ภาคผนวก ก
การติดตั้งระบบ

1. โปรแกรมที่ต้องการ

1.1 ระบบปฏิบัติการลีนุกซ์ Redhat เวอร์ชัน 9.0 (ftp://ftp.redhat.com)

1.2 โปรแกรม Snort เวอร์ชัน 2.0.0 (http://www.snort.org/downloads.html)

1.3 โปรแกรม C Compiler เวอร์ชัน 3.2.2-5 (ftp://ftp.gnu.org/gnu/gcc/)

1.4 ไลบารี LibPcap เวอร์ชัน 0.7.2-1 (http://rpmfind.net) หรือ (http://www.tcpdump.org/release/libpcap-0.7.2.tar.gz)

1.5 โปรแกรม MySql เวอร์ชัน 3.23.54a-11 (http://rpmfind.net) หรือ (http://mysql.secsup.org/Downloads/MySQL-4.0/mysql-4.0.12.tar.gz)

1.6 โปรแกรม Apache เวอร์ชัน 2.0.40-21 (http://rpmfind.net) หรือ (http://www.apache.org/dist/httpd/httpd-2.0.40.tar.gz)

1.7 โปรแกรม Acid เวอร์ชัน 0.9.6b23 (http://acidlab.sourceforge.net/acid-0.9.6b23.tar.gz)

1.8 โปรแกรม PHP เวอร์ชัน 4.2.2-17 (http://rpmfind.net) หรือ (http://www.php.net/distributions/php-4.2.2.tar.gz)

1.9 ไลบารี Adodb เวอร์ชัน 3.30 (http://phplens.com/lens/dl/adodb330.tgz)

1.10 ไลบารี PHPlot เวอร์ชัน 4.4.6 (http://www.phplot.com)

1.11 ไลบารี Gd เวอร์ชัน 2.0.11 (http://www.boutell.com/gd/)

1.12 ไลบารี JPGraph เวอร์ชัน 1.9.1 (http://jpgraph.techuk.com/jpgraph/downloads/jpgraph-1.91.tar.gz)

1.13 โปรแกรม Snortsam เวอร์ชัน 2.21 (http://www.snortsam.net/download.html)

1.14 ปลั๊กอิน Snortsam บนโปรแกรม Snort (http://www.snortsam.net/download.html)

2. การติดตั้งโปรแกรม

2.1 ไลบารี LibPcap

rpm -ivh libpcap-0.7.2-1.i386.rpm

2.2 โปรแกรม MySql

rpm mysql-3.23.54a-11 -ivh .i386.rpm

rpm mysql-server-3.23.54a-11 -ivh .i386.rpm

rpm mysql-devel-3.23.54a-11 -ivh .i386.rpm

rpm mod_auth_mysql-1.11-12 -ivh .i386.rpm

2.3 โปรแกรม Apache และ PHP

rpm -ivh httpd-2.0.40-21.i386.rpm

rpm -ivh php-4.2.2-17.i386.rpm

rpm -ivh php-mysql-4.2.2-17.i386.rpm

2.4 โปรแกรม Snort

mkdir /etc/snort

mkdir /var/log/snort

tar -xvzf snort-2.0.0.tar.gz

cd snort-2.0.0

./configure --with- mysql

make

make install

การติดตั้งกฎและไฟล์คอนฟิกุเรชัน

cd /home/temp/snort-2.0.0 (ไดเรกทอรีที่เก็บซอสโปรแกรม Snort)

cd rules

cp * /etc/snort

cd ../etc

cp snort.conf /etc/snort

cp *.config /etc/snort

2.5 ไลบารี ADODB

cp adodb330.tgz /var/www/html/

cd /var/www/html/

```
# tar -xvzf adodb330.tgz
# rm –rf adodb330.tgz
# mv  adobd-330  adobd
```

2.6 ไลบารี PHPLOT

```
# cp phplot-4.4.6.tar.gz /var/www/html/
# cd /var/www/html/
# tar -zxvf phplot-4.4.6.tar.gz
# rm -rf phplot-4.4.6.tar.gz
# mv  phplot-4.4.6  phplot
```

2.7 ไลบารี GD

```
# cp gd-2.0.11.tar.gz /var/www/html/
# cd /var/www/html/
# tar -zxvf gd-2.0.11.tar.gz
# rm -rf gd-2.0.11.tar.gz
# mv gd-2.0.11 gd
```

2.8 ไลบารี JPGraph

```
# cp jpgraph-1.91.tar.gz /var/www/html/
# cd /var/www/html/
# tar –xvzf jpgraph-1.91.tar.gz
# rm –rf jpgraph-1.91.tar.gz
# cd jpgraph-1.19
# rm -rf README
# rm -rf QPL.txt
# mv  jpgraph-1.91  jpgraph
```

2.9 โปรแกรม Acid

```
# cp acid-0.9.6b23.tar.gz /var/www/html/
# cd /var/www/html/
# tar –xvzf acid-0.9.6b23.tar.gz
# rm -rf acid-0.9.6b23.tar.gz
# mv  acid-0.9.6b23  acid
```

2.10 โปรแกรม Snortsam

```
# tar -zxvf snortsam-src-2.21.tar.gz
# cd snortsam-src-2.21
# chmod +x makesnortsam.sh
# ./makesnortsam.sh
```

2.11 ปลั๊กอิน Snortsam บนโปรแกรม Snort

```
# tar -zxvf snortsam-patch.tar.gz
# chmod +x patchsnort.sh
# ./patchsnort.sh /usr/local/src/snort
```

จากนั้นคอมไพล์โปรแกรม Snort ใหม่

```
# ./snortsam /etc/snortsam.conf
```

3. การแก้ไขไฟล์คอนฟิกุเรชันโปรแกรม Snort

ไฟล์คอนฟิกุเรชันของโปรแกรม Snort อยู่ที่ /etc/snort/snort.conf

ระบุหมายเลขเน็ตเวิร์คภายใน

```
var  HOME_NET 10.2.2.0/24
```

ระบุตำแหน่งไดเรกทอรีที่เก็บกฎ

```
var  RULE_PATH /etc/snort/
```

ระบุเอาต์พุตของระบบ (เช่นกรณีนี้ให้บันทึกลงฐานข้อมูล MySql)

```
output database: log, mysql, user=snort password=your_password dbname=snort
host=localhost
```

4. การติดตั้งฐานข้อมูลใน MySql

```
# mysql -u root
mysql> set password for 'root'@'localhost'=password('mypassword');
mysql> create database snort;
mysql> SHOW DATABASES;
+------------+
| Database
+------------+
```

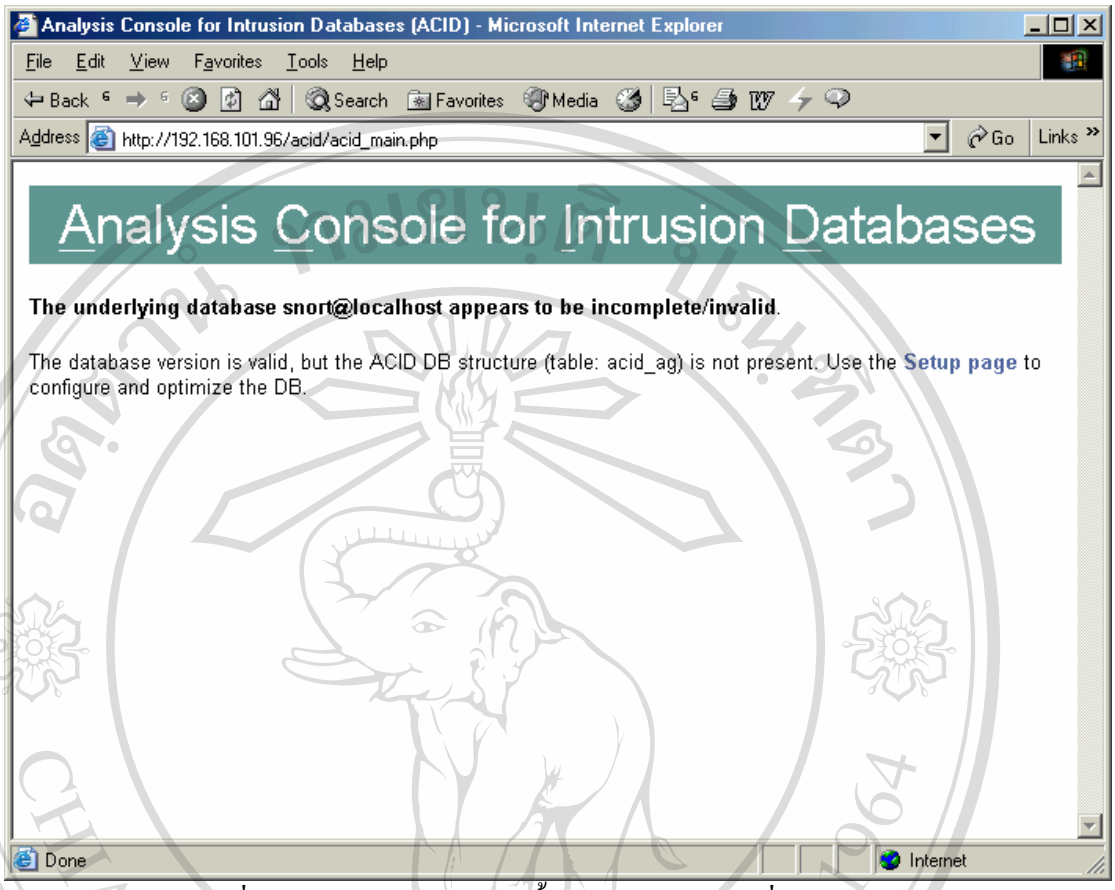
```
| mysql
| snort
| test
+------------+
3 rows in set (0.00 sec)
mysql> connect snort;
mysql> source create_mysql;
mysql> show tables;
+------------------+
| Tables_in_snort  |
+------------------+
| acid_ag          |
| acid_ag_alert    |
| acid_event       |
| acid_ip_cache    |
| data             |
| detail           |
| encoding         |
| event            |
| icmphdr          |
| iphdr            |
| opt              |
| reference        |
| reference_system |
| schema           |
| sensor           |
| sig_class        |
| sig_reference    |
| signature        |
| tcphdr           |
```

```
| udphdr          |
+-----------------+
20 rows in set (0.00 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort;
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to
snort@localhost;
mysql> connect mysql;
mysql>set password for 'snort'@'localhost'='password('mypassword');
mysql>set password for 'snort'@'%'='password('mypassword');
mysql> flush privileges;
mysql> exit
```

5. การแก้ไขไฟล์คอนฟิกุเรชันโปรแกรม ACID

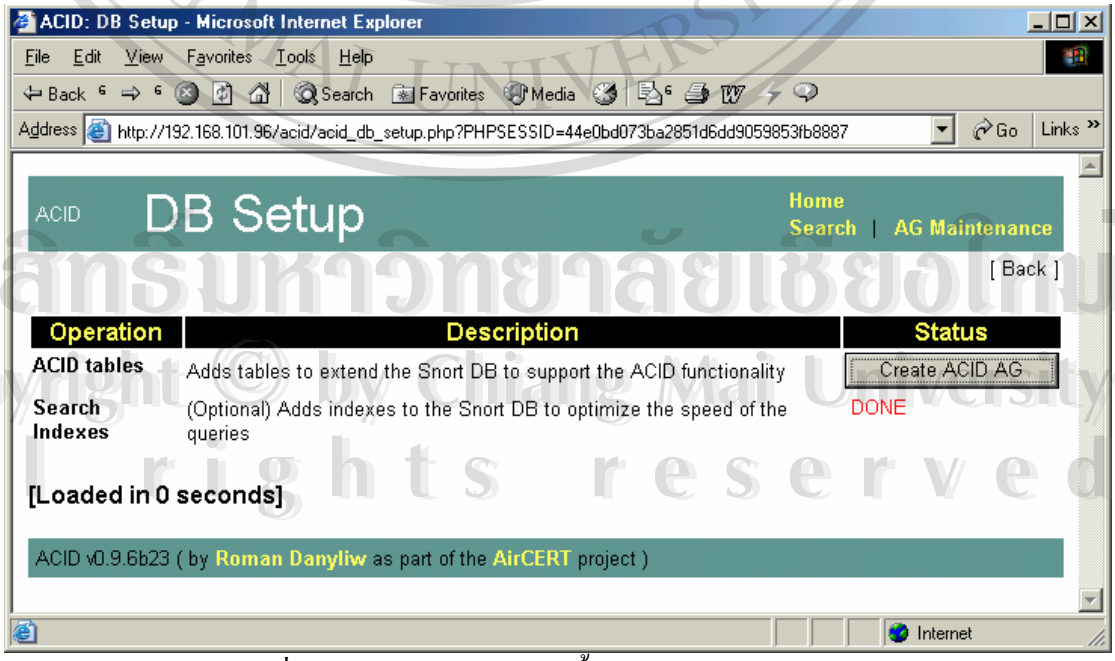
```
# vi /var/www/html/acid/acid_conf.php
$Dblib_path="../adodb";
$DBtype = "mysql";
$alert_dbname="snort";
$alert_user="snort";
$alert_password="xxx";
$Chartlib_path="../phplot";
```

จากนั้นเข้าไปที่ http://yourhost/acid/acid_main.php จะเห็นข้อความดังรูป



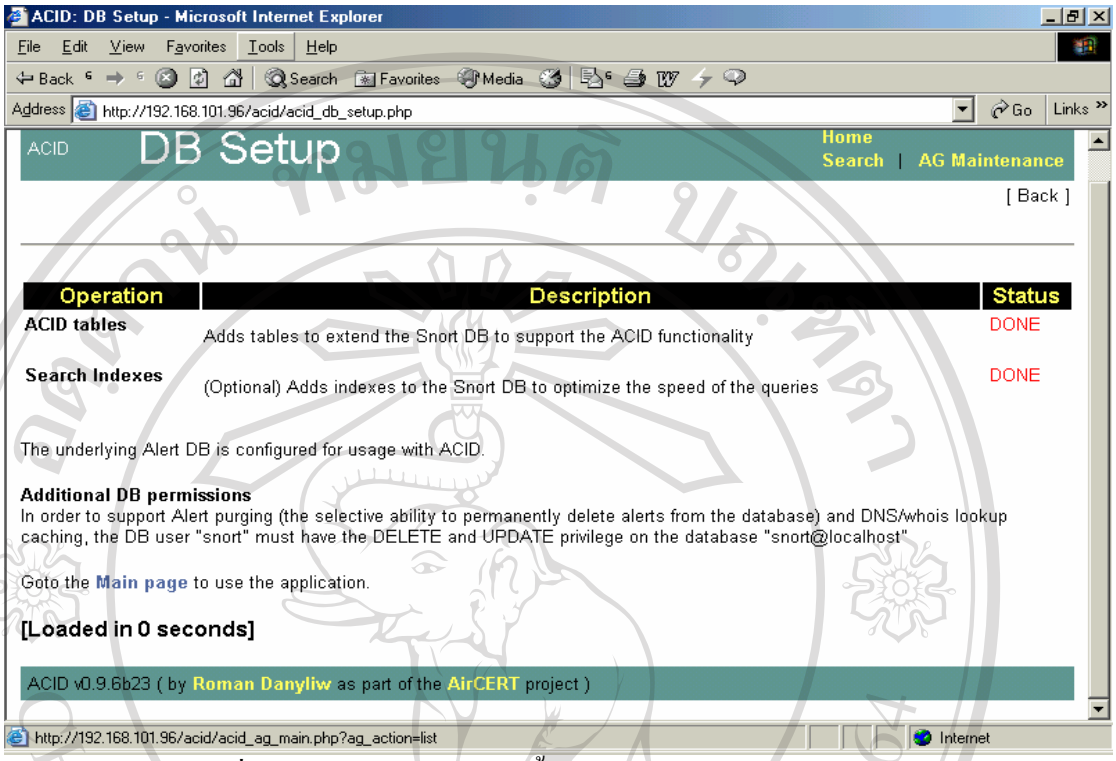
รูปที่ ก.1 หน้าจอแสดงการติดตั้งฐานข้อมูล ACID ที่ไม่สมบูรณ์

คลิกที่ไฮเปอร์ลิงค์ Setup Page จะได้หน้าจอแสดงการติดตั้งฐานข้อมูลสำหรับ ACID



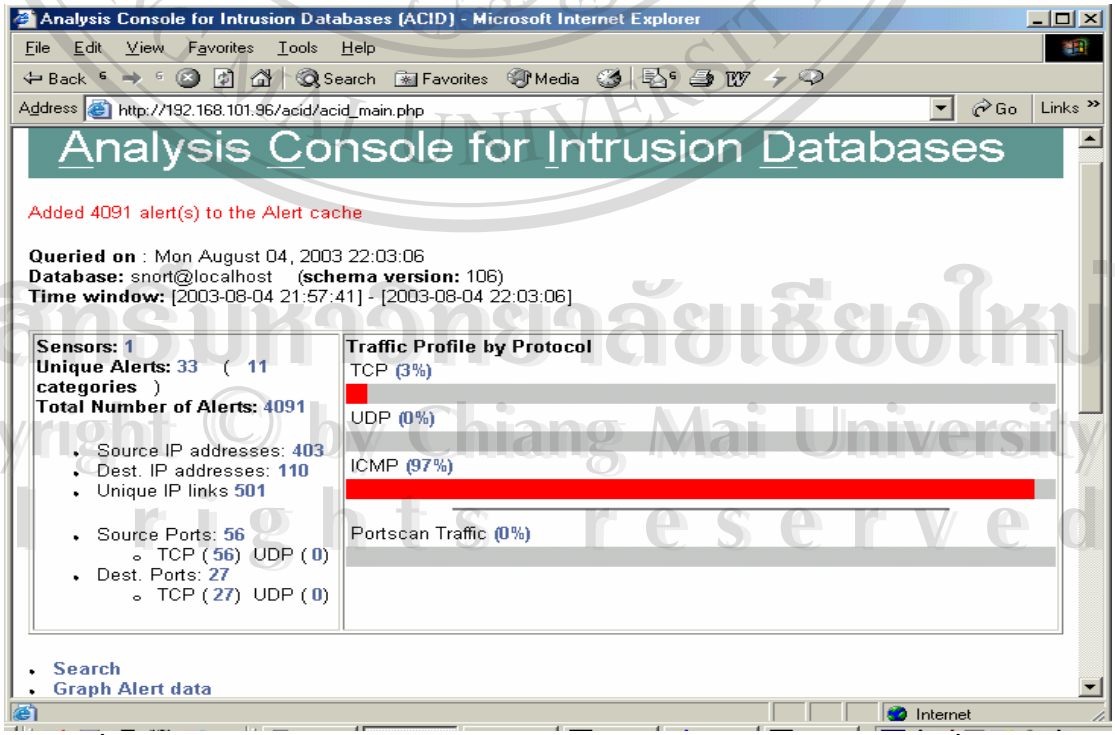
รูปที่ ก.2 หน้าจอแสดงการติดตั้งฐานข้อมูลสำหรับ ACID

คลิกที่ Create ACID AG



รูปที่ ก.3 หน้าจอแสดงการติดตั้งฐานข้อมูล ACID เสร็จสมบูรณ์

เมื่อกลับมาที่ Main Page จะเห็นหน้าจอแสดงผลการทำงานของโปรแกรม Snort ดังรูป



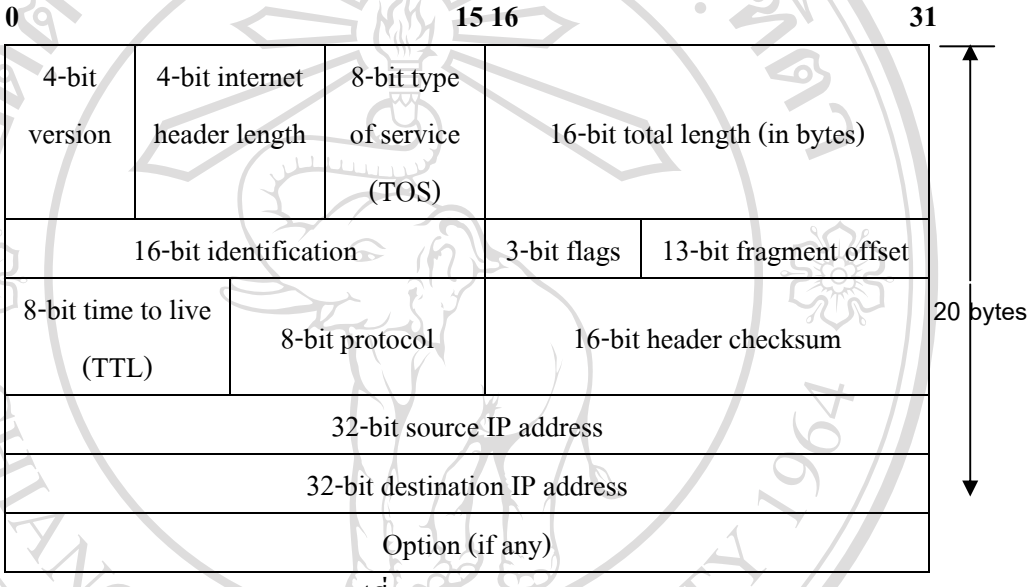
รูปที่ ก.4 หน้าจอแสดงผลการทำงานของโปรแกรม Snort ผ่านโปรแกรม ACID ที่ถูกต้อง

ภาคผนวก ข

ส่วนประกอบต่างๆในส่วนหัวของแพ็กเก็ต

1. IP Packet Header

ที่มา : http://www.rfc-editor.org/rfc/rfc791.txt



รูปที่ ข.1 IP Packet Header

IP Packet Header Field	Description
Version	The Version field indicates the format of the internet header. This document describes version 4.
IHL	Internet Header Length is the length of the internet header in 32 bit words, and thus points to the beginning of the data. Note that the minimum value for a correct header is 5.
Type of Service	The Type of Service provides an indication of the abstract parameters of the quality of service desired. These parameters are to be used to guide the selection of the actual service parameters when transmitting a datagram through a particular network. Several networks offer service precedence, which somehow treats high precedence traffic as

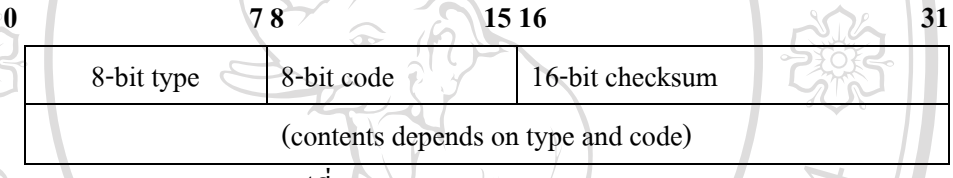
	more important than other traffic (generally by accepting only traffic above a certain precedence at time of high load). The major choice is a three way tradeoff between low-delay, high-reliability, and high-throughput. Bits 0-2: Precedence. Bit 3: 0 = Normal Delay, 1 = Low Delay. Bits 4: 0 = Normal Throughput, 1 = High Throughput. Bits 5: 0 = Normal Relibility, 1 = High Relibility. Bit 6-7: Reserved for Future Use. Precedence 111 - Network Control 110 - Internetwork Control 101 - CRITIC/ECP 100 - Flash Override 011 - Flash 010 - Immediate 001 - Priority 000 - Routine
Total Length	Total Length is the length of the datagram, measured in octets, including internet header and data. This field allows the length of a datagram to be up to 65,535 octets.
Identification	An identifying value assigned by the sender to aid in assembling the fragments of a datagram.
Flags	Various Control Flags. Bit 0: reserved, must be zero. Bit 1: (DF) 0 = May Fragment, 1 = Don't Fragment. Bit 2: (MF) 0 = Last Fragment, 1 = More Fragments.
Fragment Offset	This field indicates where in the datagram this fragment belongs.
Time to Live	This field indicates the maximum time the datagram is allowed to remain in the internet system. If this field contains the value zero, then the datagram must be destroyed. This field is modified in internet header processing. The time is measured in units of seconds, but since every module that processes a datagram must decrease the TTL by at least one even if it process the datagram in less than a second, the TTL must be thought of only as an upper bound on the time a datagram may exist. The intention is to cause undeliverable datagrams to be discarded, and to bound the maximum datagram lifetime.
Protocol	This field indicates the next level protocol used in the data portion of

	the internet datagram.
Header Checksum	A checksum on the header only. Since some header fields change (e.g., time to live), this is recomputed and verified at each point that the internet header is processed.
Source Address	The source address.
Destination Address	The destination address.

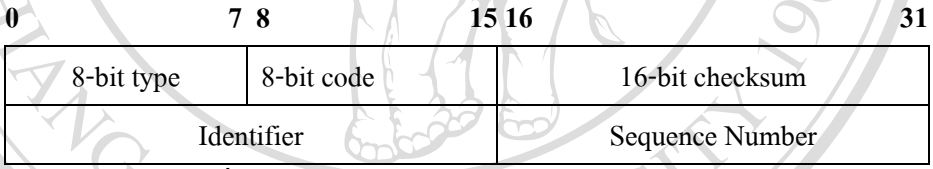
ตารางที่ ข.1 IP Packet Header Fields

2. ICMP Packet Header

ที่มา : http://www.rfc-editor.org/rfc/rfc792.txt



รูปที่ ข.2 Basic ICMP Packet Header



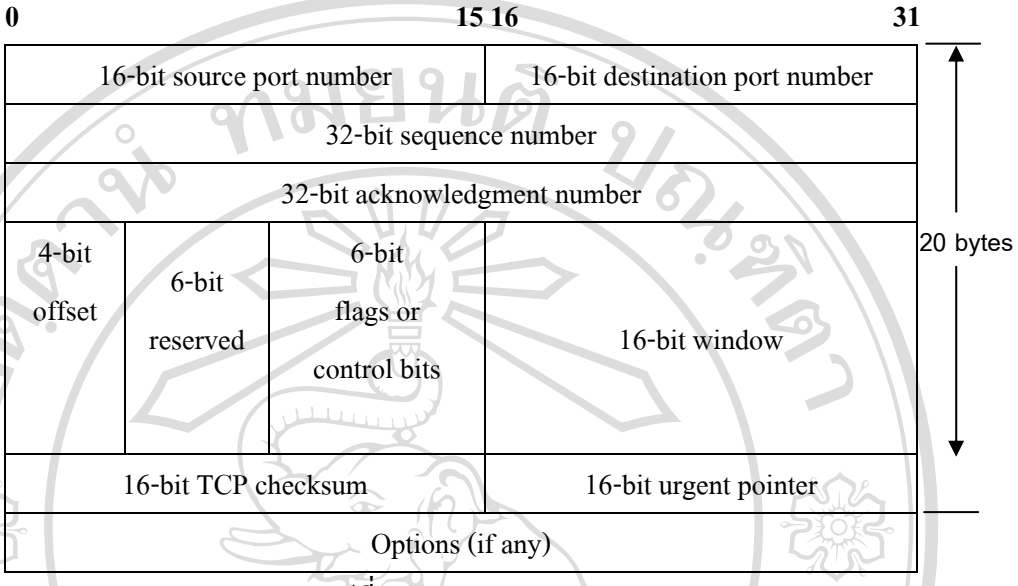
รูปที่ ข.3 ICMP Packet Header used in ping command.

ICMP Packet Header Field	Description
Type	Show type of ICMP packet.
Code	Show the sub-type of code number used for the packets. 0 = net unreachable; 1 = host unreachable; 2 = protocol unreachable; 3 = port unreachable; 4 = fragmentation needed and DF set; 5 = source route failed.
Checksum	Use to detect any errors in the ICMP packet.
Identifier	If code = 0, an identifier to aid in matching echos and replies, may be zero.
Sequence Number	If code = 0, a sequence number to aid in matching echos and replies, may be zero.

ตารางที่ ข.2 ICMP Packet Header Fields

3. TCP Packet Header

ที่มา : http://www.rfc-editor.org/rfc/rfc793.txt



รูปที่ ข.4 TCP Packet Header

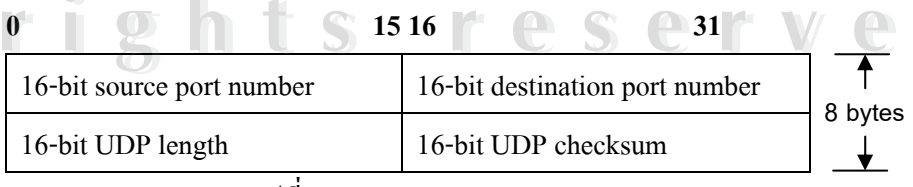
TCP Packet Header Field	Description
Source Port	Source port number.
Destination Port	The destination port number.
Sequence Number	The sequence number of the first data octet in this segment (except when SYN is present). If SYN is present the sequence number is the initial sequence number (ISN) and the first data octet is ISN+1.
Acknowledgment Number	If the ACK control bit is set this field contains the value of the next sequence number the sender of the segment is expecting to receive. Once a connection is established this is always sent.
Data Offset	The number of 32 bit words in the TCP Header. This indicates where the data begins. The TCP header (even one including options) is an integral number of 32 bits long.
Reserved	Reserved for future use. Must be zero.
Control Bits	URG: Urgent Pointer field significant ACK: Acknowledgment field significant

	PSH: Push Function RST: Reset the connection SYN: Synchronize sequence numbers FIN: No more data from sender
Window	The number of data octets beginning with the one indicated in the acknowledgment field which the sender of this segment is willing to accept. Tell th other side about the length of TCP window size.
Checksum	A checksum for TCP header and data.
Urgent Pointer	This field communicates the current value of the urgent pointer as a positive offset from the sequence number in this segment. The urgent pointer points to the sequence number of the octet following the urgent data. This field is only be interpreted in segments with the URG control bit set.
Options	Options may occupy space at the end of the TCP header and are a multiple of 8 bits in length. All options are included in the checksum. An option may begin on any octet boundary. There are two cases for the format of an option: Case 1: A single octet of option-kind. Case 2: An octet of option-kind, an octet of option-length, and the actual option-data octets. The option-length counts the two octets of option-kind and option-length as well as the option-data octets.

ตารางที่ ข.3 TCP Packet Header Fields

4. UDP Packet Header

ที่มา : http://www.rfc-editor.org/rfc/rfc768.txt



รูปที่ ข.5 UDP Packet Header

UDP Packet Header Field	Description
Source Port	An optional field, when meaningful, it indicates the port of the sending process, and may be assumed to be the port to which a reply should be addressed in the absence of any other information. If not used, a value of zero is inserted.
Destination Port	Internet destination port address.
Length	Length is the length in octets of this user datagram including this header and the data. (This means the minimum value of the length is eight.)
Checksum	Checksum is the 16-bit one's complement of the one's complement sum of a pseudo header of information from the IP header, the UDP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

ตารางที่ ข.4 UDP Packet Header Fields

ประวัติผู้เขียน

ชื่อ	นายสรวิช รุจนวิศาล
วัน เดือน ปี เกิด	19 สิงหาคม 2519
ประวัติการศึกษา	สำเร็จการศึกษามัธยมศึกษาตอนปลาย โรงเรียนมงฟอร์ตวิทยาลัย เชียงใหม่ ปีการศึกษา 2536 สำเร็จการศึกษาปริญญาวิศวกรรมศาสตรบัณฑิต สาขาวิชาคอมพิวเตอร์ มหาวิทยาลัยเชียงใหม่ ปีการศึกษา 2540
ประวิติการทำงาน	วิศวกรระบบเครือข่าย สถานบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่
ประกาศนียบัตร	CCNA 2.0 (Cisco Certified Network Associate)