โปรแกรมวิเคราะห์เครือข่ายอัตโนมัติ

AUTOMATIC NETWORK ANALYSIS PROGRAM

ชมภูนุช สันธนะผล
ชาญกฤษณ์ มากมี
ชาญวิทย์ พิณพาทย์

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปีการศึกษา 2553

ปริญญานิพนธ์ปีการศึกษา 2553

สาขาวิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง โปรแกรมวิเคราะห์เครือข่ายอัตโนมัติ

AUTOMATIC NETWORK ANALYSIS PROGRAM

ผู้จัดทำ

1. นางสาวชมภูนุช สันธนะผล รหัสนักศึกษา 50010310
2. นายชาญกฤษณ์ มากมี รหัสนักศึกษา 50010359
3. นายชาญวิทย์ พิณพาทย์ รหัสนักศึกษา 50010362

อาจารย์ที่ปรึกษา

(อาจารย์ธนัญชัย ตรีภาค)

โปรแกรมวิเคราะห์เครือข่ายอัตโนมัติ

นางสาวชมภูนุช สันธนะผล 50010310
นายชาญกฤษณ์ มากมี 50010359
นายชาญวิทย์ พิณพาทย์ 50010362
อาจารย์ธนัญชัย ตรีภาค อาจารย์ที่ปรึกษา
ปีการศึกษา 2553

บทคัดย่อ

โครงงานโปรแกรมวิเคราะห์เครือข่ายอัตโนมัติเป็นซอฟต์แวร์ ที่ใช้งานบนระบบปฏิบัติการลินุกซ์ โดยมีความสามารถของการวิเคราะห์หาสาเหตุของปัญหาที่เกิดขึ้นในระบบเครือข่าย โดยโปรแกรมจะทำงานแบบอัตโนมัติซึ่งสามารถหาสาเหตุของปัญหาที่เกิดขึ้นภายในระบบได้ภายในระยะเวลาอันสั้น

เพื่อให้การแก้ไขปัญหาของระบบเครือข่ายเป็นไปอย่างรวดเร็วและอัตโนมัติ ในโปรแกรมจึงประกอบด้วย 3 องค์ประกอบหลัก ส่วนแรกคือการกำหนดโครงสร้างของระบบเครือข่าย เป็นส่วนที่ใช้ระบุตำแหน่งการเชื่อมต่อของระบบเครือข่าย ส่วนที่สองคือการตรวจตราข้อมูลในระบบเครือข่าย เป็นการนำข้อมูลที่ได้มาแสดงในรูปแบบต่างๆที่เข้าใจได้ง่าย และส่วนสุดท้ายคือการวิเคราะห์ระบบเครือข่าย ซึ่งวิเคราะห์และแก้ปัญหาสิ่งผิดปกติที่เกิดขึ้นในระบบเครือข่ายและจากแจ้งผลวิเคราะห์ให้ผู้ดูแลระบบทราบ เพื่อที่จะได้แก้ไขได้ทันท่วงที

ในการจัดทำโปรแกรมวิเคราะห์เครือข่ายอัตโนมัตินั้น ทางผู้จัดทำได้ยึดหลักการการออกแบบที่ใช้งานได้ง่ายและใช้เทคโนโลยีที่เป็นมาตรฐานในปัจจุบัน ทำให้สามารถนำไปประยุกต์ใช้ได้กับระบบทั่วไป อีกทั้งยังสามารถแก้ไขเปลี่ยนแปลงอัลกอริธึ่มของโปรแกรม เพื่อให้มีประสิทธิภาพสูงสุดสำหรับระบบเครือข่ายในองค์กรนั้นๆได้

Automatic Network Analysis Program

Ms. Chompunoot	Santanapol	50010310
Mr. Charngrid	Magmi	50010359
Mr. Chanwit	Pinpart	50010362
Mr. Thanunchai	Threepak	Advisor

Academic Year 2010

ABSTRACT

Automatic Network Analysis Program project is software that used on Linux operating system with the capability of analyzing the cause of problem that occurs on network. Program automatically analyze network's problem which can cause problems in the system within a short time.

To solve the problem of the network is fast and automatic. It consists of three main program components. The first part is to determine the structure of the network that used to locate the network connection. The second part is the monitoring information in the network. It is obtained in various ways to show about network status at that time by simple interface. And the last part is analyzing the network. It analyzes and problem solving that happens in the network and inform the analysis of problem to administrator to know and resolved promptly.

The organizers use the principle of design and current standard technology to make this project easy to use. Application can be made available to the general system. Administrator can also change program algorithm for maximum performance in corporate networks they have.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้ได้รับคำแนะนำ และคำปรึกษาเกี่ยวกับการวิจัยและการค้นคว้าจาก อาจารย์ธนัญชัย ตรีภาค อาจารย์ที่ปรึกษาในการจัดทำปริญญานิพนธ์ กลุ่มผู้วิจัยรู้สึกซาบซึ้งเป็นอย่างยิ่งในความอนุเคราะห์จากอาจารย์เป็นอย่างสูง อีกทั้งอาจารย์อัครเดช วัชระภูพงษ์ ที่คอยช่วยตอบคำถามต่างๆ นายอุดม จิระดำเกิง รุ่นพี่ภาควิชา ที่ให้คำแนะนำในการเขียนโปรแกรม รวมไปถึงห้องวิจัยเครือข่ายสาขาวิศวกรรมคอมพิวเตอร์ ที่ได้สนับสนุนในส่วนของอุปกรณ์เครื่องมือประกอบการทำวิจัยตลอดจนข้อมูลที่สามารถค้นคว้าได้ภายในห้องวิจัยที่เอื้อประโยชน์แก่การวิจัยในครั้งนี้ด้วย

อย่างไรก็ตามกลุ่มผู้วิจัยหวังเป็นอย่างยิ่งว่ารายงานของข้าพเจ้าจะเป็นประโยชน์ต่อทุกท่านและให้คำแนะนำแก่นักศึกษารุ่นต่อไปในอนาคตข้างหน้า

ชมภูนุช สันธนะผล
ชาญกฤษณ์ มากมี
ชาญวิทย์ พิณพาทย์

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตาราง หน้า

สารบัญรูป

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

บทที่ 1
บทนำ

1.1 ความเป็นมา

ในปัจจุบันมีการใช้งานเครือข่ายอินเตอร์เน็ตในชีวิตประจำวันมากขึ้นองค์กรต่างๆในทุกๆภาคส่วนต่างก็มีเครือข่ายของตนเองและเชื่อมต่อเข้าสู่อินเตอร์เน็ตสิ่งที่ตามมาก็คือการจัดการเครือข่ายให้ทำงานได้อย่างมีประสิทธิภาพในทรัพยากรที่มีอยู่ของแต่ละระบบซึ่งเกิดปัญหาบ่อยครั้งในหน่วยงานต่างๆเพราะส่วนใหญ่จะขาดบุคลากรที่ความรู้ความสามารถในการจัดการเครือข่ายให้สามารถทำงานต่อไปได้อย่างเป็นปกติโปรแกรมวิเคราะห์เครือข่ายอัตโนมัติจึงมีบทบาทสำคัญและเป็นสิ่งจำเป็นสำหรับระบบเครือข่ายในองค์กรต่างๆ โครงการนี้มีจุดประสงค์ในการพัฒนาโปรแกรมวิเคราะห์เครือข่ายอัตโนมัติที่จะเป็นเครื่องมือที่ช่วยให้ผู้ดูแลระบบสามารถตรวจสอบความผิดปกติที่เกิดหรืออาจจะกำลังเกิดได้ง่ายขึ้น เพิ่มประสิทธิภาพในการทำงานของระบบมากขึ้น ลดโอกาสที่จะเกิดปัญหาในระบบ เหมาะสำหรับผู้ดูแลระบบทั้งมือใหม่และที่มีประสบการณ์แล้ว อีกทั้งยังสามารถคอยเตือนเกี่ยวกับความผิดปกติที่เกิดขึ้นในระบบได้อีกด้วย

1.2 ความมุ่งหมายและวัตถุประสงค์

1) เพื่อพัฒนาระบบวิเคราะห์เครือข่ายอัตโนมัติที่มีประสิทธิภาพ สำหรับองค์กรทั่วไป โดยเฉพาะองค์กรของรัฐที่ขาดเงินทุนและบุคลากร
2) เพื่อเป็นผู้ช่วยให้กับผู้ดูแลระบบในการวิเคราะห์ระบบเครือข่าย
3) เพื่อตอบโจทย์ความต้องการขององค์กรต่างๆที่ต้องการการตรวจสอบข้อผิดพลาดและปัญหาอย่างทันท่วงทีซึ่งเป็นการลดภาระของผู้ดูแลระบบ
4) เพื่อลดค่าใช้จ่ายในการจัดซื้อระบบอื่นๆที่ทำหน้าที่คล้ายคลึงกันจากต่างประเทศซึ่งมีราคาแพง
5) เพื่อนำไปประยุกต์ใช้กับงานด้านอื่นๆ ทั้งในด้านการศึกษาและเชิงพาณิชย์

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1) เป็นการพัฒนาเทคโนโลยีในการตรวจสอบและวิเคราะห์เครือข่ายให้มีประสิทธิภาพมากขึ้น ลดปัญหาที่จะเกิดขึ้นซึ่งปัญหาเหล่านั้นอาจจะส่งผลกระทบต่อระบบได้ และยังพัฒนาบนพื้นฐานของฟรีแวร์และโอเพนซอร์ส ทำให้ผู้ที่สนใจสามารถนำโปรแกรมไปพัฒนาต่อได้โดยไม่ต้องเสียค่าลิขสิทธิ์
2) ผู้ดูแลระบบสามารถตรวจหาปัญหาที่เกิดขึ้นได้รวดเร็วขึ้นและทำให้การดูแลระบบเป็นไปได้โดยง่ายขึ้น

1.4 ขอบเขตของโครงงาน

โครงงานนี้ ได้มุ่งเน้นในเรื่องของการศึกษาการตรวจสอบสิ่งผิดปกติในระบบเครือข่าย ซึ่งในการออกแบบโปรแกรมวิเคราะห์เครือข่ายอัตโนมัติแบ่งออกได้เป็น 4 ส่วนดังต่อไปนี้

1) ส่วนของการตรวจตราดูปริมาณการใช้งานระบบเครือข่าย
2) ส่วนของการวิเคราะห์ปัญหาที่เกิดขึ้นในระบบเครือข่าย
3) ส่วนของโครงสร้างระบบเครือข่ายและการเก็บข้อมูล
4) ส่วนของการติดต่อผู้ใช้

ซึ่งเมื่อโปรแกรมเสร็จสมบูรณ์ จะสามารถทำงานได้อย่างมีประสิทธิภาพในการตรวจสอบปัญหาที่อาจจะเกิดขึ้นในเครือข่ายได้อย่างทันท่วงที และสามารถแจ้งให้ผู้ใช้ได้ทราบก่อนที่จะเกิดความเสียหายไปมากขึ้น

1.5 ขั้นตอนการดำเนินงาน

1) ศึกษาหาความรู้ขั้นพื้นฐาน และรูปแบบของโปรแกรมที่เกี่ยวข้อง เพื่อนำมาใช้พัฒนาโปรแกรม
2) นำความรู้ที่ได้ทำการค้นคว้า มาทำการออกแบบส่วนต่างๆของโปรแกรม เช่นโมเดลการวิเคราะห์ระบบ เป็นต้น
3) เขียนโปรแกรมตามที่ได้ออกแบบไว้ เพื่อนำข้อมูลจริงในระบบเครือข่ายมาทดสอบ
4) สรุปผลการศึกษาและการทดลองต่างๆพร้อมจัดทำเอกสารโครงงาน

1.6 ส่วนประกอบของปริญญานิพนธ์

ปริญญานิพนธ์ฉบับนี้แบ่งออกเป็นบททั้งหมด 6 บทดังต่อไปนี้

บทที่ 1 จะกล่าวถึง ความเป็นมา, ความมุ่งหมายและวัตถุประสงค์, ประโยชน์ที่คาดว่าจะได้รับ, ขอบเขตของโครงงาน, ขั้นตอนการดำเนินงาน, ส่วนประกอบของปริญญานิพนธ์

บทที่ 2 จะกล่าวถึงทฤษฎีและรายละเอียดของโปรโตคอลทีซีพี/ไอพี

บทที่ 3 จะกล่าวถึงทฤษฎีและรายละเอียดของโปรโตคอลเอสเอ็นเอ็มพี

บทที่ 4 จะกล่าวถึงวัตถุประสงค์ของโปรแกรม รายละเอียดการพัฒนาโปรแกรม โครงสร้างของระบบ, การออกแบบและผังงานการทำงานของโปรแกรม

บทที่ 5 จะกล่าวถึงการทดสอบโปรแกรมโดยเริ่มตั้งแต่การตั้งค่าต่างๆของโปรแกรมและทำการทดสอบกับระบบ พร้อมแสดงผลลัพธ์ที่ได้จากการพัฒนาโปรแกรม

บทที่ 6 จะกล่าวถึง บทสรุปของการพัฒนาโปรแกรม ปัญหา อุปสรรค และแนวทางการแก้ไข รวมทั้งแนวทางในการพัฒนาต่อ

บทที่ 2
โปรโตคอลทีซีพี/ไอพี

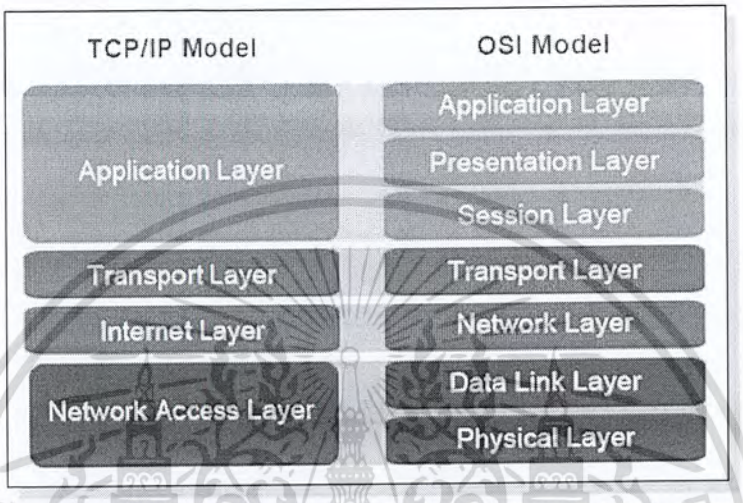
2.1 ความเป็นมาของโปรโตคอลทีซีพี/ไอพี

ทีซีพี/ไอพีเป็นมาตรฐานของการรับส่งข้อมูลระหว่างคอมพิวเตอร์ สองระบบที่มีจุดเริ่มต้นราว 30 ปีมาแล้ว เมื่อกระทรวงกลาโหมสหรัฐฯ หรือ Department Of Defense (DOD) ทำโครงการทดลองในปี ค.ศ. 1969 เชื่อมโยงคอมพิวเตอร์ทางทหารของแต่ละหน่วย ซึ่งเป็นคอมพิวเตอร์ต่างชนิดกันให้สามารถติดต่อรับส่งข้อมูลกันได้ (File Transfer) และสามารถใช้บริการอื่นๆ เช่น Remote Login รวมถึงการรับส่งจดหมาย อิเล็กทรอนิค (E-mail) ด้วย จุดประสงค์ของโครงการนี้คือสร้างระบบเครือข่ายคอมพิวเตอร์ให้สามารถส่งข้อมูลกันได้ แม้ว่าสายส่งข้อมูลบางส่วนหรือคอมพิวเตอร์บางเครื่องในเครือข่ายจะถูกทำลายเสียหายไปก็ตาม ซึ่งเป็นคุณสมบัติที่สำคัญยิ่งยามสงคราม

ในขณะนั้นกองทัพบกเลือกใช้คอมพิวเตอร์และระบบเครือข่ายของ Digital Equipment Corporation (DEC) กองทัพเรือเลือกใช้คอมพิวเตอร์ของ Unisys ส่วนกองทัพอากาศเลือกใช้คอมพิวเตอร์ของ IBM เมื่อจะทำการรบกระทรวงกลาโหมสหรัฐฯก็พบว่าคอมพิวเตอร์ของทั้ง 3 กองทัพสื่อสารข้ามระบบกันไม่ได้ จึงได้ให้ทุนในการทำโครงการเชื่อมต่อคอมพิวเตอร์ของทั้ง 3 กองทัพเข้าด้วยกันเป็นระบบเครือข่าย โดยมีคุณสมบัติพิเศษแตกต่างจากระบบเครือข่ายที่ใช้งานกันทั่วๆไปคือ การรับส่งข้อมูลจะแบ่งข้อมูลออกเป็นส่วนย่อยๆเรียกว่า “แพคเก็ต” (packet) ข้อมูลแต่ละส่วนนี้จะถูกส่งไปให้คอมพิวเตอร์ผู้รับปลายทางผ่านสายส่งข้อมูล โดยแต่ละส่วนอาจใช้เส้นทางสำหรับส่งข้อมูลคนละทางก็ได้ คอมพิวเตอร์ปลายทางจะนำข้อมูลที่ได้รับมาต่อรวมกันตามลำดับจนครบ หากเส้นทางที่ส่งข้อมูลเสียหายหรือเครื่องคอมพิวเตอร์บางส่วนในเครือข่ายเสียหายข้อมูลก็จะถูกส่งไปใหม่โดยใช้เส้นทางอื่นแทนโดยอัตโนมัติ โครงการนี้มีชื่อว่า Advance Research Projects Agency Network หรือที่รู้จักกันดีในชื่อ ARPANET ซึ่งประสบความสำเร็จอย่างสูงจนใช้งานกันอย่างจริงจังในปี ค.ศ.1975

ซอฟต์แวร์ที่ใช้ควบคุมการรับส่งข้อมูลของ ARPANET ประกอบด้วยส่วนหลักๆ 2 ส่วนคือ Transmission Control Protocol หรือทีซีพี และ Internet Protocol หรือไอพี ซึ่งทีซีพีมีหน้าที่ตรวจสอบการรับส่งข้อมูลระหว่างคอมพิวเตอร์ผู้รับและผู้ส่ง ให้ได้รับข้อมูลถูกต้องครบถ้วน หากข้อมูลสูญหายก็จะแจ้งให้ต้นทางส่งข้อมูลมาใหม่ ส่วนไอพีจะมีหน้าที่เลือกเส้นทางที่ใช้รับส่งข้อมูลผ่านระบบเครือข่าย และตรวจสอบที่แอดเดรสของผู้รับ โดยใช้ข้อมูลขนาด 4 ไบต์หรือ 32 บิตเป็นตัวกำหนดแอดเดรส ต่อมาในปี ค.ศ. 1983 ทีซีพี/ไอพีถูกกำหนดให้เป็นมาตรฐานการรับส่งข้อมูลของกระทรวงกลาโหมสหรัฐฯ เราจึงถือว่าทีซีพี/ไอพีมีต้นกำเนิดมาจากโครงการ ARPANET และ

ได้ถูกรวมเป็นส่วนหนึ่งของระบบปฏิบัติการยูนิกซ์ โดย Bolt, Beranek และ Newman ซึ่งได้รับทุนสนับสนุนจากกระทรวงกลาโหมสหรัฐฯอีกเช่นเดียวกัน ทำให้ทีซีพี/ไอพีก็ยิ่งมีบทบาทในการสื่อสารมากขึ้นเรื่อยๆ จนกระทั่งกลายเป็นอินเตอร์เน็ตในปัจจุบันโดยมี ARPANET เป็นแกนกลาง และได้มีการกำหนดมาตรฐานที่ใช้ในการรับส่งข้อมูลเครือข่ายอื่นๆเพิ่มเติมขึ้นมาในภายหลัง รวมทั้งโอเอสไอโมเดลในเวลาต่อมา



รูป 2.1 การเปรียบเทียบเลเยอร์ของทีซีพี/ไอพีกับเลเยอร์ของโอเอสไอ

2.2 หน้าที่แต่ละเลเยอร์ของโปรโตคอลทีซีพี/ไอพี

2.2.1 ชั้นแอพพลิเคชั่น (Application Layer)

ชั้นนี้รองรับการทำงานของแอพพลิเคชันต่างๆที่ทำงานเป็นโปรเซสอยู่ในเครื่องต้นทางและปลายทาง โดยจัดการเชื่อมต่อระหว่างโปรเซส หรือแอพพลิเคชันที่อยู่ต่างเครื่องกัน โดยการทำงานของแอพพลิเคชันต่างๆมีการติดต่อกันตามแต่ละโปรโตคอลเฉพาะแล้วแต่แอพพลิเคชันที่ใช้งาน ซึ่งจะขอบริการจากชั้นทรานสปอร์ตอีกทีหนึ่ง

2.2.2 ชั้นทรานสปอร์ต (Transport Layer)

มีการสร้างการเชื่อมต่อกันระหว่างแอพพลิเคชันแบบ end-to-end โดยจุดที่เชื่อมต่อกันเพื่อรับส่งข้อมูลนี้เรียกว่า พอร์ต (Port) หรือ ซ็อกเก็ต (Socket) ในชั้นนี้มีการบริการหลักอยู่ 2 แบบ คือ Connection Oriented โดยเรียกผ่านโปรโตคอลทีซีพี (TCP: Transmission Control Protocol) และ Connectionless ซึ่งเรียกผ่านโปรโตคอลยูดีพี (UDP: User Datagram Protocol) ซึ่งจะกล่าวถึงในหัวข้อถัดไป

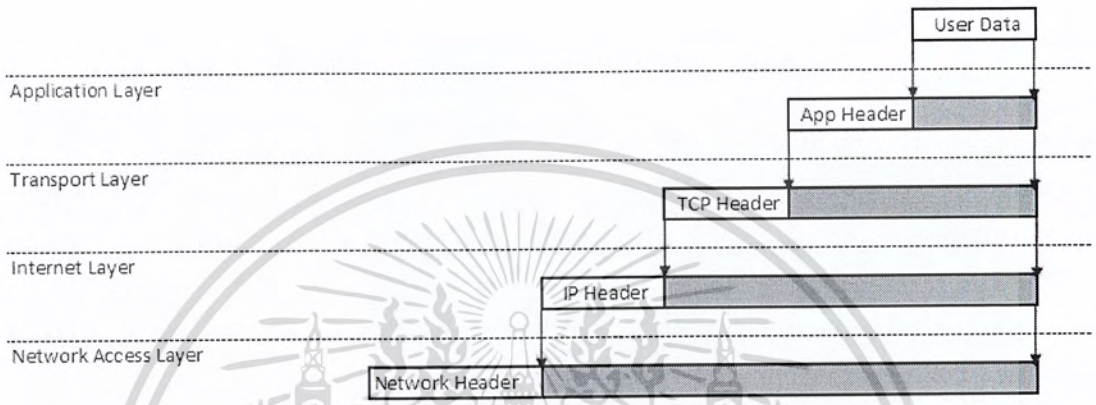
2.2.3 ชั้นอินเทอร์เน็ต (Internet Layer)

ชั้นนี้มีหน้าที่ส่งข้อมูลระหว่างเครือข่าย โดยมีโปรโตคอลที่ทำงานเป็นกลไกสำคัญในการส่งผ่านข้อมูลไปยังเครือข่ายใดๆในอินเทอร์เน็ตคือ ไอพี (IP) ซึ่งกล่าวถึงในหัวข้อถัดไป

นอกจากนี้ในชั้นนี้ยังมีโปรโตคอลทำงานอยู่ด้วยอีก 2 ชนิดคือ ไอซีเอ็มพี (ICMP) และ เออาร์พี (ARP)

2.2.4 ชั้นเน็ตเวิร์กแอคเซส (Network Access Layer)

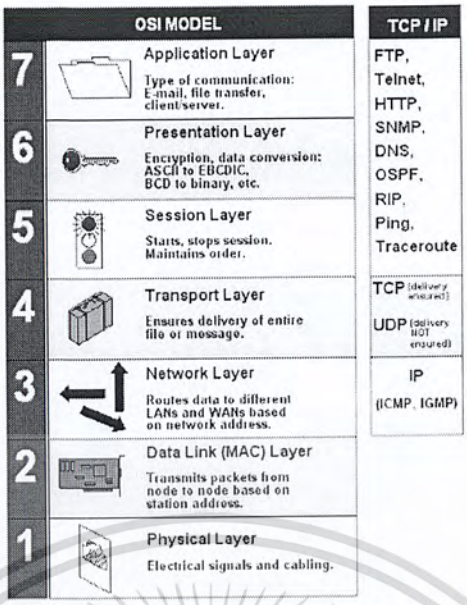
ทำหน้าที่ในการแปลงข้อมูลให้อยู่ในรูปแบบที่เหมาะสมกับเครือข่ายแต่ละแบบซึ่งแตกต่างกันออกไป และแปลงเป็นสัญญาณไฟฟ้าส่งไปยังเครือข่าย



รูป 2.2 การห่อหุ้มข้อมูลตามลำดับ

2.3 สถาปัตยกรรมโปรโตคอลทีซีพี/ไอพี

การทำงานตามโปรแกรมประยุกต์หนึ่งๆ ไม่ได้ใช้โปรโตคอลพร้อมกันทั้งชุด หากแต่ใช้เพียงโปรโตคอลที่สัมพันธ์กันไปในแต่ละระดับชั้นของแบบอ้างอิง ตัวอย่างเช่น การใช้งานเทลเน็ต (Telnet) ที่จะอาศัยทีซีพี/ไอพี ตามลำดับการซ้อนทับของโปรโตคอลจากระดับชั้นบนไปชั้นล่าง เรียกว่า โปรโตคอลแสตก (Protocol Stack) แสดงดังรูป 2.3



รูป 2.3 โปรโตคอลสแตก (Protocol Stack)

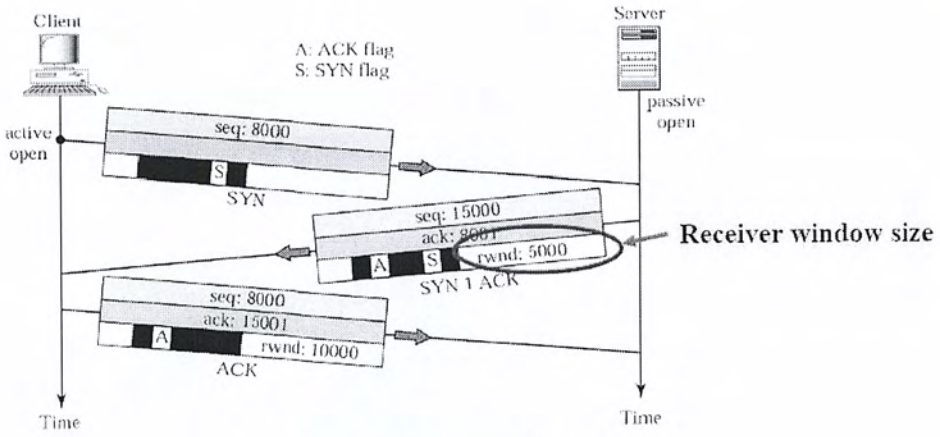
ไอพีซึ่งอยู่ในระดับชั้นเน็ตเวิร์กตามรูป 2.3 เป็นแกนสำคัญของโปรโตคอลแสตก เนื่องจากทั้งทีซีพี (TCP) และ ยูดีพี (UDP) ต้องใช้ไอพีเลือกเส้นทางส่งแพคเก็ต ในระดับชั้นเน็ตเวิร์กยังมีไอซีเอ็มพี (ICMP) สนับสนุนการทำงานของไอพี เพื่อรายงานข้อผิดปกติที่เกิดขึ้น เนื่องจากการส่งแพคเก็ต และมีไอจีเอ็มพี (IGMP) ดูแลการจัดกลุ่มโฮสต์ในเครือข่ายมัลติคาสต์

ระดับชั้นทรานสปอร์ตมี 2 โปรโตคอลสำคัญคือ ทีซีพีและยูดีพี แอพพลิเคชันจะเลือกใช้ทีซีพีหรือยูดีพีตามลักษณะงาน

โปรโตคอลระดับล่างถัดจากไอพีได้แก่ โปรโตคอลระดับเดทาลิงค์ ซึ่งกำหนดการทำงานตามเทคโนโลยีเครือข่ายที่ใช้งาน เช่น โปรโตคอลระดับเดทาลิงค์ ซึ่งกำหนดการทำงานตามมาตราฐานอีเทอร์เน็ต ในระดับชั้นนี้มีโปรโตคอลในชุดของทีซีพี/ไอพีทำหน้าที่สนับสนุนการทำงานอยู่สองโปรโตคอลคือ เออาร์พีและอาร์เออาร์พี ทั้งสองโปรโตคอลจะทำหน้าที่แปลงค่าระหว่างไอพีแอดเดรสกับฮาร์ดแวร์แอดเดรส

2.4 โปรโตคอลทีซีพี (TCP: Transmission Control Protocol)

การทำงานที่สำคัญอย่างหนึ่งของโปรโตคอลทีซีพีคือการทำ “3-way Handshake” ซึ่งเป็นกระบวนการเริ่มต้นหาการสร้างการเชื่อมต่อในชั้นทรานสปอร์ต กล่าวคือในการติดต่อกันระหว่างระบบในเครือข่ายต้องมีการสร้างการเชื่อมต่อไปยังระบบที่ให้บริการก่อน โดยผู้ขอบริการส่งสัญญาณ SYN เพื่อขอบริการ จากนั้นผู้ให้บริการจะส่งสัญญาณ ACK เพื่อตอบรับการเชื่อมต่อที่ร้องขอมาจึงสามารถรับส่งข้อมูลได้ ดังรูป 2.4



รูป 2.4 การทำ 3-way Handshake

การเชื่อมต่อแบบ 3-way Handshake นี้เป็นการตรวจสอบความพร้อมของทั้งฝ่ายส่งและฝ่ายรับ และเป็นการกำหนดค่าเริ่มต้นของพารามิเตอร์ต่างๆของทั้งสองฝ่ายให้ตรงกัน หลังจากกระบวนการทำ 3-way Handshake สิ้นสุด ทั้งสองฝ่ายจึงสามารถรับและส่งข้อมูลซึ่งกันและกันได้

ดังนั้นโปรโตคอลทีซีพีจึงเป็นโปรโตคอลที่มีการรับส่งข้อมูลแบบ “Connection Oriented” ทำให้การทำงานของทีซีพีมีความน่าเชื่อถือมากขึ้น หน้าที่การทำงานของทีซีพีในการรับส่งข้อมูลมีหน้าที่หลัก 6 ข้อคือ

1) ควบคุมการรับส่งข้อมูล (Basic Data Transfer)

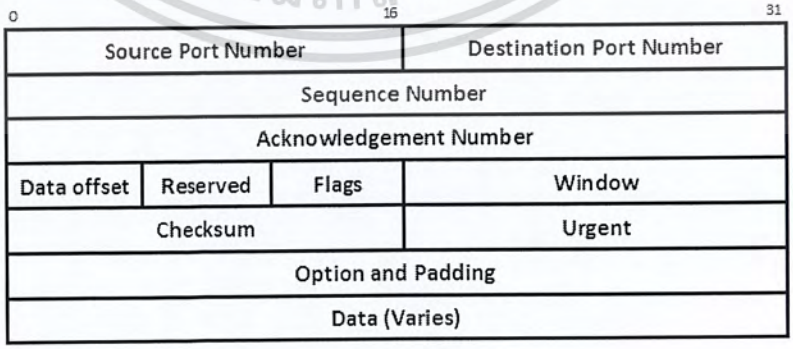
2) ความน่าเชื่อถือในการรับส่งข้อมูล (Reliability)

3) ควบคุมการไหลของข้อมูล (Flow Control)

4) การทำมัลติเพล็ก (Multiplex)

5) ควบคุมการเชื่อมต่อ (Connection Control)

6) ความปลอดภัยในการรับส่งข้อมูล (Security)



รูป 2.5 ทีซีพีเดทาแกรม

คำอธิบายรูป 2.5 ทีซีพีเดทาแกรม

Source Port Number ขนาด 16 บิต: เป็นหมายเลขพอร์ตของบริการที่เครื่องต้นทาง

Destination Port Number ขนาด 16 บิต: เป็นหมายเลขพอร์ตของบริการที่เครื่องปลายทาง

Sequence Number ขนาด 32 บิต: เป็นหมายเลขที่บอกลำดับของการรับส่งข้อมูลของเครื่องที่ต้องการของส่งข้อมูล

Acknowledgement Number ขนาด 32 บิต: เป็นหมายเลขที่บอกลำดับของการรับส่งข้อมูลที่ฝั่งรับข้อมูล ปกติค่าของ Acknowledgement Number จะมีค่าเท่ากับ Sequence Number (ของอีกฝั่ง) + 1 เสมอ

Data offset ขนาด 4 บิต: เป็นตัวบอกค่าออฟเซตของข้อมูล เพราะทีซีพีนั้นไม่มีการกำหนดความยาวที่แน่นอนของข้อมูล จึงต้องมีออฟเซตเป็นตัวบอก

Flag ประกอบด้วย 6 ฟิลด์ย่อย แต่ละฟิลด์ย่อยมีขนาด 1 บิต ได้แก่

Urgent ถ้าบิตนี้เป็น “1” หมายความว่า Urgent pointer บรรจุตำแหน่งข้อมูลที่ต้องรีบดำเนินการเร่งด่วนก่อน

Acknowledgement ถ้าบิตนี้เป็น “1” หมายถึงเป็นเซกเมนต์ตอบรับ โดยตอบอ้างอิงเลขลำดับตามที่กำหนดในฟิลด์ Acknowledgement number

Push ถ้าบิตนี้เป็น “1” หมายถึงทันทีที่สถานีปลายทางได้รับเซกเมนต์ ต้องรีบส่งข้อมูลไปยังโปรโตคอลประยุกต์ทันทีโดยไม่ต้องให้บัฟเฟอร์เต็ม

Reset ถ้าบิตนี้เป็น “1” หมายถึงให้ยกเลิกการเชื่อมต่อนี้ เนื่องจากอาจมีความผิดปกติเกิดขึ้นระหว่างคู่สถานีที่กำลังติดต่อกันอยู่ หากจำเป็นต้องส่งข้อมูลระหว่างกันอีกก็ต้องเริ่มการเชื่อมต่อใหม่

Synchronize ถ้าบิตนี้เป็น “1” หมายถึงขอเริ่มต้นการเชื่อมต่อและเมื่อการเชื่อมต่อเสร็จสิ้นบิตนี้จะถูกกำหนดให้เป็น “0” หลังจากนั้นจึงสามารถส่งผ่านข้อมูลระหว่างกันได้

Finish ถ้าบิตนี้เป็น “1” หมายถึงขอจบการเชื่อมต่อ

Window ขนาด 16 บิต: สถานีปลายทางใช้ฟิลด์นี้แจ้งขนาดบัฟเฟอร์ที่มีอยู่ (หน่วยเป็นไบต์) สถานีที่ติดต่อด้วยตัวเองไม่ต้องส่งข้อมูลเกินค่านี้

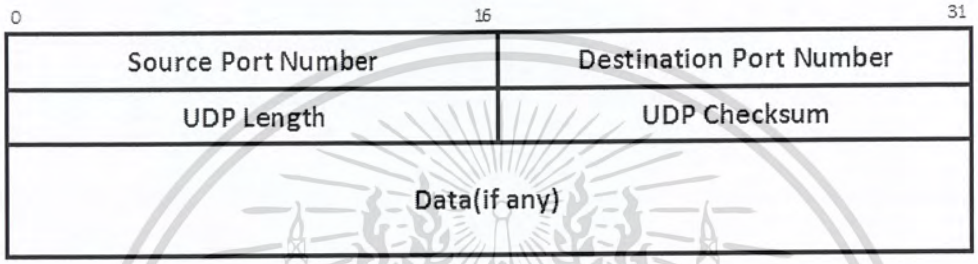
Checksum ขนาด 16 บิต: ผลรวมตรวจสอบความถูกต้องของเซกเมนต์ โดยคำนวณทั้งเฮดเดอร์และข้อมูล

Urgent ขนาด 16 บิต: พอยเตอร์ชี้ตำแหน่งไบต์ข้อมูลที่ต้องดำเนินการเร่งด่วนที่ต้องการให้โปรแกรมประยุกต์ดำเนินการทันที ค่าที่บรรจุในฟิลด์นี้จะมีความหมายก็ต่อเมื่อแฟล็ก UGR ถูกเซตเป็น “1”

Options and Padding ขนาดแปรเปลี่ยนได้ ใช้กำหนดงานเพิ่มเติมให้กับทีซีพีจะมีหรือไม่มีก็ได้ หากฟิลด์ Offset มีค่าเป็น 5 แสดงว่ามีเฮดเดอร์ขนาด 20 ไบต์ ซึ่งหมายถึงไม่ใช่ออพชัน ส่วน Padding ขนาด 0 – 24 ใช้เป็นส่วนที่ทำให้ขนาดของออพชันเป็นจำนวนเท่าของ 32 บิต

2.5 โปรโตคอลยูดีพี (UDP: User Datagram Protocol)

โปรโตคอลยูดีพีเป็นโปรโตคอลในการติดต่อสื่อสารในชั้นทรานสปอร์ต (Transport Layer) การทำงานคล้ายกับทีซีพีมากคือ จัดการเกี่ยวกับการสื่อสารระหว่างเครื่อง แต่เป็นแบบ Connectionless คือ ทั้งฝ่ายส่งและฝ่ายรับไม่จำเป็นต้องอาศัยการสร้างช่องทางเชื่อมต่อกันโดยไม่ต้องมีการแจ้งให้ฝ่ายรับข้อมูลเตรียมรับข้อมูลเหมือนโปรโตคอลทีซีพี และไม่มีการส่งสัญญาณตรวจสอบว่าข้อมูลถึงปลายทางอย่างถูกต้องครบถ้วนสมบูรณ์ ในการส่งข้อมูลแต่ละครั้งจึงไม่มีการส่งข้อมูลใหม่อีกรอบในกรณีที่เกิดความผิดพลาดของการส่งข้อมูล



รูป 2.6 ยูดีพีเดทาแกรม

Source Port Number ขนาด 16 บิต: บอกพอร์ตของเครื่องต้นทาง

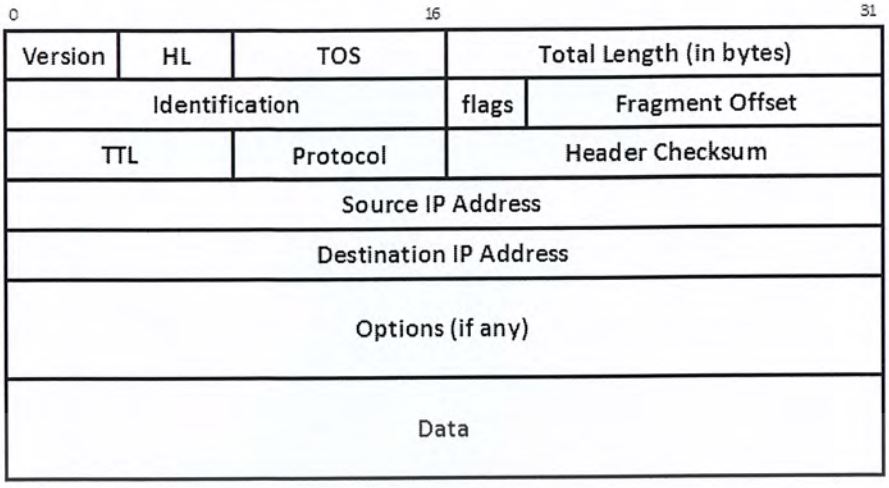
Destination Port Number ขนาด 16 บิต: บอกพอร์ตของเครื่องปลายทาง

Length ขนาด 16 บิต: บอกความยาวของเดทาแกรม (ทั้งเฮดเดอร์และข้อมูล) เป็นจำนวนไบต์

Checksum ขนาด 16 บิต: ผลรวมตรวจสอบ คำนวณจากผลรวมของเฮดเดอร์และข้อมูล

2.6 โปรโตคอลไอพี (IP: Internet Protocol)

โปรโตคอลไอพีเป็นโปรโตคอลที่จัดการเกี่ยวกับแอดเดรสของแต่ละแพคเก็ต เพื่อให้ส่งแพคเก็ตต่างๆไปยังเป้าหมายได้อย่างถูกต้อง การทำงานของไอพีเป็นเพียงการส่งข้อมูลไปยังเครื่องเป้าหมายเท่านั้นไม่มีการส่งสัญญาณขอบริการ หรือสัญญาณให้บริการระหว่างกันเหมือนทีซีพี เรียกว่าการเชื่อมต่อแบบ Connectionless ซึ่งระบบทั้งสองตั้งสมมติฐานว่าการเชื่อมต่อระหว่างกันไม่มีความผิดพลาดเกิดขึ้น



รูป 2.7 ไอพีเดทาแกรม

คำอธิบายรูป 2.7 ไอพีเดทาแกรม

Version ขนาด 4 บิต: แสดงรุ่นของโปรโตคอล

Header Length ขนาด 4 บิต: บอกความยาวเฉพาะเฮดเดอร์ของเดทาแกรม โดยนับจาก Version จนถึงไบต์สุดท้ายก่อนจะถึงข้อมูล

Type Of Service (TOS) ขนาด 8 บิต: ฟิลด์นี้ใช้กำหนดรูปแบบการให้บริการตามลักษณะโปรโตคอลแอพพลิเคชัน

Total Length มีขนาด 16 บิต: บอกถึงความยาวทั้งหมดของเดทาแกรม

Identification ขนาด 16 บิต: ใช้ในกรณีที่มีการแบ่งเดทาแกรมออกเป็นแฟรกเมนต์เมื่อนำกลับมารวมกันใหม่จะได้รู้ว่ามาจากเดทาแกรมเดียวกัน

Flags ขนาด 3บิต: ใช้ในกรณีที่มีการแบ่งข้อมูลออกเป็นแฟรกเมนต์

Time To Live (TTL) ขนาด 8 บิต: ฟิลด์นี้ใช้ในการกำหนดจำนวนเราเตอร์ที่เดทาแกรมจะเดินทางผ่านไปได้ อีกนัยหนึ่งคือ กำหนดอายุของเดทาแกรมซึ่งมีค่าสูงสุดตามขนาดฟิลด์คือ 255

Protocol ขนาด 8 บิต: ฟิลด์บอกชนิดของโปรโตคอลในระดับบนที่เอ็นแคปซูเลตในเดทาแกรมเพื่อให้สถานีปลายทางสามารถส่งข้อมูลไปยังโปรโตคอลระดับบนได้อย่างถูกต้อง

Header Checksum ขนาด 16 บิต: ใช้สำหรับตรวจสอบความผิดพลาดของเฮดเดอร์ โดยไม่รวมส่วนของข้อมูล

Source IP Address ขนาด 32 บิต: กำหนดไอพีแอดเดรสต้นทาง

Destination IP Address ขนาด 32 บิต: กำหนดไอพีแอดเดรสปลายทาง

Option ขนาดไม่คงที่: ใช้สำหรับกำหนดข่าวสารเพิ่มเติมสำหรับเดทาแกรม ค่าที่ใช้ในปัจจุบันเกี่ยวข้องกับการรักษาความปลอดภัย

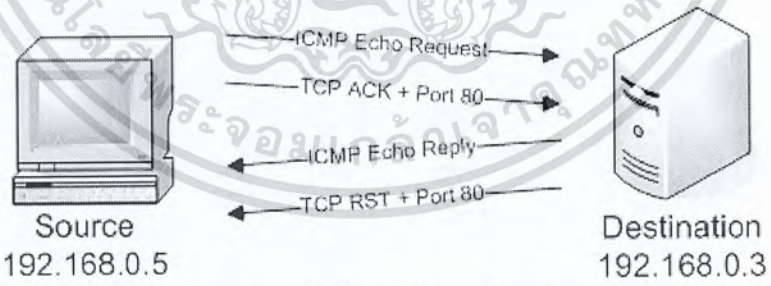
Data ขนาดไม่คงที่: ข้อมูลของโปรโตคอลระดับบน

เนื่องจากมาตราฐานในเครือข่ายมีหลากหมาย ขนาดของแพคเก็ตในแต่ละมาตราฐานจึงมีความยาวแตกต่างกันออกไป ทำให้การส่งข้อมูลระหว่างอุปกรณ์ในเครือข่ายนั้นอาจมีการแบ่งข้อมูลออกเป็นแพคเก็ตย่อยๆในระหว่างการส่ง เรียกว่าการทำแฟรกเมนเตชัน (Fragmentation) เช่น แพคเก็ต FDDI มีขนาด 4,500 ไบต์ หากเครื่องปลายทางอยู่ในเครือข่ายอีเทอร์เน็ตซึ่งมีขนาดของแพคเก็ตสูงสุด 1,500 ไบต์ ดังนั้นการส่งแพคเก็ตไปยังเครื่องปลายทางจึงต้องมีการแบ่งเป็นแพคเก็ตย่อยๆ และเมื่อแพคเก็ตย่อยมาถึงเครื่องเป้าหมายก็จะรวมกันเป็นแพคเก็ตเดิมที่มีขนาด 4,500 ไบต์อีกครั้งหนึ่ง เรียกการรวมกันนี้ว่า รีแอสเซมเบิ้ล (Reassemble) ซึ่งทำให้ได้ข้อมูลเหมือนกับที่ส่งมาจากเครื่องต้นทาง

เดทาแกรมที่ถูกแฟรกเมนต์จะมีเฮดเดอร์ประจำตัวเอง โดยมีข้อมูลเพิ่มเติมกำหนดลักษณะของเฟรกเมนต์ประกอบไปด้วย แต่ละชิ้นของแฟรกเมนต์จะเป็นเดทาแกรมที่สมบรูณ์ในตัวเอง เราเตอร์ระหว่างทางที่รับเดทาแกรมจะไม่รวมเดทาแกรม (Reassembly) แต่จะปล่อยให้เป็นหน้าที่ของเราเตอร์ปลายทาง

2.7 โปรโตคอลไอซีเอ็มพี (ICMP: Internet Control Message Protocol)

หน้าที่หลักของโปรโตคอลไอซีเอ็มพีคือ การแจ้งหรือแสดงข้อความจากระบบ เพื่อบอกให้ผู้ใช้ทราบว่าเกิดอะไรขึ้นในการส่งผ่านข้อมูลนั้น ซึ่งปัญหาส่วนมากที่พบคือส่งไปไม่ได้ หรือปลายทางรับข้อมูลไม่ได้ เป็นต้น นอกจากนี้โปรโตคอลไอซีเอ็มพียังถูกเรียกใช้งานจากเครื่องเซิร์ฟเวอร์และเราเตอร์อีกด้วย เพื่อแลกเปลี่ยนข้อมูลที่ให้ควบคุม ส่วนรูปแบบการทำงานของโปรโตคอลไอซีเอ็มพีนั้นจะทำงานควบคู่กับโปรโตคอลไอพีในระดับเดียวกัน และข้อความต่างๆที่แจ้งให้ทราบจะถูกรวบรวมอยู่ภายในข้อมูลของไอพีเดทาแกรมอีกทีหนึ่ง

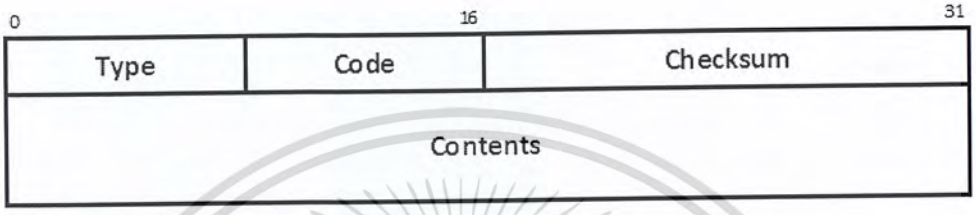


รูป 2.8 การปฏิบัติการปิง ของไอซีเอ็มพี

ข้อความที่โปรโตคอลไอซีเอ็มพีส่งนั้นแบ่งออกได้เป็น 2 แบบคือ ICMP Error Message คือข้อความแจ้งข้อผิดพลาด และ ICMP Query คือข้อความเรียกขอข้อมูลเพิ่มเติม ตัวอย่างกลไลการทำงานของโปรโตคอลไอซีเอ็มพี เช่น เมื่อมีการส่งผ่านข้อมูลจากผู้ใช้ไปยังปลายทางที่ไม่ถูกต้องหรือขณะนั้นเครื่องปลายทางเกิดปัญหาจะไม่สามารถรับข้อมูลได้ ที่เราเตอร์จะส่งข้อความเจ้งเป็นไอซีเอ็มพีที่ชื่อ Destination unreachable ให้กับผู้ส่งข้อมูล นอกจากนี้ตัวข้อมูลที่แจ้งข้อความก็จะมี

ส่วนของข้อมูลไอพีเดทาแกรมที่เกิดปัญหาด้วย ดังนั้นเมื่อผู้ส่งข้อมูลได้รับข้อความแจ้งแล้วก็จะได้ทราบว่าจุดที่เกิดปัญหาอยู่ที่ใด

ดังนั้นโปรโตคอลไอซีเอ็มพีจึงกลายเป็นเครื่องมืออย่างหนึ่งในการช่วยทดสอบเครือข่าย เช่น คำสั่ง Ping ที่เรามักใช้ทดสอบว่าเครื่องเซิร์ฟเวอร์ที่ให้บริการหรืออุปกรณ์ที่ต่ออยู่ในเครือข่ายอินเตอร์เน็ตนั้นยังทำงานเป็นปกติหรือไม่ แล้วคำสั่ง ping มีการเรียกใช้งานโปรโตคอลไอซีเอ็มพีแจ้งเป็นข่าวสารให้ทราบอีกต่อไป



รูป 2.9 ไอซีเอ็มพีเดทาแกรม

คำอธิบายรูป 2.9 ไอซีเอ็มพีเดทาแกรม

Type ขนาด 8 บิต: กำหนดทั้งค่าความผิดพลาดและการรายงานสถานะการใช้งานปัจจุบันมีทั้งหมด 15 ประเภท

Code ขนาด 8 บิต: รหัสความผิดพลาด

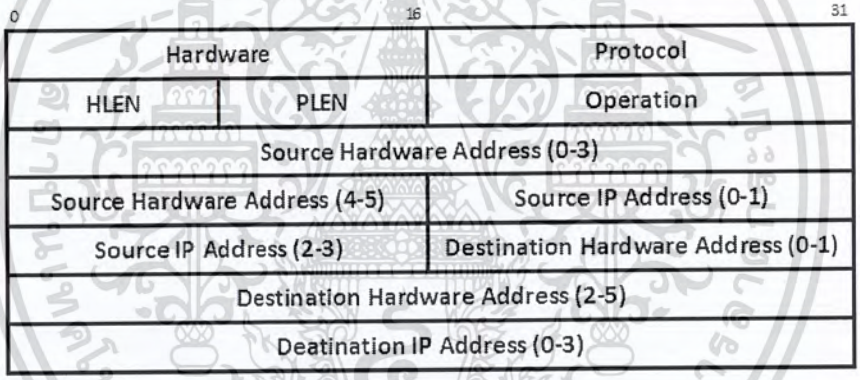
Checksum ขนาด 16 บิต: ค่าผลรวมตรวจสอบแบบ 1's complement สำหรับตรวจสอบความผิดพลาด โดยคำนวณผลรวมของ Type, Code และ Contents

Contents ขนาดไม่คงที่: ฟิลด์นี้บรรจุข้อมูลข่าวสารเพิ่มเติมเพื่อแจ้งกลับ ซึ่งจะขึ้นอยู่กับค่า Type และ Code

2.8 โปรโตคอลเออาร์พี (ARP: Address Resolution Protocol)

โปรโตคอล ARP (Address Resolution Protocol) ทำหน้าที่ในการหาแอดเดรส โดยบทบาทของโปรโตคอลเออาร์พีมีความสำคัญมาก เพราะโปรโตคอลเออาร์พีทำหน้าที่ในการจับคู่ระหว่างไอพีแอดเดรส ซึ่งเป็นแอดเดรสทางลอจิคัลกับฮาร์ดแวร์แอดเดรสซึ่งเป็นแอดเดรสทางฟิสิคัล ทั้งนี้เนื่องจากระบบของการส่งข้อมูลในระบบไอพีนั้นเป็นระบบที่ไม่ขึ้นกับฮาร์ดแวร์ใด ๆ ซึ่งหมายความว่าระบบไอพีไม่มีความสามารถในการเรียกใช้ฮาร์ดแวร์ในการส่งข้อมูลด้วยตัวเอง ทำให้เมื่อระบบไอพีต้องการส่งข้อมูล จะต้องร้องขอบริการจากระดับชั้นดาต้าลิงค์ แต่เนื่องจากระดับชั้นดาต้าลิงค์ไม่รู้จักแอดเดรสในระบบไอพี ดังนั้นระบบไอพีจึงต้องทำการหาแอดเดรสที่ระดับชั้นดาต้าลิงค์รู้จัก ซึ่งก็คือฮาร์ดแวร์แอดเดรส เพื่อที่จะสร้างเฟรมข้อมูลในชั้นดาต้าลิงค์ได้ โดยโปรโตคอลเออาร์พีจะทำหน้าที่นี้ การทำงานของอาร์พ เมื่อแพคเก็ตขาเข้าที่ระบุเครื่องโฮสต์ในระบบเครือข่ายมาถึงเกตเวย์เครื่องที่เกตเวย์จะเรียกโปรแกรมอาร์พให้หาเครื่องโฮสต์หรือแมค

แอดเดรสที่ตรงกับไอพีแอดเดรส โปรแกรมอาร์พจะหาในอาร์พแคช เมื่อพบแล้วจะแปลงแพคเก็ตเป็นแพคเก็ตที่มีความยาวและรูปแบบที่ถูกต้อง เพื่อส่งไปยังเครื่องที่ระบุไว้ แต่ถ้าไม่พบ อาร์พจะกระจายแพคเก็ตในรูปแบบพิเศษไปยังเครื่องทุกเครื่องในระบบ และถ้าเครื่องใดเครื่องหนึ่งทราบว่ามีไอพีแอดเดรสตรงกันก็จะตอบกลับมาที่อาร์พ โปรแกรมอาร์พจะปรับปรุงอาร์พแคช และส่งแพคเก็ตไปยังแมคแอดเดรสหรือเครื่องที่ตอบมา โปรโตคอลเออาร์พีได้กำหนดไว้เป็นมาตรฐานภายใต้ RFC 826 โดยการทำงานของอาร์พจะมีรูปแบบการทำงานในแบบบรอดคาสต์ ดังนั้นเครือข่ายที่ใช้งานกับโปรโตคอลเออาร์พีได้จึงต้องเป็นเครือข่ายที่มีการทำงานในแบบบรอดคาสต์ ซึ่งระบบแลนส่วนใหญ่จะมีการทำงานเป็นแบบบรอดคาสต์อยู่แล้ว จึงสามารถทำงานร่วมกับโปรโตคอลเออาร์พีได้เป็นอย่างดี และนอกเหนือจากโปรโตคอลเออาร์พีแล้วยังมีอีกโปรโตคอลหนึ่งที่ถือว่าเป็นโปรโตคอลคู่แฝดของเออาร์พี โดยจะมีการทำงานที่ย้อนกลับกันกับโปรโตคอลเออาร์พีดังนั้นจึงมีชื่อว่า RARP (Reverse ARP) โดยกำหนดไว้ภายใต้ RFC 903 โดยรูปแบบเฟรมของเออาร์พีและอาร์เออาร์พีจะมีลักษณะเหมือนกัน ดังรูป 2.10



รูป 2.10 เออาร์พีเดทาแกรม

คำอธิบายรูป 2.10 เออาร์พีเดทาแกรม

Hardware มีขนาด 16 บิต: บอกถึงชนิดของฮาร์ดแวร์ที่เออาร์พีทำงานอยู่ เช่น 1 หมายถึง เครือข่ายอีเทอร์เน็ต 4 หมายถึง เครือข่ายโทเคนริง เป็นต้น

Protocol มีขนาด 16 บิต: ทำหน้าที่บอกว่าเฟรมเออาร์พี นี้ถูกเรียกใช้จากโปรโตคอลใด

HLEN มีขนาด 8 บิต: ทำหน้าที่ระบุความยาวของฮาร์ดแวร์แอดเดรส ในกรณีของอีเทอร์เน็ตก็จะมีค่าเป็น 6

PLEN มีขนาด 8 บิต: ทำหน้าที่ระบุความยาวของแอดเดรสของโปรโตคอลที่เรียกใช้ ซึ่งในกรณีนี้ที่เรียกจากระบบไอพี ก็จะมีค่าเป็น 4

Operation มีขนาด 16 บิต: ทำหน้าที่ระบุการทำงานของอาร์พ โดยจะมี 4 ค่า ดังนี้

1) มีค่า 1 หมายถึง ARP Request ใช้ในการค้นหาหมายเลขฮาร์ดแวร์แอดเดรส

2) มีค่า 2 หมายถึง ARP Reply ใช้ในการตอบกลับเพื่อบอกหมายเลขฮาร์ดแวร์แอดเดรส

3) มีค่า 3 หมายถึง RARP Request ใช้ในการค้นหาหมายเลขของโปรโตคอล

4) มีค่า 4 หมายถึง RARP Reply ใช้ในการตอบกลับเพื่อบอกหมายเลขของโปรโตคอล

Source Hardware Address: ใช้ในการเก็บค่าฮาร์ดแวร์แอดเดรสของผู้ส่ง ไม่จำกัดความยาว

Destination Hardware Address: ใช้ในการเก็บค่าฮาร์ดแวร์แอดเดรสของผู้รับ ไม่จำกัดความยาว

Source Protocol Address: ใช้ในการเก็บค่าแอดเดรสของโปรโตคอลที่เรียกใช้ในฝั่งผู้ส่ง ไม่จำกัดความยาว

Destination Protocol Address: ใช้ในการเก็บค่าแอดเดรสของโปรโตคอลที่เรียกใช้ในฝั่งผู้รับ ไม่จำกัดความยาว

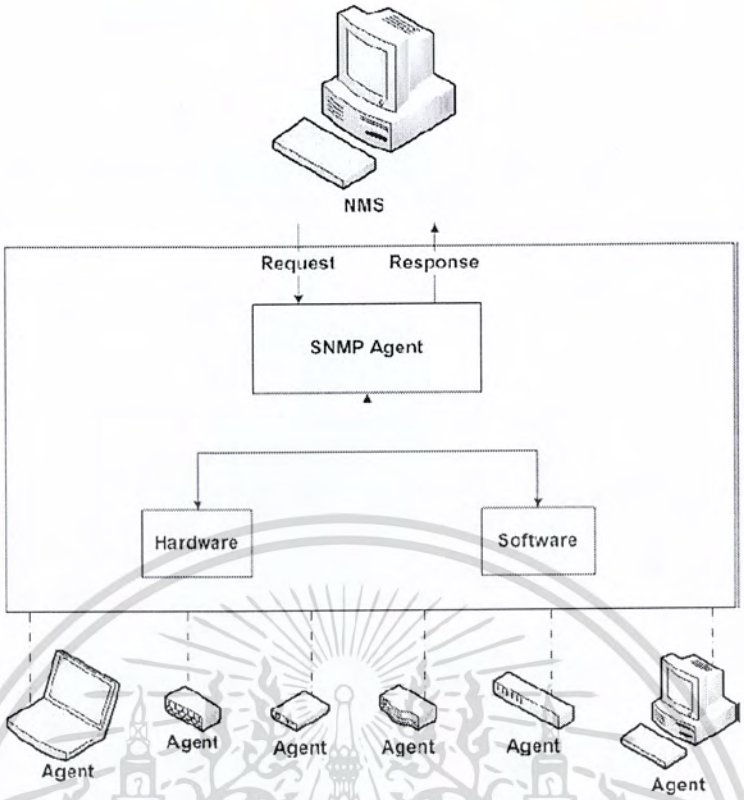
บทที่ 3
โปรโตคอลเอสเอ็นเอ็มพี

การบริหารและจัดการเครือข่ายทีซีพี/ไอพี คือ การตรวจตรา ควบคุม และวางแผนการใช้งานทรัพยากรของระบบ เพื่อให้เครือข่ายสามารถทำงานได้อย่างมีประสิทธิภาพ และสามารถตรวจหาจุดบกพร่องของเครือข่ายเมื่อเกิดปัญหา และแก้ปัญหาได้อย่างรวดเร็ว ดังนั้นในเครือข่ายจึงจำเป็นต้องมีคอมพิวเตอร์ (Computer) อย่างน้อย 1 เครื่อง เพื่อใช้ในการทำหน้าที่เป็นสถานีจัดการเครือข่ายหรือเอ็นเอ็มเอส (NMS: Network Management Station) และแต่ละเครือข่ายจะมีเอเจนต์ (Agent) หรืออุปกรณ์เครือข่ายที่มีฟังก์ชัน (Function) ให้ตรวจสอบหรือปรับเปลี่ยนการทำงานได้ โดยในเครือข่ายจะมีเอเจนต์เพียง 1 ตัว หรือหลายตัวก็ได้

ในการบริหารและจัดการเครือข่ายทีซีพี/ไอพีนั้น ผู้ที่มีหน้าที่รับผิดชอบในการบริหารจัดการจะต้องทำการบริหารจัดการเครือข่ายโดยอาศัยรูปแบบการจัดการมาตรฐานตามข้อกำหนดของโปรโตคอลเอสเอ็นเอ็มพี (SNMP Protocol) เป็นหลัก เพื่อการบริหารและจัดการเครือข่ายอย่างมีประสิทธิภาพ ดังนั้นผู้บริหารจัดการเครือข่ายควรจะต้องทำความเข้าใจในตัวโปรโตคอลเอสเอ็นเอ็มพี ซึ่งเนื้อหาในบทที่ 3 นี้ จะกล่าวถึงรายละเอียดของโปรโตคอลเอสเอ็นเอ็มพี ดังนี้

3.1 โปรโตคอลเอสเอ็นเอ็มพี

เอสเอ็นเอ็มพี (SNMP: Simple Network Management Protocol) เป็นโปรโตคอลประยุกต์ที่กำหนดรูปแบบ และกรรมวิธีในการบริหารจัดการเครือข่าย โดยจะมีสถานีจัดการเครือข่ายส่วนกลางที่เรียกว่า เอสเอ็นเอ็มพีเอเจนต์ (SNMP Agent) ทำหน้าที่ติดต่อประสานงานระหว่างเอ็นเอ็มเอส (NMS) กับอุปกรณ์เครือข่ายที่เป็นเอเจนต์ต่าง ๆ เช่น พีซี (PC: Personal Computer) โมเด็ม (Modem) ฮับ (Hub) สวิตช์ (Switch) เราเตอร์ (Router) เป็นต้น โดยเอสเอ็นเอ็มพีเอเจนต์นี้จะเชื่อมต่ออยู่กับส่วนทำงานที่เป็นฮาร์ดแวร์ และซอฟต์แวร์ของเอเจนต์ มีหน้าที่ในการคอยรับคำสั่งในการปรับเปลี่ยนการทำงานของเอเจนต์จากเอ็นเอ็มเอส และคอยรายงานข้อมูลของเอเจนต์เมื่อเอ็นเอ็มเอสร้องขอ โดยจะมีการยืนยันสิทธิในการร้องขอข้อมูลและปรับเปลี่ยนค่าของเอ็นเอ็มเอสในรูปรหัสผ่าน สำหรับการเชื่อมต่อระหว่างเอสเอ็นเอ็มพีเอเจนต์ กับส่วนทำงานที่เป็นฮาร์ดแวร์และซอฟต์แวร์ของเอเจนต์แสดงได้ดังรูป 3.1



รูป 3.1 การเชื่อมต่อเอสเอ็นเอ็มพีเอเจนต์ (SNMP Agent)

การติดต่อระหว่างเอ็นเอ็มเอสกับเอเจนต์ มีรูปแบบในการติดต่อมากมาย ขึ้นอยู่กับวัตถุประสงค์ในการติดต่อ แต่สำหรับเอสเอ็นเอ็มพีรุ่น 1 (SNMP Version 1) มีรูปแบบในการติดต่อกัน 5 แบบ ดังนี้

1) get-request: ใช้สอบถามข้อมูลจากเอเจนต์ที่อยู่บนอุปกรณ์ที่ต้องการตรวจสอบในเครือข่าย

2) get-next-request: ใช้สอบถามข้อมูลที่เรียงเป็นลำดับ เช่น ข้อมูลที่เก็บอยู่ในรูปแบบตาราง หรือในกรณีไม่ทราบชื่อตัวแปรที่แน่ชัด

3) get-response: เอเจนต์ส่งคำตอบกลับมายังผู้สอบถาม

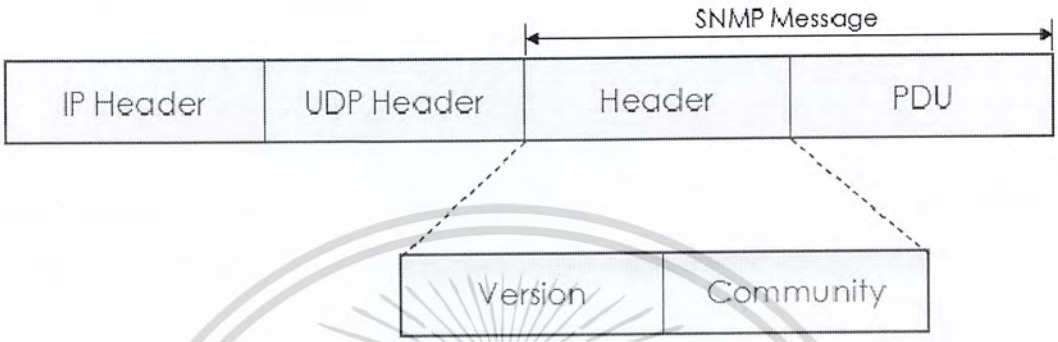
4) set-request: ใช้เปลี่ยนแปลงค่าตัวแปรที่เอเจนต์รับผิดชอบอยู่

5) trap: ใช้แจ้งเหตุการณ์ที่เกิดขึ้นในระบบเครือข่าย เช่น การเริ่มต้นทำงานใหม่ของอุปกรณ์ หรือเส้นทางที่ขัดข้อง

เอสเอ็นเอ็มพีอาศัยโปรโตคอลยูดีพีในการติดต่อ ซึ่งต้องอาศัยพอร์ต (Port) ต่าง ๆ ในการติดต่อ โดยเอสเอ็นเอ็มพีใช้พอร์ตหมายเลข 161 ในการติดต่อรูปแบบที่ 1) – 4) และใช้พอร์ตหมายเลข 162 ในการติดต่อรูปแบบที่ 5)

3.2 การเข้ารหัสข้อมูลเอสเอ็นเอ็มพี

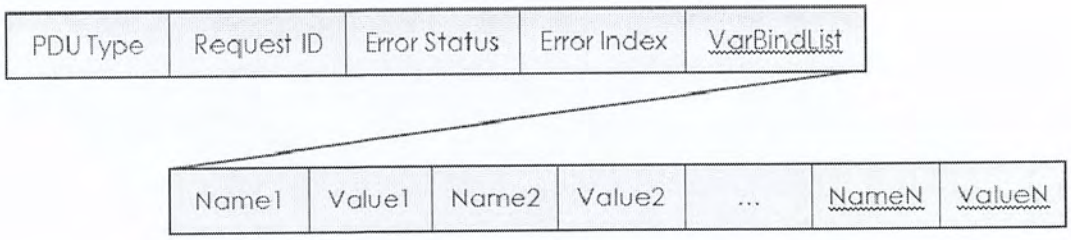
การเข้ารหัสข้อมูล หรือ การเอ็นแคปซูเลต (Encapsulate) คำสั่งและข้อมูลต่าง ๆ ในเอสเอ็นเอ็มพีแสดงได้ดังรูป 3.2 จะเห็นว่าข้อความเอสเอ็นเอ็มพี (SNMP Message) จะประกอบด้วยข้อมูล 2 ส่วนคือ เฮดเดอร์ (Header) และพีดียู (PDU)



รูป 3.2 การเข้ารหัสข้อมูลเอสเอ็นเอ็มพี

จากรูป 3.2 จะเห็นว่า ในส่วนเฮดเดอร์ของข้อความเอสเอ็นเอ็มพี จะประกอบด้วยข้อมูลอีก 2 ฟิลด์ (Field) ดังนี้

1) เวอร์ชั่น (Version) เป็นฟิลด์ที่ใช้ระบุรุ่นของโปรโตคอลเอสเอ็นเอ็มพีที่ใช้ หากใช้เอสเอ็นเอ็มพีรุ่น 1 ค่าในฟิลด์นี้จะถูกระบุเป็น 0 หากใช้เอสเอ็นเอ็มพี รุ่น 2 ค่าในฟิลด์นี้จะถูกระบุเป็น 1
2) คอมมูนิตี้ (Community) เป็นฟิลด์ที่ใช้ระบุรหัสผ่านในรูปสายอักขระ เพื่อให้เอเจนต์ใช้ในการตรวจสอบข้อความที่ส่งมา ว่ามีสิทธิ์ในการสอบถามหรือเปลี่ยนแปลงข้อมูลหรือไม่ ในส่วนพีดียูของข้อความเอสเอ็นเอ็มพีก็จะประกอบด้วยฟิลด์ย่อยเช่นกัน แต่จะมีลักษณะของฟิลด์ที่แตกต่างกันไปตามชนิดของข้อความ หากเป็นข้อความชนิด get, get-next และ get-response จะมีโครงสร้างดังรูป 3.3



รูป 3.3 โครงสร้างพีดียูของข้อความชนิด get, get-next และ get-response

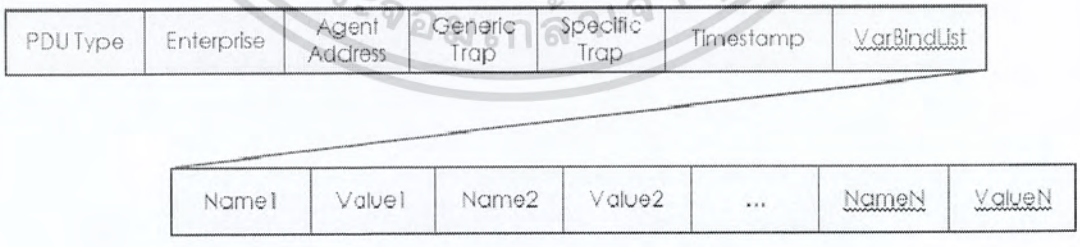
ตาราง 3.1 คำอธิบายโครงสร้างพีดียูของข้อความชนิด get, get-next และ get-response

คำศัพท์	คำอธิบาย
PDU Type	ระบุรูปแบบการติดต่อตั้งแต่รูปแบบที่ 1 -5
Request ID	กำหนดหมายเลขข้อความเพื่อใช้จับคู่ เมื่อได้รับคำตอบกลับมา
Error Status	ระบุรหัสผิดพลาดที่เกิดขึ้น ซึ่งรหัสผิดพลาดดูได้จากตารางรหัสผิดพลาดในเอสเอ็นเอ็มพี
Error Index	ดัชนีชี้ค่าผิดพลาดที่เกิดขึ้นจากตัวแปรลำดับที่เท่าไหร่ของตัวแปรทั้งหมดที่ได้ทำการสอบถามไป
VarBindList	แสดงในรูปของตัวแปร และค่าของตัวแปรต่อเนื่องกันไปเป็นรายการ

ตาราง 3.2 รหัสผิดพลาดในเอสเอ็นเอ็มพี

รหัสผิดพลาด	ชื่อความผิดพลาด	คำอธิบาย
0	noError	ไม่มีข้อผิดพลาด
1	tooBig	เอเจนต์ไม่สามารถส่งคำตอบได้ในเฟรมข้อมูลเดียว
2	noSuchName	ไม่มีตัวแปรที่ต้องการสอบถามอยู่ในฐานข้อมูล
3	badValue	ค่าที่กำหนดให้ตัวแปรไม่ถูกต้อง
4	readOnly	เปลี่ยนค่าตัวแปรไม่ได้ เพราะอ่านค่าได้เพียงอย่างเดียว
25	genErr	มีข้อผิดพลาดอื่นๆเกิดขึ้น

ส่วนข้อความชนิดที่เป็น trap จะมีลักษณะดังรูป 3.4



รูป 3.4 โครงสร้างพีดียูของข้อความชนิด trap

ตาราง 3.3 คำอธิบายโครงสร้างพีดียูของข้อความชนิด trap

คำศัพท์	คำอธิบาย
PDU Type	ระบุรูปแบบการติดต่อตั้งแต่รูปแบบที่ 1 – 5
Enterprise	ระบุชนิดของเอเจนต์ที่สร้าง trap
Agent Address	ระบุที่อยู่ของเอเจนต์ที่สร้าง trap
Generic trap type	ระบุชนิดของ Generic trap
Specific trap code	ระบุหมายเลขของ Specific trap
Time stamp	ระยะเวลาตั้งแต่เริ่มเชื่อมต่อเครือข่ายจนกระทั่งสร้าง trap
VarBindList	แสดงในรูปของตัวแปร และค่าของตัวแปรต่อเนื่องกันไปเป็นรายการ

จะเห็นว่าขนาดในแต่ละฟิลด์ของข้อความเอสเอ็นเอ็มพีจะไม่ได้ถูกกำหนดตายตัวไว้ เพราะทุกฟิลด์ของข้อความเอสเอ็นเอ็มพีจะต้องถูกเข้ารหัสข้อมูลก่อนส่ง จึงมีขนาดแตกต่างกันไปตามชนิดของข้อมูล

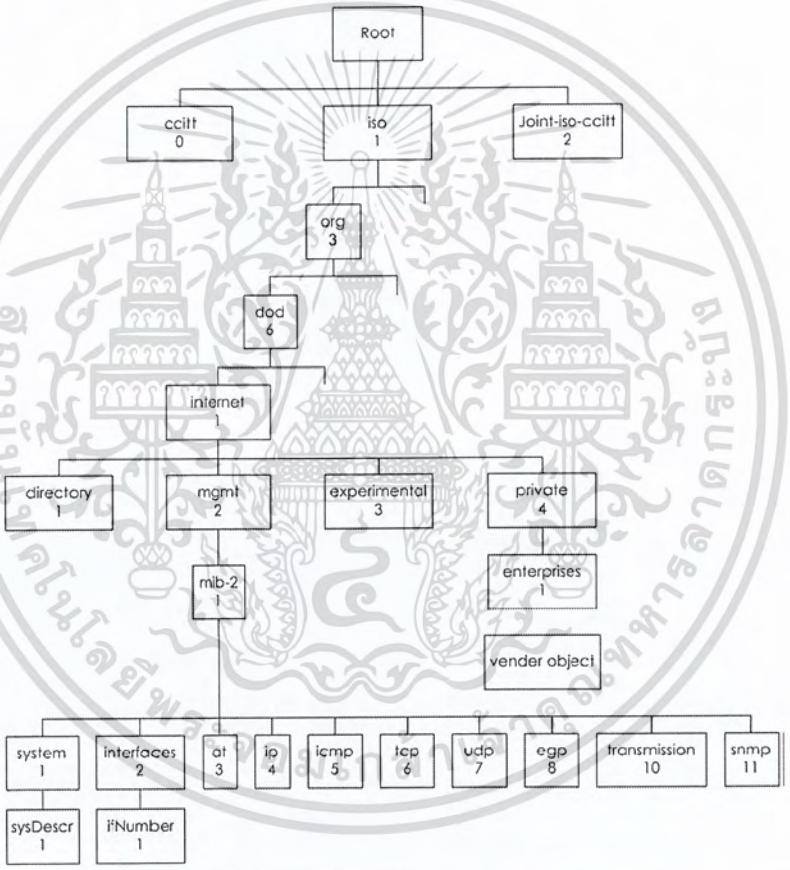
3.3 เอสเอ็นเอ็มพีรุ่นที่ 2

สำหรับในเอสเอ็นเอ็มพีรุ่น 2 นั้น ได้รับการปรับปรุงให้มีความสามารถเพิ่มขึ้นจากรุ่นแรก สำหรับรุ่นนี้ได้เพิ่มการรักษาความปลอดภัยโดยการเข้ารหัสข้อความและการพิสูจน์ตัวจริง รวมทั้งได้ขยายกลุ่มของเอ็มไอบีเพิ่มเติม และยังได้เพิ่มเติมฟังก์ชันต่าง ๆ เข้ามาอีก เช่น

1) get-bulk-request: ใช้เพื่อสอบถามค่า โดยกำหนดจำนวนวัตถุที่ต้องการได้ นำมาใช้แทนการใช้ฟังก์ชัน get-next-request หลาย ๆ ครั้ง
2) inform-request: ใช้สำหรับการสื่อสารระหว่างเอ็นเอ็มเอส เพื่อช่วยในการบริหารแบบกระจายภาระงาน

3.4 เอ็มไอบี

เอ็มไอบี (MIB: Management Information Base) หรือฐานข้อมูลสารสนเทศจัดการ ทำหน้าที่ในการเก็บตัวแปรและค่ากำหนดการทำงานประจำอุปกรณ์ ซึ่งข้อมูลประจำอุปกรณ์แต่ละตัวก็มีได้หลากหลาย และอุปกรณ์ต่างชนิดกันก็ย่อมมีข้อมูลประจำอุปกรณ์ต่างกันอีกด้วย ดังนั้นการสอบถาม (เพื่ออ่านค่า) หรือการเปลี่ยนแปลงค่า (เพื่อเขียนค่า) ในฐานข้อมูลจึงต้องมีรูปแบบที่เป็นมาตรฐานให้กับอุปกรณ์ทุกประเภท โครงสร้างที่เหมาะสมที่สุดสำหรับใช้เป็นฐานข้อมูลเพื่อจัดเก็บตัวแปรเหล่านี้คือ โครงสร้างต้นไม้แบบลำดับชั้น (Hierarchy Tree) เราเรียกโครงสร้างต้นไม้ของฐานข้อมูลนี้ว่า เอ็มไอบีทรี (MIB Tree) ซึ่งแสดงได้ดังรูป 3.5



รูป 3.5 เอ็มไอบีทรี (MIB Tree)

ในแต่ละโหนด (Node) ของเอ็มไอบีทรีนี้จะใช้แทนวัตถุ (Object) ที่มีชื่อ พร้อมทั้งเลขฐานสิบกำกับอยู่ประจำโหนด เพื่อใช้ในการอ้างอิง ยกเว้นโหนดราก (Root) ที่จะไม่มีชื่อกำกับในระดับแรกของเอ็มไอบีทรี จะมีโหนดหลัก 3 โหนด ซึ่งกำหนดกลุ่มองค์กร 3 กลุ่ม คือ ITUT(0), ISO (1) และ Joint-ISO-ITU-T (2) ภายใต้โหนด ISO มีโหนดลำดับที่ 3 คือ org (3) กำหนดองค์กรนานาชาติ และส่วนหนึ่งขององค์กรนี้คือ dod (6) หรือ Department of Defense และมีโหนด internet (1) เพื่อกำหนดกลุ่มการจัดการเครือข่ายในอินเตอร์เน็ตเมื่อต้องการอ้างอิงถึงโหนดใดในโครงสร้าง ให้

เขียนหมายเลขจากรากไปตามเส้นทางถึงโหนดนั้นและคั่นด้วยจุด เราจะเรียกลำดับตัวเลขนี้ว่า โอไอดี (OID : Object Identifier) เช่น 1.3.6.1.2.1.1 เป็นโอไอดีที่มีค่าเท่ากับชื่อ iso.org.dod.internet .mgmt.mib-2.system โหนดที่อยู่ภายใต้ 1.3.6.1.2.1 หรือในกลุ่ม mib-2 เป็นโหนดสำหรับการใช้งานเอสเอ็นเอ็มพี แต่ละโหนดจะมีโหนดย่อย เพื่ออ้างอิงถึงตัวแปรต่าง ๆ เช่น 1.3.6.1.2.1.1.1 คือ ตัวแปร sysDescr (System Description) ซึ่งทำหน้าที่เก็บคำอธิบาย เกี่ยวกับอุปกรณ์นั้น

3.5 กลุ่มในเอ็มไอบี

กลุ่มของเอ็มไอบีที่อยู่ในโลกอินเตอร์เน็ตถูกแบ่งออกเป็น 6 กลุ่มย่อย ดังนี้

1) directory: เป็นกลุ่มที่สงวนไว้สำหรับการใช้งานในอนาคต

2) mgmt: เป็นกลุ่มของเอ็มไอบีที่ใช้ในการจัดการภายใต้เอสเอ็นเอ็มพีรุ่น 1

3) experimental: ใช้สำหรับการทดลอง

4) private: สำหรับให้ผู้ผลิตกำหนดตัวแปรเฉพาะอุปกรณ์

5) security: ใช้ในระบบรักษาความปลอดภัย

6) SNMPv2: ใช้ในเอสเอ็นเอ็มพีรุ่น 2

ภายใต้กลุ่ม mib-2 จะบรรจุกลุ่มย่อยที่ใช้ในเอสเอ็นเอ็มพี ซึ่งประกอบด้วยกลุ่มต่าง ๆ ซึ่งแต่ละกลุ่ม จะประกอบด้วยตัวแปรรูปแบบต่าง ๆ กันไป ความหมายของแต่ละกลุ่มแสดงได้ดังตาราง 3.4

ตาราง 3.4 ความหมายของกลุ่มภายใต้ mib-2

ลำดับ	ชื่อกลุ่ม	ความหมาย
1	system	ข้อมูลระบบ
2	interface	ข้อมูลอินเตอร์เฟสที่ใช้เชื่อมต่อ
3	at	ข้อมูลการแปลงที่อยู่ (Address)
4	ip	ข้อมูลไอพี
5	icmp	ข้อมูลไอซีเอ็มพี
6	tcp	ข้อมูลทีซีพี
7	udp	ข้อมูลยูดีพี
8	egp	ข้อมูลโปรโตคอลเกตเวย์ภายนอก
9	transmission	ข้อมูลสายสื่อสาร
10	snmp	ข้อมูลเอสเอ็นเอ็มพี

3.6 ชนิดของตัวแปรในเอ็มไอบี

ตัวแปรแต่ละชนิดของเอสเอ็นเอ็มพีจะมีแบบข้อมูลประจำเป็นของตัวเอง ซึ่งแบบข้อมูลต่าง ๆ ที่ใช้ในเอสเอ็นเอ็มพี ก็คือตัวแปรชนิดต่าง ๆ ในเอ็มไอบีนั่นเอง และชนิดของตัวแปรต่าง ๆ ในเอ็มไอบีแสดงได้ดังตาราง 3.5

ตาราง 3.5 ชนิดของตัวแปรในเอ็มไอบี

รูปแบบข้อมูล	คำอธิบาย
Integer	ข้อมูลที่เป็นจำนวนเต็ม มีค่าได้ตั้งแต่ 0 ถึง 65,535 เช่นหมายเลขพอร์ตของโปรโตคอลทีซีพี เป็นต้น
OctetString	ข้อมูลที่เก็บเป็นสายอักขระตั้งแต่ 0 อ็อคเต็ต แต่ละอ็อคเต็ตมีค่าตั้งแต่ 0 ถึง 255 ตัวอย่างเช่น รหัสผ่าน
DisplayString	ข้อมูลที่เก็บเป็นสายอักขระตั้งแต่ 0 อ็อคเต็ต แต่ละอ็อคเต็ตต้องเป็นรหัสแบบแอสกี้ เอ็นวีที (ASCII NVT) มีความยาวตั้งแต่ 0 ถึง 255 ตัวอักษร
Null	ใช้เพื่อระบุว่าตัวแปรนั้นไม่มีค่าข้อมูลใดอยู่เลย เช่น เมื่อมีการสอบถามข้อมูลด้วยคำสั่ง get หรือ get-next-request จะทำการกำหนดรูปแบบตัวแปรเป็น Null
ObjectIdentifier	ชื่อตัวแปรในรูปของการอ้างถึงแบบตัวเลขตามโครงสร้างของเอ็มไอบี
IpAddress	เป็นสายอักขระ 4 อ็อคเต็ต แต่ละอ็อคเต็ตแทนไอพีแอดเดรสในแต่ละตำแหน่ง
PhysicalAddress	เป็นสายอักขระกำหนดหมายเลขของฮาร์ดแวร์ (Hardware Address) เช่น ในอีเทอร์เน็ตแอดเดรส (Ethernet Address) ใช้สายอักขระ 6 อ็อคเต็ต
Counter	เป็นเลขจำนวนเต็มที่ไม่คิดเครื่องหมาย มีค่าตั้งแต่ 0 ถึง 223-1 (4,294,267,295) ค่าของข้อมูลชนิดนี้จะเพิ่มขึ้นไปเรื่อย ๆ (เพิ่มอย่างเดียว) จนกระทั่งถึงค่าสูงสุด ก็จะกลับมาเริ่มต้นที่ 0 ใหม่อีกครั้ง
Gauge	เป็นเลขจำนวนเต็มที่ไม่คิดเครื่องหมาย มีค่าตั้งแต่ 0 ถึง 223-1 (4,294,267,295) เหมือน Counter แต่ค่าของข้อมูลชนิดนี้สามารถเพิ่มหรือลดค่าได้ และเมื่อค่าเพิ่มไปถึงค่าสูงสุดก็จะคงค่าไว้ตามเดิมจนกว่าจะมีการปรับค่าให้กลับมาเป็น 0 อีกครั้ง ตัวอย่างตัวแปรที่ใช้ค่านี้ เช่น จำนวนการเชื่อมโยงทีซีพีที่อนุญาตให้มีได้

ตาราง 3.5 ชนิดของตัวแปรในเอ็มไอบี (ต่อ)

รูปแบบข้อมูล	คำอธิบาย
TimeTicks	เป็นเลขจำนวนเต็มที่ใช้นับเวลาในหน่วยเศษหนึ่งส่วนร้อยของวินาที เช่น เวลานับตั้งแต่ที่ระบบทำงาน (system uptime)
Sequence	เป็นโครงสร้างแบบเรคคอร์ด (Record)
Sequence of	เป็นโครงสร้างแบบตาราง หรืออาจมองเป็นรูปของอาเรย์ (Array) เช่น ตารางเลือกเส้นทางของไอพี

บทที่ 4
การออกแบบและการพัฒนาโปรแกรม

4.1 วัตถุประสงค์ของโปรแกรม

1) สามารถที่จะรับข้อมูลจากเครือข่ายโปรโตคอลทีซีพี/ไอพีได้จาก 2 แหล่งที่มา คือ จากเอสเอ็นเอ็มพี (SNMP) และ จากตัวดักจับแพคเก็ต (Packet Sniffer)

2) สามารถตรวจจับสิ่งที่ก่อให้เกิดความผิดปกติขึ้นในระบบเครือข่ายได้ ดังนี้

2.1) ปัญหาการใช้งานในเครือข่ายมากผิดปกติ (High Bandwidth)

2.2) ปัญหาการใช้งานแพคเก็ตในเครือข่ายมากผิดปกติ (High Packet Flow)

2.3) ปัญหาการใช้งานเครือข่ายต่อบุคคลมากผิดปกติ (High Bandwidth per Host)

2.4) ปัญหาการใช้งานแพคเก็ตในเครือข่ายต่อบุคคลมากผิดปกติ (High Packet Flow per Host)

2.5) ปัญหาการใช้งานในช่องทางพอร์ต 80 มากผิดปกติ (High Port 80 bandwidth)

2.6) ปัญหาการใช้งานแพคเก็ตในช่องทางพอร์ต 80 มากผิดปกติ (High Port 80 Packet Flow)

2.7) ปัญหาขัดข้องของอุปกรณ์เครือข่ายที่สนับสนุนการตรวจสอบ (Device Malfunction)

2.8) ปัญหาการเชื่อมต่อไม่รู้จบ (Loop connection)

3) สามารถแสดงผลที่ได้จากการวิเคราะห์ ดังนี้

3.1) การแจ้งเตือนในลักษณะของข้อความ จะแจ้งเตือนเมื่อมีเหตุการณ์ผิดปกติเกิดขึ้นในระบบออกทางหน้าจอของผู้ใช้

3.2) ล็อกไฟล์ที่ทำการแจ้งเตือน จะทำการเก็บการแจ้งเตือนที่ผ่านมาไว้อ้างอิงต่อไป

3.3) การแจ้งเตือนโดยสัญญาณภาพ จะแจ้งเตือนเป็นสัญญาณไฟกระพริบ เพื่อแจ้งเตือนให้ทราบเมื่อความผิดปกติเกิดขึ้นภายในระบบ

3.4) การรายงานความผิดปกติที่เกิดขึ้นสามารถทำการแปลงเป็นเอกสารจริง หรือเป็นเอกสารอิเล็คโทรนิคและอื่นๆได้ต่อๆไป

4) ทำงานได้บนระบบปฏิบัติการลีนุกซ์

5) เป็นโอเพ่นซอร์สซึ่งนำไปพัฒนาต่อได้ในอนาคต

4.2 รายละเอียดการพัฒนาโปรแกรม

การออกแบบและพัฒนาโปรแกรม จะต้องพิจารณาถึงขั้นตอนการทำงานต่างๆ ของโปรแกรม ประสิทธิภาพและการใช้ทรัพยากรของระบบที่มีอยู่จำกัด รวมไปถึง ผลลัพธ์การวิเคราะห์ของโปรแกรมจะต้องมีความใกล้เคียงกับปัญหาที่เกิดขึ้นจริงของระบบในขณะนั้น

4.2.1 รายละเอียดการนำเข้า (Input Specification)

1) ข้อมูลโครงสร้างของระบบเครือข่าย
2) ข้อมูลในแต่ละลำดับการวิเคราะห์ของต้นไม้การตัดสินใจที่ช่วยในการวิเคราะห์ปัญหาที่เกิดขึ้น
3) ข้อมูลของเครือข่ายที่ต้องการทำการตรวจตรา
4) ข้อมูลที่ได้จากเอสเอ็นเอ็มพีของอุปกรณ์เครือข่าย
5) ข้อมูลที่ได้จากตัวดักจับแพคเก็ตในระบบเครือข่าย

4.2.2 รายละเอียดส่วนนำออก (Output Specification)

1) กราฟแสดงข้อมูลต่างๆในระบบเครือข่าย
2) โครงสร้างของเครือข่ายที่ทำการตรวจตราและวิเคราะห์
3) ระบบการเตือนเมื่อเกิดความผิดปกติขึ้นในระบบเครือข่าย
4) ผลการวิเคราะห์ระบบเครือข่ายเมื่อเกิดความผิดปกติขึ้นมาในระบบ

4.2.3 รายละเอียดฟังก์ชั่น (Functional Specification)

1) โปรแกรมสามารถสร้างเครือข่ายจำลองของเครื่องคอมพิวเตอร์ที่กำลังใช้งาน เพื่อช่วยในการวิเคราะห์ปัญญาเครือข่ายได้
2) มีโมเดลในการวิเคราะห์ปัญหาในระบบเครือข่ายที่เป็นลำดับขั้นตอนที่แน่นอนและชาญฉลาด นอกจากนี้ผู้ดูแลระบบยังสามารถเพิ่มโมเดลในการวิเคราะห์ระบบเครือข่ายได้ (Decision Tree Analysis Model)
3) โปรแกรมมีการทำงาน 3 สถานะ เพื่อลดปริมาณการใช้งานของทรัพยากรในระบบเครือข่ายที่โปรแกรมใช้
4) โปรแกรมมีระบบในการเตือนให้ผู้ดูแลระบบทราบเมื่อพบความผิดปกติ และมีระบบแจ้งเตือนไปยังผู้ใช้งาน
5) โปรแกรมสามารถตรวจวัดปริมาณการใช้งานเครือข่ายของเครื่องคอมพิวเตอร์แต่ละเครื่องและแต่ละเครือข่ายย่อยได้
6) โปรแกรมมีลักษณะการทำงานเป็นเซิฟเวอร์และแสดงผลการตรวจวัดบนหน้าเว็บเพจแสดงการใช้งานของผู้ใช้รายโฮสต์ และระบุกลุ่มไอพีผ่านหน้าเว็บเพจได้
7) โปรแกรมสามารถบันทึกสถิติการใช้งานของผู้ใช้ในระบบได้
8) ผู้ดูแลระบบและผู้ใช้สามารถดูสถิติการใช้งานได้

4.2.4 ขอบเขตและข้อจำกัดของโปรแกรม

1) โปรแกรมทำงานมีประสิทธิภาพสูงสุดบนระบบปฏิบัติการลินุกซ์เท่านั้น
2) โปรแกรมทำงานได้ดีกับระบบเครือข่ายที่มีการออกแบบเป็นชั้นการทำงานเป็น 3 ชั้น ได้แก่ชั้นใจกลาง (Core Layer), ชั้นดิสทริบิ้วชั่น (Distribution Layer), และชั้นแอคเซส (Access Layer)
3) ในการเก็บรวบรวมข้อมูลของระบบเครือข่าย จำเป็นต้องใช้เอสเอ็นเอ็มพี (SNMP) และตัวดักจับแพคเก็ต (Packet Sniffer) ดังนั้นอุปกรณ์ในระบบจะต้องสนับสนุนการทำงานของโปรโตคอลนี้ด้วย
4) โปรแกรมถูกออกแบบส่วนติดต่อกับผู้ใช้งานให้ง่ายต่อความเข้าใจ

4.2.5 เครื่องมือที่ใช้ในการพัฒนา

1) ระบบปฏิบัติการลินุกซ์ โครงงานนี้ได้เลือกใช้ระบบปฏิบัติการเซนต์ (Cent Os) เนื่องจากเป็นระบบปฏิบัติการที่เป็นฟรีแวร์ และเหมาะสำหรับการทำเป็นระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์แม่ข่าย
2) ภาษาที่ใช้ในการพัฒนาคือ ภาษาจาวา, เพิร์ล ใช้ในการเขียนโปรแกรมหลัก
3) ระบบฐานข้อมูลที่ใช้คือ เครื่องมือราวดน์โรบิน และเท็กไฟล์ (Text File)
4) อุปกรณ์เครือข่ายของสาขาวิชา ได้แก่ Cisco Catalyst 4006
5) เครื่องคอมพิวเตอร์ส่วนบุคคล 1 เครื่องและเครื่องคอมพิวเตอร์พกพา 1 เครื่อง

4.2.6 ไลบรารี่ที่ใช้ในการพัฒนา

1) เน็ต-เอสเอ็นเอ็มพี ไลบรารี่ (Net-SNMP Library) เนื่องจากเอสเอ็นเอ็มพีเป็นโปรโตคอลที่ใช้กันอย่างกว้างขวางสำหรับตรวจตราสภาพการทำงานของอุปกรณ์เครือข่ายต่างๆ (ยกตัวอย่างเช่น เราเตอร์) อุปกรณ์ทั่วไปของคอมพิวเตอร์ (ยกตัวอย่างเช่น เครื่องสำรองไฟ) ซึ่ง เน็ต-เอสเอ็นเอ็มพีเป็นชุดของคำสั่งที่ใช้ในการเรียกใช้เอสเอ็นเอ็มพีเวอร์ชัน 1, เอสเอ็นเอ็มพีเวอร์ชัน 2ซี และ เอสเอ็นเอ็มพีเวอร์ชัน 3 โดยได้ทั้ง ไอพีเวอร์ชัน 4 และไอพีเวอร์ชัน 6
2) เจกราฟ ไลบรารี่ (Jgraph Library) เป็นไลบรารี่ที่ช่วยให้สามารถสร้างกราฟหรือโมเดลชาร์ตรูปต่างๆโดยใช้ภาษาจาวา ซึ่งไลบรารี่นี้สามารถสร้างวางรูปแบบของโมเดลต่างๆได้อย่างอิสระ และสามารถปรับความสามารถต่างๆตามที่เราต้องการ ไม่ว่าจะเป็นการวางรูปแบบลักษณะถ่ายทอดเป็นลำดับชั้น, เป็นวงกลม, เป็นลักษณะของต้นไม้ และ แบบทางตรง โดยที่จะมุ่งไปในเรื่องของการสร้างและแก้ไขส่วนติดต่อใช้งานกับผู้ใช้
3) เจกราฟที ไลบรารี่ (Jgrapht Library) เป็นไลบรารี่ที่ใช้เกี่ยวกับกราฟของภาษาจาวาแบบไม่เสียค่าใช้จ่าย ซึ่งจะมีออปเจคเกี่ยวกับการคำนวณทางคณิตศาสตร์ของทฤษฎี

กราฟและอัลกอริทึ่ม ซึ่ง Jgrapht รับรองประเภทของกราฟหลากหลายรูปแบบ ดังต่อไปนี้

3.1) กราฟที่มีทิศทางและไม่มีทิศทาง

3.2) กราฟที่เส้นโยงขอบมีการถ่วงน้ำหนัก, ไม่ถ่วงน้ำหนัก, มีการติดชื่อ หรือที่ผู้ใช้ตั้งขึ้นมาเอง

3.3) ความสามารถในการสร้างเส้นโยงขอบหลากหลายรูปแบบ รวมไปถึง กราฟเดียว กราฟรวม ซูโดกราฟ

3.4) สร้างกราฟที่สามารถอ่านได้อย่างเดียวได้

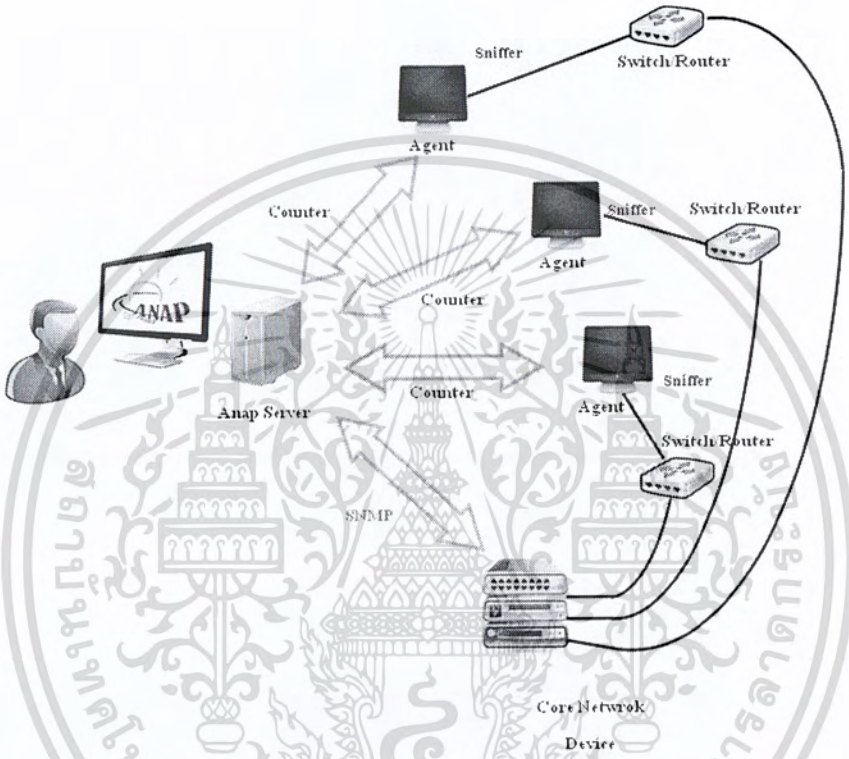
3.5) และอื่นๆที่ใช้งานในกราฟ

ถึงแม้ว่า Jgrapht จะมีความสามารถมากมาย แต่ Jgrapht ก็ถูกออกแบบมาให้ใช้ได้ง่ายและปลอดภัย ยกตัวอย่างเช่น ผู้ใช้สามารถสร้างกราฟโดยบนฐานของสตริงยูอาร์แอล เอกสารเอ็กซ์เอ็มแอล และอื่นๆ ซึ่งยังสามารถสร้างกราฟของกราฟได้อีกด้วย ซึ่ง Jgrapht นั้นจะมุ่งไปในเรื่องของโครงสร้างของข้อมูลและอัลกอริทึ่มเป็นหลักซึ่งสามารถทำงานร่วมกับไลบรารี่ Jgraph ได้ ซึ่งจะช่วยส่งเสริมให้กราฟที่สร้างมีประสิทธิภาพมากขึ้น

4) เจพีแคป ไลบรารี่ (Jpcap Library) เป็นไลบรารี่จาวาที่ใช้สำหรับดักจับและส่งแพคเก็ตในเครือข่าย การใช้ Jpcap นั้น ผู้ใช้สามารถพัฒนาโปรแกรมขึ้นมาเพื่อดักจับแพ็ตเก็ตจากอินเตอร์เฟสของเครือข่ายและทำการแสดงหรือวิเคราะห์แพคเก็ตเหล่านั้นได้ในจาวา และผู้ใช้สามารถที่จะพัฒนาโปรแกรมเพื่อที่จะส่งแพคเก็ตออกไปผ่านอินเตอร์เฟสเข้าไปยังเครือข่ายได้อีกด้วย Jpcap อยู่บนฐานของไลบรารี่ libpcap/winpcap ดังนั้น Jpcap จึงทำงานบนระบบปฏิบัติการไหนก็ได้ที่รับรองไลบรารี่ libpcap/winpcap Jpcap สามารถตรวจจับแพคเก็ตอีเธอร์เน็ต, ไอพีเวอร์ชัน 4, ไอพีเวอร์ชัน 6, เออาร์พี/อาร์เออาร์พี, ทีซีพี, ยูดีพี, และ ไอซีเอ็มพีเวอร์ชัน 4

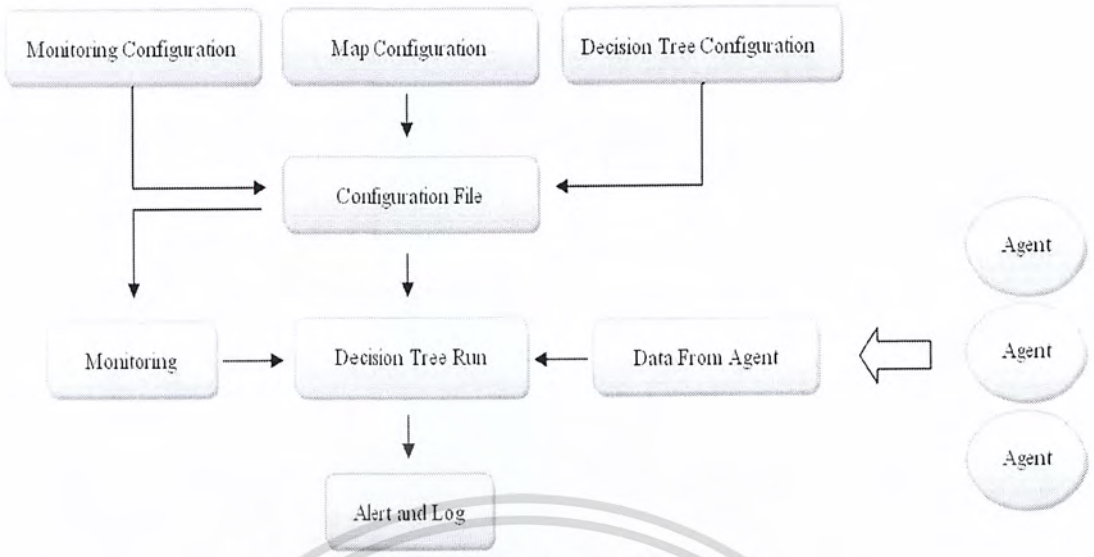
4.3 โครงสร้างของระบบ

โครงสร้างของระบบประกอบไปด้วย เซิร์ฟเวอร์ของโปรแกรมที่จะคอยรับค่านับ (Counter) จากโปรแกรมเอเจนต์ซึ่งทำการดักจับแพคเก็ตจากอุปกรณ์เครือข่ายต่างๆในเครือข่าย และรับข้อมูลเอสเอ็นเอ็มพี (SNMP) จากอุปกรณ์ที่เป็นแกนหลักของระบบเครือข่าย เพื่อนำมาวิเคราะห์และทำการแจ้งเตือนให้ผู้ใช้ได้ทราบเมื่อเกิดความผิดปกติ



รูป 4.1 โครงสร้างของระบบ

และในส่วนโครงสร้างซอฟต์แวร์ของโปรแกรมวิเคราะห์เครือข่ายอัตโนมัติ ได้แบ่งส่วนการทำงานออกเป็น 5 ส่วนหลักๆ คือ ส่วนการกำหนดค่า (Configuration) ส่วนการตรวจตราข้อมูลในระบบเครือข่าย (Monitoring) ส่วนวิเคราะห์ระบบเครือข่าย (Analysis) ส่วนการเก็บข้อมูล (Retrieval) และส่วนติดต่อผู้ใช้ (User Interface) ซึ่งมีรายละเอียดดังต่อไปนี้



รูป 4.2 โครงสร้างซอฟต์แวร์

4.3.1 ส่วนการกำหนดค่า (Configuration)

จะประกอบด้วย 3 ส่วนคือ ส่วนการกำหนดค่าการมอนิเตอริง(Monitoring) ส่วนการกำหนดแผนที่เครือข่าย (Map) และส่วนการกำหนดต้นไม้การตัดสินใจ (Decision Tree)

1) ส่วนการมอนิเตอริ่ง จะทำหน้าที่รับอินพุตจากผู้ดูแลระบบ ข้อมูลที่รับเข้ามาจะเป็นไอพีเอดเดรส (IP Address) คอมมูนิตี้สตริง (Community String) และอินเด็กซ์ (Index)
2) ส่วนการกำหนดแผนที่เครือข่าย (Map) จะทำหน้าที่รับข้อมูลการเชื่อมต่อกันของอุปกรณ์ในระบบเครือข่าย
3) ส่วนการกำหนดต้นไม้การตัดสินใจ (Decision Tree)

4.3.2 ส่วนการตรวจตราข้อมูลในระบบเครือข่าย (Monitoring)

ส่วนตรวจตราข้อมูลในระบบเครือข่าย (Monitoring) จะทำหน้าที่อ่านข้อมูลเครือข่ายจากอุปกรณ์เครือข่าย โดยการอ่านข้อมูลจะใช้โปรโตคอลเอสเอ็มเอ็นพี (SNMP Protocol) และจะนำค่าที่อ่านได้มาสร้างเป็นกราฟ เพื่อแสดงปริมาณการใช้งานเครือข่ายในขณะนั้น

4.3.3 ส่วนวิเคราะห์ระบบเครือข่าย (Analysis)

ส่วนการวิเคราะห์เครือข่าย เป็นส่วนที่ใช้วิเคราะห์สิ่งผิดปกติที่เกิดขึ้นในระบบเครือข่าย โดยมีฐานข้อมูลสำหรับเก็บข้อมูลที่จำเป็น ซึ่งได้มาจากอุปกรณ์ในระบบเครือข่าย โปรแกรมจะนำข้อมูลเหล่านั้นเข้าสู่โมเดลการวิเคราะห์ของต้นไม้การตัดสินใจเพื่อวิเคราะห์สิ่งผิดปกติที่เกิดขึ้น จากนั้นจะนำผลลัพธ์จากการวิเคราะห์แจ้งแสดงให้ผู้ดูแลระบบทราบเพื่อทำการแก้ไขปัญหาต่อไป

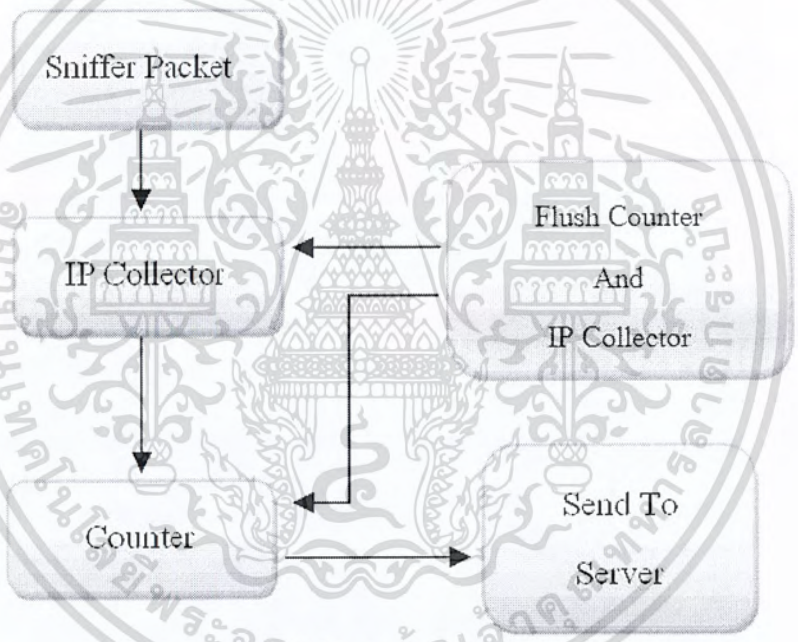
4.3.4 ส่วนการเก็บข้อมูล (Retrieval)

ส่วนการเก็บข้อมูลจะทำหน้าที่เก็บข้อมูลบนระบบเครือข่ายเพื่อนำมาใช้ในการวิเคราะห์ โดยข้อมูลของระบบจะมาจาก 2 แหล่งด้วยกัน คือ

1) ข้อมูลเครือข่ายจากเอสเอ็มเอ็นพี (SNMP) ได้แก่ ปริมาณแบนด์วิดท์ และปริมาณแพคเก็ต

2) ข้อมูลเครือข่ายจากโปรแกรมเอเจนต์ (Agent) จะได้จากดักจับแพคเก็ตจากเน็ตเวิร์คย่อยที่โปรแกรมเอเจนต์นั้นๆทำงานอยู่

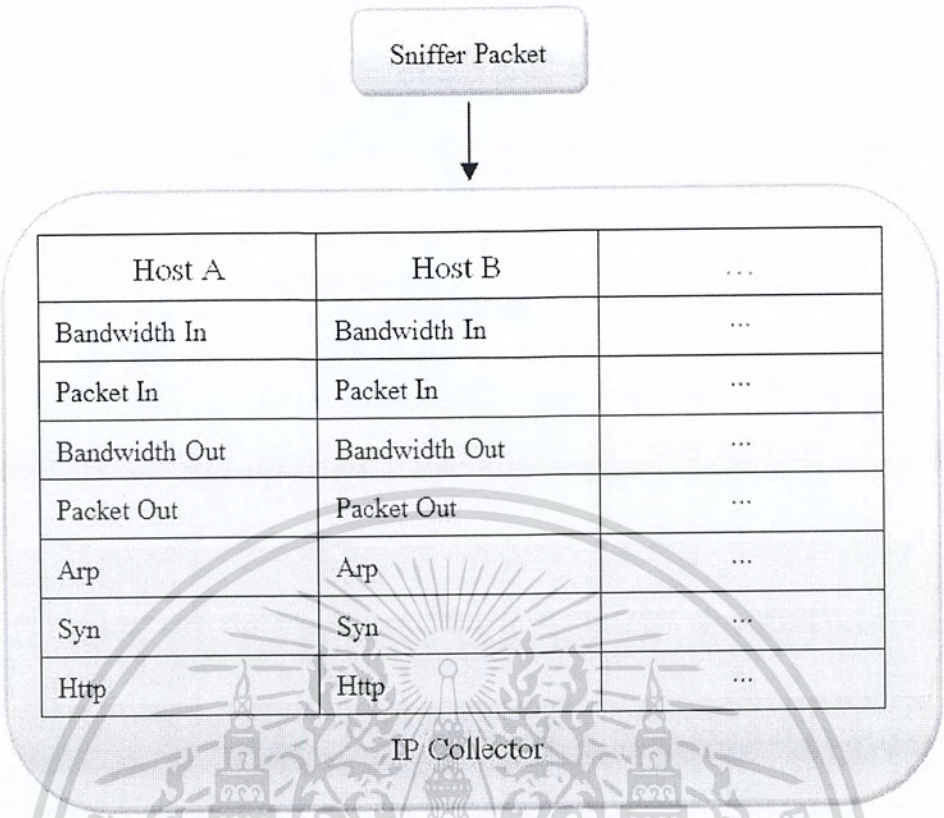
โปรแกรมเอเจนต์จะประกอบด้วย 5 ส่วน คือ ส่วนการดักจับแพคเก็ต (Packet Sniffer) ส่วนการเก็บแพคเก็ต (IP Collector) ส่วนการนับ (Counter) ส่วนการลบแพคเก็ตที่เก็บและการนับ (Flush IP Collector and Counter) และส่วนการติดต่อกับโปรแกรมเซิร์ฟเวอร์



รูป 4.3 โครงสร้างของโปรแกรมเอเจนต์

1) ส่วนการดักจับแพคเก็ต (Packet Sniffer) จะทำหน้าที่ดักจับแพคเก็ตจากระบบเครือข่ายที่เอเจนต์ถูกติดตั้งไว้

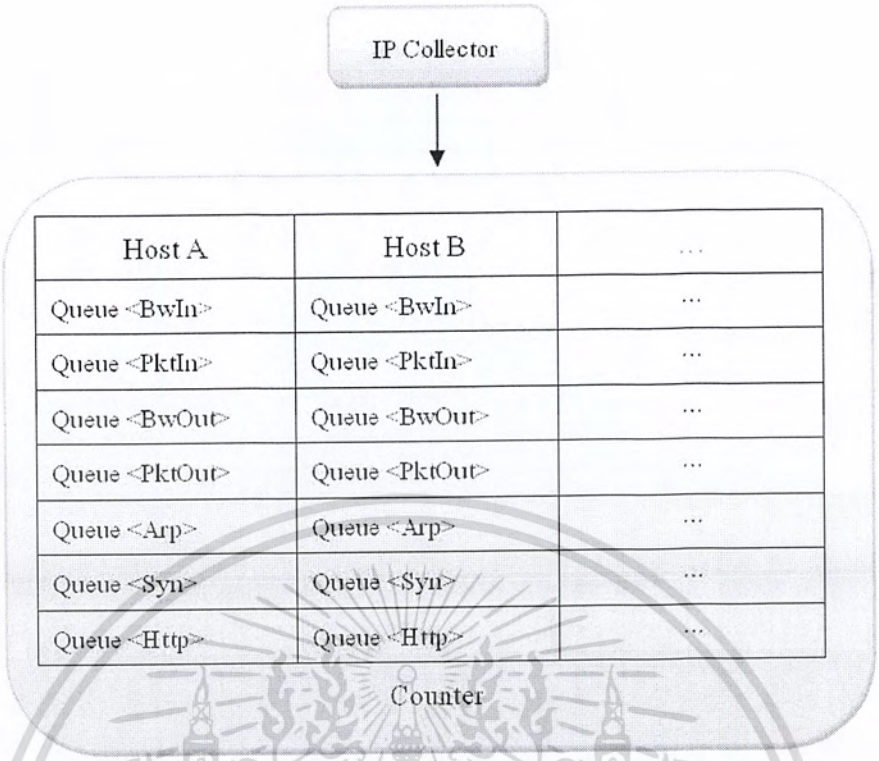
2) ส่วนการเก็บข้อมูลแพคเก็ต (IP Collector) จะรับแพคเก็ตที่ดักจับมาได้มาแยกส่วนประกอบ และจะเก็บข้อมูลเหล่านั้นไว้สำหรับทำตัวนับ (Counter)



รูป 4.4 โครงสร้างข้อมูลของส่วนการเก็บข้อมูลแพคเก็ต

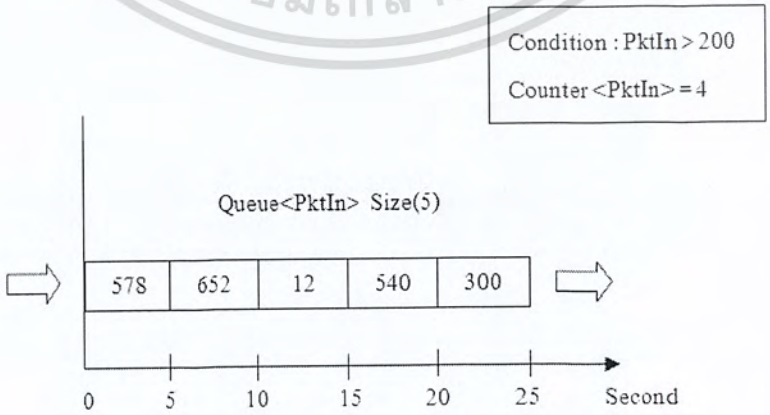
จากรูป 4.4 โครงสร้างข้อมูลที่ส่วนการเก็บข้อมูลแพคเก็ต โดยข้อมูลที่เก็บได้แต่ ปริมาณแบนด์วิดท์ ปริมาณแพคเก็ต ปริมาณอาร์พแพคเก็ต (ARP) ปริมาณซิงค์แพค เก็ต (SYN) และปริมาณแบนด์วิดท์โปรโตคอลเอชทีทีพี (HTTP) ของแต่ละโฮสที่โปรแกรมเอเจนต์ดักจับได้

3) ส่วนการนับ (Counter) จะทำหน้าที่คำนวณค่าต่างๆ เพื่อนำไปใช้ในแบบวิเคราะห์รูปแบบต้นไม้การตัดสินใจ (Decision Tree)



รูป 4.5 โครงสร้างข้อมูลที่ใช้เก็บตัวนับ (Counter)

จากรูป 4.5 ตัวนับจะทำการคำนวณค่าต่างที่แต่ละโฮสใช้ จากข้อมูลที่รับมาจากส่วนการเก็บข้อมูลแพคเก็ต (IP Collector) ข้อมูลที่คำนวณได้แก่ ปริมาณแบนด์วิดท์ ปริมาณแพคเก็ต ปริมาณอาร์พแพคเก็ต (ARP) ปริมาณซิงค์แพกเก็ต (SYN) และปริมาณแบนด์วิดท์โปรโตคอลเอชทีทีพี (HTTP) ของแต่ละโฮสที่โปรแกรมเอเจนต์ดักจับได้ ตัวนับจะใช้โครงสร้างข้อมูลแบบคิว (Queue) ในการเก็บข้อมูลต่างๆ ที่คำนวณได้ดังนี้



รูป 4.6 โครงสร้างข้อมูลแบบคิว (Queue)

จากรูป 4.6 ข้อมูลที่ตัวนับคำนวณได้จะถูกในมาเก็บในคิว เพื่อตรวจเช็คจำนวนของข้อมูลที่คำนวณได้ ที่เป็นไปตามค่าที่กำหนดไว้ในต้นไม้การตัดสินใจ (Decision Tree) จากรูป 4.6 ค่าที่กำหนดไว้จากต้นไม้การตัดสินใจคือ จำนวนแพคเก็ตขาเข้ามากกว่า 200 เมื่อโปรแกรมตรวจสอบจากคิวที่เก็บปริมาณแพคเก็ตขาเข้าจะได้ว่า ค่าของตัวนับปริมาณแพคเก็ตขาเข้าของโอสมีค่าเท่ากับ 4 ค่าของตัวนับปริมาณแพคเก็ตขานี้จะถูกส่งไปยังโปรแกรมฝั่งเซิร์เวอร์ต่อไป เมื่อเวลาผ่านไปข้อมูลในคิวจะถูกแทนที่ด้วยค่าที่คำนวณได้ใหม่ และโปรแกรมจะทำการคำนวณค่าของตัวนับต่างๆ ใหม่ และรอให้ข้อมูลถูกส่งไปยังโปรแกรมฝั่งเซิร์ฟเวอร์ จากนั้นโปรแกรมเอเจนต์จะทำการเคลียร์ค่าที่ ส่วนการเก็บข้อมูลแพคเก็ตและส่วนตัวนับออก เพื่อป้องกันปัญหาการใช้เมมโมรีมากเกินไปจนโปรแกรมไม่สามารถรันได้

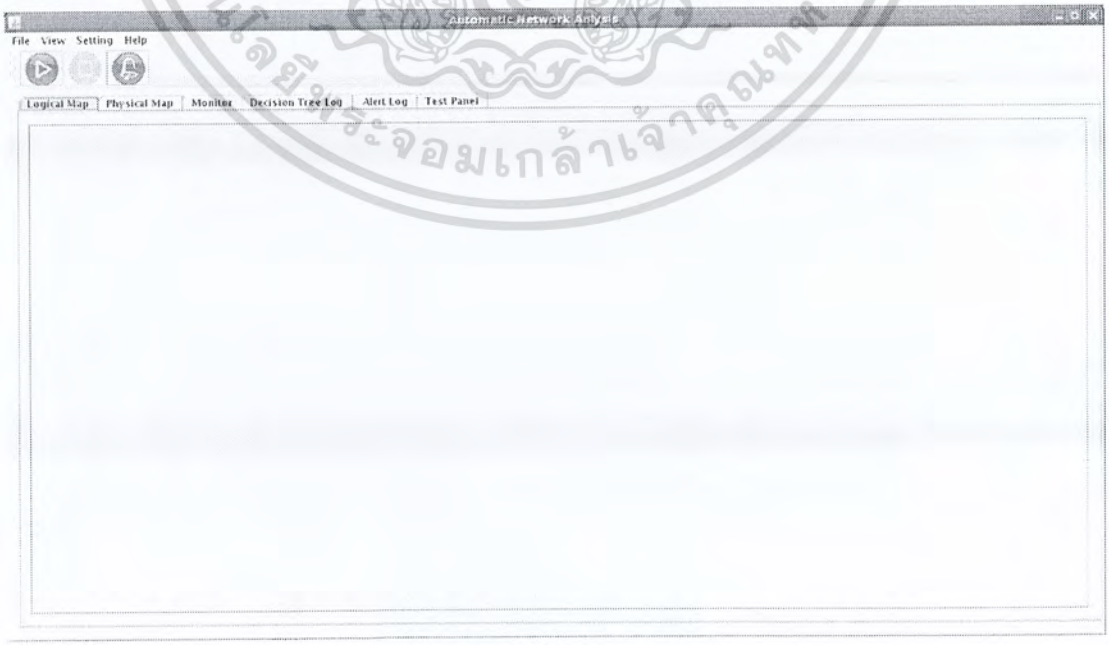
4) ส่วนการลบแพคเก็ตที่เก็บและการนับ (Flush IP Collector and Counter) จะทำการเคลียร์ค่าที่ส่วนการเก็บข้อมูลแพคเก็ตและส่วนตัวนับออก ทุกครั้งที่ข้อมูลถูกส่งไปยังโปรแกรมฝั่งเซิร์ฟเวอร์

5) ส่วนการติดต่อกับโปรแกรมเซิร์ฟเวอร์ จะทำหน้าที่ส่งข้อมูลไปยังโปรแกรมฝั่งเซิร์ฟเวอร์

4.3.5 ส่วนติดต่อผู้ใช้ (User Interface)

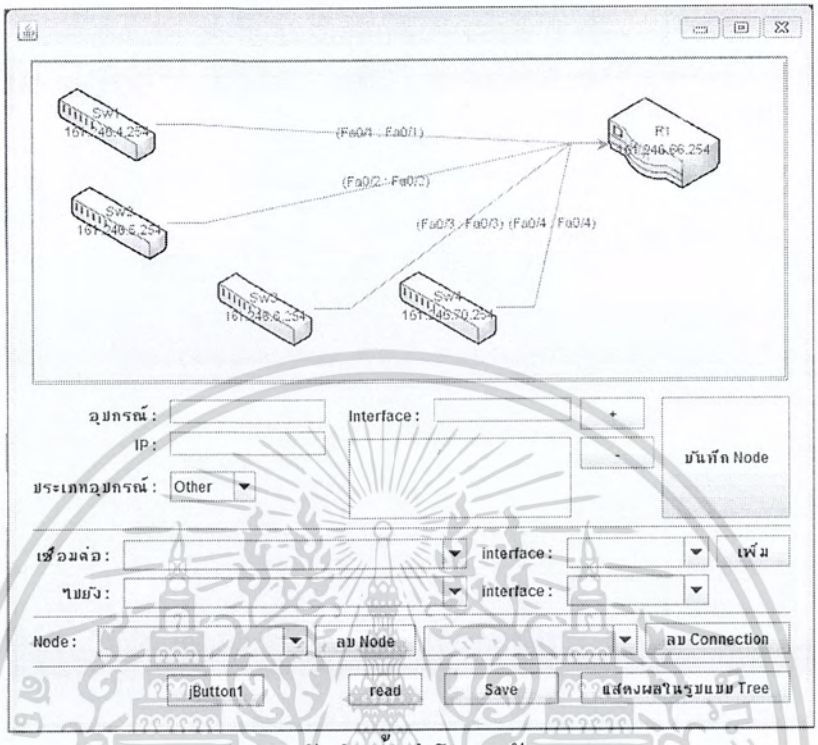
ในส่วนนี้จะกล่าวถึงหน้าตาของโปรแกรมที่ผู้ใช้จะต้องทำการตั้งค่าต่างๆ รวมไปถึงส่วนที่แสดงการแจ้งเตือนและออกรายงาน ซึ่งแบ่งได้เป็นดังนี้

1) ส่วนหน้าโปรแกรมหลัก เป็นส่วนที่ผู้ใช้จะเริ่มต้นการใช้งานโปรแกรม



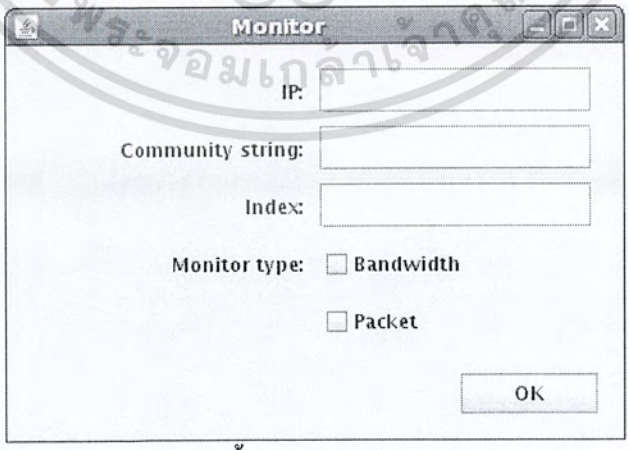
รูป 4.7 หน้าโปรแกรมหลัก

2) ส่วนหน้าต่างตั้งค่าโครงสร้างระบบเครือข่าย ซึ่งมีไว้สำหรับให้ผู้ใช้ตั้งค่าโครงสร้างของระบบเครือข่ายที่ใช้ในการตรวจตราและวิเคราะห์



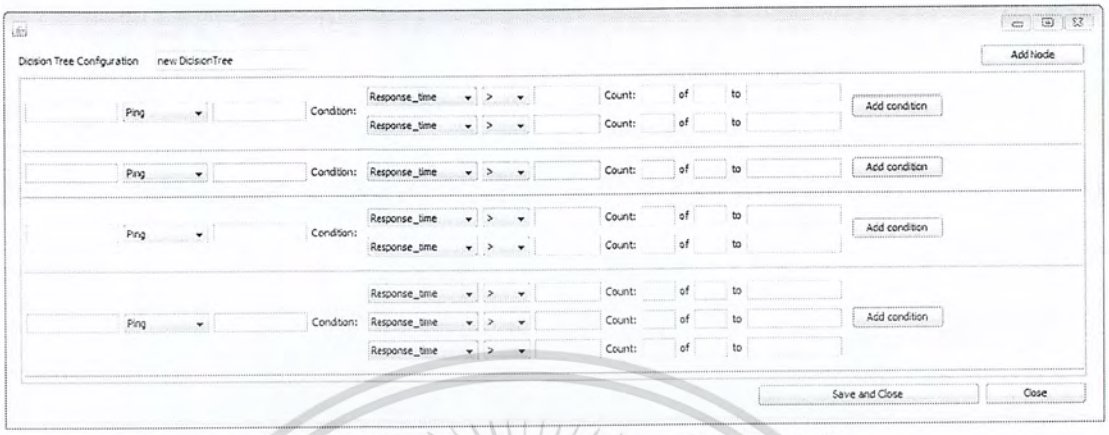
รูป 4.8 หน้าต่างตั้งค่าโครงสร้างระบบ

3) ส่วนหน้าต่างตั้งค่ารายละเอียดการตรวจตรา ซึ่งมีไว้สำหรับให้ผู้ใช้ตั้งค่าไอพีแอดเดรสของคอร์สวิตซ์ คอมมูนนิตี้สตริง และอินเด็กซ์ เพื่อใช้สำหรับตรวจตราระบบเครือข่าย



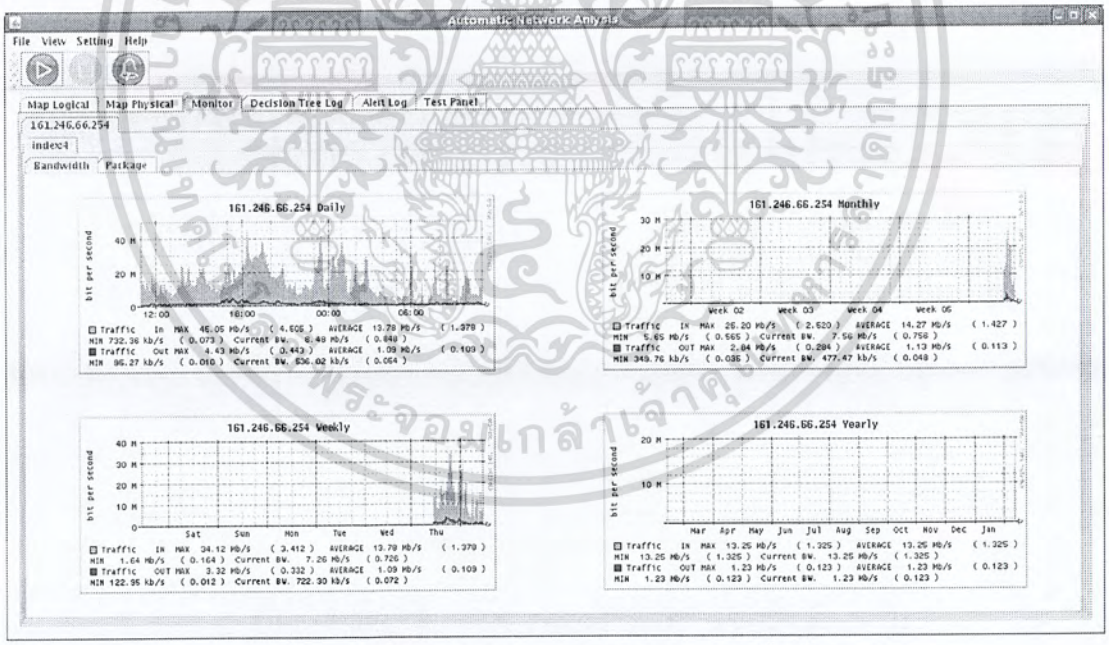
รูป 4.9 หน้าต่างตั้งค่ารายละเอียดการตรวจตรา

4) ส่วนหน้าต่างแบบวิเคราะห์รูปแบบต้นไม้ตัดสินใจ ซึ่งมีไว้สำหรับให้ผู้ใช้สร้างกฎสำหรับวิเคราะห์เครือข่ายโดยใช้แบบวิเคราะห์รูปแบบต้นไม้ตัดสินใจ



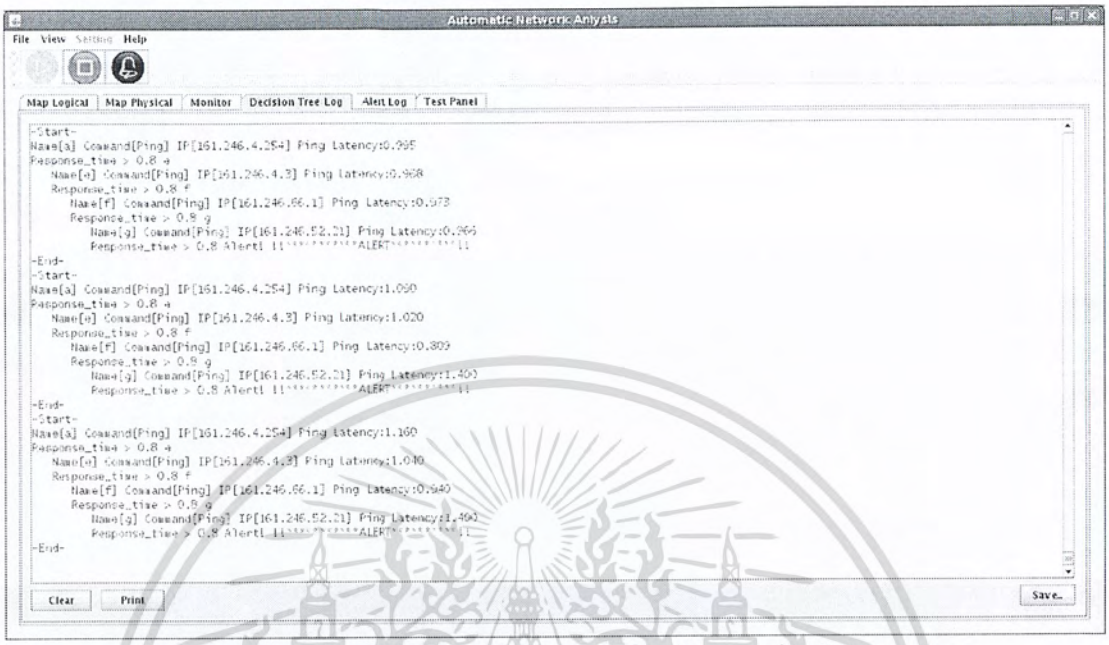
รูป 4.10 หน้าต่างแบบวิเคราะห์รูปแบบต้นไม้ตัดสินใจ

5) ส่วนหน้าต่างแสดงการตรวจตราระบบเครือข่าย เป็นส่วนที่ใช้สำหรับแสดงให้ผู้ใช้เห็นปริมาณการใช้งานเครือข่ายแบบต่างๆ



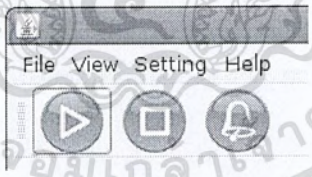
รูป 4.11 หน้าต่างแสดงการตรวจตราระบบเครือข่าย

6) ส่วนการแสดงผลการวิเคราะห์ของแบบวิเคราะห์ต้นไม้ตัดสินใจ เป็นส่วนที่จะแสดงการทำงานของแบบวิเคราะห์ ณ ขณะนั้นว่ากำลังทำงานอะไรอยู่

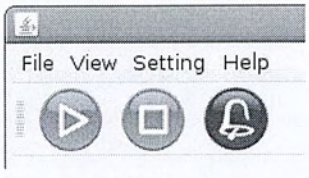


รูป 4.12 ส่วนการแสดงผลการวิเคราะห์ของแบบวิเคราะห์ต้นไม้ตัดสินใจ

7) ส่วนการแจ้งเตือนเมื่อเกิดความผิดปกติในระบบเครือข่ายแบบไฟกระพริบ เมื่อระบบทำงานปกติ ที่รูประฆังจะเป็นสีเขียวนิ่ง แต่ถ้าเกิดความผิดปกติขึ้นจะเปลี่ยนเป็นสีแดงกระพริบ

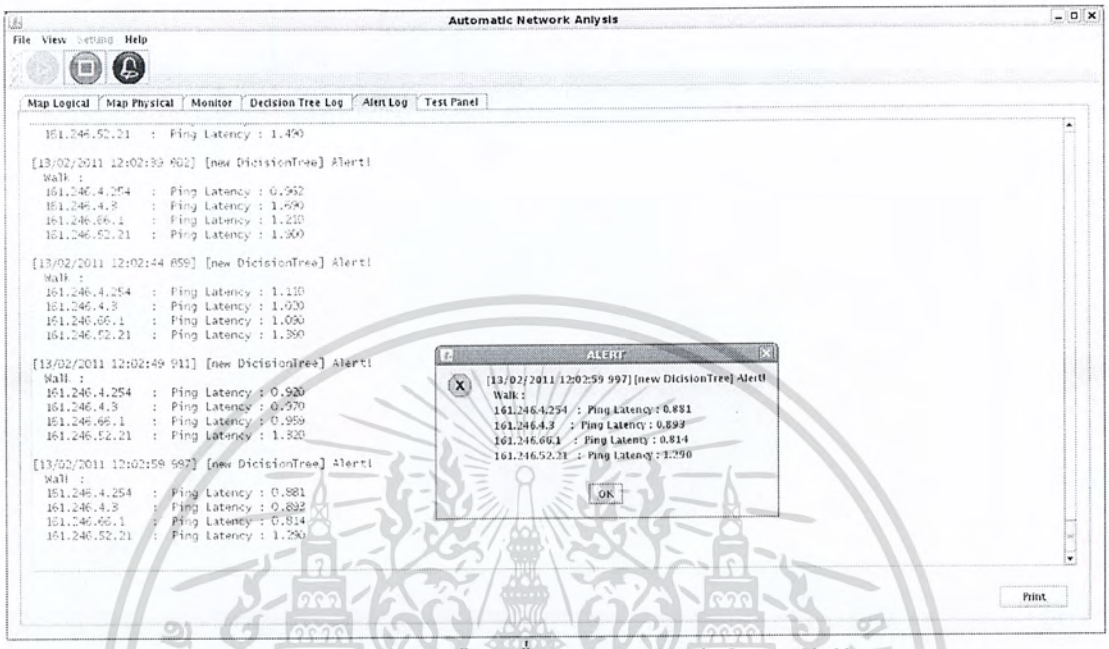


รูป 4.13 ส่วนการแจ้งเตือนในสถานะปกติ



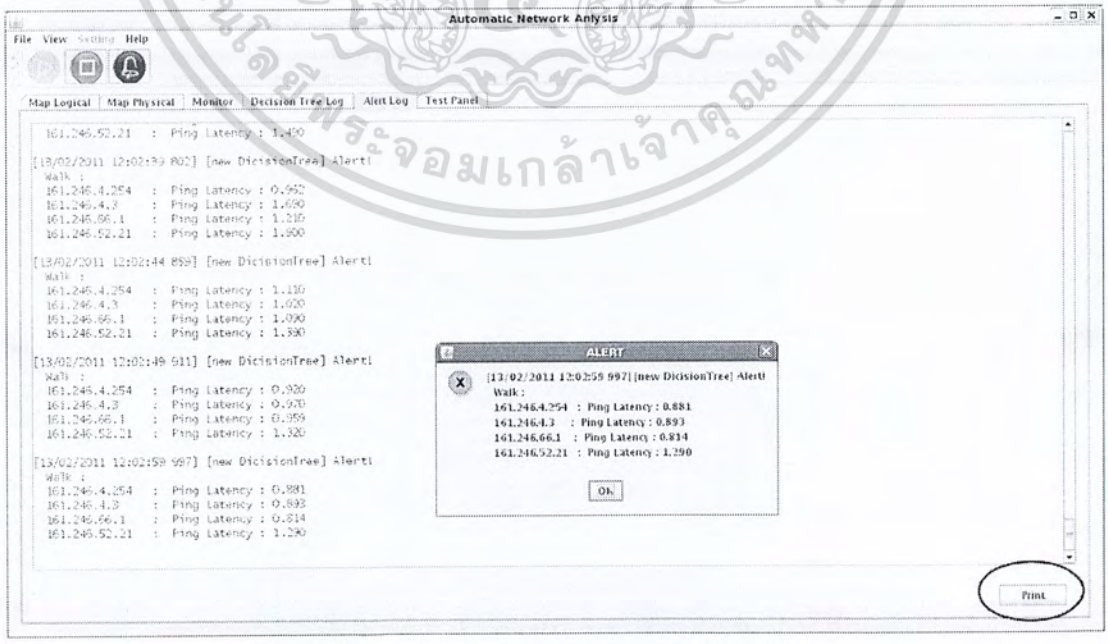
รูป 4.14 ส่วนการแจ้งเตือนในสถานะผิดปกติ

8) ส่วนการแจ้งเตือนเมื่อเกิดความผิดปกติแบบตัวอักษร เมื่อเกิดความผิดปกติขึ้นที่หน้าต่างส่วนนี้จะแสดงข้อมูลจากการวิเคราะห์ของสิ่งที่ผิดปกติให้ผู้ใช้ได้เห็นเพื่อนำไปอ้างอิงและแก้ไขต่อไป



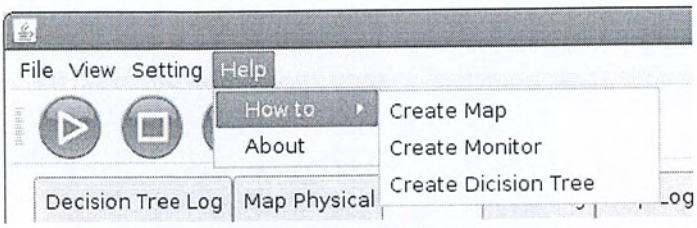
รูป 4.15 ส่วนการแจ้งเตือนเมื่อเกิดความผิดปกติแบบตัวอักษร

9) ส่วนการออกรายงานความผิดปกติ เป็นส่วนที่จะแสดงรายละเอียดที่โปรแกรมวิเคราะห์เจอออกทางหน้าเว็บเพื่อให้ผู้ใช้นำไปอ้างอิงต่อไป

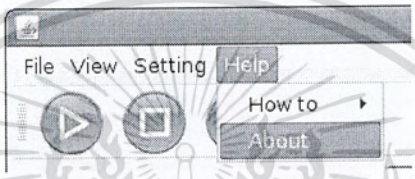


รูป 4.16 ส่วนการออกรายงานความผิดปกติ

10) ส่วนของคู่มือการใช้งานโปรแกรมและรายละเอียดของผู้จัดทำ เป็นส่วนที่จะอธิบายเกี่ยวกับการตั้งค่าต่างๆของโปรแกรมในเบื้องต้น และแสดงรายละเอียดเกี่ยวกับผู้จัดทำ



รูป 4.17 ส่วนของคู่มือการใช้งานโปรแกรม

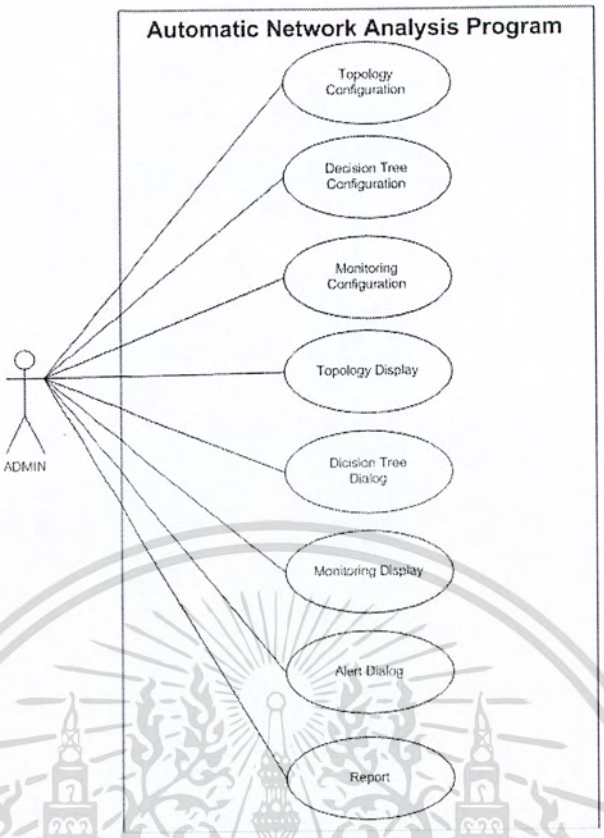


รูป 4.18 ส่วนของรายละเอียดผู้จัดทำ

4.4 การออกแบบและผังการทำงานของโปรแกรม

4.4.1 ยูสเคสไดอะแกรม (Use Case Diagram)

ผู้ใช้สามารถตั้งค่าโครงสร้างของระบบเครือข่าย ตั้งกฎที่ใช้ในการวิเคราะห์บนแบบการวิเคราะห์รูปแบบต้นไม้ตัดสินใจ และตั้งค่าการตรวจตราปริมาณในระบบเครือข่ายได้ อีกทั้งยังสามารถเรียกดูหน้าจอแสดงโครงสร้างระบบเครือข่าย หน้าต่างการวิเคราะห์ หน้าจอการตรวจตราในลักษณะกราฟ หน้าต่างบันทึกการแจ้งเตือน และออกรายงานผลการวิเคราะห์และการแจ้งเตือนได้

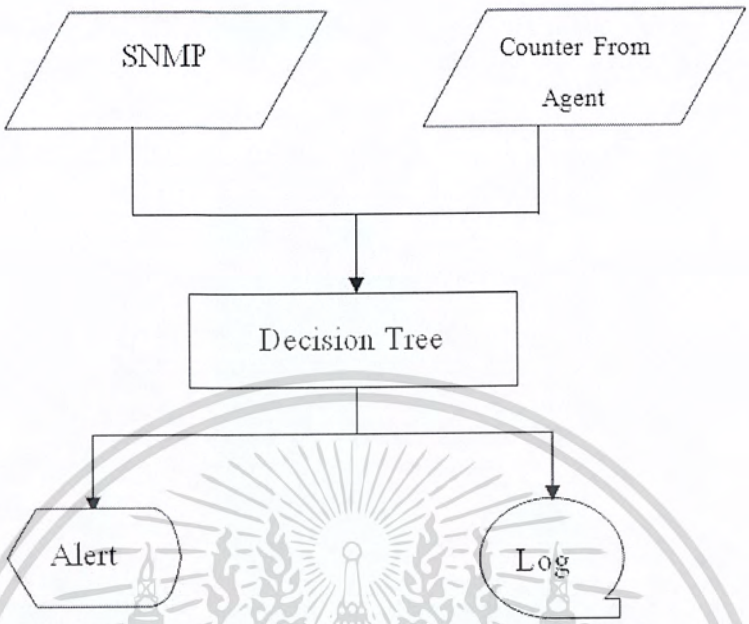


รูป 4.19 ยูสเคสไดอะแกรม

4.4.2 โครงสร้างการส่งข้อมูล (Data Flow)

โครงสร้างของการส่งข้อมูลในโปรแกรมจะถูกแบ่งออกเป็น 2 ส่วน คือ โครงสร้างของการส่งข้อมูลสำหรับโปรแกรมฝั่งเซิร์ฟเวอร์ และโครงสร้างของการส่งข้อมูลสำหรับโปรแกรมฝั่งเอเจนต์

1) โครงสร้างของการส่งข้อมูลสำหรับโปรแกรมฝั่งเซิร์ฟเวอร์



รูป 4.20 โครงสร้างของการส่งข้อมูลสำหรับโปรแกรมฝั่งเซิร์ฟเวอร์

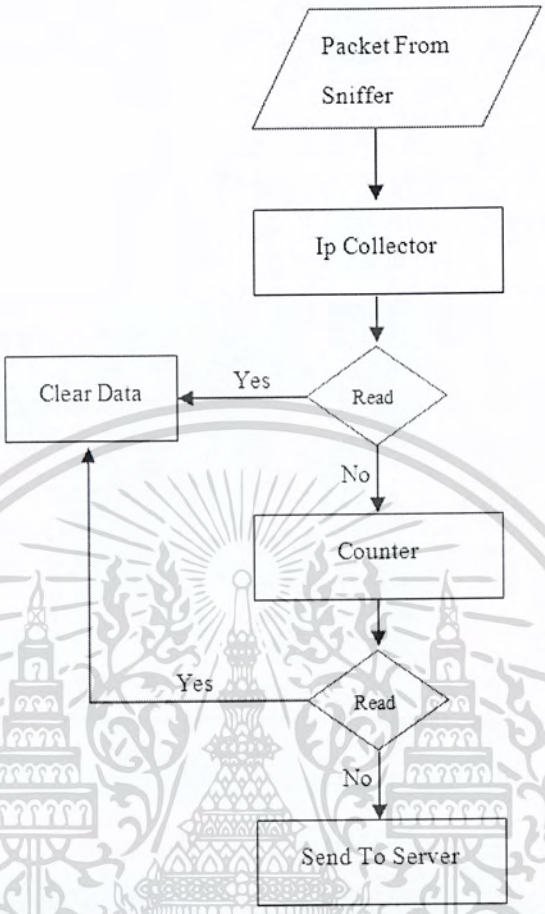
จากรูป 4.20 จะเห็นได้ว่า โปรแกรมจะรับข้อมูลมาจาก 2 แหล่ง คือ

1.1) ข้อมูลจากโปรโตคอลเอสเอ็นเอ็มพี (SNMP)

1.2) ข้อมูลบนเครือข่ายจากโปรแกรมเอเจนต์ (Agent)

ข้อมูลที่ได้รับมาจะเป็นค่าของจำนวนตัวนับ (Counter) ยกตัวอย่างเช่น จำนวนตัวนับของจำนวนแพคเก็ตขาเข้าที่ผ่านอินเทอร์เฟสของเราเตอร์ (Router) ข้อมูลเหล่านี้จะถูกนำไปใช้โดยแบบวิเคราะห์รูปแบบต้นไม้ตัดสินใจโดยจะนำไปใช้เป็นค่าคอสท์ (Cost) เพื่อใช้ในการตัดสินใจที่จะข้ามไปทำงานในสถานะอื่นๆ

2) โครงสร้างของการส่งข้อมูลสำหรับโปรแกรมฝั่งเอเจนต์



รูป 4.21 โครงสร้างของการส่งข้อมูลสำหรับโปรแกรมฝั่งเอเจนต์

ข้อมูลที่ได้รับมาจะเป็นแพคเก็ตที่ดักจับได้จากเครือข่ายที่เอเจนต์ถูกติดตั้งอยู่ แพคเก็ตจะถูกนำมาแยกชิ้นส่วนประกอบ จากนั้นจะถูกนำมาเก็บที่ไอพีคอลเล็กเตอร์ (IP Collector) ข้อมูลที่เก็บโดยไอพีคอลเล็กเตอร์จะถูกนามาคำนวณเป็นค่าตัวนับรอเวลาที่จะส่งไปยังโปรแกรมฝั่งเซิร์ฟเวอร์ เมื่อข้อมูลถูกส่งไปยัง Anap Server แล้วจะถูกลบทิ้งทันที เพื่อป้องกันการใช้หน่วยความจำของเครื่องมากเกินไป

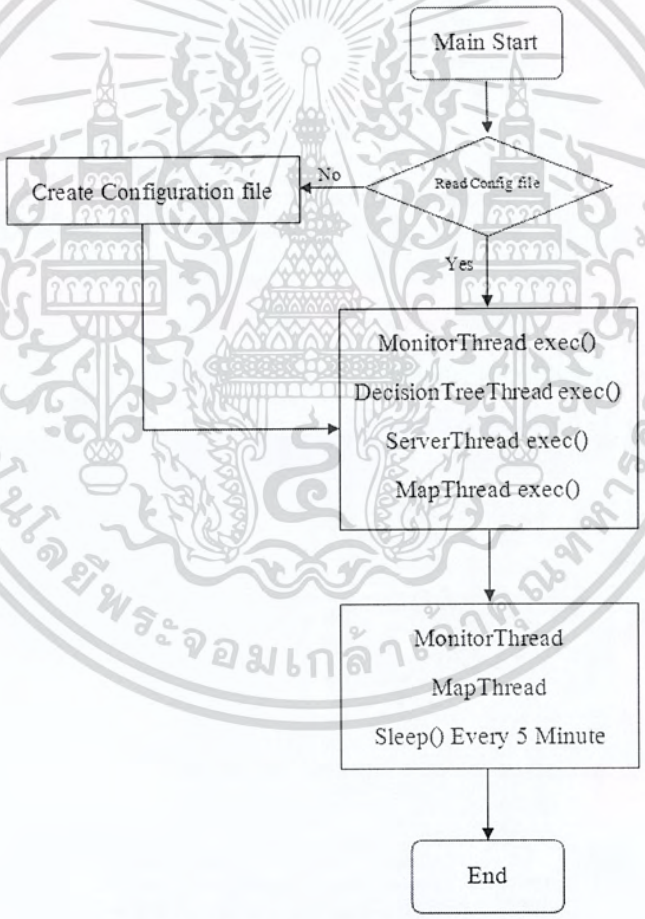
4.4.3 ผังการทำงานของโปรแกรม (Flow Chart)

โปรแกรมวิเคราะห์เครือข่ายอัตโนมัติถูกออกแบบให้มีการทำงานแบบมัลติเธรดดิง (Multithreading) คือโปรแกรมสามารถทำงานได้หลายหน้าที่การทำงานพร้อมๆ กัน โดยโปรแกรมจะถูกแบ่งออกเป็น 2 ส่วน คือ โปรแกรมฝั่งเซิร์ฟเวอร์ และโปรแกรมเอเจนต์

1) ผังการทำงานของโปรแกรมฝั่งเซิร์ฟเวอร์

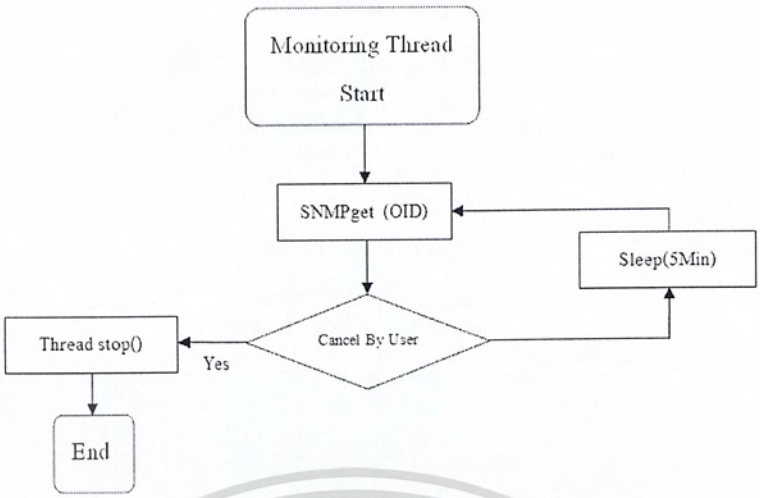
จะประกอบด้วย ส่วนการทำงานหลักของโปรแกรม (Main) ส่วนการมอนิเตอร์ริง (Monitoring) ส่วนการรับข้อมูลจากโปรแกรมเอเจนต์ (Agent to Server) และส่วนการวิเคราะห์ข้อมูล (Decision Tree)

1.1) ผังการทำงานของโปรแกรมหลัก เมื่อโปรแกรมเริ่มทำงาน โปรแกรมจะตรวจสอบไฟล์ที่เก็บค่าต่างๆของระบบไว้ ซึ่งหากไม่มีไฟล์ดังกล่าว จะต้องทำการสร้างไฟล์ขึ้นมาก่อน แต่ถ้ามีไฟล์ที่เก็บค่าต่างๆของระบบแล้วจะไปสั่งให้เธรดของการตรวจตรา เธรดของแบบวิเคราะห์ เธรดของเซิร์ฟเวอร์ และเธรดของโครงสร้างระบบเครือข่ายทำงานในส่วนเธรดตรวจตราจะทำการพักการทำงานทุก 5 นาที



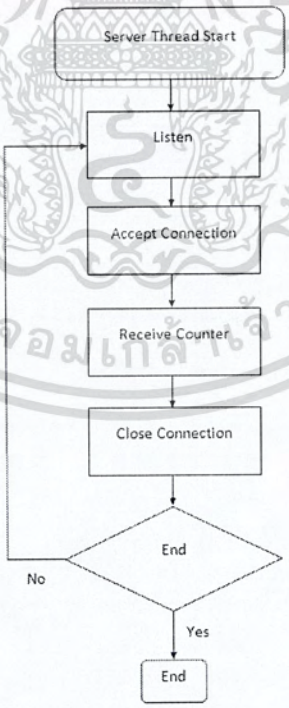
รูป 4.22 ผังการทำงานของโปรแกรมหลัก

1.2) ผังการทำงานของส่วนการตรวจตราระบบ เมื่อเธรดของการตรวจตราเริ่มทำงาน จะทำการไปอ่านค่าข้อมูลระบบบนอุปกรณ์เครือข่ายโดยใช้โปรโตคอลเอสเอ็นเอ็มพี



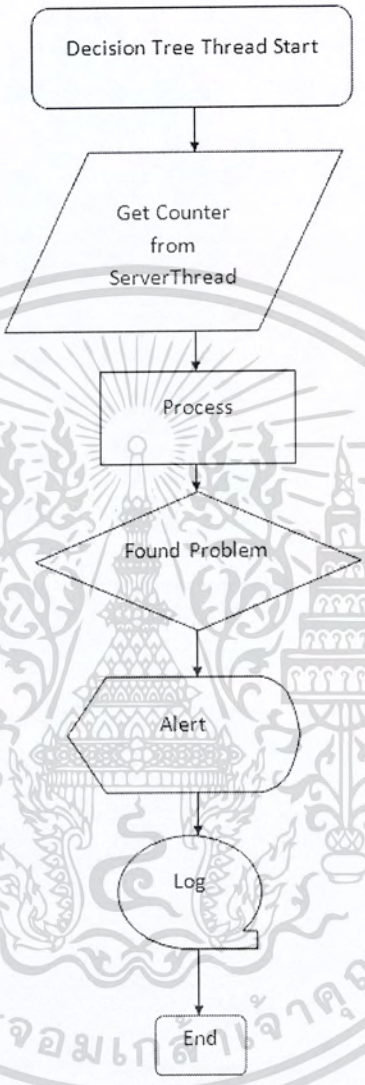
รูป 4.23 ผังการทำงานของส่วนการมอนิเตอริ่ง

1.3) ผังการทำงานส่วนการรับข้อมูลจากเอเจนต์ เมื่อเธรดของเซิร์ฟเวอร์เริ่มทำงาน ก็จะทำการรอรับการเชื่อมต่อจากโปรแกรมเอเจนต์ ซึ่งจะกว่าจะได้รับ เมื่อได้รับแล้วก็จะตอบรับการเชื่อมต่อ หลังจากนั้นก็จะทำการอ่านตัวนับที่โปรแกรมเอเจนต์ส่งมาให้ จากนั้นก็จะปิดการเชื่อมต่อ



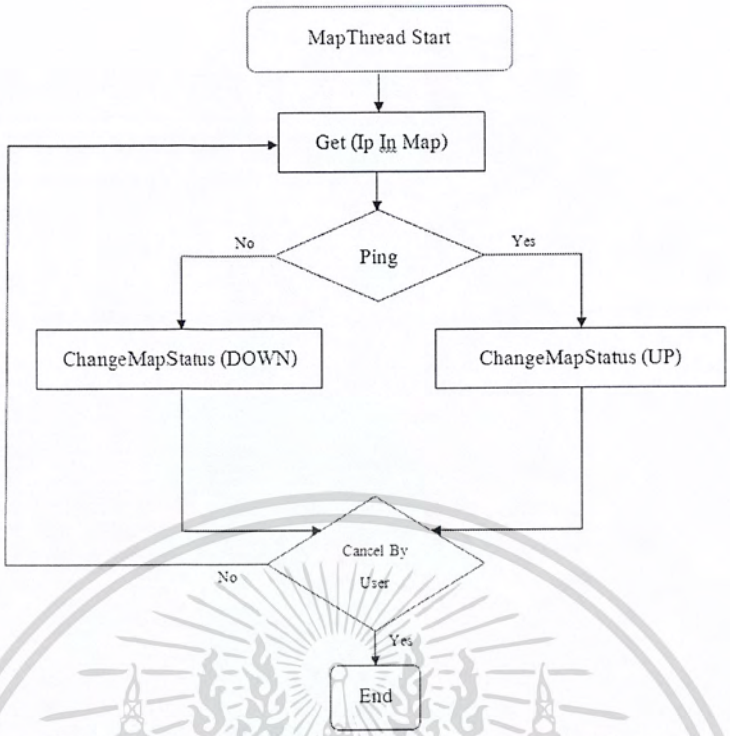
รูป 4.24 ผังการทำงานของส่วนการรับข้อมูลจากเอเจนต์

1.4) ผังการทำงานของส่วนการวิเคราะห์ เมื่อเธรดของการวิเคราะห์เริ่มต้นจะไปอ่านค่าตัวนับ (Counter) มาจากเธรดของเซิร์ฟเวอร์ แล้วจะนำค่ามาใช้กับแบบวิเคราะห์ซึ่งหากเกิดปัญหาขึ้นจะทำการแจ้งเตือนและบันทึกค่าไว้



รูป 4.25 ผังการทำงานของส่วนการวิเคราะห์

1.5) ผังการทำงานของส่วนโครงสร้างระบบเครือข่าย เมื่อเธรดของโครงสร้างระบบเครือข่ายเริ่มต้น จะไปดึงค่าไอพีแอดเดรสจากโครงสร้างระบบเครือข่ายที่ผู้ใช้สร้างไว้จากนั้นจะทำการตรวจสอบโดยการปิง หากทำการปิงประสบความสำเร็จ จะเปลี่ยนสถานะของไอพีแอดเดรสนั้นเป็นใช้งานได้ (UP) แต่หากไม่ประสบความสำเร็จจะเปลี่ยนสถานะของไอพีแอดเดรสเป็นใช้งานไม่ได้ (DOWN)



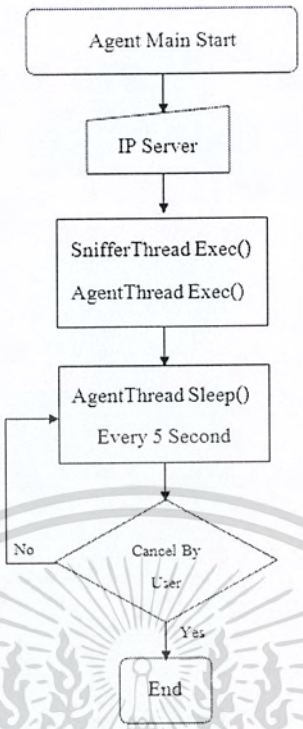
รูป 4.26 ผังการทำงานของส่วนโครงสร้างระบบเครือข่าย

2) ผังการทำงานของโปรแกรมเอเจนต์

จะประกอบด้วยส่วนการทำงานของเอเจนต์หลัก (Main Agent) ส่วนการดักจับแพคเก็ต (Packet Sniffer) และส่วนการเก็บข้อมูลและติดต่อเซิร์ฟเวอร์

2.1) ผังการทำงานส่วนการทำงานของเอเจนต์หลัก (Main Agent)

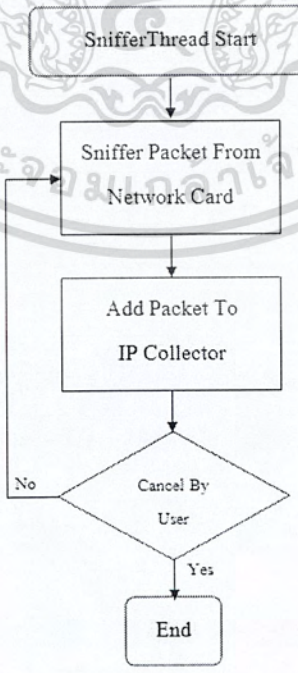
จะรับไอพีแอดเดรสของเซิร์ฟเวอร์จากผู้ใช้งาน จากนั้นจะเริ่มเธรดของการดักจับและเธรดของเอเจนต์ ซึ่งเธรดของเอเจนต์จะพักการทำงานทุกๆ 5 วินาที



รูป 4.27 ผังการทำงานของส่วนการทำงานของเอนเจนต์หลัก (Main Agent)

2.2) ผังการทำงานส่วนการดักจับแพคเก็ต (Packet Sniffer)

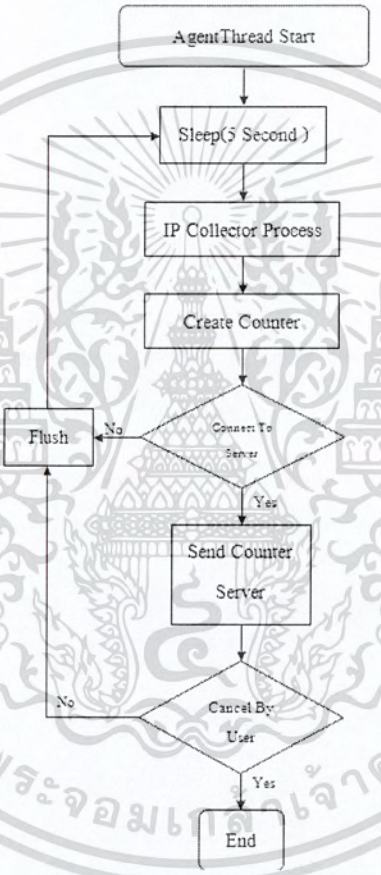
เริ่มดักจับแพคเก็ตจากการ์ดเครือข่ายซึ่งจะนำแพคเก็ตที่ดักจับได้ เก็บไว้ในไอพีคอลเลคเตอร์



รูป 4.28 ผังการทำงานส่วนการดักจับแพคเก็ต

2.3) ผังการทำงานส่วนเก็บข้อมูลและติดต่อเซิร์ฟเวอร์

เริ่มจากพักการทำงานของเธรด 5 วินาที และจะนำข้อมูลจากไอพีคอลเลคเตอร์มาทำสถิติ แล้วนำมาสร้างตัวนับ เชื่อมต่อไปยังเซิร์ฟเวอร์ ถ้าทำไม่ได้จะทำการลบค่าในไอพีคอลเลคอเตอร์และตัวนับทิ้ง แต่ถ้าเชื่อมต่อได้ ก็จะทำการร้องขอการเชื่อมต่อไปยังเซิร์ฟเวอร์ ถ้าเซิร์ฟเวอร์ตอบรับ จะทำส่งข้อมูลไปให้เซิร์ฟเวอร์ จากนั้นทำการเคลียร์ค่าในไอพีคอลเลคเตอร์และตัวนับทิ้ง ถ้าไม่เคลียร์จะเกิดปัญหาหน่วยความจำไม่เพียงพอต่อการใช้งาน (out of memory)



รูป 4.29 ผังการทำงานส่วนการติดต่อเซิร์ฟเวอร์

บทที่ 5
การทดสอบและผลลัพธ์จากการพัฒนาโปรแกรม

เป้าหมายหลักในการบริหารจัดการเครือข่ายคอมพิวเตอร์ขององค์กรที่มีระบบเครือข่ายเป็นของตนเอง คือการที่เครือข่ายสามารถให้บริการอย่างมีประสิทธิภาพและเกิดประสิทธิผลสูงสุด หรืออีกนัยหนึ่งคือการพยายามลดจำนวนปัญหาที่ขัดข้องของการให้บริการเครือข่ายเกิดขึ้นน้อยที่สุด ในกรณีทั่วไปเหตุการณ์ที่เกิดในระบบสามารถแบ่งได้เป็นสองประเภทคือ ความผิดปกติแบบธรรมดาซึ่งอาจเกิดจากอุปกรณ์ และการบริการหยุดการทำงานหรือทำงานผิดปกติ และเป็นความผิดปกติด้านความปลอดภัยอันเนื่องมาจากการกระทำอันไม่พึงประสงค์ในเครือข่ายหรือจากการบุกรุก จากความผิดปกติทั้งสองประเภทนี้ ระบบจำเป็นต้องมีกระบวนการสำหรับตรวจจับที่รวดเร็วและแม่นยำเพื่อป้องกันไม่ให้เกิดความเสียหายหรือลดความเสียหายให้น้อยที่สุดเท่าที่จะเป็นไปได้

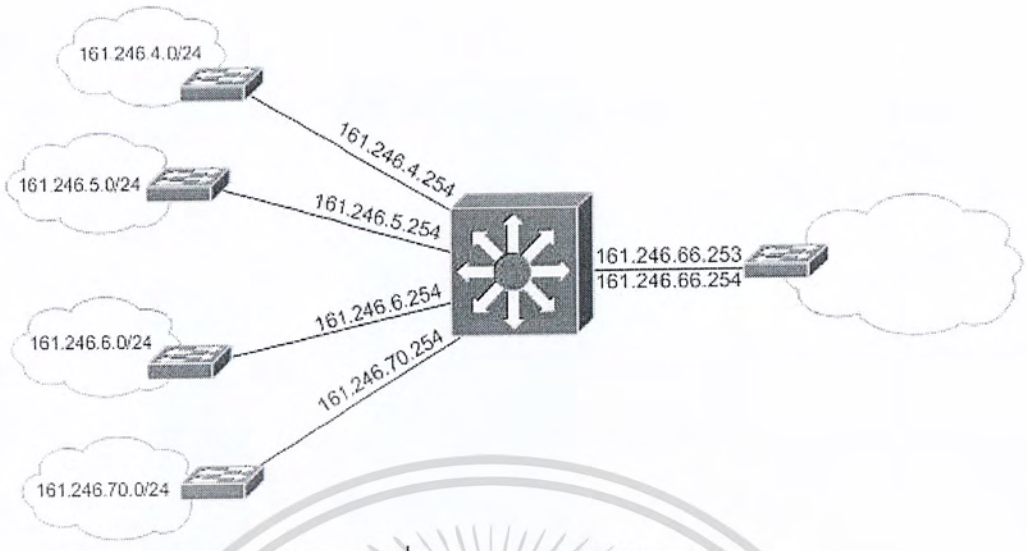
ในส่วนของบทนี้จะเป็นเนื้อหาที่เกี่ยวกับกับวิธีการต่างๆในการทำงานของโปรแกรม ตั้งแต่การตั้งค่าระบบเริ่มต้น การเก็บข้อมูลจากแหล่งที่มาต่างๆ (เอสเอ็นเอ็มพี และ ตัวดักจับแพคเก็ต) การตรวจสอบกฎที่ทำการสร้างขึ้นโดยใช้แบบการวิเคราะห์รูปแบบต้นไม้ตัดสินใจ การแจ้งเตือนในรูปแบบต่างๆ การออกรายงานแสดงผลการวิเคราะห์ รวมถึงผลลัพธ์ต่างๆ ที่ได้จากการพัฒนาโปรแกรมด้วย

5.1 วิธีการตั้งค่าเพื่อเริ่มใช้งานโปรแกรม

การตั้งค่าเพื่อเริ่มใช้งานถือเป็นส่วนแรกของโปรแกรมที่ผู้ใช้จะต้องทำการตั้งค่ารายละเอียดต่างๆ เกี่ยวกับระบบ ไม่ว่าจะเป็น ส่วนของโครงสร้างระบบเครือข่าย (Map Topology) กฎต่างๆในแบบการวิเคราะห์รูปแบบต้นไม้ตัดสินใจ (Decision Tree Analysis Model) ส่วนของการตรวจตราปริมาณต่างๆในระบบเครือข่าย (Monitoring) ซึ่งทางผู้จัดทำได้ทำการทดสอบดังต่อไปนี้

5.1.1 การตั้งค่าโครงสร้างของระบบเครือข่าย(Map Topology Configuration)

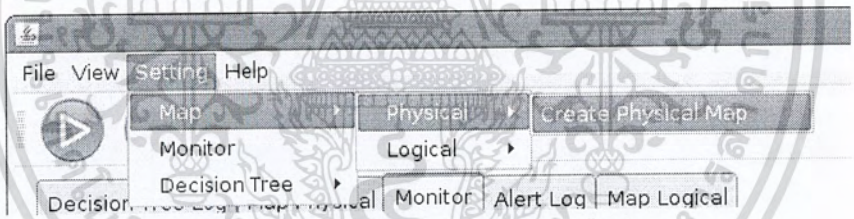
ทางผู้จัดทำได้ทำการตั้งค่าโครงสร้างของระบบโดยใช้การตั้งค่าในลักษณะเดียวกับโครงสร้างเครือข่ายของสาขาวิชา เพื่อช่วยในการอ้างอิงภาพโดยรวมของระบบเครือข่าย ดังรูป 5.1



รูป 5.1 การเชื่อมต่อภายในเครือข่ายสาขาวิชา

ซึ่งผู้ใช้จะตั้งค่าดังนี้

1) เปิดโปรแกรมวิเคราะห์เครือข่ายอัตโนมัติ จากนั้นไปที่ Setting เลือกที่ Map เลือกที่ Physical เลือกที่ Create Physical Map



รูป 5.2 การสร้างโครงสร้างระบบเครือข่าย

2) เมื่อกดแล้วจะได้หน้าต่างตั้งค่าขึ้นมาให้ทำการตั้งค่า ซึ่งผู้ใช้สามารถตั้งชื่ออุปกรณ์ กรอกไอพีแอดเดรส เลือกประเภทอุปกรณ์ เลือกอินเตอร์เฟสการเชื่อมต่อ จากนั้นทำการบันทึก ซึ่งตัวอย่างจะเป็นไปตามรายละเอียดในตาราง 5.1

ตาราง 5.1 รายชื่ออุปกรณ์ในโครงสร้างระบบเครือข่าย

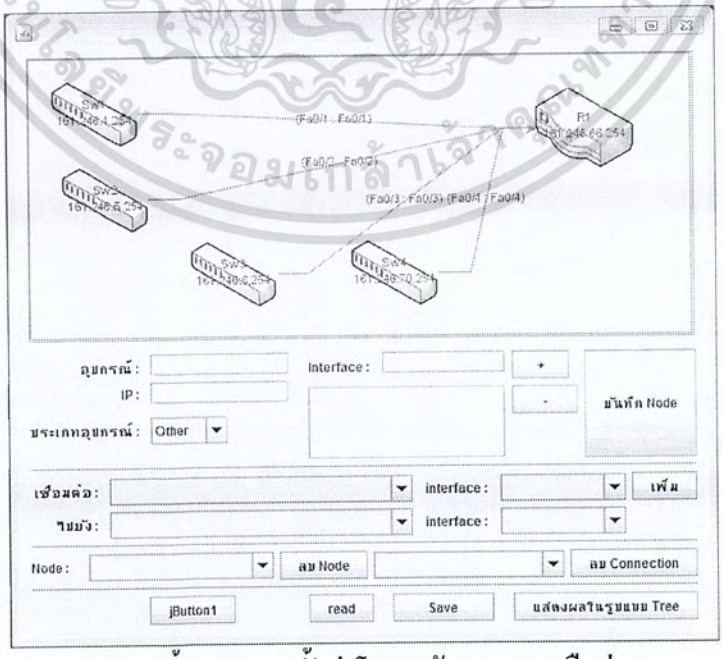
ชื่ออุปกรณ์	ไอพีแอดเดรส	ประเภทอุปกรณ์	อินเตอร์เฟส
R1	161.246.66.254	เราเตอร์	Fa0/1,Fa0/2,Fa0/3,Fa0/4
Sw1	161.246.4.254	สวิตซ์	Fa0/1
Sw2	161.246.5.254	สวิตซ์	Fa0/2
Sw3	161.246.6.254	สวิตซ์	Fa0/3
Sw4	161.246.70.254	สวิตซ์	Fa0/4

ส่วนการเชื่อมต่อจะทำการเชื่อมต่อตามตาราง 5.2

ตาราง 5.2 การเชื่อมต่อของอุปกรณ์ในโครงสร้างระบบเครือข่าย

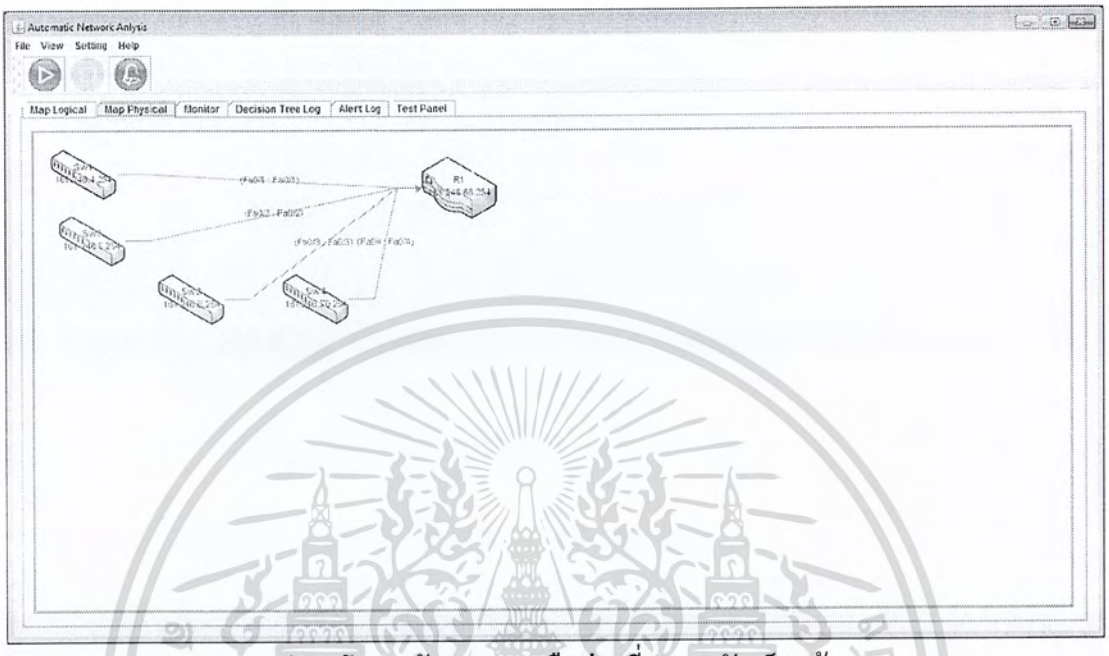
จุดเชื่อมต่อ	จากอุปกรณ์ชื่อ	อินเตอร์เฟส	ไปยังอุปกรณ์ชื่อ	อินเตอร์เฟส
1	Sw1	Fa0/1	R1	Fa0/1
2	Sw2	Fa0/2	R1	Fa0/2
3	Sw3	Fa0/3	R1	Fa0/3
4	Sw4	Fa0/4	R1	Fa0/4

ซึ่งจะได้ออกมาเป็นลักษณะนี้



รูป 5.3 ขั้นตอนการตั้งค่าโครงสร้างระบบเครือข่าย

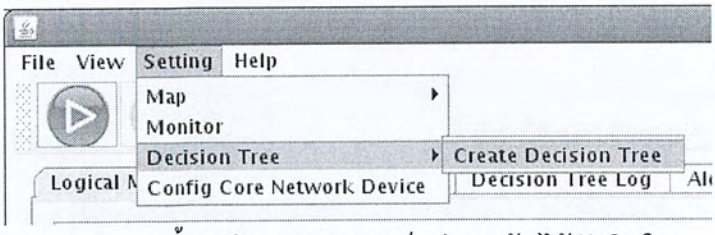
เมื่อทำการจัดเก็บโครงสร้างของระบบเครือข่ายแล้ว โปรแกรมจะทำการแสดงโครงสร้างระบบเครือข่ายที่ได้ทำการจัดเก็บออกมาแสดงบริเวณหน้าหลักของโปรแกรมดังรูป 5.4



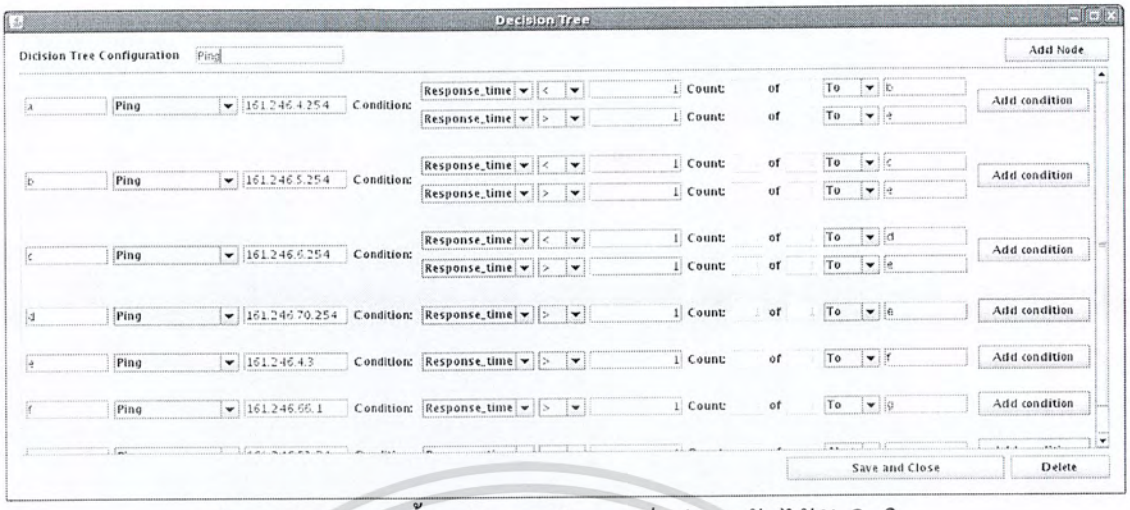
รูป 5.4 โครงสร้างระบบเครือข่ายที่ทำการจัดเก็บแล้ว

5.1.2 การตั้งกฎในแบบการวิเคราะห์รูปแบบต้นไม้ตัดสินใจ (Decision tree Analysis Model Configuration)

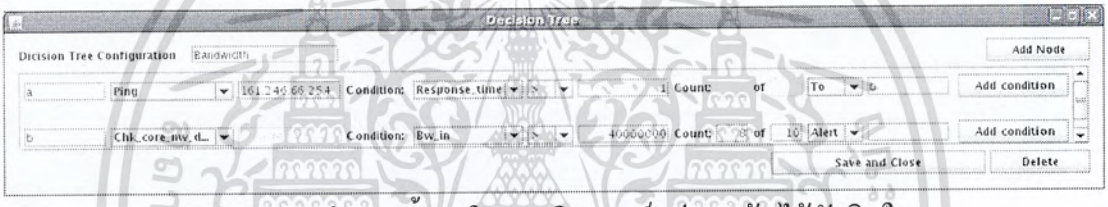
การตั้งกฎในแบบวิเคราะห์รูปแบบต้นไม้ตัดสินใจสามารถตั้งได้หลากหลายรูปแบบ ในขอบเขตของตัวแปรและข้อมูลที่มีในโปรแกรม เช่น การตั้งกฎเพื่อจะตรวจสอบการเชื่อมต่อกับเกตเวย์หรืออุปกรณ์ต่างๆ, การตั้งกฎเพื่อจะตรวจสอบการใช้งานแบนวิดท์ที่สูงเกินผิดปกติ, การตั้งกฎเพื่อจะตรวจสอบการใช้งานแพคเก็ตที่สูงเกินผิดปกติ เป็นต้น โดยที่ผู้ใช้สามารถที่จะตั้งขอบเขตการตรวจสอบได้โดยใช้ค่านับ (Count) ซึ่งมีไว้สำหรับกำหนดระดับการเปลี่ยนขั้นตอนได้ ดังรูป 5.6



รูป 5.5 การตั้งกฎในแบบวิเคราะห์รูปแบบต้นไม้ตัดสินใจ



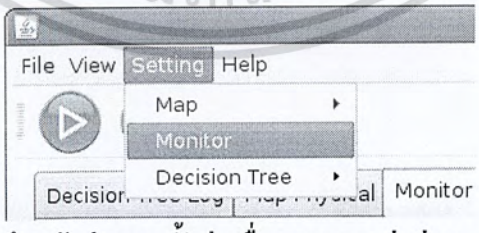
รูป 5.6 ตัวอย่างการตั้งกฎในแบบวิเคราะห์รูปแบบต้นไม้ตัดสินใจ เพื่อจะตรวจสอบการเชื่อมต่อกับเกตเวย์



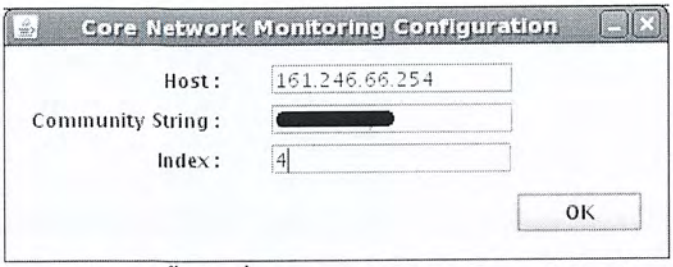
รูป 5.7 ตัวอย่างการตั้งกฎในแบบวิเคราะห์รูปแบบต้นไม้ตัดสินใจ เพื่อจะตรวจสอบการใช้งานแบนวิดท์ที่สูงเกินผิดปกติ

5.1.3 การตั้งค่าเพื่อตรวจตราค่าต่างๆจากคอร์สวิตซ์ (Monitoring Configuration)

การตั้งค่าเพื่อตรวจตราค่าต่างๆจากคอร์สวิตซ์นั้น สามารถกระทำได้โดยที่ผู้ใช้จะต้องทำการกรอกค่าต่างๆที่จำเป็นในการทำงานดังนี้



รูป 5.8 การเข้าถึงหน้าต่างการตั้งค่าเพื่อตรวจตราค่าต่างๆ จากคอร์สวิตซ์



รูป 5.9 การตั้งค่าเพื่อตรวจตราค่าต่างๆจากคอร์สวิตซ์

5.2 การทดสอบโปรแกรม

ผู้ใช้ได้ทดสอบโดยการตั้งกฎในแบบวิเคราะห์รูปแบบต้นไม้ตัดสินใจมาทั้งหมด 2 รูปแบบ ได้แก่ การตรวจสอบเวลาตอบสนองในการเชื่อมต่อของเกตเวย์ต่างๆที่อยู่ในระบบเครือข่าย และการตรวจสอบการใช้แบนด์วิดท์ผิดปกติหรือเกินขอบเขต ซึ่งได้มีการทดสอบดังนี้

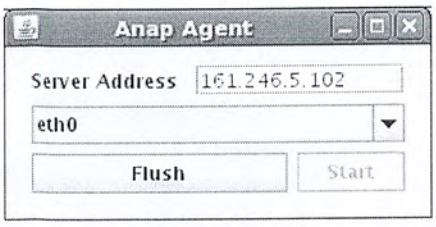
5.2.1 การเก็บข้อมูลจากคอร์สวิตซ์ของระบบผ่านเอสเอ็นเอ็มพี

เมื่อโปรแกรมหลักเริ่มทำงาน ตัวโปรแกรมจะร้องขอข้อมูลเอสเอ็นเอ็มพีจากคอร์สวิตซ์ ซึ่งข้อมูลนี้จะนำมาใช้ 2 จุดประสงค์คือ เพื่อตรวจตราปริมาณแบนด์วิดท์และปริมาณแพคเก็ตที่มีการใช้งานภายในเครือข่าย และ นำข้อมูลที่ได้มาวิเคราะห์ในแบบวิเคราะห์รูปแบบต้นไม้ตัดสินใจ ซึ่งจะได้ผลในลักษณะดังนี้

1) กรณีเวลาตอบสนองการเชื่อมต่อไปยังเกตเวย์ต่างๆ ในกฎที่ทำการทดสอบตั้งขอบเขตเวลาตอบสนองไว้ที่ 0.8 มิลลิวินาที ซึ่งเมื่อเวลาตอบสนองนั้นเกิน 0.8 มิลลิวินาทีโปรแกรมจะทำการตรวจสอบในลำดับขั้นต่อไป จนถึงลำดับสุดท้าย และจะทำการแจ้งเตือนมายังหน้าจอของโปรแกรม พร้อมทั้งแสดงบันทึกการแจ้งเตือนและบันทึกการใช้งานแบบวิเคราะห์รูปแบบต้นไม้ตัดสินใจ
2) กรณีการใช้งานแบนด์วิดท์ผิดปกติหรือมากกว่าขอบเขตที่ตั้งไว้ ในกฎที่ทำการทดสอบ ได้ตั้งขอบเขตของปริมาณแบนวิดท์รวมจะต้องไม่เกิน 20 เมกะบิตต่อวินาที ซึ่งเมื่อการใช้งานแบนด์วิดท์มากเกินกว่าขอบเขต โปรแกรมจะทำการแจ้งเตือนพร้อมทั้งแสดงบันทึกแจ้งเตือนและบันทึกการวิเคราะห์ผ่านทางหน้าโปรแกรม

5.2.2 การเก็บข้อมูลจากเอเจนต์ในระบบ

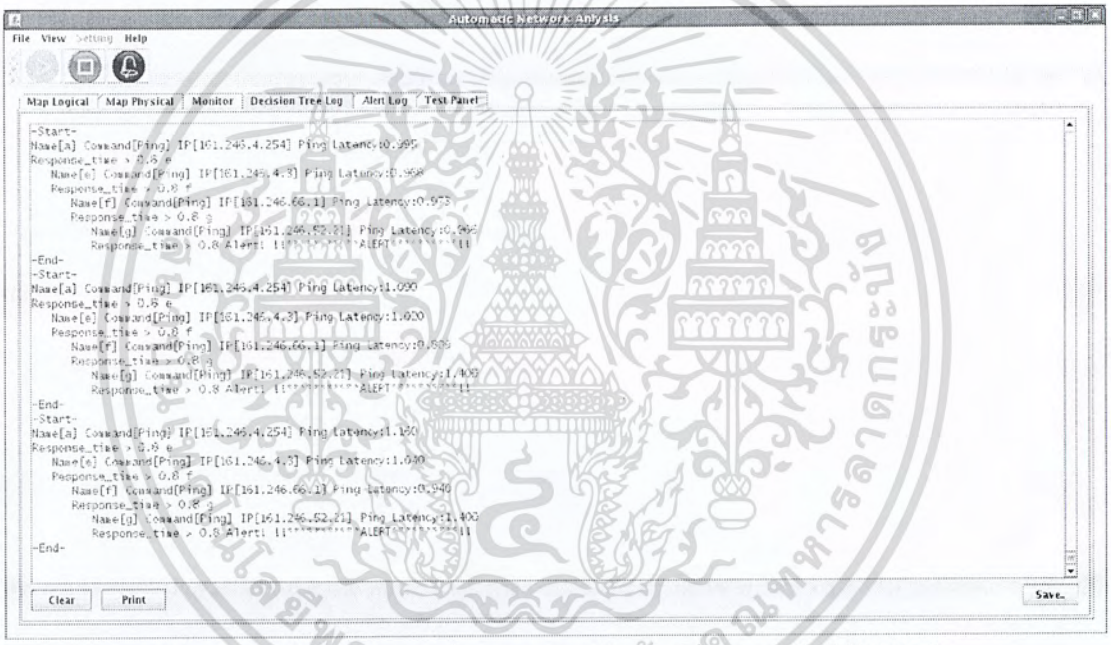
เมื่อโปรแกรมหลักเริ่มทำงาน เอเจนต์จะทำหน้าที่เป็นตัวดักจับแพคเก็ตเพื่อนำมาใช้ในการวิเคราะห์ซึ่งจะรันเป็นเบื้องหลังคอยดักจับแพคเก็ตและส่งมายังเซิร์ฟเวอร์ เพื่อทำการวิเคราะห์ต่อไป



รูป 5.10 เอเจนต์

5.2.3 การตรวจสอบกฎบนแบบการวิเคราะห์รูปแบบต้นไม้ตัดสินใจ

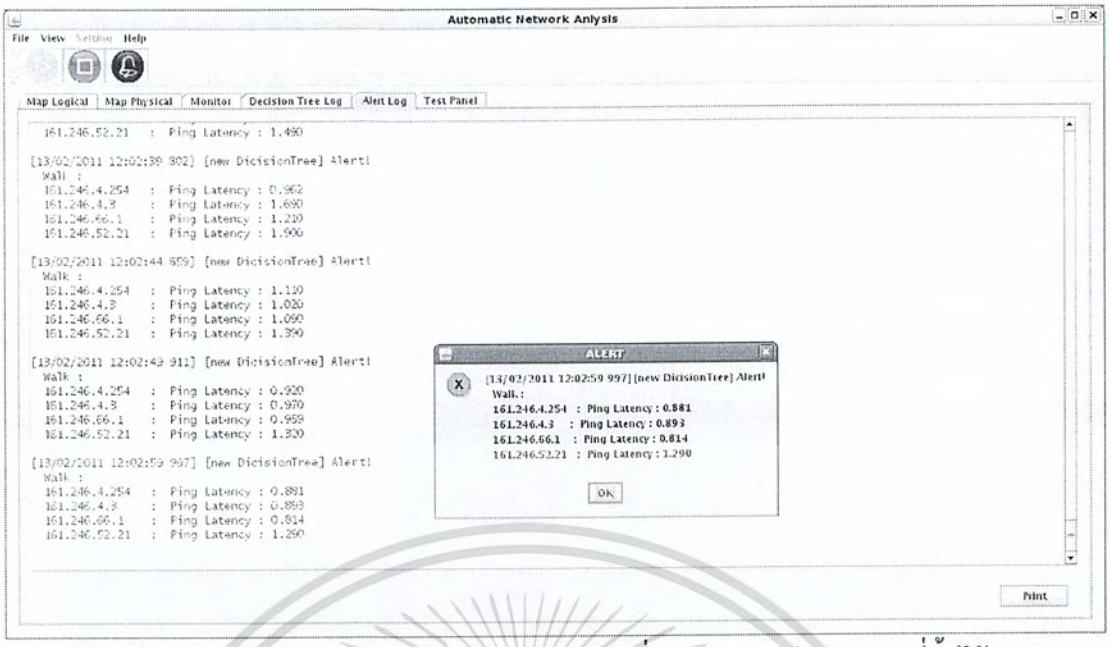
จากการทดสอบทั้ง 2 กรณีได้แก่ การทดสอบเวลาตอบสนองการเชื่อมต่อกับเกตเวย์ของเครือข่าย และการใช้งานแบนด์วิดท์ผิดปกติหรือเกินขอบเขต เห็นได้ว่ากฎบนแบบการวิเคราะห์รูปแบบต้นไม้ตัดสินใจสามารถทำงานได้อย่างถูกต้องและพร้อมกันหลายๆกฎ



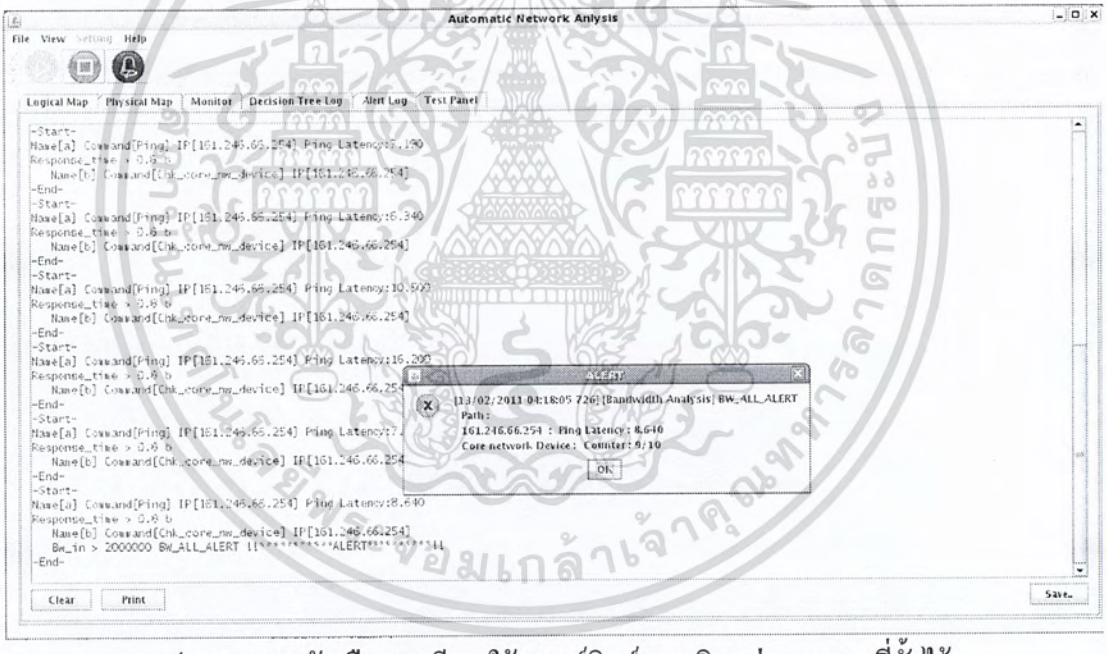
รูป 5.11 บันทึกการวิเคราะห์ของแบบการวิเคราะห์รูปแบบต้นไม้ตัดสินใจ

5.2.4 การแจ้งเตือนเมื่อเกิดความผิดปกติในระบบเครือข่าย

จากการทดสอบจากกรณีทั้ง 2 กรณีพบว่า โปรแกรมสามารถทำการแจ้งเตือนได้ถูกต้องตามกฎที่ได้วางไว้ ซึ่งจะทำการแจ้งเตือน ทั้งแบบเป็นหน้าต่างแจ้งเตือน และสัญญาณไฟกระพริบเพื่อแจ้งให้ผู้ใช้ตรวจสอบและทำการแก้ไขปัญหาต่อไป



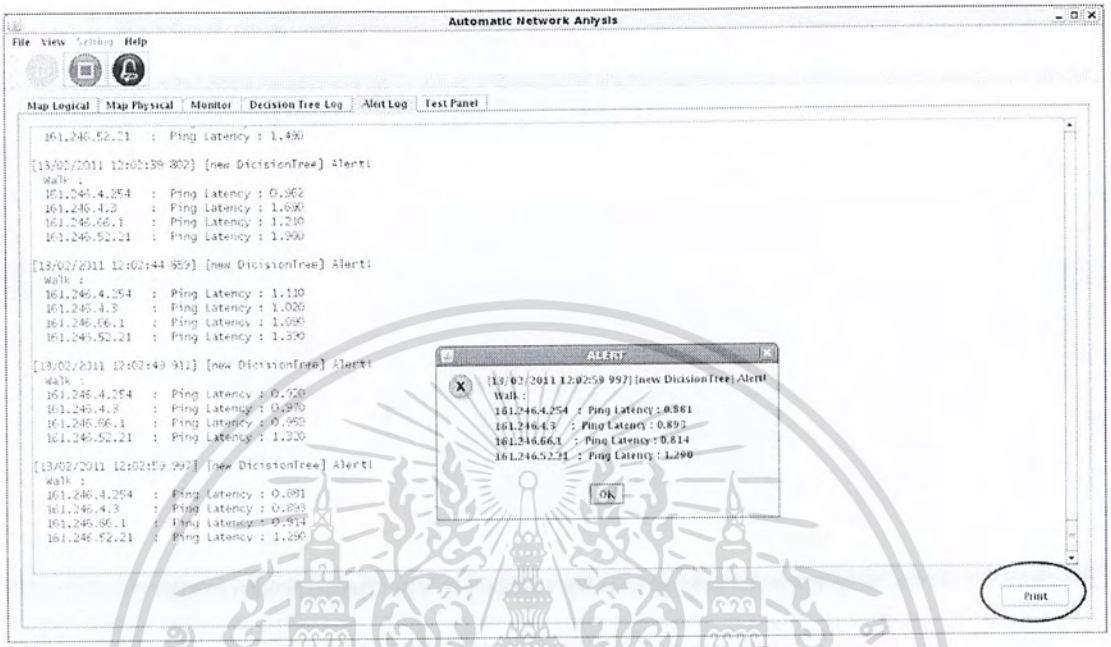
รูป 5.12 การแจ้งเตือนกรณีเวลาตอบสนองการเชื่อมต่อมากกว่าขอบเขตที่ตั้งไว้



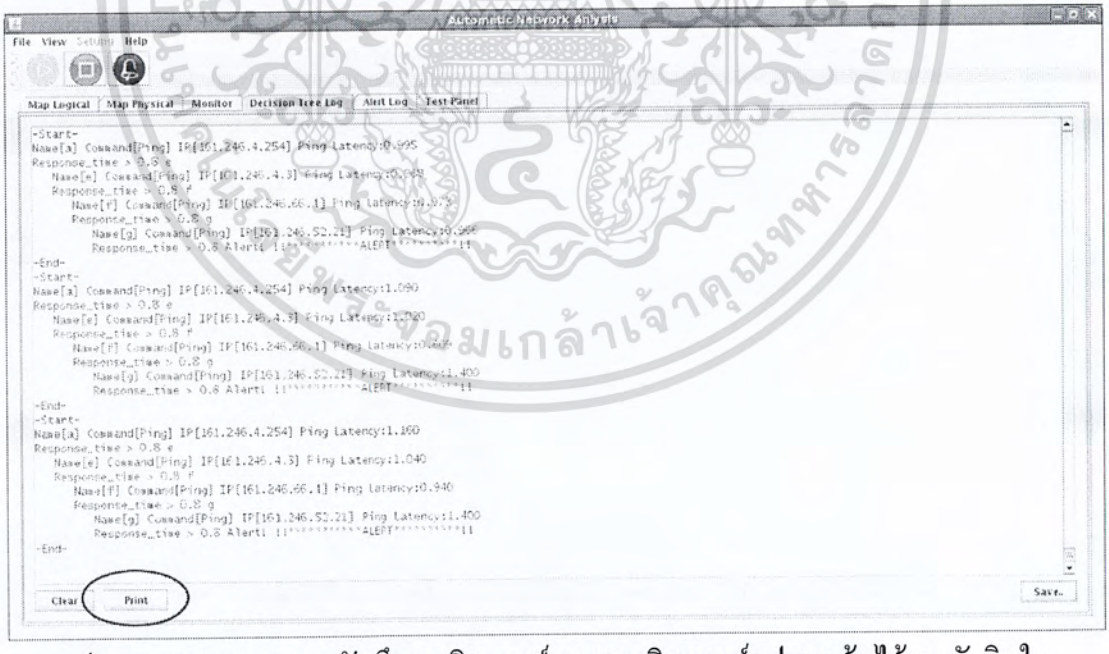
รูป 5.13 การแจ้งเตือนกรณีการใช้แบนด์วิดท์มากเกินกว่าขอบเขตที่ตั้งไว้

5.2.5 การออกรายงาน

โปรแกรมสามารถออกรายงานในรูปแบบเอกสาร เพื่อให้สามารถนำไปใช้ในการอ้างอิงในรายงานต่างๆต่อไปได้



รูป 5.14 การออกรายงานบันทึกการแจ้งเตือน



รูป 5.15 การออกรายงานบันทึกการวิเคราะห์จากแบบวิเคราะห์รูปแบบต้นไม้การตัดสินใจ

บทที่ 6
บทสรุป

6.1 สรุป

จากการทดสอบโปรแกรม สามารถสรุปได้ว่า โปรแกรมสามารถที่จะทำการวิเคราะห์ปัญหาโดยอ้างอิงกฎบนแบบวิเคราะห์รูปแบบต้นไม้ตัดสินใจได้ แล้วสามารถแจ้งเตือนปัญหาที่เกิดขึ้นได้อย่างรวดเร็ว พร้อมทั้งสามารถที่จะบันทึกการแจ้งเตือนหรือการวิเคราะห์ต่างๆ เพื่อนำมาออกรายงานเพื่อใช้ในการอ้างอิงในรายงานต่อไปได้

6.2 ปัญหาและอุปสรรค

1) ผู้พัฒนายังขาดความรู้และประสบการณ์ในการบริหารจัดการเครือข่าย ทำให้การออกแบบโมเดลการวิเคราะห์ระบบอาจมีประสิทธิภาพที่ไม่ดีในการวิเคราะห์หาสาเหตุของปัญหา
2) ข้อมูลดิบจากระบบได้มาโดยการใช้เอสเอ็มเอ็นพี จึงไม่สามารถอ่านข้อมูลในระดับเฮดเดอร์ของแพคเก็ตได้ ทำให้ข้อมูลที่ได้มาอาจไม่เพียงพอต่อการวิเคราะห์สาเหตุของในบางปัญหา
3) ข้อมูลที่โปรแกรมใช้ในการวิเคราะห์เป็นค่าเฉลี่ยของข้อมูลดิบที่ได้จากระบบ ซึ่งการนำค่าเฉลี่ยมาใช้ในการวิเคราะห์ปัญหาอาจทำให้โปรแกรมเกิดความคลาดเคลื่อนในการวิเคราะห์ปัญหาได้
4) การออกแบบโปรแกรมให้ส่วนต่างๆของโปรแกรมมีความยืดหยุ่นเพื่อให้ครอบคุมกับการใช้งานในระบบต่างๆ ได้ทำให้การเขียนโค้ดของโปรแกรมมีความซับซ้อนมากขึ้น เป็นผลให้โปร โปรแกรมเกิดความผิดพลาดในการวิเคราะห์ปัญหา

6.3 แนวทางการแก้ไข

1) ขอคำปรึกษาจากผู้มีประสบการณ์ในการบริหารจัดการเครือข่ายในเรื่องการออกแบบโมเดลการวิเคราะห์ปัญหา
2) เพิ่มฟังก์ชันการทำงานแบบดักจับแพคเก็ต เพื่อใช้ในการอ่านข้อมูลระดับเฮดเดอร์ของแพคเก็ต ทำให้โปรแกรมมีความถูกต้องในการวิเคราะห์ปัญหามากขึ้น
3) หาค่าเฉลี่ยในเวลาที่นานขึ้น เพื่อให้ค่าเฉลี่ยมีค่าใกล้เคียงกับข้อมูลการใช้งานจริงในระบบ
4) ขอคำปรึกษาจากผู้มีประสบการณ์ในการเขียนโค้ดโปรแกรม โดยขอคำแนะนำในการเขียนโค้ดโปรแกรม การออกแบบอัลกอริทึมการทำงานของโปรแกรม เพื่อให้โปรแกรมทำงานโดยใช้ทรัพยากรของระบบให้มีประสิทธิภาพมากที่สุด

6.4 แนวทางการพัฒนาต่อ

1) พัฒนาความสามารถในการค้นหาโครงสร้างของระบบเครือข่ายได้อย่างอัตโนมัติ
2) เพิ่มขีดความสามารถของเซิร์ฟเวอร์ให้สามารถรองรับกฎได้มากขึ้นโดยที่ไม่ทำให้โปรแกรมเกิดปัญหา
3) เพิ่มความสามารถในรองรับการตรวจสอบในระดับแอฟพลิเคชั่นให้มากขึ้นโดยที่ไม่ทำให้โปรแกรมเกิดปัญหา

บรรณานุกรม

เสถียรพงศ์ อิงครัตน์, เสาวลักษณ์ ตะเคียนงาม, อุดม จิระดำเกิง. 2552. "ระบบตรวจจับสิ่งผิดปกติในเครือข่าย TCP/IP." ปริญญาวิศวกรรมศาสตรบัณฑิต ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

สุรศักดิ์ สงวนพงษ์. 2545. **สถาปัตยกรรมและโปรโตคอลทีซีพี/ไอพี.** พิมพ์ครั้งที่ 2. กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

สาขาวิชาวิศวกรรมคอมพิวเตอร์ สจล. **Multi Router Traffic Grapher**. [Online]. Available : http://www.ce.kmitl.ac.th/download.php?DOWNLOAD_ID=76&database=pj_download.

ธัญญารักษ์ เอี่ยมศรี,พาริณี แสนไชยสุริยา. 2551. **SNMP และ RMON**. ขอนแก่น : คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น. [Online]. Available : http://202.28.94.55/web/322461/2550/report/g14/file/SNMP%26RMON.pdf.

North American Network Operators' Group. 2010. RRDtool. [Online]. Available : http://www.nanog.org/meetings/nanog17/presentations/rrd-slides.pdf.

Cisco Systems, Inc. 2010. **SNMP Object Navigator**. [Online]. Available : http://tools.cisco.com/Support/SNMP/do/BrowseOID.do.

Wikipedia. 2010. **Decision Tree**. [Online]. Available : http://en.wikipedia.org/wiki/Decision_tree.

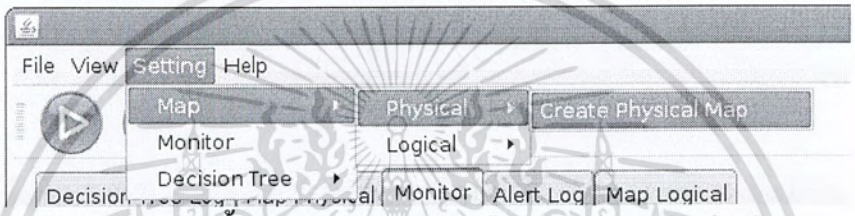
ภาคผนวก ก

คู่มือการตั้งค่าเพื่อใช้งานโปรแกรม

ก.1 การตั้งค่าโครงสร้างระบบเครือข่าย

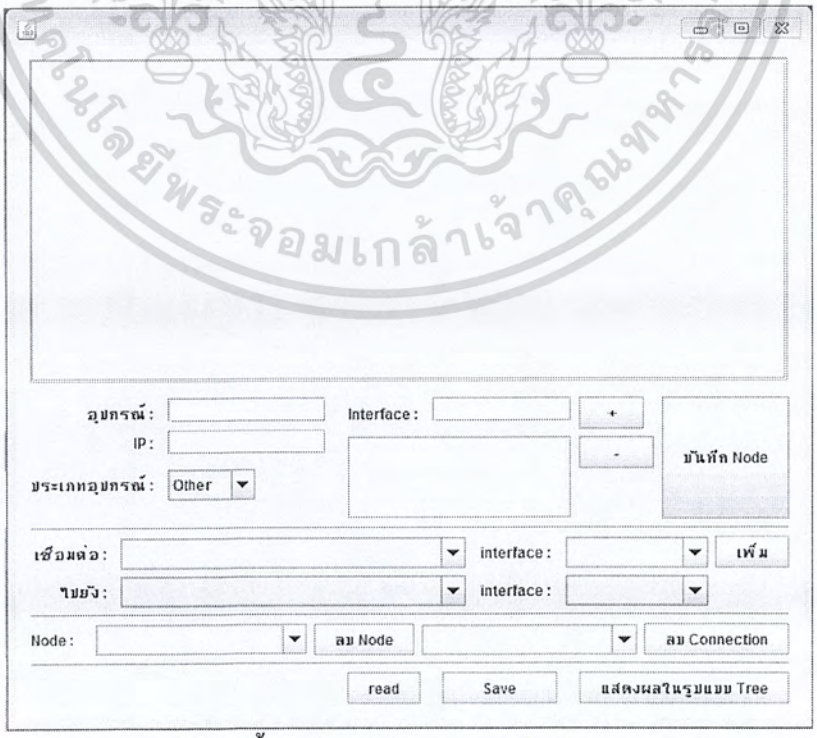
ก.1.1 การตั้งค่าโครงสร้างระบบเครือข่ายทางกายภาพ

ทำการเลื่อนเมาส์ไปชี้ที่ Setting และทำการคลิ๊ก จากนั้นชี้ที่ Map จะมีแถบขึ้นมาให้เลือก 2 แถบได้แก่ Physical และ logical ให้ชี้ที่ Physical จากนั้นคลิ๊กที่ Create Physical Map



รูป ก.1 การตั้งค่าโครงสร้างระบบเครือข่ายแบบกายภาพใหม่

จากนั้นจะได้หน้าต่างตั้งค่าโครงสร้างระบบเครือข่ายทางกายภาพขึ้นมา ซึ่งมีรายละเอียดดังนี้

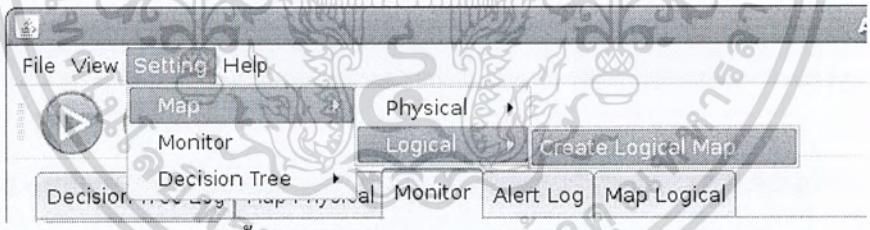


รูป ก.2 หน้าต่างตั้งค่าโครงสร้างระบบเครือข่ายแบบกายภาพ

1) อุปกรณ์ : สำหรับใส่ชื่ออุปกรณ์
2) IP : สำหรับใส่ไอพีแอดเดรสของอุปกรณ์
3) ประเภทอุปกรณ์ : สำหรับเลือกประเภทอุปกรณ์ ได้แก่ สวิตซ์ เราเตอร์ เซิร์ฟเวอร์ ไฟร์วอลล์ ฮับ อื่นๆ
4) Interface : สำหรับกรอกอินเตอร์เฟสที่ต้องการ
5) บันทึก Node : สำหรับบันทึกอุปกรณ์
6) เชื่อมต่อ : สำหรับเลือกอุปกรณ์ที่ต้องการเชื่อมต่อ (ระบุอินเตอร์เฟส)
7) ไปยัง : สำหรับเลือกอุปกรณ์ที่ต้องการให้อุปกรณ์ในข้อ 6) เชื่อมต่อไป (ระบุอินเตอร์เฟส)
8) เพิ่ม : เพิ่มการเชื่อมต่อดังกล่าว
9) Node : เลือกอุปกรณ์ที่ต้องการจะลบ
10) ลบ Node : ลบ Node ที่ต้องการออก
11) ลบ Connection : ลบ Connection ที่ต้องการออก

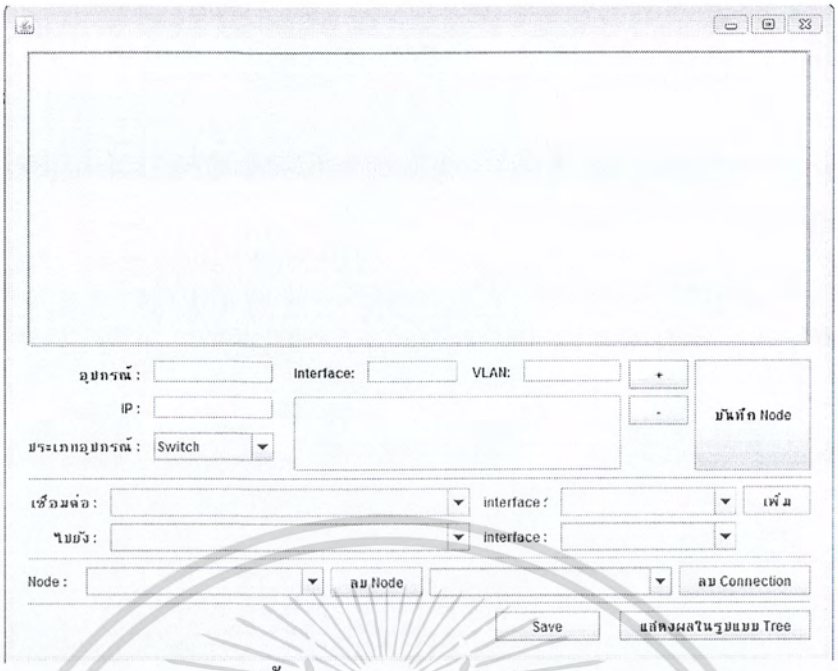
ก.1.2 การตั้งค่าโครงสร้างระบบเครือข่ายทางตรรกะ

ทำการเลื่อนเมาส์ไปชี้ที่ Setting และทำการคลิ๊ก จากนั้นชี้ที่ Map จะมีแถบขึ้นมาให้เลือก 2 แถบได้แก่ Physical และ logical ให้ชี้ที่ Logical จากนั้นคลิ๊กที่ Create Logical Map



รูป ก.3 การตั้งค่าโครงสร้างระบบเครือข่ายแบบตรรกะใหม่

จากนั้นจะได้หน้าต่างตั้งค่าโครงสร้างระบบเครือข่ายทางตรรกะขึ้นมา ซึ่งมีรายละเอียดดังนี้

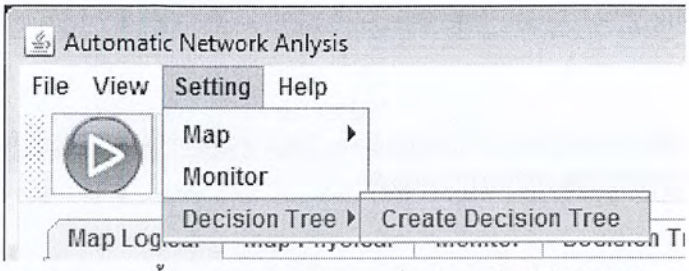


รูป ก.4 หน้าต่างตั้งค่าโครงสร้างระบบเครือข่ายแบบตรรกะ

1) อุปกรณ์ : สำหรับใส่ชื่ออุปกรณ์
2) IP : สำหรับใส่ไอพีแอดเดรสของอุปกรณ์
3) ประเภทอุปกรณ์ : สำหรับเลือกประเภทอุปกรณ์ ได้แก่ สวิตซ์ เราเตอร์ เซิร์ฟเวอร์ ไฟร์วอลล์ ฮับ อื่นๆ
4) Interface : สำหรับกรอกอินเตอร์เฟสที่ต้องการ
5) VLAN : สำหรับกำหนดวีแลนให้ระบบ
6) บันทึก Node : สำหรับบันทึกอุปกรณ์
7) เชื่อมต่อ : สำหรับเลือกอุปกรณ์ที่ต้องการเชื่อมต่อ (ระบุอินเตอร์เฟส)
8) ไปยัง : สำหรับเลือกอุปกรณ์ที่ต้องการให้อุปกรณ์ในข้อ 6) เชื่อมต่อไป (ระบุอินเตอร์เฟส)
9) เพิ่ม : เพิ่มการเชื่อมต่อดังกล่าว
10) Node : เลือกอุปกรณ์ที่ต้องการจะลบ
11) ลบ Node : ลบ Node ที่ต้องการออก
12) ลบ Connection : ลบ Connection ที่ต้องการออก

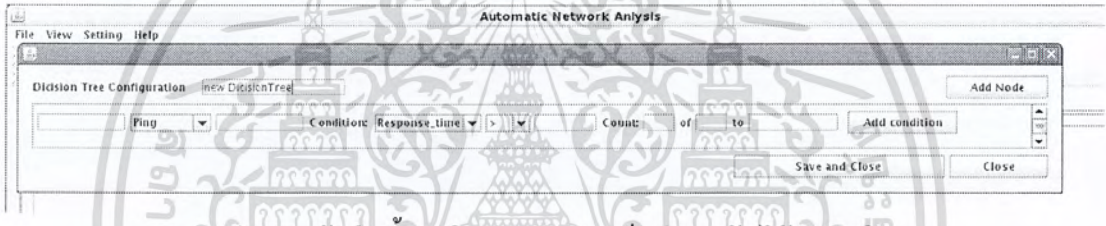
ก.2 การตั้งกฎบนแบบวิเคราะห์รูปแบบต้นไม้ตัดสินใจ

ทำการเลื่อนเมาส์ไปชี้ที่ Setting และทำการคลิ๊ก จากนั้นชี้ที่ Decision Tree จะมีแถบขึ้นมาให้เลือก จากนั้นคลิ๊กที่ Create Decision Tree



รูป ก.5 การตั้งกฎบนแบบวิเคราะห์รูปแบบต้นไม้ตัดสินใจ

จากนั้นจะได้หน้าต่างตั้งกฎบนแบบวิเคราะห์รูปแบบต้นไม้ตัดสินใจซึ่งมีรายละเอียดดังนี้

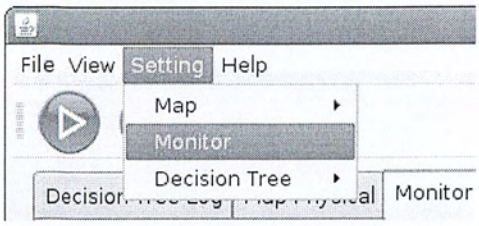


รูป ก.6 หน้าต่างตั้งกฎในแบบวิเคราะห์รูปแบบต้นไม้ตัดสินใจ

1) ช่องสำหรับตั้งชื่อชุดกฎ
2) ช่องสำหรับกำหนดลำดับขั้นตอนการทำงานแบบวิเคราะห์
3) ช่องสำหรับเลือกการกระทำ เช่น การปิง หรือ การตรวจสอบแบนวิดท์ เป็นต้น
4) ช่องสำหรับใส่ไอพีเพื่อที่ต้องการกระทำ
5) ช่องสำหรับเลือกเงื่อนไขในการวิเคราะห์ เช่น ค่าเวลาตอบสนอง หรือ ปริมาณแบนวิดท์ เป็นต้น
6) ช่องสำหรับใส่ค่าที่ต้องการจะตั้งเป็นขอบเขตในการตรวจสอบที่กฎนั้นๆ
7) ช่องสำหรับใส่ค่าของตัวนับและขอบเขตทั้งหมด เช่น หากมีการใช้งานแบนวิดท์เกินขอบเขตที่กำหนด เกิน 4 ใน 5 ครั้ง แบบวิเคราะห์จะทำการตรวจกฎต่อไปทันที
8) ช่องสำหรับกำหนดลำดับที่ต้องการจะวิเคราะห์ต่อไปของกฎ
9) Add Condition : สำหรับเพิ่มเงื่อนไขในการวิเคราะห์
10) Add Node : สำหรับเพิ่มกฎเข้าไปในแบบวิเคราะห์
11) Save and Close : สำหรับบันทึกกฎพร้อมทั้งปิดหน้าต่าง
12) Close : สำหรับปิดหน้าต่างการตั้งกฎ

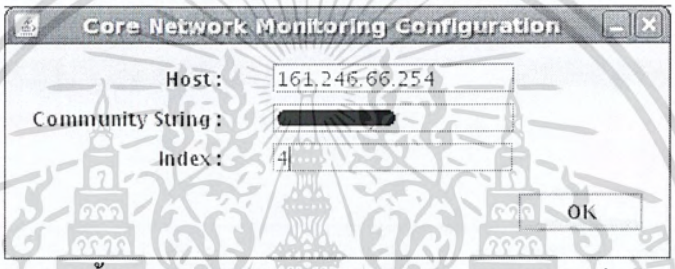
ก.3 การตั้งค่าตรวจตราปริมาณในเครือข่ายจากอุปกรณ์เครือข่ายหลัก

ทำการเลื่อนเมาส์ไปชี้ที่ Setting และทำการคลิ๊ก จากนั้นคลิ๊กที่ Monitor เพื่อเข้าสู่หน้าตั้งค่า



รูป ก.7 การตั้งค่าตรวจตราปริมาณในเครือข่ายจากอุปกรณ์เครือข่ายหลัก

จากนั้นจะได้หน้าต่างการตั้งค่าตรวจตราปริมาณซึ่งมีรายละเอียดดังนี้



รูป ก.8 หน้าต่างตั้งค่าตรวจตราปริมาณในเครือข่ายจากอุปกรณ์เครือข่ายหลัก

1) Host : สำหรับใส่ไอพีของอุปกรณ์เครือข่ายหลัก
2) Community String : สำหรับใส่ค่าสำหรับเข้าไปอ่านค่าต่างๆจากอุปกรณ์
3) index : สำหรับใส่ค่าอินเด็กซ์
4) ok : ตกลง