PC 환경에서 시뮬레이션 기능을 포함한 LAN 프로토콜 분석장비

(A LAN Protocol Analyzer including Simulation Function for PC Environment)

정 중 수 † 이 준 원 ††
(Joong-Soo Chung) (Jun-Won Lee)

요 약 오늘날 인터넷은 가장 주목받고 있는 정보통신 혁명을 주도하였다. 회사, 연구소, 대학교 등 다양한 직장에서는 서브넷에 이더넷망을 구축하고, 백본망에는 FDDI, ATM 등의 다양한 고속망을 구축하여 인터넷 서비스를 제공받고 있는 상황이다. 인터넷에서 핵심적으로 활용되는 TCP/IP 프로토콜 슈트의 처리 과정과 그 속성의 면밀한 분석은 통신망의 문제점 파악이나 통신장비의 개발에 필수적이다.

본 논문에서는 이더넷 LAN 상에서 동작되는 TCP/IP를 기반으로 하는 인터넷 프로토콜과 Netware, NetBIOS 등과 같은 비-인터넷 프로토콜을 모니터링 및 시뮬레이션하는 프로토콜 분석장비 개발을 기술하였다. 개발 환경으로는 윈도우 98 OS와 MS 비주얼 C를 사용하였다. 비주얼 C로 작성된 응용 프로그램은 NDIS 소프트웨어와 인터페이스를 수행하여 개발되었다. 또한 개발된 시스템을 실제 대학교 10Mbps 이더넷 LAN에 적용하여 인터넷 프로토콜과 비-인터넷 프로토콜 정보를 모니터링 및 시뮬레이션 하였다. 모니터링 한 결과 한 개의 패킷 처리시간은 1.5ms였다. 시뮬레이션은 TCP 접속과 해제 관점에서 살펴보았으며, 이때 TCP 접속과 해제를 한번 수행시 약 8.6ms가 소요되었다. 이 결과는 10Mbps 이더넷 LAN 환경에서 TCP/IP 프로토콜 슈트의 모니터링에는 충분한 성능을 만족하며, 아울러 네트워크 장비 개발 시 충분한 성능 검증용으로 활용될 수 있다.

키워드 : 프로토콜 분석

Abstract The Internet is absolutely contributed to information telecommunication revolution nowadays. Realizing local network at the various type of buildings such as a company and a university, ethernet is used for subnet and FDDI, ATM are used for backbone mainly in order to get internet services. Processing TCP/IP protocol suite and analyzing the protocol exactly is essential to detecting the problem occurring in the network and developing communication equipment.

This paper presents implementation of ethernet LAN protocol analyzer which monitors and simulates TCP/IP protocol suite carrying the Internet and non-Internet protocol such as Netware and NetBIOS. MS window98 and visual C are used for development environment and application program operates on the NDIS firmware. The performance analysis on the proposed system is carried out as monitoring and simulating the traffic over LAN of a university. In the result of monitoring the system, the processing time of a packet captured over the LAN is about 1.5ms. In case of simulating the system, the processing time to be taken carrying out TCP connection and disconnection once is packet is about 8.6ms. The performance analysis of monitoring and simulation results satisfies with 10 Mbps ethernet LAN environment.

Key words : Protocol Analysis

· 본 연구는 한국과학재단 해외 POST-DOC 지원 사업으로 수행되었습니다.

† 정 회 원 : 안동대학교 전자정보산업학부 교수
jschung@andong.ac.kr
†† 비 회 원 : 안동대학교 전자정보산업학부 교수
leejw@andong.ac.kr

논문접수 : 2001년 9월 28일
심사완료 : 2002년 7월 8일

1. 서 론

스위칭 망은 전화교환망(PSTN: Public Switched Telephone Network), 패킷교환망(PSPDN: Public Switched Packet Data Network), ATM(Asynchrobous Transfer Mode) 등으로 진화되고 있으며, 브로드 캐스트

망은 LAN을 중심으로 진화되었다. 특히 LAN의 구성형태는 초기에 이더넷을 근간으로 하였으며, 그 이후 네트워크가 확장되고 보다 고속의 트래픽을 처리하게 되면서 백본과 서브넷으로 분리되었다. 즉, 서브넷은 이더넷을, 백본은 FDDI, ATM을 채용하고 있다. 한편 종단 사용자 관점에서 살펴보면 이더넷 LAN 카드를 장착한 사용자 수는 LAN뿐만 아니라 공중망의 ADSL(Asynchronous Digital Subscriber Loop)까지 확대되어 가는 추세이다. 이들의 공통적인 서비스로는 인터넷 사용이 우선이나 LAN을 사용하는 회사나 연구소, 학교에의 트래픽 특성을 면밀히 분석해보면 아직 TCP/IP를 기반으로 하는 인터넷 프로토콜뿐 아니라 비-인터넷 프로토콜 정보도 많이 사용된다.

일반적으로 데이타 통신망의 구축이나 장비 개발 시 프로토콜 분석기의 필요성은 불가피하다. 프로토콜 분석기는 ISDN, ATM 등의 WAN(Wide Area Network)과 LAN 프로토콜 분석기로 분류되며, WAN 프로토콜 분석기는 모니터링과 시뮬레이션 기능을 내장하며[1,2,3,4], LAN 프로토콜 분석기는 주로 모니터링 기능만 수행하였다[5,6]. 이더넷 LAN 위에서 동작되는 TCP/IP 인터넷 프로토콜 슈트로는 네트워크 계층의 IP(Internet Protocol), 트랜스 포트 계층의 TCP(Transmission Control Protocol), 응용 프로토콜로는 HTTP(Hyper Text Transport Protocol) 등 많이 있으며, 비-인터넷 프로토콜로는 Netware, NetBIOS 등이 대표적이다. 라우터등과 같은 네트워크 관련 시스템의 개발, 네트워크 장애 검출, 및 LAN 위에서 전달되는 트래픽 분석에는 LAN 프로토콜 분석장비가 필수적이다. 현재 이러한 프로토콜 분석기는 활용성이 많음에도 불구하고 국내 개발 제품과 수입하는 장비들은 오직 단순한 모니터링 기능만을 내장하고 있다[5,6]. 특히 수입하는 장비로서는 산업용 PC 본체에 윈도우 98 위에 소프트웨어를 탑재하는 경우[5]와 윈도우 98의 일반 PC위에 소프트웨어를 탑재하는 경우[6]가 있으며, 일반적으로 성능은 대체로 우수하나 가격이 고가인 단점이 있다.

본 논문에서는 인터넷 유해 사이트의 사용자 접속 방지 시스템 개발[7]에 착안하여 TCP/IP 인터넷 프로토콜 슈트와 비-인터넷 프로토콜로는 Netware, NetBIOS 등 이더넷 LAN 위에서 동작하는 데이타의 흐름을 파악할 수 있는 프로토콜 모니터링과 시뮬레이션하는 프로토콜 분석기 개발에 대한 전반적인 설계 기법의 제시와 개발 과정 및 성능 분석을 수행하였다. LAN 프로토콜 분석기의 기능은 크게 모니터링과 시뮬레이션으로 분류되며, 이의 개발 환경으로는 펜티움 II 프로세서 800 MHz PC 기반의 윈도우 98 OS와 NDIS(Network Driver Interface Specification) Frame Work Version 4.2(편의상 NDIS라 함) 환경하에서 수행되는 MS 비주얼 C를 사용하였다.

본 논문의 구성은 제II절과 제III절에서는 LAN 프로토콜 분석 환경 및 설계 개념을 소개하였고, 이후 IV 절에서는 설계된 LAN 프로토콜 분석기의 시험환경, 성능분석 및 특징을 제시한 후 제V절에서 결론을 내렸다.

2. LAN 프로토콜 분석기 환경

2.1 프로토콜 분석기 기능

그림 1에서와 같이 LAN 프로토콜 분석기 구성은 PC 에이더넷 LAN 카드를 탑재하여 이더넷에 10BT 케이블로 접속되며, LAN 카드와 PC 본체와는 내부 시스템 버스로 접속된다. PC 본체에는 LAN 카드로부터 수신되는 정보의 처리와 LAN 카드로 송신하는 정보의 처리를 위해 NDIS 펌웨어를 로딩하였다. 펌웨어 위에 동작하는 응용 소프트웨어로는 인터넷 프로토콜 슈트와 비-인터넷 프로토콜을 모니터링과 시뮬레이션하는 부분이 있으며, 이들은 프로토콜 계층별로 처리하기 위해 블록으로 분류하여 모듈화하여 개발하였다.

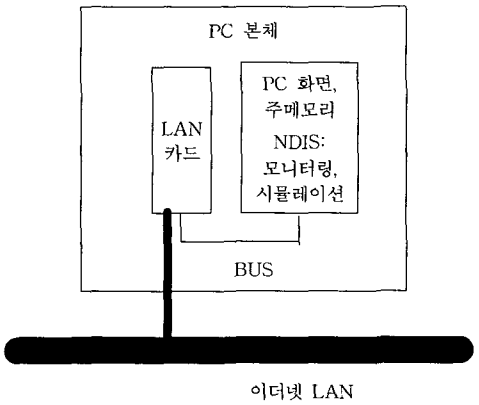

그림 1 LAN 프로토콜 분석기 구성

2.2 NDIS 인터페이스 처리부

프로토콜 분석기는 LAN 카드를 직접 제어하여 LAN 상의 패킷을 캡처링하여 분석하는 모니터링과 LAN 상으로 자신이 원하는 패킷을 형성하여 프로토콜 흐름에 맞춰 직접 송신하는 기능을 가져야 한다. 응용 프로그램과 LAN 카드의 정보 송, 수신은 NDIS 소스 중 디바이스를 열고 통신하는 과정이 필요한데, 그 절차는 다음과 같다.

1) 시스템은 우선 설치된 네트웍 디바이스를 찾아 디바이스를 연다.

```
extern "C" UNIT Capture(LPVOID lParam) {
    .....
// Find LAN card device name
    hDevice=W32N_OpenAdaptor(g_AdapterName);
// 이하 Vxd 파일 핸들을 hDevice에 넘겨줌
    .....
}
```

2) 열려진 디바이스에서 읽어들일 패킷의 종류를 결정하는 소스는 다음과 같다.

```
.....
//디바이스로부터 모든 패킷 읽음
 W32N_PacketRead(hDevice, &pPackage->
UserPacketData, &pPackage->nBytesReturned, &pPackage
->OverLapped, FALSE);
.....
//Application 영역으로 패킷 이동후 버퍼링
char* WINAP(OnPacketReceivedAPC
  (PW32N_PACKET pRAWUserPacketData){
....
CMainFrame* pfrm
 =(CMainFrame*)AfxGetApp()->m_pMainWnd;
  // Packet의 길이를 length에 저장.
pfrm->length =
 pRAWUserPacketData->nPacketDataLength;
  // Packet의 내용을 pBuffer에 저장.
pfrm->pBuffer = pRAWUserPacketData->PacketBuffer;
  // 들어오는 패킷을 들어오는 순서대로 버퍼에 저장.
for(j=0;j<pfrm->length;j++)
      pfrm->pStore[pfrm->counter][j] = pfrm->pBuffer[j];
pfrm->pLength[pfrm->counter]=pfrm->length;
pfrm->counter++;
   // 패킷이 들어오는 순서대로 화면에 디스플레이 하는
함수 호출.
::SendMessage(pfrm->GetDetailHwnd(),WM_STORE,0,0);
.....
}
```

3) PC에게 TCP/IP 패킷을 형성한 후 다음과 같은 함수를 이용하여 목적지 호스트로 전송한다. 따라서 재구성되어 전송된 패킷은 목적지 호스트인 PC로 전송이 되어 시뮬레이션 기능을 수행한다.

```
void SendPacket(){
 ....
pSendData = PacketBuffering->SendData();
  //for example protocol type: IP
memset (&pSendData[12], 0x08, 1);
memset (&pSendData[13], 0x00, 1);
memset (&pSendData[MDstAddr], 0xff,
ETHER_LEN);
memcpy(&pSendData[MSrcAddr], g_CurrentAddress,
ETHER_LEN);
....
nSendResult =
W32N_PacketSend(hDevice,pSendData, 64,
&nBytesReturned, &OverLapped, TRUE);
}
```

3. LAN 프로토콜 분석기 설계

LAN 프로토콜 분석기는 PC의 명령 수신 및 응답 송신, 수집된 데이타를 PC로 넘겨주는 기능 및 보드내의 입, 출력 기능을 제어한다. PC가 LAN 카드와 명령 및 응답을 주고받기 위한 프로토콜 시뮬레이션이나 모니터링 결과를 전달하여 그 기능을 디스플레이 하도록 한다.

3.1 프로토콜 모니터링 설계개념

프로토콜 분석기의 설계는 제 2장에서 제시된 기법을 토대로 하였다. 이더넷 LAN에 동작되는 프로토콜 모니터링은 이더넷 프로토콜위에 TCP/IP 프로토콜 슈트의 앤캡슐레이션 되는 경우와 IEEE 802.3위에 LLC (Logical Link Control) 프로토콜 필드속에 비-인터넷 프로토콜 정보가 앤캡슐레이션 되는 경우가 있다.

소프트웨어 설계는 구조와 기능의 편의상 블록으로 분류하여 처리하였는데, 모니터링 설계를 위한 프로토콜 블록과 설계된 소프트웨어를 사용자의 운용에 따라서 화면에 결과 값을 표현(display)하는 User/Interface 기능(여기서 편의상 소프트웨어 용어로 MMC 블록이라 함)으로 구분한다. 또한 이들을 LAN 카드에 내장된 프로세서와 이들 제어를 담당하는 펌웨어 블록이 정의된다. MMC 블록과 프로토콜 블록은 프로토콜 내용에 의존하여 펌웨어 블록으로부터 프로토콜 내용에 무관하게 정보 수신용 프리미티브만 정의하여 정보의 시작주소와 정보의 내용을 포함하는 정보영역을 서로 교환한다.

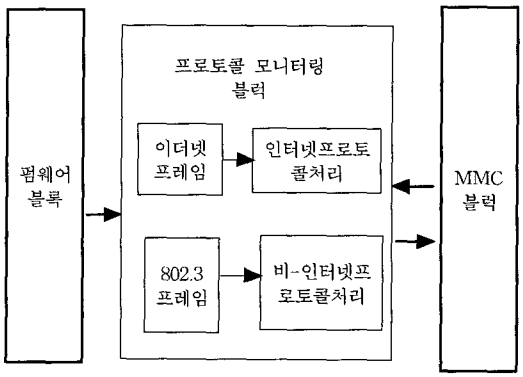

그림 2 프로토콜 모니터링 과정

프로토콜 모니터링은 운용자가 요구한 프로토콜 종류와 처리되어야 할 프로토콜 파라메터 등의 내용을 분석하여 펌웨어로부터 수신된 프로토콜 정보를 사용자의 PC 화면 출력 형태에 적합하게 디스플레이 한다. 프로토콜 모니터링 관련 소프트웨어블록의 동작은 다음과 같다.

-MMC 블럭: 프로토콜 관련블록별로 존재하고 화면으로부터 입력되는 정보를 처리하여 해당블록으로 프로토콜 처리를 하도록 하고, 프로토콜블록으로부터 결과를 수신하여 화면에 출력시킨다. 특히 윈도우환경으로부터 입력되는 정보처리가 가능하도록 하고 실행파일은 프로토콜 모니터링에 관련한 각종 메뉴를 정의하는 아이콘으로 구동되도록 하며, 디스크에 있는 해당 소프트웨어 블록을 메인 메모리에 상주시키도록 구성하였다.

- 프로토콜 모니터링 블럭: 이더넷 LAN 상에서 인터넷 프로토콜과 비-인터넷 프로토콜 모니터링 소프트웨어 중 프로토콜의 처리기능이다. 펌웨어로부터 수신된 프레임을 프레임 종류에 따라 분류하며, 이더넷 프레임은 인터넷 프로토콜을 처리하여 MMC 블록에 전달하며, LLC 프레임은 비-인터넷 프로토콜을 처리하여 MMC 블록에 전달하여 디스플레이를 요구한다.

- 펌웨어 블럭: PC기반 LAN카드를 동작시키는 부분으로 NDIS부로 구성된다.

3.2 프로토콜 시뮬레이션 설계개념

프로토콜 시뮬레이션 기법은 기본적으로 모니터링 기법의 개념을 포용하도록 설계하였다.

소프트웨어 설계는 구조와 기능의 편의상 모니터링과 같이 블록으로 분류하여 처리하였는데, MMC 블록과 프로토콜 블록은 모니터링과 마찬가지로 프로토콜 내용에 의존하여 정의될 시그널 형태에 맞게 정보를 교환하며, 프로토콜 블록과 펌웨어 블록은 프로토콜 내용에 무관하게 정보 송, 수신용 프리미티브 두 개만 정의하여 정보의 시작주소와 정보의 내용을 포함하는 정보영역을 서로 교환한다.

프로토콜 시뮬레이션 처리는 LAN 프로토콜 정보를 상대 시스템과 송, 수신하는 과정이 필요하다. 상대 시스템으로 송신하여야 할 경우는 프로토콜 정보형성과 전달이 필요하다. 이러한 정보 형성은 운용자가 요구한 프로토콜 종류와 그 내용(기본적으로 처리되어야 할 파라메터와 운용자 요구에 따른 프레임 선택별 파라메터 등)을 MMC블록을 통해 프로토콜 블록으로 정의된 시그널 형태에 맞게 전달한다. 프로토콜 블록은 프로토콜 관련 파라메터를 바탕으로 HEXA 값으로 권고안에 따라 MAC (Medium Access Control)계층부터 필요에 따라 관련 정보를 직접 코딩하여 작성하는 MANUAL 처리법과 프로토콜 파라메터 요소 값을 사용자로부터 하나씩 수신하여 처리하는 AUTOMAIC 기법이 있다. 프로토콜 블록은 수신된 시그널 구성요소를 면밀히 파악하여 그 내용을 참고하여 펌웨어 블록으로 정보를 송신하기 위에 메모리에 프로토콜 내용을 형성한다. 이후 프로토콜 블록은 펌웨어블록에게 메모리에 저장된 프로토콜 내용을 가져가라는 송신 프리미티브를 호출하며, 호출된 프로토콜의 내용이 PC화면에 표시됨과 동시에 상대 시스템으로 그 정보를 송신한다.

상대 시스템으로부터 정보를 수신하는 모드로 동작할 때는 그 정보를 먼저 PC화면에 출력하여야 하는데, 이 때는 펌웨어 블록으로부터 수신프리미티브로 전달받은 프로토콜 내용을 위 방법의 역순으로 프로토콜 모니터링 처리와 동일하다. 그림 3에서는 소프트웨어 블록의 형성과 그들간의 상호동작을 서술하였다.

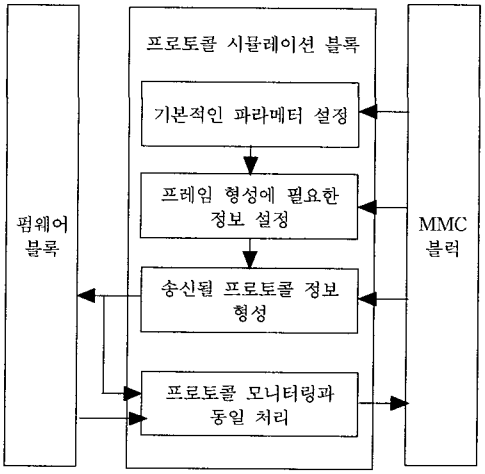

그림 3 프로토콜 시뮬레이션 과정

프로토콜 관련 소프트웨어블록은 모니터링과 비교하여 시뮬레이션 기능이 추가된다.

- 프로토콜 시뮬레이션 블럭: 이더넷 LAN에 동작되는 프로토콜 시뮬레이션은 인터넷 프로토콜과 비-인터넷 프로토콜의 처리기능이다. 사용자가 프레임을 상대 시스템으로 전달할 때는 입력된 파라메터를 바탕으로 이를 처리한 후 펌웨어로 전달하며, 상대 시스템으로부터 정보를 수신하면 모니터링과 동일한 방법으로 MMC에게 디스플레이를 요구한다.

3.3 MMC 화면 디스플레이 과정

MMC 화면 디스플레이 과정은 펌웨어 블럭으로부터 수신프리미티브로 전달받은 프로토콜 내용을 PC화면에 표시하는 모니터링 방법과 시뮬레이션 기능중 운용자에 의해 형성된 정보를 송신한 후 이의 내용을 PC화면에 표시하는 방법이 있다.

3.3.1 정보 수신 부의 처리

인터넷/비-인터넷 프로토콜 시뮬레이션 기능 수행 시

모니터링 방법과 동일하게 처리되며, 펌웨어 블록으로부터 수신프리미티브로 전달받은 프로토콜 내용을 PC화면에 표시하는 경우이며, 펌웨어로부터 "LAN 프로토콜 정보 수신" 프리미티브를 호출 후 프레임 형태의 헤더를 파악한다. 즉, 송, 수신 MAC 주소, 프레임 형태(이더넷인가, IEEE802.3 프레임인가 분리)를 판단하여 이더넷이면 인터넷프로토콜인 TCP/IP 프로토콜 슈트를 처리하는 부와 IEEE802.3이면 비-인터넷프로토콜인 NetWare, NetBIOS 등을 처리한다. 화면 출력 형태는 메시지마다 user-friendly하게 'HEXA', 'NEMONIC', '파라메터 서술부'의 조합으로 출력하여 초보자라도 프로토콜을 쉽게 이해 할 수 있도록 하였다.

3.3.2 정보 송신 부의 처리

시뮬레이션기능에 해당되며 이는 크게 시스템이 사용자의 명령에 의해 LAN 프로토콜정보를 형성하여 펌웨어로 전달한 후 그 내용을 디스플레이하는 기능과 상대 시스템에서 프로토콜 정보를 수신하면 프로토콜 상태 처리에 따라 시스템이 사용자와 무관하게 자동적으로 LAN 프로토콜을 형성하여 펌웨어로 전달한 후 그 내용을 디스플레이하는 기능이 있다.

어느 경우도 펌웨어는 상대측으로 정보 전송 후 전송된 프로토콜은 마치 상대측으로부터 수신되어 PC 화면에 표시되는 기능과 동일하게 처리한다.

4. LAN 프로토콜 분석기의 시험 및 특징

4.1 시험환경

본 시스템의 시험은 100Mbps의 FDDI 백본망에 10Mbps급 이더넷을 서브넷으로 구성되고, 인터넷망과의 접속은 DS3으로 구축되어 있는 국립 안동대학교의 LAN 환경에서 수행하였다. 따라서 10Mbps급 이더넷 LAN환경인, 현재 공과대학과 전산실이 동일한 서브넷에 접속되어 가장 심한 트래픽이 발생하여 이를 대상으로 하였다.

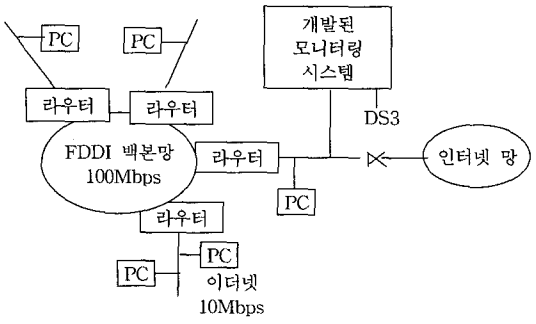

그림 4 시험환경

4.2 LAN 프로토콜 분석기의 성능해석

이더넷 LAN 상의 프로토콜 분석기 개발 후 이의 성능을 파악하는 단계이다. 본 시스템에서 하드웨어로부터 수신되는 이더넷 프로토콜 정보를 개발된 시스템에서 모니터링 하는 과정과, 시뮬레이션을 위해 한 개의 패킷을 형성하여 송신하는데 관련된 소요시간은 다음과 같다.

- 펌웨어 소요시간: 1ms
- 펌웨어와 소프트웨어간 프리미티브 호출 처리시간: 0.3ms
- 모니터링 소프트웨어 처리시간: 0.2ms
- 시뮬레이션 소프트웨어 처리시간: 0.1ms

위의 사실로 보아 한 개의 이더넷 프로토콜 정보를 확인하여 모니터링 하는데 전체 소요시간은 1.5ms이다. 따라서 개발된 시스템은 초당 약 666개의 이더넷 프레임을 모니터링할 수 있다. 또한 한 개의 이더넷 프로토콜 정보를 형성하여 송신하는데 전체 소요시간은 1.4ms이므로 초당 약 650개의 이더넷 프레임을 전송할 수 있다. 이와 같은 성능으로 다음과 같은 결론을 내릴 수 있다.

- 모니터링 관점에서 분석

그림 5는 LAN 환경에서 TCP/IP 패킷과 비-인터넷 패킷의 길이를 가변으로 하여 초당 모니터링 되는 패킷 수에 관한 처리량을 성능 파라메터로 제시하였다. 이 그림에서 초당 모니터링되는 TCP/IP 패킷과 비-인터넷 패킷 수는 패킷 길이와 거의 관계가 없음을 알 수 있다. 일반적으로 많이 적용되는 패킷의 평균길이가 128바이트인 경우에, 초당 약 976개의 패킷이 최대로 전송 될 수 있다. 그러나 이더넷 LAN 채널 사용율이 약 40%인점을 고려하면 초당 약 390개의 패킷이 최대로 전송된다. 그림 5에서 현재 개발된 프로토콜 분석기는 패킷의 평균길이가 128바이트인 경우에, 초당 약 666개의 이더넷 프레임을 모니터링 하므로 10 Mbps 이더넷 LAN 프로토콜을 충분히 모니터링할 수 있다.

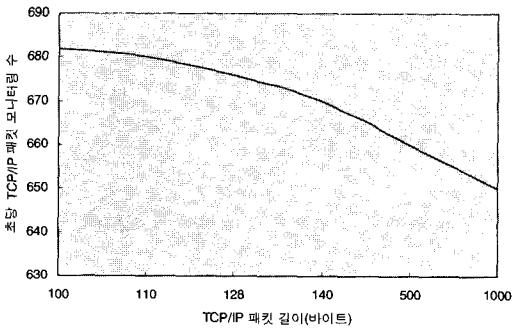

그림 5 TCP/IP 패킷 처리량

- 시뮬레이션 관점에서 분석

시뮬레이션 성능 파악은 정상적인 TCP 접속과 해제 관점에서 파악하였다. TCP 접속시 약 3개(2개 패킷 송신, 1개 패킷 수신)의 패킷과 해제시 3개(2개 패킷 송신, 1개 패킷 수신)의 패킷이 소요될 경우 한 개의 TCP 접속과 해제시에는 약 8.6ms가 소요된다. 따라서 TCP 접속과 해제를 연속할 경우 초당 약 116번 처리할 수 있는 트래픽 능력을 처리할 수 있다.

4.3 LAN 프로토콜 분석기의 특성

본 논문에서 제시된 프로토콜 분석기는 모니터링 기능과 시뮬레이션 기능을 수행하는 특징이 있으며, 그림 6은 시뮬레이션을 위하여 TCP/IP/이더넷 계열 패킷을 형성하는 개략적 단계의 흐름도이다. 우선 사용자가 여러 종류의 패킷 형성 중 TCP/IP/이더넷 계열 패킷 형성을 선택(클릭)한다. 이후 선택된 MAC이 이더넷인지, 802.3 인지 점검한다. 선택된 MAC가 이더넷이면 이더넷 프로토콜 헤더의 입력 여부를 사용자가 선택하게 한다. 이 단계에서 입력하지 않으면 디폴트값으로 설정한다. IP나 TCP 등 모든 프로토콜은 사용자의 입력 여부를 묻고 입력하지 않을 경우는 디폴트 처리를 한다. 이렇게 모든 프로토콜의 입력이 끝나면 송신하기 위한 메모리에 데이타를 일관된 값으로 저장한다. 그 후 송신 프리미티브를 펌웨어 블록으로 전달한다.

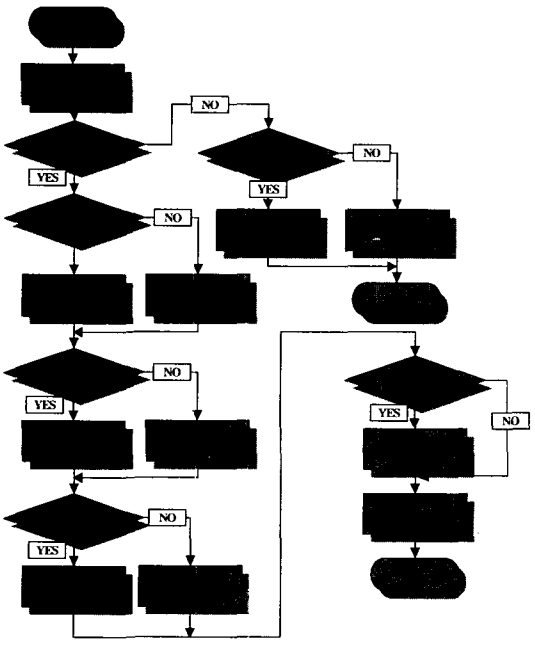

그림 6 TCP/IP/802.3 계열(이더넷) 패킷 형성 과정

그림 7은 프로토콜 데이타 유닛 송, 수신시 그 정보를 PC 화면에 출력하는 형식을 나타내었다. 이와 같이 본 장비의 PC 화면 출력은 프로토콜 관련 파라메터의 헥사 값의 조합과 그 값의 의미 및 IP의 송, 수신 주소를 연관시켜 사용자가 쉽게 파악하도록 하였다.

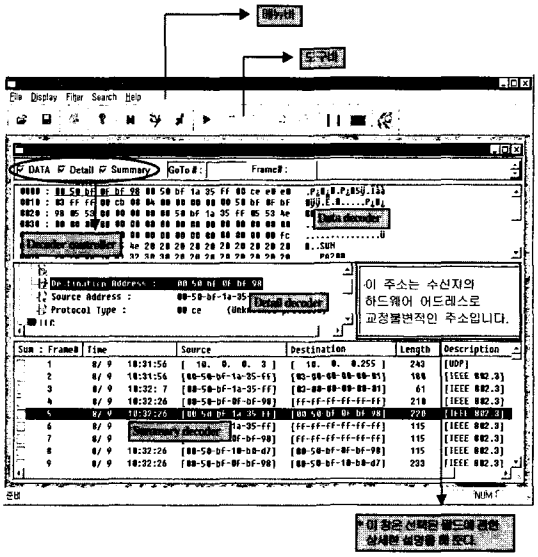

그림 7 송, 수신된 프로토콜 데이타 유닛

5. 결 론

본 논문에서는 이더넷 LAN 프로토콜중 인터넷 및 비-인터넷 근간의 프로토콜 분석기 개발을 PC기반 하에서 수행하였으며, 이의 동작과 기능을 제반환경과 더불어 살펴보았다.

프로토콜 분석기의 기능은 모니터링과 시뮬레이션 기능이 있으며, 이러한 기능 수행 시 동일한 LAN 카드위에서 NDIS 펌웨어로 구현하였으며, 소프트웨어만 운용자의 요구에 따라 각각 로딩하도록 하였다. 소프트웨어는 비주얼 C언어로 PC기반 하에서 윈도우를 운영체제로 사용함으로써 별도의 부가 장비 없이 손쉽게 프로토콜을 분석할 수 있는 환경을 구축하였으며, 추후 또 다른 프로토콜의 탑재가 가능하도록 개방된 구조로 설계하였다. 또한 TCP/IP 인터넷 및 NetWare, NetBIOS 등의 비-인터넷 프로토콜 모니터링에에 대한 성능도 분석하였는데 현재 개발된 시스템의 한 개의 패킷 처리시간은 1.5ms로서 10Mbps 이더넷 환경에서 모니터링을 완벽하게 수행함을 입증하였다. 또한 TCP/IP 패킷을 가정한 시뮬레이션 관점에서 보면 TCP 접속과 해제는 초당

약 116번 처리할 수 있으므로 이는 네트워크 장비 개발 시 충분한 성능 검증용으로 활용될 수 있다

향후 현재의 시스템 개발 기법으로는 100Mbps 이더넷 프로토콜 모니터링의 성능 만족이 문제가 되며, 이는 이미 공개된 NDIS 펌웨어의 개선이나 비주얼 C 프로그램의 설계기법의 변화와 그에 따른 모니터링 방식의 개선이 요구된다.

참 고 문 헌

[1] 정중수, "PC 환경에서 ISDN 사용자/망 프로토콜 분석기 개발", 한국통신학회 논문지 99-24-6B-9, 1999년6월호.

[2] "PT502 Protocol Analyzer User manual," Agilent, 1995, http://www.agilent.com

[3] "Agilent Advisor WAN J2300E," Agilent, 1998, http://www.agilent.com

[4] "Chameleon32+ Protocol Analyzer User manual," Tekelec, 1998, http://www.tekelec.com

[5] "Agilent Advisor LAN J3446E," 1999, http://www.agilent.com

[6] "Network Associate Sniffer Pro," 2001, http://www.sniffer.com

[7] 박형배, 정중수, "LAN 모니터링을 통한 인터넷 유해 사이트의 사용자 접속 방지 시스템 개발", 대한전자공학회 논문지 99-36S-8-1, 1999년8월호.

정 중 수

1981년 2월 영남대학교 전자공학과(학사). 1983년 2월 연세대학교 전자공학과(석사). 1993년 8월 연세대학교 전자공학과(박사). 1983년 3월 ~ 1994년 2월 ETRI 연구원, 선임연구원. 1987년 8월 ~ 1989년 8월 벨지움 Alcal/Bell Telephone사 객원연구원. 2000년 1월 ~ 2001년 1월 미국 UMASS/Lowell 전산학과 객원교수. 1994년 3월 ~ 현재 국립 안동대학교 공과대학 전자정보산업학부 부교수

이 준 원

1978년 2월 서울대학교 전자공학과(학사). 1986년 2월 충남대학교 전자계산학과(석사). 1997년 8월 충북대학교 전자공학과(박사). 1980년 3월 ~ 1994년 2월 ETRI 연구원, 책임연구원. 1986년 3월 ~ 1988년 3월 미국 AT&T사 객원연구원. 1998년 3월 ~ 현재 국립 안동대학교 공과대학 전자정보산업학부 교수