논문 99-24-3B-9 한국통신학회논문지 '99-3 Vol.24 No.3B

LAN 관리를 위한 Web기반 가시화 시스템의 설계 및 구현

정회원 안 신 영*, 안 성 진*, 정 진 욱*

Design and Implementation of Web-based Visualization System for LAN Management

Shin-Young Ahn*, Seong-Jin Ahn*, Jin-Wook Chung* *Regular Members*

요 약

본 논문에서는 RMON MIB을 이용하여 LAN을 관리하기 위해 분석 파라미터를 정의하고 이를 분석하기 위한 Web 기반 가시화 시스템을 Java로 구현하였다. 가시화 시스템은 관리자로 하여금 LAN 세그먼트의 실시간 모니터링, 트래픽 정보의 수집, 수집된 트래픽 정보의 분석 등의 관리 행위를 수행할 수 있도록 클라이언트-서버 모델로 구현되었다. 가시화 클라이언트는 분석 결과를 관리자로 출력해주는 그래프 출력 모듈과 보고서를 작성해주는 보고 처리 모듈, 그리고 관리자로부터 요구를 입력 받아 서버로 요청하는 실시간 모니터링 모듈, 수집 요구 모듈, 분석 요구 모듈로 구성된다. 가시화 서버는 클라이언트의 요청을 처리하는 실시간 모니터링 처리 모듈과 수집 처리 모듈, 분석 처리 모듈, 보고 처리 모듈, 그리고 관리 정보를 저장하고 검색하기 위한 DB 처리 모듈로 구성된다. 가시화 서버와 클라이언트간의 관리 요구와 응답을 위해 MATP가 사용된다. 구현한 시스템을 통해 성균관대학교의 203.252.53.0 네트워크를 분석함으로써 시스템의 적용성을 입증하였다. 본 논문에서 제시한 시스템은 어느 곳에서나 Web 브라우저를 통해 LAN의 문제점을 발견하고 해결을 지원하여 효율적인 LAN 운영과 계획 그리고 진단을 지원할 수 있다.

ABSTRACT

In this paper, we have defined the analysis parameters for LAN management by using RMON MIB. To analyze these parameters, we have implemented Web-based visualization system by Java. This system has been implemented as a client-server model so that it can provide three management functions: the real-time monitoring of LAN segment, the collection of LAN traffic Information, the analysis of collected traffic information. Visualization client is composed of 5 modules. Graph module shows manager analysis results. Report generation module provides the reports of analysis results. Real-time monitoring module, collection request module, and analysis request module read the request from manager, and send request message to visualization server. Server consists of real-time monitoring processor, collecting processor, analysis processor, report processor and DB handler. MATP is used to communicate between client and server. We have proved the adaptability of Visualization System by analyzing single LAN segment, 203.252.53.0 network in Sung Kyun Kwan Univ. This system can support the effective LAN management, redesigning of LAN, and fault diagnosis through Web browser.

I. 서 론

컴퓨터 네트워크가 질적 양적으로 급격히 발전함

* 성균관대학교 전기전자 및 컴퓨터공학부(syahn@Songgang.skku.ac.kr)
논문번호 : 98233-0525, 접수일자 : 1998년 5월 25일

에 따라 TCP/IP를 기반으로 하는 인터넷 또한 놀랄 만한 발전을 이루었다. 인터넷의 발전과 함께 LAN 상에서도 인트라넷이라는 형태의 네트워크 기술이 급속히 발전하여 많은 회사, 학교 등에서 내부적으로 전자 우편 및 기본적인 문서 공유 등의 간단한 작업 분야에 사용되어 왔다. 그러나 Web 기술의 발달과 함께 인트라넷의 처리능력은 점차 확대되어 전자 폼에 의한 문서 작성, 스케줄 관리, 기업 데이터 베이스와의 연계, 전자 회의 등으로 확대 발전되고 있다. 이런 다양한 응용을 수용하기위해 LAN상에서의 안정적이고 효율적인 네트워크 관리가 필요하게 되었다.

LAN 관리는 LAN 세그먼트에 연결되어 있는 여러 호스트간의 트래픽을 모니터링하여 서비스의 중단 없이 효율적으로 통신 네트워크를 운용할 수 있도록 네트워크 자원의 감시 및 보고와 필요한 경우 제어를 수행하는 제반 활동을 의미한다[1]. 이를 위한 TCP/IP 네트워크의 관리 표준으로 SNMP가 제안되었으며 WAN을 관리하기 위해서는 MIB-II가, LAN 세그먼트의 관리를 위해서는 RMON(Remote Monitoring)이 사용되고 있다. RMON은 MIB-II를 보완하여 네트워크 관리자에게 LAN 세그먼트의 트래픽 정보를 제공하는 원격 모니터링 관리 정보 베이스(RMON MIB)를 정의한다. RMON을 통해 원격 LAN세그먼트의 트래픽 정보를 수집할 수 있으며 이런 정보들로부터 유용한 정보를 추출하여 LAN 관리 행위를 실현할 수 있다. LAN 관리는 특정 클라이언트 프로그램의 설치 없이도 원격지에서 관리가 이루어질 수 있도록 지원해야 하며 본 논문에서는 이를 위해 인터넷 서비스 중 가장 많이 사용되는 WWW(World Wide Web)와 관련 정보를 손쉽게 검색할 수 있도록 하는 하이퍼 텍스트 전송 프로토콜(HTTP) 기술을 이용하여 브라우저만 있으면 어느 곳에서도 관리 행위를 수행할 수 있도록 Web 기반의 가시화 시스템을 설계하고 구현하였다. 또한 Web상에서의 정보흐름을 동적으로 수행할 수 있도록 해주는 Java 기술을 접목하여 친숙한 관리 환경을 제공하고자 한다.

최근의 Web 기반 네트워크 관리 연구 동향으로 Web 서버의 트래픽 관리를 위한 관리자 시스템을 구현한 논문[2]이 있으며 논문[3]에서는 Web을 플랫폼으로 하는 여러 네트워크 관리 도구에 대해 논의하였으나 정적인 기능만을 제공하는 WAN관리를 위한 도구들이 대부분이어서 LAN을 분석하고 관리하기에는 부족함이 있다. 또한 라우터의 입출력 트래픽 데이터를 주기적으로 수집하여 트래픽 데이터를 GIF로 저장하고 이 GIF파일이 포함된 HTML형태로 트래픽 모니터링 결과를 출력하여 주는 MRTG(Multi Router Traffic Grapher)가 있다[4]. 그 외에도 N-Vision, IntraSpection, EnterprisePRO, HP NetMetrix/UX Reporter, ANACAPA SOFTWARE[5][6][7][8] 등의 Web 기반 네트워크 관리 제품이 있다.

Ⅱ. LAN 관리 구조 및 분석 파라미터

1. LAN 관리 구조

기존의 LAN분석은 LAN에 접속되어 있는 호스트에서 LAN 분석 프로그램을 구동하거나 세그먼트에 스니퍼 같은 분석기를 붙여서 분석하였다. 그래서 관리자가 각 세그먼트를 돌아다니면서 분석을 해야 했다. 그러나 RMON을 이용하면 그림 1과 같은 구조로 관리자가 네트워크 상의 어디에 있든 관리 행위를 수행할 수 있다[9][10].

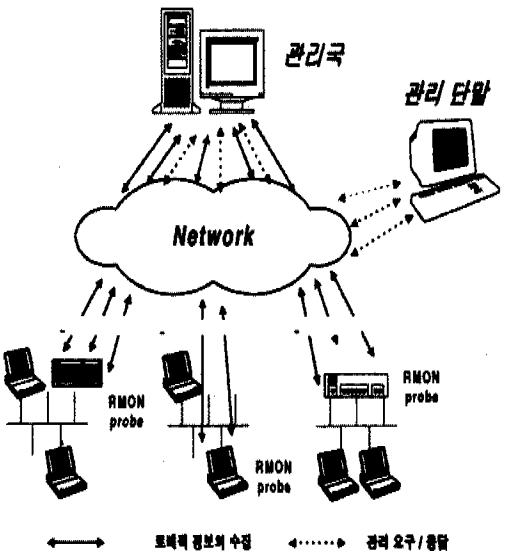


그림 1. LAN관리 구조
Fig. 1 The Architecture of LAN Management

RMON MIB을 이용하여 LAN을 관리하기 위한 기본 구조는 그림 1과 같이 원격지의 LAN 세그먼트상에 RMON probe가 탑재되어 있고 중앙의 관리국이 이런 probe로부터 각 세그먼트의 트래픽 정보 및 상태 정보를 수집하여 분석함으로써 이루어진다. 이때 각 RMON probe의 RMON MIB로부터 트래픽 정보를 수집하기 위해 사용되는 프로토콜이 SNMP이다 [11][12][13].

2. 분석 파라미터

(1) LAN 이용 현황

관리자에게 있어 가장 중요하게 보는 요인으로 이용률을 들 수 있다. 이용률은 LAN 세그먼트의 이용량을 백분율로 표시한 값으로 네트워크 대역폭의 확장 또는 분할 시기를 결정에 대한 지침을 제공한다. 패킷 크기별 분포는 LAN에 유통되는 패킷의 크기별 분포를 비교하여 분석한 것으로 사용되는 응용이 무엇인지 간접적으로 예측할 수 있다. 패킷 유형별 분포는 LAN에 유통되는 패킷의 유형별 분포를 비교 분석하는 항목으로 패킷 유형에는 유니캐스트, 멀티캐스트, 방송형의 세가지 가 있다. 만약 세그먼트상에 멀티캐스트 패킷이 많으면 이 세그먼트는 비효율적으로 동작한다고 볼 수 있다. 방송형 패킷의 갑작스러운 증가는 broadcast storm을 유발하여 네트워크 성능을 떨어뜨리는 원인이 된다. 이와 같이 LAN의 전반적인 사용현황을 파악하기 위한 지표로 LAN 이용 현황을 정의한다.

(2) LAN 건강도

세그먼트 상의 장애는 네트워크 성능에 영향을 미쳐 응답 시간을 지연시키며 처리율을 떨어뜨리고 혼잡을 발생시킨다. 그래서 세그먼트의 장애 상황을 파악하는 지표로 LAN건강도를 정의한다.

에러 패킷 원인별 분포는 세그먼트에 발생하는 에러 패킷들을 원인별로 비교 분석 한다. 에러의 원인별 분석은 세그먼트의 문제 해결에 도움을 줄뿐 아니라 네트워크 계획을 지원한다. 에러율은 세그먼트에 유통되는 전체 패킷에 대한 에러 패킷의 비율을 백분율로 표시한 값이다. 이 분석항목은 세그먼트의 질과 네트워크 성능을 저하시키는 장애 정도를 의미한다. Collision 율은 세그먼트에 유통되는 전체 패킷에 대한 충돌 패킷의 비율을 백분율로 표시한 값이다.

(3) 특정 호스트 분석

특정 호스트의 트래픽 특성을 파악하고자 할 경우나 LAN상에 장애가 있을 경우 그 원인이 되는 호스트를 확인하기위한 지표로 사용될 수 있다. 특히 특정 호스트 LAN이용률이나 특정 호스트 트래픽 점유율을 분석함으로써 특정 호스트가 얼마나 많은 트래픽을 생성하는지를 분석할 수 있다.

특정 호스트 LAN 이용률은 특정 호스트의 세그먼트 이용량을 백분율로 표시하며 특정 서버의 트래픽이 얼마나 많은지 또는 과도한 트래픽을 발생하는 호스트를 찾는데 유용하다. 호스트 입출력 바이트 비교는 특정 호스트의 입출력 바이트량을 비교함으로써 그 호스트의 트래픽 특성을 파악할 수 있다. 입력 바이트량보다 출력 바이트량이 많으면 그 호스트는 서버라고 가정할 수 있다. 호스트 입출력 패킷 비교는 특정 호스트의 입출력 패킷을 비교함으로써 그 호스트의 트래픽 특성을 파악할 수 있다. 특히 입력 패킷 수 보다 출력 패킷 수가 많으면 그 호스트는 서버라고 가정할 수 있다. 호스트 패킷 유형별 분포는 특정 호스트에 출력되는 패킷을 그 유형별(유니캐스트, 멀티 캐스트, 방송형)로 비교 분석한다. 호스트 출력 에러율은 특정 호스트의 출력 패킷 수에 대한 출력 에러 패킷수의 백분율로서 특정 호스트의 인터페이스의 장애 여부에 대한 지침을 제공한다. 특정 호스트 트래픽 점유율은 현재 세그먼트상의 전체 트래픽에 대한 특정 호스트의 트래픽 점유율이며 특정 호스트 LAN 이용률과 함께 서버의 트래픽이 얼마나 많은지를 분석할 수 있다.

(4) 호스트 순위별 분석

관리자 입장에서 LAN 세그먼트에서 트래픽을 가장 많이 출력하거나 수신하는 호스트를 식별한다거나 에러를 가장 많이 발생시키는 호스트를 확인하는 것은 LAN상의 장애나 구성 계획에 있어 지표로 사용될 수 있다.

분석 할 수 있는 항목은 입력 패킷 순위별 분석, 출력 패킷 순위별 분석, 입력 바이트 순위별 분석, 출력 바이트 순위별 분석, 방송형 패킷 순위별 분석, 멀티캐스트 패킷 순위별 분석, 출력 에러 패킷 순위별 분석이 있으며 각 항목별로 세그먼트 상위 N개 호스트들을 순위별로 분석한다.

(5) 호스트간 트래픽 분석

특정 호스트간에 트래픽 송수신량을 파악함으로써 어느 호스트간에 트래픽이 많이 발생되는지를 확인할 수 있으며 장애 원인 파악의 지표로도 사용될 수 있다. 분석할 수 있는 항목으로는 호스트간 패킷 분석, 호스트간 바이트 분석, 호스트간 에러 패킷 분석이 있다.

(6) 네트워크 프로토콜 분석

LAN상에서 가장 많이 사용되는 네트워크 계층 프로토콜을 분석함으로써 트래픽 경향을 파악할 수 있으며 장애가 발생시 가장 많이 발생하는 프로토

콜을 분석함으로써 문제 해결을 위한 지표로서도 유용하다. ARP, RARP, IP, IPX등 네트워크 레벨의 프로토콜을 분석함으로써 LAN 세그먼트서 사용되는 응용을 추측할 수 있다.

Ⅲ. 가시화 시스템의 설계 및 구현

1. 가시화 시스템 구조

그림 1에서 본 바와 같이 원격지의 LAN으로부터 트래픽 정보를 수집하고 분석하는 것은 관리국에 의해 이루어진다. 본 논문에서 구현한 Web 기반 가시화 시스템은 관리국의 LAN관리 정보 수집 및 분석 시스템에 의해 생성되는 관리 정보를 관리자가 어디에 있든지 검색할 수 있도록 하며 분석 결과를 다양한 그래프 및 표로 출력해준다.

가시화 시스템은 Web서버에 존재하는 가시화 서버와 관리 단말에 존재하는 가시화 클라이언트로 구성되며 시스템의 동작은 Web서버에 존재하는 HTML문서와 Java 바이트코드가 Web 연결에 의해 관리 단말로 전송되어 가시화 클라이언트로 동작한다. 가시화 클라이언트는 각 관리 요구별로 별개의 애플릿으로 구현되며 관리자가 관리 요구를 하면 이런 요구를 가시화 서버로 새로운 TCP연결을 통해 전송하고 그 응답을 받아 관리자에 출력해 준다. 이때 메시지를 송수신하기 위해 관리 응용 전송 프로토콜(MATP: Management Application Transfer Protocol)에서 정의된 메시지 형태가 사용된다.

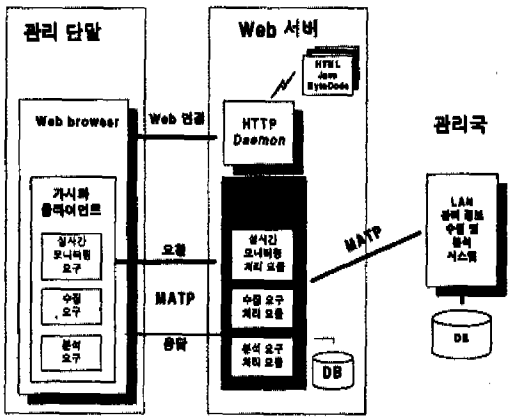


그림 2. LAN관리를 위한 가시화 시스템 전체 구조도
Fig. 2 The Architecture of Visualization System for LAN Management

가시화 서버는 네트워크상의 임의의 위치에 존재할 수 있는 가시화 클라이언트로부터의 관리 요구별로 분석된 관리 정보를 가시화 클라이언트로 송신한다. 가시화 서버는 가시화 클라이언트의 3가지 요구에 응답하며 필요에 따라 LAN 관리 정보 수집 및 분석 시스템과 연동하여 LAN 세그먼트의 트래픽 정보를 주기적으로 수집하고 분석하여 가시화 클라이언트로 응답하게 된다. 이 때 필요한 관련 정보를 데이터베이스에 저장하고 검색한다.

2. 가시화 클라이언트

2.1 구현 모델

먼저, 관리 단말상의 가시화 클라이언트는 Web 브라우저 상에서 구동하여 관리자의 관리 요청에 대한 사용자 인터페이스의 기능과 요청에 대한 응답을 수행하는 시스템으로 실시간 모니터링 모듈, 수집 요구 모듈, 분석 요구 모듈의 세 모듈과 가시화 서버로부터 수신한 트래픽 분석 결과를 출력해 주는 그래프 출력 모듈, 분석 결과를 보고를 위한 자료로 생성해 주는 리포트 요구 모듈로 구성된다. [그림 3]에 나타낸 바와 같이 가시화 클라이언트의 각 모듈의 기능 및 구성은 다음과 같다.

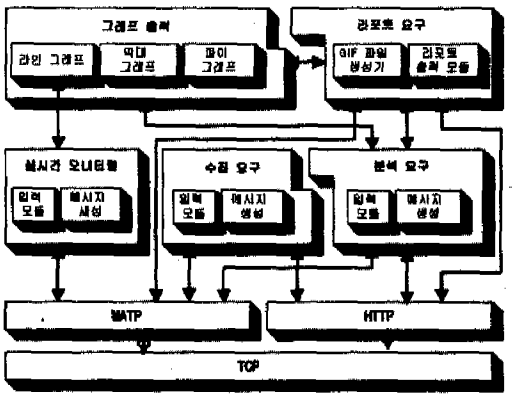


그림 3. 가시화 클라이언트의 구현 모델
Fig. 3 The Model of Visualization Client

1) 실시간 모니터링 모듈

관리자가 LAN의 현재 트래픽 상태를 분석하기 위한 요청을 입력 받고 분석 결과를 그래프 출력으로 관리자에게 보여주는 사용자 인터페이스이며 이를 위한 관리자 입력 데이터로 RMON probe의 IP 주소와 Community, 분석 항목, 모니터링 기간, 그리고 경우에 따라 세그먼트 스피드가 필요하다. 실시간 모니터링을 설계하고 구현할 때는 가시화 서버로의 연결 상태나 네트워크 다운 그리고 probe의 비동작 등을 관리자에 보고할 수 있도록 해야 한다.

다음은 실시간 모니터링을 할 수 있는 분석 파라미터이다.

표 1. 실시간 모니터링 분석 파라미터
Table 1. The Analysis Parameter for Real-time Monitoring

RMON 그룹	관리 파라미터
Statistics	이용률, 패킷 크기별 분포, 패킷 유형별 분포, Collistion율, 에러율, 에러 원인별 분석
Hosts	특정 호스트 LAN 이용률, 호스트 입출력 바이트 비교, 호스트 입출력 패킷 비교, 호스트 패킷 유형별 분포, 호스트 출력 에러율, 특정 호스트 트패픽 점유율
Filter	네트워크 프로토콜 분포

2) 수집 요구 모듈

네트워크 관리자가 장애 진단이나 성능 개선 또는 네트워크 계획을 위해 LAN의 트래픽 경향를 살펴보기 위해서는 일정 기간동안 트래픽 정보를 주기적으로 수집하도록 하는 수집 요구의 선행이 필요하며, 이 모듈은 이런 트래픽 데이터의 수집 요청을 위한 인터페이스의 기능을 수행한다. 수집 요구를 위해 Request ID, 피관리 세그먼트 목록 그리고 수집 기간과 수집 주기가 입력 데이터로 필요하다. 피관리 세그먼트 목록은 probe의 IP주소와 Community, 세그먼트 스피드, 표 2에서 명시한 수집 영역 등으로 구성된다. 수집 요구는 관리국의 파일 시스템에 트래픽 데이터를 저장하기 때문에 권한이 있는 사람만이 수집 요구를 할 수 있도록 사용자 인증 과정을 거쳐야 한다. RMON MIB로부터 정의한 관리 파라미터는 다음과 같은 5가지 수집 영역으로 나누며, 수집 요구시 각 수집 영역별로 관리 정보를 수집한다.

표 2. 수집 요구의 수집 영역
Table 2. The Domain for Collection Request

RMON 그룹	수집 영역
Statistics	LAN 통계
Hosts, Statistics	특정 호스트 분석
Hosts, HostTopN	호스트 순위별 분석
Matrix	호스트간 트래픽 분석
Filter, Capture	네트워크 프로토콜 분석

3) 분석 요구 모듈

수집 요구에 의해 수집된 트래픽 데이터의 분석 결과를 테이블과 그래프 형식으로 출력한다. 분석 요구를 위한 입력 데이터로는 Request ID, probe IP, 분석 영역, 분석 항목, 분석 기간 등이며 분석 요구는 수집 요구에서 수집을 요청한 수집 영역에 대해서만 응답이 가능하다. 분석 요구에서 분석 가능한 분석 파라미터가 표 3에 나타나 있다.

표 3. 분석 요구 파라미터
Table 3. The Parameter for Analysis Request

분석 영역	분석 파라미터
LAN 통계	이용률, 패킷 크기별 분포, 패킷 유형별 분포, Collision율, 에러율, 에러 원인별 분석
특정 호스트 분석	특정 호스트 LAN 이용률, 호스트 입출력 바이트 비교, 호스트 입출력 패킷 비교, 호스트 패킷 유형별 분포, 호스트 출력 에러율, 특정 호스트 트패픽 점유율
호스트 순위별 분석	입력 패킷 순위별 분석, 출력 패킷 순위별 분석, 입력 바이트 순위별 분석, 출력 바이트 순위별 분석, 방송형 패킷 순위별 분석, 멀티캐스트 패킷 순위별 분석, 출력 에러 패킷 순위별 분석
호스트간 트래픽 분석	호스트간 패킷 분석, 호스트간 바이트 분석, 호스트간 에러 패킷 분석
네트워크 프로토콜 분석	네트워크 프로토콜 분포

4) 그래프 출력 모듈

실시간 모니터링 요구와 분석 요구에 의한 분석 결과를 그래프로 표현하여 관리자에게 출력해준다. 그림 3에 나타낸 바와 같이 그래프 출력 모듈은 그래프 형태에 따른 3개의 소모듈로 구성된다. 분석 결과의 출력은 시간 추이 분석, 일간 주기로 분석, 주간 주기로 분석, 월간 주기로 분석, 총괄 분석, 그리고 종합 분석의 6가지 모드로 분석할 수 있다. 그래프의 형태는 라인 그래프, 막대 그래프, 파이 그래프의 세가지 형태이며 종합 분석 모드는 표 형태로 출력된다.

5) 리포트 요구 처리 모듈

그래프 출력 모듈의 출력 그래프로부터 보고를 위한 자료를 생성해 준다. Java 그래프는 직접 프린트할 수 없기 때문에 이 기능을 제공하여 프린트도 가능하게 하였다. 그래프는 GIF파일 생성기에 의해 GIF 파일로 바뀌어 가시화 서버로 보내져 HTML/GIF 캐쉬에 저장되고 리포트 출력 모듈이 HTTP를 이용하여 리포트 파일을 전송 받아 관리자에게 출력해 준다.

2.2 구현

그림 4에는 가시화 클라이언트를 구성하는 클래스들의 구조가 나타나 있다. 가시화 클라이언트의 RealClient, CollectClient, AnalysisClient와 관련 클래스는 개별적인 사용자 화면을 가지고 있으며 GraphIt과 ReportProcessor는 공통적으로 사용된다.

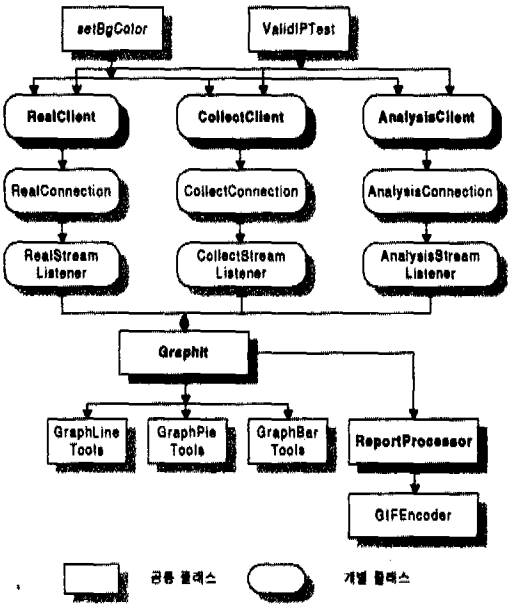


그림 4. 가시화 클라이언트의 클래스 다이어그램
Fig. 4 The Class Diagram of Visualization Client System

RealClient는 실시간 모니터링 요구를 위한 입력 화면과 사용자의 요구를 읽어 서버로의 요구 메시지를 생성하고 RealConnection를 호출하여 가시화 서버로 연결을 설정하고 요구 메시지를 전송한다. RealStreamListener는 서버로부터 응답을 받아 그래프 출력 모듈인 GraphIt을 호출하여 그래프를 출력한다.

CollectClient는 수집 요구를 위한 입력 화면과 사용자의 요구를 읽어 서버로의 수집 요구 메시지를 생성하며 CollectConnection를 호출하여 서버로 연결을 설정하고 요구 메시지를 전송한다. CollectStreamListener는 가시화 서버로부터 응답을 받아 상태 창에 수집 성공 / 실패를 알린다.

AnalysisClient는 분석 요구를 위한 입력화면으로 기존의 수집 정보로부터 분석 가능한 피관리 세그먼트에 대한 정보(분석 영역, 분석 항목, 분석 기간, 분석 모드)를 출력해주고, 사용자가 입력한 분석 요구에 대한 메시지를 생성하여 AnalysisConnection를 호출하여 서버로 전송한다. AnalysisStreamListener는 가시화 서버로부터의 응답을 기다리며, 분석 데이터를 받아 그래프 출력 모듈인 GraphIt을 호출하여 그래프를 그리도록 한다.

SetBgColor는 애플릿의 배경색을 지정하며 ValidIPTest는 각 사용자 입력에서 IP주소의 유효성을 평가한다. GraphIt은 각 요구로부터 호출되는 그래프 출력 모듈로 새로운 프레임을 생성하고 라인 그래프를 그리는 GraphLineTools, 파이 그래프를 그려주는 GraphPieTools, 막대 그래프를 그려주는 GraphBarTools을 호출하여 새로 생성된 프레임에 그래프를 그린다. 또한 "REPORT"버튼을 가지고 있어 리포트 요구를 위해 ReportProcessor를 호출하여 출력 그래프에 대한 리포트를 생성하여 출력해준다. 이 클래스는 그래프를 GIF로 저장하기 위해 GIFEncoder 클래스를 호출하여 GIF이미지를 생성한 후 가시화 서버로 전송하고 가시화 서버상에 생성된 리포트를 읽어오는 기능을 한다.

3. 가시화 서버

3.1 구현 모델

가시화 서버의 구성은 [그림 5]와 같으며 가시화 클라이언트의 요구에 대응하기 위해 특정 포트에 대한 서비스를 제공하는 데몬(daemon) 프로세스로 구현된다.

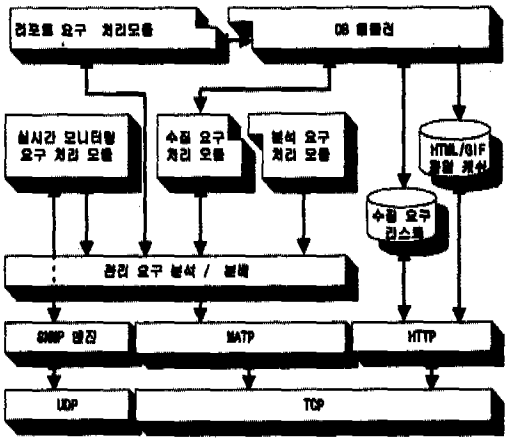


그림 5. 가시화 서버의 전체 구현 모델
Fig. 5 The Model of Visualization Server

가시화 서버는 실시간 모니터링 요구 처리 모듈, 수집 요구 처리 모듈, 분석 요구 처리 모듈 그리고 리포트 요구 처리 모듈, 관리 요구 분석/분배 모듈,

DB 핸들러 모듈로 구성된다. 관리 요구 분석/분배 모듈은 가시화 클라이언트로부터 관리 요구를 수신할 경우 그 요구 메시지를 해석하여 4개의 처리 모듈 중 하나를 호출하여 요구에 대한 응답을 수행하도록 한다. 4개의 처리 모듈은 Java 쓰레드로서 동시에 다수개의 요구를 처리할 수 있다. DB핸들러 모듈은 수집 요구 관련 정보 리스트와 임시 생성되는 HTML/GIF 파일을 저장하고 관리하는 모듈이다.

다음은 4개의 처리 모듈에 대한 설명이다.

1) 실시간 모니터링 요구 처리 모듈

RMON probe로 하여금 LAN 트래픽 데이터를 수집하도록 snmpset을 수행한 후, snmpget명령으로 RMON probe를 폴링한다. 모든 변화 추이는 단위 시간당 변화량이므로 [N]번째 폴링 데이터에서 [N-1]번째 폴링 데이터를 빼서 두 폴링간의 시간 간격으로 나누면 단위 시간당 변화량을 구할 수 있다. 모든 분석 데이터는 초단위로 계산되며 가시화 서버에서 인터페이스로 분석 데이터가 전송되면 인터페이스에서 서버로 ACK를 주는 형태의 흐름제어 기법을 이용한다.

2) 수집 요구 처리 모듈

수집 요구 처리 모듈은LAN관리 정보 수집 및 분석 시스템으로 피관리 세그먼트의 트래픽 데이터를 수집하도록 요청한다. LAN관리 정보 수집 및 분석 시스템이 RMON probe 설정을 성공하고 수집이 시작되면 가시화 서버로 수집 성공을 알리고 가시화 서버는 수집 요구 정보를 DB 핸들러 모듈을 통해 파일 시스템에 저장한다. 그리고 가시화 클라이언트로 수집 요구 성공 메시지를 전송한다.

3) 분석 요구 처리 모듈

분석 요구 처리 모듈은 LAN관리 정보 수집 및 분석 시스템에게 누적된 데이터를 분석하여 성능 및 장애 정보를 반환하도록 요청한다. 가시화 서버는 분석 데이터를 직접 가시화 클라이언트로 전송하거나 DB 핸들러를 구동하여 테이블 형태의 HTML문서를 작성하여 그 파일명만 가시화 클라이언트로 전송한다. 가시화 클라이언트가 가시화 서버로부터 분석 정보를 받으면 직접 그래프를 그리거나 HTML문서를 HTTP를 이용해 전송 받아서 관리자에게 출력한다.

4) 리포트 요구 처리 모듈

리포트 요구는 Java 애플릿의 직접 프린트 불가능한 단점을 보완하고 보고를 위한 문서를 작성하기 위한 기능이다. 그리고 모든 분석 결과를 저장할 수 있도록 한다. 가시화 클라이언트로부터 그래프의 이미지 데이터를 수신하여 파일에 저장하고 HTML 문서로 보고서를 작성하여 그 파일명을 가시화 클라이언트로 반환한다. 그러면 가시화 인터페이스는 HTML문서를 전송 받아서 관리자에게 출력한다.

3.2 구현

가시화 서버는 다중 요구를 동시에 처리할 수 있어야 하기 때문에 쓰레드로 구현된다. 그림 6은 구현 클래스를 나타낸다. Server는 Thread를 상속한 클래스로 루프를 돌면서 가시화 클라이언트로부터의 요구를 수신한다. Server 클래스에서 매번 요구를 수신할 때 마다 그 TCP연결을 관리하는 Thread로 동작하는 Connection클래스를 호출한다. 이 Connection 클래스는 하나의 관리 요구에 대한 연결을 유지하면서 Sender클래스를 호출하여 요구 메시지를 분석하고 적절한 처리 프로세스를 호출한다. 실시간 모니터링 요구일 경우에는 RealProcess를, 수집 요구이면 CollectProcess를, 분석 요구이면 AnalysisProcess를, 마지막으로 리포트 요구는 Report Process를 생성하여 호출한다.

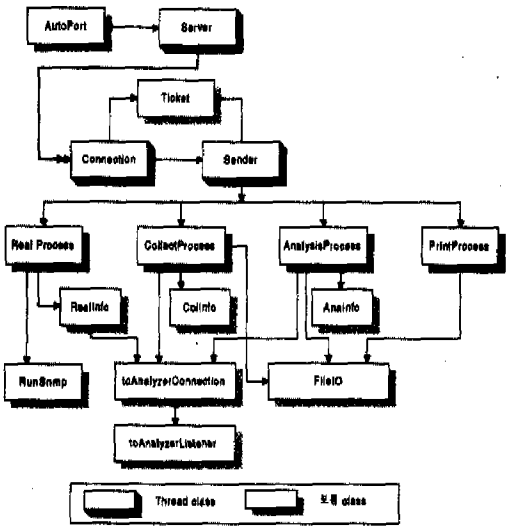


그림 6. 가시화 서버의 클래스 다이어그램
Fig. 6 The Class Diagram of Visualization Server

AutoPort 클래스는 서버가 사용하는 포트를 동적으로 할당하여 디스크에 저장하며, 가시화 가시화 클라이언트는 HTTP로 이 포트를 자동적으로 읽어 서버로 접속한다. Ticket은 메시지를 수신하고 그 응답을 보내는 TCP 소켓을 관리하는 두 쓰레드인 Connection과 Sender간의 TCP 연결에 대한 동기를 맞추기 위해 두 쓰레드 중 하나만 연결을 핸들링하

도록 하기위한 클래스이다.

RealProcess는 실시간 요구를 처리하는 클래스로 RealInfo 클래스를 호출하여 실시간 요구 메시지를 분석하여 RMON Probe를 설정하고 RunSnmp를 호출하여 probe를 연속적으로 폴링을 하여 실시간 트래픽을 분석하여 가시화 클라이언트로 응답한다. CollectProcess는 수집 요구를 처리하는 클래스로 ColInfo클래스를 호출하여 요구 메시지를 분석하고 LAN 관리 정보 수집 및 분석 시스템으로 수집 기간 동안 LAN상의 트래픽을 수집하도록 요청한다. AnalysisProcess는 분석 요구를 처리하는 클래스로 AnaInfo 클래스를 호출하여 요구 메시지를 분석하고 LAN 트래픽 분석 시스템으로 누적 트래픽 데이터에 대한 분석 요청한다. ReportProcess는 가시화 클라이언트의 리포트 요구를 처리한다. GIF 이미지를 수신하여 리포트를 작성하고 그 리포트의 파일명을 가시화 클라이언트로 전송한다.

toAnalyzerConnection는 LAN 관리 정보 수집 및 분석 시스템으로의 연결을 설정하며 toAnalyzerListener 클래스는 LAN 분석 시스템으로부터 응답을 수신한다. FileIO 클래스는 수집 정보 저장 및 리포트 파일 생성등에 관련된 파일 입출력을 담당한다.

4. 클라이언트와 서버간의 통신

이미 설명된 바와 같이 가시화 시스템은 가시화 클라이언트와 가시화 서버 그리고 LAN 관리 정보 수집 및 분석 시스템간의 통신이 필요하며 각 관리 요구와 응답에 관련된 메시지 교환 절차를 MATP(Management Application Transfer Protocol)라 명명하여 정의한다.

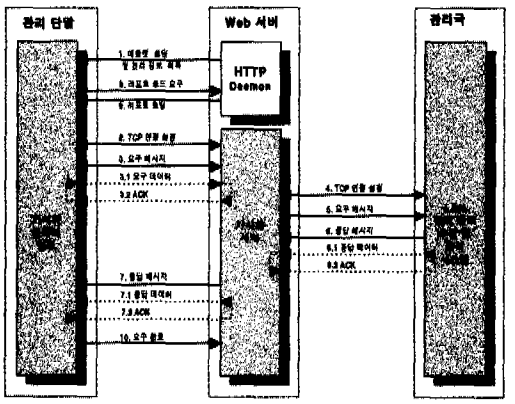


그림 7. MATP의 통신 절차
Fig. 7 The communication procedure of MATP

4.1 메시지 교환 절차

관리자의 관리 단말상의 가시화 클라이언트는 Web 서버로부터 애플릿이 로드 되어 동작하며, 관리자의 관리 요구시 서버로 TCP연결을 설정하고 요구 메시지를 전송한다. 이 때 요구 메시지와 함께 요구 데이터가 서버로 전송될 수 있으며 서버는 ACK를 전송함으로써 수신을 확인한다. 클라이언트로부터 요구를 수신한 서버는 LAN 관리 정보 수집 및 분석 시스템과 TCP 연결을 맺고 요구 메시지를 전송하고 그 응답을 수신한다. 이때 응답 데이터가 있을 경우 ACK를 반환하여 수신을 확인한다. 이렇게 처리된 요구의 결과(요구의 성공 및 실패 여부, 관리 데이터)를 클라이언트로 응답 메시지를 이용하여 반환한다. 클라이언트의 요구가 보고서 생성 요구였으면 HTTP를 이용하여 보고서 파일을 읽어다 출력해주며 서버와의 연결을 해제하도록 요구 완료 메시지를 서버로 전송한다.

4.2 메시지 정의

메시지 타입은 사용자가 가시화 서버로의 관리 요구를 구분하는 필드이며 세부 타입은 각 메시지 타입별로 세부 적인 요청을 식별하기 위한 필드이다. 요구 ID는 사용자가 각 관리 요구를 식별하기 위한 ID이며 시작 시간과 종료 시간은 수집 요구시에는 수집 기간을 명시하고 분석 요구시에는 분석 기간을 명시한다. 이 필드는 년, 월, 일, 시, 분의 세부 필드로 구성된다. 주기는 수집 요구시 폴링의 빈도를 나타내며 모드는 실시간 모니터링 요구에서 모니터링 기간을 폴링 횟수인지 폴링 기간인지를 식별하는 필드이다.

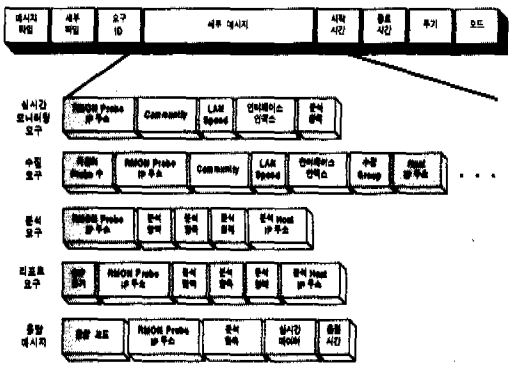


그림 8. 가시화 서버와 가시화 클라이언트 사이의 MATP 메시지 형식 정의
Fig. 8 The MATP message format for communication between visualization client and server

그림 8에는 이러한 MATP의 메시지 형식을 정의하였으며 표 4에는 각 필드에 사용되도록 정의된 값을 나타낸다.

표 4. MATP 각 메시지 필드의 사용되는 값 정의
Table 4. The Definition of Field Value for MATP Message

필드	항목	값
메시지 타입	실시간 모니터링 요구 메시지	1
	실시간 응답 메시지	2
	수집 요구 메시지	3
	수집 요구 응답 메시지	4
	분석 요구 메시지	5
	분석 요구 응답 메시지	6
	보고 요구 메시지	7
	보고 요구 응답 메시지	8
세부 타입	수집 추가 / 실시간 / 분석 / 보고	1
	수집 삭제	2
	수집 중지	3
모드	종합 분석 / 실시간 / 수집 / 보고	1
	시간대별 추이 분석	2
	일간 분석	3
	주간 분석	4
	월간 분석	5
	비교 분석	6

Ⅳ. 클라이언트 화면 구조와 실험 및 고찰

1. 화면 구조

그림 9은 LAN관리를 위한 가시화 시스템의 화면 구성이다. LAN 관리를 위한 가시화 시스템 초기 화면을 보면 좌측에 메뉴로 실시간 분석, 수집 요구, 분석 보고의 세 버튼이 있음을 볼 수 있다. 각 관리 요구로의 링크는 마우스로 이 세 버튼을 클릭함으로 써 이루어지며, 우측의 프레임에 세부 메뉴와 Java 애플릿이 사용자 화면으로 나타나다. 실시간 분석은 세부 메뉴로 LAN 이용 현황 분석, LAN Health 분석, 특정 호스트 현황 분석, 네트워크 프로토콜 분석으로 분류되어 있다. 분석 보고는 종합 분석과 심화 분석의 두가지 세부 메뉴로 구성되는데, 종합 분석은 피관리 세그먼트의 이용률과 에러율, 그리고 Collision 율을 표 형태로 보여주며 심화분석은 피관리 세그먼트에 대해 좀더 자세한 분석 결과를 그래프와 표준 출력해준다. 본 논문에서 제시한 가시화 시스템은 Java를 지원하는 모든 Web 브라우저에서 동작할 수 있으며 쉬운 사용자 인터페이스를 제공한다.

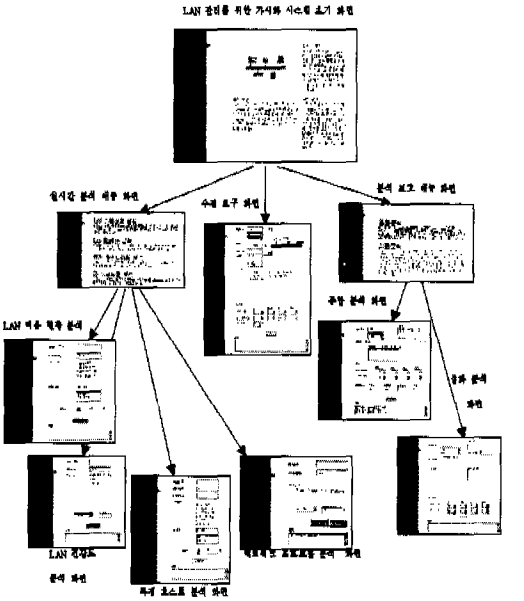


그림 9. LAN관리를 위한 가시화 시스템의 화면 구성
Fig. 9 The Structure of Request Views for Visualization System

그림 10은 가시화 클라이언트의 수집 요구 화면이다. 좌측의 수집 요구 버튼을 클릭하면 우측에 화면이 출력된다. 수집 요구를 하려면 먼저 Request ID를 입력하고 피관리 시스템 목록을 작성한 후 수집 기간과 폴링 주기를 설정한 다음 "수집 요구" 버튼을 누르면 된다. 이때 상태 창에 수집 요구가 성공했는지 실패했는지가 출력된다. 피관리 시스템 목록은 앞서 설명한 피관리 세그먼트 목록과 같은 의미이다. 특정 세그먼트를 분석하려면 그 세그먼트에 탑재되어 있는 RMON 장비를 관리하기 때문에 특정 RMON장비에 대해 필요한 파라미터를 입력하여 목록을 작성한다. 목록 작성 순서는 다음과 같다. 첫째, RMON IP 주소를 입력한다. 둘째, RMON probe의 Community를 입력한다. 셋째, LAN 스피드를 입력하고 5개의 수집 영역중 수집하고자 하는 영역을 체크한다. 이때 특정 호스트나 호스트간 트래픽 분석의 경우에는 추가적으로 분석하고자 하는 특정 호스트의 IP주소를 입력한다. 마지

막으로 "추가(>>)"버튼을 누르면 된다. 또 다른 세그먼트를 같은 Request ID로 요구하려면 위의 과정을 반복하면 된다.

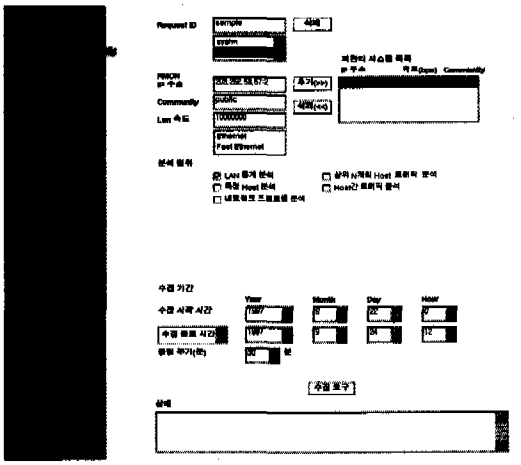


그림 10. 가시화 클라이언트의 수집 요구 화면
Fig. 10 The Collection Request View of Visualization Client

2. 실험 및 결과

2.1 실험 환경

가시화 시스템을 이용하여 성균관대학교 정보공학과의 203.252.53 LAN 세그먼트를 분석하였다. 203.252.53 네트워크에는 약 160여 개의 호스트가 연결되어 있다. 10 Mbps Ethernet LAN이다.

(1) 분석 네트워크 : 단일 LAN 세그먼트 (203.252.53.0)
(2) 폴링 주기 : 30 분 (crontab을 이용하여 주기적으로 트래픽 정보를 수집)
(3) 수집 기간 : 97년 10월 16일 ~ 97년 10월 31일
(4) RMON 허브 : 모델은 Bay Stack SA NMM (HUB의 IP : 203.252.53.57), probe의 RAM 크기는 2 Mbytes이고 RMON MIB의 9 Group을 지원

2.2 실험 결과

다음 그림 11은 203.252.53세그먼트의 LAN 사용률을 실시간 모니터링한 결과이다. X축은 시/분/초로 표현되는 시간이며 Y축은 백분율로 표시되는 이용률이다. X축을 살펴 보면 15시 19분 23초부터 21분 37초까지 모니터링한 것임을 알 수 있으며 붉은색 선이 나타내는 것은 평균 LAN 사용률이며 분석 당시 7.35%정도였다.

LAN 사용률은 관리자의 입장에서 관리를 위한 가장 중요한 성능 파라미터이다. 일반적으로 LAN 세그먼트의 사용률이 40%를 넘으면 그 세그먼트를 분할하던가 업그레이드할 필요가 있다. LAN 세그먼트 상에서 작업 중에 갑자기 응답 시간이 길어진다면 그 때 LAN 사용률을 분석함으로써 그 원인을 파악할 수 있다.

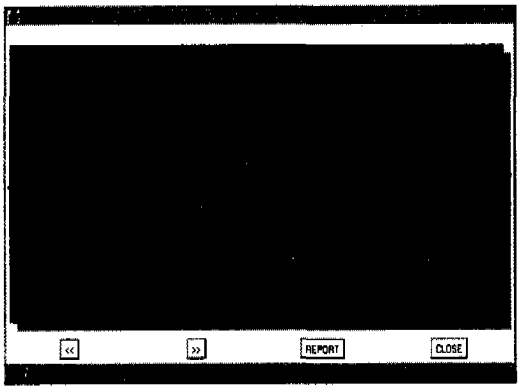


그림 11. LAN 이용률의 실시간 모니터링 결과
Fig. 11 The Real-time Monitoring Result of LAN Utilization

또한, 그림 11는 203.252.53 네트워크의 에러 원인별 분포에 대한 분석 결과를 보여준다.. 에러를 원인별로 분석함으로 써 네트워크의 장애 원인 판단에 도움을 줄 수 있다. 그림 12의 우측 상단에는 각 에러에 대한 인덱스가 나온다. 그림에서 보는 바와 같이 Fragment로 인한 에러가 가장 많음을 통해 패킷 충돌로 인해 패킷 에러가 가장 많이 발생함을 짐작할 수 있다.

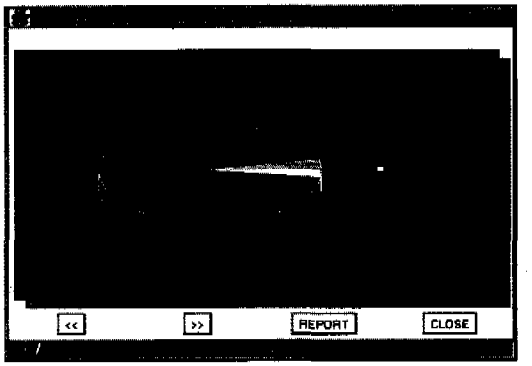


그림 12. 에러 원인별 분포의 분석 결과
Fig. 12 The Analysis Result of Error Factor Distribution

그림 13은 특정 호스트의 입출력 패킷을 비교 분석한 결과이다. X축은 시간을 의미하며 Y축은 초당 패킷 수이다. X축을 보면 알 수 있듯이 분석 기간에 대하여 하루를 주기로 매 시간의 입출력 비교를 수행한 결과임을 알 수 있다. 특정 호스트의 입출력을 분석함으로 써 그 호스트가 서버로 동작하는지를 파악할 수 있을 뿐 아니라 가장 트래픽이 많이 발생하는 시간을 피해서 작업을 할 수 있는 등 여러 가지로 활용할 수 있다.

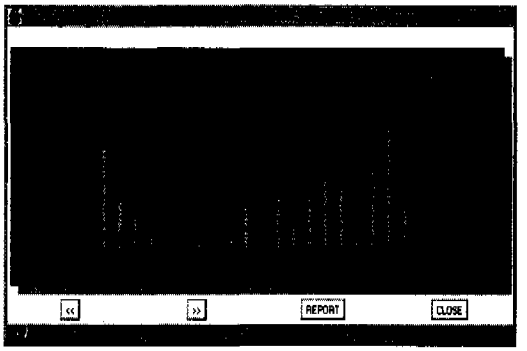


그림 13. 호스트 입출력 패킷 비교의 분석 결과
Fig. 13 The Analysis Result of Host input/output Packets Comparison

V. 결 론

본 논문에서는 LAN 트래픽을 모니터링하여 그 성능 및 장애를 분석함으로써 네트워크의 설계 및 확장 그리고 진단을 지원하는 LAN 분석 시스템을 위한 가시화 시스템을 설계하고 구현하였다. 이를 위해 먼저 LAN을 관리하기 위한 분석 파라미터를 정의하였으며 이를 기반으로 하여 실시간 모니터링 요구, 수집 요구, 분석 요구 등의 관리 요구를 위한 클라이언트 시스템과 서버 시스템을 설계 구현하였다. 클라이언트 시스템은 네트워크 상의 임의의 호스트에 존재할 수 있도록 Web 기반의 가시화 인터페이스로 구현하였으며 서버 시스템은 관리국에 Daemon으로 동작하면서 클라이언트 시스템으로부터의 요청을 처리하도록 하였다.

클라이언트 상의 관리자는 실시간 모니터링 요구를 함으로써 현재의 변화하는 트래픽 추이를 분석할 수 있으며 수집 요구와 분석 요구를 통해 특정 기간동안 트래픽 정보를 수집하여 그 누적된 데이터를 분석함으로써 네트워크의 트래픽 경향을 파악하고 장애를 진단할 수 있을 뿐 아니라 네트워크의 확장 시기를 예측할 수 있다. 또한 보고 요구를 구현하여 분석 결과를 상위의 관리자에게 보고할 수 있도록 보고서를 작성해 주는 기능을 구현하였다. 또한 구현된 시스템을 이용하여 성균관대학교의 203.252.53.0 단일 LAN 세그먼트를 분석하여 구현된 시스템의 적용성을 검증하였다.

본 논문에서 구현한 Web 기반 가시화 시스템은 관리 행위에 대한 활용 방안을 기반으로 하는 사용자 인터페이스를 제공하는 것으로 RMON probe를 이용하기 때문에 원격 LAN의 트래픽을 추출하여 그 흐름을 분석할 수 있으며, Java와 Web기술을 이용해 구현하였으므로 다른 관리 시스템에 비해 사용 방법이 쉽고 사용자 인터페이스가 Web 브라우저이므로 클라이언트 시스템의 설치가 필요 없다.

또한 관리자가 네트워크에 접속한 Web 브라우저만 있으면 어디에서라도 이러한 분석 정보를 요구하거나 수집 요구를 할 수 있으며 RMON MIB으로부터 분석 파라미터를 추출하였기 때문에 MIB-II에서 제공하지 못하는 여러 가지 분석 항목들을 이용하여 LAN 장애 등의 진단 및 확장에 대한 지원을 할 수 있어 네트워크를 보다 효율적으로 관리하도록 도움을 줄 것이다.

참 고 문 헌

[1] 최영수,안성진,정진욱,최흥진,변옥환, "TCP/IP 네트워크 관리에서 동시폴링과 순차폴링 트래픽의 특성 분석", 한국 정보처리 학회 '95년 추계 학술 발표 논문집 제 2권 2호, pp 548-552, 1995.

[2] 한정수,안성진,정진욱,박형우, "Web 응용 서비스 관리를 위한 성능 관리자 시스템의 설계 및 구현", 정보 처리 논문지 제 5권 제 1호, pp 161-171, 1998

[3] Nathan J. Muller, "Web-accessible Network Management Tools", International Journal of Network Management Volume7 , WILEY, pp 288-297, 1997

[4] http://www.ee.ethz.ch/stats/mrtg/ The Multi Router Traffic Grapher

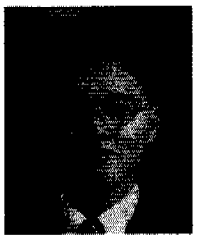
[5] http://199.0.203.52/epro/guided/tutorial/user_homepage.htm EnterpisePro User Home Page

[6] http://www.intraspection.com/Products/isspec.htm IntraSpection

[7] http://www.edge-technologies.com/EDGE/Nvision/synopsis.htm

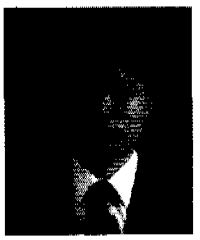
[8] http://www.anacapa.com
[9] 박철진, "SNMP MIB-II 기반의 성능 관리를 위한 Web Visualization 시스템의 설계 및 구현", 성균관대학교 정보통신공학 석사 졸업 논문, 1998
[10] H. J. Kang, J. W. Kim, S. J. Ahn, J. W. Chung, "A Circular Management Data Gathering Protocol for Efficient Network Management System", The 9th International Conference on Information Networking, 1994.
[11] William Stallings, "SNMP, SNMPv2 and RMON", Addison-Wesley Publishing Company, 1996
[12] RFC 1757 Remote Network Monitoring Management Information Base. S.Waldbusser. February 1995. (Obsoletes RFC1271) (Status: DRAFT STANDARD)
[13] Nathan J, Muller "SNMP's Remote Monitoring MIB", International Journal of Network Management Volume6 number 1, WILEY, pp 17-32, 1996

안 신 영(Shin-Young Ahn) 정회원



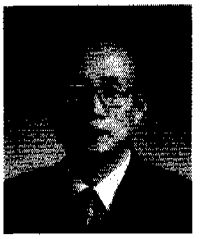
1997년 : 성균관대학교 정보공학과 졸업(공학사)
1999년 : 성균관대학교 전기전자 및 컴퓨터공학부 졸업(공학석사)
1999년~현재 : 전자통신연구원 슈퍼컴퓨터센터 위촉연구원
<주관심분야> 컴퓨터네트워크, 네트워크 관리, 초고속통신망

안 성 진(Seong-Jin Ahn) 정회원



1988년 : 성균관대학교 정보공학과(공학사)
1990년 : 성균관대학교대학원 정보공학과(공학석사)
1998년 8월 : 성균관대학교대학원 정보공학과(공학박사)
1990년~1995년 : 시스템공학연구소 연구원
1999년~현재 : 성균관대학교 컴퓨터 교육과 전임강사
<주관심 분야> 망관리, 분산시스템, 트래픽예측

정 진 욱(Jin-Wook Chung) 정회원



1974년 : 성균관대학교 전자공학과(공학과)
1979년 : 성균관대학교 전자공학과(공학석사)
1991년 : 서울대학교 계산통계학과(공학박사)
1982년~1985년 : 한국과학기술연구소 실장
1981년~1982년 : Racal Milgo Co.객원연구원
1985년~현재 : 성균관대학교 정보공학과 교수
<주관심 분야> 네트워크 관리, 네트워크 보안, 고속 및 무선통신 프로토콜