웹 기반의 실시간 인터넷 트래픽 흐름 측정 및 분석

최연숙, 김재영, 홍원기
포항공과대학교 컴퓨터공학과
분산처리 및 네트워크관리 연구실
{yschoi, jay, jwkhong}@postech.ac.kr

요 약

인터넷의 사용자가 늘어남에 따라 인터넷에서 구할 수 있는 정보와 WWW (World-Wide Web)을 통한 인터넷 서비스가 다양하게 제공되고 있다. 이러한 서비스는 네트워크와 관련되어 개발되면서 트래픽이 날로 증가하고 있다. 트래픽이 급증함에 따라 발생되는 네트워크 관련 문제들을 해결하기 위해 어느 호스트나 응용 프로그램이 많은 트래픽을 유발하는지 알아내는 일은 매우 중요한 일이다. 이를 해결하기 위해 네트워크 트래픽을 모니터링 및 분석하는 시스템의 개발이 필요하게 되었다. 본 논문에서는 웹 기반의 실시간 트래픽 흐름을 측정 및 분석할 수 있는 관리 시스템을 설계하고 구현하였다. 이는 실시간으로 처리된 네트워크 트래픽 흐름을 웹 브라우저를 통해 쉽게 분석할 수 있으며, 호스트 정보와 프로토콜 정보에 대한 트래픽량을 볼 수 있다. 각 프로토콜 정보에 대해서는 매 시간 히스토리를 저장하여 하루 동안의 정보에 대한 분석자료를 하여 보여주고 있다.

1. 서론

인터넷은 수많은 컴퓨터 통신망을 상호 연결하는 통신망 중의 통신망으로서, 1969 년 미국 국방성의 컴퓨터 통신망인 ARPANET[1]으로 시작된 이래 꾸준히 발전해 오다 최근에는 그 발전 속도가 기하급수적으로 빨라지고 있다. 최근 들어 인터넷 사용자가 늘어남에 따라 인터넷에서 구할 수 있는 정보도 빠른 속도로 늘어나고 있으며, WWW (World-Wide Web)의 대중화와 함께 WWW 을 통해 다양한 인터넷 서비스가 제공되고 있다. 이러한 서비스를 제공하는 다양한 응용 프로그램들이 네트워크와 관련되어 개발되면서 네트워크 트래픽은 날로 증가하고 있다.

급속히 증가하는 트래픽으로 인해 네트워크의 회선이 부족하게 되고, 원하는 서비스의 응답 시간이 저하되는 등의 여러 가지 문제점이 발생하고 있다. 이를 해결하기 위해 네트워크상의 장비들을 모니터링 및 분석하는 시스템 개발이 필요하게 되었다. 이러한 시스템은 현재 얼마나 많은 트래픽이 유발되고 있는지 그리고 어떤 시스템에서 병목현상을 일으키고 있으며, 최대 트래픽은 얼마인지 등에 대한 정보를 네트워크 관리자에게 제공하게 된다. 이런 정보들을 네트워크 관리자가 좀 더 쉽게 관리할 수 있도록 MRTG[2], Etherfind[3], TCPdump[4], WebTrafMon[5] 등과 같이 여러 가지 시스템들이 개발되어 왔다. 이런 시스템은 네트워크에서 수집된 데이터를 MIB 에 저장하는 SNMP agent 와 데이터를 분석하여 보여주는 기능을 가진 SNMP manager 가 하나의 시스템에서 실행되기 때문에 갑자기 폭주하는 트래픽에 대한 정보를 처리할 때 시스템 부하 및 성능 저하를 초래하였다. 따라서, 이런 경우 SNMP agent 와 SNMP manager 를 서로 분리하여 실행할 수 있는 실시간 트래픽

흐름 측정 방법을 사용하여 웹에서 트래픽량을 분석할 수 있도록 하였다.

본 논문에서는 웹 기반의 실시간 트래픽량 측정과 분석하는 관리 시스템에 대한 설계 및 구현에 관해 설명하고자 한다. 이 시스템은 관리자가 원하는 시간동안 실시간으로 처리된 네트워크 트래픽의 흐름을 웹 브라우저에서 쉽게 볼 수 있다. 또한 하나의 manager 가 여러 시스템의 트래픽 흐름을 관리할 수 있다는 장점을 지니고 있다. 반면, 하나의 시스템에서 트래픽의 흐름을 보여주는 룰셋[8]이 하나만 동작하므로, 실시간으로 처리되는 시스템에 대해서는 장시간에 대한 히스토리의 저장이 어렵다는 단점을 가지고 있다.

본 논문의 구성은 다음과 같다. 먼저 기존의 네트워크 관리 시스템 중 웹 기반으로 실시되는 MRTG[2]와 WebTrafMon[5]을 정리한 다음, 웹 기반의 실시간 트래픽 흐름 측정을 이해하기 위해 실시간 트래픽 흐름 측정의 개요와 구조를 설명한다. 그리고 웹 기반의 실시간 트래픽 흐름 측정의 구조와 특징 및 구현된 분석 결과를 살펴보고자 한다.

2. 관련연구

이 장에서는 기존에 개발되어 사용되는 모니터링 도구 중 웹 기반으로 실행되는 MRTG[2]와 WebTrafMon[5]에 대해 비교 설명한다.

2.1 MRTG

MRTG(Multi-Router Traffic Grapher)[2]는 네트워크 링크 간의 트래픽 부하량을 측정하는 도구로서, SNMP 를 통해 트래픽 모니터링을 실시하여 MIB II 의 In/Out octet 정보를 알려주고 자동으로 PNG 형식의 그래프까지 생성한다. 이 정보들은 모두 웹 페이지 형식의 HTML 로 문서화되어 단순히 웹 브라우저만 있으면 사용자는 언제 어디서나 그 정보를 읽어 들일 수 있다. MRTG 는 SNMP 요구사항을 수행하는 Perl 과 SNMP 로 수집된 트래픽 데이터의 로그 계산 수행하는 C 로 작성되어 있다. 또한, 다양한 유닉스 플랫폼과 윈도우 NT 에서 작동이 가능하여 널리 사용되고 있으며, 장기간의 네트워크 트래픽 정보를 알아볼 수 있게 하는 기능도 제공한다.

MRTG 는 트래픽 정보에 대한 로그 파일을 가지고 있으므로 하루 동안의 트래픽 정보를 보여줄 수 있으며, 일주일, 한 달간, 심지어는 1 년 동안의 트래픽 정보를 한꺼번에 표시할 수도 있다. 그러나 어느 호스트가 트래픽을 유발했으며 어느 프로토콜이 병목현상을 일으켰는가 하는 등의 관리자가 문제 해결에 있어서 가장 필요한 정보들을 제공해 주지 못한다는 단점이 있다.

2.2 WebTrafMon

WebTrafMon[5]은 웹 기반의 사용자 인터페이스를 채택하여 사용자가 트래픽 정보를, 일반적이면서도 쉽고 간편하게 구할 수 있는 웹 브라우저를 통해 접근한다. 사용자들은 오직 인터넷에 연결된 웹 브라우저만 있으면 된다. 이 시스템은 네트워크 트래픽을 자세히 보여주며 사용자들이 각각의 네트워크 계층별로 트래픽 정보를 볼 수 있고, 발신지 정보와 목적지 정보를 함께 볼 수 있다.

WebTrafMon 은 네트워크의 가장 하위 계층부터 상위계층까지 단계적으로 패킷으로부터 헤더 정보를 추출해 낸다. 이는 트래픽 정보를 발신지와 목적지를 기준으로 웹 인터페이스를 통해 보여준다. 또한 트래픽 정보를 네트워크 계층으로부터 최상위 어플리케이션 계층까지 단계적으로 나타낼 수 있는 기능도 가지고 있다. 최근에는 많은 데이터 전송을 필요로 하는 멀티미디어 정보가 점차 일반화 되면서 트래픽 관리는 더욱 중요한 문제로 대두되고 있는 것으로 보아 네트워크 관리는 매우 중요한 요소라 할 수 있다.

WebTrafMon 의 구성요소는 프로브(probe)와 뷰어(viewer)이다. 프로브는 네트워크 패킷으로부터 정보를 얻어내어 로그 파일에 저장하고, 뷰어는 사용자와 상호 대화식으로 작동하여 웹 브라우저를 통해 사용자에게 정보를 제공한다. 이는 프로브와 뷰어가 하나의 컴퓨터에서 동작하므로 트래픽이

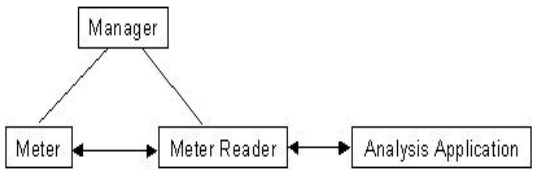
급속히 증가하는 때는 시스템의 속도나 성능저하를 초래하는 문제를 안고 있다.

3. 실시간 트래픽 흐름 측정

이 장에서는 실시간 트래픽 흐름 측정(Real-time Traffic Flow Measurement)[6,13]의 개요와 구조에 대해 설명한다. 실시간 트래픽 흐름 측정의 구성 요소 중 meter 와 manager 에 대해서 언급하고, meter 에서 실행되는 룰셋(rule set) 및 이를 새로 만들고자 할 때 사용되는 SRL(Simple Ruleset Language)[8]을 살펴보고자 한다.

3.1 개요 및 구조

실시간 트래픽 흐름 측정[6,13]은 IETF 에서 연구중에 있으며, 실시간으로 트래픽 흐름(traffic flow)을 측정하는 것을 말한다. 네트워크 상의 트래픽을 실시간으로 수립하여 흐름 단위로 정보를 분석한다. 1991 년의 RFC 1272[14]가 기본 개념을 제공하고, 1997 년 실시간 트래픽 흐름 측정의 기본구조[9]가 잡혔으며, 현재 확장작업을 하고 있다.



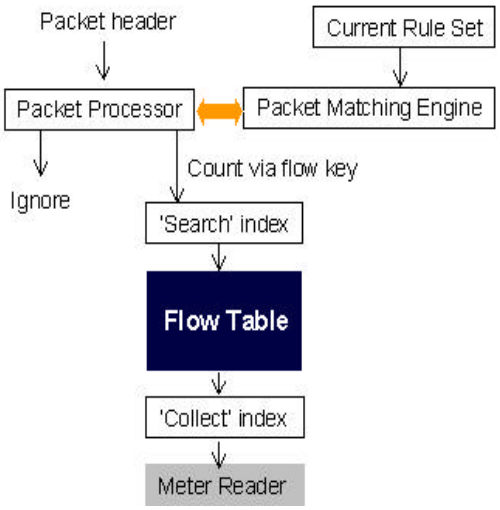
(그림 1) 실시간 트래픽 흐름 측정 구조

실시간 트래픽 흐름 측정 구조[7]는 그림 1 과 같이 meter, meter reader, manager, analysis application 으로 구성되어 있다. meter 는 네트워크 내에 주어진 측정 지점(metering point)에서 트래픽 흐름에 대한 데이터를 수집하여 측정 데이터를 만들고, meter reader 는 meter 로부터 측정 데이터를 읽어 들인다. manager 는 네트워크를 통해 meter 와 meter reader 가 통신하는 호스트에서 실행되는 프로그램으로, meter 를 설정하고 meter reader 를 제어하는 관리 모듈이며, analysis application 은 측정 데이터를 분석하여 사용자가 원하는 형태로 출력한다. meter 는 패킷이나 바이트 수와 같은 특정 속성(attribute)으로 계산하고, 발신지와 목적지 주소와 같은 다른 속성을 이용하여 셀 수 있는 개체(entity)로 분류한다. 이 개체는 네트워크 내에 사용자, 호스트 이름, 네트워크 그룹 등으로 네트워크 구성에 있어 세분화될 수 있다. 모든 속성은 manager 는 하나 또는 그 이상의 meter 를 제어할 수 있다. 현재 동작중인 meter 에 대해서는 단 하나의 manager 로 제어가 가능하다. meter 는 실시간 트래픽 흐름 측정 meter MIB 을 실행하는 SNMP agent 이고, manager 는 흐름 데이터를 저장하고 접근하기 위해 meter MIB 을 사용하는 SNMP manager 이다.

3.2 meter

meter[7]는 네트워크가 동작되는 측정 지점에 놓고, 이 지점에서 트래픽 흐름에 대한 데이터를 수집한다. 네트워크의 측정 지점을 지나가는 모든 패킷의 헤더는 meter 내에서 정의된다. 하나의 meter 는 단 하나의 룰셋을 실행시킨다. 하나의 meter 가 몇 개의 룰셋을 동시에 실행할 수는 있지만, 이 때 동작되는 모든 룰셋은 하나의 흐름 테이블(flow table)로 만들게 된다. 이는 독립적으로 몇 개의 meter 를 실행하는 것과 같다. 각 meter 는 환경구성에 따라 선택적으로 네트워크 동작을 저장할 수 있으며, 저장 전에 데이터의 조합, 변형, 처리 등이 가능하다.

그림 2 는 meter 의 구조를 나타낸 것이다. 네트워크로부터 들어오는 패킷 헤더들은 모두 패킷 프로세서를 지나가고, 패킷 프로세서는 이것들을 PME(Packet Matching Engine)로 보낸다. PME 는 가상 머신(virtual machine)으로 현재 룰셋을 가지고 패킷 매칭 프로그램을 실행함으로써 패킷들을 분류한다



(그림 2) meter의 구조

이 때 어떤 패킷들은 버려지고, 다른 패킷들은 흐름 키(flow key)를 통해 흐름 테이블에 계산된다. meter reader[7]는 어느 때든 패킷 흐름 테이블로부터 데이터를 모으게 된다. 흐름 테이블은 meter에 의해 나타나는 흐름이 저장된다. 여기에는 흐름 발신지와 목적지의 주소, 발신지에서 목적지까지 또는 목적지에서 발신지까지의 흐름 트래픽 수, 패킷이 처음 지나간 시간과 마지막으로 지나간 시간 또는 다른 속성 등을 포함하고 있다. 룰셋은 룰(rule)들의 배열형태로, 들어오는 패킷들을 분류하기 위해 meter 에서 사용된다. 룰셋은 SRL(Simple Ruleset Language)로 작성되어 있으며, SRL에 대한 자세한 설명은 3.5에서 다시 언급하겠다. 흐름을 위한 패킷이 측정 지점을 양방향으로 지나가면 meter는 패킷을 매칭시켜 각 방향에 대한 카운터를 제공한다. 만약 패킷이 한 쪽 방향으로만 지나가면 그 방향만 카운트한다.

3.3 manager

manager[7]는 meter를 구성하고 meter reader를 제어하는 응용 프로그램이다. meter는 룰셋의 배열 중 하나가 기본적인 룰셋을 가지고 있다. 이것은 변경이 불가능하며, 다른 룰셋을 원할 경우 manager로 불러들인다. 룰셋을 한 번 불러들이면 manager는 이 룰셋을 meter에 알려 실행되도록 한다. 이러한 기능은 Download Rule Set, Switch to Specified Rule Set, Set High Water Mark, Set Flow Termination Parameters, Set Inactivity Timeout 등의 제어함수[7]를 통해 meter와 상호작용을 한다.

3.4 meter MIB

meter MIB[10]은 1995년 12월 달라스 IETF 회의를 시작으로 David Perkins가 SNMPv2 MIB으로 제출하여, 1996 년 초에 개발되었다. 실시간 트래픽 흐름 측정에 쓰이는 flowMIB[10]은 flowControl, flowData, flowRules, flowMIBConformance로 구성되어 있다. flowControl은 룰의 인덱스, 크기, 소유자 등에 대한 정보나 룰셋을 위해 manager의 인덱스, 현재 사용되는 룰셋, 소유자, 현재 상태 등의 정보를 관리한다. flowData는 실제 분석하고자 하는 데이터들의 대부분을 관리하고 있다. 발신지와 수신지의 데이터 정보, 네트워크 계층, 전송 계층, 어플리케이션 계층의 프로토콜 정보 및 패킷 크기, 바이트 수 등의 정보를 관리한다. flowRules 는 룰셋을 위해 룰 테이블에 대한 정보를 가지고 있다. 트래픽 흐름 측정을 위한 정보가 저장된 flowData에서 사용된 변수는 다음과 같다. PeerType 는 PeerAddress 의 형태를 나타낸다. 1 과 2 는 각각 IPv4와 Ipv6, 3은 CLNS, 11은 IPX, 11은 appletalk, 13 은 DECnet 를 가리킨다. TransType 는 Tranport Address 의 형태를 나타내며, 값이 6 일 경우 tcp, 17인 경우는 udp, 1인 경우에는 icmp 를 나타낸다. 그 외 발신지와 수신지의 주소를 알 수 있는 변수인 SourceTransAddress 와 DestTransAddress 등을 사용하였다.

3.5 SRL

실시간 트래픽 흐름 측정 meter 는 각 흐름에서 어떤 정보들이 저장되었는지를 나타낸다. meter 를 구성하면서 사용자는 manager 로부터 읽어 들일 수 있는 새로운 룰셋을 요구한다. 이 룰셋은 meter의 PME를 위한 패킷 매칭 프로그램이다. SRL(Simple Ruleset Lanauage)[8]은 트래픽 흐름을 지정하고 명령들을 실행하기 위한 언어로 룰셋을 만드는 데 있어 보다 쉬운 방법으로 제공되고 있

다. SRL 프로그램은 meter 에 들어오는 각각의 새로운 패킷부터 실행된다. 현재 패킷이 흐름에 있어서 중요한지의 여부와 필요성 및 방향 등을 결정하고, 나머지 패킷은 버리게 된다. 흐름이거나 흐름의 정보량을 모으는데 요구되는 정보들은 저장한다. SRL 에서는 IF 문을 사용하여 패킷이나 SRL 변수로부터의 정보를 비교하고, SAVE 문은 흐름 속성을 저장한다. 또한, COUNT 문은 통계적 데이터를 모아 증가 시킨다.

다음은 SRL 프로그램의 몇 가지 규칙을 나타낸 것이다.

- '#' 다음의 문장은 주석을 나타낸다.
- 각 명령어는 스페이스로 구분한다.
- 문장의 마지막에는 세미콜론(;)을 사용한다.
- 식별자(identifier)는 영문자로 시작하며 영문자, 숫자, 특수문자 '_'를 사용할 수 있다.
- 이미 사용중인 예약어는 식별자로 사용될 수 없다.

그림 3 은 SRL 로 작성된 룰셋의 예제를 나타낸 것이다. 네트워크 계층 프로토콜 정보인 IP, EtherTalk, IPX, DECnet 등과 트랜스포트 계층 프로토콜 정보인 tcp, udp, icmp 를 보여주는 룰셋이다.

```
SourcePeerType == IP save, {

    if SourceTransType == tcp save;
    else if SourceTransType == udp save;
    else if SourceTransType == icmp save;
    count;

}
else if SourcePeerType == 12 save;   # EtherTalk
else if SourcePeerType == 2 save;    # IP6
else if SourcePeerType == 3 save;    # NSAP(CLNS)
else if SourcePeerType == 6 save;    # Other
else if SourcePeerType == 11 save;   # Novell(IPX)
else if SourcePeerType == 13 save;   # DECnet
else ignore;
count;
```

(그림 3) SRL 로 작성된 룰셋 예제

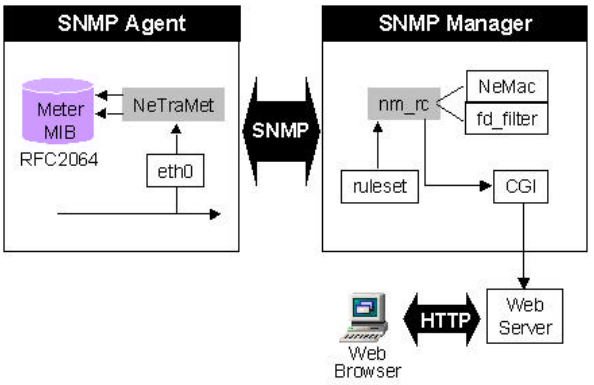
4. 웹 기반의 실시간 트래픽 흐름 측정 시스템의 설계

이 장에서는 앞에서 언급한 실시간 트래픽 흐름 측정을 웹 기반으로 설계한 웹 기반의 실시간 트래픽 흐름 측정에 대한 전체적인 구조와 각각의 구성요소에 대해 설명하고, 이 시스템의 특징들에 대해 살펴본다.

4.1 구조

웹 기반의 실시간 트래픽 흐름 측정의 구조는 그림 4 와 같다.

SNMP Agent 는 실시간 트래픽 흐름 측정 meter 인 NeTraMet[9]와 네트워크의 측정 지점에서 읽어 들인 흐름 정보를 저장하는 meter MIB[10]으로 구성되어 있다. NeTraMet meter는 SNMPv2 를 사용하는 독립적인 SNMP agent 이다. meter MIB 에 대한 자세한 정보는 RFC 2064[10]에 자세히 나와 있다. SNMP manager 는 NeTraMet 을 원격관리하기 위한 manager 인 nm_rc[11]와 룰셋, 웹 기반에 필요한 CGI 로 구성되어 있다.



(그림 4) 웹 기반의 실시간 트래픽 흐름 측정의 구조

nm_rc 는 실시간 트래픽 흐름 측정 manager 와 meter reader 를 함께 구현한 NeMac[11]과 주어진 흐름 데이터의 내용을 주어진 포맷 파일에 맞추어 필터링하여 새로운 흐름 데이터를 만드는 fd_filter[11]로 구성되어 있다. NeMac 은 주어진 룰셋에 맞추어 흐름 데이터를 읽어 들이도록 meter 에 지시하며, 주어진 시간 간격으로 특정 meter 의 흐름 데이터를 SNMP 로 읽어와서 정해진 형태로 출력한다. 이렇게 나온 결과는 웹 서버를 통해 웹 브라우저에서 볼 수 있다.

4.2 장점 및 단점

이 시스템은 SNMP agent 와 SNMP manager 를 서로 분리시켜 실행할 수 있는 것이 가장 큰 장점이라 할 수 있다. 하나의 컴퓨터에서 모든 일을 처리할 경우 manager 가 네트워크 결과는 분석하고 보여주는 데 있어 시스템 저하를 가져오는 경우가 많았다. 이 시스템은 그러한 단점을 보완하여 agent 와 manager 를 분리시켜 서로 다른 컴퓨터에서 실행할 수 있다. 또한, agent 와 manager 를 분리하여 실행함으로써 관리자는 하나의 manager 를 통해 여러 agent 의 트래픽 정보를 불러들여 관리할 수 있다.

실시간으로 읽어 들인 흐름 정보는 데이터 크기에 따라 분석되며, 각 흐름은 바이트 수, 패킷 수, 발신지 호스트와 목적지 호스트, 네트워크 계층 프로토콜, 전송 계층 프로토콜, 어플리케이션 계층 프로토콜에 대한 정보를 보여준다. 또한, 프로토콜 정보에 대해서는 한 시간마다 발생하는 흐름을 저장하여 총 하루 동안 발생된 정보를 보여준다. meter 가 실행중인 시스템의 IP 주소와 분석하고자 하는 트래픽의 시간 간격을 입력하여 manager 가 원하는 조건에 맞추어 흐름을 분석함으로써 더 자세한 정보를 얻을 수 있다.

반면, 하나의 meter 는 하나의 룰셋을 실행하는 것이 단점이라 할 수 있다. 이 시스템에서 트래픽 흐름은 호스트 및 프로토콜 정보를 세부적으로 보여주고 있다. 이 때 트래픽 흐름의 종류는 매우 다양하여 적은 용량을 요구하는 트래픽 흐름의 실시간 분석에 대해서는 높은 성능을 보이지만, 장시간의 트래픽 흐름을 저장할 경우, 분석하는 데 어려움이 있다. 따라서 이 시스템에서는 프로토콜 정보에 대한 히스토리 저장을 가능하도록 하였다.

4.3 시스템 설계

웹 기반의 실시간 트래픽 흐름 측정은 실시간으로 분석되는 흐름의 크기에 따라 분류하여 보여주도록 설계되어 있다. 각 흐름이 차지하는 크기를 퍼센트(%), 패킷 수, 바이트 수 별로 분류하여 보여준다. 프로토콜 정보에서는 네트워크 계층, 전송 계층, 어플리케이션 계층에 대한 정보를 보여주도록 되어 있으며, 네트워크 계층별로 발신지 주소와 목적지 주소를 볼 수 있고, 어플리케이션 계층에서는 발신지와 목적지에 해당하는 서비스 정보를 볼 수 있도록 되어 있다. 또한, 메뉴에서 각 프로토콜 정보별로 구분하여 해당 프로토콜 정보에 대한 트래픽량을 분석하여 설계하였다.

설계된 웹 기반의 실시간 트래픽 흐름 측정은 매 시간 별로 프로토콜에 대한 정보를 저장하여 하루 동안의 히스토리를 분석할 수 있도록 하였다.

5. 시스템 구현

이 장에서 설명한 웹 기반의 실시간 트래픽 흐름 측정을 기반으로 하여 설계된 시스템의 개발환경에 대해 설명하고, 시스템을 설치하는데 있어 요구 사항들에 대해 나열한다. 마지막으로 실제 구현된 시스템을 살펴보고자 한다.

5.1 개발환경

웹 기반의 실시간 트래픽 흐름 측정시스템은 다음과 같은 환경에서 개발하였다. Linux Kernel 2.0.32 운영 체제인 Intel Pentium 100MHz, 64MB 메모리의 컴퓨터와 Intel Pentium 133MHz, 64MB 메모리의 컴퓨터를 각각 meter 와 manager 로 사용하였다. 트래픽 모니터링 툴로 Libpcap 0.4a6[4]을 사용하고, meter 는 New Zealand 의 University of Auckland 의 Nevil Brownlee 에 의해 구현된 NeTraMet[11]을 사용하였다. 또한 manager 에서 불러들이는 룰셋은 SRL 로 구성하였다. 그 외 웹 서버로는 Apache Web Server 1.2.5 와 CGI 프로그램 작성을 위해 Perl 5.004_01, HTML 을 사용하였다.

5.2 시스템 요구사항

이 시스템을 사용하기 위해서는 manager 로 사용할 웹 서버가 구동 가능한 컴퓨터와 meter 로 사용할 Linux 나 Unix 환경의 컴퓨터가 필요하다. meter 와 manager 를 하나의 컴퓨터에서 실행하고

자 할 때는 한 대의 컴퓨터만 있으면 된다. 소프트웨어는 meter 기능을 하는 NeTraMet 또는 NetFlowMet[9]이 필요하며 NeTraMet 의 경우는 패킷을 수립할 수 있도록 Libpcap[4]이 설치되어야 한다.

5.3 시스템 구현

여기서는 실제 구현된 시스템의 실행결과 화면을 각각 살펴보고자 한다.

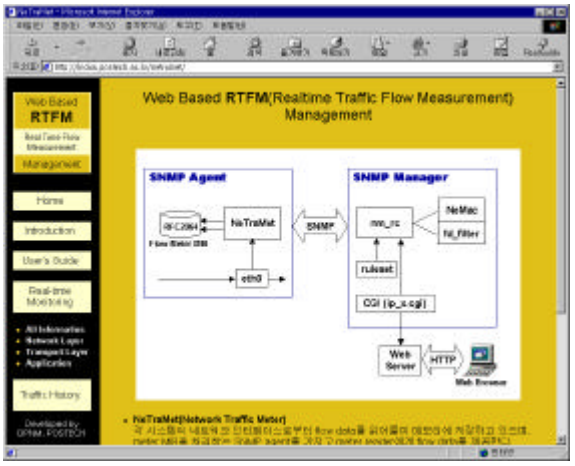
5.3.1 웹 기반의 실시간 트래픽 흐름 측정 시스템의 화면 구성

웹 기반의 실시간 트래픽 흐름 측정을 위한 룰셋 파일은 그림 5 와 같은 형태를 갖는다. 첫 줄은 현재 측정하고 있는 시스템의 호스트 정보, 인터페이스, 총 흐름 수, 패킷 및 바이트 수, 모니터링 시간 등을 보여주고 있으며, 그 다음은 모니터링 된 결과 데이터를 보여준다.

```
141.223.82.26 eth0  678 flows  7pps 890Bps  16:00:00 Fri 18 Feb 2000
29%  927759 7576 0 0 ipx 0 11 11
27%  858782 11434 0 0 oth 0 0 0
19%  605112 2382 0 0 ip4 udp  netbios-dgm netbios-dgm
5%  149528 1485 0 0 ip4 udp  netbios-ns netbios-ns
4%  104958 307  31872 92 ip4 udp  bootpc bootps
3%  85350 261 0 0 ip4 udp  efs efs
1%  42726 32 3792 32 ip4 udp  snmp 1127
1%  30114 239 0 0 ip4 udp  1050 epmap
1%  19466 204 0 0 ip4 icmp 0 0
0%  13200 120 0 0 ip4 udp  locus-con locus-map
0%  0 0 8656 7 ip4 tcp  iad2 netbios-ssn
0%  8560 40 0 0 ip4 udp  login login
```

(그림 5) 웹 기반의 실시간 트래픽 흐름 측정을 위한 룰셋 예제

그림 6 은 실제 웹 브라우저에서 실행된 시스템의 화면 구성을 나타낸 것이다. 왼쪽의 메뉴를 통해 각각의 정보를 볼 수 있으며, 현재 화면의 “Introduction”은 웹 기반의 실시간 트래픽 흐름 측정 시스템의 구조와 기능들을 소개하고 있다.

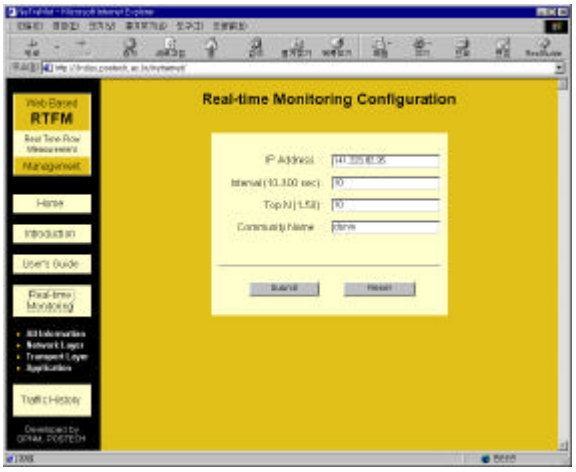


(그림 6) 웹 기반의 실시간 트래픽 흐름 측정 소개

모니터링 메뉴는 “Real-time Monitoring”과 “Traffic History” 두 가지로 나누어져 있다. “Real-time Monitoring”은 실시간으로 트래픽 정보를 분석하여 보여주며, “Traffic History”는 1 시간 단위로 저장된 트래픽 정보를 분석하여 보여준다.

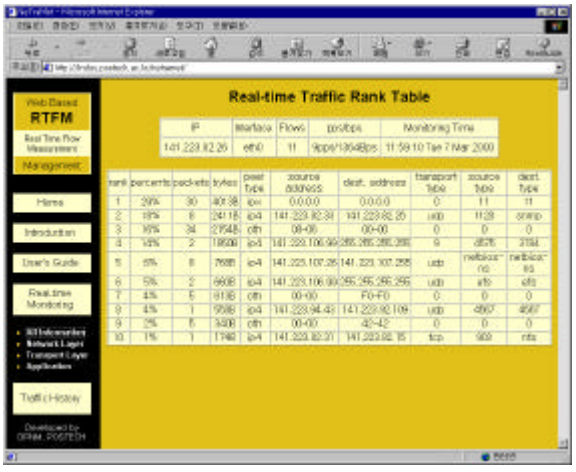
5.3.2 실시간 모니터링 구성 및 결과

이 시스템은 실시간 모니터링 분석 결과를 보여주는 기능을 가지고 있으며, “Real-time Monitoring” 메뉴를 통해 결과를 볼 수 있다. 그림 7 은 실시간으로 분석되는 트래픽 정보를 보기 위한 환경 설정으로, 원하는 서버의 IP 주소를 입력할 수 있고, 분석하고자 하는 트래픽의 시간 간격, 상위 개수 등을 입력하여 원하는 형태의 결과를 볼 수 있다. 현재 초기 시간 간격은 10 초, 상위 개수는 10 개로 설정되어 있다. 이 때 IP 주소를 적는 서버에서는 meter 를 먼저 실행시켜야 한다.



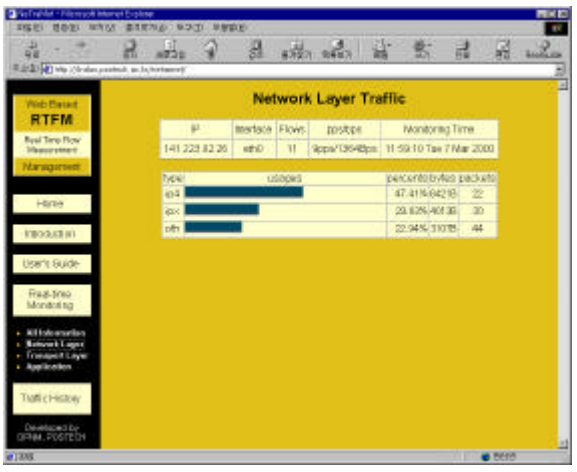
(그림 7) 시스템의 실시간 모니터링 환경 설정

그림 8 은 실시간 모니터링 분석의 전체적인 결과를 나타낸 것이다. 두 개의 테이블 중 위 테이블에서는 IP 주소, 인터페이스, 총 흐름 개수 및 모니터링 시간을 알려주고 있다. 그림 8 의 아래 테이블은 실제 트래픽의 분석 결과이다. 각 흐름의 패킷 수, 바이트 수 및 네트워크 계층 프로토콜, 발신지와 목적지 주소, 전송 계층 프로토콜, 발신지와 목적지에서 사용하는 어플리케이션 계층 프로토콜 정보를 차례로 보여주고 있다.



(그림 8) 실시간 모니터링 분석의 전체적인 결과

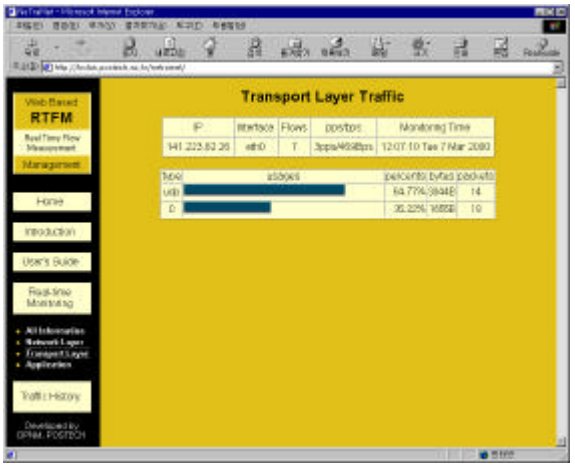
그림 9 는 그림 8 의 실시간 모니터링 분석 결과에서 네트워크 계층 프로토콜에 대한 결과만을 나타낸 것이다. 현재 화면에서는 IP 가 약 71%로 가장 많이 차지하고 있음을 알 수 있다. 여기에서도 각각의 데이터 양과 패킷 수를 보여주고 있다.



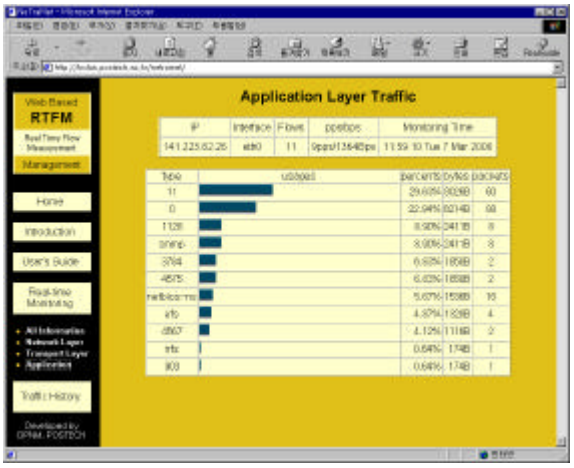
(그림 9) 네트워크 계층 프로토콜에 대한 실시간 모니터링 결과

그림 10 은 그림 8 의 실시간 모니터링 분석 결과에서 전송 계층 프로토콜에 대한 결과를 나타낸 것이다. 각각의 바이트 수와 패킷 수를 보여주고 있다.

그림 11 은 그림 8 의 실시간 모니터링 분석 결과에서 어플리케이션 계층 프로토콜에 대한 결과를 나타낸 것이다. IANA[12]에서 정의되지 않는 전송 계층 프로토콜 포트에 대해서는 포트 번호를 그대로 보여주고 있다.



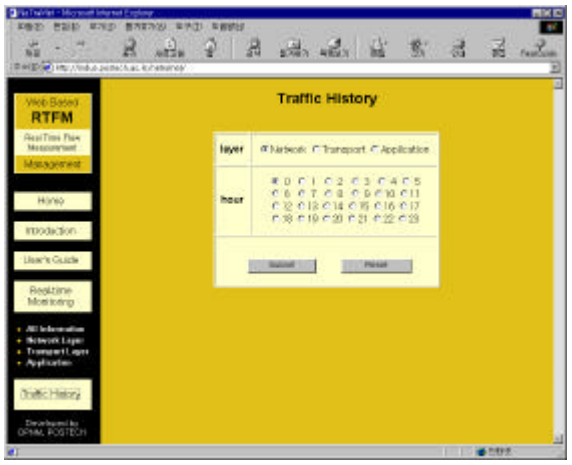
(그림 10) 전송 계층 프로토콜에 대한 실시간 모니터링 결과



(그림 11) 어플리케이션 계층 프로토콜에 대한 실시간 모니터링 결과

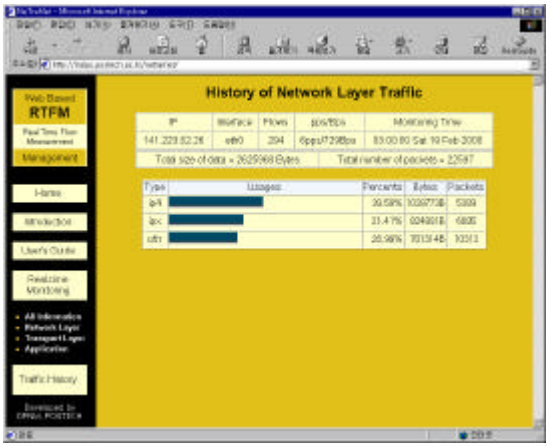
5.3.3 트래픽 히스토리 구성 및 결과

웹 기반의 실시간 트래픽 흐름 측정 시스템은 프로토콜 정보에 대해서 한 시간 단위로 트래픽 정보가 저장되어 각 시간별 분석 결과를 볼 수 있다. 그림 12 는 한 시간 단위로 저장된 트래픽 결과를 보기위한 화면이다. 네트워크 계층 프로토콜, 전송 계층 프로토콜, 어플리케이션 계층 프로토콜의 세 계층 프로토콜 정보를 보여주며, 원하는 시간을 선택함으로써 해당 시간의 트래픽 결과를 볼 수 있다.



(그림 12) 트래픽 히스토리 분석을 위한 환경설정

그림 13 은 그림 12 에서 네트워크 계층 프로토콜에 대한 한 시간대를 선택한 결과이다. 총 세 개의 테이블이 나타나며, 첫 번째 테이블에서는 IP 주소, 인터페이스, 총 흐름 개수 및 모니터링 시간을 알려준다. 두 번째 테이블은 현재 시간대의 총 데이터량과 패킷 수를 보여주고 있다. 마지막 테이블에서는 네트워크 계층 프로토콜의 정보에 대한 형태와 차지하는 범위, 데이터 양과 패킷 수를 보여준다.



(그림 13) 네트워크 계층 프로토콜에 대한 히스토리 분석 결과

그림 14는 그림 12에서 전송 계층 프로토콜에 대한 정보를 선택하여 나온 결과이다.

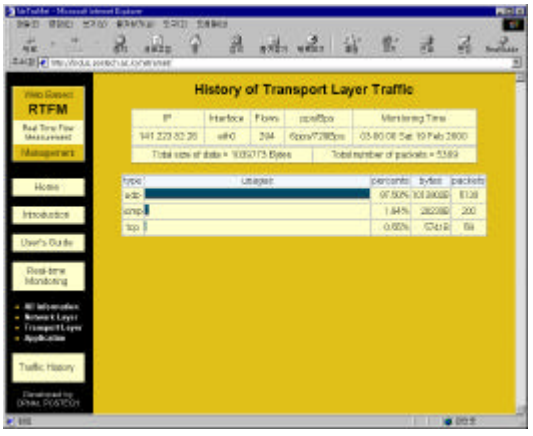


그림 14. 전송 계층 프로토콜에 대한 히스토리 분석 결과

그림 13 의 결과와 마찬 가지로 각 테이블에서는

IP 주소, 인터페이스, 모니터링 시간 및 총 바이트 수와 패킷 수를 보여주고 있다. 맨 아래 테이블은 전송 계층 프로토콜의 형태 및 각각이 차지하는 데이터 양과 패킷 수를 보여주고 있다. 현재 트래픽 결과에서는 대부분을 udp 가 차지하고 있음을 알 수 있다.

그림 15 는 그림 12 에서 어플리케이션 계층 프로토콜에 대한 정보를 선택하여 나온 결과이다. 다른 결과와 마찬 가지로 이 결과에서도 IP 주소, 인터페이스, 모니터링 시간 및 총 바이트 수와 패킷 수를 보여준다. 또한 어플리케이션 계층의 서비스 형태를 보여주고, 그에 따른 각각의 데이터 양과 패킷 수를 보여주고 있다. 서비스 형태가 숫자인 경우는 IANA[12]에서 정의되지 않은 포트 번호를 그대로 보여주는 것이다.

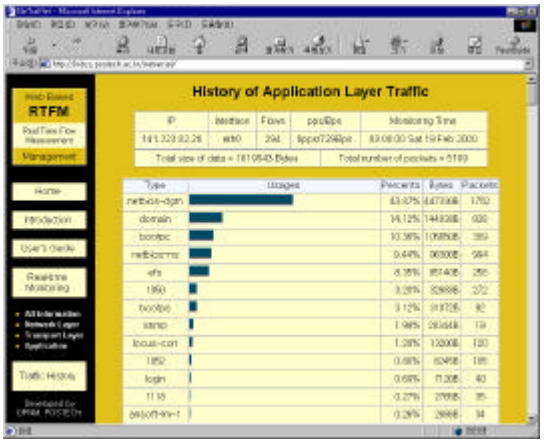


그림 15. 어플리케이션 계층 프로토콜에 대한 히스토리 분석 결과

6. 결론 및 향후과제

인터넷이 대중화 및 보편화되면서 사용자는 기하급수적으로 늘어가고, 인터넷에서 제공되는 서비스도 다양해지고 있다. 대역폭을 많이 차지하는 AOD(Audio On Demand), VOD(Video On Demand) 등의 멀티미디어 정보가 더욱 증가하면서 트래픽 관리는 더욱 중요한 요소로 대두되고 있다.

본 논문에서 언급한 웹 기반의 실시간 트래픽 흐름 측정은 웹을 기반으로 하기 때문에 인터넷을 접속하여 쉽게 트래픽의 결과를 볼 수 있음을 알 수 있었다. 이 시스템은 meter 와 manager 기능을 서로 다른 컴퓨터에서 실행되도록 함으로써 manager 는 meter 와 상관없이 트래픽 정보를 분석하여 보여줄 수 있었다. 이 경우 meter 와 manager 의 기능을 분리시켜 줌으로써 각각의 기능을 수행할 때 시스템의 부담을 줄일 수 있었으며, 하나의 manager 로 여러 meter 의 트래픽 정보를 관리할 수 있었다. 또한 manager 에서는 관리자가 분석하고자 하는 시간 간격과 출력 개수를 입력할 수 있어 사용자가 원하는 형태의 결과를 얻을 수 있었다. 또한, 시간별 히스토리를 저장하여 하루 동안의 시간별 트래픽 정보를 볼 수도 있다.

그러나 현 시스템의 meter 는 하나의 룰셋만을 실행하므로 히스토리를 저장하고자 하는 컴퓨터에 대해서는 하나의 룰셋을 실행시켜야 한다. 현재 구현된 시스템은 프로토콜 정보에 대해서만 히스토리를 저장하고 있으나 차후 보다 효율적인 룰셋을 적용하거나 히스토리를 저장하는 방법을 추가하여 실시간에서 보여지는 모든 정보를 저장하여 분석 수 있도록 하는 작업이 필요하다.

[참 고 문 헌]

[1] Michael Hauben, “History of ARPANET,” http://www.dei.isep.ipp.pt/docs/arpa-Contents.html.

[2] Tobias Oetiker and Dave Rand, “MRTG: Multi Router Traffic Grapher,” httpd://ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html.

[3] Craig Hunt, TCP/IP Network Administration, O’ Reilly and Associates, Inc., 1992.

[4] Lawrence Berkley National Laboratory, "tcpdump 3.4a6", ftp://ftp.ee.lbl.gov.

[5] J. Won-Ki Hong, Soon-Sun Kwon and Jae-Young Kim, "WebTrafMon: Web-based Internet/Intranet Network Traffic Monitoring and Analysis System", Computer Communications, Elsevier Science, Vol. 22, No. 14, September 1999, pp. 1333-1342.

[6] S. Handelman, S. Stibler, N. Brownlee and G. Ruth, "RTFM : New Attributes for Traffic Flow Measurement," RFC 2724, October, 1999.

[7] N. Brownlee, C. Mills, and G. Ruth, "Traffic Flow Measurement : Architecture," RFC2722, October 1999.

[8] N. Brownlee, "SRL : A Language for Describing Traffic Flows and Specifying Actions for Flow Groups," August 1999.

[9] N. Brownlee, "Traffic Flow Measurement : Experiences with NeTraMet," RFC 2123, March 1997.

[10] N. Brownlee, "Traffic Flow Measurement : Meter MIB," RFC 2720, October 1999.

[11] N. Brownlee, NeTraMet home page," http://www.auckland.ac.nz/net/ NeTraMet.

[12] IANA, "Protocol Numbers," ftp://ftp.isi.edu/iana/assignments/protocol-numbers .

[13] N. Brownlee, "RTFM : Applicability Statement," RFC 2721, October 1999.

[14] C. Mills, D. Hirsh, G. Ruth, "Internet Accounting : Background", RFC 1272, November 1991.

최 연 숙

1996 호남대학교, 정보통신공학과 학사

1998 충북대학교, 정보통신공학과 석사

1999-현재 포항공과대학교 정보통신연구소 연구원

관심분야: 인터넷 서비스 관리

김 재 영

1994 포항공과대학교, 전자계산학 학사

1996 포항공과대학교, 전자계산학 석사

1996-1998 포항공과대학교 학술정보센터 연구원

1998-현재 포항공과대학교 컴퓨터공학과 박사과정

관심분야: 네트워크 및 분산 시스템 관리, 분산처리, CORBA, 인터넷 서비스 관리

홍 원 기

1983 Univ. of Western Ontario, 전산학 학사

1985 Univ. of Western Ontario, 전산학 석사

1985-1986 Univ. of Western Ontario, 전산학과 강사

1986-1991 Univ. of Waterloo, 전산학 박사

1991-1992 Univ. of Waterloo, Post-Doc fellow

1992-1995 Univ. of Western Ontario, 연구교수

1995-현재 포항공과대학교 컴퓨터공학과 부교수

관심분야: 분산처리, 네트워크 및 분산 시스템 관리, CORBA, Internet 관리.