การบริหารโปรแกรมประยุกต์บนเครือข่ายระยะไกล

WAN Application Management

โดย

นายเบญศพล	มะหิงสิบ	36014236
นายพงศธร	หมื่นตาบุตร	36014273
นายสมภพ	พรพัฒนาจิรพันธ์	36014462
นายจตุรพิธ	เกราะแก้ว	36014573

อาจารย์ที่ปรึกษา

รศ.ประทีป บัญญัตินพรัตน์

อาจารย์บรรจง ปิยธำรง

วัน เดือน ปี 038309

เลขทะเบียน 1 ต.ค. 2541

เลขเรียกหนังสือ T 385ร ค.ศ.

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตร์บัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้า เจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2539

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

038309

ปีการศึกษา 2539

การบริหารโปรแกรมประยุกต์บนเครือข่ายระยะไกล

WAN Application Management

โดย

นายเบญศพล	มะหิงสิบ	36014236
นายพงศธร	หมื่นตาบุตร	36014273
นายสมภพ	พรพัฒนาจิรพันธ์	36014462
นายจตุรพิธ	เกราะแก้ว	36014573

อาจารย์ที่ปรึกษา

รศ.ประทีป บัญญัตินพรัตน์

อาจารย์บรรจง ปิยธำรง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ปริญญานิพนธ์ปีการศึกษา 2539

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง การบริหารโปรแกรมประยุกต์บนเครือข่ายระยะไกล

(WAN Application Management)

ผู้จัดทำ

1.นายเบญศพล	มะหิงสิบ	36014236
2.นายพงศธร	หมื่นตาบุตร	36014273
3.นายสมภพ	พรพัฒนาจิรพันธ์	36014462
4.นายจตุรพิธ	เกราะแก้ว	36014573

..... อาจารย์ที่ปรึกษา

(รศ.ประทีป บัญญัตินพรัตน์)

..... อาจารย์ที่ปรึกษา

(อาจารย์บรรจง ปิยธำรง)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การบริหารโปรแกรมประยุกต์บนเครือข่ายระยะไกล

นายเบญศพล มะหิงสิบ
นายพงศธร หมื่นตาบุตร
นายสมภพ พรพัฒนาจิรพันธ์
นายจตุรพิธ เกราะแก้ว

รศ.ประทีป บัญญัตินพรัตน์ อาจารย์ที่ปรึกษา
อ.บรรจง ปิยธำรง อาจารย์ที่ปรึกษา

ปีการศึกษา 2539

บทคัดย่อ

โครงงานการบริหารโปรแกรมประยุกต์บนเครือข่ายระยะไกล เป็นโครงการที่พัฒนาขึ้น เพื่อศึกษาถึงความเป็นไปได้ตลอดจนถึงวิธีการในการบริหารระบบเครือข่ายขนาดใหญ่ ที่มีการใช้โปรแกรมประยุกต์ชนิดต่าง ๆ กันออกไป โดยหลักการทำงานของโครงงานนี้เริ่มจากการกำหนดขอบเขตการทำงาน ชนิดโปรแกรมประยุกต์ที่จะทำการจัดการ และ เลือกหัวข้อสำหรับการบริหารระบบ เช่น การบริหารความปลอดภัย, การบริหารประสิทธิภาพ ฯลฯ จากนั้นก็ทำเก็บรวบรวมข้อมูลเพื่อใช้ในการบริหารระบบเครือข่าย โดยข้อมูลที่เก็บนี้ได้มาจาก 2 แนวทาง คือจากผู้บริหารระบบของแต่ละระบบเครือข่าย และ จาก Hp Openview ซึ่งเป็นแพลตฟอร์มของระบบบริหารเครือข่าย (Network Management Platform) ต่อมาก็นำข้อมูลที่เก็บรวบรวมได้นั้นมาทำการวิเคราะห์โดยอาศัยหลักในการวิเคราะห์จากหนังสือคู่มือ และ คำแนะนำจากผู้บริหารระบบเครือข่าย ผลที่ได้จากโครงงานนี้ก็คือจะทำให้ทราบถึงวิธีการและหลักการในการบริหารระบบเครือข่ายขนาดใหญ่สามารถบรรลุวัตถุประสงค์ที่ตั้งไว้ เช่น ทำการบริหารระบบได้อย่างมีประสิทธิภาพ และความปลอดภัยสูงขึ้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

WAN Application Management

Benspon Mahingsib
Phongsthorn Muenthabutr
Sompop Pornpattanajiraphun
Jaturapith Krohkaew

Associate Professor Pratheep Bunyatnoparat Advisor
Bunjong Piyathamrong Advisor

1996

ABSTRACT

This project,WAN Application Management, is developed to learn about some methods for managing WAN application. Principles of this project are, the first step, defining working boundary, selecting application to manage and management function area(s), (such as fault management, security management and etc.) for such an application management. The second step is to collect required information for such an application management. We can get informations from system administrator or using Hp Openview Network Management Platform to collect them. Then, analize the information refer to some referrence books and asking for system administrator. Result of this project make us to know about methods and principles to manage WAN application and accomplish our objectives, such as we can make network having high security, user can use application with higher performance.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

บทที่ 1

บทนำ 1

จุดประสงค์ของโครงงาน 1

ขอบข่ายของโครงงาน 1

บทที่ 2

การบริหารเครือข่ายคอมพิวเตอร์ 4

2.1 ทำไมต้องมีการบริหาร 4

2.2 เป้าหมายของการบริหาร 4

2.2.1 ประเภทของการบริหารเครือข่าย 4

2.2.1.1 การบริหารความผิดพลาดในเครือข่าย (Fault Management) 4

2.2.1.2 การบริหารเกี่ยวกับการกำหนดค่าตัวแปรขององค์ประกอบในเครือข่าย (Configuration Management) 6

2.2.1.3 การบริหารทางด้านการรักษาความปลอดภัย (Security Menagement) 7

2.2.1.4 การบริหารประสิทธิภาพของระบบ (Performance Management) 8

2.2.1.5 การบริหารแอคเคาน์ติ้ง (Accounting Management) 9

2.3 สิ่งที่จำเป็นในการบริหารเครือข่าย 11

บทที่ 3

ระบบบริหารเครือข่าย 11

3.1 การบริหารเครือข่าย 11

3.2 แพลตฟอร์มของการบริหารเครือข่าย (Network Management Platform) 12

3.2.1 ส่วนประกอบของแพลตฟอร์มการบริหารระบบ (Elements of a Management Platform) 15

3.3 แอพพลิเคชั่นการบริหารเครือข่าย (Network Management Application) 17

3.3.1 แอพพลิเคชั่นการบริหารเครือข่ายมีเป้าหมายดังต่อไปนี้ 17

3.4 เอเจ้นต์ (agent) 19

3.4.1 สัญญาณและเหตุการณ์ (Alarms and Events) 19

3.5 สถาปัตยกรรมการบริหารเครือข่ายแบบต่าง ๆ 20

3.5.1 สถาปัตยกรรมแบบระบบรวมศูนย์ (Centralized Architecture) 20

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.5.2 สถาปัตยกรรมแบบระบบระดับชั้น (Hierachical Architecture) 22
สถาปัตยกรรมแบบระบบกระจาย (Distributed Architecture) 23
3.5.3 การบริหารแบบกระจาย (Distributed Management) 25
3.6 เครื่องมืออำนวยความสะดวก (Utility) 26
3.7 ผู้จัดการของผู้จัดการ (Managers of Managers) 26
3.8 การเลือกแพลตฟอร์มในการบริหารระบบเครือข่ายคอมพิวเตอร์ 27
3.8.1 ระบบปฏิบัติการแพลตฟอร์ม 27
3.8.2 อุปกรณ์ที่ต้องการการบริหาร(Managed Devices) 29
3.9 ตัวอย่างของแพลตฟอร์ม 29
3.9.1 ผลิตภัณฑ์ของบริษัทโนเวลล์ : ระบบบริหารเครือข่ายของเน็ทแวร์
(The NetWare Management System) 29
3.9.2 ผลิตภัณฑ์ของบริษัทฮิวเล็ทแพคคาร์ด : โอเพ็นวิว (OpenView) 33
3.9.3 ซันเน็ทมาเนเจอร์ (SunNet Manager) 34
3.10 โปรโตคอลเอสเอ็นเอ็มพี (SNMP:Simple Network Management Protocol) 34
3.10.1 Promise ของการบริหารระบบเครือข่าย 34
3.10.2 เอสเอ็นเอ็มพี 35
3.10.3 เออร์โกโนมิค (Ergonomics) 36
3.10.4 ความสามารถในการปฏิบัติงานที่หลากหลาย (Interoperability) 36
3.10.5 ทีซีพี/ไอพี(TCP/IP) : มาตราฐานภายใต้การบริหารระบบเครือข่าย 36
3.10.6 เอสเอ็นเอ็มพี: มาตราฐานระบบเครือข่ายในปัจจุบันนี้ 37
3.10.7 เอสเอ็นเอ็มพีทำงานอย่างไร 37
3.10.8 เครื่องที่ทำการบริหาร เอสเอ็นเอ็มพี 38
3.11 บทสรุป 38
3.11.1 แนวคิดสำหรับ เอสเอ็นเอ็มพี 39
3.11.2 โปรโตคอลสเปคซิฟิเคชั่น (Protocol Specification) 44
3.11.3 การเลือกเครื่องทำการบริหารเครือข่าย 48
3.11.4 ข้อจำกัดของเอสเอ็นเอ็มพี 49
3.11.5 เอสเอ็นเอ็มพี เอ็มไอบี (SNMP MIB) 50
3.11.6 เอสเอ็นเอ็มพี เวอร์ชัน 2 (SNMPv2) 55
3.12 สถาปัตยกรรมแบบรวมสำหรับการบริหารระบบเครือข่ายระยะไกลและระยะใกล้ 60

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.13 ภาพรวมของสถาปัตยกรรมการบริหารเครือข่ายแบบรวมสำหรับเครือข่ายที่หลากหลายขนาดใหญ่ (Overview of An Integrated Network Management Architecture for A Large Heterogeneous Network) 64
3.13.1 สิ่งที่ต้องการสำหรับสถาปัตยกรรมการบริหารเครือข่ายแบบรวม 65
3.13.2 ทางเลือกของสถาปัตยกรรมการบริหารเครือข่ายแบบรวม 66
3.13.3 ภาพรวมของสถาปัตยกรรมการบริหารเครือข่ายแบบรวม 67
3.13.4 การบริหารเครือข่ายแบบรวมที่ขึ้นอยู่กับสถาปัตยกรรมของเครือข่ายระยะใกล้ 68
3.13.5 ข้อสรุปของการพัฒนาสถาปัตยกรรมแบบINM 70
3.14 การบริหารระบบเครือข่ายมาตรฐานที่เป็นแบบมัลติเวนเดอร์ (Standardized Multivendor Network Management) 71
3.14.1 สิ่งที่ต้องการสำหรับการบริหารเครือข่ายระยะใกล้ 71
3.14.2 การทำงานของการบริหารด้านความผิดพลาด 73
3.14.3 การแสดงสถานะของเครือข่าย 74
3.14.4 การทำงานของการบริหารด้านประสิทธิภาพ 75
3.14.5 การกระทำแบบลำดับขั้นสำหรับการรวม 76
3.14.6 การกระทำของแพลตฟอร์มสำหรับการรวม 76
3.14.7 ต้นแบบของเครื่องมือรวม 77
บทที่ 4
ระบบความปลอดภัยของระบบเครือข่าย 77
4.1 การใช้ไฟร์วอลล์ (Firewall) ในการระบบรักษาความปลอดภัยในเครือข่าย 77
4.1.1 จุดประสงค์ของการมีไฟร์วอลล์ 77
4.1.2 ที่ตั้งของไฟร์วอลล์ 78
4.1.3 องค์ประกอบของไฟร์วอลล์ 78
4.1.4 สกรีนนิงเราท์เตอร์ 79
4.1.5 การระบุโซนที่มีความเสี่ยง (Identifying zones of risk) 79
4.1.6 ความสัมพันธ์ของสกรีนนิงเราท์เตอร์ และ ไฟร์วอลล์ กับ ไอเอสโอ โมเดล 81
4.1.7 การทำงานของแพ็กเก็ตฟิลเตอริ่ง 82
4.1.8 การออกแบบแพ็กเก็ตฟิลเตอร์ 84
4.2 เอชพี แอ็ดวานซ์สแต็ค (HP AdvanceStack) 86
4.2.1 ความปลอดภัยของระบบ 86

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.2.2 ความเสี่ยงของระบบความปลอดภัย 87
4.2.3 ความปลอดภัยของระบบเครือข่าย 87
4.2.4 วิธีรักษาความปลอดภัย 88
4.2.4.1 การแบ่งระบบเครือข่ายด้วยบริดจ์และเราท์เตอร์ 89
4.2.5 ดีอีเอส 91
4.2.6 อาร์เอสเอ 91
4.2.7 การแก้ปัญหาความปลอดภัยของเอชพี แอ็ดวานซ์สเต็ค 92
4.2.8 บทสรุป 93
4.3 กรณีศึกษา (Case studies) 93
4.3.1 สถาบันการศึกษา 93
4.3.2 ห้องปฏิบัติการวิจัย (Research lab) 94
4.3.3 แอพพลิเคชั่นทางการค้า (Electronic commerce application) 94
บทที่ 5
ตัวอย่างการบริหารระบบที่ใช้งานแอพพลิเคชั่นต่าง ๆ **94**
5.1 World Wide Web (WWW) 94
5.2 เอฟทีพี (FTP : File Transfer Program) 95
5.3 เทลเน็ท (Telnet) หรือรีโหมดแอกซ์เซส (Remote Access) 96
5.4 จดหมายอิเลคทรอนิค (E-Mail) 97
5.5 การประชุมทางไกล (Video Conference) 97
5.6 วีดีโอออนดีมานด์ (Video On Demand) 98
5.7 การติดต่อแบบออนไลด์ทรานแซกชั่น (Online Transaction) 98
5.8 สรุป 99
บทที่ 6
การทดลอง และผลการทดลอง **100**
6.1 คอนฟิกกูเรชั่น (Configuration) 100
6.1.1 รายละเอียดของระบบเครือข่ายสถาบันและภาควิชาวิศวกรรมคอมพิวเตอร์ 101
6.2 การบริหารเครื่องเซิร์ฟเวอร์ที่ให้บริการเกี่ยวกับแอพพลิเคชั่นอินเตอร์เน็ต 101
6.3 ผลจากการทดลองบริหารเครือข่าย 104

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6.3.1 ข้อมูลการทดลอง (DATA) 104
6.3.2 รายละเอียดการตรวจสอบ (monitoring) 115
6.3.3 การวิเคราะห์ข้อมูล (Analysis) 117
6.4 การบริหารด้านความปลอดภัย 124
6.4.1 การควบคุมการเข้าใช้ (Access Control) 124
6.4.2 การรักษาความปลอดภัยด้านกายภาพ (Physical Security) 125
6.4.3 การใช้โปรแกรมรักษาความปลอดภัย (Security Software) 125
6.4.4 แอ็พพลิเคชั่นที่ทดลอง 125
6.5 แอ็พพลิเคชั่นที่ทดลอง 125
6.6 กรณีศึกษา 127
บทที่ 7
บทวิจารณ์และสรุป **132**
7.1 สรุปและวิจารณ์โครงงาน 132
7.2 ปัญหาที่พบ 133
7.3 ข้อเสนอแนะ 135
7.3.1 ทางด้านความปลอดภัยของเครือข่ายและระบบ 135
7.3.2 คอนฟิกกูเรชั่น (Configuration) 136
7.4 แนวทางในการพัฒนา 137
สรุปคำศัพท์
ภาคผนวก ก
ภาคผนวก ข
หนังสืออ้างอิง
กิตติกรรมประกาศ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญภาพ

รูปที่ 2.1 แสดงความผิดพลาดของเครือข่ายซึ่งวิศวกรตรวจดูได้ 5
รูปที่ 2.2 แสดงทูลในการบริหารความปลอดภัยที่ตรวจดูว่ามีผู้ใช้เข้ามาจากไหน 7
รูปที่ 2.3 ทูลของการบริหารประสิทธิภาพช่วยให้สามารถทราบว่าเกิดปัญหาขึ้น 8
รูปที่ 2.4 แสดงทูลของ account management 9
รูปที่ 3.1 แสดงระบบบริหารเครือข่าย 12
รูปที่ 3.2 แสดงความสัมพันธ์ระหว่าง แพล็ตฟอร์มละแอพพลิเคชั่น 17
รูปที่ 3.3 แสดงสถาปัตยกรรมแบบรวมศูนย์ของระบบบริหารเครือข่าย 21
รูปที่ 3.4 แสดงสถาปัตยกรรมแบบระดับชั้น 22
รูปที่ 3.5 แสดงสถาปัตยกรรมการบริหารแบบกระจาย 24
รูปที่ 3.6 ลักษณะทั่วไปของโปรโตคอลสำหรับ เอสเอ็นเอ็มพี 41
รูปที่ 3.7 โปรโตคอลคอนเท็คของเอสเอ็นเอ็มพี 40
รูปที่ 3.8 รูปแบบของข้อมูลของเอสเอ็นเอ็มพี 43
รูปที่ 3.9 โครงสร้างต้นไม้ของออบเจค 49
รูปที่ 3.10 รูปแบบของพีดียู 55
รูปที่ 3.11 แสดงส่วนประกอบของสถาปัตยกรรมการจัดการ 59
รูปที่ 3.12 แสดงการวางตำแหน่งของตัวกลาง 61
รูปที่ 3.13 แสดงสถาปัตยกรรมการจัดการเครือข่ายแบบต่าง ๆ 64
รูปที่ 3.14 แสดงภาพรวมของสถาปัตยกรรมการจัดการเครือข่ายแบบรวม 65
รูปที่ 3.15 แสดงการจัดการเครือข่ายแบบรวมที่ขึ้นอยู่กับสถาปัตยกรรมเครือข่ายระบะใกล้ 66
รูปที่ 3.16 แสดงการนำข้อมูลมาแสดงให้กับผู้ใช้ผ่านทาง GUI 67
รูปที่ 3.17 แสดงกระบวนการการทำงานของการจัดการด้านความผิดพลาด 71
รูปที่ 3.18 แสดงกระบวนการการทำงานของการจัดการด้านประสิทธิภาพ 73

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 4.1 แสดงตำแหน่งของไฟร์วอลล์ 78
รูปที่ 4.2 แสดงสกรีนนิ่งเราเตอร์สร้างรูปแบบพารามิเตอร์สำหรับความปลอดภัย 80
รูปที่ 4.3 โซนของความเสี่ยงขยายไปสู่โฮสท์ที่ไม่สนันสนุน ทีซีพี/ไอพี 81
รูปที่ 4.4 แสดง สกรีนนิ่งเราท์เตอร์ ไฟร์วอลล์และ ไอเอสโอ โมเดล 81
รูปที่ 4.5 แสดงเงื่อนไขการทำงานของแพ็กเก็ตฟิลเตอริ่ง 83
รูปที่ 4.6 แสดงการใช้สกรีนนิ่งเราท์เตอร์ในการบริหารความปลอดภัยของเครือข่าย 84
รูปที่ 4.7 แสดงการบล็อกหรือยอมให้แพ็กเก็ตผ่านเข้าเครือข่ายโดยสกรีนนิ่งเราท์เตอร์ 85
รูปที่ 6.1 แสดงระบบการเชื่อมต่อของเครือข่ายของสถาบัน 101
รูปที่ 6.2 แสดงตัวอย่างเราท์เตอร์ CAR24 102
รูปที่ 6.3 แสดงระบบเครือข่ายของภาควิชาวิศวกรรมคอมพิวเตอร์ 103
รูปที่ 6.4 แสดงคำสั่ง Top 118
รูปที่ 6.5 แสดงการ conference 126
รูปที่ 6.6 แสดง model ของ control และ data connection 127
รูปที่ 6.7 แสดงปัญหาที่เกิดขึ้นในการใช้แอพพลิเคชั่น ftp 128
รูปที่ 6.8 แสดงการทดสอบการทำงานของ Host 129
รูปที่ 6.9 แสดงการทดสอบ Routers 130
รูปที่ 6.10 แสดงการทดสอบ Medium 131
รูปที่ 6.11 แสดงสาเหตุของปัญหา 131

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 1

บทนำ

เนื่องจากการพัฒนาอย่างมากในเทคโนโลยีด้านเครือข่ายคอมพิวเตอร์และอินเตอร์เน็ตทำให้มีการขยายตัวของเครือข่ายคอมพิวเตอร์และจำนวนของผู้ใช้ ซึ่งจากการที่ในอดีตระบบเครือข่ายคอมพิวเตอร์ยังมีขนาดเล็ก, มีผู้ใช้จำนวนน้อย และมีการใช้งานเฉพาะภายในองค์กรทำให้ผู้ดูแลระบบเครือข่ายสามารถทำการควบคุมระบบเครือข่ายได้ง่าย แต่ในปัจจุบันระบบเครือข่ายมีการขยายตัวและมีการเชื่อมต่อเครือข่ายเข้าด้วยกันซึ่งก็คืออินเตอร์เน็ตนั่นเอง ที่มีผู้ใช้เป็นจำนวนมากเพราะมีการใช้งานที่ง่าย ทำให้การควบคุมระบบเครือข่ายนั้นทำได้ยาก จึงจะต้องมีส่วนที่ทำหน้าที่ในการบริหารและควบคุมเครือข่ายโดยเฉพาะซึ่งก็คือ ระบบการบริหารเครือข่าย (Network Management System) เพื่อทำการบริหารเครือข่ายให้ทำงานได้เหมาะสมกับแอพพลิเคชั่นและมีประสิทธิภาพ

จุดประสงค์ของโครงงาน

1. เพื่อทำการวิเคราะห์ความต้องการของระบบเครือข่าย และจุดประสงค์ในการบริหารเครือข่ายนั้นๆได้
2. เพื่อทำการเลือกอุปกรณ์, ระบบ และสถาปัตยกรรมการบริหารเครือข่ายได้
3. เพื่อทำการเก็บสถิติของข้อมูลและทำการวิเคราะห์ได้
4. เพื่อทำการบริหารเครือข่ายที่ใช้แอพพลิเคชั่นหนึ่ง ๆ ได้

ขอบข่ายของโครงงาน

1. ศึกษากลุ่มของแอพพลิเคชั่นที่สนใจบนเครือข่ายจากรายละเอียดของเครื่องแม่ข่ายในภาควิชา เช่น แม่ข่าย diamond สามารถให้บริการแอพพลิเคชั่น telnet, ftp, WWW ฯลฯ
2. ศึกษาสถาปัตยกรรมของเครือข่ายเป้าหมาย ได้ทำการสำรวจเครือข่ายย่อยในภาควิชาและคอนฟิกกูเรชั่นของเครื่องแม่ข่าย และลูกข่าย
3. ทำการศึกษาและใช้งานระบบการบริหารเครือข่าย คือ HP OpenView ในการบริหารเครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4. ทำการเก็บข้อมูลของการใช้งานเครือข่ายที่ผ่านเข้ามา และ ออกจากเครือข่ายของภาควิชา ฯ เช่น ปริมาณโหลดซีพียูของ diamond, In Out Octet, Packets และ Utilization ฯลฯ

5. มอนิเตอร์แนวโน้มของข้อมูลที่ทำการเก็บ

6. สำรวจระบบรักษารักษาความปลอดภัยของเครือข่าย

7. ศึกษาหลักการของไฟร์วอลล์เพื่อป้องกันเครือข่าย

8. จัดทำข้อเสนอแนะเพื่อทำการพัฒนาเครือข่าย

จากการที่มีการขยายตัวของเครือข่ายและใช้งานอินเตอร์เน็ตมากขึ้น งานส่วนใหญ่ในการบริหารก็มักจะเป็นการบริหารเครือข่ายที่เกี่ยวข้องกับแอพพลิเคชั่นที่ใช้ผ่านเครือข่ายอินเตอร์เน็ต โดยจะพิจารณาถึงการทำงานของเครือข่ายต่อแอพพลิเคชั่นหนึ่งๆ ซึ่งการบริหารเครือข่ายนั้นเราจะทำการตั้งจุดประสงค์ที่ต้องการ เช่น ต้องการให้เครือข่ายการประชุมทางไกล (Video Conference) สามารถทำงานได้อย่างไม่ติดขัด แล้วก็จะหาว่าเราจะนำข้อมูลอะไรในเครือข่ายที่จะนำมาใช้ในการตัดสินใจในการบริหารเครือข่าย ต่อมาเราก็จะทำการเลือกอุปกรณ์ซึ่งอาจเป็นซอฟท์แวร์หรือระบบที่จะใช้ในการบริหารเพื่อทำการเก็บข้อมูล ในขั้นต่อไปก็จะเป็นการเก็บข้อมูลและวิเคราะห์ข้อมูลเพื่อดูสถานะของเครือข่ายว่าเป็นไปตามจุดประสงค์ที่เราต้องการหรือไม่ ถ้าไม่เป็นตามความต้องการของเราแล้วก็จะทำการปรับปรุงระบบเครือข่ายให้มีความเหมาะสมกับความต้องการของเรา

ในส่วนของอุปกรณ์หรือระบบที่ทำการบริหารที่เราได้เลือกใช้ในการบริหารนี้คือ HP Openview ซึ่งเป็นระบบการบริหารเครือข่ายของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ที่ใช้งานอยู่บนระบบปฏิบัติการยูนิกส์ (UNIX) และมีการเชื่อมต่อกับผู้ใช้เป็นกราฟฟิก (graphic) โดยข้อมูลที่ได้นั้นจะเป็นรูปของโทโพโลยี (topology) ของเครือข่าย, กราฟการทำงานของอุปกรณ์ในเครือข่ายที่เราสนใจ, ค่าและส่วนประกอบของอุปกรณ์ในเครือข่าย และข้อมูลอื่นที่เกี่ยวข้อง HP OpenView นี้เป็นระบบการบริหารเครือข่ายทีประกอบไปด้วยหลาย ๆ ส่วน เช่น เน็ทเวิร์คโหนดแมเนเจอร์ (Network Node Manager), เน็ทเมตริกซ์ (Net Metrics) เป็นต้น ซึ่งสามารถรองรับการทำงานและหาข้อมูลที่ต้องการได้ รวมถึงการเขียนเอพีไอ (API-Application Programming Interface) เพื่อพัฒนาแอพพลิเคชั่นที่จะใช้เฉพาะในเครือข่ายของเราได้

การทำการบริหารเครือข่าย ซึ่งเครือข่ายที่เลือกมาทำการบริหารคือเครือข่ายของภาควิชาวิศวกรรมคอมพิวเตอร์ ที่มีการใช้งานแอพพลิเคชั่นผ่านเครือข่ายระยะไกลซึ่งก็คืออินเตอร์เนต

แอพพลิเคชั่น โดยทำการเก็บข้อมูลจากเครื่องเวิร์คสเตชั่น (Workstation) ในภาควิชา ข้อมูลที่ทำการเก็บนั้นจะเป็นปริมาณการส่งออกของเครือข่ายภาควิชา, รูปแบบของโทโพโลยีของเครือข่ายในภาควิชาและเครือข่ายสถาบัน และอื่นๆ และทำการวิเคราะห์หาสภาพของเครือข่ายในการใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

งานแอพพลิเคชั่นอินเตอร์เน็ตที่ผู้ใช้ทำการใช้จากข้อมูลที่เก็บได้ ในขั้นตอนสุดท้ายจะทำการบริหารให้เครือข่ายมีสภาพที่เหมาะสมกับการใช้งานตามวัตถุประสงค์ที่ต้องการ

ประโยชน์ของโครงงานนี้คือ สามารถนำความรู้ที่ได้จากโครงงานนี้ไปวิเคราะห์ระบบเครือข่ายจริงที่มีการใช้งานอยู่แล้วได้ และสามารถบริหารให้เครือข่ายนั้นสามารถใช้งานแอพพลิเคชั่นต่าง ๆ ได้ อย่างประสิทธิภาพที่ตรงตามเป้าหมายของเครือข่าย

ในปริญญานิพนธ์นี้จะอธิบายถึงหลักการในการบริหารเบื้องต้น, ระบบ และการบริหารที่เกี่ยวข้องกับการบริหารเครือข่าย ดังนี้

บทที่ 1 บทนำ

บทที่ 2 จะกล่าวถึงความต้องการที่จะต้องมีระบบการบริหารเครือข่าย เป้าหมายในการบริหารเครือข่าย และข้อมูลที่ต้องการในการบริหารเครือข่าย

บทที่ 3 จะกล่าวถึงหน้าที่ที่ทำในการบริหาร, โครงสร้างของระบบการบริหาร และทฤษฎีข่องระบบการบริหารเครือข่าย

บทที่ 4 เป็นการทำงานในเครือข่ายจริงซึ่งจะมีข้อมูลต่าง ๆ ที่ทำในการบริหารเครือข่าย

บทที่ 5 เป็นการบริหารต่าง ๆ บนเครือข่ายที่มีแอพพลิเคชั่นหนึ่งๆอยู่

บทที่ 6 จะกล่าวถึงการบริหารเครือข่ายเครือข่ายที่มีแอพพลิเคชั่นใช้งานอยู่จริง

บทที่ 7 จะสรุปในการทำงานที่กล่าวมาในบทที่ 4-6 ว่ามีการทำงานอย่างไรและควรจะมีข้อแก้ไขอย่างไร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2

การบริหารเครือข่ายคอมพิวเตอร์

2.1 ทำไมต้องมีการบริหาร

ระบบบริหารเครือข่ายระบบคอมพิวเตอร์ได้มีการกระทำกันการหลายปีแล้ว โดยเฉพาะบริษัทที่เป็นผู้เริ่มต้นทั้งหลาย เช่น Netview, AT&T เป็นต้น เครือข่ายแบบแลน (LAN) และ แบบแวน (WAN) สามารถถูกตรวจสอบ และ บริหารโดยการใช้ เอสเอ็นเอ็มพี (SNMP) จะได้รับข้อมูลดิบเป็นจำนวนมาก แต่ผู้บริหารระบบส่วนใหญ่ไม่มีความคิดว่า จริง ๆ แล้วเขาต้องการข้อมูลอะไรกัน และทำอย่างไรที่จะได้รับข้อมูลเหล่านั้นอยู่ในรูปแบบที่มีความหมาย สามารถเข้าใจได้

เมื่อเรามีระบบการบริหารเครือข่ายที่เหมาะสม และมีประสิทธิภาพแล้ว เวลาเราต้องการข้อมูลใด ๆ เพื่อใช้ในการอ้างอิงในการบริหารระดับสูง เราก็สามารถเอามาได้จากระบบบริหารเครือข่ายโดยที่ไม่ต้องเสียเวลาในการอ่านค่าข้อมูลดิบ ซึ่งไม่มีความหมายอะไรสำคัญเลย หรือเมื่อระบบของเรามีปัญหาไม่ว่าจะเป็นเรื่องใด ๆ ก็ตาม เช่น ระบบเสียหาย, หยุดทำงาน, ความเร็วตก เราก็สามารถรับรู้ถึงสาเหตุของเหตุการณ์เหล่านั้นได้ โดยอาศัยข้อมูลที่ได้รับการวิเคราะห์แล้วจากระบบบริหารเครือข่ายนั่นเอง

2.2 เป้าหมายของการบริหาร

2.2.1 ประเภทของการบริหารเครือข่าย

คือ กระบวนการในการควบคุมเครือข่ายข้อมูลที่มีความซับซ้อนให้ทำงานได้อย่างมีประสิทธิภาพสูงสุด

องค์กรมาตรฐานนานาชาติ (International Organization Standardization -ISO) ได้กำหนดขอบเขตของการบริหารเครือข่ายไว้ดังนี้

2.2.1.1 การบริหารความผิดพลาดในเครือข่าย (Fault Management)

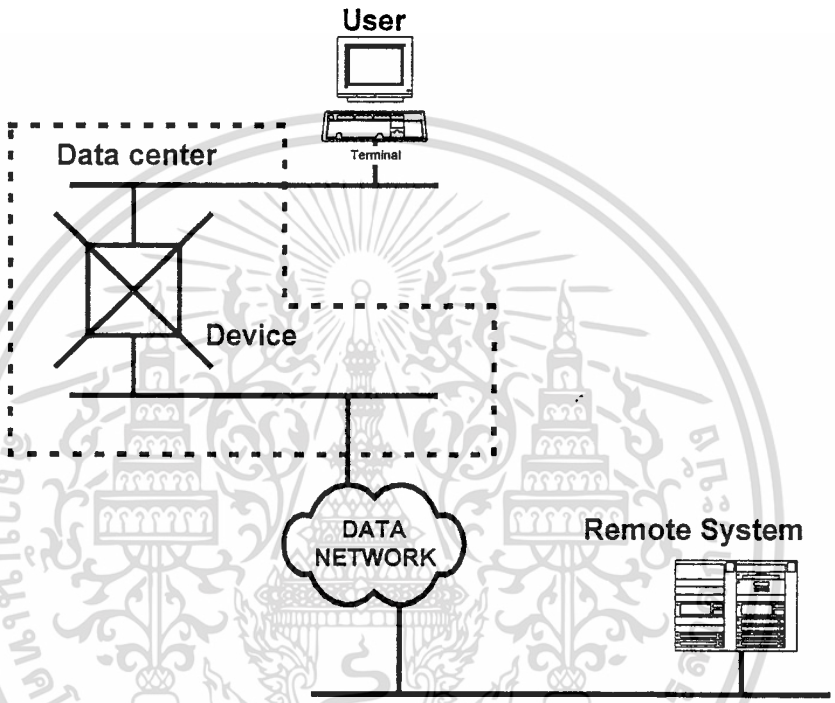
คือ กระบวนการในการค้นหาปัญหา หรือความผิดพลาดในเครื่อข่ายข้อมูล ซึ่งจะมีขั้นตอนต่อไปนี้

- ค้นหาปัญหา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- แยกแยะปัญหา
- แก้ไขปัญหา (ถ้าเป็นไปได้)

การใช้เครื่องมือบริหารความผิดพลาด (Fault management tools) วิศวกรสามารถค้นหาและแก้ไขความผิดพลาดของเครือข่ายได้เร็วยิ่งขึ้น



รูปที่ 2.1 แสดงความผิดพลาดของเครือข่ายซึ่งวิศวกรตรวจดูได้

ตัวอย่าง ในการเข้าสู่ระบบทางไกลโดยผ่านทางอุปกรณ์เครือข่ายหลาย ๆ ตัว และในทันใดนั้นการเชื่อมต่อระหว่างผู้ใช้กับเครือข่ายก็หลุดไป เมื่อผู้ใช้ก็มารายงานให้กับวิศวกรผู้ดูแลเครือข่าย วิศวกรก็จะต้องเริ่มแก้ไขปัญหาด้วยการแยกแยะปัญหาที่เกิดขึ้น

ถ้ากระบวนการเหล่านี้ทำโดยไม่มีเครื่องมือในการบริหารความผิดพลาดที่มีประสิทธิเพียงพอ สิ่งแรกที่ต้องทำ คือ วิศวกรต้องตัดสินใจว่าความผิดพลาดนั้นเกิดจากความผิดของผู้ใช้หรือไม่ เช่นการใช้คำสั่งที่ผิด หรือการพยายามเข้าใช้บริการระบบที่ไม่สามารถเข้าใช้บริการได้ (unreachable network) ถ้าพบว่าไม่มีความผิดพลาดที่เกิดจากผู้ใช้แล้วก็ต้องตรวจอุปกรณ์แต่ละตัวตามรายทางระหว่างผู้ใช้กับระบบทางไกลนั้นโดยเริ่มจากอุปกรณ์ที่ใกล้กับผู้ใช้มากที่สุด สมมติว่าพบความผิดพลาดเกิดขึ้นที่อุปกรณ์ตัวแรกดังรูป และเมื่อได้เข้าไปยังศูนย์ข้อมูลก็พบว่า สัญญาณไฟของอุปกรณ์ตัวนั้นดับหมดเลย เป็นการบอกให้ทราบว่าอุปกรณ์นั้นไม่ทำงาน เมื่อสำรวจต่อไปพบว่า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ปลั๊กของอุปกรณ์หลุด ก็สันนิษฐานว่ามีใครบางคนทำให้ปลั๊กหลุดโดยบังเอิญหลังจากที่วิศวกรได้เสียบปลั๊กกลับคืนแล้วก็ต้องทำการตรวจสอบดูอีกทีว่าอุปกรณ์นั้นสามารถทำงานได้ตามปกติ

ถ้ามีเครื่องมือในการบริหารความผิดพลาด เราสามารถแยกแยะปัญหาได้เร็วยิ่งขึ้น ในความเป็นจริงแล้วเครื่องมือนี้อาจจะทำให้เราแยกแยกและแก้ไขปัญหานี้ได้ก่อนที่ผู้ใช้จะมารายงาน

2.2.1.2 การบริหารเกี่ยวกับการกำหนดค่าตัวแปรขององค์ประกอบในเครือข่าย (Configuration Management)

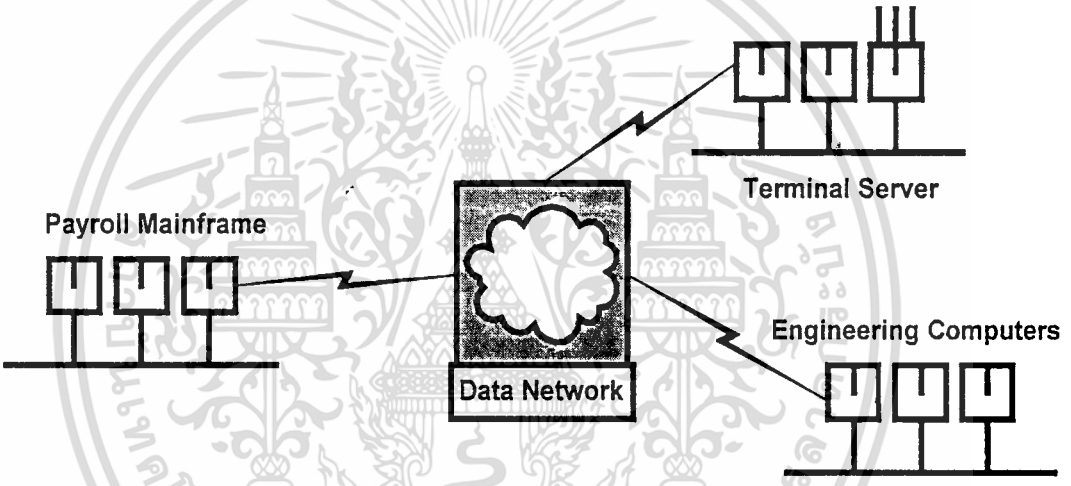
คือ กระบวนการของการค้นหาและกำหนดค่าของอุปกรณ์ต่าง ๆ ในเครือข่าย (เน้นอุปกรณ์ที่สำคัญ ๆ) สมมติว่า ซอฟแวร์เวอร์ชั่น A ของ บริดจ์ (Bridge) ในเครือข่ายข้อมูลทำให้ประสิทธิภาพของเครือข่ายลดลงและบริษัทผู้ผลิตได้ออกซอฟแวร์เวอร์ชั่น B มาให้เพื่อเพิ่มประสิทธิภาพในการทำงานของบริดจ์ ดังนั้นวิศวกรต้องทำการเปลี่ยนเปลี่ยนซอฟแวร์ในบริดจ์นับร้อยตัวในเครือข่ายให้เป็นเวอร์ชั่น B อย่างไรก็ตามวิศวกรต้องเริ่มด้วยการตรวจสอบดูว่าเวอร์ชั่นปัจจุบันของบริดจ์นั้นเป็นเวอร์ชั่นอะไร ถ้าไม่ใช่เวอร์ชั่น B ก็ให้เปลี่ยนเป็นเวอร์ชั่น B ถ้าไม่มีเครื่องมือในการบริหารการกำหนดค่าตัวแปรและองค์ประกอบ (Configuration Management Tool) แล้วคุงต้องเดินสำรวจบริดจ์ทีละตัวจนครบ เครื่องมือนี้จะแสดงรายการของบริดจ์ทั้งหมดพร้อมด้วยเวอร์ชั่นของซอฟแวร์ที่ทำงานอยู่บนบริดจ์นั้นจะช่วยให้การเปลี่ยนเวอร์ชั่นของซอฟแวร์ง่ายและรวดเร็วขึ้น

Configuration Management Information	
Bridge Name	Software Version
Corporate 1	A
Site 23	B
Site 62	B
Corporate 8	A

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2.1.3 การบริหารทางด้านการรักษาความปลอดภัย (Security Menagement)

คือ กระบวนการของการควบคุม การเข้าใช้บริการข้อมูลข่าวสารบนเครือข่ายข้อมูล ข่าวสารข้อมูลเหล่านี้ที่เก็บอยู่ในคอมพิวเตอร์บนเครือข่ายข้อมูลนั้น บางครั้งก็ไม่สามารถที่จะเปิดเผยกับผู้ใช้ทั้งหมดได้ ตัวอย่างเช่น ข้อมูลเกี่ยวกับผลิตภัณฑ์ใหม่ของบริษัทหรือฐานลูกค้าของผลิตภัณฑ์ หรือข้อมูลใด ๆ ที่ถือเป็นความลับของบริษัท สมมติว่าองค์กรได้ตัดสินใจเลือกใช้การบริหารด้านการรักษาความปลอดภัย ในการกำหนดสิทธิของการเข้าใช้บริการแบบทางไกลมายังเครือข่ายโดยผ่านทางสายโทรศัพท์บนเครื่องเทอร์มินอลเซิร์ฟเวอร์ (Therminal Server) สำหรับกลุ่มของวิศวกรดังรูป



รูปที่ 2.2 แสดงทูลในการบริหารความปลอดภัยที่ตรวจดูว่ามีผู้ใช้เข้ามาจากไหน

เมื่อวิศวกรได้ต่อไปยังเทอร์มินอลเซิร์ฟเวอร์แล้วก็สามารถลอกอิน (login) เข้าไปในโฮสต์ (host) บนเครือข่ายและทำงานต่อไปได้

หลังจากนั้นอีกประมาณ 2-3 สัปดาห์ผู้ดูแลระบบบัญชีรายจ่าย (payroll) ก็รายงานว่ามีคนพยายามจะเข้าถึงข้อมูลในเครื่องเมนเฟรมคอมพิวเตอร์ของระบบจากเทอร์มินอลเซิร์ฟเวอร์ ที่ใช้โดยกลุ่มวิศวกรและเนื่องจากเทอร์มินอลเหล่านั้นได้อนุญาตให้ผู้ใช้สามารถเข้าใช้บริการทุกเครื่องในเครือข่ายได้โดยปล่อยให้การรักษาความปลอดภัยนั้นเป็นหน้าที่ของเครื่องปลายทางที่ผู้ใช้นั้นเข้าใช้บริการ ดังนั้นไม่มีวิศวกรคนไหนที่ได้ข้อมูลจากเครื่องเมนเฟรมในระบบบัญชีรายจ่ายแต่ความจริงที่เกิดขึ้นก็คือ มีวิศวกรพยายามเข้าถึงข้อมูลในเครื่องดังกล่าว

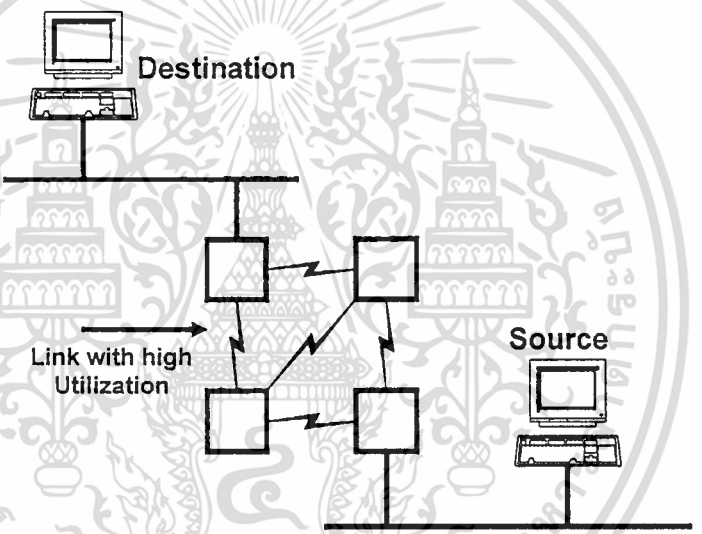
งานแรกของผู้บริหารเครือข่ายก็คือ อาจจะใช้เครื่องมือในการบริหารการกำหนดค่าตัวแปรและองค์ประกอบในการจำกัดการเข้าถึงคอมพิวเตอร์อื่น ๆ จากเทอร์มินอลเซิร์ฟเวอร์แต่อย่างไรก็

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตามการทำจะค้นหาว่าใครได้พยายามเข้าถึงข้อมูลของเครื่องเมนเฟรมในระบบรายจ่ายนั้นคงต้องทำการบันทึกเป็นช่วงเวลาที่แน่นอนว่ามีวิศวกรคนไหนเข้าใช้เทอร์มินอลเซิร์ฟเวอร์ในช่วงเวลาดังกล่าวบ้าง

เครื่องมือในการบริหารด้านการรักษาความปลอดภัย (Security Manegement Tool) ช่วยให้ผู้บริหารเครือข่ายสังเกตการณ์ (monitorring) จุดที่ทำการเข้าถึงเครือข่าย (access point) บนเทอร์มินอลเซิร์ฟเวอร์และบันทึกว่าวิศวกรคนไหนใช้อุปกรณ์อะไรบ้างในช่วงเวลาใด ๆ และยังสามารถส่งสัญญาเตือนเมื่อมีเหตุการณ์ที่ไม่ชอบมาพากลอีกด้วย

2.2.1.4 การบริหารประสิทธิภาพของระบบ (Performance Management)



รูปที่ 2.3 ทูลของการบริหารประสิทธิภาพช่วยให้สามารถทราบว่าเกิดปัญหาขึ้น

จะเกี่ยวกับการวัดประสิทธิภาพของเครือข่าย, ฮาร์ดแวร์, ซอฟแวร์, และสื่อของเครือข่าย ตัวอย่างเช่น ประะสิทธิภาพโดยรวมของระบบ (throughput), สัดส่วนการใช้งานทรัพยากรในเครือข่าย, อัตราของการเกิดความผิดพลาดและเวลาในการตอบสนอง การใช้ข้อมูลในการบริหารประสิทธิภาพวิศวกรสามารถมั่นใจได้ว่าเครือข่ายมีความสามารถในการตอบสนองความต้องการของผู้ใช้ได้ สมมติว่าผู้ใช้บ่นว่าการเคลื่อนย้ายข้อมูลข้ามเครือข่ายแย่มาก หากปราศจากเครื่องมือในการบริหารประสิทธิภาพแล้ววิศวกรก็ต้องตรวจหาความผิดพลาดของเครือข่ายเป็นอันดับแรกถ้าพบว่าไม่มีความผิดพลาดเกิดขึ้น ต่อไปก็ต้องทำการตรวจสอบประสิทธิภาพของการเชื่อมต่อของอุปกรณ์ระหว่างเครื่องปลายทางของผู้ใช้และปลายทางที่เคลื่อนย้ายข้อมูลผ่านเครือข่ายระหว่างการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ต่รวจสอบนี้อาจจะพบว่าค่าเฉลี่ยของการใช้ลิงค์ (Link) อันหนึ่งมีค่าสูงจนเกือบถึงขีดจำกัดแล้ว วิศวกรก็สามารถแก้ไขปัญหาของการเคลื่อนย้ายโดยการปรับปรุงลิงค์ หรือเพิ่มลิงค์ ใหม่เข้าไป เพื่อเพิ่มความสามารถในการเคลื่อนย้ายข้อมูล ถ้ามีเครื่องมือในการบริหารประสิทธิภาพ วิศวกรอาจจะตรวจพบได้ว่าลิงค์ นั้นเข้าใกล้ขีดจำกัดและทำการแก้ไขก่อนที่ประสิทธิภาพของระบบจะตกลง

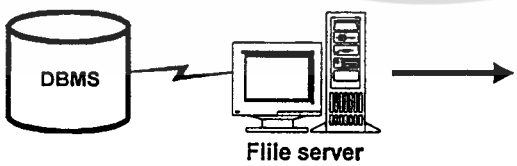
2.2.1.5 การบริหารแอคเคาน์ติ้ง (Accounting Management)

จะเกี่ยวกับการควบคุมการใช้ทรัพยากรในเครือข่ายของผู้ใช้ให้เพียงพอและคุ้มค่าที่สุดและยังเกี่ยวกับการเพิ่มหรือลบข้ออนุญาติสำหรับการเข้าใช้บริการเครือข่ายด้วย สมมติว่าเราต้องการปรับปรุงการสื่อสารกับเครือข่ายของไฟล์เซิร์ฟเวอร์ในแผนกต่าง ๆ เพราะไฟล์เซิร์ฟเวอร์รับภาระในการประมวลผลมากเกินไปถ้าปราศจากเครื่องมือในการบริหารแอคเคาน์ติ้งของเครือข่าย (accounnting management tool) แล้วเราจะไม่ทราบเลยว่าแต่ละแผนกมีไคลเอนท์ (Client) เข้าใช้บริการไฟล์เซิร์ฟเวอร์เป็นจำนวนเท่าไร ดังนั้นวิศวกรต้องถามผู้ใช้ว่ามีไคลเอ็นท์ เข้าใช้บริการไฟล์เซิร์ฟเวอร์ของแผนกต่าง ๆ เป็นเท่าไร และผลจากการตรวจสอบพบว่าแผนกเอกสารมีไคลเอ็นท์จำนวนมากที่สุดในการเข้าใช้บริการไฟล์เซิร์ฟเวอร์ และเมื่อวิเคราะห์แล้วพบว่าทราฟฟิก (traffic) ทั้งหมดของการเข้าใช้บริการไฟล์เซิร์ฟเวอร์เกือบครึ่งหนึ่งมาจากแผนกเอกสาร

วิศวกรเลยตัดสินใจเพิ่มไฟล์เซิร์ฟเวอร์ใหม่ขึ้นมาอีกหนึ่งตัวเพื่อให้แผนกเอกสารโดยเฉพาะเพื่อจะช่วยลดภาระของเซิร์ฟเวอร์ตัวเก่าลงได้ โดยการ ย้ายการอินเทอร์เฟส (Interface) ของแผนกเอกสารไปยัง เซร์ฟเวอร์ตัวใหม่

อย่างไรก็ตามถ้าหากมีเครื่องมือในการบริหารทางด้านแอคเคาน์ติ้งจะทำให้วิศวกรทราบได้อย่างรวดเร็วว่าแผนกไหนมีจำนวนไคลเอนท์เป็นเท่าไร และสามารถแก้ไขปัญหาได้เร็วยิ่งขึ้น (ดังรูป 2.4)

รูปที่ 2.4 แสดงทูลของ account management



Accounting Management Information

Account	% Network	# Client
Admin	8	3
Finance	4	2
Documentation	48	8
Sales	6	2
.	.	.
.	.	.
.	.	.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.3 สิ่งที่จำเป็นในการบริหารเครือข่าย

มีอยู่หลายสิ่งที่มีความจำเป็น สำหรับการบริหารเครือข่าย ซึ่งจะช่วยให้เราได้รับระบบบริหารเครือข่ายที่มีประสิทธิภาพมากเท่าที่เราต้องการ โดยสิ่งเหล่านั้นแบ่งออกเป็นหลัก ๆ ได้ดังนี้

- บุคลากรสำหรับการบริหาร ซึ่งก็คือผู้บริหารระบบเครือข่าย หรือ ผู้ที่ได้รับหน้าที่ในการบริหารเครือข่าย ซึ่งบุคคลเหล่านี้ต้องมีความรู้ในเรื่องทฤษฎีการบริหารและอุปกรณ์ที่ใช้สำหรับการบริหารเป็นอย่างดี
- อุปกรณ์ที่ใช้สำหรับการบริหาร ซึ่งอาจจะเป็น ฮาร์ดแวร์ หรือ ซอร์ฟแวร์ เช่น เครื่องคอมพิวเตอร์ที่ใช้สำหรับเป็นเครื่องทำการบริหาร และ ซอร์ฟแวร์การบริหาร เช่น HP-OpenView เป็นต้น อุปกรณ์เหล่านี้ก็ใช้สำหรับการเก็บข้อมูล หรือทำการตรวจสอบสภาพของระบบเครือข่ายที่เราทำการบริหาร
- ข้อมูลสำหรับการบริหาร เป็นข้อมูลเกี่ยวอุปกรณ์ หรือ ระบบที่เราทำการตรวจสอบเพื่อทำการบริหาร เช่น ข้อมูลของเครื่องเซิร์ฟเวอร์ หรือ เราท์เตอร์ ที่เราทำการตรวจจับ โดยใช้อุปกรณ์สำหรับการบริหาร
- ทฤษฎีและหลักการ ในการวิเคราะห์ข้อมูลดิบที่เก็บได้ จากอุปกรณ์ที่ใช้สำหรับการบริหารระบบ เช่น วิธีคิดคำนวณประสิทธิภาพของสายส่ง, วิธีคิดคำนวณปริมาณข้อมูลที่ส่ง และรับ ในแต่ละช่วงเวลา, วิธีคำนวณอัตราความผิดพลาดจากแต่ละแพ็กเก็ตของแต่โปรโตคอล เป็นต้น
- การวิเคราะห์ข้อมูลที่เก็บมาโดยอ้างอิงตามหลักทฤษฎีการบริหารเครือข่ายและนำเสนอแนวทางในการพัฒนาเครือข่ายเพื่อให้ได้ประสิทธิภาพและความน่าเชื่อถือที่เพิ่มขึ้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 3

ระบบบริหารเครือข่าย

3.1 การบริหารเครือข่าย

การบริหารเครือข่ายคอมพิวเตอร์ คือ กระบวนการในการควบคุมเครือข่ายข้อมูลที่มีความซับซ้อนให้ทำงานได้อย่างมีประสิทธิภาพสูงสุด

ดังที่ได้กล่าวไว้ในบทที่ 2 แล้วว่าขอบเขตของการบริหารเครือข่ายนั้นประกอบไปด้วย

- การบริหารความผิดพลาดในเครือข่าย (Fault Management)
- การบริหารเกี่ยวกับการกำหนดองค์ประกอบและตัวแปรของระบบ (Configuration Management)
- การบริหารทางด้านการรักษาความปลอดภัย (Security Menagement)
- การบริหารประสิทธิภาพของระบบ (Performance Management)
- การบริหารทางด้านแอคเคาท์ติ้ง (Accounting Management)

อุปกรณ์ในระบบเครือข่ายคอมพิวเตอร์ (Computer Network) ต้องการเครื่องมือที่ใช้ในการบริหารระบบ (Management Tools) เพื่อที่จะตรวจสอบความผิดพลาดที่เกิดขึ้น, ตรวจสอบสถานะ, ปรับแต่งระบบให้มีประสิทธิภาพหรือเพื่อเปลี่ยนค่าบางประการ รวมทั้งช่วยในการวางแผนงานด้วย มีบริษัทที่ผลิตเครื่องมือเหล่านี้จำนวนมาก โดยทำให้เป็นเครื่องมือพื้นฐานที่ช่วยให้การบริหารระบบเครือข่ายคอมพิวเตอร์เป็นไปโดยง่าย

โดยการบริหารระบบเครือข่ายนั้นจะมีสถาปัตยกรรมในการบริหารคือ

- สถาปัตยกรรมแบบระบบรวมศูนย์ (Centralized Architecture)
- สถาปัตยกรรมแบบระบบระดับชั้น (Hierachical Architecture)
- สถาปัตยกรรมแบบระบบกระจาย (Distributed Architecture)

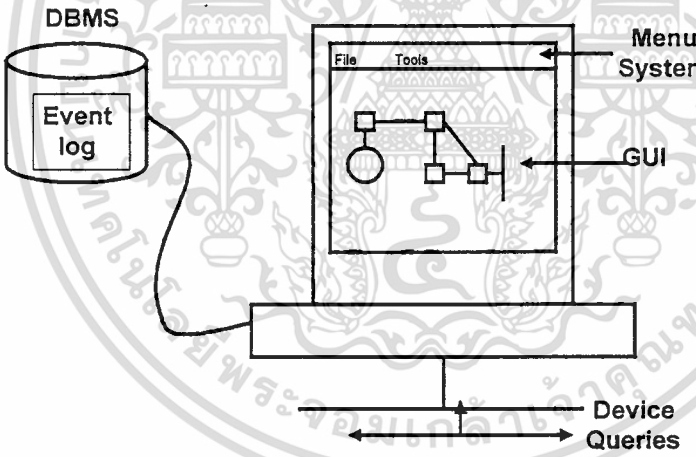
และทั้งหมดนี้จะได้กล่าวถึงรายละเอียดในหัวข้อต่อไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.2 แพลตฟอร์มของการบริหารเครือข่าย (Network Management Platform)

คือ ซอฟท์แวร์ ซึ่งจัดเตรียมหน้าที่การทำงานพื้นฐานในการบริหารเครือข่ายสำหรับองค์ประกอบต่าง ๆ ของเครือข่าย เป้าหมายของแพลตฟอร์มการบริหารเครือข่าย คือ เพื่อจัดเตรียมหน้าที่การทำงานทั่ว ๆ ไปสำหรับบริหารอุปกรณ์เครือข่ายหลาย ๆ รูปแบบที่ประกอบอยู่ในเครือข่าย (ดังรูป 3.1) หน้าที่การทำงานเหล่านี้ประกอบด้วย

- การสื่อสารกับผู้ใช้ผ่านทางภาพ (Graphic User Interface - GUI)
- แผนที่เครือข่าย (Network Map)
- ระบบจัดการฐานข้อมูล (Database Management System - DBMS)
- มาตราฐานในการค้นข้อมูลจากอุปกรณ์ต่าง ๆ ในเครือข่าย (Standard Method to query device)
- ระบบเมนูที่ผู้ใช้สามารถปรับเปลี่ยนได้ (Customize menu system)
- บันทึกเหตุการณ์บนเครือข่าย (Event log)



รูปที่ 3.1 แสดงระบบบริหารเครือข่าย

อุปกรณ์ในระบบเครือข่ายคอมพิวเตอร์ (Computer Network) ต้องการเครื่องมือที่ใช้ในการบริหารระบบ (Management Tools) เพื่อที่จะตรวจสอบความผิดพลาดที่เกิดขึ้น, ตรวจสอบสถานะ, ปรับแต่งระบบให้มีประสิทธิภาพหรือเพื่อเปลี่ยนค่าบางประการ รวมทั้งช่วยในการวางแผนงานด้วย มีบริษัทที่ผลิตเครื่องมือเหล่านี้จำนวนมาก โดยทำให้เป็นเครื่องมือพื้นฐานที่ช่วยให้การบริหารระบบเครือข่ายคอมพิวเตอร์เป็นไปโดยง่าย แต่อย่างไรก็ตาม เครื่องมือที่ผลิตขึ้นมักจะเป็นเครื่องมือเฉพาะของแต่ละบริษัทเท่านั้น เช่นระบบปฏิบัติการเครือข่ายคอมพิวเตอร์ก็จะมีกลุ่มของเครื่องมือที่ช่วยในการบริหารระบบของตัวเอง เราท์เตอร์(router) ก็จะมีเครื่องมือบริหารของตัวเอง เป็นต้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เครื่องมือในการบริหารระบบเครือข่ายคอมพิวเตอร์จะประกอบไปด้วยหลาย ๆ ส่วน เช่น ส่วนติดต่อกับผู้ใช้(user interface), ระบบส่งสัญญาณ (alarm systems) และฐานข้อมูลการบริหารระบบ (management database) ผู้ใช้จำเป็นต้องเรียนรู้วิธีใช้เครื่องมือทั้งหมดที่แตกต่างกันเหล่านี้ และเครื่องมือเหล่านี้มีบ่อยครั้งที่นำไปใช้ในระบบที่แตกต่างกัน เช่นบนระบบปฏิบัติการดอส (DOS) หรือยูนิกซ์ (UNIX) ที่แย่ที่สุดก็คือไม่มีทางที่จะรวมสิ่งต่าง ๆ เข้าเป็นอันเดียวกันได้ในระบบเครือข่ายคอมพิวเตอร์ อุปกรณ์ที่ต่ออยู่ในระบบจะถูกมองเป็นส่วนที่แยกจากกันเพื่อประโยชน์ในการบริหารระบบ

นับว่ายังโชคดีที่เครื่องมือในการบริหารระบบได้รวบรวมการบริหารต่าง ๆ มาไว้เข้าด้วยกัน เครื่องมือที่ใช้บริหารระบบเป็นซอฟท์แวร์ (software) เดี่ยวๆ ที่สามารถใช้แอพพลิเคชั่น (application) ที่เกี่ยวกันการบริหารระบบหลาย ๆ อันจากบริษัทที่ผลิตอุปกรณ์เครือข่ายได้ สิ่งสำคัญที่จะทำให้เป็นอย่างนี้ได้ก็คือ เครื่องมือที่ใช้บริหารระบบสามารถใช้ส่วนต่าง ๆ ของระบบร่วมกัน (share) คือ ส่วนติดต่อผู้ใช้, ระบบส่งสัญญาณรวมทั้งฐานข้อมูลด้วย การใช้ส่วนติดต่อผู้ใช้ร่วมกันจะทำให้ง่ายต่อการเรียนรู้ในการใช้แอพพลิเคชั่นหลาย ๆ อันได้ ,การใช้แผนที่ (map) และระบบส่งสัญญาณร่วมกันจะทำให้การมองระบบเครือข่ายเป็นส่วนเดียวกันได้ และการใช้ฐานข้อมูลร่วมกันจะทำให้มีสถิติสำหรับการวิเคราะห์ระบบและจะทำให้จัดทำรายงานได้ง่าย

อย่างไรก็ตามเครื่องมือสำหรับบริหารระบบเครือข่ายคอมพิวเตอร์ไม่ใช่ สิ่งที่จะทำทุกอย่างได้ เครื่องมือจะสนับสนุนจำนวนของแอพพลิเคชั่นที่จำกัดเท่านั้น ในระบบที่มีความซับซ้อนมาก ๆ มันจะไม่มีแอพพลิเคชั่นที่มาบริหารส่วนที่สำคัญ ๆ ของระบบได้ เช่น ระบบปฏิบัติการเครือข่าย อย่างไรก็ตาม เครื่องมือที่ใช้บริหารระบบก็สามารถลดจำนวนของสิ่งที่ต้องการในระบบบริหารลงได้ ผู้ใช้สามารถระบุเครื่องมือที่ครอบคลุมส่วนประกอบของระบบที่ต้องการการบริหารได้

องค์ประกอบย่อย ๆ ที่แยกจากกันในระบบเครือข่ายคือ แผนที่,ระบบส่งสัญญาณ,ส่วนติดต่อกับผู้ใช้และฐานข้อมูลจะถูกใช้เป็นส่วนสำคัญในการบริหารระบบของเครื่องมือต่าง ๆ โดยที่แอพพลิเคชั่นในการบริหารระบบจะแยกเป็นส่วน ๆ ตามส่วนประกอบดังที่กล่าวมา ทุกส่วนจะเป็นอิสระจากกัน และจะไม่มีการติดต่อสื่อสารกันโดยตรงกับส่วนอื่น ๆ ตัวอย่างเช่นถ้าเราท์เตอร์ เกิดมีปัญหาที่จะส่งผลกระทบถึงตัวให้บริการแฟ้มข้อมูล (file server) การติดต่อสื่อสารกันของแอพพลิเคชั่นที่ใช้บริหารระบบจะไม่สามารถส่งข้อมูลที่จะบอกถึงจุดที่เกิดปัญหาได้

ในบางแพลตฟอร์มการบริหาร (management platform) จะมีระบบส่งสัญญาณ เพื่อที่จะทำให้อุปกรณ์ที่เกิดปัญหาส่งรายงานความผิดพลาดหรือบอกปัญหาที่เกิดขึ้นได้โดยตรง ซึ่งจะทำให้ง่ายต่อการวิเคราะห์ว่าเกิดปัญหาอะไรจากอุปกรณ์ส่วนไหน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- การสื่อสารกับผู้ใช้ผ่านทางภาพมีประโยชน์หลายด้านด้วยกัน รวมทั้งทำให้ผู้ใช้เข้าถึงแพลตฟอร์มได้ง่ายยิ่งขึ้น ตัว จียูไอ(GUI) นี้อาจจะสร้างอยู่ในรูปมาตราฐานที่เรียกว่ามาตราฐาน ลุค-แอนด์-ฟีล (Look-and-Feel Standard) เช่นไมโครซอฟต์วินโดว์ ด้วยการใช้มาตราฐานของ จียูไอ นี้ทำให้แพลตฟอร์มสามารถใช้อุปกรณ์จากหลาย ๆ ยี่ห้อได้ ถ้าอุปกรณ์เหล่านั้นใช้มาตราฐาน จียูไอ เดียวกันนี้
- แผนที่จะมีประโยชน์สำหรับการบริหารเครือข่ายในทุก ๆ หน้าที่ เครื่องมือในการบริหารทางด้านความผิดพลาดสามารถใช้สีของแผนที่เป็นตัวแยกแยะปัญหาได้ เช่น สีแดง หมายถึง อุปกรณ์นั้นมีปัญหาร้ายแรง ส่วนการบริหารทางด้านการกำหนดโครงสร้างก็สามารถใช้แผนที่แสดงโครงสร้างทางกายภาพและทางตรรกะของเครือข่ายได้ในรูปแบบของรูปภาพ ส่วนการบริหารประสิทธิภาพของระบบสามารถแสดงประสิทธิภาพของระบบในรูปแบบของกราฟและใช้สีเป็นตัวแยกแยะข้อมูลในกราฟเหล่านี้เป็นต้น
- มาตราฐานในการค้นหาข้อมูลของอุปกรณ์จะสำคัญมากเพราะแพลตฟอร์มจะต้องเก็บข้อมูลขององค์ประกอบต่าง ๆ ใน เครือข่าย และอุปกรณ์จากผู้ขายต่าง ๆ กัน
- ระบบจัดการฐานข้อมูลช่วยให้ แอพพลิเคชั่นสามารถใช้ ฐานข้อมูลในการเก็บข่าวสารในการบริหารเครือข่าย สามารถใช้เทคนิคในทางฐานข้อมูลเพื่อสร้างความสัมพันธ์ของข้อมูลในระบบ เพื่อประโยชน์ในการบริหารและบำรุงรักษาระบบ ระบบจัดการฐานข้อมูลยังยอมให้ผู้ใช้สามารถออกแบบรายงานเองและจัดการสำรองข้อมูลโดยอัตโนมัติ
- สิ่งสุดท้ายที่ แพลตฟอร์มต้องมี คือ บันทึกเหตุการณ์ บันทึกเหล่านี้จะถูกเก็บอยู่ในรูปแบบที่สามารถอ่านได้เข้าใจ (Readable Format) แพลตฟอร์มจะบันทึกเหตุการณ์ต่าง ๆ ที่มันรู้จักและยังสามารถสร้างเหตุการณ์ขึ้นเองก็ได้ อุปกรณ์ในเครือข่าย ยังอาจจะส่งข่าวสาร (message) มาให้ แพลตฟอร์มแปลเป็นเหตุการณ์ที่เกิดขึ้นได้อีกด้วย แพลตฟอร์มจะไม่สนใจว่ามันจะต้องเรียนรู้เหตุการณ์เหล่านั้นหรือไม่แต่มันจะเก็บเหตุการณ์เหล่านั้นไว้เพื่อให้วิศวกรใช้ในการบริหารเครือข่าย และเพื่อปรับปรุงให้เครือข่ายทันต่อเหตุการณ์อยู่เสมอ

3.2.1 ส่วนประกอบของแพลตฟอร์มการบริหารระบบ (Elements of a Management Platform)

แพลตฟอร์มบริหารระบบประกอบไปด้วยซอฟท์แวร์ที่ทำงานบนสถานีกลางการบริหาร (management station) และสามารถที่จะแบ่งได้เป็นผู้ให้บริการการบริหาร (management server) ที่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ซึ่งใช้เก็บรวบรวมข้อมูลและเป็นที่ทำการทำงาน (processing) และอีกส่วนหนึ่งคือ ส่วนที่ใช้เป็นที่ดูแสดงสถานะต่าง ๆ (viewing station) แพลตฟอร์มกลางจะมีการติดต่อสื่อสารกับเอเจ้นต์ (agent) ที่ทำงานอยู่บนอุปกรณ์ต่าง ๆ เอเจ้นต์จะเป็นตัวเฝ้าดูอุปกรณ์ต่าง ๆ และจะส่งข้อมูลต่าง ๆ เช่น สัญญาณ,สถิติ หรือข้อมูลอื่น ๆ ที่ต้องการให้กับส่วนสถานีกลางการบริหาร

ตัวอย่างซอฟท์แวร์ที่อยู่ในแพลตฟอร์มคือ แผนที่, ฐานข้อมูล,แอพพลิเคชั่นที่ใช้บนโปรโตคอล เอสเอ็นเอ็มพี (SNMP protocol) และเครื่องมือที่ช่วยในการแก้ไขค่าผิดพลาดอย่างอัตโนมัติหรือจัดการอัพเดทข้อมูลอัตโนมัติ(autodiscovery) ในสถานีการบริหาร (management platform) ทั่ว ๆ ไปเช่น เอชพีโอเพ็นวิว(HP OpenView), ไอบีเอ็มซีสเต็มวิวเน็ทวิว (IBM SystemView NetView) ได้รวบรวมการบริหารทั่ว ๆ ไปสำหรับอุปกรณ์ที่สนับสนุนมาตรฐานของโอเอสไอ (OSI : Open System Interconnection)

3.2.1.1 ระดับชั้นแผนที่เครือข่าย (Hierarchical Network Map)

เพื่อให้วิศวกรสามารถสร้างกราฟ ได้ เช่น กราฟวงกลม หรือ กราฟแท่งและสามารถนำกราฟเหล่านี้เพื่อไปรวมกับรายงานแล้วนำเสนอต่อผู้บริหาร กราฟของความผิดพลาดในเครือข่ายช่วยได้ในงานบริหารทางด้านความผิดพลาดและประสิทธิภาพของระบบ กราฟประวัติของข้อมูลช่วยในการพยากรณ์แนวโน้มของเครือข่ายในอนาคต

แผนที่เครือข่ายที่มีการแบ่งเป็นระดับ เป็นขั้นๆ จะทำให้ผู้บริหารระบบเครือข่าย (network manager) สามารถดูเครือข่ายได้เป็นระดับ ๆ ที่แตกต่างกันได้ ตัวอย่างเช่น ในระดับสูงสุดของแผนที่จะแสดงภาพของโลก มีเส้นเชื่อมต่อระหว่างประเทศต่าง ๆ ที่มีเครือข่ายอยู่ ,ในระดับถัดลงมาอาจจะแสดงถึงประเทศสหรัฐอเมริกาที่ซึ่งมีเส้นเชื่อมต่อระหว่างเมืองต่าง ๆ ,ระดับต่อไปจะแสดงรายละเอียดในแต่ละเมือง ตำแหน่งของเครือข่ายภายในเมือง และในระดับถัด ๆ ไปก็จะแสดงรายละเอียดในระดับที่เฉพาะเจาะจงลงไปเรื่อย ๆ เช่นแสดงถึงเครือข่ายแต่ละเครือข่ายประกอบไปด้วยตัวเชื่อมต่อ (gateway) หรือฮับ (hub) อะไรบ้าง

ในแต่ละระดับผู้จัดการระบบจะสามารถเข้าไปดูรายละเอียดในตำแหน่งต่าง ๆ ที่เชื่อมกันอยู่ หรือในตำแหน่งปัจจุบันได้ เพื่อที่จะได้ไปเอารายละเอียดของข้อมูลต่าง ๆ ของตำแหน่งนั้น ๆ และในรายละเอียดเหล่านั้น ผู้จัดการระบบก็สามารถเข้าไปดูรายละเอียดของส่วนต่าง ๆ ได้อีก จะเป็นขั้น ๆ เช่นนี้เรื่อยไปจนถึงระดับที่ล่างสุด เช่นเป็นรายละเอียดของพอร์ต (port) หรือฮับต่าง ๆ

สิ่งที่กล่าวมานั้นเป็นการเข้าไปและดูรายละเอียดของแต่ละระดับโดยเริ่มจากระดับบนสุดเป็นระดับที่กว้างสุด เรื่อยลงมาระดับล่าง ๆ ซึ่งเป็นระดับที่แคบเข้ามาและจะเป็นการเฉพาะเจาะจง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

มากขึ้น ซึ่งในระดับต่าง ๆ นั้น จะมีข้อมูลที่ใช้ในการสร้างแผนที่และจะเก็บไว้ในฐานข้อมูล และเมื่อมีการแก้ไขแผนที่หรือมีการปรับปรุงก็จะมีการปรับปรุงฐานข้อมูลอัตโนมัติด้วย

สถานะภาพของอุปกรณ์ที่ต่ออยู่ในระบบและที่แสดงอยู่ในแผนที่นั้นจะถูกแทนด้วยสีต่าง ๆ เช่นสีแดงจะแทนอุปกรณ์ที่มีปัญหารุนแรง, สีเหลืองจะแทนอุปกรณ์ที่มีปัญหารองลงมาจากสีแดง สีเขียวจะเป็นสถานะปกติ อุปกรณ์ที่มีปัญหาอาจจะมีการกระพริบ และอาจมีเสียงเตือนเพื่อที่จะให้ผู้บริหารระบบได้รู้

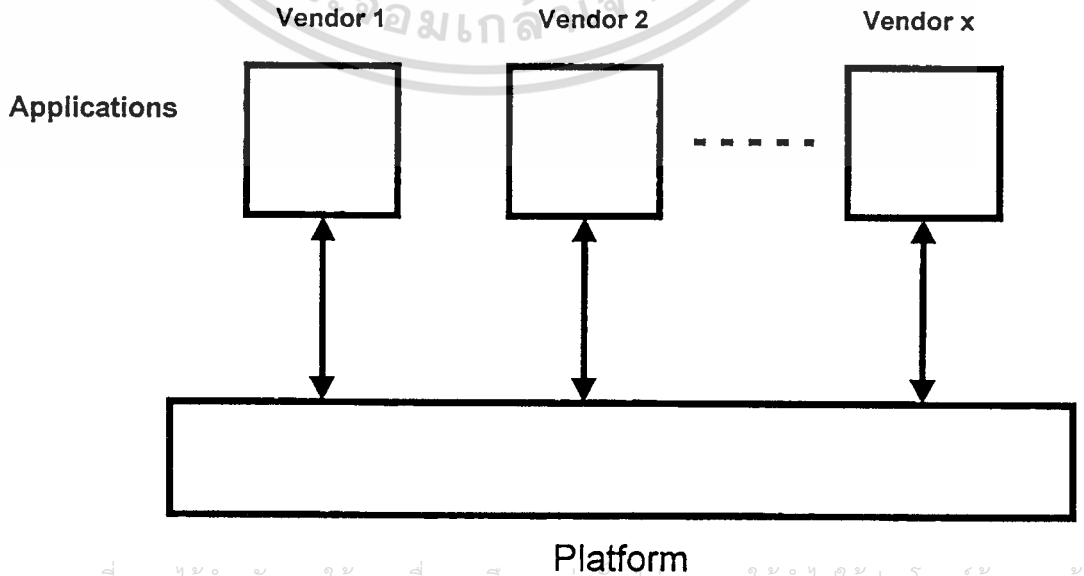
ในระบบที่ไม่มีการแบ่งแผนที่เป็นระดับขั้นนั้นจะแสดงเครือข่ายด้วยรูปภาพเรียบ ๆ ระดับเดียว ซึ่งจะเป็นระดับต่ำสุดคือจะเป็นรายละเอียดของอุปกรณ์เครือข่ายต่าง ๆ

3.2.1.2 ฐานข้อมูลของระบบเครือข่าย (Network Information Database)

ในแต่ละแพลตฟอร์มเครือข่ายจะต้องการระบบฐานข้อมูลที่จะเก็บข้อมูลเกี่ยวกับเครือข่าย และข้อมูลเกี่ยวกับอุปกรณ์ในระบบเครือข่าย เช่น เอ็นเอ็มเอฟ (Netware Management System) ที่จะใช้มาตรฐานของเน็ทแวร์ (netware) ดังนั้นแอพพลิเคชั่นที่ใช้มาตรฐานนี้จะสามารถเข้าถึงฐานข้อมูลการบริหารนี้ได้ แต่อย่างไรก็ตามบริษัทฮิวเล็ทแพ็คการ์ดไม่ได้ให้ผู้ใช้เข้าถึงฐานข้อมูลใน โอเพ็นวิว สำหรับวินโดว์ (OpenView for WINDOWS)

3.3 แอพพลิเคชั่นการบริหารเครือข่าย (Network Management Application)

เป็นซอฟต์แวร์ที่ใช้ในการบริหารเครือข่ายเหมือนกับแพลตฟอร์ม แต่แพลตฟอร์มจะมีฟังก์ชั่น ในการบริหารแบบทั่ว ๆ ไป ในขณะที่ แอพพลิเคชั่นจะเป็นการบริหารเฉพาะอุปกรณ์บางกลุ่มเป็นการเฉพาะ ความสัมพันธ์ระหว่าง แพลตฟอร์มละแอพพลิเคชั่นแสดงดังรูป



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 3.2 แสดงความสัมพันธ์ระหว่าง แพลตฟอร์มละแอพพลิเคชั่น

แอพพลิเคชั่นเหล่านี้จะถูกพัฒนาโดยผู้ขายอุปกรณ์เครือข่ายเพื่อให้ลูกค้าใช้บริหารอุปกรณ์เหล่านั้น ตัวอย่างเช่น ผู้ผลิตโมเดม, ฮับ หรือ บริดจ์ จะสร้างแอพพลิเคชั่นที่ทำงานบนแพลตฟอร์มในการสร้างเครื่องมือให้วิศวกรผู้บริหารเครือข่าย การใช้กลยุทธ์นี้วิศวกรจำเป็นต้องลงทุนเฉพาะแต่เครื่องมือที่ใช้บริหารกับอุปกรณ์เฉพาะกลุ่มเท่านั้น ตัวอย่าง เช่น ถ้าต้องการบริหารเครือข่ายของไฟล์เซิร์ฟเวอร์กับฮับ เราก็สามารถสอบถามเกี่ยวกับแอพพลิเคชั่นที่จะนำมาใช้บริหารเครือข่ายนี้เอาจากผู้ขายก็ได้ เสร็จแล้วเราก็จะได้ระบบบริหารเครือข่ายที่ประกอบด้วยแพลตฟอร์มที่มีฟังก์ชั่นในการบริหารแบบทั่ว ๆ ไป และ มีแอพพลิเคชั่นที่ใช้ในการบริหารไฟล์เซิร์ฟเวอร์และฮับที่การเฉพาะโดยแผนที่เดียวกัน ระบบเมนูเดียวกัน ใช้ภาพที่ติดต่อกับผู้ใช้อันเดียวกัน และ ใช้ระบบฐานข้อมูลเดียวกัน

3.3.1 แอพพลิเคชั่นการบริหารเครือข่ายมีเป้าหมายดังต่อไปนี้

- มีประสิทธิภาพในการบริหารเครือข่ายในกลุ่มที่จำเพาะเจาะจงเอาไว้
- หลีกเลี่ยงฟังก์ชั่นการบริหารที่จะซ้ำซ้อนกับแพลตฟอร์ม
- ทำงานร่วมกับแพลตฟอร์มผ่านทาง เอพีไอ และ ระบบเมนู
- สามารถทำงานได้กับหลาย ๆ แพลตฟอร์ม

แอพพลิเคชั่นต้องบริหารอุปกรณ์ได้อย่างมีประสิทธิภาพเพื่อช่วยเพิ่มประสิทธิภาพโดยความของเครือข่าย ตัวอย่างเช่น ผู้ผลิต ฮับ ก็จะสร้าง แอพพลิเคชั่นที่สามารถแสดงสถานะและการเชื่อมต่อของพอร์ตทางด้านกายภาพได้เมื่อผู้ใช้เลือกดูฮับจากแผนที่เครือข่าย สามารถอนุญาตให้ผู้ใช้สามารถสั่งเปิด-ปิด พอร์ตได้ หรือสังเกตการณ์อัตราการเกิดความผิดพลาด (error rate) และประสิทธิภาพโดยรวมของฮับ แอพพลิเคชั่นนี้จะช่วยให้วิศวกรบริหารในด้านการกำหนดค่าคอนฟิกกิวเรชั่นและประสิทธิภาพของฮับให้สำเร็จลุล่วงไปด้วยดี

แอพพลิเคชั่นจะต้องไม่สร้างฟังก์ชั่นที่ซ้ำซ้อนกับแพลตฟอร์มเพราะอาจจะทำเกิดการทำงานที่ซ้ำซ้อนกันเพื่อต้องการผลลัพธ์อันเดียวกัน และอาจจะทำให้ผู้ใช้เกิดความสับสนและความพยายามของนักพัฒนาแอพพลิเคชั่นนั้นสูญเปล่าอีกด้วย แต่กฎนี้มีข้อยกเว้นอยู่ คือ ในกรณีแพลตฟอร์มไม่มีฟังก์ชั่นที่แอพพลิเคชั่นต้องการ เช่น แพลตฟอร์มมีแต่ฟังก์ชั่นสำหรับสร้างกราฟแท่ง แต่ แอพพลิเคชั่นต้องการสร้างกราฟวงกลม ดังนั้น แอพพลิเคชั่นก็ต้องสร้างฟังก์ชั่นในการสร้างกราฟวงกลมขึ้นมา และถ้าแต่ละแอพพลิเคชั่นต่างก็มีฟังก์ชั่นในการสร้างกราฟวงกลมเป็นของตนเอง วิศวกรก็ต้องพยายามอย่างยิ่งที่จะต้องประสานแอพพลิเคชั่นเหล่านี้ให้ได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แอพพลิเคชั่นต้องเชื่อมเข้ากับระบบบริหารเครือข่ายทาง เอพีไอ และ ระบบเมนู เอพีไอ จะทำให้โปรแกรมภายนอกสามารถเชื่อมการทำงานเข้ากับระบบบริหารเครือข่ายได้ ส่วนระบบเมนูนั้นช่วยให้โปรแกรมที่ไม่ได้ทำงานอย่างอิสระเข้าใช้เมนูร่วมกันบนแพลตฟอร์ม

โปรแกรมภายนอกจะได้รับอนุญาตให้เข้าถึงข้อมูลเพื่อค้นข่าวสารในแพลตฟอร์มได้เฉพาะผ่านทาง เอพีไอ เท่านั้น เช่น ในการใช้แผนที่ของเครือข่าย การรวมแอพพลิเคชั่นเข้ากับระบบเมนูของแพลตฟอร์ม หรือการดึงข้อมูลจากระบบฐานข้อมูล หรือการส่งเหตุการณ์ต่าง ๆ มายังแพลตฟอร์ม และ อื่น ๆ เอพีไอ ต้องเป็นมาตราฐานที่สามารถทำงานได้กับหลาย ๆ แพลตฟอร์ม เพราะถ้าไม่เป็นเช่นนั้นแล้ว แอพพลิเคชั่นที่เขียนขึ้นมาเพื่อทำงานบนแพลตฟอร์มก็ต้องถูกเขียนใหม่เมื่อมีการเปลี่ยนแพลตฟอร์ม

แอพพลิเคชั่นในการบริหารเป็นหัวใจสำคัญของแพลตฟอร์มเครือข่ายคอมพิวเตอร์ หากปราศจากแอพพลิเคชั่นแล้ว แพลตฟอร์มก็ไม่มีประโยชน์ และเพื่อเป็นการสนับสนุนให้ผู้พัฒนาระบบสามารถสร้างแอพพลิเคชั่นได้แล้ว บริษัทผู้ผลิตแพลตฟอร์มเครือข่ายจะเสนอส่วนติดต่อของแอพพลิเคชั่น (APIs : Application Program Interface) และ เครื่องมือการพัฒนา (developer's kits) เพื่อทำให้การพัฒนาแอพพลิเคชั่นได้ง่ายขึ้น

3.4 เอเจ้นต์ (agent)

เอเจ้นต์คือเฟิร์มแวร์ (firmware) หรือซอฟท์แวร์ที่ทำหน้าที่จับตามองอุปกรณ์หรือระบบและเมื่อมีการร้องของหรือเกิดเหตุฉุกเฉินขึ้น เอเจ้นต์จะส่งข้อมูลเช่นสถิติ หรือสัญญาณไปที่แอพพลิเคชั่นบริหารเครือข่ายที่สถานีกลาง (station) เอเจ้นต์จะอยู่ภายในอุปกรณ์ที่ถูกบริหาร (managed device)

3.4.1 สัญญาณและเหตุการณ์ (Alarms and Events)

สัญญาณจะถูกทำให้เกิดโดยการกำหนดของผู้ใช้ว่าจะให้เกิดเมื่อไร เช่นในตัวเชื่อมต่อเครือข่าย (network adapter)เกิดการ ดร๊อป (drop) ของข้อมูลมากกว่าจำนวนของแพ็กเก็ตต่อชั่วโมง เอเจ้นต์ที่อยู่ในตัวเชื่อมต่อเครือข่ายจะส่งสัญญาณไปที่ส่วนกลาง การส่งสัญญาณอาจจะถูกกำหนดให้ส่งได้โดยเงื่อนไขหลาย ๆ อย่าง โดยจะส่งเมื่อเงื่อนไขเหล่านี้ต้องเกิดขึ้นพร้อมกัน การส่งสัญญาณที่ใช้ระบบผู้เชี่ยวชาญ(expert system) มาช่วยจะทำให้สามารถระบุถึงความผิดพลาดที่เกิดขึ้นได้ง่ายและชัดเจน และยังทำให้สามารถสร้างรายงานได้ง่ายอีกด้วย ซึ่งจะนำไปสู่กระบวนการแก้ไขปัญหาที่เกิดขึ้นได้ง่ายด้วย

เหตุการณ์คือข้อความที่ส่งจากเอเจ้นต์ไปสู่สถานีกลาง ซึ่งส่วนใหญ่จะเป็นรายงานธรรมดามากกว่าที่จะเป็นความผิดพลาดที่เกิดขึ้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ลักษณะเด่นอีกประการหนึ่งของแพลตฟอร์มในการบริหารเครือข่าย **คือ การรักษาความปลอดภัยของระบบบริหารเครือข่าย** การรักษาความปลอดภัยจะถูกบริหารโดยระบบปฏิบัติการของระบบคอมพิวเตอร์นั้น ๆ แต่โดยส่วนมากความปลอดภัยที่ระบบปฏิบัติการมีให้นั้นไม่เพียงพอ ดังนั้นองค์กรต้องสร้างระบบรักษาความปลอดภัยขึ้นมาเอง

หน้าที่การทำงานพื้นฐานเหล่านี้จะทำให้วิศวกรสามารถทำงานตามฟังก์ชั่นของการบริหารได้สำเร็จ วิศวกรสามารถค้นข้อมูลจากอุปกรณ์ในเครือข่ายและนำข้อมูลเหล่านั้นไปใช้ในหลาย ๆ ทาง ตัวอย่าง เช่น ต้องการสร้างกราฟแสดงปริมาณการใช้งานของซีเรียลลิงค์ (Serial link) ทั้งหมดในเครือข่าย อาจต้องทำตามขั้นตอนต่อไปนี้

1. เลือกข้อมูลที่จำเป็น (โดยปกติจะเป็น ไบต์ ที่รับเข้ามาและส่งออกไป)
2. เก็บข้อมูลที่เกี่ยวข้องโดยใช้แพลตฟอร์มบริหารเครือข่าย
3. นำข้อมูลเหล่านั้นมาสร้างกราฟที่ต้องการ

ขั้นตอนแรกจะเป็นขั้นตอนที่ยากที่สุด ถึงแม้ว่าแพลตฟอร์มจะสามารถค้นข้อมูลจากเครือข่ายได้ แต่องค์ประกอบแต่ละส่วนของเครือข่ายก็จะเก็บข้อมูลในรูปแบบที่เฉพาะยิ่งมีองค์ประกอบมากก็ยิ่งมีข้อมูลหลายรูปแบบ แต่ในปัจจุบันนี้ข้อมูลจะถูกเก็บอยู่ในรูปแบบมาตราฐาน คือ ฐานข้อมูลที่เก็บข่าวสารต่าง ๆ ในการบริหาร (Management Information Base - MIB) หมายความว่าเราเพียงเรียนรู้ข้อมูลชิ้นหนึ่งก็สามารถรู้จักข้อมูลอื่น ๆ ที่เก็บอยู่รูปแบบเดียวกันได้ แต่อย่างไรก็ตาม เอ็มไอบี ก็ยังประกอบด้วยรูปแบบข้อมูลที่เป็นมาตราฐานอยู่นับร้อยรูปแบบเหมือนกัน

3.5 สถาปัตยกรรมการบริหารเครือข่ายแบบต่าง ๆ

แพลตฟอร์มของการบริหารเครือข่ายอาจจะมีสถาปัตยกรรมหลายรูปแบบ แต่ที่รู้จักกันดีจะมีอยู่ 3 แบบ

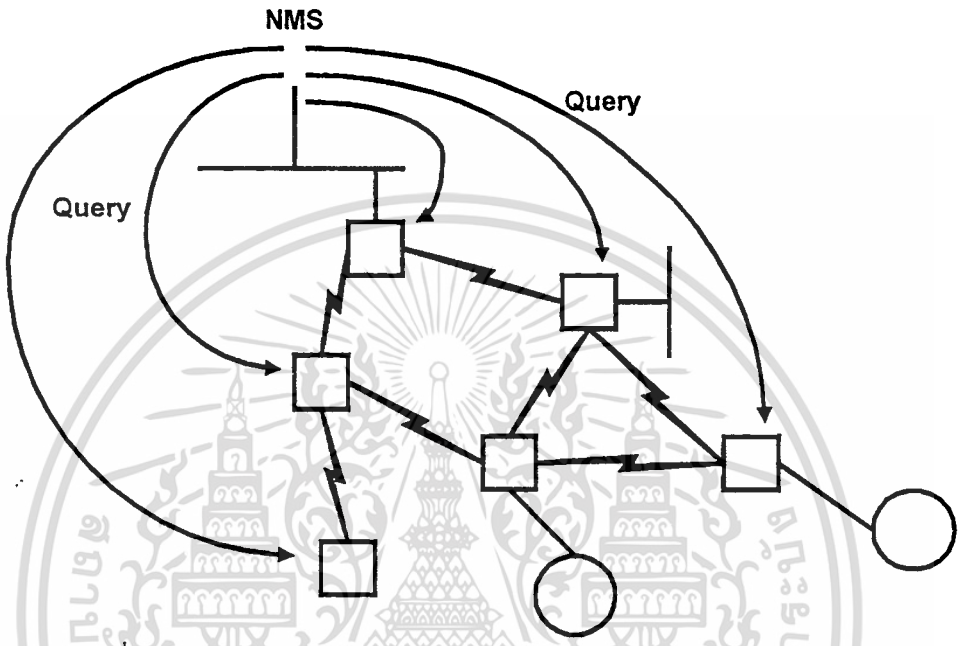
- แบบระบบรวมศูนย์ (Centralized Architecture)
- แบบระบบระดับชั้น (Hierachical Architecture)
- แบบระบบกระจาย (Distributed Architecture)

3.5.1 สถาปัตยกรรมแบบระบบรวมศูนย์ (Centralized Architecture)

ในระบบนี้จะมีแพลตฟอร์มเพียงหนึ่งตัวในการบริหารเครือข่ายทั้งหมด ดังรูป จะรวมระบบฐานข้อมูลไว้ที่จุดศูนย์กลางเพียงแห่งเดียว สำหรับการเก็บข้อมูลที่มากเกินไปจะถูกสำรองข้อมูลไปยังระบบอื่นตามช่วงเวลาอินเทอร์วอล (Interval time) ถึงแม้ว่า ระบบนี้เป็นศูนย์กลางเพียงระบบเดียวสำหรับการบริหการเครือข่ายทั้งหมด แต่มันก็ยังสามารถ แอคเซส (Access) หรือ ส่ง อีเวนต์ (Event) ไปยังจุดอื่น ๆ ในเครือข่ายได้ จุดศูนย์กลางของสถาปัตยกรรมแบบนี้จะใช้สำหรับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
038309

- รับและส่งสัญญาณเตือนทั้งหมดของเครือข่าย
- บริหารเกี่ยวกับข่าวสารทั้งหมดของเครือข่าย
- เข้าถึง แอพพลิเคชั่นทั้งหมดในเครือข่าย



รูปที่ 3.3 แสดงสถาปัตยกรรมแบบรวมศูนย์ของระบบบริหารเครือข่าย

ด้วยการใช้สถาปัตยกรรมแบบรวมศูนย์นี้วิศวกรสามารถทำงานในที่เดียวในการดูสัญญาณเตือนและเหตุการณ์ต่าง ๆ ในเครือข่าย การมีสถานที่เพียงแห่งเดียวในการควบคุมการบริหารเครือข่ายทำให้เกิดความสะดวกและเกิดความปลอดภัยเพราะจะทำให้รักษาความปลอดภัยได้ง่าย ในทางภายภาพแล้วจุดที่เป็นศูนย์กลางในการบริหารเครือข่ายจะเป็นเขตหวงห้ามและจะอนุญาตเฉพาะเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้น

อย่างไรก็ตามการมีหน้าที่การทำงานขึ้นอยู่กับระบบการบริหารเพียงระบบเดียวจะไม่ค่อยดีนักสำหรับการสำรองข้อมูลเพราะถ้าเกิดระบบฐานข้อมูลในศูนย์นี้มีปัญหานั่นคือหมายถึงข้อมูลของทั้งระบบมีปัญหาและเวลามีอุปกรณ์หรือองค์ประกอบของเครือข่ายเพิ่มมากขึ้นจะเป็นเรื่องที่ยากและต้องใช้ค่าใช้จ่ายสูงที่จะทำให้ระบบเพียงระบบเดียวรับภาระทั้งหมดที่เพิ่มขึ้น

ข้อเสียที่สำคัญของสถาปัตยกรรมแบบนี้คือ การค้นข้อมูลในตัวอุปกรณ์เพราะการค้นข้อมูลจะต้องใช้ลิงค์ทุกลิงค์ที่เชื่อมตัวอุปกรณ์กับระบบบริหารทำให้ลิงค์ทั้งหมดต้องรับภาระเพิ่มขึ้นและใช้สื่อสารข้อมูลได้น้อยลงเนื่องจากถูกแบ่งแบนด์วิธไปใช้ในการค้นข้อมูล การวางระบบบริหาร

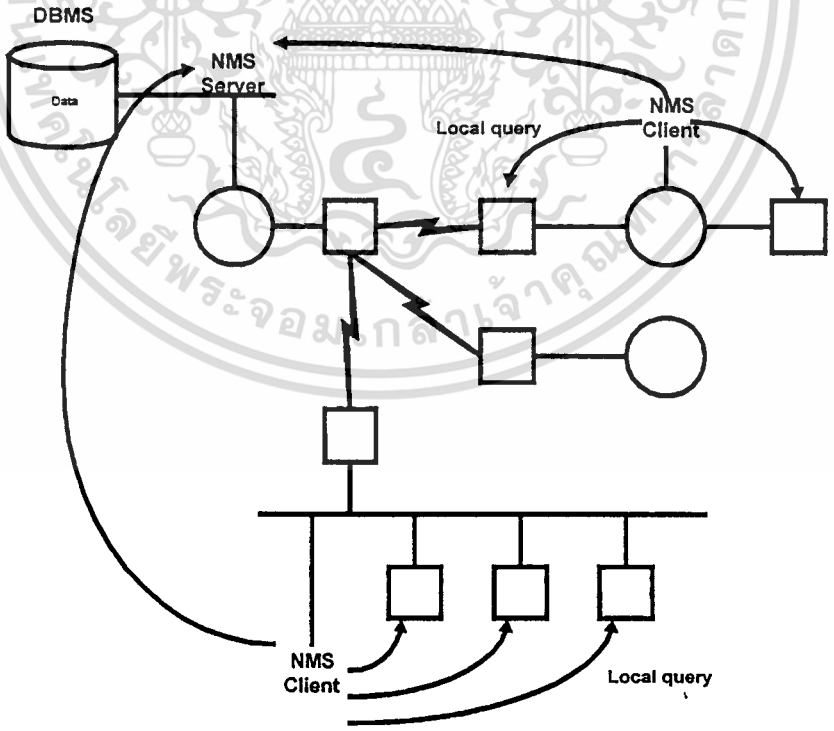
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เครือข่ายไว้ในตำแหน่งที่เป็นศูนย์กลางของเครือข่ายจะช่วยลดปัญหานี้ลงได้ แต่ในตำแหน่งดังกล่าวอาจจะไม่ใช่ตำแหน่งที่วิศวกรสามารถทำงานอยู่ได้

ตัวอย่างของแพลตฟอร์มที่มีสถาปัตยกรรมแบบรวมศูนย์ ได้แก่ IBM Netview ซึ่งทำงานบนเครื่องตัวเดียวและใช้บริการเครือข่าย System Network Architecture (SNA) ของ ไอบีเอ็ม ผู้ใช้จะสามารถเข้าถึงศูนย์บริหารเครือข่ายนี้ได้จากหลาย ๆ จุด ซึ่งจุดเหล่านี้สามารถขอดูและรับอีเวนต์ต่าง ๆ ในเครือข่ายได้ จุดเหล่านี้เรียกว่า คอนโซล (Console)

3.5.2 สถาปัตยกรรมแบบระบบระดับชั้น (Hierachical Architecture)

ในสถาปัตยกรรมแบบนี้จะใช้ระบบบริหารเครือข่ายหลาย ๆ ระบบ โดยมีระบบหนึ่งทำหน้าที่เป็นศูนย์กลาง และ ตัวที่เหลือจะทำหน้าที่เหมือนไคลเอนท์ (Client) ดังรูป บางฟังก์ชั่นในการบริหารจะอยู่ที่ตัวศูนย์กลางหรือเซิร์ฟเวอร์และฟังก์ชั่นอื่น ๆ จะอยู่ที่ตัวไคลเอนท์ ตัวอย่างเช่น วิศวกรสามารถกำหนดโครงสร้างของตัวไคลเอนท์ที่แยกออกมาต่างหากเพื่อใช้ในการสังเกตการณ์และโพลพอร์ตต่าง ๆ ของเครือข่าย



รูปที่ 3.4 แสดงสถาปัตยกรรมแบบระดับชั้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แพลตฟอร์มสามารถใช้เทคโนโลยี ไคลเอนท์/เซิร์ฟเวอร์ ในการบริหารระบบฐานข้อมูล ตัวไคลเอนท์ไม่จำเป็นต้องมีระบบฐานข้อมูลเอง แต่จะใช้ระบบฐานข้อมูลของตัวศูนย์กลางโดยเข้าถึงข้อมูลผ่านทางเครือข่าย เนื่องจากตัวศูนย์กลางนี้มีความสำคัญมากในสถาปัตยกรรมแบบ ระบบระดับชั้น ดังนั้นจำเป็นต้องมีการสำรองข้อมูลสำหรับรีดันแดนซ์ (Redundancy)

สถาปัตยกรรมแบบระบบระดับชั้นมีลักษณะเด่นดังต่อไปนี้

- ไม่ขึ้นอยู่กับระบบการบริหารเครือข่ายเพียงระบบเดียว
- มีการกระจายงานบริหารไปยังระบบบริหารอื่น ๆ ในเครือข่าย
- กระจายการสังเกตการณ์เครือข่าย ไปตลอดเครือข่าย
- มีการเก็บข้อมูลข่าวสารไว้ที่จุดศูนย์กลาง

วิธีการแบบระบบระดับชั้นช่วยแก้ปัญหาของระบบรวมศูนย์ได้อย่างหนึ่ง คือ ได้กระจายงานบริหารเครือข่ายจากศูนย์กลางออกไปยังตัวไคลเอนท์ วิศวกรสามารถกระจายงาน สังเกตการณ์ไปยังตัวไคลเอนท์ จะช่วยลดงานแบนด์วิธที่ต้องใช้ในการบริหารเครือข่ายลงได้มาก

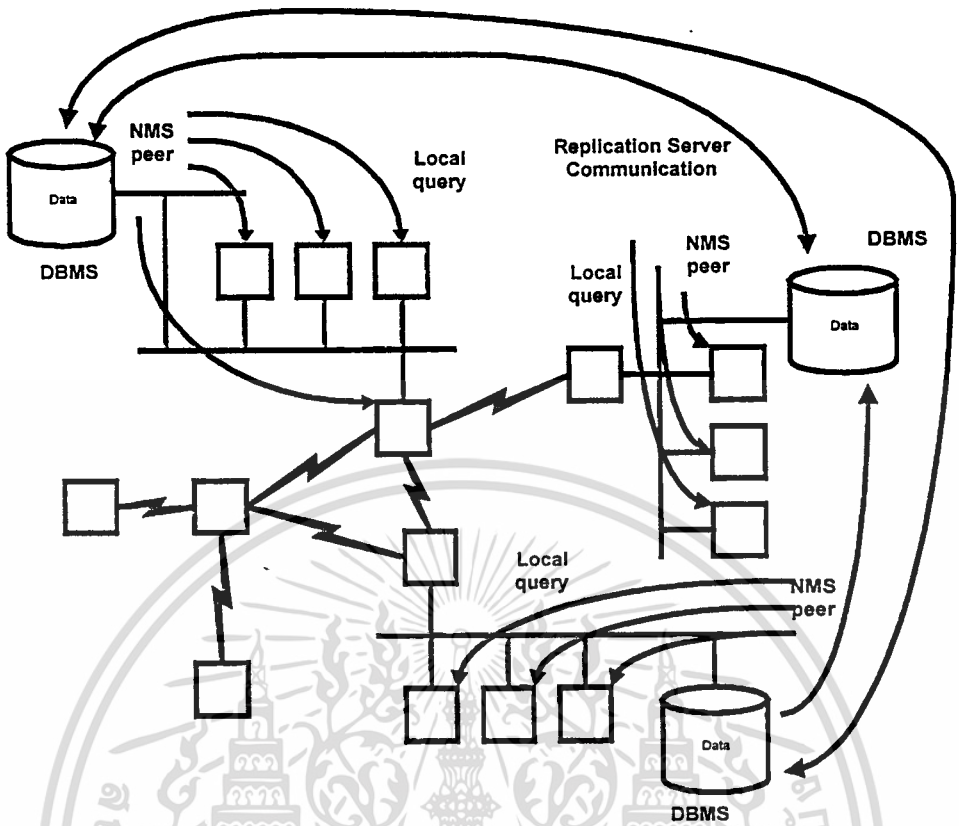
เนื่องจากระบบระดับชั้นใช้ระบบบริหารเครือข่ายหลาย ๆ ระบบทำงานด้วยกัน จึงไม่มีตำแหน่งใดเป็นศูนย์กลางอีกต่อไป ซึ่งอาจจะทำให้การเก็บข่าวสารยากขึ้นเล็กน้อยสำหรับวิศวกร และอีกปัญหาหนึ่งก็คือรายการอุปกรณ์ของแต่ละระบบบริหารต้องทำให้ชัดเจนเพราะถ้าผิดพลาดแล้วอาจจะทำให้มีการโพลอุปกรณ์ตัวเดียวกันโดยระบบบริหารมากกว่าหนึ่งระบบ ต้องเสียเวลาและแบนด์วิธโดยเปล่าประโยชน์

แพลตฟอร์มที่มีสถาปัตยกรรมแบบนี้ที่รู้จักกันดี ได้แก่ SunConnect SunNet Manager,HP Openview

สถาปัตยกรรมแบบระบบกระจาย (Distributed Architecture)

ในสถาปัตยกรรมแบบนี้จะรวมเอาแบบรวมศูนย์และระบบระดับชั้นเข้าด้วยกัน (ดังรูป 3.5) แทนที่จะใช้แพลตฟอร์มแบบศูนย์กลางและแบบระดับชั้น สถาปัตยกรรมนี้จะใช้แพลตฟอร์มที่เท่าเทียมกัน (multiple peer platforms) หลาย ๆ ตัวทำงานด้วยกัน โดยจะมีแพลตฟอร์มหนึ่งทำหน้าที่เสมือนตัวนำในกลุ่ม แต่ละแพลตฟอร์มจะมีระบบฐานข้อมูลอย่างสมบูรณ์แบบสำหรับอุปกรณ์ทุกตัวบนเครือข่ายและสามารถบริหารกับอุปกรณ์เหล่านั้นได้อย่างเต็มที่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.5 แสดงสถาปัตยกรรมการบริหารแบบกระจาย

เนื่องจากสถาปัตยกรรมแบบนี้ได้เชื่อมเอาแบบรวมศูนย์และระดับชั้นเข้าด้วยกันจึงทำให้มันมีลักษณะเด่นของทั้งสองสถาปัตยกรรมดังกล่าวรวมอยู่ด้วยกัน

- มีตำแหน่งศูนย์กลางในการเก็บข้อมูล ,สัญญาณเตือนและ เหตุการณ์ ต่าง ๆ ในเครือข่าย
- สามารถบริหารเครือข่ายได้เต็มรูปแบบจากจุดใด จุดหนึ่งก็ได้
- ไม่ขึ้นอยู่กับระบบเพียงระบบเดียว
- กระจายงานบริหารเครือข่าย
- กระจายการสังเกตการณ์ ไปตลอดเครือข่าย

ในสถาปัตยกรรมแบบนี้จะมีการ รีพลิเคชั่น ฐานข้อมูลด้วยเพื่อให้ทุกแพลตฟอร์มมีข้อมูลที่ถูกต้องและเป็นปัจจุบันอยู่เสมอซึ่งจะถูกบริหารโดยตัว รีพลิเคชั่น ด้าต้าเบส เซิร์ฟเวอร์ (Replicaion Database Server)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.5.3 การบริหารแบบกระจาย (Distributed Management)

โดยทั่ว ๆ ไปการบริหารระบบแบบกระจายจะมีประโยชน์อย่างมากในระบบเครือข่ายแบบกระจาย ซึ่งจะมีการบริหารที่หลายลักษณะ และต่อไปนี้เป็นกิจกรรมที่ต้องอ้างอิงถึงในการบริหารระบบเครือข่ายแบบกระจาย

- เอเจ้นต์หลาย ๆ ตัวจะส่งข้อมูลไปที่ตัวกลางเพียงตัวเดียว แพลตฟอร์มที่ใช้บริหารระบบเครือข่ายเกือบทั้งหมดจะมีสถาปัตยกรรมแบบนี้ เอเจ้นต์และสถานีจะติดต่อสื่อสารกันโดยใช้โปรโตคอลที่เหมาะสมเช่น เอสเอ็นเอ็มพี (SNMP)

- จะมีแพลตฟอร์มที่ใช้บริหารระบบเพียงตัวเดียวที่ทำหน้าที่เป็นตัวไต่ถาม (query) ตัวอื่น ๆ

- แพลตฟอร์ม,เอเจ้นต์หรือตัวประมวลผลของระบบเครือข่ายจะลดจำนวนของข้อมูลดิบ โดยจะทำให้อยู่ในรูปแบบของสถิติออกมาจากแหล่งกำเนิดข้อมูล และจะส่งตรงไปให้สถานี เพื่อเป็นการลดความหนาแน่นของการจราจรในการโอนย้ายข้อมูลเป็นสถิติแทนที่จะเป็นข้อมูลดิบ ๆ ที่มีขนาดใหญ่กว่า

- จะมีแพลตฟอร์มที่ใช้บริหารระบบเพียงตัวเดียวที่จะส่งสัญญาณ (alert) ไปให้กับตัวอื่น ๆ

นี้เป็นรูปแบบที่แตกต่างของระบบการบริหารเครือข่ายแบบกระจาย ซึ่งมีประโยชน์อยู่สามอย่างใหญ่ ๆ คือ อย่างแรก การประมวลผลข้อมูลต่าง ๆ ก็จะถูกแยกกันทำ อย่างที่สองจะเป็นการประหยัดการใช้ทรัพยากรณ์ของระบบเครือข่าย และอย่างสุดท้ายคือจะอนุญาตให้มีการเปลี่ยนแปลงการบริหารของบุคคลแต่ละบุคคลแบบแยกกันได้ง่าย ตัวอย่างเช่น มีคนคนหนึ่งอยู่ในนิวยอร์คกำลังบริหารระบบเครือข่ายอยู่ ขณะเดียวกันนั่นเองก็สามารถมีอีกคนที่อยู่ในรัฐอื่นที่เป็นผู้เชี่ยวชาญกำลังเข้าถึงแพลตฟอร์มเพื่อที่จะระบุปัญหาของระบบ หรือกำลังบริหารระบบเครือข่ายในพื้นที่ของของเขาได้

มันมีความเป็นไปได้ที่จะใช้แพลตฟอร์มในการบริหารระบบจากบริษัทผู้ผลิตมากกว่าหนึ่งบริษัท เช่นแพลตฟอร์มของบริษัทหนึ่งจะพิจารณาถึงภาพรวม ๆ ของระบบเครือข่ายที่มีรายละเอียดของอุปกรณ์ไม่มากนัก ขณะที่แพลตฟอร์มของอีกบริษัทหนึ่งจะพิจารณาในระดับที่ละเอียดกว่า เช่น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตัวบริหารอุปกรณ์ ซึ่งจะจำกัดของเขตอยู่ในจำนวนประเภทของชนิดอุปกรณ์ในแต่ละประเภท เช่นอุปกรณ์ของเน็ทแวร์เป็นต้น จากสิ่งที่ได้กล่าวมานั้นจะยกตัวอย่างบางระบบเช่น ในแลน (LAN) กับเน็ทแวร์ , ซันสปาร์คสเตชั่น (Sun SPARCstation), ซินออพติค ฮับหรือการเชื่อมต่อท้องถิ่น และเราท์เตอร์ ของซิสโค (Cisco) สำหรับการเชื่อมต่อแบบกว้าง ก็สามารถใช้ทั้งเอ็นเอ็มเอส(NMS) และซันเน็ท มาเนเจอร์ (SunNet Manager) โดยที่ เอนเอ็มเอสจะบริหารในสิ่งแวดล้อมของเน็ทแวร์, ซันเน็ทมาเนเจอร์จะบริหารในเครื่องเวิร์คสเตชั่นของซัน ส่วนฮับและเราท์เตอร์จะบริหารโดยเอ็นเอ็มเอส โดยใช้โปรโตคอลเอสเอ็นเอ็มพีที่มีอยู่ในตัวมันเอง และทั้งหมดนี้จะสามารถรายงานผ่านตัวโอเพ็นวิวได้ด้วย

ปัจจุบันได้มีผลิตภัณฑ์ที่เกี่ยวกับการบริหารเครือข่ายคอมพิวเตอร์จำนวนมากในท้องตลาด แต่ว่ามีเพียงไม่กี่ผลิตภัณฑ์เท่านั้นที่เป็นสถานีการบริหารเครือข่าย (management platform) ซึ่งส่วนใหญ่คือเครื่องมืออำนวยความสะดวก (utility) มากกว่าส่วนน้อยคือผู้จัดการของผู้จัดการ (manager of managers)

3.6 เครื่องมืออำนวยความสะดวก (Utility)

ผลิตภัณฑ์ส่วนใหญ่สามารถจัดประเภทเป็นเครื่องมืออำนวยความสะดวกได้ เครื่องมืออำนวยความสะดวกในการบริหารเครือข่ายคอมพิวเตอร์ส่วนใหญ่จะเป็นอะไรที่ง่าย ๆ และราคาไม่แพงไปกว่าแพลตฟอร์มเครือข่าย เครื่องมือเหล่านี้จะช่วยในการจัดหาข้อมูลที่เป็นประโยชน์ในการบริหารระบบ บางทีก็อาจจะเหมือนข้อมูลที่ได้จากแอพพลิเคชั่นที่ทำงานบนแพลตฟอร์มก็ได้ อย่างไรก็ตามเครื่องมืออำนวยความสะดวกไม่ได้ให้รายละเอียดมากนัก และไม่ได้เป็นอิสระจากชนิดของอุปกรณ์ คือในแต่ละตัวอำนวยความสะดวกนั้นมันจะสามารถทำงานได้ตามแต่ผลิตภัณฑ์ที่บริษัทนั้น ๆ ผลิตเท่านั้น

3.7 ผู้จัดการของผู้จัดการ (Managers of Managers)

ชนิดของผลิตภัณฑ์เกี่ยวกับการบริหารเครือข่ายคือผู้จัดการของผู้จัดการ ซึ่งตัวอย่างของผลิตภัณฑ์เหล่านี้คือ ไอบีเอ็มเน็ทวิว (IBM NetView) .เด็คโพลีเซ็นเตอร์เฟรมเวิร์ค (DEC's Polycenter Framework) และเอทีแอนที แอคคิวมาสเตอร์อินทีเกรทเตอร์ (AT&T AccuMaster Integrator) ซึ่งเป็นผลิตภัณฑ์ประเภทผู้จัดการของผู้จัดการที่ได้รับความนิยมอย่างแพร่หลาย

ในที่นี้จะยกตัวอย่างรายละเอียดของเน็ทวิวเท่านั้น เน็ทวิวใช้ปฏิบัติการบนเครื่องระดับเมนเฟรม (mainframe) ซึ่งจะเป็นการรวบรวมการบริหารทั้งหมดมาไว้ที่ส่วนกลางส่วนเดียว และจะ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กำหนดชนิดของสถาปัตยกรรมของเครือข่ายด้วย ตัวอย่างคือเน็ทวิวจะไม่สนับสนุน เอสเอ็นเอ็มพี ซึ่งเป็นโปรโตคอลที่สำคัญอย่างมาก

การทำงานพื้นฐานของเน็ทวิวคือรับรายละเอียดเกี่ยวกับการบริหารจากอุปกรณ์กว้าง ๆ และหลากหลายได้ และจะแสดงรายละเอียดเหล่านั้นในหน้าจอ เน็ทวิวมีความสามารถที่สลับซับซ้อนมาก เช่น การบริหารโดยระบบผู้เชี่ยวชาญเป็นต้น อย่างไรก็ตามเน็ทวิวมีราคาที่แพงมาก และเน็ทวิวได้รวมการบริหารความผิดพลาดของระบบ (fault management) สำหรับอุปกรณ์ต่าง ๆ ด้วย แต่ไม่เพียงเท่านี้ มันยังได้รวมการบริหารในส่วนอื่น ๆ เข้ามาด้วยเช่น คอนฟิกูเรชั่นและการบริหารประสิทธิภาพ (configuration and performance management) บางทีอาจเป็นเพราะเน็ทวิวถูกพัฒนาขึ้นบนเครื่องระดับเมนเฟรม มันจึงไม่เฉพาะเจาะจงมายังระบบแลน (LAN) หรือในยูนิกซ์ (UNIX)

สถานีการบริหารสามารถติดต่อสื่อสารกันได้ระหว่างผู้จัดการของผู้จัดการ เพื่อที่จะหาข้อสรุปของปัญหาที่เกิดขึ้นได้ และในสถานีส่วนใหญ่ได้กำหนดรวบรวมทางเชื่อมต่อกับเน็ทวิวไว้ด้วย

แพลตฟอร์มจะอยู่ระหว่างกลางของเครื่องมืออำนวยความสะดวกและผู้จัดการของผู้จัดการ ตัวอย่างเช่นในเน็ทวิว สามารถรับข้อมูลของผลิตภัณฑ์จากทุก ๆ บริษัทเครือข่ายจากทั้งระบบเลยก็ได้ และ เครื่องมืออำนวยความสะดวกจะรับข้อมูลจากผู้ผลิตผลิตภัณฑ์นั้น ๆ เพียงอย่างเดียวเท่านั้น แต่ว่าแพลตฟอร์ม(เพื่อไม่ให้เกิดความสับสน ต่อไปนี้จะขอเรียกแพลตฟอร์มว่า "แพลตฟอร์ม") จะสามารถรับข้อมูลจากผลิตภัณฑ์ที่จำกัดจำนวนของบริษัทผู้ผลิตเท่านั้น

3.8 การเลือกแพลตฟอร์มในการบริหารระบบเครือข่ายคอมพิวเตอร์

ในการเลือกแพลตฟอร์มในการบริหารระบบเครือข่ายคอมพิวเตอร์ สิ่งสำคัญอันแรกก็คือต้องพิจารณาแพลตฟอร์มที่มีการรวมระบบปฏิบัติการแพลตฟอร์มเข้าไว้ด้วย (platform operating system) และต้องพิจารณาอุปกรณ์ที่จะทำการบริหารด้วย รวมทั้งต้องพิจารณาความต้องการสำหรับการบริหารแบบแยก(การบริหารแบบกระจาย หรือ distributed management) และการเชื่อมต่อของระบบด้วย

3.8.1 ระบบปฏิบัติการแพลตฟอร์ม

แพลตฟอร์มจำนวนมากจะทำงานภายใต้ระบบปฏิบัติการยูนิกซ์,วินโดว์หรือโอเอสทู (OS/2) จากรูปแบบโดยทั่ว ๆ ไปของระบบปฏิบัติการที่แพลตฟอร์มต้องทำงานด้วยแล้วเราสามารถแบ่งสิ่งที่สำคัญ ๆ ที่จะต้องพิจารณาเมื่อเราจะเลือกใช้แพลตฟอร์มในการบริหารระบบคือ อย่างแรกถ้าเป็นไปได้แพลตฟอร์มที่จะใช้บริหารระบบเครือข่ายจะต้องสนับสนุนหรือใช้กับระบบปฏิบัติการที่มีอยู่ หรือกำลังใช้อยู่ปัจจุบัน อย่างที่สองคือระบบเครือข่ายที่ยิ่งใหญ่ ยิ่งซับซ้อนมันก็ยิ่งจะต้องการระบบปฏิบัติการแพลตฟอร์มที่แข็งแรงและมีความเชื่อถือได้มากขึ้นเท่านั้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โชคไม่ดีตรงที่ว่าสองสิ่งที่กล่าวมาข้างต้นนั้นบางครั้งมันก็ขัดแย้งกันเอง ตัวอย่างเช่นถ้าเรามีระบบที่ใหญ่มากซึ่งมีความซับซ้อนมากที่ทำงานโดยใช้วินโดว์ และไม่มียูนิกซ์หรือโอเอสทู อยู่เลยในระบบนั้น อย่างไรก็ตามระบบปฏิบัติการแพลตฟอร์มของทั้งยูนิกซ์และโอเอสทูจะให้ความน่าเชื่อถือและแข็งแรงกว่าระบบปฏิบัติการแพลตฟอร์มวินโดว์สามจุดหนึ่งหรือดอส ในกรณีอย่างนี้ผู้บริหารระบบต้องตัดสินใจเองว่าจะเลือกอะไรโดยพิจารณาระหว่างแพลตฟอร์มในการบริหารที่ดีที่สุด กับระบบปฏิบัติการที่กำลังใช้อยู่

แพลตฟอร์มส่วนมากจะเป็นแพลตฟอร์มที่ทำงานบนระบบปฏิบัติงานยูนิกซ์ หรือบางครั้งก็เป็นระบบปฏิบัติการโอเอสทู แต่ว่าแพลตฟอร์มที่ทำงานบนระบบวินโดว์นั้นจะมีราคาที่ถูกกว่าและเป็นระบบที่ง่ายกว่า โดยตัวของระบบปฏิบัติการวินโดว์เองนั้นมีราคาที่ไม่แพงอยู่แล้วและก็ยังเป็นระบบที่ใกล้ชิดกับผู้ใช้อีกด้วย ผู้ใช้ส่วนใหญ่จะคุ้นเคยกับวินโดว์ดี แต่จากที่ผ่าน ๆ มามันก็ไม่ได้มีประสิทธิภาพดีไปกว่ายูนิกซ์เลย ในกรณีของโอเพ็นวิว (HP OpenView) จะเป็นซอฟท์แวร์ที่ใช้ทำงานบนระบบยูนิกซ์และทำขึ้นอีกเพื่อใช้งานบนวินโดว์ ยูนิกซ์จะเป็นระบบที่ใหญ่กว่า ซับซ้อนกว่าและวินโดว์จะเป็นระบบที่เล็กกว่า เป็นเครือข่ายที่เป็นพื้นฐานกว่า อย่างไรก็ตามในระบบวินโดว์เอ็นที (Windows NT) จะมีแพลตฟอร์มในการบริหารเครือข่ายที่มีประสิทธิภาพสูงและมีความสามารถพอสมควรอยู่

ในบางระบบปฏิบัติการ เช่นระบบโอเอสทู แพลตฟอร์มที่ทำงานบนระบบนี้ก็มีเช่น เน็ท์แวร์ มาเนจเม็นต์ ซิสเต็ม (netware management system : NMS) สำหรับระบบปฏิบัติการโอเอสทูแล้วในทางเทคนิคมันพอที่จะเปรียบเทียบกับระบบปฏิบัติการยูนิกซ์ได้ ในเรื่องของเสถียรภาพ

ซอฟท์แวร์ที่ทำหน้าที่เป็นตัวบริหารระบบก็มีพลังสูง อย่างไรก็ตามผู้พัฒนาแอพพลิเคชั่นที่ใช้บริหารระบบเครือข่ายจะนิยมในการพัฒนาแอพพลิเคชั่นที่ทำงานบนยูนิกซ์มากกว่า เนื่องจากมีทางเลือกมากกว่าและก็มีเครื่องมีที่ช่วยในการพัฒนาอยู่บนระบบยูนิกซ์มากกว่าและก็มีนักเขียนโปรแกรมบนยูนิกซ์มากกว่านั้นเอง

อย่างไรก็ตามไม่ว่าแพลตฟอร์มที่ใช้จะทำงานกับระบบปฏิบัติการแบบไหนมันก็จะไม่มีผลต่อเอเจ้นต์ (agent) เพราะว่าเอเจ้นต์จะสามารถติดต่อกับแพลตฟอร์มได้ตลอดเวลาตราบเท่าที่มันใช้โปรโตคอลที่ถูกต้องอยู่ แอพพลิเคชั่นที่ใช้บริหารระบบอาจจะทำงานภายใต้ระบบวินโดว์หรือยูนิกซ์ แต่ว่า เอเจ้นต์จะทำงานภายใต้ระบบของมันอาจจะเป็นระบบปฏิบัติงานของอุปกรณ์ที่มีเอเจ้นต์เอง หรืออาจจะเป็นดอสเป็นต้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.8.2 อุปกรณ์ที่ต้องการการบริหาร(Managed Devices)

มีอยู่สามวิธีที่จะเปรียบเทียบแพลตฟอร์มบริหารระบบ ที่จะใช้ในการบริหารอุปกรณ์ที่ต้องการการบริหารคือ

1. เลือกแพลตฟอร์มที่มีแอพพลิเคชั่นที่จะบริหารกับอุปกรณ์ที่ต้องการการบริหารอยู่แล้ว
2. ในกรณีที่ระบบเครือข่ายมีความซับซ้อนมาก ๆ ข้อ 1 จะเป็นไปไม่ได้เลย ให้เลือกแพลตฟอร์มที่มีแอพพลิเคชั่นที่จะบริหารกับอุปกรณ์ที่ต้องการการบริหารตรงกับอุปกรณ์ที่มีให้มากที่สุด จากนั้นก็ให้สร้างแอพพลิเคชั่นของตัวเองขึ้นมาใช้สำหรับอุปกรณ์ที่ยังไม่มี ซึ่งในส่วนนี้ ส่วนใหญ่จะเป็นแอพพลิเคชั่นที่ทำงานบนแพลตฟอร์มของเอสเอ็นเอ็มพี
3. บริหารสร้างแอพพลิเคชั่นทั้งหมดของตัวเอง โดยใช้เครื่องอำนวยความสะดวกของเอเอ็นเอ็มพี

สองข้อแรกจะเป็นส่วนที่บริษัทผู้ผลิตจะทำมาเพื่ออุปกรณ์ต่าง ๆ แต่ในข้อที่สามนั้นจะไม่เกี่ยวข้องกับบริษัทที่ผลิตเลย ตัวอย่างเช่นไม่ได้มีการระบุเฉพาะเจาะจงบริษัทที่ผลิตฮับ เพราะว่าต้องการแอพพลิเคชั่นของบริษัทที่ผลิตฮับนั้น ๆ และถ้าใช้มาตรฐานตัวแปรของเอสเอ็นเอ็มพีแล้วมันก็สามารถนำมาใช้ได้เลยกับทุก ๆ ฮับ จากบริษัทอื่น ๆ แบบนี้ต้องใช้ความรู้ในการเขียนโปรแกรมและรายละเอียดของโปรโตคอลรวมทั้งต้องรู้สถาปัตยกรรมของการบริหารด้วย

3.9 ตัวอย่างของแพลตฟอร์ม

3.9.1 ผลิตภัณฑ์ของบริษัทโนเวลล์ : ระบบบริหารเครือข่ายของเน็ทแวร์(The NetWare Management System)

ระบบการบริหารเครือข่ายของเน็ทแวร์(NMS) เป็นแพลตฟอร์มที่ทำงานบนระบบปฏิบัติการวินโดว์ โดยที่ระบบที่ระบุมาคือ แลนของเน็ทแวร์เอง (NetWare LAN) ความสามารถของระบบเอ็นเอ็มเอสก็มี แผนที่แบบแบ่งเป็นระดับชั้นตามรายละเอียด(hierarchical mapping) ,ระบบส่งสัญญาณ (alerts) ,ระบบการติดต่อกับผู้ใช้โดยใช้วิธีแบบรูปภาพ (graphic), และมีมาตรฐานในการเข้าถึงข้อมูลของตัวเอง มาตรฐานที่ว่านี้เป็นมาตรฐานของเน็ทแวร์เอง ซึ่งผลิตภัณฑ์ที่เกี่ยวกับฐานข้อมูลของเน็ทแวร์ จะสามารถเข้าใช้ฐานข้อมูลนี้ได้ ตัวอย่างก็คือ เน็ทแวร์ เอสคิวแอล (NetWare SQL)

คอนโซล (console) ของเอ็นเอ็มเอสจะทำงานบนเครื่องเน็ทแวร์เวิร์คสเตชั่น(NetWare Workstation) และเอเจ้นต์จะทำงานอยู่ในอุปกรณ์ต่าง ๆ ตัวอย่างเช่น เอ็นแอลเอ็ม (NLM:NetWare

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Loadable Module) จะเป็นเอเจ้นต์ของระบบการบริหารโดยใช้เน็ทแวร์ ซึ่งจะทำงานอยู่บนผู้ให้บริการแฟ้มข้อมูล(file server) และระบบเอ็นเอ็มเอสจะสนับสนุนและมีความเข้ากันได้ทุกอย่างกับระบบเอสเอ็นเอ็มพี (SNMP)

3.9.1.1 ส่วนประกอบของระบบเอ็นเอ็มเอส

ระบบเอ็นเอ็มเอสมีองค์ประกอบที่สำคัญ ๆ อยู่ 4 ส่วนคือระบบแผนที่ของการบริหารแบบเน็ทแวร์, ผู้จัดการผู้ให้บริการ, เอเจ้นต์ของการบริหารแบบเน็ทแวร์ และเอเจ้นต์ของระบบเอสเอ็นเอ็มพี

3.9.1.1.1 ระบบแผนที่ของการบริหารแบบเน็ทแวร์(The NetWare Management Map)

เป็นการทำงานที่ทำงานภายใต้สิ่งแวดล้อมของระบบวินโดว์ ซึ่งก็จะมีโครงสร้างพื้นฐานตามระบบเอ็นเอ็มเอส เช่นการปฏิบัติการบริหารสิ่งแวดล้อม มีเครื่องมือที่ช่วยให้มีการบริหารงานที่ส่วนกลาง (centralized management) และก็มีเอพีไอ (API : application program interfaces) ที่ติดมาภายในด้วย เพื่อให้ผลิตภัณฑ์ของโนเวลล์ (Novell) หรือจากบริษัทอื่นสามารถทำงานกับระบบแผนที่แบบนี้ได้ นากจากนี้ก็ยังรวมถึงลักษณะสำคัญ ๆ ต่าง ๆ คือ มีการทำการอัพเดทข้อมูลอัตโนมัติ (autodiscovery) ,การรวมฐานข้อมูลไว้ที่จุดศูนย์กลางการบริหาร ,ระบบส่งสัญญาณจากจุดศูนย์กลางและเครื่องมือในการแสดงข้อมูล

ในการทำงานของระบบแผนที่นั้นได้อนุญาตให้ผู้ใช้ได้รวมแฟ้มข้อมูลที่เป็นรูปภาพหรือรูปแบบกราฟิค (graphic) เข้ากับแผนที่ของเอ็นเอ็มเอสได้อีกด้วย ซึ่งมันจะทำให้ง่ายในการกำหนดตำแหน่งต่าง ๆ และก็ยังสามารถจัดแบ่งหน้าจอ เพื่อให้ผู้ใช้ รวมทั้งผู้บริหารระบบสามารถมองเป็นรายละเอียดของเครือข่ายได้ง่าย และในแผนที่ที่ใหญ่กว่านั้นมันจะแสดงให้รู้ว่าจะทำอย่างไรให้ในแต่ละขนาดของเครือข่ายย่อย ๆ มีขนาดที่พอดีได้

ระบบออโต้ดีสคอฟเวอรี่จะทำงานกับเน็ทเอ็กโพรเรอร์ (NetExplorer) ที่ทำงานอยู่บนผู้ให้บริการแฟ้มข้อมูลของเน็ทแวร์ และผู้บริหารของเน็ทเอ็กโพรเร่อร์จะทำงานอยู่บนสถานีที่เป็นระบบปฏิบัติการวินโดว์ เราสามารถติดตั้งเน็ทเอ็กโพรเรอร์พลัสเอ็นแอลเอ็ม (NetExplorer PLUS NLMs) ในระบบผู้ให้บริการต่าง ๆ เพื่อที่จะทำให้สามารถรู้ข้อมูลรายละเอียดต่าง ๆ ของผู้ให้บริการนั้น ๆ รวมทั้งผู้ใช้ของระบบนั้น ๆ ด้วย เน็ทเอกโพรเรอร์สามารถครอบคลุมเราท์เตอร์, ผู้ให้บริการแฟ้มข้อมูล, เครื่องระดับเวิร์คสเตชั่นที่ใช้ระบบปฏิบัติการโอเอสทูหรือดอส, เราท์เตอร์อื่น ๆ ที่การสนับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สนุนการใช้โปรโตคอลอินเตอร์เน็ทโปรโตคอล (IP) และโปรโตคอลเอสเอ็นเอ็มพี รวมทั้งเครือข่ายที่เป็นอีเทอร์เน็ท (Ethernet) และโทเคนริง (token ring) และก็บริษัทอื่นก็สามารถพัฒนาระบบออโต้ดีสคอฟเวอรี่สำหรับอุปกรณ์ของตนเองขึ้นมาได้

ในการทำงานของระบบออโต้ดีสคอฟเวอรี่ จะเริ่มต้นจากผู้ให้บริการที่มีเน็ทเอกโพรเรอร์เอ็นแอลเอ็มอยู่ข้างใน ต่อไปยังอุปกรณ์ที่ผู้ให้บริการนั้น ๆ รู้จัก และจะต่อไปยังอุปกรณ์ที่อุปกรณ์เหล่านั้นรู้จักอีกที จะต่อไปเรื่อย ๆ จนกระทั้งครอบคลุมทั้งระบบเครือข่าย และเมื่อครอบคลุมหมดแล้ว ผู้บริหารของเน็ทเอกโพรเรอร์ จะแทรกอุปกรณ์อันใหม่ลงในแผนที่ และในฐานข้อมูลด้วย และก็จะปรับปรุงข้อมูลที่เกี่ยวกับอุปกรณ์นั้น ๆ เราสามารถให้เน็ทเอกโพรเรอร์ทำงานอยู่ตลอดเวลาได้ให้ปรับปรุงฐานข้อมูล, แผนที่อย่างต่อเนื่อง

ระบบเอ็นเอ็มเอสในปัจจุบันมีการส่งสัญญาณจากเงื่อนไขเดียวเท่านั้น ตัวอย่างเงื่อนไขที่ซับซ้อนเช่น ถ้า...แล้ว(IF...THEN) มันไม่สามารถทำได้ สัญญาณที่มีก็มีห้าอย่าง สามอย่างจะแสดงบนแผนที่ โดยแสดงเป็นสีเขียว เหลืองและแดง รวมทั้งมีเสียงเตือนต่าง ๆ ด้วย

3.9.1.1.2 ผู้จัดการผู้ให้บริการ(The NetWare Service Manager)

ผู้จัดการการบริการของเน็ทแวร์(NSM) ทำงานภายใต้ระบบปฏิบัติการวินโดว์ เป็นแอพพลิเคชั่นที่ใช้สำหรับดูและจัดการผู้ให้บริการแฟ้มข้อมูลของเน็ทแวร์(NetWare file server) เอ็นเอสเอ็มเป็นการส่งข้อมูลกันจริง ๆ ของผู้ให้บริการแฟ้มข้อมูลที่มีเอเจ้นต์การบริหารของเน็ทแวร์อยู่ ข้อมูลทั้งหมดจะเหมือนกับข้อมูลที่มีไว้สำหรับเครื่องมืออำนวยความสะดวกที่เป็นมาตรฐานของเอ็นเอสเอ็ม เอ็นเอสเอ็มจะมีการแสดงข้อมูลที่เป็นลักษณะรูปภาพหรือที่เรียกว่ กราฟิค เพื่อจะทำให้งานยิ่งขึ้นไปอีก ตัวอย่างเช่น จำนวนหน่วยความจำ (memory) ที่ใช้ไปจะถูกแสดงเป็นแผนภาพกราฟออกมา และ เอ็นเอสเอ็มจะมีข้อมูลเก่าที่ผ่านมาแล้วด้วย ในขณะที่เครื่องมืออำนวยความสะดวกอื่น ๆ ที่เป็นมาตรฐานของเน็ทแวร์ไม่ได้มีไว้

ตัวอย่างเช่นเราสามารถแสดงกราฟเส้นของอัตราการอ่านหรืออัตราการเขียนข้อมูล ตั้งแต่เวลาที่ผ่านมาแล้วจนถึงปัจจุบัน ข้อมูลบางอย่างอาจถูกแสดงเป็นมาตรวัด เป็นอัตราส่วนที่ดูเหมือนเทอร์โมมิเตอร์ ตัวอย่างเช่นจำนวนของแฟ้มข้อมูลที่กำลังเปิดใช้งานอยู่ เป็นต้น

และต่อไปนี้จะเป็นตัวอย่างของข้อมูลที่เอ็นเอสเอ็มสามารถแสดงออกมาได้ เราสามารถตรวจดูดการทำงานของหน่วยประมวลผลกลางได้ว่าเป็นอย่างไร มีเอ็นแอลเอ็มอะไรบ้างที่กำลังทำงานอยู่ และแต่ละเอ็นแอลเอ็มนั้นได้ใช้หน่วยความจำไปเท่าไรแล้ว ขนาดของแพคเก็ต(packet) รวม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ทั้งอัตราการส่งและรับข้อมูลเป็นอย่างไรซึ่งสามารถดูได้หลายโปรโตคอลด้วย สามารถตรวจดูผู้ให้บริการการพิมพ์ด้วยว่ามีผู้ให้บริการไหนที่มีบริการการพิมพ์อยู่ด้วย และมีเครื่องพิมพ์กี่เครื่องที่ติดตั้งอยู่ในระบบ รวมทั้งดูได้ว่ามีงานอะไรบ้างที่กำลังรอที่จะพิมพ์อยู่

3.9.1.1.3 เอเจ้นต์ของการบริหารแบบเน็ทแวร์(The NetWare Management Agent)

อุปกรณ์ของบริษัทโนเวลล์ (Novell) ที่ระบุมาในเอ็นแอลเอ็ม สำหรับบริหารผู้ให้บริการแฟ้มข้อมูลของระบบเครือข่าย เรียกว่าเอเจ้นต์การบริหารของระบบเน็ทแวร์ (NMA : NetWare Management Agent) เอ็นเอ็มเอจะติดต่อสื่อสารกับผู้จัดการผู้ให้บริการของเน็ทแวร์ โดยเอ็นเอ็มเอจะส่งสถิติ เช่นบอกว่ามี่การใช้หน่วยความจำไปเท่าไรแล้ว และพื้นที่ว่างในดิสก์มี่เท่าใด โดยจะส่งไปให้กับผู้จัดการการบริการของเน็ทแวร์(NetWare Service Manager) เพื่อให้นำข้อมูลเหล่านี้ไปวิเคราห์ และจะได้แสดงผลออกมา

เอ็นเอ็มเอสามารถสร้างสัญญาณตามที่ผู้ใช้ได้กำหนดไว้ได้ เอ็นเอ็มเอจะเก็บข้อมูลไว้ในรูปแบบที่เป็นมาตรฐานของเน็ทแวร์ ทำให้แอพพลิเคชั่นอื่น ๆ ที่สนับสนุนรูปแบบมาตรฐานนี้สามารถเข้าถึงข้อมูลได้ด้วย

3.9.1.1.4 เอเจ้นต์ของระบบเอสเอ็นเอ็มพี(The SNMP Agent)

เอเจ้นต์ของเอสเอ็นเอ็มพีของบริษัทโนเวลล์ก็ทำงานอยู่ที่ผู้ให้บริการ(server) เหมือนกับเอ็นแอลเอ็ม โดยมีจุดประสงค์เพื่อให้อุปกรณ์ที่ถูกบริหารโดยระบบเอ็นเอ็มเอสสามารถรายงานไปยังแพลตฟอร์มแบบเอสเอ็นเอ็มพีได้ เช่น เอชพีโอเพ็นวิว(HP OpenView) ,ซันเน็ทมาเนเจอร์(SunNet Manager) ซึ่งจำเป็นอย่างมากที่จะทำให้โปรแกรมเอ็นแอลเอ็มอื่น ๆ สามารถติดต่อสื่อสารกับเอเจ้นต์ของเอสเอ็นเอ็มพีแบบเอ็นแอลเอ็มได้ โนเวลล์ได้ให้เอพีไอและเครื่องมือสำหรับพัฒนามาเพื่อที่จะให้สามารถเขียนเอ็นแอลเอ็มของอุปกรณ์ต่าง ๆ เพื่อให้ติดต่อสื่อสารกับเอเจ้นต์เอสเอ็นเอ็มพีได้

อุปกรณ์ในผู้ให้บริการแฟ้มข้อมูลเช่นแหล่งกำเนิดพลังงาน จะมีเอ็นแอลเอ็มอยู่แล้ว ซึ่งสามารถติดต่อกับเอสเอ็นเอ็มพีได้เลย ส่วนอุปกรณ์ภายนอกผู้ให้บริการแฟ้มข้อมูลอาจจะสามารถติดต่อสื่อสารกับเอเจ้นต์ของเอสเอ็นเอ็มพีอื่น ๆ โดยตรงกับเอเจ้นต์เอสเอ็นเอ็มพีของตัวเอง ซึ่งจะทำให้มีประสิทธิภาพสูง อย่างไรก็ตาม อุปกรณ์ที่อยู่ภายนอกผู้ให้บริการแฟ้มข้อมูล อาจจะได้รับประโยชน์จากการติดต่อสื่อสารของเอเจ้นต์เอสเอ็นเอ็มพีมากกว่า เพราะมันไม่ต้องการปรับปรุงเอสเอ็นเอ็มพีเพิ่มเติม หรือไม่ต้องการโปรโตคอลทีซีพีไอพี(TCP/IP) ตัวอย่างเช่น ตัวดูแลระบบเครือ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ข่ายแลนเทร์น(LANtern) จะติดต่อสื่อสารกับเอเจ้นต์เอสเอ็นเอ็มพี ถึงแม้ว่าตัวมันเองไม่ได้อยู่ในตัวบริการแฟ้มข้อมูล

เอเจ้นต์เอสเอ็นเอ็มพีไม่ต้องมีการออกแบบมาเฉพาะที่จะบริหารอุปกรณ์หรือระบบต่าง ๆ มันจะเป็นการทำงานระหว่างแพลตฟอร์มอื่น ๆ กับผู้ให้บริการแฟ้มข้อมูลของเน็ทแวร์

3.9.2 ผลิตภัณฑ์ของบริษัทฮิวเล็ทแพคคาร์ด : โอเพ็นวิว (OpenView)

มีการแบ่งแยกผลิตภัณฑ์ที่แตกต่างกันภายใต้ชื่อของผลิตภัณฑ์ที่ว่า "โอเพ็นวิว" อย่างแรกเป็นผลิตภัณฑ์ที่ทำงานภายใต้ระบบปฏิบัติการยูนิกซ์บนเครื่องซัน(SUN) หรือเครื่องเวิร์คสเตชั่นของเอชพีเอง(HP workstations) และผลิตภัณฑ์นี้เป็นผลิตภัณฑ์ที่ประประสิทธิภาพสูง ส่วนอีกอย่างที่แบ่งแยกออกมานั้นเป็นผลิตภัณฑ์ที่ทำงานภายใต้สิ่งแวดล้อมของระบบวินโดว์ซึ่งจะมีประสิทธิภาพน้อยลงมา แต่ว่าจะใช้งานง่ายกว่า

3.9.2.1 โอเพ็นวิวสำหรับวินโดว์

บริษัทเอชพีไม่ได้ขายผลิตภัณฑ์โอเพ็นวิวสำหรับวินโดว์ให้กับผู้ใช้ทั่ว ๆ ไป แต่ว่าจะให้สิทธิแก่บริษัทผู้พัฒนาแอพพลิเคชั่นอื่น ๆ ในการนำเทคโนโลยีของผลิตภัณฑ์นี้ไปผลิตเป็นแอพพลิเคชั่นที่ใช้บริหารของตัวเอง

3.9.2.2 โอเพ็นวิวที่เป็นแพลตฟอร์มของการบริหารแบบกระจาย (OpenView Distributed Management Platform)

บริษัทเอชพีได้ขายผลิตภัณฑ์นี้ให้กับองค์กรทั่ว ๆ ไปซึ่งผลิตภัณฑ์นี้ได้รวมถึงโอเพ็นวิวสำหรับเอสเอ็นเอ็มพีด้วย ทั้งบริษัทเอชพีและบริษัทอื่น ๆ ได้ทำการสร้างแอพพลิเคชั่นที่ทำงานบนแพลตฟอร์มนี้ ตัวอย่างก็เช่นเน็ทแวร์โหนดมาเนเจอร์ (NetWare Node Manager) ซึ่งก็คือแอพพลิเคชั่นของเอชพีที่ทำงานกับโปรโตคอลทีซีพีไอพี (TCP/IP)

แพลตฟอร์มที่ใช้เอสเอ็นเอ็มพีของโอเพนวิวเป็นส่วนหนึ่งของแพลตฟอร์มการบริหารแบบกระจายของโอเพนวิว ข้อได้เปรียบของแพ็ทฟอร์มที่ทำการบริหารแบบกระจายก็คือ มันไม่ต้องการฮาร์ดแวร์(hardware) ใด ๆ นอกจากเครื่องยูนิกซ์เวิร์คสเตชั่นเท่านั้น หลาย ๆ บริษัทผู้ผลิตฮาร์ดแวร์ก็ได้เสนอการบริหารแบบกระจายที่ทำงานบนฮาร์ดแวร์ของตนเอง ซึ่งจะเป็นการขึ้นกับฮาร์ดแวร์ คือ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ฮาร์ดแวร์แต่ละตัวต้องมีแพลตฟอร์มของตัวเอง ตัวอย่างเช่น ผู้ให้บริการการบริหารระบบเครือข่ายแบบกระจายของบริษัทเคเบิลตรอน(Cabletron) ก็จะใช้กับฮับของบริษัทเคเบิลตรอน

3.9.3 ซันเน็ทมาเนเจอร์ (SunNet Manager)

ซันเน็ทมาเนเจอร์ เป็นผลิตภัณฑ์ของบริษัทซันคอนเน็ค(SunConnect) ทำงานบนเครื่องซันสปาร์ค(Sun SPARCstations) ภายใต้ซันโอเอส(SunOS) ซึ่งเป็นรุ่นหนึ่งของระบบปฏิบัติการยูนิกซ์ เป็นแพลตฟอร์มสำหรับบริหารเครือข่ายของซันเวิร์คสเตชั่น(Sun workstations) บริษัทซันคอนเน็คเป็นบริษัทลูกของซันไมโครซิสเต็ม(Sun Microsystems) ซึ่งเป็นผู้ผลิตฮาร์ดแวร์ของยูนิกซ์รายใหญ่ของโลก

ซันเน็ทมาเนเจอร์ เป็นการทำงานอย่างง่าย ๆ และราคาไม่แพงนัก สำหรับแพลตฟอร์มการบริหารเครือข่ายระดับสูง ซันเน็ทมาเนเจอร์มีความสามารถพื้นฐานคือ ระบบแผนที่,ระบบส่งสัญญาณ, เครื่องมืออำนวยความสะดวกในรูปแบบกราฟิค(graphic) และมีฐานข้อมูลของตัวเองอีกด้วย

บริษัทซันคอนเน็ค มีความสัมพันธ์กันอย่างใกล้ชิดกับบริษัทผู้ผลิตฮับชื่อซินออพติค(SynOptics) และยังมีความสัมพันธ์กับบริษัทผู้ผลิตเราท์เตอร์ที่ชื่อซิสโค(Cisco) ซันเน็ทมาเนเจอร์จึงมีส่วนแอพพลิเคชั่นที่มีเป้าหมายในการบริหารฮับและเราท์เตอร์จากบริษัทดังกล่าว แต่ว่าก็ยังคงสนับสนุนผลิตภัณฑ์ทางเครือข่ายของผู้ผลิตอื่น ๆ ด้วย เช่นของบริษัทสามคอม เป็นต้น

3.10 โปรโตคอลเอสเอ็นเอ็มพี (SNMP:Simple Network Management Protocol)

3.10.1 Promise ของการบริหารระบบเครือข่าย

ระบบเครือข่ายของธุรกิจในปัจจุบันมีความซับซ้อนเป็นอย่างมาก เติบโตมาจากระบบเครือข่ายแบบโลคอลเล็ก ๆ มาเป็นระบบเครือข่ายแบบร่วมกันทั่วทั้งองค์กร ฮับมีอยู่ประมาณ 75 เปอร์เซ็นต์ของการเดินสายทั้งหมด เราท์เตอร์เชื่อมต่อแลนไปยังสำนักงานที่อยู่ไกล การตรวจตราและซ่อมแซมระบบเหล่านี้เป็นสิ่งที่ท้าทาย

การบริหารระบบเครือข่ายให้ข้อแก้ไขเกี่ยวกับปัญหาเหล่านี้ ระบบเหล่านี้ให้คุณมีการแอ็คทิฟก่อนเพื่อการออกแบบระบบเครือข่าย และการอิมพลิเม็นต์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.10.2 เอสเอ็นเอ็มพี

ีอะไรคือปัญหาของระบบเครือข่าย โครงสร้างการเดินสายผิดหรือเปล่า การควบคุมเป็นอย่างไร ความปลอดภัยเป็นอย่างไร ฮาร์ดแวร์ทำงานถูกฟังก์ชันหรือเปล่า ปัญหาเกี่ยวกับระบบเครือข่ายมีอยู่มากมาย ระบบเครือข่ายที่ทำงานอย่างถูกหลักจะสามารถช่วยแก้ปัญหาเหล่านี้ได้

ต่อไปนี้คือ 6 ฟังก์ชันเพื่อการประเมินค่าระบบการบริหารระบบเครือข่าย

1. ความผิดพลาดของการเดินสาย การบริหารระบบเครือข่ายสามารถช่วยท่านบ่งชี้ถึงความผิดพลาดของการเดินสาย และการพังทลายของระบบสื่อสาร สามารถแยกแยกจุดเสียได้อย่างรวดเร็ว การแก้ปัญหาสะดวกสบาย
2. การควบคุม การบริหารระบบเครือข่ายช่วยให้ท่านควบคุมระบบเครือข่ายจากจุดศูนย์กลาง แทนที่จะกระจายออกไปยังที่ห่างไกล
3. การทำงานผิดพลาดของฮาร์ดแวร์ เมื่อเราท์เตอร์ดาวน์ ระบบก็ดาวน์ตาม การบริหารระบบเครือข่ายให้ท่านสามารถได้ยินเสียงเตือนเมื่อมีการผิดพลาดของฮาร์ดแวร์ภายในระบบเครือข่ายของท่าน
4. ความปลอดภัย บางระบบการบริหารระบบเครือข่ายให้คุณสามารถบ่งชี้พอร์ต ว่าพอร์ตไหนสามารถถูกเข้ามา และ เวิร์คสเตชั่นไหนสามารถเข้าถึงพวกมัน การล็อคประตูเป็นขั้นแรกเพื่อป้องกันผู้บุกรุก
5. การกำหนดแบ่งทรัพยากร การรู้ว่าฮับ, บริดจ์, เราท์เตอร์, เวิร์คสเตชั่น และ เซิร์ฟเวอร์ของคุณอยู่ที่ไหนเป็นสิ่งสำคัญของท่าน การกำหนดทรัพยากรช่วยให้ระบบการบริหารระบบเครือข่ายบรรยายและบำรุงรักษาส่วนต่าง ๆ ของระบบเครือข่าย
6. การแก้ปัญหาให้ผู้ใช้ ระบบการบริหารระบบเครือข่ายให้ความสามารถท่านเห็นระบบทั้งหมด จนถึงการ์ดเน็ตเวิร์คที่เชื่อมต่อกับเวิร์คสเตชั่น ถ้าปัญหาไม่ได้อยู่ในซอฟต์แวร์ท่านจะสามารถเห็นมันได้ในพริบตา

3.10.3 เออร์โกโนมิค (Ergonomics)

ระบบบริหารระบบเครือข่ายที่มีประสิทธิภาพง่ายในการใช้และเชื่อมต่อ กราฟิคบนระบบทำให้คุณสามารถเห็นระบบเครือข่ายของคุณจากจุดมองแบบโกลบอลไปยัง สเตชั่นเดี่ยวขนาดเล็ก

ระบบการบริหารระบบเครือข่ายใช้ประโยชน์จากโปรโตคอลเอสเอ็นเอ็มพี มาตราฐานการบริหารนี้ให้มุมมองหลายอย่างของระบบของคุณ เช่น การมองแบบโกลบอล, การมองแต่ละริงค์หรือแต่ละส่วน และอุปกรณ์ของระบบเครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- การมองแบบโกลบอล เป็นการแทนว่าระบบเครือข่ายมีขอบเขตถึงกันอย่างไร การมองแบบนี้แสดงให้เห็นว่าเราท์เตอร์, ริงค์, เซ็กเมนต์ และ บริดจ์ ถูกเชื่อมต่อกันที่ไหน
- การมองแบบอินเทอร์มีเดียต เป็นการแทนว่าเวิร์คสเตชั่น, คอนเซ็นเตเตอร์, เราท์เตอร์ และบริดจ์ตั้งไว้ที่ไหนบนแต่ละส่วนหรือแต่ละวง
- การมองแบบเน็ตเวิร์คอีลิเม็นท์ การมองแบบนี้จะให้กราฟิคแทนอุปกรณ์ที่จะถูกบริหาร ถ้ามันเป็นระบบที่ดีมันควรจะให้การมองแบบบิตแมบของอุปกรณ์

3.10.4 ความสามารถในการปฏิบัติงานที่หลากหลาย (Interoperability)

ระบบการบริหารระบบเครือข่ายสามารถที่จะทำงานกับโอเปอเรติ้งซิสเต็มส์, เอสเอ็นเอ็มพีเม็นเนเจอร์ และ เวิร์คสเตชั่นแพลตฟอร์ม ที่หลากหลายได้ นี้เป็นเพราะว่าองค์การของคุณอาจจะไม่เหมาะที่จะสนับสนุนบางเวิร์คสเตชั่น หรือ โอเปอเรติ้งซิสเต็มส์ และการเลือกระบบซึ่งให้คุณทำงานที่คุณต้องการทำให้คุณรู้ถึงศักยภาพของท่าน อย่างไรก็ตาม มันเป็นสิ่งสำคัญในการระลึกว่าซอฟต์แวร์ของระบบการบริหารระบบเครือข่ายส่วนมากขึ้นอยู่กับ ยูนิกซ์ โอเปอเรติ้งซิสเต็มส์ ดังนั้นควรเตรียมการเพื่อพัฒนาต่อไปในอนาคต

3.10.5 ทีซีพี/ไอพี(TCP/IP) : มาตราฐานภายใต้การบริหารระบบเครือข่าย

การบริหารระบบเครือข่ายใช้เอสเอ็นเอ็มพีเพื่อควบคุมและตรวจสอบระบบเครือข่าย ที่แตกต่างกัน เอสเอ็นเอ็มพีเป็นทรานสมิชชัน คอนโทรล โปรโตคอล/อินเทอร์เน็ต โปรโตคอล ก่อนที่คุณสามารถเข้าใจพื้นฐานของเอสเอ็นเอ็มพีและการบริหารระบบเครือข่าย เราต้องเข้าใจทีซีพี/ไอพีก่อน,มาตราฐานและโครงสร้างเปรียบเทียบกับเอสเอ็นเอ็มพีโปรโตคอล ทีซีพี/ไอพี โปรโตคอลให้การเชื่อมต่อระหว่างอุปกรณ์จากผู้ขายจำนวนมากบนหลายเทคโนโลยีระบบเครือข่าย มันประกอบด้วยโปรโตคอลการสื่อสารที่รู้จักดี และโปรโตคอลประยุกต์มาตราฐานอีกเป็นจำนวนมาก

3.10.6 เอสเอ็นเอ็มพี: มาตราฐานระบบเครือข่ายในปัจจุบันนี้

โปรโตคอลนี้อยู่บนพื้นฐานซิมเปิลเก็ทเวย์เม็นเน็จเม็นต์โปรโตคอลซึ่งถูกพัฒนาเพื่อการบริหารระบบเครือข่ายเฉพาะพื้นที่

จุดประสงค์การออกแบบของเอสเอ็นเอ็มพี คือ การบริหารระบบเครือข่ายที่รวมกันอยู่ ความสามารถในการบริหารอุปกรณ์ที่รวมกันอยู่ในระบบเครือข่ายซึ่งมาจากหลากหลายบริษัทด้วยแอพพลิเคชั่นเดียว

การทำงานร่วมกัน - ความสามารถที่อุปกรณ์จาก 1 ผู้ขายถูกบริหารโดยอุปกรณ์จากผู้ขายรายอื่น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

มาตราฐาน - มาตราฐานกำหนดวิธีการสื่อสารและโครงสร้างข้อมูลเพื่อว่าระบบเครือข่ายที่แตกต่างกันสามารถทำงานร่วมกันด้วยการบริหารระบบเครือข่าย

3.10.7 เอสเอ็นเอ็มพีทำงานอย่างไร

เอสเอ็นเอ็มพีถูกออกแบบธรรมดาเท่าที่ทำได้ และ ขึ้นอยู่ 2 องค์ประกอบ คือ เน็ตเวิร์ก เม็นเน็จเม็นต์ สเตชั่น (Network Management Station) และ เน็ตเวิร์ค อีลิเม็นท์ (Network Element)

- เน็ตเวิร์คเม็นเน็จเม็นต์สเตชั่น รับผิดชอบการรันแอพพลิเคชั่นการบริหารซึ่งตรวจสอบและควบคุมอุปกรณ์ภายในระบบเครือข่าย
- เน็ตเวิร์คอีลิเม็นต์ ฮับ, เราท์เตอร์ และ บริดจ์มีเอเจ้นต์ซึ่งถูกติดตั้งไว้ภายในอุปกรณ์ เอสเอ็นเอ็มพีเอเจ้นต์เหล่านี้รับผิดชอบเกี่ยวกับการทำหน้าที่ซึ่งถูกร้องขอโดยเครื่องทำหน้าที่บริหารระบบเครือข่าย

เอสเอ็นเอ็มพีเป็นความหมายซึ่งเครื่องที่ทำการบริหารติดต่อสื่อสารกับอุปกรณ์ภายในระบบเครือข่าย มันเป็นโปรโตคอลธรรมดาซึ่งให้ผู้บริหารระบบตรวจสอบหรือเปลี่ยนแปลงค่าต่าง ๆ บนอุปกรณ์ในระบบจากเครื่องทีทำการบริหารระยะไกล

การสื่อสารของเอสเอ็นเอ็มพีขึ้นอยู่กับยูนิเวอร์เซล ดาต้าแกรม โปรโตคอล (UDP) ของ ทีซีพี/ไอพี สแต็คเพื่อส่งข้อมูลข่าวสาร UDP ยอมให้เอเจ้นต์การบริหารเอสเอ็นเอ็มพีถูกแทนที่โดยแพ็กเก็ตเดี่ยว เพราะว่าเหตุนี้, เอสเอ็นเอ็มพีต้องการโอเวอร์เฮด (overhead) เพียงเล็กน้อยและมีการยุ่งเกี่ยวกับฟังก์ชันอื่นของระบบเครือข่ายเพียงเล็กน้อยเท่านั้น

ทุกการตรวจตราเอสเอ็นเอ็มพี ถูกกระทำโดยระบบการบริหารระบบเครือข่าย เครื่องที่ทำการบริหารโพลอุปกรณ์ภายในระบบเครือข่ายเพื่อข้อมูลที่ต้องการหรือเปลี่ยนค่า การโพลและการเปลี่ยนแปลงเหล่านี้ถูกรู้จักว่าเป็น "เก็ท" (get) ค่าที่เปลี่ยนแปลงรู้จักว่าเป็น "เซ็ทส์" (sets) เมื่ออุปกรณ์ในระบบเครือข่ายเริ่มทำการติดต่อ, การสื่อสารรู้จักเป็น "แทร็ป" (trap)

อุปกรณ์ในระบบเครือข่ายใช้ระบบสื่อสารที่เรียกว่า เอสเอ็นเอ็มพี พร็อกซี่ เอเจ้นต์ (SNMP Proxy Agent) ซึ่งเอเจ้นต์เหล่านี้ให้การสื่อสารเฉพาะระหว่างเครื่องที่ทำการบริหารและอุปกรณ์ระบบเครือข่าย พร็อกซี่ เอเจ้นต์ถูกใช้ร่วมกับอุปกรณ์การบริหารอื่น ๆ

3.10.8 เครื่องที่ทำการบริหาร เอสเอ็นเอ็มพี

เครื่องที่ทำการบริหารเอสเอ็นเอ็มพีเป็นการสะสมแอ็พพลิเคชั่นและแหล่งข้อมูลซึ่งควบคุมกลุ่มของเอเจ้นต์ เครื่องที่ทำการบริหารมีอยู่ 5 องค์ประกอบ คือ

1. ส่วนติดต่อกับผู้ใช้ ทำให้ผู้ใช้สามารถเติมคำสั่งการบริหารและรับ โดยขอร้องการตอบสนองเอเจ้นต์หรือไม่ก็ได้ อาจจะเป็นรูปแบบของข้อความหรือกราฟฟิก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2. แอพพลิคชั่นการบริหาร ช่วยในการพิจารณาและดำเนินการของข้อมูลการบริหารระบบเครือข่ายจากการดำเนินการของเอเจ้นต์
3. แหล่งข้อมูล หรือ ค่าที่น่าสนใจ มีชื่อทุกชื่อ, คอนฟิกกูเรชั่น, ประสิทธิภาพ, โทโพโลจี และ รายละเอียดข้อมูลของแลน แหล่งข้อมูลถูกแยกในหลายชนิด ซึ่งรวมทั้งแหล่งข้อมูลการบริหาร(เอ็มไอบี),แหล่งข้อมูลอุปกรณ์เครือข่าย และ แหล่งข้อมูลแอพพลิเคชั่นการบริหาร ชนิดที่สำคัญที่คือ ก็คือ เอ็มไอบี (MIB), แหล่งข้อมูลที่มีคำจำกัดความอุปกรณ์ของทรัพยากรที่ถูกบริหารในสภาพแวดล้อมเอสเอ็นเอ็มพี ในปัจจุบันมีเกือบ 1000 อ็อบเจ็กต์ซึ่งได้ถูกจำกัดความและลงทะเบียนเป็นสมาชิกมาตราฐานของอินเทอร์เน็ตเอ็มไอบี

3.11 บทสรุป

การบริหารระบบเครือข่ายเป็นความต้องการของคนซึ่งต้องการควบคุมและตรวจตราแลนและ แวนของเขา แอพพลิเคชั่นของการบริหารระบบเครือข่ายอยู่บนพื้นฐานของเอสเอ็นเอ็มพี บนมาตราฐานขั้นกับ ทีซีพี/ไอพี โปรโตคอลเพื่อตรวจตราระบบเครือข่ายที่ต่างกัน เอสเอ็นเอ็มพีอยู่ที่ชั้นแอพพลิเคชั่นของโอเอสไอ โมเดล และใช้ ยูดีพี เป็นวิธีการส่งสื่อสารของมันยูดีพีโปรโตคอลให้ความสามารถสื่อสารด้วยวิธีการใช้แบนวิธต่ำ

เพื่อให้ผู้ใช้ได้แอ็คทีฟก่อนในการตรวจตราและอิมพลีเม็นต์ระบบเครือข่าย การบริหารระบบเครือข่ายในปัจจุบันให้ระบบที่ขึ้นกับเอสเอ็นเอ็มพีที่ให้มุมมองที่ต่างกันของระบบเครือข่ายรวมทั้งโกลบอลเพอสเป็คทิฟ, เซ็กเม็นต์เพอสเป็คทิฟ และดีไวซ์ เพอสเป็คทิฟ เพื่อว่าผู้บริหารระบบเครือข่าย

3.11.1 แนวคิดสำหรับ เอสเอ็นเอ็มพี

เอสเอ็นเอ็มพี ใช้กันอย่างกว้างขวาง ในหมู่ผู้ผลิตเครื่องคอมพิวเตอร์ เครื่องเวิร์คสเตชั่น เครื่องโฮสต์ บริดจ์ เราท์เตอร์และฮับล้วนแล้วแต่สนับสนุนเอสเอ็นเอ็มพีทั้งนั้น

3.11.1.1 แนวคิดพื้นฐาน

สถาปัตยกรรมของการบริหารระบบเครือข่าย

รูปแบบของการบริหารระบบเครือข่ายซึ่งใช้ การบริหารระบบเครือข่ายแบบทีซีพี/ไอพี พร้อมด้วยองค์ประกอบดังต่อไปนี้

■ เครื่องทำการบริหาร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- เอเจ้นต์ทำการบริหาร
- แหล่งเก็บข้อมูลการบริหาร
- โปรโตคอลการบริหารระบบเครือข่าย

เครื่องทำการบริหาร

โดยทั่วไปเป็นอุปกรณ์แบบอยู่เพียงเครื่องเดียว แต่มีความสามารถในการทำงานบนระบบที่มีการแบ่งกันใช้ได้ เครื่องทำการบริหารบริการเหมือนเป็นการเชื่อมต่อสำหรับ ผู้บริหารระบบ (คน) ในระบบการบริหารระบบเครือข่าย องค์ประกอบของเครื่องทำการบริหารอย่างน้อยต้องมี

1. ชุดโปรแกรมประยุกต์การบริหาร สำหรับวิเคราะห์ข้อมูล ฟื้นฟู และอื่น ๆ
2. การเชื่อมต่อ ซึ่งผู้บริหารระบบเครือข่ายอาจตรวจสอบและควบคุมระบบเครือข่ายได้
3. ความสามารถในการแปลงความต้องการของผู้บริหารระบบไปเป็น การตรวจตราและการควบคุม อุปกรณ์ระยะไกลในระบบเครือข่าย
4. แหล่งข้อมูลที่ต่างจากแหล่งข้อมูลการบริหาร

ชิ้นส่วนอื่น ๆ ที่พร้อมทำงานในระบบการบริหารระบบเครือข่าย ก็คือ **เอเจ้นต์การบริหาร** จำพวก โฮสต์คอมพิวเตอร์ บริดจ์ เราท์เตอร์ และ ฮับ อาจจะถูกเตรียมพร้อมด้วยเอสเอ็นเอ็มพี ดังนั้นสามารถที่จะทำการบริหาร จากเครื่องทำการบริหารได้ เอเจ้นต์การบริหารตอบสนองข้อเรียกร้องสำหรับข้อมูลและคำร้องจากเครื่องทำการบริหาร และอาจจะให้ข้อมูลที่สำคัญแต่ไม่ร้องขอแก่เครื่องทำการบริหาร

ทรัพยากรในระบบเครือข่ายอาจถูกบริหารโดยแทนที่เป็น ออบเจ็คต์ โดยแต่ละ ออบเจ็คต์คือ ดาต้าวาริเอเบิล ซึ่งแทนลักษณะของเอเจ้นต์การบริหาร ออบเจ็คต์ที่รวมกันอยู่ก็คือ **แหล่งข้อมูลเพื่อการบริหาร** ทำหน้าที่เหมือนเป็นที่รวมจุดผ่านเข้าสู่เอเจ้นต์สำหรับเครื่องทำการบริหาร ซึ่งเครื่องทำการบริหารจะทำการตรวจสอบโดยเอาค่าของออบเจ็คต์แหล่งข้อมูลการบริหาร

เครื่องทำการบริหาร และ เอเจ้นต์เชื่อมถึงกันโดย **โปรโตคอลการบริหารระบบเครือข่าย** ซึ่งเป็นโปรโตคอลที่ใช้สำหรับบริหารระบบเครือข่าย ทีซีพี/ไอพี คือ โปรโตคอลการบริหารระบบเครือข่ายแบบธรรมดา ซึ่งมีองค์ประกอบดังต่อไปนี้

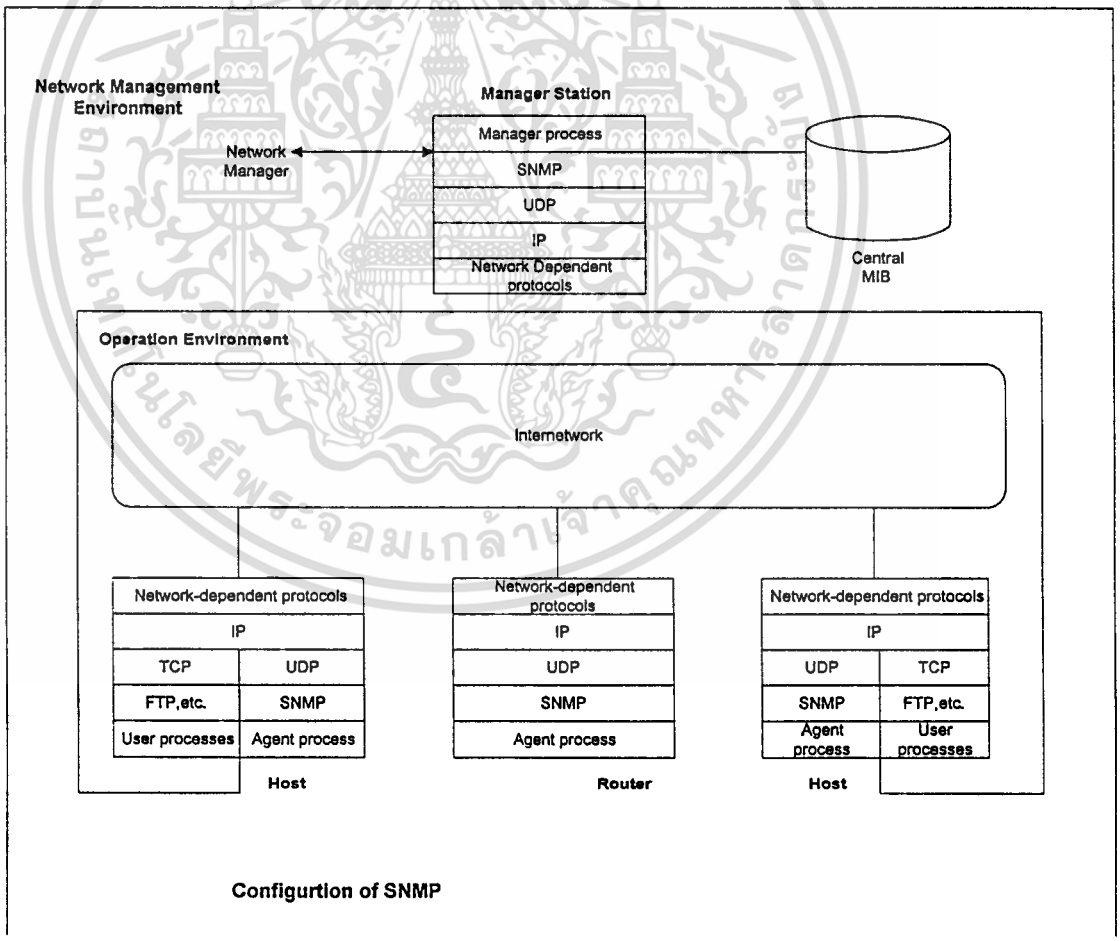
- เก็ท ให้เครื่องทำการบริหารสามารถเอาค่าของออบเจ็คต์ที่ เอเจ้นต์กลับมาได้
- เซ็ท ให้เครื่องทำการบริหารสามารถเซ็ทค่าของออบเจ็คต์ที่เอจ็นได้
- แทร็พ ให้เอเจ้นต์สามารถบอกแก่เครื่องทำการบริหารในเหตุการณ์ที่สำคัญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- ไม่มีการชี้เฉพาะในเรื่องมาตราฐานเพื่อจำนวนของ เครื่องทำการบริหาร หรือ อัตราส่วนของ เครื่องทำการบริหารต่อจำนวนเอเจ้นต์ มันเป็นการรอบคอบที่ให้อย่างน้อย 2 ระบบสามารถทำหน้าที่เป็นเครื่องทำการบริหาร เผื่อไว้ในกรณีที่มีการผิดพลาดเกิดขึ้น

สถาปัตยกรรม โปรโตคอลการบริหารระบบเครือข่าย

เอสเอ็นเอ็มพีถูกออกแบบเพื่อเป็นโปรโตคอลในระดับแอ็พพลิเคชั่น ซึ่งเป็นส่วนของชุดโปรโตคอล ทีซีพี/ไอพี มันถูกกำหนดให้กระทำบน โปรโตคอลยูสเซอร์ดาต้าแกรม รูปที่ 3.6 บอกเกี่ยวกับลักษณะทั่วไปของโปรโตคอลสำหรับ เอสเอ็นเอ็มพี สำหรับเครื่องทำการบริหารแล้ว กระบวนการทำการบริหารคอยควบคุมการเข้าถึงส่วนกลาง แหล่งข้อมูลการบริหาร ที่เครื่องทำการบริหารและให้การเชื่อมต่อไปยัง ผู้บริหารระบบเครือข่าย กระบวนการบริหารทำให้การบริหารระบบเครือข่ายสำเร็จโดยใช้ เอสเอ็นเอ็มพีซึ่งกระทำบนยอดของยูดีพี และ ไอพี

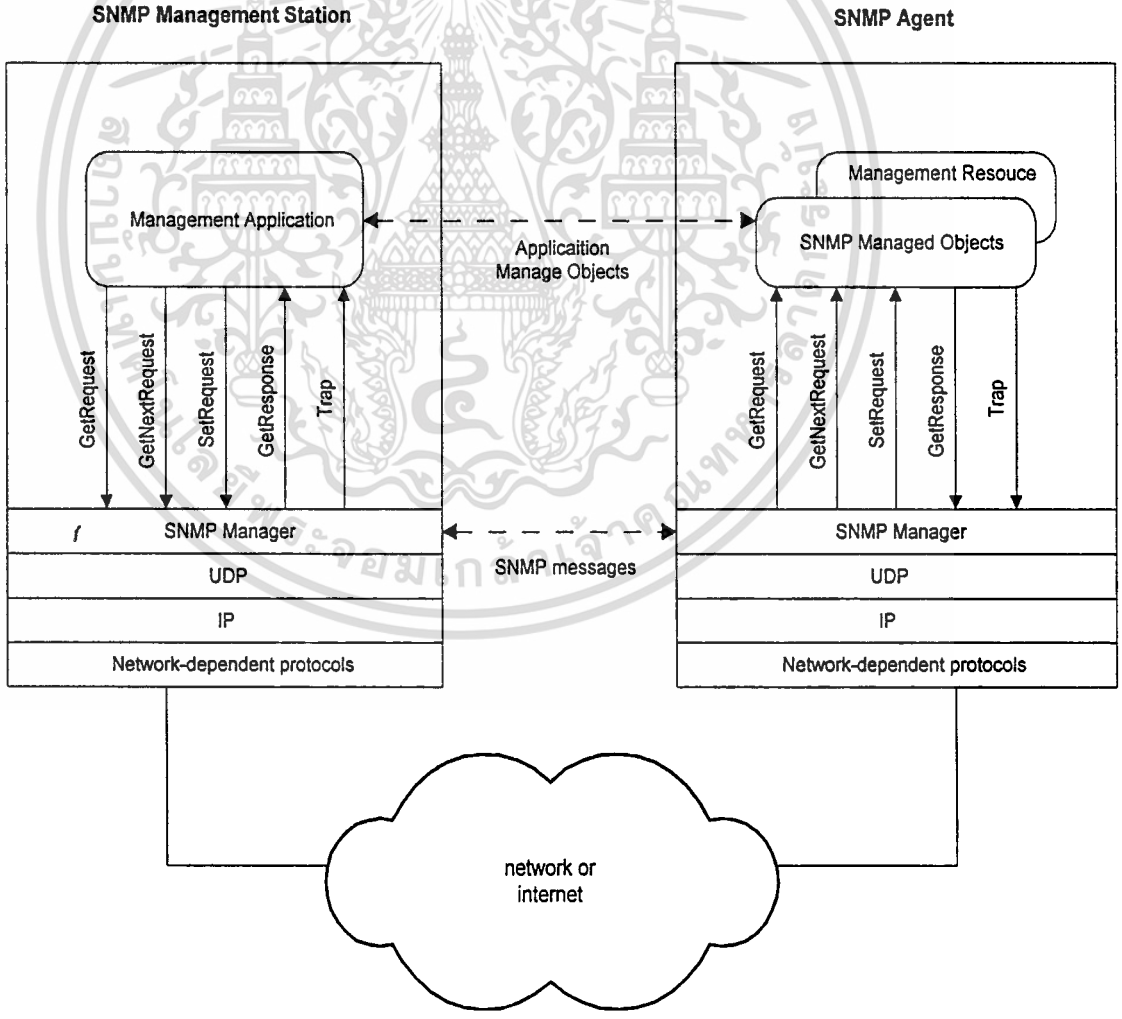


รูปที่ 3.6 ลักษณะทั่วไปของโปรโตคอลสำหรับ เอสเอ็นเอ็มพี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แต่ละเอเจ้นต์ต้องการกระทำ เอสเอ็นเอ็มพี ยูดีพี และ ไอพี ยิ่งกว่านั้น มีกระบวนการเอเจ้นต์ ซึ่งแปลข่าวสาร เอสเอ็นเอ็มพี และ ควบคุมแหล่งข้อมูลการบริหารของเอเจ้นต์ ทีซีพี และ ยูดีพีเป็นที่ต้องการ สำหรับอุปกรณ์เอเจ้นต์ ซึ่งสนับสนุนแอพพลิเคชั่นอื่น เช่น เอฟทีพี

สำหรับรูป 3.11 ให้การมองที่ค่อนข้างใกล้ชิดของโปรโตคอลคอนเท็คของเอสเอ็นเอ็มพี จากเครื่องทำการบริหาร มีอยู่ 3 ชนิดของ ข่าวสารเอสเอ็นเอ็มพีถูกส่งออกมาเพื่อแอพพลิเคชั่นการบริหาร คือ เก็ทรีเควสท์(GetRequest), เก็ทเน็ครีเควสท์(GetNextRequest) และ เซ็ทรีเควสท์ (SetRequest) ข่าวสารทั้ง 3 ตอบรับโดยเอเจ้นต์ในรูปของข่าวสารเก็ทเรสปอนส์ (GetResponse) ซึ่งส่งต่อไปยัง แอพพลิเคชั่นการบริหาร ยิ่งกว่านั้นเอเจ้นต์อาจส่งข่าวสารแทร็พ เพื่อตอบสนองเหตุการณ์ซึ่งมีผลต่อแหล่งข้อมูลการบริหารและทรัพยากรการบริหารที่สนใจ



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 3.7 โปรโตคอลคอนเท็คของเอสเอ็นเอ็มพี

แทร็พไดเร็คโพลดิ้ง (TrapDirectPollings)

ถ้าเครื่องทำการบริหารรับผิดชอบเอเจ้นต์จำนวนมากและแต่ละเอเจ้นต์มีออบเจ็คต์จำนวนมาก มันเป็นไปไม่ได้ในทางปฏิบัติที่ เครื่องทำการบริหารจะทำการโพลไปยัง เอเจ้นต์ ทุก ๆ ข้อมูลออบเจ็คต์ เอสเอ็นเอ็มพี และ แหล่งข้อมูลการบริหารถูกออกแบบมาเพื่อทำให้ผู้บริหารสามารถใช้เทคนิคที่เรียกว่า แทร็พไดเร็คโพลดิ้ง

ซึ่งวิธีที่แนะนำก็คือ ในช่วงเวลาปกติเริ่มต้น เครื่องทำการบริหาร ทำการโพลทุกเอเจ้นต์เพื่อรับข้อมูลเหตุการณ์ เมื่อเสร็จแล้วเครื่องทำการบริหารเลิกทำการโพล โดยแต่ละเอเจ้นต์จะทำการบอกเครื่องทำการบริหารเกี่ยวกับเหตุกรณ์ไม่ปกติแทน เช่น การชนกันของเอเจ้นต์และการถูกรีบูท การเสียของลิงค์ หรือ เกิดโอเวอร์เฮด เหตุการณ์เหล่านี้ถูกสื่อสารในข่าวสารเอสเอ็นเอ็มพีรู้จักกันในชื่อการ แทร็พ

มีผลในการเก็บรักษาของความจุของระบบเครือข่าย และ การดำเนินงานของเอเจ้นต์ ระบบเครือข่าย ไม่ถูกทำเพื่อขนส่งข้อมูลการบริหาร ซึ่งเครื่องทำการบริหารไม่ต้องการและเอเจ้นต์ไม่ถูกทำเพื่อตอบสนองการร้องขอสำหรับข้อมูลข่าวสารที่ไม่สำคัญ และไม่น่าสนใจ

พร็อกซี (Proxy)

การใช้เอสเอ็นเอ็มพีต้องการให้ทุก ๆ เอเจ้นต์สนับสนุน ยูดีพีและไอพี ยิ่งกว่านั้น,อาจจะมีระบบเล็ก ๆจำนวนมากซึ่งกระทำ ทีซีพี/ไอพีเพื่อสนับสนุนแอพพลิเคชั่นของระบบ แต่สำหรับระบบเหล่านั้นไม่ต้องการเพิ่มภาระของเอสเอ็นเอ็มพี เอเจ้นต์ลอจิค และการบำรุงรักษาแหล่งข้อมูลเพื่อการบริหาร

เพื่อทำให้อุปกรณ์ซึ่งไม่เอสเอ็นเอ็มพีมีความเหมาะสมแนวคิดของพร็อกซี่ถูกพัฒนาขึ้น พร็อกซี่ คือ เอเจ้นต์เอสเอ็นเอ็มพีซึ่งรักษาข้อมูลเพื่ออุปกรณ์ซึ่งไม่ใช่อุปกรณ์ เอสเอ็นเอ็มพี

การสื่อสารและชื่อคอมมิวนิตี้

ระบบเครือข่ายเอสเอ็นเอ็มพีมีอยู่หลายลักษณะ ซึ่งไม่เหมือนกับธรรมดาของแอพพลิชั่นที่มีการกระจาย เราจำเป็นต้องเห็นการบริหารระบบเครือข่ายเอสเอ็นเอ็มพีเป็นความสัมพันธ์แบบวันทูเมนนี่ ระหว่าง เอเจ้นต์และชุดของเครื่องทำการบริหาร แต่ละเอเจ้นต์ควบคุมแหล่งข้อมูลการบริหารของมัน และต้องสามารถควบคุมการใช้แหล่งข้อมูลการบริหารโดยเครื่องทำการบริหารจำนวนหนึ่ง การควบคุมนี้มีอยู่ 3 ลักษณะ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1. บริการแบบออเท็นทิเคชั่น เอเจ้นต์ต้องการจำกัดการเข้าถึงแหล่งข้อมูลการบริหาร เพื่อตรวจสอบเครื่องทำการบริหาร
2. นโยบายการเข้าถึงเอเจ้นต์ต้องการให้สิทธิการเข้าถึงที่แตกต่างกันแก่เครื่องทำการบริหารที่ต่างกัน
3. บริการพร็อกซี่เอเจ้นต์ทำตัวเป็นเหมือนพร็อกซี่เพื่อเครื่องทำการบริหารอื่นทุกอันเกี่ยวกับความปลอดภัยเอสเอ็นเอ็มพีใช้แต่วิธีเบื้องต้นและความสามารถจำกัดสำหรับความปลอดภัยโดยชื่อ แนวคิดของคอมมิวนิตี้

เอสเอ็นเอ็มพีคอมมิวนิตี้เป็นความสัมพันธ์ระหว่างเอสเอ็นเอ็มพีเอเจ้นต์และขุดของเอสเอ็นเอ็มพีผู้บริหาร ซึ่งกำหนดตามข้อ 1-3 แต่ละคอมมิวนิตี้ถูกให้ชื่อคอมมิวนิตี้ ซึ่งเป็นเอกลักษณ์ และเครื่องทำการบริหารภายใต้คอมมิวนิตี้ถูกให้ชื่อคอมมิวนิตี้ ในทุก ๆ การเก็ท และ เซ็ท

เนื่องจาก คอมมิวนิตี้ ถูกกำหนดความหมายแบบโลคอลที่เอเจ้นต์ ชื่อเดียวกันอาจจะถูกใช้โดย เอเจ้นต์ที่ต่างกัน ดังนั้นเครื่องทำการบริหารต้องเก็บชื่อคอมมิวนิตี้ที่เกี่ยวกับแต่ละเอเจ้นต์ ที่มันต้องการที่จะเข้าถึง

3.11.2 โปรโตคอลสเปคซิฟิเคชั่น (Protocol Specification)

รูปแบบของเอสเอ็นเอ็มพี

การใช้เอสเอ็นเอ็มพี ข้อมูลถูกแลกเปลี่ยนระหว่างเครื่องทำการบริหาร และ เอเจ้นต์ให้รูปของข้อมูล เอสเอ็นเอ็มพี แต่ละข่าวสารมีเลขเวอร์ชัน บอกเวอร์ชันของเอสเอ็นเอ็มพี ชื่อคอมมิวนิตี้ที่ใช้สำหรับการแลกเปลี่ยนนี้ ดังรูปที่ 3.8 และ จดบันทึกว่า เก็ทรีเควสท์, เก็ทเน็ครีเควสท์ และ เซ็ทรีเควสท์ พีดียู มีรูปแบบเหมือนกับ เก็ทเรสปอนส์พีดียู พร้อมด้วยสถานะการผิดพลาด และ ฟิลด์บ่งชี้ความผิดพลาดมักมีค่าเป็น 0

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

version	community	SNMP PDU

(a) SNMP message

PDU type	request-id	0	0	variable-bindiings

(b) GetRequest PDU, GetNextRequest PDU, and SetRequest PDU

PDU type	request-id	error-status	error-index	variable-bindings

(c) GetResponse PDU

PDU type	enterprise	agent-addr	generic-trap	specific-trap	time-stamp	variable-bindings

(d) Trap PDU

name1	value1	name2	value2	. . .	name n	value n

(e) variable-bindings

SNMP Formats

รูปที่ 3.8 รูปแบบของข้อมูลของเอสเอ็นเอ็มพี

การส่งผ่านของข่าวสารเอสเอ็นเอ็มพี

โดยหลักแล้ว เอสเอ็นเอ็มพีเอ็นติตี้ ทำขั้นตอนต่อไปนี้เพื่อส่ง 1ใน 5 ชนิดพีดียูไปยัง เอสเอ็นเอ็มพี เอ็นติตี้อื่น ๆ

1. พีดียู ถูกสร้าง โดยใช้ โครงสร้าง เอเอสเอ็น 1 ซึ่งกำหนดไว้ใน อาร์เอฟซี 1157
2. พีดียูถูกผ่านไปยังบริการตรวจสอบความถูกต้อง พร้อมด้วยต้นทางและปลายทางการขนส่ง และชื่อคอมมิวนิตี้
3. โปรโตคอลเอ็นติตี้ สร้างข่าวสาร มีเวอร์ชันฟิลด์, ชื่อคอมมิวนิตี้ และผลลัพธ์จากขั้นตอนที่ 2
4. เอเอสเอ็น 1 (ASN.1) ออบเจ็คต์ใหม่นี้ถูกเข้ารหัส และส่งไปยังบริการขนส่งสื่อสาร

การรับของข่าวสารเอสเอ็นเอ็มพี

เอสเอ็นเอ็มพีทำขั้นตอนต่อไปนี้เพื่อรับ ข่าวสารเอสเอ็นเอ็มพี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1. มันทำการเช็คความสัมพันธ์ของข่าวสาร และไม่เอาข่าวสารถ้ามันพาร์สไม่สำเร็จ
2. มันเช็คเลขเวอร์ชันและไม่เอาข่าวสาร ถ้าไม่เข้าคู่กัน
3. โปรโตคอลเอ็นติตี้ส่งชื่อผู้ใช้ ส่วนพีดียูของข่าวสาร และ ต้นทางปลายทางการขนส่งไปยังบริการตรวจสอบความถูกต้อง
4. โปรโตคอลเอ็นติตี้ทำการเช็คความสัมพันธ์ของพีดียู และไม่เอาพีดียูถ้ามันไม่สำเร็จ และถ้ามันสำเร็จ ใช้คอมมิวนิตี้ที่มีชื่อ นโยบายการเข้าถึงเอสเอ็นเอ็มพี ถูกเลือกและพีดียูถูกกระทำต่อไป

เก็ทรีเควสท์พีดียู (GetRequestPDUs)

ถูกส่งโดยเอสเอ็นเอ็มพีเอ็นติตี้เพื่อการส่งเอ็นติตี้ของแอพพลิเคชั่นเครื่องทำการบริหารระบบเครือข่าย มีฟิลด์ดังต่อไปนี้ในพีดียู

- ชนิด พีดียู บอกว่านี้คือ เก็ทรีเควสท์พีดียู
- เลขการร้องขอ entity การส่งให้เลขซึ่งแต่ละการร้องขอที่สำคัญ ไปยังเอเจ้นต์ที่เหมือนกันเป็นเอกลักษณ์ที่บ่งบอกได้
- วาริเอเบิล ไบน์ดิ้ง รายการของออบเจ็คต์อินสแตนซ์ซึ่งค่าของมันเป็นที่ต้องการ

เอสเอ็นเอ็มพีเอ็นติตี้ที่ได้รับ ตอบสนอง เก็ทรีเควสท์พีดียูด้วย เก็ทเรสปอนด์พีดียู ที่มีค่าเลขการร้องขอเหมือนกัน

เก็ทเน็ครีเควสท์พีดียู (GetNextRequestPDUs)

เก็ทเน็ครีเควสท์พีดียู เหมือน เก็ทรีเควสท์พีดียู มันมีรูปแบบการแลกเปลี่ยนพีดียูเหมือนกัน และ แบบฟอร์มเหมือนกันกับ เก็ทรีเคสท์พีดียู เก็ทเน็ครีเควสท์พีดียู เหมือน เก็ทรีเควสท์พีดียู ทุกค่าการร้องขอจะถูกคืนกลับทั้งหมด หรือไม่คืนทั้งหมด

เนื่องจากเอเจ้นต์สามารถคืนกลับเพียงค่าของออบเจ็คต์อินสแตนซ์ธรรมดา คำว่าเน็คใน เก็ทเน็ครีเควสท์พีดียู หมายถึง ออบเจ็คต์อินสแตนซ์อันต่อไปในลำดับเล็กซิโคกราฟฟิก

เซ็ทรีเควสท์พีดียู (SetRequestPDUs)

เซ็ทรีเควสท์พีดียู ถูกส่งโดยเอสเอ็นเอ็มพีเอ็นติตี้ เพื่อแอพพลิเคชั่นเครื่องทำการบริหารระบบเครือข่าย มันมีรูปแบบการแลกเปลี่ยนเหมือน พีดียู และแบบฟอร์มเดียวกับเก็ทรีเควสท์พีดียู ความแตกต่างก็คือ เซ็ทรีเควสท์ใช้เขียนค่าออบเจ็คต์ มากกว่าใช้อ่าน ดังนั้นรายการวาริเอเบิลไบน์ดิ้งในเซ็ทรีเควสท์พีดียูมีทั้งตัวบอกออบเจ็คต์อินสแตนซ์ และ ค่าที่ถูกให้แก่แต่ละรายการออบเจ็คต์อินสแตนซ์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แทร็พพีดียู (TrapPDUs)

แทร็พพีดียูถูกส่งโดย เอสเอ็นเอ็มพีเอ็นติตี้เพื่อแอพพลิเคชั่นเอเจ้นต์การบริหารระบบเครือข่าย มันใช้เพื่อให้การบอกกล่าวเหตุการณ์สำคัญ แก่ เครื่องทำการบริหาร รูปแบบของมันต่างจากเอสเอ็นเอ็มพีพีดียูอื่น ๆ มีฟิลด์ดังต่อไปนี้

- Type PDU บอกว่านี้คือ แทร็พพีดียู
- Enterprise บอกว่าระบบย่อยการบริหารระบบเครือข่ายใดทำให้เกิดแทร็พ
- Agent address ไอพีแอดเดรสของออบเจ็คต์ที่ทำให้เกิดแทร็พ
- Generic Type พรีดีไฟน์แทร็พชนิดหนึ่ง
- Specific Trap โค็ดที่บอกธรรมชาติเฉพาะของแทร็พ
- Timestamp เวลาระหว่างการเริ่มครั้งล่าสุดของ เอ็นติตี้ระบบเครือข่าย ที่ส่งแทร็พและการทำให้เกิดแทร็พ
- Variable-bindings ข้อมูลเพิ่มเติมที่เกี่ยวกับแทร็พ

ไม่เหมือนกับ เก็ทรีเควสท์, เก็ทเน็ครีเควสท์, เซ็ทรีเควสท์พีดียู แทร็พพีดียูไม่ล้วงเอาความจริงจากฝ่ายอื่น ๆ

สนับสนุนระดับการขนส่ง

เอสเอ็นเอ็มพีต้องการใช้บริการขนส่งสำหรับส่งข่าวสารเอ็สเอ็นเอ็มพี โปรโตคอลไม่มีความคิดเกี่ยวกับว่าบริการเชื่อถือได้หรือไม่ คอนเน็คชั่นเลส หรือ คอนเน็คชั่นโอเรียลเต็ท

1. บริการขนส่งแบบคอนเน็คชั่นเลส (connectionless)
2. การกระทำส่วนมากของเอสเอ็นเอ็มพีภายใต้สถาปัตยกรรมทีซีพี/ไอพีและใช้ยูเซอร์ด้าแกรมโปรโตคอลซึ่งเป็นโปรโตคอลแบบคอนเน็คชั่นเลสมันเป็นไปได้ที่จะสนับสนุนเอสเอ็นเอ็มพีด้วยโอเอสไอสถาปัตยกรรมโดยใช้ บริการขนส่งแบบคอนเน็คชั่นเลส
3. บริการขนส่งแบบคอนเน็คชั่นโอเรียลเต็ท

ถ้าเอสเอ็นเอ็มพีขึ้นกับการใช้การเชื่อมต่อการขนส่งแล้วข้อเสียของการเชื่อมต่อ ทำให้เสียประสิทธิภาพของการแลกเปลี่ยนเอสเอ็นเอ็มพี

อาร์เอฟซี 1823 กำหนดแบบแผนสำหรับการใช้เอสเอ็นเอ็มพีบน บริการขนส่งแบบคอนเน็คชั่นโอเรียลเต็ทไอเอ็สโอ เพื่อส่งเก็ทรีเควสท์ เก็ทเน็ครีเควสท์ หรือ เซ็ทรีเควสท์พีดียู, เครื่องทำการบริหารต้องจัดตั้งการเชื่อมต่อการขนส่งไปยังเอเจ้นต์ก่อน และเอเจ้นต์ต้องจัดตั้งการเชื่อมต่อการขนส่งไปยังเครื่องทำการบริหารก่อนที่จะส่งแทร็พเหมือนกัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.11.3 การเลือกเครื่องทำการบริหารเครือข่าย

เครื่องทำการบริหารระบบเครือข่ายประกอบด้วยยูสเซอร์อินเตอร์เฟซไปยัง ระบบการบริหารระบบเครือข่าทั้งหมดและให้พลังความยืดหยุ่น ง่ายต่อการใช้ การเข้าถึง สำหรับการบริหารระบบเครือข่าย รายการดังต่อไปนี้อยู่ในเครื่องทำการบริหารระบบเครือข่าย

- สนับสนุนการขยายแหล่งข้อมูลการบริหารเครื่องทำการบริหารระบบเครือข่ายควรสามารถนำคำจัดความแหล่งข้อมูลการบริหารสำหรับการขยายแหล่งข้อมูลการบริหารซึ่งถูกให้ความหมายสำหรับผลิตภัณฑ์เอเจ้นต์จากผู้ขายคนอื่น
- การเชื่อมต่อโดยสัญชาติญาณการเชื่อมต่อควรทำให้การบริหารระบบเครือข่าย ง่ายและมีพลังมากเท่าที่เป็นไปได้สำหรับผู้ใช้
- การค้นพบโดยอัตโนมัติเมื่อทำการติดตั้งครื่องทำการบริหารระบบเครือข่ายควรสามารถค้นพ้นเอเจ้นต์เพื่อสร้างแผนที่และไอคอนการจัดตั้งระบบ
- เหตุการณ์ที่ทำการโปรแกรมได้ผู้ใช้สามารถกำหนดการกระทำเมื่อมีเหตุการณ์บางอย่างเกิดขึ้น เช่น เมื่อเราท์เตอร์เสีย ให้เปลี่ยนสีของไอคอนเราท์เตอร์ หรือส่งไปรษณีย์อิเลคทรอนิคส์ให้คนรับผิดชอบ หรือส่งเสียงเตือน
- พัฒนาการควบคุมระบบเครือข่าย ตัวอย่งผู้บริหารระบบควรสามารถตั้งค่าเริ่มต้นเครื่องทำการบริหาร ให้ปิดฮับโดยอัตโนมัติ หรือ ปิดส่วนระบบเครือข่ายที่ไม่ดี เพื่อไม่ให้ระบบเครือข่ายทั้งหมดได้ความกระทบกระเทือน
- การบริหารออบเจ็คต์โอเรียลเต็ท ระบบออบเจ็คต์โอเรียลเต็ท สามารถถูกทำขึ้นเพื่อสนับสนุนเอสเอ็นเอ็มพี และสามารถปรับปรุงได้ง่ายเพื่อรันโปรโตคอลการบริหารที่หลากหลาย
- ไอคอนคอสตอม เครื่องทำการบริหารระบบเครือข่ายควรให้ผู้ใช้ สามารถสร้างไอคอนของผู้ใช้เอง

ความถี่ในการโพล

แทร็พซึ่งถูกกำหนดโดยเอสเอ็นเอ็มพีมีจำนวนน้อย ดังนั้นทุกข้อมูลที่ได้รับโดยเครื่องทำการบริหารส่วนใหญ่ได้จากการโพล ยิ่งกว่านั้น, ถ้าทำการโพลแค่ตอนเริ่มต้นและรอการแทร็พเครื่องทำการบริหารอาจไม่ทันต่อเหตุการณ์ในระบบเครือข่าย เช่น เครื่องทำการบริหารจะไม่ถูกเตือนเพื่อแก้ปัญหาในระบบเครือข่าย

เราจะกำหนดความถี่ในการโพล โดยดูจากขนาดระบบเครือข่าย และ จำนวนของเอเจ้นต์ซึ่งถูกบริหารโดยเครื่องทำการบริหาร มีสูตรในการคำนวณที่พอเป็นไปได้ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

$$N <= T/\Delta$$

ซึ่ง N = จำนวนเอเจ้นต์

T = ช่วงเวลาโพลที่ต้องการ

Δ = เวลาเฉลี่ยที่ทำการโพลแต่ละครั้ง

ปริมาณ Δ ขึ้นอยู่กับจำนวนของสาเหตุต่อไปนี้

- เวลากำเนิดการร้องขอที่เครื่องทำการบริหาร
- ความชักช้าจากผู้บริหารไปยังเอเจ้นต์
- เวลาทำการแปลงข้อมูลที่เอเจ้นต์
- เวลาทำการกำเนิดการตอบสนองที่เอเจ้นต์
- ความชักช้าจากเอเจ้นต์ไปยังผู้บริหาร
- เวลาทำการรับและแปลงการตอบสนองของผู้บริหาร
- จำนวนการเปลี่ยน รีเควสท์/เรสปอนด์ เพื่อได้รับทุกข้อมูลที่ต้องการจากเอเจ้นต์

3.11.4 ข้อจำกัดของเอสเอ็นเอ็มพี

1. เอสเอ็นเอ็มพีอาจไม่เหมาะกับระบบเครือข่ายขนาดใหญ่ เพราะการจำกัดประสิทธิภาพของการโพล
2. เอสเอ็นเอ็มพีไม่เหมาะสำหรับการเก็บข้อมูลขนาดใหญ่ เช่น ตารางเราท์ติ้งหมด
3. เอสเอ็นเอ็มพีแทร็พไม่เป็นที่ยอมรับรู้จัก ในกรณีที่ ยูดีพี/ไอพี ใช้ส่งข่าวสารแทร็พ เอเจ้นต์ไม่สามารถทำให้แน่ใจว่าข้อมูลสำคัญจะถึงเครื่องทำการบริหารระบบหรือไม่
4. เอสเอ็นเอ็มพีเหมาะกับการตรวจสอบมากกว่าทำการควบคุม
5. เอสเอ็นเอ็มพีไม่สนับสนุนคำสั่งเชิงบังคับโดยตรง ทำได้โดยเซ็ทค่าออบเจ็คต์ (ไม่โดยตรง) ยืดหยุ่นน้อย และ พลังน้อย
6. รูปแบบแหล่งข้อมูลการบริหารเอสเอ็นเอ็มพี ถูกจำกัดไม่สนับสนุนแอพพลิเคชั่นซึ่งทำการจัดเรียงการบริหารที่ทันสมัยขึ้นกับค่าของออบเจ็คต์หรือชนิดของออบเจ็คต์
7. เอสเอ็นเอ็มพีไม่สนับสุนนการสื่อสารระหว่างผู้จัดการกับผู้จัดการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.11.5 เอสเอ็นเอ็มพี เอ็มไอบี (SNMP MIB)

ทั้งสภาพแวดล้อมทีซีพี/ไอพีและโอเอสไอ, ดาต้าเบสหมายถึง แหล่งข้อมูลการบริหาร แต่ละทรัพยากรถูกบริหารโดยแทนด้วยออบเจ็คต์เอ็มไอบี ก็คือโครงสร้างที่รวมค่าต่าง ๆ ของออบเจ็คต์แต่ละโหนดในระบบจะรักษาเอ็มไอบี ซึ่งบอกสถานะของทรัพยากรการบริหารที่โหนดนั้น เอ็นติตี้การบริหารระบบเครือข่าย สามารถตรวจสอบทรัพยากรที่โหนดนั้นโดยอ่านค่าของออบเจ็คต์ในเอ็มไอบี และอาจจะควบคุมทรัพยากรที่โหนดนั้นโดยเปลี่ยนค่าเหล่านั้น

3.11.5.1 โครงสร้างของข้อมูลการบริหาร

โครงสร้างของเอ็มไอบี กำหนดเฟรมเวิร์คทั่วไปภายในซึ่งเอ็มไอบี สามารถถูกกำหนดและสร้าง เอสเอ็มไอบ่งชี้ชนิดข้อมูลซึ่งสามารถใช้ในเอ็มไอบี และทรัพยากรภายในเอ็มไอบี จะถูกแทนและตั้งชื่ออย่างไร เอ็มไอบีสามารถเก็บเพียงชนิดข้อมูลแบบธรรมดาสเกลาร์ และอะเรย์ 2 มิติของสเกลาร์ วิทยาการดังกล่าวเห็นได้ชัดในการใช้กับการบริหารแบบโอเอสไอ ซึ่งจัดทำสำหรับ โครงสร้างข้อมูลที่ซับซ้อน และกู้กลับเพื่อสนับสนุนการทำงานที่ใหญ่กว่า

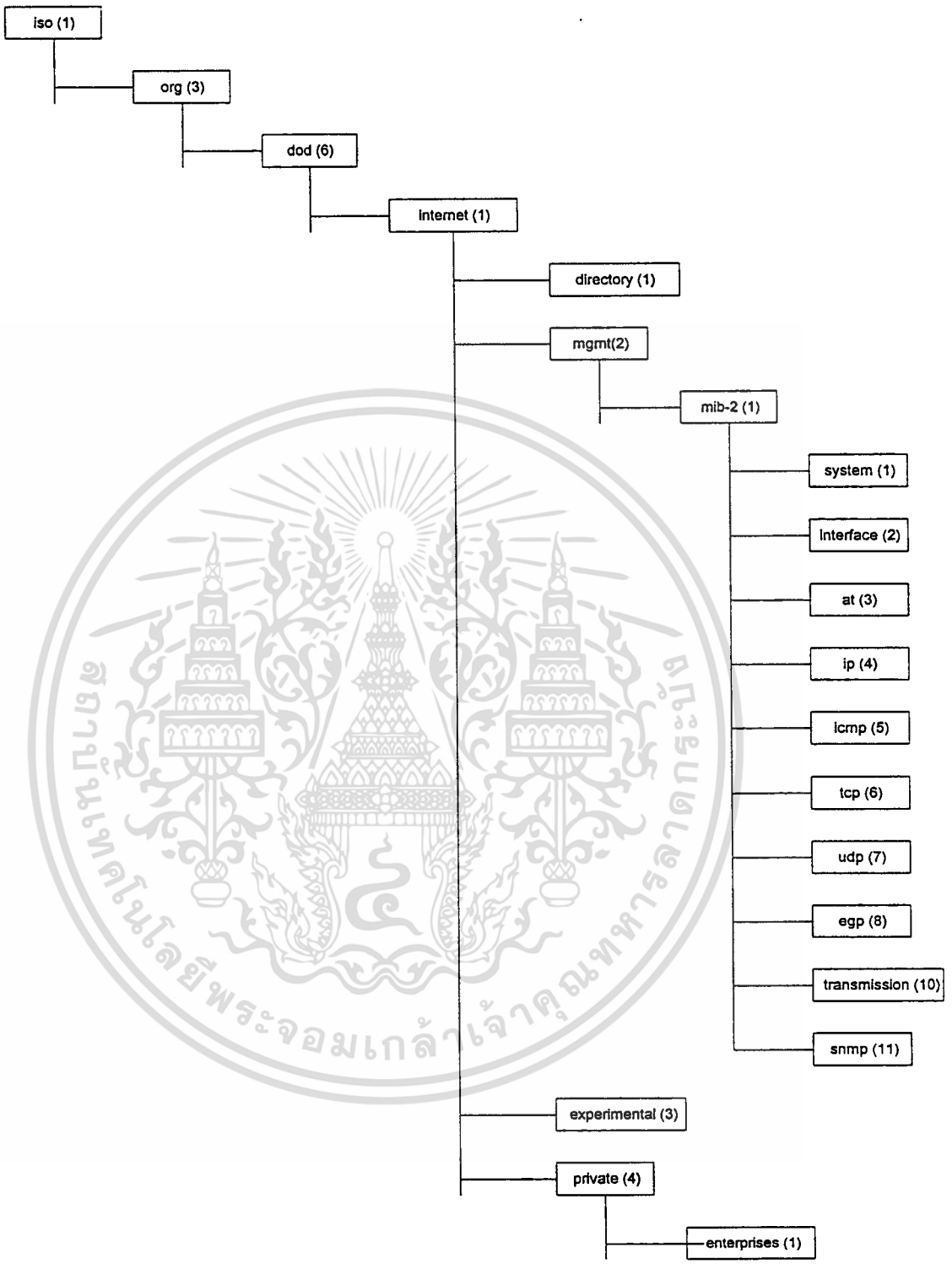
เพื่อจัดหามาตราฐานของการแทนที่ข้อมูลการบริหาร เอสเอ็มไอจะต้องจัดหามาตราฐานเทคนิคสำหรับ

1. กำหนดโครงสร้างของเอ็มไอบี โดยเฉพาะ
2. กำหนดออบเจ็คต์เฉพาะ มีความสัมพันธ์และค่าของแต่ละออบเจ็คต์
3. เข้ารหัสค่าของออบเจ็คต์

3.11.5.2 โครงสร้างของเอ็มไอบี

ตัวบ่งชี้ออบเจ็คต์ เป็นตัวบ่งชี้พิเศษสำหรับชนิดออบเจ็คต์เฉพาะค่าของมันประกอบด้วยลำดับของอินทีเจอร์ ชุดของออบเจ็คต์ที่กำหนดไว้มีโครงสร้างแบบต้นไม้ ซึ่งรูทของต้นไม้เป็นออบเจ็คต์กล่าวถึง มาตราฐานเอเอสเอ็น 1

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.9 แสดงโครงสร้างต้นไม้ของออบเจค

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 3.9 อินเทอร์เน็ตโหนดมีตัวบ่งชี้ออบเจ็คต์ ค่าของ 1.3.6.1 ค่านี้เป็นเหมือนพรีฟิกสำหรับโหนดที่ระดับต่ำกว่าต่อไปของต้นไม้

เอกสารเอสเอ็มไอ กำหนด 4 โหนดภายใต้อินเทอร์เน็ตโหนด

1. ไดเรคทอรี ซับทรีนี้กันไว้สำหรับอนาคตใช้กับ โอเอสไอไดเรคทอรี
2. mgnt ซับทรีนี้ใช้สำหรับออบเจ็คต์กำหนดไว้ในเอกสารไอเอบี
3. experimental ซับทรีนี้ใช้เพื่อบ่งบอกออบเจ็คต์ถูกใช้ในอินเทอร์เน็ต experiment
4. private ซับทรีนี้ถูกใช้เพื่อบ่งบอกออบเจ็คต์ถูกกำหนด unilaterally

ความสัมพันธ์ของออบเจ็คต์

ออบเจ็คต์ภายในเอสเอ็นเอ็มพี เอ็มไอบี และโครงสร้างเอ็มไอบีทั้งหมดถูกกำหนดโดย เอเอสเอ็น 1 เพียงซับเซ็ตที่จำกัดของ element และลักษณะของเอเอสเอ็น 1 ถูกใช้ เพื่อเก็บวัตถุประสงค์ของความธรรมดา

ชนิดยูนิเวอร์เซล

ภายในกลุ่มยูนิเวอร์เซล เพียงชนิดข้อมูลต่อไปนี้เท่านั้นที่ถูกให้ใช้เพื่อการกำหนด เอ็มไอบีออบเจ็คต์

- integer
- octet string
- null
- object identifier
- sequence of

ชนิดแอพพลิเคชั่น

อาร์เอฟซี 1155 มีรายชื่อจำนวนของชนิดข้อมูลแอพพลิเคชั่นชนิดต่อไปนี้ถูกกำหนด

- networkaddress ชนิดนี้ใช้โครงสร้าง CHOICE เพื่อให้มีการเลือกของรูปแบบที่อยู่ จาก 1 ในจำนวนของกลุ่มโปรโตคอล
- ipaddress 32 บิท address ใช้รูปแบบที่ถูกชี้เฉพาะในไอพี
- counter ไม่ใช่ negative integer ซึ่งอาจจะเพิ่มแต่ไม่ลด
- guage ไม่ใช่ negative integer ซึ่งอาจเพิ่มหรือลด ด้วยค่าสูงสุง 2^{32}-1
- timeticks ไม่ใช่ negative integer ซึ่งนับเวลา 1/100 วินาทีตั้งแต่บางช่วง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- opaque สนับสนุนความสามารถส่งผ่านข้อมูลที่ไม่มีหลักเกณฑ์

กำหนดออบเจ็คต์

แหล่งข้อมูลการบริหารประกอบด้วยชุดของออบเจ็คต์ แต่ละออบเจ็คต์มีชนิดและค่า ชนิดของออบเจ็คต์กำหนดชนิดโดยเฉพาะของออบเจ็คต์การบริหาร

กำหนดตาราง

วิธีที่ดีที่สุดเพื่ออธิบาย ความหมายของการเชื่อมต่อตาราง ก็โดยใช้ตัวอย่างพิจารณา tcpConntable มีตัวบ่งชี้ออบเจ็คต์ 1.3.6.1.2.1.6.13. ซึ่งออบเจ็คต์นี้มีข้อมูลเกี่ยวกับการรักษาการเชื่อมต่อทีซีพี โดย corresponing manager entity สำหรับแต่ละการติดต่อ ข้อมูลต่อไปนี้ถูกเก็บไว้ในตาราง

- state สถานะของการเชื่อมต่อทีซีพี
- local address คือ ip address ของ end of connection นี้
- local port คือ tcp port ของ end of connection นี้
- remote address คือ ip address ของ end of connection อื่น
- remote port คือ tcp port ของ end of conneciton อื่น

การเข้ารหัส

ออบเจ็คต์ของเอ็มไอบี ถูกเข้ารหัสโดยใช้ กฎพื้นฐานการเข้ารหัส เกี่ยวกับ เอเอสเอ็น 1 ใช้กันอย่างกว้างขวาง แม้ว่าไม่มี compact หรือประสิทธิภาพ รูปแบบของการเข้ารหัสมากนัก ทำให้เป็นมาตราฐานรูปแบบการการเข้ารหัส

3.11.5.3 เอ็มไอบี II

เอ็มไอบี II กำหนดเวอร์ชัน 2 ของเอ็มไอบี โดยเวอร์ชัน 1 ถูกส่งออกเป็น RFC 1156 เอ็มบีไอ II เป็น superset ของเอ็มไอบี I มีออบเจ็คต์เพิ่มหรือกลุ่มเพิ่ม

กฎเกณฑ์ต่อไปนี้ถูกนำมากล่าวใน RFC 1213 เพื่อประกอบเข้าเป็นออบเจ็คต์ในเอ็มไอบี II

- ออบเจ็คต์เป็นหัวใจสำคัญของการบริหาร fault และ configuration
- เข้าไปยุ่งกับออบเจ็คต์ได้เฉพาะความเสียหายจำกัด
- หลักฐานของการใช้ในปัจจุบันเป็นสิ่งที่ต้องการ
- จำนวนออบเจ็คต์เพิ่มขึ้นจากเอ็มไอบี I
- เพื่อหลีกเลี่ยงการมีมากเกินไป หรือซ้ำซ้อน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- ไม่มีการ การทำออบเจ็คต์เฉพาะ

จากรูป 3.13 เอ็มไอบี II ถูกแบ่งย่อยเป็นกลุ่มดังนี้

- system ข้อมูลทุกอย่างที่เกี่ยวกับระบบ
- interface ข้อมูลเกี่ยวกับแต่ละการเชื่อมต่อจากระบบไปยังระบบเครือข่ายย่อย
- at (address translation) บรรยายเกี่ยวกับตารางแปลงที่อยู่สำหรับอินเทอร์เน็ตไปยังการแม็พที่อยู่เครือข่ายย่อย
- ip ข้อมูลเกี่ยวกับการกระทำและ execute IP บนระบบนี้
- icmp ข้อมูลเกี่ยวกับการกระทำและ execute Icmp บนระบบนี้
- tcp ข้อมูลเกี่ยวกับการกระทำและ execute TCP บนระบบนี้
- udp ข้อมูลเกี่ยวกับการกระทำและ execute UDP บนระบบนี้
- egp ข้อมูลเกี่ยวกับการกระทำและ execute egp บนระบบนี้
- transmission ให้ข้อมูลเกี่ยวกับรูปแบบการสื่อสาร และเข้าถึงโปรโตคอลที่แต่ละระบบทำการเชื่อมโยง
- snmp ข้อมูลเกี่ยวกับการกระทำและ execute SNMP บนระบบนี้

โครงสร้างของแต่ละกลุ่มถูกกำหนดโดยโครงสร้างต้นไม้กลุ่มต่าง ๆ ดังนี้

1. system group ให้ข้อมูลทั่วไปเกี่ยวกับระบบการบริหาร ออบเจ็คต์ในกลุ่มนี้ส่วนใหญ่ต้องอธิบายเอง แต่หลาย ๆ คำแนะนำอาจเป็นประโยชน์
2. Interface group มีข้อมูลทั่วไปเกี่ยวกับการเชื่อมต่อระดับ physical ของ entity รวมทั้งข้อมูลการจัดระบบและสถิติของเหตุการณ์ที่เกิดขึ้นแต่ละการเชื่อมต่อ
3. Address translation group มี 1 ตารางแต่ละแถวในตารางแทนที่การเชื่อมแบบ physical ของระบบที่อยู่ของระบบเครือข่าย คือ IP address สำหรับระบบนี้ที่การเชื่อมต่อนี้ ฟิสิคัลแอดเดรส ขึ้นกับธรรมชาติของ ระบบเครือข่ายย่อย
4. IP group มีข้อมูลเกี่ยวกับความสัมพันธ์ของการกระทำ และการอิมพลีเม็นท์ของ IP ที่โหนดหนึ่ง
5. ICMP group มีข้อมูลเกี่ยวกับความสัมพันธ์ของการกระทำ และการอิมพลีเม็นท์ของ ICMP ที่โหนดหนึ่ง
6. TCP group มีข้อมูลเกี่ยวกับความสัมพันธ์ของการกระทำ และการอิมพลีเม็นท์ของ TCP ที่โหนดหนึ่ง ซึ่ง tcpConnTable เป็นส่วนหนึ่งของกลุ่มนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

7. UDP group มีข้อมูลเกี่ยวกับความสัมพันธ์ของการกระทำและการอิมพลีเม็นท์ของ UDP ที่โหนดหนึ่ง และยังมีข้อมูลเกี่ยวกับดาต้าแกรมส่งและรับอีกด้วย มี udp table ซึ่งมีข้อมูลเกี่ยวกับ udp ของ entity
8. EGP group มีข้อมูลเกี่ยวกับความสัมพันธ์ของการกระทำ และการอิมพลีเม็นท์ของ egp ที่โหนดหนึ่ง และยังมีข้อมูลเกี่ยวกับ ข่าวสาร egp ส่งและรับอีกด้วย มี egpNeightable ซึ่งมีข้อมูลเกี่ยวกับแต่ละ gateway ใกล้เคียงที่เป็นที่รู้จักยอมรับ entity นี้
9. Transmission group ตั้งใจให้ มีออบเจ็คต์ ซึ่งให้รายละเอียดเกี่ยวกับตัวกลางการสื่อสารของแต่ละ การเชื่อมโยงของระบบ

3.11.5.4 ของเขตของเอ็มไอบี II

ผู้ใช้จำนวนมากหวังให้บางสิ่งสำเร็จได้ด้วย เอสเอ็นเอ็มพี ความคาดหวังก็คือ เอสเอ็นเอ็มพีทำให้ผู้ใช้ทำการบริหารทรัพยากร และการบริหารระบบทั้งหมด แต่ขอบเขตของ เอสเอ็นเอ็มพีถูกจำกัดด้วยออบเจ็คต์ที่มีอยู่เพื่อการบริหาร โดยหลักการแล้วเอ็มไอบี II สนับสนุนการตรวจสอบ และบริหารระบบเครือข่ายจากชั้น transport layer ลงไป เกี่ยวกับทำอย่างไรการติดต่อเชื่อมโยงจึงจะสำเร็จ, แพ็กเก็ตมีเส้นทางเดินอย่างไรเพื่อบริหารทรัพยากร mail server และพรินเตอร์ เอ็มไอบีจำเป็นต้องมีการส่งเสริมพัฒนาให้ดีขึ้น

3.11.6 เอสเอ็นเอ็มพี เวอร์ชัน 2 (SNMPv2)

3.11.6.1 เบื้องหลังของเอสเอ็นเอ็มพีเวอร์ชัน 2

การพัฒนา เอสเอ็นเอ็มพีเวอร์ชัน 2 มีการทำทีมขึ้นมา 2 ทีม ทีมหนึ่งทำเกี่ยวกับความปลอดภัยของเอสเอ็นเอ็มพีเวอร์ชัน 2 อีกทีมทำเกี่ยวกับทุกอย่างอื่น ๆ รวมทั้งข้อมูลการบริหาร และโปรโตคอล เอสเอ็นเอ็มพีวี 2 คล้ายกับ เอสเอ็นเอ็มพี จากที่ซึ่งมันทำการพัฒนา เอสเอ็นเอ็มพีวี 2 ให้การส่งเสริมหน้าที่การทำงานแก่เอสเอ็นเอ็มพีวี 1 และปรับการส่งเสริมความปลอดภัยของเอสเอ็นเอ็มพีด้วยการเปลี่ยนแปลงบางอย่าง

การมีเอสเอ็นเอ็มพีวี 2 ทำให้เกิดความยุ่งยากแก่ผู้ใช้ในเรื่องการบริหารระบบเครือข่าย ในด้านหนึ่ง มีการติดตั้งพื้นฐานของระบบเริ่มต้นการบริหารเอสเอ็นเอ็มพี เพิ่มขึ้นมาก ผู้ใช้ส่วนใหญ่หวังให้เอสเอ็นเอ็มพีสำเร็จ ตามมาตราฐานแต่บางส่วน ต้องการใช้เอสเอ็นเอ็มพีวี 2 ทันที แต่คนอื่น ๆ ก็ยังคงอยากใช้เอสเอ็นเอ็มพีไปเรื่อย ๆ จนกว่าจะถึงการเปลี่ยนไปใช้โอเอสไอ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในอีกด้านหนึ่ง มีการเพิ่มจำนวนบริษัท โดยเฉพาะบริษัทขนาดใหญ่ที่มีการยอมรับโอเอสไอ ถ้าเอสเอ็นเอ็มพีวี 2 กลายเป็นคู่แข่งกับโอเอสไอระบบการบริหาร จะเป็นการแบ่งบริษัทออกเป็นส่วนย่อย ๆ 2 ส่วน

3.11.6.2 โครงสร้างของข้อมูลการบริหาร

โครงสร้างของข้อมูลการบริหาร สำหรับเอสเอ็นเอ็มพีวี 2 ขึ้นกับเอสเอ็มไอ สำหรับเอสเอ็นเอ็มพี, เอสเอ็นเอ็มพีวี 2 ให้รูปลักษณะและเอกสารที่ประณีตของออบเจ็คต์การบริหาร และ เอ็มไอบี แบ่งเป็น 4 ส่วน

1. กำหนดความหมายออบเจ็คต์ เหมือนเอสเอ็นเอ็มพี เอสเอ็มไอ ใช้บรรยายออบเจ็คต์การบริหาร ทั้งเอสเอ็นเอ็มพีและเอสเอ็นเอ็มพีวี 2 ชนิดของออบเจ็คต์ เป็นแบบธรรมดาหรือแอพพลิเคชั่น ชนิดธรรมดาค่อนข้างเหมือนกันทั้งคู่ แต่ต่างตรงที่เอสเอ็นเอ็มพีวี 2 ให้ 32 บิต integer ความแตกต่างอื่น ก็คือ enumerated bit-string ใช้ในเอสเอ็นเอ็มพีวี 2
2. ตารางแห่งแนวคิด เหมือนเอสเอ็นเอ็มพี ในเอสเอ็นเอ็มพีวี 2 ทำได้แต่ ออบเจ็คต์ สเกลาร์ ข้อมูลที่ซับซ้อนแทนเป็นตาราง
3. กำหนดความหมายการบอกกล่าว ใช้เพื่อกำหนดข้อมุลที่ถูกส่งโดย เอสเอ็นเอ็มพีเอ็นติตี้ เมื่อมีเหตุการณ์ที่ไม่ดีเกิดขึ้นที่เอ็นติตี้ ทั้ง แทร็พ และ รีเควสท์เป็นการบอกกล่าว
4. โมดูลข้อมูล บ่งบอกกลุ่มของความหมายที่สัมพันธ์กัน มีอยู่ 3 ชนิด ที่ใช้กัน
   - MIB module มีความหมายของ ออบเจ็คต์การบริหาร ที่สัมพันธ์กันภายใน
   - Compliance statement สำหรับ MIB module ทำโดยใช้ MODULE-COMPLIANCE และ OBJECT-GROUP
   - Capability statement สำหรับการกระทำเอเจ้นต์ ซึ่งทำโดยใช้ AGENT-CAPABILITY

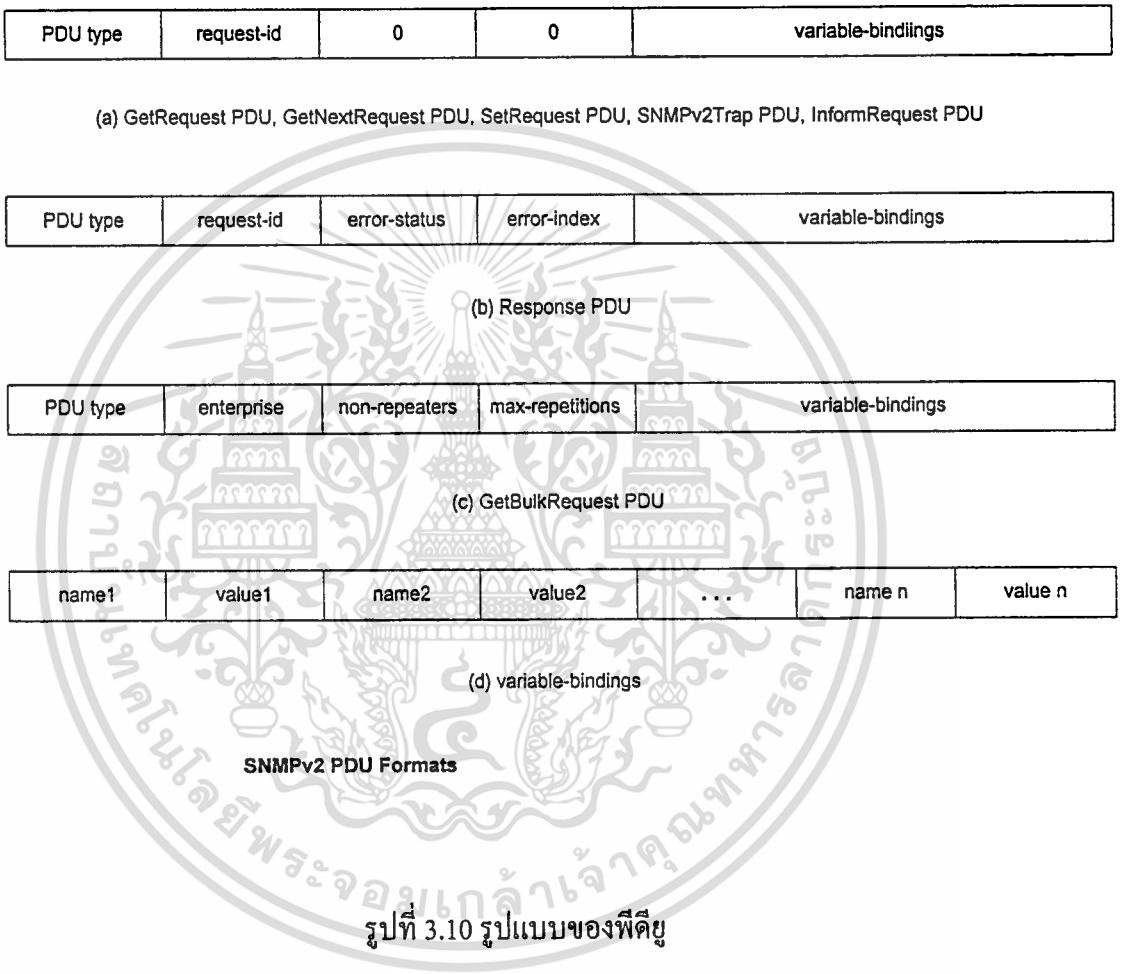
3.11.6.3 การกระทำโปรโตคอล (Protocol Operation)

เอสเอ็นเอ็มพีวี 2 พีดียู ถูกห่อหุ้มอยู่ในข่าวสาร รูปแบบข่าวสารเอสเอ็นเอ็มพีวี 2 คล้ายกับที่กำหนดให้เอสเอ็นเอ็มพี 3 รูปแบบของการเข้าถึงข้อมูลการบริหารโดยเอสเอ็นเอ็มพีวี 2

1. Manager-Agent Reqest-Respond เอสเอ็นเอ็มพีวี 2 เอ็นติตี้ที่เป็นผู้จัดการส่งรีเควสท์ไปยังเอเจ้นต์ และ เอสเอ็นเอ็มพีวี 2 เอ็นติตี้ส่งเรสปอนด์เรียกกลับมาหรือปรับปรุง ข้อมูลการบริหารที่เกี่ยวข้องกับอุปกรณ์การบริหาร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2. Manager-Manager Request-Response เอสเอ็นเอ็มพีวี 2 เอ็นติตี้ ที่เป็นผู้จัดการส่งรีเควสท์ไปยังผู้บริหาร และ เอสเอ็นเอ็มพีวี 2 เอ็นติตี้ที่เป็นผู้จัดการทำการตอบสนอง Response ใช้ส่งบอก เอสเอ็นเอ็มพีวี 2 เอ็นติตี้ที่เป็นผู้จัดการที่เกี่ยวกับอีกผู้จัดการ
3. Agent-Manager uncomfirm เอสเอ็นเอ็มพีวี 2 เอ็นติตี้ที่เป็นเอเจ้นต์ส่งค่าข้อมูลที่ไม่ได้ขอไปยังผู้บริหาร และ ไม่มีการตอบสนองกลับมาใช้ส่งบอก เอสเอ็นเอ็มพีวี เอ็นติตี้ ที่เป็นผู้จัดการ ให้รู้ถึงเหตุการณ์ผิดปกติเกี่ยวกับอุปกรณ์การบริหาร



รูปที่ 3.10 รูปแบบของพีดียู

PDU format

ดังรูป 3.14 จำไว้ว่า GetRequest, GetNextRequest, SetRequest,SNMPv2 trap และ InformRequest PDU มีรูปแบบแบบเดียวกันกับ Response PDU พร้อมด้วยสถานะการผิดพลาด และฟิล์ดของการผิดพลาดซึ่งเซ็ตเป็น 0 โดยปกติ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

GetRequest PDU

เอสเอ็นเอ็มพีวี 2 เหมือนเอสเอ็นเอ็มพี GetRequest PDU ทั้งรูปแบบและความหมายของคำ มีข้อแตกต่างคือการตอบสนองถูก handle เอสเอ็นเอ็มพี GetRequest operation เป็น atomic แต่เอสเอ็นเอ็มพีวี 2 variable มาก

GetNextRequest PDU

เอสเอ็นเอ็มพีวี 2 เหมือนเอสเอ็นเอ็มพี GetNextRequest PDU ทั้งรูปแบบและความหมายของคำ มีข้อแตกต่างคือเอสเอ็นเอ็มพี GetNextRequest operation เป็น atomic แต่เอสเอ็นเอ็มพีวี 2 variable มากเท่าที่จะทำได้

GetBulkRequest PDU

เป็นอีกอันหนึ่งที่เพิ่มขึ้นในเอสเอ็นเอ็มพีวี 2 มีเป้าหมายเพื่อลดจำนวนของ โปรโตคอลที่เปลี่ยนแปลงให้ต่ำสุด เพื่อเอาข้อมูลจากการบริหารจำนวนมากกลับมา ใช้หลักในการเลือกเหมือน GetNextRequest การเลือกมักเป็นออบเจ็คต์ต่อไปในลำดับ lexicographic ข้อแตกต่างก็คือ มันเป็นไปได้เพื่อบ่งบอกว่า lexicographic successor ถูกเลือก

SetRequest PDU

เหมือนของ เอสเอ็นเอ็มพี SetRequest PDU ทั้งรูปแบบและความหมายของคำ ที่ต่างกันก็คือ การตอบสนองถูก handle

SNMPv2 Trap PDU

ถูกสร้างและส่งโดยเอสเอ็นเอ็มพีวี 2 เอ็นติตี้ ที่เป็นเอเจ้นต์ เมื่อเหตุการณ์ไม่ปกติเกิดขึ้น SNMPv2 Trap PDU มีรูปแบบที่ต่างจาก SNMP Trap PDU

InformRequest PDU

ถูกส่งโดย เอสเอ็นเอ็มพีวี 2 ที่เป็นผู้จัดการไปยัง ผู้จัดการอื่น เพื่อให้ข้อมูลการบริหารแก่แอพพลิเคชั่น โดยใช้ latter entity

Table Operation

ให้ตัวอย่างของการใช้ลักษณะต่าง ๆ ใน SNMPv2 สำหรับการกระทำบนตาราง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.11.6.4 แผนที่ทรานสปอร์ท (Transport Mapping)

เอสเอ็นเอ็มพีวี 2 มีการตกลงของการแม็พของ เอสเอ็นเอ็มพีวี 2 บนโปรโตคอลระดับ ทรานสปอร์ท (transport) ไว้หลายอย่างดังต่อไปนี้

- UDP
- OSI connectionless
- Novell IPX
- Appletalk

3.11.6.5 เอสเอ็นเอ็มพีวี 2 แหล่งข้อมูลการบริหาร

เอสเอ็นเอ็มพีวี 2 เอ็มไอบี กำหนดออบเจ็คต์ซึ่งบรรยายพฤติกรรมของเอสเอ็นเอ็มพีวี 2 เอ็นติตี้ เอ็มไอบี มีอยู่ 5 กลุ่ม

1. SNMPv2 statistic group: ที่เก็บของออบเจ็คต์ให้ basic instrumentation ของ เอสเอ็นเอ็มพีวี 2 เอ็นติตี้
2. SNMPv1 statistic group: ที่เก็บของออบเจ็คต์ให้ basic instrumentation ของ เอสเอ็นเอ็มพีวี 2 เอ็นติตี้ ซึ่งอิมพลีเม็นต์เอสเอ็นเอ็มพีวี 1 ด้วย
3. Object resource group: ที่เก็บของออบเจ็คต์ให้ เอสเอ็นเอ็มพีวี 2 เอ็นติตี้ ที่เป็นเอเจ้นต์บรรยาย แหล่งทรัพยากร dynamically configurable object ของมัน
4. Trap group: ที่เก็บของออบเจ็คต์ซึ่งให้เอสเอ็นเอ็มพีวี 2 เอ็นติตี้ ทำการกำหนดระบบเพื่อผลิต SNMPv2-Trap PDUS เมื่อเป็นเอเจ้นต์
5. Set group: ออบเจ็คต์เดี่ยวซึ่งใช้ เอสเอ็นเอ็มพีวี 2 เอ็นติตี้ร่วมกันหลายอัน เพื่อร่วมกันใช้ชุดคำสั่งของ เอสเอ็นเอ็มพีวี 2 เมื่อเป็นผู้จัดการ

Manager to manager MIB

ประกอบด้วยชุดของออบเจ็คต์ซึ่งบรรยายพฤติกรรมของ SNMPv2 entity ซึ่งเป็นผู้จัดการ MIB ประกอบด้วย 2 กลุ่ม

1. Alarm group ที่เก็บของออบเจ็คต์ซึ่งให้ description และ configuration ของ threshold alarm จากเอสเอ็นเอ็มพีวี 2 เอ็นติตี้ ที่เป็นทั้งผู้จัดการ และ เอเจ้นต์
2. Event group ที่เก็บของออบเจ็คต์ซึ่งให้ description และ configuration ของเหตุการณ์จากเอสเอ็นเอ็มพีวี 2 เอ็นติตี้ ที่เป็นทั้งผู้จัดการ และ เอเจ้นต์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การอยู่ร่วมกันด้วย SNMP

พยายามทำให้การเปลี่ยนจาก เอสเอ็นเอ็มพีไปยังเอสเอ็นเอ็มพีวี 2 สะดวกราบรื่นที่สุดเท่าที่จะทำได้ วิธีง่ายที่สุดก็คือการปรับปรุงระบบการบริหารเพื่อสนับสนุนเอสเอ็นเอ็มพีวี 2 เพื่อให้ใช้ร่วมกันทั้ง เอสเอ็นเอ็มพีวี 2 ผู้จัดการ, เอเจ้นต์เอสเอ็นเอ็มพีวี 2 และ เอเจ้นต์เอสเอ็นเอ็มพี

ข้อมูลการบริหาร

โครงสร้างของข้อมูลการบริหาร สำหรับเอสเอ็นเอ็มพีวี 2 เกือบเป็นซุปเปอร์เซท(superset) ของเอสเอ็มไอ สำหรับเอสเอ็นเอ็มพี และ เอสเอ็นเอ็มพีวี 2 รวบรวมแบบฝึกหัดที่มีอยู่เพื่อกำหนดเอ็มไอบีโมดูล (MIB module)

การที่จะให้เอ็มไอบีโมดูล เข้ากับเอสเอ็นเอ็มพีวี 2 เอสเอ็มไอ ต้องมีการเปลี่ยนแปลงบางอย่าง มันเป็นไปได้สำหรับเอเจ้นต์ เพื่อการรักษาเอสเอ็นเอ็มพีเอ็มไอบีอันเชนจ์ (MIB unchange) และร่วมใน SNMPv2-SNMP สภาพแวดล้อม

Protocol Operation

โปรโตคอลที่กำหนดในเอสเอ็นเอ็มพีวี 2 เฟรมเวิร์ค คล้ายกับเอสเอ็นเอ็มพีเฟรมเวิร์ค ใช้รูปแบบพีดียูเหมือนกัน การเปลี่ยนแปลงหลักคือมี GetGulkRequest และ InformRequest PDU และเปลี่ยนความหมายคำเพื่อให้ได้การกระทำ (operation) ที่ให้ผลหลากหลายกว่าลักษณะอะตอมมิค

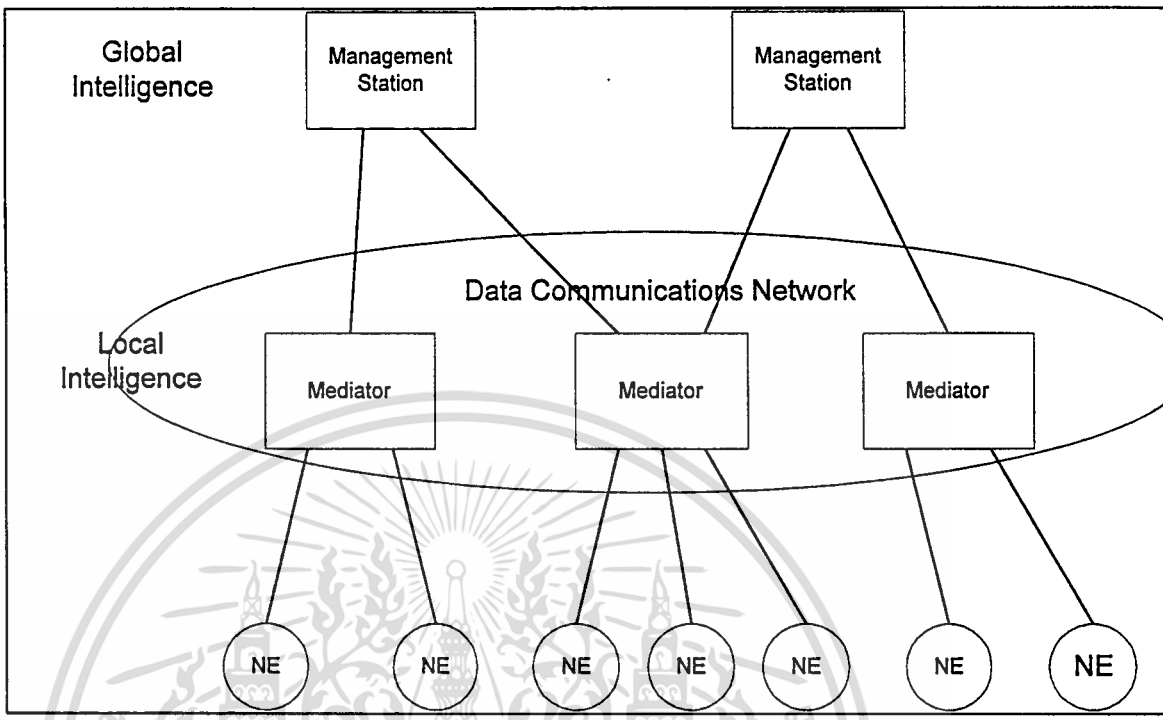
3.12 สถาปัตยกรรมแบบรวมสำหรับการบริหารระบบเครือข่ายระยะไกลและระยะใกล้

ระบบเครือข่ายระยะใกล้ได้เจริญเติบโตขึ้นในอัตราที่เร็วมาก คอมพิวเตอร์ที่ทำการเชื่อมต่อก็ได้เป็นส่วนที่สำคัญในสภาวะแวดล้อมในการเชื่อมต่อปัจจุบัน อย่างไรก็ตามหน่วยงานก็ได้เคลื่อนย้ายระบบเครือข่ายระยะใกล้เข้าสู่สภาวะแวดล้อมการเชื่อมต่อแบบกว้าง ซึ่งก็คือการที่ระบบเครือข่ายระยะใกล้และอุปกรณ์ที่สามารถเข้าถึงได้สามารถแลกเปลี่ยนข้อมูลโดยไม่ถูกจำกัดโดยความจำกัดด้านภูมิศาสตร์

การเชื่อมต่อของระบบเครือข่ายระยะใกล้นั้นทำให้มีปัญหาและงานที่จะต้องจัดการระบบเครือข่ายระยะไกลและระยะใกล้ทั้งหมดจากสถานที่ที่เป็นศูนย์กลาง จุดประสงค์ของการบริหารแบบรวมรวมถึงการปรับปรุงประสิทธิภาพในการทำงาน ,ประยุกต์ใช้โปรซีเดอร์(procedure)ที่เป็นมาตรฐานและเหมือนกัน ,ปรับปรุงการแก้ความผิดพลาด และ ปรับปรุงประสิทธิภาพรวมถึงความถูกต้องของข้อมูลจากอุปกรณ์ที่หลากหลายที่ประกอบกันเป็นเครือข่าย

ในส่วนนี้จะอธิบายโครงสร้างและส่วนประกอบของสถาปัตยกรรมสำหรับการบริหารระบบเครือข่ายระยะไกลและระยะใกล้แบบรวม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.11 แสดงส่วนประกอบของสถาปัตยกรรมการบริหาร

ส่วนประกอบของสถาปัตยกรรมการบริหารประกอบไปด้วย 3 ส่วน

- ส่วนประกอบในเครือข่าย (Network Element) รวมถึงอุปกรณ์ในระบบเครือข่ายระยะไกลและใกล้ เช่น แอปพลิเคชั่น เซิร์ฟเวอร์,บริดจ์ ,เราท์เตอร์ ,แพคเกตสวิชชิ่ง และ มัลติเพลกเซอร์
- ตัวกลาง (Mediators) เป็นการเปลี่ยนโปรโตคอลระหว่างโปรโตคอลการบริหารnetwork element กับ โปรโตคอลที่บริหารระบบเครือข่ายระยะไกลที่ใช้งานในแอปพลิเคชั่นบนเครื่องที่ทำการบริหาร นอกเหนือจากนั้นตัวกลางยังทำหน้าที่ที่สำคัญอื่นๆเช่น การกรองและเทรชโฮลดิ่ง(thresholding) ข้อมูลก่อนจะส่งไปยังเครื่องที่ทำการบริหาร และทำการกระจายเหตุการณ์ของการบริหารไปยังตำแหน่งการบริหารอื่นๆ
- เครื่องที่ทำการบริหาร (Management Station) จะทำการรับ ,วิเคราะห์ และแสดงข้อมูลของเครือข่ายทั้งหมดแก่ผู้ใช้และยังยอมให้ผู้ใช้ทำการควบคุมจากระยะไกลไปยังอุปกรณ์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สถาปัตยกรรมแบบนี้มีข้อดีมากกว่าแบบเดิมที่เป็นสถาปัตยกรรมแบบ2ปลายคือส่วนประกอบในเครือข่ายกับเครื่องที่ทำการบริหาร ประโยชน์นี้รวมถึงการออกแบบที่เป็นโมดูลที่แบ่งหน้าที่ระหว่างส่วนที่ทำการบริหารระยะไกลและใกล้ ,การรักษา bandwidth ของเครือข่ายโดยการกรองโดยตัวกลาง และ ความสามารถที่จะขยายเป็นเครือข่ายที่ใหญ่มากเพราะการใช้เทคนิคแบบกระจายส่วนประกอบของเครือข่ายระยะใกล้ในปัจจุบันส่วนใหญ่สามารถรองรับเอสเอ็นเอ็มพี เอสเอ็นเอ็มพีนี้ทำงานบน UDP อย่างไรก็ตามโปรโตคอลการบริหารได้ออกแบบเป็นอิสระจากการทำงานของโปรโตคอลการส่งข้อมูล

โปรโตคอลเอสเอ็นเอ็มพีที่เป็นการติดต่อสื่อสารระหว่างผู้บริหารกับเอเจ้นต์ต์ใช้ข้อความ 5 ชนิด

- Get และ GetNext ใช้โดยผู้บริหารทำการค้นหาค่าในMIBของเอเจ้นต์ต์
- Set ใช้โดยผู้บริหารทำการตั้งค่าในMIBของเอเจ้นต์ต์
- GetResponse ใช้โดยเอเจ้นต์ต์ที่จะทำการตอบสนองข้อมูลให้กับผู้บริหาร
- Trap ใช้โดยเอเจ้นต์ต์เพื่อทำการแจ้งต่อผู้บริหารในเหตุการณ์ที่สำคัญและร้ายแรงแบบอะซิงโครนัส

พรอกซี่เอเจ้นต์ต์(Proxy Agent) ถูกนำมาใช้ในการแปลงโปรโตคอลในการบริหารอื่นๆเป็นเอสเอ็นเอ็มพี

ส่วนประกอบส่วนที่สองของสถาปัตยกรรม ตัวกลางทำหน้าที่แปลงโปรโตคอลระหว่างข้อมูลของอุปกรณ์เอสเอ็นเอ็มพีระดับล่างกับข้อมูลระดับสูงที่เหมาะกับการประมวลผลและแสดงของเครื่องที่ทำการบริหารโดยซอฟท์แวร์ตัวกลางประกอบไปด้วย 3 ส่วน

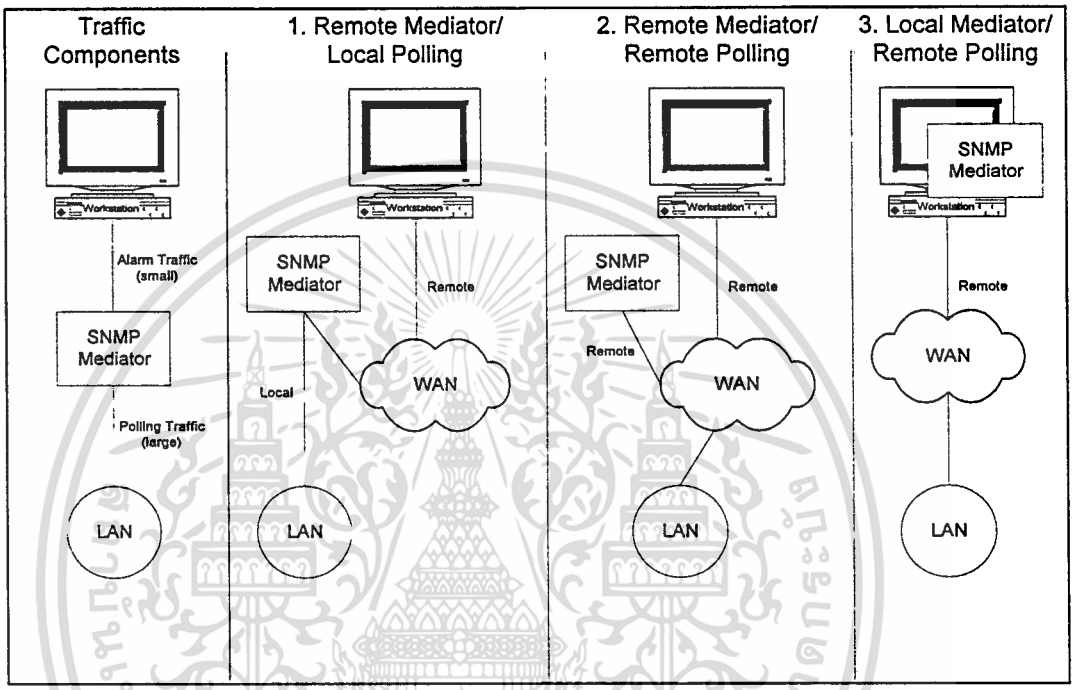
- โมดูลที่ทำการติดต่อสื่อสารของส่วนประกอบในเครือข่ายที่ใช้เอสเอ็นเอ็มพี
- โมดูลที่ทำการแจ้งเตือนที่ตรวจสอบอุปกรณ์ในระบบและสร้างการแจ้งเตือนตามที่ผู้ใช้ได้ตั้งเงื่อนไขไว้
- โมดูลที่ทำการติดต่อสื่อสารของเครื่องที่ทำการบริหารซึ่งแสดงการแจ้งเตือนและรับการควบคุมจากผู้บริหารหรือผู้ใช้

ตัวกลางจะทำการตัดสินใจว่าเมื่อใดจะส่งสัญญานแจ้งเตือนไปยังเครื่องที่ทำการบริหารที่ควบคุมโดยกฎที่ผู้ใช้กำหนดขึ้น โดยกฎนี้ก็จะระบุทั้งลักษณะและความถี่ของการพูลลิ่ง ,ค่าของMIBและเทรชโฮลที่จะเริ่มการแจ้งเตือน อย่างไรก็ตามผู้ใช้สาสารถระบุ ความร้ายแรง, โค๊ดของปัญหาและข้อความอธิบายที่อยู่ในการแจ้งเตือนที่สร้างโดยตัวกลาง ข้อมูลของตัวกลางอื่นๆจะรวมถึงรายการของอุปกรณ์ที่อยู่ในการบำรุงรักษาสำหรับการไม่สร้างสัญญานการแจ้งเตือนและค่า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในMIBที่ทำการตรวจดูเป็นระยะเพื่อทำการวิเคราะห์และแสดงโดยแอปพลิเคชั่นการบริหารด้านประสิทธิภาพ

การจราจรของการบริหารประกอบไปด้วย 2 ส่วนหลักคือ การจราจรของเอสเอ็นเอ็มพีระหว่างอุปกรณ์บนเครือข่ายระยะใกล้กับตัวกลาง และการจราจรของสัญญานควบคุมและแจ้งเตือนระหว่างเครื่องที่ทำการบริหารกับตัวกลาง



รูปที่ 3.12 แสดงการวางตำแหน่งของตัวกลาง

จากรูปการวางตำแหน่งของตัวกลางซึ่งขึ้นอยู่กับลักษณะทางภูมิศาสตร์และขนาดของเครือข่าย

1. เครือข่ายที่ใหญ่และเป็นแบบรีเจียนอลไลซ์(Regionalized) ตัวกลางจะอยู่ที่พื้นที่ในแต่ละภูมิภาคในแต่ละตัวกลางจะทำการพูลลิ่งอุปกรณ์ในเครือข่ายผ่านระบบเครือข่ายระยะใกล้ความเร็วสูง ในลักษณะแบบนี้จะให้ค่าใช้จ่ายในอุปกรณ์ที่ต่ำเพราะเฉพาะการสื่อสารของตัวกลางกับเครื่องที่ทำการบริหารเท่านั้นที่ผ่านเครือข่ายระยะไกลที่มีราคาสูง
2. เครือข่ายที่ใหญ่และมีการกระจายสูง ในกรณีนี้ตัวกลางจะทำการติดต่อจากระยะไกลจากทั้งเครื่องที่ทำการบริหารและอุปกรณ์ในเครือข่ายระยะใกล้เมื่อจะทำการพูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3. เครือข่ายขนาดเล็ก ตัวกลางจะอยู่รวมกับระบบการบริหารโดยเอสเอ็นเอ็มพีพูลลิ่งจะผ่านเครือข่ายระยะไกล

ในส่วนสุดท้ายคือเครื่องที่ทำการบริหาร โดยประกอบไปด้วยแอปพลิเคชั่นและอินเตอร์เฟสกับผู้ใช้โดยสามารถแสดงสถาปัตยกรรมแบบชั้นซึ่งประกอบด้วย 4 ชั้น

- ส่วนติดต่อกับผู้ใช้ซึ่งรับผิดชอบบนชั้นพรีเซนเทชั่น(Presentation Layer)มีหน้าที่แสดงข้อมูลแก่ผู้ใช้และรับคำสั่ง และยังสามารถจัดหาส่วนที่ธรรมดาและสามารถนำกลับมาใช้ได้อีกแก่ชั้นแอปพลิเคชั่น
- ชั้นแอปพลิเคชั่น(Application Layer) ประกอบไปด้วยทูลต่างๆที่ประกอบขึ้นเป็นระบบการบริหาร
- ชั้นโมเดลของเครือข่าย(Network Model Layer) จะแสดงส่วนประกอบของเครือข่ายและความสัมพันธ์แบบออบเจ็คต์โอเรียน และยังมีการแสดงข้อมูลซึ่งออบเจ็คต์ของโมเดลจะถูกแก้ไขข้อมูลแบบเรียลไทม์โดยข้อมูลการแจ้งเตือนและสถานะที่ได้รับจากตัวกลาง
- ชั้นการสื่อสาร (Communication Layer) ซึ่งรับผิดชอบเกี่ยวกับหน้าที่ของโปรโตคอล กับส่วนอื่นๆ เช่น ตัวกลางของระบบเครือข่ายระยะใกล้และอุปกรณ์ในระบบเครือข่ายระยะไกล

3.13 ภาพรวมของสถาปัตยกรรมการบริหารเครือข่ายแบบรวมสำหรับเครือข่ายที่หลากหลายขนาดใหญ่ (Overview of An Integrated Network Management Architecture for A Large Heterogeneous Network)

จุดประสงค์ของสถาปัตยกรรมของการบริหารเครือข่ายแบบรวมนี้คือการยอมให้การบริหารเครือข่ายแบบรวมผ่านเครือข่ายของระบบการบริหารเครือข่ายการเชื่อมต่ออัตโนมัติที่รองรับหนังสือนี้จะอธิบายโทโปโลยีและหน้าที่ของสถาปัตยกรรมที่อ้างอิงFAA ซึ่งการทำงานก็ขึ้นอยู่กับลักษณะขององค์กรของลูกค้า ซึ่งให้ต้นแบบที่สามารถประยุกต์ใช้กับองค์กรอื่นๆได้ สถาปัตยกรรมของการบริหารเครือข่ายแบบรวมมีขอบข่ายกว้างๆดังนี้

- มีการทำงานใน 6 หน้าที่ซึ่งรวมทั้งด้านการดำเนินงาน (การปฏิบัติงาน, การบำรุงรักษาการให้การบริการ) และด้านการบริหารหรือธุรกิจ (การบริหาร , การวางแผน, งานด้านวิศวกรรม) ของการบริหารการสื่อสาร
- มีเครือข่ายที่หลากหลายและระบบการสื่อสารจำนวนมาก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

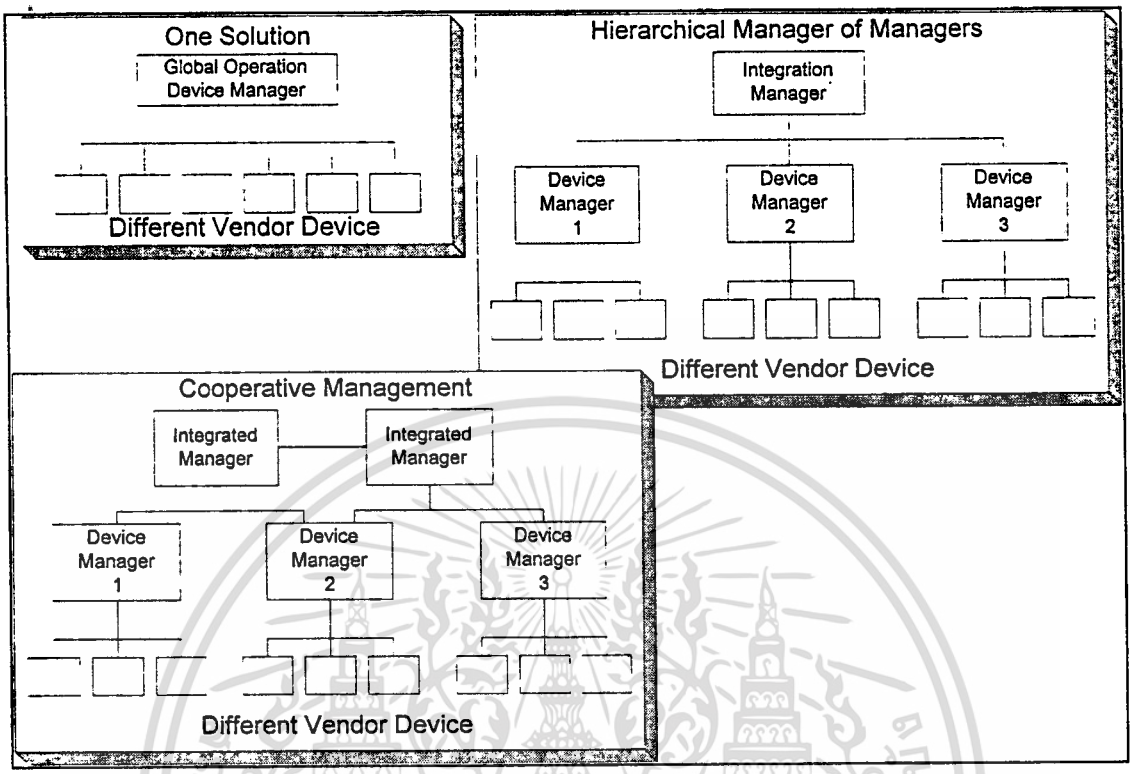
- มีโดเมนการดำเนินงานระดับต้น 4 ระดับคือ เนชั่นแนล(National) ทำการตรวจสอบและควบคุมเครือข่ายที่มีการใช้ร่วมกันในระดับชาติและการทำงานของธุรกิจสำหรับโครงการของชาติ รีเจียนนอล(Regional)เป็นอุปกรณ์การบริหารของแนชั่นแนลซึ่งรองรับการกระทำของธุรกิจ แอเรีย(Area)เป็นพื้นที่ที่มีการการปฏิบัติงานอย่างมาก โลคอล(Local)เป็นการปฏิบัติงานและการบำรุงรักษาขององค์การเบื้องต้นสำหรับที่ที่อยู่ระยะไกล ในแต่ละส่วนก็มีการทำงานโดยอัตโนมัติและมีความสำคัญต่อข้อมูลและการทำงานในแต่ละระดับแบบมีอิสระภายใน

3.13.1 สิ่งที่ต้องการสำหรับสถาปัตยกรรมการบริหารเครือข่ายแบบรวม

- มีสถาปัตยกรรมที่เข้าได้กับมาตรฐานการบริหารเครือข่าย มาตรฐานของOSIจะระบุต้นแบบเบื้องต้นสำหรับการบริหารเครือข่ายซึ่งบริหารการบริหารเครือข่ายที่กระจายกันผ่านระบบที่หลากหลาย คำจำกัดความที่ระบุก็จะเกี่ยวกับ หน้าที่การบริหารเบื้องต้น 5 หน้าที่ ,ต้นแบบของข้อมูลที่ระบุและจำกัดความออบเจ็คต์ที่ถูกบริหาร และกลุ่มของการบริการมาตรฐานและโปรโตคอลมาตรฐานที่รองรับการสื่อสารภายในระบบ
- เนื่องจากเครือข่ายประกอบด้วยเครือข่ายย่อยและระบบย่อยที่สามารถใช้ร่วมกันและรวมข้อมูลกัน จึงต้องการมาตรฐานของข้อมูล, วิธีมาตรฐานที่จะรวมข้อมูล และการรองรับการแลกเปลี่ยนข้อมูล
- เครือข่ายจะมีการเปลี่ยนแปลงเนื่องจากความต้องการและเทคโนโลยีที่เปลี่ยนไป สถาปัตยกรรมจึงควรมีความยืดหยุ่นคือระบบใหม่สามารถเพิ่มและระบบเก่าสามารถย้ายหรืออัพเกรดโดยมีผลกระทบน้อยที่สุดต่อสถาปัตยกรรมเดิม
- ผู้ที่ทำการบริหารเครือข่ายจะมีการติดต่อกับระบบต่างๆนอกเหนือจากทำงานของตนเอง เครื่องที่ทำการบริหารเครือข่ายจะยอมให้ผู้บริหารง่ายต่อการใช้ระบบรองรับของการบริหารเครือข่ายแบบรวมซึ่งก็คือการมีการติอต่อกับผู้ใช้โดยใช้GUI
- สถาปัตยกรรมควรรองรับการทำงานของการดำเนินงานเบื้องต้นซึ่งสถาปัตยกรรมของINMมีลักษณะคล้ายกับโครงสร้างขององค์กรที่มีอยู่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.13.2 ทางเลือกของสถาปัตยกรรมการบริหารเครือข่ายแบบรวม



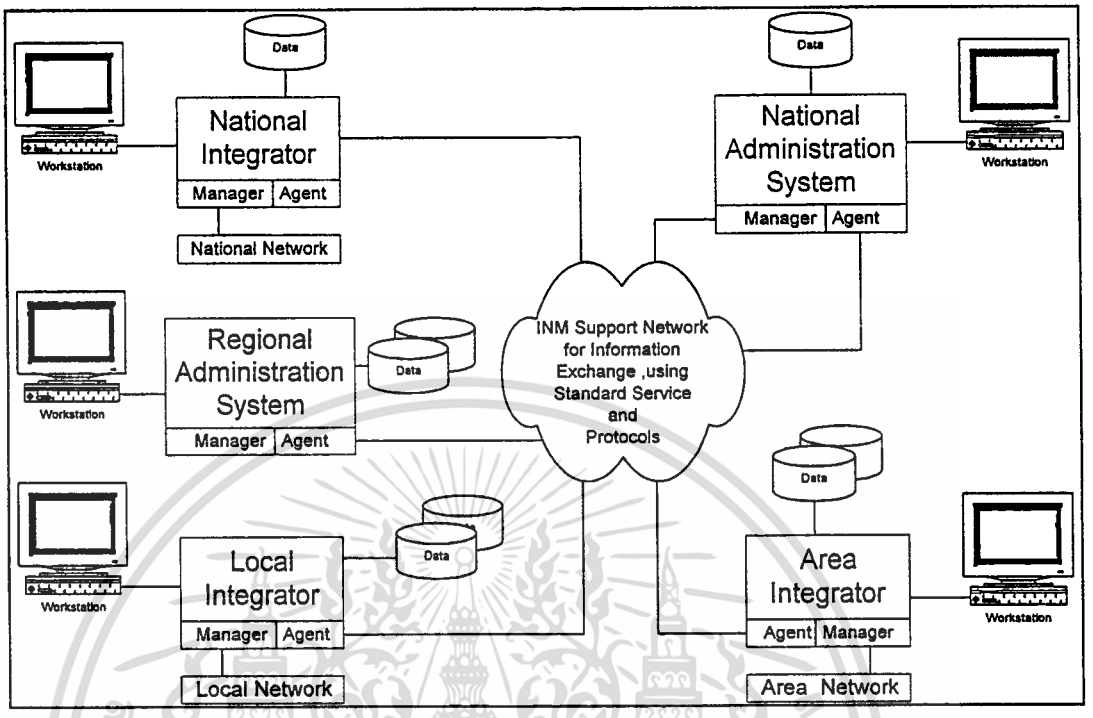
รูปที่ 3.13 แสดงสถาปัตยกรรมการบริหารเครือข่ายแบบต่าง ๆ

ตั้งแต่ 1980 สถาปัตยกรรมการบริหารเครือข่ายเบื้องต้น 3 แบบถูกนำมาใช้ในอุตสาหกรรม

- แบบวันโซลูชั่น (One Solution) สถาปัตยกรรมนี้ทำการบริหารอุปกรณ์ทั้งหมดในเครือข่าย อย่างไรก็ตามแบบนี้ทำได้กับเครือข่ายที่ประกอบด้วยอุปกรณ์ที่มีการเชื่อมต่อมาตรฐานกับตัวบริหาร
- แบบลำดับขั้นของผู้จัดการ (Hierarchical Manager of Managers) สถาปัตยกรรมแบบนี้อยู่บนความคิดที่ว่าการมีผู้จัดการเฉพาะเพิ่มอยู่ระหว่างผู้จัดการรวมที่อยู่ในระดับสูงกับกลุ่มของอุปกรณ์ธรรมดาในเครือข่าย วิธีนี้ใช้กันมากกว่าแบบวันโซลูชั่นแต่ก็ยังขึ้นอยู่กับผู้จัดการเพียงเครื่องเดียว
- แบบการบริหารร่วม(Cooperative Management) สถาปัตยกรรมนี้อยู่บนพื้นฐานของการบริหารแบบปลายซึ่งผู้จัดการหลายๆตัวสามารถใช้ร่วมกันได้ทั้งการบริการปกติและข้อมูล
- สถาปัตยกรรมการบริหารร่วมเป็นแบบที่เหมาะสมที่สุดในการบริหารเครือข่ายแบบหลากหลายเนื่องจากเครือข่ายมีขนาดใหญ่และมีแมนเนจเมนท์โดเมน (Managment Domain)มากซึ่งต้องการการใช้ข้อมูลร่วมกันและทำงานร่วมกัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.13.3 ภาพรวมของสถาปัตยกรรมการบริหารเครือข่ายแบบรวม

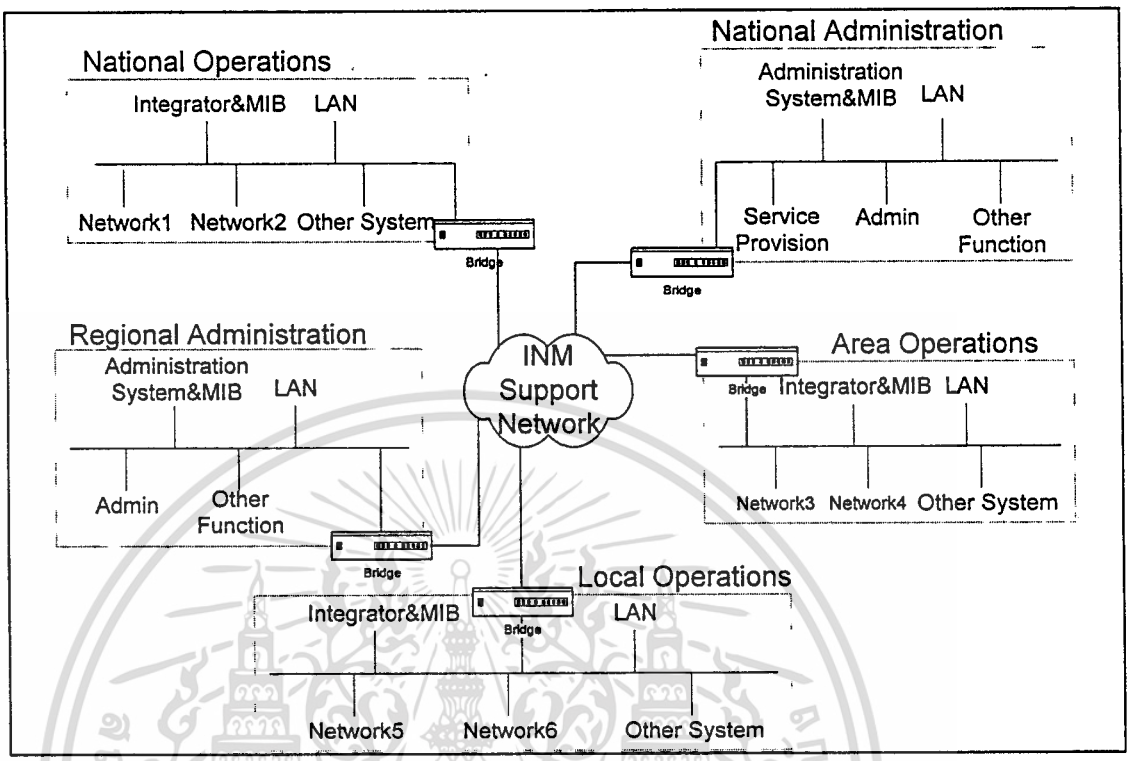


รูปที่ 3.14 แสดงภาพรวมของสถาปัตยกรรมการบริหารเครือข่ายแบบรวม

จากรูปแสดงให้เห็นสถาปัตยกรรมจากมุมมองระดับสูงซึ่งมองเห็นส่วนประกอบหลักและคุณสมบัติ ซึ่งแสดงว่าสถาปัตยกรรมนี้ทำงานโดยความต้องการของทำงานแบบเรียลไทม์ของระบบย่อยและเครือข่ายย่อยที่ตรวจสอบและควบคุมโดยมีการวิเคราะห์ระบบการบริหารที่กระจายในที่ที่ต่างกัน แต่ละแมนเนจเมนต์โดเมนก็แสดงโดยกล่องที่แรเงาที่มีผู้จัดการและเอเจ้นต์ท์ ระบบที่อยู่ในแต่ละโดเมนจะถูกตรวจสอบและควบคุมผ่านการเชื่อมต่อของผู้จัดการไปยังแต่ละระบบย่อย ซึ่งแต่ละโดเมนจะมีMIBเป็นของตัวเองซึ่งมีข้อมูลของทรัพยากรในส่วนที่ตัวเองดูแล ข้อมูลจะใช้ร่วมกันระหว่างโดเมนการบริหารตามคำจำกัดความของมาตรฐานสำหรับออบเจ็คต์ข้อมูลที่อยู่บนพื้นฐานของOSIและมาตรฐานอื่นๆ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.13.4 การบริหารเครือข่ายแบบรวมที่ขึ้นอยู่กับสถาปัตยกรรมของเครือข่ายระยะใกล้



รูปที่ 3.15 แสดงการบริหารเครือข่ายแบบรวมที่ขึ้นอยู่กับสถาปัตยกรรมเครือข่ายระบะใกล้

สถาปัตยกรรมนั้นขึ้นอยู่กับลำดับของโดเมนการบริหารเครือข่ายการเชื่อมต่อ ในโดเมนระดับแรก(เช่น แอเรีย) ระบบย่อย, เวิร์คสเตชั่น และเซิร์ฟเวอร์ก็รองรับหน้าที่ของSMIซึ่งติดต่อโดยใช้ระบบเครือข่ายระยะใกล้อีเธอร์เนต การเชื่อมต่อระหว่างแอเรียโดเมนกับโดเมนการบริหารอื่นๆ ทำได้ที่ระดับชั้นการเชื่อมต่อโดยใช้บริดจ์ระยะไกลบนเครือข่าย แพ็กเก็ตสวิชชิ่ง สถาปัตยกรรมนี้มีประโยนช์ 2 ด้านคือ ง่ายต่อการขยายและส่วนใหญ่สามารถติดตั้งได้โดยส่วนประกอบแบบ COTS บริดจ์ระยะไกลนั้นราคาถูกและมีประสิทธิภาพสูงซึ่งให้โดยผู้ผลิต ในความยืดหยุ่นถ้าระบบย่อยใหม่ถูกสร้างซึ่งจะเป็นโดเมนย่อยภายในโดเมนพื้นฐานที่มีอยู่ สถาปัตยกรรมทั้งหมดไม่มีผลกระทบ ดังนั้นถ้าภาระในการทำงานสำหรับการประมวลผลการบริหารต้องการการเพิ่มของความสามารถในการประมวลผลเพิ่ม เวิร์คสเตชั่นสามารถเพิ่มหรืออัพเกรดโดยไม่มีผลกระทบต่อเครือข่ายที่มีอยู่

การบริหารเครือข่ายแบบรวมต้องการฐานข้อมูลที่มีการพัฒนาซึ่งเป็นปกติของระบบส่วนใหญ่ ฐานข้อมูลประกอบด้วย ข้อมูลการติดตั้ง, การแจ้งเตือน, เหตุการณ์, ข้อมูลประสิทธิภาพ, ข้อมูลการบัญชี และออบเจ็คต์อื่นๆ การเก็บข้อมูลของข้อมูลที่สำคัญในการบริหารเครือข่ายใช้เทคนิคการจำลองข้อมูลแบบออบเจ็คต์โอเรียนเต็ด MIBประกอบไปด้วยข้อมูลเกี่ยวกับออบเจ็คต์ที่

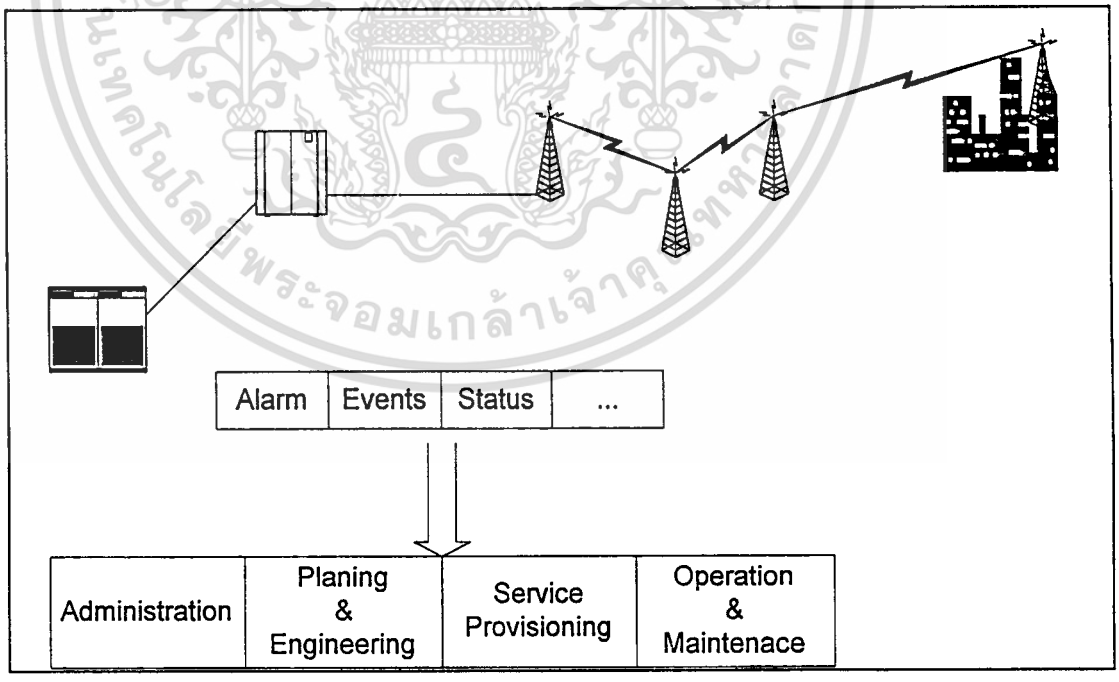
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ถูกจัดการและคุณลักษณะของออบเจ็คต์และค่าคุณลักษณะที่เกี่ยวข้อง การใช้MIBเป็นฐานของเครือข่ายทั่วๆไปจะถูกพัฒนาโดยใช้แผนภาพ E-R (entity-relationship) เพื่อแสดงภาพด้านระดับสูงของกลุ่มของออบเจ็คต์แบบจำลอง E-R นี้จะระบุทรัพยากรทั่ว ๆ ไปเช่น วงจร, อุปกรณ์ และ คุณสมบัติหรือคุณลักษณะที่เกี่ยวข้อง

3.13.4.1 การสร้าง MIB

การระบุกลุ่มของออบเจ็คต์ใช้ในการสร้างลำดับชั้นของการเก็บซึ่งอธิบายเครือข่าย เครือข่ายที่ใหญ่และซับซ้อนจะทำให้เกิดโครงสร้างลำดับชั้นที่ละเอียด โดยใช้ออบเจ็คต์ที่ต้องการจำนวนมากและการเชื่อมต่อระหว่างออบเจ็คต์ที่เลือก ความพยายามที่จะใช้ฐานข้อมูลแบบรีเลชั่นนอลในการแสดงและใช้โครงสร้างเป็นผลมาจากแอปพลิเคชั่นที่ช้าและยุ่งยาก นอกจากนั้นรูทีนจำนวนมากและหน้าที่ในการควบคุมที่ใช้บ่อยๆ เช่น การค้นหาข้อมูลของต้นไม้ของลำดับชั้นการเก็บ (containment hierarchy tree) ยากต่อการทำโดยใช้รีเลชันนอลพาราไดม (relational paradigm) ผลิตภัณฑ์ฐานข้อมูลแบบออบเจ็คต์โอเรียนเตดที่ใช้แทน ฐานข้อมูลชนิดนี้ให้ผลตอบสนองที่ดีกว่าและง่ายต่อการควบคุมออบเจ็คต์

3.13.4.2 ส่วนติดต่อกับผู้ใช้



รูปที่ 3.16 แสดงการนำข้อมูลมาแสดงให้กับผู้ใช้ผ่านทาง GUI

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ผู้บริหารเครือข่ายจะรับผิดชอบการแสดงหน้าที่ในระยะไกลของการปฏิบัติการและการบริหารเครือข่าย ซึ่งเราก็ต้องควบคุมข้อมูลเดียวกันจำนวนมากและเราเกี่ยวข้องกับเครือข่ายเดียวกันนี้บ่อยๆและไม่ผิดปกติที่ผู้ที่ทำการบริหารที่จะทำหน้าที่ซึ่งข้ามขอบเขตหน้าที่ ตัวอย่าง ผู้บริหารเครือข่ายที่ทำหน้าที่การวางแผนซึ่งอาจเป็นคนเดียวกันกับคนที่ทำด้านวิศวกรรม ผู้บริหารจะได้ผลประโยชน์จากGUIเนื่องจากที่ใช้ในปัจจุบันนั้นง่ายไม่ซับซ้อนและมีการเชื่อมแบบกราฟฟิกที่สะดวกใช้งานได้ง่าย GUIโดยปกติจะลดเวลาการฝึกหัดและให้ความรู้สึกและมองเห็นว่าถูกต้องของข้อมูล ,เครื่องมือ และแอพพลิเคชั่น ที่ต้องการในการบริหารเครือข่าย

ผลิตภัณฑ์ใหม่สำหรับการบริหารเครือข่ายมีแนวโน้มที่จะพัฒนาบนแพลตฟอร์มของเครื่องเวิร์คสเตชั่นที่ใช้ กราฟฟิก และระบบวินโดว์เบส(windows-base) ผู้ผลิตหลายๆรายจะใช้แพลตฟอร์ม UNIX กับมาตรฐานระบบกราฟฟิก X windows ที่ยอมให้เครื่องเวิร์คสเตชั่นทำการทำงานบนเครือข่าย

3.13.5 ข้อสรุปของการพัฒนาสถาปัตยกรรมแบบINM

จากการศึกษาก็พบว่ามีข้อสรุปพื้นฐาน 3 ข้อคือ

- การพัฒนาต้นแบบของข้อมูลเป็นรูปแบบหนึ่งของการเริ่มที่จะเพิ่มความสำคัญแก่ความต้องการของการบริหารเครือข่ายแบบรวม การใช้กลุ่มต้นแบบของออบเจ็คต์มาตรฐานที่มีอยู่จะทำให้มีการเริ่มต้นที่เร็ว กลุ่มมาตรฐานของออบเจ็คต์สามารถทำและปรับปรุงเป็นภาวะแวดล้อมขององค์กรโดยการใช้ออบเจ็คต์เพิ่มเติม (additional object) หรือโดยซับคลาสออบเจ็คต์ (subclass object) ในเครือข่ายขนาดใหญ่ที่มีความหลากหลายจะมีลำดับขั้นของ MIB ที่ใหญ่และซับซ้อน โดยพิจารณาการใช้ฐานข้อมูลแบบออบเจ็คต์โอเรียนเต็ดซึ่งสามารถให้ประสิทธิภาพสูงและการควบคุมความจุแบบลำดับขั้นซึ่งไม่มีในระบบการบริหารฐานข้อมูลอื่น
- ในแนวโน้มของอุตสาหกรรม เชื่อได้ว่าสถาปัตยกรรมการบริหารเครือข่ายแบบร่วม(cooperative)ที่ใช้มาตรฐาน OSI จะมีความสำเร็จในภาวะแวดล้อมของเครือข่ายขนาดใหญ่ที่มีความหลากหลาย ผลิตภัณฑ์ OSI จะถูกวางแผนและพัฒนาโดยผู้ผลิตจำนวนมาก ซึ่งเป็นผลิตภัณฑ์ที่องค์กรจัดหาและใช้งานในการบริหารเครือข่าย
- นอกจากนั้นผู้ใช้ก็จะพัฒนาความสามารถของการบริหารเครือข่ายที่ใช้บนเวิร์คสเตชั่นแบบ UNIX ก็จะพบว่าการบริหารเครือข่ายเป็นปัญหาใหญ่ซึ่งด้านอุตสาหกรรมยังคงต่อสู้อยู่ ไม่มีการทำงานภายในครั้งเดียวที่จะเปลี่ยนจากแบบรวมศูนย์ (autocracy) เป็น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แบบกระจาย (harmony) จึงต้องการการทำแบบขั้นตอน (phase approch) กับกลุ่มย่อยของปัญหาของการบริหารเครือข่ายที่มีอยู่ ดังนั้นในการที่จะเพิ่มความเข้าใจของความต้องการ และการออกแบบผลิตภัณฑ์นั้นต้นแบบควรทำก่อนเพื่อให้ผู้ใช้ตรวจสอบและแก้ไข ก่อนที่จะนำไปพัฒนาเป็นต้นแบบที่ใช้งานซึ่งจะนำมาใช้งานจริงต่อไป

3.14 การบริหารระบบเครือข่ายมาตรฐานที่เป็นแบบมัลติเวนเดอร์ (Standardized Multivendor Network Management)

3.14.1 สิ่งที่ต้องการสำหรับการบริหารเครือข่ายระยะใกล้

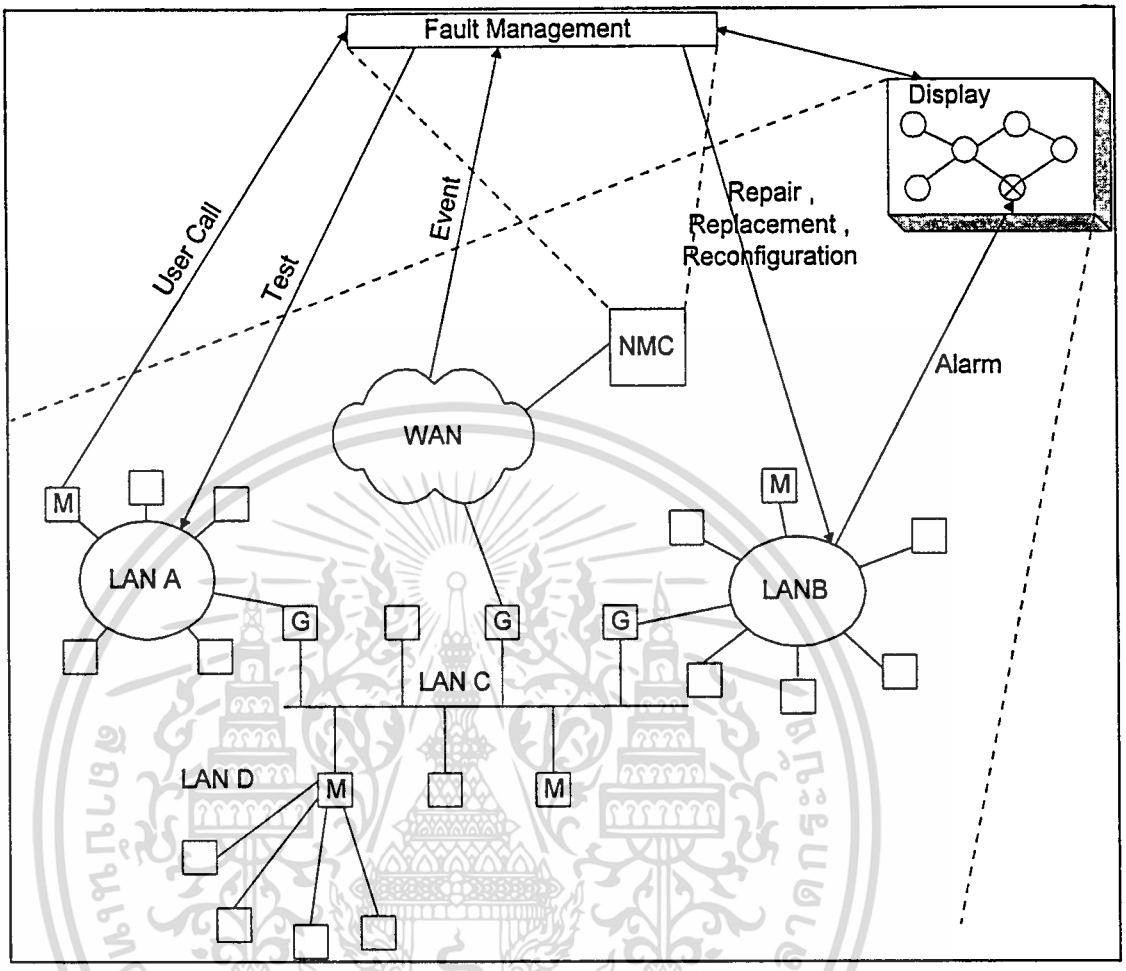
- การบริการของผู้ใช้ได้มีการเจริญเติบโตและมีการเปลี่ยนแปลงเทคโนโลยีโดยไม่มีการเพิ่มของผู้ควบคุม
- ความสามารถในการแก้ไข bypass หรือ circumvent เซิร์ฟเวอร์ของเครือข่ายระยะใกล้หลังจากมีการพบ และทำการหาปัญหาโดยอัตโนมัติ
- ความสามารถในการทำงานเมื่ออุปกรณ์ในการเชื่อมต่อเสียหาย
- การรวมตัวของการบริหารด้าน configuration กับ fault โดยการใช้ configuration database รวมกับความสามารถของ CAD
- การติดต่อกับผู้ใช้โดยตรงโดยใช้กราฟฟิกซึ่งก็คือ GUI(Graphical User Interface)
- การรวมตัวด้านนอนและด้านตั้งโดยใช้การแก้ไขปัญหาจากระบบการบริหารที่มีการเรียงเป็นลำดับขั้นและหน้าที่ของแพลตฟอร์มของการบริหารเครือข่าย
- ผลลัพธ์ที่เพิ่มขึ้นโดยการทำการตรวจสอบจากระยะไกล, การควบคุม, การบริหารโดยอุปกรณ์แบบศูนย์กลาง
- การเปลี่ยนอุปกรณ์ที่เฉพาะเป็นแอปพลิเคชั่นทั่วไปซึ่งทำหน้าที่การบริหารได้หลายหน้าที่ เช่น การบริหารด้านประสิทธิภาพ, configuration, fault, accouting, security
- การมีอยู่ของข้อมูลด้านสถิติและประวัติซึ่งเก็บในฐานข้อมูลประสิทธิภาพหรือสถิติ
- การเห็นการวัดประสิทธิภาพของเครือข่ายระยะใกล้ที่สำคัญแบบเรียลไทม์ เช่น การติดขัดของข้อมูล, การใช้งานของอุปกรณ์, จำนวนของการส่งและปฏิเสธเฟรมข้อมูล, เวลาในการส่งข้อมูลและระยะเวลาหน่วงขณะทำการเข้าใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- การบริหารที่เปลี่ยนแบบยืดหยุ่นสำหรับผลตอบสนองที่รวดเร็วและต่อเนื่องกับการเปลี่ยนแอปพลิเคชั่นในระบบเครือข่ายระยะใกล้, อุปกรณ์, การบริการ, ค่าที่กำหนด และคำอธิบาย
- การบำรุงรักษาฐานข้อมูลของ config ของเครือข่ายระยะใกล้ที่มีค่า attribute , ข้อมูลการเชื่อมต่อและการวัดสถานะแบบไดนามิก
- การทำงานแบบอัตโนมัติ, การแจ้งเตือนและวิเคราะห์อัตโนมัติ, การใช้การกรอง และ โปรซีเดอร์การบริหารด้านความผิดพลาด
- แพลตฟอร์มของการบริหารเครือข่ายระยะใกล้ที่มีความสามารถสูงสำหรับรองรับการแก้ไขปัญหาเมื่อมีการพบ, ประมาณค่าปัญหา
- ความสามารถที่จะใช้การตรวจสอบจากระยะไกลซึ่งรองรับทั้งเทคนิคการเชื่อมต่อแบบอินแบน (inband) และ เอาท์แบน (outband)
- โอเวอร์เฮดในการตรวจสอบมีค่าต่ำโดยการปรับแบบ ไดนามิกของอัตราการ พูลลิ่งสำหรับการใช้งานทรัพยากรปกติ
- การใช้มาตรฐานของเครือข่ายระยะใกล้ซึ่งใช้กันโดยทั่วไปและรองรับโดยผู้ผลิตส่วนใหญ่ เช่น SNMP ,CMIP ,CMOT ,CMOL

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.14.2 การทำงานของการบริหารด้านความผิดพลาด



รูปที่ 3.17 แสดงกระบวนการการทำงานของการบริหารด้านความผิดพลาด

การบริหารด้านความผิดพลาดเป็นการเก็บการกระทำที่ต้องการสำหรับระดับการบริหารเครือข่ายแบบ ไดนามิก ซึ่งการกระทำดังกล่าวจะต้องหาได้ โดยการเข้าใจปัญหาอย่างรวดเร็วและการลดลงของประสิทธิภาพ และโดยทำการเริ่มการควบคุมหน้าที่เมื่อจำเป็นซึ่งรวมถึง วิเคราะห์, ซ่อมแซม, ทดสอบ, แก้ไข และสำรองข้อมูล และการควบคุมล็อก (log) และเทคนิคการกระจายข้อมูลก็เช่นเดียวกัน

เหตุการณ์แบบโซลิสิต (Solicited) และอันโซลิสิต (Unsolicited) ช่วยในการตรวจพบการทำงานที่ผิดปกติ โดยปกติปัญหาดังที่กล่าวมานั้นมักจะมีการสร้างข้อความเป็นจำนวนมากในแบบอันโซลิสิต ถ้าข้อความเหล่านี้ไม่ได้กรองแล้วการทำงานของเครือข่ายระยะใกล้ก็จะมีการทำงานมากเกินไป ในขั้นแรกจะทำการกำจัดข้อความที่ไม่เกี่ยวข้อง ขั้นที่สองนำเอาข้อความที่เกียวข้องนั้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

มาระบุเหตุการณ์ และสุดท้ายเหตุการณ์จะถูกให้ค่าความสำคัญและค่าเทรชโฮล โดยความรุนแรงของเทรชโฮลและการเกิดขึ้นของเหตุการณ์ที่มีความสำคัญจะทำให้เกิดการแจ้งเตือน ในการบริหารเครือข่ายระยะใกล้ล็อกก็จะถูกเริ่มต้นโดยระดับของเหตุการณ์

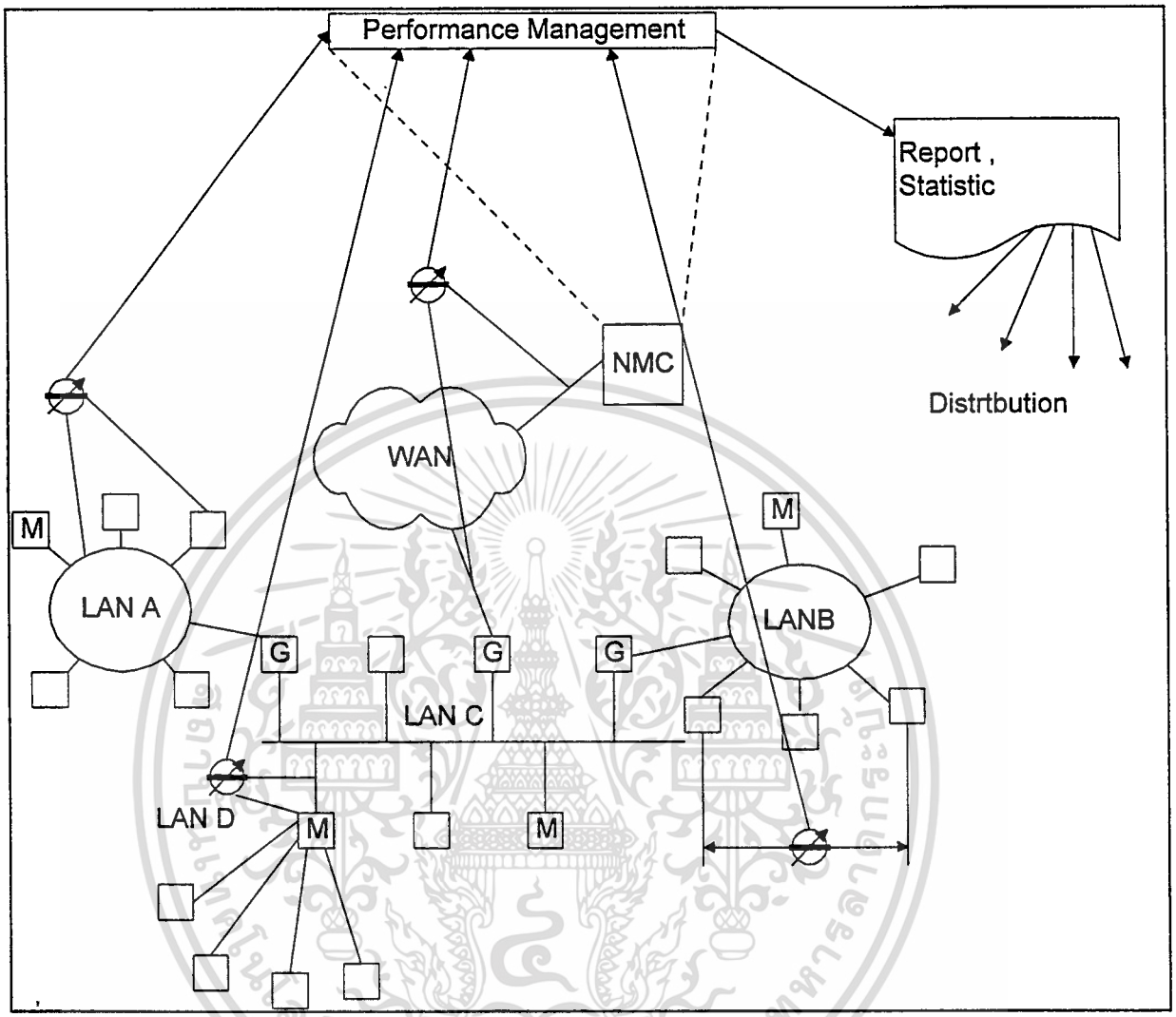
ขั้นตอนการสร้างการแจ้งเตือนนั้นถูกทำในเครือข่ายระยะใกล้โดยผู้บริหารเครือข่ายระยะใกล้ในพื้นที่นั้นๆ เช่นระบบการบริหารเครือข่ายในระดับของผู้จัดการเอสเอ็นเอ็มพี การที่ขึ้นอยู่กับความซับซ้อนและขนาดของเครือข่ายระยะใกล้ซึ่งการบริหารเหตุการณ์สามารถทำงานที่มีความยืดหยุ่นได้สูง

3.14.3 การแสดงสถานะของเครือข่าย

MIB เป็นที่เก็บข้อมูล เสมือนที่เก็บไว้ในอุปกรณ์ที่จะบริหารซึ่งรู้กันโดยทั่วกันว่า SNMP เอเจ้นต์ท์ ฐานข้อมูลนี้สร้างจากออบเจ็คต์ที่ประกอบไปด้วย ชื่อ ,ไวยากรณ์ และข้อมูลที่เข้ารหัสไว้ ชื่อนั้นเรียกว่าออบเจ็คต์ไอเดนติฟายเออร์ (Object Identifier) และเป็นชื่อเฉพาะสำหรับออบเจ็คต์หนึ่งๆไวยากรณ์นั้นหมายถึงค่าที่แสดงเช่นเลขจำนวนของแพกเก็ตที่ส่ง ประเภทของไวยากรณ์รวมถึง ค่าเคาท์เตอร์, ค่าเกจ (gauge), ข้อความของออบเจ็คต์ (object string), ค่าเน็ตเวอร์คแอดเดรส และค่าตัวเลข MIB II ระบุประเภทใหม่ของข้อความของออบเจ็คต์เรียกว่าข้อความของการแสดง (display string) ซึ่งยอมให้ข้อความของข้อมูลนั้นแสดงแก่ผู้ใช้โดยไม่ต้องมีการประมวลผลข้อความนั้นโดยระบบการบริหาร กระบวนการการเข้ารหัสจะเปลี่ยนแมชชีนโค๊ดเป็นภาษาอังกฤษ ซึ่งยอมให้ผู้เขียนโปรแกรมและผู้บริหารเครือข่ายทำการอ่านข้อมูลจากที่เครื่องที่ทำการบริหารเครือข่ายเก็บได้ MIBได้ใช้มาตรฐาน ASN.1 กฎการเข้ารหัสข้อมูลเบื้องต้น ข้อกำหนดของการเข้ารหัสที่เกี่ยวกับออบเจ็คต์คือการออกแบบอ่านได้อย่างเดียว, อ่าน-เขียน, เขียนอย่างเดียว หรือไม่สามารถเข้าถึง นอกจากนั้นข้อมูลสถานะก็ระบุเกี่ยวกับออบเจ็คต์ คือ แมนดาทอรี่ (mandatory), ออปชันนอล (optional), ออปโซเลต (obsolete) และ ดีครีเมนท์ (decremented) SNMP ที่ประกอบจากMIB II มีออบเจ็คต์ไอเดนติฟายเออร์ใหม่ที่ให้ข้อมูลทางสถิติเกี่ยวกับประสิทธิภาพของเครือข่ายแก่ผู้บริหารเครือข่าย ออบเจ็คต์ยอมให้ระบบการบริหารเครือข่ายทำการหาปริมาณของการจราจรของการบริหารที่มีการตอบสนองโดยอุปกรณ์ ค่าตัวแปรเช่น ค่าของจำนวนแพกเก็ตของเอสเอ็นเอ็มพีที่เข้าและออกจากอุปกรณ์, จำนวนของแพกเก็ตที่มีชื่อคอมมิวนิตี้ (community name) ผิด, จำนวนของแพกเก็ตที่ไม่ได้อยู่ในรูปของมาตรฐาน ASN.1 และจำนวนทั้งหมดของการร้องขอสำหรับข้อมูลที่ให้โดยเอสเอ็นเอ็มพี การมีข้อมูลชนิดนี้อยู่ทำให้ความสำคัญเพิ่มขึ้นในด้านขนาดและความซับซ้อนของเครือข่ายที่เพิ่มขึ้นอย่างมาก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.14.4 การทำงานของการบริหารด้านประสิทธิภาพ



รูปที่ 3.18 แสดงกระบวนการการทำงานของการบริหารด้านประสิทธิภาพ

การบริหารด้านประสิทธิภาพเป็นการประมาณค่าของเครือข่ายซึ่งประโยนช์เพื่อจะตรวจสอบว่าระดับการบริการใดที่จะต้องบำรุงรักษา, ระบุบอทเทิลเนค (Bottle neck) และทำการสร้างและรายงานแนวโน้มสำหรับการตัดสินใจและวางแผนในการบริหาร การสร้างและบำรุงรักษาฐานข้อมูลประสิทธิภาพของเครือข่ายระยะใกล้และโพรซีเดอร์อัตโนมัติสำหรับการบริหารเครือข่ายระยะใกล้ด้านความผิดพลาดก็ถูกรวมไว้ด้วยเช่นกัน

หลักการระบุการบริหารเครือข่ายระยะใกล้

- การใช้งานของทรัพยากร หน่วยประมวลผล ,หน่วยความจำ ,สื่อการสื่อสาร และในบางกรณีอุปกรณ์เชื่อมต่อทั้งหมดก็ถูกรวมในการทำงานที่ผู้ใช้ร้องขอ มีการใช้ความจุ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ที่มีอยู่เท่าไรและมีการสำรองเท่าไรเพื่อนำเอาข้อมูลใช้สำหรับการประมาณพร้อมกับการประมวลผลข้อมูล

- การหน่วงของการประมวลผล การร้องขอของผู้ใช้จะทำให้มีการหน่วงที่แต่ละการประมวลผลทั้งโฮสท์และเครือข่ายก็สามารถเป็นสาเหตุในการหน่วงของการประมวลผล การหน่วงของเครือข่าย เนื่องจากฮาร์ดแวร์และซอฟท์แวร์ อย่างไรก็ตามที่ระดับผู้ใช้การหน่วงของการประมวลผลทั้งหมด (เวลาการตอบสนอง) เป็นเพียงความหมายของประสิทธิภาพ
- ประสิทธิภาพโดยรวม (Troughput) ความจุในการส่งสามารถวัดได้ในรูปของประสิทธิภาพโดยรวม เป็นจำนวนของการส่งข้อความหรือไบท์ต่อหน่วยเวลา ในการวัดเครือข่ายระยะใกล้ประสิทธิภาพโดยรวมเป็นตัววัดการกระจายของความจุของเครือข่ายที่ใช้ในการส่งข้อมูล

3.14.5 การกระทำแบบลำดับขั้นสำหรับการรวม

ในลำดับแรกคือการกระทำแบบลำดับขั้น (manager of managers approch) ซึ่งก็คือการกระทำแบบลำดับขั้นที่ผู้จัดการรวมทำการติดต่อกับระบบการบริหารที่อยู่ในชั้นล่างในลำดับที่สอง การกระทำคือการกระทำของแพลตฟอร์ม (platform approch) ซึ่งผู้ผลิตต่างๆเขียนแอปพลิเคชั่นการบริหารเครือข่ายเป็นกลุ่มของ APIs

3.14.6 การกระทำของแพลตฟอร์มสำหรับการรวม

การกระทำของแพลตฟอร์มต่อการบริหารแบบรวมทำให้เกิดความเป็นไปได้ของการการรวมของผู้ผลิตหลายรายมากกว่าวิธีแมนแนเจอร์ออฟแมนแนเจอร์ในสถาปัตยกรรมแบบแมนแนเจอร์ออฟแมนแนเจอร์การติดต่อสื่อสารระหว่างระบบการบริหารจากผู้ผลิตที่ต่างกันนั้นกระทำผ่านการเชื่อมต่อของโปรโตคอลที่เป็นมาตรฐานและชุดที่มาตรฐานของคำจำกัดความของข้อมูลการบริหารในวิถีทางแบบลำดับขั้นของของข้อมูลการบริหารที่รวมกันนี้ต้องการผู้ผลิตคนเดียว (ผู้ผลิตของตัวรวม) พัฒนาซอฟท์แวร์แอปพลิเคชั่นการบริหารเครือข่ายของผู้ผลิตหลายรายทั้งหมด ผู้ผลิตอื่นๆทำหน้าที่ให้ข้อมูลดิบแก่ผู้บริหารรวมที่มีการเชื่อมต่อแบบเปิดและยอมรับคำสั่งผ่านการเชื่อมต่อระบบเปิดนั้นโดยอิสระแล้วการกระทำแบบแมนแนเจอร์ออฟแมนแนเจอร์หรือแบบแพลตฟอร์มจุดมุ่งหมายคือการบริหารของผู้ผลิตหลายราย ผู้ผลิตจะรองรับ proprietary, de facto หรือมาตรฐานแบบเปิดที่ออบเจ็คต์ที่บริหารหรือระดับแอปพลิเคชั่นการบริหาร การติดต่อข้ามผ่านเกตเวย์ (พรอกซี่เอเจ้นต์ท์) ก็ต้องการการรองรับเช่นกัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.14.7 ต้นแบบของเครื่องมือรวม

มาตรฐานการบริหารเครือข่ายระยะใกล้ช่วยในการสร้างหน้าที่และเลือกเครื่องมือได้เร็วขึ้น พื้นที่การทำงานของแอปพลิเคชั่นการบริหารที่เฉพาะซึ่งรองรับโดยหน้าที่ของการบริหารระบบและโดยข้อมูลการบริหารที่บริการส่วนประกอบในเครือข่ายที่ถูกระบุอย่างชัดเจนโดยISO ที่ทำบนเครือข่ายระยะใกล้ที่ขึ้นอยู่กับว่ามาตรฐาน de facto ที่มีอยู่ การบริหารเครือข่ายของOSIจะรวมการบริหารเครือข่ายระยะใกล้ ส่วนด้านเอสเอ็นเอ็มพีแนวโน้มนี้จะคาดหวังว่าจะเกิด

- การรองรับระดับเอสเอ็นเอ็มพีเอเจ้นต์จะมีโดยผู้ผลิตจำนวนมาก
- การรองรับระดับผู้จัดการ เอส เอ็น เอ็ม พี จะมีโดยบางผู้ผลิต ซึ่งสามารถสร้างบนแพลตฟอร์ม ที่ยอมรับกันโดยทั่วไปโดยละทิ้งการปรับปรุงและการพัฒนาของ แอพพลิเคชั่น เพิ่มเติมสำหรับผู้ผลิตและผู้ใช้
- นำสู่การผลิตผลิตภัณฑ์เครื่องมือรวมของการบริหารเครือข่ายเช่น เน็ตวิว, โอเพ่นวิว, เดคเอ็มซีซี ที่ยอมให้ผู้ผลิตทำการติดต่อผู้จัดการเอสเอ็นเอ็มพีของตนเองกับเครื่องมือรวม
- การแข่งขันของผลิตภัณฑ์ผู้จัดการเอสเอ็นเอ็มพีและแพลตฟอร์มที่มีความสำคัญมาก
- พื้นที่ส่วนตัวของMIBที่คาดว่าจะเคลื่อนตัวอย่างช้าๆไปยังพื้นที่สาธารณะและรองรับการ บริหารระบบเครือข่ายระยะใกล้แบบแตกต่างบนพื้นฐานเอสเอ็นเอ็มพี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4

ระบบความปลอดภัยของระบบเครือข่าย

4.1 การใช้ไฟร์วอลล์ (Firewall) ในการระบบรักษาความปลอดภัยในเครือข่าย

ในสมัยก่อนจะมีกำแพงอิฐที่สร้างขึ้นมากั้นระหว่างอาคาร เพื่อว่าเวลาเกิดไฟไหม้ขึ้นมาจะได้ป้องกันไม่ให้ลุกลามไปยังอาคารอื่น ๆ โดยธรรมชาติของตัวมันเองก็เลยถูกเรียกว่า ไฟร์วอลล์

ในเครือข่ายที่ทันสมัยทุกวันนี้ เช่น อินเทอร์เน็ต สามารถใช้วิธีในทำนองเดียวกันในการป้องกันทรัพยากรที่มีค่าของเครือข่ายจากอันตราย (Fire) ซึ่งจะเป็นผลให้พ่ายแพ้ในการแข่งขันทางธุรกิจหรือเกิดความเสียหายอย่างร้ายแรงต่อข้อมูลที่สำคัญ อุปกร์ที่ปกป้องเครือข่ายและทรัพยากรในเครือข่ายให้รอดพ้นจากไฟร์ภายนอกกำแพง (Walls) ของเครือข่ายก็คือ ไฟร์วอลล์

ไฟร์วอลล์ (FIREWALL) เป็นรูปแบบของระบบการรักษาความปลอดภัยของการติดต่อระหว่างเครื่องคอมพิวเตอร์เครื่องหนึ่ง ๆ กับเครือข่ายภายนอก โดยถือหลักว่า เครื่องคอมพิวเตอร์หรือเครือข่ายที่เราใช้งานอยู่จะต้องเป็นระบบที่เชื่อถือได้ ในขณะที่เครือข่ายภายนอกจะเป็นเครือข่ายที่ไม่สามารถเชื่อถือได้ จึงต้องใช้ไฟร์วอลล์มาเป็นตัวควบคุม ตรวจสอบการติดต่อกับระบบภายนอก

4.1.1 จุดประสงค์ของการมีไฟร์วอลล์

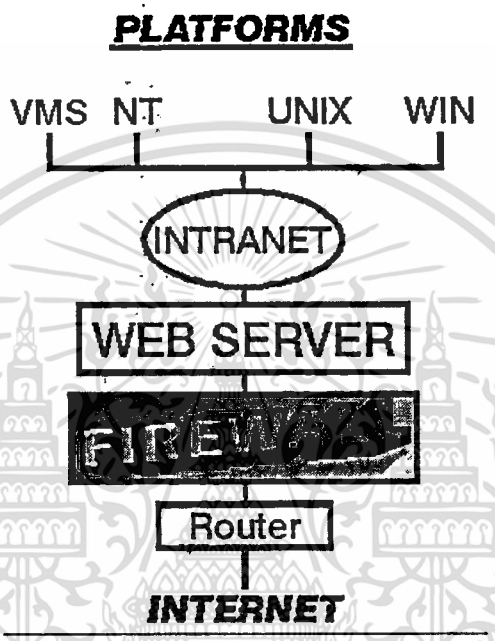
จุดประสงค์หลักของไฟร์วอลล์ก็คือ การป้องกันระบบหนึ่งจากระบบอื่น ๆ ที่อยู่ภายนอก โดยระบบที่ใช้งานอยู่จะเป็นระบบที่เราเป็นคนควบคุมดูแลเอง เพราะฉะนั้นจึงสามารถเชื่อถือในเรื่องความปลอดภัยในการใช้งาน และการส่งผ่านของข้อมูลได้ ในขณะที่ระบบภายนอกเป็นระบบที่เราไม่ได้ดูแลด้วยตัวเอง จึงไม่สามารถเชื่อถือในความปลอดภัยได้

การป้องกันระบบดังกล่าวมาข้างต้นนั้น จะเกี่ยวข้องกับการป้องกันผู้ใช้ที่ไม่สิทธิ์เข้าใช้ระบบ ขณะเดียวกัน ก็ป้องกันการเข้าใช้ข้อมูลจากผู้ใช้ที่ไม่มีสิทธิ์ในการใช้ข้อมูลนั้น ๆ ด้วย และอนุญาตให้ผู้ที่มีสิทธิ์อย่างแท้จริงสามารถเข้าใช้ระบบได้อย่างเต็มที่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1.2 ที่ตั้งของไฟร์วอลล์

ไฟร์วอลล์จะวางอยู่ระหว่างระบบภายใน หรือ เน็ตเวิร์คภายในที่เชื่อใจได้ กับ เน็ตเวิร์คภายนอกที่ไม่สามารถเชื่อถือได้ ในที่นี้เครือข่ายที่เชื่อถือได้คือเครือข่ายอินทราเน็ตขององค์กรส่วนเครือข่ายที่ไม่น่าเชื่อถืออินเทอร์เน็ต ดังรูป



รูปที่ 4.1แสดงตำแหน่งของไฟร์วอลล์

4.1.3 องค์ประกอบของไฟร์วอลล์

องค์ประกอบของไฟร์วอลล์ประกอบด้วย

- สกรีนนิงเราท์เตอร์ (Screening routers)
- ดูออล-โฮสท์ (Dual-homed hosts)
- บาสชั่น โฮสท์ (Bastion host)
- แอพพลิเคชั่นเลเวลเกตเวย์ (Application level gateways)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1.4 สกรีนนิงเราท์เตอร์

เราท์เตอร์ในทางการค้าหลาย ๆ ตัวได้เตรียมความสามารถเพื่อสกรีนแพ็กเก็ตโดยใช้เงื่อนไข เช่น ชนิดของโปรโตคอล ฟิลด์แอดเดรสของผู้ส่งและผู้รับสำหรับโปรโตคอลบางประเภท และฟิลด์คอนโทรลซึ่งเป็นส่วนหนึ่งของโปรโตคอล เราท์เตอร์นี้เรียกว่า สกรีนนิงเราท์เตอร์

ผู้ขายเราท์เตอร์หลาย ๆ รายเรียกสกรีนนิงเราท์เตอร์ของพวกเขาว่าไฟร์วอลล์ พวกมันคือไฟร์วอลล์ในความหมายที่ว่าได้เตรียมการป้องกันสำหรับเครือข่ายภายในซึ่งอยู่บนพื้นฐานของข่าวสารที่เราท์เตอร์ต้องทำการประมวลผล เนื่องจากเราท์เตอร์ทำงานที่เลเยอร์ 3 ของโอเอสไอ (OSI) โมเดล ไฟร์วอลล์ชนิดนี้เตรียมการป้องกันบนพื้นฐานของข่าวสารบนเน็ตเวิร์คเลเยอร์ของโอเอสไอโมเดล

สกรีนนิงเราท์เตอร์จัดเตรียมกลไกที่มีประโยชน์เพื่อควบคุมประเภทของการจราจรบนเครือข่ายซึ่งสามารถเกิดขึ้นได้ในทุก ๆ เซกเม้นท์ของเครือข่าย โดยการควบคุมประเภทของการจราจรนี้ตัวสกรีนนิงเราท์เตอร์สามารถควบคุมประเภทของการบริการซึ่งสามารถมีอยู่บนเซกเม้นท์ของเครือข่าย ดังนั้นการบริการซึ่งสามารถยอมประนีประนอมกับความปลอดภัยของเครือข่ายก็สามารถที่จะถูกจำกัดได้

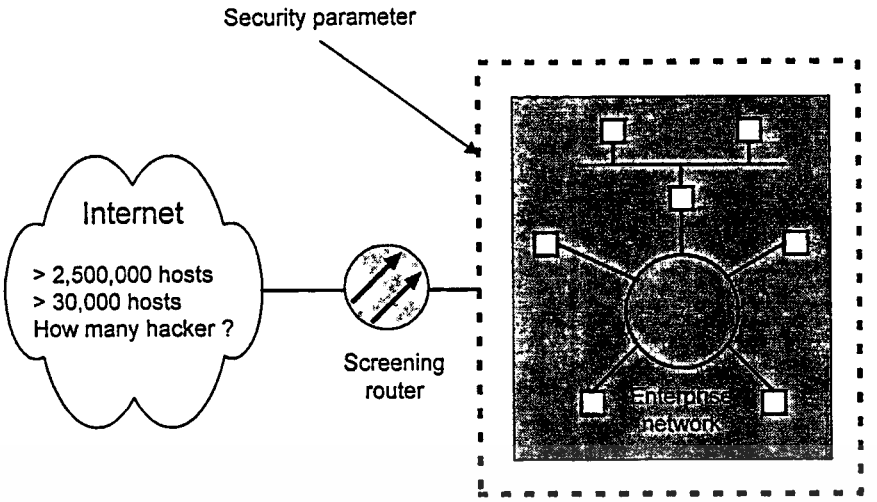
สกรีนนิงเราท์เตอร์สามารถรู้ความแตกต่างระหว่างการจราจรของเครือข่ายบนพื้นฐานของประเภทของโปรโตคอลและค่าของฟิลด์ของโปรโตคอลในแพ็กเก็ต ความสามารถในการแยกความแตกต่างของตัวเราท์เตอร์นี้และการได้จำกัดแพ็กเก็ตบนพอร์ทของมันโดยอาศัยเงื่อนไขพื้นฐานของประเภทโปรโตคอลที่เฉพาะเจาะจงนี้เรียกว่าแพ็กเก็ตฟิลเตอริ่ง (Packet filtering) ด้วยเหตุผลนี้เองสกรีนนิงจึงถูกเรียกอีกชื่อหนึ่งว่า แพ็กเก็ตฟิลเตอริ่งเราท์เตอร์ (Packet filtering router)

4.1.5 การระบุโซนที่มีความเสี่ยง (Identifying zones of risk)

จากรูป 4.2 แสดงตัวอย่างของการบริการแพ็กเก็ตฟิลเตอริ่งซึ่งอิมพลีเม้นท์โดยสกรีนนิงเราท์เตอร์ รูปนี้แสดงให้เห็นถึงเครือข่ายขององค์กรที่ต่อกับอินเทอร์เน็ตผ่านทางเราท์เตอร์ซึ่งทำแพ็กเก็ตฟิลเตอริ่ง

สถิติในปัจจุบันของอินเทอร์เน็ตแสดงให้เห็นว่ามันประกอบไปด้วยเครือข่ายมากกว่า 30,000 เครือข่ายเชื่อมต่ออยู่พร้อมด้วยผู้ใช้มากกว่า 2.5 โฮสท์ ด้วยการที่มีผู้ใช้เป็นจำนวนมากบนอินเทอร์เน็ต นั่นก็คือความโชคร้ายมีส่วนน้อยส่วนหนึ่งของผู้ใช้คือแฮคเกอร์ผู้ชั่วร้าย สถานการณ์แบบนี้เหมือนกันการเข้าไปในเมืองที่มีอาชญากรรมอยู่อย่างชุกชุม มันคือความฉลาดที่จะป้องกันที่อยู่อาศัยของคุณด้วยการล๊อคประตู ในความรอบคอบของคุณก็ยังไม่พอ ยังมีความ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.2 แสดงสกรีนนิงเราเตอร์สร้างรูปแบบพารามิเตอร์สำหรับความ

ต้องการอีกด้วยว่าถ้ามีใครมาเคาะประตูต้องสามารถตรวจสอบได้ว่าคนผู้คือใครก่อนที่จะอนุญาตให้เขาเข้ามาในบ้าน บุคคลผู้ที่เป็นอันตรายหรือดูแล้วไม่น่าไว้วางใจก็จะไม่ได้รับอนุญาตให้เข้ามา เพราะมีความเสี่ยงต่อความปลอดภัยสูง และในทำนองเดียวกันสกรีนนิงเราท์เตอร์ก็ตรวจสอบแพ็กเก็ตที่เข้ามาเพื่อตัดสินว่าอันไหนที่จะเป็นอันตราย

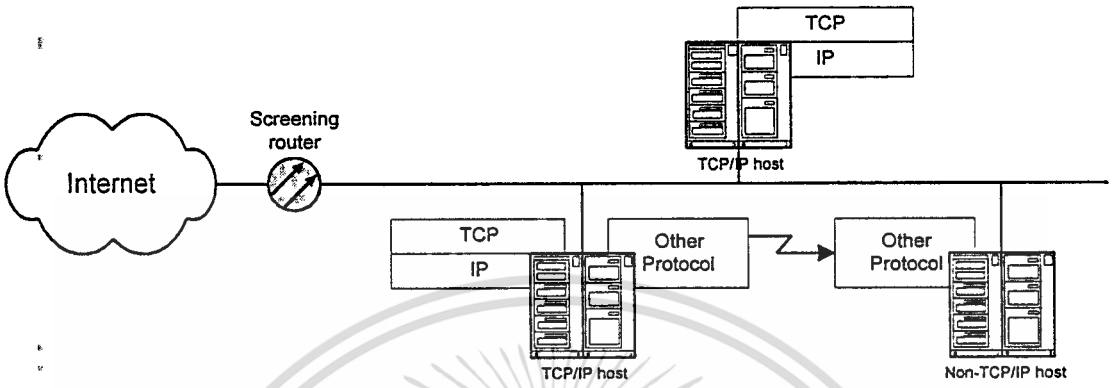
ในเครือข่ายที่ได้แสดงในรูป 4.2 ของของเครือข่ายในองค์กรเรียกว่าพารามิเตอร์ความปลอดภัย (Security parameter) เนื่องจากแฮคเกอร์ผู้ชั่วร้ายอยู่บนอินเทอร์เน็ต จะมีประโยชน์อย่างมากที่จะระบุโซนที่ความเสี่ยง บริเวณที่มีความเสี่ยงคือเครือข่ายที่สนับสนุนโปรโตคอล ทีซีพี/ไอพี (TCP/IP) และ โปรโตคอลที่ทำงานบน ทีซีพี/ไอพี ทั้งหมดที่สามารถเข้าถึงได้โดยตรงทาง อินเทอร์เน็ต

โฮสท์ที่อยู่ในโซนที่มีความเสี่ยงจะเป็นจุดอ่อนที่จะถูกโจมตี เป็นสิ่งที่ดีมากถ้าสามารถวางเครือข่ายไว้ในตำแหน่งที่อยู่นอกโซนที่มีความเสี่ยง อย่างไรก็ตามถ้าไม่มีอุปกรณ์ในการบล็อกการโจมตีเครือข่ายโซนที่มีความเสี่ยงก็จะขยายเข้ามาสู่เครือข่ายอีกจนได้ สกรีนนิงเราท์เตอร์คือหนึ่งในอุปกรณ์นั้น ซึ่งสามารถใช้เพื่อลดโซนที่มีความเสี่ยง จนกระทั่งมันไม่สามารถรุกเข้ามาที่พารามิเตอร์ความปลอดภัยของเครือข่าย

อาจจะมีโฮสท์บางตัวในเครือข่ายที่ไม่สนับสนุน ทีซีพี/ไอพี แม้กระนั้นโฮสท์เหล่านี้สามารถกลายเป็นจุดอ่อนถึงแม้ว่าในความเป็นจริงแล้วพวกมันไม่ได้เป็นส่วนหนึ่งโซนที่มีความเสี่ยงเลย การบุกรุกเครือข่ายจะเกิดขึ้นเมื่อโฮสท์ที่ไม่สนับสนุนทีซีพี/ไอพีได้เชื่อมต่อกับโฮสท์ที่สนับสนุนทีซีพี/ไอพี ผู้บุกรุกจะใช้โปรโตคอลที่ถูกสนันสนุนร่วมกันทั้งสองโฮสท์บุกรุกเข้ามายังโฮสท์ที่ไม่ได้สนับสนุนทีซีพี/ไอพีโดยผ่านทางโฮสท์อีกตัวหนึ่งที่สนันสนุนทีซีพี/ไอพี ดูรูป 4.3 ตัวอย่างเช่น ถ้าโฮสท์ทั้งหมดเชื่อมกันบนอีเทอร์เน็ตเซกเม้นท์ ผู้บุกรุกก็สามารถเข้าถึงโฮสท์ที่ขาดการป้องกันโดยผ่านทางอีเทอร์เน็ตโปรโตคอล

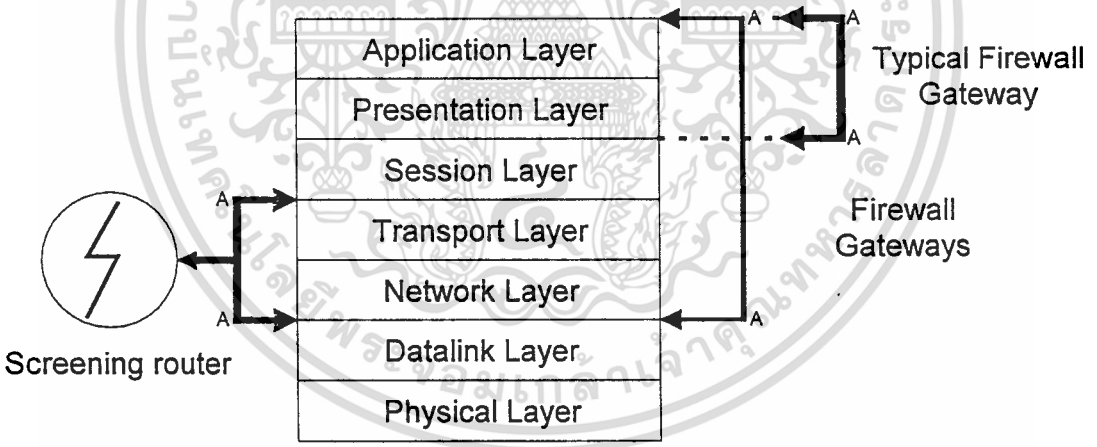
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สกรีนนิงเราท์เตอร์ ไม่สามารถกำจัดโซนที่มีความเสี่ยงได้ด้วยตัวมันเอง อย่างไรก็ตามพวกมันสามารถลดโซนที่มีความเสี่ยงได้อย่างมีประสิทธิภาพมาก



รูปที่ 4.3 โซนของความเสี่ยงขยายไปสู่โฮสท์ที่ไม่สนับสนุน ทีซีพี/ไอพี

4.1.6 ความสัมพันธ์ของสกรีนนิงเราท์เตอร์ และ ไฟร์วอลล์ กับ ไอเอสโอ โมเดล



รูปที่ 4.4 แสดง สกรีนนิงเราท์เตอร์ ไฟร์วอลล์และ ไอเอสโอ โมเดล

จากรูปจะเห็นได้ว่า สกรีนนิงเราท์เตอร์ นั้นทำงานกับเน็ตเวิร์คเลเยอร์ (IP protocol) และทรานสพอร์ทเลเยอร์ (TCP protocol) ส่วนไฟร์วอลล์มักจะถูกอธิบายในลักษณะของเกตเวย์ เกตเวย์สามารถทำการประมวลผลได้หมดทุกเลเยอร์ของ โอเอสไอ โมเดล ปกติเกตเวย์จะประมวลผลที่แอพพลิเคชั่นเลเยอร์นี่คือความจริงของไฟร์วอลล์เกตเวย์ส่วนใหญ่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

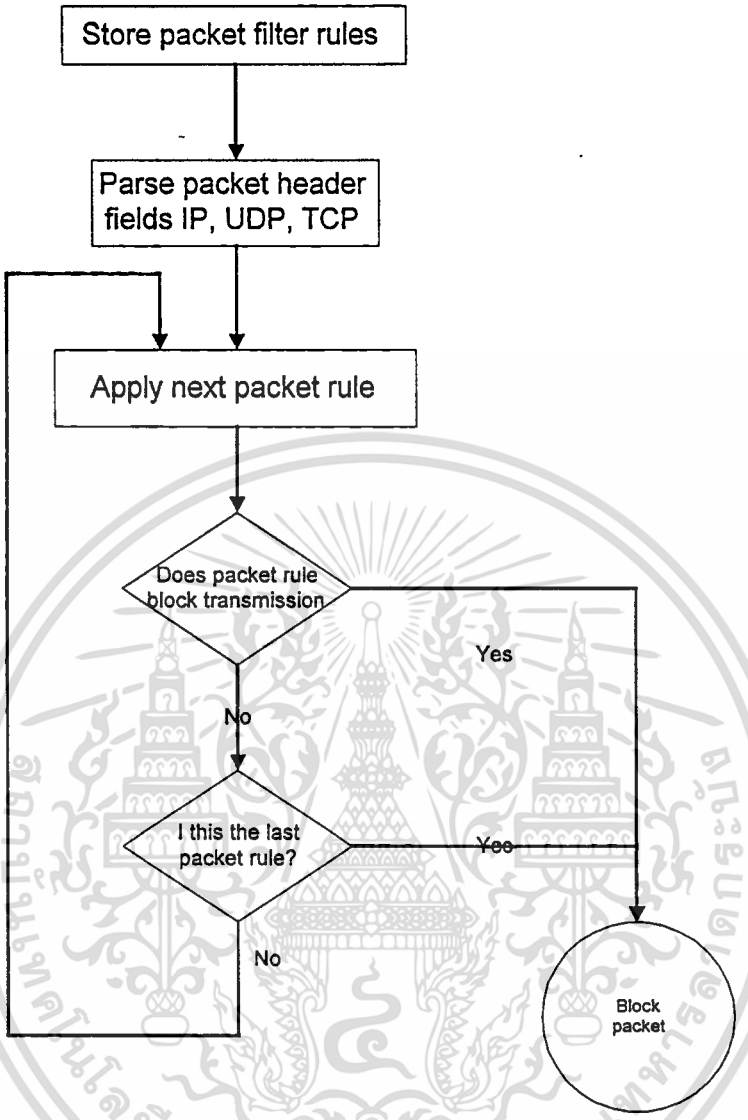
จากรูปยังแสดงให้เห็นอีกด้วยว่าเนื่องจากไฟร์วอลล์ครอบคลุมเน็ตเวิร์คและทรานสพอร์ทเลเยอร์มันจริงสามารถทำแพ็กเก็ตฟิลเตอริ่งได้

4.1.7 การทำงานของแพ็กเก็ตฟิลเตอริ่ง

1. เงื่อนไขของแพ็กเก็ตฟิลเตอริ่งต้องเก็บเอาไว้สำหรับพอร์ทของอุปกรณ์กรองแพ็กเก็ตเงื่อนไขเหล่านี้เรียกว่า แพ็กเก็ตฟิลเตอร์รูล (Packet filter rule)
2. เมื่อแพ็กเก็ตมาถึงพอร์ท ส่วนหัวของแพ็กเก็ตก็จะถูกตรวจสอบ และจะต้องเป็นส่วนหัวของ IP, TCP และ UDP เท่านั้น
3. แพ็กเก็ตฟิลเตอร์รูลจะต้องถูกเก็บเป็นลำดับที่เฉพาะ แต่ละกฎจะถูกนำมาใช้กับแพ็กเก็ตอย่างเป็นลำดับเหมือนที่จัดเอาไว้
4. ถ้ากฎบล็อกเอาแพ็กเก็ตที่ส่งออกหรือรับเข้ามาแพ็กเก็ตนั้นไม่ได้รับอนุญาตให้เดินทางต่อไป
5. ถ้ากฎอนุญาตให้แพ็กเก็ตเดินทางต่อได้ แพ็กเก็นนั้นก็จะถูกนำไปประมวลผลต่อได้
6. ถ้าแพ็กเก็ตไม่สอดคล้องกับกฎข้อใดข้อหนึ่งต้องถูกบล็อกเอาไว้

กฎเหล่านี้แสดงดังรูป 4.5

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.5 แสดงเงื่อนไขการทำงานของแพ็กเก็ตฟิลเตอริ่ง

จากกฎข้อที่ 4 และข้อที่ 5 จะเห็นความจริงว่ามันเป็นเรื่องสำคัญที่กฎจะต้องเรียงลำดับให้ถูกต้อง ถ้าวางลำดับผิดแพ็กเก็ตที่ควรจะถูกสกัดก็จะได้รับอนุญาตส่วนอันที่ควรได้รับอนุญาตก็จะถูกสกัดเอาไว้

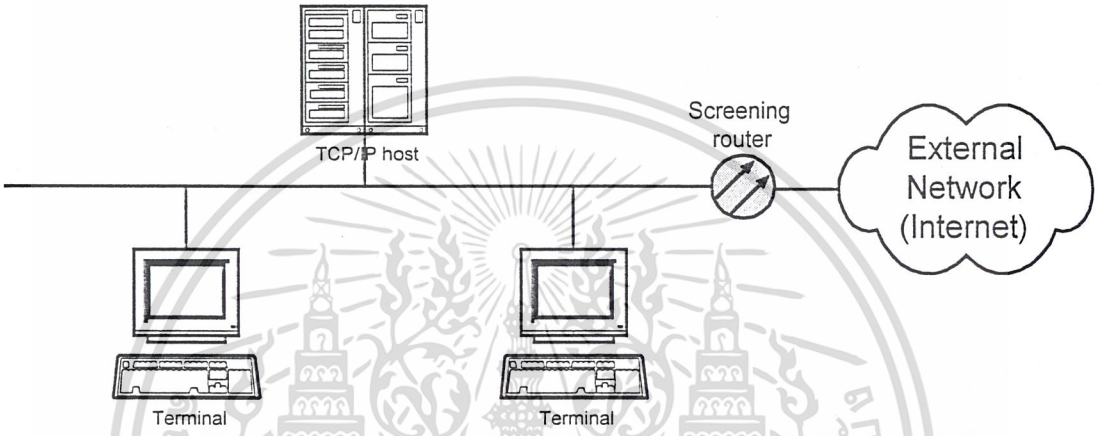
4.1.8 การออกแบบแพ็กเก็ตฟิลเตอร์

พิจารณาเครือข่ายในรูปที่ 4.6 โดยใช้ สกรีนนิงเราท์เตอร์ เป็นปราการด่านแรกที่กั้นระหว่างเครือข่ายภายในที่ต้องการป้องกันและเครือข่ายภายนอกที่ไม่น่าเชื่อถือ สมมติว่านโยบายรักษาความ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ปลอดภัยของเครือข่ายต้องการว่า อินเทอร์เน็ตเมล์ต้องได้รับจากโฮสท์ภายนอกบนเกตเวย์ที่จำเพาะเจาะจง และต้องการปฏิเสธการจราจรบนเครือข่ายที่มาจากโฮสท์ชื่อ CREEPHOST ซึ่งเราไม่ไว้ใจ

ในตัวอย่างนี้ นโยบายรักษาความปลอดภัยของเครือข่ายที่ใช้บน SMTP (Simple Mail Transfer Protocol) จะต้องถูกแปลไปเป็นแพ็กเก็ตฟิลเตอร์รูล เราต้องแปลกฎความปลอดภัยของเครือข่ายตามคำพูดต่อไปนี้



รูปที่ 4.6 แสดงการใช้สกรีนนิงเราท์เตอร์ในการบริหารความปลอดภัยของเครือข่าย

[กฎข้อที่ 1.] เราจะไม่เชื่อถือการเชื่อมต่อจากโฮสท์ที่ชื่อ CHEEPHOST

[กฎข้อที่ 2.] เราต้องการที่จะอนุญาตการเชื่อมต่อจากเมล์เกตเวย์

กฎเหล่านี้สามารถแปลงเป็นตารางของกฎตามรูป 4.7 เครื่องหมาย * คือ ค่าใด ๆ สำหรับคอลัมน์นั้น

สำหรับกฎข้อที่ 1 ในรูป 4.7 จะมีเอนทรีสำหรับคอลัมน์ *External Host* คอลัมน์อื่น ๆ ทั้งหมดจะเป็นเครื่องหมาย * แอคชั่นคือเพื่อบล๊อคการเชื่อมต่อ สามารถแปลงได้ดังนี้

"บล๊อคการเชื่อมต่อใด ๆ จาก CHEEPHOST ที่มาจากพอร์ทใด ๆ ของมันที่เข้ามาสู่พอร์ทใด ๆ ของโฮสท์ใด ๆ ของเรา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Filter Rule Number	Action	Our Host	Port On Our Host	External Host	Port On External Router	Description
1	Block	*	*	CHEEPHOST	*	Block traffic from CHEEPHOST
2	Allow	Mail-GW	25	*	*	Allow connection to our MAIL gateway

รูปที่ 4.7 แสดงการบล็อกหรือยอมให้แพ็กเก็ตผ่านเข้าเครือข่ายโดยสกรีนนิงเราท์เตอร์

สำหรับกฎข้อที่ 2 ในรูปที่ 4.7 จะได้เป็นเอนทรีของคอลัมน์ *Our Host* และ *Port On Our Host* คอลัมน์อื่น ๆ ทุกคอลัมน์จะเป็นเครื่องหมาย * แอคชั่นคือการอนุญาตการเชื่อมต่อสามารถแปลความหมายได้ดังนี้

"อนุญาตการเชื่อมต่อใด ๆ จากโฮสท์ภายนอกใด ๆ ที่มาจากพอร์ทใด ๆ ของโฮสท์นั้น มายังพอร์ท 25 ของโฮสท์ MAIL-GW ของเรา

พอร์ท 25 ที่ใช้เป็น TCP พอร์ทถูกสงวนไว้สำหรับ SMTP

4.2 เอชพี แอ็ดวานซ์สแต็ค (HP AdvanceStack)

4.2.1 ความปลอดภัยของระบบ

ปัญหาเกี่ยวกับความปลอดภัยของระบบเครือข่ายในสมัยก่อนคือ เครื่องเมนเฟรมตั้งไว้ในห้องคอมพิวเตอร์กลางเก็บข้อมูลของบริษัททั้งหมด และเข้าไปยังข้อมูลเหล่านี้ โดย ดัมพ์คอมพิวเตอร์ ผู้บริหารระบบคอมพิวเตอร์มีสิทธิในการควบคุมผู้ใช้ในระบบเครือข่ายอย่างเต็มที่ อย่างไรก็ตาม 10 ปีที่แล้ว สถาปัตย์ที่ใช้เครื่องเมนเฟรมนี้ก็ถูกแทนที่ด้วยเครื่องที่เล็กกว่า กระจายโดยใช้เครื่องคอมพิวเตอร์ส่วนบุคคลเป็นกลุ่ม ๆ และเครื่องเวิร์คสเตชั่น การพัฒนาแนวใหม่ในระบบเครือข่ายทั้งฮาร์ดแวร์และ ซอฟต์แวร์ ได้สร้างระบบ ไคลเอ็นท์/เซอร์ฟเวอร์ ซึ่งจัดหาข้อมูลและทรัพยากรให้แก่ผู้ใช้ในระบบบนระบบเครือข่ายแบบโลคอล แลน (LAN) ถูกเชื่อมเข้าด้วยกันเพื่อสร้างระบบเครือข่ายขนาดใหญ่ (WAN) ทั้งแลนและแวนเหล่านี้ได้พัฒนาเข้าไปในเครื่องมือสื่อ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารทางธุรกิจ ทำให้ง่ายต่อการเข้าไปยังข้อมูลส่วนตัวของบริษัท เนื่องจากข้อมูลมูลเหล่านี้เป็นข้อมูลที่สำคัญในการแข่งขันทางธุรกิจ, การทำลายระบบรักษาความปลอดภัยเป็นสาเหตุของความเสียหายทางด้านธุรกิจเพื่อป้องกันการทำลายระบบรักษาความปลอดภัย จำเป็นต้องเข้าใจความเสี่ยงของระบบความปลอดภัยที่เกี่ยวข้อง

4.2.2 ความเสี่ยงของระบบความปลอดภัย

เนื่องจากข้อมูลเหล่านี้ง่ายต่อการเข้าถึง หรือทำลายโดยตั้งใจหรือไม่ตั้งใจ หรือ การคุกคามโดยธรรมชาติก็แล้วแต่

การคุกคามโดยตั้งใจจากผู้ใช้ซึ่งไม่ได้รับสิทธิ์ที่ถูกต้องของระบบ ภายในหรือภายนอกก็ตาม ที่สามารถเข้ามายังข้อมูลบนระบบเครือข่าย ลักษณะเด่นของแลนในการใช้ทั่ว ๆ ไปก็คือถูกออกแบบเพื่อสื่อสารข้อมูลไปยังทุก ๆ จุดเชื่อมต่อบนส่วนต่าง ๆ ของแลน ดังนั้นก็เหมือนเป็นการอนุญาตให้ข้อมูลส่วนตัวของบริษัทง่ายต่อการเข้าถึงโดยผู้ใช้ทั่วไป สามารถที่เข้าถึงหรือทำลายเพื่อเข้าม่าในระบบเครือข่าย

การคุกคามโดยไม่ตั้งใจมีสาเหตุจากความพลั้งเผลอของลูกจ้างภายในบริษัทที่ออกจากเครื่องคอมพิวเตอร์โดยไม่ล็อคเอาท์ หรือจากลูกจ้างสร้างพาสเวิร์ดที่ง่ายเช่น ชื่อลูก หรือชื่อภรรยาเป็นต้น

ภัยจากการคุกคามโดยธรรมชาติ เช่นอุปกรณ์ทำงานผิดพลาดไม่ตรงกับคำสั่งที่ตั้งไว้ หรือภัยธรรมชาติ เช่น ไฟไหม้, น้ำท่วม,เฮอริเคน หรือ แผ่นดินไหว เป็นภัยคุกคามต่อระบบรักษาความปลอดภัยซึ่งเป็นสาเหตุความเสียหายของข้อมูลและอุปกรณ์เครื่องมือ

เพื่อป้องกันระบบเครือข่ายจากการเจาะ ,วิธีป้องกันความปลอดภัยของระบบในหลาย ๆ แง่ต้องถูกพัฒนาบนพื้นฐานของการเสี่ยงของระบบความปลอดภัย

4.2.3 ความปลอดภัยของระบบเครือข่าย

ขั้นแรกเกี่ยวกับการได้รับความรู้เรื่องการบริหาร และ การสนับสนุนของอิมพลีเม็นท์แผนการระบบความปลอดภัยของระบบ การบริหารร่วมกันต้องทำระบบรักษาความปลอดภัยเป็นองค์การ ผู้บริหารระบบเครือข่าย,คนที่เกี่ยวกับการจัดให้มีระบบเครือข่ายสำหรับผู้ใช้, ต้องทำให้ผู้ใช้ระวังเกี่ยวกับความเสี่ยงของระบบความปลอดภัยซึ่งเขาเหล่านั้นต้องเผชิญในการใช้คอมพิวเตอร์ของพวกเขาเอง หรือทำอย่างไรที่พวกเขาจะสามารถทำให้ระบบเครือข่ายของพวกเขาได้รับความปลอดภัยมากที่สุด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ขั้นต่อไปคือให้ความเข้าใจความต้องการของบริษัทเกี่ยวกับความปลอดภัยของระบบ โดยบ่งชี้พื้นที่ที่เป็นจุดอ่อน วาดแผนที่ของระบบเครือข่ายพร้อมด้วยอาคารและห้องของพื้นที่เข้า และพื้นที่ของการเข้าถึงระบบเครือข่ายอย่างชัดเจน

ขั้นต่อไปรวม การประเมินความต้องการด้านความปลอดภัยบนพื้นที่ของสิ่งคุกคามระบบความปลอดภัยที่เป็นไปได้ และ การพัฒนาวิธีรักษาความปลอดภัยสำหรับแต่ละกลุ่มหน้าที่ การพิจารณา ความเสี่ยงกับราคา ต้องใช้ในการตัดสินใจว่าจะเลือกวิธีป้องกันความปลอดภัยอันไหน

ขั้นสุดท้าย รวมการอิมพลีเม็นท์กลยุทธความปลอดภัยโดยจัดหาให้การศึกษาบริษัท และการบังคับใช้ของนโยบายรักษาความปลอดภัยที่ตั้งขึ้นและระบบรักษาความปลอดภัยต้องมีการตรวจตราเป็นประจำและอาจต้องทำการเปลี่ยนเมื่อเวลาผ่านไป

4.2.4 วิธีรักษาความปลอดภัย

มีจุดแตกต่างจำนวนหนึ่งของการเข้าถึงเพื่อควบคุมเมื่อทำการป้องกันระบบเครือข่ายของรวม ขอบเขตของความสะดวก, สายที่ต่อเชื่อมอุปกรณ์ระบบเครือข่าย และการเข้าถึงระบบเครือข่ายโดยผู้ใช้ทั่วไป ยิ่งไปกว่านั้น,ฮาร์ดแวร์และซอฟต์แวร์อีกหลายชนิดมีเพื่อการป้องกันการเข้าถึงของงข้อมูลบนระบบเครือข่าย,รวมถึง รีพีทเตอร์ บริดจ์ เราท์เตอร์ การบริหารระบบเครือข่าย การบีบอัดข้อมูล และ การเข้ารหัสข้อมูล

การรักษาความปลอดภัยขอบเขตการเข้าถึง ตัวอาคารหรือพื้นที่ของอาคาร ควรเป็นความสำคัญอันดับแรกในการบริหารเรื่องความปลอดภัยของระบบเครือข่าย พื้นที่ซึ่งข้อมูลที่มีความสำคัญถูกจัดตั้งอยู่ควรจะได้รับการรักษาความปลอดภัย เซอร์ฟเวอร์ของระบบเครือข่าย และ แหล่งข้อมูล ความถูกเก็บไว้ในระบบความปลอดภัย ต้องการใช้ บัตรผ่าน,กุญแจ,เหรียญ หรือ อุปกรณ์อื่นๆ ในการเข้ามาในพื้นที่ความปลอดภัย

รักษาความปลอดภัยห้องที่เดินสายเพื่อป้องกันผู้บุกรุกจากการเข้าไปยุ่งกับ อุปกรณ์ภายในระบบเครือข่าย หรือเจาะเข้าในระบบเครือข่าย ล็อคห้องที่เดินสายและตั้งไว้ในแอดเดรสต่างหากเพื่อป้องกันภัยธรรมชาติ และทำให้แน่ใจว่าข้อมูลถูกเก็บไว้เป็นประจำ

เพื่อจัดทำความปลอดภัยระหว่างห้องซึ่งเดินสายหรือในพื้นที่ซึ่งระบบเครือข่ายของท่านกำลังใช้ข้อมูลที่มีความสำคัญสูง และใช้ตัวกลางเคเบิลความปลอดภัย การเดินสายไฟเบอร์ ออพติค ให้ความปลอดภัย และ ให้ระยะทางในการเคเบิลเพิ่มถึง 1 กิโลเมตร สำหรับความปลอดภัยสูงสุด.สายเคเบิลที่มีการป้องกันอย่างหนาอาจใช้เพื่อกำจัดคลื่นวิทยุ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การเข้าถึงของผู้ใช้ ทำให้แน่ใจว่าพาสเวิร์ด และเบอร์ของผู้ใช้ สามารถใช้อย่างมีประสิทธิภาพ หรือ เปลี่ยนบ่อย ๆ เป็นขั้นตอนที่สำคัญในการรักษาความปลอดภัยของคอมพิวเตอร์ส่วนบุคคล เครื่องเซอร์ฟเวอร์ และเครื่องเวอร์คสเตชั่นจากการเข้าถึงโดยตรงภายในระบบเครือข่าย ลูกจ้างทุก ๆ ควรจะถูกฝึกหัดในเรื่องความปลอดภัยสำหรับคอมพิวเตอร์ของพวกเขา และ จำกัดการเข้าถึงหรือการแสดงข้อมูลส่วนตัวของบริษัท ระบบรักษาความปลอดภัยคอมพิวเตอร์ สามารถจัดหาระดับเพิ่มเติมความปลอดภัย รวมทั้งการทำให้แน่ใจว่าพาสเวิร์ดครบตามความต้องการของความปลอดภัย (จำนวนตัวอักษรครบ) ตรวจและจำกัดจำนวนของความพยามยามล็อคอินอุปกรณ์ จัดหาผู้ใช้ที่ถูกต้องของระบบ และ เวลาจำกัดในการใช้เป็นต้น

รีพีทเตอร์รักษาความปลอดภัย คือ เท็นเบส-ที (10Base-T) อุปกรณ์ฮับ ซึ่งป้องกันข้อมูลจากการถูกส่งไปหรือรับเข้ามาจากผู้ใช้ที่ไม่ถูกต้องแต่ละฮับพอร์ทจัดให้สำหรับหนึ่งแอดเดรสของเครื่องของผู้ใช้ที่ถูกต้องเพื่อใช้พอร์ทนั้น ฮับใช้แอดเดรสเครื่องที่ถูกเพื่อควบคุมการไหลของข้อมูลทั้งขาเข้าจากผู้ใช้ และขาออกจากผู้ใช้

ข้อมูลขาออกสามารถถูกรักษาความปลอดภัยโดยให้อุปกรณ์เห็นแพ็กเก็ตเหมือนข้อมูลที่มีอยู่ถ้าแพ็กเก็ตนั้นเป็นของสำหรับพวกมัน เมื่อข้อมูลถูกส่งข้ามระบบเครือข่าย ฮับเปรียบเทียบพอร์ทของแอดเดรสของเครื่องที่ถูกต้องกับแอดเดรสปลายทางของแพ็กเก็ตขาออก ถ้าแอดเดรสไม่เหมือนกันฮับจะแทนที่ฟิล์ดข้อมูลของสแตรมเบิล, ข้อมูลที่ไม่มีความหมาย ถ้าแอดเดรสเหมือนกัน, ฮับส่งแพ็กเก็ตข้อมูลที่มีอยู่

ข้อมูลขาเข้าถูกรักษาความปลอดภัยโดยเปรียบเทียบแอดเดรสต้นทางของแต่ละแพ็กเก็ตที่เข้ามาในพอร์ทกับแอดเดรสของผู้ใช้ที่ถูกต้อง ถ้าแอดเดรสไม่เหมือนกัน ฮับจะลงความเห็นว่าผู้บุกรุกกำลังพยายามเพื่อเข้ามายังระบบเครือข่าย และสามารถทำให้พอร์ทนั้นไม่สามารถใช้ได้ โดยส่งสัญญาณเตือน

4.2.4.1 การแบ่งระบบเครือข่ายด้วยบริดจ์และเราท์เตอร์

การแบ่งระบบเครือข่ายด้วยบริดจ์และเราท์เตอร์ไม่เพียงแต่เพิ่มประสิทธิภาพโดยแยกแต่ละส่วนออกจากกัน แต่ยังให้ความปลอดภัยกับระบบเครือข่ายโดยจำกัดและควบคุมการไหลของการจราจรในระบบเครือข่ายด้วย

บริดจ์ ซึ่งทำงานในระดับชั้นดาต้าลิงค์ ให้ความปลอดภัยระบบโดยใช้ตัวกรองแอดเดรสเพื่อแยกโลคอลแทรฟฟิค จาก โลคอลเน็ตเวิร์คเซ็กเม็นต์ อุปกรณ์บริดจ์บางอันให้การบริหารการกรองแอดเดรสโดยเฉพาะเพื่อควบคุมการเข้าถึงในส่วนระบบเครือข่าย ยกตัวอย่าง แผนกบัญชีสามารถแยกจากส่วนเหลือของระบบเครือข่ายเพื่อเก็บข้อมูลทางการเงินที่สำคัญไว้อีกที่หนึ่ง ตัว

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กรองแอดเดรสสามารถให้เราทำการเซ็ทค่าโคลสยูสเซอร์กรุ๊ป (Close user groups) ซียูจี อนุญาตให้ผู้บริหารระบบจำกัดว่ากลุ่มไหนสามารถคุยกับกลุ่มไหนได้ ยกตัวอย่างเช่น แผนกบัญชีและแผนกการขาย ถูกทำให้ร่วมกันโดยบริดจ์ซึ่งทำให้ทั้ง 2 แผนกติดต่อข้ามบริดจ์เหมือนว่าเป็นซียูจี แผนกอื่น ๆ ถูกกีดกันจากการเข้าถึงการสื่อสารระหว่างทั้ง 2 แผนกนี้

เราท์เตอร์สามารถให้ความปลอดภัยที่มากกว่าและการควบคุมของผู้บริหารระบบ เพราะเราท์เตอร์ ทำเกี่ยวกับความปลอดภัยในชั้นระบบเครือข่าย เราท์เตอร์จำกัดและควบคุมการไหลของการจราจรในระบบเครือข่ายโดยทำการจัดสินใจหาเส้นทางขึ้นกับแบนวิดธ์ที่มี จำนวนของการกระโดดหรือการติดต่อภายใน และความน่าเชื่อถือของเส้นทางพิเศษ ยิ่งไปกว่านั้น เราท์เตอร์สามารถถูกเซ็ทค่าเริ่มต้นด้วยตัวกรองแพ็กเก็ตเพื่อให้ควบคุมการกรองเพิ่มขึ้น

ซอฟต์แวร์เพื่อการบริหารระบบเครือข่าย ให้กราฟฟิคอินเทอร์เฟซซึ่งให้ผู้บริหารระบบเครือข่ายเซ็ทความปลอดภัยสำหรับอุปกรณ์เครือข่าย ซอฟต์แวร์เพื่อการบริหารระบบเครือข่ายสามารถให้มีหน้าที่ต่างกันขึ้นอยู่กับผู้ขาย แต่ส่วนใหญ่มีความสามารถเซ็ทพาสเวิร์ด, เซ็ทพารามิเตอร์ความปลอดภัย, รายงานการกระทำผิดความปลอดภัยในแบบเรียลไทม์ และให้บัญชีของการพยายามเข้าถึงระบบเครือข่ายโดยไม่ถูกต้อง

โปรโตคอลมาตราฐานที่เกี่ยวข้องสำหรับการบริหารระบบเครือข่าย คือ ซิมเปิล เน็ตเวิร์ค เมนเนจเม็นท์ โปรโตคอล (SNMP) ซึ่งให้ราคาที่เหมาะสมกับประสิทธิภาพทั่วไปอิมพลีเม็นเพื่อการบริหารกับอุปกรณ์ในระบบเครือข่ายเอสเอ็นเอ็มพี, แม้ว่าจะอิมพลีเม็นทั่วไป แต่ยังมีข้อจำกัดว่าจะถูกแอดเดรสโดยมาตราฐานที่จะตามมา เอสเอ็นเอ็มพี2 เอสเอ็นเอ็มพี2 จะเป็นซุปเปอร์เซ็ทของเอสเอ็นเอ็มพีอิมพลีเม็นเตชั่น รวมทั้งให้การส่งถ่ายข้อมูลจำนวนมาก, สนับสนุนโปรโตคอลจำนวนมาก และ สามารถจัดการข้อผิดพลาดได้ดีกว่า

การบีบอัดข้อมูล เป็นขบวนการของการเข้ารหัสแบบของข้อมูลที่ซ้ำ ๆ กันในแบบย่อสำหรับการส่งถ่ายบนระบบเครือข่าย การบีบอัดข้อมูลทำเพื่อปรับปรุงประสิทธิภาพของระบบเครือข่าย แต่สามารถจัดให้เพียงบางระดับของความปลอดภัย เพราะข้อมูลที่ถูกบีบอัดไม่สามารถอ่านได้อีกต่อไป เพราะว่ามันไม่ถูกออกแบบเพื่อให้ความปลอดภัยของข้อมูล อัลกอริทึมการบีบอัดรู้จักดีและมีให้อ่านได้ถ้ารูปแบบขอการบีบอัดพอจำได้ ข้อมูลอาจจะถูกคลายออกได้ง่าย

การเข้ารหัสข้อมูลเป็นวิธีสมัยใหม่ที่สุดของการป้องกันข้อมูลที่สำคัญจากการเข้าถึงโดยผู้ใช้ผู้ไม่มีสิทธิ การเข้ารหัสและการถอดรหัสเป็นขั้นตอนของการกระทำทางเลขคณิตที่ซับซ้อนโดยใช้ คีย์ เพื่อการเข้ารหัส และ ถอดรหัสข้อมูลสำหรับการขนส่งบนระบบเครือข่าย

มี 2 วิธีหลัก ๆ ของอัลกอริทึมการเข้ารหัสในปัจจุบันที่ใช้อยู่ คือ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1. อาร์เอสเอ (RSA) ใช้คีย์ในการเข้ารหัสเป็นแบบสาธารณะ และ แบบดิจิตอล ปัญหาหนึ่งของเกี่ยวกับการเข้ารหัสข้อมูลคือปัจจุบันรัฐบาลได้จำกัดการส่งของโปรแกรมการเข้ารหัสข้อมูล
2. ดีอีเอส (DES) มาตราฐาน ANSI ในปัจจุบันสำหรับส่วนตัวหรือความลับคีย์ในการเข้ารหัส เป็นมาตราฐานการเข้ารหัสของข้อมูลของรัฐบาลจาก สถาบันแห่งชาติของมาตราฐานและเทคโนโลยี

อาร์เอสเอ และ ดีอีเอส สามารถใช้ด้วยกันได้ โดยทั่วไปถูกแนะให้ใช้วิธีการเข้ารหัสแบบส่วนตัวหรือความลับ สำหรับการส่งถ่ายการเข้ารหัส และใช้การเข้ารหัสแบบสาธารณะสำหรับการแจกจ่ายคีย์และการบริหาร

4.2.5 ดีอีเอส

พัฒนาขึ้นในปี 1977 โดย National Bureau of Standards โดยอาศัยหลักการพื้นฐานที่เรียกว่า Lucifer cipher ที่พัฒนาขึ้นโดยไอบีเอ็ม

ดีอีเอส นี้จะใช้คีย์ขนาด 56 บิต นำมาใส่รหัสเข้ากับข้อมูลที่แบ่งเป็นบล็อกของข้อมูลขนาดบล็อกละ 64 บิต และผลของข้อมูลหลังจากใส่รหัสแล้วก็จะออกมามีขนาด 64 บิตเช่นเดียวกัน

ซึ่งมีหลักการทำงานดังนี้อินพุท ซึ่งเป็นข้อมูลที่เราจะส่งไปซึ่งเราแบ่งเป็นบล็อกข้อมูลขนาด 64 บิตนี้จะถูกสลับสับเปลี่ยนบิตของข้อมูลซึ่งสุดท้ายก็ยังคงได้ข้อมูลขนาด 64 บิตที่ถูกสับบิตข้อมูลแล้ว จากนั้นจะนำบิตคีย์ขนาด 56 บิต มาสร้างเป็นคีย์ขนาด 48 บิต จำนวน 16 คีย์ สำหรับใช้ในการ ใส่รหัสสให้กับอินพุทข้างต้นรอบละ 1 คีย์เป็นจำนวน 16 รอบ โดยที่แต่ละรอบของการใส่รหัสข้อมูลขนาด 48 บิต กับอินพุทขนาด 64บิตนี้จะได้เอาท์พุทขนาด 64 บิตออกมา ซึ่งจะกลายเป็นอินพุทของรอบต่อไปเรื่อย ๆ จนจบ 16 รอบ เมื่อได้เอาท์พุทในรอบที่ 16 ออกมาแล้ว ข้อมูลอันนี้จะนำไปสับเปลี่ยนบิตอีกครั้งหนึ่ง โดยครั้งนี้จะใส่หลักการสับเปลี่ยนบิต (จะกล่าวถึงต่อไป) ที่กลับกับการสับในครั้งแรก หรือ อาจกล่าวได้ว่าเป็นอินเวิร์สของการสับข้างต้นนั่นเอง

สำหรับการถอดรหัส เราต้องเริ่มต้นโดยการสับเปลี่ยนบิตโดยใช้หลักการสับเปลี่ยนดังที่ใช้กับการสับเปลี่ยนบิตในตอนแรก (นั่นคือเป็นการยกเลิก (undo) การสับเปลี่ยนในตอนสุดท้าย จากนั้นนำคีย์ที่ใช้ในการใส่รหัสในตอนแรกมาใส่โดยใส่กลับกันคือ ใส่รหัสขนาด 48 บิตรหัสที่ 16 ก่อน และสุดท้ายที่รหัสที่ 1 จากนั้นจะได้ข้อมูลซึ่งจะต้องไปทำการสับ โดยใช้วิธีการสับที่กลับกับการสับครั้งแรก หรือใช้หลักการสับของการใส่รหัสในตอนสุดท้ายนั่นเอง

4.2.6 อาร์เอสเอ

RSA มาจาก Rivest Shamir และ Adleman ซึ่งเป็นผู้คิดค้นวิธีนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

อาร์เอสเอ อาศัยหลักของพับลิคคีย์ซึ่งขนาดของคีย์จะสามารถกำหนดได้ตามต้องการ ถ้าเรากำหนดคีย์ยาว ก็จะทำให้ยากต่อการถอดรหัส หรือ ทำให้ปลอดภัยมากขึ้น แต่ถ้าเรากำหนดคีย์สั้น ก็จะทำให้มีประสิทธิภาพในการ ใช้งานมากยิ่งขึ้น แต่ตามปกตินิยมใช้ความยาวของคีย์เท่ากับ 512 บิต เช่นเดียวกับบล็อกของข้อมูล ก็สามารถกำหนดได้ตามต้องการ แต่บล็อกข้อมูล หรือ plaintext นี้จะต้องสั้นกว่าความยาวของคีย์ หรืออาจยาวเท่ากับคีย์ก็ได้

อาร์เอสเอ จะมีผลต่อการทำงานของฮาร์ดแวร์ ทำให้ใช้เวลาในการทำงานมากกว่าการใช้ ซีเครตคีย์ อัลกอริทึม อาร์เอสเอ จึงไม่นิยมใช้ในการเข้ารหัสข้อมูลที่ยาว ๆ แต่นิยมใช้ในการเข้ารหัสซีเครตคีย์ แล้วจากนั้นค่อยนำคีย์นั้นไปเข้ารหัสข้อมูลอีกครั้งหนึ่ง

4.2.7 การแก้ปัญหาความปลอดภัยของเอชพี แอ็ดวานซ์สแต็ค

เอชพี แอ็ดวานซ์สแต็ค ให้การแก้ปัญหาเพื่อสร้างระบบความปลอดภัย, รีพีทเตอร์, บริดจ์, เราท์เตอร์ และ ความสามารถในการบริหารระบบเครือข่ายเอชพี แอ็ดวานซ์สแต็คยับเป็น เท็นเบส-ที รีพีทเตอร์หลายพอร์ต ซึ่งมีความสามารถเกี่ยวกับความปลอดภัยของข้อมูลและการบริหารระบบเครือข่าย ลักษณะความปลอดภัยของข้อมูลรวมทั้งความปลอดภัยภายในและภายนอก ลักษณะเพิ่มเติมมีการเตือนเมื่อมีการทำลายระบบความปลอดภัย, ลิสต์ของผู้จัดการที่ถูกต้อง, การป้องกันพาสเวิร์ด และ LED ความปลอดภัย สำหรับการสังเกตุเห็นสภาวะปลอดภัยของฮับ

เอชพี 10:10 แลน บริดจ์ เอ็มบี และ เอชพี รีโมทบริดจ์ อาร์บี รวมตัวกรองการจราจรสมัยใหม่ซึ่งสามารถกรองและส่งต่อแพ็กเก็ตข้อมูล เร็วเท่าที่ระบบเครือข่ายสามารถทำได้ มันแยกจราจรเครือข่ายและส่งต่อเพียงแพ็กเก็ตที่มีปลายทางบนด้านอื่นของบริดจ์ ยิ่งกว่านั้น. มันสามารถเซ็ทค่าระบบด้วยคอสตอลแทร์พฟิคฟิลเตอร์ เพื่อป้องกันการจราจรที่ไม่ถูกต้องจากการผ่านเข้ามาในระบบความปลอดภัย หรือเพื่อสร้างโคลสกรุ๊ปของแอดเดรสซึ่งได้รับอนุญาตเพื่อการติดต่อข้ามบริดจ์

เอชพี แอ็ดวานซ์สแต็ค เราท์เตอร์ให้แพ็กเก็ตที่ทันสมัย และ ตัวกรองข้อมูลเราท์เตอร์อิมพลีเม็นที่เน็ตเวิร์คเลเยอร์ ตัวกรองแพ็กเก็ตความสามารถในการเซ็ตค่าของผู้ใช้ ให้การกรองจราจรเพิ่มขึ้นมากบนพื้นฐานของชนิดการบริการ, โปรโตคอล, แอดเดรสซับเน็ต, หรือ เน็ตเวิร์คสเตชั่นแอ็ดเดรส ตัวกรองข้อมูลเราท์เตอร์ป้องกันเราท์เตอร์จากการแจ้งให้ทราบของเราท์เตอร์อื่นของการคอนฟิกของระบบเครือข่าย เอชพี เราท์เตอร์ สนับสนุนหลากหลายของตัวกรอง ไอพี/ไอพีเอ็กซ์ (IP/IPX)

เอชพี แอ็ดวานซ์สแต็ค ให้ผลิตภัณฑ์การบริหารบน ดอส, วินโดวส์ และ เอชพี และ ซันยูนิกซ์ แพล็ตฟอร์มง่ายต่อการเซ็ตค่าเริ่มต้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.2.8 บทสรุป

การออกแบบและการทดลองการทำงาน ของวิธีรักษาความปลอดภัยเป็นสิ่งที่ต้องการเพื่อการป้องกันระบบเครือข่ายในทุกวันนี้ และข้อมูลที่พวกมันมีอยู่ การออกแบบวิธีการรักษาความปลอดภัยควรจะมีการสำรวจแผนที่ในส่วนฟิสิคอล และ ของแผนที่ในระบบเครือข่าย และในทุก ๆ พื้นที่ที่เป็นจุดอ่อน ขอบเขตการรักษาความปลอดภัยและการบังคับใช้พาสเวิร์ดของผู้ใช้ และ ไอดีนัมเบอร์ (ID Number) มีประสิทธิในการเข้าสู่พื้นที่ของระบบรักษาความปลอดภัยเครือข่าย ระบบเครือข่ายควรถูกออกแบบด้วยระบบความปลอดภัยโดยใช้การรักษาความปลอดภัยแกรีพีทเตอร์ซึ่งส่งข้อมูลที่อ่านได้เพียงอย่างเดียว เพื่อตรวจสอบแอดเดรสปลายทาง และเพื่อบอกและทำให้ผู้ใช้ที่ไม่ถูกต้องไม่สามารถใช้ต่อไปได้ การใช้บริดจ์และเราท์เตอร์เพื่อควบคุมการไหลของข้อมูล เข้าและออกจากระบบรักษาความปลอดภัยเครือข่าย การใช้การบริหารระบบเครือข่าย เพื่อจัดหาบัญชีร่องรอยของผู้ใช้ที่ทำการเข้ามาในระบบเครือข่าย และ อุปกรณ์ของระบบเครือข่าย หรือ การใช้การเข้ารหัสเพื่อเข้ารหัสข้อมูลที่เดินทางข้ามสาย ขั้นสุดท้ายในการอิมพลีเม็นท์วิธีรักษาความปลอดภัยเพื่อให้การศึกษาแก่พนักงานในบริษัท และ เพื่อบังคับ จัดการ และตรวจสอบนโยบายความปลอดภัยที่ได้จัดทำขึ้น สนับสนุนหลากหลายตัวกรอง -ไอพี, ไอพีเอ็กซ์ และ เลิร์นนิ่งบริดจ์ โปรโตคอล (Learning Bridge Protocol) สำหรับโปรโตคอล เฉพาะอย่าง หรือ ที่ต้องการเฉพาะ

4.3 กรณีศึกษา (Case studies)

4.3.1 สถาบันการศึกษา

ตัวอย่างเช่น มหาวิทยาลัยทั้งหลาย ปกติจะมีปัญหาเป็นส่วนมากในการติดตั้งไฟร์วอลล์ ทั้งนี้เนื่องจากผู้ใช้มีอิสระที่จะทดลองใช้แอพพลิเคชั่นอะไรก็ได้ในเครือข่าย และมักจะไม่พอใจเมื่อมีไฟร์วอลล์มาจำกัดการใช้งานของพวกเขาแถมยังพยายามที่จะทำลายไฟร์วอลล์นี้เสียด้วย นอกจากนี้สถาบันการศึกษายังมีแผนกที่มีงบประมาณไม่ขึ้นต่อกันและมีเหมือนมีสิทธิอิสระในการใช้เครือข่ายของสถาบัน ซึ่งทำให้ยากลำบากในการออกกฎข้อบังคับในการใช้ระบบรักษาความปลอดภัย ถ้าแผนกหนึ่งในสถาบันติดตั้งระบบรักษาความปลอดภัยซึ่งจะมีผลกับแผนกอื่น พวกเขาสามารถจะสร้างเครือข่ายใหม่ขึ้นมาเพื่อเป็นทางลัดผ่านระบบรักษาความปลอดภัยนี้ไปก็ได้ วิธีหนึ่งที่ดูเหมือนจะเหมาะสำหรับสถาบันการศึกษา คือ การแยกเอางานระบบที่สำคัญไว้หลังไฟร์วอลล์ระบบที่มีเรคอร์ดข้อมูลของนักศึกษา, ข้อมูลรายการยืม และรายการจ่ายเช็ค ก็ให้ทำการประมวลผลอยู่เบื้องหลังสกรีนนิงเราท์เตอร์หรือไฟร์วอลล์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3.2 ห้องปฏิบัติการวิจัย (Research lab)

แลบการวิจัยมักจะเป็นกรณีที่ยาก นักวิทยาศาสตร์คาดหวังที่จะใช้เครือข่ายสำหรับร่วมมือและค้นหาข้อมูลใหม่ อย่างไรก็ตามในหลายกรณีการวิจัยอาจจะมีความสำคัญทางเศรษฐกิจและจะต้องได้รับการป้องกัน ระบบที่มีแอพพลิเคชั่นลิขสิทธิ์, การออกแบบสำหรับผลิตภัณฑ์ที่มีเจ้าของเป็นต้น จะต้องถูกแยกออกมาต่างหากและได้รับการป้องกัน หรืออาจจะสร้างระบบใหม่ขึ้นมาอีกหนึ่งระบบที่เชื่อมต่อกับอินเทอร์เน็ตและแยกออกจากกันทางกายภาพกับระบบที่ทำงานวิจัย แลบวิจัยได้รับผบเสียจากปัญหาคล้ายกับสถาบันการศึกษา เพราะผู้ใช้ต้องการทำงานเป็นกลุ่มที่แยกต่างหากและไม่ชอบถูกรบกวนจากพวกแฮกเกอร์ หรือใคร ๆ บนอินเทอร์เน็ต บางทีก็ต้องหาเจ้าหน้าที่มาทำความเข้าใจและรับผิดชอบในการรักษาความปลอดภัยของทรัพย์สินทางปัญญา

หลาย ๆ แลบวิจัยได้เชื่อมต่อกับอินเทอร์เน็ตโดยใช้ไฟร์วอลล์แบบพร็อกซี่ (Proxy-based) ซึ่งปลอดภัยพอประมาณและสามารถแอคเซสไปยังเว็บต่าง ๆ ได้ ส่วนแลบที่เหลือก็อาศัยการแยกระบบออกมาต่างหากเพื่อเก็บข้อมูลที่มีค่า

4.3.3 แอพพลิเคชั่นทางการค้า (Electronic commerce application)

การค้าทางอิเลคทรอนิคส์มีความสำคัญมากขึ้น ความจำเป็นที่ต้องส่งข้อมูลเข้าออกผ่านไฟร์วอลล์จะกลายเป็นสิ่งสำคัญมากขึ้น การวิเคราะห์ความต้องการในเชิงการบริการจะเป็นเครื่องมือที่มีประโยชน์สำหรับออกแบบและติดตั้งระบบไฟร์วอลล์ สมมติองค์กรต้องการที่จะวางเว็บเซอร์ฟเว่อร์ไว้บนเครือข่ายภายนอก และเพื่อต้องการเตรียมการเข้าถึงฐานข้อมูลเพื่อทำการเรียงรายการข้อมูลในเครือข่ายเบื้องหลังไฟร์วอลล์ ในกรณีนี้ ความต้องการของเราก็คือให้รับข้อมูลเข้าและนำออกเฉพาะสำหรับ SQL เท่านั้น เราอาจจะเลือกเอาสกรีนนิงเราท์เตอร์ไฟร์วอลล์ และกำหนดให้อนุญาตเพียง SQL เท่านั้นในการรับ-ส่งข้อมูลข้างนอกเว็บไซท์และภายใน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5

ตัวอย่างการบริหารระบบที่ใช้งานแอพพลิเคชั่นต่างๆ

แอพพลิเคชั่น (Application) ที่จะกล่าวนี้เป็นโปรแกรมประยุกต์ที่ใช้งานบนเครือข่ายระยะไกล(WAN Application) ที่มีการใช้งานอยู่ในปัจจุบันซึ่งส่วนใหญ่ทำงานบนโปรโตคอล TCP/IP โดย มีแอพพลิเคชั่นมีดังต่อไปนี้

1. World Wide Web (WWW)
2. การโอนย้ายแฟ้มข้อมูลระยะไกล (FTP : File Transfer Program)
3. การรีโหมดลอกอิน (Telnet)
4. จดหมายอิเลคทรอนิค (E-mail)
5. ออนไลค์ ทรานแซกชั่น (Online Transaction)
6. การประชุมทางไกล (Video Conference)
7. วีดีโอออนดีมานด์ (Video On Demand)

ในการใช้งาน แอพพลิเคชั่น ที่ใช้งานบนโปรโตคอล TCP นั้นจะมีการสร้างการเชื่อมต่อในการส่งข้อมูลเนื่องจากเป็นโปรโตคอลแบบคอนเนคชั่นโอเรียนเต็ด(Connection Oriented) สามารถทำให้เราทราบปริมาณการใช้งานของแอพพลิเคชั่นเหล่านั้นได้โดยการดูที่ปริมาณ การเชื่อมต่อ (Connection) ที่เกิดขึ้น

5.1 World Wide Web (WWW)

เป็นแอพพลิเคชั่นที่ใช้ในการค้นหาข้อมูลผ่านทางระบบเครือข่ายระยะไกลที่ทำงานบนโปรโตคอHTTP และ TCP/IP แบบ TCP โดยการติดต่อเพื่อใช้ WWW นั้นจะต้องมีการส่งข้อมูลผ่านทางเข้าสู่เครือข่ายของเราทางใดทางหนึ่งซึ่งส่วนใหญ่จะเป็น เกตเวย์(Gateway) ของแต่ละเครือข่าย โดยการใช้งานนั้นจะใช้เวบเบราเซอร์(Web Browser) ซึ่งก็คือ แอพพลิเคชั่นที่ใช้งาน WWW ซึ่งมีความสามารถทั้งการรับส่งแฟ้มข้อมูล และ การส่งข้อความในรูปของจดหมายอิเลคทรอนิค

จุดประสงค์ในการบริหาร

1.ในการใช้งานมีความเร็วที่เพียงพอต่อการใช้งาน เมื่อมีการใช้งานในทุกๆเครื่องในเครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การบริหาร

1. ทำการมอนิเตอร์(Monitor) การใช้งานและความหนาแน่นของข้อมูลที่ผ่าน เกตเวย์(Gateway) โดยทำการมอนิเตอร์ จากการดูยูทิไลเซชั่น(Utilization) ของสายเชื่อมต่อที่ต่อกับเกตเวย์นั้นเมื่อมีการพบว่ามีความหนาแน่นของข้อมูลสูงมาก จะทำการแก้ไขโดยการ เพื่อความจุของการส่งข้อมูลของสายเชื่อมต่อ, เปลี่ยน เกตเวย์ ให้มีความสามารถในการส่งผ่านข้อมูลได้มากขึ้น หรือ ทำการแบ่งส่วนเครือข่ายเป็นส่วนย่อยๆ
2. ทำการตรวจความหนาแน่นของข้อมูลในแลน(LAN) โดยการตรวจที่สายเชื่อมต่อระหว่างเครื่องเมื่อมีการพบความหนาแน่นของข้อมูล ทำการแก้ไขได้โดยเพิ่มความจุของการส่งข้อมูลของสายเชื่อมต่อ, เปลี่ยนโทโพโลยี(Topology) ของเครือข่าย หรือทำการแยกส่วนของเครือข่ายโดยใช้บริดจ์(bridge)
3. ทำการตรวจการใช้งานของผู้ใช้ในแต่ละโอสท์(Host) ว่ามีการใช้งานเป็นอย่างไร ถ้ามีการติดต่อเพื่อทำการใช้งานมากอาจทำการเพิ่มโฮสต์ และแบ่งผู้ใช้ไป

5.2 เอฟทีพี (FTP : File Transfer Program)

เป็นโปรแกรมในการรับส่งข้อมูลผ่านทางระบบเครือข่ายในรูปของแฟ้มข้อมูลโดยในส่วนนี้ไม่ได้เกี่ยวข้องกับการรับส่งแฟ้มข้อมูลที่ผ่านเวบเบราว์เซอร์ ซึ่งในส่วนนี้การทำงานจะเป็นลักษณะที่เป็นโปรแกรมที่ใช้ในการรับส่งแฟ้มข้อมูลโดยเฉพาะที่ทำงานบนโปรโตคอลเอฟทีพี (FTP) ซึ่งมีการทำงานที่เป็นแบบคอนเนคชั่นโอเรียนเต็ดของทีซีพี โดยจุดประสงค์ของเอฟทีพี คือ ทำการใช้ไฟล์และข้อมูลร่วมกัน ,ป้องกันผู้ใช้จากการเปลี่ยนแปลงระบบการจัดเก็บไฟล์ และ ทำการส่งข้อมูลโดยมีความเชื่อถือได้และมีประสิทธิภาพ ซึ่งใช้การใช้งานได้โดยตรงจากผู้ใช้ที่เครื่องเทอมินอล

จุดประสงค์ในการบริหาร

1. ทำการรับส่งแฟ้มข้อมูลได้รวดเร็วและมีความถูกต้องในข้อมูล
2. สามารถทำการเอฟทีพีได้สะดวกเช่น มีพื้นที่ของฮาร์ดดิสค์(HardDisk) เพียงพอ ,มีโปรแกรมที่สามารถเอฟทีพีได้สะดวกและอยู่บนระบบปฏิบัติการที่มีอยู่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การบริหาร

1. มีการตรวจสอบการใช้งานของสายเชื่อมต่อ
2. ทำการตรวจสอบพื้นที่ของฮาร์ดดิสค์ ในระบบ
3. ทำเอฟทีพีไซต์(FTP Site) ขึ้นมาภายในองค์กรเนื่องจากการส่งข้อมูลมีความเร็วสูงและไม่ทำให้เสียความจุของสายเชื่อมต่อในการใช้งานเอฟทีพีไปในการเชื่อมต่อผ่านเครือข่ายระยะไกล

5.3 เทลเน็ท (Telnet) หรือรีโหมดแอกซ์เซส (Remote Access)

เป็นโปรแกรมในการทำการติดต่อล็อกอินระยะไกล(remote login) กับโอสท์ทีซีพีไอพี ที่เรามีบัญชี่ชื่อ(account) อื่นๆ โดยเป็นเวอร์ชวลเทอร์มินอล(virtual terminal) อิสระ เหมือนกับเป็นการติดต่อส่วนท้องถิ่น การทำงานของเทลเน็ทเป็นการทำงานแบบฟลู-ดูเพลกซ์(full duplex)

จุดประสงค์ในการบริหาร

1. ทำการติดต่อกับHostอื่นๆได้ง่ายและมีการตอบสนองที่รวดเร็ว
2. มีความปลอดภัยในการติดต่อต่อผู้ใช้และโอสท์

การบริหาร

1. ทำการตรวจการใช้งานของสายเชื่อมต่อว่ามีการใช้งานมากหรือไม่โดยจะพิจารณาที่สายเชื่อมต่อภายในจนถึงเราท์เตอร์ถ้าเกิดการแออัดของข้อมูลที่ภายนอกเครือข่ายเราไม่สามารถทำการแก้ไขได้แต่ถ้าการแออัดของข้อมูลเกิดขึ้นภายในก็ควรจะเปลี่ยนอุปกรณ์หรือเพิ่มช่องทางในการติดต่อ
2. ทำการตรวจการใช้งานแอพพลิเคชั่นบนเครื่องเซิร์ฟเวอร์ว่ามีการใช้งานมากหรือไม่ ถ้าการติดขัดของข้อมูลเกิดเนื่องจากการใช้งานบนเซิร์ฟเวอร์ก็ควรจะเพิ่มเครื่องเซิร์ฟเวอร์และ แบ่งผู้ใช้เพื่อลดภาระการทำงาน
3. ในการรักษาความปลอดภัยนี้เป็นการรักษาความปลอดภัยจากการtelnetเข้ามายังเครือข่ายของเรา เครือข่ายควรจะมีการเข้ารหัสข้อมูลเมื่อมีการloginเข้ามาใช้จากการเทลเน็ทซึ่งจะมีการส่งข้อมูลของผู้ใช้และรหัสผ่านผ่านตามเครือข่ายที่ง่ายต่อการกระทำอันตรายต่อข้อมูลและเครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.4 จดหมายอิเลคทรอนิค (E-Mail)

เป็นโปรแกรมที่ทำการส่งจดหมายอิเลคทรอนิคโดยจะมีการส่งผ่านไปที่ตู้ไปรษณีย์(mailbox) ของเครื่องเซิร์ฟเวอร์ของเครือข่ายเราเพื่อทำการส่งผ่านไปยังจุดหมายปลายทาง ในกรณีเดียวกันเมื่อเราเป็นฝ่ายรับเซิร์ฟเวอร์เมื่อได้รับจดหมายมาแล้วก็จะทำการเก็บไว้และส่งไปยังที่ตู้ไปรษณีย์ของแต่ละคน

จุดประสงค์ในการบริหาร

1. สามารถรับ-ส่งจดหมายอิเลคทรอนิคได้

การบริหาร

1. ทำการตรวจสอบปริมาณจดหมายอิเลคทรอนิคในตู้ไปรษณีย์ ถ้ามีจำนวนมากแล้วจะทำให้เปลืองเนื้อที่ของฮาร์ดดิสค์ของเซิรฟ์เวอร์และเมื่อทำการส่งจดหมายอิเลคทรอนิคออกจากเครื่องเซิร์ฟเวอร์จะใช้เวลาในการประมวลผลมาก ดังนั้นควรจะทำการตรวจสอบว่ามีผู้ใช้คนใดที่ทำการรับส่งจดหมายอิเลคทรอนิคเป็นจำนวนเท่าใดโดยการตรวจที่เฮดเดอร์ของจดหมายแล้วทำการสร้างmailboxที่เซิร์ฟเวอร์อื่นแล้วแบ่งผู้ใช้ให้ไปใช้ตู้ไปรษณีย์ที่สร้างใหม่นั้น
2. ทำการตรวจสอบการทำส่งต่อจดหมาย(forward mail) ของผู้ใช้ว่ามีการทำการส่งต่อแบบวนหรือไม่

5.5 การประชุมทางไกล (Video Conference)

เป็นโปรแกรมที่ทำการส่งข้อมูลมัลติมีเดีย(Multimedia) โดยส่งทั้งภาพเคลื่อนไหว ,เสียง และข้อมูลในรูปอื่นๆผ่านทางระบบเครือข่ายระยะไกลเพื่อใช้ในการติดต่อสื่อสารโดยจะมีการส่งข้อมูลผ่านเครือข่ายโดยตรงในกรณีที่ทำการติดต่อกันเพียง 2 เครื่องแต่ถ้ามีมากกว่า 2 จะมีการส่งข้อมูลผ่านรีเฟลกเตอร์(reflector)เพื่อให้ส่งต่อไปยังเครื่องอื่นๆให้มีการติดต่อได้

จุดประสงค์ในการบริหาร

1. ทำการติดต่อสื่อสารได้โดยไม่ติดขัดและรวดเร็ว
2. ทำการสื่อสารโดยมีความปลอดภัยของข้อมูล

การบริหาร

1. ทำการตรวจสอบการส่งข้อมูลในสายเชื่อมต่อในเครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2. ทำการตรวจสอบที่รีเฟลกเตอร์ว่ามีการใช้ความจุของสายเชื่อมต่อเป็นอย่างไร
3. ทำการตรวจสอบที่รีเฟลกเตอร์ว่ามีการใช้งานของซีพียู(CPU) ว่าเป็นอย่างไร
4. ทำการจำกัดผู้ใช้เพื่อไม่ให้มีการใช้ความจุของสายเชื่อมต่อมากจนเกิดการแออัดของข้อมูล ซึ่งบางแอพพลิเคชั่นก็จะจำกัดผู้ใช้ไว้ด้วย
5. ทำการเข้ารหัสข้อมูลที่ส่งผ่านเครือข่ายทั้งภายในและส่งออกไปเครือข่ายระยะไกล

5.6 วีดีโอออนดีมานด์ (Video On Demand)

เป็นแอพพลิเคชั่นที่ทำการส่งข้อมูลมัลติมีเดียผ่านเครือข่ายจากเครื่องเซิร์ฟเวอร์ไปยังกลุ่มของเครื่องไคลเอนต์โดยมีการส่งข้อมูลมัลติมีเดียนั้นผ่านเครือข่าย และมีการติดต่อแบบ 2 ทางกับผู้ใช้คือมีการตอบโต้กับผู้ใช้

จุดประสงค์ในการบริหาร

1. สามารถรับข้อมูลมัลติมีเดียได้อย่างไม่ติดขัด

การบริหาร

1. ทำการตรวจสอบการใช้งานของสายเชื่อมต่อและอุปกรณ์ในการส่งข้อมูลว่ามีการใช้งานมากหรือไม่ ถ้าเกิดการติดขัดเนื่องจากการส่งแล้วก็จะทำการเพิ่มความจุของสายเชื่อมต่อหรือลดจำนวนผู้ใช้(ทำการแบ่งผู้ใช้หรือแบ่งเครือข่าย)เพื่อให้มีการส่งข้อมูลลดลง
2. ถ้าเป็นการทำวีดีโอออนดีมานด์ ภายในเครือข่ายการส่งข้อมูลที่ช้าหรือติดขัดนั้นอาจเกิดจากการทำงานของเครื่องเซิร์ฟเวอร์ได้ การแก้ไขทำโดยการแบ่งผู้ใช้ออกเป็นกลุ่มและเพิ่มจำนวนเซิร์ฟเวอร์

5.7 การติดต่อแบบออนไลด์ทรานแซกชั่น (Online Transaction)

การติดต่อแบบออนไลด์ทรานแซกชั่น คือการติดต่อสื่อสารที่มีการตอบสนองกันของทั้งสองฝ่ายในการทำงานหนึ่งๆ เช่น การถอนเงินผ่านเครื่องถอนเงินอัตโนมัติ(ATM) ,ระบบการจำหน่ายตั๋ว ,ระบบสั่งซื้อผ่านเครือข่าย เป็นต้น โดยส่วนใหญ่เป็นเครือข่ายเฉพาะ

จุดประสงค์ในการบริหาร

1. ทำการสื่อสารข้อมูลได้อย่างไม่ติดขัดและมีการตอบสนองที่รวดเร็ว

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2. ทำการสื่อสารข้อมูลโดยมีความปลอดภัยสูง

การบริหาร

1. ตรวจสอบการเชื่อมต่อและสายเขื่อมต่อว่าสามารถใช้งานได้หรือไม่
2. ทำการเข้ารหัสข้อมูลที่ทำการส่ง

5.8 สรุป

การใช้งานแอพพลิเคชั่นบนอินเทอร์เนทบนเครือข่ายนี้ส่วนใหญ่แล้วจะมีการบริหารเครือข่ายที่ใช้แอพพลิเคชั่นเหล่านี้หลักๆ 2 ด้านคือ

1. ด้านประสิทธิภาพของเครือข่าย โดยมักจะทำการตรวจสอบการใช้งานของสายเชื่อมต่อของระบบเครือข่ายหรือการทำงานของเครื่องเซิร์ฟเวอร์ที่ทำงานด้านนั้นๆ และโดยปกติแล้วการวัดการใช้งานของสายส่งก็จะมีแอพพลิเคชั่นที่ทำการวัดและสามารถกำหนดขีดจำกัด(treshold) ของสายเชื่อมต่อได้เพื่อทำการเตือนเมื่อมีการใช้งานมากๆ
2. ด้านความปลอดภัยของเครือข่าย โดยเครือข่ายในปัจจุบันจะมีการใช้ firewall ในการป้องกันการทำอันตรายจากอินเทอร์เนท และมีการป้องกันเครือข่ายตามปกติเช่น การทำแอกเซสล็อก(Access log) ,การตรวจสอบการทำงานหรือการใช้ทรัพยากรของผู้ใช้ ,การตรวจสอบข้อบกพร่องของระบบปฏิบัติการจากผู้ผลิตและแหล่งข้อมูลอื่นๆ ส่วนด้านความปลอดภัยของข้อมูลที่ทำการส่งออกไปความปลอดภัยขึ้นอยู่กับความสามารถด้านการรักษาความปลอดภัยของซอฟท์แวร์ที่ใช้ว่ามีการเข้ารหัสข้อมูลหรือไม่

ส่วนในด้านอื่นๆ เช่น ด้านความผิดพลาดนั้นส่วนใหญ่เกิดจากเครือข่ายที่เราติดต่อด้วยซึ่งเราไม่มีสิทธิในการบริหาร แต่ความผิดพลาดของเครือข่ายเรานั้นก็จะทำการแก้ไขปัญหาตามปกติของเครือข่ายทั่วๆไป ด้านคอนฟิกูเรชั่น(configuration) ก็จะทำการหาซอฟท์แวร์ใหม่ๆที่มีความสามารถสูงมาใช้ในองค์กรรวมทั้งการติดตั้งอุปกรณ์และปรับปรุง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 6

การทดลอง และ ผลการทดลอง

เนื่องด้วยระบบการจัดการ แบ่งออกเป็น 5 ฟังก์ชั่นการทำงานหลัก เราจึงได้เลือกการทดลองตามหัวข้อการทำงานเหล่านั้นโดยเราได้ทำการเลือกสถานที่ทำการทดลองเป็นสองที่ คือ ภาควิชาคอมพิวเตอร์ และ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

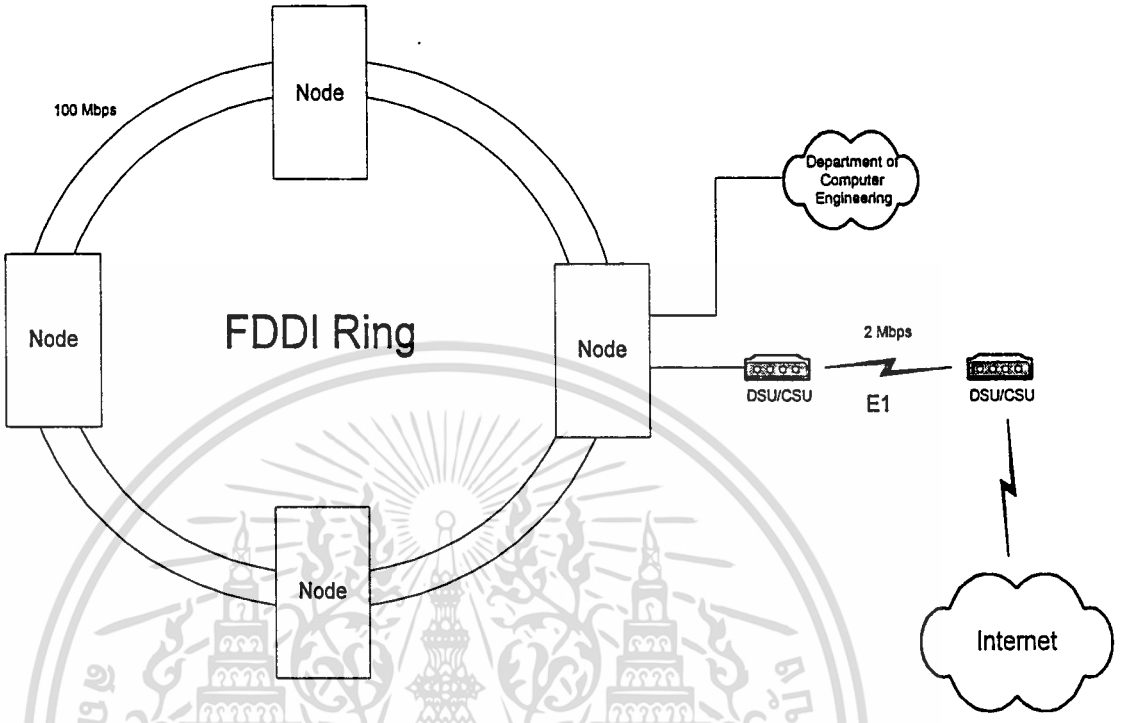
โดยในส่วนของภาควิชาคอมพิวเตอร์ เราได้ทำการแบ่งการบริหารระบบออกเป็น 2 หัวข้อหลัก ๆ ดังต่อไปนี้คือ

6.1 คอนฟิกกูเรชั่น (Configuration)

ในส่วนนี้เราได้ทำการเก็บรวบรวมข้อมูลมาจากผู้บริหารภาคคอมพิวเตอร์ และ ผู้บริหารของศูนย์วิจัยคอมพิวเตอร์ (ห้องเซิร์ฟเวอร์เจ้าคุณ) แล้วนำมาเปรียบเทียบกับที่เราได้จากการ สังเกตุจากแผนที่ของ OpenView จะพบได้ว่าความละเอียดเพิ่มขึ้นมากกว่าการรับฟังข้อมูลจาก ผู้บริหารระบบเพียงอย่างเดียว, เห็นภาพพจน์ชัดเจนยิ่งขึ้น (รูปธรรมมากขึ้น) มีผลการทดลองดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6.1.1 รายละเอียดของระบบเครือข่ายสถาบันและภาควิชาวิศวกรรมคอมพิวเตอร์

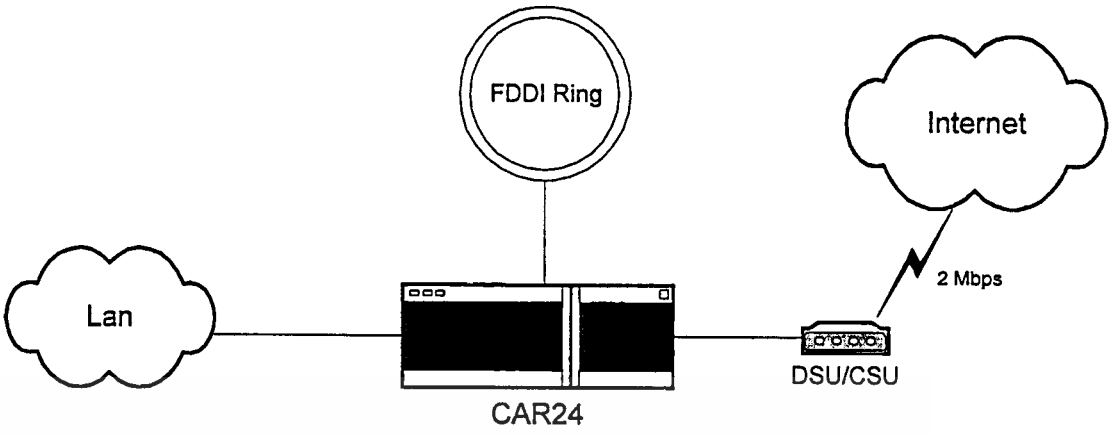


รูปที่ 6.1 แสดงระบบการเชื่อมต่อของเครือข่ายของสถาบัน

ภายในสถาบันได้มีโหนด(node) สำหรับระบบเครือข่ายอยู่ด้วยกันทั้งหมด 4 โหนด โดยที่แต่ละโหนดนั้นก็จะต่อไปยังเครือข่ายย่อยต่าง ๆ ของแต่ละสถานที่ โดยที่ระหว่างโหนดนั้นเชื่อมต่อกันด้วยเคเบิ้ลใยแก้วนำแสง ตามสถาปัตยกรรมแบบเอฟดีดีไอ(FDDI) ซึ่งมีความเร็วของอัตราส่งผ่านข้อมูลอยู่ที่ประมาณ100 ล้านบิตต่อวินาที

โหนดที่เราสนใจนั้น คือโหนดที่ตั้งอยู่ที่ตึกคอมพิวเตอร์ ดังแสดงในรูปคือตู้เราท์เตอร์ซึ่งจะประกอบไปด้วยเราท์เตอร์ 4 ตัว แต่ละตัวจะมีอยู่ 3 พอร์ท และทุกตัวจะมีอยู่ 1 พอร์ทที่ใช้เชื่อมต่อเข้ากับเอฟดีดีไอ หมายความว่า จะมีพอร์ทเหลืออยู่ 2 พอร์ทของเราท์เตอร์แต่ละตัว

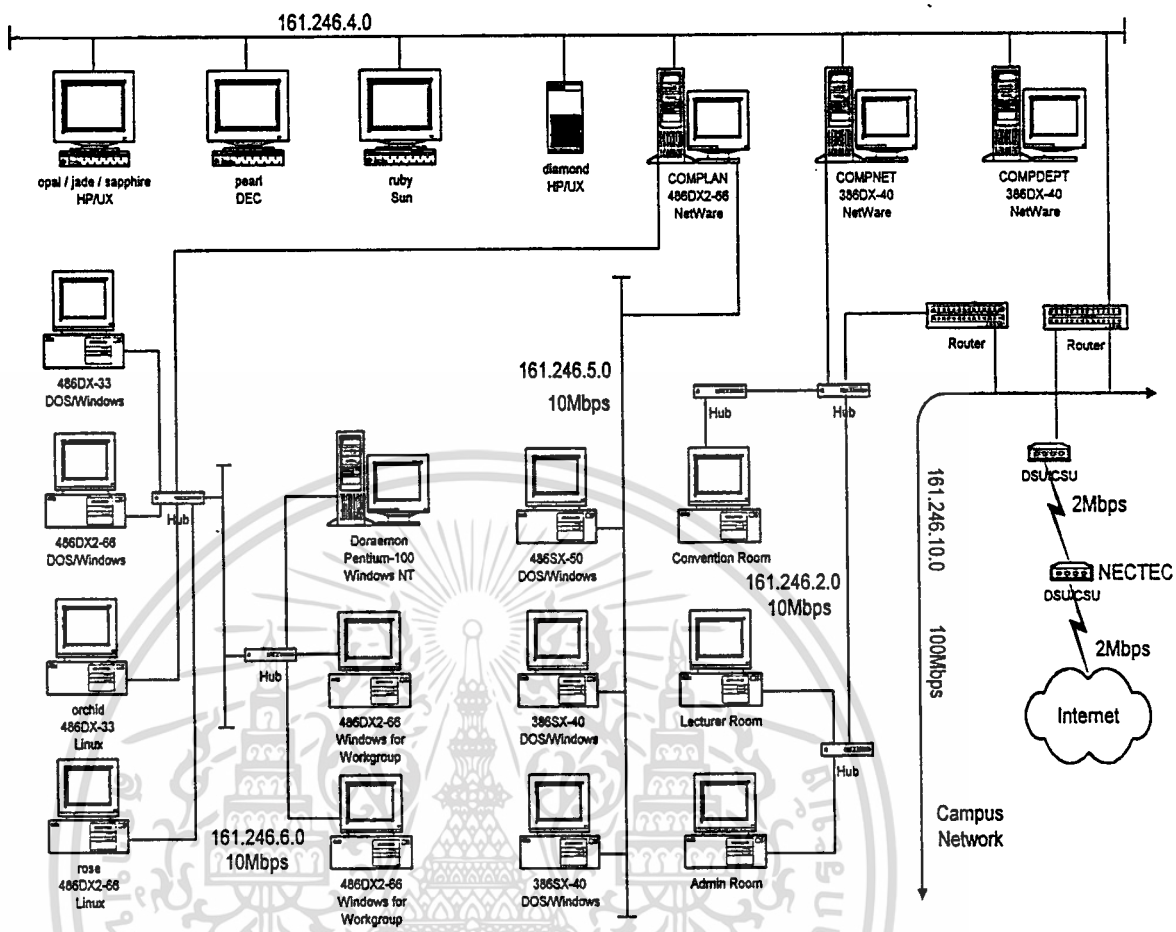
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 6.2 แสดงตัวอย่างเราท์เตอร์ CAR24

ชื่อของเราท์เตอร์ในโหนดนี้คือ CAR21,CAR22,CAR23 และ CAR24 เราจะสนใจเฉพาะ CAR24 เท่านั้น เนื่องจากเป็นจุดที่เครือข่ายของภาควิชาต่อเชื่อมอยู่ และที่ CAR24 นี้มีพิเศษอยู่อีกก็คือ จะใช้เชื่อมต่อเข้ากับโมเด็มที่จะต่อไปที่ศูนย์เทคโนโลยีอิเลคโทรนิคและคอมพิวเตอร์แห่งชาติ หรือที่เรียกว่าเนคเทค(NECTEC : National Electronics and Computer Technology Center) ซึ่งมีตัวเดียวเท่านั้นของสถาบัน หมายความว่าจุดที่จะต่อออกไปอินเทอร์เน็ทก็คือออกทางเราเตอร์ที่ชื่อ CAR24 โดยผ่านที่ NECTEC นั้นเอง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 6.3 แสดงระบบเครือข่ายของภาควิชาวิศวกรรมคอมพิวเตอร์

ดังที่กล่าวมาแล้วว่าพอร์ทของ CAR24 นั้น พอร์ทหนึ่งจะต่อเข้ากับ FDDI , พอร์ทหนึ่งต่อเข้ากับอินเทอร์เน็ท และอีกพอร์ทหนึ่งจะต่อเข้ากับเครือข่ายของภาควิชาคอมพิวเตอร์ ตรงนี้จะใช้สายโคแอกเชี่ยลเดินออกมาเชื่อมต่อไปยังโฮสต่าง ๆ สำหรับ Complan นั้นจะมีฮับต่อออกมาไปที่ห้องคอมพิวเตอร์ใหญ่ และห้องเพ็นเทียม ตรงนี้เป็นสายยูทีพี(UTP) ซึ่งจะมี IP address เป็น 161.246.6 และจะมีสายต่อจากฮัพที่เป็นโคแอกเชี่ยลเข้าไปที่ห้อง isonet

สำหรับระบบแลนในภาคคอมพิวเตอร์ที่เป็นไอพีแอดเดรสเบอร์ 161.246.6 ซึ่งจะเป็นเครื่องในห้องคอมพิวเตอร์ใหญ่,เครื่องในห้องเพ็นเทียมและเครื่องในห้องไอโซเนท จะเป็นสถาปัตยกรรมแบบ ฟิสิคอลสตาร์ลอจิกคอลริง(physical star-logical ring)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6.2 การบริหารเครื่องเซิร์ฟเวอร์ที่ให้บริการเกี่ยวกับแอพพลิเคชั่นอินเทอร์เน็ต

ในส่วนนี้เนื่องจากเราได้เลือกแอพพลิเคชั่นที่จะทำการจัดการบริหาร คือ แอพพลิเคชั่นเกี่ยวกับอินเทอร์เน็ต เช่น ftp, http, telnet, finger และ mail โดยเรายึดหลักการข้อที่ว่าแอพพลิเคชั่นทุกอย่างที่มีการส่งผ่านข้อมูลหรือ แพ็คเก็ตของมันข้ามออกจากระบบเครือข่ายแบบแลน เราถือว่าเป็นแอพพลิเคชั่นเกี่ยวกับอินเทอร์เน็ตทั้งหมดดังนั้นเราจึงต้องทำการเก็บรวบรวมข้อมูลเพื่อทำการบริหารจาก เครื่องที่ทำหน้าที่เป็นเซิร์ฟเวอร์ ซึ่งก็คือเครื่อง diamond นั่นเอง

ข้อสังเกตุ ลักษณะที่เหมือนกันสำหรับการบริหารระบบเครือข่ายไม่ว่า ระบบนั้นจะมีลักษณะเป็นอย่างไร ใหญ่หรือเล็กแตกต่างกัน ทำการบริหารแอพพลิเคชั่นใด ๆก็ตาม จะมีหลักที่เหมือนกันในบริหารก็คือการตรวจสอบอุปกรณ์ที่ทำการต่อจากภายนอก เข้ามาสู่ภายในของระบบเครือข่ายนั้นเช่น ในกรณีของการบริหารระบบเครือข่ายของภาคคอมพิวเตอร์นั้น เราก็ต้องทำการตรวจสอบเริ่มจาก โมเด็ม ที่ทำการต่อไปยัง NECTEC โดยต่อเข้ากับเราท์เตอร์ที่ตั้งอยู่ในภาควิชาคอมพิวเตอร์ คือเราท์เตอร์เบอร์ 161.246.10.11 หรือ CAR24 นั่นเอง => สายที่ต่อระหว่างตัวเราท์เตอร์และโมเด็มจาก NECTEC => ตัวเราท์เตอร์ CAR24 => สายที่ต่อจากเราท์เตอร์ไปยังเครื่องเซิร์ฟเวอร์ (diamond) => เครื่องเซิร์ฟเวอร์ => สายที่ต่อจากเซิร์ฟเวอร์ไปยังเครื่อง terminal => เครื่องหรืออุปกรณ์ฮาร์ดแวร์ที่อยู่ปลายทาง => การตั้งค่าระบบของซอร์ฟแวร์

6.3 ผลจากการทดลองบริหารเครือข่าย

สำหรับเนื้อหาในส่วนการทดลองนี้ เราได้แบ่งออกเป็นส่วนย่อย ๆ 3 ส่วนดังต่อไปนี้

- ข้อมูลในการทดลอง(DATA)
- รายละเอียดการตรวจสอบ(MONITORING)
- การวิเคราะห์ข้อมูล (ANALYSIS)

6.3.1 ข้อมูลการทดลอง (DATA)

ในส่วนของข้อมูลที่เกี่ยวข้องกับการทดลองนี้เราก็ได้ทำการเก็บข้อมูลตามที่เรากำหนดว่าจะทำการทดลอง ใด ๆ ข้อมูลเหล่านี้เป็นข้อมูลในช่วงเวลาหนึ่งเปลี่ยนแปลงได้ตลอดเวลา ซึ่งก็คือข้อมูลเกี่ยวกับเครื่องเซิร์ฟเวอร์, gateway และ เราท์เตอร์ ที่เกี่ยวข้องภายในขอบข่ายการทดลองของเรา ดังต่อไปนี้

6.3.1.1 เครื่อง diamond

เป็นเครื่องเซิร์ฟเวอร์ภายในภาควิชาของเราเครื่องหนึ่ง ซึ่งเกี่ยวกับแอพพลิเคชั่นที่เราจะทำการบริหาร มีรายละเอียดของมูลดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จำนวนแพ็คเก็ตต่อวินาที

xnmgraph ascii dump to /tmp/traf43.data on 05/15/96 19:29:28

ran with 10 arguments:

/usr/OV/bin/xnmgraph -title Monitor: Interface Traffic -units Packets / Sec -helpFile ovip/OVW/Functions/netIfTraffic -mib .1.3.6.1.2.1.2.2.1.11:Packets Received::.1.3.6.1.2.1.2.2.1.3:^[^1]$|^1.$|^2[^4]$|^[3-9].$:.1.3.6.1.2.1.2.2.1.2:::,.1.3.6.1.2.1.2.2.1.14:Errors Received::.1.3.6.1.2.1.2.2.1.3:^[^1]$|^1.$|^2[^4]$|^[3-9].$:.1.3.6.1.2.1.2.2.1.2:::,.1.3.6.1.2.1.2.2.1.17:Packets Transmitted::.1.3.6.1.2.1.2.2.1.3:^[^1]$|^1.$|^2[^4]$|^[3-9].$:.1.3.6.1.2.1.2.2.1.2:::,.1.3.6.1.2.1.2.2.1.20:Errors Transmitted::.1.3.6.1.2.1.2.2.1.3:^[^1]$|^1.$|^2[^4]$|^[3-9].$:.1.3.6.1.2.1.2.2.1.2:: 161.246.4.3

#

mibSpec: .1.3.6.1.2.1.2.2.1.11:Packets Received::.1.3.6.1.2.1.2.2.1.3:^[^1]$|^1.$|^2[^4]$|^[3-9].$:.1.3.6.1.2.1.2.2.1.2:::,.1.3.6.1.2.1.2.2.1.14:Errors Received::.1.3.6.1.2.1.2.2.1.3:^[^1]$|^1.$|^2[^4]$|^[3-9].$:.1.3.6.1.2.1.2.2.1.2:::,.1.3.6.1.2.1.2.2.1.17:Packets Transmitted::.1.3.6.1.2.1.2.2.1.3:^[^1]$|^1.$|^2[^4]$|^[3-9].$:.1.3.6.1.2.1.2.2.1.2:::,.1.3.6.1.2.1.2.2.1.20:Errors Transmitted::.1.3.6.1.2.1.2.2.1.3:^[^1]$|^1.$|^2[^4]$|^[3-9].$:.1.3.6.1.2.1.2.2.1.2:::

ข้อมูลของกราฟที่เก็บอยู่ในไฟล์

the graph can be re-created using a command like:

cat /tmp/traf43.data | /usr/OV/bin/xnmgraph -title "Monitor: Interface Traffic" -units "Packets / Sec" -helpFile ovip/OVW/Functions/netIfTraffic -mib "-1:Packets Received:::::::161.246.4.3,-2:Errors Received:::::::161.246.4.3,-3:Packets Transmitted:::::::161.246.4.3,-4:Errors Transmitted:::::::161.246.4.3,"

#

displayWidth: 1h endTime: 05/15/96 19:29:12

resolution by data

#

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

y-axis scaling by entire data set

ข้อมูลกราฟเส้นที่ 1 ของจำนวนแพ็กเก็ต

####################

line 1: (161.246.4.3 Packets Received.lan0) 139 points

139 points representing 10.94h

starting Wed May 15 08:29:50.0 1996 ending Wed May 15 08:30:00.0 1996

MIB: ".1.3.6.1.2.1.2.2.1.11"

instance: "4"

####################

#line	start	stop	min	avg	max
#----	---------	---------	-----	-----	-----
1	832123790	832123800	30.4407	30.4407	30.4407
1	832123800	832123810	0	0	0
1	832123810	832123820	0	0	0
1	832123820	832123830	31.3429	31.3429	31.3429
1	832123830	832123840	0	0	0
1	832123840	832123850	0	0	0
1	832123850	832123860	34.2863	34.2863	34.2863
1	832123860	832123870	0	0	0
1	832123870	832124170	10.8763	10.8763	10.8763

ข้อมูลกราฟเส้นที่ 2 ของจำนวนแพ็กเก็ต

####################

line 2: (161.246.4.3 Errors Received.lan0) 2 points

2 points representing 10.94h

starting Wed May 15 08:29:50.0 1996 ending Wed May 15 08:30:00.0 1996

MIB: ".1.3.6.1.2.1.2.2.1.14"

instance: "4"

####################

#line	start	stop	min	avg	max

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

#----	---------	---------	-----	-----	-----
2	832123790	832123800	0	0	0
2	832123800	832163172	0	0	0

ข้อมูลกราฟเส้นที่ 3 ของจำนวนแพ็กเก็ต

####################

line 3: (161.246.4.3 Packets Transmitted.lan0) 139 points

139 points representing 10.94h

starting Wed May 15 08:29:50.0 1996 ending Wed May 15 08:30:00.0 1996

MIB: ".1.3.6.1.2.1.2.2.1.17"

instance: "4"

####################

#line	start	stop	min	avg	max
#----	---------	---------	-----	-----	-----
3	832123790	832123800	44.8681	44.8681	44.8681
3	832123800	832123810	0	0	0
3	832123810	832123820	0	0	0
3	832123820	832123830	49.7651	49.7651	49.7651
3	832123830	832123840	0	0	0
3	832123840	832123850	0	0	0
3	832123850	832123860	53.8709	53.8709	53.8709

จำนวนออกเตตเข้า (InOctets) ต่อวินาที

xnmgraph ascii dump to /tmp/inoc43.data on 05/15/96 19:32:01

ran with 3 arguments:

/usr/OV/bin/xnmgraph -mib .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets::::::::161.246.4.3

#

mibSpec: .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets::::::::161.246.4.3

#

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
# the graph can be re-created using a command like:
# cat /tmp/inoc43.data | /usr/OV/bin/xnmgraph -mib "-1:ifInOctets:::::::161.246.4.3,-
2:ifInOctets:::::::161.246.4.3,-3:ifInOctets:::::::161.246.4.3,-4:ifInOctets:::::::161.246.4.3,"
#
#
# displayWidth: 1h endTime: 05/15/96 19:31:45
# resolution by data
#
# y-axis scaling by displayed data
####################
# line 1: (161.246.4.3 ifInOctets.1) 2 points
# 2 points representing 10.45h
# starting Wed May 15 09:01:44.0 1996 ending Wed May 15 09:01:54.0 1996
# MIB: ".1.3.6.1.2.1.2.2.1.10"
# instance: "1"
####################
#line      start       stop        min         avg         max
#----     ---------   ---------   -----       -----       -----
  1       832125704   832125714   0           0           0
  1       832125714   832163325   0           0           0
####################
# line 2: (161.246.4.3 ifInOctets.2) 2 points
# 2 points representing 10.45h
# starting Wed May 15 09:01:44.0 1996 ending Wed May 15 09:01:54.0 1996
# MIB: ".1.3.6.1.2.1.2.2.1.10"
# instance: "2"
####################
#line      start       stop        min         avg         max
#----     ---------   ---------   -----       -----       -----
  2       832125704   832125714   0           0           0
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2 832125714 832163325 0 0 0

####################

line 3: (161.246.4.3 ifInOctets.3) 2 points

2 points representing 10.45h

starting Wed May 15 09:01:44.0 1996 ending Wed May 15 09:01:54.0 1996

MIB: ".1.3.6.1.2.1.2.2.1.10"

instance: "3"

####################

#line	start	stop	min	avg	max
#----	---------	---------	-----	-----	-----
3	832125704	832125714	0	0	0
3	832125714	832163325	0	0	0

จำนวนออกเตตออก(OutOctets)ต่อวินาที

xnmgraph ascii dump to /tmp/outoc43.data on 05/15/96 19:32:30

ran with 3 arguments:

/usr/OV/bin/xnmgraph -mib .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets::::::::161.246.4.3

#

mibSpec: .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets::::::::161.246.4.3

#

the graph can be re-created using a command like:

cat /tmp/outoc43.data | /usr/OV/bin/xnmgraph -mib "-1:ifOutOctets::::::::161.246.4.3,-2:ifOutOctets::::::::161.246.4.3,-3:ifOutOctets::::::::161.246.4.3,-4:ifOutOctets::::::::161.246.4.3,"

#

#

displayWidth: 1h endTime: 05/15/96 19:31:01

resolution by data

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
#
# y-axis scaling by displayed data
####################
# line 1: (161.246.4.3 ifOutOctets.1) 2 points
# 2 points representing 10.43h
# starting Wed May 15 09:02:20.0 1996 ending Wed May 15 09:02:30.0 1996
# MIB: ".1.3.6.1.2.1.2.2.1.16"
# instance: "1"
####################
```

#line	start	stop	min	avg	max
#----	---------	---------	-----	-----	-----
1	832125740	832125750	0	0	0
1	832125750	832163281	0	0	0

```
####################
# line 2: (161.246.4.3 ifOutOctets.2) 2 points
# 2 points representing 10.43h
# starting Wed May 15 09:02:20.0 1996 ending Wed May 15 09:02:30.0 1996
# MIB: ".1.3.6.1.2.1.2.2.1.16"
# instance: "2"
####################
```

#line	start	stop	min	avg	max
#----	---------	---------	-----	-----	-----
2	832125740	832125750	0	0	0
2	832125750	832163281	0	0	0

```
####################
# line 3: (161.246.4.3 ifOutOctets.3) 2 points
# 2 points representing 10.43h
# starting Wed May 15 09:02:20.0 1996 ending Wed May 15 09:02:30.0 1996
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

MIB: ".1.3.6.1.2.1.2.2.1.16"

instance: "3"

####################

#line	start	stop	min	avg	max
#----	---------	---------	-----	-----	-----
3	832125740	832125750	0	0	0
3	832125750	832163281	0	0	0

การเชื่อมต่อทีซีพีไอพี(TCP/IP)

Title: TCP Connection Table : 161.246.4.3

Name or IP Address: 161.246.4.3

Local Address	Remote Address	(state)
161.246.4.3.ftp-data	Chaokhun.47574	CLOSED-WAIT
161.246.4.3.ftp	Chaokhun.47503	CLOSED-WAIT
161.246.4.3.telnet	161.246.4.3.4740	CLOSED-WAIT
161.246.4.3.telnet	161.246.6.8.1025	CLOSED-WAIT
161.246.4.3.telnet	161.246.34.39.1086	CLOSED-WAIT
161.246.4.3.telnet	202.44.235.131.1447	CLOSED-WAIT
161.246.4.3.http	195.31.135.163.1154	TIME-WAIT
161.246.4.3.http	195.31.135.163.1184	TIME-WAIT
161.246.4.3.http	195.31.135.163.1191	TIME-WAIT
161.246.4.3.http	195.31.135.163.1194	TIME-WAIT
161.246.4.3.http	205.252.75.11.1407	TIME-WAIT
161.246.4.3.http	205.252.75.11.1412	TIME-WAIT
161.246.4.3.login	161.246.10.22.1014	CLOSED-WAIT
161.246.4.3.login	161.246.10.22.1021	CLOSED-WAIT
161.246.4.3.1126	202.44.144.53.6667	CLOSED-WAIT
161.246.4.3.1769	207.82.250.8.http	TIME-WAIT

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

161.246.4.3.1919 206.139.231.80.ftp CLOSED-WAIT

161.246.4.3.1961 206.139.231.80.ftp-data CLOSED-WAIT

161.246.4.3.2004 207.34.254.9.http TIME-WAIT

เนื้อที่ภายใน diamond

Title: Disk Space : 161.246.4.3

Name or IP Address: 161.246.4.3

Filesystem	kbytes	used	avail	capacity	Mounted on
/dev/dsk/c0t1d0	2037469	1688984	144738	92%	/users
/dev/dsk/c0t2d0	2037469	1476262	357460	81%	/dsk1
/dev/vg00/lvol1	299157	51102	218139	19%	/
/dev/vg00/lvol3	288157	85216	174125	33%	/tmp
/dev/vg00/lvol4	1033849	235750	694714	25%	/usr
/dev/vg00/lvol5	288157	72905	186436	28%	/var
/dev/vg01/lvol1	1976525	1603253	175619	90%	/dsk3
/dev/vg02/lvol1	103754	77853	15525	83%	/old/root
/dev/vg02/lvol3	483082	288329	146444	66%	/old/usr
/dev/vg02/lvol4	698826	290003	338940	46%	/dsk2

การใช้งานซีพียู (CPU)

xnmgraph ascii dump to /tmp/cpu43.data on 05/15/96 19:30:04

ran with 11 arguments:

/usr/OV/bin/xnmgraph -title Monitor: CPU Load -units Load Avg -hideMultiplier -helpFile ovhpux/OVW/Functions/HP.cpuLoad -mib .1.3.6.1.4.1.11.2.3.1.1.3:1 Min:0:::::.01:,.1.3.6.1.4.1.11.2.3.1.1.4:5 Min:0:::::.01:,.1.3.6.1.4.1.11.2.3.1.1.5:15 Min:0:::::.01: 161.246.4.3

#

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

mibSpec: .1.3.6.1.4.1.11.2.3.1.1.3:1 Min:0::::.01:,.1.3.6.1.4.1.11.2.3.1.1.4:5 Min:0::::.01:,.1.3.6.1.4.1.11.2.3.1.1.5:15 Min:0::::.01:

#

the graph can be re-created using a command like:

cat /tmp/cpu43.data | /usr/OV/bin/xnmgraph -title "Monitor: CPU Load" -units "Load Avg" -hideMultiplier -helpFile ovhpux/OVW/Functions/HP.cpuLoad -mib "-1:1 Min:::::::161.246.4.3,-2:5 Min:::::::161.246.4.3,-3:15 Min:::::::161.246.4.3,"

#

#

displayWidth: 1h endTime: 05/15/96 19:29:04

resolution by data

#

y-axis scaling by displayed data

####################

line 1: (161.246.4.3 1 Min) 133 points

133 points representing 10.84h

starting Wed May 15 08:35:32.0 1996 ending Wed May 15 08:35:42.0 1996

MIB: ".1.3.6.1.4.1.11.2.3.1.1.3"

instance: "0"

####################

#line	start	stop	min	avg	max
#----	---------	---------	-----	-----	-----
1	832124132	832124142	15	15	15
1	832124142	832124152	13	13	13
1	832124152	832124162	34	34	34
1	832124162	832124462	16	16	16
1	832124462	832124762	9	9	9
1	832124762	832125062	29	29	29
1	832125062	832125362	75	75	75
1	832125362	832125662	22	22	22

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1	832125662	832125962	5	5	5
1	832125962	832126262	1	1	1

######################

line 2: (161.246.4.3 5 Min) 133 points

133 points representing 10.84h

starting Wed May 15 08:35:32.0 1996 ending Wed May 15 08:35:42.0 1996

MIB: ".1.3.6.1.4.1.11.2.3.1.1.4"

instance: "0"

######################

#line	start	stop	min	avg	max
#----	---------	---------	-----	------	-----
2	832124132	832124142	22	22	22
2	832124142	832124152	22	22	22
2	832124152	832124162	26	26	26
2	832124162	832124462	26	26	26
2	832124462	832124762	21	21	21
2	832124762	832125062	32	32	32
2	832125062	832125362	58	58	58
2	832125362	832125662	51	51	51
2	832125662	832125962	25	25	25
2	832125962	832126262	13	13	13

######################

line 3: (161.246.4.3 15 Min) 132 points

132 points representing 10.84h

starting Wed May 15 08:35:32.0 1996 ending Wed May 15 08:35:42.0 1996

MIB: ".1.3.6.1.4.1.11.2.3.1.1.5"

instance: "0"

######################

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

#line	start	stop	min	avg	max
#----	---------	---------	-----	-----	-----
3	832124132	832124142	24	24	24
3	832124142	832124152	24	24	24
3	832124152	832124162	25	25	25
3	832124162	832124462	26	26	26
3	832124462	832124762	24	24	24
3	832124762	832125062	28	28	28
3	832125062	832125362	41	41	41
3	832125362	832125662	44	44	44
3	832125662	832125962	35	35	35
3	832125962	832126262	27	27	27

6.3.1..2 เครื่องเราท์เตอร์ 161.246.10.11 (CAR24) เป็นเครื่องเราท์เตอร์ที่ตั้งอยู่ภายในภาควิชาของเรา เป็นทางออกของข้อมูลทั้งหมด ภายในสถาบันของเรา รวมทั้งข้อมูลจากภาควิชาของเราด้วย มีรายละเอียดข้อมูลดังนี้

- **จำนวนแพ็คเก็ตต่อวินาที**
- **จำนวนออกเตตเข้า(InOctets)ต่อวินาที**
- **จำนวนออกเตตออก(OutOctets)ต่อวินาที**

6.3.2 รายละเอียดการตรวจสอบ(MONITORING)

6.3.2.1 เครื่องที่ทำการจัดการ

คือเครื่องที่เราสนใจในการจัดการซึ่งมีดังนี้

- Diamond (161.246.4.3) เป็นเครื่องเซิร์ฟเวอร์ที่เป็นเครื่องให้บริการแอพพลิเคชั่นอินเตอร์เน็ตตามที่ผู้ใช้ต้องการ
- Chaokhun (161.246.10.21) เป็นเครื่องที่เกาะติดอยู่บนวง FDDI เหมือนกัน
- CAR 24 (161.246.10.11) เป็นเครื่องเราท์เตอร์ที่ตั้งอยู่ภายในภาควิชาของเรา เป็นทางออกของข้อมูลทั้งหมด ภายในสถาบันของเรา รวมทั้งข้อมูลจากภาควิชาของเราด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6.3.2.2 แอพพลิเคชั่นที่ทำงานอยู่ในระบบเครือข่าย

การทำงานของแอพพลิเคชั่นบนระบบเครือข่าย ที่มาใช้บริการเครื่อง diamond ที่เราสนใจคืออินเตอร์เน็ตแอพพลิเคชั่น ได้แก่ WWW ,ftp ,telnet ,finger ที่ใช้กันเป็นส่วนใหญ่

6.3.2.3 site ที่ผู้ใช้ทำการติดต่อโดยใช้แอพพลิเคชั่นส่วนใหญ่

ในการใช้แอพพลิเคชั่นส่วนใหญ่ก็จะมีการใช้ WWW ซึ่งsiteที่ผู้ใช้ทำการติดต่อเพื่อทำการใช้งานมากๆมีดังนี้

- www.yahoo.com
- www.metacrawler.com
- www.download .com
- www.cdrom.com
- www.ibm.com
- www.hp.com
- www.realordio.com
- www.cisco.com
- www.microsoft.com
- ฯลฯ

ส่วนในการดาวน์โหลดไฟล์ผ่านอินเตอร์เน็ต เนื่องจากขนาดของไฟล์มีผลต่อการใช้งานสายเชื่อมต่อ ทำให้ต้องรับภาระหนักเพิ่มขึ้น โปรแกรมที่ทำการดาวน์โหลบ่อยครั้งมีดังนี้

- Microsoft Internet Explorer
- Network Security
- Winzip 32-bit
- McAfee Virus Scan for Windows 95
- Clean Sweep 32-bit
- Games
- Music song
- ฯลฯ

ในการใช้แอพพลิเคชั่น web browser นั้นการค้นหาข้อมูลโดยใช้ search engine เพื่อทำการค้นหาข้อมูลนั้นส่วนใหญ่จะมีการใช้ yahoo ,lycos เป็น search engine

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การใช้งาน telnet ก็ จะเป็นการติดต่อไปยังเครื่องเซิร์ฟเวอร์อื่นที่เรามี account สามารถทำการเข้าใช้ได้ ในการใช้งาน telnet ส่วนใหญ่ในภาควิชาวิศวกรรมคอมพิวเตอร์จะเป็นการติดต่อไปยังเครื่องดังนี้ Chaokhun.kmitl.ac.th, au2.au.ac.th, nontri.ku.ac.th, orchid.bu.ac.th ,mucc.mahidol .ac.th

6.3.2.4 วัน ,เวลา และจำนวนผู้ใช้

ในการใช้งานแอพพลิเคชั่น จากการตรวจสอบโดยใช้คำสั่ง W, top เพื่อทำการตรวจสอบผู้ใช้ในระบบว่ามีการใช้งานในแอพพลิเคชั่นใดและใช้ในวันเวลาไหน แบ่งเป็นรายละเอียดได้ดังนี้

- ปริมาณการเข้าใช้ คือปริมาณการใช้งานโดยทราบจากจำนวนพอร์ทที่ทำการติดต่อของ TCP/IPในแอพพลิเคชั่นที่ผู้ใช้ใช้งาน และการสังเกตจาเหตุการณ์จริงในเวลาที่ทำการทดลอง
- วัน เวลา ที่เข้าใช้ แบ่งออกเป็น 2 ช่วง คือ
- - ช่วงเปิดเทอม ส่วนใหญ่จะใช้ในช่วงเวลากลางวัน (11.00-13.00น.) ช่วงเวลา (16.00-19.00) และ สุดท้ายคือช่วงค่ำ (22.00 - 01.00 น.)
- -ช่วงปิด เทอมหรือใกล้สอบ ส่วนใหญ่จะใช้ในช่วงเวลากลางวันเท่านั้น และช่วงอื่น ๆ ปริมาณคนจะน้อยลง

6.3.3 การวิเคราะห์ข้อมูล (ANALYSIS)

6.3.3.1 การวิเคราะห์ข้อมูล CPU ,คำสั่ง Top และ TCP Connection

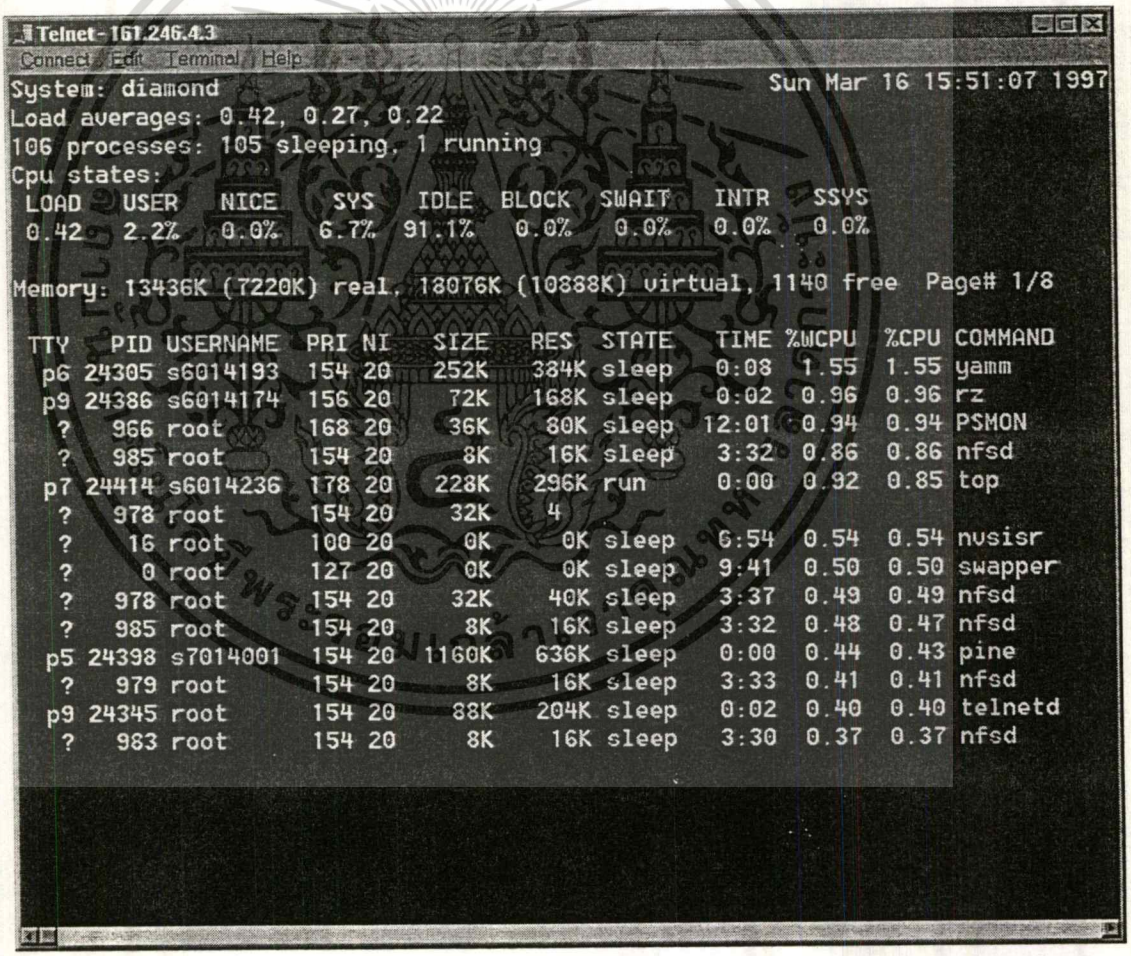
ข้อมูลที่ได้รับจาก CPU ของเครื่อง diamond นั้นเราได้ทำการวิเคราะห์ โดยแบ่งผลการวิเคราะห์ออกตามหัวข้อต่อไปนี้คือ

- **ช่วงปิดเทอม** ในช่วงนี้แบ่งย่อยออกเป็น 2 ข้อ
  1. ปริมาณการใช้ CPU ปกติ มีค่า 0.2 - 0.5 Load AVG
  2. ปริมาณการใช้ CPU มากเกินปกติ มีค่า 1.0 - 1.5 Load AVG โดยมีช่วงเวลาดังนี้
     * 22.00 - 02.00 น. เกือบทุกวัน
- **ช่วงปิดเทอม** ในช่วงนี้แบ่งย่อยออกเป็น 2 ข้อ
  1. ปริมาณการใช้ CPU ปกติ มีค่า 1.5 - 2.0 Load AVG
  2. ปริมาณการใช้ CPU มากเกินปกติ มีค่า 2.0 - 3.0 Load AVG โดยมีช่วงเวลาดังนี้
     * 15.00 - 17.00 น. วันจันทร์ - วันศุกร์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

* 21.00 - 24.00 น. ทุกวัน

● **ข้อมูลที่ได้จากการใช้คำสั่ง top** เนื่องจาก Hp OpenView เวอร์ชันที่ได้ใช้อยู่ตอนนี้ไม่สามารถทำการเก็บข้อมูลได้ละเอียด มากเกินกว่านี้คือ ไม่สามารถทราบได้ว่าขณะนั้น ๆ ได้มีการใช้งานแอพพลิเคชั่นใด,เรียกใช้คำสั่งใดอยู่ หรือจัดการอะไรกับข้อมูลและทรัพยากรใน diamond ดังนั้นถ้าหาจะทำการบ่งชี้ลงไปอย่างแน่นอนว่าอะไรคือสาเหตุของการใช้ CPU มากเกินกว่าปกติ อาจจะทำได้โดยการใช้คำสั่ง top ร่วมกับการใช้ข้อมูลจาก TCP connection ก็อาจจะพอทำให้เราสามารถบอกได้ว่าอะไรที่ใช้ CPU มาก ซึ่งแอพพลิเคชั่นนั้นก็คือสาเหตุที่ทำให้ CPU ต้องใช้งานหนัก และถ้าเราเห็นว่าแอพพลิเคชั่นนั้นไม่จำเป็น ก็อาจจะทำการกำจัดแอพพลิเคชั่นนั้นก็ได้ เช่น irc, talk หรือการ load รูปภาพอนาจาร เป็นต้น



รูปที่ 6.4 แสดงคำสั่ง Top

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

● **ปริมาณการใช้งานโดยใช้ TCP connection**

■ มากกว่า 40 เปอร์เซ็นต์ ของการใช้งาน เป็นการเชื่อมต่อเข้ามา ใช้บริการ WWW ของ diamond ก็ คือ มีผู้ใช้จากข้างนอกทำการเข้ามาเปิด WEB page ของภาคคอมพิวเตอร์ โดยส่วนใหญ่เป็นการเชื่อมโยงจากปลายทางที่อยู่ต่างประเทศ

■ ประมาณ 20 เปอร์เซ็นต์ของการใช้งาน เป็นการใช้คำสั่ง telnet เข้ามายัง diamond ซึ่งผู้ใช้ส่วนใหญ่เป็นนักศึกษาภายในสถาบันนั่นเอง โดยเครื่องที่ใช้ในการเชื่อมโยงมาถึงก็เป็นเครื่องภายในสถาบัน

■ ประมาณ 15 เปอร์เซ็นต์ของการใช้งานเป็นการใช้คำสั่ง ftp เพื่อทำการโอนย้ายข้อมูล เช่นเดียวกันกับ คำสั่ง telnet ผู้ใช้ส่วนใหญ่เป็นนักศึกษาภายในสถาบัน อาจจะมีบางส่วนที่มาจากที่อื่นบ้าง

■ ประมาณ 10 เปอร์เซ็นต์ของการใช้งานเป็นการใช้ irc และ mail ใช้โปรโตคอล smtp แต่ไม่สามารถบ่งชี้ได้ว่าใครเป็นคนใช้ หรือ ใช้มาจากสถานที่ใด

■ ที่เหลือเป็นการใช้งานชนิดอื่น ๆ ไม่สามารถบอกได้คืออะไร

ซึ่งข้อมูลที่เราเก็บรวบรวมมาได้นี้เราสามารถวิเคราะห์ได้ว่า ปริมาณการใช้งาน CPU ในขณะนั้นเป็นอย่างไร,จำนวน process ที่ทำงานอยู่มีมากน้อยเท่าไหร่ และเรายังสามารถทำการลดหรือกำจัด process ที่ไม่สำคัญได้ในกรณีที่ช่วงเวลานั้นมี load AVG สูงอีกด้วย

6.3.3.2 การวิเคราะห์ความสัมพันธ์ของ packets/sec และ octets/sec

จากข้อมูลเกี่ยวกับ packets/sec และ octets/sec เราสามารถวิเคราะห์ได้ว่าข้อมูลทั้ง 2 ไม่มีความสัมพันธ์กันเลย เนื่องจากในขณะเวลาใด ๆ จำนวน packets/sec มีค่าสูง แต่ปริมาณ octets/sec กลับไม่สูงตาม หรือขณะที่ปริมาณ octets/sec สูงแต่จำนวน packets/sec กลับไม่สูง

สรุปได้ว่าข้อมูลทั้ง 2 ไม่มีความสัมพันธ์กันเลย และที่สำคัญคือเราสามารถหาขนาดของข้อมูลต่อแพ็คเก็ตได้ โดยใช้ปริมาณออกเตตต่อวินาที หารด้วย จำนวนแพ็คเก็ตต่อวินาที ค่าที่ได้ออกมามีหน่วยเป็นออกเตตต่อแพ็คเก็ตและเมื่อทำการคูณด้วย 8 ก็จะได้หน่วย เป็น บิต ต่อ แพ็คเก็ต แต่ว่าค่าที่ได้ออกมานี้เป็นค่าประมาณไม่สามารถ นำมาคำนวณหาชนิดของแอพพลิเคชั่นได้

6.3.3.3 การคำนวณหาค่าการใช้งานในสายเชื่อมต่อจากค่าออกเตตของอินเตอร์เฟส

ในการประมาณสภาพเครือข่ายนั้นจะมีการประมาณในเวลาที่เครือข่ายมีการใช้งานสูงสุด เพื่อหาสภาพของเครือข่ายว่าสามารถรองรับการใช้งานได้หรือไม่

วิธีคำนวณการหาค่าการใช้งานในสายเชื่อมต่อ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Utilization = 8(ifInOctet+ifOutOctet-ifInError-ifOutError)/*ค่าแบนด์วิธของสายส่ง

เนื่องจากค่า ifInError และค่า ifOutError มีค่าน้อยมากจึงคิดค่าเป็น 0 จึงได้

Utilization = 8(ifInOctet+ifOutOctet)/*ค่าแบนด์วิธของสายส่ง

หน่วยของค่าการใช้งานในสายเชื่อมต่อมีค่าระหว่าง 0 ถึง 1 โดยนำมาคูณกับ 100 จะได้ค่าเปอร์เซนต์การใช้งานในสายเชื่อมต่อ

6.3.3.4 การคำนวณหาค่าการใช้งานในสายเชื่อมต่อของ Diamond (161.246.4.3)

อินเตอร์เฟส1 เป็น lan0

ifInOctet มีค่าออกเตดเข้าสูงสุด 35940 ออกเตด/วินาที

LineNo	Start	Stop	MinVal	AvgVal	MaxVal
4	832134824	832135124	2608.26	2608.26	2608.26
4	832135124	832135424	23185.7	23185.7	23185.7
4	832135424	832135724	34040.6	34040.6	34040.6
4	832135724	832136024	35900.2	35900.2	35900.2
4	832136024	832136324	32222	32222	32222
4	832136324	832136624	35940.2	**35940.2**	35940.2
4	832136624	832136924	38226.1	38226.1	38226.1

ifOctetOut มีค่าออกเตดออกสูงสุดประมาณ 2610.72 ออกเตด/วินาที

LineNo	Start	Stop	MinVal	AvgVal	MaxVal
4	832135080	832135380	1861.44	1861.44	1861.44
4	832135380	832135680	2313.85	2313.85	2313.85
4	832135680	832135980	2275.85	2275.85	2275.85
4	832135980	832136280	2610.72	**2610.72**	2610.72

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4	832136280	832136580	2221.66	2221.66	2221.66
4	832136580	832136880	2067.1	2067.1	2067.1

- ออกเดตรวมจะเท่ากับ 35940+2610.72 = 38550.72 ออกเดต/วินาที
- ค่าบิตต่อวินาทีจะเท่ากับ 8*(38550.72) = 308405.76 บิต/วินาที
- ค่าการใช้งานของสายส่งจะเท่ากับ (308405.76*100)/10M = 3.0840576 %หรือประมาณ 3.1%

6.3.3.5 การคำนวณหาค่าการใช้งานในสายเชื่อมต่อของ CAR 24 (161.246.10.11)

1 อินเตอร์เฟส1 เป็น FDDI

- ifOctetIn มีค่าออกเดตเข้าสูงสุด = 174158 ออกเดต/วินาที

LineNo	Start	Stop	MinVal	AvgVal	MaxVal
1	854508184	854509984	6924.41	42641.9	78359.4
1	854509984	854511784	56354.6	66500.7	76646.8
1	854511784	854513584	113810	**174158**	234506
1	854513584	854515384	138418	172084	205750
1	854515384	854517184	108299	110571	112842
1	854517184	854518984	104052	114078	124103
1	854518984	854520784	113087	155115	197143
# <15m gap>					
1	854521684	854523484	12991.7	15160.6	17329.5

- ifOctetOut มีค่าออกเดตออกสูงสุด = 231422 ออกเดต/วินาที

LineNo	Start	Stop	MinVal	AvgVal	MaxVal
9	854507284	854509084	29927.6	30137.5	30347.4
9	854509084	854510884	99526.5	99542.5	99558.4
9	854510884	854512684	84307	109899	135490
9	854512684	854514484	223284	**231422**	239560
9	854514484	854516284	149641	174611	199581

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

9	854516284	854518084	137794	140164	142534
9	854518084	854519884	115658	120601	125544
9	854519884	854521684	61703.2	89403.8	117104

-ออกเตดรวมจะเท่ากับ 174158+231422 = 405580 ออกเตด/วินาที

-ค่าบิตต่อวินาทีจะเท่ากับ 8*405580 = 3244640 บิต/วินาที

-ค่าการใช้งานของสายส่งจะเท่ากับ (3244640*100)/100M = 3.24464%

หรือ

ประมาณ 3.2%

2 อินเตอร์เฟส2 เป็น Ether0

● ifOctetIn มีค่าออกเตดเข้าสูงสุด = 152339 ออกเตด/วินาที

LineNo	Start	Stop	MinVal	AvgVal	MaxVal
2	855860899	855861799	77617.1	77617.1	77617.1
2	855861799	855862699	181063	181063	181063
2	855862699	855863599	136978	136978	136978
# <15m gap>					
2	855864499	855865399	152339	**152339**	152339
2	855865399	855866299	131261	131261	131261
2	855866299	855867199	50943.3	50943.3	50943.3
2	855867199	855868099	114336	114336	114336
2	855868099	855868999	20994.9	20994.9	20994.9

● ifOctetOut มีค่าออกเตดออกสูงสุด = 77083 ออกเตด/วินาที

LineNo	Start	Stop	MinVal	AvgVal	MaxVal
10	855862699	855863599	59988.8	59988.8	59988.8
10	855863599	855864499	53192.7	53192.7	53192.7
10	855864499	855865399	77083.1	**77083.1**	77083.1
10	855865399	855866299	71993.1	71993.1	71993.1
10	855866299	855867199	35717.7	35717.7	35717.7
10	855867199	855868099	72541.4	72541.4	72541.4

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

10	855868099	855868999	13656.8 13656.8 13656.8
10	855868999	855869899	1319.96 1319.96 1319.96

-ออกเตดรวมจะเท่ากับ 152339+77083 = 229422 ออกเตด/วินาที

-ค่าบิตต่อวินาทีจะเท่ากับ 8*229422 = 1835376 บิต/วินาที

-ค่าการใช้งานของสายส่งจะเท่ากับ (1835376*100)/10M = 18.35376% หรือประมาณ 18.4%

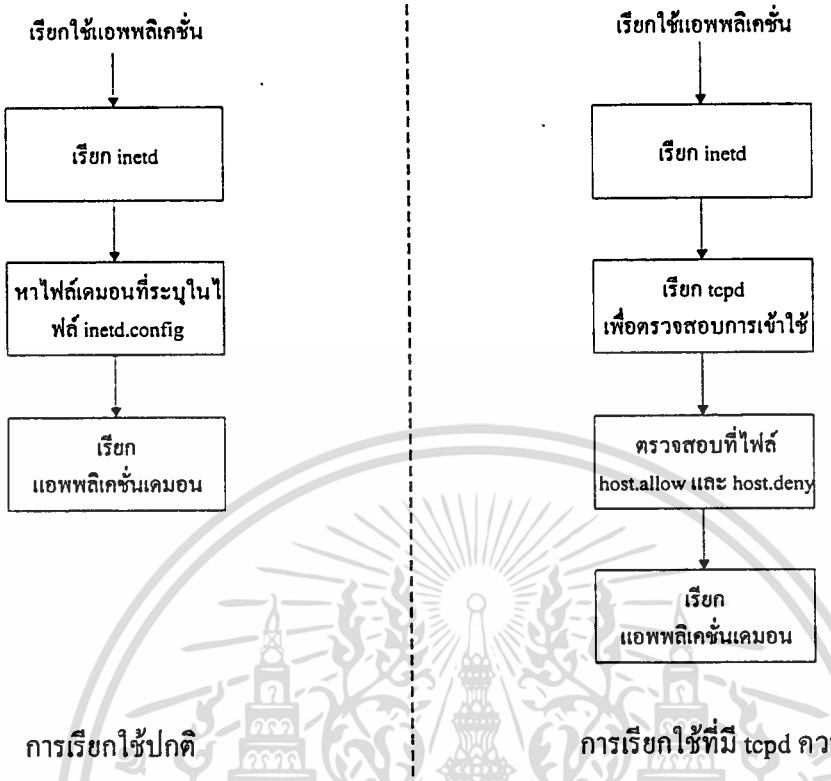
6.4 การบริหารด้านความปลอดภัย

ในส่วนนี้จะมีการบริหารอยู่ 3 ส่วน คือ

6.4.1 การควบคุมการเข้าใช้ (Access Control) ซึ่งการทำนี้เราแบ่งได้เป็น

- การควบคุมโดยใช้แอคเคาท์และรหัสผ่าน(Account and Password) เราจะทำการควบคุมโดยการกำหนดสิทธิการใช้งาน ,ไฟล์ ,พื้นที่ในการเก็บข้อมูล และรหัสผ่าน ในการตรวจสอบการใช้งานจะใช้คำสั่ง last เพื่อดูว่ามีแอคเคาท์ใดทำการเข้าใช้ ในเวลาใด
- การควบคุมการใช้บริการของแอพพลิเคชั่นบน TCP/IP ทำได้โดยสร้างไฟล์ tcpd เพื่อให้มีการตรวจสอบเมื่อมีการเรียกใช้แอพพลิเคชั่นซึ่งจะมีการเรียกไฟล์ inetd ที่จะทำการเรียกใช้ เดมอนของแอพพลิเคชั่นที่ทำการเรียกต่อไปซึ่งระบุในไฟล์ inetd.config โดยการควบคุมนี้จะอยู่ที่ไฟล์ tcpd ที่จะมีการสร้างไฟล์ host.allow และ host.deny ซึ่งจะระบุโฮสท์และบริการที่ทำการเข้าใช้ให้ใช้หรือไม่ใช้ตามลำดับ ดังรูป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



การเรียกใช้ปกติ การเรียกใช้ที่มี tcpd ควบคุม

- การควบคุมการเข้าใช้โดยใช้ ไฟร์วอลล์(Firewall) ในการควบคุมนี้เราเลือกไฟร์วอลล์แบบ สกรีนโฮสท์เกตเวย์(Screen Host Gateway) ในแบบนี้ประกอบไปด้วย สกรีนเราท์เตอร์(Screen Router) และแอพพลิเคชั่นเกตเวย์(Application Gateway) ซึ่งจะมีการติดตั้งที่ เราท์เตอร์ CAR24 และที่โฮสท์ตัวใดตัวหนึ่งในเครือข่ายตามลำดับ

6.4.2 การรักษาความปลอดภัยด้านกายภาพ (Physical Security)

ในการรักษาความปลอดภัยนี้คือ ระบบสำรองไฟฟ้า ,ระบบป้องกันไฟ ,ระบบการเข้าใช้ห้องโดยการใช้คอมพิวเตอร์ในแต่ละห้องจะมีการเข้าใช้ห้องละประตู

6.4.3 การใช้โปรแกรมรักษาความปลอดภัย(Security Software)

โปรแกรมรักษาความปลอดภัยนี้จะช่วยในการตรวจสอบและควบคุมการใช้งาน ซึ่งแบ่งได้เป็น 2 ประเภทคือ โปรแกรมรักษาความปลอดภัยเครือข่าย(Network Security Software) และโปรแกรมรักษาความปลอดภัยระบบ(System Security Software)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6.5 แอ็พพลิเคชั่นที่ทดลอง

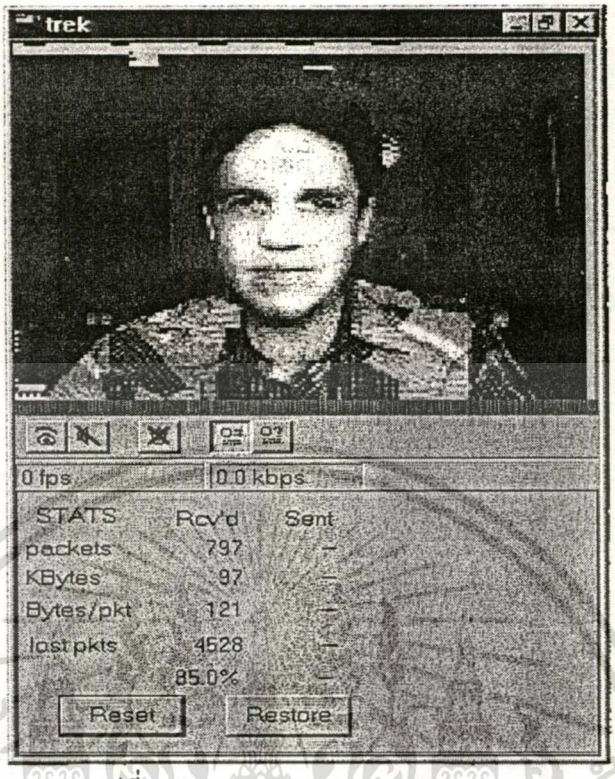
6.5.1.VDO conference

เราได้ทำการทดลองติดตั้ง software VDO conference ในภาควิชาของเราและทำการตรวจเก็บข้อมูลเพื่อการทดลองได้ข้อมูลดังต่อไปนี้

6.5.1.1 ตารางแสดงผลการทดลอง VDO Conferencing

ค่าที่สนใจ	ค่าขณะทำการทดลอง	Threshold	ค่าเฉลี่ยก่อนทำงาน
InOctet CAR24 serial	40000-65000	50000	น้อยกว่า 3000
InOctet CAR24 ether	30000-60000	170000	น้อยกว่า 10000
OutOctet CAR24 serial	10000-15000	20000	น้อยกว่า 5000
OutOctet CAR24 ether	50000-70000	90000	น้อยกว่า 5000

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 6.5 แสดงการ conference

6.5.1.2 สรุปและวิจารณ์การทดลอง

1.เนื่องจากได้มีการกำหนดค่า ขนาดข้อมูลที่ส่งออกจาก VDO conference = 80Kb/s ซึ่งมีค่าใกล้เคียงกับ OutOctet CAR24 serial - ค่าเฉลี่ยก่อนการเรียกใช้ VDO conference

2.เนื่องจากได้มีการกำหนดค่า ขนาดข้อมูลที่รับจากการ conference = 300Kb/s ซึ่งค่าที่ได้จาก OutOctet CAR24 ether - ค่าเฉลี่ยก่อนการเรียกใช้ VDO conference ประมาณ 60000 Octet เพราะฉะนั้นมีค่าการ error = (300000-60000)/300000 * 100 = 80 %

3.Utilization ที่สายต่อ Ether มีค่า 10.4 % {(70000+60000=130000) * 8}/10000000

4.Utilization ที่สายต่อ Serial (2 Mb) มีค่า 40 % {(15000+65000=750000) * 8}/2000000

5.สาเหตุอื่นที่ทำให้ VDO conference ช้า หรือมี error มากทั้งภาพ และ เสียง

- bandwidth ที่ต่อไปภายนอก เช่น สาย 2 Mb หรือ สายที่ต่อใน Internet

- ประสิทธิภาพของกล้องที่ต่อกับ port parallel

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

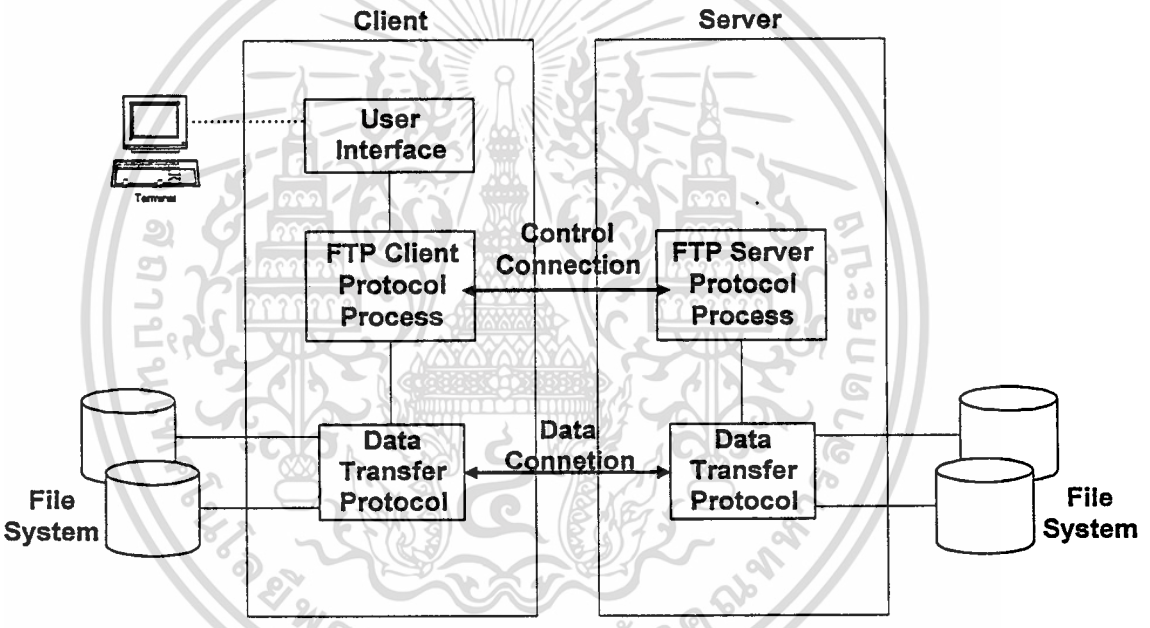
6.5.2.FTP

เนื่องจากขณะที่มีการเกิดข้อผิดพลาดกับ FTP นั้นเราได้ทำการเก็บข้อมูลแล้วพบว่า ค่าของข้อมูลไม่แตกต่างจากสภาพปกติเลย ดังนั้นจึงไม่สามารถใช้ข้อมูลที่เก็บมาเพื่อบ่งชี้ได้ว่าจุดใดเป็นสาเหตุของข้อผิดพลาดที่เกิดขึ้น เราจึงได้ทำเป็นกรณีศึกษา

6.6 กรณีศึกษา

การบริหารแอพพลิเคชั่น FTP ในเชิง Fault Management

หลักการทำงานของ ftp



รูปที่ 6.6 แสดง model ของ control และ data connection

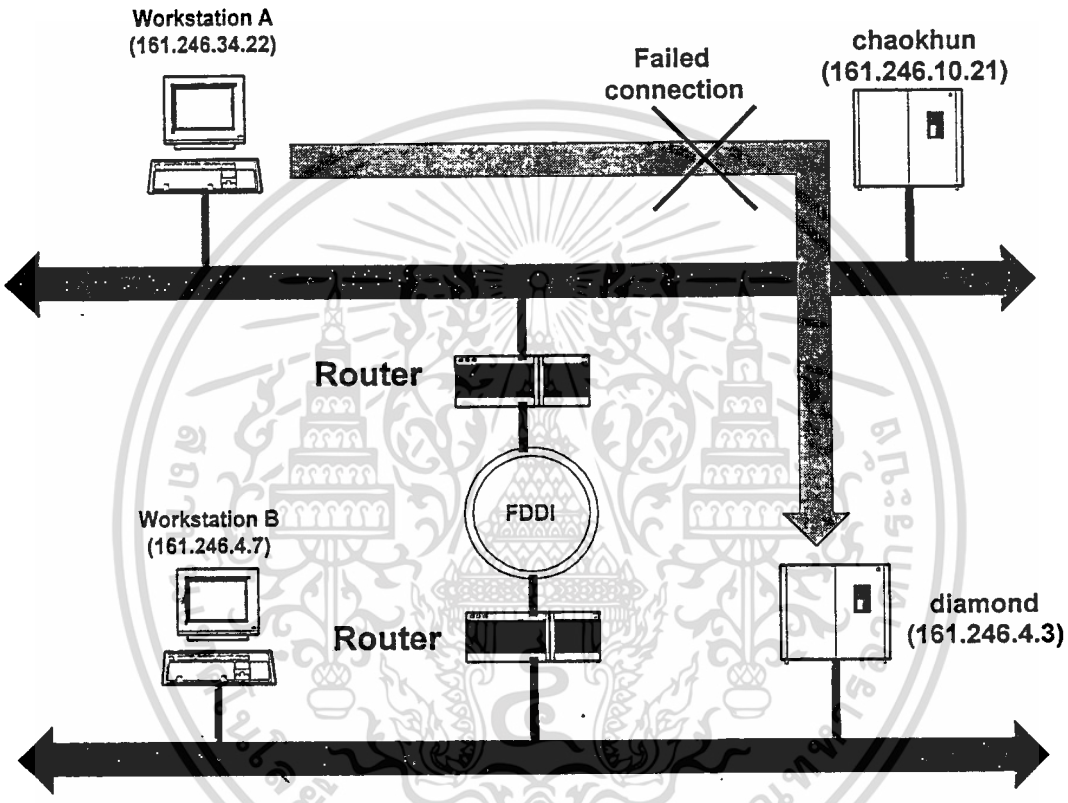
จากรูป การติดต่อระหว่าง Client กับ Sever จะกระทำทาง Control Connection ซึ่งใช้ในการส่งคำสั่งและการตอบรับระหว่าง Client และ Server และเมื่อตกลงส่งข้อมูลกันจริง ๆ แล้วจึงสร้าง Data Connection ขึ้นมาเพื่อส่งข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การแก้ปัญหา connection closed ; transfer aborted

ปัญหาที่เกิดขึ้น

ไม่สามารถใช้ แอพพลิเคชั่น ftp ระหว่าง workstation A กับ diamond ได้ ดังรูป



รูปที่ 6.7 แสดงปัญหาที่เกิดขึ้นในการใช้แอพพลิเคชั่น ftp

ข้อมูลในการแก้ปัญหา

วันที่เกิดปัญหา	**15 กุมภาพันธ์ 2540**
Application ที่เกิดปัญหา	**ftp ระหว่าง workstation A กับ dimaond**
Error message	**426 Connection closed ; transfer aborted**
Remote host name และ IP Address	**diamond (161.246.4.3)**
User host name และ IP Address	**blue (161.246.34.22)**

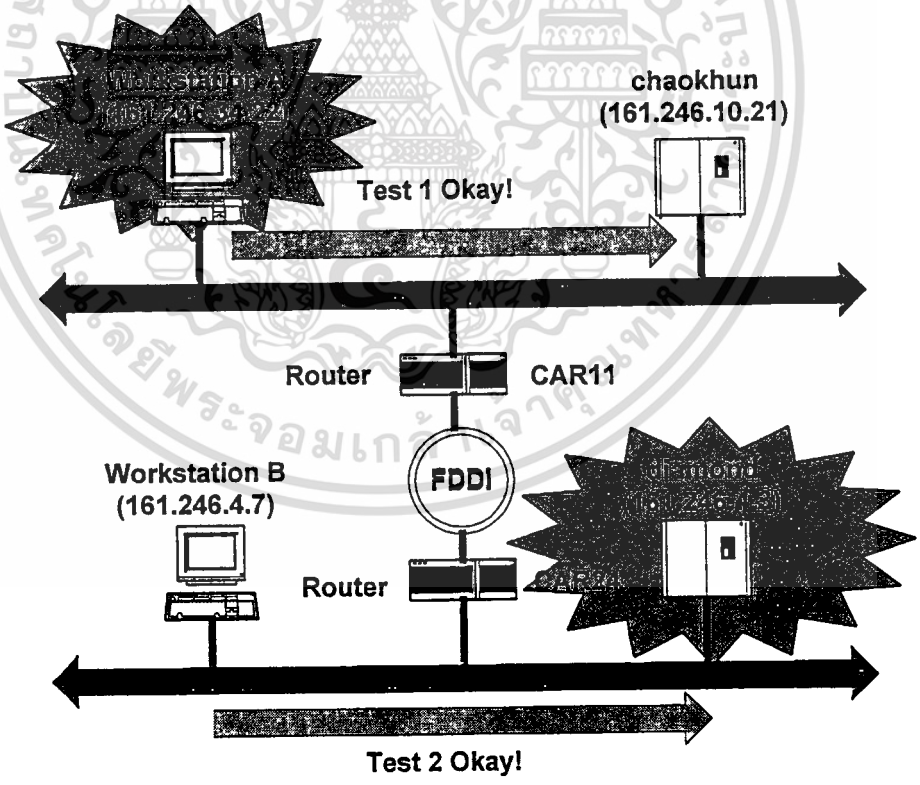
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สมมติฐานในการแก้ปัญหา

- workstation A หรือ diamond เครื่องใดเครื่องหนึ่งหรือทั้งสองเครื่องมีปัญหา
- เราท์เตอร์ทำงานผิดพลาด
- มีปัญหาที่สายนำสัญญาณ (Fiber Optic ของ FDDI Ring)

การทดสอบ เครื่องคอมพิวเตอร์ที่ใช้งานแอพพลิเคชั่น (host)

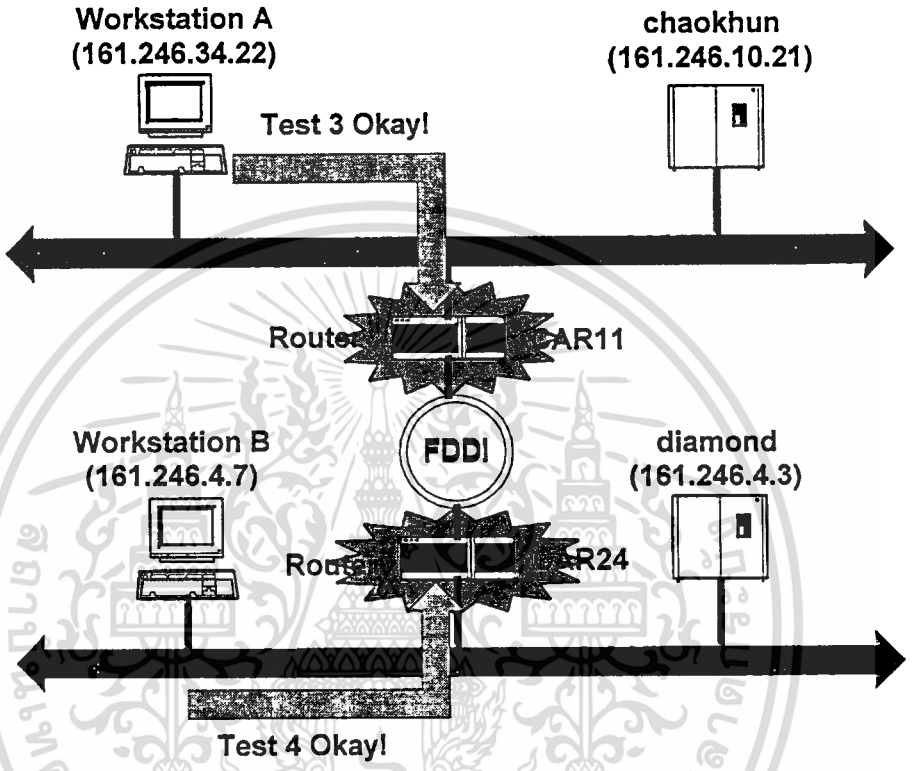
- workstation A หรือ diamond เครื่องใดเครื่องหนึ่งหรือทั้งสองเครื่องมีปัญหา ตรวจสอบโดยการรันแอพพลิเคชั่น ftp ที่ทั้งสอง host ภายในเครือข่ายเดียวกันโดยไม่ผ่านเราท์เตอร์ ผลปรากฏว่าไม่มีเครื่องใดทำงานผิดพลาด ดังรูป สรุปได้ว่าสาเหตุของปัญหาไม่ได้อยู่ที่ตัว host ที่ใช้งาน



รูปที่ 6.8 แสดงการทดสอบการทำงานของ hosts

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

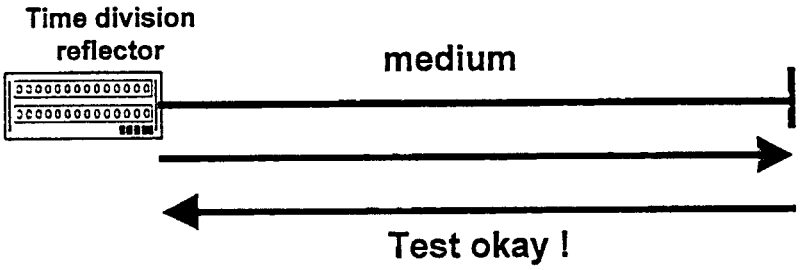
● เราท์เตอร์ทำงานผิดพลาด ทดสอบโดยการ ping ไปที่ เราเตอร์ทั้งสองจาก host ในเครือข่ายเดียวกัน ดังรูป ผลปรากฏว่าเราท์เตอร์สามารถทำงานได้ถูกต้อง เราสรุปได้ว่าสาเหตุของปัญหาไม่ได้อยู่ที่ตัวเราท์เตอร์

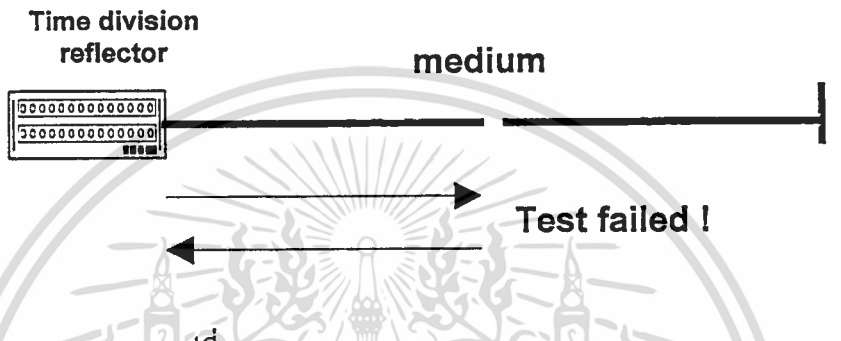


รูปที่ 6.9 แสดงการทดสอบ routers

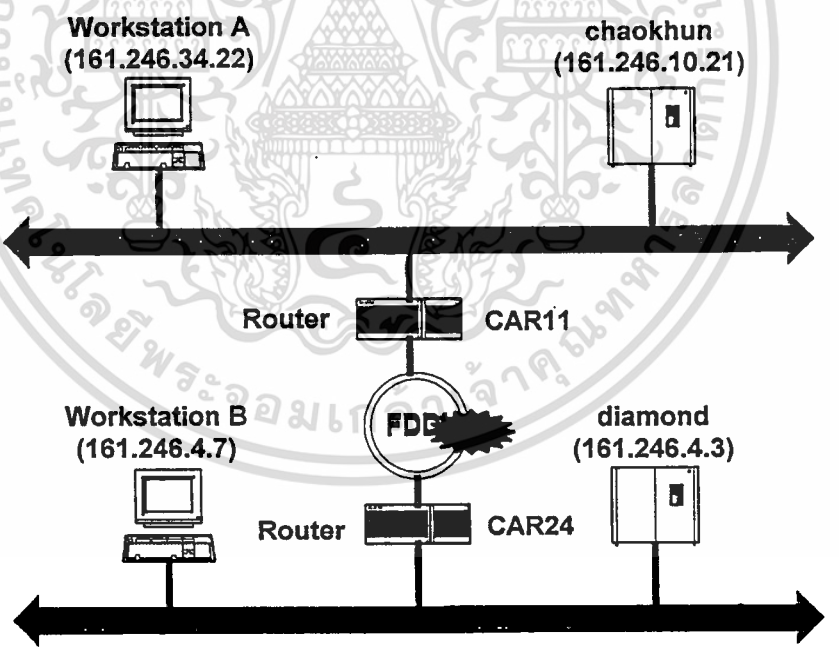
● มีปัญหาที่สายนำสัญญาณ (Fiber Optic ของ FDDI Ring) เราสามารถพิสูจน์สมมติฐานนี้โดยการใช้อุปกรณ์ที่เรียกว่า time division reflector เพื่อตรวจสอบสภาพของสายสัญญาณว่ามีการขาดอยู่ช่วงไหนบ้างหรือเปล่า ดังรูป ผลการทดสอบปรากฏว่าสาย Fiber ขาดอยู่ระหว่าง workstation A กับ diamond จึงสรุปได้ว่าสาเหตุของการผิดพลาดในการใช้แอพพลิเคชั่น ftp

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้





รูปที่ 6.10 แสดงการทดสอบ medium



รูปที่ 6.11 แสดงสาเหตุของปัญหา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 7

บทวิจารณ์และสรุป

7.1 สรุปและวิจารณ์โครงงาน

โครงงานนี้ได้จัดทำขึ้นเพื่อต้องการเพิ่มประสิทธิภาพการใช้แอพพลิเคชั่นบนเครือข่าย โดยการเพิ่มประสิทธิภาพของเครือข่ายในด้านต่าง ๆ ซึ่งผู้จัดทำต้องเริ่มด้วยการระบุความต้องการ ซึ่งก็คือ แอพพลิเคชั่นที่ต้องการบริหาร หลังจากนั้นแล้วก็ต้องศึกษาว่าข้อมูลใดบ้างที่จำเป็นต้องใช้ในการบริหารนั้น ต่อไปก็ทำการเก็บข้อมูล กระบวนการนี้อาจใช้เครื่องมือต่าง ๆ ช่วยในการเก็บข้อมูล โดยในโครงงานนี้ใช้ระบบบริหารเครือข่ายของสำนักวิจัยและบริการคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง คือ HP-OpenView หลังจากนั้นจึงนำข้อมูลที่เก็บได้มาทำความเข้าใจและวิเคราะห์และนำเสนอแนวทางในการพัฒนาเครือข่ายให้แก่ผู้ดูแลเครือข่าย

ในการทำโครงงานนี้ค่อนข้างใหญ่และจะต้องพึ่งพาอุปกรณ์ช่วยเป็นอย่างมาก คือ อย่างน้อยที่สุดต้องมีระบบบริหารเครือข่ายช่วยในการตรวจสอบและเก็บข้อมูลจากเครือข่าย ทั้งยังต้องสามารถสั่งงานบางอย่างผ่านตัวระบบบริหารเครือข่ายนี้ด้วย เช่น สั่งให้พอร์ตของฮับ เปิดหรือปิด เรียกว่า การการสั่งงานระยะไกล (Remote setup) ดังนั้นถ้าหากเครื่องมือเหล่านี้ไม่มีหรือมีไม่ครบก็จะทำให้การดำเนินเป็นไปด้วยความยากลำบากและล่าช้า

จากผลการทดลองทำการจัดการระบบเครือข่ายภายในสถาบันของเรานั้น สามารถสรุปได้ว่า

1. การใช้งานของ CPU ของเครื่อง diamond ซึ่งเป็นเครื่องเซิร์ฟเวอร์ ที่เราทำการจัดเก็บข้อมูลที่เกี่ยวข้อง มีการใช้งานยังไม่มากหรือหนักจนเกินไป, มี process ใดบ้างจำนวนเท่าใด ที่เข้ามาทำงานอยู่ และ ที่สำคัญคือเมื่อ load AVG สูงเกินไปเราอาจทำการกำจัด process ที่มีความสำคัญน้อยทิ้งไปได้ ดังหัวข้อที่ 6.3.1

2. สามารถสรุปได้ว่า จำนวนแพ็คเก็ตเข้าและออกจากเครื่อง diamond ไม่มีความสัมพันธ์กับจำนวนอ็อคเต็ตที่เข้าหรือออกเลย เนื่องจากแพ็คเก็ตที่ทำงานอยู่บนเครื่อง diamond นั้นมีอยู่หลายชนิดของแอพพลิเคชั่น ซึ่งแต่ละแอพพลิเคชั่นก็มีขนาดแพ็คเก็ตไม่เท่ากัน และ Hp OpenView ที่เราใช้อยู่ก็ไม่สามารถทำการบ่งชี้ชนิดแอพพลิเคชั่นได้ด้วย จึงทำให้เราไม่สามารถ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จะรู้ได้เลยว่าจริง ๆ แล้วในขณะเวลาใด ๆ มีการใช้แอพพลิเคชั่นชนิดใดอยู่มากน้อยเพียงใด ดังหัวข้อที่ 6.3.2

3. การใช้งานในสายเชื่อมต่อ ภายในภาควิชาวิศวกรรมคอมพิวเตอร์ และภายในระบบเครือข่าย FDDI ของสถาบัน สามารถรองรับการใช้งานของผู้ใช้เพิ่มขึ้นจากเดิมได้ โดยทำการวิเคราะห์ข้อมูลจากหัวข้อ 6.3.3 เรื่องการคำนวณหาค่าการใช้งานในสายเชื่อมต่อ

4. จากข้อ 1 และ 3 เราก็สามารถสรุปเพิ่มเติมได้อีกว่าถ้าหาก ขณะที่ทำงานแอพพลิเคชั่นใด ๆ ที่เกี่ยวกับอินเทอร์เน็ต แล้วมีปัญหาเราก็สามารถจะทำการตรวจสอบ ได้โดยใช้ข้อมูลข้างต้น ซึ่งเราก็จะพบว่าจริง ๆ แล้ว ทั้งสายเชื่อมต่อ และ CPU ของเครื่อง diamond ยังสามารถใช้งานได้ดี ดังนั้นสาเหตุของปัญหานั้นอาจจะเกิดจากสาเหตุอื่น ๆ เช่น เราท์เตอร์, เกทเวย์ หรือโมเด็มที่ต่อไปยัง Nectec ซึ่งเราก็ต้องทำการตรวจสอบต่อไป

5. การใช้งานเครือข่ายส่วนใหญ่ที่พบจากการดูกระบวนการที่ทำงานบนเครื่อง diamond พบว่าการใช้งาน netscape และ ftp เป็นการใช้งานของผู้ใช้เป็นส่วนใหญ่ดังนั้นการจัดการเครือข่ายควรจะทำการจัดการเครือข่ายเพื่อรองรับการทำงานของเครือข่ายในด้านอินเตอร์เน็ต

6. ในการจัดการเครือข่ายนี้เราสามารถวิเคราะห์การทำงานของเครือข่ายได้อย่างคร่าวๆ และได้น้อยเนื่องจากซอฟแวร์ที่ใช้จัดการ(Hp OpenView) มีโมดูลส่วนประกอบไม่ครบ ทำให้จำนวนและประเภทของข้อมูลที่ทำการเก็บมาจากระบบการจัดการนั้นมีจำนวนน้อยและไม่เพียงพอในการวิเคราะห์การทำงานของเครือข่ายในด้านอื่นๆ

7.2 ปัญหาที่พบ

7.2.1 แผนที่ใน Hp Openview มีสัญลักษณ์ไม่ครบ เมื่อทำการเปรียบเทียบ Configuration ที่ได้จากผู้บริหารระบบของทั้งภาคคอมพิวเตอร์ และ สำนักวิจัย แล้วพบว่ามีคอมพิวเตอร์บางตัวที่ไม่อยู่บน แผนที่ที่เราเปิดขึ้นมา ดังนั้นเราจึงทำการเพิ่มสัญลักษณ์ของคอมพิวเตอร์เครื่องนั้นเข้าไป โดยอาจจะทำการ telnet ไปยังเครื่องคอมพิวเตอร์นั้น, ส่ง mail ไปยังเครื่องคอมพิวเตอร์นั้น หรืออาจจะทำการเพิ่มออบเจ็คจากเมนุบาร์ (เมนู Edit) แล้วทำการเพิ่มการเชื่อมต่อจากเมนูเดียวกัน เราก็จะได้รับ เครื่องคอมพิวเตอร์ที่ขาดไปกลับมา และสามารถกระทำการใด ๆ กับสัญลักษณ์นั้นได้อย่างปกติ

7.2.2 เครื่องมักหยุดทำงานไปเฉย ๆ ในกรณีที่ทำการโหลดข้อมูล หรือทำการเก็บค่าของข้อมูลที่สูงมาก ๆ เกินปกติ ขณะที่ทำงานอยู่นั้นเครื่องก็หยุดไปเฉย ๆ ทำให้เสียเวลาในการเริ่มทำงานใหม่ทุกครั้ง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

7.2.3 การเรียกใช้งานแต่ละครั้งช้ามาก ในขณะที่ทำงานอยู่นั้นถ้าหากมีการเปลี่ยนหน้าต่างการทำงาน หรือเปลี่ยนชุดคำสั่ง เครื่องจะทำการตอบสนองช้ามาก ทำให้ในบางครั้งเราเข้าใจว่าเครื่องหยุดทำงานไปแล้ว ทำให้เราเปลี่ยนการทำงาน หรือ ออกจากโปรแกรมไปเลย เสียเวลาโดยเปล่าประโยชน์

7.2.4 ไม่มีเมนูสำหรับพิมพ์รูปภาพ ในกรณีที่ข้อมูลที่เราต้องการมีลักษณะ เป็นกราฟหรือรูปภาพต่าง ๆ เราต้องการเก็บข้อมูลมา แต่ไม่เมนูสำหรับการพิมพ์ภาพเหล่านั้น และหาโปรแกรมสำหรับพิมพ์ภาพจากระบบยูนิกซ์ไม่ได้ ดังนั้นจึงต้องใช้คำสั่ง xwd และ xpr ซึ่งทำให้เกิดความยุ่งยาก และเสียเวลาในการศึกษาชุดคำสั่งเหล่านี้

7.2.5 ไม่มี printer ที่ต่อกับเครื่องเวิร์คสเตชั่น ภายในภาคคอมพิวเตอร์ของเรา จะสังเกตุได้ว่าไม่มีเครื่อง printer ที่เชื่อมต่ออยู่กับเครื่องเวิร์คสเตชั่นอยู่เลย ทำให้เมื่อต้องการพิมพ์ข้อมูลอะไรออกมาจึงจำเป็นต้องไปขอใช้ในห้องเซิร์ฟเวอร์เจ้าคุณที่ศูนย์วิจัย ซึ่งมีปัญหาในการเข้าใช้งาน

7.2.6 ปัญหาในการเก็บข้อมูล ขณะที่ทำการเก็บข้อมูลจากภาคคอมพิวเตอร์หลายครั้ง (5 - 10 ครั้ง) จะต้องมีเหตุทำให้การเก็บข้อมูลไม่สำเร็จ เช่น เครื่องหยุดทำงานไปเฉย ๆ , เซิร์ฟเวอร์หยุดทำงาน, เครื่องถูกบุคคลไม่หวังดีปิด, การกระทำอันทำให้เครื่องหยุดทำงานโดยผู้ไม่หวังดี,เอเจ้นต์ในเครื่องที่ทำการเก็บข้อมูลเช่น diamond เกิดมีปัญหา หรือกรณีล่าสุดก็คือสายเชื่อมระหว่างภาคคอมพิวเตอร์กับสำนักวิจัยขาดลงเนื่องจากถูกรถชนเสาไฟฟ้าหัก

7.2.7 เนื้อที่ไม่พอต่อการเก็บข้อมูล เนื่องจากเครื่องที่ใช้งานอยู่นั้นมีการใช้งานเป็น จำนวนมากอยู่ก่อนหน้าที่เราจะเข้าไปใช้งานแล้ว ดังนั้นเนื้อที่ที่เหลือภายในฮาร์ดดิสค์ จึงเหลือไม่มาก และที่สำคัญคือข้อมูลที่เราทำการเก็บนั้นแต่ละไฟล์ มีขนาดใหญ่มากดังนั้นเก็บได้เพียงไม่เท่าไร เนื้อที่ก็เต็มแล้ว ทำให้ต้องเสียเวลาเก็บ และลบทิ้งทันที ไม่มีการเก็บไฟล์เก่าไว้ เมื่อมีปัญหาเกิดขึ้นจึงไม่สามารถนำ ไฟล์เก่านั้นกลับมาแก้ไขได้

7.2.8 ขาดคู่มือการใช้งาน Hp Openview เนื่องจากโปรแกรม Hp Openview นั้นเป็นโปรแกรมที่ใช้สำหรับงานการจัดการ ซึ่งเป็นงานของผู้บริหารระบบ ดังนั้นจึงไม่มีคู่มือสำหรับผู้ใช้โดยทั่วไป จะมีก็แต่คู่มือสำหรับผู้บริหารระบบโดยตรง ซึ่งต้องมีการใช้คำสั่งในระดับที่เราไม่สามารถทำความเข้าใจได้ ดังนั้นประสิทธิภาพในการใช้โปรแกรมนี้จึงอาจจะไม่สูงสุด

7.2.9 Hp Openview ไม่ใช่ชุดเต็ม เนื่องจากในครั้งแรกที่เราเริ่มทำโปรเจ็คนี้ เราได้พูดคุยกับพี่ที่รับผิดชอบเกี่ยวกับ การลงโปรแกรม Hp Openview นี้ ได้รับการบอกกล่าวว่าชุดส่วนประกอบ คือ โปรแกรมใช้งานต่าง ๆ ที่ใช้ร่วมกันกับ Hp Openview นั้นจะมีการติดตั้งตามมากทีหลัง จากบริษัทผู้รับผิดชอบ การขายโปรแกรมนี้ ซึ่งถ้าหากครบชุดที่สั่งไปนั้น Hp Openview จะเป็นโปรแกรมที่มีประสิทธิภาพสูงมาก สิ่งใดที่ต้องการก็จะได้รับตามความต้องการเกือบทุกอย่างแต่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เนื่องจากผู้ขายซึ่งรับผิดชอบเกี่ยวกับการติดตั้ง Hp Openview นี้ได้ลาออกจากบริษัท ไม่มีผู้ดำเนินการแทน และที่สำคัญคืออาจารย์ที่รับผิดชอบท่านไม่ได้ตามเรื่องนี้ ดังนั้นจึงทำให้ Hp Openview ที่เราใช้งานอยู่นี้ยังมีครบชุดตามที่สั่งไป คงมีแต่เพียง Hp Openview Node Manager เพียงเท่านั้น ไม่สามารถทำงานตามที่เราคาดหวังไว้ได้ตั้งแต่เริ่มโปรเจ็ค (ทราบเรื่องตอนเดือนกุมภาพันธ์ก่อนสอบ)

7.2.10 ปัญหาในการใช้ห้องที่ศูนย์วิจัย เนื่องจากโปรแกรม Hp Openview ที่เราใช้อยู่นี้เราต้องทำการ telnet เข้าไปใช้ที่เครื่อง EMS2 ในห้องเซิร์ฟเวอร์เจ้าคุณ ดังนั้นเมื่อเกิดปัญหาจากข้อ 5 และ 6 ทำให้เราจำเป็นต้องไปขอใช้เครื่อง EMS2 โดยตรงจากห้องเซิร์ฟเวอร์เพื่อแก้ปัญหาที่เกิดขึ้น

เนื่องจากห้องเซิร์ฟเวอร์ที่ตึกสำนักวิจัยนั้น เป็นที่เก็บเซิร์ฟเวอร์ และอุปกรณ์ต่าง ๆ เกี่ยวกับระบบเครือข่ายภายในสถาบันเรา จึงมีความสำคัญและต้องมีการระมัดระวังจากการใช้ของคนภายนอกที่ไม่เกี่ยวข้อง ดังนั้นการที่เราจะเข้าไปใช้ห้องจึงต้องทำการขออนุญาตอาจารย์ผู้คุมสำนักวิจัย และ ท่านอาจารย์ก็ไม่อนุญาตให้เราเข้าใช้ ดังนั้นการจะเข้าไปใช้ในห้องเซิร์ฟเวอร์นั้นจึงต้องเข้าไปใช้ในขณะที่พี่ที่เรารู้จักอยู่ เหตุดังกล่าวนี้จึงเป็นสาเหตุที่เราไม่สามารถใช้งานเครื่องภายในห้องเซิร์ฟเวอร์นั้นได้เต็มที่

7.3 ข้อเสนอแนะ

จากการทดลองเก็บข้อมูลในเครือข่ายและนำมาวิเคราะห์แล้ว ทางทีมงานได้เกิดแนวความคิดเกี่ยวเครือข่ายที่ดีขึ้นในอนาคต ว่า ควรจะมีการปรับปรุง หรือเพิ่มเติม ทางด้านต่อไปนี้ โดยอ้างอิงตามฟังก์ชั่นการบริหารเครือข่ายของ ISO

7.3.1 ทางด้านความปลอดภัยของเครือข่ายและระบบ

จากการสำรวจพบว่าความรักษาความปลอดภัยของเครือข่ายและเปรียบเทียบกับมาตราฐาน แล้วมีข้อเสนอแนะดังนี้

- ทางด้านฟิสิคอล

แต่ละห้องที่แยกจากกันนั้นยังมีทางเข้าร่วมกันอยู่เป็นบางห้อง ถ้าจะให้มีความปลอดภัยเพิ่มขึ้นควรจะมีทางเข้าที่แยกจากกันต่างหาก ซึ่งปัจจุบันนี้ก็สามารถทำได้เพราะห้องคอมพิวเตอร์ทุกห้องมีทั้งประตูร่วมกันและที่แยกจากกันต่างหาก เราสามารถล๊อคประตูร่วม (common door) แล้วใช้ประตูของเฉพาะแต่ละห้อง

การอ่านบาร์โค้ดยังไม่เพียงพอที่จะอนุญาตให้ผู้ใช้คนนั้นเข้าห้องคอมพิวเตอร์ได้เพราะในบางกรณีบาร์โค้ดที่นำมาให้เครื่องอ่านนั้นเป็นสำเนาที่ถ่ายเอกสารมาจากเพื่อนในภาควิชาคอมพิวเตอร์ ควรมีพนักงานงานคอยรับบัตรนักศึกษาตอนเข้าใช้ห้องคอมพิวเตอร์และคืนให้ตอน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เลิกใช้ ด้วยวิธีนี้ ยังสามารถทำการบันทึกได้ด้วยว่าผู้ใช้คนใด ๆ เข้ามาในห้องคอมพิวเตอร์ ณ เวลา และวัน ใด บ้าง

ข้อจำกัดอีกประการหนึ่งของการใช้บาร์โค้ด คือ ถ้าหากเครื่องอ่านบาร์โค้ดถูกเปิดทิ้งลืมไว้ทั้งคืน ก็จะเปิดโอกาสให้ผู้ที่มีบาร์โค้ดเข้ามาในห้องคอมพิวเตอร์แล้วทำอะไรก็ได้ แต่อย่างไรก็ตาม เครื่องอ่านบาร์โค้ดยังมีการบันทึกรหัส, วัน และเวลาที่นักศึกษารหัสนั้นเข้าใช้คอมพิวเตอร์

ควรจำกัดเวลาการให้บริการ จากที่พบเห็นอยู่ห้องคอมพิวเตอร์ให้บริการเกือบ 24 ชั่วโมง ยิ่งในเวลาดึกยิ่งมีคนน้อย บุคคลภายนอกอาจมีสำเนาบาร์โค้ดของนักศึกษาในภาควิชาแล้วสามารถเข้ามาในเวลานี้ได้

- **ทางด้านลอจิคอล**

เราท์เตอร์ที่ต่อมาจาก campus network นั้นยังเป็นเหมือนเกตเวย์ของเครือข่ายภาควิชาอีกด้วย เพราะเป็นทางเดียวที่สามารถสื่อสารจากภาควิชาออกไปภายนอกได้และยังเป็นทางออกทางเดียวกของ campus network ไปยัง nectec ด้วย ปัจจุบันเราท์เตอร์ตัวนี้เป็นเพียง ซอฟต์แวร์เราท์เตอร์ คือ มีซอฟต์แวร์ที่ทำหน้าที่เราท์ติ้งติดตั้งอยู่บน complan เพื่อป้องกันเครือข่ายจากบุคคลภายนอก น่าจะมีการติดตั้ง firewall

แต่อย่างไรก็ตามผู้ดูแลเครือข่ายของภาควิชาก็ได้ให้ความคิดเห็นว่า การติดตั้งระบบรักษาความปลอดภัยที่เข้มงวดก็ต้องแลกกับความยืดหยุ่นในการใช้บริการซึ่งในปัจจุบันของเครือข่ายภาควิชาในปัจจุบัน ยังต้องการให้บริการแก่นักศึกษาให้ได้ประโยชน์และความรู้มากที่สุด จึงไม่ได้ติดตั้งระบบรักษาความปลอดภัยที่เข้มงวดมากมายนัก

7.3.2 คอนฟิกกูเรชั่น (configuration)

เครื่องคอมพิวเตอร์บางเครื่องในห้องปฏิบัติการคอมพิวเตอร์ของภาควิชา เก่าเกินไปไม่สนับสนุนแอพพลิเคชั่นใหม่ ๆ หรือบางเครื่องก็มีอุปกรณ์ประกอบที่ไม่เหมาะสม เช่น จอโมโนโครม หรือ อุปกรณ์บางอย่างไม่มีหรือใช้งานไม่ได้ เช่น เมาส์ ซึ่งเป็นสิ่งที่จำเป็นสำหรับแอพพลิเคชั่นใหม่ เช่น โปรแกรมต่าง ๆ บนวินโดวส์ ด้วยเหตุนี้ทำให้บางครั้งเครื่องคอมพิวเตอร์ไม่เพียงพอต่อความต้องการใช้งานของนักศึกษา ควรเพิ่มอุปกรณ์เครือข่ายให้มากขึ้นเพื่อความสะดวกในการปฏิบัติงานที่จะมีมากขึ้นในอนาคต

ควรจะมี print server เพื่อความสะดวกในการทำโครงงานหลาย ๆ อย่าง ดังเช่นอุปสรรคที่เจอระหว่างทำโครงงานคือไม่สามารถพิมพ์ผลลัพธ์ของการมอนิเตอร์ออกทาง เครื่องพิมพ์ได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

7.4 แนวทางในการพัฒนา

สามารถการทำโมดูลเพื่อทำการจัดการเครือข่ายเฉพาะที่เราต้องการจะจัดการ โดยทำจากส่วน API ของ HP OpenView เพราะ API เปิดโอกาสให้ผู้บริหารกำหนดฟังก์ชั่นต่าง ๆ ในการบริหารเองได้ คล้าย ๆ กับการเขียนโปรแกรมสั่งงาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สรุปคำศัพท์

(Glossary)

- **การบริหารคอนฟิกกูเรชั่น** (configuration management) การระบุองค์ประกอบของเครือข่าย และตรวจสอบว่าพวกมันถูกติดตั้งอย่างถูกต้อง ควบคุมให้มีการเชื่อมต่อและตัดการเชื่อมต่อกับเครือข่าย และเปลี่ยนแปลงค่าที่ได้ติดตั้งขององค์ประกอบเหล่านั้นเมื่อเครือข่ายมีการเติบโตและเปลี่ยนแปลงหรือมีปัญหาเกิดขึ้น

- **การสำรอง** (backup) ใช้ในการคัดลอกในกรณีที่ต้นฉบับถูกทำลาย ไฟล์แบ็คอัพ คือ สำเนาสำรองของไฟล์คือสำเนาอันที่สองที่อาจจะถูกเก็บในเทป ฟลอปปี้ดิสก์ หรือ ฮาร์ดดิสก์ การแบ็คอัพทำให้มั่นได้ว่าถ้าสำเนาต้นถูกทำลายแล้วไฟล์สามารถกู้กลับคืนมาได้ อย่างน้อยก็บางส่วน

- **การสื่อสารกับผู้ใช้ผ่านทางรูปภาพ** (graphic user interface - GUI) คือการใช้รูปภาพแทนการป้อนคำสั่งในการสื่อสารระหว่างผู้ใช้คอมพิวเตอร์กับอุปกรณ์คอมพิวเตอร์

- **เกตเวย์** (gateway) เป็นอุปกรณ์สามารถเชื่อมต่อเครือข่ายที่ไม่เหมือนกันได้ตั้งแต่สองเครือข่ายขึ้นไปหรือเชื่อมต่อเครือข่ายเข้ากับเครื่องคอมพิวเตอร์เมนเฟรมหรือมินิคอมพิวเตอร์เกตเวย์สามารถคอนเวิร์ตทุกเลเยอร์ของมาตราฐาน 7 เลเยอร์ของโอเอสไอ ในอินเทอร์เน็ตเกตเวย์คือจุดซึ่งสามารถฟอร์เวิร์ดแพ็กเก็ตไปยังจุดอื่น ๆ ได้

- **ข้อความกระจายข่าว** (broadcast message) คือการที่ข้อความจากผู้ใช้คนหนึ่งส่งไปยังผู้ใช้ทุกคนในเครือข่ายในกลุ่มที่แน่นอน

- **คอนเซ็นเตรเตอร์** (concentrator) เป็นแหล่งศูนย์กลางที่รวมการเดินทางของข้อมูลในเครือข่ายที่มีลักษณะทางกายภาพเป็นแบบสตาร์ ทำหน้าที่เหมือนฮับ แต่อาจจะมีโมดูลที่ใหญ่กว่า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- **คอนฟิกกูเรชั่น** (configuration) เป็นกลุ่มของตัวแปรซึ่งสามารถเปลี่ยนแปลงหรือปรับได้สำหรับอุปกรณ์ฮาร์ดแวร์หรือซอฟต์แวร์ คอนฟิกกูเรชั่นอาจจะถูกปรับเปลี่ยนผ่านทางการกำหนดสวิทช์ จัมเปอร์ คำสั่งทางซอฟแวร์

- **เครือข่ายระดับท้องถิ่น** (local area network) เครือข่ายข้อมูลที่มีขนาดจำกัดทางด้านภูมิศาตร์ ในระยะใกล้ มันจัดเตรียมการสื่อสารระหว่างคอมพิวเตอร์กับอุปกรณ์เชื่อมต่อภายนอก

- **เครือข่ายระยะไกล** (wide area network - WAN) เครือข่ายการสื่อสารข้อมูลซึ่งรวมถึงลิ้งค์ที่เชื่อมต่อข้ามเครือข่ายสาธารณะ ตัวอย่างเช่น คู่สายเช่า จากบริษัทโทรศัพท์ท้องถิ่นหรือไฟเบอร์ออฟติคลิ้งค์ที่จัดเตรียมโดยหนึ่งในผู้จัดเตรียมสำหรับการสื่อสารระยะไกล

- **ไคลเอนท์** (Client) คือ ผู้ขอบริการในเครือข่ายคอมพิวเตอร์

- จุด (node) จุดในเครือข่ายซึ่งคอยจัดเตรียมการบริการ บริการที่ใช้หรือช่องทางการสื่อสารเหล่านั้นถูกเชื่อมต่อรวมกัน

- **ซีมอท** (CMIP Over TCP/IP) การขนส่งข่าวสารของซีมิพบนโปรโตคอลทีซีพี/ไอพี

- **ซีมิพ** (CMIP - Common Management Infomation Protocol) เป็นมาตราฐานการบริหารเครือข่ายของการเชื่อมต่อแบบระบบเปิด (Open System Interconnection)

- **เซิร์ฟเวอร์** (Server) คือ ผู้ให้บริหารในเครือข่ายคอมพิวเตอร์

- **ดีบีเอ็มเอส** (DBMS - Database Management System) คือระบบบริหารฐานข้อมูล โปรแกรมหรือคอลเล็คชั่นของโปรแกรมที่สร้างและบำรุงรักษาฐานข้อมูลและอนุญาตให้ผู้ใช้ค้นหาข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- **ตัวควบคุมการสื่อสารของเครือข่าย** (network interface controller) วงจรอิเลคทรอนิกส์ซึ่งเชื่อมต่อจุดกับเครือข่าย ปกติจะเป็นการ์ดที่เสียบอยู่ในเครื่องคอมพิวเตอร์

- **ทีซีพี/ไอพี** (TCP/IP - Transmission Control Protocol/Internet Protocol) เป็นกลุ่มของโปรโตคอลการสื่อสาร จัดเตรียมการเคลื่อนย้ายไฟล์และการส่งจดหมายอิเลคทรอนิกส์ ปัจจุบันนี้ TCP/IP ได้มีการใช้อย่างกว้างขวางในระบบคอมพิวเตอร์ทั่ว ๆ ไป

- **เทรสโซลด์** (Threshold) คือ จุดหรือปริมาณที่เหมาะสมหรือพอดี เช่น ซีพียู ยูทิไลเซชั่น มีปริมาณการรับ load ที่เหมาะสมเป็น 80 %

- **เทลเน็ต** (Telnet) คือการขอเข้าใช้บริการโฮสต์ตัวอื่น ๆ ที่ไม่ใช่ตัวที่ผู้ใช้กำลังใช้งานอยู่ในปัจจุบัน ตัวอย่างเช่น ผู้ใช้กำลังทำงานอยู่บน diamond และต้องการเข้าทำงานบน chaokhun ก็ต้องใช้คำสั่ง telnet chaokhun

- **บริดจ์** (birdge) เป็นอุปกรณ์ที่สามารถต่อเครือข่ายตั้งแต่สองเครือข่ายขึ้นไป ซึ่งมีโปรโตคอลในระดับดาต้าลิ้งค์เดียวกัน

- **บล๊อก** (block) เป็นคอลเล็คชั่นของข่าวสารที่ถูกส่งซึ่งอยู่ในรูปของดิสครีตเอนทิตี้ (discrete entity) ปกติบล๊อกจะประกอบด้วยข้อมูลที่เกี่ยวกับ ที่อยู่ การควบคุม การหาเส้นทาง และการตรวจหาข้อผิดพลาด

- **บันทึกเหตุการณ์** (Event log) คือฐานข้อมูลที่บันทึกเหตุการณ์ต่าง ๆ ที่เกิดขึ้นในเครือข่าย เพื่อประโยชน์ในการนำไปบริหารเครือข่าย หรือเก็บไว้เพื่อวางแผนแนวโน้มของเครือข่ายในอนาคต

- **บีเราเตอร์** (brouter) เป็นอุปกรณ์เครือข่ายซึ่งมีความสามารถในการทำงานทั้งแบบบริดจ์และเราเตอร์รวมกัน มันสามารถหาเส้นทางในโปรโตคอลระดับเน็ตเวิร์คเลเยอร์ตัวเดียวกันและทำหน้าที่เหมือนบริดจ์เมื่อเจอกับโปรโตคอลอื่น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- **แบทช์โปรเซสซิ่ง** (batch processing) เป็นรูปแบบการหนึ่งของการประมวลผลข้อมูลโดยที่ทรานแซกชั่นจะถูกจับรวมกันเป็นกลุ่มถูกส่งและประมวลผลโดยเครื่องคอมพิวเตอร์เดียวกันในเวลาเดียวกัน ในแบทช์โปรเซสซิ่ง การตอบสนองแบบทันทีทันใดไม่ใช่สิ่งที่จำเป็นนักและไม่ต้องการอินพุทจากผู้ใช้ในขณะที่ทำการประมวลผล ตัวอย่างของแบทช์โปรเซสซิ่งคือการทำบัญชีรายจ่าย เวลาการทำงานของลูกจ้างทั้งหมดถูกประมวลผลในครั้งเดียว

- **แบนด์วิธ** (bandwidth) ความสามารถของตัวอุปกรณ์หรือการเชื่อมต่อที่สามารถส่งข่าวสารได้ โดยปกติจะวัดในหน่วยของบิตต่อวินาที (bps) ในเครือข่าย แบนด์วิธที่มากกว่าก็จะให้การส่งข้อมูลที่มากกว่า และการส่งข้อมูลเร็วกว่า

- **โปรโตคอล** (protocol) กฎซึ่งตกลงกันเกี่ยวกับกลวิธีในการจัดรูปแบบ, จับเวลา, จัดลำดับ และควบคุมความผิดพลาดของข้อมูลที่จะส่งผ่านเครือข่าย

- **แพ็กเก็ต** (packet) เป็นลำดับของบิต รวมทั้งเฮดเดอร์ แอดเดรส ส่วนควบคุม และข้อมูล แพ็กเก็ตมักจะอยู่ในเลเยอร์ 3 (network layer) ของ OSI

- **แพลตฟอร์ม** (platform) เป็นชุดของซอฟต์แวร์สำหรับการทำงานของโปรแกรมอื่น ๆ เช่น Windows platform, Novell's Netware management system. Hewlett-packard's OpenView และ Sun's SunNet Manager ซึ่งทั้งหมดนี้จะเป็นแพลตฟอร์มสำหรับซอฟต์แวร์ประยุกต์สำหรับบริหารเครือข่ายอื่น ๆ

- **แพลตฟอร์มการบริหารเครือข่าย** (Network Management Platform) เป็นซอฟต์แวร์ที่ให้ในการเตรียมการบริหารเครือข่าย โดยตัวมันเองจะมีฟังก์ชั่นพื้นฐานที่ใช้ในการบริหารส่วนการบริหารอุปกรณ์ที่จำเพาะ ก็จะมีให้โปรแกรมแอพพลิชั่นอื่น ๆ มาทำงานด้วยกันโดยเชื่อมการทำงานกันผ่านทาง เอ พี ไอ หรือ ระบบเมนู

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- **มอนิเตอร์** (Monitor) คือการสังเกตการณ์ การมอนิเตอร์ในการบริหารเครือข่ายคือการสั่งให้เอเย่นต์ คอยสังเกตการณ์ เหตุการณ์ (event) แล้วส่งมาให้แพลตฟอร์มทำการบันทึก

- **มาตราฐานแอนซี** (ANSI - American National Standard Institute) เป็นสถาบันมาตราฐานแห่งชาติของอเมริกาซึ่งช่วยกำหนดมาตราฐานของเหล่าสมาชิกซึ่งเป็นอาสาสมัครและเป็นตัวแทนของอเมริกาในบางมาตราฐานที่เป็นนานาชาติ

- **ระบบบริหารเครือข่าย** (network management system - NMS) ระบบที่ใช้ในการบริหารเครือข่าย ประกอบด้วย แพลตฟอร์ม และ แอพพลิเคชั่น ที่ใช้ในการบริหารองค์ประกอบของเครือข่าย

- **ระบบปฏิบัติการของเครือข่าย** (network management system - NOS) เป็นโปรแกรมซึ่งสั่งให้คอมพิวเตอร์จัดเตรียมการบริการ (โดยเฉพาะ ไฟล์ การพิมพ์และการสื่อสาร) สำหรับไคลเอนท์ในเครือข่าย ตัวอย่างของ NOS ซอฟต์แวร์ ได้แก่ Netware, LAN Manager และ AppleShare File Server.

- **รีโมต ลอกอิน** (remote login - RMON) คือ การขอเข้าระบบหรือเครือข่ายคอมพิวเตอร์แบบทางไกล เช่น การใช้เทอร์มินอลจากลาดกระบัง ลอกอิน เข้า โฮสต์ au2.au.ac.th ที่เอแบค เป็นต้น โดยปกติจะผ่านทางโมเดม

- **เราเตอร์** (router) เราเตอร์เป็นอุปกรณ์ในเครือข่ายซึ่งสามารถเชื่อมเครือข่ายมากกว่าสองเครือข่ายเข้าด้วยกันในระดับเน็ตเวิร์คเลเยอร์ เราเตอร์สามารถส่งข้อมูลข้ามเครือข่ายได้โดยการระบุเครือข่ายปลายทาง เนื่องจากเราเตอร์ทำงานที่เน็ตเวิร์คเลเยอร์มันจึงสามารถส่งข้อมูลที่มีดาต้าลิ้งค์โปรโตคอลที่แตกต่างกันได้ เช่น อีเทอร์เน็ตและโทเค้นริง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- **ลอกอิน** (login) คือ การที่ผู้ใช้ขอเข้าในระบบหรือเครือข่ายคอมพิวเตอร์

- **เวิร์คสเตชั่น** (workstation) โดยปกติจะจำกัดอยู่ที่อุปกรณ์ซึ่งมีตัวประมวลผลเป็นของตัวเอง เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล หรือ บางครั้งก็หมายถึงเครื่องที่มีความละเอียดทางด้านกราฟฟิกสูง เช่น ยูนิกซ์

- **เวิร์ลด ไวด์ เว็บ** (world wide web - WWW) เป็นเครือข่ายการสื่อสารที่สามารถติดต่อได้ทั่วโลกที่การสื่อสารสามารถเข้าไปถึง

- **สถาปัตยกรรม** (architecture) เป็นวิธีที่ฮาร์ดแวร์หรือซอฟต์แวร์จะถูกจัดโครงสร้าง ว่าระบบหรือหรือโปรแกรมจะถูกสร้างอย่างไร องค์ประกอบต่าง ๆ จะรวมกันได้อย่างไร และเกี่ยวกับโปรโตคอลและอินเตอร์เฟสที่ถูกใช้ในการสื่อสารและการทำงานร่วมกันของโมดูลหรือองค์ประกอบของระบบ สถาปัตยกรรมของเครือข่ายได้กำหนดฟังก์ชั่นและอธิบายของรูปแบบข้อมูลและโปรแกรมย่อยที่ถูกใช้สำหรับการสื่อสารระหว่างจุด (node) หรือเวิร์คสเตชั่น (workstation)

- **สถาปัตยกรรมของเครือข่าย** (network architecture) โครงสร้างและโปรโตคอลของเครือข่ายคอมพิวเตอร์

- **ออดิต เทรล** (audit trail) เป็นบันทึกของเหตุการณ์ ระบบปฏิบัติการของเครือข่ายสามารถถูกกำหนดให้ทำการบันทึกว่าใครใช้อุปกรณ์อะไรบ้างที่เวลาใด ๆ เป็นเครื่องมือที่มีความสำคัญในการบริหารเครือข่าย โดยเฉพาะการบริหารทางด้านแอคเค้าน์ติ้ง (Accounting management) และความปลอดภัย (Security management)
- **ออนไลน์ ทรานแซกชั่น** (Online Transaction) การทำทรานแซกชั่นแบบออนไลน์ ทรานแซกชั่นที่ทำจะถูกประมวลผลในทันที ณ เวลาที่ทำงาน

- **อัตราการใช้งาน** (Utilization) คือ การใช้งานของอุปกรณ์ใด ๆ เทียบกับความสามารถที่จะรับได้ของอุปกรณ์ตัวนั้น เช่น สายโคแอกเชี่ยล สามารถรองรับทราฟฟิกได้ 10 เมกกะบิตต่อวินาที

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

และจากการมอนิเตอร์พบว่าทราฟฟิกในสายตอนนี้เป็น 5 เมกกะบิตต่อวินาที จะได้ว่า Utilization ของ สายตอนนี้เท่ากับ 50 %

- **อินเทอร์เน็ต** (Internet) เป็นการเชื่อมต่อของเครือข่ายต่าง ๆ ที่มีอยู่ตามที่ต่าง ๆ ในโลก ผู้ที่อยู่บนอินเทอร์เน็ตสามารถติดต่อไปยังที่ใด ๆ ก็ได้ ที่เชื่อมต่ออยู่กับอินเทอร์เน็ตด้วยกัน

- **เอทีเอ็ม** (ATM - Asynchronous Transfer Mode) เป็นเทคโนโลยีแบบคอนเน็คชั่นโอเรียนเต็ด (Connection-Oriented) ทั้งในเครือข่ายระยะไกล (WAN) และ เครือข่ายในท้องถิ่น (LAN) ซึ่งอาศัยพื้นฐานของการสวิทชิ่งความเร็วสูง (High-speed switching) ของเซลล์ที่มีขนาด 53 ไบต์ สามารถรองรับการส่งข้อมูลที่มีแบนด์วิธกว้าง ๆ ได้ดี

- **เอ็ม ไอ บี** (MIB) เป็นฐานข้อมูลที่ใช้ในการบริหารเครือข่ายมีโครงสร้างแบบระดับชั้น (heirachical) ใช้ในการกำหนดอินฟอร์เมชั่นซึ่งสามารถนำมาบริหารเครือข่ายได้

- **เอเจ็นต์** (Agent) คือ ซอฟต์แวร์ที่ทำหน้าที่ในการเก็บข้อมูลเพื่อส่งมาให้ศูนย์บริหารเครือข่ายนำไปใช้ และรับคำสั่งจากศูนย์ ฯ เพื่อไปทำงานกับส่วนที่มันเชื่อมต่ออยู่ ตัวอย่างของเอเย่นต์ เช่น โปรแกรมบริหารเราท์เตอร์ที่ผู้ขายให้มากับเราท์เตอร์

- **เอส เอ็น เอ็ม พี** (SNMP - Simple Network Management Protocol) เป็นโปรโตคอลซึ่งอนุญาตให้บริหารสเตชั่นหรือคอนโซลบนเครือข่ายเพื่อรับข้อมูลที่จะนำไปใช้ในการบริหารและส่งคำสั่งเพื่อกระจายไปยังเอเย่นต์ (agent) ที่ติดตั้งไว้แล้ว ในหลาย ๆ เอนทิตี้ที่แตกต่างกัน เช่น คอนเซนเตรเตอร์ เราเตอร์ หรือเซิร์ฟเวอร์

- **แอดเดรสต้นทาง** (source address) เป็นส่วนของข้อความซึ่งบ่งบอกว่าใครเป็นคนส่งข้อความ มักจะรวมอยู่ในส่วนหัวของแพ็กเก็ต

- **แอดเดรสปลายทาง** (destination address) เป็นส่วนหนึ่งข้อความซึ่งบอกรู้ว่าข้อความนี้จะส่งไปที่ไหน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- **แอพพลิเคชั่น** (application) เป็นซอฟต์แวร์โปรแกรมซึ่งใช้ประโยชน์ในงานเฉพาะอย่าง ตัวอย่างเช่น Database manager, spreadsheets, communications packages, graphics programs และ word processors

- **แอพพลิเคชั่นบนแวน** (WAN Application) เป็นการใช้โปรแกรมประยุกต์บนเครือข่ายระยะไกล (ดูคำว่า WAN และ application) ตัวอย่างของแอพพลิเคชั่นบนแวน ได้แก่ การเคลื่อนย้ายไฟล์ (ftp), การเรียกดูโฮมเพจทางอินเทอร์เน็ต (netscape), การรับ-ส่ง E-mail เป็นต้น

- **แอพพลิเคชั่นโปรแกรมอินเตอร์เฟส** (application program interface-API) เป็นเซ็ตของคำสั่งและรูปแบบ ปกติจะเป็นภาษาในการเขียนโปรแกรม สำหรับให้โปรแกรมเมอร์ใช้ในการพัฒนาแอพพลิเคชั่น API ทำให้การพัฒนาโปรแกรมและการปรับปรุงฟังก์ชั่นทำได้ง่ายขึ้น เช่น องค์ประกอบของ GUI ตัว API จะทำให้มันง่ายต่อผู้พัฒนาโปรแกรมที่จะสร้างโปรโตคอล

- **ฮับ** (hub) เป็นอุปกรณ์ซึ่งทำหน้าที่ในระบบดับฟิสิคอลซึ่งเป็นศูนย์กลางในระบบเครือข่ายที่ต่อแบบสตาร์ทุก ๆ จุดจะต่อสายเคเบิลจากฮับ

- **โฮสต์** (host) เป็นระบบคอมพิวเตอร์ปกติมักจะเป็นเมนเฟรมหรือมินิคอมพิวเตอร์ ซึ่งจัดเตรียมการบริการสำหรับผู้ใช้จำนวนหนึ่ง ในอินเทอร์เน็ตจุดใด ๆ อาจจะเป็นโฮสต์หรือเกตเวย์ก็ได้ แต่โฮสต์ไม่สามารถฟอร์เวิร์ดแพ็กเก็ตได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

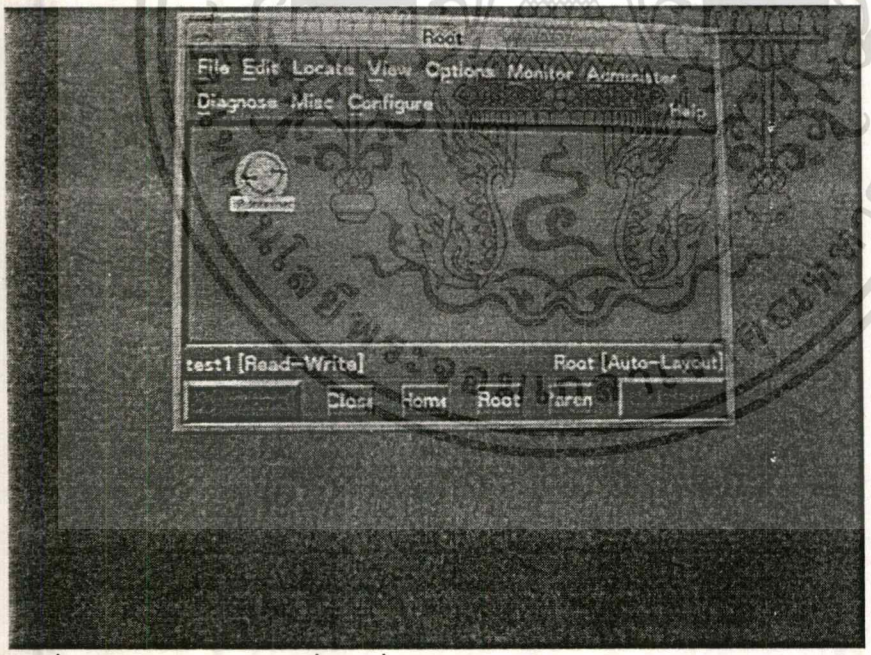
ภาคผนวก ก

HP OpenView management Platform

หมายถึง ผลิตภัณฑ์ที่เป็นซอฟท์แวร์ ที่ให้ผู้พัฒนาโปรแกรมประยุกต์ทำการสร้าง multivendor network management application ซึ่งตัว Openviw platform นี้มีทั้งเหตุการณ์ และ ข้อมูลบริการการบริหาร ติดต่อกับผู้ใช้โดยใช้กราฟฟิค ไปยัง platform การบริหารระบบเครือข่าย ก็คือ Hp OpenView Windows

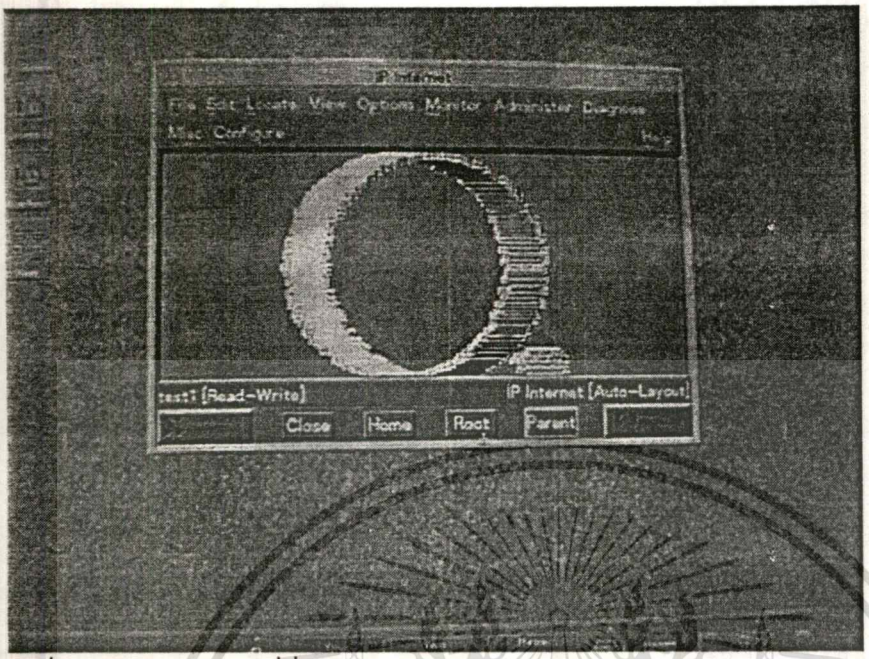
Hp OpenView Windows ก็หมายถึงเป็นวิธีการเชื่อมต่อไปยังผู้ใช้ สำหรับ Hp OpenView Windows SNMP Platform ซึ่งแสดงแผนของระบบเครือข่าย และรวบรวมโปรแกรมประยุกต์การบริหาร และระบบการบริหาร ดังนั้นผู้ใช้สามารถบริหารระบบบนระบบเครือข่ายของเขา

แนะนำ Hp OpenView

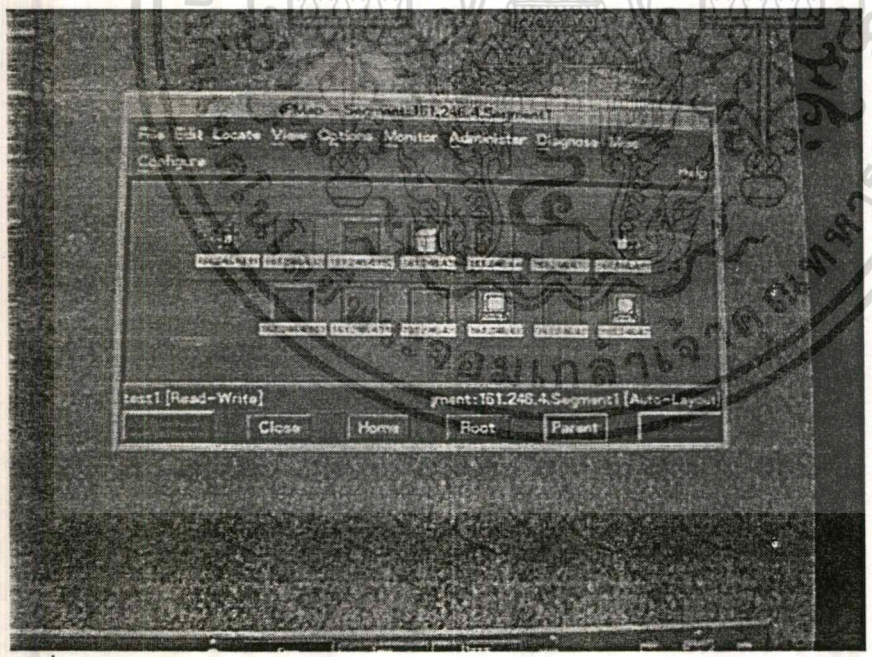


รูปที่ 1 หน้าต่างแสดงแผนที่แรกที่ทำงาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

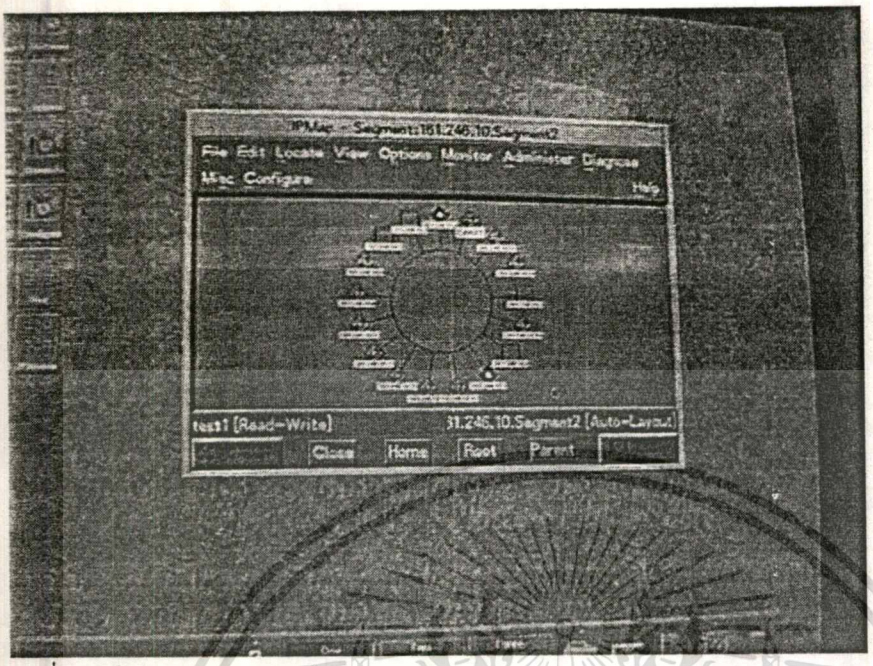


รูปที่ 2 หน้าต่างแสดงแผนที่ที่ 2 ของการทำงาน(รายละเอียด)

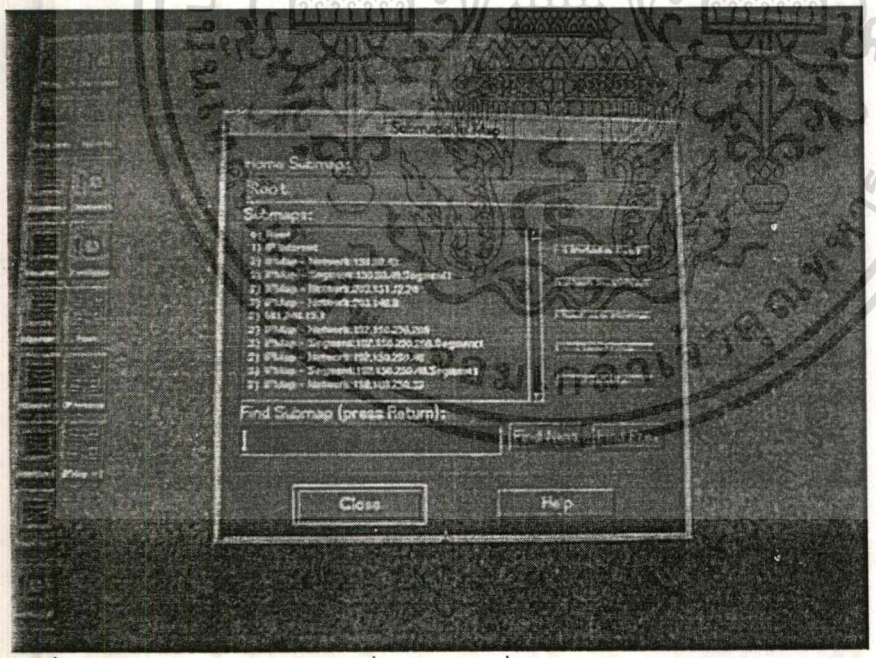


รูปที่ 3 หน้าต่างแสดงระบบเครือข่ายหมายเลขใด ๆ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

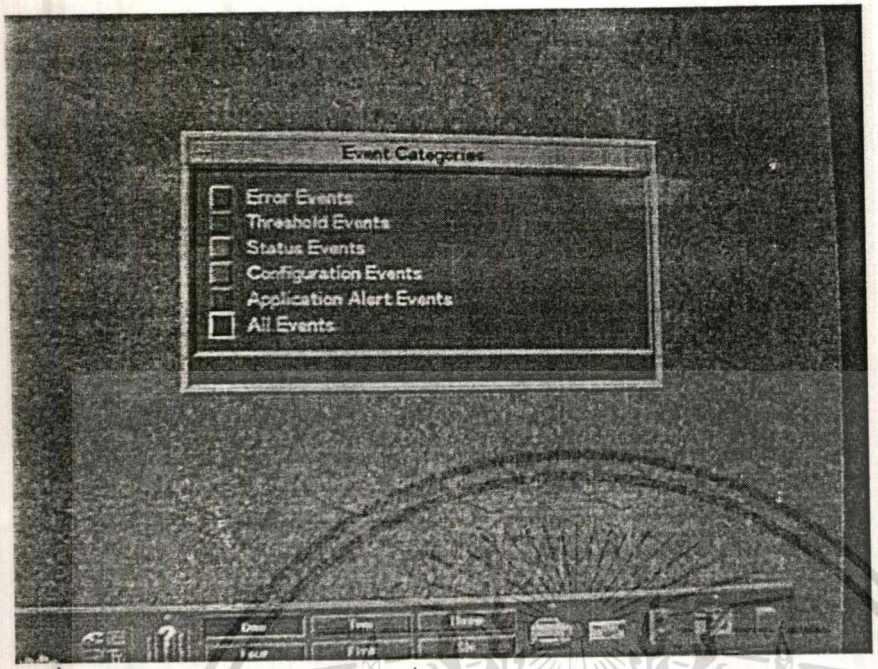


รูปที่ 4 หน้าต่างแสดงระบบเครือข่าย เจาะจง segment

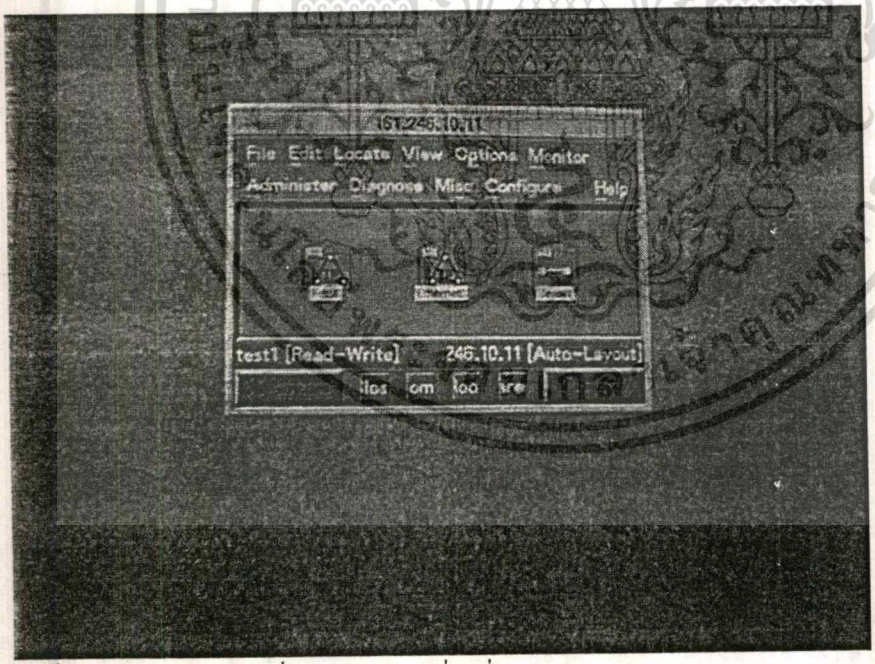


รูปที่ 5 หน้าต่างแสดงการเลือกแผนที่ย่อยในแผนที่ใหญ่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

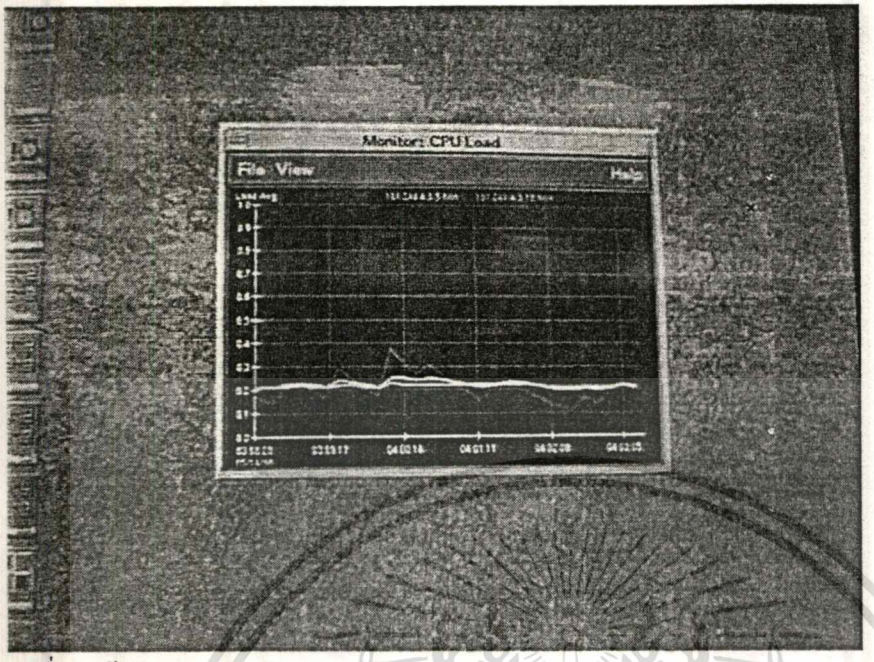


รูปที่ 6 หน้าต่างแสดงชนิดของเหตุการณ์ต่าง ๆ

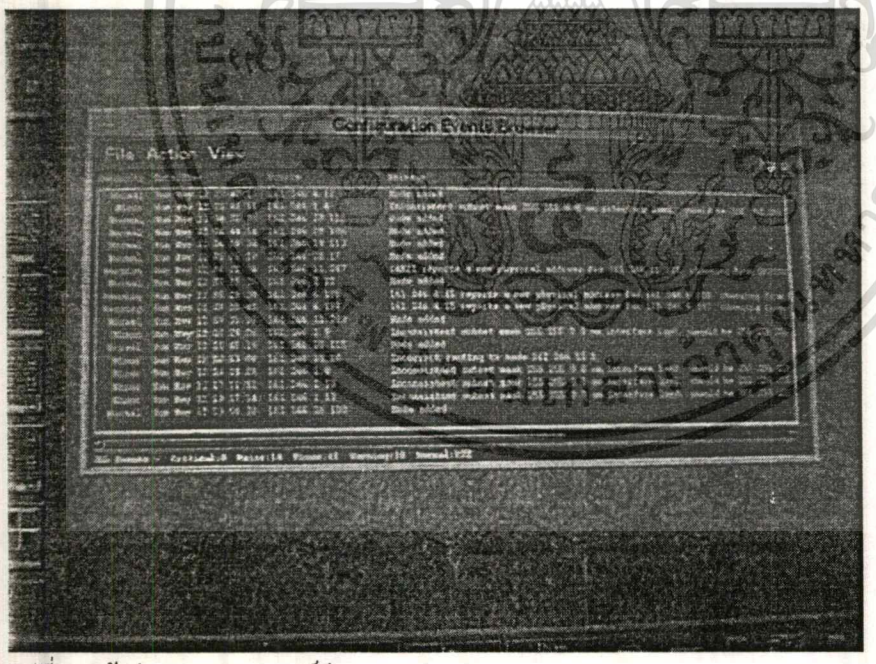


รูปที่ 7 หน้าต่างแสดงการเชื่อมต่อภายในเครื่องที่ตรวจสอบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 8 หน้าต่างแสดงกราฟการตรวจจับ



รูปที่ 9 หน้าต่างแสดงเหตุการณ์ต่าง ๆ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Title: System Information : 161.246.4.3

Name or IP Address: 161.246.4.3

System Name : diamond.ce.kmitl.ac.th

System Description : HP-UX diamond B.10.01 A 9000/827 703625111

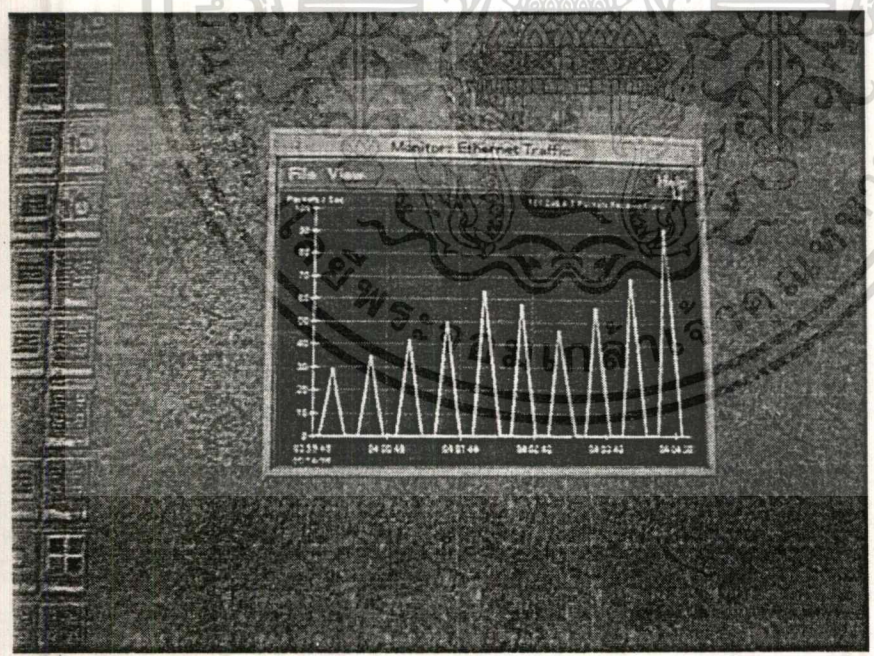
System Contact :

System Location :

System Object ID : .iso.org.dod.internet.private.enterprises.hp.nm.system.hpux.hp9000s800

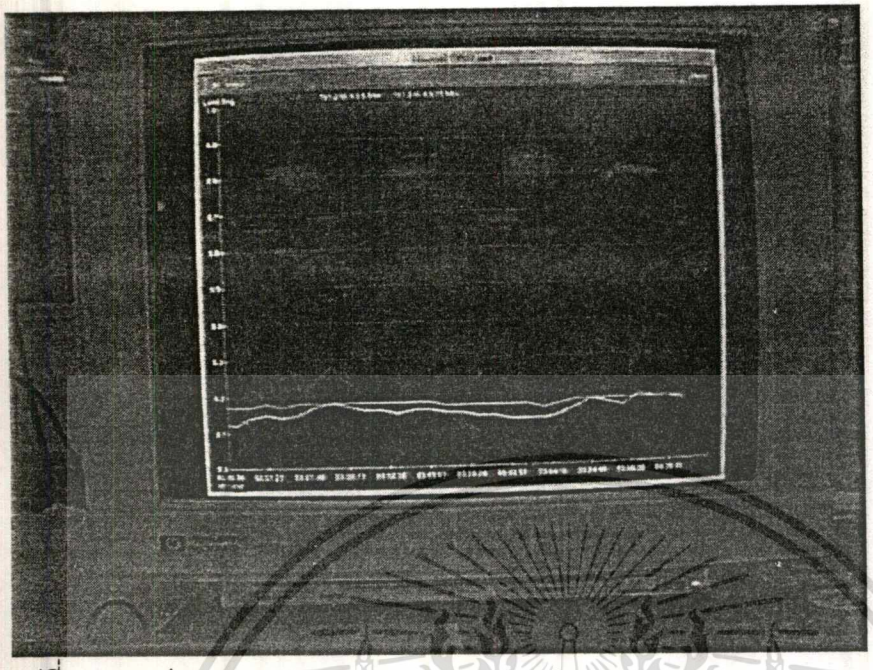
System Up Time : (4430944) 12:18:29.44

รูปที่ 10 ข้อมูลเกี่ยวกับระบบ

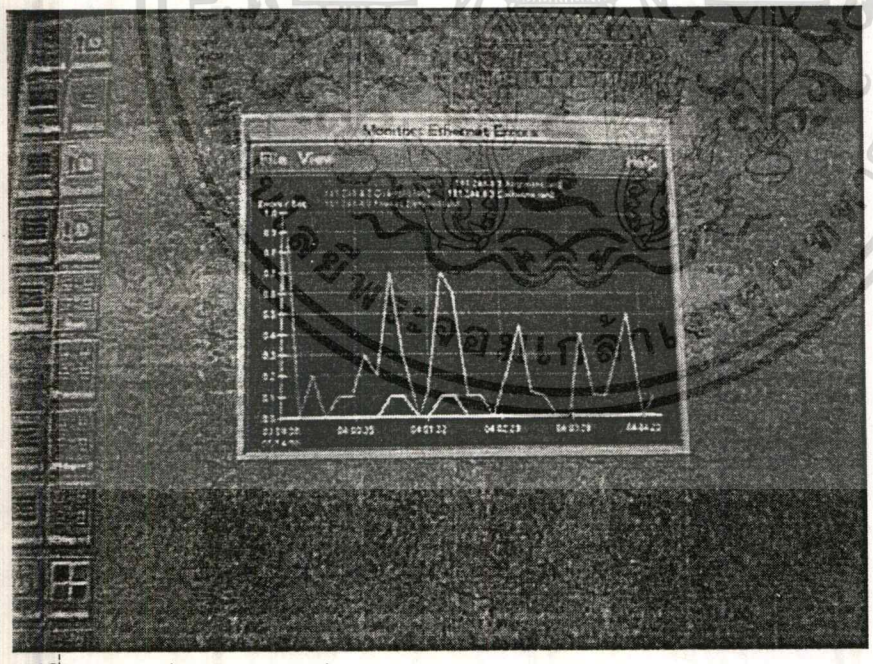


รูปที่ 11 กราฟแสดง packet in และ packet out ของ 161.246.4.3

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

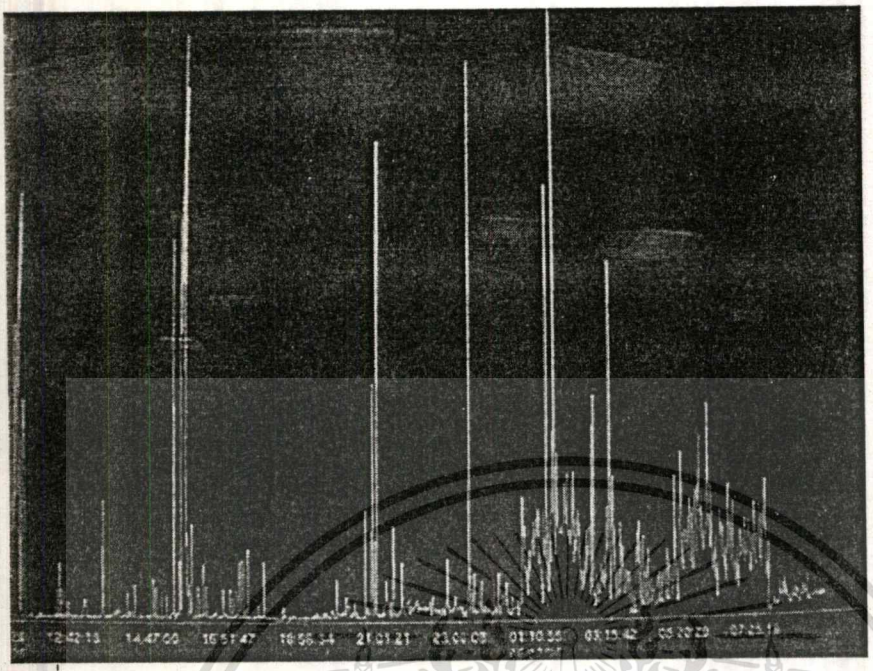


รูปที่ 12 กราฟแสดง cpu load ของ 161.246.4.3

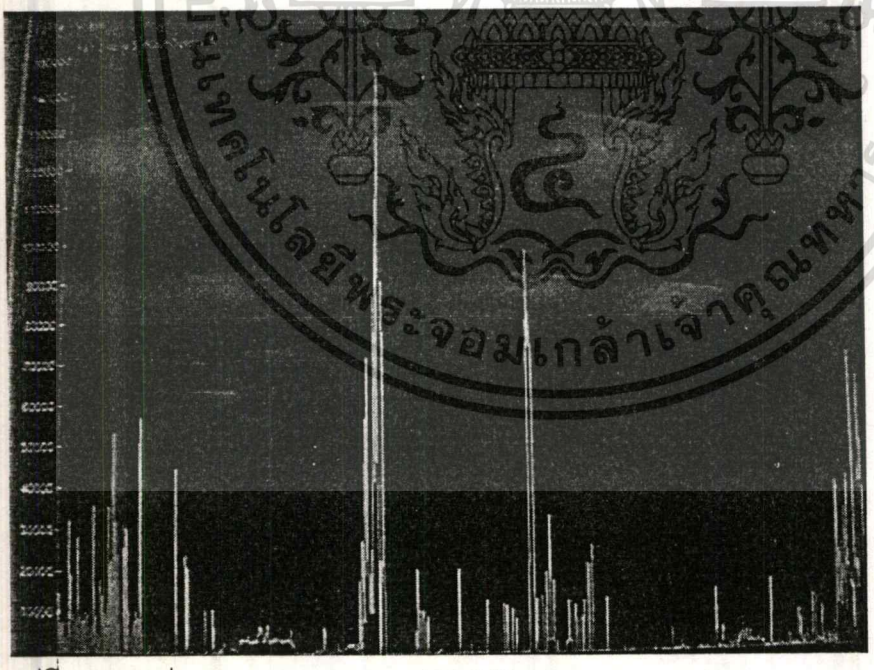


รูปที่ 13 กราฟแสดง error ต่าง ๆ ของ 161.246.4.3

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

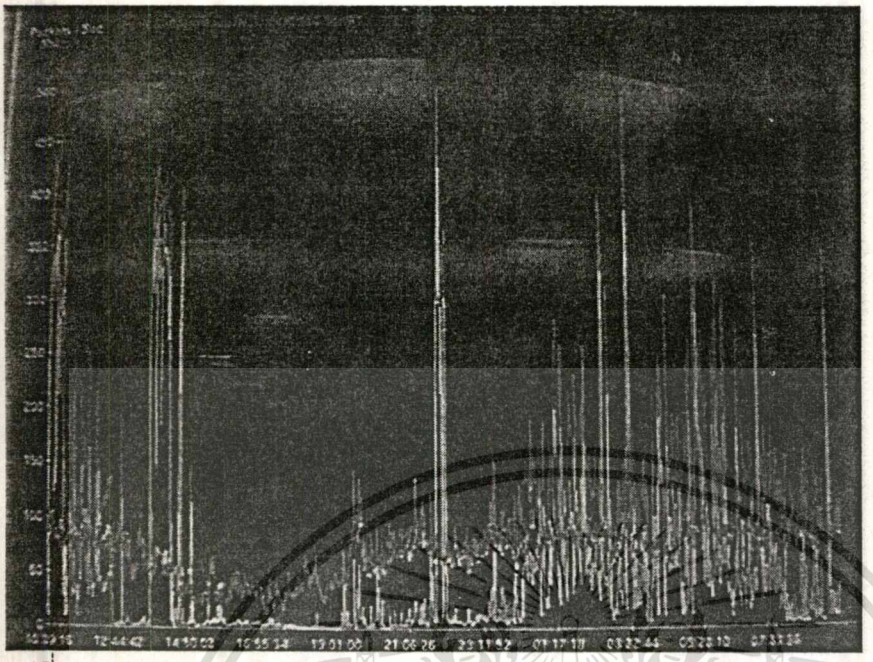


รูปที่ 14 กราฟแสดง octet in ของ 161.246.4.3

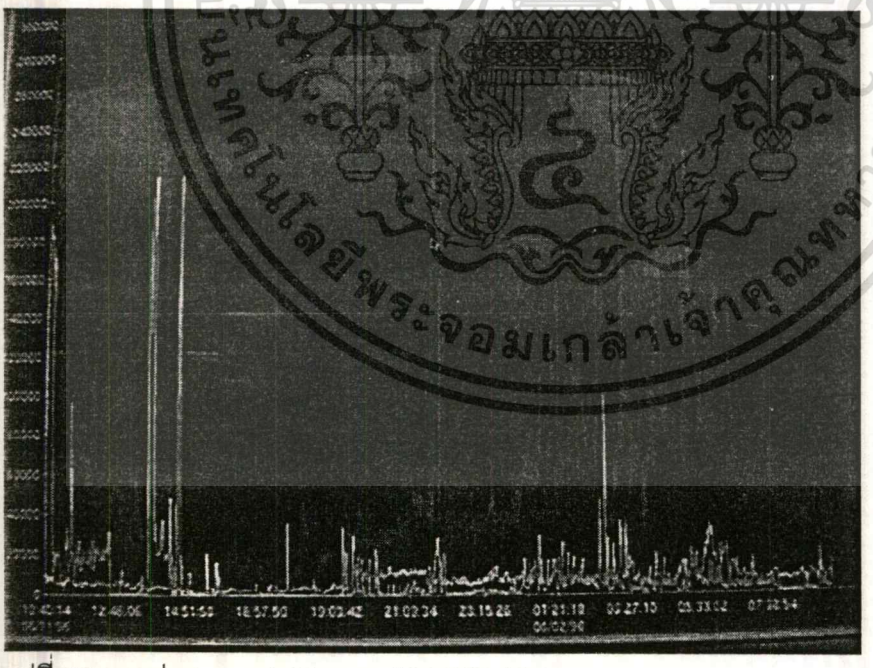


รูปที่ 15 กราฟแสดง octet out ของ 161.246.4.3

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

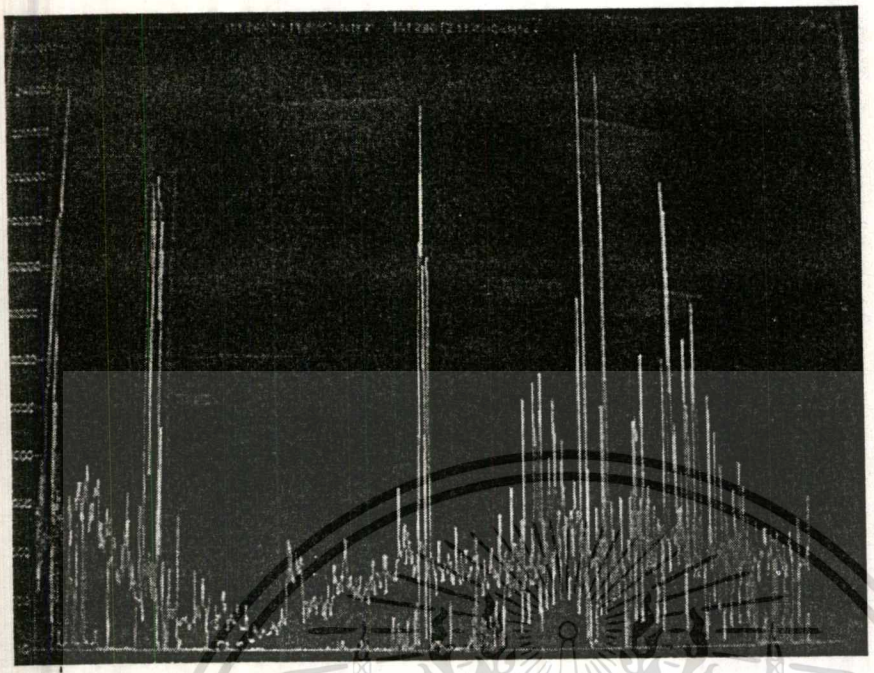


รูปที่ 16 กราฟแสดง packet in และ packet out ของ 161.246.10.11



รูปที่ 17 กราฟแสดง octet in ของ 161.246.10.11

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 18 กราฟแสดง octet out ของ 161.246.10.11

ขั้นตอนการเข้าใช้ HP OpenView

1.$ xhost +161.246.10.223

2.$ telnet 161.246.10.223

3.login ben

4.passwd heart36014236

5.$ DISPLAY=161.246.4.7:0.0

6.$ export DISPLAY

7.$ cd /usr/OV/bin

8.ovw

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

คีย์การทำงานต่าง ๆ ภายใน HP OpenView

1. Event ต่าง ๆ ที่บอกเกี่ยวกับเหตุการณ์ต่าง ๆ ที่เกิดขึ้นมีดังต่อไปนี้
   - ErrorEvent ยกตัวอย่างในกรณีที่ทำการแทร็พแต่ไปไม่ถึงจุดหมายปลายทาง ก็จะมีการแจ้งให้ทราบว่าเครื่องใดทำการแทร็พ และ ไปไม่ถึงเครื่องใด
   - StatusEvent บอกเกี่ยวกับวันเวลา, ต้นทาง, ปลายทาง,โหนดที่เสีย หรือระบบเครือข่ายส่วนใดที่เสีย รวมถึงระดับความรุนแรงที่เกิดขึ้นด้วย
   - ConfigurationEvent เหตุการณ์ทุกอย่างที่เกี่ยวข้องกับการจัดตั้งระบบ เช่น การเพิ่มเครื่องใหม่, การเปลี่ยน physical address ของเครื่อง และการทำการ routing ที่ไม่สำเร็จของเครื่องใด ๆ
2. Topology status polling เป็น option หนึ่งในหลาย ๆ option
   - สามารถกำหนดช่วงเวลาในการ poll ได้
   - กำหนดการลบเครื่องที่เสียได้ภายในกี่วันก็ได้
   - กำหนดให้มีค้นหาเครื่องใหม่ หรือไม่ก็ได้
3. Network configuration
   - interface บอกเกี่ยวกับ interface ประเภทหรือชนิดใด, แพ็กเก็ตเข้าออกเป็นจำนวนเท่าใด, ความผิดพลาดของขาเข้าและออกเป็นเท่าใด
   - address บอกที่อยู่ของ object ที่เราทำการตรวจสอบอยู่
   - Routing table
   - ARP CACHE
   - service มีการใช้โปรโตคอลอะไรบ้าง เช่น tcp,udp
4. Device Configuration มีอยู่ 2 อย่าง
   - System information บอกรายละเอียดของ object ที่ทำการตรวจสอบ เช่น Name, Description, Contact, Location, Object ID และ Uptime
   - SNMP Event Notification รับข้อมูลจากการ Notification ของเครื่องใดบ้าง
5. Network Connectivity การติดต่อกับระบบเครือข่ายอื่น ๆ ได้หลายวิธี
   - Demand Poll ทำการ poll ไปยังเครื่องที่ต้องการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Ping
- Remote Ping ต้องทำงานบน HP OpenView SNMP Agent ถึงได้
- Locate Route กำหนดให้ทำการ route ไปที่ไหน

6. Terminal connect ทำการติดต่อกับเครื่องอื่นได้ 2 แบบคือ Telnet(hpterm)- Telnet(xterm)
7. Event SNMP เหตุการณ์ที่ได้ขึ้นบนการใช้ SNMP- เครื่องในแผนที่เสีย (node down)- เครื่องในแผนที่เพิ่มขึ้น (node up)
8. Network activity มีอยู่ 4 ประเภท
   - TCP connection เก็บค่าว่าใครเข้ามาหาเรา ทำอะไรกับเรา เช่น HTTP, TELNET, finger
   - Interface traffic
   - SNMP เกี่ยวเรื่องต่าง ๆ ที่รันบน SNMP
   - interface
   - traffic
   - error
   - Ethernet เกี่ยวกับเรื่องต่างๆ บน Ethernet- traffic- error
9. System activity มีอยู่ 2 ประเภท
   - CPU load การรับภาระของหน่วยประมวลผลกลาง
   - Disk space พื้นที่ว่างในแต่ละไดเรคทอรีของเครื่องที่เราตรวจสอบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก ข

คำศัพท์ที่เกี่ยวกับ HP OpenView

1. Agent หมายถึง ขบวนการที่รันบนโหมดเพื่อตอบสนอง SNMP request และส่ง SNMP trap หรืออาจจะหมายถึงเครื่องที่ตอบสนอง SNMP request และส่ง SNMP trap
2. Child submap รายละเอียดการมองของออบเจ็ค ข้อความของออบเจ็คบนแผนที่ ดับเบิ้ลคลิ้กบนสัญลักษณ์ เพื่อเปิด child submap
3. Event หมายถึง การแจ้งข้อความที่ไม่ใช่ร้องขอจาก manager หรือ SNMP agent ซึ่งเกิดขึ้นจากสาเหตุต่อไปนี้
   - เกิดความผิดพลาดขึ้น
   - เกินจำนวนจำกัด threshold
   - สถานะออบเจ็คเปลี่ยน
   - configuration ของออบเจ็คเปลี่ยน
4. IP address บ่งชี้เครื่องที่อยู่บนระบบเครือข่าย ซึ่ซ้ ปี รโตคอล TCP/IP โดยแต่ละเครื่องดังกล่าวต้องมี IP address เป็นเอกลักษณ์ แบ่งออกเป็น 2 ส่วน
   - Network field กล่าวถึงระบบเครือข่ายแบบ physical ของอินเทอร์เน็ต
   - Host field กล่าวถึงเครื่องที่ติดต่อกับระบบเครือข่ายแบบ physical
5. Interface การเชื่อมต่อทั้งแบบ logical และ physical ของเครื่องไปยังระบบเครือข่าย อาจเป็นทั้งซอฟท์แวร์ และ ฮาร์ดแวร์ เช่น แลนซอฟท์แวร์ (netware),Ethernet LAN card หรือ ตัวแปลงสัญญาณให้เหมาะสมกับสาย (cable transceivers)
6. MIB application เป็นโปรแกรมประยุกต์ เพื่อตรวจสอบอุปกรณ์ระบบเครือข่ายแบบ multivendor ผ่าน SNMP
7. MIB object คือ manage object ที่กำหนดตาม RFCD 1155 : โครงสร้างและการบ่งชี้ขอข้อมูลการบริหารสำหรับ TCP/IP base Internet
8. Managed object หมายถึง object ซึ่งถูกบริหารแบบแอ็คทิพ สามารถตรวจสอบและบริหาร object โดยใช้ topology, สถานะ และการเขียนการบริหารระบบ managed object แสดงสถานะของมันบน submap ของแผนที่เปิดอยู่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

9. Management Region ชุดของ managed object บนเฉพาะแผนที่ซึ่ง กำหนดขอบเขตของระบบเครือข่ายที่จะบริหารแตกต่างตามแผนที่
10. Manager ระบบซึ่ง execute ซอฟท์แวร์การบริหาร เช่น HP OpenView
11. Name ถูกบริหารให้กับ element OpenView ที่แตกต่างกัน เช่น object, แผนที่, แผนที่ย่อย และ สัญลักษณ์
12. Network Analyzer อุปกรณ์ระบบเครือข่ายซึ่งรับการจราจรบนแลน สามารถโปรแกรมให้มันตรวจสอบพิจารณา และ กรองข้อมูลการจราจรที่มันได้รับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หนังสืออ้างอิง

ก วารสาร

1. สาทิพย์ กองจันทรา ,"เครือข่ายเสมือน เทคโนโลยีแห่งอนาคต(VLAN-Technology of Future)" ,ไมโครคอมพิวเตอร์,ฉบับที่ 135 ,ตุลาคม 2539 ,หน้า 212-219
2. "รอบรู้เรื่องVLAN" ,Business Computer Magazine ,ฉบับที่ 96 ,กุมภาพันธ์ 2540 ,หน้า 161-164

ข หนังสือ

1. "เครือข่ายคอมพิวเตอร์ " ,ฟิสิกส์เซ็นเตอร์ ,281 หน้า ,2536
2. Alan R. Simon ,"Network Re-Engineering : Foundations of enterprise computing" ,AP Professional
3. Allan Leinwand and Karen Fang Conroy ,"Network Management : A Practical Perspective 2nd Edition" ,Addison-Wesley ,338 p ,1996
4. Joseph M. Veoni ,"IEEE 1992 Network Operations and Management Symposium : Overview of An Integrated Network Management Architechture for A Large Heterogeneous Network" ,pp 10.3.1-10.3.11
5. Kornel Terplan ,"IEEE 1992 Network Operations and Management Symposium : Standardized Multivendor Network Management" ,pp 16.1.1-16.2-1.11
6. Marshall T. Rose ,"The Simple Book: An Introduction to Internet Management. 2nd ed." ,Prentice-Hall ,1994
7. Robert P. Davidson and Nathan J. Muller ,"Internet working LANs : Operation ,Design and Management" ,Artech House

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

8. Sameh Rabie and Xi-Nam Dam ,"IEEE 1992 Network Operations and Management Symposium : AIntegrated Architecture for LAN/WAN Management" ,pp 10.1.1-10.1.11
9. Steve Steinke ,"Guide to Managing PC Networks : Tools and Techniques for Running LANs" ; Prentice Hall ,392 p ,1995
10. William Stallings ,"SNMP, SNMPv2, and CMIP : The Practical Network Management" ,Addison-Wesley ,1996.

ค WWW

1. Douglas W. Stevenson ,"Network Management : What it is and what it isn't." ,http://net man.cit.buffalo.edu/Doc/DStevenson/
2. Marcus J. Ranum ,"How to pick an Internet Firewall" ,http://www.v-one. com/newpag es/fwpick.html
3. "Network Management Server (SMS)" ,http://netman.cit.buffalo.edu/
4. "NCSA - National Computer Security Association" ,http://www.ncsa.com/
5. "HP Openview" ,http://www.hp.com:80/nsmd/ov/main.html
6. "And Communications, Glad To Have You Here" ,http://www.and.com

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

การทำโครงงานรวมทั้งการทำวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี โดยได้รับความช่วยเหลือและได้รับความแนะนำจากบุคคลหลายท่าน ได้แก่

ท่านอาจารย์บรรจง ปิยธำรง และท่านอาจารย์ประทีป บัญญัตินพรัตน์ เป็นอาจารย์ที่ปรึกษาและคอยให้คำแนะนำและเสนอแนวทางในการทำโครงงานนี้

ขอบคุณคณาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้ให้มีความสามารถที่จะทำโครงงานนี้ได้

พี่จุ๊กและพี่กฤต พี่นักศึกษาปริญญาโท คณะเทคโนโลยีสารสนเทศ ที่ให้ความรู้เกี่ยวกับการใช้โปรแกรม HP OpenView และแนะนำรายละเอียดต่าง ๆ ที่เป็นประโยชน์ให้เป็นข้อมูลในการทำงาน

พี่อ๋ำ ที่ปรึกษาทางด้านภาษาต่างประเทศ

คิมและหนุ่มแห่งภาควิชาอุตสาหกรรมอาหาร ผู้เอื้อเฟื้อเครื่องพิมพ์เลเซอร์ในการพิมพ์วิทยานิพนธ์ฉบับนี้

ตี๋เล็กเพื่อนผู้แสนดี ที่ทำให้มีเสียงเพลงระหว่างการทำงาน

รวมทั้งเพื่อน ๆ น้อง ๆ และผู้ไม่ประสงค์จะออกนามทุกคนที่ทำให้เวลาทำงานเต็มไปด้วยความคึกคื้น ไม่เงียบเหงา

คณะผู้จัดทำขอแสดงความนับถือ และขอขอบพระคุณในความกรุณาของทุก ๆ ท่านที่ได้เอ่ยนามมาแล้วข้างต้น รวมทั้งผู้ที่ไม่ต้องการเปิดเผยนาม มาไว้ ณ โอกาสนี้

คณะผู้จัดทำ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้