

ระบบตรวจสอบและแจ้งผลการทำงานของอุปกรณ์เครือข่ายคอมพิวเตอร์

พลภัทร มั่นยานนท์*

ผู้ช่วยศาสตราจารย์ ดร. ประจวบ วานิชชัชวาล**

บทคัดย่อ

ปัจจุบันเครือข่ายคอมพิวเตอร์ได้มีบทบาทต่อชีวิตประจำวันมากขึ้นทุกขณะ การเจริญเติบโตของเครือข่ายคอมพิวเตอร์เหล่านี้เป็นไปอย่างต่อเนื่อง และยังมีสัญญาณบ่งบอกว่า จะมีลลิตัวแต่อย่างใด เครือข่ายคอมพิวเตอร์ท้องถิ่น (LAN) ในองค์กรต่าง ๆ ตลอดจน บริษัท สถานการศึกษาส่วนใหญ่มากกว่า 80% จะนิยมใช้เครือข่าย Ethernet ด้วยความต้องการ การส่งผ่านข้อมูลที่เพิ่มขึ้นอย่างรวดเร็วตามขนาดและจำนวนเครื่องคอมพิวเตอร์ที่ต่ออยู่บนเครือข่าย ตลอดจนการเติบโตของอินเทอร์เน็ตอย่างรวดเร็ว จึงทำให้ผู้ดูแลเครือข่ายคอมพิวเตอร์ จะต้องการ ทำการจัดการอุปกรณ์ที่มีคุณสมบัติที่ดี และเหมาะสมเข้ามาติดตั้งและให้บริการบนเครือข่าย คอมพิวเตอร์ เพื่อตอบสนองความต้องการดังกล่าว หากแต่การให้บริการที่ดีเยี่ยม นั้น จะต้อง รวมถึงการตรวจสอบและซ่อมบำรุงหรือเฝ้าดูระบบเครือข่ายให้สามารถใช้งานได้อย่างมีประสิทธิภาพ ดังนั้นงานของผู้จัดการระบบเครือข่ายจึงจำเป็นต้องมีเครื่องมือที่ดี และเหมาะสม กับระบบเครือข่ายของตนเอง เพื่อใช้ในการบริหารจัดการ เฝ้าติดตาม วิเคราะห์ และแก้ไขปัญหา ของเครือข่ายคอมพิวเตอร์ที่อาจจะเกิดขึ้นได้ การแก้ไขปัญหาต่าง ๆ เป็นงานสำคัญอย่างยิ่งของ ผู้จัดการเครือข่ายคอมพิวเตอร์และงานที่สำคัญยิ่งของการแก้ไขปัญหาก็คือ การตรวจสอบระบบ เครือข่าย ดังนั้นควรมีระบบตรวจสอบและรายงานการทำงานของอุปกรณ์เครือข่าย คอมพิวเตอร์เพื่อเป็นเครื่องมือสนับสนุนการทำงานของผู้ดูแลระบบเครือข่ายคอมพิวเตอร์

โครงการนี้จึงได้ถูกพัฒนาขึ้น โดยใช้ภาษา PHP (PHP Hypertext Preprocessor) เป็น เครื่องมือหลักในการออกแบบและพัฒนา โดยมีการทำงานร่วมกับโปรโตคอล SNMP (Simple Network Management Protocol) ซึ่งเป็นโปรโตคอลที่อยู่ระดับบนในชั้นการประยุกต์ และเป็น ส่วนหนึ่งของชุดโปรโตคอล TCP/IP ในการบริการและจัดการเครือข่ายต้องใช้อุปกรณ์ต่าง ๆ มี ส่วนของการทำงานร่วมกับระบบจัดการเครือข่าย ซึ่งเราเรียกว่า เอเจนต์ (Agent) เอเจนต์เป็น ส่วนของซอฟต์แวร์ที่อยู่ในอุปกรณ์ รวมทั้งยังใช้คุณสมบัติของโปรแกรม MRTG (Multi Router Traffic Grapher) เพื่อบันทึกสถิติการทำงานของอุปกรณ์ระบบเครือข่าย และนำมาแสดงผลใน รูปแบบของกราฟและตัวเลขของการไหลข้อมูล ผ่านทางเว็บไซต์

* นักศึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ มหาวิทยาลัยธุรกิจบัณฑิตย์

** ที่ปรึกษาโครงการ

บทนำ

ปัญหาและความสำคัญ

ในการบริหารจัดการเครือข่ายคอมพิวเตอร์ภายในองค์กรที่นับวันจะทวีความซับซ้อนมากยิ่งขึ้น ทั้งนี้เนื่องจากความมีการใช้งานเทคโนโลยีสารสนเทศเพิ่มมากขึ้นทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ ซึ่งสารสนเทศดังกล่าว จะต้องมีระบบเครือข่ายที่มีประสิทธิภาพและความน่าเชื่อถือ ดังนั้นงานของผู้จัดการระบบเครือข่ายจึงจำเป็นต้องมีเครื่องมือที่ดี และเหมาะสมกับระบบเครือข่ายของตนเอง เพื่อใช้ในการบริหารจัดการ ฝ้าติดตาม วิเคราะห์ และแก้ไขปัญหาของระบบ ที่อาจจะเกิดขึ้นได้ การแก้ไขปัญหาต่าง ๆ เป็นงานสำคัญอย่างมากของผู้จัดการระบบเครือข่าย และงานที่สำคัญยิ่งของการแก้ไขปัญหาก็คือ การตรวจสอบระบบเครือข่ายก่อนข้อผิดพลาดจะเกิดขึ้น ซึ่งโปรแกรมตรวจสอบการทำงานของระบบเครือข่าย (Network Monitoring) โดยใช้โปรโตคอล SNMP สามารถตรวจสอบการทำงานของอุปกรณ์เครือข่ายได้ ปัญหาส่วนใหญ่ของระบบเครือข่ายที่มักจะเกิดขึ้นเราอาจจะแบ่งออกได้ 2 ลักษณะใหญ่ ๆ คือ ประการแรก อุปกรณ์ระบบเครือข่ายไม่ทำงานตามที่คาดหมายไว้ เช่น อุปกรณ์เครือข่ายไม่สามารถรับส่งข้อมูลได้ตามปกติ ในประการนี้ ผู้ดูแลระบบสามารถตรวจสอบการทำงานของอุปกรณ์เครือข่ายได้โดยใช้ระยะเวลาไม่นาน ส่วนประการที่สอง ระบบเครือข่ายมีประสิทธิภาพการทำงานที่ผิดปกติ เช่น รับส่งข้อมูลได้ช้าลง ในประการนี้ผู้ดูแลระบบต้องอาศัยความรู้ความสามารถในการวิเคราะห์ระบบโดยรวม รวมถึงการตรวจสอบประสิทธิภาพการทำงานของอุปกรณ์เครือข่ายในแต่ละส่วนและจะต้องใช้ระยะ รวมถึงการตรวจสอบประสิทธิภาพการทำงานของอุปกรณ์เครือข่ายในแต่ละส่วน และจะต้องใช้ระยะเวลาหนึ่งในการวิเคราะห์หาสาเหตุทำการแก้ไขปัญหาของระบบซึ่งผู้ดูแลระบบจำเป็นต้องอาศัยเครื่องมือต่าง ๆ เพื่อช่วยตรวจสอบและรวบรวมข้อมูลการทำงาน ในการวิเคราะห์เพื่อเฝ้าระวังและแก้ไขปัญหาได้รวดเร็วยิ่งขึ้น

ขอบเขตโครงการบริหารจัดการเครือข่าย (Network Management System)

การบริหารจัดการเครือข่าย (Network Management System) เป็นการดูแลเครือข่ายคอมพิวเตอร์ และจัดการทรัพยากรในเครือข่ายหนึ่ง ๆ ให้สามารถทำงานได้อย่างมีประสิทธิภาพสูงสุด โดยการเก็บรวบรวมข้อมูล และวิเคราะห์ข้อมูลรวมถึงการดูแลปริมาณของข้อมูลที่มีอยู่ในเครือข่ายคอมพิวเตอร์ไม่ให้มากจนเกินไปเพื่อนำมาตัดสินใจต่อการจัดการเครือข่าย ซึ่งการจัดการระบบเครือข่ายคอมพิวเตอร์นั้นสามารถที่จะแบ่งออกเป็นส่วนต่าง ๆ ได้เป็น 5 ส่วนหลักคือ

1. การจัดการระบบความผิดพลาดของเครือข่าย (Fault Management)
 - การตรวจสอบสถานะของระบบคอมพิวเตอร์ และ เครือข่าย
 - การตรวจสอบปัญหาและการแจ้งปัญหา

- การวิเคราะห์ถึงเหตุของปัญหา
 - การแก้ไขปัญหา
 - การบันทึกปัญหา และวิธีการแก้ไข
2. การจัดการคุณสมบัติของอุปกรณ์ของเครือข่าย (Performance Management)
- การดำเนินการเพื่อให้ระบบเครือข่ายสามารถใช้ได้อย่างเต็มประสิทธิภาพ
 - สิ่งที่เป็นจะต้องคำนึงถึง
 - Throughput
 - Utilization
 - Error
 - Response Time
 - มีการกำหนดค่ามาตรฐานในการใช้งานเครือข่าย
 - มีระบบเตือนผู้ดูแลหากมีการใช้งานเกินค่ามาตรฐานดังกล่าว เพื่อให้มีการดำเนินการอื่น ๆ ต่อไป
3. การจัดการรูปแบบของเครือข่าย (Configuration Management)
- ลักษณะการเชื่อมต่อ และความสัมพันธ์ต่าง ๆ ของระบบ
 - ข้อมูลต่าง ๆ ของอุปกรณ์ เช่น รุ่น ยี่ห้อ คุณลักษณะ ซอฟต์แวร์
 - ข้อมูล Configuration ต่าง ๆ ที่ทันสมัยอยู่ตลอดเวลา
 - การทำ Change Management เพื่อวิเคราะห์ถึงการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้น ไม่ว่าจะ เป็น Configuration, Hardware, Software
 - ข้อมูลต่าง ๆ เกี่ยวกับระบบที่เก็บไว้นั้น ต้องสามารถเข้าถึงได้อย่างรวดเร็วในกรณีฉุกเฉิน
4. การจัดการระบบบัญชีของเครือข่าย (Accounting Management)
- การบันทึกกิจกรรมต่าง ๆ ในระบบเครือข่าย
 - การคำนวณต้นทุนในการใช้งานระบบเครือข่าย
 - การดำเนินการเพื่อลดต้นทุน การกำหนดนโยบาย หรือ Quota ในการใช้งาน
5. การจัดการระบบความปลอดภัยของเครือข่าย (Security Management)
- การควบคุมการเข้าถึงทรัพยากรต่าง ๆ ของระบบเครือข่าย (ACL)
 - การจัดตั้งนโยบายรักษาความปลอดภัยการใช้งานเครือข่ายคอมพิวเตอร์
 - มีการนำระบบ AAA เข้ามาใช้งาน
 - Authentication

- Authorization
- Accounting
- มีการตรวจสอบบันทึกการเข้าถึง (Logging) อย่างสม่ำเสมอ
- การทำ Data Encryption

สำหรับในโครงการการนี้ ผู้พัฒนามุ่งเน้นพัฒนาในส่วนของการเฝ้าระวังและการแจ้งเตือน หรือการจัดการระบบความผิดปกติของเครือข่าย (Fault Management) และการจัดการคุณสมบัติของอุปกรณ์ของเครือข่าย (Performance Management) เป็นหลัก

ทฤษฎีและเทคโนโลยีที่ใช้ในโครงการ

ระบบตรวจสอบและแจ้งผลการทำงานของอุปกรณ์เครือข่ายคอมพิวเตอร์ พัฒนาขึ้นโดยใช้ภาษา PHP เป็นภาษาหลัก ระบบพัฒนาได้ใช้เทคโนโลยีดังนี้

โปรแกรม XAMPP 5.5.19 ทำงานในลักษณะของ Webserver ซึ่งประกอบไปด้วยชุดโปรแกรมย่อยๆ คือ

- PHP version 5.5.24
- MySQL version 5.6.24
- phpMyadmin version 4.4.3
- Apache version 2.4

ภาษา Script ที่เลือกใช้คือ PERL (ActivePerl-5.20.2.2001-MSWin32-x64-298913) พัฒนาโปรแกรมอินเตอร์เฟซ แบบ Common Gateway (Common Gateway Interface) ทำงานร่วมกับ MRTG (The Multi Router Traffic Grapher)

เครื่องมือที่ใช้สำหรับการมอนิเตอร์ เพื่อรวบรวมข้อมูลจากตัวอุปกรณ์คือ คือ MRTG (Multi Router Traffic Grapher) version 2.17-4

โปรโตคอลสำหรับใช้ในการตรวจสอบสถานะของตัวอุปกรณ์ในทุก ๆ ช่วงเวลา คือ โปรโตคอล ICMP (Internet Control Message Protocol)

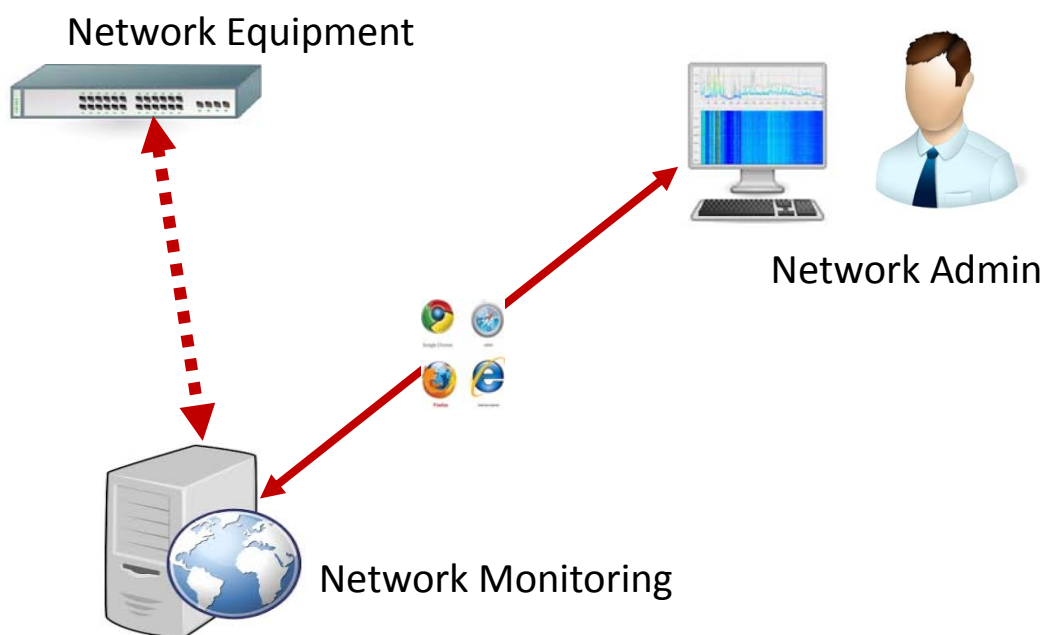
Template OID ของข้อมูลเพื่อเปรียบเทียบกับข้อมูลบนตัวอุปกรณ์ หรือ MIB (Management Information Base) ซึ่งเป็นฐานข้อมูล ที่เอเจนต์ใช้ตรวจสอบสภาพการทำงานของอุปกรณ์ เช่น สถานะ ข้อมูลเชิงปริมาณและทางสถิติของอุปกรณ์เครือข่าย

ระบบความปลอดภัย เข้ารหัสด้วย MD5 สำหรับการตรวจสอบสิทธิ์เพื่อเชื่อมต่อกับ Mail Server ส่วนกลาง ใช้ในการแจ้งเตือนสถานะด้วย e-mail

การออกแบบและการพัฒนา

ระบบตรวจสอบและแจ้งผลการทำงานของอุปกรณ์เครือข่ายคอมพิวเตอร์เป็นโปรแกรมประยุกต์บนเว็บ (Web Application) ที่สามารถเข้าถึงได้จากทุกจุดที่มีสัญญาณอินเทอร์เน็ต

หลักการออกแบบและพัฒนาระบบคือ มี Dashboard หลัก 3 menu เพื่อให้สามารถใช้งานได้ครอบคลุมตามวัตถุประสงค์ ได้แก่ MyView, Status และ Alert menu

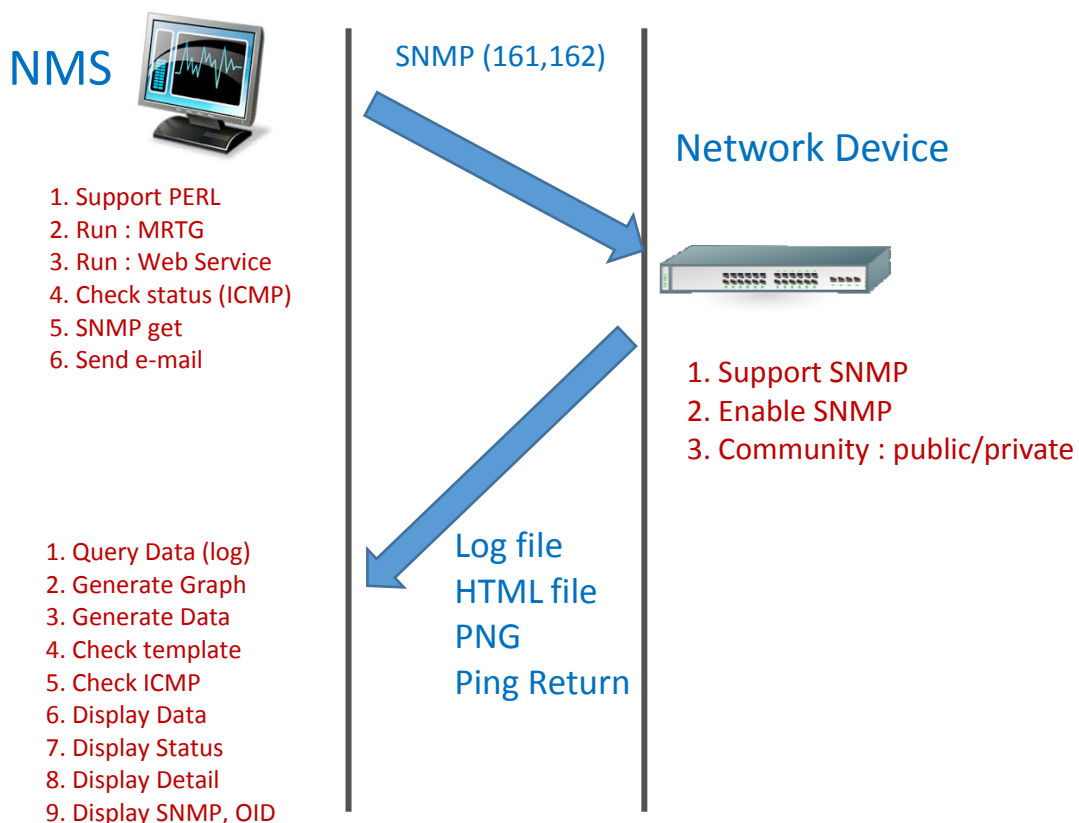


ภาพที่ 1 แสดงภาพการติดต่อสื่อสารระหว่างอุปกรณ์และระบบ NMS

การใช้งานจะทำการ Login เข้าสู่ระบบผ่าน Web Browser ตาม URL ที่ได้กำหนด โดยผู้ใช้งานไม่จำเป็นต้องติดตั้งโปรแกรมใดๆ บนเครื่องคอมพิวเตอร์ที่ทำหน้าที่ Monitor แต่อย่างไรก็ตามเนื่องจากการ Monitor จะกระทำงาน Protocol HTTP และใช้ Port 80 ซึ่งช่องทางมาตรฐานที่มีการใช้งานปกติ

กระบวนการทำงานเริ่มขึ้นจากเครื่องที่ทำหน้าที่เป็น NMS (Network Management System) ในที่นี้ทำหน้าที่เป็นระบบตรวจสอบและแจ้งผลการทำงานของอุปกรณ์เครือข่ายคอมพิวเตอร์ จะทำการส่งคำสั่งไปยังอุปกรณ์เครือข่ายด้วย MRTG ผ่านโปรโตคอล SNMP เพื่อนำข้อมูลที่ได้มาจัดเก็บไว้ ทั้งในรูปแบบของ html, log และ image file พร้อมทั้งทำการประมวลและนำข้อมูลที่ได้แสดงผ่าน Browser ไปยังผู้ร้องขอ หรือ Network Admin และในเวลาเดียวกันก็จะทำการ ส่งคำสั่ง SNMP get เพื่อขอข้อมูลใน MIB ที่อยู่บนตัวอุปกรณ์และใช้ในการแสดง

รายละเอียดของอุปกรณ์ เช่น Host Name, IP Address, MAC Address, Syscontact, และ Location เป็นต้น หลังจากส่งคำสั่งข้างต้นเพื่อเก็บข้อมูลที่ต้องการแล้ว ระบบยังได้ส่ง ICMP หรือทำการ Ping ไปยังอุปกรณ์ตามหมายเลข IP Address ของตัวอุปกรณ์ เพื่อตรวจสอบสถานะว่า อยู่ในสถานะ ON/OFF โดยทำการเปรียบเทียบกับข้อมูลล่าสุดและทำการบันทึก สถานะล่าสุดที่มีการเปลี่ยนแปลงไว้ 15 Status



ภาพที่ 2 แสดงการติดต่อสื่อสารระหว่าง NMS และ Equipment

หลังจาก NMS ได้รับค่าจากการส่งคำสั่งไปยังอุปกรณ์แล้ว ก็จะทำกรตรวจสอบ Log file ที่ได้รับมาเพื่อตรวจสอบ Parameter ต่าง ๆ ที่ถูกจัดเก็บไว้ภายใน เช่น ค่า max input , max output เวลาที่ทำการบันทึกข้อมูล และค่าอื่น ๆ ที่จำเป็น เพื่อนำมาประมวลผลและส่งไปยังส่วนแสดงรายงาน สำหรับกราฟที่ใช้ในการแสดงระบบจะทำการจัดเรียงใหม่ และส่งไปยังส่วนแสดงผลให้ตรงตามรูปแบบที่ได้กำหนดไว้

สำหรับการตรวจสอบสถานะ ON/OFF ของอุปกรณ์ ระบบจะทำการส่งคำสั่งสั้น ๆ เพื่อตรวจสอบเป็นช่วงเวลา ทุก ๆ 5 วินาที ด้วยวิธีการส่งคำสั่ง Ping ไปยังปลายทาง แล้วนำผลที่ได้มาทำการบันทึกและเปรียบเทียบกับค่าก่อนหน้า หากมีการเปลี่ยนแปลงสถานะ จากสถานะเดิมที่

ได้ทำการบันทึกไว้ก่อนหน้า ระบบจะทำการแสดงสถานะที่เปลี่ยนไปพร้อมกับช่วงเวลาที่ตรวจพบ การเปลี่ยนสถานะ ในรูปสัญลักษณ์ 3 แบบ คือ On Line, Off Line และ Destination host unreachable และทุก ๆ ที่มีการเปลี่ยนแปลงสถานะระบบจะทำการส่ง e-mail Alert ไปยัง e-mail ที่กำหนดทันที

สรุปผลการศึกษา และข้อเสนอแนะ

จากการทดสอบระบบตรวจสอบและแจ้งผลการทำงานของอุปกรณ์เครือข่ายคอมพิวเตอร์ เป็นการทดลองกับเครือข่ายที่มีการใช้งานจริงและเครือข่ายจำลอง ว่าสามารถทำงานได้ถูกต้องตามที่ได้กำหนดไว้หรือไม่ ซึ่งผลที่ได้จากการทดสอบติดตั้งใช้งาน สร้างความพึงพอใจให้กับผู้ใช้งานทั้งเจ้าหน้าที่และผู้บริหาร ดังนี้

1. สามารถแสดงการไหลของข้อมูลที่วิ่งผ่านสวิตช์ได้จริง ตามความต้องการของผู้ดูแลระบบเครือข่าย
2. ช่วยเพิ่มความคล่องตัวในการตรวจสอบหรือ Monitoring ระบบเครือข่ายโดยรวมได้ง่ายและสะดวกรวดเร็วยิ่งขึ้น
3. สามารถนำผลที่ได้จากระบบมาช่วยในการวิเคราะห์แก้ปัญหาของระบบเครือข่าย

ข้อเสนอแนะ
ระบบตรวจสอบและแจ้งผลการทำงานของอุปกรณ์เครือข่ายคอมพิวเตอร์ ที่ผู้ศึกษาได้พัฒนาขึ้นนี้ ผู้ศึกษามีข้อเสนอแนะในการพัฒนาต่อ เพื่อให้การใช้งานระบบฯ มีประสิทธิภาพมากยิ่งขึ้นดังนี้

1. พัฒนาให้สามารถใช้ได้กับผลิตภัณฑ์หรือทุกผลิตภัณฑ์
2. ควรมี Module สำหรับค้นหาอุปกรณ์ (Network Scan) เพื่อเพิ่มรายละเอียดที่ค้นหาได้เข้าสู่ระบบต่อไป
3. ควรเพิ่มขีดความสามารถในหัวข้อที่เกี่ยวกับการ รายงานด้าน Time Up/Down เพื่อเป็นการวัดประสิทธิภาพในการให้บริการของตัวอุปกรณ์

บรรณานุกรม

ภาษาไทย

หนังสือ

ชาญชัย สุภอรรรถกร. (2552). คู่มือการเขียนเว็บอีคอมเมิร์ซด้วย PHP + MySQL

กรุงเทพมหานคร: สำนักพิมพ์ซัคเซส มีเดีย.

กิตติศักดิ์ เจริญโภคานนท์. (2548). คู่มือการเขียนเว็บอีคอมเมิร์ซด้วย PHP5 (พิมพ์ครั้งที่

1). กรุงเทพมหานคร: สำนักพิมพ์ซัคเซส มีเดีย.

กิตติ ภัคดีวัฒนกุล. (2548). พื้นฐานการวิเคราะห์และออกแบบระบบเชิงวัตถุด้วย UML

(พิมพ์ครั้งที่ 1). กรุงเทพมหานคร: สำนักพิมพ์เคทีพี คอมพ์ แอนด์ คอนซัลท์.

สารสนเทศจากสื่ออิเล็กทรอนิกส์

XAMPP. สืบค้นเมื่อ 1 พฤศจิกายน 2557,

จาก <https://www.apachefriends.org/index.html>

MRTG. สืบค้นเมื่อ 5 ตุลาคม 2557,

<http://oss.oetiker.ch/mrtg/>

การติดตั้ง MRTG บน windows. สืบค้นเมื่อ 10 ธันวาคม 2557,

<http://www.appservnetwork.com/resume-app/portfolio/www.apples.f2s.com/mrtg.php3>

ตัวอย่างการเขียน code php สืบค้นเมื่อ 1 มกราคม 2557,

<http://sukumal.brinkster.net/meaploy/angel/color.html>

<http://www.thaidev.com/>

การแก้ Error บน PHP สืบค้นเมื่อ 5 ธันวาคม 2557,

<http://www.thaiadmin.org/tamain.php>

SNMP+OID สืบค้นเมื่อ 5 ธันวาคม 2557

<http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&translate=Translate>

<http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&translate=Translate>
&objectInput=1.3.6.1.2.1.1.4#oidContent