การพัฒนาระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง

โดย

นายฉลอง วิริยะธรรม

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาวิทยาการคอมพิวเตอร์

ภาควิชาคอมพิวเตอร์

บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร

ปีการศึกษา 2551

การพัฒนาระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง

โดย

นายฉลอง วิริยะธรรม

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาวิทยาการคอมพิวเตอร์

ภาควิชาคอมพิวเตอร์

บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร

ปีการศึกษา 2551

DEVELOPMENT OF LIMITED ROUTER CPU UTILIZATION

By

Chalong Viriyathum

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE

Department of Computing

Graduate School

SILPAKORN UNIVERSITY

2008

บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร อนุมัติให้วิทยานิพนธ์เรื่อง “ การพัฒนาระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง ” เสนอโดย นายฉลอง วิริยะธรรม เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์

……..

(รองศาสตราจารย์ ดร.ศิริชัย ชินะตังกูร)

คณบดีบัณฑิตวิทยาลัย

วันที่.....เดือน..... พ.ศ.....

อาจารย์ที่ปรึกษาวิทยานิพนธ์

ผู้ช่วยศาสตราจารย์ ดร.ปานใจ ธารทัศนวงศ์

คณะกรรมการตรวจสอบวิทยานิพนธ์

..... ประธานกรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.ปราณี นิลกรณ์)

...../...../.....

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.ฐาปนีย์ ธรรมเมธา)

...../...../.....

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.ปานใจ ธารทัศนวงศ์)

...../...../.....

47307312 : สาขาวิชาวิทยาการคอมพิวเตอร์
คำสำคัญ : การจำกัดการประมวลผล อุปกรณ์ค้นหาเส้นทาง

ฉลอง วิริยะธรรม : การพัฒนาระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง. อาจารย์ที่ปรึกษาวิทยานิพนธ์ : ผศ.ดร.ปานใจ ธารทัศนวงศ์. 65 หน้า.

การจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง เป็นการศึกษาผลกระทบในการรับส่งข้อมูลที่มีขนาดใหญ่บนระบบเครือข่ายที่มีจำนวนมาก หรือมีการสร้างการเชื่อมต่อ (connection) จากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งหรือจากเครื่องหนึ่งไปยังหลาย ๆ เครื่องเป็นจำนวนมาก ซึ่งทำให้การประมวลของอุปกรณ์ค้นหาเส้นทางมีค่าสูงขึ้น ซึ่งปรากฏการณ์ดังกล่าวจะส่งผลให้ประสิทธิภาพการรับส่งข้อมูลช้าลง หรือไม่สามารถรับส่งได้

ดังนั้นงานวิจัยนี้ได้นำเสนอวิธีการแก้ปัญหาดังกล่าวข้างต้น ผู้วิจัยได้นำเสนอวิธีการจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทางไว้ 3 วิธีดังนี้ 1. การควบคุมปริมาณของข้อมูลที่รับส่ง (Bandwidth Model) 2. การกำหนดความสำคัญของข้อมูล (Priority Model) และ 3. การป้องกันการส่งข้อมูล (Deny Model) จากผลการทดลองพบว่า การควบคุมปริมาณของข้อมูลที่รับส่งเป็นวิธีการที่ดีที่สุด รองลงมาเป็นการป้องกันการส่งข้อมูล สำหรับการกำหนดความสำคัญของข้อมูล เหมาะสำหรับองค์กรขนาดใหญ่ที่มีการส่งข้อมูลจำนวนมาก ดังนั้นการจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทางจึงเป็นแนวทางสำหรับหน่วยงานที่มีอุปกรณ์ค้นหาเส้นทางขนาดเล็ก โดยนำเทคนิคทั้งสามแบบที่กล่าวมาข้างต้นมากำหนดนโยบายบริหารจัดการเครือข่ายเพื่อทำให้ระบบเครือข่ายสามารถใช้งานอย่างมีเสถียรภาพ ประสิทธิภาพและสนับสนุนการทำงานให้เป็นไปตามเป้าหมายของหน่วยงาน และยังทำให้หน่วยงานสามารถประหยัดงบประมาณในการลงทุนอุปกรณ์ราคาสูงได้เป็นอย่างดี

ภาควิชาคอมพิวเตอร์ บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร ปีการศึกษา 2551

ลายมือชื่อนักศึกษา.....

ลายมือชื่ออาจารย์ที่ปรึกษาวิทยานิพนธ์ .....

47307312 : MAJOR : COMPUTER SCIENCE
KEY WORD : PROCESS LIMITED, ROUTER
CHALONG VIRIYATHUM : DEVELOPMENT OF LIMITED ROUTER CPU UTILIZATION.
THESIS ADVISOR : ASST.PROF.PANJAI TANTATASANAWONG Ph.D. 65 pp.

"Limited Router CPU Utilization" is a study about the effect of sending and receiving large amount of data across network systems, or over interconnecting computers of more than one machines, which can cause high Router CPU utilization and thus reducing effectiveness of data transmission to zero.

This research proposed three models to overcome the problem of "Limited Router CPU Utilization" which are 1) Bandwidth control (Bandwidth Model), 2) Data priority assignment (Priority model), and 3) Sending denial model (Deny Model). The experimental results reveal that the Bandwidth Model is the most effective, followed by the Deny Model. The Priority model is suitable for large enterprise organizations with huge amount of data transmission. The Limited Router CPU Utilization is therefore recommended for small enterprises with small router.

These three models can be combined with network management policy. The developed application can ensure stability, reliability, and effectiveness of data transmission for working as per the set objective of the enterprise, and effective investment cost control for network equipments.

Department of Computing Graduate School, Silpakorn University Academic Year 2008
Student's signature Chalong Viriyathum
Thesis Advisor's signature Panjai Tantatasanawong

กิตติกรรมประกาศ

วิทยานิพนธ์นี้ประสบความสำเร็จเป็นอย่างดีด้วยคำแนะนำของอาจารย์ที่ปรึกษาคือ ผู้ช่วยศาสตราจารย์ ดร. ปานใจ ธารทัศนวงศ์ และกรรมการวิทยานิพนธ์ทั้ง 2 ท่าน คือ ผู้ช่วยศาสตราจารย์ ดร. ปราณี นิลกรณ์ และ ผู้ช่วยศาสตราจารย์ ดร. ฐาปนีย์ ธรรมเมธา ทางผู้วิจัยต้องขอขอบพระคุณกรรมการทั้ง 3 ท่านเป็นอย่างสูง ที่แนะนำตลอดมา

ทางผู้วิจัยขอขอบพระคุณผู้อำนวยการศูนย์คอมพิวเตอร์ มหาวิทยาลัยศิลปากร ที่ให้ความช่วยเหลือด้านอุปกรณ์และสถานที่สำหรับทำงานวิจัยนี้ และขอขอบคุณพี่ ๆ เพื่อน ๆ และน้อง ๆ ศูนย์คอมพิวเตอร์ มหาวิทยาลัยศิลปากร ที่ช่วยเหลือด้วยดีมาตลอด

ทางผู้วิจัยต้องขอขอบพระคุณบิดา มารดา และพี่ ๆ ที่ให้การสนับสนุน และให้กำลังใจกับผู้วิจัยเป็นอย่างดียิ่ง จนกระทั่งวิทยานิพนธ์นี้เสร็จสมบูรณ์

สารบัญ

สารบัญตาราง

สารบัญภาพ

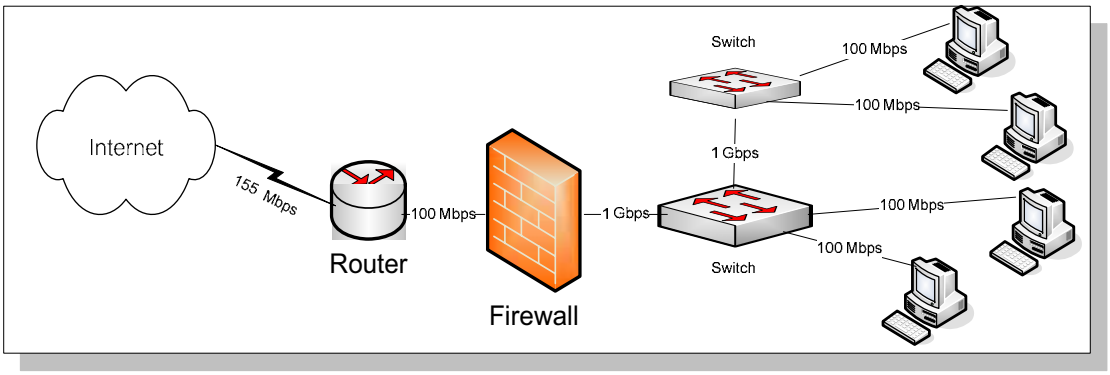
ภาพที่ หน้า

บทที่ 1
บทนำ

ในปัจจุบันนี้การติดต่อสื่อสารแลกเปลี่ยนข้อมูลผ่านระบบเครือข่ายคอมพิวเตอร์ได้เข้ามามีบทบาทต่อการทำงานในชีวิตประจำวันของทุกคน ผู้ที่มีโอกาสเข้าถึงข้อมูลย่อมเป็นผู้ที่ได้เปรียบในการทำงานและการตัดสินใจมากกว่า ดังนั้นทุกคนต่างมีความต้องการ การติดต่อสื่อสารและพยายามหาวิธีที่ทำให้การติดต่อสื่อสารมีพื้นที่ครอบคลุมให้มากที่สุดเท่าที่ทำได้ ระบบเครือข่ายอินเตอร์เน็ตเป็นระบบเครือข่ายหนึ่งที่มีผู้ใช้มากที่สุด เนื่องจากเป็นระบบเครือข่ายที่มีการเชื่อมโยงครอบคลุมทุกพื้นที่ของโลก สามารถรับและส่งข้อมูลในรูปแบบต่าง ๆ ได้ เช่น การรับส่งอีเมล์ (e-mail) การส่งข้อความสนทนา (chat messages) การรับส่งรูปภาพ เสียง หรือ วิดีโอ (picture, voice, video) ระบบเครือข่ายอินเตอร์เน็ตยังใช้ในการค้นหาความรู้ การศึกษา และงานวิจัย อย่างไรก็ตามผู้ใช้ยังต้องให้ระบบเครือข่ายใช้งานได้อย่างต่อเนื่องตลอดเวลาที่ใช้งาน ไม่มีใครต้องการให้การใช้งานขัดข้องหรือขาดการติดต่อ และไม่ต้องการให้ความเร็วในการรับส่งข้อมูลช้าลง ด้วยเหตุนี้ผู้ดูแลระบบเครือข่ายจำเป็นต้องคอยตรวจสอบและแก้ไขระบบเครือข่ายคอมพิวเตอร์ให้สามารถใช้งานได้ตลอดเวลา

1. ความสำคัญและปัญหา

การติดต่อสื่อสารของระบบเครือข่ายคอมพิวเตอร์ มีอุปกรณ์เครือข่ายหลายชนิดเชื่อมโยงถึงกันดังตัวอย่างภาพที่ 1 การเชื่อมต่อระบบเครือข่าย ซึ่งแต่ละอุปกรณ์ก็มีหน้าที่ในการทำงานที่แตกต่างกันไป แต่มีอุปกรณ์ชนิดหนึ่งที่ทำหน้าที่ต่อเชื่อมระบบเครือข่ายภายในองค์กรกับระบบเครือข่ายภายนอกองค์กรเข้าด้วยกัน และทำหน้าที่หลักในการค้นหาเส้นทางการส่งข้อมูลไปยังผู้รับ โดยเลือกเส้นทางว่าควรส่งไปยังภายนอกองค์กร หรือส่งเข้ามาภายในองค์กร อุปกรณ์ดังกล่าวเรียกว่า “อุปกรณ์ค้นหาเส้นทาง” (Router)



ภาพที่ 1 การเชื่อมต่อระบบเครือข่าย

อุปกรณ์ค้นหาเส้นทางจะสามารถทำงานอย่างเป็นปกติได้ ถ้าการรับส่งข้อมูลเป็นไปตามรูปแบบหรือตามมาตรฐานของแต่ละโปรโตคอล (Protocol) หรือแต่ละโปรแกรมประยุกต์ (Application Program) ถึงจะมีข้อมูลหรือมีเครื่องคอมพิวเตอร์ ผู้ใช้ (Client) จำนวนมากก็ตาม ซึ่งอาจจะมีบางปัจจัยที่ส่งผลต่อการทำงานของซีพียูของอุปกรณ์ค้นหาเส้นทางบ้างแต่ก็ไม่สูงขึ้นมากและรวดเร็ว แต่หากมีผู้ใช้บางคนหรือมีบางโปรแกรมประยุกต์หรือมีไวรัสคอมพิวเตอร์ ส่งข้อมูลที่ผิดแปลกจากรูปแบบหรือมาตรฐานที่กำหนดไว้ ก็จะส่งผลให้การทำงานของซีพียูของอุปกรณ์ค้นหาเส้นทางเพิ่มขึ้นอย่างรวดเร็ว ทำให้ค่าการทำงานของซีพียูมีค่าสูงถึง 99 เปอร์เซ็นต์ (Cisco 2007 a) และมีผลให้อุปกรณ์ค้นหาเส้นทางมีประสิทธิภาพการทำงานช้าลง หรือมีการตอบสนองการทำงานช้าลง หรือไม่มีการส่งแพ็กเก็ตข้อมูลใหม่ไปยังผู้รับหรือในที่สุดก็หยุดทำงานทุกอย่าง ต้องแก้ไขโดยการปิดและเปิดอุปกรณ์นี้ใหม่ ถ้าปัญหาข้างต้นเกิดขึ้นในช่วงเวลาที่ผู้ดูแลระบบเครือข่ายได้ทำการมอนิเตอร์ (Monitor) อยู่ก็สามารถที่จะปิดและเปิดอุปกรณ์ค้นหาเส้นทางใหม่ได้ แต่ถ้ายังมีการรับส่งข้อมูลที่ผิดปกติอยู่ ก็ทำให้เกิดปัญหาเช่นเดิมซ้ำอีก ทำให้ผู้ใช้ที่กำลังใช้งานบนระบบเครือข่ายได้รับผลกระทบจากปัญหาดังกล่าวด้วย และถ้าเป็นช่วงเวลาที่มีความต้องการติดต่อรับส่งข้อมูลที่สำคัญและเร่งด่วน ก็ไม่สามารถติดต่อสื่อสารกันได้ ทำให้เกิดความเสียหายต่อระบบงานหรือต่อระบบธุรกิจได้

จากปัญหาข้างต้นได้ส่งผลให้ระบบงานต่าง ๆ ที่ใช้งานบนระบบเครือข่ายคอมพิวเตอร์นี้เกิดความเสียหาย ผู้พัฒนาระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง มีความเห็นว่ามีความจำเป็นอย่างยิ่งต้องทำการศึกษาวิจัยค้นหาสาเหตุของการเกิดปัญหา เพื่อสร้างกฎมาควบคุมหรือยับยั้งการทำงานที่ผิดปกติของการประมวลผลของอุปกรณ์ค้นหาเส้นทาง โดยมุ่งหวังว่าระบบเครือข่ายยังคงสามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพตามที่มีการออกแบบและติดตั้งไว้

2. วัตถุประสงค์ของงานวิจัย

1. เพื่อศึกษาวิเคราะห์ออกแบบและพัฒนาระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง

2. เพื่อประเมินระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง โดยจำลองสถานการณ์

3. ประโยชน์ที่ได้รับ

1. เพื่อให้ระบบเครือข่ายคอมพิวเตอร์ สามารถใช้งานได้อย่างต่อเนื่อง

2. เพื่อให้ทราบข้อมูลลักษณะหรือรูปแบบของแพ็กเก็ตข้อมูลที่มีผลกระทบต่อการประมวลผลของอุปกรณ์ค้นหาเส้นทาง (Router CPU Utilization)

3. เพื่อให้สามารถหยุดหรือยับยั้งการรับส่งข้อมูลที่ผิดปกติ ได้อย่างอัตโนมัติและทันเวลา ป้องกันไม่ให้มีผลกระทบต่อการประมวลผลของอุปกรณ์ค้นหาเส้นทางตามเกณฑ์ที่ตั้งไว้ (router cpu utilization threshold)

4. เพื่อให้ผู้ดูแลระบบเครือข่ายหรือเจ้าหน้าที่ที่เกี่ยวข้องรับทราบถึงความผิดปกติของอุปกรณ์ค้นหาเส้นทางหรือของระบบเครือข่าย ได้อย่างรวดเร็วและทันเวลา โดยการรับข้อความสั้น ๆ (short message) จากระบบที่พัฒนาระบบขึ้น

5. เพื่อให้สามารถออกรายงานถึงผลกระทบและรูปแบบความผิดปกติของการรับส่งแพ็กเก็ตข้อมูลที่เกิดขึ้นได้

6. เพื่อให้สามารถปรับปรุงเงื่อนไขของการใช้ระบบเครือข่าย (Network Policy) ให้สอดคล้องกับสถานการณ์ที่เกิดขึ้นได้โดยอัตโนมัติ

7. เพื่อนำผลจากการศึกษาวิจัยนี้มาใช้สำหรับการวางแผนปรับปรุงระบบเครือข่ายต่อไป

4. ขอบเขตการวิจัย

1. การศึกษาและวิเคราะห์ข้อมูลจะใช้การรับส่งแพ็กเก็ตข้อมูลทั้งบนระบบไอพีแอดเดรสรุ่น 4 (IP version 4) และระบบไอพีแอดเดรสรุ่น 6 (IP version 6)

2. การศึกษาและวิเคราะห์ข้อมูลจะสนใจการรับส่งแพ็กเก็ตข้อมูลที่ส่งผลกระทบต่อการประมวลผลของอุปกรณ์ค้นหาเส้นทาง (Router CPU Utilization)

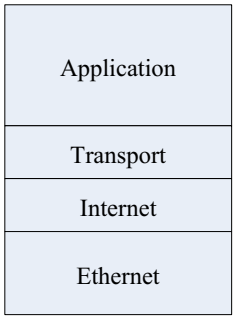
3. การศึกษาและวิเคราะห์ข้อมูลจะใช้ มหาวิทยาลัยศิลปากร วิทยาเขตพระราชวังสนามจันทร์เป็นกรณีศึกษา

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

การติดต่อสื่อสารระบบเครือข่ายคอมพิวเตอร์และระบบอินเตอร์เน็ต ในปัจจุบันได้รับความนิยมอย่างกว้างขวางในการใช้โปรโตคอลชุดของ ทีซีพี/ไอพี (TCP/IP Protocol Suite) เป็นมาตรฐานในการติดต่อสื่อสาร ดังนั้นก่อนที่จะพัฒนาระบบกำจัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง ผู้พัฒนาจะขอกล่าวถึงพื้นฐานของโปรโตคอลชุด ทีซีพี/ไอพี เพื่อทำให้มีความเข้าใจระบบเครือข่ายคอมพิวเตอร์และระบบอินเตอร์เน็ต ตลอดจนถึงขั้นตอนการรับส่งข้อมูลบนระบบเครือข่าย และการทำงานของแต่ละโปรโตคอลที่ใช้งาน

1. ความรู้พื้นฐานเกี่ยวกับโปรโตคอลทีซีพี/ไอพี

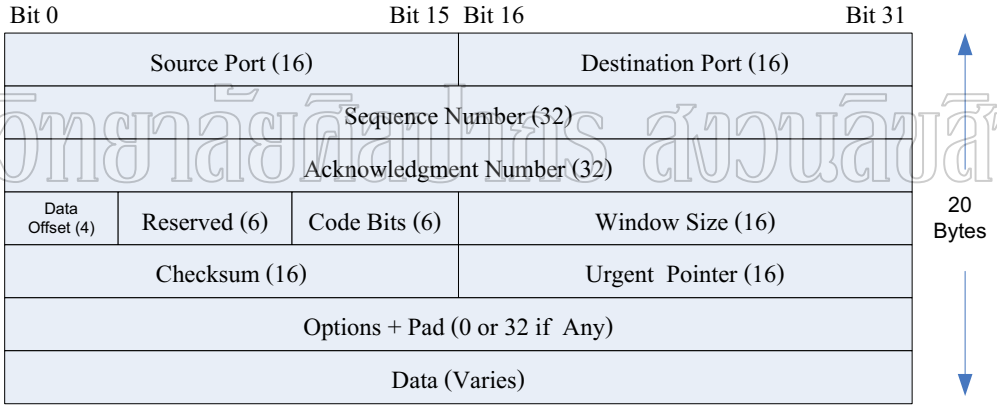
โปรโตคอลชุด ทีซีพี/ไอพี ได้พัฒนาขึ้นมาโดยองค์กร Defense Advanced Research Projects Agency (DARPA) ของประเทศสหรัฐอเมริกา เพื่อใช้ในการติดต่อสื่อสารภายในองค์กร ต่อมา TCP/IP ได้รับการผนวกเข้าเป็นส่วนหนึ่งของระบบปฏิบัติการยูนิกส์ (Berkeley Software Distribution of UNIX) และในปัจจุบันได้กลายมาเป็นมาตรฐานที่เป็นการยอมรับกันโดยทั่วไปโดยปริยาย (de facto standard) สำหรับการสื่อสารระหว่างเครือข่ายและทำหน้าที่ในการถ่ายทอดข่าวสารจากอุปกรณ์เครือข่ายตัวหนึ่งไปยังอีกตัวหนึ่ง (transport protocol stack) โปรโตคอล TCP/IP ช่วยให้เกิดการสื่อสารระหว่างเครือข่ายต่าง ๆ ที่เชื่อมต่อเข้าด้วยกันและสามารถนำไปใช้ในสื่อสารได้ดีทั้งในระบบเครือข่าย LAN และ WAN มีการแบ่งชั้นของการสื่อสารออกเป็น 4 ชั้น ดังรูปที่ 2 ชั้นของโปรโตคอลทีซีพี/ไอพี



ภาพที่ 2 ชั้นของโปรโตคอลทีซีพี/ไอพี
ที่มา : ซิสโก้, หลักสูตร CCNA 2 Cisco Network Academy Program CCNA 2 (กรุงเทพฯ : เพียร์สัน เอ็ดดูเคชั่น อินโดไชน่า, 2543), 22.

1.1 ชั้นแอพลิเคชั่น (Application Layer) มีโปรโตตอลที่รู้จักกันหลายตัวที่ใช้สนับสนุนการถ่ายโอนแฟ้มข้อมูล เช่น เอสเอ็มทีพี (SMTP) ที่ใช้ในการรับส่งอีเมล์, เอชทีทีพี (HTTP) ใช้เป็นมาตรฐานในระบบอินเตอร์ที่สนับสนุนการแลกเปลี่ยนข่าวสารบน World Wide Web (WWW) เอ็ฟทีพี (FTP) ใช้ในการถ่ายโอนแฟ้มข้อมูล เป็นต้น

1.2 ชั้นทรานสปอร์ต (Transport Layer) มีโปรโตคอล Transmission Control Protocol (TCP) และ User Datagram Protocol (UDP) ซึ่งโปรโตคอลทีซีพีมีหน้าที่นำส่งข้อมูลโดยมีการรับประกันความเชื่อถือ หากมีแพ็กเก็ตสูญหาย ทีซีพีด้านผู้ส่งต้องมีการส่งแพ็กเก็ตใหม่ ส่วนทีซีพีด้านผู้รับมีหน้าที่จัดแพ็กเก็ตให้ถูกต้องตามลำดับและกำจัดแพ็กเก็ตที่ซ้ำซ้อน และเป็นโปรโตคอลแบบ “connection oriented” คือต้องสถาปนาการเชื่อมต่อระหว่างสถานีต้นทางและปลายทางก่อนการส่งข้อมูล และขณะที่มีการส่งข้อมูลผ่านชั้นทรานสปอร์ต จะเพิ่มเฮดเดอร์ของทีซีพีเข้าไป ดังรูปที่ 3 ทีซีพีเดทาแกรม



ภาพที่ 3 ทีซีพีเดทาแกรม

ที่มา : สุรศักดิ์ สงวนวงศ์, สถาปัตยกรรมและโปรโตคอลทีซีพี/ไอพี (กรุงเทพฯ : ซีเอ็ดยูเคชั่น จำกัด(มหาชน), 2543), 218-219.

- Source Port ขนาด 16 บิต : หมายเลขพอร์ตของสถานีต้นทางที่ส่ง
- Destination Port ขนาด 16 บิต : หมายเลขพอร์ตของสถานีปลายทางที่รับ
- Sequence Number ขนาด 32 บิต : ทีซีพีใช้ เลขลำดับ เป็นตัวนับจำนวนไบต์ที่ส่งทุกครั้งที่สถาปนาการเชื่อมโยงทีซีพีจะเลือกเลขลำดับเริ่มต้นสำหรับชี้ตำแหน่งข้อมูลไบต์แรกที่จะจัดส่ง หมายเลขเริ่มต้นไม่จำเป็นต้องเริ่มด้วย 1 แต่อาจเริ่มด้วยค่าใด ๆ ก็ได้ ข้อมูลในเซกเมนต์ถัดไปจะมีเลขลำดับที่สัมพัทธ์เลขลำดับในเซกเมนต์ก่อนหน้า

- Acknowledgment Number ขนาด 32 บิต : ค่ากำหนด เลขตอบรับ ซึ่งใช้ตอบกลับไปว่าได้รับข้อมูลแล้ว เลขตอบรับจะมีค่าเท่ากับเลขลำดับประจำเซกเมนต์บวกด้วยจำนวนไบต์ข้อมูลและบวกด้วยหนึ่ง เช่น เซกเมนต์หนึ่งมีเลขลำดับเท่ากับ 10 และมีข้อมูล 50 ไบต์ เลขตอบรับที่ต้องส่งกลับไปจะเท่ากับ 10+50+1=62 ซึ่งแจ้งว่าได้รับข้อมูลตั้งแต่ต้นถึงไบต์ลำดับที่ 61 แล้ว และคาดว่าไบต์ถัดไปคือไบต์ที่ 62

- Data Offset (Offset) ขนาด 4 บิต : บอกถึงตำแหน่งเริ่มต้นของไบต์ข้อมูลหรืออีกนัยหนึ่งใช้บอกขนาดเฮดเดอร์ ตัวเลขนี้มีหน่วยเป็นจำนวนเท่าของ 4 ไบต์ เช่นเดียวกับที่ใช้ในไอพีเดทาแกรม เฮดเดอร์ของทีซีพีมีความยาวขึ้นกับฟิลด์ option ตัวเลขในฟิลด์ offset จะเท่ากับ 5 ซึ่งเท่ากับ 20 ไบต์ (5x4=20) หากไม่ใช้ออพชันใด

- Reserved (RSV) ขนาด 6 บิต : สำรองไว้ใช้ในอนาคต

- Code Bit ประกอบด้วย 6 ฟิลด์ย่อย แต่ละฟิลด์ย่อยมีขนาด 1 บิต ทำหน้าที่เป็นแฟล็ก เรียงลำดับจากซ้ายไปขวาดังต่อไปนี้

URG	ACK	PSH	RST	SYN	FIN

  - URGent ถ้าบิตนี้เป็น “1” หมายความว่า Urgent pointer บรรจุตำแหน่งข้อมูลที่ต้องรีบดำเนินการเร่งด่วนก่อน
  - ACKnowledgement ถ้าบิตนี้เป็น “1” หมายถึงเป็นเซกเมนต์ตอบรับ โดยตอบอ้างอิงเลขลำดับตามที่กำหนดในฟิลด์ Acknowledgement number
  - PuSH ถ้าบิตนี้เป็น “1” หมายความว่าทันทีที่สถานีปลายทางได้รับเซกเมนต์ต้องรีบส่งข้อมูลไปยังโปรโตคอลประยุกต์ทันทีโดยไม่ต้องรอให้บัฟเฟอร์เต็ม
  - ReSeT ถ้าบิตนี้เป็น “1” หมายถึงให้ยกเลิกการเชื่อมต่อนี้
  - SYNchronize ถ้าบิตนี้เป็น “1” หมายถึงขอเริ่มต้นสถาปนาการเชื่อมต่อและเมื่อการสถาปนาเสร็จสิ้น บิตนี้จะถูกกำหนดให้เป็น “0” หลังจากนั้นจึงสามารถส่งผ่านข้อมูลระหว่างกันได้
  - FINish ถ้าบิตนี้เป็น “1” หมายถึงขอจบการเชื่อมต่อ

- Window Size ขนาด 16 บิต : สถานีปลายทางใช้ฟิลด์นี้แจ้งขนาดบัฟเฟอร์ที่มีอยู่ (หน่วยเป็นไบต์) สถานีที่ติดต่อด้วยต้องไม่ส่งข้อมูลเกินค่านี้

- Checksum ขนาด 16 บิต : ผลรวมตรวจสอบความถูกต้องของเซกเมนต์โดยคำนวณทั้งเฮดเดอร์และข้อมูล (ใช้เฮดเดอร์เทียมเช่นเดียวกับยูดีพี)

- Urgent pointer ขนาด 16 บิต : พอยเตอร์ชี้ตำแหน่งไบต์ข้อมูลที่ต้องดำเนินการเร่งด่วนที่ต้องการให้โปรแกรมประยุกต์ดำเนินการทันที ค่าที่บรรจุในฟิลด์นี้จะมีความหมายก็ต่อเมื่อแฟล็ก URG ถูกเซ็ตเป็น “1”

- Options ขนาดแปรเปลี่ยนได้ : ใช้กำหนดงานเพิ่มเติมให้กับทีซีพีซึ่งจะมีหรือไม่ก็ได้ หากฟิลด์ offset หากมีค่าเป็น 5 แสดงว่ามีเฮดเดอร์มีขนาด 20 ไบต์ซึ่งหมายถึงไม่ใช้ออพชันออพชันที่มีให้ใช้งาน

- Pad ขนาด 0 ถึง 24 บิต : ใช้เป็นส่วนที่ทำให้ขนาดของออพชันเป็นจำนวนเท่าของ 32 บิต (เพื่อให้เฮดเดอร์ลงตัวที่ค่าจำนวนเท่าของ 32)

โปรโตคอลยูดีพีให้บริการแบบ “connectionless” กล่าวคือไม่สถาปนาการเชื่อมต่อระหว่างสถานีต้นทางและปลายทาง ยูดีพีส่งเดทาแกรมโดยไม่ตรวจสอบว่าสถานีปลายทางพร้อมที่จะติดต่อหรือไม่ การสื่อสารลักษณะนี้อาจเทียบได้กับการส่งจดหมาย ผู้ส่งเพียงแต่มอบหมายให้ไปรษณีย์จัดส่งโดยไม่ต้องทราบว่าผู้รับปลายทางพร้อมรับหรือไม่ ข้อได้เปรียบของยูดีพี คือมีความเร็วในการทำงานสูง เนื่องจากไม่มีการใช้การตอบรับ ทำให้มีการถ่ายทอดข้อมูลทำได้เร็วขึ้น ซึ่งมีรายละเอียดของเดทาแกรม ดังรูปที่ 4 ยูดีพีเดทาแกรม

Bit 0 – Bit 15	Bit 16 – Bit 31
Source Port (16)	Destination Port (16)
Length (16)	Checksum (16)
Data (Varies)	

ภาพที่ 4 ยูดีพีเดทาแกรม

ที่มา : สุรศักดิ์ สงวนวงศ์, สถาปัตยกรรมและโปรโตคอลทีซีพี/ไอพี (กรุงเทพฯ : ซีเอ็ดยูเคชั่นจำกัด(มหาชน), 2543), 208-209.

- Source port ขนาด 16 บิต : พอร์ตสถานีต้นทางที่ส่ง

- Destination port ขนาก 16 บิต : พอร์ตสถานีปลายทางที่รับ

- Length ขนาก 16 บิต : บอกความยาวของเดทาแกรม (ทั้งเฮดเดอร์และข้อมูล) เป็นจำนวนไบต์

- Checksum ขนาด 16 บิต : ผลรวมตรวจสอบ คำนวณจากผลรวมของเฮดเดอร์และข้อมูล

ในการติดต่อสื่อสารต้องระบุพอร์ตที่ใช้ในการติดต่อสื่อสาร โดยพอร์ตที่ใช้ทั้งโปรโตคอลทีซีพีและยูดีพีมีการแบ่งไว้ 3 ช่วงดังนี้

○ Well-known ports มีค่าระหว่าง 0 ถึง 1023 เป็นพอร์ตที่มีการกำหนดไว้เป็นมาตรฐานว่าพอร์ตใดใช้เกี่ยวกับอะไร

○ Registered ports มีค่าระหว่าง 1024 ถึง 49151 เป็นพอร์ตที่มีการลงทะเบียนไว้แล้วว่ากับแอพลิเคชั่นใด

○ Dynamic or Private ports มีค่าระหว่าง 49152 ถึง 65535

1.3 ชั้นของไอพี (Internet Layer) หรือชั้นของเน็ตเวอร์ต (Network Layer) เป็นโปรโตคอลที่มีหน้าที่รับผิดชอบในการกำหนดหมายเลขที่อยู่ที่ช่วยให้แพ็กเก็ตสามารถส่งในระบบเครือข่ายไปยังเป้าหมายได้อย่างถูกต้อง โดยอุปกรณ์ค้นหาเส้นทางจะใช้หมายเลขไอพีแอดเดรสและใช้ข้อมูลในส่วนหัวของแพ็กเก็ตไอพีในการตรวจว่าแพ็กเก็ตนั้นควรส่งออกไปทางใดของการเชื่อมต่อเพื่อให้ส่งไปยังเป้าหมายได้ โปรโตคอลที่ใช้ในชั้นนี้มีดังนี้

1.3.1 โปรโตคอลไอพี (IP : Internet Protocol) ทำหน้าที่กำหนดรูปแบบของแอดเดรสประจำเครื่องเพื่อใช้ในการลำเลียงข้อมูลจากเครื่องต้นทางไปยังเครื่องปลายทาง นอกจากนี้ยังทำหน้าที่เลือกเส้นทางส่งข้อมูล ตลอดจนแบ่งขนาดข้อมูลให้เหมาะกับฮาร์ดแวร์ระดับล่าง ซึ่งในปัจจุบันไอพีแอดเดรสที่นิยมใช้อยู่มี 2 รุ่นด้วยกัน คือ ไอพีแอดเดรสรุ่นที่ 4 มีรายละเอียดของเดทาแกรมดังรูปที่ 5 และไอพีแอดเดรสรุ่นที่ 6 มีรายละเอียดของเดทาแกรมดังรูปที่ 6

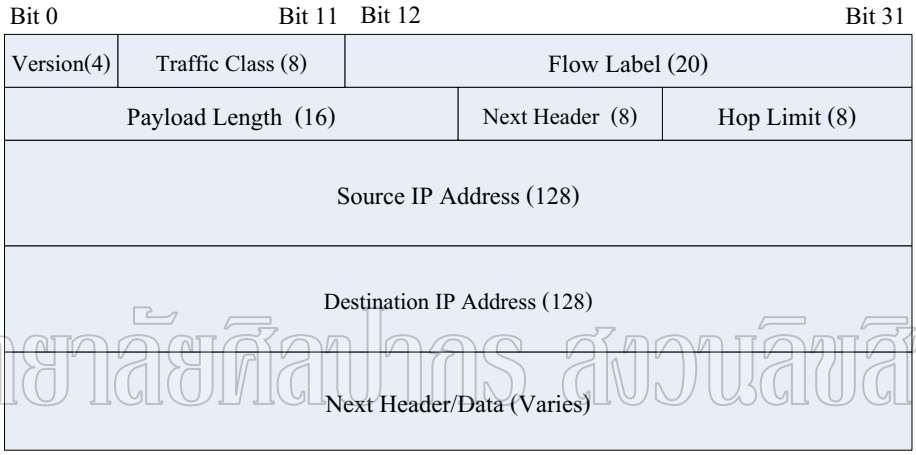
Bit 0		Bit 15 Bit 16	Bit 31
Version(4)	IHL (4)	TOS (8)	Total Length (16)
Identification (16)		Flags (3)	Flagment Offset (13)
Time To Live (8)	Protocol (8)		Header Checksum (16)
Source IP Address (32)			
Destination IP Address (32)			
Options + Pading			
Data (Varies)			

ภาพที่ 5 ไอพีเดทาแกรมรุ่นที่ 4

ที่มา : สุรศักดิ์ สงวนวงศ์, สถาปัตยกรรมและโปรโตคอลทีซีพี/ไอพี (กรุงเทพฯ : ซีเอ็ดยูเคชั่น จำกัด(มหาชน), 2543), 88-90.

- Version ขนาด 4 บิต : แสดงรุ่นของโปรโตคอล มีค่า 4
- Internet Header Length (IHL) ขนาด 4 บิต : บอกความยาวเฉพาะเฮดเดอร์ของเดทาแกรมโดยนับจาก version จนถึงไบต์สุดท้ายก่อนที่จะถึงข้อมูล หน่วยนับความยาวจะบอกเป็นจำนวนเท่าของ 4 ไบต์ (หรือ 32 บิตเวิร์ด) หาก IHL มีค่าเท่ากับ 5 จะหมายถึงส่วนหัวมีขนาด 20 ไบต์ ซึ่งเป็นค่าที่บอกว่าไม่มี options และ padding อยู่ในเดทาแกรม
- Type of Service (TOS) ขนาด 8 บิต : ฟิลด์นี้ใช้กำหนดรูปแบบการให้บริการตามลักษณะโปรโตคอลแอพลิเคชัน
- Total length มีขนาด 16 บิต : บอกถึงความยาวทั้งหมดของเดทาแกรม (เฮดเดอร์และข้อมูล) โดยมีหน่วยนับเป็นไบต์ เนื่องจากฟิลด์นี้มีขนาด 16 บิต ไอพีเดทาแกรมจึงมีขนาดใหญ่สุดเท่ากับ 2^{16}-1 หรือ 65,535 ไบต์
- Identification ขนาด 16 บิต
- Flags ขนาด 3 บิต
- Fragment offset ขนาด 13 บิต
- Time to Live (TTL) ขนาด 8 บิต : ฟิลด์นี้ใช้กำหนดจำนวนเราเตอร์ที่เดทาแกรมจะเดินทางผ่านได้หรืออีกนัยหนึ่งคือกำหนดอายุของเดทาแกรมซึ่งมีค่าได้สูงสุดตามขนาดฟิลด์คือ 2^{8}-1 หรือ 255 สถานีที่ส่งเดทาแกรมจะตั้งค่า TTL ไว้ที่ค่าใดค่าหนึ่ง เราเตอร์ที่รับเดทาแกรมจะปรับลดค่านี้ลงหนึ่งหน่วย หากลดลงเป็น 0 เราเตอร์จะทิ้งเดทาแกรมนั้นและรายงานกลับไปด้วยไอซีเอ็มพี วิธีนี้ช่วยป้องกันปัญหาเดทาแกรมวนรอบ (routing loop) สถานีต้นทางต้องเลือกใช้ค่านี้ให้เหมาะสม เนื่องจากหากมีค่าน้อยไปจะทำให้เดทาแกรมเดินทางไปไม่ถึงปลายทาง หรือหากตั้งไว้มากเกินไปก็จะสร้างภาระให้ระบบเมื่อมีความผิดปกติด้านการเลือกเส้นทาง ค่าโดยปกติที่ใช้คือ 64
- Protocol ขนาด 8 บิต : ฟิลด์บอกชนิดของโปรโตคอลระดับบนที่เอ็นแคปซูเลตในเดทาแกรม เพื่อให้สถานีปลายทางและสามารถส่งข้อมูลไปยังโปรโตคอลระดับบนได้ถูกต้อง ค่าที่ใช้ประจำโปรโตคอล
- Header Checksum ขนาด 16 บิต : ใช้ตรวจสอบความผิดพลาดเฉพาะเฮดเดอร์โดยไม่รวมส่วนข้อมูล การคำนวณผลรวมตรวจสอบจะเริ่มต้นด้วยการให้ฟิลด์ checksum มีค่าเป็น 0 จากนั้นจึงบวกเฮดเดอร์ครั้งละ 16 บิตแบบเติมเต็มหนึ่ง (1's complement) เมื่อได้ผลลัพธ์แล้ว จะนำไปใส่ในฟิลด์ checksum ไอพีปลายทางเมื่อได้รับเดทาแกรมแล้วก็เพียงแต่บวกเฮดเดอร์ทั้งหมดครั้งละ 16 บิตแบบเติมเต็มหนึ่ง หากค่าที่ได้ไม่เท่ากับศูนย์แสดงว่ามีข้อผิดพลาดในเฮดเดอร์
- Source IP Address ขนาด 32 บิต : กำหนดไอพีแอดเดรสต้นทาง

- Destination IP Address ขนาด 32 บิต : กำหนดไอพีแอดเดรสปลายทาง
- Option ขนาดไม่คงที่ : ใช้สำหรับกำหนดข่าวสารเพิ่มเติมสำหรับเดทาแกรม ค่าที่ใช้ในปัจจุบันจะเกี่ยวข้องกับการรักษาความปลอดภัย และการบันทึกผลลัพธ์จากการทำงานของคำสั่ง traceroute หรือ ping ซึ่งจะได้กล่าวในหัวข้อที่ 5.7
- Padding ขนาด 0 ถึง 3 ไบต์ : ใช้สำหรับผนวกเพิ่มเพื่อให้จำนวนไบต์ของ option รวมกับ padding เป็นจำนวนเท่าของ 32 บิต ค่าในฟิลด์ padding จึงไม่มีความสำคัญใด
- Data ขนาดไม่คงที่ : ข้อมูลจากโปรโตคอลระดับบน



ภาพที่ 6 ไอพีเดทาแกรมรุ่นที่ 6
ที่มา : สุรศักดิ์ สงวนวงศ์, สถาปัตยกรรมและโปรโตคอลทีซีพี/ไอพี (กรุงเทพฯ : ซีเอ็ดยูเคชั่น จำกัด(มหาชน), 2543), 441-442.

- Version ขนาด 4 บิต : แสดงรุ่นของโปรโตคอล มีค่า 6
- Traffic Class ขนาด 8 บิต : กำหนดกลุ่มแพ็กเก็ตตามคลาสและลำดับความสำคัญ
- Flow Label ขยาด 20 บิต : กำหนดรูปแบบการสื่อสาร
- Payload Length ขนาด 16 บิต : บอกขนาดข้อมูลในหน่วยไบต์โดยไม่รวมกับเฮดเดอร์
- Next Header ขนาด 8 บิต : ทำหน้าที่ทั้งตัวกำหนดชนิดโปรโตคอลและออพชั่นประจำเดทาแกรม หากใช้จะบบจุค่าแสดงเฮดเดอร์ของออพชันที่ใช้งานที่บรรจุอยู่ต่อจากเฮดเดอร์ปกติ
- Next Hop ขนาด 8 บิต : ใช้กำหนดระยะทางที่แพ็กเก็ตจะเดินทางผ่านได้ เราเตอร์ที่รับแพ็กเก็ตจะปรับค่าลดลงหนึ่งหน่วย หากเป็น 0 เราเตอร์จะกำจัดแพ็กเก็ตนั้นไป

- Source IP Address ขนาด 128 บิต : กำหนดไอพีแอดเดรสต้นทาง
- Destination IP Address ขนาด 128 บิต : กำหนดไอพีแอดเดรสปลายทาง

1.3.2 โปรโตคอลไอซีเอ็มพี (ICMP : Internet Control Message Protocol) สนับสนุนการควบคุมการทำงานหรือใช้รายงานสถานะความผิดพลาดที่เกิดขึ้น

1.3.3 โปรโตคอลเออาร์พี (ARP : Address Resolution Protocol) ทำหน้าที่ค้นหาที่อยู่ในชั้นสื่อสาร data link layer (MAC Address) สำหรับอุปกรณ์ที่รู้จักหมายเลขไอพี

1.3.4 โปรโตคอลอาร์เออาร์พี (RARP : Reverse Address Resolution Protocol) ทำหน้าที่ค้นหาที่ในชั้น network layer เมื่อรู้ที่ในชั้นของ data link layer แล้ว

1.4 ชั้นของอีเธอร์เน็ต (Ethernet Layer) หรือเดทาลิงค์ (Data Link Layer) เป็นชั้นที่ทำงานในระดับฮาร์ดแวร์ เช่นการกำหนดหมายเลขประจำการ์ดแลน (MAC Address)

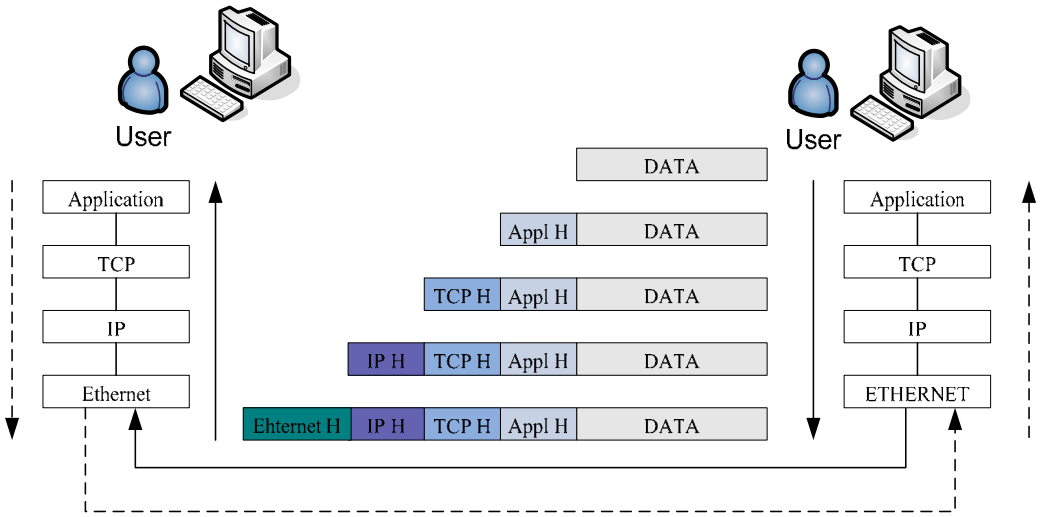
2. การส่งถ่ายข้อมูลระหว่างชั้นทีซีพี/ไอพี

โปรโตคอลในแต่ละชั้นล้วนมีหน้าที่เกี่ยวข้องในการส่งผ่านข้อมูลจากสถานีต้นทางไปยังสถานีปลายทาง ข้อมูลจะถูกส่งผ่านจากโปรโตคอลระดับบนสุดจากสถานีต้นทางไปยังระดับล่างจนกระทั่งข้อมูลถูกแปลงให้อยู่ในรูปของสัญญาณไฟฟ้า จึงส่งผ่านทางผ่านเครือข่ายไปยังสถานีปลายทางโปรโตคอลระดับล่างสุดที่สถานีปลายทางจะรับสัญญาณ และส่งผ่านขึ้นไปยังโปรโตคอลระดับบนต่อไป

เมื่อข้อมูลผ่านแต่ละระดับชั้น โปรโตคอลในชั้นนั้นจะผนวกข่าวสารกำกับการทำงานประจำโปรโตคอลซึ่งเรียกว่า โปรโตคอลเฮดเดอร์ (protocol header) เข้ากับข้อมูล เฮดเดอร์และตัวข้อมูลจากระดับบนจะถูกส่งผ่านไปยังระดับล่าง โปรโตคอลระดับล่างจะมองเฮดเดอร์และตัวข้อมูลรวมเป็นเสมือนข้อมูลและเพิ่มเฮดเดอร์ประจำชั้นเข้าไป ข้อมูลเดิมจึงมีเฮดเดอร์หุ้มเป็นชั้น ๆ กระบวนการนี้เรียกว่า การเอ็นแคปซูเลต (encapsulation)

เมื่อสถานีปลายทางได้รับแพ็กเก็ตก็จะดำเนินการส่งไปตามลำดับชั้น โปรโตคอลประจำชั้นจะถอดเฮดเดอร์ออกและส่งส่วนที่เหลือไปยังชั้นถัดไป เฮดเดอร์จะถูกถอดออกเหลือเฉพาะข้อมูลเมื่อถึงชั้นบนสุด กระบวนการนี้เรียกว่า การดีแคปซูเลต (decapsulation)

การเอ็นแคปซูเลตและการดีแคปซูเลต สามารถแสดงได้ดังรูปที่ 7 การเอ็นแคปซูเลตและดีแคปซูเลตของทีซีพี/ไอพี



ภาพที่ 7 แสดงการเอ็นแคปซูเลตและดีแคปซูเลตแพ็กเก็ตของทีซีพี/ไอพี

Appl H : Application Header

TCP H : TCP Heard

IP H : IP Header

Ethernet H : Ethernet Header

3. การประมวลผลของอุปกรณ์ค้นหาเส้นทาง

จากผู้ผลิตอุปกรณ์ค้นหาเส้นทาง (Cisco 2007 b) ได้อธิบายเกี่ยวกับการประมวลผลของอุปกรณ์ค้นหาเส้นทาง เพื่อให้ทราบว่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางทำงานสูงหรือผิดปกติหรือไม่ โดยให้สังเกตหรือปฏิบัติ ดังนี้

3.1 โดยใช้คำสั่ง show process cpu

3.2 ประสิทธิภาพในการทำงานช้าลง (slow performanc)

3.3 การตอบสนองการทำงานช้าลงหรือหยุดทำงาน เช่น การตอบสนองของการใช้คำสั่ง telnet ไปยังอุปกรณ์ค้นหาเส้นทาง การตอบสนองเมื่อใช้การต่อผ่านคอนโซล (console port) การตอบสนองจากการใช้คำสั่ง ping หรืออุปกรณ์ค้นหาเส้นทางไม่มีการแพ็กเก็ตใหม่ไปยังอุปกรณ์ค้นหาเส้นทางตัวอื่น

แนวทางตรวจสอบและแก้ไขเมื่อการประมวลผลของอุปกรณ์ค้นหาเส้นทางมีค่าสูง มีวิธีดังนี้

- โดยการตรวจสอบว่าเครื่องคอมพิวเตอร์ในระบบเครือข่ายมี worm หรือไวรัสคอมพิวเตอร์หรือไม่ ถ้าหากตรวจสอบได้ว่าเป็น worm หรือไวรัส สามารถที่ใช้คำสั่ง access-list ควบคุมปัญหานี้ได้
- โดยการตรวจสอบจากใช้คำสั่ง show logging เพื่อตรวจสอบว่ามีข้อผิดพลาดเกิดขึ้นหรือไม่
- โดยการตรวจสอบการทำงานของแต่ละชนิดต่อไปนี้ ว่ามีการทำงานอยู่มากน้อยเพียงใด
    - ARP Input
    - BGP Router High CPU หรือ BGP Scanner High CPU
    - EXEC High CPU Utilization
    - Hybridge Input
    - IP Input
    - IP SNMP (Simple Network Management Protocol)

การอ่านค่าต่าง ๆ จากการใช้คำสั่ง show process cpu เมื่อใช้คำสั่งจะแสดงรายละเอียดดังนี้

CPU utilization for five seconds: X% / Y%;; one minute : Z%; five minutes : W%

PID Runtimes(ms) invokes uSecs 5Sec 1Min 5Min TTY Process

X : ค่าเฉลี่ยรวมทั้งหมดการทำงาน (interrupts และ process) เมื่อ 5 นาทีที่ผ่านมา โดยค่าการทำงานของซีพียูเท่ากับ X – Y

Y : ค่าเฉลี่ยการทำงานของ interrupts เมื่อ 5 นาทีที่ผ่านมา

Z : ค่าเฉลี่ยรวมทั้งหมดของการทำงาน เมื่อ 1 นาทีที่ผ่านมา

W : ค่าเฉลี่ยรวมทั้งหมดของการทำงาน เมื่อ 5 นาทีที่ผ่านมา

PID : Process ID

Runtimes : ค่าซีพียูที่ใช้ในการทำงาน (หน่วยเป็น milliseconds)

uSec : ค่า Microseconds ของของซีพียูที่ใช้ทำงานของแต่ละ process ที่อ้างถึง

5Sec : ค่าการทำงานของซีพียู เมื่อ 5 วินาทีที่ผ่านมา

1Sec : ค่าการทำงานของซีพียู เมื่อ 1 นาทีที่ผ่านมา

5Min : ค่าการทำงานของซีพียู เมื่อ 5 นาทีที่ผ่านมา

TTY : ค่า Terminal ที่กำลังทำงาน (0 – 2 : ภายใน 3 – 15 : จากภายนอก เช่น telnet)

Process : ชื่อของการทำงาน

4. วิธีการดักจับข้อมูลบนระบบเครือข่าย โดยวิธี Packet Sniffer

การใช้วิธี Packet Sniffer (เรืองไกร รังสิพล 2544 : 79-91) เป็นเครื่องมือสำหรับการดักอ่านแพ็กแก็ตข้อมูลที่มีการรับส่งบนเน็ตเวิร์ก เดิมทีคำว่า Sniffer นั้นเป็นเครื่องหมายทางการค้าซึ่งจดทะเบียนไว้โดยบริษัท Network Associates Inc. ในสหรัฐฯ เพื่อใช้ในผลิตภัณฑ์ของตนเองชื่อ Sniffer Network Analyzer ซึ่งเป็นโปรแกรมวิเคราะห์เน็ตเวิร์ก โดยอาศัยการดักอ่านข้อมูลทั้งหมดบนเน็ตเวิร์กมาทำการวิเคราะห์แยกแยะการใช้งานเน็ตเวิร์กออกไปตามโปรโตคอลที่ใช้งานกันอยู่ เพื่อช่วยในการวางแผน ตรวจสอบและแก้ไขข้อบกพร่องที่อาจมีขึ้นในเน็ตเวิร์ก แต่เนื่องจากคำนี้เป็นที่เรียกขานกันแพร่หลายจนเป็นที่เข้าใจกันว่าสนิฟเฟอร์เป็นเครื่องมือที่ดักอ่านข้อมูลบนเน็ตเวิร์ก ซึ่งหากจะเรียกให้ถูกต้องแล้วอุปกรณ์ประเภทนี้ควรจะเรียกว่า Network Wire Tapping Device สนิฟเฟอร์มีองค์ประกอบพื้นฐาน 4 ส่วนคือ

- Hardware หมายถึงอุปกรณ์อิเล็กทรอนิคส์ต่างๆ ที่สามารถดักอ่านสัญญาณจากเน็ตเวิร์กเข้ามาได้ และสามารถนำสัญญาณที่ได้ส่งต่อไปประมวลผลออกมาเป็นข้อมูลทางคอมพิวเตอร์ได้ ซึ่งมีหน้าที่หลักคือจัดการกับการรับข้อมูลในระดับฟิสิคัล เช่นระดับแรงดันสัญญาณรบกวนการแก้ไขข้อผิดพลาดของสัญญาณ อุปกรณ์นี้โดยทั่วไปก็คือเน็ตเวิร์กอะแดปเตอร์นั่นเอง

- Driver เป็นโปรแกรมระดับล่างที่ควบคุมการดักข้อมูลของฮาร์ดแวร์ และนำสัญญาณที่ได้จากฮาร์ดแวร์ไปเก็บเป็นข้อมูลดิบรอการประมวลผลในลำดับถัดไป

- Buffer เป็นหน่วยความจำที่ใช้พักข้อมูลจากการดักมาได้ของ Driver โดยจะทำการจัดเก็บเพียงชั่วคราว และหมุนเวียนข้อมูลใหม่เข้ามาเสมอเมื่อมีข้อมูลใดปรากฏขึ้นบนเน็ตเวิร์ก กลไกการนำข้อมูลจากไดรเวอร์มาเก็บยังบัฟเฟอร์นี้จะเป็นตัวบ่งบอกสมรรถนะของการดัก ข้อมูลของสนิฟเฟอร์นั้นว่าจะสามารถดักข้อมูลได้ความเร็วสูงสุดเท่าใด หากกระบวนการนำข้อมูลไปเก็บเป็นไปอย่างล่าช้า ย่อมทำให้สนิฟเฟอร์ไม่สามารถดักข้อมูลที่อยู่บนเน็ตเวิร์กได้ทันและต้องปล่อยข้อมูลนั้นทิ้งไป

- Software เพื่อทำหน้าที่จัดการข้อมูลที่ได้รับเข้ามาโดยการประมวลผลตามวัตถุประสงค์ของการดักอ่านข้อมูลนั้น เนื่องจากข้อมูลดิบที่ดักอ่านขึ้นมาได้นั้นจะเป็นข้อมูลในระดับต่ำ คือ Data Link Layer ซึ่งจะมีข้อมูลที่ยังไม่ได้ผ่านการดีมัลติเพล็กซ์และจัดรูปแบบให้เข้าใจได้ สิ่งที่ได้จะเป็นข้อมูลเลขฐานสอง 0 กับ 1 จำนวนมหาศาลที่ต้องมาแปลความหมายกันอีกอีกประการหนึ่งคือข้อมูลที่ดักอ่านมาได้นั้นเป็นข้อมูลจากการสื่อสารของทุก ๆ โฮสต์ที่ใช้เน็ตเวิร์กนั้นร่วมกันอยู่ ผสมปนเปกันอย่างไร้ระเบียบและไม่มีการแยกแยะว่าเป็นการสื่อสารเรื่องอะไรระหว่างโฮสต์ใดกับโฮสต์ใด การที่จะแปลความหมายของข้อมูลเหล่านี้ได้ก็จำเป็นอย่างยิ่งที่จะต้อง

มีโปรแกรมสำหรับทำหน้าที่จัดการกับกองข้อมูลขนาดใหญ่นี้ให้อยู่ในรูปแบบที่สามารถเข้าใจได้มากขึ้น นั่นคือทำหน้าที่คล้ายคลึงกับการดีมัลติเพล็กของโปรโตคอลปกติ แต่จะมีข้อแตกต่างคือจะเป็นการดีมัลติเพล็กซ์ของข้อมูลทุก ๆ โฮสต์โดยไม่สนใจว่าเป็นข้อมูลของโฮสต์ใด

หลังจากข้อมูลผ่านการดีมัลติเพล็กซ์แล้วก็จะอยู่ในรูปที่สามารถเข้าใจได้ง่ายขึ้น มัลติเพล็กซ์ได้จนถึงโปรโตคอลเลเยอร์ที่สูงเช่น HTTP, SMTP สนิฟเฟอร์ส่วนใหญ่จึงทำให้การเก็บข้อมูลดิบไว้ก่อนแล้วค่อยนำมาประมวลผลในภายหลัง ซึ่งจะมีประสิทธิภาพและความเที่ยงตรงมาก และเครื่องคอมพิวเตอร์เป็นฮาร์ดแวร์ที่นิยมนำมาเป็นสนิฟเฟอร์มากที่สุด

การที่สนิฟเฟอร์สามารถดักอ่านข้อมูลที่อยู่บนเน็ตเวิร์กได้นั้นมีสาเหตุที่สำคัญคือ ด้วยลักษณะของโปรโตคอลอีเธอร์เน็ตที่ใช้หลักการกระจายของข้อมูลไปยังทุกโฮสต์ที่อยู่ในเน็ตเวิร์กและอาศัยโฮสต์แต่ละตัวทำหน้าที่จำแนกการสื่อสารของตนเอง นั่นหมายความว่าข้อมูลทุกแพ็กเก็ตที่ใช้สื่อสารกันนั้นได้ถูกต้องนั้นโฮสต์แต่ละตัวจะต้องมีกระบวนการที่สามารถรู้ได้ว่าข้อมูลแพ็กเก็ตใดเป็นของตนเอง และข้อมูลแพ็กเก็ตใดมิใช่ของตนเอง ทุกๆ แพ็กเก็ตที่กระจายลงบนเน็ตเวิร์กนั้นจะมีหมายเลขระบุชัดเจนคือ MAC Address ซึ่งจะเป็นสิ่งที่บอกว่าแพ็กเก็ตมาจากฮาร์ดแวร์ใดในเน็ตเวิร์ก ทำให้สามารถระบุได้ว่าแพ็กเก็ตนั้นส่งมาจากโฮสต์ใด และต้องการส่งให้โฮสต์ใด โหมดการทำงานที่อนุญาตให้ฮาร์ดแวร์รับข้อมูลของผู้อื่นเข้ามาได้โดยไม่มีการปิดกั้นนั้นเรียกว่า โพรมิสคูอัสโหมด (Promiscuous Mode) เป็นโหมดที่ทำให้ฮาร์ดแวร์อ่านข้อมูลดิบทั้งหมดบนเน็ตเวิร์กเข้ามาในเครื่องคอมพิวเตอร์ของตนเองได้โดยไม่สนใจว่าจะเป็นของใคร ส่งให้ใครและเป็นการละเมิดข้อบังคับของโปรโตคอลหรือไม่

5. งานวิจัยที่เกี่ยวข้อง

งานวิจัย ระบบกระจายการตรวจวัดและเฝ้าดูการส่งข้อมูลในระบบเครือข่าย (ไพศาล ไตรชวโรจน์ 2547) ได้ศึกษาระบบกระจายการตรวจจับและเฝ้าดูการส่งผ่านข้อมูลในระบบเครือข่ายของมหาวิทยาลัย ด้วยวิธีดักจับข้อมูลในลักษณะของโปรแกรม Packet Sniffer และโปรแกรม Visual C# และโปรแกรม ASP.Net ในการพัฒนาระบบด้วย การดักจับข้อมูลที่ส่งผ่านระบบเครือข่าย การศึกษาให้ความสนใจเกี่ยวกับโปรโตคอล TCP, UDP, ICMP และ ARP โดยวัดผลการตรวจจับและเฝ้าดูในเชิงปริมาณ เพื่อวัดความแออัดบนระบบเครือข่ายและประเมินประสิทธิภาพของระบบเครือข่าย สามารถรองรับการทำงานได้หรือไม่ และวิเคราะห์ผลว่าเป็นไปตามจุดประสงค์ของการติดตั้งและออกแบบไว้หรือไม่ โดยสรุปปริมาณการใช้งานบนระบบเครือข่ายตามคาบเวลาที่กำหนดไว้ จากผลการประเมินประสิทธิภาพความถูกต้องของระบบอยู่ใน

เกณฑ์ที่มีประสิทธิภาพดีมากและเป็นมาตรฐาน ระบบมีการจำแนกประเภทจำนวนขนาดของข้อมูลได้อย่างถูกต้อง

งานวิจัย ระบบวิเคราะห์ข้อมูลผู้บุกรุกแจ้งเตือนไปยังโทรศัพท์มือถือ (สันติ ดลนภาเขตดำเกิง 2547) ได้ศึกษาวิธีการดักจับข้อมูลผู้บุกรุกด้วยโปรแกรม Snort และ Swatch เพื่อตรวจวัดพฤติกรรมการส่ง ICMP Echo Request จำนวนมาก (Ping Flooding) การส่ง TCP SYN แพ็กเก็ตจำนวนมาก (SYN Flooding) การลักลอบสแกนต์พอร์ต (Stealth Post Scan) การสแกนหาระบบปฏิบัติการ (OS Determination Scan) และโจมตีเว็ปไซต์โดยใช้ช่องโหว่ของซีจีไอ (Web CGI Attack) จากการประเมินผลของระบบถือว่าสามารถวิเคราะห์ข้อมูลผู้บุกรุกแต่ละประเภทได้ในเกณฑ์ดี

งานวิจัย การจัดการแบนท์วิธในเครือข่ายด้วยลินุกซ์ (สุทธิชัย สุทธิทศธรรม 2550) ได้ศึกษาโดยการใช้ระบบปฏิบัติการลินุกซ์ร่วมกับการใช้โปรแกรม tc (Traffic Control) และโปรแกรม iptables มาพัฒนาการสร้างกฎของการใช้แบนด์วิธของแต่ละเครื่องคอมพิวเตอร์หรือกลุ่มเครื่องคอมพิวเตอร์ (IP Address หรือ Subnet)โดยควบคุมปริมาณการใช้ทราฟฟิก ด้วยวิธีการกำหนดพารามิเตอร์ เช่น Priority ความเร็วขั้นต่ำ และความเร็วสูงสุด เป็นต้น ซึ่งโปรแกรม tc สามารถแยกแพ็กเก็ตออกตามคลาสหรือหมวดหมู่ที่กำหนดไว้ได้ จากนั้นนำผลที่แยกหมวดหมู่ไปใช้ในนโยบาย (Policy) ที่กำหนดไว้ เช่น ถ้าหากอัตราความเร็วเข้ามาเกินที่กำหนดไว้สูงสุดลินุกต์จะทำการลบแพ็กเก็ตทิ้งไปหรือใช้การ burst ของแพ็กเก็ต จากผลการวิจัยพบว่าสามารถควบคุมและจัดการแบนด์วิธได้ในระดับที่น่าพอใจ จากงานของสุทธิชัย ผู้พัฒนาระบบจำกัดการประมวลผลอุปกรณ์ค้นหาเส้นทาง ได้นำเทคนิคการควบคุมแบนท์วิธการรับส่งข้อมูลบนระบบเครือข่าย การกำหนดความสำคัญผู้ใช้ (Priority) การเปิดหรือปิดช่องทางการติดต่อสื่อสารมาพัฒนากฎหรือนโยบายควบคุมการส่งผ่านแพ็กเก็ตไปยังอุปกรณ์ค้นหาเส้นทาง สำหรับควบคุมหรือกำจัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง เพื่อให้เป็นไปตามเป้าหมายที่วางไว้

บทที่ 3
วิธีการดำเนินการวิจัย

การดำเนินงานของการพัฒนาระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง ผู้พัฒนาใช้โปรแกรมที่เป็น Open Source มาใช้พัฒนาเป็นหลัก และแบ่งขั้นตอนการดำเนินการวิจัยครั้งนี้ แบ่งเป็น 5 ขั้นตอน ดังนี้

ขั้นตอนที่ 1 การศึกษาและออกแบบระบบ

ขั้นตอนที่ 2 การพัฒนาระบบ

ขั้นตอนที่ 3 การทดสอบบนระบบเครือข่ายต้นแบบ (Prototype Network System)

ขั้นตอนที่ 4 การทดสอบบนระบบเครือข่ายจริง

ขั้นตอนที่ 5 การสรุปผลและทำรายงาน

รายละเอียดในแต่ละขั้นตอนแสดงดังนี้

1. การศึกษาและออกแบบระบบ

1.1 ขั้นตอนการศึกษาระบบ

ขั้นตอนในการศึกษาระบบ จะศึกษาถึงปัจจัยหรือสาเหตุต่าง ๆ ที่มีผลต่อการประมวลผลของอุปกรณ์ค้นหาเส้นทาง โดยศึกษาเครื่องมือที่มีอยู่ในระบบ Open Source เพื่อใช้สำหรับข้อมูลที่ส่งผ่านบนระบบเครือข่ายคอมพิวเตอร์ เครื่องมือสำหรับควบคุมรับส่งข้อมูล (traffic control) และเครื่องมือสำหรับเปิดหรือปิดการรับส่งข้อมูล (firewall) เพื่อนำข้อมูลที่ได้มาศึกษาวิเคราะห์และออกแบบระบบในขั้นตอนต่อไป ซึ่งจากการศึกษาผู้พัฒนาได้เขียนโปรแกรมด้วยภาษา perl, และ php มาใช้ในการตรวจจับ ควบคุม เปิดและปิดการรับส่งข้อมูลในระบบเครือข่ายคอมพิวเตอร์ และระบบแจ้งเตือน เก็บสถิติและรายงานผลผ่านเว็บ ซึ่งทำให้ผู้ดูแลระบบสามารถรับข่าวได้อย่างทันท่วงที และสามารถตรวจสอบผลผ่านเว็บไซต์ และจากการศึกษาผู้พัฒนาได้แบ่งขั้นตอนการศึกษาและการดำเนินงาน ดังนี้

1.1.1 ศึกษาการทำงานและคำสั่งต่าง ๆ ในการจัดการอุปกรณ์ค้นหาเส้นทาง

1.1.2 ศึกษาถึงปัจจัยหรือสาเหตุ ที่ทำให้การประมวลผลของอุปกรณ์ค้นหาเส้นทางทำงานมากหรือทำให้ cpu utilization สูงขึ้น หรือทำงานช้า หรือหยุดการทำงานการรับส่งผ่านข้อมูล

1.1.3 ศึกษาวิธีการตรวจจับผู้บุกรุกและวิธีการบุกรุกในรูปแบบต่าง ๆ

1.1.4 ศึกษาการทำงานของโปรแกรม tc, cbq, iptables

1.1.5 ศึกษาการรับส่งข้อมูลผ่านระบบเครือข่ายคอมพิวเตอร์ ตั้งแต่เริ่มรับส่งและสิ้นสุดการรับส่งในแต่ละครั้ง

1.1.6 ศึกษาการทำงานของระบบปฏิบัติการลินุกซ์

1.1.7 ศึกษาการเขียนโปรแกรมบนระบบปฏิบัติการลินุกซ์

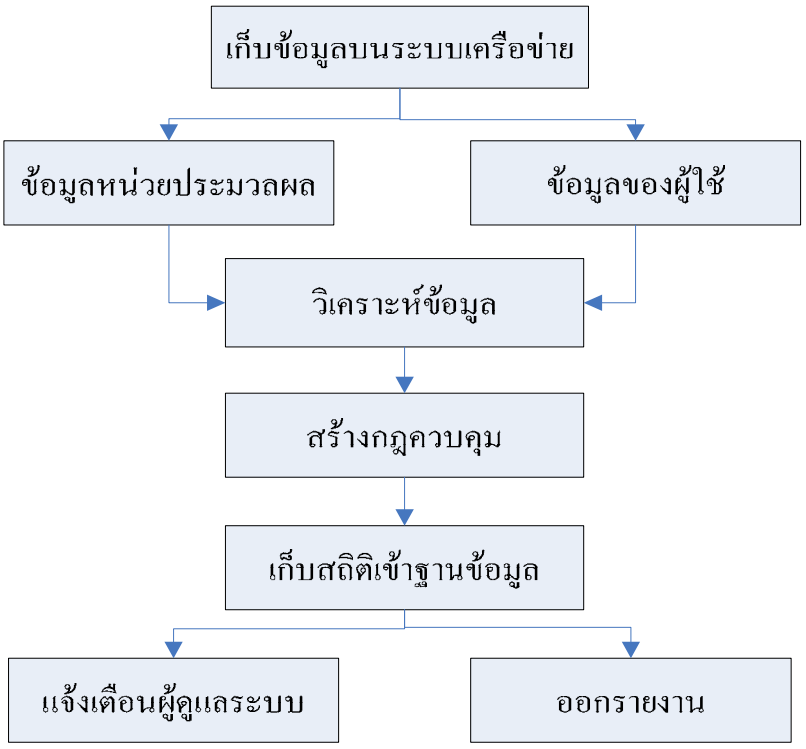
1.1.8 ศึกษาการทำงานของโปรแกรม mrtg และ rrdtools เพื่อใช้สำหรับแสดงผลการทำงานรับส่งผ่านข้อมูลของระบบที่พัฒนา แสดงสถิติการทำงานของการประมวลผลของอุปกรณ์ค้นหาเส้นทาง

1.1.9 ศึกษาและติดตั้งระบบปฏิบัติการลินุกซ์บนเครื่องไมโครคอมพิวเตอร์เพื่อใช้ทำหน้าที่เป็นอุปกรณ์ค้นหาเส้นทาง (linux pc router)

1.1.10 ศึกษาระบบ log file ของโปรแกรม Check Point

1.2 ขั้นตอนการออกแบบระบบ

การออกแบบระบบจำกัดการประมวลผลอุปกรณ์ค้นหาเส้นทาง ได้ออกแบบขั้นตอนการทำงานดังไดอะแกรมภาพที่ 8 แสดงการวิเคราะห์และออกแบบระบบ ซึ่งแต่ละส่วนมีรายละเอียดดังนี้



ภาพที่ 8 แสดงการวิเคราะห์และออกแบบระบบ

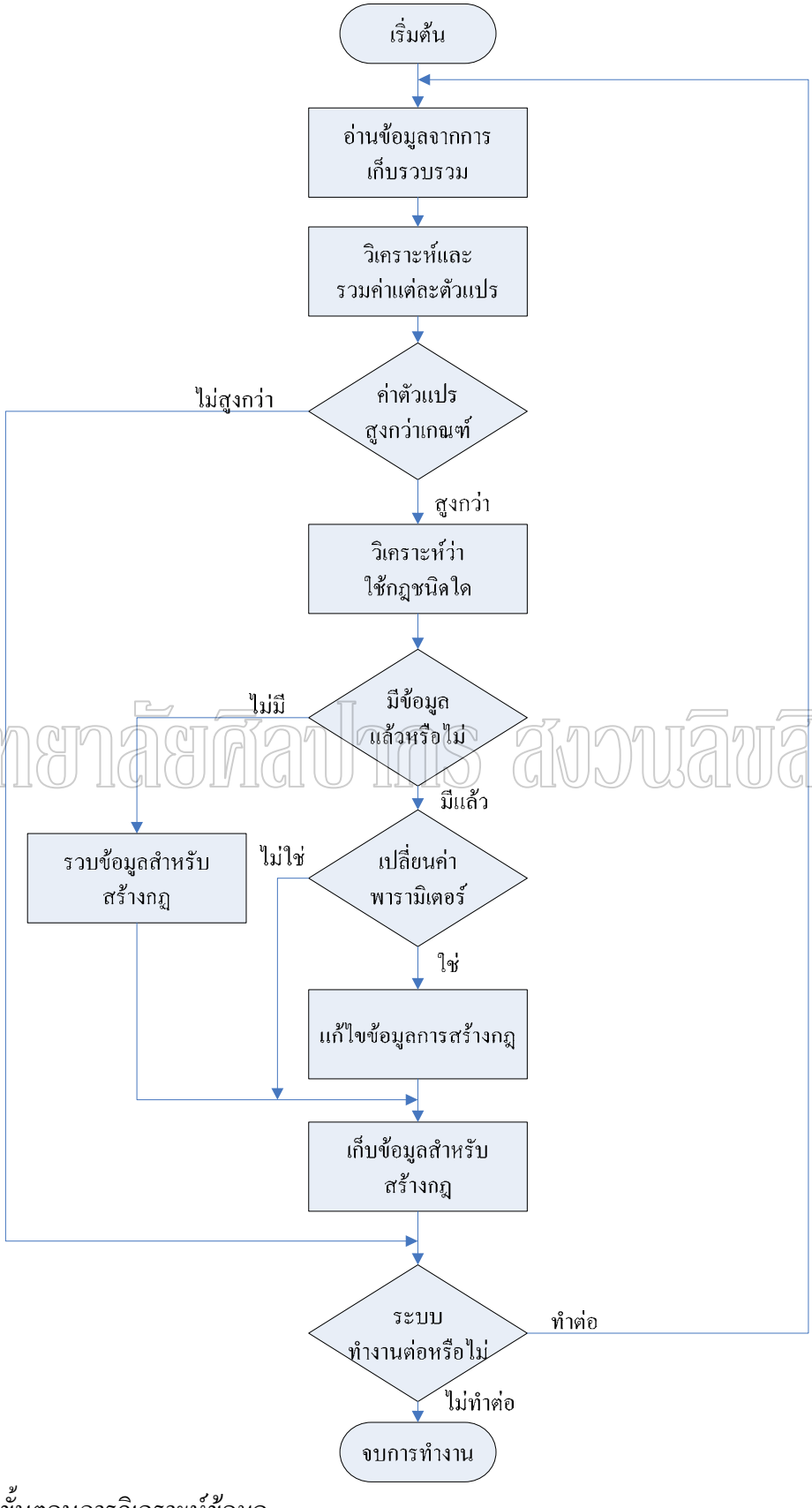
1.2.1 การเก็บข้อมูลบนระบบเครือข่าย

ในขั้นตอนนี้แบ่งเป็น 2 ส่วน คือ ส่วนแรก การเก็บข้อมูลเพื่อใช้เป็นข้อมูลต้นแบบ สำหรับการศึกษาวิเคราะห์ และนำไปใช้พัฒนาการจำลองการทำงานของระบบ โดยเก็บข้อมูลการประมวลผลของอุปกรณ์ค้นหาเส้นทาง (Router CPU Utilization) ผ่านโปรโตคอลเอสเอ็นเอ็มพี (SNMP : Simple Network Management Protocol) และข้อมูลการใช้งานบนระบบเครือข่ายของผู้ใช้ (Network Traffic) จากโปรแกรมที่พัฒนาขึ้นด้วยภาษา Perl แต่ข้อมูลที่จัดเก็บนั้นจะเลือกเก็บเฉพาะช่วงเวลาที่ค่าเฉลี่ยของการประมวลผลของอุปกรณ์ค้นหาเส้นทางมีค่าตั้งแต่ 90 เปอร์เซ็นขึ้นไปเท่านั้น และเก็บข้อมูลครั้งละ 5 นาที

ส่วนที่สอง การเก็บข้อมูลสำหรับการทำงานของระบบ ในส่วนของการเก็บข้อมูลการประมวลของอุปกรณ์ค้นหาเส้นทางนั้น จะเก็บข้อมูลเมื่อเวลาผ่านไปทุก 30 วินาที และเก็บค่าเฉลี่ยของการประมวลผลที่ 5 วินาที 1 นาที และ 5 นาที จากโปรแกรมที่พัฒนาขึ้นด้วยภาษา Perl ผ่านโปรโตคอลเทลเน็ท (telnet) และสำหรับข้อมูลการใช้งานบนระบบเครือข่ายของผู้ใช้นั้นจะแบ่งการจัดเก็บออกเป็น 4 ช่วง ช่วงเวลาละ ๆ 10 นาที หมุนเวียนกันไป และลบข้อมูลช่วงนั้นออกจากฐานข้อมูล ถ้าพบว่าในช่วงเวลานั้นค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางมีค่าไม่เกิน threshold ที่กำหนดไว้ แต่ถ้าสูงกว่าจะนำข้อมูลไปวิเคราะห์เพื่อสร้างกฎควบคุมต่อไป

1.2.2 การวิเคราะห์ข้อมูล

ในขั้นตอนนี้เป็นการวิเคราะห์หาสาเหตุว่าอะไรเป็นต้นเหตุ ที่ทำให้การทำงานของการประมวลผลของอุปกรณ์ค้นหาเส้นทาง สูงกว่าค่า threshold ซึ่งจะต้องหาให้ได้ว่า ไอพีแอดเดรสใดได้ติดต่อไปไอพีแอดเดรสใด และใช้บริการอะไรหรือใช้พอร์ตอะไรติดต่อกัน หรือมีจำนวนเซสชั่น (session) มากน้อยเพียงใด ตลอดจนมีขนาดของข้อมูลในการรับส่งเล็กหรือใหญ่ในช่วงเวลาก่อนที่ค่าการประมวลผลการทำงานของอุปกรณ์ค้นหาเส้นทาง จะมีค่าสูงเกินค่า threshold แล้วนำข้อมูลที่ได้มาสร้างกฎควบคุมการรับส่งข้อมูลผ่านระบบ ซึ่งเขียนผังดำเนินงานได้ดังภาพที่ 9 ขั้นตอนการวิเคราะห์ข้อมูล



ภาพที่ 9 ขั้นตอนการวิเคราะห์ข้อมูล

1.2.3 การสร้างกฎควบคุม

ในขั้นตอนนี้เป็นขั้นตอนกำหนดกฎควบคุมการรับส่งข้อมูล โดยใช้ความสามารถของโปรแกรม cbq และโปรแกรม iptables ทำหน้าที่ควบคุม โดยมุ่งเน้นให้ผู้ใช้ยังคงสามารถติดต่อสื่อสารได้เหมือนก่อนมีการควบคุม มากกว่าการยับยั้งไม่ให้ใช้งาน และติดตามผลกฎที่สร้างขึ้นมาสามารถควบคุมการประมวลผลของอุปกรณ์ค้นหาเส้นทางให้มีค่าลดลงมาอยู่ในเกณฑ์ที่กำหนดหรือไม่ เมื่อมีการปรับค่าพารามิเตอร์ให้เหมาะสม จากนั้นเก็บข้อมูลที่ได้ลงฐานข้อมูล ซึ่งการสร้างกฎควบคุมมีอยู่ 2 วิธี คือ วิธีแรก การสร้างกฎโดยผู้ดูแลระบบหรือผู้พัฒนาเป็นผู้กำหนดเงื่อนไขขึ้นเอง (Manual Policy) โดยอาศัยข้อมูลที่ได้ศึกษาวิเคราะห์มาจากเอกสารหรืองานวิจัยต่าง ๆ เช่น โปรโตคอลที่ใช้ในการติดต่อสื่อสาร ลักษณะของโปรแกรมที่ใช้งาน พอร์ตที่เปิดให้บริการหรือเครื่องคอมพิวเตอร์ที่ได้รับการยกเว้น เป็นต้น และกฎที่สร้างขึ้นมานี้อาจมีการเปลี่ยนแปลงค่าพารามิเตอร์ให้เหมาะสมตามสภาวะการใช้งาน วิธีที่สอง การสร้างกฎแบบให้ระบบเรียนรู้ โดยระบบจะนำข้อมูลที่ได้จากขั้นตอนการวิเคราะห์ข้อมูลมาสร้างกฎควบคุม

ระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง ผู้วิจัยได้ออกแบบการสร้างกฎควบคุมเป็น 3 วิธี คือ การควบคุมปริมาณของข้อมูลที่รับส่ง (Bandwidth Model) การกำหนดความสำคัญของข้อมูล (Priority Model) และการป้องกันการส่งข้อมูล (Deny Model) ซึ่งแต่ละวิธีมีรายละเอียด ดังนี้

1.2.3.1 การควบคุมปริมาณของข้อมูลที่รับส่ง (Bandwidth Model) เป็นวิธีควบคุมปริมาณของข้อมูลที่รับส่ง เมื่อตรวจพบว่ามีไอพีแอดเดรสเครื่องคอมพิวเตอร์ของผู้ใช้ รับหรือส่งข้อมูลปริมาณมาก จนกระทั่งทำให้ค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทาง (Router CPU Utilization) มีค่าสูงกว่า threshold ที่กำหนดไว้ ซึ่งวิธีนี้จะกำหนดขนาดแบนท์วิธการรับหรือส่งให้กับไอพีแอสเดรสเครื่องคอมพิวเตอร์ที่ตรวจพบ

1.2.3.2 การกำหนดความสำคัญของข้อมูล (Priority Model) เป็นวิธีกำหนดความสำคัญ (priority) ของการรับหรือส่งข้อมูล เมื่อตรวจพบว่ามีไอพีแอดเดรสเครื่องคอมพิวเตอร์ของผู้ใช้ ได้สร้างการเชื่อมต่อ (connection) เพื่อรับหรือส่งข้อมูลบนระบบเครือข่ายจำนวนมากไปยังเครื่องคอมพิวเตอร์เครื่องใดเครื่องหนึ่ง แต่ข้อมูลที่รับหรือส่งมีปริมาณไม่มากหรือไม่สูงกว่า threshold ของ Bandwidth Model แต่ทำให้ค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทาง (Router CPU Utilization) มีค่าสูงกว่า threshold ที่กำหนดไว้ ระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง จะลดระดับความสำคัญ (priority) การรับหรือส่งข้อมูลของไอพีแอดเดรสเครื่องคอมพิวเตอร์ที่ตรวจพบ จากระดับความสำคัญสูงสุดที่ระดับความสำคัญเป็น 7 มาเป็นระดับ 3 สำหรับการตรวจพบครั้งแรก และเป็นระดับ 1 สำหรับการตรวจพบครั้งที่ 2

1.2.3.3 การป้องกันการส่งข้อมูล (Deny Model) สำหรับวิธีนี้ผู้วิจัยให้ความสำคัญมากที่สุด เนื่องจากการประมวลผลของอุปกรณ์ค้นหาเส้นทางมีค่าสูงได้จากหลายสาเหตุ เมื่อระบบตรวจพบว่าไอพีแอดเดรสเครื่องคอมพิวเตอร์ของผู้ใช้ มีการรับส่งข้อมูลปริมาณมากและมีการสร้างการเชื่อมต่อ (connection) การรับหรือส่งข้อมูลจำนวนมากไปยังเครื่องคอมพิวเตอร์จำนวนมากพร้อมกัน หรือการส่งข้อมูลในลักษณะเดียวกับการทำ sync flood หรือ scan port แล้วทำให้ค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทาง (Router CPU Utilization) มีค่าสูงกว่า threshold ถ้าตรวจพบครั้งแรก จะใช้ทั้งวิธีการควบคุมปริมาณของข้อมูลที่รับส่ง (Bandwidth Model) ที่ระดับต่ำสุด (128 Kbps) และการกำหนดระดับความสำคัญที่ระดับต่ำสุด (ระดับ 1) ถ้าตรวจพบเป็นครั้งที่สอง จะยับยั้งการรับและส่งข้อมูลของเครื่องคอมพิวเตอร์ที่ตรวจพบนี้ชั่วคราวเป็นเวลา 15 นาที จากนั้นจะยกเลิกการควบคุม แต่ถ้ายังตรวจพบว่ายังทำผิดกฎนี้อีก 3 ครั้งติดต่อกัน ระบบจะปิดกั้นอย่างถาวร จนกว่าผู้ดูแลระบบจะมาแก้ไข

1.2.4 การเก็บสถิติลงฐานข้อมูล

การออกแบบการเก็บสถิติลงฐานข้อมูล ผู้วิจัยใช้ระบบการจัดการฐานของ MySql ในการเก็บข้อมูล และออกแบบโครงสร้างฐานข้อมูล ซึ่งมีตาราง (table) ที่เก็บข้อมูล ดังนี้

1.2.4.2 ตาราง RcpuTab ใช้สำหรับเก็บค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทาง มีรายละเอียดโครงสร้าง ดังนี้

ลำดับที่	ชื่อ field	คำอธิบาย	ความยาว	ชนิด
1	Rip	IP Address ของอุปกรณ์ค้นหาเส้นทาง	6	Varchar
2	UnitTime	วันที่และเวลาจัดเก็บเป็นเวลาแบบ unix	-	Tinytext
3	Fsecond	ค่าเฉลี่ยการประมวลผลที่ 5 วินาที	2	Tinyint
4	OneMin	ค่าเฉลี่ยการประมวลผลที่ 1 นาที	2	Varchar
5	FiveMin	ค่าเฉลี่ยการประมวลผลที่ 5 นาที	2	Varchar
6	TimeStamp	วันที่และเวลาจัดเก็บข้อมูล	-	Timestamp

1.2.4.3 ตาราง PacketCap11, PacketCap12, PacketCap21 และ PacketCap22 ใช้สำหรับเก็บข้อมูลการใช้งานบนระบบเครือข่าย มีรายละเอียดโครงสร้าง ดังนี้

ลำดับที่	ชื่อ field	คำอธิบาย	ความยาว	ชนิด
1	SaveTime	เวลาที่เก็บข้อมูลเป็นแบบ Unix	10	Varchar
2	Src_IP	หมายเลขไอพีแอดเดรสของผู้ใช้ต้นทาง	16	Varchar
3	Src_Port	พอร์ตที่ใช้ของผู้ใช้ต้นทาง	5	Smallint
4	Dest_IP	หมายเลขไอพีแอดเดรสของผู้ใช้ปลายทาง	16	Varchar
5	Dest_Port	พอร์ตที่ใช้ของผู้ใช้ปลายทาง	2	Varchar
6	Protocal	ชนิดของโปรโตคอลที่ใช้ (16 = TCP, 17 = UDP)	4	Varchar
7	Plength	ขนาดของแพ็กเก็ตข้อมูล	6	Smallint
8	Flags	ค่าสถานะการรับส่งข้อมูล	4	Tinyint
9	Fdata	ตัวอย่างข้อมูล 16 ไบท์แรก	16	Varchar

1.2.4.4 ตาราง Use1MinTab และ Use5MinTab ใช้ในการเก็บข้อมูลที่ได้จากการวิเคราะห์ข้อมูล มีรายละเอียดโครงสร้าง ดังนี้

ลำดับที่	ชื่อ field	คำอธิบาย	ความยาว	ชนิด
1	SaveTime	เวลาที่เก็บข้อมูลเป็นแบบ Unix	10	Int (auto)
2	Client_IP	หมายเลขไอพีแอดเดรสของผู้ใช้	16	Varchar
3	BWupload	ปริมาณข้อมูลที่ส่งออก หน่วยเป็นไบท์ผ่านโปรโตคอลทีซีพี	11	Bigint
4	BWdown	ปริมาณข้อมูลที่รับเข้า หน่วยเป็นไบท์ ผ่านโปรโตคอลทีซีพี	11	Bigint
5	ConnUp	จำนวนครั้งการเชื่อมต่อเพื่อส่งข้อมูลผ่านโปรโตคอลทีซีพี	10	Int
6	ConnDown	จำนวนครั้งการเชื่อมต่อเพื่อรับ	10	Int

		ข้อมูล ผ่านโปรโตคอลทีซีพี		
7	BadBWUp	ปริมาณข้อมูลที่ส่งออก หน่วยเป็นไบท์ผ่านโปรโตคอลยูดีพีและโปรโตคอลอื่น ๆ	11	Bigint
8	BadBWDown	ปริมาณข้อมูลที่รับเข้า หน่วยเป็นไบท์ ผ่านโปรโตคอลยูดีพีหรือโปรโตคอลอื่น ๆ	11	Bigint
9	BadConnUp	จำนวนครั้งการเชื่อมต่อเพื่อส่งข้อมูลผ่านโปรโตคอลยูดีพีหรือโปรโตคอลอื่น ๆ	10	Int
10	BadConnDown	จำนวนครั้งการเชื่อมต่อเพื่อรับข้อมูล ผ่านโปรโตคอลยูดีพีหรือโปรโตคอลอื่น ๆ	10	Int

1.2.4.5 ตาราง RuleTab ใช้ในการเก็บข้อมูลเพื่อใช้สร้างกฎและการออกรายงาน มีรายละเอียดโครงสร้าง ดังนี้

ลำดับที่	ชื่อ field	คำอธิบาย	ความยาว	ชนิด
1	RuleNo	ลำดับที่การรายงาน	10	int (auto)
2	RuleModel	ชนิดของกฎ (1 = Bandwidth Model 2 = Priority Model 3 = Deny Model)	20	Varchar
3	RuleIP	หมายเลขไอพีแอดเดรสที่ถูกควบคุม	10	Varchar
4	RuleTime	เวลาที่สร้างกฎ แบบ Unit	10	Varchar
5	RuleBWUp	ปริมาณข้อมูลที่ส่งออกทั้งหมด หน่วยเป็นไบท์		
6	RuleBWDW	ปริมาณข้อมูลที่รับเข้าทั้งหมด หน่วยเป็นไบท์		
7	RuleConnUp	จำนวนครั้งการเชื่อมต่อเพื่อส่งข้อมูล		

		ทั้งหมด		
8	RuleConnDW	จำนวนครั้งการเชื่อมต่อเพื่อรับข้อมูลทั้งหมด		
9	RuleCount	ชนิดของการดำเนินการ (01 = สร้างกฎใหม่ 02 = แก้ไขความสำคัญ (Priority) 03 = แก้ไขความเร็วที่กำหนด 04 = แก้ไขความเร็วที่ใช้สูงสุด 99 = ยกเลิกกฎ)	2	Varchar
10	RuleRate	ขนาดแบนท์วิธที่ควบคุมการใช้งาน	255	Varchar
11	RulePrio	ระดับความสำคัญของการใช้งาน	255	Varchar
12	RuleAlert	รูปแบบการส่งแจ้งผู้ดูแลระบบ (0 = ยังไม่ได้แจ้ง 1 = แจ้งทางอีเมล์ 2 = แจ้งข้อความเข้ามือถือ 3 = แจ้งทางอีเมล์และส่งข้อความไปยังมือถือ)	1	Int
13	RuleCreate	วันที่และเวลาที่สร้างกฎ	-	Datetime
14	RuleUpdate	วันที่และเวลาที่เปลี่ยนแปลงล่าสุด	-	Datetime

1.2.5 การแจ้งเตือนผู้ดูแลระบบ

การแจ้งเตือนผู้ดูและระบบนั้น การวิเคราะห์และออกแบบระบบ ได้ออกแบบเป็น 2 แบบ คือ

1.2.5.2 การแจ้งเตือนผู้ดูแลระบบโดยส่งข้อความสั้น ๆ (short message) เฉพาะภาษาอังกฤษ ไปยังระบบมือถือ

1.2.5.3 การแจ้งเตือนผู้ดูแลระบบโดยส่งข้อความผ่านระบบอีเมล์ (e-mail)

1.2.6 การออกรายงาน

การออกรายงาน ผู้วิจัยได้พัฒนาโปรแกรมด้วยภาษา Perl และภาษา php ซึ่งได้ออกแบบเป็น 3 ส่วนหลัก คือ

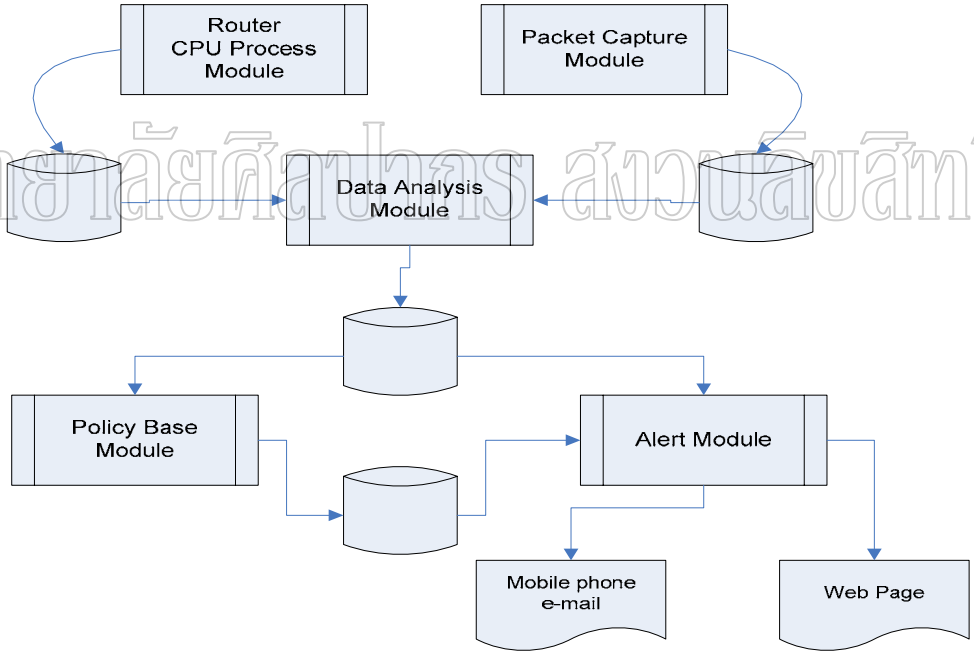
1.2.6.2 การออกรายงาน เพื่อแสดงการทำงานของระบบผ่านเว็บ ซึ่งมีรายละเอียดปริมาณข้อมูลที่รับและส่งผ่านระบบเครือข่าย รายละเอียดข้อมูลการเชื่อมต่อ (connection)

1.2.6.3 การออกรายงาน เพื่อแสดงว่ามีกฎอะไรบ้างที่ระบบกำลังทำงานอยู่หรือที่เคยใช้ในรูปของโฮมเพจ โดยการเขียนโปรแกรม php ใช้ข้อมูลที่เก็บไว้ในฐานข้อมูล

1.2.6.4 การออกรายงาน เพื่อแสดงค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทาง โดยแสดงผลเป็นกราฟเส้น

2. การพัฒนาระบบ

การพัฒนาระบบ ได้พัฒนาขึ้นตามที่ได้ศึกษาและออกแบบไว้เป็นส่วน ๆ (Module) สามารถแสดงในลักษณะของผังดำเนินงานดังภาพที่ 10 การเชื่อมโยงของการพัฒนาระบบ



ภาพที่ 10 การเชื่อมโยงของการพัฒนาระบบ

จากภาพที่ 10 มีรายละเอียดในแต่ละส่วน (module) ดังนี้

Router CPU Process Module ทำหน้าที่อ่านข้อมูลการประมวลผลของอุปกรณ์ค้นหาเส้นทางทุก 30 วินาที จากนั้นบันทึกค่าที่อ่านได้ไปยังฐานข้อมูล RcpuDB ในตาราง RcpuTab

Packet Capture Module ทำหน้าที่อ่านค่าการรับส่งข้อมูลของผู้ใช้บนระบบเครือข่ายผ่านระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง จากนั้นบันทึกค่าที่อ่านได้ไปยังฐานข้อมูล RcpuDB ตาราง PacketCap11, PacketCap12, PacketCap21, PacketCap22 ตามลำดับเวลาในแต่ละช่วง

Data Analysis Module ทำหน้าที่อ่านค่าจากฐานข้อมูลตามที่ Router Process Module และ Packet Capture Module เก็บไว้ เพื่อทำงานวิเคราะห์ตามภาพที่ 9 จากนั้นเก็บผลที่ได้ไปยังฐานข้อมูล RcpuDB ตาราง Use1MinTab หรือลบข้อมูลจาก Packet Capture Module เก็บไว้ออกในกรณีที่ค่าของการประมวลผลของอุปกรณ์ค้นหาเส้นทางไม่เกินค่า threshold

Policy Base Module ทำหน้าที่นำผลที่ได้จากส่วนของ Data Analysis Module มาวิเคราะห์และสร้างกฎเพื่อจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง และบันทึกค่าของกฎไปยังฐานข้อมูลตาราง RuleTab

Alert Module ทำหน้าที่อ่านค่าที่ได้จาก Data Analysis Module และ Policy Base Module เพื่อนำมาออกรายงานและส่งอีเมล์หรือข้อความไปยังผู้ดูแลระบบ

3. การทดสอบบนระบบเครือข่ายต้นแบบ (Prototype Network System)

3.1 เครื่องมือที่ใช้ในระบบเครือข่ายต้นแบบ

เครื่องมือและซอฟต์แวร์ต่าง ๆ ที่ใช้สำหรับทดสอบระบบควบคุมการประมวลผลของอุปกรณ์ค้นหาเส้นทาง สามารถแบ่งได้เป็น 2 ส่วน คือ

3.1.1 เครื่องมือด้านฮาร์ดแวร์ (Hardware) ประกอบด้วย

ก) เครื่องคอมพิวเตอร์สำหรับติดตั้งระบบ จำนวน 1 เครื่อง

ข) เครื่องคอมพิวเตอร์สำหรับทำหน้าที่เป็นอุปกรณ์ค้นหาเส้นทางจำนวน 1 เครื่อง

ค) อุปกรณ์ค้นหาเส้นทางจำนวน 2 ชุด

ง) อุปกรณ์กระจายสัญญาณระบบเครือข่าย (switch) จำนวน 2 ชุด

จ) เครื่องคอมพิวเตอร์สำหรับทำหน้าที่เป็นเครื่องผู้ใช้ จำนวน 2 เครื่อง

ฉ) Network card สำหรับเครื่องติดตั้งระบบ จำนวน 3 การ์ด

3.1.2 เครื่องมือด้านซอฟต์แวร์ ประกอบด้วย

ก) ระบบปฏิบัติการลินุกซ์ CentOS 5.2

ข) ระบบปฏิบัติการวินโดวส์ XP

ค) โปรแกรมควบคุมการรับส่งข้อมูล cbq 0.73

ง) โปรแกรมให้บริการโฮมเพจ apache server 2.2.3

จ) โปรแกรม perl 5.8, php5

ฉ) โปรแกรมแสดงกราฟสถิติการทำงาน mrtg

ช) โปรแกรมจัดการฐานข้อมูล MySql Server 5.0

ซ) โปรแกรมสำหรับรับส่งข้อมูล wget, ftp และ WinScp

3.2 วิธีทดสอบระบบ

การทดสอบบนระบบเครือข่ายต้นแบบ มีวิธีการทดสอบ ดังนี้

3.2.1 การทดสอบโดยการใช้อุปกรณ์ค้นหาเส้นทางที่มีความแตกต่างกัน เพื่อวัดค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางของแต่ละชนิดหรือแต่ละรุ่น มีค่าแตกต่างกันหรือไม่

3.2.2 การทดสอบโดยกำหนดขนาดข้อมูล ผู้วิจัยใช้ข้อมูลขนาด 10 MB 50 MB 100 MB 200 MB และ 500 MB ทำการทดสอบ เพื่อศึกษาว่าขนาดข้อมูลมีผลต่อการประมวลผลของอุปกรณ์ค้นหาเส้นทางหรือไม่

3.2.3 การทดสอบโดยกำหนดขนาดแบนท์วิธของการรับส่งข้อมูลทางด้านเครื่องคอมพิวเตอร์ผู้ใช้ เพื่อเป็นการศึกษาว่า ถ้าสามารถกำหนดขนาดแบนท์วิธการรับส่งข้อมูลได้ ค่าของการประมวลผลของอุปกรณ์ค้นหาเส้นทางเปลี่ยนแปลงอย่างไร และนำผลที่ได้มาเป็นพารามิเตอร์สำหรับการสร้างกฎควบคุมการรับส่งข้อมูล ซึ่งผู้วิจัยใช้แบนท์วิธขนาด 128 Kbps ขนาด 256 Kbps และขนาด 512 Kbps ทำการทดสอบ

3.2.4 การทดสอบโดยติดตั้งระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง แต่ไม่มีการสร้างกฎควบคุมการรับส่งข้อมูล และการทดสอบโดยไม่ติดตั้งระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง เพื่อศึกษาว่าระบบที่พัฒนาขึ้นนี้มีผลกระทบต่อการทำงานของอุปกรณ์ค้นหาเส้นทางหรือไม่

3.2.5 การทดสอบระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง โดยมีการสร้างกฎควบคุมการรับส่งข้อมูลตามที่ได้ออกแบบไว้ในข้อ 1.2.3 เพื่อประเมินผลการทำงานของระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง เป็นตามวัตถุประสงค์ของการวิจัยหรือไม่

4. การทดสอบบนระบบเครือข่ายจริง

ขั้นตอนการทดสอบบนระบบเครือข่ายจริง เป็นการนำระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทางไปติดตั้งบนระบบเครือข่ายของมหาวิทยาลัยศิลปากร วิทยาเขตพระราชวังสนามจันทร์ โดยให้เครื่องผู้ใช้บริการต่าง ๆ บนระบบอินเตอร์เน็ท ทำหน้าที่เป็นเครื่อง

ให้บริการเหมือนกับเครื่อง Server ในระบบเครือข่ายต้นแบบ (Prototype Network System) เครื่องคอมพิวเตอร์ของผู้ใช้ภายในมหาวิทยาลัย เป็นเครื่องคอมพิวเตอร์ client และใช้อุปกรณ์ค้นหาเส้นทางของมหาวิทยาลัยสำหรับใช้ในการทดสอบ แล้วนำผลที่ได้มาประเมินว่าระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง ที่ผู้วิจัยพัฒนาขึ้นสามารถทำงานได้ตามวัตถุประสงค์หรือไม่

5. การสรุปผลและทำรายงาน

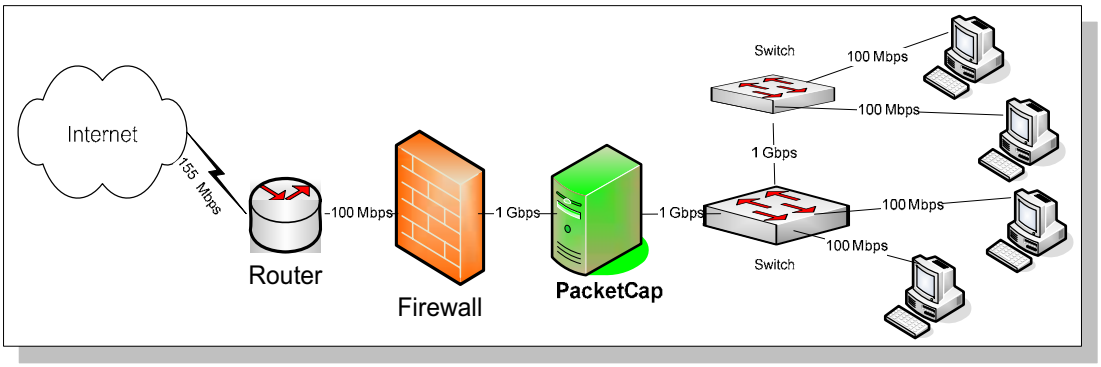
สำหรับขั้นตอนการสรุปผลและทำรายงานนี้ เป็นขั้นตอนสรุปผลการทำวิจัยที่ผู้วิจัยได้พัฒนาขึ้น และนำผลที่ได้จากการทดสอบตามวิธีที่กำหนดไว้ในข้อ 3.2 มาทำรายงานต่อไป

บทที่ 4
ผลการดำเนินการวิจัย

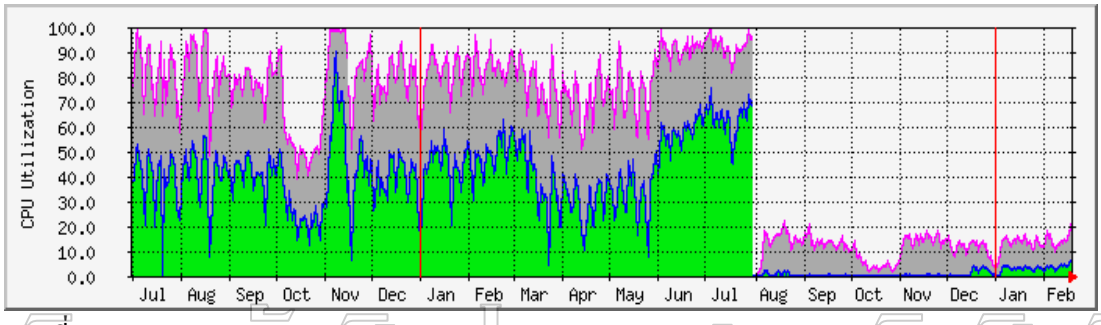
ในบทนี้จะกล่าวถึงผลการดำเนินการวิจัยของระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง (Limited Router CPU Utilization ผู้วิจัยตั้งชื่อย่อว่า “LRCU”) ก่อนที่จะมีการจำลองระบบสำหรับทดสอบในการวิจัย ผู้วิจัยพัฒนาเครื่องมือเพื่อใช้สำหรับเก็บแพ็กเก็ตข้อมูลที่มีการรับและส่งบนระบบเครือข่ายจริง สำหรับศึกษาลักษณะของการรับส่งแพ็กเก็ตข้อมูล และนำผลที่ได้ไปใช้สำหรับการวิเคราะห์และออกแบบระบบเครือข่ายต้นแบบ จากนั้นผู้วิจัยได้ดำเนินการวิจัยตามขั้นตอนที่กำหนดไว้ในบทที่ 3 เพื่อดูผลการทำงานของการประมวลผลของอุปกรณ์ค้นหาเส้นทาง (Router) ว่ามีค่าการเปลี่ยนแปลงอย่างไร และประเมินว่าจำเป็นต้องมีระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทางหรือไม่ ซึ่งมีผลการดำเนินการวิจัยแสดงตามลำดับดังนี้

1. ผลการศึกษาและออกแบบระบบ

ผู้วิจัยได้พัฒนาเครื่องมือสำหรับเก็บแพ็กเก็ตข้อมูล Packet Capture (PacketCap) และได้นำต่อเชื่อมกับระบบเครือข่ายของมหาวิทยาลัยศิลปากร วิทยาเขตพระราชวังสนามจันทร์ ดังภาพที่ 11 การต่อเชื่อมระบบเก็บข้อมูลกับระบบเครือข่าย เพื่อเก็บหมายเลขไอพีแอดเดรสของผู้ส่ง (Source IP) พอร์ตที่ใช้งาน (Source Port) หมายเลขไอพีแอดเดรสของผู้รับ (Destination IP) พอร์ตที่ให้บริการ (Destination Port) ขนาดความยาวของแพ็กเก็ต สถานการณ์รับส่ง (Flags) เวลาที่ใช้ติดต่อ (Time stamp) และข้อมูล 16 Byte แรกของแพ็กเก็ต ระหว่างวันที่ 3 มิถุนายน 2551 ถึงวันที่ 25 กรกฎาคม 2551 โดยสุ่มเก็บข้อมูลเป็นช่วง ๆ ละ 5 นาที แต่จะเลือกเก็บเฉพาะข้อมูลที่มีค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางตั้งแต่ 90 เปอร์เซ็นต์เป็นต้นไป ซึ่งได้ผลสรุปตามตารางที่ 1 สรุปปริมาณการใช้งานบนระบบเครือข่าย และตารางที่ 2 การใช้งานบนระบบเครือข่ายแยกตามโปรโตคอล ส่วนผลการทำงานของการประมวลผลของอุปกรณ์ค้นหาเส้นทาง (Router CPU Utilization) แสดงดังภาพที่ 12



ภาพที่ 11 การต่อเชื่อมระบบเก็บข้อมูลกับระบบเครือข่าย



ภาพที่ 12 แสดงการทำงานของ Router CPU Utilization

จากภาพที่ 12 เป็นการแสดงค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทาง ด้วยโปรแกรม mrtg ด้านแกน Y (CPU Utilization) เป็นเปอร์เซ็นค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทาง ด้านแกน X เป็นช่วงเวลาที่เก็บข้อมูล

ตารางที่ 1 สรุปปริมาณการใช้งานบนระบบเครือข่าย

จำนวนหมายเลขไอพีแอดเดรสของผู้ใช้	จำนวนครั้งที่รับหรือส่งข้อมูล	ขนาดของแพ็กเก็ตข้อมูล (byte)	ปริมาณข้อมูล (MB)
286 – 852	23 – 142,256	24 – 1,453	0.1 – 258.5

จากตารางที่ 1 สรุปปริมาณการใช้งานบนระบบเครือข่าย มีรายละเอียด ดังนี้

จำนวนหมายเลขไอพีแอดเดรสของผู้ใช้ หมายถึง ค่าเฉลี่ยจำนวนหมายเลขไอพีแอดเดรสของผู้ใช้ที่มีการรับส่งข้อมูลทั้งหมด มีค่าต่ำสุดเท่ากับ 286 หมายเลข และค่าสูงสุดเท่ากับ 852 หมายเลข

จำนวนครั้งที่รับหรือส่งข้อมูล หมายถึง ค่าเฉลี่ยจำนวนครั้งที่รับหรือส่งข้อมูล มีค่าต่ำสุดเท่ากับ 23 ครั้งและค่าสูงสุดเท่ากับ 142,256 ครั้ง ต่อ 1 หมายเลขไอพีแอดเดรส

ขนาดของแพ็กเก็ตข้อมูล หมายถึง ค่าเฉลี่ยของขนาดแพ็กเก็ตข้อมูลที่รับหรือส่ง มีค่าต่ำสุดเท่ากับ 24 ไบท์ และค่าสูงสุดเท่ากับ 1,453 ไบท์

ปริมาณข้อมูล หมายถึง ค่าเฉลี่ยของปริมาณข้อมูลที่รับหรือส่ง มีค่าต่ำสุดเท่ากับ 0.1 MB และค่าสูงสุดเท่ากับ 258.5 MB ต่อ 1 หมายเลขไอพีแอดเดรส

ตารางที่ 2 การใช้งานบนระบบเครือข่ายแยกตามโปรโตคอล

โปรโตคอล (หรือพอร์ตที่ขอใช้บริการ)	จำนวนครั้งที่รับหรือส่งข้อมูล	ขนาดของแพ็กเก็ตข้อมูล (byte)	ปริมาณข้อมูล (MB)	เปอร์เซ็นต์การใช้
เฮ็ดทีทีพี (80)	224,305 – 365,754	54 – 1,453	125.5 – 765.5	68.5 – 86.8
เอฟทีพี (21)	22,854 – 77,529	98 – 1,453	26.5 – 654.2	18.2 – 30.5
อาร์ทีเอส (554)	10,895 – 23,065	72 – 1,208	64.5 – 330.2	5.7 – 12.5
อื่น ๆ	978 – 1,478	16 – 756	13.8 – 82.6	0.1 – 11.4

จากตารางที่ 2 การใช้งานบนระบบเครือข่ายแยกตามโปรโตคอล มีรายละเอียด ดังนี้

โปรโตคอล (หรือพอร์ตที่ขอใช้บริการ) หมายถึง หมายเลขพอร์ตที่เครื่องคอมพิวเตอร์ปลายทางหรือผู้ให้บริการ

จำนวนครั้งที่รับหรือส่งข้อมูล หมายถึง ค่าเฉลี่ยจำนวนครั้งที่รับหรือส่งข้อมูลทั้งหมด เช่น ของโปรโตคอลเฮ็ดทีทีพี มีค่าต่ำสุดเท่ากับ 224,305 ครั้ง และค่าสูงสุดเท่ากับ 365,754 ครั้ง

ขนาดของแพ็กเก็ตข้อมูล หมายถึง ค่าเฉลี่ยของขนาดแพ็กเก็ตข้อมูลที่รับหรือส่งทั้งหมด เช่น ของโปรโตคอลเอฟทีพีมีค่าต่ำสุดเท่ากับ 98 ไบท์ และค่าสูงสุดเท่ากับ 1,453 ไบท์

ปริมาณข้อมูล หมายถึง ค่าเฉลี่ยของปริมาณข้อมูลที่รับหรือส่งทั้งหมด เช่น ของโปรโตคอลอาร์ทีเอส มีค่าต่ำสุดเท่ากับ 64.5 MB และค่าสูงสุดเท่ากับ 330.2 MB

เปอร์เซ็นต์การใช้ หมายถึง ค่าเฉลี่ยของเปอร์เซ็นต์การใช้งานของผู้ใช้ที่รับหรือส่งข้อมูลทั้งหมด เช่น ของโปรโตคอลเฮ็ดทีทีพี มีค่าต่ำสุดเท่ากับ 68.5 เปอร์เซ็นต์ และค่าสูงสุดเท่ากับ 86.8 เปอร์เซ็นต์

2. ผลการพัฒนาระบบ

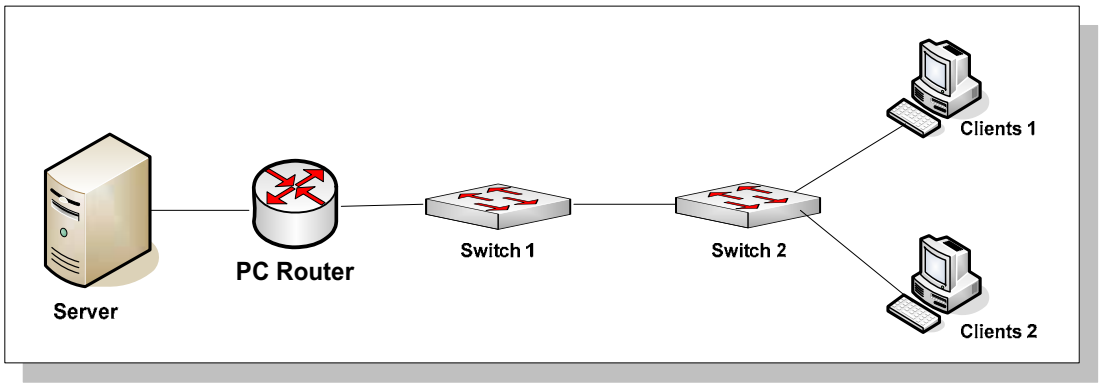
ผลของขั้นตอนการพัฒนาระบบ สามารถแสดงรายละเอียดได้ตามภาคผนวก ก.

3. ผลการทดสอบบนระบบเครือข่ายต้นแบบ (Prototype Network System)

การทดสอบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทางบนระบบเครือข่ายต้นแบบ มีผลการทดสอบแสดงตามลำดับ ดังนี้

3.1 การใช้เครื่องคอมพิวเตอร์ทำหน้าที่เป็นอุปกรณ์ค้นหาเส้นทาง (PC Router)

การทดสอบระบบเครือข่ายต้นแบบ โดยใช้เครื่องคอมพิวเตอร์ทำหน้าที่เป็นอุปกรณ์ค้นหาเส้นทาง นั้น ผู้วิจัยได้ทำการทดสอบจำนวนทั้งหมด 40 ครั้ง โดยให้เครื่องคอมพิวเตอร์ client 1 รับและส่งข้อมูลขนาด 200 MB จากเครื่อง Server ผ่านโปรโตคอล เฮ็ดทีทีพี (HTTP) และ เอฟทีพี (FTP) จำนวนอย่างละ 5 ครั้ง ผ่านอุปกรณ์กระจายสัญญาณเครือข่ายที่ 1, 2 (switch 1, switch 2) และผ่านเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นอุปกรณ์ค้นหาเส้นทางดังภาพที่ 13 ระบบเครือข่ายต้นแบบที่ใช้เครื่องคอมพิวเตอร์ทำหน้าที่เป็นอุปกรณ์ค้นหาเส้นทาง ซึ่งได้ผลเฉลี่ยของค่าการประมวลผลเปลี่ยนแปลงเพิ่มขึ้น 2 – 3 เปอร์เซ็นต์ และทดสอบโดยให้เครื่องคอมพิวเตอร์ client 1 และเครื่องคอมพิวเตอร์ client 2 รับและส่งข้อมูลพร้อมกันผ่านโปรโตคอลเฮ็ดทีทีพี และโปรโตคอลเอฟทีพี ซึ่งได้ผลเฉลี่ยของค่าการประมวลผลเพิ่มขึ้น 2 – 3 เปอร์เซ็นต์เช่นเดียวกัน



ภาพที่ 13 ระบบเครือข่ายต้นแบบที่ใช้เครื่องคอมพิวเตอร์ทำหน้าที่เป็นอุปกรณ์ค้นหาเส้นทาง

จากภาพที่ 13 ระบบเครือข่ายต้นแบบที่ใช้เครื่องคอมพิวเตอร์ทำหน้าที่เป็นอุปกรณ์ค้นหาเส้นทาง มีรายละเอียดการทำงานแต่ละส่วนดังนี้

เครื่องคอมพิวเตอร์ Server ทำหน้าที่ให้บริการรับหรือส่งข้อมูล โดยให้บริการทั้งโปรโตคอลเฮ็ดทีทีพีและโปรโตคอลเอฟทีพี

เครื่องคอมพิวเตอร์ PC Router ทำหน้าที่เป็นอุปกรณ์ค้นหาเส้นทาง ในงานวิจัยนี้ใช้เครื่องคอมพิวเตอร์มีการประมวลผลรุ่นเพ็นเทียมโฟ (Pentium V) ความเร็ว 1.6 GHz มีหน่วยความจำหลัก 512 MB ติดตั้งระบบปฏิบัติการลินุกส์ CentOS 4.2 และโปรแกรม IP Route

อุปกรณ์กระจายสัญญาณเครือข่าย (switch 1 และ switch 2) ทำหน้าที่ต่อเชื่อมเครื่องคอมพิวเตอร์ ให้สามารถรับส่งข้อมูลกันได้

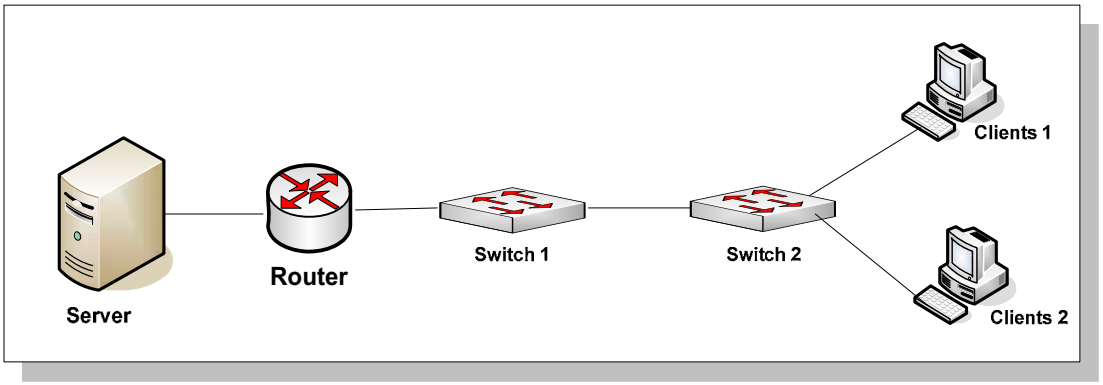
เครื่องคอมพิวเตอร์ client 1 และ client 2 ทำหน้าที่เป็นเครื่องคอมพิวเตอร์ของผู้ใช้งานบนระบบเครือข่าย

3.2 การใช้อุปกรณ์ค้นหาเส้นทางทำหน้าที่ค้นหาเส้นทาง

การทดสอบระบบเครือข่ายต้นแบบที่ใช้อุปกรณ์ค้นหาเส้นทาง มีการต่อเชื่อมกันดังภาพที่ 14 ระบบเครือข่ายต้นแบบที่ใช้อุปกรณ์ค้นหาเส้นทาง ผู้วิจัยได้ใช้อุปกรณ์ค้นหาเส้นทาง 2 ชุด โดยชุดที่ 1 ใช้อุปกรณ์ค้นหาเส้นทางของบริษัทซิสโก้ รุ่น 3660 มีการประมวลผลความเร็ว 248 MHz หน่วยความจำหลัก 256 MB และไอโอเอสเวอร์ชัน 12.2 (T) ทำการทดสอบผ่านโปรโตคอลเฮ็ดทีทีพีและเอฟทีพีเช่นเดียวกับระบบเครือข่ายต้นแบบที่ใช้เครื่องคอมพิวเตอร์ทำหน้าที่เป็นอุปกรณ์ค้นหาเส้นทาง ได้ผลค่าเฉลี่ยของการประมวลผลสูงสุดของ 12 เปอร์เซ็นและ 13 เปอร์เซ็น ตามลำดับ

ชุดที่ 2 ใช้อุปกรณ์ค้นหาเส้นทางของบริษัทซิสโก้ รุ่น 2511 มีหน่วยความจำหลัก 16 MB และไอโอเอสเวอร์ชัน 12.0 (9) ทำการทดสอบผ่านโปรโตคอลเฮ็ดทีทีพีและเอฟทีพี

เช่นเดียวกับระบบเครือข่ายต้นแบบที่ใช้เครื่องคอมพิวเตอร์ทำหน้าที่เป็นอุปกรณ์หาเส้นทาง ได้ผลค่าเฉลี่ยของการใช้การประมวลผลสูงสุด 70 เปอร์เซ็นต์และ 72 เปอร์เซ็นต์ ตามลำดับ

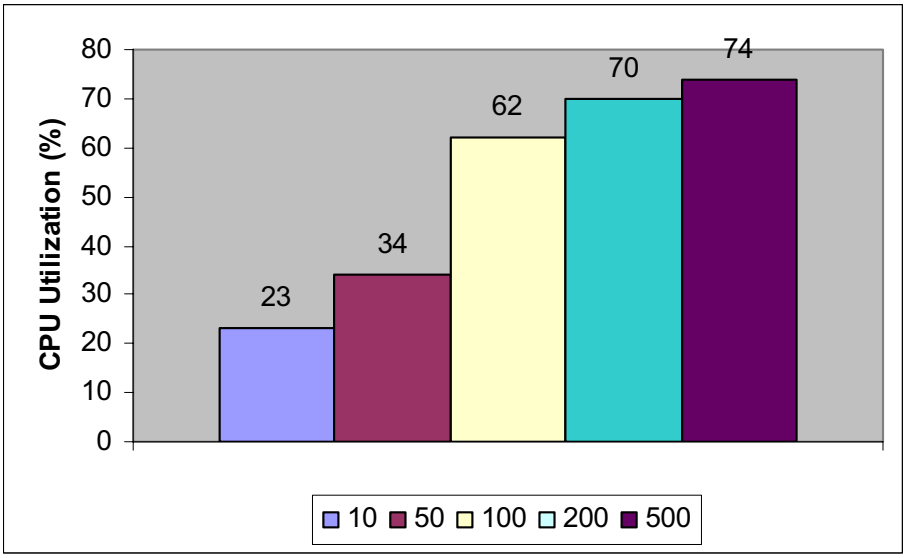


ภาพที่ 14 ระบบเครือข่ายต้นแบบที่ใช้อุปกรณ์ค้นหาเส้นทาง

ดังนั้นจะเห็นได้ว่าการใช้อุปกรณ์ค้นหาเส้นทางที่มีความแตกต่างกัน จะได้ค่าการประมวลผลที่แตกต่างกัน แม้ว่าจะใช้สภาวะแวดล้อมที่เหมือนกันและทำการทดสอบด้วยวิธีเดียวกัน ดังนั้นผู้วิจัยได้เลือกใช้อุปกรณ์ค้นหาเส้นทางของบริษัทซิสโก้ “รุ่น 2511” สำหรับระบบเครือข่ายต้นแบบทั้งหมด เพราะมีผลการเปลี่ยนแปลงการประมวลผลของอุปกรณ์ค้นหาเส้นทางชัดเจนที่สุด ทำให้สังเกตุค่าของการเปลี่ยนแปลงได้ง่ายที่สุด

3.3 การทดสอบบนระบบเครือข่ายต้นแบบ โดยกำหนดขนาดข้อมูล

การทดสอบบนระบบเครือข่ายต้นแบบ โดยกำหนดขนาดข้อมูลให้มีความแตกต่างกัน ผู้วิจัยได้ทำการทดสอบระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง โดยใช้ขนาดข้อมูล 10 MB, 50 MB, 100 MB, 200 MB และ 500 MB และทำการทดสอบด้วยวิธีเช่นเดียวกับการทดสอบระบบเครือข่ายต้นแบบที่ใช้เครื่องคอมพิวเตอร์ทำหน้าที่เป็นอุปกรณ์ค้นหาเส้นทางแต่ทำการทดสอบจำนวน 100 ครั้งของแต่ละขนาดข้อมูล สามารถสรุปการวัดค่าเฉลี่ยที่ 5 นาทีสูงสุดของค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทาง ในแต่ละขนาดข้อมูลดังภาพที่ 15 ค่าการประมวลผลเมื่อใช้ข้อมูลแต่ละขนาด และได้ผลสรุปเฉลี่ยจำนวนปริมาณการเชื่อมต่อในการรับหรือส่งข้อมูลภายใน 5 นาทีสูงสุด ของข้อมูลแต่ละขนาด ดังนี้คือ ขนาด 10 MB เท่ากับ 7,153 ครั้ง ขนาด 50 MB เท่ากับ 35,620 ครั้ง ขนาด 100 MB เท่ากับ 70,664 ครั้ง ขนาด 200 MB เท่ากับ 82,763 ครั้ง และขนาด 500 MB เท่ากับ 82,758 ครั้ง

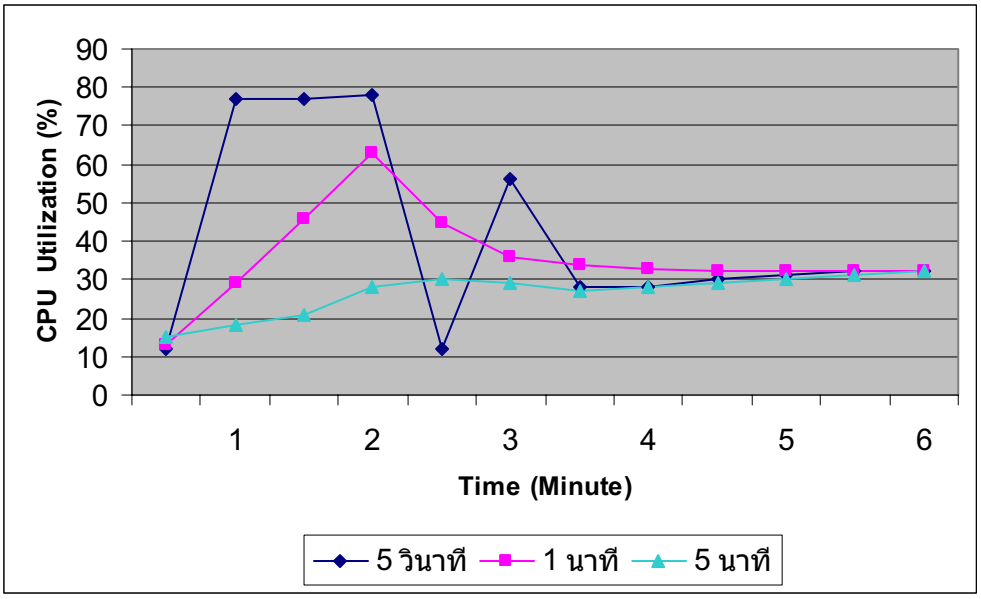


ภาพที่ 15 ค่าการประมวลผล เมื่อใช้ข้อมูลแต่ละขนาด

จากภาพที่ 15 ค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางเมื่อใช้ข้อมูลแต่ละขนาด จะพบว่าเมื่อใช้ข้อมูลขนาด 10 MB ทดสอบการรับหรือส่งข้อมูลบนระบบเครือข่ายต้นแบบ ได้ค่าเฉลี่ยสูงสุดของการประมวลผลของอุปกรณ์ค้นหาเส้นทาง เท่ากับ 23 เปอร์เซ็นต์ และเมื่อใช้ข้อมูลขนาด 50 MB, 100 MB, 200 MB และ 500 MB ได้ค่าเฉลี่ยสูงสุดเท่ากับ 34, 62, 70 และ 74 เปอร์เซ็นต์ ตามลำดับ

3.4 การทดสอบบนระบบเครือข่ายต้นแบบ โดยกำหนดขนาดแบนท์วิธ

ผู้วิจัยได้ทดสอบระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง โดยกำหนดขนาดแบนท์วิธทางด้านเครื่องคอมพิวเตอร์ผู้ใช้จำนวน 20 ครั้งของแต่ละขนาดแบนท์วิธ โดยใช้โปรแกรม WinSCP ผ่านโปรโตคอลเอฟทีพี และทดสอบกำหนดแบนท์วิธที่ 128 Kbps, 256 Kbps และ 512 Kbps ของข้อมูลขนาด 200 MB การทดสอบเริ่มจากการไม่กำหนดขนาดแบนท์วิธ (ค่า None เป็นค่าเริ่มต้นของโปรแกรม) ได้ผลการทดสอบดังภาพที่ 16 ภาพที่ 17 ภาพที่ 18 ตารางที่ 3 ตารางที่ 4 และ ตารางที่ 5 ตามลำดับ

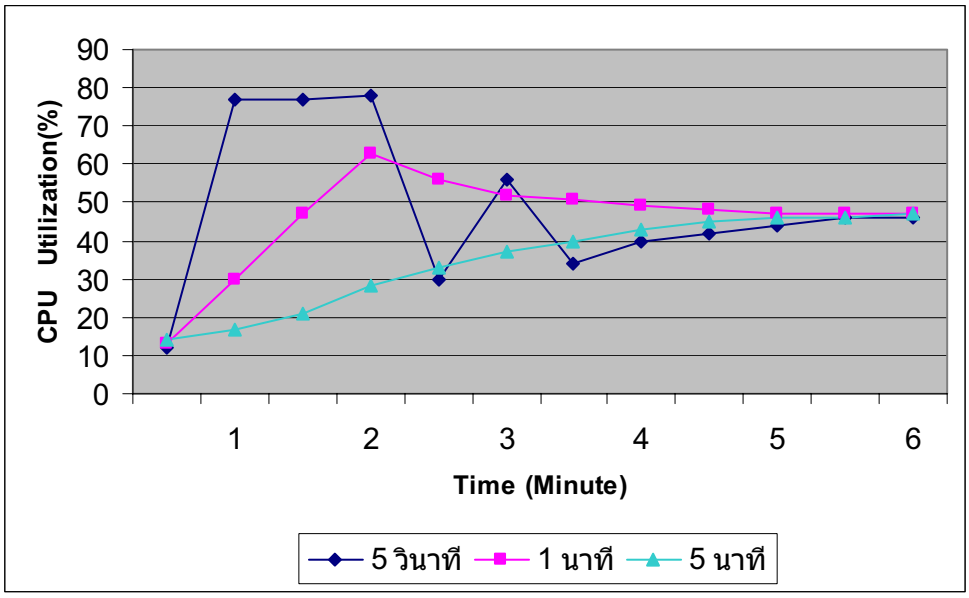


ภาพที่ 16 ค่าการประมวลผล เมื่อกำหนดแบนท์วิธ 128 Kbps

ตารางที่ 3 ค่าการประมวลผล เมื่อกำหนดแบนท์วิธ 128 Kbps

เวลาผ่านไป (นาที)	ค่าการประมวลผล 5 วินาที	ค่าการประมวลผล 1 นาที	ค่าการประมวลผล 5 นาที
0	12	13	15
1	77	46	21
2	12	45	30
3	28	34	27
4	30	32	29
5	32	32	31
6	32	32	32

จากภาพที่ 16 และตารางที่ 3 ค่าการประมวลผล เมื่อกำหนดแบนท์วิธ 128 Kbps ผู้วิจัยได้ลดแบนท์วิธการส่งข้อมูลเป็น 128 Kbps เมื่อเวลาการส่งข้อมูลไปยังเครื่องคอมพิวเตอร์ Server ผ่านไปประมาณ 2.30 นาที จะเห็นว่าค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางได้ลดลง และพบว่าค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางสูงสุด 32 เปอร์เซ็นต์ แสดงว่าการกำหนดแบนท์วิธที่ 128 Kbps สามารถลดการประมวลผลของอุปกรณ์ค้นหาเส้นทางได้



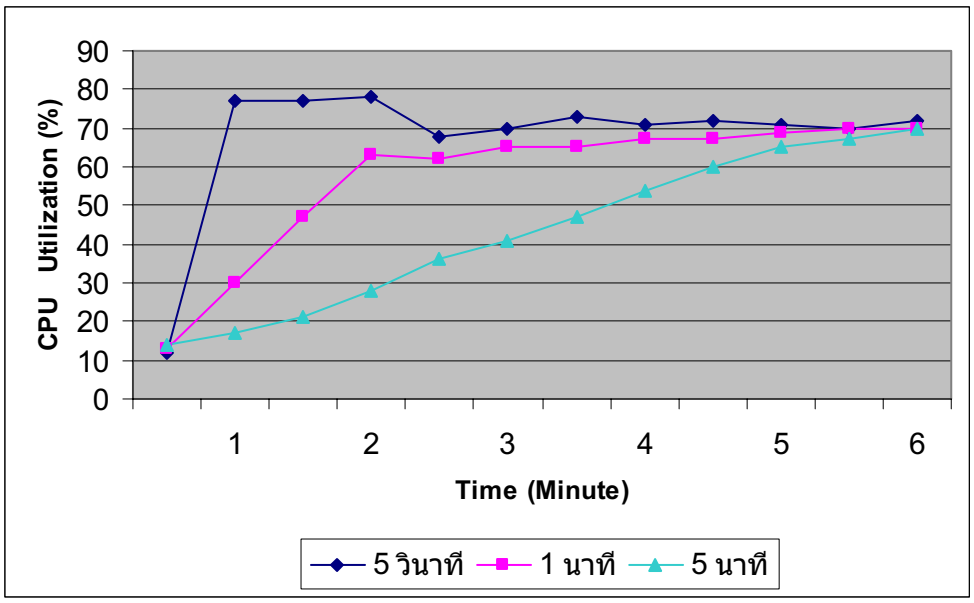
ภาพที่ 17 ค่าการประมวลผล เมื่อกำหนดแบนท์วิธ 256 Kbps

ตารางที่ 4 ค่าการประมวลผล เมื่อกำหนดแบนท์วิธ 256 Kbps

เวลาผ่านไป (นาที)	ค่าการประมวลผล 5 วินาที	ค่าการประมวลผล 1 นาที	ค่าการประมวลผล 5 นาที
0	12	13	14
1	77	47	21
2	30	56	33
3	34	51	40
4	42	48	45
5	46	47	46
6	46	47	47

จากภาพที่ 17 และตารางที่ 4 ค่าการประมวลผล เมื่อกำหนดแบนท์วิธ 256 Kbps ผู้วิจัยได้ลดแบนท์วิธการส่งข้อมูลเป็น 256 Kbps เมื่อเวลาส่งข้อมูลไปยังเครื่องคอมพิวเตอร์ Server ผ่านไปประมาณ 2.30 นาที จะเห็นว่าค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางได้ลดเรื่อย ๆ และ

พบว่าค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางสูงสุด 47 เปอร์เซ็นต์ แสดงว่าการกำหนดแบนท์วิธที่ 256 Kbps สามารถลดการประมวลผลของอุปกรณ์ค้นหาเส้นทางได้



ภาพที่ 18 ค่าการประมวลผล เมื่อกำหนดแบนท์วิธ 512 Kbps

ตารางที่ 5 ค่าการประมวลผล เมื่อกำหนดแบนท์วิธ 512 Kbps

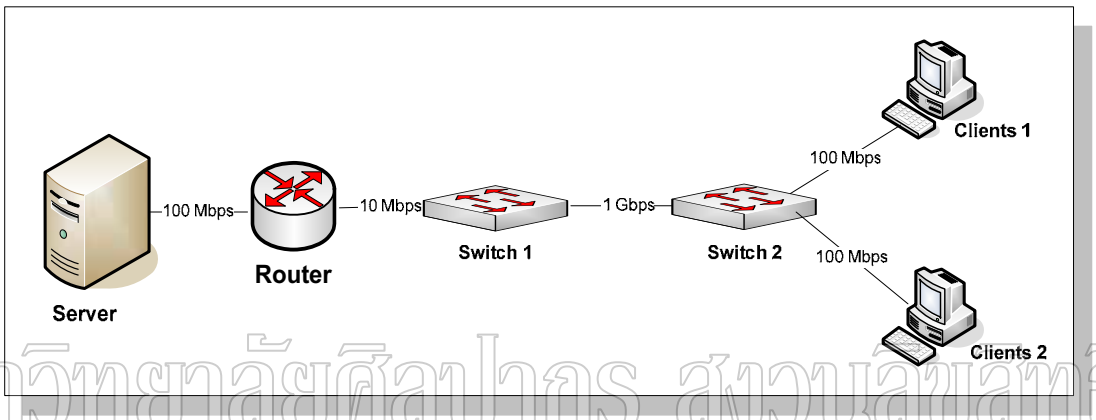
เวลาผ่านไป (นาที)	ค่าการประมวลผล 5 วินาที	ค่าการประมวลผล 1 นาที	ค่าการประมวลผล 5 นาที
0	12	13	14
1	77	47	21
2	68	62	36
3	73	65	47
4	72	67	60
5	70	70	67
6	72	70	70

จากภาพที่ 18 และตารางที่ 5 ค่าการประมวลผล เมื่อกำหนดแบนท์วิธ 512 Kbps ผู้วิจัยได้ลดแบนท์วิธการส่งข้อมูลเป็น 512 Kbps เมื่อเวลาส่งข้อมูลไปยังเครื่องคอมพิวเตอร์ Server ผ่านไปประมาณ 2.30 นาที จะเห็นว่าค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางเปลี่ยนแปลงเล็กน้อย

และพบว่าค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางสูงสุด มีค่าเท่ากับ 70 เปอร์เซ็นต์ แสดงว่าการกำหนดแบนท์วิธที่ 512 Kbps ไม่สามารถลดการประมวลผลของอุปกรณ์ค้นหาเส้นทางได้

3.5 ผลการทดสอบบนระบบเครือข่ายต้นแบบ ที่ไม่มีระบบ LRCU

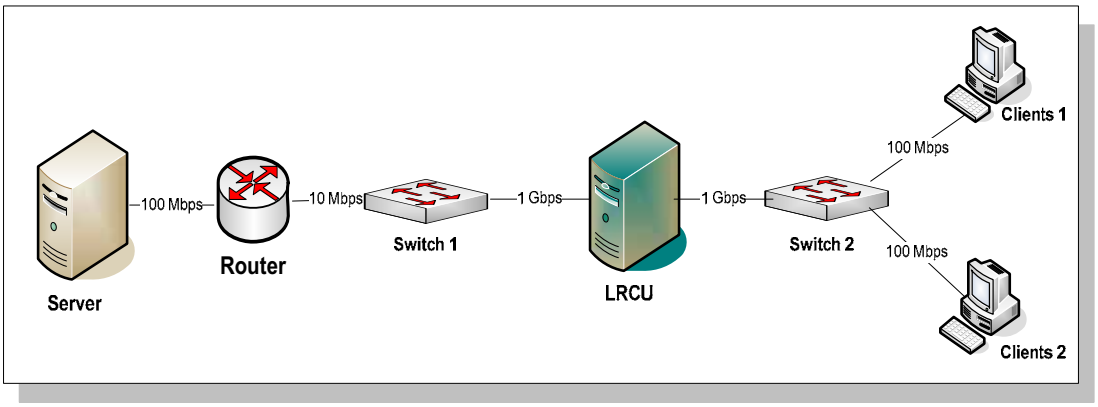
การทดสอบการรับส่งข้อมูลผ่านระบบเครือข่าย ตามภาพที่ 19 ระบบเครือข่ายต้นแบบ ที่ไม่มีระบบ LRCU เพื่อทดสอบว่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางในสถานการณ์ปกติ มีการทำงานมากน้อยเพียงใด



ภาพที่ 19 ระบบเครือข่ายต้นแบบ ที่ไม่มีระบบ LRCU

3.6 ผลการทดสอบบนระบบเครือข่ายต้นแบบ ที่มีระบบ LRCU

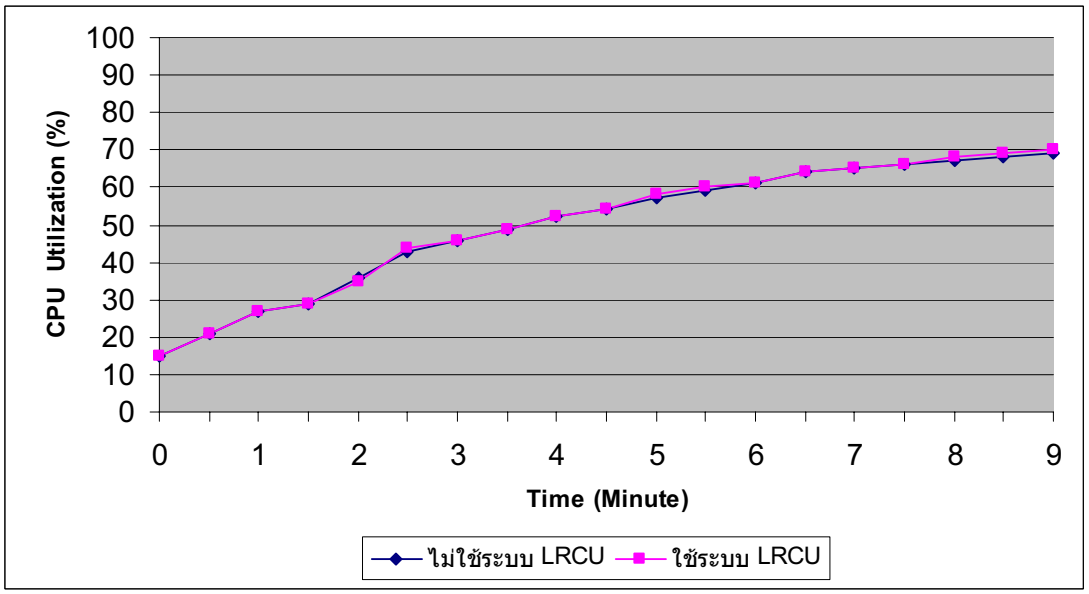
การทดสอบระบบเครือข่ายที่ใช้ระบบ LRCU จะเชื่อมต่อตามภาพที่ 20 ระบบเครือข่ายต้นแบบ ที่มีระบบ LRCU ผู้วิจัยได้ทำการทดสอบเป็น 2 รูปแบบ คือ รูปแบบที่ 1 เป็นการต่อผ่านเครื่อง LRCU แต่ยังไม่ได้เปิดระบบให้ทำงาน เพียงเป็นการส่งข้อมูลผ่านเครื่อง แบบที่ 2 เปิดระบบ LRCU ให้ทำงานเพื่อควบคุมการรับส่งข้อมูล เพื่อให้มีผลกระทบต่อการประมวลผลของอุปกรณ์ค้นหาเส้นทางให้น้อยที่สุด และมุ่งหวังให้อุปกรณ์ค้นหาเส้นทางยังคงทำงานได้ตามปกติ



ภาพที่ 20 ระบบเครือข่ายต้นแบบ ที่มีระบบ LRCU

จากภาพที่ 19 และภาพที่ 20 ระบบเครือข่ายต้นแบบ ประกอบด้วยเครื่องคอมพิวเตอร์ที่ติดตั้งระบบ LRCU ทำหน้าที่ในการรับส่งข้อมูลระหว่างเครื่อง clients กับเครื่อง server ที่มีการควบคุมการรับส่งข้อมูลและไม่มีการควบคุม เครื่อง server มีหน้าที่ในการให้บริการข้อมูลกับเครื่อง clients ผ่านโปรโตคอล FTP และ HTTP แต่ละเครื่อง

การทดสอบบนระบบทั้ง 2 แบบ ทำโดยการส่งข้อมูลขนาด 200 MB จากเครื่อง client ไปยัง server ผ่านโปรโตคอล FTP จำนวนหลาย 20 ครั้ง และผู้วิจัยได้จับเวลาการส่งข้อมูลผ่านระบบทั้ง 2 แบบ พบว่าเวลาของการส่งข้อมูลมีค่าแตกต่างกันน้อยกว่า 0.1 วินาที สำหรับผลการทดสอบการประมวลผลของอุปกรณ์ค้นหาเส้นทางได้ผลดังภาพที่ 21 แสดงค่าการประมวลผลเมื่อยังไม่สร้างกฎควบคุม

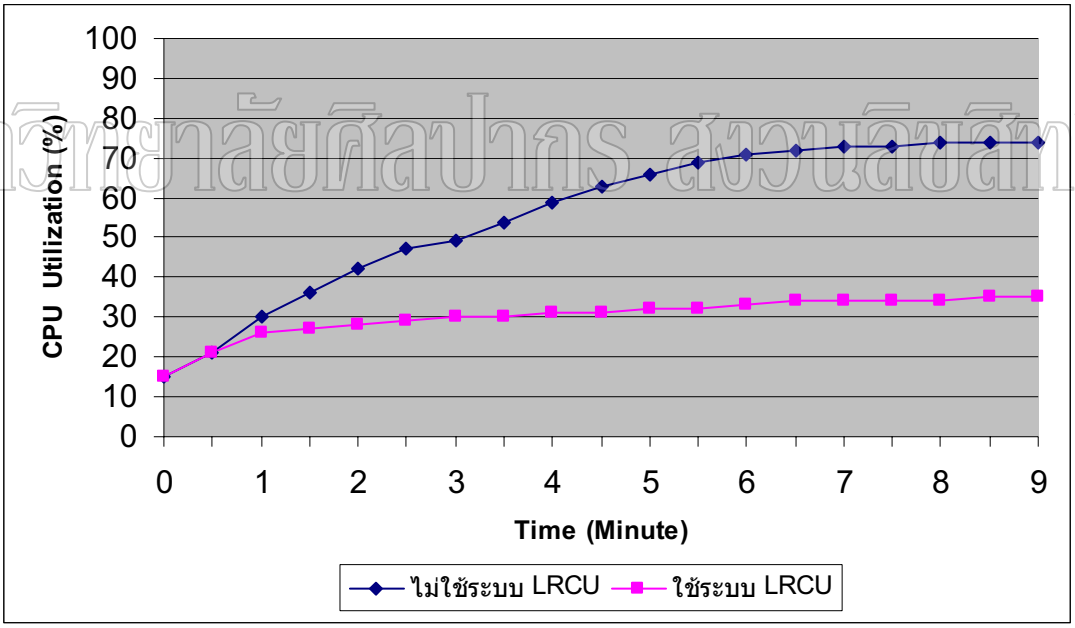


ภาพที่ 21 ค่าการประมวลผลเมื่อยังไม่สร้างกฎควบคุม

จากภาพที่ 21 ค่าประมวลผลเมื่อยังไม่สร้างกฎควบคุม และจากผลการจับเวลาการส่งข้อมูล แสดงว่าระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทางไม่มีผลกระทบต่อการรับหรือส่งข้อมูล เมื่อยังไม่ได้สร้างกฎควบคุมการรับส่งข้อมูลของผู้ใช้

3.7 ผลการทดสอบบนระบบเครือข่ายต้นแบบ ด้วยวิธี Bandwidth Model

การทดสอบบนระบบเครือข่ายต้นแบบ ด้วยวิธีการควบคุมปริมาณการรับส่งข้อมูล (Bandwidth Model) ได้ผลดังภาพที่ 22 ค่าการประมวลผลเมื่อใช้ระบบ LRCU ด้วยวิธี Bandwidth Model โดยทำการทดสอบจำนวน 80 ครั้ง ให้เครื่องคอมพิวเตอร์ client 1 รับและส่งข้อมูลขนาด 200 MB ผ่านโปรโตคอลเฮ็ดทีทีพีและเอฟทีพี ซึ่งได้ตั้งค่า threshold การประมวลผลของอุปกรณ์ค้นหาเส้นทางไว้ที่ 60 เปอร์เซ็น และค่า threshold ปริมาณข้อมูลรับหรือส่งเท่ากับ 130 MB และใช้แบนท์วิธ 128 Kbps สำหรับการสร้างกฎควบคุมการรับส่งข้อมูลของเครื่อง client 1

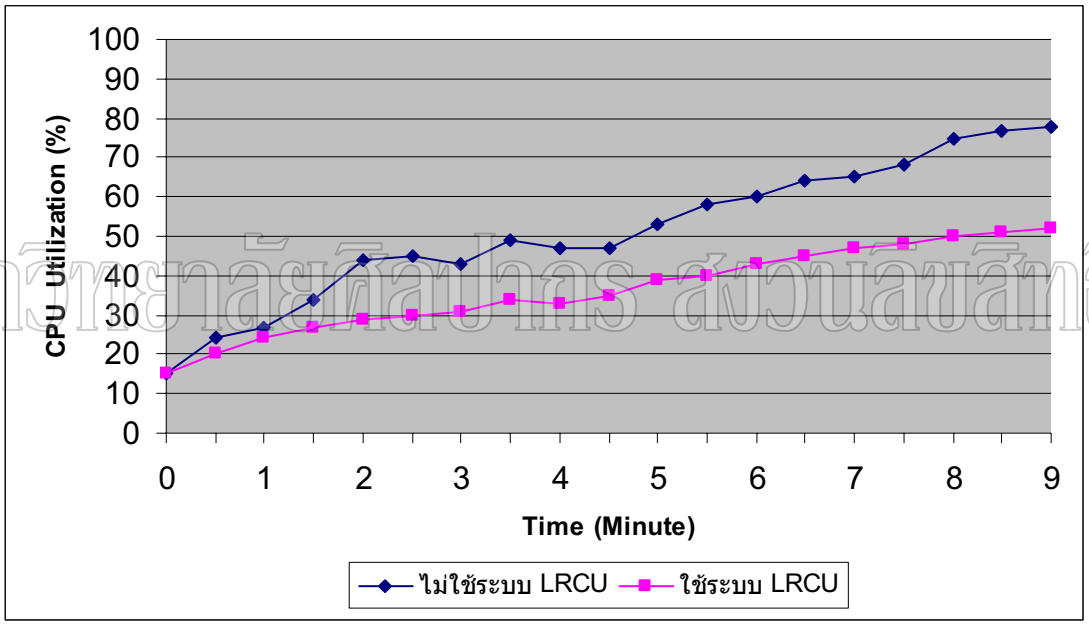


ภาพที่ 22 ค่าการประมวลผลเมื่อใช้ระบบ LRCU ด้วยวิธี Bandwidth Model

จากภาพที่ 22 ค่าการประมวลผลเมื่อใช้ระบบ LRCU ด้วยวิธี Bandwidth Model จะเห็นว่าการควบคุมการปริมาณการรับส่งข้อมูล ระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง สามารถควบคุมค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางไม่ให้เกินค่า threshold ที่กำหนดได้ และพบว่าค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทาง มีค่าสูงสุดไม่เกิน 35 เปอร์เซ็นต์

3.8 ผลการทดสอบบนระบบเครือข่ายต้นแบบ ด้วยวิธี Priority Model

การทดสอบบนระบบเครือข่ายต้นแบบ ด้วยวิธีการกำหนดความสำคัญของข้อมูล (Priority Model) ได้ผลการทดสอบดังภาพที่ 23 ค่าการประมวลผลเมื่อใช้ระบบ LRCU ด้วยวิธี Priority Model โดยผู้วิจัยทำการทดสอบการรับส่งข้อมูลและกำหนดค่า threshold ไว้ที่ 60 เปอร์เซ็นต์ เช่นเดียวกับวิธี Bandwidth Model และค่า threshold จำนวนเชื่อมต่อการับหรือส่งเท่ากับ 65,000 ครั้ง โดยเครื่องคอมพิวเตอร์ client 1 ทำหน้าที่รับและส่งข้อมูลขนาด 50 MB จำนวน 20 เซสชั่น (session) พร้อม ๆ กัน เพื่อสร้างจำนวนการเชื่อมต่อให้มีจำนวนมาก และสำหรับเครื่อง client 2 ทำหน้าที่รับส่งข้อมูลขนาด 10 MB ทุก ๆ 5 นาที เพื่อให้มีการรับส่งข้อมูลทั้ง 2 เครื่องปะปนกันไป

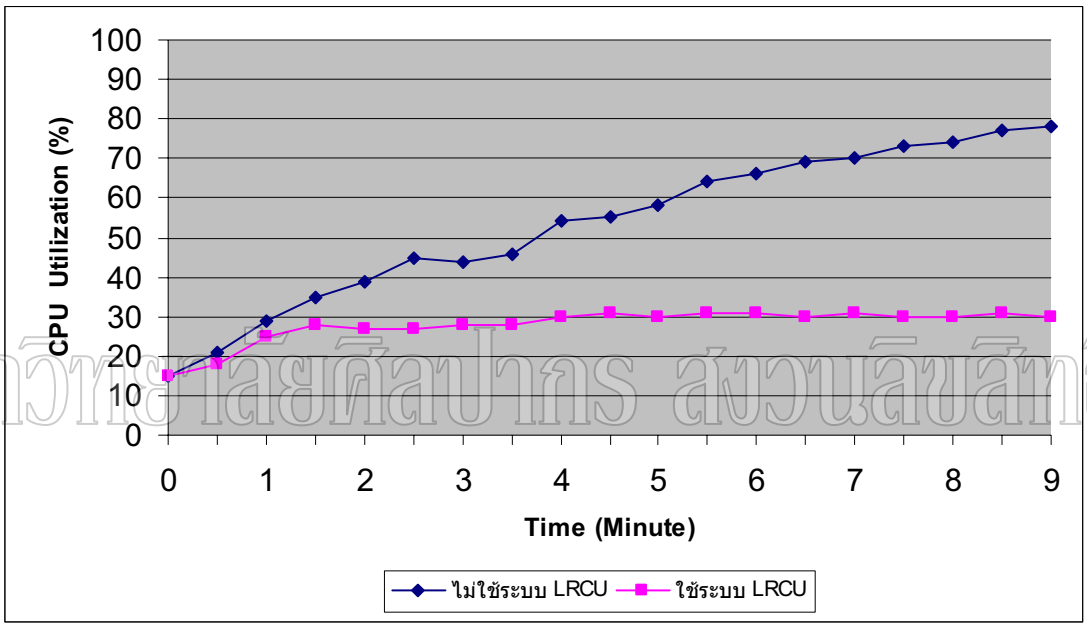


ภาพที่ 23 ค่าการประมวลผลเมื่อใช้ระบบ LRCU ด้วยวิธี Priority Model

จากภาพที่ 23 ค่าการประมวลผลเมื่อใช้ระบบ LRCU ด้วยวิธี Priority Model จะเห็นว่าการกำหนดความสำคัญของข้อมูล ระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง สามารถควบคุมค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางไม่ให้เกินค่า threshold ได้ และพบว่าค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางมีค่าสูงสุดไม่เกิน 52 เปอร์เซ็นต์

3.9 ผลการทดสอบบนระบบเครือข่ายต้นแบบ ด้วยวิธี Deny Model

การทดสอบระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง ด้วยวิธีการป้องกันการส่งข้อมูล (Deny Model) ผู้วิจัยใช้วิธีการสร้างกฎแบบผู้ดูแลกำหนดเอง (Manual Policy) จากนั้นได้ทำการทดสอบโดยการกำหนดค่า threshold ไว้ที่ 60 เปอร์เซ็นต์ เช่นเดียวกับวิธี Bandwidth Model และ Priority Model แต่กำหนดใช้ขนาดการรับส่งข้อมูลของเครื่อง client 1 เป็น 100 MB ซึ่งได้ผลการทดสอบดังภาพที่ 24 ค่าการประมวลผลเมื่อใช้ระบบ LRCU ด้วยวิธี Deny Model



ภาพที่ 24 ค่าการประมวลผลเมื่อใช้ระบบ LRCU ด้วยวิธี Deny Model

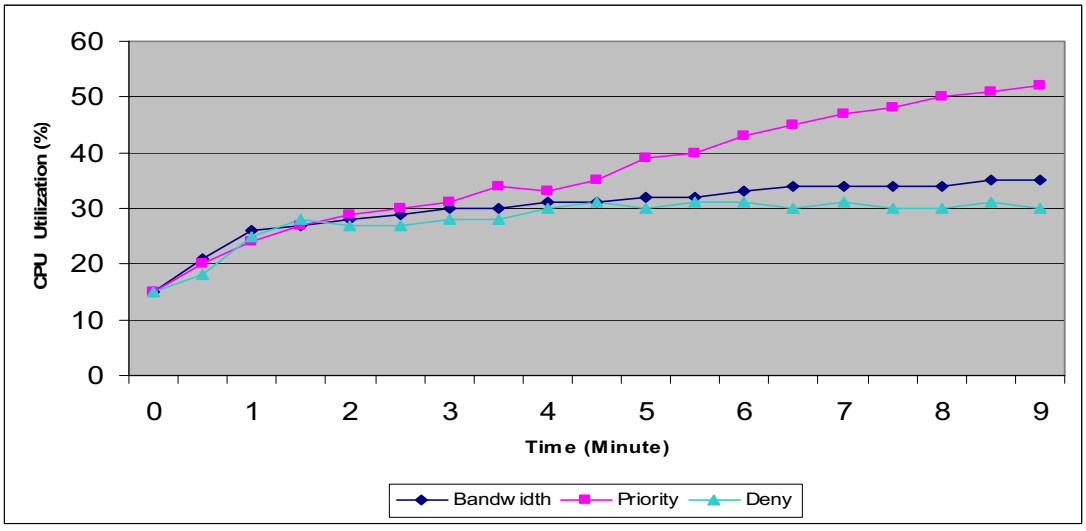
จากภาพที่ 24 ค่าการประมวลผลเมื่อใช้ระบบ LRCU ด้วยวิธี Deny Model จะเห็นว่าการป้องกันการส่งข้อมูล ระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง สามารถควบคุมค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางไม่ให้เกินค่า threshold ที่กำหนดได้ และพบว่าค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางมีค่าสูงสุดไม่เกิน 30 เปอร์เซ็นต์

3.10 ผลการทดสอบบนระบบเครือข่ายจริง

การทดสอบระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทางบนระบบเครือข่ายจริง ผู้วิจัยได้นำระบบไปติดตั้งบนระบบเครือข่ายของมหาวิทยาลัยศิลปากร วิทยาเขตพระราชวังสนามจันทร์ ระหว่างวันที่ 19 มกราคม 2552 ถึงวันที่ 26 มกราคม 2552 โดยกำหนด threshold ไว้ที่ 60 เปอร์เซ็นต์ การทดสอบพบว่าตลอดช่วงเวลาการทดสอบค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางมีค่าสูงสุด 15 เปอร์เซ็นต์ และมีเครื่องคอมพิวเตอร์ของผู้ใช้สร้างจำนวนการเชื่อมต่อ (connection) สูงสุด 175,630 ครั้งต่อช่วงเวลาการรับส่งข้อมูล 5 นาที ดังนั้นจะเห็นว่า ค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทาง มีค่าไม่เกิน threshold ที่กำหนดไว้ เนื่องมาจากทางศูนย์คอมพิวเตอร์ ได้เปลี่ยนอุปกรณ์ค้นหาเส้นทางใหม่แทนอุปกรณ์ค้นหาเส้นทางเดิมที่ใช้ในการเก็บข้อมูลเพื่อใช้ศึกษาและออกแบบระบบ โดยเปลี่ยนเป็นของบริษัท ซิสโก้ จากรุ่น 7204 เป็นรุ่น 7604 ซึ่งที่มีการประมวลผลความเร็ว 1.2 GHz มีหน่วยความจำหลัก 1 GB และไอโอเอสเวอร์ชัน 12.2(33r)

3.11 การเปรียบเทียบผลการทดสอบของแต่ละวิธี

ผู้วิจัยได้นำผลการทดสอบของวิธีการควบคุมปริมาณการรับส่งข้อมูล (Bandwidth Model) การกำหนดความสำคัญของข้อมูล (Priority Model) และการป้องกันการส่งข้อมูล (Deny Model) มาเปรียบเทียบ ซึ่งสามารถแสดงผลการเปรียบเทียบดังภาพที่ 25 ค่าการประมวลผลของอุปกรณ์ค้นหาเส้น ของแต่ละวิธี



ภาพที่ 25 ค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทาง ของแต่ละวิธี

จากภาพที่ 25 ค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทาง ของแต่ละวิธี จะเห็นว่า การจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง ด้วยวิธีป้องกันการส่งข้อมูลควบคุมให้อุปกรณ์ค้นหาเส้นทาง มีการประมวลผลน้อยที่สุด รองลงมาเป็นวิธีการควบคุมปริมาณการรับส่งข้อมูล และวิธีการกำหนดความสำคัญของข้อมูลมีค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางมากที่สุด จากการทดสอบในห้องปฏิบัติการยังพบว่าการควบคุมด้วยวิธีการป้องกันการส่งข้อมูลใช้เวลาการรับหรือส่งข้อมูลมากที่สุดเมื่อใช้ขนาดข้อมูลเท่ากัน การกำหนดความสำคัญของข้อมูลใช้เวลาการรับหรือส่งข้อมูลน้อยที่สุด แต่การประมวลผลของอุปกรณ์ค้นหาเส้นทางมีค่ามากกว่าค่า threshold ในกรณีที่มีเครื่องคอมพิวเตอร์ใช้งานบนระบบเครือข่ายจำนวน 1 เครื่อง ส่วนวิธีการควบคุมปริมาณของข้อมูลที่รับส่ง การประมวลผลของอุปกรณ์ค้นหาเส้นทางมีค่าไม่เกิน threshold และการรับส่งข้อมูลทำได้เป็นปกติ และใช้เวลาการรับส่งข้อมูลมากกว่าการใช้งานปกติเล็กน้อย ถ้ากำหนดแบนท์วิธให้เหมาะสมกับปริมาณการใช้งานทั้งหมดบนระบบเครือข่าย

ดังนั้นสรุปผลการทดสอบได้ว่าวิธีการควบคุมปริมาณของข้อมูลที่รับส่ง (Bandwidth Model) เป็นวิธีที่ดีสุด สำหรับระบบเครือข่ายต้นแบบ (Prototype Network System) นี้ รองลงมาเป็นวิธีการป้องกันการส่งข้อมูล (Deny Model) และวิธีการกำหนดความสำคัญของข้อมูลนั้นใช้ได้ผลดีกับเครือข่ายขนาดใหญ่

บทที่ 5
สรุปผลการวิจัยและข้อเสนอแนะ

ในบทนี้จะกล่าวถึงบทสรุปทั้งหมด ที่ดำเนินการวิจัย เริ่มจากการศึกษาการเก็บข้อมูลบนระบบเครือข่าย การพัฒนาเครื่องมือจำกัดการประมวลของอุปกรณ์ค้นหาเส้นทางที่ใช้ทดสอบบนระบบเครือข่ายต้นแบบ สรุปผลการทดสอบ ปัญหาที่พบ และข้อเสนอแนะ ตามลำดับ ดังนี้

1. การศึกษาการเก็บข้อมูลบนระบบเครือข่าย

เป็นการศึกษาการเก็บข้อมูลแพ็กเก็ตการรับและส่งบนระบบเครือข่าย เพื่อนำไปใช้เป็นข้อมูลต้นแบบ สำหรับทดสอบระบบจำกัดการประมวลผลของอุปกรณ์ ซึ่งผู้วิจัยได้พัฒนาเครื่องมือชื่อว่า PacketCab ขึ้นใช้เอง แต่พบว่าไม่สามารถนำข้อมูลดังกล่าวไปสร้างเป็นต้นแบบการรับส่งข้อมูลที่มีลักษณะเดียวกันได้ทั้งหมด เนื่องจากมีสภาวะแวดล้อมที่แตกต่างกัน และพบว่าบางครั้งการประมวลผลของอุปกรณ์ค้นหาเส้นทางมีค่าสูง ผู้วิจัยคาดว่าเกิดจากการที่มีปริมาณของข้อมูล (bandwidth) ที่รับส่งข้อมูลจำนวนมากหรือเกิดจากการใช้งานเป็นจำนวนมาก จนกระทั่งเต็มประสิทธิภาพของอุปกรณ์ หรือเกิดจากโปรแกรมประยุกต์ (Application) อื่น ๆ ที่อยู่นอกเหนือความสนใจของการวิจัยนี้

2. การพัฒนาระบบ

ผู้วิจัยได้พัฒนาระบบจำกัดการทำงานการประมวลผลของอุปกรณ์ค้นหาเส้นทาง หรือ Limited Router CPU Utilization (LRCU) โดยแบ่งการพัฒนาออกเป็นส่วน (Module) ดังนี้ การเก็บข้อมูลบนระบบเครือข่าย การวิเคราะห์ข้อมูล การสร้างกฎควบคุม การแจ้งเตือนและการออกรายงาน โดยผลจากการเก็บข้อมูลบนระบบเครือข่าย จะนำไปใช้ในส่วนของการวิเคราะห์ข้อมูล จากนั้นนำส่งต่อไปยังการสร้างกฎควบคุม แจ้งเตือน และออกรายงาน ตามลำดับ ซึ่งผู้วิจัยพัฒนาระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง ให้สามารถทำงานได้ทั้งแบบอัตโนมัติ และแบบผู้ดูแลระบบสร้างกฎควบคุมได้เอง สามารถตรวจสอบผล และรายงานผลการทำงานของระบบได้โดยการใช้งานผ่านเว็บ

3. การทดสอบระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง

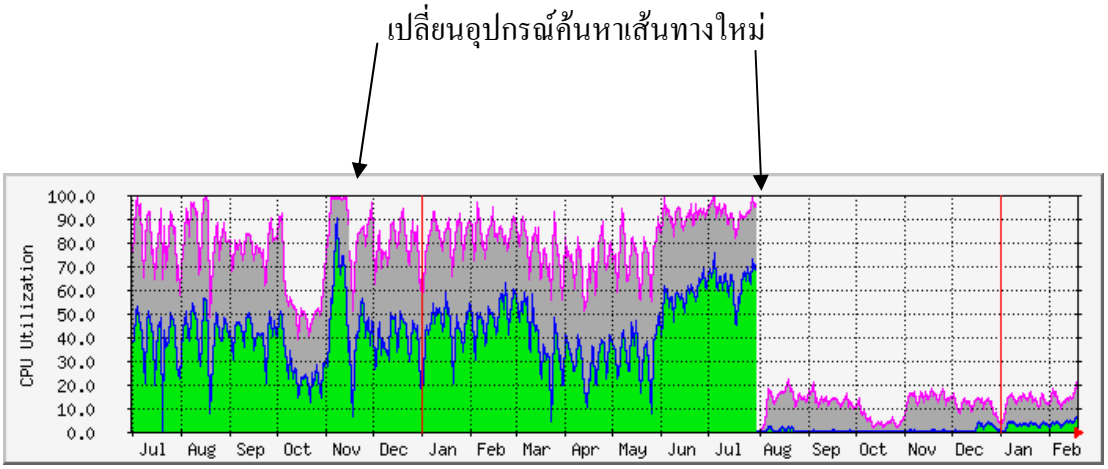
จากผลการทดสอบระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง พบว่าขนาดของอุปกรณ์ค้นหาเส้นทาง ขนาดของข้อมูลที่รับหรือส่ง และขนาดของแบนท์วิธที่ใช้รับส่งข้อมูลมีผลกระทบต่อการประมวลผลของอุปกรณ์ค้นหาเส้นทาง ถ้าปริมาณข้อมูลที่รับหรือส่งมีขนาดใหญ่ หรือจำนวนการติดต่อรับส่งข้อมูลจำนวนมาก ก็จะมีผลกระทบมาก ผู้วิจัยได้ออกแบบวิธีจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทางเป็น 3 วิธี ดังนี้ 1. การควบคุมปริมาณของข้อมูลที่รับส่ง (Bandwidth Model) 2. การกำหนดความสำคัญของข้อมูล (Priority Model) และ 3. การป้องกันการส่งข้อมูล (Deny Model) ซึ่งจากผลการวิจัยทั้ง 3 วิธี พบว่าการควบคุมปริมาณของข้อมูลที่รับส่ง เป็นวิธีการที่ดีที่สุด รองลงมาเป็นการป้องกันการส่งข้อมูล สำหรับการกำหนดความสำคัญของข้อมูล เหมาะสำหรับระบบเครือข่ายขนาดใหญ่หรือองค์ขนาดใหญ่ที่มีจำนวนเครื่องคอมพิวเตอร์ใช้งานบนระบบเครือข่ายจำนวนมาก โดยทั้ง 3 วิธีสามารถจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทางได้ ทำให้การติดต่อแลกเปลี่ยนข้อมูลบนระบบเครือข่ายทำได้เป็นปกติ ตรงตามวัตถุประสงค์ที่ตั้งไว้ นอกจากนี้ยังพบว่าถ้าหากอุปกรณ์ค้นหาเส้นทางมีขนาดหรือประสิทธิภาพแตกต่างกัน การประมวลผลของอุปกรณ์ค้นหาเส้นทางมีค่าที่แตกต่างกัน โดยค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางขนาดเล็ก มีการเปลี่ยนแปลงที่รวดเร็วและมีค่าการประมวลผลสูง และทำให้มีโอกาสได้รับผลกระทบง่ายกว่าอุปกรณ์ค้นหาเส้นทางที่มีขนาดใหญ่ แม้ว่าจะใช้งานในสภาวะแวดล้อมที่เหมือนกัน

ดังนั้นสำหรับหน่วยงานที่มีอุปกรณ์ค้นหาเส้นทางขนาดเล็ก สามารถนำวิธีการจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทางเช่นเดียวกับงานวิจัยนี้ไปประยุกต์ใช้ โดยใช้เทคนิคทั้ง 3 วิธีที่กล่าวมาข้างต้น ไปกำหนดเป็นนโยบายการบริหารจัดระบบเครือข่าย เพื่อทำให้ระบบเครือข่ายสามารถใช้งานอย่างมีเสถียรภาพ ประสิทธิภาพและสนับสนุนการทำงาน เป็นไปตามเป้าหมายของหน่วยงาน และยังทำให้หน่วยงานสามารถประหยัดงบประมาณในการลงทุนอุปกรณ์ราคาสูงได้เป็นอย่างดี

4. ปัญหาที่พบ

เนื่องจากศูนย์คอมพิวเตอร์ได้มีการปรับเปลี่ยนโครงสร้างของเครือข่ายบ่อยครั้ง เพื่อเพิ่มประสิทธิภาพของการใช้งานเครือข่ายดังรูปที่ 26 แสดงการประมวลผลของอุปกรณ์ค้นหาเส้นทางในปัจจุบัน เป็นสาเหตุให้ผู้วิจัยต้องใช้เวลาในการศึกษารูปแบบการใช้งานบนระบบเครือข่ายนานขึ้น นอกจากนี้ยังพบว่ามีจำนวนเครื่องคอมพิวเตอร์ของผู้ใช้มีจำนวนเพิ่มขึ้น และมี

Application หลากหลาย ทำให้ยากต่อการวิเคราะห์รูปแบบการรับส่งข้อมูล จึงจำเป็นต้องศึกษาเครื่องมือต่าง ๆ เพิ่มขึ้น และนำผลของเครื่องมือต่าง ๆ เหล่านั้นมาช่วยในการวิเคราะห์



ภาพที่ 26 แสดงการประมวลผลของอุปกรณ์ค้นหาเส้นทางในปัจจุบัน

จากภาพที่ 26 แสดงการประมวลผลของอุปกรณ์ค้นหาเส้นทางในปัจจุบัน จะเห็นว่าเมื่อมีการเปลี่ยนแปลงอุปกรณ์ค้นหาเส้นทางแต่ละครั้ง ค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางเปลี่ยนแปลงไป ดังจะเห็นได้ชัดเจนตั้งแต่การเปลี่ยนอุปกรณ์ค้นหาเส้นทางครั้งหลังสุด ค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางมีค่าไม่เกิน 20 เปอร์เซ็นต์

การเก็บข้อมูลของการใช้งานบนระบบเครือข่ายมีปริมาณมากเกินกว่าที่ระบบจะรองรับได้ จำเป็นต้องแบ่งช่วงเวลาในการเก็บ โดยการสุ่มเก็บข้อมูลเป็นช่วง ๆ และบางครั้งเมื่อเก็บข้อมูลมาแล้ว พบว่าการทำงานของอุปกรณ์ค้นหาเส้นทางยังทำงานได้เป็นปกติ ทำให้ข้อมูลในช่วงเวลาดังกล่าวอาจจะเป็นข้อมูลตัวอย่างที่ไม่ดี ผู้วิจัยต้องเก็บข้อมูลใหม่หลายครั้ง และยังพบว่าระบบเครือข่ายต้นแบบไม่สามารถจำลองการรับส่งข้อมูลให้เหมือนกับข้อมูลที่เก็บมาในขณะที่เกิดปัญหาขึ้นกับอุปกรณ์ค้นหาเส้นทางได้

อีกปัญหาหนึ่งที่เกิดขึ้นในการทดสอบระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง ผู้วิจัยไม่สามารถใช้อุปกรณ์ค้นหาเส้นทางที่มีคุณสมบัติเทียบเท่ากับอุปกรณ์จริงได้ ทำให้ข้อกำหนดต่าง ๆ ในช่วงทำการทดสอบ ไม่สามารถใช้ได้เมื่อนำไปทดสอบกับระบบเครือข่ายที่เหมือนจริง

5. ข้อเสนอแนะ

5.1 ข้อเสนอแนะสำหรับการนำไปใช้

ในส่วนของเครื่องมือที่พัฒนาขึ้น สามารถนำไปประยุกต์ใช้สำหรับการควบคุมการ Bandwidth บนระบบเครือข่ายของแต่ละผู้ใช้ได้ (IP Address) แต่การแก้ไขข้อกำหนดการทำงาน ทำได้ไม่สะดวกนัก ถ้าต้องการให้สามารถนำไปใช้งานง่ายขึ้นควรได้รับการพัฒนาในส่วนของการติดต่อกับผู้ใช้งาน (User Interfaces) เพิ่มขึ้นมากกว่านี้

จากการทดสอบบนระบบเครือข่ายต้นแบบ จะเห็นได้ว่าสามารถดำเนินการได้ดีกับอุปกรณ์ค้นหาเส้นทางที่มีขนาดเล็ก ดังนั้นระบบที่พัฒนาขึ้นนี้จึงเหมาะกับองค์กรขนาดเล็ก ส่วนองค์กรที่มีอุปกรณ์ค้นหาเส้นทางขนาดใหญ่ และรองรับปริมาณการใช้งานระบบเครือข่ายจำนวนมาก มักไม่ประสบปัญหากับการประมวลผลของอุปกรณ์ค้นหาเส้นทาง จึงไม่เหมาะกับการนำระบบนี้ไปใช้ ยกเว้นจะนำไปประยุกต์กับการใช้งานแบบอื่น ๆ ตามที่กล่าวไว้ในข้างต้น

5.2 ข้อเสนอแนะเพื่อการวิจัยต่อ

งานวิจัยครั้งนี้ ผู้วิจัยได้ทดสอบการใช้งานผ่านเฉพาะโปรโตคอลเฮ็ดทีทีพี และเอฟทีพีเท่านั้น ดังนั้นควรทำการวิจัยกับโปรโตคอลอื่น ๆ เช่น โปรโตคอลอาร์ทีเอส ที่ใช้การรับส่งข้อมูลแบบ streaming หรือนำไปทดสอบกับ Application ประเภทเพียร์ทูเพียร์ (peer to peer) บิตทอร์เร็นท์ (bit torrent) ระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทางนี้จะให้ผลตามวัตถุประสงค์ที่ตั้งไว้หรือไม่ และนำผลการวิจัยเสนอต่อไป

บรรณานุกรม

ภาษาไทย

ซิสโก้. หลักสูตร CCNA 2 Cisco Network Academy Program CCNA 2. กรุงเทพฯ : เพียร์สัน เอ็ดดูเคชั่น อินโดไชน่า, 2547.

ไพศาล ไตรชวโรจน์. “ระบบกระจายการตรวจวัดและเฝ้าดูการส่งข้อมูลในระบบเครือข่าย.” วิทยานิพนธ์ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ, 2547.

เรืองไกร รังสิพล. เจาะระบบ TCP/IP จุดอ่อนของโปรโตคอลและวิธีป้องกัน. กรุงเทพฯ : โปรวิชั่น จำกัด, 2544.

สันติ ดลนภาเขตดำเกิง. “ระบบวิเคราห์ข้อมูลผู้บุกรุกแจ้งเตือนไปยังโทรศัพท์มือถือ.” วิทยานิพนธ์ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ, 2547.

สุทธิชัย สุทธิทศธรรม. “การจัดการแบนด์วิธในเครือข่ายด้วยลินุกซ์.” ในการสัมมนาวิชาการ เรื่อง การ ประชุมวิชาการทางคอมพิวเตอร์และเทคโนโลยีสารสนเทศ, 23 – 31. ตรัง : ม.ป.ท., 2550. (อัดสำเนา)

สุรศักดิ์ สงวนวงศ์. สถาปัตยกรรมและโปรโตคอลทีซีพี/ไอพี. กรุงเทพฯ : ซีเอ็ดยูเคชั่น จำกัด(มหาชน), 2543.

ภาษาต่างประเทศ

Cisco. a Troubleshooting High CPU Utilization on Cisco Routers [Online]. Accessed 12 January 2007. Available from http://www.cisco.com/warp/public/63/highcpu.pdf.

_____. b Troubleshooting High CPU Utilization in IP Input Process [Online]. Accessed 12 January 2007. Available from http://ww.cisco.com/warp/public/63/highcpu_ip_input.pdf.

Stallings,William. Computer Networking with Internet Protocol and Technology. USA : Peason Prentice Hall, 2004.

ภาคผนวก

ภาคผนวก ก

ผลการทดลอง

การพัฒนาระบบการประมวลผลของอุปกรณ์ค้นหาเส้นทาง ประกอบด้วยโปรแกรมต่าง ๆ ดังนี้

โปรแกรมเก็บข้อมูลบนระบบเครือข่าย

PacketCap ทำหน้าที่เก็บข้อมูลการใช้งานบนระบบเครือข่าย ได้ข้อมูลดังภาพที่ 27 ตัวอย่างข้อมูลการใช้งานบนระบบเครือข่าย

GetcpuMysql ทำหน้าที่เก็บค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทาง ได้ข้อมูลดังภาพที่ 28 ตัวอย่างข้อมูลการประมวลผลของอุปกรณ์ค้นหาเส้นทาง

โปรแกรมวิเคราะห์ข้อมูล

Use5Min ทำหน้าที่คำนวณปริมาณการใช้งานของแต่ละไอพีแอดเดรส โดยคำนวณทุก 1 นาทีและ 5 นาที ได้ข้อมูลดังภาพที่ 29 ตัวอย่างข้อมูลที่ได้จากการวิเคราะห์

SaveRule ทำหน้าที่ตรวจสอบการประมวลผลของอุปกรณ์ค้นหาเส้นทาง มีค่ามากว่าค่า threshold หรือไม่ ถ้ามีค่ามากว่าจะเก็บไอพีแอดเดรส ที่ทำให้การประมวลผลของอุปกรณ์ค้นหาเส้นทางมีค่ามากกว่า threshold เมื่อส่งให้โปรแกรมสร้างกฎ ทำงานต่อไป ได้ข้อมูลดังภาพที่ 30 ตัวอย่างข้อมูลจากการสร้างกฎ

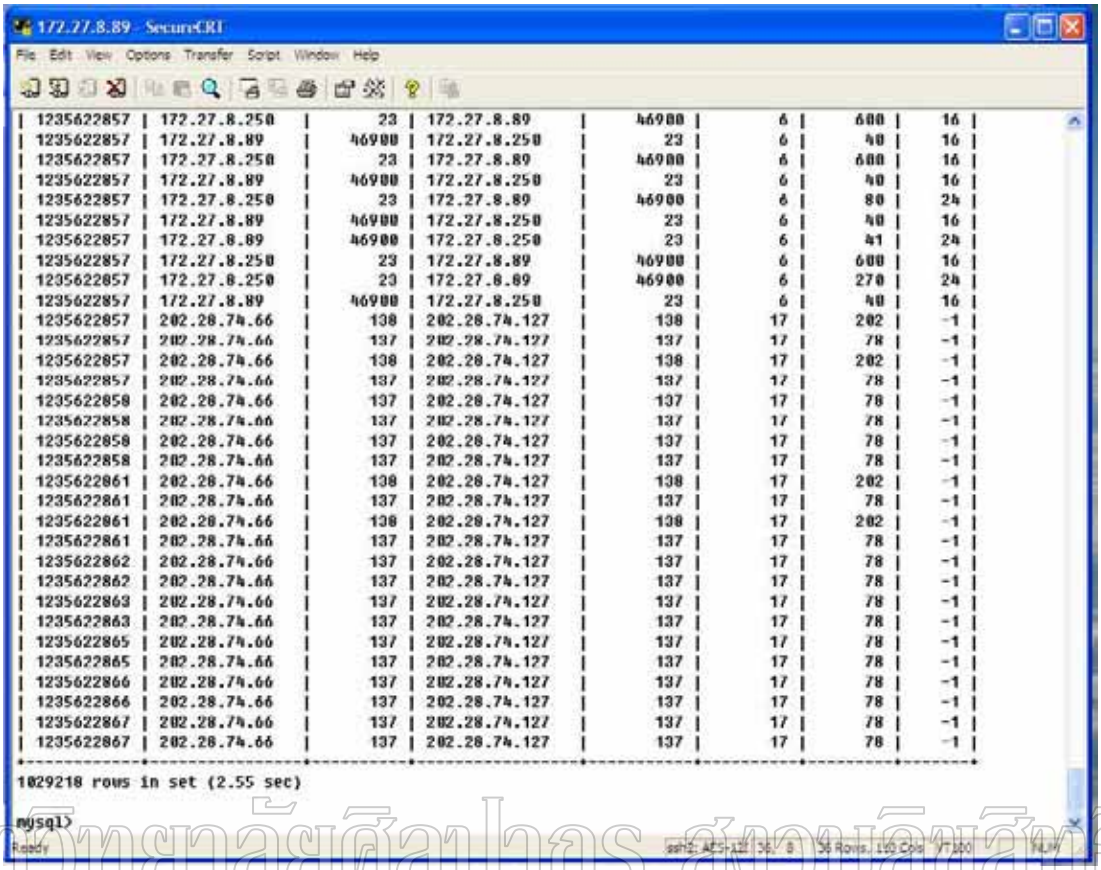
โปรแกรมสร้างกฎควบคุม

ActiveRule ทำหน้าที่วิเคราะห์ข้อมูล สมควรสร้างกฎควบคุมวิธีใดและสร้างกฎควบคุม เพื่อจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง และทำหน้าที่แจ้งเตือนผู้ดูแลระบบ

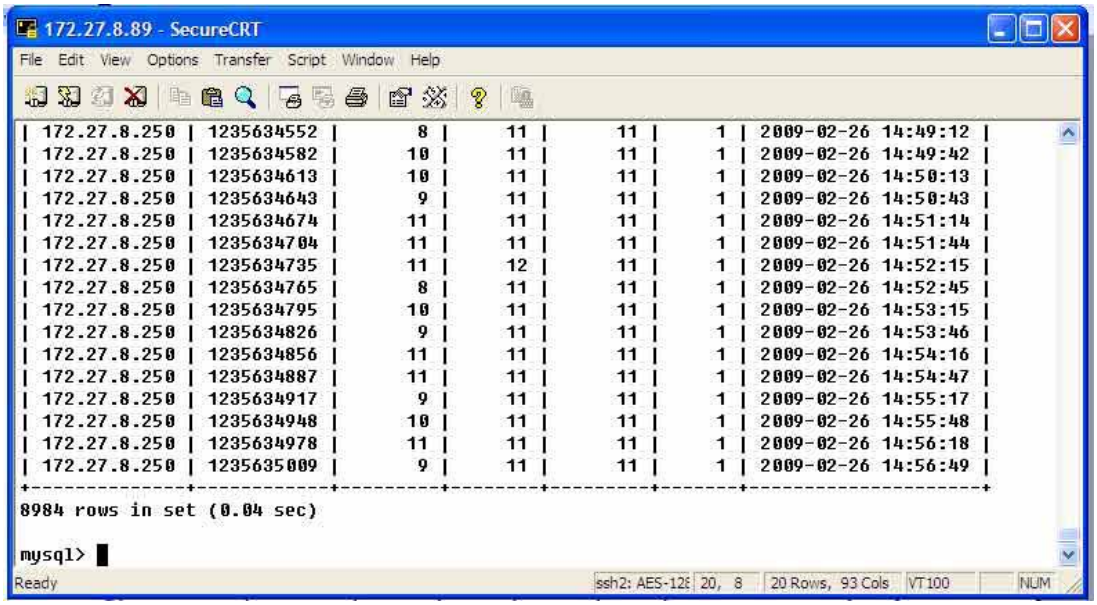
NormalRule ทำหน้าที่ตรวจสอบว่ากฎควบคุม สมควรยกเลิกเพื่อกลับไปทำงานปกติหรือไม่เมื่อเวลาผ่านไปทุก ๆ 15 นาที ถ้าการประมวลผลของอุปกรณ์ค้นหาเส้นทางมีค่าไม่มากกว่าค่า threshold

โปรแกรมรายงานผล

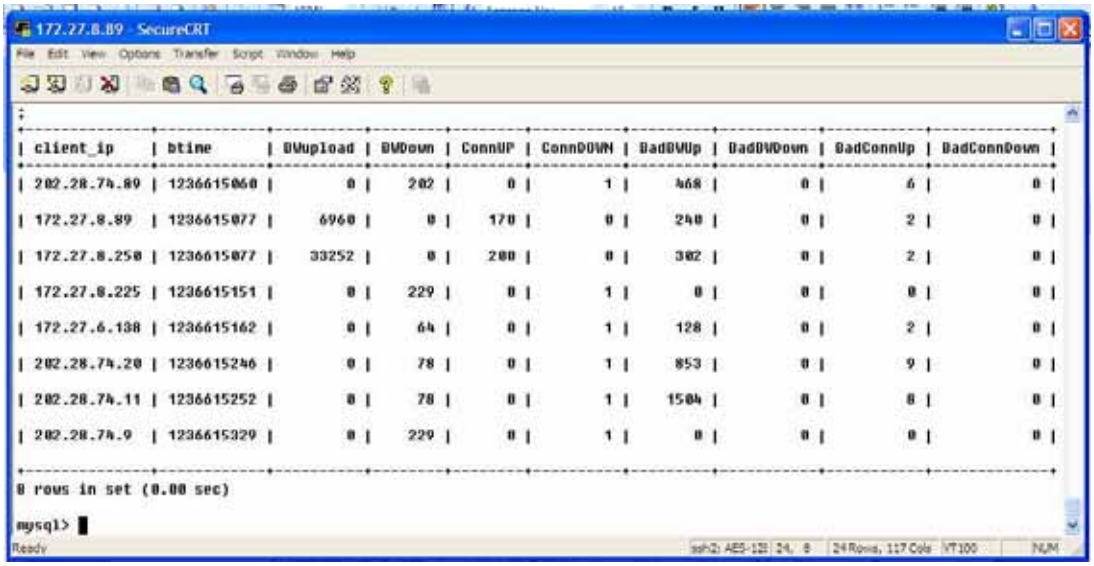
ReportRule ทำหน้าที่รายงานผลการทำงานของระบบ



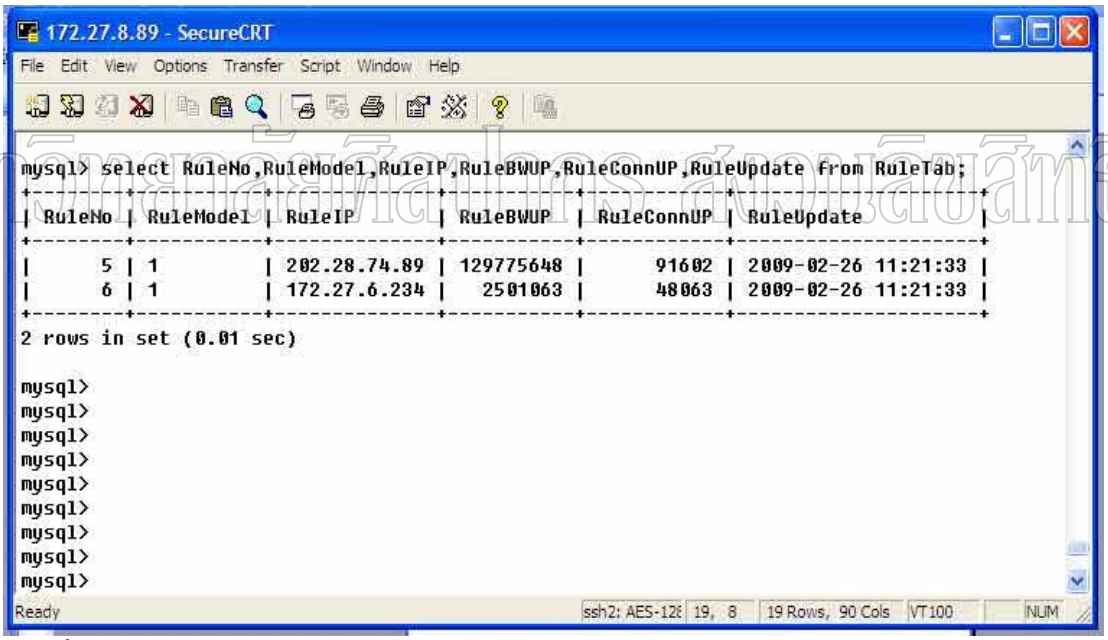
ภาพที่ 27 ตัวอย่างข้อมูลการใช้งานบนระบบเครือข่าย



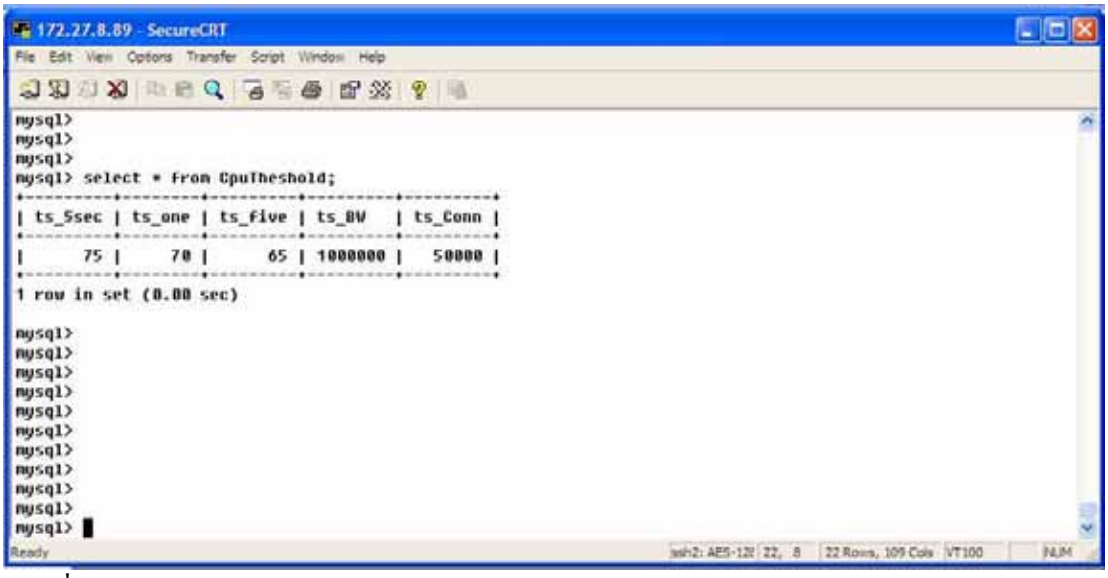
ภาพที่ 28 ตัวอย่างข้อมูลการประมวลผลของอุปกรณ์ค้นหาเส้นทาง



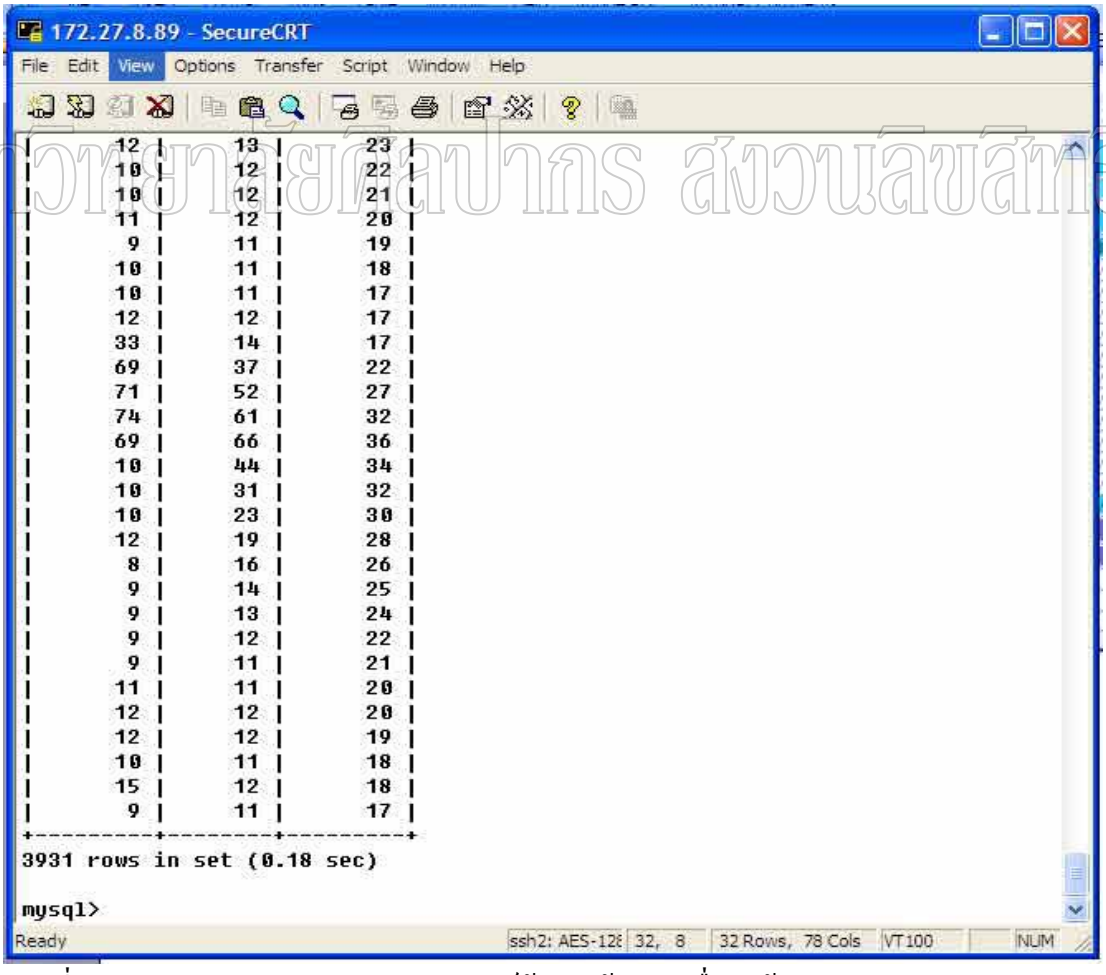
ภาพที่ 29 ตัวอย่างข้อมูลที่ได้การวิเคราะห์ข้อมูล



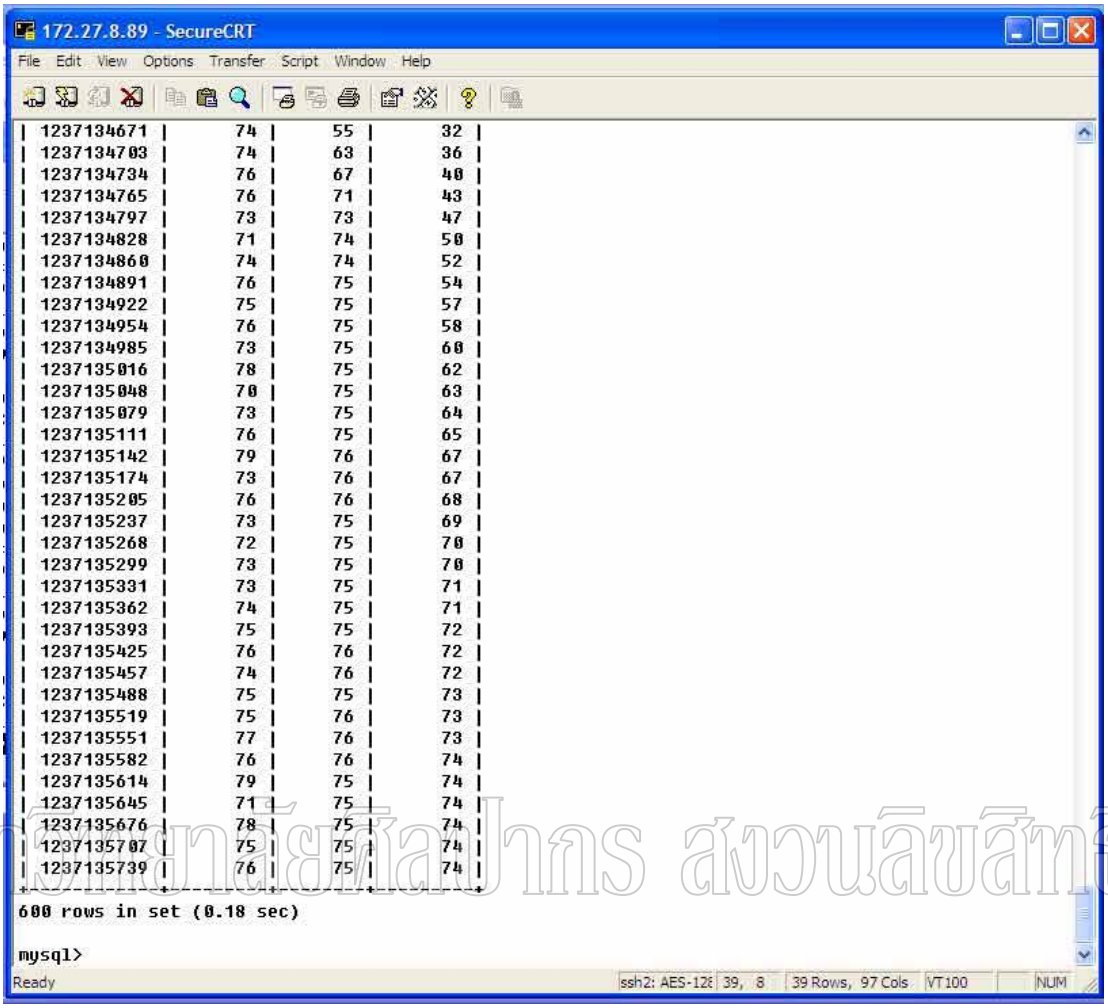
ภาพที่ 30 ตัวอย่างข้อมูลจากการสร้างกฎควบคุม



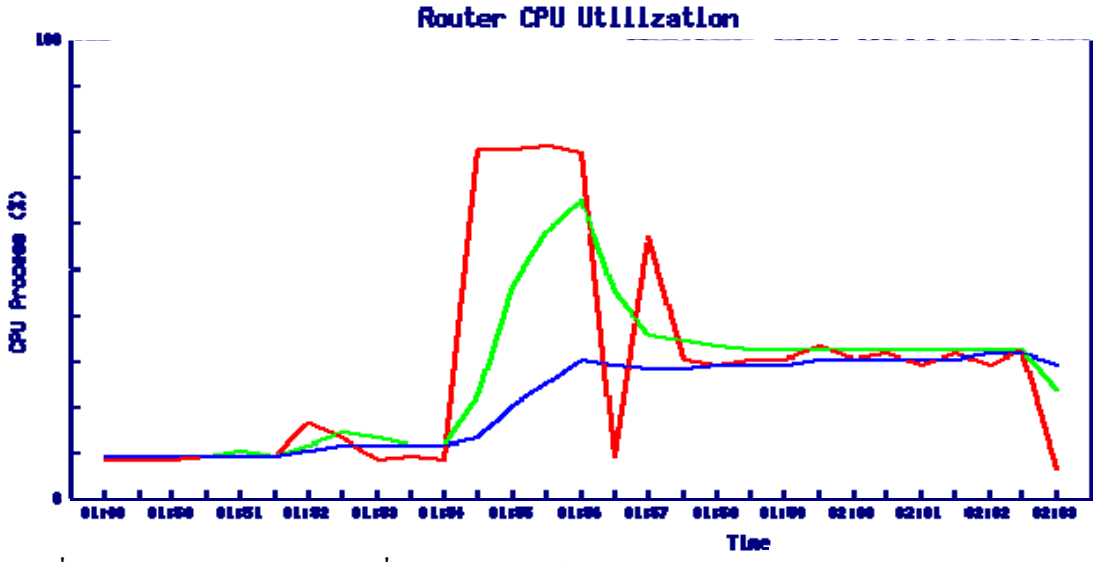
ภาพที่ 31 ตัวอย่างข้อมูลการกำหนดค่า threshold



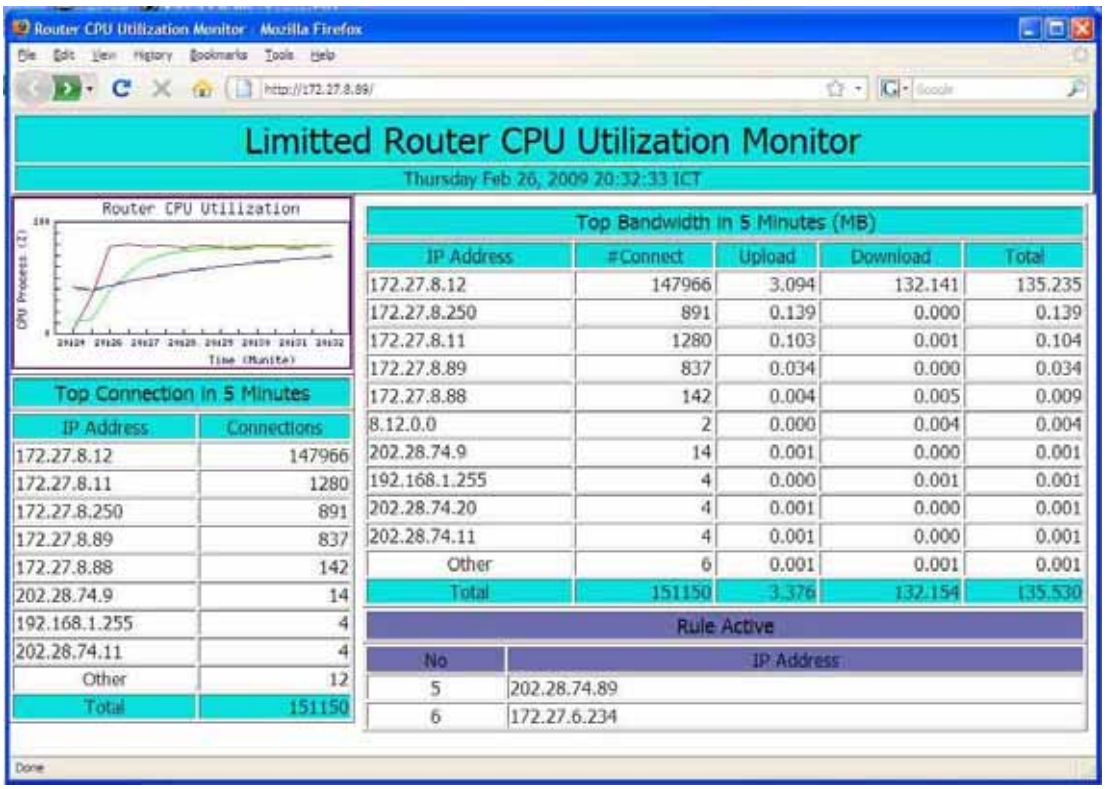
ภาพที่ 32 ตัวอย่างการประมวลผลของอุปกรณ์ค้นหาเส้นทาง เมื่อส่งข้อมูลขนาด 50 MB



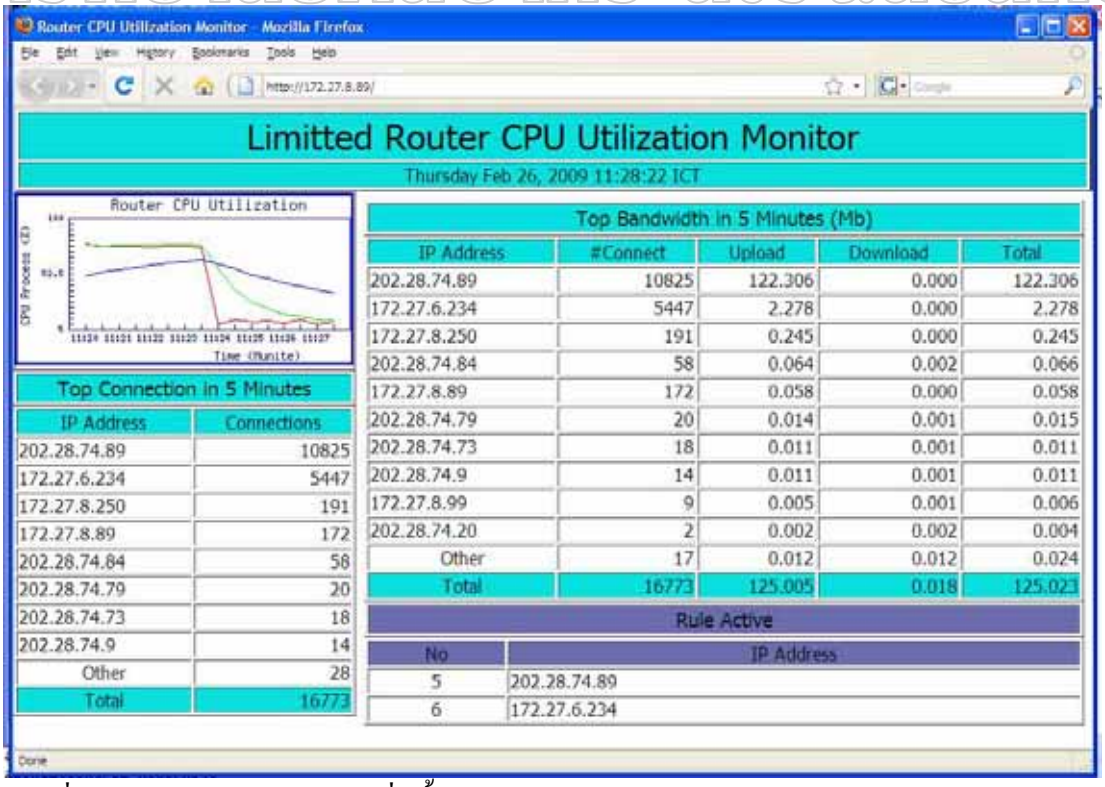
ภาพที่ 33 ตัวอย่างการประมวลผลของอุปกรณ์ค้นหาเส้นทาง เมื่อส่งข้อมูลขนาด 500 MB



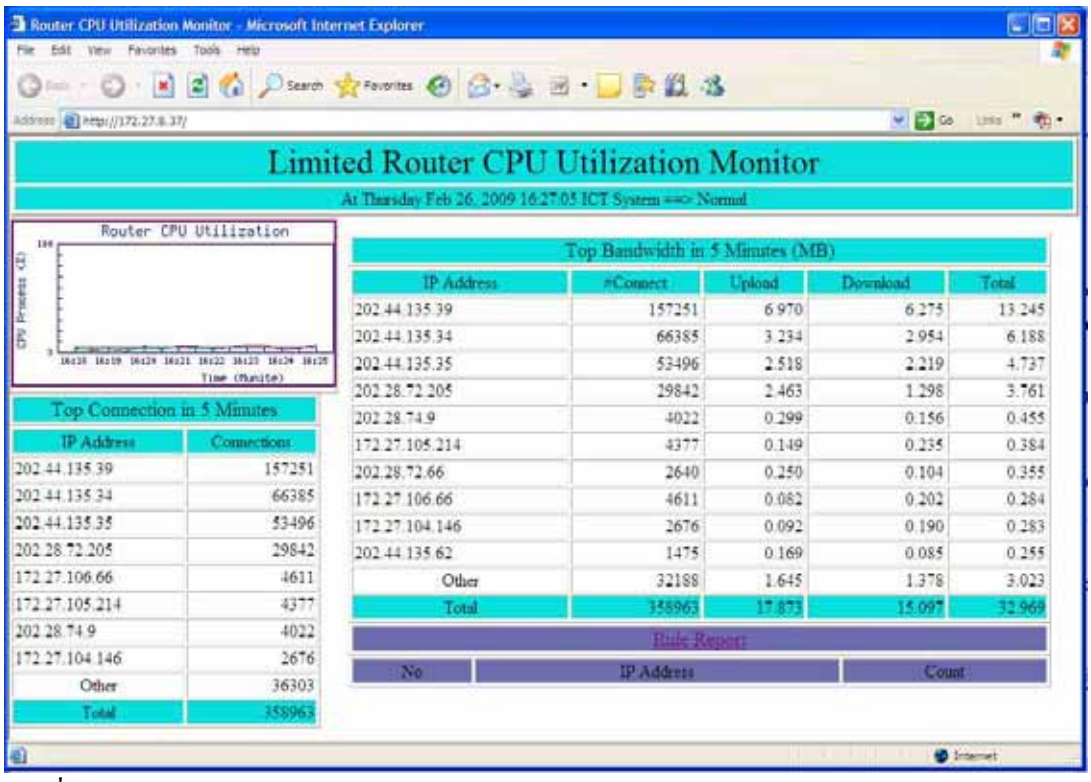
ภาพที่ 34 ตัวอย่างผลการทดลอง เมื่อกำหนดแบนท์วิธขนาด 128 Kbps



ภาพที่ 35 ตัวอย่างผลการทดลอง เมื่อเริ่มรับข้อมูล



ภาพที่ 36 ตัวอย่างผลการทดลอง เมื่อสิ้นสุดการรับข้อมูล



ภาพที่ 37 ผลการทดสอบบนระบบเครือข่ายจริง

ตัวอย่างข้อมูลที่ 1 การสร้างกฎควบคุม ด้วยวิธีควบคุมปริมาณการส่งข้อมูล

DEVICE=eth1,100Mbit,10Bit

RATE=512Kbit

WEIGHT=10Kbit

PRIO=5

IP=172.27.8.8,

ตัวอย่างข้อมูลที่ 2 การสร้างกฎควบคุม ด้วยวิธีควบคุมปริมาณการรับข้อมูล

DEVICE=eth0,100Mbit,10Bit

RATE=128Kbit

WEIGHT=10Kbit

PRIO=5

IP=172.27.8.8

ตัวอย่างข้อมูลที่ 3 การสร้างกฎควบคุม ด้วยวิธีกำหนดความสำคัญของข้อมูลที่ส่ง

DEVICE=eth1,100Mbit,10Bit

RATE=512Mbit

WEIGHT=128Kbit

PRIO=1

IP=172.27.8.8,

ตัวอย่างข้อมูลที่ 4 การสร้างกฎควบคุม ด้วยวิธีกำหนดความสำคัญของข้อมูลที่รับ

DEVICE=eth0,100Mbit,10Bit

RATE=512Mbit

WEIGHT=128Kbit

PRIO=1

IP=172.27.8.8

ตัวอย่างข้อมูลที่ 5 การสร้างกฎควบคุม ด้วยวิธีป้องการส่งข้อมูลไปยังระบบเครือข่ายอื่น

DEVICE=eth1,100Mbit,10Bit

RATE=128Mbit

WEIGHT=128Kbit

PRIO=1

IP=172.27.8.8,

ตัวอย่างข้อมูลที่ 6 การสร้างกฎควบคุม ด้วยวิธีป้องการส่งข้อมูลเข้ามายังระบบเครือข่ายภายใน

DEVICE=eth0,100Mbit,10Bit

RATE=128Mbit

WEIGHT=128Kbit

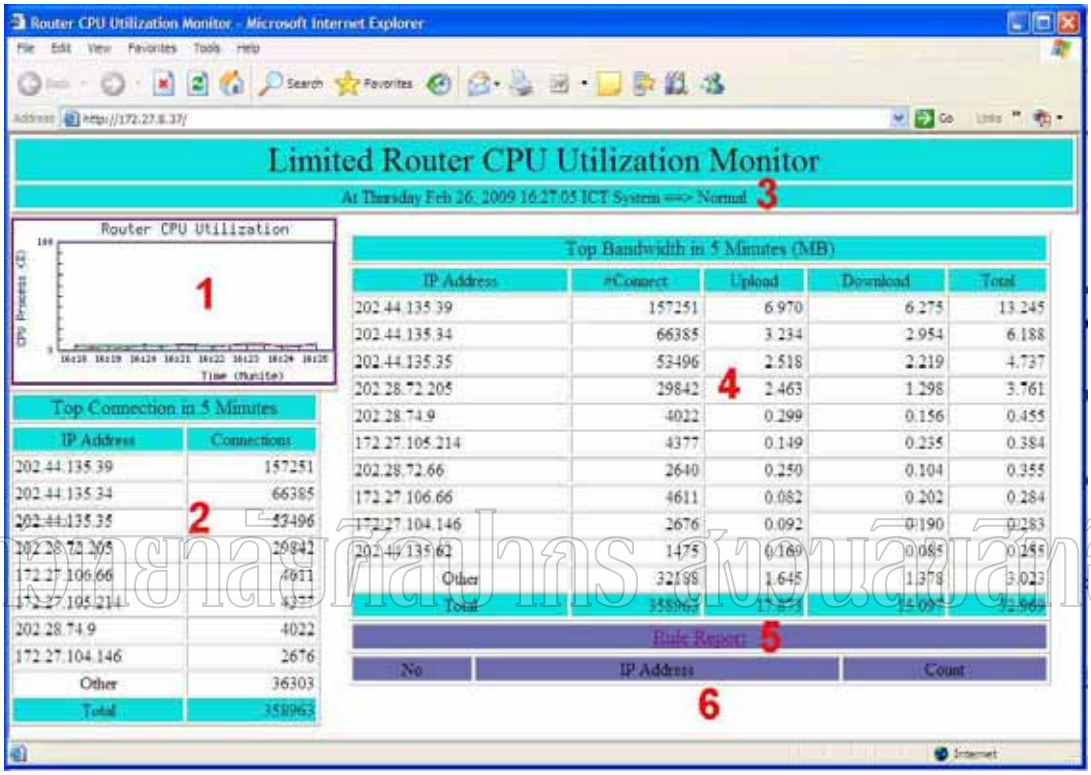
PRIO=1

IP=172.27.8.8

ภาคผนวก ข

การใช้งานระบบ

ระบบจำกัดการประมวลผลของอุปกรณ์ค้นหาเส้นทาง สามารถตรวจสอบการทำงานของระบบ ผ่านเว็บเบราพ์เซอร์ เช่น Internet Explorer (IE) หรือ Firefox ทางยูอาร์แอล (url) หรือไอพีแอดเดรสของเครื่องคอมพิวเตอร์ที่ติดตั้งระบบ (http://172.27.8.89) ได้รายละเอียดดังภาพที่ 38 ตัวอย่างการรายงานผลของระบบ



ภาพที่ 38 ตัวอย่างการรายงานผลของระบบ

จากภาพที่ 38 ตัวอย่างการรายงานผลของระบบ มีรายละเอียดการแสดงผลการทำงานของระบบ 6 ส่วน ดังนี้

ส่วนที่ 1 แสดงกราฟการประมวลผลของอุปกรณ์ค้นหาเส้นทาง (Router CPU Utilization) ถ้าต้องการแสดงโดยละเอียดให้คลิกไปที่รูปกราฟ

ส่วนที่ 2 แสดงปริมาณการเชื่อมต่อ (connection) บนระบบเครือข่ายของแต่ละหมายเลขไอพีแอดเดรส โดยเรียงจากมากไปน้อย

ส่วนที่ 3 แสดงสถานการณ์ทำงานของระบบ เพื่อแจ้งให้ทราบว่าระบบเครือข่ายเป็นปกติ (Normal) หรือตรวจพบว่าค่าการประมวลผลของอุปกรณ์ค้นหาเส้นทางสูงกว่าค่า threshold ที่กำหนดไว้ (Alert)

ส่วนที่ 4 แสดงปริมาณข้อมูลที่รับ (Download) และส่ง (Upload) ของแต่ละหมายเลขไอพีแอดเดรส โดยเรียงจากมากไปน้อย

ส่วนที่ 5 ใช้สำหรับแสดงรายละเอียดหมายเลขไอพีแอดเดรส เวลา การแจ้งเตือน และวิธีที่ระบบควบคุมการทำงาน (Bandwidth, Priority หรือ Deny Model)

ส่วนที่ 6 แสดงหมายเลขไอพีแอดเดรสที่ถูกระบบควบคุม โดยเรียงจากเวลาที่เกิดขึ้นล่าสุดไปยังเวลาที่เกิดขึ้นนานที่สุด

ประวัติผู้วิจัย

ชื่อ-สกุล นายฉลอง วิริยะธรรม
ที่อยู่ ห้อง 303 แฟลตทรงพล 4 มหาวิทยาลัยศิลปากร อ.เมือง จ.นครปฐม 73000
ที่ทำงาน ศูนย์คอมพิวเตอร์ มหาวิทยาลัยศิลปากร อ.เมือง จ. นครปฐม

ประวัติการศึกษา

พ.ศ. 2531 สำเร็จการศึกษาปริญญาวิทยาศาสตรบัณฑิต สาขาศาสตรคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยรามคำแหง

พ.ศ. 2547 ศึกษาต่อระดับปริญญามหาบัณฑิต สาขาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยศิลปากร

ประวัติการทำงาน

พ.ศ. 2531- ปัจจุบัน ศูนย์คอมพิวเตอร์ มหาวิทยาลัยศิลปากร