ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจล.

ระบบเฝ้าสังเกตเครือข่ายสารสนเทศ

Network Monitoring System

โดย

นิเวช มิ่งมิตรโอฬาร

รหัสประจำตัว 46066945

b11749660
IT29 22/47

อาจารย์ที่ปรึกษา

ผศ.ดร.ภัทรชัย ลลิตโรจน์วงศ์

วัน เดือน ปี 21 พ.ค. 2550
เลขทะเบียน 03260
เลขเรียกหนังสือ วท. ม467ร 2548
"ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจล."

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการศึกษากรณีพิเศษ

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 2 ปีการศึกษา 2548

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

H003260

ชื่อหัวข้อ	ระบบเฝ้าสังเกตเครือข่ายสารสนเทศ
นักศึกษา	นายนิเวช มิ่งมิตรโอพาร
อาจารย์ที่ปรึกษา	ผศ.ดร. ภัทรชัย ลลิตโรจน์วงศ์
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	การจัดการเทคโนโลยีสารสนเทศ
ปีการศึกษา	2548

บทคัดย่อ

ระบบเฝ้าสังเกตเครือข่ายสารสนเทศ เป็นระบบที่ช่วยให้ผู้ดูแลระบบเครือข่ายทราบถึงปัญหาที่เกิดขึ้นกับเครือข่าย โดยระบบจะทำการส่งไอซีเอ็มพีแพ็กเก็ตไปตามหมายเลขไอพีแอดเดรสของปลายทางที่ต้องการตรวจสอบหรือโหนดแล้วดูผลลัพธ์ของการส่ง เพื่อนำผลลัพธ์ที่ได้มาแสดงเป็นภาพโดยมีสีเป็นตัวบอกสถานะผ่านทางเว็บแอ็พพลิเคชั่น ทำให้ผู้ดูแลระบบเครือข่ายมีสะดวกในการใช้งานและเข้าถึงระบบ เมื่อเกิดปัญหาขึ้นกับระบบเครือข่ายผู้ดูแลระบบสามารถดูรายละเอียดข้อมูลของปลายทางและผู้ให้บริการวงจรได้ทันทีทำให้มีความรวดเร็วในการแก้ปัญหา สามารถบันทึกสาเหตุของปัญหาที่เกิดขึ้น ระบบสามารถคำนวณระยะเวลาที่เกิดปัญหาและทำรายงานสรุป ระบบนี้ทำให้ลดค่าใช้จ่ายในซื้อระบบบริหารจัดการเครือข่ายที่มีราคาแพง โครงการนี้ เริ่มต้นด้วยการศึกษาและวิเคราะห์ปัญหาของระบบงานปัจจุบัน ทำการวิเคราะห์และออกแบบระบบงานใหม่โดยใช้ภาษายูเอ็มแอล จัดเก็บข้อมูลแบบฐานข้อมูลเชิงสัมพันธ์ โดยใช้ MySQL เขียนโปรแกรมเพื่อตรวจสอบสถานะของระบบเครือข่ายด้วยภาษา Perl และใช้ภาษา PHP เพื่อสร้างเว็บแอ็พพลิเคชั่น

Title	Network Monitoring System
Student	Mr. Niwech Mingmitolan
Advisor	Asst.Prof.Dr. Pattarachai Lalitrojwong
Level of Study	Master of Science in Information Technology
Major	Information Technology Management
Academic Year	2005

ABSTRACT

Network Monitoring System is a system designed to provide a web-based application for network administrators to monitor network abnormalities. The system operates by transmitting ICMP packets to designated IP addresses, or nodes, to determine network connectivity then reports onto a web page. Should any node fails to respond, the network administrator could be able to attain informative details regarding the certain node, and its circuit provider; and thus quickly take action against the problem. The system records all history of all problems occurred onto a log and provides a report on demand. This project begins with analyzing problems yielded by the current system, and then uses UML in representation of the new system analysis and design. An open-source relational database MySQL is used in corporate with server-side script PHP and PERL for construction of the web-base application system.

กิตติกรรมประกาศ

โครงการศึกษากรณีพิเศษ เรื่อง การพัฒนาระบบเฝ้าสังเกตเครือข่ายสารสนเทศนี้สามารถดำเนินการจนสำเร็จได้ด้วยความกรุณาจากบุคคลหลายท่าน โครงการนี้จะสำเร็จไม่ได้หากไม่มีบุคคลเหล่านี้ ซึ่งผู้จัดทำขอขอบพระคุณ ผศ.ดร.ภัทรชัย ลลิตโรจน์วงศ์ อาจารย์ที่ปรึกษาโครงการศึกษากรณีพิเศษนี้ ขอขอบคุณสำนักบริการเทคโนโลยีสารสนเทศภาครัฐ (สบทร.) ที่ให้โอกาสในการทำงานและเรียนรู้ด้านเครือข่ายคอมพิวเตอร์ ขอขอบคุณ นายวรกร คุรุวงศ์วัฒนา ที่ช่วยเหลือในเรื่องโปรแกรม ขอขอบคุณเพื่อนๆ ITM14 ทุกท่านที่ช่วยเหลือและเป็นกำลังใจให้ตลอดมา สุดท้ายนี้ ขอขอบคุณ คุณปรียาวรรณ มิ่งมิตรโอพาร ภรรยาที่คอยให้กำลังใจและสนับสนุนตลอดมาจนทำให้ประสบความสำเร็จได้ในวันนี้

นิเวช มิ่งมิตรโอพาร

สารบัญ

หน้า

บทคัดย่อภาษาไทย I
บทคัดย่อภาษาอังกฤษ II
กิตติกรรมประกาศ III
สารบัญ IV
สารบัญตาราง VI
สารบัญรูป VII
บทที่
1. บทนำ 1
1.1 ความเป็นมา 1
1.2 วัตถุประสงค์การพัฒนาระบบ 1
1.3 ขอบเขตของการพัฒนาระบบ 2
1.4 ขั้นตอนการพัฒนาระบบ 2
1.5 ประโยชน์ที่คาดว่าจะได้รับ 3
2. ทฤษฎีและเทคโนโลยี 4
2.1 แนวคิดเชิงวัตถุและยูเอ็มแอล 4
2.2 Perl 6
2.3 PHP 7
2.4 MySQL 8
2.5 ไอพีแอดเดรส 9
2.6 โพรโทคอล ไอซีเอ็มพี 10
3. การวิเคราะห์ระบบสารสนเทศ 16
3.1 ระบบที่ใช้ทำงานในปัจจุบัน 16
3.2 ปัญหาของระบบการทำงานในปัจจุบัน 17

สารบัญ (ต่อ)

หน้า

3.3 การวิเคราะห์ความต้องการของผู้ใช้ 17
3.4 การวิเคราะห์ระบบสารสนเทศใหม่ 17
3.5 แบบจำลองข้อมูลของระบบ 28
4. การออกแบบระบบสารสนเทศ 29
4.1 การออกแบบการทำงานของระบบ 29
4.2 การออกแบบสถาปัตยกรรมของระบบ 34
5. การออกแบบฐานข้อมูล 37
6. การพัฒนาระบบ 42
6.1 โครงสร้างเว็บหลักของระบบ 42
6.2 รายละเอียดการทำงานของระบบ 44
7. บทสรุป 54
7.1 สรุปผลโครงการ 54
7.2 ปัญหา ข้อจำกัด และข้อเสนอแนะ 54
บรรณานุกรม 56
ประวัติผู้เขียน 57

สารบัญตาราง

หน้า

ตารางที่

3.1 รายละเอียดยูสเคส Add New Node 20

3.2 รายละเอียดยูสเคส Edit Node 22

3.3 รายละเอียดยูสเคส Ping 23

3.4 รายละเอียดยูสเคส Monitor Node 25

3.5 รายละเอียดยูสเคส Record Problem Cause 26

3.6 รายละเอียดยูสเคส Availability Report 27

4.1 คุณสมบัติของเครื่องเซิร์ฟเวอร์ 36

5.1 พจนานุกรมข้อมูลของตาราง NODE 38

5.2 พจนานุกรมข้อมูลของตาราง NODE_TYPE 39

5.3 พจนานุกรมข้อมูลของตาราง LOG 39

5.4 พจนานุกรมข้อมูลของตาราง PROBLEM_TICKET 40

5.5 พจนานุกรมข้อมูลของตาราง USER 40

5.6 พจนานุกรมข้อมูลของตาราง POSITION 40

5.7 พจนานุกรมข้อมูลของตาราง PROVIDER 41

5.8 พจนานุกรมข้อมูลของตาราง GROUP 41

สารบัญรูป

หน้า

รูปที่

2.1 ขั้นตอนการ Encapsulate ICMP Packet 10
2.2 ตัวอย่างการเชื่อมต่อเครือข่าย 12
2.3 การส่ง ICMP Redirect 13
2.4 การใช้คำสั่ง ping แล้วไม่มีแพ็กเก็ตใดๆตอบกลับ 14
2.5 การใช้คำสั่ง ping แล้วมีแพ็กเก็ตตอบกลับ 15
3.1 ตัวอย่างการแสดงผลของโปรแกรมHP Openview 16
3.2 ยูสยูสเคสไดอะแกรมของระบบเฝ้าสังเกตเครือข่ายสารสนเทศ 18
3.3 แอกทิวิตีไดอะแกรมของการเพิ่มโหนด 21
3.4 แอกทิวิตีไดอะแกรมของการแก้ไขข้อมูลโหนด 22
3.5 แอกทิวิตีไดอะแกรมของยูสเคส Ping 24
3.6 แอกทิวิตีไดอะแกรมของการตรวจสอบสถานะโหนด 25
3.7 แอกทิวิตีไดอะแกรมของยูสเคส Record Problem Cause 26
3.8 แอกทิวิตีไดอะแกรมของยูสเคส Availability Report 27
3.9 คลาสไดอะแกรมของระบบเฝ้าสังเกตเครือข่ายสารสนเทศ 28
4.1 ซีเควนซ์ไดอะแกรมของการเพิ่มโหนด 29
4.2 ซีเควนซ์ไดอะแกรมของการแก้ไขข้อมูลโหนด 30
4.3 ซีเควนซ์ไดอะแกรมของการดูสถานะการทำงานของโหนด 31
4.4 ซีเควนซ์ไดอะแกรมของการส่งไอซีเอ็มพีแพ็กเก็ตเพื่อตรวจสอบสถานะของโหนด 32
4.5 ซีเควนซ์ไดอะแกรมของการระบุสาเหตุของปัญหา 33
4.6 ซีเควนซ์ไดอะแกรมของการแสดงรายงานสรุป 34

สารบัญรูป (ต่อ)

หน้า

รูปที่

4.7 การออกแบบเครือข่าย 35

5.1 แผนภาพความสัมพันธ์ระหว่างเอนทิตี 38

6.1 วินโดว์เนวิเกชันไดอะแกรมส่วนเชื่อมต่อกับผู้ใช้ระบบ 43

6.2 หน้าจอการเข้าสู่ระบบ 44

6.3 หน้าจอการเข้าสู่ระบบสำเร็จ 45

6.4 หน้าจอเกิดความผิดพลาดในการเข้าสู่ระบบ 45

6.5 หน้าจอการตรวจสอบสถานะของโหนดโดยการเลือกชนิดวงจร 46

6.6 หน้าจอการตรวจสอบสถานะของโหนด 47

6.7 หน้าจอการเลือกวันที่รายงานปัญหา 48

6.8 หน้าจอการการรายงานปัญหา 48

6.9 หน้าจอการการระบุปัญหา 49

6.10 หน้าจอการเพิ่มโหนดใหม่ 50

6.11 หน้าจอการเพิ่มโหนดใหม่เรียบร้อยแล้ว 50

6.12 หน้าจอการเปลี่ยนแปลงแก้ไขข้อมูลโหนด 51

6.13 หน้าจอการเปลี่ยนแปลงแก้ไขข้อมูลโหนด 52

6.14 หน้าจอการเปลี่ยนแปลงแก้ไขข้อมูลโหนดเรียบร้อยแล้ว 52

6.15 หน้าจอการดูรายงาน 53

บทที่ 1
บทนำ

1.1 ความเป็นมา

หน่วยงานที่ทำหน้าที่เป็นศูนย์ปฏิบัติการเครือข่าย มีหน้าที่คอยดูแล เฝ้าระวัง และ ตรวจสอบการใช้งานระบบเครือข่ายทั้งหมดที่หน่วยงานรับผิดชอบตลอด 24 ชั่วโมง ระบบสารสนเทศที่จำเป็นที่ควรนำมาใช้ในการควบคุมการปฏิบัติงานเหล่านี้ให้มีประสิทธิภาพในการทำงานมากขึ้น คือระบบเฝ้าสังเกตเครือข่าย เพื่อช่วยให้เจ้าหน้าที่ผู้ดูแลระบบเครือข่ายสามารถทราบถึงปัญหาที่เกิดขึ้นกับระบบเครือข่ายได้ทันทีและสามารถแก้ปัญหาได้อย่างรวดเร็ว ในการรับประกันคุณภาพในการให้บริการการตอบสนองต่อปัญหาและการแก้ปัญหาอย่างรวดเร็วมีความจำเป็นอย่างยิ่ง รวมถึงการทำรายงานสรุปปัญหาต่างๆที่เกิดขึ้น เพื่อนำเสนอต่อผู้บริหารและนำเสนอต่อหน่วยงานที่ขอใช้บริการ ซึ่ง ในปัจจุบันมีระบบเฝ้าสังเกตเครือข่ายจำนวนมากหลากหลายรูปแบบ แต่บางครั้งไม่ตรงตามความต้องการของผู้ใช้งานอย่างแท้จริง บางระบบมีความสามารถมากเกินความจำเป็น ทำให้เกิดความยุ่งยากในการดูแลรักษาและมีราคาแพง บางระบบมีความสามารถน้อยกว่าความต้องการทำให้การ ดูแลเครือข่ายไม่มีประสิทธิภาพ

ดังนั้น การพัฒนาระบบระบบเฝ้าสังเกตเครือข่ายสารสนเทศขึ้นมาด้วยตนเอง จะทำให้ได้ระบบที่ตรงตามความต้องการของผู้ใช้งาน และสามารถปรับแก้คุณลักษณะของระบบได้ตามความเหมาะสมกับการใช้งานจริงมากที่สุด สามารถทำรายงานสรุปปัญหาที่เกิดขึ้นเพื่อให้ผู้บริหารสามารถนำข้อมูลมาวิเคราะห์เพื่อหาวิธีการป้องกันปัญหาที่จะเกิดขึ้นในอนาคต

1.2 วัตถุประสงค์ของการพัฒนาระบบ

1. เพื่อให้ได้ระบบเฝ้าสังเกตเครือข่ายสารสนเทศที่ตรงตามความต้องการและความเหมาะสมของการใช้งานมากที่สุด
2. เพื่อให้เจ้าหน้าที่ผู้ดูแลระบบเครือข่ายสามารถใช้เป็นเครื่องมือในการดูแลเครือข่ายให้กับหน่วยงานที่รับผิดชอบ
3. เพื่อให้เจ้าหน้าที่ผู้ดูแลระบบเครือข่ายสามารถแก้ปัญหาได้อย่างรวดเร็วในกรณีที่ระบบเครือข่ายเกิดปัญหาขึ้น
4. เพื่อให้มั่นใจได้ว่าปัญหาที่เกิดขึ้นมีผู้ดูแลในการแก้ปัญหาจนหมดปัญหาอย่างแน่นอน

5. เพื่อให้การจัดทำรายงานสรุปคุณภาพในการให้บริการของผู้ให้บริการวงจรมีความถูกต้องแม่นยำมากขึ้น และสามารถนำไปวางแผนปรับปรุงคุณภาพในการให้บริการได้ต่อไป
6. เพื่อให้การจัดทำรายงานสรุประยะเวลาที่เกิดปัญหาในแต่ละครั้งมีความถูกต้องแม่นยำมากขึ้น และนำไปคำนวณรับเงินกับผู้ให้บริการต่อไป

1.3 ขอบเขตของการพัฒนาระบบ

ในการพัฒนาระบบเฝ้าสังเกตเครือข่ายสารสนเทศนี้ จะติดตั้งเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ที่ทำหน้าที่ส่งไอซีเอ็มพีแพ็กเก็ตไปยังปลายทางหรือโหนดต่างๆ เพื่อตรวจสอบสถานะการทำงานของแต่ละโหนดว่ามีความพร้อมในการใช้งานอยู่หรือไม่ โดยมีหมายเลขไอพีแอดเดรสเป็นตัวบอกตำแหน่งของโหนดนั้นๆ โดยสถิติการเกิดปัญหาและวิธีการแก้ปัญหาจะถูกเก็บบันทึกลงฐานข้อมูล

ระบบเฝ้าสังเกตเครือข่ายสารสนเทศจะสามารถแสดงสถานะการทำงานของโหนด ในลักษณะกราฟฟิก โดยผู้ใช้งานระบบสามารถใช้ระบบได้โดยใช้ผ่านเว็บแอพพลิเคชัน ที่ใช้สีเป็นตัวบอกสถานการณ์ทำงาน เช่น สีเขียวแทนการทำงานที่ปกติไม่เกิดปัญหาใดๆ สีแดงแสดงสถานะว่าระบบเครือข่ายเกิดปัญหาขึ้น เจ้าหน้าที่ผู้ดูแลระบบเครือข่ายสามารถเพิ่มข้อมูล แก้ไขปรับปรุงข้อมูล หรือเรียกดูของโหนดได้ทันที เมื่อเกิดปัญหาขึ้นกับระบบเครือข่ายผู้ดูแลระบบเครือข่ายสามารถดูรายละเอียดข้อมูลของปลายทางและผู้ให้บริการวงจรได้ทันทีทำให้มีความรวดเร็วในการแก้ปัญหา สามารถบันทึกสาเหตุของปัญหาที่เกิดขึ้น ระบบสามารถคำนวณระยะเวลาที่เกิดปัญหาและทำรายงานสรุป

1.4 ขั้นตอนการพัฒนาระบบ

1. ศึกษาการทำงานของระบบงานปัจจุบัน วิเคราะห์ปัญหาที่เกิดจากการทำงานโดยดูจากระบบสารสนเทศระบบเฝ้าสังเกตเครือข่ายที่ใช้อยู่ปัจจุบัน
2. ออกแบบระบบฐานข้อมูลโดยใช้ระบบฐานข้อมูล MySQL
3. วิเคราะห์และออกแบบระบบงานใหม่ โดยใช้แบบจำลองเชิงวัตถุด้วยภาษายูเอ็มแอล (UML : Unified Modeling Language)
4. ติดตั้งเครื่องเซิร์ฟเวอร์ที่ทำหน้าที่ส่งไอซีเอ็มพีแพ็กเก็ตไปยังโหนดต่างๆ และแสดงสถานะต่างๆ โดยใช้ระบบปฏิบัติการลินุกส์
5. พัฒนาระบบโดยใช้ภาษา Perl เพื่อสร้างโปรแกรมในการตรวจสอบสถานะของโหนดต่างๆ
6. พัฒนาระบบโดยใช้ภาษา PHP เพื่อสร้างเว็บแอพพลิเคชั่น
7. ทดสอบการทำงานของระบบ

8. สรุปผลการศึกษาและจัดทำเอกสารการพัฒนาระบบ

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. เจ้าหน้าที่ดูแลเครือข่ายมีเครื่องมือในการทำงาน เพื่อช่วยให้ทราบถึงปัญหาที่เกิดขึ้นกับเครือข่าย และสามารถติดตามผลได้ตลอดเวลา
2. คุณภาพในการให้บริการเครือข่ายดีขึ้น เนื่องจากปัญหาที่อาจเกิดขึ้นมีการติดตามและเฝ้าระวัง
3. ประหยัดในการซื้อระบบบริหารจัดการเครือข่ายที่มีราคาแพง
4. ระบบที่พัฒนามีลักษณะเป็นเว็บแอพพลิเคชั่น เพิ่มความสะดวกในการเข้าใช้งานระบบของเจ้าหน้าที่และผู้บริหารสามารถเข้าถึงข้อมูลได้ตลอด 24 ชั่วโมง
5. ผู้บริหารมีข้อมูลในเรื่องคุณภาพการให้บริการขององค์กร เพื่อนำไปวิเคราะห์และวางแผนต่อไป

บทที่ 2
ทฤษฎีและเทคโนโลยีที่เกี่ยวข้อง

2.1 แนวคิดเชิงวัตถุและยูเอ็มแอล (สุนทริน วงศ์ศิริกุล. 2537)

แนวคิดเรื่องโปรแกรมเชิงวัตถุหรือ OOP (Object-Oriented Programming) เป็นเรื่องที่สำคัญอย่างยิ่งสำหรับนักพัฒนาระบบงานสมัยใหม่ เพราะแนวคิดการโปรแกรมแบบเดิมๆเริ่มจะใช้ไม่ได้ผล หรือไม่ค่อยมีประสิทธิภาพนัก กับงานที่มีขอบเขตของงานขนาดใหญ่และมีความซับซ้อนมากๆ

หลักของการคิดเชิงวัตถุ เป็นการมองการพัฒนาระบบ เหมือนกับการมองโลกแห่งความเป็นจริง คือมองสิ่งต่างๆเป็นวัตถุ หรือ อ็อบเจกต์จะมีคุณสมบัติและการทำงานเฉพาะตัว บางอ็อบเจกต์ก็มีความสัมพันธ์กับอ็อบเจกต์อื่นๆ และถ้าอ็อบเจกต์ที่มีคุณลักษณะบางประการคล้ายๆกัน เราจะจัดกลุ่มให้แก่อ็อบเจกต์เหล่านั้น

ในการแก้ปัญหาเรื่องการออกแบบ ไม่ว่าจะเป็นระบบคอมพิวเตอร์หรือระบบอื่นๆก็ตาม โดยทั่วไปจำเป็นจะต้องมีการใช้เครื่องมือจำพวกโมเดลหรือไดอะแกรมเข้ามาช่วยในการออกแบบ เพื่ออำนวยความสะดวกและทำให้เข้าใจได้ง่ายขึ้น การที่จะเลือกว่าจะใช้โมเดลหรือไดอะแกรมอะไรนั้น ขึ้นอยู่กับว่าปัญหาและวิธีการแก้ไขปัญหามีลักษณะอย่างไร

ในส่วนของการออกแบบและพัฒนาระบบคอมพิวเตอร์ตั้งแต่อดีตจนถึงปัจจุบัน มีเครื่องมือที่ช่วยในการออกแบบและการพัฒนาอยู่หลากหลาย ซึ่งผู้ออกแบบและพัฒนาจะเป็นผู้เลือกใช้เองตามแต่จะเห็นว่าเหมาะสม และสิ่งที่ผู้ออกแบบและพัฒนาระบบตระหนักดีก็คือ ในระบบที่มีการซับซ้อนมากๆ ยังไม่ปรากฏว่าจะมีวิธีแก้ไขปัญหาใดเลยที่ใช้โมเดลเพียง 1 โมเดล แล้วสามารถรองรับกับปัญหาได้ทั้งหมด เราจำเป็นต้องมีการดึงเอาโมเดลหนึ่งมาใช้ในขั้นตอนหนึ่ง และนำเอาอีกโมเดลหนึ่งมาใช้อีกขั้นตอนหนึ่งด้วยเหตุนี้

ในภายหลังจึงได้มีการคิดกันว่า วิธีที่ดีที่สุดคือการนำเอาโมเดลหลายๆโมเดลมาช่วยแก้ปัญหา โดยในแต่ละโมเดลที่ผู้พัฒนาคิดค้นขึ้นมาหรือนำมาใช้นั้น ควรที่จะให้ภาพหรือความชัดเจนในระดับที่แตกต่างกันไป กล่าวคือ โมเดลที่ใช้ควรมีมุมมองได้ครบถ้วน เช่น มุมมองของผู้ออกแบบระบบ มุมมองของผู้พัฒนาโปรแกรม และมุมมองของผู้ใช้งานระบบ เป็นต้น

เพราะฉะนั้น เป้าหมายในขั้นตอนต่อมาคือ จะต้องเลือกเอาโมเดลที่ดีและเหมาะสมที่สุดมาใช้งาน แต่คำถามที่ติดตามมาก็คือ โมเดลที่ดีควรมีลักษณะอย่างไร ซึ่งข้อสรุปข้อใหญ่ที่ผู้ออกแบบ

และพัฒนาระบบสรุปออกมาได้คือ โมเดลที่ดีจะต้องทำให้เกิดวิธีการแก้ไขปัญหาในโลกแห่งความเป็นจริงได้

ทั้งนี้ การที่เราจะหาโมเดลที่ทำให้เกิดวิธีการแก้ไขปัญหาในโลกแห่งความเป็นจริงได้นั้น หมายความว่า วิธีนั้นจะต้องตอบสนองต่อความต้องการของอุตสาหกรรมซอฟต์แวร์ด้วย และในภาพรวมเทคนิคที่อุตสาหกรรมซอฟต์แวร์ ต้องการมีคุณสมบัติดังนี้คือ

- ลดค่าใช้จ่าย
- ลดเวลาในการพัฒนาระบบ
- สามารถจัดการกับความซับซ้อนของปัญหาได้เสมอ ถึงแม้ว่าขอบเขตละขนาดของปัญหาจะขยายใหญ่ขึ้นก็ตาม

ด้วยสาเหตุและความจำเป็นที่ได้กล่าวมาข้างต้น จึงเป็นแรงผลักดันให้บุคคล 3 ท่านอันได้แก่ Grady Booch, James Rumbaugh และ Ivar Jacobson ได้นำเอาโมเดลของตนมารวมกันและมีการพัฒนาปรับปรุงจนกลายมาเป็นภาษาที่ใช้ในการสร้างโมเดลภาษาใหม่ที่เรียกว่า ยูเอ็มแอลUML (Unified Modeling Language)

นับเป็นเรื่องที่สำคัญอย่างยิ่งที่เราจะมีการวางแผนหรือสร้างความคาดหวังไว้ตั้งแต่ต้นว่าระบบงานของเรามีทิศทางไปอย่างไร พร้อมทั้งมีการจัดการในส่วนของการเปลี่ยนแปลงที่อาจเกิดขึ้นมาอย่างระมัดระวัง การสร้างโมเดลจะทำให้เราสามารถพัฒนาระบบงานได้อย่างมีขั้นตอน และมีความเข้าใจในระบบงานที่กำลังจะพัฒนามากขึ้น

เป้าหมายของโมเดลที่ใช้ในการพัฒนาซอฟต์แวร์ คือ

- โมเดลช่วยให้เราสามารถมองเห็นภาพของระบบงานได้ชัดเจนขึ้นว่า ระบบงานจะออกมาในลักษณะไหน หรือมองเห็นภาพว่า เราต้องการให้ระบบงานออกมาในทิศทางใด
- โมเดลจะทำให้เราสามารถระบุถึงโครงสร้างและพฤติกรรมของระบบงานที่จะพัฒนาได้
- โมเดลเป็นเสมือนเทมเพล็ตให้แก่การสร้างระบบงานจริงๆ
- โมเดลช่วยให้เราสามารถทำให้การตัดสินใจในเรื่องต่างๆอยู่ในรูปของเอกสารอ้างอิงได้ง่ายขึ้น

การใช้โมเดลไม่ได้จำกัดเฉพาะกับระบบงานที่มีความซับซ้อนเท่านั้น ระบบงานขนาดเล็กก็สามารถใช้โมเดลเข้ามาช่วยได้

ยูเอ็มแอล (UML) ย่อมาจาก United Modeling Language เป็นภาษาเพื่อใช้อธิบายโมเดลต่างๆ ถ้าพูดถึงภาษา เราจะนึกถึงข้อความ (Text) ที่มีไวยากรณ์ต่างๆ แต่ภาษาอีกรูปแบบหนึ่งที่เราอาจจะไม่ค่อยได้คุ้นเคยกันก็คือ ภาษาที่มีลักษณะของภาษาสัญลักษณ์ที่ใช้อธิบายแสดงรายละเอียด กล่าวคือ UML เป็น ภาษาสัญลักษณ์หรือภาษาที่ใช้กราฟิกเป็นสัญลักษณ์ โดยภาษาในลักษณะนี้ จะใช้กับคนเฉพาะบางกลุ่ม เช่น นักออกแบบ หรือนักพัฒนาระบบคอมพิวเตอร์ เป็นต้น

ยูเอ็มแอลไดอะแกรม (UML Diagram) ประกอบด้วยแบบจำลองทางสถาปัตยกรรมของระบบในมุมมองต่าง ๆ ซึ่งประกอบไปด้วยไดอะแกรมต่างๆ โดยแต่ละไดอะแกรมให้มุมมองในแง่มุมที่แตกต่างกัน เพื่อให้เข้าใจระบบงานมากขึ้น

2.2 Perl

Perl ย่อมาจาก Practical Extraction and Report Language โดย Perl พัฒนาขึ้นในปี ค.ศ. 1986 โดยนาย Larry Wall มีรากฐานการพัฒนามาจากภาษา C ในปัจจุบัน Perl ถูกนำมาใช้พัฒนาในการจัดการข้อมูลบนอินเทอร์เน็ทและการสร้างแอ็พพลิเคชั่นขึ้น

เหตุผลที่ต้องเลือกใช้ภาษา Perl

1. Perl นั้นเป็นของฟรี ไม่ต่องเสียค่าลิขสิทธิ์
2. ติดตั้งมาแล้วกับยูนิกส์หรือ ลินุกส์
3. สามารถติดตั้งบน Win 32 ได้
4. ผู้ที่มีพื้นฐานภาษาซีจะสามารถเขียนภาษา Perl ได้ง่าย เพราะมีรากฐานมาจากภาษาซี มีฟังก์ชันสำเร็จรูปมาให้ ทำให้สะดวกในการพัฒนาระบบ
5. มีแหล่งข้อมูลเพื่อสืบค้นมากมาย ทั้งจากหนังสือและในอินเทอร์เน็ต

รูปแบบของการโค้ด Perl ดังตัวอย่างต่อไปนี้

```
#!/usr/bin/perl
print "Content-type: text/html\n\n";
```

#!/usr/bin/perl หมายถึงการแจ้งให้ สคริปต์Perl ทราบว่าเส้นทางของคอมไพเลอร์อยู่ที่ใดบนเซิร์ฟเวอร์

(เฉพาะบน ยูนิกส์ ส่วนบนวินโดวส์ไม่ต้องมี)

print "Content-type: text/html\n\n"; เป็นการแจ้งให้เว็บบราวเซอร์ทราบว่า ข้อมูลที่ส่งมาเป็นข้อมูลรูปแบบ html

2.3 PHP (สมประสงค์ ธิตินิลนิธิ. 2547)

PHP ย่อมาจาก Hypertext Preprocessor เป็นภาษาสคริปต์ด้านเซิร์ฟเวอร์ เช่นเดียวกันกับ ASP ซึ่งรูปแบบในการเขียนคำสั่งการทำงานนั้นจะมีลักษณะคล้ายกับภาษา Perl หรือภาษา C และสามารถใช้ร่วมงานกันกับ ภาษา HTML ได้อย่างมีประสิทธิภาพ

โดยที่ PHP นั้นสามารถที่จะติดต่อกับโปรแกรมจัดการฐานข้อมูลที่มีอยู่มากมาย เช่น Microsoft Access Sybase MySQL Oracle MS SQL Server เป็นต้น

จากที่กล่าวไปข้างต้นแล้วว่า PHP ก็เป็นภาษาสคริปต์ด้านเซิร์ฟเวอร์ อีกภาษาหนึ่งเช่นเดียวกันกับ ASP แต่คุณสมบัติที่มากกว่าก็คือ

1. PHP นั้นสามารถรันบนระบบปฏิบัติการได้มากมาย เช่น Windows, Unix, Linux
2. PHP นั้นรองรับกับการใช้งานร่วมกับโปรแกรมเว็บเซิร์ฟเวอร์จำลองมากมาย เช่น Apache, IIS และอื่นๆ
3. PHP นั้นเป็นของฟรี ไม่ต่องเสียค่าลิขสิทธิ์

รูปแบบการเขียนโค้ด PHP ร่วมกับ HTML แบบปกติ จะมีรูปแบบดังนี้

```
<?php
        คำสั่งในภาษา PHP ;
?>
```

การเขียนโค้ดในรูปแบบ JavaScript จะมีรูปแบบดังนี้

```
<Script Language="php">
        คำสั่งในภาษา PHP ;
</Script>
```

การทำงานของเว็บเพจที่ฝังสคริปต์ภาษา PHP ไว้ เมื่อเว็บบราวเซอร์ร้องขอไฟล์ PHP ไฟล์ใด เว็บเซิร์ฟเวอร์จะเรียก PHP engine ขึ้นมาแปล และประมวลผลคำสั่งที่อยู่ในไฟล์ PHP นั้น โดยอาจมีการดึงข้อมูลจากฐานข้อมูล หรือเขียนข้อมูลลงไปยังฐานข้อมูลด้วย หลังจากนั้นผลลัพธ์ในรูปแบบ HTML (และสคริปต์ที่ทำงานทางฝั่งบราวเซอร์ เช่น JavaScript จะถูกส่งกลับไปยังบราวเซอร์ บราวเซอร์ก็จะแสดงผลตามคำสั่ง HTML ที่ได้รับมา ซึ่งย่อมไม่มีคำสั่ง PHP ใดๆ หลงเหลืออยู่ เนื่องจากถูกแปลและประมวลผลโดย PHP Engine ที่ฝั่งเซิร์ฟเวอร์ไปหมดแล้ว

การฝังสคริปต์ PHP ไว้ในเว็บเพจ ช่วยให้เราสร้างเว็บเพจแบบ dynamic ได้ ซึ่งหมายถึงเว็บเพจที่มีเนื้อหาสาระและ/หรือหน้าตาเปลี่ยนแปลงไปได้ในแต่ละครั้งที่ผู้ใช้เปิดดู โดยขึ้นอยู่กับ

เงื่อนไขต่างๆ เช่น ข้อมูลที่ผู้ใช้ส่งมาให้ (ผ่านมาทางฟอร์มของ HTML) ข้อมูลในฐานข้อมูล และอื่นๆ

PHP Engine จะแปลและประมวลผลเฉพาะคำสั่งที่อยู่ภายในแท็กของ PHP เท่านั้น การทำงานที่เกิดขึ้นคือ หลังจาก PHP Engine ถูกเว็บเซิร์ฟเวอร์เรียกขึ้นมาประมวลผลไฟล์ PHP แล้ว มันจะส่งผ่านเนื้อหาของไฟล์ไปยังบราวเซอร์โดยไม่ทำอะไรกับเนื้อหานั้น ยกเว้นเมื่อพบกับสัญลักษณ์ (แท็ก) ที่ระบุจุดเริ่มต้นของบล็อคคำสั่ง PHP มันก็จะแปลและประมวลผลคำสั่งต่างๆไปตามลำดับ (ภายในบล็อค PHP นี้ การส่งผลลัพธ์ให้แก่บราวเซอร์ เราจะต้องเรียกใช้คำสั่ง/ฟังก์ชั่นของ PHP เช่น echo หรือ print เอาเอง) โดยเมื่อพบสัญลักษณ์ปิดท้ายบล็อคคำสั่ง PHP engine ก็จะหันกลับมาส่งผ่านเนื้อหาของไฟล์ต่อไปเช่นเดิม จนกว่าจะพบสัญลักษณ์ระบุจุดเริ่มต้นของบล็อคคำสั่ง PHP อีก และเป็นอย่างนี้เรื่อยไปจนจบไฟล์

ความสามารถของ PHP มีหลายอย่าง ได้แก่

1. ความสามารถในการจัดการกับตัวแปรหลายๆประเภท เช่น เลขจำนวนเต็ม, เลขทศนิยม, สตริง และอาร์เรย์ เป็นต้น
2. ความสามารถในการรับข้อมูลจากฟอร์มของ HTML
3. ความสามารถในการรับ-ส่งคุกกี้
4. ความสามารถเกี่ยวกับ เซสชั่น (ตั้งแต่ PHP เวอร์ชั่น 4 ขึ้นไป)
5. ความสามารถทางด้าน OOP (Object Oriented Programming) ซึ่งรองรับการเขียนโปรแกรมเชิงวัตถุ
6. ความสามารถในการติดต่อและจัดการฐานข้อมูล
7. ความสามารถในการสร้างภาพกราฟิก

2.4 MySQL

MySQL เป็นฐานข้อมูลแบบ Open Source ที่ได้รับความนิยมในการใช้งานสูงสุดโปรแกรมหนึ่งบนเครื่องให้บริการ มีความสามารถในการจัดการกับฐานข้อมูลด้วยภาษา SQL (Structure Query Language) อย่างมีประสิทธิภาพ มีความรวดเร็วในการทำงาน รองรับการทำงานจากผู้ใช้หลายๆ คนและหลายๆ งานได้ในขณะเดียวกัน

MySQL ถูกพัฒนาขึ้นโดย MySQL AB โดยมีลิขสิทธิ์การใช้งาน 2 แบบ นั่นคือ ผู้ดูแลระบบสามารถใช้งานซอฟต์แวร์ MySQL ได้โดยไม่มีค่าใช้จ่ายใดๆ ภายใต้ลิขสิทธิ์ของ GNU General Public License หรืออาจเลือกใช้แบบที่มีลิขสิทธิ์ทางการค้าของ MySQL AB ซึ่งเป็นผู้ผลิตและพัฒนาซอฟต์แวร์โดยตรงก็ได้

คำอธิบายเพิ่มเติมเกี่ยวกับหน้าที่ ความสามารถและการทำงานของโปรแกรม MySQL มีดังต่อไปนี้

1. MySQL ถือเป็นระบบจัดการฐานข้อมูล (DataBase Management System (DBMS)) ฐานข้อมูลมีลักษณะเป็นโครงสร้างของการเก็บรวบรวมข้อมูล การที่จะเพิ่มเติม เข้าถึง หรือประมวลผลข้อมูลที่เก็บในฐานข้อมูล จำเป็นจะต้องอาศัยระบบจัดการฐานข้อมูล ซึ่งจะทำหน้าที่เป็นตัวกลางในการจัดการกับข้อมูลในฐานข้อมูล ทั้งสำหรับการใช้งานเฉพาะ และรองรับการทำงานของแอพลิเคชันอื่นๆ ที่ต้องการใช้งานข้อมูลในฐานข้อมูล เพื่อให้ได้รับความสะดวกในการจัดการกับข้อมูลจำนวนมาก MySQL ทำหน้าที่เป็นทั้งตัวฐานข้อมูลและระบบจัดการฐานข้อมูล
2. MySQL เป็นระบบจัดการฐานข้อมูลแบบเชิงสัมพันธ์ ฐา นข้อมูลเชิงสัมพันธ์ จะเก็บข้อมูลทั้งหมดในรูปแบบของตารางแทนการเก็บข้อมูลทั้งหมดลงในไฟล์เพียงไฟล์เดียว ทำให้ทำงานได้รวดเร็วและมีความยืดหยุ่น นอกจากนั้น แต่ละตารางที่เก็บข้อมูลสามารถเชื่อมโยงเข้าหากันทำให้สามารถรวมหรือจัดกลุ่มข้อมูลได้ตามต้องการ โดยอาศัยภาษา SQL ที่เป็นส่วนหนึ่งของโปรแกรม MySQL ซึ่งเป็นภาษามาตรฐานในการเข้าถึงฐานข้อมูล
3. MySQL แจกจ่ายให้ใช้งานแบบเปิดเผยซอร์ส (Open Source) นั่นคือ ผู้ใช้งาน MySQL ทุกคนสามารถใช้งานและปรับแต่งการทำงานได้ตามต้องการ สามารถดาวน์โหลดโปรแกรม MySQL ได้จากอินเทอร์เน็ตและนำมาใช้งานโดยไม่มีค่าใช้จ่ายใดๆ

นอกจากนั้น MySQL ถูกออกแบบและพัฒนาขึ้นมาเพื่อทำหน้าเป็นเครื่องให้บริการรองรับการจัดการกับฐานข้อมูลขนาดใหญ่ ซึ่งการพัฒนายังคงดำเนินอยู่อย่างต่อเนื่อง ส่งผลให้มีฟังก์ชันการทำงานใหม่ๆ ที่อำนวยความสะดวกแก่ผู้ใช้งานเพิ่มขึ้นอยู่ตลอดเวลา รวมไปถึงการปรับปรุงด้านความต่อเนื่อง ความเร็วในการทำงาน และความปลอดภัย ทำให้ MySQL เหมาะสมต่อการนำไปใช้งานเพื่อเข้าถึงฐานข้อมูลบนเครือข่ายอินเทอร์เน็ต

2.5 ไอพีแอดเดรส (เอกสิทธิ์ วิริยจารี. 2548)

หมายเลขไอพีแอดเดรส (IP Address) เป็นแอดเดรสที่ผู้ติดตั้งระบบเครือข่ายจำเป็นต้องกำหนดให้กับเครื่องคอมพิวเตอร์ที่รันโพรโทคอลทีซีพีไอพี (TCP/IP) เพื่อใช้บ่งบอกตำแหน่งที่อยู่ของเครื่องคอมพิวเตอร์ในระบบ เมื่อเครื่องคอมพิวเตอร์ต้องการส่งข้อมูลไปให้เครื่องปลายทางโดยอาศัยโพรโทคอลทีซีพีไอพีจำเป็นต้องระบุหมายเลขไอพีแอดเดรสของเครื่องปลายทางให้ถูกต้อง และในทางกลับกัน เมื่อเครื่องปลายทางต้องการส่งข้อมูลกลับไปเครื่องต้นทาง จะมีการอ้างตำแหน่งของเครื่องต้นทางด้วยหมายเลขไอพีแอดเดรสอีกเช่นเดียวกัน

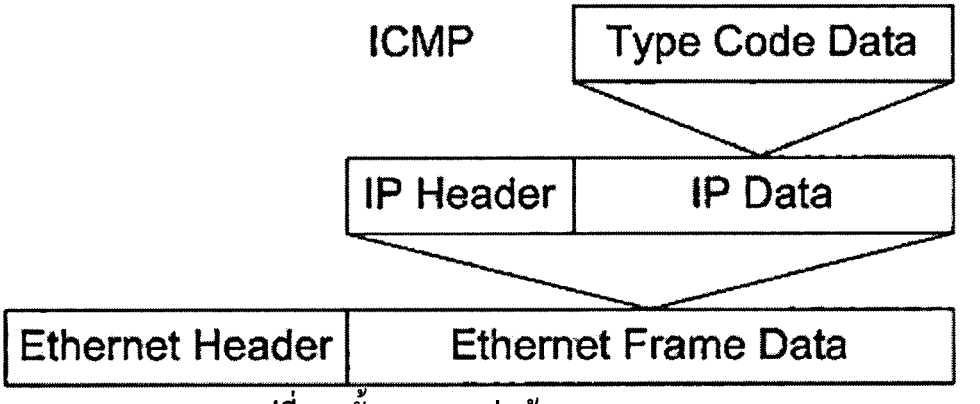
มาตรฐานของไอพีแอดเดรสปัจจุบันเป็นมาตรฐานเวอร์ชั่น 4.0 ซึ่งได้กำหนดไอพีแอดเดรสมีทั้งหมด 32 บิต หรือ 4 ไบต์ แต่ละไบต์จะถูกคั่นด้วยจุด (.) ตัวอย่างเช่น 168.108.2.12 แต่อย่างไรก็ดี ภายในหมายเลขที่เราเห็นนี้ยังถูกแบ่งออกเป็น 2 ส่วนดังนี้

1. ส่วนแรกเรียกว่า หมายเลขเน็ตเวิร์กแอดเดรส (Network Address)
2. ส่วนที่สองเรียกว่า หมายเลข โฮสท์แอดเดรส (Host Address)

สำหรับบนอินเทอร์เฟซของเราเตอร์แต่ละอินเทอร์เฟซ ก็จำเป็นต้องได้รับการกำหนดหมายเลขไอพีแอดเดรสและซับเน็ตมาสค์ (Subnet Mask) ขึ้นมาเช่นกัน โดยหมายเลขไอพีแอดเดรสที่ระบุลงไปบนอินเทอร์เฟซของเราเตอร์จะต้องเป็นหมายเลขไอพีแอดเดรสที่เหมาะสม และไม่ซ้ำกันกับหมายเลขไอพีแอดเดรสบนอินเทอร์เฟซอื่นๆ

ซับเน็ตมาสค์ เป็นพารามิเตอร์อีกตัวหนึ่งที่ต้องระบุควบคู่กับหมายเลขไอพีแอดเดรส หน้าที่ของซับเน็ตมาสค์ก็คือ การช่วยในการแยกแยะว่าส่วนใดภายในหมายเลขไอพีแอดเดรสเป็นหมายเลขเน็ตเวิร์กแอดเดรส และส่วนใดเป็นหมายเลขโฮสท์แอดเดรส ดังนั้น จะสังเกตได้ว่าเมื่อระบุหมายเลขไอพีแอดเดรสให้กับเครื่องคอมพิวเตอร์ จำเป็นต้องระบุซับเน็ตมาสค์กำกับลงไปด้วยทุกครั้ง

2.6 โพรโทคอล ไอซีเอ็มพี (เอกสิทธิ์ วิริยจารี. 2548)



รูปที่ 2.1 ขั้นตอนการห่อหุ้ม ICMP Packet

โพรโทคอลไอซีเอ็มพี เป็นโพรโทคอลที่ช่วยในการแจ้งสถานะ หรือรายงานข้อผิดพลาดที่เกิดขึ้นกับการทำงานของโพรโทคอลทีซีพีไอพี(TCP/IP) ให้กับโฮสต์ต้นทางหรือกับเราเตอร์ทราบ อย่างไรก็ตาม โพรโทคอลไอซีเอ็มพีนั้น เพียงแต่แจ้งรายงานปัญหาหรือสถานะต่างๆเท่านั้น แต่ไม่ได้ช่วยแก้ปัญหาให้โดยตรง แต่ข้อความต่างๆที่มันแจ้งให้ทราบ จะมีประโยชน์ต่อผู้ดูแลระบบ

เครือข่ายในการวิเคราะห์ปัญหาต่างๆที่เกิดได้ง่ายขึ้น โดยทั้งโฮสต์ต้นทาง ปลายทาง หรือเราเตอร์มีสิทธิ์ส่งแพ็กเก็ตไอซีเอ็มพีออกมาได้ทั้งสิ้น

แพ็กเก็ตของโพรโทคอลไอซีเอ็มพีจะถูกห่อหุ้มลงมาในแพ็กเก็ตไอพีอีกทีหนึ่ง ดังแสดงในรูปโดยภายในแพ็กเก็ตไอซีเอ็มพีเองจะประกอบด้วยฟิลด์ต่างๆได้แก่ Type, Code และ Data โดย Type จะเป็นตัวกำหนดประเภทของแพ็กเก็ต ICMP ว่าเกี่ยวข้องกับเรื่องใด และ Code จะเป็นเสมือนกับซับฟิล์ดย่อยที่ช่วยบอกรายละเอียดหรือให้ข้อมูลเพิ่มเติมเกี่ยวกับ Type นั้นๆอีกทีหนึ่ง

2.6.1 ICMP Type 8 และ Type 0- Echo Request และ Echo Reply

Type หรือประเภทของแพ็กเก็ต ICMP ที่พบบ่อยที่สุด เห็นจะหนีไม่พ้น Type8 และ Type0 โดยทั้งสอง Type นี้ได้ถูกใช้งานโดยโปรแกรมที่เรารู้จักกันดีในนาม ping เมื่อเราออกคำสั่ง ping แล้วตามด้วย IP Address ของโฮสต์ปลายทางเพื่อ

1. ทดสอบหรือตรวจดูสถานะของเครื่องโฮสต์ปลายทางว่า ขณะนี้ยังมีชีวิตอยู่หรือไม่ และ
2. เพื่อทดสอบเน็ตเวิร์กจากต้นทางไปยังปลายทางว่ายังใช้งานได้ตามปกติหรือไม่

สิ่งที่โปรแกรม ping กระทำก็คือ มันจะส่งแพ็กเก็ต ICMP ที่มี Type เป็นหมายเลข 8 ซึ่งหมายถึง ICMP Type Echo Request ไปยังเครื่องปลายทาง ถ้าสถานะที่ต้องการทั้ง 2 ข้อเป็นจริงคือเครื่องปลายทางทำงานและเน็ตเวิร์กอยู่ในสถานะปกติ เครื่องโฮสต์ปลายทางจะตอบสนองกลับมาด้วยการส่งแพ็กเก็ต ICMP Type Echo Reply ซึ่งเป็นหมายเลข Type 0 ถ้าโฮสต์ต้นทางได้รับ ICMP Echo Reply กลับมา นั่นแสดงว่าทุกอย่างเรียบร้อย

ใน ICMP Type นี้จะใช้เฉพาะค่าฟิลด์ Type ที่เป็น 8 หรือ 0 เท่านั้น และไม่ใช้ค่าฟิลด์ Code จึงปล่อยไว้ให้เป็น 0 ไป

2.6.2 ICMP Type 3-Destination Uncreachable

ถ้าเราเตอร์ไม่สามารถส่งผ่านแพ็กเก็ตต่อไปให้ถึงโฮสต์ปลายทางได้ ไม่ว่าจะด้วยสาเหตุใดก็แล้วแต่ มันจะส่งแพ็กเก็ต ICMP ที่มี Type เท่ากับ 3 กลับไปให้โฮสต์ต้นทาง เพื่อแจ้งสถานะให้ทราบ ส่วนสาเหตุว่าทำไมจึงไปไม่ถึงนั้น จะอยู่ในฟิลด์ Code ซึ่งมีอยู่ด้วยกันหลาย Code ได้แก่

Code = 0 หมายถึง Network Unreachable

Code = 1 หมายถึง Host Unreachable

Code = 2 หมายถึง Protocol Unreachable

Code = 3 หมายถึง Port Unreachable

Code = 4 หมายถึง Fragmentation needed and do not fragment bit set

Code = 5 หมายถึง Source Route Failed

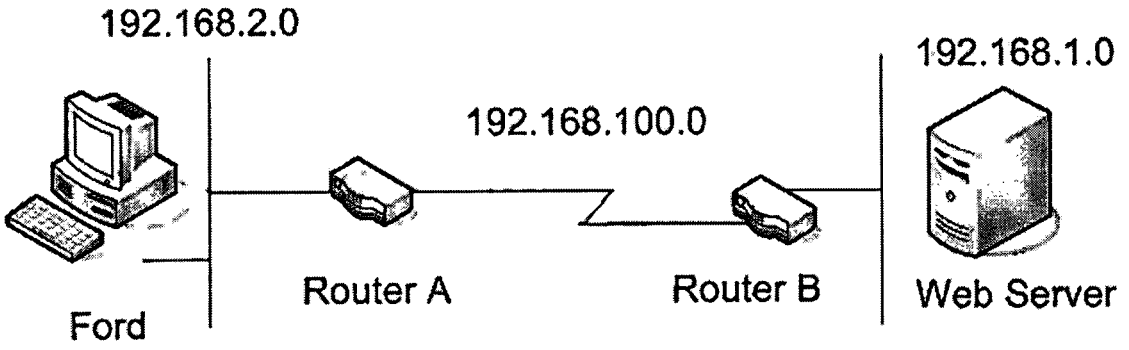
โดย Code ที่พบบ่อยคือ Code 0 และ Code 1 ดังนี้

Code 0 Network Unreachable เป็นไปได้ว่าซับเน็ตแอดเดรสปลายทางไม่มีอยู่ในเราติ้งเทเบิลของเราเตอร์ ทำให้เราเตอร์ไม่ทราบเส้นทางว่า ในการส่งแพ็กเก็ตไปยังซับเน็ตแอดเดรสปลายทางนั้น จะต้องส่งแพ็กเก็ตออกไปทางอินเทอร์เฟซใด

Code 1 Host Unreachable เป็นไปได้ว่า เราเตอร์ทราบเส้นทางในการส่งแพ็กเก็ต (เพราะมีอยู่ในเราติ้งเทเบิลแล้ว) แต่เมื่อพยายามส่งให้ไปหาโฮสต์ปลายทางกลับส่งไม่ได้ เช่น บังเอิญโฮสต์ปลายทางได้ดาวน์หรือแครชไป หรือเน็ตเวิร์กระหว่างเราเตอร์ตัวนั้นกับโฮสต์ปลายทางมีปัญหา หรือแอดเดรสปลายทางของโฮสต์ไม่ถูกต้อง

Code 0 และ Code 1 นี้จะถูกส่งจากเราเตอร์กลับมายังโฮสต์ต้นทาง

จากรูป2.2ตัวอย่างการเชื่อมต่อเครือข่าย



รูปที่ 2.2 ตัวอย่างการเชื่อมต่อเครือข่าย

กรณีที่หนึ่ง: ถ้าเครื่อง Ford ต้องการติดต่อกับเว็บเซิร์ฟเวอร์แน่นอนว่ามันต้องส่งแพ็กเก็ตไปให้เราเตอร์ A ก่อน ถ้าเราเตอร์ A ไม่รู้เส้นทางที่จะส่งต่อไปยัง 192.168.1.0 (ซึ่งเป็นสับเน็ตแอดเดรสของเว็บเซิร์ฟเวอร์) เราเตอร์ A จะส่งแพ็กเก็ต ICMP Type 3 (Destination Unreachable) และ Code 0-Network Unreachable กลับมาแจ้งให้เครื่องต้นทางคือ Ford ทราบ

กรณีที่สอง: ถ้าเครื่อง Ford ต้องการติดต่อกับเว็บเซิร์ฟเวอร์ เช่นเดิม คราวนี้เราเตอร์ A ทรบแล้ว (จากตารางเราติ้งเทเบิล) ว่าต้องส่งต่อไปให้เราเตอร์ B เมื่อแพ็กเก็ตไปถึงเราเตอร์ B เราเตอร์ B ก็จะตรวจสอบเส้นทางต่อ พบว่ามันสามารถส่งตรงไปยังเว็บเซิร์ฟเวอร์ ได้เลย แต่ถ้าเว็บเซิร์ฟเวอร์ดาวน์ลงไป เราเตอร์ B จะไม่ได้รับ ARP Reply กลับมาเมื่อทำ ARP Request เพื่อหา MAC Address

ของเว็บเซิร์ฟเวอร์ ดังนั้น เราเตอร์ B จะส่งแพ็คเก็ต ICMP Type 3 (Destination Unreachable), Code1-Host Unreachable กลับไปแจ้งให้เครื่องต้นทาง Ford ทราบ

ในกรณีที่ทดลองใช้คำสั่ง Ping ไปยังเครื่องโฮสต์ปลายทางที่อยู่ต่างซับเน็ตกัน แล้ว ping ไม่ได้ โดยข้อความจะแจ้งข้อผิดพลาดขึ้นมาเป็น Destination Unreachable สามารถตรวจสอบดูเราติ้งเทเบิลบนโฮสต์ต้นทางและบนเราเตอร์ระหว่างทาง เพราะมีแนวโน้มเป็นไปได้ว่า

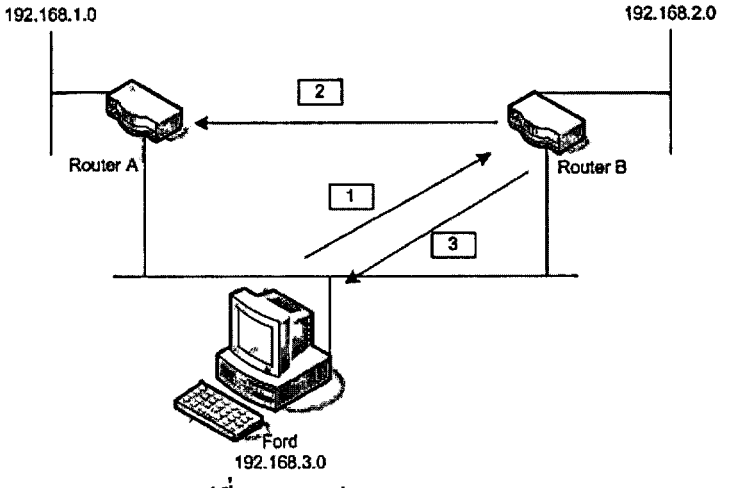
1. ที่เครื่องโฮสต์ต้นทางไม่ได้เซตหมายเลข IP Address ของดีฟอลต์เกตเวย์ไว้ หรือ
2. ตารางเราติ้งเทเบิ้ลบนเราเตอร์มีข้อมูลไม่ครบถ้วน

2.6.3 ICMP Type 4, Code 0 – Source Quench

แพ็กเก็ต ICMP ประเภทนี้จะถูกส่งจากเราเตอร์ไปแจ้งให้โฮสต์ต้นทางหรือไปแจ้งให้เราเตอร์อื่นที่เชื่อมต่ออยู่ด้วยโดยตรงทราบ เพื่อให้โฮสต์ต้นทางหรือเราเตอร์ตัวอื่นลดอัตราการส่งแพ็กเก็ตที่เข้ามาหาตัวมัน เพราะถ้าหากส่งมาเร็วไป มันจะรับไม่ทัน แพ็กเก็ตอาจล้นบัฟเฟอร์และสูญหายในที่สุด

2.6.4 ICMP Type 5 – Redirect

ปกติโฮสต์ต้นทางอย่างเช่นวินโดว์ไคลแอนต์ มักเซตดีฟอลต์เกตเวย์ให้ชี้ไปยังเราเตอร์เพียงตัวเดียวอยู่แล้วเพื่อความสะดวก ดังนั้น ไม่ว่าซับเน็ตปลายทางที่โฮสต์ต้นทางต้องการติดต่อด้วยจะเป็นซับเน็ตไหนก็แล้วแต่ มันจะส่งออกไปยังดีฟอลต์เกตเวย์ทุกครั้ง แต่ในบางสถานการณ์ ถ้าเราเตอร์ที่ทำหน้าที่เป็นดีฟอลต์เกตเวย์ให้กับเครื่องต้นทางพบว่า โฮสต์ต้นทางควรส่งแพ็กเก็ตออกไปทางเราเตอร์ตัวอื่นจะเร็วกว่า เราเตอร์นั้นจะส่ง ICMP Redirect แจ้งกลับมาให้โฮสต์ต้นทางทราบว่าในอนาคตถ้าต้องการติดต่อกับซับเน็ตแอ็ดเดรสนั้นๆ ให้ส่งไปหาเราเตอร์ตัวอื่นแทนดังรูป



รูปที่ 2.3 การส่ง ICMP Redirect

จากรูป 2.3 การส่ง ICMP Redirect

ขั้นที่ 1 เครื่อง Ford ต้องการติดต่อกับ Subnet 192.168.1.0 ซึ่งอยู่ต่างซับเน็ตกัน ดังนั้น จึงส่งแพ็กเก็ตนี้ไปหาเราเตอร์ B ซึ่งเป็นดีฟอลต์เกตเวย์

ขั้นที่ 2 เราเตอร์ B สามารถส่งผ่านแพ็กเก็ตต่อไปยังเราเตอร์ A ได้ เพื่อให้เราเตอร์ A ส่งแพ็กเก็ตต่อไปยังโฮสต์ในซับเน็ต 192.168.1.0

ขั้นที่ 3 เนื่องจากเราเตอร์ B พบว่าเครื่อง Ford น่าจะส่งแพ็กเก็ตไปยังเราเตอร์ A ได้ทันที โดยไม่ต้องผ่านเราเตอร์ B จึงส่ง ICMP Redirect แจ้งกลับมาแนะนำเครื่อง Ford ให้ Ford ทราบ เพื่อว่าในอนาคตหาก Ford ต้องการส่งแพ็กเก็ตไปยัง 192.168.1.0 Ford ก็จะสามารถส่งไปหาเราเตอร์ A ได้เลยทันที ซึ่งจะเร็วกว่ามาผ่านที่ตัวเราเตอร์ B ก่อน (ไม่ต้องอ้อม 2 Hop ส่งตรงเลยแค่ Hop เดียว) Ford จะนำเอาสิ่งที่เราเตอร์ B แจ้งกลับมาไปรวมไว้ในเราติ้งเทเบิ้ลของเราเตอร์ B ด้วย เพื่อไว้ใช้หาเส้นทางในครั้งถัดไป

นอกจาก Type ต่างๆ ที่กล่าวไปข้างต้นแล้ว ยังมี Type อื่นๆอีกหลาย Type เช่น

ICMP Type 11 – Time exceeded for datagram

ICMP Type 12 – Parameter problem on datagram

ICMP Type 13 – Timestamp Request

ICMP Type 14 – Timestamp Reply

ICMP Type 17 – Address Mask Request

ICMP Type 18 – Address Mask Reply

อย่างไรก็ดี การอิมพลีเมนต์ ICMP Type ต่างๆนี้ จะขึ้นกับระบบปฏิบัติการและขึ้นกับอุปกรณ์เน็ตเวิร์กด้วยว่าจะบรรจุการสนับสนุนการส่ง ICMP Type ใดเข้าไปบ้าง

ตัวอย่างการส่งไอซีเอ็มพี แพ็กเก็ตด้วยคำสั่ง ping ในระบบปฏิบัติการลินุกส์ และไม่มีแพ็กเก็ตใดๆตอบกลับมาสามารถแสดงได้ดังรูปที่ 2.4 และตัวอย่างกรณีมีแพ็กเก็ตตอบกลับมาแสดงได้ดังรูปที่ 2.5

```
$
$
$ ping 202.47.249.1
PING 202.47.249.1 (202.47.249.1): 56 data bytes

--- 202.47.249.1 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
$
$
$
```

รูปที่ 2.4 การใช้คำสั่ง ping แล้วไม่มีแพ็กเก็ตใดๆตอบกลับ

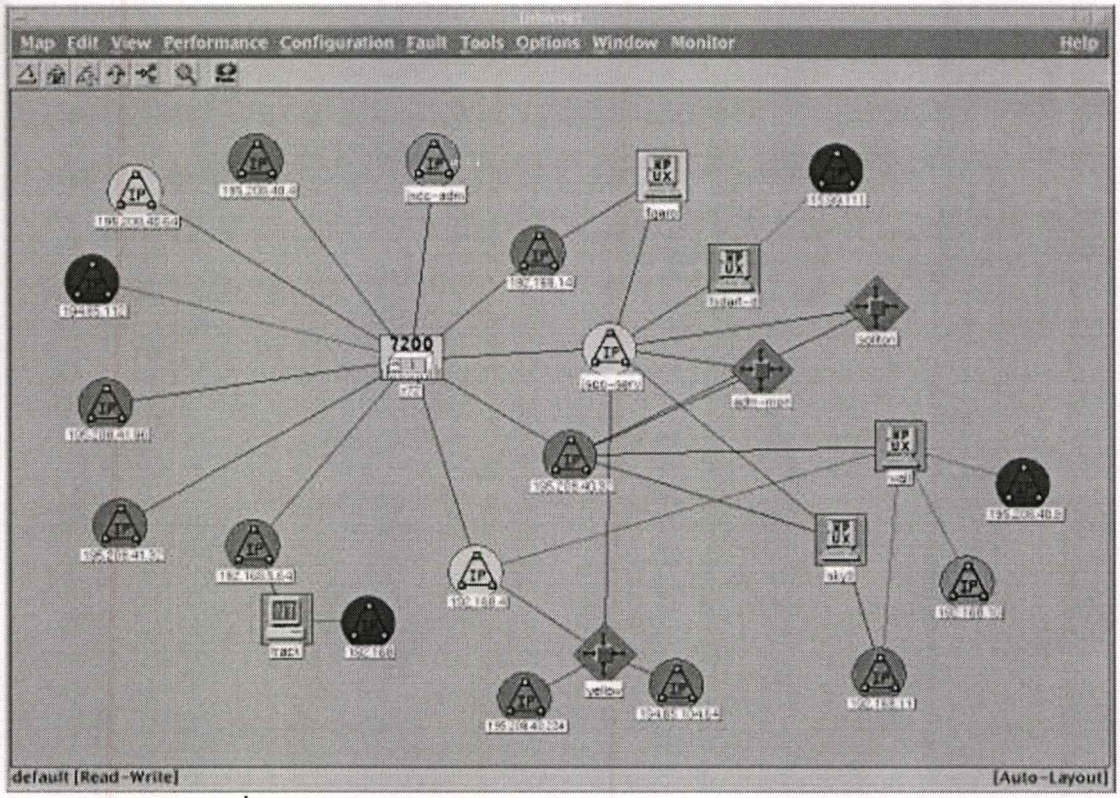
```
$
$
$ ping 202.47.249.7
PING 202.47.249.7 (202.47.249.7): 56 data bytes
64 bytes from 202.47.249.7: icmp_seq=0 ttl=246 time=1.973 ms
64 bytes from 202.47.249.7: icmp_seq=1 ttl=246 time=1.519 ms
64 bytes from 202.47.249.7: icmp_seq=2 ttl=246 time=1.461 ms
64 bytes from 202.47.249.7: icmp_seq=3 ttl=246 time=2.051 ms
64 bytes from 202.47.249.7: icmp_seq=4 ttl=246 time=1.533 ms

--- 202.47.249.7 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.461/1.707/2.051/0.251 ms
$
$
```

รูปที่ 2.5 การใช้คำสั่ง ping แล้วมีแพ็กเก็ตตอบกลับ

บทที่ 3
การวิเคราะห์ระบบปัจจุบัน

3.1 ระบบที่ใช้ทำงานในปัจจุบัน

ระบบสารสนเทศที่ใช้ในการเฝ้าสังเกตเครือข่ายในปัจจุบัน มีทั้งซอฟท์แวร์ที่ต้องเสียค่าใช้จ่ายและไม่เสียค่าใช้จ่าย ระบบเฝ้าสังเกตเครือข่ายที่นิยมใช้ในการบริหารจัดการเครือข่ายขนาดใหญ่ๆ ในปัจจุบันได้แก่โปรแกรม HP Openview ซึ่งเป็นโปรแกรมที่จะตอบสนองหรือแก้ไขเหตุการณ์ที่สำคัญโดยอัตโนมัติ สามารถรายงานเหตุเร่งด่วนให้ผู้ใช้งานทราบเพื่อแก้ปัญหาทันที โดยสามารถรายงานเหตุสำคัญผ่านอีเมล มีระบบแสดงผลที่ใช้สีเพื่อบอกสีที่แตกต่างโดยขึ้นอยู่กับระดับความสำคัญและผลกระทบของปัญหา ดังรูปที่ 3.1



รูปที่ 3.1 ตัวอย่างการแสดงผลของโปรแกรม HP Openview

ห้องสมุดคณะเทคโนโลยีสารสนเทศ ๔๐๘.

3.2 ปัญหาของระบบการทำงานในปัจจุบัน

ระบบสารสนเทศที่ใช้ในการเฝ้าสังเกตเครือข่ายในปัจจุบันมีปัญหาดังต่อไปนี้

1. ระบบเฝ้าสังเกตเครือข่ายจะมีราคาแพง ทั้งด้านค่าซอฟท์แวร์และฮาร์ดแวร์ที่ใช้ในการติดตั้งระบบ รวมถึงค่าดูแลรักษา
2. การใช้งานระบบเฝ้าสังเกตเครือข่ายมีความซับซ้อน และต้องใช้เจ้าหน้าที่ที่ได้รับการฝึกอบรมเฉพาะ
3. มีความสามารถเกินความจำเป็นที่ไม่ได้ใช้งาน ทำให้ต้องเสียค่าใช้จ่ายในส่วนที่ไม่ได้ใช้งานไปด้วย
4. ในการเข้าถึงและเข้าใช้งานระบบ ต้องลงโปรแกรมที่ใช้ในการเปิดโปรแกรมเฉพาะทำให้ไม่สะดวกในการใช้งาน

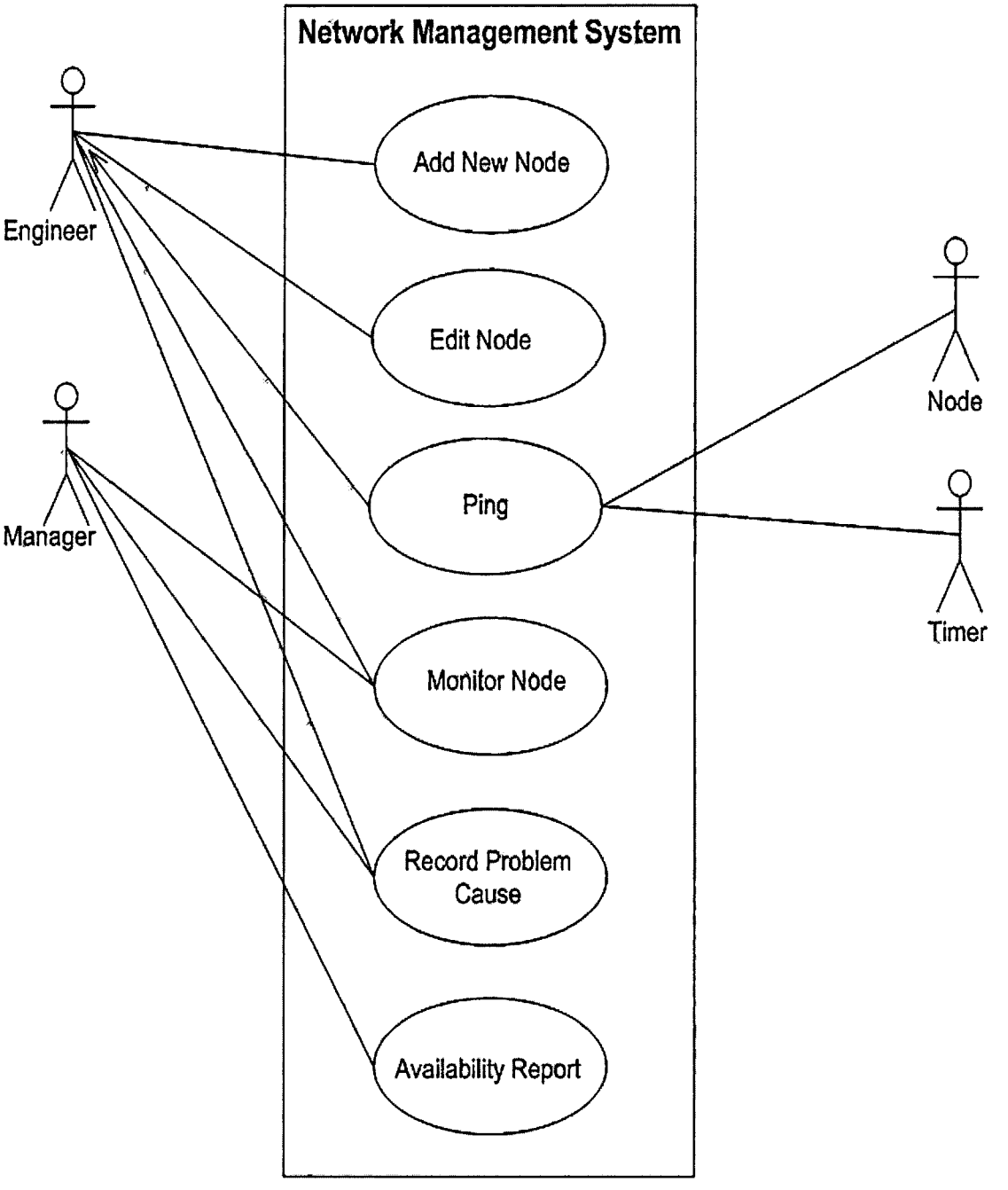
3.3 การวิเคราะห์ความต้องการของผู้ใช้

1. มีระบบที่สามารถเข้าถึงได้ตลอดเวลา โดยใช้โปรแกรมเว็บบราวเซอร์ โดยไม่จำเป็นต้องติดตั้งโปรแกรมใดๆเพิ่ม
2. มีระบบที่มีความปลอดภัยในการเข้าใช้งานและต้องกำหนดสิทธิในการขอเข้าใช้งานระบบได้
3. มีระบบที่สามารถแจ้งปัญหาผ่านทางเว็บแอ็พพลิเคชั่น เพื่อให้ผู้ดูแลระบบเครือข่ายสามารถทราบถึงปัญหาได้ทันที และเก็บข้อมูลของปัญหาต่างๆได้
4. มีระบบที่สามารถสรุปเป็นรายงานคุณภาพการให้บริการของโหนดทั้งหมดได้ เพื่อให้ผู้บริหารสามารถนำมาวิเคราะห์และตัดสินใจ

3.4 การวิเคราะห์ระบบสารสนเทศใหม่

จากการวิเคราะห์ความต้องการของผู้ใช้ เพื่อนำมาออกแบบระบบงานใหม่โดยใช้ UML มาวิเคราะห์และออกแบบเชิงวัตถุ โดยใช้สัญลักษณ์ที่ใช้อธิบายแสดงรายละเอียดจำลองการสร้างเพื่อให้การออกแบบซอฟต์แวร์ทำได้โดยง่าย และเพื่อเป็นเครื่องมือในการสื่อสารให้เกิดความเข้าใจตรงกันระหว่างผู้ใช้งานกับนักวิเคราะห์ระบบ

การนำความต้องการของระบบมาสร้างเป็นยูสเคสไดอะแกรม เป็นการบอกและเน้นผู้ใช้งานว่าต้องการทำอะไรในระบบ โดยพิจารณาจากมุมมองของผู้ใช้ ซึ่งประกอบด้วยแอกเตอร์ (Actor) และ ยูสเคส (Use Case) ต่าง ๆ ดังแสดงได้ดังรูปที่ 3.2 ดังนี้



รูปที่ 3.2 ยูสเคสไดอะแกรมของระบบเฝ้าสังเกตเครือข่ายสารสนเทศ

3.4.1 แอกเตอร์ของระบบ

แอกเตอร์ (Actor) ที่เกี่ยวข้องในระบบมี 4 แอกเตอร์ คือ

1. วิศวกร (Engineer) คือเจ้าหน้าที่ดูแลระบบเครือข่าย มีหน้าที่ดูแลระบบเครือข่าย แก้ปัญหาเมื่อมีปัญหาเกิดขึ้นกับระบบเครือข่ายตลอด 24 ชั่วโมง โดยมีการทำงานในลักษณะเข้ากะผลัดกันตลอดทั้งวัน
2. ผู้จัดการ (Manager) คือหัวหน้าทีมเจ้าหน้าที่ดูแลระบบเครือข่าย มีหน้าที่ควบคุมการทำงานของวิศวกรในทีม ตรวจสอบระบบเครือข่ายและดูผลรายงานด้านเครือข่าย
3. โหนด (Node) คือปลายทางที่ระบบจะทำการตรวจสอบสถานะโดยการส่งไอซีเอ็มพีแพ็กเก็ตตามหมายเลขไอพีแอดเดรสของโหนด และโหนดจะทำการตอบกลับมายังระบบ
4. ตัวจัดการเวลา (Timer) จะกำหนดระยะเวลาที่ระบบจะส่งไอซีเอ็มพี แพ็กเก็ตไปยังโหนดต่างๆ

3.4.2 รายละเอียดของยูสเคส

ยูสเคส ที่เกี่ยวข้องกับการทำงานของระบบมีดังนี้

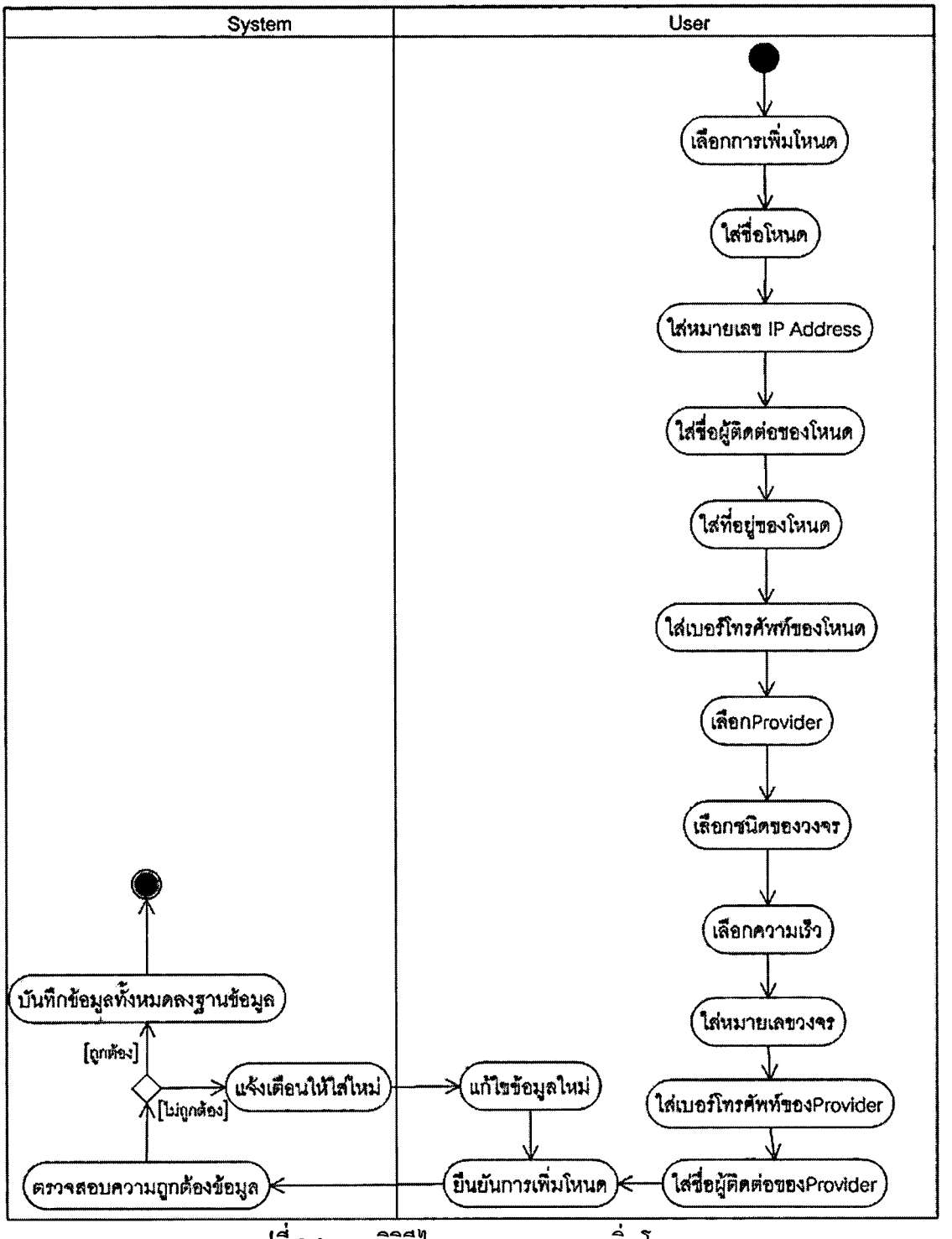
1. Add New Node คือ การเพิ่มข้อมูลโหนดใหม่เข้าสู่ระบบ
2. Edit Node คือ การแก้ไขข้อมูลรายละเอียดของโหนด ในกรณีที่มีการเปลี่ยนแปลงข้อมูล
3. Ping คือ การส่งไอซีเอ็มพีแพ็กเก็ตไปยังโหนดต่างๆ เพื่อตรวจสอบสถานะของแต่ละโหนด
4. Monitor Node คือ การตรวจสอบสถานะของโหนด และแสดงผลสถานะของโหนดผ่านเว็บแอพพลิเคชั่น
5. Record Problem Cause คือ การแจ้งการเกิดปัญหาของโหนด และให้เจ้าหน้าที่ดูแลระบบเครือข่ายระบุสาเหตุของปัญหา
6. Availability Report คือ การรายงานสรุปคุณภาพในการให้บริการเครือข่าย

ในแต่ละยูสเคสของระบบเฝ้าสังเกตเครือข่ายสารสนเทศ สามารถแสดงรายละเอียดของแต่ละยูสเคสได้ดังต่อไปนี้

ตารางที่ 3.1 รายละเอียดยูสเคส Add New Node

Use Case : Add New Node	
Brief Description :	การเพิ่มโหนดใหม่เข้ามาในระบบ
Actor :	Engineer
Precondition :	ต้องผ่านการล็อกอินเข้าสู่ระบบแล้ว
Basic Flow :	1) ใส่ชื่อโหนด 2) ใส่หมายเลขไอพีแอดเดรส 3) ใส่ชื่อผู้ติดต่อ 4) ใส่ที่อยู่ของโหนด 5) ใส่หมายเลขโทรศัพท์ 6) เลือกผู้ให้บริการ 7) เลือกชนิดวงจร 8) เลือกความเร็ว 9) ใส่หมายเลขวงจร 10) ใส่หมายเลขโทรศัพท์ของผู้ให้บริการ 11) ใส่ชื่อผู้ติดต่อของผู้ให้บริการ 12) ระบบตรวจสอบความถูกต้องและความครบถ้วนของข้อมูลที่ใส่ 13) ระบบบันทึกข้อมูลทั้งหมดลงฐานข้อมูล
Alternative Flows:	12a) ระบบจะแจ้งเตือน และให้ใส่ข้อมูลใหม่

เพื่อให้เกิดความเข้าใจและเห็นภาพขั้นตอนการทำงานของเหตุการณ์ที่ยูสเคสการเพิ่มโหนด ตามที่ได้อธิบายในรายละเอียดของยูสเคสชัดเจนยิ่งขึ้น จะอธิบายด้วยแอกทิวิตีไดอะแกรม ดังรูปที่ 3.3 ดังนี้

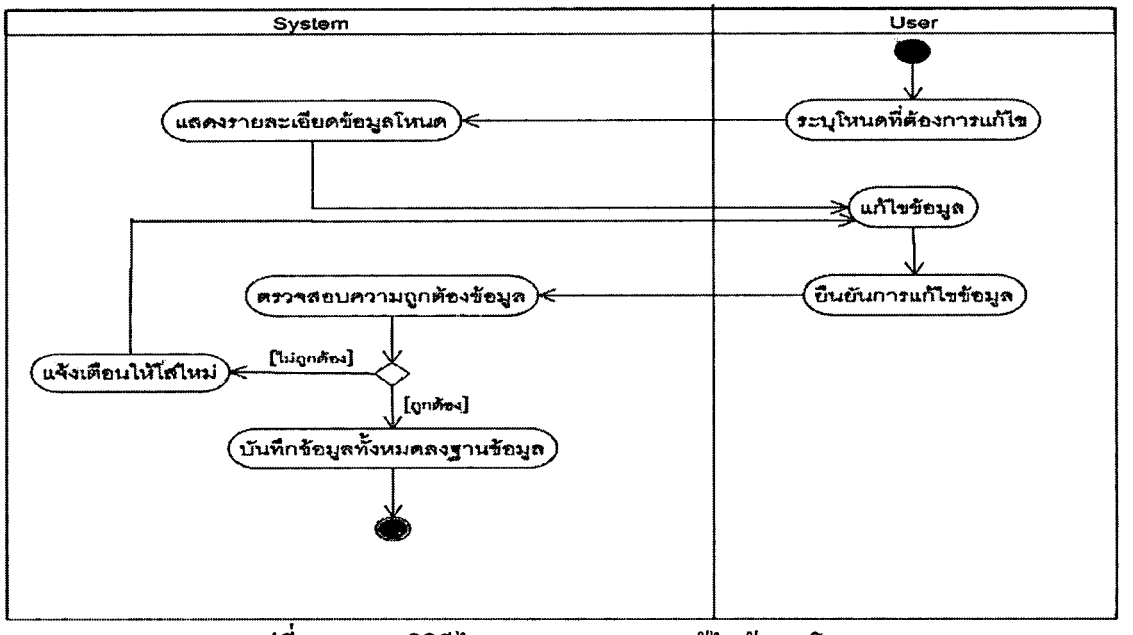


รูปที่ 3.3 แอกทิวิตีไดอะแกรมของการเพิ่มโหนด

ตารางที่ 3.2 รายละเอียดยูสเคส Edit Node

Use Case : Edit Node	
Brief Description :	เจ้าหน้าที่เข้าแก้ไขข้อมูลโหนด
Actor :	Engineer
Precondition :	ผ่านการล็อกอินเข้าสู่ระบบแล้ว
Basic Flow :	1) ระบุโหนดที่ต้องการแก้ไข 2) ระบบแสดงรายละเอียดข้อมูลของโหนด 3) แก้ไขข้อมูล 4) ระบบตรวจสอบความถูกต้องของข้อมูลที่ใส่ 5) ระบบบันทึกข้อมูลใหม่ลงฐานข้อมูล
Alternative Flows:	3a) ระบบแจ้งเตือน และให้ใส่ข้อมูลใหม่

เพื่อให้เกิดความเข้าใจและเห็นภาพขั้นตอนการทำงานของเหตุการณ์ที่ยูสเคสการการแก้ไขข้อมูลโหนด ตามที่ได้อธิบายในรายละเอียดของยูสเคสชัดเจนยิ่งขึ้น จะอธิบายด้วยแอกทิวิตีไดอะแกรมดังรูปที่ 3.4 ดังนี้

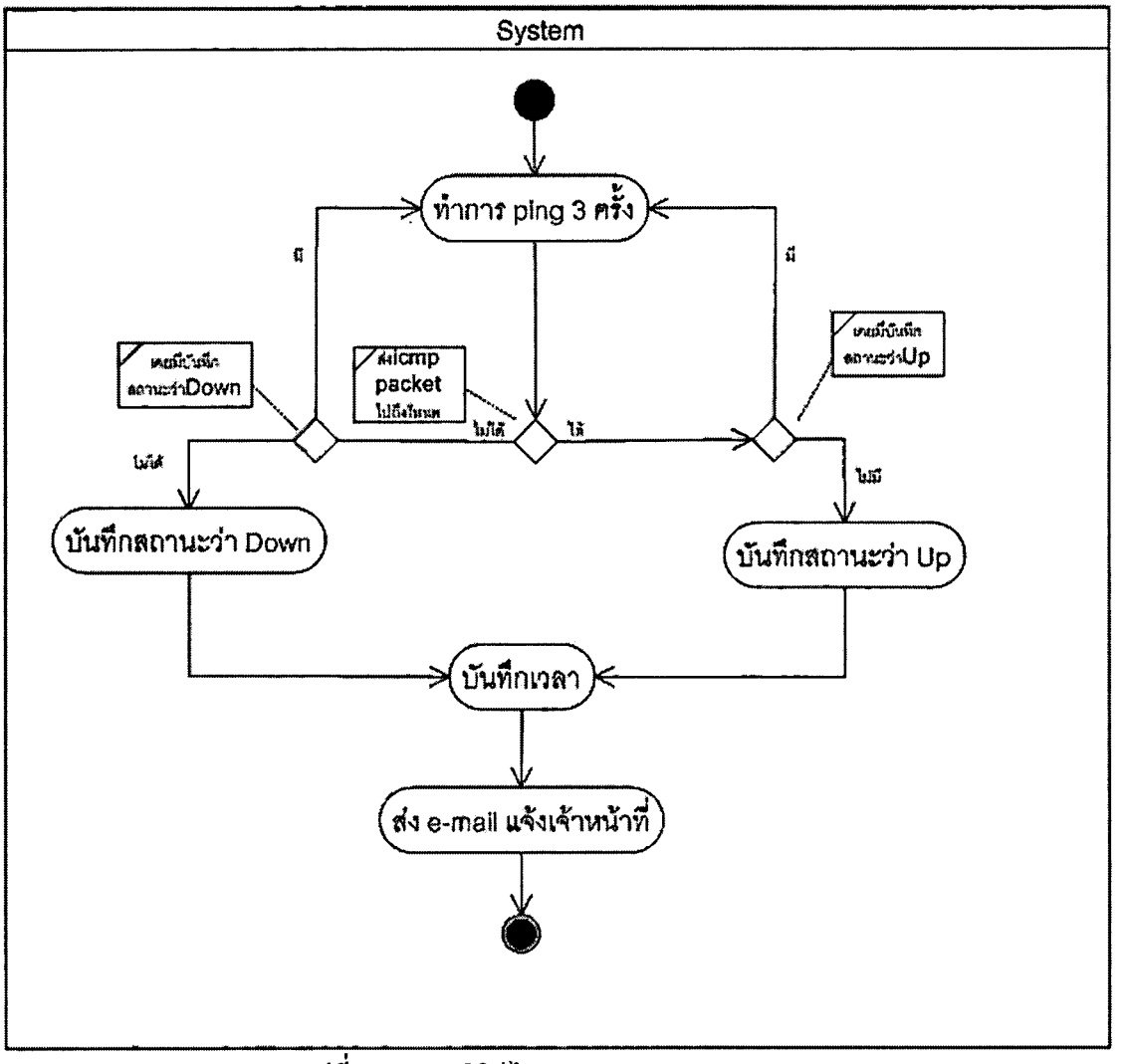


รูปที่ 3.4 แอกทิวิตีไดอะแกรมของการแก้ไขข้อมูลโหนด

ตารางที่ 3.3 รายละเอียดยูสเคส Ping

Use Case : Ping	
Brief Description :	ส่งไอซีเอ็มพี แพ็กเก็ตไปยังโหนดต่างๆเพื่อตรวจสอบสถานะ
Actor :	Timer
Precondition :	-
Basic Flows:	1) ระบบส่งไอซีเอ็มพีแพ็กเก็ตไปยังโหนดตามหมายเลขไอพีแอดเดรสที่ระบุ ในตารางข้อมูลโหนดเป็นจำนวน 3 ครั้ง 2) ถ้าไอซีเอ็มพีแพ็กเก็ตสามารถส่งถึงโหนด ระบบทำ S-1 3) ถ้าไอซีเอ็มพีแพ็กเก็ตไม่สามารถส่งถึงโหนด ระบบทำ S-2
Sub Flows :	S-1 : 1) ตรวจสอบสถานะของโหนดที่บันทึกไว้ล่าสุด 2) ถ้าบันทึกไว้ว่า Up แสดงว่าสถานะยังไม่มีการเปลี่ยนแปลง ระบบจะกลับไปขั้นตอนแรกคือการส่งไอซีเอ็มพีแพ็กเก็ตไปยังโหนด S-2 : 1) ตรวจสอบสถานะของโหนดที่บันทึกไว้ล่าสุด 2) ถ้าบันทึกไว้ว่า Down แสดงว่าสถานะยังไม่มีการเปลี่ยนแปลง ระบบจะกลับไปขั้นตอนแรกคือการส่งไอซีเอ็มพีแพ็กเก็ตไปยังโหนด
Alternative Flows:	S-1 : 2a) สถานะที่ถูกบันทึกไว้ล่าสุดเป็น Down แสดงว่าสถานะมีการเปลี่ยนแปลงจาก Down เป็น Up ระบบจะบันทึกการเปลี่ยนแปลง 2b) ส่งอีเมลแจ้งผู้ดูแลระบบเครือข่ายให้ทราบการเปลี่ยนแปลง S-2 : 2a) สถานะที่ถูกบันทึกไว้ล่าสุดเป็น Up แสดงว่าสถานะมีการเปลี่ยนแปลงจาก Up เป็น Down ระบบจะบันทึกการเปลี่ยนแปลง 2b) ส่งอีเมลแจ้งผู้ดูแลระบบเครือข่ายให้ทราบการเปลี่ยนแปลง

เพื่อให้เกิดความเข้าใจและเห็นภาพขั้นตอนการทำงานของเหตุการณ์ที่ยูสเคส Ping ตามที่ได้อธิบายในรายละเอียดของยูสเคสชัดเจนยิ่งขึ้น จะอธิบายด้วยแอกทิวิตีไดอะแกรมดังรูปที่ 3.5 ดังนี้

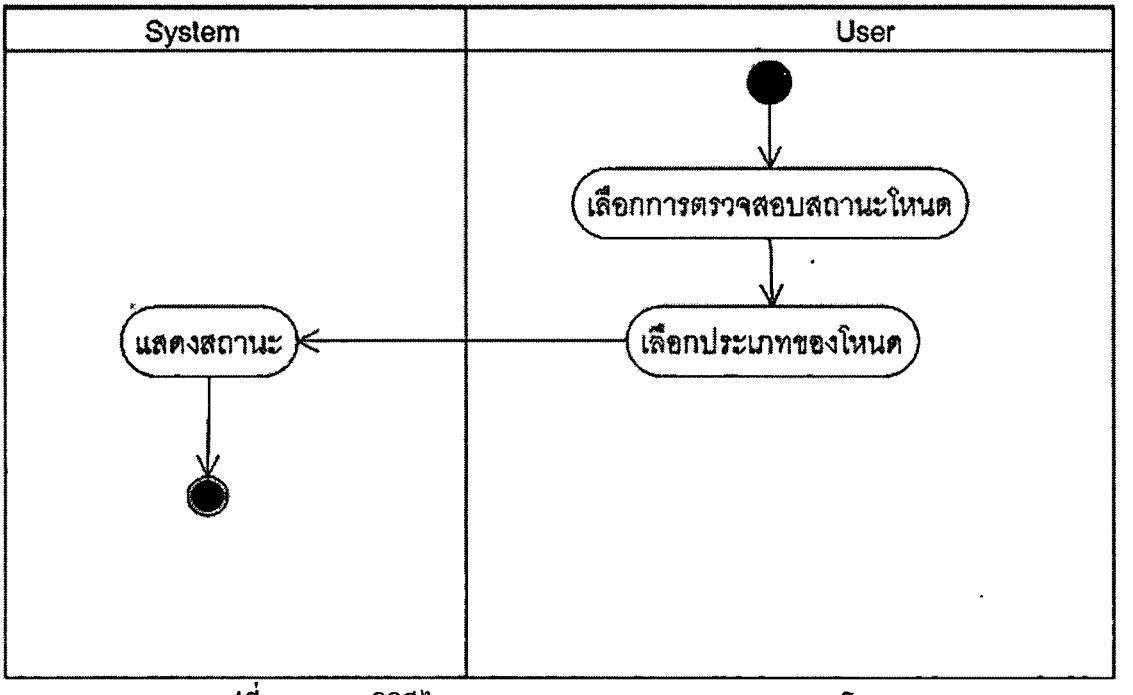


รูปที่ 3.5 แอกทิวิตีไดอะแกรมของยูสเคส Ping

ตารางที่ 3.4 รายละเอียดยูสเคส Monitor Node

Use Case : Monitor Node	
Brief Description :	แสดงผลสถานะของโหนดผ่านเว็บบราวเซอร์
Actor :	Engineer และ Manager
Precondition :	ผ่านการล็อกอินเข้าสู่ระบบแล้ว
Basic Flow :	1) ผู้ใช้งานเลือกการตรวจสอบสถานะโหนด 2) ผู้ใช้งานเลือกประเภทของโหนด 3) ผู้ใช้งานยืนยันการเลือกตรวจสอบ 4) ระบบแสดงสถานะของโหนดผ่านเว็บแอพพลิเคชั่น
Post Condition :	-

เพื่อให้เกิดความเข้าใจและเห็นภาพขั้นตอนการทำงานของเหตุการณ์ที่ยูสเคสการตรวจสอบสถานะโหนด ตามที่ได้อธิบายในรายละเอียดของยูสเคสชัดเจนยิ่งขึ้น จะอธิบายด้วยแอกทิวิตีไดอะแกรมดังรูปที่ 3.6 ดังนี้

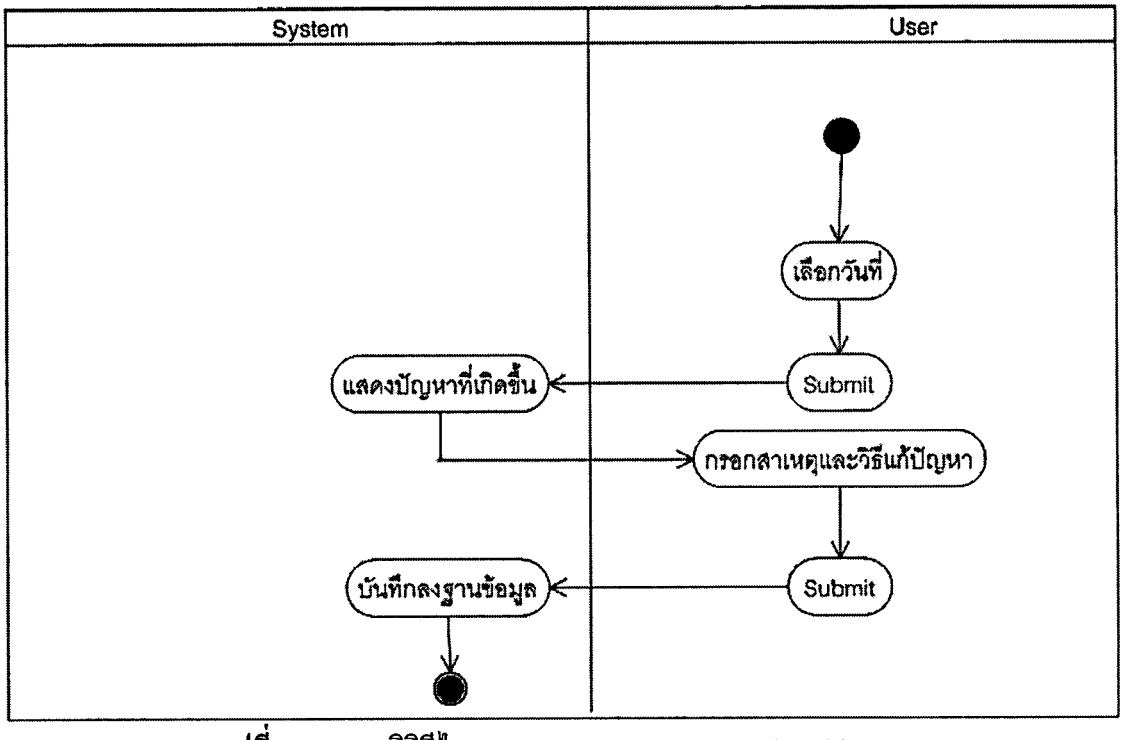


รูปที่ 3.6 แอกทิวิตีไดอะแกรมของการตรวจสอบสถานะโหนด

ตารางที่ 3.5 รายละเอียดยูสเคส Record Problem Cause

Use Case : Record Problem Cause	
Brief Description :	แจ้งการเกิดปัญหา เพื่อให้เจ้าหน้าที่บันทึกปัญหาและสาเหตุของปัญหา
Actor :	Engineer และ Manager
Precondition :	ผ่านการล็อกอินเข้าสู่ระบบแล้ว
Basic Flow :	1) ผู้ใช้งานเลือกวันที่ของปัญหาที่ต้องการระบุ 2) ระบบแสดงปัญหา 3) ผู้ใช้งานระบุปัญหา 4) ระบบจะบันทึกข้อมูลปัญหาลงฐานข้อมูล
Post Condition :	สาเหตุของปัญหาจะถูกบันทึกลงฐานข้อมูล

เพื่อให้เกิดความเข้าใจและเห็นภาพขั้นตอนการทำงานของเหตุการณ์ที่ยูสเคส Record Problem Cause ตามที่ได้อธิบายในรายละเอียดของยูสเคสชัดเจนยิ่งขึ้น จะอธิบายด้วยแอกทิวิตีไดอะแกรมดังรูปที่ 3.7 ดังนี้

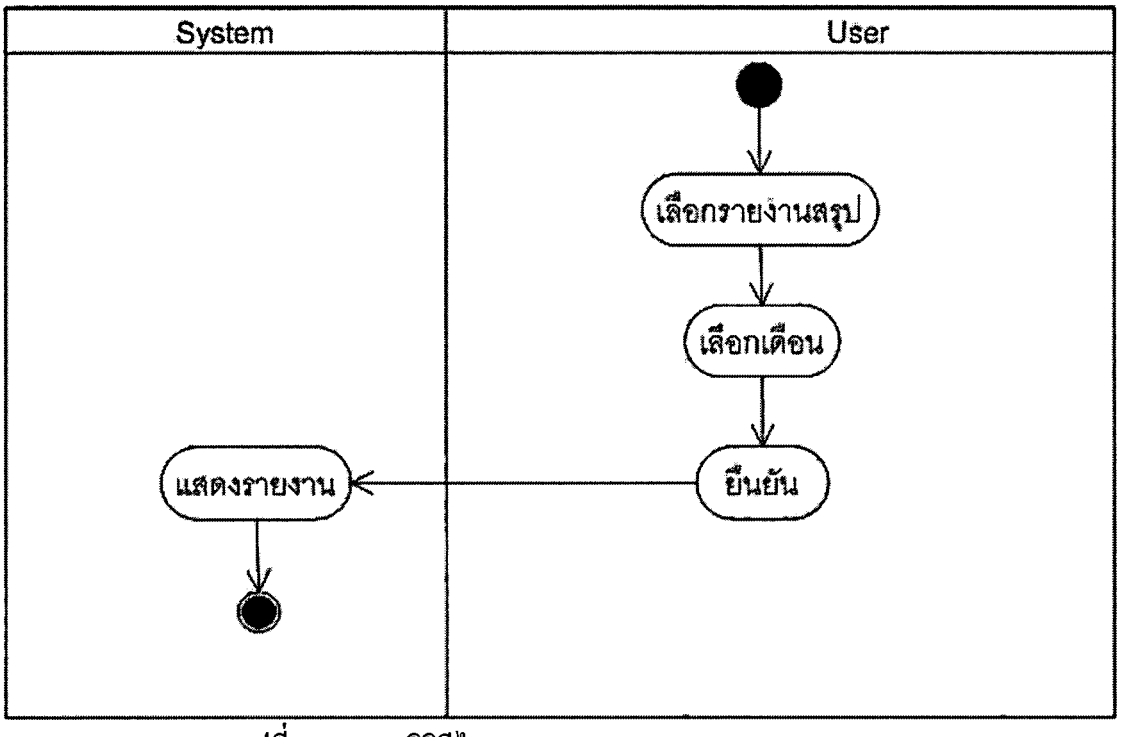


รูปที่ 3.7 แอกทิวิตีไดอะแกรมของยูสเคส Record Problem Cause

ตารางที่ 3.6 รายละเอียดยูสเคส Availability Report

Use Case : Availability Report	
Brief Description :	รายงานสรุปคุณภาพในการให้บริการในแต่ละโหนดเป็นรายเดือน
Actor :	Manager
Precondition :	-
Basic Flow :	1) ผู้ใช้งานเลือกเดือนที่ต้องการรายงานสรุป 2) ระบบแสดงรายงาน
Post Condition :	-

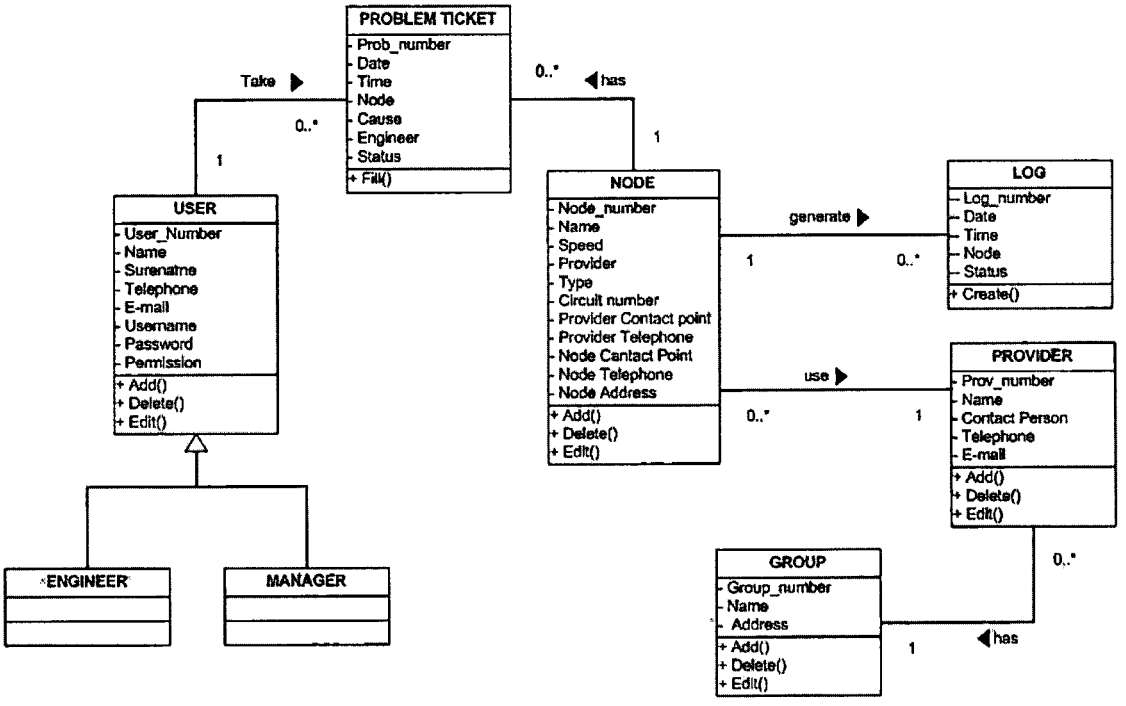
เพื่อให้เกิดความเข้าใจและเห็นภาพขั้นตอนการทำงานของเหตุการณ์ที่ยูสเคส Availability Report ตามที่ได้อธิบายในรายละเอียดของยูสเคสชัดเจนยิ่งขึ้น จะอธิบายด้วยแอกทิวิตีไดอะแกรมดังรูปที่ 3.8 ดังนี้



รูปที่ 3.8 แอกทิวิตีไดอะแกรมของยูสเคส Availability Report

3.5 แบบจำลองข้อมูลของระบบ

จากยูสเคสไดอะแกรมของระบบสามารถสร้างการจำลองแบบเชิงโครงสร้างเพื่อให้มองเห็นโครงสร้างระบบใหม่ โดยแสดงเป็นคลาสไดอะแกรมดังรูปที่ 3.9 ดังนี้



รูปที่ 3.9 คลาสไดอะแกรมของระบบเฝ้าสังเกตเครือข่ายสารสนเทศ

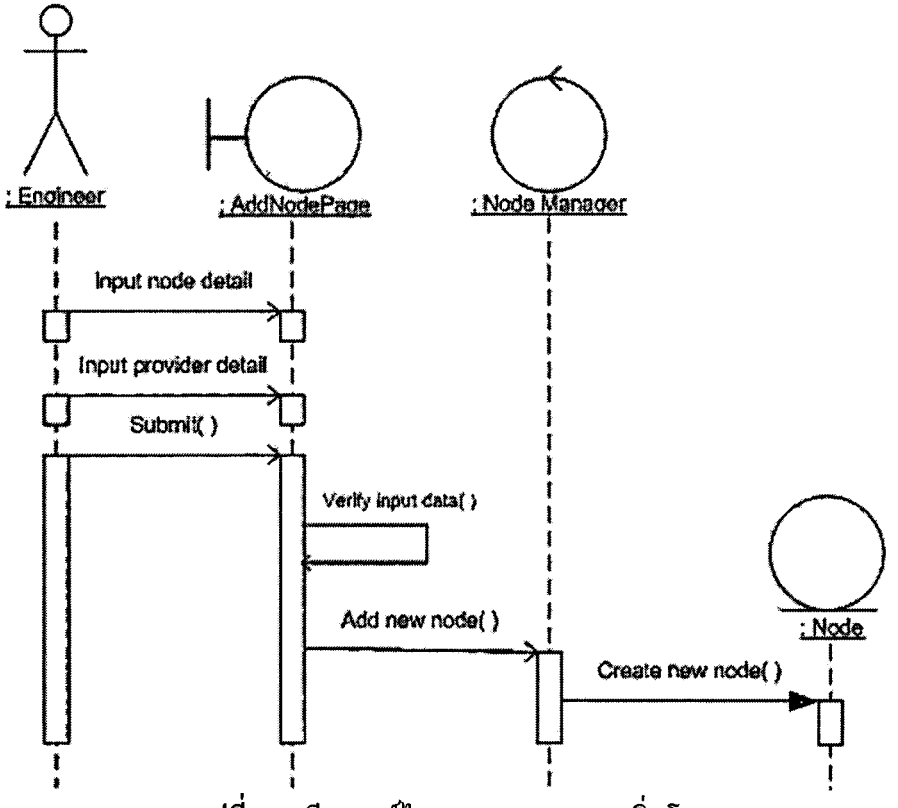
จากคลาสไดอะแกรมแสดงให้เห็นความสัมพันธ์ของคลาสต่างๆ ในระบบ โดยแต่ละคลาสมีความหมายดังนี้

1. คลาส User เป็นคลาสผู้ใช้งาน
2. คลาส Engineer เป็นคลาสกลุ่มผู้ใช้งานที่เป็นวิศวกรผู้ดูแลระบบเครือข่าย
3. คลาส Manager เป็นคลาสผู้ใช้งานที่เป็นผู้จัดการด้านเครือข่าย
4. คลาส Problem Ticket เป็นคลาสปัญหาที่เกิดขึ้นและสาเหตุของปัญหา
5. คลาส Node เป็นคลาสเก็บข้อมูลโหนด
6. คลาส Log เป็นคลาสของเหตุการณ์การเปลี่ยนแปลงที่เกิดขึ้นกับโหนด
7. คลาส Provider เป็นคลาสของผู้ให้บริการสายสัญญาณในการเชื่อมต่อโหนด
8. คลาส Group เป็นคลาสกลุ่มของผู้ให้บริการสายสัญญาณในการเชื่อมต่อโหนด

บทที่ 4
การออกแบบระบบเฝ้าสังเกตเครือข่ายสารสนเทศ

4.1 การออกแบบการทำงานของระบบ

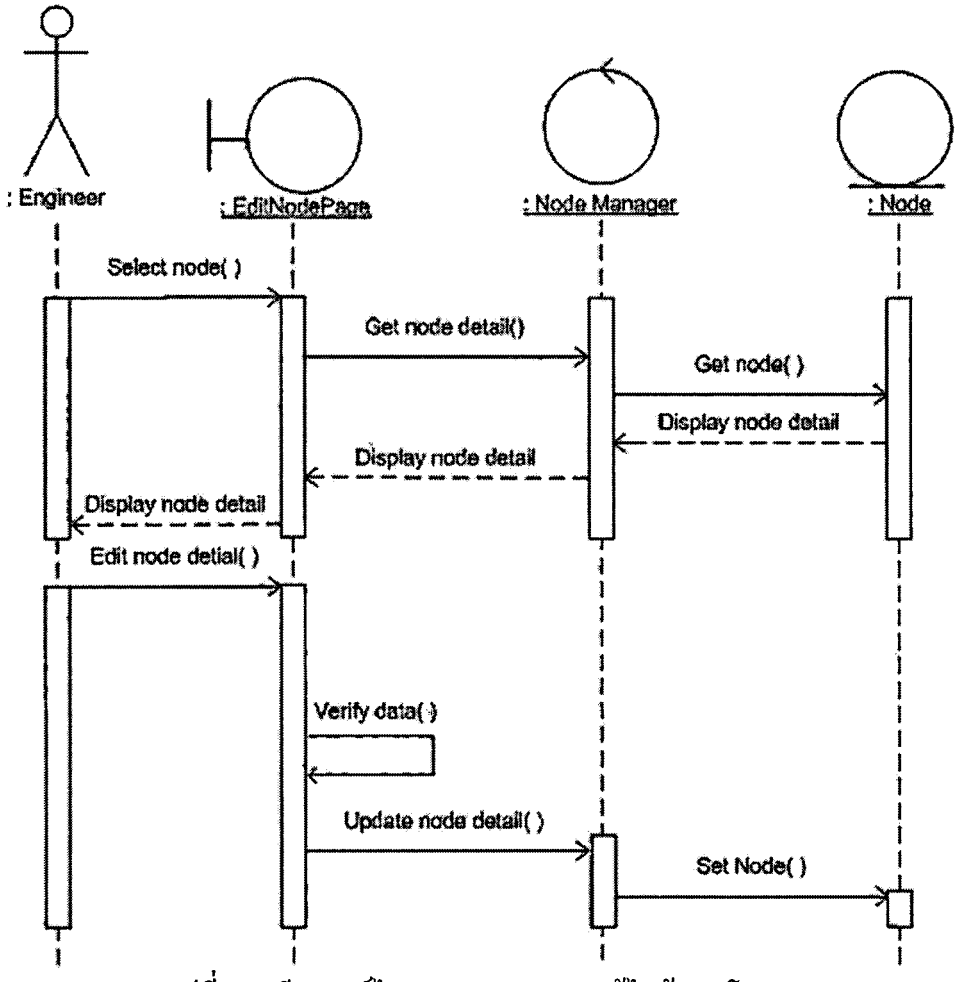
จากยูสเคสไดอะแกรมและคลาสไดอะแกรมที่ได้สร้างขึ้น นำมาออกแบบการทำงานเพื่อดูว่าแต่ละยูสเคสมีคลาสหรืออ็อบเจกต์ที่มีความสัมพันธ์กันในเชิงกิจกรรมอย่างไร ตามลำดับเวลาของกิจกรรมที่เกิดขึ้น และเพื่อกำหนดส่วนประกอบอื่นๆ ที่จำเป็นสำหรับระบบ โดยแสดงด้วยตัวอย่างซีเควนซ์ไดอะแกรมดังรูปที่ 4.1 - 4.6 ดังนี้



รูปที่ 4.1 ซีเควนซ์ไดอะแกรมของการเพิ่มโหนด

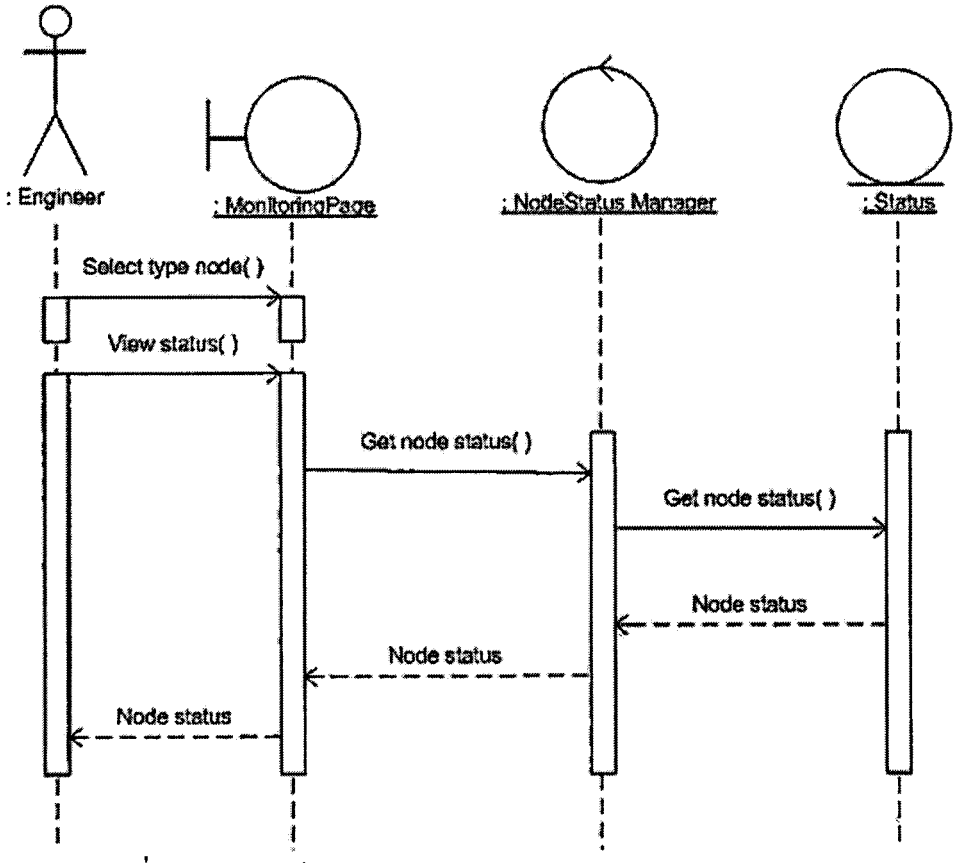
จากรูปที่ 4.1 แสดงให้เห็นถึงกิจกรรมการเพิ่มโหนดในระบบเพื่อให้ระบบตรวจสอบสถานะของโหนดต่อไป โดยรูปแสดงกรณีที่วิศวกรเพิ่มโดยใส่ข้อมูลต่างๆของโหนด และรายละเอียดของผู้ให้บริการสายสัญญาณ โดยระบบจะตรวจสอบความครบถ้วนและความถูกต้อง

ของรายละเอียดที่วิศวกรป้อน แล้วจึงเพิ่มข้อมูลโหนดในฐานข้อมูลเป็นการสิ้นสุดกิจกรรมการเพิ่มโหนด



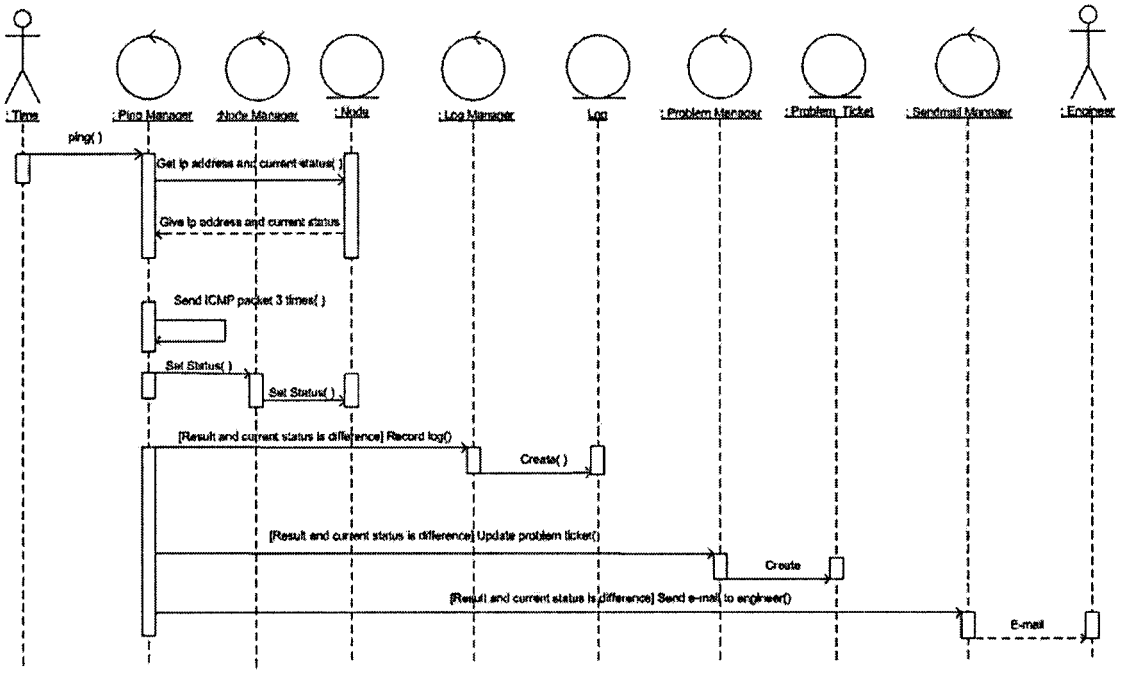
รูปที่ 4.2 ซีเควนซ์ไดอะแกรมของการแก้ไขข้อมูลโหนด

จากรูปที่ 4.2 แสดงให้เห็นถึงกิจกรรมการแก้ไขข้อมูลโหนด เป็นตัวอย่างในกรณีที่ผู้ใช้ระบบคือวิศวกรแก้ไขข้อมูลโหนด โดยเลือกโหนดที่ต้องการแก้ไขข้อมูลแล้วระบบจะติดต่อกับฐานข้อมูลเพื่อแสดงรายละเอียดเดิมของโหนดนั้นๆ แล้วจึงแก้ไขข้อมูลโหนดโดยระบบจะตรวจสอบความถูกต้องและครบถ้วนของข้อมูลแล้วจึงแก้ไขข้อมูลในฐานข้อมูล เป็นการสิ้นสุดกิจกรรมการแก้ไขข้อมูลโหนด



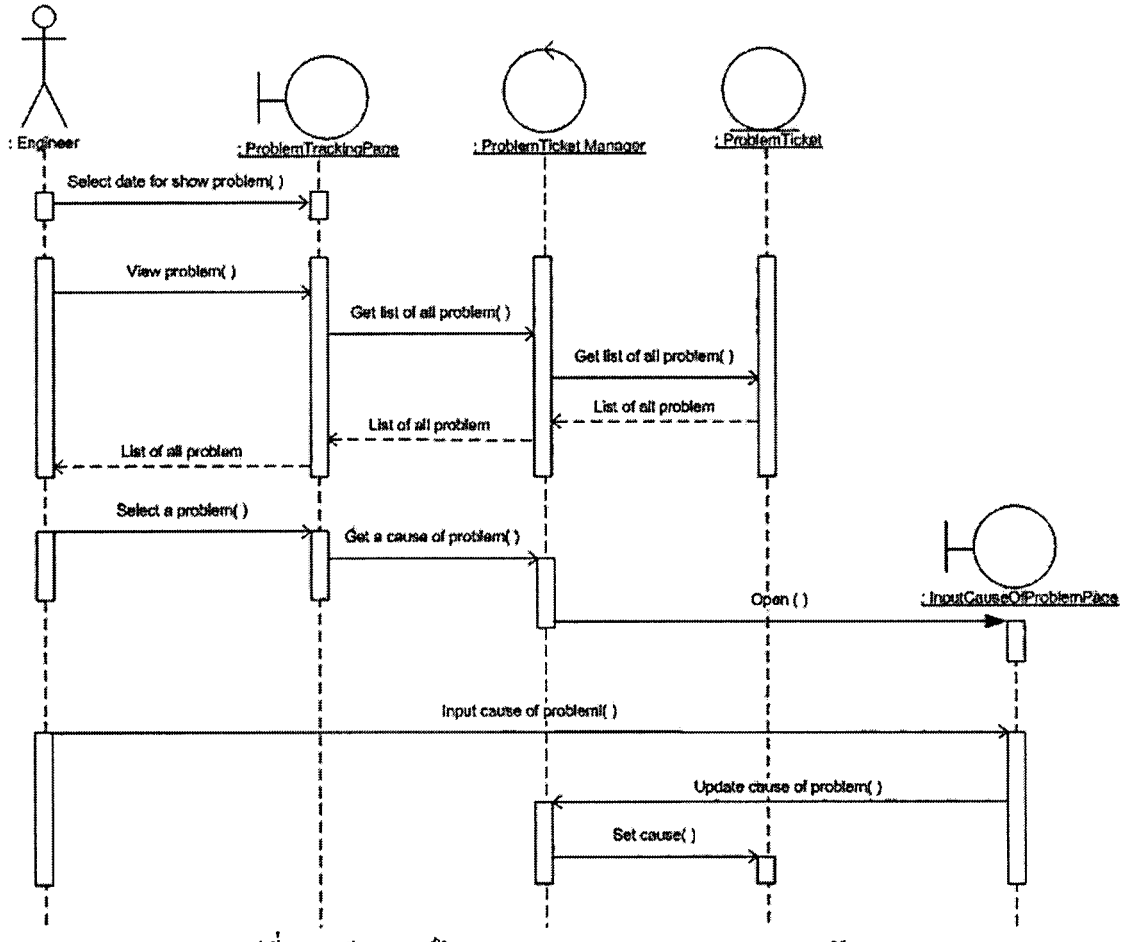
รูปที่ 4.3 ซีเควนซ์ไดอะแกรมของการดูสถานะการทำงานของโหนด

จากรูปที่ 4.3 แสดงให้เห็นถึงกิจกรรมการดูสถานะการทำงานของโหนด เป็นตัวอย่างในกรณีที่ผู้ใช้ระบบคือวิศวกรดูสถานะการทำงานโหนด โดยเลือกลักษณะโหนดที่ต้องการต้องการตรวจสอบสถานะ แล้วระบบจะติดต่อกับฐานข้อมูลเพื่อแสดงสถานะของโหนดนั้นให้กับผู้ใช้งานทราบผ่านเว็บแอพพลิเคชั่น เป็นการสิ้นสุดกิจกรรมการดูสถานะการทำงานของโหนด



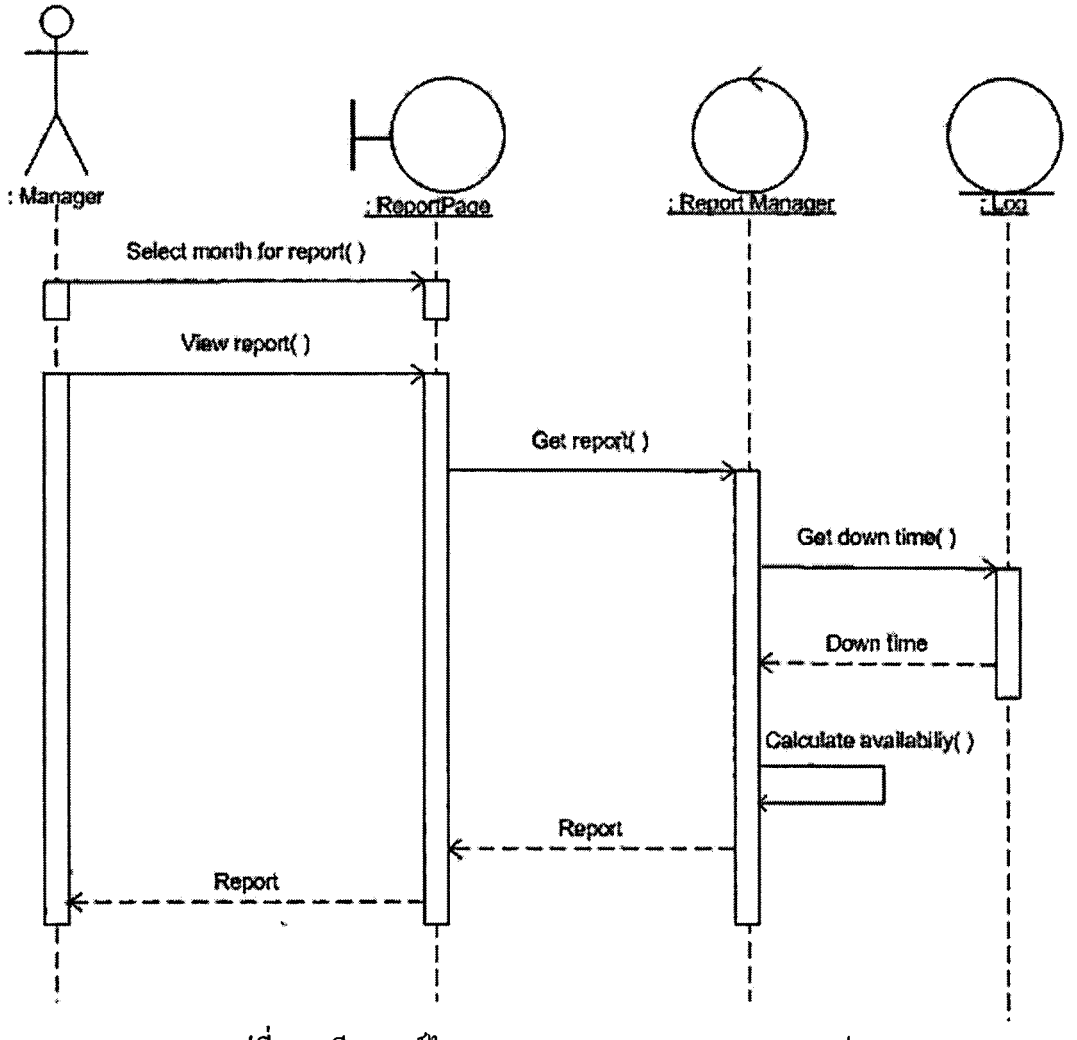
รูปที่ 4.4 ซีเควนซ์ไดอะแกรมของการส่งไอซีเอ็มพีแพ็กเก็ตเพื่อตรวจสอบสถานะของโหนด

จากรูปที่ 4.4 แสดงให้เห็นถึงกิจกรรมการส่งไอซีเอ็มพีแพ็กเก็ตเพื่อตรวจสอบสถานะของปลายทาง (โหนด) โดยเมื่อถึงเวลาที่กำหนดระบบจะขอข้อมูลไอพีแอดเดรสและสถานะปัจจุบันของโหนดจากฐานข้อมูลโหนดแล้ว จะส่งไอซีเอ็มพีแพ็กเก็ตไปยังโหนดตามหมายเลขไอพีแอดเดรสจำนวน 3 ครั้ง เมื่อได้ผลลัพธ์ของสถานะโหนดจะบันทึกสถานะลงฐานข้อมูลโหนด หากผลลัพธ์ของสถานะหลังจากการตรวจสอบมีความแตกต่างกับสถานะที่บันทึกไว้ในปัจจุบัน ระบบจะบันทึกการเปลี่ยนแปลงลงฐานข้อมูล LOG และฐานข้อมูล PROBLEM_TICKET แล้วส่งอีเมลแจ้งให้กับผู้ดูแลระบบทราบ เป็นการสิ้นสุดกิจกรรมการส่งไอซีเอ็มพีแพ็กเก็ตเพื่อตรวจสอบสถานะของโหนด



รูปที่ 4.5 ซีเควนซ์ไดอะแกรมของการระบุสาเหตุของปัญหา

จากรูปที่ 4.5 แสดงให้เห็นถึงกิจกรรมการระบุสาเหตุของปัญหา เป็นตัวอย่างในกรณีที่ผู้ใช้ระบบคือวิศวกรระบุสาเหตุของปัญหาที่เกิดขึ้น โดยเลือกวันที่ที่ต้องการแสดงปัญหา ระบบจะติดต่อกับฐานข้อมูลเพื่อแสดงปัญหาที่เกิดขึ้นทั้งหมดในวันนั้นๆ วิศวกรเลือกปัญหาที่ต้องการระบุสาเหตุระบบจะติดต่อฐานข้อมูลเพื่อแสดงรายละเอียดปัญหาที่อาจมีการบันทึกไว้แล้ว วิศวกรระบุสาเหตุของปัญหาระบบจะติดต่อกับฐานข้อมูลเพื่อบันทึกสาเหตุของปัญหา เป็นการสิ้นสุดกิจกรรมการระบุสาเหตุของปัญหา



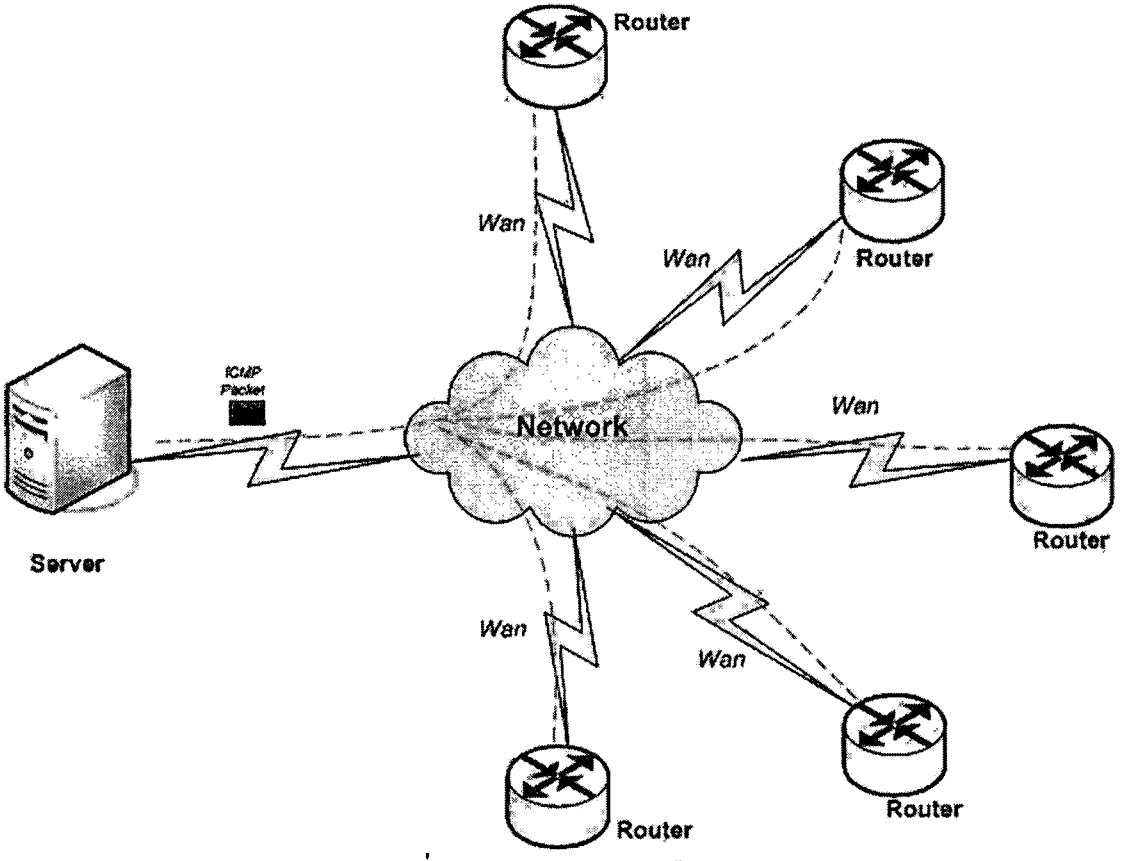
รูปที่ 4.6 ซีเควนซ์ไดอะแกรมของการแสดงรายงานสรุป

จากรูปที่ 4.6 แสดงให้เห็นถึงกิจกรรมการแสดงรายงานสรุป เป็นตัวอย่างในกรณีที่ผู้ใช้ระบบคือผู้จัดการ ต้องการดูรายงานสรุปคุณภาพในการให้บริการของโหนดในแต่ละเดือน โดยเลือกเดือนที่ต้องการดูรายงาน ระบบจะติดต่อกับฐานข้อมูลเพื่อคำนวณเวลาทั้งหมดที่แต่ละโหนดเกิดปัญหาขึ้น แล้วทำรายงานสรุปเป็นเปอร์เซ็นต์คุณภาพในการให้บริการของแต่ละโหนดให้ผู้ใช้งานทราบผ่านเว็บแอพพลิเคชั่น เป็นการสิ้นสุดกิจกรรมการแสดงรายงานสรุป

4.2 การออกแบบสถาปัตยกรรมของระบบ

การออกแบบสถาปัตยกรรมของระบบสำหรับการตรวจสอบเครือข่ายแสดงดังรูปที่ 4.7 โดยมีเซิร์ฟเวอร์กลางที่ติดตั้งระบบเฝ้าสังเกตเครือข่ายสารสนเทศ ทำหน้าที่ส่งไอซีเอ็มพีแพ็กเก็ตโดยใช้คำสั่ง ping ในระบบปฏิบัติการลีนุกส์ไปยังหมายเลขไอพีแอดเดรสของปลายทางหรือโหนด

เพื่อตรวจสอบสถานะการทำงานเพื่อแสดงผลและทำรายงานต่างๆให้ผู้ใช้งานระบบทราบ โดยมีระบบบริหารจัดการฐานข้อมูล MySQL เป็นตัวจัดการระบบฐานข้อมูล



รูปที่ 4.7 การออกแบบเครือข่าย

ข้อกำหนดคุณลักษณะฮาร์ดแวร์ของเครื่องเซิร์ฟเวอร์ ซึ่งทำหน้าที่ส่งไอซีเอ็มพีแพ็กเก็ตไปยังปลายทางเพื่อตรวจสอบสถานะการทำงานแล้วนำผลการตรวจสอบมานำเสนอในรูปแบบเว็บแอ็พพลิเคชั่น มีรายละเอียดส่วนประกอบต่างๆ ของระบบดังตารางที่ 4.1

ตารางที่ 4.1 คุณสมบัติของเครื่องเซิร์ฟเวอร์

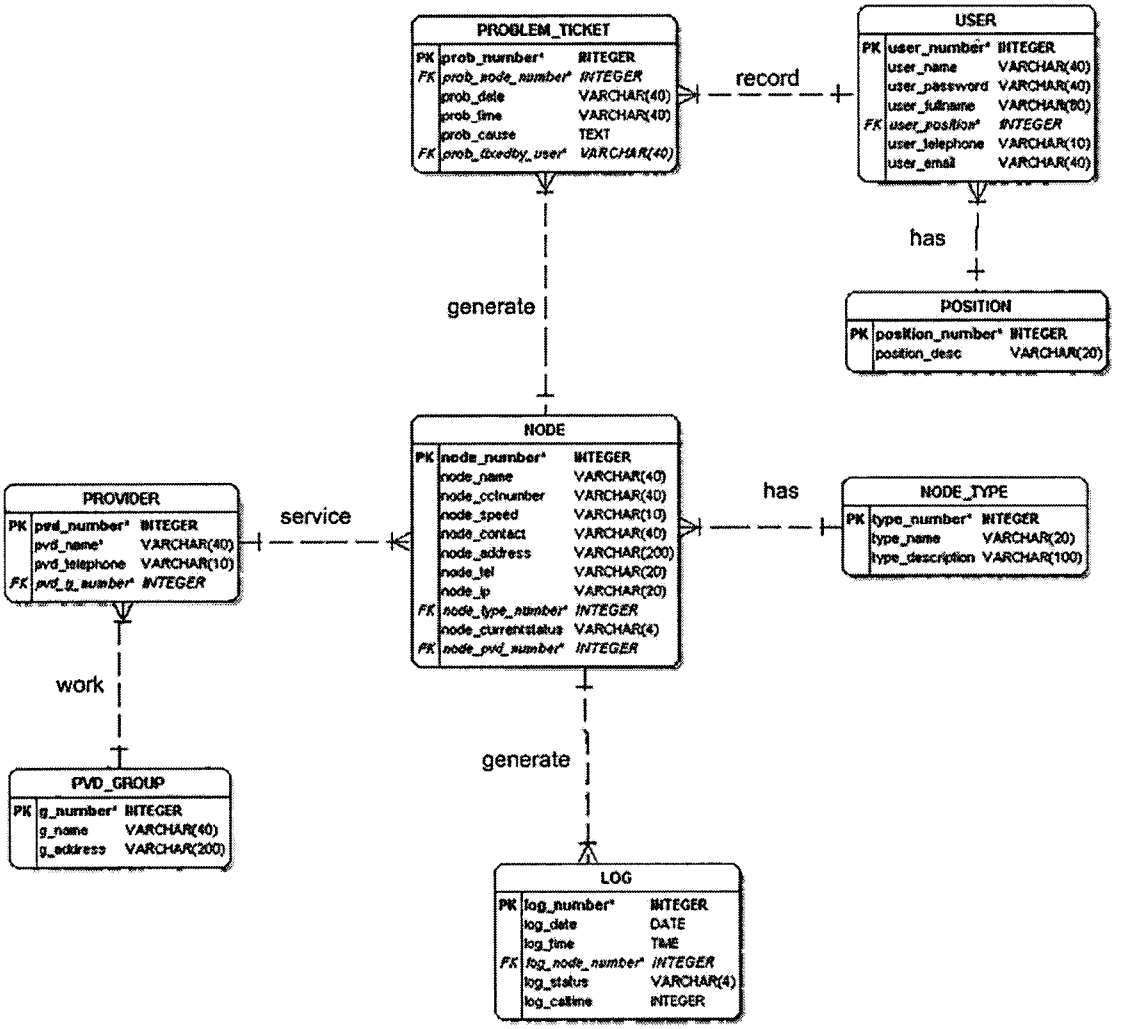
หน่วยประมวลผลกลาง	Intel Pentium 4
ฟรอนต์ไซส์บัส	800 MHz
ความเร็วคล็อก	3.2 GHz
หน่วยความจำแคช	2MB L2 cache
หน่วยความจำหลัก	1 GB
จอภาพ	LCD 17 นิ้ว
ฮาร์ดดิสก์	80 GB (7,200 rpm)
ซีดีรอม	ความเร็ว 52 X
ฟล็อปปี้ดิสก์	ความจุ 1.44 MB
แป้นพิมพ์	USB Keyboard
เมาส์	USB Mouse
ช่องเชื่อมอุปกรณ์	1 Parallel Port, 2 Serial, 1 VGA Adapter, 4 USB 2.0 ports
เน็ตเวิร์กอินเทอร์เฟซการ์ด	10/100/1000 LAN
ระบบปฏิบัติการ	ลินุกส์ Fedora
ดาต้าเบส	MySQL
โปรแกรม	Apache, SendMail

บทที่ 5

การออกแบบฐานข้อมูล

จากการวิเคราะห์ระบบเฝ้าสังเกตเครือข่ายสารสนเทศทำให้สามารถออกแบบฐานข้อมูลที่เป็นฐานข้อมูลเชิงสัมพันธ์ แสดงโดยแผนภาพความสัมพันธ์ระหว่างเอนทิตีแบบ Crow's Foot Model ซึ่งประกอบด้วยตารางสำหรับจัดเก็บข้อมูลต่าง ๆ ดังนี้

1. NODE ใช้สำหรับเก็บข้อมูลโหนดปลายทางที่ต้องการให้ระบบตรวจสอบสถานะการทำงาน และให้ผู้ดูแลระบบเครือข่ายคอยตรวจสอบการทำงาน
2. NODE_TYPE ใช้สำหรับเก็บข้อมูลชนิดของโหนด เช่น โหนดเป็นลักษณะวงจรเช่าหรือ เฟรมรีเลย์ เป็นต้น
3. LOG ใช้สำหรับเก็บข้อมูลการเปลี่ยนแปลงสถานะของทั้งหมดที่เกิดขึ้นกับโหนด
4. PROBLEM_TICKET ใช้สำหรับเก็บข้อมูลปัญหาที่เกิดขึ้นกับโหนดและสาเหตุของปัญหานั้น โดยมีผู้ดูแลระบบเป็นผู้บันทึกสาเหตุของปัญหานั้นๆ
5. USER ใช้สำหรับเก็บข้อมูลผู้ใช้งานระบบ
6. POSITION ใช้สำหรับเก็บข้อมูลตำแหน่งงานของผู้ใช้งานระบบ
7. PROVIDER ใช้สำหรับเก็บข้อมูลบุคคลผู้ให้บริการสายสัญญาณของโหนดนั้นๆ
8. GROUP ใช้สำหรับเก็บข้อมูลองค์กรของผู้ให้บริการสายสัญญาณของโหนด



รูปที่ 5.1 แผนภาพความสัมพันธ์ระหว่างเอนทิตี

รายละเอียดของตารางต่างๆ สามารถแสดงได้ด้วยพจนานุกรมข้อมูล ดังตารางที่ 5.1 – 5.8 ดังนี้

ตารางที่ 5.1 พจนานุกรมข้อมูลของตาราง NODE

ชื่อแอตทริบิวต์	ชนิดข้อมูล	คำอธิบาย	คีย์	ตารางอ้างอิง
node_number	INTEGER	หมายเลขโหนด	PK	
node_name	VARCHAR(40)	ชื่อโหนด		
node_cctnumber	VARCHAR(40)	เลขวงจรของโหนด		
node_speed	VARCHAR(10)	ความเร็วของโหนด		

ตารางที่ 5.1 พจนานุกรมข้อมูลของตาราง NODE (ต่อ)

ชื่อแอตทริบิวต์	ชนิดข้อมูล	คำอธิบาย	คีย์	ตารางอ้างอิง
node_contact	VARCHAR(40)	ผู้ติดต่อของโหนด		
node_address	VARCHAR(200)	ที่อยู่ของโหนด		
node_ip	VARCHAR(20)	หมายเลขไอพีแอดเดรส		
node_type_number	INTEGER	ชนิดของวงจร	FK	NODE_TYPE
node_currentstatus	VARCHAR(4)	สถานะโหนด		
node_pvd_number	INTEGER	หมายเลขผู้ให้บริการ	FK	PROVIDER

ตารางที่ 5.2 พจนานุกรมข้อมูลของตาราง NODE_TYPE

ชื่อแอตทริบิวต์	ชนิดข้อมูล	คำอธิบาย	คีย์	ตารางอ้างอิง
type_number	INTEGER	หมายเลขชนิดวงจร	PK	
type_name	VARCHAR(20)	ชื่อชนิดวงจร		
type_description	VARCHAR(100)	รายละเอียดของวงจร		

ตารางที่ 5.3 พจนานุกรมข้อมูลของตาราง LOG

ชื่อแอตทริบิวต์	ชนิดข้อมูล	คำอธิบาย	คีย์	ตารางอ้างอิง
log_number	INTEGER	หมายเลขของการเปลี่ยนแปลง	PK	
log_date	DATE	วันที่ของการเปลี่ยนแปลง		
log_time	TIME	เวลาของการเปลี่ยนแปลง		
log_node_number	INTEGER	หมายเลขโหนดที่เกิดเปลี่ยนแปลง	FK	NODE
log_status	VARCHAR(4)	สถานะของการเปลี่ยนแปลง		
log_caltime	INTEGER	เวลาที่ใช้สำหรับการคำนวณ		

ตารางที่ 5.4 พจนานุกรมข้อมูลของตาราง PROBLEM_TICKET

ชื่อแอตทริบิวต์	ชนิดข้อมูล	คำอธิบาย	คีย์	ตารางอ้างอิง
prob_number	INTEGER	หมายเลขปัญหา	PK	
prob_node_number	INTEGER	โหนดที่เกิดปัญหา	FK	NODE
prob_date	Date	วันที่เกิดปัญหา		
prob_time	VARCHAR(40)	เวลาที่เกิดปัญหา		
prob_cause	TEXT	สาเหตุของปัญหา		
prob_fixedby_user	VARCHAR(40)	ผู้ที่ระบุปัญหา	FK	USER

ตารางที่ 5.5 พจนานุกรมข้อมูลของตาราง USER

ชื่อแอตทริบิวต์	ชนิดข้อมูล	คำอธิบาย	คีย์	ตารางอ้างอิง
user_number	INTEGER	หมายเลขผู้ใช้งาน	PK	
user_name	VARCHAR(40)	ชื่อผู้ใช้งาน		
user_password	VARCHAR(40)	รหัสผ่าน		
user_position	INTEGER	ตำแหน่งของผู้ใช้งาน	FK	POSITION
user_telephone	VARCHAR(10)	หมายเลขโทรศัพท์		
user_email	VARCHAR(40)	อีเมลของผู้ใช้งาน		

ตารางที่ 5.6 พจนานุกรมข้อมูลของตาราง POSITION

ชื่อแอตทริบิวต์	ชนิดข้อมูล	คำอธิบาย	คีย์	ตารางอ้างอิง
position_number	INTEGER	หมายเลขตำแหน่งงาน	PK	
position_desc	VARCHAR(20)	ตำแหน่งงาน		

ตารางที่ 5.7 พจนานุกรมข้อมูลของตาราง PROVIDER

ชื่อแอตทริบิวต์	ชนิดข้อมูล	คำอธิบาย	คีย์	ตารางอ้างอิง
pvd_number	INTEGER	หมายเลขผู้ให้บริการสายสัญญาณโหนด	PK	
pvd_name	VARCHAR(40)	ชื่อบุคคลที่ดูแลโหนดนั้นๆ		
pvd_telephone	VARCHAR(10)	หมายเลขโทรศัพท์สำหรับติดต่อ		
pvd_g_number	INTEGER	องค์กรของผู้ให้บริการ	FK	GROUP

ตารางที่ 5.8 พจนานุกรมข้อมูลของตาราง GROUP

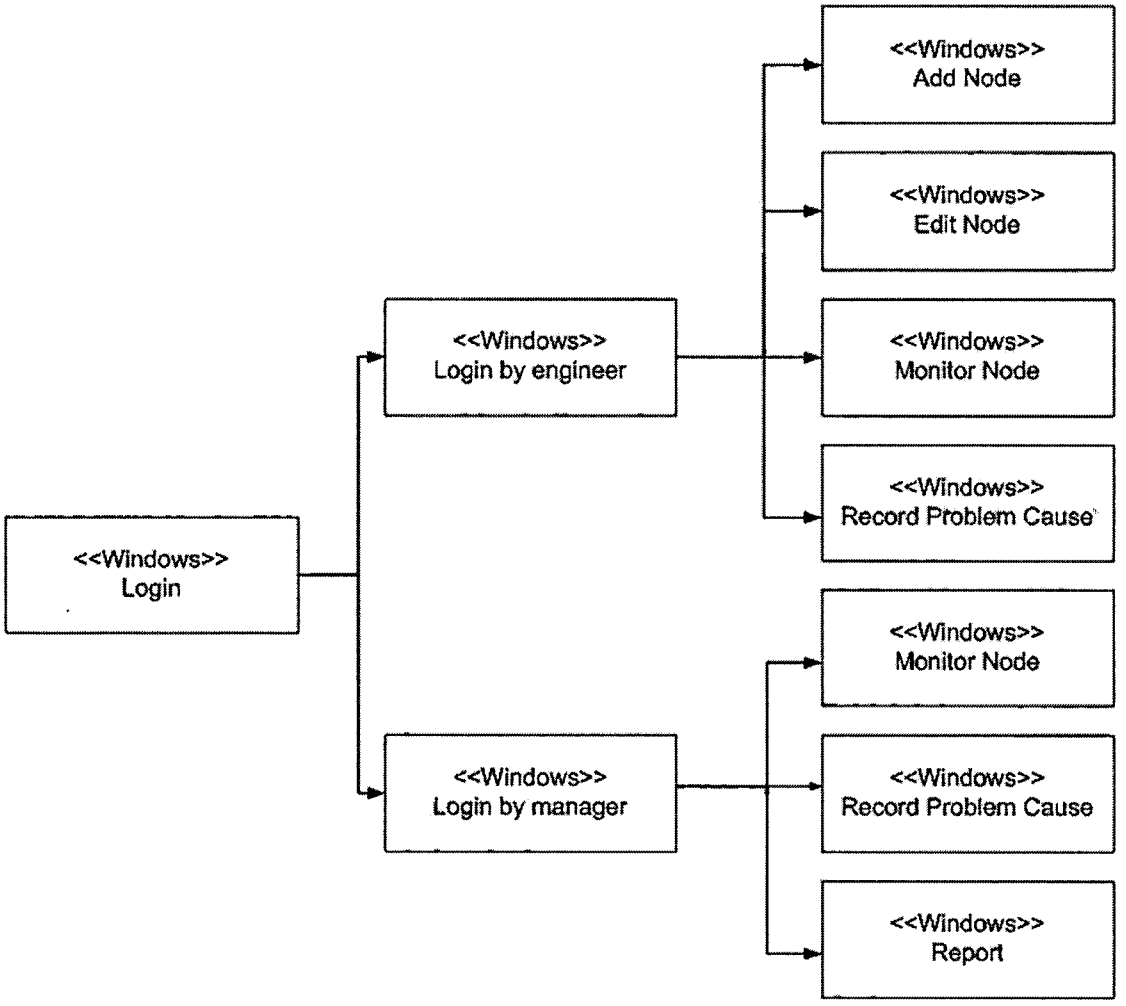
ชื่อแอตทริบิวต์	ชนิดข้อมูล	คำอธิบาย	คีย์	ตารางอ้างอิง
g_number	INTEGER	หมายเลของค์กรผู้ให้บริการสายสัญญาณ	PK	
g_name	VARCHAR(40)	ชื่อขององค์กร		
g_address	VARCHAR(200)	ที่อยู่ขององค์กร		

บทที่ 6
การพัฒนาระบบ

6.1 โครงสร้างเว็บหลักของระบบ

ระบบเฝ้าสังเกตเครือข่ายสารสนเทศ ได้รับการพัฒนาให้มีการทำงานเป็น 6 ส่วน ดังนี้

1. การเข้าสู่ระบบ
2. การตรวจสอบสถานะของโหนด
3. การรายงานปัญหาและระบุปัญหาที่เกิดขึ้น
4. การเพิ่มโหนด
5. การเปลี่ยนแปลงแก้ไขข้อมูลโหนด
6. การดูรายงาน

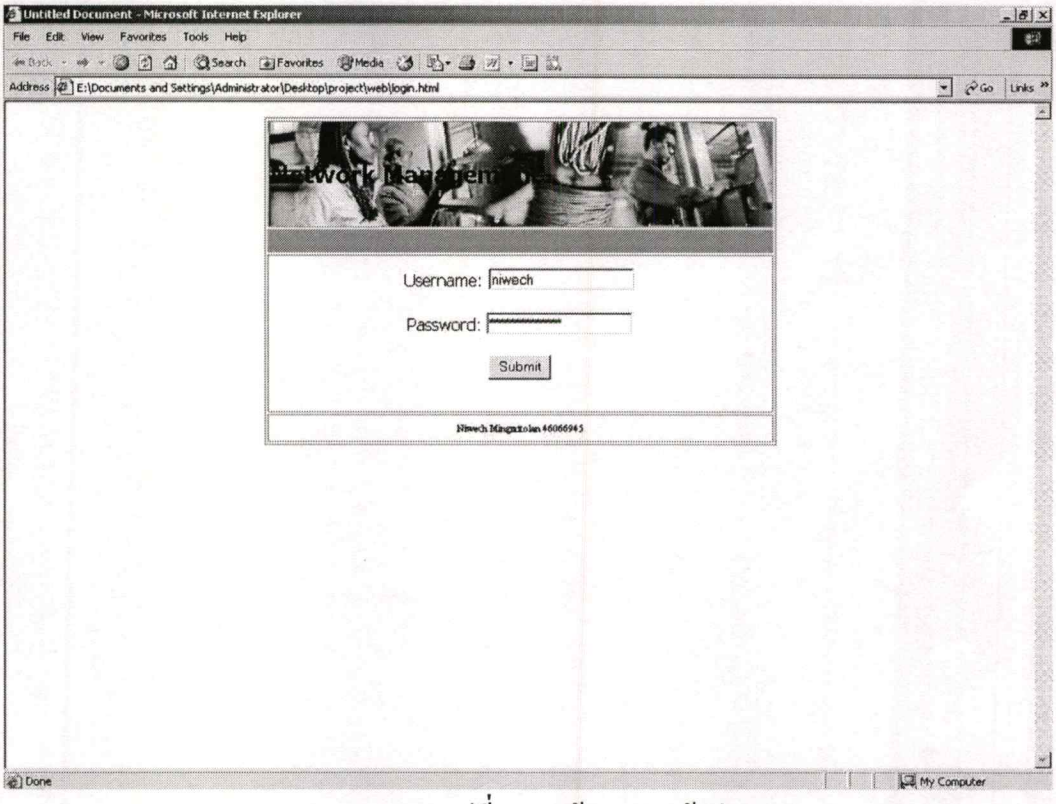


รูปที่ 6.1 วินโดว์เนวิเกชันไดอะแกรมส่วนเชื่อมต่อกับผู้ใช้ระบบ

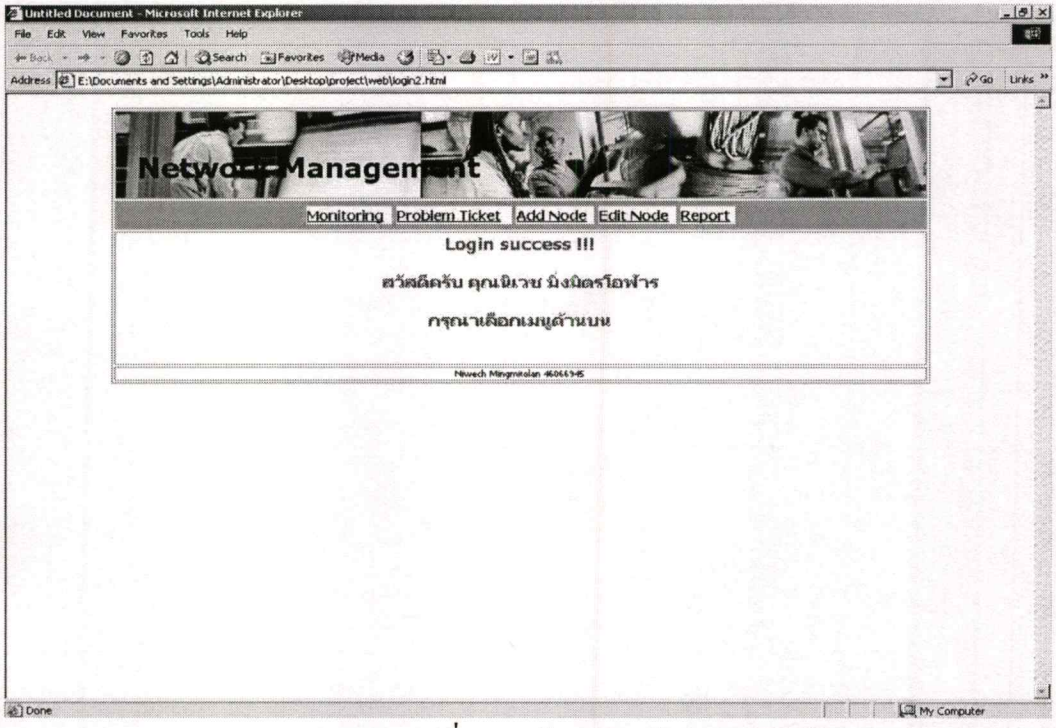
6.2 รายละเอียดการทำงานของระบบ

6.2.1 การเข้าสู่ระบบ

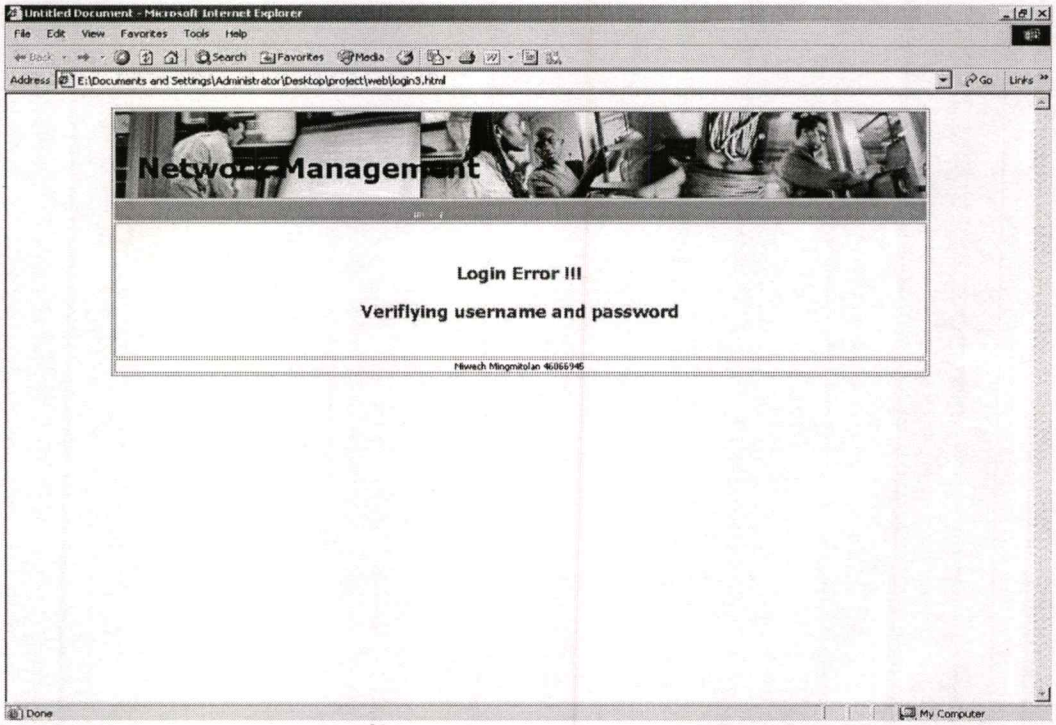
เมื่อผู้ใช้งานระบบเรียกโปรแกรมเฝ้าสังเกตเครือข่ายสารสนเทศ ระบบจะแสดงหน้าจอการเข้าสู่ระบบ ดังรูปที่ 6.2 โดยผู้ใช้ระบบทำการใส่ชื่อและรหัสผ่าน แล้วกดปุ่ม "Submit" ระบบจะทำการตรวจสอบความถูกต้องจากฐานข้อมูลผู้ใช้งานระบบ ถ้าชื่อผู้ใช้ระบบและรหัสผ่านถูกต้อง ระบบจะทำการแสดงหน้าจอการเข้าสู่ระบบสำเร็จ ดังรูปที่ 6.3 หากชื่อผู้ใช้ระบบและรหัสผ่านไม่ถูกต้อง ระบบจะทำการแสดงหน้าจอการเข้าสู่ระบบไม่สำเร็จ ดังรูปที่ 6.4



รูปที่ 6.2 หน้าจอการเข้าสู่ระบบ



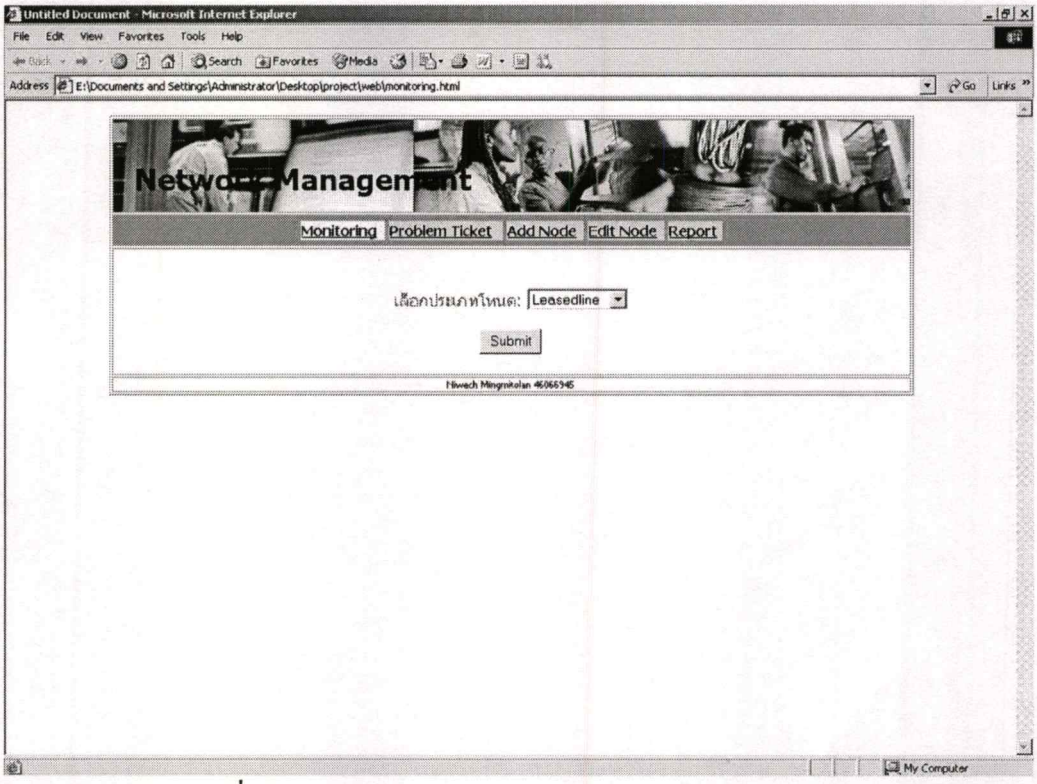
รูปที่ 6.3 หน้าจอการเข้าสู่ระบบสำเร็จ



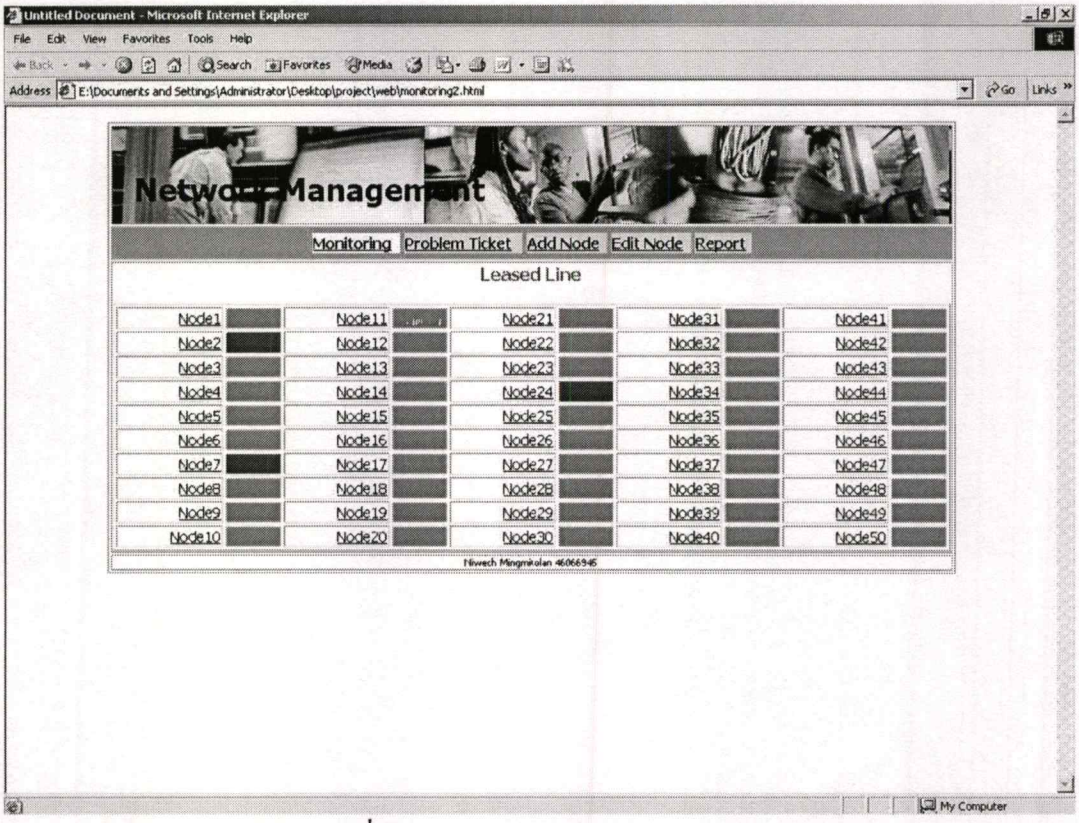
รูปที่ 6.4 หน้าจอเกิดความผิดพลาดในการเข้าสู่ระบบ

6.2.2 การตรวจสอบสถานะของโหนด

เมื่อผู้ใช้งานระบบต้องการดูสถานะปัจจุบันของโหนด ผู้ใช้งานระบบจะต้องเลือกชนิดของวงจร ดังรูปที่ 6..5 แล้วกดปุ่ม “Submit” ระบบจะทำการแสดงสถานะปัจจุบันของโหนดที่บันทึกไว้ในฐานข้อมูลโหนด ดังรูปที่ 6.6



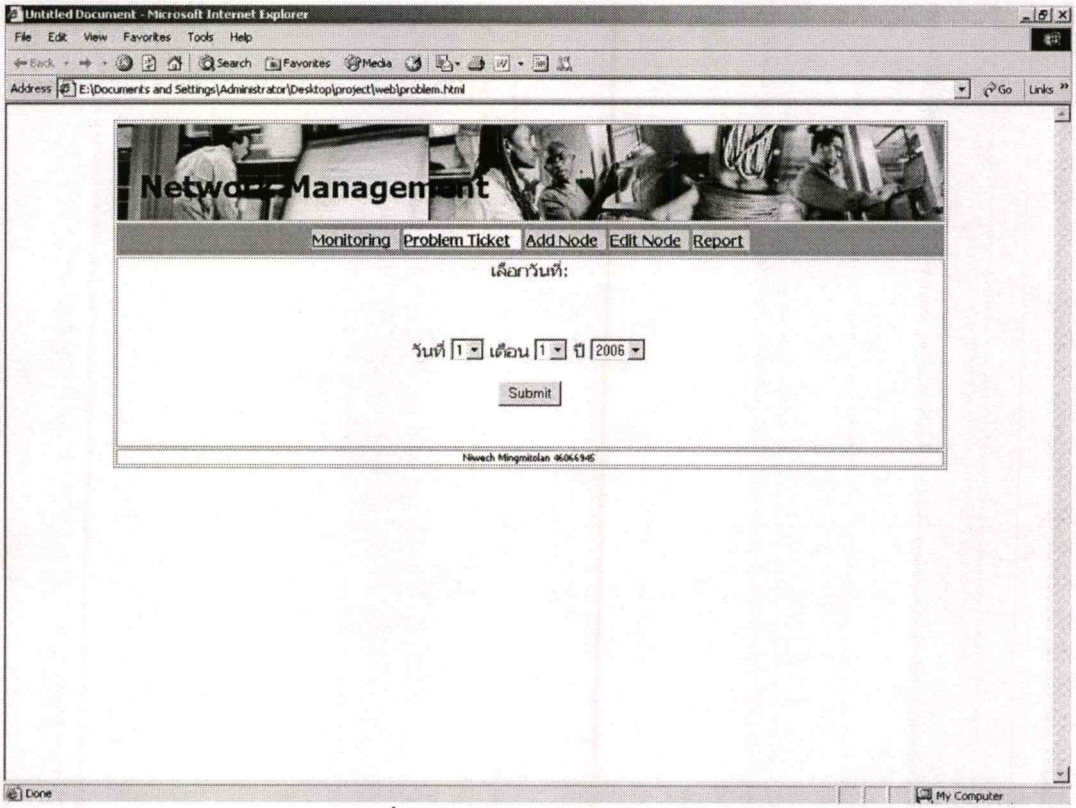
รูปที่ 6.5 หน้าจอการตรวจสอบสถานะของโหนดโดยการเลือกชนิดวงจร



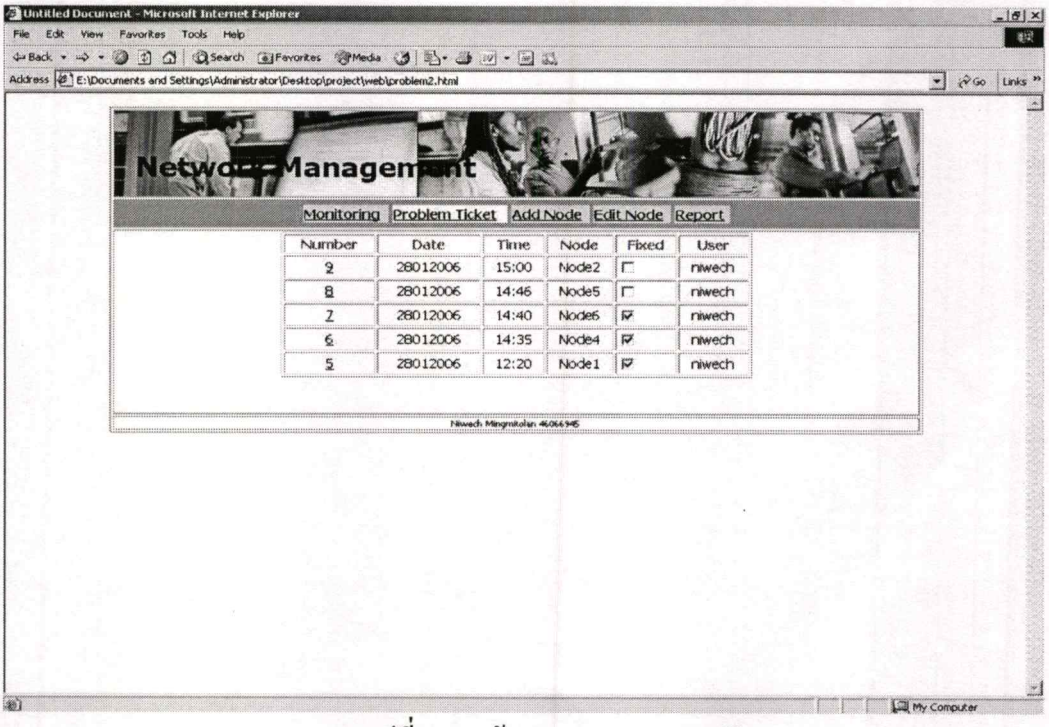
รูปที่ 6.6 หน้าจอการตรวจสอบสถานะของโหนด

6.2.3 การรายงานปัญหาและระบุปัญหาที่เกิดขึ้น

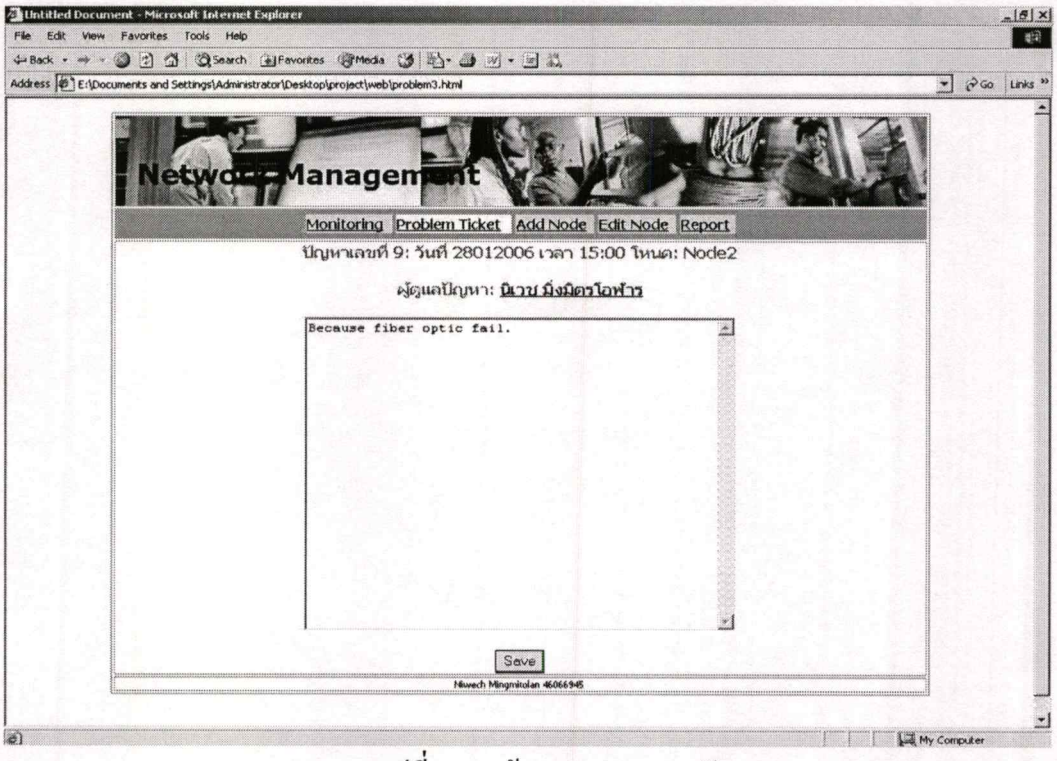
เมื่อผู้ใช้งานระบบต้องการเรียกดูรายงานปัญหาและระบุปัญหาที่เกิดขึ้น โหนดผู้ใช้งานระบบจะต้องเลือกวันที่ที่ปัญหาเกิดขึ้น ดังรูปที่ 6..7 แล้วกดปุ่ม “Submit” ระบบจะทำการแสดงปัญหาทั้งหมดตามวันที่ที่กำหนด ผู้ใช้งานระบบสามารถเลือกรายการปัญหาที่เกิดขึ้นเพื่อดูรายงานปัญหาและระบุปัญหา ดังรูปที่ 6.9



รูปที่ 6.7 หน้าจอการเลือกวันที่รายงานปัญหา



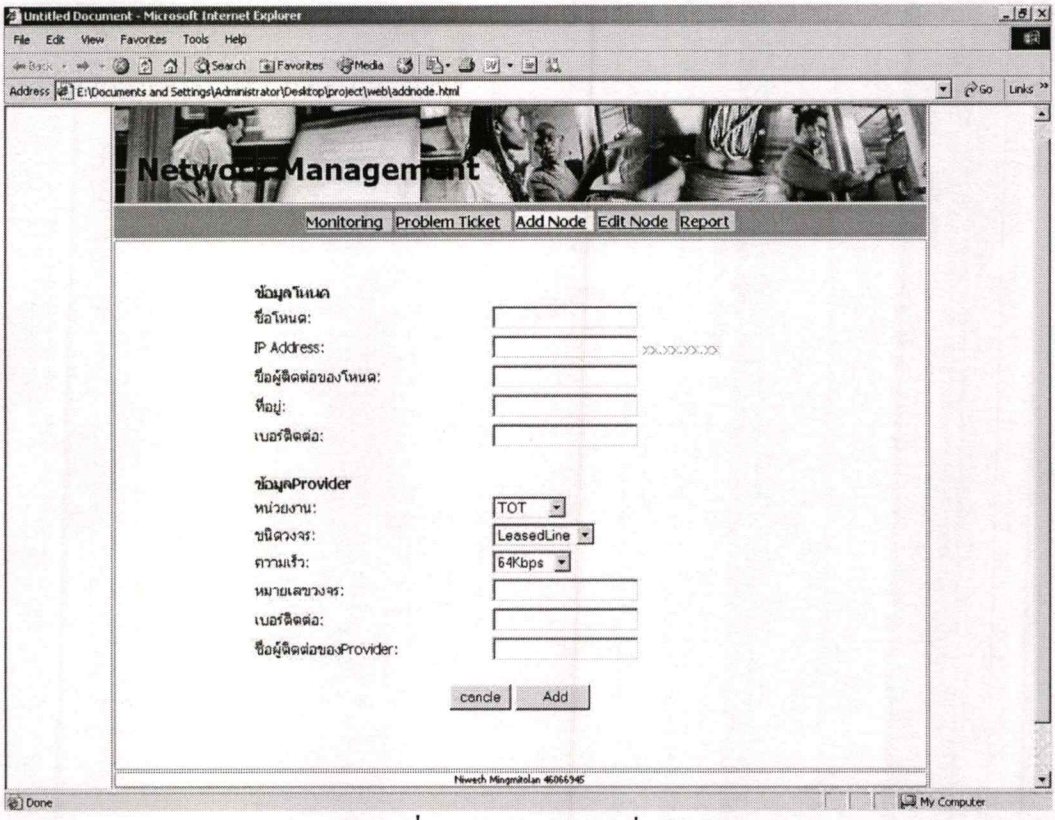
รูปที่ 6.8 หน้าจอการการรายงานปัญหา



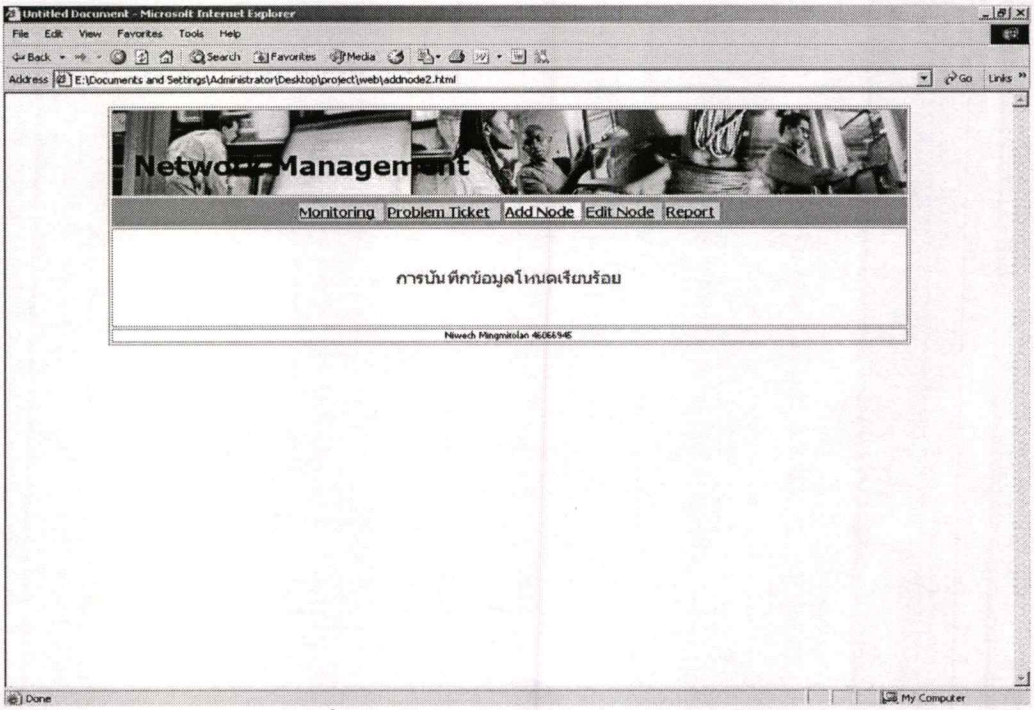
รูปที่ 6.9 หน้าจอการการระบุปัญหา

6.2.4 การเพิ่มโหนด

เมื่อผู้ใช้งานระบบต้องการเพิ่มข้อมูลโหนดใหม่เข้าในระบบ ผู้ใช้งานระบบจะใส่ข้อมูลโหนดทั้งหมด ดังรูปที่ 6.10 แล้วกดปุ่ม “Add” ระบบจะทำการบันทึกข้อมูลของโหนดใหม่ลงฐานข้อมูล และแสดงหน้าจอการเพิ่มโหนดใหม่สำเร็จ ดังรูปที่ 6.11 หลังจากนั้นระบบเฝ้าสังเกตเครือข่ายสารสนเทศจะทำการตรวจสอบสถานะของโหนดทันที



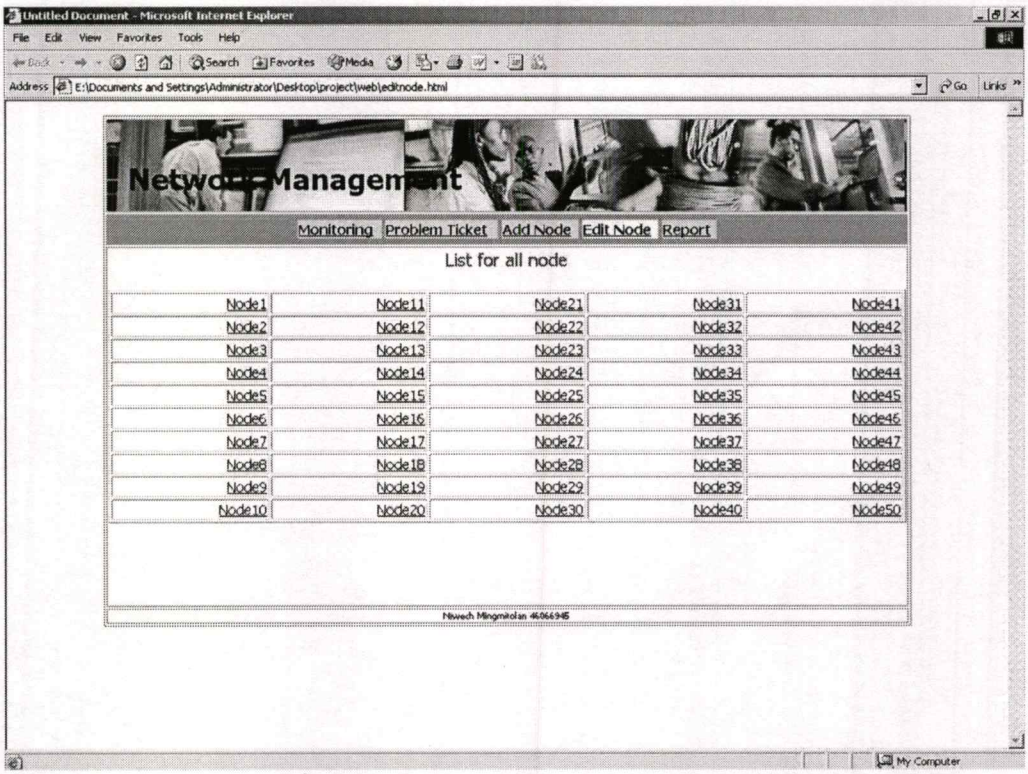
รูปที่ 6.10 หน้าจอการเพิ่มโหนดใหม่



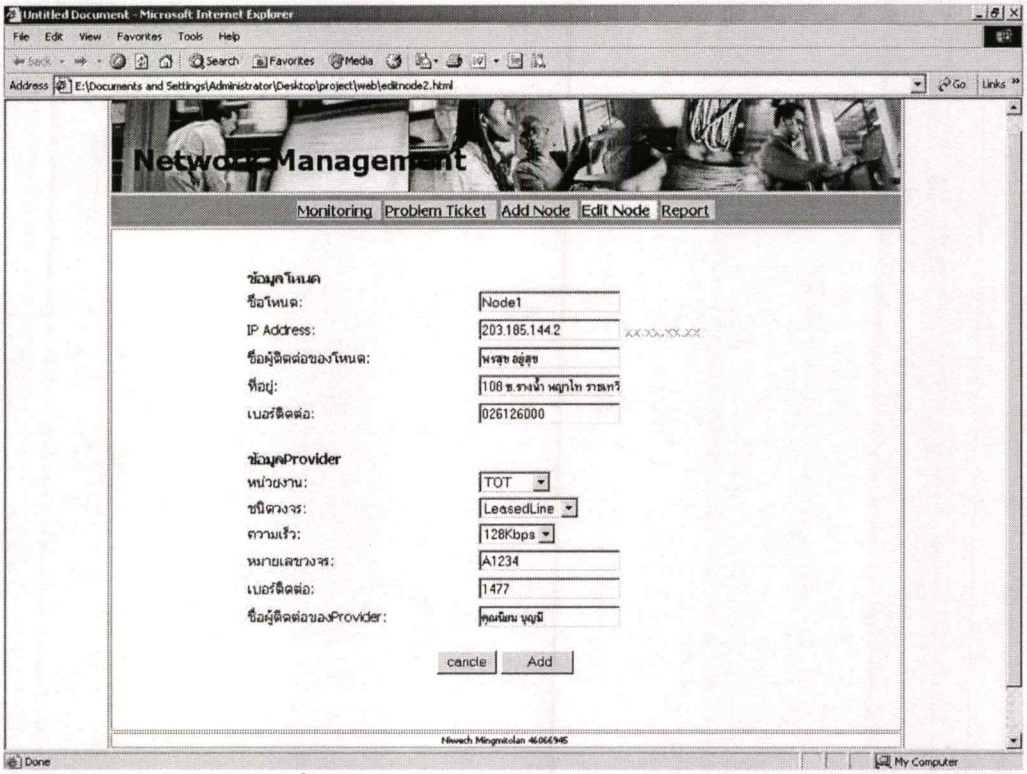
รูปที่ 6.11 หน้าจอการเพิ่มโหนดใหม่เรียบร้อยแล้ว

6.2.5 การเปลี่ยนแปลงแก้ไขข้อมูลโหนด

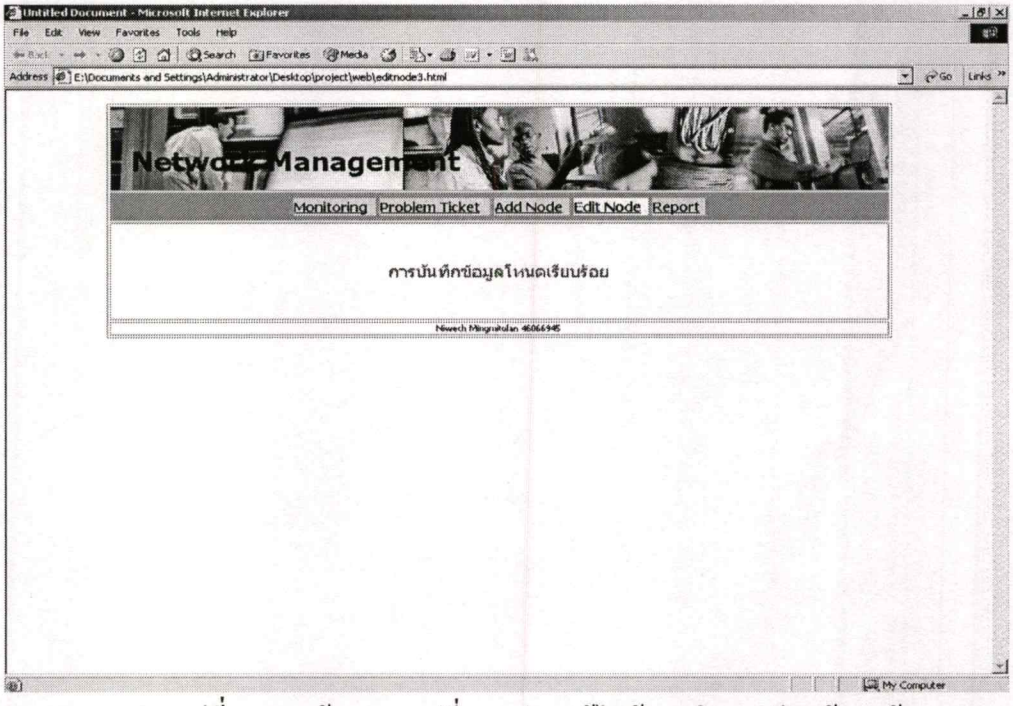
เมื่อผู้ใช้งานระบบต้องการเปลี่ยนแปลงแก้ไขข้อมูลโหนด ระบบจะแสดงโหนดทั้งหมด ดังรูปที่ 6.12 ผู้ใช้งานระบบจะทำการเปลี่ยนแปลงแก้ไขข้อมูลโหนดได้โดยเลือกโหนดที่ต้องการแก้ไข ระบบจะทำการแสดงข้อมูลของโหนดนั้นๆ ดังรูปที่ 6.13 ผู้ใช้งานระบบสามารถแก้ไขข้อมูลโหนด และกดปุ่ม "Add" เพื่อทำการบันทึกข้อมูลใหม่ของโหนด เมื่อการบันทึกข้อมูลเรียบร้อยระบบจะแสดงหน้าจอ ดังรูปที่ 6.14



รูปที่ 6.12 หน้าจอการเปลี่ยนแปลงแก้ไขข้อมูลโหนด



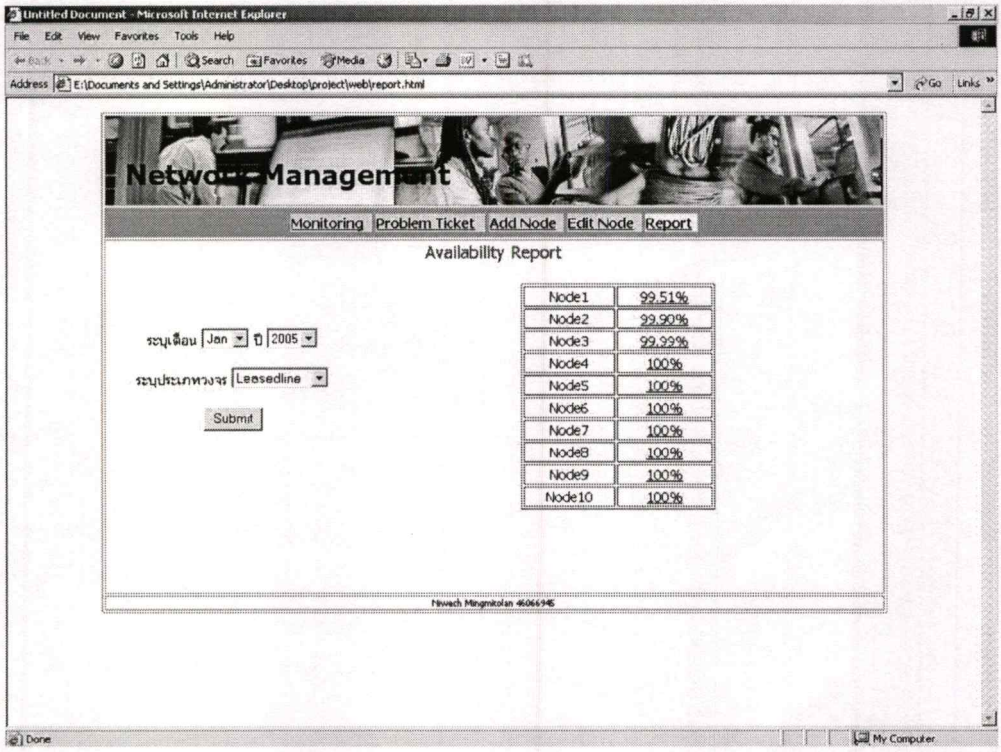
รูปที่ 6.13 หน้าจอการเปลี่ยนแปลงแก้ไขข้อมูลโหนด



รูปที่ 6.14 หน้าจอการเปลี่ยนแปลงแก้ไขข้อมูลโหนดเรียบร้อยแล้ว

6.2.6 การดูรายงาน

เมื่อผู้ใช้งานระบบต้องการทราบเปอร์เซ็นต์คุณภาพในการให้บริการของแต่ละโหนด จะต้องการเลือกเดือนที่ต้องการให้ระบบแสดง แล้วกดปุ่ม “Submit” ระบบจะทำการคำนวณเปอร์เซ็นต์คุณภาพในการให้บริการของแต่ละโหนดมาแสดง ดังรูปที่ 6.15



รูปที่ 6.15 หน้าจอการดูรายงาน

บทที่ 7
บทสรุป

7.1 สรุปผลโครงการ

เครือข่ายคอมพิวเตอร์ เป็นโครงสร้างพื้นฐานในการรับส่งข้อมูลสารสนเทศที่มีความสำคัญเป็นอย่างยิ่ง ทั้งในเรื่องของการทำงานและการสื่อสารปัจจุบัน ดังนั้น หากระบบเครือข่ายคอมพิวเตอร์ไม่สามารถใช้งานได้ย่อมส่งผลกระทบต่อหน่วยงานเป็นอย่างมาก ในการทำสัญญาการใช้บริการระหว่างผู้ใช้บริการและผู้ให้บริการจึงมีข้อตกลงที่เข้มงวดในเรื่องของคุณภาพการให้บริการเพื่อให้มั่นใจว่า เครือข่ายคอมพิวเตอร์สามารถใช้งานได้อย่างตลอดเวลา การแก้ปัญหาที่เกิดขึ้นกับเครือข่ายจึงจำเป็นที่จะต้องรวดเร็ว ดังนั้น จะต้องมีเจ้าหน้าที่คอยดูแลระบบเครือข่ายและคอยแก้ปัญหาอยู่ตลอดเวลา การใช้ระบบแอพพลิเคชั่นด้านการจัดการเครือข่ายจึงจำเป็นอย่างยิ่งในการบริหารจัดการและดูแลเครือข่าย

ระบบเฝ้าสังเกตเครือข่ายสารสนเทศที่ได้พัฒนาขึ้นในโครงการนี้ จะช่วยเป็นเครื่องมือให้เจ้าหน้าที่ใช้ในการดูแลเครือข่ายผ่านทางเว็บแอพพลิเคชั่น ทำให้สะดวกในการเข้าใช้งานระบบและประหยัดค่าใช้จ่ายในการซื้อระบบจากต่างประเทศที่มีราคาแพง

โครงการพัฒนาระบบเฝ้าสังเกตเครือข่ายสารสนเทศนี้ เริ่มต้นด้วยการศึกษาและวิเคราะห์ระบบเฝ้าสังเกตเครือข่ายที่มีในปัจจุบัน วิเคราะห์และออกแบบระบบงานใหม่โดยใช้ยูเอ็มแอล จัดเก็บข้อมูลแบบฐานข้อมูลเชิงสัมพันธ์ ใช้โปรแกรมไมโครซอฟต์วิซิโอ 2003 (Microsoft Visio 2003) ในการสร้างไดอะแกรมต่าง ๆ และใช้โปรแกรมดีไซน์ฟอร์ดาต้าเบส (Dezign for Database) จัดทำแผนภาพเชิงสัมพันธ์ระหว่างเอนทิตีในการออกแบบฐานข้อมูลเชิงสัมพันธ์ พัฒนาโปรแกรมโดยใช้ภาษา Perl และใช้ PHP ในการพัฒนาเว็บแอพพลิเคชัน

7.2 ปัญหา ข้อจำกัดของระบบ และข้อเสนอแนะ

1. ในการตรวจสอบสถานะของเครือข่ายด้วยการส่งไอซีเอ็มพีแพ็กเก็ตไปยังปลายทางนั้น ปลายทาง (โหนด) จะต้องอนุญาตให้สามารถส่งไอซีเอ็มพีแพ็กเก็ตมาถึงได้และตอบกลับ เพื่อให้สามารถตรวจสอบสถานะได้

2. ระบบเฝ้าสังเกตเครือข่ายสารสนเทศส่วนการติดระบุสาเหตุของปัญหา สามารถนำไปพัฒนาเพิ่มเติมในเรื่องการติดตามปัญหาเพื่อให้ปัญหาถูกติดตามจนเสร็จปัญหา และสามารถนำสาเหตุและวิธีการแก้ปัญหาต่างไปพัฒนาเป็นองค์ความรู้ขององค์กรได้ต่อไป

3. การรายงานเปอร์เซ็นต์คุณภาพในการให้บริการของแต่ละโหนดเป็นรายเดือน ไม่สามารถดูรายงานของเดือนปัจจุบันได้ และการคำนวณเปอร์เซ็นต์คุณภาพในการให้บริการคิดจากสูตรดังต่อไปนี้

เปอร์เซ็นต์คุณภาพ = 100 – (เวลาที่เกิดปัญหาขึ้นทั้งหมด / เวลาทั้งหมดของเดือน)x100

บรรณานุกรม

กิตติ ภักดีวัฒนะกุล. 2547. **คัมภีร์ PHP**. กรุงเทพฯ : เคทีพี คอมพ์ แอนด์ คอนซัลท์.

ชาลี วรกุลพิพัฒน์ และ เทพฤทธิ์ บัณฑิตวัฒนาวงศ์. 2544. **UML ภาษามาตรฐานเพื่อผู้พัฒนาซอฟต์แวร์.** กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

ทรงเกียรติ ภาวดี. 2542. **เริ่มเขียนสคริปต์ด้วยภาษา Perl.** กรุงเทพฯ: วิตตี กรุ๊ป.

สมประสงค์ ธิตินิลนิธิ. 2547. **เรียนลัด PHP 4 ครอบคลุมเวอร์ชั่น 4.2.** กรุงเทพฯ : โปรวิชั่น.

สุนทริน วงศ์ศิริกุล. 2537. **พัฒนาโมเดลยุคใหม่ UML Unified Modeling Language มาตรฐานการสร้างโมเดลระบบงาน.** กรุงเทพฯ: ซัคเซส มีเดีย.

วิเชียร เปรมชัยสวัสดิ์. 2546. **ระบบฐานข้อมูล.** กรุงเทพฯ : สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น).

เอกสิทธิ์ วิริยจารี. 2548. **เรียนรู้ระบบเน็ตเวิร์กจากอุปกรณ์ของ Cisco ภาคปฏิบัติ.** กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

Rob, P. and Coronel, C. 2002. **Database Systems.** Sixth Edition. Boston, Massachusetts: Course Technology.

ประวัติผู้เขียน

ชื่อผู้เขียน	นายนิเวช มิ่งมิตรโอฬาร
วัน เดือน ปีเกิด	10 มิถุนายน 2521
สถานที่เกิด	สุพรรณบุรี
วุฒิการศึกษาระดับปริญญาตรี	วิศวกรรมศาสตรบัณฑิต (โทรคมนาคม) มหาวิทยาลัยเทคโนโลยีสุรนารี
การทำงาน	ผู้จัดการส่วนปฏิบัติการเครือข่ายและระบบ สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ