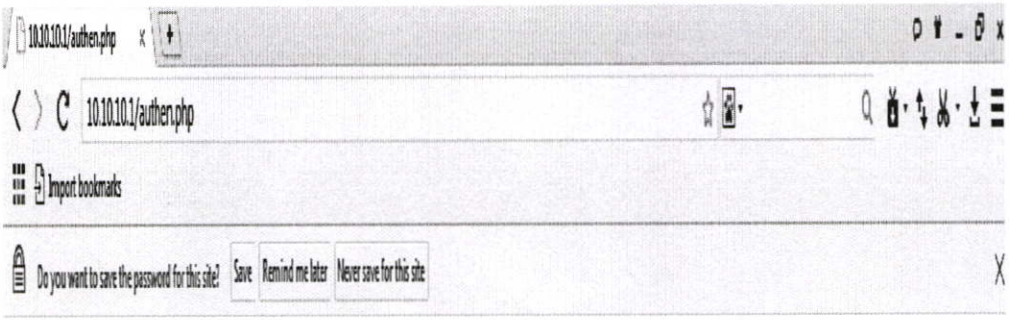
รูปที่ 4.10 ผลการทดลองการยืนยันตัวตน ครั้งที่ 2

จากรูปที่ 4.8 และ 4.9 เมื่อทำการกรอก user name กับ password ที่ไม่ตรงกับฐานข้อมูลของระบบ จะเห็นได้ว่าผลที่ได้คือระบบจะไม่อนุญาติให้ผู้ใช้เข้าใช้งานอินเตอร์เน็ต

ทำการทดลองครั้งที่ 3 โดยกรอก username = user4 และ password = pin4



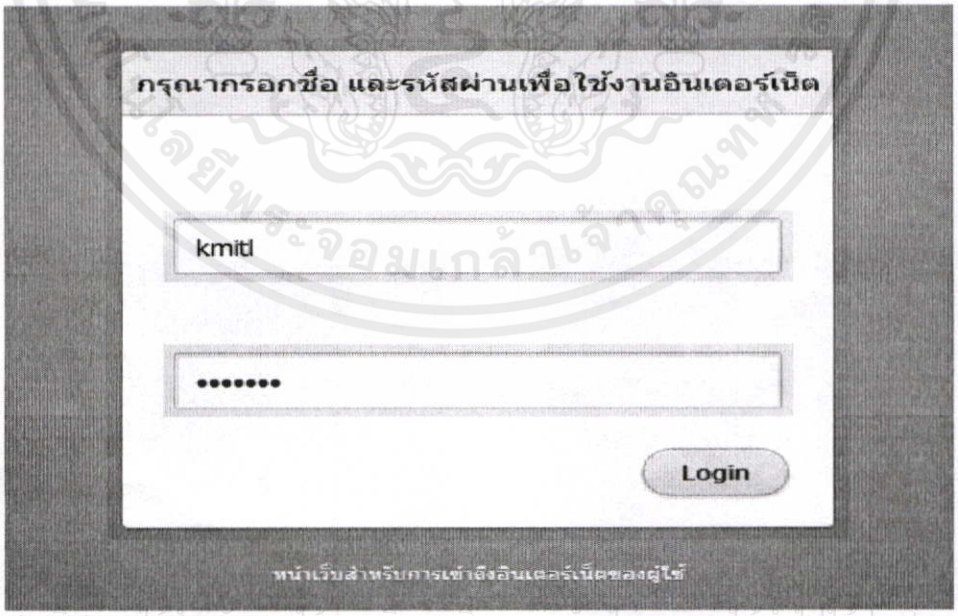
รูปที่ 4.11 การทดลองการยืนยันตัวตน ครั้งที่ 3



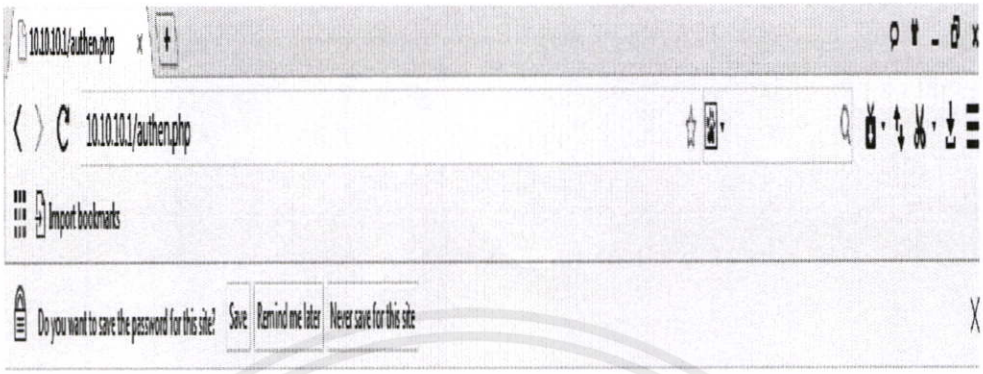
รูปที่ 4.12 ผลการทดลองการยืนยันตัวตน ครั้งที่ 3

จากรูปที่ 4.10 และ 4.11 เมื่อทำการกรอก user name กับ password ที่ไม่ตรงกับฐานข้อมูลของระบบ จะเห็นได้ว่าผลที่ได้คือระบบจะไม่อนุญาติให้ผู้ใช้เข้าใช้งานอินเตอร์เน็ตได้

ทำการทดลองครั้งที่ 4 โดยกรอก username = kmitl และ password = telecom



รูปที่ 4.13 การทดลองการยืนยันตัวตน ครั้งที่ 4



รูปที่ 4.14 ผลการทดลองการยืนยันตัวตน ครั้งที่ 4

จากรูปที่ 4.12 และ 4.13 เมื่อทำการกรอก user name กับ password ที่ไม่ตรงกับฐานข้อมูลของระบบ จะเห็นได้ว่าผลที่ได้คือระบบจะไม่อนุญาตให้ผู้ใช้เข้าใช้งานอินเตอร์เน็ต

จากการทดลองของฟังก์ชันการยืนยันตัวตน เมื่อทำการกรอก user name และ password ที่ตรงกับฐานข้อมูลของระบบ ระบบจะอนุญาตให้ผู้ใช้งานสามารถเข้าใช้อินเตอร์เน็ตได้ แต่ถ้าผู้ใช้กรอก user name และ password ไม่ตรงกับฐานข้อมูลของระบบ ระบบจะไม่อนุญาติให้ผู้ใช้เข้าสู่อินเตอร์เน็ต

4.2 การทดลองของฟังก์ชัน Web Caching (Proxy)

4.2.1ทำการทดลองหาTCP_MISS และTCP_HIT

ซึ่งทำการเข้าเว็บไซต์ที่แตกต่างกันดังต่อไปนี้

1.) http://www.tee-pak.net/doolakorn

2.) http://www.watchlakorn.in/tag/อายุน้อยร้อยล้าน

3.) http://fo3.garena.in.th/main

ทำการทดลองเข้าสู่เว็บไซต์ที่เป็น TCP_MISS แล้วทำการจับเวลา ต่อมาทำการเข้าเว็บไซต์เดิมที่เป็น TCP_HIT แล้วทำการจับเวลา เพื่อเปรียบเทียบความแตกต่างระหว่าง TCP_MISS กับ TCP_HIT แล้วทำการทดลองในลักษณะเดิมกับเว็บไซต์อื่นๆรวมทั้งหมด 3 ครั้งดังนี้

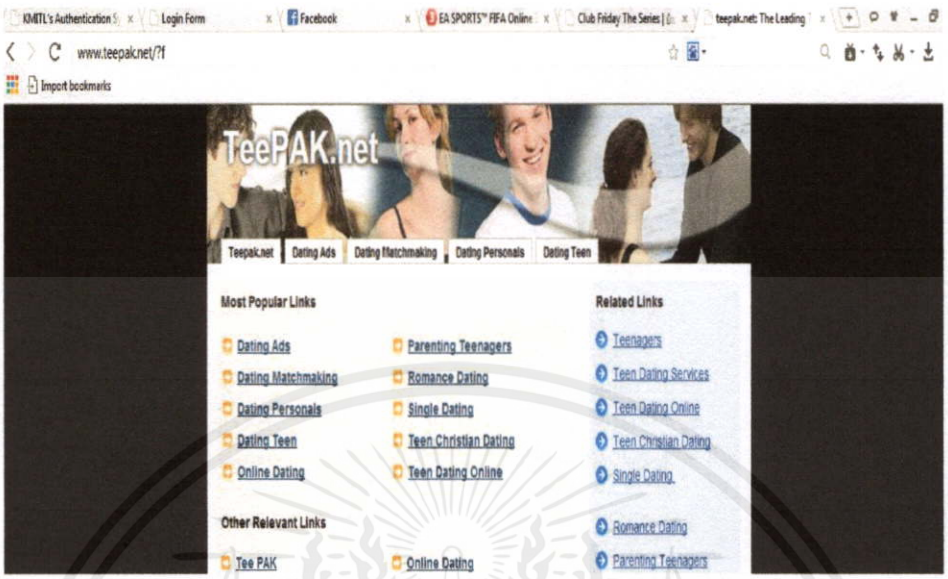
ทำการทดลองครั้งที่ 1

ทำการทดลองเข้าสู่เว็บไซต์ http://www.tee-pak.net/doolakorn ครั้งแรก ซึ่งเป็นสถานะ TCP_MISS

```
  7 10.10.10.41 TCP_MISS/200 900 GET http://www.dek-d.com/bannercode/adjs.php? -
  7 10.10.10.41 TCP_MISS/200 899 GET http://www.dek-d.com/bannercode/adjs.php? -
 50 10.10.10.41 TCP_MISS/200 982 GET http://pubads.g.doubleclick.net/gampad/ads?
  5 10.10.10.41 TCP_MISS/200 532 GET http://www.google-analytics.com/collect? - (
  4 10.10.10.41 TCP_MISS/200 532 GET http://www.google-analytics.com/collect? - (
  9 10.10.10.41 TCP_MISS/200 532 GET http://www.google-analytics.com/collect? - (
  9 10.10.10.41 TCP_MISS/200 2570 GET http://addoer.com/showfixads.php? - ORIGINA
 12 10.10.10.41 TCP_MISS/200 356 GET http://lvs.truehits.in.th/ckid2.php - ORIGIN
  4 10.10.10.41 TCP_MISS/200 445 GET http://ads.dek-d.com/adserver/adlog.php? - (
  5 10.10.10.41 TCP_MISS/200 445 GET http://ads.dek-d.com/adserver/adlog.php? - (
  4 10.10.10.41 TCP_MISS/200 445 GET http://ads.dek-d.com/adserver/adlog.php? - (
207 10.10.10.41 TCP_MISS/200 532 GET http://www.google-analytics.com/collect? - (
 47 10.10.10.41 TCP_MISS/301 590 GET http://www.youtube.com/embed/xApTzEPWPiI? -
  5 10.10.10.41 TCP_MISS/200 10222 GET http://static.ak.facebook.com/connect/xd_
```

รูปที่ 4.15 สถานะ TCP_MISS

ทำการจับเวลาในการเข้าสู่เว็บไซต์ http://www.tee-pak.net/doolakorn ที่เป็น TCP_MISS ได้เท่ากับ 5.1 วินาที



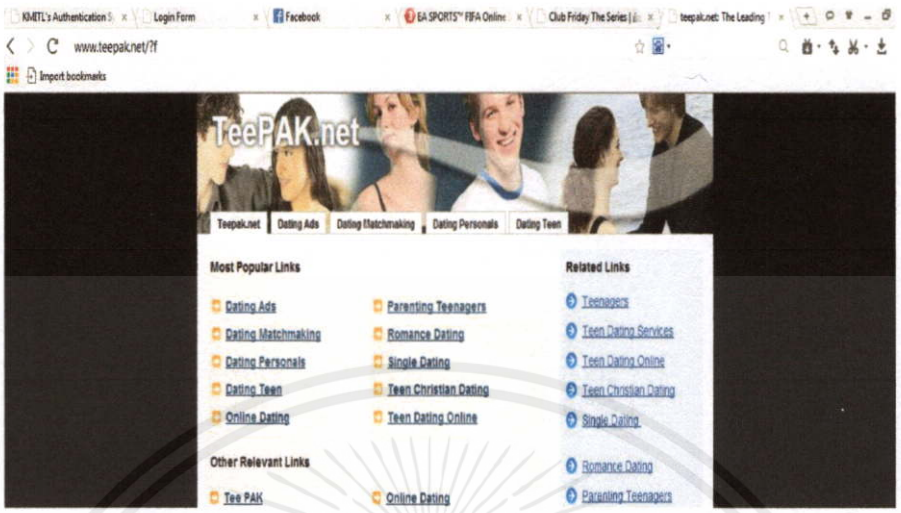
รูปที่ 4.16 เว็บไซต์ที่เป็น TCP_MISS

ทำการทดลองเข้าเว็บไซต์อีกครั้ง ซึ่งฟังก์ชัน Proxyจะเก็บออบเจ็กต์ของเว็บไซต์ http://www.tee-pak.net/doolakorn ซึ่งจะทำให้เป็นสถานะ TCP_HIT

```
261 10.10.10.31 TCP_HIT/200 1375 GET http://yourjavascript.com/2421164
260 10.10.10.31 TCP_HIT/200 1577 GET http://yourjavascript.com/2652325
261 10.10.10.31 TCP_HIT/200 5781 GET http://yourjavascript.com/0131202
 31 10.10.10.31 TCP_HIT/200 71299 GET http://s7.addthis.com/static/r07
 52 10.10.10.31 TCP_HIT/200 26545 GET http://widgets.amung.us/tab.js -
143 10.10.10.31 TCP_HIT/200 17245 GET http://s7.addthis.com/static/r07
 53 10.10.10.31 TCP_HIT/200 23920 GET http://s7.addthis.com/static/r07
113 10.10.10.41 TCP_HIT/200 66074 GET http://tns.nipa.co.th/img-active
112 10.10.10.41 TCP_HIT/200 75971 GET http://tns.nipa.co.th/img-active
111 10.10.10.41 TCP_HIT/200 80300 GET http://tns.nipa.co.th/img-active
 79 10.10.10.41 TCP_HIT/200 36062 GET http://tns.nipa.co.th/img-active
 58 10.10.10.31 TCP_HIT/200 2911 GET http://cdn.imgth.wat
 87 10.10.10.31 TCP_HIT/200 1231 GET http://cdn.imgth.wat
 88 10.10.10.31 TCP_HIT/200 1240 GET http://cdn.imgth.wat
```

รูปที่ 4.17 สถานะ TCP_HIT

ทำการจับเวลาในการเข้าสู่เว็บไซต์ http://www.tee-pak.net/doolakorn ที่เป็น TCP_HIT ได้เท่ากับ 3 วินาที



รูปที่ 4.18 เว็บไซต์ http://www.tee-pak.net/doolakorn ที่เป็น TCP_HIT

จากรูปที่ 4.17 กับ 4.18 จะเห็นว่าการเข้าสู่เว็บไซต์ http://www.tee-pak.net/doolakorn ที่เป็น TCP_MISS จะช้ากว่าแบบ TCP_HIT

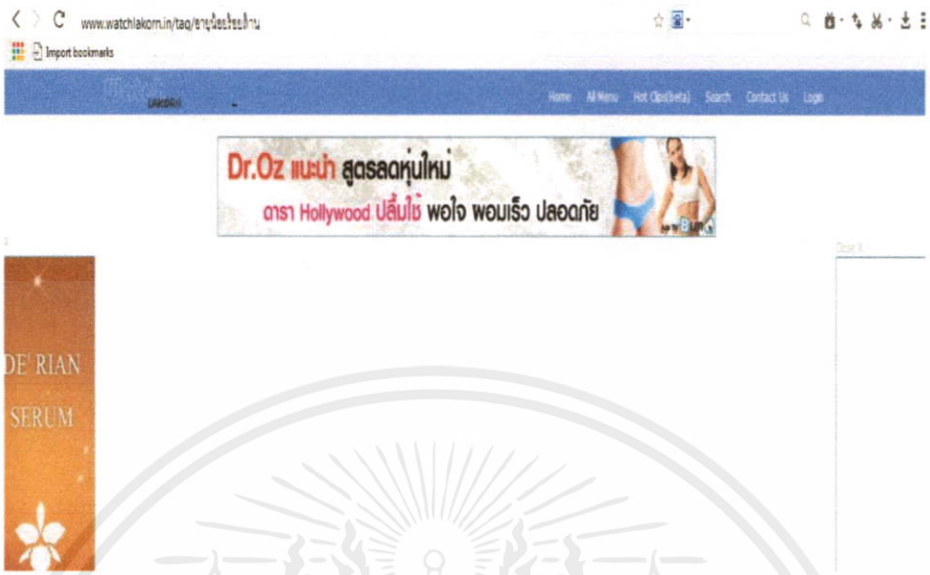
ทำการทดลองครั้งที่2

ทำการทดลองเข้าสู่เว็บไซต์ http://www.watchlakorn.in/tag/อายุน้อยร้อยล้าน ครั้งแรก ซึ่งเป็นสถานะ TCP_MISS

```
 28 10.10.10.41 TCP_MISS/304 285 GET http://pagead2.googlesyndication.com/pagead
 13 10.10.10.41 TCP_MISS/200 398 GET http://lvs.truehits.in.th/goggen.php? - ORI
  5 10.10.10.41 TCP_MISS/200 529 GET http://ads.dek-d.com/adserver/adjs.php? - O
  9 10.10.10.41 TCP_MISS/200 874 GET http://ads.dek-d.com/adserver/adjs.php? - O
 11 10.10.10.41 TCP_MISS/200 874 GET http://ads.dek-d.com/adserver/adjs.php? - O
221 10.10.10.41 TCP_MISS/200 3006 GET http://search.gogorithm.com/st? - ORIGINAL
  5 10.10.10.41 TCP_MISS/200 445 GET http://ads.dek-d.com/adserver/adlog.php? -
  8 10.10.10.41 TCP_MISS/200 28680 GET http://ads.dek-d.com/adserver/banner/bann
  4 10.10.10.41 TCP_MISS/200 445 GET http://ads.dek-d.com/adserver/adlog.php? -
  5 10.10.10.41 TCP_MISS/200 10222 GET http://static.ak.facebook.com/connect/xd
```

รูปที่ 4.19 สถานะ TCP_MISS

ทำการจับเวลาในการเข้าสู่เว็บไซต์ http://www.watchlakorn.in/tag/อายุน้อยร้อยล้านที่เป็น TCP_MISS ได้เท่ากับ 8.7 วินาที



รูปที่ 4.20 เว็บไซต์ http://www.watchlakorn.in/tag/อายุน้อยร้อยล้าน ที่เป็น TCP_MISS

ทำการทดลองเข้าเว็บไซต์อีกครั้ง ซึ่งฟังก์ชัน Proxyจะเก็บออบเจ็กต์ของเว็บไซต์ http://www.watchlakorn.in/tag/อายุน้อยร้อยล้าน ซึ่งจะทำให้เป็นสถานะ TCP_HIT

```
 58 10.10.10.31 TCP_HIT/200 2911 GET http://cdn.imgth.wat
 87 10.10.10.31 TCP_HIT/200 1231 GET http://cdn.imgth.wat
 88 10.10.10.31 TCP_HIT/200 1240 GET http://cdn.imgth.wat
104 10.10.10.31 TCP_HIT/200 3286 GET http://cdn.imgth.wat
 14 10.10.10.31 TCP_HIT/200 2279 GET http://cdn.imgth.wat
114 10.10.10.31 TCP_HIT/200 10175 GET http://cdn.imgth.wa
 11 10.10.10.31 TCP_HIT/200 10181 GET http://cdn.imgth.wa
126 10.10.10.31 TCP_HIT/200 20062 GET http://cdn.imgth.wa
 24 10.10.10.31 TCP_HIT/200 13311 GET http://cdn.imgth.wa
 41 10.10.10.31 TCP_HIT/200 19918 GET http://cdn.imgth.wa
```

รูปที่ 4.21 สถานะ TCP_HIT

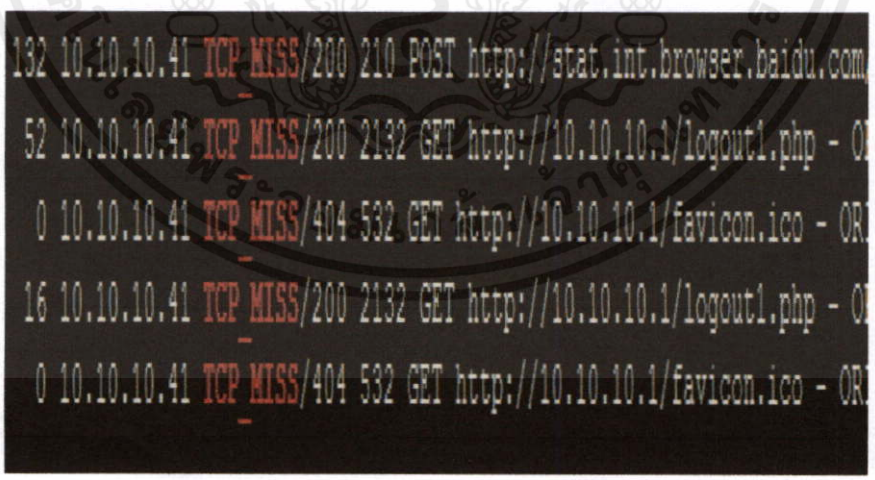
ทำการจับเวลาในการเข้าสู่เว็บไซต์ http://www.watchlakorn.in/tag/อายุน้อยร้อยล้าน ที่เป็น TCP_HIT ได้เท่ากับ 4.5 วินาที

รูปที่ 4.22 เว็บไซต์ http://www.watchlakorn.in ที่เป็นTCP_HIT

จากรูปที่4.21กับ4.22จะเห็นว่าการเข้าสู่เว็บไซต์ http://www.watchlakorn.in/tag/ อายุน้อยร้อยล้าน ที่เป็น TCP_MISS จะช้ากว่าแบบ TCP_HIT

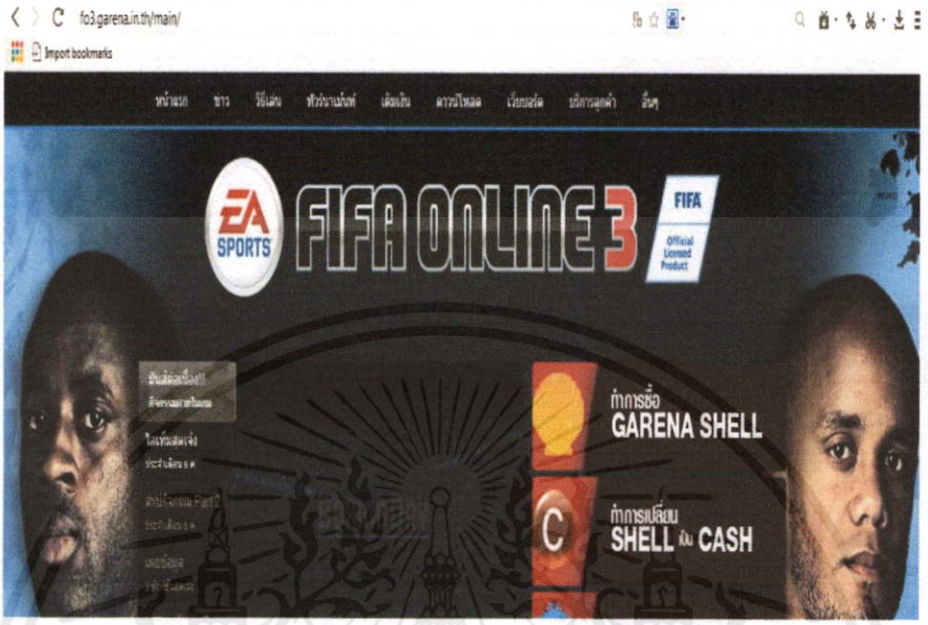
ทำการทดลองครั้งที่3

ทำการทดลองเข้าสู่เว็บไซต์ http://fo3.garena.in.th/main/ ครั้งแรก ซึ่งเป็นสถานะ TCP_MISS



รูปที่ 4.23 สถานะ TCP_MIS

ทำการจับเวลาในการเข้าสู่เว็บไซต์ http://fo3.garena.in.th/main/ ที่เป็น TCP_MISS ได้เท่ากับ 11.5 วินาที

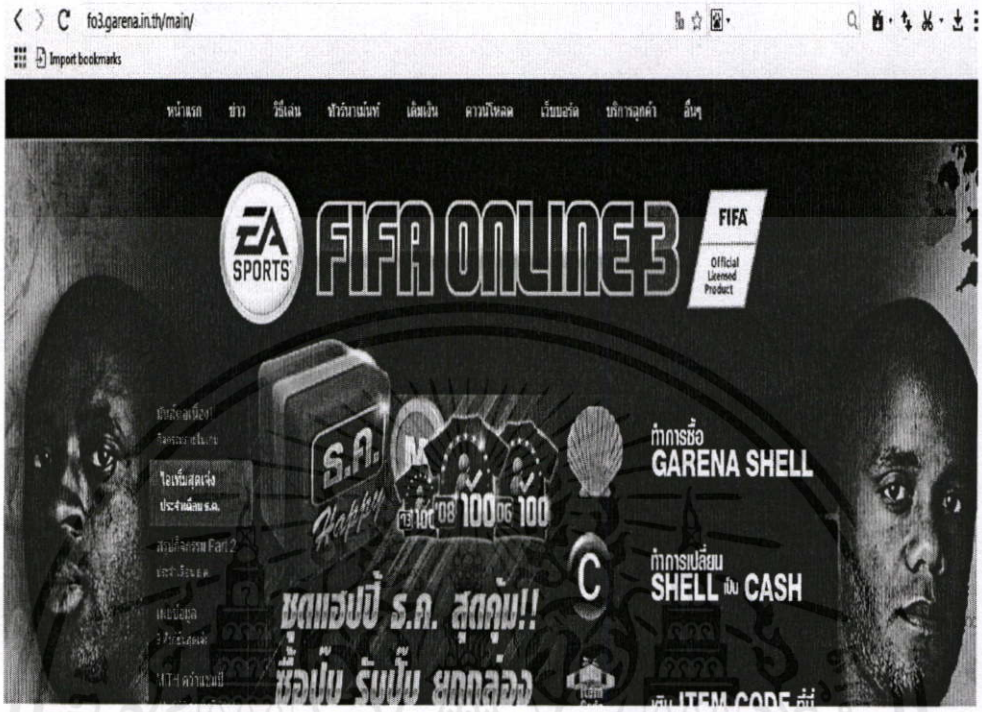


รูปที่ 4.24 เว็บไซต์ http://fo3.garena.in.th/main ที่เป็น TCP_MISS

ทำการทดลองเข้าเว็บไซต์อีกครั้ง ซึ่งฟังก์ชัน Proxyจะเก็บออบเจ็กต์ของเว็บไซต์ http://fo3.garena.in.th/main/ ซึ่งจะทำให้เป็นสถานะ TCP_HIT

รูปที่ 4.25 สถานะ TCP_HIT

ทำการจับเวลาในการเข้าสู่เว็บไซต์ http://fo3.garena.in.th/main/ ที่เป็น TCP_HIT ได้เท่ากับ 3.5 วินาที



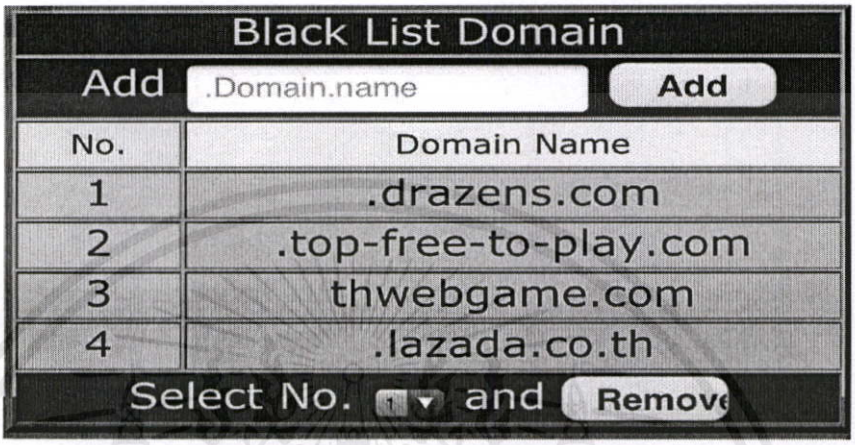
รูปที่ 4.26 เว็บไซต์ http://fo3.garena.in.th/main/ ที่เป็นTCP_HIT

จากรูปที่ 4.25 กับ 4.26 จะเห็นว่าการเข้าสู่เว็บไซต์ http://fo3.garena.in.th/main/ ที่เป็น TCP_MISS จะช้ากว่าแบบ TCP_HIT

จากการทดลองของฟังก์ชัน Web Caching เมื่อทำการเข้าสู่เว็บไซต์ที่ไม่มีการถูกบันทึกออบเจ็กต์ไว้ในเซิร์ฟเวอร์ จะถูกกำหนดให้เป็น TCP_MISS หรือถ้าทำการเข้าสู่เว็บไซต์ที่มีการบันทึกออบเจ็กต์ไว้ในเซิร์ฟเวอร์แล้ว จะถูกกำหนดให้เป็น TCP_HIT ซึ่งจะพบว่าการเข้าสู่เว็บไซต์ที่เป็น TCP_MISS จะช้ากว่าการเข้าสู่เว็บไซต์ที่เป็น TCP_HIT ซึ่งแต่ละเว็บจะใช้เวลาในการเข้าสู่เว็บไซต์ต่างกัน จะขึ้นอยู่กับปริมาณข้อมูลในเว็บไซต์และความเร็วอินเตอร์เน็ต

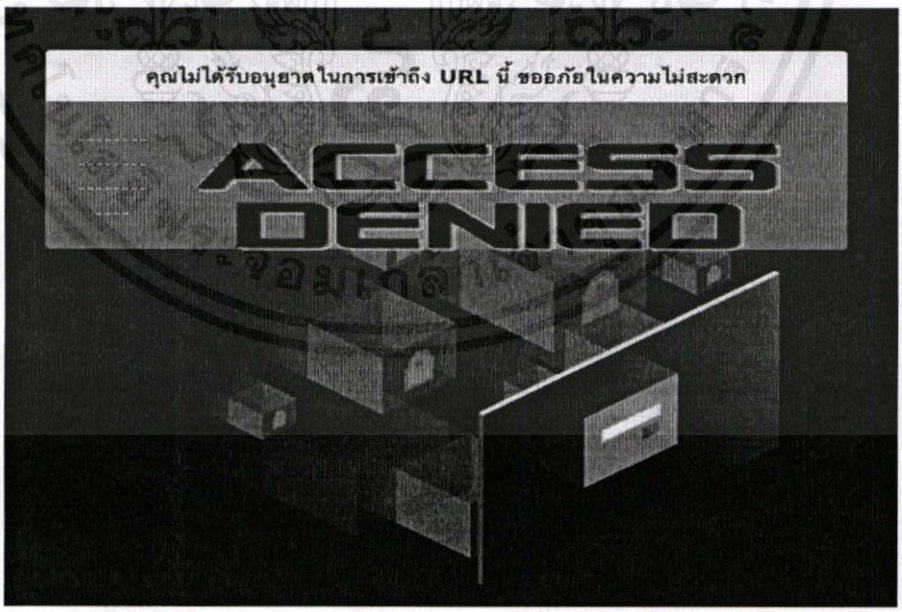
4.2.2 ทำการทดลอง Black List Domain

โดยหลักการนี้จะทำการบล็อกเว็บไซร์ต์ที่เป็นเนื้อหาที่อันตรายหรือไม่เหมาะสม ระบบจะไม่อนุญาตให้ผ่านเข้าสู้เว็บไวต์ดังกล่าว จึงมีหน้าที่เป็นไฟร์วอลล์ในระดับแอปพิเคชันเลเยอร์



รูปที่ 2.27 รายชื่อเว็บไซต์ที่ระบบได้ทำการ Black List Domain

ทดลองเข้าสู่เว็บไซต์ที่ระบบได้ทำการบล็อกดังนี้ 1) www.lazada.co.th 2) www.drazens.com 3) www.thwebgame.com 4) www.top-free-to-play.com ระบบจะทำการ รีไดเร็ก(Redirect) ไปยังหน้า URL



รูปที่ 4.28 หน้า URL ที่อันตรายหรือไม่เหมาะสม

ทำการ Remove www.lazada.co.th โดยเลือกไปที่ลำดับที่ 4

รูปที่ 4.29 Remove Black List ในลำดับที่4

รูปที่ 4.30 หลังที่ได้ทำการ Remove

ทดลองเข้าเว็ปไซต์ที่ได้ทำการ Remove ไปคือ www.lazada.co.th

รูปที่ 4.31 หน้า URL ของเว็ปไซต์ www.lazada.co.th

การบล็อกหน้าเว็ป URL จะทำในฟังก์ชัน Web Caching (Proxy) ซึ่งทำงานในชั้นแอปพิเคชันเลเยอร์ จากการทดสอบระบบจะเห็นได้ว่าระบบสามารถที่จะบล็อกเว็ปไซต์ที่เป็นเนื้อหาที่อันตรายหรือไม่เหมาะสมได้อย่างมีประสิทธิภาพ

4.3 การทดลองของฟังก์ชัน (Multiple – Gateways)

4.3.1 ทำการทดลองฟังก์ชัน Multiple-Gateway แบบ Weighted Round Robin

โดยการโยนทราฟฟิก(Traffic)ออกไปสู่อินเตอร์เน็ตสองอินเตอร์เฟส (Interface) เพื่อเปรียบเทียบปริมาณของทราฟฟิกที่เซิร์ฟเวอร์ทำการกระจายงาน โดยทำการคอนฟิกระบบออกเป็น 3 อินเตอร์เฟสดังนี้

อินเตอร์เฟส 1 เป็น Gateway1 เท่ากับ GW1 มี IP เป็น 161.246.18.249 ที่P1P1

อินเตอร์เฟส 2 เป็น Gateway 2 เท่ากับ GW2 มี IP เป็น 191.168.2.1 ที่P2P1

อินเตอร์เฟส 3 เป็น LAN ภายในระบบ เท่ากับ LAN มี IP เป็น 10.10.10.1 ที่P4P1

จะทำการทดลองการกระจายงานของเซิร์ฟเวอร์ โดยการกำหนดค่า Gateways Ratio Weighting เป็น 3 กรณีคือ

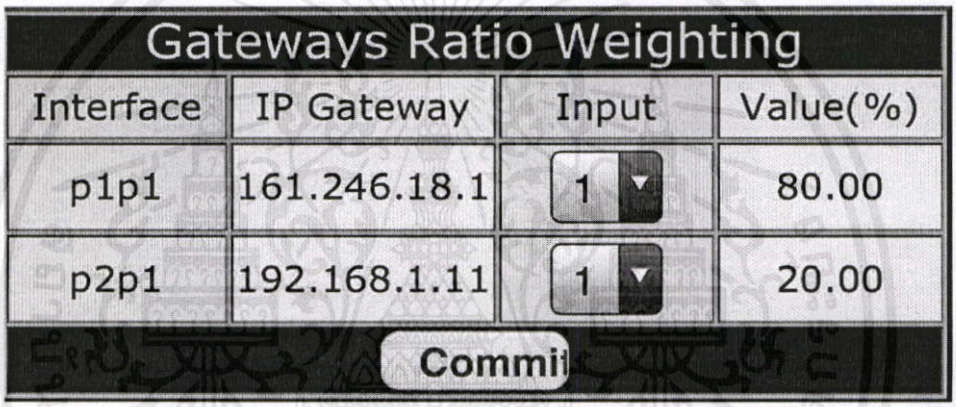
กรณีที่ 1 กำหนดค่า Weighting ของอินเตอร์เฟส 1 เท่ากับ 4 และกำหนดค่าของอินเตอร์เฟส 2เท่ากับ 1

กรณีที่ 2 กำหนดค่า Weighting ของอินเตอร์เฟส 1 เท่ากับ 1 และกำหนดค่าของอินเตอร์เฟส 2 เท่ากับ 1

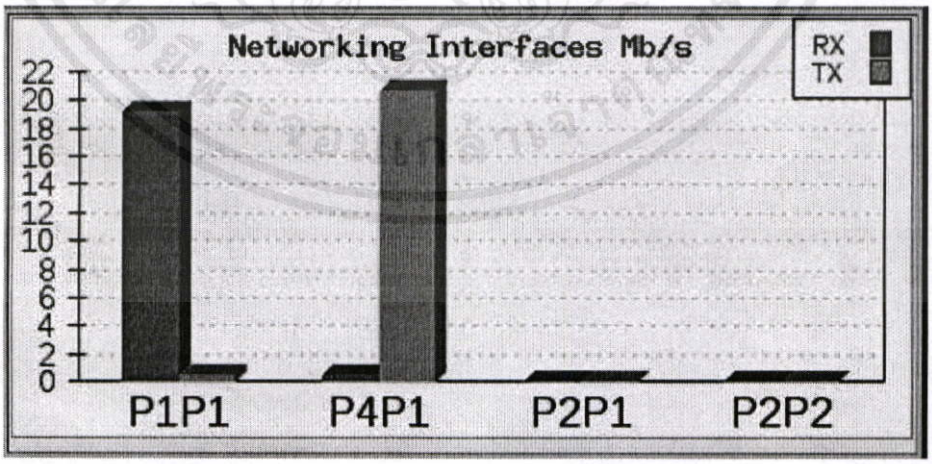
กรณีที่ 3 กำหนดค่า Weighting ของอินเตอร์เฟส 1 เท่ากับ 1 และกำหนดค่าของอินเตอร์เฟส 2 เท่ากับ 4

ถ้าเทียบบัญญัติไตรยางศ์และคิดที่ 100เปอร์เซ็นต์ (percentage/percent) จะได้ว่า โอกาสที่ปริมาณ Concurrent Login Users ของผู้ใช้จะมีโอกาสออกสู่อินเตอร์เน็ตทางด้าน GW1มีค่าเท่ากับ Weighting ของอินเตอร์เฟส 1 / Weighting ของอินเตอร์เฟส 1 + Weighting อินเตอร์เฟส 2 ส่วน Weighting ของอินเตอร์เฟส 2 / Weighting ของอินเตอร์เฟส 1 + Weighting อินเตอร์เฟส 2 แล้วนำไปคูณด้วย 100 เพื่อเทียบเป็นเปอร์เซ็นต์แล้วทำการเปรียบเทียบหาค่าประสิทธิภาพของระบบในการกระจายงาน

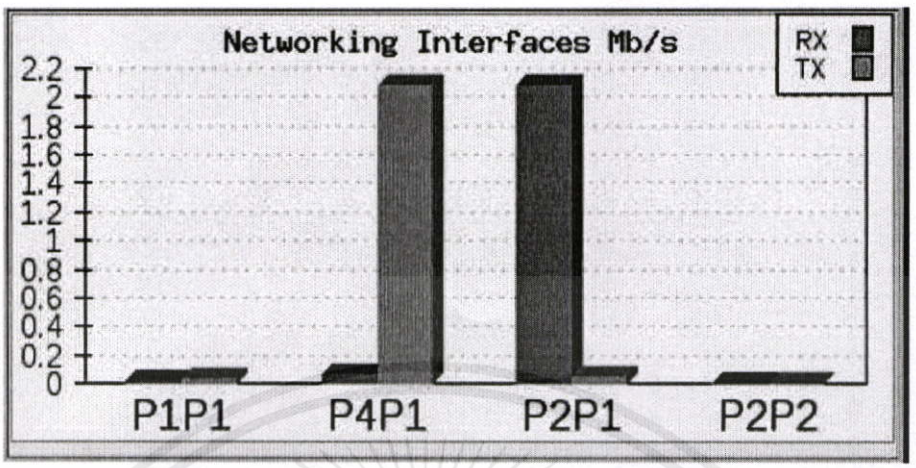
1). กำหนดค่า Weighting ของอินเตอร์เฟส 1 เท่ากับ 4 และกำหนดค่าของอินเตอร์เฟส 2เท่ากับ 1



รูปที่ 4.32 กำหนดค่า Gateways Ratio Weighting เป็น GW1:GW2 เท่ากับ 4:1



รูปที่ 4.33 เซิร์ฟเวอร์กระจายงานไปยัง Gateway1 ที่ Port : P1P1



รูปที่ 4.34 เซิร์ฟเวอร์กระจายงานไปยัง Gateway2 ที่ Port : P2P1

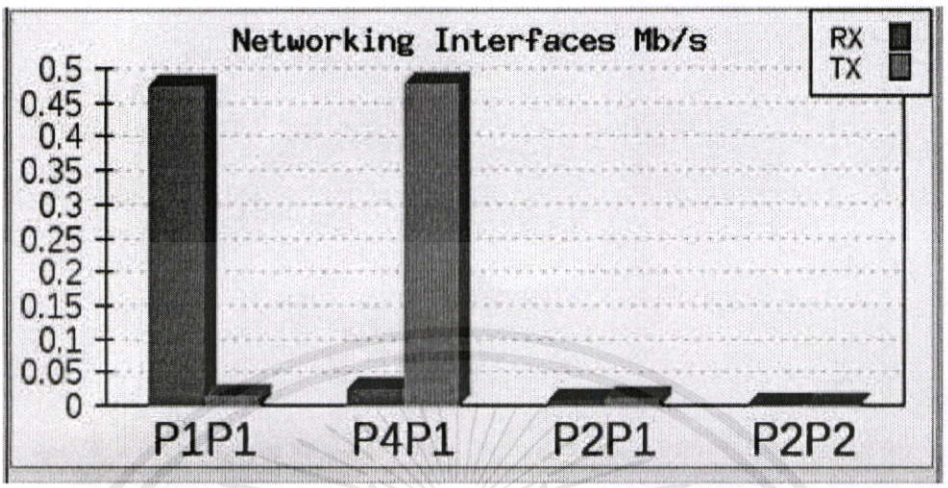
ตารางที่ 4.1 การทดลองการกระจายงานของเซิร์ฟเวอร์ กรณีที่ 1

Concurrent Sessions.	ครั้งที่1	ครั้งที่2	ครั้งที่3	ครั้งที่4	ครั้งที่5	ครั้งที่6	ครั้งที่7	ครั้งที่8	ครั้งที่9	ครั้งที่10
User	GW 1	GW 1	GW 1	GW 2	GW 1	GW 2	GW 1	GW 1	GW 1	GW 1

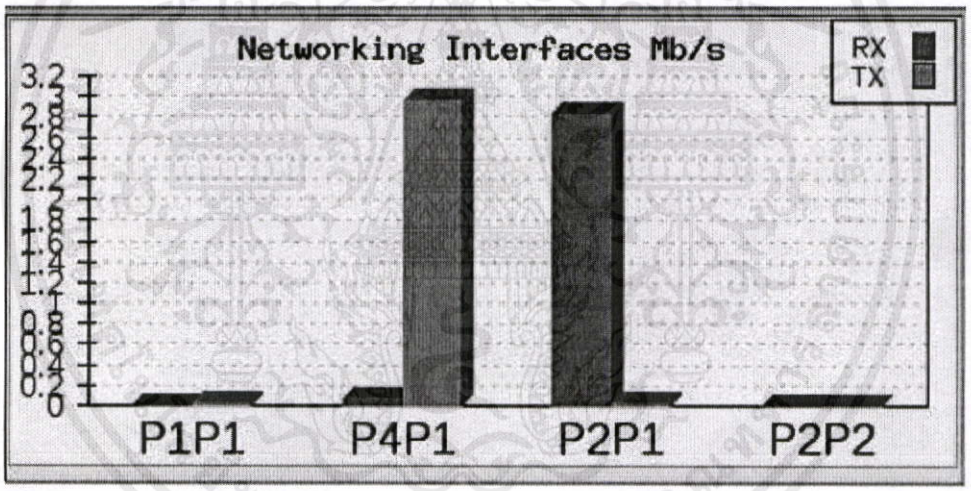
เมื่อนับการกระจายงานของเซิร์ฟเวอร์ที่เกิดจาก Concurrent Sessions ของผู้ใช้งานในระบบได้ดังนี้ User : GW1=8 , GW=2 ซึ่งจากการทดลองพบว่าปริมาณ Concurrent Sessions ที่ออกสู่อินเตอร์เน็ตเป็นไปตามค่า Weighted Round Robin ในอัตตราส่วน 4:1

2). กำหนดค่า Weighting ของอินเตอร์เฟส 1 เท่ากับ 1 และกำหนดค่าของอินเตอร์เฟส 2 เท่ากับ 1

รูปที่ 4.35 กำหนดค่า Gateways Ratio Weighting เป็น GW1:GW2 เท่ากับ 1:1



รูปที่ 4.36 เซิร์ฟเวอร์กระจายงานไปยัง Gateway1 ที่ Port : P1P1



รูปที่ 4.37 เซิร์ฟเวอร์กระจายงานไปยัง Gateway2 ที่ Port : P2P1

ตารางที่ 4.2 การทดลองการกระจายงานของเซิร์ฟเวอร์ กรณีที่ 2

Concurrent Sessions.	ครั้งที่1	ครั้งที่2	ครั้งที่3	ครั้งที่4	ครั้งที่5	ครั้งที่6	ครั้งที่7	ครั้งที่8	ครั้งที่9	ครั้งที่10
User	GW 1	GW 2	GW 1	GW 1	GW 2	GW 1	GW 2	GW 1	GW 2	GW 1

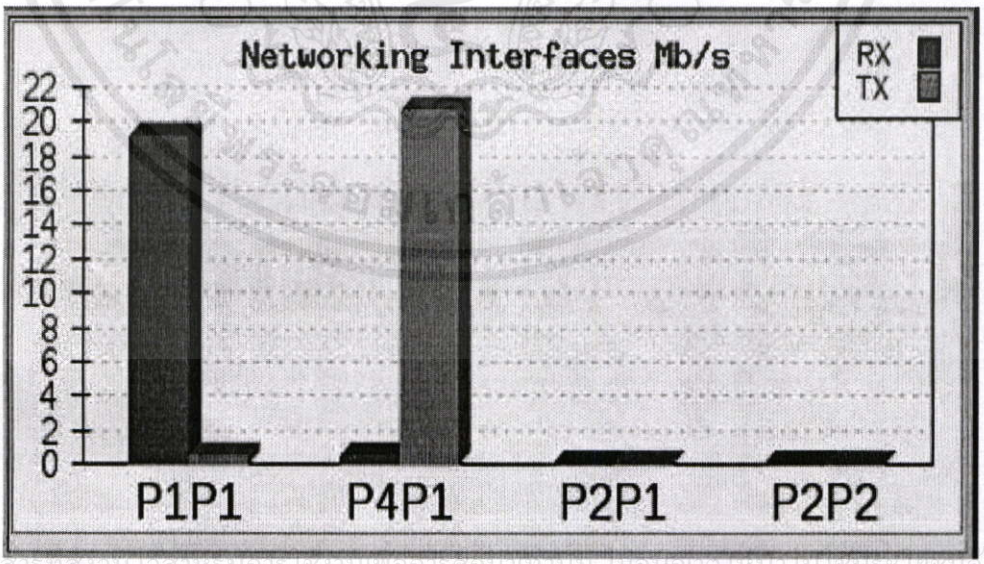
เมื่อให้ผู้ใช้งานภายในระบบได้ทำการสร้าง Concurrent Sessions เข้าไปในระบบ จากการทดลองจะพบว่า ปริมาณของ Concurrent Sessions ที่ออกสู่อินเตอร์เน็ตทางด้านของ GW1 มีค่าคลาดเคลื่อนเล็กน้อย ซึ่งค่าตามทฤษฎีมีค่าเท่ากับ 5 แต่ค่าที่ทดลองได้เท่ากับ 6 และปริมาณ Concurrent Sessions ทางด้าน GW2 มีค่าคาดเคลื่อนเล็กน้อย ซึ่งตามทฤษฎีมีค่าเท่ากับ 5 แต่ค่าที่ทดลองได้ เท่ากับ 4 ในอัตราส่วน GW1:GW2 เท่ากับ 1:1

3). กำหนดค่า Weighting ของอินเตอร์เฟส 1 เท่ากับ 1 และกำหนดค่าของอินเตอร์เฟส 2 เท่ากับ 4

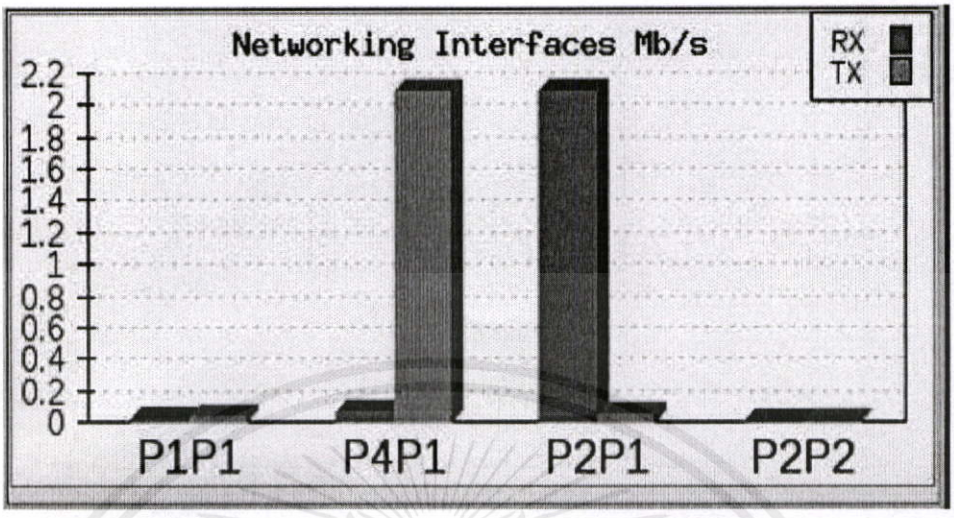
Gateways Ratio Weighting

Interface	IP Gateway	Input	Value(%)
p1p1	161.246.18.1	1	20.00
p2p1	192.168.1.11	1	80.00

รูปที่ 4.38 กำหนดค่า Gateways Ratio Weighting เป็น GW1:GW2 เท่ากับ 1:4



รูปที่ 4.39 เซิร์ฟเวอร์กระจายงานไปยัง Gateway1 ที่ Port : P1P1



รูปที่ 4.40 เซิร์ฟเวอร์กระจายงานไปยัง Gateway2 ที่ Port : P2P1

ตารางที่ 4.3 การทดลองการกระจายงานของเซิร์ฟเวอร์ กรณีที่ 3

Concurrent Sessions.	ครั้งที่1	ครั้งที่1	ครั้งที่1	ครั้งที่1	ครั้งที่1	ครั้งที่1	ครั้งที่1	ครั้งที่1	ครั้งที่1	ครั้งที่1
User	GW 2	GW 2	GW 1	GW 2	GW 2	GW 2	GW 1	GW 2	GW 1	GW 2

เมื่อให้ผู้ใช้งานภายในระบบได้ทำการสร้าง Concurrent Sessions เข้าไปในระบบ จากการทดลองจะพบว่า ปริมาณของ Concurrent Sessions ที่ออกสู่อินเตอร์เน็ตทางด้านของ GW1 มีค่าคลาดเคลื่อนเล็กน้อย ซึ่งค่าตามทฤษฎีมีค่าเท่ากับ 2 แต่ค่าที่ทดลองได้เท่ากับ 3 และปริมาณ Concurrent Sessions ทางด้าน GW2 มีค่าคาดเคลื่อนเล็กน้อย ซึ่งตามทฤษฎีมีค่าเท่ากับ 8 แต่ค่าที่ทดลองได้ เท่ากับ 7 ในอัตราส่วน GW1:GW2 เท่ากับ 1:4

บทที่ 5

สรุปผลและข้อเสนอแนะ

5.1 สรุปผล

โครงงานนี้ได้ทำการออกแบบฟังก์ชันที่ใช้ในการบริหารจัดการในการเข้าถึงข้อมูลอินเตอร์เน็ตของผู้ใช้บริการ สามารถตรวจสอบสิทธิ์ในการใช้งานของผู้ใช้บริการ ดูแลรักษาความปลอดภัยเครือข่ายและข้อมูลของผู้ใช้บริการ รวมทั้งตรวจสอบสถานะของระบบสำหรับบริหารจัดการระบบให้เหมาะสมเพื่อควบคุมและจำกัดการเข้าถึงข้อมูลอินเตอร์เน็ตของผู้ใช้บริการได้อย่างมีประสิทธิภาพ ซึ่งเป็นการนำฮาร์ดแวร์และซอฟแวร์มาบริหารจัดการโครงข่ายเพื่อความสะดวกและเหมาะสมในการเข้าใช้งานอินเตอร์เน็ต

5.2 ข้อเสนอแนะ

5.2.1 สามารถนำเซิร์ฟเวอร์ที่ทำการออกแบบไว้ไปใช้กับอุปกรณ์ในโครงข่าย ยกตัวอย่างเช่น Switch , WiFi router, ใช้สายสัญญาณ UTP เพื่อขยายโครงข่ายให้มีขนาดใหญ่ขึ้น เพื่อรองรับการใช้งานที่มากขึ้น

5.2.2 เซิร์ฟเวอร์ที่ได้ทำการออกแบบขึ้นมา สามารถนำไปใช้ทำธุรกิจขนาดย่อมได้ โดยนำเซิร์ฟเวอร์ที่เราได้ทำการออกแบบ เข้าไปบริหารจัดการ หอพัก คอนโด หรือ องค์กรที่ต้องการใช้บริการ แล้วทำการเก็บค่าใช้บริการแบบรายเดือน ซึ่งจะทำให้ผู้ใช้บริการไม่ต้องทำการบำรุงรักษาโครงข่าย และไม่ต้องกังวลเหมือนการใช้อินเตอร์เน็ตรายเดือนที่ต้องเสียค่าบริการทุกเดือนแม้ว่าจะไม่ได้ใช้งานก็ตาม แต่ถ้าใช้บริการเซิร์ฟเวอร์ที่ออกแบบขึ้นมาก็จะสามารถเลือกได้ว่าเดือนไหนจะใช้บริการบ้าง

5.2.3 serverที่ทำการออกแบบขึ้นมาสามารถเพิ่มขีดความสามารถในการรองรับการให้บริการของผู้ใช้งานจำนวนมากๆได้ โดยใช้เทคนิค ดังต่อไปนี้ LOAD BALANCE CONTROLLER, PROXY, FIREWALL , GRAPHIC USER INTERFACE INTERFACE MANAGEMENT สามารถนำไปพัฒนา ต่อยอดในการให้บริการสำหรับเครื่องลูกข่ายที่มีจำนวนมากๆขึ้นได้ และสามารถให้บริการได้อย่างมีประสิทธิภาพได้

บรรณานุกรม

[1]พรพิมล ทองภาสตร์. “ระบบสื่อสารข้อมูลและเครือข่าย.” เครือข่ายส่วนบุคคล(PAN). https://sites.google.com/site/natpornpimon54/2-1-pra-pheth-khxng-kherux-khay-pan-man-wan-lan

[2] พรพิมล ทองภาสตร์. “ระบบสื่อสารข้อมูลและเครือข่าย.” เครือข่ายระดับท้องถิ่น(LAN). https://sites.google.com/site/natpornpimon54/2-1-pra-pheth-khxng-kherux-khay-pan-man-wan-lan

[3] พรพิมล ทองภาสตร์. “ระบบสื่อสารข้อมูลและเครือข่าย.” เครือข่ายระดับเมือง(MAN). https://sites.google.com/site/natpornpimon54/2-1-pra-pheth-khxng-kherux-khay-pan-man-wan-lan

[4] พรพิมล ทองภาสตร์. “ระบบสื่อสารข้อมูลและเครือข่าย.” เครือข่ายระยะไกล(WAN). https://sites.google.com/site/natpornpimon54/2-1-pra-pheth-khxng-kherux-khay-pan-man-wan-lan

[5] แสงดาว เฉยฉิน “รูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์.” โครงข่ายแบบเส้นตรง. https://sangdao53.wordpress.com/บทที่-3/รูปแบบการเชื่อมต่อระบบ/

[6] แสงดาว เฉยฉิน “รูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์.” โครงข่ายแบบดาว. https://sangdao53.wordpress.com/บทที่-3/รูปแบบการเชื่อมต่อระบบ/

[7] แสงดาว เฉยฉิน “รูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์.” โครงข่ายแบบวงแหวน. https://sangdao53.wordpress.com/บทที่-3/รูปแบบการเชื่อมต่อระบบ/

[8] แสงดาว เฉยฉิน “รูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์.” โครงข่ายแบบต้นไม้. https://sangdao53.wordpress.com/บทที่-3/รูปแบบการเชื่อมต่อระบบ/

[9] แสงดาว เฉยฉิน “รูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์.” โครงข่ายแบบเมช. https://sangdao53.wordpress.com/บทที่-3/รูปแบบการเชื่อมต่อระบบ/

[10] แสงดาว เฉยฉิน “รูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์.” โครงข่ายแบบผสม. https://sangdao53.wordpress.com/บทที่-3/รูปแบบการเชื่อมต่อระบบ/

[11] TRIPOD “NECTEC WEB BASE LEARNIMG.”Linux คืออะไร. http://linuxunix54321.tripod.com/Linux01.htm

[12] Mindphp “DNS คือ อะไร.”http://archive.mindphp.com/modules.php?name=News&file=article&sid=115

[13] IT Guide “Firewall คืออะไร.”
http://it-guides.com/training-a-tutorial/network-system/what-is-firewall[14] IT Guide “Firewall คืออะไร.” Network Level Firewall.http://it-guides.com/training-a-tutorial/network-system/what-is-firewall

[15] IT Guide “Firewall คืออะไร.” Application Layer Firewall. http://it-guides.com/training-a-tutorial/network-system/what-is-firewall

[16] Sorasak Sittayanuwat “การสร้างเว็บเพจด้วยภาษา HTML.” http://www.yupparaj.ac.th/CAI/create_web/htm1.htm

[17] จักกกริช พฤษการ. การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์. กรุงเทพฯ :ท้อป,2549

[18] ก่อกิจ วีระอาชากุล. Network, Guide& Practice Network Aministion.พิมพ์ครั้งที่ 5. นนทบุรี : ไอดีซีฯ, 2553.

[19] พนิดา พานิชกุล. การใช้โปรแกรมคอมพิวเตอร์ เบื้องต้น ด้วยภาษา JAVA พิมพ์ครั้งที่ 5. กรุงเทพฯ : เคทีพี, 2554.

[20] อนรรฆนงค์ คุณมนี. คู่มือเขียนโปรแกรมภาษา JAVA ฉบับผู้เริ่มต้น. พิมพ์ครั้งที่ 1. นนบุรี : ไอดีซีฯ, 2551

[21] ดร. ยรรยง เต็งอำนวย. ระบบปฏิบัติการ(Operating system). กรุงเทพฯ : บริษัท ซีเอ็ดยูเคชั่น จำกัด

[22] Arkom Thaicharoen. “คำสั่งลินุกซ์” http://www.slideshare.net/arkomt?utm_campaign=ProFiletracking&utm_medium=sssite&utm_source=ssslideview.

[23] ทิวานนท์ จำพรต,เทพสรรค์ ปลอดอินทร์,ธนกร ดอนนา.“ตัวควบคุมโพลิซีไฟร์วอลโดยตรง.” วิทยานิพนธ์ปริญญาวิศวกรรมศาสตร์บัณฑิต, สาขาวิชาวิศวกรรมโทรคมนาคม คณะวิศวกรรมศาสตร์, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง, 2556.

[24]ดิษยา วงศ์บุญยิ่ง,เต็มสิริ แสงนวกิจ,ทองดี สินปุณย์.“การควบคุมแบนวิดธ์สำหรับหลายผู้ใช้บริการ.”วิทยานิพนธ์ปริญญาวิศวกรรมศาสตร์บัณฑิต, สาขาวิชาวิศวกรรม. โทรคมนาคม คณะวิศวกรรมศาสตร์, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง, 2556.

[26] ทศพล บุตรพรหม,ทิฏฐวัฒน์ คำเมือง,ธเนศ สีเชียงพิมพ์..“ระบบควมคุมการกระจายภาระงานเครื่องแม่ข่าย.”วิทยานิพนธ์ปริญญาวิศวกรรมศาสตร์บัณฑิต, สาขาวิชาวิศวกรรมโทรคมนาคม คณะวิศวกรรมศาสตร์, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง, 2556.