2000 년 한국정보처리학회 추계 학술발표논문집 제 7 권 제 2 호

웹 기반 네트워크 트래픽 분석 시스템

최재원, 전환식, 배진호, 송용주, 배진우, 김태수, 이광휘
창원대학교 전자계산학과
e-mail : jwchoi@cdcs.changwon.ac.kr

Web-Based Network Traffic Analysis System

JW-Choi, WS-Chun, JH-Bae, YJ-Song, JW-Bae, TS-Kim, KH-Lee
Dept. of Computer Science, Changwon National University

요 약

본 논문에서는 네트워크 트래픽 분석은 물론 자원을 관리하고 서버 및 특정 서비스에 대한 분석 자료를 제공하는 통합 시스템을 자바 언어로 구현하였다. SNMP 지원 모듈과 TCPdump 모듈, 그리고 시스템 관리 명령 모듈 등을 이용하여 구성 관리, 성능 관리, 장애 관리 및 시스템 자원 관리와 같은 상세 정보의 제공과 함께 다양한 자료 수집과 통계 분석을 통해 상세 보고서를 생성한다. 뿐만 아니라, 관리 대상 범위를 도메인 별로 구분하여 자료 수집을 독립시킴으로써 관리를 위한 트래픽이 전체 네트워크에 영향을 미치지 않도록 설계하였고, 실시간 모니터링은 물론 DB 에 최소화된 자료를 유지함으로써 네트워크 및 시스템에 대한 영속적인 관리 및 통계가 가능하도록 하여 운영의 항구성과 안정성, 분석의 정확성과 일치성, 사용의 편의성과 효용성을 제공하고자 하였다.

1. 서론

오늘날 정보 사회의 고도화로 인해 컴퓨터가 널리 보급되고 있으며, 정보 공유라는 마인드의 확산과 더불어 인터넷 및 네트워크의 사용이 급격히 증가하고 있다. 또한, 사용자의 요구를 충족시키기 위한 다양한 서비스의 제공을 통해 네트워크의 사용량과 그 활용 분야는 더욱 광범위해지고 있다. 이는 네트워크 및 시스템의 무분별한 사용을 방지하고 좀 더 효율적으로 자원을 관리해야 할 필요성을 야기시킨다[1].

초기의 네트워크 관리 시스템은 ping, traceroute, netstat 등의 기본 명령어를 이용하여 간단하게 네트워크의 구성이나 상황을 확인하는 수준이어서 사실상 전체적인 관리가 이루어지지 않았다. 또한, 특정 장비의 벤더들에 의해 몇몇 관리 툴이 제공되기는 했지만, 이 또한 개별 장비를 위주로 한 것이어서 통합된 네트워크 관리 수단으로는 활용되지 못했다[2]. 1980 년대 말 IETF(Internet Engineering Task Force)에서는 SNMP(Simple Network Management Protocol)라고 하는 단순 망 관리 프로토콜을 제안하였는데, 현재 인터넷을 기반으로 한 대부분의 네트워크 관리는 SNMP 를 이용하여 특정 장비의 MIB(Management Information Base) 값을 보여주거나, 이를 단순히 분석하는 수준에 그치고 있다[3]. 즉, 현재까지 연구 개발된 네트워크 관리 시스템들은 장비 자체나 트래픽 분석에만 치우치고 있고 사용하기 어려우며 통합된 환경을 제공하지 못한다는 단점이 있다.

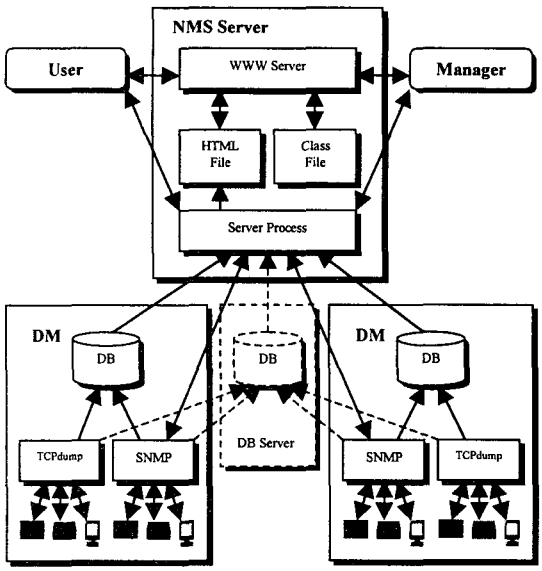
위의 필요성을 충족시키고 언급된 단점들을 보완하기 위해서는 자바라는 개발 언어를 이용하여 어플리케이션과 더불어 웹 인터페이스를 제공함으로써 운용의 독립성과 사용의 편의성을 도모하는 것이 유용하다[4, 5]. 그리고, SNMP 를 지원하는 장비와 그렇지 않는 장비에 대한 통합 관리와 더불어 실시간 모니터링은 물론 누적된 데이터를 활용하여 통계 자료를 제공할 수 있는 방법도 모색되어야 할 것이다. 또한, 네트워크 트래픽의 분석에 치우진 관리 방법에서 벗어나 특정 서버 혹은 제공하는 서비스에 대한 분석을 수행하고 네트워크 및 시스템의 새로운 정책 수립을 위한 기초 자료를 제공할 수 있어야 한다.

본 논문에서는 이러한 통합 관리 시스템을 설계하고 실제 구현된 사례를 보임으로써 효과적인 네트워크 및 시스템 관리를 위한 방법을 제시하고자 한다.

2. 관리 시스템의 구조

본 논문에서는 네트워크 및 시스템에 대한 통합 관리를 위하여 어플리케이션은 물론 웹 인터페이스를 통하여 NMS(Network Management System)에 접속 가능

하도록 시스템을 설계하였다. 또한, 각각의 도메인으로 관리 영역을 분할하여 관리를 위한 트래픽이 전체 네트워크에 영향을 주지 않도록 구성하고, 별도의 데이터베이스를 구성하여 누적된 통계 자료를 제공할 수 있도록 하였다. <그림 1>은 이러한 통합 관리 시스템의 전체 구조를 보여 준다.



<그림 1> 관리 시스템의 전체 구조도

2.1 User 와 Manager

일반 사용자(user)와 관리자(manager)는 네트워크가 가능한 곳이라면 어디서든지 웹 브라우저를 통해 NMS 에 접속하여 네트워크 및 시스템에 대한 관리 정보를 얻고 모니터링할 수 있는데, 필요할 경우 웹 서버로부터 사용자 인증을 거치게 된다. 사용자는 NMS 내에서 수행되고 있는 서버용 프로그램에 의해 생성된 웹 파일을 보거나, 애플릿을 통하여 필요한 정보를 요청하고 분석된 결과를 얻을 수 있다. 특정 관리 정보에 대해서는 관리자가 직접 어플리케이션을 통해 서버용 프로그램과 통신함으로써 좀더 분석적인 작업을 수행하는 것이 가능하다.

2.2 NMS Server

사용자와 관리자가 웹 또는 어플리케이션을 통해 접속하는 서버이다. WWW Server 는 웹 브라우저를 통한 사용자의 요구에 따라 웹 파일 또는 자바 클래스 파일을 사용자 측으로 전송하게 된다. Server Process 는 독립적인 여러 모듈들로 구성되는데, 사용자의 요구에 따라 관리 정보를 수집하고 자체적인 분석 작업을 수행하여 그 결과를 다양한 방법으로 제공하게 된다.

2.3 DM(Domain Manager)

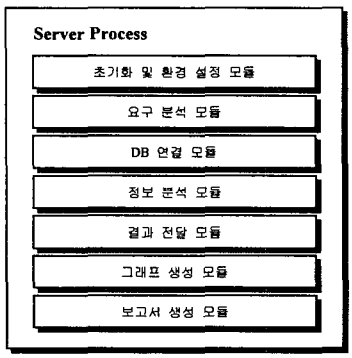
DMS(Domain Management System)는 SNMP Manager 와 TCPdump 프로그램을 관리하며, 이들 프로그램에 의해 수집된 정보를 저장하는 DB 를 가진다. SNMP 프로그램은 여러 가지 네트워크 장비와 서버에 대해 SNMP 지원 가능 여부를 판별하여 SNMP 에이전트(agent)가 동작하는 장치에 대하여 필요한 정보를 수집하여 DB 에 저장한다. TCPdump 프로그램은 SNMP 를 지원하지 않는 장비에 대한 정보를 수집하는데, 네트워크 선로를 따라 흐르는 패킷을 필터링(filtering)하여 특정 서버 혹은 서비스에 대한 분석을 수행하고 그 정보를 DB 에 저장한다. 이렇게 도메인 별로 정보 수집용 관리 프로그램을 운용함으로써, 관리 정보를 수집하기 위한 트래픽이 전체 네트워크에 대한 영향을 최소화하도록 하였다. DB 의 경우 필요에 따라 하나의 통합된 서버로도 구축 가능하며, 데이터량을 최소화하기 위해 최근 자료에 대해서만 삽입(insert) 연산이 수행되고, 일정한 기간이 경과된 자료에 대해서는 계산된 결과값만 유지된다.

3. 관리 시스템의 개요 및 동작

본 장에서는 <그림 1>에서 보여준 Server Process 와 SNMP 및 TCPdump 프로그램에 관해 좀 더 구체적으로 언급하고, 관리를 위한 세부 항목들이 어떻게 구성되는지 살펴 본다.

3.1 Server Process 부분

사용자의 웹 인터페이스 또는 어플리케이션과 직접적으로 통신하며 여러 가지 정보를 제공하고 별도의 작업들을 수행하는 서버 프로세스는 크게 나누어 <그림 2>에서 제시하는 모듈들로 구성된다.



<그림 2> Server Process를 구성하는 모듈

(1) 초기화 및 환경 설정 모듈
관리 대상 목록과 정보를 관리자에게 제공하여 정보 수집을 위한 요구 조건을 설정하도록 한다.

(2) 요구 분석 모듈
웹 인터페이스 또는 어플리케이션으로부터 받은 사용자의 요구를 분석한다.

(3) DB 연결 모듈

JDBC(Java DataBase Connectivity)를 이용해 DB 에 접속하여 필요한 정보를 가져온다.

(4) 정보 수집 모듈
사용자의 요구에 따라 장비 또는 시스템의 관리 정보를 직접 얻어 온다.

(5) 결과 전달 모듈
사용자가 요구한 정보를 어플리케이션이나 웹 인터페이스의 자바 애플릿으로 전달한다.

(6) 그래프 생성 모듈
DB 에 저장된 수집 정보를 이용하여 여러 가지 그래프를 생성하여 파일로 저장한다.

(7) 보고서 생성 모듈
여러 가지 관리 정보를 응용하여 보고서 형식의 웹 파일을 생성한다.

3.2 SNMP 부분

네트워크 장비 또는 시스템의 MIB 값을 구해 오는 하나의 독립된 모듈로서, 일정한 주기에 의해 자체적으로 동작하며 JDBC 를 이용하여 DB 에 그 정보를 저장하기도 하고, NMS 의 Server Process 에 의해 직접 호출되어 그 결과를 반환하기도 한다. [표 1]은 사용자의 요구에 따라 SNMP Manager 가 제공하는 관리 정보들의 일부를 간략하게 보여 준다.

[표 1] 관리 정보를 위한 분석 항목

관리 항목	관리 정보
구성 관리	IP Address, ifIndex, ifDescr, ifType, ifMTU, ifOperStat, ifSpeed, ifPhysAddress, sysName, sysServices, ipRouteNextHop, ...
성능 관리 및 장애 관리	ifIndex, SysUpTime, ifInOctects, ifOutOctects, ifInErrors, ifOutErrors, ipForwarding, ipInReceives, ipInDiscards, ipOutDiscards, tcpInSegs, tcpOutSegs, tcpInErrs, tcpOutErrs, udpInDatagrams, udpOutDatagrams, udpNoPorts, udpInErrors, snmpInPkts, snmpOutPkts, ...

3.3 TCPdump 부분

트래픽 분석에 편중된 네트워크 및 시스템 관리 방법에서 벗어나 특정 서버나 서비스에 대한 차별화된 분석 정보를 제공하기 위한 것으로 네트워크 선로를 따라 흐르는 패킷을 필터링하게 되는데, 패킷의 근원지 주소와 목적지 주소, 프로토콜, 포트 번호 등의 정보를 추출한다. 이를 통하여 전체 트래픽에 대한 프로토콜별 사용률, 특정 서비스에 대한 이용률, 내외부 웹 서버에 대한 접속 순위 등에 대한 상세 통계 정보를 제공하게 된다.

3.4 시스템 관리 명령어 처리 부분

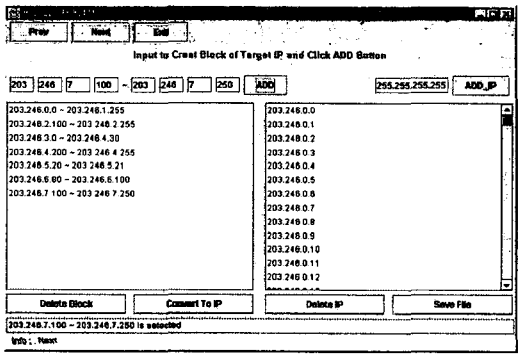
특정 시스템의 사용 현황 등을 파악하기 위한 것으로 [표 2]에서 사용되는 관리 항목들을 보여 준다.

[표 2] 시스템 관리 항목

관리 명령	항목 설명
ping, nslookup	IP 주소와 도메인 이름
uname	시스템 이름
dmesg	시스템 진단 메시지
iostat	I/O 통계
vmstat	가상 메모리 통계
df	디스크 블록과 파일 시스템

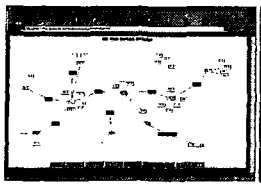
4. 구현 화면 및 결과 고찰

초기화를 담당하는 프로그램은 관리자로 하여금 네트워크 및 시스템 자원에 대한 관리 범위를 설정하게 한 후, 장비에 대한 SNMP 지원 여부를 판별하고 IP 에 대한 논리적 중복성을 배제한다. 그리고, 관리 대상 항목에 대한 기본적인 정보를 수집하여 파일 및 DB 에 저장하는데, NMS 의 서버 프로그램은 이러한 환경 설정 정보를 바탕으로 해서 모든 관리 대상에 대한 정보 수집과 분석 작업을 수행되게 된다. <그림 3>은 초기화 프로그램의 실행 결과 화면 중에 하나를 보여 준다.

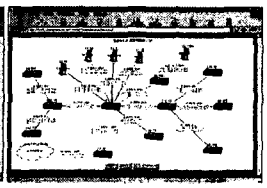


<그림 3> 초기화 프로그램 실행 화면

<그림 4>는 웹 브라우저에서 실행되는 애플릿으로 수집된 정보에 의해 전체 네트워크가 어떻게 구성되는지를 자동으로 시뮬레이션하여 보여 준다. 전체 네트워크에 대한 백본 트래픽 현황을 실시간으로 모니터링할 수 있는 애플릿의 실행 결과 화면은 <그림 5>에 나타내었다. 여기서는 네트워크 연결 구성도를 바탕으로 최대 속도, 입력, 출력, 사용률 등을 알 수 있다.

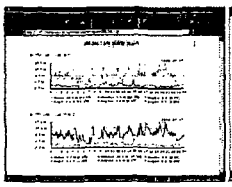


<그림 4> 네트워크 연결 구성도

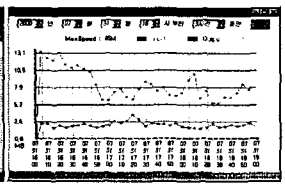


<그림 5> 백본 트래픽 현황

<그림 6>에서는 자동으로 생성된 일별, 주별, 월별, 연별 트래픽 보고서를 IP 에 대한 인터페이스 별로 볼 수 있다. <그림 7>은 사용자가 선택한 IP, 인터페이스 또는 프로토콜, 특정 기간 동안의 입력, 출력, 에러에 대한 비율을 도식화해서 보여 준다.

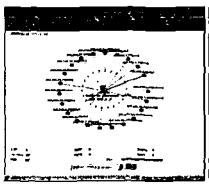


<그림 6> 인터페이스별 트래픽 보고서

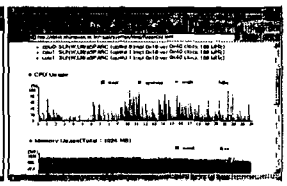


<그림 7> 특정 기간별 트래픽 정보

<그림 8>은 현재 특정 서버에 어떤 호스트들이 어떠한 프로토콜을 이용해 접속하고 있는지를 보여 주고, <그림 9>는 특정 서버의 시스템 이름을 비롯하여, CPU 타입과 개수 및 사용률, 전체 메모리와 사용률, 전체 디스크의 사용률과 파일 시스템 정보 등에 대한 보고서를 보여 준다.

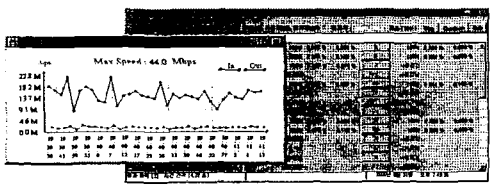


<그림 8> 서버별 접속 현황



<그림 9> 시스템별 사용 현황

<그림 10>은 사용자가 요구하는 IP 에 대하여 인터페이스별로 실시간 트래픽 현황을 보여 주는 어플리케이션의 실행 결과 화면이다.



<그림 10> 실시간 인터페이스 사용 현황

5. 결론 및 향후 연구

본 논문에서는 SNMP MIB-II 로부터 얻을 수 있는 기본 관리 정보를 제공함과 더불어, 다각도로 트래픽 분석 작업을 수행할 수 있는 시스템을 설계 및 구현하였고, TCPdump 프로그램을 이용하여 서버나 특정 서비스에 대한 통계 자료도 제공할 수 있도록 하였다. 뿐만 아니라, 시스템 관리 명령을 이용하여 자원에 대한 이용률을 여러 가지 정보로써 제공하였다.

제안 시스템의 구현을 위해 네트워킹과 보안 기능이 뛰어나며 멀티스레딩(multi-threading)과 웹과의 연동 기술이 우수한 자바 언어를 사용하였으므로, 소스 프로그램의 변경 없이 플랫폼(platform) 독립적으로 관리 프로그램이 수행될 수 있고, 관리자는 어플리케이션이나 웹과 같은 쉬운 인터페이스를 통해 어디서든지 관리 시스템에 접속하여 네트워크 및 시스템에 대한 분석 작업과 모니터링을 수행하고 보고서를 제공받을 수 있게 된다.

본 논문에서 제안한 시스템은 창원대학교 네트워크 상에서 실제 운용 중인 것으로, 주요 라우터와 서버 등의 장비로부터 관리 정보를 수집하고 분석 정보를 제공하여 네트워크 및 시스템 관리자는 물론 상위 부서에 대한 보고 자료로도 활용되고 있어 운용의 타당성과 새로운 설비 투자에 대한 근거 자료로서의 신빙성을 입증하고 있다.

본 논문에서 제안하여 설계 및 구현한 시스템은 관리자 측면의 어플리케이션을 비롯하여 일반 사용자까지도 웹이라는 인터페이스를 통하여 자신이 사용하고 있는 네트워크와 시스템에 대한 관리 정보를 직접 확인할 수 있도록 함으로써 자원의 활용과 이용 분야에 대한 인식을 고취시키고, 이를 통해 기존 자원을 더욱 효율적으로 사용할 수 있게 한다.

향후 연구로는 자바 서블릿(servlet) 기술을 적용하여 프로그램의 효율은 최대화하는 반면 부하는 최소화하여 시스템의 성능을 개선하고, 더 나아가 다양한 네트워크들 간의 연동 기술 및 ORB(Object Request Broker)를 이용한 분산 기술의 적용이 필요하리라 본다.

참고문헌

[1] John Bommers, "Practical Planning for Network Growth", Prentice Hall PTR, 1996

[2] Heinz-Gerd, Hegering Abeck, "Integrated Network and System Management", Addison Wesley, 1995

[3] William Stallings, "SNMP, SNMPv2, SNMPv3, and RMON 1 and RMON2", 3rd Edition, Addison Wesley, 1998

[4] 최문석, 강진희, 임효택, 이광형, 이재욱, "JAVA 를 이용한 네트워크 트래픽 감시 도구의 설계 및 구현", 한국통신학회 '98 추계 종합학술발표회 Vol.18 No.1, 1998

[5] 유승근, 최영수, 정진욱, "네트워크 및 시스템 관리를 위한 웹 기반 통합 관리 시스템의 설계 및 구현", 1999 년 한국정보처리학회 추계 학술발표논문집 제 6 권 제 2 호, 1999