โปรแกรมจัดเก็บและช่วยวิเคราะห์ข้อมูลล็อก

Enhanced Syslog Analyzer Tool

โดย

สกล เขียวลำยอง

รหัสประจำตัว 46066837

อาจารย์ที่ปรึกษา

ผศ.ดร. โชติพัชร์ ภรณวลัย

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
ภาคเรียนที่ 2 ปีการศึกษา 2548
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	โปรแกรมจัดเก็บและช่วยวิเคราะห์ข้อมูลล็อก
นักศึกษา	นาย สกล เขียวลำยอง
อาจารย์ที่ปรึกษา	ผศ.ดร. โชติพัชร์ ภรณวลัย
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2548

บทคัดย่อ

โครงงานนี้จะนำเสนอทั้งทฤษฎีและตัวอย่างการสร้างโปรแกรม Syslog server ที่ทำหน้าที่รวบรวมล็อกไฟล์จากอุปกรณ์ต่างๆในเครือข่าย เนื่องมาจากล็อกไฟล์นั้นนับเป็นข้อมูลที่ความสำคัญมากที่สุด เพราะสามารถบ่งชี้ถึงเหตุการณ์ที่เกิดขึ้นในช่วงเวลาหนึ่งที่ช่วยให้ผู้ดูแลระบบสามารถค้นหาข้อบกพร่องหรือตรวจจับเหตุการณ์ที่ผิดปกติได้ และยังเป็นหลักฐานที่สำคัญเมื่อมีเหตุการณ์ละเมิดความปลอดภัยคอมพิวเตอร์เกิดขึ้นอีกด้วย แต่เนื่องจากจำนวนอุปกรณ์ในเครือข่ายอาจมีเป็นจำนวนมาก ทำให้ข้อมูลล็อกที่เก็บมาได้นั้นมีจำนวนมากและทำให้ยากต่อการค้นหาข้อมูลที่จำเป็นได้ ซึ่งนับเป็นข้อจำกัดของโปรแกรมที่มีอยู่ในปัจจุบัน ทั้งนี้เพื่อเป็นการเพิ่มเติมความสามารถของโปรแกรมที่ใช้อยู่ในปัจจุบันให้มีความสามารถมากขึ้น ในโครงงานพัฒนาระบบนี้จะทำเพิ่มเติมความสามารถในการกรองข้อมูล และค้นหาข้อมูล และสามารถดึงเอาข้อมูลเหล่านั้นมาแสดงผลให้ผู้ดูแลระบบใช้งานได้ในเวลาอันรวดเร็ว เพื่อเพิ่มความสะดวกในการควบคุมดูแลเครือข่ายกับผู้ดูแลระบบให้มากขึ้น

Title	Enhanced Syslog analyzer tool
Student	Mr. Sakon Khiewlamyong
Advisor	Asst. Prof. Dr. Chotipat Pornavalai
Level of Study	Master of Science in Information Technology
Major	Information Science
Academic Year	2005

ABSTRACT

This software development project will present the theories of Syslog protocol and the Syslog server program which response to collect the logs from any Syslog protocol compatible devices in the network. Because of the logs that generate from the devices is very important, they can help the network administrator to troubleshoot the problem that occurred in the network and the logs are also the evidences of the network computer security violation. But a lot of devices may generate many logs so it is difficult to search the necessary data in time. This project will enhance the ability of the ubiquitous software to search and filter the log data in a short time and will make more convenience to administrator.

กิตติกรรมประกาศ

โครงการพัฒนาระบบงานโปรแกรมจัดเก็บและช่วยวิเคราะห์ข้อมูลล็อกสำเร็จได้ด้วยความกรุณาจากอาจารย์ที่ปรึกษา ผศ.ดร. โชติพัชร์ ภรณวลัย ที่ให้ความช่วยเหลือ ให้คำชี้แนะช่วยแก้ปัญหาตลอดจนให้ความรู้และประการณ์ที่ดีแก่ข้าพเจ้า

ขอขอบพระคุณ รศ.ดร. นพพร โชติกกำธร และผศ.ดร. จันทร์บูรณ์ สถิตวิริยวงศ์ กรรมการสอบโครงการพัฒนาระบบงานที่ได้กรุณาให้คำแนะนำตลอดจนข้อชี้แนะ จนในที่สุดทำให้โครงการพัฒนาระบบงานนี้สำเร็จลงได้

ขอขอบพระคุณครอบครัวอันเป็นที่รักยิ่งซึ่งได้เลี้ยงดูข้าพเจ้ามาเป็นอย่างดี พร้อมทั้งให้โอกาสในการศึกษาอย่างเต็มที่ และยังให้กำลังใจ เอาใจใส่เสมอมา

สำหรับคุณงามความดีอันใดที่เกิดจากโครงการพัฒนาระบบงานฉบับนี้ ข้าพเจ้าขอมอบให้กับบิดามารดา ซึ่งเป็นที่รักและเคารพยิ่ง ตลอดจนครูอาจารย์ที่เคารพทุกท่านที่ได้ประสิทธิประสาทวิชาความรู้และถ่ายทอดประสบการณ์ที่ดีให้แก่ข้าพเจ้า

สกล เขียวลำยอง

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญรูป

รูปที่ **หน้า**

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มาของโครงการ

ล็อกไฟล์เป็นข้อมูลที่ความสำคัญมากที่สุด เนื่องจากสามารถบ่งชี้ถึงเหตุการณ์ที่เกิดขึ้นในช่วงเวลาหนึ่งที่ช่วยให้ผู้ดูแลระบบสามารถค้นหาข้อบกพร่องหรือตรวจจับเหตุการณ์ที่ผิดปกติได้ และยังเป็นหลักฐานที่สำคัญเมื่อมีเหตุการณ์ละเมิดความปลอดภัยคอมพิวเตอร์เกิดขึ้น

หน่วยงาน IETF ได้ประกาศมาตรฐานโปรโตคอล syslog สำหรับการทำ logging ซึ่งนิยมนำมาใช้กับระบบปฏิบัติการยูนิกซ์และลินุกซ์โดยโปรแกรมแดมอนที่ชื่อว่า syslogd โดยโปรแกรม syslogd เป็นกลไกที่ใช้ในการเก็บข้อมูลล็อกของ kernel และ application บนระบบยูนิกซ์และลินุกซ์ ที่ถูกติดตั้งมาให้พร้อมกับการติดตั้งระบบปฏิบัติการ โดยผู้ดูแลระบบสามารถปรับแต่งไฟล์ configuration เพื่อควบคุมการทำงานของ syslogd ได้ เช่น ให้ syslogd เก็บข้อมูลไปไว้ที่ไฟล์ใด หรือให้ส่งข้อมูลล็อกนี้ไปเก็บไว้ยังเครื่องอื่นในเครือข่าย

ปัจจุบันได้มีการพัฒนาโปรแกรมที่ทำหน้าที่เป็น syslog server ที่สามารถทำงานบนระบบปฏิบัติการวินโดวส์ได้ เช่นKIWI Syslog ซึ่งเป็นโปรแกรมที่ได้รับความนิยมในกลุ่มของผู้ดูแลระบบ เนื่องจากใช้งานได้ง่าย และเป็นโปรแกรมที่สามารถนำมาใช้ได้โดยไม่เสียค่าใช้จ่าย แต่ข้อจำกัดของโปรแกรมนั้นได้แก่ ไม่สามารถทำการกรองข้อมูล หรือค้นหาข้อมูลได้ตามที่ต้องการได้ ซึ่งถ้าหากระบบเครือข่ายและจำนวนอุปกรณ์ที่ทำหน้าที่ส่งล็อกมาให้มีจำนวนมากแล้ว การค้นหาข้อมูลที่จำเป็นในเวลาที่ต้องแก้ไขปัญหาในเวลาจำกัดนั้นจะเป็นไปได้ยาก

โปรแกรมที่ได้ทำการพัฒนาขึ้นในโครงงานพัฒนาระบบนี้ จะพัฒนาโปรแกรมที่มีความสามารถเป็น syslog server ที่ใช้บนระบบปฏิบัติการวินโดวส์ รวมถึงสามารถทำการกรองข้อมูล หรือค้นหาข้อมูลได้ตามที่ต้องการ เพื่อช่วยในการวิเคราะห์ปัญหาที่เกิดขึ้นได้รวดเร็วมากขึ้น

1.2 วัตถุประสงค์ของโครงการ

1. ศึกษาเรื่องโปรโตคอล syslog และเทคโนโลยีที่เกี่ยวข้อง ได้แก่ Syslog protocol, Syslogd
2. ศึกษาการสร้าง syslog server โดยใช้เทคโนโลยี .NET ได้แก่ VB.NET
3. พัฒนาโปรแกรม syslog server ที่ใช้รับล็อกจากอุปกรณ์ต่างๆ ที่นำมาใช้งานได้บนระบบปฏิบัติการวินโดวส์ โดยพัฒนาจากเทคโนโลยี VB.NET

4. ศึกษาการจับคู่รูปแบบของอักขระโดยใช้ Regular Expression

1.3 ขอบเขตของการพัฒนาโครงการ

1. วิเคราะห์ ออกแบบ พัฒนาโปรแกรม syslog server โดยใช้เทคโนโลยี VB.NET เพื่อจัดเก็บลงฐานข้อมูล
2. ฟังก์ชันพื้นฐานของระบบ ซึ่งประกอบด้วยส่วนการเปิดซ็อกเก็ตเพื่อรอรับข้อมูลล็อกไฟล์ ผ่านพอร์ต UDP 514 และส่วนแสดงผลให้กับผู้ใช้งาน
3. ฟังก์ชันในการกรองข้อมูล หรือค้นหาข้อมูลได้ตามที่ต้องการได้
4. ฟังก์ชันในการจับคู่ข้อมูลที่สนใจในข้อมูลล็อกได้
5. สร้างเอกสารประกอบการพัฒนาโครงการ ซึ่งคลอบคลุมเนื้อหาของกระบวนการวิเคราะห์ออกแบบและพัฒนาระบบงาน

1.4 วิธีการดำเนินงานโครงการ

1. ศึกษาทฤษฎีของการเขียนโปรแกรมแบบซ็อกเก็ต ลักษณะการทำงานของโปรแกรมเครือข่ายแบบซ็อกเก็ต
2. ศึกษาการพัฒนาโปรแกรม syslog server
3. พัฒนาโปรแกรมที่ทำหน้าที่เป็น syslog server ด้วยเทคโนโลยี VB.NET
4. พัฒนาส่วนการจัดเก็บข้อมูลเพื่อเก็บลงฐานข้อมูลสำหรับการนำข้อมูลมากรองและค้นหา เพื่อให้เกิดความรวดเร็ว และได้ข้อมูลที่เป็นประโยชน์
5. พัฒนาส่วนอินเตอร์เฟสที่ติดต่อกับผู้ใช้งาน โดยการดึงเอาข้อมูลในฐานข้อมูลขึ้นมแสดงผลให้ผู้ดูแลระบบสามารถแสดงผลข้อมูลล็อกที่เก็บมาได้และค้นหาข้อมูลตามที่ต้องการ

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้รับความรู้ในวิธีการพัฒนาโปรแกรมเครือข่าย syslog server ที่มีการเปิดใช้งานซ็อกเก็ตเพื่อรอรับข้อมูลที่ส่งมายังพอร์ต

2. โปรแกรมต้นแบบ syslog server ซึ่งพัฒนาโดยเทคโนโลยี VB.NET และทำงานบนระบบปฏิบัติการวินโดวส์ ที่จะช่วยให้มีความสะดวกและรวดเร็วในการใช้งานมากขึ้น โดยโปรแกรมจะทำหน้าที่เก็บข้อมูลล็อกจากอุปกรณ์ต่างๆ และเก็บลงยังฐานข้อมูล นอกจากนี้ ผู้ดูแล

ระบบจะสามารถดูข้อมูลได้โดยเลือกการแสดงผลตามที่ต้องการ โดยระบุได้ตามรายอุปกรณ์ที่ส่งข้อมูลมา หรือตามเงื่อนไขที่ผู้ดูแลระบบต้องการ

สารบัญตาราง

หน้า

ตารางที่

สารบัญรูป

หน้า

รูปที่

บทที่ 2
โปรโตคอล SYSLOG

เนื่องจากการขยายตัวของระบบเครือข่ายเกิดขึ้นอย่างรวดเร็ว ทำให้ระบบการจัดเก็บล็อกมารวมยังศูนย์กลางมีความสำคัญมากในการช่วยดูแลความปลอดภัยของระบบเครือข่าย การแก้ไขปัญหาที่เกิดขึ้น การตรวจหาสิ่งปกติและข้อมูลต่างๆที่เกี่ยวข้องและเป็นประโยชน์กับผู้ดูแลระบบ รูปแบบการทำงานของกลไกการเก็บล็อกโดยพื้นฐานแล้วไม่ได้มีความซับซ้อนมาก โปรแกรมที่ทำหน้าที่เป็นเซิร์ฟเวอร์ จะทำการเปิดพอร์ตเพื่อรอรับฟังข้อมูลผ่านพอร์ตยูดีพี 514 และนำข้อมูลที่ได้รับมา จัดเก็บลงไฟล์ข้อมูล หรือฐานข้อมูล แต่ความสามารถอื่นๆที่นอกจากการเก็บล็อกเช่น การกรองข้อมูล การแสดงผลข้อมูล การแจ้งเตือนผู้ดูแลระบบเมื่อตรวจพบสิ่งปกติ เพื่อช่วยให้การทำงานของผู้ดูแลระบบสามารถทำงานได้ง่ายขึ้น และยังลดเวลาในการทำงานอีกด้วย

ปัจจุบันมีโปรแกรมประเภทนี้ที่จำหน่ายและแจกฟรีที่ได้เพิ่มเติมความสามารถดังกล่าวเข้าไปด้วย ยกตัวอย่างโปรแกรมที่ได้รับความนิยมเช่น KIWI syslog server ซึ่งเป็นโปรแกรมฟรีแวร์ และมีความสามารถในการเก็บล็อกและแสดงผล รวมทั้งแสดงข้อมูลตามสถิติได้ แต่พบว่ายังมีความสามารถอื่นๆที่ยังไม่เพียงพอต่อความต้องการของผู้ดูแลระบบ โครงงานที่ได้จัดทำขึ้นจะเพิ่มความสามารถในการ การกรองข้อมูล การแสดงผลข้อมูล และการค้นหาข้อมูลที่มีประสิทธิภาพและรวดเร็ว

2.1 Syslog

Syslog พัฒนาขึ้นจากมหาวิทยาลัยแคลิฟอร์เนีย เพื่อใช้งานกับระบบปฏิบัติการยูนิกส์ ได้รับการประกาศเป็นมาตรฐานโดยหน่วยงาน IETF ใน RFC 1364 โดยนิยามว่า โปรโตคอล syslog จะทำหน้าที่ในการขนส่งขอมูลจากเครื่องที่ส่งข้อความแจ้งเตือนผ่านเครือข่ายไอพีไปยังเครื่องที่ทำหน้าที่รวบรวมข้อความเหตุการณ์เหล่านี้ ซึ่งจะเรียกว่า syslog server

2.1.1 Syslog message คือเมสเสจที่สร้างขึ้นโดยเครื่องที่ส่งข้อมูลผ่านเครือข่ายไอพีมายัง syslog server ได้ โดยในเมสเสจเหล่านี้จะประกอบไปด้วยข้อมูลรูปแบบต่างๆที่เข้ากันได้กับโปรโตคอล syslog ยกตัวอย่างเช่น เราเตอร์สามารถสร้างเมสเสจสำหรับแจ้งว่ามีการเปลี่ยนแปลงสเตจของอินเตอร์เฟสเป็น up หรือ down นอกจากนี้เราเตอร์ยังสามารถสร้างเมสเสจ syslog ได้ในกรณีที่มีการละเมิดข้อกำหนดทางความปลอดภัยจากการกำหนด ACL อีกด้วย เมสเสจเหล่านี้จะถูกส่งผ่านระบบเครือข่าย โดยมีการกำหนดในคอนฟิกูเรชันของตัวอุปกรณ์เหล่านั้น แต่ต้องมั่นใจว่า

จากอุปกรณ์เหล่านั้นสามารถเชื่อมต่อถึงกันได้กับ syslog server และทั้งสองฝ่ายต้องสามารถเข้าใจถึงรูปแบบของ syslog ด้วยเนื่องจากผู้ผลิตอุปกรณ์ต่างก็มีมาตรฐานของตัวเอง ดังนั้นจึงต้องมีการกำหนดมาตรฐานของรูปแบบของ syslog เมสเสจเพื่อให้เข้าใจตรงกันและสื่อสารกันได้ Syslog เองก็มีจุดอ่อนในด้านความปลอดภัยของข้อมูล และลักษณะการส่งข้อมูลที่เป็นแบบ best effort ซึ่งขณะนี้ จุดอ่อนเหล่านี้กำลังได้รับการปรับปรุงและเตรียมประกาศเป็น RFC ตัวใหม่ในปี 2549

ระบบปฏิบัติการ โพรเซส และแอพพลิเคชัน ถูกเขียนขึ้นให้มีการแจ้งสถานะของตัวเองหรือเมสเสจที่บอกถึงเหตุการณ์ที่เกิดขึ้นมายังเครื่องตัวเองเท่านั้น เมื่อระบบปฏิบัติการ โพรเซส และแอพพลิเคชันถูกพัฒนาให้มีความซับซ้อนมากยิ่งขึ้น ระบบจึงต้องมีการจัดกลุ่มของเมสเสจเหล่านั้นเผื่อให้ผู้ดูแลระบบสามารถรับรู้และแก้ปัญหาได้รวดเร็วมากขึ้นจากเมสเสจที่เป็นข้อความที่สามารถเข้าใจได้ง่าย

Syslog เป็นมาตรฐานที่ได้รับการยอมรับจากหลายระบบปฏิบัติการ มีความยืดหยุ่นในการคอนฟิกกูเรชันเครื่องปลายทางที่จะทำการส่งเมสเสจไปให้ และนอกจากจะเก็บและแสดงผลได้ในเครื่องตัวเองแล้วนั้น ยังสามารถส่งเมสเสจไปตามเครือข่ายเพื่อไปเก็บยังเครื่องอื่นและนำเมสเสจออกไปแสดงผลได้อีกด้วย ทั้งนี้ยังเป็นการช่วยเพิ่มความสามารถในการเก็บเมสเสจให้นานมากขึ้นเนื่องจากข้อจำกัดและพื้นที่ในการจัดเก็บของตัวอุปกรณ์ด้วย

- เมสเสจและเหตุการณ์ที่เกิดขึ้นขณะที่ผู้เขียนทำการเขียนแอพพลิเคชัน โพรเซส และระบบปฏิบัติการแอพพลิเคชันนั้นก็ได้เขียนเมสเสจที่ใช้สำหรับควบคุมการทำงานให้เป็นไปตามที่ต้องการด้วย เมสเสจนั้นอาจกล่าวถึงสถานะหรือพบว่ามีเงื่อนไขตรงตามที่ให้สร้างเมสเสจออกมา บางเมสเสจก็จะมีสัญญาณแจ้งเตือนด้วย ซึ่งเมสเสจต่างๆก็จะถูกจัดกลุ่มได้ตาม facility และ severity ของเมสเสจเหล่านั้น ช่วยให้ผู้ดูแลระบบสามารถตรวจสอบและตอบสนองต่อเมสเสจได้ตามลำดับความสำคัญ เพิ่มเติมด้วยความสามารถที่จะจัดเก็บเมสเสจและแสดงเมสเสจด้วย อุปกรณ์จะต้องมีการปรับแต่งค่าเพื่อให้แสดงเมสเสจหรือส่งต่อเมสเสจไปเก็บยังเครื่องอื่นซึ่งช่วยให้มีความยืดหยุ่นมากขึ้น เนื่องจากผู้ดูแลระบบอาจต้องการเก็บเมสเสจที่เกิดขึ้นไว้และส่งต่อเมสเสจที่มีลำดับความ สำคัญสูงไปยังอีกเครื่องหนึ่ง ดังนั้นเมสเสจจึงมีรูปแบบการอ่านแบบง่ายเพื่อให้ผู้ที่ได้รับเมสเสจเกิดความเข้าใจ นอกจากนี้ในตัวเมสเสจยังระบุเวลาอ้างอิงและชื่อโพรเซสที่สร้างเมสเสจขึ้นมาด้วย อุปกรณ์ที่ไม่มีพื้นที่จัดเก็บข้อมูลในตัวเอง เช่น เราเตอร์ สวิทช์ ก็จะสามารถส่งเมสเสจไปยังเซิร์ฟเวอร์ที่ทำหน้าที่จัดเก็บเมสเสจ และผู้ดูแลระบบสามารถตรวจสอบปัญหาที่เกิดได้ง่ายมากขึ้น
- การทำงานของตัวรับเมสเสจ ตัวรับเมสเสจหรือ syslog server โดยทั่วไปแล้วก็จะนำ

ข้อมูลเหล่านั้นมาแสดงผล จัดเก็บลงดิสค์ ส่งต่อไปยังตัวรับเมสเสจอื่น ๆ ซึ่งขึ้นอยู่กับความต้องการของผู้ดูแลระบบ แต่เป้าหมายหลักก็คือทำให้เกิดการเป็นศูนย์กลางของการเก็บรวมเมสเสจขึ้น เพื่อให้ผู้ดูแลระบบสามารถตรวจสอบข้อมูลได้ง่ายขึ้น

2.1.2 Transport Layer Protocol เมสเสจ syslog จะใช้โปรโตคอลยูดีพีในการทำงาน โดยยูดีพีพอร์ต ที่ใช้คือพอร์ต 514 จำเป็นที่ต้องระบุว่าซอร์สพอร์ตจะต้องเป็นพอร์ต 514 เพื่อระบุถึงว่าเมสเสจที่ส่งมาเป็นเมสเสจ syslog แต่ถ้าหากส่งมานอกเหนือจากพอร์ต 514 ก็จำเป็นที่จะต้องจัดรูปแบบข้อมูลให้ถูกต้องด้วย

2.1.3 โครงสร้างของ sys log server รูปแบบการเชื่อมต่อระหว่างอุปกรณ์ที่สร้างเมสเสจและเครื่องที่ทำหน้าที่จัดเก็บเมสเสจนั้นอาจเป็นไปได้ดังนี้

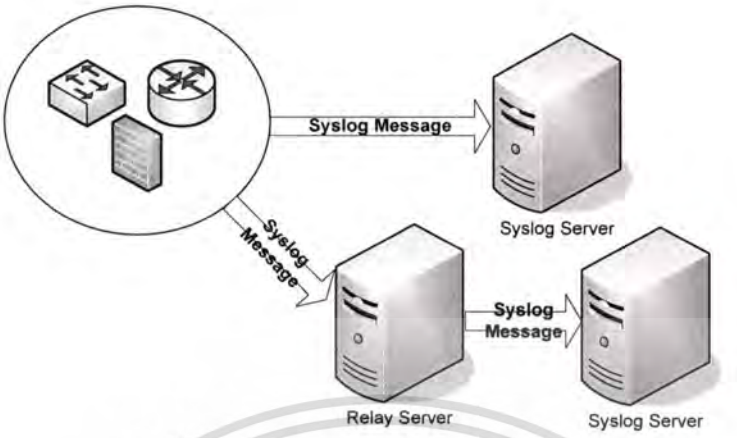
- มีการเชื่อมต่อถึงกันโดยตรงผ่านระบบเครือข่าย โดยเมื่อมีการสร้างเมสเสจ เมสเสจเหล่านั้นก็จะถูกจัดส่งไปยังเซิร์ฟเวอร์ที่ทำการจัดเก็บทันที

รูปที่ 2.1 syslog server เชื่อมต่อถึงกันโดยตรงผ่านระบบเครือข่าย

- มีการเชื่อมต่อถึงกันโดยผ่านตัวกลางที่เรียกว่ารีเลย์เซิร์ฟเวอร์ โดยที่รีเลย์เซิร์ฟเวอร์นี้จะทำการส่งต่อเมสเสจผ่านระบบเครือข่ายไปยังเซิร์ฟเวอร์ที่ทำการจัดเก็บต่อไป

รูปที่ 2.2 syslog server เชื่อมต่อถึงกันโดยผ่านตัวกลางที่เรียกว่ารีเลย์เซิร์ฟเวอร์

- การเชื่อมต่อไปยังยังเซิร์ฟเวอร์ที่ทำการจัดเก็บหลายตัวได้ในเวลาเดียวกันอาจต่อผ่านเครือข่ายโดยตรงไปยังเซิร์ฟเวอร์ที่ทำการจัดเก็บหรือผ่านทางรีเลย์เซิร์ฟเวอร์ก็ได้



รูปที่ 2.3 sys log server เชื่อมต่อถึงกันแบบผสม

2.1.4 Packet Format and Contents ข้อความในไอพีแพ็กเก็ตจะประกอบไปด้วยยูดีพีปลายทางที่พอร์ต 514 ที่ระบุว่าเป็นเมสเสจ syslog ซึ่งจำเป็นจะต้องให้เป็นไปตามมาตรฐานเดียวกัน โดยจะประกอบไปด้วย 3 ส่วน ส่วนแรกเรียกว่า PRI ส่วนที่สองเรียกว่า HEADER และส่วนสุดท้ายคือ MSG ความยาวรวมของแพ็กเก็ตไม่เกิน 1024 ไบต์

1. PRI จะมี สาม สี่ หรือ ห้าตัวอักษรพร้อมด้วยเครื่องหมาย <> (angle brackets) ข้อมูลในเครื่องหมายวงเล็บนี้ จะบอกถึง priority และแสดงถึง Facility และ Severity ด้วย Facility และ Severity จะเป็นตัวเลขฐานสิบ ซึ่งมีความหมายดังตารางต่อไปนี้

ตารางที่ 2.1 syslog Message Facilities

Numerical Code	**Facility**
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages (note 1)
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon (note 2)

ตารางที่ 2.1 (ต่อ)

Numerical Code	Facility
10	security/authorization messages (note 1)
11	FTP daemon
12	NTP subsystem
13	log audit (note 1)
14	log alert (note 1)
15	clock daemon (note 2)
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

นอกจากนี้ ใน priority ยังบอกถึง Severity ด้วยซึ่งมีความหมายดังตารางด้านล่าง

ตารางที่ 2.2 syslog Message Severities

Numerical Code	Severity
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

Priority จะถูกคำนวณมาจากการคูณ Facility ด้วย 8 และจากนั้นบวกด้วยเลข Severity ยกตัวอย่างเช่น "local use 4" message (Facility=20) กับ Severity of Notice (Severity=5) จะมี priority เท่ากับ 165 ดังนั้นในแพ็กเก็ต syslog ส่วน PRI ก็จะมีการแสดงข้อความเป็น <165>

2. HEADER จะประกอบไปด้วยตัวระบุเวลาที่เหตการณ์เกิดและชื่อหรือไอพีแอดเดรสของอุปกรณ์ที่สร้างเมสเสจนี้ขึ้น ตัวระบุเวลาจะอยู่ในรูปแบบ "Mmm dd hh:mm:ss" และจะเป็นเวลาท้องถิ่นตามอุปกรณ์ตัวนั้น และในฟิลด์โฮสต์เนมจะมีข้อมูลของชื่อโฮสต์เนม IPv4 sinv IPv6 ซึ่งแนะนำให้ระบุเป็นชื่อโฮสต์เนม

3.MSG จะเป็นส่วนที่เหลือทั้งหมดของแพ็กเก็ต syslog ซึ่งจะประกอบไปด้วยข้อมูลของโพรเซสที่สร้างเมสเสจขึ้น และข้อความอธิบายเมสเสจนั้น

2.2 การประยุกต์ใช้โปรโตคอล syslog กับ อุปกรณ์ในระบบเครือข่าย

อุปกรณ์ในระบบเครือข่าย CISCO เช่น เราเตอร์ ไฟล์วอลและอุปกรณ์วีพีเอ็น จะทำการสร้างเมสเสจ syslog เพื่อแจ้งข้อมูลและข้อความแจ้งเตือนมายังผู้ดูแลระบบ โดยเราเตอร์จะทำการสร้างเมสเสจเมื่อมีอินเตอร์เฟสที่หยุดทำงานหรือมีการเปลี่ยนแปลงค่าการปรับแต่งต่างๆ และเช่นกัน อุปกรณ์ไฟล์วอลก็จะสร้างเมสเสจเมื่อมีการบล็อกคอนเน็กชันทีซีพี
อุปกรณ์ของ CISCO สามารถปรับแต่งค่าให้ส่งเมสเสจของ syslog ไปยังอุปกรณ์ภายนอกที่ทำหน้าที่เป็น syslog server ได้อีกด้วย โดยปกติแล้วเมสเสจ syslog จะเก็บไว้ที่ภายในตัวอุปกรณ์เอง ดังนั้นหากการเชื่อมต่อระหว่างตัวอุปกรณ์และ syslog server มีปัญหาเกิดขึ้น ก็จะไม่สามารถส่งเมสเสจถึงกันได้ ในกรณีนี้ผู้ดูแลระบบจำเป็นจะต้องเข้าไปดูเมสเสจจากที่ตัวอุปกรณ์เท่านั้น

เนื่องจากการ Syslog ใช้โปรโตคอล UDP (User Datagram Protocol) ในการสื่อสารตามลักษณะการทำงานของโปรโตคอลนี้จึงไม่มีการตอบกลับ (acknowledgment) และที่แอพพลิเคชันเลเยอร์ก็ไม่มีการตอบกลับเช่นกัน จึงไม่สามารถทราบได้ว่ามี syslog server ได้รับเมสเสจจริงหรือไม่ และไม่ว่า syslog server จะอยู่หรือไม่ก็ตาม ตัวอุปกรณ์ก็จะยังส่งเมสเสจมาเสมอ
แพ็กเก็ต syslog จะมีขนาด 1024 ไบต์และประกอบไปด้วยข้อมูลต่อไปนี้

- Facility
- Severity
- Hostname
- Timestamp
- Message
- Facility

เมสเสจ syslog แบ่งประเภทตามแหล่งที่สร้างเมสเสจออกมา เช่น ระบบปฏิบัติการ โพรเซส หรือแอพพลิเคชัน โดยแต่ละค่าจะมีความหมายของ facility เป็นไปตามตารางที่ 2.1 ซึ่งถ้าหากไม่มีค่าที่กำหนดไว้ก่อนตามตารางดังกล่าว อาจจะนำค่า local ค่าใดค่าหนึ่งมาใช้ก็ได้

Severity

นอกจากค่า Facility แล้ว ยังมีค่าความสำคัญที่เรียกว่า severity อีกด้วย ซึ่งมีความหมายตามตารางที่ 2.2 อุปกรณ์ของ CISCO จะใช้ค่าลำดับความสำคัญนี้สำหรับแจ้งเตือนปัญหาของซอร์ฟแวร์และฮาร์ดแวร์ ยกตัวอย่างเช่น อินเตอร์เฟสมีการเปลี่ยนแปลงค่าเป็น up หรือdown หรือมีการรีสตาร์ทระบบ จะมีค่าความสำคัญเป็นระดับ 5 และการรีโหลดระบบมีค่าความสำคัญเป็นระดับ 6

Hostname

ฟิลด์นี้จะประกอบด้วย hostname ที่ถูกตั้งค่าไว้หรือไอพีแอดเดรส ในตัวอุปกรณ์ได้แก่เราเตอร์หรือไฟล์วอลที่มีหลายอินเตอร์เฟส syslog จะใช้ไอพีแอดดเดรสของอินเตอร์เฟสนั้นเพื่อส่งเมสเสจมา

Timestamp

Timestamp จะเป็นเวลาท้องถิ่นในรูปแบบ MMM DD HH:MM:SS ในขณะที่มีการสร้างเมสเสจ แม้ว่าตาม RFC 3164 ไม่ได้ระบุการใช้ timezone มา แต่ระบบปฏิบัติการของอุปกรณ์ CISCO ยอมให้มีการตั้งค่าเพื่อส่งข้อมูลเวลาตาม timezone ได้ timestamp จะถูกสร้างโดยมีเครื่องหมายพิเศษอยู่ด้านหน้า timezone เช่น an asterisk (*) หรือ colon (:) เพื่อป้องกันการแปลความผิดพลาดของ syslog server โดยรูปแบบการส่ง timestampt แบบ timezone จะเป็น MMM DD HH:MM:SS Timezone *.

Message

Message จะเป็นส่วนที่เป็นข้อความพร้อมด้วยข้อมูลเพิ่มเติมเกี่ยวกับโพรเซสที่สร้างเมสเสจมา เมสเสจที่สร้างจากระบบปฏิบัติการของ CISCO จะเริ่มด้วยเครื่องหมายเปอร์เซ็นต์ (%) ดังนี้

%FACILITY-SEVERITY-MNEMONIC: Message-text

ยกตัวอย่างเช่น

*Mar 6 22:48:34.452 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

ความหมายของแต่ละฟิลด์เป็นดังนี้

- FACILITY บอกถึงแหล่งที่สร้างเมสเสจ เช่นตัวอุปกรณ์ , โปรโตคอล หรือโมดูลของซอร์ฟแวร์ ซึ่งค่า Facility ของอุปกรณ์ CISCO จะเกี่ยวข้องเฉพาะเมสเสจของตนเองเท่านั้น ซึ่งจะแตกต่างไปจากที่ระบุไว้ตาม RFC 3164
- SEVERITY— ตามที่ระบุในตารางที่ 2.2
- MNEMONIC—เป็นโค้ดเฉพาะของอุปกรณ์
- Message-text— เป็นข้อความที่อธิบายรายละเอียดเช่นพอร์ตหรือเน็ตเวิร์คแอดเดรส

รูปแบบของเมสเสจ syslog ที่สร้างจาก CatOS จะมีความแตกต่างไปเล็กน้อยจาก IOS ยกตัวอย่างเช่น

mm/dd/yyy:hh/mm/ss:facility-severity-MNEMONIC:Message-text

รูปแบบของเมสเสจ syslog ที่สร้างจากไฟล์วอลรุ่น PIX จะเริ่มต้นด้วยเครื่องหมายเปอร์เซ็นต์ ยกตัวอย่างเช่น

%PIX-Level-Message_number: Message_text

2.3 โปรแกรม Kiwi syslog server

Syslog server นั้นสามารถทำได้บนระบบปฏิบัติการ Linux Unix หรือ windows ก็ได้ ยกตัวอย่างเช่นโปรแกรม Kiwi Syslogd Server ซึ่งเป็นที่นิยมใช้กันมากในกลุ่มของผู้ดูแลระบบ ซึ่งมีข้อดีดังนี้

- เป็นโปรแกรมฟรี ไม่เสียค่าใช้จ่าย
- ทำงานเป็นแบลกกราวน์โพรเซส
- ง่ายต่อการจัดการเนื่องจากเป็น GUI
- ใช้ได้ทั้งมีซีพีและยูดีพี ดังนั้นจึงสามารถรับ TCP syslog จาก PIX ได้
- มี syslog viewer ในตัวซึ่งสามารถดูข้อมูลแบบทันทีได้
- มีฟังก์ชันในการตัดไฟล์อัตโนมัติซึ่งสามารถเลือกตั้งได้

- สามารถแสดงสถิติด้วยกราฟได้
- มีฟังก์ชันในการส่งสัญญาณเตือน หรือส่งจดหมายอิเล็กทรอนิกส์ไปยังผู้ดูแลระบบ

ตัวอย่างข้อความจากโปรแกรม Kiwi Syslogd Server เป็นดังนี้

2005-04-16 21:50:56 Local7.Notice 192.168.0.10 9071: Apr 16 20:50:57.852 PST: %SYS-5-CONFIG_I: Configured from console by vty0 (192.168.0.150)

2005-04-16 21:50:56 Local7.Notice 192.168.0.10 9072: Apr 16 20:50:58.388 PST: %LINK-5-CHANGED: Interface Loopback0, changed state to administratively down

2005-04-16 21:50:58 Local7.Notice 192.168.0.10 9073: Apr 16 20:50:59.380 PST: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to down

CISCO ก็มีโปรแกรมที่เป็นเซิร์ฟเวอร์ของไฟล์วอลเช่นกัน ซึ่งทำงานบนระบบปฏิบัติการวินโดว์เป็นเซอร์วิส ไม่มีการแสดงผล GUI รอรับฟังข้อมูลได้ทั้งทีซีพีและยูดีพี ซึ่งโปรแกรมนี้สามารถนำไปใช้กับอุปกรณ์ประเภทอื่นได้เช่นกัน

ข้อเสียของโปรโตคอล syslog คือด้านความปลอดภัย โดยมีข้อด้อยดังนี้

1. Clear text เนื่องจาก syslog จะมีการส่งข้อมูลแบบเคลียร์เท็กซ์ ซึ่งสามารถตรวจจับได้จากโปรแกรมตรวจจับข้อมูลเช่น sniffer เพื่อป้องกันเหตุการณ์เหล่านี้ เมสเสจของ syslog ควรจะมีการส่งไปยังระบบเครือข่ายแยกต่างหากโดยใช้อินเตอร์เฟสอีกอินเตอร์เฟสหนึ่ง หรืออาจใช้ IP Security (IPSec) ในการเข้ารหัสข้อมูลระหว่างอุปกรณ์และเซิร์ฟเวอร์ได้เช่นกัน

2. UDP เนื่องจาก syslog ใช้โปรโตคอลยูดีพีในการสื่อสาร ดังนั้นผู้โจมตีระบบจะสามารถปลอมแปลงไอพีเอดเดรสของผู้ส่งและส่งเมสเสจปลอมมาให้ หากต้องการป้องกันปัญหานี้ควรให้ syslog ทำงานบนโปรโตคอลทีซีพี

3. Centralized location แม้ว่าการส่งเมสเสจมารวมยังที่เดียวจะเป็นประโยชน์สำหรับผู้ดูแลระบบ แต่หากผู้โจมตีระบบสามารถเจาะระบบเข้ามาก็จะสามารถลบเมสเสจที่จะแจ้งให้ทราบเกี่ยวกับบุกรุกได้ทั้งหมด ซึ่งเซิร์ฟเวอร์ควรป้องกันโดยการติดตั้งชุดความปลอดภัยให้ทันต่อเหตุการณ์ปัจจุบันเสมอ

2.4 การปรับแต่งค่าคอนฟิกกูเรชันบนอุปกรณ์ CISCO

อุปกรณ์ของ CISCO เกือบทั้งหมดใช้โปรโตคอล syslog ในการจัดการล็อกของระบบและการแจ้งเตือน แต่มีข้อจำกัดที่ความจุของหน่วยเก็บข้อมูล ซึ่งมีวิธีแก้ไขดังนี้

- **Internal buffer** เป็นหน่วยความจำขนาดเล็กที่ใช้เก็บล็อกปัจจุบัน เมื่อมีการรีบูตระบบ ล็อกเหล่านี้ก็จะหายไป

- **Syslog** เป็นรูปแบบของ Unix syslog protocol เพื่อส่งล็อกไปยังหน่วยจัดเก็บภายนอก ซึ่งช่วยแก้ไขปัญหาหน่วยความจำที่จำกัดในตัวอุปกรณ์ได้ ซึ่งต้องมีการตั้งค่าในแต่ละตัวอุปกรณ์เพิ่มเติมโดยก่อนการปรับแต่งให้อุปกรณ์ทำการส่งล็อกออกมาภายนอก ควรตั้งค่าเวลาให้ถูกต้องก่อนตามเวลาที่ใช้งานจริง

2.4.1 การปรับแต่งค่าคอนฟิกกูเรชันสำหรับอุปกรณ์เราเตอร์

สำหรับอุปกรณ์เราเตอร์จะมีการตั้งค่าคอนฟิกกูเรชันดังนี้

ตารางที่ 2.3 การปรับแต่งค่าคอนฟิกกูเรชันสำหรับอุปกรณ์เราเตอร์

Step	Command	Purpose
1	Router# **configure terminal**	Enters global configuration mode.
2	Router(config)# **service timestamps** *type* **datetime** [*msec*] [*localtime*] [*show-timezone*]	Instructs the system to timestamp syslog messages; the options for the *type* keyword are **debug** and **log**.
3	Router(config)#**logging** *host*	Specifies the syslog server by IP address or host name; you can specify multiple servers.
4	Router(config)# **logging trap** *level*	Specifies the kind of messages, by severity level, to be sent to the syslog server. The default is informational and lower. The possible values for *level* are as follows: Emergency: **0** Alert: **1** Critical: **2**

ตารางที่ 2.3 (ต่อ)

Step	Command	Purpose
		Error: **3** Warning: **4** Notice: **5** Informational: **6** Debug: **7** Use the debug level with caution, because it can generate a large amount of syslog traffic in a busy network.
5	Router(config)# **logging facility** *facility-type*	Specifies the facility level used by the syslog messages; the default is **local7**. Possible values are **local0, local1, local2, local3, local4, local5, local6**, and **local7**.
6	Router(config)# **End**	Returns to privileged EXEC mode.
7	Router# **show logging**	Displays logging configuration.

ตัวอย่างการตั้งค่าเราเตอร์ให้ส่งเมสเสจไปยังเซิร์ฟเวอร์ไอพีแอดเดรส 192.168.0.30 เป็นดังนี้

Router-Dallas#

Router-Dallas#**config terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router-Dallas(config)#**logging 192.168.0.30**

Router-Dallas(config)#**service timestamps debug datetime localtime show-timezone msec**

Router-Dallas(config)#**service timestamps log datetime localtime show-timezone msec**

Router-Dallas(config)#**logging facility local3**

Router-Dallas(config)#**logging trap warning**

Router-Dallas(config)#**end**

Router-Dallas#**show logging**

Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)

Console logging: level debugging, 79 messages logged

Monitor logging: level debugging, 0 messages logged

Buffer logging: disabled

Trap logging: level warnings, 80 message lines logged

Logging to 192.168.0.30, 57 message lines logged

2.4.2 การปรับแต่งค่าคอนฟิกกูเรชันสำหรับอุปกรณ์สวิทช์

สำหรับอุปกรณ์สวิทช์ที่ทำงานบนระบบปฏิบัติการ CATOS นั้นจะมีการตั้งค่าคอนฟิกกูเรชันดังนี้

ตารางที่ 2.4 การปรับแต่งค่าคอนฟิกกูเรชันสำหรับอุปกรณ์สวิทช์

Step	Command	Purpose
1	Switch>**(enable) set logging timestamp {enable | disable}**	Configures the system to timestamp messages.
2	Switch>**(enable) set logging server ip-address**	Specifies the IP address of the syslog server; a maximum of three servers can be specified.
3	Switch>**(enable) set logging server severity server_severity_level**	Limits messages that are logged to the syslog servers by severity level.
4	Switch>**(enable) set logging server facility server_facility_parameter**	Specifies the facility level that would be used in the message. The default is local7. Apart from the standard facility names listed in Table 4-1, Cisco Catalyst switches use facility names that are specific to the switch. The following facility levels generate syslog messages with fixed severity levels: 5: System, Dynamic-Trunking-Protocol, Port-Aggregation-Protocol, Management, Multilayer

ตารางที่ 2.4 (ต่อ)

Step	Command	Purpose
		Switching 4: CDP, UDLD 2: Other facilities
5	Switch>**(enable) set logging server enable**	Enables the switch to send syslog messages to the syslog servers.
6	Switch>**(enable) Show logging**	Displays the logging configuration.

ตัวอย่างการตั้งค่าสวิทช์ให้ส่งเมสเสจไปยังเซิร์ฟเวอร์ไอพีแอดเดรส 192.168.0.30 เป็นดังนี้

Console> (enable) **set logging timestamp enable**

System logging messages timestamp will be enabled.

Console> (enable) **set logging server 192.168.0.30**

192.168.0.30 added to System logging server table.

Console> (enable) **set logging server facility local4**

System logging server facility set to <local4>

Console> (enable) **set logging server severity 4**

System logging server severity set to <4>

Console> (enable) **set logging server enable**

System logging messages will be sent to the configured syslog servers.

Console> (enable) **show logging**

Logging buffered size: 500

timestamp option: enabled

Logging history size: 1

Logging console: enabled

Logging server: enabled

{192.168.0.30}

server facility: LOCAL4

server severity: warnings(4)

2.4.3 การปรับแต่งค่าคอนฟิกกูเรชันสำหรับอุปกรณ์ไฟร์วอล

สำหรับอุปกรณ์ไฟร์วอล นั้นจะมีการตั้งค่าคอนฟิกกูเรชันดังนี้

ตารางที่ 2.5 การปรับแต่งค่าคอนฟิกกูเรชันสำหรับอุปกรณ์ไฟร์วอล

Step	Command	Purpose
1	Pixfirewall# **config terminal**	Enters global configuration mode.
2	Pixfirewall(config)#**logging timestamp**	Specifies that each syslog message should have a timestamp value.
3	Pixfirewall(config)#**logging host** [*interface connected to syslog server*] *ip_address* [*protocol / port*]	Specifies a syslog server that is to receive the messages sent from the Cisco PIX Firewall. You can use multiple **logging host** commands to specify additional servers that would all receive the syslog messages. The *protocol* is UDP or TCP. However, a server can only be specified to receive either UDP or TCP, not both. A Cisco PIX Firewall only sends TCP syslog messages to the Cisco PIX Firewall syslog server.
4	Pixfirewall(config)#**logging facility** *facility*	Specifies the syslog facility number. Instead of specifying the name, The default is **20**. the PIX uses a 2-digit number, as follows: local0 - **16** local1 - **17** local2 - **18** local3 - **19** local4 - **20** local5 - **21** local6 - **22** local7 - **23**

ตารางที่ 2.5 (ต่อ)

Step	Command	Purpose
5	pixfirewall(config)#**logging trap** *level*	Specifies the syslog message level as a number or string. The *level* that you specify means that you want that *level* and those values less than that *level*. For example, if *level* is **3**, syslog displays **0, 1, 2**, and **3** messages. Possible number and string *level* values are as follows: **0**: Emergency; System-unusable messages **1**: Alert; Take immediate action **2**: Critical; critical condition **3**: Error; error message **4**: Warning; warning message **5**: Notice; normal but significant condition **6**: Informational: information message **7**: Debug; debug messages and log FTP commands and WWW URLs
6	pixfirewall(config)#**logging on**	Starts sending syslog messages to all output locations.
7	pixfirewall(config)#**no logging message** <*message id*>	Specifies a message to be suppressed.
8	pixfirewall(config)#**exit**	Exits global configuration mode.

ตัวอย่างการตั้งค่าไฟร์วอลให้ส่งเมสเสจไปยังเซิร์ฟเวอร์ไอพีแอดเดรส 192.168.0.30 เป็นดังนี้

Firewall-Dallas#

Firewall-Dallas# **config terminal**

Firewall-Dallas(config)# **loggin time**

Firewall-Dallas(config)# **logging host 192.168.0.30**

Firewall-Dallas(config)# **logging facility 21**

Firewall-Dallas(config)# **logging trap 7**

Firewall-Dallas(config)# **logging on**

Firewall-Dallas(config)# **no logging message 111005**

rewall-Dallas(config)# **exit**

Firewall-Dallas# **show logging**

Syslog logging: enabled

Facility: 21

Timestamp logging: enabled

Standby logging: disabled

Console logging: disabled

Monitor logging: disabled

Buffer logging: disabled

Trap logging: level debugging, 6 messages logged

Logging to inside 192.168.0.30

History logging: disabled

Device ID: disabled

2.5 Regular expression

Regular expression เป็นการกรอง (filter) ข้อมูลหรือกำหนดรูปแบบเพื่อการค้นหาข้อความหรือตัวอักษรว่ามีอยู่ในข้อความที่กำหนดหรือไม่ เช่น ตรวจสอบข้อความที่มีคนกรอกแบบฟอร์มเข้ามาบนเว็บ ก็จะใช้ Regular expression เป็นตัวตรวจสอบ นอกจากจะใช้ตรวจสอบแล้ว ยังสั่งแก้ได้อีกด้วย เช่น จะแก้คำว่า ประสิทธิ์ เป็นคำว่า ประสาท โดยไม่ต้องไปค้นหาเอง แต่สั่งให้โปรแกรมค้นหา โดยใช้ Regular expression แล้วแทนที่คำคำนั้น ด้วยคำที่ต้องการ

ถ้านึกถึงโปรแกรมพิมพ์เอกสาร ที่มีฟังก์ชั่นให้สามารถค้นและแก้ไขคำที่พิมพ์โดยการสั่ง replace ก็พอจะเข้าใจแนวคิดของ Regular expression แล้ว เพียงแต่ว่า Regular expression มีความสามารถมากกว่านั้น นักเขียนโปรแกรมบนเว็บส่วนมากใช้ Regular expression เพื่อตรวจสอบอีเมลเบื้องต้น ว่า ผู้ใช้พิมพ์อีเมลเข้ามาถูกรูปแบบหรือไม่ บางครั้งก็ใช้ในการตรวจสอบรูปแบบ เช่น หมายเลขประจำตัวนักศึกษา ซึ่งมีรูปแบบแน่นอน ถ้าพิมพ์มาไม่ถูกรูปแบบก็แสดงว่าพิมพ์ผิด เป็น

ต้นและที่ใช้กันบ่อยมากบนเว็บก็คือ การตรวจสอบข้อมูลบนฟอร์ม Regular expression ใช้ง่าย และทำให้ขนาดของโปรแกรมสั้นลง สัญลักษณ์ของ Regular expression สรุปได้ดังนี้

ตารางที่ 2.6 สัญลักษณ์ของ Regular expression

สัญลักษณ์	ความหมาย
^	คำ/อักษรที่อยู่หน้าเครื่องหมายนี้ ต้องเป็นคำขึ้นต้นของข้อความที่นำมาตรวจสอบเช่น "^การ" เป็นการกำหนดว่า คำที่นำมาตรวจสอบต้องขึ้นต้นด้วยคำว่า การ เช่น "การทำดี" "การบ้าน" เป็นต้น คำพวกนี้จะผ่านการทดสอบ
$	คำ/อักษรที่อยู่หน้าเครื่องหมายนี้ ต้องอยู่ตอนท้ายของข้อความที่นำมาตรวจสอบ เช่น "มา$" จะถือว่าคำต่อไปนี้ถูกตามเงื่อนไข "ตามา" "ขอขมา" หรือแม้แต่คำว่า "หมา" แต่คำว่า "ทำดี" จะไม่ผ่านเพราะไม่ได้ลงท้ายด้วยคำว่า "มา" ตามเงื่อนไขนั่นเอง
+	คำ/อักษรที่อยู่หน้าเครื่องหมายนี้ ต้องมีปรากฏในคำที่นำมาตรวจสอบ อย่างน้อย 1 ตัว เช่น "ท+" จะถือว่าคำต่อไปนี้ผ่านการตรวจสอบ เช่น "ทองจุล" "วันทนา" "ถนนหนทางทุกแห่ง"
?	คำ/อักษรที่อยู่หน้าเครื่องหมายนี้ อาจจะมีปรากฏในคำที่นำมาตรวจสอบ หรือไม่ก็ได้ ถ้ามีจะมีกี่ตัวก็ได้ "ก?ข+$" หมายถึง อาจจะมีด้วยตัว ก และอักษรตัวสุดท้ายต้องมีตัว ข อย่างน้อย 1 ตัว (เครื่องหมาย + แสดงว่ามีอย่างน้อย 1 และเครื่องหมาย $ แสดงว่าเป็นตัวสุดท้าย)
*	เหมือนกับ ?
\s	ช่องว่าง หรือ whitespace
.	ใช้แทนตัวอักษรอะไรก็ได้ · "ก.[0-9]" หมายถึง ตัว ก ตามด้วยตัวอักษรอะไรก็ได้ และต่อด้วยเลขอารบิค เลข 0-9 · "^.{3}$" หมายถึง ต้องมีตัวอักษรเพียง 3 ตัวเท่านั้น เป็นตัวเลข ตัวอักษร ภาษาไทย ภาษาอังกฤษ ได้ทั้งนั้น

ตารางที่ 2.6 (ต่อ)

สัญลักษณ์	ความหมาย
[ ]	ใช้ระบุตำแหน่งในคำว่า ในตำแหน่งนี้จะมีตัวอักษรอะไรได้บ้าง เช่น "[นร]" เป็นการกำหนดว่า คำที่นำมาตรวจสอบ ต้องเป็นตัว น หรือ ตัว ร เท่านั้นจึงจะผ่าน มีความหมายเช่นเดียวกับ "น|ร" "[ก-ค]" เป็นการบอกว่า คำที่นำมาจะต้องเป็น ตัว ก ข ค เท่านั้น เช่น ในกรณีเลขประจำตัวที่ขึ้นต้นด้วย ก ข หรือ ค เท่านั้น ถ้าพิมพ์ตัวแรกเป็นตัวอักษรตัวอื่นก็แสดงว่าพิมพ์ผิด เราจะเขียนได้ดังนี้ ^[ก-ค] "^[a-zA-Z]" เป็นการบอกว่า คำที่นำมาตรวจสอบต้องขึ้นต้นด้วยตัวอักษร จะเป็นตัวเล็ก คือ a ถึง z หรือ ตัวใหญ่ คือ A ถึง Z ก็ได้ "[0-9๐-๙]%" เป็นการบอกว่า ให้มีตัวเลข 1 ตัว เลขอะไรก็ได้ เลข 0 ถึง เลข 9 เป็นได้ทั้งเลขไทยและอารบิค ต่อด้วยเครื่องหมาย % [ก-ฮ] ตัว ก ถึง ฮ รวมทั้งสระทุกตัว และ ตัวเลขไทย ๐ ถึง ๙ [0-9๐-๙] เลข 0-9 ทั้งเลขไทยและฝรั่ง ^[0-9๐-๙]+$ ให้มีเฉพาะตัวเลข 0-9 เลขไทยหรือเลขฝรั่งก็ได้ แต่ห้ามมีตัวอักษรใด ๆ "^[กข]{3}[-][0-9]$" ขึ้นต้นด้วยตัว ก หรือ ข จำนวน 3 ตัว ต่อด้วยเครื่องหมาย – และจบด้วยตัวเลขอารบิค เลข 0-9 เช่น "กขก-5" "กกก-3" เป็นต้น สิ่งต่อไปนี้จะไม่ผ่านหรือเป็นเท็จ เช่น "กกกขข" เพราะ ตัวที่ 4 ไม่ใช้เครื่องหมาย – และตัวสุดท้ายไม่ใช่ตัวเลข "ขขข-๘" ตัวเลขสุดท้ายเป็นเลขไทย ไม่ว่าตัวอักษร หรือสัญลักษณ์ใด ๆ ที่อยู่ภายในเครื่องหมาย [ ] จะกลายเป็นสัญลักษณ์ธรรมดา เช่น + กลายเป็นเครื่องหมายบวก แทนที่จะหมายถึงว่า ต้องมีตัวอักษรอย่างน้อย 1 ตัว
{ }	แสดงจำนวนครั้งที่ซ้ำกัน เช่น "กข{2}" หมายถึงให้มีตัว ข จำนวน 2 ตัว เช่น "กขข" "กข{2,} หมายถึงให้มีตัว ข อย่างน้อย 2 ตัว เช่น "กขขขข" "กข{3,5} หมายถึงให้มีตัว ข จำนวน 3-5 ตัวเท่านั้น คือ "กขขข" "กขขขข" และ "กขขขขข"

ตารางที่ 2.6 (ต่อ)

สัญลักษณ์	ความหมาย
( )	ใช้รวมกลุ่มเข้าด้วยกันเป็นส่วนเดียวกัน เช่น “ก(ขค)*” หมายถึง ตัว ก และอาจจะตามด้วยตัว ขค หรือไม่มีตัว ขค ก็ได้ เครื่องหมาย * แสดงว่าจะมีหรือไม่ก็ได้ “ก(ขค){1,5}” หมายถึง ตัว ก แล้วจะตามด้วย ขค จำนวน 1-5 ชุด เช่น “กขคขคขค” หรือ “กขคขค” ก็ได้
|	เสนอทางเลือกอย่างใดอย่างหนึ่ง เช่น “การ|ความ” เป็นการบอกว่า จะใช้คำว่า การ หรือ ความ ก็ได้ “(ก|ขค)งจ” เช่น กงจ หรือ ขคงจ ก็ได้
^[1-9][0-9]*$	ขึ้นต้นด้วยเลข 1-9 และอาจจะต่อด้วย เลข 0-9 กี่ตัวก็ได้ ในกรณีนี้ ถ้าเป็นเลข 0 ก็จะไม่ผ่าน จะผ่านตั้งแต่ 1 2 3 4 ไปเรื่อย ๆ
^(0|[1-9][0-9]*)$	อาจจะขึ้นต้นด้วยเลข 0 หรือเลข 1-9 ก็ได้ และอาจจะต่อด้วยเลข 0-9 ในกรณีนี้ เราใช้ตรวจสอบการพิมพ์ที่เป็นตัวเลขตั้งแต่ 0 ขึ้นไป ถ้ามีตัวอักษร ก็จะไม่ผ่านการตรวจสอบ หรือ เป็นเท็จ นั่นเอง
^(0|-?[1-9][0-9]*)$	เหมือน ^(0|[1-9][0-9]*)$ เพียงแต่ ถ้าไม่ขึ้นต้นด้วยเลข 0 สามารถมีเครื่องหมาย ลบ ได้ หรือจะไม่มีเครื่องหมายลบ ก็ได้ เครื่องหมาย ? แสดงว่า จะมีหรือไม่มี ก็ได้
^[0-9]+(\.[0-9]+)?$	ขึ้นต้นด้วย 0-9 อย่างน้อย 1 ตัว และอาจจะมี จุดและต่อด้วยตัวเลข 0-9 อย่างน้อย 1 ตัว อย่างนี้ เป็นการบอกว่าจะทศนิยมหรือไม่มีก็ได้ (สังเกตเครื่องหมาย ? อยู่หลังกลุ่มทั้งหมดซึ่งอยู่ในวงเล็บ เป็นการบอกว่า กลุ่มนี้ คือ (\.[0-9]+) จะมีหรือไม่มีก็ได้) แต่จะมีแค่ จุดเฉย ๆ เช่น 15. อย่างนี้ไม่ได้ ต้องเป็น 15.2 หรือ 15.38 ก็ได้ (เพราะเครื่องหมาย + อยู่หลัง [0-9] แสดงว่า ตำแหน่งนี้ คือต่อจาก จุด ยังไง ๆ ก็ต้องมีตัวเลข 0 ถึง 9 อย่างน้อย 1 ตัว จะเป็น 2 ตัว 5 ตัว 10 ตัว ก็ได้)
^[0-9]+(\.[0-9]{2})?$	เหมือนข้างบน แต่บังคับว่า ถ้ามีทศนิยม ทศนิยมต้องมี 2 ตำแหน่ง เท่านั้น เครื่องหมาย {} กำหนดว่าจะต้องมีซ้ำกี่ครั้ง
^[0-9]+(\.[0-9]{1,2})?$	เหมือนข้างบน แต่อนุญาตให้มีทศนิยม 1 หรือ 2 ตำแหน่ง สังเกตการเขียนตัวเลข ในระหว่างเครื่องหมาย { และ }

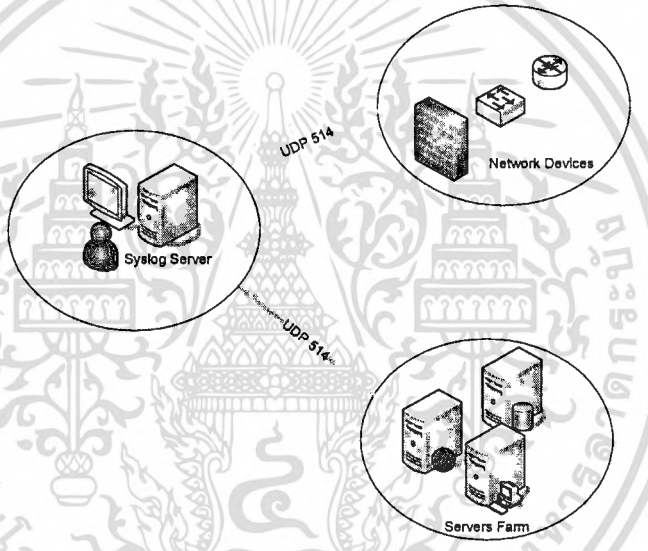
ตารางที่ 2.6 (ต่อ)

สัญลักษณ์	ความหมาย
^[0-9]{1,3}(,[0-9]{3})*(\.[0-9]{1,2})?$	ต้องขึ้นต้นด้วยตัวเลข 0-9 หรือ อาจจะตามด้วยเครื่องหมาย คอมม่า และตัวเลข 0-9 อีก 3 ตัว และอาจจะต่อด้วยทศนิยม 1 หรือ 2 ตำแหน่ง
^([0-9]+|[0-9]{1,3}(,[0-9]{3})*)(\.[0-9]{1,2})?$	เหมือนข้างบน แต่กำหนดให้การมีเครื่องหมาย คอมม่า อาจจะมีหรือไม่มีก็ได้ วิธีกำหนดทางเลือกใช้เครื่องหมาย | แทนที่จะใช้ ? การเลือกใช้ต้องอยู่ที่เราจะตัดสินใจว่าจะเลือกใช้อะไรจึงจะเหมาะสม นี่แหละเสน่ห์ของการเขียนโปรแกรม มีวิธีการหลายอย่างที่จะได้มาซึ่งผลลัพธ์อย่างเดียวกัน แต่อย่างไหนจะเหมาะ ต้องเลือกดู เลือกใช้ให้เหมาะสม

บทที่ 3

การวิเคราะห์และออกแบบระบบงาน

ในระบบงานที่จะทำการพัฒนาในโครงงานก็จะประกอบไปด้วยสองส่วน โดยจะแบ่งการทำงานออกเป็น ส่วนที่ทำหน้าที่รอรับฟังข้อมูลผ่านพอร์ตยูดีพี 514 และจัดเก็บลงฐานข้อมูล และส่วนที่ทำหน้าที่รวบรวมข้อมูลจากฐานข้อมูลที่มีอยู่มาแสดงผลและทำรายงานสรุปผลสำหรับให้ผู้ดูแลระบบเรียกดูข้อมูลตามที่ต้องการได้

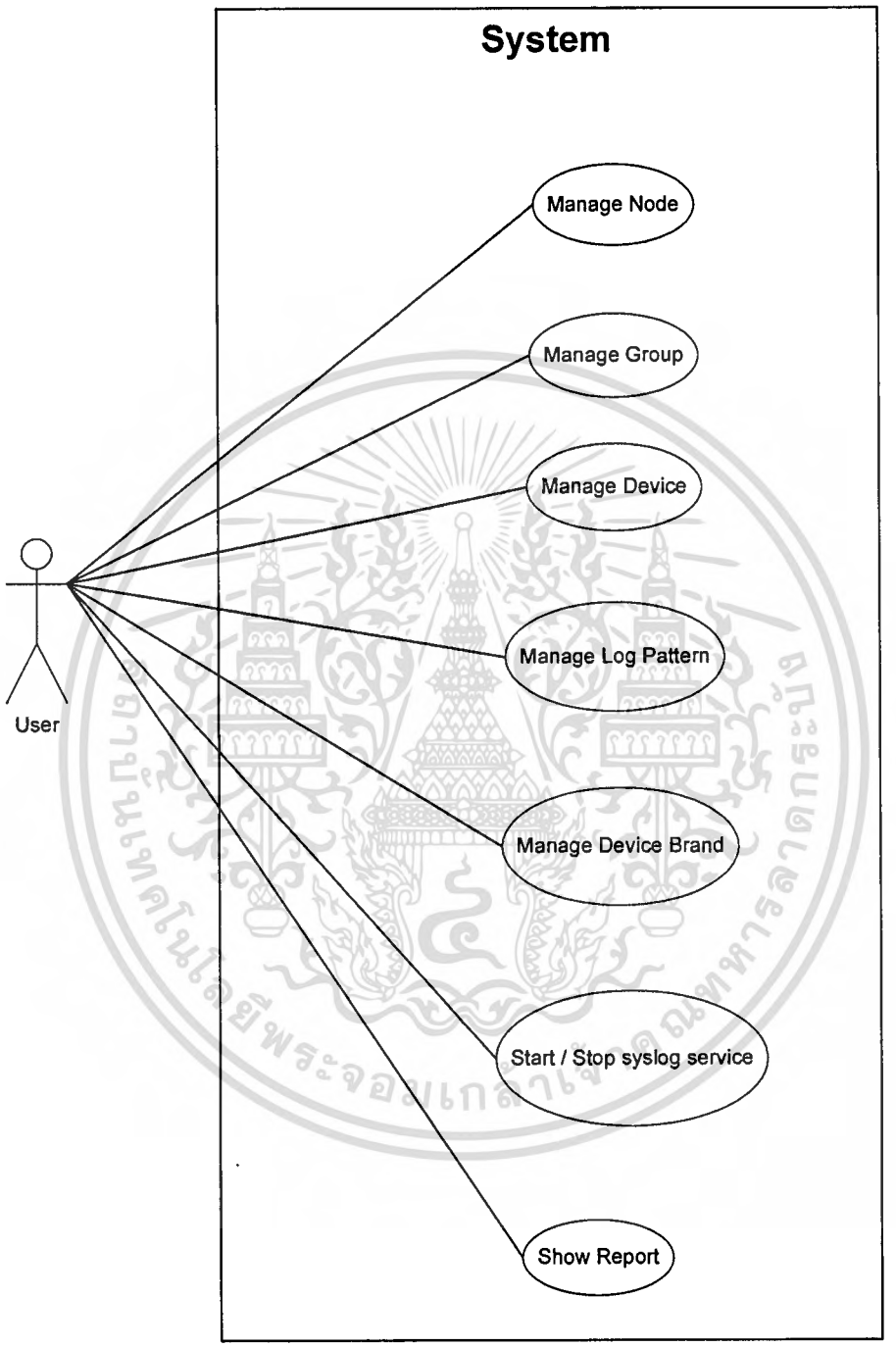


รูปที่ 3.1 โปรแกรมจัดเก็บและช่วยวิเคราะห์ข้อมูลล็อก

3.1 การออกแบบระบบ

การวิเคราะห์และการออกแบบที่ดีจะช่วยให้การสร้างระบบเป็นไปได้อย่างรวดเร็วและตรงตามความต้องการ ดังนั้นการวิเคราะห์และการออกแบบระบบ จึงนับเป็นส่วนสำคัญอย่างยิ่งอีกส่วนหนึ่งในการพัฒนาระบบงาน ในโครงงานนี้จะใช้ภาษา UML ซึ่งเป็นภาษาที่ช่วยสร้างไดอะแกรมต่างๆในการออกแบบระบบ มาช่วยทำให้การออกแบบระบบมีมาตรฐานและง่ายต่อความเข้าใจของผู้พัฒนาระบบต่อๆไปอีก ด้วย

3.1.1 ออกแบบโครงสร้าง จะทำการออกแบบโครงสร้างของระบบว่าประกอบด้วยส่วนใดบ้างแต่ละส่วนแบ่งเป็นคลาสย่อย ๆ ใดบ้าง และสร้างคลาสต่างๆ ขึ้นเพื่อช่วยในการทำความเข้าใจระบบ โดยในส่วนของ Use Case Diagram จะแบ่งดังนี้



รูปที่ 3.2 ยูสเคสโปรแกรมจัดเก็บและช่วยวิเคราะห์ข้อมูลล็อก

1. Manage Node เป็นฟังก์ชันที่ทำหน้าที่เพิ่ม ลบ แก้ไขข้อมูลของผู้ใช้งานระบบแต่ละคน เพื่อจัดเก็บลงฐานข้อมูล รายละเอียดแสดงดังตารางที่ 3.1

ตารางที่ 3.1 รายละเอียดของยูสเคส Manage Node

Use case	Manage Node	ID : 01
Primary actor	User	
รายละเอียดโดยย่อ	เพิ่ม ลบ แก้ไขข้อมูลของโหนดแต่ละโหนดเพื่อจัดเก็บลงฐานข้อมูล	
ความสัมพันธ์	Association : User	
ลำดับเหตุการณ์	1. ผู้ใช้งานเลือกเพิ่ม ลบ หรือแก้ไขข้อมูลโหนด 2. ตรวจสอบรายการโหนดที่มีอยู่ 3. ทำการเพิ่ม ลบ หรือแก้ไขข้อมูลโหนด	

2. Manage Group เป็นฟังก์ชันที่ใช้สำหรับที่ทำหน้าที่เพิ่ม ลบ แก้ไขข้อมูลของกลุ่มของกลุ่มอุปกรณ์ รายละเอียดแสดงดังตารางที่ 3.2

ตารางที่ 3.2 รายละเอียดของยูสเคส Manage Group

Use case	Manage Group	ID : 02
Primary actor	User	
รายละเอียดโดยย่อ	เพิ่ม ลบ แก้ไขข้อมูลของกลุ่มอุปกรณ์เพื่อจัดเก็บลงฐานข้อมูล	
ความสัมพันธ์	Association : User	
ลำดับเหตุการณ์	1. ผู้ใช้งานเลือกเพิ่ม ลบ หรือแก้ไขข้อมูลกลุ่มของโหนด 2. ตรวจสอบรายการกลุ่มของโหนดที่มีอยู่ 3. ทำการเพิ่ม ลบ หรือแก้ไขข้อมูลกลุ่มของโหนด	

3. Manage Device เป็นฟังก์ชันที่ใช้สำหรับที่ทำหน้าที่เพิ่ม ลบ แก้ไขข้อมูลของชนิดอุปกรณ์ รายละเอียดแสดงดังตารางที่ 3.3

ตารางที่ 3.3 รายละเอียดของยูสเคส Manage Device

Use case	Manage Device	ID : 03
Primary actor	User	
รายละเอียดโดยย่อ	เพิ่ม ลบ แก้ไขข้อมูลของอุปกรณ์แต่ละตัวเพื่อจัดเก็บลงฐานข้อมูล	
ความสัมพันธ์	Association : User	
ลำดับเหตุการณ์	1. ผู้ใช้งานเลือกเพิ่ม ลบ หรือแก้ไขข้อมูลชนิดอุปกรณ์ 2. ตรวจสอบรายการชนิดอุปกรณ์ที่มีอยู่ 3. ทำการเพิ่ม ลบ หรือแก้ไขข้อมูลชนิดอุปกรณ์	

4. Manage Log Pattern เป็นฟังก์ชันที่ใช้สำหรับที่ทำหน้าที่เพิ่ม ลบ แก้ไขข้อมูลของชนิดอุปกรณ์ รายละเอียดแสดงดังตารางที่ 3.4

ตารางที่ 3.4 รายละเอียดของยูสเคส Manage Log Pattern

Use case	Manage Log Pattern	ID : 04
Primary actor	User	
รายละเอียดโดยย่อ	เพิ่ม ลบ แก้ไขข้อมูลของรูปแบบล็อกเพื่อจัดเก็บลงฐานข้อมูล	
ความสัมพันธ์	Association : User	
ลำดับเหตุการณ์	1. ผู้ใช้งานเลือกเพิ่ม ลบ หรือแก้ไขรูปแบบล็อก 2. ตรวจสอบรายการรูปแบบล็อกที่มีอยู่ 3. ทำการเพิ่ม ลบ หรือแก้ไขข้อมูลรูปแบบล็อก	

5. Manage Device Brand เป็นฟังก์ชันที่ใช้สำหรับที่ทำหน้าที่เพิ่ม ลบ แก้ไขข้อมูลของชนิดอุปกรณ์ รายละเอียดแสดงดังตารางที่ 3.5

ตารางที่ 3.5 รายละเอียดของยูสเคส Manage Device Brand

Use case	Manage Device Brand	ID : 05
Primary actor	User	
รายละเอียดโดยย่อ	เพิ่ม ลบ แก้ไขข้อมูลของยี่ห้ออุปกรณ์เพื่อจัดเก็บลงฐานข้อมูล	
ความสัมพันธ์	Association : User	
ลำดับเหตุการณ์	1. ผู้ใช้งานเลือกเพิ่ม ลบ หรือแก้ไขยี่ห้ออุปกรณ์ 2. ตรวจสอบรายการยี่ห้ออุปกรณ์ที่มีอยู่ 3. ทำการเพิ่ม ลบ หรือแก้ไขข้อมูลยี่ห้ออุปกรณ์	

6. Manage Log Pattern เป็นฟังก์ชันที่ใช้สำหรับที่ทำหน้าที่เพิ่ม ลบ แก้ไขข้อมูลของชนิดอุปกรณ์ รายละเอียดแสดงดังตารางที่ 3.6

ตารางที่ 3.6 รายละเอียดของยูสเคส Start / Stop syslog service

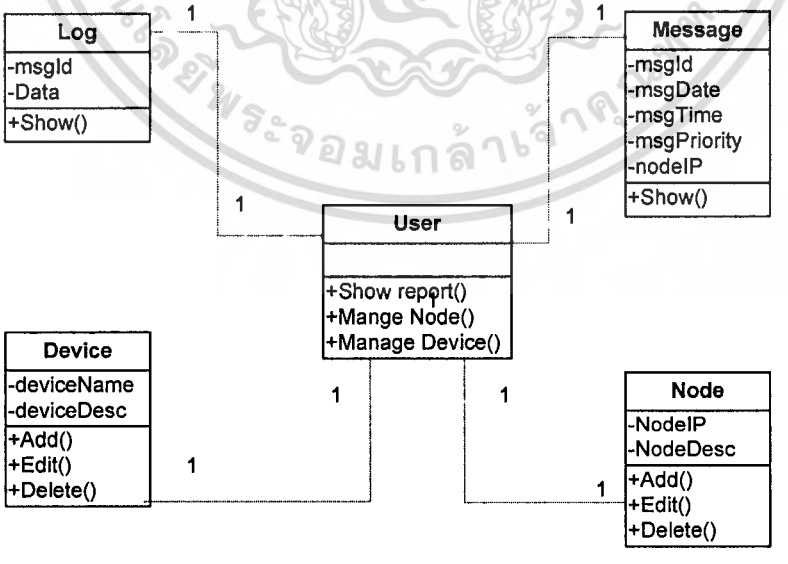
Use case	Start / Stop syslog service	ID : 06
Primary actor	User	
รายละเอียดโดยย่อ	สั่ง เริ่มทำงาน / ยกเลิกการทำงานของการเก็บข้อมูลล็อก	
ความสัมพันธ์	Association : User	
ลำดับเหตุการณ์	1. ผู้ใช้งานเลือกคำสั่ง เริ่มทำงาน / ยกเลิกการทำงาน 2. ระบบทำการเริ่มทำงาน / ยกเลิกการทำงาน	

7. Show Report เป็นฟังก์ชันที่ใช้สำหรับที่ทำหน้าที่เพิ่ม ลบ แก้ไขข้อมูลของชนิดอุปกรณ์ รายละเอียดแสดงดังตารางที่ 3.7

ตารางที่ 3.7 รายละเอียดของยูสเคส Show Report

Use case	Show Report	ID : 07
Primary actor	User	
รายละเอียดโดยย่อ	แสดงข้อมูลในรูปแบบรายงานตามเงื่อนไขที่ระบุ	
ความสัมพันธ์	Association : User	
ลำดับเหตุการณ์	1. ผู้ใช้งานเลือกแสดงผลข้อมูล 2. ดึงข้อมูลจากฐานข้อมูลตามเงื่อนไขที่ระบุ 3. แสดงผลข้อมูล	

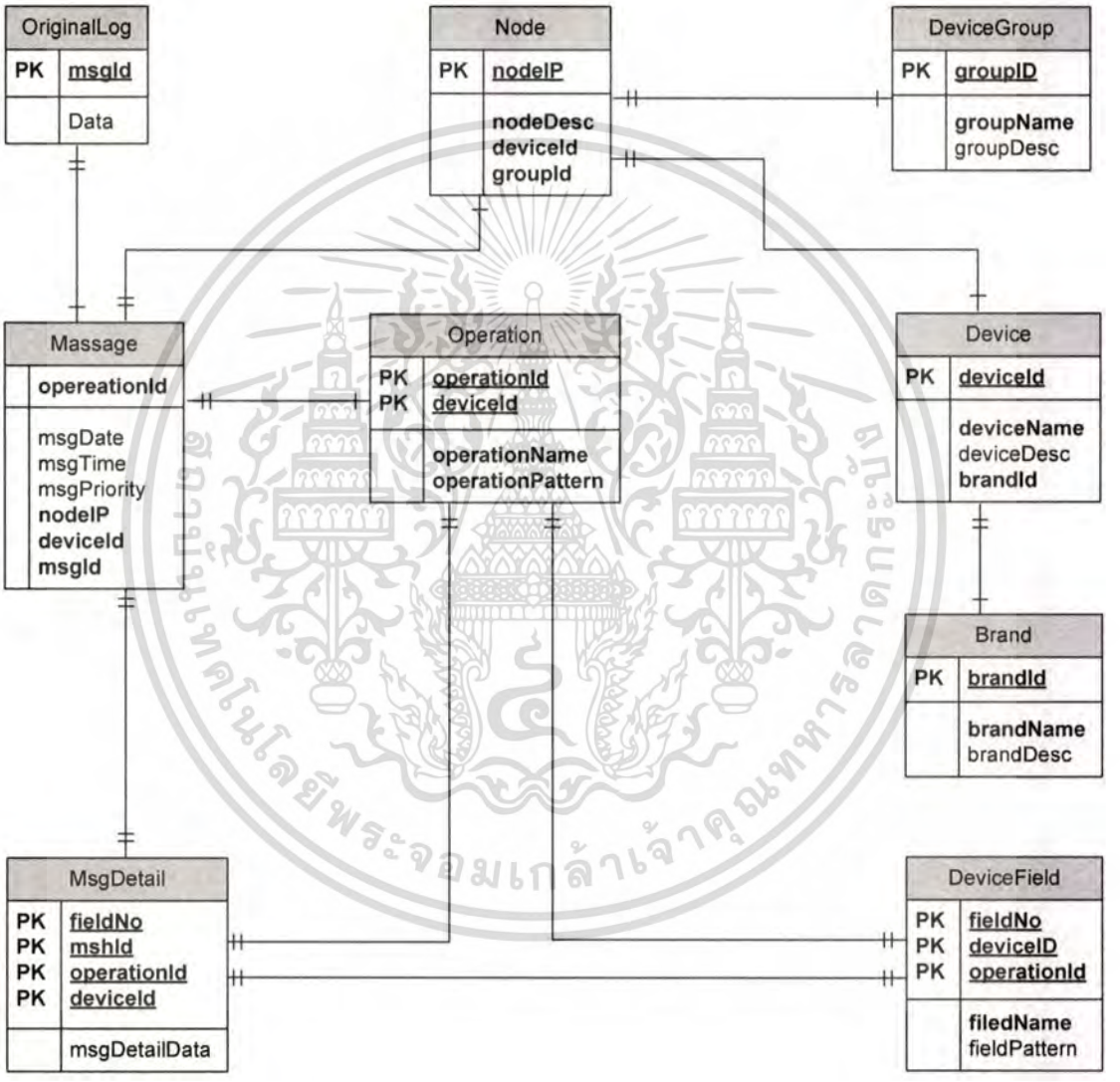
3.1.2 ออกแบบรายละเอียดของแต่ละคลาส จะแบ่งซอฟแวร์ออกเป็นคลาสย่อยๆ และทำการออกแบบแต่ละคลาสตามหลักอ็อบเจคโดยออกแบบบริการต่าง ๆ รวมถึงการอินเทอร์เฟสระหว่างคลาสด้วย



รูปที่ 3.3 คลาสไดอะแกรมของโปรแกรมจัดเก็บและช่วยวิเคราะห์ข้อมูลล็อก

3.1.3 แผนภาพแสดงการออกแบบฐานข้อมูลเชิงสัมพันธ์ (Entity Relationship Diagram)

แสดงแผนภาพความสัมพันธ์ของแต่ละเอ็นติตี้ในฐานข้อมูล ซึ่งทำการแปลงจากคลาสไดอะแกรมมาในรูปแบบหนึ่งต่อหนึ่ง และเพิ่มเติมตารางที่จำเป็นเข้าไปด้วยจะประกอบไปด้วย 9 เอ็นติตี้ได้แก่ Operation, DeviceField, DeviceGroup, Node , Brand, Device, OriginalLog, Message, MsgDetail



รูปที่ 3.4 แผนภาพแสดงการออกแบบฐานข้อมูลเชิงสัมพันธ์ (Entity Relationship Diagram)

3.2 พจนานุกรมข้อมูล

ตารางที่ 3.8 รายละเอียดของตาราง Operation

Table Name: Operation **Table Description:**						
เลขที่	**ชื่อฟิลด์**	**รายละเอียด**	**ประเภท**	**ค่าว่าง**	**ชนิดคีย์**	**ตารางที่อ้างถึง**
1.	deviceId	รหัสอุปกรณ์	Integer	not null	PK	DeviceFi
2.	OperationId	รหัสเหตุการณ์	Integer	not null	PK	eld
3.	operationName	ชื่อของเหตุการณ์	Text	not null	-	
4.	operationPattern	รูปแบบเหตุการณ์	Text	not null	-	

ตารางที่ 3.9 รายละเอียดของตาราง DeviceField

Table Name: DeviceField **Table Description:** เก็บข้อมูล						
เลขที่	**ชื่อฟิลด์**	**รายละเอียด**	**ประเภท**	**ค่าว่าง**	**ชนิดคีย์**	**ตารางที่อ้างถึง**
1.	deviceId	รหัสอุปกรณ์	Integer	not null	PK,FK	Operation,
2.	operationId	รหัสเหตุการณ์	Integer	not null	FK	Device
3.	fieldNo	เลขลำดับของฟิลด์ข้อมูล	Integer	not null		
4.	fieldname	ชื่อฟิลด์ข้อมูล	Text	not null		
5.	fieldPattern	รูปแบบฟิลด์ข้อมูล	Text	-		

ตารางที่ 3.10 รายละเอียดของตาราง DeviceGroup

Table Name: DeviceGroup **Table Description:** เก็บข้อมูล						
เลขที่	**ชื่อฟิลด์**	**รายละเอียด**	**ประเภท**	**ค่าว่าง**	**ชนิดคีย์**	**ตารางที่อ้างถึง**
1.	groupId	รหัสกลุ่มอุปกรณ์	Integer	not null	PK,FK	Node
2.	groupName	ชื่อกลุ่มอุปกรณ์	Text	not null	PK	
3.	groupDesc	รายละเอียดกลุ่มอุปกรณ์	Text	-		

ตารางที่ 3.11 รายละเอียดของตาราง Node

Table Name: Node **Table Description:** เก็บข้อมูล						
เลขที่	**ชื่อฟิลด์**	**รายละเอียด**	**ประเภท**	**ค่าว่าง**	**ชนิดคีย์**	**ตารางที่อ้างถึง**
1.	nodeIP	ไอพีแอดเดรสของโหนด	Text	not null	PK	
2.	nodeDesc	รายละเอียดของโหนด	Text	not null		
3.	deviceId	รหัสอุปกรณ์	Interger	not null		
4.	groupId	รหัสกลุ่มอุปกรณ์	Integer	not null		

ตารางที่ 3.12 รายละเอียดของตาราง Device

Table Name: Device **Table Description:** เก็บข้อมูล						
เลขที่	**ชื่อฟิลด์**	**รายละเอียด**	**ประเภท**	**ค่าว่าง**	**ชนิดคีย์**	**ตารางที่อ้างถึง**
1.	deviceId	รหัสอุปกรณ์	Integer	not null	PK	
2.	deviceName	ชื่ออุปกรณ์	Text	not null		
3.	deviceDesc	รายละเอียดอุปกรณ์	Text	-		
4.	brandId	ยี่ห้ออุปกรณ์	Integer	not null	FK	Brand

ตารางที่ 3.13 รายละเอียดของตาราง Brand

Table Name: Brand **Table Description:** เก็บข้อมูล						
No.	**Field**	**Contents**	**Type**	**Null**	**Key**	**Default**
1.	brandId	รหัสยี่ห้ออุปกรณ์	Interger	not null	PK	
2.	brandName	ยี่ห้ออุปกรณ์	Text	not null		
3.	brandDesc	รายละเอียดยี่ห้ออุปกรณ์	Text	-		

ตารางที่ 3.14 รายละเอียดของตาราง OriginalLog

Table Name: OriginalLog **Table Description:** เก็บข้อมูล						
เลขที่	**ชื่อฟิลด์**	**รายละเอียด**	**ประเภท**	**ค่าว่าง**	**ชนิดคีย์**	**ตารางที่อ้างถึง**
1.	msgId	รหัสข้อความ	Text	not null	PK,FK	Message
2.	Data	รายละเอียดข้อความ	Text	not null		

ตารางที่ 3.15 รายละเอียดของตาราง Message

Table Name: Message **Table Description:** เก็บข้อมูล						
เลขที่	**ชื่อฟิลด์**	**รายละเอียด**	**ประเภท**	**ค่าว่าง**	**ชนิดคีย์**	**ตารางที่อ้างถึง**
1.	operationId	รหัสเหตุการณ์	Text	not null	PK	
2.	msgDate	วันที่เกิดเหตุการณ์	Date/Time	not null		
3.	msgTime	เวลาที่เกิดเหตุการณ์	Date/Time	not null		
4.	msgPriority	ลำดับความสำคัญเหตุการณ์	Integer	not null		
5.	nodeIP	ไอพีแอดเดรสของโหนด	Text	not null		
6.	deviceId	รหัสอุปกรณ์	Interger	not null		
7.	msgId	รหัสข้อความ	Text	not null		

ตารางที่ 3.16 รายละเอียดของตาราง MsgDetail

Table Name: MsgDetail **Table Description:** เก็บข้อมูล						
เลขที่	**ชื่อฟิลด์**	**รายละเอียด**	**ประเภท**	**ค่าว่าง**	**ชนิดคีย์**	**ตารางที่อ้างถึง**
1.	fieldNo	เลขที่ฟิลด์ข้อมูล	Integer	not null	PK	
2.	msgId	รหัสข้อความ	Text	not null	PK	
3.	operationId	รหัสเหตุการณ์	Integer	not null	PK	
4.	deviceId	รหัสอุปกรณ์	Integer	not null	PK	
5.	msgDeviceData	รายละเอียดของเมสเสจ	Text	-		

3.3 สิ่งแวดล้อมที่ใช้พัฒนาระบบ

สิ่งแวดล้อมที่ใช้พัฒนาระบบได้แก่

ตารางที่ 3.17 รายละเอียดของสิ่งแวดล้อมที่ใช้พัฒนาระบบ

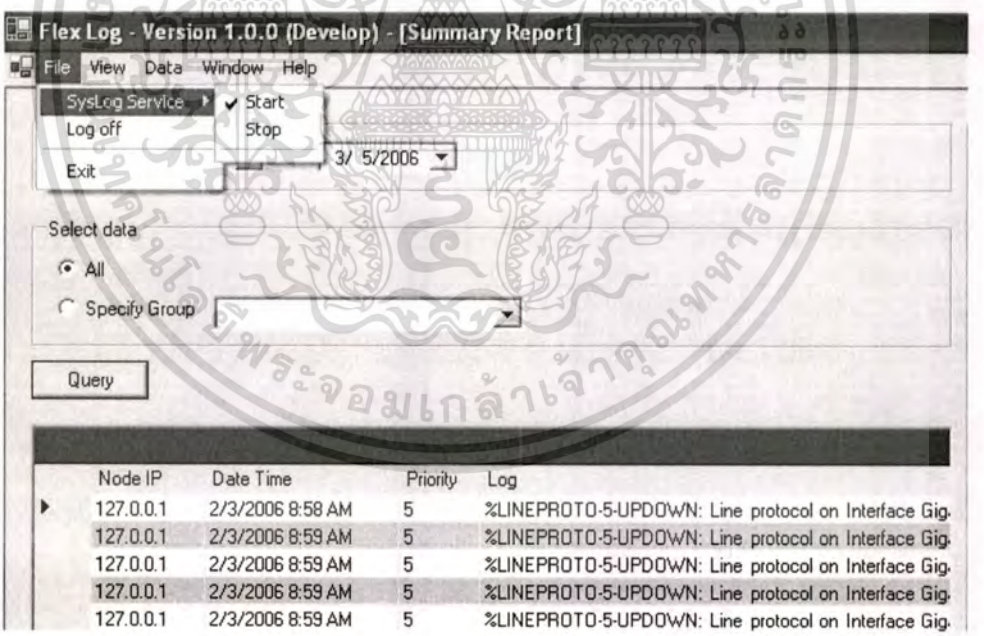
หน่วยพัฒนา	โปรแกรม
Enhanced Syslog Analyzer Tool	Microsoft Windows XP service pack 2 Microsoft Visual Studio .NET 2003 (VB.NET) Microsoft Access

บทที่ 4
ผลการพัฒนาระบบ

ส่วนการทำงานของโปรแกรมจะแยกออกเป็นสามระบบหลักได้แก่ส่วนการเข้าสู่เมนูหลัก ส่วนการแสดงผลข้อมูล และ การจัดการข้อมูลในฐานข้อมูล ซึ่งแต่ละส่วนได้มีการออกแบบหน้าจอการแสดงผลตามความเหมาะสม

4.1 ส่วนการเข้าสู่เมนูหลัก

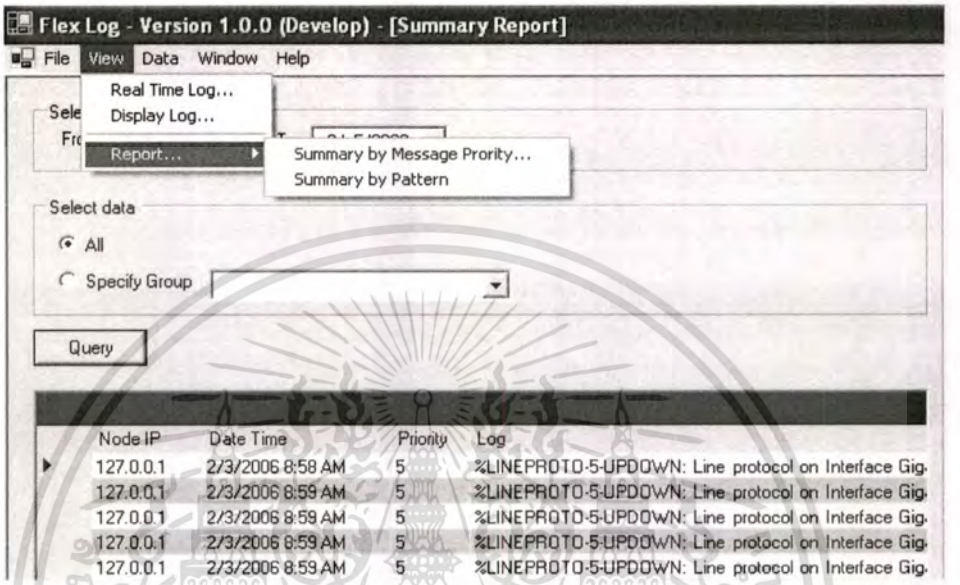
เมื่อเข้าสู่โปรแกรมจะต้องผ่านหน้าต่างการตรวจสอบสิทธิ์ผู้ใช้งานก่อน และเมื่อเข้าสู่เมนูหลักจะสามารถเลือกให้เริ่มหรือทำการเก็บล็อกได้ โดยการทำงานปกติ เมื่อเปิดโปรแกรมขึ้นมานั้น โปรแกรมจะทำการสั่งเริ่มเก็บข้อมูลล็อกในทันที



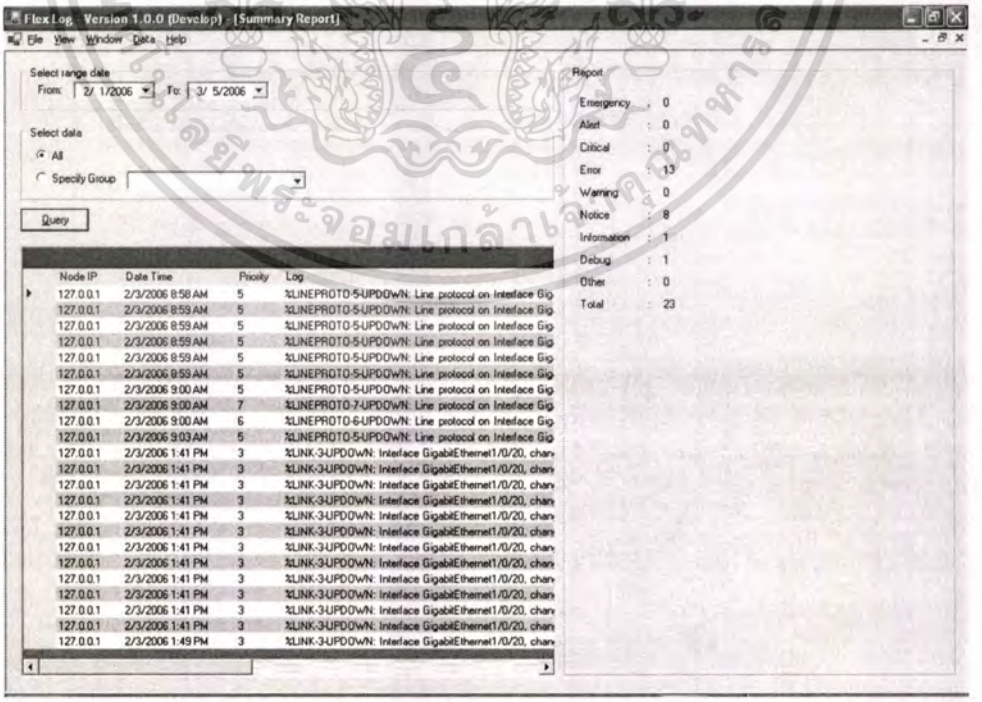
รูปที่ 4.1 เมนูหลัก

4.2 ส่วนการแสดงผลข้อมูล

สามารถเลือกให้แสดงข้อมูลในเวลาปัจจุบัน หรือแสดงข้อมูลตามเงื่อนไขที่ต้องการได้ และยังรวมถึงการออกรายงานตามความสำคัญของล็อกและตามรูปแบบของล็อกได้อีกด้วย



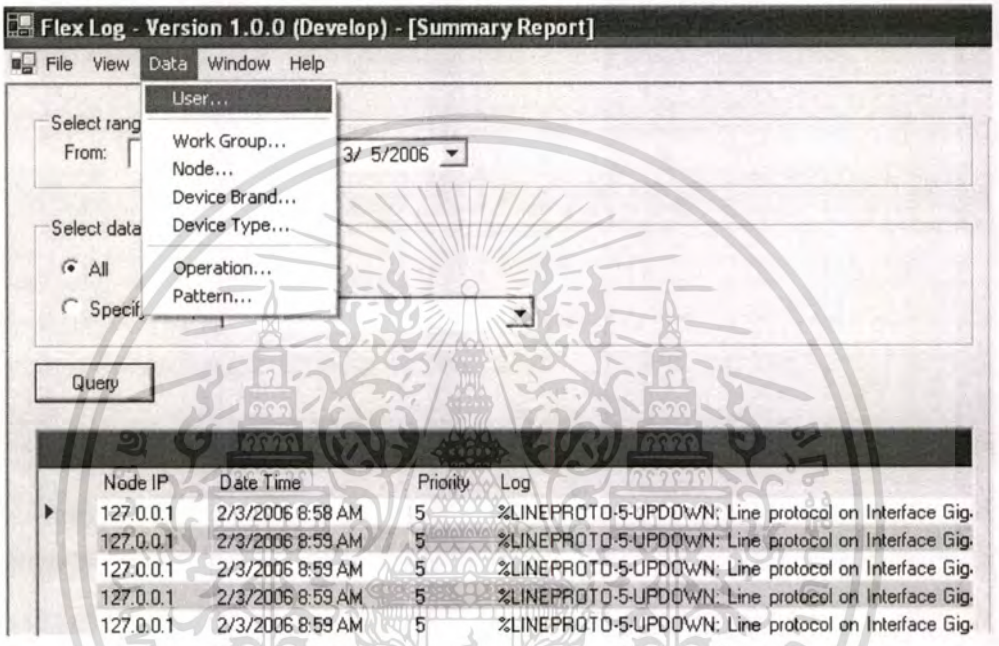
รูปที่ 4.2 ส่วนการแสดงผลข้อมูล



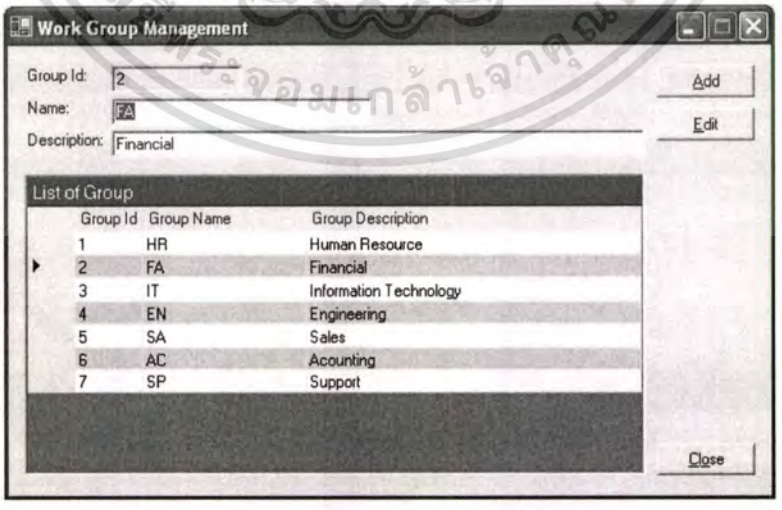
รูปที่ 4.3 ส่วนการแสดงผลข้อมูลตามรูปแบบของข้อมูลล็อก

4.3 การจัดการข้อมูลในฐานข้อมูล

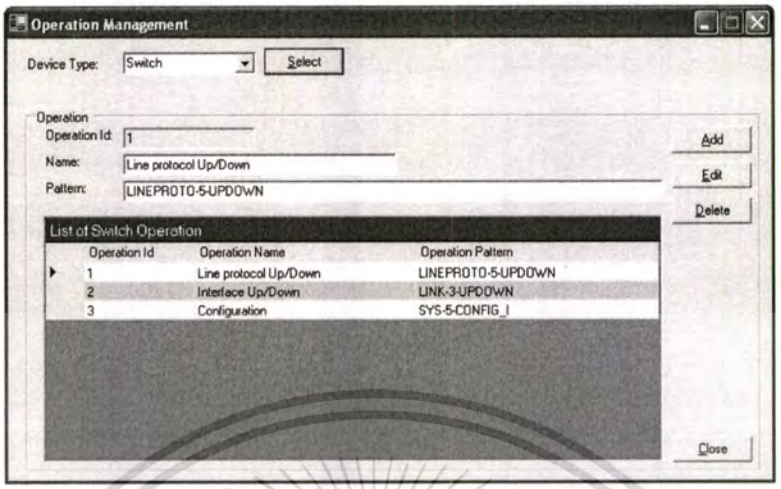
ประกอบไปด้วยการจัดการข้อมูลผู้ใช้ ข้อมูลกลุ่มอุปกรณ์ ข้อมูลโหนด ข้อมูลยี่ห้ออุปกรณ์ และชนิดของอุปกรณ์ นอกจากนี้ยังมีส่วนข้อมูลรูปแบบการกระทำการของเมสเสจและรูปแบบของเมสเสจอีกด้วย โดยในการพัฒนาส่วนนี้ ได้นำ Regular expression เข้ามาช่วยในการจัดการรูปแบบต่างๆให้สั้นและง่ายต่อการออกแบบโปรแกรมยิ่งขึ้น



รูปที่ 4.4 การจัดการข้อมูลในฐานข้อมูล



รูปที่ 4.5 การจัดการข้อมูลกลุ่มอุปกรณ์



รูปที่ 4.6 การจัดการข้อมูลรูปแบบการกระทำการของเมสเสจ

บทที่ 5
สรุปผลการพัฒนาระบบ

ผลที่ได้รับจากโครงการพัฒนาระบบงาน "โปรแกรมจัดเก็บและช่วยวิเคราะห์ข้อมูลล็อก" ที่ได้จัดทำขึ้นนี้ ได้เกิดขึ้นจากการนำความรู้ในหลายๆ ด้านมาประกอบกันเพื่อใช้ในการวิเคราะห์ออกแบบระบบงาน การออกแบบฐานข้อมูลเพื่อจัดเก็บข้อมูลสถิติ การพัฒนาระบบภายใต้ .NET แพลตฟอร์ม โดยการพัฒนาโครงงานนี้มีจุดประสงค์ของการพัฒนาระบบเพื่อเพิ่มเติมความสามารถในการจัดเก็บล็อกซึ่งถือเป็นข้อมูลที่มีประโยชน์ในการนำมาช่วยในการวิเคราะห์ปัญหาที่เกิดขึ้นในระบบเครือข่ายให้ได้รวดเร็วยิ่งขึ้น และการแสดงผลที่สามารถเลือกได้ตามความต้องการของผู้ใช้งาน เพื่อนำข้อมูลที่ได้รับไปใช้งานในภายหลัง

5.1 ประโยชน์ที่ได้รับ

จากการพัฒนาโครงงานนี้ทำให้ได้รับความรู้ในวิธีการพัฒนาโปรแกรมเครือข่าย syslog server ที่มีการเปิดใช้งานซ็อกเก็ตเพื่อรอรับข้อมูลที่ส่งมายังพอร์ตยูดีพี 514 รวมทั้งนำความรู้ดังกล่าวมาสร้าง โปรแกรมต้นแบบ syslog server ซึ่งพัฒนาโดยเทคโนโลยี VB.NET และทำงานบนระบบปฏิบัติการวินโดวส์ ที่จะช่วยให้มีความสะดวกและรวดเร็วในการใช้งานมากขึ้น โดยโปรแกรมจะทำหน้าที่เก็บข้อมูลล็อกจากอุปกรณ์ต่างๆ และเก็บลงยังฐานข้อมูล นอกจากนี้ ผู้ดูแลระบบจะสามารถดูข้อมูลได้โดยเลือกการแสดงผลตามที่ต้องการ โดยระบุได้ตามรายอุปกรณ์ที่ส่งข้อมูลมา หรือตามเงื่อนไขที่ผู้ดูแลระบบต้องการอีกด้วย

5.2 ข้อเสนอแนะ

เนื่องจากจุดประสงค์ของการพัฒนาระบบงาน ได้ออกแบบมาสำหรับอุปกรณ์ CISCO เป็นหลัก ลักษณะการแสดงผลจึงถูกออกแบบมาเพื่อให้เหมาะสมกับอุปกรณ์ CISCO เท่านั้น แม้ว่าการออกแบบจะอิงตามมาตรฐานของ IETF แต่หากนำโปรแกรมไปใช้กับอุปกรณ์อื่นๆ อาจต้องมีการปรับแต่งการแสดงผลบ้างเพื่อให้เหมาะสมตามอุปกรณ์นั้นๆ เพื่อช่วยให้การดูแลระบบเครือข่ายมีประสิทธิภาพมากยิ่งขึ้น

นอกจากนี้ในส่วนของการแสดงผล อาจพัฒนาเพิ่มเติมในลักษณะที่เป็นเว็บเบสแอพพลิเคชัน เพื่อให้เกิดความสะดวกต่อการจัดการโดยที่ผู้ดูแลระบบไม่จำเป็นต้องมาทำงานที่หน้าจอ

คอนโซลหลัก และอาจเพิ่มเติมในการจัดการสิทธิ์การเข้าใช้งาน เพื่อให้ผู้มีสิทธิ์เข้าใช้งานมีความแตกต่างกันในส่วนของการใช้งาน และการปรับแต่งค่าต่างๆ

ในส่วนงานที่มีการรับเมสเสจล็อกมาไว้ที่เซิร์ฟเวอร์เพียงแหล่งเดียวอาจเกิดเป็น single point of failure ได้ อาจเพิ่มเติมในส่วนที่ทำหน้าที่รีพลิเคทข้อมูลอัตโนมัติไปยังเซิร์ฟเวอร์ตัวอื่น ที่เป็นเซิร์ฟเวอร์สำรองได้อีกด้วย

บรรณานุกรม

จักรพันธุ์ โพธิวรรณา และ อัมรินทร์ เพ็ชรกุล. 2537. **Microsoft Visual Studio.net.** กรุงเทพฯ: ซีเอ็ดยูเคชั่น.

สุรสิทธิ์ คิวประสพศักดิ์ และ นันทนี แขวงโสภา. 2546. **อินไซท์ Visual Basic.NET.** กรุงเทพฯ: โปรวิชั่น.

โอกาส เอี่ยมสิริวงศ์. 2546. **การวิเคราะห์และออกแบบระบบ.** กรุงเทพฯ: ซีเอ็ดยูเคชั่น.

C. Lonvick. 2001. **RFC3164 : The BSD syslog Protocol**. IEEE/IFIP Network Operations & Management Symposium.

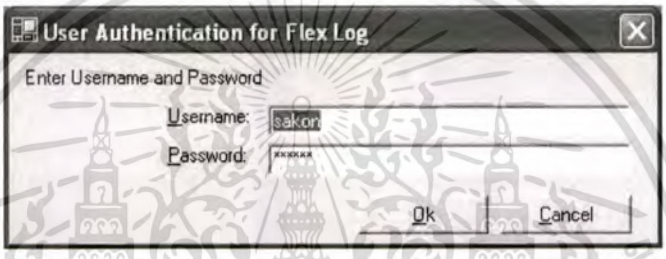
Richard Murphy. 2001. **How to Integrate Centralized Logging with Centralized Monitoring.** SANS Security Essentials GSEC Practical Assignment.

Wajih-ur-Rehman. 2003. **Introduction to Syslog Protocol.** Monitorware.

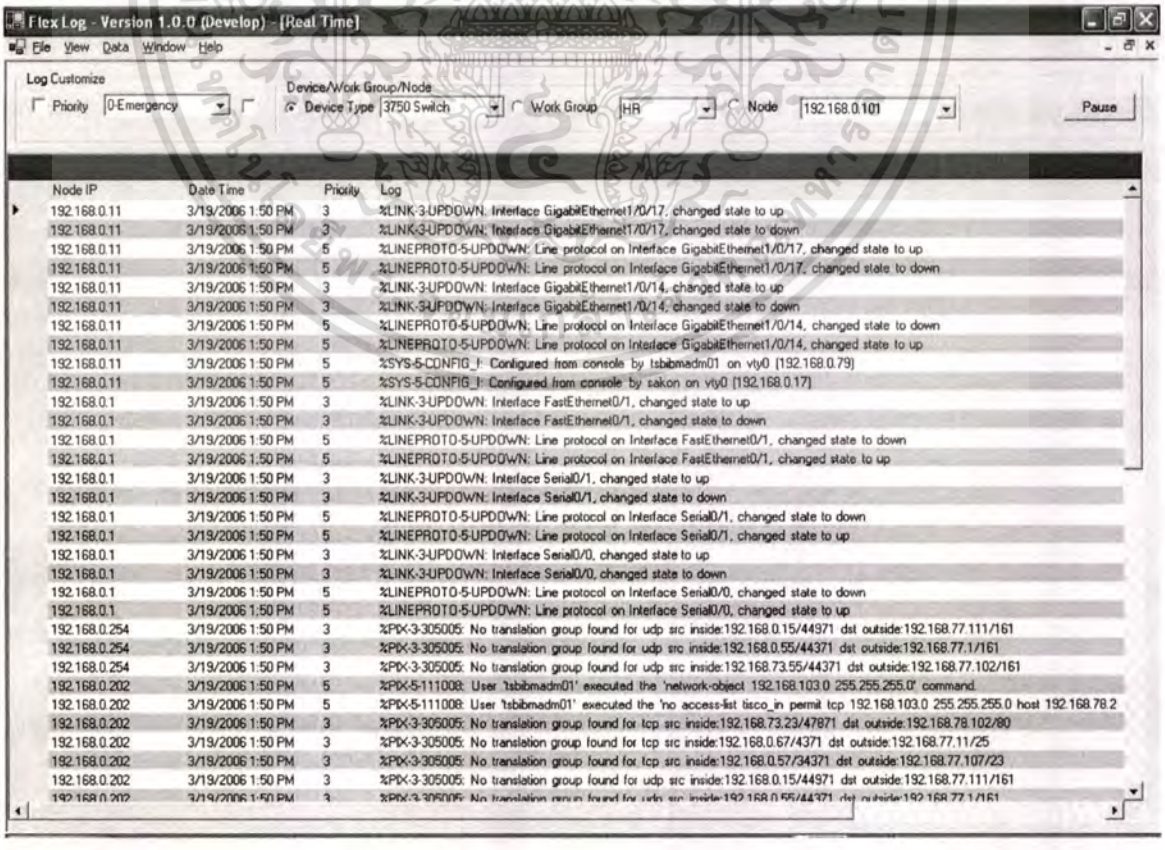
ภาคผนวก

ในภาคผนวกนี้แสดงถึงหน้าจอโปรแกรมและวิธีการใช้งานโปรแกรมโปรแกรมจัดเก็บและช่วยวิเคราะห์ข้อมูลล็อก

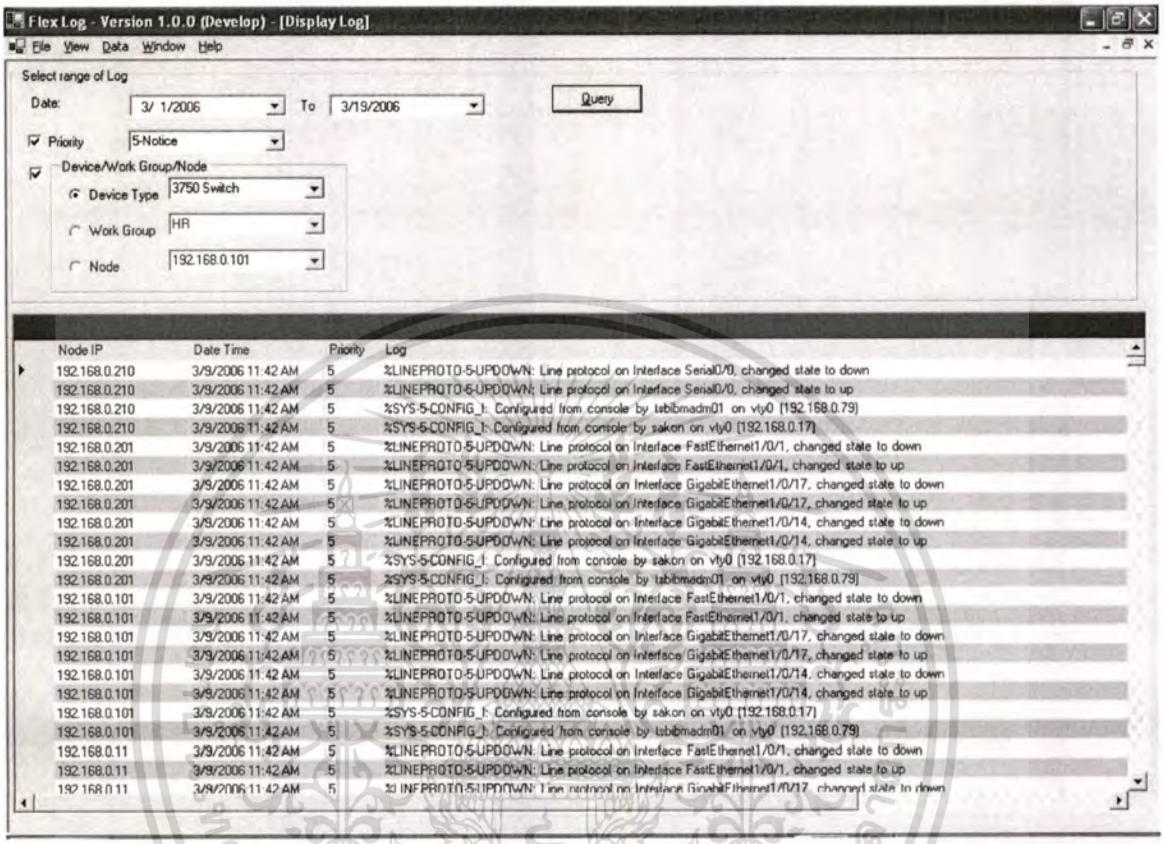
1. เมื่อเข้าสู่โปรแกรมจะต้องผ่านหน้าต่าง Login เพื่อตรวจสอบสิทธิ์การเข้าใช้งาน



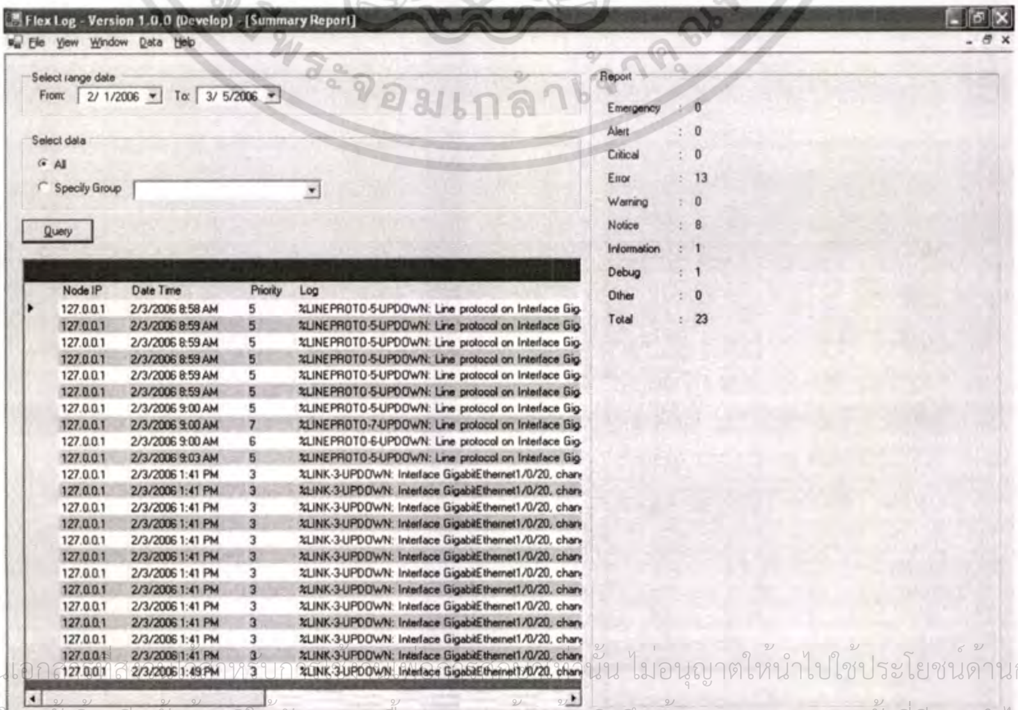
2. โปรแกรมจะทำการเริ่มเก็บข้อมูลล็อกในทันทีที่มีการเปิดโปรแกรมขึ้นมา และแสดงผลในหน้าจอ Real Time Log



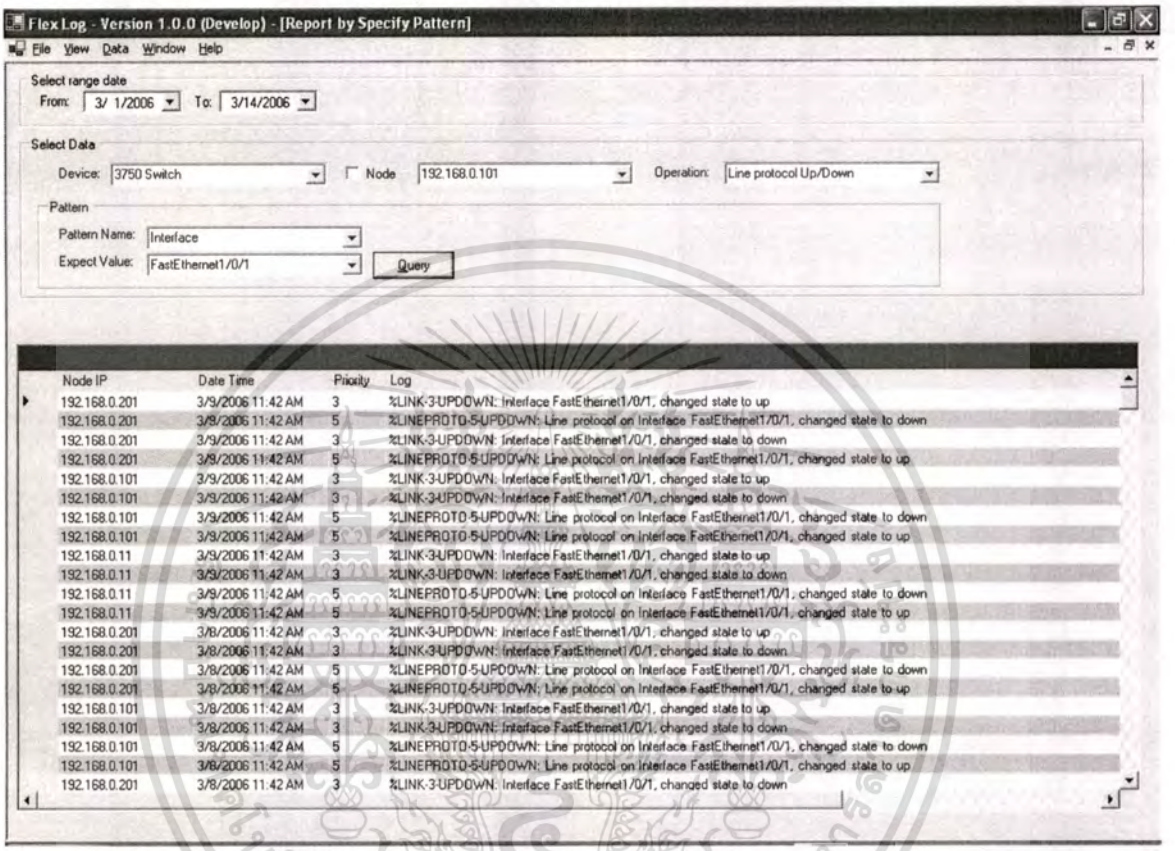
3. หากต้องการเลือกดูล็อกตามเงื่อนไขที่กำหนด จะสามารถเลือกได้จากหน้าจอ Display log by query



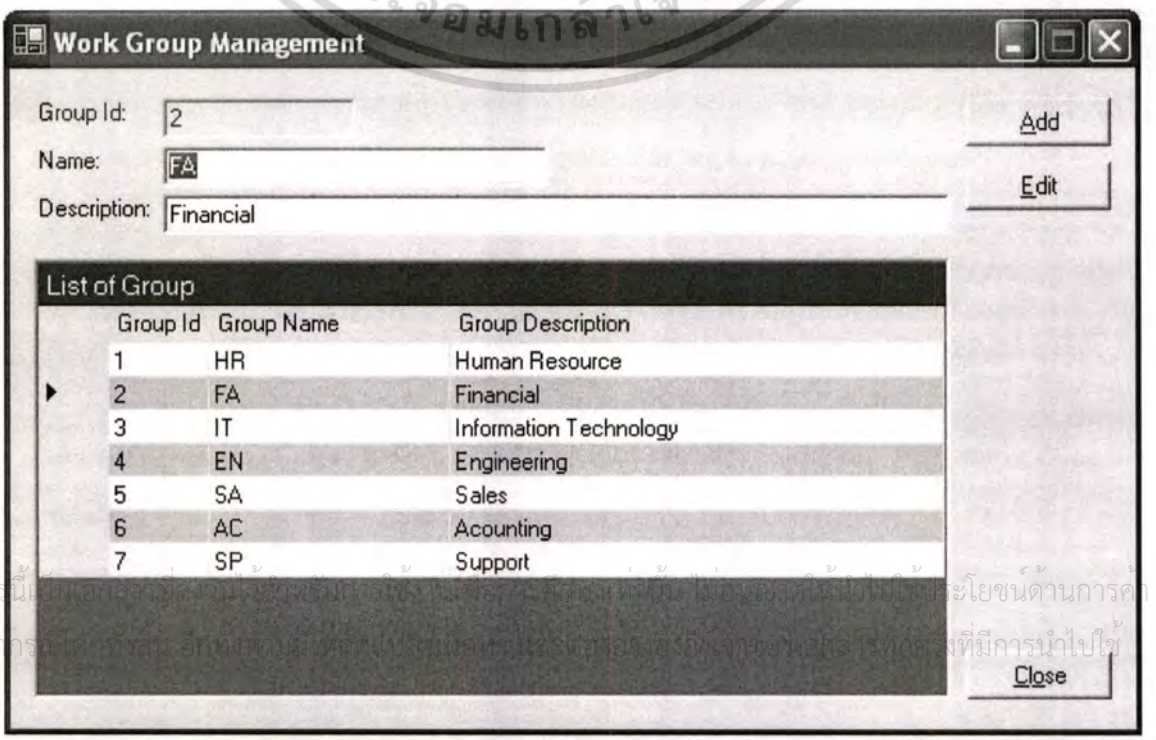
4. สามารถเลือกให้ออกรายงานตามความสำคัญของล็อกได้



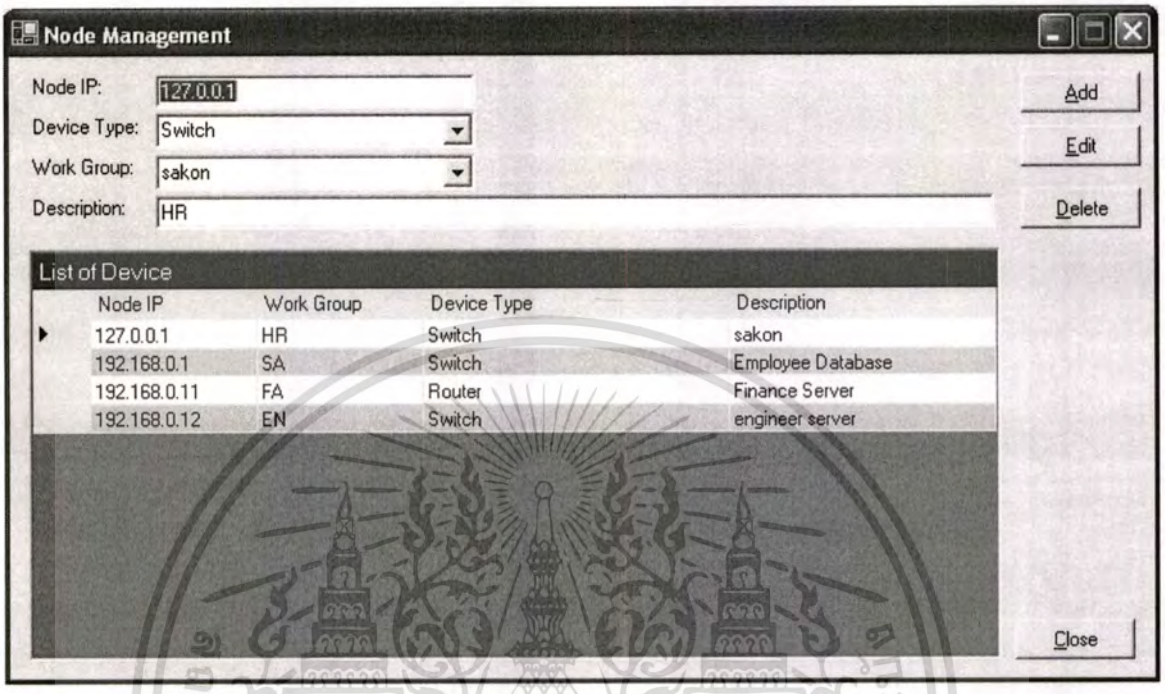
5. สามารถเลือกให้ออกรายงานตามรูปแบบของล็อกได้



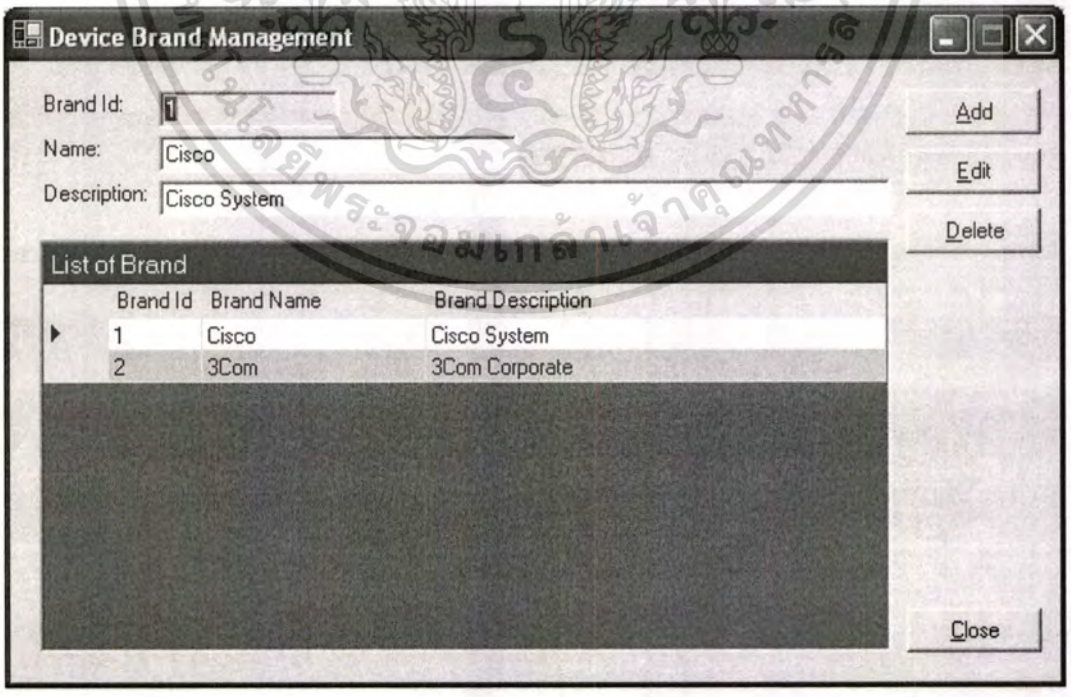
6. เลือกจัดการเพิ่มลบข้อมูลของ workgroup ได้จากหน้าจอ Work Group Management



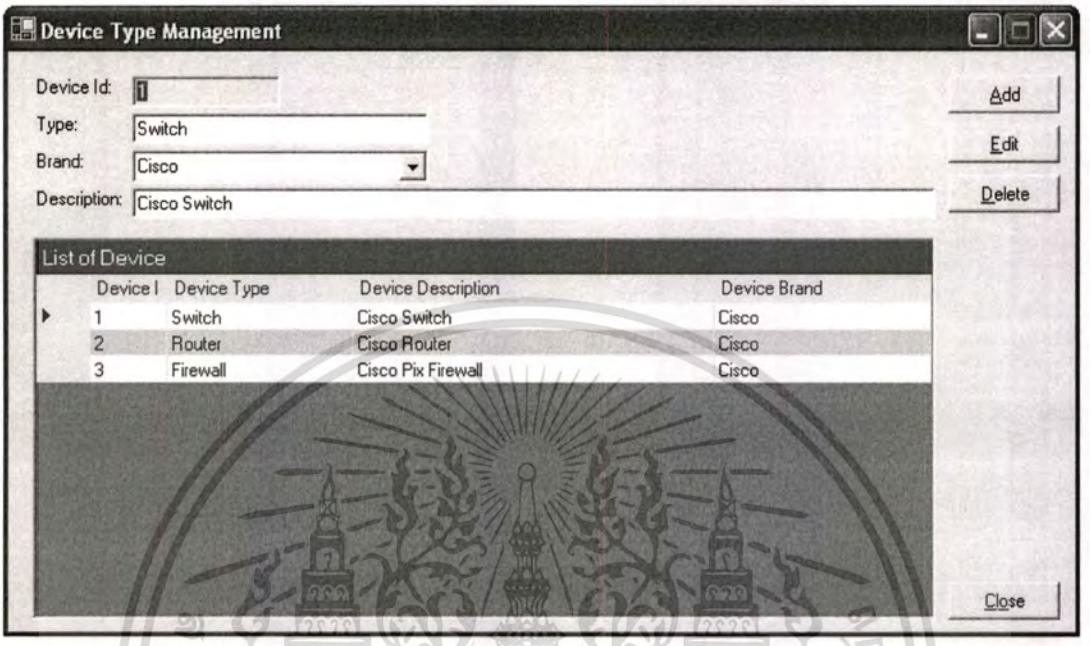
7. เลือกจัดการเพิ่มลบข้อมูลของโหนดได้จากหน้าจอ Node Management



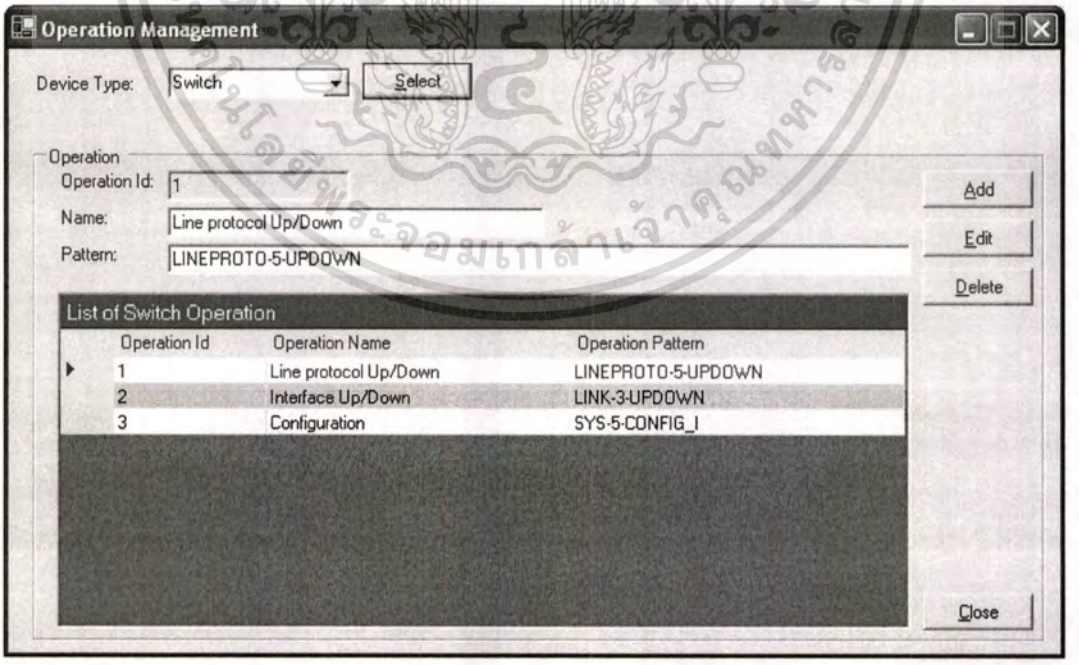
8. เลือกจัดการเพิ่มลบข้อมูลของอุปกรณ์ได้จากหน้าจอ Device Brand Management



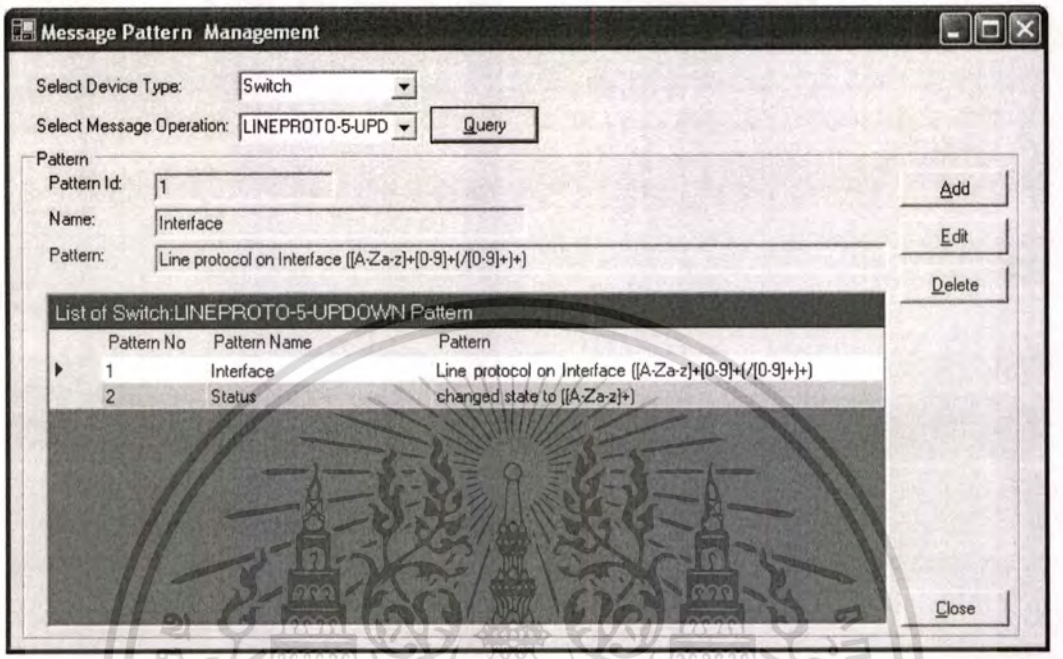
9. เลือกจัดการเพิ่มลบข้อมูลชนิดของโหนดได้จากหน้าจอ Device Type Management



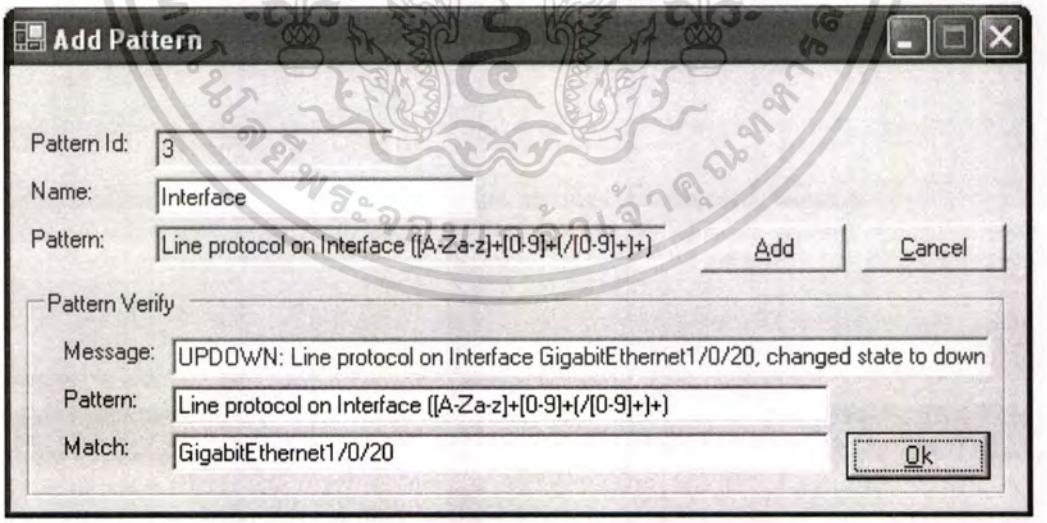
10. เลือกจัดการเพิ่มลบข้อมูลส่วนข้อมูลรูปแบบการกระทำการของเมสเสจได้จากหน้าจอ Operation Management



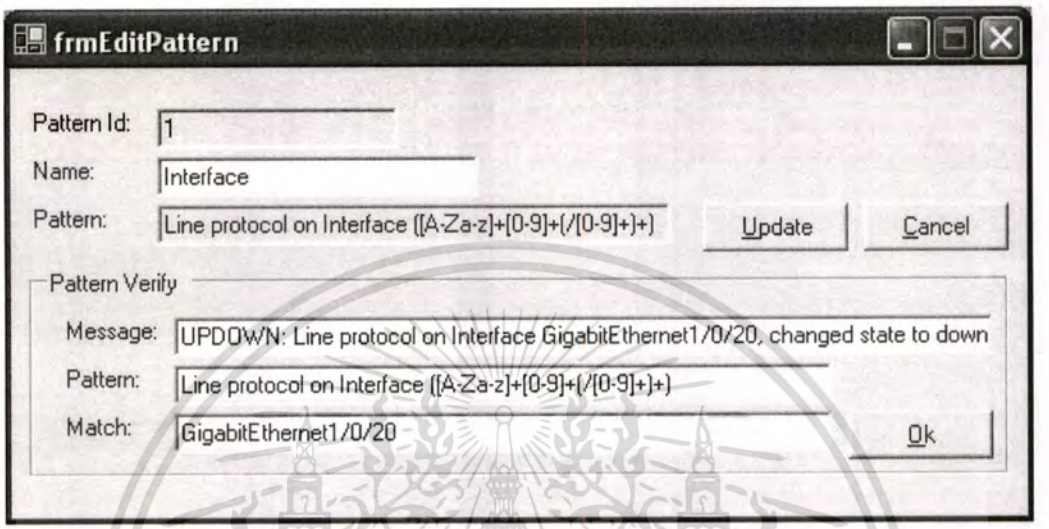
11. เลือกจัดการเพิ่ม แก้ไข และลบข้อมูลส่วนรูปแบบของเมสเสจได้จากหน้าจอ Message Pattern Management



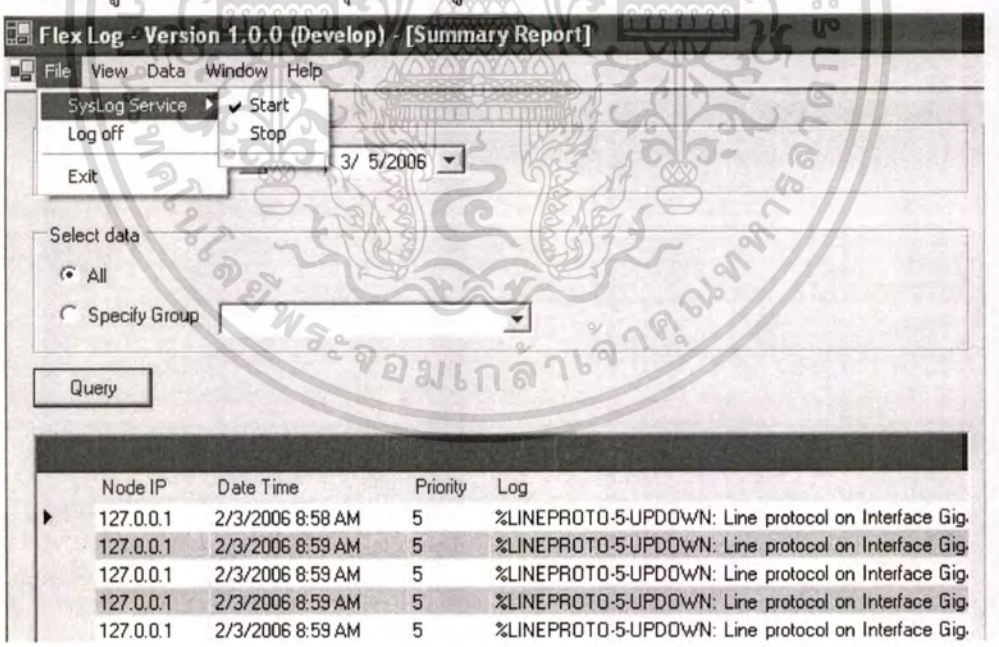
12. คลิกที่ปุ่ม Add เมื่อต้องการเพิ่มรูปแบบของเมสเสจ จะปรากฏหน้าต่าง Add Pattern ให้ทำการพิมพ์ข้อมูลลงไปยังแต่ละช่องข้อความจากนั้นกด Ok



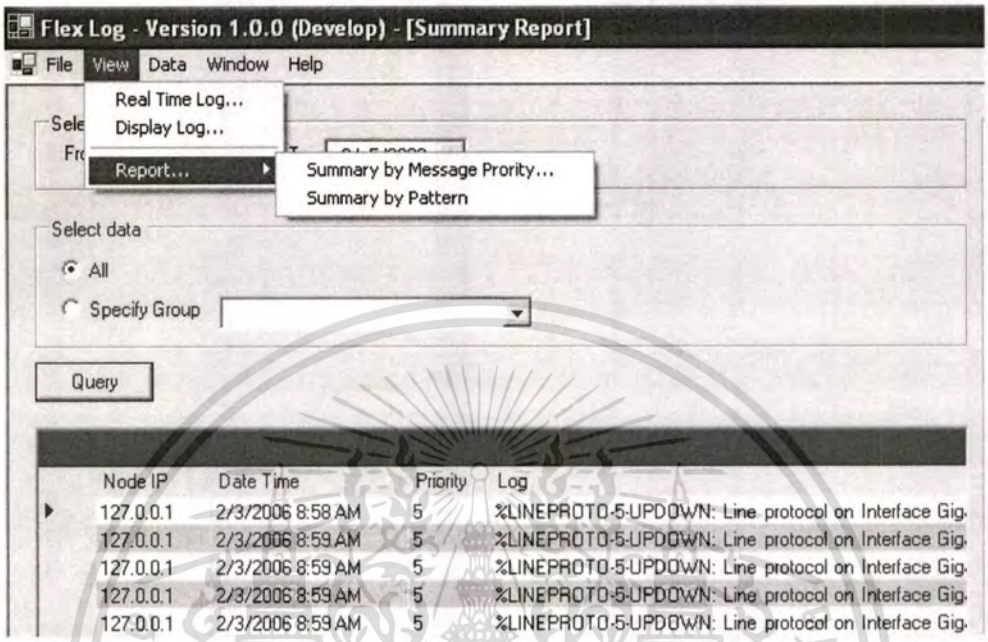
13. คลิกที่ปุ่ม Edit เมื่อต้องการแก้ไขรูปแบบของเมสเสจ จะปรากฏหน้าต่าง Edit Pattern และให้ทำการพิมพ์ข้อมูลลงไปยังแต่ละช่องข้อความจากนั้นกด Ok



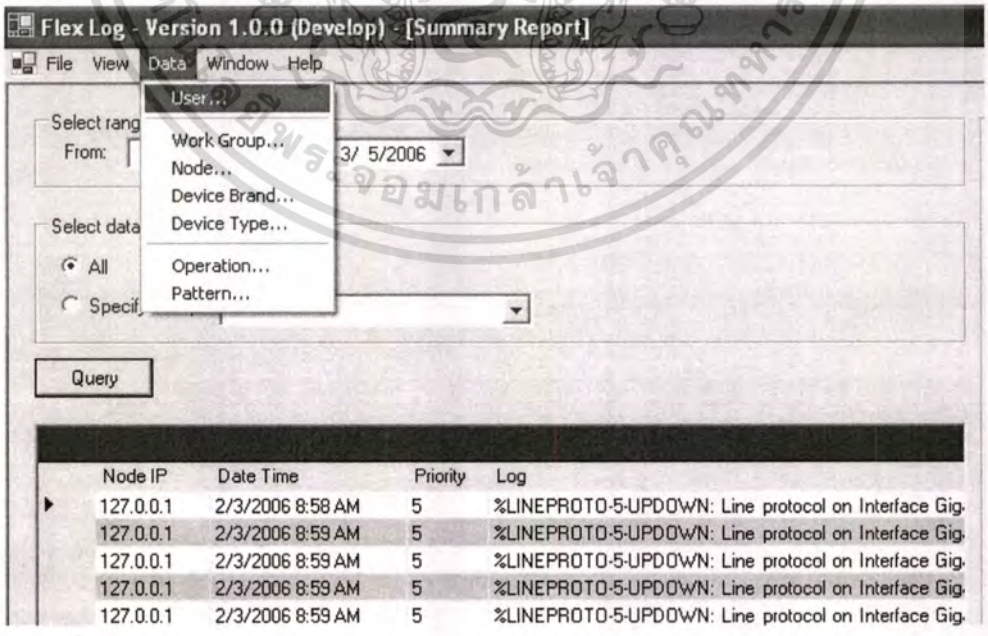
14. แสดงถึงเมนูหลักที่สั่งเริ่มหรือหยุดเก็บข้อมูลล็อก



15. เป็นเมนูที่สามารถเลือกให้แสดงข้อมูลในเวลาปัจจุบัน หรือแสดงข้อมูลตามเงื่อนไขที่ต้องการได้ และยังรวมถึงการออกรายงานตามความสำคัญของล็อกและตามรูปแบบของล็อกได้อีกด้วย



16. เป็นเมนูที่ประกอบไปด้วยการจัดการข้อมูลผู้ใช้ ข้อมูลกลุ่มอุปกรณ์ ข้อมูลโหนด ข้อมูลยี่ห้ออุปกรณ์ และชนิดของอุปกรณ์ นอกจากนี้ยังมีข้อมูลรูปแบบการกระทำการของเมสเสจและรูปแบบของเมสเสจ



ประวัติผู้เขียน

ชื่อผู้เขียน	นายสกล เขียวลำยอง
วันเดือนปีเกิด	17 กุมภาพันธ์ 2521
สถานที่เกิด	กำแพงเพชร
วุฒิการศึกษาระดับปริญญาตรี	วิศวกรรมศาสตรบัณฑิต (วศ.บ. วิศวกรรมคอมพิวเตอร์)
สถานที่สำเร็จการศึกษา	มหาวิทยาลัยนเรศวร
ปีที่สำเร็จการศึกษา	ปีการศึกษา 2544
สถานที่ทำงานปัจจุบัน	บริษัท ซีเลสติกา (Celestica Ltd.)