การตรวจสอบทราฟฟิคโดยการรวมเราเตอร์เพื่อช่วยการออกแบบระบบเครือข่ายคอมพิวเตอร์

TOTAL TRAFFIC MONITORING-BASED INTEGRATED ROUTERS FOR COMPUTER NETWORK AIDED-DESIGN

สุชาติ สิทธิสำอางค์

SUCHART SITTHISAM-ANG

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า
บัณฑิตวิทยาลัย
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2543

ISBN 974-622-703-3

การตรวจสอบทราฟฟิคโดยการรวมเราเตอร์เพื่อช่วยการออกแบบระบบเครือข่ายคอมพิวเตอร์

TOTAL TRAFFIC MONITORING-BASED INTEGRATED ROUTERS FOR COMPUTER NETWORK AIDED-DESIGN

สุชาติ สิทธิสำอางค์

SUCHART SITTHISAM-ANG

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมไฟฟ้า

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2543

ISBN 974-622-703-3

TOTAL TRAFFIC MONITORING-BASED INTEGRATED ROUTERS FOR COMPUTER NETWORK AIDED-DESIGN

SUCHART SITTHISAM-ANG

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF ENGINEERING IN ELECTRICAL ENGINEERING

SCHOOL OF GRADUATE STUDIES

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2000

ISBN 974-622-703-3

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ การตรวจสอบทราฟฟิคโดยการรวมเราเตอร์เพื่อช่วยการออกแบบระบบเครือข่ายคอมพิวเตอร์

TOTAL TRAFFIC MONITORING-BASED INTEGRATED ROUTERS FOR COMPUTER-NETWORK-AIDED-DESIGN

ชื่อนักศึกษา นายสุชาติ สิทธิสำอางค์

รหัสประจำตัว 40061042

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชา วิศวกรรมไฟฟ้า

อาจารย์ผู้ควบคุมวิทยานิพนธ์ รศ.ดร.กอบชัย เดชหาญ

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
ดร.วรวัฒน์	ลิ้มโภคำ	
ผศ.สมศักดิ์	มิตะถา	
ผศ.ดร.ไกรสิน	ส่งวัฒนา	
รศ.ดร.ฟูศักดิ์	ชีวสุวิทย์	
รศ.ดร.กอบชัย	เดชหาญ	

วัน/เดือน/ปี ที่สอบ 9 มีนาคม 2543 เวลา 11.00 - 12.00 น.

สถานที่สอบ ณ ห้องสอบวิทยานิพนธ์ คณะวิศวกรรมศาสตร์ ตึก 12 ชั้น ชั้น 4 ห้อง (E12-402)

บัณฑิตวิทยาลัยรับรองแล้ว

(รศ.ดร.มนัส สังวรศิลป์)

คณบดีบัณฑิตวิทยาลัย

วันที่ 12 **เดือน** มีนาคม **พ.ศ.** 2543

หัวข้อวิทยานิพนธ์	การตรวจสอบทราฟฟิคโดยการรวมเราเตอร์เพื่อช่วยการออกแบบระบบเครือข่ายคอมพิวเตอร์
นักศึกษา	นายสุชาติ สิทธิสำอางค์
รหัสประจำตัว	40061042
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมไฟฟ้า
พ.ศ.	2543
อาจารย์ผู้ควบคุมวิทยานิพนธ์	รศ.ดร.กอบชัย เดชหาญ

บทคัดย่อ

ระบบเครือข่ายคอมพิวเตอร์และสื่อสารข้อมูลในปัจจุบัน มีการเชื่อมต่อเข้าด้วยกันเป็นจำนวนมาก ไม่ว่าจะเป็นหน่วยงานของรัฐบาล เอกชน หรือสถาบันการศึกษาต่างๆ โดยเฉพาะอย่างยิ่ง การเชื่อมต่อกันผ่านระบบเครือข่ายอินเตอร์เน็ต เมื่อมีการเชื่อมต่อเครือข่ายเพิ่มมากขึ้น จะทำให้ปริมาณความหนาแน่นของทราฟฟิคในระบบเครือข่ายเพิ่มมากขึ้นตามไปด้วย วิทยานิพนธ์ฉบับนี้ได้ทำการศึกษาเกี่ยวกับการติดตั้งระบบเครือข่ายคอมพิวเตอร์ของกรมศุลกากรซึ่งมีการเชื่อมต่อระบบแบบออนไลน์ทั่วประเทศ และทำการวิเคราะห์ทราฟฟิคของเราเตอร์ เพื่อช่วยในการออกแบบระบบเครือข่ายคอมพิวเตอร์ และเพื่อรองรับการขยายตัวของระบบเครือข่ายในอนาคต ให้สามารถทำงานได้อย่างมีประสิทธิภาพ

Thesis Title	Total Traffic Monitoring-Based Integrated Routers for Computer Network Aided-Design
Student	Mr. Suchart Sitthisam-ang
Student ID.	40061042
Degree	Master of Engineering
Programme	Electrical Engineering
Year	2000
Thesis Advisor	Assoc.Prof.Dr.Kobchai Dejhan

ABSTRACT

There are interlinkages between computer network from government and private sector to academic organizations, all networks are connected via the Internet system. The traffic is increased with more connected networks. This thesis presents a study on the computer network of The Royal Thai Customs which has an on-line system all over the country. The router traffic has been analyzed in order to design the system to better serve the rapid growth of the network with better performance in the future.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้อย่างดี ด้วยคำแนะนำและคำปรึกษาเกี่ยวกับระบบเครือข่ายคอมพิวเตอร์และการตรวจสอบทราฟฟิคที่เกิดขึ้นบนระบบเครือข่าย ซึ่งผู้วิจัยขอขอบพระคุณแก่บุคคลดังต่อไปนี้

ขอขอบพระคุณ รองศาสตราจารย์ ดร.กอบชัย เดชหาญ ที่ช่วยให้คำแนะนำและช่วยเหลือทุกๆ อย่างในการจัดทำวิทยานิพนธ์

ขอขอบคุณ คุณทนง ธนพันธุ์พาณิชย์ และคุณเมธี โขนงนุช ที่ให้คำแนะนำ แลกเปลี่ยนความรู้และค้นคว้าข้อมูลเกี่ยวกับระบบเครือข่ายคอมพิวเตอร์และสื่อสารข้อมูล

ขอขอบคุณ Mr. Tobias Oetiker ที่ให้คำแนะนำและการทำความเข้าใจเกี่ยวกับการ Setup Configuration ของโปรแกรม MRTG

ขอขอบพระคุณ คุณพ่อ คุณแม่ พี่ๆ น้องๆ และเพื่อนๆ ที่ให้กำลังใจในการทำวิจัยเสมอมาจนวิทยานิพนธ์สำเร็จอย่างสมบูรณ์

คุณค่าและประโยชน์อันพึงมีจากวิทยานิพนธ์ฉบับนี้ ผู้วิจัยขอมอบแด่ผู้มีพระคุณทุกท่าน

สุชาติ สิทธิสำอางค์

สารบัญ

หน้า

บทคัดย่อภาษาไทย.....I

บทคัดย่อภาษาอังกฤษ.....II

กิตติกรรมประกาศ.....III

สารบัญ.....IV

สารบัญตาราง..... VII

สารบัญรูป..... VIII

บทที่ 1 บทนำ.....1

1.1 แนวความคิดของวิทยานิพนธ์ 1

1.2 วัตถุประสงค์ในการทำวิทยานิพนธ์ 1

1.3 รายละเอียดในวิทยานิพนธ์.....2

บทที่ 2 การออกแบบระบบเครือข่ายคอมพิวเตอร์.....3

2.1 ทฤษฎีการออกแบบระบบเครือข่ายคอมพิวเตอร์ 3

2.2 อุปกรณ์ที่ใช้ในการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ 5

2.2.1 ทรานซีฟเวอร์.....5

2.2.2 การ์ดเชื่อมโยงระบบเครือข่าย..... 6

2.2.3 รีพีทเตอร์..... 8

2.2.4 ฮับ..... 9

2.2.5 บริจ..... 11

2.2.6 เราเตอร์..... 16

2.3 IP ADDRESS.....24

บทที่ 3 อีเทอร์เน็ต 25

3.1 มาตรฐานของอีเทอร์เน็ต 26

3.1.1 ระบบเครือข่ายธิคอีเทอร์เน็ต..... 27

3.1.2 ระบบเครือข่ายธินอีเทอร์เน็ต..... 30

3.1.3 ระบบเครือข่ายมาตรฐาน 10BaseT..... 32

3.2 หลักการทำงานของอีเทอร์เน็ต 35

สารบัญ

หน้า

3.3 รูปแบบโครงสร้างการเชื่อมต่อของเครือข่าย.....35
3.3.1 โทโปโลยีแบบบัส..... 36
3.3.2 โทโปโลยีแบบริง..... 36
3.3.3 โทโปโลยีแบบสตาร์..... 37
3.4 ส่วนประกอบของอีเทอร์เน็ตเฟรม 38

บทที่ 4 โปรโตคอล เอสเอ็นเอ็มพี..... 40
4.1 ระดับชั้นของโปรดตคอลที่ใช้ในโปรแกรมบริหารระบบเครือข่าย 40
4.2 โครงสร้างของการบริหารระบบเครือข่าย 41
4.3 สถาปัตยกรรมของโปรโตคอลบริหารระบบเครือข่าย.....42
4.4 โครงสร้างของ Management Information.....42
4.4.1 การกำหนดรูปแบบโดยใช้ ASN.1 42
4.4.2 โครงสร้างและการแทนชื่อวัตถุที่อยู่ใน MIB 43
4.5 Simple Network Management Protocol.....48
4.6 SNMP Message Format 50

บทที่ 5 เราติงโปรโตคอล..... 53
5.1 เราติงโปรโตคอล.....53
5.1.1 Static Routing Protocol.....53
5.1.2 Dynamic Routing Protocol..... 53
5.2 Autonomous System 54
5.3 การติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์กับเราเตอร์ 55
5.4 การติดต่อสื่อสารระหว่างเราเตอร์กับเราเตอร์ 56
5.4.1 Interior Routing Protocol.....56
5.4.1.1 Routing Information Protocol.....57
5.4.1.2 Open Shortest Path First (OSPF).....57
5.4.1.3 Interior Gateway Routing Protocol (IGRP).....58

สารบัญ

หน้า

5.4.2 Exterior Routing Protocol..... 58
5.4.2.1 Exterior Gateway Protocol (EGP)..... 58
5.4.2.2 Border Gateway Protocol (BGP)..... 59

บทที่ 6 การติดตั้งระบบเครือข่ายคอมพิวเตอร์ของกรมศุลกากร 60
6.1 การติดตั้งระบบเครือข่ายคอมพิวเตอร์ตามหน่วยงานต่างๆ
ภายในกรมศุลกากรและบริเวณใกล้เคียง 63
6.1.1 ระบบเครือข่ายคอมพิวเตอร์ของ Central Router 1..... 64
6.1.2 ระบบเครือข่ายคอมพิวเตอร์ของ Central Router 2.....66
6.1.3 ระบบเครือข่ายคอมพิวเตอร์ของ Central Router 3..... 68
6.1.4 ระบบเครือข่ายคอมพิวเตอร์ของ Central Router 4.....70
6.1.5 ระบบเครือข่ายคอมพิวเตอร์ของ Central Router 5.....72
6.1.6 ระบบเครือข่ายคอมพิวเตอร์ของ Central Router 6.....74
6.2 การติดตั้งระบบเครือข่ายคอมพิวเตอร์ตามหน่วยงานต่างๆ
ภายนอกกรมศุลกากรและตามด่านศุลกากรภูมิภาคต่างๆ ทั่วประเทศ 76

บทที่ 7 การตรวจสอบทราฟฟิคของระบบเครือข่ายคอมพิวเตอร์ 78
7.1 MRTG (Multi Router Traffic Grapher) 78
7.2 การตรวจสอบทราฟฟิคที่เครือข่ายโดยรวมของเราเตอร์.....79
7.3 การตรวจสอบทราฟฟิคที่เครือข่ายย่อยของเราเตอร์.....91

บทที่ 8 บทสรุปและข้อเสนอแนะ..... 103

เอกสารอ้างอิง.....115

ภาคผนวก.....116
ประวัติผู้เขียน.....117

สารบัญตาราง

ตารางที่ หน้า

2.1 ระยะทางสูงสุดและอัตราเร็วการรับส่งข้อมูลของ Ethernet 4

2.2 ระยะทางสูงสุดและอัตราเร็วการรับส่งข้อมูลของ Fast Ethernet 4

2.3 ระยะทางสูงสุดและอัตราเร็วการรับส่งข้อมูลของ ATM 5

3.1 แสดงมาตรฐาน IEEE 802 ของเครือข่ายคอมพิวเตอร์ 25

3.2 ตำแหน่งขาสัญญาณของ 10BaseT 33

4.1 การแบ่งกลุ่มของ MIB.....45

4.2 ตัวอย่างชื่อตัวแปรใน MIB.....46

4.3 คำสั่งที่ใช้ใน SNMP.....48

สารบัญรูป

รูปที่ หน้า

2.1 ลักษณะของอุปกรณ์แบบธิคทรานซีฟเวอร์..... 5

2.2 Block Diagram ของการ์ดเชื่อมโยงระบบเครือข่าย..... 7

2.3 การเชื่อมต่อ IEEE 802.3 Repeater..... 8

2.4 การเชื่อมต่อภายในของ Hub configuration เบื้องต้น..... 9

2.5 Hub หรือ Concentrator Configuration..... 10

2.6 Local Bridge และ Remote Bridge..... 12

2.7 Bridging..... 13

2.8 Spanning Tree Algorithm..... 14

2.9 Source Route Bridging..... 15

2.10 Encapsulation และ Translation Bridging..... 16

2.11 การเปรียบเทียบ OSI 7-Layer กับอุปกรณ์เครือข่าย..... 17

2.12 ตัวอย่างการกำหนดค่า Network Number ของ TCP/IP และ IPX..... 18

2.13 ข้อแตกต่างการใช้ประโยชน์ของเส้นทางการสื่อสารของ Bridge กับ Router..... 18

2.14 ความแตกต่างของการส่งเฟรมข้อมูลผ่าน Bridge และ Router..... 20

2.15 การเปรียบเทียบ Protocol TCP/IP กับ OSI 7-Layer..... 21

2.16 ระดับมาตรฐานของ IP Address..... 22

2.17 แสดงการแบ่ง IP Address ตาม Class ต่างๆ..... 24

3.1 มาตรฐานของการให้บริการที่เป็นไปตามมาตรฐาน IEEE 802..... 26

3.2 การเชื่อมต่อระหว่างเซกเม็นท์..... 27

3.3 ส่วนประกอบของธิคอีเทอร์เน็ต..... 27

3.4 การเชื่อมต่อเครือข่ายธิคอีเทอร์เน็ต..... 29

3.5 ส่วนประกอบของธินอีเทอร์เน็ต..... 30

3.6 การเชื่อมต่อเครือข่ายธินอีเทอร์เน็ต..... 31

3.7 พอร์ทของการ์ดเชื่อมโยงระบบเครือข่ายแบบ 10BaseT..... 32

3.8 ลักษณะของ 10BaseT plug RJ-45 Connector..... 33

3.9 ลักษณะการต่อสายของ 10BaseT..... 34

3.10 ลักษณะการเชื่อมต่อเครือข่ายแบบ 10BaseT..... 34

สารบัญรูป

รูปที่ หน้า

3.11 การเชื่อมต่อโทโปโลยีแบบบัส..... 36

3.12 การเชื่อมต่อโทโปโลยีแบบริง.....37

3.13 การเชื่อมต่อโทโปโลยีแบบสตาร์.....38

3.14 โครงสร้างของอีเทอร์เน็ตเฟรม..... 38

4.1 Configuration ของ SNMP..... 43

4.2 การแทนชื่อวัตถุที่อยู่ใน MIB.....44

4.3 ค่า MIB ที่อยู่ภายใต้ iso.org.dod.internet.mgmt.mib หรือ 1.3.6.1.2..... 45

4.4 การทำงานของโปรโตคอล SNMP.....49

5.1 โครงสร้างของระบบ Routing Protocol.....54

5.2 ตัวอย่างการเชื่อมต่อของ Automous System.....55

6.1 ส่วนประกอบคอมพิวเตอร์หลักของระบบเครือข่าย.....61

6.2 แสดงแบบที่ได้จากการสำรวจตำแหน่งติดตั้งระบบเครือข่ายคอมพิวเตอร์.....62

6.3 การเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ภายในบริเวณกรมศุลกากร..... 63

6.4 การเชื่อมต่อระบบเครือข่ายของ Central Router 1.....65

6.5 การเชื่อมต่อระบบเครือข่ายของ Central Router 2.....67

6.6 การเชื่อมต่อระบบเครือข่ายของ Central Router 3.....69

6.7 การเชื่อมต่อระบบเครือข่ายของ Central Router 4.....71

6.8 การเชื่อมต่อระบบเครือข่ายของ Central Router 5.....73

6.9 การเชื่อมต่อระบบเครือข่ายของ Central Router 6.....75

6.10 การเชื่อมต่อระบบเครือข่ายภายนอกเข้ามาที่ศูนย์คอมพิวเตอร์หลัก.....76

6.11 การเชื่อมต่อระบบเครือข่ายจากสำนักงานศุลกากรภาคต่างๆ ทั่วประเทศ..... 77

7.1 ตัวอย่าง Interface Port ชนิดต่างๆ ของ Router.....79

7.2 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Central Router 1..... 80

7.3 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Central Router 2..... 81

7.4 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Central Router 3..... 82

7.5 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Central Router 4..... 83

7.6 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Central Router 5..... 84

7.7 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Central Router 6..... 85

สารบัญรูป

รูปที่ หน้า

7.8 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Access Router 1..... 86

7.9 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Access Router 2..... 87

7.10 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Access Router 3.....88

7.11 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Central Router 1..... 94

7.12 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Central Router 2..... 95

7.13 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Central Router 3..... 96

7.14 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Central Router 4..... 97

7.15 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Central Router 5..... 98

7.16 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Central Router 6..... 99

7.17 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Access Router 1.....100

7.18 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Access Router 2.....101

7.19 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Access Router 3.....102

8.1 แสดงการเชื่อมโยงระบบโทรศัพท์และแฟกซ์ผ่านระบบเครือข่ายแบบ Direct Line..... 105

8.2 แสดงการเชื่อมโยงระบบโทรศัพท์และแฟกซ์ผ่านระบบเครือข่ายแบบ Remote Extension... 105

8.3 แสดงการเชื่อมโยงระบบโทรศัพท์และแฟกซ์ผ่านระบบเครือข่ายแบบ Tie Line..... 107

8.4 แสดงการเฉลี่ยภาระของ Central Router 4 ให้กับ Central Router 1,2 และ 3 109

บทที่ 1
บทนำ

1.1 แนวความคิดของวิทยานิพนธ์

การออกแบบและติดตั้งระบบเครือข่ายคอมพิวเตอร์ เมื่อดำเนินการติดตั้งเสร็จแล้วและเริ่มมีการใช้งานจริง ผู้ดูแลและบริหารระบบเครือข่ายควรทำการตรวจสอบประสิทธิภาพของระบบเครือข่ายว่าสามารถใช้งานได้ดีเพียงใด ดังนั้นจึงเกิดแนวความคิดของวิทยานิพนธ์ฉบับนี้คือ การพิจารณาในการตรวจสอบทราฟฟิคของการรับส่งข้อมูลในแต่ละเครือข่ายย่อย ไปจนถึงเครือข่ายโดยรวมของระบบทั้งหมด สามารถทำการวิเคราะห์ได้จากปริมาณทราฟฟิคที่ผ่านเซนทอลเราเตอร์ ซึ่งเซนทอลเราเตอร์จะมีเครือข่ายย่อยหลายวงเชื่อมต่ออยู่ ในระบบเครือข่ายใหญ่ๆ ที่มีการเชื่อมต่อแบบออนไลน์ทั่วประเทศ จะมีเซนทอลเราเตอร์ต่ออยู่ในระบบหลายตัว เมื่อทำการวิเคราะห์ทราฟฟิคของเซนทอลเราเตอร์ทุกตัวก็สามารถจะทำให้ทราบถึงประสิทธิภาพโดยรวมของระบบเครือข่ายคอมพิวเตอร์ที่ทำการออกแบบไว้ได้

1.2 วัตถุประสงค์ในการทำวิทยานิพนธ์

ในการทำวิทยานิพนธ์เรื่อง การตรวจสอบทราฟฟิคโดยการรวมเราเตอร์เพื่อช่วยในการออกแบบระบบเครือข่ายคอมพิวเตอร์ ได้ศึกษาถึงการออกแบบติดตั้งระบบเครือข่ายคอมพิวเตอร์และศึกษาติดตามผลของการติดตั้งระบบ โดยการตรวจสอบจากปริมาณทราฟฟิคที่เกิดขึ้นในระบบเครือข่าย โดยได้กำหนดจุดประสงค์ไว้ดังนี้

- เพื่อศึกษาการออกแบบระบบเครือข่ายคอมพิวเตอร์สำหรับหน่วยงานขนาดใหญ่ที่มีเครือข่ายทั่วประเทศ ในที่นี้จะกล่าวถึงการออกแบบระบบเครือข่ายคอมพิวเตอร์ของกรมศุลกากร
- เพื่อศึกษาระบบเครือข่ายคอมพิวเตอร์แบบอีเทอร์เน็ต
- เพื่อศึกษาโปรโตคอล SNMP (Simple Network Management Protocol) ซึ่งเป็นโปรโตคอลที่ใช้สำหรับช่วยในการ จัดการระบบเครือข่าย
- เพื่อศึกษาและตรวจสอบประสิทธิภาพของระบบเครือข่าย ที่ทำการออกแบบและติดตั้งแล้ว
- เพื่อศึกษาการนำ Free Ware มาช่วยในการตรวจสอบทราฟฟิคของระบบเครือข่าย

1.3 รายละเอียดในวิทยานิพนธ์

ในวิทยานิพนธ์ฉบับนี้ ได้แบ่งเนื้อหาออกเป็นบทได้ทั้งหมด 8 บท โดยบทที่ 1 จะเป็นการกล่าวนำถึง แนวความคิดและวัตถุประสงค์ในการทำวิทยานิพนธ์ และได้กล่าวถึงเนื้อหาโดยย่อของแต่ละบท ซึ่งในบทอื่นๆ จะมีเนื้อหาดังนี้

บทที่ 2 กล่าวถึงการออกแบบระบบเครือข่ายคอมพิวเตอร์

บทที่ 3 กล่าวถึงทฤษฎีและหลักการของระบบเครือข่ายอีเทอร์เน็ต

บทที่ 4 กล่าวถึงชุดโปรโตคอล SNMP

บทที่ 5 กล่าวถึงเราติงโปรโตคอลที่ใช้งานในระบบเครือข่ายคอมพิวเตอร์

บทที่ 6 กล่าวถึงการติดตั้งระบบเครือข่าย ทั้งบริเวณภายในและภายนอกกรมศุลกากร รวมถึงด่านศุลกากรต่างๆ ทั่วประเทศ

บทที่ 7 กล่าวถึงวิธีการทำการทดลองตรวจสอบทราฟฟิคจากเครือข่ายที่ใช้งานอยู่จริง

บทที่ 8 กล่าวสรุปผลที่ได้รับและประโยชน์จากการทำวิจัยที่เกิดขึ้น และข้อเสนอแนะที่ได้จากประสบการณ์ในการติดตั้งระบบเครือข่ายคอมพิวเตอร์

บทที่ 2
การออกแบบระบบเครือข่ายคอมพิวเตอร์

2.1 การออกแบบระบบเครือข่ายคอมพิวเตอร์

การดำเนินงานติดตั้งระบบเครือข่ายคอมพิวเตอร์ มีขั้นตอนต่างๆ ดังต่อไปนี้คือ

1. ทำการกำหนดจุดหรือสถานที่ ที่จะให้มีการใช้ระบบเครือข่ายคอมพิวเตอร์แบบออนไลน์ ซึ่งประกอบไปด้วย

   1.1 ศูนย์คอมพิวเตอร์ประมวลผลหลัก ซึ่งใช้เป็นศูนย์กลางในการควบคุมการประมวลผลของระบบ อยู่ที่กรมศุลกากร คลองเตย

   1.2 หน่วยงานต่างๆ ภายในกรมศุลกากรและบริเวณใกล้เคียง

   1.3 หน่วยงานต่างๆ ภายนอกกรมศุลกากรรวมถึงด่านศุลกากรตามภูมิภาคต่างๆ ทั่วประเทศ

2. ทำการเลือกมาตรฐานของระบบเครือข่ายว่าจะใช้เป็นมาตรฐานเดียวกัน (Homogeneous Protocol) หรือจะใช้มาตรฐานการเชื่อมต่อหลายแบบ (Heterogeneous Protocol) ซึ่งมีมาตรฐานให้เลือกใช้หลายมาตรฐานด้วยกันเช่น TCP/IP, DECnet, OSI/ISO, Novell IPX, XNS, และ AppleTalk เป็นต้น หากทำการเลือกใช้มาตรฐานหลายแบบ สิ่งที่ต้องคำนึงถึงคือ จะต้องมีเกตเวย์ (Gateway) เพื่อใช้ในการจัดการกับการติดต่อสื่อสารระหว่างมาตรฐานที่ต่างกัน

3. เลือกสื่อกลางที่ใช้ในการเชื่อมต่อว่าจะใช้สื่อกลางชนิดใดบ้าง เช่น สื่อกลางมาตรฐาน 10Base5,10Base2, 10BaseT, 10BaseF, FDDI, Dial up, Leased line, Microwave, และ Satellite link เป็นต้น ซึ่งสื่อกลางแต่ละชนิดมีราคาที่แตกต่างกัน ความยากง่ายในการติดตั้งและการดูแลรักษา นอกจากนี้ยังมีระยะทางในการเชื่อมต่อที่แตกต่างกันอีกด้วย

4. เมื่อเลือกสื่อกลางได้แล้วก็ต้องทำการกำหนดโทโปโลยี (Topology) ซึ่งเป็นการกำหนดรูปแบบการเชื่อมต่อจุดต่างๆ เข้าด้วยกัน ซึ่งจะต้องสอดคล้องกับมาตรฐานของสื่อกลางที่ได้ทำการเลือกไว้ ในการกำหนดโทโปโลยี การเชื่อมต่อทำให้เราทราบว่า ระบบเครือข่ายที่ออกแบบไว้มีเซกเม็นท์ (Segment) ทั้งหมดกี่เซกเม็นท์ แต่ละเซกเม็นท์มีคอมพิวเตอร์เชื่อมต่ออยู่ทั้งหมดกี่เครื่อง และจำนวนอุปกรณ์ที่ใช้ในการเชื่อมต่อเซกเม็นท์ต่างๆ เข้าด้วยกัน เช่น รีพีทเตอร์, บริจ, เราเตอร์, และเกทเวย์

5. เมื่อทราบลักษณะการเชื่อมต่อและอุปกรณ์ที่ต้องใช้ทั้งหมดจากการออกแบบโทโปโลยีแล้ว ก็จะทำการเลือกอุปกรณ์ต่างๆ ที่จะนำมาเชื่อมต่อกันว่าสามารถทำงานร่วมกันได้หรือไม่ และจะต้องสามารถติดตั้งอุปกรณ์เหล่านั้นได้โดยง่าย

6. จัดทำ Network Blueprint ซึ่งการทำ Blueprint นี้จะคล้ายกับการออกแบบโทโปโลยีของระบบเครือข่าย แต่จะมีรายละเอียดในส่วนของความยาวและตำแหน่งหรือเส้นทางการติดตั้งของสายสัญญาณรายละเอียดของอุปกรณ์ฮาร์ดแวร์ต่างๆ รวมไปถึงองค์ประกอบของระบบเครือข่าย เช่น เวิคสเตชัน เซิฟเวอร์ รีพีทเตอร์ เราเตอร์ และเกทเวย์ เป็นต้น

7. จัดเตรียมคณะทำงาน เพื่อทำการติดตั้งระบบและเดินสายสัญญาณตามที่กำหนด และทำการทดสอบการทำการงานของระบบ [1]

การเลือกชนิดของมาตรฐาน, อุปกรณ์สื่อสาร, ชนิดของเครื่องคอมพิวเตอร์ หรือสายสัญญาณต่างๆ ที่จะใช้ในการเชื่อมต่อระบบ จะต้องพิจารณาจากส่วนประกอบหลายๆ อย่าง เช่น งบประมาณ, ความเร็วที่ต้องการในการรับส่งข้อมูลของระบบ, ระยะทางในการเชื่อมต่อระหว่างอุปกรณ์ชนิดต่างๆ และการเพิ่มเติมขยายระบบในอนาคต เป็นต้น สิ่งต่างๆ เหล่านี้มีความสำคัญอย่างมากในการออกแบบระบบเครือข่าย ตารางที่1,2 และ 3 แสดงชนิดของสายสัญญาณ, ความเร็วในการรับส่งข้อมูล และระยะทางที่สามารถใช้ในการติดตั้งอุปกรณ์ของมาตรฐาน Ethernet, Fast Ethernet และ ATM

ตารางที่ 2.1 แสดงระยะทางสูงสุดและอัตราการรับส่งข้อมูลของ Ethernet

Physical Media	**Max. Distance** (meters)	**Data Rate** (Mbps)
10base-T unshielded twisted pair	Up to 100	10
10base-2 thin coaxial cable	Up to 185	10
10base-5 thick coaxial cable	Up to 500	10
10base-F fiber optic cable	Up to 2,000	10

ตารางที่ 2.2 แสดงระยะทางสูงสุดและอัตราการรับส่งข้อมูลของ Fast Ethernet

Physical Media	**Max. Distance** (meters)	**Data Rate** (Mbps)
62.5 Micron multimode fiber optic Cabling (100base-FX)	Up to 412	100
Category 3 unshielded twisted pair (100base-T4)	Up to 100	100
Category 5 unshielded twisted pair (100base-TX)	Up to 100	100

ตารางที่ 2.3 แสดงระยะทางสูงสุดและอัตราการรับส่งข้อมูลของ ATM

Physical Media	**Max. Distance** (meters)	**Data Rate** (Mbps)
Category 3 unshielded twisted pair	Up to 100	25.6
Category 5 unshielded twisted pair	Up to 100	155.52
62.5 Micron multimode fiber optic Cabling	Up to 2,000	155.52

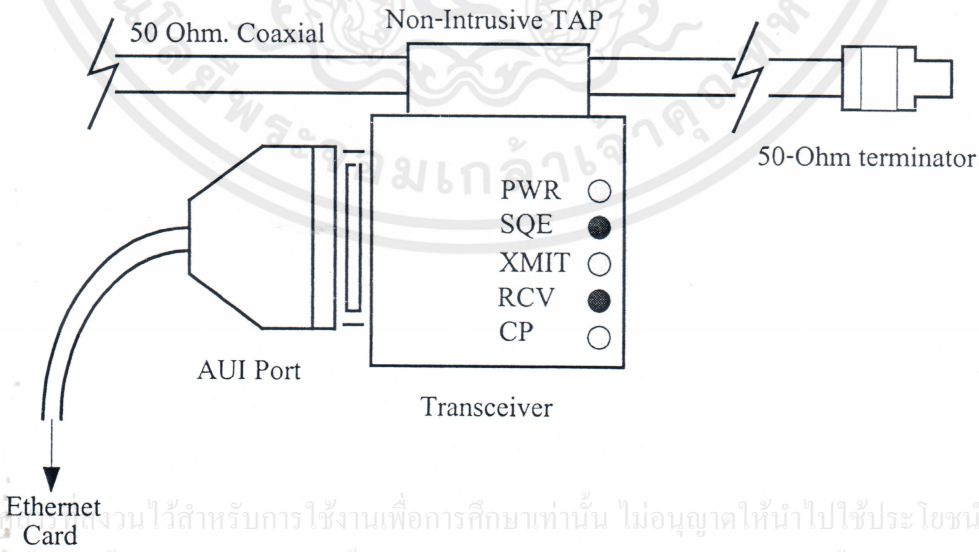
2.2 อุปกรณ์ที่ใช้ในการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์

อุปกรณ์สื่อสารที่ใช้ในการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์มีหลายชนิดด้วยกัน ซึ่งอุปกรณ์แต่ละชนิดจะมีลักษณะของการทำงานและหน้าที่ที่แตกต่างกันออกไป สามารถแบ่งชนิดของอุปกรณ์สื่อสารเหล่านี้ได้เป็น [2-3]

2.2.1 ทรานซีฟเวอร์ (Transceiver)

ทรานซีฟเวอร์ เป็นอุปกรณ์เครือข่ายที่มีใช้กันแทบทุกองค์กร เพราะเป็นอุปกรณ์ที่ทำหน้าที่แปลงสัญญาณจากสายเคเบิลชนิดต่างๆ ของระบบอีเทอร์เน็ตเป็นสัญญาณ AUI (Attachment Unit Interface) ผ่านการ์ดเชื่อมโยงระบบเครือข่าย (NIC-Network Interface Card) เข้าสู่สัญญาณคอมพิวเตอร์ ซึ่งสามารถจำแนกตามชนิดของสายเคเบิลบนระบบอีเทอร์เน็ตได้ดังนี้

1. Thick Transceiver จะแปลงสัญญาณจากสายธิคอีเทอร์เน็ต (Thick Ethernet) เป็นสัญญาณ AUI ต่อเข้ากับเครื่องคอมพิวเตอร์ในลักษณะบัสโทโปโลยี ลักษณะของอุปกรณ์แบบธิคทรานซีฟเวอร์แสดงได้ดังรูปที่ 2.1



รูปที่ 2.1 แสดงลักษณะของอุปกรณ์แบบธิคทรานซีฟเวอร์

2. Thin Transceiver ทำหน้าที่คล้ายกับธิคทรานซีฟเวอร์ คือมีพอร์ทที่ใช้ต่อกับสาย ธินอีเทอร์เน็ต (Thin Ethernet) และอีกด้านหนึ่งเป็นพอร์ท AUI

3. UTP Transceiver ใช้ต่อระหว่างสัญญาณ UTP (RJ-45 Connector) และสัญญาณ AUI ซึ่งเชื่อมต่อในลักษณะของโทโปโลยีแบบสตาร์ หรือแบบ Point-to-Point Network

4. Fiber Optic Transceiver ใช้เชื่อมระหว่างสัญญาณสาย Fiber Optic กับสัญญาณ AUI (ST-Connector) ใช้เชื่อมต่อในลักษณะเช่นเดียวกับโทโปโลยีของ UTP Transceiver

2.2.2 การ์ดเชื่อมโยงระบบเครือข่าย (NIC-Network Interface Card)

การที่จะต่อเครื่องคอมพิวเตอร์ต่างๆ เข้ากับระบบเครือข่าย โดยผ่านสายสัญญาณเคเบิลนั้น จำเป็นจะต้องมี Adapter Card ที่เปลี่ยนสัญญาณของเครื่องคอมพิวเตอร์เป็นสัญญาณเครือข่าย นั่นก็คือการ์ดเชื่อมโยงระบบเครือข่าย หรือเรียกอีกอย่างหนึ่งว่า LAN Adapter Card ซึ่งการ์ดเชื่อมโยงระบบเครือข่ายนี้นี้ มีพอร์ทเช่นเดียวกับทรานซีฟเวอร์ คือมีพอร์ทสำหรับต่อสายธินอีเทอร์เน็ต (BNC Connector), สาย UTP (RJ-45 Connector), Fiber Optic (ST Connector) และรวมทั้งพอร์ทสัญญาณ AUI ที่จะต่อเข้ากับทรานซีฟเวอร์อีกชั้นหนึ่ง

การที่จะติดตั้งการ์ดเชื่อมโยงระบบเครือข่ายนี้นี้ จำเป็นต้องมีโปรแกรมหรือที่เรียกว่า Driver ช่วยให้การ์ดเชื่อมโยงระบบเครือข่าย ทำงานบนเครื่องคอมพิวเตอร์ได้ ซึ่ง Driver นี้มีความแตกต่างกันมากมายตามแต่ชนิดของผู้ผลิต เช่น ODI (Open Data Link Interface) ของบริษัท Novell NDIS (Network Driver Interface Specification) ของ Microsoft และ Packet Driver ชนิดต่างๆ

หน้าที่ที่สำคัญของส่วนประกอบภายในวงจรทางด้านกายภาพของ Network Adapter ได้แก่

1 Transmit/receive module เป็นของวงจรที่ทำหน้าที่ในการ drive สัญญาณรับหรือส่งออกสู่สายสัญญาณ ในระดับพลังงานที่ขึ้นอยู่กับมาตรฐานที่กำหนดไว้

2 Encode/decode module เป็นชุดของวงจรที่ทำหน้าที่ในการเข้าหรือถอดรหัสจากสัญญาณที่จะส่งหรือรับเข้ามาจากเครือข่ายตามลำดับ เช่น มาตรฐานอีเทอร์เน็ตและ IEEE 802.3 จะใช้วิธีการเข้ารหัสแบบที่เรียกว่า Manchester Encoding, IEEE 802.5 เข้ารหัสแบบ Differential Manchester Encoding และถ้าเป็นกรณีเป็น FDDI จะใช้วิธีการเข้ารหัสผสมระหว่าง Non Return to Zero Inverted (NRZI) กับ 4B/4B encoding เป็นต้น

3 Frame buffer area เป็นพื้นที่ที่ใช้ในการพักข้อมูลก่อนที่จะมีการรับหรือส่ง ซึ่งเป็นพื้นที่พิเศษที่เป็น RAM อยู่บนการ์ดเชื่อมโยงระบบเครือข่าย ซึ่งอาจจะมีเนื้อที่ตั้งแต่ไม่กี่ Kbyte จนถึงขนาด Mbyte ทั้งนี้ก็ขึ้นอยู่กับชนิดหรือรุ่นของการ์ดเชื่อมโยงระบบเครือข่าย

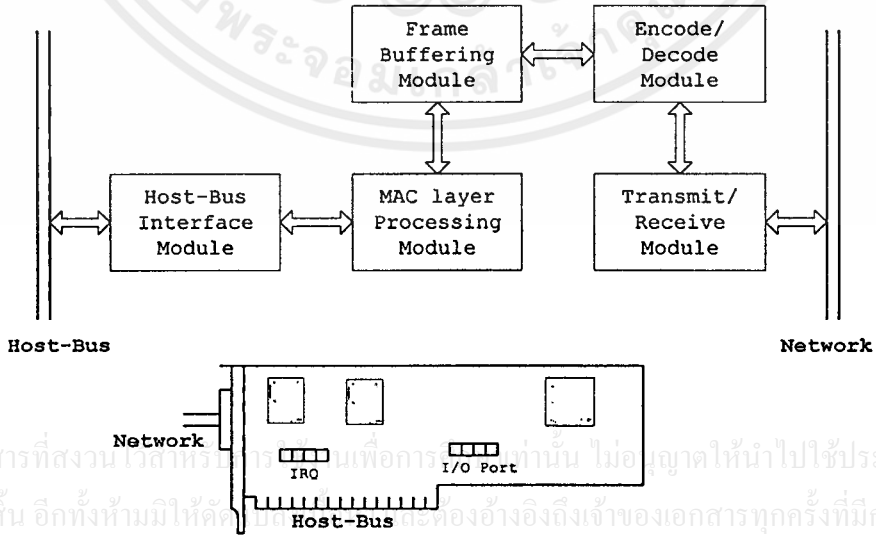
4 MAC layer processing module ชุดของส่วนที่เป็น MAC layer processing module เป็นส่วนที่สำคัญมากส่วนหนึ่งของการ์ดเชื่อมโยงระบบเครือข่าย ซึ่งทำหน้าที่ดังต่อไปนี้ คือ

Encapsulation/Decapsulation ขบวนการ Encapsulation function เป็นชุดที่ทำหน้าที่กระทำการแทรกข้อมูลข่าวสารต่างๆ เกี่ยวกับเวิคสเตชัน ระหว่างเวิคสเตชันต้นทางและปลายทาง ก่อนที่จะทำการส่งข้อมูล รามทั้งการสร้างข้อมูลเกี่ยวกับ correct address, control และ frame check sequence field เป็นต้น ส่วน Decapsulation จะทำหน้าที่ตรงข้ามกับขบวนการ Encapsulation กล่าวคือทำหน้าที่ในส่วนที่เกี่ยวกับชุดของขบวนการรับสัญญาณแล้วทำการถอด หรือตัดรหัสข้อมูลต่างๆ จนได้ข้อมูลที่แท้จริง

Implementation ในส่วนที่เกี่ยวกับ MAC algorithms (CSMA/CD access mechanism for Ethernet และ token access mechanism for Token ring) ซึ่งในปัจจุบัน ขบวนการทำงานของวิธีการ access ข้อมูลใน network จะบันทึกหรือสร้างเป็น special microprocessors ที่มี ROM หรือ microcode บันทึกเกี่ยวกับ MAC algorithms

5 Host-bus interface module เป็นส่วนที่ทำหน้าที่ในการ โต้ตอบสัญญาณ ควบคุม และจัดการเกี่ยวกับ data information ระหว่างการ์ดเชื่อมโยงระบบเครือข่ายผ่านทาง host-bus interface มาตรฐานที่เกี่ยวกับ Bus interface เช่น ISA bus, EISA bus หรือ Micro channel bus, PCI bus เป็นต้น

ซึ่งลักษณะทางด้านการเชื่อมต่อเป็นวงจรประกอบเข้าด้วยกันดังแสดงตามรูปที่ 2.2



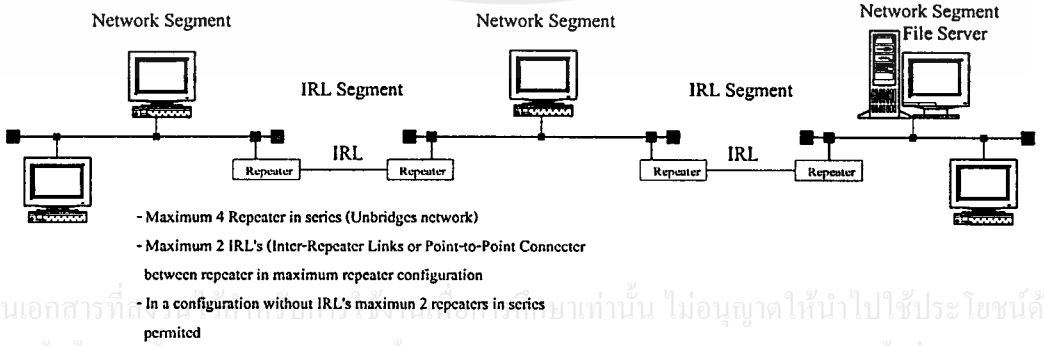
รูปที่ 2.2 แสดง Block Diagram ของการ์ดเชื่อมโยงระบบเครือข่าย

2.2.3 รีพีทเตอร์ (Repeater)

มาตรฐานสายเคเบิลต่างๆ นั้น ต่างก็มีขีดจำกัด ไม่ว่าจะเป็นความยาวสูงสุด หรือจำนวนจุดที่จะสามารถต่อเข้ากับคอมพิวเตอร์ดังที่กล่าวมาแล้ว แต่อย่างไรก็ตามด้วยความจำเป็นของเครือข่ายที่ต้องการใช้งานสูงเกินขีดจำกัดของมาตรฐานสายเคเบิล จึงได้มีอุปกรณ์ที่ทำหน้าที่ทวนสัญญาณทางไฟฟ้า (Signal Generating & Timing Repeating) เพื่อขยายขีดจำกัดการใช้งานให้มากขึ้น ซึ่งเรียกว่ารีพีทเตอร์ โดยทั่วไปแล้วจะมีพอร์ทด้วยกัน 2 พอร์ท ส่วนใหญ่จะมีพอร์ท AUI อย่างน้อย 1 พอร์ทเสมอ ทั้งนี้เพราะพอร์ท AUI สามารถเลือกต่อเข้ากับสายสัญญาณเคเบิลชนิดใดก็ได้ เพียงใช้อุปกรณ์ทรานซีฟเวอร์เข้ามาประกอบเท่านั้น แต่บางครั้งอุปกรณ์รีพีทเตอร์เอง ก็มีแบบชนิดหลายพอร์ทที่ใช้เชื่อมเข้ากับระบบเครือข่ายบนสายสัญญาณเคเบิลได้หลายเซกเม็นท์

เนื่องจากอุปกรณ์รีพีทเตอร์ ทำหน้าที่ในการทวนสัญญาณทางไฟฟ้าเท่านั้น จึงไม่สามารถแยกออกได้ว่า สัญญาณไฟฟ้านั้นเป็นข้อมูลชนิดใดของเครือข่าย ซึ่งในระบบเครือข่ายมาตรฐานที่เป็นอีเทอร์เน็ตนั้น จะมีข้อมูลชนิดหนึ่งที่เรียกว่า Jam Packet ซึ่งเกิดจากการชนกันของข้อมูล โดยเมื่อเกิดปรากฏการณ์นี้เกิดขึ้น จะทำให้ระบบเครือข่ายหยุดทำงานได้ชั่วขณะ จนกว่าข้อมูลนี้จะหายไป ดังนั้นการใช้งานอุปกรณ์รีพีทเตอร์จึงมีขีดจำกัดในระดับหนึ่งดังนี้

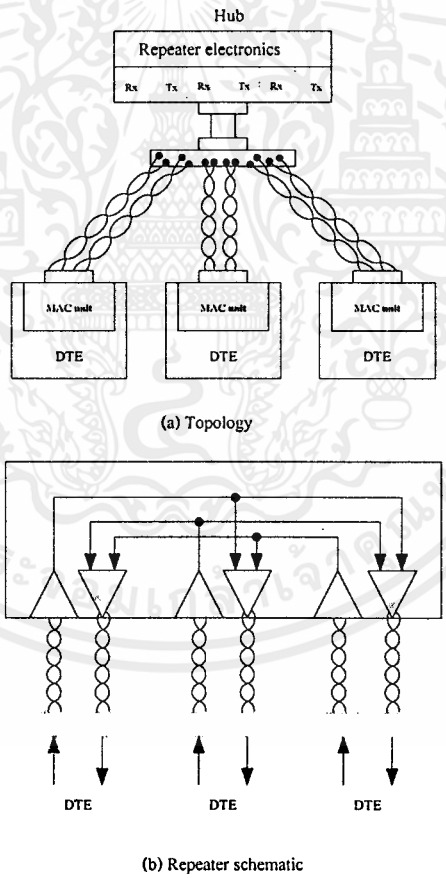
1. จะไม่นิยมใช้อุปกรณ์รีพีทเตอร์ชนิดหลายพอร์ทมากเกินไป เพราะเมื่อระบบเครือข่ายมีหลายเซกเม็นท์ หรือจำนวนเครื่องคอมพิวเตอร์มาก โอกาสที่จะเกิดการชนกันของข้อมูล หรือ Jam Packet ก็จะมีมากขึ้น
2. จำนวนเซกเม็นท์ของระบบการเชื่อมต่อในลักษณะอนุกรม (Series Connection) โดยมีอุปกรณ์รีพีทเตอร์เป็นตัวเชื่อมได้สูงสุด 4 เครื่อง (Repeater Hop) และมี 5 เซกเม็นท์ โดยที่ 2 เซกเม็นท์เป็นลักษณะ IRL (Inter-Repeater Links) ที่ไม่มีคอมพิวเตอร์ต่อเชื่อมอยู่ ดังรูปที่ 2.3



รูปที่ 2.3 แสดงการเชื่อมต่อ IEEE 802.3 Repeater

2.2.4 Hub หรือ Concentrator

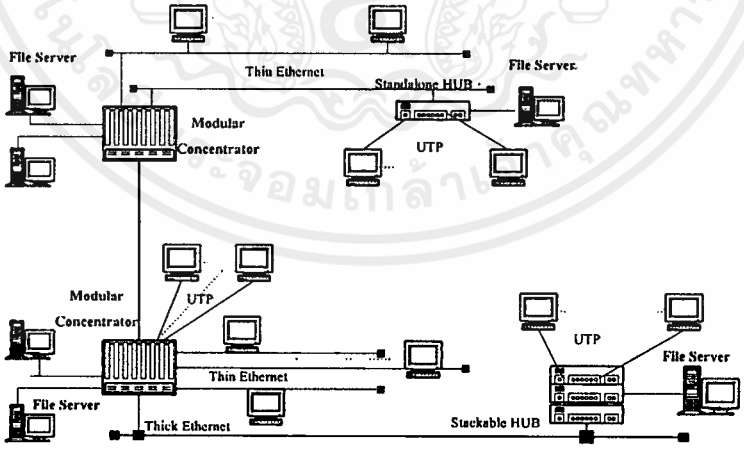
ส่วนใหญ่แล้วอุปกรณ์รีพีทเตอร์จะใช้กับมาตรฐานสายเคเบิลชนิดธิคอีเทอร์เน็ตและธินอีเทอร์เน็ต ส่วนสายเคเบิล UTP และ Fiber Optic นั้น จะนิยมใช้ในลักษณะโทโปโลยีแบบสตาร์ โดยมีจุดรวม (Center) แล้วกระจายสายเคเบิลออกไปในแต่ละจุด ซึ่งมองอีกมุมหนึ่งก็เป็นเสมือนอุปกรณ์ รีพีทเตอร์ชนิดหลายพอร์ท (Multiport Repeater) ที่ใช้กับมาตรฐานสายสัญญาณ UTP หรือ Fiber Optic นั้นเอง และก็เป็นที่นิยมใช้กันมากในปัจจุบัน โดยสามารถแบ่งตามจำนวนของพอร์ท UTP เช่น Hub ขนาดเล็กจะมีจำนวนพอร์ท UTP 8-12 พอร์ท และมีพอร์ทของสายเคเบิลแบบธิน (BNC Connector) หรือพอร์ท AUI อีก 1 พอร์ท ซึ่งบางครั้งเรียก Hub ชนิดนี้ว่า Standalone Hub และเมื่อเพิ่มจำนวนพอร์ท ขึ้นมาอยู่ในช่วง 24-100 พอร์ท พร้อมกับพอร์ทชนิดอื่น (BNC,ST,AUI) อีก 2-10 พอร์ท จะพบใน Hub ที่เรียกว่า Stackable Hub โดยมีลักษณะพิเศษที่สามารถเพิ่มจำนวนพอร์ทได้โดยผ่านสาย External Bus ซึ่งจะไม่เพิ่มจำนวนโหนด (Repeater Hop) แก่ระบบเครือข่าย



รูปที่ 2.4 แสดงการเชื่อมต่อภายในของ Hub configuration เบื้องต้น

นอกจากนี้ยังมีการออกแบบให้ Hub สามารถรองรับจำนวนพอร์ทต่างๆ ของสายสัญญาณ ได้เป็นจำนวนมาก (100-200 พอร์ท) ซึ่งจะมีโครงสร้างในลักษณะ Module และเรียก Hub ชนิดนี้ว่า Modular Concentrator และเนื่องจากว่า Hub นั้นได้ถูกออกแบบให้สามารถต่อเชื่อมได้หลายระบบหลายเซกเม็นท์ ซึ่งเกินขีดจำกัดของรีพีทเตอร์ ดังนั้น Hub จึงมีฟังก์ชันการทำงานมากขึ้นคือ

1. Automatically Segment Isolation เนื่องจาก Hub เชื่อมต่อเครือข่ายหลายเซกเม็นท์ จึงมีโอกาสที่จะเกิด Packet Jam สูง ดังนั้นเพื่อป้องกันการรบกวนของข้อมูลนี้ไม่ให้มีผลต่อเซกเม็นท์อื่น Hub จะทำการตัดการสื่อสารทางโลจิคอลกับเซกเม็นท์ที่เกิด Packet Jam จนกว่าจะกลับเข้าสู่ภาวะปกติ จึงจะทำการสื่อสารข้อมูลอีกครั้ง ซึ่งช่วยให้ลดอัตราการหยุดทำงานของระบบเครือข่ายลง
2. Auto Reverse Polarity เนื่องจากว่า Hub จะใช้เชื่อมต่อกับสายเคเบิล UTP เป็นส่วนใหญ่ และระบบสัญญาณของสายเคเบิล UTP นั้น มีขั้วบวกและขั้วลบ (Tx+, Tx- , Rx+, Rx-) และมีโอกาสอย่างมากที่จะมีการสลับขั้วของสายเคเบิล ซึ่งทำให้ไม่สามารถทำงานได้ ดังนั้น Hub จึงควรสามารถที่จะทำการตรวจสอบและแก้ไขสลับขั้วให้ถูก
3. Data Detection คือความสามารถที่จะแยกแยะข้อมูลต่างๆ ในระดับ Physical layer ได้ เช่น Sent/Receive Data, Collision Data, Auto Partition, Jabbers, Check sequence, Short Frame ,Too Long Frame, และ Alignment เป็นต้น ซึ่งจะช่วยให้ผู้ที่ดูแลระบบเครือข่ายแก้ปัญหาของระบบได้ในระดับหนึ่ง



รูปที่ 2.5 แสดง Hub หรือ Concentrator Configuration

2.2.5 Bridge

เมื่อระบบเครือข่ายคอมพิวเตอร์มีการขยายอย่างรวดเร็ว อุปกรณ์ดังเช่น Hub และรีพีทเตอร์จะไม่สามารถรองรับได้ ทั้งนี้เนื่องจากขีดหรือข้อจำกัดในการทำงานของอุปกรณ์ หรือลักษณะระบบเครือข่ายเองที่ไม่สามารถจะทำการขยายได้ ซึ่งสามารถสรุปได้ดังนี้

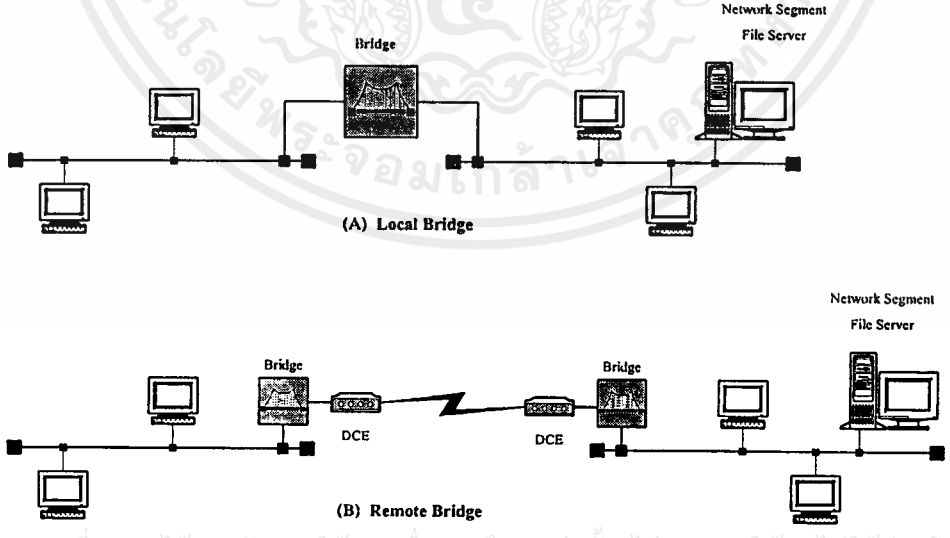
1. ในการติดต่อสื่อสารของเครื่องคอมพิวเตอร์ในแต่ละครั้ง เส้นทางที่ติดต่อกันนั้นจะต้องผ่าน Hub หรือรีพีทเตอร์ได้ไม่เกิน 4 ตัว โดยที่มีสายเชื่อมต่อ Hub หรือรีพีทเตอร์โดยตรง (IRL-Inter Repeater Link) ได้ไม่เกิน 2 ส่วน ตามข้อกำหนดที่ได้ระบุไว้
2. เมื่อมีจำนวนเครื่องคอมพิวเตอร์มากขึ้น ย่อมหมายถึงจำนวนข้อมูลที่สื่อสารกันในระบบเครือข่ายมากขึ้นด้วย ทำให้โอกาสที่จะมีการชนกันของข้อมูลสูง เป็นสาเหตุที่ทำให้เกิด Packet Jam ยังผลทำให้ประสิทธิภาพการทำงานของระบบต่ำลง เพราะเกิดความช้าในการสื่อสารบนเครือข่าย ดังนั้นจำเป็นจะต้องมีอุปกรณ์ที่สามารถจัดแบ่งปริมาณของข้อมูล ของระบบได้ ซึ่งฟังก์ชัน Automatically Segment Isolation ของ Hub ช่วยได้ในระดับหนึ่งเท่านั้น
3. ในการขยายระบบอาจมีการเชื่อมโยงติดต่อสื่อสารกันกับสาขาต่างๆ ที่อยู่ห่างไกลออกไปเกินขีดจำกัดของสายสัญญาณข้อมูล เช่นธิคอีเทอร์เน็ตสามารถวางแนวสายได้ไกลเพียง 2500 เมตรเท่านั้น ดังนั้นต้องอาศัยตัวกลางของระบบ WAN เช่น ระบบสายโทรศัพท์ ดาวเทียม ไมโครเวฟ ระบบ Fiber Optic ที่ให้บริการสาธารณะ เป็นต้น ซึ่ง Hub และรีพีทเตอร์ไม่สามารถรองรับการทำงานในระดับนี้ได้
4. ในบางระบบอาจมีการใช้มาตรฐานของระบบข้อมูลที่ต่างกันและเชื่อมเข้าด้วยกัน เช่น อาจมีระบบอีเทอร์เน็ตกับ Token Ring หรือระบบอีเทอร์เน็ต เชื่อมกับระบบ FDDI เป็นต้น โดยที่ Hub และรีพีทเตอร์ไม่มีความสามารถที่จะเชื่อมต่อระบบเหล่านี้เข้าด้วยกันได้
5. ในระบบที่ขาดการเดินสายที่ได้มาตรฐาน เมื่อมีการขยายขนาดของระบบของเครือข่ายออกไป ส่งผลทำให้การดูแลรักษาโดยเฉพาะสายสัญญาณสื่อสารข้อมูลนั้น จะมีความยุ่งยากมาก ซึ่งอาจมีผลมาจากการวางหรือเดินสายสัญญาณข้อมูลผิดไปจากข้อกำหนดหรือกฎเกณฑ์ที่ได้ระบุไว้ ทำให้เกิดการวนลูป (Loop) ของระบบ และส่งผลทำให้เกิดปัญหาอย่างร้ายแรงได้
6. เนื่องจากฟังก์ชันหลักของ Hub และรีพีทเตอร์คือทวนสัญญาณทางไฟฟ้าไปตามพอร์ทต่างๆ เท่านั้น ดังนั้นข้อมูลต่างๆ ที่อยู่ในระหว่างการติดต่อสื่อสารกันของคอมพิวเตอร์เครื่องใดๆ ก็ตาม จะถูกส่งไปทุกๆ ส่วนของระบบ และระบบที่มีเพียง Hub หรือรีพีทเตอร์จึงขาดในเรื่องความปลอดภัยของระบบ (Security)

จาก 6 ข้อหลักที่กล่าวมานั้น จึงจำเป็นต้องมีอุปกรณ์เครือข่ายที่มีฟังก์ชันการทำงานมากขึ้น ซึ่งในปัจจุบันมีด้วยกัน 2 กลุ่ม คือ Bridge และเราเตอร์โดยที่ Bridge ทำงานในระดับ Data Link Layer ส่วนเราเตอร์มีการทำงานที่ซับซ้อนมากขึ้นในระดับ Network Layer

2.2.5.1 คุณลักษณะของ Bridge

Bridge เป็นอุปกรณ์คอมพิวเตอร์ที่มีฟังก์ชันการทำงานในระดับ Data Link ดังนั้น Bridge จึงสามารถอ่านและเข้าใจเฟรมข้อมูลในระดับ Data Link Layer ได้ ซึ่งต่างกับ Hub หรือรีพีทเตอร์ที่ทำหน้าที่เพียงทวนสัญญาณทางไฟฟ้าในลักษณะบิทต่อบิทเท่านั้น Bridge จะมีหน่วยประมวลผลกลางและหน่วยความจำที่ใช้ในการพิจารณาความหมายของเฟรมข้อมูลที่ส่งผ่าน โดยปกติแล้วเฟรมข้อมูลใน Data Link layer ประกอบด้วย 3 ส่วนใหญ่ๆ คือ ส่วนหัว ส่วนข้อมูล และส่วนตรวจสอบ ในส่วนหัว (Header) ของข้อมูลจะมีค่าแสดงที่อยู่ (Address) ของเครื่องต้นทางที่จะส่ง (SA-Source Address) และเครื่องปลายทาง (DA-Destination Address) ที่ข้อมูลนั้นจะส่งไปถึง ดังนั้น Bridge จึงสามารถพิจารณาในการติดต่อสื่อสารกันแต่ละครั้งได้ว่าข้อมูลควรจะถูกส่งไปยังเซกเม็นท์ใดในระบบ

Bridge สามารถแบ่งได้เป็น 2 ชนิด คือ Bridge ที่ใช้ขยายระบบลักษณะในพื้นที่ใกล้กันเรียกว่า Local Bridge และที่ใช้เชื่อมระบบที่อยู่ไกลกันที่ต้องอาศัย WAN ประกอบ เรียกว่า Remote Bridge เนื่องจากระบบมาตรฐานต่างๆ เช่นระบบอีเทอร์เน็ต, Token Ring และ FDDI มีความแตกต่างกัน ดังนั้น Bridge ที่ใช้สำหรับแต่ละระบบจึงมีฟังก์ชันการทำงานที่แตกต่างกัน ดังนี้

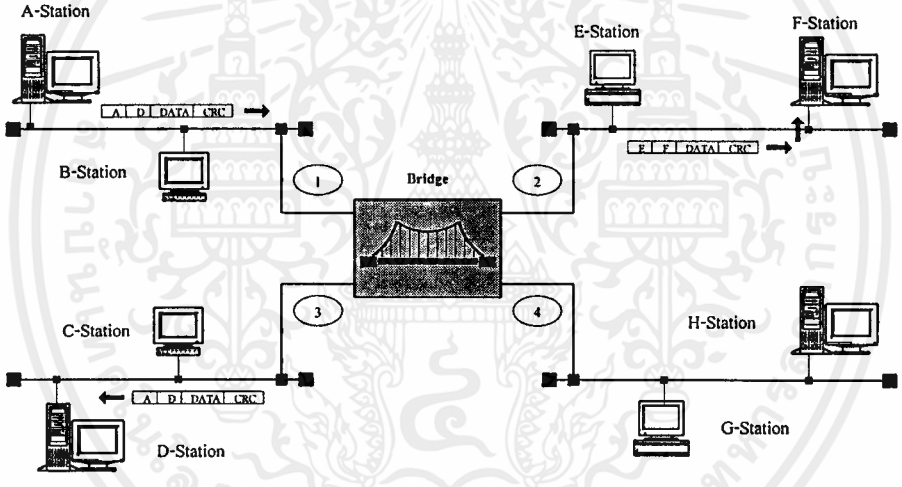


รูปที่ 2.6 แสดง Local Bridge และ Remote Bridge

2.2.5.2 TB (Transparent Bridge)

TB หรือบางครั้งเรียกว่า Leaning Bridge เป็น Bridge ที่ใช้ในระบบมาตรฐานอีเทอร์เน็ต และระบบ FDDI หลักการของ TB คือ Bridge จะมีตารางข้อมูลที่เก็บค่าที่อยู่ของเครื่องต่างๆ (MAC Address Table) Bridge จะใช้ตารางนี้พิจารณาว่าเครื่องคอมพิวเตอร์เครื่องใดอยู่ในเซกเม็นท์ใดของระบบ

การสร้างตาราง MAC Address นี้ Bridge จะอาศัยการเรียนรู้ค่าที่อยู่ของเครื่องต้นทาง (SA) และเครื่องปลายทาง (DA) ในเฟรมข้อมูลต่างๆ ที่ผ่านตัวมัน โดยค่าที่อยู่ของเครื่องต้นทางคือเครื่องที่มีค่าอยู่บนเซกเม็นท์ด้านที่รับเฟรมข้อมูลนั้น ส่วนค่าที่อยู่ของเครื่องปลายทาง Bridge จะพิจารณาที่ตารางค่า MAC Address ว่าค่านี้ อยู่ที่เซกเม็นท์ใด แล้วก็ส่งผ่านเฟรมข้อมูลออกไปที่เซกเม็นท์นั้น แต่ถ้าค่าที่อยู่ของเครื่องปลายทางนั้น ไม่มีในตาราง MAC Address Bridge ก็จะส่งข้อมูลไปทุกๆ เซกเม็นท์จนกว่า Bridge จะเรียนรู้ว่าค่าที่อยู่ค่านี้อยู่ที่เซกเม็นท์ด้านใด

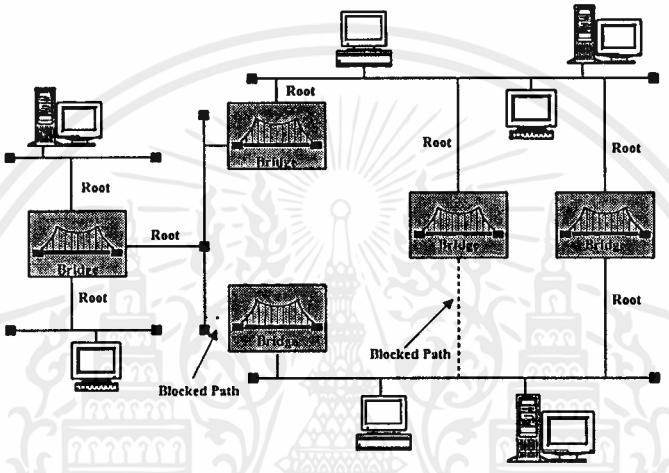


รูปที่ 2.7 แสดง Bridging

จากรูปที่ 2.7 เมื่อเฟรมข้อมูลจากเครื่อง A ถูกส่งผ่านเข้ามาที่เซกเม็นท์ที่ 1 ถ้า Bridge ตรวจดู แล้วปรากฏว่าค่าที่อยู่ของเครื่องปลายทางคือเครื่องที่ D ก็จะส่งผ่านข้อมูลนั้นออกไปยังเซกเม็นท์ที่ 3 และถ้าที่อยู่ของเครื่องปลายทางเป็นเครื่องที่ B ก็จะส่งข้อมูลนั้นกลับไปยังเซกเม็นท์เดิม (เซกเม็นท์ที่ 1)

จากการที่ TB สามารถอ่านและรู้ว่าเฟรมข้อมูลนั้น ถูกส่งจากที่ใดและจะไปที่เซกเม็นท์ไหนทำให้สามารถช่วยลดจำนวนปริมาณข้อมูลที่ไม่จำเป็นในแต่ละเซกเม็นท์ของระบบได้ (Isolate Intrasegment traffic) ซึ่งโอกาสที่จะเกิดสาเหตุของ Packet Jam จึงมีน้อยลง ทำให้ระบบเครือข่ายสามารถเชื่อมต่อจำนวนคอมพิวเตอร์ได้มากขึ้น

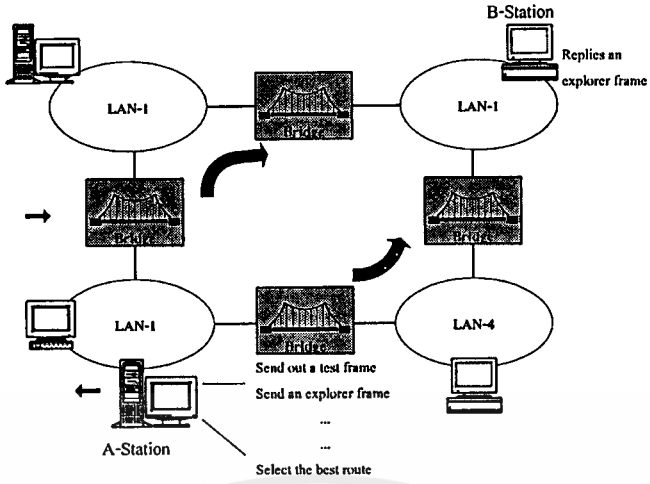
สำหรับปัญหาของระบบที่เกิดจากการวนลูปของเส้นทาง Bridge จะสามารถแก้ปัญหานี้ได้โดยวิธี Spanning Tree Algorithm ซึ่ง Bridge ทุกเครื่องจะมีการติดต่อสื่อสารกัน แล้วเลือกมาเครื่องหนึ่งเรียกว่า Root Bridge จะคอยทำหน้าที่เลือกเส้นทางหลัก (Root Path) สำหรับการติดต่อสื่อสารของระบบ ซึ่งจะผ่านไปทุกๆ ส่วนโดยไม่มีการวนลูป ส่วนเส้นทางที่ไม่ได้เลือก Bridge จะกันไม่ให้มีข้อมูลวิ่งผ่าน และจะใช้ก็ต่อเมื่อเส้นทางหลักใช้งานไม่ได้เท่านั้น หลังจากนั้นก็จะแจ้งไปให้ Bridge เครื่องอื่นๆ รับทราบกัน ดังนั้นเมื่อมีการเพิ่มหรือลดจำนวนของ Bridge จะทำให้ระบบเครือข่ายเกิดการหยุดการทำงานชั่วคราวเพื่อหา Root Bridge และ Root Path ตามลำดับ



รูปที่ 2.8 แสดง Spanning Tree Algorithm

2.2.5.3 SRB (Source Route Bridge)

SRB เป็น Bridge ที่ใช้กับระบบมาตรฐาน Token Ring ของ IBM ระบบนี้ Bridge จะทำหน้าที่เพียงส่งผ่านหรือกันข้อมูลเท่านั้น ส่วนการเลือกเส้นทางของการติดต่อสื่อสารข้อมูล เครื่องคอมพิวเตอร์ที่จะส่ง จะต้องพิจารณาเลือกเส้นทางเอง ก่อนที่จะมีการติดต่อสื่อสารกันในแต่ละครั้ง เครื่องจะส่งข้อมูลที่เรียกว่า Explorer frame ออกไป ซึ่งเฟรมข้อมูลนี้จะส่งผ่านไปยังทุกส่วนของระบบ จนกระทั่งเครื่องปลายทางได้รับเฟรมข้อมูลและตอบรับกลับมา เมื่อเครื่องต้นทางได้รับเฟรมข้อมูลตอบรับ (ปกติจะมีเฟรมข้อมูลตอบรับมากกว่าหนึ่งเฟรม) ก็จะพิจารณาเส้นทางต่างๆ ซึ่งถูกบันทึกไว้ในเฟรมนั้น โดยเลือกเส้นทางที่ดีที่สุด และก็ทำการเริ่มต้นติดต่อสื่อสารข้อมูลกัน โดยที่เฟรมข้อมูลที่ส่งออกไปนั้น จะมีส่วนเก็บรายละเอียดของเส้นทางการติดต่อสื่อสาร เรียกว่า RIF (Routing Information Field) Bridge จะใช้ข้อมูลใน RIF พิจารณาว่าเฟรมข้อมูลที่จะส่งนั้น ควรส่งผ่านไปยัง Ring วงใดต่อไป ดังแสดงได้ตามรูปที่ 2.9



รูปที่ 2.9 แสดง Source Route Bridging

2.2.5.4 SRT (Source Route Transparent)

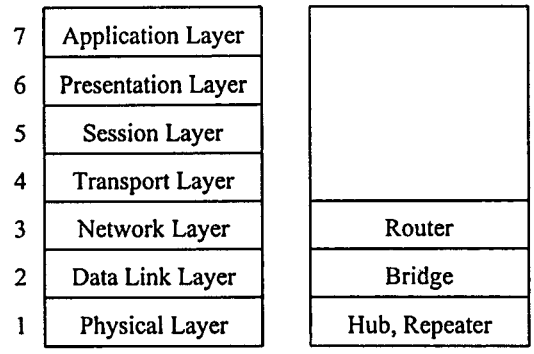
ในระบบเครือข่ายคอมพิวเตอร์ที่มีการเชื่อมระหว่างระบบอีเทอร์เน็ตกับระบบ Token Ring ในตัวอุปกรณ์ Bridge เองสามารถที่จะอ่านและเข้าใจเฟรมข้อมูลทั้งด้านที่ต่อกับอีเทอร์เน็ตและด้านที่ต่อกับ Token Ringได้ เฟรมข้อมูลที่ส่งผ่าน Bridge นั้นจะถูกเปลี่ยนรูปแบบของเฟรมใหม่ให้ถูกต้องกับระบบด้านที่จะส่งผ่านออกไป ดังนั้นจึงทำให้เครื่องคอมพิวเตอร์ที่อยู่บนอีเทอร์เน็ต สามารถติดต่อสื่อสารกับเครื่องที่อยู่ในวงของ Token Ring ได้ เช่นในระบบ NetWare เครื่องคอมพิวเตอร์อยู่บนอีเทอร์เน็ตสามารถที่จะทำการ login เข้าใช้ File Server ที่อยู่บน Token Ring เป็นต้น

Translational Bridge

เป็น Bridge ที่ใช้สำหรับเครือข่ายที่มีการใช้มาตรฐาน FDDI กับระบบอื่น เช่น FDDI กับอีเทอร์เน็ตเป็นต้น เมื่อมีเฟรมข้อมูลที่จะส่งผ่านไปยังอีกระบบ Bridge ก็จะทำการเปลี่ยนโครงสร้างทั้งหมดของเฟรมข้อมูลจากระบบหนึ่งไปยังอีกระบบหนึ่ง

Encapsulation Bridge

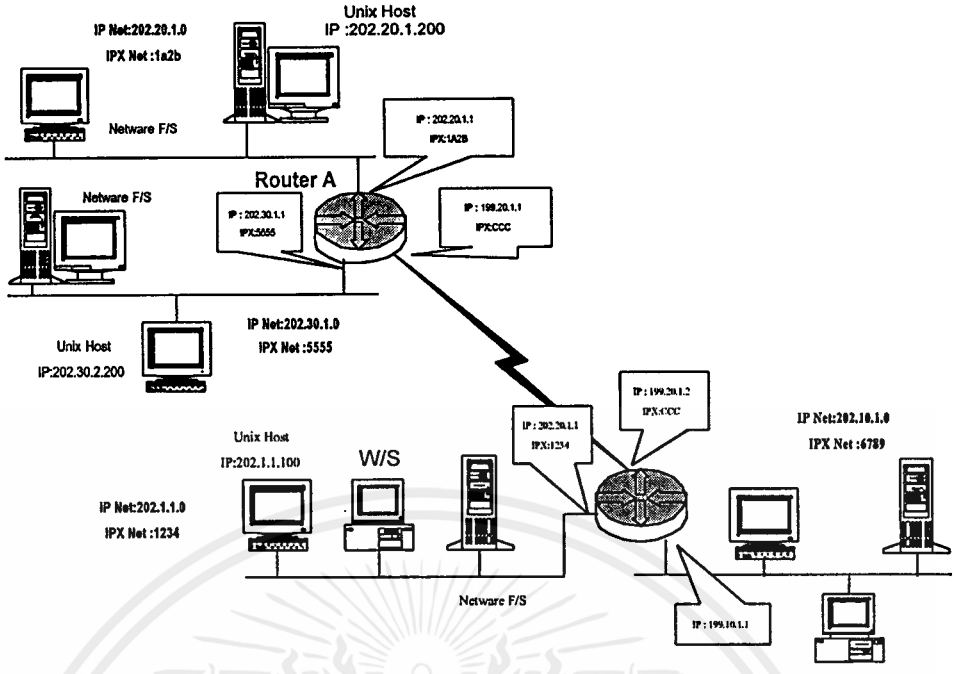
ในระบบเครือข่ายผสมที่มีระบบมาตรฐาน FDDI อยู่ด้วยนั้น นอกจากจะใช้วิธีการเปลี่ยนแปลงโครงสร้างทั้งหมดของเฟรมข้อมูลแล้ว ยังสามารถใช้วิธีหุ้มข้อมูลของระบบนั้น ด้วยรูปแบบและมาตรฐานของ FDDI แล้วแกะหรือถอดส่วนที่หุ้มนั้นออกเมื่อถึง Bridge ปลายทาง



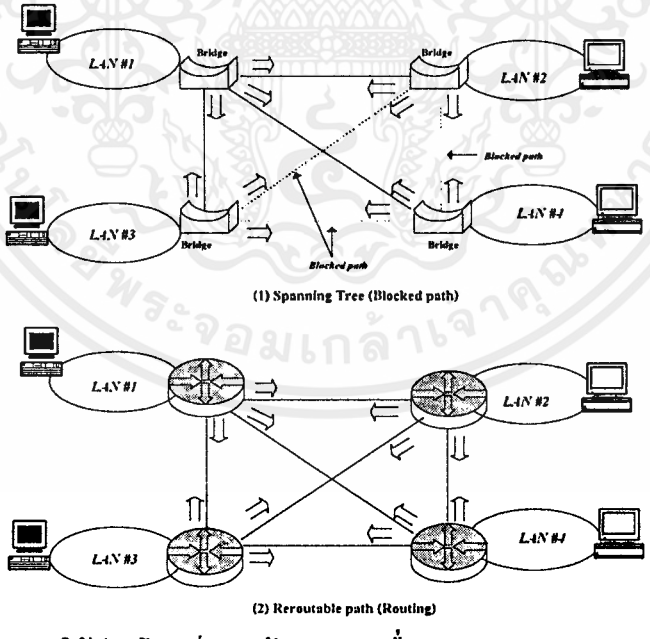
รูปที่ 2.11 แสดงการเปรียบเทียบ OSI 7-Layer กับอุปกรณ์เครือข่าย

2. การควบคุมและการออกแบบระบบเครือข่าย ตามที่ได้กล่าวมาแล้วว่า ระบบหรือเครือข่ายคอมพิวเตอร์ต่างๆ จะติดต่อสื่อสารกันได้ จะต้องใช้รหัสตัวเลขหรือระบบ Address เป็นจุดอ้างอิงเสมอ เช่นในระดับ Data Link Layer ก็จะใช้ค่าของ MAC Address เป็นจุดอ้างอิงเครื่องต้นทางและปลายทาง ค่านี้มีขนาด 6 ไบท์ ซึ่งกำหนดมาจากโรงงานผลิตโดยตรง และจะมีอยู่กับทุกเครื่องคอมพิวเตอร์ที่ต่อเป็นเครือข่าย เนื่องจากค่านี้มีจำนวนและรูปแบบตัวเลขที่มาก ทำให้ยากต่อการจดจำ และตรวจสอบของผู้บริหารเครือข่าย เมื่อผู้บริหารเครือข่ายจะออกแบบระบบ Address ให้กับเครื่องคอมพิวเตอร์นั้น ถ้าใช้ค่า MAC Address แล้ว จะมีความยุ่งยากอย่างมาก และการทำงานของระบบคอมพิวเตอร์ในระดับ Network Layer จะมีค่าระบบ Address ซึ่งเป็นค่าทางเชิงโลจิคอลที่สามารถกำหนดขึ้นเองได้ พร้อมทั้งมีรูปแบบที่ง่ายและสะดวกต่อการออกแบบเป็นอย่างมาก เช่นในระบบ UNIX มีค่า IP Address ซึ่งได้แบ่งออกเป็น 2 ฟิลด์ย่อย คือ IP Network Address และ IP Host Address เป็นตัวอ้างอิง และในระบบเครือข่ายที่มีค่า Internal Network Number และ External Network Number เป็นตัวอ้างอิง ดังแสดงตามรูปที่ 2.12 ดังนั้นโดยทั่วไปแล้ว ในปัจจุบันผู้บริหารเครือข่ายจะใช้ข้อกำหนดนี้ เป็นค่าอ้างอิงในการออกแบบและกำหนดเครือข่ายขององค์กร

3. การใช้ประโยชน์ของเส้นทางสื่อสาร ในระบบเครือข่ายที่มีขนาดใหญ่ และมีการเชื่อมโยงกันหลายๆ เครือข่าย ทั้งในเครือข่ายหลักและเครือข่ายย่อย (Sub Network) เส้นทางการเชื่อมต่อนั้นจะเป็นลักษณะใยแมงมุม (Mesh Topology) และมีจำนวนลูปมาก ซึ่ง Bridge จะใช้โครงสร้างที่เรียกว่า Spanning Tree ทำการเลือกเส้นทางหลัก (Root Path) ของระบบในลักษณะ Tree ที่ไม่มีการวนลูป คล้ายกับรากของต้นไม้ที่ขยายเรื่อยๆ ไปนั่นเอง ในลักษณะเช่นนี้ จะทำให้มีเส้นทางที่เชื่อมต่อระบบบางเส้นทางไม่ได้ใช้ประโยชน์อย่างมีประสิทธิภาพ หรือแม้แต่เส้นทางหลักที่เลือกนั้น อาจไม่ใช้เส้นทางที่ดีที่สุดของเครือข่ายคอมพิวเตอร์คู่ใดคู่หนึ่ง ดังแสดงตามรูปที่ 2.13



รูปที่ 2.12 ตัวอย่างการกำหนดค่า Network Number ของ Protocol TCP/IP และ IPX



รูปที่ 2.13 ข้อแตกต่างการใช้ประโยชน์ของเส้นทางการสื่อสารของ Bridge กับ Router

4. ปัญหาของระบบมาตรฐาน Data Link ที่ต่างกัน และถ้ามีการเชื่อมต่อระบบเครือข่ายที่แตกต่างกัน (อีเทอร์เน็ตกับ Token Ring, หรืออีเทอร์เน็ต กับ FDDI เป็นต้น) ด้วย Bridge จะใช้หลักการแปลงเฟรมข้อมูลไปมาระหว่างระบบนั้นๆ ซึ่งจะเพิ่มการทำงานของอุปกรณ์ และระบบนี้ก็ยังไม่เป็นมาตรฐานดีพอในปัจจุบัน แต่ถ้าเชื่อมต่อระบบเครือข่ายด้วยเราเตอร์แล้ว เราเตอร์จะพิจารณารูปแบบเฟรมข้อมูลของระบบ Network layer เท่านั้น ทำให้ปัญหาการเชื่อมต่อหลายๆ แบบของระบบเครือข่ายหมดไป

5. ความผิดพลาดของระบบเครือข่าย เมื่อส่งข้อมูลผ่าน Bridge หรือเราเตอร์มีขนาดเกินขีดจำกัด ข้อมูลนั้นก็จะถูกอุปกรณ์นั้นๆ ตัดทิ้ง (Drop) แต่สิ่งที่ต่างกันระหว่าง Bridge กับเราเตอร์คือ Bridge ไม่มีส่วนที่ตรวจสอบความผิดพลาดของเฟรมข้อมูล ซึ่งจะทำการตัดข้อมูลนี้ทิ้งอย่างเดียวโดยไม่มีการแจ้งกลับไปยังเครื่องต้นทาง ทำให้เกิดความพยายามที่จะส่งข้อมูลนั้นอีกหลายครั้ง ซึ่งมีผลทำให้ประสิทธิภาพโดยรวมของระบบจะมีค่าความผิดพลาดของข้อมูลมาก แต่สำหรับเราเตอร์แล้วสามารถแจ้งกลับไปยังเครื่องต้นทางได้ ซึ่งทำให้ลดค่าความผิดพลาดลงได้ดี

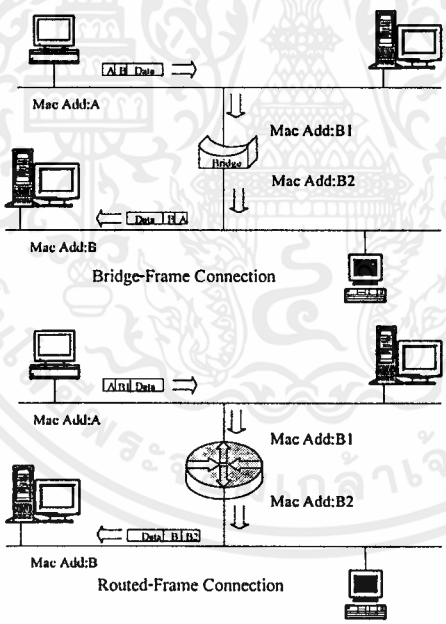
กล่าวโดยรวมแล้ว Bridge จะถูกออกแบบไว้สำหรับเครือข่ายที่มีขนาดไม่ใหญ่มากนัก มีการติดต่อสื่อสารข้ามเซกเม็นท์เพียง 1-2 เซกเม็นท์ แต่สำหรับเราเตอร์แล้ว จะถูกออกแบบให้เป็นตัวรองรับจุดเชื่อมศูนย์กลางของระบบเครือข่ายขนาดใหญ่ ซึ่งสามารถจัดสรรเส้นทางการวิ่งของข้อมูลได้อย่างมีประสิทธิภาพดี

2.2.6.1 การทำงานของเราเตอร์

การที่จะเข้าใจการทำงานของเราเตอร์ได้ดีนั้น ไม่ใช้เป็นสิ่งที่ง่ายนัก เพราะในการติดตั้งเราเตอร์ต้องกำหนดพารามิเตอร์ต่างๆ มาก ซึ่งจุดนี้เองทำให้ผู้บริหารเครือข่ายทั้งหลาย ไม่ชอบที่จะใช้เราเตอร์มาช่วยขยายระบบในช่วงแรก ต่างกับ Bridge ที่เพียงเปิดไฟแล้วใช้งานได้เลย (Plug and Play) แต่อย่างไรก็ตาม ด้วยเหตุผลต่างๆ ที่ได้กล่าวมาแล้ว ทำให้ผู้บริหารเครือข่ายต่างยอมรับและพยายามศึกษาเรียนรู้ระบบเราเตอร์กันมากขึ้น ในการพิจารณาการทำงานของระบบเราเตอร์ได้ดีนั้น ควรพิจารณาการทำงานของระบบเครือข่ายเป็น 2 ส่วน คือ การติดต่อสื่อสารระหว่างเราเตอร์กับเครื่องคอมพิวเตอร์ และการติดต่อสื่อสารระหว่างเราเตอร์กับเราเตอร์

ในระบบคอมพิวเตอร์โดยทั่วไป จะมีการแบ่งขอบเขตของการสื่อสารกัน เพื่อประสิทธิภาพโดยรวมของระบบที่ดี ซึ่งในการแบ่งขอบเขตนั้นจะแบ่งในลักษณะเชิงลอจิกเป็นกลุ่มๆไป โดยที่เครื่องคอมพิวเตอร์จะติดต่อสื่อสารกันได้โดยตรงเฉพาะที่อยู่ในกลุ่มเดียวกัน และในแต่ละกลุ่มก็จะมีรหัสตัวเลขที่ใช้เรียกแทนชื่อกลุ่ม ซึ่งเรียกว่า Network Number Address โดยค่านี้เป็นค่าที่ผู้ดูแลระบบเครือข่ายสามารถกำหนดขึ้นเองได้ ดังนั้นถ้าเครื่องคอมพิวเตอร์ใดมีค่า Network Number Address เดียวกัน ก็จะสามารถติดต่อกันได้โดยตรง แต่ถ้า Network Number Address ต่างกัน จะไม่สามารถติดต่อกันได้เลยถึงแม้ว่าจะอยู่บนเซกเม็นท์ของสายสัญญาณเดียวกันก็ตาม จะต้องส่งผ่าน

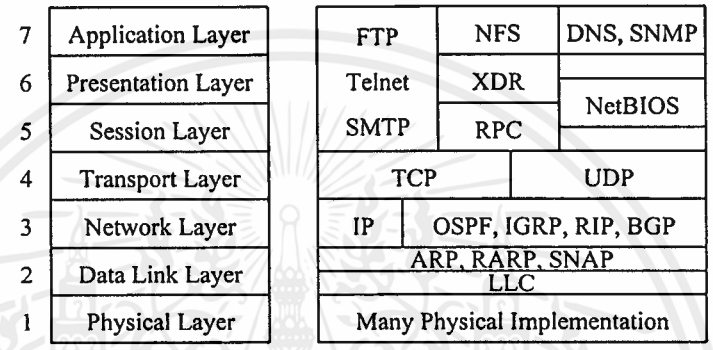
ข้อมูลที่จะติดต่อสื่อสารนั้นผ่านตัวเราเตอร์ก่อน จึงจะสามารถติดต่อสื่อสารกันได้ นั่นก็คือโดยเบื้องต้นแล้วเราเตอร์จะเชื่อมต่อ เครือข่ายต่างๆ กันเข้าด้วยกัน ในการทำงานของเราเตอร์โดยทั่วๆ ไปแล้ว จะมีโครงสร้างทำนองเดียวกับ Bridge คือเราเตอร์จะมีตารางระบุค่าเครือข่ายต่างๆ ที่เรียกว่า Routing Table ซึ่งมีลักษณะคล้ายกับตาราง MAC Address ของ Bridge โดยที่เราเตอร์จะใช้ค่าตารางนี้พิจารณาว่า เฟรมข้อมูลนี้จะส่งผ่านไปยังเซกเม็นท์ใดของระบบ การส่งผ่านเฟรมข้อมูลของเราเตอร์นั้น จะต่างกับ Bridge ตรงที่ Bridge จะทำการส่งเฟรมข้อมูลนั้นๆ ออกไปเลย โดยมีค่า MAC Address ของเครื่องคอมพิวเตอร์ทั้งต้นทางและปลายทางที่ไม่มีการเปลี่ยนแปลงใดๆ เปรียบเสมือนการติดต่อสื่อสารกันโดยตรง แต่สำหรับเราเตอร์แล้ว จะทำการแบ่งการติดต่อสื่อสารนั้นออกโดยจะทำการหลอกและเปลี่ยนแปลงค่า MAC Address ของเครื่องคอมพิวเตอร์ปลายทางและต้นทางเป็นของเราเตอร์นั้นๆ แทน ดังแสดงตามรูปที่ 2.14 ซึ่งวิธีนี้ สามารถควบคุมการติดต่อสื่อสารของระบบเครือข่ายได้ดีกว่า Bridge และสำหรับรายละเอียดของการติดต่อสื่อสารของระบบเครือข่ายผ่านเราเตอร์นั้น จะมีความแตกต่างกันตามชนิดของระบบคอมพิวเตอร์นั้นๆ เช่น UNIX, NetWare และ DecNet เป็นต้น



รูปที่ 2.14 แสดงความแตกต่างของการส่งเฟรมข้อมูลผ่าน Bridge และ Router

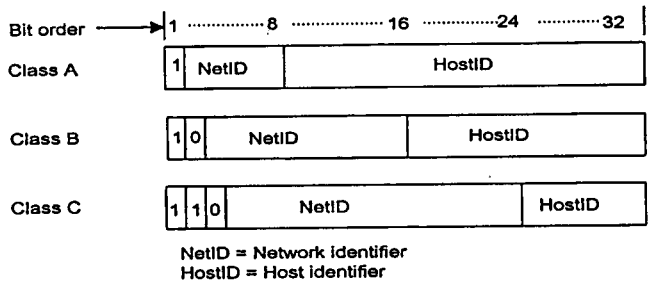
2.2.6.2 เราเตอร์กับระบบ UNIX System

คอมพิวเตอร์ที่ทำงานภายใต้ระบบ UNIX เป็นระบบที่ใช้มาตรฐานอินเตอร์เน็ตโปรโตคอล (IP-Internet Protocol) เป็นโครงสร้างในการติดต่อสื่อสารซึ่งมีการใช้งานอย่างแพร่หลายมากที่สุด โดยเฉพาะในส่วนของระบบเครือข่ายมหาวิทยาลัยหรือสถาบันการศึกษาต่างๆ ซึ่งมีระบบมาตรฐาน TCP/IP เป็นส่วนใหญ่ของระบบ นอกจากนั้นระบบเครือข่ายอินเตอร์เน็ตสากล ที่กำลังเป็นที่นิยมกันทั่วโลกในขณะนี้ ก็เป็นระบบมาตรฐานอินเตอร์เน็ตโปรโตคอลด้วย ดังนั้นจะเห็นได้ว่า ในปัจจุบันระบบมาตรฐาน TCP/IP เองก็มี มาตรฐานแยกย่อยมากมายกว่าระบบคอมพิวเตอร์อื่น



รูปที่ 2.15 แสดงการเปรียบเทียบ OSI 7-Layer กับ Protocol TCP/IP

สำหรับการพิจารณาการทำงานของเราเตอร์กับระบบมาตรฐาน TCP/IP ถ้าทำการแยกฟังก์ชันการทำงานต่างๆ ของระบบมาตรฐานอินเตอร์เน็ตโปรโตคอลเทียบกับมาตรฐานอ้างอิง OSI 7-Layer ดังแสดงตามรูปที่ 2.15 แล้วจะพบว่า มาตรฐานที่เกี่ยวข้องกับการทำงานของเราเตอร์นั้น มีด้วยกัน 3 กลุ่มคือ กลุ่มมาตรฐานระดับ Data Link Layer (ARP,RARP,ANAP) กลุ่มมาตรฐานระดับ Network Layer (IP, Routing Protocol) และ กลุ่มมาตรฐานระดับ Transport Layer (TCP, UDP) จากที่ได้กล่าวมาแล้วว่าฟังก์ชันในระดับ Network Layer นี้ จะมีโครงสร้างค่าที่อยู่ของเครื่อง ดังเช่นในระบบมาตรฐานอินเตอร์เน็ตโปรโตคอลนี้ ก็จะใช้ค่า IP Address ซึ่งประกอบด้วย 2 ส่วนคือ IP Network Address และ IP Host Address ค่า IP Address นี้เป็นค่าทางโลจิค สามารถกำหนดเองได้โดยผู้บริหารเครือข่าย จะสะดวกต่อการออกแบบและควบคุมระบบเครือข่ายเป็นอย่างมาก โครงสร้างของ IP Address จะประกอบด้วยตัวเลข 4 หน่วย โดยแต่ละหน่วยมีขนาด 8 บิท ดังแสดงตามรูปที่ 2.16 เนื่องจากระบบนี้เป็นระบบที่ใช้กันแพร่หลายและเป็นสากล ดังนั้นระบบค่าที่อยู่นี้จึงถูกกำหนดแบ่งเป็นระดับ (Class) และที่ใช้กันในปัจจุบันมีอยู่ด้วยกัน 3 ระดับคือ Class A, Class B และ Class C โดยความแตกต่างระหว่างระดับคือ จำนวนขนาดของค่า Host IP Address ที่จะรองรับได้ในหนึ่งค่าของ Network IP Address



รูปที่ 2.16 ระดับมาตรฐานของ IP Address

2.3 IP Address

การกำหนด IP Address ให้กับองค์กรต้องเป็นไปตามสัญญาการประมูล แต่ถ้าไม่ได้กำหนดไว้ ก็ให้เลือกออกแบบให้เหมาะสมกับจำนวน Hosts และจำนวน Network ในระบบ และถ้าต้องการ IP Address มาตรฐานในการเชื่อมต่อกับระบบอินเตอร์เน็ต ต้องขอ IP Address จากหน่วยงานที่ให้บริการทางด้านนี้ เช่น NECTEC หรือ KSCNet เป็นต้น

IP Address มีจำนวน 32 บิท แบ่งออกเป็น 4 ส่วน แต่ละส่วนจะมี 8 bit field หรือ octet ซึ่งถูกแสดงด้วยเลขฐานสิบระหว่าง 0-255 และแต่ละส่วนจะถูกแบ่งด้วยจุด เช่น 123.150.182.32 IP Address 32 บิท จะถูกแบ่งเป็น 2 subfield คือ เครือข่าย (netid = Network Identifier) และ host (hostid = Host Identifier) สามารถแบ่งเป็น Class ต่างๆ ได้ดังนี้ คือ [1-2]

Class A บิทแรกจะถูกกำหนดเป็น 0 ส่วน 7 บิทต่อมา จะเป็นเครือข่ายและ 24 บิทที่เหลือจะเป็น host ใน Class A สามารถมีเครือข่ายได้ 127 เครือข่าย และแต่ละเครือข่ายสามารถมีจำนวน host ได้ถึง 16,777,214 host

Class B บิทแรกจะถูกกำหนดเป็น 1 และบิทที่สองจะถูกกำหนดเป็น 0 ส่วน 14 บิทต่อมาจะเป็นเครือข่าย และ 16 บิทที่เหลือจะเป็น host ใน Class B สามารถมีเครือข่ายได้ 16,383 เครือข่าย และแต่ละเครือข่ายสามารถมีจำนวน host ได้ถึง 65,534 host

Class C สองบิทแรกจะถูกกำหนดเป็น 1 และบิทที่สามจะถูกกำหนดเป็น 0 ส่วน 21 บิทต่อมาจะเป็นเครือข่าย และ 8 บิทที่เหลือจะเป็น host ใน Class C สามารถมีจำนวนเครือข่ายได้ถึง 2,097,151 เครือข่าย และแต่ละเครือข่ายสามารถมีจำนวน host ได้ 254 host

Class D สามบิทแรกจะถูกกำหนดเป็น 1 และบิทที่สี่ จะถูกกำหนดเป็น 0 Class D นี้จะถูกกำหนดไว้ใช้สำหรับ Multicast Address ซึ่งการกำหนด IP Address ตาม Class ต่างๆ นั้น ได้แสดงไว้ตามรูปที่ 2.17

ในการที่จะทำความเข้าใจและอ่านค่า IP Address ได้ง่ายขึ้น จึงได้มีการเขียนเป็นเลขฐานสิบจำนวน 4 ส่วน แต่ละส่วนถูกแบ่งด้วยจุด (dot) ลักษณะแบบนี้เรียกว่า Dotted Decimal Notation ตัวอย่างเช่น

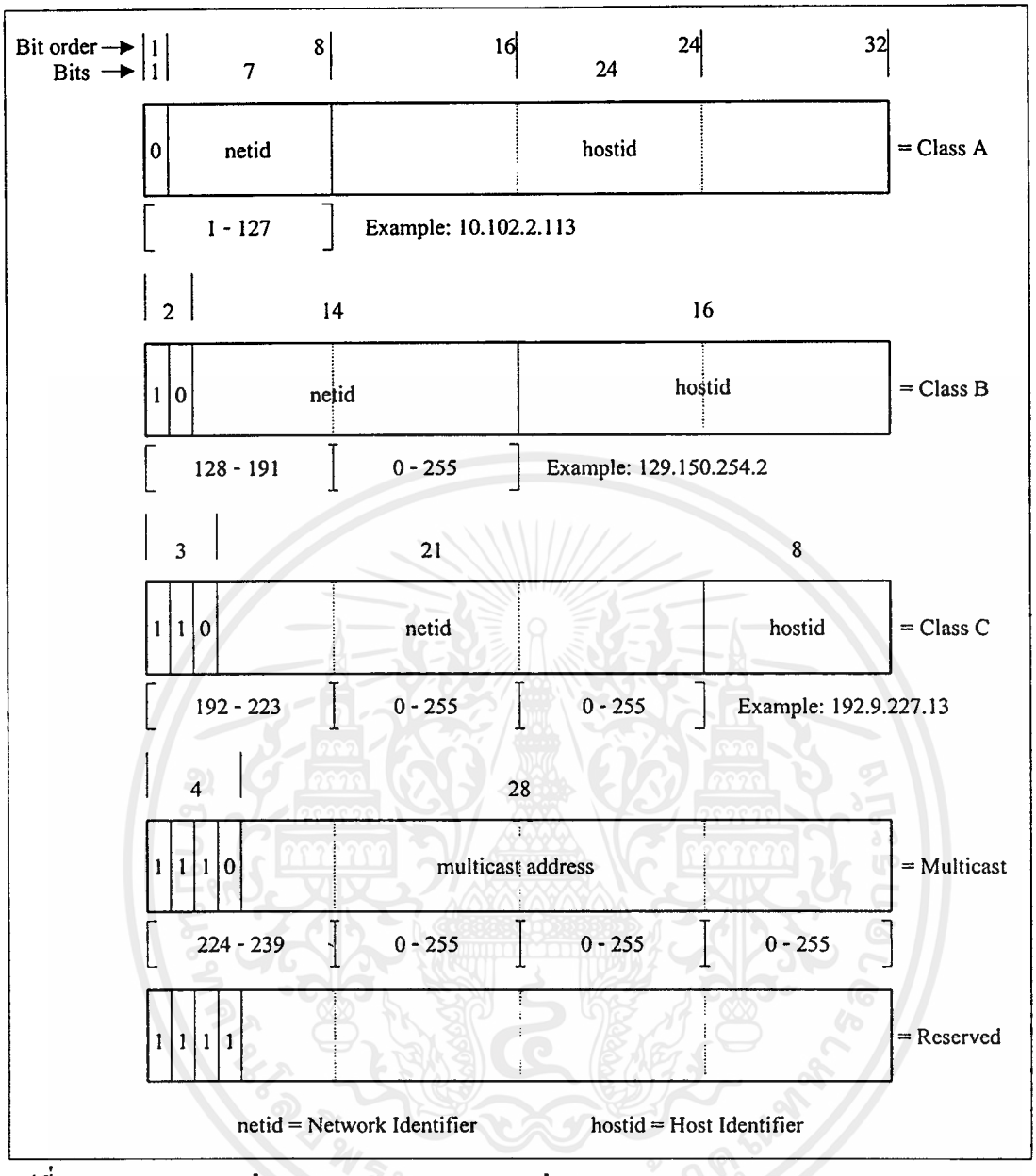
00001010 00000000 00000000 00000000	= 10.0.0.0 = Class A
	= netid 10
10000000 00000011 00000010 00000011	= 128.3.2.3 = Class B
	= netid 128.3 , hostid 2.3
11000000 00000001 00000010 00000011	= 192.1.2.3 = Class C
	= netid 192.1.2 , hostid 3

ข้อกำหนดในการกำหนด IP Address

1. ในระบบเครือข่าย Internet หมายเลข 127.0.0.0 (Class A) จะถูกสงวนไว้สำหรับการทดสอบระบบการสื่อสารบนตัวเอง เรียกว่า Loopback นอกจากนี้ยังสามารถกำหนด Loopback อื่นๆ ได้ โดยกำหนดให้มี netid = 127 ส่วน hostid จะกำหนดอย่างไรก็ได้

2. บิทที่ใช้ในการกำหนด host ของ IP Address จะต้องไม่เป็นบิท 1 ทั้งหมด เพราะจากมาตรฐานที่กำหนดไว้นั้น IP Address ที่มี host ประกอบด้วยบิท 1 ทั้งหมด จะหมายถึง host ทุกเครื่อง เช่น 129.12.255.255 จะหมายถึง host ทุกตัวที่อยู่บนเครือข่าย 129.12

3. บิทที่ใช้ในการกำหนดเครือข่ายของ IP Address จะต้องไม่เป็น 0 ทั้งหมด เพราะจากมาตรฐานที่กำหนดไว้นั้น host ที่ประกอบด้วยบิท 0 ทั้งหมด จะหมายถึงเฉพาะเครือข่ายนี้ เช่น 0.0.0.123 จะหมายถึง host 123 บนเครือข่ายนี้



รูปที่ 2.17 แสดงการแบ่ง IP Address ตาม Class ต่างๆ

บทที่ 3
อีเทอร์เน็ต

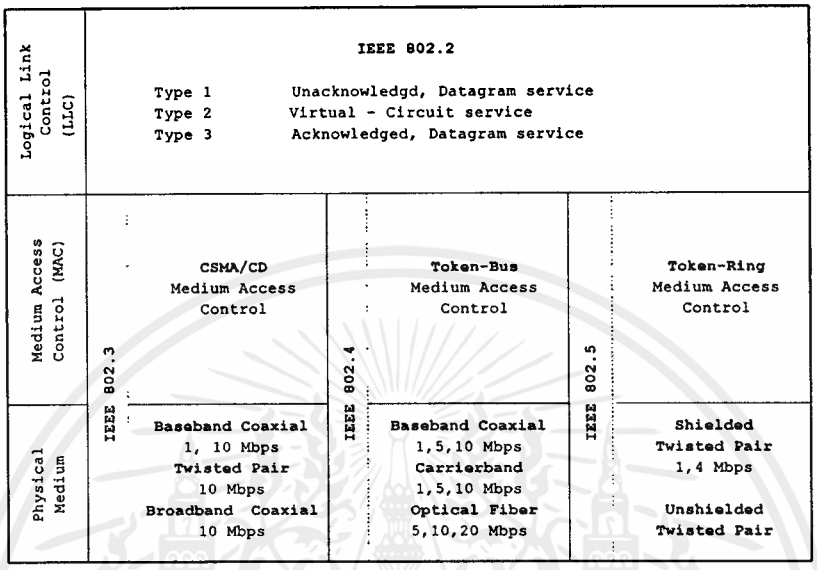
การสื่อสารแบบอีเทอร์เน็ตจะเป็นไปตามมาตรฐานของ IEEE 802.3 โดยจะใช้สายเชื่อมต่อสัญญาณหรือสายเคเบิลบนสถาปัตยกรรมหรือโทโปโลยีแบบบัส สามารถเชื่อมต่อเวิคสเตชันต่างๆ ได้จำนวนมาก จำนวนเวิคสเตชันที่นำมาเชื่อมต่อกันได้ ขึ้นอยู่กับชนิดของสายเคเบิลที่ใช้ สายเคเบิลที่ใช้ในระบบอีเทอร์เน็ตแบบบัส จะเป็นสายโคแอคเซียล (Coaxial) แบ่งออกเป็นอย่างบางและอย่างหนา อย่างบางเรียกว่าธินโคแอคเซียลหรือธินอีเทอร์เน็ต (Thin Ethernet) อย่างหนาเรียกว่า ธิคโคแอคเซียล หรือธิคอีเทอร์เน็ต (Thick Ethernet) ข้อดีของธิคอีเทอร์เน็ตคือสามารถส่งสัญญาณได้ไกลกว่าธินอีเทอร์เน็ต และยังสามารถป้องกันสัญญาณรบกวนได้ดีกว่ามาก [2-3]

ตารางที่ 3.1 เป็นการแสดงมาตรฐานของ IEEE 802 ที่กำหนดคุณลักษณะเกี่ยวกับการเชื่อมต่อของอุปกรณ์คอมพิวเตอร์รวมกันเป็นเครือข่ายทั้งส่วนที่เป็นในระดับกายภาพจนถึงข้อกำหนดเกี่ยวกับโปรโตคอลที่ใช้ในการโต้ตอบระหว่างอุปกรณ์เครือข่าย

ตารางที่ 3.1 แสดงมาตรฐาน IEEE 802 ของเครือข่ายคอมพิวเตอร์

IEEE Standard	**มาตรฐานของเครือข่าย**
IEEE 802.1	LAN Bridging
IEEE 802.2	Logical Link Control (LLC)
IEEE 802.3	Standardization of Ethernet Technology. Include 100BASE-TX, 100 BASE-TF, and 100BASE-T4 (Fast Ethernet)
IEEE 802.4	Token Bus standard
IEEE 802.5	Token Ring standard
IEEE 802.6	Metropolitan Area Network (MAN)
IEEE 802.7	Broadband technical advisory
IEEE 802.8	Fiber-optic technical advisory
IEEE 802.9	Integrated Voice/Data (IVD)
IEEE 802.10	LAN security
IEEE 802.11	Wireless LANs
IEEE 802.12	100BASE-VG (100VG-AnyLAN)

สำหรับสถาปัตยกรรมระดับชั้นของ IEEE 802 ที่กำหนดคุณลักษณะของระดับการให้บริการและคุณลักษณะทางด้านกายภาพ ในการเชื่อมโยงของอุปกรณ์สื่อสารข้อมูลที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ แสดงดังรูปที่ 3.1

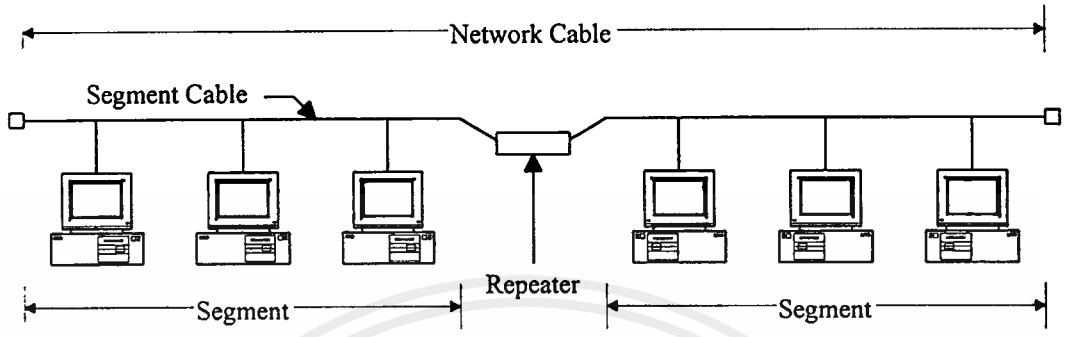


รูปที่.3.1 มาตรฐานของการให้บริการที่เป็นไปตามมาตรฐาน IEEE 802

3.1 มาตรฐานของเครือข่ายอีเทอร์เน็ต

ในระบบเครือข่าย ได้แก่เครือข่ายที่เป็นวงเดียวกัน สามารถใช้ได้ทั้งสายแบบบางและแบบหนาผสมกันไป โดยที่จะต้องคำนึงสถานที่หรือสภาวะสิ่งแวดล้อม อีกทั้งราคาค่าสายเป็นส่วนประกอบอีกด้วย ในสถานที่เช่นสำนักงานทั่วไป ที่มีระยะทางการเชื่อมต่อของสถานีไม่เกินข้อกำหนดของสาย เช่น ไม่เกิน 185 เมตรนั้น เลือกใช้สายแบบบางจะเหมาะกว่า แต่ถ้าเป็นระยะทางที่มากกว่านั้น แต่ไม่เกิน 500 เมตร การใช้สายแบบหนาดูเหมือนว่าจะคุ้มค่ากว่า การใช้สายแบบบางร่วมกับรีพีทเตอร์ที่มีราคาแพง นอกจากนี้ประโยชน์ของสายแบบหนาคือ สามารถต่อเชื่อมกับสายแบบบางในกรณีที่ เส้นทางเดินของสายเคเบิลจะต้องผ่านสถานีที่มีสัญญาณรบกวนมาก ๆ หรือเดินสายผ่านออกนอกอาคาร ด้วยเหตุผลที่ว่าสายแบบหนามีความสามารถในการป้องกันการรบกวนได้ดี สายเคเบิลเส้นหนึ่งเรียกว่า 1 เซกเม็นท์ ใน 1 เซกเม็นท์สามารถมีความยาวไม่เกินข้อกำหนดตามชนิดของสาย จำนวนของเวิคสเตชันที่เชื่อมต่อใน 1 เซกเม็นท์ขึ้นอยู่กับข้อกำหนดของชนิดของสายเช่นกัน ถ้าเกินข้อกำหนดแล้วจะต้องต่อรีพีทเตอร์ด้วยทุกครั้ง ระบบแลนหนึ่งวงสามารถต่อเซกเม็นท์ได้อย่างมีขีดจำกัด เช่น สายแบบบางสามารถมีเซกเม็นท์ได้ไม่เกิน 5 เซกเม็นท์นั่นคือความยาวสูงสุดที่สามารถทำได้คือ 185x5 เท่ากับ 925 เมตรหรือ 3035 ฟิต จำนวนของรีพีทเตอร์ที่จะต้องใช้คือ 4 ชุดส่วนสายแบบหนา สามารถต่อเซกเม็นท์ได้ไม่เกิน 5 เซกเม็นท์เช่นกัน แต่ละเซกเม็นท์มี

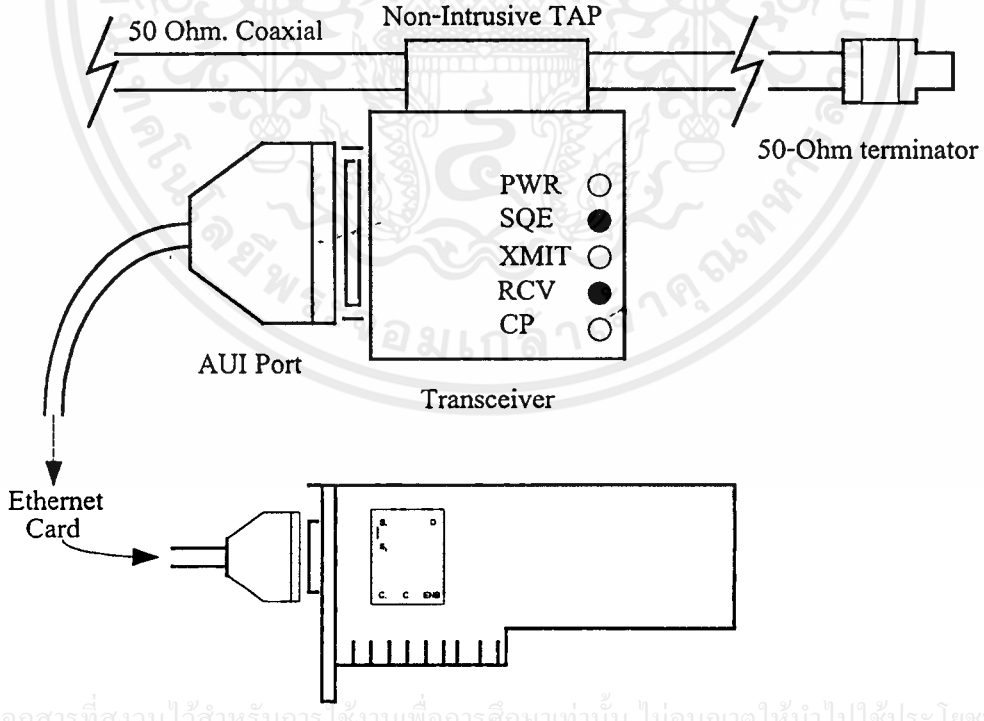
ความยาวไม่เกิน 500 เมตร ดังนั้นความยาวรวมทั้งหมดจะได้เท่ากับ 2500 เมตรหรือ 8200 ฟีต จำนวนของรีพีทเตอร์ที่ใช้คือ 4 ชุด



รูปที่ 3.2 แสดงการเชื่อมต่อระหว่างเซกเม็นท์

3.1.1 ระบบเครือข่ายธิคอีเทอร์เน็ต

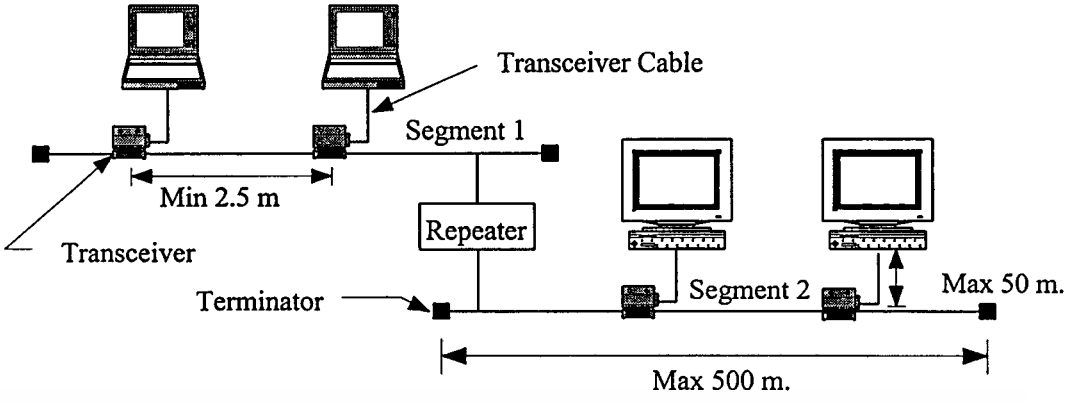
ระบบเครือข่ายแบบธิคอีเทอร์เน็ต หรือ 10Base5 จะมีรูปแบบและส่วนประกอบต่างๆ ที่เกี่ยวข้องตามรูปที่ 3.3



รูปที่ 3.3 แสดงส่วนประกอบของธิคอีเทอร์เน็ต

อุปกรณ์ที่สำคัญของการเชื่อมต่อแบบธิคอีเทอร์เน็ต คือ

1. การ์ดเชื่อมโยงระบบเครือข่าย (NIC – Network Interface Card) เป็นส่วนที่ติดตั้งบนเครื่องเวิคสเตชันทำหน้าที่รับและส่งข้อมูลจากซีพียูไปยังเวิคสเตชันต่างๆ หรือเป็นตัวกลางเชื่อมระหว่างเวิคสเตชันกับเครือข่าย
2. ทรานซีฟเวอร์ เป็นอุปกรณ์ที่ทำหน้าที่ในการรับส่งผ่านสัญญาณ โดยการต่อเข้ากับสายโคแอคเซียลแบบหนา ซึ่งอุปกรณ์ชนิดนี้จะมีลักษณะเป็นบล็อคมีคอนเนคเตอร์ 2 ข้าง ข้างหนึ่งจะเป็นขั้วสำหรับต่อเข้ากับสายโคแอคเซียล และอีกข้างจะเป็นพอร์ทที่เรียกกันว่าเอยูไอ พอร์ท เพื่อเชื่อมเข้ากับการ์ดเชื่อมโยงเครือข่ายที่อยู่บนเวิคสเตชัน และบนบล็อคของทรานซีฟเวอร์ ก็จะมีสัญญาณไฟแอลอีดีแสดงสถานะการทำงาน จะสังเกตุได้ว่า การเชื่อมต่อในลักษณะนี้ จะมีอุปกรณ์ทรานซีฟเวอร์อยู่ภายนอกวงจร ทั้งนี้เนื่องจากว่า บนการ์ดเชื่อมโยงระบบเครือข่าย ไม่มีชุดของวงจรรับส่งอยู่บนการ์ดนั่นเอง
3. สายสัญญาณชนิดเอยูไอ เป็นสายสัญญาณที่ใช้เชื่อมต่อระหว่างอุปกรณ์ทรานซีฟเวอร์กับการ์ดเชื่อมโยงเครือข่าย ซึ่งกำหนดให้มีความยาวไม่เกิน 50 เมตร
4. สไลด์ล็อค เป็นตัวยึดกับสายเคเบิลที่เชื่อมต่อกับการ์ดเชื่อมโยงเครือข่าย ปกติจะติดมากับการ์ดเชื่อมโยงเครือข่าย ช่วยยึดสายที่เชื่อมต่อให้แน่น
5. สายสัญญาณธิคอีเทอร์เน็ตคือสายโคแอคเซียลแบบหนาเบอร์ RG8A/U มีขนาดเส้นผ่านศูนย์กลาง 0.4 นิ้ว มีค่าความต้านทาน 50 โอห์ม มีปลายทั้งสองด้านของสายต่อด้วย N-SERIES แบบตัวผู้
6. เทอมิเนเตอร์ ที่มีค่าความต้านทาน 50 โอห์ม ใช้เชื่อมต่อที่ปลายสายของธิคโคแอคเซียลเคเบิล ทำหน้าที่จำลองค่าความยาวของสายสัญญาณเป็น infinity ทั้งนี้เพื่อป้องกันไม่ให้สัญญาณที่วิ่งอยู่บนสายสัญญาณ เกิดการสะท้อนกลับที่ปลายสาย



รูปที่ 3.4 แสดงการเชื่อมต่อเครือข่ายธิคอีเทอร์เน็ต

3.1.1.1 ข้อจำกัดของธิคอีเทอร์เน็ต

1. จำนวนของเซกเม็นท์มีได้ 5 เซกเม็นท์
2. ความยาวสูงสุดต่อ 1 เซกเม็นท์คือ 500 เมตร
3. ความยาวรวมทั้งหมดของทุกเซกเม็นท์ เท่ากับ 2500 เมตร
4. ระยะห่างน้อยที่สุดระหว่างเวิคสเตชันเท่ากับ 2.5 เมตร
5. จำนวนของเวิคสเตชันที่สามารถเชื่อมต่อได้ใน 1 เซกเม็นท์เท่ากับ 100 เวิคสเตชัน
6. จำนวนของเวิคสตเช้นสูงสุดที่เชื่อมต่อได้เท่ากับ 1024 เวิคสเตชัน
7. จำนวนของรีพีทเตอร์สูงสุดที่ใช้ได้คือ 2 ชุด (ต่อแบบ without IRLs:Inter Repeater Link-segment)
8. จำนวนรวมของรีพีทเตอร์สูงสุดที่ใช้ได้คือ 4 ชุด (ต่อแบบ with IRLs)
9. ขนาดความยาวสูงสุดระหว่างเวิคสเตชันไปยังทรานซีฟเวอร์ไม่เกิน 50 เมตร
10. อัตราการรับส่งข้อมูลสูงสุด 10 Mbps

3.1.1.2 กฎการติดตั้งของธิคอีเทอร์เน็ต

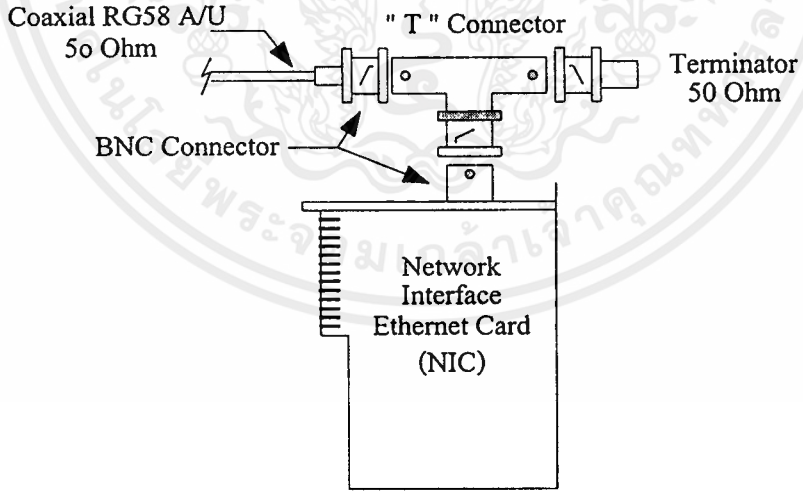
1. ต้องติดตั้งเทอมิเนเตอร์ ที่ปลายทั้งสองด้านในส่วนที่ไม่ได้เชื่อมต่อกับเวิคสเตชันใดเสมอ และจะต้องมีด้านใดด้านหนึ่งของเทอมิเนเตอร์ที่ต่อลงกราวด์
2. จำนวนของข้อต่อสายเคเบิล จะต้องมีจำนวนน้อยที่สุดเท่าที่จะทำได้ ทั้งนี้เพื่อความเชื่อถือได้ในการทำงานของระบบ พยายามใช้สายยาวที่สุดเท่าที่จะทำได้ โดยไม่เกินข้อกำหนดของสายนั้นๆ

3.1.2 ระบบเครือข่ายธินอีเทอร์เน็ต

ระบบเครือข่ายแบบธินอีเทอร์เน็ต หรือ 10Base2 จะมีรูปแบบและส่วนประกอบต่างๆ ที่เกี่ยวข้องตามรูปที่ 3.5

อุปกรณ์ที่สำคัญของการเชื่อมต่อแบบธินอีเทอร์เน็ต คือ

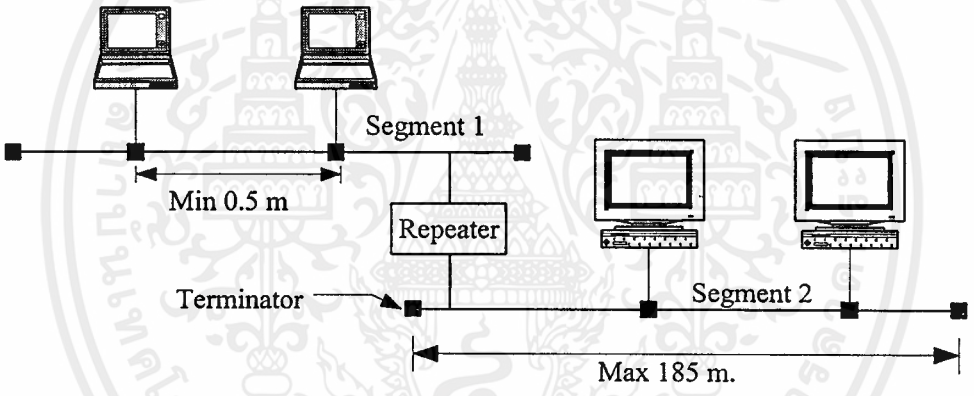
1. การ์ดเชื่อมโยงระบบเครือข่าย เป็นส่วนที่ติดตั้งบนเครื่องเวิคสเตชันทำหน้าที่รับและส่งข้อมูลจากซีพียูไปยังเวิคสเตชันต่างๆ หรือเป็นตัวกลางเชื่อมระหว่างเวิคสเตชันกับเครือข่าย
2. BNC Connector เป็นข้อต่อที่ใช้เชื่อมต่อกันระหว่างอุปกรณ์ของแลนต่างๆ เช่น BNC Connector Jack เป็นคอนเนคเตอร์ที่ออกมาจากการ์ดเชื่อมโยงระบบเครือข่าย จะต้องเชื่อต่อกับ BNC T-Connector และปลายด้านหนึ่งของ BNC T-Connector นั้นจะต้องเชื่อมต่อกับสายโคแอคเซียลที่มีด้านหนึ่งเป็นหัว BNC Connector Plug ปลายด้านหนึ่งของ BNC T-Connector จะต้องเชื่อมต่อกับสายโคแอคเซียลและโยงไปถึงเวิคสเตชันหนึ่ง แต่ถ้าหากไม่ต่อเชื่อมกับเวิคสเตชันใดแล้วจะต้องปิดด้วย Ground BNC Terminator ขนาด 50 โอห์ม
3. สายธินโคแอคเซียล คือสายส่งหรือนำสัญญาณมีขนาดเส้นผ่าศูนย์กลาง 0.2 นิ้ว แบบ RG58A/U ขนาด 50 โอห์ม ปลายของสายทั้งสองด้านจะเป็น BNC Connector Plug



รูปที่ 3.5 แสดงส่วนประกอบของธินอีเทอร์เน็ต

3.1.2.1 ข้อจำกัดของธินอีเทอร์เน็ต

1. จำนวนของเซกเม็นท์มีได้ 5 เซกเม็นท์
2. ความยาวสูงสุดต่อ 1 เซกเม็นท์คือ 185 เมตร
3. ความยาวรวมทั้งหมด 5 เซกเม็นท์เท่ากับ 925 เมตร
4. ระยะห่างน้อยที่สุดระหว่างเวิคสเตชันเท่ากับ 0.5 เมตร
5. จำนวนของเวิคสเตชันที่สามารถเชื่อมต่อได้ใน 1 เซกเม็นท์เท่ากับ 30 เวิคสเตชัน
6. จำนวนของเวิคสเตชันสูงสุดที่เชื่อมต่อได้เท่ากับ 1024 เวิคสเตชัน
7. จำนวนรวมของรีพีทเตอร์สูงสุดที่ใช้ได้คือ 2 ชุด (ต่อแบบ without IRLs)
8. จำนวนรวมของรีพีทเตอร์สูงสุดที่ใช้ได้คือ 4 ชุด (ต่อแบบ with IRLs)
9. อัตราการรับส่งข้อมูลสูงสุด 10 Mbps



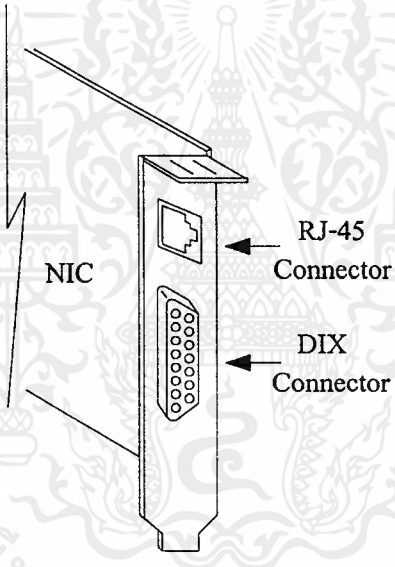
รูปที่ 3.6 แสดงการเชื่อมต่อเครือข่ายธินอีเทอร์เน็ต

3.1.2.2 กฎการติดตั้งของธินอีเทอร์เน็ต

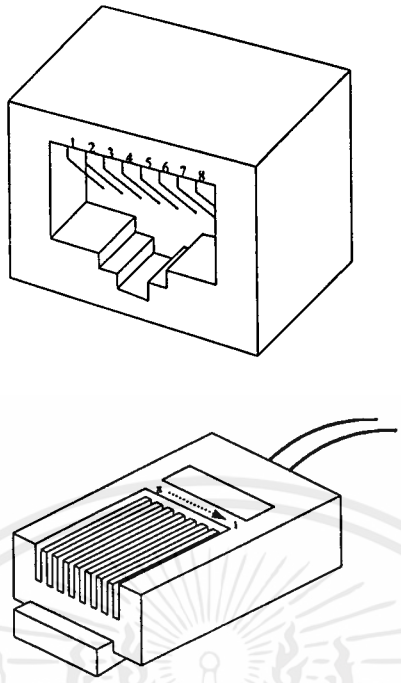
1. จะต้องติดตั้ง BNC Terminator ที่ปลายทั้งสองด้านของเครือข่ายหรือเวิคสเตชันส่วนที่ไม่เชื่อมต่อกับเวิคสเตชันใด และจะต้องมีด้านใดด้านหนึ่งต่อลงกราวด์เสมอ
2. พยายามใช้ความยาวของสายสัญญาณให้มากที่สุดต่อ 1 เซกเม็นท์ โดยลดจำนวนข้อต่อให้น้อยที่สุด ถ้าจำนวนของข้อต่อและความยาวสายน้อยเท่าใด หมายถึงความเชื่อถือได้ของระบบเครือข่ายมีมากเท่านั้น

3.1.3 ระบบเครือข่ายมาตรฐาน 10BaseT

โครงข่ายมาตรฐานที่เรียกกันว่า 10BaseT เป็นโครงข่ายที่นิยมใช้กันมากในปัจจุบัน ทั้งนี้เนื่องจากว่า มีความสะดวกและง่ายในการดูแลบำรุงรักษา และมีลักษณะการเชื่อมต่อเป็นแบบสตาร์ โดยเฉพาะอย่างความมีเสถียรภาพของเครือข่าย กล่าวคือจะไม่มีผลกระทบกับอุปกรณ์คอมพิวเตอร์ที่เชื่อมต่ออยู่เป็นส่วนใหญ่เมื่อมีอุปกรณ์คอมพิวเตอร์ตัวใดตัวหนึ่งเกิดปัญหาขึ้นมา เพราะว่าอุปกรณ์ที่มีหน้าที่เป็น Switching ในการกระจายสัญญาณให้กับเวิคสเตชันด้วยพอร์ทต่างๆ จะมีวงจรการรับส่งผ่านสัญญาณที่เป็นอิสระต่อกัน จากรูปที่ 3.7 แสดงการ์ดเชื่อมโยงระบบเครือข่ายที่มีพอร์ท ที่เรียกกันว่าพอร์ท RJ-45 ซึ่งเป็นพอร์ทที่ใช้ในการเชื่อมต่อสายสัญญาณแบบ 10BaseT คือใช้สายประเภท UTP ต่อเชื่อมเข้ากับ plug RG-45 ตัวผู้ แล้วก็ทำการ plug เข้ากับการ์ดเชื่อมโยงระบบเครือข่ายที่มีพอร์ท RJ-45 connector ดังรูปที่ 3.8



รูปที่ 3.7 แสดงพอร์ทของการ์ดเชื่อมโยงระบบเครือข่ายแบบ 10BaseT

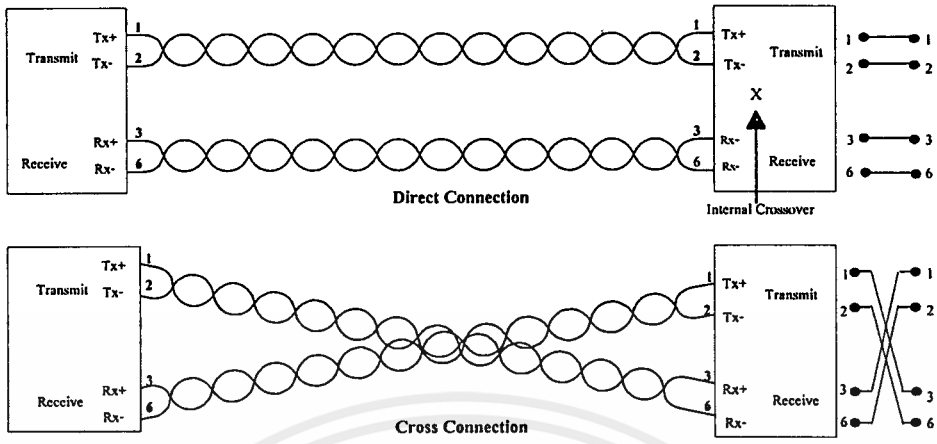


รูปที่ 3.8 แสดงลักษณะของ 10BaseT plug RJ-45 Connector

ข้อกำหนดที่เกี่ยวกับสัญญาณและ code สีของสายสัญญาณ UTP สามารถแสดงได้ดังตารางที่ 3.2 ซึ่งมีอยู่ 2 มาตรฐาน คือ มาตรฐาน AT&T T568B และ มาตรฐาน TIA นอกจากนั้นยังมีข้อจำกัดอื่นๆ กล่าวคือ สามารถรองรับความยาวของสายสัญญาณได้สูงสุดเท่ากับ 100 เมตร , รองรับความเร็วในการส่งผ่านสัญญาณได้ตั้งแต่ 10 - 100 Mbps ทั้งนี้ขึ้นอยู่กับชนิดของสาย UTP ที่ใช้และความสามารถของอุปกรณ์ switching

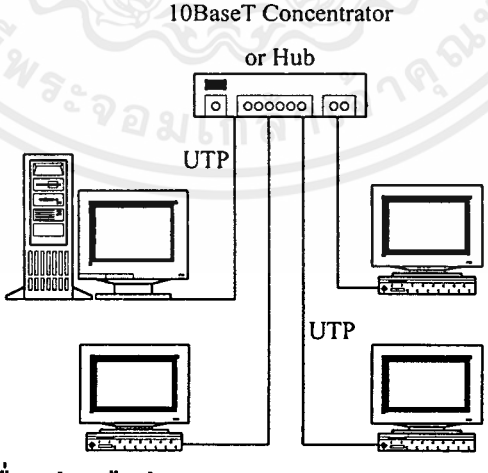
ตารางที่ 3.2 แสดงตำแหน่งขาสัญญาณของ 10BaseT

Contact	**MDI signal**	**Wire Color Code In AT&T T568B**	**Wire Color Code In TIA 2840 for T568B-UTP**
1	TD+	White with Orange band	White-Green
2	TD-	Orange with White band	Green
3	RD+	White with Green band	White-Orange
4	Not used by 10BASE-T	Blue with White band	Blue
5	Not used by 10BASE-T	White with Blue band	White-blue
6	RD-	Green with White band	Orange
7	Not used by 10BASE-T	White with Brown band	White-Brown
8	Not used by 10BASE-T	Brown with White band	Brown



รูปที่ 3.9 แสดงลักษณะการต่อสายของ 10BaseT

ลักษณะในการเชื่อมต่อทางด้านกายภาพนั้น จะใช้สายสัญญาณ UTP เชื่อมหัวท้ายด้วย Connector RJ-45 ซึ่งมีขาจำนวน 8 ขา แต่จะใช้เพียง 4 ขาสัญญาณคือขา 1 และ 2 (Tx+,Tx-) กับขา 3 และ 6 (Rx+,Rx-) ตามมาตรฐาน 10BaseT จากรูปที่ 3.9 แสดงการเชื่อมต่อสายสัญญาณ ซึ่งสามารถต่อเชื่อมได้ 2 แบบ กล่าวคือ แบบต่อตรงและแบบต่อไขว้กัน (cross) ทั้งนี้ขึ้นอยู่กับวงจรภายในของ switching หรือ Hub ว่า มี switch สำหรับการสลับวงจรรับและส่งในลักษณะที่สอดคล้องกันหรือไม่ และสำหรับรูปที่ 3.10 จะเป็นการแสดงลักษณะการเชื่อมต่อโครงข่ายแบบสตาร์ซึ่งมีอุปกรณ์ switching ที่เรียกว่า Hub เป็นจุดศูนย์กลางในการเชื่อมต่อกับอุปกรณ์คอมพิวเตอร์เข้าด้วยกัน



รูปที่ 3.10 แสดงลักษณะการเชื่อมต่อเครือข่ายแบบ 10BaseT

3.2 หลักการทำงานของอีเทอร์เน็ต

อีเทอร์เน็ตโดยทั่วไปแล้วจะมีลักษณะการใช้งานเป็นการจัดการช่วงการสื่อสารร่วมกันโดยกระจายการควบคุม ซึ่งเรียกว่า CSMA/CD (Carrier Sense Multiple Access with Collision Detection) โดยวิธีนี้จะไม่มีส่วนจัดการควบคุมส่วนกลางไปยังช่องสัญญาณต่างๆ และจะไม่มีการแบ่งช่องสัญญาณของ Time Slot หรือ Frequency Bands เมื่อเวิคสเตชันต้องการที่จะส่งข้อมูล เวิคสเตชันนั้น จะร้องขอสิทธิในการส่งข้อมูลไปยังส่วนที่ทำหน้าที่กระจายการสื่อสาร เมื่อได้รับสิทธิจากช่องการสื่อสารแล้ว เวิคสเตชันก็สามารถที่จะส่งแพกเก็ตข้อมูลออกไปได้

ในการที่จะได้ช่องการสื่อสารนั้น เวิคสเตชันจะคอยตรวจสอบในเมื่อเครือข่ายยังไม่ว่าง คือมีการรับส่งข้อมูลอยู่ และเวิคสเตชันจะรอคอยการส่ง จนกระทั่งช่องการสื่อสารนั้นว่าง คือไม่มีการสื่อสารเกิดขึ้น เมื่อเวิคสเตชันสามารถที่ตรวจจับได้ว่าช่องสัญญาณนั้นว่าง เวิคสเตชันนั้นก็จะเริ่มทำการส่งข้อมูลได้ และในขณะที่กำลังส่งข้อมูลอยู่นั้น ก็จะต้องคอยตรวจสอบว่ามีสัญญาณการชนกันของข้อมูลหรือไม่ สัญญาณการชนกันที่เกิดขึ้นนั้น จะเกิดขึ้นในช่วงเวลาสั้นๆ ในการเริ่มส่งข้อมูลเท่านั้น ถ้าไม่มีสัญญาณการชนกันเกิดขึ้น ผู้ส่งก็สามารถได้รับช่องสัญญาณและสามารถส่งแพกเก็ตออกไปได้ ถ้าในกรณีที่เวิคสเตชันตรวจพบการชนกันของข้อมูลเกิดขึ้น การส่งข้อมูลก็จะถูกสั่งให้หยุดทำการส่งแพกเก็ตข้อมูลโดยทันที เพื่อที่จะให้เวิคสเตชันต่างๆ ที่เกี่ยวข้องรับรู้การเกิดการชนกันของข้อมูลขึ้น ซึ่งก็จะรู้ทันทีว่าเกิดการติดขัดของช่องสัญญาณขึ้น ตัวของเวิคสเตชันก็จะรับรู้ถึงการเกิดการชนกันของข้อมูลขึ้น คือจะต้องทำการส่งกลับไปใหม่ โดยช่วงเวลาของการส่งกลับไปใหม่นั้น จะใช้เป็นช่วงเวลาของการสุ่ม

3.3 รูปแบบโครงสร้างการเชื่อมต่อของเครือข่าย

มาตรฐานของเครือข่ายเฉพาะบริเวณหรือแลน จะมีข้อกำหนดเกี่ยวกับรูปแบบ ลักษณะในการเชื่อมต่อ โดยอาศัยสายสัญญาณ ซึ่งข้อกำหนดเหล่านี้ก็คือกฎเกณฑ์ที่ระบุเกี่ยวกับวิธีการเชื่อมต่อของมีเดียแบบต่างๆ รวมไปถึงทั้งฮาร์ดแวร์และส่วนประกอบรอบข้างที่เกี่ยวข้อง ซึ่งมีข้อกำหนดพื้นฐานจำนวน 2 ชนิดที่เกี่ยวข้องกัน ก็คือ ชนิดของมีเดีย (สายเคเบิล) และ รูปแบบของการเชื่อมต่อ

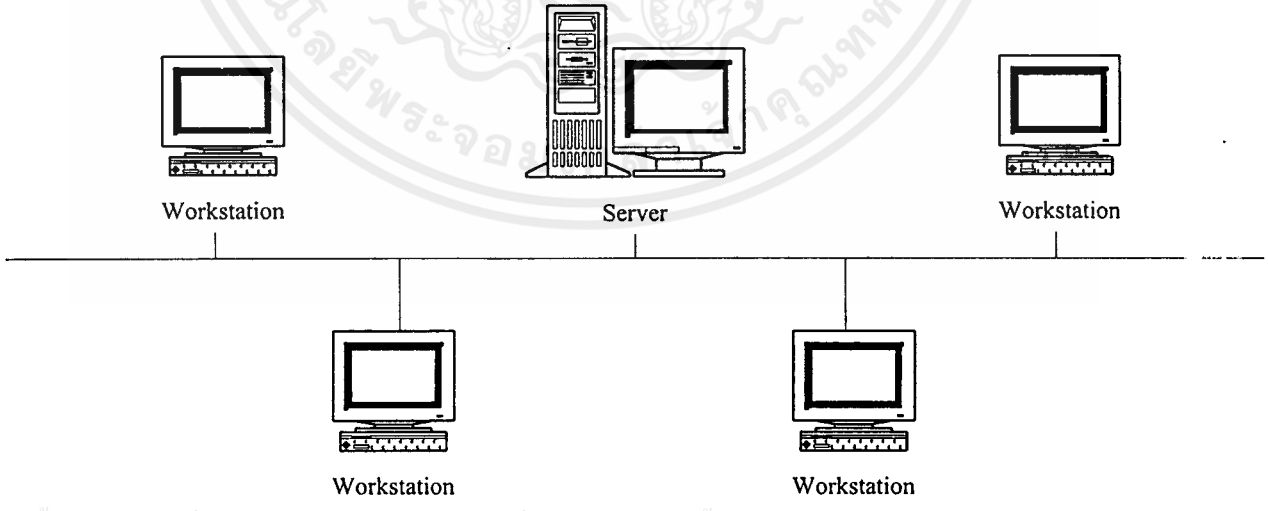
วิธีการเชื่อมต่อเป็นเครือข่ายสื่อสารในรูปแบบต่างๆ เรียกว่าโทโปโลยี ซึ่งโทโปโลยี ต่างๆ ที่นิยมใช้เชื่อมต่อกันได้แก่ เครือข่ายลักษณะแบบบัส, แบบริง และแบบสตาร์ ซึ่งแต่ละแบบมีลักษณะการเชื่อมต่อดังนี้

3.3.1 โทโปโลยีแบบบัส

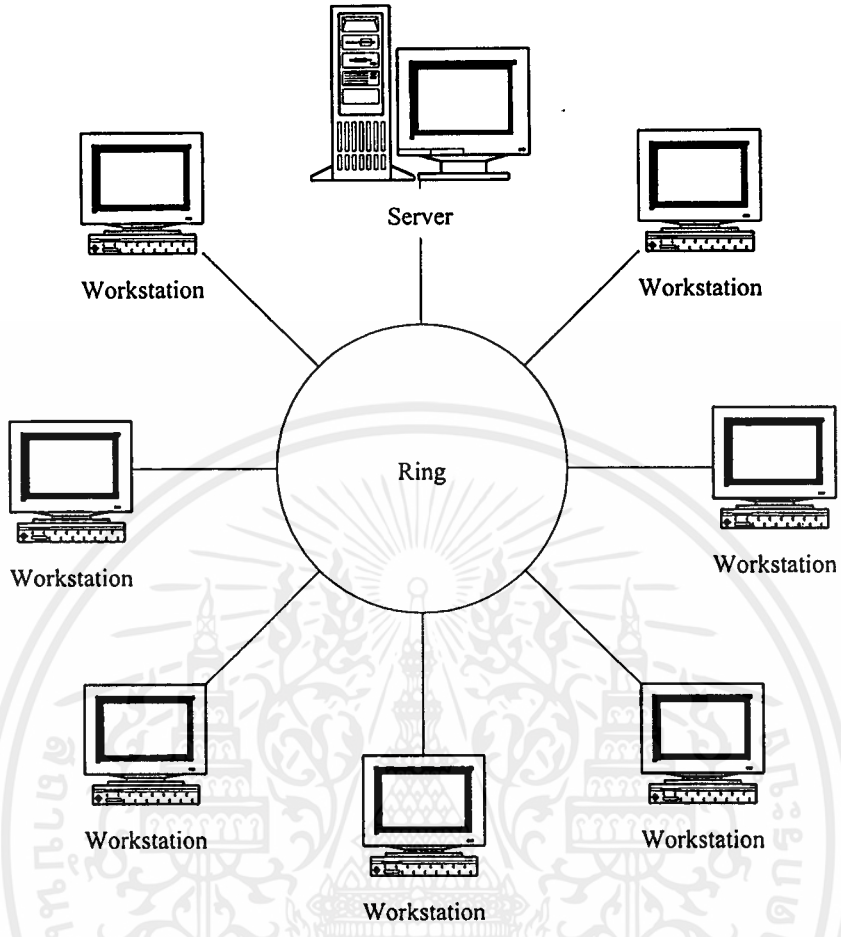
เป็นระบบแลนที่ใช้สายเคเบิลเชื่อมต่อกันระหว่างเซิฟเวอร์กับเวิคสเตชันต่างๆ เพียงตัวเดียวหรือหลายๆ ตัว ระบบที่ใช้แบบบัสได้แก่ระบบอีเทอร์เน็ต การส่งข้อมูลจากจุดหนึ่งไปยังอีกจุดหนึ่งหรือจากเวิคสเตชันไปยังเซิฟเวอร์ หรือทั้งไปและกลับโดยใช้สายเคเบิลเพียงเส้นเดียวไปยังผู้รับปลายทาง ซึ่งข้อมูลหรือสัญญาณนี้จะต้องผ่านเวิคสเตชันอื่นๆ ทุกเวิคสเตชัน แต่จะมีเพียงเวิคสเตชันเดียวที่สามารถรับข้อมูลนี้ได้ เนื่องจากการส่งข้อมูล ได้มีการกำหนดแอดเดรสที่แน่นอนของผู้รับ ระบบบัสนี้มีข้อดีคือโครงสร้างการส่งข้อมูลเป็นแบบง่ายๆ เพราะใช้สายส่งข้อมูลเพียงเส้นเดียว สะดวกต่อการเดินสายและติดตั้งสามารถเพิ่มเซิฟเวอร์และเวิคสเตชันได้ง่าย ข้อเสียคือหากสายเคเบิลเกิดชำรุดขึ้นมาที่จุดใดจุดหนึ่ง ไม่ว่าจะเป็นปัญหาจากข้อต่อสาย หรือที่สายเคเบิลเอง จะทำให้ระบบแลนทั้งระบบไม่ทำงานทันที

3.3.2 โทโปโลยีแบบริง

เป็นระบบที่มีการเชื่อมต่อแบบวงแหวน กล่าวคือต้นทางและปลายทางจะต้องเชื่อมต่อกันดังรูปที่ 3.12 การส่งสัญญาณในระบบริงนี้ สัญญาณจะเดินทางไปรอบๆ ริง โดยมีแอดเดรสกำกับว่าผู้รับคือใคร แม้ว่าสัญญาณจะผ่านไปที่ทุกเวิคสเตชัน แต่ก็จะมีเพียงเวิคสเตชันเดียวเท่านั้นที่สามารถรับข้อมูลได้ ระบบริงมีข้อดีคือเหมาะกับการที่จะนำไปใช้แบบ Fiber Optic เพราะการส่งข้อมูลแบบ Fiber Optic สามารถส่งได้ด้วยความเร็วสูงและมีทิศทางการส่งไปในทางเดียวกัน ข้อเสียคือ หากเวิคสเตชันใดเวิคสเตชันหนึ่งไม่ทำงาน ทั้งระบบจะไม่ทำงานด้วย



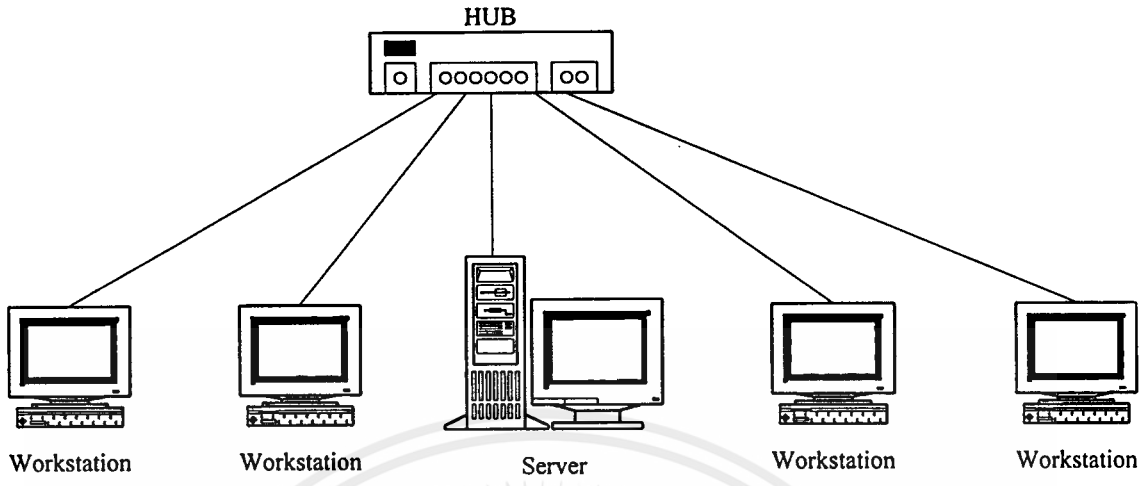
รูปที่ 3.11 แสดงการเชื่อมต่อโทโปโลยีแบบบัส



รูปที่ 3.12 แสดงการเชื่อมต่อโทโปโลยีแบบริง

3.3.3 โทโปโลยีแบบสตาร์

เป็นระบบแลนที่มีการเชื่อมต่อแบบกระจายออกมาจากจุดศูนย์กลาง โดยมีศูนย์ควบคุมที่ทำหน้าที่เป็นตัวควบคุมการรับส่งสัญญาณของเวิคสเตชันต่างๆ ศูนย์ควบคุมนี้เรียกว่า Hub ระบบสตาร์มีข้อดีคือ ง่ายต่อการดูแลตรวจสอบเมื่อมีข้อขัดข้องเกิดขึ้น ข้อเสียคือ ถ้า Hub เสียจะทำให้ทั้งระบบหยุดการทำงาน



รูปที่ 3.13 แสดงการเชื่อมต่อโทโปโลยีแบบสตาร์

3.4 ส่วนประกอบของอีเทอร์เน็ตเฟรม

Preamble	Destination Address	Source Address	Type	Data	FCS

รูปที่ 3.14 โครงสร้างของอีเทอร์เน็ตเฟรม

พรีเอมเบิล (Preamble)

มีขนาด 64 บิท ใช้เพื่อสร้างสัญญาณพร้อม (Synchronize signal) กับเวิคสเตชันที่เป็นผู้รับ โดยปกติจะใช้พรีเอมเบิลแสดงจุดเริ่มต้นของแพกเก็ต หรือเฟรม ด้วยเหตุที่พรีเอมเบิลเป็นสัญญาณที่ใช้ สร้างสัญญาณพร้อมเท่านั้น ดังนั้นภายในจึงประกอบด้วยบิทของข้อมูลที่ไม่มีความหมายต่อเวิคสเตชันผู้รับ

ที่อยู่ปลายทาง (Destination Address)

มีขนาด 48 บิท ใช้สำหรับเวิคสเตชันนั้นๆ ในการที่จะส่งแพกเก็ตไปยังเวิคสเตชันอื่น ซึ่งแต่ละเวิคสเตชันจะทำการตรวจสอบฟิลด์นี้ว่า ควรจะรับแพกเก็ตนี้หรือไม่ เลขฮาร์ดแวร์แอดเดรสขนาด 48 บิทนี้เรียกว่าอีเทอร์เน็ตแอดเดรสหรือแมคแอดเดรส การ์ดเชื่อมต่อระบบเครือข่ายทุกการ์ด จะมีเลข 48 บิทนี้ ใช้บอกถึงเลขประจำตัวของการ์ดเชื่อมต่อนั้นๆ ของเวิคสเตชันที่ต้องการส่งข้อมูลไป

ที่อยู่ต้นทาง (Source Address)

มีขนาด 48 บิท เป็นแอดเดรสของตัวสถานีที่ส่งเอง และแอดเดรสก็จะไม่ซ้ำกันกับอีเทอร์เน็ตแอดเดรสอื่นๆ

ไทป์ (Type)

มีขนาด 16 บิท เป็นข้อมูลที่ระบุชนิดของโปรโตคอลของแพกเก็ต เช่น TCP/IP, OSI, IPX และ XNS เป็นต้น ถ้ามีการใช้งานหลายโปรโตคอลในระดับเดียวกันบนสื่อเดียวกัน จะใช้ค่านี้บอกถึงโปรโตคอลในระดับชั้นบนขึ้นไป

ข้อมูล (Data)

เป็นข้อมูลที่มีขนาดอย่างน้อย 46 ไบท์ แต่เมื่อรวมกับฟิลด์ต่างๆ เข้าด้วยกันแล้ว จะมีขนาดไม่น้อยกว่า 72 ไบท์ ถ้าแพกเก็ตใดๆ ของอีเทอร์เน็ตมีขนาดเล็กกว่านี้ จะถือว่าเป็นแพกเก็ตที่ไม่สมบูรณ์ ขนาดที่ใหญ่ที่สุดของข้อมูลคือ 1500 ไบท์

เอฟซีเอส (FCS – Frame Check Sequence)

อีเทอร์เน็ตใช้เอฟซีเอส สำหรับตรวจสอบความผิดพลาดที่เกิดขึ้น ภายในฟิลด์จะประกอบด้วย บิทของข้อมูลที่เรียกว่า Cyclic Redundancy Check ที่ได้มาจากการคำนวณจากฟิลด์อื่นๆ ในเฟรม เมื่อเวิคสเตชันได้รับเฟรมแล้ว ก็จะทำการคำนวณอีกครั้งหนึ่ง โดยเทียบกับข้อมูลที่ได้รับกับค่าที่ได้จากการคำนวณ และเฟรมก็จะทราบว่าเกิดความผิดพลาดขึ้นหรือไม่

บทที่ 4
โปรโตคอล เอสเอ็นเอ็มพี

ปัจจุบันนี้มีเครื่องคอมพิวเตอร์จำนวนมากเชื่อมต่อเข้าด้วยกันเป็นระบบเครือข่าย โดยเฉพาะอย่างยิ่งในลักษณะของระบบอินเตอร์เน็ต ดังนั้นจึงจำเป็นที่จะต้องหาวิธีการเพื่อมาช่วยในการบริหารและดูแลระบบเครือข่ายให้ใช้งานได้อย่างมีประสิทธิภาพมากที่สุด และอาจใช้ในการค้นหาสาเหตุที่ทำให้ระบบเครือข่ายทำงานผิดพลาด ความจำเป็นในการดูแลและบริหารระบบเครือข่ายคอมพิวเตอร์มีความสำคัญมากขึ้นทุกวัน เพราะระบบเครือข่ายทุกวันนี้มีขนาดใหญ่ขึ้นอย่างรวดเร็วมาก เครื่องมือที่นิยมนำมาใช้ทุกวันนี้จะอยู่ในรูปของโปรแกรมบริหารระบบเครือข่ายที่ใช้โปรโตคอล SNMP (Simple Network Management Protocol) เป็นตัวช่วยในการจัดการ

4.1 ระดับชั้นของโปรโตคอลที่ใช้ในโปรแกรมบริหารระบบเครือข่าย

ในระบบเครือข่ายบางชนิดมีโปรแกรมบริหารระบบเครือข่ายที่ใช้โปรโตคอลในระดับล่างๆ เมื่อมีปัญหาเกิดขึ้นกับอุปกรณ์ตัวใดตัวหนึ่ง ผู้ดูแลระบบสามารถจัดการโดยให้อุปกรณ์ตัวที่อยู่ข้างเคียงส่งข้อมูลที่มีรหัสควบคุม (control packet) ไปเพื่อให้อุปกรณ์ตัวนั้นหยุดการทำงานจากสภาวะปกติที่เคยทำอยู่ หลังจากนั้นผู้ดูแลก็สามารถ ตรวจสอบปัญหา แก้ไขปัญหา หรือเปลี่ยนเส้นทางการส่งข้อมูลไปยังอุปกรณ์ตัวอื่นได้ แต่ในระบบเครือข่ายอินเตอร์เน็ตมีโปรโตคอลหลายระดับประกอบกับมีอุปกรณ์หลายประเภทเชื่อมต่อกันอยู่ภายในระบบ จึงไม่เหมาะที่จะใช้โปรโตคอลระดับล่างๆ ในการบริหารระบบเครือข่าย ซึ่งการใช้โปรโตคอลชั้นบนในการบริหารดูแลระบบเครือข่ายก็มีทั้งข้อดีและข้อเสียแตกต่างกัน

ข้อดีของการใช้โปรโตคอลระดับบน

1. เนื่องจากโปรโตคอลระดับบนสามารถใช้งานโปรโตคอลชั้นต่ำกว่าโดยไม่ต้องสนใจรายละเอียดหรือการทำงานของอุปกรณ์ จึงสามารถนำโปรแกรมที่ใช้ในการบริหารระบบเครือข่ายไปใช้ได้กับทุกเครือข่ายโดยไม่ต้องสนใจว่าภายในระบบเครือข่ายนั้นๆ จะมีอุปกรณ์ชนิดใดอยู่บ้าง

2. โปรแกรมบริหารระบบเครือข่ายส่วนใหญ่ใช้โปรโตคอล TCP/IP และอุปกรณ์เราเตอร์ก็สนับสนุนโปรโตคอล IP อยู่แล้ว จึงทำให้การบริหารระบบเครือข่ายสามารถทำจากที่ใดก็ได้ในระบบเครือข่าย

ข้อเสียของการใช้โปรโตคอลระดับบน

1. ถ้าระบบปฏิบัติการหรือโปรแกรมที่ใช้ในการติดต่อสื่อสารเกิดมีข้อผิดพลาดก็จะทำให้การบริหารไม่สามารถเข้าถึงระบบเครือข่ายนั้นได้

2. ถ้าระบบปฏิบัติการของอุปกรณ์เราเตอร์ทำงานผิดพลาดก็ทำให้การบริหารไม่สามารถเข้าถึงระบบเครือข่ายนั้นได้เช่นกัน

ถึงแม้ว่าการใช้โปรโตคอลในระดับบนจะมีข้อเสียอยู่บ้างแต่เมื่อพิจารณาถึงประโยชน์ที่ได้รับเนื่องจากการควบคุมดูแลระบบเครือข่ายจากที่ใดก็ได้ภายในระบบแล้ว ก็คุ้มค่าพอที่จะเลือกใช้โปรโตคอลระดับบนในการส่งข้อมูลของโปรแกรมบริหารระบบเครือข่าย

4.2 โครงสร้างของการบริหารระบบเครือข่าย

การบริหารระบบเครือข่ายที่ใช้โปรโตคอล TCP/IP ประกอบด้วยส่วนต่างๆ ดังต่อไปนี้

1. สถานีส่วนกลางที่ใช้ในการตรวจสอบสภาพของระบบ (Management Station, MS)
2. ซอฟต์แวร์ที่คอยเก็บข้อมูลและส่งสัญญาณเตือนเมื่อเกิดความผิดพลาดในระบบ (Managed Agent, MA)
3. โครงสร้างของข้อมูลที่เก็บ (Management Information Base, MIB)
4. โปรโตคอลที่ใช้ในการสื่อสาร (Network Management Protocol, NMP)

Management Station มีส่วนประกอบที่สำคัญคือ

1. ซอฟต์แวร์ที่ใช้ในการวิเคราะห์ข้อมูลและแก้ไขข้อผิดพลาดที่เกิดขึ้น
2. ระบบอินเตอร์เฟสที่ใช้ในการตรวจสอบและควบคุมระบบเครือข่าย
3. มีความสามารถตรงกับความต้องการของผู้ดูแลระบบที่ใช้ในการตรวจสอบสภาพความเป็นจริงของระบบและสามารถควบคุมอุปกรณ์ที่อยู่ในระยะไกลได้
4. ความสามารถในการดึงข้อมูลจาก MIB

อุปกรณ์ต่างๆ ที่อยู่ในระบบเครือข่ายต้องมี SNMP agent จึงจะสามารถควบคุมจาก MS ได้ ซึ่ง agent เหล่านี้จะคอยตอบข้อมูลที่ MS ร้องขอมาหรือไม่ก็ตอบสนองต่อการกระทำที่ส่งมาจาก MS ทรัพยากรต่างๆ ที่อยู่ในระบบถูกมองเป็นวัตถุ โดยวัตถุแต่ละตัวเป็นตัวแปรที่ถูกเก็บรวบรวมไว้ใน MIB ซึ่ง MIB มีหน้าที่เป็นจุดเชื่อมต่อระหว่าง agent และ MS โดย MS สามารถตรวจสอบสภาพต่างๆ ของระบบโดยดูจากค่าของตัวแปรที่เก็บอยู่ใน MIB MS สามารถสั่งให้ agent ทำงานตามที่ต้องการโดยแก้ไขค่าของตัวแปรพิเศษของ agent หรือไม่ก็สามารถเปลี่ยนแปลง Configuration ของ agent ได้ MS และ agent สามารถติดต่อสื่อสารกันได้โดยใช้ NMP และโปรโตคอลที่ใช้ในการบริหารระบบเครือข่าย TCP/IP คือ SNMP ซึ่ง ตัวโปรโตคอลมีความสามารถในการ

1. ทำให้ MS สามารถดึงข้อมูลจาก agent ได้ (get)

2. ทำให้ MS สามารถเปลี่ยนแปลงแก้ไขค่าตัวแปรของ agent ได้ (set)

3. ทำให้ agent สามารถแจ้งเตือน MS ในกรณีที่มีความผิดพลาดเกิดขึ้นในระบบ (trap)

โดยทั่วไปแล้วไม่มีข้อกำหนดว่าควรมี MS กี่ตัวในระบบหรือควรมีอัตราส่วนระหว่าง MS กับ agent เป็นเท่าไหร่ แต่เพื่อความรอบคอบควรมี MS อย่างน้อย 2 ตัว เพื่อป้องกันข้อผิดพลาดที่เกิดจาก MS ไม่ทำงาน [4]

4.3 สถาปัตยกรรมของโปรโตคอลบริหารระบบเครือข่าย

SNMP เป็นโปรโตคอลที่จัดอยู่ในชั้นของ Application level ของโปรโตคอล TCP/IP โดยโปรโตคอล SNMP จะทำงานบนโปรโตคอล UDP ซึ่งเป็นโปรโตคอลแบบ connectionless ไม่ต้องมีการสร้าง connetion ก่อนการส่งข้อมูล จากรูปที่ 4.1 จะเห็นได้ว่ามี MS อยู่เครื่องหนึ่งซึ่งมี Manager Process (MP) คอยควบคุมการเข้าถึง MIB ส่วนกลางที่อยู่ใน MS และ MP ยังเป็นส่วนการติดต่อระหว่าง MS กับผู้ดูแลระบบเครือข่าย MP จะใช้โปรโตคอล SNMP ติดต่อระหว่าง MS และ agent โดย agent จะมีโปรเซสซึ่งทำหน้าที่ในการแปลความของ message ที่อยู่ใน SNMP แล้วไปควบคุม MIB ของ agent

4.4 โครงสร้างของ Management Information

มีการกำหนดมาตรฐานในการตั้งชื่อตัวแปรของ MIB ซึ่งรู้จักกันในชื่อของ Structure of Management Information (SMI) ประกอบไปด้วยกฎในการตั้งชื่อตัวแปรและความหมายของตัวแปร และเพื่อความง่ายต่อการนำไปใช้กับ NMP จึงมีการจำกัดชนิดของตัวแปรที่อนุญาตให้ใช้ใน MIB นอกจากนี้ SMI ยังมีกฎในการสร้างชนิดของตัวแปร และยังกำหนดวิธีการอ้างอิงตัวแปรต่างๆ ที่อยู่ใน MIB [5]

4.4.1 การกำหนดรูปแบบโดยใช้ ASN.1

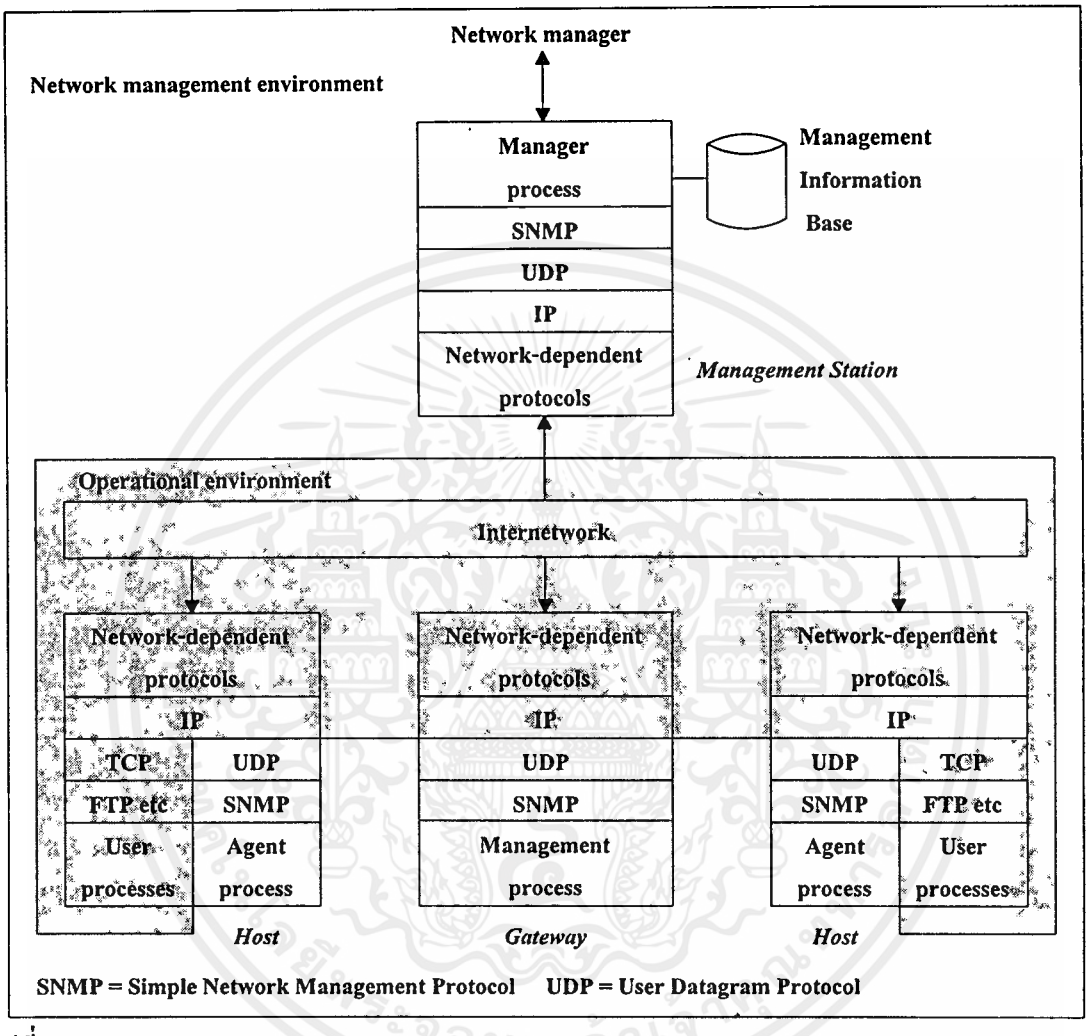
เนื่องจาก SMI ใช้มาตรฐาน ISO ที่มีชื่อว่า Abstract Syntax Notation 1 (ASN.1) ในการกำหนดตัวแปรและการอ้างถึงตัวแปรใน MIB ซึ่ง ASN.1 ประกอบไปด้วยหลักการใหญ่ๆ 2 ส่วนคือ

การใช้สัญลักษณ์ที่มนุษย์สามารถเข้าใจความหมายแทนข้อมูล

การเข้ารหัสข้อมูลที่มนุษย์เข้าใจเพื่อนำไปใช้กับโปรโตคอลในการติดต่อสื่อสาร

ซึ่งสัญลักษณ์ที่ใช้ในทั้ง 2 กรณีต้องไม่มีความสับสนในเรื่องของความหมายและการแสดงแทนข้อมูล เช่น แทนที่จะประกาศว่าเป็นตัวแปรชนิด integer เพียงอย่างเดียวก็กำหนดให้แน่นอนลงไปว่ามีค่าอยู่ในช่วงใดด้วย เพราะว่าบางครั้งอาจนำไปใช้กับเครื่องคอมพิวเตอร์ต่างชนิดกัน ซึ่งมี

ความแตกต่างในเรื่องการแทนข้อมูลและช่วงค่าของตัวแปร ASN.1 ยังกำหนดวิธีการเข้ารหัสของชื่อและข้อมูลอีกทั้งวิธีการแปลงข้อมูลที่อยู่ในรูปสัญลักษณ์ที่มนุษย์สามารถเข้าใจไปเป็นข้อมูลที่เข้ารหัสที่ใช้ในการส่งข้อมูลของ SNMP

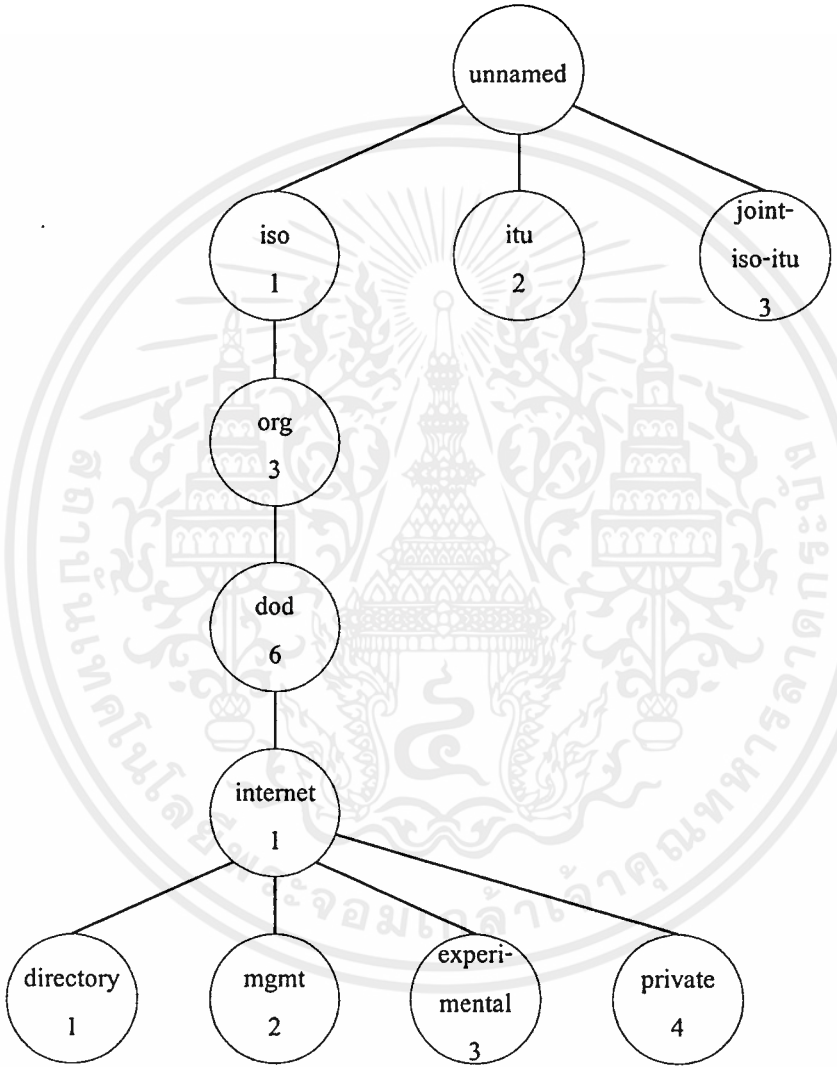


รูปที่ 4.1 แสดง Configuration ของ SNMP

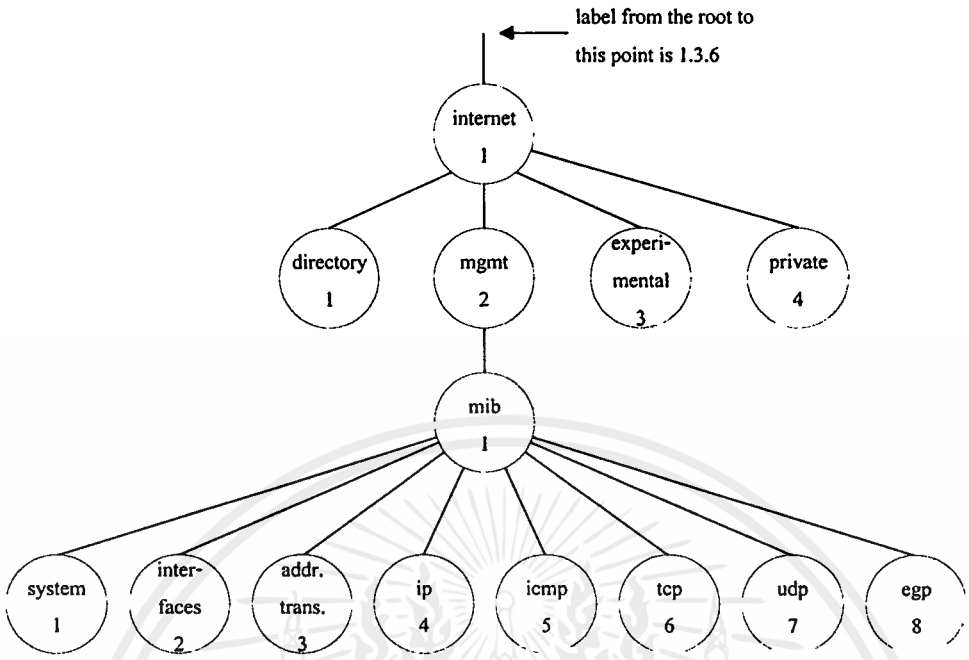
4.4.2 โครงสร้างและการแทนชื่อวัตถุที่อยู่ใน MIB

ชื่อที่ใช้สำหรับตัวแปรใน MIB ถูกกำหนดโดย ISO และ ITU ซึ่งชื่อที่นำมาตั้งให้วัตถุแต่ละตัวไม่มีข้อจำกัดใดๆ และไม่จำเป็นต้องใช้ในการบริหารระบบเครือข่ายเพียงอย่างเดียว ชื่อที่นำมาตั้งจะถูกแบ่งเป็นลำดับชั้นแต่ละชั้นก็มีสิทธิในการตั้งชื่อให้กับวัตถุต่างๆ โดยไม่ต้องเกี่ยวข้องกับลำดับชั้นบนสุด แต่ละชื่อที่ตั้งจะไม่ซ้ำกับชื่ออื่นเลยแม้ว่าจะอยู่กันคนละระดับชั้นก็ตาม จากรูปที่ 4.2 จะเห็นได้ว่าชั้นบนสุดไม่มีการตั้งชื่อไว้ แต่ชั้นถัดมาจะแบ่งออกเป็น 3 กลุ่มคือ ISO, ITU และการใช้ร่วมกันระหว่าง ISO กับ ITU ลำดับชั้นถัดมาได้กำหนดเป็นข้อความสั้นๆ กับตัวเลขประจำข้อความนั้น สาเหตุที่กำหนดอย่างนั้นก็เพื่อให้มนุษย์สามารถเข้าใจความหมายได้ทันทีในขณะที่

ตัวเลขนำไปใช้เมื่อต้องการเข้ารหัสของชื่อโดยใช้คอมพิวเตอร์ ชื่อของวัตถุที่อยู่ในลำดับชั้นประกอบด้วยลำดับของตัวเลขประจำแต่ละระดับไปจนถึงชั้นที่วัตถุตัวนั้นอยู่ ระหว่างตัวเลขเหล่านั้นจะมีจุดแยกออกจากกันเช่น ชื่อ 1.3.6.1.1 ใช้แทนวัตถุที่ชื่อ directory และ MIB ที่อยู่ภายใต้ลำดับชั้นของ internet และ mgmt ดังนั้นตัวแปรของ MIB ทุกตัวจะมีชื่อ 1.3.6.1.2.1 นำหน้าเสมอดังรูปที่ 4.3



รูปที่ 4.2 แสดงการแทนชื่อวัตถุที่อยู่ใน MIB



รูปที่ 4.3 แสดงค่า MIB ที่อยู่ภายใต้ iso.org.dod.internet.mgmt.mib หรือ 1.3.6.1.2.1

จากรูปที่ 4.3 MIB ถูกแบ่งออกเป็นกลุ่มใหญ่ได้ 8 ประเภทตามตารางที่ 4.1

ตารางที่ 4.1 แสดงการแบ่งกลุ่มของ MIB

System	1
Interfaces	2
address translation	3
Ip	4
Icmp	5
Tcp	6
Udp	7
Egp	8

ตารางที่ 4.2 แสดงตัวอย่างชื่อตัวแปรใน MIB

MIB Variable	Category.	Meaning
SysUpTime	system	Time since last reboot
IfNumber	interfaces	Number of network interfaces
IfMtu	interfaces	MTU for a particular interface
ipDefaultTTL	ip	Value IP uses in time-to-live field
ipInReceives	ip	Number of datagrams received
ipForwDatagrams	ip	Number of datagrams forward
ipOutNoRoutes	ip	Number of routing failures
ipReasmOKs	ip	Number of datagrams reassembled
ipFragOKs	ip	Number of datagrams fragmented
ipRoutingTable	ip	IP Routing Table
icmpInEchos	icmp	Number of ICMP Echo Requests received
tcpRtoMin	tcp	Minimum retransmission time TCP allows
tcpMaxConn	tcp	Maximum TCP connections allowed
tcpInSegs	tcp	Number of segments TCP has received
udpInDatagrams	udp	Number of UDP datagrams received
egpInMsgs	egp	Number of EGP messages received

ตัวอย่างต่อไปนี้จะช่วยให้เข้าใจการอ้างอิงถึงตัวแปรใน MIB มากขึ้น จากรูปที่ 4.3 ถ้าจะอ้างถึง label ที่ชื่อ IP สามารถอ้างได้ 2 แบบ คือ

1.3.6.1.2.1.4

iso.org.dod.internet.mgmt.mib.ip

ภายใต้ label IP ก็จะมีชื่อตัวแปรอื่นๆ เช่น ipInReceives ซึ่งมีหมายเลข 3 ประจำ label ถ้าจะอ้างถึงก็จะได้

1.3.6.1.2.1.4.3

iso.org.dod.internet.mgmt.mib.ip.ipInReceives

เมื่อจะนำชื่อตัวแปรใน MIB ไปใช้กับ NMP แต่ละชื่อต้องมีคำลงท้าย เช่นคำลงท้ายด้วย "0" หมายถึงเป็นชื่อของตัวแปรตัวนั้น ดังนั้นถ้าจะส่งตัวแปรชื่อ ipInReceives ไปให้เราเตอร์ จะแทนเป็นตัวเลขได้ 1.3.6.1.2.1.4.3.0

เนื่องจากไม่สามารถคาดเดาหมายเลขที่จะแทนชื่อตัวแปรและค่าที่อยู่หลังชื่อได้ ดังนั้นการแปลงชื่อที่อยู่ในรูปข้อความให้เป็นตัวเลขต้องใช้วิธีดูค่าจากตารางอย่างเดียวเพราะไม่มีความสัมพันธ์ระหว่างชื่อที่เป็นตัวอักษรกับชื่อที่เป็นตัวเลข และเมื่อพิจารณาถึงตัวแปรที่มีความสลับซับซ้อนมากขึ้นอย่าง ipAddrTable ก็จะเข้าใจว่าไม่สามารถหาความสัมพันธ์ในการแปลงได้

ipAddrTable เป็นตัวแปรที่ประกอบด้วยหมายเลข IP สำหรับแต่ละ network interface โดยตัวแปรนี้อยู่ใต้เลเบล IP อีกชั้นและมีหมายเลขประจำตัวคือ 20 ดังนั้นสามารถอ้างถึงโดยใช้ 1.3.6.1.2.1.4.20 หรือ iso.org.dod.internet.mgmt.mib.ip.ipAddrTable ในภาษาที่ใช้ในการโปรแกรม โดยทั่วๆ ไปอาจมอง Ip Address Table เป็นอะเรย์ 1 มิติ ที่แต่ละสมาชิกในอะเรย์เป็นเรคอร์ดที่ประกอบด้วย 5 ฟิลด์ คือ IPAddress , ตัวเลขที่เป็น index ของแต่ละ interface , IP subnet mask , IP broadcast address และตัวเลขที่ระบุ datagram ขนาดสูงสุดที่เราเตอร์สามารถรับได้ MIB ก็มีชื่อของตัวแปรเหล่านี้ด้วยถ้ามันมีอยู่ในเราเตอร์ สามารถใช้ ASN.1 กำหนด ipAddrTable ได้ดังนี้

ipAddrTable ::= SEQUENCE OF IpAddrEntry

SEQUENCE และ OF เป็นคำที่ใช้กำหนดให้ ipAddrTable เป็นอะเรย์ 1 มิติของ IpAddrEntry แต่ละสมาชิกในอะเรย์จะกำหนดเป็นฟิลด์ 5 ฟิลด์ได้ดังนี้เมื่อสมมุติว่าได้มีการกำหนดนิยามของ IpAddress ขึ้นก่อนหน้าแล้ว

```
IpAddrEntry ::= SEQUENCE {
    ipAdEntAddr
        IpAddress,
    ipAdEntIfIndex
        INTEGER,
    ipAdEntNetMask
        IpAddress,
    ipAdEntBcastAddr
        IpAddress,
    ipAdEntReasmMaxSize
        INTEGER(0..65535)
}
```

นอกจากนั้นยังต้องกำหนดหมายเลขให้ ipAddrEntry และสมาชิกที่อยู่ใน ipAddrEntry ด้วย เช่น

ipAddrEntry {ipAddrTable 1}

หมายถึง ipAddrEntry อยู่ใน ipAddrTable และมีค่าประจำคือ 1 เช่นเดียวกัน สมาชิกใน ipAddrEntry ก็จะมีการกำหนดค่าดังนี้

ipAdEntNetMask {ipAddrEntry 3}

หมายถึง ipAdEntNetMask อยู่ใน ipAddrEntry และมีค่าประจำคือ 3

ถึงแม้ว่าจะมอง ipAddrTable เป็นอะเรย์ 1 มิติก็ตาม แต่วิธีการอ้างถึงสมาชิกที่อยู่ในอะเรย์นั้นแตกต่างจากภาษาที่ใช้ในการโปรแกรมโดยทั่วไป ภาษาเหล่านั้นใช้ index ในการอ้างถึงสมาชิกที่อยู่ในอะเรย์ เช่น member[3] หมายถึง สมาชิกตัวที่ 3 ที่อยู่ในอะเรย์ member ASN.1 ไม่ได้ใช้วิธีการอ้างถึงสมาชิกในอะเรย์โดยใช้ index แต่จะใช้การเติมคำลงท้ายหลังชื่อตัวแปรเพื่อเลือกสมาชิกที่อยู่ในอะเรย์ เช่น ถ้าต้องการจะอ้างถึงค่าตัวแปรที่อยู่ในฟิลด์ subnet mask ของ ipAddrTable โดยกำหนดให้ฟิลด์นั้นเก็บค่า 255.255.255.192 จะอ้างได้ดังนี้

iso.org.dod.internet.mgmt.mib.ip.ipAddrTable.ipAddrEntry.ipAdEntNetMask.255.255.255.192

หรือในรูปตัวเลขจะได้

1.3.6.1.2.1.4.20.1.3.255.255.255.192

4.5 Simple Network Management Protocol (SNMP)

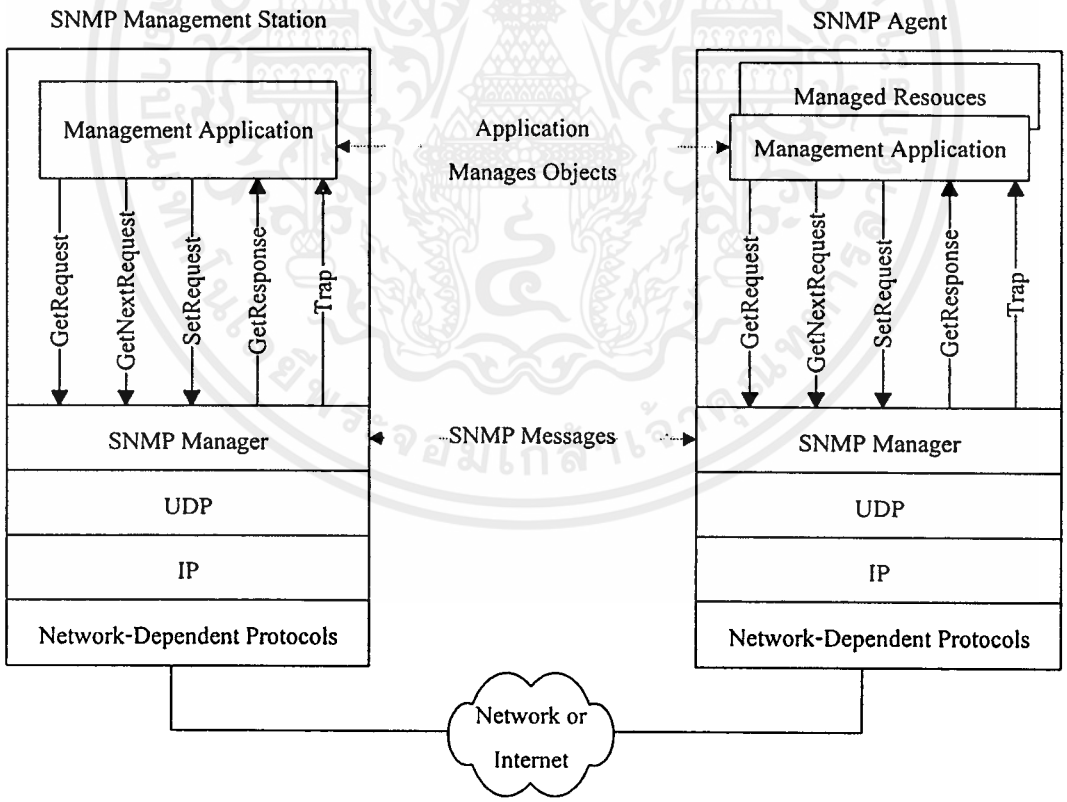
Network Management Protocol ใช้ในการติดต่อระหว่างโปรแกรมที่เป็นลูกข่ายกับโปรแกรมหลักที่รันอยู่บนโฮสหรือเราเตอร์ โปรโตคอลเหล่านี้ต้องมีการออกแบบรูปแบบคำสั่งในการทำงานเช่นการ reboot ระบบ , การเพิ่มหรือลดเส้นทาง , การอนุญาตหรือไม่อนุญาต การเชื่อมต่อระหว่าง interface ต่างๆ ซึ่งเมื่อดูรูปแบบคำสั่งโดยรวมแล้วจะทำให้โปรโตคอลมีความซับซ้อนมากยิ่งขึ้นไม่เหมาะกับการนำไปใช้งาน SNMP พยายามลดความซับซ้อนของโปรโตคอลลงโดยใช้หลักการ fetch และ store ในการดึงค่าจากตัวแปรและแก้ไขค่าในตัวแปรถึงแม้ว่าจะไม่มีคำสั่ง reboot แต่ก็สามารถบูตระบบใหม่ได้โดยไปตั้งค่าเวลาของตัวแปรที่เกี่ยวกับการบูตระบบครั้งต่อไปให้เป็นศูนย์ เนื่องจาก SNMP มีเพียงการ fetch และ store จึงทำให้ง่ายต่อการสร้างและการดีบักเพราะไม่มีกรณีพิเศษสำหรับแต่ละคำสั่ง ดังแสดงตามตารางที่ 4.3

ตารางที่ 4.3 แสดงคำสั่งที่ใช้ใน SNMP

Command	Meaning
get-request	Fetch a value from a specific variable
get-next-request	Fetch a value without knowing its exact name
get-response	Reply to a fetch operation
set-request	Store a value in a specific variable
Trap	Reply triggered by an event

คำสั่ง get-request , get-response และ set-request อยู่ในรูปของการ fetch และ store ข้อมูลในตัวแปร นอกจากนี้ทุกคำสั่งที่ใช้ใน SNMP จะถือว่าเป็น atomic นั่นคือถ้ามีการกระทำเกิดขึ้นกับตัวแปรหลายๆ ตัว จะต้องไม่มีตัวแปรตัวใดตัวหนึ่งเกิดข้อผิดพลาด ถ้ามีข้อผิดพลาดเกิดขึ้นจะยกเลิกการกระทำนั้น ส่วนคำสั่ง Trap มีไว้เพื่อถ้าเกิดเหตุการณ์ที่สำคัญๆ ขึ้นมา เช่น interface เสีย ก็ให้ agent ส่ง Trap ไปบอกโปรแกรมที่ทำหน้าที่ดูแลระบบ

จากที่ได้กล่าวไปแล้วว่า ASN.1 ไม่มี index ในการอ้างถึงสมาชิกที่อยู่ในอะเรย์แต่จะใช้การเติมคำลงท้ายต่อหลังชื่อตัวแปรเพื่ออ้างถึงแทนเนื่องจากไม่รู้จำนวนสมาชิกที่อยู่ในอะเรย์เหล่านั้น SNMP จึงมีคำสั่ง get-next-request ในการดึงค่าถัดไปของอะเรย์โดยมีกฎว่าเมื่อฝ่ายส่ง ส่งคำสั่ง get-next-request ต้องระบุ prefix ของตัวแปรตัวนั้นให้ถูกต้องสมมติว่าเป็น P ฝ่ายรับก็จะตรวจสอบดูว่า prefix นั้นครอบคลุมตัวแปรใดอยู่บ้าง แล้วเลือกตัวแปรที่มีค่ามากกว่า P ส่งไปให้ฝ่ายรับโดยใช้คำสั่ง get-response ดังนั้นในการอ้างถึงตัวแปรของ MIB ที่อยู่ในรูปตารางก็เพียงส่ง prefix ที่ระบุชื่อตารางนั้นไปก็จะได้รับสมาชิกตัวแรกของตารางกลับมา ถ้าต้องการสมาชิกตัวที่สองก็ส่งชื่อของสมาชิกตัวแรกไปก็จะได้รับสมาชิกตัวที่สองกลับมา



รูปที่ 4.4 แสดงการทำงานของโปรโตคอล SNMP

4.6 SNMP Message Format

SNMP ไม่เหมือนโปรโตคอลตัวอื่นๆ ใน TCP/IP เพราะว่า SNMP message ไม่มีการกำหนดขนาดที่แน่นอน การเข้ารหัสกำหนดโดยมาตรฐาน ASN.1 ในที่นี้จะกล่าวถึงส่วนประกอบต่างๆ ของ SNMP message อย่างคร่าวๆ

SNMP message ประกอบด้วย 3 ส่วน คือ

- protocol version
- SNMP community identifier
- data area

ในส่วนของ data area ยังแบ่งออกเป็น protocol data units (PDUs) แต่ละ PDU ประกอบด้วย request ถ้าส่งโดย client และ response ที่ส่งโดย server

ตัวอย่างของ message ที่กำหนดโดย ASN.1

```
SNMP-Message ::=
    SEQUENCE    {
        version INTEGER    {
            version-1 (0)
        },
        community
            OCTEC STRING,
        data
            ANY
    }
```

ตัวอย่างของ PDU

```
SNMP-PDUS ::=
    CHOICE  {
        get-request
            GetRequest-PDU,
        get-next-request-PDU
            GetNextRequest-PDU,
        get-response
            GetResponse-PDU,
        get-request
            SetRequest-PDU,
        trap
            Trap-PDU,
    }
```

ตัวอย่างของ get-request

```
GetRequest-PDU ::= [0]
    IMPLICIT SEQUENCE   {
        request-id
            RequestID,
        error-status
            ErrorStatus,
        error-index
            ErrorIndex,
        variable-bindings
            VarBindList
    }
```

RequestID เป็น integer ขนาด 4 ไบท์ ใช้ในจับคู่ระหว่าง responses และ queries

Error-Status และ ErrorIndex เป็น integer ขนาด 1 ไบท์

VarBindList ประกอบไปด้วยชื่อของวัตถุที่ต้องการหาค่า ใน ASN.1 ระบุว่าเป็นคู่ของชื่อวัตถุกับค่าประจำวัตถุตัวนั้น

Network Management Protocol ช่วยให้ผู้ดูแลระบบสามารถตรวจสอบและดูแลอุปกรณ์ภายในระบบเครือข่ายได้ โดยมีตัวโปรแกรมหลักคอยรับข้อมูลจากโปรแกรมย่อยที่อยู่บนอุปกรณ์ต่างๆ หรือที่เรียกว่า agent และเนื่องจากในระบบเครือข่ายอินเตอร์เน็ตมีอุปกรณ์หลากหลายชนิดอยู่ในเครือข่ายจึงใช้โปรโตคอล UDP ในการติดต่อระหว่างโปรแกรมหลักและโปรแกรมย่อย NMP เป็นโปรโตคอลที่กำหนดขึ้นมาเพื่ออำนวยความสะดวกในการขอดูข้อมูลต่างๆ ของ Management Information Base (MIB) โดยตัวโปรโตคอลมีเพียงรูปแบบคำสั่งพื้นฐานเพียงสองแบบเท่านั้น คือ Fetch ใช้ในการดึงค่าของตัวแปรใน MIB และ Store สำหรับเปลี่ยนแปลงค่าตัวแปรใน MIB ชื่อตัวแปรที่อยู่ใน MIB มีข้อกำหนดในการตั้งชื่อและอ้างอิงโดยใช้มาตรฐาน ASN.1 ตัวมาตรฐานยังกำหนดวิธีการเข้ารหัสข้อมูลจากรูปแบบที่มนุษย์เข้าใจความหมายไปเป็นรูปแบบข้อมูลที่ใช้ในการสื่อสารของโปรโตคอล SNMP นอกจากนี้ตัวมาตรฐานแบ่งชื่อของตัวแปรของ MIB ออกเป็นลำดับชั้นเพื่อรับประกันว่าชื่อของตัวแปรแต่ละตัวจะไม่ซ้ำกันเลย

บทที่ 5
เราติงโปรโตคอล

ในการเชื่อมต่อระบบเครือข่าย ซึ่งอาจจะมีจำนวนหลายเครือข่ายหลายที่เชื่อมต่อเข้าด้วยกัน และมีจำนวนเราเตอร์ที่ใช้ในการส่งข้อมูลระหว่างเครือข่ายอยู่หลายตัว จึงมีความจำเป็นที่จะต้องนำเราติงโปรโตคอล ซึ่งมีหน้าที่ในการช่วยหาเส้นทางให้กับเราเตอร์ เพื่อช่วยให้การส่งข้อมูลเป็นไปได้อย่างรวดเร็ว เนื่องจากเราติงโปรโตคอลสามารถรู้เส้นทางที่ดีที่สุดในการส่งข้อมูลได้

5.1 เราติงโปรโตคอล

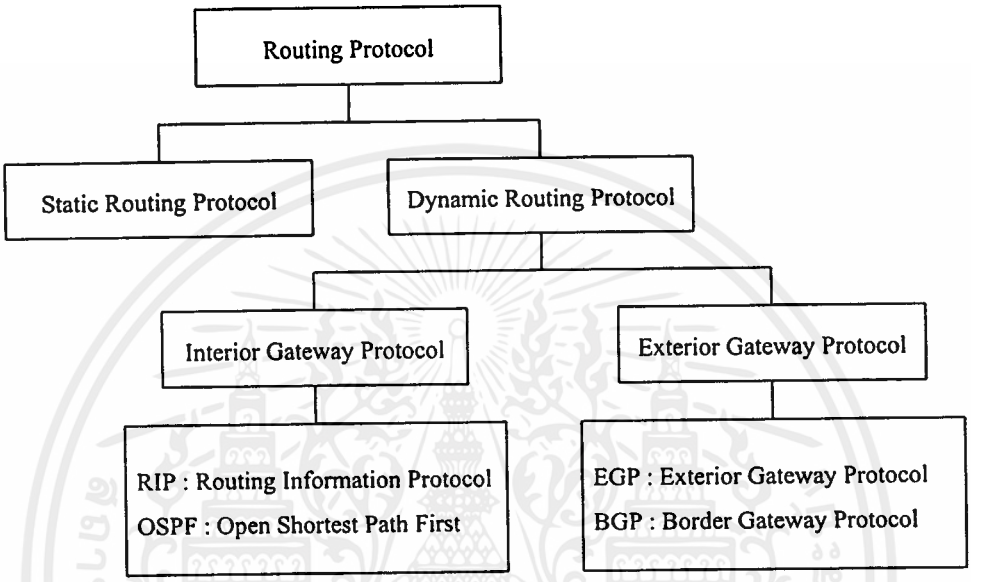
เราติงโปรโตคอล เป็นระบบที่เราเตอร์ต่างๆ ในระบบเครือข่ายใช้เป็นข้อตกลงในการแลกเปลี่ยนข่าวสารระหว่างกัน เมื่อมีเฟรมข้อมูลในการส่งผ่านเข้ามา ก็จะเรียนรู้ได้ทันทีว่าจะส่งเฟรมข้อมูลนี้ออกไปยัง Port Interface ใด เพื่อที่จะให้เฟรมข้อมูลนี้ถูกส่งผ่านออกไปจนถึงเครื่องคอมพิวเตอร์ปลายทางได้อย่างสมบูรณ์ ในปัจจุบันมาตรฐานการทำงานของเราติงโปรโตคอล มีหลายชนิดด้วยกัน ซึ่งสามารถแบ่งออกได้เป็น 2 กลุ่มใหญ่ๆ คือ

5.1.1 Static Routing Protocol เป็นระบบที่จะต้องมีการกำหนดหมายเลขเส้นทางของการเชื่อมต่อเพื่อส่งผ่านข้อมูลแบบ Manual กล่าวคือ ผู้ที่ดูแลระบบเครือข่าย จะต้องกำหนดเส้นทาง (Port Interface) และ IP Network ต่างๆ ให้เราเตอร์รู้จักอยู่เสมอ เช่น ถ้าต้องการให้เราเตอร์สามารถส่งผ่านเฟรมข้อมูลไปที่แห่งใดได้บ้างนั้น ก็จะต้องกำหนดลงไปในซอฟแวร์ของเราเตอร์นั้นๆ ให้เราเตอร์รู้จัก ซึ่งเราเตอร์ก็จะรู้จักเส้นทางที่จะส่งผ่านเฟรมข้อมูลหรือ IP Network ตามที่ได้กำหนดในซอฟแวร์ของเราเตอร์เท่านั้น ไม่สามารถที่จะเรียนรู้ได้เองอย่างอัตโนมัติ เมื่อมีการเพิ่มเส้นทางหรือ IP Network ขึ้นมา หรือมีการเปลี่ยนแปลงเส้นทางที่มีอยู่เดิม เราเตอร์จะไม่สามารถเรียนรู้ได้เลยจนกว่าจะมีการกำหนดหรือแก้ไขในซอฟแวร์เราเตอร์ใหม่

5.1.2 Dynamic Routing Protocol เป็นเราติงโปรโตคอลที่มีการกำหนดค่าพารามิเตอร์และขอบเขตการทำงานบางอย่างให้กับซอฟแวร์ของเราเตอร์นั้น หลังจากนั้นเราเตอร์จะทำการแลกเปลี่ยนข้อมูลต่างๆ กับเราเตอร์อื่นๆ ที่ต่อเชื่อมกัน จากนั้นเราเตอร์ก็จะสามารถเรียนรู้เส้นทางและค่า IP Network ต่างๆ ในระบบเครือข่ายได้เอง และเมื่อมีการเปลี่ยนแปลงเส้นทางหรือ IP Network ในระบบเครือข่ายใดๆ เราเตอร์ที่ทำงานในฟังก์ชันนี้ก็จะสามารถเรียนรู้การเปลี่ยนแปลงเหล่านั้นได้เองโดยอัตโนมัติ

Dynamic Routing Protocol สามารถแบ่งออกได้เป็น 2 ชนิดตามลักษณะการใช้งานคือ

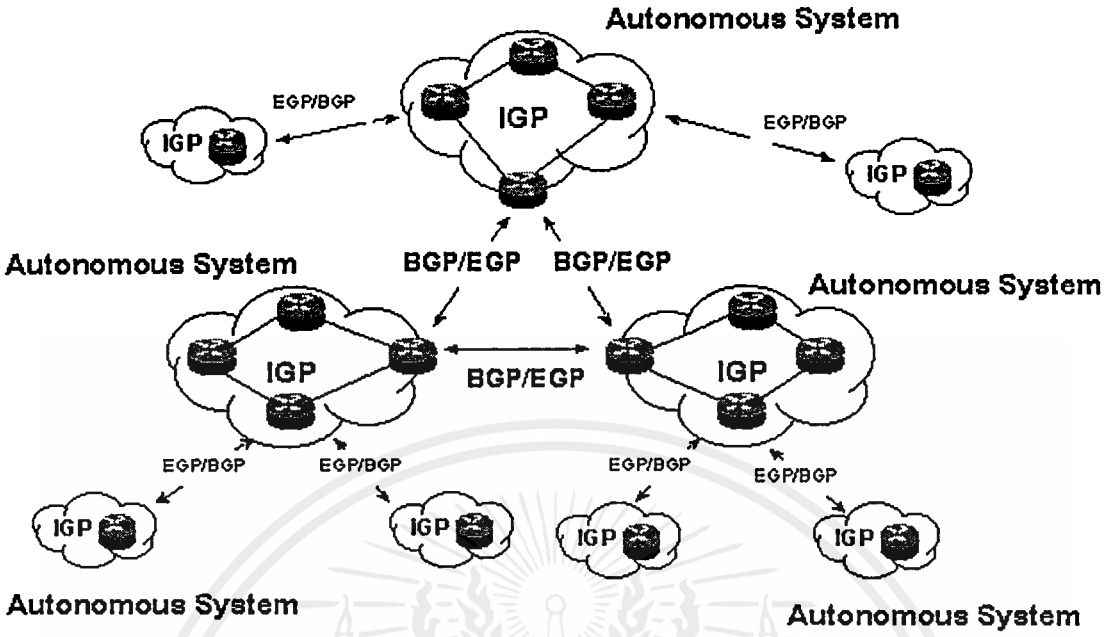
1. **Interior Gateway Protocol (IGP)** เป็นโปรโตคอลในการแลกเปลี่ยนข้อมูลระหว่างเราเตอร์ภายใน Autonomous System เดียวกัน
2. **Exterior Gateway Protocol (EGP)** เป็นโปรโตคอลที่ใช้ในการแลกเปลี่ยนข้อมูลระหว่างเราเตอร์ที่อยู่ใน Autonomous System ที่ต่างกัน



รูปที่ 5.1 แสดงโครงสร้างของระบบ Routing Protocol

5.2 Autonomous System (AS)

Autonomous System คือกลุ่มของเราเตอร์และเครือข่ายที่อยู่ภายใต้การจัดการจากส่วนเดียวกัน โดย AS อาจจะประกอบด้วยเราเตอร์เพียงหนึ่งตัว และระบบเครือข่ายที่เชื่อมต่อกับอินเตอร์เน็ตเพียงเครือข่ายเดียว แต่ไม่มีกฎเกณฑ์ใดๆ ที่จะมากำหนดว่า ใน AS หนึ่งๆ นั้นจะต้องมีขนาดเท่าใด โดยใน AS หนึ่งๆนั้นสามารถที่จะมีเราเตอร์ได้หลายตัวและมีเครือข่ายที่เชื่อมต่อเข้ากับระบบอินเตอร์เน็ตได้หลายๆ เครือข่าย ภายใน AS แต่ละตัวนั้นจะต้องมีการทำการเชื่อมต่อเราเตอร์ทุกตัวเข้าด้วยกันเพื่อที่จะทำการแลกเปลี่ยนข้อมูลระหว่างเราเตอร์แต่ละตัว โดยการแลกเปลี่ยนข้อมูลภายใน AS เดียวกันนั้นจะใช้โปรโตคอลที่เป็น Interior Gateway Protocol ซึ่งใน AS แต่ละตัวนั้นไม่จำเป็นที่จะต้องใช้โปรโตคอลตัวเดียวกันแต่ต้องเป็น IGP เหมือนกัน ในส่วนของ AS แต่ละตัวนั้นก็จำเป็นที่จะต้องมีการเชื่อมต่อเราเตอร์เพื่อแลกเปลี่ยนข้อมูลระหว่าง AS เช่นเดียวกัน โดยโปรโตคอลที่ใช้เชื่อมต่อเราเตอร์ข้าม AS นี้จะเป็นโปรโตคอลประเภท Exterior Gateway Protocol ซึ่งถ้าหาก AS ตัวใดมีการเชื่อมต่อกับหลายๆ AS ในการเชื่อมต่อกับแต่ละ AS นั้นไม่จำเป็นที่จะต้องใช้โปรโตคอลตัวเดียวกัน แต่ต้องเป็น EGP เหมือนกัน [6]



รูปที่ 5.2 แสดงตัวอย่างการเชื่อมต่อของ Autonomous System

5.3 การติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์กับเราเตอร์

เมื่อระบบ Application ต่างๆ ของคอมพิวเตอร์ เช่น FTP,Telnet และ SMTP เป็นต้น ถูกเรียกใช้งาน ข้อมูลเหล่านี้จะถูกกำหนดด้วยค่าประจำพอร์ท (Port Number) ของมาตรฐาน TCP (Transmission Control Protocol) หรือมาตรฐาน UDP (User Datagram Protocol) ดังเช่นการใช้งานบริการเครื่อง Unix Host ก็จะทำการ Telnet ไปเรียกผ่านพอร์ทหมายเลข 23 ของมาตรฐาน TCP หรือการส่งผ่านข้อมูลด้วยวิธี TFTP (Trivial File Transfer Protocol) ก็จะมีหมายเลขประจำพอร์ทของมาตรฐาน UTP ที่ 69 เป็นต้น เมื่อระบบ Application ได้ถูกส่งผ่านและหุ้มด้วยโครงสร้างมาตรฐาน TCP หรือ UDP ที่มีค่าหมายเลขพอร์ทประจำตามชนิดของบริการกำกับอยู่ แล้วส่งผ่านไปยังระดับที่ 3 (Network Layer) ซึ่งฟังก์ชันในการทำงานในระดับนี้คอมพิวเตอร์จะพิจารณาว่า ข้อมูลนี้จะส่งไปยังเครื่องคอมพิวเตอร์เครื่องใด โดยจะพิจารณาที่ค่า IP Address เป็นจุดแรก ซึ่งค่านี้ถูกแปลงเป็นค่า MAC Address อีกทีหนึ่ง โดยใช้หลักของมาตรฐาน ARP (Address Resolution Protocol) ถ้า IP Address ปลายทางอยู่ใน Network Address เดียวกัน เครื่องคอมพิวเตอร์ก็จะติดต่อกันได้โดยตรง แต่ถ้าอยู่คนละ Network Address เฟรมข้อมูลนั้นก็จะถูกส่งไปยังเราเตอร์ซึ่งมีค่าตาราง Network Address (Routing Table) อยู่แล้วเราเตอร์ก็จะถูกส่งผ่านข้อมูลนี้ออกไปยังปลายทาง และในทางกลับกัน ข้อมูลที่ถูกส่งถึงเครื่องปลายทางก็จะมีลักษณะเช่นเดียวกันด้วย

5.4 การติดต่อสื่อสารระหว่างเราเตอร์กับเราเตอร์

ในการติดต่อเราเตอร์นั้น ต้องกำหนดค่าพารามิเตอร์ Network Address ที่เราเตอร์เชื่อมต่ออยู่ และในระบบเครือข่ายขนาดใหญ่มีหลาย Network ซึ่งจะต้องใช้เราเตอร์จำนวนหลายตัวเชื่อมต่อทั้งในส่วนเครือข่ายท้องถิ่น (LAN) และเครือข่ายระยะไกล (WAN) เราเตอร์จะมีโครงสร้างมาตรฐานชนิดหนึ่ง (Routing Protocol) ที่แลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับค่า Network Address ให้แก่กัน ทำให้เราเตอร์หนึ่งๆ สามารถเรียนรู้ Network Address ใดๆ ของระบบทั้งหมดได้ ซึ่งช่วยให้การส่งเฟรมข้อมูลไปยังปลายทางได้อย่างถูกต้องนั่นเอง นอกจากโครงสร้างของมาตรฐานเราติงโปรโตคอลที่ใช้เรียนรู้ตำแหน่งของค่า Network แล้วนั้น ยังสามารถที่จะทำฟังก์ชันการทำงานในด้านอื่นๆ เช่น การหาเส้นทางสำรองหรือเส้นทางใหม่ (Rerouting) เมื่อเส้นทางหลักมีปัญหาสามารถส่งผ่านเฟรมข้อมูลนั้นได้ดียิ่งขึ้น หรือการแยกแยะคุณสมบัติของเส้นทางของเฟรมข้อมูลที่จะส่งผ่านว่า เส้นทางใดเหมาะสมและดีที่สุดเป็นต้น ดังนั้นในปัจจุบันจึงทำให้ในส่วนของมาตรฐานเราติงโปรโตคอลมีมากมายหลายชนิด ซึ่งสามารถแบ่งตามกลุ่มของระบบเครือข่ายได้ดังนี้ [6-7]

5.4.1 Interior Routing Protocol

เป็นกลุ่มมาตรฐานเราติงโปรโตคอลที่ใช้สำหรับระบบเครือข่ายท้องถิ่น (LAN) หรือเรียกว่า Interior Gateway Protocol (IGP) ซึ่งโดยรวมแล้วจะมีระบบการติดต่อสื่อสารกันระหว่างเราเตอร์ ซึ่งจะช่วยให้สามารถเรียนรู้การเปลี่ยนแปลงต่างๆ ของระบบเครือข่ายได้อย่างรวดเร็ว สำหรับการสื่อสารข้อมูลในกลุ่มของระบบเครือข่ายท้องถิ่น ซึ่งลักษณะการเชื่อมต่อและการทำงานของกลุ่มระบบเครือข่ายท้องถิ่นต่างๆ นั้นจะมีความคล้ายคลึงกันคือ

1. เส้นทางที่เชื่อมต่อระหว่างกลุ่มเครื่องคอมพิวเตอร์ต่างๆ ในระบบเครือข่ายนั้น จะมีเป็นจำนวนมาก ซึ่งเป็นลักษณะคล้ายเส้นใยแมงมุม (Mesh Topology)
2. การเปลี่ยนแปลงของระบบเครือข่าย ในส่วนของเส้นทางการเชื่อมต่อต่างๆ จะมีอัตราการเปลี่ยนแปลงที่สูงมาก คือจะมีการเพิ่มหรือลดการเชื่อมต่อระบบเครือข่ายอยู่ตลอดเวลา
3. ความเร็วของระบบที่ใช้ ส่วนใหญ่จะมีความเร็วสูงมาก เช่น ระบบ Token Ring มีความเร็วในการส่งผ่านข้อมูลได้สูงสุด 16 Mbps ระบบอีเทอร์เน็ตมีความเร็ว 10 Mbps หรือระบบ Fast Ethernet สามารถส่งผ่านข้อมูลได้สูงถึง 100 Mbps เป็นต้น
4. ค่าใช้จ่ายในการติดตั้งสำหรับเชื่อมต่อเส้นทางต่างๆ ในระบบเครือข่ายท้องถิ่นจะมีราคาต่ำสามารถที่จะเพิ่มได้ง่าย

ดังนั้นฟังก์ชันเราติงโปรโตคอลในระบบ IGP จะมีโครงสร้างการทำงาน ที่สามารถรองรับลักษณะของระบบเครือข่ายท้องถิ่นได้เป็นอย่างดี ซึ่งในปัจจุบันระบบ Routing IGP ได้มีมาตรฐานที่พัฒนานำมาใช้งานกัน ค่อนข้างจะหลากหลายมาตรฐาน ได้แก่

5.4.1.1 Routing Information Protocol (RIP)

RIP เป็นโปรโตคอลที่ไม่มีความซับซ้อน สามารถทำการ Config ได้ง่ายมีข้อแตกต่างจากโปรโตคอลอื่นที่ใช้วิธีเดียวกันในหลายๆ ด้าน เช่น ชนิดของ Metric , โครงสร้างของ Address และจำนวนการเชื่อมต่อที่สามารถรับได้เป็นต้น โดยทั่วไปแล้ว RIP จะใช้ Address ที่เป็น Internet Address และใช้ Hop Count เป็น Metric สำหรับใช้ในการหาเส้นทางของเราเตอร์และ RIP สามารถสนับสนุนทั้งการเชื่อมต่อที่เป็นแบบจุดต่อจุด (Point-to-Point Links) และแบบกระจายทั้งเครือข่าย (Broadcast networks) โดยแพกเก็ตของ RIP ที่จะทำการส่งไปยังเราเตอร์ตัวอื่นนั้นจะถูกส่งไปโดยใช้ UDP และ IP ในการส่ง โดยข้อมูลในแพกเก็ตก็คือค่าของ Routing Table นั่นเอง RIP จะมีการทำการส่งแพกเก็ตทุกๆ 30 วินาที หรือเมื่อมีการ เปลี่ยนแปลงค่าใน Routing Table โปรโตคอล RIP จะเหมาะสมสำหรับเครือข่ายที่ไม่มีขนาดใหญ่มากนัก เนื่องจาก RIP จะกำหนดขนาดของ Hop Count ไว้ที่ 16 และ RIP ค่อนข้างจะสนใจ Cost ที่เป็น Real Time ดังนั้นการที่จะนำ RIP ไปใช้กับเครือข่ายขนาดใหญ่ๆ นั้น จึงค่อนข้างจะลำบากแต่ในปัจจุบันก็มีโปรโตคอลที่มีความเหมาะสมสำหรับเครือข่ายขนาดใหญ่ๆ มากกว่า RIP เช่น RIP II , OSPF เป็นต้น

5.4.1.2 Open Shortest Path First (OSPF)

เมื่อปี ค.ศ. 1978 กลุ่มวิศวกรของสถาบัน IETF (Internet Engineering Task Force) ได้พัฒนาระบบเครือข่ายสากลบนพื้นฐานโปรโตคอล TCP/IP ขึ้นมา ซึ่งเดิมชื่อว่าระบบ ARPAnet และต่อมาเปลี่ยนชื่อเป็นระบบเครือข่ายอินเตอร์เน็ต ซึ่งเป็นระบบเครือข่ายที่มีความคล่องตัวเป็นอย่างสูง โดยจะเห็นได้จากทุกวันนี้มีการใช้งานอย่างแพร่หลายมาก กลุ่มวิศวกร IETF ที่ได้พัฒนาระบบมาตรฐานเราติงโปรโตคอลขึ้นมาใหม่ เพื่อรองรับระบบเครือข่ายอินเตอร์เน็ตใหม่ที่เรียกว่ามาตรฐาน OSPF ซึ่งมีค่าพารามิเตอร์ต่างๆ มากขึ้นและมีความยืดหยุ่นคล่องตัวมากกว่ามาตรฐาน RIP เป็นอย่างมาก ดังนั้นในระบบเครือข่ายขนาดใหญ่ ไม่ว่าจะเป็นเครือข่ายมหาวิทยาลัยหรือหน่วยงานต่างๆ จะใช้มาตรฐาน OSPF สำหรับออกแบบระบบเราเตอร์เสมอ โดย OSPF จะมีความพิเศษคือ

1. สามารถแยกระหว่างโฮสกับเราเตอร์ได้
2. สนับสนุนการทำงานของ Broadcast Networks เช่นอีเทอร์เน็ต หรือ FDDI
3. สนับสนุนการทำงานของ Nonbroadcast Networks เช่น X.25 หรือ ATM
4. สามารถแบ่งเครือข่ายขนาดใหญ่ๆ เป็น Area ย่อยๆ ได้ นั่นคือถ้ามีเครือข่ายขนาดใหญ่ๆ อยู่จะต้องทำการแบ่งเครือข่ายนั้นให้เป็น Area ย่อยๆ โดย Area ย่อยทุก Area จะมีหมายเลขประจำ Area โดย Area หมายเลข 0 จะทำหน้าที่เป็น Backbone และ Area อื่นๆ จะไม่สามารถเชื่อมต่อกันโดยตรงได้แต่ทุก Area จะต้องทำการเชื่อมต่อเข้ากับ Area 0

5.4.1.3 Interior Gateway Routing Protocol (IGRP)

เมื่อระบบเครือข่ายของเอกชนต่างๆ (Private Network) ที่ใช้พื้นฐานของมาตรฐาน TCP/IP ได้มีขนาดใหญ่เกินกว่ามาตรฐาน RIP ที่จะรองรับได้ บริษัท Cisco System ก็ได้พัฒนาระบบเราติงโปรโตคอลที่ใช้กันภายในเครือข่ายท้องถิ่น ซึ่งมีชื่อเรียกว่า IGRP และปรากฏว่าระบบเราติงโปรโตคอลชนิดนี้ ได้เป็นที่นิยมกันมาก ทั้งนี้เพราะว่าระบบ IGRP ถูกออกแบบให้มีค่าพารามิเตอร์หลายอย่างเช่นเดียวกับระบบ OSPF จึงสามารถรองรับระบบเครือข่าย TCP/IP ขนาดใหญ่ได้ดี

5.4.2 Exterior Routing Protocol

เป็นกลุ่มมาตรฐานที่ออกแบบสำหรับการติดต่อสื่อสารระหว่างเราเตอร์ที่ใช้เชื่อมต่อกลุ่มเครือข่าย (Autonomous System) ในระบบเครือข่ายระยะไกล (WAN) โดยกลุ่มมาตรฐานนี้จะแตกต่างจาก IGP ตรงที่ความถี่หรือชนิดของข้อมูลที่สื่อสารกันของเราเตอร์นั้นจะน้อยกว่า ส่วนใหญ่จะเป็นข้อมูลสรุปของกลุ่มเครือข่าย แล้วส่งไปยังเราเตอร์อีกฝั่งหนึ่ง มีลักษณะที่สำคัญดังนี้

1. เส้นทางในการเชื่อมต่อ ส่วนใหญ่จะเป็นลักษณะจุดต่อจุด (Point-to-Point Topology) ไม่ได้มีเส้นทางหลายๆเส้นทางสลับซับซ้อนเหมือนการเชื่อมต่อภายในระบบเครือข่ายท้องถิ่น
2. การเปลี่ยนแปลงของเส้นทางที่เชื่อมต่อค่อนข้างจะมีอัตราการเปลี่ยนแปลงที่น้อยมาก เมื่อเทียบกับการเชื่อมต่อภายในกลุ่มระบบเครือข่ายท้องถิ่นด้วยกัน
3. ความเร็วในการส่งผ่านข้อมูลระหว่างกลุ่มเครือข่าย ส่วนใหญ่จะมีอัตราความเร็วที่ต่ำกว่า เมื่อเทียบกับความเร็วของระบบเครือข่ายท้องถิ่น โดยอัตราความเร็วในการส่งผ่านข้อมูลจะอยู่ในย่านตั้งแต่ 9600 bps – 2 Mbps ทั้งนี้ก็ขึ้นอยู่กับระบบโทรคมนาคมที่มีให้บริการ
4. ค่าใช้จ่ายในการติดตั้งเส้นทางที่ต่อเชื่อมระหว่างกลุ่มเครือข่ายท้องถิ่น ค่อนข้างจะมีราคาที่สูง และมีความยุ่งยาก

ในปัจจุบันมาตรฐานที่อยู่ในกลุ่มนี้และเป็นที่นิยมกันมีด้วยกัน 2 ชนิดคือ

5.4.2.1 Exterior Gateway Protocol (EGP)

เป็นมาตรฐานแรกที่ออกแบบใช้งานในระบบเครือข่าย Internet แต่เนื่องจากมาตรฐานนี้ ใช้ค่าพารามิเตอร์เพียงพื้นฐานเท่านั้น จึงทำให้ขาดความคล่องตัวเป็นอย่างมาก และต่อมามีการพัฒนาเป็นมาตรฐานอื่นที่เรียกว่า BGP

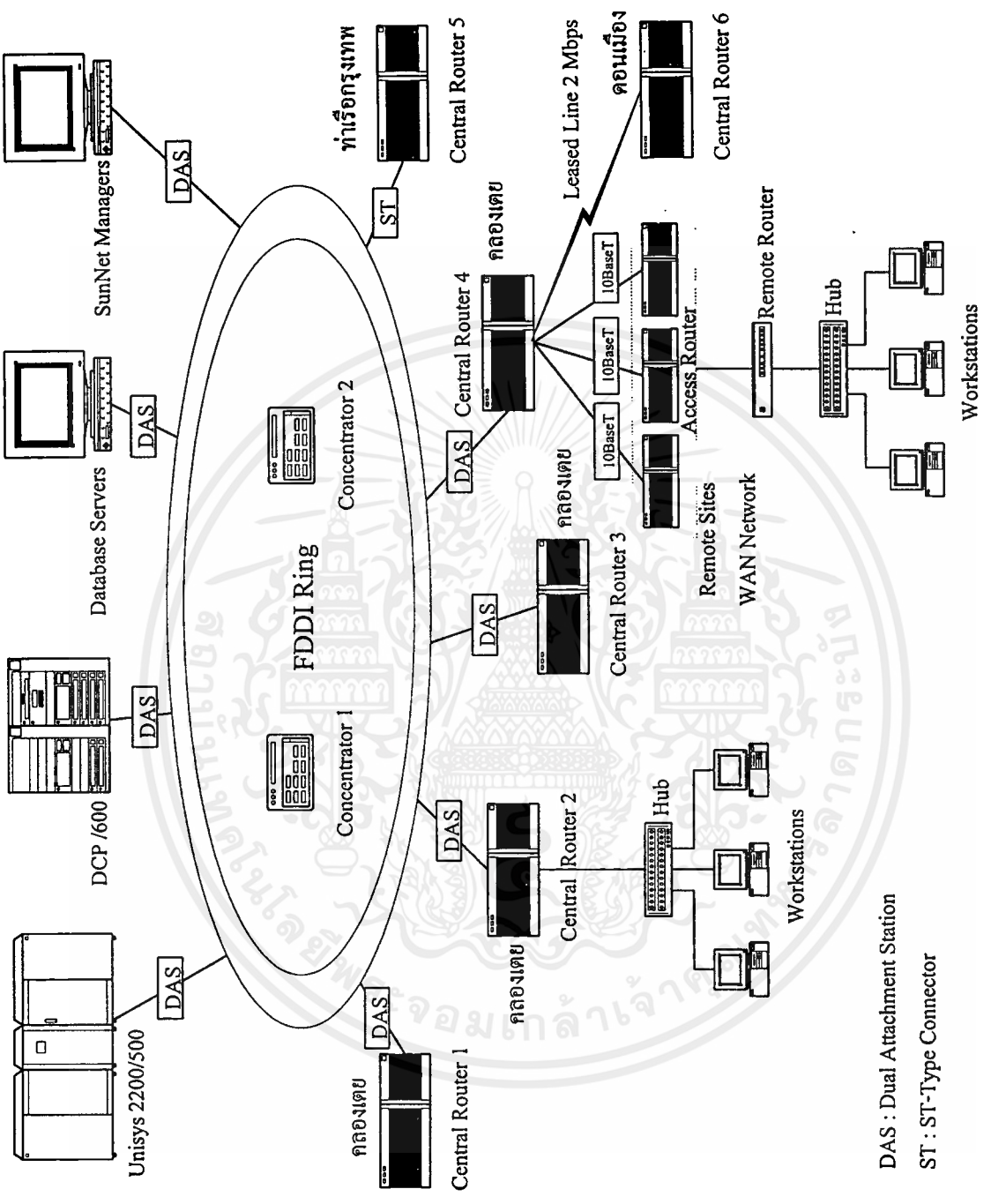
5.4.2.2 Border Gateway Protocol (BGP)

เป็นมาตรฐานที่ใช้พัฒนาจากระบบ EGP ซึ่งได้แก้ไขจุดบกพร่องต่างๆ ของ EGP เช่น สามารถต่อระบบเครือข่าย โดยรวมในลักษณะวนลูปได้ เป็นต้น ทำให้การเชื่อมต่อระหว่างกลุ่มเครือข่ายต่างๆ มีความคล่องตัวมาก ระบบเครือข่ายอินเตอร์เน็ตในปัจจุบันจะใช้มาตรฐานนี้ เพื่อใช้ช่วยเชื่อมต่อกลุ่มเครือข่ายต่างๆ ทั่วโลกเข้าด้วยกัน และล่าสุดมาตรฐานนี้ได้พัฒนาใน Version 4 หรือเรียกว่า BGP4

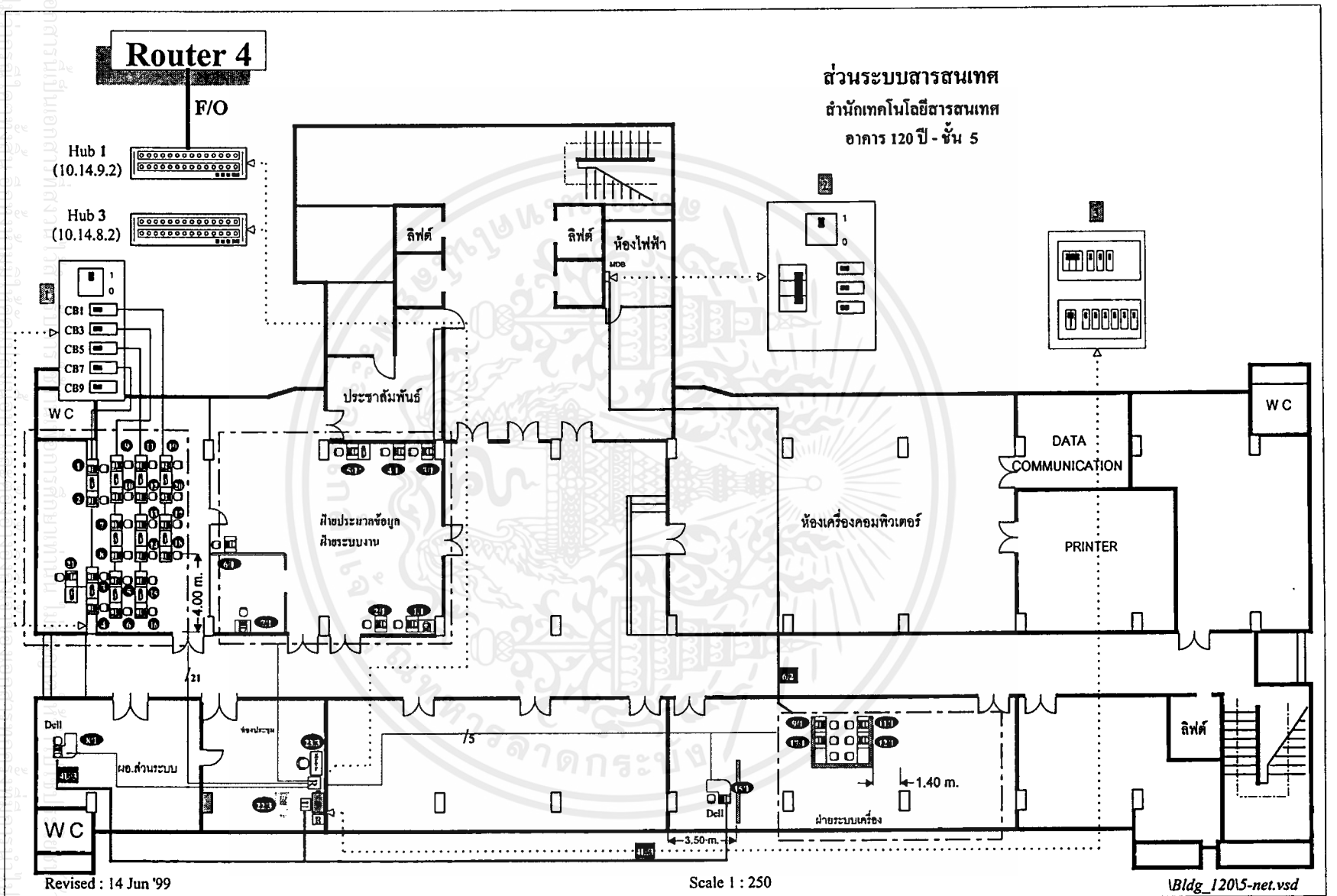
บทที่ 6
การติดตั้งระบบเครือข่ายคอมพิวเตอร์กรมศุลกากร

การออกแบบติดตั้งระบบเครือข่ายคอมพิวเตอร์ของกรมศุลกากร ระบบที่ออกแบบจะใช้มาตรฐานของ International Standards Organization (ISO) สำหรับ Open System Interconnection (OSI) Model ระบบเครือข่ายที่ใช้ทั้งภายในกรมศุลกากร และการเชื่อมต่อระบบกับหน่วยงานของกรมศุลกากรที่อยู่ภายนอกกรม รวมถึงด่านศุลกากรต่างๆ ทั่วประเทศ จะใช้มาตรฐานของอีเทอร์เน็ต ใช้ทีซีพี/ไอพีเป็นโปรโตคอลในการติดต่อสื่อสารข้อมูลของระบบเครือข่าย และใช้ระบบ FDDI เป็น Backbone ขั้นตอนในการติดตั้งระบบเครือข่ายคอมพิวเตอร์ของกรมศุลกากร สามารถแบ่งออกได้เป็น 2 ส่วนใหญ่ๆ คือ การติดตั้งตามหน่วยงานต่างๆ ภายในกรมศุลกากรและบริเวณใกล้เคียง และการติดตั้งตามหน่วยงานต่างๆ ภายนอกกรมศุลกากรรวมถึงด่านศุลกากรตามภูมิภาคต่างๆ ทั่วประเทศ จากรูปที่ 6.1 แสดงการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ภายในศูนย์คอมพิวเตอร์ประมวลผลหลัก ซึ่งใช้เป็นศูนย์กลางในการควบคุมการประมวลผลของระบบ การติดตั้ง Backbone ของระบบเครือข่ายใช้แบบ FDDI มีการเชื่อมต่อทางฟิสิคอลเป็นแบบสตาร์โทโปโลยี ส่วนการเชื่อมต่อทางโลจิคอล จะต่อโทโปโลยีแบบดูออลริง ความเร็วที่ใช้ในการรับส่งข้อมูลระหว่างเซนทอลเราเตอร์กับ FDDI Backbone มีค่าเท่ากับ 100 Mbps

ขั้นตอนในการติดตั้งเครื่องคอมพิวเตอร์ อุปกรณ์เชื่อมต่อระบบเครือข่ายและระบบงาน จะแบ่งออกเป็นหลายช่วงของการติดตั้ง ในการจัดสรรจำนวนเครื่องให้กับหน่วยงานต่างๆ จะมีการประชุมกันระหว่างสำนักเทคโนโลยีสารสนเทศ หน่วยงานต่างๆ ของกรมศุลกากรที่มีส่วนเกี่ยวข้อง ทีมงานพัฒนาระบบงาน ทีมงานติดตั้งระบบเครือข่าย และทีมงานที่ปรึกษา หลังจากได้ข้อสรุปแล้ว ทีมงานติดตั้งระบบเครือข่ายจึงทำการสำรวจสถานที่ ติดตั้งระบบไฟฟ้า ระบบสัญญาณสื่อสาร สำหรับเครื่องคอมพิวเตอร์ให้กับหน่วยงานนั้นๆ ดังแสดงตัวอย่างตามรูปที่ 6.2 เมื่อติดตั้งเครื่องเรียบร้อยแล้ว ทีมพัฒนาระบบงานจะทำการทดสอบระบบงานและใช้งานจริงตามที่ได้จัดเตรียมไว้ และจะดำเนินลักษณะงานตามลักษณะนี้จนกระทั่งจบโครงการ



รูปที่ 6.1 แสดงส่วนประกอบคอมพิวเตอร์หลักของระบบเครือข่าย

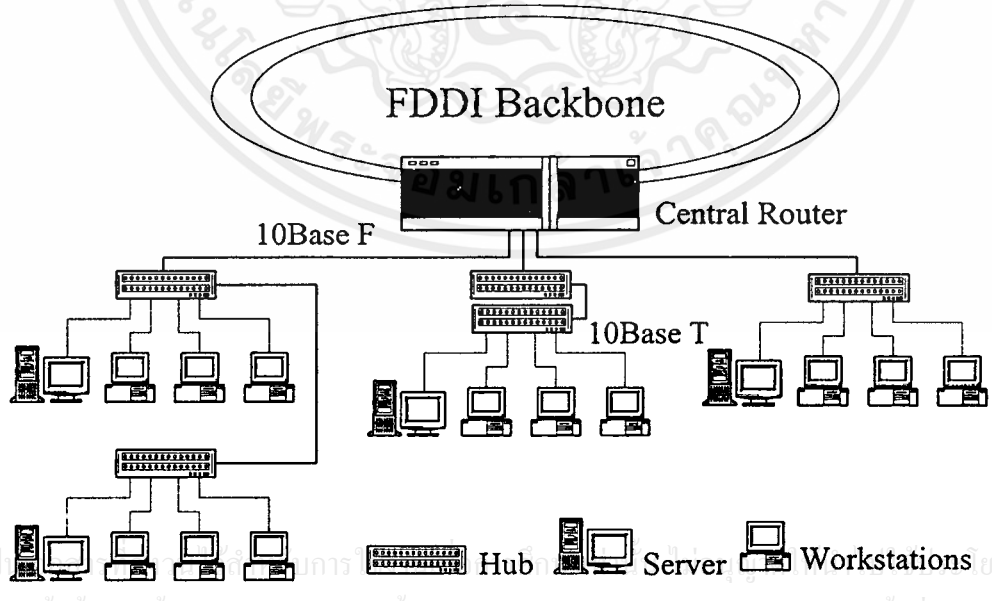


รูปที่ 6.2 แสดงแบบที่ได้จากการสำรวจตำแหน่งติดตั้งระบบเครือข่ายคอมพิวเตอร์

6.1 การติดตั้งระบบเครือข่ายคอมพิวเตอร์ตามหน่วยงานต่างๆ ภายในกรมศุลกากรและบริเวณใกล้เคียง

ภายในกรมศุลกากรคลองเตย จะมีอาคารอยู่หลายอาคาร ซึ่งใช้เป็นที่ปฏิบัติงานของหน่วยงานต่างๆ อาคารที่มีการติดตั้งเครื่องคอมพิวเตอร์เป็นจำนวนมาก จะมีการติดตั้งเซนทอลเราเตอร์ ไว้สำหรับให้บริการในการติดต่อกับเครือข่ายที่อาคารนั้นๆ ส่วนอาคารที่มีจำนวนของเครื่องคอมพิวเตอร์ไม่มาก จะมีการติดตั้งเซนทอลเราเตอร์ ไว้ในตำแหน่งที่เหมาะสมและใช้งานร่วมกัน แต่ละหน่วยงานจะมีการต่อระบบเครือข่ายคอมพิวเตอร์เป็นแลนวงย่อยๆ ซึ่งจะประกอบไปด้วยเซิฟเวอร์และเวิคสเตชัน ทั้งเซิฟเวอร์และเวิคสเตชัน จะต่อเข้ากับ Hub ด้วยมาตรฐานอีเทอร์เน็ต 10BaseT และจาก Hub จะต่อเข้ากับเซนทอลเราเตอร์ ด้วยมาตรฐาน 10BaseF ดังแสดงไว้ตามรูปที่ 6.3

ในส่วนของกรมศุลกากรในบริเวณการท่าเรือแห่งประเทศไทยได้ทำการติดตั้งเซนทอลเราเตอร์ไว้หนึ่งตัวสำหรับไว้ให้บริการตามหน่วยงานต่างๆ และการเชื่อมต่อระบบเครือข่ายจากเซนทอลเราเตอร์ จะเชื่อมต่อกับระบบ FDDI Backbone เข้ามาที่กรมศุลกากรคลองเตยโดยตรง สำหรับกรมศุลกากรดอนเมือง ตามหน่วยงานต่างๆ ก็จะมีการต่อระบบเครือข่ายเป็นแลน วงย่อยๆ เหมือนกัน และระบบเครือข่าย ที่กรมศุลกากรดอนเมืองสามารถเชื่อมต่อเข้ากับระบบเครือข่าย ที่กรมศุลกากรคลองเตย โดยการเชื่อมต่อเซนทอลเราเตอร์ ของทั้งสองด้านผ่านสายสัญญาณ Leased line ขององค์การโทรศัพท์แห่งประเทศไทย ด้วยความเร็ว 2 Mbps



รูปที่ 6.3 แสดงการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ภายในบริเวณกรมศุลกากร

6.1.1 ระบบเครือข่ายคอมพิวเตอร์ของเซนทอลเราเตอร์ 1

ที่อาคาร 1 ได้ทำการติดตั้งเซนทอลเราเตอร์ไว้ 2 ตัว ซึ่งเซนทอลเราเตอร์ 1 จะเป็นเราเตอร์ที่ให้บริการกับหน่วยงานต่างๆ ที่บริเวณอาคาร 1 ทั้งหมด สำหรับติดต่อกับระบบเครือข่าย และที่อาคาร 1 นี้ระบบเครือข่ายประกอบไปด้วย

Network Equipment

Central Router	1	(Central Router 1)
Cabletron SEHI-22 Hub	5	
Cabletron SEHI-24 Hub	6	
Cabletron EPIM-F2	11	(10BaseFl module – 1 per Hub)

Central Router 1 Capacity

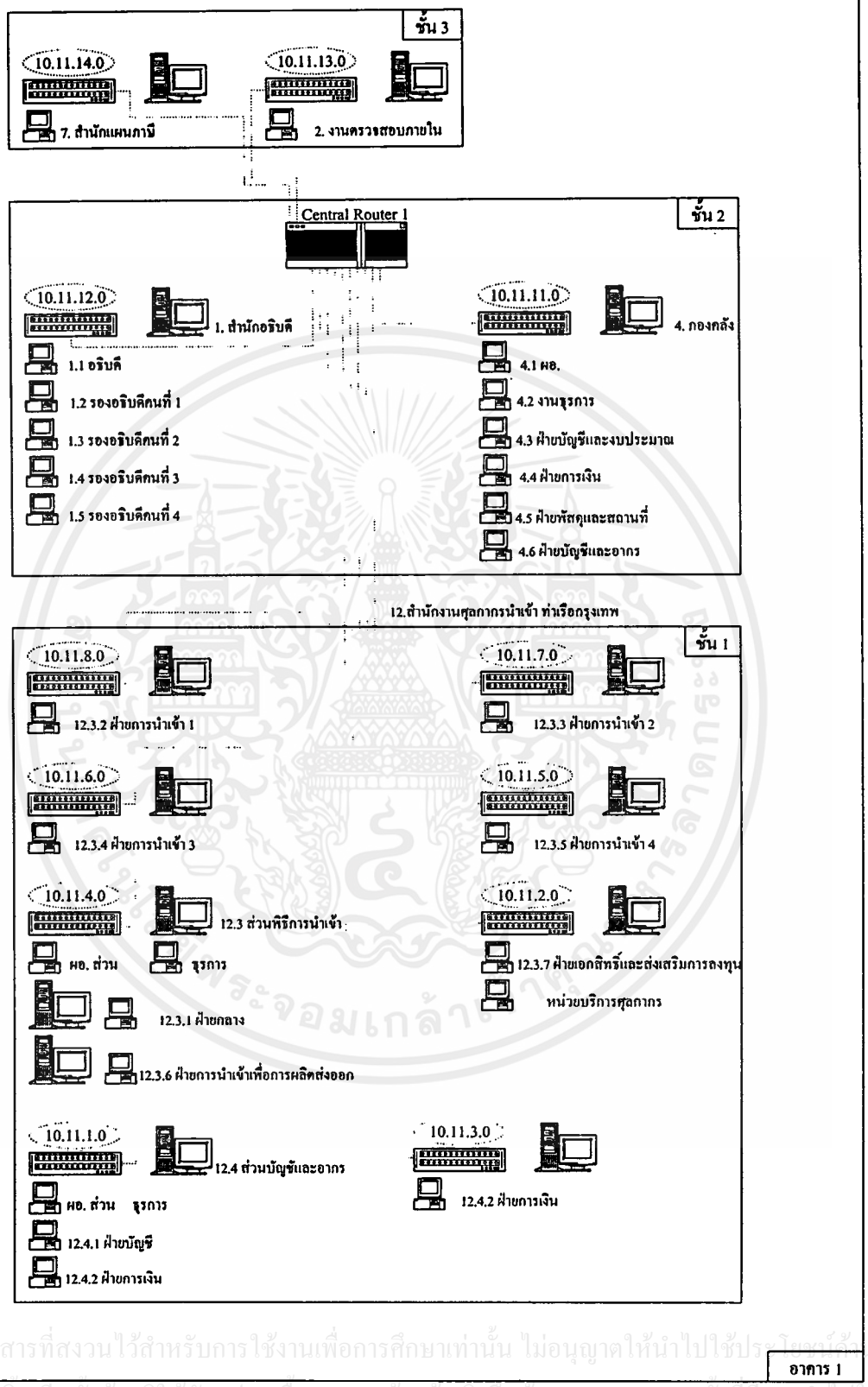
FDDI Ports	1	(Used)
Ethernet Ports (AUI)	14	(Used 11)
Cabletron FOT-F24	14	(10BaseFl module for router)
Serial Ports	4	(No plan to use)
Spare Interface Card Slots	0	

Racks

15U	3
27U	3
39U	1

Server (SUN Sparc)

Small Server	2
Medium Server	5
Large Server	6



รูปที่ 6.4 แสดงการเชื่อมต่อระบบเครือข่ายของเซนทอลเราเตอร์ 1

6.1.2 ระบบเครือข่ายคอมพิวเตอร์ของเซนทอลเราเตอร์ 2

เซนทอลเราเตอร์ 2 ได้ทำการติดตั้งอยู่ที่บริเวณอาคาร 1 เป็นเราเตอร์ที่ทำหน้าที่ให้บริการหน่วยงานต่างๆ ที่อาคาร 2,3,4,6,8,9 และ19 ในส่วนของเครื่องคอมพิวเตอร์ที่อาคาร 8 จะเชื่อมต่อเข้ากับ hub ที่อาคาร 9 โดยใช้สายยูทีพี และเครื่องคอมพิวเตอร์ที่อาคาร 19 จะเชื่อมต่อเข้ากับ hub ที่อาคาร 6 โดยใช้สายยูทีพีเช่นกัน เนื่องจากทั้ง 2 อาคารนี้มีจำนวนเครื่องที่ติดตั้งน้อย จึงไม่ได้ติดตั้งจุดเชื่อมต่อ Optic Fiber ไว้ ระบบเครือข่ายที่เชื่อมต่อกับเซนทอลเราเตอร์ 2 ประกอบไปด้วย

Network Equipment

Central Router	1	(Central Router 2)
Cabletron SEHI-22 Hub	8	
Cabletron SEHI-24 Hub	3	
Cabletron EPIM-F2	9	(10BaseFl module – 1 per Hub)

Central Router 2 Capacity

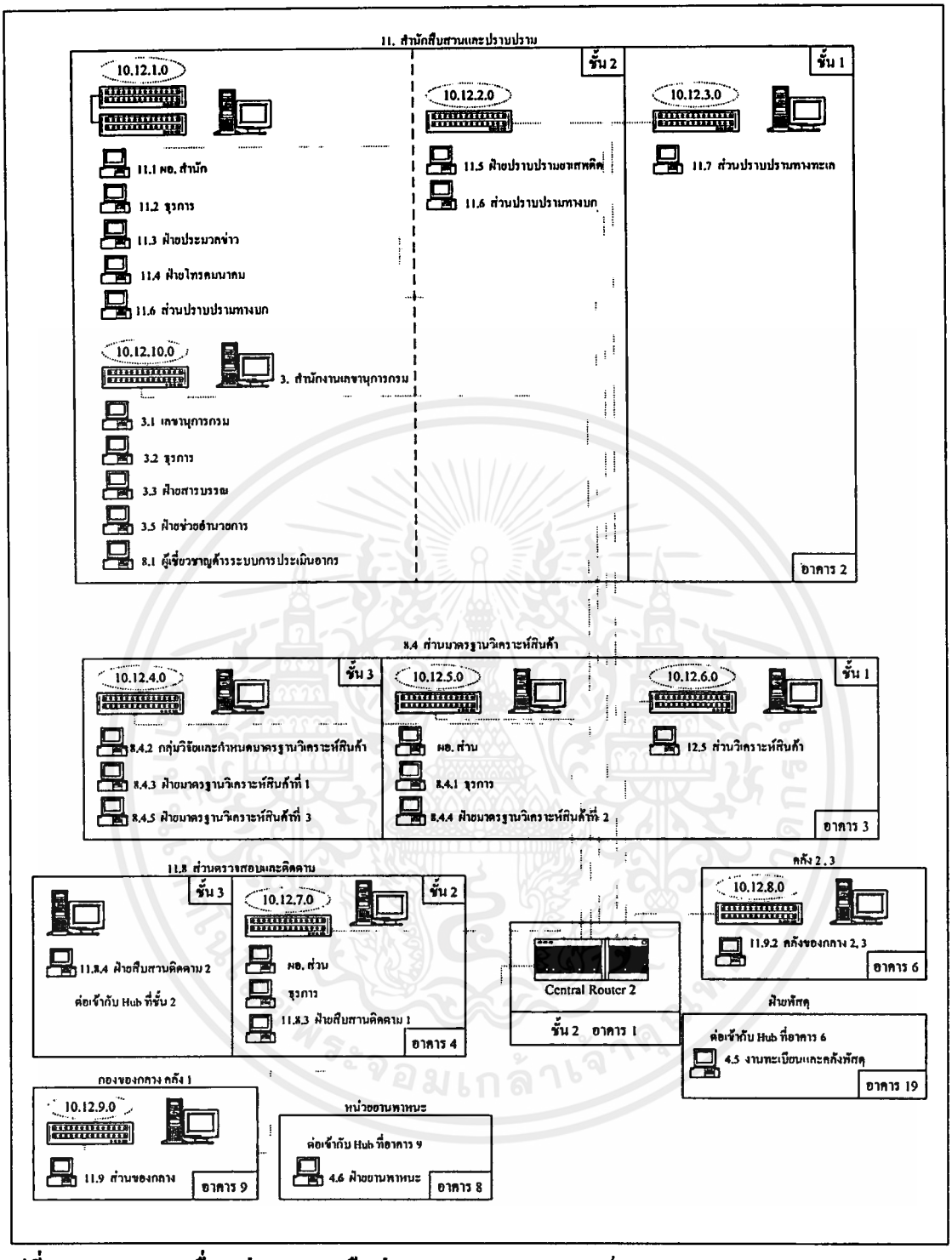
FDDI Ports	1	(Used)
Ethernet Ports (AUI)	14	(Used 9)
Cabletron FOT-F24	13	(Take 1 from CR4, = 14)
Serial Ports	4	(No plan to use)
Spare Interface Card Slots	0	

Racks

15U	8

Server (SUN Sparc)

Small Server	3
Medium Server	6



รูปที่ 6.5 แสดงการเชื่อมต่อระบบเครือข่ายของเซนทอลเราเตอร์ 2

6.1.3 ระบบเครือข่ายคอมพิวเตอร์ของเซนทอลเราเตอร์ 3

เซนทอลเราเตอร์ 3 ได้ทำการติดตั้งอยู่ที่ศูนย์คอมพิวเตอร์หลักบริเวณอาคาร 120 ปี เป็นเราเตอร์ที่ทำหน้าที่ให้บริการหน่วยงานต่างๆ ของอาคาร 120 ปี ทุกชั้น ในแต่ละชั้นจะมีจุดเชื่อมต่อ Optic Fiber เพื่อให้ hub ต่อเข้ามาที่เซนทอลเราเตอร์ ระบบเครือข่ายที่เชื่อมต่อกับเซนทอลเราเตอร์ 3 ประกอบไปด้วย

Network Equipment

Central Router	1	(Central Router 3)
Cabletron SEHI-22 Hub	9	
Cabletron SEHI-24 Hub	8	
Cabletron EPIM-F2	16	(10BaseFl module – 1 per Hub)

Central Router 3 Capacity

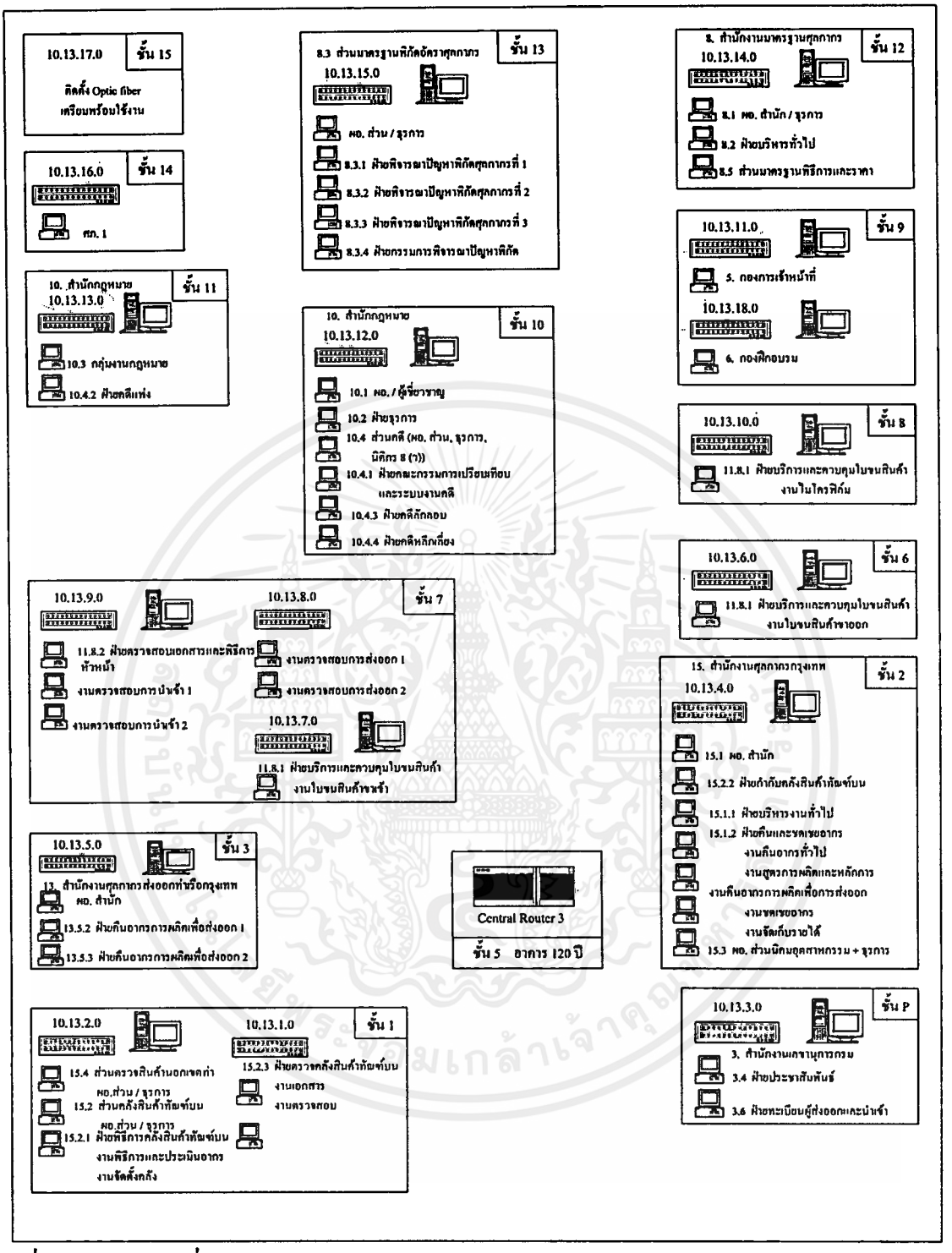
FDDI Ports	1	(Used)
Ethernet Ports (AUI)	18	(Used 17 + 1 for 15th floor)
Cabletron FOT-F24	15	(Take 3 from CR4, = 18)
Serial Ports	4	(No plan to use)
Spare Interface Card Slots	0	

Racks

15U	13

Server (SUN Sparc)

Small Server	3
Medium Server	9
Large Server	3

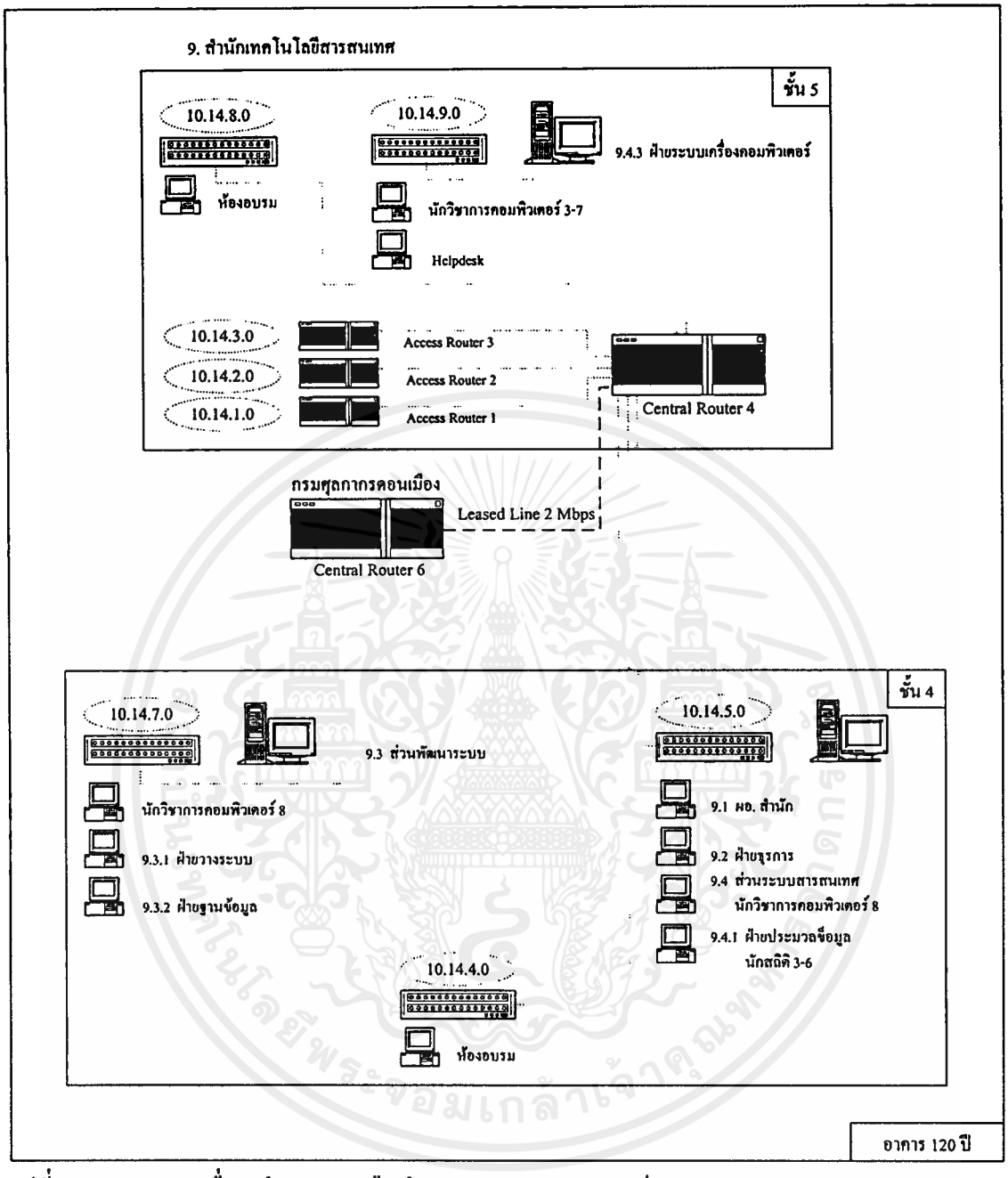


รูปที่ 6.6 แสดงการเชื่อมต่อระบบเครือข่ายของเซนทอลเราเตอร์ 3

6.1.4 ระบบเครือข่ายคอมพิวเตอร์ของเซนทอลเราเตอร์ 4

เซนทอลเราเตอร์ 4 ได้ทำการติดตั้งอยู่ที่ศูนย์คอมพิวเตอร์หลักบริเวณอาคาร 120 ปี เป็นเราเตอร์ที่ทำหน้าที่ให้บริการหน่วยงานต่างๆ ของอาคาร 120 ปี บริเวณชั้นที่ 4 และ 5 และทำหน้าที่เป็นเกทเวย์ให้กับด่านศุลกากรที่อยู่ภายนอกกรม รวมถึงด่านศุลกากรภูมิภาคต่างๆ ทั่วประเทศ โดยด่านต่างๆ เหล่านี้จะเชื่อมต่อกับแอคเซสเราเตอร์ที่ต่อกับเซนทอลเราเตอร์ 4 อีกทีหนึ่ง สำหรับการเชื่อมต่อจากกรมศุลกากรดอนเมือง ได้ทำการเชื่อมต่อจากเซนทอลเราเตอร์ 6 ที่กรมศุลกากรดอนเมืองเข้ากับเซนทอลเราเตอร์ 4 ที่คลองเตย โดยผ่านสายสัญญาณ Leased Line ขององค์การโทรศัพท์แห่งประเทศไทยด้วยความเร็ว 2 Mbps ระบบเครือข่ายที่เชื่อมต่อกับเซนทอลเราเตอร์ 4 ประกอบไปด้วย

Network Equipment		
Central Router	1	(Central Router 4)
Cabletron SEHI-22 Hub	1	
Cabletron SEHI-24 Hub	4	
Cabletron EPIM-F2	5	(10BaseFl module – 1 per Hub)
Access Router (Cisco 7010)	3	(In Computer Room Rack)
98098 10Base2 Transceivers	6	(Access Router to Central Router Connections)
Central Router 4 Capacity		
FDDI Ports	1	(Used)
Ethernet Ports (AUI)	10	(Used 7 Hubs, 3 Access Routers)
Cabletron FOT-F24	13	(Used 7, + 4 to other routers, = 11)
Serial Ports (High Speed)	2	(No plan to use)
Serial Ports (E1)	2	(Used 1 for Airport link)
Spare Interface Card Slots	1	
Racks		
15U	1	
27U	1	
39U	4	
Server (SUN Sparc)		
Large Server	3	



รูปที่ 6.7 แสดงการเชื่อมต่อระบบเครือข่ายของเซนทอลเราเตอร์ 4

6.1.5 ระบบเครือข่ายคอมพิวเตอร์ของเซนทอลเราเตอร์ 5

เซนทอลเราเตอร์ 5 ได้ทำการติดตั้งอยู่ที่ศูนย์เพิ่มประสิทธิภาพ ส่วนตรวจสินค้าขาเข้า กรมศุลกากร ในการท่าเรือแห่งประเทศไทย เป็นเราเตอร์ที่ให้บริการหน่วยงานต่างๆ ของกรมศุลกากรทั้งหมดในบริเวณการท่าเรือแห่งประเทศไทย สำหรับการเชื่อมต่อของเซนทอลเราเตอร์ 5 เข้ากับศูนย์คอมพิวเตอร์หลัก จะเชื่อมต่อโดยใช้ Optic Fiber ต่อกับ Backbone โดยตรง ระบบเครือข่ายที่เชื่อมต่อกับเซนทอลเราเตอร์ 5 ประกอบไปด้วย

Network Equipment

Central Router	1	(Central Router 5)
Cabletron SEHI-22 Hub	14	
Cabletron SEH-24 Hub	1	
Cabletron SEHI-24 Hub	6	
Cabletron Stack Cable	1	
Cabletron EPIM-F2	21	(10BaseFl module – 1 per Hub)
10BaseFl / 10Base2 Media Converter	5	

Central Router 5 Capacity

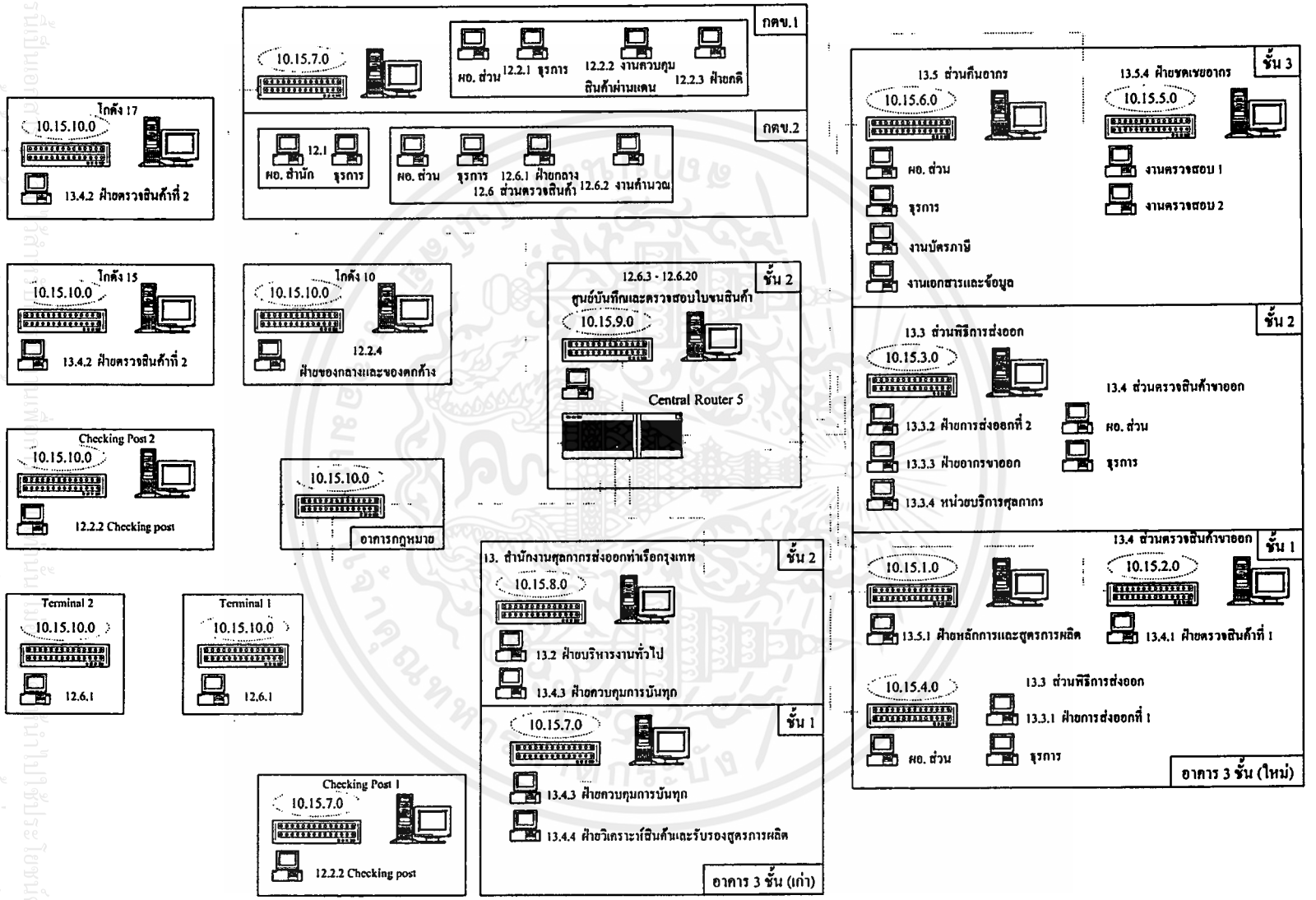
FDDI Ports	1	(Used)
Ethernet Ports (AUI)	10	(Used 10)
Cabletron FOT-F24	12	(Used 10)
Serial Ports	4	(No plans to use)
Spare Interface Card Slots	1	

Racks

15U	14
27U	1

Server (SUN Sparc)

Small Server	6
Medium Server	5
Large Server	4



รูปที่ 6.8 แสดงการเชื่อมต่อระบบเครือข่ายของเซนทอลเราเตอร์ 5 (บริเวณการท่าเรือแห่งประเทศไทย)

6.1.6 ระบบเครือข่ายคอมพิวเตอร์ของเซนทอลเราเตอร์ 6

เซนทอลเราเตอร์ 6 ได้ทำการติดตั้งอยู่ที่อาคารคลังสินค้า 2 ในการท่าอากาศยานกรุงเทพ (ดอนเมือง) เป็นเราเตอร์ที่ให้บริการหน่วยงานต่างๆ ของกรมศุลกากรทั้งหมดในบริเวณการท่าอากาศยานกรุงเทพ สำหรับการเชื่อมต่อของเซนทอลเราเตอร์ 6 เข้ากับศูนย์คอมพิวเตอร์หลัก จะเชื่อมต่อโดยใช้สายสัญญาณ Leased Line ขององค์การโทรศัพท์แห่งประเทศไทยด้วยความเร็ว 2 Mbps ต่อเข้ากับเซนทอลเราเตอร์ 4 ที่กรมศุลกากรคลองเตย ระบบเครือข่ายที่เชื่อมต่อกับเซนทอลเราเตอร์ 6 ประกอบไปด้วย

Network Equipment

Central Router	1	(Central Router 6)
Cabletron SEHI-22 Hub	21	
Cabletron SEH-24 Hub	4	
Cabletron SEHI-24 Hub	2	
Cabletron Stack Cable	4	
Cabletron EPIM-F2	22	(10BaseFl module – 1 per Hub)
UTP-Fiber Converter	8	

Central Router 6 Capacity

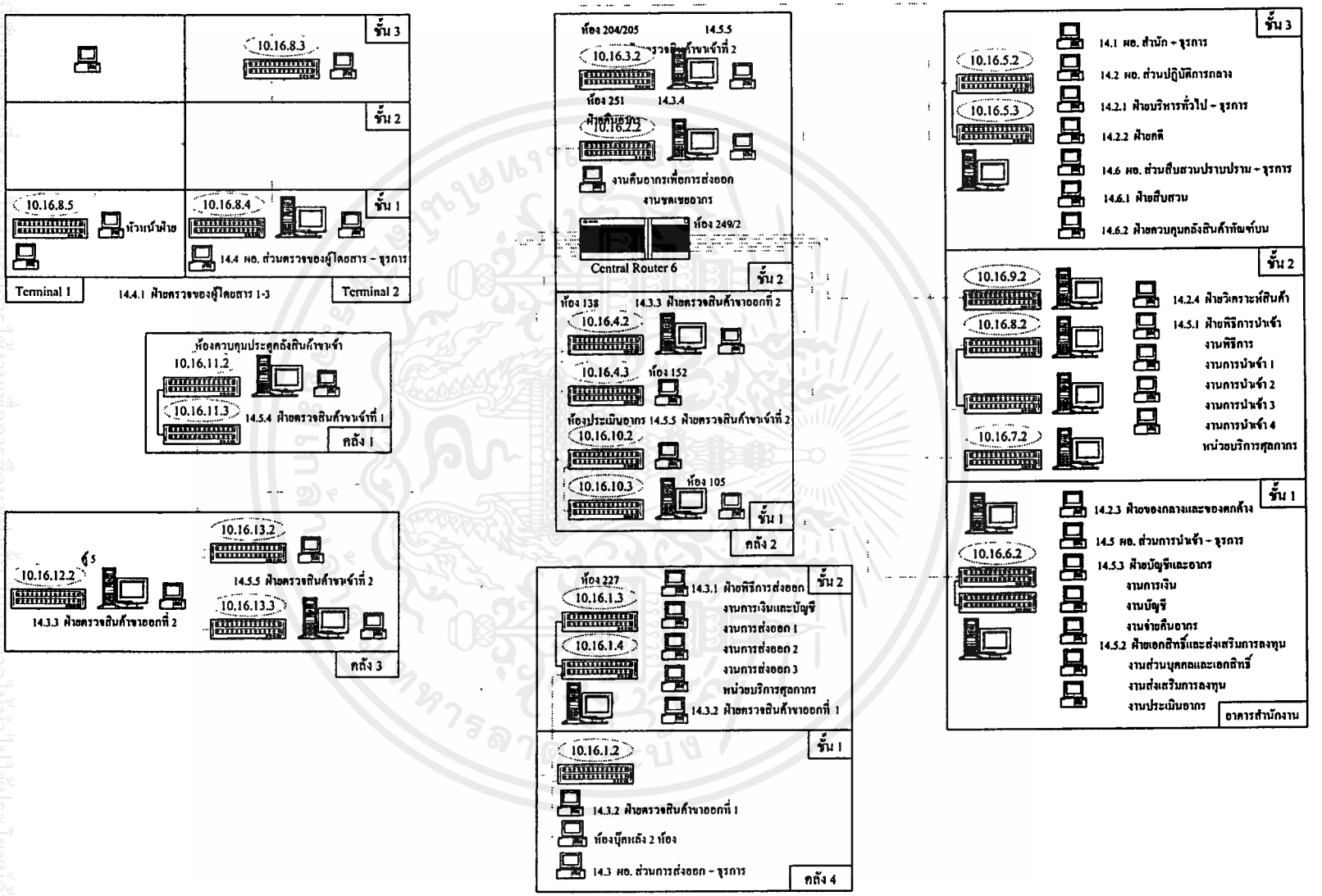
FDDI Ports	1	(Not Used)
Ethernet Ports (AUI)	12	(Used 12)
Cabletron FOT-F24	12	
Serial Ports (E1)	2	
Serial Ports	4	(Used 2)
Spare Interface Card Slots	1	

Racks

15U	16
27U	2

Server (SUN Sparc)

Small Server	6
Medium Server	10



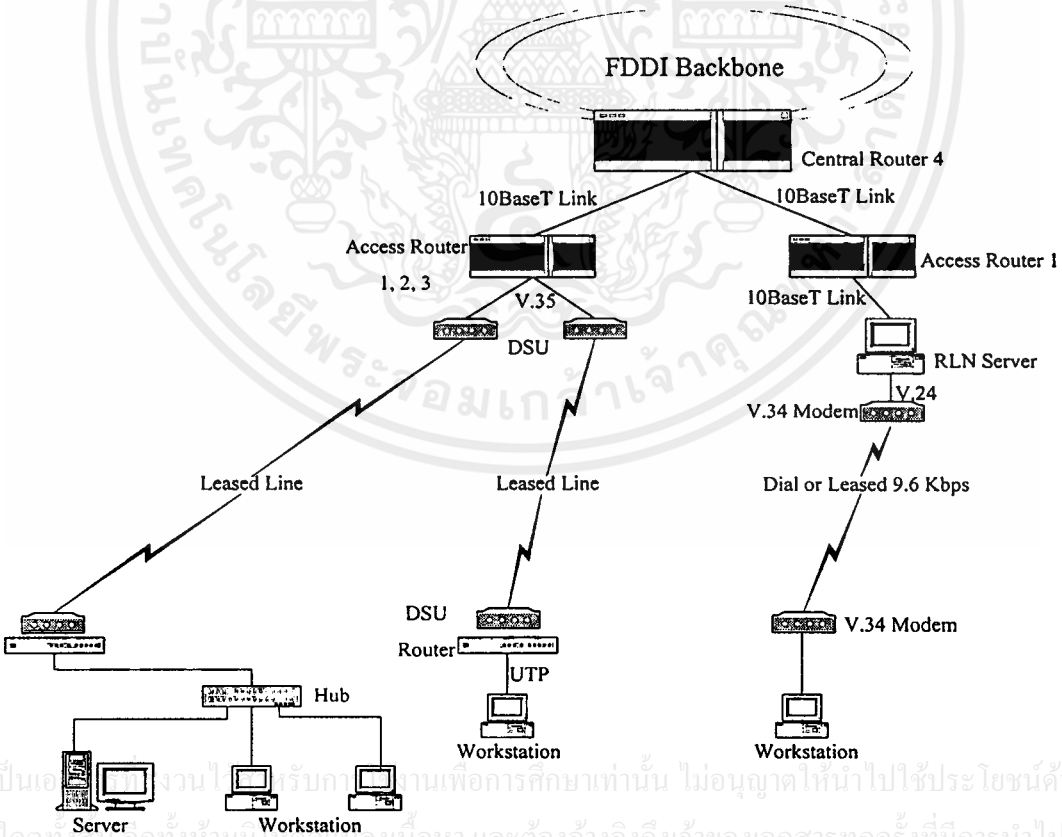
รูปที่ 6.9 แสดงการเชื่อมต่อระบบเครือข่ายของเซนทอลราเตอร์ 6 (บริเวณท่าอากาศยาน ดอนเมือง)

6.2 การติดตั้งระบบเครือข่ายคอมพิวเตอร์ตามหน่วยงานต่างๆ ภายนอกกรมศุลกากร และตามด่านศุลกากรภูมิภาคต่างๆ ทั่วประเทศ

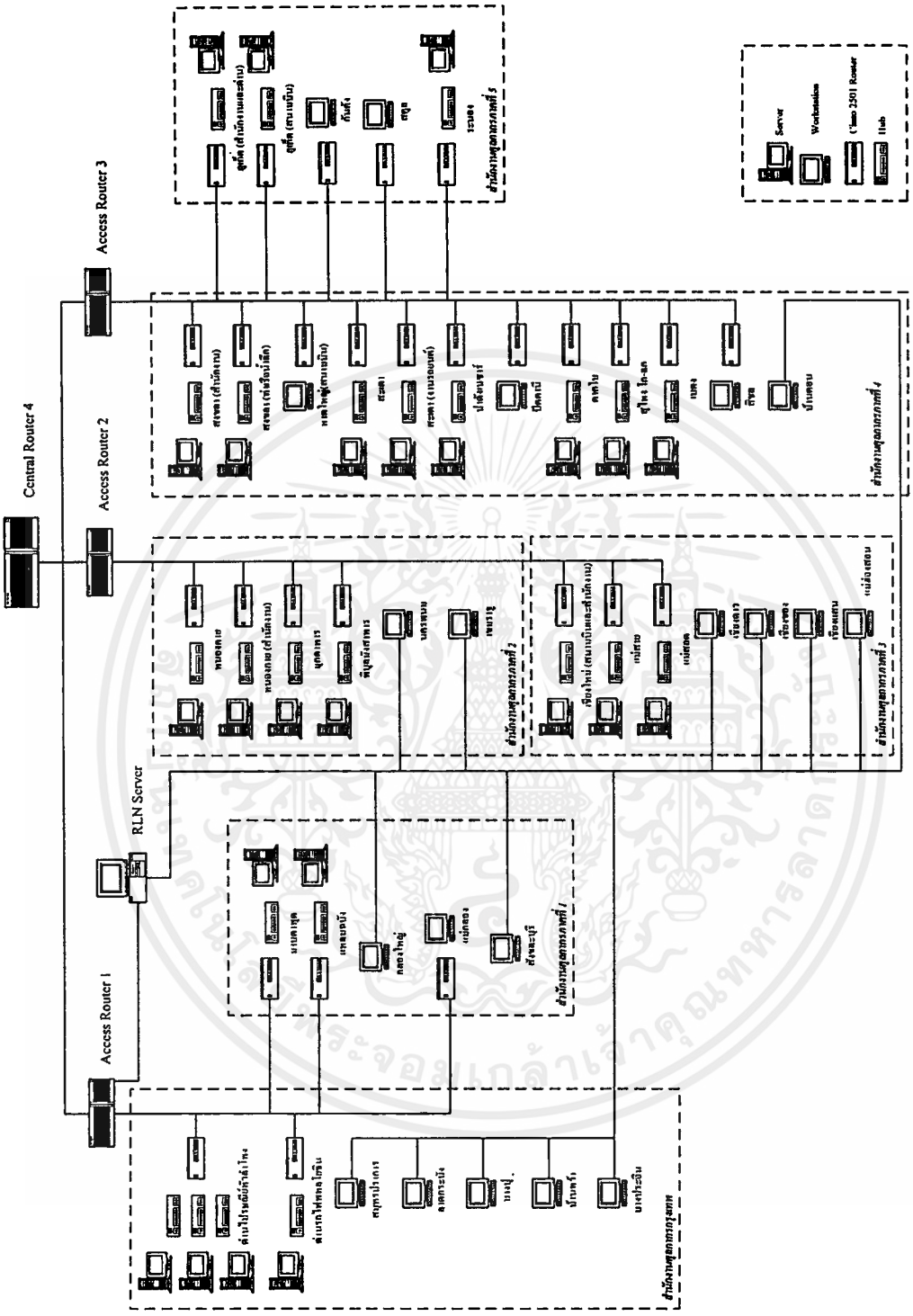
ตามด่านศุลกากรต่างๆ ที่อยู่นอกบริเวณกรมศุลกากรทั้งในกรุงเทพฯ และภูมิภาค สามารถเชื่อมต่อเข้ากับระบบเครือข่ายภายในกรมศุลกากรได้โดยต่อผ่านทางโมเด็ม ซึ่งที่ศูนย์คอมพิวเตอร์ประมวลผลหลักจะมีแอคเซสเราเตอร์ ติดตั้งอยู่ 3 ชุด และแอคเซสเราเตอร์นี้ จะทำหน้าที่เชื่อมโยงระบบเครือข่าย ในส่วนภูมิภาคหรือด่านศุลกากรต่างๆ ที่อยู่ภายนอกกรมผ่านรีโมทเราเตอร์ ไปยังเซนทอลเราเตอร์ ดังที่ได้แสดงไว้ตามรูปที่ 6.10 และ 6.11

ลักษณะการเชื่อมต่อจากด่านศุลกากรภายนอก แบ่งออกเป็น 3 แบบคือ

1. มีจำนวนเครื่องคอมพิวเตอร์หลายเครื่อง ต่อกับ hub และเราเตอร์ เชื่อมต่อเข้ากับศูนย์คอมพิวเตอร์หลักด้วยสายสัญญาณ Leased Line 64 Kbps
2. มีจำนวน 1 เครื่องคอมพิวเตอร์ต่อกับเราเตอร์ เชื่อมต่อเข้ากับศูนย์คอมพิวเตอร์หลักด้วยสายสัญญาณ Leased Line 64 Kbps
3. มีจำนวน 1 เครื่องคอมพิวเตอร์ต่อกับโมเด็ม เชื่อมต่อเข้ากับศูนย์คอมพิวเตอร์หลักด้วยสายสัญญาณ Leased Line โดยใช้ Remote LAN Node Server



รูปที่ 6.10 แสดงการเชื่อมต่อระบบเครือข่ายภายนอกเข้ามาที่ศูนย์คอมพิวเตอร์หลัก



รูปที่ 6.11 แสดงการเชื่อมต่อระบบเครือข่ายจากสำนักงานศุลกากรภาคต่างๆ ทั่วประเทศ

บทที่ 7
การประยุกต์ใช้งาน

ในขณะนี้ระบบเครือข่ายคอมพิวเตอร์ของกรมศุลกากร กำลังอยู่ในระหว่างดำเนินการติดตั้ง ซึ่งในส่วนของระบบคอมพิวเตอร์หลักได้ทำการติดตั้งเรียบร้อยแล้ว เหลือเพียงเซิฟเวอร์ เวิคสเตชัน และอุปกรณ์สื่อสารบางส่วนที่รอการติดตั้งตามที่กรมศุลกากรกำหนดไว้ จากการนำเครื่องมือตรวจสอบทราฟฟิค MRTG (Multi Router Traffic Grapher) มาติดตั้งบนระบบเครือข่ายคอมพิวเตอร์ของกรมศุลกากรซึ่งมีลักษณะระบบเครือข่ายแบบออนไลน์ทั่วประเทศที่ใช้งานอยู่จริง เพื่อทำการเก็บข้อมูลจากเราเตอร์มาทำการตรวจสอบปริมาณทราฟฟิคบนระบบเครือข่าย ทั้งเครือข่ายย่อยและเครือข่ายโดยรวมของเราเตอร์ ซึ่งจะได้กราฟที่แสดงสถิติของทราฟฟิคที่เกิดขึ้นที่เราเตอร์แบบรายวัน รายสัปดาห์ รายเดือนและรายปี โดยข้อมูลที่ได้นี้จะใช้เพื่อเป็นประโยชน์ในการให้ผู้ดูแลและบริหารระบบเครือข่ายใช้เป็นข้อมูลในการวิเคราะห์และปรับปรุงระบบเครือข่ายต่อไป

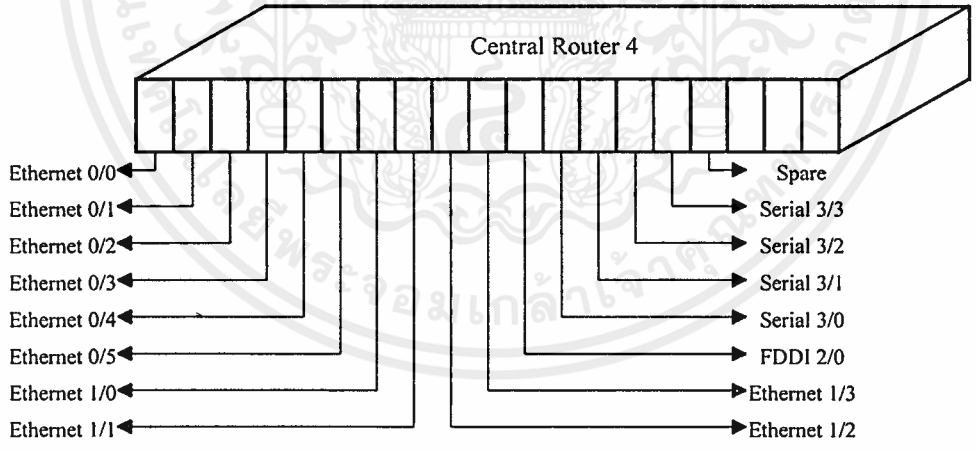
7.1 MRTG (Multi Router Traffic Grapher)

MRTG (Multi Router Traffic Grapher) [10] เป็นเครื่องมือที่ใช้สำหรับตรวจสอบปริมาณทราฟฟิคของข้อมูลที่เข้า-ออกผ่านตัวเราเตอร์บนระบบเครือข่าย สามารถ Download และดูรายละเอียดการ Setup ได้ที่ http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html ตัวโปรแกรม MRTG สร้างจาก Perl และ C สามารถ run ได้บน Unix และ Windows NT และแสดงผลในรูปของกราฟบน html page หลักการทำงานของ MRTG คือใช้ Perl script ในการเขียนคำสั่งให้โปรโตคอล SNMP อ่านข้อมูลที่แสดงปริมาณทราฟฟิคผ่านเราเตอร์จากค่า Traffic counter ที่เป็นข้อมูลเก็บอยู่ในเราเตอร์ และข้อมูลที่อ่านได้นี้จะถูกเก็บไว้บน Log file และใช้ C ในการสร้างรูปกราฟแบบ GIF image ซึ่งรูปกราฟที่ได้นี้จะแสดงผลบน Web page โดยผ่านโปรแกรม Web browser และกราฟที่แสดงผล สามารถแสดงผลข้อมูลเชิงสถิติที่จัดเก็บไว้แบบรายวัน รายสัปดาห์ รายเดือน และรายปี ซึ่งการอ่านข้อมูลที่ได้จากเราเตอร์จะเก็บไว้ในรูปของ Log file โดยโปรแกรมจะทำการอ่านค่าจากเราเตอร์ทุกๆ 5 นาที กราฟแบบรายวัน รายสัปดาห์ รายเดือนและรายปี จะมีการคำนวณคิดค่าเฉลี่ยทุก 5 นาที 30 นาที 2 ชั่วโมงและ 24 ชั่วโมง ตามลำดับ ส่วนกราฟที่ได้ในแต่ละแบบจะมีค่าสูงสุดและค่าเฉลี่ยที่ไม่เท่ากัน เนื่องจากโปรแกรมจะแยกคำนวณค่าเหล่านี้จาก Log file ในช่วงของการเก็บข้อมูลและช่วงเวลาที่ต่างกัน

ในการติดตั้ง MRTG บนระบบเครือข่ายคอมพิวเตอร์ของกรมศุลกากร โดยการ Download โปรแกรมจากอินเตอร์เน็ตเพื่อนำมาติดตั้งบนเครื่อง Sun Sparc 5 และทำการ Setup Configuration ให้สามารถติดต่อและอ่านข้อมูลการตรวจสอบปริมาณทราฟฟิคจาก Central Router 6 ตัว และ Access Router อีก 3 ตัว ซึ่งได้ทำการติดตั้งให้ MRTG สามารถอ่านข้อมูลที่แสดงปริมาณทราฟฟิคทุกๆ เครือข่ายย่อยของเราเตอร์แต่ละตัว และปริมาณทราฟฟิคโดยรวมของเราเตอร์แต่ละตัวด้วยเช่นกัน

7.2 การตรวจสอบทราฟฟิคที่เครือข่ายโดยรวมของเราเตอร์

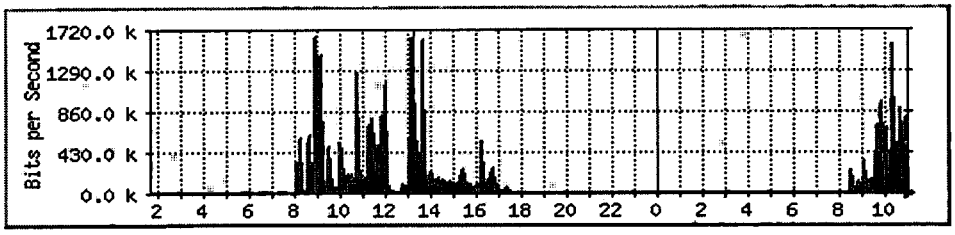
เราเตอร์ที่ติดตั้งบนระบบเครือข่ายคอมพิวเตอร์ของกรมศุลกากรแต่ละตัวจะมี Interface port ที่ประกอบไปด้วย Ethernet port, Serial port และ FDDI port ซึ่งจำนวน port แต่ละชนิดที่ใช้ของเราเตอร์แต่ละตัว จะแตกต่างกันไปตามลักษณะของการเชื่อมต่อและปริมาณของจำนวนเครือข่ายที่เชื่อมต่อกับเราเตอร์ตัวนั้นๆ โดยที่ Ethernet port จะเป็น Interface ที่ใช้เชื่อมต่อ Hub หรือเครือข่ายย่อยของ LAN แต่ละวง ส่วน Serial port จะเป็น Interface ที่ใช้เชื่อมต่อกับเครือข่ายย่อยที่เป็น Remote site และ FDDI port จะเป็น Interface ที่ใช้เชื่อมต่อกับ Concentrator เพื่อติดต่อกับ Backbone ของระบบ



รูปที่ 7.1 แสดงตัวอย่าง Interface port ชนิดต่างๆ ของเราเตอร์

Traffic Analysis for Central Router 1

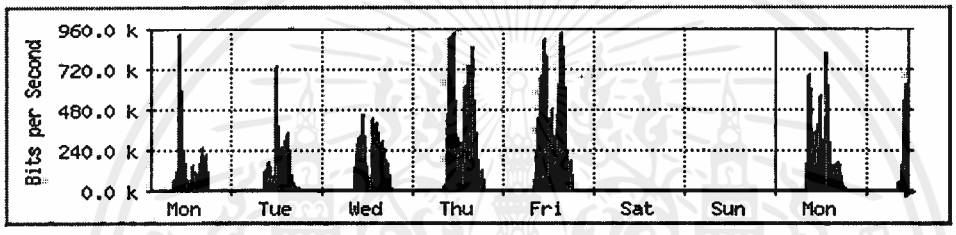
`Daily' Graph (5 Minute Average)



Max In: 1648.8 kb/s (16.5%) Average In: 111.1 kb/s (1.1%) Current In: 284.4 kb/s (2.8%)

Max Out: 1695.9 kb/s (17.0%) Average Out: 111.1 kb/s (1.1%) Current Out: 293.0 kb/s (2.9%)

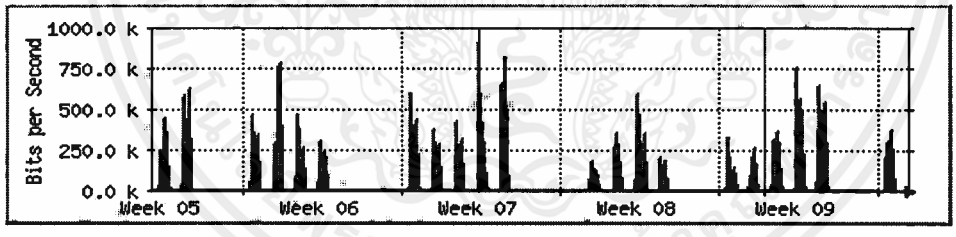
`Weekly' Graph (30 Minute Average)



Max In: 939.8 kb/s (9.4%) Average In: 87.2 kb/s (0.9%) Current In: 510.8 kb/s (5.1%)

Max Out: 937.9 kb/s (9.4%) Average Out: 87.2 kb/s (0.9%) Current Out: 558.8 kb/s (5.6%)

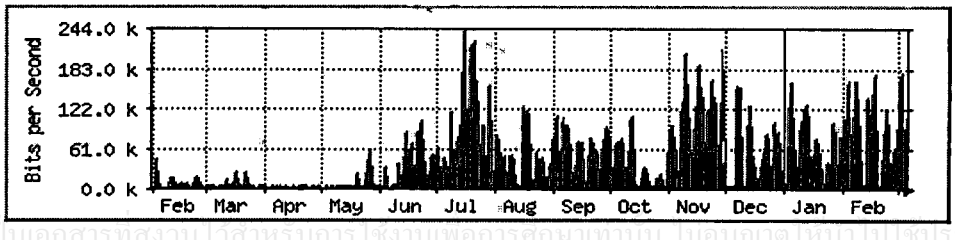
`Monthly' Graph (2 Hour Average)



Max In: 915.7 kb/s (9.2%) Average In: 74.2 kb/s (0.7%) Current In: 31.2 kb/s (0.3%)

Max Out: 987.6 kb/s (9.9%) Average Out: 73.8 kb/s (0.7%) Current Out: 30.6 kb/s (0.3%)

`Yearly' Graph (1 Day Average)



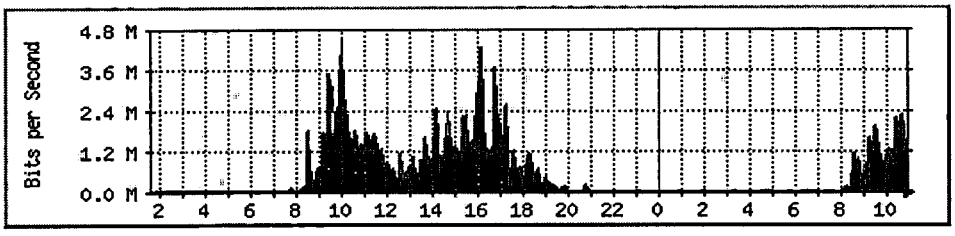
Max In: 239.6 kb/s (2.4%) Average In: 39.7 kb/s (0.4%) Current In: 111.3 kb/s (1.1%)

Max Out: 240.8 kb/s (2.4%) Average Out: 40.0 kb/s (0.4%) Current Out: 110.5 kb/s (1.1%)

รูปที่ 7.2 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Central Router 1

Traffic Analysis for Central Router 2

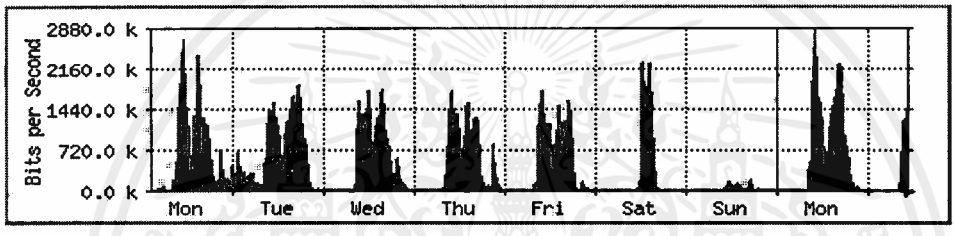
'Daily' Graph (5 Minute Average)



Max In: 4279.9 kb/s (42.8%) Average 523.1 kb/s (5.2%) Current In: 1535.6 kb/s (15.4%)

Max Out: 4505.8 kb/s (45.1%) Average Out: 524.6 kb/s (5.2%) Current Out: 1537.1 kb/s (15.4%)

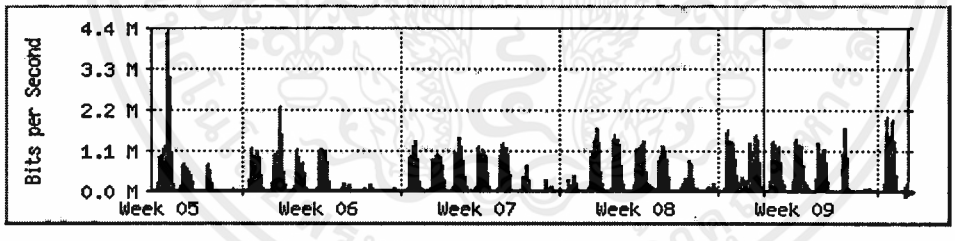
'Weekly' Graph (30 Minute Average)



Max In: 2538.1 kb/s (25.4%) Average In: 432.1 kb/s (4.3%) Current In: 1441.9 kb/s (14.4%)

Max Out: 2841.9 kb/s (28.4%) Average Out: 415.2 kb/s (4.2%) Current Out: 1439.7 kb/s (14.4%)

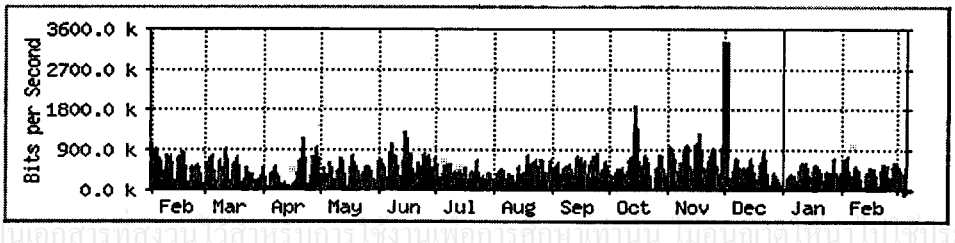
'Monthly' Graph (2 Hour Average)



Max In: 4302.5 kb/s (43.0%) Average In: 350.9 kb/s (3.5%) Current In: 223.6 kb/s (2.2%)

Max Out: 4343.1 kb/s (43.4%) Average Out: 323.5 kb/s (3.2%) Current Out: 222.2 kb/s (2.2%)

'Yearly' Graph (1 Day Average)



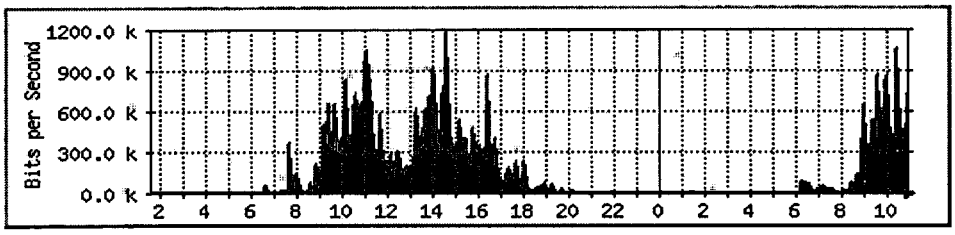
Max In: 3320.8 kb/s (33.2%) Average 433.8 kb/s (4.3%) Current In: 527.9 kb/s (5.3%)

Max Out: 1764.7 kb/s (17.6%) Average Out: 391.5 kb/s (3.9%) Current Out: 530.8 kb/s (5.3%)

รูปที่ 7.3 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Central Router 2

Traffic Analysis for Central Router 3

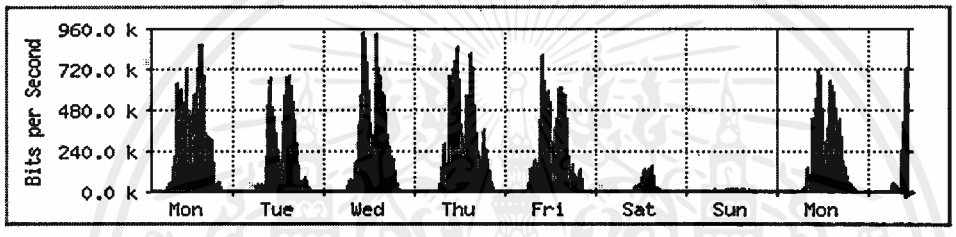
`Daily' Graph (5 Minute Average)



Max I 1187.6 kb/s (11.9%) Average 159.8 kb/s (1.6%) Current I 734.0 kb/s (7.3%)

Max Out: 1180.2 kb/s (11.8%) Average Out: 159.1 kb/s (1.6%) Current Out: 733.4 kb/s (7.3%)

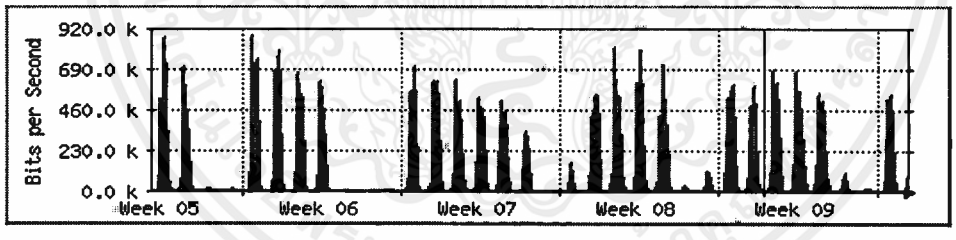
`Weekly' Graph (30 Minute Average)



Max I 934.2 kb/s (9.3%) Average 146.0 kb/s (1.5%) Current I 593.8 kb/s (5.9%)

Max Out: 933.0 kb/s (9.3%) Average Out: 146.2 kb/s (1.5%) Current Out: 592.8 kb/s (5.9%)

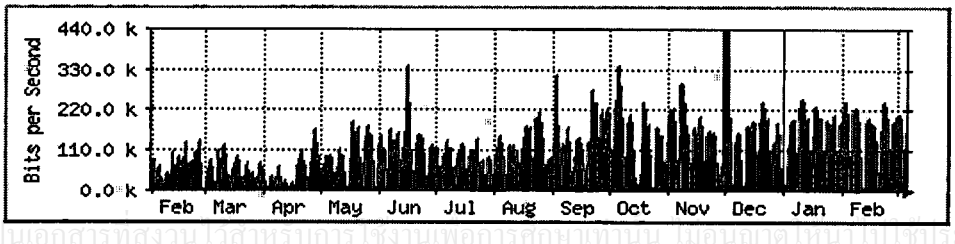
`Monthly' Graph (2 Hour Average)



Max In: 882.7 kb/s (8.8%) Average 130.8 kb/s (1.3%) Current In 85.1 kb/s (0.9%)

Max Out: 882.2 kb/s (8.8%) Average Out: 130.9 kb/s (1.3%) Current Out: 84.9 kb/s (0.8%)

`Yearly' Graph (1 Day Average)



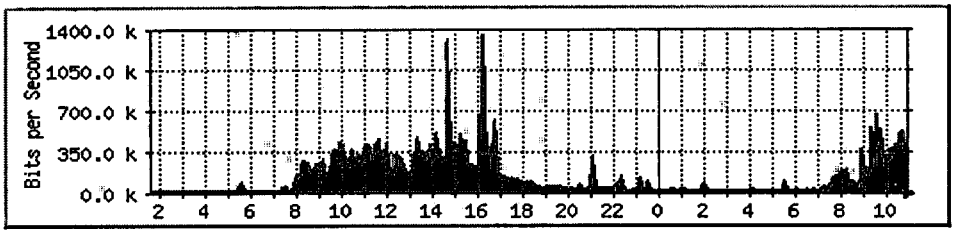
Max I 439.4 kb/s (4.4%) Average 95.1 kb/s (1.0%) Current I 159.2 kb/s (1.6%)

Max Out: 362.1 kb/s (3.6%) Average Out: 94.7 kb/s (0.9%) Current Out: 158.2 kb/s (1.6%)

รูปที่ 7.4 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Central Router 3

Traffic Analysis for Central Router 4

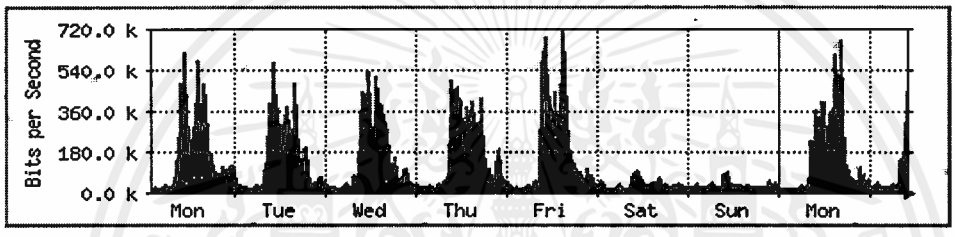
`Daily' Graph (5 Minute Average)



Max In: 1366.2 kb/s (13.7%) Average In: 154.6 kb/s (1.5%) Current In: 453.1 kb/s (4.5%)

Max Out: 1341.0 kb/s (13.4%) Average Out: 145.9 kb/s (1.5%) Current Out: 446.4 kb/s (4.5%)

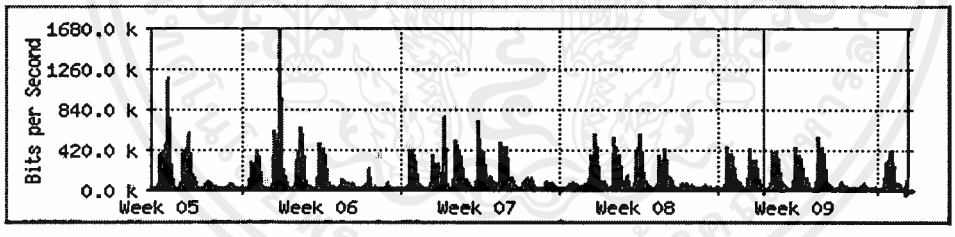
`Weekly' Graph (30 Minute Average)



Max In: 713.8 kb/s (7.1%) Average In: 133.5 kb/s (1.3%) Current In: 450.4 kb/s (4.5%)

Max Out: 695.5 kb/s (7.0%) Average Out: 123.7 kb/s (1.2%) Current Out: 420.5 kb/s (4.2%)

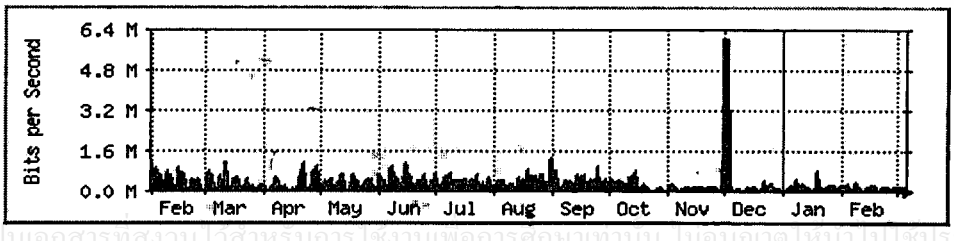
`Monthly' Graph (2 Hour Average)



Max In: 1677.7 kb/s (16.8%) Average In: 139.2 kb/s (1.4%) Current In: 129.2 kb/s (1.3%)

Max Out: 1670.6 kb/s (16.7%) Average Out: 132.7 kb/s (1.3%) Current Out: 126.8 kb/s (1.3%)

`Yearly' Graph (1 Day Average)



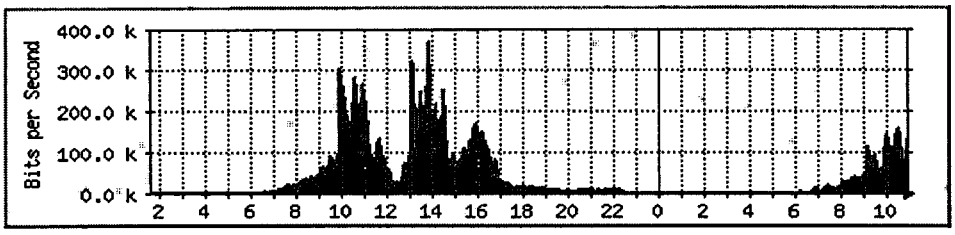
Max In: 6060.9 kb/s (60.6%) Average In: 334.8 kb/s (3.3%) Current In: 150.9 kb/s (1.5%)

Max Out: 5982.1 kb/s (59.8%) Average Out: 328.3 kb/s (3.3%) Current Out: 142.7 kb/s (1.4%)

รูปที่ 7.5 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Central Router 4

Traffic Analysis for Central Router 5

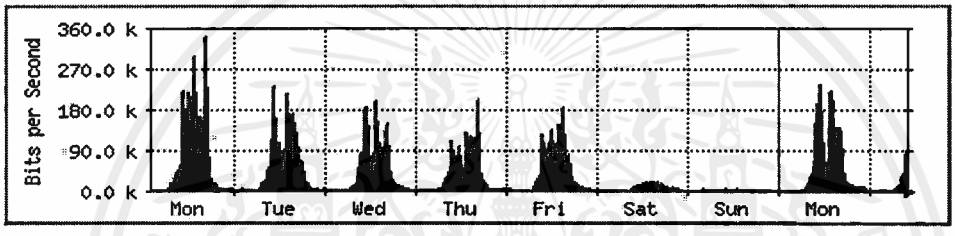
`Daily' Graph (5 Minute Average)



Max In: 370.7 kb/s (3.7%) Average In: 44.2 kb/s (0.4%) Current In: 132.5 kb/s (1.3%)

Max Out: 369.6 kb/s (3.7%) Average Out: 43.2 kb/s (0.4%) Current Out: 131.4 kb/s (1.3%)

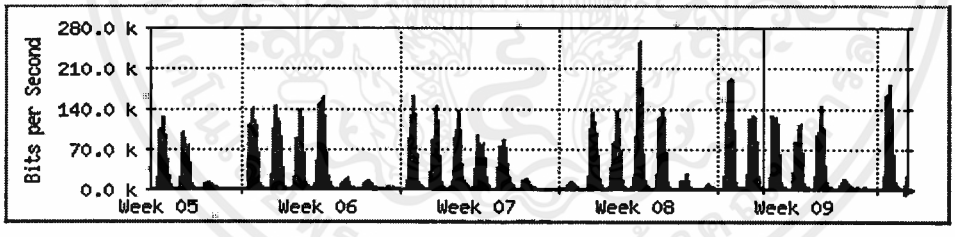
`Weekly' Graph (30 Minute Average)



Max In: 340.6 kb/s (3.4%) Average In: 35.8 kb/s (0.4%) Current In: 84.7 kb/s (0.8%)

Max Out: 339.2 kb/s (3.4%) Average Out: 34.8 kb/s (0.3%) Current Out: 83.0 kb/s (0.8%)

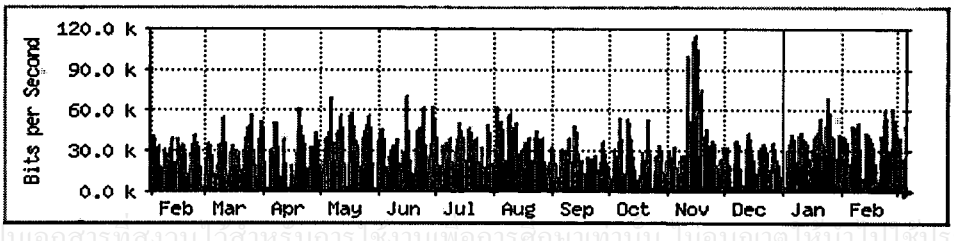
`Monthly' Graph (2 Hour Average)



Max In: 257.1 kb/s (2.6%) Average In: 30.4 kb/s (0.3%) Current In: 26.0 kb/s (0.3%)

Max Out: 255.6 kb/s (2.6%) Average Out: 29.4 kb/s (0.3%) Current Out: 24.7 kb/s (0.2%)

`Yearly' Graph (1 Day Average)



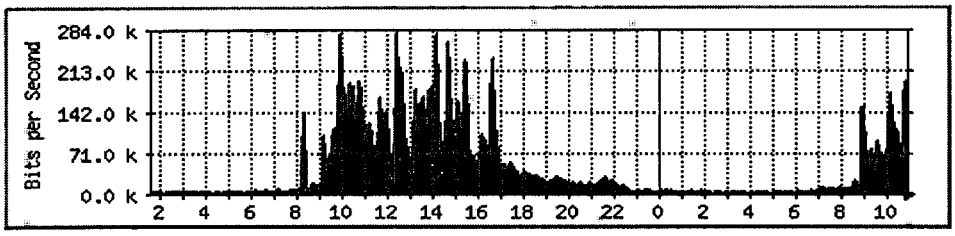
Max In: 114.5 kb/s (1.1%) Average In: 26.0 kb/s (0.3%) Current In: 48.2 kb/s (0.5%)

Max Out: 115.1 kb/s (1.2%) Average Out: 25.3 kb/s (0.3%) Current Out: 47.2 kb/s (0.5%)

รูปที่ 7.6 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Central Router 5

Traffic Analysis for Central Router 6

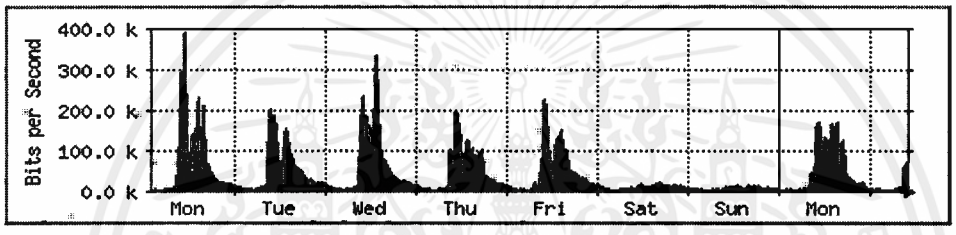
`Daily' Graph (5 Minute Average)



Max In: 279.3 kb/s (2.8%) Average In: 44.8 kb/s (0.4%) Current In: 117.4 kb/s (1.2%)

Max Out: 280.5 kb/s (2.8%) Average Out: 45.2 kb/s (0.5%) Current Out: 117.2 kb/s (1.2%)

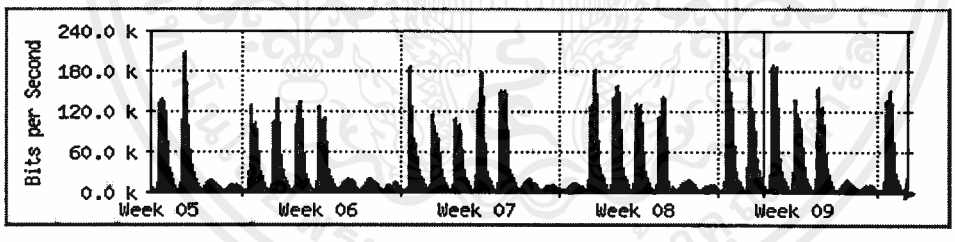
`Weekly' Graph (30 Minute Average)



Max In: 390.6 kb/s (3.9%) Average In: 40.1 kb/s (0.4%) Current In: 75.7 kb/s (0.8%)

Max Out: 390.7 kb/s (3.9%) Average Out: 40.5 kb/s (0.4%) Current Out: 75.3 kb/s (0.8%)

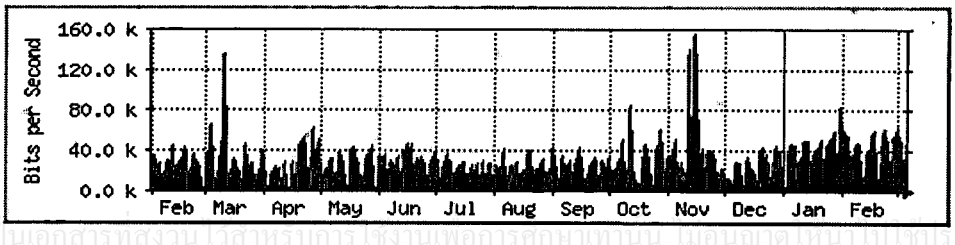
`Monthly' Graph (2 Hour Average)



Max In: 238.2 kb/s (2.4%) Average In: 34.4 kb/s (0.3%) Current In: 22.6 kb/s (0.2%)

Max Out: 238.1 kb/s (2.4%) Average Out: 34.9 kb/s (0.3%) Current Out: 22.8 kb/s (0.2%)

`Yearly' Graph (1 Day Average)



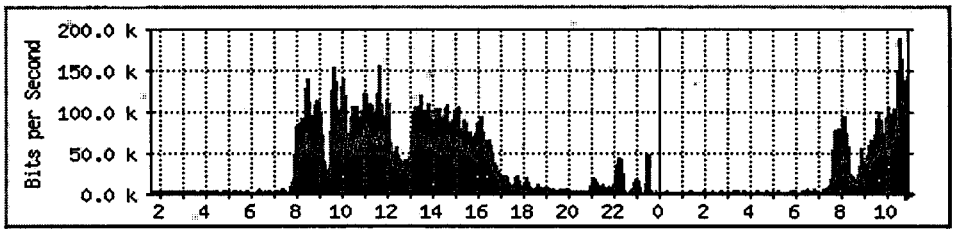
Max In: 153.9 kb/s (1.5%) Average In: 23.7 kb/s (0.2%) Current In: 47.5 kb/s (0.5%)

Max Out: 154.8 kb/s (1.5%) Average Out: 24.5 kb/s (0.2%) Current Out: 48.0 kb/s (0.5%)

รูปที่ 7.7 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Central Router 6

Traffic Analysis for Access Router 1

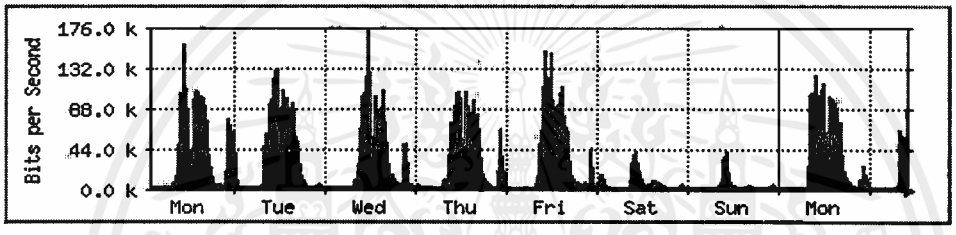
`Daily' Graph (5 Minute Average)



Max In 189.4 kb/s (1.9%) Average In 36.3 kb/s (0.4%) Current In 146.0 kb/s (1.5%)

Max Out: 131.2 kb/s (1.3%) Average Out: 23.0 kb/s (0.2%) Current Out: 110.0 kb/s (1.1%)

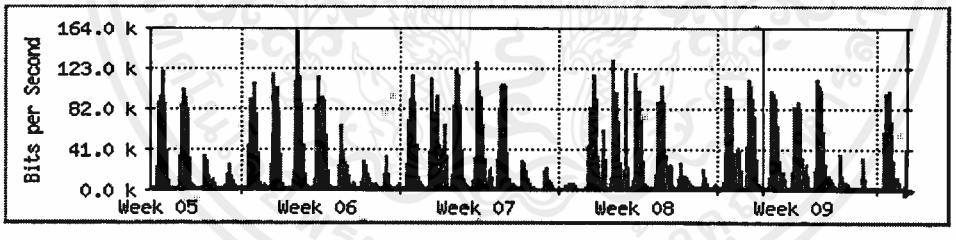
`Weekly' Graph (30 Minute Average)



Max 175.7 kb/s (1.8%) Average 29.7 kb/s (0.3%) Current 87.7 kb/s (0.9%)

Max Out: 106.5 kb/s (1.1%) Average Out: 19.9 kb/s (0.2%) Current Out: 54.9 kb/s (0.5%)

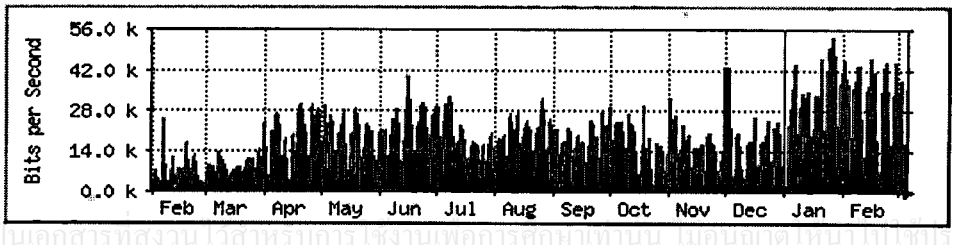
`Monthly' Graph (2 Hour Average)



Max In 161.0 kb/s (1.6%) Average 28.1 kb/s (0.3%) Current 41.5 kb/s (0.4%)

Max Out: 112.4 kb/s (1.1%) Average Out: 20.5 kb/s (0.2%) Current Out: 23.9 kb/s (0.2%)

`Yearly' Graph (1 Day Average)



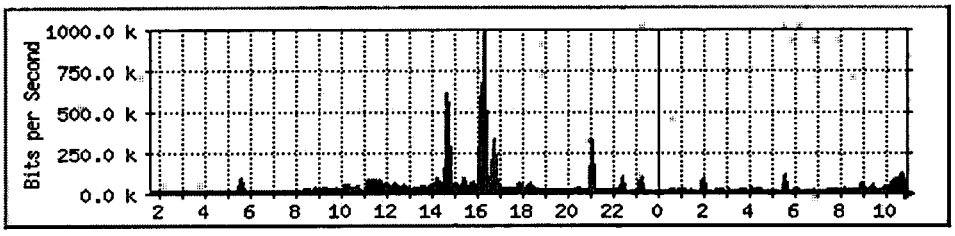
Max In 53.2 kb/s (0.5%) Average 16.4 kb/s (0.2%) Current In 35.9 kb/s (0.4%)

Max Out: 48.7 kb/s (0.5%) Average Out: 14.4 kb/s (0.1%) Current Out: 22.3 kb/s (0.2%)

รูปที่ 7.8 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Access Router 1

Traffic Analysis for Access Router 2

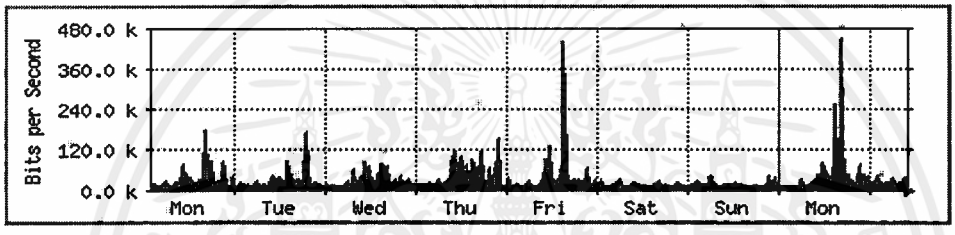
`Daily' Graph (5 Minute Average)



Max In: 988.3 kb/s (9.9%) Average In: 43.3 kb/s (0.4%) Current In: 83.4 kb/s (0.8%)

Max Out: 986.8 kb/s (9.9%) Average Out: 42.2 kb/s (0.4%) Current Out: 82.6 kb/s (0.8%)

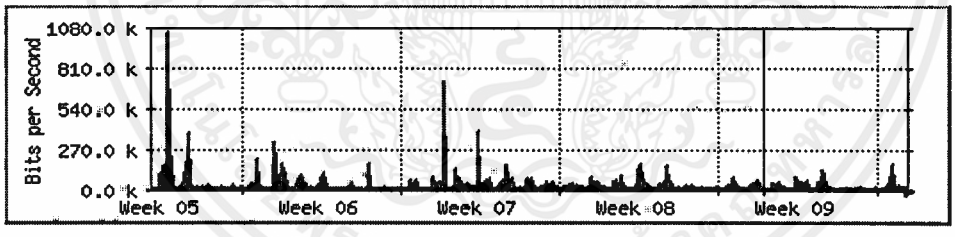
`Weekly' Graph (30 Minute Average)



Max In: 448.2 kb/s (4.5%) Average In: 32.4 kb/s (0.3%) Current In: 31.8 kb/s (0.3%)

Max Out: 446.8 kb/s (4.5%) Average Out: 31.5 kb/s (0.3%) Current Out: 31.2 kb/s (0.3%)

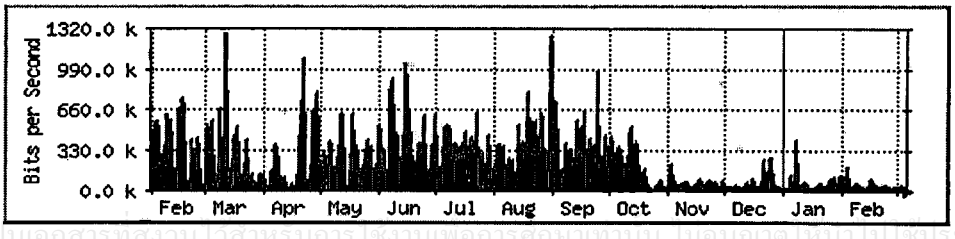
`Monthly' Graph (2 Hour Average)



Max In: 1058.3 kb/s (10.6%) Average In: 43.6 kb/s (0.4%) Current In: 25.6 kb/s (0.3%)

Max Out: 1057.7 kb/s (10.6%) Average Out: 42.7 kb/s (0.4%) Current Out: 25.7 kb/s (0.3%)

`Yearly' Graph (1 Day Average)



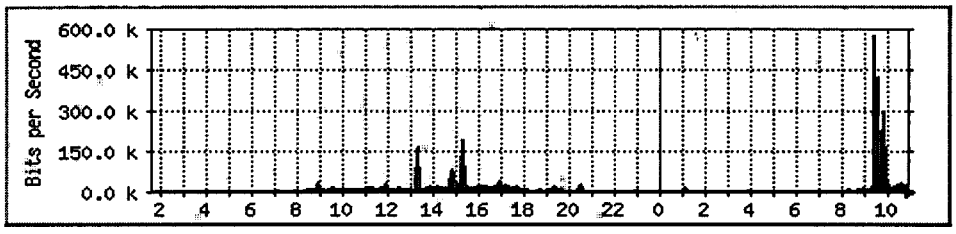
Max In: 1281.0 kb/s (12.8%) Average In: 218.1 kb/s (2.2%) Current In: 42.1 kb/s (0.4%)

Max Out: 1274.4 kb/s (12.7%) Average Out: 217.9 kb/s (2.2%) Current Out: 40.8 kb/s (0.4%)

รูปที่ 7.9 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Access Router 2

Traffic Analysis for Access Router 3

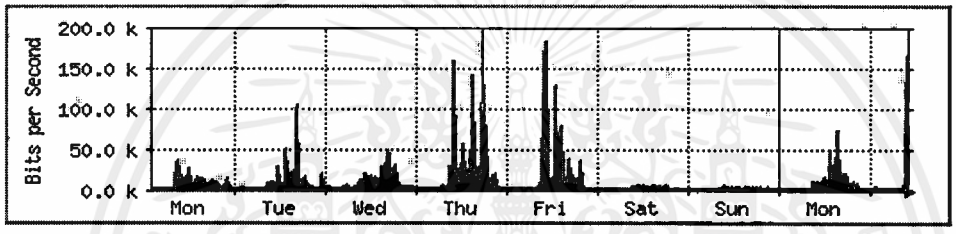
`Daily' Graph (5 Minute Average)



Max In: 578.5 kb/s (5.8%) Average In: 13.4 kb/s (0.1%) Current In: 34.7 kb/s (0.3%)

Max Out: 574.8 kb/s (5.7%) Average Out: 12.7 kb/s (0.1%) Current Out: 34.5 kb/s (0.3%)

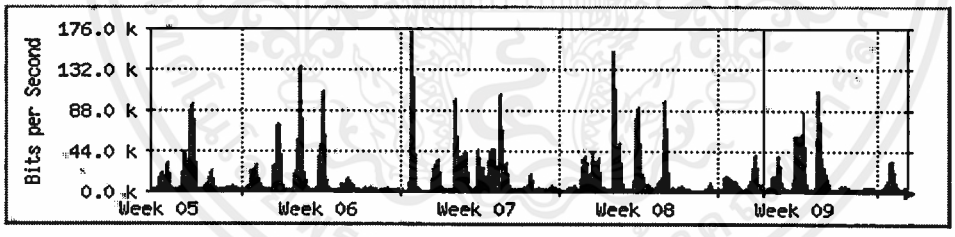
`Weekly' Graph (30 Minute Average)



Max In: 184.8 kb/s (1.8%) Average In: 12.1 kb/s (0.1%) Current In: 167.6 kb/s (1.7%)

Max Out: 197.2 kb/s (2.0%) Average Out: 12.0 kb/s (0.1%) Current Out: 167.6 kb/s (1.7%)

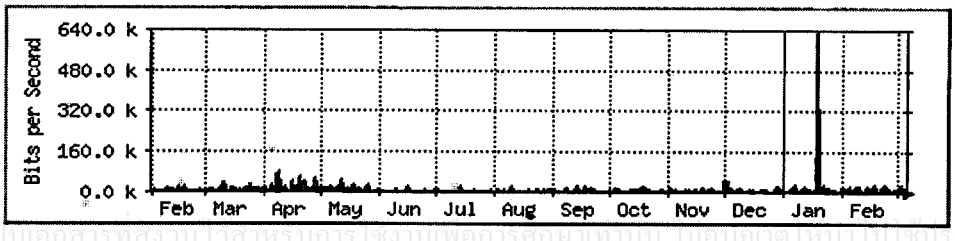
`Monthly' Graph (2 Hour Average)



Max In: 172.5 kb/s (1.7%) Average In: 13.3 kb/s (0.1%) Current In: 4984.0 b/s (0.0%)

Max Out: 172.1 kb/s (1.7%) Average Out: 13.1 kb/s (0.1%) Current Out: 4912.0 b/s (0.0%)

`Yearly' Graph (1 Day Average)



Max In: 630.5 kb/s (6.3%) Average In: 11.7 kb/s (0.1%) Current In: 9400.0 b/s (0.1%)

Max Out: 628.9 kb/s (6.3%) Average Out: 10.9 kb/s (0.1%) Current Out: 8688.0 b/s (0.1%)

รูปที่ 7.10 กราฟแสดงปริมาณทราฟฟิคโดยรวมของ Access Router 3

การตรวจสอบทราฟฟิคที่เครือข่ายโดยรวมของเราเตอร์ จะตรวจสอบในส่วนที่เป็น Interface port ทุก port ที่มีอยู่ในเราเตอร์แต่ละตัว จะได้ผลรวมของการตรวจสอบปริมาณทราฟฟิคตามรูปที่ 7.2-7.10 ซึ่งเป็นการแสดงปริมาณทราฟฟิคโดยรวมของเซนทอลเราเตอร์ 6 ตัว และแอคเซสเราเตอร์อีก 3 ตัว ในแต่ละรูปจะแสดงกราฟ 4 แบบคือแสดงปริมาณทราฟฟิคแบบรายวัน รายสัปดาห์ รายเดือนและรายปี ซึ่งการอ่านข้อมูลที่ได้จากเราเตอร์จะเก็บไว้ในรูปของ Log file โดยโปรแกรมจะทำการอ่านค่าจากเราเตอร์ทุกๆ 5 นาที ซึ่งเวลาในการอ่านค่าจากเราเตอร์นี้สามารถกำหนดได้โดยการ Set ค่า Configuration ของโปรแกรม จากกราฟในแนวแกน X จะกำหนดให้แสดงค่าของคาบเวลา โดยกราฟแบบรายวันจะแสดงค่าของปริมาณทราฟฟิคของแต่ละชั่วโมงในช่วง 0-24 นาฬิกา และคำนวณค่าเฉลี่ยทุก 5 นาที กราฟแบบรายสัปดาห์จะแสดงค่าของปริมาณทราฟฟิคของแต่ละวันในช่วงวันอาทิตย์ถึงวันเสาร์ และคำนวณค่าเฉลี่ยทุก 30 นาที กราฟแบบรายเดือนจะแสดงค่าของปริมาณทราฟฟิคของแต่ละสัปดาห์ในช่วง 4 สัปดาห์ที่ผ่านมาจนถึงสัปดาห์ปัจจุบันและคำนวณค่าเฉลี่ยทุก 2 ชั่วโมง และกราฟแบบรายปีจะแสดงค่าของปริมาณทราฟฟิคของแต่ละเดือนในช่วงเดือนมกราคมถึงธันวาคมและคำนวณค่าเฉลี่ยทุก 24 ชั่วโมง กราฟในแนวแกน Y จะกำหนดให้แสดงค่าของปริมาณของอัตราการรับส่งข้อมูลที่ผ่านเข้า-ออกที่เราเตอร์มีหน่วยเป็น Bits Per Second ในส่วนของรูปกราฟที่แสดงจะแบ่งเป็น 2 ส่วนคือสีเขียว(สีอ่อน)จะแสดงถึงปริมาณทราฟฟิคที่ผ่านเข้ามาที่ Interface port นี้ สีน้ำเงิน(สีเข้ม) จะแสดงถึงปริมาณทราฟฟิคที่ผ่านออกจากเราเตอร์ที่ Interface port นี้

ภายใต้กราฟทั้ง 4 แบบจะแสดงค่าต่างๆ ที่คำนวณได้จาก Log file ดังนี้คือ

Max In : คือค่าสูงสุดของปริมาณทราฟฟิคที่ผ่านเข้ามาที่ Interface port ของเราเตอร์

Max Out : คือค่าสูงสุดของปริมาณทราฟฟิคที่ผ่านออกจาก Interface port ของเราเตอร์

Average In : คือการแสดงค่าเฉลี่ยของปริมาณทราฟฟิคที่ผ่านเข้ามาที่ Interface port ของเราเตอร์

Average Out : คือการแสดงค่าเฉลี่ยของปริมาณทราฟฟิคที่ผ่านออกจาก Interface port ของเราเตอร์

Current In : คือการแสดงค่าของปริมาณทราฟฟิคที่ผ่านเข้ามาที่ Interface port ณ เวลาปัจจุบัน

Current Out : คือการแสดงค่าของปริมาณทราฟฟิคที่ผ่านออกจาก Interface port ณ เวลาปัจจุบัน

ค่าของ Max In, Max Out, Average In, Average Out, Current In และ Current Out จะแสดงหน่วยของการวัดเป็น b/s หรือ kb/s ขึ้นอยู่กับปริมาณความมากน้อยของทราฟฟิคที่ผ่านเข้าออกที่ตัวเราเตอร์ และค่าของตัวเลขที่แสดงเป็นเปอร์เซ็นต์ในวงเล็บด้านหลังของค่าต่างๆ เช่นรูปที่ 7.2 ซึ่งเป็นกราฟแสดงปริมาณทราฟฟิคโดยรวมของเซนทอลเราเตอร์ 1 จากกราฟแบบรายวันจะมีค่าสูงสุดของปริมาณทราฟฟิคที่ผ่านเข้ามาที่ ของเราเตอร์ คือ Max In : 1648.8 kb/s (16.5%)

ค่าเปอร์เซ็นต์ที่ได้นี้จะคำนวณเทียบกับอัตราการรับส่งข้อมูลมาตรฐานของระบบอีเทอร์เน็ตคือ

10 Mb/s หรือ 10,000 kb/s คิดเป็น 100 %

Max In 10,000 kb/s	=	100 %
Max In 1648.8 kb/s	=	(1648.8 x 100) / 10,000 %
จะได้ค่าของ Max In	=	16.488
	≈	16.5 %

จากรูปที่ 7.2 เป็นกราฟแสดงปริมาณทราฟฟิคโดยรวมของเซนทอลเราเตอร์ 1 จะเห็นได้ว่ารูปกราฟแบบรายวันปริมาณทราฟฟิคจะเริ่มเกิดขึ้นหลังเวลา 8:00 น. และจะมีค่าปริมาณทราฟฟิคเกิดขึ้นต่อเนื่องไปเรื่อยๆ จะมากหรือน้อยขึ้นอยู่กับปริมาณการรับส่งข้อมูล ณ ช่วงเวลานั้นๆ จนถึงเวลาหลัง 12:00 น. ปริมาณทราฟฟิคจะค่อยๆ ลดลงเพราะเป็นช่วงเวลาพักกลางวัน ปริมาณทราฟฟิคจะเริ่มเพิ่มขึ้นอีกหลัง 13:00 น. และจะลดลงจนถึง 0 หลัง 17:00 น. ซึ่งเป็นช่วงเวลาเลิกงาน ปริมาณทราฟฟิคของวันจันทร์ถึงวันศุกร์ส่วนใหญ่จะมีค่าใกล้เคียงกัน ยกเว้นในวันเสาร์และอาทิตย์อาจจะมีปริมาณทราฟฟิคเกิดขึ้นบ้างเพียงเล็กน้อยหรืออาจจะไม่มีเกิดขึ้นเลย สำหรับกราฟแบบรายปี สังเกตได้ว่ามีปริมาณทราฟฟิคเพิ่มมากขึ้นในช่วงปลายเดือนพฤษภาคม 2542 ซึ่งค่าของปริมาณทราฟฟิคที่เพิ่มขึ้นนี้ เกิดได้จากมีการติดตั้งระบบเครือข่ายคอมพิวเตอร์ของเซนทอลเราเตอร์ 1 เสร็จสมบูรณ์เพิ่มมากขึ้น ประกอบกับระบบงานที่ออกแบบมาให้ใช้สำหรับหน่วยงานที่มีเครือข่ายเชื่อมต่อกับเซนทอลเราเตอร์ 1 เริ่มเสร็จและให้หน่วยงานนั้นๆ ทดลองใช้งานจริง ปริมาณทราฟฟิคโดยรวมทั่วๆ ไปของเซนทอลเราเตอร์ 1 จัดได้ว่ามีค่าของปริมาณทราฟฟิคที่ยังไม่มาก สามารถที่จะขยายระบบเครือข่ายเพิ่มเติมได้อีกเป็นจำนวนมาก

จากรูปที่ 7.3 เป็นกราฟแสดงปริมาณทราฟฟิคโดยรวมของเซนทอลเราเตอร์ 2 ลักษณะการพิจารณาปริมาณทราฟฟิคโดยทั่วไปของเซนทอลเราเตอร์ 2 จะคล้ายกับเซนทอลเราเตอร์ 1 แต่จะมีปริมาณทราฟฟิคที่มากกว่า จากรูปกราฟแบบรายปี จะสังเกตุได้ว่ามีปริมาณทราฟฟิคค่อนข้างสม่ำเสมอมาเป็นระยะเวลาหลายเดือนแต่ก็ยังจัดได้ว่ามีค่าของปริมาณทราฟฟิคเพียงเล็กน้อย สามารถที่จะขยายระบบเครือข่ายเพิ่มเติมได้อีกเป็นจำนวนมากเช่นกัน

จากตัวอย่างของกราฟที่แสดงปริมาณทราฟฟิคของเซนทอลเราเตอร์ 1 และ 2 ที่ได้อธิบายมาแล้ว เมื่อพิจารณาจากรูป 7.2-7.10 จะสังเกตได้ว่ามีลักษณะของกราฟที่คล้ายคลึงกันคือ กราฟแบบรายวันจะเริ่มเกิดปริมาณทราฟฟิคหลังเวลา 8:00 น. เป็นส่วนใหญ่ แต่อาจจะมีบางรูปที่เริ่มเกิดปริมาณทราฟฟิคขึ้นก่อนเวลา 8:00 น. ซึ่งสาเหตุอาจเกิดได้จากลักษณะของการทำงานที่เร่งด่วนหรือบางหน่วยงานต้องปฏิบัติงานตลอด 24 ชั่วโมง เช่นที่ด่านศุลกากรดอนเมือง ด่านศุลกากรตามชายแดนต่างๆ เป็นต้น ช่วงเวลาที่ปริมาณทราฟฟิคเริ่มลดลงจนกระทั่งกราฟมีค่าตกลงถึง 0 จะเป็นช่วงหลังเวลา 17:00 น.แต่ก็มีบางรูปที่ปริมาณทราฟฟิคเริ่มลดลงหลังเวลา 22:00 น. ซึ่งสาเหตุก็มาจากลักษณะของการทำงานเช่นกัน ช่วงเวลาที่ปริมาณทราฟฟิคตกลงถึง 0 แสดงว่าไม่มีการรับส่งข้อมูลผ่านตัวเราเตอร์ กราฟแบบรายสัปดาห์โดยส่วนมากจะมีการรับส่งข้อมูลหรือมีปริมาณทราฟฟิคเป็นปกติในช่วงวันจันทร์ถึงวันศุกร์ ยกเว้นบางรูปที่ในวันเสาร์และอาทิตย์ก็จะมีการรับส่ง

ข้อมูลแต่เป็นปริมาณทราฟฟิคที่เกิดขึ้นในปริมาณที่น้อยมาก กราฟแบบรายเดือนจะมีลักษณะของการเกิดปริมาณทราฟฟิคและการพิจารณาคล้ายกับกราฟแบบรายสัปดาห์ เมื่อสังเกตลักษณะการเกิดปริมาณทราฟฟิคของกราฟแต่ละแบบนำมาพิจารณารวมกัน จะทำให้สามารถมองเห็นสภาพการเกิดปริมาณทราฟฟิคโดยรวมของเราเตอร์แต่ละตัว ซึ่งผู้ดูแลและบริหารระบบเครือข่ายสามารถที่จะทราบถึง Bandwidth ที่ใช้หรือเกิดขึ้นในระบบเครือข่าย, ปริมาณของการรับส่งข้อมูลที่ผ่านตัวเราเตอร์, ช่วงเวลาที่เกิดปริมาณทราฟฟิคมากหรือเกิด Bottleneck, ช่วงเวลาที่เกิดปริมาณทราฟฟิคน้อย หรือ ช่วงเวลาที่ไม่มีการรับส่งข้อมูลเกิดขึ้นเลยในระบบ

จากสภาพการใช้งานโดยรวมทั่วๆไปของเราเตอร์แต่ละตัว จัดได้ว่ามีการเกิดปริมาณทราฟฟิคขึ้นในระดับที่ไม่มาก อาจเกิดจากสาเหตุคือ ถึงแม้ว่าระบบเครือข่ายคอมพิวเตอร์ของเราเตอร์แต่ละตัวจะมีการติดตั้งเสร็จสมบูรณ์แล้วก็ตาม แต่ระบบงานหรือแอพพลิเคชันต่างๆ ที่นำมาใช้ยังไม่เสร็จสมบูรณ์ บางระบบอยู่ในระหว่างการปรับปรุงแก้ไข บางระบบอยู่ในระหว่างการทดลองใช้งานจริง และบางระบบก็สามารถใช้งานจริงได้ตามปกติแล้ว เพราะฉะนั้นในการที่จะพิจารณาว่าปริมาณทราฟฟิคที่เกิดขึ้นของเราเตอร์แต่ละตัวจะมีมากหรือน้อยแค่ไหน ควรพิจารณาในตอนที่ระบบงานต่างๆ ที่ออกแบบมาให้ใช้ ได้ถูกใช้งานอย่างเต็มที่

7.3 การตรวจสอบทราฟฟิคที่เครือข่ายย่อยของเราเตอร์

ในการตรวจสอบปริมาณทราฟฟิคที่เครือข่ายย่อยของเราเตอร์แต่ละตัว เปรียบเทียบได้กับเป็นการตรวจสอบปริมาณทราฟฟิคของ LAN วงย่อยๆ แต่ละวงที่เชื่อมต่อกับเซนทอลเราเตอร์ และเป็นการตรวจสอบปริมาณทราฟฟิคของ Remote Site ที่เชื่อมต่อกับแอคเซสเราเตอร์ซึ่งก็คือหน่วยงานศุลกากรต่างๆ ที่อยู่ภายนอกกรมศุลกากร ลักษณะของการอ่านค่าต่างๆ ที่ได้จากกราฟในแต่ละแบบ รวมถึงการคำนวณค่าของ Max In, Max Out, Average In, Average Out, Current In และ Current Out จะใช้วิธีและหลักการเหมือนดังที่กล่าวมาแล้วในหัวข้อ 7.2 เรื่องการตรวจสอบทราฟฟิคที่เครือข่ายโดยรวมของเราเตอร์ จากรูปที่ 7.11-7.19 เป็นตัวอย่างของกราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของเราเตอร์แต่ละตัว ซึ่งมี Interface Port ชนิดต่างๆ กันคือ

รูปที่ 7.11 และ 7.15 จะเป็นเครือข่ายย่อยของ Interface Port ชนิด Fiber Optic ซึ่งค่าต่างๆ ที่อ่านได้จะคิดคำนวณเป็นเปอร์เซ็นต์เทียบกับอัตราการรับส่งข้อมูลมาตรฐานของ FDDI Backbone ที่ใช้ในระบบคือ 100 Mb/s หรือ 100,000 kb/s คิดเป็น 100 % ตัวอย่างเช่น รูปที่ 7.11 กราฟแบบรายสัปดาห์อ่านค่าของ Max In ได้ 806.5 kb/s (0.8%)

Max In 100,000 kb/s	=	100 %
Max In 806.5 kb/s	=	(806.5 x 100) / 100,000 %
จะได้ค่าของ Max In	=	0.8065
	≈	0.8 %

รูปที่ 7.19 จะเป็นเครือข่ายย่อยของ Interface Port ชนิด Serial Port ซึ่งค่าต่างๆ ที่อ่านได้จะคิดคำนวณเป็นเปอร์เซ็นต์เทียบกับอัตราการรับส่งข้อมูลมาตรฐานของ Leased line ที่ใช้ในระบบ คือ 64 kb/s หรือ 64,000 b/s คิดเป็น 100 % ตัวอย่างเช่น รูปที่ 7.19 กราฟแบบรายเดือนอ่านค่าของ Average Out ได้ 480.0 b/s (0.8%)

Average Out 64,000 b/s	=	100 %
Average Out 480.0 b/s	=	(480.0 x 100) / 64,000 %
จะได้ค่าของ Max In	=	0.75
	≈	0.8 %

รูปที่ 7.12, 7.13, 7.14, 7.16, 7.17 และ 7.18 จะเป็นเครือข่ายย่อยของ Interface Port ชนิดอีเทอร์เน็ต ซึ่งการคำนวณจะเหมือนกับที่ได้อธิบายไว้แล้วในหัวข้อ 7.2

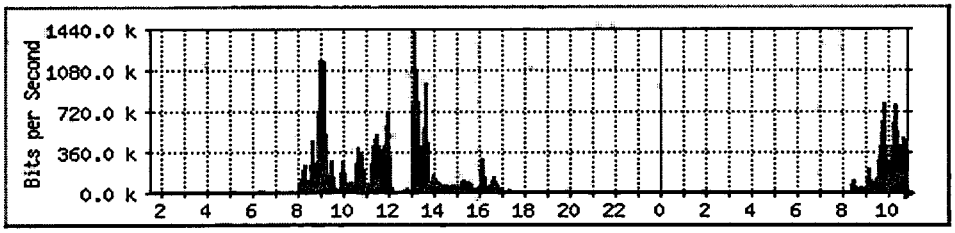
จากการมองภาพโดยรวมของการตรวจสอบปริมาณทราฟฟิคที่เครือข่ายย่อยของเราเตอร์ จะเห็นได้ว่ามีปริมาณของค่าต่างๆ ที่วัดได้คือ Max In, Max Out, Average In, Average Out, Current In และ Current Out ในระดับที่น้อยมาก ซึ่งบางค่ายังวัดค่าได้ไม่ถึง 1 % จากการวิเคราะห์สาเหตุเกิดจากเมื่อแบ่งเครือข่ายเป็น LAN หลายๆ วงหรือแบ่งเครือข่ายเป็น Sub Network จะทำให้เครื่องคอมพิวเตอร์ถูกแบ่งเป็นเครือข่ายย่อยๆ หลายเครือข่าย ลักษณะของการสื่อสารข้อมูลเมื่อมีการแลกเปลี่ยนข้อมูลของเครื่องคอมพิวเตอร์เกิดขึ้นภายใน LAN วงเดียวกัน จะไม่มีข้อมูลผ่านออกไปที่พอร์ทของเราเตอร์ การที่จะเกิดทราฟฟิคหรือมีการรับส่งข้อมูลเกิดขึ้นผ่านพอร์ทของเราเตอร์ จะเกิดในกรณีที่มีการติดต่อสื่อสารของเครื่องคอมพิวเตอร์จาก LAN วงหนึ่งไปยังอีกวงหนึ่งที่เชื่อมต่อกันอยู่คนละ Interface Port ของเราเตอร์ หรือมีการติดต่อสื่อสารกับเครื่องที่เป็น Data Base Server หรือเครื่อง Main Frame ที่ติดตั้งอยู่ที่ศูนย์คอมพิวเตอร์ประมวลผลหลัก อีกสาเหตุหนึ่งที่ทำให้ปริมาณทราฟฟิคเกิดขึ้นบนเครือข่ายย่อยมีค่าน้อยคือ ที่ LAN แต่ละวงจะมีเซิฟเวอร์ติดตั้งอยู่ และได้ทำการติดตั้งโปรแกรมหรือ Data Base ต่างๆ ที่มีความจำเป็นต้องใช้งานบ่อย ไว้คอยให้บริการกับเครื่องคอมพิวเตอร์ที่ต่ออยู่กับ LAN วงนั้นๆ ทำให้ลดการส่งผ่านข้อมูลที่จะต้องผ่านพอร์ทของเราเตอร์ได้ในส่วนหนึ่ง

สำหรับการขยายเครือข่ายเพิ่มเติมในอนาคต สามารถใช้กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายโดยรวมและเครือข่ายย่อยของเราเตอร์มาช่วยในการพิจารณาประกอบกันได้ โดยประการแรกควรทราบตำแหน่งหรือสถานที่ที่จะทำการติดตั้งเครื่องเพิ่มเติม เพื่อที่จะได้ทราบว่าควรจะนำเครื่องใหม่นี้ไปเชื่อมต่อกับเราเตอร์ตัวใดและเครือข่ายย่อยวงใดที่มีปริมาณทราฟฟิคน้อยกว่า Interface Port อื่นๆ ในเราเตอร์ตัวเดียวกัน หรือ Interface Port ที่พิจารณาแล้วมีความเหมาะสมที่สุด ซึ่งผู้ออกแบบระบบเครือข่ายต้องเป็นผู้พิจารณาเอง ขั้นต่อไปควรทราบจำนวนของเครื่องที่จะติดตั้งเพิ่มด้วย เพื่อเป็นข้อมูลในการตรวจสอบอุปกรณ์เชื่อมต่อระบบเครือข่ายว่าเพียงพอต่อความต้องการหรือไม่ เช่น มีเครื่องเชื่อมต่ออยู่ในระบบเครือข่ายเดิม 20 เครื่องใช้ Hub ชนิด 24 พอร์ท ต้องการ

เพิ่มเติมเครื่องอีก 9 เครื่อง ซึ่งทำให้พอร์ทของ Hub ที่เหลือไม่พอใช้ จะต้องทำการติดตั้ง Hub เพิ่มเติมเข้าไปในระบบด้วย เพื่อให้เพียงพอต่อการให้บริการเครื่องทั้งหมด เป็นต้น และอุปกรณ์เชื่อมต่อระบบเครือข่ายที่จะต่อเพิ่มเติมเข้าไปใหม่ ควรได้มาตรฐานและมีความสามารถในการติดตั้งรวมถึงการใช้งานร่วมกับระบบเดิมได้เป็นอย่างดี

Traffic Analysis for Fddi 4/0 of Central Router 1

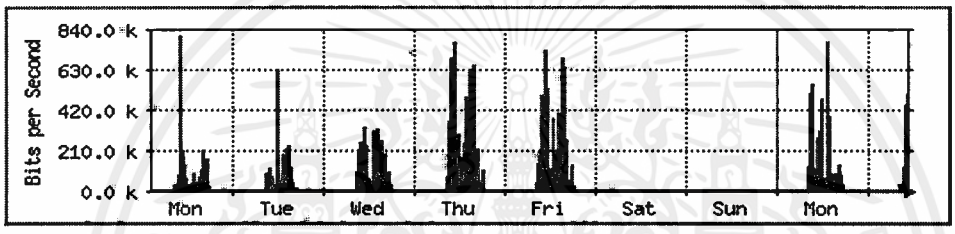
`Daily' Graph (5 Minute Average)



Max In: 1412.3 kb/s (1.4%) Average In: 90.2 kb/s (0.1%) Current In: 485.1 kb/s (0.5%)

Max Out: 214.8 kb/s (0.2%) Average Out: 20.7 kb/s (0.0%) Current Out: 159.0 kb/s (0.2%)

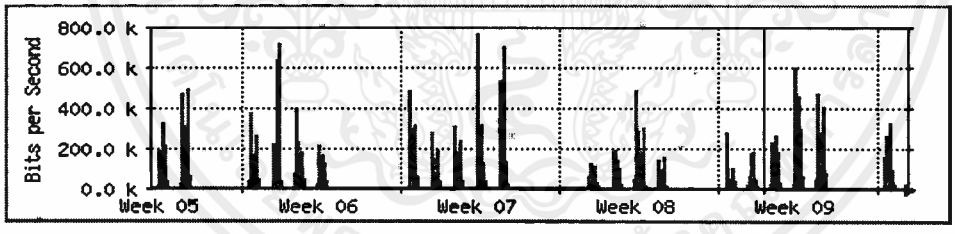
`Weekly' Graph (30 Minute Average)



Max In: 806.5 kb/s (0.8%) Average In: 66.7 kb/s (0.1%) Current In: 506.1 kb/s (0.5%)

Max Out: 239.8 kb/s (0.2%) Average Out: 20.5 kb/s (0.0%) Current Out: 125.7 kb/s (0.1%)

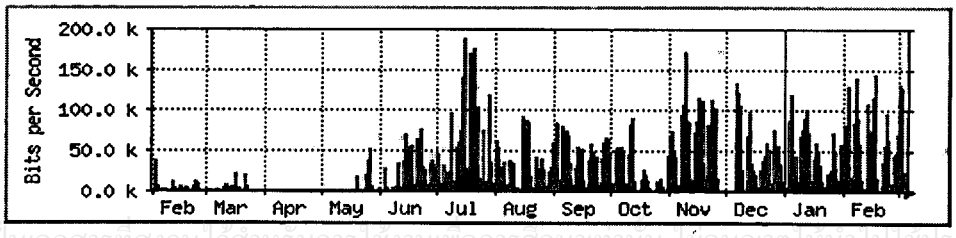
`Monthly' Graph (2 Hour Average)



Max In: 769.5 kb/s (0.8%) Average In: 57.6 kb/s (0.1%) Current In: 21.6 kb/s (0.0%)

Max Out: 239.5 kb/s (0.2%) Average Out: 17.8 kb/s (0.0%) Current Out: 10.4 kb/s (0.0%)

`Yearly' Graph (1 Day Average)



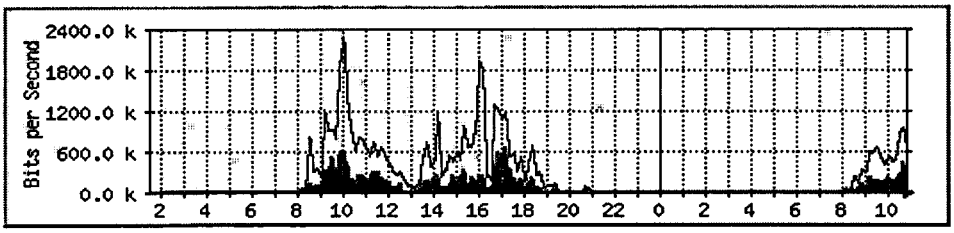
Max In: 188.6 kb/s (0.2%) Average In: 29.9 kb/s (0.0%) Current In: 92.9 kb/s (0.1%)

Max Out: 74.9 kb/s (0.1%) Average Out: 10.2 kb/s (0.0%) Current Out: 19.8 kb/s (0.0%)

รูปที่ 7.11 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Central Router 1

Traffic Analysis for Ethernet 0/0 of Central Router 2

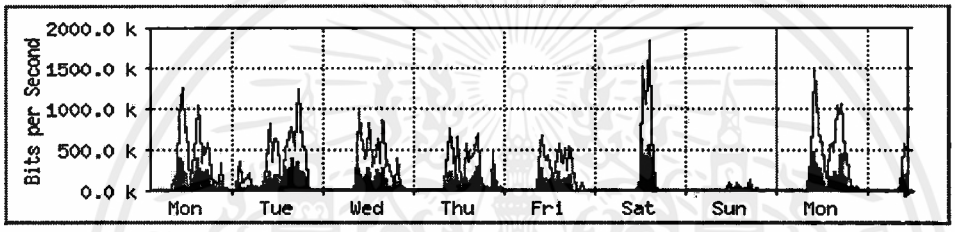
`Daily' Graph (5 Minute Average)



Max In: 673.3 kb/s (6.7%) Average In: 92.6 kb/s (0.9%) Current In: 302.3 kb/s (3.0%)

Max Out: 2253.1 kb/s (22.5%) Average Out: 250.9 kb/s (2.5%) Current Out: 628.2 kb/s (6.3%)

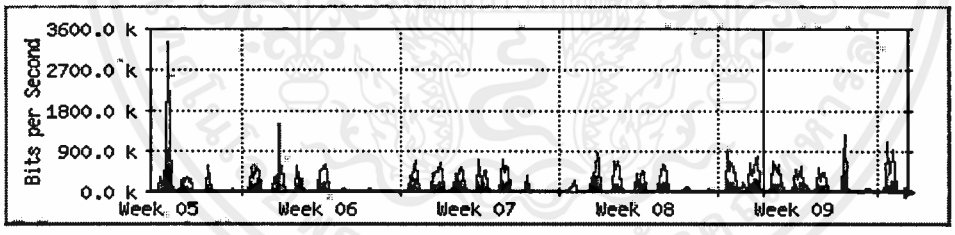
`Weekly' Graph (30 Minute Average)



Max In: 653.0 kb/s (6.5%) Average In: 79.5 kb/s (0.8%) Current In: 224.8 kb/s (2.2%)

Max Out: 1821.0 kb/s (18.2%) Average Out: 201.6 kb/s (2.0%) Current Out: 572.6 kb/s (5.7%)

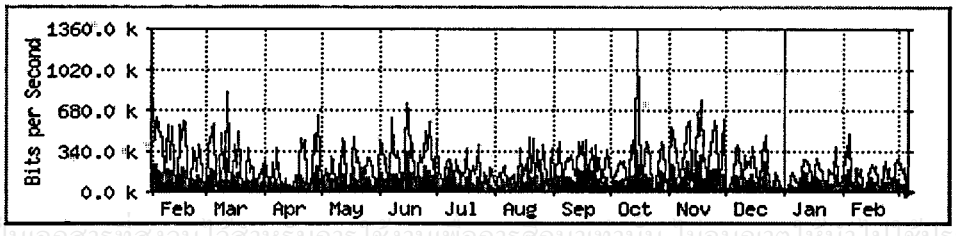
`Monthly' Graph (2 Hour Average)



Max In: 1519.1 kb/s (15.2%) Average In: 68.1 kb/s (0.7%) Current In: 37.5 kb/s (0.4%)

Max Out: 3306.6 kb/s (33.1%) Average Out: 147.8 kb/s (1.5%) Current Out: 85.4 kb/s (0.9%)

`Yearly' Graph (1 Day Average)



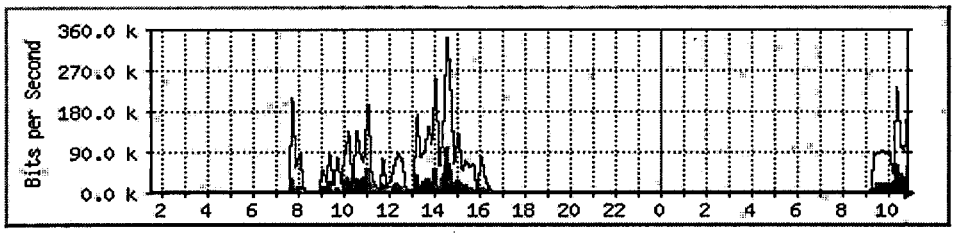
Max In: 363.7 kb/s (3.6%) Average In: 94.6 kb/s (0.9%) Current In: 87.6 kb/s (0.9%)

Max Out: 1343.7 kb/s (13.4%) Average Out: 220.8 kb/s (2.2%) Current Out: 256.0 kb/s (2.6%)

รูปที่ 7.12 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Central Router 2

Traffic Analysis for Ethernet 2/2 of Central Router 3

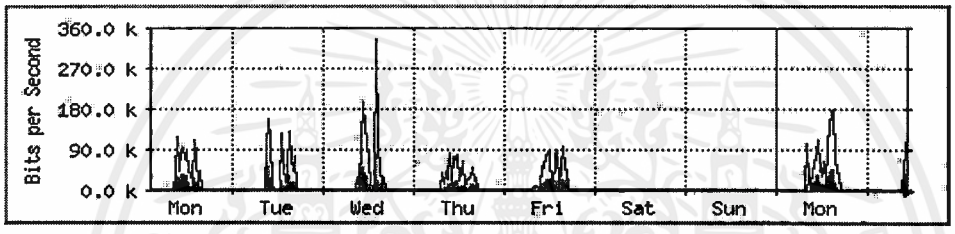
`Daily' Graph (5 Minute Average)



Max In: 104.4 kb/s (1.0%) Average In: 6920.0 b/s (0.1%) Current In: 62.3 kb/s (0.6%)

Max Out: 338.6 kb/s (3.4%) Average Out: 25.2 kb/s (0.3%) Current Out: 206.5 kb/s (2.1%)

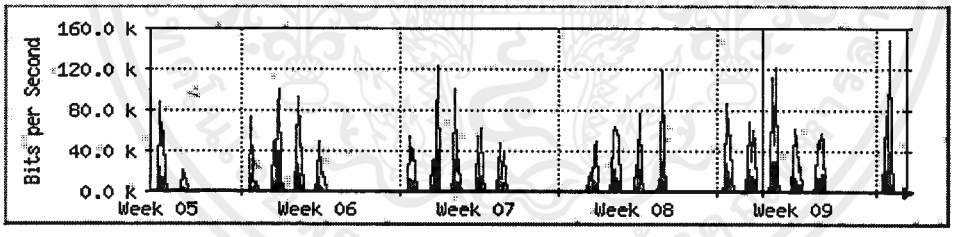
`Weekly' Graph (30 Minute Average)



Max In: 83.7 kb/s (0.8%) Average In: 4440.0 b/s (0.0%) Current In: 40.4 kb/s (0.4%)

Max Out: 333.6 kb/s (3.3%) Average Out: 15.4 kb/s (0.2%) Current Out: 126.7 kb/s (1.3%)

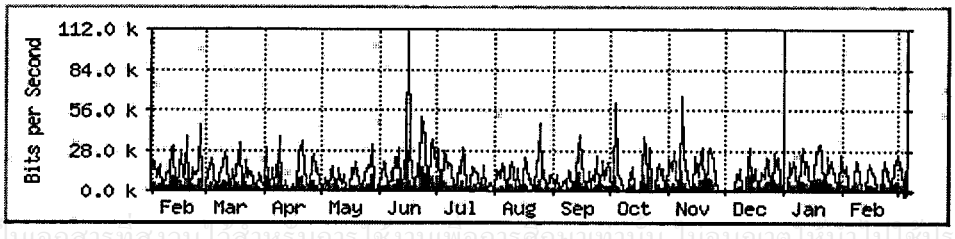
`Monthly' Graph (2 Hour Average)



Max In: 42.2 kb/s (0.4%) Average In: 2920.0 b/s (0.0%) Current In: 168.0 b/s (0.0%)

Max Out: 147.8 kb/s (1.5%) Average Out: 9848.0 b/s (0.1%) Current Out: 208.0 b/s (0.0%)

`Yearly' Graph (1 Day Average)



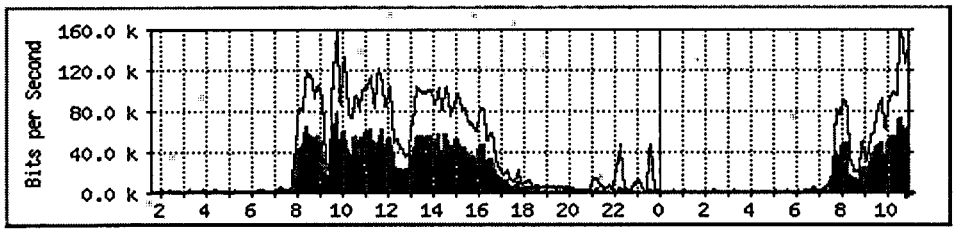
Max In: 27.8 kb/s (0.3%) Average In: 3232.0 b/s (0.0%) Current In: 7456.0 b/s (0.1%)

Max Out: 109.0 kb/s (1.1%) Average Out: 11.5 kb/s (0.1%) Current Out: 27.8 kb/s (0.3%)

รูปที่ 7.13 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Central Router 3

Traffic Analysis for Ethernet 0/0 of Central Router 4

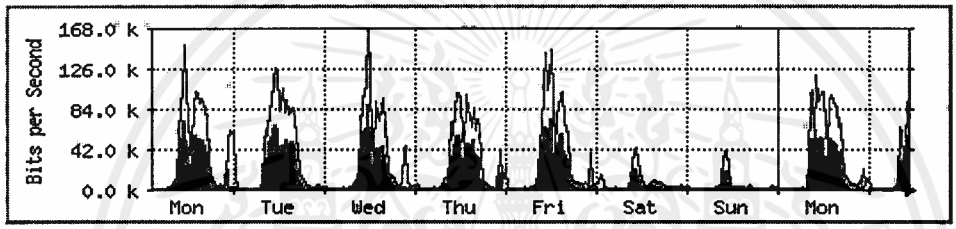
`Daily' Graph (5 Minute Average)



Max In: 78.8 kb/s (0.8%) Average In: 18.0 kb/s (0.2%) Current In: 64.9 kb/s (0.6%)

Max Out: 158.6 kb/s (1.6%) Average Out: 33.2 kb/s (0.3%) Current Out: 138.9 kb/s (1.4%)

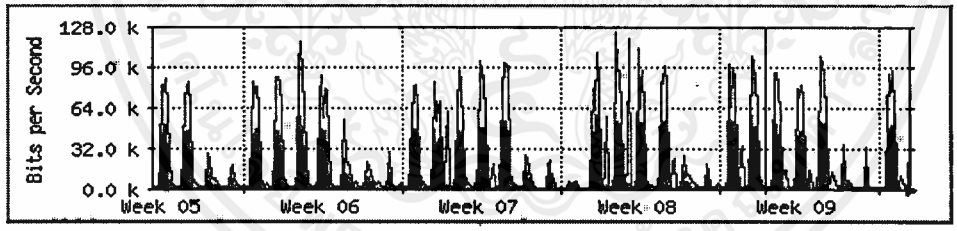
`Weekly' Graph (30 Minute Average)



Max In: 89.9 kb/s (0.9%) Average In: 14.5 kb/s (0.1%) Current In: 58.5 kb/s (0.6%)

Max Out: 164.9 kb/s (1.6%) Average Out: 26.8 kb/s (0.3%) Current Out: 105.5 kb/s (1.1%)

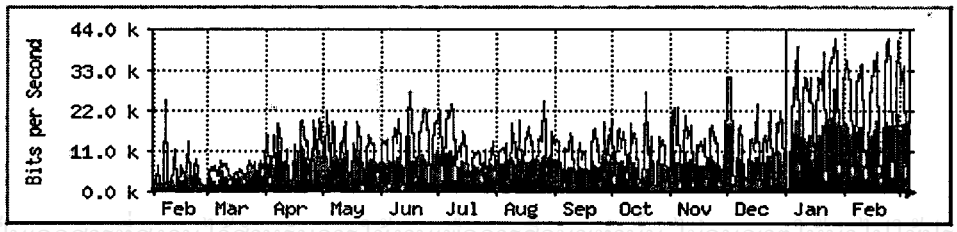
`Monthly' Graph (2 Hour Average)



Max In: 62.0 kb/s (0.6%) Average In: 12.4 kb/s (0.1%) Current In: 22.3 kb/s (0.2%)

Max Out: 124.0 kb/s (1.2%) Average Out: 23.6 kb/s (0.2%) Current Out: 40.4 kb/s (0.4%)

`Yearly' Graph (1 Day Average)



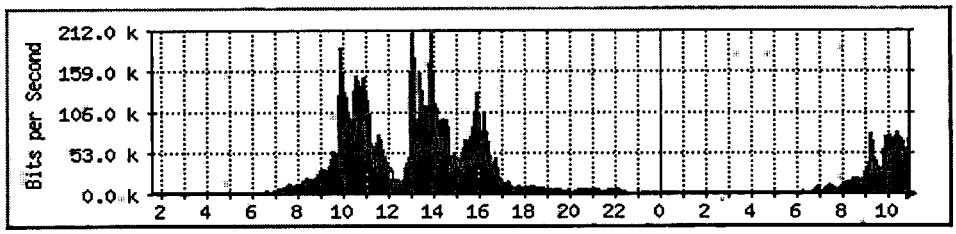
Max In: 28.2 kb/s (0.3%) Average In: 6808.0 b/s (0.1%) Current In: 18.2 kb/s (0.2%)

Max Out: 41.1 kb/s (0.4%) Average Out: 12.3 kb/s (0.1%) Current Out: 32.8 kb/s (0.3%)

รูปที่ 7.14 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Central Router 4

Traffic Analysis for Fddi 3/0 of Central Router 5

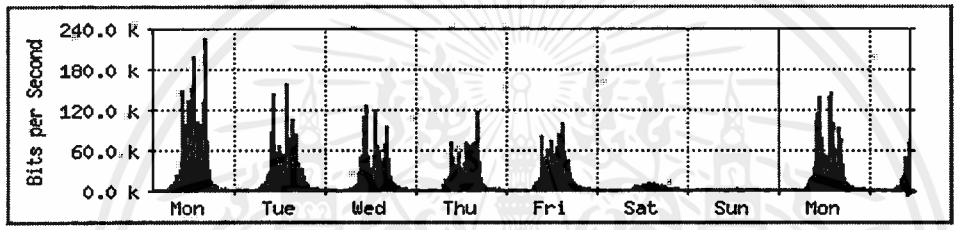
`Daily' Graph (5 Minute Average)



Max In: 209.1 kb/s (0.2%) Average In: 27.3 kb/s (0.0%) Current In: 72.1 kb/s (0.1%)

Max Out: 108.8 kb/s (0.1%) Average Out: 17.5 kb/s (0.0%) Current Out: 55.2 kb/s (0.1%)

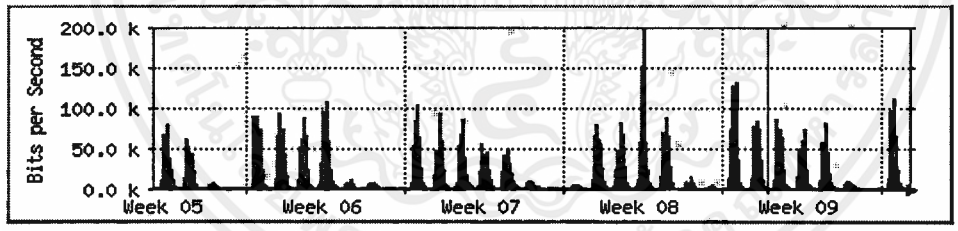
`Weekly' Graph (30 Minute Average)



Max In: 227.2 kb/s (0.2%) Average In: 22.5 kb/s (0.0%) Current In: 74.0 kb/s (0.1%)

Max Out: 95.9 kb/s (0.1%) Average Out: 14.2 kb/s (0.0%) Current Out: 53.8 kb/s (0.1%)

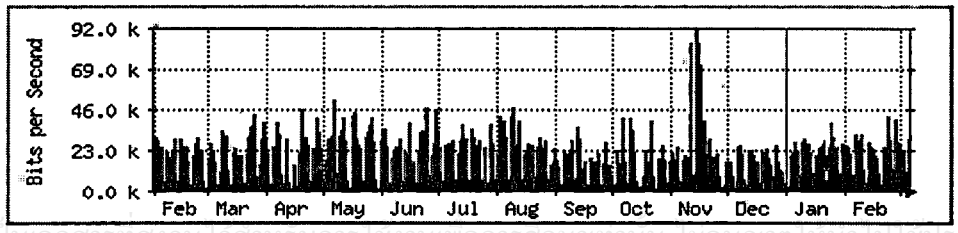
`Monthly' Graph (2 Hour Average)



Max In: 199.1 kb/s (0.2%) Average In: 19.1 kb/s (0.0%) Current In: 3272.0 b/s (0.0%)

Max Out: 66.3 kb/s (0.1%) Average Out: 11.7 kb/s (0.0%) Current Out: 2136.0 b/s (0.0%)

`Yearly' Graph (1 Day Average)



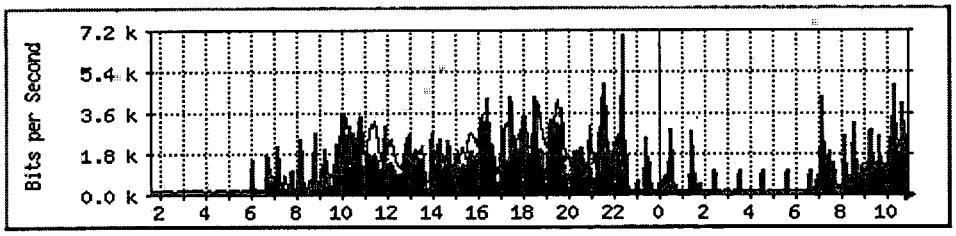
Max In: 91.9 kb/s (0.1%) Average In: 18.5 kb/s (0.0%) Current In: 30.3 kb/s (0.0%)

Max Out: 36.9 kb/s (0.0%) Average Out: 7784.0 b/s (0.0%) Current Out: 18.7 kb/s (0.0%)

รูปที่ 7.15 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Central Router 5

Traffic Analysis for Ethernet 0/0 of Central Router 6

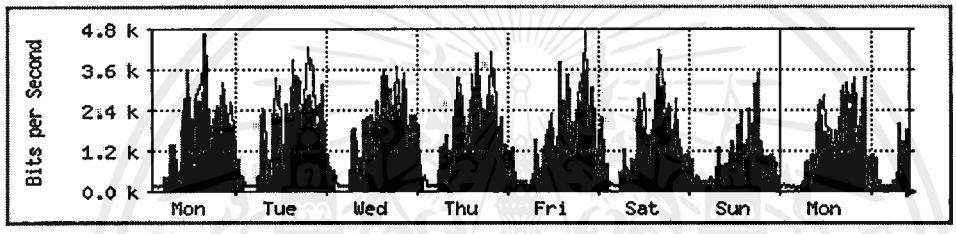
`Daily' Graph (5 Minute Average)



Max In: 6992.0 b/s (0.1%) Average 1200.0 b/s (0.0%) Current In: 2128.0 b/s (0.0%)

Max Out: 4176.0 b/s (0.0%) Average Out: 1120.0 b/s (0.0%) Current Out: 3192.0 b/s (0.0%)

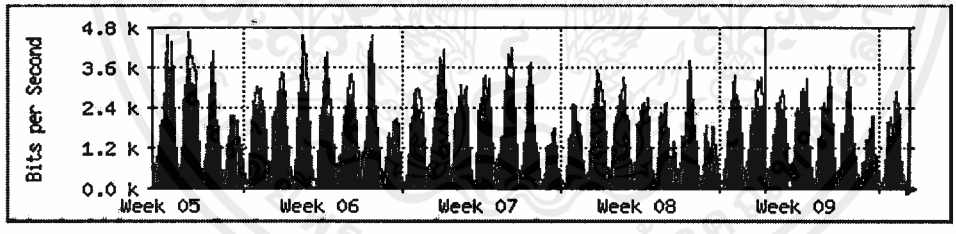
`Weekly' Graph (30 Minute Average)



Max In: 4696.0 b/s (0.0%) Average 1392.0 b/s (0.0%) Current In: 1568.0 b/s (0.0%)

Max Out: 4776.0 b/s (0.0%) Average Out: 1400.0 b/s (0.0%) Current Out: 1152.0 b/s (0.0%)

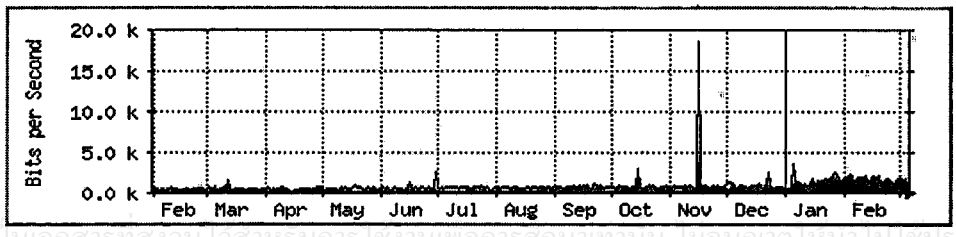
`Monthly' Graph (2 Hour Average)



Max In: 4376.0 b/s (0.0%) Average In: 1504.0 b/s (0.0%) Current In: 1384.0 b/s (0.0%)

Max Out: 4648.0 b/s (0.0%) Average Out: 1552.0 b/s (0.0%) Current Out: 1016.0 b/s (0.0%)

`Yearly' Graph (1 Day Average)



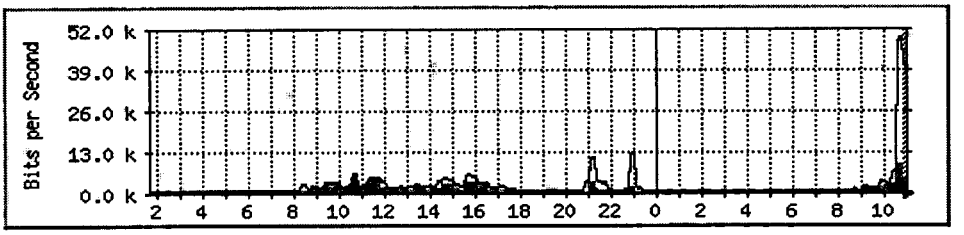
Max In: 3936.0 b/s (0.0%) Average In: 520.0 b/s (0.0%) Current In: 1024.0 b/s (0.0%)

Max Out: 18.4 kb/s (0.2%) Average Out: 800.0 b/s (0.0%) Current Out: 992.0 b/s (0.0%)

รูปที่ 7.16 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Central Router 6

Traffic Analysis for Ethernet 0/1 of Access Router 1

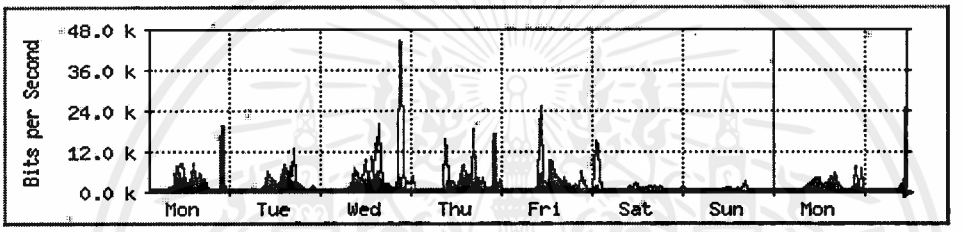
`Daily' Graph (5 Minute Average)



Max In: 9448.0 b/s (0.1%) Average In: 1232.0 b/s (0.0%) Current In: 4944.0 b/s (0.0%)

Max Out: 48.9 kb/s (0.5%) Average Out: 2392.0 b/s (0.0%) Current Out: 40.5 kb/s (0.4%)

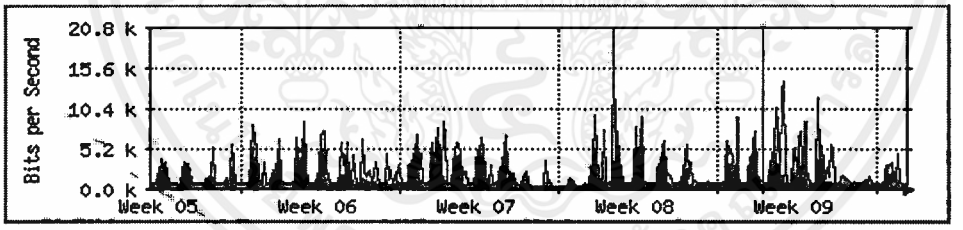
`Weekly' Graph (30 Minute Average)



Max In: 19.9 kb/s (0.2%) Average In: 1584.0 b/s (0.0%) Current In: 7192.0 b/s (0.1%)

Max Out: 44.5 kb/s (0.4%) Average Out: 2624.0 b/s (0.0%) Current Out: 44.5 kb/s (0.4%)

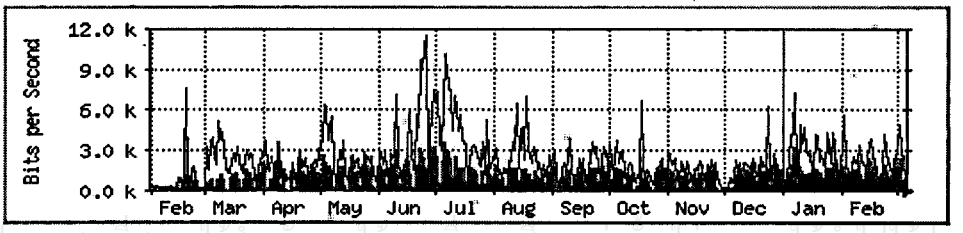
`Monthly' Graph (2 Hour Average)



Max In: 9520.0 b/s (0.1%) Average In: 1408.0 b/s (0.0%) Current In: 480.0 b/s (0.0%)

Max Out: 20.6 kb/s (0.2%) Average Out: 2208.0 b/s (0.0%) Current Out: 784.0 b/s (0.0%)

`Yearly' Graph (1 Day Average)



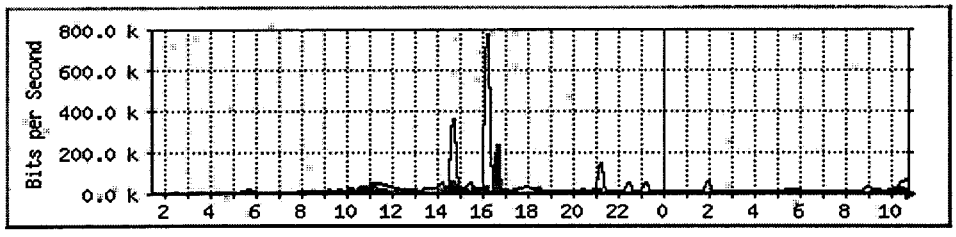
Max In: 3688.0 b/s (0.0%) Average In: 1104.0 b/s (0.0%) Current In: 1184.0 b/s (0.0%)

Max Out: 11.4 kb/s (0.1%) Average Out: 2312.0 b/s (0.0%) Current Out: 1592.0 b/s (0.0%)

รูปที่ 7.17 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Access Router 1

Traffic Analysis for Ethernet 0/1 of Access Router 2

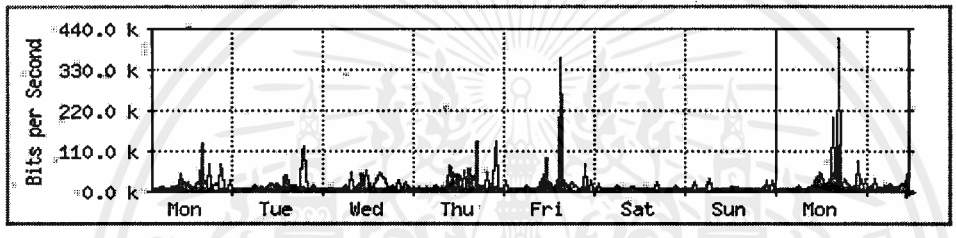
`Daily' Graph (5 Minute Average)



Max In: 240.0 kb/s (2.4%) Average In: 16.7 kb/s (0.2%) Current In: 31.4 kb/s (0.3%)

Max Out: 773.6 kb/s (7.7%) Average Out: 27.1 kb/s (0.3%) Current Out: 29.6 kb/s (0.3%)

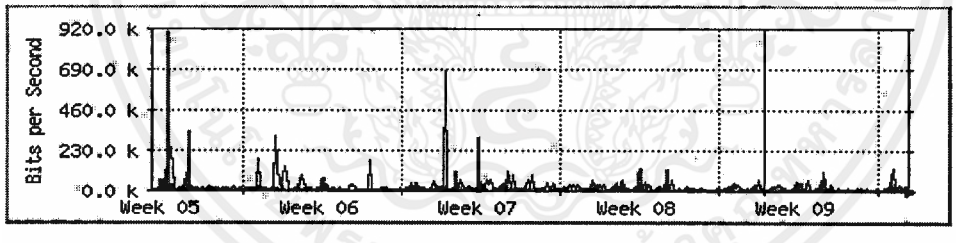
`Weekly' Graph (30 Minute Average)



Max In: 265.8 kb/s (2.7%) Average In: 12.5 kb/s (0.1%) Current In: 29.4 kb/s (0.3%)

Max Out: 412.0 kb/s (4.1%) Average Out: 18.6 kb/s (0.2%) Current Out: 52.1 kb/s (0.5%)

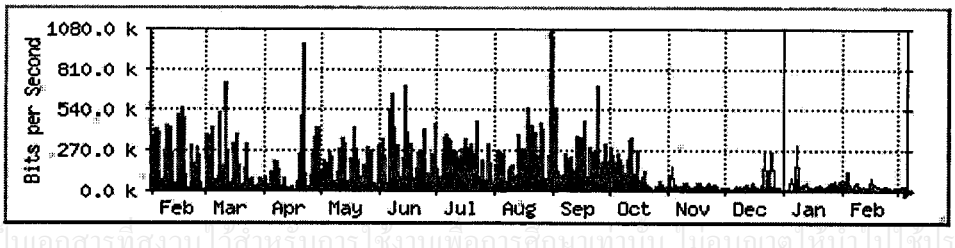
`Monthly' Graph (2 Hour Average)



Max In: 910.2 kb/s (9.1%) Average In: 17.8 kb/s (0.2%) Current In: 11.6 kb/s (0.1%)

Max Out: 672.3 kb/s (6.7%) Average Out: 23.9 kb/s (0.2%) Current Out: 14.2 kb/s (0.1%)

`Yearly' Graph (1 Day Average)



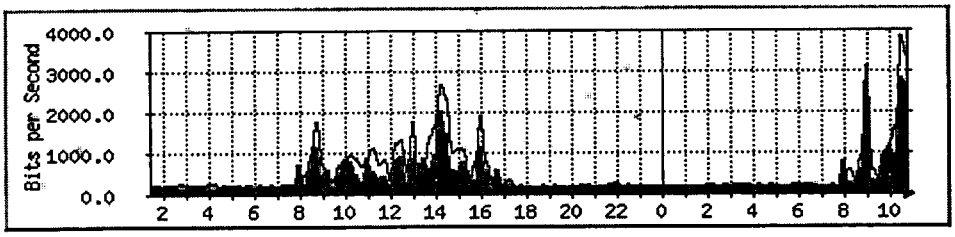
Max In: 1077.8 kb/s (10.8%) Average In: 146.8 kb/s (1.5%) Current In: 15.7 kb/s (0.2%)

Max Out: 335.0 kb/s (3.4%) Average Out: 65.2 kb/s (0.7%) Current Out: 26.3 kb/s (0.3%)

รูปที่ 7.18 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Access Router 2

Traffic Analysis for Serial 2/7 of Access Router 3

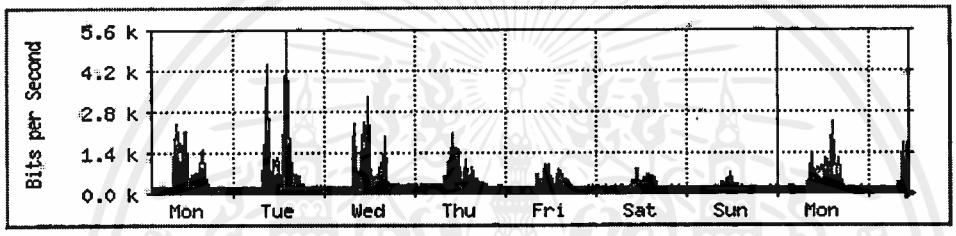
`Daily' Graph (5 Minute Average)



Max In: 2848.0 b/s (4.5%) Average In: 392.0 b/s (0.6%) Current In: 2720.0 b/s (4.2%)

Max Out: 3800.0 b/s (5.9%) Average Out: 504.0 b/s (0.8%) Current Out: 3368.0 b/s (5.3%)

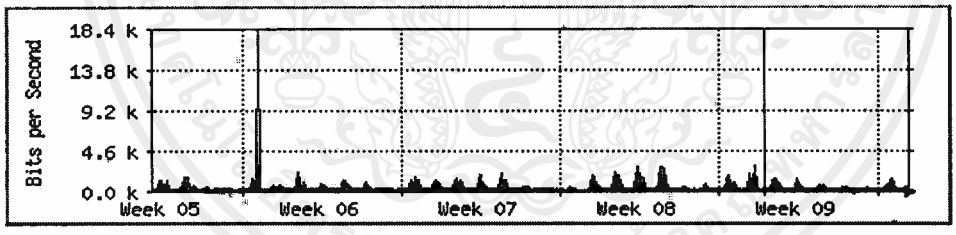
`Weekly' Graph (30 Minute Average)



Max In: 3984.0 b/s (6.2%) Average In: 368.0 b/s (0.6%) Current In: 1728.0 b/s (2.7%)

Max Out: 5584.0 b/s (8.7%) Average Out: 432.0 b/s (0.7%) Current Out: 2440.0 b/s (3.8%)

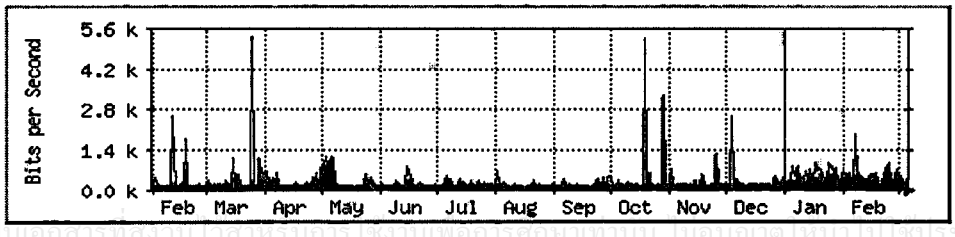
`Monthly' Graph (2 Hour Average)



Max In: 3168.0 b/s (5.0%) Average In: 376.0 b/s (0.6%) Current In: 584.0 b/s (0.9%)

Max Out: 18.0 kb/s (28.2%) Average Out: 480.0 b/s (0.8%) Current Out: 664.0 b/s (1.0%)

`Yearly' Graph (1 Day Average)



Max In: 3208.0 b/s (5.0%) Average In: 232.0 b/s (0.4%) Current In: 360.0 b/s (0.6%)

Max Out: 5288.0 b/s (8.3%) Average Out: 312.0 b/s (0.5%) Current Out: 488.0 b/s (0.8%)

รูปที่ 7.19 กราฟแสดงปริมาณทราฟฟิคที่เครือข่ายย่อยของ Access Router 3

บทที่ 8
บทสรุปและข้อเสนอแนะ

บทสรุป

การนำระบบเครือข่ายคอมพิวเตอร์มาใช้กับหน่วยงานขนาดใหญ่ โดยมีการออกแบบระบบเครือข่ายที่ดี มีการเลือกใช้อุปกรณ์หรือสื่อกลางต่างๆ ที่ได้มาตรฐานเหมาะสมกับประเภทของงาน และมีการติดตั้งระบบโดยทีมงานที่มีความรู้ ความสามารถในการปฏิบัติงาน จะทำให้ระบบเครือข่ายที่ติดตั้ง เป็นระบบเครือข่ายคอมพิวเตอร์ที่สมบูรณ์แบบ และมีประสิทธิภาพในการปฏิบัติงานสูง สามารถรองรับระบบงานหรือแอพพลิเคชันต่างๆ ที่ใช้ภายในระบบ ให้ทำงานได้อย่างต่อเนื่อง มีความถูกต้อง แม่นยำ และรวดเร็วในการประมวลผลข้อมูล ซึ่งสิ่งเหล่านี้จะส่งผลให้หน่วยงานนั้นๆ มีศักยภาพในการบริหารงาน และทำให้เกิดความเจริญก้าวหน้าในการพัฒนาประเทศ

จากการตรวจสอบทราฟฟิคบนระบบเครือข่ายที่เราเตอร์ทุกตัว จะได้ผลการตรวจสอบ ซึ่งเป็นกราฟแสดงสถิติของทราฟฟิคแบบรายวัน รายสัปดาห์ รายเดือนและรายปี จากกราฟนี้ทำให้ผู้ดูแลและบริหารระบบสามารถทราบถึง Bandwidth ที่ใช้ในระบบ, ปริมาณข้อมูลที่ผ่านเข้า-ออกในระบบ, ช่วงเวลาที่มีทราฟฟิคมาก, ช่วงเวลาที่มีทราฟฟิคน้อย หรือช่วงเวลาที่ไม่มีทราฟฟิคในระบบและสภาพโดยรวมทั่วๆไปของระบบ ซึ่งลักษณะเหล่านี้ถือเป็นรูปแบบของทราฟฟิค (Traffic Pattern) [8] สาเหตุของการเกิดทราฟฟิค ไม่ว่าจะมาจากเซิฟเวอร์, เวิคสเตชัน หรืออุปกรณ์เชื่อมต่อระบบสื่อสารต่างๆ รวมถึงโปรแกรมประยุกต์ที่ถูกนำมาใช้ในระบบ เมื่อผู้ดูแลและบริหารระบบทำความเข้าใจเกี่ยวกับรูปแบบของทราฟฟิค ที่เกิดขึ้นในระบบจะทำให้เกิดประโยชน์ คือ

1. สามารถที่จะทราบได้ว่าจะเกิด Bottlenecks ขึ้นที่ส่วนไหนของระบบ โดยสังเกตได้จากกราฟ ณ ช่วงเวลานั้นว่าปริมาณข้อมูลที่ผ่านเข้า-ออกจากเราเตอร์ มีค่าใกล้เคียงกับค่าสูงสุดของ Bandwidth บนระบบเครือข่ายหรือไม่ ถ้าใกล้เคียงแสดงว่าช่วงเวลานั้นกำลังเกิด Bottlenecks

2.สามารถที่จะรู้การเปลี่ยนแปลงที่เกิดขึ้นบนระบบได้อย่างรวดเร็ว

3. รู้ช่วงเวลาที่มีปริมาณทราฟฟิคสูงและต่ำที่เกิดขึ้นบนระบบ

4.สามารถวางแผนสำหรับการแก้ไข บำรุงรักษาระบบให้ดีขึ้น รวมถึงการขยายระบบเพิ่มเติมในอนาคต

5. สามารถที่จะกำหนดเวลาในการ Upgrade และบำรุงรักษาระบบตามวาระที่กำหนด (Routine Maintenance) โดยจะเลือกช่วงเวลาที่ระบบเครือข่ายมีการใช้งานน้อยหรือในช่วงเวลาที่เป็นวันหยุด แต่ถ้าระบบงานต้องทำงานตลอดเวลา เมื่อมีความจำเป็นที่จะต้องทำการ Upgrade หรือบำรุงรักษาระบบ ผู้ดูแลและบริหารระบบเครือข่าย จะต้องทำการกำหนดวันเวลาที่แน่นอน และประกาศให้หน่วยงานต่างๆ ที่มีความเกี่ยวข้องได้ทราบอย่างทั่วถึงก่อนปฏิบัติการ

แนวทางในการปรับปรุงและพัฒนาระบบเครือข่ายคอมพิวเตอร์ของกรมศุลกากร

1. เสนอการปรับปรุงระบบเครือข่ายโดยการ Upgrade เราเตอร์ให้สามารถบริการได้ทั้งข้อมูลและเสียง (Data and Voice)

สำหรับการ Upgrade ระบบเครือข่ายคอมพิวเตอร์ของกรมศุลกากรแนะนำให้ Upgrade อุปกรณ์เชื่อมโยงระบบเครือข่ายที่เป็นเราเตอร์ ทั้ง Central Router, Access Router และ Remote Router ที่เกี่ยวข้องกับการให้บริการ Remote Site ให้สามารถบริการได้ทั้งข้อมูลและเสียง เพื่อที่จะได้สามารถทำการเชื่อมโยงระบบโทรศัพท์และแฟกซ์ผ่านระบบเครือข่ายสื่อสาร ซึ่งเมื่อพิจารณาถึงการใช้งานระยะยาวในอนาคต จะทำให้ลดค่าใช้จ่ายจากค่าโทรศัพท์ทางไกลและค่าส่งแฟกซ์ทางไกลเป็นอย่างมาก

ลักษณะการเชื่อมโยงระบบโทรศัพท์และแฟกซ์ผ่านระบบเครือข่ายในปัจจุบันมีใช้กันอยู่ 3 แบบคือ

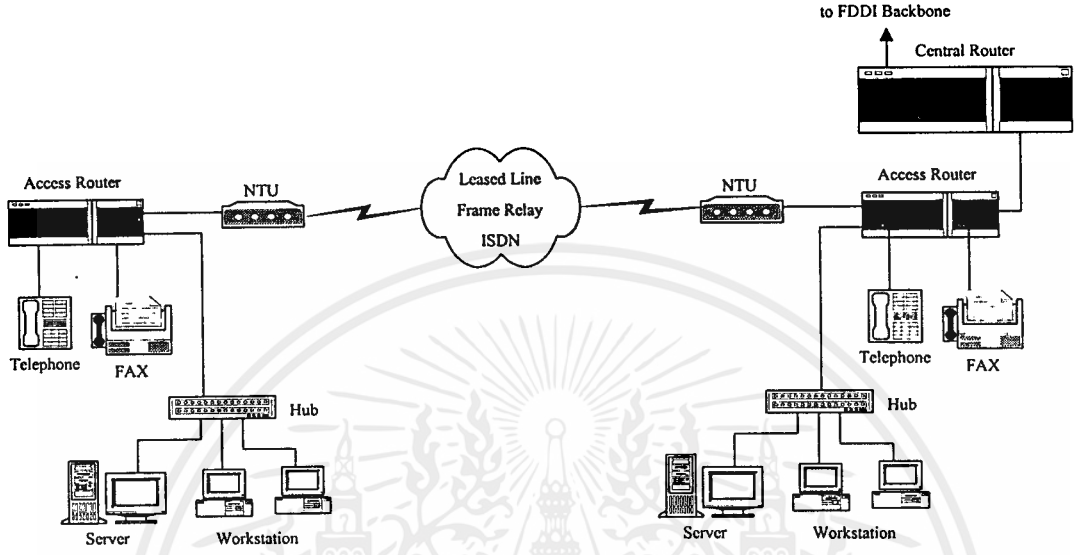
1. Direct Line

เป็นการเชื่อมโยงโดยการนำเครื่องโทรศัพท์และแฟกซ์มาต่อที่ Channel Voice ของอุปกรณ์เราเตอร์ทั้งฝั่งต้นทางและฝั่งปลายทาง ซึ่งมีวิธีการทำงานโดยถ้าฝั่งต้นทางยกหูโทรศัพท์ ฝั่งปลายทางจะได้ยินเสียงกระดิ่งของเครื่องโทรศัพท์ดัง และถ้าฝั่งปลายทางยกหูโทรศัพท์ก็สามารถสนทนาหรือส่งแฟกซ์ได้ทันที

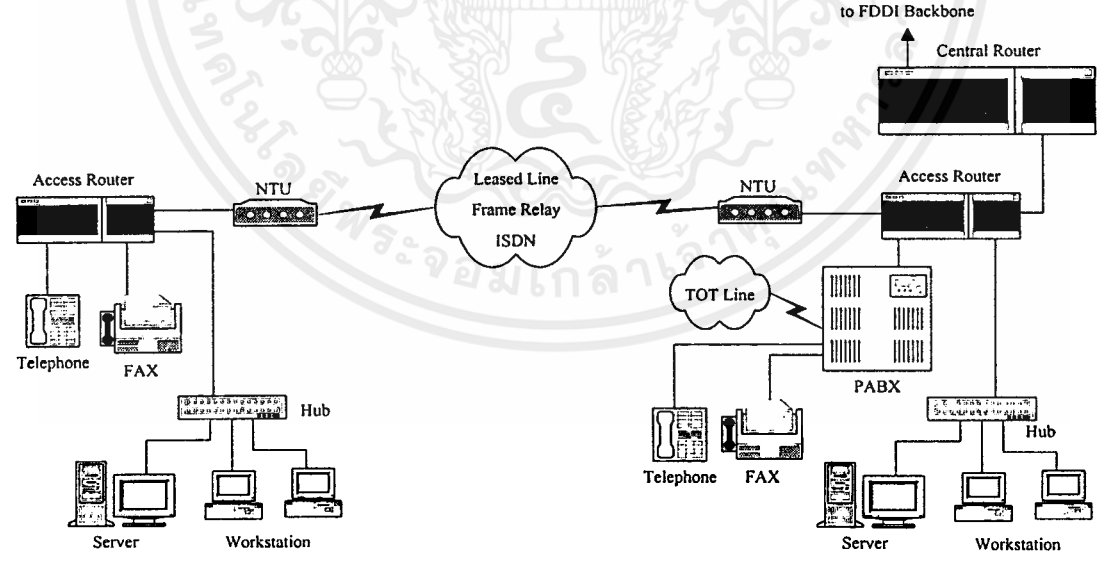
2. Remote Extension

เป็นวิธีการเชื่อมโยงระบบโดยการนำความสามารถของตู้ PABX มาต่อเชื่อมใช้งาน โดยนำ Extension (คู่สายภายใน) มาต่อที่ Channel Voice ของอุปกรณ์เราเตอร์ฝั่งต้นทางและนำเครื่องโทรศัพท์และแฟกซ์มาต่อที่ Channel Voice ของฝั่งปลายทาง ซึ่งมีวิธีการทำงานโดยถ้าฝั่งต้นทางยกหูโทรศัพท์แล้วกดหมายเลข Extension ที่กำหนดไว้ ที่ฝั่งปลายทางจะได้ยินเสียงกระดิ่งของเครื่องโทรศัพท์ดัง ถ้าฝั่งปลายทางยกหูก็สามารถสนทนาหรือส่งแฟกซ์ได้ และสามารถโอนสายไปยังหมายเลข Extension อื่นภายในสำนักงานที่กำหนดไว้ได้ ในทำนองเดียวกันฝั่งปลายทางยกหูโทรศัพท์แล้วกดหมายเลข Extension ที่กำหนดในฝั่งต้นทางหรือสำนักงานส่วนภูมิภาคอื่น จะได้ยินกระดิ่งของเครื่องโทรศัพท์ดัง ถ้ายกหูก็สามารถสนทนาหรือส่งแฟกซ์ได้ และถ้าฝั่งปลายทางยกหู

โทรศัพท์แล้วกด 9 ก็จะสามารถโทรศัพท์ออกคู่สายนอกของฝั่งต้นทางโดยจะสนทนานานเท่าไรก็ได้ จะเสียค่าใช้จ่ายเพียง 3 บาท



รูปที่ 8.1 แสดงการเชื่อมโยงระบบโทรศัพท์และแฟกซ์ผ่านระบบเครือข่ายแบบ Direct Line



รูปที่ 8.2 แสดงการเชื่อมโยงระบบโทรศัพท์และแฟกซ์ผ่านระบบเครือข่ายแบบ Remote Extension

3. Tie Line (Trunk to Trunk)

เป็นวิธีการเชื่อมโยงโดยนำตู้ PABX ทั้งฝั่งต้นทางและฝั่งปลายทางเชื่อมโยงเข้าหากัน โดยแบ่งวิธีการเชื่อมโยงคู่สายได้ 2 วิธีคือ

3.1 2 Wire E&M ซึ่งจะใช้คู่สายทองแดงจำนวน 4 เส้น โดยแบ่งออกเป็นคู่รับ (RX) คู่ส่ง (TX) ในสายคู่เดียวกันจำนวน 2 เส้น และสัญญาณในการยกหู (E) จำนวน 1 เส้น สัญญาณในการวางหู (M) จำนวน 1 เส้น ซึ่งเชื่อมโยงมาจากตู้ PABX โดยในตู้ PABX จะต้องมี Card Tie Line เชื่อมโยงมายัง Channel E&M Voice ของอุปกรณ์เราเตอร์

3.2 4 Wire E&M ซึ่งจะใช้คู่สายทองแดงจำนวน 6 เส้น โดยแบ่งออกเป็นคู่รับ (RX) จำนวน 2 เส้น และคู่ส่ง (TX) จำนวน 2 เส้นในสายคู่เดียวกันจำนวน 2 เส้น และสัญญาณในการยกหู (E) จำนวน 1 เส้น สัญญาณในการวางหู (M) จำนวน 1 เส้น ซึ่งเชื่อมโยงมาจากตู้ PABX โดยในตู้ PABX จะต้องมี Card Tie Line เชื่อมโยงมายัง Channel E&M Voice ของอุปกรณ์เราเตอร์

วิธีการต่อเชื่อมโยงระบบโทรศัพท์แบบ Tie Line สมควรเลือกแบบ 4 Wire E&M เพราะว่าแยกคู่รับ (RX) และคู่ส่ง (TX) คนละคู่สายทองแดงกัน ซึ่งจะทำให้ไม่มีการรบกวนสัญญาณในขณะใช้งานคู่สายโทรศัพท์ผ่านระบบเครือข่าย ซึ่งมีวิธีการโดยถ้าฝั่งต้นทางทำการยกหูโทรศัพท์แล้วกดสัญญาณ Digi Tone ที่กำหนดไว้ในการเชื่อมโยงกับฝั่งปลายทางแล้วกดหมายเลข Extension (คู่สายภายใน) ของตู้ PABX ฝั่งปลายทางก็จะสามารถสนทนาหรือส่งแฟกซ์ได้ทันที และถ้าฝั่งต้นทางกดสัญญาณ Digi Tone แล้วกด 9 ก็จะได้สัญญาณของคู่สายตอนนอกของตู้ PABX ฝั่งปลายทาง โดยจะสามารถโทรศัพท์ออกไปภายนอกสำนักงานนานเท่าไรก็ได้จะเสียค่าใช้จ่ายเพียง 3 บาท ในทำนองเดียวกันถ้าฝั่งปลายทางทำการยกหูโทรศัพท์แล้วกดสัญญาณ Digi Tone ที่กำหนดไว้ในการเชื่อมโยงกับฝั่งต้นทางแล้วกดหมายเลข Extension (คู่สายภายใน) ของตู้ PABX ฝั่งต้นทาง ก็จะสามารถสนทนาหรือส่งแฟกซ์ได้ทันที และถ้าฝั่งปลายทางกดสัญญาณ Digi Tone แล้วกด 9 ก็จะได้สัญญาณของคู่สายตอนนอกของตู้ PABX ฝั่งต้นทาง โดยจะสามารถโทรศัพท์ออกไปภายนอกสำนักงานนานเท่าไรก็ได้ จะเสียค่าใช้จ่ายเพียง 3 บาท

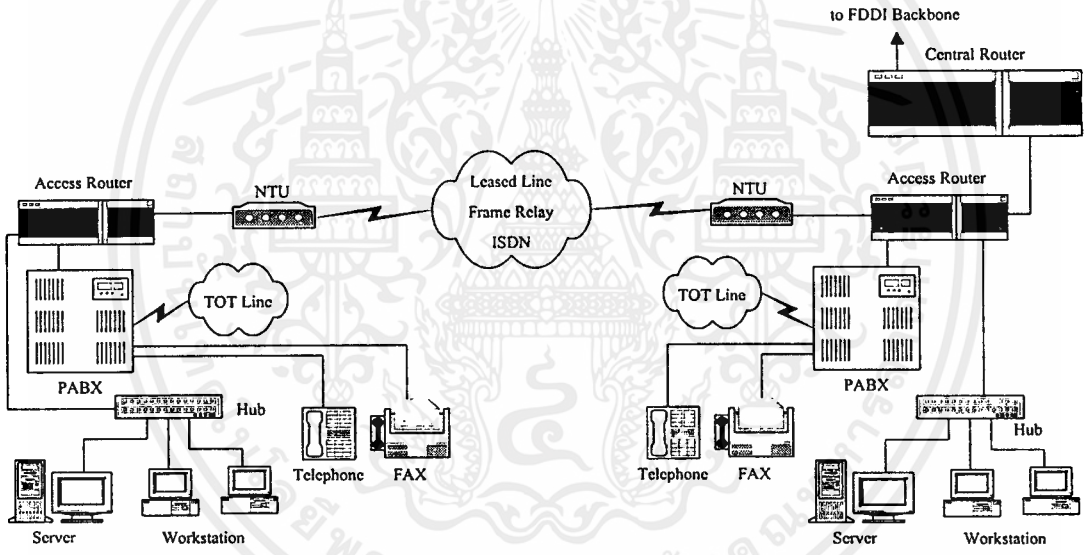
จากวิธีการเชื่อมโยงระบบโทรศัพท์และแฟกซ์ผ่านระบบเครือข่ายทั้ง 3 แบบแนะนำให้ใช้การเชื่อมต่อใช้งานในลักษณะ Remote Extension เพราะง่ายต่อการติดตั้งระบบและมีความยืดหยุ่นในการใช้งาน โดยใช้ความสามารถในการทำงานของตู้ PABX เดิมที่มีการใช้งานอยู่ในปัจจุบัน เพื่อให้ง่ายต่อการใช้งานและการบำรุงรักษา ควรใช้การเชื่อมโยงระบบจากตู้ PABX มายังอุปกรณ์เราเตอร์ที่ติดตั้งอยู่ที่ศูนย์คอมพิวเตอร์หลัก ในการเชื่อมโยงระบบโทรศัพท์และแฟกซ์ไปที่สำนักงานในส่วนภูมิภาคโดยผ่านคู่สายวงจรเช่าความเร็วสูงนั้น สามารถเชื่อมโยง Voice Channel ผ่านอุปกรณ์ Access Router ได้ทั้งเครื่องโทรศัพท์และแฟกซ์โดยที่ไม่มีผลกระทบต่อการใช้ระบบงาน Application ต่างๆ รวมถึงการใช้งาน Internet และการรับส่ง Mail

ประโยชน์ที่จะได้รับจากการเชื่อมโยงระบบโทรศัพท์ผ่านระบบเครือข่ายสื่อสารคอมพิวเตอร์คือ

1. ทำให้ประหยัดงบประมาณค่าใช้จ่ายในการใช้โทรศัพท์ทางไกลและแฟกซ์ โดยการติดต่อโทรศัพท์และแฟกซ์ในแต่ละครั้งจะไม่เสียค่าใช้จ่าย และไม่จำกัดเวลาในการใช้งานแต่ละครั้ง

2 กรมศุลกากรในส่วนภูมิภาคสามารถติดต่อโทรศัพท์และแฟกซ์ กับหน่วยงานราชการต่างๆ ภายนอกกรมศุลกากร(กรุงเทพฯ) โดยจะโทรติดต่องานนานเท่าไรก็ได้ จะเสียค่าใช้จ่ายครั้งละ 3 บาท

3. หน่วยงานราชการต่างๆ สามารถติดต่อโทรศัพท์และแฟกซ์ กับกรมศุลกากรในส่วนภูมิภาค โดยการโทรศัพท์มาที่กรมศุลกากรในกรุงเทพฯ แล้วโอนสายติดต่อไปยังกรมศุลกากรในส่วนภูมิภาคโดยเสียค่าใช้จ่ายครั้งละ 3 บาท



รูปที่ 8.3 แสดงการเชื่อมโยงระบบโทรศัพท์และแฟกซ์ผ่านระบบเครือข่ายแบบ Tie Line

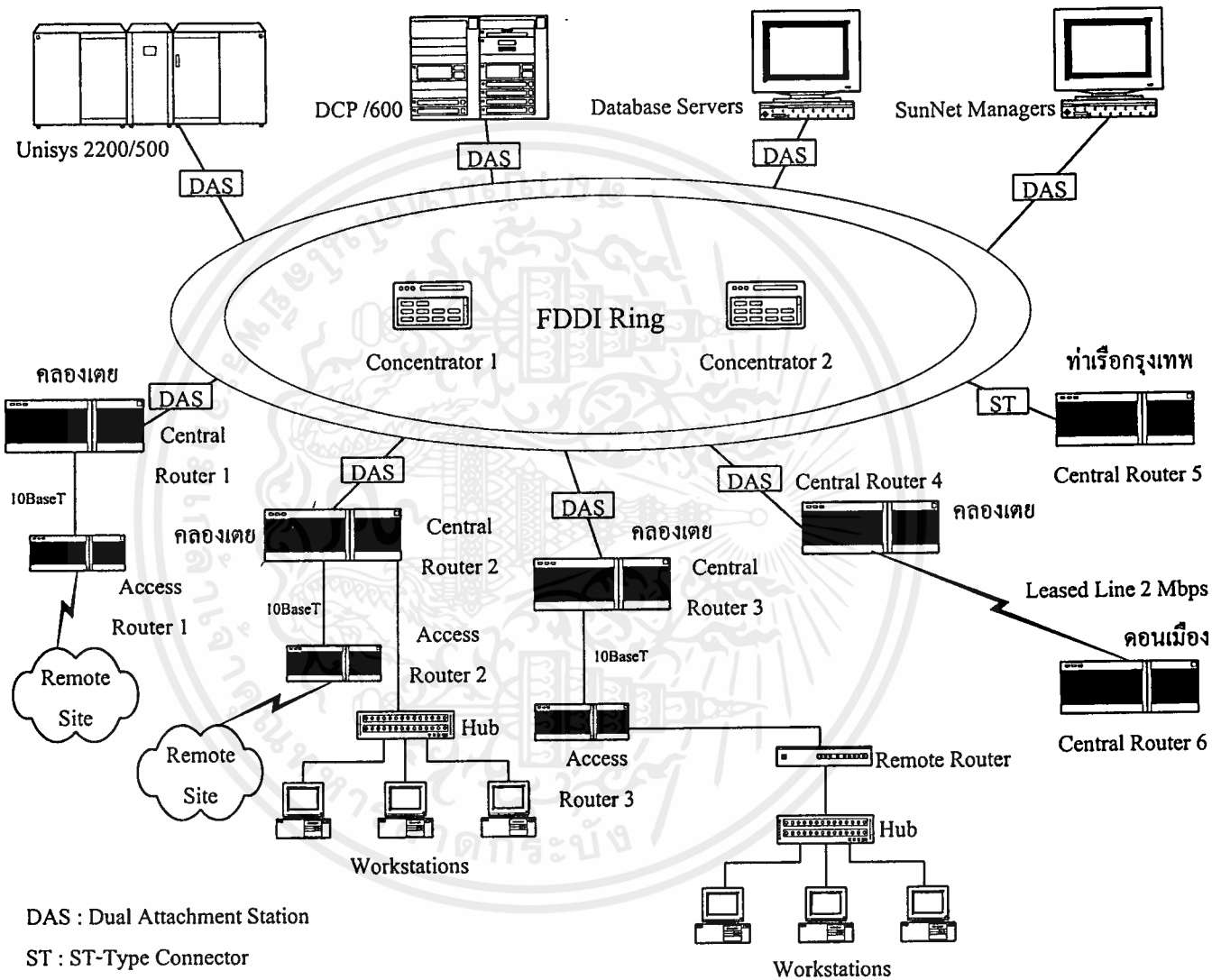
2. จุดที่น่าจะปรับปรุงในการเชื่อมต่อเราเตอร์ในระบบเครือข่ายคอมพิวเตอร์

จากการพิจารณารูปที่ 6.1 ที่แสดงส่วนประกอบคอมพิวเตอร์หลักของระบบเครือข่าย จะสังเกตเห็นว่า Central Router 4 เป็นเราเตอร์ที่รับภาระและมีความสำคัญมากกว่าเราเตอร์ตัวอื่นๆ เพราะต้องคอยให้บริการ การเชื่อมต่อกับ Central Router 6 จากกรมศุลกากรดอนเมืองและเชื่อมต่อกับ Access Router อีก 3 ตัวที่เป็นเราเตอร์สำหรับให้บริการกับ Remote Site จากการวิเคราะห์ระบบเครือข่ายเมื่อระบบการทำงานของ Central Router 4 เกิดปัญหาหรือข้อขัดข้องต่างๆ (Hardware Error or System Down) ในการที่จะตรวจสอบหรือหาสาเหตุการขัดข้องที่เกิดขึ้นกับตัวเราเตอร์จะมีผลทำให้การเชื่อมต่อจากกรมศุลกากรดอนเมืองและการให้บริการกับ Remote Site ต่างๆ

ทั่วประเทศต้องถูกตัดขาดจากเครือข่ายภายนอก (WAN) ซึ่งจะทำให้เกิดความเสียหายในการปฏิบัติงานได้ แนะนำการแก้ไขปัญหานี้โดยควรที่จะมีการเฉลี่ยหรือแบ่งภาระและความสำคัญของ Central Router 4 ไปให้กับ Central Router ตัวอื่นๆ ตัวอย่างเช่น เชื่อมต่อ Access Router 1 กับ Central Router 1, เชื่อมต่อ Access Router 2 กับ Central Router 2, เชื่อมต่อ Access Router 3 กับ Central Router 3 สำหรับ Central Router 6 เชื่อมต่อกับ Central Router 4 เหมือนเดิม ลักษณะการเชื่อมต่อเราเตอร์แบบนี้ จะไม่ทำให้เราเตอร์ตัวใดตัวหนึ่งมีความสำคัญหรือต้องรับภาระมากเกินไป และอีกสิ่งหนึ่งที่ควรพิจารณาคือความเป็นไปได้และความเหมาะสมในการเชื่อมต่อระหว่างเราเตอร์ด้วย ถ้าสามารถทำการเชื่อมต่อเราเตอร์ตามที่ยกตัวอย่างได้ จะทำให้ประสิทธิภาพในการรับส่งข้อมูลของระบบเครือข่ายดีขึ้น

3. วิเคราะห์การออกแบบระเครือข่ายคอมพิวเตอร์ที่ใช้งานอยู่ในปัจจุบัน

ในขณะที่ทำการวิเคราะห์และตรวจสอบปริมาณทราฟฟิคบนระบบเครือข่ายของกรมศุลกากร มีเซิฟเวอร์เชื่อมต่ออยู่ในระบบประมาณ 100 เครื่อง, เวิคสเตชันประมาณ 1300 เครื่อง และเครื่องพิมพ์ประมาณ 700 เครื่องและระบบแอพพลิเคชันต่างๆ มีการใช้งานประมาณ 85 เปอร์เซ็นต์ เมื่อทำการวิเคราะห์ปริมาณทราฟฟิคที่ตรวจสอบได้จากกราฟแบบรายวัน รายสัปดาห์ รายเดือนและรายปี ของกราฟแสดงปริมารทราฟฟิคโดยรวมของ Central Router ทั้ง 6 ตัวและ Access Router อีก 3 ตัว พบว่าปริมาณทราฟฟิคโดยเฉลี่ยทั้งปริมาณทราฟฟิคที่ผ่านเข้าเราเตอร์และปริมาณทราฟฟิคที่ออกจากเราเตอร์มีปริมาณที่น้อยมาก ค่าเฉลี่ยสูงสุดที่ตรวจสอบได้เป็นค่าเฉลี่ยของรูปที่ 7.3 ซึ่งแสดงปริมาณทราฟฟิคโดยรวมของ Central Router 2 ในรูปของกราฟแบบราบวันที่มีค่า Average In และ Average Out เท่ากับ 5.2 เปอร์เซ็นต์ สาเหตุที่เป็นเช่นนี้น่าจะมาจากการออกแบบระบบเครือข่ายที่ใช้อุปกรณ์เชื่อมต่อระบบเครือข่ายที่เป็นเราเตอร์มากเกินความจำเป็น (Over Design) แนะนำการแก้ไขปัญหานี้โดยลดจำนวนอุปกรณ์เชื่อมต่อระบบเครือข่ายที่เป็นเราเตอร์ลง โดยเครื่องเราเตอร์ที่ลดลงนี้สามารถที่นำไปใช้ประโยชน์สำหรับโครงการอื่นหรือระบบงานอื่นได้ เมื่อทำการลดจำนวนเราเตอร์ลงแล้วให้ทำการเพิ่ม Interface Port กับเราเตอร์ที่เหลืออยู่ให้เพียงพอต่อความต้องการที่จะเชื่อมต่อกับเครือข่ายย่อยต่างๆ ให้สามารถทำงานได้ตามปกติ



รูปที่ 8.4 แสดงการเฉลี่ยภาระของ Central Router 4 ให้กับ Central Router 1,2 และ 3

ข้อเสนอแนะ

ในการออกแบบติดตั้งระบบเครือข่ายคอมพิวเตอร์ขนาดใหญ่ควรมีการพิจารณาในการเตรียมสถานที่ที่ใช้ในการติดตั้งระบบต่างๆ , การเลือกอุปกรณ์สื่อสารข้อมูลที่ใช้ในระบบเครือข่าย และการเตรียมงานหรือติดต่อประสานงานก่อนเข้าปฏิบัติงานจริง ซึ่งสามารถแยกได้ดังนี้คือ

การจัดเตรียมสถานที่ติดตั้งระบบ

การจัดเตรียมสถานที่ที่ติดตั้งโฮสคอมพิวเตอร์ (Host Computer or Main Frame), อุปกรณ์ต่อพ่วง และอุปกรณ์สื่อสาร ที่ใช้เป็นศูนย์คอมพิวเตอร์ประมวลผลหลัก

1. สถานที่ที่ใช้ในการติดตั้ง ต้องมีขนาดใหญ่เพียงพอที่จะรองรับการติดตั้งอุปกรณ์ทั้งหมดได้
2. สำหรับห้องควบคุมระบบนี้มีความสำคัญอย่างมาก ควรจัดทำระบบรักษาความปลอดภัยเพื่ออนุญาตให้ผู้ที่มีส่วนเกี่ยวข้องเท่านั้นที่สามารถเข้า-ออกห้องนี้ได้
3. จัดทำระบบป้องกันอัคคีภัย
4. ติดตั้งระบบปรับอากาศ และติดตั้งอุปกรณ์ตรวจวัดความชื้น
5. ติดตั้งระบบไฟฟ้ากำลังและระบบแสงสว่าง ให้ได้มาตรฐานตามที่เครื่องต้องการ
6. ทำการวัดค่าสัญญาณต่างๆ เช่น สัญญาณรบกวนจากสนามแม่เหล็ก, สัญญาณรบกวนจากสถานีรับส่งต่างๆ และสัญญาณรบกวนจากระบบไฟฟ้ากำลัง เป็นต้น เพราะสัญญาณเหล่านี้ ถ้ามีมากเกินข้อกำหนดที่เครื่องสามารถรับได้ จะทำให้เครื่องและระบบควบคุมต่างๆ ทำงานผิดพลาดได้

รายละเอียดตามข้อต่างๆที่ได้กล่าวมาแล้วนั้น ควรศึกษาเพิ่มเติมจากคู่มือการจัดเตรียมและติดตั้งของเครื่องรุ่นนั้นๆ จะเป็นประโยชน์มากที่สุด เพราะเครื่องแต่ละรุ่น แต่ละยี่ห้อ จะมีการออกแบบความต้องการในการติดตั้งที่แตกต่างกันไป

การพิจารณาเลือกเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสาร

ข้อควรพิจารณาในการเลือกโฮสคอมพิวเตอร์

การเลือกโฮสคอมพิวเตอร์ ให้เหมาะสมกับระบบงาน มีหลักการในการพิจารณา คือ

1.ความสามารถในการเชื่อมต่อกับระบบงานเดิม และระบบงานที่จะขยายเพิ่มเติมในอนาคต

2.โฮสคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต้องมีความสามารถในการปฏิบัติงาน มีความเชื่อถือได้ของระบบสูง และมีความสามารถในการรองรับระบบงานทั้งหมดได้

3. สามารถรองรับจำนวน ออนไลน์ยูสเซอร์ ได้ตามที่กำหนด

4. ความสามารถในการ Access Application ของระบบ
5. มีช่วงเวลาในการประมวลผลที่เหมาะสมตามที่กำหนด (Processing Transaction)
6. ลักษณะของการจัดเก็บข้อมูล (Data Storage)
7. ลักษณะของระบบงาน และปริมาณของระบบงาน

นอกจากข้อต่างๆ ที่ได้กล่าวมาแล้วนั้น ผู้ออกแบบระบบสามารถหาข้อมูลเพิ่มเติมได้จากรายละเอียดในความต้องการของระบบงานที่กำลังออกแบบอยู่ หรือศึกษาจากหน่วยงานอื่นๆ ที่มีการติดตั้งระบบที่เสร็จสมบูรณ์แล้ว [10]

ข้อควรพิจารณาในการเลือกอุปกรณ์สื่อสารข้อมูล

Access Router และ Remote Router

1. Support Network Protocols ที่เป็นมาตรฐาน เช่น
   - IP (Internet Protocol)
   - PPP (Point-to-Point Protocol)
   - X.25
   - โปรโตคอลอื่นๆ ที่ระบบต้องการ
2. Support Routing Protocols ที่เป็นมาตรฐาน เช่น
   - RIP (Routing Information Protocol)
   - OSPF (Open Shortest Path First)
   - EGP (Exterior Gateway Protocol)
   - BGP (Border Gateway Protocol)
3. Support การจัดการเครือข่ายที่เป็นมาตรฐาน เช่น
   - SNMP (Simple Network Management Protocol)
   - MIB II (Management Information Base Version 2)
4. มีอีเทอร์เน็ตพอร์ท (Ethernet Port) และแวนพอร์ท (WAN Port) เพียงพอต่อความต้องการของระบบ
5. สามารถทำการ Configure และ Maintain จาก Remote ได้

Central Route

Central Router จะมีหลักการพิจารณาเหมือน Access Router และ Remote Router แต่มีข้อที่ควรพิจารณาเพิ่มเติม คือ

1. Support Bridge Function ที่เป็น มาตรฐาน เช่น Translational Bridging บน FDDI เพื่อรองรับโปรโตคอล เช่น Net BIOS หรือ Net BEUI (Net BIOS Extended User Interface)
2. เราเตอร์แต่ละชุด ต้องมีจำนวนพอร์ท เหมาะสมกับเครือข่ายที่ออกแบบ และสามารถขยายจำนวนแวนพอร์ท และอีเทอร์เน็ตพอร์ทได้
3. แต่ละพอร์ทต้องมีความสามารถในการกรองแพคเก็ตที่ไม่ต้องการ ไม่ให้เข้าสู่ใน Backbone ได้
4. สามารถสร้างและปรับปรุงเปลี่ยนแปลง Routing Table ได้โดยอัตโนมัติและโดยผู้ควบคุมระบบ
5. มี RS-232 Port เพื่อทำการ Setup และปรับปรุงเปลี่ยนแปลง Configuration ผ่านเทอมินอล
6. สามารถสับเปลี่ยนอุปกรณ์ในเราเตอร์ และ I/O พอร์ทโดยไม่ต้องปิดเครื่อง
7. ควรมี Redundant Power Supply

Modem

1. Support การ Modulation มี Error Control และ Data Compression ตามมาตรฐาน CCITT
2. สามารถใช้ได้กับสายโทรศัพท์ประเภท Leased line ทั้งระบบ 2 เส้น และ 4 เส้น และ Public Switched Line
3. สามารถที่จะหมุนโทรศัพท์และตอบรับโดยอัตโนมัติ (Auto Dial / Auto Answer) และหมุนโทรศัพท์ได้ทั้งแบบ Tone และ Pulse
4. สามารถลดและเพิ่มความเร็วในการรับส่งข้อมูลโดยอัตโนมัติขึ้นอยู่กับสภาพของ Connection
5. สามารถทำงานได้ทั้งการสื่อสารแบบ Synchronous และ Asynchronous
6. สามารถทำการทดสอบการทำงานของตนเองได้โดย Local Analog Loopback, Local Digital Loopback, Remote Digital Loopback และ End-to-End Test
7. สามารถทำ Automatic Auto Dial Backup ได้

Hub

1 Support การจัดการเครือข่ายที่เป็นมาตรฐาน เช่น

SNMP (Simple Network Management Protocol)

MIB II (Management Information Base Version 2)

2.มีจำนวนพอร์ท (เช่น 10Base F และ 10Base T) เพียงพอต่อการใช้งาน

3. ถ้าสามารถทำการ Configure ได้ จะเป็นการสะดวกต่อการควบคุมดูแล

ข้อแนะนำในการปฏิบัติงานเกี่ยวกับการติดตั้งระบบเครือข่าย

1. ควรจัดให้ทุกทีมงานมีการประชุมกันอย่างสม่ำเสมอ เพื่อจะได้ทราบถึงความก้าวหน้าของงาน ปัญหาต่างๆ ที่เกิดขึ้น และแนวทางในการแก้ไขปัญหาร่วมกัน
2. การเลือกใช้อุปกรณ์ที่ไม่ได้มาตรฐาน จะก่อให้เกิดปัญหาในระหว่างปฏิบัติงาน ทำให้เกิดความล่าช้าและสิ้นเปลืองงบประมาณที่จะต้องจัดหาอุปกรณ์ที่ได้มาตรฐานมาทดแทน
3. การเลือกใช้มาตรฐานในการติดตั้ง ทุกทีมงานที่เกี่ยวข้องจะต้องรับทราบและใช้มาตรฐานเดียวกัน เพื่อความสะดวกในการติดตั้งและบำรุงรักษา เช่น การเลือกใช้สายสัญญาณ การเข้าสายสัญญาณ RJ-45 connector ว่าจะใช้ Wire Color Code แบบ AT&T T568B หรือ TIA 2840 for T568B-UTP เป็นต้น
4. ในการติดตั้งอุปกรณ์ต่างๆ ควรทำการตรวจสอบสภาพแวดล้อมของสถานที่ ที่จะทำการติดตั้งว่าเมื่อทำการติดตั้งไปแล้วระบบที่ติดตั้งใหม่และระบบงานเดิม สามารถทำงานได้ตามปกติหรือไม่ เช่น การติดตั้งระบบไฟฟ้าสำรอง (UPS) ถ้าติดตั้งใกล้กับระบบสื่อสารอาจทำให้ระบบสื่อสารมีปัญหาในการรับส่งสัญญาณ หรือการติดตั้งเครื่องคอมพิวเตอร์ใกล้กับระบบไฟฟ้าแรงสูงหรือสถานีส่งสัญญาณ จะทำให้จอภาพสั่น เป็นต้น
5. ควรทำการสำรวจสถานที่ ก่อนที่จะทำการติดตั้งอุปกรณ์ เพราะจะทำให้ได้ข้อมูลที่ใช้ในการออกแบบระบบ เช่น
   - ระยะทางในการติดตั้งอุปกรณ์
   - การเลือกจุดเชื่อมต่อที่เหมาะสม
   - การจัดหาระบบไฟฟ้าที่จะมาจ่ายให้กับอุปกรณ์ที่ติดตั้ง
   - ระบบไฟฟ้าเดิมเพียงพอกับภาระ (Load) ที่เพิ่มขึ้นหรือไม่
   - ถ้ามีความจำเป็นที่จะต้องเดินสายสัญญาณ ระบบไฟฟ้าหรืออื่นๆ ทีเกี่ยวข้องกับการติดตั้งในสถานที่ของหน่วยงานอื่น จะต้องทำเรื่องขออนุญาตก่อนเข้าทำการปฏิบัติงาน เช่น การติดตั้งระบบเครือข่ายคอมพิวเตอร์ของกรมศุลกากรในบริเวณการท่าเรือแห่งประเทศไทย และการท่าอากาศยานกรุงเทพ เป็นต้น

6. สายสื่อสารที่จะต้องเดินภายในอาคาร เช่น สายโทรศัพท์ สาย Fiber Optic และสาย UTP จะต้องมีการป้องกันความเสียหายที่จะเกิดขึ้นกับสาย เช่น การกัดแทะของหนู โดยการร้อยสายในท่อ Flexible Metal Conduit หรืออื่นๆ ที่เหมาะสมและได้มาตรฐาน
7. การเดินสายสื่อสาร (เช่น Fiber Optic) ระหว่างอาคารและการเดินผ่านที่สาธารณะ จะต้องคำนึงถึงความสะดวกในการบำรุงรักษา และการป้องกันความเสียหายที่อาจเกิดโดยอุบัติเหตุ หรือเกิดจากภัยธรรมชาติ เช่น พายุ ฟ้าผ่า และน้ำท่วม เป็นต้น

เอกสารอ้างอิง

[1] Sun Microsystems Inc., "Solaris 2.x Network Administration", September 1993.

[2] K. Siyan, "NetWare The Professional Reference", New Riders Pub., 1994.

[3] F. Halsall, "Data Communications,Computer Networks and Open Systems", Addison-Wesley Pub., 1996.

[4] W. Stallings, "SNMP, SNMPv2, and RMON", Addison-Wesley Pub.,1996.

[5] D.E. Comer, "Internetworking with TCP/IP Volume I", Prentice-Hall Inc., 1995.

[6] C. Huitema, "Routing in the Internet", Prentice-Hall Inc., 1995.

[7] http://www.cisco.com

[8] http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html

[9] Unisys Corporation, "2200/500 System Preinstallation Planning Guide", March 1994.

ภาคผนวก

ผลงานทางวิชาการที่ได้รับการตีพิมพ์

[1] สุชาติ สิทธิสำอางค์, กอบชัย เดชหาญ "ระบบอินเตอร์เน็ตกับการแข่งขันกีฬา" การประชุมวิชาการของมหาวิทยาลัยเกษตรศาสตร์ ครั้งที่ 35 หน้า 410-418, กุมภาพันธ์ 2540.

[2] สุชาติ สิทธิสำอางค์, อนุชิต ธูปเหลือง, กอบชัย เดชหาญ "การออกแบบระบบเครือข่ายคอมพิวเตอร์สำหรับหน่วยงานขนาดใหญ่" วารสารสำนักงานคณะกรรมการวิจัยแห่งชาติ, ปีที่ 29 เล่มที่ 2, หน้า 199-218, กรกฎาคม-ธันวาคม 2540.

[3] สุชาติ สิทธิสำอางค์, กอบชัย เดชหาญ "การออกแบบระบบเครือข่ายคอมพิวเตอร์โดยรวมเราเตอร์เพื่อตรวจสอบทราฟฟิค" วิศวสารลาดกระบัง, ปีที่ 17 ฉบับที่ 1, มีนาคม 2543.

ประวัติผู้เขียน

นายสุชาติ สิทธิสำอางค์ เกิดเมื่อวันที่ 15 มกราคม 2510 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาวิศวกรรมศาสตรบัณฑิต (วิศวกรรมไฟฟ้า) จากสถาบันเทคโนโลยีราชมงคล ปีการศึกษา 2536

ปี พ.ศ. 2533 เข้าทำงานกับบริษัท ยิบอินซอย จำกัด ตำแหน่ง Junior Customer Service Engineer Level I ดูแลรับผิดชอบเกี่ยวกับคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ที่บริษัทประมูลงานได้ตามหน่วยงานต่างๆ เช่น การไฟฟ้านครหลวง กรมทางหลวง กรมบัญชีกลาง สำนักเศรษฐกิจการคลัง กระทรวงการคลัง สำนักงานสลากกินแบ่งรัฐบาล สำนักตรวจงบประมาณแผ่นดินและกรมศุลกากร เป็นต้น ปัจจุบันรับตำแหน่ง Supervisor Customer Service Engineer ดูแลระบบเครือข่ายคอมพิวเตอร์ของกรมศุลกากร