論文2000-37TE-3-13

객체지향형 언어를 사용한 LAN 기반의 TCP/IP 프로토콜 분석기 구현

(Implementation of LAN-based TCP/IP Protocol Analyzer using the object-oriented programming)

李是縣*, 姜廷震*, 張學信*, 曺秉珣**, 崔圭珉**, 鄭重壽***

(S.H. Lee, J.J. Kang, H.S. Chang, B.S. Cho, K.M. Choi, J.S. Jung)

요 약

본 논문에서는 윈도우 환경에서 객체지향언어(Object-Oriented Programming)를 사용하여 LAN(Local Area Network) 기반의 TCP/IP(Transmission Control Protocol/Internet Protocol) 프로토콜을 분석할 수 있는 프로토콜 분석기를 개발하였다. TCP/IP 프로토콜 분석기는 윈도우 98/NT 환경에서 VC++ 6.0을 사용하여 프로토콜을 분석할 수 있도록 인터페이스 카드, 모니터 및 에뮬레이션 소프트웨어와 GUI(Graphic User Interface)를 개발하였다. 프로토콜 분석 소프트웨어는 네트워크에서 수집(capture)되는 정보를 실시간으로 분석할 수 있도록 실시간 객체(Real-Time Object)를 사용하였고, 모니터링 기능과 에뮬레이션 기능을 제공하도록 설계하였다. 성능시험 결과 LAN 기반에서 프레임 에러(frame error) 없이 TCP/IP 프로토콜 데이터를 실시간으로 수집하고 분석할 수 있음을 보였다. 본 연구에서 개발된 프로토콜 분석기는 기존의 프로토콜 분석기보다 안정적이고 다양한 결과를 보였으며, 통신 및 네트워크 분야의 개발용으로 사용될 수 있으므로 수입대체 효과를 가져올 수 있다.

Abstract

In this paper, we develop protocol analyzer that can analyze and monitor LAN(Local Area Network)-based TCP/IP protocol using the OOP(object-oriented programming) in Windows98/NT environment. TCP/IP(Transmission Control Protocol/Internet Protocol) protocol analyzer is consist of interface hardware, protocol analysis software and GUI(Graphic User Interface). It is designed for the real-time analysis using the real-time object. In results of performance test, TCP/IP protocol analyzer is showed that it can analyze and monitor without frame error in LAN-based. Also, developed protocol analyzer operates better than conventional protocol analyzer in performance. It can be used in maintenance fields of communication and network.

* 正會員, 동서울大學 電子通信科
(Dept. of Electronic Communication, Dong Seoul College)
** 正會員, 시앤시 인스트루먼트(주)
(C & C Instrument Co.)
*** 正會員, 安東大學 電子情報産業學部
(Dept. of Electronic Information Industrial, An Dong University)
接受日字:2000年5月15日, 수정완료일:2000年9月14日

Ⅰ. 서 론

최근 정보화 사회로 이동됨에 따라 가정, 학교 및 기업 등에서 다양한 정보가 필요하게 되었고 이에 따라 정보통신 분야는 많은 변화를 가져오게 되었다. 이러한 환경 변화에 따라 통신망은 다양한 형태로 발전되고 있으며, 대학, 산업체 및 공공기관에서 정보를 공유하고 빠르게 서비스하기 위한 목적으로 LAN을 이용

하여 각종 멀티미디어 서비스를 제공하고 있다. 이러한 통신 서비스를 위한 장비개발이나 시험을 위한 프로토콜 분석기는 고가일 뿐만 아니라 전량 수입에 의존하고 있으므로 이에 대한 개발이 매우 시급한 실정이다.

따라서 본 논문에서는 기존의 프로토콜 분석기의 문제점을 개선하고 독자적인 모델 개발을 목적으로 윈도우 환경에서 객체지향 언어를 사용하여 LAN 기반의 TCP/IP 프로토콜을 분석할 수 있는 TCP/IP 프로토콜 분석기를 개발하였다. 개발된 프로토콜 분석기는 네트워크에서 데이터를 수집하기 위한 인터페이스 기능, TCP/IP 프로토콜 분석 소프트웨어 및 사용자 인터페이스를 개발하였다. 본 연구에서 개발된 TCP/IP 프로토콜 분석기는 기존의 분석기에 비해서 안정적으로 동작됨을 보였고, 지금까지 수입에 의존하여 왔던 고가의 장비에 대한 수입대체 효과를 가져올 수 있다.

Ⅱ. LAN 기반의 TCP/IP 프로토콜 분석기 설계 및 구현

1. 프로토콜 분석기 구조

프로토콜 분석기(protocol analyzer)는 네트워크 상에서 전달되고 있는 데이터를 정확하게 수집하고 이를 분석하는 것이다. LAN기반의 프로토콜 분석기는 패킷의 프로토콜 헤더를 분석하여 사용자에게 정보를 제공하는 패킷의 프로토콜 헤더 중심 방식과 패킷의 실제 데이터를 중심으로 분석하는 애플리케이션 중심 방식으로 구분된다. 개발된 프로토콜 분석기는 네트워크 상에서 교환되는 방법과 네트워크의 상황을 쉽게 분석할 수 있는 프로토콜 헤더 중심 방식으로 설계하였다.

설계한 프로토콜 분석기는 그림 1과 같이 윈도우 98/NT 환경에서 펌웨어, 에뮬레이션 소프트웨어 및 GUI로 구성된다. 에뮬레이션 블록은 인터페이스 하드웨어로부터 수집된 데이터를 분석하고 처리하는 기능이다. GUI 블록은 분석된 데이터를 사용자의 요구에 맞게 출력하고 환경을 설정하는 기능이다. 프로토콜 분석 소프트웨어는 모니터링 기능과 시뮬레이션 기능으로 구분되며, 모니터링 기능은 윈도우즈의 NDIS (Network Driver Interface Specification) 인터페이스 환경을 이용하여 인터페이스 하드웨어를 직접 제어하여 라인상으로 전송되는 데이터 패킷을 모니터링 한다. 에뮬레이션 기능은 NDIS로 인터페이스 하드웨어를 직접 컨트롤하여 사용자가 원하는 패킷생성 방식을 선택하고 가상 패킷을 생성하여 전송된 패킷과 응답은 모두 모니터링 기능을 사용하여 결과를 분석한다.

TCP/IP 프로토콜 분석기는 Windows 98 환경에서 Visual C++ 6.0을 사용하였으며, 인터페이스 하드웨어와 사용자 인터페이스를 해주는 가상 장치 드라이버 (VxD : Virtual Device Driver)는 NDIS Frame Work 4.2를 사용하여 구현하였다.

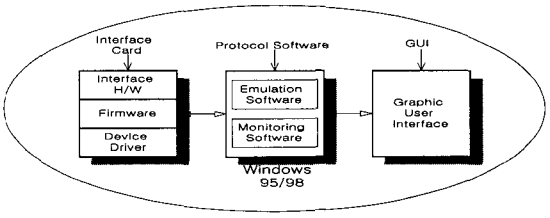

그림 1. TCP/IP 프로토콜 분석기의 구성
Fig. 1. Configuration of TCP/IP protocol analyzer.

2. 인터페이스 설계

LAN 기반의 TCP/IP 프로토콜 분석기는 그림 2와 같이 인터페이스 하드웨어(interface hardware), 펌웨어(firmware), 디바이스 드라이브(device driver)로 구성된다. 인터페이스 하드웨어는 네트워크의 데이터를 수집하여 프로토콜 소프트웨어에서 처리할 수 있도록 하는 부분이며, 시스템 제어부, ISDN 접속부, PC 접속부로 구성된다. 시스템 제어부는 80C32 마이크로컨트롤러, 시스템 메모리 그리고 컨트롤 회로 부분으로 구성되며 80C32는 PC의 명령어 및 데이터 처리, 수집한 데이터를 PC로 넘겨주는 기능 및 보드 내의 입·출력을 제어한다. 80C32의 포트 데이터/어드레스 버스(포트-0)와 포트-1은 I/O(Input/Output) 출력 포트용으로 사용하고, 포트-3을 주변의 I/O로부터의 상태를 입력받는 범용 포트로 사용하였다. ISDN 접속부는 PSB2186(ISAC-S : ISDN Subscriber Access Controller for Terminals) IC를 사용하여 라인을 통과하는 데이터를 수집할 수 있도록 PSB2186 IC를 사용하였다. PC 접속부는 ISA 버스를 이용하여 PC상의 메인 프로그램과 정보 및 데이터를 송·수신 하는 기능을 하는 부분으로서 I/O 어드레스 선택부, 명령/응답 송·수신부, DPRAM(Dual Port RAM) 어드레스 선택부, DPRAM, 인터럽트 선택부로 구성된다. DPRAM은 2-KByte 용량의 IDT71321을 사용하여 설계하였다. 인터페이스의 명령 및 응답의

송수신 방법은 그림 2와 같이 보드 측에서 라인 모니터링 한 데이터를 DPRAM의 000H 번지로부터 저장한 후 유효한 메모리 길이 값을 특정번지(7F0H, 7F1H)에 저장한 후 7EFH에 플래그 데이터 값(55H)을 라이트(write)하여 PC측에 인터럽트를 발생시킨다. PC측은 Interrupt 루틴에서 7F0H, 7F1H 번지의 값을 읽어 그 수만큼의 DPRAM의 데이터를 메모리로 덤프(Dump)하고 이벤트 카운트(event_count) 값을 1 증가시킨 후 7EFH 번지의 데이터를 읽어 자기 측의 인터럽트를 해제시킨다.

펌웨어(firmware)는 인터페이스 하드웨어에서 하드웨어를 초기화하고 라인으로부터 수집된 데이터를 프로토콜 처리할 수 있도록 전달하고 시스템 초기화, PC 인터페이스, 인터럽트 처리, 명령어 처리, DPRAM의 데이터 처리 기능을 제어한다. 또한 펌웨어 블록은 NDIS를 제어하는 부로 NDIShook.Vxd 가 주역할을 하는 프로토콜 분석기의 엔진부이다. 이 NDIShook.Vxd는 가상 장치 드라이버(Virtual Device Driver)로 네트워크 카드와 커널이 제공하는 적절한 NDIS API를 호출하므로서 그 디바이스 드라이버를 여는 어플리케이션에서 네트워크 상의 모든 패킷(packet)을 받아들일 수 있다. 이 가상 장치 드라이버는 현재 NDIS 3.0을 지원 가능하다.

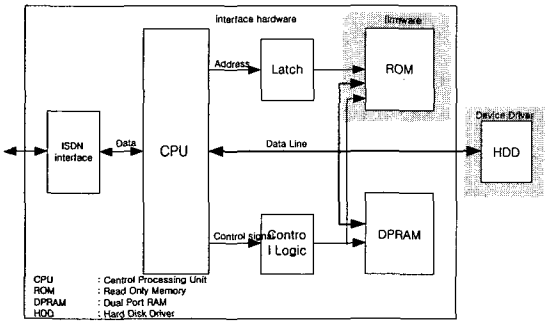

그림 2. 인터페이스 하드웨어의 구조
Fig. 2. Architecture of interface hardware.

디바이스 드라이브는 펌웨어와 OS를 인터페이스 하는 기능으로 OS(Operating System)가 시스템에 사용된 디바이스를 인식하여 데이터 및 명령어를 처리 할 수 있도록 하는 것이다. 또한 디바이스 드라이브는 수집된 데이터 처리를 위한 메세지의 전달, 시스템에서 발생된 인터럽트를 처리한다.

2. TCP/IP 프로토콜 분석 소프트웨어 설계

프로토콜 분석 소프트웨어는 인터페이스를 통해서 입력되는 네트워크 상의 데이터를 분석하기 위한 기능을 제공한다. 프로토콜 분석 소프트웨어는 그림 3과 같이 모니터링과 에뮬레이션 기능을 할 수 있도록 되었으며, 모니터링 기법은 이더넷 상에 패킷 자체를 브로드캐스팅 할 경우 각각의 호스트는 자신에게 오는 패킷만을 직접 처리하고 나머지는 폐기 처분한다. 그러나 설계한 프로토콜 분석기에서는 윈도우 환경에서 NDIS 인터페이스를 통하여 폐기 처분되는 패킷까지 모두 읽어 올 수 있도록 하였다. 프로토콜 분석기에 의해서 모니터링을 하기 위한 첫 단계인 설치된 디바이스를 찾아 패킷을 잡기 위한 특정 상태로 오픈한다. 이때 특정 상태로 열려진 디바이스 드라이버는 모든 패킷을 읽어들여 애플리케이션으로 로딩(loading)하고 열려진 디바이스 드라이버는 프로그램 종료 시 닫아 주어야 한다.

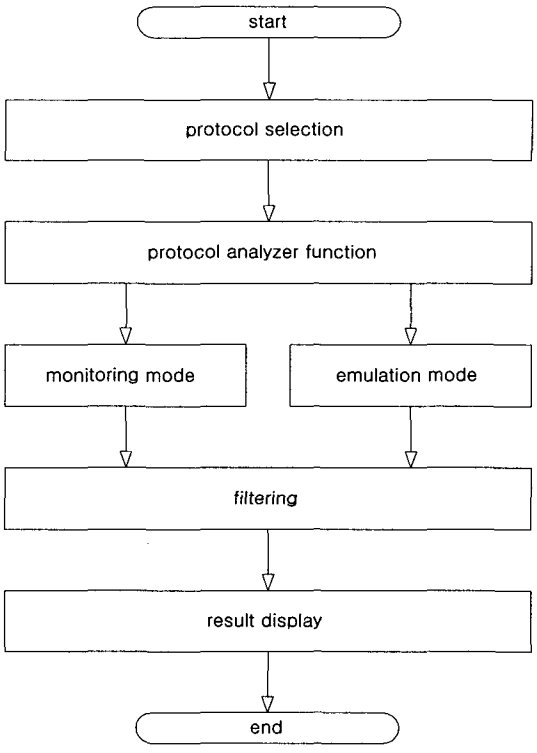

그림 3. 프로토콜 분석 소프트웨어 구조
Fig. 3. Architecture of software for protocol analysis.

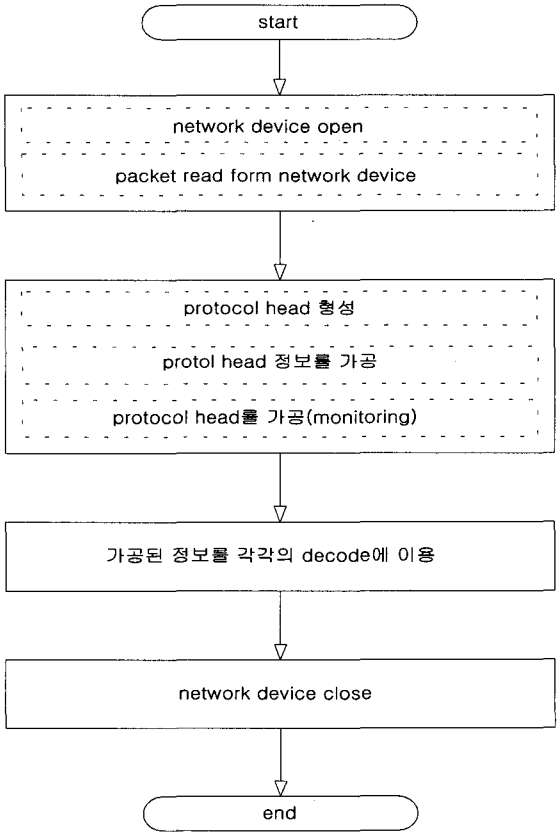

그림 4. TCP/IP 프로토콜을 분석하기 위한 과정
Fig. 4. Sequence for TCP/IP protocol analysis.

그림 5와 그림 6은 데이터 링크 계층의 소스 어드레스를 얻고 프로토콜 모니터링 블록에서 가공된 헤더 정보를 처리하기 위한 부분의 코드이다.

```
CString CTcpIp::GetSouceAddress_Eth()
{
    CString PType;
    return PType.Format("%02x-%02x-%02x-%02x-%02x-%02x",
            unMAC.Detail.S_ADD[0], unMAC.Detail.S_ADD[1],
            unMAC.Detail.S_ADD[2], unMAC.Detail.S_ADD[3],
            unMAC.Detail.S_ADD[4], unMAC.Detail.S_ADD[5]);
}
```

그림 5. 소스 어드레스를 얻기 위한 코드
Fig. 5. Code for getting source address.

프로토콜 에뮬레이션 방법은 프로토콜 정보를 상대 시스템과 송·수신하는 과정이 필요하며, 상대 시스템으로 송신하여야 할 경우는 프로토콜 정보형성과 전달

```
void CDtDecView::DLC_Display()
{
        TV_INSERTSTRUCT tvstruct;
        HTREEITEM       rghItem,subhItem;
        ...
        tvstruct.hParent=0;
        tvstruct.item.iImage=TCPIP_IMG;
        tvstruct.item.pszText = MAC->GetSouceAddress_Tcp();
        rghItem=GetTreeCtrl().InsertItem(&tvstruct);
        hTrTitle_Eth = rghItem;
        ...
}
```

그림 6. 소스 어드레스를 출력하기 위한 코드
Fig. 6. Code for output of source address.

이 필요하다. 이러한 정보 형성은 운영자가 요구한 프로토콜 종류와 그 내용(기본적으로 처리되어야 할 파라메터와 운영자 요구에 따른 프로토콜별 파라메터 등)을 사용자 블록을 통해 프로토콜 블록으로 정의된 시그널 형태에 맞게 전달한다. 프로토콜 블록은 수신된 시그널 구성요소를 분석하여 펌웨어 블록으로 정보를 송신하기 위한 메모리에 완전한 프로토콜 형태로 저장된다. 이후 프로토콜 블록은 펌웨어 블록에게 메모리에 저장된 프로토콜 내용을 가져가라는 송신 프리미티브를 호출하며, 호출된 프로토콜의 내용이 PC 화면에 출력됨과 동시에 상대 시스템으로 그 정보를 송신한다.

프로토콜 에뮬레이션 블록은 LAN 상으로 프레임을 송신할 수 있는 완전한 형태의 프로토콜 형태를 갖추는 단계이다. 그림 7은 TCP/IP 계열 패킷을 형성하는 단계의 흐름도 이다. 우선 사용자가 여러 종류의 패킷 형성 중 TCP/IP 계열 패킷 형성을 선택하면 선택된 MAC이 이더넷인지, 802.3인지 확인하고 선택된 MAC이 이더넷이면 이더넷 프로토콜 헤더를 입력 여부를 사용자가 선택하게 되고 이 단계에서 입력하지 않으면 디폴트값으로 설정된다. 모든 프로토콜의 입력이 끝나면 송신하기 위한 메모리에 데이터를 일관된 값으로 저장한다. 그 후 송신 프리미티브를 펌웨어 블록으로 전달한다.

2. GUI 설계

GUI는 네트워크에서 캡처된 데이터를 처리하고 프로토콜을 분석하기 위한 환경을 설정하기 위해 사용자 인터페이스 기능을 제공하는 기능이다. 프로토콜 분석기에서 GUI(Graphic user interface)는 사용자가 프로토

콜 분석기의 환경을 설정하고 네트워크에서 수집된 데이터의 분석된 결과를 출력하는 기능이다. 네트워크에서 수집된 데이터는 인터페이스의 펌웨어로 전달되고 프로토콜 분석 소프트웨어에서 처리된 후 결과를 출력하게 된다. 개발된 GUI는 수집된 데이터를 사용자가 데이터를 분석하고 수집할 데이터에 대한 항목과 수집 방법 등의 항목을 설정하는 기능이다. GUI는 그림 8과 같이 구성되며, 각 계층의 헤드 입력에서 이더넷, IP 어드레스 및 IP 헤드를 설정하고 MAC 어드레스와 IP 어드레스 및 목적지 어드레스(target address)를 설정한다.

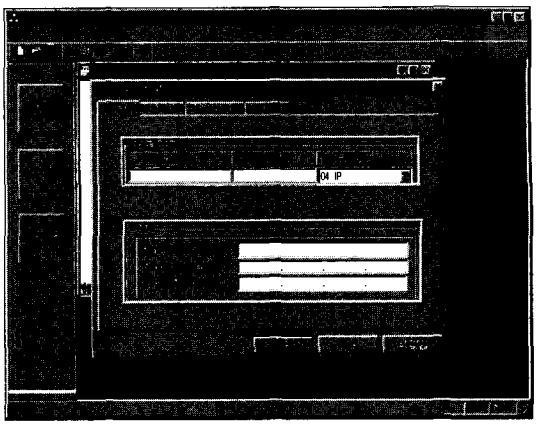

그림 8. 프로토콜 분석과 환경 설정을 위한 GUI
Fig. 8. GUI for protocol analysis and environment setting.

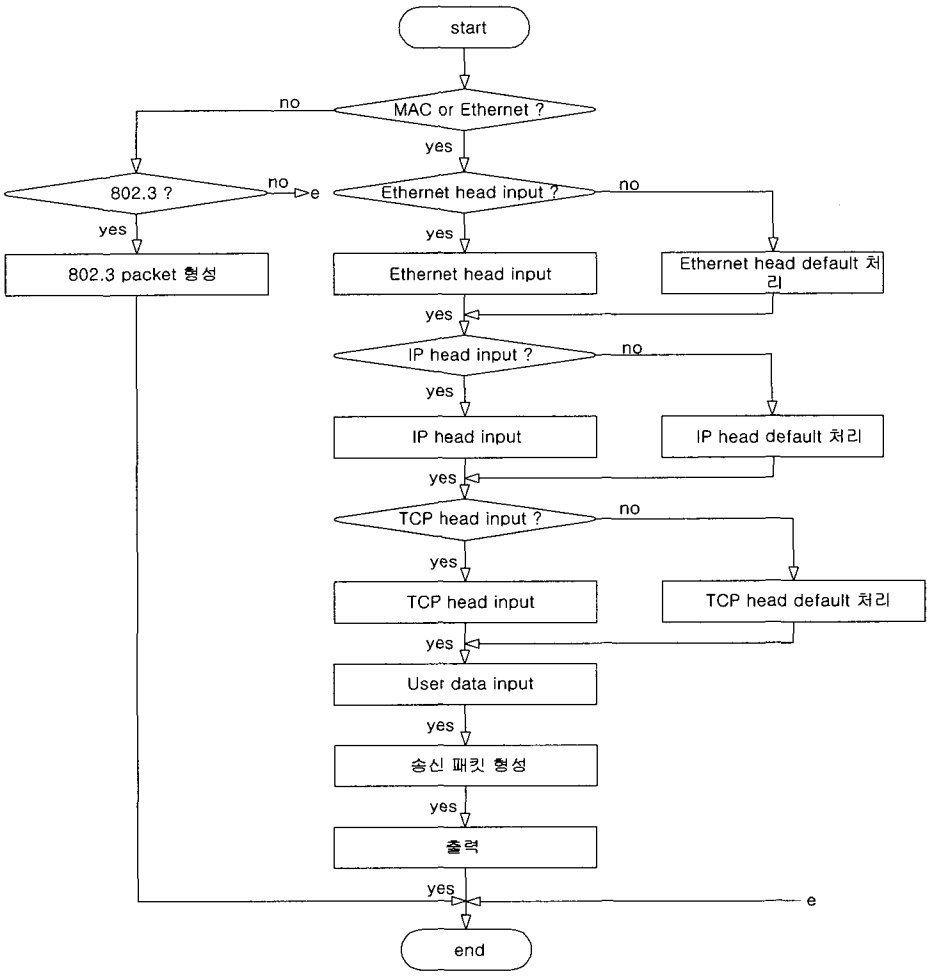

그림 7. TCP/IP의 패킷 형성 과정
Fig. 7. Packet encapsulation sequence of TCP/IP.

Ⅲ. 성능시험 및 결과

1. 시험환경

본 논문에서 개발한 LAN 기반의 TCP/IP 프로토콜 분석기의 성능평가는 PC(CPU : PentiumⅡ333MHz, RAM : 64Mbyte에 OS : Windows 98) 환경에서 100Mbps의 FDDI 백본망에서 10Mbps급 이더넷을 서브넷으로 사용하고, 외부 망과의 접속은 T1급으로 구축하였다. 10Mbps급 이더넷 LAN환경에 클라이언트와 본 논문에서 개발된 프로토콜 분석기를 접속하여 시험하였다. 프로토콜 분석기는 시험 환경에서 전 부하 트래픽 발생을 위해 임의의 프레임과 네트워크의 TCP/IP 패킷 사용하였다.

2 시험결과

본 논문에서 개발된 TCP/IP 프로토콜 분석기에 대한 성능 평가 결과 모니터링을 수행한 한 결과 그림 9와 같이 초당 480개의 패킷을 정상적으로 분석함을 보였다. 캡쳐된 패킷중 400개는 전부하 트래픽을 위해 특정 프로토콜 발생기에서 발생된 패킷과 80개는 실제 일반 사용자들에 의해 발생된 패킷을 수신한 것이다. 이러한 결과는 현재 10 Mbps 서브넷의 클라이언트에 5.36Mbps의 데이터를 정상적으로 처리됨을 보였다.

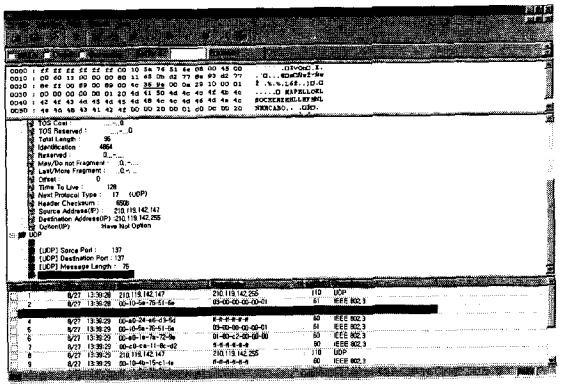

그림 9. TCP/IP 프로토콜 분석 결과
Fig. 9. Analysis results of TCP/IP protocol.

Ⅳ. 결 론

본 논문에서는 윈도우 환경에서 통신 장비 및 시스템의 개발에 사용할 목적으로 LAN 기반의 TCP/IP 프로토콜 분석기를 개발하였다. 프로토콜 분석기는 모니터링과 시뮬레이션 기능을 제공하고 있으며 PC 확장보드에서 구현되었고 소프트웨어만 운용자의 요구에 따라 각각 로딩 하도록 설계하였다. 소프트웨어는 PC기반 하에서 Windows 98 운영체제를 사용함으로써 별도의 부가 장비 없이 손쉽게 프로토콜을 분석할 수 있는 환경을 구축하였으며, 추후 다른 프로토콜의 탑재가 가능하도록 개방된 구조로 설계하였다. 개발된 프로토콜 분석기의 성능시험 결과 LAN 기반에서 TCP/IP 프로토콜이 정상적으로 분석할 수 있음을 보였고 10Mbps 이더넷 LAN 환경에서 모니터링 방법으로 기능을 충분히 수행됨을 보였다. 향후 연구과제는 개발 시스템의 성능 향상을 통해 100Mbps 고속 이더넷, 기가비트 이더넷 등 초고속 통신망에서도 안정적으로 유지해야 하며, LAN 상에서 수집된 패킷 데이터를 효율적으로 저장 및 처리하기 위한 방법과 데드라인 스케줄링 기법을 도용한 메모리의 효율적 관리체계, 완벽한 User Interface의 지원 및 패킷 필터 엔진이 구축되어야 할 것이다.

참 고 문 헌

[1] "PT502 Protocol Analyzer User manual", 1994.

[2] 장학신, 강정진, 이시현, "객체지향형 ISDN 프로토콜 분석기 기본기능 개발", 특정연구개발과제 과학기술부(KISTEP) 1차년도 보고서, 1999. 9

[3] 강정진, 이시현, 장학신, 조병순, 정중수, "윈도우 환경에서 ISDN Q.921/Q.931 프로토콜 분석기 구현", 한국통신학회논문지, Vol. 25, No. 6T, pp.34-39, 2000. 6

[4] James Martin, Joe Leben, TCP/IP Networking, 이한 출판사, 1998

[5] Data Book, Embedded microcontroller, Intel Corp., 1998

[6] MYKE PREDKO, The 8051 microcontroller, McGraw-Hill, 1998.

[7] 이상엽, Visual C++ 6.0 Bible, 영진출판사, 1999

[8] 곽준기 외1, Visual C++ 6.0, 삼각형 프레스, 1999

저 자 소 개

李 是 縣(正會員)

1999년 2월 건국대학교 대학원 전자공학과 졸업(공학박사). 1991년 1월~1996년 1월 : 현대전자(주) 정보통신연구소 근무. 1998년 3월~2000년 현재 : 동서울대학 전자통신과 교수

姜 廷 震(正會員) 電子工學會 第37卷 TE編 第2號 參照
현재 동서울대학 전자통신과 교수

張 學 信(正會員)

1991년 2월 : 건국대학교 대학원 전자공학과 졸업(공학박사) 1978년 9월~2000년 현재 : 동서울대학 전자통신과 교수

曺 秉 珣(正會員)

1986년 2월 : 서울산업대학교 전자공학과 졸업. 2000년 2월 : 성남시 신지식인상 수상. 1991년 6월~2000년 현재 : 시앤시 인스트루먼트(주) 대표이사

崔 圭 珉(正會員)

1997년 3월~2000년 2월 국립 안동대학교 전자정보통신학과 3년수료후 휴학. 1999년 11월~2000년 현재 시앤시 인스트루먼트(주) 사원.

鄭 重 壽(正會員)

1993년 8월 : 연세대학교 전자공학과 졸업(공학박사). 1983년 3월~1994년 2월 : ETRI근무, 선임연구원. 1994년 3월~2000년 현재 : 국립 안동대학교 전자정보산업학부 교수