การออกแบบวิธีการเฝ้าติดตามและวิธีการแก้ไขปัญหาการทำงานของแลน

นายอนุวัฒน์ จีนะวัฒน์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2544
ISBN 974-03-1119-9

A DESIGN OF MONITORING AND PROBLEM SOLVING METHODOLOGY FOR LOCAL AREA NETWORKS

Mr.Anuwath Jeenawath

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science in Computer Science

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2001

ISBN 974-03-1119-9

หัวข้อวิทยานิพนธ์	การออกแบบวิธีการเฝ้าติดตามและวิธีการแก้ไขปัญหาการทำงานของแลน
โดย	นายอนุวัฒน์ จีนะวัฒน์
ภาควิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษา	ผู้ช่วยศาสตราจารย์ วิชาญ เลิศวิภาตระกูล
อาจารย์ที่ปรึกษาร่วม	รองศาสตราจารย์ สมชาย ทยานยง

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร.สมศักดิ์ ปัญญาแก้ว)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(รองศาสตราจารย์ ดร.วันชัย ริ้วไพบูลย์)

..... อาจารย์ที่ปรึกษา
(ผู้ช่วยศาสตราจารย์ วิชาญ เลิศวิภาตระกูล)

..... อาจารย์ที่ปรึกษาร่วม
(รองศาสตราจารย์ สมชาย ทยานยง)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ สุเมธ วัชระชัยสุรพล)

อนุวัฒน์ จีนะวัฒน์ : การออกแบบวิธีการเฝ้าติดตามและวิธีการแก้ไขปัญหาการทำงานของแลน (A DESIGN OF MONITORING AND PROBLEM SOLVING METHODOLOGY FOR LOCAL AREA NETWORKS)
อ.ที่ปรึกษา : ผู้ช่วยศาสตราจารย์ วิชาญ เลิศวิภาตระกูล, อ.ที่ปรึกษาร่วม : รองศาสตราจารย์ สมชาย ทยานยง, 143 หน้า. ISBN 974-03-1119-9

วิทยานิพนธ์ฉบับนี้มีวัตถุประสงค์เพื่อออกแบบวิธีการและขั้นตอนการดำเนินงานในการตรวจวัดข้อผิดพลาดของระบบเครือข่ายและเป็นแนวทางในการแก้ไขปัญหาของอุปกรณ์เครือข่ายสื่อสาร รวมทั้งเป็นแนวทางในการสร้างระบบสำหรับวางแผนการดูแลและบำรุงรักษาเครือข่าย โดยระบบที่ทำการออกแบบสามารถระบุความสามารถของแต่ละผู้ใช้ได้ตามความสำคัญ และทำการศึกษาโปรแกรมจัดการเครือข่ายที่มีโมดูลที่เฝ้าติดตามและวิธีการแก้ปัญหาการทำงานของแลนเพื่อนำมาใช้งาน รวมทั้งได้ออกแบบเพิ่มเติมในส่วนของการเตรียมอุปกรณ์หรือเครื่องมือเครื่องใช้ในการแก้ไขปัญหาต่างๆ ที่เกิดขึ้นในระบบเครือข่าย เพื่อให้สามารถใช้ในการแก้ไขปัญหาระบบแลนได้รวดเร็วและมีประสิทธิภาพมากยิ่งขึ้น

จากการวิจัยพบว่า ระบบที่ทำการออกแบบสามารถอำนวยความสะดวกให้กับผู้ใช้งานเป็นอย่างมากสามารถส่งงานระหว่างพนักงานที่ปฏิบัติงานตามคาบเวลาได้อย่างมีประสิทธิภาพ มีรายงานแสดงถึงสถานะของอุปกรณ์แต่ละชนิดทำให้สามารถรายงานต่อผู้บริหาร เพื่อเป็นข้อมูลในการตัดสินใจในการปรับปรุงระบบเครือข่าย นอกจากนี้ยังสามารถใช้ข้อมูลเพื่อเป็นแนวทางในการวางระบบเครือข่ายแลน โดยมีการพิจารณาว่าก่อนที่จะทำการติดตั้งระบบเครือข่ายแลนให้มีประสิทธิภาพนั้น ควรเตรียมการอย่างไรบ้าง และหลังจากติดตั้งควรทำอย่างไร

ภาควิชา .....วิศวกรรมคอมพิวเตอร์..... ลายมือชื่อนิสิต.....
สาขาวิชา....วิทยาศาสตร์คอมพิวเตอร์..... ลายมือชื่ออาจารย์ที่ปรึกษา.....
ปีการศึกษา..2544..... ลายมือชื่ออาจารย์ที่ปรึกษาร่วม.....

4171522121 : MAJOR COMPUTER SCIENCE

KEY WORD : LAN, NETWORK, PROBLEM SOLVING

ANUWATH JEENAWATH : THESIS TITLE. (A DESIGN OF MONITORING AND PROBLEM SOLVING METHODOLOGY FOR LOCAL AREA NETWORKS) THESIS ADVISOR : ASSIST. PROF. WICHARN LERTWIPATRAKUN, THESIS CO-ADVISOR : ASSO.PROF.SOMCHAI THAYARNYONG, 143 pp. ISBN 974-03-1119-9

The objective of the thesis is to design method and monitor process of network management, including problem solving support on network device. The author had suggested a guideline to create and planning network management maintenance. The design can define user's priority and feasibility on network management program module usage for monitoring and trouble shooting of the local area networks (LAN). Besides, there is the additional design to support device preparation per case for faster and more efficient on network problem solving.

The research indicated the design of monitoring and problem solving methodology for local area networks was very convenience to usage. The operator can increase co-ordinate efficiency to send job between period, including the device status report to decision-making involves adapted network system. Furthermore, the information is a guideline to implement local area network system how to consider pre-implementing and post-implementing for more efficiency and advantage.

Department .....Computer Engineering..... Student's signature.....

Field of study .....Computer Science..... Advisor's signature.....

Academic year ....2001..... Co-advisor's signature.....

กิตติกรรมประกาศ

ในการทำวิทยานิพนธ์ฉบับนี้ผู้เขียนขอกราบขอบพระคุณ อาจารย์ที่ปรึกษาวิทยานิพนธ์ รองศาสตราจารย์ สมชาย ทยานยง และผู้ช่วยศาสตราจารย์ วิชาญ เลิศวิภาตระกูล ซึ่งท่านได้เสียสละเวลาให้คำแนะนำและข้อคิดเห็นต่างๆ ที่เป็นประโยชน์สำหรับการทำการวิจัยมาโดยตลอด จนกระทั่งวิทยานิพนธ์ฉบับนี้เสร็จสมบูรณ์

และขอขอบพระคุณธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ที่กรุณาให้ใช้อุปกรณ์ สถานที่ และระบบจัดการเครือข่ายแลนเป็นกรณีศึกษา

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูปภาพ

สารบัญรูปภาพ (ต่อ)

สารบัญรูปภาพ (ต่อ)

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันความต้องการในการใช้สารสนเทศที่มีมากขึ้นจากเดิมเมื่อต้องการใช้สารสนเทศ จะสามารถดำเนินการโดยทำการประมวลผลกับระบบคอมพิวเตอร์ที่มีอยู่ ณ.หน่วยงานหรือส่วนงานนั้นๆ เอง ซึ่งสารสนเทศที่ได้รับอาจจะไม่เพียงพอต่อความต้องการ จึงมีความจำเป็นที่ต้องทำการเชื่อมโยงระบบคอมพิวเตอร์ที่มีอยู่เข้าด้วยกัน เพื่อเพิ่มขีดความสามารถในการประมวลผลให้สามารถตอบสนองต่อความต้องการใช้งานสารสนเทศ

ระบบเครือข่ายคอมพิวเตอร์ระดับท้องถิ่นหรือที่เรียกว่าแลน (Local Area Network หรือ LAN) เป็นระบบเครือข่ายคอมพิวเตอร์ที่ทำการเชื่อมโยงระบบคอมพิวเตอร์ภายในองค์กรที่ทำงานลักษณะที่ไม่อยู่ในที่เดียวกัน โดยอาจจะอยู่ภายในอาคารสำนักงานเดียวกันหรือใกล้เคียงหรือภายในระยะทางที่ไม่ไกลมากเกินไป ให้สามารถทำการติดต่อสื่อสารถึงกันได้ทำการแลกเปลี่ยนข้อมูลระหว่างกันได้ด้วยความเร็วตั้งแต่ 10 เมกกะบิทต่อวินาที (MB/Second) ขึ้นไป เพื่อช่วยให้การประมวลผลสารสนเทศของหน่วยงานและองค์การต่างๆ มีสมรรถนะมากยิ่งขึ้น

การใช้งานแลนของธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ปัจจุบันเชื่อมต่อกันแสดงได้ดังรูปที่ 1.1.1 โดยมีงานที่ใช้อยู่บนแลนสรุปได้พอสังเขป ดังนี้

1.1.1 ระบบสอบถามข้อมูลลูกค้าเงินกู้ ลูกค้าเงินฝาก

1.1.2 ระบบอินเตอร์เนท (Internet) และระบบอินทราเนท (Intranet)

1.1.3 ระบบสารสนเทศ (Information System) อันได้แก่

- ระบบการจัดการสารสนเทศทางด้านการเงิน (Finance Management Information System (FMIS))
- ระบบการจัดการสารสนเทศทางด้านบุคคลาการ (Personal Information System (PIS))
- ระบบการจัดการสารสนเทศทางด้านทั่วๆ ไป (General Information System (GIS))

1.1.4 ระบบการเรียกพิมพ์รายงานประจำวัน ประจำเดือน และประจำปี

1.1.5 ระบบการรายงานสรุปผลรายวัน รายเดือน และรายปี

1.1.6 ระบบการรายงานผลการกระทบยอดเงินฝากรายวัน

1.1.7 ระบบสำนักงานอัตโนมัติ (Office Automation :OA) ที่ใช้ภายในธนาคารในสำนักงานใหญ่ อันได้แก่ อีเมล (Email)

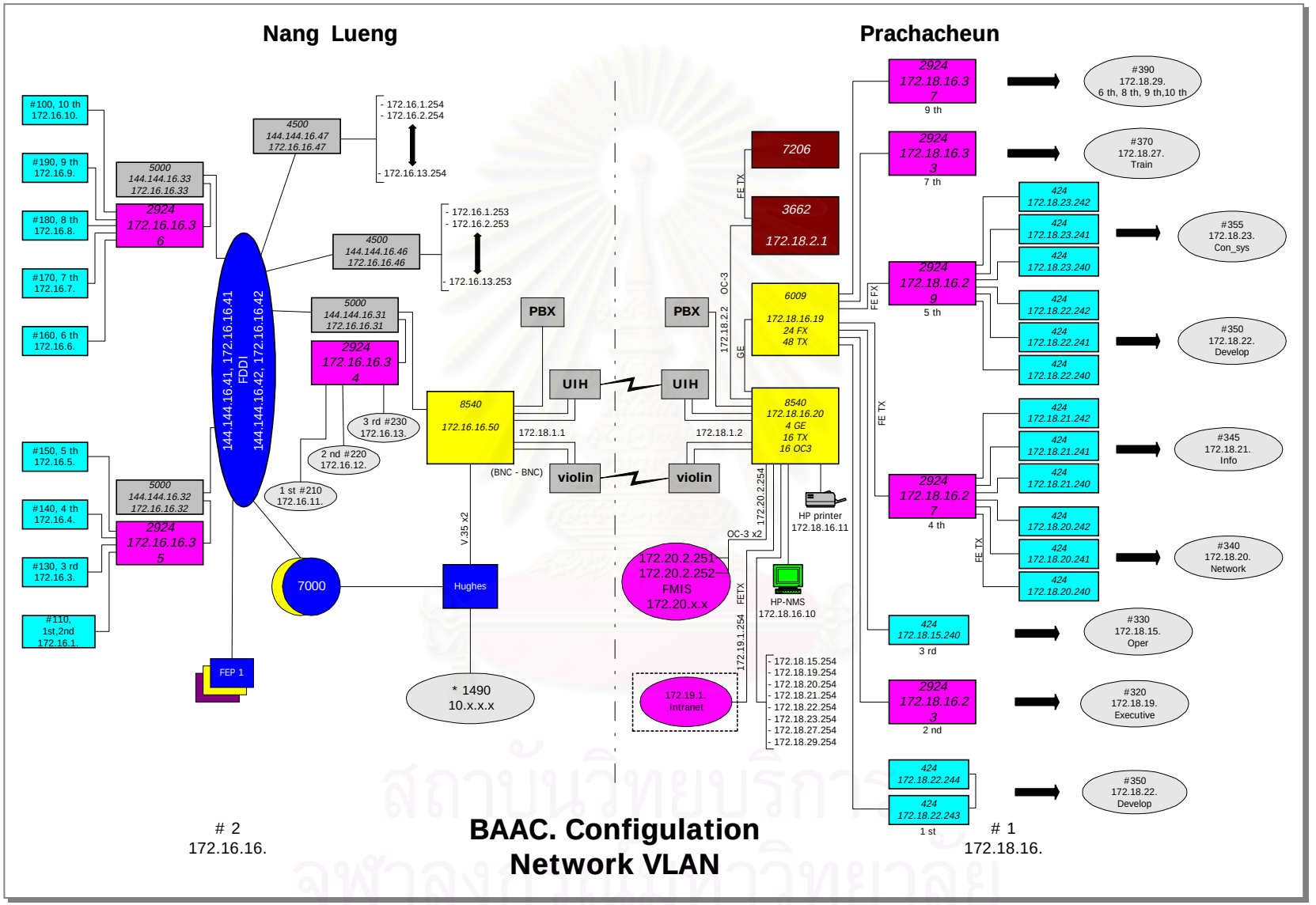
จากการใช้งานแลนของธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ซึ่งใช้เป็นกรณีศึกษาปรากฏว่าในกรณีที่มีปัญหาไม่ได้มีการรวบรวมข้อมูลเพื่อนำมาวิเคราะห์ ดังนี้

- วิธีการเฝ้าติดตามการทำงานของระบบ เพื่อให้ระบบแจ้งเหตุก่อนมีปัญหาเกิดขึ้น
- แนวคิดแนวทางปฏิบัติ เพื่อให้สามารถทราบถึงปัญหาที่เกิดขึ้น
- วิธีการในการแยกแยะปัญหา เพื่อระบุว่าปัญหาที่เกิดขึ้นเป็นปัญหาทางด้านใดอย่างชัดเจน
- วิธีการกำหนดแบบแผนและขั้นตอนในการแก้ไขปัญหาที่เกิดขึ้นในระบบ
- วิธีการและแบบแผนในการควบคุมการใช้งานโปรแกรมจัดการเครือข่าย

ดังนั้นถ้าองค์กรมีการออกแบบวิธีการเฝ้าติดตามการทำงานของระบบและวิธีการที่ดีในการวางแนวทางในการแก้ไขปัญหาที่เกิดขึ้น จะช่วยให้สามารถแก้ไขปัญหาที่เกิดขึ้นได้อย่างทันท่วงที

บางครั้งเมื่อเกิดปัญหาเกี่ยวกับแลนนักบริหารระบบไม่สามารถทำการวิเคราะห์ข้อผิดพลาดที่เกิดขึ้นได้อย่างรวดเร็ว หรือไม่สามารถแก้ปัญหาได้อย่างถูกต้องและรวดเร็ว เนื่องจากระบบแลนประกอบด้วยอุปกรณ์ต่างๆ หลายส่วน ดังนั้นการออกแบบวิธีการเฝ้าติดตามและวิธีการแก้ไขปัญหาการทำงานแลน ทำให้สามารถทราบถึงปัญหาหรือแนวโน้มของปัญหาที่ใกล้เคียงที่สุด ตลอดจนแนวทางการแก้ไขปัญหาที่เกิดขึ้นได้อย่างเป็นมาตรฐานเดียวกัน

ระบบปฏิบัติการ CISCO Works2000 เป็นระบบปฏิบัติการที่ทำหน้าที่ในการวิเคราะห์ควบคุม ตรวจสอบและแยกแยะปัญหาของระบบแลนได้ โดยระบบปฏิบัติการดังกล่าวถูกพัฒนามาในเชิงการค้าในส่วนของการนำไปใช้งาน นักบริหารระบบจำเป็นต้องทราบวิธีการนำไปประยุกต์ใช้ให้เกิดประโยชน์สูงสุดกับองค์การโดยการออกแบบวิธีการเฝ้าติดตามและวิธีการแก้ไขปัญหาที่เกิดขึ้น เพื่อนำไปปฏิบัติและรายงานผลต่อไป



รูปที่1.1.1 แสดงระบบเครือข่ายระดับท้องถิ่นของธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร

1.2 วัตถุประสงค์ในการดำเนินการวิจัย

วัตถุประสงค์ในการดำเนินการวิจัย

1.2.1 เพื่อออกแบบวิธีการและขั้นตอนการดำเนินงานในการตรวจวัดข้อผิดพลาดของระบบเครือข่าย

1.2.2 เพื่อเป็นแนวทางในการแก้ไขปัญหาของอุปกรณ์และเครือข่ายสื่อสาร

1.2.3 เพื่อเป็นแนวทางในการสร้างระบบสำหรับวางแผนการดูแลและบำรุงรักษาเครือข่าย

1.3 ขอบเขตของการวิจัย

ขอบเขตของการวิจัย ประกอบด้วยขอบเขต ดังนี้

1.3.1 ศึกษาและใช้ระบบเครือข่ายระดับท้องถิ่นของธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร เป็นระบบทดสอบดังรูปที่ 1.1.1

1.3.2 การเก็บรวบรวมข้อมูลการทำงานของระบบเครือข่ายคอมพิวเตอร์ระดับท้องถิ่นจะใช้โปรแกรมจัดการเครือข่ายดังนี้

1.3.2.1) โปรแกรม CISCO Works2000 ที่ทำงานอยู่บนเครื่องคอมพิวเตอร์ ยี่ห้อ SUN รุ่น SUN Ultra10

1.3.3 ผลลัพธ์ของการวิจัย ประกอบด้วย

1.3.3.1) ขั้นตอนในการแก้ไขปัญหาของแต่ละอุปกรณ์ และรายละเอียดของรายการอะไหล่สำรองที่จำเป็นต้องใช้ในการแก้ไขปัญหาที่เกิดขึ้น

1.3.3.2) แบบฟอร์มสำหรับใช้งานในการเฝ้าติดตามและแก้ไขปัญหา

1.3.3.3) รายงานสรุปผลการเฝ้าติดตามและรายงานสรุปผลการแก้ไขปัญหา

1.3.4 ขอบเขตของการวิจัยจะไม่รวมถึงข้อผิดพลาดที่เกิดขึ้นจากการทำงานของโปรแกรมใช้งาน (Applications) จะคลอบคลุมเฉพาะการทำงานของระบบโดยรวม

1.4 ขั้นตอนและวิธีการดำเนินการวิจัย

ขั้นตอนและวิธีการดำเนินการวิจัย

1.4.1 ศึกษาระบบจัดการเครือข่าย CiscoWorks2000 ที่เกี่ยวกับการเฝ้าติดตาม และแก้ไขปัญหาการทำงานของระบบแลน

1.4.2 ศึกษาวิเคราะห์ และเก็บรวบรวมข้อมูลการทำงานของระบบเครือข่าย ของกรณีศึกษา

1.4.3 ออกแบบขั้นตอนการใช้งานโมดูลต่าง ๆ และพัฒนาโปรแกรมในการนำข้อมูลมาใช้ในการเฝ้าติดตาม และแก้ไขปัญหาระบบแลน

1.4.4 จัดทำรายงานและข้อเสนอแนะ

1.4.5 จัดทำเอกสารสรุปผลการวิจัยและข้อเสนอแนะ

1.5 ประโยชน์ที่คาดว่าจะได้รับในการดำเนินการวิจัย

ประโยชน์ที่คาดว่าจะได้รับในการดำเนินการวิจัย ดังนี้

1.5.1 เป็นแนวทางในการวางแผนแก้ไขปัญหาการดำเนินงานแลนที่ใช้เป็นกรณีศึกษา และระบบอื่นๆ ที่มีลักษณะการดำเนินการที่คล้ายคลึงกัน

1.5.2 เป็นแนวทางในการวางแผนขยายการดำเนินงานและการให้บริการต่างๆ เพิ่มเติมบนแลนที่ใช้เป็นกรณีศึกษา

บทที่ 2

แนวความคิดและทฤษฎีที่เกี่ยวข้อง

2.1 นิยามและคำจำกัดความ

แนวความคิดและทฤษฎีที่เกี่ยวข้องกับหัวข้อการวิจัย ประกอบด้วย

2.1.1 การบริหารระบบเครือข่าย (Network Management)

2.1.2 การควบคุมการดำเนินงานของระบบ (Network Operational Control)

2.1.3 การบริหารระบบ (Network Administraion)

2.1.4 การวิเคราะห์การดำเนินงานของระบบ (Network Analysis and Tuning)

2.1.5 การพิจารณาความสามารถรับการเพิ่มภาระงานของระบบ (Network Capacity Planning)

2.1.1 การบริหารระบบเครือข่าย (Network Management)

การบริหารระบบเครือข่าย (Network Management) ถือได้ว่าเป็นผลรวมมาจากการดำเนินการตามกิจกรรมต่าง ๆ ที่เกี่ยวข้องซึ่งกันและกันได้แก่ การวางแผนกำหนดขั้นตอนการปฏิบัติการ ติดตั้งอุปกรณ์รวมทั้งรูปแบบการเชื่อมต่อ การติดตามควบคุมการดำเนินการของระบบตลอดจนการหาแนวทางป้องกันข้อผิดพลาดที่อาจเกิดขึ้นต่อระบบรวมถึงการแก้ไขปัญหาที่เกิดขึ้นในระบบ

Open Systems Interconnection Model (OSI) Management Functional Areas ได้กำหนดหน้าที่ในการบริหารระบบเครือข่ายคอมพิวเตอร์ไว้ 5 ประการ ดังนี้ (Allan, Karen,1996)

2.1.1.1 การแก้ไขข้อผิดพลาด (Fault Management)

เกี่ยวข้องกับการตรวจหา และรายงานข้อผิดพลาดที่เกิดขึ้น รวมถึงการทำการวินิจฉัย

สาเหตุของปัญหา การแก้ไขปัญหาต่าง ๆ ซึ่งสามารถกระทำได้ 3 ขั้นตอนด้วยกันคือ

- การระบุสิ่งที่เกิดขึ้นของข้อผิดพลาดบนเครือข่ายข้อมูล (Discover the problem)
- การแยกสาเหตุของข้อผิดพลาด (Isolation the problem)
- การจัดการกับข้อผิดพลาด (Fix the problem)

2.1.1.2 **การบันทึกและติดตามการใช้งานระบบ** (Accounting Management)

เป็นการจัดสรรการใช้ทรัพยากรของระบบ ควบคุมดูแลการใช้ทรัพยากรต่าง ๆ ของระบบตลอดจนการกำหนดขอบเขตการใช้งาน รวมถึงการจัดทำบัญชีรายชื่อของผู้ใช้ ซึ่งรวมไปถึงการจัดการทางด้านการใช้ทรัพยากรของแต่ละระบบ (Account) ว่ามีเปอร์เซนต์เท่าไร มีจำนวนผู้ใช้มากน้อยเพียงใดมี 3 ขั้นตอนประกอบด้วย

- รวบรวมข้อมูล เกี่ยวกับการ Utilization ของ Network resources
- ตั้งค่าโควต้าการใช้งานของระบบ
- แจ้งการใช้งานเครือข่ายของแต่ละ User

2.1.1.3 **การจัดการพื้นฐานเบื้องต้นในระบบ** (Configuration Management)

กำหนดการเชื่อมต่ออุปกรณ์ต่าง ๆ ในระบบทั้งในด้านกายภาพ และตรรกะการควบคุมของอุปกรณ์ต่างๆ รวมทั้งสถานะของอุปกรณ์และโปรแกรมประยุกต์ต่าง ๆ ที่นำมาใช้งานในระบบให้ถูกต้องและปรับปรุงรายการให้ถูกต้องสอดคล้องกับระยะเวลาดำเนินงาน มีหลัก 3 ประการ ประกอบด้วย

- รวบรวมข้อมูล เกี่ยวกับสภาพแวดล้อมของเน็ตเวิร์กปัจจุบัน
- ใช้ข้อมูลเพื่อปรับปรุงแก้ไข Configuration ของอุปกรณ์ และการต่อเชื่อม และตรวจสอบการเปลี่ยนแปลงของอุปกรณ์
- เก็บข้อมูล ให้มีข้อมูลที่ทันสมัยอยู่เสมอ เพื่อนำมาผลิตรายงานที่หลากหลาย

2.1.1.4 **การจัดการให้ระบบดำเนินงานได้อย่างมีสมรรถนะ** (Performance Management)

ในการที่จะทำให้ระบบสามารถทำงานได้อย่างมีสมรรถนะ หากไม่สามารถที่จะทำการวัดการทำงานของระบบเพื่อประเมินพฤติกรรมการทำงานแล้ว จะทำให้ไม่สามารถบริหารการทำงานของระบบนั้น ๆ ได้ มี 4 ขั้นตอนต่อไปนี้

- รวบรวมข้อมูลของการ Utilization ของอุปกรณ์เครือข่าย และลิงค์
- วิเคราะห์ข้อมูลที่มีความสัมพันธ์กัน
- ตั้งค่า Utilization Thresholds

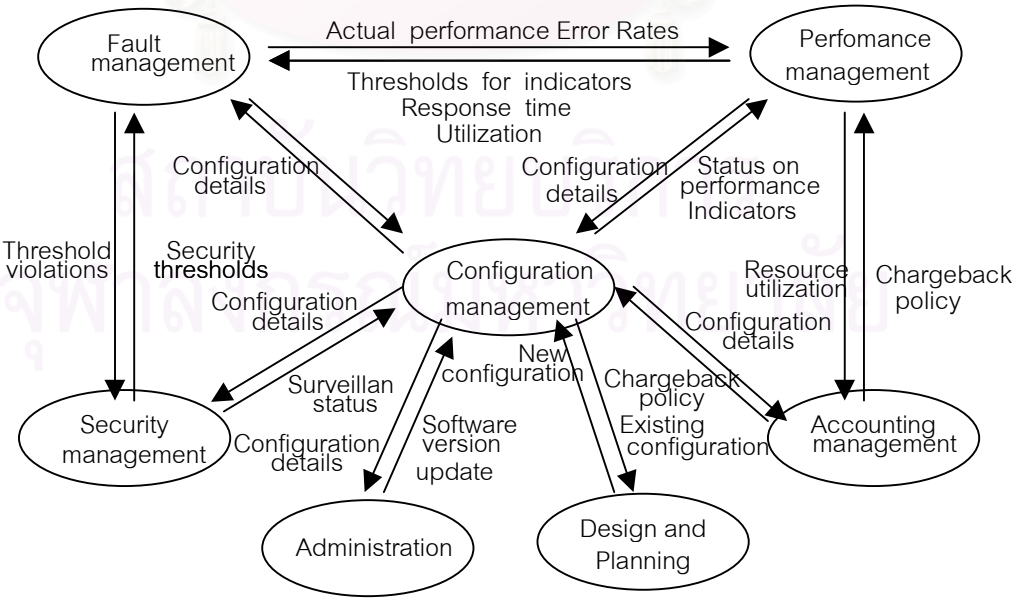
- Simulate เครือข่าย

2.1.1.5 **การจัดการความปลอดภัยในระบบ (Security Management)**

การกำหนดมาตรการรักษาความปลอดภัยในระบบก็เหมือนการจัดให้มีการป้องกันภัยให้แก่ระบบขึ้น ซึ่งอาจจะไม่มีการตระหนักถึงความสำคัญของการจัดให้มีระบบรักษาความปลอดภัยขึ้นจนกว่า จะเกิดปัญหาขึ้นในระบบ ตัวอย่างในการกำหนดมาตรการรักษาความปลอดภัยในระบบได้แก่ การกำหนดให้มีการตรวจสอบการมีสิทธิในการใช้งานอุปกรณ์และบริการต่าง ๆ ที่มีอยู่ในระบบให้เป็นไปอย่างถูกต้องเหมาะสมและเกิดความปลอดภัยต่อการทำงานของระบบและผู้ใช้ มี 4 ขั้นตอนดังต่อไปนี้

- กำหนดข้อมูลที่สำคัญ ที่น่าจะมีความเสี่ยง
- หาจุดที่สามารถเข้าถึงข้อมูลนั้นได้
- กำหนดความปลอดภัยของการเข้าถึงข้อมูล ณ จุดดังกล่าว
- ดูแลบำรุงรักษา การกำหนดความปลอดภัย

หน้าที่ทั้ง 5 ประการดังกล่าวข้างต้นมีความเกี่ยวข้องกันซึ่งกันและกันดังรูปที่ 2.1.1 (Terplan, 1996)



รูปที่ 2.1.1 แสดงถึงความสัมพันธ์ระหว่างหน้าที่ 5 ประการในการบริหารระบบ

ปัจจัยที่มีผลกระทบต่อความสำเร็จในการบริหารระบบเครือข่ายคอมพิวเตอร์ที่สำคัญมีอยู่ด้วยกัน 3 ประการด้วยกัน (Terplan, 1996) คือ

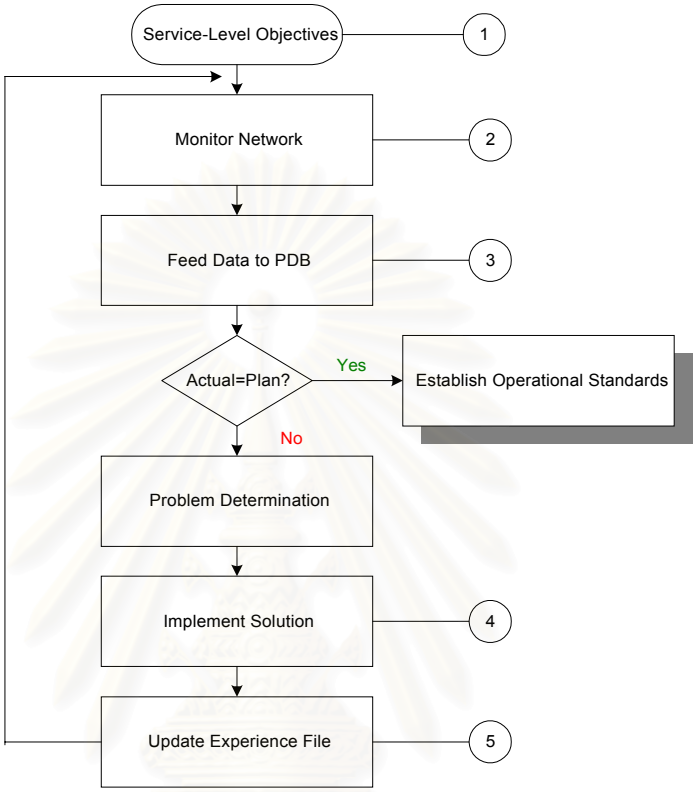
- กระบวนการหรือขั้นตอนวิธีในการดำเนินการแก้ไขปัญหา (Methods หรือ Procedures) ซึ่งจะขึ้นอยู่กับระบบเครือข่ายและโครงสร้างนั้น ๆ ทั้งนี้รวมถึงโปรแกรมจัดการเครือข่ายที่นำมาใช้งานเพื่อบรรลุถึงหลักการหรือรูปแบบที่ต้องดำเนินการในการบริหารระบบที่เรียกว่า Open Systems Interconnection Model (OSI) Management Functional Areas
- อุปกรณ์หรือเครื่องมือ (Instruments หรือ Tools) ที่นำมาใช้ในการควบคุม ติดตามและทดสอบการทำงานของอุปกรณ์ต่าง ๆ รวมถึงการทำงานของระบบโดยรวม
- บุคลากร (Human Resources) ที่รับผิดชอบในการควบคุม ดูแล และแก้ไขปัญหาของระบบซึ่งจะต้องเป็นผู้ที่มีความรู้และประสบการณ์

กล่าวได้ว่าในการควบคุมดูแลให้ระบบแลนดำเนินไปได้อย่างมีสมรรถนะนั้น มีกิจกรรมหลัก ๆ ที่ต้องดำเนินการควบคู่กันไป ได้แก่ (Terplan, 1987)

2.1.2 <u>การควบคุมการดำเนินงานของระบบ</u> (Network Operational Control)

ประกอบด้วยกิจกรรมต่าง ๆ ที่ต้องดำเนินการเพื่อให้ระบบสามารถดำเนินงานได้อย่างต่อเนื่อง โดยสามารถตระหนักถึงปัญหาที่เกิดขึ้น หรือที่กำลังจะเกิดทั้งในด้านการทำงานของอุปกรณ์และสมรรถนะการดำเนินงานของระบบได้อย่างรวดเร็ว ทันต่อเหตุการณ์

แบบแผนขั้นตอนการดำเนินการควบคุมการดำเนินงานของระบบสามารถแสดงได้ดังรูปที่ 2.1.2



รูปที่ 2.1.2 แสดงถึงแบบแผนขั้นตอนการควบคุมการทำงานของระบบ

2.1.3 <u>การบริหารระบบ</u> (Network Administration)

เป็นกิจกรรมทั้งในระยะสั้น และระยะยาว ซึ่งเกี่ยวข้องกับการติดตามการทำงานของระบบการแก้ไขเปลี่ยนแปลงระบบ การรักษาความปลอดภัยระบบ การควบคุมจำนวนอุปกรณ์ที่มีอยู่ในระบบแบบแผนขั้นตอนการบริหารระบบ (Network Administration Methodology) สามารถแสดงได้ดังรูปที่ 2.1.3

2.1.4 **<u>การวิเคราะห์การดำเนินงานของระบบ</u>** (Network Analysis and Tuning)

เป็นการวิเคราะห์การดำเนินงานของระบบที่ดำเนินอยู่ว่ามีผลการดำเนินงานเป็นอย่างไร จำเป็นต้องปรับปรุงแก้ไขการดำเนินงาน ณ ส่วนใดของระบบหรือไม่ เป็นการสืบหาข้อมูลในเชิงปริมาณ โดยมีเทคนิควิธีในการตรวจวัด และทดสอบอยู่ 3 วิธี คือ (Fortier, 1992)

2.1.4.1 แอนนาลิติคคอล โมเดลลิ่ง (Analytical Modeling)

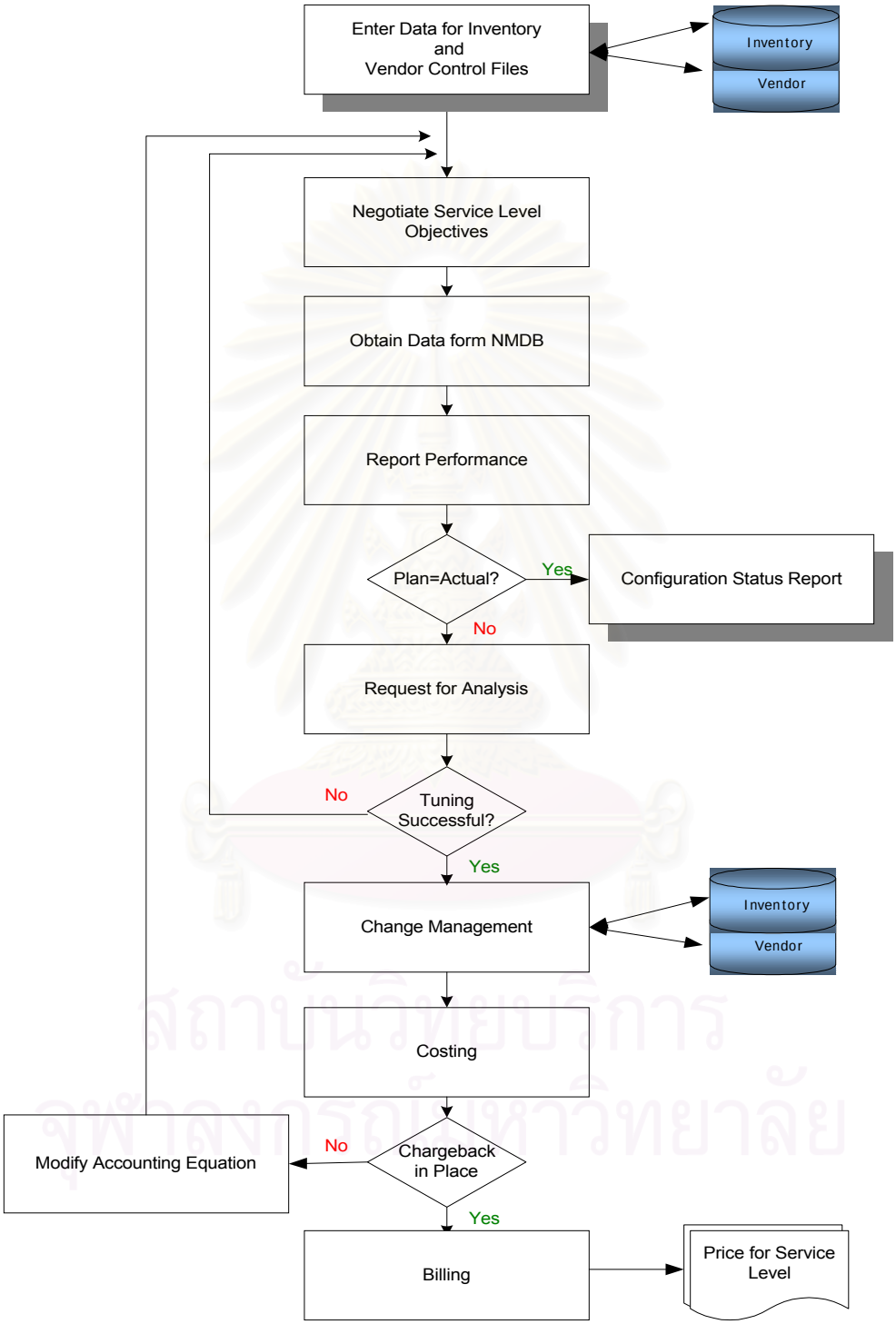
2.1.4.2 ซิมูเลชั่น โมเดลลิ่ง (Simulation Modeling)

2.1.4.3 เอ็มพีริคัล โมเดลลิ่ง (Empirical Modeling)

2.1.4.1 แอนนาลิติค โมเดลลิ่ง (Analytic Modeling)

ใช้เทคนิคที่นิยมใช้ในการออกแบบระบบเครือข่ายคอมพิวเตอร์ที่เรียกว่า ตัวแบบแถวคอย (Queueing Models) ซึ่งตัวแบบดังกล่าวจะมีการเก็บรวบรวมข้อมูลที่จะนำมาวิเคราะห์การดำเนินงานของระบบอย่างละเอียด โดยปกติแล้ว เทคนิคตัวแบบแถวคอย จะสามารถแสดงให้ทราบถึงสมรรถนะการดำเนินงานของระบบในประเด็นต่าง ๆ ดังนี้

- ค่าเฉลี่ยความยาวแถวคอย
- ค่าเฉลี่ยเวลาที่คอยอยู่ในแถวคอย
- ค่าสถิติการใช้งานระบบ
- ค่าเฉลี่ยเวลาตอบสนอง



รูปที่ 2.1.3 แสดงถึงแบบแผนขั้นตอนการบริหารระบบ

2.1.4.2 **ซิมูเลชั่น โมเดลลิ่ง** (Simulation Modeling)

เป็นเทคนิคที่ให้ผลการวิเคราะห์ที่สอดคล้องกับการดำเนินงานของระบบมากกว่าอนาลิติต โมเดลลิ่ง อย่างไรก็ตามเทคนิคดังกล่าวก็มีข้อจำกัดตรงที่ว่า ผลของการจำลองการดำเนินงานของระบบอาจจะไม่สามารถแสดงถึงสภาวะที่เกิดขึ้นจากการดำเนินงานจริงของระบบก็ได้

2.1.4.3 **เอ็มพีริคัล โมเดลลิ่ง** (Empirical Modeling)

เป็นวิธีการที่สามารถแสดงสมรรถนะการทำงานของระบบได้ดีที่สุด เนื่องจากว่าทำการประเมินการทำงานของระบบจากอุปกรณ์ที่กำลังดำเนินงานอยู่จริง ซึ่งการวิเคราะห์และประเมินการทำงานสามารถดำเนินการได้ทั้งแบบพลวัตน์ และแบบสถิตย์

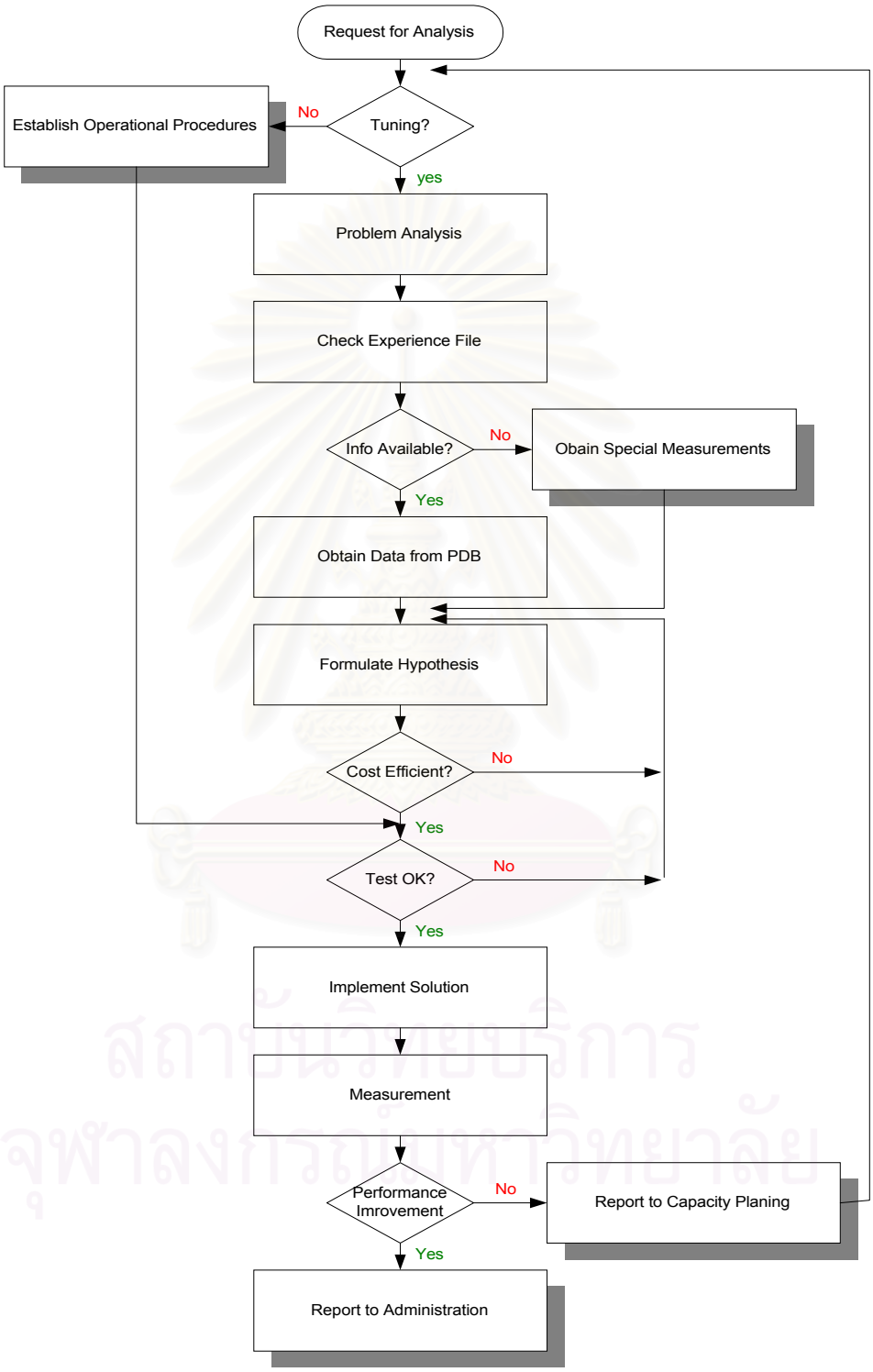
- การประเมินแบบพลวัตน์

  ดำเนินการโดยมีการพิจารณากำหนดค่าพารามิเตอร์ที่สนใจไว้ล่วงหน้าสำหรับกรณีศึกษาที่สนใจ เพื่อที่จะลดผลกระทบของจำนวนประเภทและปริมาณของข้อมูลที่ต้องจัดเก็บ วิธีการดังกล่าวจะมีประโยชน์อย่างมากในการติดตามสมรรถนะการทำงานของระบบในระหว่างดำเนินการ เพื่อให้ทราบถึงผลกระทบของภาระงานที่มีต่อระบบของระบบ

- การประเมินแบบสถิตย์

  จะมีประโยชน์อย่างมากต่อการประเมินสมรรถนะของระบบทั้งในปัจจุบันและอนาคต โดยจะดำเนินการควบคุมภาระงานของระบบและจะทำการเก็บรวบรวมข้อมูล เพื่อประเมินประสิทธิภาพของการดำเนินงาน

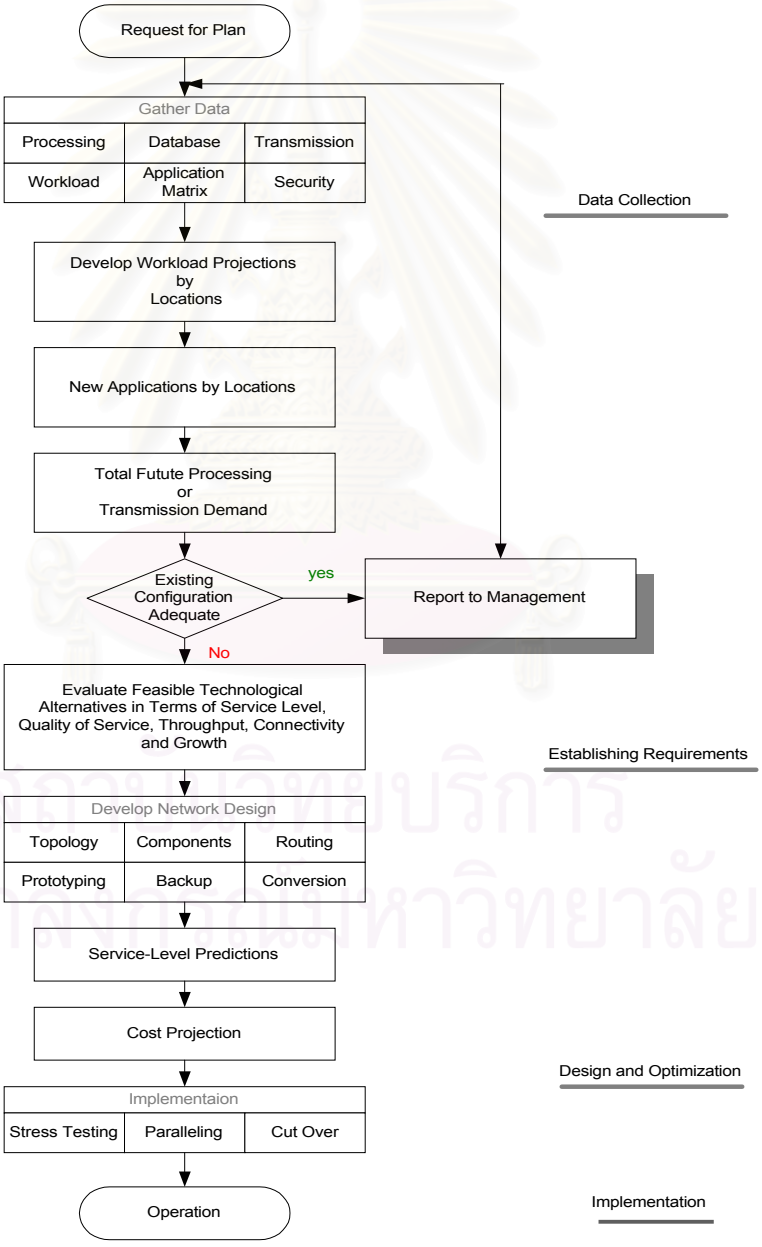
แบบแผนขั้นตอนวิเคราะห์และปรับปรุงสมรรถนะ (Network Performance Analysis Methodology) แสดงได้ดังรูปที่ 2.1.4



รูปที่ 2.1.4 แสดงแบบแผนขั้นตอนการประเมินการดำเนินงานของระบบ

2.1.5 การพิจารณาความสามารถรับการเพิ่มภาระงานของระบบ (Network Capacity Planning)

เป็นกระบวนการในการพิจารณาว่าระบบเครือข่ายคอมพิวเตอร์ที่มีอยู่มีความสามารถรับการเพิ่มภาระงานได้ปริมาณเท่าใด การพิจารณาจะขึ้นอยู่กับข้อมูลที่ได้มาจากการวิเคราะห์การดำเนินงานของระบบ แบบแผนขั้นตอนการพิจารณาความสามารถรับการเพิ่มภาระงานของระบบ (Network Capacity Planning) แสดงได้ดังรูปที่ 2.1.5



รูปที่ 2.1.5 แสดงถึงแบบแผนขั้นตอนการพิจารณาความสามารถรับการเพิ่มภาระงานของระบบ

2.2 องค์ประกอบในการบริหารระบบเครือข่าย

องค์ประกอบสำคัญในการบริหารระบบเครือข่ายคอมพิวเตอร์ มีดังนี้ (Stalling, 1994)

2.2.1 สถานีที่ทำหน้าที่ในการจัดการและแก้ไขปัญหา (Management Station)

โดยทั่วไปแล้วจะเป็นเครื่องคอมพิวเตอร์ที่แยกอิสระจากระบบโดยจะทำหน้าที่ในการเฝ้าติดตามการทำงานของระบบ และเมื่อเกิดข้อผิดพลาดขึ้นก็สามารถดำเนินการแก้ไขปัญหาจากระบบคอมพิวเตอร์ดังกล่าวได้ เปรียบเสมือนเป็นสิ่งที่ทำให้มีการเชื่อมต่อระหว่างผู้บริหารระบบกับระบบการ จัดการเครือข่าย

2.2.2 โปรแกรมที่ทำหน้าที่ติดตามการทำงานของอุปกรณ์แต่ละอุปกรณ์ (Management Agent)

เป็นโปรแกรมที่ติดตั้งลงในอุปกรณ์ที่ทำหน้าที่สำคัญในการรับ-ส่งข้อมูล เช่น เราเตอร์ คอนเซ็นเตรเตอร์ ฮับ เป็นต้น โดยโปรแกรมดังกล่าวจะทำหน้าที่ติดตามการทำงานของอุปกรณ์ว่ามีสถานะการทำงานเป็นอย่างไร โดยจะทำการติดต่อสื่อสารกับโปรแกรมเมเนเจอร์ที่คอยควบคุมและสั่งการที่ทำงานอยู่บนสถานีบริหารระบบอีกชั้นหนึ่ง

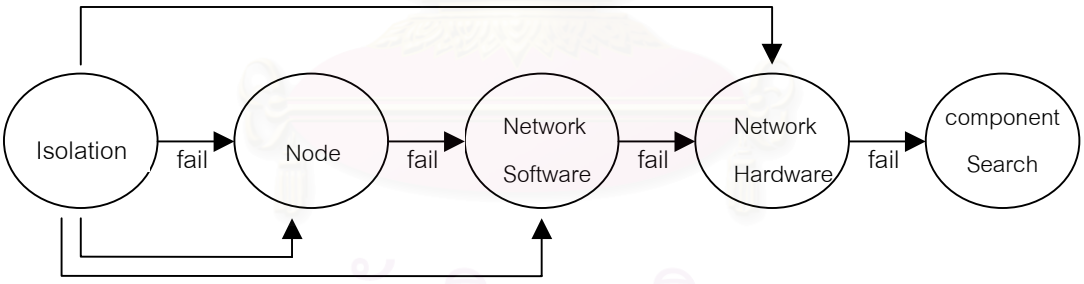
2.2.3 ฐานข้อมูลที่ใช้ในการแก้ไขปัญหาและอุปสรรคในการทำงานของระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์

ในการบริหารระบบเครือข่ายคอมพิวเตอร์เพื่อที่จะทำการแก้ไขปัญหาต่าง ๆ นั้น จะดำเนินการโดยการกำหนดองค์ประกอบต่างๆ ของระบบและอุปกรณ์ออกมาเป็นวัตถุ (Object) โดยแต่ละวัตถุจะมีคุณสมบัติต่าง ๆ ซึ่งจะกำหนดค่าของคุณสมบัตินั้นๆ ออกมาในรูปของค่าตัวแปรต่าง ๆ (Data Variables) และจะทำการเก็บไว้ในฐานข้อมูลของวัตถุนั้น ๆ เองเรียกว่า แมนเนจเม้นท์ อินฟอร์เมชั่น เบส (Management Information Base หรือ MIB ซึ่งจะถือว่า มิบ (MIB) ของแต่ละวัตถุเป็นศูนย์รวมของการให้บริการและดำเนินกิจกรรมของการดำเนินงานของโปรแกรมเอเยนต์ ที่ทำงานอยู่บนวัตถุนั้น ๆ เมื่อสถานีที่ทำหน้าที่เป็นศูนย์กลางในการบริหารและแก้ไขปัญหาร้องขอมา

2.2.4 **เน็ทเวอร์ค แมนเนจเม้นท์ โปรโตคอล** (Network Management Protocol)

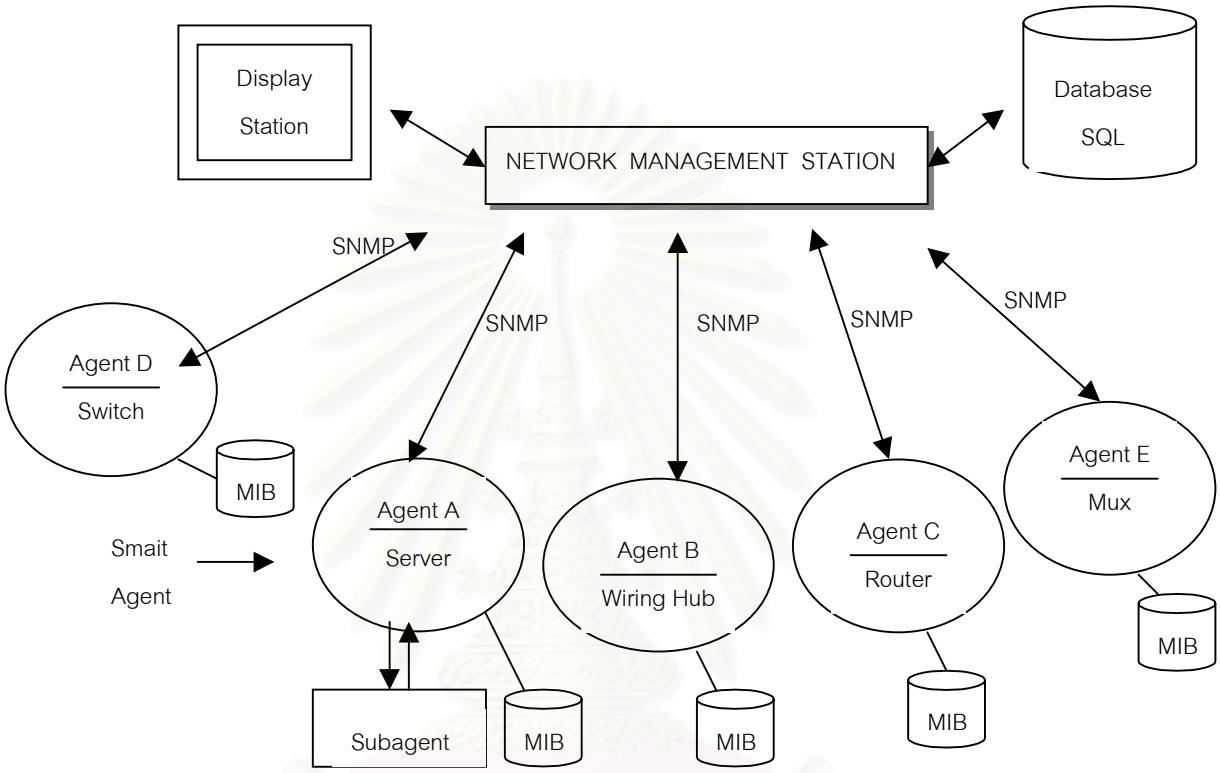
ในการติดตามการทำงานและแก้ไขปัญหาของอุปกรณ์ต่าง ๆ ที่นำมาต่อเชื่อมเข้ามาในระบบเครือข่ายคอมพิวเตอร์ที่ใช้ ทีซีพี/ไอพี โปรโตคอล เป็นข้อกำหนดในการติดต่อสื่อสารนั้น จะมีการใช้โปรโตคอลที่ใช้ในการบริหารระบบฯ ได้แก่ ซิมเปิล เน็ทเวอร์ค แมนเนจเม้นท์ โปรโตคอล (Simple Network Management Protocol หรือ SNMP มาทำการติดตามการทำงานของอุปกรณ์ต่าง ๆ ตลอดจนการแก้ไขปรับปรุงการทำงาน สำหรับในส่วนของรายละเอียดของข้อกำหนดของเอสเอ็นเอ็มพี (SNMP) นั้น ได้ทำการกำหนดเกี่ยวกับโครงสร้างของข้อมูลที่ต้องการจัดเก็บสำหรับ Object ต่าง ๆ ในระบบ รูปแบบไวยากรณ์ต่าง ๆ ที่ใช้ในการจัดเก็บข้อมูล การจำแนกหมวดหมู่ของ Object ต่าง ๆ ซึ่งจะไม่ขอกล่าวในรายละเอียด ณ ที่นี้

สำหรับแนวทางในการแก้ไขปัญหาที่เกิดขึ้นในระบบแลน สามารถกำหนดลำดับการดำเนินการในการพิจารณาหาสาเหตุของปัญหาได้ดังรูปที่ 2.2.1) (Fortier, 1992)



รูปที่ 2.2.1 แสดงลำดับในการพิจารณาการแก้ไขปัญหาที่เกิดขึ้นในระบบเครือข่ายคอมพิวเตอร์

จากที่กล่าวมาข้างต้นสามารถแสดงถึงสถาปัตยกรรมในการบริหาร และบทบาทของ SNMP ได้ดังรูปที่ 2.2.2



รูปที่ 2.2.2 แสดงถึงโครงสร้างในการนำ SNMP มาใช้ในการบริหารระบบเครือข่ายคอมพิวเตอร์

2.3 องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

ระบบเครือข่ายคอมพิวเตอร์ มีองค์ประกอบหลายส่วนด้วยกัน หากจำแนกองค์ประกอบที่สำคัญของระบบแล้ว สามารถจำแนกออกเป็น 2 ส่วนที่สำคัญ ได้แก่

2.3.1 ส่วนประกอบของระบบ (Components)

ได้แก่ อุปกรณ์ต่าง ๆ ที่ต่อเชื่อมอยู่ในระบบเครือข่ายคอมพิวเตอร์ เช่น เราเตอร์ (Rounter) ฮับ (Hub) สวิทช์ (Switch) แผ่นวงจรเชื่อมต่ออุปกรณ์เข้าสู่ระบบเครือข่าย รวมถึงโปรแกรมระบบปฏิบัติการเครื่องคอมพิวเตอร์ที่นำมาต่อเชื่อม โปรโตคอล (Protocol) ที่ใช้ในการสื่อสารข้อมูลในระบบเครือข่าย เป็นต้น

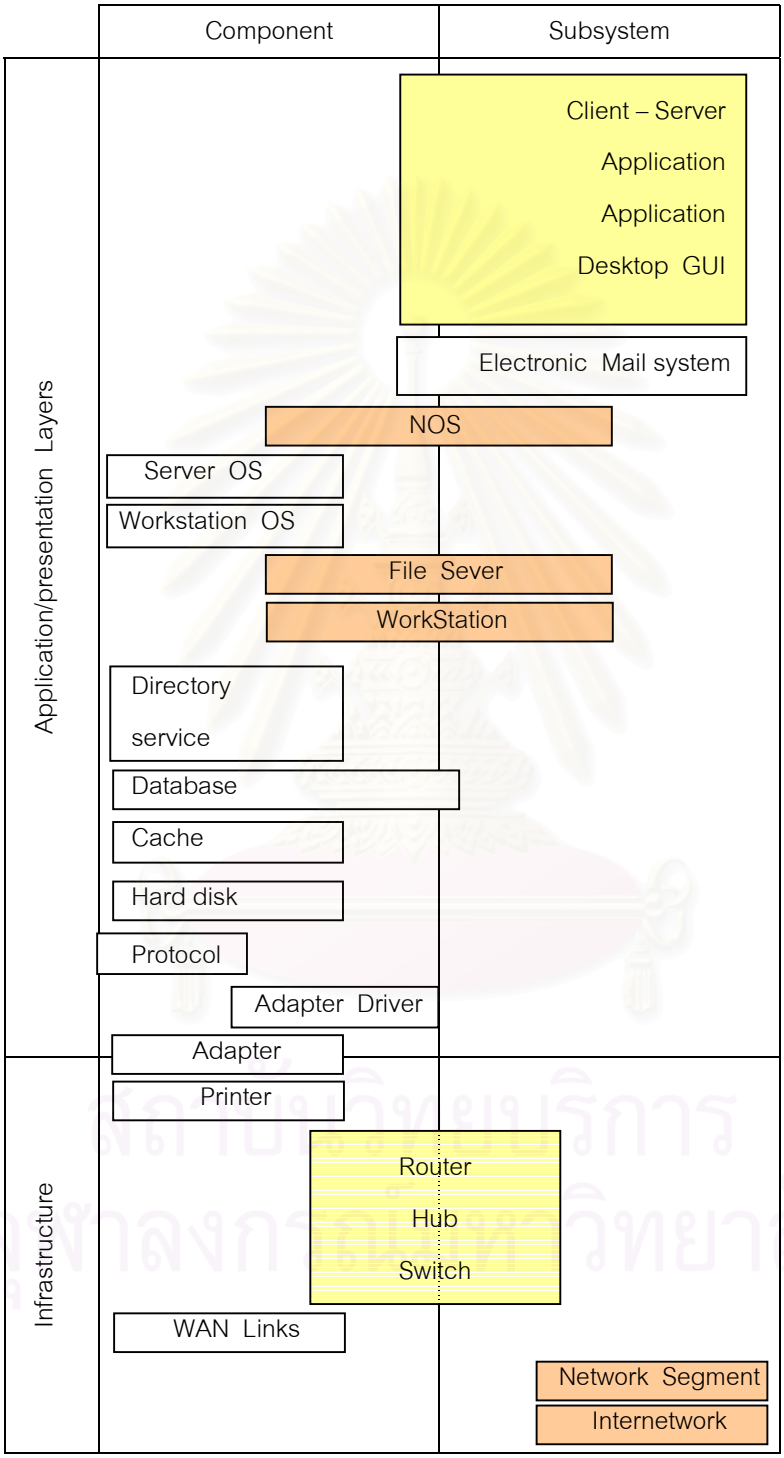
2.3.2 **ระบบย่อย** (Subsystems)

ได้แก่ ระบบการทำงานของอุปกรณ์ต่าง ๆ ที่สำคัญในระบบเครือข่ายคอมพิวเตอร์ที่สนใจศึกษา การเชื่อมต่ออุปกรณ์ต่าง ๆ ในการรับ-ส่งข้อมูลโดยพิจารณาตั้งแต่จุดเริ่มต้นจนถึงจุดสิ้นสุดของการรับ-ส่งข้อมูลในเส้นทางการรับ-ส่งข้อมูลที่สนใจศึกษา การทำงานของโปรแกรมประยุกต์ระบบต่าง ๆ ในรูปแบบผู้ให้บริการ และผู้รับบริการ

องค์ประกอบทั้ง 2 ประการดังกล่าวข้างต้น สามารถแสดงได้ดังรูปที่ 2.3

รูปที่ 2.3 แสดงองค์ประกอบของระบบเครือข่ายคอมพิวเตอร์ ซึ่งประกอบด้วยส่วนต่าง ๆ โดยที่การทำงานของส่วนประกอบเหล่านี้ จะมีผลต่อกันและกันและจะมีผลกระทบต่อแบบแผนการทำงานของระบบโดยรวม เนื่องจากระบบเครือข่ายคอมพิวเตอร์ประกอบด้วยองค์ประกอบต่าง ๆ อยู่หลายส่วนด้วยกัน ดังนั้นจุดที่อาจเกิดความล้มเหลวในการทำงานหรืออาจก่อให้เกิดข้อผิดพลาดในระบบ จะมีอยู่หลายจุดด้วยเช่นกัน และจะมีความสลับซับซ้อนมากยิ่งขึ้น

ในการศึกษา วิเคราะห์การทำงานของระบบเครือข่ายคอมพิวเตอร์ โดยดำเนินการทดสอบการทำงานของส่วนประกอบของระบบ และระบบย่อย ด้วยแบบแผนการทำงานในลักษณะต่าง ๆ ที่กำหนดขึ้น โดยอาศัยแบบแผนการทำงานที่เกิดขึ้นจริงเป็นบรรทัดฐานในการกำหนดรูปแบบ และเงื่อนไขของการทดสอบ วัตถุประสงค์ของการดำเนินการดังกล่าว ก็เพื่อให้ทราบถึงแบบแผนการทำงานในสภาวะการณ์ต่าง ๆ ของส่วนประกอบของระบบ และระบบย่อย ซึ่งอยู่ในภาวะการทำงานที่สอดคล้องและใกล้เคียงกับสภาวะการณ์ของการทำงานจริงที่ระบบดำเนินงานอยู่ โดยที่ผลของการทดสอบจะช่วยให้การวินิจฉัยปัญหาที่เกิดขึ้นในระบบระหว่างที่ทำงานจริงเป็นไปอย่างรวดเร็ว มีประสิทธิภาพและเป็นแนวทางในการพัฒนาระบบต่อไปในอนาคต



รูปที่ 2.3 แสดงถึงส่วนประกอบของระบบ และระบบย่อยของระบบเครือข่ายคอมพิวเตอร์

2.4 การวิเคราะห์การทำงานของระบบเครือข่ายคอมพิวเตอร์

การศึกษา วิเคราะห์การทำงานของระบบเครือข่ายคอมพิวเตอร์ เพื่อให้ทราบถึงแบบแผนการทำงานของส่วนประกอบของระบบ และระบบย่อยนั้น กล่าวได้ว่ามีองค์ประกอบอยู่ 3 ประการ ที่ จะต้องดำเนินการควบคู่กันไป เพื่อให้ได้ข้อสรุปและนำมาเป็นแนวทางในการวินิจฉัยถึงสาเหตุของข้อผิดพลาด และแก้ไขปัญหาที่อาจเกิดขึ้นต่อไป องค์ประกอบ 3 ประการ ได้แก่ (Buchanan,1996 :23)

2.4.1 **การทดสอบเครือข่าย** (Network Testing)

การทดสอบการทำงานของระบบเครือข่ายคอมพิวเตอร์ จะช่วยให้ทราบถึงแบบแผนการทำงานของระบบ ประสิทธิภาพในการทำงาน แนวโน้มของปัญหาที่อาจเกิดขึ้นได้ในอนาคตตลอดจนปัญหาและอุปสรรคที่เกิดขึ้นจริงในระบบระหว่างการทดสอบ เพื่อกำหนดแนวทางแก้ไข

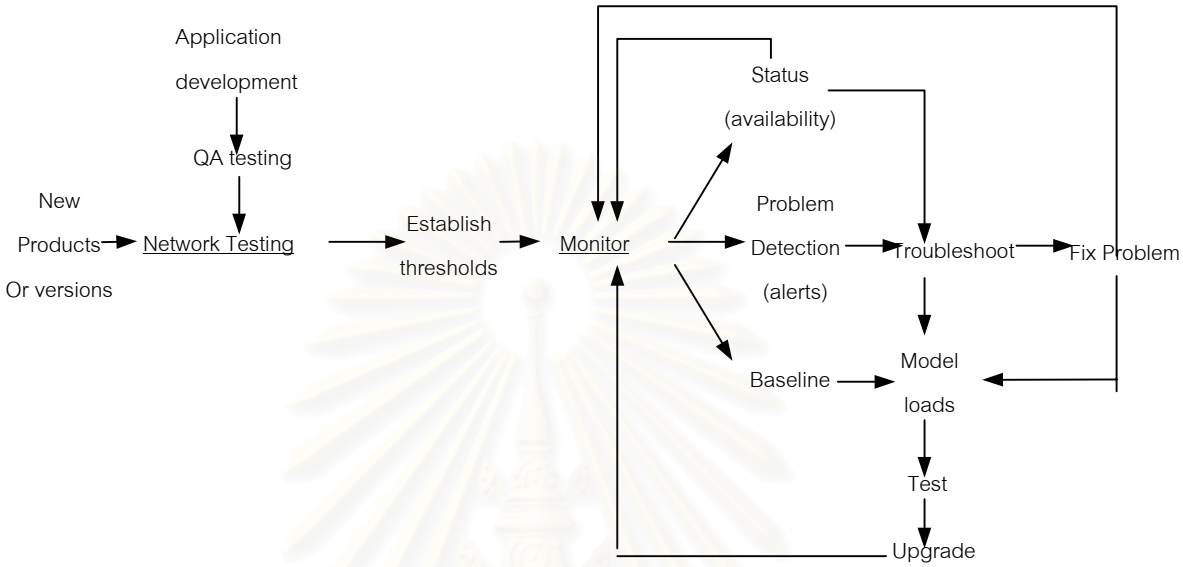
2.4.2 **การเฝ้าคุมการทำงานของระบบ** (Network Monitoring)

การเฝ้าคุมการทำงานของระบบเครือข่ายคอมพิวเตอร์ เป็นกระบวนการหนึ่ง ซึ่งจะต้องดำเนินการควบคู่ไปกับการทดสอบระบบ ในระหว่างการเฝ้าคุมการทำงานของส่วนประกอบของระบบ และระบบย่อยนั้น จะทำการบันทึกค่าพารามิเตอร์ที่สำคัญที่เกิดขึ้น และนำมาศึกษา วิเคราะห์ ให้ทราบถึงแบบแผนพฤติกรรมการทำงาน ตลอดจนปัญหาและอุปสรรคที่เกิดขึ้น หรืออาจจะเกิดขึ้นในระบบ

2.4.3 **การแก้ไขปัญหาเครือข่าย** (Network Troubleshooting)

เป็นกระบวนการในการแก้ไขปัญหาที่เกิดขึ้นจากการทำงานผิดพลาดของส่วนประกอบของระบบ และระบบย่อย และการแก้ไขปัญหาซึ่งเป็นผลมาจากการที่แบบแผนพฤติกรรมการทำงานของส่วนประกอบของระบบ และระบบย่อย แสดงถึงแนวโน้มที่จะเกิดข้อผิดพลาดขึ้นกับระบบและจะส่งผลกระทบต่อประสิทธิภาพการทำงานของระบบโดยรวม เมื่อพิจารณาแล้วเห็นว่ามีความจำเป็นที่จะต้องดำเนินการแก้ไขให้อยู่ในสภาวะที่ระบบสามารถดำเนินงานต่อไปได้

องค์ประกอบทั้ง 3 ประการ สามารถแสดงได้ดังรูปที่ 2.4



รูปที่ 2.4 แสดงองค์ประกอบ 3 ประการที่ช่วยให้การบริหารและการจัดการระบบเป็นไปอย่างมีประสิทธิภาพ

ในการศึกษาวิเคราะห์การทำงานของระบบเครือข่ายคอมพิวเตอร์ โดยทำการทดสอบการทำงานของส่วนประกอบของระบบ และระบบย่อย และดำเนินการเฝ้าคุมการทดสอบดังกล่าว จำเป็นจะต้องพิจารณาและศึกษาถึงรูปแบบสถาปัตยกรรมของระบบเครือข่ายคอมพิวเตอร์ ที่ได้ออกแบบและใช้งานอยู่จริง รวมถึงพิจารณาลักษณะการทำงานของระบบ การพิจารณาดังกล่าวจะช่วยให้ศึกษา วิเคราะห์การทำงานของระบบเป็นไปอย่างมีประสิทธิภาพ

2.5 ลักษณะการทำงานของระบบเครือข่ายคอมพิวเตอร์

ลักษณะการทำงานของระบบเครือข่ายคอมพิวเตอร์สามารถแบ่งออกได้เป็น 4 ประการที่ สำคัญ คือ

2.5.1 การจัดเก็บข้อมูล (Storage)

2.5.2 การเรียกใช้ข้อมูลและการบันทึกข้อมูล (I/O)

2.5.3 การส่งผ่านข้อมูล (Data Transmission)

2.5.4 การใช้งานลักษณะการคำนวณ (Computing)

2.6 วัฏจักรของระบบเครือข่ายคอมพิวเตอร์ (Life Cycle of Network)

วัฏจักรของระบบเครือข่ายคอมพิวเตอร์ สามารถแบ่งออกได้เป็น 5 ระยะด้วยกันคือ (Buchanan,1996 : 53-54)

2.6.1 ระยะที่ 1 การวางแผนและการออกแบบ (Planing and Design)

พิจารณาและออกแบบสถาปัตยกรรมระบบเครือข่ายคอมพิวเตอร์ให้สอดคล้องกับลักษณะงานที่ดำเนินการอยู่ เช่น รูปแบบการต่อเชื่อมอุปกรณ์ต่าง ๆ การพิจารณาคุณสมบัติของอุปกรณ์ต่าง ๆ ที่ต้องนำมาใช้ เป็นต้น

2.6.2 ระยะที่ 2 การพัฒนา (Development)

ภายหลังจากที่ได้ทำการติดตั้งอุปกรณ์ต่าง ๆ และติดตั้งโปรแกรมประยุกต์เพื่อใช้งานบนระบบแล้ว การดำเนินการทดสอบการทำงานของระบบ โดยพิจารณาถึงภาระงานของระบบ เวลาตอบสนอง ประสิทธิภาพการทำงาน และความเชื่อถือได้ของระบบ เป็นต้น เพื่อปรับปรุงการทำงานของระบบต่อไป

2.6.3 ระยะที่ 3 การกำหนดการใช้ระบบ (Deployment)

ได้แก่การเพิ่มจำนวนอุปกรณ์ จำนวนผู้ใช้ ระบบงานและโปแกรมประยุกต์ต่าง ๆ จากที่มีอยู่เดิมในระบบ การดำเนินการดังกล่าวจะมีผลกระทบต่อการทำงานของระบบ เช่น ประสิทธิภาพ ความน่าเชื่อถือของระบบ อย่างไร

2.6.4 ระยะที่ 4 การใช้งานระบบ (Production)

เป็นระยะที่ผู้ใช้ได้ใช้งานโปรแกรมประยุกต์ และระบบงานต่าง ๆ ที่ติดตั้งอยู่บนระบบเครือข่ายคอมพิวเตอร์ โดยอาศัยการทำงานของส่วนประกอบของระบบ และระบบย่อยต่าง ๆ ของระบบเครือข่ายคอมพิวเตอร์

2.6.5 ระยะที่ 5 การวิวัฒนาการของระบบ (Evolution)

เป็นระยะที่ทำการขยายการใช้งานระบบเดิมที่มีอยู่ โดยพิจารณาจากศักยภาพของระบบเดิมที่มีอยู่ เช่น การรองรับภาระงานที่เพิ่มขึ้น ความเชื่อถือได้ของระบบ เวลาตอบสนองของระบบ เป็นต้น

ในระยะต่าง ๆ ของวัฏจักรระบบเครือข่ายคอมพิวเตอร์ ดังกล่าวข้างต้น หากได้ดำเนินการทดสอบการทำงานของระบบตามลักษณะการทำงานของระบบดังที่ได้กล่าวข้างต้น ผลจากการทดสอบ จะช่วยให้ผู้มีหน้าที่ในการบริหารและจัดการระบบ สามารถดำเนินการแก้ไขปัญหา และปรับปรุงประสิทธิภาพของระบบ ให้สอดคล้องเหมาะสมต่อการดำเนินงานมากยิ่งขึ้น

การทดสอบการทำงานของระบบเครือข่ายคอมพิวเตอร์ เพื่อทำการวิเคราะห์ถึงแบบแผนของการสื่อสารข้อมูลในระบบอย่างมีประสิทธิภาพนั้น ควรจะทำการวิเคราะห์ทั้งในส่วนของโครงสร้างพื้นฐานของระบบ (Network Infrastructure) และการใช้งานโปรแกรมประยุกต์ต่าง ๆ (Network Application)

2.7 การทดสอบการทำงานของระบบเครือข่ายคอมพิวเตอร์

กล่าวถึงการทดสอบระบบเครือข่ายคอมพิวเตอร์สามารถจำแนกวัตถุประสงค์ของการทดสอบออกเป็น 10 ประการด้วยกัน (Buchanan,1996 : 66-77) คือ

2.7.1 การทดสอบเวลาตอบสนองของการใช้งานโปรแกรมประยุกต์ (Application Response Time Testing)

การทดสอบนี้จะทำการตรวจวัดเวลาที่ใช้ไป ในการทำงานตามคำสั่งของการใช้งานโปรแกรมประยุกต์ เช่น การอ่านแฟ้มข้อมูล การค้นหาข้อมูลที่ต้องการ การอ่านแฟ้มข้อมูล และการบันทึกกลับ เป็นต้น นอกจากนี้จะทำการตรวจวัดเวลาที่ใช้ไปในการทำงานตามคำสั่งข้างต่าง ๆ เมื่อมีการเพิ่มจำนวนผู้ใช้เข้าสู่ระบบ

2.7.2 การทดสอบความสามารถและความถูกต้องการทำงานของโปรแกรมประยุกต์ (Application/Functional Testing)

การทดสอบนี้จะตรวจสอบการทำงานของโปรแกรมประยุกต์ที่ใช้งานอยู่บนระบบ โดยพิจารณาความสามารถในการทำงานได้ถูกต้อง และครบถ้วนตามที่ได้กำหนดหรือออกแบบไว้หรือไม่ โดยจะทดสอบในสภาวะที่ปริมาณงานภาระงานในระบบมีปริมาณน้อยจนถึงปริมาณภาระงานที่มีขนาดปานกลาง

2.7.3 การทดสอบเพื่อประเมินการเสื่อมถอยของประสิทธิภาพการทำงานของระบบ (Regression Testing)

การทดสอบนี้มีวัตถุประสงค์เพื่อเปรียบเทียบประสิทธิภาพ ความน่าเชื่อถือของการทำงานระบบเดิม และการทำงานของระบบใหม่ก่อนที่จะมีการปรับปรุง หรือเปลี่ยนแปลงอุปกรณ์โปรแกรมประยุกต์ที่ใช้งานอยู่ ทั้งนี้ เพื่อเป็นการยืนยันว่าการดำเนินการปรับปรุงเปลี่ยนแปลงดังกล่าว จะไม่ทำให้ประสิทธิภาพการทำงานของอุปกรณ์ หรือโปรแกรมประยุกต์ที่ทำงานอยู่บนระบบเสื่อมถอยลง

2.7.4 การทดสอบปริมาณ (Throughput Testing)

การทดสอบนี้จะทำการตรวจวัดปริมาณข้อมูลที่ทำการรับ-ส่ง ระหว่างส่วนประกอบของระบบต่าง ๆ ที่สนใจศึกษา เช่น บริดจ์ เราเตอร์ ฮับ หรือ สวิทช์ เป็นต้น การตรวจวัดปริมาณงานช่วยให้ทราบถึง สภาวะการทำงานของอุปกรณ์ต่าง ๆ ประสิทธิภาพการทำงานของระบบโดยรวม การเกิดสภาวะคอขวด ณ จุดต่าง ๆ เป็นต้น

2.7.5 การทดสอบการยอมรับ (Acceptance Testing)

การทดสอบนี้เป็นกระบวนการในการที่ช่วยให้ผู้ใช้ระบบเชื่อมั่นว่าระบบใหม่สามารถทำงานได้อย่างมีเสถียรภาพ และมีประสิทธิภาพ การทดสอบควรดำเนินการในช่วงระยะของการติดตั้งระบบใหม่ การปรับปรุงระบบที่มีอยู่เดิม และโดยเฉพาะอย่างยิ่งระบบที่มีการดำเนินงานในลักษณะผู้ให้บริการ-ผู้รับบริการ ลักษณะงานที่มีความสำคัญ ตลอดจนการใช้งานในลักษณะที่ผู้ใช้กระจายอยู่ทั่วไปตามสถานที่ต่าง ๆ เป็นจำนวนมาก

2.7.6 **การทดสอบรูปแบบการต่อเชื่อม** (Configuration Sizing)

การทดสอบนี้จะทำการวัดค่าพารามิเตอร์ต่าง ๆ ซึ่งจะแสดงให้เห็นถึงประสิทธิภาพการทำงานของระบบ เช่น เวลาตอบสนอง ปริมาณงาน เป็นต้น ซึ่งค่าที่ตรวจวัดได้เป็นผลมาจากการต่อเชื่อมอุปกรณ์ในรูปแบบต่าง ๆ และนำมาเปรียบเทียบเพื่อให้ทราบถึงความแตกต่างด้านประสิทธิภาพ

2.7.7 **การทดสอบความเชื่อถือได้ของระบบ**(Reliability Testing)

การทดสอบนี้จะทดสอบการทำงานของระบบ ในสภาวะที่ระบบจำเป็นต้องรับภาระงานซึ่งมีปริมาณปานกลาง จนถึงปริมาณสูง โดยที่ปริมาณภาระงานในช่วงเวลาต่าง ๆ และระยะเวลาที่ระบบจะต้องรับภาระปริมาณภาระงานดังกล่าว จะต้องเป็นปริมาณภาระงานที่สูง และระยะเวลาที่ระบบต้องรับภาระงานดังกล่าวนานพอที่จะทำให้ระบบทำงานผิดพลาด วัตถุประสงค์ของการทดสอบนี้ต้องการที่จะทราบว่า เมื่อไรจะเกิดความล้มเหลวในการทำงานของระบบ และภาวะการล้มเหลวของระบบเป็นอย่างไร

2.7.8 **การประเมินความสามารถในการทำงานของอุปกรณ์ต่าง ๆ** (Product Evaluation)

การทดสอบนี้จะทำการตรวจวัดค่าพารามิเตอร์ต่าง ๆ เช่น ปริมาณงานที่เกิดขึ้น เวลาการตอบสนองในการทำงาน ความมีเสถียรภาพและความเชื่อถือได้ของระบบ และส่วนประกอบของระบบ โดยจะทำการเปรียบเทียบค่าพารามิเตอร์ต่าง ๆ ของระบบและส่วนประกอบของระบบที่ต้องการปรับปรุง หรือเปลี่ยนใหม่ โดยมีวัตถุประสงค์เพื่อขยายความสามารถในการรับภาระงานที่เพิ่มขึ้นของระบบ และเป็นการทดสอบเพื่อให้ทราบว่า เมื่อใดระบบปัจจุบันจำเป็นต้องเพิ่มทรัพยากรเข้าสู่ระบบเดิม เพื่อมิให้การทำงานของระบบเสื่อมถอยลง ในการทดสอบ จะดำเนินการ โดยเพิ่มปริมาณภาระงานเข้าสู่ระบบจนกระทั่งประสิทธิภาพของระบบเสื่อมถอยลงจนถึงระดับที่ไม่สามารถยอมรับได้

2.7.9 **การวางแผนการรองรับการเพิ่มการใช้งานระบบ** (Capacity Planning)

การทดสอบนี้เพื่อให้ทราบว่าเมื่อใดจึงจะต้องดำเนินการเพิ่มขีดความสามารถของระบบ เพื่อให้ระบบสามารถรองรับภาระงานที่เพิ่มขึ้นจากการเพิ่มจำนวนของผู้ใช้ ก่อนที่ประสิทธิภาพโดยรวมของระบบเสื่อมถอยลงถึงระดับที่ไม่สามารถยอมรับได้

2.7.10 การกำหนดการเกิดภาวะคอขวด และการแยกแยะปัญหา (Bottleneck Identification and Problem Isolation)

การทดสอบนี้จะดำเนินการกับส่วนประกอบของระบบ และระบบย่อยต่าง ๆ ทีละส่วน ที่สนใจศึกษา โดยทำการเก็บค่าปริมาณงานที่เกิดขึ้นของแต่ละส่วน และนำมาเปรียบเทียบกับปริมาณงานสูงสุดของระบบที่ระบบสามารถดำเนินงานอยู่ได้ ภาวะคอขวดที่เกิดขึ้นจะส่งผลกระทบต่อปริมาณงานของระบบโดยรวมและเวลาตอบสนองการทำงานของโปรแกรมประยุกต์ต่าง ๆ ที่ทำงานอยู่บนระบบ

จากวัตถุประสงค์การทดสอบระบบทั้ง 10 ประการข้างต้น สามารถนำมากำหนดและปรับใช้ให้สอดคล้องกับวัฏจักรระบบเครือข่ายคอมพิวเตอร์ได้ โดยสามารถแสดงได้ดังตารางที่ 2.7

ตารางที่ 2.7 แสดงถึงวัตถุประสงค์การทดสอบระบบในระยะต่าง ๆ ของวัฏจักรระบบเครือข่ายคอมพิวเตอร์

Network Application/Presentation Layers

Test Objective	Planing	Development	Deployment	Production	Evolution
ApplicationResponse Time	X	X	X	X	
Application Feature/Functionality		X	X	X	
Regression		X			X
Throughput	X	X	X		
Acceptance		X	X		
Configuration Sizing		X			X
Reliability	X	X			
Product Evaluation	X				
Capacity Planing			X		X
Bottleneck Identification				X	

บทที่ 3

การวิเคราะห์การทำงานของระบบแลนของธกส.

3.1 ลักษณะการเชื่อมต่อของระบบแลน

จากรูปที่ 1.1.1 แสดงถึงอุปกรณ์ในระบบแลนของธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร (ธกส.) ซึ่งมีตึกสำนักงานอยู่ 2 แห่ง กล่าวคือ สำนักงานใหญ่นางเลิ้งมี 2 อาคาร และตึกสำนักงานเทคโนโลยีสารสนเทศประชาชื่น และทั้งสองตึกดังกล่าวมีการต่อเชื่อมระบบแลน (LAN) เข้าด้วยกัน โดยมีคู่สายเช่าจำนวน 4 เส้นๆ ละ 2 เมกกะบิทเปอร์เซ็ค (Mbps) เป็นตัวกลางในการเชื่อมต่อกันซึ่งโปรแกรมจัดการเครือข่ายสามารถมองอุปกรณ์เครือข่ายต่างๆ ทั้งหมดทั้ง 2 แห่งได้ ถ้าอุปกรณ์เครือข่ายนั้นสนับสนุนโปรแกรมพื้นฐาน SNMP ว่ามีอุปกรณ์หน่วยใดบ้างที่สนับสนุนโปรแกรมพื้นฐานดังกล่าว

3.1.1 อุปกรณ์และการต่อเชื่อม ณ.สำนักงานใหญ่นางเลิ้ง

ประกอบด้วยอุปกรณ์อยู่ทั้งสิ้นจำนวน 37 หน่วย ดังนี้

อุปกรณ์ FDDI Concentrator	2 หน่วย	สนับสนุน SNMP
อุปกรณ์ Router	5 หน่วย	สนับสนุน SNMP
อุปกรณ์ LAN Switch	3 หน่วย	สนับสนุน SNMP
อุปกรณ์ Main Lan Switch	1 หน่วย	สนับสนุน SNMP
อุปกรณ์ Hub 24 Port	26 หน่วย	ไม่สนับสนุน SNMP

การเชื่อมต่อหลักเป็นระบบ FDDI แบบ Dual Attach โดยมีอุปกรณ์ FDDI Concentrator ยี่ห้อ CISCO รุ่น Catalyst 1400 จำนวน 2 หน่วยต่อเชื่อมกันด้วยความเร็ว 100 เมกกะบิท (Mbps) ระหว่างตึก 3 ชั้นและตึก 10 ชั้นของอาคารสำนักงานใหญ่ ซึ่งแต่ละตึกเชื่อมต่อจากอุปกรณ์ FDDI Concentrator ไปยังชุดอุปกรณ์ LAN Switch ยี่ห้อ CISCO รุ่น Catalyst 5000 และ Catalyst 2924 MXL ที่ตึก 10 ชั้นจำนวน 2 ชุด ที่ตึก 3 ชั้นจำนวน 1 ชุด จากนั้นก็ต่อสายกระจายไปยังอุปกรณ์ Hub 24 Ports ทั้งนี้ขึ้นกับจำนวนผู้ใช้ในแต่ละชั้นว่ามากน้อยเพียงใด โดยจะต่อไปยัง Outlet Terminal ด้วยความเร็วพอร์ตละ 10 Mbps

ส่วนการต่อเชื่อมกับพอร์ต (Port) หรือเซริฟเวอร์ (Server) ประกอบด้วย Router 2 หน่วยยี่ห้อ CISCO รุ่น 4000 ต่อกับ FDDI Concentrator ทั้งสองตัว ตัวละ 1 Port ด้วยความเร็ว 100 Mbps และจาก Router ดังกล่าวจะต่อเข้ากับระบบคอมพิวเตอร์ Mainframe จำนวน 4 Ports ที่

ความเร็วพอร์ตละ 10 Mbps ซึ่งปัจจุบันเครื่องเมนเฟรมดังกล่าวไม่ได้ใช้งานแล้ว จะมี Rounter ยี่ห้อ CISCO รุ่น 2500 ต่อตรงกับ LAN Switch เพื่อต่อออกไปยัง Internet Provider ของ KSC โดยมี Firewall กั้นระหว่าง Router กับ LAN Switch

ในส่วนของเซริฟเวอร์ที่ทำหน้าที่เป็น Font-End Processor จำนวน 2 ระบบ โดยต่อตรงเข้ากับ FDDI Concentrator ด้วยความเร็ว 100 Mbps และในส่วนของการเชื่อมกับสาขาและอาคารสำนักงานประชาชื่น โดยมี Router ยี่ห้อ CISCO รุ่น 7000 ต่อกับ FDDI Concentrator ทั้ง 2 หน่วยๆละ 1 Port และต่อกับอุปกรณ์ WAN ซึ่งเป็น Frame Relay Switch จากนั้นจะต่อเข้ากับ Main LAN Switch ยี่ห้อ CISCO 8540 รุ่น Catalyst ที่ต่อเชื่อมไปยังอาคารสำนักงานประชาชื่น

3.1.2 อุปกรณ์และการต่อเชื่อม ณ.สำนักงานเทคโนโลยีสารสนเทศประชาชื่น

อุปกรณ์และการต่อเชื่อม ณ.สำนักงานเทคโนโลยีสารสนเทศประชาชื่น ประกอบด้วยอุปกรณ์อยู่ทั้งสิ้น จำนวน 31 หน่วย ดังนี้

อุปกรณ์ Main LAN Switch	1 หน่วย สนับสนุน SNMP
อุปกรณ์ Central LAN Switch	1 หน่วย สนับสนุน SNMP
อุปกรณ์ LAN Switch	5 หน่วย สนับสนุน SNMP
อุปกรณ์ Fast Hub	22 หน่วย สนับสนุน SNMP
อุปกรณ์ Router	2 หน่วย สนับสนุน SNMP

การต่อเชื่อมประกอบด้วย Main LAN Switch ยี่ห้อ CISCO รุ่น Catalyst 8540 ต่อเชื่อมกับ Main LAN Switch ของอาคารสำนักงานใหญ่นางเลิ้ง และเชื่อมโยงไปยัง Central LAN Switch ยี่ห้อ CISCO รุ่น Catalyst 6009 ต่อสายกระจายไปยังชั้นต่างๆ ของอาคารด้วยความเร็ว 100 Mbps โดยมีอุปกรณ์ LAN Switch ยี่ห้อ CISCO รุ่น 2924 MXL ที่ชั้น 2,4,5 และ 9 เพื่อต่อกับ Fast Hub ที่ความเร็ว 100 Mbps และที่ชั้น 1,3,6,7,8 และ 10 มีการต่อเข้ากับ Fast Hub โดยตรง จากนั้นก็จะต่อตรงไปยัง Outlet ของผู้ใช้ตามจำนวนที่แตกต่างกันตามความจำเป็นของการใช้งาน รวมทั้งมีการต่อเชื่อม Router ยี่ห้อ CISCO รุ่น 3662 กับ Main LAN Switch และ Central LAN Switch อย่างละ 1 Port ที่ความเร็ว 100 Mbps และมี Router CISCO รุ่น 7206 ต่อตรงกับ 3662 เพื่อเตรียมไว้ต่อกับเซริฟเวอร์ของ Internet ซึ่งย้ายจากสำนักงานใหญ่นางเลิ้งมายังสำนักงานสารสนเทศประชาชื่น และเซริฟเวอร์อื่นๆ ที่จะจัดหามาใหม่เพื่อรองรับงานที่จะเกิดขึ้น

ในอนาคต

3.2 ลักษณะการทำงานของระบบแลน

ในการทำงานของระบบแลนของธกส. สามารถแบ่งออกเป็น 2 ลักษณะตามการส่งผ่านข้อมูล กล่าวคือ

3.2.1 ระบบที่ส่งผ่านข้อมูลมาจากระบบแวน (WAN)

ระบบที่ส่งผ่านข้อมูลมาจากระบบแวน (WAN) เป็นการส่งข้อมูลจะถูกสร้างขึ้นโดยสาขาและผ่านอุปกรณ์ WAN Switch ไปยัง FDDI Concentrator เพื่อทำการส่งต่อไปยังโอส (Host) หรือเซริฟ์เวอร์ (Server) ที่เก็บโปรแกรมประยุกต์ของระบบงานที่แตกต่างกันและมีการส่งข้อมูลจากโอส (Host) หรือเซริฟ์เวอร์ (Server) ผ่านระบบแลน (LAN) ไปยังระบบแวน (WAN) ไปยังโฮสปลายทางหรือเซริฟ์เวอร์ที่สาขา ดังเช่น ระบบงานฝาก-ถอนต่างสาขา ระบบการเงิน (FMIS : Financial Management Information System) ระบบการจัดการสารสนเทศทั่วๆ ไป (GMIS : General Management Information System) เป็นต้น

3.2.2 ระบบงานที่ใช้ข้อมูลเฉพาะในสำนักงานใหญ่

ระบบงานที่ใช้ข้อมูลเฉพาะในสำนักงานเป็นการส่งข้อมูลภายในสำนักงานใหญ่ที่มีการแลกเปลี่ยนข้อมูลระหว่างกันเฉพาะในโฮสที่สำนักงานใหญ่ โดยส่งข้อมูลผ่านอุปกรณ์แลนเท่านั้น ดังเช่น ระบบการออกรายงานสรุปที่ใช้เฉพาะสำนักงานใหญ่ ระบบทรัพยากรบุคคล (PIS : Personnel Information System) ระบบสำนักงานอัตโนมัติ (OA : Office Automation) และระบบเมล์ภายใน (Mailing) เป็นต้น

จะเห็นได้ว่าไม่ว่าจะเป็นการทำงานของระบบแลนลักษณะใดก็ตาม จะต้องมีการส่งต่อข้อมูลระหว่างอุปกรณ์ต่างๆ ในระบบแลนและมีปริมาณข้อมูลที่ผ่านเข้าสู่ระบบที่มีปริมาณแตกต่างกัน ซึ่งหากเกิดปัญหาขึ้นกับระบบแลน ณ.ที่ใดที่หนึ่ง จึงยากต่อการวิเคราะห์ปัญหาที่แท้จริง ซึ่งจากเหตุการณ์ที่ผ่านมาได้มีการเก็บข้อมูลที่เกิดขึ้นกับปัญหาของระบบแลน และนำมาจัดทำตารางและทำมาเทียบกับสัญญาณบอกเหตุการณ์ต่างๆ เพื่อเป็นแนวทางในการวิเคราะห์ปัญหาได้ดังหัวข้อต่อไปนี้

3.3 <u>สภาพการเกิดปัญหาและสัญญาณบอกเหตุ</u>

จากการที่ระบบเครือข่ายแลนประกอบด้วยส่วนประกอบต่างๆ ที่ทำให้ระบบสามารถทำงานได้อย่างมีประสิทธิภาพ ดังนั้นการทำงานผิดพลาดของอุปกรณ์ในแต่ละส่วนจะมีผลกระทบต่อการทำงานโดยรวมของระบบ การทำงานผิดพลาดของระบบสามารถพิจารณารูปแบบหรือแบบแผนการทำงานที่ต่างไปจากสภาวะการทำงานตามปกติ โดยสามารถติดตามและเฝ้าควบคุมจาก Network Management Station สภาพการเกิดปัญหาและสัญญาณบอกเหตุดังต่อไปนี้ จะช่วยเป็นแนวทางในการให้ผู้ควบคุมการทำงานของระบบสามารถตระหนักและรับรู้ถึงปัญหาที่ดำรงอยู่ในระบบ เพื่อเป็นแนวทางในการแก้ปัญหาดังกล่าว สามารถแสดงรายละเอียดได้ดังตารางที่ 3.3

ตารางที่ 3.3 แสดงสภาพการเกิดข้อผิดพลาดและสัญญาณบอกเหตุ

<u>สภาพการเกิดข้อผิดพลาด</u>	*สัญญาณบอกเหตุ*
สายสัญญาณไฟเบอร์ออพติกชำรุด	• โหนดไม่ทำงาน • ไม่สามารถให้บริการแฟ้มข้อมูลผ่านระบบเครือข่าย • เกิดสภาวะการติดขัดของการส่งข้อมูล
การต่อเชื่อมสายสัญญาณไม่สมบรูณ์	• เกิดสภาวะ Bad Packet มาก • การชนกันของสัญญาณมากขึ้น • อัตราการเกิดข้อผิดพลาดการส่งข้อมูลมากขึ้น • ประสิทธิภาพโดยรวมของระบบลดลง • ข้อมูลในแฟ้มข้อมูลผิดพลาดไม่สมบรูณ์
การทำงานของเราน์เตอร์ผิดพลาด	• โหนดไม่ทำงาน • การชนกันของสัญญาณมากขึ้น • อัตราการเกิดข้อผิดพลาดการส่งข้อมูลมากขึ้น • ประสิทธิภาพโดยรวมของระบบลดลง • การทำงานของแฟ้มข้อมูลบนระบบช้าลง

ตารางที่ 3.3 แสดงสภาพการเกิดข้อผิดพลาดและสัญญาณบอกเหตุ (ต่อ)

สภาพการเกิดข้อผิดพลาด	*สัญญาณบอกเหตุ*
การทำงานของเราน์เตอร์ผิดพลาด	• เวลาที่ใช้ในการตอบสนองของระบบเพิ่มขึ้น • อัตราการส่งทวนข้อมูลมีมากขึ้น
เกิดสภาวะการส่งข้อมูลในลักษณะของบรอดคาสต์มากขึ้น	• การทำงานของเราน์เตอร์เกินสภาวะปกติ • โปรแกรมการบริหารงานระบบทำงานเกินสภาวะปกติ • การตั้งค่าเตือนของระบบมีมากเกินไป • ประสิทธิภาพการทำงานของระบบไม่คงที่
อุปกรณ์ในระบบทำให้เกิดสภาวะการเกิดสภาพบรอดคาสต์	• การชนกันของสัญญาณมีมากขึ้น • ประสิทธิภาพการทำงานของระบบลดลง • อัตราการส่งทวนข้อมูลมีมากขึ้น • เวลาที่ใช้ในการตอบสนองของระบบเพิ่มขึ้น • เกิดสภาวะความหนาแน่นการส่งข้อมูลของระบบแฟ้มข้อมูล ระบบเครือข่ายและเครื่องคอมพิวเตอร์ที่นำมาต่อเชื่อม
การกำหนดและติดตั้งสภาวะการทำงานของระบบผิดพลาด	• จำนวนของ Bad Packet มีมากขึ้น • การทำงานของเราน์เตอร์เกินสภาวะปกติเกิดข้อผิดพลาดในการ Encapsulate ของข้อมูลที่ทำการรับส่ง • อัตราการเกิดข้อผิดพลาดการส่งข้อมูลมากขึ้น • ประสิทธิภาพโดยรวมของระบบลดลง • อัตราการส่งทวนข้อมูลมีมากขึ้น • เวลาที่ใช้ในการตอบสนองของระบบเพิ่มขึ้น • เกิดสภาวะความหนาแน่นการส่งข้อมูลของระบบแฟ้มข้อมูล ระบบเครือข่ายและเครื่องคอมพิวเตอร์ที่นำมาต่อเชื่อม
การเชื่อมต่อและติดตั้งสัญญาณไม่สมบรูณ์	• จำนวนของ Bad Packet มีมากขึ้น • อัตราการเกิดข้อผิดพลาดการส่งข้อมูลมากขึ้น • การชนกันของสัญญาณมากขึ้น • อัตราการส่งทวนข้อมูลมีมากขึ้น

ตารางที่ 3.3 แสดงสภาพการเกิดข้อผิดพลาดและสัญญาณบอกเหตุ (ต่อ)

สภาพการเกิดข้อผิดพลาด	*สัญญาณบอกเหตุ*
การเชื่อมต่อและติดตั้งสัญญาณไม่สมบรูณ์	• เกิดสภาวะความหนาแน่นการส่งข้อมูลของระบบแฟ้มข้อมูล ระบบเครือข่ายและเครื่องคอมพิวเตอร์ที่นำมาต่อเชื่อม
ทรานซิฟเวอร์ทำงานผิดพลาด	• จำนวนของ Bad Packet มีมากขึ้น • อัตราการเกิดข้อผิดพลาดการส่งข้อมูลมากขึ้น • การชนกันของสัญญาณมากขึ้น • เกิดสภาวะความหนาแน่นการส่งข้อมูลของเครื่องคอมพิวเตอร์ที่นำมาต่อเชื่อม
ระบบเครือข่ายเกิดสภาพความหนาแน่นปริมาณการรับ-ส่งข้อมูลเกินสภาวะปกติ	• อัตราการเกิดข้อผิดพลาดการส่งข้อมูลมากขึ้น
เกิดข้อผิดพลาดกับ SNMP Agent	• ไม่สามารถทำการเก็บข้อมูลทางสถิติของระบบได้
สายสัญญาณที่นำมาต่อเชื่อมยาวเกินไป	• จำนวนของ Bad Packet มีมากขึ้น • การทำงานของบริดท์เกินสภาวะปกติ • เกิดข้อผิดพลาดในการ Encapsulate ของข้อมูลที่ทำการรับ-ส่ง • การชนกันของสัญญาณมีมากขึ้น • ประสิทธิภาพโดยรวมของระบบลดลง • อัตราการส่งทวนข้อมูลมีมากขึ้น • เวลาที่ใช้ในการตอบสนองของระบบเพิ่มขึ้น • เกิดสภาวะความหนาแน่นการส่งข้อมูลของระบบแฟ้มข้อมูล ระบบเครือข่ายและเครื่องคอมพิวเตอร์ที่นำมาต่อเชื่อม
การติดตั้ง NIC ไม่ถูกต้อง	• การชนกันของสัญญาณมีมากขึ้น • ประสิทธิภาพโดยรวมของระบบลดลง • อัตราการส่งทวนข้อมูลมีมากขึ้น • โหนดไม่ทำงาน

ตารางที่ 3.3 แสดงสภาพการเกิดข้อผิดพลาดและสัญญาณบอกเหตุ (ต่อ)

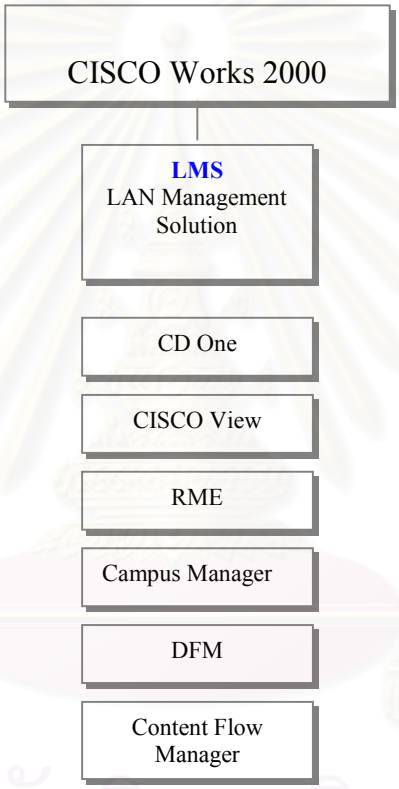
สภาพการเกิดข้อผิดพลาด	*สัญญาณบอกเหตุ*
NIC ทำงานในขณะที่ทำการ Disable โหนด	• จำนวนของ Bad Packet มีมากขึ้น • ประสิทธิภาพโดยรวมของระบบลดลง • เวลาที่ใช้ในการตอบสนองของระบบเพิ่มขึ้น • เกิดสภาวะความหนาแน่นการส่งข้อมูลของระบบแฟ้มข้อมูล ระบบเครือข่ายและเครื่องคอมพิวเตอร์ที่นำมาต่อเชื่อม • ไม่พื้นที่ว่างบนดิสก์และไฟล์
เกิดข้อผิดพลาดกับโปรโตคอล	• จำนวนของ Bad Packet มีมากขึ้น • การทำงานของ Repeater Bridge หรือเราน์เตอร์เกินสภาวะปกติ • เกิดข้อผิดพลาดในการ Encapsulate ของข้อมูลที่ทำการรับ-ส่ง
เกิดข้อผิดพลาดกับโปรโตคอล	• การชนกันของสัญญาณมีมากขึ้น • ประสิทธิภาพโดยรวมของระบบลดลง • อัตราการส่งทวนข้อมูลมีมากขึ้น • เวลาที่ใช้ในการตอบสนองของระบบเพิ่มขึ้น • เกิดสภาวะความหนาแน่นการส่งข้อมูลของระบบแฟ้มข้อมูล ระบบเครือข่ายและเครื่องคอมพิวเตอร์ที่นำมาต่อเชื่อม
การสอบถามข้อมูลไม่ทำการ Optimize ณ.เครื่องคอมพิวเตอร์ที่ทำการสอบถาม	• จำนวนของ Bad Packet มีมากขึ้น • ระบบเครือข่ายทำงานเกินสภาวะปกติการรับ-ส่งข้อมูลโดยการ Encapsulate ของข้อมูลที่ทำการรับส่งมีมากกว่าปกติ • การชนกันของสัญญาณมีมากขึ้น • ประสิทธิภาพโดยรวมของระบบลดลง • เวลาที่ใช้ในการตอบสนองของระบบเพิ่มขึ้น
การทำงานของเราน์เตอร์เกินสภาวะปกติ	• จำนวนของ Bad Packet มีมากขึ้น • การทำงานของบริดท์เกินสภาวะปกติ

ตารางที่ 3.3 แสดงสภาพการเกิดข้อผิดพลาดและสัญญาณบอกเหตุ (ต่อ)

สภาพการเกิดข้อผิดพลาด	*สัญญาณบอกเหตุ*
การทำงานของเราน์เตอร์เกินสภาวะปกติ	• การชนกันของสัญญาณมีมากขึ้น • ประสิทธิภาพโดยรวมของระบบลดลง • อัตราการส่งทวนข้อมูลมีมากขึ้น • เวลาที่ใช้ในการตอบสนองของระบบเพิ่มขึ้น • เกิดสภาวะความหนาแน่นการส่งข้อมูลของระบบแฟ้มข้อมูล ระบบเครือข่ายและเครื่องคอมพิวเตอร์ที่นำมาต่อเชื่อม
มีการรับ-ส่งข้อมูลของ SNMP มากเกินไปในระบบ	• จำนวนของ Bad Packet มีมากขึ้น • การชนกันของสัญญาณมีมากขึ้น • ประสิทธิภาพโดยรวมของระบบลดลง • อัตราการส่งทวนข้อมูลมีมากขึ้น • เวลาที่ใช้ในการตอบสนองของระบบเพิ่มขึ้น
มีการรับ-ส่งข้อมูลของ SNMP มากเกินไปในระบบ	• เกิดสภาวะความหนาแน่นการส่งข้อมูลของระบบแฟ้มข้อมูล ระบบเครือข่ายและเครื่องคอมพิวเตอร์ที่นำมาต่อเชื่อม
สายสัญญาณ UTP ไม่ได้มาตรฐานหรือเสื่อมคุณภาพ	• จำนวนของ Bad Packet มีมากขึ้น • ข้อมูลในแฟ้มข้อมูลเสียหาย • การชนกันของสัญญาณมีมากขึ้น • ประสิทธิภาพโดยรวมของระบบลดลง • อัตราการส่งทวนข้อมูลมีมากขึ้น • เวลาที่ใช้ในการตอบสนองของระบบเพิ่มขึ้น • เกิดสภาวะความหนาแน่นการส่งข้อมูลของระบบแฟ้มข้อมูล ระบบเครือข่ายและเครื่องคอมพิวเตอร์ที่นำมาต่อเชื่อม • เกิดข้อผิดพลาดในการ Encapsulate โหนดไม่สามารถติดต่อได้ • การทำงานของโปรโตคอลผิดพลาด

3.4 การทำงานของระบบจัดการเครือข่าย CISCO Works 2000

เนื่องจากระบบที่ออกแบบเป็นระบบที่ต้องใช้โปรแกรมจัดการเครือข่าย CISCO Works 2000 ซึ่งในส่วนของโปรแกรมจัดการเครือข่ายแลนดังกล่าวประกอบด้วยโมดูล (Module) หลักๆ 6 โมดูลด้วยกัน ดังแสดงในรูปที่ 3.4



รูปที่ 3.4 แสดงโมดูลของโปรแกรมจัดการเครือข่าย CISCO Works 2000 ในส่วนของ LMS

จากรูปที่ 3.4 โมดูลของโปรแกรมจัดการเครือข่าย CISCO Works 2000 ประกอบด้วยโมดูลของวิธีการแก้ไขปัญหาการจัดการระบบแลน (LAN Management Solution : LMS)

3.5 ฟังก์ชั่นการทำงานของโปรแกรมจัดการเครือข่าย CISCO Works 2000

โปรแกรมการจัดการระบบเครือข่าย CISCO Works 2000 เป็นชื่อทางการค้าของระบบการจัดการด้านระบบแลน โดยประกอบด้วยโปรแกรมการจัดการแก้ไขปัญหาของแลน (LAN Management Solution (LMS)) ซึ่งเป็นส่วนหนึ่งของ CISCO Works 2000 และโปรแกรมการจัดการแก้ไขปัญหาของแลน (LMS) ประกอบด้วยโปรแกรมที่แยกหน้าที่การทำงาน ได้ดังนี้

3.5.1 CISCO Works 2000 Campus Manager

3.5.1.1 หน้าที่ของโปรแกรม Campus Manager

เป็นโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อการจัดการพื้นฐานเบื้องต้นในระบบ ซึ่งมีหน้าที่หลัก ดังนี้

- สามารถทำการค้นหาและแสดงรูปแบบเครือข่ายเลเยอร์ 2 ขนาดใหญ่
- กำหนดค่าวีแลน (VLAN) การจำลองแลน (LAN Emulation) และอซิงโครนัสทรานสเฟอโหมด (ATM : Asynchronous Transfer Mode)
- แสดงการเชื่อมต่อและสถานะของอุปกรณ์บนพื้นฐานของ เอสเอ็นเอ็มพี (SNMP: Simple Network Management Protocal)
- กำหนดความขัดแย้งของโครงสร้างในเลเยอร์ 2
- วินิจฉัยความสัมพันธ์ของปัญหาระหว่างอุปกรณ์ปลายทางและอุปกรณ์ในเลเยอร์ 2 และเลเยอร์ 3
- ระบุตำแหน่งที่อยู่และความสัมพันธ์โดยอัตโนมัติให้กับผู้ใช้ โดยการใช้ แมค (MAC: Media Access Control) ไอพีแอทเดรส (IP Address) เอ็นที (NT) หรือเอ็นดีเอส (NDS: Netware Directory Services) ล็อคอิน โฮสเนมกับความสัมพันธ์ทางกายภาพไปยังสวิตซ์เน็ทเวริค์ (Switch Network)
- เฝ้าติดตามเส้นทางในระดับเลเยอร์ 2 และเลเยอร์ 3 ของแหล่งที่มาและปลายทาง
- สามารถส่งผ่านรูปแบบการต่อเชื่อม (Topology Maps) ไปยังวิสิโอ (Visio)
- ใช้เครื่องมือของจาวา (Java) ในการพัฒนาประสิทธิภาพของการโต้ตอบ

3.5.1.2 **โปรแกรมย่อยของ** Campus Manager

โปรแกรม Campus Manager ประกอบด้วยโปรแกรมย่อยอีก 3 ระบบที่สามารถเรียกผ่านบราวน์เซอร์ (Browser) ของผู้ใช้ปลายทาง กล่าวคือ

- **Topology Services**
  เป็นการต่อเชื่อมโดยแสดงเป็นตารางสรุประดับเลเยอร์ 2 ในลักษณะของต้นไม้ (Tree)

- **User Tracking**
  เป็นโปรแกรมสนับสนุนการกำหนดการเชื่อมต่อของปลายทาง (End-Station) กับการสวิซท์การค้นหา (Access Switch) ที่กำหนดเป็นตารางและข้อมูลการสร้างการเชื่อมต่อของเลเยอร์ 2

- **Path Analysis**
  เป็นโปรแกรมสำหรับการจัดการสวิซท์เน็คเวอร์ (Switch Network) ซึ่งมีความสามารถในการวิเคราะห์ปัญหาของการต่อเชื่อมเส้นทาง นำเสนอในรูปภาพ ซึ่งมีการจัดการเฉพาะส่วนของไอพีแอสเดรส (IP Address) วีแลน (VLAN)

3.5.1.3 **ลักษณะของ** Campus Manager 3.1

Campus Manager ประกอบด้วยฟังก์ชั่นต่างๆ ได้แก่ Topology Service, User Tracking, Path Analysis และ VLAN/ LANE Port Assignment โดยที่ผู้บริหารเครือข่ายสามารถใช้ เรียนรู้ ตรวจสอบ กำหนดค่า วิเคราะห์และเปลี่ยนแปลงค่าต่างๆ ไปยังระบบเครือข่าย ซึ่งสามารถถูกเปลี่ยนแปลงแก้ไขได้

Topology Services ทำหน้าที่ในการประมวลรูปแบบกว้างๆ ของการต่อเชื่อมทางกายภาพ (Physical) และตรรกภาพ (Logical) สรุปรายชื่อของอุปกรณ์ พอร์ต และความสัมพันธ์ของเครือข่าย

หน้าที่หลักๆ ของ Topology Service ประกอบด้วย

- การค้นหาโดยอัตโนมัติ (Autodiscovery) และแสดงอุปกรณ์ CISCO Switch และเราน์เตอร์ (Router) โดยใช้ CISCO Discovery Protocal (CDP) และ SNMP
- แสดงการเชื่อมต่อทางกายภาพ (Physical) และตรรกภาพ (Logical) ในเลเยอร์ที่ 2 (Layer)
- จุดเด่นของระบบสามารถกำหนดเฉพาะเจาะจงไปยังอุปกรณ์ของ CISCO และอุปกรณ์อื่นๆ ที่สัมพันธ์กับ CISCO
- สามารถขยายเพื่อรับอุปกรณ์ได้มากกว่า 2000 ชนิดที่เป็น CISCO
- สามารถระบุสถานะของอุปกรณ์บนพื้นฐานของ CDP, ILMI, ELMI และ SNMP
- รายงานสิ่งที่ไม่ถูกต้องอัตโนมัติในระหว่างการพบปัญหาการเชื่อมต่อ เช่นการเชื่อมต่อผิด
- แสดงผลการเชื่อมต่อในลักษณะรูปภาพสำหรับการสร้าง VLAN, LANE สำหรับ Ethernet และ Token Ring
- แสดงการเชื่อมต่อและวิเคราะห์โปรโตคอล ATM

3.5.1.4 VLAN/LANE Configuration and Port Assignment

Campus Manager เป็นตัวจัดการการแสดงในลักษณะกราฟิก เพื่อสร้าง แก้ไขและลบค่าของ VLAN/ LANE ของอุปกรณ์หรือกำหนดพอร์ตของ VLAN สามารถสร้างแก้ไขพอร์ตและผู้ใช้เปลี่ยนแปลงในขณะที่แก้ไขและส่งไปยังอุปกรณ์สวิทช์ เพื่อแก้ไขการกำหนดการเชื่อมต่อเฉพาะสวิทช์พร้อมทั้งผู้บริหารเครือข่ายสามารถดูตารางของการต่อเชื่อมแบบต้นไม้ (Spanning-Tree States) และวีทีพีทรังช์ (VTP Trunks) พอร์ตที่เชื่อมต่อของสวิทช์และส่วนของ LANE ที่ใช้อยู่

การบริหารจัดการ VLAN มีหน้าที่ครอบคลุม ดังนี้

- ทำตารางสรุปของ VLAN เพื่อแสดงสถานะต่างๆ ของพอร์ต อุปกรณ์ลักษณะการต่อเชื่อม
- สามารถกำหนดค่า VLAN แบบกราฟิก ทำให้ง่ายต่อการใช้และบริหาร
- รวมการให้บริการการกำหนดค่า LANE ใน VLAN เพื่อประสิทธิภาพสูงสุดของผู้ใช้งานและการจัดการควบคุม

- แยกส่วนติดต่อของผู้บริหารระบบเพื่อง่ายต่อการค้นหา โดยใช้หลักเกณฑ์ที่หลากหลายและกำหนดเลือกพอร์ตและสวิทช์ โดยเฉพาะหรือทั้งหมดไปยัง VLAN
- แสดงตรรกภาพของโครงสร้าง VLAN ง่ายต่อการเข้าใจ
- รายงานสิ่งที่ขัดแย้งอัตโนมัติเน้นทางด้านปัญหาการเชื่อมต่อและการเชื่อมต่อที่ผิด
- ขึ้นทะเบียนสมาชิกใหม่อัตโนมัติ ช่วยลดเวลาการให้บริการและการกำหนดการต่อเชื่อมต่อ

3.5.1.5 **การจัดการในส่วนของเอทีเอ็ม** (ATM)

Campus Manager เสนอเครื่องมือการจัดการเอทีเอ็มเน็คเวิร์ด (ATM Network) ในรูปแบบของกราฟิก ซึ่งง่ายต่อการกำหนดค่าต่างๆ และการตรวจเช็คประสิทธิภาพของเครือข่ายเอทีเอ็ม จะถูกแสดงบนโทโปโลยีแผนที่ (Topology Map) และตรรกภาพ VLAN และเอทีเอ็ม (ATM) กับส่วนประกอบเอทีเอ็มสวิซท์และ LANE โดยมีฟังก์ชั่นต่างๆ ดังนี้

- ค้นหาอัตโนมัติของเอทีเอ็มสวิทช์ (ATM Switch) ทั้ง SVC และ PVC
- ตรวจสอบการเชื่อมต่อของ SVC และ PVC
- เส้นทางของวงจรเสมือนเอ็น-ทู-เอ็น (End-to-end) และวิเคราะห์การเชื่อมต่อ
- แก้ไขและวิเคราะห์ปัญหา LANE
- กำหนดค่าคุณภาพของการให้บริการ (Qos) เพื่อง่ายต่อการกำหนดค่าของความหนาแน่นของเน็ทเวิร์ค (Network) ดังเช่น วีดีโอ (VDO) หรือคอนสแตนท์บิทเรท (Constant-bit-rate: CBR)
- สามารถทำการรวบรวมและวิเคราะห์เอทีเอ็ม (ATM) แบบระยะไกล (RMON)

3.5.1.6 **ยูสเซอร์แทรกกิ่ง** (User Tracking)

สามารถหาที่ตั้งของเซริฟ์เวอร์ (Server) เอ็นยูสเซอร์ (End-User) และ CISCO Voice over IP: VOIP) และสวิทช์ที่ต่ออยู่บนเลเยอร์ 2 ในระหว่างกระบวนการ

ตรวจพบนี้มีการกำหนดการจัดตารางข้อมูลการเชื่อมต่อ ซึ่งประกอบด้วย

- ชื่อของ VLAN และโดเมนของ VTP
- เลขที่ของสวิทซ์พอร์ต (Switch Port Number) ชื่อและสถานะ
- MAC และหมายเลขของ IP Address ของสถานีและซับเน็ท (Subnet)
- รายชื่อตารางและรายละเอียดของตารางการเรียงลำดับของสวิทซ์ทั้งหมดที่ต่อกับส่วนอื่น
- สถานที่ตรวจพบท้ายสุดใน Time Stamp
- ชื่อล็อกอินของผู้ใช้ผ่านระบบอัตโนมัติจาก Windows NT หรือ Novell หรือ UNIX

ดังนั้น Campus Manager นั้นง่ายต่อความยืดหยุ่นทางธุรกิจหลายประเภท โดยกำหนดค่ากว้าง (Large Number) ของค่าพารามิเตอร์การจัดลำดับ (Sorting Parameters) ซึ่งสามารถใช้หาที่ตั้งสถานีของผู้ใช้ปลายทาง การตรวจสอบผู้ใช้งาน (User Tracking) สามารถตรวจพบสถานีปลายทางที่เชื่อมต่อไปยังพอร์ตของสวิทซ์โดยอัตโนมัติ และจัดการแสดงผลให้กับผู้ใช้โดยกำหนด VLAN ของผู้ใช้และการเชื่อมต่อไปยังสถานีต้นทาง ทั้งนี้การตรวจสอบผู้ใช้งาน (User Tracking) สามารถรองรับเสียงหรือข้อมูล รวมทั้งส่วนที่ติดต่อไปยัง CISCO Call Manager สำหรับที่อยู่ของ IP และ MAC (IP/MAC Address) ที่สัมพันธ์กันใน VOIP Handset ด้วยการกำหนดหมายเลขโทรศัพท์และผู้ใช้

การบริหารจัดการตรวจสอบผู้ใช้งาน (User Tracking) มีหน้าที่ครอบคลุม ดังนี้

- สามารถรองรับสถานีผู้ใช้ปลายทางได้ถึง 40,000 สถานี
- แจ้งรายงานแสดงการจำลองที่อยู่ของ IP และที่อยู่ของ MAC และพอร์ตกับอีกหลายๆ ที่อยู่ของ MAC
- ที่อยู่ของ IP และที่อยู่ของ MAC ของ VOIP Handsets ที่ตรวจพบด้วยการกำหนดหมายเลขโทรศัพท์และผู้ใช้
- แสดงผลในรูปของตาราง (Tabular) และความสามารถในการจัดลำดับพอร์ตของสวิทซ์ที่เกี่ยวข้องกันกับสถานีของผู้ใช้ปลายทางและ IP Handsets
- ทำตารางสำหรับแจ้งผู้ใช้ และทำรายละเอียดของรายงาน
- ระบบการแสดงผลแบบกราฟิก (GUI) สำหรับผู้ใช้ๆ เป็นแนวทางของโครงสร้าง

ตารางข้อมูล เพื่อรองรับการเคลื่อนไหวและเปลี่ยนแปลงของผู้ใช้

- จัดการตารางสำหรับการเปลี่ยนแปลงที่อยู่ที่มีการเปลี่ยนแปลงโดยอัตโนมัติ
- ง่ายต่อการใช้งานเพื่อหาที่ตั้งของผู้ใช้ โดยกำหนด MAC Address, IP Address, DNS Hostname, Port Label, Switch และ Option Voice Handsets

3.5.1.7 **การวิเคราะห์เส้นทาง** (Path Analysis)

การวิเคราะห์เส้นทางเป็นเครื่องมือในการวิเคราะห์ที่สมบรูณ์แบบสำหรับกำหนดส่วนของเลเยอร์ 2 และเลเยอร์ 3 เมื่อ Campus Manager มีการตรวจพบข้อมูลที่สถานีปลายทางหรือข้อมูลโครงสร้าง VLAN/ VLANE และข้อมูลแบบเรียลไทม์ (Real-Time) ของเลเยอร์ 3 และการคำนวณ Spanning-Tree

การวิเคราะห์เส้นทาง ประกอบด้วย

3.5.1.7.1 ส่วนข้อมูลของเลเยอร์ 2 และเลเยอร์ 3 หรืออุปกรณ์เลเยอร์ 2 และเลเยอร์ 3 หรือทิศทางของเส้นทาง (Route)

3.5.1.7.2 ลักษณะเฉพาะในส่วนของเลเยอร์ 2 และเลเยอร์ 3 ประกอบด้วย

- IP Address และส่วนติดต่อ
- ชื่อโดเมนของ VLAN และ VTP
- ความเร็วของพอร์ตและการตั้งแบบ Duplex

3.5.1.7.3 ทำการตรวจสอบได้ทันทีหรือตั้งเป็นตารางกำหนดการตรวจสอบ

3.5.1.7.4 ทำการตรวจสอบ IP Address, ชื่อของ DNS หรือหมายเลขโทรศัพท์สำหรับเสียงเรียกเช่นเดียวกับจุดเริ่มต้นและสิ้นสุด

3.5.1.8 Built-on the CISCO Works2000 Manager Servers

CISCO Works2000 Manager Server เป็นตัวจัดการการใช้ทรัพยากรร่วมกัน ได้แก่ การบริหารเว็บ การค้นพบการแชร์ฐานข้อมูลและแชร์การบริการ การจัดการเดสท็อบ (Desktop) หรือการบริหารการเชื่อมต่อของ CISCO ซึ่งถือว่าเป็นบริการหนึ่งบนเซริฟ์เวอร์ของ CISCO Works2000 ประกอบด้วยชุดเครื่องมือสำหรับการรวม

โปรแกรมเข้าไปในการจัดการเดสท็อบ โดยใช้มาตรฐานของรูปแบบและเทคโนโลยีของอินเทอร์เน็ต (Internet) เครื่องมือเหล่านี้ยอมให้ผู้ใช้เชื่อมต่อไปยังโปรแกรมการจัดการเว็บเบส (Web-Based) ไปยังผลิตภัณฑ์ของตระกูล CISCO Works2000 และผู้พัฒนาโปรแกรมสามารถเชื่อมไปยังเว็บเบส (Web-Based) ได้สะดวกและง่ายขึ้น โดยการมีการรับรองการลงทะเบียน การบริหารการเชื่อมต่อของ CISCO ใช้ได้กับ CISCO และผู้ขายระบบการจัดการเครือข่ายอีก 30 ราย ได้แก่ Hewlett-Packard (HP), Computer Asso-ciates, SUN Microsystems และ Tivoli Systems ได้รับรองการสร้างการบริหารจัดการเชื่อมโยงสำหรับโปรแกรมผู้ขายทำให้ผู้ใช้สามารถจัดการอินเทอร์เน็ต (Internet) ได้ง่าย และเชื่อมต่อไปยังโปรแกรมการจัดการรูปแบบเว็บ

3.5.2 CISCO Works2000 Device Fault Manager (DFM)

Device Fault Manager (DFM) เป็นสมาชิกใหม่ของตระกูล CISCO Works2000 ในการจัดการวิเคราะห์ความผิดพลาดแบบเรียลไทม์ (Real-Time) สำหรับอุปกรณ์ของ CISCO โดยใช้ความหลากหลายของข้อมูลที่จัดเก็บไว้และใช้การวิเคราะห์ทางเทคนิค DFM ทำให้เกิด Intelligent CISCO Traps สามารถส่งต่อไปยังอุปกรณ์ของผู้ขายรายอื่นๆ ที่เคยติดตั้งระบบการจัดการในระบบเครือข่าย โดยส่งไปยัง E-Mail/ Pager Gateway หรือแสดงใน DFM Alarm Window

DFM จัดการวิเคราะห์รายละเอียดความผิดพลาดแบบเรียลไทม์ (Real-Time) โดยมีการออกแบบเป็นพิเศษสำหรับอุปกรณ์ของ CISCO โดย DFM สามารถควบคุม CISCO Technology-Based Network สำหรับความหลากหลายของความผิดพลาด ดังนั้น DFM จึงมีการออกแบบมาให้รองรับกับ Router, Switch, Access Servers และ Hub ของ CISCO ได้มากกว่า 100 เครื่อง รวมทั้ง DFM สามารถมองเห็นและตรวจสอบได้อัตโนมัติไปยังลำดับของปัญหาธรรมดาที่ระดับอุปกรณ์และระดับ VLAN ทั้งหมดปราศจากการร้องขอจากผู้ใช้ที่เขียนกฎหรือ
กำหนด Polling หรือค่าเริ่มต้น เช่นเดียวกันกับระบบเครือข่ายที่โตขึ้นและเปลี่ยนแปลงไป DFM จะทำการตรวจสอบการเปลี่ยนแปลงในอุปกรณ์ของ CISCO และจัดให้เข้าระดับตามการวิเคราะห์

ลักษณะของ DFM ประกอบด้วย

3.5.2.1 จุดศูนย์รวมการวิเคราะห์ปัญหาความผิดพลาด

DFM จะทำการตรวจสอบขนาดของปัญหาโดยปรากฏใน CISCO Internetworking และตรวจสอบความแตกต่างของสภาวะต่างๆ ทางอินเทอร์เน็ตคอนโทรลแมสเซทโปรโตคอล (Internet Control Message Protocal: ICMP), SNMP, MIB และ SNMP trap recieption กรณีที่ DFM รับข้อมูลจากอุปกรณ์ซึ่งเป็นปัญหาที่อยู่นอกเหนือจากข้อกำหนด DFM ก็จะปล่อยปัญหาดังกล่าว ดังนั้นการจัดการนี้เป็นโอกาสสำหรับ IT Manager ที่ทำการจัดการกับอุปกรณ์ CISCO ที่ผิดพลาด รวมทั้ง DFM สามารถจดจำได้อย่างง่ายดาย ถ้าชุดของพอร์ตเกิดการล่ม (Down) ซึ่งมีการแสดงผลที่เกิดขึ้นด้วยชุดของพอร์ตที่ล่ม โดย DFM จะจดจำแต่ละพอร์ตที่อยู่บนโมดูลเดียวกันและบอกผู้ใช้ว่าโมดูลใดเกิดการล่ม ในส่วนของการวิเคราะห์ DFM เหมาะแก่การวิเคราะห์อย่างต่อเนื่องสำหรับอุปกรณ์ของ CISCO และพอร์ตบนอุปกรณ์ DFM สามารถมองลักษณะของปัญหาภายในอุปกรณ์ประกอบด้วย

- **การจัดการแบล็คแพลน** (Backplane Utilization)
  เป็นการจัดการเพื่อให้เกิดประโยชน์สูงสุด
- **หน่วยความจำ**
  การจัดการเนื้อที่ๆ ว่างเล็กที่ไม่สามารถนำมาใช้งานได้ (Fragmentation), Buffer Miss Rate, Buffer Utilization และ Free Memory
- Network Adapters
  กระตุ้นการทำงานของ Backup, Error ของระบบและ VLAN, Broadcase Rate, Collision Rate, Discard Rate, Flapping, Maximum Uptime, Queue Drop Rate และการใช้ประโยชน์
- Power Supplies
  มีระยะของ Voltage
- Processors
  ใช้ทรัพยากรให้เป็นประโยชน์
- SNMP Agent
  เมื่อไม่มีการตอบสนอง
- **ระบบ** (System)
  สามารถทำการ Restart ได้

- **อุณหภูมิ** (Temporary)
  มีการกำหนดค่าช่วงของอุณหภูมิ
- **การจัดการเกี่ยวกับพัดลม** (Fan)
  มีการแจ้งสถานะที่ผิดปกติของพัดลม

3.5.2.2 สิ่งที่รวบรวมไว้กับ CISCO Works2000

DFM ออกแบบให้ทำงานกับผลิตภัณฑ์ตระกูลของ CISCO Works2000 ส่วนประกอบของ DFM ที่รวบรวมไว้กับ CISCO Works2000 กล่าวคือ

- มี Device Fault Manager Folder ใหม่บน CISCO Works2000
- ใช้กระบวนการของ CISCO Works2000 Server และมีการจัดการ Backup
- นำเข้าอุปกรณ์ของ CISCO อัตโนมัติจาก Resource Manager Essentials (RME) หรือ ทั้งDFM และ RME

3.5.2.3 สิ่งที่รวบรวมไว้กับ Enterprise Management Systems

DFM สามารถใช้ได้เช่นเดียวกันกับ CISCO Fault Subsystems ทำให้เกิด Intelligent CISCO Traps ไปยังอุปกรณ์อื่นๆ และผู้ขายรายอื่นๆ ที่ได้ติดตั้งระบบการจัดการไว้ CISCO Network ทำงานได้เกือบใกล้เคียงกับแนวทางของ Enterprise Management Systems

3.5.2.4 รองรับกับอุปกรณ์ Layer 2 และ Layer 3

สามารถสนับสนุนอุปกรณ์ใหม่ของ CISCO ที่เพิ่มขึ้นในระบบเครือข่ายที่ Layer 2 และ Layer 3

3.5.2.5 เพิ่มอุปกรณ์ที่สามารถรองรับได้

อุปกรณ์ใหม่ของ CISCO ที่เพิ่มขึ้นในระบบเครือข่าย DFM สามารถทำการปรับปรุงแก้ไขได้อย่างง่ายดายโดยทำปรับปรุงแก้ไขอุปกรณ์ผ่านทาง CISCO Software เพื่อทำการวิเคราะห์และรายงานความผิดพลาดใน CISCO Network ลักษณะเฉพาะเมื่อมีการติดตั้งบนเซริฟเวอร์สามารถทำการตรวจสอบเครือข่ายได้ถึง 30000 CISCO ports ดังนั้นการใช้ประโยชน์ของ DFM (Device Fault Manager) สามารถใช้ใน LAN Management Solution เช่นเดียวกันกับที่เพิ่มไปในการติดตั้ง CISCO Works2000

3.5.3 CISCO Works2000 CISCO View 5.3

CISCO View Device Manager เป็นโปรแกรมประยุกต์ทางด้านการจัดการเกี่ยวกับอุปกรณ์ของ CISCO ได้แก่ Web-based, CISCO Works2000 CISCO View นั้นยอมให้ติดต่อกับทุกๆ ไคลเอนต์ (Clients) ตามมาตรฐานของเบราเซอร์เน็ทเวริค์ (Browser Network) และความต้องการทางด้านฮาร์ดแวร์น้อยที่สุดสำหรับผู้ใช้งานที่ต่อเนื่อง รวมทั้งสามารถไว้ใจได้ในการอินเทอเฟส (Interface) ในการเฝ้าดูอุปกรณ์แบบ Real-Time และง่ายต่อการกำหนดค่าบนอุปกรณ์ใน CISCO View ซึ่งเป็นฟังก์ชั่นหนึ่งที่เพิ่มขึ้นมาใช้งาน การใช้งานง่ายมากเมื่อมีการใช้ร่วมกับผลิตภัณฑ์ของ CISCO Works2000 CISCO View มีการจัดการอุปกรณ์แบบผู้ใช้หลายผู้ใช้ (Multi-Users) และคอยแก้ไขปัญหาในลักษณะของ End-to-End Management Intranet

CISCO View Web-based Management เป็นตัวช่วยจัดการเน็ทเวริค์ โดยสามารถทำการแสดงผลทางกายภาพของอุปกรณ์ CISCO และดูรหัสสี (Color Coding) ของพอร์ต เพื่อทำการตรวจสอบแต่ละสถานะของพอร์ตซึ่งทำให้ผู้ใช้เข้าข้อมูลได้รวดเร็วขึ้นและง่ายขึ้น รูปแบบของ CISCO View เป็นแบบไดนามิก (Dynamic) สามารถเฝ้าดูอุปกรณ์และค่าคอนฟิกได้

สำหรับผลิตภัณฑ์ของ CISCO Internetworking อันได้แก่ Routers, Switches และ Access Products สิ่งที่เพิ่มขึ้นได้แก่

- การเฝ้าติดตามของผลิตภัณฑ์ CISCO ในลักษณะของเว็บเบส (Web-based) ซึ่งผู้ดูแลระบบเน็ทเวิร์คสามารถตรวจสอบจาก ภายนอกโดยไม่ต้องดูจากอุปกรณ์จริงของแต่ละอุปกรณ์
- มีการปรับปรุงแก้ไขอย่างต่อเนื่องในแง่ของกายภาพของ Routers, Hubs, Switches หรือเซริฟ์เวอร์ที่ติดต่อกันในระบบเครือข่าย
- การเฝ้าติดตามผลแบบเรียลไทม์ (Real-Time) และแทรกกิ่ง (Tracking) ตามคีย์ข้อมูลและข้อมูลที่เกี่ยวข้องกับอุปกรณ์ที่ปฏิบัติการอยู่ ความหนาแน่นของการจราจรในระบบเครือข่าย และสภาพแวดล้อมโดยการวัดค่า ได้แก่ เปอร์เซนต์ที่ใช้ได้ เฟรมของการรับและส่ง ความผิดพลาดและตัวชี้วัดของอุปกรณ์
- สามารถติดต่อระหว่างอุปกรณ์ที่มีอยู่กับอุปกรณ์ CISCO ตัวใหม่ๆ ได้ โดยผ่านการสนับสนุนจากเว็บเบสแพ็คเกจ (Web-based Package Support Updater :PSU) ในเวอร์ชั่นใหม่ของ CISCO View
- สนับสนุนผู้ใช้หลายผู้ใช้ (Multi-Users) ในการติดต่อกับตัวเซริฟ์เวอร์ของ Single CISCO View ผ่านเว็บเบสของผู้ใช้ปลายทาง

3.5.3.1 **ลักษณะเด่นของ** CISCO View 5.3

ลักษณะเด่นของ CISCO View 5.3 ประกอบด้วย

- เว็บเบสแพ็คเกจ (Web-based Package Support Updater :PSU) เป็นตัวกำหนดและดูปริมาณอุปกรณ์ที่รองรับการดาว์นโหลดจาก CCO
- รายชื่ออุปกรณ์ที่นำเข้ามาเพื่อสามารถทำการโหลดข้อมูลได้รวดเร็วยิ่งขึ้น และติดต่อกับอุปกรณ์ได้หลังจากนั้น
- สามารถทำการปรับปรุงแก้ไขอุปกรณ์ระยะไกลของผู้ใช้และอุปกรณ์แพ็คเกจ (Device Packages) จากเวอร์ชั่นที่แล้ว
- ตัวชี้วัดความก้าวหน้า สนับสนุนการย้อนกลับเมื่อเกิดภาวะการรับงานที่เกินสถานะ
- มีการปรับปรุงประสิทธิภาพในตัวโปรแกรมแสดงผลการกำหนดค่าเมนู

3.5.3.2 **ข้อกำหนดพื้นฐานการจัดการ** (Common Management Foundation)

CISCO View 5.3 ใช้ส่วนประกอบมากมายใน CISCO Works2000 ในการจัดการพื้นฐานร่วมกัน ประโยชน์โดยรวมเหมาะกับ CISCO Works2000 Application ทั้งหมดที่ใช้ร่วมกับ Third-Party Network Management System (NMSs) สำหรับผู้ใช้ที่มีการออกแบบได้โดยอิสระ ดังต่อไปนี้

- รวมกันระหว่างแอ็บพิเคชั่นบนเซริฟ์เวอร์ที่มีระบบปฏิบัติการแตกต่างกัน
- ไดนามิกอัพเดทที่มีข้อมูลร่วมกันใน NMS
- สามารถอัพเกรดไดนามิคที่ NMS เวอร์ชั่นใหม่ โดยไม่ต้องมีการติดตั้งระบบใหม่ใน CISCO Works2000
- ความยืดหยุ่นในการจัดการสภาพแวดล้อมอินทราเนต โดยใช้เครื่องมือของเว็บเบสทั้งหมดจาก CISCO

หมายเหตุ NMS Supports คือการอัพเดทความถี่และแฟ้มข้อมูล ซึ่งสามารถดาวน์โหลดได้จาก CCO ที่เกี่ยวข้องกับ CISCO View Planner

ตาราง 3.5.3 แสดงอุปกรณ์ที่สามารถสนับสนุนการทำงาน

Access Servers	Catalyst Switchs	Routers	Others
Access AS5200	Catalyst 1900	Router 1400	Cisco 1538
Access AS5300	Catalyst 2820	Router 1600	Cisco 1548
Access AS5800	Catalyst 2900	Router 1700	FastHub 300
Access AS5350	Catalyst 2900XL	Router 2500	LightStream 1010
Access AS5400	Catalyst 2926	Router 2600	MicroHub 1516
	Catalyst 2948G	Router 3600	StackMaker
	Catalyst 2948GL3	Router 3800	Switch Addlets
	Catalyst 2980G	Router 4000	UBR 7200
	Catalyst 3500XL	Router 700	UBR 900
	Catalyst 4000	Router 7000	VPN 3000
	Catalyst 4840GL3	Router 800	IAD 2400
	Catalyst 4908GL3	Router 12000	Metro 1500
	Catalyst 5000		URM (1.0)
	Catalyst 5500		
	Catalyst 5505		
	Catalyst 5509		
	Catalyst 6000		
	Catalyst 6000IOS		
	Catalyst 8500		
	Catalyst 8510		
	Catalyst 8540		

3.5.4 CISCO Works2000 Content Flow Monitor 1.2

ในทางธุรกิจการขยายตัวของอินเทอร์เน็ตและอินทราเน็ต (Internet/ Intranet) และสามารถทำการค้นหาข้อมูลและการบริการผ่านเว็บ (Web) ความจำเป็นในการหาข้อมูลหรือเนื้อหาที่ง่ายขึ้นและรวดเร็วในการติดต่อกับเว็บเซริฟ์เวอร์ (Web Server) ทำให้ธรุกิจเกิดการขยายตัวและเพิ่มปริมาณในการส่งข้อมูลภายในองค์กรและภายนอกองค์กร ความต้องการริเริ่มการจัดการที่เหมาะสมของการจัดการส่งข้อมูลที่บรรจุในรูปแบบของแพ็คเกจผ่านระบบเครือข่าย (Content Delivery Network Management) กับอุปกรณ์จำพวกโหลดบาลานซิ่ง (Load Balancing) ที่ต่อเนื่อง

3.5.4.1 **ลักษณะทั่วไปของ** Content Flow Monitor

Content Flow Monitor คือเว็บเบสแบบ Real-Time Server Lead-Balancing กระทำในส่วนของการเฝ้าดูโปรแกรมที่ถูกออกแบบขึ้นมา สำหรับกิจการทางด้านเว็บโฮสติ่ง (Web Hosting) ที่จำเป็นในการเฝ้าดูและบริหารอุปกรณ์ Content Delivery ได้แก่ CISCO Local Director หรือ Catalyst 4840G สิ่งสำคัญในการส่งไปยังตัววิเคราะห์แบบประยุกต์และบริการเฝ้าดู Content Flow ทำให้ผู้ดูแลเน็ตเวิร์คได้เข้าใจถึงระบบปฏิบัติการขององค์ประกอบใน CISCO ทำให้การตัดสินใจของเซริฟ์เวอร์ Load Balancing มีความเที่ยงตรงและรวดเร็วมากที่จะเปลี่ยนการไหลหรือการใช้ Patterns Content Flow Monitors คือส่วนของ LAN Management Solution ที่เสนอไปยังตระกูล CISCO Works2000 ของ Network Management Products

3.5.4.2 **โครงสร้างสถาปัตยกรรมของ** Content Flow

องค์ประกอบสำหรับเซริฟ์เวอร์ Load-Balancing ที่ได้รับการจัดการภายในโครงสร้างสถาปัตยกรรม Content Flow ดังนี้

- **เอเจนต์ของโฟลเมเนจเมนท์** (Flow Management Agents: FMA)
  Flow Management Agent (FMA) คือศูนย์กลางองค์ประกอบของเซริฟ์เวอร์โหลดบาลานซิ่ง (Server Load Balancing) ทำการตัดสินใจในการทำบาลานซิ่ง ความสามารถของเซริฟ์เวอร์และลำดับขั้นการกระจาย

โหลด FMA ปกติ ทำงานใน CISCO Local Director หรือ Catalyst 4840g Chassis

- **เอเจนต์ของโฟลดีลิเวอร์ลี่** (Flow Delivery Agents: FDA)
  Flow Delivery Agent (FDA) คือแพ็คเกจแบบเปลี่ยนทางใหม่ (Redirect) ที่ส่งพื้นฐานของแพ็คเกจโดยใช้คำสั่งจาก FMA, FDA ปกติทำงานที่ CISCO IOS Routers ได้แก่ CISCO 7200, 8500 และ3600 Routers

- **เรียลเซริฟ์เวอร์** (Real Servers)
  เรียลเซริฟ์เวอร์เป็นแพล็ทฟอร์มที่หลากหลายในการส่งการบริการที่แท้จริงและแอ็พพิเคชั่นที่ผู้ใช้ต้องการจัดการ

- **เวอร์ชวลเซริฟ์เวอร์** (Virtual Servers)
  เวอร์ชวลเซริฟ์เวอร์ คือลักษณะของเอ็นทิตี้ที่แสดงให้เห็นถึงฟอร์มเซริฟ์เวอร์ (Form Server) และซิงเกอร์เซริฟ์เวอร์ (Single Server)

สถาปัตยกรรมของ Content Flow นิยามได้ว่าเป็นการทำงานร่วมกันระหว่าง FMA กับ FDA และเป็นฐานข้อมูลในการให้บริการระบบเน็ทเวิร์คอัจฉริยะ แบบกระจาย (Distributed-Intelligent Networking Service) สถาปัตยกรรมแบบนี้เป็นการกระจายการทำงานแบบโหลดบาลานซิ่ง (Load-Balancing Function) ผ่านอุปกรณ์มัลติคอนเท็นดิลิเวอร์ลี่ (Multi-Content Delivery) สำหรับเวอร์ชวลเซริฟ์เวอร์การเฝ้าดู Content Flow เป็นการก้าวหน้าอีกขั้นหนึ่งของสถาปัตยกรรมของ CISCO Content Flow ซึ่งเป็นอุปกรณ์ที่สถานะสมบรูณ์บริการที่ใช้ง่าย รายละเอียดอุปกรณ์ที่ถูกกำหนดค่าคอนฟิกคงที่และแบบเรียลไทม์ เริ่มจากเบราเซอร์ของ Content Flow Monitor โดยมีการกำหนดขอบเขตของระบบเครือข่ายที่ทำการวิเคราะห์ การเฝ้าดู Content Flow ถูกออกแบบในลักษณะของโปรแกรมเว็บเบสที่สนับสนุนการทำงานของไคลแอนท์เซริฟ์เวอร์ ดังนั้นสถาปัตยกรรมของ Content Flow สามารถแบ่งได้ 2 ส่วน กล่าวคือ

- **Content Flow Monitor Server**

  เป็นการติดตั้ง CISCO Works2000 บนเซิร์ฟเวอร์ โปรโตคอลที่ใช้เป็นแบบ SNMP ส่วนประกอบสถาปัตยกรรม Content Flow ที่สัมพันธ์กัน ประกอบด้วย FMA, FDAs, Real Server และ Virtual Server รวมทั้งคุณลักษณะของการกำหนดค่าคงที่ของอุปกรณ์ Content Delivery และลักษณะของเรียลไทม์ (Real-Time) ได้แก่ หมายเลขทั้งหมดของ Flows และ Cache Entries ต่อ FDA หมายเลขทั้งหมดของการเชื่อมต่อและเวอร์ชวลเซริฟ์เวอร์ (Virtual Server) เป็นต้น

  สำหรับการทำงานในส่วนของ Local Directory Content Flow Monitor Server มีการแสดงผลในลักษณะของกราฟิกหรือที่เรียกว่ากุยอี้โหมด (GUI: Graphic User Interface) ผ่านตัวเว็บเบสของ CISCO Works2000 บนเดสทอป โดยสามารถทำการเซตอัพอินเตอร์เฟสทั้งนี้เพื่อเพิ่ม ลด หรือแก้ไข FDA และ FMA สำหรับค้นหาส่วนประกอบของ Content Flow และสามารถกำหนดรายละเอียดในส่วนของโพลระหว่าง FDA และ FMA

- **Content Flow Monitor Client**

  เป็นการใช้เครื่องของจาวาแอ็พเพลท (Java Applet) โดยทำการเชื่อมโยงระบบจาก Common CISCO Works2000 Desktop ผ่านตัวบราวเซอร์ (Browser Interface) สามารถทำให้ผู้ใช้เก็บข้อมูลของผู้ใช้กับข้อมูลในส่วนของวิกฤตและข้อมูลทางสถิติ ได้แก่ Content Flow Element

  องค์ประกอบของ Content Flow Monitor Client ประกอบด้วย

  - ค่าสถิติที่แสดงในลักษณะของกราฟิกแบบเรียลไทม์ (Real-Time Statistic Graphic) ได้แก่ หมายเลขของการเชื่อมโยงของการนับแพ็คเกจ (Packet Count) ไปยังเวอร์ชวลเซริฟ์เวอร์ (Virtual Server) และเรียลเซริฟ์เวอร์ (Real Server)
  - เพื่อเฝ้าดูการกระจายการจราจรของการส่งข้อมูลแบบเรียลไทม์ (Real-Time Traffic Distribution Monitoring) ระหว่างเรียลเซริฟ์เวอร์ (Real Server) สำหรับทุกๆ เวอร์ชวลเซริฟ์เวอร์ (Virtual Server)
  - สรุปสถานะของอุปกรณ์ที่สมบรูณ์และการบริการที่หาได้ง่ายในการส่งข้อมูลผ่านระบบเครือข่าย (Content Delivery Network)

- รายละเอียดคุณลักษณะของการกำหนดค่าอุปกรณ์ Content Delivery และสถิติทางด้านการให้บริการ
- On-demand Update ของคุณลักษณะการกำหนดค่าและสถิติสำหรับทุกๆ Content Delivery

Content Flow Monitor รองรับสถาปัตยกรรมทั้งหมดของระบบเครือข่าย CISCO Contents Delivery ทั้งหมดและการออกแบบ ได้แก่ ลำดับการต่อเชื่อมของ Integrated CISCO IOS Server Load Balancing: ISLB), Accelerated Server Load Balancing: ASLB), Standalone Local Director และ Multimode Local Balancing:MNLB)

Catalyst 4840G เป็นสวิทช์เลเยอร์ของ Integrated server Load Balancing จำนวน 3 สวิทช์ (Switch) ที่ใช้เทคโนโลยีของ Catalyst 8500 ด้วยความเร็ว 10/100 Mbps จำนวน 40 พอร์ตกับ 2 GB Uplink ส่วน CISCO ISO (ISLB) ทำงานที่ Wire Speed Catalyst 4840g รองรับการเชื่อมต่อ 30,000 คอนเน็กชั่นเปอร์วินาที ทำให้ใช้ได้พร้อมกันถึง 24,000 คอนเน็กชั่น

CISCO Catalyst 6000 รองรับการทำงานของ CISCO ISO Server Load Balancing และ Multilayer Switch Feature Card: MSFC) รวมทั้งสามารถรองรับการทำงานของ ASLB โดยใช้ External Local Director ตาม FMA ดังนั้นการทำงานของ CISCO Catalyst 6000 จึงจัดว่าเป็น FDA ในการกำหนดค่ากับ Wire Speed Switching และส่งข้อมูลได้ถึง 15 Mbps

CISCO Local Director เป็นการแก้ปัญหาแบบเบ็ดเสร็จ ทั้งนี้ขึ้นกับการติดตั้งและบริหารจัดการกับลักษณะเด่นของ Advance Load Balancing ได้แก่ Secure Socket Layer: SSL) และสภาพการ Fail-Over ดังนั้น CISCO Local Director จัดว่าเป็น Local Load Balancing และรองรับการส่งผ่านข้อมูลได้ถึง 240 เมกกะบิท (Mbps) และ 18,000 คอนเน็กชั่นเปอร์วินาที (Connection/Second)

MNLB เป็นอีกทางเลือกหนึ่งของทำการ Load Balancing กับ Multiple Load Balancing Device ทำงานในลักษณะของเว็บแอ็พพิเคชั่น เพื่อให้สามารถ

ทำงานได้ประสิทธิภาพสูงสุดในการใช้งานและสามารถขยายงานได้สูงสุด

ดังนั้นเซริฟ์เวอร์ของ Content Flow Monitor ถูกติดตั้งใน CISCO Works2000 Management Server ได้แก่ ผลิตภัณฑ์อื่นๆ ในตระกูลของ CISCO Works2000 ในส่วนของ LAN Management Solution ง่ายในการจัดการแบบ Integrated Management Solution, Web-based Interface และง่ายต่อการแบ่งปันการใช้งานของทรัพยากร การวิเคราะห์ในการตัดสินใจการติดต่อเชื่อมโยงหรือความรวดเร็วในการประเมินในการปรับสวิทซ์และแก้ไขเปลี่ยนแปลงลิงค์ (Link) ดังนั้น Content Flow Monitor เป็นการขยายการออกแบบของอุปกรณ์ในส่วนของ CISCO Works2000 LAN Management Solution

3.5.5 CISCO Works2000 Resource Manager Essentials 3.3 (RME)

Resource Manager Essentials 3.3 (RME) มีการจัดการกับระบบเครือข่ายที่ง่ายและมีการแก้ไขฟังก์ชั่นการทำงานใหม่ให้ดีขึ้น สำหรับการจัดการเกี่ยวกับสวิทซ์ (Switch) การให้บริการการค้นหา (Access Service) เราว์เตอร์ (Router) ของ CISCO ที่เกี่ยวข้องกับการแก้ไขปัญหาการบริหารงานของแลน (LAN Management Solution), การแก้ไขปัญหาการบริหารงานของเส้นทางแวน (Routed WAN Management Solution) รวมทั้งสามารถใช้ได้กับเครื่องของฮิวเล็ทแพ็ทการ์ด (HP-UX) และของไอบีเอ็ม (AIX)

3.5.5.1 ลักษณะการทำงานของ RME 3.3

ลักษณะการทำงานของ RME 3.3 ประกอบด้วย

- ตรวจสอบและรายงานด้านฮาร์ดแวร์ โครงสร้างและรายการอื่นๆ ที่มีการเปลี่ยนแปลง
- สามารถจัดการและจัดโครงสร้างที่เปลี่ยนแปลงได้อย่างเหมาะสมและแก้ไขปรับปรุงซอร์ฟแวร์ไปยังอุปกรณ์ต่างๆ ได้
- ง่ายต่อการตรวจสอบและแก้ไขปัญหาทรัพยากรของแลน (LAN) และแวน (WAN)

- Virtual Provide Network (VPN) Management Solution เป็นจุดรวมพื้นฐานของการบริหารแบบ VPN ซึ่งการบริหารแบบ VPN เป็นการจัดรวบรวมงานพื้นฐานการจัดการ VPN กล่าวคือการกำหนดชุดของอุปกรณ์ VPN ทำให้สามารถกำหนดปัญหาเกี่ยวกับตัวจัดการบริหารระบบเครือข่ายของ VPN ซึ่งตัวจัดการบริหารระบบเครือข่ายของ VPN สามารถแบ่งได้ 3 ลักษณะกล่าวคือ

    - **ทางด้านโครงสร้าง**

      ผู้ใช้สามารถเปรียบเทียบหรือเทียบโครงสร้างของอุปกรณ์ VPN ได้อย่างรวดเร็ว และสามารถทำการค้นหาอุปกรณ์ VPN ที่เพิ่มขึ้นในระบบเครือข่าย

    - **ทางด้านรายการอุปกรณ์**

      ผู้ใช้สอบถามด้านระบบเพื่อกำหนดอุปกรณ์ VPN ประกอบด้วยโมดูลของการเข้ารหัสของฮาร์ดแวร์ (Hardware Encryption Modules) อุปกรณ์ของ CISCO ต้องการรุ่นที่ถูกต้องผู้ใช้สามารถทำรายการเพื่อกำหนดอุปกรณ์ในฐานข้อมูลของ Inventory Manager เมื่อต้องการแก้ไขอุปกรณ์ในระบบเครือข่าย VPN

    - **ทางด้านผู้บริหารเครือข่าย**

      สามารถแยกปัญหาของ VPN ในลักษณะของการทำรายงานการตรวจสอบความผิดพลาดของการเข้ารหัสของฮาร์ดแวร์ (Hardware Encryption), Internet Key Exchange (IKE), Certificate สรุปผลและตรวจสอบการพยายามบุกรุกในลักษณะรายงานของ Packet Relay

3.5.5.2 **โปรแกรมบริหารเครือข่าย** RME 3.3

โปรแกรมบริหารเครือข่าย RME 3.3 ประกอบด้วย

- Inventory Manager

  เป็นการจัดการเกี่ยวกับฐานข้อมูลรายการอุปกรณ์ของ CISCO ให้ทันสมัย ในตระกูลของ CISCO 7000 series, ISDN Router, Switch ตระกูล IGX, BPX และ MGX โดยที่ตัวฐานข้อมูลของอินเว็นทอรี่ (Inventory Database) ทำการจัดการข้อมูลเกี่ยวกับรายละเอียดและคุณสมบัติของอุปกรณ์ ได้แก่ ชนิดของโครงสร้าง ส่วนของการติดต่อ เวอร์ชั่นของซอร์ฟแวร์ หน่วยความจำ ลักษณะเฉพาะของเฟล็ซ (Flash) และอื่นๆ

  ลักษณะการทำงานและข้อกำหนดของ Inventory Manager มีดังนี้

  - ทำการปรับปรุงข้อมูลให้ทันสมัย ในส่วนที่เกี่ยวกับรายการอุปกรณ์ต่างๆ ของ CISCO ทั้งหมดในระบบเครือข่าย ซึ่งประกอบด้วย CISCO Call Manager, VPN 3000 Concentrator (VPNc3000), IGX, BPX และ MGX
  - สรุปข้อมูลของฮาร์ดแวร์และซอร์ฟแวร์ เช่นเดียวกันกับรายงานในกลุ่มอุปกรณ์ ซึ่งประกอบด้วยชนิดของโครงสร้าง ส่วนของการติดต่อ เวอร์ชั่นของซอร์ฟแวร์ หน่วยความจำ ลักษณะเฉพาะของเฟล็ซ (Flash) และรายละเอียดลักษณะอื่นๆ ของฮาร์ดแวร์และซอร์ฟแวร์
  - อุปกรณ์นำเข้าของ CISCO WAN Manager เช่นเดียวกันกับ CWSI Campus 2.x, Campus Manager 3.0, HP Openview, Tivoli Net View และอื่นๆ
  - ปริมาณความหนาแน่นของข้อมูลถือจากจำนวนทั้งหมดของสล็อท (Slots) ทั้งที่ใช้งานและไม่ได้ใช้งาน
  - รายงานเกี่ยวกับ Multiservice Port บนจำนวนและตำแหน่งของ Catalyst Switches
  - การรองรับอุปกรณ์ที่สามารถแลกเปลี่ยนได้จาก XML กับโปรแกรมการจัดการอื่นๆ
  - สามารถทำการเลือก VPN เช่น กลุ่มของอุปกรณ์สำหรับทำรายงาน

3.5.5.3 Device Configuration Manager

เป็นการจัดการบำรุงรักษาให้อุปกรณ์สามารถดำเนินการต่อไปได้ และจัดการปรับปรุงโครงสร้างระหว่างเราว์เตอร์และสวิทซ์ของ CISCO การจัดการกำหนดค่าและการเฝ้าดูการเปลี่ยนแปลงของโครงสร้างในระบบเครือข่าย รวมทั้งสามารถทำการแก้ไขเมื่อตรวจพบการเปลี่ยนแปลงและบันทึกข้อมูลไปยังการให้บริการตรวจสอบความเปลี่ยนแปลง (Change Audit Service) ในส่วนของการติดต่อกับผู้ใช้สามารถสอบถามเอกสารหรือบันทึกลักษณะการกำหนดค่าต่างๆ คุณสมบัติ และเปรียบเทียบ เพื่อสะดวกในการแยกแยะความเหมือนหรือต่างกัน RME 3.3 ประกอบด้วยอิดิเตอร์ของโปรแกรมอยู่ในรูปแบบของเว็บที่สามารถทำการตรวจสอบการบันทึกที่มีการแก้ไขหรือเปลี่ยนแปลง อิดิเตอร์สามารถสืบค้น แทนที่ คัดลอก ตัด เปรียบเทียบและเปลี่ยนแปลงรายละเอียดของข้อมูล

ลักษณะการทำงานและข้อกำหนดของ Device Configuration Manager มีดังนี้

- จัดการบันทึกข้อมูลให้ทันสมัยโดยอัตโนมัติและเก็บไปยังแฟ้มข้อมูลของการกำหนดค่า (Configuration File)
- การแก้ไขในรูปแบบของเว็บ ทำให้สะดวกในการแก้ไขและดาวน์โหลดการกำหนดค่าที่มีการแก้ไข
- ยอมให้มีการเปลี่ยนแปลงการกำหนดค่า เมื่อมีความผิดพลาดเกิดขึ้นที่เราว์เตอร์หรือสวิทซ์ในระบบเครือข่าย
- จัดเตรียมในรูปแบบของวิทซาร์ด (Wizard) ทำให้สะดวกในการใช้งานและลดความยุ่งยาก
- CISCO ได้จัดกระบวนการเปลี่ยนแปลงการกำหนดค่าแบบง่ายในการติดต่อกับ SNMP, Terminal Access Controller Access Control System (TACACS), Enable, Syslog, SNMP Trap Destination, CISCO Discovery Protocal (CDP), DNS และอื่นๆ

- ง่ายในการใช้งานในลักษณะของคอมมานไลน์ (Command Line) ในการกำหนดสิทธิ์ของผู้ใช้หรือกลุ่มของผู้ใช้
- รองรับไฟล์ที่เก็บการกำหนดค่า เพื่อใช้ในการกำหนดโครงสร้างลักษณะของอุปกรณ์และโครงสร้างของคุณสมบัติ
- ส่วนติดต่อแสดงคำสั่งเพื่อใช้ในการทำงานประมวลผลกลุ่มของอุปกรณ์ที่ผิดพลาดคล้ายกับเป็นตารางการปฏิบัติงาน
- สามารถแยกแยะและดูอุปกรณ์ VPN และการกำหนดค่าของ PIX Firewall

3.5.5.4 Software Image Manager

เป็นการจัดการในการแก้ไขเราน์เตอร์และสวิทซ์ของ CISCO ผ่านตัววิทซาด ทำให้ง่ายและเหมาะสมต่อการใช้งาน รวมทั้งสามารถทำการสร้างในรูปแบบของตาราง การดาวน์โหลด และการตรวจสอบก่อนทำการแก้ไขรายการควรมีการพิจารณาข้อมูลที่ผิดพลาดของเราน์เตอร์และสวิทซ์ เพื่อทำการแก้ไขข้อผิดพลาดได้สำเร็จ

เมื่ออุปกรณ์เริ่มมีการแก้ไข Software Image Manager มีการดาวน์โหลดงานพร้อมกันและยอมให้ผู้ใช้งานตรวจสอบการเพิ่มขึ้นของงาน ตารางงานเป็นตัวควบคุมไปยังกระบวนการ Signoff สามารถกำหนดสิทธิ์ก่อนที่ทำการแก้ไข (Upgrade) แต่ละงาน RME 3.3 สามารถวิเคราะห์การอัพเกรดของซอร์ฟแวร์ในรูปแบบของ IGX, BPX และ MGX ทำให้ง่ายและลดผลกระทบในการกำหนดการอัพเกรดของซอร์ฟแวร์

ลักษณะการทำงานและข้อกำหนดของ Software Image Manager มีดังนี้

- จัดการวิเคราะห์รายงานการอัพเกรดซอร์ฟแวร์ โดยทำการแสดงสิ่งที่จำเป็นและผลกระทบต่อการแก้ไข

- ลดระยะเวลาให้เหมาะสมในการทำงานของเราน์เตอร์หรือ Switch Software Images
- ใช้บังคับงานสองระดับยอมให้มีการแก้ไขงาน ทำให้มีการยอมรับหรือตรวจสอบก่อนนำไปประมวลผล
- ทำการตรวจสอบ Image Software ในระบบเครือข่ายและ Software Library ให้สอดคล้องและสัมพันธ์กัน
- ใช้ CCO รายงานข้อบกพร่องของซอร์ฟแวร์ที่กระทบต่ออุปกรณ์ในระบบเครือข่าย
- จำกัดเว็บพร็อกซี่ (Web Proxy) ในการติดต่อกับ CCO ได้ดียิ่งขึ้น
- จัดการวิเคราะห์การอัพเกรดซอร์ฟแวร์ในรูปแบบของ IGX, BPX และ MGX

3.5.5.5 Change Audit Service

เป็นการแสดงรายการสรุปซอร์ฟแวร์และฮาร์ดแวร์ รวมทั้งการเปลี่ยนแปลงโครงสร้าง ในการสรุปข้อมูลในรูปแบบที่ง่ายในการแสดงประเภทของการเปลี่ยนแปลง โดยทำการเปลี่ยนแปลงจาก Telnet หรือ Control CLI หรือจากโปรแกรมของ CISCO Works2000 ในการแสดงลักษณะของการเปลี่ยนแปลงไปยังรายละเอียดของการรายงาน ได้แก่ การเพิ่มหรือลดคาร์ด เปลี่ยนหน่วยความจำ เปลี่ยนโครงสร้างและอื่นๆ

ลักษณะการทำงานและข้อกำหนดของ Change Audit Service มีดังนี้

- จัดการรวบรวมการตรวจสอบการเปลี่ยนแปลงที่เกิดขึ้นในระบบเครือข่าย โดยนำเสนอในรูปแบบรายงานตามลำดับของวันเดือนปี
- เสนอรายงานการเปลี่ยนแปลงโดยใช้เกณฑ์ที่ง่ายหรือซับซ้อน
- การเปลี่ยนแปลงระบบเครือข่ายทำระหว่างเวลาตรวจสอบระบบเครือข่าย

3.5.5.6 Availability Manager

ตัว “Reachability Dashboard” สามารถกำหนดสถานะการวิเคราะห์เราน์เตอร์และสวิทช์ให้สามารถทำการตรวจสอบได้ง่าย โดยสามารถเฉพาะเจาะจงลงไปที่อุปกรณ์เพื่อดูรายละเอียดเกี่ยวกับเวลาการตอบสนอง การใช้งาน การรีโหลด โปรโตคอล และสถานะการเชื่อมต่อ

ลักษณะการทำงานและข้อกำหนดของ Availablility Manager มีดังนี้

- สรุปรายงานการวิเคราะห์อุปกรณ์ไปถึงการออฟไลน์ (Offline) และการรีโหลด (Reload)
- เสนอรายงานในรูปแบบของกราฟิกของแนวทางในการใช้เวลาการตอบสนองของอุปกรณ์
- รายงานสถานะของเราน์เตอร์และสวิทช์
- จัดการเชื่อมต่อไปยัง CCOs Stack Decoder เพื่อทำการแก้ไขปัญหาข้อผิดพลาด
- แสดงรูปของโปรโตคอลที่อุปกรณ์สามารถทำการตอบสนองไปยังเครื่องมือเชื่อมต่อ ได้แก่ UDP,TCP, HTTP, SNMP เป็นต้น

3.5.5.7 Syslog Analyzer

เป็นตัวแยกสภาวะความผิดพลาดของระบบเครือข่ายและแนะนำสาเหตุของปัญหาที่เกิดขึ้น โดยที่ซีสล็อกแอนนาไลเซอร์ (Syslog Analyzer) ทำหน้าที่กรองข้อความที่ล็อกโดยเราน์เตอร์ (Router) สวิทช์ (Switch) การเข้าถึงเซริฟ์เวอร์ (Access Server) ของ CISCO และ CISCO IOS Firewalls รวมทั้งยอมให้ข้อความที่ได้เชื่อมโยงไปยังข้อมูลคล้ายกับเว็บเบส (Web-based) หรือ Common Gateway Interface (CGI) Script ดังนั้นเทคโนโลยีของ CISCO IOS เป็นตัวจัดการรายละเอียดข้อมูลของอุปกรณ์เสนอในรูปแบบที่ชัดเจน

ลักษณะการทำงานและข้อกำหนดของ Syslog Analyzer มีดังนี้

- สามารถแสดงรูปแบบผิดพลาดตลอดเวลา ทำให้สามารถทำการแก้ไขปัญหาได้อย่างรวดเร็ว
- สรุปเหตุการณ์ที่เกิดขึ้น โดยการกวดขันหรือผู้ใช้มีเกณฑ์สำหรับเราน์เตอร์ (Router) สวิทช์ (Switch) และ CISCO IOS และ PIX Firewalls
- ยอมให้ข้อความที่ต้องการส่งไปยัง RMB Server
- แยกข้อความที่ไม่ต้องการ
- แจ้งให้ผู้ใช้ทราบถึงสคริป (Script) หรือเชื่อมโยงไปยังเว็บเพจ (Web Page)

3.5.5.8 CISCO Management Connection

เป็นตัวจัดการบริหารการเชื่อมโยงของ CISCO ไปยังโปรแกรมการจัดการ (Application Management) รวมทั้งเป็นเครื่องมือสำหรับการรวบรวมโปรแกรมโดยใช้มาตรฐานรูปแบบและเทคโนโลยีของอินเทอร์เน็ต (Internet) ทำให้ผู้ใช้สามารถเชื่อมโยงไปที่โปรแกรมการจัดการเว็บเบสไปยัง CISCO Works2000 และยอมให้ผู้พัฒนาโปรแกรมเชื่อมต่อไปยังโปรแกรมของเว็บเบสหรือตัวจัดการบริหารการเชื่อมโยงของ CISCO (CISCO Management Connection)

ลักษณะการทำงานและข้อกำหนดของ Syslog Management Connection มีดังนี้

- เชื่อมไปยัง CISCO Works2000 ด้วยโปรแกรมประยุกต์ผ่านตัวจัดการบริหารการเชื่อมโยงของ CISCO (CISCO Management Connection)
- เชื่อมไปยัง CISCO Works2000 ด้วยโปรแกรมประยุกต์ผ่านเว็บเบสอื่นๆ จาก CISCO (Web-based)
- เพิ่มประสิทธิภาพด้วยการรวมกับโปรแกรมที่เป็นผู้นำทางด้านระบบเครือข่าย

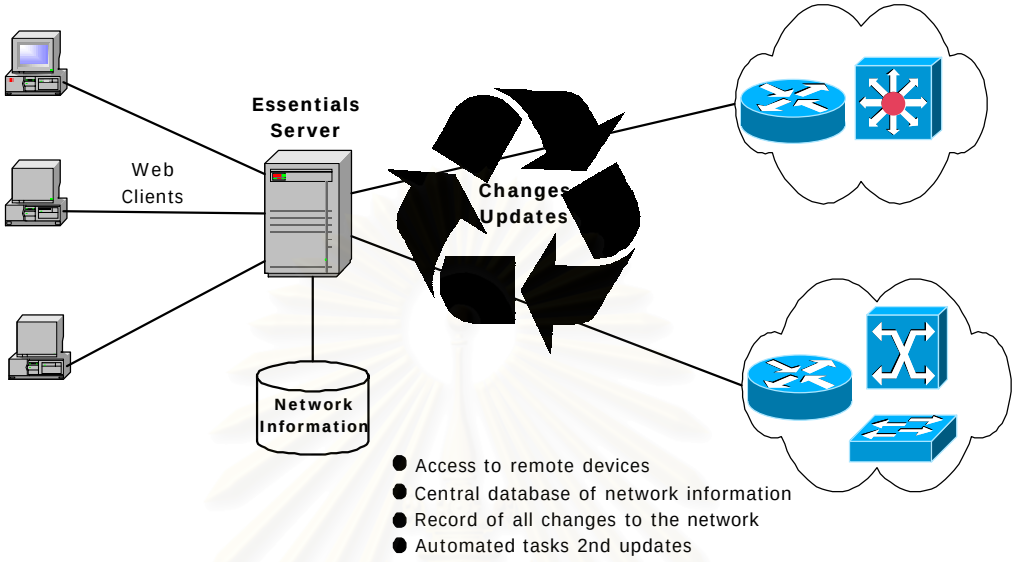
3.5.5.9 Integrated Access to CISCO Connection Online (CCO)

Resource Manager Essentials ช่วยในการปรับจูนระบบเครือข่ายให้สามารถเข้าถึงระดับสูงสุดของการบริหารระบบเครือข่าย RME จัดเตรียมโปรแกรมใหม่ๆ สำหรับการเข้าถึง CCO ทำให้ง่ายต่อการทำงานค้นหาผลิตภัณฑ์ล่าสุดที่ทำการเพิ่มเข้า ทำการวิเคราะห์และตรวจหาข้อบกพร่องของข้อมูล

เมื่อมีการเชื่อมโยงไปยัง CCO, RME อนุญาตให้มีการรายงานปัญหา TAC, ตรวจสอบ SMARTnet™, การเปลี่ยนสถานะของเราน์เตอร์ใหม่, การหาข้อผิดพลาดบน CISCO IOS/ Catalyst Releases,วางแผนความจุบนพื้นฐานของ CCO

3.6 ขั้นตอนการทำงานของโปรแกรมจัดการเครือข่ายและซอร์ฟแวร์ปัจจุบัน

วิธีการแก้ไขปัญหาการจัดการระบบแลน (LAN Management Solution : LMS) เป็นโมดูลที่ทำงานภายใต้ CISCO Works 2000 เป็นเว็บเทคโนโลยี โดยมีโมดูลที่จัดการในส่วนของเซริฟ์เวอร์ของ CISCO Works 2000 / CMF, CISCO View, Integration Utility และในการปฏิบัติงานของแอลเอ็มเอส (LMS) ผู้ใช้จะทำการติดต่อไปยังเซริฟ์เวอร์แต่จะไม่มีการติดต่อตรงไปยังอุปกรณ์ปลายทางดังแสดงในรูปที่ 3.3 เพราะฉะนั้นในบางกรณีอาจจะได้ข้อมูลที่ไม่ทันสมัยเนื่องจากต้องรอรอบของการทำพอลลิ่ง (Polling) และในการเข้าปฏิบัติงานของผู้ใช้ต้องระบุไปยังพอร์ตของเซริฟ์เวอร์ ซึ่งในกรณีนี้ใช้พอร์ตที่ 1741 โดยระบุเว็บแอสเดรส ดังนี้ htty:xxxxxxxxx:1741 โดยที่ xxxxxxxx เป็นการระบุไปยังเซริฟ์เวอร์

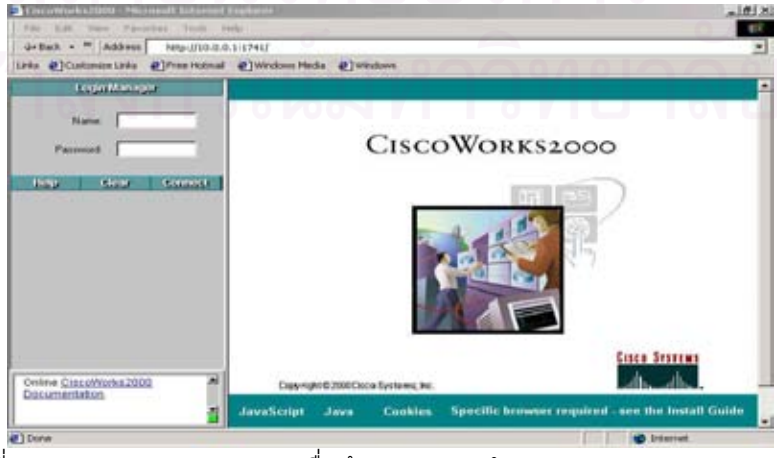


รูปที่ 3.6 แสดงการเชื่อมโยงของแอลเอ็มเอส (LAN Management Solution : LMS)

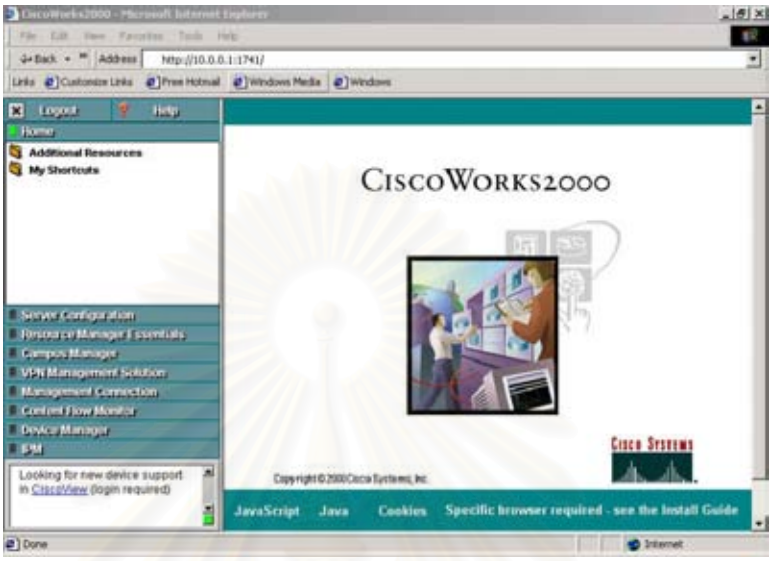
3.7 ขั้นตอนการเข้าถึงระบบของโปรแกรมจัดการเครือข่าย CISCO Works 2000

3.7.1 การเข้าถึงระบบการจัดการเครือข่าย

เปิดโปรแกรมการจัดการเครือข่าย CISCO Works 2000 LMS บนเครื่องคอมพิวเตอร์ต่ออยู่กับระบบ โดยทำการเปิดบราว์เซอร์ (Browser) และใส่ IP Address ของเครื่องซันเซิร์ฟเวอร์ (SUN server) แล้วตามด้วยพอร์ต (Port) 1741 ดังแสดงในรูปที่ 3.7.1 และรูปที่ 3.7.2



รูปที่ 3.7.1 แสดงลักษณะจอภาพเพื่อเข้าสู่ระบบการทำงานของ CISCO Works 2000



รูปที่ 3.7.2 แสดงลักษณะจอภาพภายหลังการเข้าสู่ระบบการทำงานของ CISCO Works 2000

จากรูปที่ 3.7.1 ระบบจะให้ระบุชื่อ (Username) และรหัสผ่าน (Password) ซึ่งถูกระบุไว้แล้วโดยผู้บริหารระบบและได้กำหนดถึงความสามารถเข้าถึงระบบของแต่ละคนได้ว่า มีความสามารถได้มากน้อยเพียงใดโดยสามารถดูรายละเอียดต่างๆ ของการเข้าสู่ระบบได้จากรายงานสิทธิ์การใช้งาน (Permission Report) โดยมีขั้นตอนการใช้งาน ดังนี้

3.7.1.1 เข้าสู่หน้าจอหลักของ Server Configuration แล้วทำการเลือก Setup Folder

3.7.1.2 เลือก Security>Permission Report ลักษณะของรายงานแสดงได้ดังรูปที่ 3.7.1.3

รูปที่ 3.7.1.3 แสดงลักษณะรายงานสิทธิ์การใช้งาน (Permission Report)

โดยที่รายงานสิทธิ์การใช้งาน (Permission Report) จะกำหนดความสามารถของแต่ละผู้ใช้ว่าอยู่ในระดับอะไร เช่น ผู้ดูแลระบบ (System Administrator), ผู้ดูแลระบบเครือข่าย (เครือข่าย Administrator), ผู้ปฏิบัติการเครือข่าย (เครือข่าย Operator) หรืออื่นๆ ซึ่งลักษณะหน้าจอหลักที่ปรากฏหลังจากที่ระบุชื่อและรหัสผ่านที่ถูกต้องแล้วจะปรากฏขึ้นตามสิทธิ์การใช้งานที่ถูกกำหนดไว้ ซึ่งลักษณะหน้าจอหลักที่สามารถใช้งานได้แสดงดังรูปที่ 3.7.1.2 โดยมีการกำหนดค่าการเข้าถึงข้อมูลและความสามารถในการประมวลผลระบบเครือข่ายของผู้ใช้ดังกล่าว ซึ่งเป็นส่วนหนึ่งของการระบุการรักษาความปลอดภัยของระบบเครือข่ายที่ระบบบริหารการจัดการมีการกำหนดให้แล้ว

3.7.2 อธิบายลักษณะหน้าจอภาพหลักและการทำงานของระบบจัดการเครือข่าย

จากรูปที่ 3.7.1.2 จะปรากฏลักษณะของจอภาพหลัก โดยแบ่งเป็น 2 ส่วนหลักๆ คือ ส่วนทางด้านซ้ายมือเป็นส่วนของคำสั่ง และส่วนทางด้านขวามือเป็นส่วนการแสดงผล ในส่วนทางด้านซ้ายมือของหน้าจอประกอบด้วย บรรทัดแรกการให้ออกจากระบบ โดย Logout และ Help เป็นส่วนที่เป็นคำอธิบายการใช้งานในส่วนที่เคอเซอร์ (Cursor) ชี้อยู่ ส่วนบรรทัดที่สองเป็น Home เป็นส่วนของผู้ใช้สำหรับใช้งาน คือ Additional Resources เป็นที่สำหรับเก็บเอกสารต่างๆ และในส่วนที่ของสนับสนุนการให้บริการ ตลอดจนติดต่อกับ CISCO's Home Page และ My Shortcuts เป็นส่วนที่เก็บเมนูย่อยของผู้ใช้งานแต่ละคนที่ใช้อยู่เป็นประจำหรือใช้บ่อยๆ ซึ่งในการออกแบบวิธีการเฝ้าติดตามและวิธีการแก้ไขปัญหาการทำงานของแลนใช้ส่วนนี้ในการเก็บเมนูที่ออกแบบ

ส่วนถัดมาเป็นส่วนของโปรแกรมย่อยที่แยกหน้าที่การทำงาน และในส่วนล่างสุดของส่วนซ้ายมือเป็นข่าวสารต่างๆ ที่รับจาก CISCO Works 2000 ซึ่งปรากฏขึ้นเปลี่ยนแปลงตามเวลาที่ทำ Polling ไว้ ในส่วนหน้าจอทางด้านขวามือด้านล่างจะบอกสถานะของระบบที่เป็นองค์ประกอบของ CISCO Works 2000 เช่น Java Script, Java Cookies และ Specific Browser ความต้องการอื่นๆ ว่า Enableอยู่หรือไม่

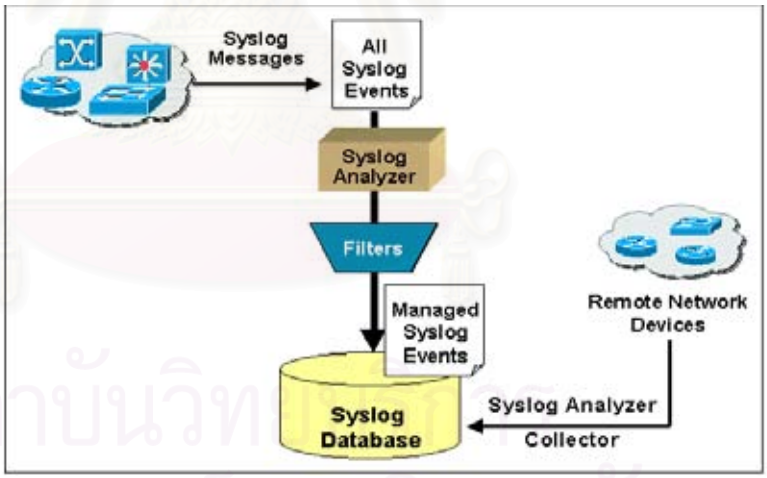
3.7.3 อธิบายหลักการทำงานในกรณีอุปกรณ์เครือข่ายมีปัญหา

ระบบการจัดการ CISCO Works 2000 ออกแบบมาโดยจัดให้มีการเก็บข้อความที่ผิดพลาด

จากอุปกรณ์ทุกตัวที่สนับสนุนการทำงานของ SNMP ทั้งนี้มีการจัดเก็บในรูปของ System Message Log ในที่นี้เรียกว่า SYSLOG ทำให้ผู้บริหารระบบทราบว่าอุปกรณ์ใดเกิดข้อผิดพลาดเกิดขึ้น มีการเปลี่ยนแปลง Configuration หรือเกิดการ Reloaded ของอุปกรณ์ สามารถแยกแยะและหาวิธีการแก้ไขปัญหาได้รวดเร็วขึ้น สามารถทราบถึงต้นเหตุของปัญหาที่เข้าขั้นวิกฤต

3.7.3.1 หลักการสร้าง SYSLOG ของระบบ

อุปกรณ์เครือข่ายทุกตัวที่สนับสนุนการทำงานของ SNMP และเป็นอุปกรณ์ของ CISCO โดยมีการคอนฟิกให้สามารถส่งข้อความของ SYSLOG ไปยังเซิร์ฟเวอร์ ในกรณีนี้จะเรียกว่า RME Server หรือ Remote Syslog Analyze Collector (Remote SAC) และจะถูกอ่านด้วย Syslog Analyzer Process ทุกๆ 5 นาทีเก็บไว้ที่ Syslog Database ดังแสดงในรูปที่ 3.7.3.1



รูปที่ 3.7.3.1 แสดงขั้นตอนของ Syslog Analyzer

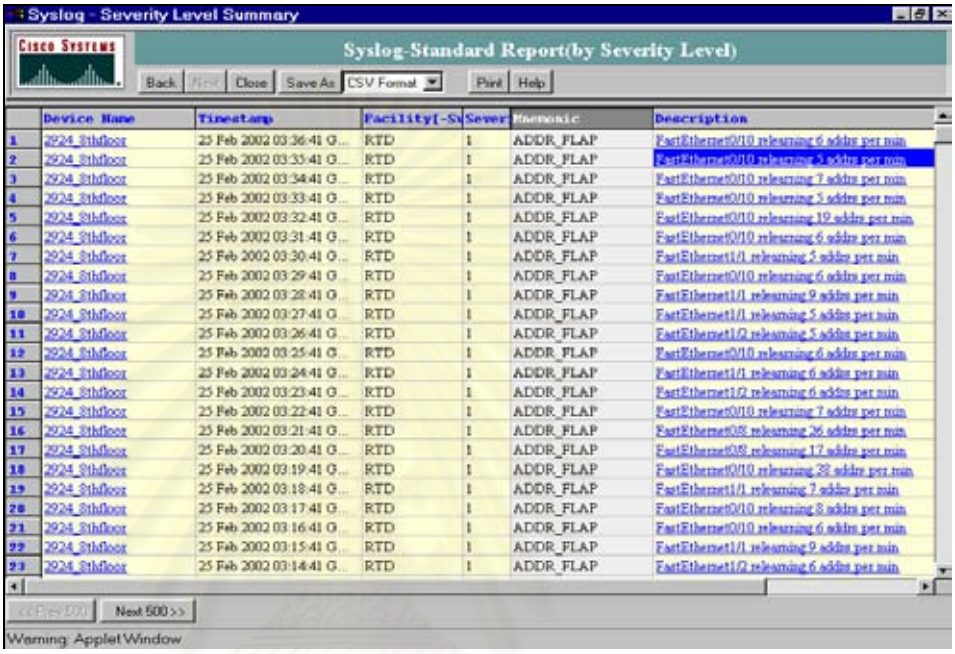
ซึ่งลักษณะการเก็บแฟ้มของ SYSLOG ประกอบด้วยฟิลด์ (Field) ต่างๆ ดังตารางที่ 3.7.3.1

ตารางที่ 3.7.3.1 แสดงลักษณะการเก็บแฟ้มของ SYSLOG

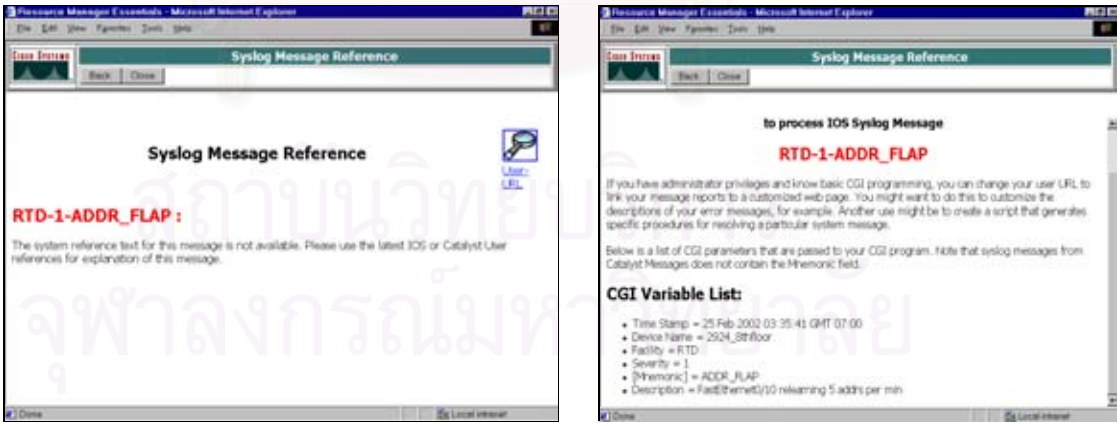
ฟิลด์	*คำอธิบาย*
Device Name	เป็นชื่ออุปกรณ์เครือข่ายที่เกิดเรคคอร์ดใน SYSLOG
Time	เป็นวันเวลาที่เกิด Log Message บนอุปกรณ์นั้นๆ
Facility Subfacility	• Facility คือเครื่องมือฮาร์ดแวร์หรือโปรโตคอล (Protocal) หรือโมดูลของซอร์ฟแวร์ระบบ • Subfacility คือส่วนขยายของ Facility ที่ทำให้เกิด SYSLOG Message ตัวอย่างของฟิลด์นี้ ได้แก่ SYS-5-CONFIGI
Severity	เป็นส่วนที่เก็บระดับความรุนแรงของปัญหา สามารถแบ่งได้ 7 ระดับ กล่าวคือ ระดับที่ 0 เป็นปัญหาฉุกเฉิน (Emergency) ระดับที่ 1 เป็นสัญญาณการเตือน (Alert) ระดับที่ 2 เป็นการเข้าขั้นวิกฤต (Critical) ระดับที่ 3 เป็นการแสดงข้อผิดพลาด (Error) ระดับที่ 4 เป็นการเตือนธรรมดา (Warning) ระดับที่ 5 เป็นข้อสังเกต (Notification) ระดับที่ 6 เป็นการบอกข้อมูลข่าวสาร (Information)
Mnemonic	เป็นรหัสที่ไม่ซ้ำกันซึ่งสามารถแยก Error Message แต่เฉพาะอุปกรณ์ซึ่งเป็น IOS ส่วนอุปกรณ์ Catalyst ไม่สามารถแสดงได้
Description	เป็นคำอธิบายหรือชื่อของ Syslog Message ซึ่งสามารถลิงค์ไปยัง User-URL เพื่อหารายละเอียดต่อไปได้

จากฟิลด์ของ Severity สามารถแบ่งระดับความรุนแรงของปัญหาได้ 7 ระดับ ตัวอย่างข้อมูลของ SYSLOG ทั้ง 7 ระดับ แสดงได้ดังรูปที่ 3.7.3.2 ถึงรูปที่ 3.7.3.11 ตามลำดับ

Severity 1



รูปที่ 3.7.3.2 แสดงระดับความรุนแรงระดับ 1 (Severity 1)



รูปที่ 3.7.3.3 แสดงรายละเอียดของระดับความรุนแรงระดับ 1 (Severity 1)

ตัวอย่าง **Severity Text File Level 1**

Syslog-Standard Report(by Severity Level)

"Device Name","Timestamp","Facility[-SubFacility]","Severity","Mnemonic","Description"

"2924_8thfloor","25 Feb 2002 15:16:16 GMT+07:00","RTD","1","ADDR_FLAP","FastEthernet0/10 relearning 13 addrs per min"

"2924_8thfloor","25 Feb 2002 15:14:56 GMT+07:00","RTD","1","ADDR_FLAP","FastEthernet0/10 relearning 21 addrs per min"

"2924_8thfloor","25 Feb 2002 15:13:56 GMT+07:00","RTD","1","ADDR_FLAP","FastEthernet0/10 relearning 5 addrs per min"

"2924_8thfloor","25 Feb 2002 15:11:36 GMT+07:00","RTD","1","ADDR_FLAP","FastEthernet0/10 relearning 13 addrs per min"

"2924_8thfloor","25 Feb 2002 15:10:36 GMT+07:00","RTD","1","ADDR_FLAP","FastEthernet0/10 relearning 6 addrs per min"

"2924_8thfloor","25 Feb 2002 15:09:16 GMT+07:00","RTD","1","ADDR_FLAP","FastEthernet1/1 relearning 5 addrs per min"

"2924_8thfloor","25 Feb 2002 15:06:46 GMT+07:00","RTD","1","ADDR_FLAP","FastEthernet0/10 relearning 6 addrs per min"

"2924_8thfloor","25 Feb 2002 15:05:46 GMT+07:00","RTD","1","ADDR_FLAP","FastEthernet0/10 relearning 5 addrs per min"

"2924_8thfloor","25 Feb 2002 15:04:46 GMT+07:00","RTD","1","ADDR_FLAP","FastEthernet1/2 relearning 5 addrs per min"

"2924_8thfloor","25 Feb 2002 14:59:26 GMT+07:00","RTD","1","ADDR_FLAP","FastEthernet0/10 relearning 6 addrs per min"

"2924_8thfloor","25 Feb 2002 14:58:26 GMT+07:00","RTD","1","ADDR_FLAP","FastEthernet0/10 relearning 9 addrs per min"

"2924_8thfloor","25 Feb 2002 14:57:16 GMT+07:00","RTD","1","ADDR_FLAP","FastEthernet1/1 relearning 7 addrs per min"

"2924_8thfloor","25 Feb 2002 14:56:16 GMT+07:00","RTD","1","ADDR_FLAP","FastEthernet1/2 relearning 5 addrs per min"

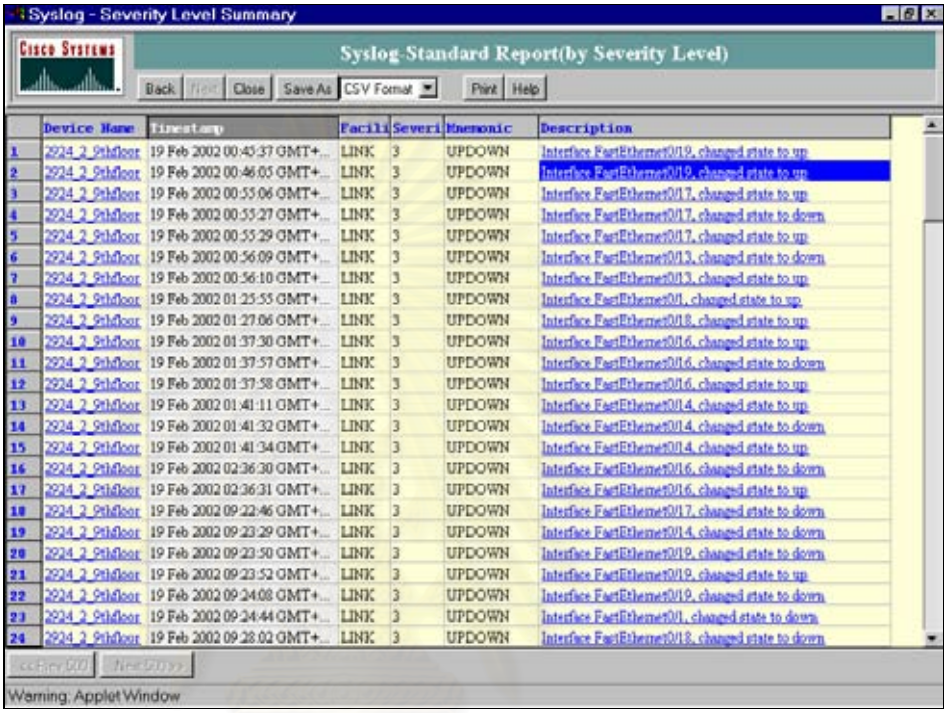
"2924_8thfloor","25 Feb 2002 14:55:06 GMT+07:00","RTD","1","ADDR_FLAP","FastEthernet0/10 relearning 20 addrs per min"

"2924_8thfloor","25 Feb 2002 14:54:06 GMT+07:00","RTD","1","ADDR_FLAP","FastEthernet0/10 relearning 5 addrs per min"

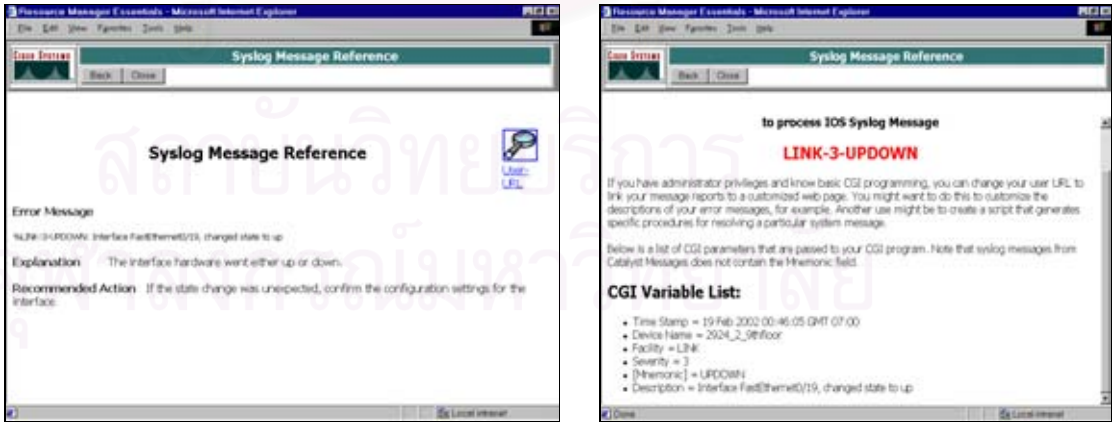
"2924_8thfloor","25 Feb 2002 14:53:06 GMT+07:00","RTD","1","ADDR_FLAP","FastEthernet1/1 relearning 7 addrs per min"

"2924_8thfloor","25 Feb 2002 14:51:06 GMT+07:00","RTD","1","ADDR_FLAP","FastEthernet1/1 relearning 5 addrs per min"

Severity 3



รูปที่ 3.7.3.4 แสดงระดับความรุนแรงระดับ 3 (Severity 3)



รูปที่ 3.7.3.5 แสดงรายละเอียดของระดับความรุนแรงระดับ 3 (Severity 3)

ตัวอย่าง **Severity Text File Level 3**

Syslog-Standard Report(by Severity Level)

"Device Name","Timestamp","Facility[-SubFacility]","Severity","Mnemonic","Description"

"2924_2_9thfloor","25 Feb 2002 01:09:23 GMT+07:00","LINK","3","UPDOWN","Interface FastEthernet0/19, changed state to up"

"2924_2_9thfloor","25 Feb 2002 01:09:22 GMT+07:00","LINK","3","UPDOWN","Interface FastEthernet0/19, changed state to down"

"2924_2_9thfloor","25 Feb 2002 01:08:55 GMT+07:00","LINK","3","UPDOWN","Interface FastEthernet0/19, changed state to up"

"2924_2_9thfloor","25 Feb 2002 01:01:53 GMT+07:00","LINK","3","UPDOWN","Interface FastEthernet0/18, changed state to up"

"2924_2_9thfloor","25 Feb 2002 00:39:51 GMT+07:00","LINK","3","UPDOWN","Interface FastEthernet0/13, changed state to up"

"2924_2_9thfloor","25 Feb 2002 00:39:49 GMT+07:00","LINK","3","UPDOWN","Interface FastEthernet0/13, changed state to down"

"2924_2_9thfloor","25 Feb 2002 00:39:26 GMT+07:00","LINK","3","UPDOWN","Interface FastEthernet0/13, changed state to up"

"2924_2_9thfloor","25 Feb 2002 00:34:31 GMT+07:00","LINK","3","UPDOWN","Interface FastEthernet0/1, changed state to up"

"2924_2_9thfloor","22 Feb 2002 12:14:02 GMT+07:00","LINK","3","UPDOWN","Interface FastEthernet0/13, changed state to down"

"2924_2_9thfloor","22 Feb 2002 12:01:23 GMT+07:00","LINK","3","UPDOWN","Interface FastEthernet0/1, changed state to down"

"2924_2_9thfloor","22 Feb 2002 09:48:52 GMT+07:00","LINK","3","UPDOWN","Interface FastEthernet0/16, changed state to down"

"2924_2_9thfloor","22 Feb 2002 09:26:59 GMT+07:00","LINK","3","UPDOWN","Interface FastEthernet0/18, changed state to down"

"2924_2_9thfloor","22 Feb 2002 04:56:18 GMT+07:00","LINK","3","UPDOWN","Interface FastEthernet0/19, changed state to down"

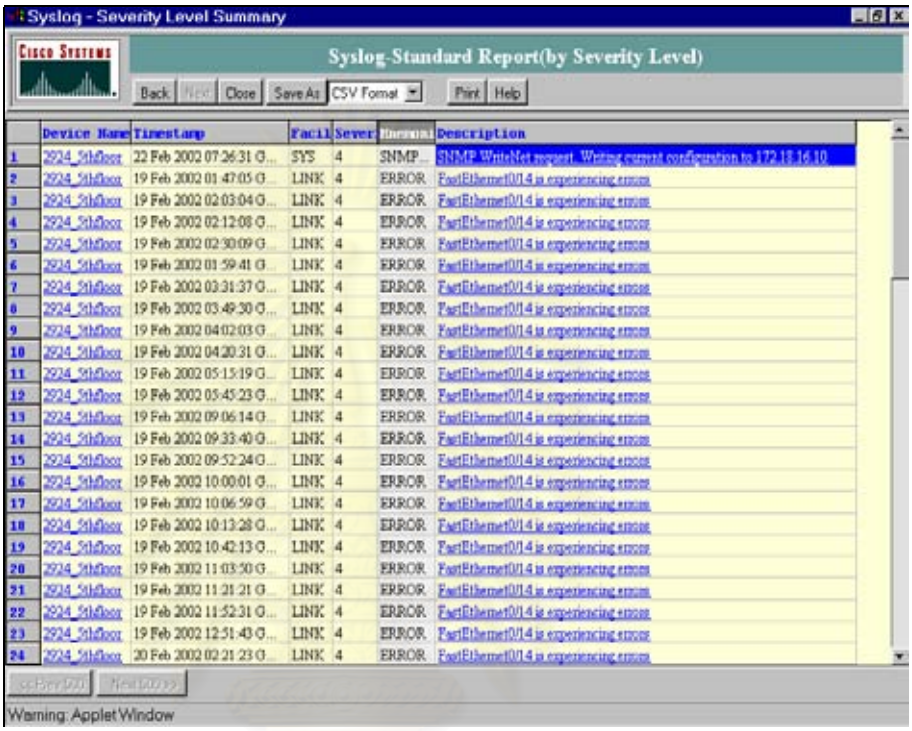
"2924_2_9thfloor","22 Feb 2002 04:08:48 GMT+07:00","LINK","3","UPDOWN","Interface FastEthernet0/16, changed state to up"

"2924_2_9thfloor","22 Feb 2002 04:08:47 GMT+07:00","LINK","3","UPDOWN","Interface FastEthernet0/16, changed state to down"

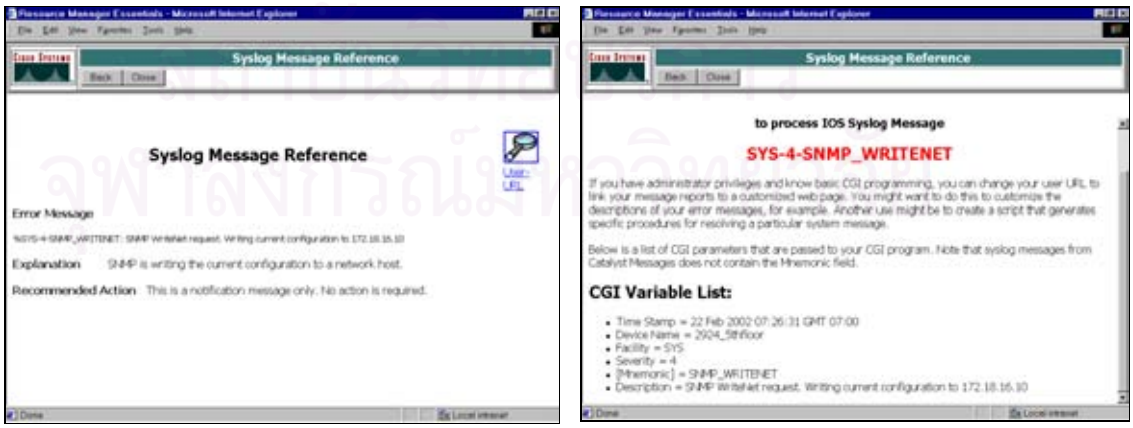
"2924_2_9thfloor","22 Feb 2002 02:53:43 GMT+07:00","LINK","3","UPDOWN","Interface FastEthernet0/17, changed state to up"

"2924_2_9thfloor","22 Feb 2002 02:53:41 GMT+07:00","LINK","3","UPDOWN","Interface FastEthernet0/17, changed state to down"

Severity 4



รูปที่ 3.7.3.6 แสดงระดับความรุนแรงระดับ 4 (Severity 4)



รูปที่ 3.7.3.7 แสดงรายละเอียดของระดับความรุนแรงระดับ 4 (Severity 4)

ตัวอย่าง **Severity Text File Level 4**

Syslog-Standard Report(by Severity Level)

"Device Name","Timestamp","Facility[-SubFacility]","Severity","Mnemonic","Description"

"2924_5thfloor","25 Feb 2002 15:03:54 GMT+07:00","LINK","4","ERROR","FastEthernet0/14 is experiencing errors"

"2924_5thfloor","25 Feb 2002 14:17:12 GMT+07:00","LINK","4","ERROR","FastEthernet0/14 is experiencing errors"

"2924_5thfloor","25 Feb 2002 06:25:27 GMT+07:00","LINK","4","ERROR","FastEthernet0/14 is experiencing errors"

"2924_5thfloor","25 Feb 2002 05:59:56 GMT+07:00","LINK","4","ERROR","FastEthernet0/14 is experiencing errors"

"2924_5thfloor","25 Feb 2002 05:51:41 GMT+07:00","LINK","4","ERROR","FastEthernet0/14 is experiencing errors"

"2924_5thfloor","25 Feb 2002 05:43:08 GMT+07:00","LINK","4","ERROR","FastEthernet0/14 is experiencing errors"

"2924_5thfloor","25 Feb 2002 05:38:28 GMT+07:00","LINK","4","ERROR","FastEthernet0/14 is experiencing errors"

"2924_5thfloor","25 Feb 2002 05:33:35 GMT+07:00","LINK","4","ERROR","FastEthernet0/14 is experiencing errors"

"2924_5thfloor","25 Feb 2002 05:29:15 GMT+07:00","LINK","4","ERROR","FastEthernet0/14 is experiencing errors"

"2924_5thfloor","25 Feb 2002 05:02:08 GMT+07:00","LINK","4","ERROR","FastEthernet0/14 is experiencing errors"

"2924_5thfloor","25 Feb 2002 02:11:56 GMT+07:00","LINK","4","ERROR","FastEthernet0/14 is experiencing errors"

"2924_5thfloor","25 Feb 2002 01:56:24 GMT+07:00","LINK","4","ERROR","FastEthernet0/14 is experiencing errors"

"2924_5thfloor","22 Feb 2002 13:32:41 GMT+07:00","LINK","4","ERROR","FastEthernet0/14 is experiencing errors"

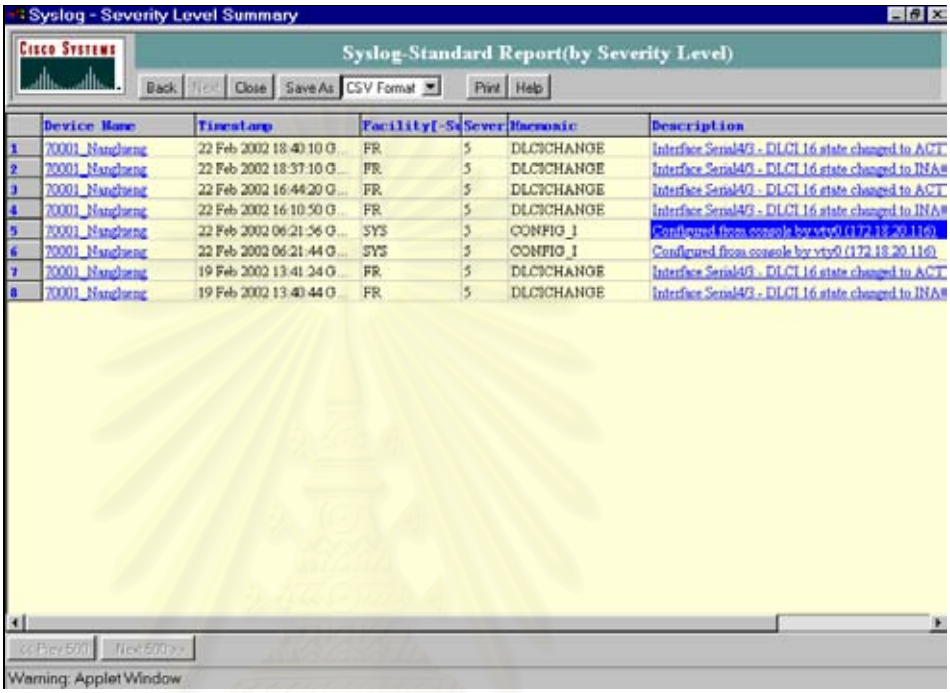
"2924_5thfloor","22 Feb 2002 11:25:38 GMT+07:00","LINK","4","ERROR","FastEthernet0/14 is experiencing errors"

"2924_5thfloor","22 Feb 2002 10:43:51 GMT+07:00","LINK","4","ERROR","FastEthernet0/14 is experiencing errors"

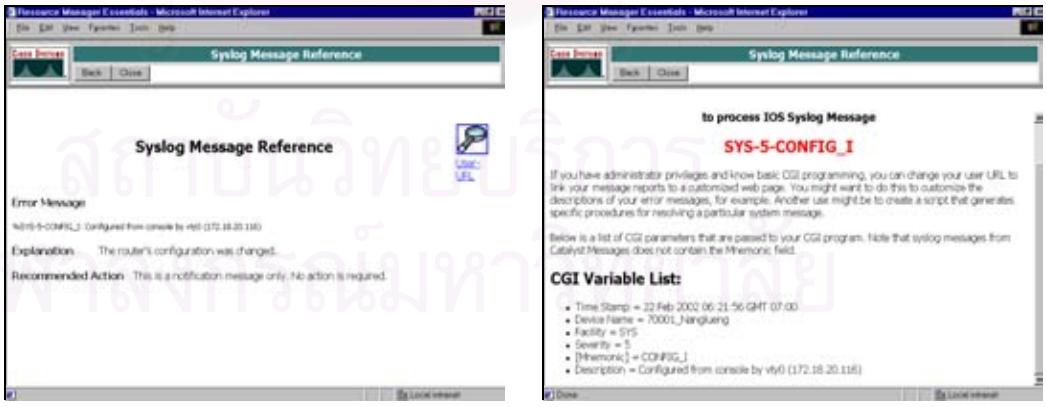
"2924_5thfloor","22 Feb 2002 08:36:06 GMT+07:00","LINK","4","ERROR","FastEthernet0/14 is experiencing errors"

"2924_5thfloor","22 Feb 2002 07:26:31 GMT+07:00","SYS","4","SNMP_WRITENET","SNMP WriteNet request. Writing current configuration to 172.18.16.10"

Severity 5



รูปที่ 3.7.3.8 แสดงระดับความรุนแรงระดับ 5 (Severity 5)



รูปที่ 3.7.3.9 แสดงรายละเอียดของระดับความรุนแรงระดับ 5 (Severity 5)

ตัวอย่าง **Severity Text File Level 5**

Syslog-Standard Report(by Severity Level)

"Device Name","Timestamp","Facility[-SubFacility]","Severity","Mnemonic","Description"

"70001_Nanglueng","22 Feb 2002 18:40:10 GMT+07:00","FR","5","DLCICHANGE","Interface Serial4/3 - DLCI 16 state changed to ACTIVE"

"70001_Nanglueng","22 Feb 2002 18:37:10 GMT+07:00","FR","5","DLCICHANGE","Interface Serial4/3 - DLCI 16 state changed to INACTIVE"

"70001_Nanglueng","22 Feb 2002 16:44:20 GMT+07:00","FR","5","DLCICHANGE","Interface Serial4/3 - DLCI 16 state changed to ACTIVE"

"70001_Nanglueng","22 Feb 2002 16:10:50 GMT+07:00","FR","5","DLCICHANGE","Interface Serial4/3 - DLCI 16 state changed to INACTIVE"

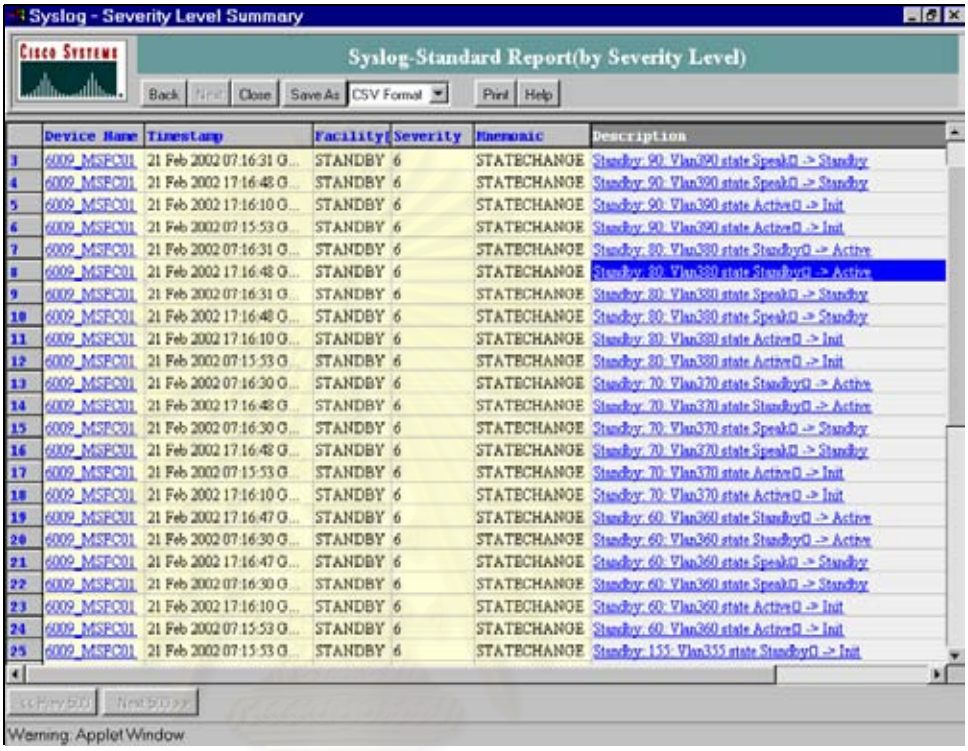
"70001_Nanglueng","22 Feb 2002 06:21:56 GMT+07:00","SYS","5","CONFIG_I","Configured from console by vty0 (172.18.20.116)"

"70001_Nanglueng","22 Feb 2002 06:21:44 GMT+07:00","SYS","5","CONFIG_I","Configured from console by vty0 (172.18.20.116)"

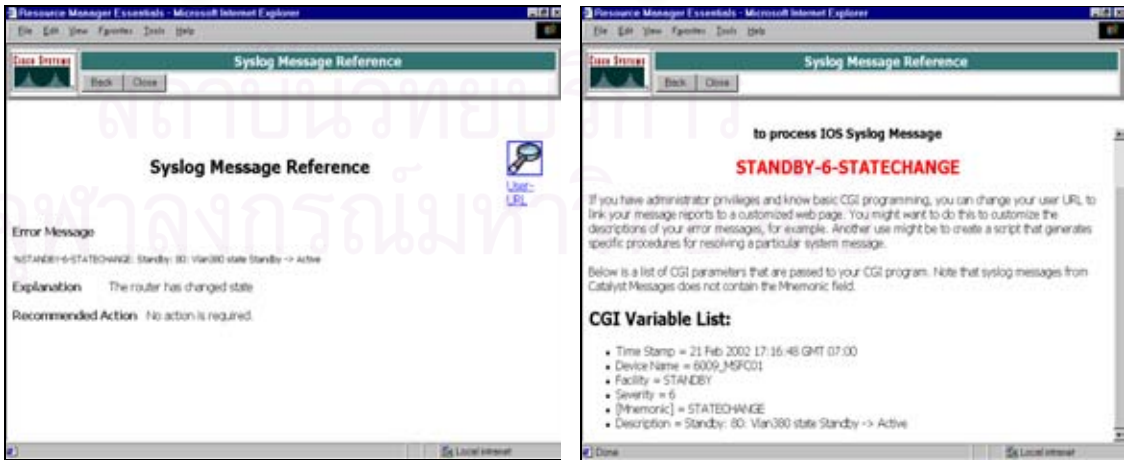
"70001_Nanglueng","19 Feb 2002 13:41:24 GMT+07:00","FR","5","DLCICHANGE","Interface Serial4/3 - DLCI 16 state changed to ACTIVE"

"70001_Nanglueng","19 Feb 2002 13:40:44 GMT+07:00","FR","5","DLCICHANGE","Interface Serial4/3 - DLCI 16 state changed to INACTIVE"

Severity 6



รูปที่ 3.7.3.10 แสดงระดับความรุนแรงระดับ 6 (Severity 6)



รูปที่ 3.7.3.11 แสดงรายละเอียดของระดับความรุนแรงระดับ 6 (Severity 6)

ตัวอย่าง **Severity Text File Level 6**

Syslog-Standard Report(by Severity Level)

"Device Name","Timestamp","Facility[-SubFacility]","Severity","Mnemonic","Description"

"6009_MSFC01","21 Feb 2002 07:16:31 GMT+07:00","STANDBY","6","STATECHANGE","Standby: 90: Vlan390 state Standby, -> Active"

"6009_MSFC01","21 Feb 2002 17:16:48 GMT+07:00","STANDBY","6","STATECHANGE","Standby: 90: Vlan390 state Standby, -> Active"

"6009_MSFC01","21 Feb 2002 17:16:48 GMT+07:00","STANDBY","6","STATECHANGE","Standby: 90: Vlan390 state Speak, -> Standby"

"6009_MSFC01","21 Feb 2002 07:16:31 GMT+07:00","STANDBY","6","STATECHANGE","Standby: 90: Vlan390 state Speak, -> Standby"

"6009_MSFC01","21 Feb 2002 17:16:10 GMT+07:00","STANDBY","6","STATECHANGE","Standby: 90: Vlan390 state Active, -> Init"

"6009_MSFC01","21 Feb 2002 07:15:53 GMT+07:00","STANDBY","6","STATECHANGE","Standby: 90: Vlan390 state Active, -> Init"

"6009_MSFC01","21 Feb 2002 17:16:48 GMT+07:00","STANDBY","6","STATECHANGE","Standby: 80: Vlan380 state Standby, -> Active"

"6009_MSFC01","21 Feb 2002 07:16:31 GMT+07:00","STANDBY","6","STATECHANGE","Standby: 80: Vlan380 state Standby, -> Active"

"6009_MSFC01","21 Feb 2002 17:16:48 GMT+07:00","STANDBY","6","STATECHANGE","Standby: 80: Vlan380 state Speak, -> Standby"

"6009_MSFC01","21 Feb 2002 07:16:31 GMT+07:00","STANDBY","6","STATECHANGE","Standby: 80: Vlan380 state Speak, -> Standby"

"6009_MSFC01","21 Feb 2002 07:15:53 GMT+07:00","STANDBY","6","STATECHANGE","Standby: 80: Vlan380 state Active, -> Init"

"6009_MSFC01","21 Feb 2002 17:16:10 GMT+07:00","STANDBY","6","STATECHANGE","Standby: 80: Vlan380 state Active, -> Init"

"6009_MSFC01","21 Feb 2002 07:16:30 GMT+07:00","STANDBY","6","STATECHANGE","Standby: 70: Vlan370 state Standby, -> Active"

"6009_MSFC01","21 Feb 2002 17:16:48 GMT+07:00","STANDBY","6","STATECHANGE","Standby: 70: Vlan370 state Standby, -> Active"

"6009_MSFC01","21 Feb 2002 07:16:30 GMT+07:00","STANDBY","6","STATECHANGE","Standby: 70: Vlan370 state Speak, -> Standby"

"6009_MSFC01","21 Feb 2002 17:16:48 GMT+07:00","STANDBY","6","STATECHANGE","Standby: 70: Vlan370 state Speak, -> Standby"

"6009_MSFC01","21 Feb 2002 17:16:10 GMT+07:00","STANDBY","6","STATECHANGE","Standby: 70: Vlan370 state Active, -> Init"

จากแฟ้มของ SYSLOG ดังกล่าวข้างต้นสามารถนำมาวิเคราะห์และออกแบบวิธีการแก้ไขปัญหาเพิ่มเติมต่อจากระบบของ CISCO Works 2000 โดยจะเน้นการใช้งานทางด้านการชี้แนะในแง่ของเครื่องอุปกรณ์ อะไหล่สำรอง ที่จะนำมาใช้ในการแก้ไขปัญหา ซึ่งรายละเอียดของการวิเคราะห์และออกแบบโปรแกรมจะมีการนำตัวเท็กซ์ไฟล์ (Text File) ของ SYSLOG เป็นเกณฑ์ในการวิเคราะห์และออกแบบ โดยสามารถแสดงรายละเอียดของการวิเคราะห์และออกแบบได้ในบทต่อไป (บทที่ 4)

บทที่ 4

การออกแบบวิธีการเฝ้าติดตามและแก้ไขปัญหาการทำงานของระบบแลนของธกส.

จากการศึกษาระบบแลนของหน่วยงานที่ใช้เป็นกรณีศึกษา พบว่าการจัดการเกี่ยวกับระบบแลนของธกส.ยังมีปัญหาต่าง ๆ ที่ต้องการการแก้ไขปรับปรุง ซึ่งสามารถสรุปได้ดังนี้

- ไม่มีระบบจัดการเครือข่ายที่ใช้เป็นระบบเฝ้าติดตามและแก้ไขปัญหา
- เมื่อเกิดปัญหาขึ้นจะแก้ไขในลักษณะของการลองผิดลองถูก
- ไม่มีระบบแจ้งเตือนถึงความพร้อมให้บริการของอุปกรณ์เครือข่าย
- จะทราบว่ามีปัญหาเมื่อปัญหาได้เกิดขึ้นแล้ว
- ไม่มีระบบที่จะแสดงความสามารถรองรับงานของอุปกรณ์เครือข่าย
- ขาดขั้นตอนการปฏิบัติงานและส่งต่องานของ Network Operator ในแต่ละกะ
- ขาดรายงานสรุปผลการแก้ไขปัญหาของระบบแลน เพื่อให้ผู้บริการนำไปวิเคราะห์ต่อ

จากปัญหาต่าง ๆ ตามที่ได้กล่าวมานี้ จำเป็นต้องมีการแก้ไขโดยทำการออกแบบระบบเพื่อเฝ้าติดตามและแก้ไขปัญหาการทำงานของระบบแลน ตามที่กำหนดขอบเขตและผลลัพธ์ โดยสรุปได้ 3 ประการ ดังนี้

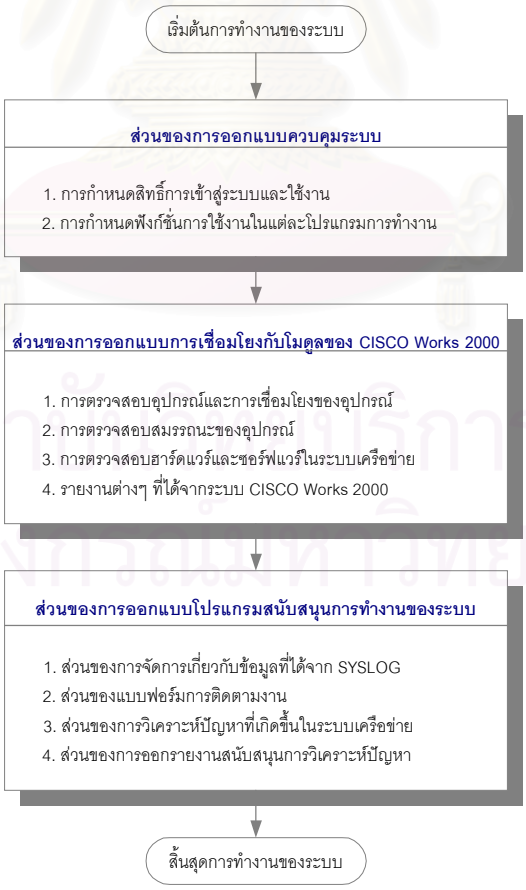
- ขั้นตอนในการแก้ไขปัญหาแต่ละอุปกรณ์ และรายละเอียดของรายการอะไหล่สำรองที่จำเป็นต้องใช้ในการแก้ไขปัญหา
- แบบฟอร์มสรุปผลการเฝ้าติดตาม และแก้ไขปัญหา
- รายงาน สรุปผลการเฝ้าติดตาม และรายงานสรุปผลการแก้ไขปัญหา

โดยระบบที่ทำการออกแบบสามารถนำมาใช้งานเพื่อแก้ไขปัญหาต่างๆ ข้างต้นได้อย่างมีประสิทธิภาพ เนื่องจากระบบที่ทำการออกแบบได้ใช้หลักการบริหารระบบเครือข่าย ซึ่งกำหนดหน้าที่ในการบริหารเครือข่ายไว้ 5 ประการ ตามทฤษฎีที่กล่าวข้างต้นในหัวข้อที่ 2.1.1.1 จนกระทั่งถึงหัวข้อที่ 2.1.1.5 รวมทั้งใช้หลักการควบคุมการดำเนินงานของระบบ (Network Operation Control) ตามหัวข้อที่ 2.1.2 ในการออกแบบระบบเฝ้าติดตามและแก้ไขปัญหาการทำงานของแลนได้ทำการออกแบบให้เป็นระบบที่สามารถใช้งานได้อย่างง่าย (User Friendly) ในลักษณะเป็นหน้าจอเพื่อเลือกเมนูต่าง ๆ ที่ถูกกำหนดไว้แล้ว แยกตามฟังก์ชันงานและได้ออกแบบการส่งค่าพารามิเตอร์ต่าง ๆ ไปยังโปรแกรมจัดการ CISCOWorks2000 เพื่อดึงโมดูลต่างๆ มาใช้งานโดยได้ทำการศึกษาและวิเคราะห์ โมดูลต่าง ๆ เหล่านั้นแล้วว่า มีความสำคัญและจำเป็นต่อการเฝ้าติดตาม และแก้ไขปัญหาระบบแลน เนื่องจากโปรแกรมจัดการเครือข่าย CISCOworks2000 มีฟังก์ชันในการจัดการเครือข่ายที่หลากหลาย ในบางโมดูลรวมเอาหลักการบริหารระบบเครือข่ายไว้มากกว่า 1 หน้าที่มาประยุกต์ให้เข้ากับการใช้

งาน ซึ่งในแต่ละโมดูลที่นำมาใช้งานจะกล่าวต่อไป และนอกจากนี้ยังมีการออกแบบเพิ่มเติม โดยนำแฟ้มข้อมูลของระบบจัดการเครือข่าย ที่เรียกชื่อว่า SYSLOG มาทำการจัดรูปแบบให้เป็น SQL เพื่อทำการออกแบบต่อในส่วนของการแจ้งเตือนปัญหาที่เกิด และการเตรียมอุปกรณ์ที่จะใช้ในการแก้ไขปัญหานั้นๆ รวมทั้งการออกรายงาน และการออกแบบฟอร์มการส่งต่องาน ซึ่งในรายละเอียดของระบบที่ทำการออกแบบกล่าวในหัวข้อของการออกแบบ

4.1 การออกแบบวิธีการเฝ้าติดตาม และแก้ไขปัญหาการทำงานของระบบแลน

ในการออกแบบวิธีเฝ้าติดตาม และแก้ไขปัญหาการทำงานของระบบแลน สามารถแบ่งได้ 3 ส่วนหลักๆ กล่าวคือ ส่วนของการออกแบบควบคุมระบบ ส่วนของการออกแบบการเชื่อมโยงกับโมดูลของ CISCO Works 2000 และส่วนของการออกแบบโปรแกรมสนับสนุนการทำงานของระบบ ซึ่งแสดงได้ดังรูปที่ 4.1



รูปที่ 4.1 แสดงการออกแบบวิธีการเฝ้าติดตามและการแก้ไขปัญหาของระบบแลนของธกส.

4.1.1 ส่วนของการออกแบบควบคุมระบบ

เป็นส่วนที่ใช้ควบคุมการทำงานของ Network Operator มีการกำหนดสิทธิของการใช้งานโปรแกรม และกำหนดขั้นตอนต่าง ๆ ของการเฝ้าติดตาม และแก้ไขปัญหาระบบแลน ซึ่งเป็นการออกแบบการใช้งานของผู้ใช้ ในการกำหนดสิทธิ์การใช้งานที่แตกต่างกันตามอำนาจหน้าที่ของผู้ใช้แต่ละคนว่าสามารถมีสิทธิ์เข้ามาใช้งานในระบบได้มากน้อยแค่ไหน โดยสามารถกำหนดระดับของผู้ใช้ได้ 3 ระดับ ดังนี้

- A = Administrator เป็นระดับผู้บริหารระบบ
- O = Operator เป็นระดับปฏิบัติการ สามารถทำการเฝ้าดูระบบและเรียกใช้โปรแกรมได้ แต่ไม่สามารถทำการเซตอัพระบบ
- U = User เป็นระดับของผู้ใช้งานทั่วๆ ไป

4.1.2 ส่วนของการออกแบบการเชื่อมโยงกับโมดูลของ CISCO Works 2000

เป็นการเชื่อมโยงระบบที่ออกแบบให้สามารถลิงค์ไปยัง ระบบจัดการ CISCO Works 2000 เพื่อดึงโมดูลต่าง ๆ มาใช้งาน ทั้งนี้มีการออกแบบการเชื่อมโยงกับระบบจัดการของ CISCO Works 2000 เพื่อนำเอาโมดูลย่อยต่างๆ ในระบบการจัดการมาใช้งาน โดยมีการส่งค่าของชื่อเซิฟเวอร์และหมายเลขพอร์ตแล้วตามด้วย ยูอาร์แอล (URL) ของแต่ละฟังก์ชั่นการทำงานในหน้าจอของการเฝ้าติดตามระบบเครือข่าย (Network Monitoring) ดังนั้นผู้ใช้งานต้องมีการป้อนข้อมูลของชื่อและรหัสผ่านที่สามารถเข้าไปใช้งานกับ CISCO Works 2000 ก่อน ทั้งนี้เพราะว่าเป็นการรักษาความปลอดภัยของระบบเครือข่าย รวมทั้งมีการพัฒนาโปรแกรมการเชื่อมโยงไปยัง CISCO Works 2000 ให้เข้ากับระบบที่ทำการออกแบบ ซึ่งประกอบด้วยส่วนของ

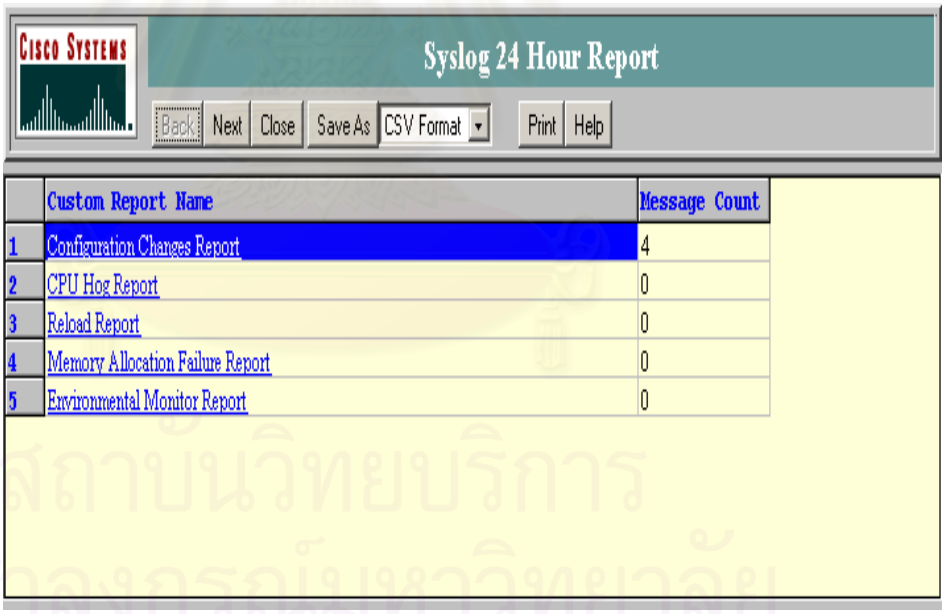
1) **การตรวจสอบอุปกรณ์และการเชื่อมโยงของอุปกรณ์**

- SYSLOG Message

  แสดง SYSLOG หรือค่าความผิดปกติของอุปกรณ์เครือข่าย ในระบบเครือข่ายภายใน 24 ชม. ว่ามีการเปลี่ยนแปลงอะไรเกิดขึ้นบ้าง ซึ่งแสดงได้ดังรูปที่ 4.1.2.1 โดยระบบจะระบุให้อุปกรณ์ส่งค่าความผิดปกติของอุปกรณ์เครือข่ายมาเก็บไว้ที่ CISCO Works 2000 Server ซึ่งแบ่งแยกความรุนแรงของความผิดปกติเป็น 7 ระดับ คือ ระดับ 0-6 ซึ่งระดับ Severity ควรสูงกว่า Level 4 (4-7) ซึ่งถือว่าเป็นระดับที่เกิดขึ้นเล็กน้อยอาจเกิด

จากการเซ็ทค่าต่างๆ ของอุปกรณ์เปลี่ยนไป หากต่ำกว่านี้ (0-3) แสดงว่าเกิดความผิดปกติกับอุปกรณ์เครือข่ายขึ้นจริงและระบบยังจัดหมวดหมู่ของความผิดพลาด ให้ดังนี้

- รายงานของ Configuration Change จะทำการรายงานเมื่อ Configuration ของอุปกรณ์มีการเปลี่ยนแปลง
- รายงาน CPU Hog จะทำการรายงานเมื่อ CPU load ของอุปกรณ์เกินความสามารถที่จะรับได้
- รายงาน Reload จะทำการรายงานเมื่ออุปกรณ์มีการ Reload ตัว เนื่องจากเกิดเหตุการณ์ต่างๆ เช่น ไฟตก เป็นต้น
- รายงาน Memory Allocation Failure จะทำการรายงานเมื่อมีการจัดการกับหน่วยความจำของอุปกรณ์
- รายงาน Environmental Monitor จะทำการรายงานเมื่อสภาพแวดล้อมของอุปกรณ์ก่อนที่จะเกิดปัญหา เช่น อุณหภูมิ ความชื้น เป็นต้น



รูปที่ 4.1.2.1 แสดงลักษณะหน้าจอของ SYSLOG Message

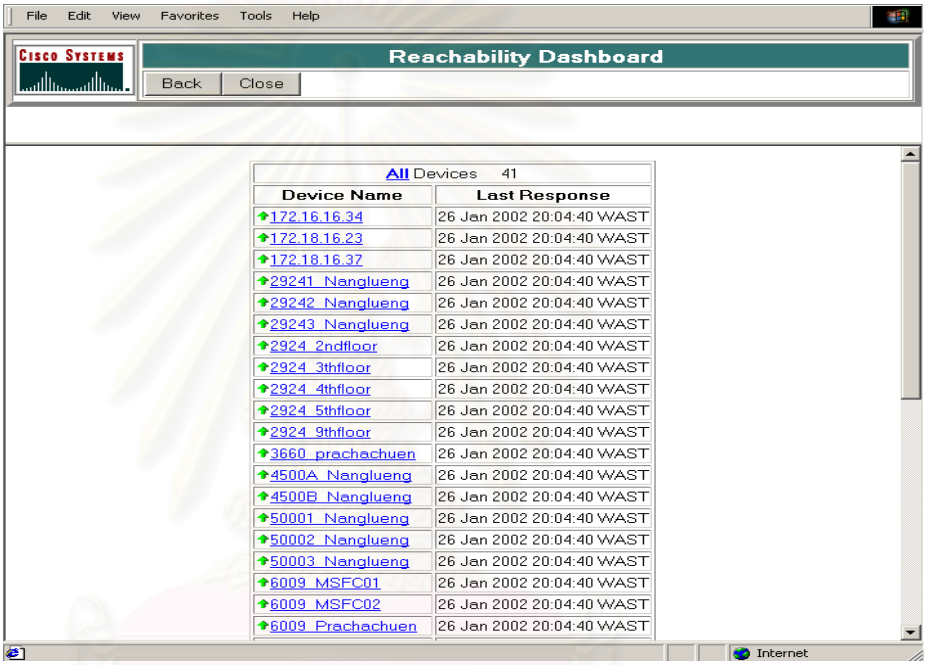
- Reachability Dashboard

เป็น Tool ใช้ในการตรวจสอบว่า ณ.ขณะนั้นๆ ในระบบเครือข่ายมีอุปกรณ์เครือข่าย ตัวใดทำงานอยู่ และมีตัวไหนบ้างที่หยุดทำงานบ้าง หากมีอุปกรณ์ตัวใดตัวหนึ่งหยุดการทำงานแสดงว่าจะต้องเกิดความผิดปกติกับส่วนใดส่วนหนึ่งของอุปกรณ์เครือข่าย โดย

ระบบจะแสดงอุปกรณ์ทั้งหมดด้วย ชื่ออุปกรณ์ และเวลา วันที่ล่าสุดที่แสดงสถานะของอุปกรณ์ สามารถแสดงได้ดังรูปที่ 4.1.2.2

หมายเหตุ  กรณีที่ Up แสดงว่าปกติ

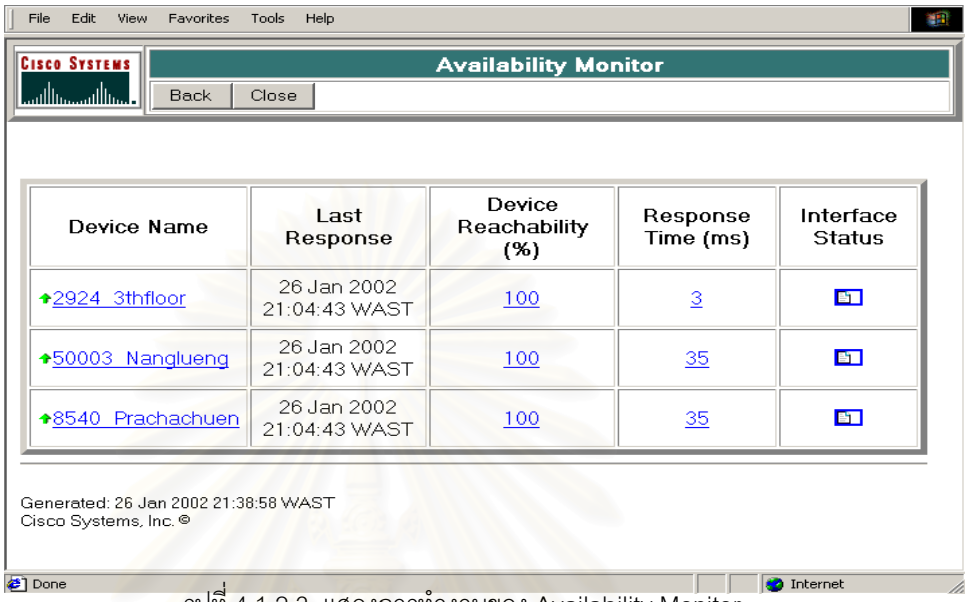
 กรณีที่ Down แสดงว่าไม่ปกติ



รูปที่ 4.1.2.2 แสดงการทำงานของ Reachability Dashboard

- Availability Monitor

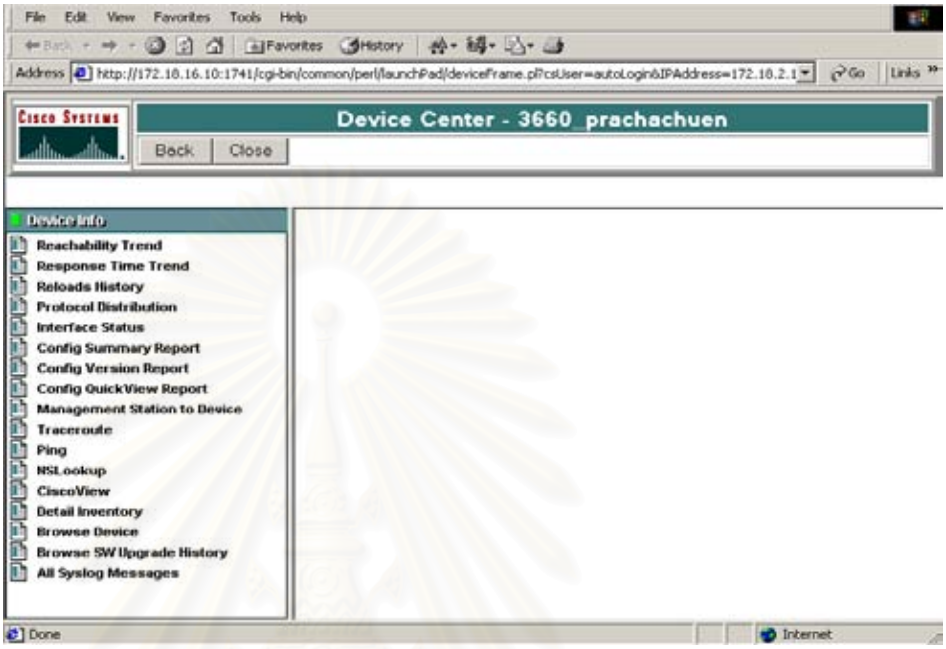
ใช้ในการตรวจสอบค่า Available ของอุปกรณ์ชนิดนั้นๆ ซึ่งAvailable ของอุปกรณ์แต่ละตัวควรเป็น 100% หากไม่ใช่ค่านี้แสดงว่าเกิดความผิดปกติกับอุปกรณ์เครือข่าย โดยระบบจะแสดงชื่ออุปกรณ์ เวลาวันที่ที่แสดงสถานะ %ของ Response Time เป็น Milisecond และการแสดงสถานะการต่อเชื่อมโดยสามารถคลิกดูรายละเอียดได้ ดังแสดงในรูปที่ 4.1.2.3



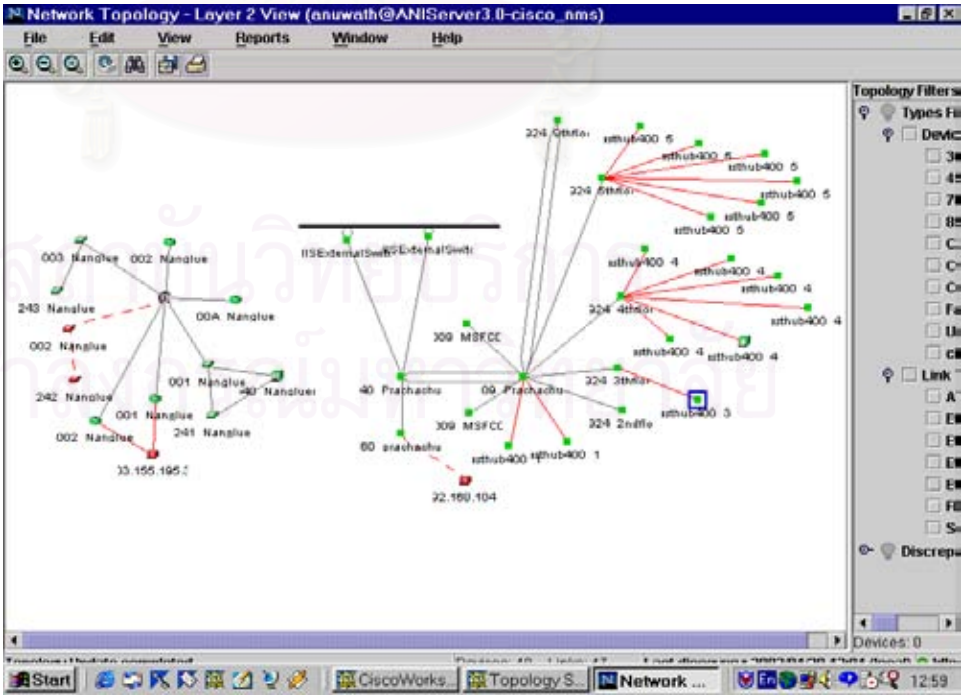
รูปที่ 4.1.2.3 แสดงการทำงานของ Availability Monitor

- Topology Service

  เป็นการเลือกอุปกรณ์เครือข่ายที่ต้องการตรวจสอบสมรรถนะของอุปกรณ์ จากนั้น right-click แล้วเลือก Device Center จะปรากฏหน้าจอ Device Center ขึ้นมา แสดงดังรูปที่ 4.1.2.4 ในกรณีที่ต้องการตรวจสอบการต่อเชื่อมของอุปกรณ์ทั้งหมดในภาพรวมให้ใช้เมนู Topology Service แสดงรูปแบบการต่อเชื่อมของวงเครือข่ายทั้งหมดโดยรวม แต่จะแสดงเฉพาะอุปกรณ์ของ CISCO เท่านั้นที่สามารถทราบว่าเป็นอุปกรณ์ประเภทอะไร เช่น Router รุ่น 4500 จำนวน 2 ยูนิต และ Router รุ่น 7000 จำนวน 2 ยูนิต ประเภทของลิงค์ที่ต่อเชื่อมกันอยู่มี ATM 156 M จำนวน 2 ลิงค์ เป็นต้น แสดงได้ดังรูปที่ 4.1.2.5 โดยรูปที่แสดงด้านขวามือเป็นการสรุปและสามารถดูรายละเอียดของแต่ละลิงค์ที่เชื่อมกัน โดยนำเคอเซอร์ชี้ไปที่ลิงค์ที่ต้องการระบบจะแสดงรายละเอียดของลิงค์ว่าต่อเชื่อมจากอุปกรณ์อะไรมายังอุปกรณ์อะไร ด้วยลิงค์ประเภทไหนและยังสามารถปรับแต่งรูปตามที่เราต้องการได้โดยการชี้ไปยังอุปกรณ์และลากไปยังตำแหน่งที่เราต้องการ



รูปที่ 4.1.2.4 แสดงลักษณะหน้าจอของ Device Center



รูปที่ 4.1.2.5 แสดงลักษณะการเชื่อมต่อของตัวอุปกรณ์

- **Search Archive by Device**

  ใช้ตรวจสอบ Configuration files ที่จัดเก็บไว้ภายในอุปกรณ์ เครือข่าย โดยจะสามารถแสดงผลได้ทั้งที่เป็น StartUp Configuration, Running Configuration และสามารถหาความแตกต่างของ config ทั้งสองได้อีกด้วย แสดงได้ดังรูปที่ 4.1.2.6

รูปที่ 4.1.2.6 แสดงลักษณะหน้าจอของ Device Configuration Viewer

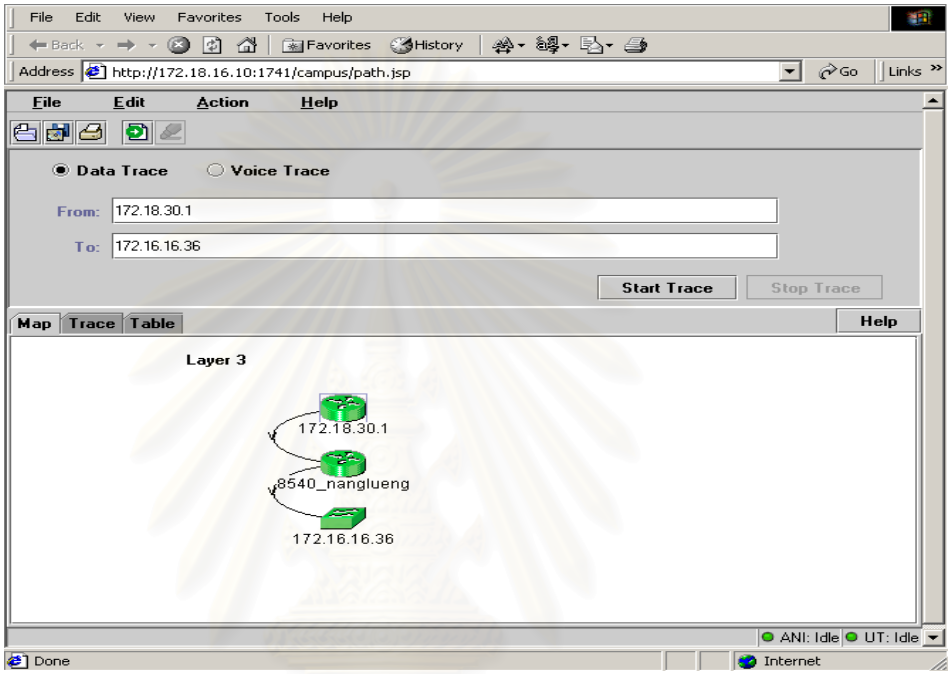
- **Path Analysis**

  หากพบว่าปัญหานั้นๆเกิดขึ้นกับ workstation (เช่น workstation ไม่สามารถเชื่อมต่อกับระบบเครือข่ายได้) ให้ใช้ Path Analysis ในการวิเคราะห์หาเส้นทางว่าระบบเครือข่ายมีปัญหาที่จุดไหนในระบบเครือข่าย สามารถแสดงได้ดังรูปที่ 4.1.2.7

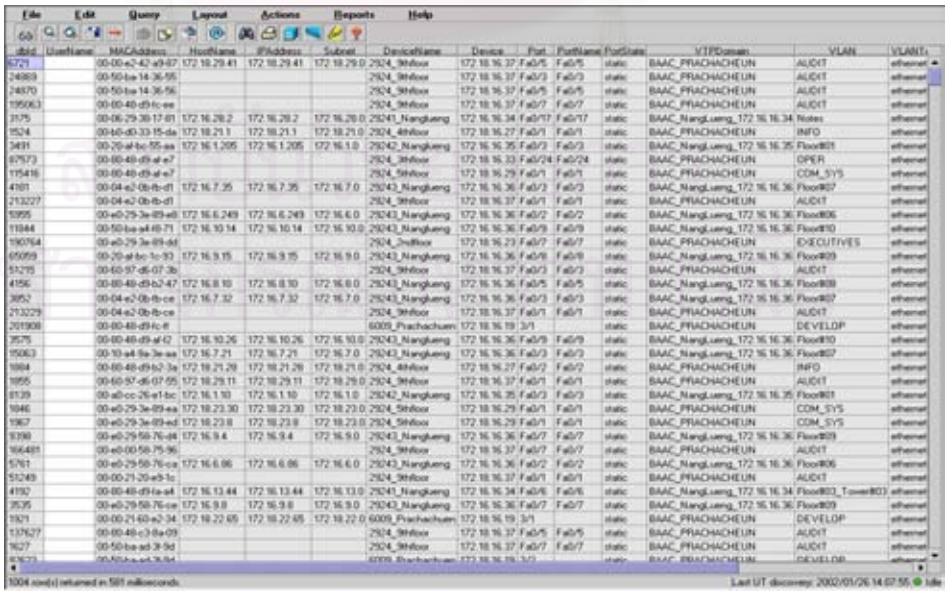
- **User Tracking**

  หากไม่ทราบว่า workstation นั้นๆเชื่อมต่อกับ hub/switch ที่ port ไหน ให้ใช้ User Tracking ในการตรวจสอบ IP Address กับตำแหน่งที่ต่อกับ Port ของ hub/switch นอกจาก User Tracking จะสามารถใช้ตรวจสอบได้ว่า workstation นั้นๆเชื่อมต่อกับ hub/switch ที่ port ไหนแล้ว ยังสามารถตรวจสอบการ Duplicate ของ IP Address ได้อีกด้วย โดยเลือกที่ Reports → Duplicate IP โปรแกรมจะแสดง IP Address ที่ตรวจ

สอบได้ว่ามีการกำหนด Duplicate IP Address กันออกมา ซึ่งสามารถ แสดง User Tracking ได้ดังรูปที่ 4.1.2.8



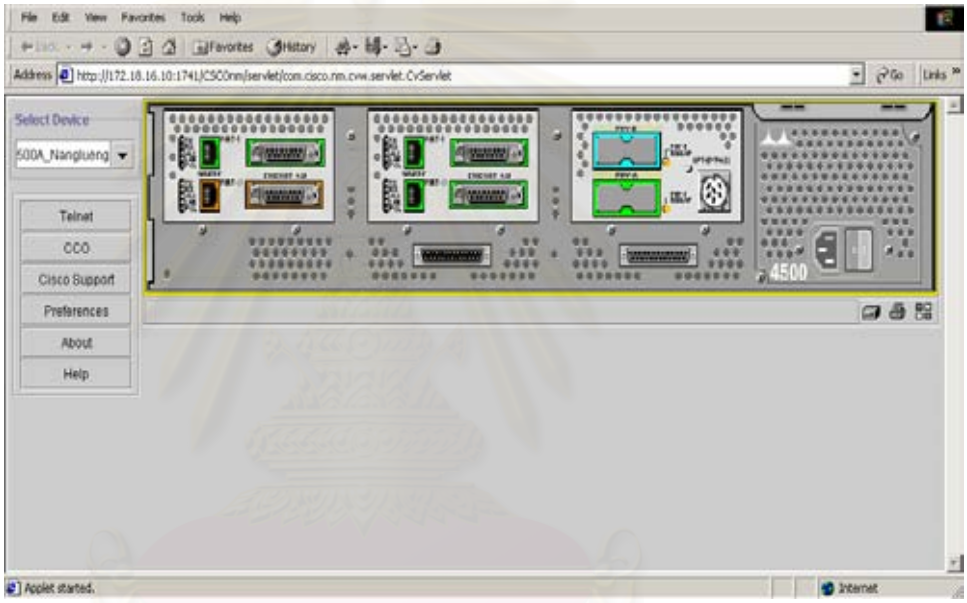
รูปที่ 4.1.2.7 แสดงลักษณะหน้าจอของ Path Analysis



รูปที่ 4.1.2.8 แสดงลักษณะรายละเอียดของ User Tracking

- CISCO View

  CiscoView สามารถที่จะแสดงผลเป็นแบบ GUI โดยจะแสดงรูปของอุปกรณ์ เครือข่ายนั้นๆ และสามารถบอกได้ว่า interface ใดของตัวอุปกรณ์ที่มีการเชื่อมต่ออยู่บ้าง ซึ่งแสดงรูปแบบของอุปกรณ์ที่เหมือนจริงกับอุปกรณ์ที่ต่อเชื่อมอยู่และสามารถบอกสถานะของอุปกรณ์นั้นๆ ว่าเปิดหรือปิด หรือว่าพอร์ตใดเปิดหรือพอร์ตใดปิด เป็นต้น แสดงดังรูปที่ 4.1.2.9

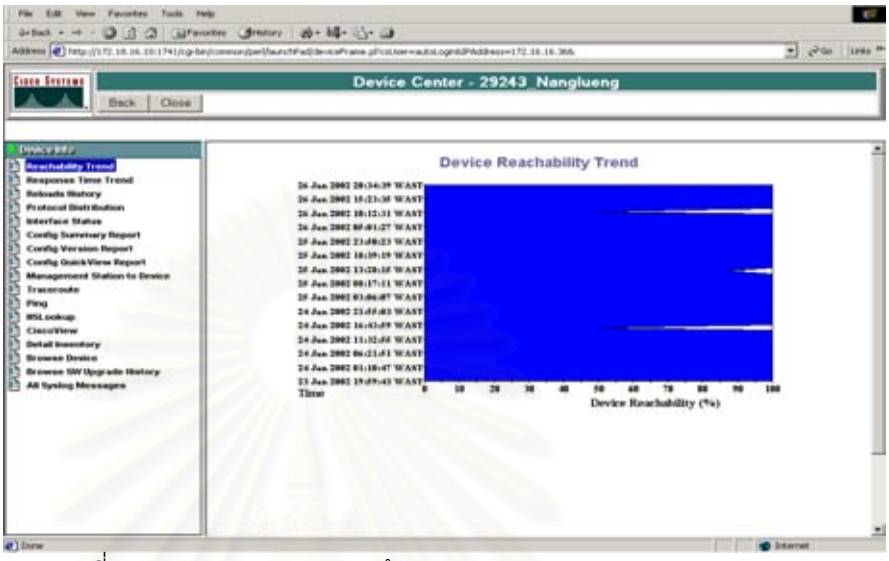


รูปที่ 4.1.2.9 แสดงรูปการเชื่อมต่อของระบบเครือข่าย

2) **การตรวจสอบสมรรถนะของอุปกรณ์**

- Reachability Trend

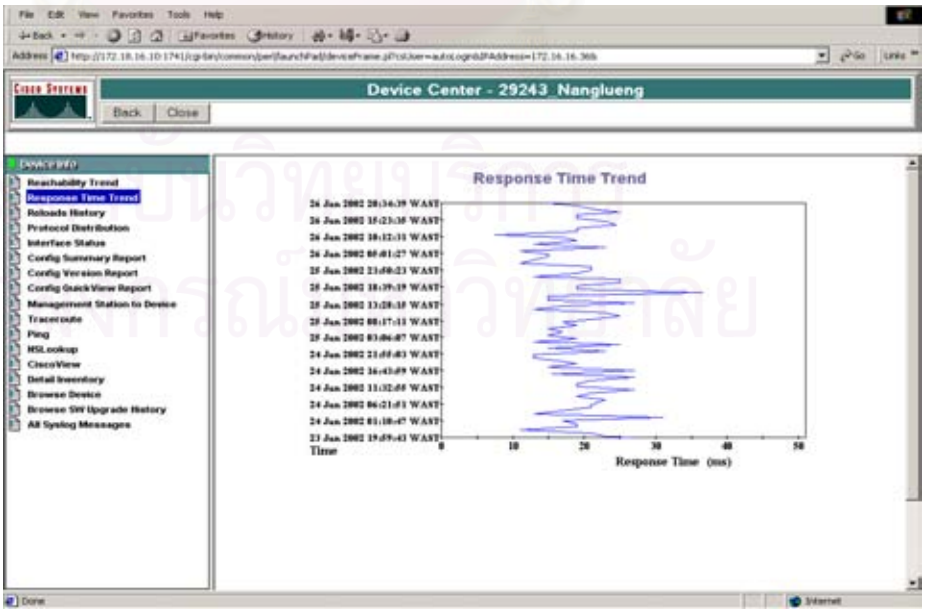
  Reachability Trend จะแสดงค่าความ reliability ของอุปกรณ์นั้นๆ โดยจัดเก็บเป็นค่าในเชิงสถิติ แสดงดังรูปที่ 4.1.2.10 อุปกรณ์ที่มีสมรรถนะสูง ควรจะมีค่ากราฟแสดงผล Reachabilty Trend สูง หากค่าของกราฟมีน้อยแสดงว่าอุปกรณ์ตัวนั้น reliability ต่ำ



รูปที่ 4.1.2.10 แสดงลักษณะหน้าจอของ Device Reachablity Trend

- **Response Time Trend**

Response Time Trend จะแสดงค่า response time ของอุปกรณ์นั้นๆ โดยจัดเก็บเป็นค่าในเชิงสถิติ แสดงดังรูปที่ 4.1.2.11 อุปกรณ์ที่มี performance สูงควรจะมีค่ากราฟแสดงผล Response Time Trend ต่ำ หากค่าของกราฟมีมากแสดงว่าอุปกรณ์ตัวนั้นสมรรถนะต่ำ

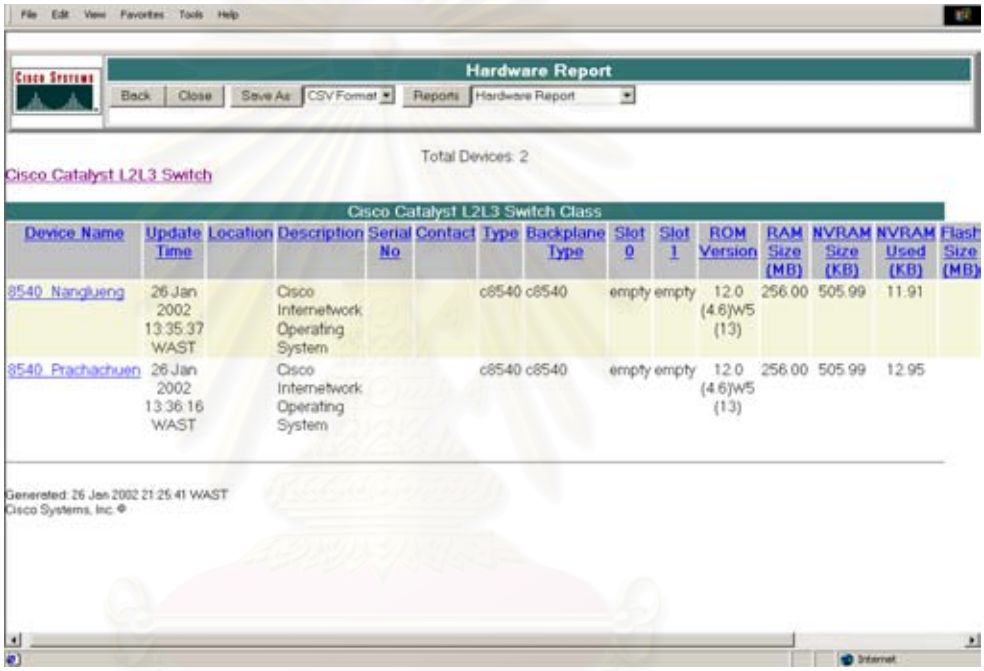


รูปที่ 4.1.2.11 แสดงลักษณะหน้าจอของ Response Time Trend

3) **การตรวจสอบฮาร์ดแวร์และซอร์ฟแวร์ในระบบเครือข่าย**

- Hardware Summary Graph

  เป็นการตรวจสอบรายละเอียดทางฮาร์ดแวร์ของอุปกรณ์เครือข่าย โดยจะแจกแจงรายละเอียดตามชนิดของอุปกรณ์ แล้วจึงลงในรายละเอียดของอุปกรณ์นั้นๆ อาทิ เช่น ฮาร์ดแวร์รุ่นไหน มีขนาดของ flash และ หน่วยความจำเท่าไร แสดงดังรูปที่ 4.1.2.12



รูปที่ 4.1.2.12 แสดงลักษณะหน้าจอของรายงานฮาร์ดแวร์ (Hardware Report)

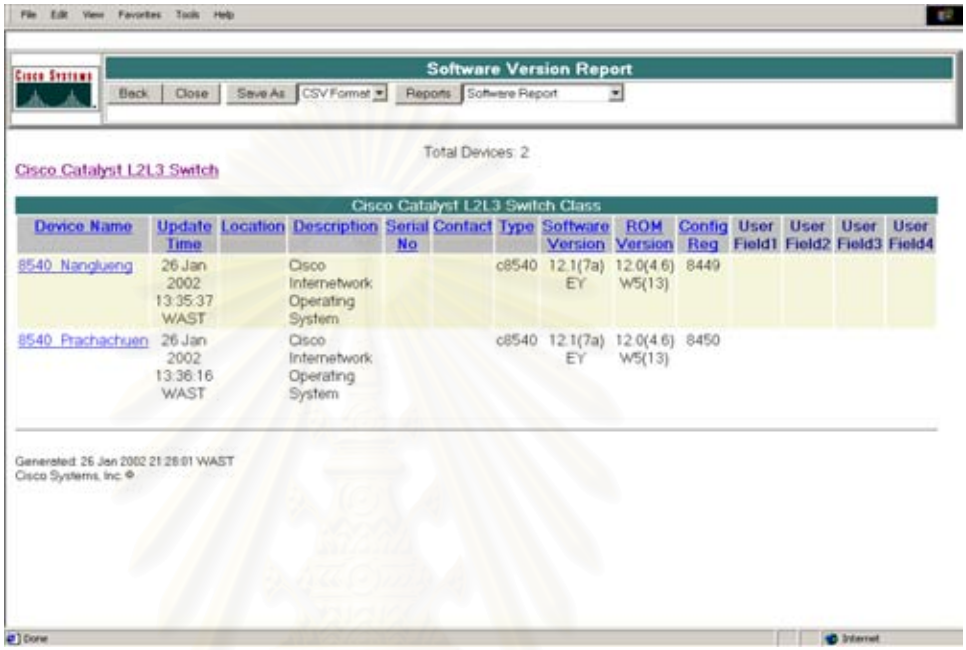
- Software Version Graph

  เป็นการตรวจสอบรายละเอียดทาง Software ของอุปกรณ์ เครือข่าย โดยจะแจกแจงรายละเอียดตามชนิดของอุปกรณ์ แล้วจึงลงในรายละเอียดของอุปกรณ์นั้นๆ อาทิ เช่น อุปกรณ์นั้นๆใช้ IOS หรือ Catalyst OS รุ่นใด เป็นแบบไหน แสดงดังรูปที่ 4.1.2.13

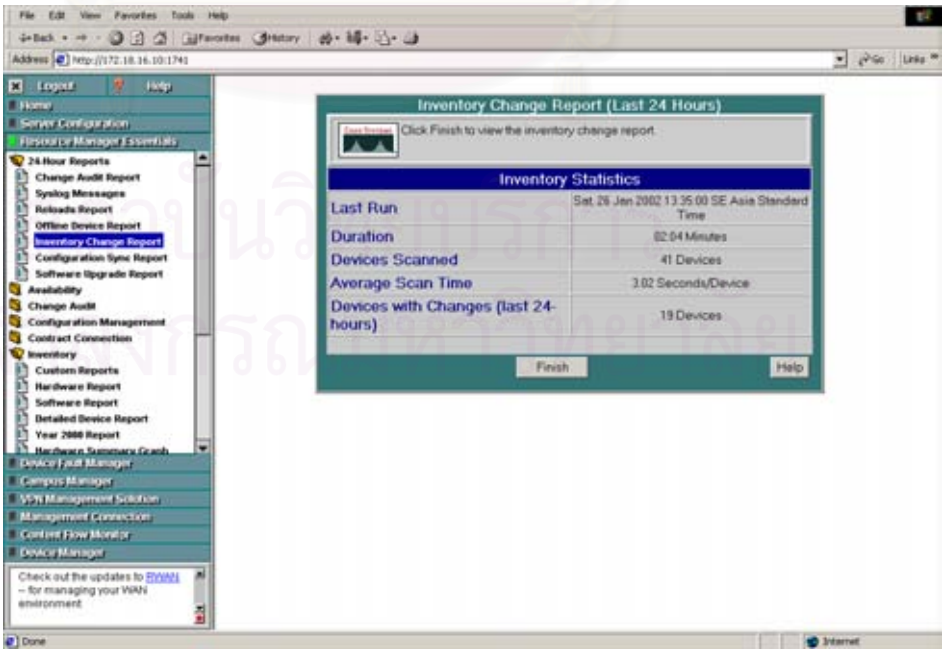
- Inventory Change

  เป็นเครื่องมือที่ใช้ในการตรวจสอบการเปลี่ยนแปลงภายในระบบ เครือข่าย ระบบจะทำการสแกนหาอุปกรณ์และบอกจำนวนอุปกรณ์ที่มีการเปลี่ยนแปลงในช่วง 24 ชั่วโมง และถ้าต้องการดูในรายละเอียดสามารถกด Finish ซึ่งระบบจะแสดงอุปกรณ์และเลือก

ดูแต่ละอุปกรณ์ได้ แสดงได้ดังรูปที่ 4.1.2.14



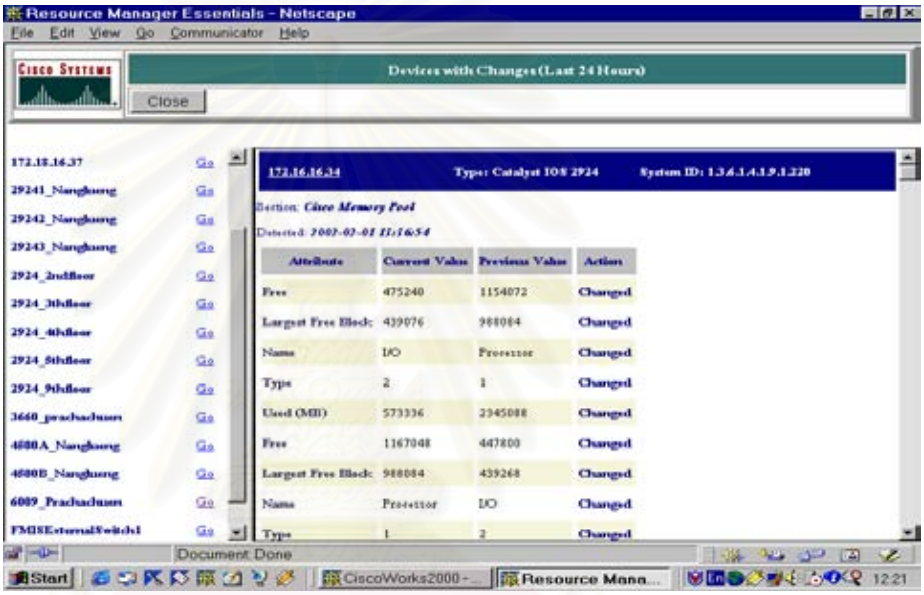
รูปที่ 4.1.2.13 แสดงลักษณะหน้าจอของรายงานซอฟท์แวร์ (Software Report)



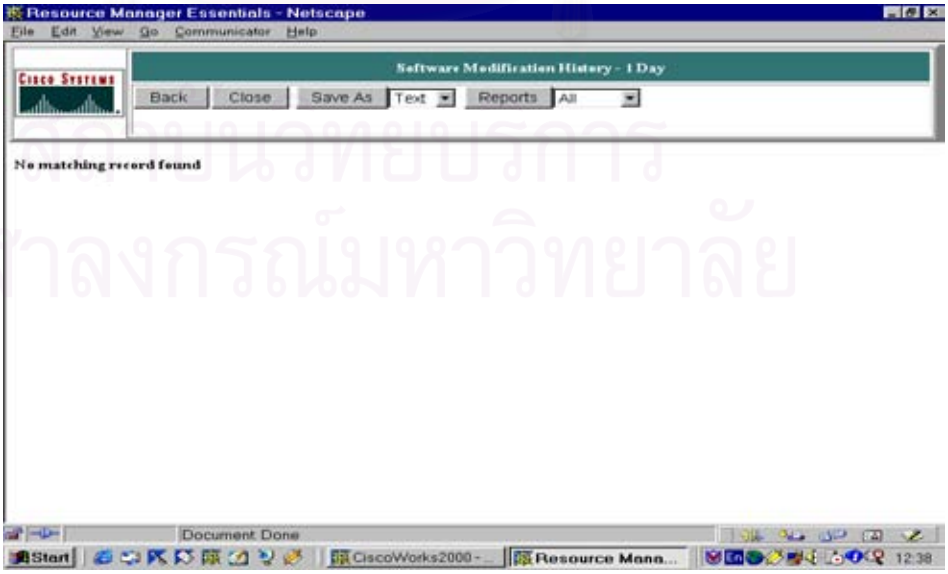
รูปที่ 4.1.2.14 แสดงลักษณะหน้าจอของ Inventory Change

- Software Upgrade History

  หากต้องการทราบว่ามีการเปลี่ยนแปลง Software OS (IOS, Catalyst OS) ของอุปกรณ์เครือข่ายหรือไม่ เลือกที่ Software Upgrade History ซึ่งในกรณีนี้จะมีการเปลี่ยนแปลงค่อนข้างน้อยมากหากไม่พบการเปลี่ยนแปลงระบบ ก็จะแสดงข้อมูลว่าไม่มีการเปลี่ยนแปลง แสดงได้ดังรูปที่ 4.1.2.15 และรูปที่ 4.1.2.16



รูปที่ 4.1.2.15 แสดงลักษณะหน้าจอของ Inventory Change (1)

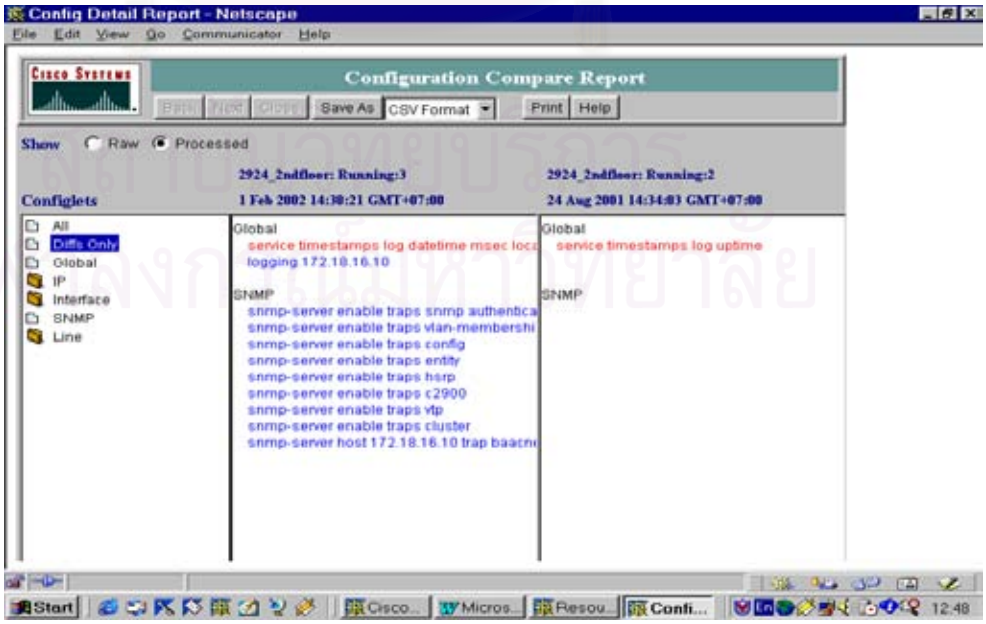


รูปที่ 4.1.2.16 แสดงลักษณะหน้าจอของ Inventory Change (2)

- **Change Audit**

  แสดงการเปลี่ยนแปลง/ แก้ไข ค่าการใช้งานต่างๆ ใน CISCO Work 2000 Server โดยสามารถตรวจสอบได้ว่า การเปลี่ยนแปลงนั้นๆ ถูกกระทำโดย Account user ใดและกระทำอย่างไร เมื่อเวลาใด และดูรายละเอียดได้อีกด้วย แสดงในรูปที่ 4.1.2.17 และรูปที่ 4.1.2.18

รูปที่ 4.1.2.17 แสดงลักษณะหน้าจอของรายงาน Change Audit

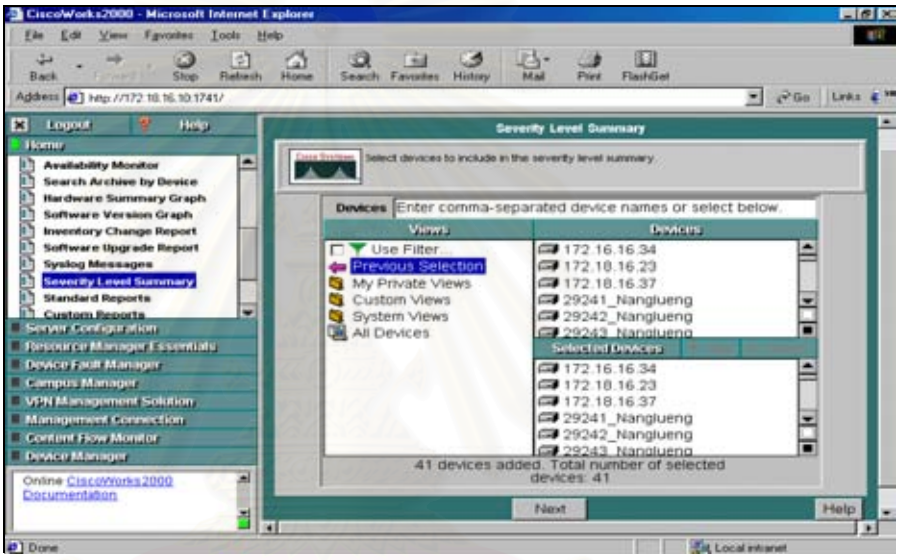


รูปที่ 4.1.2.18 แสดงรายงานการเปรียบเทียบการ Configuration

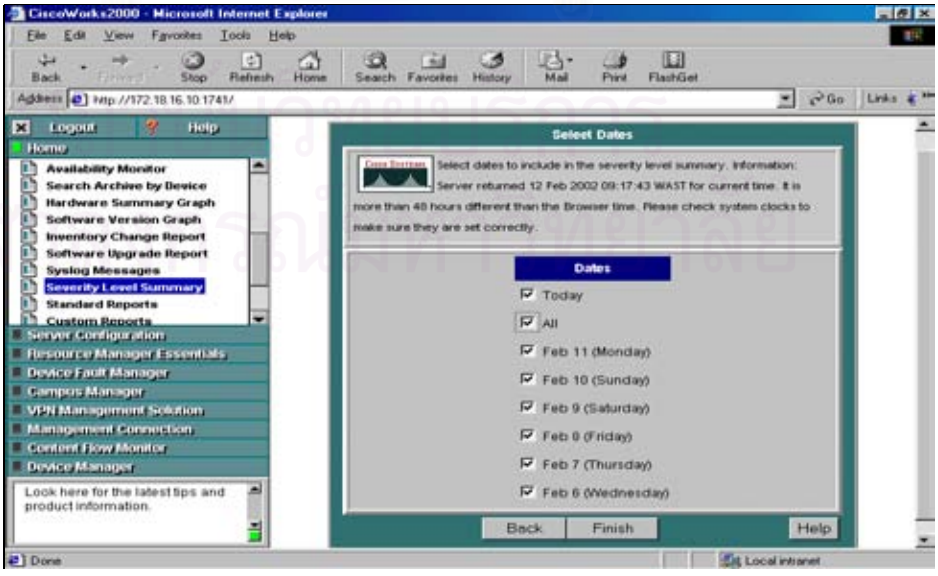
4) **รายละเอียดของการแสดงรายงานต่าง ๆ**

- Severity Level Report

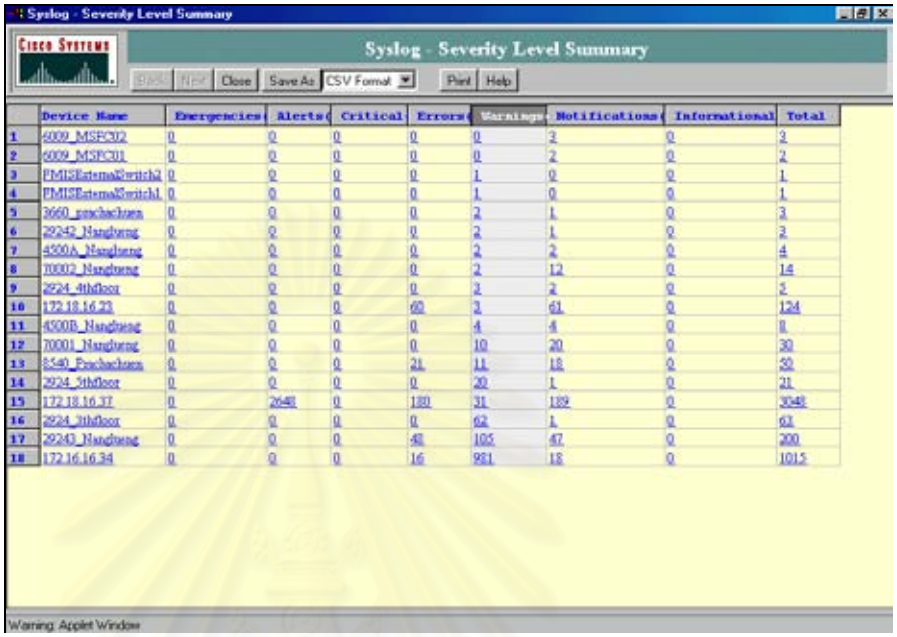
แสดงรายงานตามระดับของความรุนแรงของปัญหาโดยสามารถเลือกอุปกรณ์ และวันที่ต้องการทราบ จากวันปัจจุบันย้อนไปอีก 7 วัน หรือจะให้แสดงทั้ง 7 วันก็ได้ และสามารถดูรายละเอียดของแต่ละระดับความรุนแรงได้อีกด้วย ดังแสดงในรูปที่ 4.1.2.18 ถึงรูปที่ 4.1.2.22



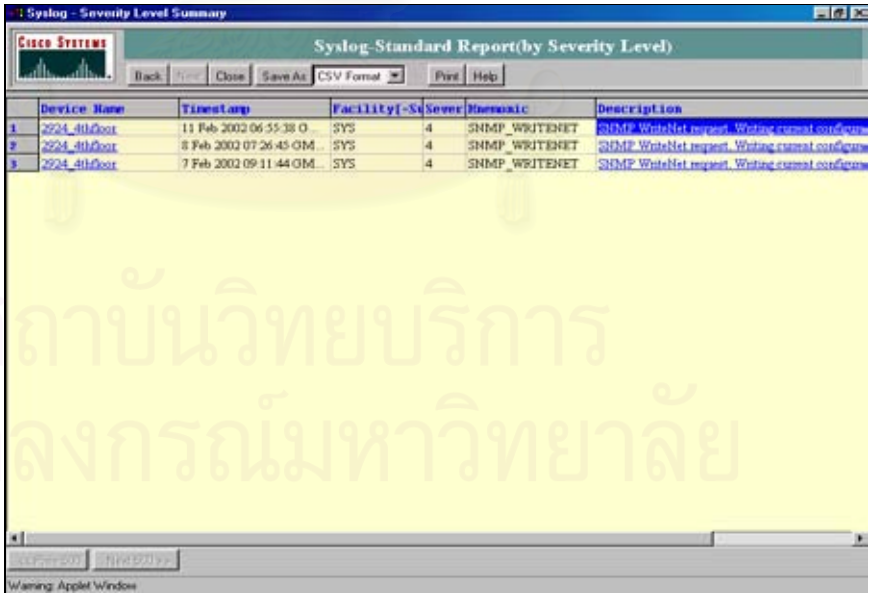
รูปที่ 4.1.2.18 แสดงหน้าจอแรกเพื่อเลือกอุปกรณ์ที่ต้องการดูรายงาน



รูปที่ 4.1.2.19 แสดงหน้าจอเพื่อเลือกวันที่ ที่ต้องการดูรายงาน



รูปที่ 4.1.2.20 แสดงระดับของความผิดพลาด (Error level)

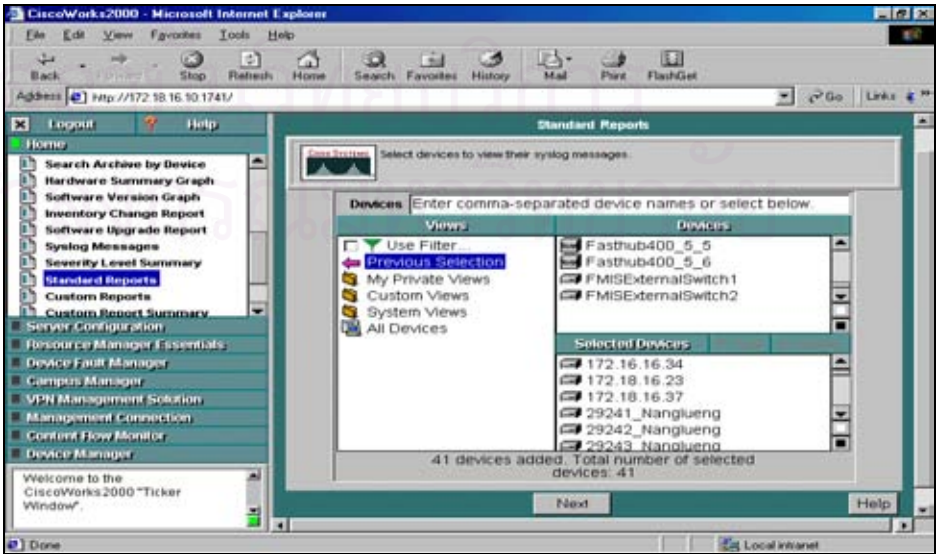


รูปที่ 4.1.2.21 แสดง SYSLOG ที่เกี่ยวข้องกับอุปกรณ์

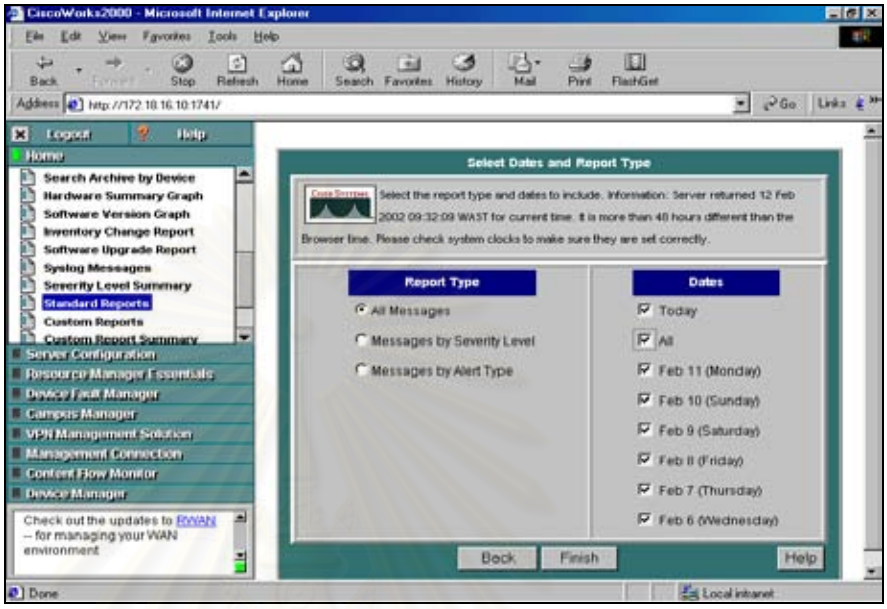
รูปที่ 4.1.2.22 แสดงรายละเอียด SYSLOG Message

- Standard Report

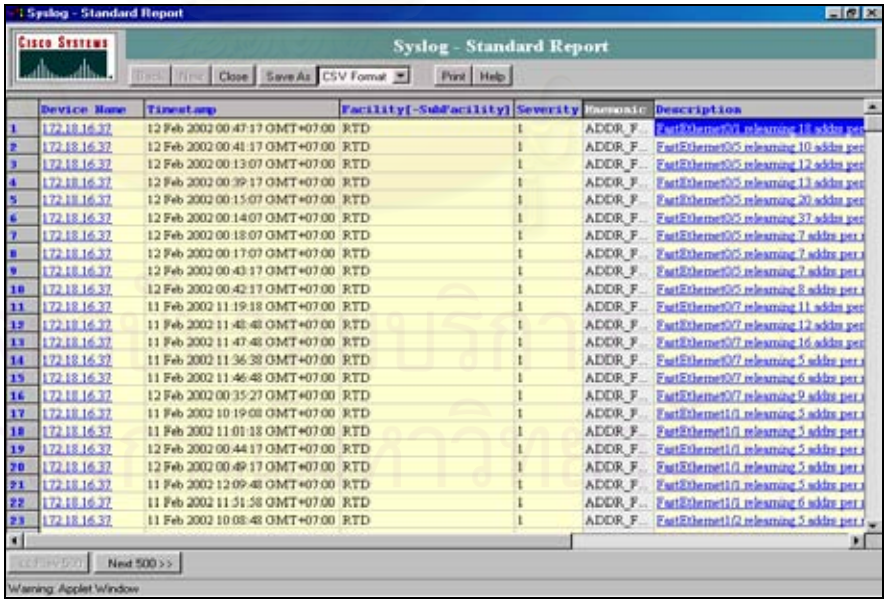
  แสดง Messages และสามารถเลือกวันที่แสดงรายงานได้ จากวันที่ปัจจุบันย้อนหลังไป อีก 7 วัน หรือจะแสดงทั้งหมด และเลือกอุปกรณ์ได้ตามที่ต้องการ ดังแสดงในรูปที่ 4.1.2.23 ถึงรูปที่ 4.1.2.26



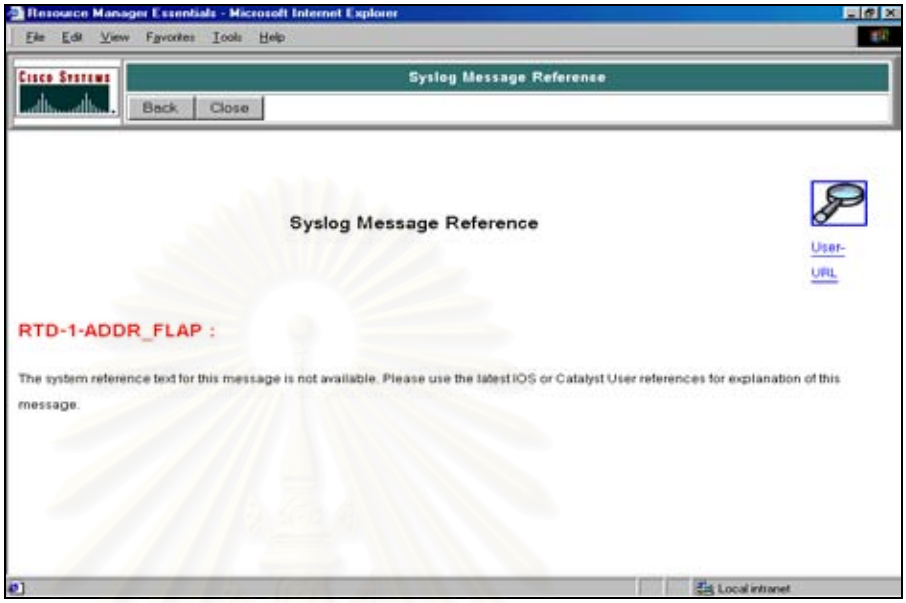
รูปที่ 4.1.2.23 แสดงหน้าจอแรกเพื่อเลือกอุปกรณ์ที่ต้องการดูรายงาน



รูปที่ 4.1.2.24 แสดงการเลือก Message และวันที่ ที่ต้องการดูรายงาน



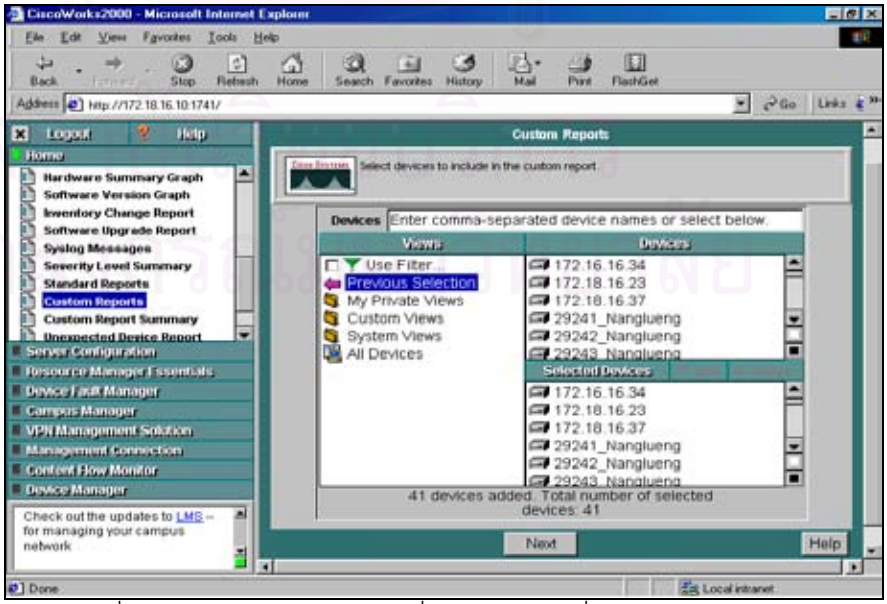
รูปที่ 4.1.2.25 แสดงรายละเอียด Syslog ของอุปกรณ์



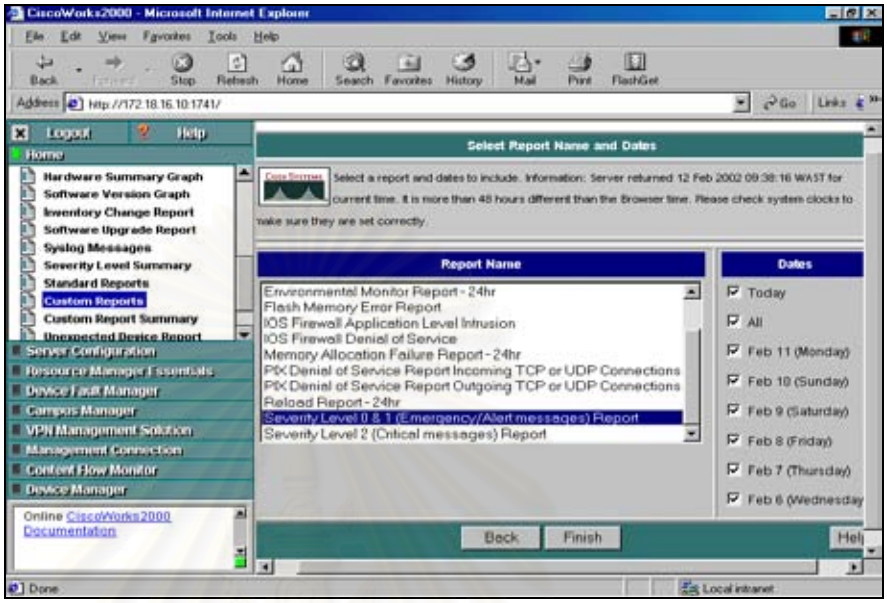
รูปที่ 4.1.2.26 แสดงรายละเอียดของ Syslog Message Reference

- Custom Report

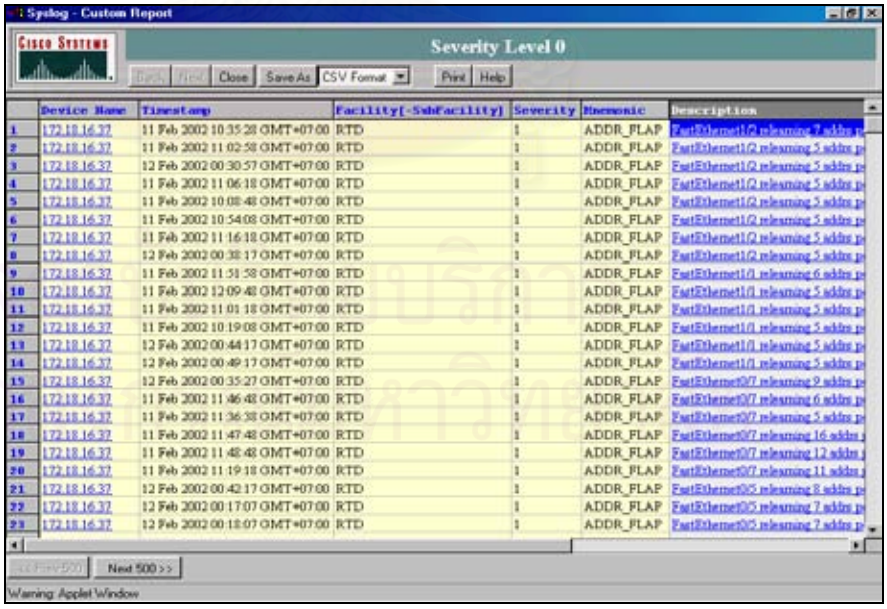
แสดงรายงานแยกตามประเภทของปัญหา และตาม Product เช่น Duplicate IP Report, Flash Memory Error Report เป็นต้น และสามารถเลือกอุปกรณ์ และวันที่ ดังแสดงในรูปที่ 4.1.2.27 ถึงรูปที่ 4.1.2.30



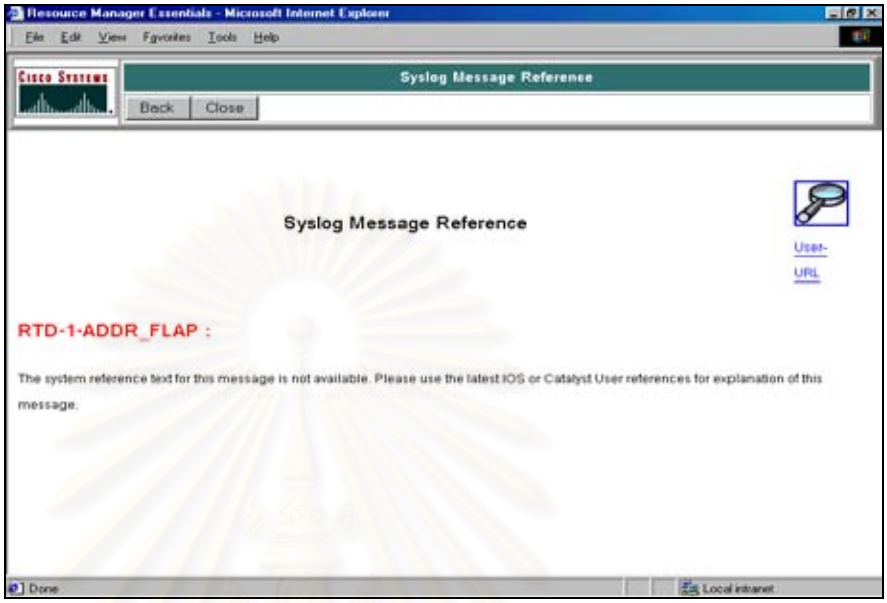
รูปที่ 4.1.2.27 แสดงหน้าจอแรกเพื่อเลือกอุปกรณ์ที่ต้องการดูรายงาน



รูปที่ 4.1.2.28 เลือกกลุ่มและวันที่ ที่ต้องการทำรายงาน



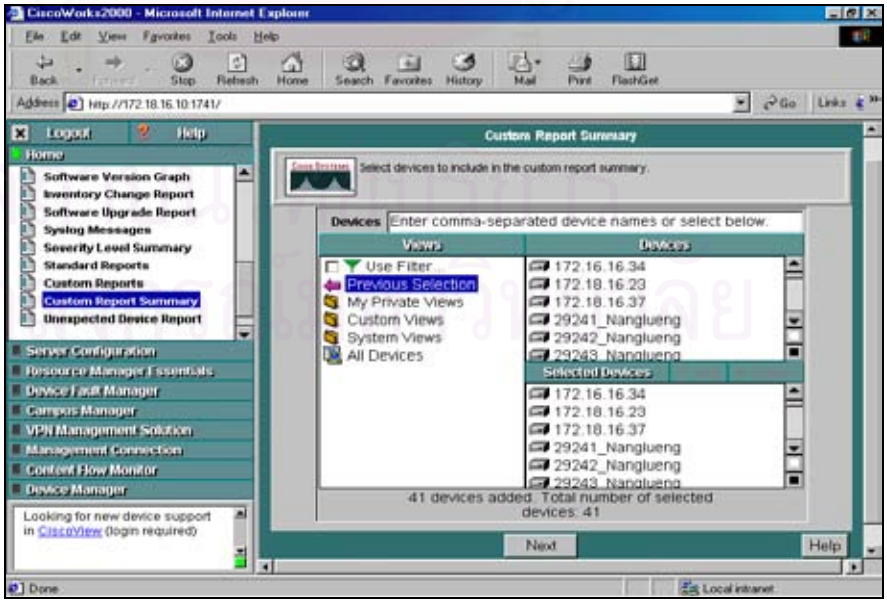
รูปที่ 4.1.2.29 แสดงรายละเอียด Syslog ของอุปกรณ์



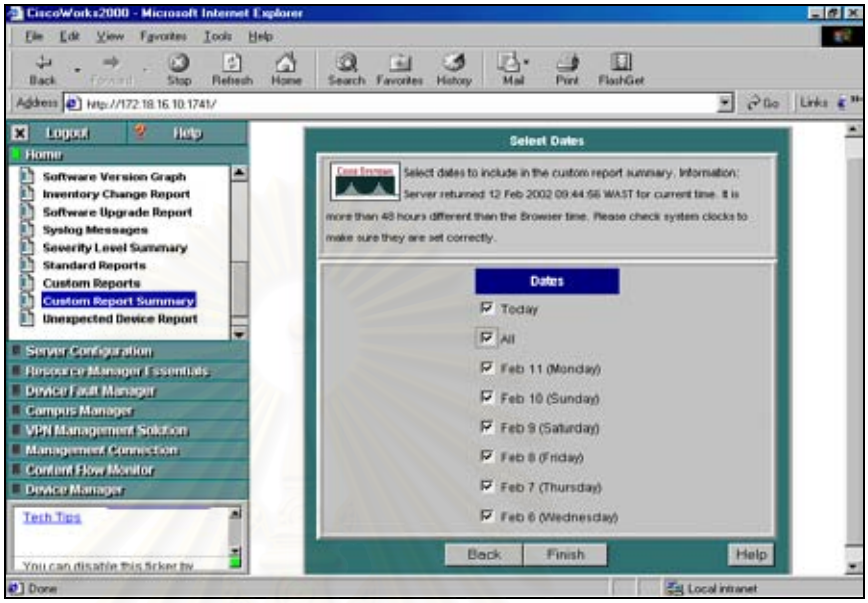
รูปที่ 4.1.2.30 แสดง Syslog Message Reference

- Custom Reports Summary

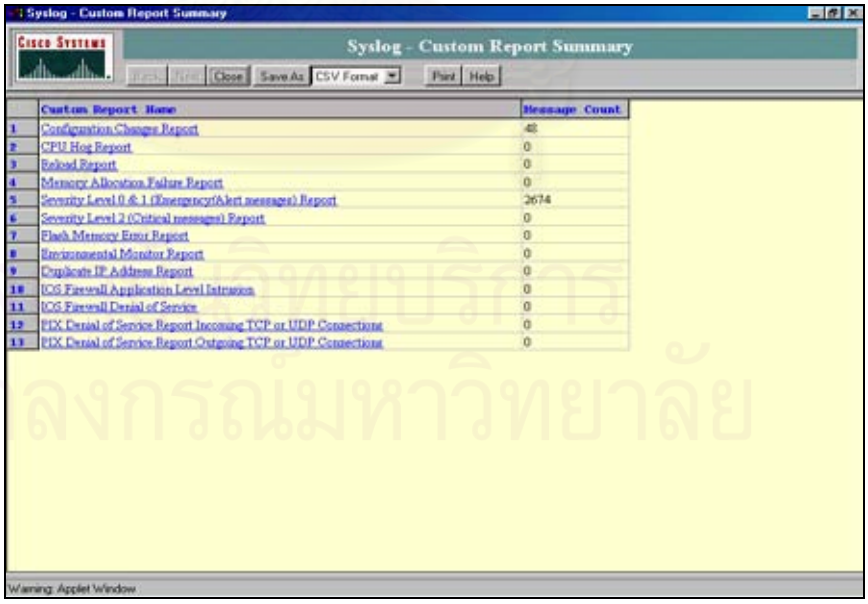
แสดงรายงานสรุปแยกตามปัญหาที่เกิดโดยรวมปัญหาแต่ละประเภทของแต่ละอุปกรณ์ตามที่เลือก และเลือกวันที่จะแสดง ดังแสดงในรูปที่ 4.1.2.31 ถึงรูปที่ 4.1.2.33



รูปที่ 4.1.2.31 แสดงหน้าจอแรกเพื่อเลือกอุปกรณ์ที่ต้องการดูรายงาน



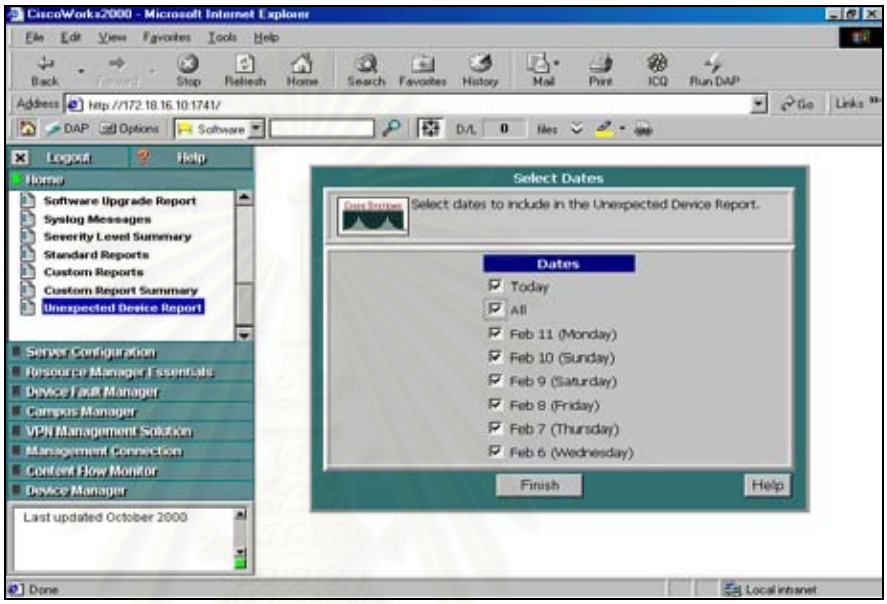
รูปที่ 4.1.2.32 แสดงการเลือกวันที่ ที่ต้องการดูรายงาน



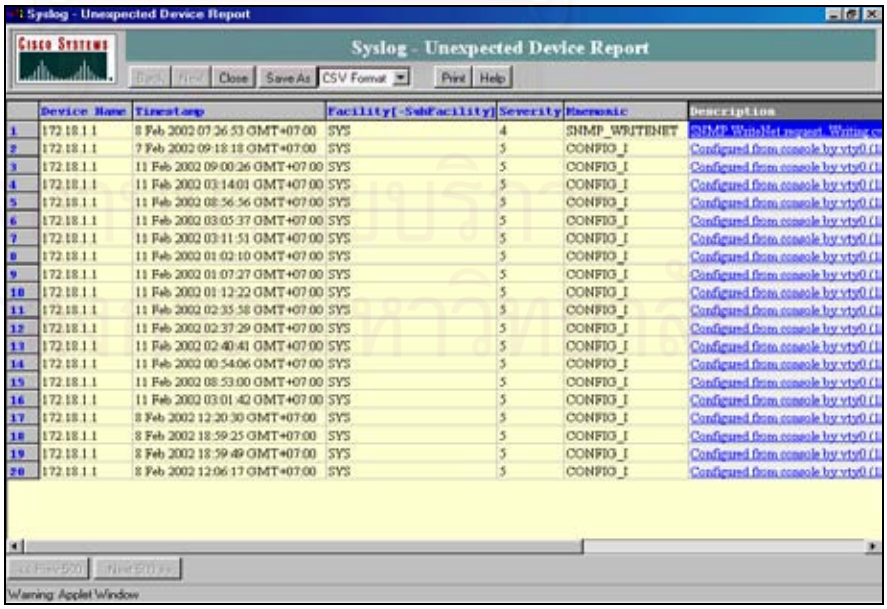
รูปที่ 4.1.2.33 แสดงรายงานโดยสรุปของปัญหากลุ่มต่าง ๆ

- Unexpected Device Report

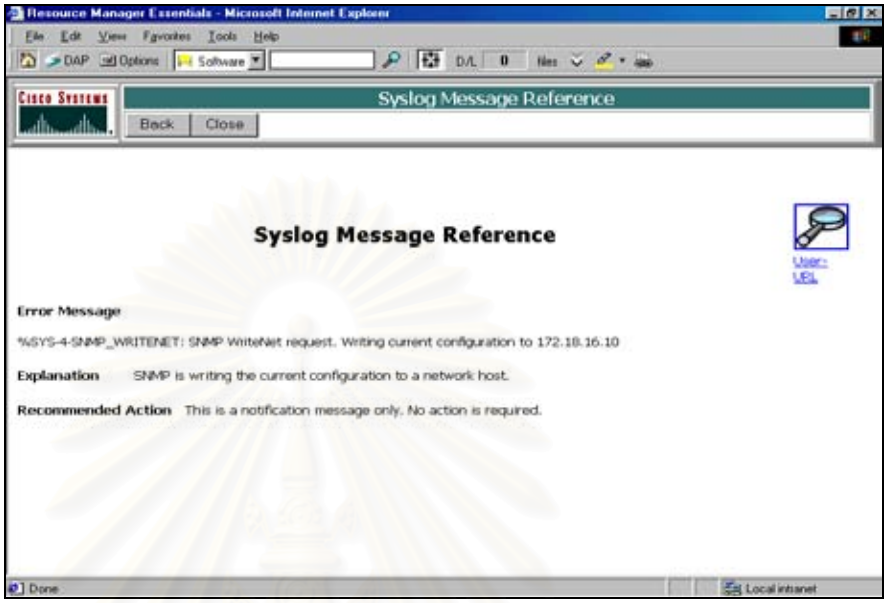
แสดงรายงานของอุปกรณ์ที่ไม่ใช่ Cisco แต่ Support SNMP และเกิดปัญหาตามวันที่เลือก ดังแสดงในรูปที่ 4.1.2.34 ถึงรูปที่ 4.1.2.36



รูปที่ 4.1.2.34 เลือกวันที่ ที่ต้องการทำงายงาน



รูปที่ 4.1.2.35 แสดงรายละเอียด Syslog ของอุปกรณ์



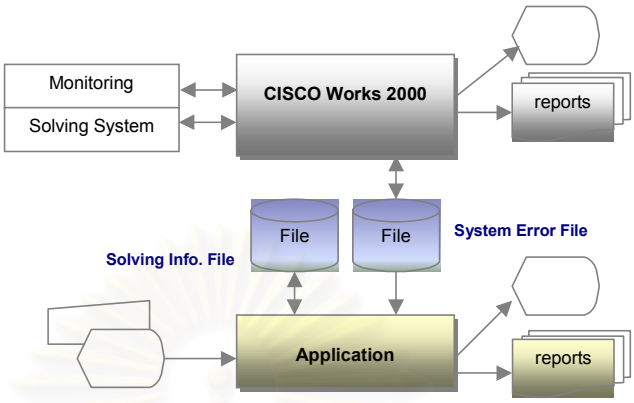
รูปที่ 4.1.2.36 แสดง Syslog Message Reference

ตัวอย่างลักษณะการใช้งานในโปรแกรม

http://172.18.16.10:1741/JSP/cmf/security/AutoLogin.jsp?URL=http://172.18.16.10:1741/cgi-bin/SYSLOGa/wizDeviceSelector.pl?sa_selection=20

4.1.3 ส่วนของการออกแบบโปรแกรมสนับสนุนการทำงานของระบบ

เป็นส่วนที่ออกแบบเพิ่มเติมในการวิเคราะห์ปัญหาที่เกิดขึ้นในระบบเครือข่ายและวิธีการแก้ไขปัญหา โดยมีการนำข้อมูลที่ได้มาจากระบบจัดการ CISCO Works 2000 ในส่วนของ SYSLOG ซึ่งเป็นแฟ้มข้อมูลที่เก็บสถานะของปัญหาของอุปกรณ์ในระบบ มาทำการวิเคราะห์การแก้ไขปัญหาที่เกิดขึ้นในระบบ รวมทั้งมีการออกแบบ แบบฟอร์มการใช้งานรวมของการเฝ้าติดตามและแก้ไขปัญหาเพื่อให้ผู้ใช้งานระบบเครือข่ายดำเนินการเป็นขั้นเป็นตอน ดังแสดงในผังระบบ (System Flow) ได้ดังรูปที่ 4.1.3.1



รูปที่ 4.1.3.1 แสดงผังระบบของการออกแบบโปรแกรมเชื่อมโยงกับ CISCO Works 2000

ในส่วนของการออกแบบโปรแกรมสนับสนุนการทำงานของระบบ ประกอบด้วยส่วนหลักๆ ดังนี้

- **ส่วนของการจัดการเกี่ยวกับข้อมูล** SYSLOG

  เป็นส่วนในการจัดการโหลดข้อมูล SYSLOG จากระบบ CISCO Works 2000 ในลักษณะของเท็กซ์ไฟล์ (Text File) โดยนำข้อมูลดังกล่าวมาเก็บในฟอร์แม็ทที่ฐานข้อมูลออกแบบรองรับไว้ เพื่อนำไปวิเคราะห์วิธีการแก้ไขปัญหา

- **ส่วนของการวิเคราะห์ปัญหาเกิดขึ้นในระบบ**

  เป็นส่วนที่ออกแบบระบบเพื่อรองรับการวิเคราะห์แก้ไขปัญหา ซึ่งประกอบด้วย

  - การเก็บอุปกรณ์ทั้งหมดที่ใช้ในระบบเครือข่าย
  - วิธีการแก้ไขปัญหาและอุปกรณ์ที่ต้องใช้ในการแก้ปัญหา

- **ส่วนของการออกแบบฟอร์มและรายงาน**

  เนื่องจากการปฏิบัติงานของเนตเวิร์ก โอเปอร์เรเตอร์ (Network Operator) ของหน่วยงานธ.ก.ส. ซึ่งเป็นหน่วยงานกรณีศึกษา ปฏิบัติงานตลอด 24 ชั่วโมง โดยแบ่งเป็น 3 กะ กะแรกตั้งแต่เวลา 7.00น. ถึง 15.00น. กะที่สอง ตั้งแต่เวลา 15.00 น. ถึง 23.00น. กะที่สาม ตั้งแต่เวลา 23.00 น. ถึง 7.00 น. ซึ่งในการดำเนินการปัจจุบันยังไม่มีรูปแบบและวิธีการปฏิบัติงานในส่วนของการเฝ้าติดตาม และแก้ไขปัญหาระบบแลน รวมถึงการส่งต่องานกันระหว่าง

กะ จึงจำเป็นอย่างยิ่งที่ต้องมีแบบฟอร์ม เพื่อให้เนตเวิร์ก โอเปอร์เรเตอร์ (Network Operator) ใช้ กำหนดเป็นขั้นตอนของการตรวจสอบอุปกรณ์ ตรวจสอบการเชื่อมต่อ ตรวจสอบการเปลี่ยนแปลงแก้ไขอุปกรณ์ ตรวจสอบ Performance ของอุปกรณ์ ตรวจสอบ Hardware / Software ขั้นตอนการออกรายงาน และขั้นตอนที่ต้องเนินการต่อ ดังแสดงในรูปแบบของจ็อบลิส (Job List) รูปที่ 4.1.3.2 จากจ็อบลิส (Job List) ดังกล่าว ทำให้สามารถเก็บแฟ้มข้อมูลของแบบฟอร์มไว้ได้และสามารถเรียกดูประวัติของแฟ้มข้อมูลโดยระบุวันที่ และกะที่ รวมทั้งสามารถพิมพ์แบบฟอร์มดังกล่าวเข้าแฟ้มงานประจำวันได้ตามที่ต้องการ

ในส่วนของการออกแบบรายงานที่ใช้ในการเฝ้าติดตามและแก้ไขปัญหาของระบบแลน ประกอบด้วยส่วนหลัก ๆ 4 ส่วนด้วยกัน คือ

- รายงานประจำวัน (Daily Report)
  รายงานการแก้ไขปัญหาจาก SYSLOG ประจำวัน

- รายงานประจำเดือน (Monthly Report)
  รายงานการแก้ไขปัญหาจาก SYSLOG ประจำเดือน

- รายงานประจำปี (Yearly Report)
  รายงานการแก้ไขปัญหาจาก SYSLOG ประจำปี

- รายงานสรุปการเกิดปัญหาจาก SYSLOG

แบบฟอร์มการเฝ้าติดตามและการแก้ไขปัญหาแลน (LAN)

ประจำวันที่ xx/xx/xxxx กะที่ x

ขั้นตอนการตรวจสอบอุปกรณ์

1. ☐ Reachability Dashboard
2. ☐ Availability Monitor
3. ☐ Syslog Message
   ☐ Save Syslog into CISCO log file
4. ☐ Trouble Shooting

สามารถพบวิธีการแก้ไขปัญหา ☐ ได้

☐ ไม่ได้ วิเคราะห์ต่อโดย ☐ 5. Path Analysis

☐ 6. User Tracking

ขั้นตอนการตรวจสอบการเชื่อมต่อ

7. ☐ Topology Service
8. ☐ Search Archive by Device
9. ☐ Cisco View

ขั้นตอนการตรวจสอบการเปลี่ยนแปลงอุปกรณ์

10. ☐ Inventory Charge Report
11. ☐ Software Upgrade History
12. ☐ Change Audit Report

ขั้นตอนการตรวจสอบสมรรถนะของอุปกรณ์

13. ☐ Reachability Trend
14. ☐ Response Time Trend

ขั้นตอนการตรวจสอบฮาร์ดแวร์และซอฟท์แวร์

15. ☐ Hardware summary Graph
16. ☐ Software Version Graph

ขั้นตอนการตรวจสอบออกรายงาน

17. ☐ Severity Level Summary
18. ☐ Standard Reports
19. ☐ Custom Reports
20. ☐ Custom Reports Summary
21. ☐ Unexpected Device Report
    ☐ Trouble Shooting and Equipment List Report

ปัญหาที่อยู่ในระหว่างการแก้ไข สิ่งที่ต้องดำเนินการต่อ

....
....
....
....

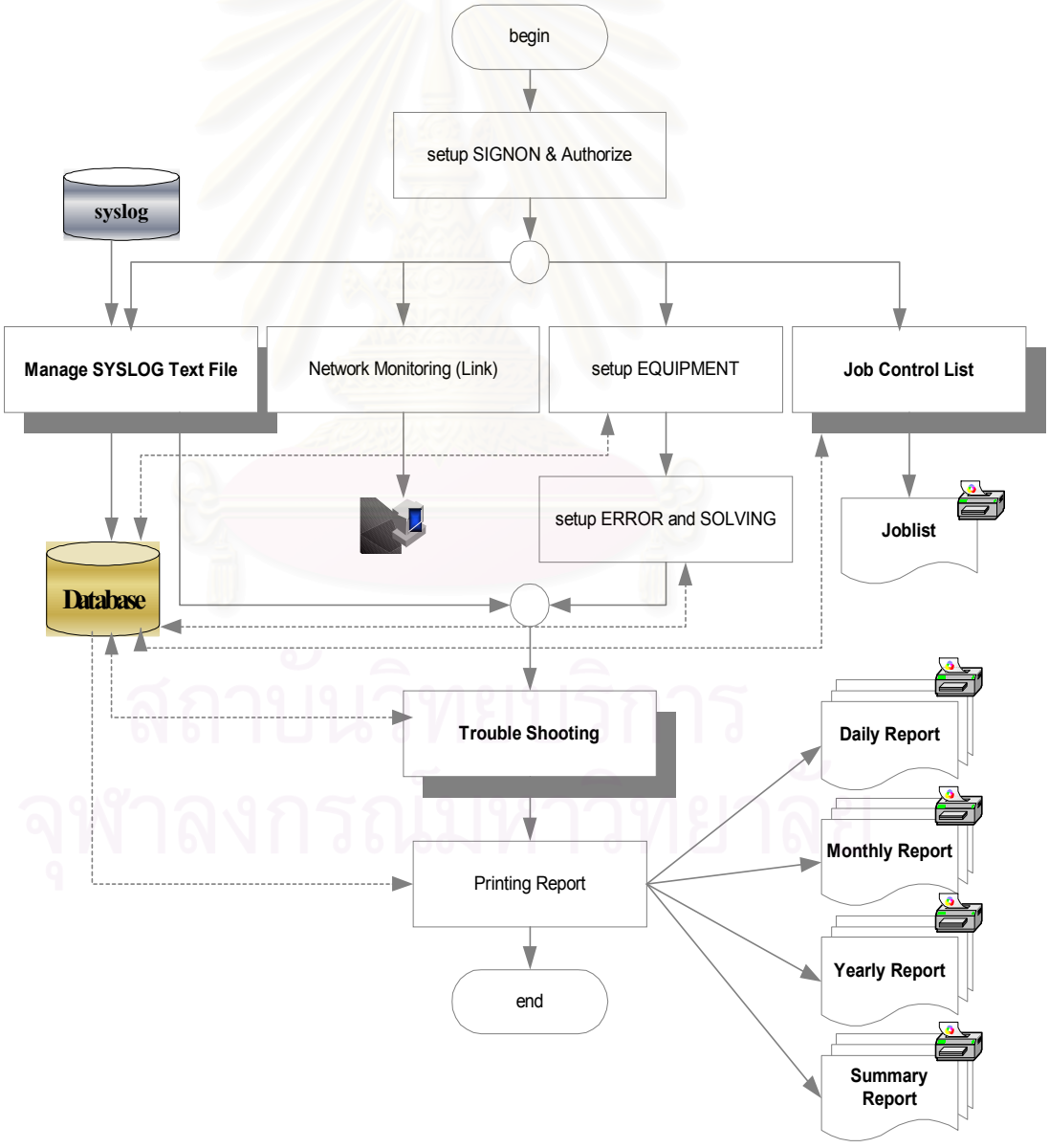
ผู้ปฏิบัติงาน ผู้ควบคุมกะ

เวลาผู้ปฏิบัติงาน เวลาผู้ควบคุมกะ

รูปที่ 4.1.3.2 แสดงลักษณะแบบฟอร์มการติดตามงาน (Job List)

4.2 ขั้นตอนการออกแบบโปรแกรม

ในส่วนของการวิเคราะห์และออกแบบโครงสร้างแฟ้มข้อมูลและผังระบบ ได้มีการออกแบบโครงสร้างแฟ้มข้อมูลรองรับตัวโครงสร้างไฟล์ของ SYSLOG แล้วจึงมีการส่งต่อข้อมูลไหลเข้าสู่ระบบ เพื่อนำข้อมูลเข้ามาทำการวิเคราะห์ปัญหาที่เกิดขึ้นในลักษณะงานที่เป็นเสมือนแฟ้มข้อมูลเก็บประวัติการแก้ไขปัญหาที่เกิดขึ้น ดังนั้นการทำงานของระบบที่ทำการออกแบบสามารถแสดงได้ดังรูปที่ 4.2.1



รูปที่ 4.2.1 แสดงลักษณะการทำงานของระบบที่ทำการออกแบบ

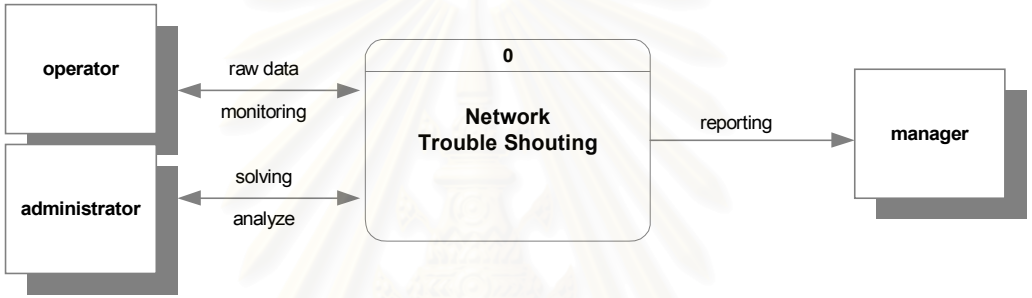
ดังนั้นแฟ้มข้อมูลทั้งหมดของระบบประกอบด้วยแฟ้มข้อมูลทั้งหมด 11 แฟ้มข้อมูล และสามารถแสดงรายละเอียดได้ดังตารางที่ 4.2.1

ตารางที่ 4.2.1 แสดงแฟ้มข้อมูลที่ใช้ในระบบ

ชื่อแฟ้มข้อมูล	ชื่อย่อ	*รายละเอียด*	*จำนวนคอลัมน์*
solution_equipment	D1	แฟ้มข้อมูลการเก็บปัญหาที่เกิดขึ้นในระบบเครือข่าย (SYSLOG) ที่ได้มาจาก CISCO Works 2000	6
message_log	D2	แฟ้มข้อมูลการเก็บข้อมูลที่ใช้ในการแก้ไขปัญหา	8
t_codeequipment	D3	แฟ้มข้อมูลของรายการอุปกรณ์เครือข่าย	2
t_errorcode	D4	แฟ้มข้อมูลของความผิดพลาดที่เกิดขึ้น	3
t_historylog	D5	แฟ้มข้อมูลเก็บข้อมูลประวัติผู้ใช้ระบบ	4
t_icon	D6	แฟ้มข้อมูลเก็บข้อมูลการคอนโทรลไอคอน	2
t_authorize	D7	แฟ้มข้อมูลเก็บข้อมูลกำหนดสิทธิ์ผู้ใช้ระบบ	2
t_userstatus	D8	แฟ้มข้อมูลเก็บข้อมูลระดับของสิทธิ์การใช้งาน	2
help_authorize_working	D9	แฟ้มข้อมูลเก็บข้อมูลการกำหนดการทำงาน	3
help_authorize_user	D10	แฟ้มข้อมูลเก็บข้อมูลผู้ใช้ระบบ	6
joblist	D11	แฟ้มข้อมูลเก็บข้อมูลของการติดตามงาน	28

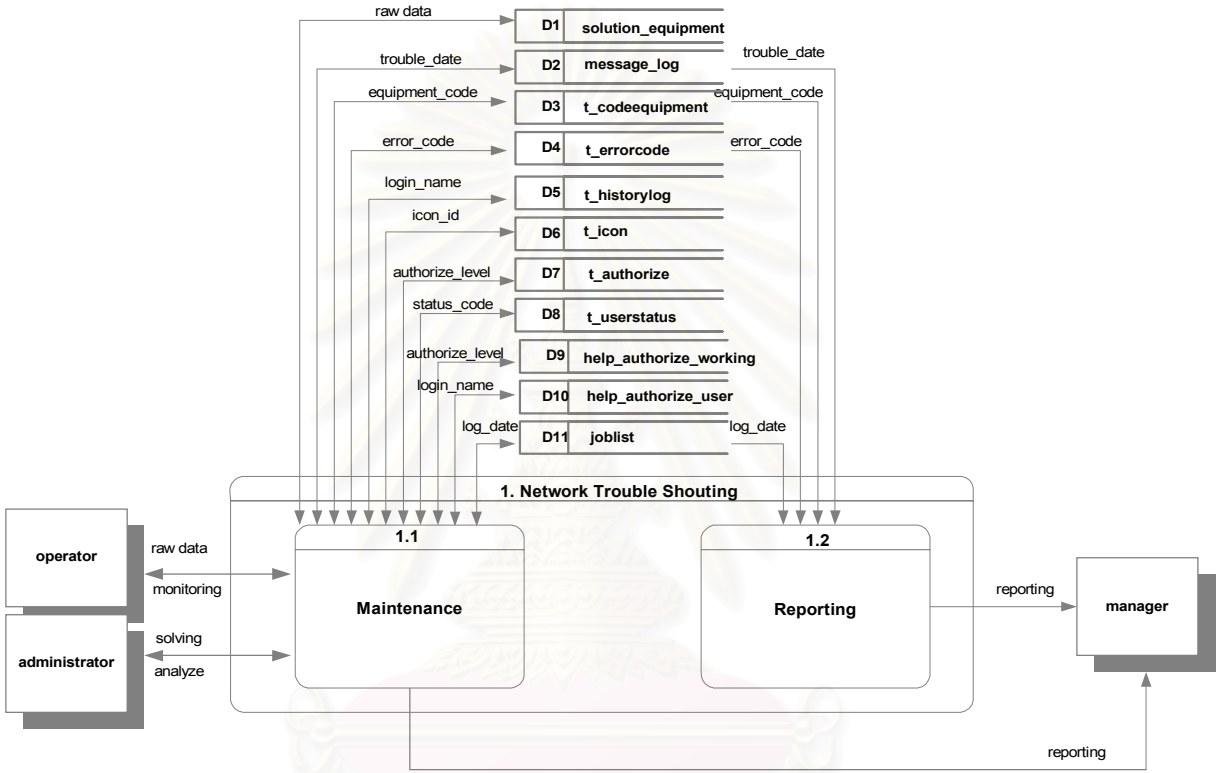
หมายเหตุ สามารถดูรายละเอียดของโครงสร้างแฟ้มข้อมูลได้ในภาคผนวก ข
ภาคผนวก ข - โครงสร้างแฟ้มข้อมูล

ดังนั้นระบบที่ทำการวิเคราะห์และออกแบบสามารถนำมาเขียนในรูปแบบของ Context Diagram และ DFD (Data Flow Diagram) แสดงได้ดังรูปที่ 4.2.2 และรูปที่ 4.2.4

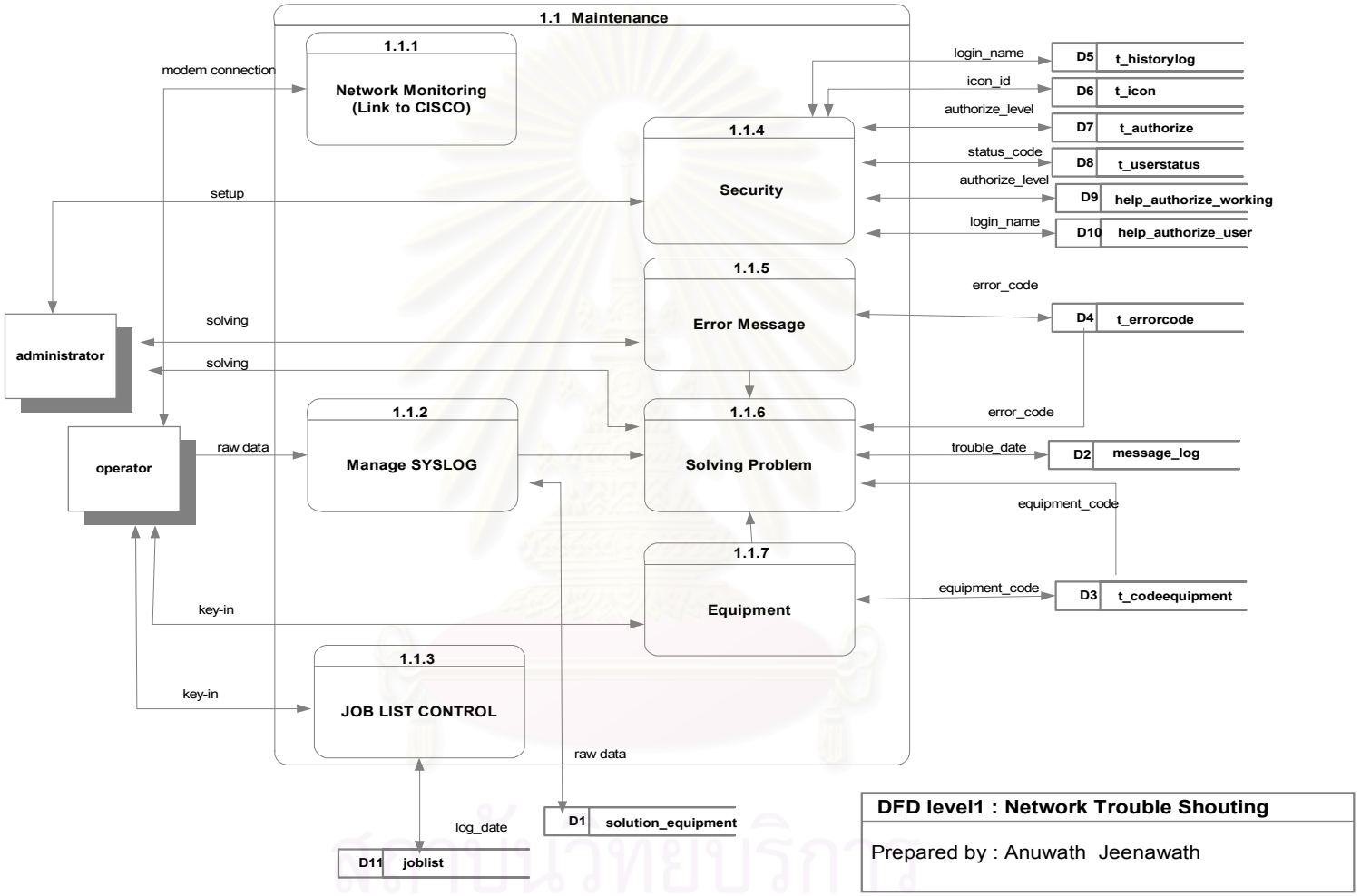


Context Diagram : Network Trouble Shouting
Prepared by : Anuwath Jeenawath

รูปที่ 4.2.2 แสดงลักษณะคอนแท็กซ์ไดอะแกรมของระบบที่ทำการออกแบบ (Context Diagram)



รูปที่ 4.2.3 แสดงลักษณะการไหลของแฟ้มข้อมูลในระดับศูนย์ (DFD level-0)



รูปที่ 4.2.4 แสดงลักษณะการไหลของแฟ้มข้อมูลในระดับหนึ่ง (DFD level-1)

องค์ประกอบของเครื่องมือ (Tools) ที่ใช้ในการออกแบบระบบ ประกอบด้วย

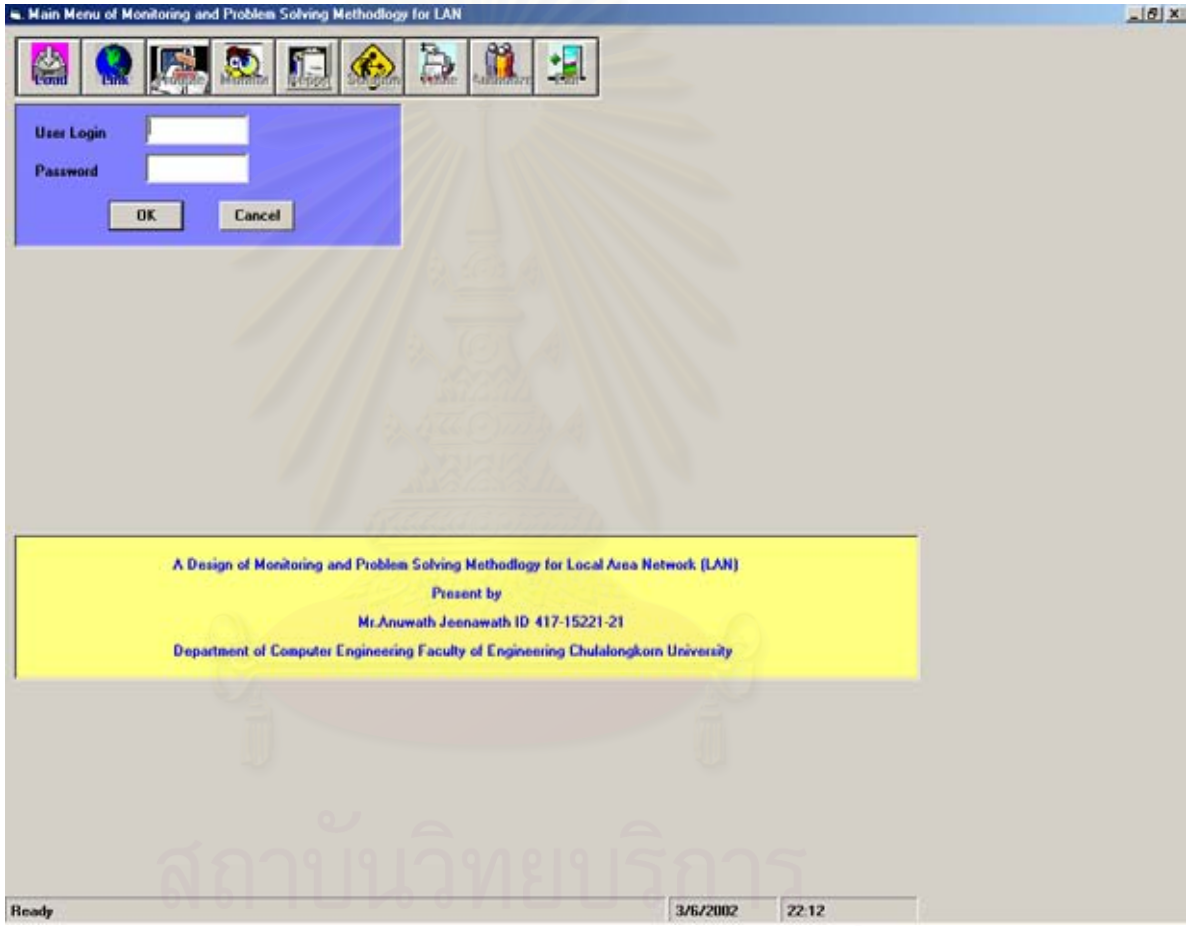
- Database Server : MSSQL version 7.0
- Programming Tools : Microsoft Visual Basic v.6.0
  Segate Crystal Report v.8.0

4.3 การออกแบบลักษณะหน้าจอของโปรแกรมระบบ

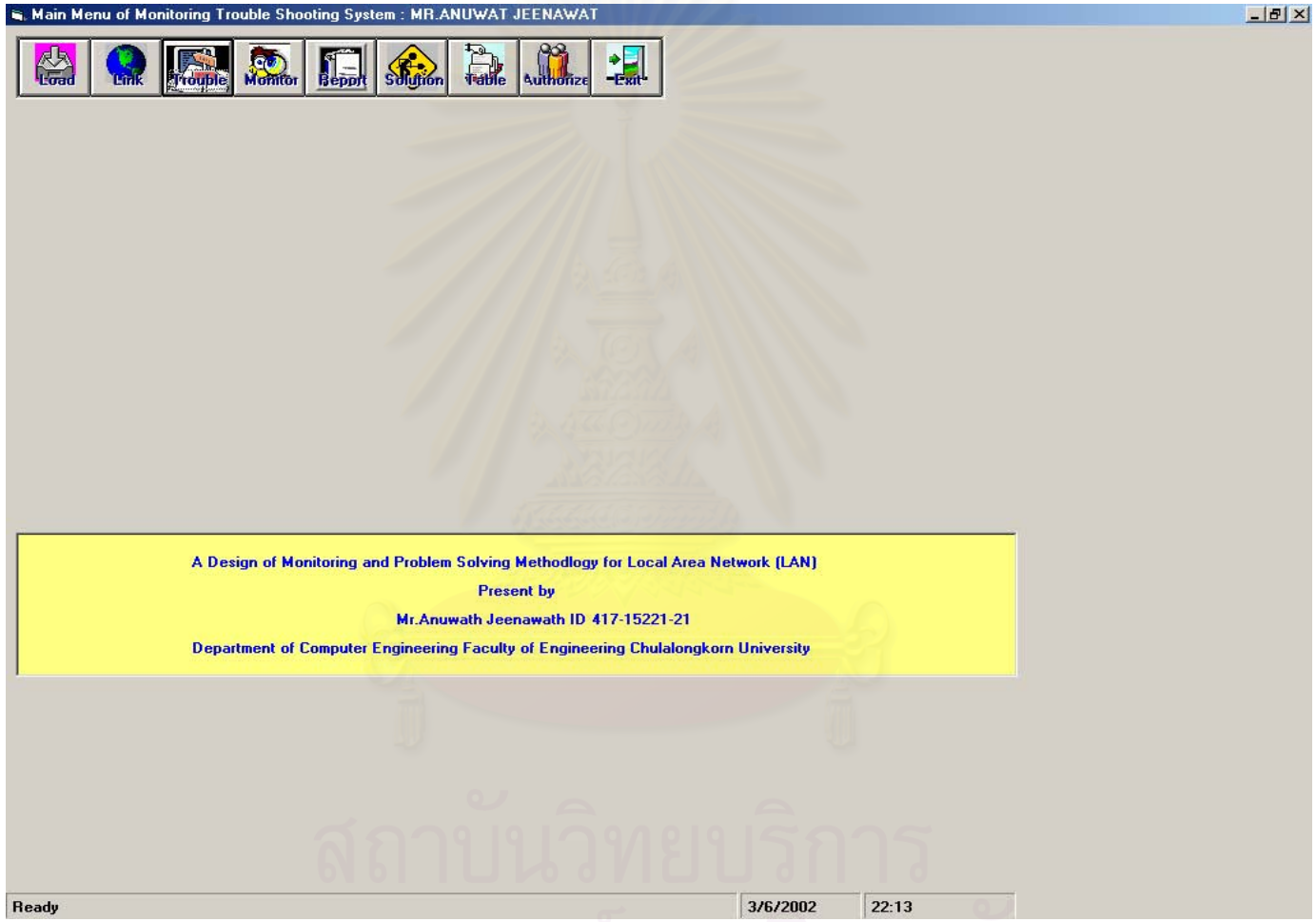
ลักษณะหน้าจอของระบบประกอบด้วย

- ลักษณะหน้าจอของการเข้าสู่ระบบ
- ลักษณะหน้าจอของการเชื่อมโยงไปยังระบบ CISCO Works 2000 (Network Monitor)
- ลักษณะหน้าจอของการจัดการเกี่ยวกับ SYSLOG
- ลักษณะหน้าจอของการกำหนดสิทธิ์การเข้าสู่ระบบและการใช้งาน
- ลักษณะหน้าจอของการจัดการ Table
- ลักษณะหน้าจอของการติดตามงาน (Job List Control)
- ลักษณะหน้าจอของการวิเคราะห์ปัญหา (Trouble Shooting)
- ลักษณะหน้าจอของการแก้ไขปัญหาและอุปกรณ์ที่ใช้ในการแก้ไข (Solving Problem)
- ลักษณะหน้าจอของการออกรายงาน

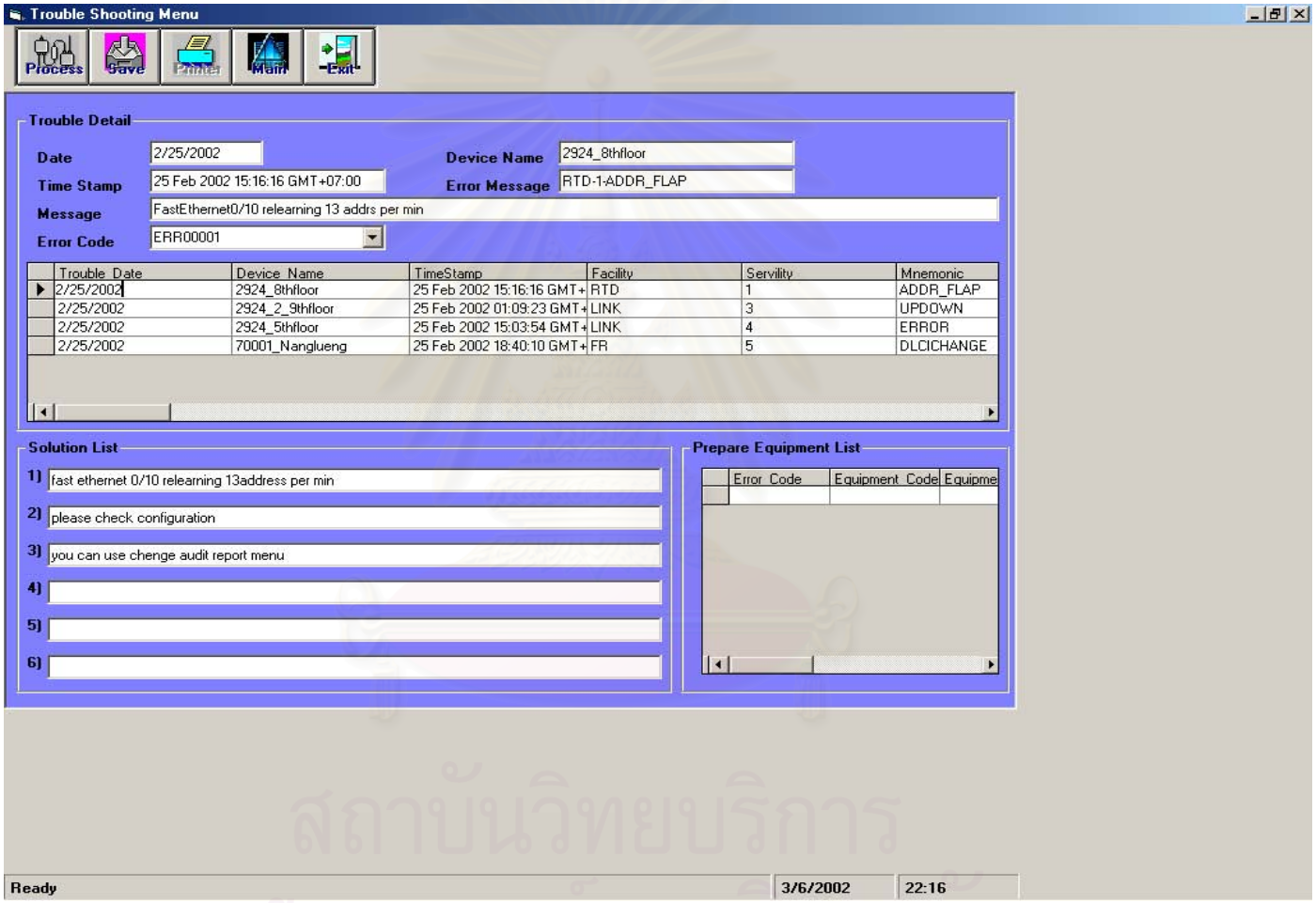
ทั้งนี้สามารถแสดงลักษณะหน้าจอดังกล่าวข้างต้น ได้ดังรูปที่ 4.3.1 ถึงรูปที่ 4.3.13



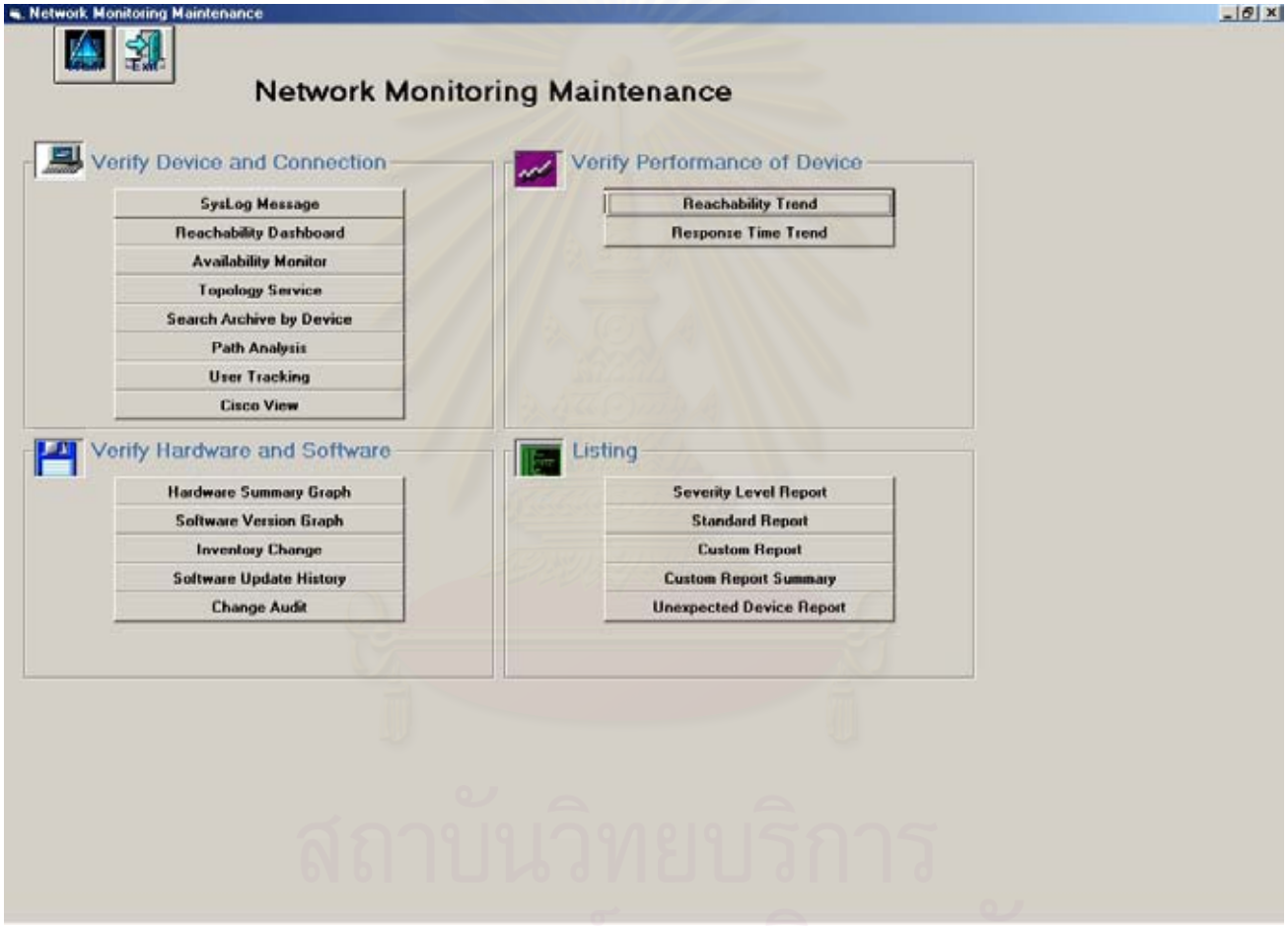
รูปที่ 4.3.1 แสดงลักษณะหน้าจอของการเข้าสู่ระบบ



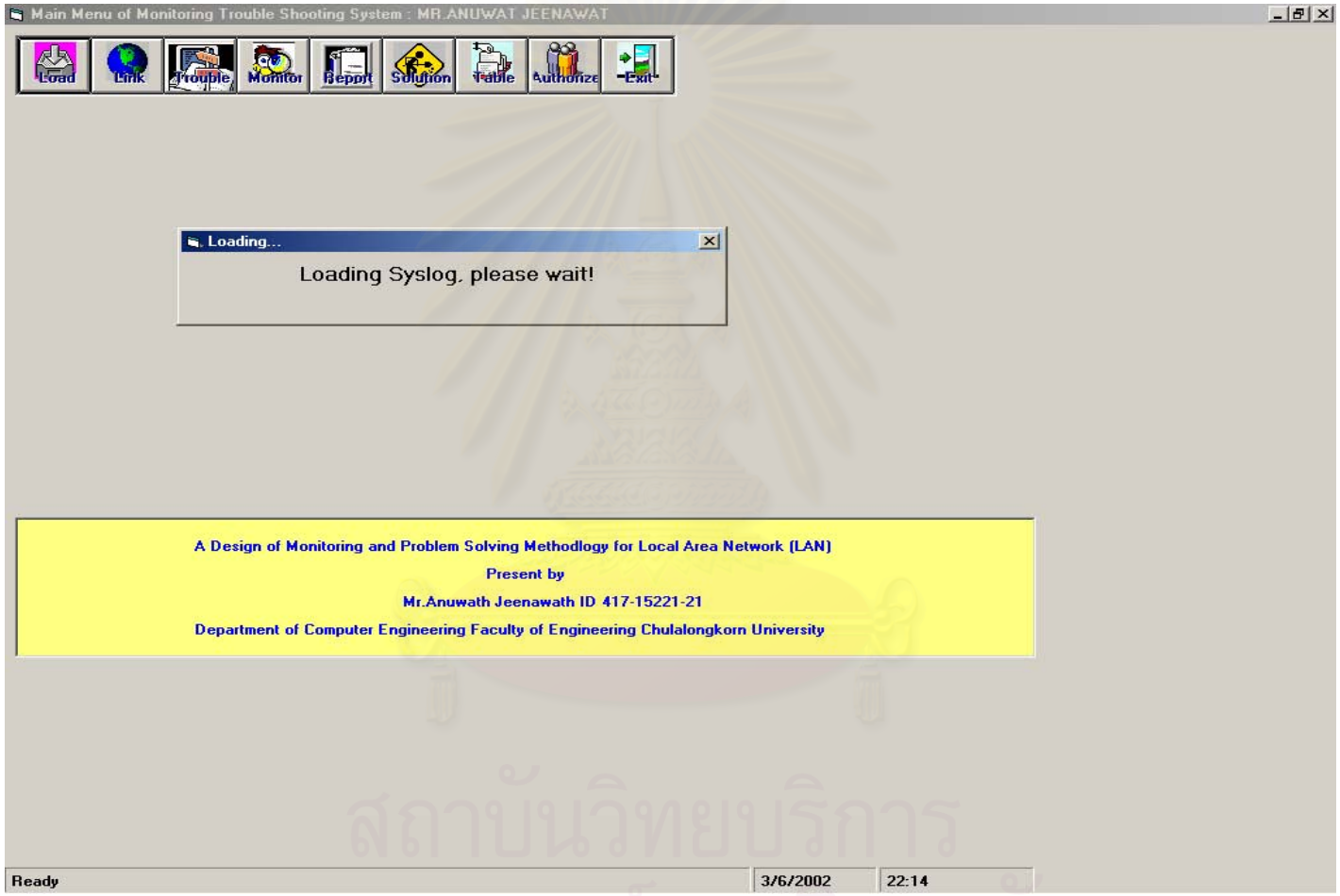
รูปที่ 4.3.2 แสดงลักษณะหน้าจอภายหลังการเข้าสู่ระบบ



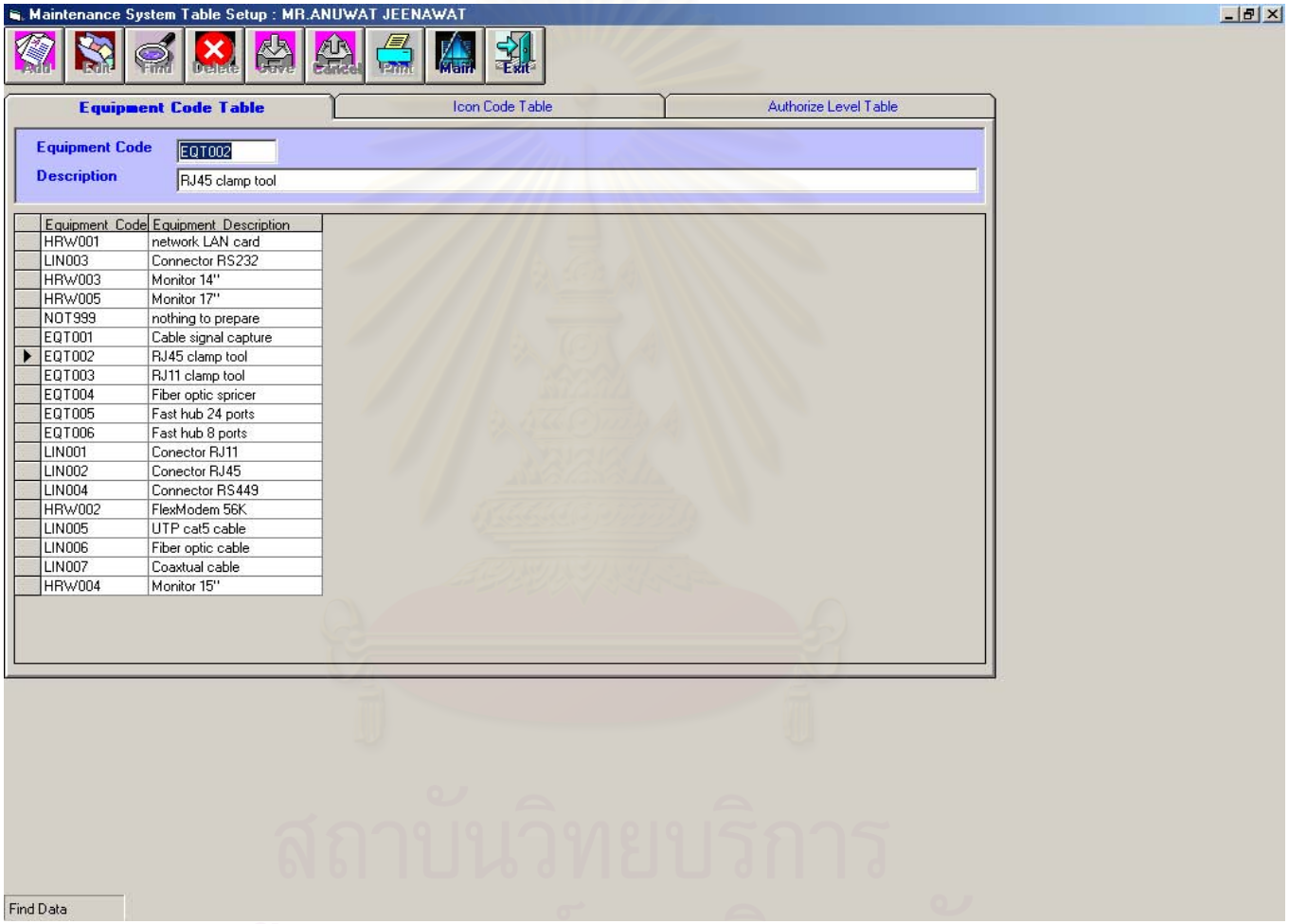
รูปที่ 4.3.3 แสดงลักษณะหน้าจอของ Trouble Shooting



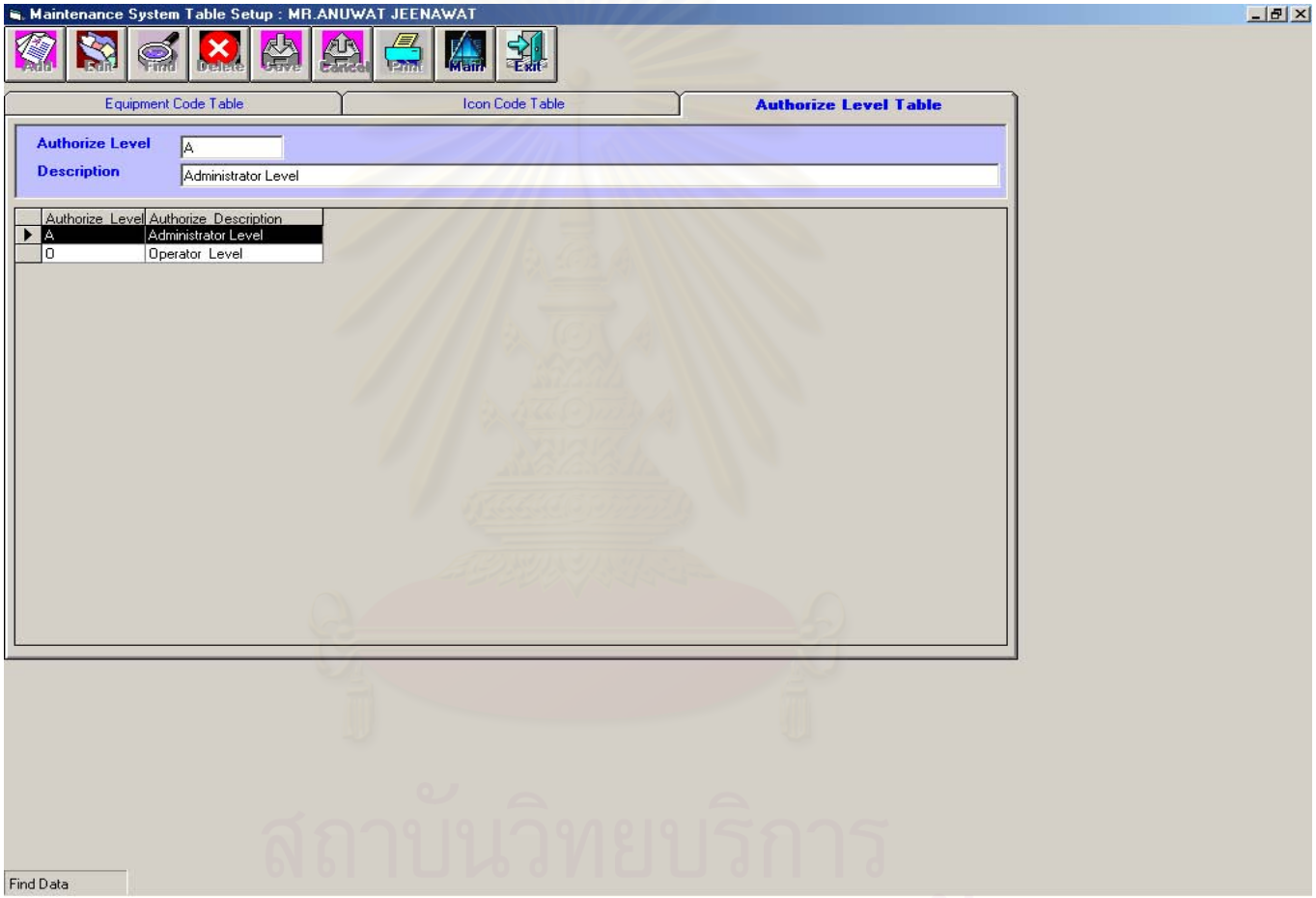
รูปที่ 4.3.4 แสดงลักษณะหน้าจอของการเชื่อมโยงไปยังระบบ CISCO Works 2000



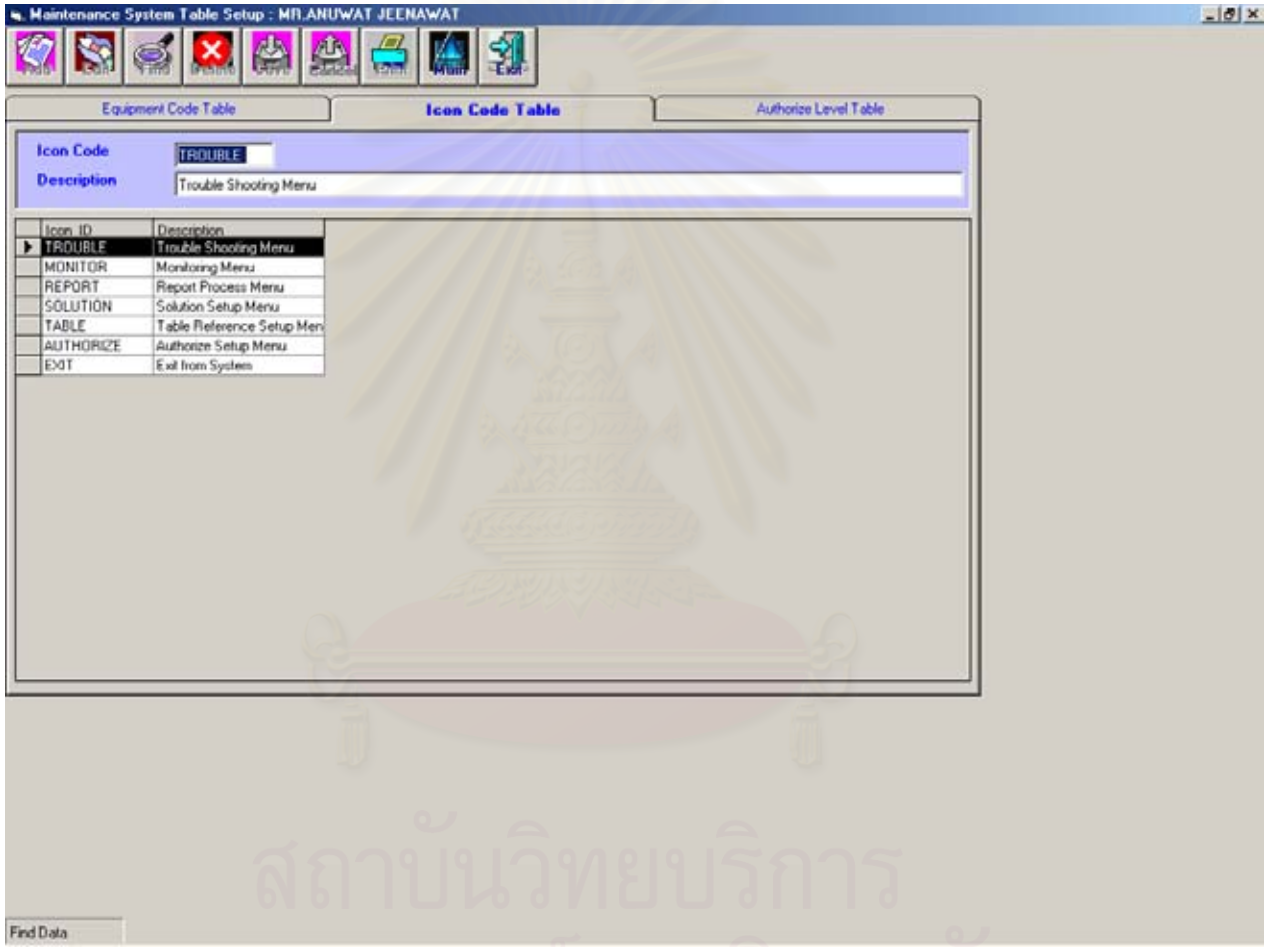
รูปที่ 4.3.5 แสดงลักษณะหน้าจอของการจัดการเกี่ยวกับ SYSLOG



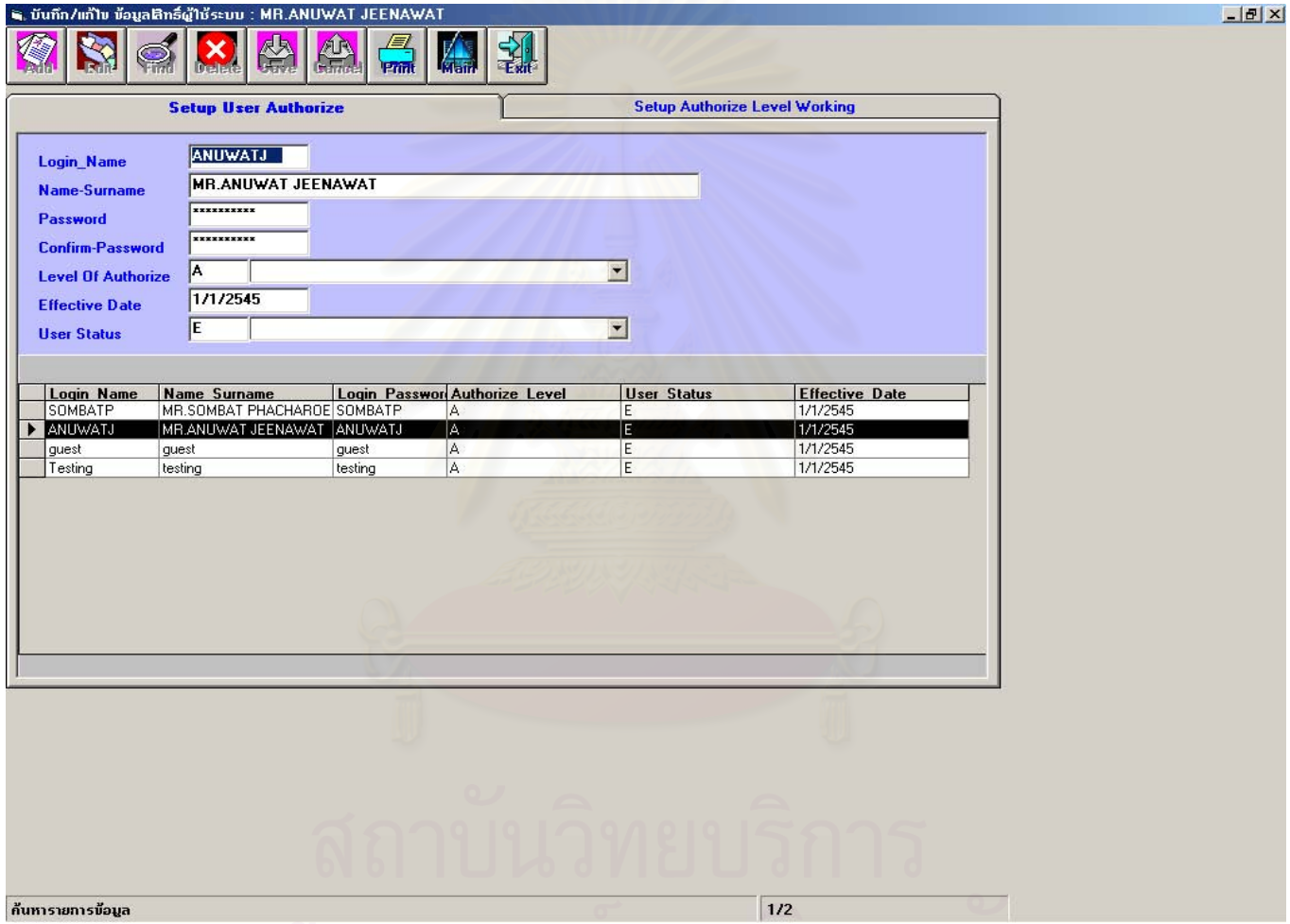
รูปที่ 4.3.6 แสดงลักษณะหน้าจอของการจัดการ Table : Setup Equipment Code



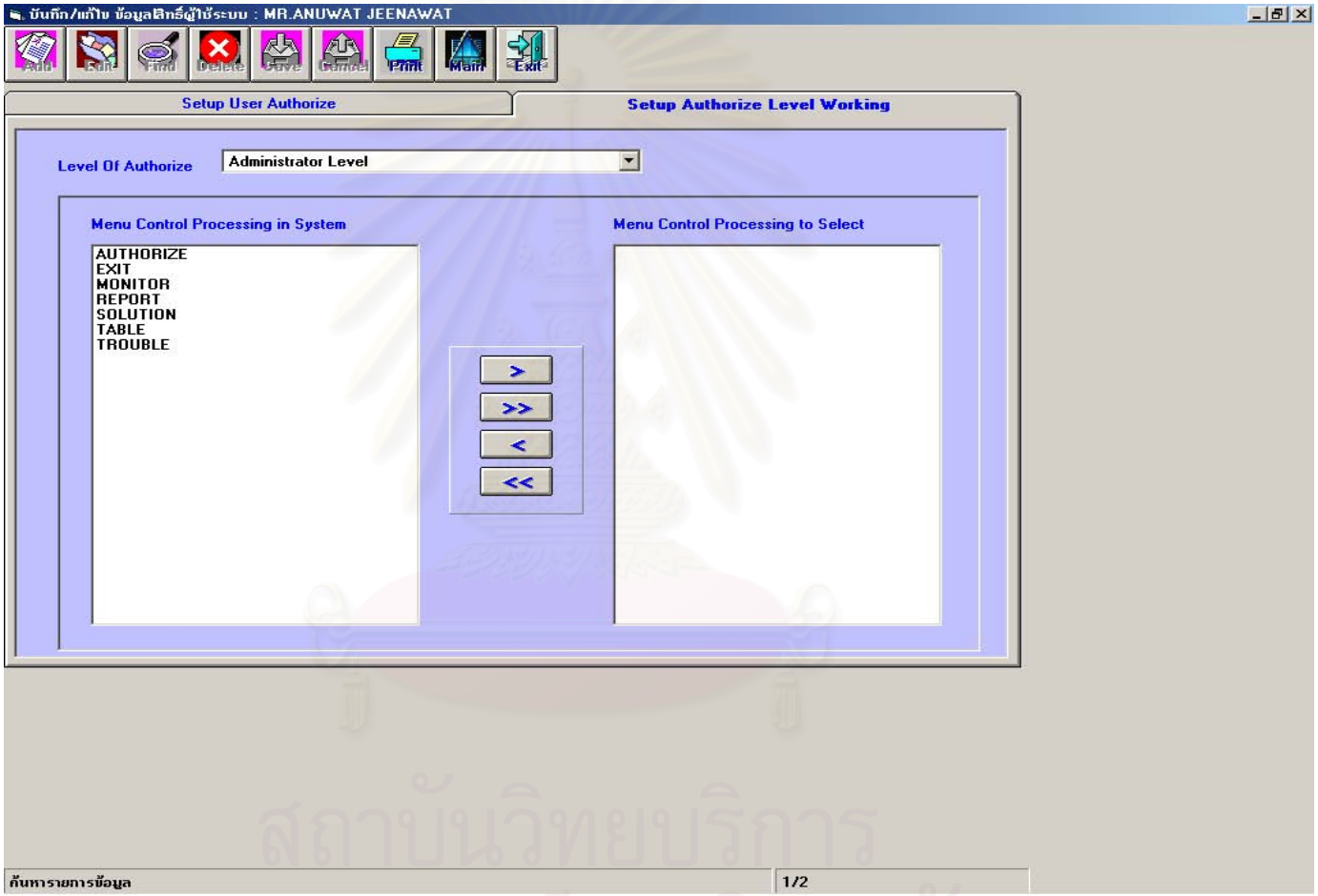
รูปที่ 4.3.7 แสดงลักษณะหน้าจอของการจัดการ Table : Setup Authorize Level



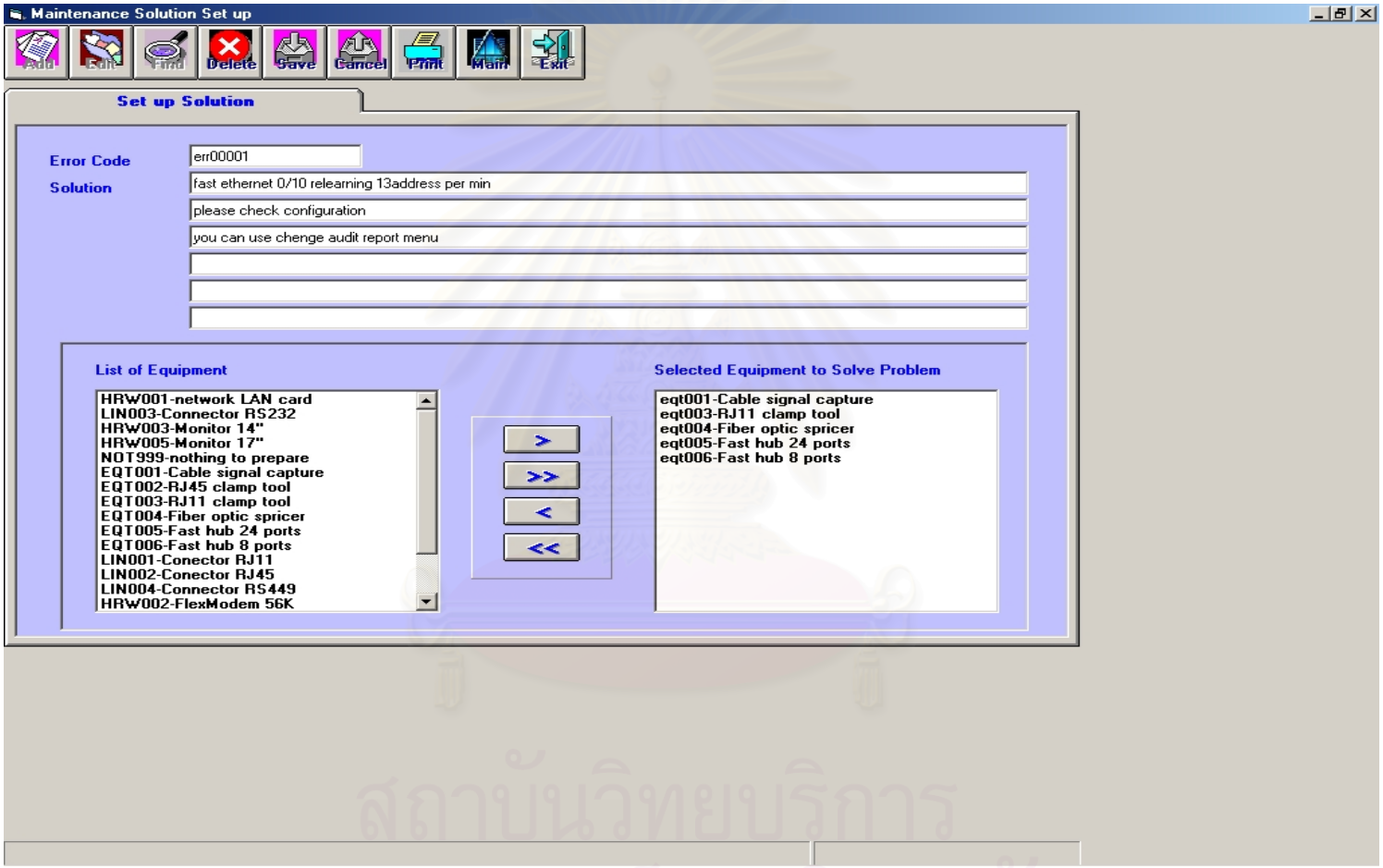
รูปที่ 4.3.8 แสดงลักษณะหน้าจอของการจัดการ Table : Setup Icon



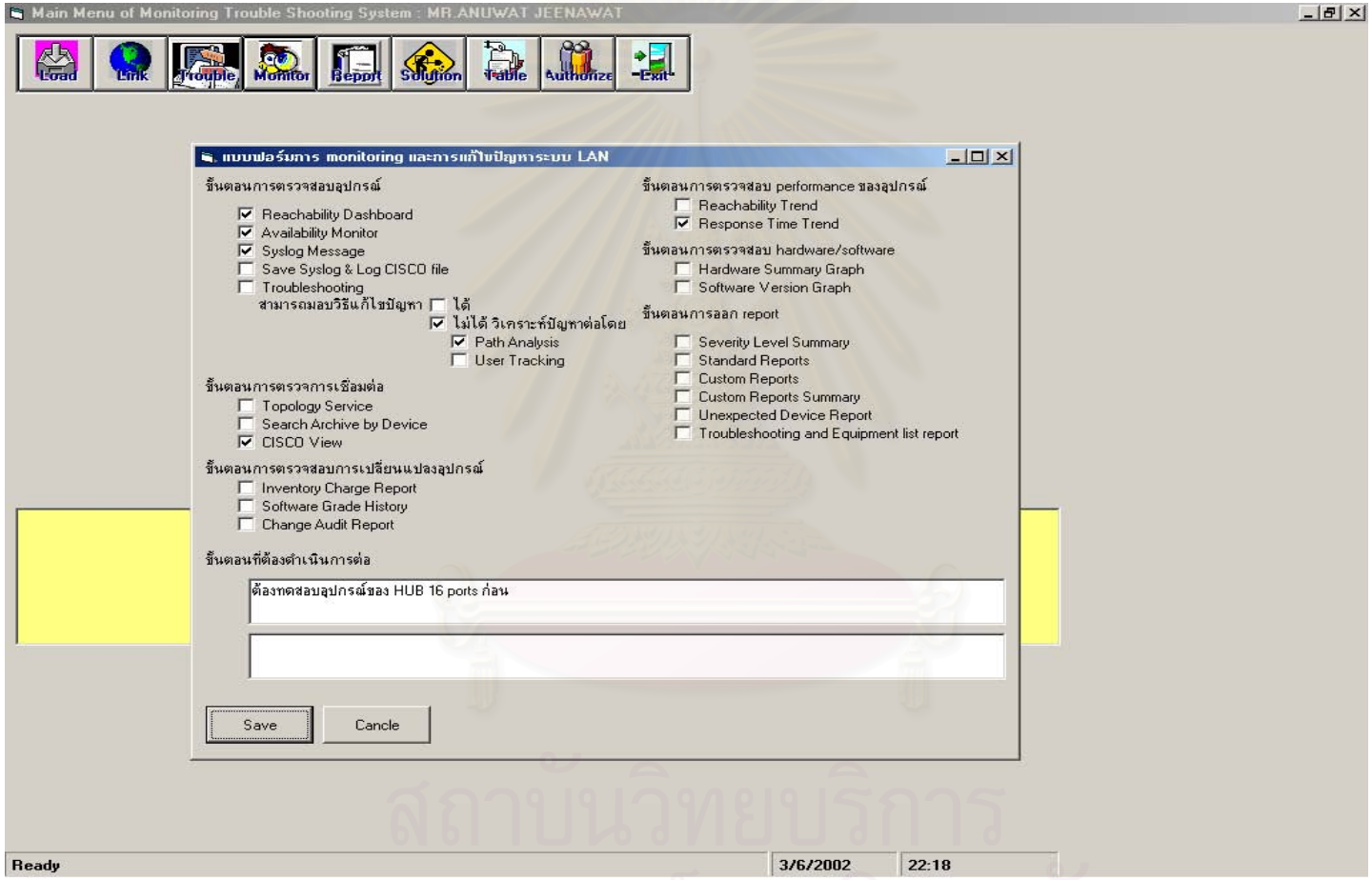
รูปที่ 4.3.9 แสดงลักษณะหน้าจอของการระบุระดับของผู้ใช้ในระบบ (User Level)



รูปที่ 4.3.10 แสดงลักษณะหน้าจอของการระบุระดับการใช้งานของผู้ใช้



รูปที่ 4.3.11 แสดงลักษณะหน้าจอของการแก้ไขปัญหาและอุปกรณ์ที่นำไปใช้ (Solving Problem)



รูปที่ 4.3.12 แสดงลักษณะหน้าจอของการแบบฟอร์มติดตามงาน (Joblist)

รูปที่ 4.3.13 แสดงลักษณะหน้าจอของการออกรายงาน (Report)

บทที่ 5

สรุปผลการวิจัยและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

การวิจัยนี้เป็นการออกแบบการเฝ้าติดตามและแก้ไขปัญหาการทำงานของแลน โดยระบบที่ออกแบบได้มีส่วนควบคุม ด้วยการแบ่งระดับการเข้าทำงานของผู้ใช้งานไว้หลายระดับตามความเหมาะสม และได้นำเอาการทำงานของระบบจัดการเครือข่ายแลนที่มีอยู่แล้ว มาใช้งานโดยการเชื่อมโยงระบบที่ออกแบบให้สามารถดึงเอาโมดูลต่าง ๆ ของระบบจัดการเครือข่ายมาใช้งานโดยอัตโนมัติ และออกแบบเพิ่มเติมส่วนที่ระบบยังขาดให้สมบูรณ์มากยิ่งขึ้น และสามารถใช้งานได้ดีกับสภาวะแวดล้อมของกรณีศึกษา โดยมีวัตถุประสงค์เพื่อนำมาประยุกต์ใช้งานให้เหมาะสมที่สุด พร้อมทั้งกำหนดแนวทางปฏิบัติในการเฝ้าติดตามและแก้ไขระบบเครือข่ายเป็นขั้นตอน พร้อมทั้งแนะนำวิธีการแก้ไขรวมทั้งอุปกรณ์ที่จะนำมาใช้ในการแก้ไขปัญหาเครือข่าย

จากการศึกษา พบว่าระบบจัดการเครือข่าย ประกอบด้วยโมดูลต่างๆ ที่สามารถใช้ช่วยเฝ้าติดตามและวิเคราะห์ปัญหาต่าง ๆ หลายรูปแบบ แต่การรายงานค่าต่างๆ จากระบบจัดการเครือข่ายเหล่านั้น ไม่สามารถใช้งานได้ตรงตามวัตถุประสงค์ทั้งหมด ดังนั้นผู้วิจัย ได้วิเคราะห์ถึงโมดูลต่างๆ และนำมาเลือกใช้เฉพาะโมดูลที่เหมาะสม รวมทั้งได้ทำการออกแบบระบบเพิ่มเติมในส่วนที่ระบบจัดการเครือข่ายไม่มี เนื่องจากระบบที่ออกแบบ เป็นลักษณะของการเก็บข้อมูลที่เคยเก็บขึ้นมาแล้ว ในลักษณะเดียวกับการตรวจสุขภาพของคน หรือ การตรวจสภาพของรถยนต์ และประวัติการซ่อมต่างๆ ว่าเคยมีปัญหาอย่างนี้ และแก้ไขอย่างไร ใช้เครื่องมือ หรือ อุปกรณ์อะไร เพื่อใช้เป็นข้อมูลเพื่อการปรับปรุง แก้ไขปัญหาให้รวดเร็วขึ้นและมีประสิทธิภาพมากที่สุด

สำหรับระบบที่ออกแบบได้อาศัยแบบฟอร์มที่ใช้ควบคุมการทำงานของผู้ปฏิบัติการระบบเครือข่ายทำให้ช่วยอำนวยความสะดวกและสามารถลดขั้นตอน และความสับสนในการทำงานสามารถส่งต่องานกันระหว่างกะได้ ทำให้ประสิทธิภาพในการทำงานของผู้ปฏิบัติการระบบเครือข่ายเพิ่มขึ้น สามารถรายงานข้อมูลไปยังระดับบริหารถึงปัญหาของอุปกรณ์เครือข่าย ที่มีแนวโน้มว่าจะไม่สามารถรองรับปริมาณที่เพิ่มขึ้นได้ ช่วยให้ระดับบริหารมีข้อมูลในการตัดสินใจที่จะลงทุนในการจัดหาอุปกรณ์ใหม่มาใช้ได้

5.2 ปัญหาและข้อเสนอแนะ

การบริหารจัดการของระบบเครือข่ายแลนอย่างถูกต้อง และมีการใช้งานเต็มประสิทธิภาพ ต้องอาศัยความรู้ความเข้าใจในระบบ และความเข้าใจหลักการทำงานของระบบปฏิบัติการเครือข่าย ที่นำมาใช้ช่วยในการจัดการ ซึ่งรวมทั้งการเฝ้าติดตามและการแก้ปัญหาของระบบนำมาประยุกต์ใช้งานให้เป็นขั้นตอนให้ได้เพื่อให้มีวิธีการทำงานที่เป็นรูปแบบมาตรฐานเดียวกัน สามารถส่งต่องานกันได้ในแต่ละกะ เพราะการจัดการระบบเครือข่าย จำเป็นต้องมีผู้ปฏิบัติงานดูแลอยู่ตลอดเวลา

5.2.1 ปัญหาและอุปสรรคที่เกิดขึ้นในการวิจัย

- ผู้วิจัยพบว่าระบบปฏิบัติการเครือข่ายที่ติดตั้งใช้งาน ณ.หน่วยงานตัวอย่าง มีฟังก์ชันบางตัวที่ควรกำหนดค่าไว้ก่อน เช่นการกำหนดให้อุปกรณ์ส่งค่าความผิดพลาดมายังเซิร์ฟเวอร์ แต่ไม่มีการกำหนด ทำให้ไม่สามารถดูได้ว่าอุปกรณ์ทำงานเป็นปกติหรือไม่ เป็นต้น ผู้วิจัยตั้งสมมุติฐานว่า เกิดจากการติดตั้งใช้งานแต่เดิม ไม่มีผู้ที่เข้าไปศึกษาระบบ และวิธีการอย่างจริงจัง และไม่มีหนังสือคู่มือระบบที่เขียนอธิบายไว้อย่างละเอียด

- ปัญหาเกี่ยวกับการติดตั้งระบบการจัดการเครือข่ายล่าช้า เพิ่งแล้วเสร็จประมาณกลางเดือนธันวาคม 2544 ทำให้ผู้วิจัยมีเวลาศึกษาเกี่ยวกับระบบดังกล่าว เพียง 3 เดือนละเอียดบางประการอาจตกหล่นไป เนื่องจากเวลาจำกัด

5.2.2 ข้อเสนอแนะ

- ก่อนการติดตั้งระบบเครือข่ายแลน ควรมีการเตรียมการต่างๆ และมีเอกสารประกอบการเตรียมการ ดังรูปที่ 5.2.1

- หลังการติดตั้งระบบเครือข่ายแลน ควรมีการตรวจเช็คความพร้อมใช้งานและควรมีเอกสารประกอบการตรวจเช็คความพร้อม ดังรูปที่ 5.2.2

แบบฟอร์มตรวจสอบก่อนการติดตั้งระบบเครือข่าย

- ศึกษาระบบการต่อเชื่อมของเครือข่ายโดยรวม
- กำหนดการจัดกลุ่มของอุปกรณ์ และการส่งผ่านข้อมูล <VLAN>
- กำหนดมาตรฐานของ IP Address แต่ละอุปกรณ์
- กำหนด Parameter ของแต่ละอุปกรณ์ในส่วนต่อเชื่อม
- กำหนด Parameter ของแต่ละอุปกรณ์ในส่วน Management
- กำหนดระยะเวลาการติดตั้ง
- กำหนดแผนการ Test ระบบ

รูปที่ 5.2.1 แสดงการตรวจสอบก่อนการติดตั้งระบบเครือข่าย

แบบฟอร์มตรวจสอบหลังการติดตั้งระบบเครือข่าย

- ตรวจเช็คการเชื่อมต่อของอุปกรณ์ทุกตัวในระบบ
- ตรวจเช็ค Parameter ในอุปกรณ์กับ Parameter ที่ระบุไว้
  - ในส่วนต่อเชื่อม
  - ในส่วน Management
- ตรวจเช็ค File ต่าง ๆ ที่เกี่ยวข้องกับระบบเครือข่าย
  - Logging File
  - Network Database
  - Parameter File
- ตรวจเช็ค Function การทำงานของระบบจัดการเครือข่าย

รูปที่ 5.2.2 แสดงการตรวจสอบหลังการติดตั้งระบบเครือข่าย

- การใช้งานของระบบจัดการเครือข่าย ที่ใช้อยู่ ณ ส่วนงานตัวอย่าง ยังขาดในส่วนของโมดูลที่จัดการเกี่ยวกับทราฟฟิก (Traffic Director) ซึ่งเป็นอีกโมดูลหนึ่งซึ่งมีความสำคัญอย่างยิ่ง หากมีการจัดซื้อจัดหาโมดูลดังกล่าว จะทำให้สามารถทราบถึงการส่งผ่านข้อมูล ปริมาณข้อมูล และสามารถจัดการระบบได้มีประสิทธิภาพมากยิ่งขึ้น

- ในการจัดหาอุปกรณ์ LAN เพิ่มเติม หรือ WAN เพิ่มเติม ถ้าพิจารณาในลักษณะของการจัดการ ควรพิจารณาให้สามารถทำงานร่วมกันได้โดยใช้โปรแกรมจัดการตัวเดียวกัน หรือตระกูลเดียวกัน จะทำให้ง่ายต่อการศึกษา และใช้งานได้อย่างเต็มประสิทธิภาพ

รายการอ้างอิง

ภาษาอังกฤษ

Allan Leinwand, Karen Fang, Network Management a Practical Perspective., Addison-Wesley Publishing Company, Inc.,1996.

Fortier Paul J., Handbook of LAN Technology., New York : McGraw-Hill, Inc.,1992.

Stallings William., SNMP,SNMpv2 and CMIP, The Practical Guide to Network Management Standards., Massachusetts : Addison-Wesley Publishing Company,Inc.,1994.

Terplan Kornel., Effective Management to LANs Functions, Instrument, and People., United States of America : McGraw-Hill,Inc.,1996.

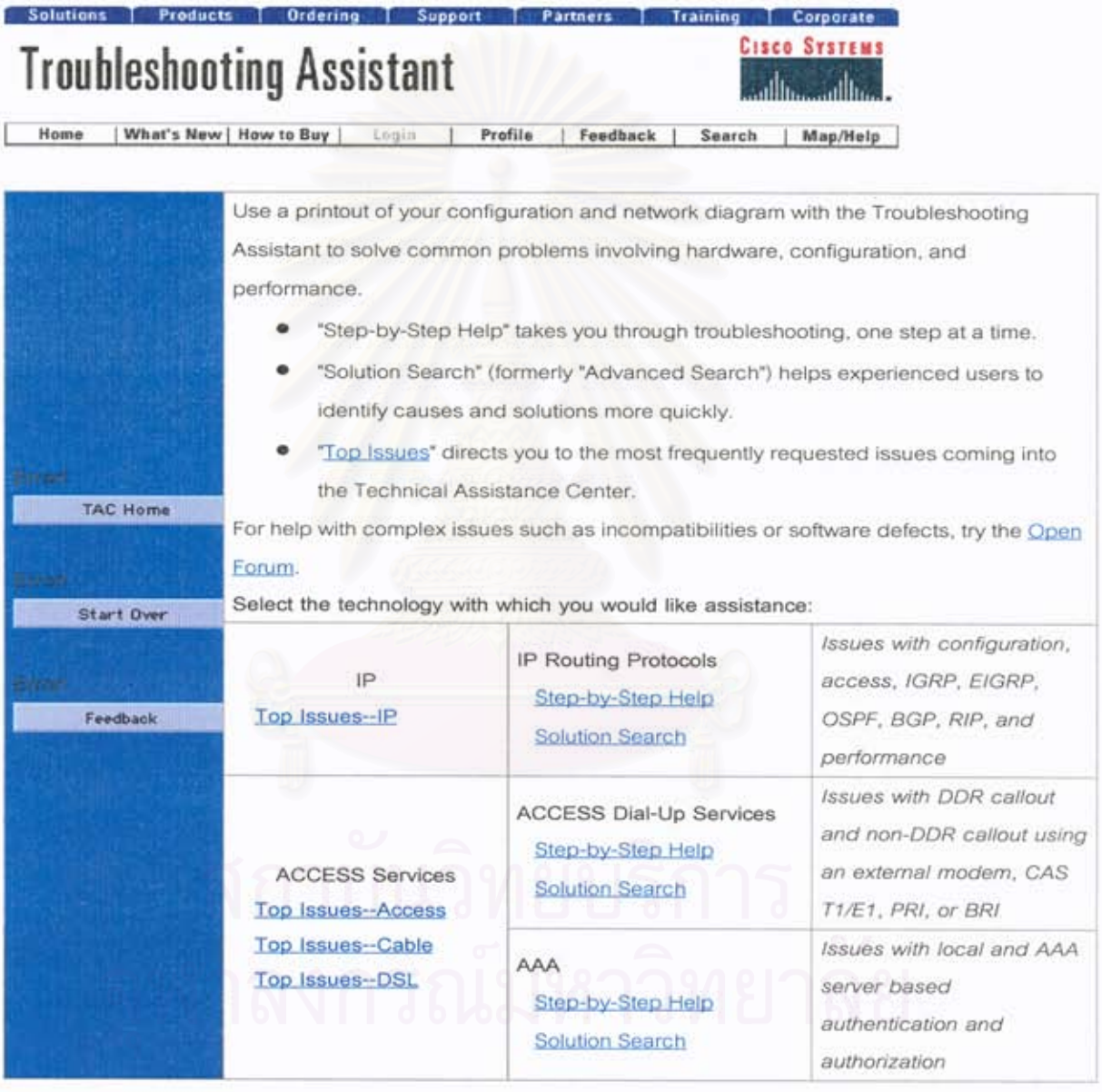
Terplan Kornel., Communication Networks Management., New Jersey : Prentice-Hall,Inc.,1987.

ภาคผนวก

ภาคผนวก ก

Trouble Shooting

ก. แสดงรายละเอียดของ Trouble Shooting



Solutions | Products | Ordering | Support | Partners | Training | Corporate

Troubleshooting Assistant

Cisco Systems

Home | What's New | How to Buy | Login | Profile | Feedback | Search | Map/Help

TAC Home

Start Over

Feedback

Use a printout of your configuration and network diagram with the Troubleshooting Assistant to solve common problems involving hardware, configuration, and performance.

- "Step-by-Step Help" takes you through troubleshooting, one step at a time.
- "Solution Search" (formerly "Advanced Search") helps experienced users to identify causes and solutions more quickly.
- "Top Issues" directs you to the most frequently requested issues coming into the Technical Assistance Center.

For help with complex issues such as incompatibilities or software defects, try the Open Forum.

Select the technology with which you would like assistance:

IP Top Issues--IP	IP Routing Protocols Step-by-Step Help Solution Search	*Issues with configuration, access, IGRP, EIGRP, OSPF, BGP, RIP, and performance*
ACCESS Services Top Issues--Access Top Issues--Cable Top Issues--DSL	ACCESS Dial-Up Services Step-by-Step Help Solution Search	*Issues with DDR callout and non-DDR callout using an external modem, CAS T1/E1, PRI, or BRI*
	AAA Step-by-Step Help Solution Search	*Issues with local and AAA server based authentication and authorization*

		Cable Technologies Step-by-Step Help Solution Search	*Includes the uBR900 series cable access routers, and the uBR72xx and uBR7246VXR CMTS and CVA12x series*
		DSL Step-by-Step Help Solution Search	*Includes 600 series ADSL modems, 1400 series routers, 6100 & 6200 series DSLAMs, 6400 series broadband concentrator, and 6510 SSG, 800 series and 7200 series router.*
		PPP Step-by-Step Help Solution Search	*Issues with LCP and NCP negotiations, authentication failure, link stability, and routing packets*
	LAN Top Issues--ATM Top Issues--LAN	ATM Media Support Step-by-Step Help	*Issues with ATM link level access*
		LAN Switching Solution Search	*Issues with configuration, connectivity, VLANs, trunking, autonegotiation, and passwords*
	WAN Top Issues--WAN Switching	WAN Switching Step-by-Step Help	*Node-related problems, connection-related problems, and trunk errors*
		Voice over WAN Switching Equipment Step-by-Step Help	*Issues with Voice quality with the CDP module or IGX 84xx with UVM or CVM modules*

		Frame Relay Step-by-Step Help	*Cisco 1000, 2500, 4000, and 7000 product lines*
	Platform Help	800 Router Step-by-Step Help	*Issues with cabling, configuration, hardware, password recovery, debug commands, and ISDN*
		1600 Router Step-by-Step Help Solution Search	*Issues with the console, booting, modules, memory, and downloading images*
		2500 Router Step-by-Step Help Solution Search	*Issues with the console, booting, modules, memory, and downloading images*
		3600 Router Step-by-Step Help Solution Search	*Issues with the console, booting, modules, memory, and downloading images*
		7000 Router Step-by-Step Help	*Issues with the console, route processor, configuration, and password recovery*
		7304 Router Step-by-Step Help	*Problems specific to the 7304 router and general router issues as applied to the 7304*

	Voice Top Issues--Voice, Telephony, and Messaging	PSTN/PBX Telephony Signaling Step-by-Step Help	*Issues with connections between POTS (Plain Old Telephone Systems) and Cisco (IOS based) voice enabled router/gateways. Covers Analog E&M, Analog FXS/FXO, and Digital E1 R2.*
	Security Applications Top Issues--PIX Top Issues--VPN	Cisco Secure PIX Firewall Series Step-by-Step Help Solution Search	*Includes all PIX hardware models and software versions. Covers issues with installation and software upgrades, password recovery, passing traffic, redundancy (failover), VPN (IPSec and PPTP), and remote connectivity for firewall management.*
		Virtual Private Networks (VPN) Solution Search	*Issues with IPSec between the Cisco Secure PIX Firewall Series and the Cisco Unity Client (VPN Client 3.x), Cisco VPN Client 2.5, and the Cisco Secure VPN Client 1.0 and 1.1.*
	Network Management Top Issues	Network Registrar Step-by-Step Help	*Issues with installation, configuration, upgrades, error messages, and access*

	 Last Modified: February 20, 2002

ภาคผนวก ข

โครงสร้างแฟ้มข้อมูล

ข. ตารางแสดงโครงสร้างแฟ้มข้อมูลที่ทำการวิเคราะห์และออกแบบ

ตารางที่ ข-1 โครงสร้างแฟ้มข้อมูลของ SYSLOG

Data Store Name	Solution_equipment				
Alias	D1				
Description	แฟ้มข้อมูลการเก็บปัญหาที่เกิดขึ้นในระบบเครือข่าย (SYSLOG)				
Sources					Destinations
		Picture Value		Not		
no	Name	Type	Length	Null	Key	Descriptions
1	Facility	Char	15	Y		เครื่องมือฮาร์ดแวร์หรือโปรโตคอล (Protocal) หรือโมดูลของซอร์ฟแวร์ระบบ
2	Severity	Char	15	Y		เป็นส่วนที่เก็บระดับความรุนแรงของปัญหา สามารถแบ่งได้ 7 ระดับ กล่าวคือ ● ระดับที่ 0 เป็นปัญหาฉุกเฉิน (Emergency) ● ระดับที่ 1 เป็นสัญญาณการเตือน (Alert) ● ระดับที่ 2 เป็นการเข้าขั้นวิกฤต (Critical) ● ระดับที่ 3 เป็นการแสดงข้อผิดพลาด (Error) ● ระดับที่ 4 เป็นการเตือนธรรมดา (Warning) ● ระดับที่ 5 เป็นข้อสังเกต (Notification) ● ระดับที่ 6 เป็นการบอกข้อมูลข่าวสาร (Information)
3	Mnemonic	Char	15	Y		เป็นรหัสที่ไม่ซ้ำกันซึ่งสามารถแยก Error Message แต่เฉพาะอุปกรณ์ซึ่งเป็น IOS ส่วนอุปกรณ์ Catalyst ไม่สามารถแสดงได้
4	Equipment_code	Char	6	Y		รหัสของอุปกรณ์ในระบบเครือข่าย
5	Create_datetime	datetime	8			

ตารางที่ ข-2 โครงสร้างแฟ้มข้อมูลการเก็บข้อมูลที่ใช้ในการแก้ไขปัญหา (Solving Problem)

Data Store Name	Message_log
Alias	D2
Description	แฟ้มข้อมูลการเก็บข้อมูลที่ใช้ในการแก้ไขปัญหา (Solving Problem)

Sources	Destinations

no	Name	Picture Value		Not Null	Key	Descriptions
		Type	Length			
1	Trouble_date	Datetime	8	Y	Y	รหัสของปัญหาที่เกิดขึ้น
2	Device_name	Char	30	Y		วันที่ที่เกิดปัญหา
3	Time_stamp	Char	30	Y		รหัสความผิดพลาด
4	Facility	Char	15	Y		วันที่ทำการปรับปรุงข้อมูลล่าสุด
5	Severity	Char	15	Y		ผู้ใช้ระบบที่ทำการปรับปรุงข้อมูลล่าสุด
6	Mnemonic	Char	15	Y		รหัสความผิดพลาด
7	Message_description	Char	200			วันที่ทำการปรับปรุงข้อมูลล่าสุด
8	Error_code	Char	8	Y		ผู้ใช้ระบบที่ทำการปรับปรุงข้อมูลล่าสุด

ตารางที่ ข-3 โครงสร้างแฟ้มข้อมูลรายการอุปกรณ์เครือข่าย

Data Store Name	T_codeequipment
Alias	D3
Description	แฟ้มข้อมูลการเก็บข้อมูลรายการอุปกรณ์เครือข่าย

Sources	Destinations

no	Name	Picture Value		Not Null	Key	Descriptions
		Type	Length			
1	Equipment_code	Char	6	Y	Y	รหัสของอุปกรณ์เครือข่าย
2	Equipment_desc	Char	80			รายละเอียดของอุปกรณ์เครือข่าย

ตารางที่ ข-4 โครงสร้างแฟ้มข้อมูลของความผิดพลาดที่เกิดขึ้น

Data Store Name	T_errorcode					
Alias	D4					
Description	แฟ้มข้อมูลเก็บข้อมูลของความผิดพลาดที่เกิดขึ้น					
Sources						Destinations
no	Name	Picture Value		Not Null	Key	Descriptions
		Type	Length			
1	Error_code	Char	8	Y	Y	รหัสของความผิดพลาด
2	Message_error	Char	200			รายละเอียดของความผิดพลาด
3	Equipment_code	Char	6	Y		รหัสของอุปกรณ์เครือข่าย

ตารางที่ ข-5 โครงสร้างแฟ้มข้อมูลเก็บประวัติข้อมูลผู้ใช้ระบบ

Data Store Name	T_historylog					
Alias	D5					
Description	แฟ้มข้อมูลเก็บข้อมูลประวัติผู้ใช้ระบบ					
Sources						Destinations
no	Name	Picture Value		Not Null	Key	Descriptions
		Type	Length			
1	Login_name	Char	10	Y	Y	ชื่อผู้ใช้ระบบ
2	Login_date	Datetime	8			วันที่ที่เข้าใช้งานในระบบ
3	Login_amount	int	4			จำนวนครั้งที่เข้ามาใช้งาน
4	Logoff_date	Datetime	8			วันที่ออกจากระบบครั้งล่าสุด

ตารางที่ ข-6 โครงสร้างแฟ้มข้อมูลของการคอนโทรลไอคอน

Data Store Name	T_icon					
Alias	D6					
Description	แฟ้มข้อมูลของการคอนโทรลไอคอน					
Sources						Destinations
no	Name	Picture Value		Not Null	Key	Descriptions
		Type	Length			
1	Icon_id	Char	10	Y	Y	รหัสไอคอน
2	Description	Char	80			รายละเอียดของไอคอน

ตารางที่ ข-7 โครงสร้างแฟ้มข้อมูลกำหนดสิทธิ์ผู้ใช้ระบบ

Data Store Name	T_authorize					
Alias	D7					
Description	แฟ้มข้อมูลของกำหนดสิทธิ์ผู้ใช้ระบบ					
Sources						Destinations
no	Name	Picture Value		Not Null	Key	Descriptions
		Type	Length			
1	Authorize_level	Char	1	Y	Y	ระดับของการใช้งาน
2	Authorize_description	Char	80			รายละเอียดของระดับการใช้งาน

ตารางที่ ข-8 โครงสร้างแฟ้มข้อมูลระดับของสิทธิ์การใช้งาน

Data Store Name	T_userstatus					
Alias	D8					
Description	แฟ้มข้อมูลของระดับของสิทธิ์การใช้งาน					
Sources						Destinations
no	Name	Picture Value		Not Null	Key	Descriptions
		Type	Length			
1	Status_code	Char	1	Y	Y	รหัสสถานะ
2	Status_description	Char	50			รายละเอียดของสถานะ

ตารางที่ ข-9 โครงสร้างแฟ้มข้อมูลการกำหนดการทำงาน

Data Store Name	Help_authorize_working					
Alias	D9					
Description	แฟ้มข้อมูลของการกำหนดการทำงาน					
Sources						Destinations
no	Name	Picture Value		Not Null	Key	Descriptions
		Type	Length			
1	Authorize_level	Char	1	Y	Y	ระดับของสิทธิ์การใช้งาน
2	Icon_id	Char	10	Y		หมายเลขไอคอน
3	Create_datetime	datetime	8			วันเวลาที่ทำการสร้าง

ตารางที่ ข-10 โครงสร้างแฟ้มข้อมูลของผู้ใช้ระบบ

Data Store Name	Help_authorize_user
Alias	D10
Description	แฟ้มข้อมูลของผู้ใช้ระบบ

Sources	Destinations

no	Name	Picture Value		Not Null	Key	Descriptions
		Type	Length			
1	Login_name	Char	10	Y	Y	ชื่อผู้เข้าใช้ระบบ
2	Name_surname	Char	80			ชื่อ-นามสกุลของผู้ใช้งาน
3	Login_password	Char	10	Y		รหัสผ่าน
4	Authorize_level	Char	1			ระดับของสิทธิ์การใช้งาน
5	User_status	Char	1			สถานะของผู้ใช้
6	Effective_date	datetime	8	Y		วันที่มีผลบังคับใช้

ตารางที่ ข-11 โครงสร้างแฟ้มข้อมูลการติดตามงาน (Joblist)

Data Store Name	joblist
Alias	D11
Description	แฟ้มข้อมูลของการติดตามงาน (Joblist)

Sources	Destinations

no	Name	Picture Value		Not Null	Key	Descriptions
		Type	Length			
1	Log_date	Date	8	Y	Y	วันที่ที่ทำการติดตามงาน
2	Chk01	Char	1			Reachability Dashboard
3	Chk02	Char	1			Availability Monitor
4	Chk03	Char	1			Syslog Message
5	Chk04	Char	1			Save syslog into file

ตารางที่ ข-11 โครงสร้างแฟ้มข้อมูลการติดตามงาน (Joblist) (ต่อ)

Data Store Name	joblist
Alias	D11
Description	แฟ้มข้อมูลของการติดตามงาน (Joblist)

Sources	Destinations

no	Name	Picture Value		Not Null	Key	Descriptions
		Type	Length			
6	Chk05	Date	8	Y	Y	Trouble shouting
7	Chk06	Char	1			Yes
8	Chk07	Char	1			No
9	Chk08	Char	1			Path Analysis
10	Chk09	Char	1			User Tracking
11	Chk10	Char	1			Topology Service
12	Chk11	Char	1			Search Archive by Device
13	Chk12	Char	1			CISCO View
14	Chk13	Char	1			Inventory Change Report
15	Chk14	Char	1			Software Grade History
16	Chk15	Char	1			Change Audit Report
17	Chk16	Char	1			Reachability Trend
18	Chk17	Char	1			Response Time Trend
19	Chk18	Char	1			Hardware Summary Graph
20	Chk19	Char	1			Software Summary Graph
21	Chk20	Char	1			Severity Level Summary
22	Chk21	Char	1			Standard Reports
23	Chk22	Char	1			Custom Reports
24	Chk23	Char	1			Custom Reports Summary
25	Chk24	Char	1			Unexpected Device Report
23	Chk25	Char	1			Troubleshooting and Equipment List Report
24	Note1	Char	150			Next Step 1
25	Note2	Char	150			Next Step 2

ประวัติผู้เขียนวิทยานิพนธ์

นาย อนุวัฒน์ จีนะวัฒน์ เกิดเมื่อวันที่ 16 มกราคม 2505 ที่สมุทรปราการ ได้สำเร็จการศึกษาระดับปริญญาตรีวิทยาศาสตร์บัณฑิต สาขาสถิติ คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร ปีการศึกษา 2527 และเข้าศึกษาต่อในระดับปริญญาโทหลักสูตรวิทยาศาสตร์มหาบัณฑิต สาขาวิทยาศาสตร์คอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ภาคปีการศึกษา 2541