รายการอ้างอิง

1. Naugle, Mathew and Black, Uyless. Network Protocol Handbook. New York : McGraw-Hill, 1994.
2. Postel, J. Internet Protocol. Internet : RFC 791, 1 September 1981.
3. Reynolds, J. and Postel, J. Assigned Numbers. Internet : RFC 1700, October 1994.
4. Brownlee, N. Traffic Flow Measurement Architecture. Internet : RFC 2063, January 1997.
5. Brownlee, N. Traffic Flow Measurement Meter MIB. Internet : RFC 2064, January 1997.
6. Larry Wall and Randal L. Scbwartz. Programming perl. New York : O'Reilly & Associates Inc, March 1992.

ภาคผนวก ก

รายชื่อการจัดแบ่งเลขที่อยู่ไอพีโดยสำนักเทคโนโลยีสารสนเทศ เดือน มีนาคม 2542

ชื่อ กลุ่ม	เลขที่อยู่ไอพีของเครือข่าย	จำนวนบิต ของเลขเครือข่ายย่อย
CHULA	161.200.0.0	16
CHULA	202.6.90.0	24
CHULA	192.207.64.0	24
Dial-CU	161.200.1.0	24
Chulajakapong	161.200.128	25
CUUC	161.200.4.0	22
Language institute	161.200.8.0	24
Prachatipok	161.200.21.32	27
Chulajak	161.200.27.192	26
Pol-Sci	161.200.31.0	25
Res-institute2	161.200.32.0	25
Res-institute3	161.200.33.0	24
Veterinary	161.200.35.0	24
Dentistry	161.200.36.0	24
Pharmacy	161.200.40.0	24
Pharmacy	161.200.41.224	27
Sasin	161.200.42.0	24
PPC	161.200.43.0	24
Nursing	161.200.44.0	24
Arts	161.200.48.0	24
Arts	161.200.49.128	25
Fine-arts	161.200.49.0	28
Architecture	161.200.52.0	24

ชื่อ กลุ่ม	เลขที่อยู่ไอพีของเครือข่าย	จำนวนบิต ของเลขเครือข่ายย่อย
Allied-health	161.200.54.0	24
Economic	161.200.63.0	24
Accountancy	161.200.64.0	21
Accountancy	202.6.90.0	24
Engineer	161.200.80.0	20
Medicine	161.200.96.0	23
Medicine	161.200.100.0	24
Science	161.200.116.0	22
Science	161.200.116.0	22
Science	192.207.64.0	24
Dial-CU	161.200.129.0	24
KongPlan	161.200.132.0	27
Graduate-school	161.200.132.32	27
Academic-affair	161.200.132.64	27
Research	161.200.132.128	27
Jamjuree3	161.200.132.160	27
Jamjuree4	161.200.132.192	27
Registration	161.200.133.192	26
Withayapattana	161.200.134.128	25
University-office	161.200.135.0	24
Computer-Service	161.200.136.0	24

ชื่อ กลุ่ม	เลขที่อยู่ไอพีของเครือข่าย	จำนวนบิตของ เลขเครือข่ายย่อย
Comp-engineer	161.200.138.0	24
CU-book	161.200.139.0	24
CAR	161.200.144.0	23
Education	161.200.152.0	24
Sec-cud	161.200.153.128	25
Pri-cud	161.200.154.0	25
Communicate-art	161.200.160.0	24
Laws	161.200.168.0	24
ChulaNet	161.200.192.0	27
ChulaNet	161.200.192.192	28
ChulaNet	161.200.224.0	28
IT-office	161.200.192.64	27
CacheEngine	161.200.255.161	32
CacheEngine	161.200.255.162	32

ภาคผนวก ข

รายชื่อของบริการที่สำนักเทคโนโลยีสารสนเทศได้ทำการเปิดให้มีการเรียกใช้บริการผ่านเครือข่ายอินเทอร์เน็ตได้โดยการใช้ระบบไฟร์วอล (FireWall)

ชื่อของบริการ	หมายเลขโพรโทคอล	หมายเลขช่องบริการ
FTP	6	20-21
SSH	6	22
Telnet	6	23
SMTP	6	25
TIME	6	37
TIME	17	37
Whois	6	43
DNS	6	53
DNS	17	53
TFTP	17	69
Gopher	6	70
Finger	6	79
WWW	6	80
POP3	6	110
IDENT	6	113
NNTP	6	119
NTP	6	123
NTP	17	123
IMAP	6	143
Talk	6	517
Ntalk	6	518
IRC	6	6665-6669
ICMP	1	0-65535

ภาคผนวก ค

รูปแบบข้อมูลของเน็ตโฟล์ว

1. ข้อมูลของเน็ตโฟล์วซึ่งถูกจัดเก็บบนเร้าเตอร์จะประกอบด้วยข้อมูลดังนี้คือ

1.1. source IP address

1.2. destination IP address

1.3. source TCP/UDP application port

1.4. destination TCP/UDP application port

1.5. next hop router IP address

1.6. input physical interface index

1.7. output physical interface index

1.8. packet count for this flow

1.9. byte count for this flow

1.10. start of flow timestamp

1.11. end of flow timestamp

1.12. IP Protocol (Exp TCP=6, UDP=17)

1.13. Type of Service (ToS) byte

1.14. TCP Flags

1.15. source AS number

1.16. destination AS number

1.17. source subnet mask

1.18. destination subnet mask

2. ข้อมูลของเน็ตโฟล์วที่ส่งออกจากเร้าเตอร์

เร้าเตอร์จะทำการส่งข้อมูลของเน็ตโฟล์วไปยังเครื่องอ่านค่าเครื่องวัดที่มีโปรแกรมโฟล์วคอเร็กเตอร์ ที่ถูกเปิดไว้เพื่อรอรับข้อมูลนำไปประมวลเพื่อสรุปข้อมูลโดยมีโครงสร้างข้อให้เลือกส่งอยู่ 2 รุ่นด้วยกันคือ

2.1. บรรจุภัณฑ์รุ่นที่ 1 ซึ่งมีโครงสร้างของข้อมูลส่วนหัวดังตารางที่ ค.1.1 และ โครงสร้างของข้อมูลส่วนระเบียนดังตารางที่ ค.1.2

ไบต์	บรรจุ	รายละเอียด
0-1	Version	NetFlow export format version number
2-3	Count	Number of flows exported in this packet (1-24)
4-7	SysUptime	Current time in milliseconds since the export device booted
8-11	Unix_secs	Current count of seconds 0000 UTC 1970
12-16	Unix_nsecs	Residual nanoseconds since 0000 UTC 1970

ตารางที่ ค.1.1 โครงสร้างหัวของบรรจุภัณฑ์เน็ตโฟล์วรุ่น 1

ไบต์	บรรจุ	รายละเอียด
0-3	Srcaddr	Source IP address
4-7	Dstaddr	Destination IP address
8-11	Nexthop	IP address of next hop router
12-13	Input	SNMP index of input interface
14-15	Output	SNMP index of output interface
16-19	dPkts	Packets in the flow
20-23	dOctets	Total number of Layer 3 bytes in the packets of the flow
24-27	First	SysUptime at start of flow
28-31	Last	SysUptime at the time the last packet of the flow was received
32-33	srcport	TCP/UDP source port number or equivalent
34-35	dstport	TCP/UDP destination port number or equivalent
36-37	pad1	Unused (zero) bytes
38	Prot	IP protocol type (for example, TCP=6; UDP=17)
39	Tos	IP type of service (ToS)
40	Flags	Cumulative OR of TCP flags
41-43	pad1, pad2, pad3	Unused (zero) bytes
44-48	Reserved	Unused (zero) bytes

ตารางที่ ค.1.2 โครงสร้างระเบียนของบรรจุภัณฑ์เน็ตโฟล์วรุ่น 1

2.2. บรรจุภัณฑ์รุ่นที่ 5 ซึ่งมีโครงสร้างของข้อมูลส่วนหัวดังตารางที่ ค.2.1 และ โครงสร้างของข้อมูลส่วนระเบียนดังตารางที่ ค.2.2

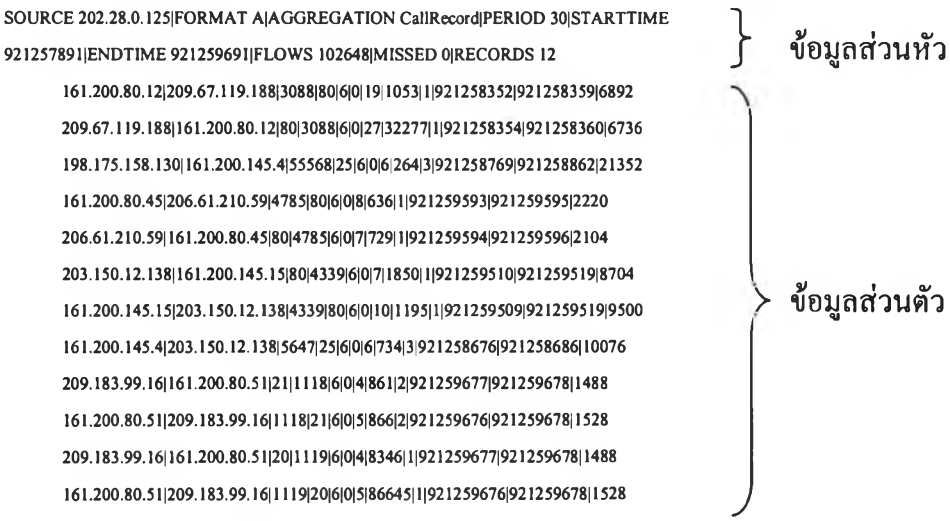
ไบต์	บรรจุ	รายระเอียด
0-1	Version	NetFlow export format version number
2-3	Count	Number of flows exported in this packet (1-30)
4-7	SysUptime	Current time in milliseconds since the export device booted
8-11	Unix_secs	Current count of seconds 0000 UTC 1970
12-15	Unix_nsecs	Residual nanoseconds since 0000 UTC 1970
16-19	Flow_sequence	Sequence counter of total flows seen
20	Engine_type	Type of flow-switching engine
21	Engine_id	Slot number of the flow-switching engine
22-23	Reserved	Unused (zero) bytes

ตารางที่ ค.2.1 โครงสร้างหัวของบรรจุภัณฑ์เน็ตโฟล์วรุ่น 5

ไบต์	บรรจุ	รายละเอียด
0-3	Srcaddr	Source IP address
4-7	Dstaddr	Destination IP address
8-11	Nexthop	IP address of next hop router
12-13	Input	SNMP index of input interface
14-15	Output	SNMP index of output interface
16-19	DPkts	Packets in the flow
20-23	Doctets	Total number of Layer 3 bytes in the packets of the flow
24-27	First	SysUptime at start of flow
28-31	Last	SysUptime at the time the last packet of the flow was received
32-33	Srcport	TCP/UDP source port number or equivalent
34-35	Dstport	TCP/UDP destination port number or equivalent
36	Pad1	Unused (zero) bytes
37	Tcp_flags	Cumulative OR of TCP flags
38	Prot	IP protocol type (for example, TCP=6; UDP=17)
39	Tos	IP type of service (ToS)
40-41	Src_as	Autonomous system number of the source, either origin or peer
42-43	Dst_as	Autonomous system number of the destination, either origin or peer
44	Src_mask	Source address prefix mask bits
45	Dst_mask	Destination address prefix mask bits
46-47	Pad2	Unused (zero) bytes

ตารางที่ ค.2.1 โครงสร้างระเบียนของบรรจุภัณฑ์เน็ตโฟล์วรุ่น 5

3. รูปแบบข้อมูลที่ถูกสรุปโดยโปรแกรมเน็ตโฟล์วคอเร็กเตอร์



รูปที่ ค.1 ตัวอย่างข้อมูลที่ถูกจัดเก็บโดยโปรแกรมเน็ตโฟล์วคอเร็กเตอร์

ตัวอย่างข้อมูลที่ได้จากการสรุปข้อมูลแบบคอลเรคคอร์ด โดยโปรแกรมเน็ตโฟล์วคอเร็กเตอร์ ดังรูปที่ ค.1 ซึ่งจะประกอบด้วย

3.1. ข้อมูลส่วนหัว

จะบอกถึงราบละเอียดของการสรุปผลซึ่งประกอบด้วย

3.1.1. เลขที่อยู่ไอพีของเร้าเตอร์ที่ส่งข้อมูลการจัดเก็บ

3.1.2. รูปแบบการจัดเก็บ A เป็นการจัดเก็บแบบอักขระ

3.1.3. รูปแบบการสรุปรายงาน

3.1.4. ระยะเวลาที่จัดเก็บ

3.1.5. เวลาที่เริ่มต้นการจัดเก็บ

3.1.6. เวลาที่สิ้นสุดการจัดเก็บ

3.1.7. จำนวนของโฟล์วที่ได้รับ

3.1.8. จำนวนของโฟล์วที่ไม่สามารถรับได้

3.1.9. จำนวนของระเบียน

3.2. ข้อมูลส่วนตัว

ประกอบด้วยระเบียนของข้อมูลที่ได้รับการสรปแล้วซึ่งมีความหมายของแต่ละเขตข้อมูลดังต่อไปนี้

3.2.1. Key fields

3.2.1.1. Srcaddr	Source IP address
3.2.1.2. Dstaddr	Destination IP address
3.2.1.3. Srcport	TCP/UDP source port number
3.2.1.4. Dstaddr	TCP/UDP destination port number
3.2.1.5. Protocol	IP protocol type (example TCP=6, UDP=17)
3.2.1.6. ToS	IP type of service

3.2.2. Value fields

3.2.2.1. Packet count	Packet count as part of this record
3.2.2.2. Byte count	Total number of Layer 3 bytes counted as part of this record
3.2.2.3. Flow count	Total number of flows aggregated into this record
3.2.2.4. First Time Stamp	The time in UTC seconds, of the first packet summarized into this record
3.2.2.5. Last Time Stamp	The time in UTC seconds, of the last packet summarized into this record
3.2.2.6. Total Active Time	The sum of individual active time for all the flows summarized into the current record

ประวัติผู้วิจัย

นายภาณุพันธ์ สุวรรณมาตร์ เกิดเมื่อวันอังคารที่ 4 เมษายน พ.ศ. 2516 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาปริญญาตรีวิทยาศาสตร์บัณฑิต สาขาคณิตศาสตร์ ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าธนบุรี (ปัจจุบันเปลี่ยนชื่อเป็น มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี) ในปีการศึกษา 2537 และเข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต ที่ภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัย เมื่อ พ.ศ. 2538 ปัจจุบันรับราชการที่สถาบันวิทยบริการจุฬาลงกรณ์มหาวิทยาลัย