# Report on Information Networking Seminar II: Design and Implementation of Network Analyzers
## — Challenges Toward Advanced Network Education in Osaka University —

Hiroyuki Ohsaki and Go Hasegawa

Department of Information Networking
Graduate School of Information Science and Technology, Osaka University
1-3, Machikaneyama, Toyonaka, Osaka 560-8531, Japan
Tel: +81-6-6850-6611, Fax: +81-6-6850-6614
E-mail: {oosaki,hasegawa}@ist.osaka-u.ac.jp

# Abstract

This paper reports on Information Networking Seminar II "Design and Implementation of Network Analyzers" conducted in 2002 at Osaka University Graduate School of Information Science and Technology's networking department. A seminar called "Information Networking Seminar II" was conducted in the second semester of 2002 (180 min. × 15 classes) with 29 graduate students in the Department of Information Networking. Students taking this seminar did not treat a network as merely a "black box" but rather analyzed traffic passing through a network in detail and, moreover, mastered extremely advanced network technology through the advanced network programming performed. This seminar was extremely unique and yet the educational impact was extremely substantial. There are two goals of this seminar. First is a deeper understanding a working TCP/IP network at its protocol level through actually observing traffic flowing on a TCP/IP network using existing network analyzers. Next is having students taking the seminar perform design and implementation of network analyzers themselves through reference to existing network analyzers and master advanced network programming techniques.

# Keywords

Information Networking, Network Analyzer, TCP/IP Network, Network Protocol, Network Programming

# 1 Introduction

This paper reports on Information Networking Seminar II “Design and Implementation of Network Analyzers” conducted in 2002 at Osaka University Graduate School of Information Science and Technology’s networking department [1]. A seminar called “Information Networking Seminar II” was conducted in the second semester of 2002 (180 min. × 15 classes) with 29 graduate students in the Department of Information Networking. Students taking this seminar did not treat a network as merely a “black box” but rather analyzed traffic passing through a network in detail and, moreover, mastered extremely advanced network technology through the advanced network programming performed. This seminar was extremely unique and yet the educational impact was extremely substantial.

There are two goals of this seminar. First is a deeper understanding a working TCP/IP network [2] at its protocol level through actually observing traffic flowing on a TCP/IP network using existing network analyzers. Next is having students taking the seminar perform design and implementation of network analyzers themselves through reference to existing network analyzers and master advanced network programming techniques.

This seminar consists of four topics: (1) mastery of typical network analyzers such as tcpdump [3] or Ethereal [4], (2) design and implementation of a traffic volume analysis and visualization program using a pcap library [3] (general-purpose packet capture library), (3) design and implementation of a TCP/IP protocol analysis program, and (4) devising and specification design of an application (DoS attack detection program, intrusion detection system, etc.) using the network analyzer.

The structure of this report is as follows. First, Osaka University Graduate School of Information Science and Technology’s Department of Information Networking, which conducted the seminar, is introduced in Section 2. What type of software a network analyzer, as was handled in this seminar, is is explained in Section 3. Additionally, details of the network analyzer exercise conducted in Information Networking Seminar II are explained in Section 4. Impressions of students taking this seminar are listed in Section 5. Finally, a summary of this report and topics for the future are discussed in Section 6.

# 2 Introduction to the Department of Information Networking

Osaka University Graduate School of Information Science and Technology’s Department of Information Networking [1] is a new organization that was established in the year 2002 and implements specialized and advanced education relating to network technologies. The Department of Information Networking was established on the basis of the following philosophy.

For a communication-oriented society that began with phone networks providing means of communication that overcome the distance between people, the formation of a new society oriented towards advanced information communication is becoming a reality through the appearance of modes of communication processing including information processing between people and computers and between computers themselves. In recent years, the development of information networks in particular, without being limited to a revolution in the structure of an industrial society, has changed lifestyles in civil society into completely new ones and today it has the potential to cause a third industrial revolution to follow the first industrial revolution accompanying the invention of the steam engine and the second industrial revolution based on oil (internal-combustion engines), electricity (electric motors), and heavy and chemical industries.

In addition, the possibility of being able to construct new information spaces that exchange and share multimedia information that overcomes distance as well as time and space network technology through fusion with multimedia technology is also apparent. Moreover, formation of spaces where information is shared free of geographical constraints through fusion with information networks including information processing has also become important with regard to mobile wireless technology that was previously developed as a means of communication between people as well. In addition, the development of network security is also essential for a safe and comfortable information-oriented society in the 21st century.

The Department of Information Networking, to shape a rich, highly reliable, and safe society oriented towards advanced information communication and to construct smart information networks to flexibly and dynamically provide multimedia information distribution, conducts education and research regarding multimedia networking technology, intelligent networking technology, distributed mobile computing technology, and information distribution platform configuration technology.

The Department of Information Networking in particular conducts encompassing education from basic technology for networks to service technology and proceeds with educational research aimed at the organic fusion of various technologies like computers and communication, wire and wireless/mobile technology, hardware and software, communications and broadcasting, and electronics and photonics that were previously developed separately while actively liaising between courses as well. Beginning with a system-oriented approach like this, the creation of new systems and services that are truly useful for a industrial society and civil society will be possible.

The Department of Information Networking offers the following six courses.

**(1)** Multimedia networking course

To conduct education and research with regard to computer network configuration technology for construction of multimedia information network infrastructure.

- Media communication processing technology
- Multimedia communication quality-of-service (QoS) technology
- Multimedia communication protocol
- Network middleware

**(2)** Intelligent networking course

To conduct education and research with regard to intelligent networking architecture based on new paradigms integrating multimedia information transmission networks and network control networks.

- Intelligent optical network technology
- Network technology fusing communications and broadcasting
- Advanced service control architecture

**(3)** Information distribution platform course

To conduct education and research from the aspects of both hardware and software with regard to information distribution platforms combining network and information processing features for the support of information industries such as e-commerce, inter-corporate communication, and content distribution.

- High-reliability platform configuration technology
- Content distribution networks
- E-commerce architecture

**(4)** Mobile computing course

To conduct education and research with regard to construction of large-scale network systems and middleware fusing mobile communication environments and high-speed information communication networks and new information processing technology fusing wireless communication technology and distributed processing technology.

- Mobile computing and ad-hoc networks
- Network protocols
- Information processing technology for networks

**(5)** Advanced network architecture course (cooperative course with Cybermedia Center)

To conduct education and research with regard to advanced network architecture for high-speed broadband networks to construct advanced information communication infrastructure.

- High-speed protocol processing technology
- Photonic Internet technology
- High-speed switching processing technology
- High-speed end-system configuration technology

**(6)** Cyber-communication course (course in concert with Nippon Telegraph and Telephone Corporation)

To conduct education and research with regard to a variety of technology to achieve natural communication between people in cyberspace.

- Cyber-community formation technology
- Cyber-communication basic technology
- Multimedia content distribution technology

## 3 Network Analyzer

In this seminar, all of the students taking it received a deeper understanding of a workings TCP/IP network at the protocol level by first operating a network analyzer themselves and then observing traffic passing through a TCP/IP network [2]. Thus, what sort of features the network analyzer used in this seminar has and what sort of purposes it can be used for are explained in this section.

A network analyzer is software to collect packets passing through a TCP/IP network and to analyze the contents of communication at the protocol level. A network analyzer is normally equipped with both sniffer and analyzer features. First, all packets passing through a TCP/IP network, regardless of whether the packet is self-addressed or addressed to someone else, are collected using the sniffer features. Then, the header information and payload of collected packets and what sort of communication is being performed are analyzed using the analyzer features.

In this seminar, Ethernet is used for a layer-2 network and TCP/IP for a layer-3 network. With Ethernet, all of the packets (Ethernet frames) can be collected through operation of the network interface in a special operating mode called “promiscuous mode”.

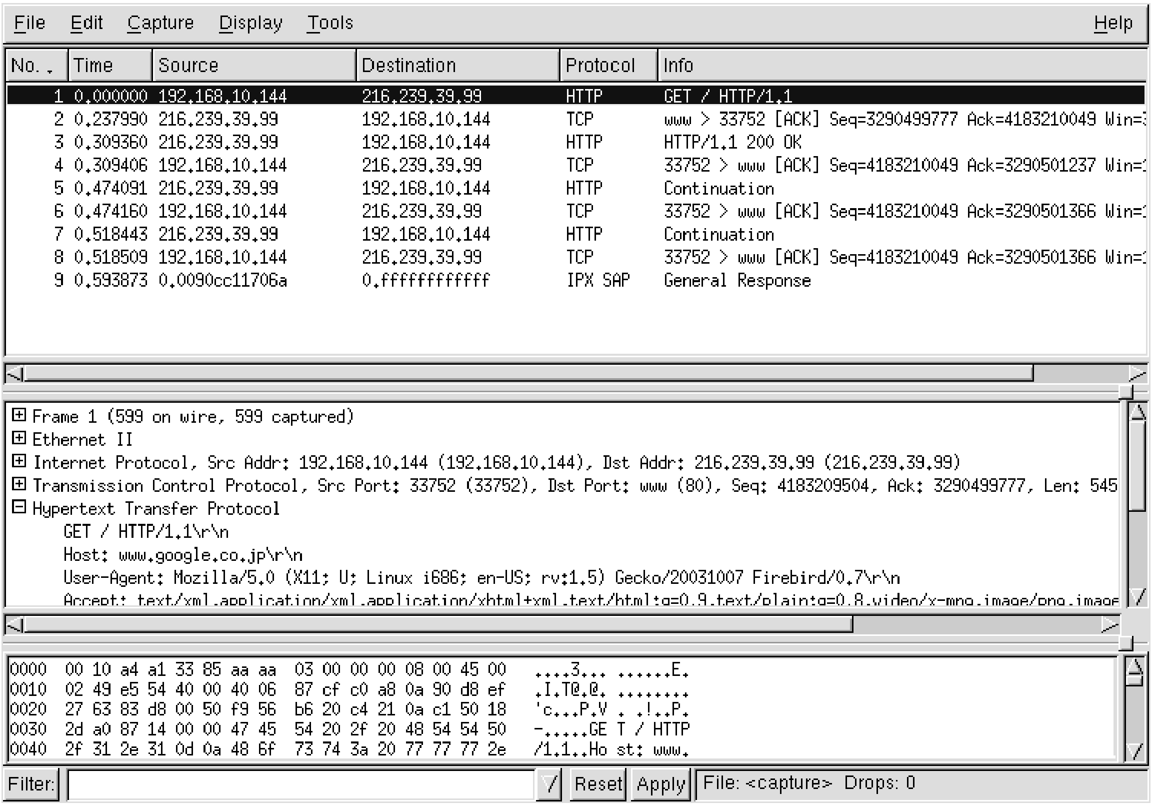
Specifically what sort of communication (WWW, e-mail, file transfer, etc.) is being performed in the network can be analyzed through use of the network analyzer. A network analyzer can generally be used for protocol analysis for networks, fault diagnosis for networks, and the like.

In this seminar, tcpdump [3] and Ethereal [4], which can be used freely, were used as typical network analyzers. tcpdump is a network analyzer that was developed by Van Jacobson and is operated with a command line; it allows analysis of a variety of network protocols such as IPv4, ICMPv4, IPv6, ICMPv6, UDP, TCP, SNMP, AFS, BGP, RIP, PIM, DVMRP, IGMP, SMB, OSPF, and NFS. tcpdump examples are shown in Fig. 1. Here, results of running tcpdump when accessing `http://www.google.co.jp/` from a WWW browser are indicated.

```
17:02:30.340910 192.168.10.144.33752 > 216.239.39.99.www: P 4183210049:4183210594(545) ack \
3290501366 win 17520 (DF)
17:02:30.342849 192.168.10.144.32783 > 192.168.10.1.domain:  18792+ PTR? 99.39.239.216.in-a\
ddr.arpa. (44) (DF)
17:02:30.579423 216.239.39.99.www > 192.168.10.144.33752: . ack 545 win 30660 [tos 0x10]
17:02:30.596622 216.239.39.99.www > 192.168.10.144.33752: . ack 545 win 30660 [tos 0x10]
17:02:30.632244 216.239.39.99.www > 192.168.10.144.33752: . ack 545 win 30660 [tos 0x10]
17:02:30.649372 216.239.39.99.www > 192.168.10.144.33752: . ack 545 win 30660 [tos 0x10]
17:02:30.653463 216.239.39.99.www > 192.168.10.144.33752: P 1:1461(1460) ack 545 win 32120 \
[tos 0x10]
17:02:30.653494 192.168.10.144.33752 > 216.239.39.99.www: . ack 1461 win 20440 (DF)
17:02:30.671764 216.239.39.99.www > 192.168.10.144.33752: P 1:1461(1460) ack 545 win 32120 \
[tos 0x10]
17:02:30.671834 192.168.10.144.33752 > 216.239.39.99.www: . ack 1461 win 20440 (DF)
17:02:30.792474 216.239.39.99.www > 192.168.10.144.33752: P 1461:1590(129) ack 545 win 3212\
0 [tos 0x10]
17:02:30.792551 192.168.10.144.33752 > 216.239.39.99.www: . ack 1590 win 20440 (DF)
17:02:30.877994 192.168.10.1.domain > 192.168.10.144.32783:  18792 NXDomain 0/1/0 (104) (DF)
17:02:30.878604 192.168.10.144.32783 > 192.168.10.1.domain:  18793+ PTR? 144.10.168.192.in-\
addr.arpa. (45) (DF)
17:02:31.002532 192.168.10.1.domain > 192.168.10.144.32783:  18793 NXDomain 0/1/0 (122) (DF)
17:02:31.003042 192.168.10.144.32783 > 192.168.10.1.domain:  18794+ PTR? 1.10.168.192.in-ad\
dr.arpa. (43) (DF)
17:02:31.101979 192.168.10.1.domain > 192.168.10.144.32783:  18794 NXDomain 0/1/0 (120) (DF)
```

Figure 1: tcpdump examples (accessing `http://www.google.co.jp/`)

Ethereal [4] is a network analyzer operated with a graphical user interface (GUI) on a UNIX or Windows platform. Ethereal can currently be used to analyze 407 types of protocols. Ethereal examples are shown in Fig. 2. Here, results of running Ethereal when accessing `http://www.google.co.jp/` from a WWW browser are indicated.



```
No. . Time     Source            Destination       Protocol  Info
    1 0.000000 192.168.10.144    216.239.39.99     HTTP      GET / HTTP/1.1
    2 0.237990 216.239.39.99     192.168.10.144    TCP       www > 33752 [ACK] Seq=3290499777 Ack=4183210049 Win=3
    3 0.309360 216.239.39.99     192.168.10.144    HTTP      HTTP/1.1 200 OK
    4 0.309406 192.168.10.144    216.239.39.99     TCP       33752 > www [ACK] Seq=4183210049 Ack=3290501237 Win=1
    5 0.474091 216.239.39.99     192.168.10.144    HTTP      Continuation
    6 0.474160 192.168.10.144    216.239.39.99     TCP       33752 > www [ACK] Seq=4183210049 Ack=3290501366 Win=1
    7 0.518443 216.239.39.99     192.168.10.144    HTTP      Continuation
    8 0.518509 192.168.10.144    216.239.39.99     TCP       33752 > www [ACK] Seq=4183210049 Ack=3290501366 Win=1
    9 0.593873 0.0090cc11706a    0.ffffffffffff    IPX SAP   General Response
```

```
⊞ Frame 1 (599 on wire, 599 captured)
⊞ Ethernet II
⊞ Internet Protocol, Src Addr: 192.168.10.144 (192.168.10.144), Dst Addr: 216.239.39.99 (216.239.39.99)
⊞ Transmission Control Protocol, Src Port: 33752 (33752), Dst Port: www (80), Seq: 4183209504, Ack: 3290499777, Len: 545
⊟ Hypertext Transfer Protocol
     GET / HTTP/1.1\r\n
     Host: www.google.co.jp\r\n
     User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.5) Gecko/20031007 Firebird/0.7\r\n
     Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image
```

```
0000  00 10 a4 a1 33 85 aa aa  03 00 00 00 08 00 45 00   ....3... ......E.
0010  02 49 e5 54 40 00 40 06  87 cf c0 a8 0a 90 d8 ef   .I.T@.@. ........
0020  27 63 83 d8 00 50 f9 56  b6 20 c4 21 0a c1 50 18   'c...P.V . .!..P.
0030  2d a0 87 14 00 00 47 45  54 20 2f 20 48 54 54 50   -.....GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
```

```
File: <capture>  Drops: 0
```

Figure 2: Ethereal examples (accessing `http://www.google.co.jp/`)

# 4 Information Networking Seminar II: Network Analyzer Exercise

Details of network analyzer exercise conducted in Information Networking Seminar II will be explained in this section.

In this seminar, all of the students participating were not assembled into a classroom and the exercise conducted; rather, the exercise was conducted in laboratories the individual students participating are assigned to. Thus, all of the materials relating to exercise problems were included on WWW pages and e-mail was used for contacting students from instructors and questions from students to instructors.

Three exercise problems as conducted in this seminar are introduced below.

## 4.1 Problem 1: Create a simple program to use tcpdump/Ethereal

### Goals

Learn how to use a free network analyzer such as tcpdump or Ethereal. Using VMware Workstation, consider what sort of information and to what extent can be obtained with these tools by actually collecting packets.

### Exercise preparations

**(1)** Install the trial version of VMware Workstation 3.2 [5]

You can try the application for 30 days with the trial version, so install it on the PC you are using (we will switch to a licensed version later). Use Windows 2000/XP for the host OS. Contact the instructor responsible before 2002/11/8 (Fri.) if you want to use Linux as the host OS.

**(2)** Install Linux (either RedHat 7.3/8.0 English version or Debian GNU/Linux 3.0) as the VMware guest OS

Be sure to use the version specified.

**(3)** Install tcpdump [3] and Ethereal [4]

Use version 3.6 or above for tcpdump and version 0.9.4 or above for Ethereal.

**(4)** Carefully read the manuals and related documentation for tcpdump and Ethereal

Refer to online manuals, related WWW pages, etc. and understand each tool. Understanding of these tools is required for Problem 2.

#### Exercise content

**(1)** Learn methods of traffic analysis using Ethereal.

A variety of protocol traffic will occur between the host and guest OSs; capture it using the Ethereal tool. Based on those results, check in detail what sort of information can be obtained to the extent possible.

**(2)** Learn methods of traffic analysis using tcpdump.

A variety of protocol traffic will occur between the host and guest OSs; capture it using the tcpdump tool. Based on those results, check in detail what sort of information can be obtained to the extent possible.

**(3)** Discuss the differences in the two tools (tcpdump and Ethereal) and their advantages and disadvantages.

Run tcpdump and Ethereal in a guest OS in VMware. Do not capture network traffic in the laboratory without permission from the instructor of the laboratory you are assigned to.

Use host-only mode as the type of network when installing the VMware guest OS. If you inadvertently use bridged mode, this may inconvenience other computers, so use caution.

#### Report

Create a report with regard to Problem 1 and submit it by e-mail to the instructor responsible by 2002/11/19 (Tues.) 17:00. Submit it by in the form of a file in PDF or PostScript format attached to e-mail.

For this, look at the protocol list as listed on the WWW and report on the individually assigned protocol. The format of the report is not specified, but describe how problems were addressed, what results were obtained, what your thoughts were, and the like in easily understandable form and in detail to the extent possible. Use about 10 A4 pages, single-spaced as a guideline. The contents of the report will be disclosed to other students participating at a later date.

### 4.2 Problem 2: Create traffic volume analysis programs

#### Exercise goals

The goals of the current exercise are to be able to create programs like those below.

**(1)** A program to collect traffic flowing on a network using a pcap library.

**(2)** A program to analyze a variety of traffic characteristics based on collected packets.

**(3)** A program to display the traffic characteristics analyzed on screen as a graph.

#### Exercise content

**(1)** Create a traffic collection program using a pcap library.

Create a program using libpcap to collect all of the packets flowing on the network. With regard to each packet collected, display as much information as possible such as the sending time, protocol type, protocol version, and packet length in text format.

With regard to IP packets, display as much information as possible such as the IP address of the sending host, the IP address of the receiving host, and IP options.

With regard to UDP/TCP packets, display as much information as possible such as the port number of the sending host, the port number of the receiving host, the sequence number, and checksums.

You can refer to source code such as tcpdump or Ethereal. Use C or C++ as the development language. You are free to select an OS for the development platform and type of compiler.

**(2)** Create a program to analyze traffic characteristics.

Using results output from the program developed in (1), analyze statistical information for traffic flowing on the network. Specifically, create a program to check statistical information traffic like that below.

You are free to select a development language, development platform, compiler, and the like. This would probably be easy using a scripting language Perl or Ruby. It may be implemented via an Excel macro.

- Analyze statistical information for traffic

  Create a program to output in text format statistical information for traffic like that below at the specified time interval [s].

  - Average transmission rate [Mbit/s]
  - Total amount of data transmitted [byte]
  - Average packet length [byte]
  - Average packet arrival interval [s]

  For example, when the time interval is 10.0 [s], output the distribution above for $0 \leq t < 10, 10 \leq t < 20 \ldots$.

  With regard to both sent packets and received packets, output four types of results for the total for all packets, IP packets only, TCP packets only, and UDP packets only (i.e., a total of 8 types).

  Analysis of the traffic distribution is the goal. You are free to design program details such as the output format.

**(3)** Create a program to display analysis results as a graph.

Create a program to display statistical information and the distribution for traffic obtained with the program developed in (2) as a graph.

The goal is to visualize how statistical information for traffic varies and what sort of distribution traffic takes for each type of protocol. Devise a technique allowing an easily understandable graph such as using a three-dimensional graph or histogram.

Actually collect network traffic and display statistical information and the distribution for that traffic as a graph.

You are free to select a development language, development platform, compiler, and the like. This would probably be easy using a scripting language Tcl/Tk, Perl/Tk, or Ruby/Tk. Use of Excel, Gnuplot, or the like is acceptable.

### Report

Create a report with regard to Problem 2 and submit it by e-mail to the instructor responsible by 2002/12/10 (Tues.) 17:00. Submit it by in the form of a file in PDF or PostScript format attached to mail. The format of the report is not specified, but describe how problems were addressed, what results were obtained, what your thoughts were, and the like in easily understandable form and in detail to the extent possible. Use about 10 A4 pages, single-spaced as a guideline. The contents of the report will be disclosed to other students participating at a later date.

## 4.3 Problem 3: Create protocol analysis programs

### Exercise goals

The goals of the current exercise are to be able to create/design programs like those below.

**(1)** Create a program to trace TCP sessions and analyze the content of communications.

**(2)** Design an application.

**Exercise content**

**(1)** Create a program to trace TCP sessions and analyze the content of communications.

Create a program to collect packets flowing on the network and analyze the content of communications for a specific TCP session. Display analysis results in text format. Use the traffic collection program created in Problem 2 (adding features if needed ) to collect packets.

TCP session is differentiated by the IP address of the sending host, the IP address of the receiving host, the port number of the sending host, the port number of the receiving host, and the initial sequence number.

For output results of the program to create, look only at those and include information only for protocol operations such as HTTP and FTP that can be analyzed. Output results in Ethereal (i.e., Tools → Follow TCP Stream) may serve as a reference. Be careful with establishment/disconnection of TCP sessions and resending control for TCP.

You are free to design program details. You are free to select a development language, development platform, compiler, and the like. This would probably be easy using a scripting language Perl.

**(2)** Design an application.

Use the knowledge you obtained in the "network analyzer exercise," consider two types of applications, and design one. Expect free thought such as a program to detect denial-of-service service (DoS) attacks or an intrusion detection system (IDS) through the collection of traffic flowing on a network.

Perform concept design of the application considered and summarize those details in a report (one per application, about 2–4 A4 pages). Include information such as the concept, envisaged use, features, characteristics, advantages, disadvantages, method of accomplishment, operation algorithm, and a block diagram.

**Report**

Create a report with regard to Problem 3 and submit it by e-mail to the instructor responsible by 2003/1/7 (Tues.) 17:00. Submit it by in the form of a file in PDF or PostScript format attached to e-mail.

The format of the report is not specified, but describe how problems were addressed, what results were obtained, what your thoughts were, and the like in easily understandable form and in detail to the extent possible. Use about 10 A4 pages, single-spaced as a guideline. Do not include design of the application in that page count. The contents of the report will be disclosed to other students participating at a later date.

## 5 Impressions from Students Taking the Seminar

In this section, an excerpt of impressions from students participating in this seminar as written in reports.

- Actually collecting and analyzing traffic passing through a network is necessary to achieve a safe network environment. I was able to absorb specific knowledge and technology with regard to networks through this seminar and it was extremely good study.
- The content was extremely difficult in exercise problems 1, 2, and 3 as well as through the exercise as a whole.
- The programs developed in this seminar (network analyzer exercise) were often quite practical, so there was a substantial sense of achievement for me myself. However, digesting the exercise problems took an extremely long amount of time and the workload was substantial.
- Participating in this seminar was extremely difficult, but I was able to acquire knowledge relating to networks that was completely unknown to me. For me, participating in this seminar was a very good thing.
- This seminar was difficult for students who originally did not have much background knowledge with regard to networks.
- The process from looking at the content of the problem to doing all of the problems took an extremely long amount of time. Having a little more time allocated to problems might have been better.

- I previously thought that networks were safe to a certain extent. However, I was surprised upon participating in this seminar to see in reality how easily one can actually communicate with other people. My own knowledge with respect to security has changed because I participated in this seminar. In the future, the importance of network security will increase further, so this was a meaningful exercise.
- The time allotted for each problem was short, so not adequately deepening my understanding was a regret. If it is possible to allot a little more time for each problem, then understanding can probably be deepened and satisfactory results obtained.

## 6 Summary and Future Topics

This paper reported on Information Networking Seminar II "Design and Implementation of Network Analyzers" conducted in 2002 at Osaka University Graduate School of Information Science and Technology's networking department. Through this seminar, the students participating acquired a variety of knowledge with regard to networks.

Exercises for the year 2002 were the first conducted by Osaka University Graduate School of Information Science and Technology's networking department. Although the results obtained through the conduct of the exercises was substantial, at the same time a variety of problems occurred. Lacking time to perform all of the exercise problems was frequently pointed out by students participating, so there are plans to conduct a review of the content of the exercise and exercise problems. In addition, there are plans to gauge further enhancement of the support system for students participating through the employment of postdoctoral students who participated in this seminar in the year 2002 as teaching assistants (TAs).

## References

[1] "Department of Information Networking, Graduate School of Information Science and Technology, Osaka University." `http://www.ist.osaka-u.ac.jp/net/index.html`.

[2] W. R. Stevens, *TCP/IP Illustrated, Volume 1: The Protocols*. New York: Addison-Wesley, 1994.

[3] "TCPDUMP public repository." `http://www.tcpdump.org/`.

[4] "The Ethereal network analyzer." `http://www.ethereal.com/`.

[5] I. VMWare, "Download - vmware workstation 3.2." `http://www.vmware.com/download/workstation.html`.