WebTrafMon: Web-based Internet/Intranet Network Traffic Monitoring and Analysis System

POSTECH DPE Lab.

권 순선

Contents

- Introduction
- Related Work
- System Requirements
- System Design
- Implementation
- Demo & Our experience
- Conclusion and Future work

Introduction

- More systems are connected to the network
- More applications are developed with direct relation with network
- The popularity of Internet and WWW
- Increasing network traffic!!!

Introduction(2)

- Network traffic analysis became an important factor

- how much traffic is transferred?
- what type of traffic is transferred?
- which system or application is causing bottlenecks?

Introduction(3)

- MRTG, Etherfind, Argus, TCPdump……
  - none of them satisfied us
- WebTrafMon!
  - Benefits of Web
  - Show host information
  - Show protocol information

Related Work-MRTG

- Web-based traffic monitor system
- using SNMP
- Long term analysis

- Cannot show host information
- Cannot show protocol information

Related Work-Packet capturing tools

- Etherfind, NFSwatch
  - system specific interface
- TCPdump

- Does not provide Web interface
- No analysis facility
  - inappropriate for long term analysis

Related Work-Argus

- Generic IP network transaction auditing tool
- Mostly for network security
  - detect service failure, DOS(Denial Of Service) attacks, network configuration problems
- Does not provide Web interface
- Missing detailed protocol information

Related Work-Summary

	MRTG	Etherfind	NFSwatch	TCPdump	Argus
Web-based?	Yes	No	No	No	No
Analysis capability?	Yes	No	No	No	Yes
Per Host Traffic Information?	No	No	No	No	Yes
Per Protocol Traffic Information?	No	No	No	No	No

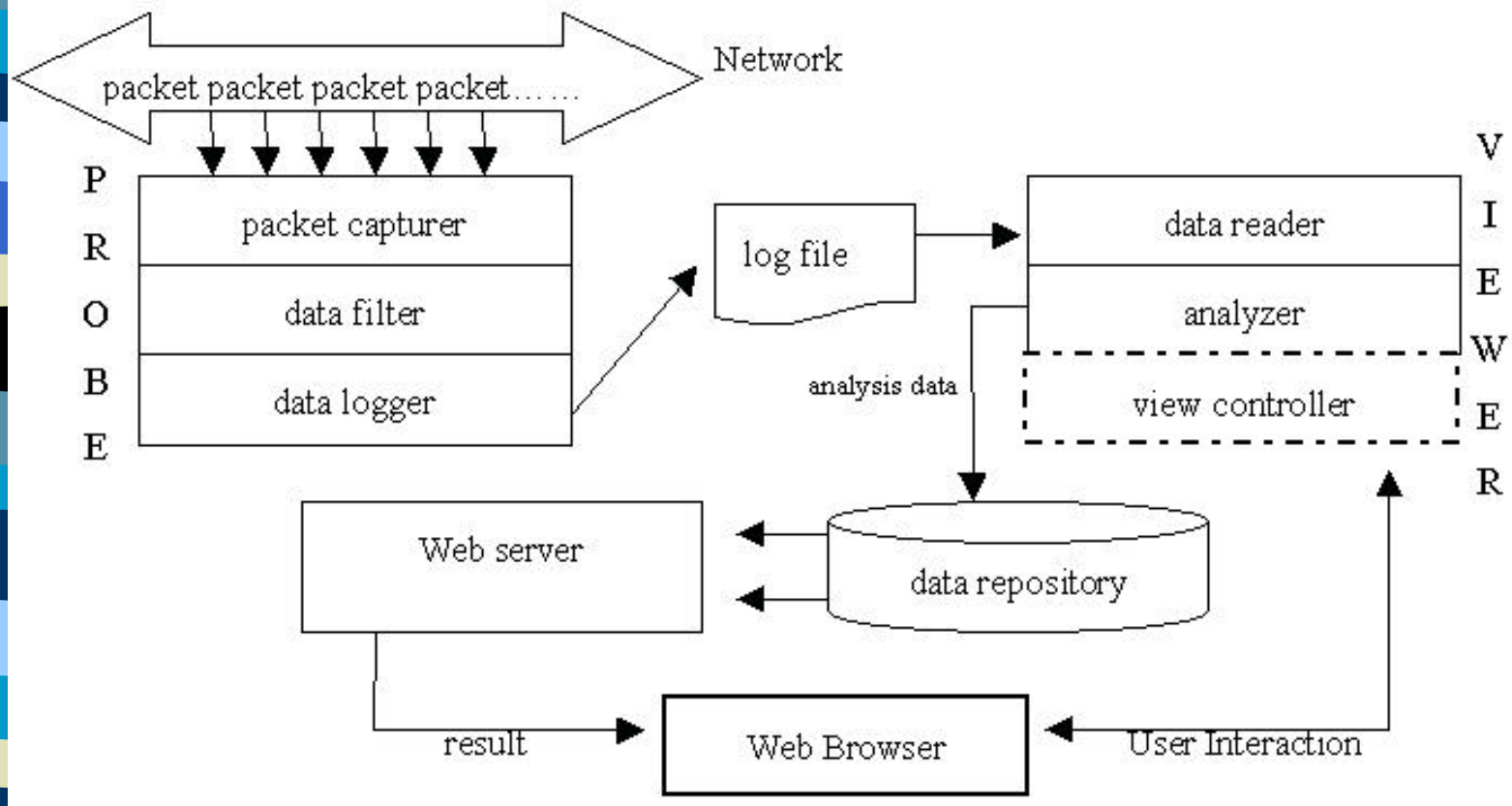
Requirements

- Platform Independence
- Web-based User Interface
  - system independent
  - location independent
  - anytime, anywhere, anyone can use it
  - beautiful user interface and ubiquitous browser
- Guaranteed Packet Capturing
  - for the accuracy of traffic information

Requirements(2)

- Classification of all possible protocol information
  - show information per each network layer
- Mobility
- Security
- Real-time & Historical Traffic information analysis

Design


packet packet packet packet……
Network
P
R
O
B
E
packet capturer
data filter
data logger
log file
data reader
analyzer
view controller
V
I
E
W
E
R
analysis data
Web server
data repository
result
Web Browser
User Interaction

Design-probe

- MAC layer
  - packet size
- Network layer
  - IP(host information), ARP, RARP….
- Transport layer
  - TCP, UDP….
- Application layer
  - Telnet, FTP, HTTP….

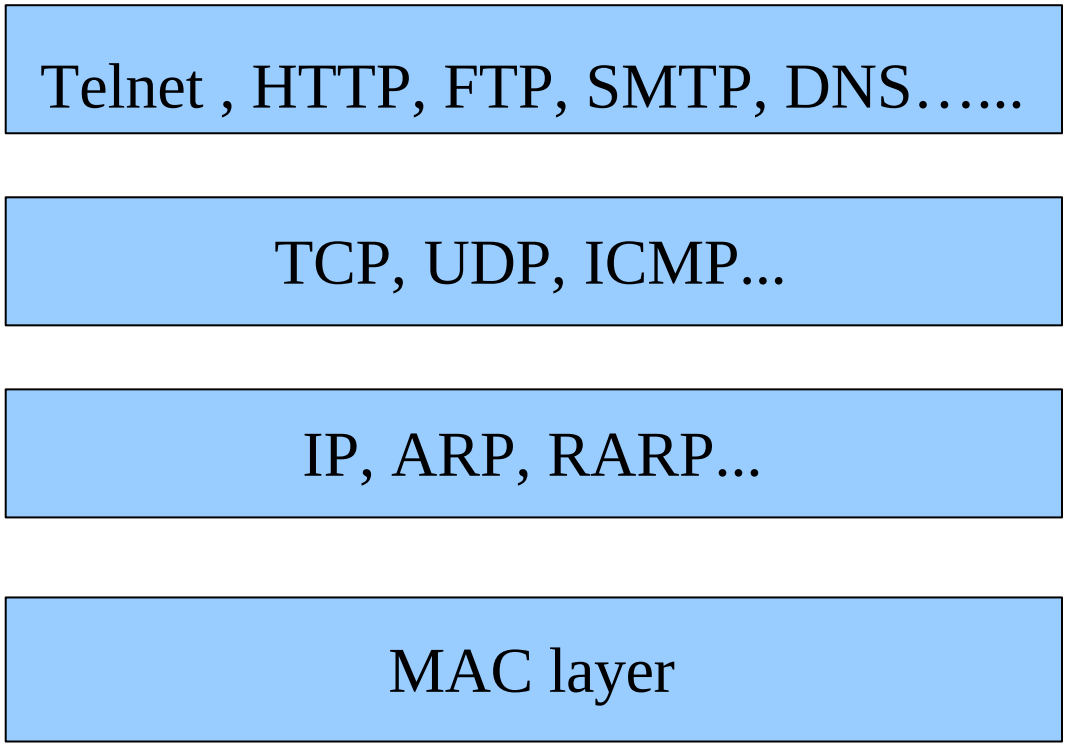
Design-viewer

- Data reader
  - read the log file that the probe has generated
- Analyzer
  - analyze information that the view controller has requested
- View controller
  - user interaction via Web browser

Implementation

- Operating System
  - Linux(kernel 2.0.32)
  - Intel x86
- libpcap 0.4a6
- Perl 5.004_01
- Apache Web Server 1.2.5

Implementation-probe

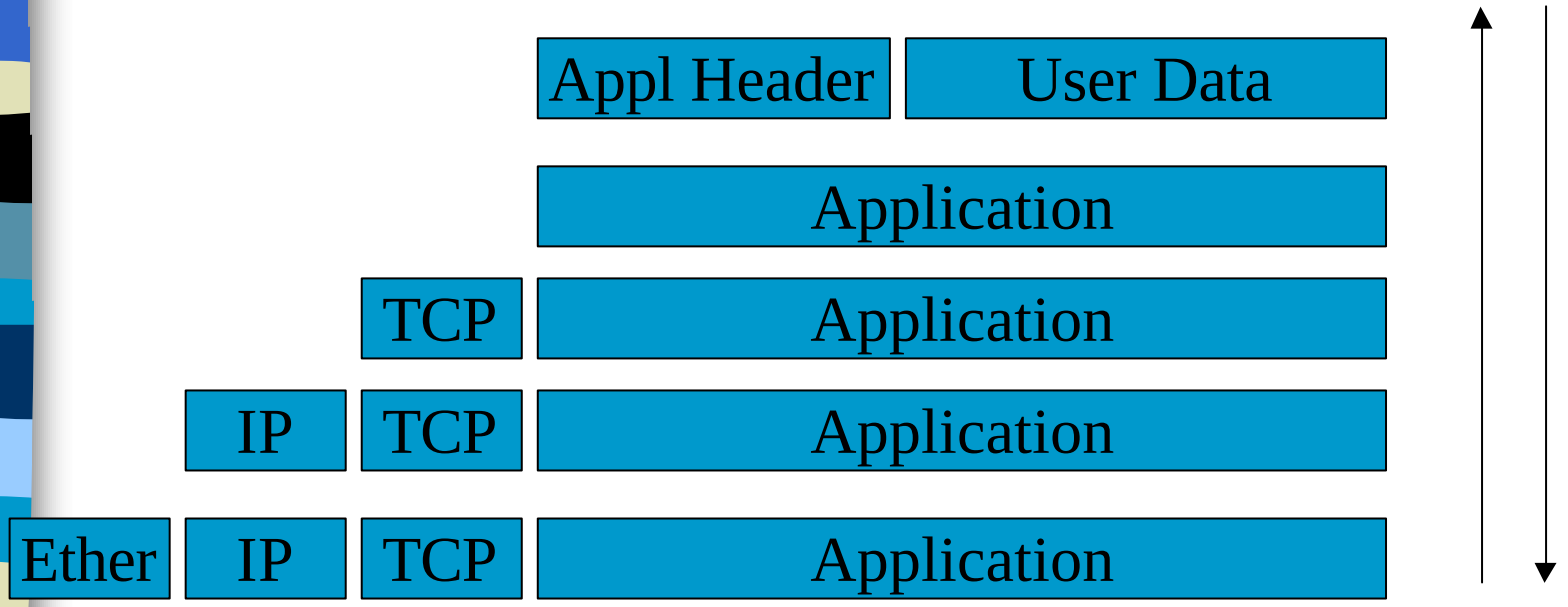


Implementation-probe(2)

- Using libpcap
  - system independent packet capturing library

346	164.124.96.18	141.223.82.4	udp	telnet
64	141.223.82.4	141.223.82.26	tcp	http
112	rarp			
64	arp			
74	141.223.99.99	141.223.82.28	icmp	

Implementation-probe(3)



Implementation-viewer

- Using Perl
  - good for text processing
  - classify each field of the log file and sort them
- Enable password checking for security

Demo & Our experience

- Live demonstration
- Our experience

Conclusion and Future work

- New Network Traffic Monitoring System
  - Web-based system
    - anytime, anywhere, anyone can use it easily
  - Show host information
    - source, destination, source-destination pair
  - Show protocol information
    - classified information per each network layer
  - Long term analysis as well as short term(Real-time) analysis

Conclusion and Future work(2)

- Speed enhancement
  - processing a larger log file
- Integrate with MRTG
  - configure to run when the network traffic peaks