ระบบบริหารดูแลเครือข่ายแบบค้นหา

DISCOVERY NETWORK MONITORING SYSTEM

รณรงค์ ศรีสุวรรณ์

RONNARONG SRISUWAN

อาจารย์ที่ปรึกษา

ดร.ปานวิทย์ ธุวะนุติ

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ 2

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ 2 ปีการศึกษา 2556

DISCOVERY NETWORK MONITORING SYSTEM

RONNARONG SRISUWAN

A REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS OF THE COURSE

INDEPENDENT STUDY 2

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2/2013

หัวข้อ ระบบบริหารดูแลเครือข่ายแบบค้นหา

นักศึกษา นายรณรงค์ ศรีสุวรรณ์

รหัสนักศึกษา 52660529

ปริญญา วิทยาศาสตรมหาบัณฑิต

สาขาวิชา เทคโนโลยีสารสนเทศ

แขนงวิชา เทคโนโลยีระบบสารสนเทศ

ปีการศึกษา 2556

อาจารย์ที่ปรึกษา ดร.ปานวิทย์ ธุวะนุติ

บทคัดย่อ

ระบบเครือข่ายจำเป็นต้องมีการบริหารที่ดี โดยเฉพาะเครือข่ายขนาดใหญ่อย่างอินเทอร์เน็ต หากไม่มีการบริหารที่ดีก็จะทำให้การสื่อสารข้อมูลเกิดการผิดพลาดขึ้นได้ โปรโตคอลบริหารจัดการเครือข่าย Simple Network Management Protocol (SNMP) จึงเกิดขึ้นเพื่อใช้ในการบริหารจัดการเครือข่าย และติดตามตรวจสอบอุปกรณ์เครือข่ายต่าง ๆ

ระบบบริหารจัดการเครือข่ายแบบค้นหานี้พัฒนาขึ้นมาเพื่อ เป็นระบบบริหารจัดการเครือข่ายที่สามารถค้นหาอุปกรณ์เครือข่ายที่เชื่อมต่อในระบบเครือข่ายได้ โดยใช้โปรโตคอล SNMP เป็นโปรโตคอลซึ่งเป็นโปรโตคอลที่ใช้ในการบริหารจัดการเครือข่ายในการพัฒนาประกอบกับการพัฒนาในรูปแบบ web base application เพื่อให้สามารถประยุกต์ใช้ได้กับทุกเครือข่าย สามารถใช้งานได้ง่าย

ระบบบริหารจัดการเครือข่ายแบบค้นหาที่พัฒนาขึ้นมานี้ สามารถค้นหาอุปกรณ์เครือข่าย และ สามารถนำข้อมูลการเชื่อมต่อที่ได้มาแสดงเป็นแผนภาพโทโปโลยีได้ และสามารถรวบรวมข้อมูลเชิงสถิติของอุปกรณ์มาแสดงผล สามารถแสดงรายการของอุปกรณ์เครือข่าย และสามารถตรวจจับ ข้อความ Trap ที่ถูกส่งออกมาจากอุปกรณ์เครือข่าย เมื่อเกิดเหตุการณ์ต่างๆขึ้นกับอุปกณ์เครือข่ายได้ ทั้งนี้ผู้พัฒนาได้เล็งเห็นว่า หากระบบเครือข่ายมีขนาดค่อนข้างใหญ่แล้ว จะทำให้เป็นการยุ่งยากสำหรับผู้ดูแลเครือข่ายในการเพิ่มและแก้ไขข้อมูลของอุปกรณ์เครือข่ายด้วยตัวเอง หากมีระบบที่สามารถค้นหาอุปกรณ์เครือข่ายได้ด้วยตัวเองก็จะเป็นประโยชน์กับผู้ดูแลระบบ ผู้พัฒนาจึงได้มีการพัฒนาระบบบริหารจัดการเครือข่ายแบบค้นหาขึ้นมาเพื่อเป็นต้นแบบ

หัวข้อ ระบบบริหารดูแลเครือข่ายแบบค้นหา

นักศึกษา นายรณรงค์ ศรีสุวรรณ์

รหัสนักศึกษา 52660529

ปริญญา วิทยาศาสตรมหาบัณฑิต

สาขาวิชา เทคโนโลยีสารสนเทศ

แขนงวิชา เทคโนโลยีสารสนเทศ

ปีการศึกษา 2556

อาจารย์ที่ปรึกษา ดร.ปานวิทย์ ธุวะนุติ

บทคัดย่อ

ระบบเครือข่ายจำเป็นต้องมีการบริหารที่ดี โดยเฉพาะเครือข่ายขนาดใหญ่อย่างอินเทอร์เน็ต หากไม่มีการบริหารที่ดีก็จะทำให้การสื่อสารข้อมูลเกิดการผิดพลาดขึ้นได้ โปรโตคอลบริหารจัดการเครือข่าย Simple Network Management Protocol (SNMP) จึงเกิดขึ้นเพื่อใช้ในการบริหารจัดการเครือข่าย และติดตามตรวจสอบอุปกรณ์เครือข่ายต่าง ๆ

ระบบบริหารจัดการเครือข่ายแบบค้นหานี้พัฒนาขึ้นมาเพื่อ เป็นระบบบริหารจัดการเครือข่ายที่สามารถค้นหาอุปกรณ์เครือข่ายที่เชื่อมต่อในระบบเครือข่ายได้ โดยใช้โปรโตคอล SNMP เป็นโปรโตคอลซึ่งเป็นโปรโตคอลที่ใช้ในการบริหารจัดการเครือข่ายในการพัฒนาประกอบกับการพัฒนาในรูปแบบ web base application เพื่อให้สามารถประยุกต์ใช้ได้กับทุกเครือข่าย สามารถใช้งานได้ง่าย

ระบบบริหารจัดการเครือข่ายแบบค้นหาที่พัฒนาขึ้นมานี้ สามารถค้นหาอุปกรณ์เครือข่าย และ สามารถนำข้อมูลการเชื่อมต่อที่ได้มาแสดงเป็นแผนภาพโทโปโลยีได้ และสามารถรวบรวมข้อมูลเชิงสถิติของอุปกรณ์มาแสดงผล สามารถแสดงรายการของอุปกรณ์เครือข่าย และสามารถตรวจจับ ข้อความ Trap ที่ถูกส่งออกมาจากอุปกรณ์เครือข่าย เมื่อเกิดเหตุการณ์ต่างๆขึ้นกับอุปกณ์เครือข่ายได้ ทั้งนี้ผู้พัฒนาได้เล็งเห็นว่า หากระบบเครือข่ายมีขนาดค่อนข้างใหญ่แล้ว จะทำให้เป็นการยุ่งยากสำหรับผู้ดูแลเครือข่ายในการเพิ่มและแก้ไขข้อมูลของอุปกรณ์เครือข่ายด้วยตัวเอง หากมีระบบที่สามารถค้นหาอุปกรณ์เครือข่ายได้ด้วยตัวเองก็จะเป็นประโยชน์กับผู้ดูแลระบบ ผู้พัฒนาจึงได้มีการพัฒนาระบบบริหารจัดการเครือข่ายแบบค้นหาขึ้นมาเพื่อเป็นต้นแบบ

Title	Discover Network Mornitoring System
Student	Mr. Ronnarong Srisuwan
Student ID	52660529
Degree	Master of Science
Program	Information Technology
Major	Information System Technology
Acadamic Year	2014
Advisor	Dr. Panwit Tuwanuti

ABSTRACT

The appropriate network system management is essential, especially for those intensive network like internet. The inappropriate management might lead to the failure of message communication. Hence, Simple Network Management Protocol (SNMP) is invented to manage the network and to monitor its network devices.

Discovery network monitoring system is developed, using SNMP protocol, browsing devices connected to the network. In addition, it is developed based on web base application that user friendly and applicable to all networks.

Discovery network monitoring system is capable to search network devices, analyse data and display Network topology, collect statistic data and represent results, listing network devices, and detect trap message that transmitted by network devices. The size and complexcity of network system is the key barrier for network ooperators to add and edit information of network device themselves. Therefore, the developer has developed the system that capable to searching network devices themselves to assist the operators.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้ไม่อาจบรรลุผลสำเร็จได้ หากขาดความกรุณาจากอาจารย์ที่ปรึกษา ดร.ปานวิทย์ ธุวะนุติ ที่ให้ความกรุณา ความช่วยเหลือ คำแนะนำที่ดี ในการพัฒนาโครงการและการปรับปรุง แก้ไขปัญหาต่างๆ มาโดยตลอด

ขอขอบคุณทุกคนที่บริษัทเวสเทิร์นดิจิตอลประเทศไทย ที่คอยสนับสนุน และช่วยเหลือมาโดยตลอด ขอบคุณน้องเกียรติ และน้องนิก ที่เป็นที่ปรึกษาเป็นอย่างดี

ขอขอบคุณอาจารย์คณะเทคโนโลยีสาระสนเทศสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุกท่านที่ ช่วยให้อบรมสั่งสอน และมอบความรู้ ที่สามารถนำมาแก้ไขปัญหาต่างๆ ให้สำเร็จลุล่วงไปได้ด้วยดี และเป็นตัวอย่างที่ดีในการศึกษาเล่าเรียนและการทำงาน

สุดท้ายนี้ขอขอบคุณเพื่อนๆ พี่น้อง และเจ้าหน้าที่ฝ่ายทะเบียนคณะเทคโนโลยีสารสนเทศสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุกคนที่ได้ให้การช่วยเหลือและกำลังใจเพื่อให้โครงงานชิ้นนี้สำเร็จลุล่วงได้โดยสมบูรณ์

รณรงค์ ศรีสุวรรณ์

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญรูป

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

สารบัญตาราง

ตารางที่ หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

เนื่องด้วยปัจจุบัน เทคโนโลยีทางด้านเครือข่ายการสื่อสารข้อมูลมีการพัฒนาอย่างรวดเร็ว และองค์กรต่างๆในปัจจุบันมีการนำเทคโนโลยีด้านเครือการสื่อสารข้อมูลไปใช้ในองค์กรเป็นส่วนมาก ซึ่งการใช้เครือข่ายการสื่อสารข้อมูลนั้นจะมีการติดต่อเพื่อส่งข้อมูลกันทั้งภายในและภายนอกองค์กรเพื่อช่วยขับเคลื่อนให้องค์กรแต่ละแห่งทำงานได้อย่างมีประสิทธิภาพ ดังนั้นเราจะเห็นได้ว่าเครือข่ายการสื่อสารข้อมูลมีความจำเป็นต่อองค์กรหนึ่งๆเป็นอย่างมากและการใช้เครือข่ายการสื่อสารข้อมูลจึงจำเป็นที่จะต้องมีประสิทธิภาพในการทำงานที่สูงเพื่อเป็นการสนับสนุนให้ประสิทธิภาพการทำงานขององค์กรสูงขึ้นด้วย

การที่จะใช้งานเครือข่ายการสื่อสารข้อมูลให้มีประสิทธิภาพองค์กรจำเป็นต้องมีระบบที่ช่วยในการควบคุมจัดการและบริหารเครือข่ายการสื่อสารข้อมูล(Network Management software)ที่มีประสิทธิภาพ ระบบที่ใช้ในการสนับสนุนการบริหารและจัดการเครือข่ายการสื่อสารจึงจำเป็นอย่างมากเพื่อที่ช่วยสนับสนุนการทำงานของผู้ดูแลระบบเครือข่ายการสื่อสาร ซึ่งในระบบจะประกอบไปด้วยส่วนประกอบต่างๆมากมาย ทั้งทางด้านฮาร์ดแวร์ ระบบซอฟต์แวร์ และตัวกลางเชื่อมต่อการสื่อสารข้อมูล ระบบควบคุมจัดการและบริหารเครือข่ายการสื่อสารข้อมูลจะต้องพิจารณาและจัดการและการเข้าถึงการทำงานของอุปกรณ์เหล่านี้ ซึ่งในปัจจุบันเราจะเห็นได้ว่าระบบหรือซอฟต์แวร์ควบคุมจัดการและบริหารเครือข่ายการสื่อสารนั้นมีอยู่มากมายด้วยเช่นกัน มีทั้งระบบที่พัฒนามาเพื่อการค้าและระบบที่ไม่ต้องเสียค่าใช้จ่ายและระบบที่แจกจ่ายต้นฉบับเพื่อให้ผู้อื่นพัฒนาต่อ(open - source) โดยที่ระบบเดิมที่มีอยู่นั้นโดยส่วนมากแล้วจะเป็นที่ผู้ที่ดูแลระบบเป็นจะต้องเป็นผู้ที่เพิ่มเติมรายละเอียดของอุปกรณ์เครือข่ายในระบบ จึงค่อนข้างที่จะยุ่งยากมากหากระบบที่เราต้องการจะควบคุมจัดการและบริหารเครือข่ายนั้นเป็นระบบที่ค่อนข้างใหญ่และมีอุปกรณ์เครือข่ายมาก ทำให้เสียเวลาในการจัดการในขั้นตอนการเพิ่มเติมอุปกรณ์และรายละเอียดของอุปกรณ์เข้าไป

ระบบบริหารจัดการเครือข่ายแบบค้นหาที่จะพัฒนาขึ้นมานี้ จะเข้ามาช่วยในเรื่องการทำงาน ของผู้ดูแลเครือข่ายให้สามารถทำงานได้สะดวกมากขึ้น ทั้งในแง่ของการเพิ่มเติมอุปกรณ์เข้าไปในระบบและในส่วนของการควบคุมจัดการและบริหารเครือข่าย

1.2 วัตถุประสงค์

1. ศึกษาหลักการในการบริหารงานและจัดการเครือข่ายการสื่อสารข้อมูล
2. ศึกษา Simple Network Management Protocol (SNMP) ซึ่งเป็นโปรโตคอลที่ใช้ในการ บริหารงานและจัดการเครือข่ายการสื่อสารข้อมูล และศึกษา Management Information Base (MIB) ซึ่งเป็นส่วนของข้อมูลรายละเอียดต่างๆของอุปกรณ์ที่ถูกบริหาร
3. วิเคราะห์และออกแบบระบบที่จะทำการพัฒนาโดยใช้ ASP.Net และมีการทำงานแบบ web-based ซึ่งมีลักษณะเป็นแบบเวลาจริง (Real Time system)
4. สามารถทำให้มองภาพรวมของเครือข่ายโดยได้ผลลัพธ์ออกมาเป็นโครงสร้างเชิงตรรกะของระบบทั้งหมดที่ต้องการในรูปแบบของโทโพโลยี (Topology) และทราบข้อมูลเกี่ยวกับอุปกรณ์บนเครือข่าย
5. ระบบที่พัฒนาสามารถนำมาใช้งานได้กับระบบเครือข่ายการสื่อสารที่มีอยู่ได้จริงและมีการทำงานที่มีประสิทธิภาพ
6. วิเคราะห์และหาเหตุผลของข้อผิดพลาดที่เกิดขึ้นกับระบบได้ง่ายเพื่อใช้ช่วยแก้ปัญหาที่เกิดขึ้นได้

1.3 ขอบเขตของโครงงาน

1. ระบบสามารถค้นหาและแสดงอุปกรณ์เครือข่ายทั้งหมดที่มีตามหมายเลขไอพีที่กำหนด
2. ระบบสามารถสร้างการเชื่อมต่อไปยังอุปกรณ์เครือข่ายได้โดยทำการวาดเป็นโทโพโลยีไดอะแกรมรูปภาพอุปกรณ์เครือข่ายที่เชื่อมต่อในเครือข่ายได้ถูกต้อง

1.4 วิธีการดำเนินงาน

1. ศึกษาทฤษฎีต่างๆที่เกี่ยวข้องกับโครงงานนี้ ซึ่งมีหัวข้อหลักๆอยู่ดังนี้
   - ทฤษฎีและหลักการในการจัดการเครือข่าย
   - หลักในการจัดการฐานข้อมูลบนฐานข้อมูลของ MIB
   - Simple Network Management Protocol (SNMP)
   - หลักการค้นหาอุปกรณ์บนเครือข่ายด้วยโปรโตคอล SNMP

- หลักการวาดโทโพโลยีของเครือข่าย

2. ศึกษาหลักการและเมธอดต่างๆใน Library SNMP ที่ใช้ภาษา VB (ASP.net)ในการพัฒนา ระบบแบบ web-base อย่างไร
3. ทำการวิเคราะห์และออกแบบขั้นตอนการทำงานในระบบที่กำลังพัฒนา
4. ทำการทดสอบและการวิเคราะห์ผลการทำงานของระบบ
5. สรุปผลการทดสอบระบบและแก้ไขข้อบกพร่องที่เกิดขึ้น

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. ระบบการบริหารและจัดการเครือข่ายการสื่อสารแบบค้นหาสามารถนำมาใช้งานกับเครือข่าย การสื่อสารที่มีอยู่ได้อย่างมีประสิทธิภาพ
2. ระบบการบริหารและจัดการเครือข่ายการสื่อสารแบบค้นหาสามารถช่วยผู้ดูแลระบบในแง่การจัดการอุปกรณ์เครือข่ายได้สะดวกมากขึ้น
3. ผู้ดูแลระบบสามารถมองเห็นภาพรวมของระบบเครือข่าย ได้จากโทโพโลยี ของระบบการบริหารและจัดการเครือข่ายการสื่อสารแบบค้นหา

1.6 โครงสร้างของโครงการ

เนื้อหาของโครงการระบบบริหารดูแลเครือข่ายแบบค้นหา ประกอบด้วยเนื้อหาทั้งหมด 5 บทดังนี้

บทที่ 1 บทนำ จะอธิบายถึงที่มาของปัญหาและความสำคัญของปัญหา เพราะเหตุใดผู้พัฒนาจึงได้พัฒนาระบบบริหารเครือข่ายแบบค้นหาขึ้นมา อธิบายลักษณะและขอบเขตของโครงการที่พัฒนาขึ้นมา วิธีการในการดำเนินการในแต่ละขั้นตอนทั้งการศึกษาทฤษฎีที่เกี่ยวข้องเพื่อนำมาใช้ในการพัฒนาโครงการ รวมไปถึงการคาดการประโยชน์ที่จะได้รับจากโครงการและการพัฒนาโครงการ

บทที่ 2 ทฤษฎีและหลักการที่เกี่ยวข้อง จะอธิบายถึงทฤษฎีต่างๆที่ผู้พัฒนาได้ทำการศึกษามาเพื่อนำมาใช้พัฒนาโครงการซึ่งเนื้อหาจะครอบคลุมเรื่อง ทฤษฎีและหลักการในการบริหารจัดการเครือข่าย, โปรโตคอล SNMPv3 ซึ่งเป็นเป็นหัวใจหลักของการบริหารจัดการเครือข่าย และการใช้ asp.net ที่เกี่ยวข้องกับ การเชื่อมต่อ SNMP

บทที่ 3 การออกแบบ ในบทนี้จะกล่าวถึงวิธีการที่ผู้พัฒนาใช้ในการพัฒนาโครงการ เริ่มตั้งแต่การออกแบบระบบ และการพัฒนาระบบ

บทที่ 4 ทดสอบ เป็นการนำเอาระบบที่พัฒนาขึ้นมาทำการทดสอบให้สามารถใช้งานได้ รวมไปถึงการค้นหาข้อผิดพลาดที่เกิดขึ้นเพื่อนำไปปรับปรุงระบบให้มีประสิทธิภาพดีขึ้น พร้อมทั้งเข้าใจในปัญหาที่เกิดขึ้น

บทที่ 5 สรุป จะกล่าวถึงข้อสรุปของโครงการที่พัฒนาขึ้น สามารถเปรียบเทียบข้อดีข้อเสียของโครงการได้

บทที่ 2
ทฤษฎีและหลักการที่เกี่ยวข้อง

2.1 หลักการจัดการระบบเครือข่าย (Network Management Principle)

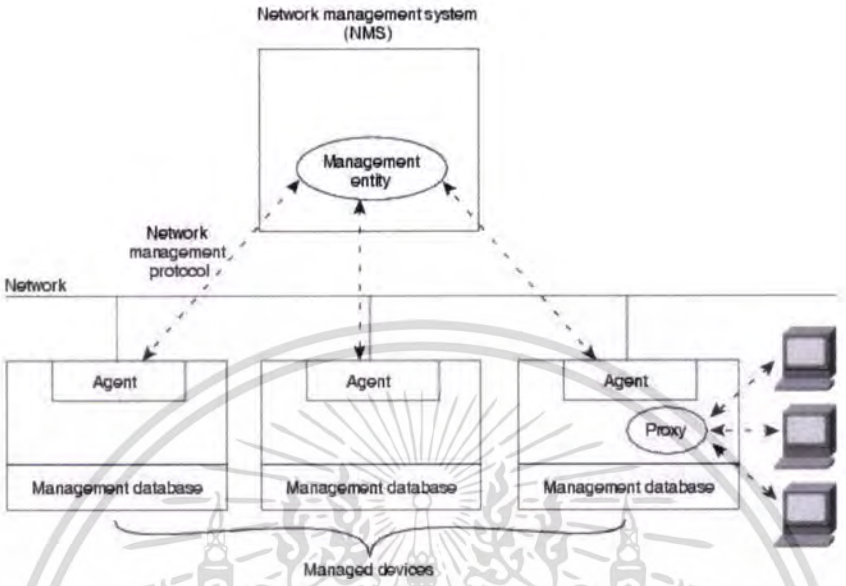
เป็นการที่ให้ความช่วยเหลือแก่ผู้ดูแลระบบเครือข่ายโดยสังเกตและควบคุมพฤติกรรมของเครือข่ายด้วย โปรโตคอลที่ใช้ในการวิเคราะห์ การจัดการระบบเครือข่ายรวมทั้งการกระจายฐานข้อมูล มีการสำรวจอุปกรณ์เครือข่ายแบบอัตโนมัติและมีความสามารถสูงในการสร้างมุมมองกราฟฟิกแบบเวลาจริง(real time) ของโทโพโลยีของเครือข่ายที่เปลี่ยนแปลงและข้อมูลทราฟฟิกของการส่งข้อมูล โดยทั่วไปการจัดการระบบเครือข่ายคือการบริการที่มีเครื่องมือที่เข้ามาช่วยอย่างหลากหลาย,โปรแกรมประยุกต์ และอุปกรณ์เพื่อช่วยผู้ดูแลเครือข่ายในการสังเกต,ควบคุมและการรักษาเครือข่าย ให้เกิดการทำงานที่มีประสิทธิภาพและได้ผลลัพธ์ในการแก้ไขปัญหาต่างๆ รวมถึงมีการจัดเก็บสถานการณ์ต่างๆที่เกิดขึ้นในเครือข่าย ตัวอย่างของระบบจัดการเครือข่าย เช่น NetHam, Cacti, Nagios เป็นต้น

2.2 สถาปัตยกรรมของการจัดการระบบเครือข่าย (Network Management Architecture)

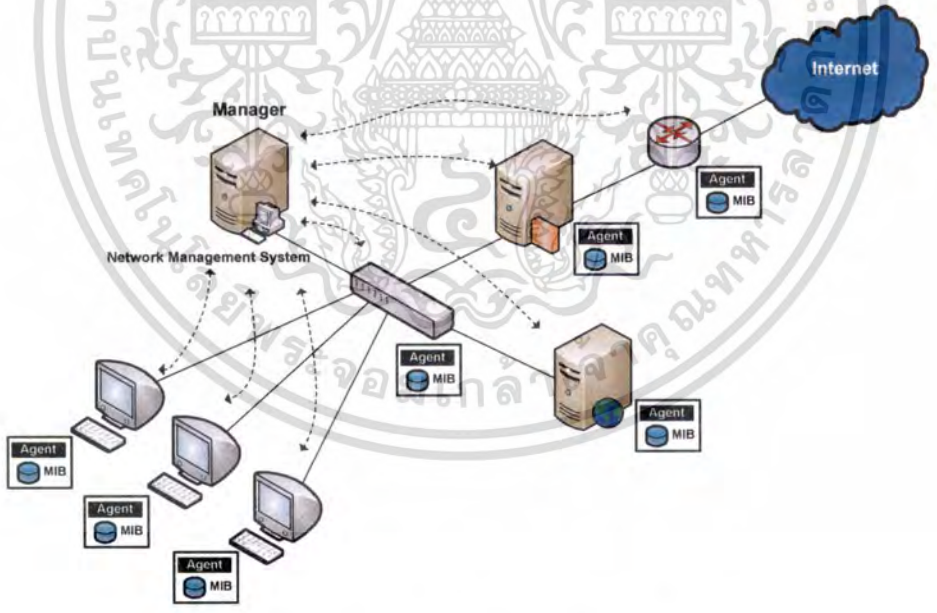
ส่วนใหญ่สถาปัตยกรรมของการจัดการระบบเครือข่ายใช้โครงสร้างพื้นฐานที่เหมือนๆกันและกลุ่มความสัมพันธ์ของอุปกรณ์ที่ต้องการจัดการ เช่นระบบคอมพิวเตอร์ และอุปกรณ์เครือข่ายประเภทอื่นๆ การที่ใช้ระบบที่สามารถมีการแจ้งเตือนเมื่อเกิดปัญหาที่รู้จักหรือเกิดขึ้นโดยทั่วไป ในเวลาที่ได้รับการแจ้งเตือน การจัดการที่มีอยู่ทำการโปรแกรมเพื่อที่จะโต้ตอบโดยการดำเนินการ ซึ่งประกอบด้วย การทำงานที่มีการเตือนล่วงหน้า,บันทึกเหตุการณ์ที่เกิดขึ้น,ปิดระบบ และ พยายามที่จะซ่อมแซมระบบโดยอัตโนมัติ

การจัดการที่มีอยู่นั้นสามารถสำรวจอุปกรณ์เพื่อตรวจสอบค่าเธรสโฮล์ด (Threshold) การสำรวจสามารถทำได้แบบอัตโนมัติหรือผู้ใช้เป็นผู้เริ่มการทำงาน แต่agentในอุปกรณ์ทั้งหมดที่จัดการจะตอบสนองการสำรวจ agent คือส่วนระบบที่มีขั้นตอนการทำงานโดยในอันดับแรกมีการรวบรวมข้อมูลที่เกี่ยวกับอุปกรณ์ที่มีอยู่ แล้วเก็บข้อมูลเหล่านี้ในฐานข้อมูลการจัดการและสุดท้ายมีการจัดหาให้มีการจัดการภายในระบบการจัดการเครือข่าย network management systems (NMSs) โดยผ่าน โปรโตคอลการจัดการเครือข่ายโปรโตคอลที่รู้จักกันดีประกอบด้วย Simple Network

Management Protocol (SNMP) ตัวแทนที่ได้รับหน้าที่ในการจัดการนั้นจัดหาข้อมูลบนตัวแทนที่นอกเหนือจากนี้



รูปที่ 2.1 บรรยายตัวอย่างของสถาปัตยกรรมการจัดการเครือข่าย



รูปที่ 2.2 ตัวอย่างการเชื่อมต่อระบบจัดการเครือข่าย

2.3 รูปแบบการจัดการเครือข่ายตามมาตรฐาน ISO (ISO Network Management Model)

International Organization for Standardization (IOS) มีการพัฒนาโครงสร้างสำหรับการจัดการของเครือข่ายในพื้นฐานของ Structure of Management Information (SMI) โดยโครงสร้างมีการแบ่งแยกกระบวนการการจัดการเครือข่ายออกเป็น 5 ฟังก์ชั่นหลักๆ แต่ละฟังก์ชั่นจะมีความสัมพันธ์กับกระบวนการการจัดการ IT ระดับสูง คือ

2.3.1 Performance Management

เป็นตัวชี้วัดและหลักเกณฑ์ของประสิทธิภาพของเครือข่ายที่มีอยู่อย่างหลากหลาย ดังนั้นประสิทธิภาพระหว่างเครือข่ายสามารถถูกรักษาในระดับที่ยอมรับได้ ตัวอย่างของตัวแปรประสิทธิภาพ เช่น ค่าเปอร์เซ็นต์การใช้งานบนเครือข่าย (Utilization), จำนวนข้อมูลเข้าและออกในช่วงเวลาหนึ่งๆของเครือข่าย (Byte), แพกเกต(Packet) เป็นต้น
การจัดการประสิทธิภาพรวมถึงขั้นตอนหลัก 3 ขั้นตอน

1. ข้อมูลเชิงประสิทธิภาพถูกรวบรวมบนตัวแปรที่ผู้ดูแลเครือข่ายสนใจ
2. ข้อมูลถูกวิเคราะห์เพื่อกำหนดระดับปกติ เป็นเกณฑ์มาตรฐาน
3. ค่าเธสโฮล์ ที่เหมาะสมที่เกี่ยวข้องกับเครือข่ายถูกกำหนดสำหรับแต่ละตัวแปรทสำคัญ

ดังนั้นเมื่อค่าตัวแปรมากกว่า ค่าเธสโฮล์ จะชี้บอกถึงปัญหาที่เกิดขึ้นกับเครือข่าย การจัดการที่มีอยู่สามารถสังเกตเฝ้าระวังตัวแปรของประสิทธิภาพได้อย่างต่อเนื่อง เมื่อค่าเชิงประสิทธิภาพมากกว่าค่าเธสโฮล์ จะมีการแจ้งเตือนและส่งไปให้ระบบการจัดการเครือข่าย แต่ละขั้นตอนได้อธิบายในส่วนกระบวนการตั้งค่าของระบบโต้ตอบ เมื่อประสิทธิภาพเริ่มไม่เป็นที่ยอมรับเพราะเกินกว่าค่าเธสโฮล์ที่ผู้ใช้กำหนดไว้ ระบบจะโต้ตอบโดยการส่งข้อความแล้วการจัดการประสิทธิ -ภาพจึงยอมรับให้มีการเริ่มการทำงาน ตัวอย่างการจำลองเครือข่ายที่วางแผนจะทำให้เครือข่ายที่ขยายเติบโตนั้นส่งผลต่อระบบเมตริกที่เกี่ยวข้องกับประสิทธิภาพของเครือข่ายอย่างไร ดังนั้นการจำลองสามารถแจ้งเตือนผู้ดูแลระบบให้ทราบปัญหาที่ใกล้จะเกิดขึ้น ทำให้เป็นตัววัดเพื่อให้ขัดขวางพฤติกรรมนั้นล่วงหน้า

2.3.2 Configuration Management

เป็นกระบวนการเก็บข้อมูลจากเครือข่ายและใช้ข้อมูลในการจัดการตั้งค่าอุปกรณ์เครือข่ายทั้งหมด ซึ่งประกอบด้วย

1. การเก็บข้อมูลเกี่ยวกับองค์ประกอบของเครือข่าย(network configuration)ปัจจุบัน

2. การใช้ข้อมูลทำการแก้ไของค์ประกอบของเครือข่าย(network configuration)อุปกรณ์
3. การเก็บข้อมูล,การดูแลรักษาข้อมูลที่มีให้นั้นใหม่อยู่เสมอ

การสร้างรายงานจากข้อมูลที่ได้การทำ Configuration management ประกอบด้วยขั้นตอนการทำงานดังนี้

1. การรวบรวมข้อมูลเกี่ยวกับสภาวะแวดล้อมของเครือข่ายล่าสุด ข้อผิดพลาดในการเก็บข้อมูลจะทำให้ผู้ดูแลเสียเวลาในการแก้ไขปัญหาเครือข่าย ที่เกิดจากองค์ประกอบ ที่ผิดพลาดแบบง่ายๆ การเก็บข้อมูลสามารถทำได้แบบ manual โดยผู้ดูแล และแบบอัตโนมัติ โดยระบบ

2. การใช้ข้อมูลเพื่อแก้ไของค์ประกอบของอุปกรณ์เครือข่าย จากการที่สภาวะแวดล้อมของอุปกรณ์เครือข่าย มีการเปลี่ยนแปลงอยู่เสมอ ดังนั้นความสามารถในการแก้ไของค์ประกอบแบบ real time เป็นสิ่งที่จำเป็น การแก้ไขอาจทำได้แบบ manual หรืออัตโนมัติ ขึ้นอยู่กับรูปแบบการเก็บข้อมูลว่าเป็นแบบ manual หรืออัตโนมัติ

3. การเก็บข้อมูล, ดูแลรักษาข้อมูล รายการของอุปกรณ์ให้ใหม่อยู่เสมอ ในทุกๆส่วนของเครือข่าย และการสร้างรายงานแบบ ต่างๆ

ประโยชน์ที่ได้จากการทำ Configuration Management

ผลที่ได้อย่างแรกคือการเพิ่มความสามารถของผู้ดูแลที่จะควบคุมองค์ประกอบของอุปกรณ์เครือข่าย ซึ่งทำได้โดยการเสนอการเข้าถึงข้อมูลองค์ประกอบที่สำคัญของแต่ละอุปกรณ์ ในระบบที่ซับซ้อนขึ้นจะช่วยให้ผู้ดูแลเปรียบเทียบองค์ประกอบที่ใช้งานอยู่ (running configuration) กับองค์ประกอบที่เก็บไว้ในระบบ และทำการเปลี่ยนองค์ประกอบได้ง่ายตามต้องการ

ในบางกรณีที่อุปกรณ์มีการแก้ไข เช่นการที่ต้องแก้ไขอินเตอร์เฟซที่ทำให้เกิดข้อผิดพลาดบนส่วนของ LAN โดยการใช้เครื่องมือ configuration management สามารถทำ remote configuration มายังอุปกรณ์เพื่อยกเลิกการใช้งาน interface นั้น แล้วทำการตรวจสอบ configuration ของอินเตอร์เฟซและสังเกตว่ามีการตั้งค่า configure ที่ผิดพลาดทำให้เกิดข้อผิดพลาดขึ้น การใช้เครื่องมือ configuration management ทำให้สามารถแก้ไขค่า configure ที่ผิดพลาดให้ถูกต้องและทำการ active interface นั้นขึ้นมาใหม่

2.3.3 Accounting Management

เป็นตัววัดประสิทธิภาพที่ได้จากปัจจัยของเครือข่ายทำให้ผู้ใช้หรือกลุ่มผู้ใช้บนเครือข่ายโดยถูกควบคุมดูแลได้อย่างเหมาะสม ดังนั้นการควบคุมดูแลทำให้เกิดปัญหาน้อยลง และ มีการเข้าถึงเครือข่ายได้อย่างถูกต้องของผู้ใช้ทุกคนให้ได้มากที่สุด เหมือนกับ performance management

โดยขั้นตอนแรก accounting management เป็นการหาค่าการใช้ประโยชน์ของทรัพยากรที่สำคัญในเครือข่ายทั้งหมด การวิเคราะห์ของผลลัพธ์ให้เข้าใจในรูปแบบที่ใช้ในปัจจุบัน และส่วนแบ่งที่ใช้ให้เกิดประโยชน์สามารถถูกตั้งค่าได้ ข้อเท็จจริงบางส่วนคือมีความต้องการให้มีการเข้าถึงที่ดีที่สุดจากจุดนี้ และไปเรื่อยๆ การประมาณการใช้ทรัพยากรสามารถให้ทำรายการของข้อมูลที่ดีเท่ากับข้อมูลที่ใช้เป็นทรัพย์สินที่ถูกต้องต่อไปและเป็นการใช้ทรัพยากรให้เกิดประโยชน์สูงสุด

2.3.4 Fault Management

เป็นกระบวนการที่ใช้กำหนดตำแหน่งและแก้ไขปัญหาเครือข่าย ที่เรียกว่า Fault (ข้อผิดพลาด) ซึ่งจากการที่ Network management มีการทำงานย่อยรวมอยู่หลายงาน Fault management เป็นงานที่จัดว่ามีความสำคัญสูงสุด ซึ่งประกอบด้วย

1. การระบุการเกิดของข้อผิดพลาดบน data network
2. การหาสาเหตุของข้อผิดพลาด
3. การแก้ไขข้อผิดพลาด(ถ้าทำได้)

การเก็บรวบรวมข้อมูลที่ใช้ในการระบุปัญหา ต้องทำการรวบรวมข้อมูล ที่เกี่ยวข้องกับสถานะของเครือข่าย ซึ่งจะมีวิธี 2วิธี

1. ข้อมูลที่เกี่ยวข้องกับ สถานการณ์วิกฤติของเครือข่าย (Critical network event) ที่ถูกส่งมาให้โดยอุปกรณ์เครือข่าย ในขณะที่เกิด ข้อผิดพลาดขึ้น เช่น Link fail, การที่อุปกรณ์ restart หรือการที่โฮสต์ทำการตอบสนองช้า โดยส่วนใหญ่การเชื่อถือข้อมูลเพียงบางเหตุการณ์จะไม่เพียงพอที่นำมาใช้สำหรับการทำFault management ที่มีประสิทธิภาพ ตัวอย่าง เช่น ถ้าอุปกรณ์เครือข่ายไม่สามารถทำงานต่อได้อย่างสมบรูณ์ ก็ไม่สามารถส่ง event ต่างๆได้ดังนั้น Fault management tool ที่ใช้ เพียงบาง สถานการณ์วิกฤติของเครือข่าย (Critical network event) ก็อาจจะไม่มีการอัพเดตกับสถานะของอุปกรณ์เครือข่าย

2. การ polling ไปยังอุปกรณ์เครือข่ายเป็นช่วงๆ จะช่วยทำให้พบปัญหาที่เกิดขึ้นได้ขึ้นอยู่กับช่วงเวลาที่ใช้ polling อย่างไรก็ตามต้องยอมรับผลของการใช้วิธีนี้ ความเร็วของการตรวจพบขึ้นอยู่กับความถี่ของการ polling ซึ่งขึ้นกับการเปรียบเทียบความถี่ของการ polling แล้วทำให้พบปัญหาได้เร็วกับแบนด์วิดท์ (bandwidth) ที่ถูกใช้ไป ดังนั้นถ้าต้องการให้พบปัญหาได้เร็วที่สุดต้องใช้แบนด์วิดท์ที่มาก ซึ่งปัจจัยอื่นที่ใช้พิจารณาเมื่อทำการตัดสินในการกำหนดค่าช่วงเวลา polling time คือ จำนวนของอุปกรณ์ที่ทำการ poll และแบนด์วิดท์ของ link นั้นๆการกำหนดว่าจะใช้ข้อผิดพลาดค่าใดเพื่อนำมาจัดการระบบ data network ซึ่งควรถูกกำหนดโดยปัจจัยดังต่อไปนี้

- ขอบเขตของการดูแลเครือข่ายซึ่งมีผลต่อจำนวนของข้อมูลที่จะเก็บจากอุปกรณ์เครือข่าย
- ขนาดของเครือข่าย

Fault management tools ต่างๆที่ใช้ตั้งแต่ใช้ง่ายๆจนถึงเครื่องมือที่พิเศษที่ออกแบบมาทำงาน Fault management โดยเครื่องมือที่ง่ายๆสามารถใช้หาจุดที่เกิดปัญหาได้แต่ไม่สามารถบอกสาเหตุได้ ส่วน เครื่องมือที่มีความซับซ้อนมากกว่าจะใช้ข้อได้เปรียบของโฮสต์ (host) และอุปกรณ์เครือข่ายเพื่อส่ง สถานการณ์วิกฤติของเครือข่าย (Critical network event) ซึ่งสามารถใช้หาสาเหตุของปัญหาได้ ส่วน Advance tool สามารถทำได้เหนือกว่าอีกระดับโดยสามารถแก้ปัญหาที่เกิดขึ้นให้ทันที

รูปแบบของการรายงาน Fault รูปแบบที่ใช้มีความสำคัญเช่นกัน โดยปกติจะแสดงได้ 3 รูปแบบดังนี้

- ข้อความ (Text)
- รูป (Graphic)
- เสียง (Voice)

โดยแบบข้อความเป็นแบบที่ควรเลือกใช้ในเบื้องต้นเพราะสามารถทำงานได้บนจอหรือ terminal ได้ทุกแบบ แต่อย่างไร ก็ตามแบบรูปภาพจะดูแล้วสื่อความหมายได้ดีที่สุด โดยการแสดงผลแบบนี้ต้องใช้หน้าจอสีที่ปกติใช้กับเครื่องมือที่ใช้บน Network management system อยู่แล้ว โดยถ้าไม่มีสีก็สามารถทำให้รูปภาพกระพริบได้ ส่วนแบบที่ใช้เสียงมีจุดเด่น ในการเตือนให้ผู้ดูแลทราบได้เร็วที่สุดในการแสดงผลถ้าสามารถระบุได้ถึงจุดที่มีผลกระทบด้วยก็จะทำให้สามารถแยกแยะปัญหาได้เร็วขึ้น

2.3.5 Security Management

จุดประสงค์ของ Security Management คือการควบคุมการเข้าถึงทรัพยากรบนเครือข่าย ซึ่งสอดคล้องกับนโยบายที่เฉพาะ ดังนั้นเครือข่ายไม่สามารถถูกก่อกวนหรือทำลายได้ทั้งแบบเจตนาหรือไม่เจตนา และ มีการรับรู้ทันทีเมื่อมีข้อมูลที่ไม่สามารถเข้าถึงโดยที่ไม่ได้รับการอนุญาติที่เหมาะสมระบบย่อยในSecurity Management ตัวอย่าง เช่น สามารถเฝ้าระวังหรือสังเกตจากบันทึกพฤติกรรมของผู้ใช้ที่เข้ามาใช้ทรัพยากรบนเครือข่าย และ สามารถปฏิเสธการเข้าถึงของรหัสของผู้ใช้ในการเข้าถึงที่ไม่เหมาะสม

ระบบย่อยใน Security Management ทำงานโดยใช้หลักการในการแบ่งทรัพยากรบนเครือข่ายให้กับผู้ที่ได้รับอนุญาติและผู้ที่ไม่ได้รับอนุญาติ สำหรับผู้ใช้บางคนเข้าถึงทรัพยากรบางส่วนที่ไม่เหมาะสม โดยทั่วไปจะเป็นเพราะผู้ใช้เป็นคนภายนอกบริษัท สำหรับเครือข่ายอื่นๆภายในผู้ใช้สามารถเข้าถึงข้อมูลที่สร้างจากแผนกงานต่างๆก็เป็นสิ่งที่ไม่เหมาะสม อย่างการเข้าถึงไฟล์ที่เกี่ยวกับทรัพยากรบุคคล

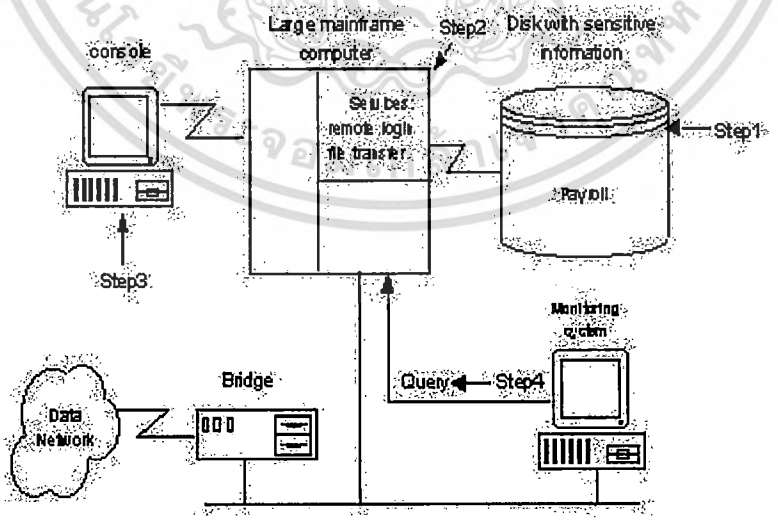
ระบบย่อยใน Security Management แสดงการทำงานหลายวิธี มีการกำหนดทรัพยากรบนเครือข่ายและให้มีการจับกลุ่มระหว่างทรัพยากรกับกลุ่มผู้ใช้ที่อนุญาติ และมีการเฝ้าสังเกตที่จุดที่มีการเข้าถึงทรัพยากรและบันทึกการเข้าถึงทรัพยากรที่ไม่เหมาะสม

ประโยชน์ของการทำ Security Management

สิ่งที่ต้องคำนึงอย่างแรกสำหรับผู้ใช้หลายๆคนเกี่ยวกับการต่อเครื่องแม่ข่ายไปยัง data network คือแนวโน้มของการขาด Security ของข้อมูลที่มีความสำคัญที่อยู่บน host เพื่อหลีกเลี่ยงปัญหานี้การที่เครื่องแม่ข่าย ทำงานกับข้อมูลที่มีความสำคัญสามารถหลีกเลี่ยงการเชื่อมต่อเครือข่ายและส่งผ่านข้อมูลได้โดยใช้ movable media เช่น เทปแม่เหล็ก,Optical disc และวิธีอื่นๆ โดยวิธีนี้ถ้าผู้ใช้ที่มี physical security access ไปยัง host สามารถเข้าถึงข้อมูลที่มีความสำคัญได้ อย่างไรก็ตามแม้ว่าวิธีนี้จะปลอดภัย แต่ก็ไม่สะดวกที่จะใช้งาน

การตั้งค่าที่เหมาะสมและการบำรุงรักษา Security management ที่ดี ทำให้สามารถที่จะเสนอแนวทางปฏิบัติได้หลายอย่าง เพื่อบรรเทาความกังวลเรื่องความปลอดภัย ของผู้ใช้และเพิ่มความเชื่อมั่นในประสิทธิภาพของเครือข่าย และ security การสร้างความเชื่อมั่นและการป้องกันข้อมูลที่สำคัญเป็นผลประโยชน์หลักที่ได้จากการทำ Security management

ผลเสียของการที่ไม่มี Security management ในเครือข่ายสามารถแสดงให้เห็นได้ไม่ยาก โดยสมมุติว่า private data network ขององค์กร เชื่อมต่อไปยัง public data network และถ้าคอมพิวเตอร์ภายใน เครือข่ายของบริษัทมีข้อมูลเงินเดือนอยู่ให้บริการข้อมูลกับใครก็ได้ที่มาร้องขอ ซึ่งผลของการที่ไม่จำกัดสิทธิการ เข้าถึงไปยังข้อมูลที่สำคัญอาจทำให้เกิดความเสียหายกับองค์กรได้



รูปที่ 2.3 ขั้นตอนการทำ Security Management

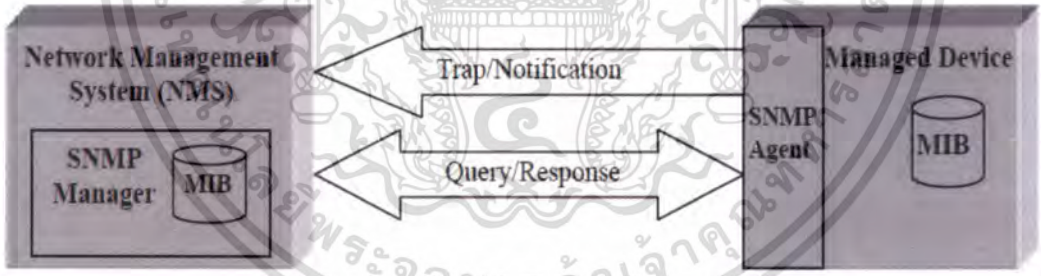
เหตุผลในการบริหารและจัดการเครือข่ายการสื่อสาร

- เพื่อตรวจหาสถานะการทำงานของอุปกรณ์และการสื่อสารภายในครือข่าย

- เพื่อการบริหารจัดการเครือข่ายขนาดใหญ่ที่ซับซ้อนได้ดียิ่งขึ้น
- เพื่อการตรวจสอบสถานะของ threshold ที่ถูกกำหนดไว้
- เพื่อจัดเตรียมเครือข่ายไว้สำหรับอุปกรณ์ชนิดใหม่ๆ
- เพื่อความสะดวกในการเปลี่ยนแปลงคุณลักษณะต่างๆของระบบเครือข่าย
- เพื่อการใช้งานเครือข่ายการสื่อสารของผู้ใช้ให้มีประสิทธิภาพมากยิ่งขึ้น
- เพื่อทำการปรับประสิทธิภาพและความสามารถในการทำงานของเครือข่ายให้สมดุลกัน
- เพื่อรักษาต้นทุนในการจัดการเครือข่าย

2.4 SNMP (Simple Network Management Protocol)

SNMP เป็น Network Management Protocol ตัวหนึ่งสำหรับการบริหารจัดการเครือข่าย ซึ่งทำงานบน Application Layer ของชุดโปรโตคอล TCP/IP ซึ่งจะช่วยให้ผู้ดูแลระบบเครือข่ายสามารถจัดการเครือข่ายได้อย่างมีประสิทธิภาพ สามารถวิเคราะห์ปัญหา และให้ข้อมูลเพื่อใช้วางแผนในการปรับปรุงเครือข่าย การจัดการเครือข่ายด้วยโปรโตคอล SNMP จะประกอบด้วยด้วยองค์ประกอบหลักอยู่ 4 อย่าง คือ ใช้แนวคิดของ ผู้จัดการ(Manager) และ ตัวแทน(Agent) ชุดคำสั่งที่ใช้สำหรับการสื่อสารแลกเปลี่ยนข้อมูล และฐานข้อมูลสารสนเทศ(Management Information Base) หรือ "MIB"



รูปที่ 2.4 องค์ประกอบของการจัดการเครือข่ายด้วยโปรโตคอล SNMP

ซึ่ง Manager นั้นส่วนใหญ่ก็จะเป็น Host(PC) ซึ่งจะคอยควบคุมดูแลและติดตามกลุ่มของ Agent มักจะเป็น อุปกรณ์เครือข่าย SNMP ถูกออกแบบมาให้ทำงานบน Application Layer ดังนั้นจึงสามารถติดตาควบคุมอุปกรณ์ที่ผลิตมาต่างกันได้ รวมไปถึงการติดตั้งทางกายภาพที่แตกต่างกันด้วย

สถานีบริหารจัดการ คือ "Manager" จะเป็นเครื่อง PC ที่มี ซอฟต์แวร์แมเนเจอร์ทำงานอยู่ ส่วนสถานีที่ถูกบริหารจัดการ คือ "Agent" มักจะเป็นอุปกรณ์เครือข่ายซึ่งจะมีซอฟต์แวร์เอเจนต์

ทำงานอยู่ เพื่อทำหน้าที่รอรับคำสั่งการปรับค่าการทำงานของอุปกรณ์จาก Manager และรอรับคำสั่งการสอบถามจาก Manager มาแปลผลเพื่อดึงเอาข้อมูลที่ต้องการในฐานข้อมูล MIB ส่งกลับไปให้กับ Manager นอกจากนี้ยังทำหน้าที่ในการแจ้งเตือนเหตุการณ์บางอย่างที่เกิดขึ้นภายในอุปกรณ์ให้กับ Managerโดยไม่ต้องมีการร้องขอจาก Manager ซึ่งจะสรุปการบริหารจัดการเครือข่ายโดย SNMP จะมีแนวคิดพื้นฐานดังนี้

1. Manager จะร้องขอข้อมูลกับ Agent และจะนำข้อมูลที่ได้รับจาก Agent ไปตรวจสอบพฤติกรรม เช่น นำค่าของจำนวน Packet ไปตรวจสอบความคับคั่งของเครือข่าย ซึ่งการร้องขอข้อมูลจาก Agent หรือการเฝ้าติดตามการทำงานของอุปกรณ์ต่างๆในเครือข่ายนั้นจะใช้วิธีการโพล (Polling) อุปกรณ์ที่มีซอฟต์แวร์เอเจนต์ทำงานอยู่ นั่นคือ Manager จะคอยส่งคำสั่งสอบถามข้อมูลตามช่วงเวลาไปยังตัว Agent ต่างๆ ซึ่งจะเห็นได้ว่าจะทำให้แพ็คเก็ตในการจัดการเครือข่ายเป็นจำนวนมาก

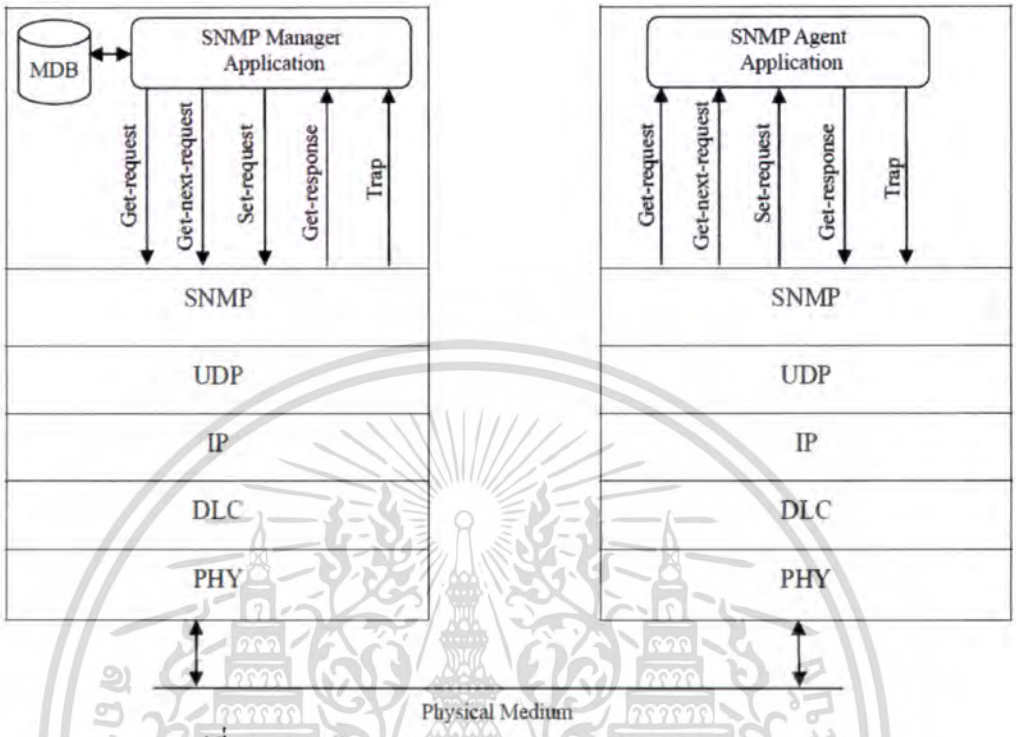
2. Manager สั่งให้ Agent ดำเนินการทำงานโดยทำการเปลี่ยนค่าใหม่ในฐานข้อมูลของ

3. Agent สามารถที่จะช่วยเหลือกระบวนการบริหารจัดการโดยการส่งข้อความเตือน (Trap) ไปยัง Manager เมื่อมีสถานะไม่ปกติ เช่น มีการเปลี่ยนแปลงสถานะของอินเทอเฟส Agent จะส่งข้อความเตือนไปยัง Manager ทันทีเป็นต้น คำสั่ง Trap เป็นคำสั่งหนึ่งที่ช่วยลดจำนวนแพ็คเก็ตของการจัดการเครือข่ายได้ เพราะ Agent สามารถสร้างคำสั่งเพื่อแจ้งเตือนไปยัง Manager โดยที่ Manager ไม่จำเป็นต้องส่งคำสั่งเพื่อร้องขอข้อมูลอยู่ตลอดเวลา

ในส่วนของฐานข้อมูล MIB จะมีอยู่ทั้งใน Manager และ Agent ซึ่งในฐานข้อมูลนี้จะเก็บตัวแปรของออปเจ็คต์ต่างๆเพื่อใช้ในการอ้างถึงข้อมูลของอุปกรณ์ เช่น ชื่อของอุปกรณ์ (sysName) จำนวนเวลาทั้งหมดที่อุปกรณ์ทำงานต่อเนื่องกันมา(sysUptime) จำนวนแพ็กเก็ตขาเข้าทั้งหมด (ifInOctets) เป็นต้น ซึ่ง MIB ถูกอธิบายและกำหนดขึ้นตามโครงสร้างของการจัดการข้อมูลสารสนเทศ (Structure of Management Information : SMI) โดยผู้ผลิตแต่ละรายสามารถนำ SMI ไปใช้เป็นมาตรฐานในการกำหนดและอธิบายกลุ่มของออบเจ็คสำหรับใช้ในการจัดการอุปกรณ์ของตนเองได้

SNMP ได้มีการพัฒนามาอย่างต่อเนื่อง จาก SNMPv1 จนมาถึงปัจจุบันนี้คือ SNMPv3 โดยที่ เวอร์ชั่นที่ 1 และ เวอร์ชั่นที่ 2 มีลักษณะของสถาปัตยกรรมและการทำงานที่คล้ายคลึงกันโดยในเวอร์ชั่นที่ 2 ได้พัฒนาขึ้นเพื่อยกระดับความสามารถและประสิทธิภาพของการทำงานจากเวอร์ชั่นที่ 1 เช่น การเพิ่มสั่งสำหรับใช้ในการจัดการเครือข่าย, การเพิ่มกลุ่มของออบเจ็คภายในฐานข้อมูล MIB เป็นต้น และในเวอร์ชั่นที่ 3 จะเป็นการพัฒนาเพื่อแก้ปัญหาความไม่ปลอดภัยในโปรโตคอล SNMP

2.5 SNMPv1 (Simple Network Management Protocol version 1)

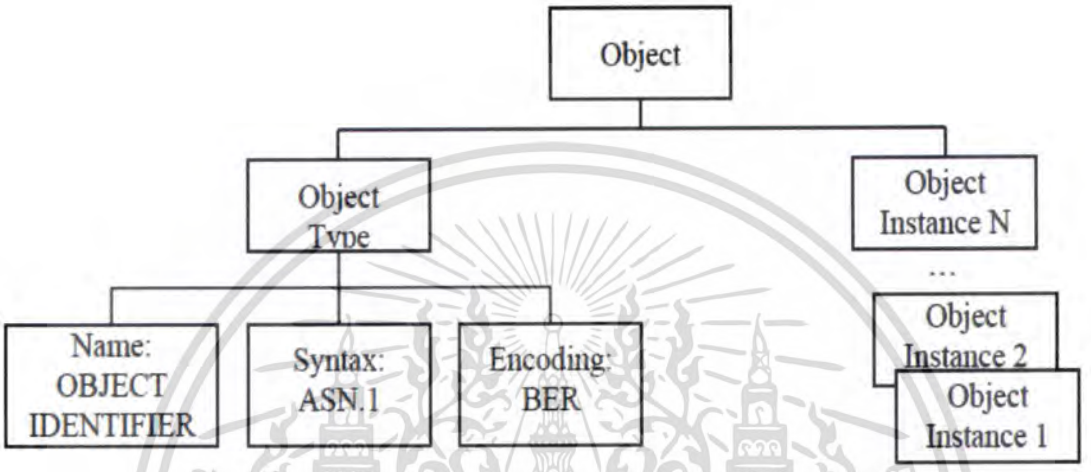


รูปที่ 2.5 สถาปัตยกรรมของ SNMPv1[MANI2000]

อธิบายถึงภาพรวมของสถาปัตยกรรมของโปรโตคอล SNMPv1 ซึ่งได้แสดงการรับส่งข้อมูลจัดการเครือข่ายระหว่าง Manager กับ Agent ผ่านทางชุดโปรโตคอล TCP/IP ซึ่ง SNMP เป็นโปรโตคอลที่ทำงานในระดับ Application Layer โดยเลือกใช้โปรโตคอล UDP ในระดับ Transport Layer เพื่อส่งผ่านข้อมูลผ่านทางพอร์ต 161 และพอร์ต 162 สำหรับใช้ในการส่ง Trap ซึ่งโปรโตคอล SNMPv1 มีคำสั่งพื้นฐานในการติดต่อ สื่อสารเพื่อแลกเปลี่ยนข้อมูลการจัดการระหว่าง Manager กับ Agent อยู่ 5 คำสั่งคือ get-request, get-next-request, set-request จะถูกสร้างจากฝั่ง Manager ไปยัง Agent และ get-response กับ Trap จะถูกสร้างจากฝั่ง Agent ไปยัง Manager ฐานข้อมูลของแมเนเจอร์ในระบบจัดการเครือข่ายจะมีอยู่สองอย่าง คือ ฐานข้อมูลที่มีอยู่จริงซึ่งจะให้เก็บค่าออบเจ็คที่ได้จากการส่งคำสั่งสอบถามข้อมูลโดยการโพลจากเอเจนต์ซึ่งฐานข้อมูลชนิดนี้จะมีขนาดใหญ่และมีการเปลี่ยนแปลงบ่อย และอีกฐานข้อมูลหนึ่งเป็นฐานข้อมูลแบบเสมือนที่มีอยู่ที่ตัวเอเจนต์ด้วย คือ ฐานข้อมูล MIB ซึ่งจะใช้เก็บข้อมูลออบเจ็คและค่าคงที่ที่ไม่ค่อยมีการเปลี่ยนแปลงเพื่อใช้สำหรับการอ้างถึงค่าของข้อมูลที่ต้องการ

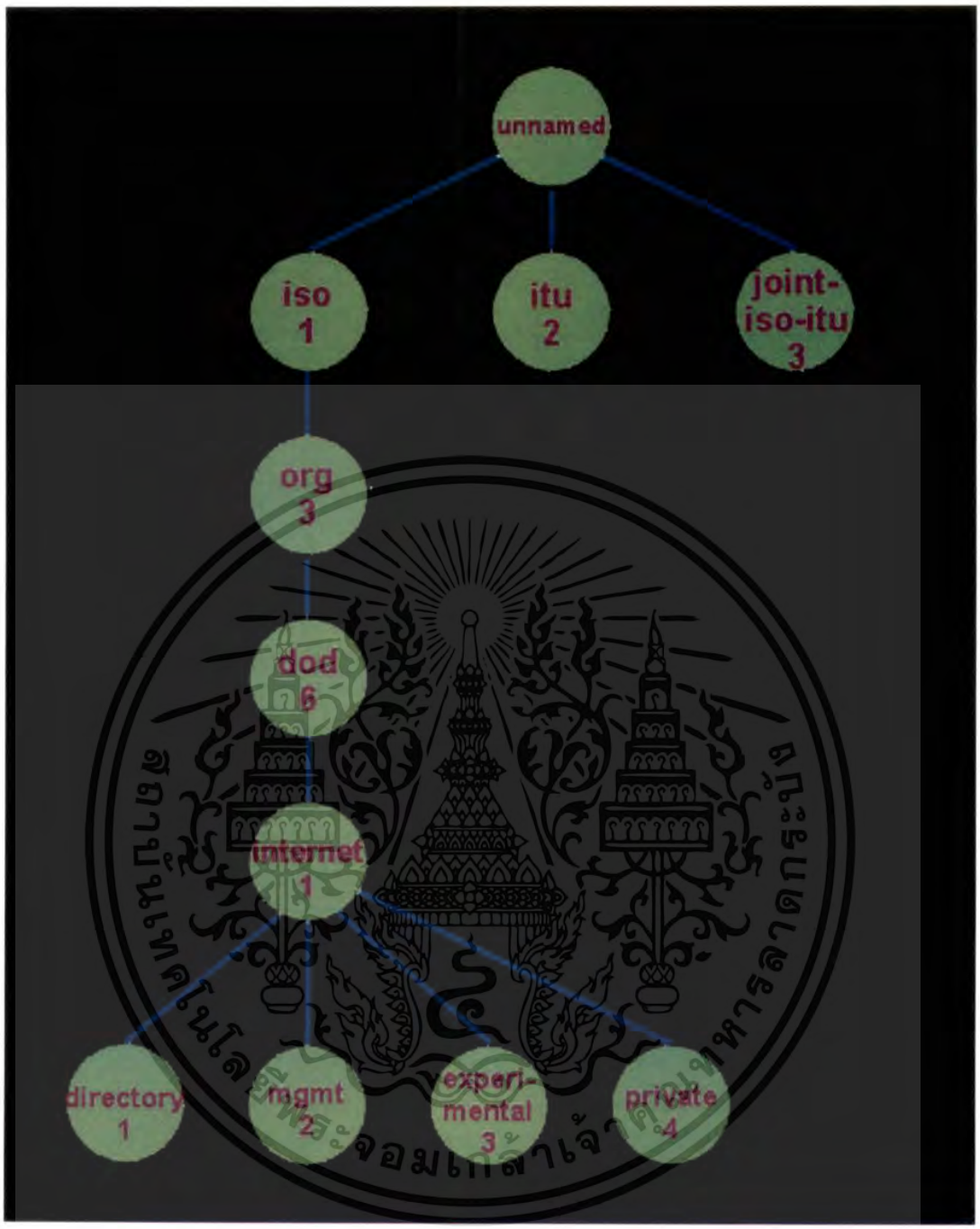
2.5.1 Structure of management Information (SMI)

SMI (Structure of Management Information) ใช้สำหรับกำหนดรายละเอียดและโครงสร้างของ managed object คือ ออบเจ็คหนึ่งในฐานข้อมูล MIB หรืออาจจะหมายถึงอุปกรณ์ต่างๆในเครือข่ายที่สามารถถูกจัดการได้จากระบบจัดการเครือข่าย โดยมีชนิดของออบเจ็ค (object type) และตัวแทนของออบเจ็ค (object instance) เป็นส่วนประกอบ



รูปที่ 2.6 ส่วนประกอบของ Managed Object [MANI2000]

SMI นั้นจะกำหนดรายละเอียดเฉพาะในส่วนของ object type เท่านั้น ในส่วนของ object instance ไม่ได้กำหนดรายละเอียดไว้ใน object type และใน object type เดียวกันสามารถมีได้อย่างน้อยหนึ่ง object instance.ออบเจ็คในฐานข้อมูล MIB มีโครงสร้างแบบต้นไม้ (Management Information Tree: MIT) โดยมีโหนดรากหนึ่งโหนดอยู่บนสุดและมีโหนดอื่นๆอยู่ภายใต้โหนดรากนี้ในระดับต่างๆ



รูปที่ 2.7 โครงสร้างข้อมูลการจัดการแบบต้นไม้ของ OSI

ในแต่ละโหนดจะใช้แทนหนึ่งออบเจ็คที่ประกอบด้วยชื่อของออบเจ็คและตัวเลขจำนวนเต็มที่มีค่าไม่ซ้ำกับโหนดอื่นๆเพื่อใช้เป็นตัวระบุหรือใช้อ้างถึงในแต่ละออบเจ็ค ซึ่งการอ้างถึงออบเจ็คนั้นจะใช้ตัวเลขและใช้จุดคั่นระหว่างตัวระบุของแต่ละออบเจ็คโดยออบเจ็คที่ใช้ในเครือข่ายอินเตอร์เน็ตจะอยู่ในระดับที่ 4 ภายใต้โหนด dod (Department of Defense) และมีตัวระบุเท่ากับ 6 ดังนั้นการอ้างถึงออบเจ็คนี้ได้เท่ากับ 1.3.6

Object type จะประกอบด้วย ชื่อ, Syntax และ การเข้ารหัส โดยสำหรับชื่อ จะใช้ในการระบุหรืออ้างถึงออบเจ็คซึ่งจะต้องมีค่าที่ไม่ซ้ำกันกับออบเจ็คอื่น และจะใช้ภาษา Abstract Syntax Notation (ASN.1) ในการกำหนดรายละเอียดของ Syntax ของแต่ละ object type และส่วนของการเข้ารหัสจะใช้ Basic Encoding Rule (BER) ในการเข้ารหัสของการส่งข้อมูลไปมาระหว่างแมเนเจอร์และเอเจนต์ Name ชื่อจะต้องไม่ซ้ำกันในแต่จะออบเจ็ค โดยการระบุด้วย DESCRIPTOR และ OBJECT IDENTIFYER ที่สัมพันธ์กัน

สำหรับใน SNMPv1 นั้นจะมีออบเจ็คย่อยภายใต้ internet อยู่ 4 ออบเจ็ค คือ

1. directory(1) สงวนเอาไว้ใช้ในอนาคต → OBJECT IDENTIFIER ::={internet 1}
2. mgmt(2) ใช้ในการเก็บออบเจ็คมาตรฐานทั้งหมดที่กำหนดขึ้นโดย IETF → OBJECT IDENTIFIER ::={internet 2}
3. experimental(3) ใช้สำหรับเก็บออบเจ็คในการทดลอง → OBJECT IDENTIFIER ::={internet 3}
4. private(4) ใช้เก็บออบเจ็คทั้งหมดของผู้ผลิตอุปกรณ์แต่ละราย → OBJECT IDENTIFIER ::={internet 4}

Syntax เป็นการกำหนดรายละเอียดของแต่ละ Object type โดยใช้ Syntax เพียงบางส่วนของภาษา ASN.1 ซึ่งจะแบ่งกลุ่มชนิดข้อมูลออกเป็น 3 กลุ่มคือ

1. Primitive type ใช้เป็นชนิดข้อมูลพื้นฐาน ได้แก่ Integer, Octet String, Object Identifier และ Null
2. Defined type ชนิดข้อมูลใหม่ที่กำหนดจากชนิดข้อมูลเดิมได้แก่ Network Address, IpAddress, Counter, Gauge, TimeTicks และ Opaque
3. Constructor type ใช้ในการสร้างลิสต์และตารางได้แก่ SEQUENCE และ SEQUENCE OF

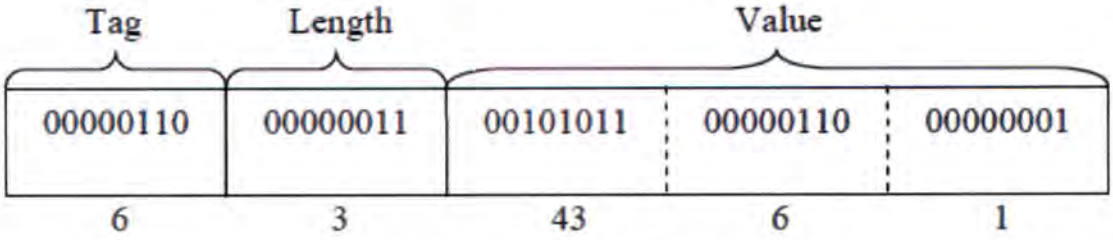
ตารางที่ 2.1 ชนิดข้อมูลของ SMIv1

Type	Size	Description
INTEGER	4 byte	เป็นเลขจำนวนเต็มมีค่าระหว่าง -2^{31} ถึง $2^{31}-1$
Integer32	4 byte	เหมือนกับ INTEGER
Unsigened32	4 byte	ไม่มีเครื่องหมาย มีค่าอยู่ระหว่าง 0 ถึง $2^{32}-1$
OCTET STRING	Variable	Byte String ยาวได้ 65,535 Byte
OBJECT IDENTIFIER	Variable	ชื่อของ Object ID
IPAddress	4 byte	เป็น IP Address ประกอบด้วยตัวเลข 4 ชุด
Counter32	4 byte	เป็นเลขจำนวนเต็มเพิ่มขึ้นจาก 0 - 2^{32} แล้วกลับมานับที่ 0 ใหม่
Counter64	8 byte	นับ 64 bit
Gauge32	4 byte	เหมือน couter32 แต่เมื่อนับถึงจุดสูงสุดแล้ว ไม่กลับไปที่ 0 แต่จะคงค่านั้นอยู่ จนกว่าจะถูก Reset
TimeTicks	4 byte	ใช้นับเลขจำนวนเต็ม นับเวลาในหน่วยเศษหนึ่งส่วนร้อยวินาที
BITS		สายของ bit
Opaque	Variable	ไม่สามารถแปล String ได้

ตารางที่ 2.2 Code ของชนิดข้อมูล Tag

Data Type	Class	Format	Number	Tag(Binary)	Tag(Hex)
INTEGER	00	0	00010	00000010	02
OCTET STRING	00	0	00100	00000100	04
OBJECT INDENTIFIER	00	0	00110	00000110	06
NULL	00	0	00101	00000101	05
Sequence , Sequence of	00	1	10000	00110000	30
IPAddress	01	0	00000	01000000	40
Counter	01	0	00001	01000001	41
Gauge	01	0	00010	01000010	42
TimeTicks	01	0	00011	01000011	43
Opaque	01	0	00100	01000100	44

Encoding SNMP จะใช้การเข้ารหัสแบบ Basic Encoding Rule (BER) ในการส่งข้อมูลไปมาระหว่างแมเนเจอร์และเอเจนต์ ซึ่งมีส่วนประกอบ 3 ส่วนคือ Tag, Length และ Value หรือเรียกว่า TLV โดยที่ Tag จะใช้ในการกำหนดประเภทของแต่ละชนิดข้อมูลที่จะเข้ารหัสตามตารางที่ 2 ส่วนฟิลด์ Length จะใช้ในการกำหนดความยาวหรือจำนวนของ Octet ที่อยู่ในส่วนของ Value โดยกำหนดให้บิตซ้ายสุดมีค่าเป็น 0 ส่วนอีก 7 บิตที่เหลือจะใช้กำหนดความยาว ดังนั้นจึงสามารถใช้กำหนดความยาวของข้อมูลได้สูงสุด 128 ไบต์ (OCTET) แต่ถ้าความยาวมีมากกว่า 128 ไบต์บิตซ้ายสุดมีค่าเป็น 1 แล้วใช้อีก 7 บิตที่เหลือกำหนดจำนวนของไบต์ที่ใช้ในการกำหนดความยาวที่อยู่ถัดไป ซึ่งเป็นไบต์ที่ใช้กำหนดความยาวข้อมูล และส่วนของฟิลด์ Value จะใช้ในการกำหนดค่าของข้อมูล ตัวอย่าง การเข้ารหัสที่มีข้อมูลแบบ OBJECT IDENTIFIER ของออบเจ็ค internet ที่มีค่าเท่ากับ 1.3.6.1 ซึ่งจะใช้สูตรคณิตศาสตร์เพื่อคำนวณการเข้ารหัส คือ (x*40) + y โดยที่ x คือหมายเลขของตัวระบุย่อยตัวที่หนึ่ง ซึ่งในที่นี้คือ 1 และ y คือหมายเลขของตัวระบุย่อยตัวที่สอง ซึ่งในที่นี้คือ 3 ซึ่งจะได้ในส่วนของ Tag คือ 06H (OBJECT IDENTIFIER) ส่วนของ Length เท่ากับ 3 Octet และส่วนของ Value เท่ากับ 43 6 1 ดังรูป 2.8



รูปที่ 2.8 แสดงการเข้ารหัสของออบเจ็ค internet

2.5.2 การระบุ Object Instances ของ Managed Object

ระบบจัดการเครือข่ายจะสอบถามข้อมูลที่ต้องการจากเอเจนต์ โดยใช้ตัวแปรในการระบุซึ่งประกอบด้วย OBJECT IDENTIFIER (IOD) และ Object Instance ของออบเจ็คนั้น โดย Object Instance นั้นจะหมายถึงตัวแทนของการอ้างถึงค่าของออบเจ็คนั้น เช่นถ้าเราต้องการข้อมูลที่เป็นชื่อของระบบ (sysName) ต้องระบุ OID และ Instance ดังนี้

iso org dod internet mgmt mib-2 system sysName Instance

1 3 6 1 2 1 1 5 0

ซึ่งตัวแปรที่จะใช้ในการสอบถามคือ 1.3.6.1.2.1.1.5.0 ในกรณีที่ออบเจ็คนั้นเป็นตารางซึ่งสามารถมี Instance ได้มากกว่าหนึ่งค่า วิธีการอ้างถึงข้อมูลที่ตำแหน่งของ Instance ใดๆ หรืออาจจะหมายถึงแถวที่เท่าไรนั้นสามารถดูได้จากข้อมูลของคอลัมน์ที่ถูกกำหนดให้เป็นอินเด็กซ์โดยสามารถดูได้จากรายละเอียดของออบเจ็คในฐานข้อมูล MIB เช่น ตารางของไอพีแอดเดรสซึ่งมีรายละเอียดดังนี้

```
ipAddrTable OBJECT-TYPE
        SYNTAX SEQUENCE OF IpAddrEntry
        ACCESS not-accessible
        STATUS mandatory
        DESCRIPTION
                "The table of addressing information relevant to
                this entity's IP addresses."
        ::= { ip 20 }
ipAddrEntry OBJECT-TYPE
        SYNTAX IpAddrEntry
        ACCESS not-accessible
```

```
        STATUS mandatory
        DESCRIPTION
                "The addressing information for one of this
                entity's IP addresses."
        INDEX { ipAdEntAddr }
        ::= { ipAddrTable 1 }
IpAddrEntry ::=
        SEQUENCE {
                ipAdEntAddr
                        IpAddress,
                ipAdEntIfIndex
                        INTEGER,
                ipAdEntNetMask
                        IpAddress,
                ipAdEntBcastAddr
                        INTEGER,
                ipAdEntReasmMaxSize
                        INTEGER (0..65535)
        }
```

ตารางที่ 2.3 ตัวอย่างของข้อมูลในตารางไอพีแอดเดรส

ipAdEntAddr	ipAdEntIfIndex	ipAdEntNetMask	ipAdEntBcastAddr	ipAdEntReasmMaxSize
127.0.0.1	1	255.0.0.0	1	65535
192.168.10.181	4	255.255.255.0	1	65535
192.168.152.1	3	255.255.255.0	1	65535
192.168.254.1	2	255.255.255.0	1	65535

จากตัวอย่างข้อมูลใน จะเห็นได้ว่าคอลัมน์ ipAdEntAddr ถูกกำหนดให้เป็นอินเด็กซ์ในการอ้างถึงแถวข้อมูลที่ต้องการ และจะแสดงตัวอย่างของข้อมูลที่มี 4 แถวหรือ 4 Instance ในตารางไอพีแอดเดรส ดังนั้นความปีนไปได้ในการอ้างถึงข้อมูลของออบเจ็ค ipAdEntNetMask ซึ่งมี OID เท่ากับ

iso.org.dod.internet.mgmt.mib2.ip.ipAddrTable.ipAddrEntry.ipAdEntNetMask

หรือ 1.3.6.1.2.1.4.20.1.3 มีดังนี้

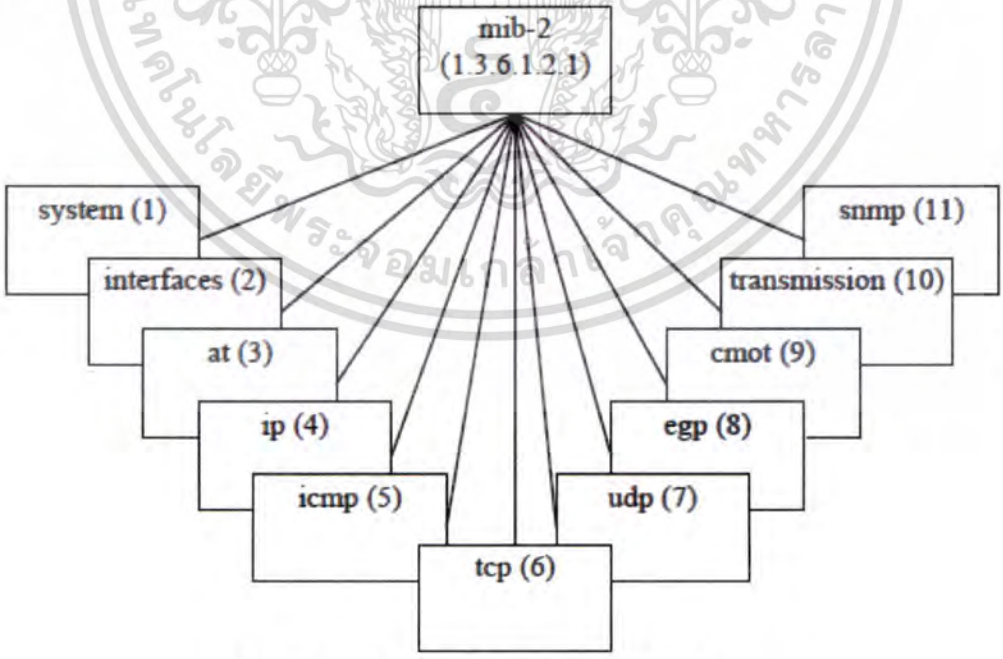
แถวที่ 1 คือ 1.3.6.1.2.1.4.20.1.3.127.0.0.1 มีค่าเท่ากับ 255.0.0.0

แถวที่ 2 คือ 1.3.6.1.2.1.4.20.1.3.192.168.10.181 มีค่าเท่ากับ 255.255.255.0

แถวที่ 3 คือ 1.3.6.1.2.1.4.20.1.3.192.168.152.1 มีค่าเท่ากับ 255.255.255.0

แถวที่ 4 คือ 1.3.6.1.2.1.4.20.1.3.192.168.254.1 มีค่าเท่ากับ 255.255.255.0

2.5.3 Management Information Base (MIB)



รูปที่ 2.9 โครงสร้างต้นไม้ของกลุ่มออบเจ็คใน MIB-II

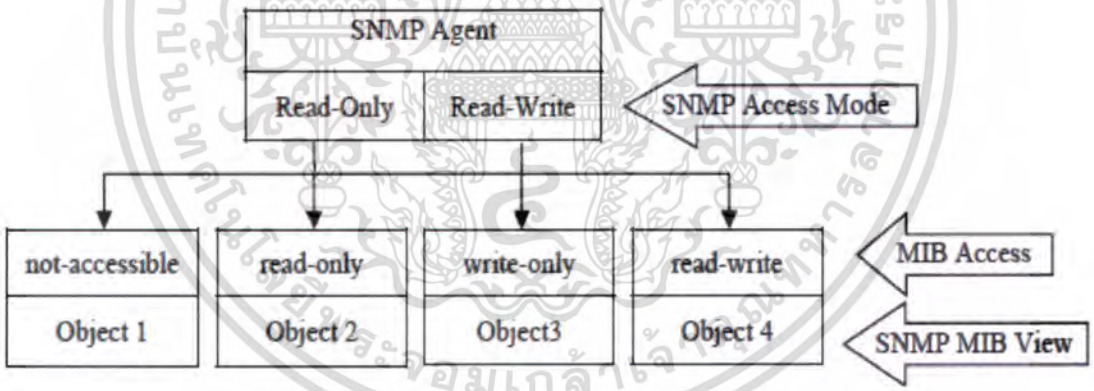
MIB เป็นฐานข้อมูลแบบเสมือนที่ใช้เก็บกลุ่มและความสัมพันธ์ของออบเจ็ค ในการกำหนดและอธิบายออบเจ็คใน MIB ประกอบด้วยสามส่วน คือ ชื่อ (OBJECT DESCRITOR และ OBJECT IDENTIFIER) SYNTAX (ASN.1) และการเข้ารหัส (BER) ซึ่งในกลุ่มออบเจ็คใน MIB-II จะมี OBJECT IDENTIFIER ที่ขึ้นต้นด้วย

mib-2 OBJECT IDENTIFIER := {mgmt 1} หรือ 1.3.6.1.2.1

กลุ่มของออบเจ็คภายใน MIB ของ SNMPv1 นั้นจะมีทั้งหมด 11 กลุ่ม ดังรูปที่ 2.9

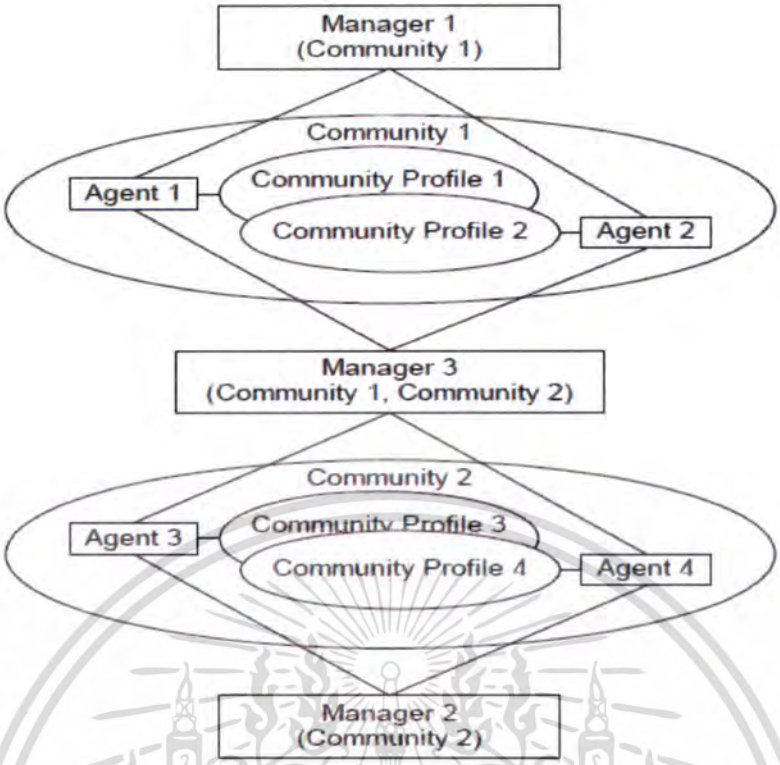
2.5.4 SNMP Communities

ในการจัดการเครือข่ายด้วยโปรโตคอล SNMP v1 นั้นได้กำหนดให้มีการติดต่อสื่อสารเพื่อแลกเปลี่ยนข้อมูลระหว่างแมเนเจอร์และเอเจนต์ ทั้งแมเนเจอร์ และเอเจนต์นั้นต้องอยู่ภายใน community เดียวกันและทั้งแมเนเจอร์และเอเจนต์นั้นสามารถอยู่ใน community อื่นๆได้มากกว่าหนึ่ง community โดยใช้ชุดของตัวอักษรแทนชื่อ community ซึ่งชื่อนี้เปรียบได้กับรหัสผ่าน (password) ที่ใช้ในการพิสูจน์ตัวตนระหว่างแมเนเจอร์และเอเจนต์แต่ในการสื่อสารนั้นจะไม่มีขั้นตอนในการเข้ารหัสข้อมูลให้เป็นความลับ ดังรูปที่ 2.10



รูปที่ 2.10 SNMP Commuity Profile [MANI2000]

ชื่อ community นี้จะกำหนดขึ้นตามรูปแบบในการเข้าถึงของ SNMP (SNMP Access Mode) ซึ่งจะมีการเข้าถึงอยู่สองแบบ คือการเข้าถึงแบบอ่านข้อมูลได้อย่าเดียว (Read-Only) และการเข้าถึงแบบอ่านหรือเขียนข้อมูลได้ (Read-Write) นอกจากนี้ที่เอเจนต์ยังสามารถกำหนดกลุ่มของออบเจ็คใดบ้างที่สามารถมองเห็นได้ (MIB View) โดยส่วนของ SNMP Access Mode และ MIB view รวมกันเรียกว่า Community Profile



รูปที่ 2.11 นโยบายการเข้าถึงของ SNMP[MANI2000]

ซึ่งการดำเนินการของการสอบถามข้อมูลหรือเปลี่ยนแปลงค่าของออบเจ็คจะถูกตัดสินใจจากส่วนของ community Profile และสิทธิ์ที่สามารถเข้าถึงออบเจ็คนั้นได้ (MIB Access) คือ not-access, read-only, write-only และ read-write

2.5.5 คำสั่งพื้นฐานของ SNMP

ในการติดต่อสื่อสารกันระหว่างแมเนเจอร์และเอเจนต์ของโปรโตคอล SNMP นั้นจะสร้าง Protocol Data Unit (PDU) ของแต่ละคำสั่งเพื่อใส่ขอ้มูลต่างๆลงไป จากนั้นก็จะรวม PDU เข้ากับส่วนของเวอร์ชั่นของ SNMP และชื่อ community โดยเลือกใช้โปรโตคอล UDP ในการขนส่งข้อมูลไปมาระหว่างแมเนเจอร์และเอเจนต์ผ่านทางพอร์ตหมายเลข 161 สำหรับกลุ่มคำสั่ง get กับ set และใช้พอร์ตหมายเลข 162 สำหรับคำสั่ง trap โดยทุกชุดคำสั่งจะมีรูปแบบของ PDU อยู่สองชนิด คือ PDU สำหรับคำสั่ง get กับ set

PDU Type	RequestID	Error Status	Error Index	VarBind 1 Name	VarBind 1 Value	...	VarBind n Name	VarBind n Value

รูปที่ 2.12 PDU สำหรับคำสั่งกลุ่ม Get และ Set[MANI2000]

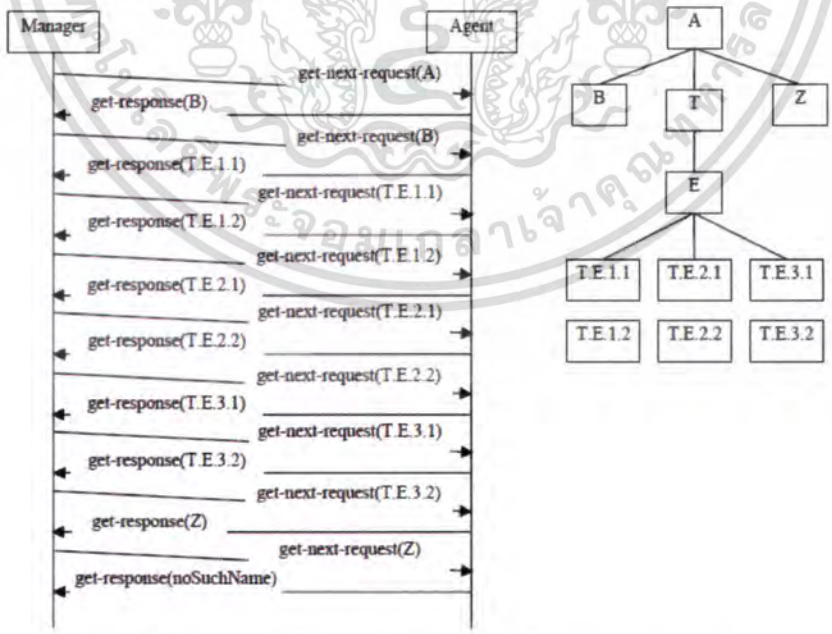
PDU Type	Enterprise	Agent Address	Generic Trap Type	Specific Trap Type	Time stamp	VarBind 1 Name	VarBind 1 Value	...	VarBind n Name	VarBind n Value

รูปที่ 2.13 PDU สำหรับคำสั่ง Trap[MANI2000]

โดยมีคำสั่งทั้งหมดของโปรโตคอล SNMPv1 อยู่ 5 คำสั่งคือ get-response, get-next-request และ set-request เป็นชุดคำสั่งที่สร้างขึ้นจากแมเนเจอร์ไปยังเอเจนต์ get-response และ trap เป็นชุดคำสั่งที่สร้างขึ้นจากเอเจนต์ไปยังแมเนเจอร์

Get-Request เป็นคำสั่งที่ใช้สำหรับร้องขอค่าข้อมูลของออบเจ็คจากตัวเอเจนต์โดยที่แมเนเจอร์จะระบุตัวแปรหรือ OID ที่ต้องการไป เช่นต้องการค่าของออบเจ็ค sysName.0 จากนั้นเมื่อเอเจนต์ได้รับและตรวจสอบความถูกต้องของ PDU ที่ได้รับแล้วก็ใส่ค่าของออบเจ็คนั้นเพื่อจะตอบกลับไปด้วยคำสั่ง get-response ส่งกลับไปให้แมเนเจอร์

Get-Next-Request เป็นคำสั่งที่ใช้สำหรับร้องขอค่าของข้อมูลจากเอเจนต์เหมือนคำสั่ง get-request แต่จะต่างกันที่ค่าของออบเจ็คที่ร้องขอนั้นจะเป็นค่าออบเจ็คย่อยตัวถัดไปจากอบบเจ็คที่ร้องขอไป หรือการใช้วิธีค้นหาแบบ depth-first-search เช่นถ้าต้องการค่าของออบเจ็คตัวต่อไปจากออบเจ็ค sysUpTime.0 ก็จะเป็นค่าของ sysContact.0 โดยจะแสดงลำดับการทำงานของคำสั่ง get-next-request ดังรูป 2.14 จะเห็นว่าคำสั่ง get-next-request จะมีประโยชน์มากเมื่อใช้กับออบเจ็คที่เป็นตาราง เพราะเราไม่รู้จำนวนแถวที่แน่นอนของตาราง



รูปที่ 2.14 ตัวอย่างลำดับการทำงานคำสั่ง get-next-request

Set-Request จะใช้สำหรับกำหนดหรือเปลี่ยนแปลงแก้ไขค่าของข้อมูลและการทำงานของอุปกรณ์ โดยส่งคำร้องขอที่กำหนดตัวแปรหรือออบเจ็คในฐานข้อมูล MIB และค่าของออบเจ็คที่ต้องการเปลี่ยนไปยังเอเจนต์

Get-Response เป็นคำสั่งที่ใช้สำหรับตอบสนองคำสั่ง get-request, get-next-request และ set-request ที่ส่งมาจากแมเนเจอร์ โดยจะส่งค่าของออบเจ็คที่ร้องขอ และส่งผลลัพธ์ของการใช้คำสั่ง set กลับไปยังแมเนเจอร์

Trap จะใช้สำหรับการแจ้งเตือนเหตุการณ์บางอย่างที่เกิดขึ้นให้กับแมเนเจอร์โดยที่แมเนเจอร์ไม่ต้องมีการร้องขอ เช่น link down, link up ค่าของซีพียูหรืออุณหภูมิสูงเกินกว่าที่กำหนดไว้ (Threshold) เป็นต้น

2.6 Simple Network Management Protocol Version2 (SNMPv2)

โปรโตคอล SNMPv2 ได้รับการปรับปรุงแก้ไขข้อจำกัดของเวอร์ชัน 1 แต่ในแง่ของความปลอดภัยยังไม่ได้รับการปรับปรุงในเวอร์ชัน 2 นี้ โดยยังใช้ชื่อ community เป็นหลักเหมือนกันกับเวอร์ชัน 1 ซึ่งเรียกกันในชื่อว่า SNMPv2c โดยการเปลี่ยนแปลงหลักๆ ของ SNMPv2 มีดังนี้

เพิ่มคำสั่งพื้นฐานสำหรับใช้ในการจัดการเครือข่ายขึ้นอีก 2 ชุดคำสั่ง คือ คำสั่ง Get-Bulk-Request เพื่อใช้สำหรับการสอบถามข้อมูลครั้งละปริมาณมากๆ ซึ่งจะทำให้มีการทำงานที่เร็วกว่าการใช้คำสั่ง Get-Next-Request ซึ่งทำให้การสอบถามข้อมูลจากตารางทำได้ง่ายและมีประสิทธิภาพมากยิ่งขึ้น และอีกคำสั่งหนึ่ง คือ คำสั่ง Inform-Request ที่ใช้สำหรับติดต่อสื่อสารกันระหว่างสองระบบจัดการเครือข่าย (Manager - to - Manager) นอกจากนี้ยังมียังมีอีกหนึ่งคำสั่งที่ถูกกำหนดขึ้นในเวอร์ชันนี้แต่ยังไม่ได้ไม่ได้นำมาใช้งาน คือ คำสั่ง Report

ข้อกำหนดของ SMI และ trap ที่ใช้ใน SNMPv1 ถูกนำมารวมกันและแก้ไขปรับปรุงเป็น SMIv2

Textual Conversations เกี่ยวกับการกำหนดชนิดข้อมูลแบบใหม่โดยใช้โครงสร้างตามที่กำหนดใน SMIv2 เพื่อทำให้ชนิดข้อมูลนั้นมีความหมายที่ชัดเจนและมนุษย์สามารถอ่านเข้าใจได้ง่ายขึ้น

Conformance Statements เกี่ยวกับข้อกำหนดที่ผู้ผลิตแต่ละรายนั้นจะต้องทำตาข้อกำหนดนี้เป็นอย่างน้อยในการอุปกรณ์ เพื่อให้ผลิตภัณฑ์สามารถใช้งานร่วมกับมาตรฐานของโปรโตคอล SNMP ได้ และนอกจากนี้ ผู้ผลิตนั้นสามารถที่จะเพิ่มเติมส่วนต่างๆเฉพาะของตนเข้าไปได้

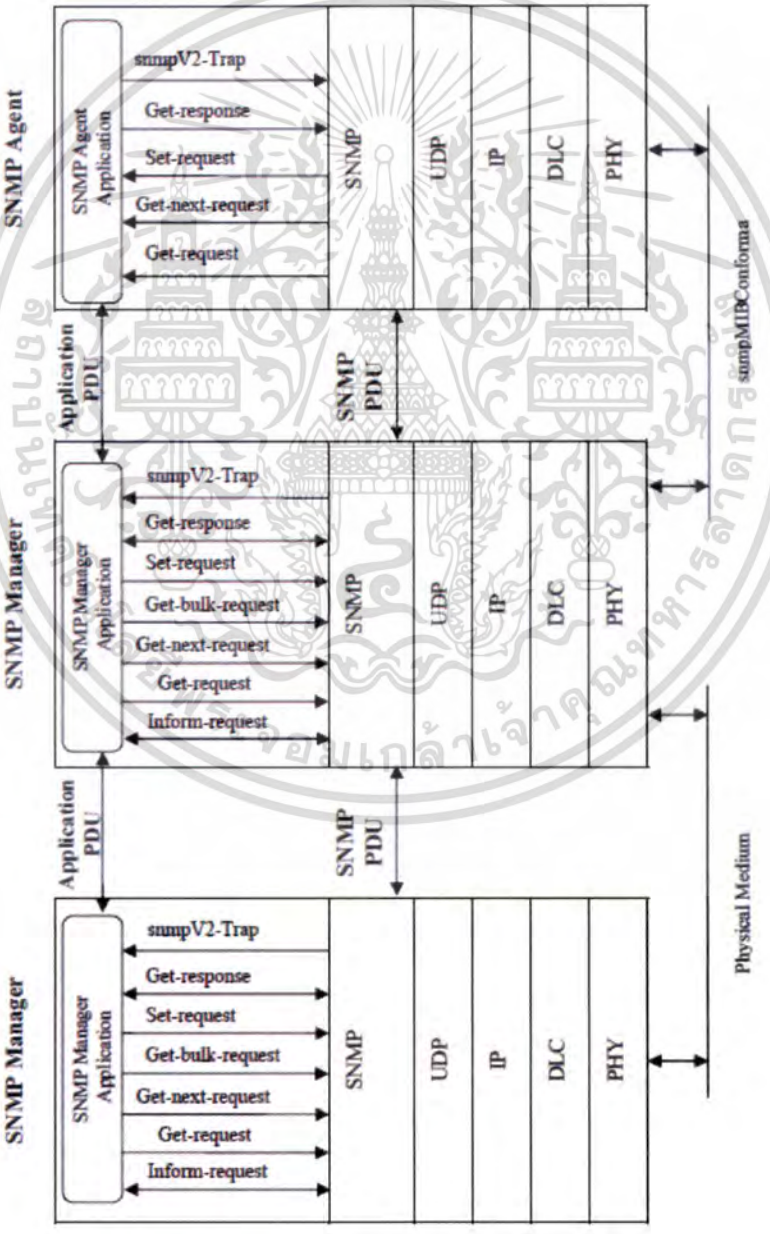
การเพิ่มความสามารถในการทำงานกับตาราง โดยที่สามารถต่อเติมคอลัมน์ของตารางที่มีอยู่ก่อนได้ รวมทั้งสร้างและลบแถวของข้อมูลในตารางได้ปรับปรุงออบเจ็คในฐานข้อมูล MIB โดย

การเพิ่มกลุ่มออบเจ็คภายใต้โหนด internet การเปลี่ยนแปลงกลุ่มของออบเจ็ค system และ snmp และเพิ่มกลุ่มออบเจ็คภายใต้โหนด mib-2 เป็นต้น

Transport mappings เกี่ยวกับข้อกำหนดและรายละเอียดของโปรโตคอลในระดับชั้น Transport Layer ที่นอกเหนือจากการใช้โปรโตคอล UDP ของ TCP/IP ทีสามารถใช้งานร่วมกับ SNMP ได้ เช่น OSI, IPX, DDP เป็นต้น

2.6.1 สถาปัตยกรรม

องค์ประกอบพื้นฐานของ SNMPv2 จะเหมือนกับเวอร์ชัน 1 คือ ประกอบด้วยแมเนเจอร์และเอเจนต์ ดังนี้



รูปที่ 2.15 สถาปัตยกรรมของ SNMPv2

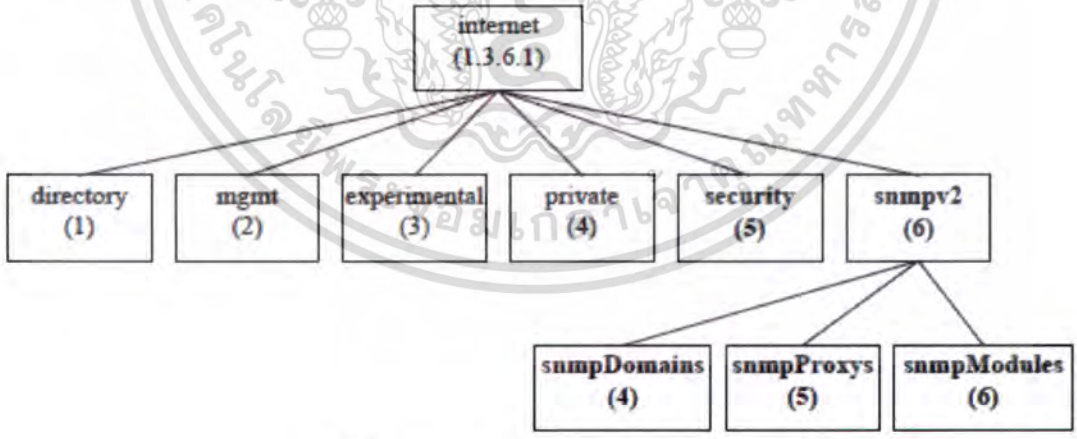
แต่มีส่วนการยกระดับความสามารถและประสิทธิภาพของการทำงานได้ดีจาก SNMPv1 คือ

- มีการยกระดับเพื่อให้สามารถเลือกใช้โปรโตคอลสำหรับการขนส่งข้อมูลในระดับชั้น Transport Layer ได้หลายแบบ เช่น เอเจนต์สามารถเลือกใช้โปรโตคอล CLNS (Connectionless Mode Network Service) ของ OSI ติดต่อสื่อสารกับแมเนเจอร์ที่ใช้ UDP

- มีคำสั่งสำหรับใช้ในการทำงานเพิ่มขึ้นจากเดิมสองคำสั่งรวมเป็น 7 คำสั่ง โดยมีคำสั่ง inform-request สำหรับให้แมเนเจอร์หนึ่งติดต่อสื่อสารกับแมเนเจอร์อื่นๆได้ และคำสั่ง get-bulk-request สำหรับใช้สอบถามข้อมูลได้ทีละมากๆ เช่นข้อมูลที่เป็นตารางซึ่งใช้คำสั่งนี้จะทำงานได้เร็วและมีประสิทธิภาพมากกว่าคำสั่ง get-request-next คำสั่งอื่นที่เหลือยังคงรูปแบบการทำงานเหมือนกับเวอร์ชัน 1 ส่วนคำสั่ง get-response ยังคงรูปแบบเหมือนเดิมแต่ในเวอร์ชันนี้สามารถสร้างขึ้นได้ทั้งจากเอเจนต์เพื่อตอบสนองต่อคำสั่งกลุ่ม get กับ set และสร้างขึ้นจากแมเนเจอร์เพื่อใช้ตอบสนองคำสั่ง inform-request จากแมเนเจอร์อื่นๆ คำสั่ง trap คงรูปแบบเดิมแต่ได้ยกเลิกการใช้รูปแบบ UDP ของ trap ในเวอร์ชัน 1 แล้วปรับมาใช้โครงสร้างของ PDU ที่เหมือนกับคำสั่งอื่น

2.6.2 Structure of Management Information version 2 (SMIv2)

สำหรับ SMI เวอร์ชัน 2 ได้เพิ่ม 2 กลุ่มออบเจ็คใหม่ขึ้นภายใต้โหนด internet คือ ออบเจ็ค security {1.3.6.1.5} และ snmpv2 {1.3.6.1.6} และออบเจ็ค snmpDomains, snmpProxys และ snmpModules ภายใต้โหนด snmpv2



รูปที่ 2.16 กลุ่มของออบเจ็คใน snmpv2

SMIv2 ถูกแบ่งออกเป็น 3 ส่วนคือ Module definitions เป็นส่วนที่ใช้อธิบายเกี่ยวกับความหมายของข้อมูล (Information modules) เช่นส่วนของฐานข้อมูล MIB, Object definitions เป็นส่วนที่ใช้อธิบายเกี่ยวกับอ็อบเจ็ค (Managed Objects) และ Notification definitions เป็นส่วนที่ใช้อธิบายเกี่ยวกับการส่งข้อมูลที่ไม่ได้มีการร้องขอ เช่น Trap

ตารางที่ 2.4 Textual Conventions ของ SMIv2

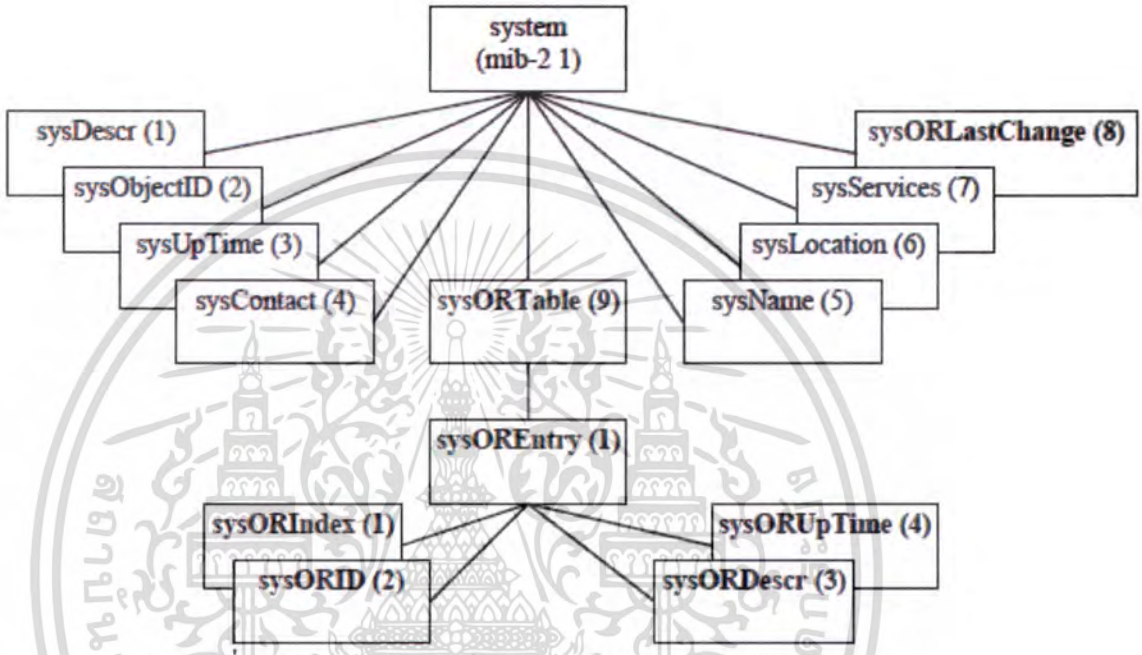
ชนิดข้อมูล	คำอธิบาย
DisplayString	ใช้แทนสายอักขระตามตัวอักษรใน NVT ASCII
PhysAddress	แอดเดรสในระดับ Media หรือ Physical
MacAddress	แอดเดรส MAC ของ IEEE 802 ซึ่งมีความยาวเท่ากับ 6 Octets
TruthValue	ใช้แทนค่าที่เป็นจริงหรือเท็จ โดยใช้ INTEGER {true(1), false(2)}
TestAndIncr	ใช้สำหรับกำหนดให้ไม่มีการทำงานกับอ็อบเจ็คนี้ได้ในเวลาเดียวกัน
AutonomousType	ค่า OID ที่ใช้สำหรับการกำหนด subtree ใน MIB
VariablePointer	ค่า OID ที่เป็นตัวชี้ไปยังค่าของ object instance ที่กำหนด เช่น sysContact.0
RowPointer	ค่า OID ที่เป็นตัวชี้ไปยังแถวในตาราง
RowStatus	ใช้แทนค่าสถานะของการสร้างและลบแถวในตาราง
TimeStamp	ค่าของ sysUpTime ที่ใช้ระบุเวลาที่เกิดขึ้น
TimeInterval	ใช้สำหรับวัดช่วงของเวลาในหน่วย 0.01 วินาที
DateAndTime	ใช้สำหรับกำหนดวันที่และเวลา
StorageType	ใช้สำหรับกำหนดชนิดของหน่วยความจำที่เอเจนต์ใช้
TDomain	ใช้แสดงชนิดของ Transport service
TAddress	ใช้แสดงหมายเลขของ Transport service

2.6.3 Management Information Base

ฐานข้อมูล MIB สำหรับ SNMPv2 นี้ได้ปรับปรุงแก้ไขกลุ่มของอ็อบเจ็ค system และ snmp ภายใต้โหนด mib-2 ที่ใช้ใน SNMPv1 และได้เพิ่มกลุ่มอ็อบเจ็คใหม่ขึ้นมาสองกลุ่มภายใต้โหนด internet ดังรูปที่ 14 คือ security และ snmpv2 โดยที่โหนด security นี้ยังไม่ได้มีการนำมาใช้งานเวอร์ชันนี้ และภายใต้โหนด snmpv2 นั้นจะมีอีกสามโหนดย่อย คือ snmpDomains ที่ใช้อ้างถึงอ็อบเจ็คสำหรับระบบที่ส่งข้อมูลผ่านทางโปรโตคอลการส่งข้อมูล (Transmission Protocols) รูปแบบต่างๆ เช่น UDP, IPX เป็นต้น, snmpProxys ใช้อ้างถึงอ็อบเจ็คสำหรับระบบที่ใช้โปรโตคอลจัดการ

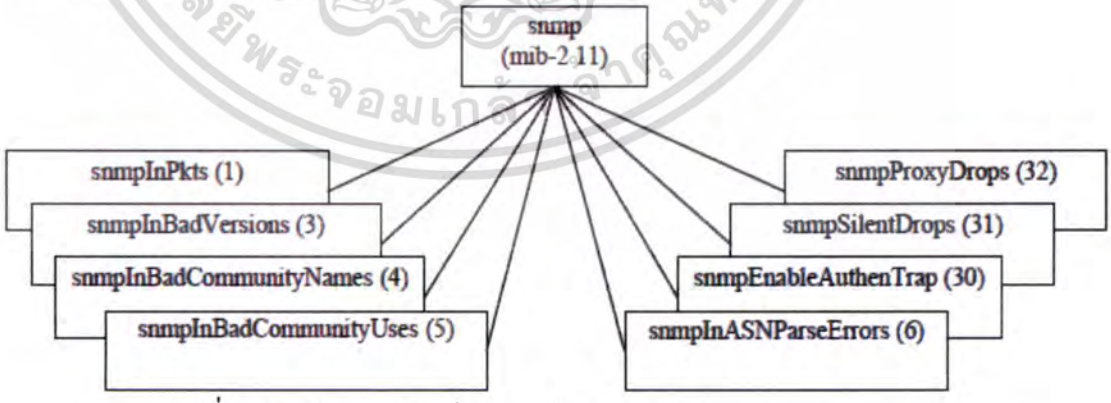
เครือข่ายอื่นมาทำงานร่วมกับ SNMPv2 ผ่านทางบริการของ proxy และโหนด snmpModule ที่ใช้ในการอ้างถึงออบเจ็คต่างๆของ SNMPv2 สำหรับใช้ในการจัดการเครือข่ายโดยจะอธิบายถึงรายละเอียดของการเปลี่ยนแปลงของฐานข้อมูล MIB ดังนี้

2.6.3.1 เปลี่ยนแปลงออบเจ็คของกลุ่ม system



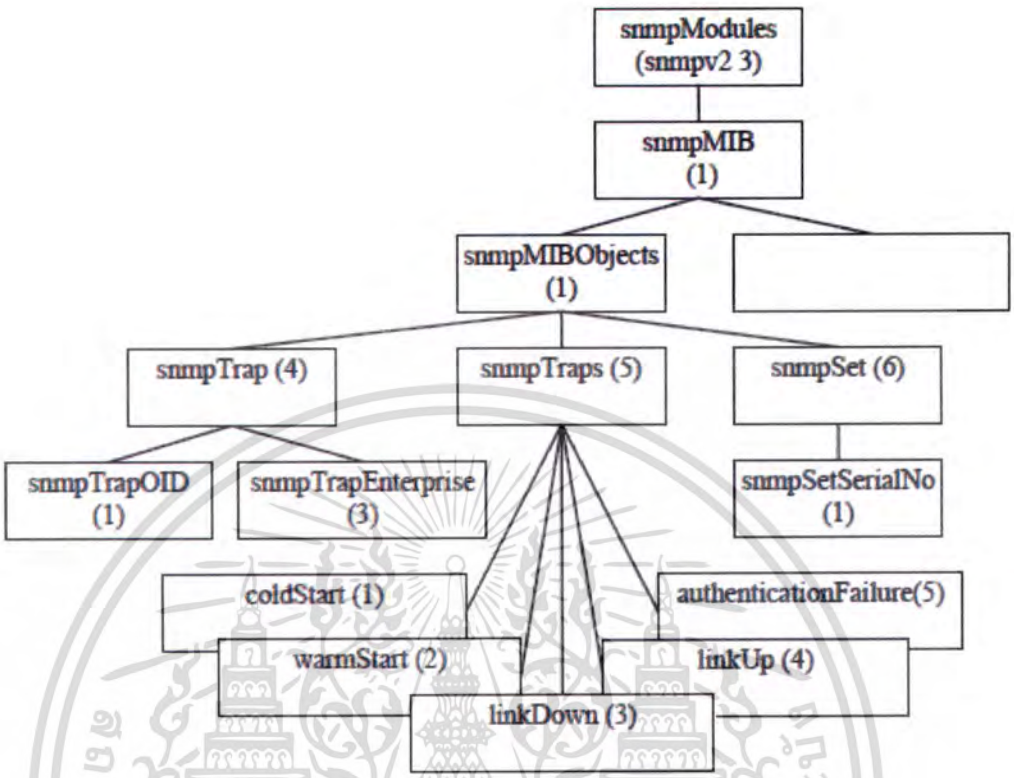
รูปที่ 2.17 กลุ่มของออบเจ็ค system ใน SNMPv2

2.6.3.2 เปลี่ยนแปลงออบเจ็คของกลุ่ม snmp



รูปที่ 2.18 กลุ่มของออบเจ็ค snmp ใน SNMPv2

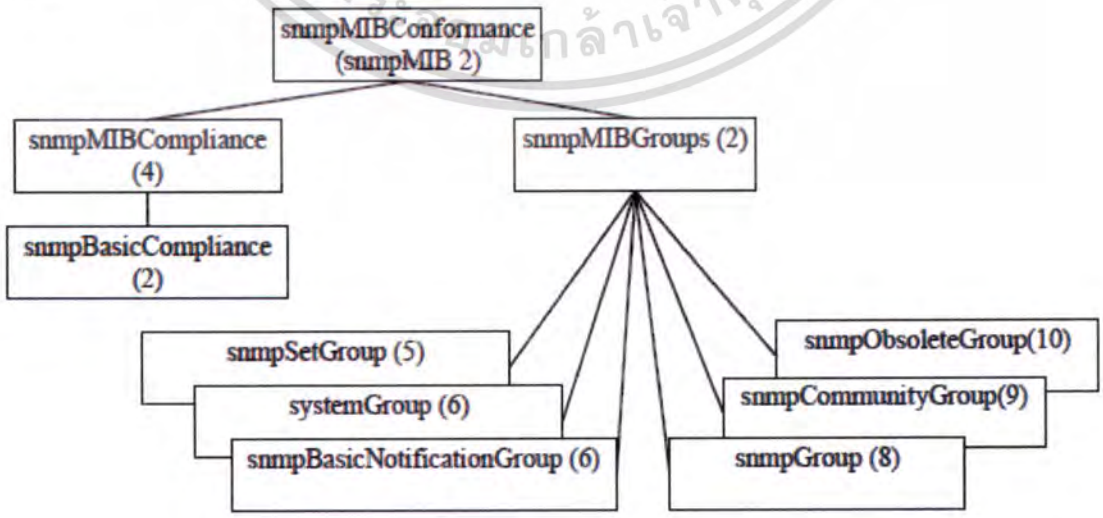
2.6.3.3 เพิ่มอ็อบเจ็คเกี่ยวกับข้อมูลของการแจ้งเตือน



รูปที่ 2.19 กลุ่มของอ็อบเจ็คภายใต้ snmpModule

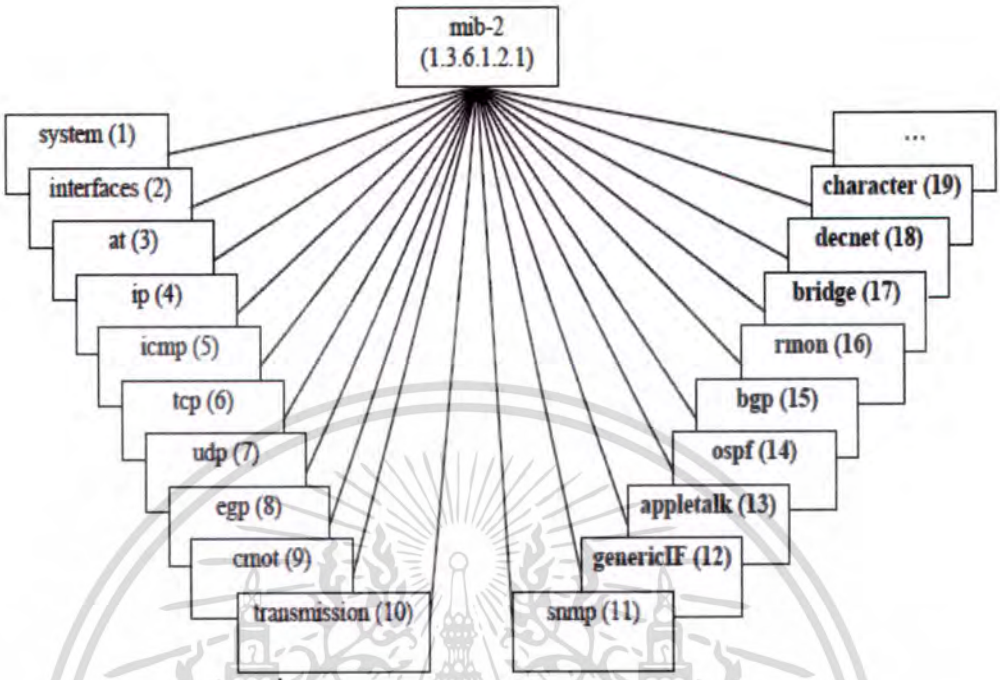
2.6.3.4 เพิ่มอ็อบเจ็คเกี่ยวกับข้อมูลของการปฏิบัติตาม

กลุ่มของอ็อบเจ็คของการปฏิบัติตาม (Conformance) คือ snmpMIBConformance อยู่ภายใต้โหนด snmpMIB สำหรับเก็บข้อมูลของอ็อบเจ็คที่จำเป็นจะต้องมีในฐานข้อมูล MIB ที่ใช้สำหรับ SNMPv2



รูปที่ 2.20 กลุ่มของอ็อบเจ็คภายใต้ snmpMIBConformance

2.6.3.5 เพิ่มอ็อบเจ็คภายใต้อ็อบเจ็ค mib-2



รูปที่ 2.21 กลุ่มของอ็อบเจ็คภายใต้ mib-2

2.6.4 คำสั่งพื้นฐานของ SNMPv2

การติดต่อสื่อสารกันของ SNMP เวอร์ชันนี้ยังคงใช้ชื่อ Community เป็นหลักสำหรับการกำหนดสิทธิในการเข้าถึงข้อมูลในแต่ละอุปกรณ์ โดยมีคำสั่งเพื่อใช้ในการจัดการเครือข่ายเพิ่มขึ้นอีกสองคำสั่ง คือ คำสั่ง get-bulk-request เพื่อใช้สอบถามข้อมูลเป็นกลุ่ม และคำสั่ง inform-request เพื่อใช้ในการติดต่อสื่อสารกันระหว่างแมเนเจอร์กับแมเนเจอร์ และเปลี่ยน PDU ของคำสั่ง trap ในเวอร์ชัน 1 ให้มาใช้รูปแบบเดียวกันกับ PDU ของคำสั่งอื่น ยกเว้น PDU ของคำสั่ง get-bulk-request

แต่ยังคงมีหน้าที่เหมือนกับเวอร์ชัน 1 และเรียกชื่อใหม่ว่า snmpv2-trap และนอกจากนี้ยังได้มีการกำหนดสถานะข้อผิดพลาด (Error status) เพิ่มจากเดิมด้วย โดยจะอธิบายการทำงานของชุดคำสั่งที่เพิ่มขึ้นในเวอร์ชันสองนี้

PDU Type	RequestID	Error Status	Error Index	VarBind 1 Name	VarBind 1 Value	...	VarBind n Name	VarBind n Value

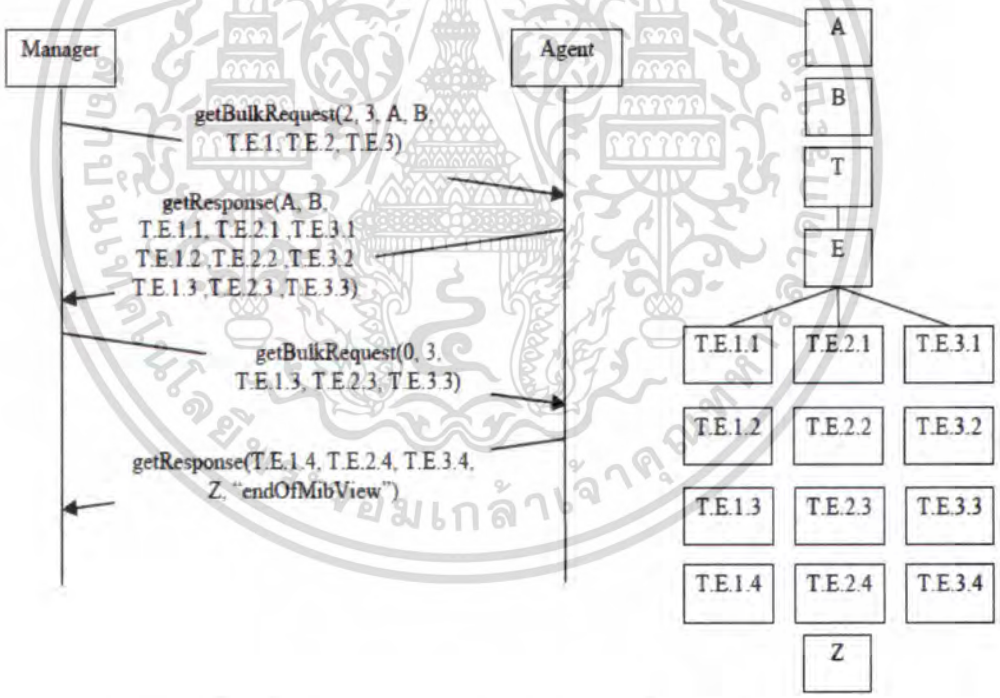
รูปที่ 2.22 PDU สำหรับชุดคำสั่งทั้งหมดใน snmpv2 ยกเว้นคำสั่ง get-bulk-request

PDU Type	RequestID	Non-Repeaters	Max-Repetitions	VarBind 1 Name	VarBind 1 Value	...	VarBind n Name	VarBind n Value

รูปที่ 2.23 PDU สำหรับคำสั่ง get-bulk-request

Inform-request เป็นคำสั่งที่เพิ่มเข้ามาใน SNMPv2 เพื่อใช้ในการติดต่อสื่อสารเพื่อแลกเปลี่ยนข้อมูลกันระหว่างแมเนเจอร์กับแมเนเจอร์ได้โดยตรง โดยที่คำสั่งนี้จะมีหน้าที่การทำงานที่คล้ายกับคำสั่ง trap แต่จะต่างกันที่ผู้รับนั้นจะส่งคำสั่ง get-response ตอบกลับมาให้กับผู้ส่งด้วย ซึ่งแมเนเจอร์จะทำหน้าที่ในการสร้างและรับคำสั่งนี้

Get-bulk-request เป็นคำสั่งที่เพิ่มเข้ามาใน SNMPv2 เพื่อใช้สอบถามกลุ่มของข้อมูลจากเอเจนต์ซึ่งมีประโยชน์มากเมื่อใช้สอบถามข้อมูลที่อยู่ในตาราง โดยคำสั่งนี้จะมีการทำงานคล้ายกับคำสั่ง get-next-request ซึ่ง PDU ของคำสั่ง get-bulk-request ได้มีฟิลด์ Non-Repeater เพื่อระบุจำนวนของออบเจ็คที่ไม่ต้องการให้มีการดึงข้อมูลซ้ำซึ่งส่วนใหญ่จะใช้กับออบเจ็คที่ไม่อยู่ในตาราง เช่น sysName, sysDescr และฟิลด์ max-Repetitions ใช้สำหรับระบุจำนวนสูงสุดของการดึงข้อมูลซ้ำหรือจำนวนของการดึงข้อมูลของออบเจ็คตัวต่อไป ซึ่งส่วนใหญ่จะใช้ดึงข้อมูลของออบเจ็คซ้ำตามจำนวนแถวที่อยู่ในตารางโดยจะแสดงลำดับการทำงานของการเรียกคำสั่งนี้ดังรูปที่ 2.24 ซึ่งมีการสอบถามข้อมูล 2 ออบเจ็คที่ไม่ต้องการให้ซ้ำและให้มีการดึงข้อมูลต่อไปของออบเจ็คซ้ำเป็นจำนวน 3 ครั้ง

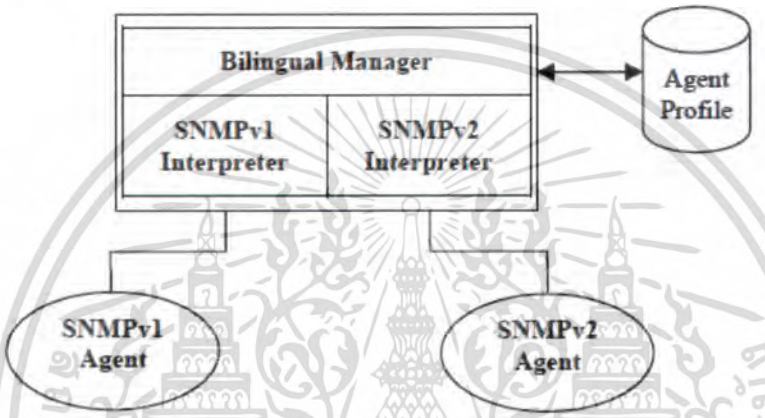


รูปที่ 2.24 ลำดับการทำงานของคำสั่ง get-bulk-request

2.6.5 การใช้งานร่วมกันกับ SNMPv1

เนื่องจากการปรับเปลี่ยนแก้ไขหลายๆอย่างใน SNMPv2 ทั้งส่วนของ SMI และฐานข้อมูล MIB จึงทำให้ไม่สามารถนำไปใช้งานได้ร่วมกันกับในเวอร์ชัน 1 ดังนั้นกลุ่มผู้ดูแลรับผิดชอบในการพัฒนามาตรฐาน SNMP ของ IETF ได้กำหนดมาตรฐานของการใช้งานร่วมกันทั้งสองเวอร์ชั่น โดยได้นำเสนอรูปแบบของการใช้งานร่วมกันไว้ 2 รูปแบบคือ Bilingual Manager และ SNMP Proxy server

1. Bilingual Manager

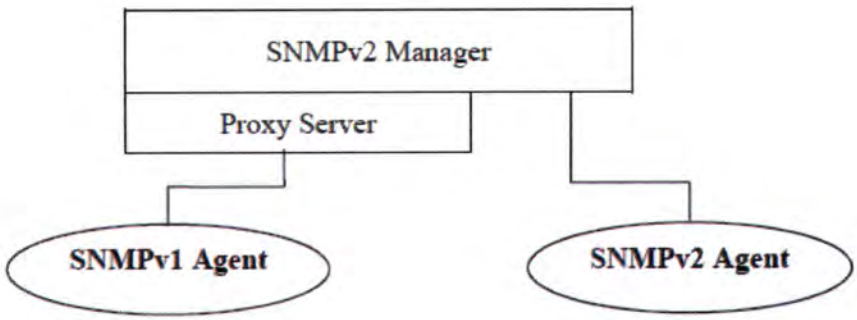


รูปที่ 2.25 รูปแบบการพัฒนาแมนเนเจอร์แบบ Bilingual

เป็นวิธีหนึ่งที่ใช้เปลี่ยน SNMPv1 เป็น SNMPv2 โดยการพัฒนาแมเนเจอร์ให้มีส่วนตัวแปลความหมายของ SNMP ของเอเจนต์ทั้งหมดเอาไว้ แล้วทำการปรับเปลี่ยนตัวแปรหรือออบเจ็คของฐานข้อมูล MIB และส่วนของคำสั่งให้เหมาะสมกับเวอร์ชันของ SNMP ในแต่ละเอเจนต์ ซึ่งการใช้วิธีแบบนี้จะทำให้ต้องมีค่าใช้จ่ายในการพัฒนาและบำรุงรักษาที่สูง เพราะทุกๆแมเนเจอร์จะต้องมีการพัฒนาทั้งส่วนของ SNMPv1 และ SNMPv2

2. SNMP Proxy Server

การใช้พร็อกซี่โดยทั่วๆไปแล้วจะใช้กับการจัดการเครือข่ายที่อุปกรณ์นั้นไม่สนับสนุนโปรโตคอล SNMP แต่ในที่นี้แมเนเจอร์จะใช้พร็อกซี่เพื่อปรับเปลี่ยนคำสั่งและตัวแปรไปมาระหว่าง SNMPv1 และ SNMPv2 โดยที่เอเจนต์ที่สนับสนุน SNMPv2 นั้นจะสามารถติดต่อสื่อสารกับแมเนเจอร์ได้โดยตรงแต่ SNMPv1 นั้นจะติดต่อสื่อสารกับแมเนเจอร์โดยผ่านทางพร็อกซี่ดังรูป



รูปที่ 2.26 รูปแบบการพัฒนาแมนเนเจอร์แบบ Proxy Sever

บทที่ 3

วิเคราะห์และออกแบบระบบการจัดการเครือข่ายแบบค้นหา

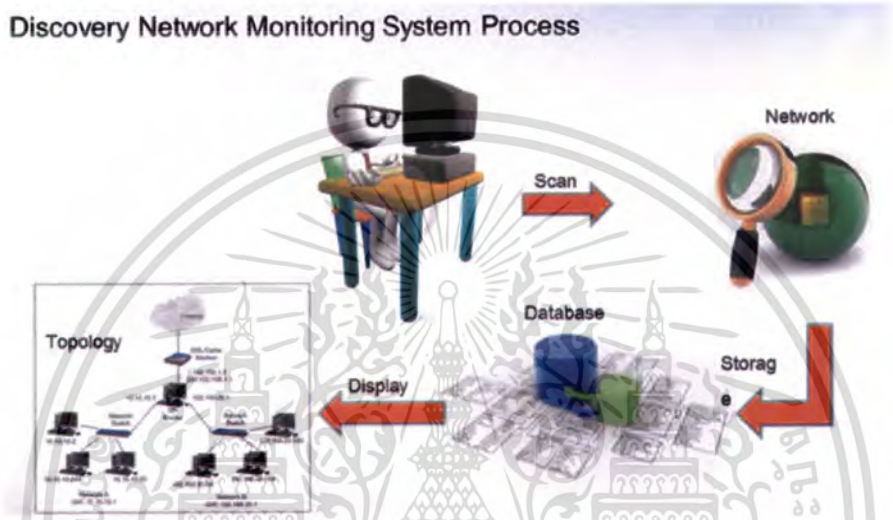
เมื่อศึกษาการทำงานของระบบบริหารจัดการเครือข่าย และศึกษาการทำงานของโปรโตคอล SNMP ที่เกี่ยวข้องกับระบบบริหารจัดการเครือข่ายแบบค้นหา การทำงานในการค้นหาอุปกรณ์เครือข่ายของระบบได้ จะต้องใช้ชุดข้อมูลจากฐานมูล MIB ของโปรโตคอล SNMB มาประกอบกัน อาทิเช่น ข้อมูลของ routing table , ARP cache และ Bridge-MIB ของอุปกรณ์เครือข่ายที่เชื่อมต่ออยู่ในระบบ โดยที่ผู้พัฒนาจะมีแนวคิดและวิธีในการสืบค้นข้อมูลอุปกรณ์เครือข่ายเพื่อให้ได้มาซึ่งข้อมูลอุปกรณ์เครือข่ายโดยจะใช้ชุดข้อมูลเพื่อค้นหาดังต่อไปนี้

ตารางที่ 3.1 ตารางข้อมูล MIB ที่ใช้ในการค้นหาอุปกรณ์

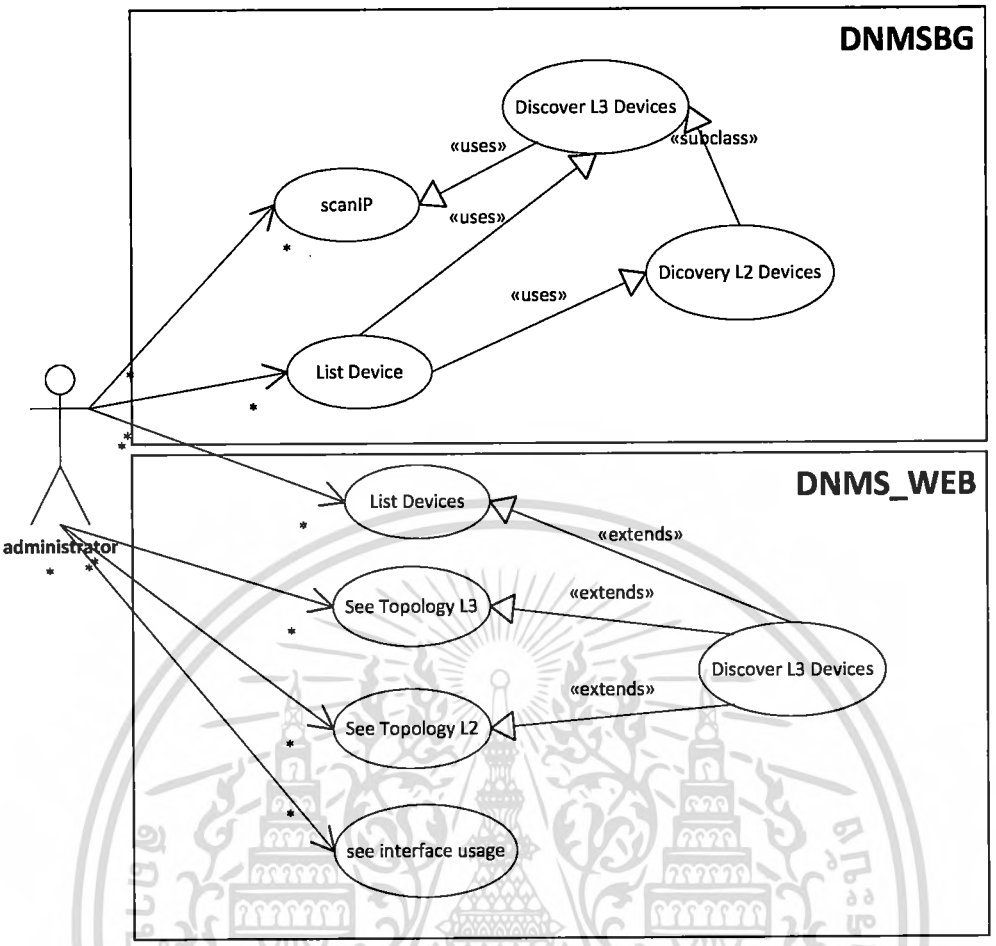
MIB	MIB object	OID	Significance of MIB
MIB II (RFC-1213-MIB)	**Sytem** -sysName -sysDescr	1.3.6.1.2.1.1	ข้อมูลชุดนี้ใช้เพื่อการทดลองเชื่อมต่อโปรโตคอล SNMP และเพื่อเก็บข้อมูลชื่อและข้อมูลรายละเอียดของอุปกรณ์
	ifTable -ifIndex -ifDescr -ifPhysicalAddress	1.3.6.1.2.1.2.2.1	ข้อมูลชุดนี้ใช้เพื่อตรวจสอบพอร์ตที่มีอยู่บนอุปกรณ์เครือข่าย และเพื่อเก็บข้อมูลการรับส่งข้อความบนพอร์ต
	ip -ipForwarding	1.3.6.1.2.1.4	เพื่อดูว่าอุปกรณ์สามารถส่งผ่านข้อความได้หรือไม่
	ipRouteTable -ipRouteNextHop -ipRouteType	1.3.6.1.2.1.4.21	ข้อมูลชุดนี้เพื่อตรวจสอบการหาเส้นทางของอุปกรณ์เลเยอร์ 3 ว่ามีการค้นหาเส้นทางแบบไหนและตัวถัดไปที่จะส่งข้อความ(Next Hop)
	ipAddrTable -ipAdEntAddr -ipAdEntNetMask	1.3.6.1.2.1.4.20	เพื่อตรวจสอบว่าอุปกรณ์ตัวนั้นๆ มีไอพีหลายหมายหรือไม่
	ipNetToMediaTable -ipNetToMediaNetAddress -ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22	เพื่อจับคู่ของMAC และ IP address ที่มีการเรียนรู้เข้าในตัวอุปกรณ์เครือข่าย
Q-BRIDGE 1.3.6.1.2.1.17 dot1dBridge	**dot1dBasePortTable** -dot1dbasePortEntry -dot1dBasePort -dot1dBasePortIfIndex	1.3.6.1.2.1.17.1.4	เพื่อจับคู่พอร์ตและ index ของพอร์ต
	dot1dTpFdbTable -dot1dTpFdbEntry -dot1dTpFdbAddress -dot1dTpFdbPort dot1dTpFdbStatus	1.3.6.1.2.1.17.4.3	เพื่อดูข้อมูลMACที่มีการส่งผ่านบนพอร์ต และจะนำข้อมูล MAC จากตาราง ipNetToMedia มาเปรียบเทียบกับ MAC ในตารางนี้

หลังจากนั้นจึงได้ทำการวิเคราะห์และออกแบบระบบ โดยแสดงรายละเอียดขั้นตอนการทำงานและความสัมพันธ์ของข้อมูลชุดต่างๆที่เป็นองค์ประกอบของระบบ ซึ่งจะแสดงอยู่ในรูปภาพแผนภูมิยูสเคส(Use Case Diagram) และ แผนภาพขั้นตอนการทำงานของระบบจะแสดงด้วยแผนภาพกิจกรรม (Activity Diagram) และโครงสร้างข้อมูลที่จัดเก็บ ดังต่อไปนี้

3.1 กระบวนการทำงานของระบบโดยรวม



รูปที่ 3.1 แสดงกระบวนการทำงานของระบบโดยภาพรวม



รูปที่ 3.2 ยูสเคสไดอะแกรมของระบบบริหารเครือข่ายแบบค้นหา

จากแผนภาพยูสเคสการทำงานของระบบบริหารเครือข่ายแบบค้นหา จะมีการทำงานอยู่สองส่วนคือ ระบบการค้นหาอุปกรณ์เครือข่ายที่เชื่อมต่อ และ ระบบแสดงผลในรูปเว็บไซต์ ซึ่งในแต่ละส่วนจะมีหน้าที่การทำงานดังต่อไปนี้

3.1.1 ระบบการค้นหาอุปกรณ์เครือข่าย

ระบบการค้นหาอุปกรณ์เครือข่าย เป็นระบบที่ทำงานอยู่เบื้องหลัง ทำหน้าที่แสกนหาอุปกรณ์เครือข่าย โดยผู้ดูแลเครือข่ายจะเป็นคนสั่งให้ระบบทำงาน ซึ่งระบบจะสามารถทำงานได้ก็ต่อเมื่อคอมพิวเตอร์ที่โปรแกรมค้นหาทำงานอยู่ได้มีการเชื่อมต่อกับเครือข่าย และสามารถใช้งานได้เป็นปกติ

ระบบจะทำงานเพื่อค้นหาอุปกรณ์เครือข่าย และรวบรวมเก็บไว้ในฐานข้อมูลที่สร้างขึ้น เพื่อที่ให้ระบบเว็บไซต์เรียกประมวลผลใช้งานเพื่อแสดงข้อมูลในรูปแบบต่างๆ เช่น แสดงรายการอุปกรณ์ แสดงแผนภาพการเชื่อมต่อของอุปกรณ์เครือข่าย (Topology) ซึ่งจะแสดงแผนภาพการเชื่อมต่อเครือข่ายของอุปกรณ์เครือข่ายเลเยอร์ 3 และแผนภาพการเชื่อมต่อของอุปกรณ์เครือข่าย

เลเยอร์ 2 แสดงข้อมูลการส่งผ่านของแต่ละอินเทอร์เฟส และแสดงรายการตรวจจับข้อความ Trap ที่ถูกส่งมาจากอุปกรณ์เครือข่ายในกรณีที่เกิดเหตุการณ์บนอุปกรณ์เครือข่ายตัวนั้นๆ

3.1.2 ซอฟต์แวร์ระบบ

หลังจากการทำงานของระบบค้นหาอุปกรณ์เครือข่ายที่เชื่อมต่อในระบบทำงานเสร็จแล้ว เราก็จะได้ชุดข้อมูลของอุปกรณ์เครือข่าย โดยจะนำข้อมูลที่ได้นั้นมาแสดงผลในรูปแบบของเว็บไซต์ ซึ่งในซอฟต์แวร์ระบบมีความสามารถดังต่อไปนี้ คือ

1. แสดงรายการของอุปกรณ์เครือข่าย

ซอฟต์แวร์ระบบสามารถแสดงรายการอุปกรณ์เครือข่ายทั้งหมด โดยจะแสดงข้อมูลตามที่ได้จัดเก็บไว้ในฐานข้อมูล และสามารถนำข้อมูลเหล่านี้ออกมาในรูปแบบ excel ได้เพื่อสามารถนำไปเป็นรายงานอุปกรณ์เครือข่ายได้

2. แสดงแผนภาพการเชื่อมต่อของอุปกรณ์เครือข่าย (Topology)

ซอฟต์แวร์ระบบจะนำข้อมูลของอุปกรณ์เครือข่ายที่ค้นหาได้มาแสดงเป็นแผนภาพการเชื่อมต่อ โดยจะแบ่งเป็นสองแผนภาพคือ แผนภาพการเชื่อต่อของอุปกรณ์เครือข่ายเลเยอร์ 3 ซึ่งเป็นโครงสร้างหลักของระบบเครือข่ายที่ทำการทดสอบ และ แผนภาพการเชื่อมต่อของอุปกรณ์เครือข่ายเลเยอร์ 2 ที่มีการเชื่อมต่ออยู่กับอุปกรณ์เครือข่ายเลเยอร์ 3 ตัวหนึ่งๆ

3. แสดงรายละเอียดของอินเตอร์เฟสบนตัวอุปกรณ์เครือข่าย

ซอฟต์แวร์ระบบจะเชื่อมต่อโปรโตรคอล SNMP เพื่อดึงข้อมูลของตาราง ifTable มาแสดงผลเพื่อเป็นข้อมูลว่าที่อุปกรณ์ตัวหนึ่งๆ มีปริมาณการใช้งานมากเพียงใดและเพื่อเก็บข้อมูลปริมาณการใช้งานบนอินเตอร์เฟสนั้นๆด้วย

4. แสดงการตรวจจับการใช้งานบนอินเตอร์เฟส

ที่อินเตอร์เฟสบนอุปกรณ์เครือข่ายซอฟต์แวร์ระบบมีการดึงข้อมูลการรับส่งข้อความมาแสดงเป็นกราฟ เพื่อดูปริมาณการใช้งานบนอินเตอร์เฟสใดๆได้ โดยในส่วนนี้จะใช้การดึงข้อมูลเป็นช่วงเวลา (pooling) เพื่อนำข้อมูลในแต่ละช่วงเวลามาแสดงในรูปแบบกราฟ โดยได้ออกแบบให้มีการดึงข้อมูลทุกๆ 5 นาที

5. แสดงข้อความ Trap ที่ถูกส่งออกมาจากอุปกรณ์เครือข่าย

ระบบสามารถตรวจสอบข้อความ Trap ที่ถูกส่งออกมาจากอุปกรณ์เครือข่ายเมื่อเกิดเหตุการณ์ไม่ปกติขึ้นกับอุปกรณ์เครือข่ายตัวนั้นๆ ซึ่งมีการออกแบบให้ผู้ดูแลเครือข่ายสามารถตรวจสอบข้อความผ่านทางเว็บไซต์ระบบ และการส่งอีเมลไปยังผู้ดูแลเครือข่ายได้

3.2 สมมติฐานของระบบ

1. การเชื่อมต่อของอุปกรณ์เครือข่าย คอมพิวเตอร์ที่ทำงานในส่วนของโปรแกรมการค้นหาอุปกรณ์เครือข่าย ต้องมีการเชื่อมต่อกับเครือข่ายที่จะทำการค้นหา และต้องสามารถติดต่อกับเครือข่ายย่อยๆได้

2. โปรโตคอล SNMP ระบบนี้ตั้งอยู่บนสมมติฐานที่ อุปกรณ์เครือข่ายที่ใช้งานนั้นต้องมีการคอนฟิกเพื่อเปิดใช้งานโปรโตคอล SNMPv1 และ SNMPv2 เท่านั้น โดยที่ระบบไม่สามารถใช้กับโปรโตคอล SNMPv3

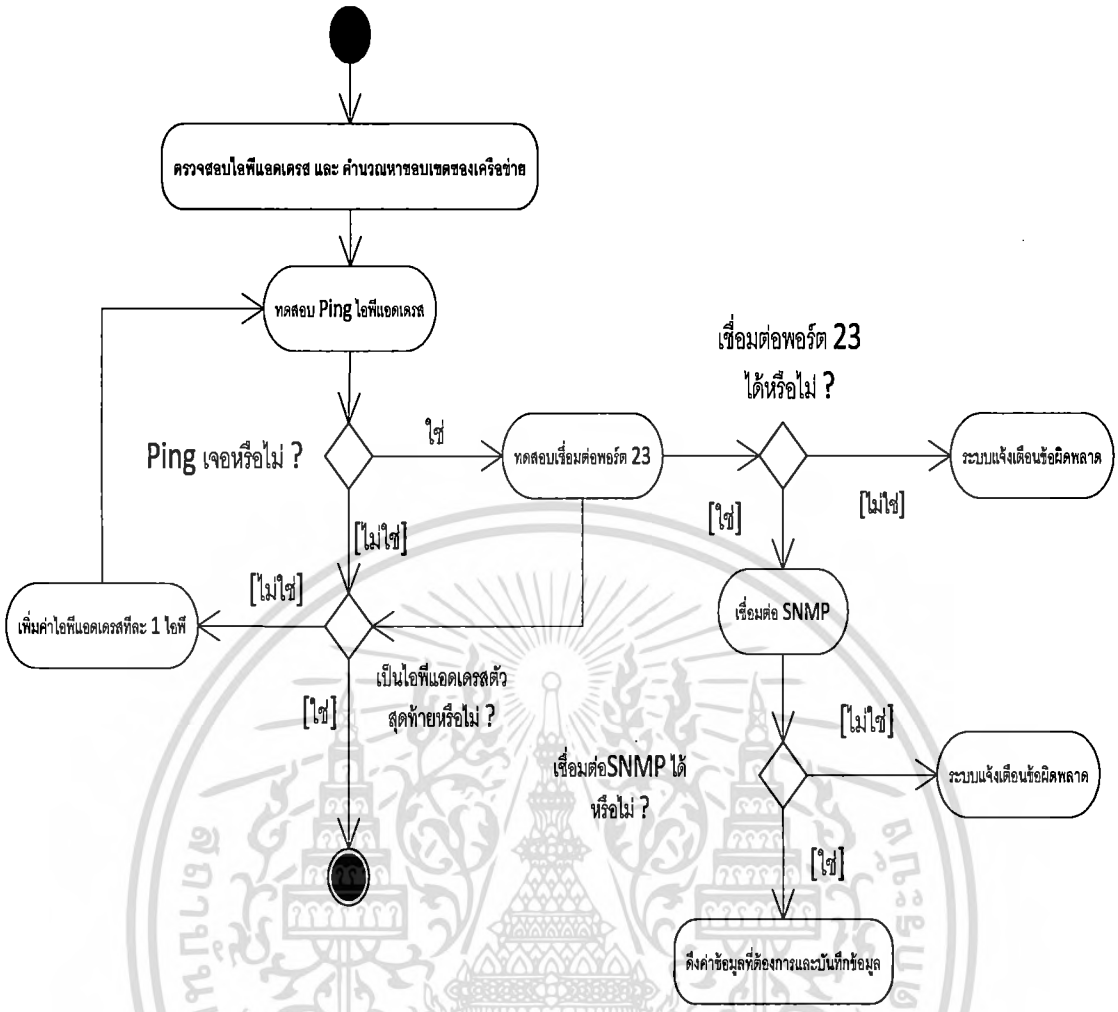
3. อุปกรณ์เครือข่ายที่เชื่อมต่อในระบบทดสอบต้องให้บริการโปรโตคอล SNMP

4. SNMP community อุปกรณ์เครือข่ายที่เชื่อมต่อในระบบทดสอบต้องให้บริการโปรโตคอล SNMP Community string ที่ใช้ในการเชื่อมต่อระหว่างเอเจนต์และแมเนเจอร์นั้น ต้องใช้ community string ตัวเดียวกันทั้งระบบ ทั้งนี้เนื่องเพื่อให้เป็นมาตรฐานและความสะดวกของโปรแกรมในการเชื่อมต่อโปรโตคอล SNMP ซึ่งอาจจะต้องมีการเชื่อมต่อหลายๆครั้ง

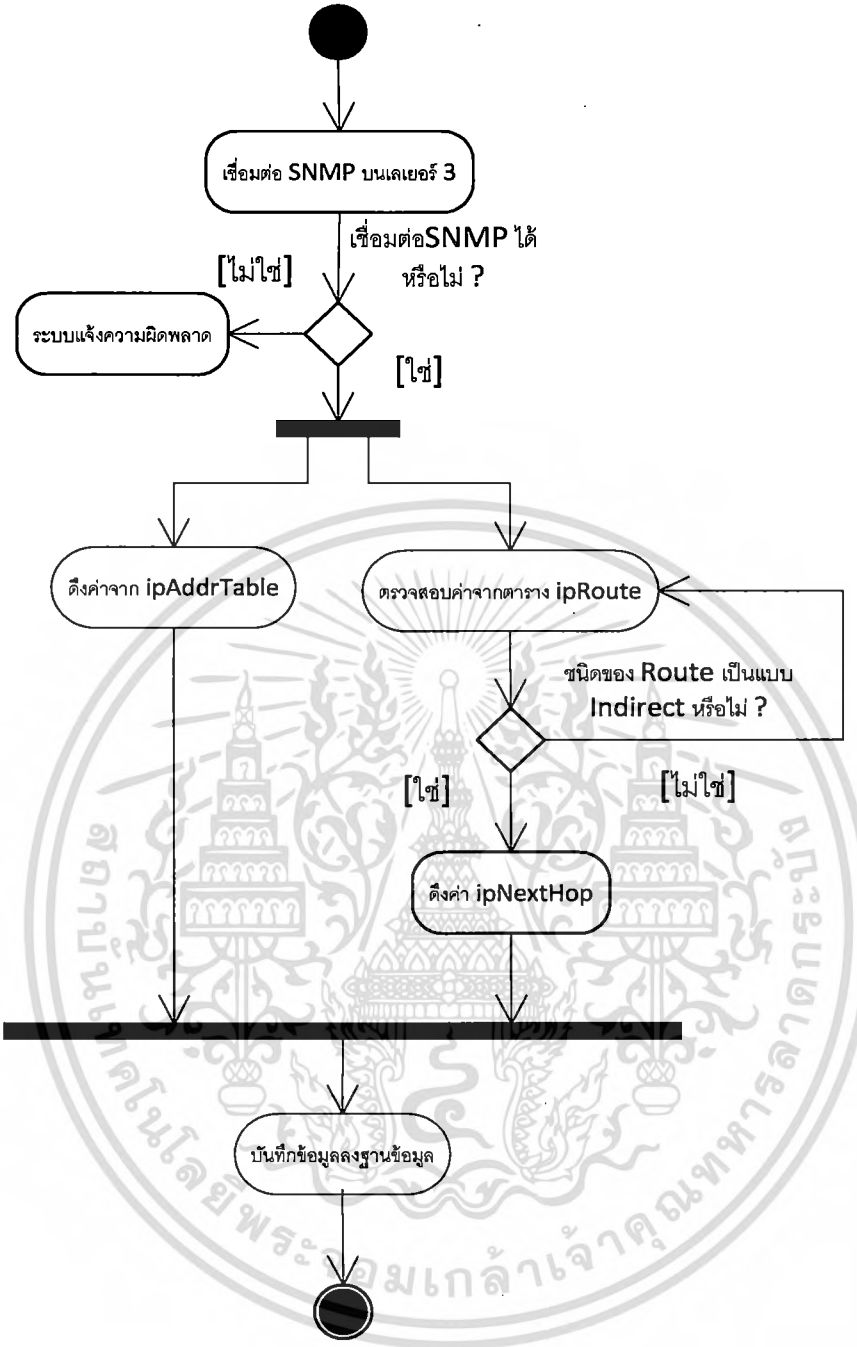
3.3 แผนภาพกิจกรรมของระบบ

แผนภาพกิจกรรมของระบบค้นหาอุปกรณ์เครือข่าย ซึ่งจะแสดงแผนภาพกิจกรรมหลักๆของระบบบริหารจัดการเครือข่ายแบบค้นหาตามที่ได้วิเคราะห์และออกแบบมา ดังนี้

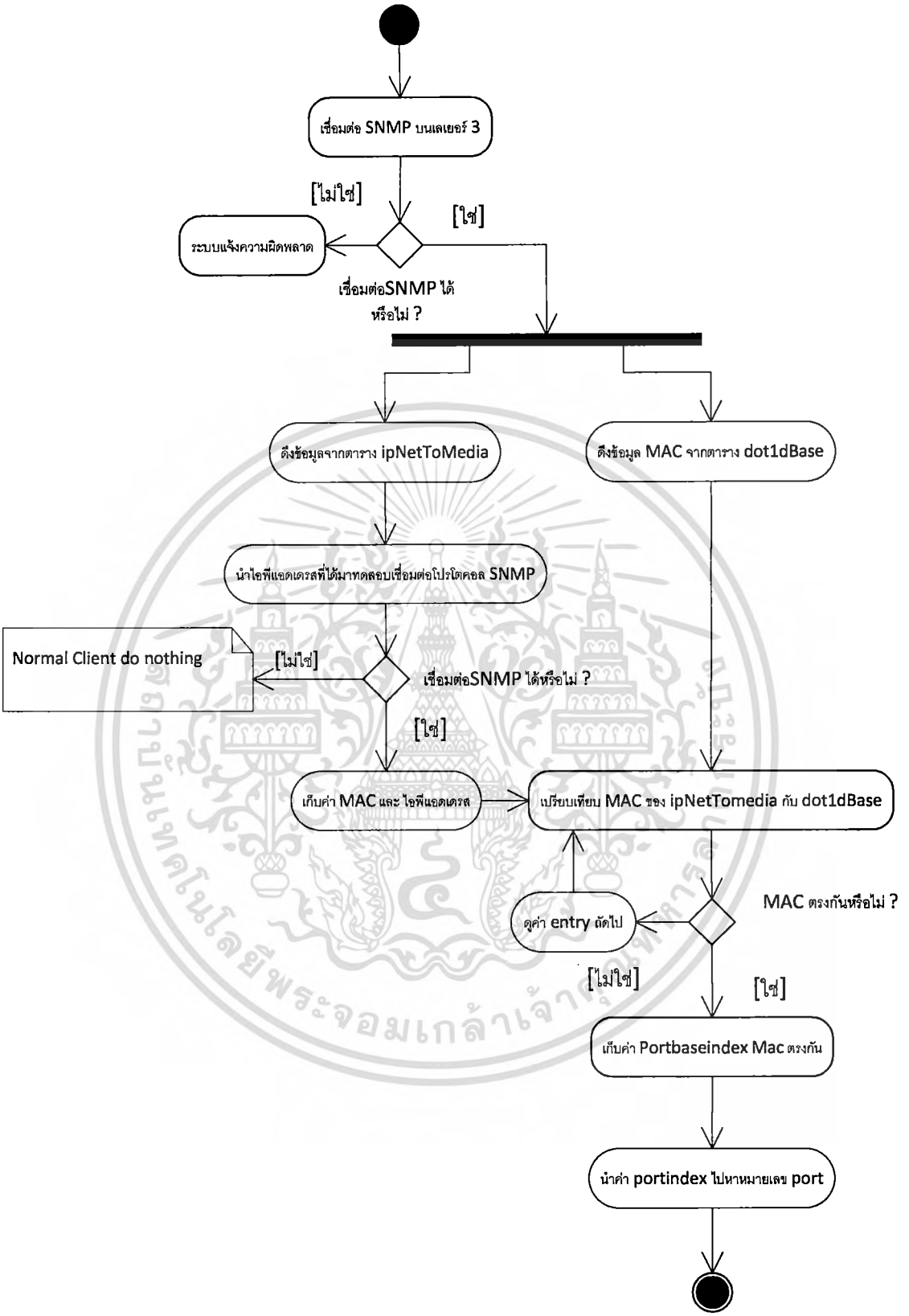
- แผนภาพกิจกรรมการแสกนไอพีเครือข่าย
- แผนภาพกิจกรรมของระบบค้นหาอุปกรณ์เครือข่าย
- แผนภาพกิจกรรมของระบบค้นหาการเชื่อมต่ออุปกรณ์เครือข่าย



รูปที่ 3.3 แผนภาพกิจกรรมการแสกนไอพีเครือข่ายซึ่งเป็นจุดเริ่มต้นของการค้นหาอุปกรณ์เครือข่าย



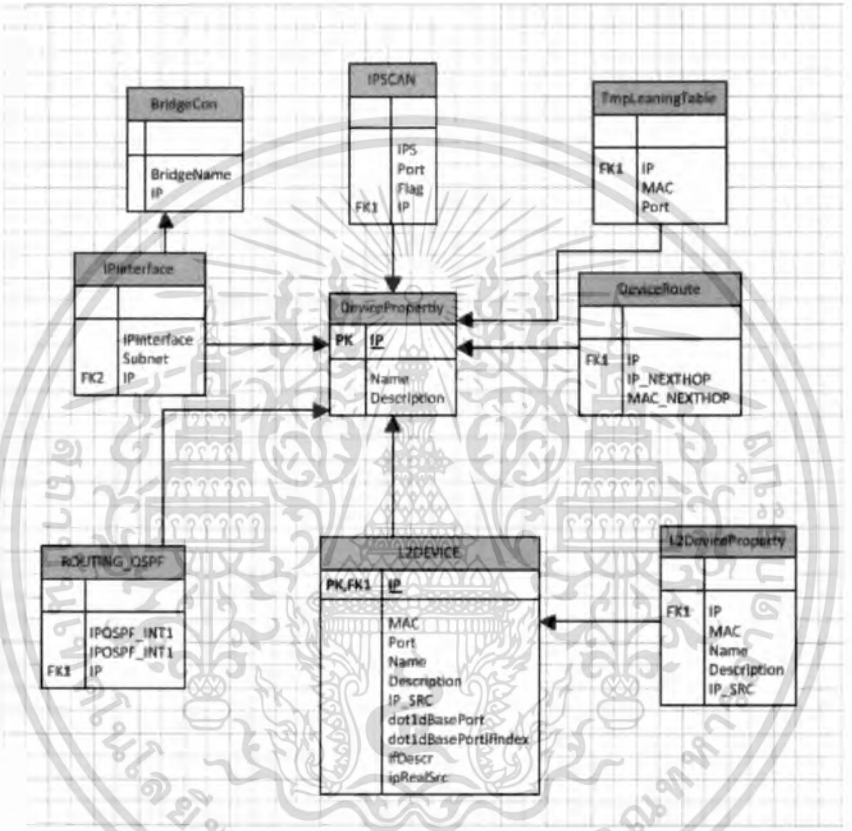
รูปที่ 3.4 แผนภาพกิจกรรมของระบบค้นหาอุปกรณ์เครือข่าย



รูปที่ 3.5 แผนภาพกิจกรรมของระบบค้นหาการเชื่อมต่อของอุปกรณ์เครือข่าย

3.4 ระบบฐานข้อมูล

หลังจากขั้นตอนการออกแบบขั้นตอนการทำงานของตัวระบบ เราจะได้ข้อมูลเพื่อนำมาสร้างฐานข้อมูลของระบบเพื่อจัดเก็บข้อมูลที่ค้นหาได้และเพื่อนำข้อมูลเหล่านั้นไปใช้งานต่อไป โดยได้มีการออกแบบฐานซึ่งจะมีโครงสร้างตารางดังต่อไปนี้ และระบบที่พัฒนาขึ้นจะใช้ SQL เป็นซอฟต์แวร์ในการจัดการฐานข้อมูล



รูปที่ 3.6 แผนภาพความสัมพันธ์ระหว่างตารางในฐานข้อมูล

บทที่ 4
ต้นแบบระบบบริหารดูแลเครือข่ายแบบค้นหา

4.1 ส่วนประกอบของระบบ

4.1.1 ผู้ใช้งานระบบ

ผู้ใช้งานระบบบริหารจัดการเครือข่ายแบบค้นหา ในโปรแกรมต้นแบบที่พัฒนาขึ้นนี้จะมีเฉพาะ administrator เป็นผู้ใช้งานเท่านั้น โดย administrator จะทำหน้าที่ในการสั่งให้โปรแกรมค้นหาอุปกรณ์เครือข่ายเริ่มต้นทำงาน รวมไปถึง คอยตรวจสอบข้อมูลที่ค้นหามาได้มีความถูกต้องมากน้อยแค่ไหน และในส่วนระบบแสดงผล ก็จะสามารถเรียกใช้งานได้ทุกฟังก์ชั่น ซึ่งในอนาคตก็จะมีการพัฒนาให้มีระบบลอกอินเพื่อจำแนกยูสเซอร์ที่จะเข้ามาใช้งานในระบบแสดงผล

4.1.2 ระบบเครือข่าย และ อุปกรณ์เครือข่าย

ระบบเครือข่ายและอุปกรณ์เครือข่าย เนื่องจากระบบบริหารจัดการเครือข่ายแบบค้นหาที่พัฒนาขึ้นจะสามารถทำงานได้ก็ต่อเมื่อระบบมีการเชื่อมต่ออยู่ในระบบเครือข่าย และผู้พัฒนาไม่มีทรัพยากรที่เพียงพอในการจำลองระบบเครือข่ายเพื่อใช้ในการทดสอบระบบ ดังนั้นจึงมีความจำเป็นที่จะต้องทดสอบระบบเครือข่ายของบริษัท ซึ่งทำให้การเข้าถึงข้อมูลอุปกรณ์เครือข่ายไม่สมบูรณ์เนื่องจากไม่สามารถเข้าถึงอุปกรณ์เครือข่ายเหล่านั้นได้

4.1.3 ระบบฐานข้อมูล

ฐานข้อมูลของระบบเมื่อระบบค้นหาอุปกรณ์ทำงานเสร็จสิ้นจึงจะได้ข้อมูลของอุปกรณ์เครือข่ายที่สมบูรณ์ และจะจัดเก็บไว้ในที่ซอฟต์แวร์ระบบสามารถเรียกใช้งานเพื่อที่จะนำข้อมูลมานำเสนอบนเว็บไซต์ได้ และยังมีข้อมูลบางส่วนที่จะต้องมีการเก็บข้อมูลอย่างต่อเนื่องหลังจากโปรแกรมการค้นหาทำงานเสร็จแล้ว เช่น ข้อมูลการรับส่งข้อความบนอินเตอร์เฟสต่างๆของอุปกรณ์เครือข่าย

4.1.4 ซอฟต์แวร์ระบบ

ซอฟต์แวร์ที่ใช้ในระบบบริหารจัดการเครือข่ายแบบค้นหานี้ถูกพัฒนาขึ้นด้วยภาษา VB.net บนเครื่องคอมพิวเตอร์ที่ติดตั้งระบบปฏิบัติการไมโครซอฟต์วินโดว์เซเว่น (Microsoft Window 7)

4.2 การทำงานของระบบ

4.2.1 การค้นหาอุปกรณ์

ขั้นตอนวิธีในการค้นหาอุปกรณ์เครือข่ายที่เชื่อมต่ออยู่ในระบบด้วยระบบบริหารดูแลเครือข่ายแบบค้นหา จะใช้โครงสร้างฐานข้อมูลของ SNMP โปรโตคอลดังที่ได้กล่าวมาจากหัวข้อก่อนหน้า ซึ่งจะได้ข้อมูลในการค้นหาอุปกรณ์เครือข่ายที่เชื่อมต่ออยู่ในระบบ โดยที่สามารถค้นหาอุปกรณ์เครือข่ายที่ทำงานอยู่ในเลเยอร์ 3 และเลเยอร์ 2 รวมทั้งยังสามารถค้นหาได้ถึง อุปกรณ์ที่เชื่อมต่อในระดับปลายทาง เช่น อุปกรณ์คอมพิวเตอร์ เครื่องถ่ายเอกสาร หรือเครื่องพิมพ์เอกสาร เป็นต้น ซึ่งจะมีขั้นตอนและวิธีการดังต่อไปนี้ ระบบจะเริ่มด้วยการตรวจสอบหมายเลขไอพีแอดเดรส หมายเลขซับเน็ตมาสก์ และ ค่าดีฟอลต์เกตเวย์ของเครื่องที่รันระบบ และจะทำการคำนวณขอบเขตของเครือข่ายที่เครื่องที่ระบบค้นหาอุปกรณ์เครือข่ายเชื่อมต่ออยู่ หลังจากนั้นในรอบแรกระบบจะทำการค้นหาไอพีแอดเดรสในขอบเขตที่เชื่อมต่ออยู่ด้วยการทดสอบด้วยโปรโตคอล ICMP จากการ PING ไปยังทุกไอพีแอดเดรสที่คำนวณได้ หากไอพีแอดเดรสใดที่ส่ง message reply กลับมาแสดงว่าไอพีนั้นๆมีการเชื่อมต่ออยู่และระบบก็จะทำการทดลองเชื่อมต่อโดยโปรโตคอล SNMP หากเชื่อมต่อไอพีแอดเดรสใดๆได้ก็แสดงว่าไอพีแอดเดรสนั้นคืออุปกรณ์เครือข่าย ก็จะทำการเข้าไปเอาข้อมูลของโปรโตคอล SNMP และมีการจัดเก็บลงฐานข้อมูลของระบบ ซึ่งในครั้งแรกของการค้นหานี้ จะมีอย่างน้อย 1 ไอพีแอดเดรสที่สามารถเชื่อมต่อโปรโตคอล SNMP ได้ คือ ไอพีของดีฟอลต์เกตเวย์ ซึ่งดีฟอลต์เกตเวย์อาจจะเป็นไอพีแอดเดรสของอินเตอร์เฟสหนึ่งของเราต์เตอร์หรืออาจจะเป็นไอพีอินเทอร์เฟสของอุปกรณ์เน็ตเวิร์กนั่นเอง

เราจะพบว่าเมื่อเชื่อมต่อโปรโตคอล SNMP และสามารถดึงข้อมูลจากฐานข้อมูล MIB มาได้แล้วนั้นการที่จะหาตัวอุปกรณ์เน็ตเวิร์กเพื่อมาสร้างโทโพโลยีนั้นเราจะใช้ชุดข้อมูลของฐานข้อมูลการหาเส้นทาง(routing) ของอุปกรณ์เครือข่ายที่ทำงานอยู่บนเลเยอร์ 3 ซึ่งจะถูกจัดเก็บในตาราง ipRouteTable ของโปรโตคอล SNMP โดยเราจะสนใจเฉพาะชุดข้อมูล ipRouteNextHop และ ipRouteType ของตารางนี้เท่านั้นซึ่งจะได้ข้อมูลการเชื่อมต่อของอุปกรณ์เลเยอร์ 3 ipRouteNextHop จะหมายถึงค่าไอพีแอดเดรสของอุปกรณ์ตัวถัดไป และค่าของ ipRouteType คือชนิดของการเรียนรู้เส้นทางของอุปกรณ์ตัวนั้นๆ ซึ่งจะมีอยู่ด้วยกัน 4 ค่า คือ indirect , direct , invalid และ other เราจะสนใจเฉพาะเส้นทางที่เป็นชนิด indirect ซึ่งจะหมายความว่า เป็นเส้นทางที่ไม่ได้สร้างจากอุปกรณ์นั้นๆ และจะมีการเรียนรู้มาจากอุปกรณ์ตัวอื่นๆ ผ่านทางอุปกรณ์ตัวถัดไป (next hop)

จากข้อมูล ipRouteTable เราจะใช้เพื่อค้นหาอุปกรณ์เลเยอร์ 3 แต่ในการค้นหาอุปกรณ์เลเยอร์ 2 นั้นเราจะใช้ข้อมูลจากตารางอื่นนั่นก็คือ ipNetToMediaTable เป็นตารางที่มีการเก็บข้อมูลที่

จับคู่กันของไอพีแอดเดรสกับ ฟิสิคัลแอดเดรส (MAC address) ข้อมูลในตาราง ipNetToMedia นี้จะได้มาจากการเรียนรู้มาจาก โปรโตคอล ARP และจะนำเอาไอพีแอดเดรสที่ได้จาก ตาราง ipNetToMedia มาทดสอบเชื่อมต่อโปรโตคอล SNMP ก่อนอีกครั้งเพื่อทดสอบว่าเป็นไอพีแอดเดรสของอุปกรณ์เครือข่ายหรือไม่ หากเชื่อมต่อได้ก็จะจัดเก็บข้อมูลลงฐานข้อมูลของระบบ

4.2.2 การค้นหาการเชื่อมต่อของอุปกรณ์

ในการค้นหาการเชื่อมต่อของอุปกรณ์นั้น หลังจากได้ไอพีแอดเดรสและ MAC Address จากการค้นหาอุปกรณ์ในขั้นตอนการค้นหาอุปกรณ์เครือข่าย หลังจากนั้นระบบจะทำการดึงข้อมูลจากออบเจ็ค Bridge MIB โดยจะใช้ข้อมูล จากตาราง dot1dBasePortEntry เพื่อหาข้อมูลของแต่ละพอร์ต และจากตาราง dot1dTpFdTable เพื่อตรวจสอบ MAC address ที่มีการส่งผ่านในแต่ละพอร์ต นำ MAC address มาเปรียบเทียบกับ MAC address ที่ค้นหาได้จากขั้นตอนการค้นหาอุปกรณ์เครือข่าย ซึ่งจะได้ข้อมูลของ MAC address และ ค่าของพอร์ต (dot1dTpFdbPort) ที่ MAC address มีการเรียนรู้เข้ามา และ จะเอาค่าพอร์ตไปเทียบกับ index ของตาราง dot1dBasePortEntry และตาราง ifTable ก็จะได้พอร์ตในการเชื่อมต่อของอุปกรณ์แต่ละตัว หากค่าของพอร์ตที่หามาได้มีค่า MAC address เพียงค่าเดียวแสดงว่า ที่พอร์ตนั้นๆ มีอุปกรณ์เครือข่ายเชื่อมต่ออยู่เพียงตัวเดียวก็สามารถเก็บข้อมูลของอุปกรณ์เครือข่ายและพอร์ตที่เชื่อมต่อลงฐานข้อมูลได้ แต่หากที่พอร์ตใดๆมี MAC address ที่เรียนรู้เข้ามามากกว่าหนึ่งแอดเดรส จะหมายความว่าพอร์ตนั้นมีการเชื่อมต่ออยู่กับอุปกรณ์เครือข่ายที่ มีอุปกรณ์เครือข่ายเชื่อมต่ออยู่บนตัวมันอีกที เราต้องหาว่าอุปกรณ์เครือข่ายที่เชื่อมต่อที่พอร์ตนั้นคือไอพีแอดเดรสอะไร แล้วเข้าไปค้นหาข้อมูลที่ ตาราง dot1dBasePortEntry และ dot1dTpFdTable อีกครั้งก็จะได้การเชื่อมต่อของอุปกรณ์เครือข่าย

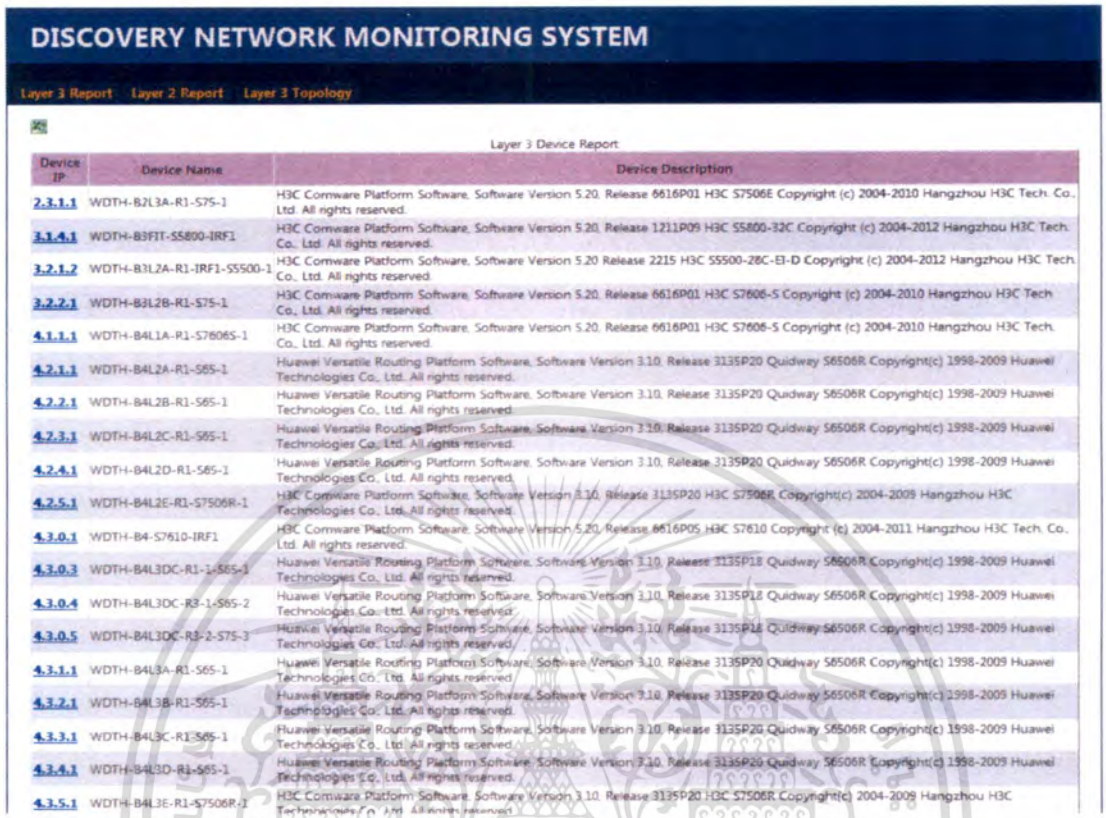
4.2.3 ขั้นตอนการวาดรูปเพื่อแสดงการเชื่อมต่อของอุปกรณ์

ในการวาดแผนภาพการเชื่อมต่อนั้นจะใช้ออบเจ็คของซอฟแวร์ nevron ซึ่งเป็น libraly ในการเขียน organization chart และสามารถดาวน์โหลดได้จากอินเตอร์เน็ต โดยหลังจากระบบค้นหาทำงานเสร็จแล้วนั้นจะเก็บข้อมูลรายละเอียดของอุปกรณ์เครือข่ายลงในฐานข้อมูลของระบบตามที่ได้ออกแบบไว้ โดยจะมีข้อมูลที่แยกกันของอุปกรณ์เครือข่ายเลเยอร์ 3 และอุปกรณ์เครือข่ายเลเยอร์ 2 และมีข้อมูลความสัมพันกันของแต่ละอุปกรณ์ด้วย ซอฟแวร์ระบบก็จะดึงข้อมูลจากฐานข้อมูลมาสร้างเป็นแผนภาพการเชื่อมต่อของอุปกรณ์ที่เลเยอร์ 3 และแผนภาพการเชื่อมต่อของอุปกรณ์เครือข่ายเลเยอร์ 2 บนอุปกรณ์เครือข่ายเลเยอร์ 3

4.2.4 ตรวจจับการส่งข้อความ Trap จากอุปกรณ์เครือข่าย

การตรวจสอบข้อความ Trap ที่ถูกส่งมาจากอุปกรณ์เครือข่าย ระบบบริหารจัดการเครือข่ายแบบค้นหาที่พัฒนาขึ้นมาจะสามารถรับข้อความ Trap ที่อุปกรณ์เครือข่ายส่งออกมาแจ้งเตือนเมื่อเกิดเหตุการณ์ขึ้นกับตัวอุปกรณ์เครือข่าย เช่น อินเทอร์เฟสอัพ หรือ อินเทอร์เฟสดาวน์ เป็นต้น โดยจะมีการแสดงผลผ่านทางเว็บไซต์ของระบบ รวมทั้งยังสามารถส่งอีเมลแจ้งเตือนไปให้กับผู้ดูแลเครือข่ายเพื่อความรวดเร็วได้เช่นกัน

4.3 ซอฟต์แวร์ระบบ



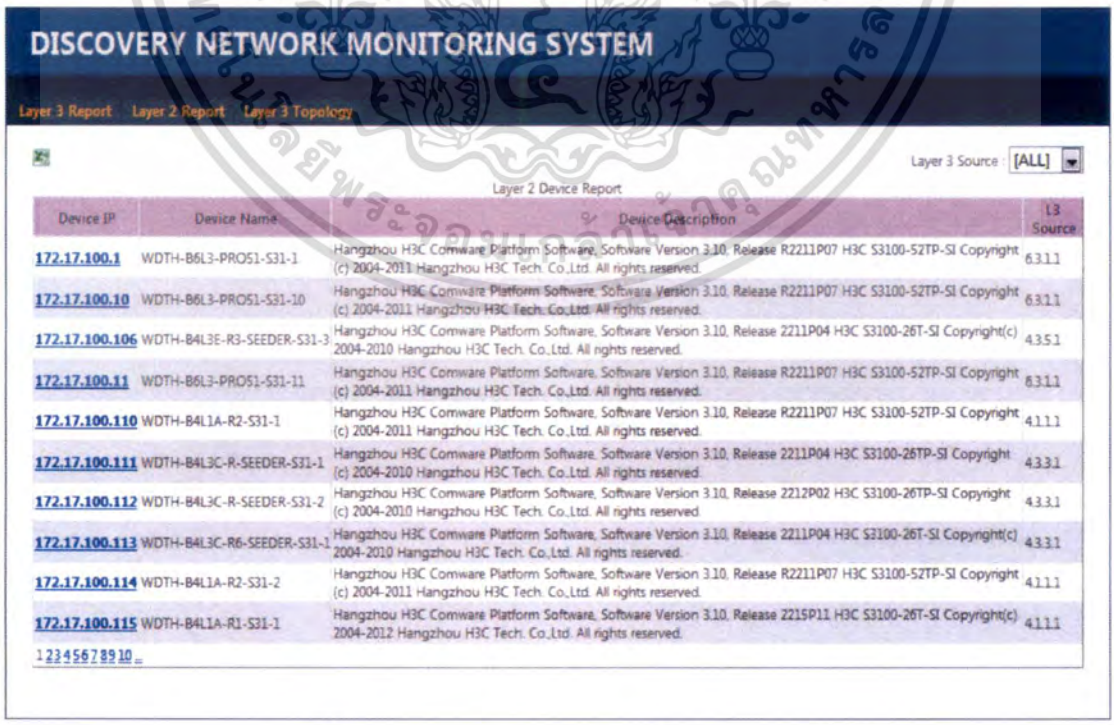
DISCOVERY NETWORK MONITORING SYSTEM

Layer 3 Report Layer 2 Report Layer 3 Topology

Layer 3 Device Report

Device IP	Device Name	Device Description
2.3.1.1	WDTH-B2L3A-R1-S7S-1	H3C Comware Platform Software, Software Version 5.20, Release 6616P01 H3C S7506E Copyright (c) 2004-2010 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
3.1.4.1	WDTH-B3FIT-S5800-IRF1	H3C Comware Platform Software, Software Version 5.20, Release 1211P09 H3C S5800-32C Copyright (c) 2004-2012 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
3.2.1.2	WDTH-B3L2A-R1-IRF1-S5500-1	H3C Comware Platform Software, Software Version 5.20 Release 2215 H3C S5500-28C-EI-D Copyright (c) 2004-2012 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
3.2.2.1	WDTH-B3L2B-R1-S7S-1	H3C Comware Platform Software, Software Version 5.20, Release 6616P01 H3C S7606-S Copyright (c) 2004-2010 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
4.1.1.1	WDTH-B4L1A-R1-S7606S-1	H3C Comware Platform Software, Software Version 5.20, Release 6616P01 H3C S7606-S Copyright (c) 2004-2010 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
4.2.1.1	WDTH-B4L2A-R1-S6S-1	Huawei Versatile Routing Platform Software, Software Version 3.10, Release 3135P20 Quidway S6506R Copyright(c) 1998-2009 Huawei Technologies Co., Ltd. All rights reserved.
4.2.2.1	WDTH-B4L2B-R1-S6S-1	Huawei Versatile Routing Platform Software, Software Version 3.10, Release 3135P20 Quidway S6506R Copyright(c) 1998-2009 Huawei Technologies Co., Ltd. All rights reserved.
4.2.3.1	WDTH-B4L2C-R1-S6S-1	Huawei Versatile Routing Platform Software, Software Version 3.10, Release 3135P20 Quidway S6506R Copyright(c) 1998-2009 Huawei Technologies Co., Ltd. All rights reserved.
4.2.4.1	WDTH-B4L2D-R1-S6S-1	Huawei Versatile Routing Platform Software, Software Version 3.10, Release 3135P20 Quidway S6506R Copyright(c) 1998-2009 Huawei Technologies Co., Ltd. All rights reserved.
4.2.5.1	WDTH-B4L2E-R1-S7506R-1	H3C Comware Platform Software, Software Version 3.10, Release 3135P20 H3C S7506E Copyright(c) 2004-2009 Hangzhou H3C Technologies Co., Ltd. All rights reserved.
4.3.0.1	WDTH-B4-S7610-IRF1	H3C Comware Platform Software, Software Version 5.20, Release 6616P05 H3C S7610 Copyright (c) 2004-2011 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
4.3.0.3	WDTH-B4L3DC-R1-1-S6S-1	Huawei Versatile Routing Platform Software, Software Version 3.10, Release 3135P18 Quidway S6506R Copyright(c) 1998-2009 Huawei Technologies Co., Ltd. All rights reserved.
4.3.0.4	WDTH-B4L3DC-R3-1-S6S-2	Huawei Versatile Routing Platform Software, Software Version 3.10, Release 3135P18 Quidway S6506R Copyright(c) 1998-2009 Huawei Technologies Co., Ltd. All rights reserved.
4.3.0.5	WDTH-B4L3DC-R3-2-S7S-3	Huawei Versatile Routing Platform Software, Software Version 3.10, Release 3135P18 Quidway S6506R Copyright(c) 1998-2009 Huawei Technologies Co., Ltd. All rights reserved.
4.3.1.1	WDTH-B4L3A-R1-S6S-1	Huawei Versatile Routing Platform Software, Software Version 3.10, Release 3135P20 Quidway S6506R Copyright(c) 1998-2009 Huawei Technologies Co., Ltd. All rights reserved.
4.3.2.1	WDTH-B4L3B-R1-S6S-1	Huawei Versatile Routing Platform Software, Software Version 3.10, Release 3135P20 Quidway S6506R Copyright(c) 1998-2009 Huawei Technologies Co., Ltd. All rights reserved.
4.3.3.1	WDTH-B4L3C-R1-S6S-1	Huawei Versatile Routing Platform Software, Software Version 3.10, Release 3135P20 Quidway S6506R Copyright(c) 1998-2009 Huawei Technologies Co., Ltd. All rights reserved.
4.3.4.1	WDTH-B4L3D-R1-S6S-1	Huawei Versatile Routing Platform Software, Software Version 3.10, Release 3135P20 Quidway S6506R Copyright(c) 1998-2009 Huawei Technologies Co., Ltd. All rights reserved.
4.3.5.1	WDTH-B4L3E-R1-S7506R-1	H3C Comware Platform Software, Software Version 3.10, Release 3135P20 H3C S7506R Copyright(c) 2004-2009 Hangzhou H3C Technologies Co., Ltd. All rights reserved.

รูปที่ 4.1 แสดงรายการอุปกรณ์เครือข่ายเลเยอร์ 3



DISCOVERY NETWORK MONITORING SYSTEM

Layer 3 Report Layer 2 Report Layer 3 Topology

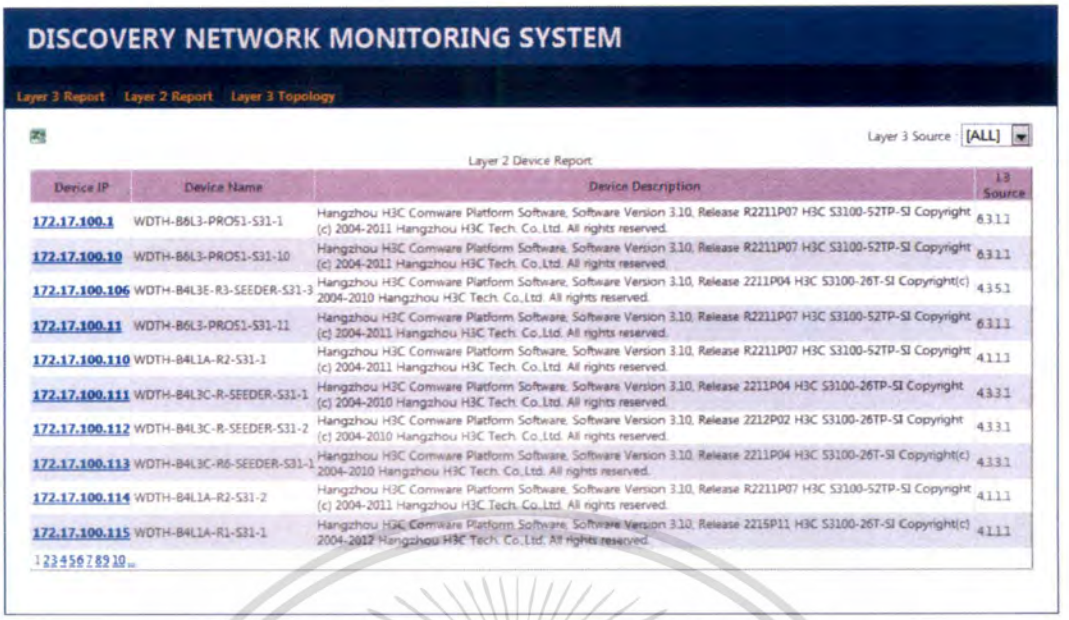
Layer 3 Source [ALL]

Layer 2 Device Report

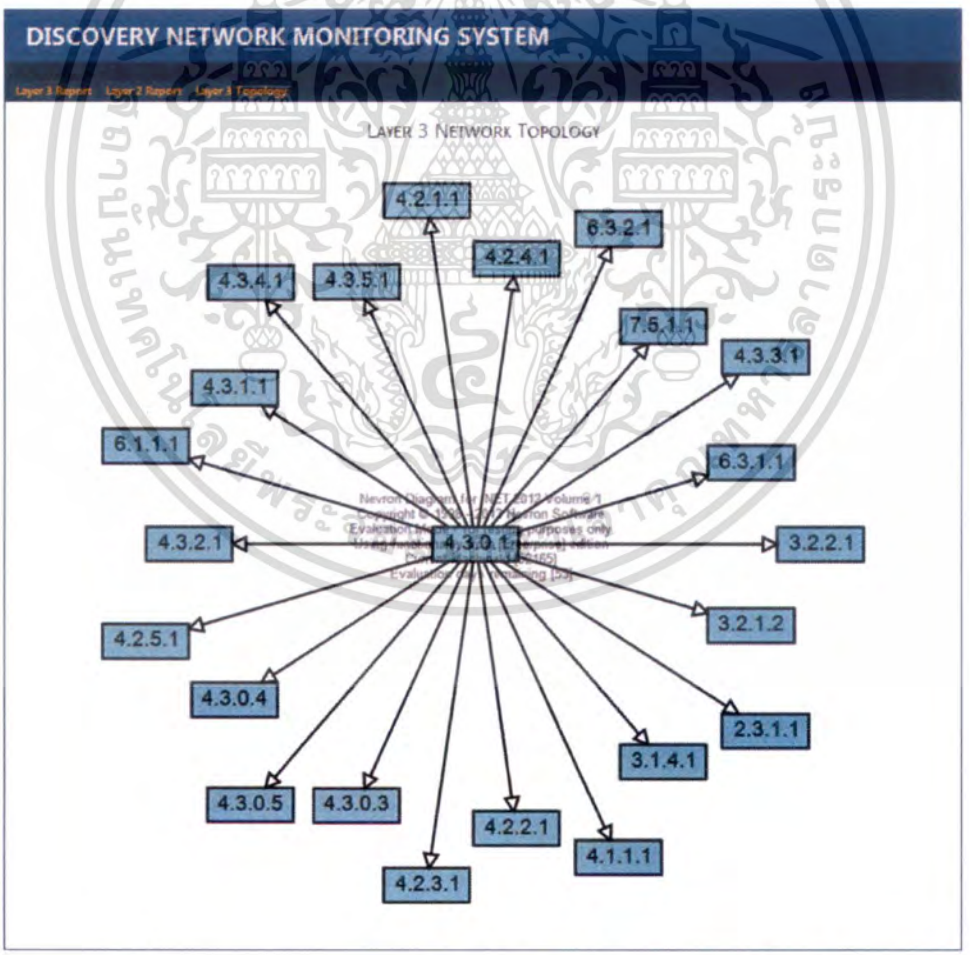
Device IP	Device Name	Device Description	L3 Source
172.17.100.1	WDTH-B6L3-PRO51-S31-1	Hangzhou H3C Comware Platform Software, Software Version 3.10, Release R2211P07 H3C S3100-52TP-SI Copyright (c) 2004-2011 Hangzhou H3C Tech. Co.,Ltd. All rights reserved.	63.1.1
172.17.100.10	WDTH-B6L3-PRO51-S31-10	Hangzhou H3C Comware Platform Software, Software Version 3.10, Release R2211P07 H3C S3100-52TP-SI Copyright (c) 2004-2011 Hangzhou H3C Tech. Co.,Ltd. All rights reserved.	63.1.1
172.17.100.106	WDTH-B4L3E-R3-SEEDER-S31-3	Hangzhou H3C Comware Platform Software, Software Version 3.10, Release 2211P04 H3C S3100-26T-SI Copyright(c) 2004-2010 Hangzhou H3C Tech. Co.,Ltd. All rights reserved.	43.5.1
172.17.100.11	WDTH-B6L3-PRO51-S31-11	Hangzhou H3C Comware Platform Software, Software Version 3.10, Release R2211P07 H3C S3100-52TP-SI Copyright (c) 2004-2011 Hangzhou H3C Tech. Co.,Ltd. All rights reserved.	63.1.1
172.17.100.110	WDTH-B4L1A-R2-S31-1	Hangzhou H3C Comware Platform Software, Software Version 3.10, Release R2211P07 H3C S3100-52TP-SI Copyright (c) 2004-2011 Hangzhou H3C Tech. Co.,Ltd. All rights reserved.	41.1.1
172.17.100.111	WDTH-B4L3C-R-SEEDER-S31-1	Hangzhou H3C Comware Platform Software, Software Version 3.10, Release 2211P04 H3C S3100-26TP-SI Copyright (c) 2004-2010 Hangzhou H3C Tech. Co.,Ltd. All rights reserved.	43.3.1
172.17.100.112	WDTH-B4L3C-R-SEEDER-S31-2	Hangzhou H3C Comware Platform Software, Software Version 3.10, Release 2212P02 H3C S3100-26TP-SI Copyright (c) 2004-2010 Hangzhou H3C Tech. Co.,Ltd. All rights reserved.	43.3.1
172.17.100.113	WDTH-B4L3C-R6-SEEDER-S31-1	Hangzhou H3C Comware Platform Software, Software Version 3.10, Release 2211P04 H3C S3100-26T-SI Copyright(c) 2004-2010 Hangzhou H3C Tech. Co.,Ltd. All rights reserved.	43.3.1
172.17.100.114	WDTH-B4L1A-R2-S31-2	Hangzhou H3C Comware Platform Software, Software Version 3.10, Release R2211P07 H3C S3100-52TP-SI Copyright (c) 2004-2011 Hangzhou H3C Tech. Co.,Ltd. All rights reserved.	41.1.1
172.17.100.115	WDTH-B4L1A-R1-S31-1	Hangzhou H3C Comware Platform Software, Software Version 3.10, Release 2215P11 H3C S3100-26T-SI Copyright(c) 2004-2012 Hangzhou H3C Tech. Co.,Ltd. All rights reserved.	41.1.1

1 2 3 4 5 6 7 8 9 10 ...

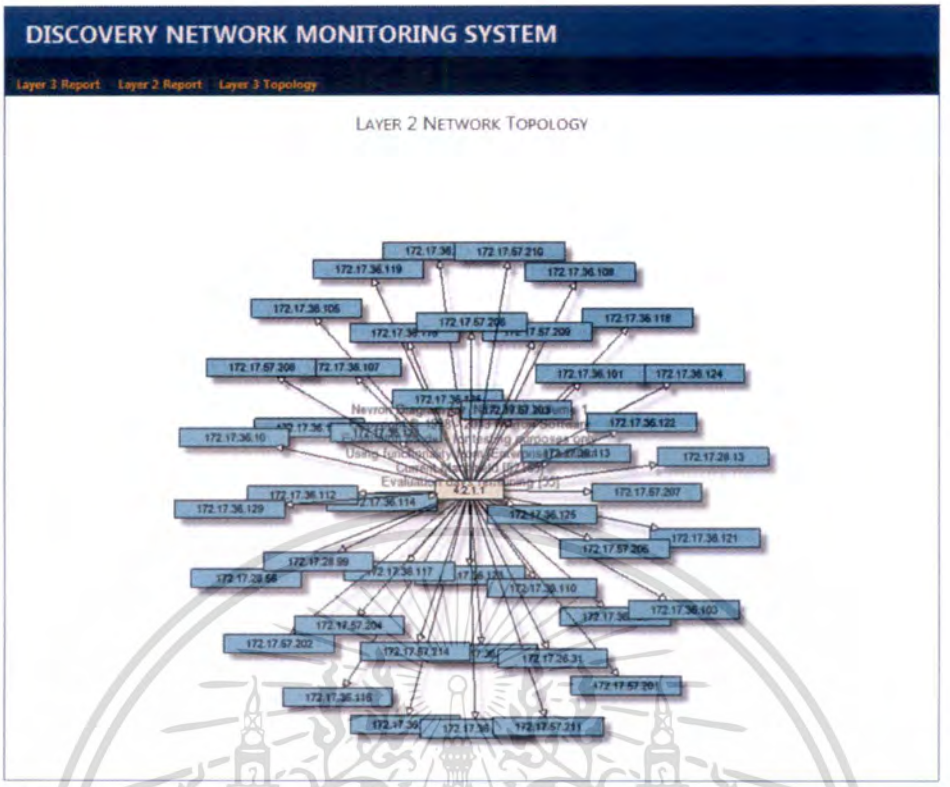
รูปที่ 4.2 แสดงรายการอุปกรณ์เครือข่ายเลเยอร์ 2



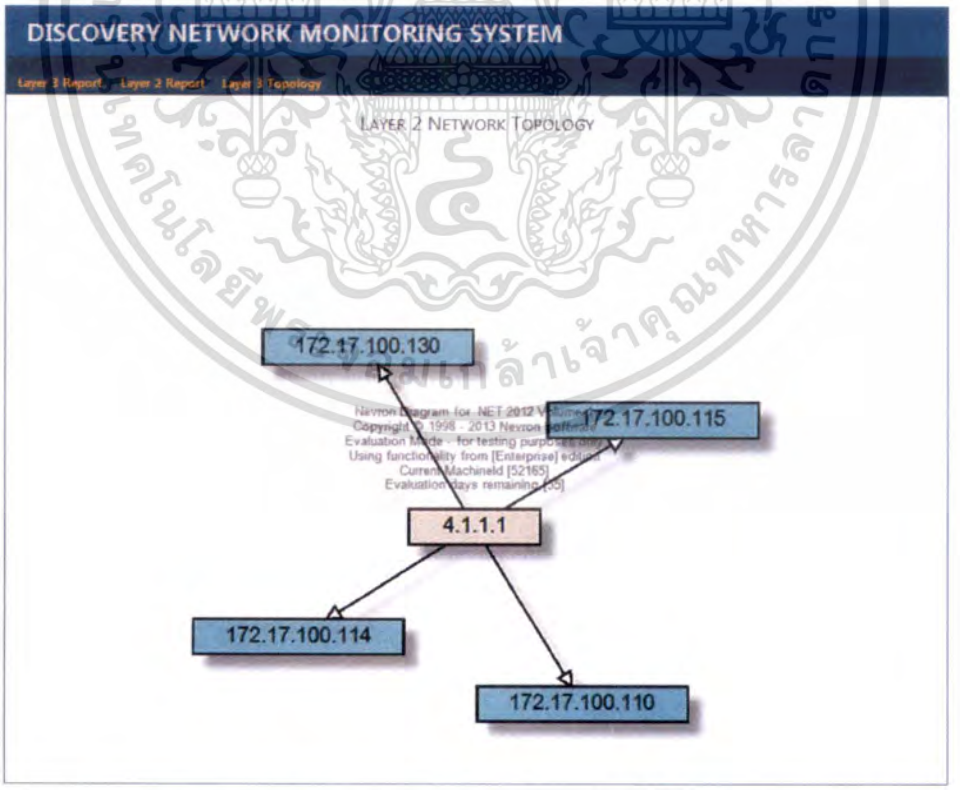
รูปที่ 4.3 แสดงรายการอุปกรณ์เครือข่ายเลเยอร์ แยกตาม source



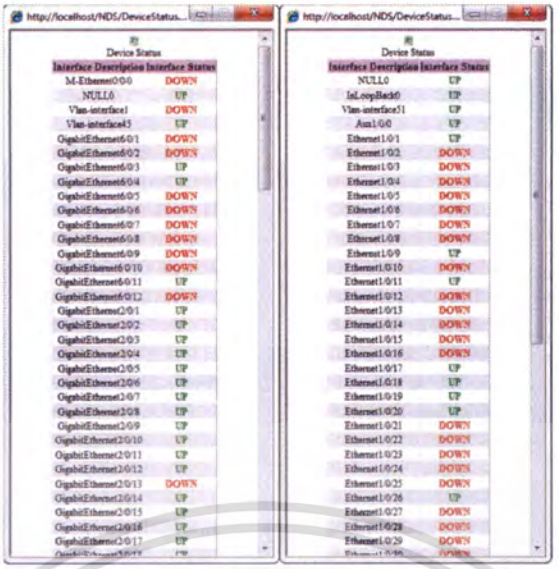
รูปที่ 4.4 แสดงการแผนภาพโทโพโลยีการเชื่อมต่ออุปกรณ์เลเยอร์ 3



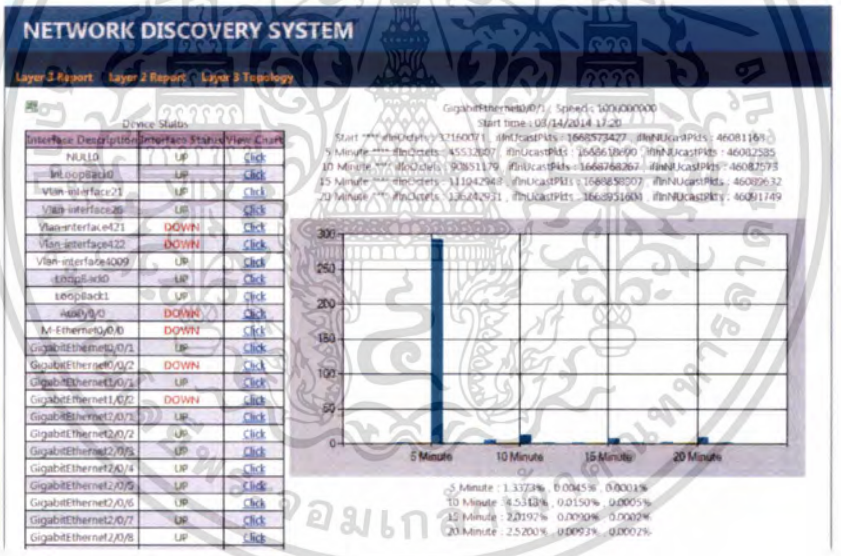
รูปที่ 4.5 ตัวอย่างแผนภาพโทโพโลยีของอุปกรณ์เลเยอร์ 2 ที่เชื่อมต่อบนอุปกรณ์เลเยอร์ 3



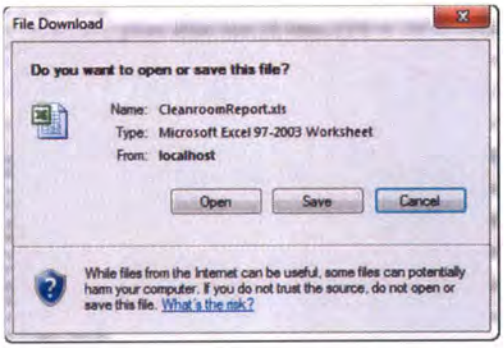
รูปที่ 4.6 ตัวอย่างแผนภาพโทโพโลยีของอุปกรณ์เลเยอร์ 2 ที่เชื่อมต่อบนอุปกรณ์เลเยอร์ 3



รูปที่ 4.7 หน้าต่างแสดงข้อมูลของอินเทอร์เฟสบนอุปกรณ์เลเยอร์ 3 และ เลเยอร์ 2



รูปที่ 4.8 แสดงปริมาณข้อมูลที่ส่งผ่านพอร์ต

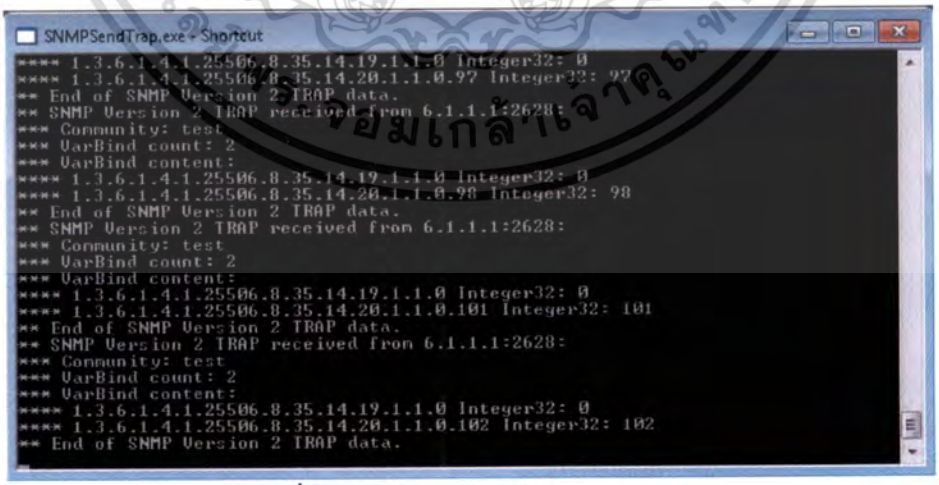


รูปที่ 4.9 ข้อความแสดงการร้องขอ export ข้อมูลในรูปแบบ excel

Layer 3 Device Report

Device IP	Device Name	Device Description
2.3.1.1	WDTH-B2L3A-R1-S75-1	H3C Comware Platform Software, Software Version 5.20, Release 6616P01 H3C S7506E Copyright (c) 2004-2010 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
3.1.4.1	WDTH-B3FIT-S5800-IRF1	H3C Comware Platform Software, Software Version 5.20, Release 1211P09 H3C S5800-32C Copyright (c) 2004-2012 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
3.2.1.2	WDTH-B3L2A-R1-IRF1-S5500-1	H3C Comware Platform Software, Software Version 5.20 Release 2215 H3C S5500-28C-EI-D Copyright (c) 2004-2012 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
3.2.2.1	WDTH-B3L2B-R1-S75-1	H3C Comware Platform Software, Software Version 5.20, Release 6616P01 H3C S7606-S Copyright (c) 2004-2010 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
4.1.1.1	WDTH-B4L1A-R1-S7606S-1	H3C Comware Platform Software, Software Version 5.20, Release 6616P01 H3C S7606-S Copyright (c) 2004-2010 Hangzhou H3C Tech. Co., Ltd. All rights reserved.

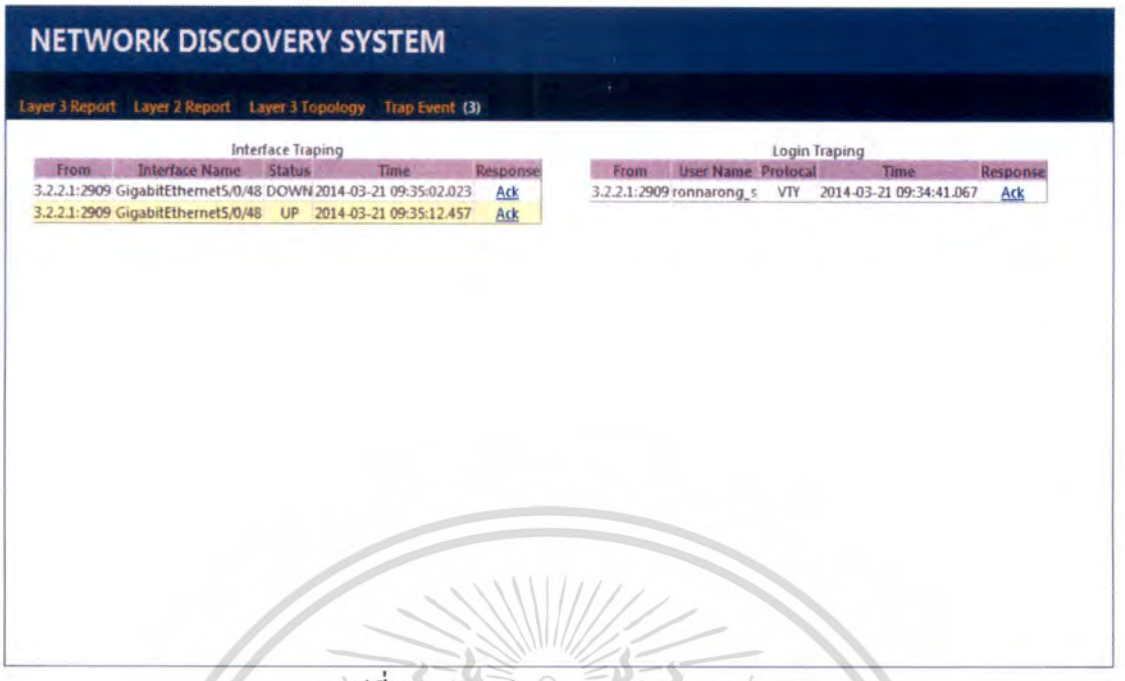
รูปที่ 4.10 ตัวอย่างข้อมูลข้อมูลที่ export ออกมาเป็น excel file



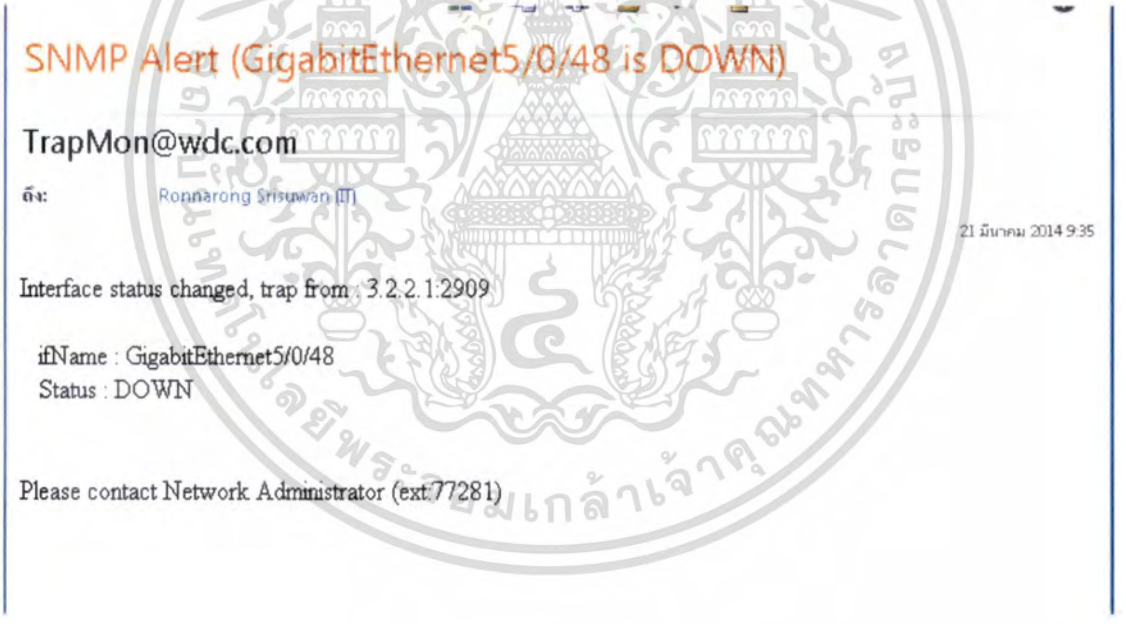
รูปที่ 4.11 รูปแบบการรับข้อความ Trap

โดยบนตัวอุปกรณ์เครือข่ายจะมีการคอนฟิกคำสั่งดังต่อไปนี้เพื่อเป็นการให้อุปกรณ์เครือข่ายสร้างข้อความ Trap และกำหนดเป้าหมายในการส่งข้อความ

```
snmp-agent target-host trap address udp-domain 172.17.25.132 params securityname test v2c

snmp-agent trap enable

snmp-agent trap source LoopBack1

snmp-agent trap queue-size 200

snmp-agent trap if-mib link extended
```



รูปที่ 4.12 ตัวอย่างการแสดง Trap event



รูปที่ 4.13 ตัวอย่างข้อความทางอีเมล

บทที่ 5
บทสรุป และข้อเสนอแนะ

5.1 สรุปผลของโครงงาน

ระบบบริหารเครือข่ายแบบค้นหาเริ่มต้นศึกษาทฤษฎีระบบบริหารจัดการเครือข่าย และโปรโตคอลที่ใช้ในการบริหารจัดการเครือข่ายต่างๆ แล้วนำความรู้มาวิเคราะห์และออกแบบระบบขึ้นตามที่ได้ออกแบบไว้โดยระบบการจัดการเครือข่ายแบบค้นหาที่พัฒนาขึ้นมีคุณสมบัติดังนี้

5.1.1 ระบบค้นหาอุปกรณ์เครือข่าย

5.1.2 การค้นหาเครือข่ายและอุปกรณ์เครือข่ายที่เชื่อมต่อ

5.1.3 ระบบสามารถทำการสืบค้นหาอุปกรณ์เครือข่ายที่เชื่อมต่อได้ โดยระบบใช้การทำงานร่วมกันของโปรโตคอล ICMP, ARP และโปรโตคอล SNMP เพื่อทดสอบสถานะของอุปกรณ์เครือข่าย และ เชื่อมต่ออุปกรณ์เพื่อดึงข้อมูลมาใช้ในซอฟต์แวร์ระบบ

5.1.4 ซอฟต์แวร์ระบบ

5.1.5 การวาดโทโพโลยีการเชื่อมต่อของอุปกรณ์เครือข่ายในระบบ

5.1.6 ซอฟต์แวร์ระบบจะนำข้อมูลของอุปกรณ์เครือข่ายที่ค้นหาได้มาแสดงเป็นแผนภาพการเชื่อมต่อ โดยจะแบ่งเป็นสองแผนภาพคือ แผนภาพการเชื่อต่อของอุปกรณ์เครือข่ายเลเยอร์ 3 ซึ่งเป็นโครงสร้างหลักของระบบเครือข่ายที่ทำการทดสอบ และ แผนภาพการเชื่อมต่อของอุปกรณ์เครือข่ายเลเยอร์ 2 ที่มีการเชื่อมต่ออยู่กับอุปกรณ์เครือข่ายเลเยอร์ 3 ตัวหนึ่งๆ

5.1.7 การสร้างลิสต์ของอุปกรณ์เครือข่าย

5.1.8 ซอฟต์แวร์ระบบสามารถแสดงรายการอุปกรณ์เครือข่ายทั้งหมด โดยจะแสดงข้อมูลตามที่ได้จัดเก็บไว้ในฐานข้อมูล และสามารถนำข้อมูลเหล่านี้ออกมาในรูปแบบ excel ได้เพื่อสามารถนำไปเป็นรายงานอุปกรณ์เครือข่ายได้

5.1.9 ตรวจจับข้อมูลที่มีการส่งผ่านบนอินเตอร์เฟส

5.1.10 ที่อินเตอร์เฟสบนอุปกรณ์เครือข่ายซอฟต์แวร์ระบบมีการดึงข้อมูลการรับส่งข้อความมาแสดงเป็นกราฟ เพื่อดูปริมาณการใช้งานบนอินเตอร์เฟสใดๆได้

5.2 ปัญหาและอุปสรรค

1. เนื่องจากระบบที่พัฒนาจำเป็นต้องหาระบบเครือข่ายที่มีการใช้งานอยู่จริง เพื่อให้สามารถทดสอบเชื่อมต่อและการเข้าถึงชุดข้อมูลของโปรโตคอลSNMP ของอุปกรณ์เครือข่าย ดังนั้นจึงเลือกใช้เครือข่ายของบริษัทที่มีการใช้งานอยู่ แต่เนื่องด้วยเป็นเครือข่ายที่มีการใช้งานอยู่ตลอดเวลาดังนั้นจะต้องมีความระมัดระวังในการทดสอบเป็นอย่างมากเพื่อป้องกันปัญหาระบบเครือข่ายล่มจากการทดลอง

2. อุปกรณ์เครือข่ายที่ใช้งานของระบบที่ทดสอบจะมีอุปกรณ์ที่จำกัด และไม่หลากหลาย ซึ่งหลังจากที่ทดลองและได้ข้อมูลมาจะพบว่าอุปกรณ์ที่ตรวจพบจะเป็นอุปกรณ์ยี่ห้อ Huawei และ H3C เท่านั้น เนื่องด้วยอุปกรณ์ที่ไม่หลากหลายทำให้ระบบไม่มีความหลากหลายเท่าที่ควร รวมไปถึงอุปกรณ์ที่ค้นหาได้จะมีแค่ อุปกรณ์เครือข่ายเลเยอร์ 2 และ เลเยอร์ 3

3. ชุดโครงสร้างข้อมูล MIB ของอุปกรณ์ ในแต่ละรุ่นวางในตำแหน่งที่ไม่แน่นอน และไม่มีการเผยแพร่อย่างกว้างขวางทำให้เสียเวลาในการสืบค้น

4. ในส่วนของการวาดแผนภาพต้องใช้เวลาในการศึกษาเพิ่มเติมเพื่อให้ได้แผนภาพที่มีความสวยงาม และเป็นระเบียบมากกว่านี้

5.3 ข้อเสนอแนะ และแนวทางในการพัฒนาในอนาคต

1. ศึกษาเพิ่มเติมของการทำงานของโปรโตคอล SNMP ระหว่างแมเนเจอร์และเอเจนต์ในการส่งคำสั่ง Trap เพื่อนำมาพัฒนาระบบแจ้งเตือนเมื่อมีความผิดปกติเกิดขึ้นกับอุปกรณ์เครือข่าย

2. สามารถประยุกต์ระบบค้นหาอุปกรณ์เครือข่ายให้สามารถรันเป็นช่วงเวลา หรือมีระบบคอยตรวจสอบอุปกรณ์เครือข่ายที่อาจจะมีการเชื่อมต่อเพิ่มเติม

3. สามารถที่จะให้ผู้ที่มีส่วนเกี่ยวข้องเข้ามาใช้งานระบบได้ด้วยการให้สิทธิ์ในการเข้าดูข้อมูลที่จำเป็น

บรรณานุกรม

"Mani Subramanian, Network Management Principles and Practice", Publish by Addison Wesley,2000

"Simple Network Management Protocol", [ออนไลน์]. เข้าถึงได้จาก :http://en.wikipedia.org/wiki/SNMP

"SNMP Trap Basic", [ออนไลน์]. เข้าถึงได้จาก :http://www.dpstele.com/dpsnews/techinfo/snmp/snmp_trap_basics.php

"The SNMP Protocol", [ออนไลน์].เข้าถึงได้จาก :http://www.snmp.com/protocol/index.shtml

"Topology Discovery in Heterogeneous IP Networks" ,Y. Breitbart, M. Garofalakis, C. Martin, R. Rastogi, S. Seshadri, and A. Silberschatz, in Proceedings of IEEE INFOCOM'2000,Tel Aviv,Israel, Mar. 2000.

"190 SNMP SMIv1 and v2 MIBs (50 SMIv1, 140 SMIv2) for Huawei", [ออนไลน์]. เข้าถึงได้จาก :http:// http://mibdepot.com/cgi-bin/mibvendors_multi.cgi?id=93313

ประวัติผู้เขียน

ชื่อ	นาย รณรงค์ ศรีสุวรรณ์
วัน เดือน ปี เกิด	7 กรกฎาคม 2523
ที่อยู่	เลขที่ 113 หมู่ที่ 11 ตำบลคลองเปียะ อำเภอจะนะ จังหวัดสงขลา 90130
ประวัติการศึกษา	วิศกรรมศาสตร์บัณฑิต สาขาเทควิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีมหานคร กรุงเทพมหานคร
	วิทยาศาสตรมหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง