บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

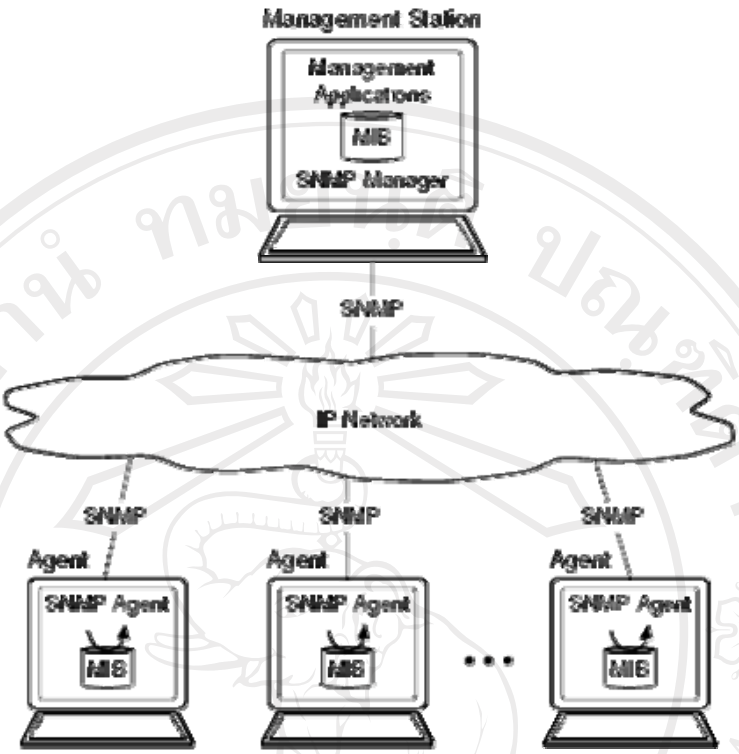
ระบบเครือข่ายในปัจจุบันนี้มีความสำคัญอย่างมาก ไม่ว่าจะเป็นองค์กรขนาดเล็กหรือขนาดใหญ่ล้วนแล้วแต่ต้องนำระบบเครือข่ายเข้ามาใช้เพื่อให้องค์กรมีการทำงานที่มีประสิทธิภาพและประหยัดต้นทุนการผลิต สำหรับทางด้านระบบการตรวจสอบข้อผิดพลาดนั้นมีความสำคัญเป็นอย่างยิ่งที่จะทำให้การทำงานเป็นไปอย่างราบรื่น การตรวจสอบข้อผิดพลาดของระบบจึงมีความจำเป็นเป็นอย่างมาก แต่เนื่องจากเครื่องมือที่ใช้ในการตรวจสอบข้อผิดพลาด ของระบบยังมีอยู่น้อยมาก เป็นผลจากสาเหตุทางด้านฮาร์ดแวร์ ที่มีราคาสูง จึงมีระบบจำนวนน้อยมากที่ยอมลงทุนกับการแก้ปัญหาในด้านนี้ นี่จึงเป็นสาเหตุหนึ่งในการจัดทำโครงงานพิเศษ ในเรื่องโปรแกรมตรวจสอบระบบเครือข่าย (Network Monitor) นี้ขึ้น

2.1 ทฤษฎีพื้นฐานของการบริหารระบบเครือข่าย

ชัยพร ใจแก้ว และคณะ (2543) กล่าวว่า ในการบริหารระบบเครือข่ายขนาดใหญ่ที่ประกอบไปด้วยคอมพิวเตอร์และอุปกรณ์สื่อสารนับร้อยนับพันนั้น มีความสลับซับซ้อนเป็นอย่างยิ่ง มาตรฐานที่ใช้กันแพร่หลายที่สุดคือ SNMP หรือ Simple Network Management Protocal ซึ่งกำหนดโดย IETF (International Engineering Task Force) มาตรฐาน SNMP ครอบคลุมทั้งในเรื่องสถาปัตยกรรมในการบริหารระบบเครือข่าย โปรโตคอลซึ่งใช้ในการติดต่อสื่อสารระหว่างอุปกรณ์และซอฟต์แวร์ต่าง ๆ รวมทั้งลักษณะของข้อมูลซึ่งแสดงคุณสมบัติของอุปกรณ์ในระบบเครือข่าย

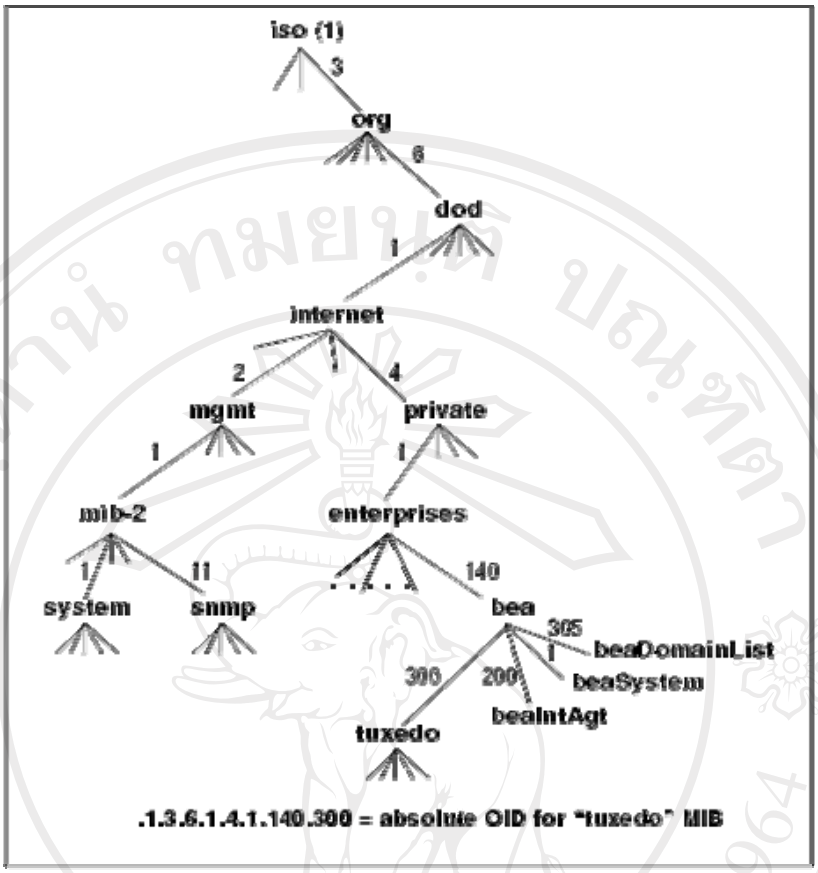
2.2 สถาปัตยกรรมการบริหารระบบเครือข่ายมาตรฐาน SNMP

ชัยพร ใจแก้ว และคณะ (2543) รายงานว่า การบริหารระบบเครือข่ายตามมาตรฐาน SNMP นั้น จำแนกอุปกรณ์ต่าง ๆ ในระบบออกเป็น 2 ชนิด (ดังแสดงในรูปที่ 3) คือ สถานีผู้ดูแลระบบ (Network Management Station-NMS) เป็นส่วนที่ควบคุมการทำงานของเครือข่ายโดยที่ในสถานีจะต้องมีโปรแกรมที่เรียกว่า SNMP Manager ซึ่งทำงานอยู่ตลอดเวลาอุปกรณ์ที่ถูกจัดการ (Managed Node) คือ อุปกรณ์ใดๆในระบบที่สามารถตรวจสอบและควบคุมได้ เช่น โฮสต์ เราเตอร์ ฮับ เป็นต้น



รูปที่ 2.1 องค์ประกอบการจัดการเครือข่ายในเอสเอ็นเอ็มพี

ในอุปกรณ์ระบบเครือข่ายจะต้องมีโปรแกรมที่เรียกว่า SNMP Agent ทำงานอยู่ คุณสมบัติต่าง ๆ ของอุปกรณ์จะถูกเก็บไว้ในมีฐานข้อมูลพิเศษที่ชื่อว่า Management Information Base (MIB) อุปกรณ์ระบบเครือข่ายจะรายงานสถานะไปยัง SNMP Manager โดยอ่านจาก MIB นี้ ภายใน MIB จะบรรจุข้อมูลหลายชนิด เช่น ข้อมูลสถานะของอุปกรณ์และระบบ (System and Device Status Information) สถิติด้านประสิทธิภาพของอุปกรณ์ (Performance Statistics) และค่าต่างของอุปกรณ์ที่กำหนดไว้ (Configuration Parameters) โครงสร้างของ MIB ถูกกำหนดโดย ISO ให้โครงสร้างแบบต้นไม้ (Tree) ในการอ้างถึงแต่ละ Node ภายใน Tree นี้ ทำโดยเริ่มตั้งแต่โหนดที่เป็นรากแล้วไล่ไปกิ่งต่างๆ จนถึงโหนดที่ต้องการ ลักษณะการอ้างโหนดเช่นนี้จะเรียกว่า Object Identifier ดังรูปที่ 2.2



รูปที่ 2.2 โครงสร้างและรูปแบบของ SNMP MIB Object Identifier

การส่งข้อมูลไปสอบถามยังตัว SNMP Agent นั้นจำเป็นที่จะต้องเข้ารหัสตามมาตรฐาน ASN.1 ก่อนที่จะส่งออกไป การติดต่อสื่อสารระหว่างเอเจนต์ต่าง ๆ จะใช้ SNMP โปรโตคอลซึ่งทำงานอยู่บนโปรโตคอล UDP (User Datagram Protocal) ข้อมูลที่มีการส่งโดยอาศัยโปรโตคอล SNMP หรือ SNMP Message ซึ่งช่วยให้เรียกถามสถานะและควบคุมอุปกรณ์ต่างๆ ได้ง่าย

2.3 หลักการพื้นฐานของโปรโตคอล TCP/IP

2.3.1 ลำดับชั้นการทำงานของโปรโตคอล

อนุสรณ์ ใจแก้ว (2548 : 33-37) รายงานว่า ในการศึกษาหลักการทำงานของโปรโตคอลในระบบเครือข่าย (Network Protocols) ใดๆ จะเริ่มต้นด้วยการมองการทำงานของมันเป็นชั้นๆ หรือที่เรียกว่าเลเยอร์ (Layer) การทำงานทั้งหมดของโปรโตคอลจะประกอบไปด้วยหลายๆ เลเยอร์ซึ่งนำมาวางซ้อนกันได้ออกมาเป็นรูปแบบที่เราเรียกว่า Protocol Stack แต่ละเลเยอร์ก็จะมีหน้าที่การทำงานที่ชัดเจนและไม่เกี่ยวข้องกัน แต่ละชั้นจะรู้เพียงวิธีการส่งข้อมูลไปยังชั้นอื่นๆ จะไม่รู้ถึงการทำงานข้างในเลย แต่ละชั้นจะมีการแบ่งการทำงานออกเป็นโปรโตคอลต่างๆ จำนวนไม่

เท่ากัน ทำให้เป็นการยากที่จะระบุว่าโปรโตคอลในระบบเครือข่ายโดยรวมแล้วมีทำงานกี่เลเยอร์ แต่ก็มีมาตรฐานที่เป็นที่ยอมรับกันโดยทั่วไป เรียกว่า Open System Interconnect (OSI) Reference Model ซึ่งทำการแบ่งการทำงานของโปรโตคอลในระบบเครือข่ายออกเป็น 7 เลเยอร์ ดังนี้

7	Application Layer
6	Presentation Layer
5	Session Layer
4	Transport Layer
3	Network Layer
2	Data Link Layer.
1	Physical Layer.

รูปที่ 2.3 โมเดล OSI

แต่ละชั้นก็มีข้อกำหนดและการทำงานที่แน่นอนและไม่เกี่ยวข้องกับชั้นอื่น สำหรับการศึกษาโปรโตคอล TCP/IP นั้นบางที่ก็จะไม่อ้างอิง OSI Reference Model เนื่องจากมีการแบ่งชั้นการทำงานอย่างละเอียดทำให้เข้าใจยาก ดังนั้นจึงมีจะสร้างโมเดลขึ้นมาใหม่เพื่อให้ในการอธิบายการทำงานของโปรโตคอล TCP/IP โดยแบ่งออกเป็น 4 ชั้นดังนี้

Application Layer	Telnet, FTP, e-mail, etc
Transport Layer	TCP, UDP
Internet Layer	IP, ICMP, IGMP
Link Layer	Device driver and interface card

รูปที่ 2.4 โมเดล Internet Reference TCP/IP

1.) เลเยอร์ Application ทำหน้าที่จัดการเกี่ยวกับแอพริเคชันหรือโปรแกรมต่างๆที่ถูกใช้งานโดยผู้ใช้ ตัวอย่างของแอพริเคชันที่ใช้งานโดยทั่วไป เช่น

- Telnet หรือ Remote login เป็นบริการให้ผู้ใช้งานสามารถเรียกใช้งานเครื่องคอมพิวเตอร์จากเครื่องคอมพิวเตอร์ที่อยู่ห่างออกไปได้
- FTP (File Transfer Protocol) เป็นบริการในการโอนถ่ายแฟ้มข้อมูลระหว่างเครื่องคอมพิวเตอร์
- SMTP (Simple Mail Transfer Protocol) เป็นบริการในการรับ-ส่งจดหมายอิเล็กทรอนิกส์
- DNS (Domain Name Service) เป็นบริการแปลงชื่อจากรูปแบบของโดเมนเนม เช่น cmu.chiangmai.ac.th เป็นแบบไอพีแอดเดรส เช่น 202.28.249.1 หรือทำกลับกันในการแปลงไอพีแอดเดรสไปเป็นชื่อโดเมนเนม
- NFS (Network File System) เป็นบริการในการใช้ทรัพยากร เช่น แฟ้มข้อมูลหรือเนื้อที่ระหว่างเครื่องคอมพิวเตอร์ผ่านระบบเครือข่าย

2.) เลเยอร์ Transport ทำหน้าที่ในการจัดเตรียมช่องทางในการส่งผ่านข้อมูลของเลเยอร์ Application ระหว่างโฮสต์ ในเลเยอร์ Transport นี้ยังแบ่งออกเป็น 2 โปรโตคอล ได้แก่

- UDP (User Datagram Protocol)

มีหน้าที่เพียงแค่ทำการจัดส่งข้อมูลที่เรียกว่า Datagram ไปยังโฮสต์ปลายทางโดยไม่มีการตรวจสอบกับปลายทางว่ามีผู้รับหรือไม่ ดังนั้น Datagram ที่ถูกส่งไปอาจจะไม่ถึงปลายทางก็ได้ โดยปกติแล้วถ้าหากใช้โปรโตคอลนี้แล้วต้องการตรวจสอบว่าข้อมูลถึงปลายทางจริงหรือไม่ จะให้โปรแกรมในเลเยอร์ Application ทำหน้าที่ในการตรวจสอบแทน

- TCP (Transmission Connection Protocol)

มีหน้าที่ในการจัดเตรียมเกี่ยวกับความถูกต้องแน่นอนของข้อมูลระหว่างโฮสต์ มีการตรวจสอบข้อมูลระหว่างต้นทางและปลายทาง รวมถึงการจัดการแบ่งข้อมูลจากแอพริเคชันให้มีขนาดพอเหมาะกับเลเยอร์ Network กำหนด Time out ของสัญญาณตอบรับจากโฮสต์ปลายทางและอื่นๆ

3.) เลเยอร์ Network หรือเรียกอีกชื่อหนึ่งว่าเลเยอร์ Internet ทำหน้าที่จัดการเกี่ยวกับการส่งผ่านข้อมูลไปมาของ Packet ในเครือข่ายหรือทำการจัดการเกี่ยวกับการหาเส้นทาง (Routing) นั้นเอง โปรโตคอลในเลเยอร์นี้ได้แก่

- IP (Internet Protocol)

เป็นโปรโตคอลหลักที่ทำงานอยู่ในโปรโตคอล TCP/IP ทำหน้าที่ในการติดต่อกับโปรโตคอลต่างๆทั้ง TCP, UDP, ICMP และ IGMP ในรูปของไอพีดาตาแกรม (IP Datagram) ซึ่งการส่งข้อมูลนั้นจะเป็นการส่งแบบ Connectionless คือจะไม่มีการตรวจสอบ

ปลายทางว่ามีผู้รับหรือไม่ โปรโตคอล IP จะทำหน้าที่เพียงส่งข้อมูลแต่ละดาตาแกรมออกไป และถ้าหากเกิดความผิดพลาดบางอย่างเช่น เกิดปัญหาที่เราเตอร์ก็จะทำเพียงแค่การส่งข้อความด้วย ICMP กลับไปบอกแก่ต้นทางเท่านั้น การตรวจสอบข้อมูลจะเป็นหน้าที่ของเลเยอร์ที่อยู่สูงกว่าขึ้นไป

- ICMP (Internet Control Message Protocol)

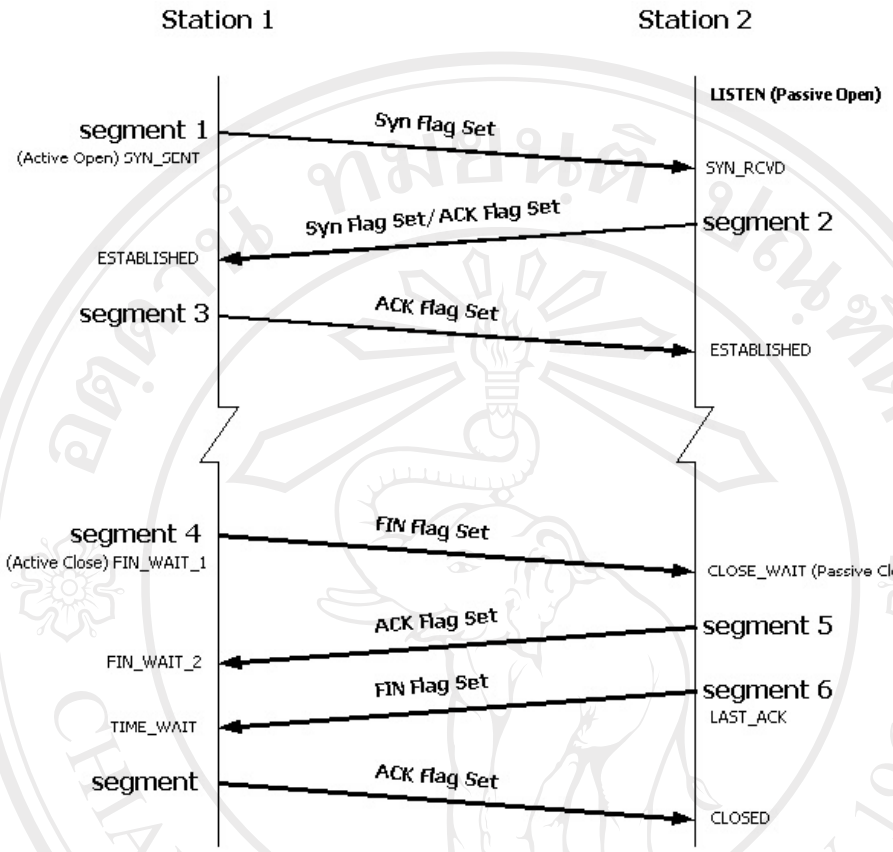
เป็นส่วนประกอบของ IP ซึ่งถูกใช้โดยเลเยอร์ IP ในการเปลี่ยนข้อมูลความผิดพลาดที่สำคัญต่างๆ อันเกิดจากเลเยอร์ IP ของโฮสต์หรือเราเตอร์ต่างๆ ให้เป็นข้อความโดยปกติแล้ว ICMP จะถูกใช้โดยเลเยอร์ IP แต่ก็สามารถถูกใช้โดยเลเยอร์ Application ก็ได้ ตัวอย่างเช่น โปรแกรม Ping และ Traceroute ซึ่งคำสั่งทั้งคู่เป็นแอพริเคชันที่ใช้โปรโตคอล ICMP

- IGMP (Internet Group Management Protocol)

เป็นโปรโตคอลที่ถูกใช้งานโดยโฮสต์และเราเตอร์ที่สนับสนุนการทำงานแบบมัลติแทสกิง (Multicasting) ทำหน้าที่ในการเก็บและส่งข้อมูลเกี่ยวกับมัลติแทสกิงกรุ๊ปของโฮสต์ต่างๆในระบบเครือข่าย โปรโตคอล IGMP เป็นโปรโตคอลที่คล้ายกับ ICMP คือเป็นโปรโตคอลที่เป็นส่วนประกอบของเลเยอร์ IP และข้อมูลถูกส่งออกสู่เครือข่ายด้วยไอพีดาตาแกรม จุดที่แตกต่างจากโปรโตคอลอื่นๆคือ IGMP message จะมีขนาดคงที่เสมอ

4.) เลเยอร์ Link หรือเรียกอีกชื่อหนึ่งว่าเลเยอร์ Data-link โดยปกติแล้วจะหมายถึงไดฟ์เวอร์ของอุปกรณ์ ระบบปฏิบัติการ เน็ตเวิร์คอินเตอร์เฟสการ์ด (Network Interface Card) ของคอมพิวเตอร์ รวมถึงรายละเอียดเกี่ยวกับเคเบิ้ลอินเตอร์เฟส (Cable Interface) ด้วย

2.3.2 สถานะของโปรโตคอล TCP ในการเชื่อมต่อการทำงาน



รูปที่ 2.5 แสดงลำดับและสถานะต่างๆของโปรโตคอล TCP ในการเริ่มต้นและสิ้นสุดการเชื่อมต่อ

ตารางที่ 2.1 แสดงสถานะในการรับส่งของโปรโตคอล TCP

3-Character abbreviation	คำอธิบาย
URG	The urgent pointer is valid
ACK	The acknowledgement number is valid
PSH	Push data to receiving process as soon as possible
RST	Reset connection
SYN	Synchronize sequence numbers
FIN	Sender is finished sending data

2.4 แนวคิด 10 อย่างเพื่อการสร้างเน็ตเวิร์กรีพอร์ตอย่างมีประสิทธิผล

ฟ้าใหม่ สรรค์ใจ (2545) กล่าวไว้ว่า กระแสของอีคอมเมิร์ซทำให้ธุรกิจต้องอาศัยระบบเครือข่ายมากขึ้น และประสิทธิภาพของระบบเครือข่ายก็เป็นผลมาจากการออกแบบ การใช้งานจากภายในหรือภายนอกองค์กร โพรโตคอลที่เลือกใช้ และความผิดปกติของอุปกรณ์ต่างๆ ดังนั้นผู้บริหารเครือข่ายจึงจำเป็นต้องมีเน็ตเวิร์กรีพอร์ต (Network Report) เพื่อใช้แสดงถึงปัญหา ความหนาแน่นในการใช้งาน และการทำงานของระบบเครือข่ายทั้งหมด

ประโยชน์สำคัญที่จะได้รับจากการสร้างเน็ตเวิร์กรีพอร์ตก็คือ ช่วยให้ตัดสินใจแก้ไขปัญหาได้ง่ายขึ้น วางแผนล่วงหน้าได้ และสามารถปรับขนาดระบบเครือข่ายให้สอดคล้องกับการทำงานของผู้ใช้ได้ด้วย ดังนั้นบทความนี้จึงขอนำเสนอแนวคิดในการสร้างเน็ตเวิร์กรีพอร์ต เพื่อให้สร้างรีพอร์ตได้ตรงตามวัตถุประสงค์ของการตรวจสอบยิ่งขึ้น

1. รวบรวมข้อมูลที่มีผลกระทบต่อประสิทธิภาพโดยรวม

เมื่อต้องการสร้างเน็ตเวิร์กรีพอร์ต สิ่งแรกที่ต้องกระทำก็คือการสร้างเนื้อหาในตัวรีพอร์ตซึ่งเกี่ยวข้องกับสิ่งที่ผู้บริหาร หรือลูกค้าของคุณ เห็นว่ามีผลกระทบต่อระบบเครือข่าย โดยลักษณะของเนื้อหาจะขึ้นอยู่กับเทคโนโลยีที่ใช้ในระบบ โพรโตคอล อุปกรณ์ที่ใช้ในระบบเครือข่าย และเน็ตเวิร์กไดอะแกรม ส่วนการสร้างเนื้อหานั้นขอให้ดูเพิ่มเติมจากกรอบ “คำแนะนำในการสร้างเนื้อหาของรีพอร์ต”

2. ใช้รูปช่วยแสดงเนื้อหาที่สำคัญ

ตัวอย่างรูปที่สำคัญได้แก่ ปริมาณแบนด์วิดธ์ที่เครื่องต่างๆ ใช้ในการรับส่งข้อมูล ซึ่งจะช่วยให้วิเคราะห์ต่อไปได้ว่า ทำไมเครื่องคอมพิวเตอร์ดังกล่าวจึงใช้แบนด์วิดธ์มาก หรือเครื่องดังกล่าวมีการทำงานที่ผิดปกติหรือไม่ ซึ่งสาเหตุอาจจะมาจากการสำรองข้อมูลจากไฟล์เซิร์ฟเวอร์ (File Server) หรืออาจจะกำลังรับส่งข้อมูลที่เป็นรูปภาพอยู่

คุณอาจจะจับภาพ (Capture) แอพพลิเคชันที่ใช้วิเคราะห์ระบบเครือข่าย (Network Analyzer) มาประกอบการสร้างรีพอร์ตก็ได้ และแอพพลิเคชันวิเคราะห์ระบบเครือข่ายบางตัว ก็มีความสามารถในการบันทึกภาพอยู่แล้ว

3. แสดงแผนผังระบบเครือข่าย

โดยทั่วไปคุณควรจะมีแผนผังระบบเครือข่ายที่ต้องการตรวจสอบอยู่แล้ว โดยในนั้นจะต้องแสดงถึงเน็ตเวิร์กแอดเดรส การเชื่อมต่อของอุปกรณ์ต่างๆ ตำแหน่งของไฟร์วอลล์ และที่ตั้งของอุปกรณ์ทั้งหมด โดยควรจะแสดงจุดแท็ปข้อมูลสำหรับทำเน็ตเวิร์กรีพอร์ตเอาไว้ อีกทั้งต้องระบุขั้นตอนพิเศษในการตรวจสอบที่เกี่ยวข้องกับอุปกรณ์ในระบบด้วยเช่น ถ้าระบบส่วนใหญ่ประกอบไปด้วยสวิตช์ ก็ต้องระบุด้วยว่าใช้ Port Spanning หรือ Port Mirroring ในการวิเคราะห์

4. ให้คำแนะนำเพิ่มเติมในกรณีที่ไม่สามารถตรวจสอบบางจุดได้

ในระบบเครือข่ายบางแห่ง เราอาจจะไม่สามารถตรวจสอบบางจุดได้ทันที อันเนื่องมาจากตัวระบบประกอบด้วยเทคโนโลยีที่ทันสมัยเกินความสามารถของเครื่องมือที่มีอยู่ หรือมีส่วนใดส่วนหนึ่งของระบบที่เราไม่มีความชำนาญในการตรวจสอบวิเคราะห์ ดังนั้นเราจึงควรแนะนำการตรวจสอบในขั้นต่อไป เช่น ติดตามหาหนทางการทดสอบที่จำเป็น หรือแนะนำผู้ที่มีความชำนาญในส่วนนั้นให้เข้ามาตรวจสอบต่อไป เป็นต้น

การสำรวจระบบก่อนที่จะตรวจสอบนั้นมีความจำเป็นมาก เพราะว่าแอพพลิเคชันที่ใช้อยู่ ระบบปฏิบัติการ โพรโตคอล และอุปกรณ์ที่ใช้ในระบบ จะส่งผลต่อกระบวนการตรวจสอบโดยตรง ซึ่งในกรณีที่ต้องส่งรายงานฉบับนี้ให้กับลูกค้า คุณอาจจะต้องสอบถามข้อมูลจากผู้ดูแลระบบเครือข่ายของลูกค้าก่อน เพื่อให้สามารถตรวจสอบระบบได้ง่ายมากขึ้น

5. สร้างรีพอร์ตให้เข้าใจได้ง่าย

โดยทั่วไปคุณควรระลึกอยู่เสมอว่า ผู้ที่อ่านรีพอร์ตไม่ได้มีประสบการณ์ในการตรวจสอบวิเคราะห์ระบบเครือข่ายลึกถึงระดับแพ็กเกตมากนัก ดังนั้นผู้พิจารณารีพอร์ตจึงเป็นปัจจัยที่ต้องพิจารณาประกอบไปด้วย โดยการสร้างรีพอร์ตให้เข้าใจง่ายนั้น อาจจะใช้วิธีอธิบายคำศัพท์ต่างๆ ที่ใช้ในการตรวจสอบระบบเครือข่าย เช่น คำว่า Latency หรือ Persistent ARP คำอธิบายนั้นควรจะมีเนื้อหาที่กระชับ และเข้าใจง่าย ซึ่งไม่ทำให้ผู้อ่านเกิดความรำคาญขึ้น รวมทั้งอาจจะให้ข้อมูลจากแหล่งอ้างอิงที่น่าเชื่อถืออื่นๆ ประกอบกัน เพื่อให้ผู้อ่านมีความเข้าใจมากขึ้น เช่น ถ้าคุณแสดงความเห็นที่เกี่ยวข้องกับ ARP Querie แบบที่ไม่เป็นมาตรฐานในรีพอร์ต คุณอาจจะต้องให้ข้อมูลเรื่องการควบคุม ARP ใน Request for Comment (RFC) 826 ซึ่งเป็นเรื่องที่อธิบายการติดต่อของ ARP บนอีเทอร์เน็ต

6. ทำรีพอร์ตให้มีเนื้อหากะทัดรัด

เนื่องจากผู้บริหารระบบเครือข่าย หรือหัวหน้าฝ่ายเทคโนโลยี (Chief Technology Office) มีเรื่องที่ต้องพิจารณามากมายในการทำงาน จึงทำให้มีเวลาเหลือในแต่ละวันไม่มากนัก ดังนั้นเนื้อหาของรีพอร์ตจึงต้องกระชับ และชี้แจงสิ่งที่ต้องการทราบอย่างตรงไปตรงมา สำหรับการทำให้รีพอร์ตมีเนื้อหาที่กะทัดรัดนั้น มีเคล็ดลับง่ายๆ ในการทำรีพอร์ตอย่างหนึ่งคือ ที่หน้าแรกของรีพอร์ต (หลังคำนำ) ควรจะเป็นเนื้อหาสำคัญของผลการตรวจสอบระบบโดยสรุป ซึ่งตรงกับสิ่งที่ต้องการทราบจากระบบ ทำให้ผู้บริหารระบบเครือข่ายหรือ CTO สามารถอ่านและเข้าใจผลสรุปได้อย่างรวดเร็ว ส่วนเคล็ดลับอีกอย่างหนึ่งก็คือ ก่อนที่จะเข้าไปตรวจสอบวิเคราะห์ระบบเครือข่าย เราควรจะถามผู้บริหารระบบถึงสิ่งที่เขาต้องการทราบจากการตรวจสอบระบบเครือข่ายอย่างละเอียด เพื่อให้เนื้อหาในรีพอร์ตตรงตามความต้องการอย่างแท้จริง

7. อ้างอิงแพ็กเกตข้อมูลที่ใช้ตรวจสอบ

ในรีพอร์ตควรจะมีบันทึกของแอพพลิเคชันวิเคราะห์ตรวจสอบระบบเครือข่าย (Trace File) ในระดับแพ็กเกตข้อมูล โดยอาจจะใช้ Trace File แสดงการรับส่งของแพ็กเกตในรีพอร์ตก็ได้ ดังนั้นเราจึงควรส่ง Trace File ให้กับผู้บริหารระบบด้วยเสมอ โดยอาจจะบรรจุไว้ในแผ่นดิสก์หรือซีดีรอมก็ได้ เพื่อให้ผู้บริหารระบบสามารถเรียกดูได้ในภายหลัง

8. เรียงเนื้อหาของรีพอร์ตให้เป็นไปตามโมเดลของ OSI

โมเดลของ OSI (Open System Interconnection Model) คือรูปแบบของโครงร่างที่ช่วยให้ผู้พัฒนาผลิตภัณฑ์ทางด้านเน็ตเวิร์กต่างๆ สามารถนำผลิตภัณฑ์จากผู้ผลิตต่างราย มาเชื่อมต่อกันและสื่อสารกันได้ ซึ่งชั้นล่างสุดคือ Physical Layer ถัดมาคือ Data Link Layer ไล่ขึ้นไปจนถึง Application Layer

การเรียงเนื้อหาของรีพอร์ตนั้นควรจะเรียงไปตามโมเดลของ OSI กล่าวคือเรียงเนื้อหาจากการตรวจสอบวิเคราะห์ในระดับ Physical Layer, Data Link Layer, Network Layer เรียงไปจนถึง Application Layer ทั้งนี้เนื่องจากผลของการตรวจสอบสิ่งที่เกิดขึ้นในเลเยอร์ล่าง มักจะเป็นสิ่งที่เข้าใจได้ง่ายกว่าในเลเยอร์ระดับบน ดังนั้นการเรียงเนื้อหารีพอร์ตแบบนี้ก็คือการเรียงเนื้อหาจากง่ายไปสู่ยากนั่นเอง ตัวอย่างเช่น เราอาจจะเริ่มต้นเนื้อหาของรีพอร์ตด้วยการตรวจสอบความหนาแน่นของแพ็กเกตอีเทอร์เน็ต หรือโทเคนริง (Physical Layer) จากนั้นจึงตรวจสอบการบรอดแคสต์ข้อมูล (Data Link Layer) ตรวจสอบการข้ามเครือข่าย (Network Layer) ตรวจสอบการส่งผ่านของโพรโตคอล TCP/IP หรือ IPX (Transport layer) แล้วไล่ไปจนถึงการตรวจสอบในเลเยอร์ระดับบนต่อไป รวมไปถึงสิ่งอื่นๆ ที่ต้องการตรวจสอบ

9. ส่งรีพอร์ตที่เป็นไฟล์ด้วย

นอกจากจะส่งรีพอร์ตที่เป็นรูปเล่มแล้ว คุณก็ควรส่งรีพอร์ตที่อยู่ในรูปของไฟล์แนบไปด้วย เพื่อให้ผู้บริหารระบบสามารถแก้ไข หรือเพิ่มเติมรีพอร์ต ได้ในภายหลังตามต้องการ นอกจากนี้แล้วเนื้อหาของรีพอร์ตควรมีความยาวไม่เกิน 30 หน้า ทั้งนี้ขึ้นอยู่กับขนาดของระบบเครือข่ายที่ตรวจสอบด้วย

10. พึงระลึกอยู่เสมอว่าข้อมูลในรีพอร์ตเป็นความลับ

สิ่งต่างๆ ที่อยู่บนระบบเครือข่ายไม่ว่าจะเป็น พาสเวิร์ด โพรโตคอล ค่าคอนฟิกกูเรชัน เน็ตเวิร์กแอดเดรส ฯลฯ ของแต่ละบริษัทถือเป็นความลับ ดังนั้นข้อมูลในรีพอร์ตซึ่งมีรายละเอียดต่างๆ ของระบบเครือข่ายจึงต้องเป็นความลับด้วย ถ้าจำเป็นต้องส่งไฟล์รีพอร์ตให้กับผู้บริหารเครือข่ายทางอินเทอร์เน็ต ก็ให้เข้ารหัสหรือใส่พาสเวิร์ดให้กับรีพอร์ตไฟล์ รวมไปถึง Trace File ที่แนบไปกับรีพอร์ตด้วย หรือในบางกรณี ก็อาจจะใช้วิธีซ่อนเน็ตเวิร์กแอดเดรสหรือโหนดแอดเดรส

ใน Trace File โดยกำหนดให้ผู้บริหารระบบเท่านั้นที่มีสิทธิดูได้ แต่วิธีที่ดีที่สุดก็คือการส่งถึงมือผู้บริหารเครือข่ายด้วยตัวเอง

ทั้งหมดที่กล่าวมาถือเป็นแนวคิดในการสร้างเน็ตเวิร์กรีพอร์ตอย่างหนึ่ง เพื่อให้รีพอร์ตมีความน่าอ่าน ง่ายต่อการเข้าใจ มีข้อมูลที่ตรงตามความต้องการ และมีประโยชน์มากพอสำหรับการนำไปใช้ในงานด้านอื่นได้ อย่างไรก็ตามการทำเน็ตเวิร์กรีพอร์ตที่ดีก็มีแนวทางในการสร้างได้หลายวิธี

ในการสร้างเนื้อหาของรีพอร์ตนั้น จะสร้างขึ้นจากสิ่งที่ผู้บริหารระบบ หรือลูกค้า ต้องการจากการตรวจสอบวิเคราะห์ หรือสิ่งที่มีผลกระทบต่อระบบเครือข่าย เมื่อรวบรวมความต้องการได้แล้ว เราอาจจะนำความต้องการเหล่านั้นมาเรียบเรียงเป็นบทนำก่อน แล้วจึงตรวจสอบวิเคราะห์ไปตามบทนำที่ได้ร่างไว้ สิ่งที่ผู้บริหารระบบมักต้องการทราบมีดังนี้ เช่น ในขณะนี้การรับส่งข้อมูลในระบบอีเทอร์เน็ต (หรือโทเคนริง) เป็นอย่างไร มีความหนาแน่นมากน้อยแค่ไหน ประสิทธิภาพของการออกแบบระบบโดยรวมเป็นอย่างไร มีความสามารถในการรองรับงานได้เท่าไร บางครั้งก็ไม่สามารถส่งข้อมูลที่ใช้โพรโตคอล TCP/IP ไปยังสำนักงานต่างสาขาได้ เราเตอร์ทำงานผิดปกติหรือไม่ มีสิ่งผิดปกติอื่นๆ เกี่ยวกับการติดต่อสื่อสารหรือไม่ และอย่างไร จากคำถามจะเห็นได้ว่า สิ่งที่ผู้บริหารต้องการทราบ หรือปัญหาต่างๆ ที่เกิดขึ้นในระบบเครือข่าย จะขึ้นอยู่กับโพรโตคอลที่ใช้ ระบบปฏิบัติการเครือข่าย (NOS) การทำงานของอุปกรณ์สื่อสารเช่น ฮับ สวิตช์ หรือเราเตอร์ คอนฟิกกูเรชันของตัวอุปกรณ์ โทโปโลยีของระบบ จำนวนผู้ใช้หรือการเพิ่มขยายระบบ และการทำงานของแอพพลิเคชันในระบบเครือข่าย สิ่งต่างๆ เหล่านี้ล้วนมีผลกระทบต่อการทำงานของระบบทั้งสิ้น ดังนั้นผู้ที่ตรวจสอบวิเคราะห์ระบบเครือข่ายจึงจำเป็นต้องมีประสบการณ์ และเข้าใจการทำงานของระบบเครือข่ายในระดับแพ็กเกตเป็นอย่างดี เพื่อให้ได้ผลการตรวจสอบที่ถูกต้อง และสามารถนำผลไปใช้งานในด้านอื่นๆ ได้อย่างมีประสิทธิภาพ เมื่อได้สิ่งที่ผู้บริหารต้องการทราบแล้ว คุณก็นำคำถามเหล่านี้มาสร้างหัวข้อ และเนื้อหาในการตรวจสอบระบบ โดยตัวอย่างคำถามดังกล่าวจะนำไปสู่หัวข้อในรีพอร์ตต่อไป

2.5 โปรแกรม MRTG

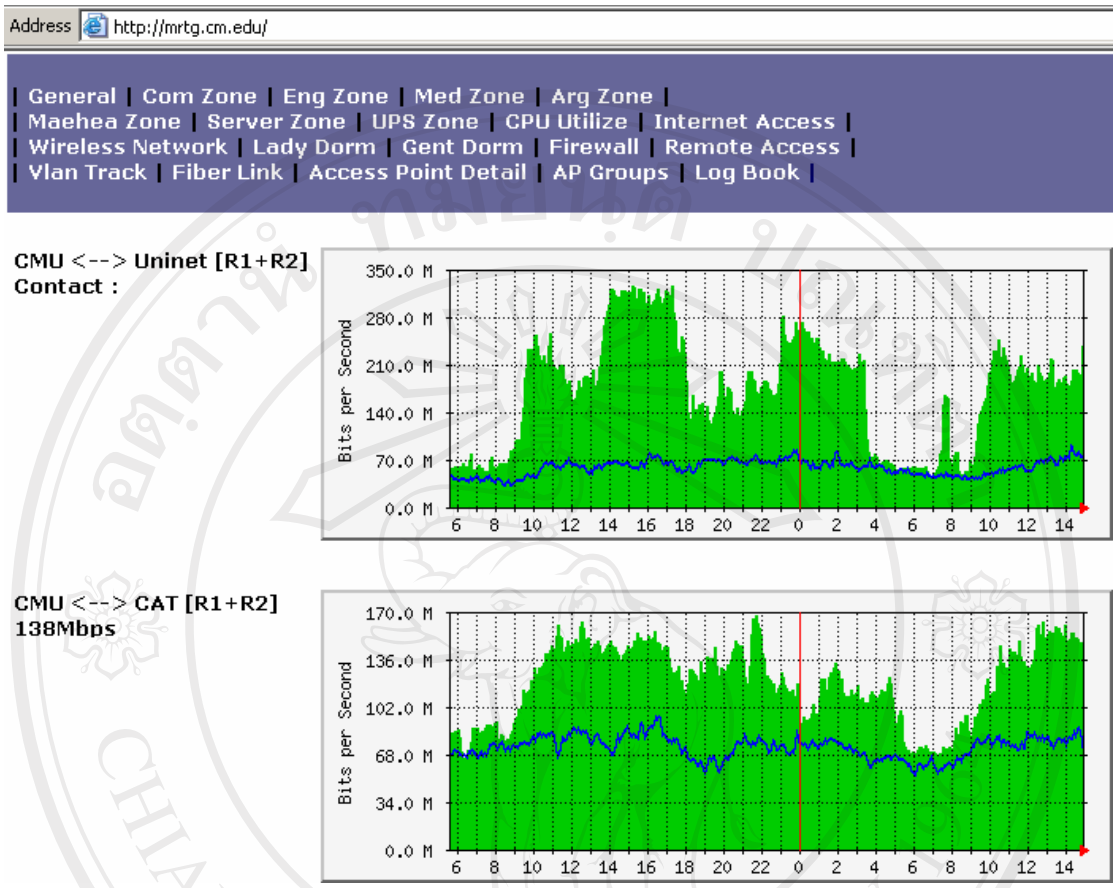
ธรีภัทร มนตรีศาสตร์ (2545) รายงานว่า MRTG ย่อมาจาก Multi Router Traffic Grapher เป็นโปรแกรมที่ใช้งานได้ฟรี สามารถ Download ได้จากเว็บไซต์ต่างๆ โดยโปรแกรม MRTG สามารถตรวจสอบสถานะปริมาณของ ทราฟฟิกบนระบบเครือข่าย และ แสดงเป็นรูปกราฟผ่านหน้าเว็บเพจ ซึ่งสามารถมอนิเตอร์ข้อมูลผ่านโปรแกรมเว็บบราวเซอร์ได้ทันที การนำไปใช้งานส่วนใหญ่จะใช้ตรวจสอบว่ามีอัตราการส่งข้อมูลมากน้อยเพียงใด และ สามารถตรวจสอบได้ว่าเกิดปัญหาในช่วงเวลาใด แต่คุณสมบัติเหล่านี้ไม่ได้เกิดจากตัวโปรแกรม MRTG แต่เพียงลำพัง ยังต้องอาศัยโปรแกรมอื่น ๆ เข้ามาสนับสนุนอีกจึงจะสามารถทำงานที่กล่าวไว้ได้ครบถ้วนสมบูรณ์ ซึ่งมีลำดับการทำงานดังนี้

1. การที่จะรวบรวมข้อมูลต่างๆ จากระบบเครือข่ายมาได้ จำเป็นต้องอาศัยเครื่องมือที่ทำหน้าที่เป็นตัวแทนของเรา หรือที่ เรียกว่า Agent เฝ้าจับตาดูความเปลี่ยนแปลงของระบบเครือข่ายและส่งข้อมูลออกมาให้ทราบ โดยปรกติจะอาศัยโปร โตคอล SNMP (Simple Network Management Protocol) ซึ่งเป็นคุณสมบัติหนึ่งภายในอุปกรณ์เราเตอร์ (Router) หรือ สวิตซ์ (Switches) ทำหน้าที่เป็น Network Management Server

2. โปรแกรม MRTG จะอ่านข้อมูลผ่าน SNMP Agent ตามระยะเวลาการสุ่มข้อมูลที่กำหนดไว้ แล้วพล๊อตกราฟ เป็นไฟล์รูปภาพ เก็บไว้ ที่ไดเร็คทอรี่ที่กำหนดไว้

3. โปรแกรมที่ทำหน้าที่เป็นเว็บเซิร์ฟเวอร์จะนำเสนอข้อมูลกราฟที่สร้างจาก MRTG ผ่านทางโปร โตคอล HTTP ทำให้สามารถดูกราฟแสดงรายงานการใช้แบนด์วิธได้จากโปรแกรมเว็บบราวเซอร์

จากการค้นหาข้อมูลทำให้ทราบสถานบันหลายแห่งที่ได้ใช้โปรแกรม MRTG ในการตรวจสอบ Network Traffic ตัวอย่างเช่น มหาวิทยาลัยเชียงใหม่ บริษัท เอเน็ตจำกัด มหาวิทยาลัยศรีนครินทรวิโรฒ มหาวิทยาลัยราชภัฏสงขลา มหาวิทยาลัยมหาสารคาม ฯลฯ และในส่วนของสถาบันต่างประเทศที่ใช้งานโปรแกรม MRTG ได้มีการรวบรวมไว้ที่เว็บไซต์
http://www.mrtg.jp/en/users.html



รูปที่ 2.6 แสดงรูปภาพแสดงการใช้งานโปรแกรม MRTG ของมหาวิทยาลัยเชียงใหม่

จากการศึกษาและใช้งานโปรแกรม MRTG นี้ทำให้ทราบถึงปัญหาที่เกิดขึ้นในโปรแกรมนี้ คือจะไม่สามารถเรียกข้อมูลที่เก็บรายละเอียดต่อวันย้อนหลังกลับมาแสดงผลได้อีก ทำให้การเรียกดูข้อมูลย้อนหลังนั้นเรียกดูได้ไม่ครบถ้วนหรือขาดหายไปในบางช่วงเวลา ข้อมูลนี้มีความจำเป็นในบางกรณีเช่น กรณีที่ระบบมีปัญหาไม่สามารถให้บริการกับลูกค้ารายองค์กร ที่ได้ทำสัญญาว่า เมื่อระบบเกิดปัญหาไม่สามารถให้บริการอินเทอร์เน็ตได้จะมีการเรียกเก็บเงินคืนตามระยะเวลาที่ขาดหายไปนั้น โปรแกรม MRTG นี้จะไม่สามารถแสดงช่วงเวลาที่ระบบขัดข้องย้อนหลังได้เมื่อเหตุการณ์ได้ผ่านไปแล้ว 1 วัน

2.6 โปรแกรม CACTI Traffic Grapher

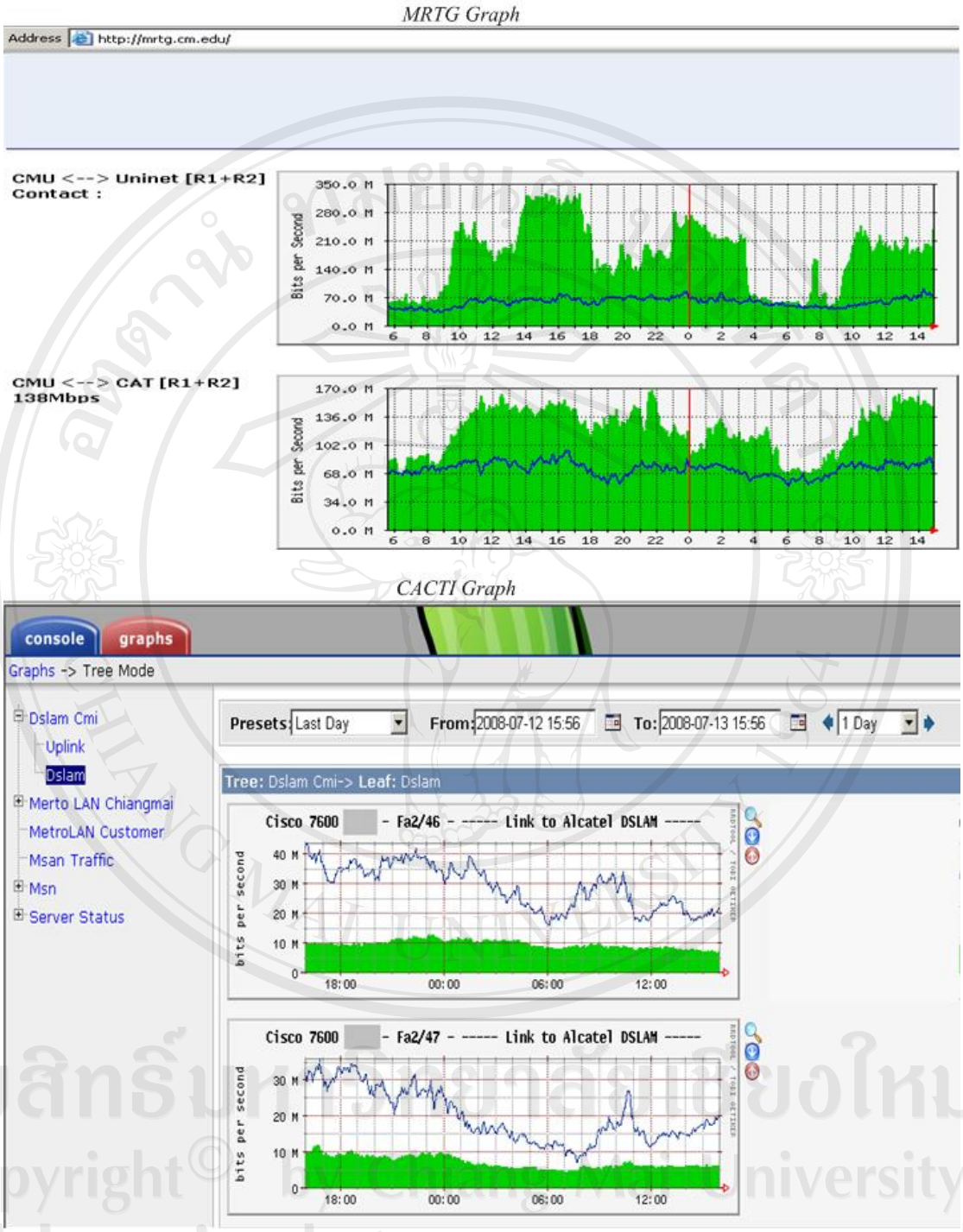
Ian Berry and others (2550) โปรแกรม CACTI Traffic Grapher หรือเรียกกันสั้นๆว่า “CACTI” เป็น Open Source Software ซึ่งทำหน้าที่ในการแสดงปริมาณข้อมูลทั้งขาเข้า/ออก ในเครือข่าย โดยจะแสดงผลออกมาในรูปแบบของกราฟ สามารถเข้าใจและเปรียบเทียบระดับการใช้

งานได้ง่ายขึ้น อีกทั้งยังมีประสิทธิภาพเพิ่มขึ้นจาก กราฟในรูปแบบเดิมซึ่งใช้ โปรแกรม MRTG ด้วยความละเอียดของมุมมองด้านต่างๆ ที่มากขึ้น โปรแกรม CACTI จะใช้หลักการทำงานของโปรโตคอล Simple Network Management Protocal (SNMP) ซึ่งหมายความว่าอุปกรณ์ทุกชนิดที่มีการใช้โปรโตคอล SNMP โปรแกรม CACTI จะสามารถทำการตรวจสอบสถานะของอุปกรณ์นั้นๆ ได้ และการจะนำข้อมูลมาใช้งานได้นั้นจะต้องมีการสร้าง Script เพื่อเป็นตัวเชื่อมต่อไปยังอุปกรณ์ที่เราต้องการร้องขอข้อมูลมาใช้งาน โปรแกรม CACTI ได้ใช้ RRDTool เพื่อทำการจัดเก็บข้อมูล

RRD เป็นคำศัพท์ที่ย่อมาจาก Round Robin Database ซึ่งเป็นระบบที่มีการจัดเก็บและแสดงผลข้อมูลตามช่วงเวลาที่มีความต่อเนื่อง ยกตัวอย่างข้อมูลประเภทนี้เช่น ปริมาณการใช้ Bandwidthของเครือข่าย อุณหภูมิของห้องคอมพิวเตอร์ Sever load average ฯลฯ ซึ่งข้อมูลจะมีการเก็บอย่างกระชับแน่นอน จะไม่มีการขยายพื้นที่เพิ่มขึ้นแม้ว่าเวลาจะมีเพิ่มขึ้นก็ตาม

จากที่ได้ทำการค้นคว้าข้อมูลเกี่ยวกับโปรแกรม CACTI Traffice Grapher ทำให้ได้ทราบว่าได้มีองค์กรที่ได้ใช้โปรแกรม CACTI Traffice Grapher ในองค์กรแล้ว คือ ทีโอที จำกัด บริษัท กสท โทรคมนาคม จำกัด (มหาชน) มหาวิทยาลัยราชภัฏเชียงราย ฯลฯ

โดยหลักการทำงานทั่วไป ทั้ง MRTG และ CACTI สามารถแสดงผลกราฟได้เหมือนกัน แต่มีความแตกต่างระหว่าง MRTG กับ CACTI Traffic Grapher คือ CACTI ใช้ RRDTool เป็นตัวทำงาน จึงสามารถเก็บข้อมูลให้อยู่ในรูปแบบ Database จึงทำให้สามารถย้อนกลับไปดูกราฟในวันและเวลาที่ต้องการ อีกทั้งยังสามารถ Zoom กราฟที่แสดงเพื่อรายละเอียดที่มากขึ้น รวมถึงรูปแบบการแสดงผลที่สวยงาม และมีประสิทธิภาพมากกว่า ซึ่งทั้งหมดนี้สามารถทำให้เข้าใจและนำข้อมูลสถิติต่างๆมาใช้ได้ง่ายขึ้น



รูปที่ 2.7 แสดงรูปภาพแสดงการแสดงผลกราฟระหว่างโปรแกรม MRTG กับโปรแกรม CACTI

2.7 โปรแกรม Whatsup Gold

Ipswitch (2548) โปรแกรม Whatsup Gold เป็นโปรแกรมที่ทำงานบนระบบปฏิบัติการ Windows ซึ่งทำให้เกิดความสะดวกและงานในการตรวจสอบระบบเครือข่าย โปรแกรมนี้จะช่วยให้

ผู้จัดการระบบเครือข่ายเก็บรวบรวมข้อมูลระบบเครือข่ายเพื่อนำไปใช้ในการวิเคราะห์และวางแผนการใช้งานทรัพยากรณ์ระบบให้เหมาะสมกับองค์ ณ ปัจจุบันที่ผู้วิจัยได้ทำการศึกษาอยู่นี้ได้มีถึง Version 11 ซึ่งมีคุณลักษณะดังนี้

- มีระบบการค้นหาอุปกรณ์ Network ที่อยู่ในระบบเครือข่ายขององค์กร
- มีส่วนติดต่อผู้ใช้งานให้สามารถรับข้อมูลอุปกรณ์เครือข่ายที่ไม่อยู่ใน Network ขององค์กรและอุปกรณ์ประเภท Virtualized devices
- โปรแกรมรองรับการตรวจสอบผ่านมาตราฐาน SNMP และ WMI
- มีการแจ้งเตือนแก่ผู้ดูแลระบบเมื่อมีการเปลี่ยนแปลงสถานะของอุปกรณ์ที่ทำการตรวจสอบสถานะ
- สามารถเพิ่มหรือลดข้อมูล MIB ที่ต้องการตรวจสอบตามมาตรฐาน SNMP และ WMI ด้วยการ Drag and Drop
- มีการเก็บข้อมูลระบบเครือข่ายแบบ Real-time เพื่อนำมาทำเป็นรายงานทั้งรูปแบบทาง Technical และ Business
- โปรแกรมพัฒนาโดยมีหลักการทำงานแบบ Workspace และสร้างเป็นแผนภาพระบบเครือข่าย เพื่ออำนวยความสะดวกแก่ผู้ดูแลระบบในการระบุปัญหาที่เกิดขึ้นในระบบเครือข่าย
- เป็นโปรแกรมที่สามารถควบคุมผ่านทางเว็บไซต์ หรือ โทรศัพท์เคลื่อนที่เพื่ออำนวยความสะดวกแก่ผู้ดูแลระบบ

เมื่อติดตั้งโปรแกรมเรียบร้อยแล้วนั้น โปรแกรมจะทำการกำหนดค่า Simple Network Management Protocol (SNMP) เพื่อตรวจสอบประสิทธิภาพของอุปกรณ์เครือข่ายหลัก 5 รายการต่อไปนี้

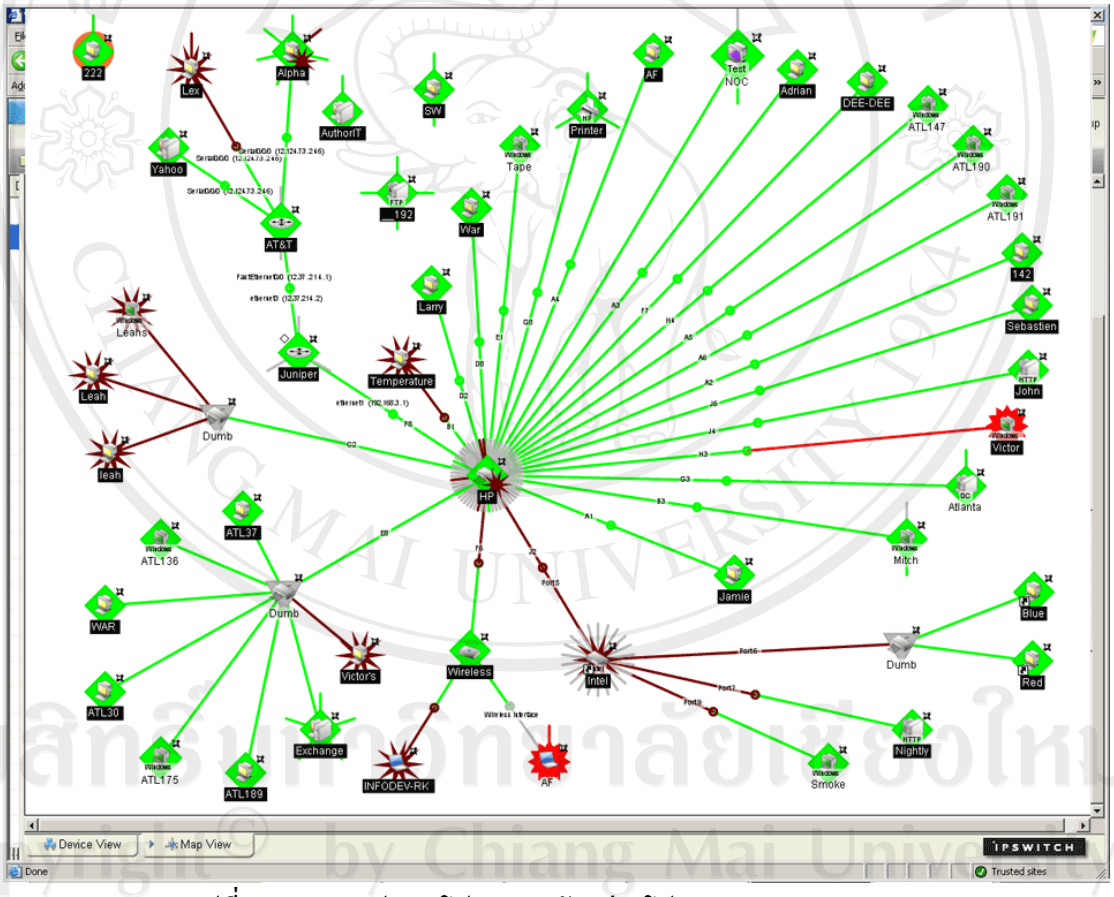
- CPU Utilization Performance Monitor Library
- Disk Utilization
- Interface Utilization (Bandwidth)
- Interface Utilization (Bandwidth)
- Memory Utilization
- Ping Latency and Availability

โดยการตรวจสอบประสิทธิภาพของอุปกรณ์นั้นถูกออกแบบมาให้สามารถใช้งานร่วมกับอุปกรณ์ที่มีความหลากหลายจึงใช้หลักการตามมาตรฐาน SNMP เป็นหลักแทนการใช้มาตรฐาน WMI ซึ่ง WMI เป็นมาตรฐานบนอุปกรณ์ที่ใช้กับระบบปฏิบัติการวินโดวส์ อย่างไรก็ตามอุปกรณ์ที่

ใช้ระบบปฏิบัติการวินโดวส์ ก็ไม่จำเป็นต้องใช้มาตรฐาน WMI ในการเก็บรวบรวมข้อมูลเสมอไป ถ้าหากว่าอุปกรณ์นั้นได้มีการเปิดใช้มาตรฐาน SNMP ที่อุปกรณ์นั้นๆ ซึ่ง WMI นี้จะจำเป็นต้องเรียกใช้งานในกรณีที่ผู้ดูแลระบบต้องการจะตรวจจับค่าที่ไม่ใช่ค่าหลักที่โปรแกรมได้ตั้งไว้เท่านั้น

Software Requirements ความต้องการของโปรแกรม

- ระบบปฏิบัติการ Windows XP, Windows 2000, Windows 2003 Server
- Microsoft Internet Explorer 5.01 หรือสูงกว่า
- การเชื่อมต่อกับระบบอินเทอร์เน็ต
- 265 MB HD space เป็นอย่างน้อย



รูปที่ 2.8 แสดงรูปภาพโปรแกรมตัวอย่างโปรแกรม Whatsup Gold

2.8 สรุปผลการศึกษาเลือกใช้โปรแกรม

จากการศึกษา โปรแกรมทั้ง 3 สามารถสรุปข้อดีและข้อเสียแต่ละโปรแกรมได้ดังนี้

ตาราง 2.2 แสดงข้อดีข้อเสียของโปรแกรม

โปรแกรม	ข้อดี	ข้อเสีย
MRTG	1.สามารถแสดงปริมาณทราฟฟิกของอุปกรณ์เครือข่ายได้ 2.สามารถติดตั้งได้ทั้งระบบปฏิบัติการ Windows และ Linux 3.ติดตั้งได้ง่าย 4.เป็นโปรแกรมที่อนุญาตให้นำไปใช้งานได้โดยไม่เสียค่าลิขสิทธิ์	1.การแสดงผลในรูปแบบกราฟมีข้อกำจัด ไม่สามารถเรียกข้อมูลย้อนหลังกลับมาแสดงผลได้อีก 2.รูปแบบกราฟของโปรแกรมอยู่ในรูปแบบไฟล์ PNG ไม่เหมาะสำหรับการเก็บสำรองข้อมูล 3.ข้อมูลของโปรแกรมไม่ได้จับเก็บในรูปแบบ Database ทำให้เกิดข้อจำกัดในการนำข้อมูลระบบไปพัฒนาเพิ่ม
CACTI	1.สามารถแสดงปริมาณทราฟฟิกของอุปกรณ์และข้อมูลอื่นที่สนับสนุนโปรโตคอล SNMP 2.สามารถติดตั้งได้ทั้งระบบปฏิบัติการวินโดวส์ และ ลีนุกซ์ 3.เป็นโปรแกรมที่อนุญาตให้นำไปใช้งานได้โดยไม่เสียค่าลิขสิทธิ์ 4.โปรแกรมพัฒนาจากภาษา PHP และ MySQL Database ทำให้ผู้พัฒนาระบบสามารถพัฒนาเพิ่มเติมให้เหมาะสมกับความต้องการของผู้ใช้งานในแต่ละองค์กรได้ 5.ข้อมูลของโปรแกรมถูกจัดเก็บในรูปแบบ Database ทำให้โปรแกรมมีประสิทธิภาพในการแสดงผลในรูปแบบกราฟที่ดีขึ้น	1.การติดตั้งมีความซับซ้อนกว่า MRTG 2.ส่วนติดต่อกับผู้ใช้งานโปรแกรมยังมีความซับซ้อนพอสมควร ทำให้เกิดความยุ่งยากในการกำหนดค่าให้กับโปรแกรมในช่วงเริ่มต้นใช้งาน

ตาราง 2.2 แสดงข้อดีข้อเสียของโปรแกรม (ต่อ)

โปรแกรม	ข้อดี	ข้อเสีย
	6.เนื่องจากเป็นโปรแกรมที่เป็น Open Source จึงมีนักพัฒนามากมายร่วมมือกันพัฒนาระบบอย่างต่อเนื่อง	
Whatsup Gold	1.เป็นโปรแกรมที่พัฒนาขึ้นเพื่อใช้ควบคุมระบบเครือข่ายโดยเฉพาะจึงมีฟังก์ชันให้เลือกใช้มากและใช้งานได้สะดวก 2.ติดตั้งได้ง่าย	1.เป็นโปรแกรมเชิงพาณิชย์ดังนั้นต้องจ่ายค่าลิขสิทธิ์ที่สูงมากก่อนนำไปใช้งาน โดยราคาเริ่มต้นที่ประมาณ หนึ่งแสนบาท 2.เป็นโปรแกรมสำเร็จรูปไม่สามารถแก้ไขรูปแบบโปรแกรมได้ 3.เป็นโปรแกรมที่ติดตั้งได้บนระบบปฏิบัติการวินโดวส์ เท่านั้น ซึ่งเป็นระบบปฏิบัติการที่ต้องจ่ายค่าลิขสิทธิ์ก่อนนำไปใช้งาน

ดังนั้นผู้วิจัยจึงตัดสินใจเลือกโปรแกรม CACTI มาใช้ในการพัฒนาระบบ เนื่องจากโปรแกรมนี้นอกจากสามารถแสดงผลในรูปแบบกราฟที่มีประสิทธิภาพแล้ว ยังเป็นโปรแกรมที่อนุญาตให้นำไปใช้งานได้ โดยไม่เสียค่าลิขสิทธิ์ ซึ่งพัฒนามาจากภาษา PHP ซึ่งผู้ศึกษาจะสามารถพัฒนาโปรแกรมเพิ่มเติมให้เหมาะสมกับความต้องการในการใช้งานขององค์กรต่อไปได้