# ระบบตรวจสอบทราฟฟิกของเครือข่ายสำหรับข้อมูล ที่ถูกส่งผ่านบนเครือข่ายระยะไกล

# NETWORK TRAFFIC MONITORING SYSTEM FOR SENDING DATA ON WIDE AREA NETWORK (WAN)



โดย

อภิชาต ชะโลธร

APICHAT CHALOTHORN

อาจารย์ที่ปรึกษา

รศ.ดร.จันทร์บูรณ์ สถิตวิริยวงศ์



รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ 2 ปีการศึกษา 2552

# NETWORK TRAFFIC MONITORING SYSTEM FOR SENDING DATA ON WIDE AREA NETWORK (WAN)

APICHAT CHALOTHORN

A REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS OF THE COURSE

SYSTEM DEVELOPMENT PROJECT

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2/ 2009

**ใบรับรองโครงการพัฒนาระบบงาน (System Development Project)**

**เรื่อง**

# ระบบตรวจสอบทราฟฟิกของเครือข่ายสำหรับข้อมูลที่ถูกส่งผ่านบนเครือข่ายระยะไกล

# Network Traffic Monitoring System for Sending Data on Wide Area Network (WAN)


**นายอภิชาต ชะโลธร**

**รหัสประจำตัว 48066837**


ขอรับรองว่ารายงานฉบับนี้ข้าพเจ้าไม่ได้คัดลอกมาจากที่ใด

รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของ

การศึกษาวิชาโครงการพัฒนาระบบงาน หลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)

ภาคเรียนที่ 2 ปีการศึกษา 2552

..... อาจารย์ที่ปรึกษา

(รศ.ดร.จันทร์บูรณ์ สถิตวิริยวงศ์)

..... กรรมการสอบ

(รศ.ดร.โชติพัชร์ ภรณวลัย)

..... กรรมการสอบ

(รศ.ดร.นพพร โชติกกำธร)

| | |
|---|---|
| **หัวข้อ** | ระบบตรวจสอบทราฟฟิกของเครือข่ายสำหรับข้อมูลที่ถูกส่งผ่านบนเครือข่ายระยะไกล |
| **นักศึกษา** | นายอภิชาต ชะโลธร |
| **รหัสนักศึกษา** | 48066837 |
| **ปริญญา** | วิทยาศาสตรมหาบัณฑิต |
| **สาขาวิชา** | เทคโนโลยีสารสนเทศ |
| **แขนงวิชา** | วิทยาการสารสนเทศ |
| **ปีการศึกษา** | 2552 |
| **อาจารย์ที่ปรึกษา** | รศ.ดร.จันทร์บูรณ์ สถิตวิริยวงศ์ |

## บทคัดย่อ


การเชื่อมต่อระบบเครือข่ายภายในขององค์กรโดยผ่านระบบเครือข่ายระยะไกล (Wide Area Network : WAN) มีปัจจัยที่เป็นตัวกำหนดประสิทธิภาพของเครือข่ายอยู่หลายประเภท โดยปัจจัยที่สำคัญที่องค์กรส่วนใหญ่คำนึงถึงคือความเร็วในการส่งข้อมูลและปริมาณย่านความถี่ (Bandwidth) ที่ถูกใช้ไปในการติดต่อสื่อสาร การที่องค์กรมีระบบที่คอยตรวจสอบ ทราฟฟิก (Traffic) จะช่วยให้ผู้ดูแลระบบสามารถตรวจสอบดูว่าลิงค์ (Link) ที่เชื่อมต่อกับเครือข่ายระยะไกลมี Utilization อย่างไร มีแอพพลิเคชัน (Application) ใดบ้างที่ใช้งานบนลิงค์นั้นอยู่ ซึ่งสามารถระบุไปถึงผู้ใช้งานได้ด้วย และที่สำคัญคือทำให้ผู้ดูแลระบบสามารถตรวจสอบได้ว่าเครือข่ายที่ดูแลอยู่มีความผิดปกติหรือไม่ เช่นติดไวรัสคอมพิวเตอร์ หรือมีเครื่องคอมพิวเตอร์ในเครือข่ายถูกคุกคาม

โครงการนี้จะเสนอแนวทางในการพัฒนาระบบตรวจสอบทราฟฟิกของระบบเครือข่ายระยะไกล โดยข้อมูลที่ใช้ในการสื่อสารจะเป็นข้อมูลที่ใช้สำหรับส่งผ่านไปในเครือข่ายระยะไกล โดยจะนำหลักการของทฤษฎีการส่งต่อข้อมูลของระบบเครือข่ายคอมพิวเตอร์แบบไคลเอ็นต์เซิร์ฟเวอร์ เช่น SYSLOG เข้ามาช่วยในการพัฒนาระบบ โดยส่งข้อมูลจากตัวสวิตซ์ (Switch) เข้ามาเก็บที่เซิร์ฟเวอร์ และใช้แอพพลิเคชัน ASP.NET มาพัฒนาแอพพลิเคชันในการนำข้อมูลมาแปลงให้อยู่ในรูปของฐานข้อมูลเพื่อให้ง่ายในการเข้าถึงและตรวจสอบ นอกจากนั้นยังได้พัฒนาแอพพลิเคชันเพื่อเป็นตัวช่วยนำข้อมูลนี้มาเสนอผ่านทางเว็บ (Web) ซึ่งการนำเสนอสามารถเลือกการนำเสนอแบบโปรโตคอล (Protocol) หรือนำเสนอแบบเลือกซัพเน็ต (Subnet) ซึ่งในทุกๆการนำเสนอจะแสดงรูปแบบเป็นกราฟ เช่นกราฟแท่ง กราฟเส้น หรือกราฟวงกลม นอกจากนี้ยังสามารถเลือกช่วงเวลาของข้อมูลที่ต้องการตรวจสอบได้ ในส่วนของผู้ดูแลระบบจะมีฟังก์ชันในการจัดการกับข้อมูลของซับเน็ตหรือโพรโตคอลขององค์กรที่ต้องการจะตรวจสอบทราฟฟิก รวมทั้งระบบเองยังสามารถแจ้งเตือนในกรณีที่มีการใช้งานของโพรโตคอลในการติดต่อสื่อสารเกินกว่าค่าที่กำหนดไว้

| | |
|---|---|
| **Title** | Network Traffic Monitoring System for sending Data on Wide Area Network (WAN) |
| **Student** | Mr. Apichat Chalothorn |
| **Student ID.** | 48066837 |
| **Degree** | Master of Science |
| **Program** | Information Technology |
| **Major** | Information Science |
| **Academic Year** | 2009 |
| **Advisor** | Assoc.Prof. Dr.Chanboon Sathitwiriyawong |


## ABSTRACT

Data communication in the organization via using Wide Area Network (WAN) has many factors to determine the performance of Network. The important factors which most organizations consider are speed of data transmission and bandwidth of the communication link. The organization which has traffic monitoring system will help network administrator to make sure how utilization of WAN communication link is. And what application is communicated on the link. Moreover, network administrator can specify which user communicates during that period. Especially, network administrator can verify whether network status is normal or not such as infected virus within organization or network threats.

This project will provide guidance in the development of traffic monitoring system on Wide Area Network. Data which are passed in communication link are transmitted between each organization passing Wide Area Network. The principle of computer network in category of client/server message transmission such as SYSLOG protocol is used for this development project. Data which are sent from switch and collected in server are transformed into Database format by using ASP.NET as data registration application. And then, web application which is developed to query data from Database and present as Webpage for user. The presentation can show data categorized into Protocol and Network Subnet. It is easy to understand because it presents by using graph format such as pie chart or line chart. User can specify monitoring period to scope data for checking. For system administrator, there are functions to maintain data such as subnet, protocol which the organization uses for traffic monitor. Moreover, the system itself, has ability to alarm when frequency of communication access is over the limitation which is set by system administrator.

# กิตติกรรมประกาศ

ในการศึกษาและพัฒนาโครงการพัฒนาระบบงานในหัวข้อระบบตรวจสอบทราฟฟิกของเครือข่ายสำหรับข้อมูลที่ถูกส่งผ่านบนเครือข่ายระยะไกลที่จัดทำขึ้นมานี้ ผู้จัดทำขอขอบพระคุณ รศ.ดร.จันทร์บูรณ์ สถิตวิริยวงศ์ อาจารย์ที่ปรึกษาของโครงงานพัฒนาระบบงาน ที่กรุณาให้ความรู้ คำชี้แนะ คำแนะนำและแนวทางการทำโครงการฯอันเป็นประโยชน์อย่างมากต่อการพัฒนาโครงงานนี้ ตลอดจนตรวจสอบแก้ไขจนกระทั่งโครงงานสำเร็จลุล่วง

นอกจากนี้ขอขอบพระคุณรศ.ดร.โชติพัชร์ ภรณวลัย ที่กรุณาให้คำแนะนำและความรู้เกี่ยวกับระบบเน็ตเวิร์คตั้งแต่พื้นฐานจนถึงขั้นประยุกต์ ซึ่งเป็นส่วนสำคัญอีกส่วนในการทำโครงการในครั้งนี้

ขอขอบคุณบุคคลากรของคณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุกท่าน ที่ให้ความช่วยเหลือเรื่องเอกสารและให้ความอนุเคราะห์ตลอดมา

ขอขอบคุณเพื่อนๆ พี่ๆ และน้องๆ สาขาวิชาเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง และเพื่อนๆทุกๆคนที่ได้ให้คำแนะนำ ให้กำลังใจ และช่วยเหลือผู้จัดทำ ในเรื่องแนวทางการพัฒนาระบบ การเขียนและแก้ไขแอพพลิเคชันให้สามารถทำงานได้ประสบผลสำเร็จ

ที่สำคัญเป็นอย่างยิ่ง ขอขอบคุณบริษัทฟูจิตสึ (ประเทศไทย) จำกัด และบริษัทโตชิบาสตอเรจ ดีไวส์ (ประเทศไทย) จำกัด ที่อนุเคราะห์ให้ยืมอุปกรณ์ ตลอดจนระบบต่างๆภายในองค์กรจนทำให้โครงการพัฒนานี้สำเร็จได้ผลเป็นอย่างดี

สุดท้ายนี้ผู้จัดทำขอกราบขอบพระคุณ บิดา มารดา และครอบครัวที่เป็นทั้งกำลังใจ และให้การสนับสนุนในทุกๆเรื่อง จนทำให้ผู้จัดทำสามารถทำโครงงานสำเร็จลุล่วงด้วยดี

คุณค่าและประโยชน์อันพึงมาจากโครงงานพัฒนาระบบงานฉบับนี้ ผู้จัดทำขอมอบแด่ผู้มีพระคุณทุกท่าน

อภิชาต ชะโลธร

# สารบัญ


หน้า

บทคัดย่อภาษาไทย ..... I

บทคัดย่อภาษาอังกฤษ ..... II

กิตติกรรมประกาศ ..... III

สารบัญ ..... IV

สารบัญตาราง ..... VI

สารบัญรูป ..... VII

บทที่ 1 บทนำ ..... 1

1.1 ความเป็นมาและความสำคัญของปัญหา ..... 1

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา ..... 1

1.3 ขอบเขตของโครงงาน ..... 2

1.4 ขั้นตอนของการศึกษา ..... 3

1.5 ประโยชน์ที่คาดว่าจะได้รับ ..... 3

1.6 เครื่องมือที่ใช้ในการพัฒนาระบบ ..... 3

บทที่ 2 ทฤษฎีที่เกี่ยวข้อง ..... 4

2.1 SYStem LOG Protocol (SYSLOG Protocol) ..... 4

2.2 สถาปัตยกรรมของ SYSLOG Protocol ..... 6

2.3 การทำงานของโพรโตคอล HTTP ..... 12

2.4 หลักการเบื้องต้นของภาษา ASP.NET ..... 14

บทที่ 3 การวิเคราะห์และออกแบบการทำงานของระบบ ..... 15

3.1 การวิเคราะห์ความต้องการ ..... 15

3.2 โครงสร้างของระบบ ..... 16

3.3 ลักษณะการทำงาน ..... 17

3.4 แผนภาพแสดง Flowchart ของการรีจีสเตอร์ข้อมูล ..... 21

3.5 แผนภาพแสดง Use Case Diagram ..... 22

3.6 แผนภาพแสดง Sequence Diagram ..... 24

3.7 การออกแบบฐานข้อมูล ..... 32

# สารบัญ (ต่อ)


หน้า

บทที่ 4 การพัฒนาระบบงาน ..... 35
4.1 เครื่องมือที่ใช้ในการพัฒนาระบบ ..... 35
4.2 คู่มือการใช้งานระบบของผู้ใช้ ..... 46

บทที่ 5 สรุปผลและข้อเสนอแนะ ..... 71
5.1 สรุปผลการดำเนินการพัฒนาระบบ ..... 71
5.2 ประโยชน์ที่ได้รับจากการพัฒนาระบบ ..... 72
5.3 ปัญหาและอุปสรรคในการพัฒนาระบบ ..... 73
5.4 ข้อเสนอแนะและแนวทางในการพัฒนาเพิ่มเติม ..... 73

บรรณานุกรม ..... 75
ภาคผนวก ..... 76
ประวัติผู้เขียน ..... 82

# สารบัญตาราง

ตารางที่ หน้า

3.1 ตาราง PORT เก็บข้อมูลของพอร์ตที่ใช้ในการติดต่อสื่อสาร..... 33

3.2 ตาราง FTC_SUBNET เก็บข้อมูลของซับเน็ตในองค์กร..... 33

3.3 ตาราง TRAFFIC_LOG เก็บข้อมูลของการติดต่อสื่อสาร..... 34

A-1 ตารางซับเน็ตขององค์กร..... 80

# สารบัญรูป


| รูปที่ | | หน้า |
|---|---|---|
| 2.1 | การทำงานของโพรโตคอล SYSLOG | 4 |
| 2.2 | แผนภาพระดับชั้นการส่งข้อมูลของโพรโตคอล SYSLOG | 6 |
| 2.3 | ตัวอย่างการติดต่อสื่อสารในการส่งข้อมูลของโพรโตคอล SYSLOG | 8 |
| 2.4 | รูปแบบข้อความ SYSLOG ตามมาตรฐาน RFC 5234 | 9 |
| 2.5 | Syslog message facilities | 10 |
| 2.6 | Syslog message severities | 11 |
| 2.7 | การรับส่งข้อมูลของ HTTP โดยอาศัยหลักการไคลเอ็นต์-เซิร์ฟเวอร์ | 13 |
| 2.8 | ขั้นตอนการติดต่อสื่อสารบนโพรโตคอล HTTP | 13 |
| 3.1 | การเชื่อมต่ออุปกรณ์เน็ตเวิร์คขององค์กรในส่วนที่เชื่อมต่อกับเครือข่ายระยะไกล | 17 |
| 3.2 | การเชื่อมต่อของ Syslog server ภายในเครือข่ายภายในองค์กร | 18 |
| 3.3 | ขั้นตอนในการดำเนินการจากฝั่งไคลเอ็นต์ | 18 |
| 3.4 | ภาพระบบโดยรวม | 20 |
| 3.5 | Flowchart การรีจีสเตอร์ข้อมูลลงฐานข้อมูล | 21 |
| 3.6 | แผนภาพ Use Case Diagram ของระบบ | 23 |
| 3.7 | แผนภาพ Sequence Diagram ของกระบวนการ Login | 25 |
| 3.8 | แผนภาพ Sequence Diagram ของกระบวนการ Maintain data | 26 |
| 3.9 | แผนภาพ Sequence Diagram ของกระบวนการ Search | 27 |
| 3.10 | แผนภาพ Sequence Diagram ของกระบวนการ Set data condition | 28 |
| 3.11 | แผนภาพ Sequence Diagram ของกระบวนการ Show data | 29 |
| 3.12 | แผนภาพ Sequence Diagram ของกระบวนการ Get Log from Device | 30 |
| 3.13 | แผนภาพ Sequence Diagram ของกระบวนการ Register Log to Database | 31 |
| 3.14 | ความสัมพันธ์ของข้อมูลของระบบตรวจสอบทราฟฟิกของเครือข่ายระยะไกล | 32 |

# สารบัญรูป (ต่อ)

รูปที่ หน้า

4.1 คำสั่งคอนฟิกูเรชันโพรโตคอล SYSLOG บนสวิตซ์ ..... 36
4.2 หน้าจอของแอพพลิเคชัน Kiwi Syslog Daemon version 8.2.18 ..... 37
4.3 หน้าจอหลักของการเซตอัพค่าของแอพพลิเคชัน Kiwi Syslog Daemon ..... 38
4.4 การเซตอัพค่าไดเรกทอรีและรูปแบบในการเก็บล็อกไฟล์ของแอพพลิเคชัน Kiwi Syslog Daemon ..... 39
4.5 การเซตอัพค่า DNS ของแอพพลิเคชัน Kiwi Syslog Daemon ..... 40
4.6 หน้าจอของแอพพลิเคชัน Kiwi Syslog Daemon เมื่อได้รับข้อมูลจากตัวสวิตซ์ ..... 41
4.7 หน้าจอของแอพพลิเคชัน FJ-WAN Database builder ..... 42
4.8 หน้าจอของแอพพลิเคชัน FJ-WAN Database builder ขณะที่มีการรีจีสเตอร์ข้อมูล ..... 43
4.9 ขั้นตอนการร้องขอข้อมูลจากไคลเอ็นต์และการตอบสนองของเซิร์ฟเวอร์ ..... 45
4.10 หน้าจอหลักของระบบตรวจสอบทราฟฟิกบนเครือข่ายระยะไกล ..... 46
4.11 หน้าจอกำหนดเงื่อนไขเพื่อดูของมูลการใช้แบบโพรโตคอล ..... 48
4.12 กราฟแสดงหน้าผลการใช้งานย่านความถี่โดยแบ่งตามโพรโตคอล ..... 49
4.13 หน้าจอกำหนดเงื่อนไขเพื่อดูของมูลการใช้แบบซับเน็ต ..... 50
4.14 กราฟแสดงหน้าผลการใช้งานย่านความถี่โดยแบ่งตามซับเน็ต ..... 51
4.15 เมนูย่อยภายใต้หัวข้อ Show pages as link ..... 52
4.16 หน้าจอกำหนดเงื่อนไขเพื่อดูของมูลการใช้ ..... 53
4.17 กราฟแสดงหน้าผลการใช้งานย่านความถี่โดยแบ่งตามโพรโตคอล ..... 54
4.18 หน้าจอกำหนดเงื่อนไขเพื่อดูของมูลการใช้แบบซับเน็ต ..... 55
4.19 กราฟแสดงหน้าผลการใช้งานย่านความถี่โดยแบ่งตามซับเน็ต ..... 56
4.20 การเลือกลักษณะของกราฟในแบบต่างๆเพื่อให้แสดงบนหน้าจอ ..... 57
4.21 ข้อมูลการใช้งานของโพรโตคอล HTTP ในช่วงเวลาหนึ่ง ..... 58
4.22 หน้าจอแสดงเงื่อนไขรายละเอียดของโพรโตคอล HTTP ..... 59
4.23 กราฟแสดงเครื่องคอมพิวเตอร์ที่ใช้โพรโตคอล HTTP บนเครือข่ายระยะไกล ..... 60
4.24 ข้อมูลการใช้งานโพรโตคอล HTTP เครื่อง 10.164.46.86 ณ วันที่18 มิถุนายน ค.ศ.2009 ..... 61
4.25 หน้าจอแสดงเงื่อนไขรายละเอียดเครื่อง 10.164.46.86 ณ ช่วงเวลาที่กำหนด ..... 62
4.26 ข้อมูลเครื่องคอมพิวเตอร์ที่ติดต่อกับเครื่อง 10.164.46.86 โดยใช้งานโพรโตคอล HTTP ณ วันที่18 มิถุนายน ค.ศ.2009 ..... 63

# สารบัญรูป (ต่อ)


รูปที่ หน้า

4.27 หน้าจอกรอกชื่อและรหัสผ่านก่อนเข้าสู่เมนู Maintenance ..... 64

4.28 หน้าจอการบำรุงรักษาระบบ ..... 65

4.29 หน้าจอแสดงโพรโตคอลเบื้องต้นที่กำหนดไว้ ..... 66

4.30 การเพิ่มค่าโพรโตคอลเข้าในระบบ ..... 67

4.31 ข้อมูลโพรโตคอลที่เพิ่มเข้าไปในระบบ ..... 68

4.32 เมนูย่อยในส่วนการบำรุงรักษาซับเน็ต ..... 69

4.33 ซับเน็ตขององค์กรที่ใส่ลงในระบบ ..... 70

A-1 แผนภาพการเชื่อมต่อระบบเครือข่าย ..... 78

# บทที่ 1
# บทนำ

## 1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเทคโนโลยีในการเชื่อมต่อระบบเครือข่ายภายในองค์กรมีการพัฒนาอย่างต่อเนื่อง ไม่ว่าจะเป็นการนำเอาฮาร์ดแวร์หรือซอฟแวร์เข้ามาช่วยในการรับส่งข้อมูล สำหรับการเชื่อมต่อระบบเครือข่ายภายในขององค์กรโดยผ่านทางระบบเครือข่ายระยะไกล (Wide Area Network : WAN) นั้นมีปัจจัยที่เป็นตัวกำหนดประสิทธิภาพของเครือข่ายอยู่หลายประเภท ไม่ว่าจะเป็นสายสัญญาณที่ใช้ในการเชื่อมต่อ อุปกรณ์ในระบบเครือข่ายที่ใช้ทั้งฝั่งต้นทางและฝั่งปลายทาง แต่ปัจจัยที่สำคัญที่องค์กรส่วนใหญ่คำนึงถึงก็คือความเร็วในการรับส่งข้อมูล และปริมาณย่านความถี่ (Bandwidth) ที่ถูกใช้ไปในการติดต่อสื่อสาร การที่องค์กรมีระบบที่คอยตรวจสอบทราฟฟิก (Traffic) ของการรับส่งข้อมูลภายในเครือข่ายระยะไกล จะช่วยให้ผู้ดูแลระบบสามารถตรวจสอบดูว่าลิงค์ (Link) ที่เชื่อมต่อของเครือข่ายระยะไกลก่อประโยชน์ (Utilization) ต่อองค์กรได้มากน้อยเพียงใด ในการติดต่อระหว่างองค์กรนั้นๆ มีการใช้แอพพลิเคชั่น (Application) ใดบ้างที่ใช้งานบนลิงค์นั้นอยู่ และถ้าหากระบบตรวจสอบนั้นสามารถที่จะระบุได้ถึงต้นทางหรือผู้ใช้งานว่าใช้ไอพีแอดเดรส (IP Address) ใดติดต่อกับฝั่งปลายทางด้วยไอพีแอดเดรสใดอยู่ ก็ยิ่งจะเป็นการช่วยให้ผู้ดูแลระบบสามารถตรวจสอบได้ว่าเครือข่ายที่ดูแลอยู่นั้นมีความผิดปกติหรือไม่ เช่น เครือข่ายภายในถูกโจมตีหรือคุกคามจากผู้ประสงค์ร้าย หรือมีการแพร่กระจายของไวรัสคอมพิวเตอร์ซึ่งทำให้การใช้ความถี่ของเครือข่ายเพิ่มสูงขึ้นอย่างผิดปกติ ดังนั้นผู้ดูแลระบบจึงสามารถนำเอาประโยชน์จากระบบตรวจสอบทราฟฟิกนี้มาช่วยป้องกันไม่ให้องค์กรได้รับผลกระทบหรือความเสียหายที่อาจจะเกิดขึ้นได้

## 1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

ระบบตรวจสอบทราฟฟิกของเครือข่ายสำหรับข้อมูลที่ถูกส่งผ่านบนเครือข่ายระยะไกล มีวัตถุประสงค์ดังต่อไปนี้

1. เพื่อสร้างระบบที่สามารถตรวจสอบทราฟฟิกที่ถูกใช้งานอยู่ในระบบเครือข่ายระยะไกลได้
2. เพื่อวิเคราะห์ว่าในการติดต่อสื่อสารขององค์กร มีแอฟพลิเคชั่นใดบ้างที่ใช้งานอยู่ รวมทั้งสามารถตรวจสอบแอฟพลิเคชั่นที่นอกเหนือจากการใช้งานปกติได้
3. เพื่ออำนวยความสะดวกให้แก่ผู้ดูแลระบบให้สามารถตรวจสอบการติดต่อสื่อสารของข้อมูลบนเครือข่ายระยะไกลได้ง่ายขึ้น

4. เพื่อเก็บข้อมูลต้นทางและปลายทางในการสื่อสารแต่ละครั้ง และนำมาตรวจสอบว่าระบบเครือข่ายนี้มีสิ่งผิดปกติเกิดขึ้นหรือไม่
5. เพื่อวิเคราะห์ว่าในการติดต่อสื่อสารบนเครือข่ายระยะไกลนั้น คู่สนทนาต้นทางและปลายทางใช้ประโยชน์ของลิงค์ได้ตรงตามเป้าหมายขององค์กรหรือไม่

## 1.3 ขอบเขตของการศึกษา

การพัฒนาระบบตรวจสอบทราฟฟิกของเครือข่ายสำหรับข้อมูลที่ถูกส่งผ่านบนเครือข่ายระยะไกลเป็นเก็บข้อมูลเครื่องคอมพิวเตอร์ต้นทางและปลายทางที่ติดต่อสื่อสารกันระหว่างองค์กร 2 แห่ง โดยได้กำหนดขอบเขตของการศึกษาไว้ดังนี้คือ

1. สามารถระบุถึงข้อมูลของเครื่องคอมพิวเตอร์ต้นทางและเครื่องคอมพิวเตอร์ปลายทางที่มีการสื่อสารกันบนเครือข่ายระยะไกล

2. สามารถนำข้อมูลคู่การสื่อสารมาแสดงให้อยู่ในรูปของกราฟแบบต่างๆได้ เช่นกราฟวงกลม กราฟแท่ง เป็นต้น

3. สามารถแสดงว่ามีโพรโตคอลใดใช้งานอยู่บ้าง โดยสามารถแสดงให้อยู่ในรูปของกราฟแบบต่างๆได้เช่นเดียวกัน

4. สามารถเพิ่มหรือลบค่าตัวเลขของพอร์ต (Port number) หรือชื่อของโพรโตคอลหากในตัวโปรแกรมไม่ได้ระบุไว้ได้

5. สามารถเพิ่มหรือลบซับเนท (Subnet) ของระบบเครือข่ายได้ หากในระบบเครือข่ายมีการเพิ่มวงซับเนทหรือลดวงซับเนทที่ต้องการตรวจสอบ

6. ในส่วนของเซิร์ฟเวอร์ (Server) ที่ใช้ในการเก็บข้อมูลนั้น จะใช้การเก็บข้อมูลการสื่อสาร โดยข้อมูลนี้จะถูกส่งมาจากตัวสวิตซ์ (Switch) โดยผ่านทางโพรโตคอล SYSLOG ซึ่งข้อมูลจะเก็บอยู่ในรูปแบบของ Text ก่อน หลังจากนั้นซึ่งจะมีโปรแกรมที่ใช้ในการดึงข้อมูลมาและแปลงให้อยู่ในรูปของฐานข้อมูล เพื่อง่ายต่อการเข้าถึง และข้อมูลนี้จะถูกนำแสดงยังหน้าจอของผู้ใช้งาน

7. ในส่วนของผู้ใช้งาน เมื่อต้องการจะดูข้อมูลจะสามารถดูได้ผ่านทางเวปบราวเซอร์ (Web browser) ต่างๆในรูปแบบของ HTML

## 1.4 ขั้นตอนของการศึกษา

1. ศึกษาและรวบรวมข้อมูลความต้องการของระบบงาน
   - ศึกษาโครงสร้างการเชื่อมต่อระบบเครือข่ายระยะไกลขององค์กร
   - ศึกษาและรวบรวมข้อมูลการใช้งานพื้นฐานขององค์กรว่ามีการใช้โพรโตคอลหลักใดบ้าง รวมทั้งข้อมูลของซับเนท (Subnet) ที่องค์กรใช้งานอยู่

- ศึกษาการทำงานของโพรโตคอล SYSLOG
- ศึกษาการออกแบบระบบและการพัฒนาโปรแกรมประยุกต์โดยใช้โปรแกรมภาษา ASP.Net
- ศึกษาการติดตั้งและคำสั่งในการคอนฟิกูเรชัน (Configuration) สวิตซ์

2. วิเคราะห์และออกแบบการจัดการระบบฐานข้อมูล
   - ออกแบบโครงสร้างฐานข้อมูลเพื่อใช้ในการจัดเก็บข้อมูลที่ส่งมาจากสวิตซ์
   - ออกแบบโครงสร้างโปรแกรม
3. พัฒนาระบบตามการออกแบบที่ได้วางไว้
4. ทดสอบและปรับปรุงระบบให้ใช้งานได้ง่ายและตรงตามความต้องการของผู้ใช้งาน
5. จัดทำเอกสารประกอบการใช้งานระบบ

## 1.5 ประโยชน์ที่คาดว่าจะได้รับ

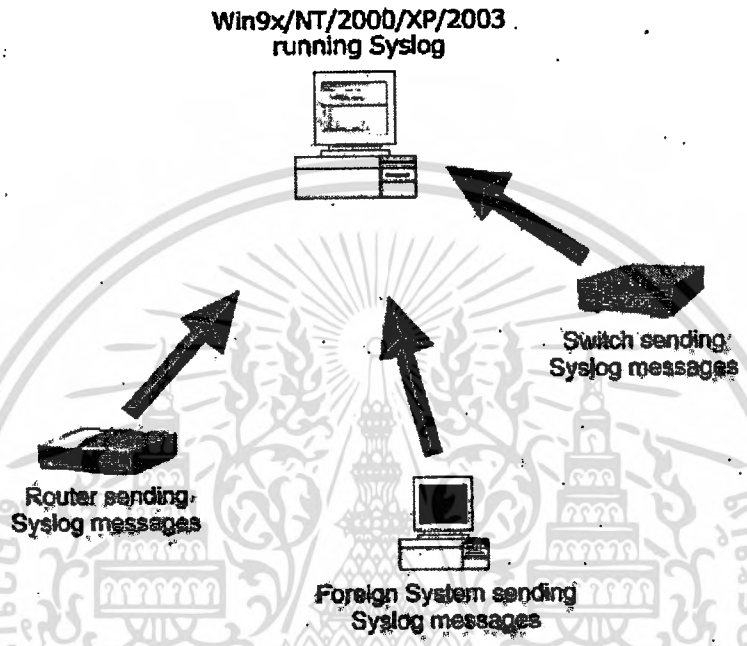
1. เพื่อช่วยอำนวยความสะดวกให้ผู้ดูแลระบบสามารถตรวจสอบว่าระบบเครือข่ายระยะไกลขององค์กรมีการใช้งานตรงตามความต้องการขององค์กรหรือไม่
2. ช่วยให้ผู้ดูแลระบบสามารถตรวจสอบว่าในขณะนั้นระบบเครือข่ายมีความเสี่ยงที่จะถูกโจมตีจากผู้ไม่ประสงค์ดี หรือจากไวรัสคอมพิวเตอร์หรือไม่ โดยพิจารณาจากพอร์ตหรือไอพีแอดเดรสต้นทางและปลายทางที่ติดต่อสื่อสารกันอยู่
3. เพื่อช่วยในการประเมินการเบื้องต้นว่าปริมาณย่านความถี่ที่องค์กรใช้งานอยู่เพียงพอต่อการใช้งานจริงๆของผู้ใช้งานหรือไม่

## 1.6 เครื่องมือที่ใช้ในการพัฒนาระบบ

1. ฮาร์ดแวร์
   - เครื่องคอมพิวเตอร์ที่มีคุณสมบัติ
     1. ซีพียู (CPU) ขั้นต่ำ Intel Pentium IV processor 3.0 GHz.
     2. Hard disk ความจุขั้นต่ำ 100 GB
     3. RAM 2GB
   - สวิตซ์ เลเยอร์ (layer) 2 และ 3 รุ่น Extreme Summit-48si
2. ซอฟต์แวร์
   - Microsoft Internet Explorer
   - VB.NET และ ASP.NET
   - Kiwi Syslog Deamon Version 8.2.18
   - Oracle Enterprise Version 9.2.0.1

# บทที่ 2
# ทฤษฎีที่เกี่ยวข้อง

## 2.1 SYStem LOG Protocol (SYSLOG Protocol)




**รูปที่ 2.1** การทำงานของโพรโตคอล SYSLOG

การติดต่อสื่อสารภายในองค์กรประกอบด้วยอุปกรณ์มากมายด้วยกัน ไม่ว่าจะเป็นเครื่องคอมพิวเตอร์ส่วนบุคคล เซิร์ฟเวอร์ (Server) อุปกรณ์ทางด้านเน็ตเวิร์คหรืออุปกรณ์ที่ใช้ในการติดต่อสื่อสารเช่นเราเตอร์ (Router) สวิตซ์ (Switch) ฮับ (Hub) ซึ่งอุปกรณ์เหล่านี้เมื่อนำมาเชื่อมต่อเข้าด้วยกันเป็นระบบเครือข่ายย่อมจะมีความสลับซับซ้อนแตกต่างกันออกไปตามแต่ขนาดหรือการใช้งานขององค์กรนั้นๆ ในการดูแลรักษาระบบเครือข่ายคอมพิวเตอร์ซึ่งประกอบไปด้วยเครื่องมือต่างๆนั้นหากไม่มีระบบเข้ามาช่วยดูแล จะก่อให้เกิดปัญหายุ่งยากต่อทั้งผู้ดูแลระบบเองและต่อผู้ใช้งานด้วย ดังนั้นจึงมีความจำเป็นที่จะต้องหาวิธีการดูแลและบริหารระบบเครือข่ายให้มีประสิทธิภาพ มีความน่าเชื่อถือต่อการใช้งาน และมีเสถียรภาพในการใช้งาน โดยสามารถส่งข้อมูลและสถานะของตัวอุปกรณ์ต่างๆมายังเซิร์ฟเวอร์ (Server) ที่ผู้ดูแลระบบจัดทำขึ้นมาเก็บข้อมูลเหล่านี้โดยเฉพาะได้ ซึ่งมาตรฐานของ TCP/IP ที่ง่ายต่อการติดตั้งรวมทั้งสะดวกต่อผู้ดูแลระบบในการจัดการระบบเครือข่ายซึ่งเป็นที่นิยมใช้มากที่สุดคือโพรโตคอลที่มีชื่อว่า SYSLOG หรือ SYStem LOG Protocol ซึ่งเป็นโพรโตคอลที่กำหนดโดยองค์กร IETF (International Engineering Task Force) โดยโพรโตคอลเป็นมาตรฐานในการส่งข้อความในการแจ้งเกี่ยวกับ

สถานะ รวมทั้งเหตุการณ์ (Event) ต่างๆที่เกิดขึ้นกับตัวอุปกรณ์โดยผ่านทางระบบเครือข่ายไปยังอุปกรณ์ที่ใช้ในการจัดเก็บข้อความซึ่งเรียกว่าคอเล็กเตอร์ (Collector) ตัวคอเล็กเตอร์ มีชื่อเรียกหลากหลายด้วยกัน ไม่ว่าจะเป็น syslogd หรือ syslog daemon หรือ syslog server สำหรับ SYSLOG โดยแท้จริงแล้วจะมีความหมายด้วยกัน 2 แบบ คือความหมายของตัวโพรโตคอล SYSLOG ที่แท้จริง และความหมายเกี่ยวกับการส่งข้อความของตัว SYSLOG จากทางแอพพลิเคชัน (Application) หรือตัวไลบรารี (Library)

โดยทั่วไปแล้ว ในระบบการควบคุมจัดการและบริหารเครือข่ายจะใช้โพรโตคอล SYSLOG เป็นโพรโตคอลพื้นฐานในการบริหารระบบและตรวจสอบความมั่นคงปลอดภัยของระบบ แม้ว่าตัวโพรโตคอล SYSLOG จะมีจุดบกพร่องอยู่บ้าง แต่เนื่องจากโพรโตคอลเองสนับสนุนต่อการใช้งานของอุปกรณ์ที่หลากหลายประเภท รวมทั้งตัวคอเล็กเตอร์เองก็สามารถใช้ได้กับแฟลตฟอร์ม (Platform) หรือระบบปฏิบัติการ (Operating System) ที่หลากหลาย ผู้ดูแลระบบจึงสามารถประยุกต์นำเอาโพรโตคอล SYSLOG ไปใช้ในการรวบรวมข้อมูลล็อก (Log data) จากระบบที่มีความหลากหลายประเภทมารวมในตัวคอเล็กเตอร์กลางได้

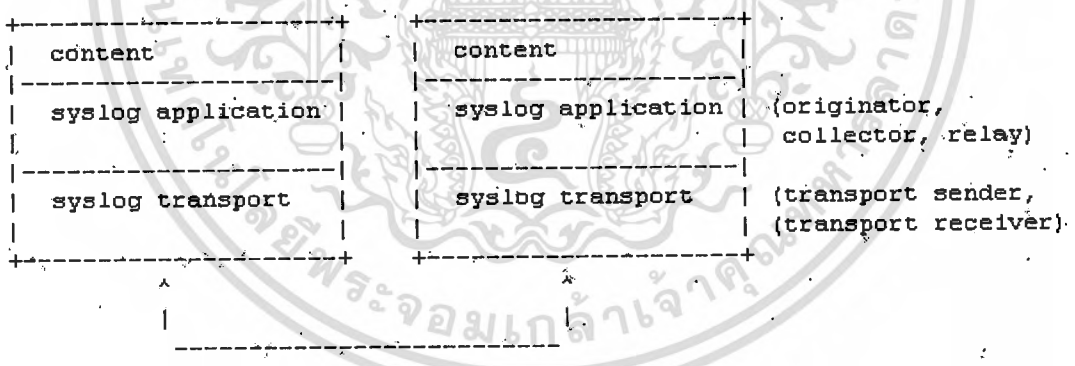
เนื่องจากการที่โพรโตคอล SYSLOG สนับสนุนต่อกระบวนการ (Process) แอพพลิเคชันและระบบปฏิบัติการต่างๆที่หลากหลาย จึงทำให้มีปัญหาการการจัดการหัวข้อ (Content) ของข้อความ SYSLOG ให้เป็นในแนวทางเดียวกันอยู่บ้าง ด้วยเหตุผลนี้จึงทำให้ไม่มีข้อสรุปของรูปแบบที่ใช้ในการจัดการหัวข้อของข้อความที่ใช้ในการส่งไปยังคอเล็กเตอร์ โพรโตคอล SYSLOG ถูกออกแบบมาเพื่อให้ง่ายต่อการส่งข้อความของตัวอุปกรณ์แต่ละตัวโดยใช้กระบวนการ SYSLOG ที่อยู่ในตัวอุปกรณ์นั้นๆเองไปยังตัวคอเล็กเตอร์ โดยจะไม่มีการส่งข้อความตอบรับจากตัวคอเล็กเตอร์กลับมายังอุปกรณ์ เนื่องจากมาตรฐานการออกแบบจะใช้โพรโตคอล UDP (User Datagram Protocol) ในระดับชั้น Transport layer ของ OSI model ในการติดต่อสื่อสาร โดยใช้พอร์ต (Port) หมายเลข 514 เป็นตัวติดต่อ ซึ่งโดยทั่วไปการส่งข้อมูลจะอยู่ในรูปของเท็กซ์ (Text) ทั่วไป แต่ผู้ใช้งานยังสามารถใช้การเข้ารหัส (Encryption) เช่น Stunnel, SSLIO และ SSLWARAP มาห่อหุ้มข้อมูลแพ็กเกจ (Packet) ของ SYSLOG ได้โดยดำเนินการในการเข้ารหัสที่ส่วน SSL/TLS

ในทางทฤษฎีเบื้องต้นของโพรโตคอล SYSLOG และกระบวนการในการดำเนินงานจะอยู่ในรูปแบบที่ง่าย โดยไม่จำเป็นต้องมีการทำงานประสานกันระหว่างอุปกรณ์ที่จะส่งข้อความ SYSLOG และตัวรับข้อมูลหรือคอเล็กเตอร์ ดังนั้นการส่งข้อมูลของ SYSLOG จะเริ่มต้นได้โดยที่มาจำเป็นต้องมีการติดตั้งตัวรับหรือคอเล็กเตอร์ไว้ก่อน ในทางกลับกันตัวอุปกรณ์ก็สามารถรับข้อความได้โดยที่ไม่จำเป็นต้องได้รับการคอนฟิกูเรชันหรือการระบุตัวอุปกรณ์ ซึ่งความง่ายต่อการใช้งานทั้งหมดนี้เป็นข้อดีของโพรโตคอล SYSLOG ที่ทำให้ผู้ใช้งานยอมรับและนำไปประยุกต์ใช้ในองค์กร

ขนาดของแพ็กเกจของข้อความ SYSLOG จะถูกจำกัดไว้ไม่เกิน 1024 ไบท์ (Byte) ซึ่งข้อมูลที่บรรจุอยู่ในแพ็กเกจจะประกอบไปด้วย

1. Facility เป็นเลขจำนวนเต็มที่ใช้ระบุประเภทของต้นทางที่สร้างข้อความ SYSLOG มา ซึ่งตัวต้นทางนี้สามารถจำแนกเป็นระบบปฏิบัติการ กระบวนการ หรือแอพพลิเคชันก็ได้
2. Severity เป็นเลขจำนวนเต็ม 1 หลักใช้ในการบ่งบอกค่าความรุนแรงของข้อความ
3. Hostname ในฟิลด์ (Field) ของชื่อเครื่อง (Hostname) จะประกอบไปด้วย ชื่อของเครื่องที่ถูกคอนฟิกูเรชันไว้ หรือไอพีแอดเดรส สำหรับอุปกรณ์เช่นตัวเราเตอร์หรือไฟร์วอลล์ (Firewall) ที่มีการเชื่อมต่อด้วยอินเทอร์เฟซหลายตัว โพรโตคอล SYSLOG จะใช้ไอพีแอดเดรสของอินเทอร์เฟซที่ข้อความถูกส่งผ่านออกมา
4. Timestamp เป็นเวลาเฉพาะของตัวอุปกรณ์เมื่อข้อความถูกสร้างขึ้นมา โดยจะอยู่ในรูปแบบของ MMM DD HH:MM:SS
5. Message เป็นข้อความของ SYSLOG ที่อยู่ในรูปแบบของเท็กซ์ (Text) พร้อมทั้งข้อมูลเพิ่มเติมที่ได้ของกระบวนการในการสร้างข้อความ

## 2.2 สถาปัตยกรรมของ SYSLOG Protocol




**รูปที่ 2.2** แผนภาพระดับชั้นการส่งข้อมูลของโพรโตคอล SYSLOG

โพรโตคอล SYSLOG แบ่งเป็น 3 ระดับด้วยกันคือ

1. Syslog content เป็นข้อมูลการจัดการที่ถูกบรรจุอยู่ในข้อความของ SYSLOG
2. Syslog application เป็นระดับชั้นที่ใช้ในการสร้าง (Generation) แปรความหมาย (Interpretation) การหาเส้นทาง (Routing) และการจัดเก็บ (Storage) ของข้อความ ในระดับชั้นนี้สามารถแบ่งรายละเอียดได้เป็น
   - Originator เป็นฝั่งที่เริ่มต้นสร้าง Syslog content เพื่อที่จะนำไปใส่ในข้อความ

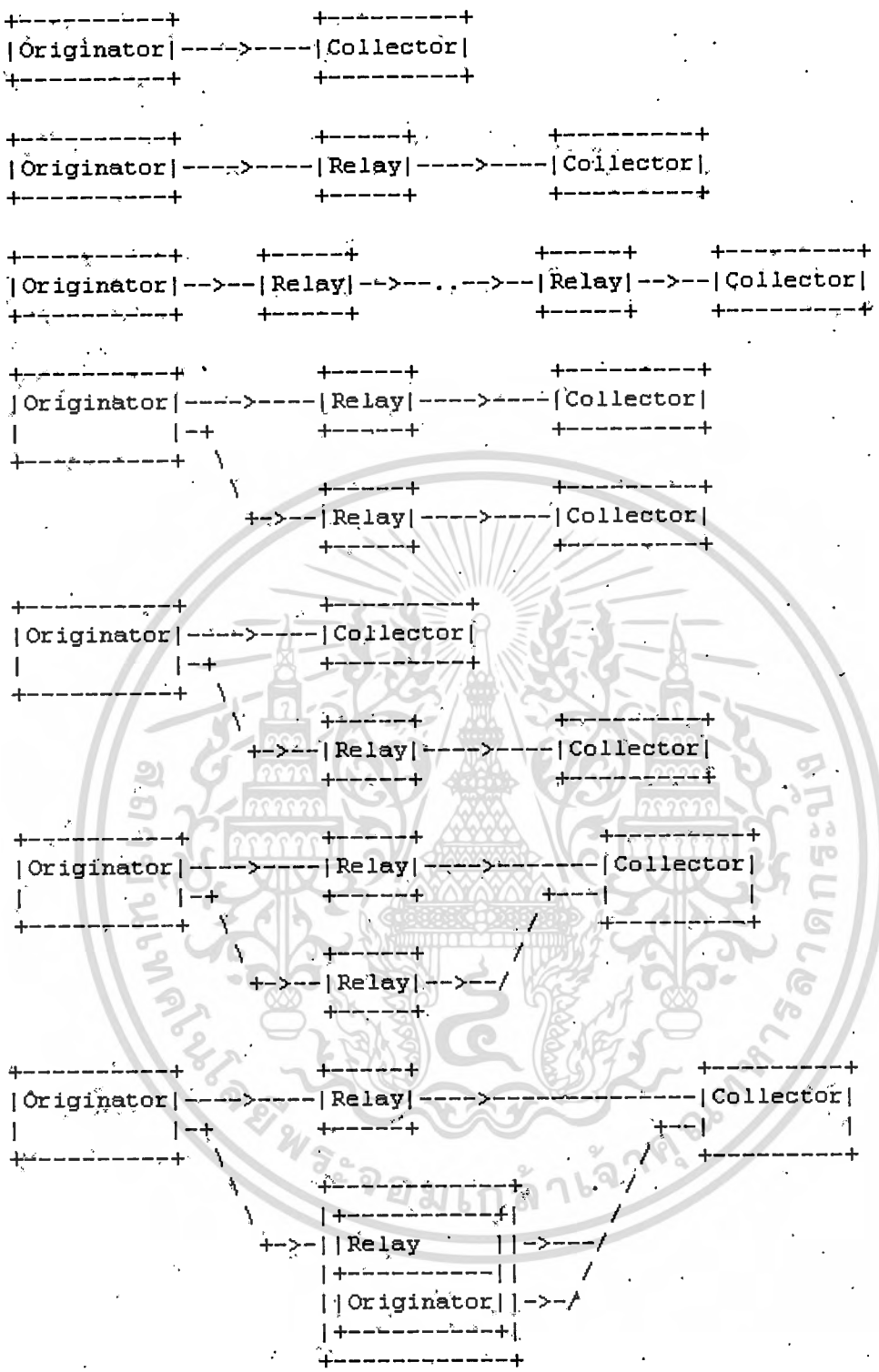
- Collector เป็นฝั่งที่รวบรวม Syslog content เพื่อนำไปใช้ในการวิเคราะห์ต่อไป
- Relay ใช้ในการส่งต่อข้อความ ยอมรับข้อความที่ส่งมาจาก Originator หรือรีเลย์ (Relay) ตัวอื่นๆ และส่งไปให้ยังตัว Collector หรือรีเลย์อื่นๆต่อไป

3. Syslog transport เป็นระดับชั้นในการนำข้อความป้อนเข้าสู่สายเชื่อมต่อเช่นสาย UTP และส่งข้อความออกไป สามารถแบ่งออกเป็น
   - Transport sender ส่งผ่านข้อคววม SYSLOG ไปยัง Transport protocol ที่รพบุไว้
   - Transport receiver เป็นตัวนำข้อความ SYSLOG ที่ได้รับมาจาก Transport protocol ที่ระบุไว้

หลักการทำงานพื้นฐานของโพรโตคอล SYSLOG ในการติดต่อสื่อสารเพื่อส่งข้อความนั้นจะมีหลักด้วยกัน 3 ประการคือ

1. โพรโตคอล SYSLOG ไม่มีการจัดเตรียมตอบรับของข้อความที่ได้รับ แม้ว่าในระดับชั้น Transport layer จะสนับสนุนข้อมูลของสถานะก็ตาม เนื่องจากโพรโตคอล SYSLOG เป็นโพรโตคอลที่ใช้ในการสื่อสารแบบง่ายๆ
2. Originator และรีเลย์อาจถูกคอนฟิกูเรชันเพื่อให้ส่งข้อความที่เหมือนกันไปให้กับ Collector หรือรีเลย์อื่นๆได้
3. Originator รีเลย์ และ Collector อาจจะอยู่ภายในระบบเดียวกันก็ได้

สำหรับตัวอย่างของการติดต่อสื่อสารในการส่งข้อมูลของโพรโตคอล SYSLOG จะเป็นดังรูปที่ 2.3 ซึ่งในความเป็นจริงแล้วอาจมีรูปแบบที่หลากหลายกว่านี้ตามแต่ผู้ดูแลระบบจะดำเนินการ ในตัวอย่างจะพบว่ารีเลย์อาจจะส่งข้อความทั้งหมด หรือแค่บางส่วนที่ได้รับ และในทางกลับกันคืออาจจะข้อความทั้งหมดหรือบางส่วนที่ตัวมันสร้างขึ้นมาได้




**รูปที่ 2.3** ตัวอย่างการติดต่อสื่อสารในการส่งข้อมูลของโพรโตคอล SYSLOG

รูปแบบข้อความ SYSLOG ตามมาตรฐาน RFC 5234 จะถูกกำหนดตามรูปที่ 2.4 คือ

```
SYSLOG-MSG      = HEADER SP STRUCTURED-DATA [SP MSG]

HEADER          = PRI VERSION SP TIMESTAMP SP HOSTNAME
                  SP APP-NAME SP PROCID SP MSGID
PRI             = "<" PRIVAL ">"
PRIVAL          = 1*3DIGIT ; range 0 .. 191
VERSION         = NONZERO-DIGIT 0*2DIGIT
HOSTNAME        = NILVALUE / 1*255PRINTUSASCII

APP-NAME        = NILVALUE / 1*48PRINTUSASCII
PROCID          = NILVALUE / 1*128PRINTUSASCII
MSGID           = NILVALUE / 1*32PRINTUSASCII

TIMESTAMP       = NILVALUE / FULL-DATE "T" FULL-TIME
FULL-DATE       = DATE-FULLYEAR "-" DATE-MONTH "-" DATE-MDAY
DATE-FULLYEAR   = 4DIGIT
DATE-MONTH      = 2DIGIT  ; 01-12
DATE-MDAY       = 2DIGIT  ; 01-28, 01-29, 01-30, 01-31 based on
                          ; month/year
FULL-TIME       = PARTIAL-TIME TIME-OFFSET
PARTIAL-TIME    = TIME-HOUR ":" TIME-MINUTE ":" TIME-SECOND
                  [TIME-SECFRAC]
TIME-HOUR       = 2DIGIT  ; 00-23
TIME-MINUTE     = 2DIGIT  ; 00-59
TIME-SECOND     = 2DIGIT  ; 00-59
TIME-SECFRAC    = "." 1*6DIGIT
TIME-OFFSET     = "Z" / TIME-NUMOFFSET
TIME-NUMOFFSET  = ("+" / "-") TIME-HOUR ":" TIME-MINUTE

STRUCTURED-DATA = NILVALUE / 1*SD-ELEMENT
SD-ELEMENT      = "[" SD-ID *(SP SD-PARAM) "]"
SD-PARAM        = PARAM-NAME "=" %d34 PARAM-VALUE %d34
SD-ID           = SD-NAME
PARAM-NAME      = SD-NAME
PARAM-VALUE     = UTF-8-STRING ; characters '"', '\' and
                               ; ']' MUST be escaped.
SD-NAME         = 1*32PRINTUSASCII
                  ; except '=', SP, ']', %d34 (")

MSG             = MSG-ANY / MSG-UTF8
MSG-ANY         = *OCTET ; not starting with BOM
MSG-UTF8        = BOM UTF-8-STRING
BOM             = %xEF.BB.BF

UTF-8-STRING    = *OCTET ; UTF-8 string as specified
                  ; in RFC 3629

OCTET           = %d00-255
SP              = %d32
PRINTUSASCII    = %d33-126
NONZERO-DIGIT   = %d49-57
DIGIT           = %d48 / NONZERO-DIGIT
NILVALUE        = "-"
```

**รูปที่ 2.4** รูปแบบข้อความ SYSLOG ตามมาตรฐาน RFC 5234

1. ความยาวข้อความ (Message length) ขนาดความยาวของข้อความ SYSLOG จะถูกกำหนดโดย Syslog transport mapping ที่ใช้งานอยู่ โดยจะมีขนาดได้อย่างน้อยที่สุดคือ 480 Octet
2. Header ในฟิลด์นี้จะมีขนาดได้ 7 ตัวอักษรที่เป็นแบบ ASCII ซึ่งจะแบ่งเป็น
   - PRI มีขนาด 3-5 ตัวอักษรโดยมีเครื่องหมาย "<" และ ">" ปิดระหว่างหัวและท้ายข้อมูล โดยข้อมูลจะมีลักษณะเป็นตัวเลขซึ่งใช้ในการระบุ Priority value (PRI) ที่มีค่าได้ตั้งแต่ 0 ถึง 999 และทำหน้าที่แทน Facility ดังรูป 2.5 และ Severity ดังรูป 2.6

| Numerical Code | Facility |
|---|---|
| 0 | kernel messages |
| 1 | user-level messages |
| 2 | mail system |
| 3 | system daemons |
| 4 | security/authorization messages |
| 5 | messages generated internally by syslogd |
| 6 | line printer subsystem |
| 7 | network news subsystem |
| 8 | UUCP subsystem |
| 9 | clock daemon |
| 10 | security/authorization messages |
| 11 | FTP daemon |
| 12 | NTP subsystem |
| 13 | log audit |
| 14 | log alert |
| 15 | clock daemon (note 2) |
| 16 | local use 0 (local0) |
| 17 | local use 1 (local1) |
| 18 | local use 2 (local2) |
| 19 | local use 3 (local3) |
| 20 | local use 4 (local4) |
| 21 | local use 5 (local5) |
| 22 | local use 6 (local6) |
| 23 | local use 7 (local7) |

**รูปที่ 2.5** Syslog message facilities

| Numerical Code | Severity |
|---|---|
| 0 | Emergency: system is unusable |
| 1 | Alert: action must be taken immediately |
| 2 | Critical: critical conditions |
| 3 | Error: error conditions |
| 4 | Warning: warning conditions |
| 5 | Notice: normal but significant condition |
| 6 | Informational: informational messages |
| 7 | Debug: debug-level messages |

**รูปที่ 2.6** Syslog message severities

- เวอร์ชัน (Version) ใช้ในการระบุเวอร์ชันที่ใช้งานอยู่ของโพรโตคอล SYSLOG ซึ่งจะมีค่าแตกต่างออกไปตามมาตรฐานที่ได้กำหนดไว้ เช่น รูปแบบของ Header ฟิลด์ที่ใช้งานอยู่ เป็นต้น
- Timestamp เป็นค่าที่ระบุเวลาของอุปกรณ์แต่ละตัวเมื่อข้อความ SYSLOG ถูกสร้างขึ้น
- Hostname ใช้ระบุชื่อของอุปกรณ์ที่ส่งข้อความ SYSLOG ในฟิลด์นี้จะประกอบด้วย Hostname และ Domain name ซึ่งทั้งหมดอยู่ในรูปของ FQDN (Fully Qualified Domain Name) ซึ่งในความเป็นจริงอุปกรณ์บางตัวอาจจะไม่สนับสนุนต่อชื่อที่อยู่ในรูปแบบ FQDN ดังนั้นจึงสามารถใช้ข้อมูลแบบอื่นๆเป็นตัวแทนตามลำดับได้ดังนี้
  1. FQDN
  2. Static IP Address
  3. Hostname
  4. Dynamic IP Address
  5. the NILVALUE
- APP-NAME ใช้ระบุอุปกรณ์หรือแอพพลิเคชันที่สร้างข้อความ
- PROCID ใช้ในการระบุชื่อของกระบวนการหรือ Process ID ที่เชื่อมโยงกับข้อความ SYSLOG ใดๆ
- MSGID ใช้ในการระบุชนิดของข้อความ เช่นในไฟร์วอลล์จะใช้ "TCPIN" สำหรับ TCP traffic ขาเข้า (Incoming) และใช้ "TCPOUT" สำหรับ TCP traffic ขาออก (Outgoing)

3. STRUCTURED-DATA เป็นกลไกที่ใช้ในการแสดงข้อมูลให้ง่ายต่อการเข้าใจและแปลรูปแบบของข้อมูล โดยจะประกอบไปด้วย

- SD-ELEMENT ประกอบไปด้วยส่วนสำคัญ 2 ส่วนคือ SD-NAME ซึ่งใช้ระบุชนิดและวัตถุประสงค์ของ SD-ELEMENT และ SD-PARAM ซึ่งจะเป็นพารามิเตอร์ (Parameter) คู่กันระหว่างชื่อ (PARAM-NAME) และค่าของพารามิเตอร์ (PARAM-VALUE)

4. MSG เป็นส่วนที่ใช้ในการจัดหาข้อมูลของเหตุการณ์นั้นๆ ซึ่งโดยทั่วไปตัวอักษรจะต้องอยู่ในรูปของ Unicode ที่มีการเข้ารหัส (Encode) แบบ UTF-8 แต่ถ้าหากข้อความไม่สามารถเข้ารหัสแบบ Unicode ได้ก็สามารถที่จะเข้ารหัสแบบอื่นๆได้เช่นกัน

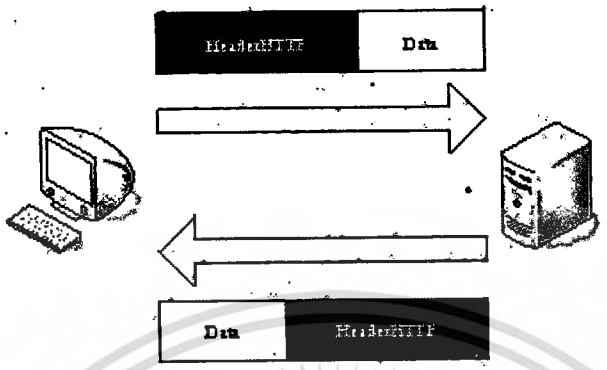
## 2.3 การทำงานของโพรโตคอล HTTP

โพรโตคอล HTTP (HyperText Transfer Protocol) ทำงานอยู่บนพื้นฐานของไคลเอ็นต์ (Client) และเซิร์ฟเวอร์ (Server) ในระดับชั้นแอพพลิเคชันเลเยอร์ (Application layer) ของ OSI model ซึ่งจะต้องมีมาตรฐานในการร้องขอ (Request) และการตอบรับ (Response) ระหว่างเครื่องลูกข่ายกับเครื่องแม่ข่าย ซึ่งเครื่องลูกข่ายคือผู้ใช้ปลายทาง (End-user) และเครื่องแม่ข่ายคือเว็บไซต์ (website server) เครื่องลูกข่ายจะสร้างการร้องขอ HTTP ผ่านทางเว็บบราวเซอร์ (web browser) เว็บครอว์เลอร์ (Web caller) หรือเครื่องมืออื่น ๆ ที่จัดว่าเป็น ตัวแทนผู้ใช้ (User agent) ส่วนเครื่องแม่ข่ายที่ตอบรับ ซึ่งเก็บบันทึกหรือสร้างทรัพยากร (Resource) อย่างเช่นไฟล์ HTML หรือรูปภาพ จะเรียกว่า เครื่องให้บริการต้นทาง (Origin server) ในระหว่างตัวแทนผู้ใช้กับเครื่องให้บริการต้นทางอาจมีสื่อกลางหลายชนิด อาทิ Proxy Gateway และ Tunnel

ปกติเครื่องลูกข่าย HTTPจะเป็นผู้เริ่มสร้างการร้องขอก่อน โดยเปิดการเชื่อมต่อด้วยเกณฑ์วิธีควบคุมการขนส่งข้อมูล (TCP) ไปยังพอร์ตเฉพาะของเครื่องแม่ข่าย (พอร์ต 80 เป็นค่า Default ที่ระบุไว้ของโพรโตคอล HTTP) เครื่องแม่ข่าย HTTPที่เปิดรอรับอยู่ที่พอร์ตนั้น จะเปิดรอให้เครื่องลูกข่ายส่งข้อความร้องขอเข้ามา เมื่อได้รับการร้องขอแล้ว เครื่องแม่ข่ายจะตอบรับด้วยข้อความสถานะอันหนึ่ง ตัวอย่างเช่น "HTTP/1.1 200 OK" ตามด้วยเนื้อหาของมันเองส่งไปด้วย เนื้อหานั้นอาจเป็นแฟ้มข้อมูลที่ร้องขอ ข้อความแสดงข้อผิดพลาด หรือข้อมูลอย่างอื่นเป็นต้น ในทางปฏิบัติ นอกจากจะเชื่อมต่อโดยใช้พอร์ต 80 แล้ว ผู้ดูแลระบบอาจกำหนดค่าพอร์ตเป็นตัวเลขอื่นๆได้ตามความต้องการ แต่ผู้ใช้งานจะต้องระบุหมายเลขพอร์ตลงไปในค่าที่อยู่ของ URL (URL Address) เมื่อต้องการเชื่อมต่อไปยังหน้านั้นๆ

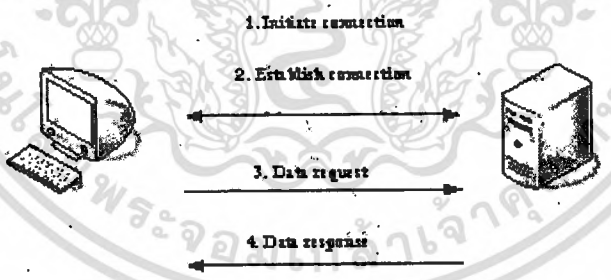
ในการร้องขอจากเครื่องไคลเอ็นต์และการตอบสนองจากเซิร์ฟเวอร์จะต้องมีการรับส่งข้อความระหว่างกัน แต่ข้อมูลที่รับส่งให้กันในแต่ละครั้งไม่ได้มีเฉพาะข้อมูลเพียงอย่างเดียว โดยแต่ละฝ่ายจะต้องมีการใส่ HTTP Header เข้าไปในส่วนหัวของข้องมูลด้วย โดย HTTP Header จะ

ใช้เป็นตัวบอกว่าข้อมูลที่ส่งหลังจากนี้เป็นข้อมูลของการร้องขอมาจากไคลเอ็นต์ใดหรือเป็นข้อมูลที่ตอบสนองมาจากเซิร์ฟเวอร์ใดดังรูปที่ 2.7




รูปที่ 2.7 การรับส่งข้อมูลของ HTTP โดยอาศัยหลักการไคลเอ็นต์-เซิร์ฟเวอร์

สำหรับขั้นตอนการติดต่อสื่อสารของโพรโตคอล HTTP นั้นจะต้องมีการสื่อสารกันทั้ง 2 ฝ่ายคือฝ่ายเครื่องลูกข่ายหรือไคลเอ็นต์ที่ทำการร้องขอ และฝ่ายเครื่องแม่ข่ายหรือเซิร์ฟเวอร์ที่ทำการตอบสนอง จึงจะทำให้การสื่อสารนั้นสมบูรณ์ โดยการติดต่อสื่อสารของโพรโตคอล HTTP นี้จะมีขั้นตอนดังรูปที่ 2.8




รูปที่ 2.8 ขั้นตอนการติดต่อสื่อสารบนโพรโตคอล HTTP

จากรูปที่ 2.8 เครื่องไคลเอ็นต์จะทำการร้องขอโดยผ่านทางเว็บบราวเซอร์ โดยเริ่มสร้างการติดต่อกับทางเซิร์ฟเวอร์ผ่านทางซ็อกเก็ต (Socket) เมื่อทางฝั่งเซิร์ฟเวอร์ได้รับซ็อกเก็ตและทำการเชื่อมต่อสมบูรณ์แล้ว เครื่องไคลเอ็นต์จะส่งคำร้องขอข้อมูลไปยังตัวเซิร์ฟเวอร์ หลังจากที่เซิร์ฟเวอร์ได้รับการร้องขอข้อมูลและตรวจสอบว่าข้อมูลที่ได้รับร้องขอมาจากไคลเอ็นต์มีอยู่หรือไม่แล้วส่งข้อมูลนั้นๆกลับมายังฝั่งไคลเอ็นต์ และเมื่อข้อมูลที่ได้รับครบการเชื่อมต่อก็จะถูกตัดขาดหรือทำการปลดการเชื่อมต่อของซ็อกเก็ตนั้นๆออก

การทำงานของโพรโตคอล HTTP นั้นจะแสดงข้อมูลที่ถูกร้องขอในรูปแบบของภาษา HTML ซึ่งถือว่าเป็นภาษาพื้นฐานในการทำเว็บ (Web) ไม่มีความยืดหยุ่นในการแสดงข้อความ การกำหนดหรือสร้างตัวแปร รวมไปถึงการกำหนดและตรวจสอบเงื่อนไขของการเข้าถึงข้อมูลจากผู้ใช้งานได้ ดังนั้นในปัจจุบันจึงได้มีการพัฒนาภาษา HTML ให้สามารถเพิ่มสคริปต์ (Script) เข้าไปยังภาษา HTML ได้ ซึ่งสคริปต์จะเป็นชุดคำสั่งย่อยๆที่มีหน้าที่เพิ่มเติมความสามารถของโปรแกรมต่างๆ โดยสริปต์จะสามารถแบ่งออกเป็น 2 ประเภทใหญ่ๆตามลักษณะของการแปรภาษา คือ

1. Client-side script เป็นสคริปต์ที่มีการแปลชุดคำสั่งทางฝั่งเครื่องไคลเอ็นต์ โดยตัวสคริปต์จะถูกแปลโดยเว็บบราวเซอร์ เช่น Internet Explorer ตัวอย่างของสคริปต์ประเภทนี้ได้แก่ JavaScript VBScript
2. Server-side script เป็นสคริปต์ที่มีการแปลชุดคำสั่งผ่านทางฝั่งเครื่องเซิร์ฟเวอร์ โดยสคริปต์เหล่านี้จะถูกแปลผ่านทางเว็บบราวเซอร์ เช่น IIS (Internet Information Services) หรือ PWS ให้กลายมาเป็นภาษา HTML แล้วจึงค่อยส่งภาษา HTML นั้นกลับมาให้กับตัวบราวเซอร์แปลต่อไป ตัวอย่างของสคริปต์ประเภทนี้ได้แก่ CGI PHP JSP และที่สำคัญคือ ASP และ ASP.NET

## 2.4 หลักการเบื้องต้นของภาษา ASP.NET

ภาษา ASP.NET มีอีกชื่อหนึ่งว่า ASP+ ซึ่งได้รับการพัฒนาต่อจากภาษา ASP เดิมโดยบริษัทไมโครซอฟท์ ดังนั้นจึงทำให้ ASP.NET มีข้อดีคือ

1. ใช้ภาษาใดๆในการเขียนสคริปต์ได้ จากเดิมที่จะต้องเขียนภาษาโดยใช้เพียงแค่ภาษาที่เป็นสคริปต์เช่น VBScript หรือ Jscript
2. มีความยืดหยุ่นในการเขียนโปรแกรมมากขึ้น โดยสามารถใช้ภาษาในการเขียนได้มากกว่า 1 ภาษาในไฟล์เดียวกัน จึงทำให้สามารถเลือกรูปแบบในการเขียนภาษาได้ง่ายที่สุดต่อการเขียนโปรแกรมในแต่ละส่วน แต่ผู้พัฒนาโปรแกรมจะต้องเป็นผู้กำหนดให้ชัดเจนว่าส่วนไหนใช้ภาษาอะไรในการเขียน
3. ใช้งานได้ง่าย โดยคอมโพเน็นต์ (Component) จะถูกติดตั้งโดยอัตโนมัติหลังจากที่ผู้พัฒนาโปรแกรมถ่ายโอนข้อมูลไฟล์ไปเก็บไว้ในไดเรกทอรี (Directory) ที่ผู้ดูแลเซิร์ฟเวอร์กำหนด
4. ไม่ขึ้นตรงกับฮาร์ดแวร์ ทั้งนี้เพราะเป็นระบบใน .NET Framework จึงมีคุณสมบัติของ Common Language Runtime (CLR) ทำให้มีการคอมไพล์ (Compile) โปรแกรมเป็นภาษามาตรฐานก่อน
5. แยกส่วนที่เป็น HTML กับ ASP ออกจากกันอย่างชัดเจน

# บทที่ 3

# การวิเคราะห์และออกแบบการทำงานของระบบ

## 3.1 การวิเคราะห์ความต้องการ

จากการศึกษาและทดลองใช้โปรแกรมในการตรวจสอบทราฟฟิกของเครือข่ายที่มีใช้อยู่ทั่วไป ไม่ว่าจะเป็น Netflow ของบริษัท Cisco หรือ NetFlow Traffic Analysis ของบริษัท SolarWinds เป็นต้น ซึ่งแอพพลิเคชันเหล่านี้เป็นที่นิยมใช้กันอย่างกว้างขวางในการนำมาตรวจสอบและวิเคราะห์การใช้งานของเครือข่ายเน็ตเวิร์ก ซึ่งมีฟังก์ชันในการทำงานหลักๆทั่วไปคล้ายคลึงกัน ได้แก่

1. สามารถระบุเครื่องคอมพิวเตอร์ต้นทางและปลายทางของการติดต่อสื่อสารในระบบเครือข่ายได้
2. สามารถระบุพอร์ตของแอพพลิเคชันที่ใช้ในการเชื่อมต่อได้ เพราะให้ผู้ดูแลระบบสามารถตรวจสอบได้ง่าย
3. สามารถสร้างรายงานและแสดงให้อยู่ในรูปแบบที่ดูง่าย เช่นกราฟในรูปแบบต่างๆได้
4. ติดตั้งง่าย ไม่ยุ่งยากในการทำงานของผู้ดูแลระบบ
5. ไม่ก่อให้เกิดการใช้ย่านความถี่เพิ่มขึ้นมาจากเดิมมากนัก

อย่างไรก็ตาม แอพพลิเคชันเหล่านี้ผู้ใช้งานจำเป็นต้องทำการซื้อลิขสิทธิ์ (License) จากผู้ผลิตมาก่อนที่จะทำการติดตั้งในระบบภายในขององค์กรนั้นๆ ซึ่งค่าลิขสิทธิ์ของแอพพลิเคชันเหล่านี้ ส่วนใหญ่จะคิดตามจำนวนผู้ใช้งาน หรือคิดตามย่านความถี่ของข้อมูลที่ต้องการที่จะตรวจสอบ ซึ่งทำให้บางองค์กรไม่สามารถจัดหาแอพพลิเคชันเหล่านี้มาใช้งานได้ นอกจากนั้นในส่วนของ NetFlow ของ Cisco เอง ตัวอุปกรณ์เน็ตเวิร์คยังจะต้องเป็นเราท์เตอร์ หรือสวิชต์ของ Cisco เอง และยังต้องสนับสนุนต่อคุณสมบัติ (Feature) ของ NetFlow อีกด้วย ซึ่งพบว่าในองค์กรที่มีขนาดเล็ก หรือองค์กรที่ใช้อุปกรณ์รุ่นเดิมอยู่หรือไม่ได้ใช้อุปกรณ์ของ Cisco ก็จะไม่สนับสนุนคุณสมบัติดังกล่าว

ดังนั้นการที่องค์กรสามารถพัฒนาแอพพลิเคชันที่มีคุณสมบัติใกล้เคียงกับแอพพลิเคชันที่มีขายตามท้องตลาด จึงช่วยให้องค์กรสามารถลดงบประมาณที่จะต้องจ่ายออกไปได้ด้วย รวมทั้งการพัฒนาแอพพลิเคชันเอง ยังมีความยืดหยุ่นในแง่ของการเพิ่มหรือลดฟังก์ชันที่ผู้ดูแลระบบต้องการได้ ตามความเหมาะสม

## 3.2 โครงสร้างของระบบ

การทำงานของระบบตรวจสอบทราฟฟิกของเครือข่ายจะมีบุคคลที่เกี่ยวข้องด้วยกัน 2 ส่วน ได้แก่ผู้จัดการแผนก และผู้ดูแลระบบเครือข่าย โดยระบบจะได้รับข้อมูลของทราฟฟิกจากสวิตช์ที่มีการเชื่อมต่อกันบนเครือข่ายระยะไกลก่อน และนำข้อมูลนี้มาแปลงและจัดเก็บให้อยู่ในรูปแบบของฐานข้อมูล ซึ่งเมื่อผู้ที่เกี่ยวข้องต้องการที่จะตรวจสอบสถานณะการใช้งานของย่ายความถี่บนเครือข่ายระยะไกล ก็จะเข้าไปดูได้จากหน้าเว็บบราวเซอร์ของระบบ ซึ่งจะสามารถแสดงค่าออกมาเป็นค่าตัวอักษร หรือกราฟในรูปแบบต่างๆที่ง่ายต่อการตรวจสอบ การพัฒนาระบบตรวจสอบทราฟฟิกนี้ได้กำหนดรูปแบบโครงสร้างของระบบไว้ดังนี้

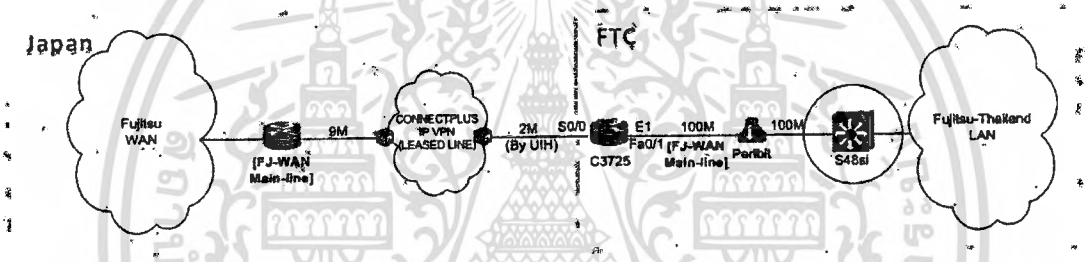
1. ส่วนที่ทำงานบนเซิร์ฟเวอร์ เป็นส่วนที่ใช้ในการติดต่อกับตัวอุปกรณ์เน็ตเวิร์คในเครือข่ายเพื่อรับข้อมูลของทราฟฟิกมา โดยตัวอุปกรณ์เน็ตเวิร์คในที่นี้จะใช้สวิตช์ที่มีการใช้โพรโตคอล SYSLOG ในการส่งข้อมูล ตัวเซิร์ฟเวอร์เมื่อรับข้อมูลมาโดยมีการใช้แอพพลเคชันที่ทำหน้าที่เป็น Syslog server หรือเรียกอีกชื่อหนึ่งว่า Syslog Daemon เพื่อรับ เก็บข้อมูลที่ได้มาและบันทึกล็อกลงในตัวเซิร์ฟเวอร์ในรูปแบบของเท็กซ์ หลังจากนั้นจะมีตัวแอพพลเคชันที่พัฒนาขึ้นมาโดยใช้ภาษา ASP.NET ทำการดึงข้อมูลล็อกมีเปลี่ยนให้อยู่ในรูปแบบของฐานข้อมูลเพื่อให้ง่ายถ้าหากมีผู้ใช้งานต้องการสืบค้าข้อมูลโดยตรงจากฐานข้อมูลที่มีอยู่ นอกจากนั้นตัวแอพพลิเคชันนี้ยังมีฟังก์ชันที่ใช้เพื่อนำข้อมูลที่ได้จัดเก็บในฐานข้อมูลมาแสดงให้กับผู้ใช้งานโดยผ่านทางเว็บบราวเซอร์อีกด้วย
2. ส่วนที่ทำงานบนไคลเอ็นต์ ในส่วนนี้ผู้ใช้งานเพียงแค่ใช้โปรแกรมเว็บบราวเซอร์ เช่น Internet Explorer เชื่อมต่อไปยัง URL ของตัวระบบตรวจสอบทราฟฟิกของเครือข่าย โดยในการเชื่อมต่อก็จะใช้โพรโตคอล HTTP ติดต่อกันระหว่างเซิร์ฟเวอร์และไคลเอ็นต์ หน้าจอของระบบจะแบ่งเป็นเมนูต่างๆให้ผู้ใช้งานได้เลือกใช้ว่าต้องการที่จะดูข้อมูลของทราฟฟิกในด้านใด เช่นต้องการดูเป็นโพรโตคอลที่ใช้ในการเชื่อมต่อหรือต้องการดูเป็นซับเน็ต (Subnet) ของเครือข่าย นอกจากนั้นหน้าจอยังมีส่วนเฉพาะสำหรับผู้ดูแลระบบจะทำการแก้ไข เพิ่มเติม หรือเปลี่ยนแปลงค่าเช่นค่าโพรโตคอลหรือค่าซับเน็ตได้ โดยเมนูจะต้องมีการใส่ชื่อผู้ใช้งาน และรหัสผ่านที่ถูกต้องตรงกับที่ระบบได้บันทึกไว้เท่านั้นจึงจะสามารถเข้าไปดำเนินการได้

## 3.3 ลักษณะการทำงาน

การทำงานของระบบตรวจสอบทราฟฟิกของเครือข่ายระยะไกลนี้ใช้เทคโนโลยีต่างๆ ผ่านทางการทำงานของไคลเอ็นต์และเซิร์ฟเวอร์ในการพัฒนาเพื่อช่วยให้ระบบทำงานได้อย่างมีประสิทธิภาพ ซึ่งโดยการทำงานของระบบสามารถแบ่งออกได้เป็น 3 ส่วนหลักๆด้วยกันคือ

3.3.1. ส่วนอุปกรณ์เน็ตเวิร์ค

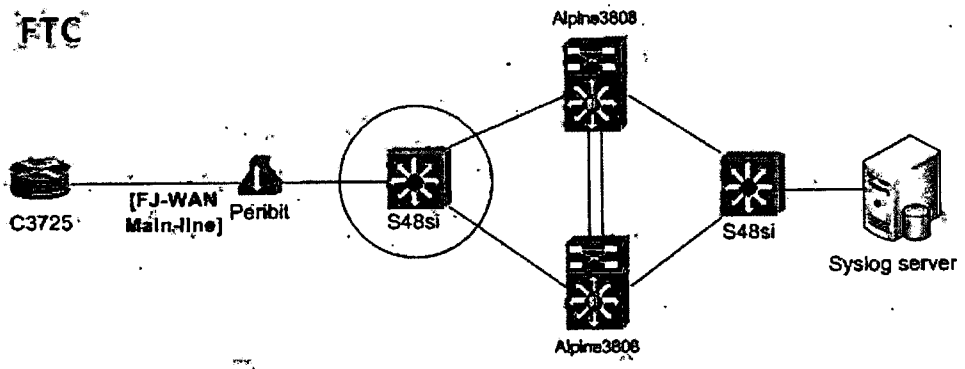
เนื่องจากการพัฒนาระบบตรวจสอบทราฟฟิกของเครือข่ายระยะไกลนี้ได้พัฒนาอยู่บนเครือข่ายเน็ตเวิร์คของบริษัทฟูจิตสึซึ่งมีการเชื่อมต่อระบบเครือข่ายภายในจากประเทศไทยไปยังประเทศญี่ปุ่นโดยผ่านทาง Leased line ซึ่งผู้ดูแลระบบของบริษัทในประเทศไทยจะสามารถควบคุมและตรวจสอบอุปกรณ์ได้จากสวิตซ์ที่เชื่อมต่อกับเราเตอร์หลักเท่านั้น ดังนั้นข้อมูลการติดต่อสื่อสารของเครือข่ายระยะไกลที่ได้ทั้งหมดจะได้รับจากตัวสวิตซ์นี้ ดังรูปที่ 3.1




**รูปที่ 3.1** การเชื่อมต่ออุปกรณ์เน็ตเวิร์คขององค์กรในส่วนที่เชื่อมต่อกับเครือข่ายระยะไกล

3.3.2. ส่วนดำเนินการจัดการ (ส่วนเซิร์ฟเวอร์)

จากรูปที่ 3.2 เครื่องเซิร์ฟเวอร์จะติดตั้งไว้อยู่ในระบบเครือข่ายภายในของบริษัท ซึ่งตัวสวิตซ์ที่ได้ทำการติดตั้งโพรโตคอล SYSLOG ที่ได้กล่าวมาแล้วในข้อ 1 จะเป็นตัวส่งล็อกทั้งหมดของการติดต่อสื่อสารระหว่างเครือข่ายมายังตัวเซิร์ฟเวอร์นี้ โดยที่ตัวเซิร์ฟเวอร์จะทำการติดตั้งแอพพลิเคชัน Kiwi Syslog Daemon ซึ่งใช้เป็น Syslog server เพื่อทำการรับล็อกที่ส่งมาและบันทึกลงในตัวไดเรกทอรีของเซิร์ฟเวอร์ตามที่ได้คอนฟิกูเรชันไว้

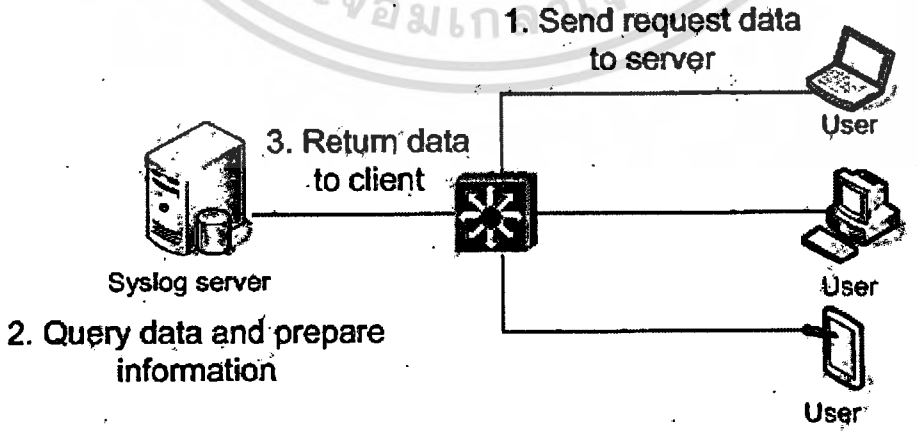



**รูปที่ 3.2** การเชื่อมต่อของ Syslog server ภายในเครือข่ายภายในองค์กร

นอกจากนี้ เซิร์ฟเวอร์เองยังมีแอพพลิเคชันที่ทำงานเพื่อใช้ในการรีจีสเตอร์ (Register) ข้อมูลจากที่อยู่ในรูปแบบเท็กซ์ไฟล์ให้อยู่ในรูปแบบของฐานข้อมูลโดยใช้แอพพลิเคชันออราเคิล (Oracle) ซึ่งเป็นระบบจัดการฐานข้อมูลเชิงสัมพันธ์ (Relational Database Management System : RDBMS) เป็นตัวควบคุมอีกทีหนึ่ง แอพพลิเคชันที่ใช้รีจีสเตอร์ข้อมูลจะทำงานแบบวงลูป (Loop) เป็นรอบการทำงานทุกๆ 2 ชั่วโมง

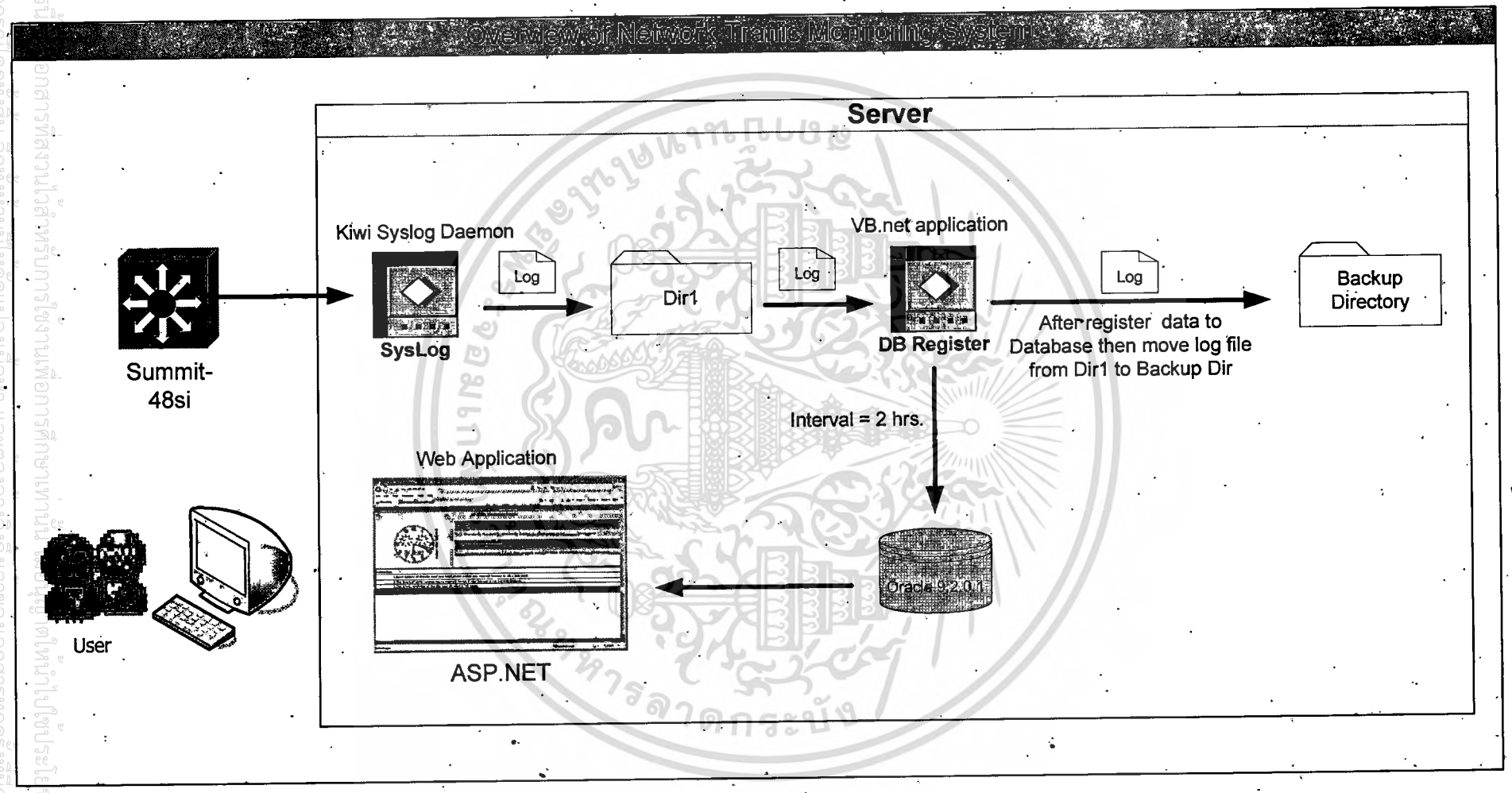
3.3.3. ส่วนผู้ใช้งานระบบ

สำหรับผู้ใช้งานระบบตรวจสอบทราฟฟิกของเครือข่ายระยะไกลนั้นจะสามารถเข้าดูข้อมูลได้โดยผ่านทางเว็บบราวเซอร์ เช่น Microsoft Internet Explorer โดยการทำงานจะอ้างอิงหลักการของไคลเอ็นต์เซิร์ฟเวอร์ คือเมื่อผู้ใช้งานมีกระบวนการเรียกดูข้อมูลใดๆของระบบ จะทำการส่งข้อมูลเพื่อร้องขอไปยังเซิร์ฟเวอร์ เมื่อเซิร์ฟเวอร์ได้รับคำร้องขอแล้ว จะประมวลผลและส่งผลลัพธ์ที่ได้กลับมายังตัวไคลเอ็นต์หรือเครื่องของผู้ใช้งานอีกทีหนึ่ง ดังรูปที่ 3.3




**รูปที่ 3.3** ขั้นตอนในการดำเนินการจากฝั่งไคลเอ็นต์

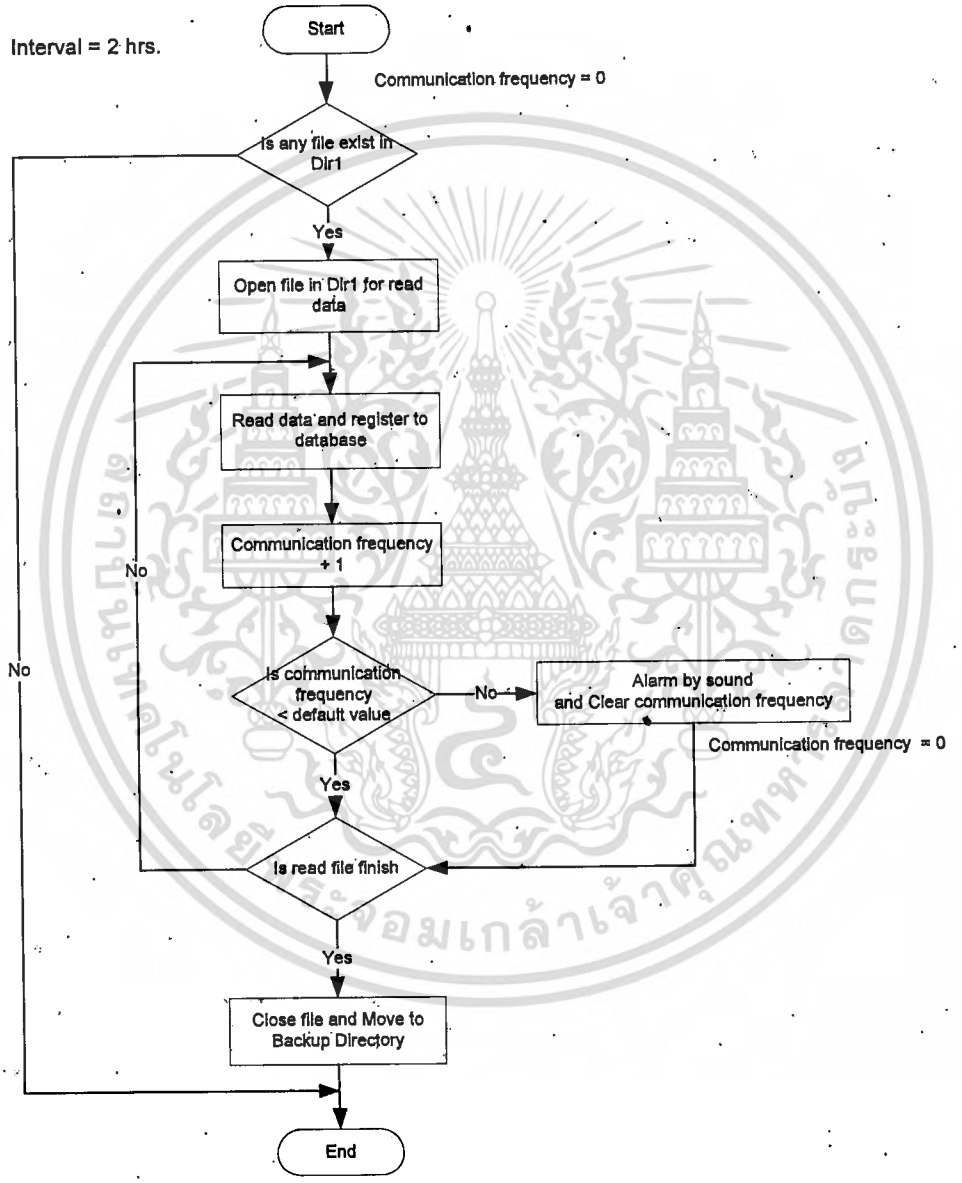
ดังนั้น เมื่อนำทั้ง 3 ส่วนมาประกอบกัน จะสามารถแสดงภาพโดยรวมของระบบตรวจสอบทราฟฟิกของเครือข่ายสำหรับข้อมูลที่ถูกส่งผ่านบนเครือข่ายระยะไกลได้ดังรูปที่ 3.4




รูปที่ 3.4 ภาพระบบโดยรวม

## 3.4 แผนภาพแสดง Flowchart ของการรีจีสเตอร์ข้อมูล

แอพพลิเคชัน FJ-WAN Database Builder เป็นแอพพลิเคชันที่ทำการนำเท็กซ์ไฟล์ที่ได้รับมาจากแอพพลิเคชัน Kiwi Syslog Daemon มาเปลี่ยนรูปแบบให้เก็บอยู่ในฐานข้อมูลโดยใช้ Oracle เป็น DBMS ซึ่งในการทำงานจะมี Flowchart ดังรูปที่ 3.5



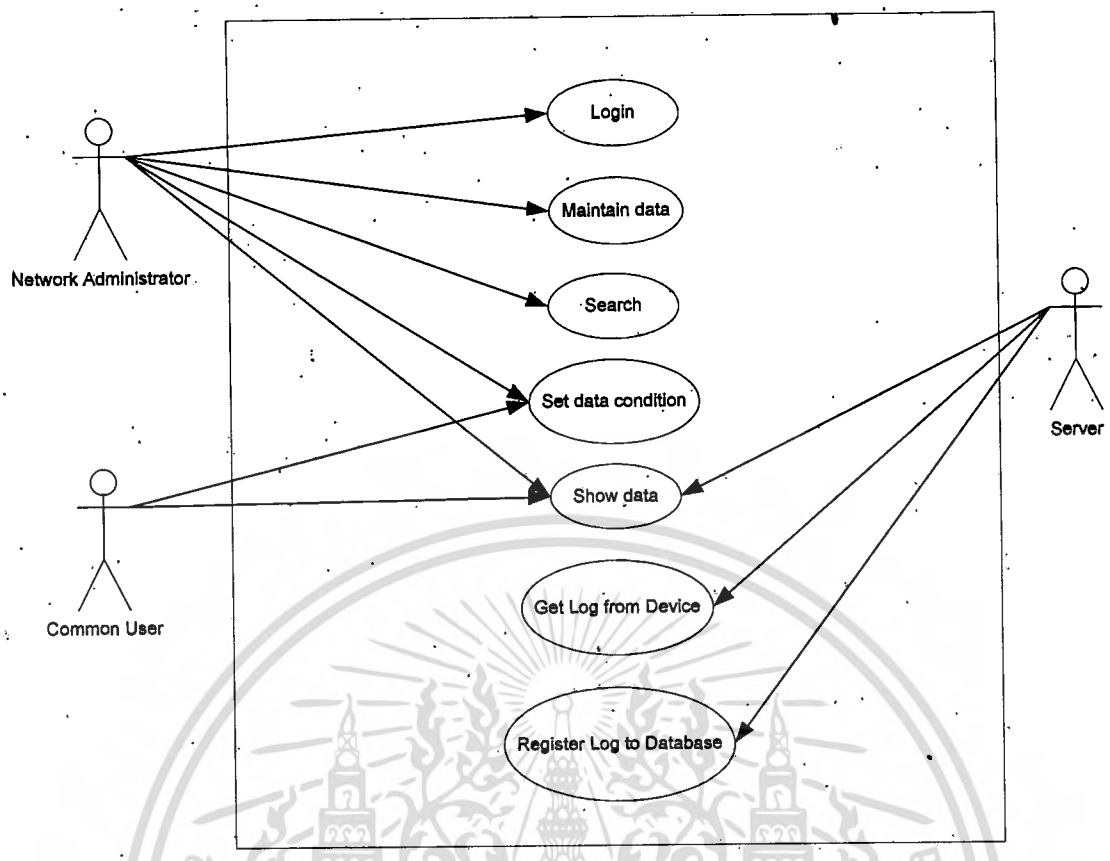

**รูปที่ 3.5** Flowchart การรีจีสเตอร์ข้อมูลลงฐานข้อมูล

ขั้นตอนการนำข้อมูลที่ได้จัดเก็บในรูปเท็กซ์ไฟล์ของแอพพลิเคชัน Kiwi Syslog Daemon มารีจีสเตอร์ลงในฐานข้อมูลนั้น มีขั้นตอนด้วยกันดังนี้

1. ตรวจสอบว่าในไดเรกทอรีที่ Kiwi Syslog Daemon นำข้อมูลล็อกจากสวิตซ์มาเก็บ มีเท็กซ์ไฟล์อยู่หรือไม่โดยจะทำการตรวจสอบทุกๆ 2 ชั่วโมง
2. หากไม่มี แอพพลิเคชันจะจบการทำงาน และรอรอบการตรวจสอบครั้งถัดไป ถ้าหากมีเท็กซ์ไฟล์อยู่ แอพพลิเคชันจะทำการเปิดและอ่านข้อมูลในเท็กซ์ไฟล์ โดยจะทำการรีจีสเตอร์ข้อมูลจากรูปแบบของเท็กซ์ไฟล์ไปเป็นรูปแบบของฐานข้อมูล
3. ในขณะที่ข้อมูลในเท็กซ์ไฟล์ยังไม่หมด โปรแกรม FJ-WAN Database Builder จะทำการรีจีสเตอร์ข้อมูลไปเรื่อยๆจนกว่าจะครบทุกบรรทัดในเท็กซ์ไฟล์
4. แอพพลิเคชันปิดเท็กซ์ไฟล์ที่เปิดขึ้นมาอ่านข้อมูล และทำการย้ายพาธที่ใช้ในการเก็บไฟล์จากไดเรกทอรีปัจจุบันไปยังไดเรกทอรีที่ใช้เพื่อสำรองข้อมูลเก่าเก็บไว้
5. จบการทำงานของแอพพลิเคชัน โดยแอพพลิเคชันจะรอการทำงานในรอบการทำงานถัดไป

## 3.5 แผนภาพแสดง Use Case Diagram

การอธิบายถึงการทำงานของระบบโดยรวมสามารถอธิบายได้จากการสร้างแผนภาพ ซึ่งจะบอกถึงบุคคลที่เกี่ยวข้องกับการทำงานของกิจกรรมนั้นๆทั้งหมด รูปที่ 3.6 แสดงถึงแผนภาพ Use Case ของระบบ




**รูปที่ 3.6** แผนภาพ Use Case Diagram ของระบบ

ระบบจะมีองค์ประกอบดังนี้ คือ

1. Actors แสดงถึงผู้ที่มีส่วนเกี่ยวข้องกับระบบ ได้แก่
   - Network Administrator ผู้ดูแลระบบเครือข่าย
   - Common User ผู้ใช้งานทั่วไปที่ต้องการเข้าดูข้อมูลของระบบ
   - Server ส่วนที่รับข้อมูลล็อกจากอุปกรณ์เน็ตเวิร์ค ทำการรีจีสเตอร์ข้อมูลลงฐานข้อมูล และส่งผลกลับไปยังผู้ใช้งาน
2. Process แสดงถึงกระบวนการในการทำงานหลักภายในระบบ โดยมีการทำงานต่างๆ ดังนี้
   - Login เป็นกระบวนการตรวจสอบสิทธิในการเข้าใช้งานของระบบเพื่อที่จะทำการบำรุงรักษาข้อมูล ซึ่งสิทธิในการเข้าแก้ไขนี้จะอนุญาตให้เพียงผู้ดูแลระบบเครือข่ายเท่านั้น
   - Maintain data เป็นกระบวนการในการแก้ไข เปลี่ยนแปลงข้อมูลหลักของระบบ ผู้ที่จะใช้กระบวนการนี้ได้จะต้องผ่านกระบวนการ Login มาก่อนเท่านั้น

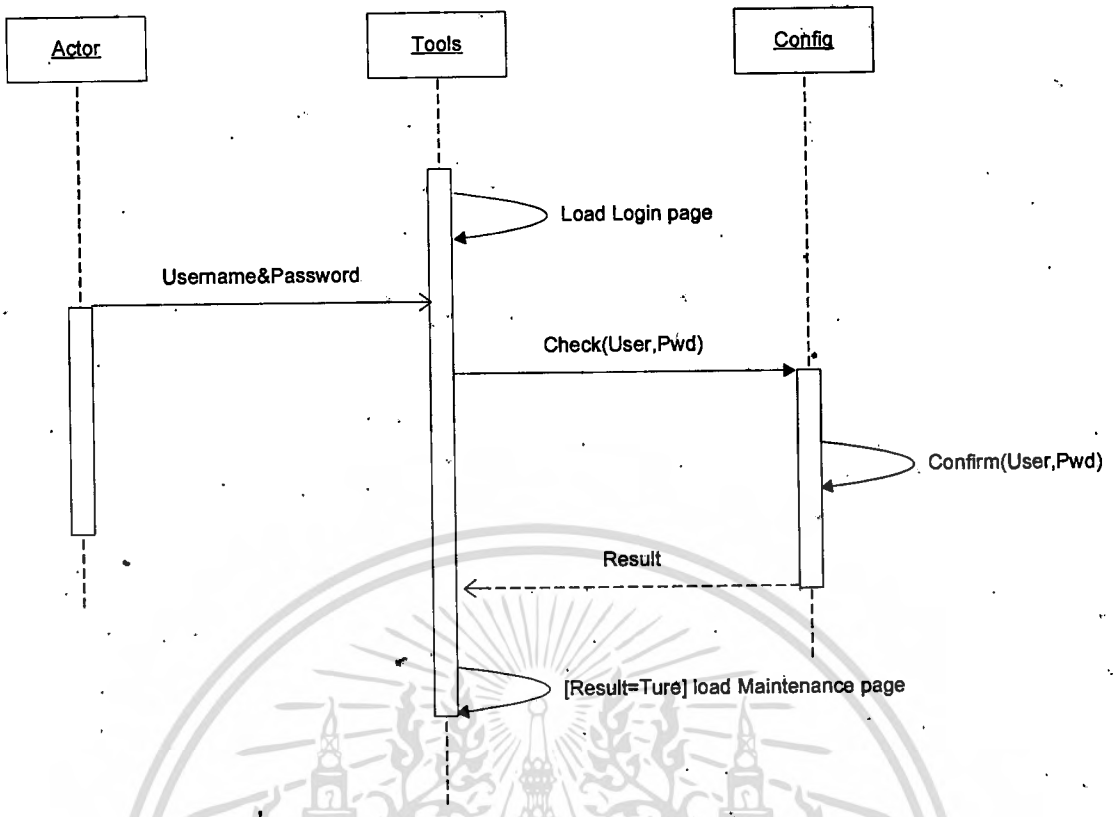
- Search กระบวนการค้นหาข้อมูลหลักของระบบ ผู้ที่ทำการค้นหาได้จะต้องมีสิทธิเข้าถึงระบบก่อนเท่านั้น
- Set data condition กระบวนการกำหนดเงื่อนไขของข้อมูลที่ต้องการจะตรวจสอบหรือให้แสดงผลบนหน้าจอ
- Show data กระบวนการในการแสดงรายละเอียดของทราฟฟิกที่ตรวจสอบได้จากเงื่อนไขที่กำหนด
- Get Log from Device กระบวนการรับล็อกไฟล์ที่ถูกส่งมาจากอุปกรณ์ระบบเครือข่ายและทำการจัดเก็บลงในระบบ
- Register Log to Database กระบวนการนำล็อกมารีจีสเตอร์ลงในฐานข้อมูล

## 3.6 แผนภาพแสดง Sequence Diagram

การแสดงการทำงานของระบบที่มีการบอกรายละเอียดที่เกิดขึ้นภายในระบบ รวมทั้งอธิบายถึงผู้ที่เข้ามาใช้งานในระบบหรือผู้ที่มีส่วนเกี่ยวข้องกับระบบว่าต้องมีขั้นตอนการทำงานในลักษณะต่างๆอย่างไรบ้าง ซึ่งสามารถอธิบายโดยใช้แผนภาพ Sequence Diagram ได้

### 3.6.1. แผนภาพแสดง Sequence Diagram ของการ Login

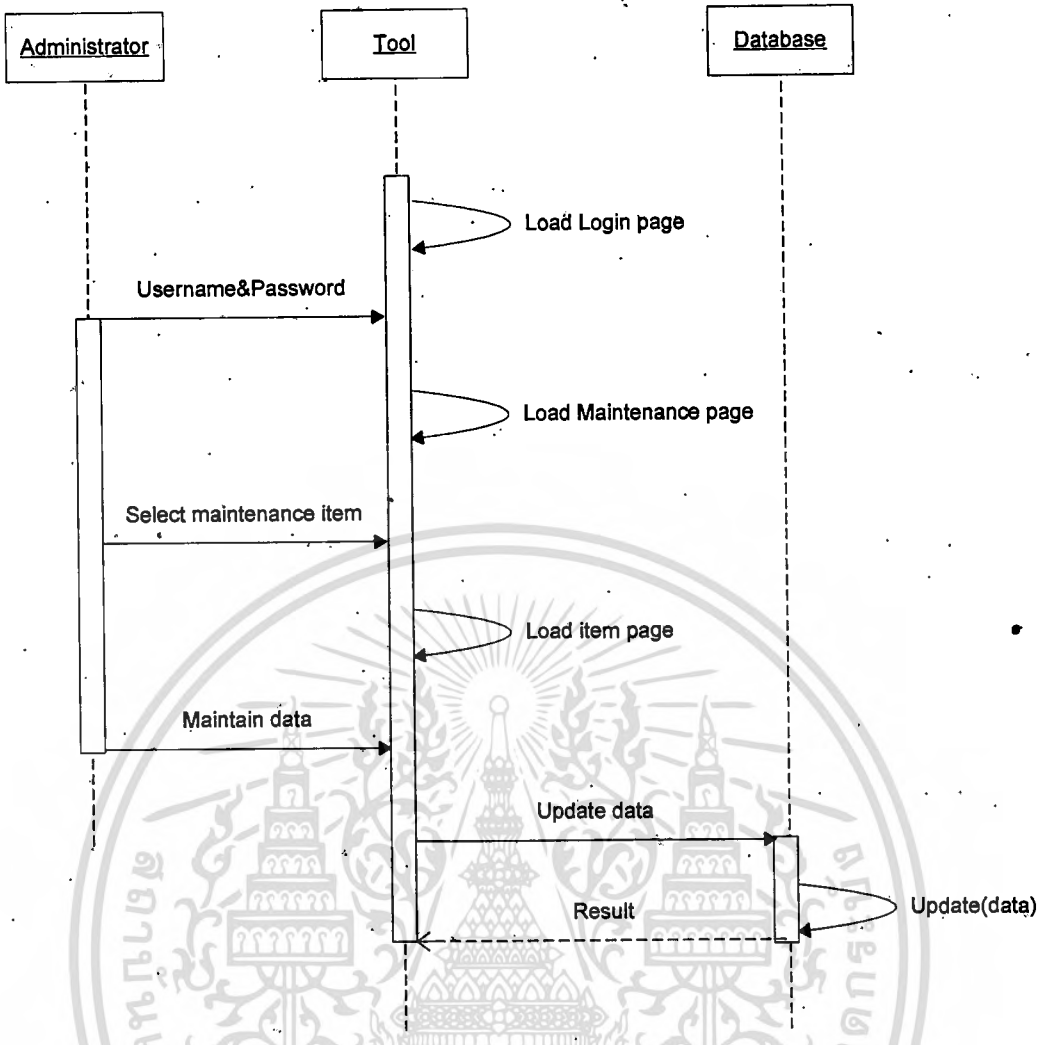
กระบวนการทำงานของการ Login เพื่อเป็นการตรวจสอบสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบ โดยระบบจะแบ่งผู้ใช้งานเป็น 2 ประเภทคือผู้ใช้งานทั่วไป ซึ่งไม่จำเป็นต้องมีสิทธิ์ในการ Login สามารถเข้าดูข้อมูลของระบบได้จากหน้าเว็บ ผู้ใช้งานระบบอีกประเภทได้แก่ผู้ดูแลระบบเครือข่าย ซึ่งผู้ใช้งานกลุ่มนี้จะสามารถเข้าไปแก้ไข เปลี่ยนแปลงค่าของระบบได้ โดยเมื่อผู้ดูแลระบบต้องการเปลี่ยนแปลงแก้ไขค่า จะต้องกรอกข้อมูลชื่อผู้ใช้และรหัสผ่านให้ถูกต้องก่อน ซึ่งถ้าหากใส่ข้อมูลถูกต้องตามที่ระบบได้ตรวจสอบกับค่าคอนฟิกูเรชัน ผู้ดูแลระบบถึงจะสามารถดำเนินการต่อได้ ดังรูปที่ 3.7




**รูปที่ 3.7** แผนภาพ Sequence Diagram ของกระบวนการ Login

3.6.2. แผนภาพแสดง Sequence Diagram ของการ Maintain data

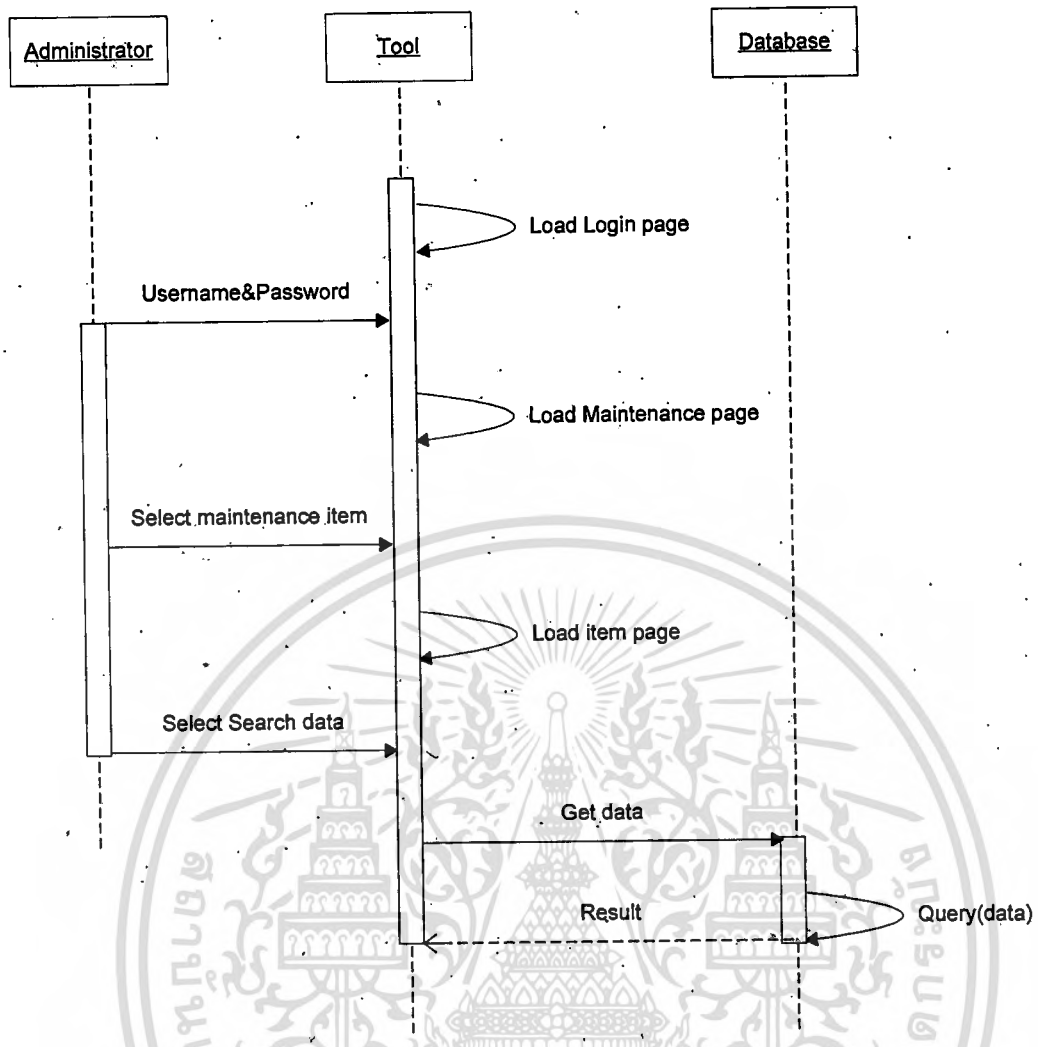
กระบวนการ Maintenance data เป็นการแก้ไขเปลี่ยนแปลงข้อมูลที่มีอยู่ของระบบ โดยจะเป็นกระบวนการต่อจากการ Login ซึ่งการแก้ไขเปลี่ยนแปลงข้อมูลนั้น จะประกอบด้วย 2 ส่วนคือ ข้อมูลและรายละเอียดของพอร์ตที่ใช้ในการติดต่อสื่อสารภายในระบบเครือข่าย และข้อมูลซับเน็ตที่องค์กรใช้งานอยู่ โดยการแก้ไขเปลี่ยนแปลงนั้นจะรวมถึงการเพิ่ม การลด และการแก้ไขค่าต่างๆ ดังรูปที่ 3.8




**รูปที่ 3.8** แผนภาพ Sequence Diagram ของกระบวนการ Maintain data

3.6.3. แผนภาพแสดง Sequence Diagram ของการ Search

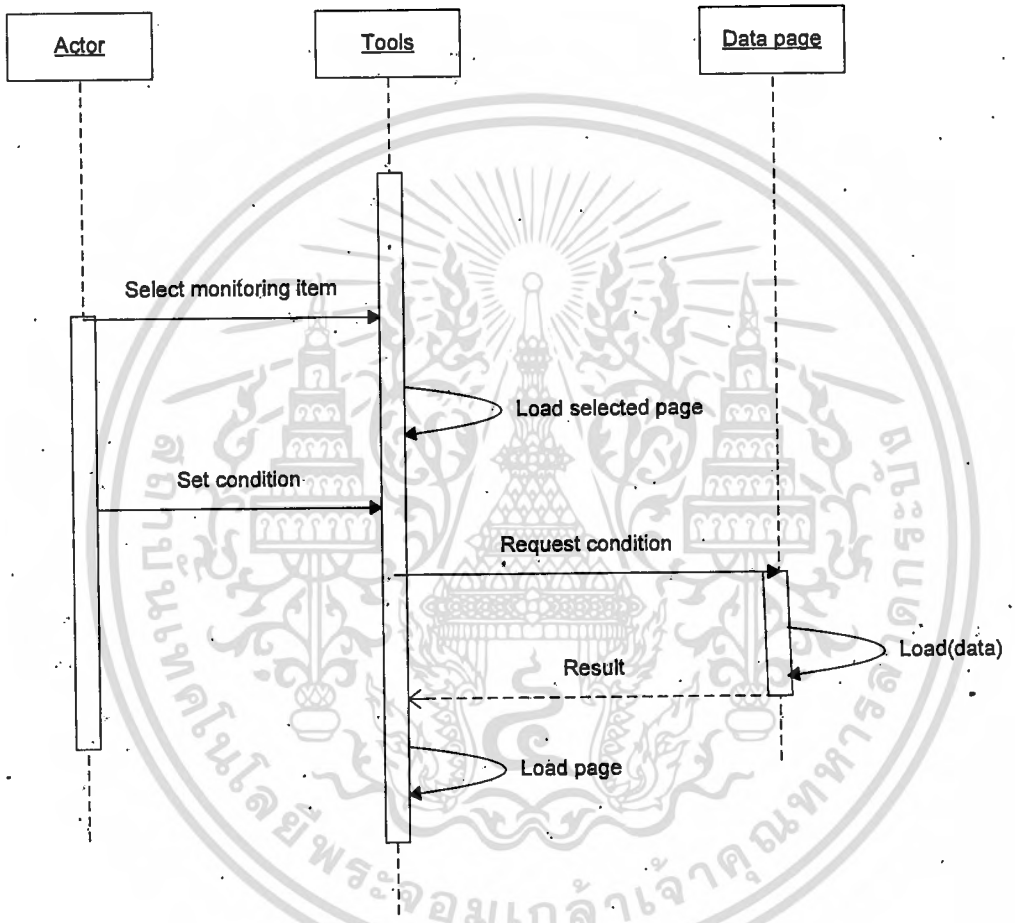
กระบวนการ Search เป็นการค้นหาข้อมูลที่มีอยู่ของระบบ โดยจะเป็นกระบวนการต่อจากการ Login ซึ่งการค้นหาข้อมูลนั้น จะประกอบด้วย 2 ส่วนคือข้อมูลและรายละเอียดของพอร์ตที่ใช้ในการติดต่อสื่อสารภายในระบบเครือข่าย และข้อมูลซับเน็ตที่องค์กรใช้งานอยู่ แผนภาพแสดงการค้นหาข้อมูลสามารถแสดงได้ดังรูปที่ 3.9




**รูปที่ 3.9** แผนภาพ Sequence Diagram ของกระบวนการ Search

3.6.4. แผนภาพแสดง Sequence Diagram ของการ Set data condition

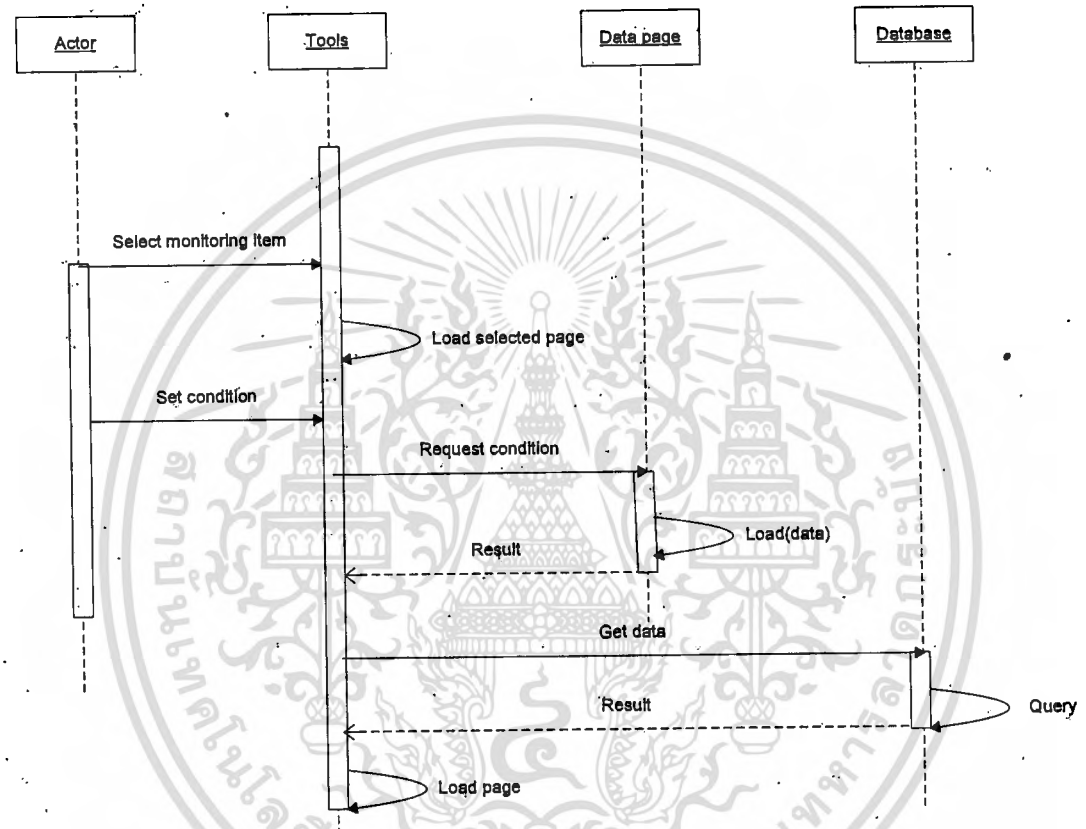
กระบวนการ Set data condition เป็นการกำหนดเงื่อนไขเบื้องต้นของข้อมูลที่ผู้ใช้งานต้องการจะให้ระบบแสดงผลออกมา เช่นต้องการให้ลักษณะของกราฟออกมาในรูปแบบใด มีการแสดงข้อมูลเพิ่มเติมบนกราฟหรือไม่ เป็นต้น แผนภาพแสดงการตั้งค่าเบื้องต้นเพื่อใช้ในการแสดงผลสามารถแสดงได้ดังรูปที่ 3.10




**รูปที่ 3.10** แผนภาพ Sequence Diagram ของกระบวนการ Set data condition

3.6.5. แผนภาพแสดง Sequence Diagram ของการ Show data

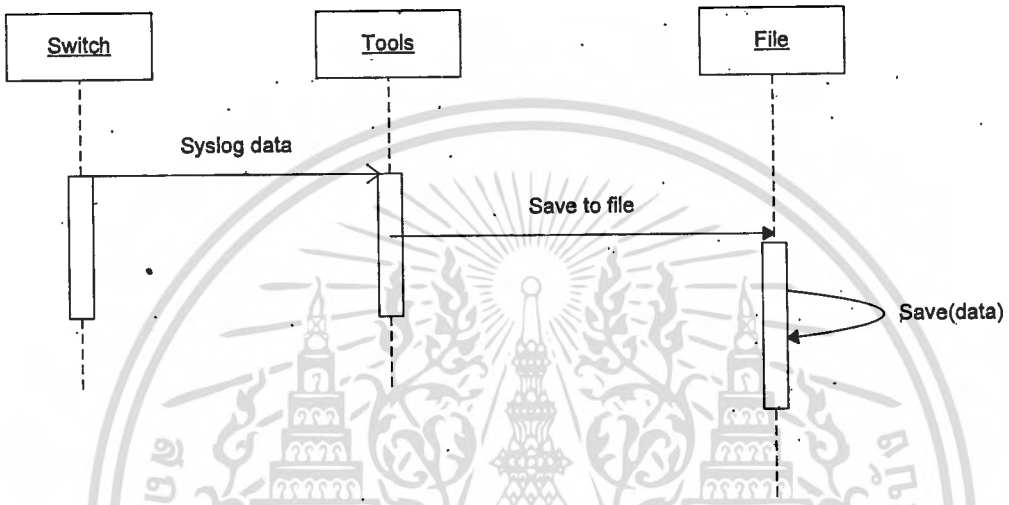
กระบวนการ Show data เป็นการแสดงข้อมูลของทราฟฟิกที่ใช้ไปตามเงื่อนไขที่ได้กำหนดในการแสดงตามกระบวนการ Set data condition ซึ่งจะต้องมีการติดต่อกับฐานข้อมูลเพื่อคิวรี (Query) ข้อมูลออกมาด้วย แผนภาพแสดงการแสดงผลของระบบสามารถแสดงได้ดังรูปที่ 3.11




**รูปที่ 3.11** แผนภาพ Sequence Diagram ของกระบวนการ Show data

3.6.6. แผนภาพแสดง Sequence Diagram ของการ Get Log from Device

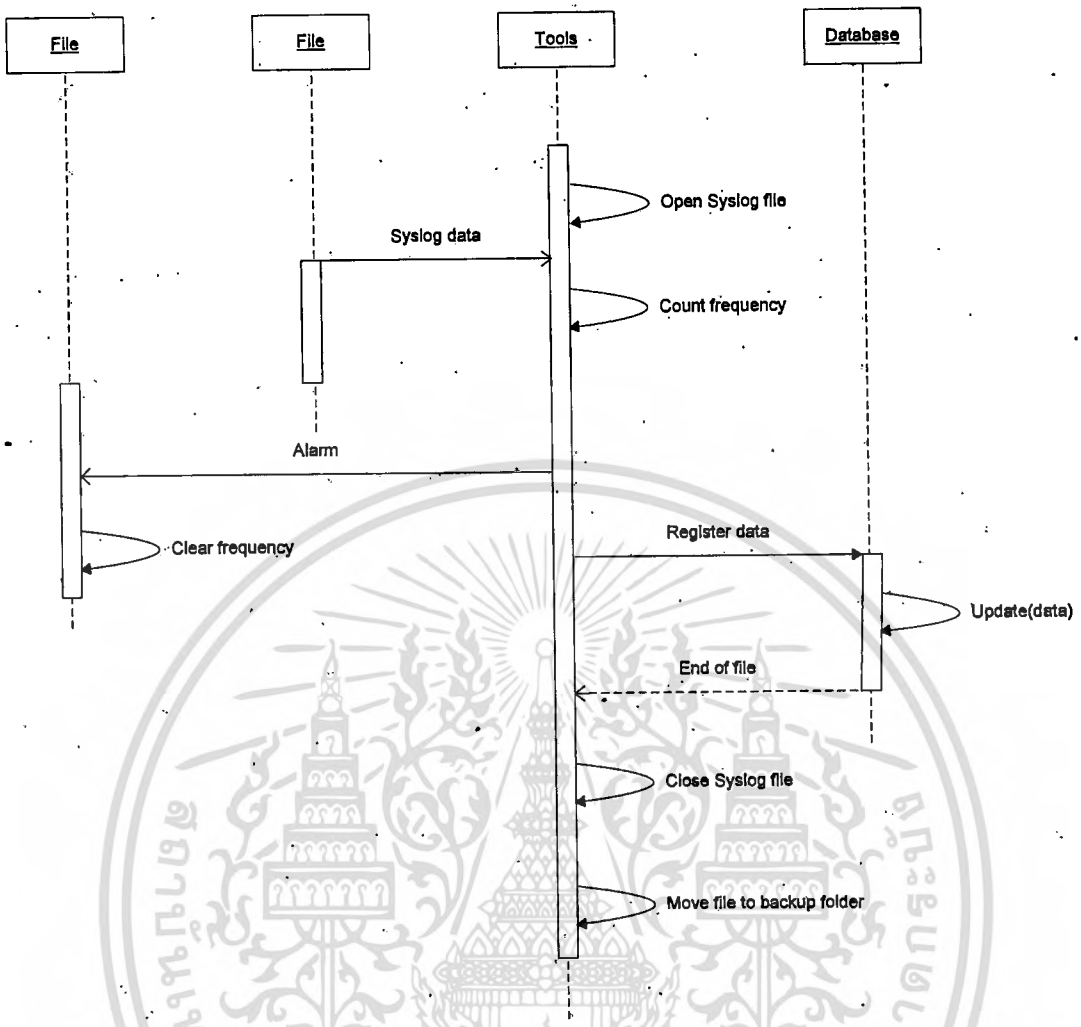
กระบวนการ Get Log from Device เป็นกระบวนการที่แอพพลิเคชันที่ตัวเซิร์ฟเวอร์ได้รับล็อกไฟล์จากสวิตซ์ซึ่งเป็นอุปกรณ์เน็ตเวิร์คมา และทำการบันทึกลงในเครื่องในรูปแบบของเท็กซ์ไฟล์ โดยมีการแยกเก็บไฟล์ของแต่ละชั่วโมงเพื่อง่ายในกระบวนการต่อไป แผนภาพแสดงการการรับล็อกไฟล์มาเก็บในระบบสามารถแสดงได้ดังรูปที่ 3.12




**รูปที่ 3.12** แผนภาพ Sequence Diagram ของกระบวนการ Get Log from Device

3.6.7. แผนภาพแสดง Sequence Diagram ของการ Register Log to Database

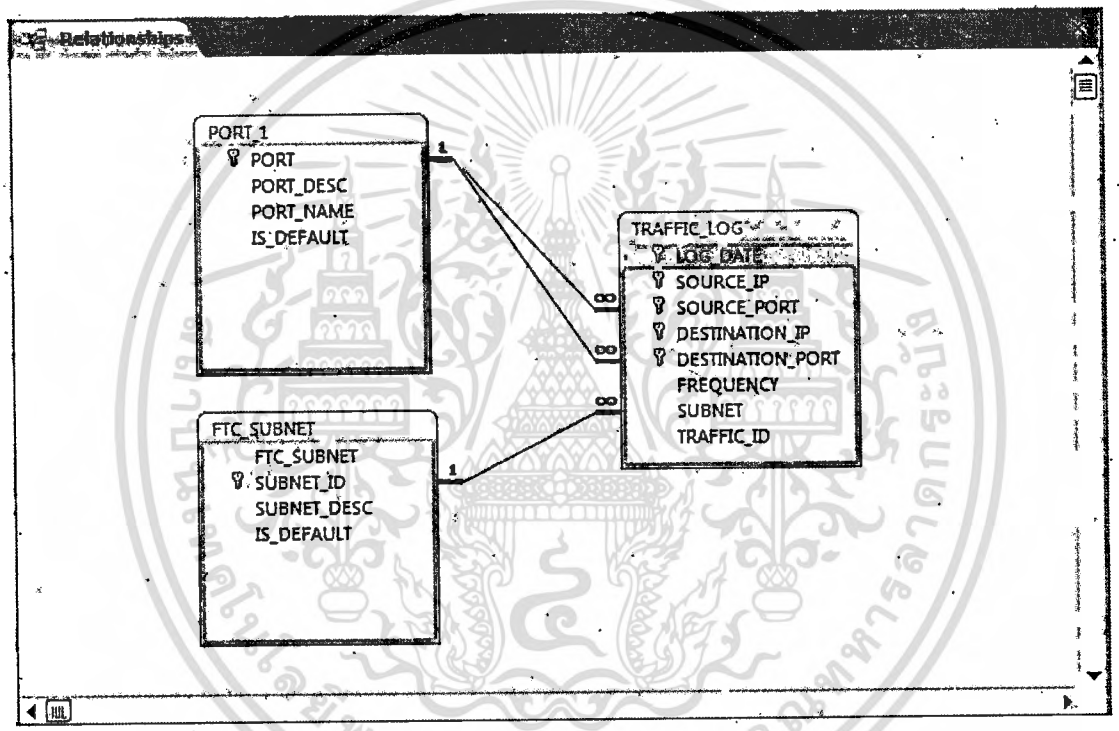
กระบวนการ Register Log to Database เป็นกระบวนการที่แอพพลิเคชันที่ตัวเซิร์ฟเวอร์ทำการเปิดข้อมูลล็อกที่อยู่ในรูปเท็กซไฟล์ นำมาอ่านแล้วรีจีสเตอร์ค่านั้นเข้าสู่ฐานข้อมูล โดยเมื่อรีจีสเตอร์ค่าที่อยู่ภายในเท็กซ์ไฟล์นั้นๆเรียบร้อยแล้ว จะทำการย้ายไดเรกทอรีในการเก็บไปไว้ยัง Backup folder แผนภาพแสดงการการรีจีสเตอร์ข้อมูลลงฐานข้อมูลสามารถแสดงได้ดังรูปที่ 3.13




**รูปที่ 3.13** แผนภาพ Sequence Diagram ของกระบวนการ Register Log to Database

## 3.7 การออกแบบฐานข้อมูล

การออกแบบฐานข้อมูลเป็นการแสดงถึงโครงสร้างความสัมพันธ์ระหว่างข้อมูลที่มีอยู่ในระบบ โดยจะต้องออกแบบให้มีการเก็บข้อมูลแยกเป็นส่วนๆตามคุณสมบัติหรือความสัมพันธ์เกี่ยวข้องกันของข้อมูล ตามหลักการของการออกแบบฐานข้อมูลเชิงสัมพันธ์ เพื่อให้สะดวกในการนำข้อมูลมาประมวลผล และง่ายต่อการจัดเก็บ และจัดการของฐานข้อมูล ซึ่งหลังจากที่ทำการวิเคราะห์การทำงานของระบบโดยใช้ User Case diagram ควบคู่กับ Sequence diagram แล้ว สามารถออกแบบระบบฐานข้อมูลได้ดังรูปที่ 3.14




**รูปที่ 3.14** ความสัมพันธ์ของข้อมูลของระบบตรวจสอบทราฟฟิกของเครือข่ายระยะไกล

จากความสัมพันธ์ข้างต้นสามารถแบ่งตารางออกเป็น 3 ตารางด้วยกันดังนี้

3.7.1. ตาราง PORT

ตารางเก็บรายละเอียดของพอร์ตที่ใช้ในการติดต่อสื่อสาร รวมทั้งคำอธิบายและชื่อโพรโตคอลที่ใช้ในการเรียกพอร์ตนั้นๆ

**ตารางที่ 3.1** ตาราง PORT เก็บข้อมูลของพอร์ตที่ใช้ในการติดต่อสื่อสาร

| ชื่อ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตารางอ้างอิง |
|---|---|---|---|---|
| PORT | หมายเลขพอร์ต | Number | Primary | TRAFFIC_LOG |
| PORT_DESC | คำอธิบายรายละเอียดของพอร์ต | Varchar2 | | |
| PORT_NAME | ชื่อพอร์ต/ชื่อโพรโตคอล | Varchar2 | | |
| IS_DEFAULT | กำหนดเป็นพอร์ตเบื้องต้นในการแสดง | Number | | |

3.7.2. ตาราง FTC_SUBNET

ตารางเก็บรายละเอียดของซับเน็ตและรายละเอียดของซับเน็ตขององค์กรที่ใช้งานอยู่ภายใน

**ตารางที่ 3.2** ตาราง FTC_SUBNET เก็บข้อมูลของซับเน็ตในองค์กร

| ชื่อ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตารางอ้างอิง |
|---|---|---|---|---|
| SUBNET | ค่าของซับเน็ต | Varchar2 | | |
| SUBNET_ID | หมายเลขอ้างอิงซับเน็ต | Number | Primary | TRAFFIC_LOG |
| SUBNET_DESC | คำอธิบายรายละเอียดของซับเน็ต | Varchar2 | | |
| IS_DEFAULT | กำหนดเป็นซับเน็ตเบื้องต้นในการแสดง | Number | | |

3.7.3. ตาราง TRAFFIC_LOG

ตารางเก็บรายละเอียดของล็อกที่ได้จากสวิตช์ซึ่งส่งมาที่ระบบและได้รับการรีจีสเตอร์ให้อยู่ในรูปของฐานข้อมูล

**ตารางที่ 3.3** ตาราง TRAFFIC_LOG เก็บข้อมูลของการติดต่อสื่อสาร

| ชื่อ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตารางอ้างอิง |
|---|---|---|---|---|
| LOG_DATE | วันที่และเวลาที่ล็อกถูกบันทึก | Date | Primary | |
| SOURCE_IP | ไอพีแอดเดรสของเครื่องคอมพิวเตอร์ต้นทาง | Varchar2 | Primary | |
| SOURCE_PORT | พอร์ตในการสื่อสารของเครื่องคอมพิวเตอร์ต้นทาง | Number | Primary | |
| DESTINATION_IP | ไอพีแอดเดรสของเครื่องคอมพิวเตอร์ปลายทาง | Varchar2 | Primary | |
| DESTINATION_PORT | พอร์ตในการสื่อสารของเครื่องคอมพิวเตอร์ปลายทาง | Number | Primary | |
| FREQUENCY | ความถี่ของการสื่อสารระหว่างเครื่องคอมพิวเตอร์ต้นทางและปลายทาง | Number | | |
| SUBNET | ซับเน็ตของเครื่องคอมพิวเตอร์ | Varchar2 | | |
| TRAFFIC_ID | หมายเลขอ้างอิงการติดต่อ | Number | | |

# บทที่ 4
# การพัฒนาระบบงาน

การพัฒนาระบบตรวจสอบทราฟฟิกของเครือข่ายสำหรับข้อมูลที่ถูกส่งผ่านเครือข่ายระยะไกลนั้นได้แบ่งการพัฒนาออกเป็น 2 ส่วนหลักๆด้วยกัน คือส่วนการแก้ไขเปลี่ยนแปลงคอนฟิกูเรชันของสวิตซ์เพื่ออีนาเบิล (Enable) ฟังก์ชันโพรโตคอล SYSLOG และกำหนดค่าของ Syslog server (หรือ Syslog Daemon) ว่าให้ล็อกของข้อมูลการติดต่อสื่อสารของสวิตซ์นั้นส่งค่ามาเก็บที่ตัวเซิร์ฟเวอร์ใด และการพัฒนาระบบในส่วนที่ 2 คือการพัฒนาโปรแกรมในการรีจีสเตอร์ล็อกที่ได้มาจากสวิตซ์ซึ่งมีรูปแบบเป็นเท็กซ์ไฟล์ ให้อยู่ในรูปแบบของฐานข้อมูลโดยใช้ออราเคิลเป็น DBMS ในการจัดการฐานข้อมูล แอพพลเคชันนี้พัฒนาโดยใช้โปรแกรมภาษา VB.NET นอกจากนั้นในส่วนของเซิร์ฟเวอร์ยังมีการพัฒนาแอพพลิเคชันในการนำเอาข้อมูลจากฐานข้อมูลมาแสดงในรูปแบบของ HTML โดยใช้ภาษา ASP.NET เป็นเครื่องมือช่วยในการพัฒนา

## 4.1 เครื่องมือที่ใช้ในการพัฒนาระบบ

ระบบตรวจสอบทราฟฟิกบนเครือข่ายระยะไกลนั้น ดังที่ได้กล่าวมาแล้วในบทที่ 3 ว่ามีการแบ่งการทำงานออกเป็น 3 ส่วนหลักๆด้วยกัน ได้แก่

1. ส่วนอุปกรณ์เน็ตเวิร์ค
2. ส่วนดำเนินการจัดการ (ส่วนเซิร์ฟเวอร์)
3. ส่วนผู้ใช้งานระบบ

ซึ่งแต่ละส่วนจะมีเครื่องมือและการดำเนินการติดตั้งดังนี้คือ

### 4.1.1 ส่วนอุปกรณ์เน็ตเวิร์ค

อุปกรณ์เน็ตเวิร์คที่เป็นตัวส่งข้อมูลของล็อกของทราฟฟิกที่ถูกส่งผ่านบนเครือข่ายระยะไกลนั้น ในการพัฒนาระบบนี้จะใช้อุปกรณ์สวิตซ์ เลเยอร์ 2 ยี่ห้อ Extreme รุ่น Summit-48si ซึ่งมีสเปก (Specification) ของอุปกรณ์ดังนี้

- 48 connection port 10/100BASE-TX (P1-P48) and 2 connection port 1000BASE-X SFP (P49-P50)
- Layer 2 and Layer 3 switch
- Hardware based Access Control Lists (ACLs)
- 17.5 Gbps switch fabric

- 128K MAC Address

นอกจากนี้ ตัวสวิตช์ S-48si ยังมีคำสั่งที่ง่ายต่อการคอนฟิกูเรชันอีกด้วย

สำหรับการเชื่อมต่อกับเครือข่ายขององค์กรนั้น จะกำหนดให้พอร์ตหมายเลข 1 เป็นพอร์ตที่ใช้ในการเชื่อมต่อกับเราเตอร์หลักขององค์กรเพื่อต่อออกไปยังระบบเครือข่ายระยะไกลขององค์กรอีกทอดหนึ่ง ส่วนพอร์ตหมายเลข 49 และพอร์ตหมายเลข 50 ซึ่งเป็นพอร์ตที่ต้องเชื่อมต่อด้วยสายไฟเบอร์ออปติก (Fiber optic) จะเป็นพอร์ตที่เชื่อมต่อไปยังเราเตอร์ภายในองค์กรเองอีกทีหนึ่ง ซึ่งเราเตอร์ตัวนี้จะทำหน้าที่เราต์ (Route) เส้นของของเครือข่ายภายในบริษัทเท่านั้น

ในการคอฟิกูเรชันสวิตช์เพื่อให้สามารถส่งล็อกมายังตัว Syslog server ได้นั้น จะมีคำสั่งที่เกี่ยวข้องด้วยกัน คือ

- การอีนาเบิลโพรโตคอล SYSLOG
- การกำหนดหมายเลขไอพีแอดเดรสของ Syslog server เพื่อให้สวิตช์รู้ปลายทางที่จะต้องส่งล็อกไป โดยในส่วนนี้จะรวมถึงการกำหนดรูปแบบของข้อความล็อกที่จะส่งไปยังตัวเซิร์ฟเวอร์

รูปที่ 4.1 เป็นคำสั่งที่เกี่ยวข้องกับการคอนฟิกูเรชันโพรโตคอล SYSLOG บนสวิตช์ S-48si เพื่อให้สามารถส่งล็อกมาที่ตัว Syslog server ได้ โดยในรูปจะละคำสั่งที่ไม่เกี่ยวข้องออกไป

```
# Event Management System Log Target Configuration
enable syslog

configure syslog add 10.193.87.44:514 local0
configure log target syslog 10.193.87.44:514 local0 from 10.193.65.23
configure log target syslog 10.193.87.44:514 local0 filter "DefaultFilter" severity debug-data
configure log target syslog 10.193.87.44:514 local0 match ""
configure log target syslog 10.193.87.44:514 local0 format priority on date mmm-dd time seconds host-
name off tag-name on tag-id off sequence-number off severity off event-name none process-name off
process-id off source-function off source-line off
enable log target syslog 10,193.87.44:514 local0
```

**รูปที่ 4.1** คำสั่งคอนฟิกูเรชันโพรโตคอล SYSLOG บนสวิตช์

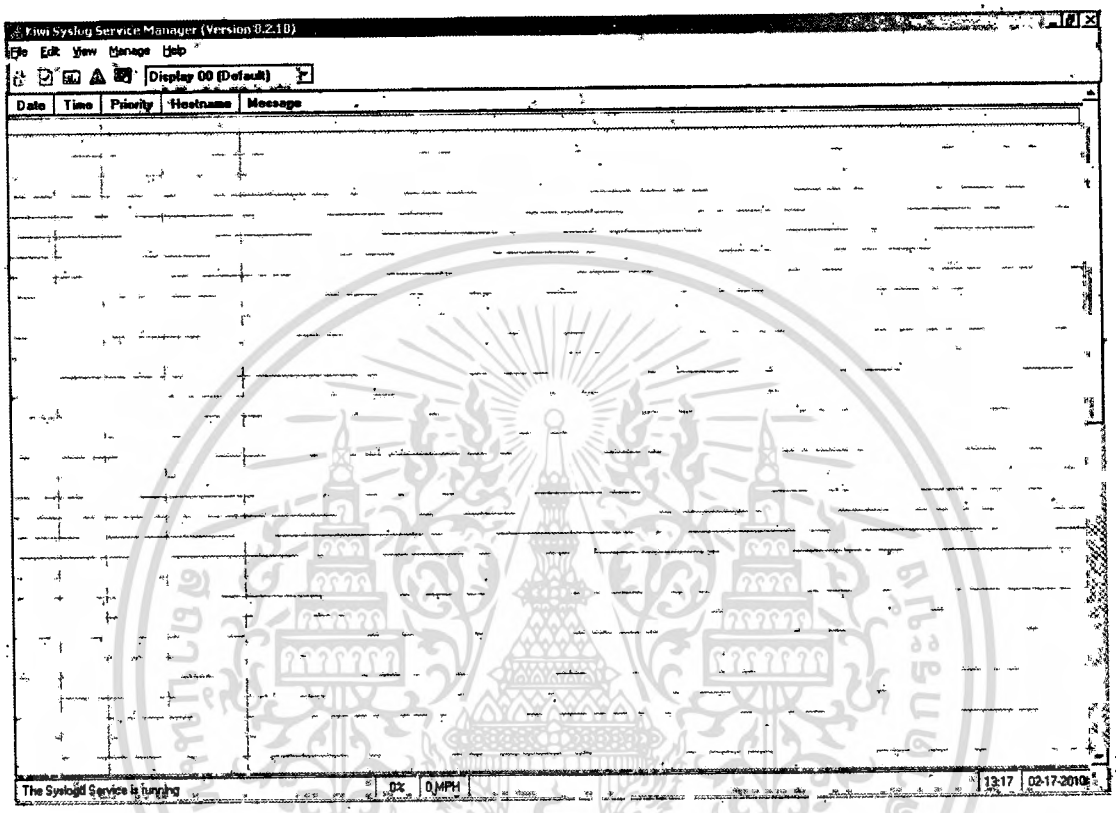
### 4.1.2 ส่วนดำเนินการจัดการ (ส่วนเซิร์ฟเวอร์)

ในส่วนของเซิร์ฟเวอร์ จะมีหน้าที่อยู่ 2 ส่วนหลักด้วยกันคือ

1. ทำหน้าที่เป็น Syslog server เพื่อรับล็อกที่ส่งมาจากสวิตช์และทำการบันทึกลงในไดเรกทอรีที่ได้กำหนดไว้อีกครั้ง โดยในการพัฒนาระบบนี้จะใช้แอพพลิเคชัน Kiwi

Syslog Daemon version 8.2.18 เป็นตัว Syslog server ซึ่งเมื่อติดตั้งแอพพลิเคชันนี้เรียบร้อยและเอ็กซิคิวต์ (Execute) แล้วจะมีหน้าจอดังรูปที่ 4.2

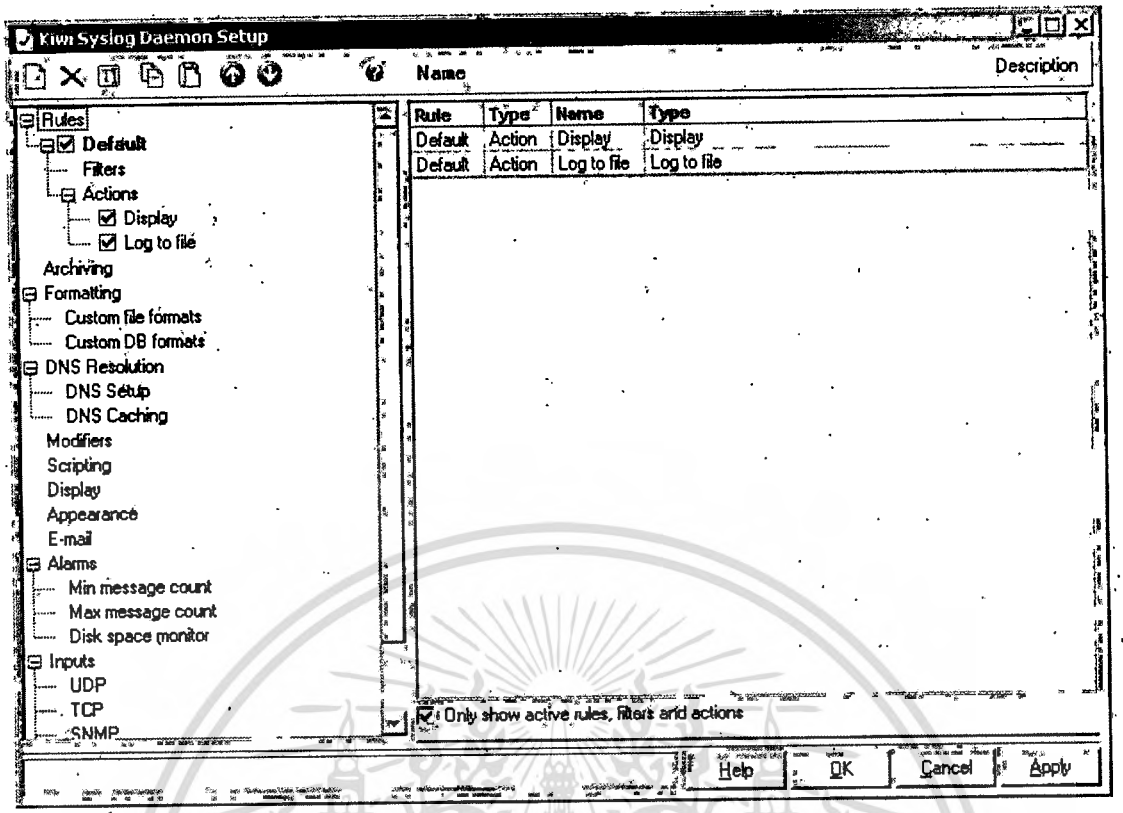
นอกจากนี้ ผู้ดูแลระบบจำเป็นที่จะต้องคอนฟิกูเรชันค่าบางประการของแอพพลเคชันนี้เพื่อให้สามารถง่ายต่อการควบคุม ดังนี้




**รูปที่ 4.2** หน้าจอของแอพพลิเคชัน Kiwi Syslog Daemon version 8.2.18

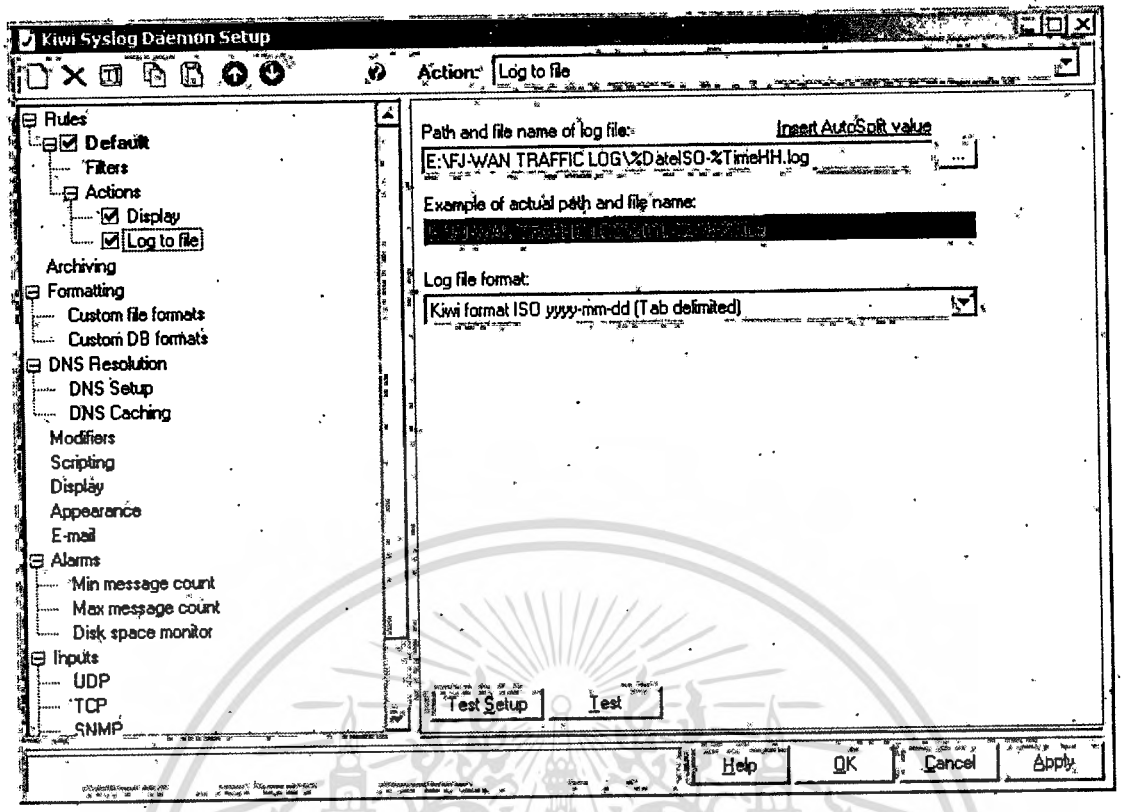
นอกจากนี้ ผู้ดูแลระบบจำเป็นที่จะต้องคอนฟิกูเรชันค่าบางประการของแอพพลิเคชันนี้เพื่อให้สามารถง่ายต่อการควบคุม โดยทำการแก้ไขค่าจากเมนูหลัก ดังนี้

- เลือกเมนู ไฟล์ (File) \ เซตอัพ(Setup) จะพบหน้าจอหลักดังรูปที่ 4.3



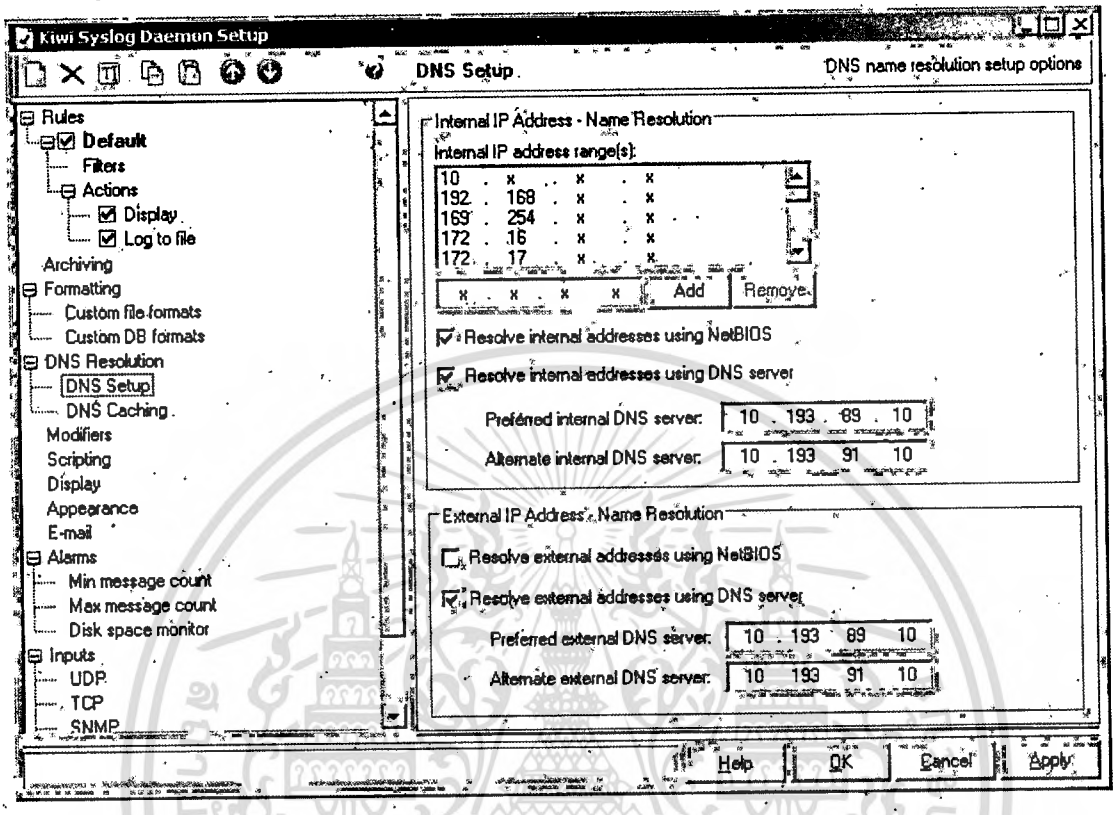

**รูปที่ 4.3** หน้าจอหลักของการเซตอัพค่าของแอพพลิเคชัน Kiwi Syslog Daemon

- เซตค่าพาธ (Path) ที่ต้องการให้ล็อกไปเก็บไว้ดังรูปที่ 4.4 โดยไปที่ Rule \ Default \ Action \ Log to File โดยในการพัฒนาระบบนี้จะเป็นไว้ไดเรกทอรีภายในของเซิร์ฟเวอร์เอง และมีรูปแบบของชื่อไฟล์ที่ใช้เก็บเป็น YYYY-MM-DD-HH (ปี-เดือน-วัน-ชั่วโมง) ซึ่งเหตุผลที่ทำการแบ่งล็อกไฟล์แยกเป็นของมูลในแต่ละชั่วโมงเพื่อให้ง่ายหากผู้ดูละระบบต้องการที่จะดูข้อมูลดิบ รวมทั้งเมื่อนำแอพพลิเคชันมาช่วยในการรีจีสเตอร์ข้อมูลลงไปในฐานข้อมูล จะใช้เวลาเข้าถึงข้อมูลได้รวดเร็วมากยิ่งขึ้น



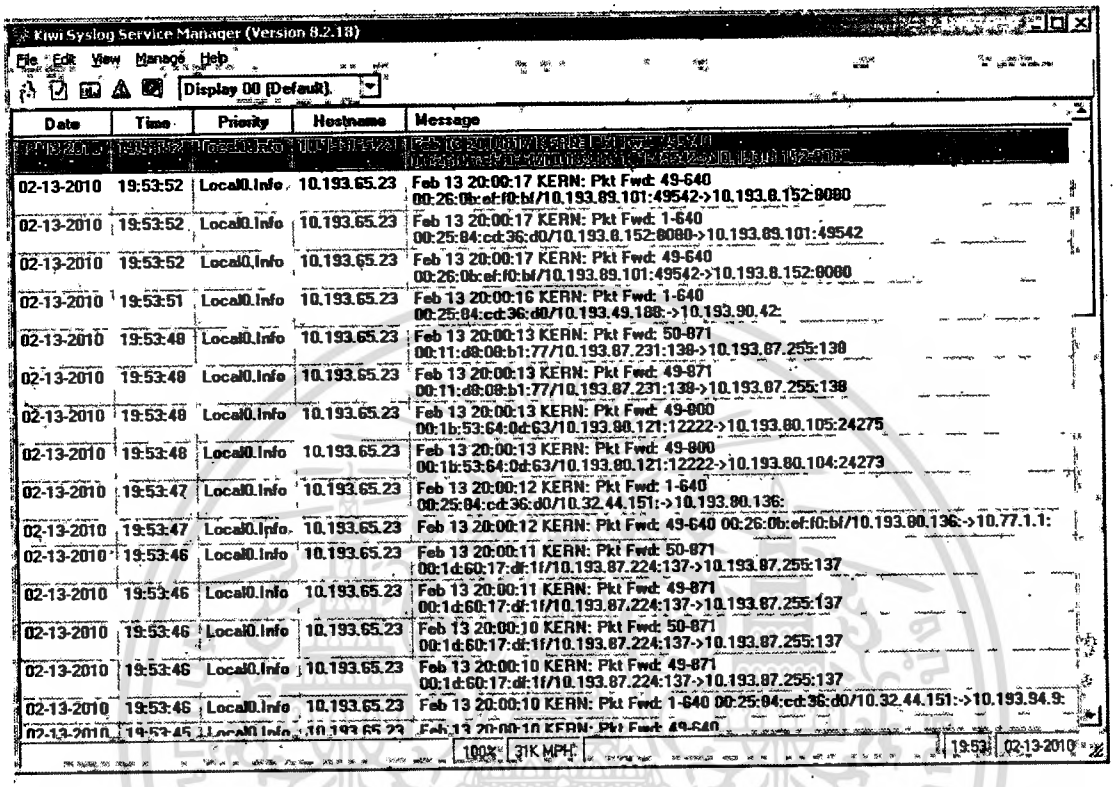

**รูปที่ 4.4** การเซตอัพค่าไดเรกทอรีและรูปแบบในการเก็บล็อกไฟล์ของแอพพลิเคชัน Kiwi Syslog Daemon

- รูปที่ 4.5 แสดงการคอนฟิกูเรชันค่าของ DNS ของเครือข่ายภายใน เมื่อทำการติดตั้งค่าครบเรียบร้อยแล้ว ให้กดปุ่ม “OK” เพื่อยืนยันการติดตั้ง



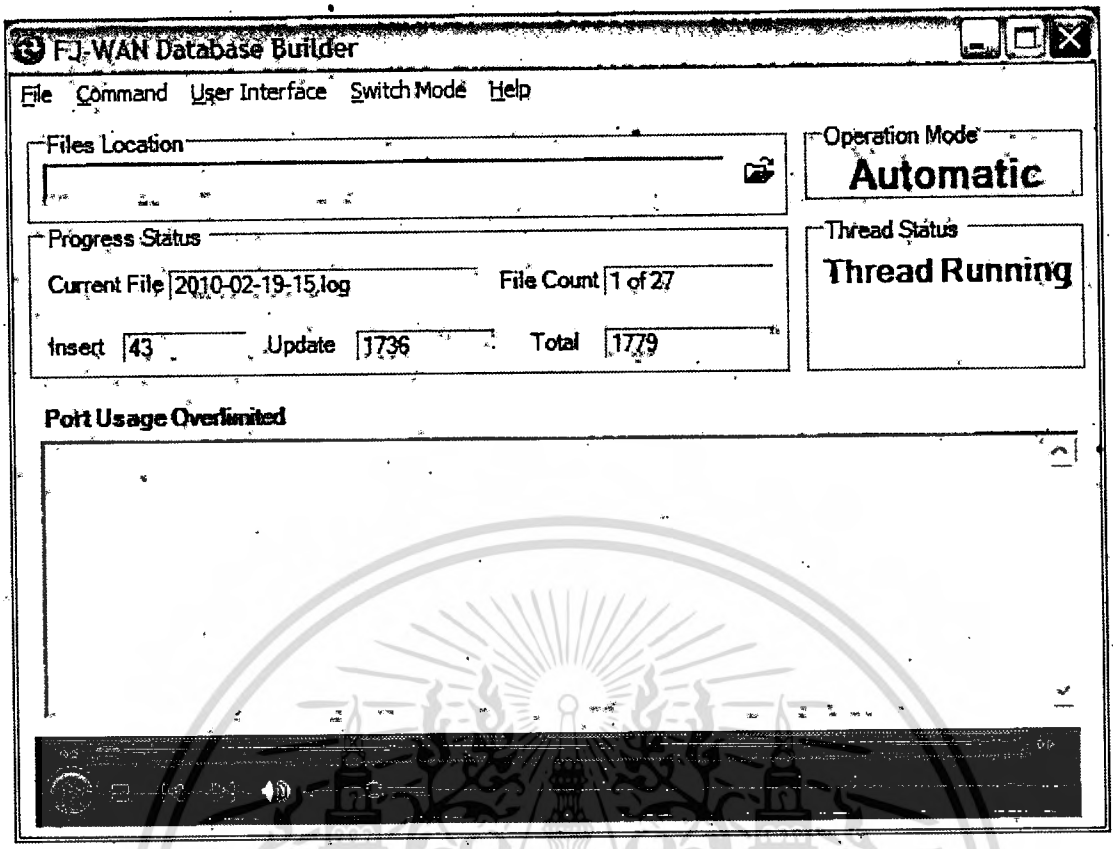

**รูปที่ 4.5** การเซตอัพค่า DNS ของแอพพลิเคชัน Kiwi Syslog Daemon

- เมื่อสวิตซ์ทำการส่งล็อกมายังตัวเซิร์ฟเวอร์โดยผ่านโพรโตคอล SYSLOG ตัวแอพพลิเคชัน Kiwi Syslog Daemon จะได้รับข้อมูลมา ซึ่งสามารถแสดงได้ดังรูปที่ 4.6



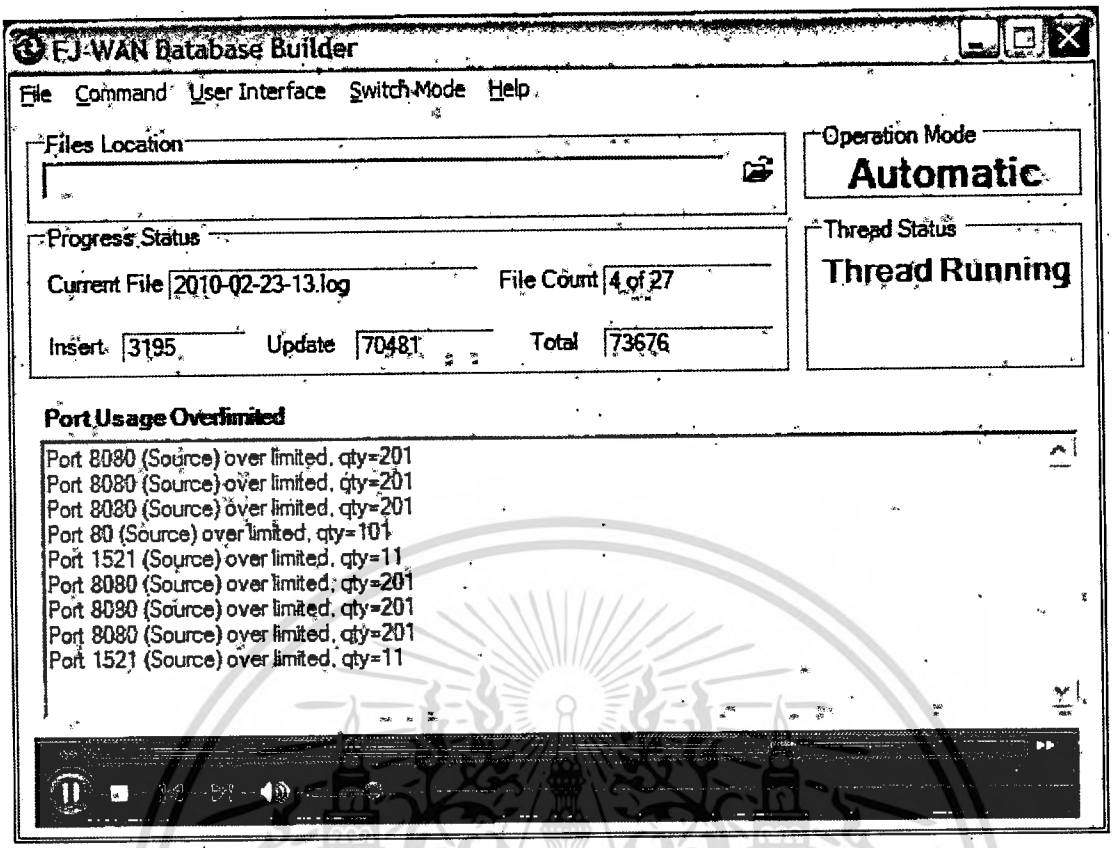

**รูปที่ 4.6** หน้าจอของแอพพลิเคชัน Kiwi Syslog Daemon เมื่อได้รับข้อมูลจากตัวสวิตซ์

2. ทำหน้าที่นำล็อกไฟล์ที่จัดเก็บจากแอพพลิเคชัน Kiwi Syslog Daemon มารีจีสเตอร์ยังฐานข้อมูล โดยแอพพลิเคชัน FJ-WAN Database Builder ที่พัฒนาขึ้นมานี้ จากพัฒนาขึ้นมาจากภาษา VB.NET เมื่อทำการเอ็กซิคิวต์แอพพลิเคชัน จะมีหน้าจอดังรูปที่ 4.7




**รูปที่ 4.7** หน้าจอของแอพพลิเคชัน FJ-WAN Database builder

โดยแอพพลิเคชันนี้จะทำการอ่านเท็กซ์ไฟล์และนำมารีจีสเตอร์ลงในฐานข้อมูลทุกๆระยะรอบเวลา 2 ชั่วโมง รูปที่ 4.8 แสดงหน้าจอของแอพพลิเคชันในขณะที่มีการรีจีสเตอร์ข้อมูลลงในฐานข้อมูล และถ้าหากพบว่าในขณะนั้นมีการติดต่อสื่อสารโดยใช้โพรโตคอลนั้นๆเกินกว่าที่ผู้ดูแลระบบกำหนดไว้ จะมีการแจ้งเตือนโดยใช้สัญญาณเสียงดังขึ้นเพื่อให้ผู้ดูแลระบบทราบถึงความผิดปกติของการใช้ข้อมูลในการติดต่อสื่อสารของเครือข่าย ซึ่งเมื่อผู้ดูแลระบบรับทราบและทำการปิดสัญญาณเสียง ความถี่ในการนับการใช้โพรโตคอลจะถูกล้างค่าให้เป็น 0 เพื่อเริ่มการนับค่าความถี่ใหม่อีกครั้ง




**รูปที่ 4.8** หน้าจอของแอพพลิเคชัน FJ-WAN Database builder ขณะที่มีการรีจีสเตอร์ข้อมูล

จากรูป 4.8 ในส่วนของ Progress Status จะแสดงสถานะของแอพพลิเคชันในขณะนั้น ดังนี้

- Current File : ไฟล์ปัจจุบันที่แอพพลิเคชันกำลังทำการรีจีสเตอร์ข้อมูลลงในฐานข้อมูล
- File Count : จำนวนไฟล์ทั้งหมดที่เหลืออยู่ในไดเรกทอรีซึ่งกำลังรอการรีจีสเตอร์อยู่ รวมทั้งจำนวนไฟล์ที่ได้รับการรีจีสเตอร์ลงในฐานข้อมูลเสร็จเรียบร้อยแล้ว
- Insert : จำนวนเรคอร์ด (Record) ที่ถูกเพิ่มเข้าไปในฐานข้อมูล ซึ่งเป็นข้อมูลใหม่เมื่อเปรียบเทียบจากข้อมูลในไฟล์ที่กำลังรีจีสเตอร์อยู่ เช่น ไอพีแอดเดรสต้นทาง ไอพีแอดเดรสปลายทาง หรือพอร์ตที่ใช้เชื่อมต่อใหม่
- Update : จำนวนเรคอร์ดที่ทำการนับเพิ่ม (Count) เข้าไปเนื่องจากเป็นข้อมูลเดิมที่มีอยู่แล้ว เช่น ไอพีแอดเดรสต้นทาง ไอพีแอดเดรสปลายทาง หรือพอร์ตที่ใช้ในการติดต่อมีค่าที่ถูกรีจีสเตอร์เข้าไปในฐานข้อมูลเรียบร้อยแล้ว เมื่อเปรียบเทียบจากข้อมูลของไฟล์ที่กำลังรีจีสเตอร์อยู่ ณ ขณะนั้น
- Total : จำนวนข้อมูลทั้งหมดที่ได้รับการรีจีสเตอร์ลงไปในฐานข้อมูล โดยสามารถคำนวณได้จากผลบวกของข้อมูลที่ Insert และข้อมูลที่ Update (Total data = Insert data + Update data)

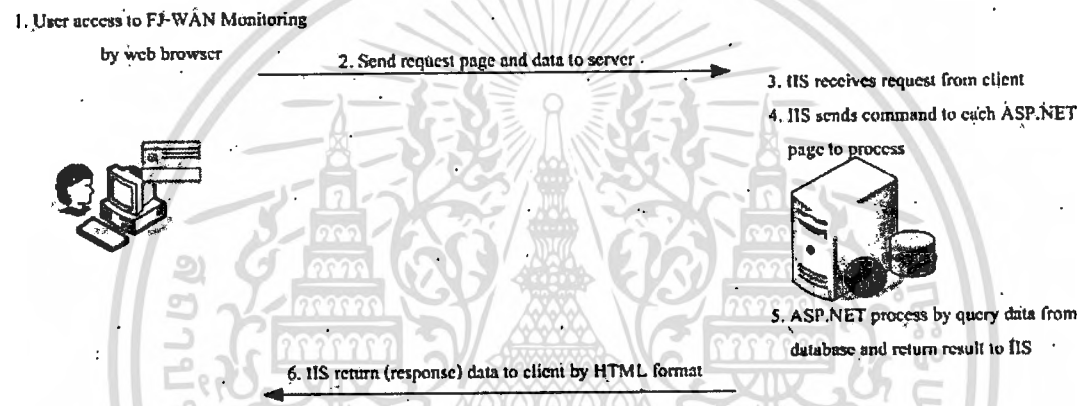
หลังจากที่แอพพลิเคชันทำการรีจีสเตอร์ข้อมูลให้อยู่ในรูปฐานข้อมูลแล้ว ไฟล์ข้อมูลที่อยู่ในไดเรกทอรีจะถูกย้ายไปอยู่ในส่วนของแบ็กอัพไดเรกทอรี (Backup directory) ซึ่งเป็นคนละไดเรกทอรีกันกับพาธ (Path) ที่เก็บข้อมูลของ Kiwi Syslog Daemon ทั้งนี้แบ็กอัพไดเรกทอรี จะมีการจัดการแบ่งข้อมูลจัดเก็บลงในโฟลเดอร์ (Folder) แต่ละโฟลเดอร์โดยแบ่งเป็นโฟลเดอร์ละเดือน (YYYY-MM) และเมื่อข้อมูลได้รับการรีจีสเตอร์ครบ 1 เดือนและถูกย้ายมายังแบ็กอัพไดเรกทอรีครบหมดก็จะถูกบีบอัด (Compress) ขนาดของข้อมูลของไฟล์เพื่อเป็นการลดพื้นที่ที่ใช้ในการจัดเก็บ

### 4.1.3 ส่วนผู้ใช้งานระบบ

สำหรับส่วนของผู้ใช้งานนั้น จะแบ่งผู้ใช้งานออกเป็น 2 ประเภทด้วยกัน ได้แก่

1. ผู้ใช้งานที่เป็นผู้ดูแลระบบเครือข่าย (Network administrator)
   ในส่วนของผู้ดูแลระบบนี้จะมีฟังก์ชันเพิ่มขึ้นมาจากผู้ใช้งานทั่วไป คือสามารถทำการแก้ไขเปลี่ยนแปลงค่าพอร์ต (Connection port) รวมทั้งแก้ไขเปลี่ยนแปลงซับเน็ต (Subnet) ขององค์กรได้ ซึ่งการเข้าหน้าจอเพื่อเปลี่ยนแปลงข้อมูลนี้จะต้องผู้ดูแลระบบจะต้องทำการป้อนชื่อผู้ใช้งานรวมทั้งรหัสผ่าน ซึ่งข้อมูลทั้งสองนี้ จะต้องถูกต้องตรงตามข้อมูลที่ได้ระบุไว้ในคอนฟิกูเรชันไฟล์ (Configuration file) ของตัวแอพพลิเคชัน
2. ผู้ใช้งานทั่วไป
   ผู้ใช้งานทั่วไป จะหมายถึงบุคลากรทั่วไปภายในองค์กร ซึ่งสามารถเชื่อมต่อเข้ากับระบบเครือข่ายภายในขององค์กร การที่ให้สิทธิ์ในการเข้าดูข้อมูลกับบุคลากรทั่วไปขององค์กรทั้งนี้เพราะบริษัทมีนโยบายให้พนักงานโดยเฉพาะในระดับบริหารสามารถตรวจสอบถึงสถานะการใช้ย่านความถี่ของระบบเครือข่ายระยะไกลขององค์กร ว่าในหน่วยงานใดๆ มีพนักงานหรือเครื่องคอมพิวเตอร์ใดใช้งานย่านความถี่นั้นๆอยู่บ้าง ซึ่งจะทำให้สามารถตรวจสอบได้ หากมีการใช้งานที่ผิดปกติไปจากเดิม เช่นมีการติดต่อสื่อสารกันระหว่างระบบเครือข่ายโดยใช้พอร์ตที่แปลกไปจากเดิมที่มีการกำหนดไว้
   รูปที่ 4.9 แสดงขั้นตอนในการร้องขอข้อมูลจากเครื่องไคลเอ็นต์ไปยังเซิร์ฟเวอร์ เพื่อดูข้อมูลของระบบ โดยที่เครื่องไคลเอ็นต์นั้น ผู้ใช้งานไม่จำเป็นต้องติดตั้งแอพพลิเคชันใดๆเพิ่มเติม ทั้งนี้เพราะระบบตรวจสอบทราฟฟิกนี้จะแสดงผลผ่านทางเว็บบราวเซอร์ เช่น Microsoft Internet Explorer หรือ Mozilla Firefox ซึ่งโดยทั่วไปเครื่องคอมพิวเตอร์ทุกเครื่องจะได้รับการติดตั้ง เว็บบราวเซอร์เหล่านี้อยู่แล้ว
   เมื่อผู้ใช้งานเข้าสู่หน้าจอส่วนต่างๆของระบบ จะหมายถึงเครื่องไคลเอ็นต์ได้ส่งคำร้องขอไปยังเซิร์ฟเวอร์ ซึ่งเมื่อเซิร์ฟเวอร์ได้รับคำร้องขอนั้นๆแล้ว ที่ตัวเซิร์ฟเวอร์ซึ่ง

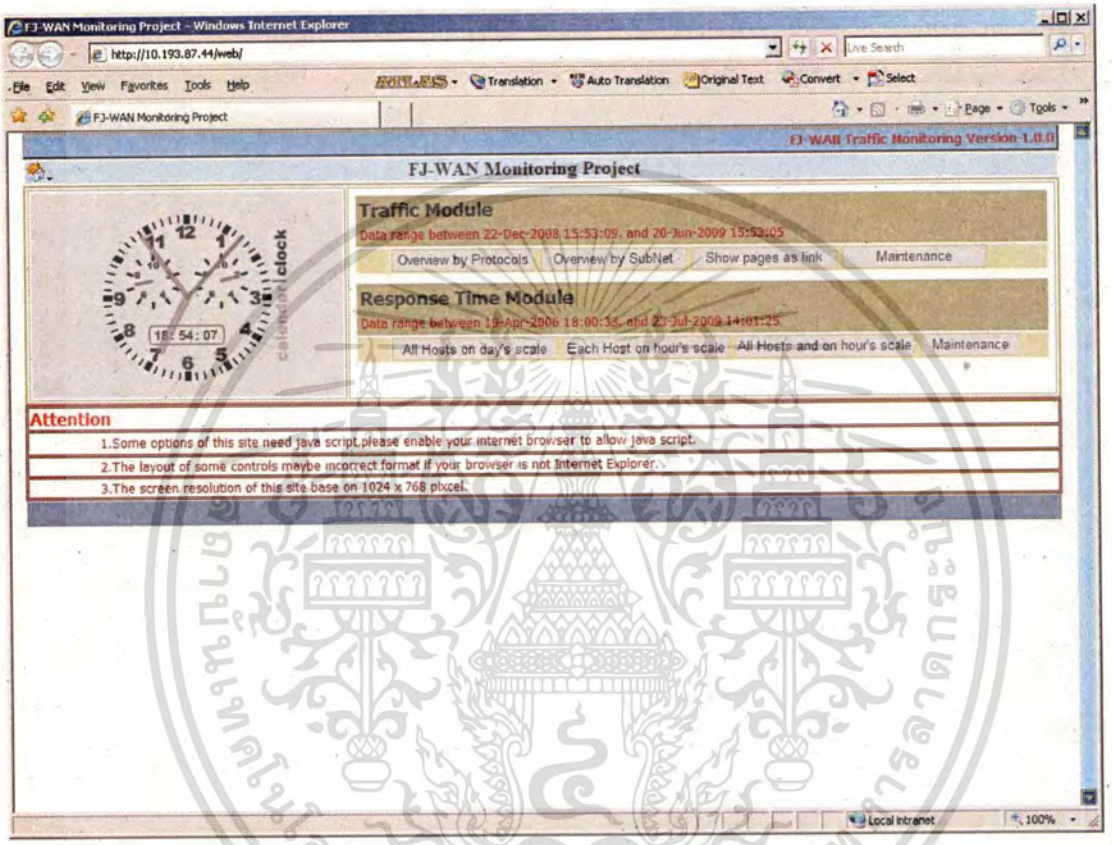
อีนาเบิล IIS (Internet Information Services) และได้คอนฟิกูเรชันค่าเบื้องต้น (Default) เช่นพาธที่ใช้เก็บข้อมูลของเว็บไซต์ ระบุไฟล์ที่ทำเป็นหน้าหลักของตัวเว็บไซต์ เป็นต้น จะรับค่าคำร้องจากไคลเอ็นต์มาและส่งให้กับเว็บแอพพลิเคชัน (Web application) ที่พัฒนาขึ้นมาจากภาษา ASP.NET ทำหน้าที่เป็นตัวประมวลผลของคำร้องขอที่ได้มาจากไคลเอ็นต์ นำข้อมูลร้องขอที่ได้มาสืบค้น (Query) จากฐานข้อมูลที่ได้รับการรีจีสเตอร์จากแอพพลิเคชัน FJ-WAN Database Builder หลังจากนั้นจะส่งผลลัพธ์ที่ได้กลับไปให้กับ IIS อีกครั้งหนึ่ง ซึ่ง IIS จะทำการจัดข้อมูลให้อยู่ในรูปแบบของ HTML และส่งผลที่ได้นั้นกลับไปยังเครื่องไคลเอ็นต์เพื่อให้ผู้ใช้งานได้ดูผลที่ผู้ใช้งานเรียกดู




**รูปที่ 4.9** ขั้นตอนการร้องขอข้อมูลจากไคลเอ็นต์และการตอบสนองของเซิร์ฟเวอร์

## 4.2 คู่มือการใช้งานระบบของผู้ใช้

เมื่อผู้ใช้ระบบภายในองค์กรทำการเอ็กซีคิวต์เว็บบราวเซอร์เช่น Microsoft Internet Explorer และใส่ค่า URL ของระบบตรวจสอบทราฟฟิกของเครือข่ายสำหรับข้อมูลที่ถูกส่งผ่านบนเครือข่ายระยะไกลของบริษัทฟูจิตสึ (ประเทศไทย) จะปรากฏหน้าจอดังรูปที่ 4.10




**รูปที่ 4.10** หน้าจอหลักของระบบตรวจสอบทราฟฟิกบนเครือข่ายระยะไกล

หน้าจอหลักนี้จะมีเมนูสำหรับผู้ใช้งานให้เลือกด้วยกัน 4 หัวข้อ ได้แก่

1. Overview by Protocols เป็นเมนูในการแสดงผลของการตรวจสอบทราฟฟิกที่ใช้งานย่านความถี่ของเครือข่ายระยะไกลโดยจะแบ่งตามโพรโตคอลที่ใช้ในการติดต่อสื่อสารกัน เช่น POP, IMAP4, HTTP เป็นต้น
2. Overview by SubNet เป็นเมนูในการแสดงผลของการตรวจสอบทราฟฟิกที่ใช้งานย่านความถี่ของเครือข่ายระยะไกลโดยจะแบ่งตามซับเน็ตของเครื่องต้นทางที่เป็นตัวเริ่มการติดต่อสื่อสารใดๆ โดยในการพัฒนาระบบนี้จะอ้างอิงจากซับเน็ตของบริษัทฟูจิตสึ (ประเทศไทย)

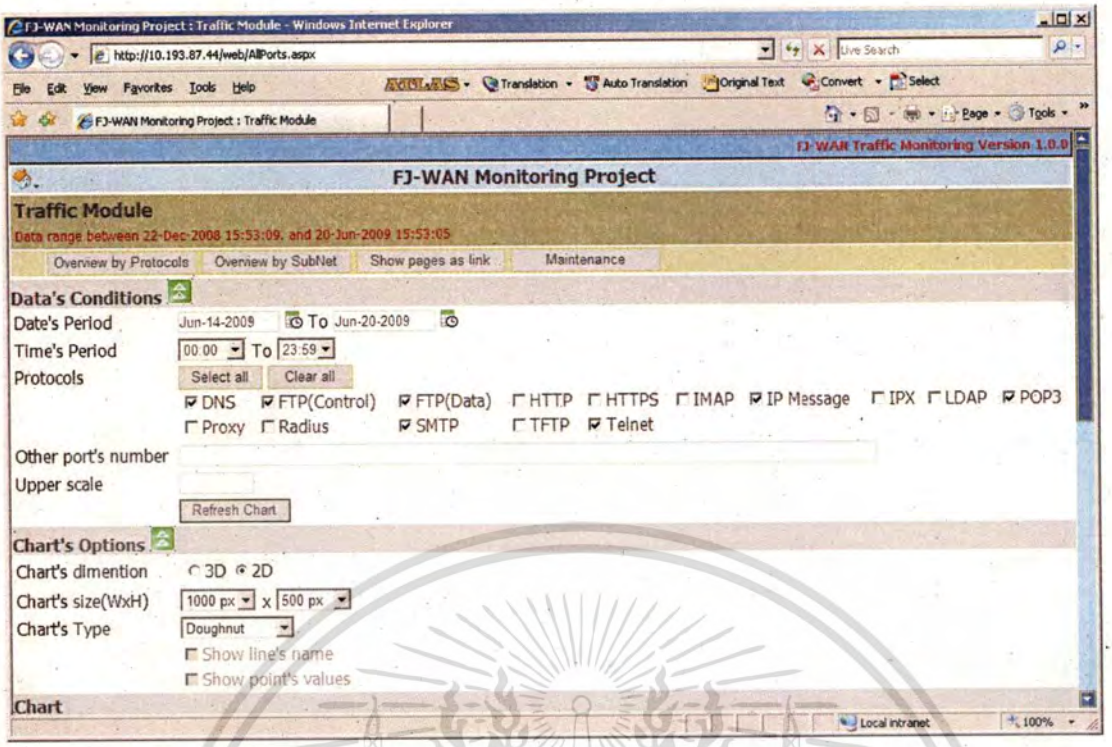
3. Show pages as link เป็นเมนูในการแสดงข้อมูลที่ละขั้นตอนที่มีอยู่ทั้งหมดของการแสดงผล ทั้งนี้เพื่ออำนวยความสะดวกให้แก่ผู้ใช้งาน ในกรณีที่ต้องการตรวจสอบข้อมูลเชิงลึก ก็สามารถเข้าได้จากเมนูย่อยที่มีอยู่ในหัวข้อนี้ได้โดยตรง โดยไม่จำเป็นต้องเข้าไปทีละขั้นตอนจากขอบเขตที่กว้างก่อนและทำการคลิ้ก (Click) เพื่อลงรายละเอียดลึกไปเรื่อยๆ
4. Maintenance เป็นเมนูที่มีไว้สำหรับผู้ดูแลระบบเครือข่ายทำการแก้ไขเปลี่ยนแปลงค่าต่างๆของระบบ อันได้แก่
   - การแก้ไข เพิ่มเติม ลบพอร์ตและโพรโตคอลที่ใช้ในการติดต่อสื่อสาร
   - การแก้ไข เพิ่มเติม ลบซับเน็ตขององค์กร

### 4.2.1 Overview by Protocols

ดังที่ได้กล่าวมาแล้ว เมื่อผู้ใช้งานเข้ามาสู่เมนูนี้ หน้าเว็บบราวเซอร์จะแสดงหน้าจอในการกำหนดเงื่อนไขในการดูข้อมูลการใช้ปริมาณย่านความถี่ของระบบเครือข่ายระยะไกลตามโพรโตคอลที่ใช้ในการติดต่อสื่อสาร โดยผู้ใช้งานจะต้องเลือกข้อมูลดังนี้

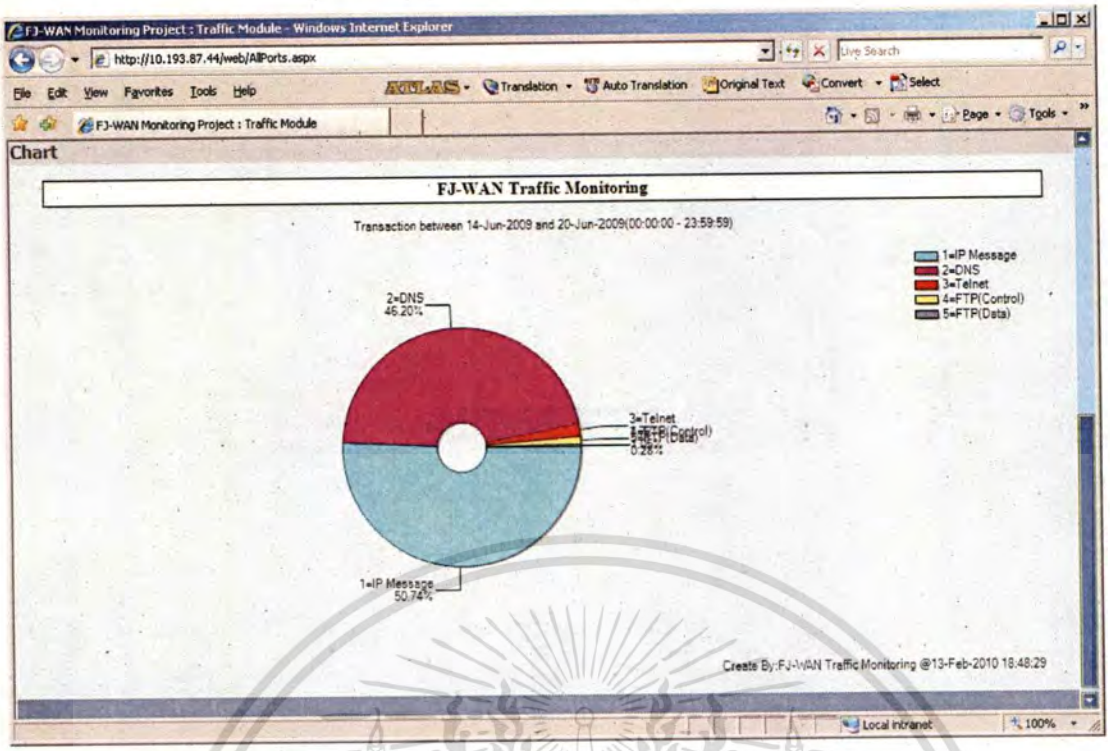
1. วันที่เริ่มต้นและวันที่สิ้นสุดสำหรับการดูข้อมูล โดยเบื้องต้นแอพพลิเคชันจะถูกเลือกให้แสดงข้อมูลในช่วง 1 สัปดาห์
2. เวลาเริ่มต้นและเวลาสิ้นสุดสำหรับการดูข้อมูล โดยเบื้องต้นแอพพลิเคชันจะถูกเลือกให้แสดงข้อมูลเวลาตั้งแต่ 0:00 นาฬิกา ถึง 23:59 นาฬิกา
3. โพรโตคอลที่ต้องการดูข้อมูล โดยเบื้องต้นจะมีโพรโตคอลที่ได้รับการเลือกให้แสดงอยู่จำนวนหนึ่งแล้วเช่นโพรโตคอลDNS, FTP, SMTP, IMAP เป็นต้น ผู้ใช้งานสามารถที่จะเลือกโพรโตคอลเพิ่มเติมจากที่ถูกเลือกอยู่ หรือนำโพรโตคอลที่ถูกเลือกออก นอกจากนี้ยังสามารถระบุโพรโตคอลเพิ่มได้ หากในรายการโพรโตคอลไม่มีให้เลือก
4. ลักษณะของกราฟที่ต้องการแสดง เช่นเป็นกราฟแบบ 2 มิติ หรือ 3 มิติ ขนาดของกราฟ (ขนาดความกว้างและความยาวของกราฟ) ที่ต้องการแสดงบนหน้าจอ และลักษณะของกราฟที่ต้องการให้แสดงเช่นเป็นกราฟวงกลม กราฟแท่ง หรือกราฟเส้น เป็นต้น

รูปที่ 4.11 แสดงหน้าจอของการกำหนดเงื่อนไขการแสดงการใช้ปริมาณย่านความถี่ของระบบเครือข่ายระยะไกลโดยกำหนดเงื่อนไขในการตรวจสอบแบบโพรโตคอล




**รูปที่ 4.11** หน้าจอกำหนดเงื่อนไขเพื่อดูของมูลการใช้แบบโพรโตคอล

เมื่อผู้ใช้งานได้ทำการเลือกค่าต่างๆครบหมดตามที่ต้องการและทำการกดปุ่ม Refresh Chart กราฟด้านล่างจะแสดงข้อมูลที่ได้จากเงื่อนไขข้างต้นที่ถูกส่งคำร้องขอไปยังเซิร์ฟเวอร์เพื่อประมวลผลและส่งผลลัพธ์กลับมา ดังตัวอย่างในรูปที่ 4.12 ซึ่งจะแสดงผลลัพธ์ที่ได้จากเงื่อนไขการแสดงโพรโตคอลที่ใช้ปริมาณย่านความถี่มากสุด 20 อันดับแรกในช่วงวันที่ 14 มิถุนายน ค.ศ. 2009 ถึงวันที่ 20 มิถุนายน ค.ศ.2009




**รูปที่ 4.12** กราฟแสดงหน้าผลการใช้งานย่านความถี่โดยแบ่งตามโพรโตคอล

### 4.2.2 Overview by Subnet

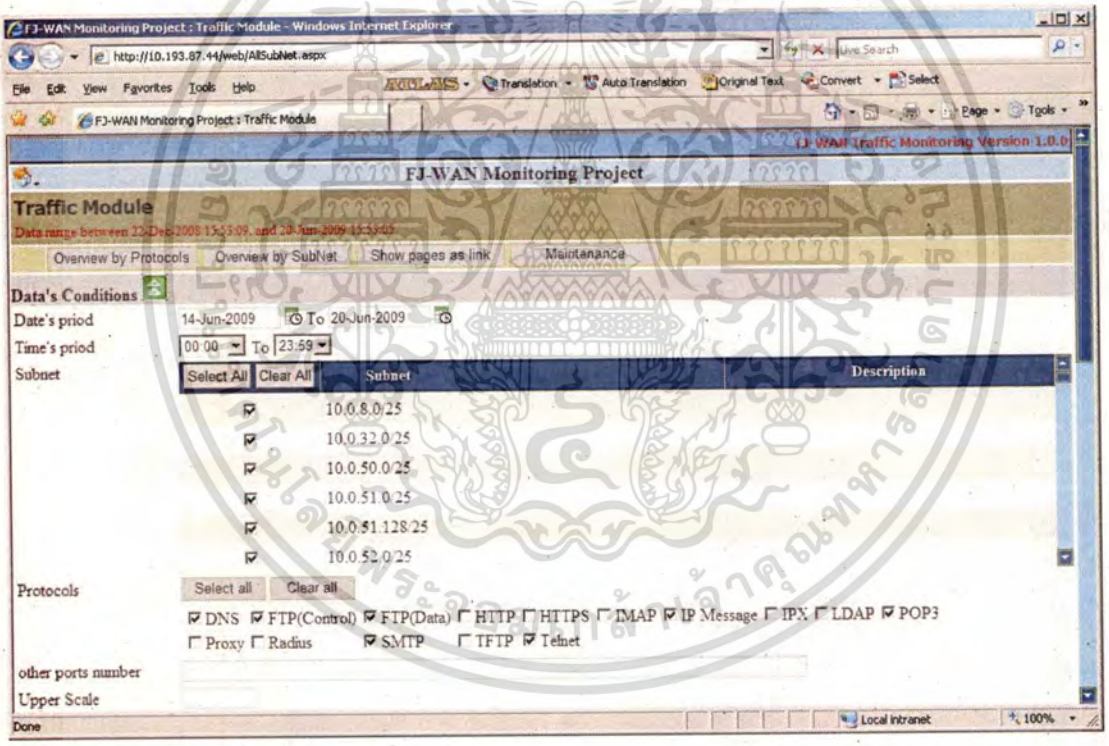
เมื่อผู้ใช้งานเข้ามาสู่เมนู Overview by Subnet นี้ หน้าเว็บบราวเซอร์จะแสดงหน้าจอในการกำหนดเงื่อนไขในการดูข้อมูลการใช้ปริมาณย่านความถี่ของระบบเครือข่ายระยะไกลตามซับเน็ตที่ใช้งานอยู่ขององค์กร โดยผู้ใช้งานจะต้องเลือกข้อมูลดังนี้

1. วันที่เริ่มต้นและวันที่สิ้นสุดสำหรับการดูข้อมูล โดยเบื้องต้นแอพพลิเคชันจะถูกเลือกให้แสดงข้อมูลในช่วง 1 สัปดาห์
2. เวลาเริ่มต้นและเวลาสิ้นสุดสำหรับการดูข้อมูล โดยเบื้องต้นแอพพลิเคชันจะถูกเลือกให้แสดงข้อมูลเวลาตั้งแต่ 0:00 นาฬิกา ถึง 23:59 นาฬิกา
3. ซับเน็ตที่ผู้ใช้งานต้องการจะตรวจสอบว่าในช่วงเวลาข้างต้น มีการใช้งานปริมาณย่านความถี่เท่าใด โดยเบื้องต้นแอพพลเคชันจะเลือกให้แสดงข้อมูลของซับเน็ตทั้งหมดขององค์กรอยู่แล้ว แต่ถ้าหากผู้ใช้งานต้องการที่จะระบุลงไปเฉพาะเจาะจงเพียงซับเน็ตใดซับเน็ตหนึ่ง หรือกลุ่มของซับเน็ตใด (ทั้งนี้เพราะในบางหน่วยงานหรือแผนก อาจมีการใช้ซับเน็ตมากกว่า 1 ตัว ซึ่งการเลือกเป็นกลุ่มของซับเน็ตจะสามารถตรวจสอบการใช้งานของหน่วยงานหรือแผนกนั้นๆได้) ก็สามารถที่จะเลือกเฉพาะได้เช่นกัน
4. โพรโตคอลที่ต้องการดูข้อมูล เพื่อเป็นการระบุลงไปว่าในกลุ่มของซับเน็ตในข้อบนผู้ใช้งานต้องการดูการใช้งานย่านความถี่ของเครือข่ายระยะไกลที่มีการติดต่อสื่อสาร

ระหว่างกันด้วยโพรโตคอลได้บ้าง โดยเบื้องต้นจะมีโพรโตคอลที่ได้รับการเลือกให้แสดงอยู่จำนวนหนึ่งแล้วเช่นโพรโตคอลDNS, FTP, SMTP, IMAP เป็นต้น ผู้ใช้งานสามารถที่จะเลือกโพรโตคอลเพิ่มเติมจากที่ถูกเลือกอยู่ หรือนำโพรโตคอลที่ถูกเลือกออก นอกจากนี้ยังสามารถระบุโพรโตคอลเพิ่มได้ หากในรายการโพรโตคอลไม่มีให้เลือก

5. ลักษณะของกราฟที่ต้องการแสดง เช่นเป็นกราฟแบบ 2 มิติ หรือ 3 มิติ ขนาดของกราฟ (ขนาดความกว้างและความยาวของกราฟ) ที่ต้องการแสดงบนหน้าจอ และลักษณะของกราฟที่ต้องการให้แสดงเช่นเป็นกราฟวงกลม กราฟแท่ง หรือกราฟเส้น เป็นต้น

รูปที่ 4.13 แสดงหน้าจอของการกำหนดเงื่อนไขการแสดงการใช้ปริมาณย่านความถี่ของระบบเครือข่ายระยะไกลโดยกำหนดเงื่อนไขในการตรวจสอบแบบซับเน็ต



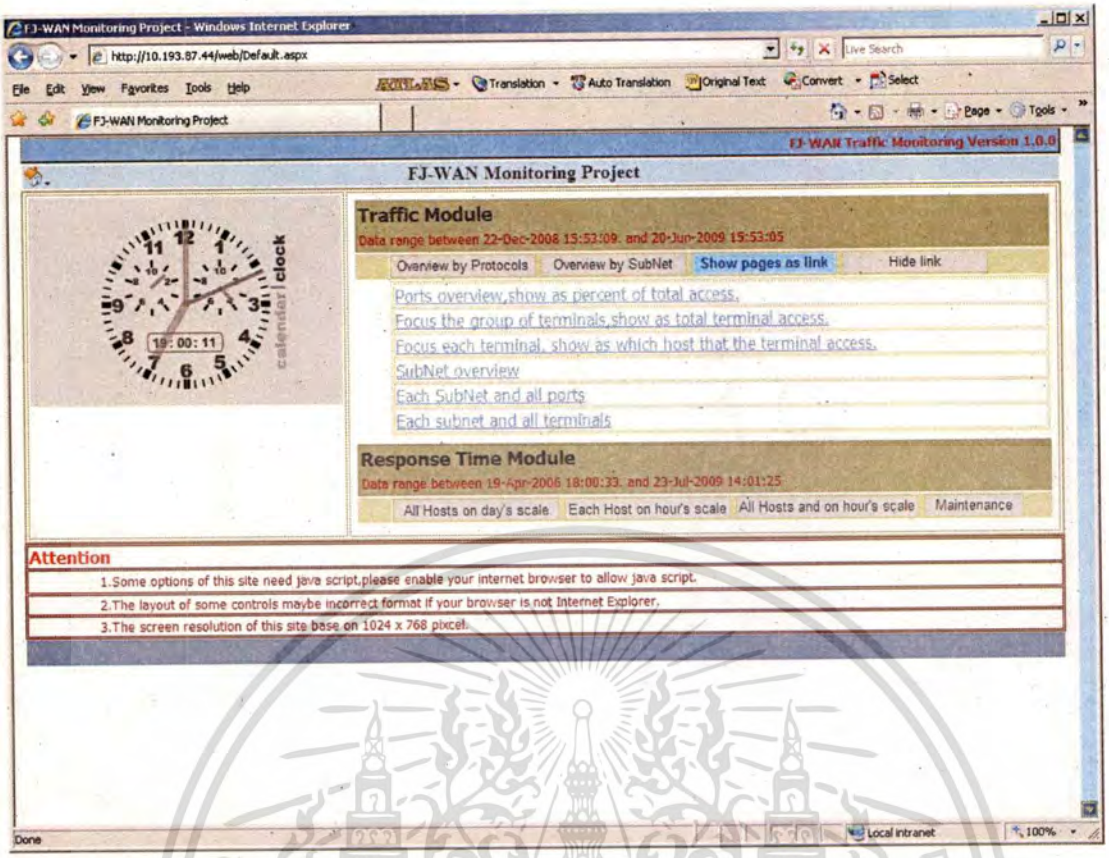

**รูปที่ 4.13** หน้าจอกำหนดเงื่อนไขเพื่อดูของมูลการใช้แบบซับเน็ต

เมื่อผู้ใช้งานได้ทำการเลือกค่าต่างๆครบหมดตามที่ต้องการและทำการกดปุ่ม Refresh Chart กราฟด้านล่างจะแสดงข้อมูลที่ได้จากเงื่อนไขข้างต้นที่ถูกส่งคำร้องขอไปยังเซิร์ฟเวอร์เพื่อประมวลผลและส่งผลลัพธ์กลับมา ดังตัวอย่างในรูปที่ 4.14 ซึ่งจะแสดงผลลัพธ์ที่ได้จากเงื่อนไขการแสดงซับเน็ตใช้ปริมาณย่านความถี่มากสุด 20 อันดับแรกในช่วงวันที่ 14 มิถุนายน ค.ศ.2009 ถึงวันที่ 20 มิถุนายน ค.ศ.2009


**รูปที่ 4.14** กราฟแสดงหน้าผลการใช้งานย่านความถี่โดยแบ่งตามซับเน็ต

### 4.2.3 Show pages as link

ในเมนู Show pages as link จะเป็นการดูข้อมูลการใช้ปริมาณย่านความถี่ของระบบเครือข่ายระยะไกล ซึ่งเมนูย่อยเหล่านี้จะเป็นเหมือนเมนูลัดในการเข้าไปดูข้อมูลต่างๆ ทั้งนี้เพราะใน 2 เมนูหลักข้างต้น เมื่อต้องการดูข้อมูลรายละเอียดเชิงลึกในแต่ละตัว ผู้ใช้งานจะต้องค่อยๆ คลิ้ก (Click) เพื่อเข้าไปดูรายละเอียดที่ละขั้นตอนลงไปเรื่อยๆ แต่สำหรับเมนูนี้ จะเป็นการนำเอาขั้นตอนทั้งหมดมาให้ผู้ใช้งานได้เลือก ดังนั้นเมื่อต้องการดูข้อมูลในระดับลึกใด ก็สามารถเข้าได้จากเมนูย่อยที่มีได้ ดังแสดงในรูปที่ 4.15

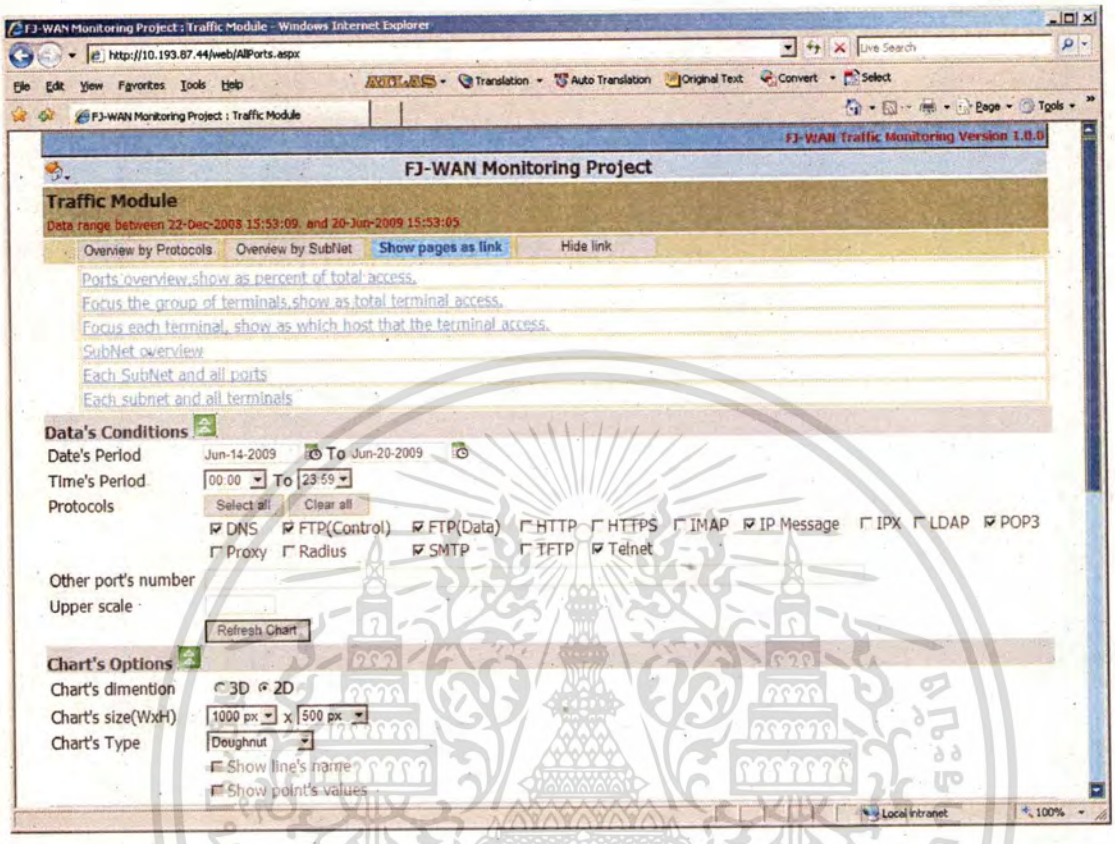



**รูปที่ 4.15** เมนูย่อยภายใต้หัวข้อ Show pages as link

ตัวอย่างของการเข้าดูข้อมูลเมื่อผู้ใช้งานกดที่เมนูย่อย Ports overview show as percent of total access หน้าจอเว็บบราวเซอร์จะแสดงข้อมูลเช่นเดียวกับการดูของมูลแบบระบุโพรโตคอล เพื่อให้ผู้ใช้งานได้เลือกข้อมูลที่ต้องการตรวจสอบในขั้นตอนต่อไปดังนี้

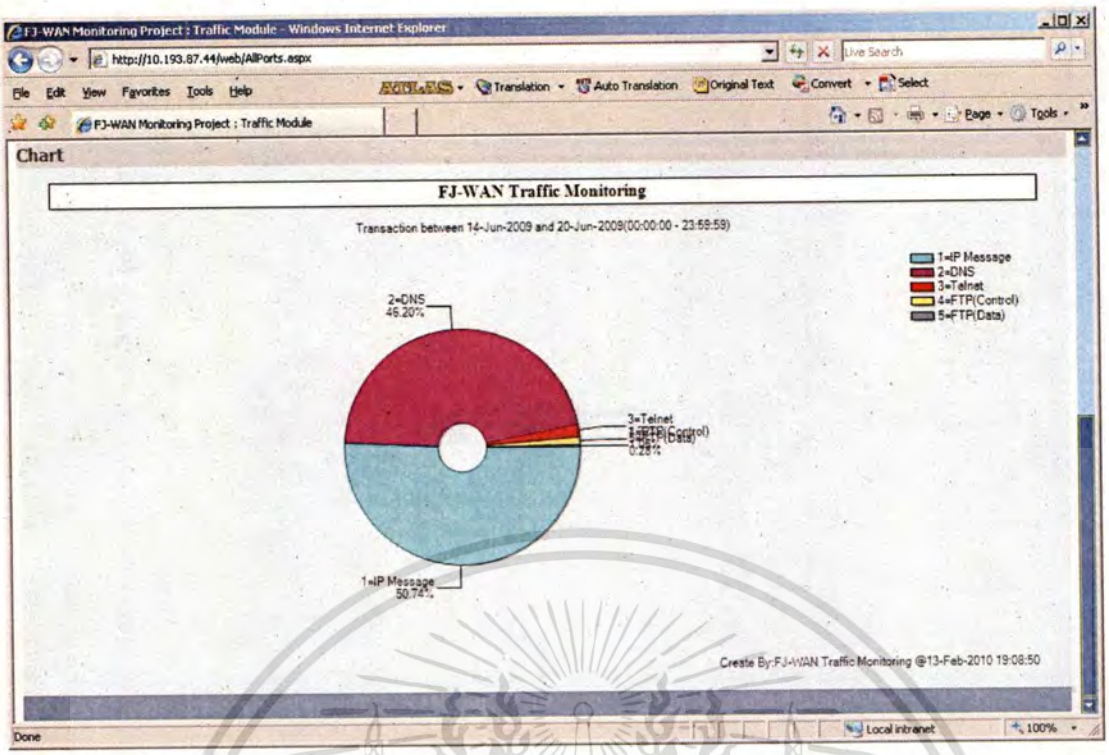
1. วันที่เริ่มต้นและวันที่สิ้นสุดสำหรับการดูข้อมูล โดยเบื้องต้นแอพพลิเคชันจะถูกเลือกให้แสดงข้อมูลในช่วง 1 สัปดาห์
2. เวลาเริ่มต้นและเวลาสิ้นสุดสำหรับการดูข้อมูล โดยเบื้องต้นแอพพลิเคชันจะถูกเลือกให้แสดงข้อมูลเวลาตั้งแต่ 0:00 นาฬิกา ถึง 23:59 นาฬิกา
3. โพรโตคอลที่ต้องการดูข้อมูล โดยเบื้องต้นจะมีโพรโตคอลที่ได้รับการเลือกให้แสดงอยู่จำนวนหนึ่งแล้วเช่นโพรโตคอลDNS, FTP, SMTP, IMAP เป็นต้น ผู้ใช้งานสามารถที่จะเลือกโพรโตคอลเพิ่มเติมจากที่ถูกเลือกอยู่ หรือนำโพรโตคอลที่ถูกเลือกออก นอกจากนี้ยังสามารถระบุโพรโตคอลเพิ่มได้ หากในรายการโพรโตคอลไม่มีให้เลือก
4. ลักษณะของกราฟที่ต้องการแสดง เช่นเป็นกราฟแบบ 2 มิติ หรือ 3 มิติ ขนาดของกราฟ (ขนาดความกว้างและความยาวของกราฟ) ที่ต้องการแสดงบนหน้าจอ และลักษณะของกราฟที่ต้องการให้แสดงเช่นเป็นกราฟวงกลม กราฟแท่ง หรือกราฟเส้น เป็นต้น

รูปที่ 4.16 แสดงหน้าจอของการกำหนดเงื่อนไขการแสดงการใช้ปริมาณย่านความถี่ของระบบเครือข่ายระยะไกลโดยกำหนดเงื่อนไขในการตรวจสอบเช่นเดียวกับเงื่อนไขโพรโตคอล




**รูปที่ 4.16** หน้าจอกำหนดเงื่อนไขเพื่อดูของมูลการใช้

เมื่อผู้ใช้งานได้ทำการเลือกค่าต่างๆครบหมดตามที่ต้องการและทำการกดปุ่ม Refresh Chart กราฟด้านล่างจะแสดงข้อมูลที่ได้จากเงื่อนไขข้างต้นที่ถูกส่งคำร้องขอไปยังเซิร์ฟเวอร์เพื่อประมวลผลและส่งผลลัพธ์กลับมา ดังตัวอย่างในรูปที่ 4.17 ซึ่งจะแสดงผลลัพธ์ที่ได้จากเงื่อนไขการแสดงโพรโตคอลที่ใช้ปริมาณย่านความถี่มากสุด 20 อันดับแรกในช่วงวันที่ 14 มิถุนายน ค.ศ. 2009 ถึงวันที่ 20 มิถุนายน ค.ศ.2009




**รูปที่ 4.17** กราฟแสดงหน้าผลการใช้งานย่านความถี่โดยแบ่งตามโพรโตคอล

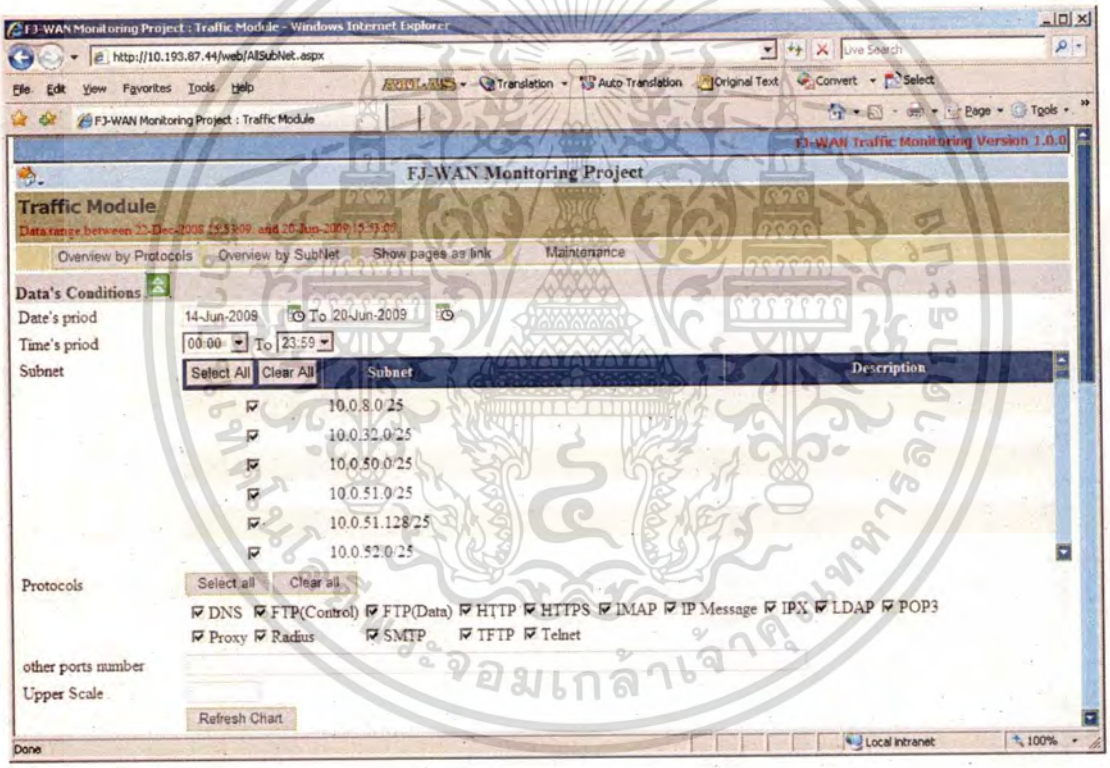
ตัวอย่างของการเข้าดูข้อมูลเมื่อผู้ใช้งานกดที่เมนูย่อย Subnet overview หน้าจอเว็บบราวเซอร์จะแสดงข้อมูลเช่นเดียวกับการดูของมูลแบบระบุซับเน็ต เพื่อให้ผู้ใช้งาน ได้เลือกข้อมูลที่ต้องการตรวจสอบในขั้นตอนต่อไปดังนี้

1. วันที่เริ่มต้นและวันที่สิ้นสุดสำหรับการดูข้อมูล โดยเบื้องต้นแอพพลิเคชันจะถูกเลือกให้แสดงข้อมูลในช่วง 1 สัปดาห์
2. เวลาเริ่มต้นและเวลาสิ้นสุดสำหรับการดูข้อมูล โดยเบื้องต้นแอพพลิเคชันจะถูกเลือกให้แสดงข้อมูลเวลาตั้งแต่ 0:00 นาฬิกา ถึง 23:59 นาฬิกา
3. ซับเน็ตที่ผู้ใช้งานต้องการจะตรวจสอบว่าในช่วงเวลาข้างต้น มีการใช้งานปริมาณย่านความถี่เท่าใด โดยเบื้องต้นแอพพลเคชันจะเลือกให้แสดงข้อมูลของซับเน็ตทั้งหมดขององค์กรอยู่แล้ว แต่ถ้าหากผู้ใช้งานต้องการที่จะระบุลงไปเฉพาะเจาะจงเพียงซับเน็ตใดซับเน็ตหนึ่ง หรือกลุ่มของซับเน็ตใด (ทั้งนี้เพราะในบางหน่วยงานหรือแผนก อาจมีการใช้ซับเน็ตมากกว่า 1 ตัว ซึ่งการเลือกเป็นกลุ่มของซับเน็ตจะสามารถตรวจสอบการใช้งานของหน่วยงานหรือแผนกนั้นๆได้) ก็สามารถที่จะเลือกเฉพาะได้เช่นกัน
4. โพรโตคอลที่ต้องการดูข้อมูล เพื่อเป็นการระบุลงไปว่าในกลุ่มของซับเน็ตในข้อบนผู้ใช้งานต้องการดูการใช้งานย่านความถี่ของเครือข่ายระยะไกลที่มีการติดต่อสื่อสารระหว่างกันด้วยโพรโตคอลได้บ้าง โดยเบื้องต้นจะมีโพรโตคอลที่ได้รับการเลือกให้

แสดงอยู่จำนวนหนึ่งแล้วเช่นโพรโตคอลDNS, FTP, SMTP, IMAP เป็นต้น ผู้ใช้งานสามารถที่จะเลือกโพรโตคอลเพิ่มเติมจากที่ถูกเลือกอยู่ หรือนำโพรโตคอลที่ถูกเลือกออก นอกจากนี้ยังสามารถระบุโพรโตคอลเพิ่มได้ หากในรายการโพรโตคอลไม่มีให้เลือก

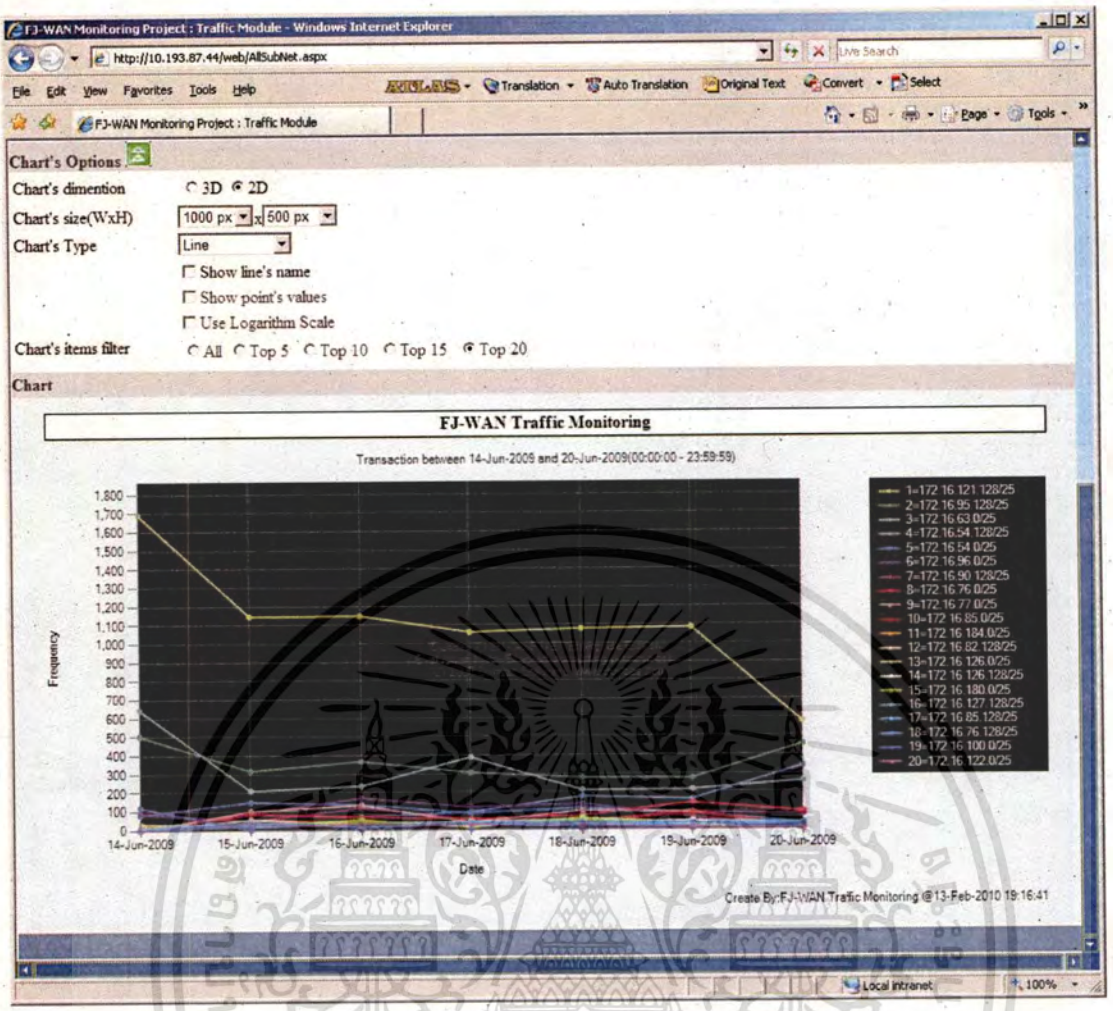
5. ลักษณะของกราฟที่ต้องการแสดง เช่นเป็นกราฟแบบ 2 มิติ หรือ 3 มิติ ขนาดของกราฟ (ขนาดความกว้างและความยาวของกราฟ) ที่ต้องการแสดงบนหน้าจอ และลักษณะของกราฟที่ต้องการให้แสดงเช่นเป็นกราฟวงกลม กราฟแท่ง หรือกราฟเส้น เป็นต้น

รูปที่ 4.18 แสดงหน้าจอของการกำหนดเงื่อนไขการแสดงการใช้ปริมาณย่านความถี่ของระบบเครือข่ายระยะไกลโดยกำหนดเงื่อนไขในการตรวจสอบแบบซับเน็ต



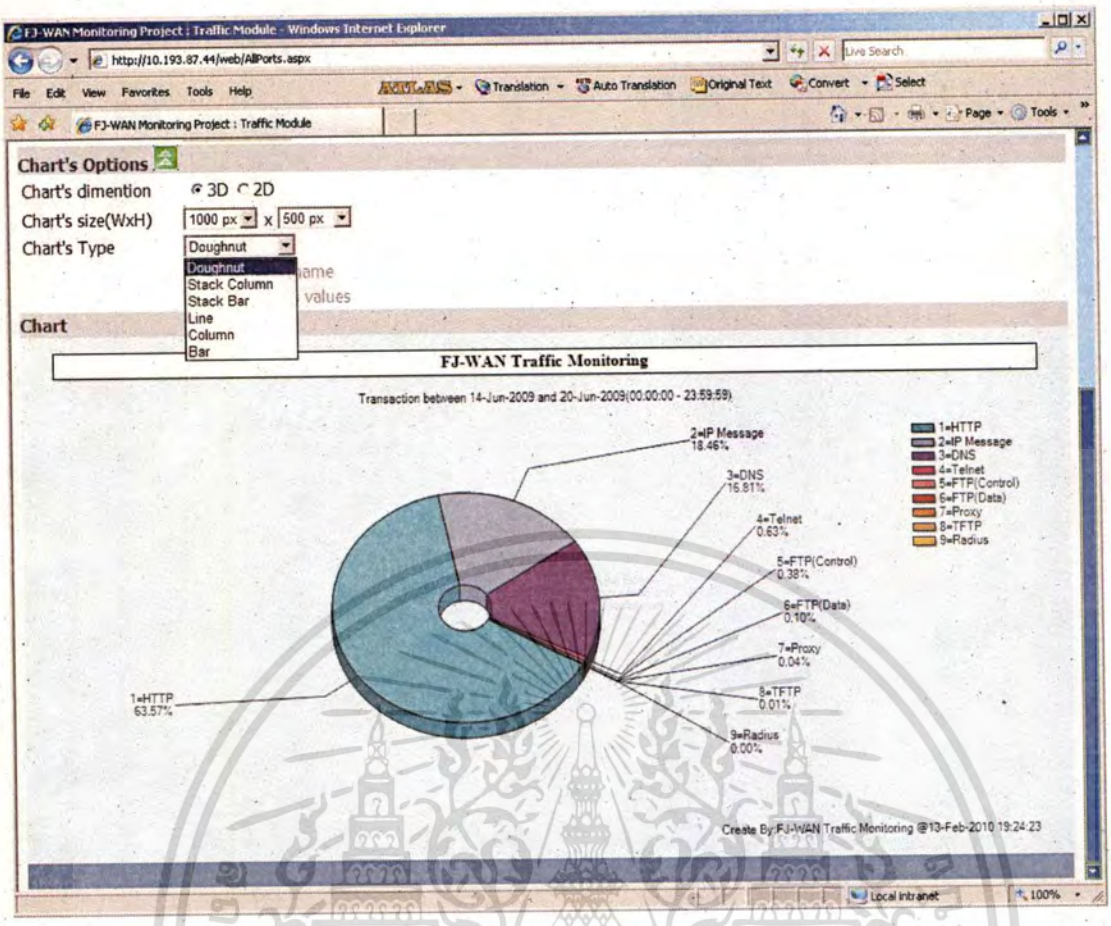

**รูปที่ 4.18** หน้าจอกำหนดเงื่อนไขเพื่อดูของมูลการใช้แบบซับเน็ต

เมื่อผู้ใช้งานได้ทำการเลือกค่าต่างๆครบหมดตามที่ต้องการและทำการกดปุ่ม Refresh Chart กราฟด้านล่างจะแสดงข้อมูลที่ได้จากเงื่อนไขข้างต้นที่ถูกส่งคำร้องขอไปยังเซิร์ฟเวอร์เพื่อประมวลผลและส่งผลลัพธ์กลับมา ดังตัวอย่างในรูปที่ 4.19 ซึ่งจะแสดงผลลัพธ์ที่ได้จากเงื่อนไขการแสดงซับเน็ตใช้ปริมาณย่านความถี่มากสุด 20 อันดับแรกในช่วงวันที่ 14 มิถุนายน ค.ศ.2009 ถึงวันที่ 20 มิถุนายน ค.ศ.2009



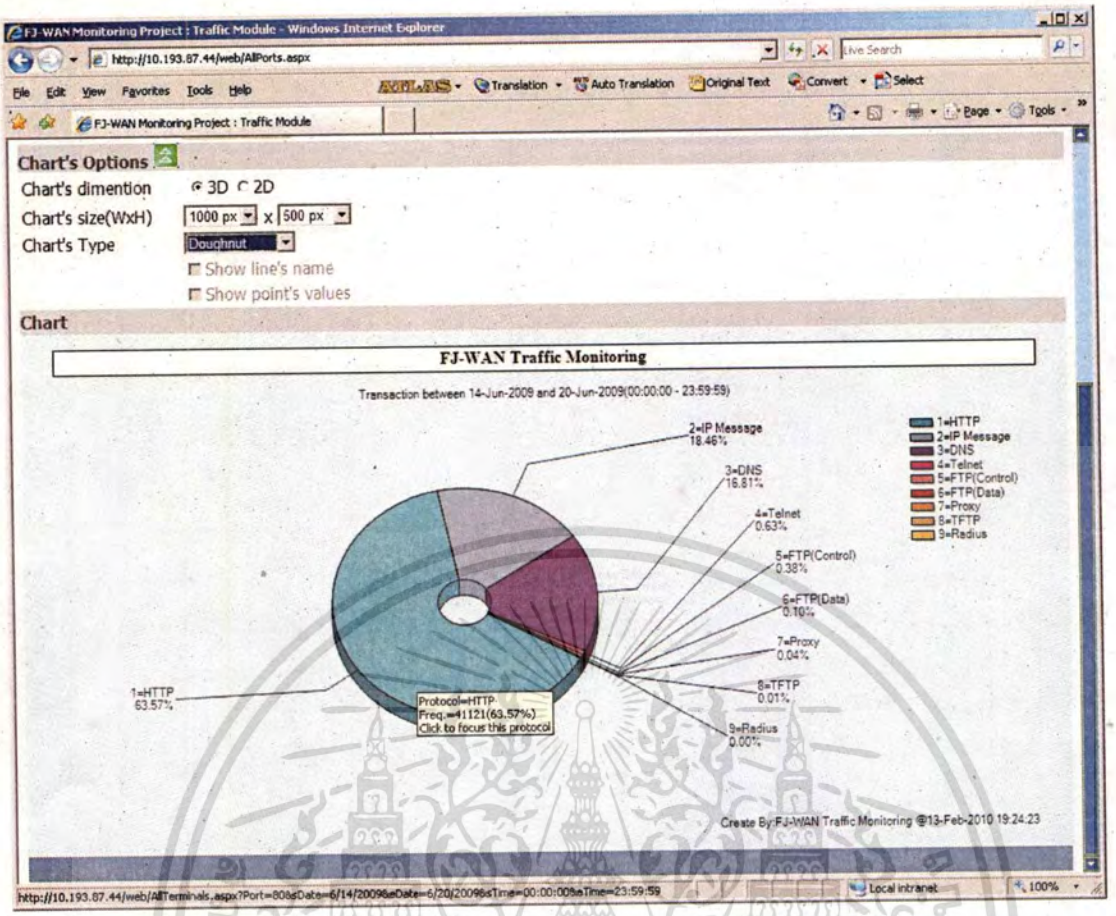

**รูปที่ 4.19** กราฟแสดงหน้าผลการใช้งานย่านความถี่โดยแบ่งตามซับเน็ต

สำหรับการเปลี่ยนแปลงลักษณะของกราฟที่ต้องการแสดงบนหน้าจอ ผู้ใช้งานสามารถเลือกลักษณะต่างๆได้จากชนิดของกราฟที่แอพพลิเคชันได้จัดเตรียมไว้ให้ นอกจากนี้ยังสามารถเลือกมิติในการนำแสดงกราฟได้เป็นแบบ 2 มิติ หรือแบบ 3 มิติได้อีกด้วย โดยในรูปที่ 4.20 จะแสดงการเลือกลักษณะของกราฟที่ต้องการแสดงบนหน้าจอให้เป็นแบบโดนัท (Doughnut) และแสดงลักษณะเป็นแบบ 3 มิติ



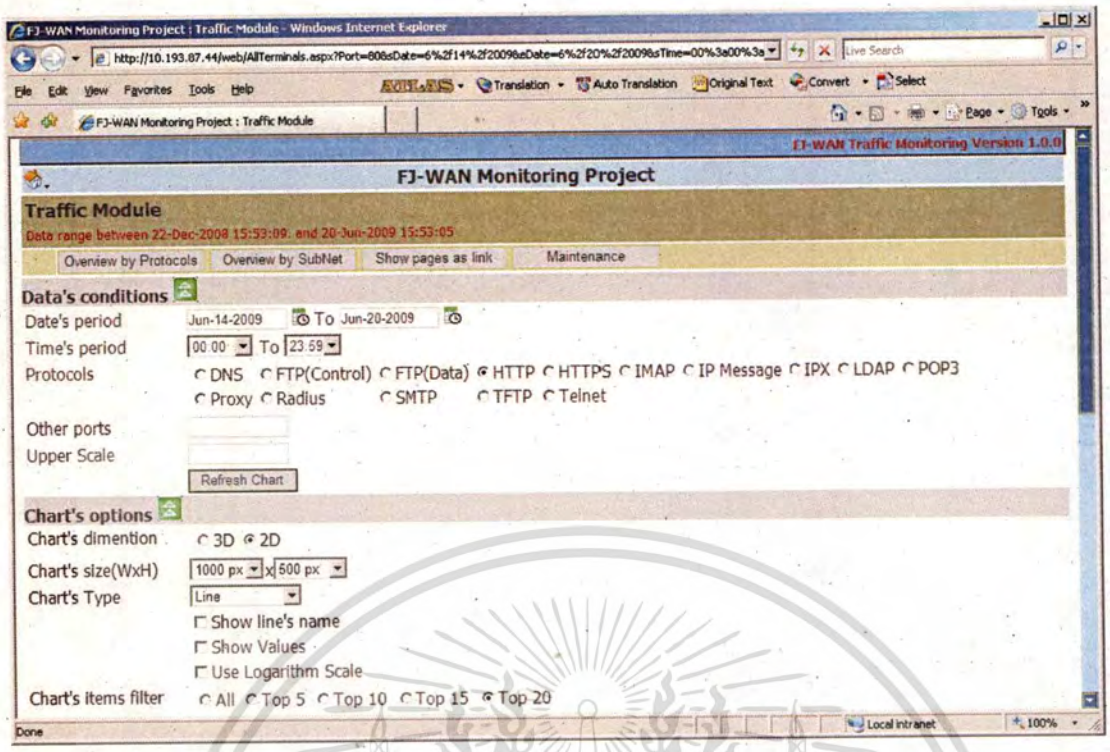

**รูปที่ 4.20** การเลือกลักษณะของกราฟในแบบต่างๆเพื่อให้แสดงบนหน้าจอ

สำหรับการดูรายละเอียดในเชิงลึกของข้อมูลที่แสดงในกราฟนั้น ผู้ใช้งานสามารถทำได้โดยคลิ๊ก (Click) บนตัวกราฟ ณ จุดที่ผู้ใช้งานต้องการตรวจสอบ เช่นการรูปที่ 4.21 ต้องการตรวจสอบพฤติกรรมการใช้งานโพรโตคอล HTTP ในช่วงวันที่ 14 มิถุนายน ค.ศ.2009 ถึงวันที่ 20 มิถุนายน ค.ศ.2009 เมื่อนำเมาส์ (Mouse) ไปวางบนตำแหน่งกราฟของโพรโตคอล HTTP ก็จะมีข้อมูลแสดงขึ้นมาให้ผู้ใช้งานได้ทราบว่าในช่วงเวลาดังกล่าว โพรโตคอล HTTP นี้มีความถี่ในการติดต่อสื่อสารเท่าใด (จำนวนครั้งที่ฝั่งต้นทางทำการติดต่อกับฝั่งปลายทาง) และคิดเป็นกี่เปอร์เซนต์ของการติดต่อสื่อสารทั้งหมด



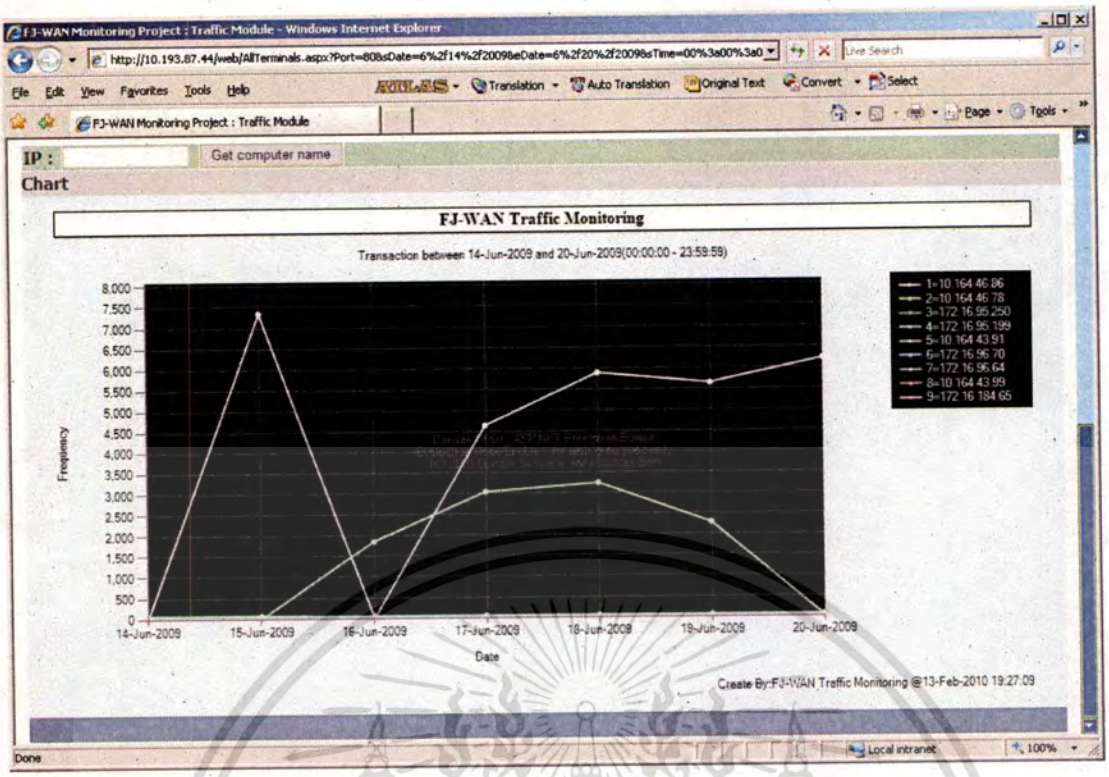

**รูปที่ 4.21** ข้อมูลการใช้งานของโพรโตคอล HTTP ในช่วงเวลาหนึ่ง

เมื่อผู้ใช้งานได้คลิ้กเข้าไปตรงโพรโตคอล HTTP เว็บบราวเซอร์จะเข้าไปสู่หน้าจอเพื่อให้เลือกลักษณะของกราฟที่ต้องการจะให้แสดงบนหน้าจอ โดยในที่นี้จะสังเกตุได้ว่า โพรโตคอลที่ถูกเลือก จะมีเพียงโพรโตคอล HTTP เท่านั้น ดังรูปที่ 4.22



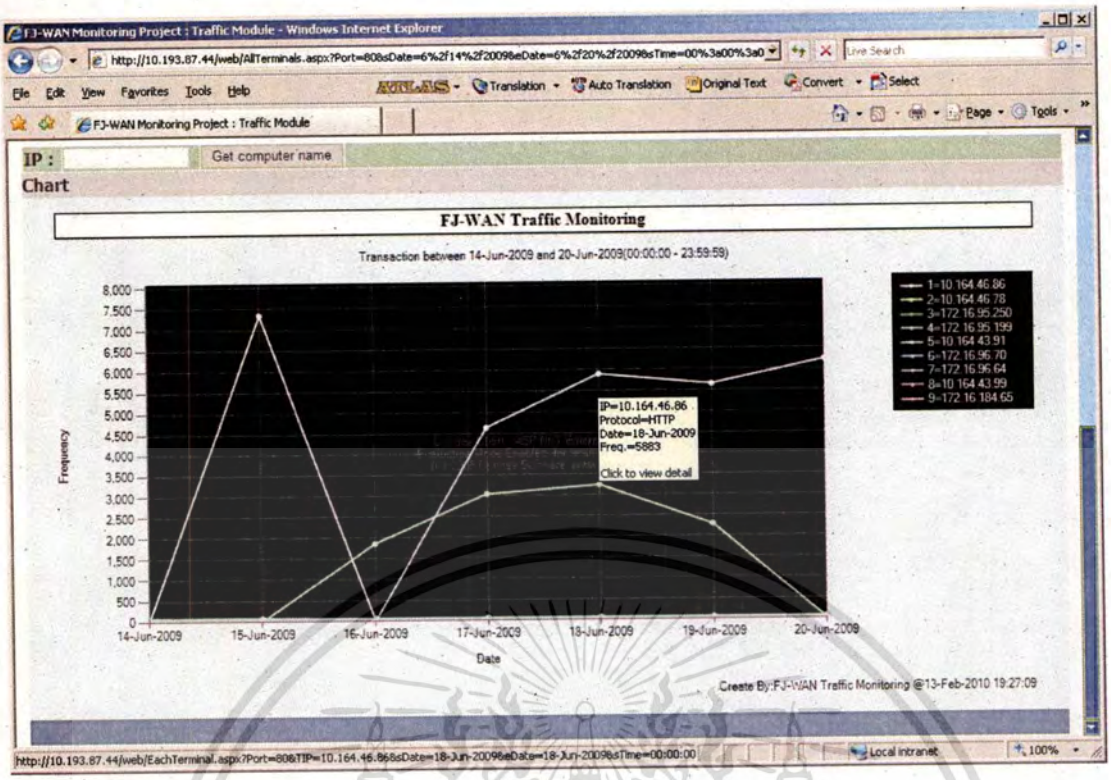

**รูปที่ 4.22** หน้าจอแสดงเงื่อนไขรายละเอียดของโพรโตคอล HTTP

เมื่อผู้ใช้กำหนดลักษณะของกราฟที่ต้องการให้แสดงเสร็จและกดปุ่ม Refresh Chart แล้ว กราฟด้านล่างจะแสดงข้อมูลที่ได้จากเงื่อนไขข้างต้นที่ถูกส่งคำร้องขอไปยังเซิร์ฟเวอร์เพื่อประมวลผลและส่งผลลัพธ์กลับมา ดังตัวอย่างในรูปที่ 4.23 ซึ่งจะแสดงผลลัพธ์ที่ได้จากเงื่อนไขการใช้โปรโตคอล HTTP ของเครื่องคอมพิวเตอร์ในองค์กรที่ใช้ปริมาณย่านความถี่มากสุด 20 อันดับแรกในช่วงวันที่ 14 มิถุนายน ค.ศ.2009 ถึงวันที่ 20 มิถุนายน ค.ศ.2009



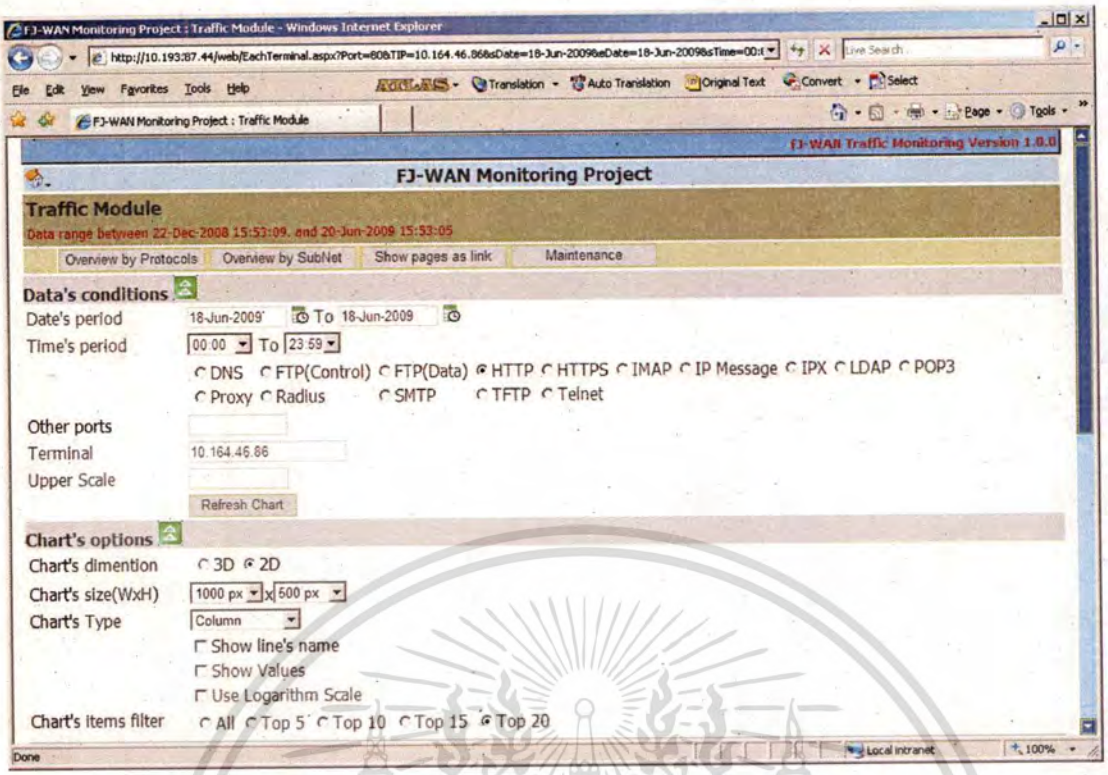

**รูปที่ 4.23** กราฟแสดงเครื่องคอมพิวเตอร์ที่ใช้โพรโตคอล HTTP บนเครือข่ายระยะไกล

หากผู้ใช้งานต้องการที่จะรู้รายละเอียด ณ จุดใดๆของกราฟ สามารถทำได้โดยวางเมาส์ไว้ ณ จุดนั้นๆ ดังเช่นรูปที่ 4.24 จะพบว่าในวันที่ 18 มิถุนายน ค.ศ.2009 เครื่องคอมพิวเตอร์ที่มีไอพีแอดเดรสเป็น 10.164.46.86 มีปริมาณการใช้โปรโตคอล HTTP บนเครือข่ายระยะไกลเป็นจำนวนทั้งสิ้น 5,883 ครั้ง และถ้าหากผู้ใช้งานต้องการทราบข้อมูลเชิงลึกอีกว่า ณ ช่วงเวลาที่กำหนดเครื่องคอมพิวเตอร์นี้ติดต่อกับเครื่องใดอยู่บ้างโดยใช้โปรโตคอล HTTP ก็สามารถทำได้โดยการคลิ้กที่ตำแหน่งนั้นๆ




**รูปที่ 4.24** ข้อมูลการใช้งานโพรโตคอล HTTP เครื่อง 10.164.46.86 ณ วันที่18 มิถุนายน ค.ศ.2009

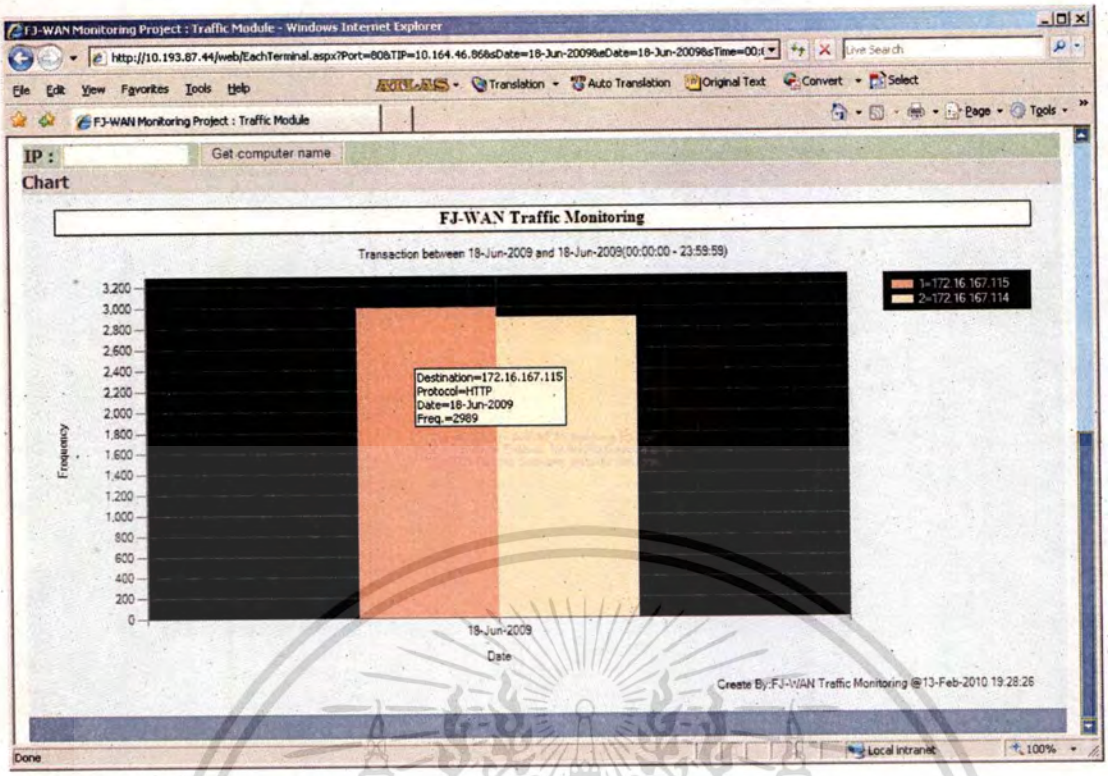
เมื่อผู้ใช้งานได้คลิ๊กเข้าไป ณ วันที่ต้องการตรวจสอบ เว็บบราวเซอร์จะเข้าไปสู่หน้าจอเพื่อให้เลือกลักษณะของกราฟที่ต้องการจะให้แสดงบนหน้าจอ โดยในที่นี้จะสังเกตุได้ว่าโพรโตคอลที่ถูกเลือก จะมีเพียงโพรโตคอล HTTP และเครื่องคอมพิวเตอร์จะระบุเป็นไอพีแอดเดรส 10.164.46.86 เท่านั้น ดังรูปที่ 4.25




**รูปที่ 4.25** หน้าจอแสดงเงื่อนไขรายละเอียดเครื่อง 10.164.46.86 ณ ช่วงเวลาที่กำหนด

เมื่อผู้ใช้กำหนดลักษณะของกราฟที่ต้องการให้แสดงเสร็จและกดปุ่ม Refresh Chart แล้ว กราฟด้านล่างจะแสดงข้อมูลที่ได้จากเงื่อนไขข้างต้นที่ถูกส่งคำร้องขอไปยังเซิร์ฟเวอร์เพื่อประมวลผลและส่งผลลัพธ์กลับมา ดังตัวอย่างในรูปที่ 4.26 ซึ่งจะแสดงผลลัพธ์ที่ได้จากเงื่อนไขเครื่องคอมพิวเตอร์ที่มีการติดต่อกับเครื่องคอมพิวเตอร์ที่มีไอพีแอดเดรส 10.164.46.86 และเป็นการติดต่อสื่อสารโดยใช้โปรโตคอล HTTPในวันที่ 18 มิถุนายน ค.ศ 2009 มากสุด 20 อันดับแรก

จากกราฟจะพบว่ามีเครื่องคอมพิวเตอร์อยู่เพียง 2 เครื่องที่มีการติดต่อกับเครื่องคอมพิวเตอร์ที่มีไอพีแอดเดรส 10.164.46.86 โดยโพรโตคอล HTTP ซึ่งได้แก่เครื่องคอมพิวเตอร์ที่มีไอพีแอดเดรส 172.16.167.114 และ 172.16.167.115 ซึ่งถ้าหากผู้ใช้งานต้องการที่จะรู้ว่าเครื่องคอมพิวเตอร์ดังกล่าวมีจำนวนครั้งในการติดต่อกับเครื่องเป้าหมายแรกที่กำหนดไว้ ก็สามารถทำได้โดยนำเมาส์ไปวาง ณ จุดของกราฟที่ตรงกับเครื่องคอมพิวเตอร์ไอพีแอดเดรสนั้นๆ ก็จะมีหน้าต่างแสดงผลออกมาให้ดู ดังตัวอย่างจะพบว่าเครื่องคอมพิวเตอร์ไอพีแอดเดรส 172.16.167.115 ได้ติดต่อกับเครื่องคอมพิวเตอร์เป้าหมายหลักคือ 10.164.46.86 โดยโพรโตคอล HTTP ณ วันที่ 18 มิถุนายน ค.ศ.2009 เป็นจำนวนทั้งสิ้น 2,989 ครั้ง

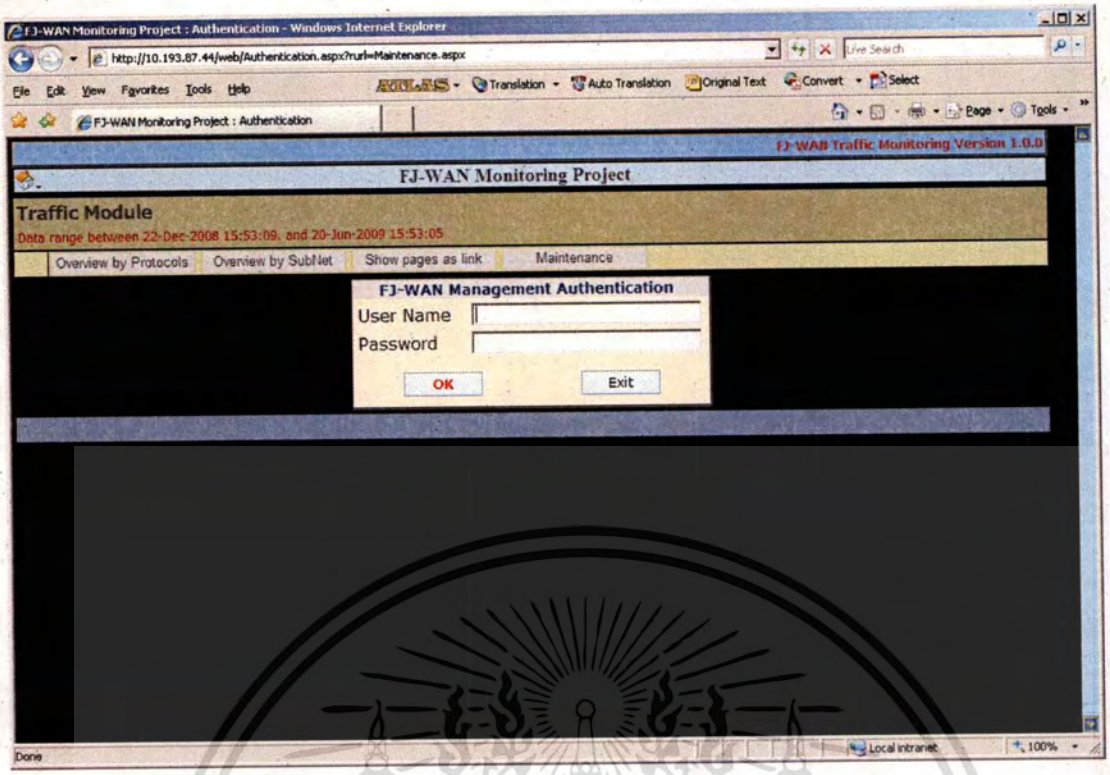



**รูปที่ 4.26** ข้อมูลเครื่องคอมพิวเตอร์ที่ติดต่อกับเครื่อง 10.164.46.86 โดยใช้งานโพรโตคอล HTTP ณ วันที่18 มิถุนายน ค.ศ.2009

### 4.2.4 Maintenance

เมนู Miantenance จะเกี่ยวข้องกับการแปลี่ยนแปลง แก้ไขค่าต่างๆของระบบ ดังนั้นผู้ที่สามารถเข้ามาแก้ไขได้ จะต้องมีสิทธิ์ในการเข้าถึงเท่านั้น โดยจะต้องเป็นผู้ที่มีชื่อและรหัสผ่านตรงตามที่ได้กำหนดไว้ในคอนฟิกูเรชันของแอพพลิเคชัน ซึ่งโดยทั่วไปก็จะคือผู้ดูแลระบบเครือข่ายนั่นเอง ชื่อและรหัสผ่านนี้สามารถแก้ไข เปลี่ยนแปลงได้ในคอนฟิกูเรชันไฟล์ของระบบ

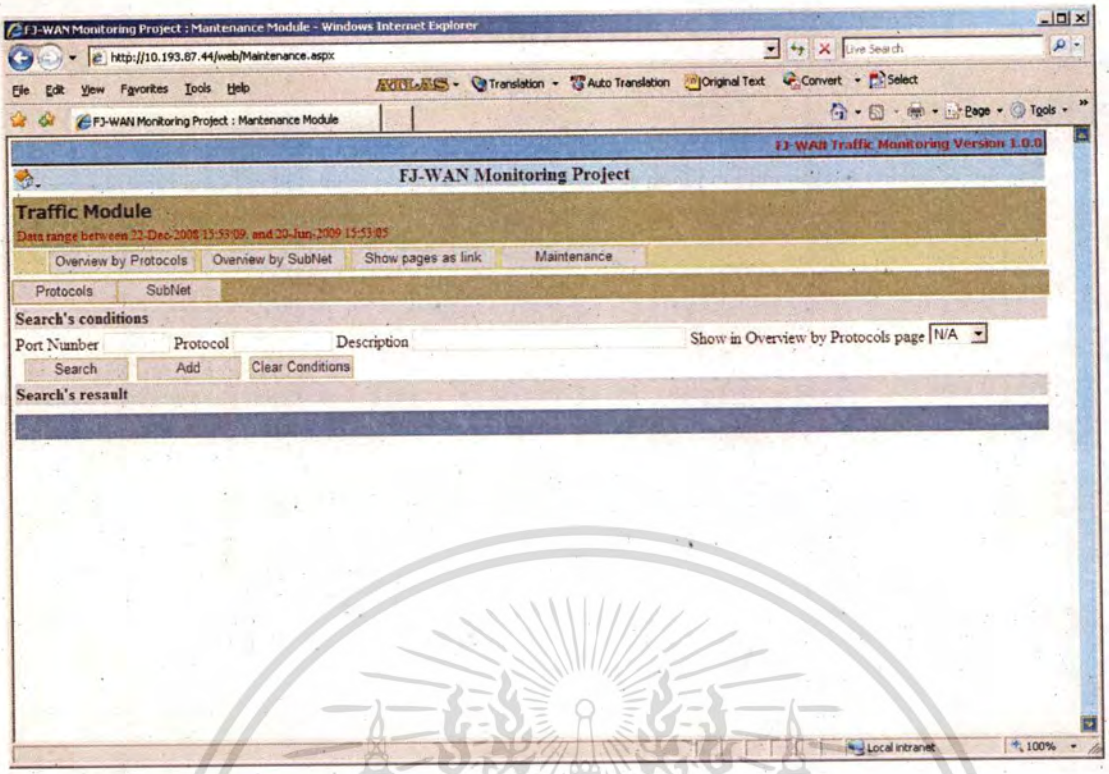
เมื่อผู้ใช้งานเข้าสู่เมนู Maintenance จะมีหน้าจอแสดงขึ้นมาเพื่อให้ใส่ชื่อและรหัสผ่านดังรูปที่ 4.27




**รูปที่ 4.27** หน้าจอกรอกชื่อและรหัสผ่านก่อนเข้าสู่เมนู Maintenance

หากผู้ใช้งานใส่ข้อมูลชื่อและรหัสผ่านถูกต้อง หน้าจอของระบบจะเข้าสู่หน้าจอการบำรุงรักษาระบบ ดังรูปที่ 4.28 โดยในการแก้ไขเปลี่ยนแปลงค่าของระบบนี้ ผู้ใช้งานที่มีสิทธิ์สามารถแก้ไขได้ 2 ส่วนด้วยกัน ได้แก่

1. การแก้ไขค่าโพรโตคอล
2. การแก้ไขค่าซับเน็ต

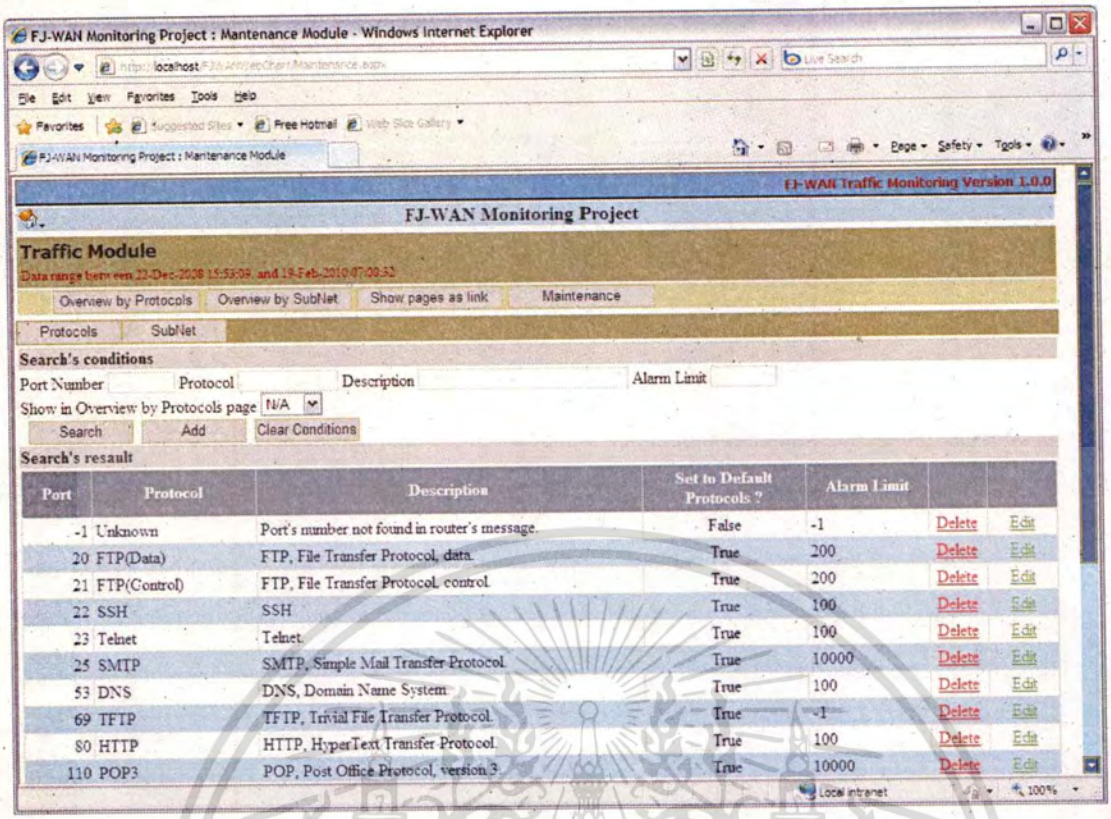



**รูปที่ 4.28** หน้าจอการบำรุงรักษาระบบ

1. Protocol maintenance

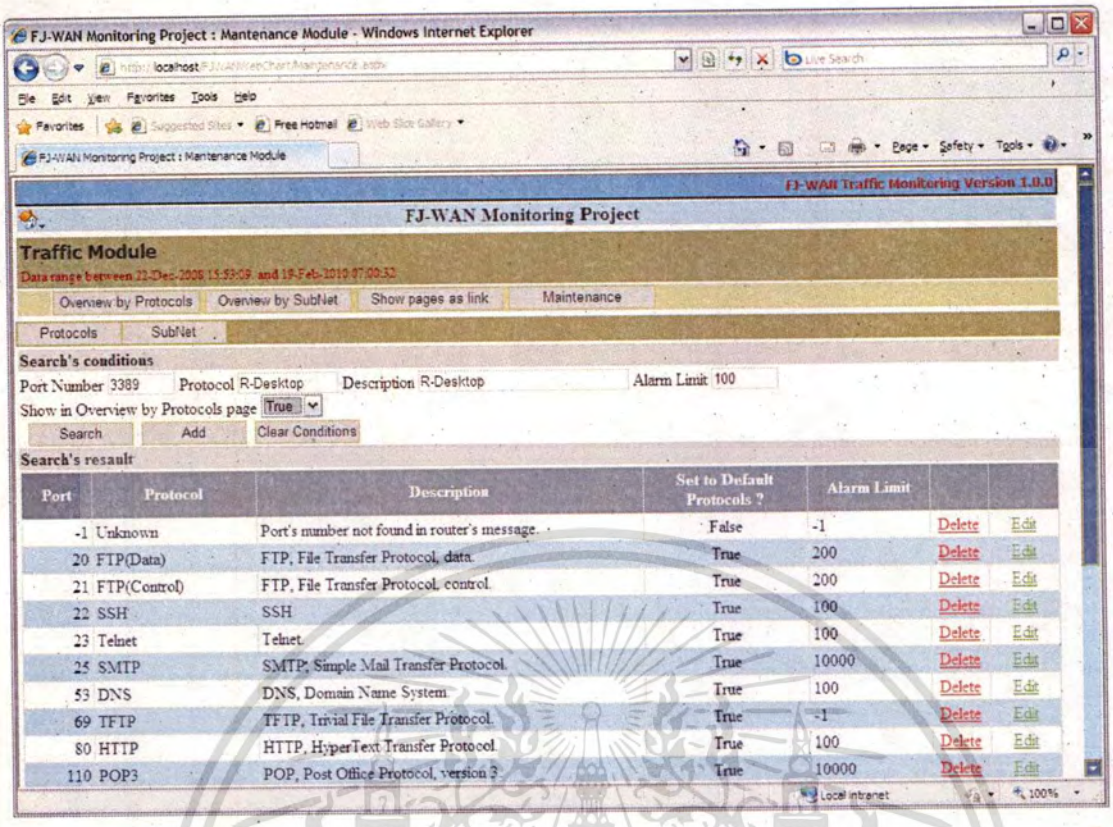
เมื่อผู้ใช้งานคลิ้กไปยังโพรโตคอล หน้าจอระบบจะแสดงค่าของโพรโตคอลที่ได้รับการใส่ค่าลงไปในระบบดังรูปที่ 4.29 โดยจะแสดง

- หมายเลขพอร์ต (Port number) เป็นหมายเลขพอร์ตของโพรโตคอลแต่ละตัวที่ใช้ในการติดต่อสื่อสาร
- ชื่อโพรโตคอล (Protocol) ชื่อมาตรฐานของโพรโตคอลนั้นๆ
- คำอธิบาย (Description) ส่วนอธิบายเพิ่มเติมของโพรโตคอล
- Set to default protocol? โพรโตคอลที่มีการกำหนดให้มีค่าเป็น True จะถูกเลือกโดยอัตโนมัติเมื่อผู้ใช้งานต้องการดูข้อมูลแบบแบ่งเป็นโพรโตคอลของการใช้งานของย่านความถี่แบบ
- Alarm limit กำหนดค่าจำกัดเบื้องต้นสำหรับความถี่ในการติดต่อสื่อสารโดยใช้โพรโตคอลนั้นๆ
- ลบ (Delete) ลบโพรโตคอลรวมทั้งรายละเอียดออกจากคอนฟิกูเรชันของระบบ
- แก้ไข (Edit) ผู้ใช้งานต้องการเปลี่ยนแปลงค่าต่างๆของโพรโตคอล



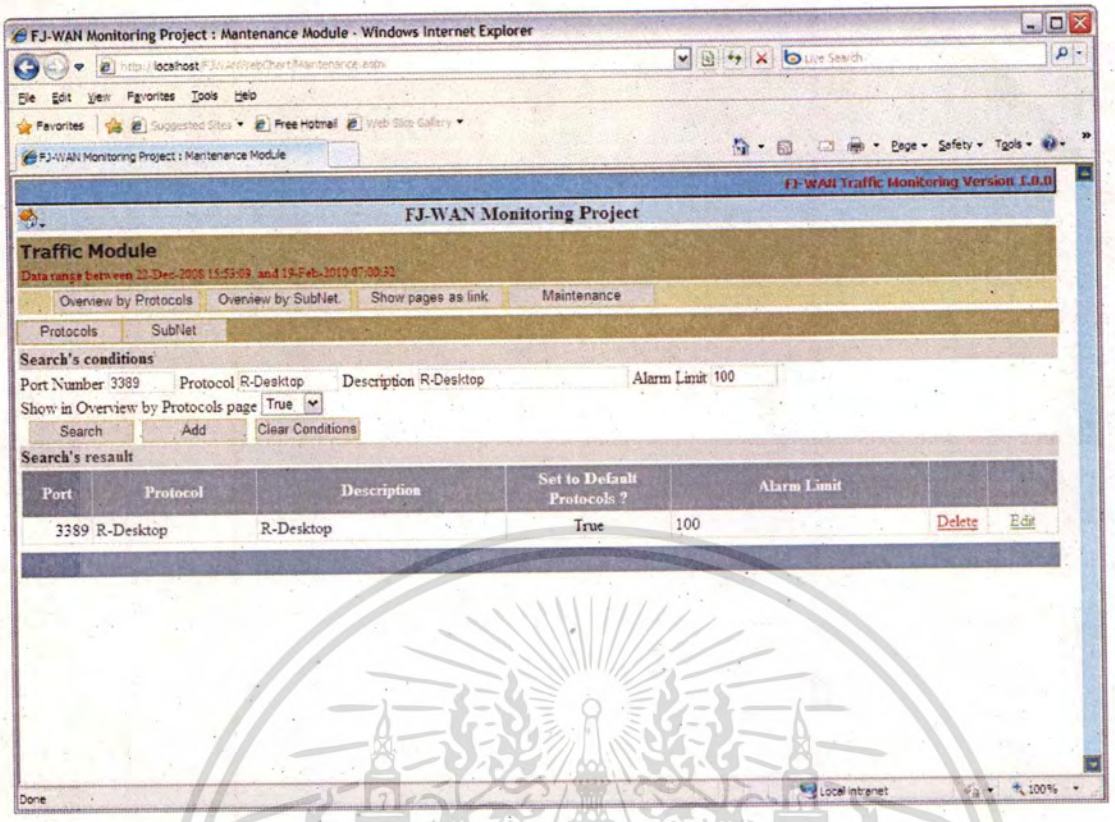

**รูปที่ 4.29** หน้าจอแสดงโพรโตคอลเบื้องต้นที่กำหนดไว้

สำหรับโพรโตคอลที่ยังไม่ได้รับการใส่ค่าลงในระบบ ผู้ดูแลระบบเครือข่ายสามารถเพิ่มเติมลงไปได้ โดยกรอกค่าต่างๆที่ต้องการลงในช่องดังตัวอย่างรูปที่ 4.30 ผู้ดูแลระบบใส่ค่าโพรโตคอล SSH เข้าไปเพิ่มในระบบ




**รูปที่ 4.30** การเพิ่มค่าโพรโตคอลเข้าในระบบ

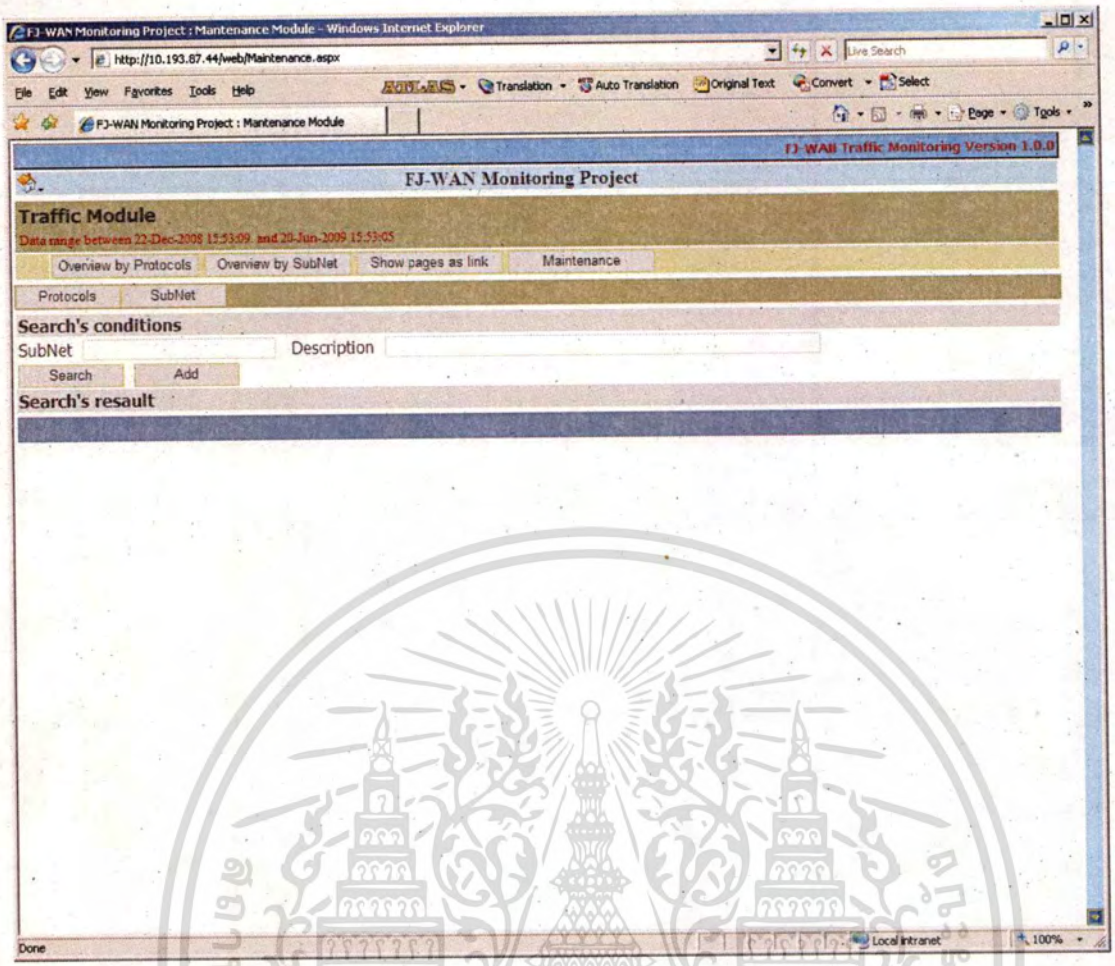
เมื่อกรอกข้อมูลครบแล้ว ผู้ใช้งานจะต้องคลิ้กที่ปุ่ม Add เพื่อเพิ่มรายละเอียดที่กรอกไปในระบบ ซึ่งหน้าจอจะแสดงรายละเอียดที่เพิ่มไป ดังรูปที่ 4.31




**รูปที่ 4.31** ข้อมูลโพรโตคอลที่เพิ่มเข้าไปในระบบ

2. Subnet maintenance

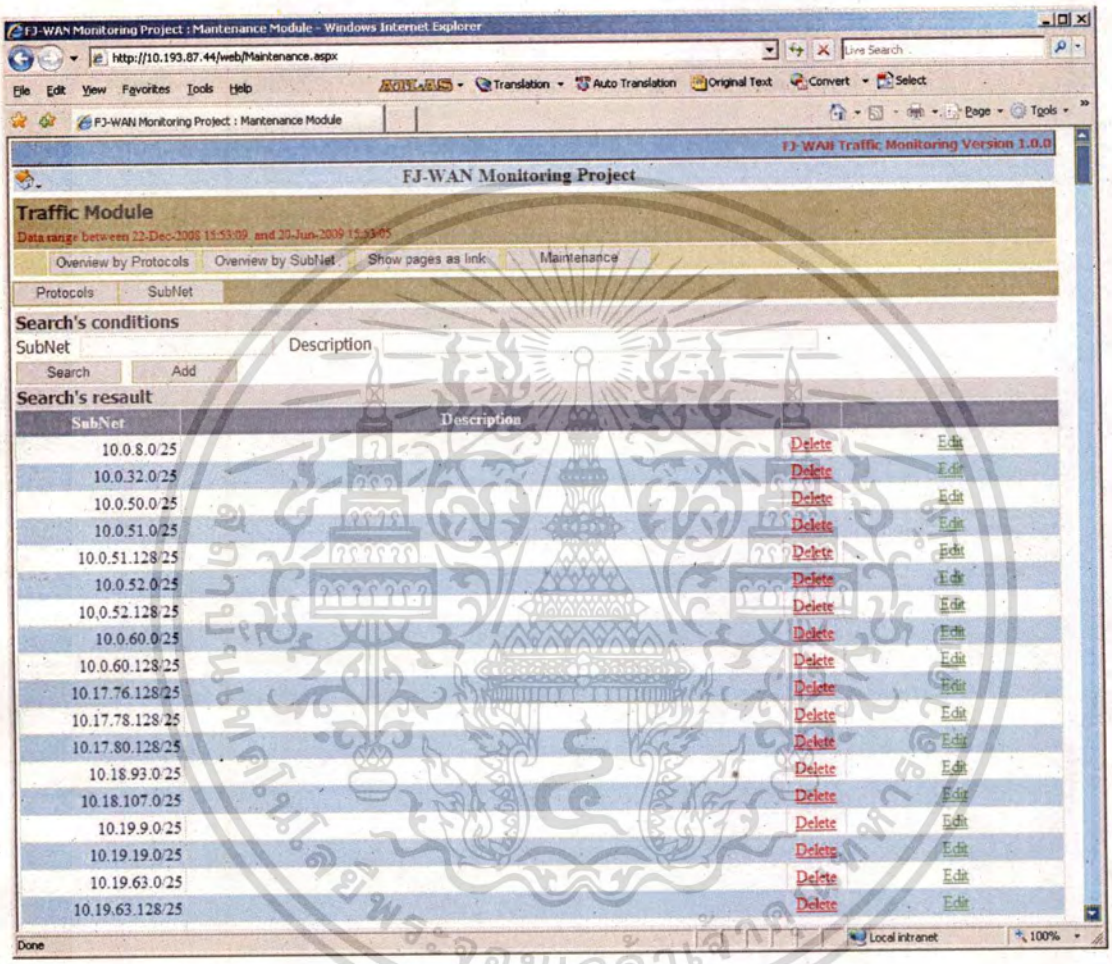
เมื่อผู้ใช้งานคลิ้กไปยังซับเน็ต หน้าจอระบบมีเมนูย่อยให้ผู้ใช้งานเลือกอยู่ 2 ส่วนคือ ส่วนการค้นหา (Search) และส่วนเพิ่มเติม (Add) ดังรูปที่ 4.32




**รูปที่ 4.32** เมนูย่อยในส่วนการบำรุงรักษาซับเน็ต

หากผู้ใช้งานต้องการค้าหาซับเน็ตทั้งหมดขององค์กรที่ได้รับการใส่ข้อมูลเข้าไปในระบบ เมื่อผู้ใช้งานคลิ้กที่แถบ Search หน้าจอจะแสดงค่าของซับเน็ตที่ได้รับการใส่ค่าลงไปในระบบดังรูปที่ 4.33 โดยจะแสดง

- ชื่อซับเน็ต (Subnet) ค่าซับเน็ตต่างๆขององค์กร
- คำอธิบาย (Description) ส่วนอธิบายเพิ่มเติมของโพรโตคอล




**รูปที่ 4.33** ซับเน็ตขององค์กรที่ใส่ลงในระบบ

ในหน้าจอนี้ผู้ใช้งานสามารถลบค่าและรายละเอียดของซับเน็ตนั้นๆได้ โดยคลิ้กที่ Delete หรือหากต้องการแก้ไขเปลี่ยนแปลง เช่นเพิ่มคำอธิบาย แก้ไข Subnet mask ก็สามารถทำได้โดยคลิ้กที่ Edit

# บทที่ 5
# สรุปผลและข้อเสนอแนะ

บทนี้จะกล่าวสรุปถึงภาพโดยรวมของการศึกษาและพัฒนาระบบตรวจสอบทราฟฟิกของเครือข่ายสำหรับข้อมูลที่ถูกส่งผ่านบนเครือข่ายระยะไกล ประโยชน์ที่ได้รับจากการพัฒนาระบบ ปัญหาและอุปสรรคของการพัฒนาระบบ และข้อเสนอแนะสำหรับต่อยอดของการพัฒนาระบบต่อไปในอนาคต

## 5.1 สรุปผลการดำเนินการพัฒนาระบบ

ระบบตรวจสอบทราฟฟิกของเครือข่ายสำหรับข้อมูลที่ถูกส่งผ่านบนเครือข่ายระยะไกลที่พัฒนาขึ้นมานี้เกิดความต้องการในการตรวจสอบการใช้งานของเครือข่ายขององค์กรเพื่อให้ใช้ย่านความถี่ได้อย่างมีประสิทธิภาพและตรงตามวัตถุประสงค์ในการเชื่อมต่อเครือข่าย ซึ่งเมื่อพัฒนาระบบเป็นที่เรียบร้อยและเริ่มให้ผู้ใช้งานทำการทดสอบและใช้งานจริง ปรากฏว่าระบบที่พัฒนาขึ้นมานี้ ตรงตามความต้องการของผู้ใช้งานทุกส่วน ไม่ว่าจะเป็นฝ่ายบริหาร ผู้ดูแลระบบเครือข่าย หรือแม้กระทั่งผู้ใช้งานทั่วไป ซึ่งสามารถสรุปความสามารถของระบบได้ดังนี้

1. ง่ายสำหรับผู้ดูแลระบบในการแก้ไขเปลี่ยนแปลงค่าของซับเน็ตและโพรโตคอล เพื่อให้ตรงตามการใช้งานตามความเป็นจริงขององค์กร
2. สามารถเลือกลักษณะของกราฟที่ใช้ในการแสดงบนหน้าจอคอมพิวเตอร์หลายรูปแบบ ทำให้ผู้ใช้งานเลือกลักษณะต่างๆได้ตามความต้องการให้สอดคล้องกับการตรวจสอบ ณ เวลานั้นๆ
3. ระบบสามารถตรวจสอบได้ว่า ณ ขณะช่วงเวลาหนึ่ง มีโพรโตคอลใดที่ถูกใช้ในการติดต่อสื่อสารระหว่างองค์กรโดยผ่านทางเครือข่ายระยะไกลได้ โดยสามารถเรียงลำดับจากโพรโตคอลที่ถูกใช้มากสุดถัดไปเรื่อยๆ พร้อมทั้งบอกความถี่ที่ถูกใช้งาน
4. ระบบสามารถตรวจสอบได้ว่า ณ ขณะช่วงเวลาหนึ่ง ซับเน็ตใดบ้างที่ใช้ย่านความถี่ของเครือข่ายระยะไกลในการติดต่อสื่อสาร ซึ่งสามารถตรวจสอบรายละเอียดลงไปถึงคู่ไอพีแอดเดรสต้นทางและไอพีแอดเดรสปลายทางที่กำลังติดต่อสื่อสารกันอยู่
5. ผู้บริหารสามารถตรวจสอบได้ว่าในหน่วยงานของตน มีการใช้ประสิทธิภาพของย่านความถี่ของเครือข่ายระยะไกลได้ตรงตามหน้าที่ของหน่วยงานนั้นๆหรือไม่ โดยสามารถตรวจสอบได้จากข้อมูลการใช้งานของซับเน็ต

6. ผู้ดูแลระบบสามารถตรวจสอบได้ว่าการติดต่อสื่อสารของเครือข่ายระยะไกลขององค์กรมีสิ่งผิดปกติเกิดขึ้นหรือไม่ เช่นสามารถตรวจสอบได้จากโพรโตคอลที่ผิดปกติที่เกิดขึ้นมาจากข้อมูลการตรวจจับ หรือความถี่ที่ใช้งานของโพรโตคอลหรือความถี่ในการสื่อสารที่เพิ่มขึ้นอย่างผิดปกติ ซึ่งอาจเป็นการถูกโจมตีจากผู้ไม่ประสงค์ดี หรือเครื่องคอมพิวเตอร์ในองค์กรติดไวรัสคอมพิวเตอร์ก็เป็นได้
7. ผู้ใช้งานไม่จำเป็นต้องติดตั้งแอพพลิเคชันเพิ่มเติมเมื่อต้องการใช้ระบบนี้เพราะจะใช้เพียงเว็บบราวเซอร์ในส่วนของผู้ใช้งานเท่านั้น ทำให้ไม่เสียเวลาในการติดตั้ง
8. ระบบมีการแบ็กอัพ (Backup) ข้อมูลล็อกไฟล์ไปไว้ ณ แบ็กอัพไดเรกทอรีเพื่อป้องกันการเกิดปัญหาหากข้อมูลในฐานข้อมูลเสียหายได้ โดยหากเกิดปัญหาขึ้นผู้ดูแลระบบสามารถนำข้อมูลที่แบ็กอัพกลับมารีจีสเตอร์ในระบบโดยใช้แอพพลิเคชันที่มีอยู่ได้

## 5.2. ประโยชน์ที่ได้รับจากการพัฒนาระบบ

จากการพัฒนาระบบตรวจสอบทราฟฟิกของเครือข่ายสำหรับข้อมูลที่ถูกส่งผ่านบนเครือข่ายระยะไกลตั้งแต่เริ่มต้น สามารถแยกประโยชน์ที่ได้รับออกเป็น

1. ประโยชน์ที่ผู้พัฒนาระบบได้รับ
   - ได้ศึกษาการคอนฟิกูเรชันสวิตซ์ยี่ห้อ Extreme เพื่อใช้เป็นอุปกรณ์ในการส่งล็อกมาเก็บยังระบบ
   - ได้ศึกษาการติดตั้งและออกแบบฐานข้อมูลโดยใช้ Oracle version 9.2.0.1 เป็น DBMS
   - เพิ่มทักษะในการพัฒนาโปรแกรมด้วยภาษา VB.NET
   - เพิ่มทักษะในการออกแบบและพัฒนาเว็บด้วยภาษา ASP.NET
   - ได้รับความรู้และเทคโนโลยีใหม่ๆอันเกิดขึ้นจากการพัฒนาระบบ
   - ได้รับความรู้ด้านการวิเคราะห์และออกแบบระบบ
2. ประโยชน์ที่ผู้ใช้งานระบบได้รับ
   - สามารถคาดการณ์การใช้ย่านความถี่ของเครือข่ายระยะไกลได้ โดยอาศัยข้อมูลการใช้งาน ณ ปัจจุบัน เพื่อเตรียมพร้อมสำหรับการออกแบบระบบถ้าหากมีความต้องการใช้งานเพิ่มขึ้นในอนาคต
   - สามารถป้องกันการถูกโจมตีในเครือข่ายได้ โดยทำการสร้าง Access Control List ขึ้นมาเพื่อระงับการใช้พอร์ตหรือโพรโตคอลที่คาดว่าเป็นสาเหตุของปัญหา
   - ลดค่าใช้จ่ายในการสั่งซื้อแอพพลิเคชันเพื่อมาตรวจสอบระบบ เนื่องจากองค์กรสามารถพัฒนาได้เอง

- สามารถดูแนวโน้มการใช้งานของระบบเครือข่ายได้จากกราฟที่แสดง

## 5.3 ปัญหาและอุปสรรคในการพัฒนาระบบ

ปัญหาและอุปสรรคที่เกิดขึ้นในขณะพัฒนาระบบ สามารถสรุปได้ดังนี้

1. ผู้พัฒนาระบบมีทักษะทางด้านการพัฒนาแอพพลิเคชันด้วยภาษา VB.NET และ ASP.NET น้อย ทำให้ต้องเสียเวลาในการศึกษาคำสั่งและรูปแบบของภาษาอยู่นาน
2. เซิร์ฟเวอร์ที่ใช้งานจะต้องมีขนาดความจุของฮาร์ดดิสก์ (Harddisk) ที่มาก ทั้งนี้เพราะขนาดล็อกไฟล์ที่ตัวสวิตซ์ส่งมาจะมีข้อมูลที่เยอะมาก ทำให้ต้องหาฮาร์ดดิสก์ขนาดความจุที่สูง
3. เนื่องจากเซิร์ฟเวอร์ที่ใช้ในการพัฒนาระบบ ทำหน้าที่เป็นทั้งดาต้าเบสเซิร์ฟเวอร์ (Database server) และเว็บเซิร์ฟเวอร์ (Web server) จึงทำให้ต้องใช้เซิร์ฟเวอร์ที่มีสเปก (Spec) ที่สูง เพื่อรองรับต่อกระบวนการต่างๆที่เกิดขึ้นภายในระบบได้ และตอบสนองต่อผู้ใช้งานได้อย่างรวดเร็ว
4. การพัฒนาระบบนี้ทำอยู่บนสภาพแวดล้อม (Environment) ของระบบเครือข่ายจริง ดังนั้นการแก้ไขหรือเปลี่ยนแปลงคอนฟิกูเรชันของตัวเครือข่าย เช่นการเพิ่มคอนฟิกูเรชันของสวิตซ์จะต้องทำด้วยความระมัดระวังเพื่อไม่ให้กระทบถึงค่าเดิมที่ได้คอนฟิกูเรชันไว้
5. หากมีการเปลี่ยนแปลงซับเน็ตของระบบเครือข่ายที่ใช้งาน เช่นยกเลิกการใช้ซับเน็ตหรือมีการเพิ่มซับเน็ตขึ้นมา ผู้ดูแลระบบจะต้องทำการแก้ไขค่าซับเน็ตของระบบด้วยเช่นกัน มิฉะนั้นจะทำให้ข้อมูลที่แสดงบนกราฟไม่ครบถ้วนหรือผิดพลาด
6. เนื่องจากระบบนี้ใช้สวิตซ์ Extreme รุ่น Summit-48si เป็นตัวส่งล็อกเข้ามาเก็บยัง Syslog server ซึ่งข้อจำกัดของสวิตซ์รุ่นนี้คือล็อกที่เก็บจะเป็น Inbound คือเป็นข้อมูลที่เข้ามายังสวิตซ์เท่านั้น จึงทำให้สามารถตรวจสอบการใช้ข้อมูลของเครือข่ายได้ในทิศทางเดียวเท่านั้น

## 5.4 ข้อเสนอแนะและแนวทางในการพัฒนาเพิ่มเติม

1. ควรเพิ่มความสามารถในการรักษาความมั่นคงปลอดภัยของระบบ โดยนำเซิร์ฟเวอร์ไปผูกกับ Active Directory ขององค์กร เพื่อให้ง่ายในการกำหนดสิทธิ์ในการเข้าถึงระบบของผู้ใช้งานในระดับต่างๆได้ง่ายขึ้น รวมทั้งเพื่อป้องกันไม่ให้บุคคลภายนอกองค์กรสามารถเข้าถึงข้อมูลของระบบได้

2. หากในอนาคตมีการเปลี่ยนสวิตซ์จาก Extreme ไปเป็น Cisco ระบบจะสามารถตรวจสอบล็อกได้ทั้งขาเข้า (Inbound) และขาออก (Outbound) ของสวิตซ์ ทั้งนี้เพราะสวิตซ์ Cisco รองรับการเก็บล็อกทั้งสองประเภทอยู่แล้ว ทำให้ผู้ดูแลระบบสามารถตรวจสอบการใช้งานของเครือข่ายได้ละเอียดขึ้นกว่าเดิมได้
3. การใช้ Oracle Enterprise Edition เป็น DBMS ในการจัดการฐานข้อมูล เป็นสิ่งที่สิ้นเปลืองในด้านของการลงทุนค่าลิขสิทธิ์ ดังนั้นหากเปลี่ยนมาใช้ DBMS ที่ราคาต่ำกว่าจะช่วยลดต้นทุนค่าใช้จ่ายขององค์กรลงได้
4. ควรเพิ่มความสามารถในการส่งเมล์แจ้งไปยังผู้ดูแลระบบ โดยเป็นรายงานสรุปการใช้งานในแต่ละวัน พร้อมทั้งกราฟแสดงเพื่อให้ผู้ดูแลระบบสามารถวิเคราะห์ข้อมูลได้
5. หากผู้ดูแลระบบมีสิทธิ์ในการแก้ไขคอนฟิกูเรชันของเราเตอร์ที่เชื่อมต่อของเครือข่ายระยะไกลให้สามารถส่งล็อกมายัง Syslog server ได้ จะช่วยให้ข้อมูลล็อกที่ได้ตรงตามวัตถุประสงค์ของการพัฒนาระบบ

# บรรณานุกรม


ญาณี กาชัย. 2000. จัดการระบบฐานข้อมูลอย่างมืออาชีพ Oracle DBA. กรุงเทพฯ : Infopress Developer Book

ทวีชัย หงษ์สุมาลย์. 2545. **อินไซท์ ASP และ ASP.NET ฉบับสมบูรณ์**. กรุงเทพฯ : Provision

ภูวดล ด่านระหาญ. 2544. **ทำความรู้จัก Syslogd**. [Online]. Avaliable : http://www.thaicert.org/paper/unix_linux/linux_syslog.php.

อดิสร ขาวสังข์. 2549. **ตัวอย่างการใช้งาน Syslog Server เพื่อรับ log จาก Cisco Router**. [Online]. Available : http://howto.south.cattelecom.com/router/cisco/syslog/kiwi_syslog_server.html.

Extreme Network. 2009. **SUMMIT48SI**. [Online]. Available : http://www.extremenetworks.com/products/summit-48si.aspx.

James F. Kurose. 2005. **Computer Networking A Top-Down Approach Featuring the Internet, Third Edition**. New York. Addision-Wesley

Javvin Technologies, Inc.. 2009. **Syslog Protocol**. [Online]. Available : http://www.javvin.com/SyslogProtocol.html.

John W. Satinger. 2004. **System Analysis and Design in a Changing World, Third Edition**. New York. Thomson Course Technology

Kiwi . 2009. **Kiwi Syslog Server**. [Online]. Avaliable : http://www.kiwisyslog.com/kiwi-syslog-server-overview/.

Network Dictionary. 2010. **Syslog Protocol**. [Online]. Available : http://www.networkdictionary.com/protocols/SyslogProtocol.php.

Perter Rob. 2004. **Database Systems : Design, Implementation, and Management, Sixth Edition**. New York. Thomson Course Technology

Philip Miller. 1997. **TCP/IP EXPLAINED**. USA. Digital Press

R. Gerhards. 2009. **The Syslog Protocol**. [Online]. Available : http://tools.ietf.org/search/rfc5424.

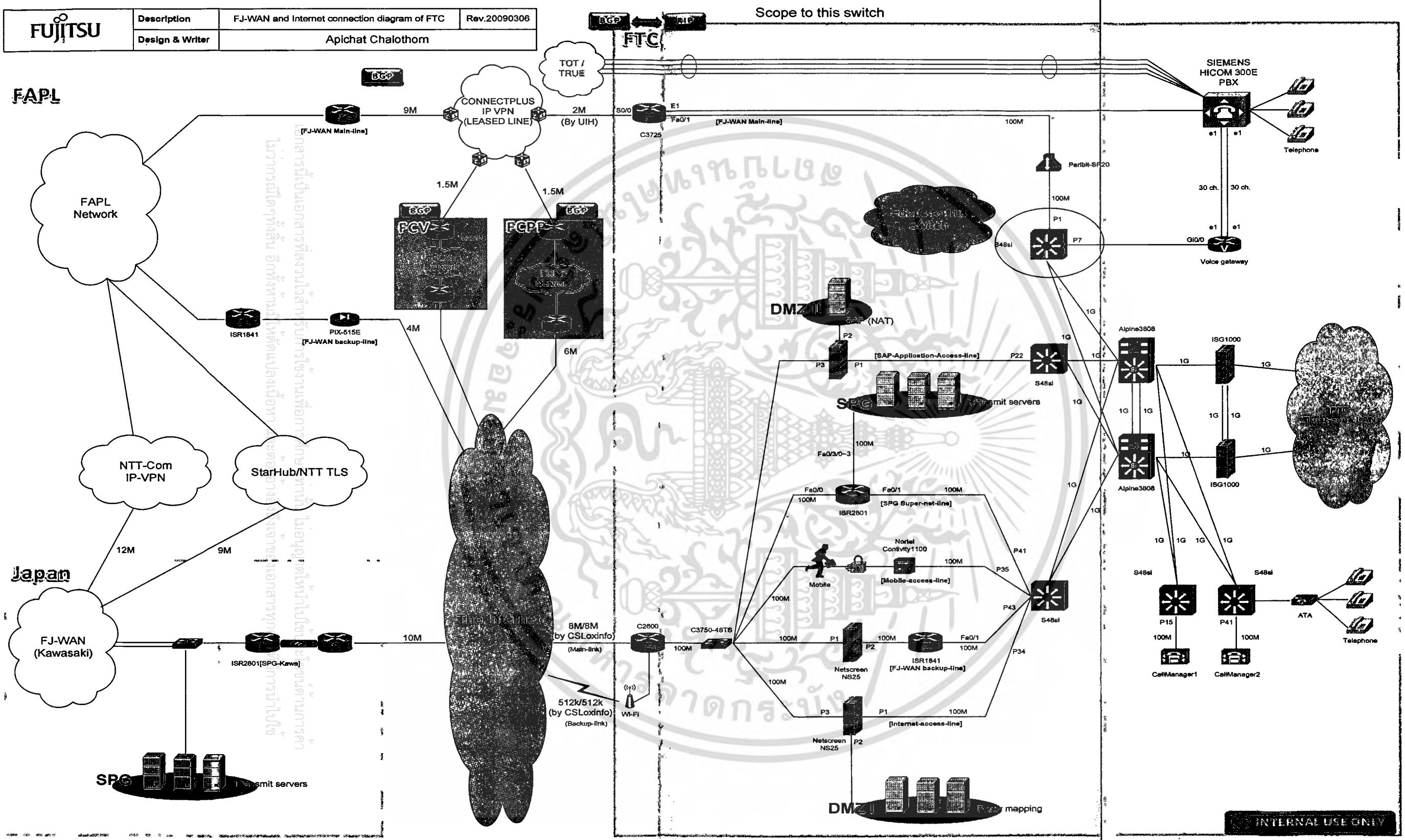
Wikipedia. 2010. **Syslog**. [Online]. Avaliable : http://en.wikipedia.org/wili/Syslog.

# ภาคผนวก

## 1. แผนภาพการเชื่อมต่อเระบบครือข่ายขององค์กร

การเชื่อมต่อเครือข่ายภายในบริษัทฟูจิตสึ (ประเทศไทย) จำกัด กับระบบเครือข่ายระยะไกลของบริษัทในเครือฟูจิตสึนั้น สามารถแสดงได้ดังรูปที่ A-1 ซึ่งในโครงการพัฒนานี้ จะมุ่งเน้นไปที่การทำการตรวจสอบทราฟฟิกระหว่างฝั่งประเทศไทย และญี่ปุ่นเท่านั้น

| FUJITSU | Description | FJ-WAN and Internet connection diagram of FTC | Rev.20090306 |
|---|---|---|---|
| | Design & Writer | Apichat Chalothom | |




**รูปที่ A-1** แผนภาพการเชื่อมต่อระบบเครือข่าย

## 2. ตารางซับเน็ตขององค์กร

ซับเน็ตในระบบเครือข่ายภายในขององค์กร สามารถแสดงได้ดังตารางที่ A-1

**ตารางที่ A-1** ตารางแสดงซับเน็ตที่ใช้ภายในองค์กร

| Category | Description | Current FTC subnet 172.16.0.0/25 | Factory | Floor | Area | Remark |
|---|---|---|---|---|---|---|
| Network equipment | FTC Admin/H-1F Server Room (FTC to WAN connection Link) | 172.16.90.0 | F / H | | Server room | |
| | FTC RMC-Net (Remote Maintenance Subnet) | 172.16.175.0 | FTC | | Network rack | |
| | FTC Untrust-Zone Backbone | 172.16.100.0 | H | 1 | Server room | |
| | FTC H-Factory Trust-Zone Backbone | 172.16.100.128 | | | | |
| | FTC I-Factory Trust-Zone Backbone | 172.16.125.0 | I | 1 | Server room | |
| | FTC-Backup-line | 172.16.241.128 | F | 2 | Spare Part room | |
| | SPGnet | 172.16.241.0 | | | | |
| | FTC SPGnet Server | 172.16.188.128 | | | | |
| | FTC H-factory to I-factory Backbone(EIGRP-1)(core-7) | 172.16.64.0 | H / I | 1 | Server room | |
| | FTC H-factory to I-factory Backbone(EIGRP-3)(core-8) | 172.16.64.128 | | | | |
| | FTC H-factory to I-factory Backbone(EIGRP-2)(core-7) | 172.16.65.0 | | | | |
| | FTC H-factory to I-factory Backbone(EIGRP-4)(core-8) | 172.16.65.128 | | | | |
| | FTC H-1F Server Room (ESRP Group-1) S48si ICMP ESRP V-IP | 172.16.66.0 | H | 1 | Server room | |
| | FTC H-1F Server Room (ESRP Group-1) S48si ICMP ESRP Core to Core | 172.16.66.128 | | | | |
| | FTC H-1F Server Room C6k(core3,4) to X450(core5,6) Backbone | 172.16.67.0 | | | | |
| | FTC H-1F Server Room C6k(core3,4) core to core | 172.16.67.128 | | | | |
| | FTC I-1F PCS Room C4k(core7,8) core to core | 172.16.68.0 | I | 1 | Server room | |
| | FTC F-2F DMZ-Zone (Mapping Subnet) | 172.16.98.0 | F | 2 | Spare Part room | |
| | FTC H-1F Server-room Untrust-Zone (Core1 to Core2) Core to Core link | 172.16.123.0 | H | 1 | Server room | |
| | FTC H-1F Server-room Trust-Zone (Core5 to Core6) Core to Core link | 172.16.123.128 | | | | |
| | FTC H-1F Server-Room Trust-Zone (ISG1000 to Core3/4 Link) | 172.16.121.0 | | | | |
| | FTC H-1F Server-Room Untrust-Zone (Core1/2 to ISG1000 Link) | 172.16.98.128 | | | | |
| | FTC R&D T/L (Untrust-Zone) | 172.16.30.128 | | | | |
| | FTC R&D T/L (Untrust-Zone) | 172.16.31.0 | | | | |
| | FTC R&D T/L (Untrust-Zone) | 172.16.31.128 | | | | |
| | FTC R&D T/L (Untrust-Zone) | 172.16.32.0 | | | | |
| | FTC R&D [Analysis Office & Calibration Room] (Untrust-Zone) | 172.16.125.128 | | | | |
| | FTC F-2F Office[Milacl-Room & Meeting-Room-2/3] (Untrust-Zone) | 172.16.54.0 | F | 2 | Office area | |
| | FTC F-2F Office[PCS] (Untrust-Zone) | 172.16.54.128 | | | | |
| | FTC F-2F Office[BC & Finence & Account & President & Document-Control] (Untrust-Zone) | 172.16.76.128 | | | | |
| | FTC F-2F Office[PCE & EES] (Untrust-Zone) | 172.16.76.0 | | | | |
| | FTC F-2F Offce (Untrust-Zone) | 172.16.77.128 | | | | |
| | FTC F-2F Office[MFG & FA & QA & IPQC & QSM] (Untrust-Zone) | 172.16.77.0 | | | | |
| | FTC F-2F Office[BPA & Purchasing] (Untrust-Zone) | 172.16.82.128 | | | | |
| | FTC F-2F Office[Training & IQA & HMQE & SQE] (Untrust-Zone) | 172.16.85.0 | | | | |
| | FTC F-2F Office[Plan Service & EQ] (Untrust-Zone) | 172.16.85.128 | | | | |
| Untrust zone | FTC F-2F Office[DEV] (Untrust-Zone) | 172.16.180.0 | | | | |
| | FTC F-2F EM | 172.16.126.128 | | | | |
| | FTC F-2F Office[EES & Training-Room & EQ & PCBA-Support] (Untrust-Zone) | 172.16.126.0 | | | | |
| | FTC F-2F Office[PE & EQD & "I&E"] (Untrust-Zone) | 172.16.96.128 | | | | |
| | FTC F-2F PCS Milacl-Server Room Untrust-Zone(Security VLAN) | 172.16.52.128 | | | | |
| | FTC SPGnet Server | 172.16.188.128 | | | Spare Part room | |
| | FTC E-1F Untrust-Zone | 172.16.121.128 | E | 1 | | |
| | FTC Admin Office (Untrust-Zone) | 172.16.96.0 | ADM | 1, 2 | | |
| | FTC Admin/F-2F | 172.16.90.128 | | 1 | | |
| | FTC H-1F Server-Room Untrust-Zone(Enterprise Server Pool) | 172.16.127.0 | H | 1 | Server room | |
| | FTC H-1F T/L OBA CERES | 172.16.120.128 | | | | |
| | FTC H-1F CR & Pahse-1 MFG Staff Area (Untrust-Zone) | 172.16.184.0 | | | | |
| | FTC H-2F CR Phase-1/2 Untrust-Zone(Data) | 172.16.184.128 | | 2 | | |
| | FTC H-1F Server-Room Untrust-Zone(Enterprise Server Pool) | 172.16.120.0 | | 1 | | |
| | FTC H-1F OBA-Zone (Untrust-Zone) | 172.16.180.128 | | | | |
| | FTC H-2F MFG-Offce Untrust-Zone(Data) | 172.16.93.0 | | 2 | | |
| | FTC Admin-1F Server-Room & H-1F Server-Room Untrust-Zone(Enterprise Server Pool) | 172.16.95.128 | ADM / H | 1 | Server room | |
| | FTC I-1F [OBA Area] (Untrust-Zone) | 172.16.176.0 | I | 1 | | |
| | FTC I-1F [OBA Area] (Untrust-Zone) | 172.16.175.128 | | | | |
| | FTC I-1F [MFG Staff Area & EQ Tech & Training] (Untrust-Zone) | 172.16.70.0 | | | | |
| | FTC I-2F,Canteen-5 Untrust-Zone(data) | 172.16.70.128 | | 2 | | |
| | FTC H-1F Server-Room & 2F Technician-Room(Phase2) (Untrust-Zone) | 172.16.63.0 | H | 2 | | |
| | FTC I-1F [CR & Receiving Area & Shipping Area] (Untrust-Zone) | 172.16.236.128 | | | | |
| Spare | FTC I-Factory "S" (Spare) | 172.16.124.128 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.127.128 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.167.0 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.183.0 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.183.128 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.211.0 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.212.0 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.213.0 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.213.128 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.218.0 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.218.128 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.219.0 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.219.128 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.220.0 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.220.128 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.239.0 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.240.0 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.240.128 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.242.0 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.245.128 | | | | |
| | FTC I-Factory "S" (Spare) | 172.16.253.0 | | | | |
| Voice zone | FTC H-1F Server-Room Untrust-Zone(Enterprise Server Pool) | 172.16.127.0 | H | 1 | | |
| | FTC I-1F Untrust-Zone(voice) | 172.16.71.0 | I | 1 | | |
| | FTC I-2F Canteen-5 Untrust-Zone(voice) | 172.16.71.128 | | 2 | | |
| | FTC [E-factory & F-Factory] Voice | 172.16.6.128 | E / F | 1 / 2 | | |

**ตารางที่ A-1 (ต่อ)** ตารางแสดงซับเน็ตที่ใช้ภายในองค์กร

| Category | Description | Current FTC subnet 172.16.0.0/25 | Factory | Floor | Area | Remark |
|---|---|---|---|---|---|---|
| Trust zone | FTC H-1F Server-Room (IPX-318 Control subnet) | 172.16.91.0 | H | 1 | Server room | |
| | FTC H-1F T/L Pahse-1 (Trust-Zone) | 172.16.181.128 | | | | |
| | FTC H-1F Server-Room (Server-Pool) | 172.16.97.0 | | | Server room | |
| | FTC H-1F Server-Room (Server-Pool) | 172.16.97.128 | | | | |
| | FTC I-Factory (Server-Pool) | 172.16.122.0 | | | | |
| | FTC H-1F Server-Room (Server-Pool) | 172.16.122.128 | | | | |
| | FTC H-1F T/L Pahse-1 (Trust-Zone) | 172.16.94.0 | | | | |
| | FTC H-1F T/L Pahse-1 (Trust-Zone) | 172.16.243.128 | | | | |
| | FTC H-1F T/L Pahse-1 (Trust-Zone) | 172.16.243.0 | | | | |
| | FTC H-1F T/L Pahse-1 (Trust-Zone) | 172.16.242.128 | | | | |
| | FTC H-1F T/L Pahse-1 (Trust-Zone) | 172.16.182.0 | | | | |
| | FTC H-1F T/L Pahse-1 (Trust-Zone) | 172.16.182.128 | | | | |
| | FTC H-1F T/L Pahse-1 (Trust-Zone) | 172.16.86.0 | | | | |
| | FTC H-1F T/L Pahse-1 (Trust-Zone) | 172.16.93.128 | | | | |
| | FTC H-1F Server-Room (Server-Pool) | 172.16.95.0 | | | Server room | |
| | FTC H-1F T/L Pahse-1 (Trust-Zone) | 172.16.94.128 | | | | |
| | FTC H-1F T/L 4C Pahse-2 (Trust-Zone) | 172.16.181.0 | | | | |
| | FTC H-1F T/L (Trust-Zone) | 172.16.244.128 | | | | |
| | FTC H-1F T/L Pahse-2 (Trust-Zone) | 172.16.246.0 | | | | |
| | FTC H-1F T/L Pahse-2 (Trust-Zone) | 172.16.246.128 | | | | |
| | FTC H-1F T/L Pahse-2 (Trust-Zone) | 172.16.247.0 | | | | |
| | FTC H-1F T/L Pahse-2 (Trust-Zone) | 172.16.247.128 | | | | |
| | FTC H-1F T/L Pahse-2 (Trust-Zone) | 172.16.248.0 | | | | |
| | FTC H-1F T/L Pahse-2 (Trust-Zone) | 172.16.248.128 | | | | |
| | FTC H-1F T/L Pahse-2 (Trust-Zone) | 172.16.249.0 | | | | |
| | FTC H-1F T/L Pahse-2 (Trust-Zone) | 172.16.249.128 | | | | |
| | FTC H-1F T/L SRT-Zone (Trust-Zone) | 172.16.165.0 | | | | |
| | FTC H-1F T/L SRT-Zone (Trust-Zone) | 172.16.165.128 | | | | |
| | FTC H-1F T/L SRT-Zone (Trust-Zone) | 172.16.166.0 | | | | |
| | FTC H-1F T/L SRT-Zone (Trust-Zone) | 172.16.166.128 | | | | |
| | FTC H-1F T/L SRT-Zone (Trust-Zone) | 172.16.166.128 | | | | |
| | FTC H-1F Washing-Room Pahse-1 (Trust-Zone) | 172.16.244.0 | | | | |
| | FTC H-2F CR Phase-1 (Trust-Zone) | 172.16.92.128 | | 2 | | |
| | FTC H-2F CR Phase-1 (Trust-Zone) | 172.16.245.0 | | | | |
| | FTC H-2F CR Phase-1 (Trust-Zone) | 172.16.99.128 | | | | |
| | FTC H-2F CR Phase-1 (Trust-Zone) | 172.16.92.0 | | | | |
| | FTC H-2F CR Phase-1 (Trust-Zone) | 172.16.91.128 | | | | |
| | FTC H-2F CR Phase-1 (Trust-Zone) | 172.16.99.0 | | | | |
| | FTC H-2F CR Phase-1 (Trust-Zone) | 172.16.254.128 | | | | |
| | FTC H-2F CR Phase-2 (Trust-Zone) | 172.16.250.0 | | | | |
| | FTC H-2F CR Phase-2 (Trust-Zone) | 172.16.250.128 | | | | |
| | FTC H-2F CR Phase-2 (Trust-Zone) | 172.16.251.0 | | | | |
| | FTC H-2F CR Phase-2 (Trust-Zone) | 172.16.251.128 | | | | |
| | FTC H-2F CR Phase-2 (Trust-Zone) | 172.16.252.0 | | | | |
| | FTC H-2F CR Phase-2 (Trust-Zone) | 172.16.252.128 | | | | |
| | FTC H-2F CR Phase-2 (Trust-Zone) | 172.16.254.0 | | | | |
| | FTC H-2F CR Phase-2 (Trust-Zone) | 172.16.253.128 | | | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.229.0 | I | 1 | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.229.128 | | | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.230.0 | | | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.230.128 | | | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.231.0 | | | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.231.128 | | | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.232.0 | | | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.232.128 | | | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.233.0 | | | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.233.128 | | | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.234.0 | | | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.234.128 | | | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.235.0 | | | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.235.128 | | | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.237.0 | | | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.237.128 | | | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.238.0 | | | | |
| | FTC I-1F [CR & Receiving Area & Shipping Area] (Trust-Zone) | 172.16.236.128 | | | | |
| | FTC I-1F Phase-1 [T/L] (Trust-Zone) | 172.16.238.128 | | 1 | | |
| | FTC I-1F [CR & Receiving Area & Shipping Area] (Trust-Zone) | 172.16.176.128 | | | | |
| | FTC I-1F [Diagnosis] (Trust-Zone) | 172.16.236.0 | | | | |
| | FTC I-1F PCS-Room (Trust-Zone) | 172.16.239.128 | | | Server room | |
| | FTC I-1F [New CR] (Trust-Zone) | 172.16.173.0 | | | | |
| | FTC I-1F [New CR] (Trust-Zone) | 172.16.173.128 | | | | |
| | FTC I-1F [New CR] (Trust-Zone) | 172.16.174.0 | | | | |
| | FTC I-1F [New CR] (Trust-Zone) | 172.16.174.128 | | | | |
| | FTC I-1F Phase-2 [T/L] (Trust-Zone) | 172.16.171.0 | | | | |
| | FTC I-1F Phase-2 [T/L] (Trust-Zone) | 172.16.171.128 | | | | |
| | FTC I-1F Phase-2 [T/L] (Trust-Zone) | 172.16.208.0 | | | | |
| | FTC I-1F Phase-2 [T/L] (Trust-Zone) | 172.16.172.128 | | | | |
| | FTC I-1F Phase-2 [T/L] (Trust-Zone) | 172.16.209.0 | | | | |
| | FTC I-1F Phase-2 [T/L] (Trust-Zone) | 172.16.208.128 | | | | |
| | FTC I-1F Phase-2 [T/L] (Trust-Zone) | 172.16.209.128 | | | | |
| | FTC I-1F Phase-2 [T/L] (Trust-Zone) | 172.16.210.128 | | | | |
| | FTC I-1F Phase-2 [T/L] (Trust-Zone) | 172.16.211.128 | | | | |
| | FTC I-1F Phase-2 [T/L] (Trust-Zone) | 172.16.212.128 | | | | |
| | FTC I-1F Phase-2 [T/L] (Trust-Zone) | 172.16.172.0 | | | | |
| | FTC I-1F Phase-2 [T/L] (Trust-Zone) | 172.16.210.0 | | | | |
| | FTC I-2F Phase-1 [CR-1] (Trust-Zone) | 172.16.168.0 | | 2 | | |
| | FTC I-2F Phase-1 [CR-1] (Trust-Zone) | 172.16.168.128 | | | | |
| | FTC I-2F Phase-1 [CR-2] (Trust-Zone) | 172.16.169.0 | | | | |
| | FTC I-2F Phase-1 [CR-2] (Trust-Zone) | 172.16.169.128 | | | | |
| | FTC I-2F Phase-1 [CR-3] (Trust-Zone) | 172.16.170.0 | | | | |
| | FTC I-2F Phase-1 [CR-3] (Trust-Zone) | 172.16.170.128 | | | | |
| | FTC I-2F Phase-1 [CR] (Trust-Zone) | 172.16.167.128 | | | | |

# ประวัติผู้เขียน

| | |
|---|---|
| ชื่อ | นายอภิชาต ชะโลธร |
| วัน-เดือน-ปีเกิด | 27 พฤษภาคม พ.ศ.2520 |
| สถานที่เกิด | กรุงเทพมหานคร |
| วุฒิการศึกษา | วิศวกรรมศาสตรบัณฑิต<br>ภาควิชาวิศวกรรมคอมพิวเตอร์<br>คณะวิศวกรรมศาสตร์<br>มหาวิทยาลัยเทคโนโลยีพระจอมเกล้า ธนบุรี |
| ประวัติการทำงาน | พ.ศ.2542 – พ.ศ.2552<br>บริษัทฟูจิตสึ (ประเทศไทย) จำกัด<br>พ.ศ.2552 – ปัจจุบัน<br>บริษัท โตชิบา สตอเรส ดีไวส์ (ประเทศไทย) จำกัด |