Distributed Network Traffic Monitoring and Analysis using Load Balancing Technology

Soon-Hwa Hong, Jae-Young Kim, Bum-Rae Cho and James W. Hong

DP&NM Lab.

Dept. of Computer Science and Engineering

POSTECH, Pohang Korea

Email: {padosori, jay, brcho, jwkhong}@postech.ac.kr

http://dpnm.postech.ac.kr/

Introduction

- Network traffic (text, image, software, audio, video) is increasing continuously both on the Internet and Intranet.
- A simple, accurate and efficient network traffic monitoring and analysis is required to understand the current usage as well as to plan for future.
- Many shortcomings exist in currently available monitoring systems.
  - cannot analyze long-term traffic.
  - do not have monitoring capability from multiple network points.
  - capture, analysis and presentation all in one machine.
  - cannot prevent packet drops from the system overload.
- WebTrafMon II attempts to overcome these shortcomings using distributed architecture and load balancing technique.

Related Work

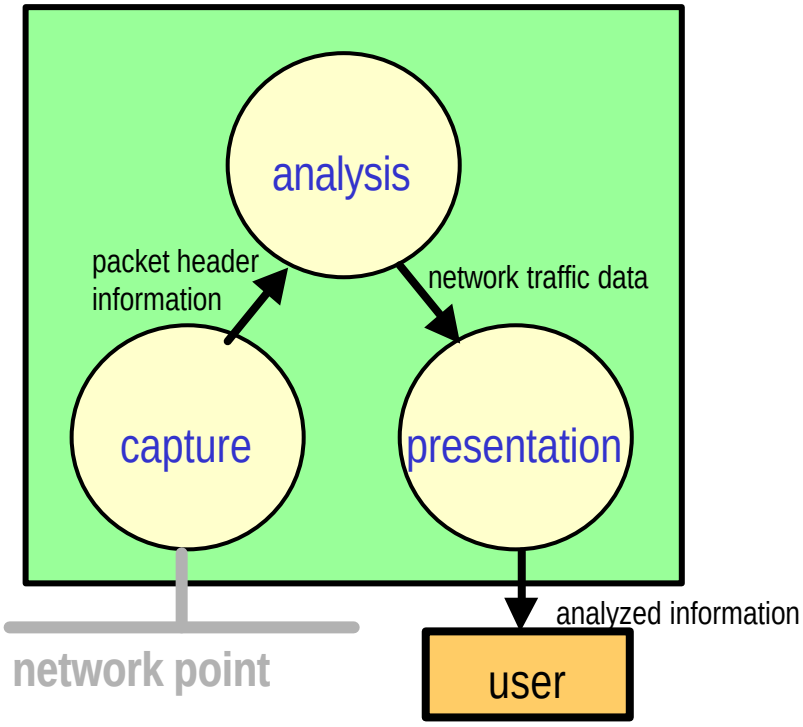
	Capture Method	Analysis Method	Analysis Interval	Analysis Scope	Support for Multiple network points	Distributed Architecture	User Interface
tcpdump	libpcap	real time	current	layer 7	no	no	Text
ntop	libpcap	batch	5 second, hourly	layer 7	no	no	Web
ethereal	libpcap	real time, batch	current, user-specified time	layer 7	no	no	X-Windows
MRTG	snmp agent	batch	5 minute, hourly, daily, weekly, monthly	layer 2	yes	yes	Web
WebTrafMon	libpcap	real time, batch	current, hourly	layer 7	no	no	Web
WebTrafMon II	libpcap	real time, batch	current, hourly, daily, monthly, yearly	layer 7	yes	yes	Web

WebTrafMon II Requirements

- analyze various types of information: host information, network, transport, and application layer protocols.
- analyze present real-time, hourly, daily, monthly and yearly network traffic data automatically.
- analyze multiple network points traffic.
- no packet drops.
- web-based graphical user interface.

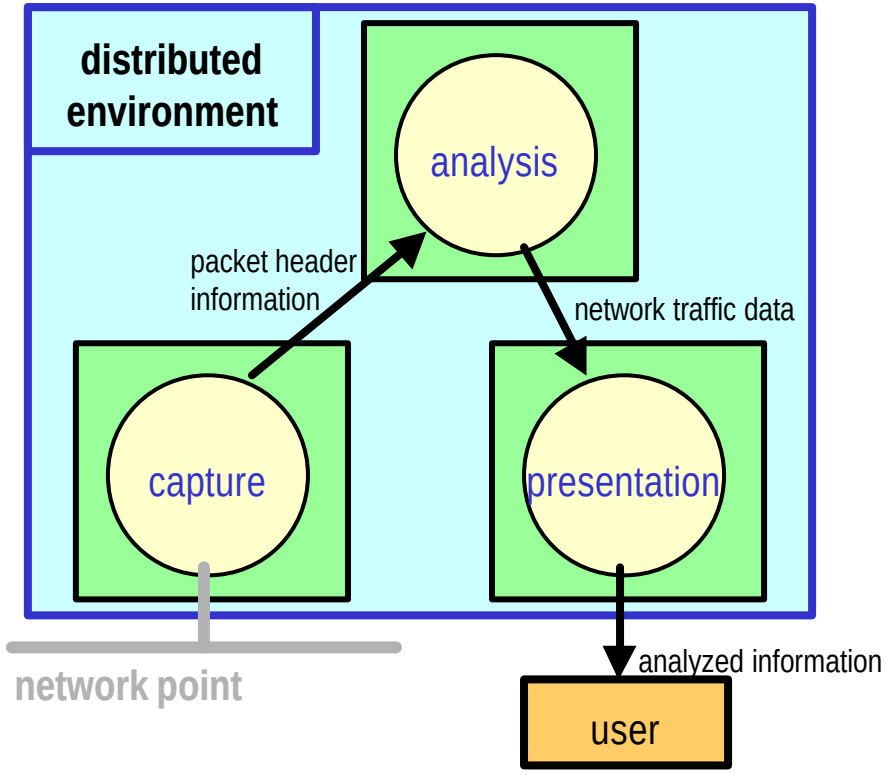
Centralized vs. Distributed

Centralized Traffic Analysis Architecture



- system overload occurs frequently and many packets are dropped
- cannot support for multiple network points
- presentation time is slow

Distributed Traffic Analysis Architecture



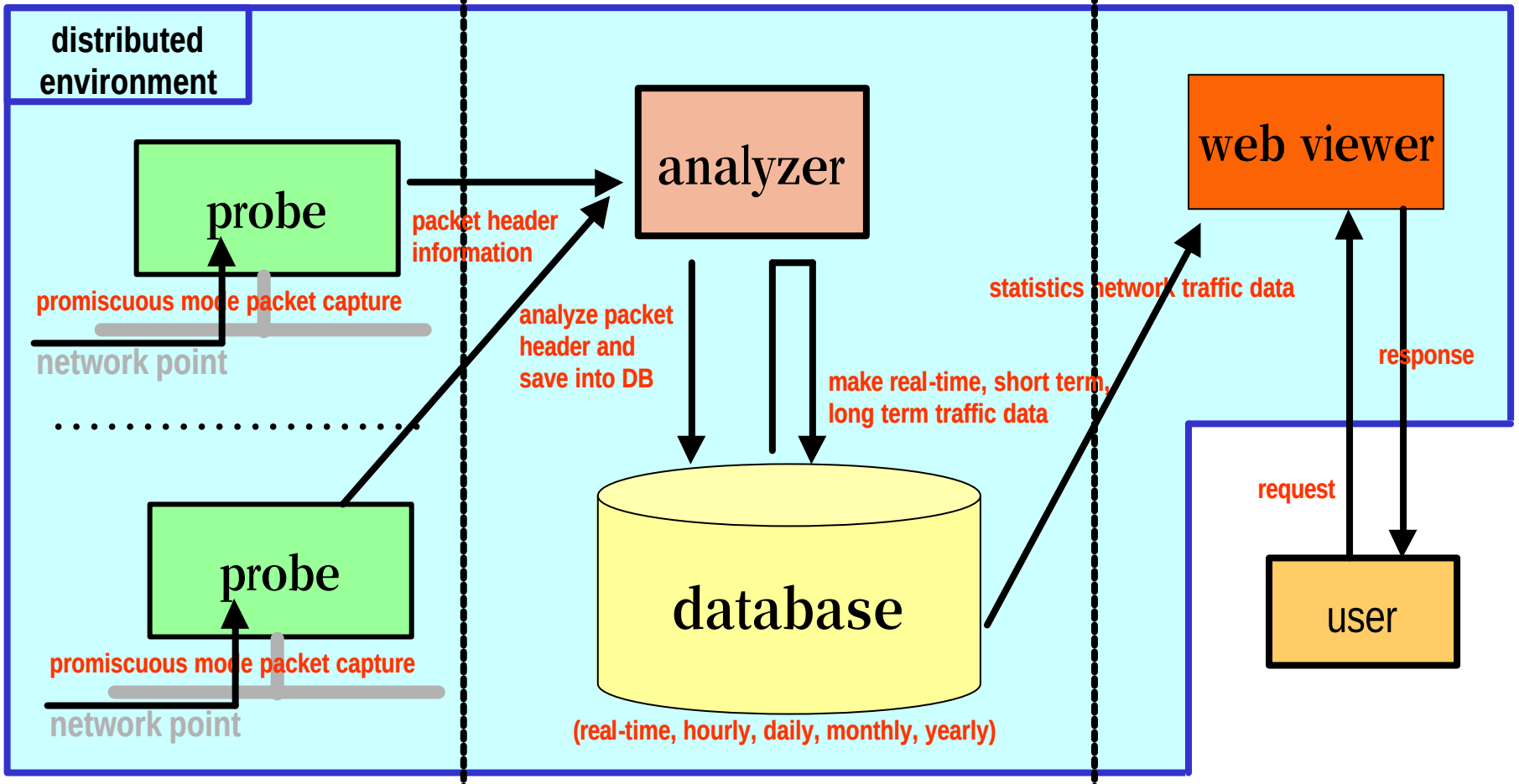
- capture, analysis and presentation modules execute on separate machines to minimize system overload
- can support for multiple network points
- presentation time is fast

WebTrafMon II: Design

1. multiple network point packet capture and analyze packet header

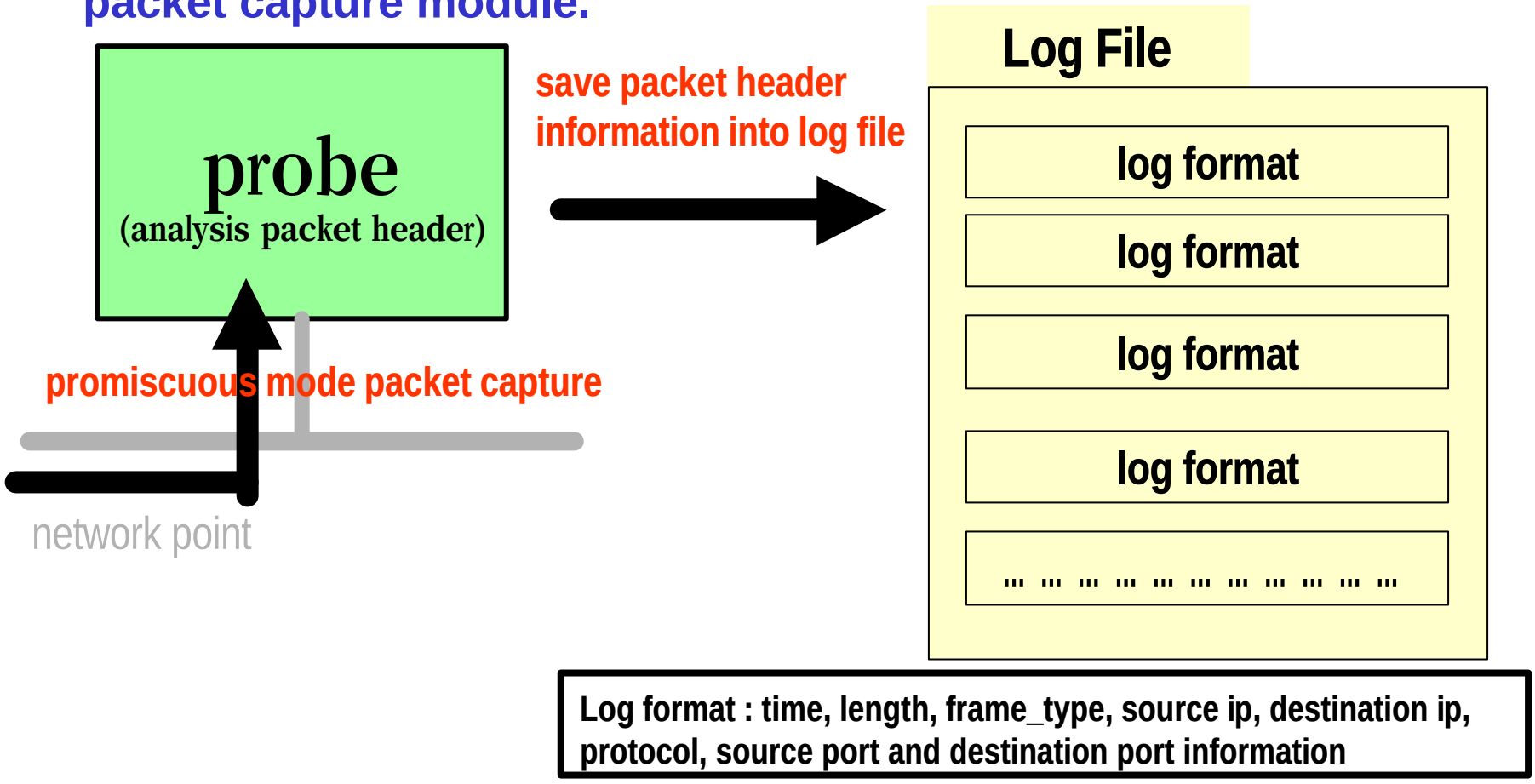
2. analyze packet header and save into DB and make short term and long term traffic data

3. query to database from user request and give information to user

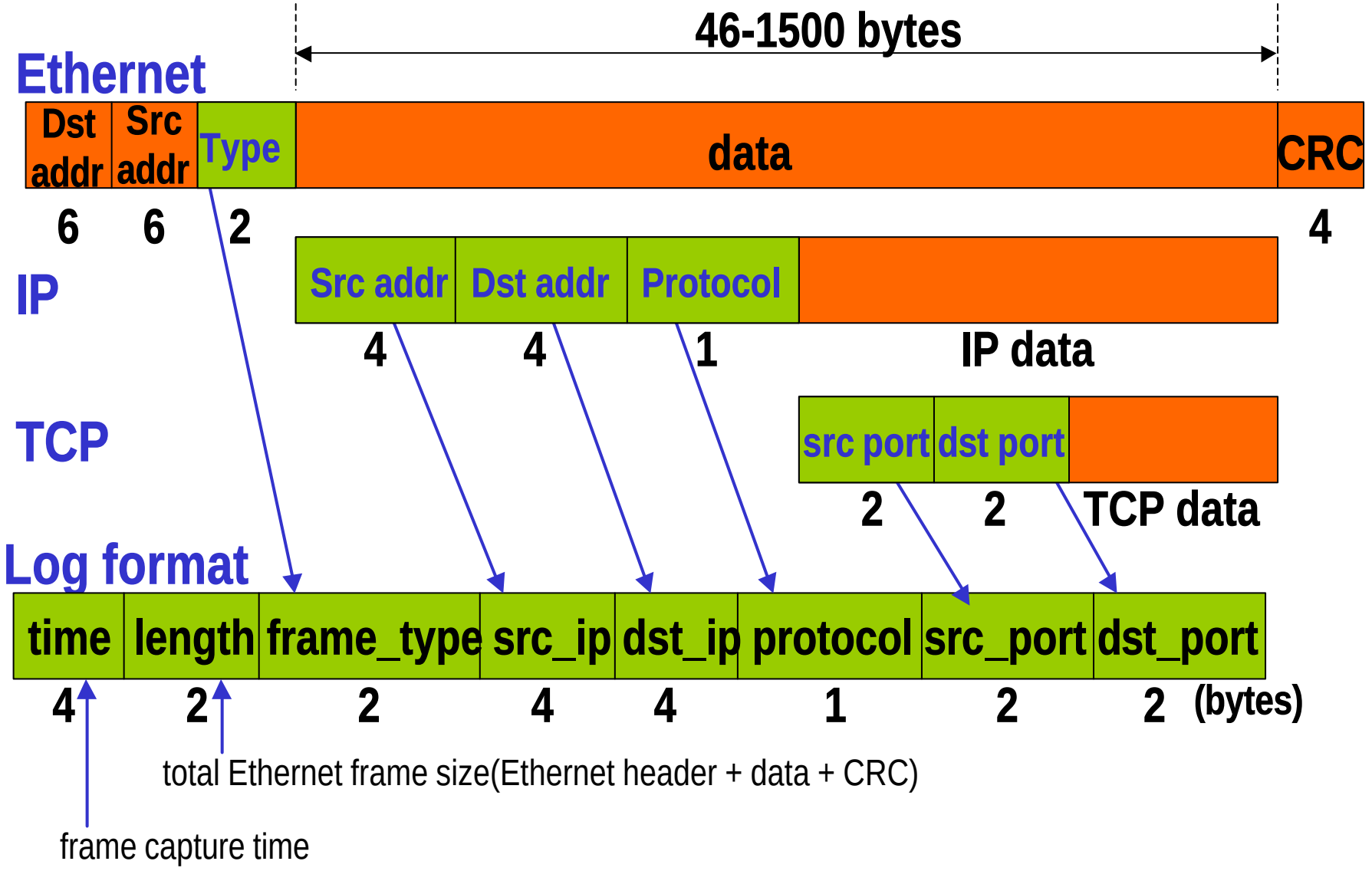


Packet Capture Module (Probe)

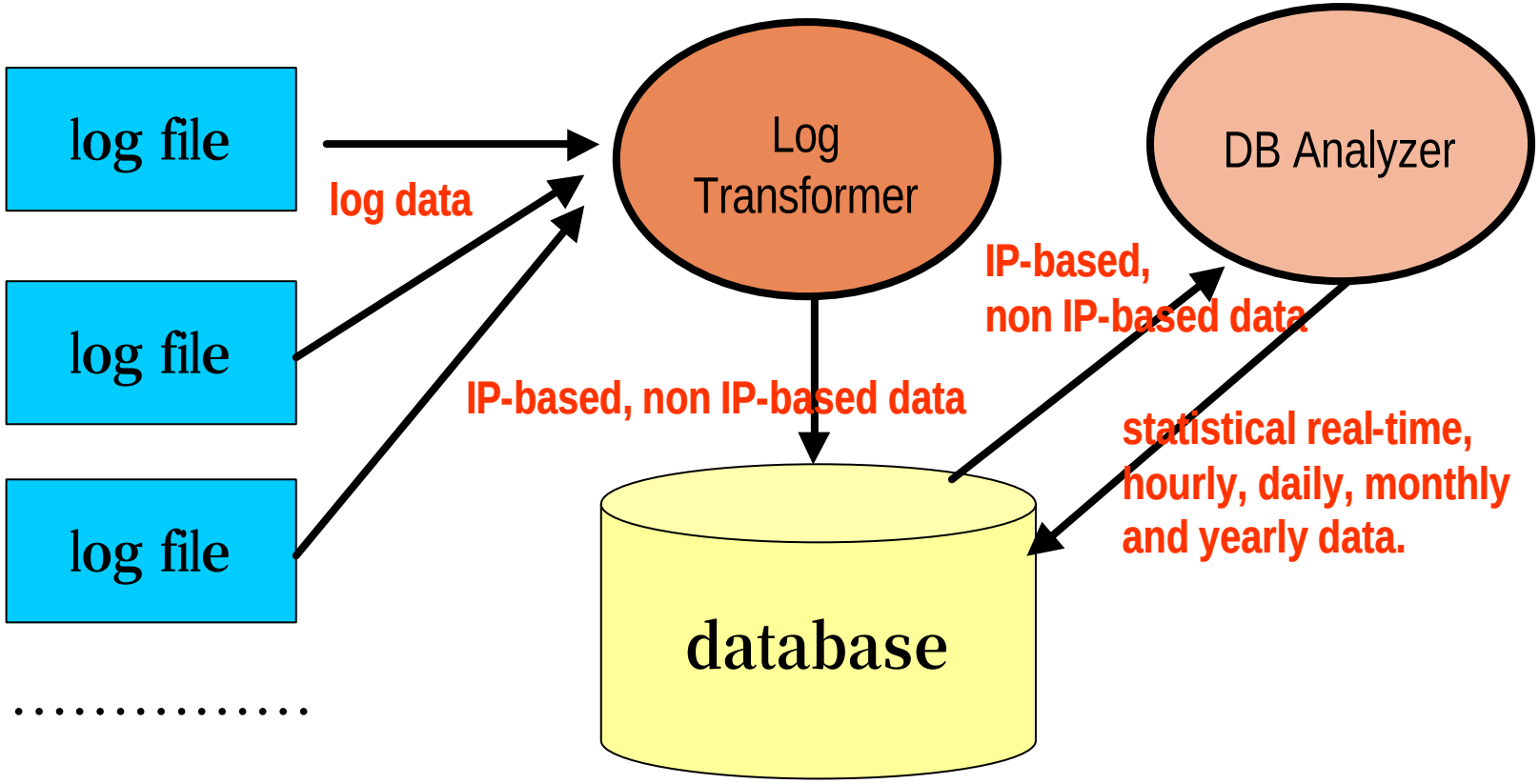
- Probe captures packet with promiscuous mode, analyzes packet header and saves into log file
- No packet drops from system overload using an independent packet capture module.



Log Format

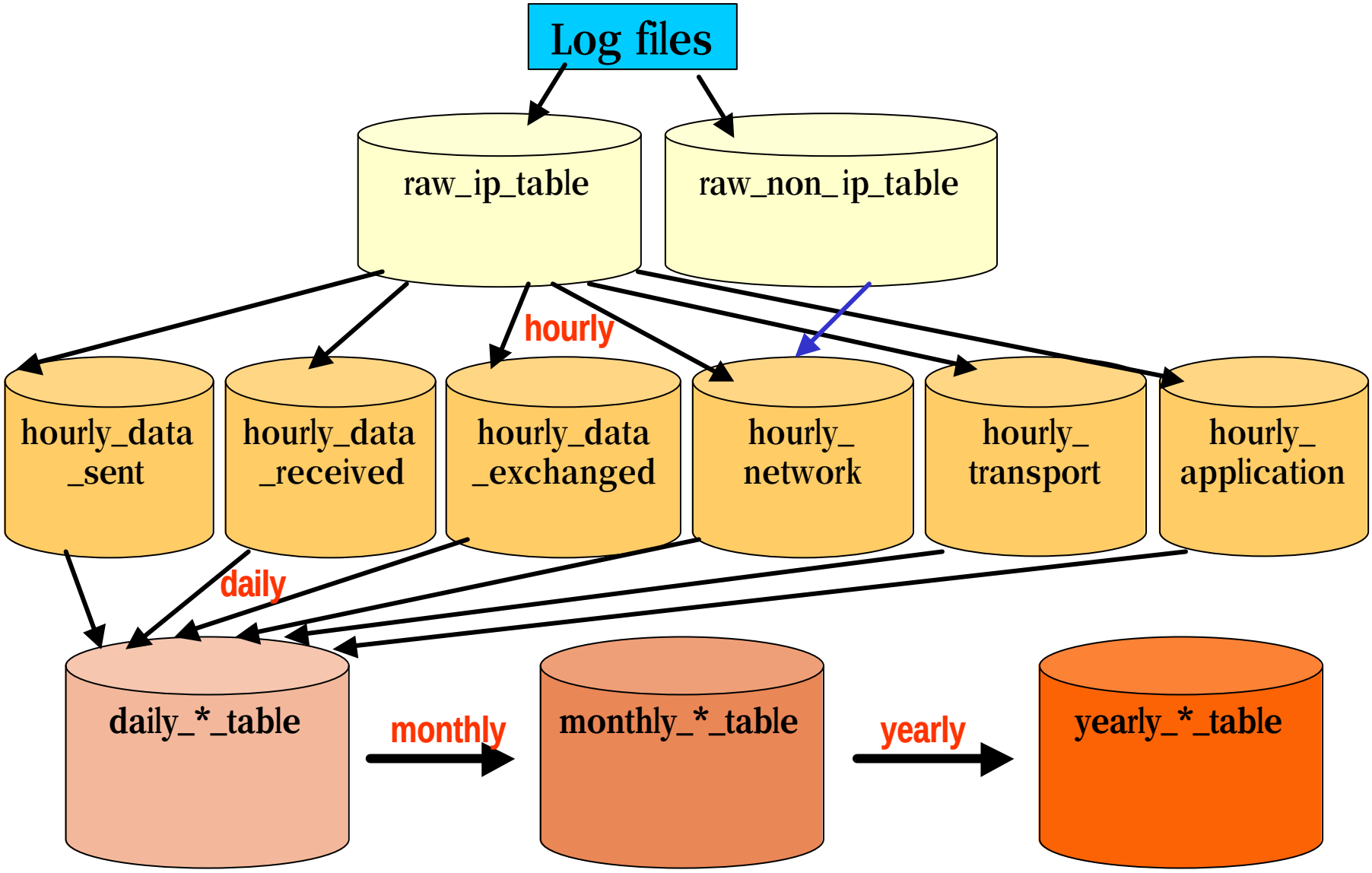

46-1500 bytes
Ethernet
Dst addr
Src addr
Type
data
CRC
6
6
2
4
IP
Src addr
Dst addr
Protocol
IP data
4
4
1
TCP
src port
dst port
TCP data
2
2
Log format
time
length
frame_type
src_ip
dst_ip
protocol
src_port
dst_port
4
2
2
4
4
1
2
2
(bytes)
total Ethernet frame size(Ethernet header + data + CRC)
frame capture time

Packet Analysis Module (Analyzer)

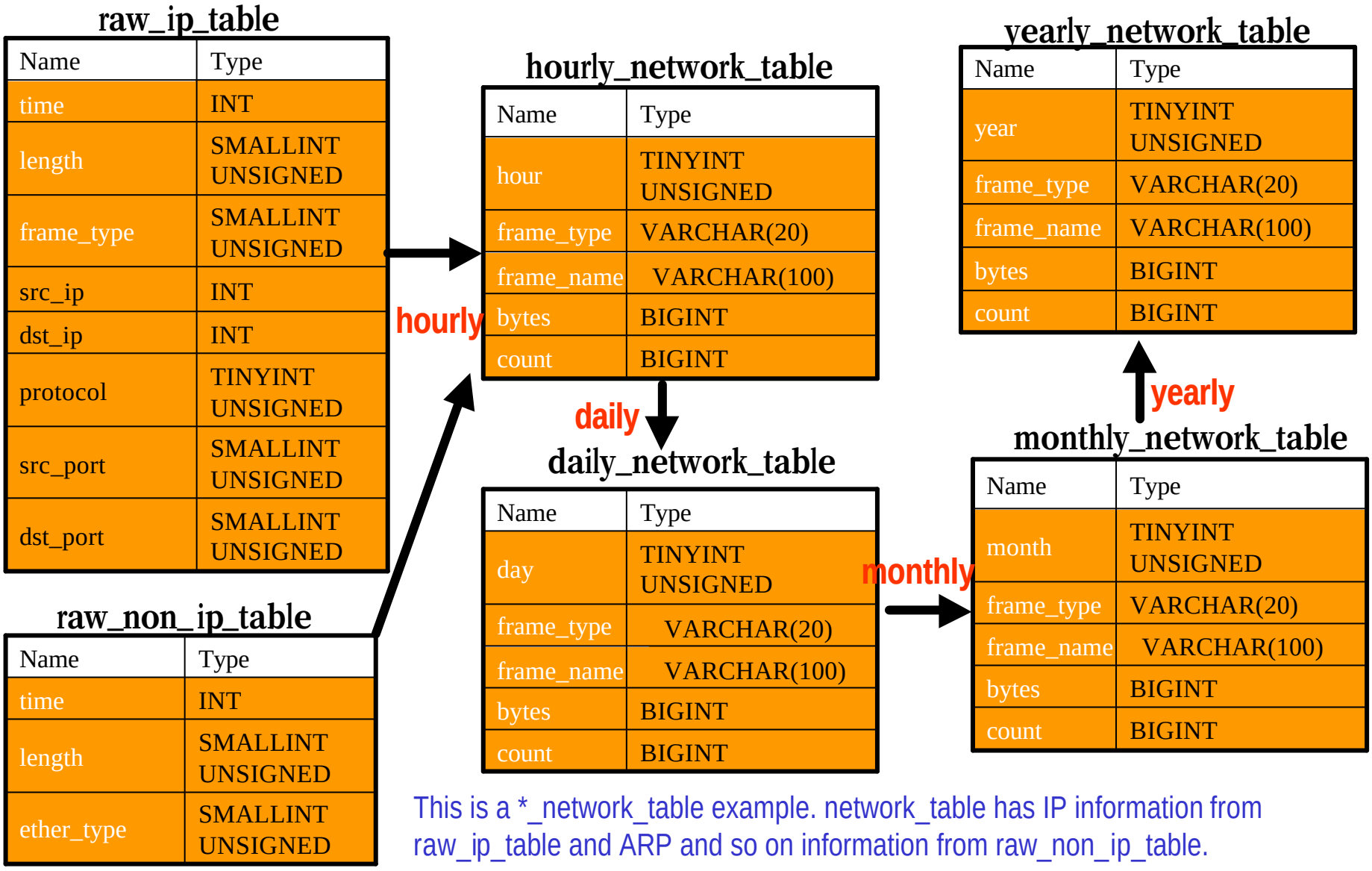


- An Analyzer is divided into a Log Transformer module and DB Analyzer module.
- Log Transformer assorts log files into IP-based data, and non IP-based data (e.g., ARP, RARP, IPX).
- Log Transformer saves these assorted data to database.
- DB Analyzer analyzes assorted data in database and makes statistical real-time,hourly, daily, monthly and yearly data.

Data Translation by Analyzer for Long-Term Traffic

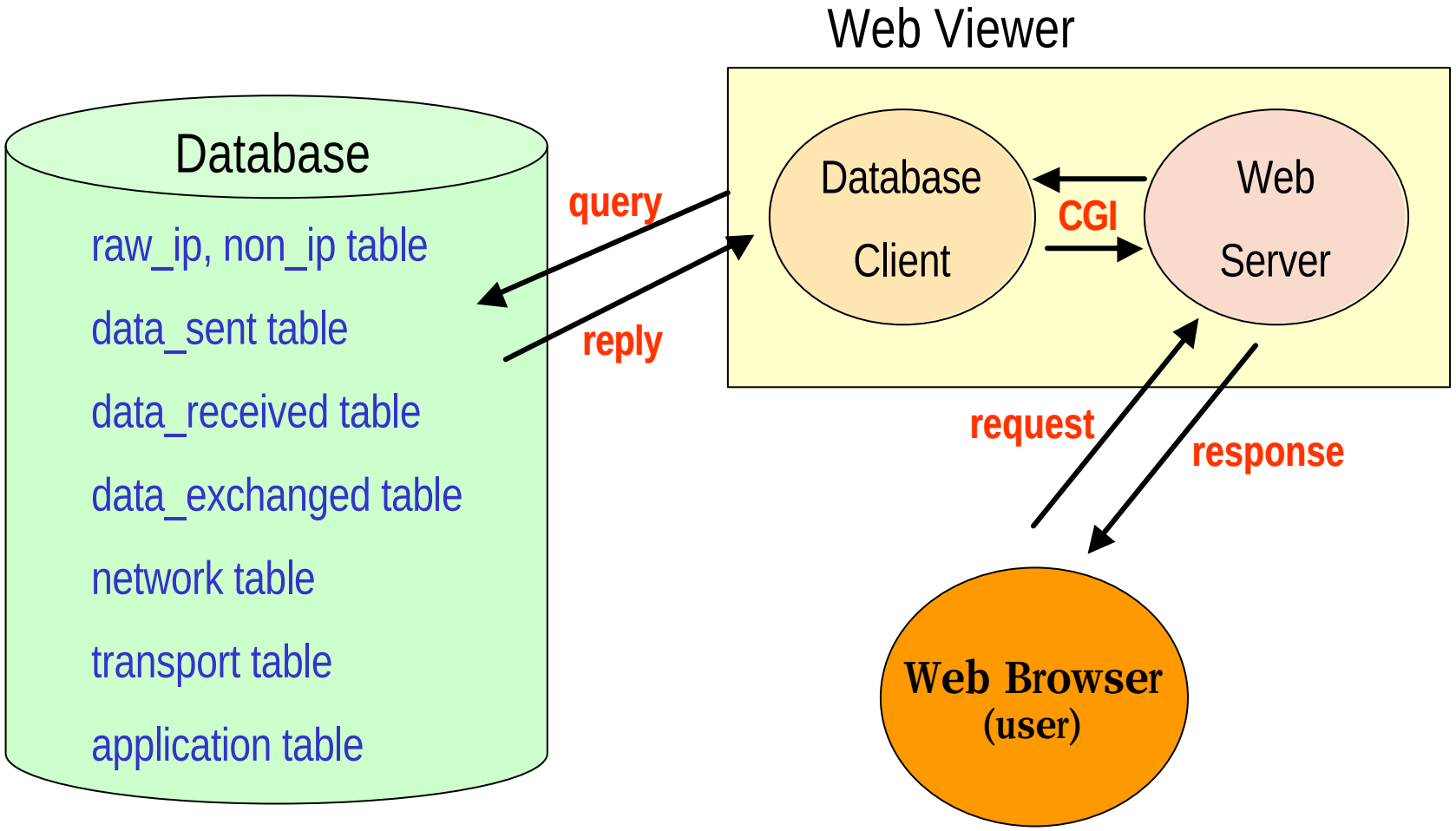


DB Schema

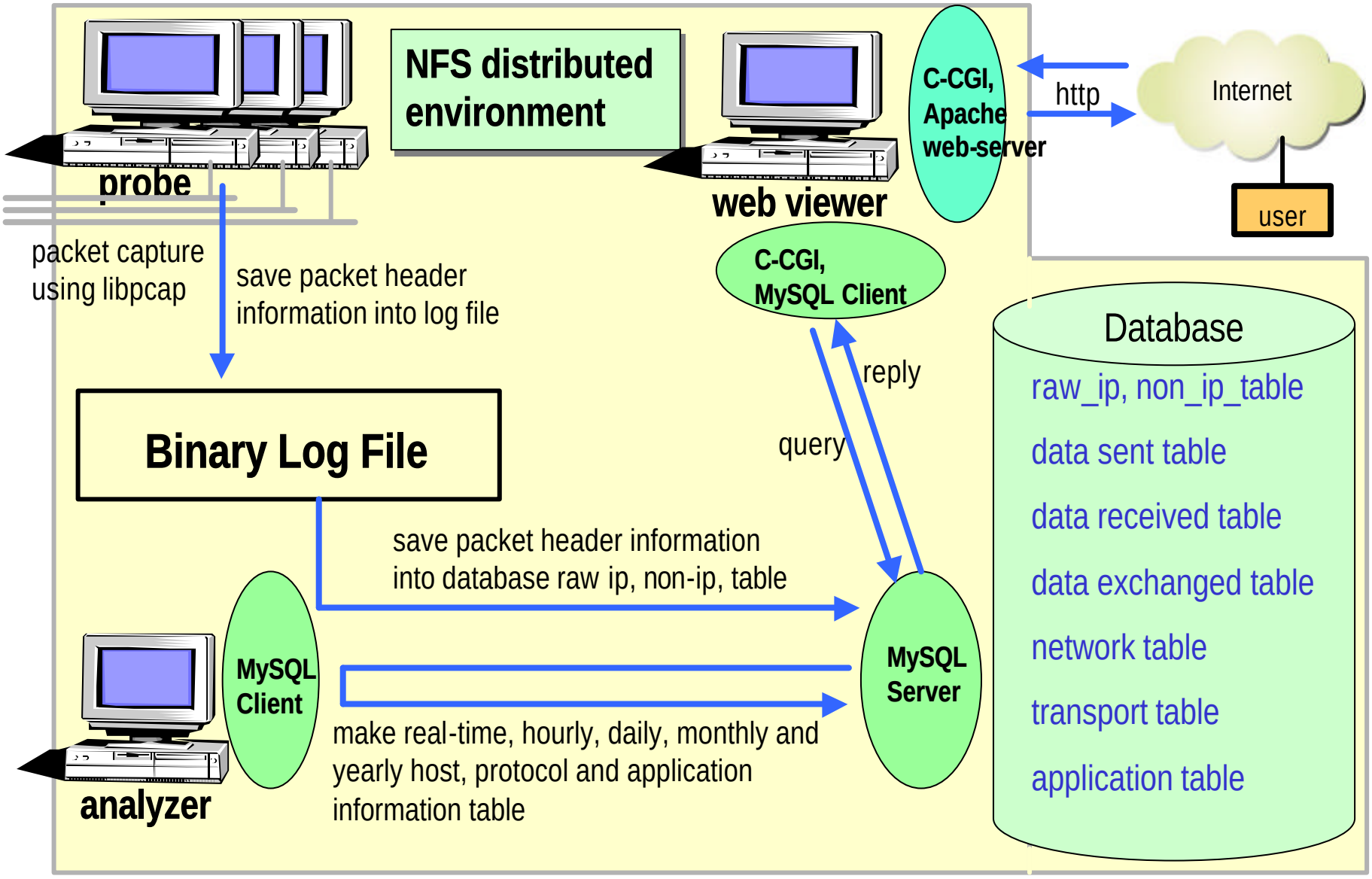


This is a *_network_table example. network_table has IP information from raw_ip_table and ARP and so on information from raw_non_ip_table.

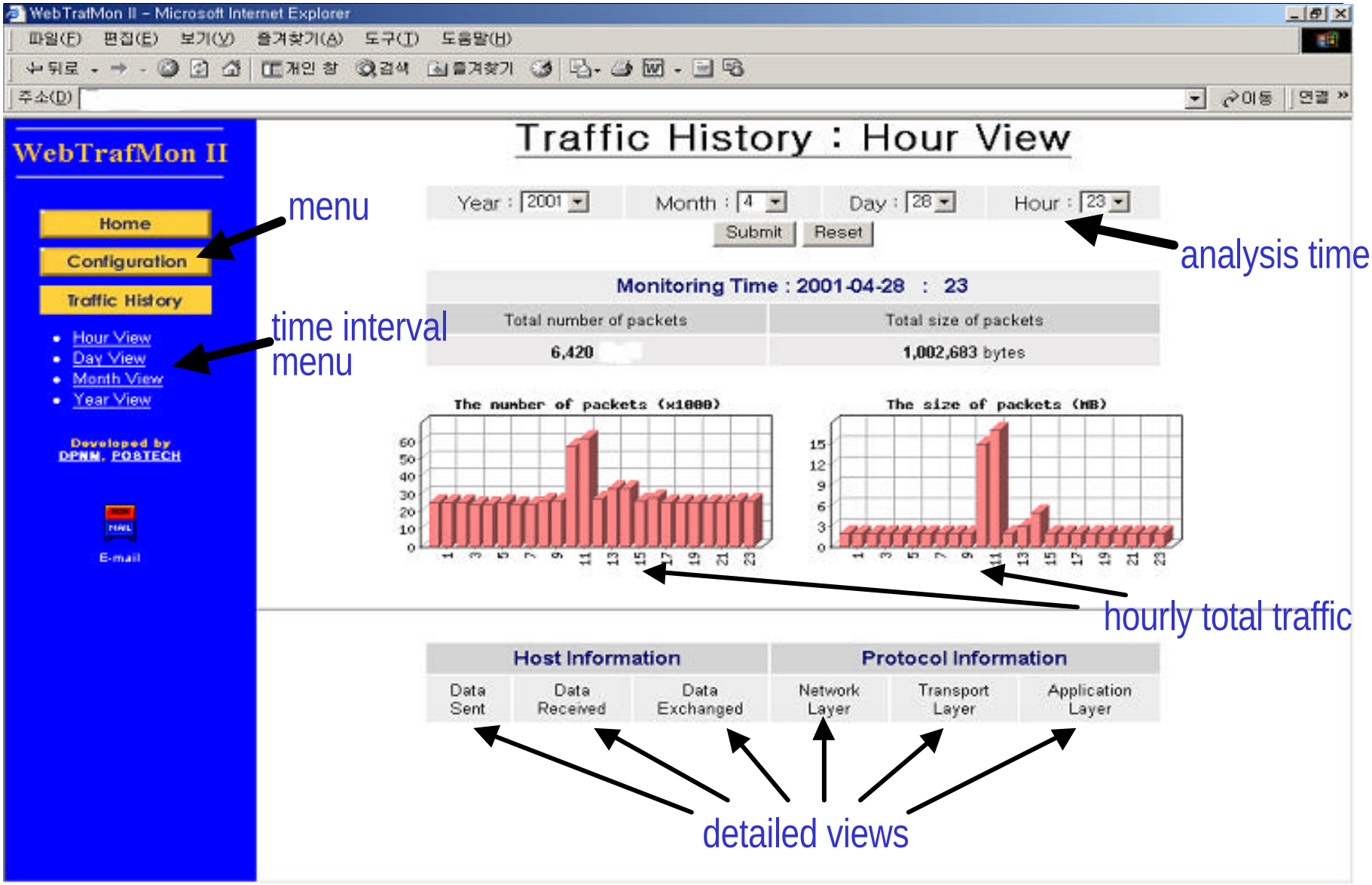
Web Viewer Module Design



Implementation

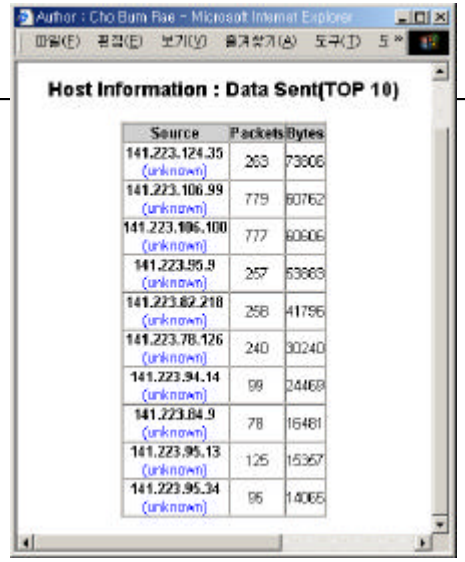


Web-based User Interface: Main View



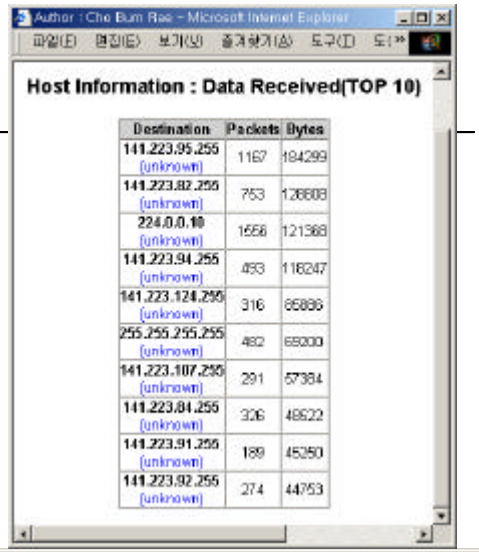
Detailed Views

1



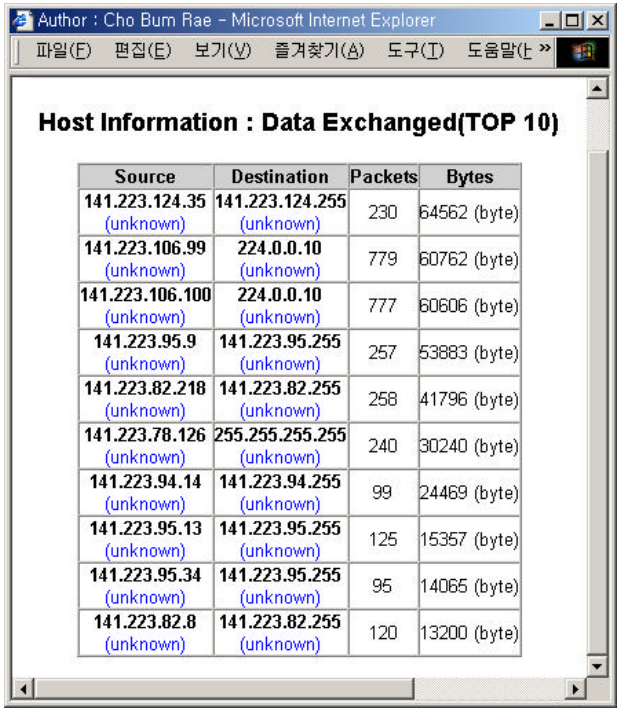
Source	Packets	Bytes
141.223.124.35 (unknown)	263	73606
141.223.106.99 (unknown)	779	60762
141.223.106.100 (unknown)	777	60606
141.223.95.9 (unknown)	257	53883
141.223.82.218 (unknown)	258	41796
141.223.78.126 (unknown)	240	30240
141.223.94.14 (unknown)	99	24469
141.223.84.9 (unknown)	78	16481
141.223.95.13 (unknown)	125	15357
141.223.95.34 (unknown)	95	14065

2



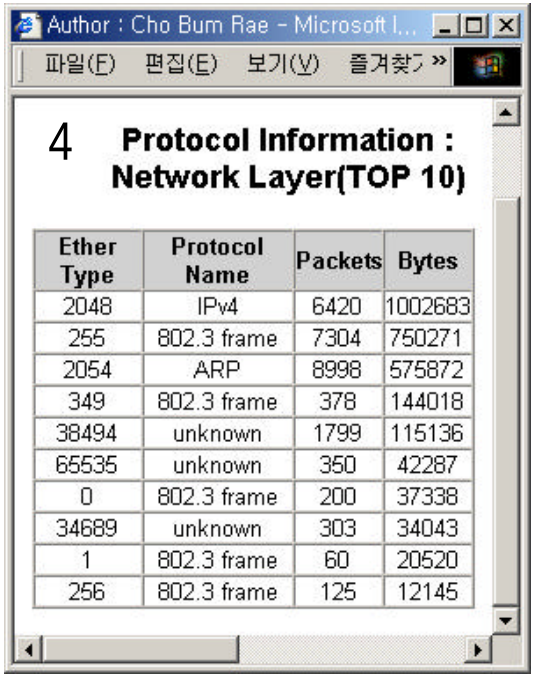
Destination	Packets	Bytes
141.223.95.255 (unknown)	1167	184299
141.223.82.255 (unknown)	753	126608
224.0.0.10 (unknown)	1556	121368
141.223.94.255 (unknown)	493	116247
141.223.124.255 (unknown)	316	85886
255.255.255.255 (unknown)	482	69300
141.223.107.255 (unknown)	291	57384
141.223.84.255 (unknown)	326	48622
141.223.91.255 (unknown)	189	45350
141.223.92.255 (unknown)	274	44753

3



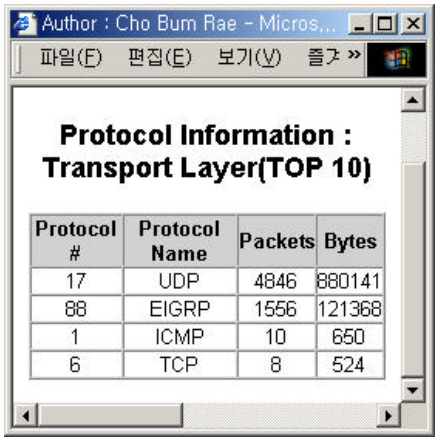
Source	Destination	Packets	Bytes
141.223.124.35 (unknown)	141.223.124.255 (unknown)	230	64562 (byte)
141.223.106.99 (unknown)	224.0.0.10 (unknown)	779	60762 (byte)
141.223.106.100 (unknown)	224.0.0.10 (unknown)	777	60606 (byte)
141.223.95.9 (unknown)	141.223.95.255 (unknown)	257	53883 (byte)
141.223.82.218 (unknown)	141.223.82.255 (unknown)	258	41796 (byte)
141.223.78.126 (unknown)	255.255.255.255 (unknown)	240	30240 (byte)
141.223.94.14 (unknown)	141.223.94.255 (unknown)	99	24469 (byte)
141.223.95.13 (unknown)	141.223.95.255 (unknown)	125	15357 (byte)
141.223.95.34 (unknown)	141.223.95.255 (unknown)	95	14065 (byte)
141.223.82.8 (unknown)	141.223.82.255 (unknown)	120	13200 (byte)

4



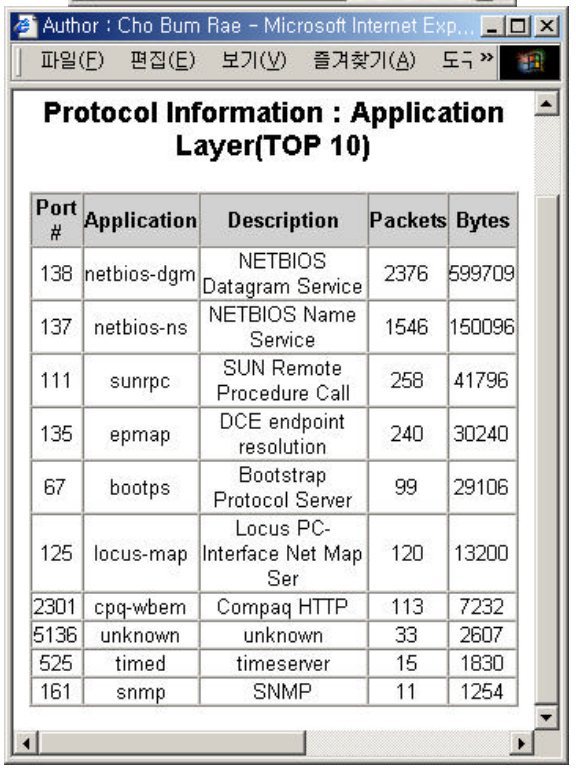
Ether Type	Protocol Name	Packets	Bytes
2048	IPv4	6420	1002683
255	802.3 frame	7304	750271
2054	ARP	8998	575872
349	802.3 frame	378	144018
38494	unknown	1799	115136
65535	unknown	350	42287
0	802.3 frame	200	37338
34689	unknown	303	34043
1	802.3 frame	60	20520
256	802.3 frame	125	12145

5



Protocol #	Protocol Name	Packets	Bytes
17	UDP	4846	880141
88	EIGRP	1556	121368
1	ICMP	10	650
6	TCP	8	524

6



Port #	Application	Description	Packets	Bytes
138	netbios-dgm	NETBIOS Datagram Service	2376	599709
137	netbios-ns	NETBIOS Name Service	1546	150096
111	sunrpc	SUN Remote Procedure Call	258	41796
135	epmap	DCE endpoint resolution	240	30240
67	bootps	Bootstrap Protocol Server	99	29106
125	locus-map	Locus PC-Interface Net Map Ser	120	13200
2301	cpq-wbem	Compaq HTTP	113	7232
5136	unknown	unknown	33	2607
525	timed	timeserver	15	1830
161	snmp	SNMP	11	1254

Summary & Future Work

- WebTrafMon II overcomes many shortcomings of existing monitoring and analysis systems.
- can analyze real-time and hourly, daily, monthly and yearly network traffic data.
- With load balancing, independent packet capture prevents packet drops from monitoring system overload.
- WebTrafMon II can analyze multiple network points traffic.
- Future work on WebTrafMon II
  - More analysis on host and application relationships.
  - Adapt to monitor and analyze other types of IP networks (IPoA, IPoWDM, etc.)
  - Traffic analysis based on contents (video, audio, etc.)