รายงานการศึกษาเปรียบเทียบซอฟต์แวร์ NTOP กับซอฟต์แวร์อื่นๆ ในท้องตลาด (Commercial Software)

จัดทำโดย

โสภณ มงคลลักษมี
พนิตา พงษ์ไพบูลย์

หน่วยปฏิบัติการวิจัยเทคโนโลยีเครือข่าย
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
National Electronic and Computer Technology Center (NECTEC)

31 ตุลาคม 2551

รายงานนี้เป็นส่วนหนึ่งของโครงการวิจัยระบบบริหารจัดการเครือข่ายอัจฉริยะ (NT5001) โปรแกรมวิศวกรรมความรู้

สารบัญ

1 ความเป็นมา/วัตถุประสงค์ 1
2 รายการซอฟต์แวร์ Commercial Traffic Monitoring Systems 1
2.1 Colasoft Capsa 1
2.2 Network Probe 4
2.3 Netflow Analyzer 6
2.4 IP Traffic Monitor 8
2.5 PRTG Traffic Grapher 9
2.6 SoftPerfect Traffic Meter 11
2.7 Ultra Network Analyzer 12
3 สรุปผลการเปรียบเทียบ 13

สารบัญรูปภาพ

รูปที่ 1 ตัวอย่างหน้าจอ Colasoft Capsa..... 2
รูปที่ 2 ตัวอย่างหน้าจอ Network Probe..... 4
รูปที่ 3 ตัวอย่างหน้าจอ NetFlow Analyzer..... 6
รูปที่ 4 ตัวอย่างหน้าจอ IP Traffic Monitor..... 9
รูปที่ 5 ตัวอย่างหน้าจอ PRTG Traffic Grapher..... 10
รูปที่ 6 ตัวอย่างหน้าจอ SoftPerfect Traffic Meter..... 11
รูปที่ 7 ตัวอย่างหน้าจอ Ultra Network Analyzer..... 12

1 ความเป็นมา/วัตถุประสงค์

จากที่ซอฟต์แวร์ NTOP (Network TOP) เป็นซอฟต์แวร์ open-source ที่ได้รับความนิยมเป็นอย่างสูง สำหรับใช้ตรวจวัดและวิเคราะห์ปัญหาความผิดปกติในเครือข่าย ซอฟต์แวร์ NTOP สามารถตรวจวัดและวิเคราะห์การใช้งานเครือข่ายได้ทั้ง IPv4 และ IPv6 อย่างไรก็ตาม ซอฟต์แวร์ NTOP ยังมีข้อจำกัดหลายอย่าง อาทิเช่น ไม่สามารถจำแนกการใช้งาน IPv6 ตามแอพพลิเคชั่นได้ ไม่สามารถเก็บและค้นคืนข้อมูลจากฐานข้อมูล และมีการแสดงผลที่ดูยาก

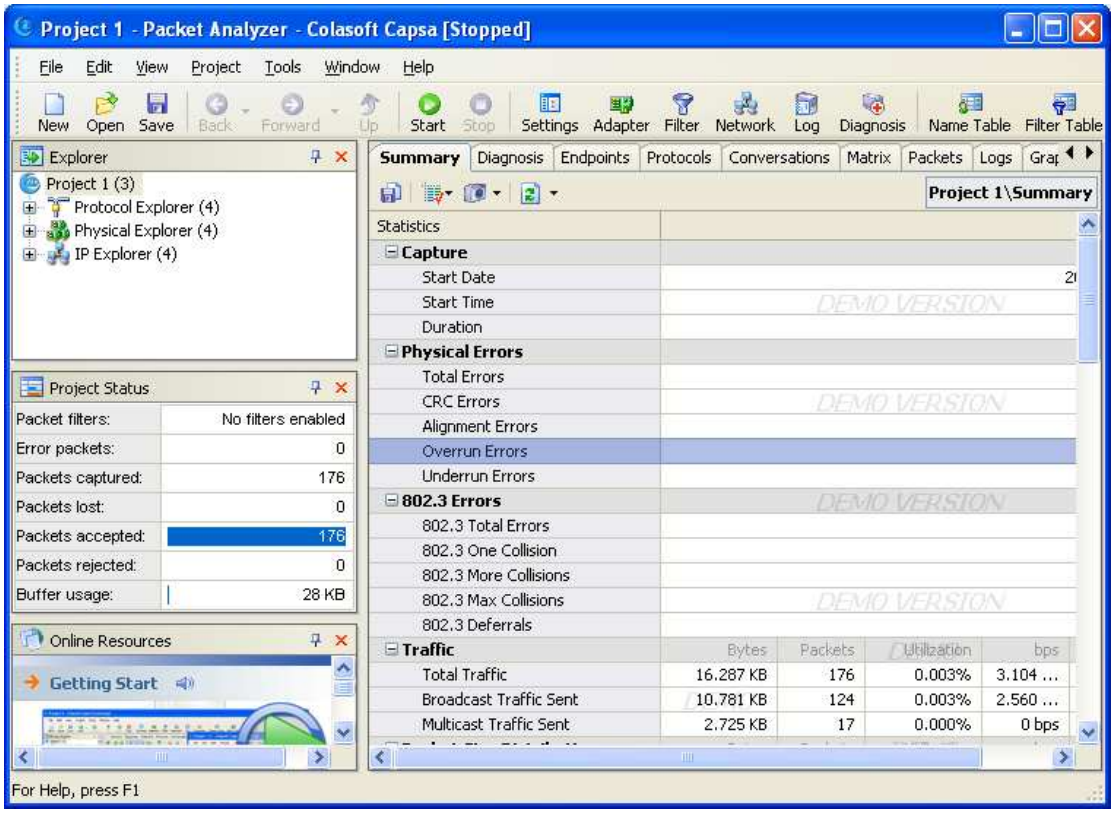
หลักจากได้ทำการพัฒนาปรับปรุงซอฟต์แวร์ NTOP ให้สามารถเก็บและค้นคืนข้อมูลจากฐานข้อมูล MySQL ได้ และมีการแสดงผลที่ง่ายต่อความเข้าใจของผู้ใช้งาน จึงได้ทำการการศึกษาเปรียบเทียบซอฟต์แวร์ NTOP กับซอฟต์แวร์อื่นๆ ในท้องตลาด (Commercial Software)

2 รายการซอฟต์แวร์ Commercial Traffic Monitoring Systems

ในการศึกษาเปรียบเทียบคุณสมบัติและความสามารถของ ntop กับ commercial (close-source) software ประเภทเดียวกันเพื่อประเมินความสามารถในการแข่งขันในเชิงพาณิชย์ และได้เลือก Commerical (close-source) software สำหรับตรวจวัดและวิเคราะห์ข้อมูลในเครือข่าย 7 software มาทำการศึกษาเปรียบเทียบ ได้แก่ Colasoft Capsa, Ntwork Probe, Netflow Analyzer, IP Traffic Monitor, PRTG Traffic Grapher, SoftPerfect Traffic Meter และ Ultra Network Analyzer

2.1 Colasoft Capsa

เป็นโปรแกรมประเภท Network analyzer (protocol analyzer และ packet sniffer) โปรแกรมมีความสามารถหลายอย่างเช่น สามารถดักจับ packet ได้แบบ real time, สามารถใช้ในการ monitor เครือข่ายได้ตลอด 24/7, สามารถแสดงรายงานโดยละเอียด packet , มีการวิเคราะห์ protocol ขั้นสูง และมีระบบวิเคราะห์ปัญหาอย่างผู้เชี่ยวชาญแบบอัตโนมัติ ตัวโปรแกรมสามารถแสดงผลเครือข่ายที่มีความซับซ้อนให้อยู่ในรูปแบบที่ชัดเจนและเข้าใจง่าย, วิเคราะห์ในระดับ packet และสามารถแก้ไขปัญหาของเครือข่าย



รูปที่ 1 ตัวอย่างหน้าจอ Colasoft Capsa

คุณสมบัติเด่น

- **Traffic Statistics & Bandwidth Use** แสดงผลการ monitor traffic และ bandwidth ที่ถูกใช้งานในรูปแบบของกราฟและตัวเลข
- **Advanced Protocol Analysis** สามารถวิเคราะห์และระบุชนิดของ network protocol ได้มากว่า 300 protocol
- **In-depth Packet Decoding** แสดงสรุปผลของ packet ต่างๆพร้อมทั้งรายละเอียดต่างๆที่ทำการถอดระหัสเรียบร้อยแล้ว
- **Monitor Multiple Network Behaviors** เฝ้าดูและตรวจสอบการใช้งาน web site ต่างๆ, รายละเอียดของ email, การสนทนาแบบ online และอื่นๆ
- **Map out Each Host in Network** แสดงรายการ host ต่างๆภายในเครือข่าย รวมทั้งรายละเอียดของแต่ละ host เช่น IP address, MAC และอื่นๆ
- **Automatic Expert Network Diagnosis** แสดงการวิเคราะห์ปัญหาภายในเครือข่ายอัตโนมัติพร้อมคำแนะนำในการแก้ไข
- **Visualize all Connections in Matrix** แสดงแบบจำลองการเชื่อมต่อของอุปกรณ์ต่างๆในเครือข่ายพร้อมทั้งปริมาณ traffic
- **Conversation & Packet Stream** สามารถเฝ้าดูและสร้าง packet ต่างๆที่เกิดขึ้นในระหว่างการสนทนาได้

- **Useful & Valuable Built-in Tools** มี built-in tool ที่ให้มาพร้อมกับโปรแกรมซึ่งสามารถสร้าง packet และ replay packet ได้ตามต้องการ รวมทั้งการ scan และ ping เพื่อตรวจสอบเครือข่าย
- **Quick & Intuitive Report** สามารถสร้างรายงานเกี่ยวกับการเชื่อมต่อที่สนใจได้อย่างรวดเร็ว

ความต้องการของโปรแกรม

Minimum requirement

- P4 1.2G CPU
- 512 MB RAM
- Internet Explorer 5.5 or higher

Recommended requirements

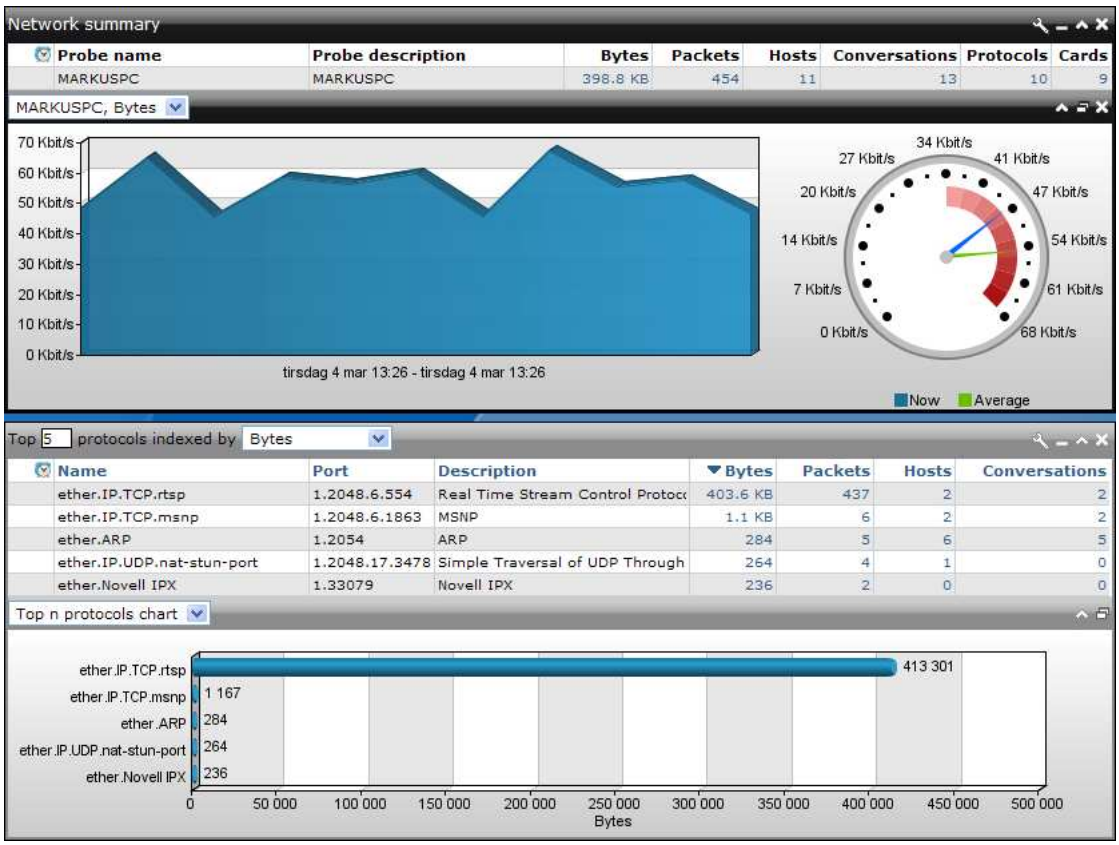
- P4 3.0G CPU
- 1GB RAM or more
- Internet Explorer 6.0 or higher

Supported Windows Platforms

- Windows 2000 (SP 4 or later)
- Windows XP (SP 1 or later) and 64 Edition
- Windows Server 2003 and 64 Edition
- Windows Vista

2.2 Network Probe

Network Probe เป็นโปรแกรมที่ทำหน้าที่เป็น network traffic monitor และ protocol analyzer ที่มีการรายงานผลในรูปแบบของภาพ ซึ่งแสดงชนิดและปริมาณของ network traffic พร้อมทั้งช่วยชี้ให้เห็นถึงจุดที่อาจเป็นต้นเหตุของปัญหาและจุดที่เป็นคอขวดของเครือข่าย เมื่อใดที่ network ช้าลงหรือไม่สามารถใช้งานได้ Network probe สามารถที่จะชี้ให้เห็นถึงสาเหตุของปัญหาว่าใครเป็นผู้สร้าง traffic และมีการรับส่งข้อมูลอยู่ที่ใดภายในเครือข่าย ได้อย่างรวดเร็ว



รูปที่ 2 ตัวอย่างหน้าจอ Network Probe

คุณสมบัติเด่น

- **Search** สามารถค้นหาข้อมูลของ host และ protocol ที่สนใจ ด้วยการ search ซึ่งจะแสดงรายละเอียดของ host และ protocol นั้นๆออกมาหากพบภายในเครือข่าย
- **Alarms** Network Probe อนุญาติให้ผู้ใช้สามารถเพิ่มการแจ้งเตือนสำหรับส่วนต่างๆภายในเครือข่ายเช่น host, protocol, network card และอื่นๆที่ถูก monitor ด้วย network probe ซึ่งผู้ใช้สามารถระบุคุณสมบัติต่างๆของการแจ้งเตือนได้เช่น เงื่อนไขในการแจ้งเตือน, ข้อความที่ต้องการแสดงเพื่อแจ้งเตือน และสามารถส่ง Email ไปยังผู้ดูแลเครือข่ายหรือ start program ที่ต้องการเมื่อเกิดเหตุการณ์ที่กำหนด

- **Network summary** Network probe แสดงข้อมูลสำคัญต่างๆเกี่ยวกับเครือข่ายที่ทำการเฝ้าดู เช่น throughput ทั้งหมดของเครือข่าย, จำนวนของข้อมูลเป็น byte, จำนวนของ packet, จำนวนของ host, จำนวนของ conversation, protocol และ network card
- **Top protocols, talkers, listeners, and conversations** Network probe สามารถแสดงข้อมูลของ protocol ที่ใช้งานมากที่สุด, ผู้ที่มีการรับหรือส่งข้อมูลมากที่สุด ซึ่งผู้ใช้สามารถระบุจำนวนของอันดับที่ต้องการได้เช่น 5 อันดับ หรือ 10 อันดับ และจัดรูปแบบการเรียงของข้อมูลที่แสดงได้เอง พร้อมทั้งสามารถแสดงค่า throughput ประกอบ
- **User-selected protocols, hosts, and conversations** สามารถระบุ protocol, host และ conversation ที่ต้องการเฝ้าดูเป็นพิเศษได้เมื่อสงสัยว่ากิจกรรมต่างๆอาจส่งผลกระทบต่อเครือข่าย หรือเป็นการติดต่อสื่อสารที่มีความสำคัญ
- **Detailed protocol statistics** Network probe สามารถแสดงรายละเอียดของ protocol ต่างๆที่มีการใช้งานภายในเครือข่าย ซึ่งรายละเอียดต่างๆนั้นประกอบด้วย ชื่อ, ports, คำบรรยาย, จำนวนของ traffic ที่พบ, throughput และจำนวนของ host และ conversion ที่ใช้ protocol นั้นๆ
- **See who is using your network** แสดงสถิติของทุกๆ host ที่รับส่งข้อมูลภายในเครือข่าย โดย Network probe แสดงข้อมูลต่างๆประกอบด้วย host name, IP address, จำนวน packet และ byte ที่รับส่ง, จำนวนของ protocol ที่ใช้ , จำนวนของ conversation ของแต่ละ host กับ host ต่างๆที่มีการติดต่อด้วยและจำนวน bandwidth ที่แต่ละ hostใช้
- **See conversations on your network** แสดงสถิติการของ host ได้รับข้อมูลจากใคร และส่งข้อมูลให้ใคร โดย network probe เก็บชื่อ source และ ชื่อ destination รวมทั้ง IP address สำหรับ แต่ละ conversation ที่เกิดขึ้นในเครือข่าย และจัดแสดงจำนวนของ packet , byte ของข้อมูลที่ส่ง พร้อมทั้ง bandwidth ที่ถูกใช้ไปในแต่ละ conversation

ความต้องการของโปรแกรม

Network Probe Server:

- Windows Vista, Windows XP, Windows 2003, Windows 2000 (with admin access)
- Linux, FreeBSD, MacOS X and Solaris (with root access)
- Sun Java Runtime Environment 1.3 or higher. GNU Java is not fully supported yet

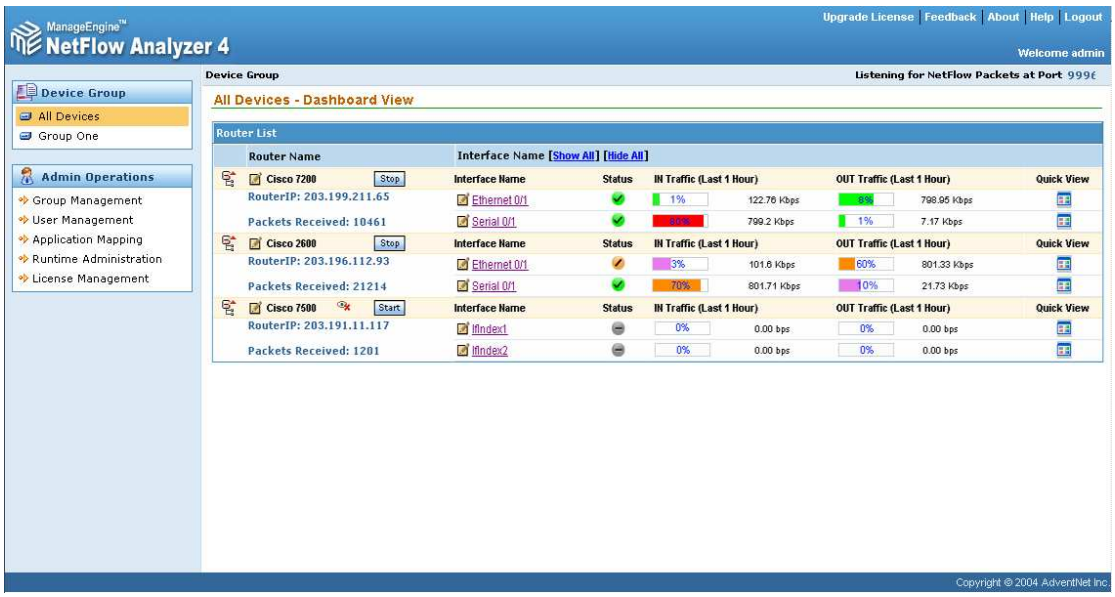
- A network card supporting promiscuous mode connected to a SPAN port
- Recommended hardware is at least a 2GHz CPU and 1 GB of RAM

Network Probe Client - tested web browsers:

- Windows: Internet Explorer 6 and newer
- Windows: Firefox 1.5 and 2.0
- Windows: Opera 8.54
- Linux: Firefox 1.5 and 2.0

2.3 Netflow Analyzer

NetFlow Analyzer เป็น bandwidth monitoring ที่สามารถให้ข้อมูลในเชิงลึกของ traffic และรูปแบบของ traffic ภายในของเครือข่าย สามารถแสดงพฤติกรรมของ Traffic ต่างๆ ได้แบบ real-time และผลกระทบที่มีต่อประสิทธิภาพโดยรวมของเครือข่าย



รูปที่ 3 ตัวอย่างหน้าจอ NetFlow Analyzer

คุณสมบัติเด่น

- **Simplified Bandwidth Monitoring** โดยทั่วไปในบริษัทต่างๆ ที่ไม่ได้มีการจัดสรรค์ bandwidth จึงมีโอกาสให้ application ที่ไม่เหมาะสมมีความสำคัญเหนือกว่า application ที่มีความสำคัญต่อธุระกิจในช่วงเวลาเร่งด่วนของการทำงาน รายงานการใช้ Bandwidth ของ NetFlow Analyzer สามารถแสดงข้อมูลที่แท้จริงของการใช้งาน bandwidth ในช่วงเวลาดังกล่าวและยังสามารถแสดงอันดับของเครื่องที่ application ที่

ส่งผลการทบธุระกิจดังกล่าว ด้วยข้อมูลดังกล่าวทำให้สามารถควบคุมการใช้งาน bandwidth และประยุกต์ใช้งาน policy ที่เหมาะสมได้

- **In-depth Traffic Analysis** ไม่จำเป็นต้องติดตั้ง hardward หรือ tool ใดๆเพิ่มเพื่อการเก็บข้อมูล เพียงแต่ปรับให้ router/switching ต่างๆ ส่งข้อมูล netflow ไปยัง NetFlow Analyzer โดย NetFlow Analyzer ใช้ NetFlow, sFlow, cflowd, J-Flow, IPFIX, NetStream and Cisco NBAR ในการแสดงข้อมูล TOP application, top host, top conversations ที่ใช้ bandwidth ข้อมูลเหล่านี้สำคัญมากในการที่จะเข้าใจการใช้งานในช่วงเวลาเร่งด่วนของการทำงาน และ historical trends ช่วยในการวางแผนการปรับปรุงความเร็วของเครือข่าย และการบังคับใช้ policy ต่างๆ

- **QoS validation using Cisco CBQoS** เพื่อให้แน่ใจว่า application ที่มีความสำคัญกับธุรกิจต่างๆได้รับความสำคัญสูงสุดในเครือข่าย คุณสามารถประยุกต์ใช้ qos policy ได้ ด้วยการใช้ NetFlow Analyzer สามารถที่จะเรียกดู policy ที่ใช้ใน interface ต่างๆ และสามารถ ตรวจสอบความถูกต้องของ QOS policy ด้วยการ monitoring ในส่วนของ pre-policy และ post-policy ในแต่ละ class ได้

- **Alerting Based on Thresholds** NetFlow Analyzer สามารถแจ้งเตือนหรือส่ง email ไปยังผู้ดูแลเมื่อการใช้งาน bandwidth เกินค่าทำกำหนดไว้ และยังสามารถส่ง snmp traps ไปยัง NMS/EMS application เมือเป็นการแจ้งเตือนที่ร้ายแรง ซึ่งจะช่วยให้สามารถแก้ไขปัญหาได้อย่างทันท่วงที

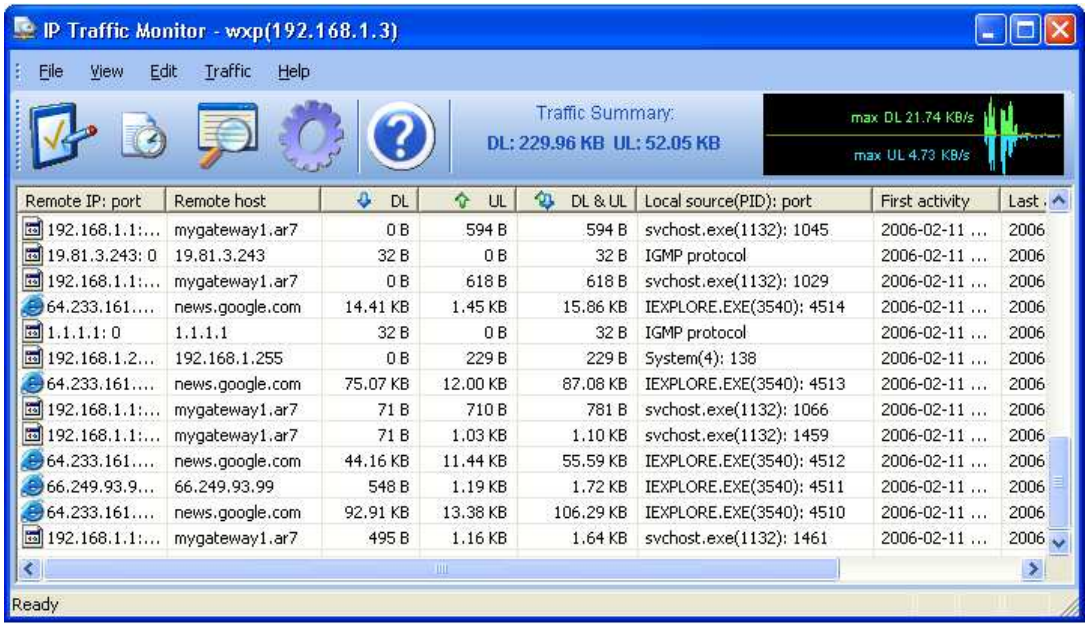
- **Departmental Bandwidth Usage** สามารถที่จะสร้างกลุ่มของ IP address ตามส่วนหรือหน่วยงาน เพื่อ monitor การใช้งาน bandwidth ของแต่ละกลุ่ม IP address ได้ ซึ่งข้อมูลดังกล่าวช่วยให้สามารถจัดสรรค์ค่าใช้จ่ายได้
- **Custom Reports** NetFlow Analyzer มีการกำหนดรูปแบบของรายงานการใช้งาน Bandwidth อย่างยอดเยี่ยมไว้ให้แล้ว ซึ่งช่วยในการวิเคราะการใช้งาน bandwidth จาก application, user และในมุมมองของ Conversation ด้วยข้อมูลที่ละเอียดทำให้ทราบได้ถึงการใช้งานที่ผิดของ user เช่นการใช้งาน application ที่ไม่อนุญาต นอกจากนั้นยังอนุญาตให้ผู้ดูแลระบบสามารถกำหนดคุณสมบัติของรายงานที่ต้องการได้เอง เช่น สามารถเลือกดูข้อมูลการใช้งาน bandwidth โดยระบุ Host หรือ network ที่ต้องการ หรือแม้แต่เลือกดูข้อมูลเกียวกับ application ที่สนใจในช่วงเวลาที่ต้องการ
- **Reduced Training and Operational Costs** NetFlow Analyzer มีรูปแบบของ interface ที่สามารถใช้และทำความเข้าใจได้ง่ายทำให้ไม่จำเป็นต้องสิ้นเปลืองในการอบรมหรือเวลาในการทำความเข้าใจ ซึ่งผู้ใช้สามารถที่จะควบคุมการทำงานต่างๆผ่าน

หน้าจอทั้งสิน นอกจากนั้นแล้ว NetFlow Analyzer ได้รวม MySQL ซึ่งใช้เป็นฐานข้อมูลในการเก็บข้อมูลต่างๆไว้ด้วยแล้วจึงไม่จำเป็นที่จะต้องติดตั้งฐานข้อมูลใดๆเพิ่มและไม่ต้องกังวลในเรื่องการเข้ากันได้ของส่วนต่างๆ

- **Effective Data Storage** NetFlow Analyzer จัดเก็บข้อมูลทั้งที่ได้ทำการสรุปผลแล้วและข้อมูลที่เป็นข้อมูลดิบ โดยข้อมูลที่เป็นข้อมูลสรุป Top 100 จะจัดเก็บไว้ตลอดเพื่อใช้ในการทำรายงานแบบระยะยาวเพื่อใช้ในการตัดสินใจวางแผนเกี่ยวกับเครือข่าย ส่วนข้อมูลที่เป็นข้อมูลดิบจะย้อนหลังเพียง 1 เดือนและสามารถค้นหาข้อมูลได้ละเอียดในระดับ 1 นาที
- **Completely Web Based** NetFlow Analyzer สามารถทำงานในแบบของ web ทำให้ผู้ใช้สามารถเข้าถึงข้อมูลต่างๆได้ผ่านทาง web browser จากทุกๆที่

2.4 IP Traffic Monitor

IP Traffic Monitor เป็น application ที่สามารถในการวิเคราะห์และให้ข้อมูลเกี่ยวกับทิศทางและปริมาณของ internet traffic ในแบบ real-time, ความปลอดภัยและการตรวจสอบการใช้งานทรัพยากรซึ่งเป็นเรื่องที่สำคัญในสภาพแวดล้อมแบบ internet นอกจากนั้น IP Traffic Monitor เป็นเครื่องมือที่ช่วยให้แก้ปัญหาต่างๆได้อย่างรวดเร็ว และช่วยให้สามารถตรวจสอบกิจกรรมต่างๆในเครือข่ายทำให้สามารถรู้ได้ว่าใครเป็นผู้ที่ทำให้เกิด traffic ในปริมาณมากๆ นอกจากนั้นยังสามารถที่จะติดตามร่องรอยของ traffic ต่างๆซึ่งช่วยให้สามารถตรวจพบ spyware, adware, virus และอื่นๆ ที่มีลักษณะการทำงานที่ไม่ถูกต้อง ก่อนที่จะส่งผลกระทบในเรื่องของความปลอดภัย



รูปที่ 4 ตัวอย่างหน้าจอ IP Traffic Monitor

คุณสมบัติเด่น

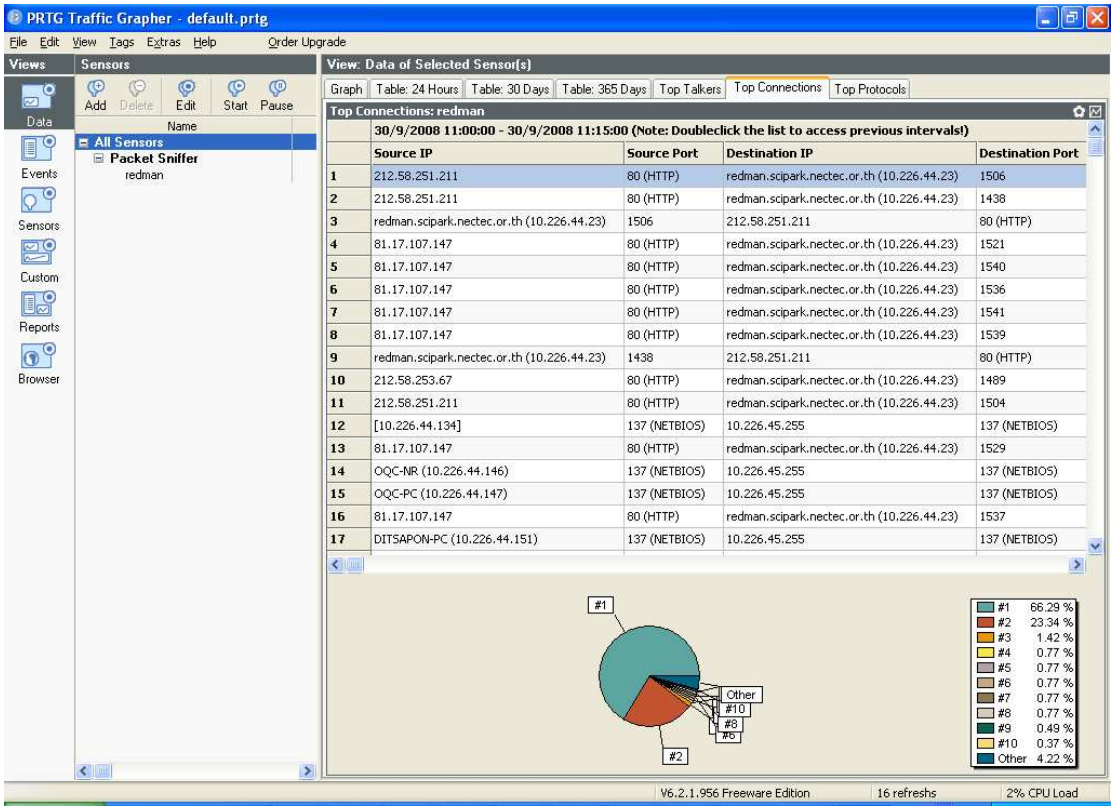
- Monitors IP traffic ได้แบบ real-time
- ดักจับ traffic ต่างๆแบบ real-time
- สามารถแสดงผลข้อมูลในแบบพายกราฟ
- สามารถดักจับ TCP/IP packet และบันทึกลงไฟล์
- สามารถทำงานร่วมกับ Proxy Server
- มีการบันทึก log ของ traffic ต่างๆ
- แสดงผลกิจกรรมต่างๆในเครือข่ายในรูปแบบของภาพ graphic
- แสดงข้อความแทน host ด้วย IP address และชื่อ
- แยกไฟล์ในการจัดเก็บ log เพื่อความสะดวกในการวิเคราะห์ในอนาคต
- สามารถทำงานร่วมกับ ADSL, ISDN, Dial-Up, Cable Modem, Ethernet cards และอื่นๆ
- สามารถตั้งให้ทำงานอัตโนมัติได้

ความต้องการของโปรแกรม

- Windows® NT/2000/XP/2003
- 3 MB of freedisk space

2.5 PRTG Traffic Grapher

PRTG Traffic Grapher เป็นซอฟต์แวร์ที่ Monitor และแจกแจงการใช้งาน bandwidth โดยมีระบบการจัดการที่ช่วยให้สามารถรู้ถึงข้อมูลในณ.ขณะเวลาปัจจุบันและสามารถแสดงแนวโน้มการใช้งาน bandwidthของอุปกรณ์network ต่างๆ และนอกจากจะสามารถใช้ในการบริหารจัดการ bandwidth แล้วยังสามารถที่จะใช้ในการ monitor ในจุดประสงค์ต่างๆได้เช่นการใช้งาน memory และ CPU ของอุปกรณ์ต่างๆ



รูปที่ 5 ตัวอย่างหน้าจอ PRTG Traffic Grapher

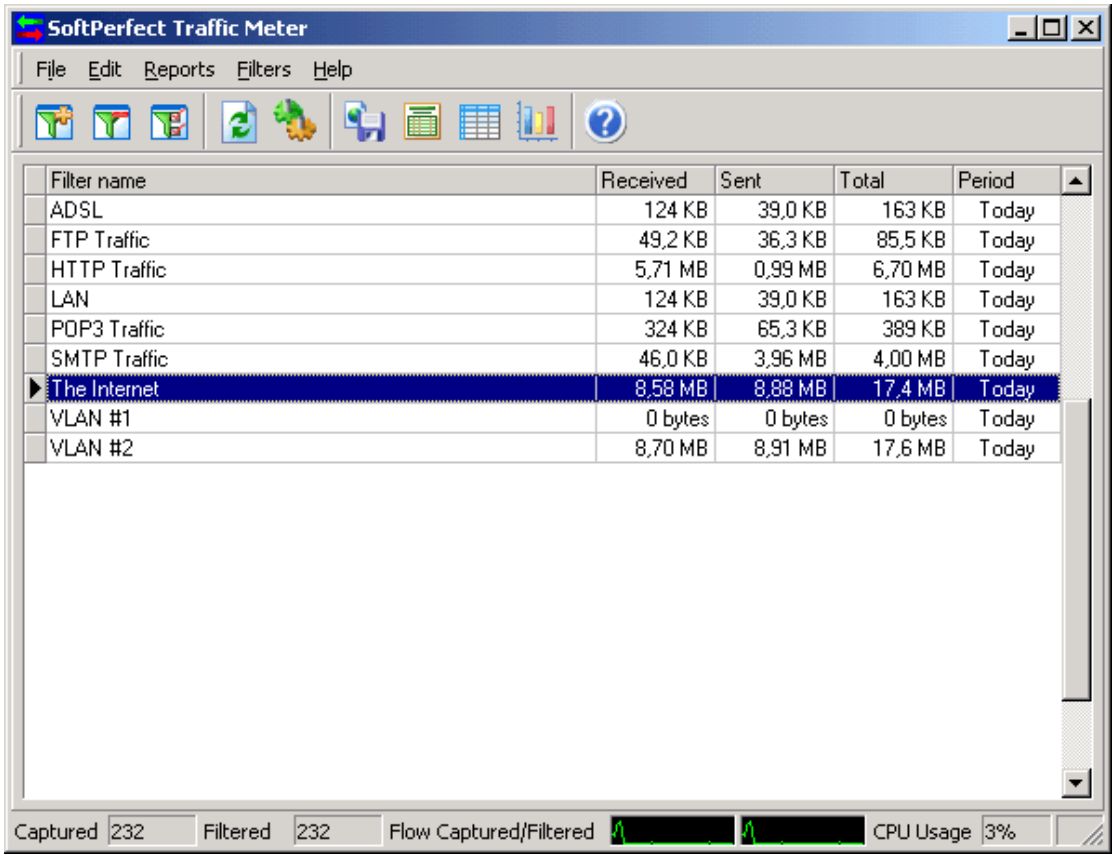
คุณสมบัติเด่น

- เป็น network monitoring tool ที่เชื่อถือได้มีการใช้งานมากกว่า 100,000 รายต่อวัน
- รองรับวิธีการเก็บข้อมูลหลายรูปแบบเช่น SNMP, packet sniffing, NetFlow protocol และ การวัดจาก latency
- สามารถแยกแยะประเภทของ traffic ด้วย IP address, protocol และ parameters อื่นๆ
- สามารถทำงานร่วมกับอุปกรณ์ network ได้หลายชนิดเช่น router, firewalls, switch
- มีขั้นตอนการติดตั้งที่ง่าย
- มีโครงสร้างที่สามารถรองรับการ monitor ได้จำนวนหลายพัน Sensors
- สามารถตั้งกำหนดการในการรายงานผลข้อมูลที่ได้จากการ monitor ได้
- สามารถกำหนดการแจ้งเตือนหรือส่ง email ไปยังผู้ดูแลระบบเมื่อเกิดข้อผิดพลาดหรือพบการทำงานที่หนักเกินไปของ sensor ได้
- มี web server และ web base interface ที่ช่วยให้ผู้ใช้สามารถเรียกดูข้อมูลจากที่ใดก็ได้
- จัดเก็บข้อมูลในฐานข้อมูลซึ่งสามารถที่จะ export ข้อมูลออกมาในรูปแบบของ csv และรองรับการจัดทำ backup และ ลบข้อมูลเก่าๆได้

- สามารถจัดทำรายงานได้หลายรูปแบบทั้งแบบของภาพกราฟและตารางข้อมูล(HTML, Excel, TIF, RTF, PDF)

2.6 SoftPerfect Traffic Meter

SoftPerfect traffic Meter เป็น network monitoring tool ที่สามารถทำงานได้ในแบบ real time ซึ่งสามารถแสดงผลข้อมูลได้ทั้งแบบกราฟและตัวเลข SoftPerfect สามารถสร้างรายงานได้ทั้งที่เป็นรูปกราฟและตารางของปริมาณข้อมูลที่ส่งและรับต่อวัน, สัปดาห์ หรือเดือน นอกจากนั้นยังสามารถ export ข้อมูลในรูปแบบของ program ต่างๆ เช่น Microsoft Excel เพื่อนำไปใช้งานการประมวลผลเพิ่มเติมในอนาคต SoftPerfect Traffic Meter สามารถตรวจจับปัญหาต่างๆที่เกิดขึ้นภายใน LAN โปรแกรม SoftPerfect Traffic Meter สามารถตรวจวัดปริมาณ data transmission rates ภายในเครือข่าย และรู้ได้ว่า host ใดเป็นผู้ที่สร้าง traffic มากที่สุด ค้นหาปริมาณของ traffic ที่ถูกใช้โดยแต่ละ application โปรแกรมสามารถทำงานร่วมกับ proxy server ต่างๆได้ เช่น WinGate, WinRoute และอื่นๆ หรือแม้แต่ทำงานอิสระโดยการเข้าถึง network card ของ computer โดยตรง



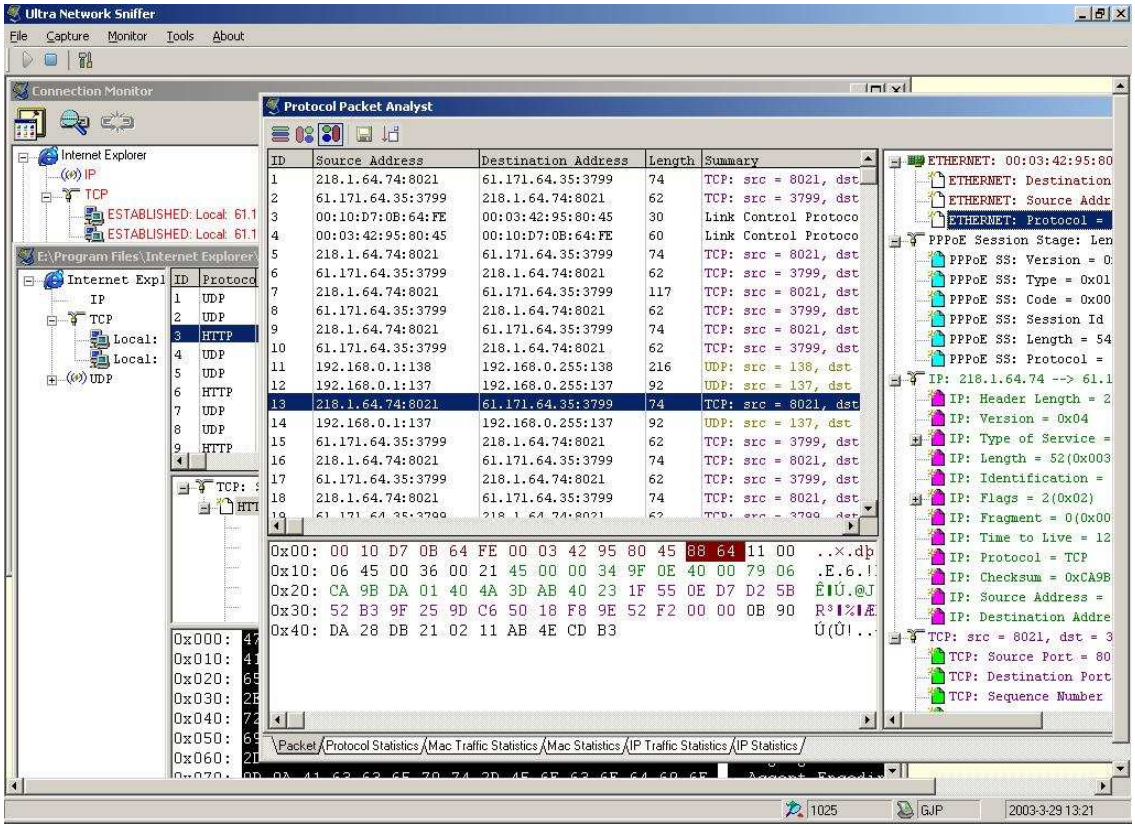
รูปที่ 6 ตัวอย่างหน้าจอ SoftPerfect Traffic Meter

คุณสมบัติเด่น

- สามารถ Export report ออกมาได้หลายรูปแบบ เช่น Excel, MS word และ HTML
- มีการจัดเก็บ log ของ TCP/IP อย่างละเอียด
- สามารถ Monitors traffic ของ host หรือ port ที่สนใจได้อย่างยืดหยุ่นด้วยการกำหนดค่า filter
- สามารถทำงานร่วมกับ Dial up, Ethernet adapters, token ring และอื่นๆ
- ทำงานบน windows ได้เป็นอย่างๆดี (windows 98, ME, NT, 2000, XP, 2003)

2.7 Ultra Network Analyzer

เป็นเครื่องมือที่สามารถทำงานในลักษณะของ network sniffer, packet sniffer, sockets sniffer และ protocol sniffer ซึ่งประกอบด้วยฟังก์ชั่นต่างๆที่ช่วยในการแก้ไขปัญหาของ network โปรแกรม Ultra Network Analyzer ดักจับทุก packet แบบ real-time จากทุก network card (รวมถึง modem,ISDN,ADSL) และยังสามารถดักจับ packet แยกตามชนิดของ application ได้ (SOCKET,TDI และอื่นๆ) ผู้ใช้สามารที่จะเฝ้าดูทุก traffic ของทุก application ที่สนใจ โปรแกรทมีรูปแบบการใช้งานที่ง่าย และ ยังมี plugin ต่างๆสำหรับแต่ละ protocol เช่น ETHERNET, IP, TCP, UDP ,PPOE, HTTP, FTP, WINS, PPP, SMTP, POP3 และอื่นๆ



รูปที่ 7 ตัวอย่างหน้าจอ Ultra Network Analyzer

คุณสมบัติเด่น

- ใช้งานได้ทุก version ของ windows (Windows XP/2000/NT/ME/98/95)
- Monitor กิจกรรมต่างๆในเครือข่ายแบบ real-time
- มีการแสดงผลข้อมูลสถิติและกราฟต่างๆเปลี่ยนไปตามการเปลี่ยนแปลงตามของข้อมูลณ.ขณะเวลา
- สามารถ Export ข้อมูลในรูปแบบของ HTML ที่สวยงามและเข้าใจได้ง่าย
- สามารถดักจับข้อมูลของ traffic ต่างๆเพื่อใช้ในการวิเคราะห์ได้
- สามารถดักจับ traffic แยกแยะตาม application ได้
- มีเครื่องมือที่สามารถใช้สร้าง traffic เพื่อตรวจวัดค่าต่างๆเช่น เวลาในการตอบสนอง, จำนวน hops หรือเพื่อใช้ในการแก้ปัญหาต่างๆ

3 สรุปผลการเปรียบเทียบ

จากความข้อมูลของ software ต่างๆที่แสดงดังหัวข้อที่ 2 สามารถนำมาสรุปเป็นตารางข้อมูลเปรียบเทียบกับ software NTOP ที่ได้พัฒนาขึ้นได้ดังตารางที่ 1 ซึ่งจากข้อมูลในตารางแสดงให้เห็นได้ว่าต้นแบบ ntopThai-1.2 มีคุณสมบัติที่เทียบได้กับ Commercial Software และเด่นกว่าได้ด้านของการรายงานข้อผิดพลาดและความเสี่ยงจากการถูกจู่โจมในเครือข่าย และการบันทึกข้อมูลลงฐานข้อมูลเพื่อความสะดวกในการค้นคืนข้อมูลย้อนหลังในมิติต่างๆ นอกจากนี้ พบว่าCommercial Software สำหรับตรวจวัดและวิเคราะห์ข้อมูลในเครือข่ายนั้นมีค่าลิขสิทธิ์ที่แพงมาก หากนำมาใช้งานในระดับหน่วยงานที่มีคอมพิวเตอร์ในเครือข่ายมากกว่า 10 ตัวขึ้นไป จะมีค่าใช้จ่าย site license ขั้นต่ำ US$300 หรือมากกว่า 10,000 บาท

ตารางที่ 1 สรุปเปรียบเทียบคุณสมบัติและความสามารถของ ntopThai1.2 เทียบกับ Commercial Software

Features	Ntop (ntopThai-1.2)	Colasoft Capsa	Network Probe	Netflow Analyzer	IP Traffic monitor	PRTG Traffic Grapher	SoftPerfect Traffic Meter	Ultra Network Analyzer
Thai GUI	มี	-	-	-	-	-	-	-
Attack detection	มี	-	-	-	-	-	-	-
History log	มี	มี	มี	มี	มี	-	มี	-
DB support	MySQL, rrdtool	-	-	-	-	มี	-	-
Application & host report	มี	มี	มี	มี	มี	มี	มี	มี
Matrix view	มี	มี	-	-	-	-	-	-

Features	Ntop (ntopThai-1.2)	Colasoft Capsa	Network Probe	Netflow Analyzer	IP Traffic monitor	PRTG Traffic Grapher	SoftPerfect Traffic Meter	Ultra Network Analyzer
Alarm	มี	มี	มี	มี	-	มี	-	-
Passive/active	passive	passive, active	passive	passive	passive	passive	passive	passive, active
Traffic stat	มี	มี	มี	มี	มี	มี	มี	มี
Protocol stat	มี	มี	มี	มี	-	มี	มี	มี
Error packet stat	มี	มี	-	-	-	-	-	-
Search	มี	-	มี	-	-	-	-	-
Print data	-	มี	-	มี	-	มี	-	-
Summary	มี	มี	มี	มี	มี	มี	มี	มี
Network segment view	มี	มี	มี	-	มี	มี	-	-
Web-based view	ใช่	ใช่	ใช่	ใช่	-	ใช่	-	ใช่
Packet analyzer	-	มี	-	-	-	-	มี	มี
Summary snapshots	มี	มี	-	-	-	-	มี	มี
Physical host location (map)	มี	-	-	-	-	-	-	-
OS Platform	FreeBD , Linux, Solaris, Irix, AIX, Mac OS X, Windows 95 and up including Vista	Linux, Windows 2000, XP, 2003, Vista	Windows 2000, 2003, XP, Linux, FreeBSD, MacOS X, Solaris	Windows 2000, XP, 2003, Vista, Redhat Linux 8.0, 9.0	Windows NT, 2000, XP, 2003	Windows 2000, XP, 2003, Vista	Windows 98, ME, XP, NT, 2000, 2003	Windows 95, 98, ME, NT, 2000, XP
Hardware requirement	Memory: a few MB to 100MB CPU load: less than 10% of overall CPU load	P4 1.2G CPU 512 MB RAM	2GHz CPU 1 GB RAM	2.6 GHz CPU 512 MB RAM 20 GB disk space	3 MB disk space	64 MB RAM 20 MB disk space 25 -300kB disk space per sensor per day	N/A	N/A

Features	Ntop (ntopThai-1.2)	Colasoft Capsa	Network Probe	Netflow Analyzer	IP Traffic monitor	PRTG Traffic Grapher	SoftPerfect Traffic Meter	Ultra Network Analyzer
License fee	GPL (open - source)	$399 Professional edition	$600	$795 Professional edition	$20.00 (single) $500 (site)	Commercial or freeware	$49 (single) $200(10PCs) $700 (site)	$29.95 (single) $299.92 (site)
Free trial period	-	15 วัน	-	-	-	30 วัน	-	-