SNMP를 이용한 실시간 네트워크 트래픽 모니터링 시스템
(Real-Time Network Traffic Monitoring System using SNMP)

박 진 호*, 정 진 욱**
(Jin-ho Park*, Jin-wook Chung**)

요 약 본 논문에서는 SNMP를 이용하여 네크워크 트래픽을 실시간으로 모니터링하는 시스템을 제안하였다. 제안된 시스템은 네트워크 정보를 수집하여 분석하고, 실시간 모니터링을 지원하는 분석 서버 시스템과 분석된 결과를 그래픽적으로 보여주는 클라이언트 시스템으로 구성된다. 분석 서버 시스템은 클라이언트 시스템의 분석 요구에 따라 네트워크 트래픽의 정보를 수집하여 분석하고 응답한다. 클라이언트 시스템은 사용자의 관리 요청에 대한 사용자 인터페이스 기능과 분석된 결과를 출력하는 기능이 있으며, 실제 네트워크 상에서의 활용성을 높이기 위해 웹 기반 기술을 적용하였다. 제안된 시스템은 사용자가 웹을 통해 네트워크 상의 관리 행위를 효과적으로 수행할 수 있도록 도움을 줄 것이다.

Abstract *In this paper, we propose the realtime network traffic monitoring system usin SNMP that* can supported network and system operation, management, expansion, and design using network analysis and diagnosis to a network administrator. The proposed system consists of two parts: analysis server for collection and analysis of the network information, and supports real-time monitoring of network traffic, and client system shows user a graphical data that analyzed a returned result from the server. This system implements web-based technology using Java and contributes to enhance the effectiveness of network administrator's management.

1. 서 론

최근 인터넷이 대중화되면서 네트워크 이용자들도 급속히 증가하게 되었고, 이와 더불어 정보화 사회로 접어들면서 컴퓨터 통신 기술이 급속히 발전되었다. 그리고 컴퓨터 네트워크를 이용하는 사용자들의 요구사항이 점점 복잡하고 다양화 되어 가고 있는 추세이다[1]. 또한, 네트워크 기술의 발전과 다양한 응용 프로그램의 사용에 따라 네트워크 트래픽은 현재 텍스트 형태의 데이터에서 음성, 영상, 그리고 동영상 등 멀티미디어 데이터를 포함하게 되었고, 대부분의 응용 서비스들은 대용량의 데이터와 실시간 처리를 요구하는 멀티미디어 서비스로 변해가고 있다[2]. 이를 관리하기 위해서는 기존의 자원 관리 방식에서 벗어나 응용 서비스를 대상으로 하는 새로운 관리 방식이 필요하게 되었다[3].

특히, 현재 대부분의 네트워크가 TCP/IP(Transmission Control Protocol/Internet Protocol)를 지원하고 있기 때문에 TCP/IP 프로토콜을 기반으로 하는 네트워크에서 트래픽의 분석을 위해 사용되는 관리 표준으로 SNMP(Simple Network Management Protocol)를 이용한 관리 시스템의 필요성이 대두되고 있다[4][5].

이에 따라 관리자의 관리 행위를 돕기 위하여 다양한 형태의 관리 도구가 개발되었으나, 이와 같은 관리도구들은 근본적으로 관리 기능의 한계, 사용의 불편함, 대규모 네트

* 대덕대학 인터넷정보기술계열 전임강사
** 성균관대학교 전기전자 및 컴퓨터공학부 교수

워크로의 확장성 부족, 분석 결과의 활용 방안의 문제점 등과 같은 제약을 가지고 있었기 때문에 관리자의 관리 행위는 제한적으로 수행되었다[6]. 이와 같은 문제점을 해결하기 위해 웹 관련 기술을 적용하여 관리 공간의 제약과 사용의 불편성이라는 한계를 웹이라는 플랫폼에 적용시켜 효율을 높이고자 하는 연구가 시도되고 있으나, 많은 도구들이 WAN 관리를 위한 도구들이거나 LAN 환경에 적합한 관리를 위해 세그먼트 뿐만 아니라 세그먼트 내의 모든 노드들의 통신 행위까지 모니터링하여 관리 정보를 분석하는 기능을 포함하지 못하고 있다. 또한, 추출된 관리 정보의 가공 없이 정적인 상태의 정보를 제공함으로써 분석 결과의 숙지가 어렵다는 점과 같은 단점을 포함하고 있다[7][8].

본 논문에서는 이러한 문제점을 해결하기 위하여 표준 MIB-II의 확장인 RMON MIB과 웹 기반 관리 기술을 함께 적용하여 관리자의 입장에서 의미있는 네트워크 성능 및 장애 분석 항목을 정의하였다. 그리고 웹 관련 기술을 네트워크 관리에 적용하여 네트워크 트래픽 모니터링 시스템을 구현함으로써 기존의 관리 도구들이 가지고 있는 문제점을 해결하려고 노력하였으며, 제안된 시스템은 관리자로 하여금 관리 행위를 극대화 할 수 있도록 도움을 줄 것이다.

2. 네트워크 트래픽 모니터링 시스템

본 논문에서 제안한 네트워크 트래픽 모니터링 시스템의 전체 구조는 그림 1.과 같다. 제안된 시스템은 네트워크상의 피관리 시스템들의 네트워크 활동을 모니터링하여 관리 정보를 수집하고, 그 결과를 분석하는 분석 서버와 분석 결과에 대한 활용을 높이기 위해 그래픽 데이터를 제공하는 클라이언트 시스템으로 구성된다.

모니터링 시스템은 웹 서버에 존재하는 인터넷 서버, 인트라넷 서버, 그리고 데이터베이스로 구성되며, 시스템의 동작은 웹 서버에 존재하는 HTML 문서와 자바 바이트 코드가 클라이언트로 전송되어 동작한다. 클라이언트는 애플릿으로 구현되며 사용자가 관리 요구를 하면 서버로 새로운 연결을 통해 전송하고 그 응답을 받아 사용자에게 그래프 형태로 출력한다. 이 때 메시지를 송수신하기 위해 관리 응용 전송 프로토콜(MATP : Management Application Transfer Protocol)에서 정의된 메시지 형태가 사용된다[9].

분석 서버는 클라이언트의 분석항목에 따라 실시간 분석일 경우에는 실시간 요구에 응답하며 실시간으로 정보를 수집하고 분석하여 응답한다. 누적 분석일 경우에는 데이터베이스에 있는 자료를 폴링하여 클라이언트의 요구에 응답한다.

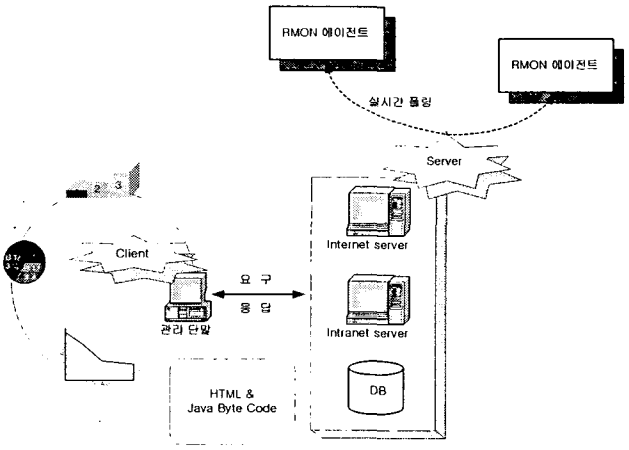


그림 1. 네트워크 트래픽 모니터링 시스템의 전체 구조
Fig 1. The structure of network traffic monitoring system

2.1 Internet 분석서버

Internet 서버는 인터넷 클라이언트(인터페이스)로 부터의 분석 요청에 대한 응답을 처리하며 이러한 처리를 위한 연결 설정이나 메시지 생성, 각 분석 항목별 데이터 처리 및 전송 등을 처리하며 웹 서버가 설치된 곳에 함께 설치되어 동작하게 된다. 그림 2.는 Internet 서버의 전체 구조이다.

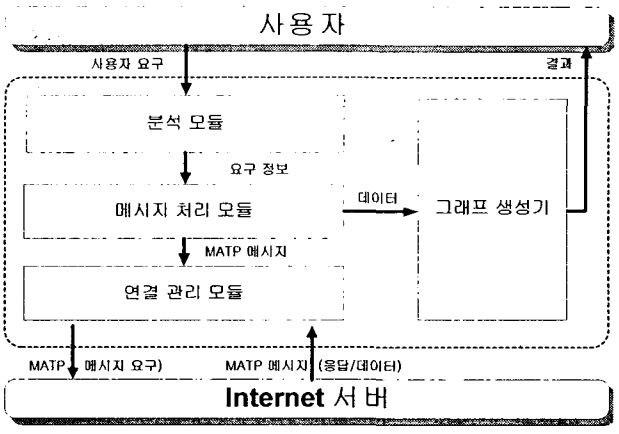


그림 2. Internet 서버의 전체 구조
Fig 2. The structure of internet server

분석 요청 메시지를 수신한 경우, 분석 모듈은 분석 항목 처리자로 메시지를 전송하고, 각 분석 항목에 따라서 관련된 관리 정보들을 폴링하기 위하여 자바로 구현된

SNMP 사용자의 호출을 통해 관리 정보를 획득하고 실시간으로 분석 정보를 생성하여 Internet 클라이언트 시스템에게 전송하게 된다.

(1) SNMP 관리자(SNMP Manager)

SNMP 관리자는 실시간 분석 요청 메시지에 대하여 Internet 서버가 분석 정보를 도출해 내기 위해 관련 MIB 정보를 폴링하기 위한 SNMP 관리자 시스템의 기능을 수행한다.

(2) 메시지 처리 모듈(Message Processing Module)

메시지 처리 모듈은 사용자가 요청한 형태에 따라 수신된 메시지를 처리하는 기능을 가지며 요청 메시지를 분석하고 해당 처리 모듈로 전송하게 된다. 이 처리 모듈과 상호 작용을 하는 모듈은 분석 모듈과 그래프 생성기 모듈에 의해 요구한 분석 항목에 대한 처리 결과를 그래프의 형태로 사용자에게 제공하게 된다.

(3) 분석 모듈(Analysis Module)

분석 모듈은 사용자가 인터넷의 현황을 분석하려는 요청에 대한 실시간 응답을 처리하는 모듈이다. 클라이언트로부터의 요청 메시지와 데이터로부터 현재의 분석 항목의 값에 대한 추출을 위하여 분석을 위한 관련 MIB 정보들을 SNMP 관리자 시스템을 호출하여 폴링을 수행하게 되며 획득한 정보를 이용하여 분석항목 처리자에게 전달하며, 매 폴링시마다 클라이언트에게 분석 정보 데이터를 전송하게 된다.

(4) 분석 항목 처리자(Analyzing Item Processor)

분석 항목 처리자는 분석 모듈에 의해서 각 분석 항목마다 폴링된 관리 정보들로부터 분석 결과를 도출하는 함수의 기능을 수행한다. 폴링된 관리 정보들은 실시간 분석 모듈의 요청에 의하여 SNMP 관리자의 수행으로 네트워크 장비들로부터 수집되며 각 분석 항목의 유형에 따라서 다른 분석 방법을 이용하여 매 시점의 분석 결과를 계산하여 실시간 분석 모듈에게 전달한다.

2.2 Intranet 서버

다음 그림 3.는 Intranet 서버의 전체 구조이다. 각각의 모듈은 LAN 분석을 위하여 자신의 기능을 가지고 있고, 그 기능들은 다음과 같다.

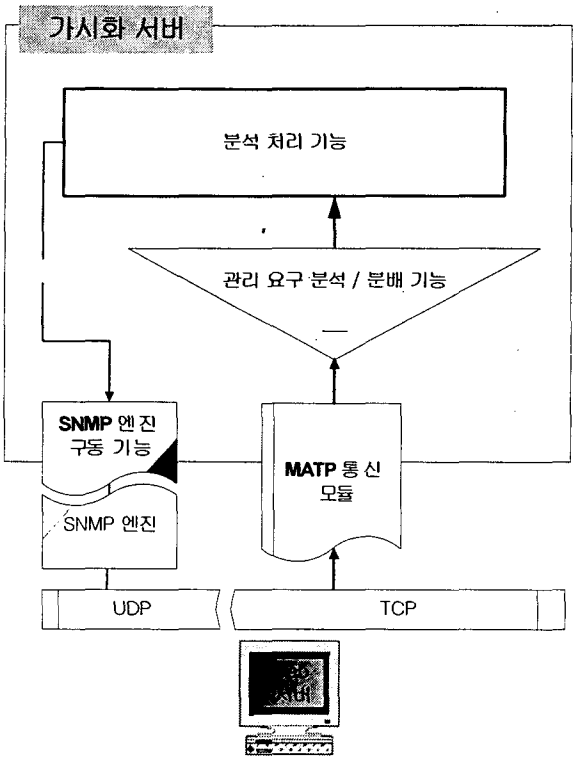


그림 3. Intranet 서버의 전체 구조
Fig 3. The structure of intranet server

(1) 웹 인터페이스

웹 인터페이스는 LAN 분석 시스템에 포함되지 않는 외부 사용자 인터페이스로서 분석 시스템에게 사용자 요구를 전달하고 또한 분석 시스템으로부터 받은 분석 결과를 사용자에게 가시화하는 부분의 인터페이스이다. 이 웹 인터페이스 부분은 Java로 구현되어지고 사용자로부터 요청을 받는 부분과 결과를 여러 가지 그래프 형태로 보여주는 부분으로 Intranet 분석 시스템과 통신한다.

(2) 사용자 요구 제어

사용자 요구 제어는 클라이언트로 전송된 메시지를 받아서 분석하여 알맞은 요구를 처리하도록 Msg를 전달한다. 클라이언트로부터 받은 메시지를 먼저 Msg 구조체에 저장하고 그 메시지의 헤더를 분석하여 각 분석항목에 해당하는 모듈로 제어를 넘긴다.

(3) RMON 설정 모듈

RMON 설정 모듈은 RMON을 설정하여 valid 또는 invalid하는 RMON 제어 모듈로서 분석항목에 따라 이 모

듈을 필요로 하는 곳에서 RMON을 제어한다.

(3) RMON 검사 모듈

사용자 요구로부터 들어온 피관리 시스템, 즉 RMON을 검사하여 RMON probe의 기능을 확인하고 관리 정보의 수집을 위해 아무런 이상이 없는지를 조사하는 기능을 수행한다. 사용자의 요구로부터 들어온 피관리 시스템들을 각각 모두 폴링하여 그 기능과 상태를 파악한다.

(4) 분석 관리 모듈

실시간으로 수집되어 축적된 관리 정보 파일을 입력으로 하여 분석 결과를 계산하여 웹 인터페이스로 전송한다.

2.3 클라이언트 시스템

클라이언트 시스템의 전체 구조는 그림 4.와 같다. 클라이언트 시스템은 사용자 클라이언트의 웹 브라우저 상에서 구동 되어지고, 크게 사용자의 관리 요청에 대한 사용자 입력 인터페이스 기능과 요청에 대한 응답을 수행하는 실시간 모니터링 기능, 정보 수집/중지 기능, 누적 분석 모니터링 기능, MIB 브라우저 기능과 분석 서버로부터 수신한 트래픽 결과를 출력해주는 그래프 출력 기능, 메시지 출력 기능 등으로 구성된다.

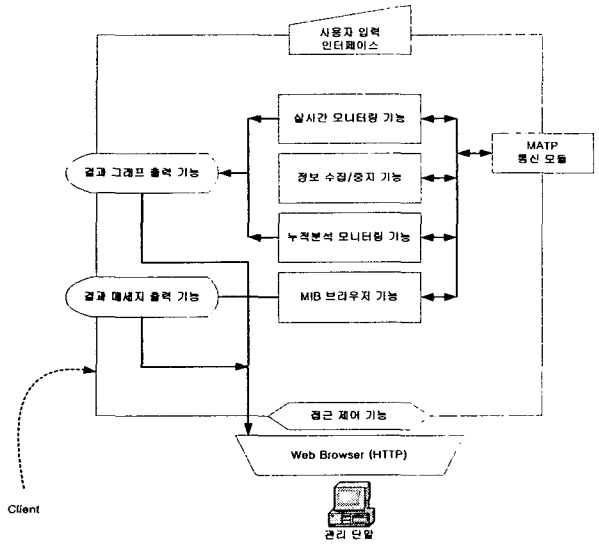


그림 4. 클라이언트 시스템의 전체 구조
Fig 4. The structure of client system

(1) 실시간 모니터링 기능

사용자가 LAN의 현재 트래픽 상태와 장애 상태를 분석하기 위한 기능으로 사용자는 피관리 시스템의 장비명, IP 주소, 포트 번호, Community, 선로 속도, 폴링 횟수 등을 입력으로 제공해야 한다. 특히, 장비명과 IP 주소는 결과를 출력할 때 어떤 장비를 분석했는지를 나타나기 위해 사용된다. 실시간 모니터링 기능은 사용자가 LAN의 현재 트래픽 상태를 분석하기 위한 요청을 입력 받고 분석 결과를 실시간으로 그래프 출력을 통해 사용자에게 보여주는 사용자 인터페이스이다. 다음 표 1.은 실시간 모니터링 기능에 대한 분석 항목이다.

(2) 수집 요구/중지 기능

사용자가 망의 성능 향상과 망 설계, 그리고 장애 진단과 같은 관리 행위를 하기 위해서는 세그먼트 상의 트래픽 통계를 수집하여 그 흐름과 경향을 분석하는 것이 필요하다. 수집 요구는 사용자의 요구에 따라 트래픽 관리 정보를 수집 중지 요구가 있을때까지 주기적으로 수집하여 데이터베이스에 저장하는 기능을 수행한다.

(3) 누적 분석 모니터링 기능

누적 분석 모니터링 기능은 LAN의 일정 기간 동안의 트래픽 상태와 장애 상태를 분석하기 위한 기능으로 RequestID, IP 주소, 폴링 횟수 등의 입력이 필요하다. 누적 분석은 수집 요구 기능에 의해 수집된 트래픽 데이터의 분석 결과를 기반으로 그래프 형식으로 출력하여 사용자에게 보여준다. 누적 분석 모니터링의 분석항목은 표 1.의 실시간 모니터링 분석 항목과 동일하다.

(4) MIB 브라우저 기능

MIB 브라우저 기능은 현재 대상 장비의 MIB 변수 값을 위한 요청을 입력받고, 해당 MIB 변수의 값을 사용자에게 보여주는 사용자 인터페이스이다. MIB 브라우저를 위해 사용자 인터페이스에서 입력받아야 할 데이터로는 해당 장비의 IP 주소와 community가 필요하다. MIB 브라우저에서 제공되는 항목들로는 크게 system, interface, at, ip, icmp, tcp, udp, egp 등이 있다.

(5) 결과 그래프 출력 기능

실시간 모니터링 요구와 누적 분석 요구에 의한 분석 결과를 그래프로 표현하여 사용자에게 출력한다. 그래프 출력은 LAN 성능 및 장애 분석 항목의 결과 출력에 가장 적합한 라인 그래프, 막대 그래프, 파이 그래프 등으로 출력한다.

(6) 결과 메시지 출력 기능

사용자의 요구에 의해 MIB 변수값을 출력하기 위한 기능으로, 간단한 메시지 형태로 사용자가 쉽게 알아 볼 수 있도록 출력한다.

표 1. 실시간 모니터링 분석 항목
Table 1. Real-time monitoring analysis item

종 류	분 석 항 목
인터넷 분석	선로 이용율
	입출력 트래픽
	선로 에러율
	패킷 손실율
	패킷 유형별 분석
	시스템 패킷 비율
인트라넷 분석	세그먼트 이용율
	세그먼트 Collision율
	세그먼트 에러율
	세그먼트 패킷 / 바이트

2.4 클라이언트와 서버 통신

웹 기반 네트워크 트래픽 모니터링 시스템은 클라이언트 시스템과 분석 서버로 구성된다. 각각의 구성 요소는 사용자로부터의 요구와 시스템 내의 응답을 주고받기 위해서는 관련된 메시지 교환 절차가 필요하다.

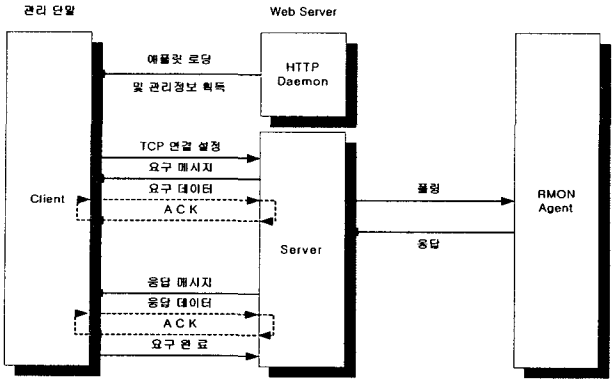


그림 5. 클라이언트와 서버간의 통신 절차
Fig 5. Communication between client and server

사용자가 인터페이스하는 클라이언트 시스템은 사용자의 관리 요구시 분석 서버로 TCP 연결을 설정하고 요구 메시지를 전송한다. 이 때 요구 메시지와 함께 요구 데이터가 서버로 전송될 수 있으며 서버는 ACK를 전송함으로써 수신을 확인한다. 클라이언트로부터 요구를 수신한 서버는 RMON Agent와 연결을 맺고 폴링을 시작한다. RMON agent는 처리된 요구의 결과를 서버로 응답하고, 서버는 처리 결과를 클라이언트로 응답 메시지를 이용하여 반환한다. 그림 5.는 이러한 클라이언트와 서버간의 통신 절차를 보여주고 있다.

그림 6.은 클라이언트와 서버간의 통신절차상에서 서로 주고 받는 메시지의 형식을 나타내고 있다.

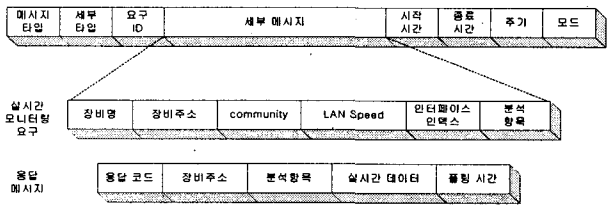


그림 6. 메시지 형식의 정의
Fig 6. Definition of message format

메시지 타입은 사용자가 분석 서버로 요청한 관리 요구의 종류를 구분하는 필드이며 세부 타입은 각 메시지 타입별로 세부적인 요청을 식별하기 위한 필드이다. 요구 ID는 사용자가 각 관리 요구를 식별하기 위한 ID이고 세부 메시지는 메시지 타입에서 각 요구에 대한 세부적인 요청을 위한 타입이다. 시작 시간 및 종료 시간은 수집 요구시에는 수집 기간을 명시하고 누적 분석 요구시에는 누적된 기간을 명시한다. 주기는 수집 요구시 폴링의 빈도를 나타내며 모드는 분석시 분석 방법을 명시하는 필드이다.

3. 실험결과 및 평가

웹 기반 네트워크 트래픽 모니터링 시스템은 사용자의 요구에 따라 실시간 분석 기능, 수집 요구/중지 기능, 누적 분석 기능, MIB 브라우저 기능 등으로 구분된다. 웹 상에서 이와 같은 기능을 처리하기 위해서 클라이언트 시스템과 분석 서버는 해당 처리 모듈을 포함하고 있다. 그림 7.은 분석 항목의 트리 구조 인터페이스와 해당 처리 기능을 수행하고자 할 때 필요한 항목 설정으로 클라이언트 시스템에서 보여지는 내용이다. 각 항목 설정은 사용자가 편리하도록 동일한 인터페이스 구조를 가지며, 분석 항목 선택시 요구하는 항목만을 설정하도록 제공한다.

실시간 분석 기능은 LAN의 현재 이용 현황 및 장애 상태를 분석하여 동적인 그래프 뷰를 제공함으로써 사용자에게 망의 진단에 대한 이해를 용이하도록 돕는다. 이러한 실시간 모니터링에 대한 결과 화면은 그림 8.에 나타나 있다. 그림 8.은 실시간으로 LAN 상의 선로 이용율을 보여

주는 그래프와 입출력 트래픽 비율을 보여주는 그래프의 예를 보여주고 있다.

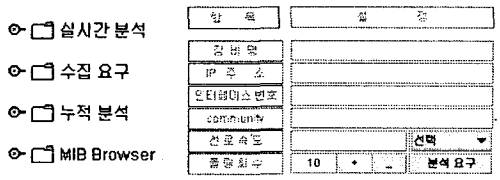


그림 7. 분석 항목 및 항목 설정
Fig 7. The example of analysis item

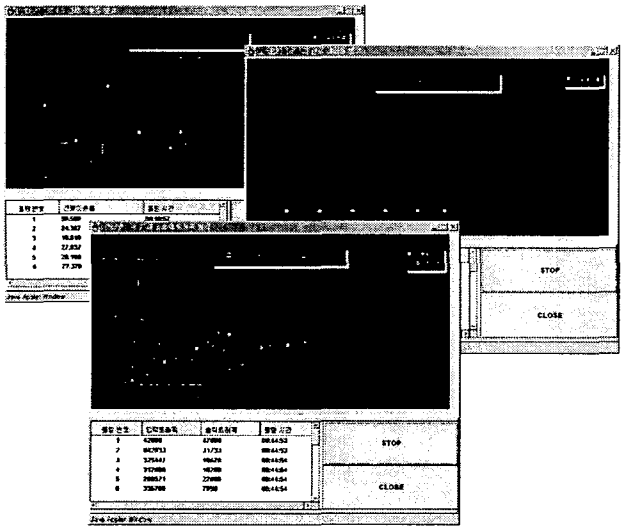


그림 8. 실시간 분석 기능의 결과 화면
Fig 8. The example of real-time analysis

수집 요구/중지 기능은 LAN에 대한 관리 정보를 누적 분석하기 위하여 LAN을 모니터링하여 관리 정보 수집을 요구하는 기능이다. 이 기능을 수행하기 위해서는 관리 대상이 되는 세그먼트의 RMON 에이전트의 IP 주소와 community, 세그먼트 속도, 관리 정보 등을 입력해야 하고 분석 서버는 이를 바탕으로 관리 정보들을 수집하게 된다. 수집 요구/중지 기능을 수행했을 때 사용자에게는 해당 메시지가 보여지게 된다.

누적 분석 기능은 LAN 상의 기본이 되는 관리 사항을 분석하기 위한 기능이다. 일정 기간동안 누적된 정보를 근거로 하여 산출된 분석 결과 정보를 다양한 형태의 그래프 뷰를 통해 제공함으로써 사용자의 이해를 용이하도록 구현되어져 있다. LAN 상의 기본적인 분석 항목인 선로 이용율, 에러율, collision율 등을 다양한 그래프 뷰를 통해 사용자는 수집된 기간의 정보를 비교해 LAN의 이상 유무를 파악할 수 있다. 그림 9.는 이러한 누적 분석 기능의 결과 화면이다.

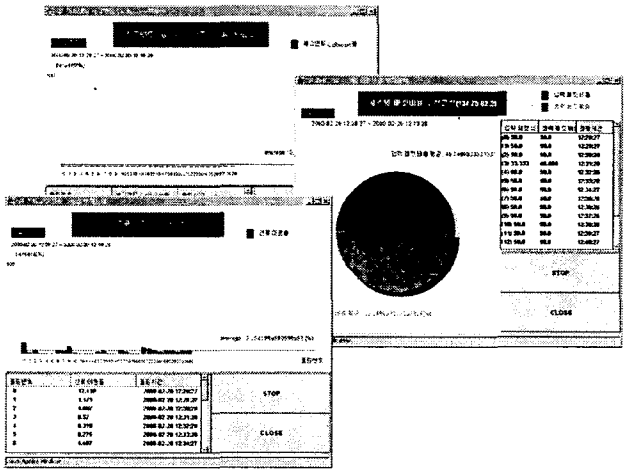
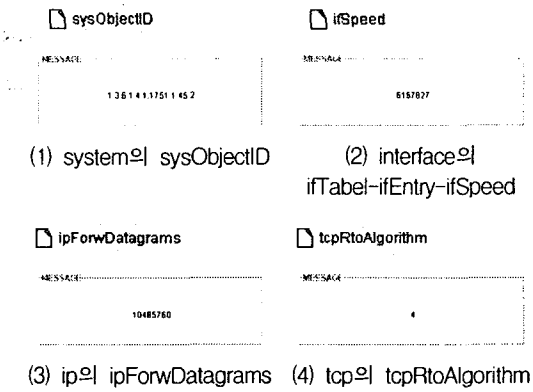


그림 9. 누적 분석 기능의 결과 화면
Fig 9. The example of accumulation analysis

MIB 브라우저 기능은 사용자가 MIB 변수의 내용을 쉽게 볼 수 있도록 제공하는 기능이다. 그림 10.에서 보듯이 MIB 브라우저의 경우 해당 항목의 결과가 MESSAGE를 통해 출력된다. 따라서 사용자는 해당 MIB 변수의 결과를 쉽게 확인할 수 있다.



(1) system의 sysObjectID (2) interface의 ifTabel-ifEntry-ifSpeed

(3) ip의 ipForwDatagrams (4) tcp의 tcpRtoAlgorithm

그림 10. MIB 브라우저의 결과 화면
Fig 10. The example of MIB browser

4. 결 론

본 논문에서는 표준 MIB인 MIB-II와 RMON MIB을 다각도로 분석하여 관련 MIB 오브젝트들을 도출하였고, 관리

자의 관리 행위의 제약을 없애고 보다 친숙한 관리툴의 사용 방법을 제공하기 위해 웹을 기반으로 하는 실시간 네트워크 트래픽 모니터링 시스템을 설계 및 구현하였다. 실시간 네트워크 트래픽 모니터링 시스템은 관리 효율과 분산 관리 기능을 제공하기 위하여 클라이언트 시스템과 분석 서버 시스템으로 구성되어진다. 클라이언트 시스템은 웹 상에서 사용자 인터페이스와 분석 결과를 명확하고 동적으로 나타내기 위한 그래프 기능을 제공하기 위해 JAVA와 웹 관련 기술로 구현되었다. 클라이언트는 사용자의 요구를 받아들이는 실시간 분석 기능, 수집 요구/중지 기능, 누적 분석 기능, MIB 브라우저 기능 등을 제공한다. 분석 서버는 클라이언트로부터 전송된 사용자 요구를 분석하여 처리하며, 그 결과를 클라이언트로 반환하는 역할을 수행한다. 따라서 분석 서버는 각각의 요구를 쓰레드를 통하여 동시에 처리할 수 있는 기능들로 구현되어져 있다.

본 논문에서 제시된 실시간 네트워크 트래픽 모니터링 시스템은 망 관리자의 관점에서 망의 품질과 상태를 진단하여 최적의 성능 제공과 장애 복구, 그리고 망 구성에 척도가 되는 관리 정보들을 제공한다. 따라서 제안된 시스템은 관리자가 관리하기 쉽지 않은 복잡한 LAN 상의 관리 행위를 효과적으로 수행할 수 있도록 도움을 줄 것이다.

참고문헌

[1] Nathan Kalowski, "Applying the RMON Standard to Switched Environments", International Journal of Network Management Vol.7, Wiley, 1997.

[2] William Stallings, "SNMP, SNMPv2 and RMON : Practical Network Management", Addison-Wesley Publishing Company, 1996.

[3] Gilbert Held, "LAN Management with SNMP and RMON", John Wildy & Sons Inc, 1996.

[4] Nathan J. Muller, "Web-accessible Network Management Tools", International Journal of Network Management Vol.7, Wiley, 1997.

[5] Wilco Kasteleijn, "Web based Management", M.Sc Thesis Univerity of Twente Department of Computer Science & Department of Electrical Engineering Tele-Informatics and Open System Group 13-20 63-65, 1997.

[6] Allan Leinwand, Karen Fang Conroy, "Network Management", Addison-Wesley Publishing Commpany, 1996

[7] Rechard E.Caruso, "Network Management : A Tutorial Overview", IEEE Comm. Magazine, March 1990.

[8] Allan Leinwand, "Accomplish Performance Management with SNMP", INET'93, 1993

[9] John Blommers, "Practical for Planning for Network Growth", Prentice Hall PTR, 1996

[10] Sang-Chul Shin, Seong Jin Ahn, Jin Wook Chung, "Design and Implementation of SNMP-based Performance Parameter Extraction System", APNOMS, 1997, 10.