SNMP를 이용한 인터넷 분석 파라미터 추출 시스템의 설계 및 구현

신 상 철† · 안 성 진†† · 정 진 욱†††

요 약

이 논문에서는 TCP/IP를 기반으로 하는 인터넷을 분석하기 위해 SNMP를 사용하여 인터넷 분석 파라미터를 추출해주는 시스템을 설계하고 구현하였다. 인터넷 분석 파라미터 추출 시스템은 크게 피관리 시스템으로부터 관리정보를 수집해오는 수집 모듈 부분과 수집된 관리정보를 이용하여 인터넷 분석 파라미터를 계산하는 분석모듈 부분으로 나뉜다. 관리자가 수집요구나 분석요구를 하면 요구제어 모듈에서 이들 요구를 분석하여 해당 모듈로 전달한다. 수집요구 모듈에서는 피관리 시스템으로부터 관리 정보를 추출해내기 위해 폴링 스크립트를 생성하고, 지정된 수집 주기를 바탕으로 주기적으로 관리 정보를 추출해낸다. 분석요구 모듈에서는 수집모듈에서 수집한 관리 정보를 이용하여 유통 트래픽 분석/인터페이스 유통 패킷 분석/패킷 트래픽 및 관리 트래픽 분석 파라미터를 추출할 수 있으며, 관리를 편리하게 하기 위하여 기본분석/심화분석으로 나누었다. 기본분석은 다수의 피관리 시스템으로부터 이상이 있는 시스템을 분별하기 위해서 사용되며 심화분석은 특정 시스템을 자세하게 분석하기 위해 사용된다. 또, 분석 파라미터에 대해 시간대별, 일일, 주별, 월별 분석을 제공하여 보다 세밀한 분석이 가능하다. 실험 및 고찰에서는 분석 파라미터 추출 시스템을 활용하는 예를 보이기 위해 실제환경에서의 분석결과를 보이고 있다. 인터넷 분석 파라미터 추출 시스템은 관리자가 망 구성요소에 대한 상태를 파악하는데 도움을 줄 수 있고, 대역폭 계획 및 망 장비에 대한 성능 개선 작업 등의 지표로서 사용될 수 있을 것이다.

The Design and Implementation of Parameter Extraction System for Analyzing Internet Using SNMP

Sang-Chul Shin† · Seong-Jin Ahn†† · Jin-Wook Chung†††

ABSTRACT

In this paper, we have designed and implemented a parameter extraction system for analyzing Internet using SNMP. The extraction system has two modules; one is collection request module, and the other is analysis request module. The collection request module generates a polling script, which is used to collect management information from the managed system periodically. With this collected data, analysis request module extracts analysis parameters. These parameters are traffic flow analysis, interface traffic analysis, packet traffic analysis, and management traffic analysis parameter. For management activity, we have introduced two-step-analysis-view. One is Summary-View, which is used to find out malfunction of a system among the entire managed systems. The Other is Specific-View. With this view we can analyze the specific system with all our analysis parameters. To show availability of this system, some analysis results are shown and analyzed about routers on real environments. The parameter extraction system will help a network manager grasp the current status of network elements and use the available data as indicators for line capacity planning, network redesigning, decision making of performance upgrade for a network device and things like that.

† 정 회 원 : 콤텍시스템 기술연구소 연구원
†† 종신회원 : 성균관대학교 컴퓨터교육학과 교수
††† 종신회원 : 성균관대학교 전기전자 및 컴퓨터공학부 교수
논문접수 : 1998년 8월 29일, 심사완료 : 1998년 12월 18일

1. 서 론

얼마전까지만 해도 인터넷이나 망이란 개념은 일반 인들에게는 의미가 전달 되지않는 모호한 개념이었다. 하지만 이들 개념은 월드 와이드 웹의 등장과 함께 전산 관련 분야에 종사하는 사람들만이 아니라 일반 사용자들에게도 널리 퍼지게 되었다. 이와 동시에 인터넷에 접속하여 사용하는 사용자들의 수는 급격히 증가하고 있다. 현재 가장 널리 사용되고 있는 월드 와이드 웹은 문자 정보만을 제공하는 형태에서 출발하였다. 하지만 사용자들의 정보에 대한 욕구와 이에 상응하는 망 기술의 발전으로 문자 정보만이 아니라 음성이나 화상 등의 멀티미디어 정보도 제공할 수 있는 형태로 발전해왔다. 이러한 환경의 변화로 인해 통신망에서의 트래픽 양이 급격히 증가하고 있으며 기존의 통신망으로는 이를 수용하기 어렵게 되었다. 이는 망의 고속화에 대한 요구를 촉발시켰으며, 통신망에 대한 관리 문제도 함께 부각되고 있다. 사용자의 폭넓은 요구를 충족시키기 위해 망 관리자는 망의 상태를 주시하고 이를 분석하여 보다 효율적으로 망을 설계, 운용해야 하는 책임이 어느 때보다도 중요한 시점이다[1][2].

인터넷 망을 관리하는 표준으로 SNMP(Simple Network Management Protocol)가 있다. SNMP는 TCP/IP의 표준 망 관리 프로토콜로서 프로토콜 자체만이 아니라, 관리 데이터베이스 구조에 대한 사양, 자료 객체들과 같은 망 관리에 필요한 여러 가지 기능들에 대한 표준을 의미한다[3]. SNMP가 다양한 장비에 적용되어 활용범위가 확장됨에 따라 SNMP를 이용하여 망을 관리하는 기법에 대한 연구가 진행되어왔다[4][5]. SNMP의 MIB 변수를 조합하여 선로의 이용률, 에러율, 방송형 패킷 비율을 구하는 방법에 대한 기존의 연구가 있었다[6][7][8]. 그리고, 인터넷 분석 파라미터를 정의하여 유통 트래픽 분석, 인터페이스 유통 패킷 분석, 패킷 트래픽 및 관리 트래픽 분석에 관한 파라미터를 정의한 연구가 있었다. 지금까지의 연구에서는 분석 방법에 대한 연구는 진행된 바가 있으나 실제로 이러한 파라미터를 이용한 분석 방법론을 적용하여 인터넷 상에서 망을 분석해주는 분석 파라미터 추출 시스템을 구현한 바는 없었다[9]. 본 논문에서는 인터넷 표준 관리 정보를 기반으로 한 기존의 인터넷 분석 파라미터를 이용하여 관리자가 TCP/IP 망에 대하여 분석을 쉽게 할 수 있도록 기본 분석과 심화 분석의 개념을 두었다. 그리고, 이들 분석 파라미터를 월별/주별/일별/시간대별 등과 같이 분류하여 수집된 데이터를 기반으로 추이를 분석할 수 있는 인터넷 분석 파라미터 추출 시스템을 설계하고, 구현하였다. 분석 시스템은 C 언어를 이용하여 Sun UltraSPARC 및 호환 기종에서 동작되도록 구현되었으며, 운영체제는 Solaris 2.5을 이용하였다.

본 논문의 2장에서는 인터넷 분석 파라미터의 종류와 의미에 대해 설명하였고, 3장에서는 인터넷 분석 파라미터 추출 시스템의 설계 및 구현에 대해 세부적으로 설명하였다. 그리고 4장에서는 본 논문에서 설계 및 구현한 인터넷 분석 파라미터 추출 시스템을 사용하여 실제 인터넷 망을 대상으로 관리 정보를 수집하여 분석한 결과를 보이고 있다.

2. 인터넷 분석 파라미터

본 논문에서는 TCP/IP 기반의 인터넷 망을 관리하기 위하여 인터넷 분석 파라미터를 이용하여 망을 분석한다. 이들 인터넷 분석 파라미터는MIB-II에 정의되어 있는 MIB 변수들 중 성능과 장애에 관련된 변수들을 추출하고, 추출된 MIB 변수를 이용하여 유통 트래픽 분석 파라미터, 인터페이스 유통 패킷 파라미터, 패킷 트래픽 및 관리 트래픽 분석 파라미터를 정의했다[9]. 이들 파라미터 외에도 구성 관리에 필요한 장비 관련 정보 및 인터페이스 관련 정보를 추가하였다.

2.1 유통 트래픽 분석 파라미터

(1) 선로 이용률

선로 이용률은 대역폭을 기준으로 선로의 이용량을 백분율로 나타낸 분석 파라미터이다.

(2) 가동률

가동률은 관리하고자 하는 시스템이 분석 기간 동안에 얼마만큼 가동을 했는지를 표시하는 분석 파라미터이다.

(3) 입출력 트래픽률

입출력 트래픽률은 단위 시간당 인터페이스에서 입출력되는 트래픽의 비율로 전체 송수신 바이트량과 송/수신 각각에 대한 비율로 나타낸다.

2.2 인터페이스 유통 패킷 분석

(1) 인터페이스 패킷 송수신률

인터페이스 패킷 송수신률은 단위 시간당 인터페이스

에 유출입되는 패킷을 나타내주는 파라미터이다. 관리자는 인터페이스 패킷 송수신율 파라미터를 통해서 한 인터페이스에 유출입되는 패킷의 비율을 알 수 있다.

(2) 방송형 송수신 트래픽 비율

방송형 트래픽 송수신 트래픽 비율은 전체 패킷 중 방송형인 패킷의 비율을 보여주는 분석 파라미터이다.

(3) 인터페이스 패킷 송수신 손실률

인터페이스 패킷 송수신 손실률은 단위 시간당 인터페이스에서 손실되는 패킷의 율을 나타내주는 파라미터이다.

(4) 에러 수신율

에러 수신율은 원격지 시스템으로부터 유입되는 프레임 등의 에러에 의해서 상위 계층 프로토콜로 전송되지 못하는 수신 패킷의 수를 의미한다.

2.3 패킷 트래픽 분석 및 관리 트래픽 분석 파라미터

(1) 시스템 패킷 입출력률

시스템 패킷 입출력률은 단위 시간당 인터페이스에 입출력되는 트래픽의 비율이다. 이 분석항목을 통하여 관리자는 전체 시스템에 입출력된 패킷의 양을 파악할 수 있다.

(2) 패킷 전달률

패킷 전달률은 MIB-II의 오브젝트 중 ipForwarding이 1일 경우에만 측정할 수 있는 파라미터이다.

(3) 시스템 패킷 송수신 손실률

시스템 패킷 송수신 손실률은 시스템에서 손실되는 패킷의 율을 나타내주는 파라미터이다. 이 파라미터는 특정 인터페이스에서 손실되는 패킷의 율을 나타내는 인터페이스 패킷 송수신 손실률과는 달리 전체 시스템에서 손실되는 패킷의 율을 나타내는 파라미터이다.

(4) 시스템 자원 부하율

시스템 자원 부하율은 관리자에게 시스템에서 사용하는 망 버퍼의 부하율을 알려주는 파라미터이다.

(5) 경로 설정 실패율

경로 설정 실패율은 시스템에서 경로 설정을 수행하지 못하는 패킷의 율을 나타내는 파라미터이다.

(6) 관리 트래픽 이용률

관리 트래픽 이용률은 전체 트래픽에 대한 관리 트래픽의 이용량을 나타내주는 파라미터이다.

2.4 구성 관리 파라미터

(1) 인터넷 장비 현황

인터넷 장비 현황은 관리하고자 하는 피관리 시스템의 이름, 위치, 버전, 책임자와 같이 관리자가 필요로 하는 장비의 구성에 관련된 파라미터이다.

〈표 1〉 인터넷 장비 현황 파라미터
〈Table 1〉 The configuration parameters for Internet devices

파라미터	MIB 객체
시스템 이름	SysName
시스템 위치	SysLocation
시스템 정보	SysDescr
시스템 책임자	SysContact

(2) 인터넷 장비 인터페이스 현황

인터넷 장비 포트 현황은 장비의 인터페이스가 몇 개인지 그리고, 각 인터페이스의 현재 상태 및 인터페이스 타입 등의 인터페이스에 관련된 구성 정보를 관리자에게 알려주는 파라미터이다.

〈표 2〉 인터넷 장비 인터페이스 현황
〈Table 2〉 The configuration parameters of Internet device's interface

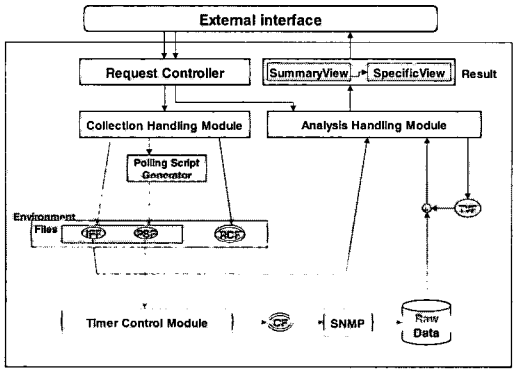
파라미터	MIB 객체
인터페이스 상태	IfAdminStatus
인터페이스 정보	IfDescr
인터페이스 형태	IfType
인터페이스 번호	IfNumber

3. 인터넷 분석 파라미터 추출 시스템의 설계 및 구현

3.1 인터넷 분석 파라미터 추출 시스템의 전체 구조

인터넷 분석 파라미터 추출 시스템의 전체 구조는 (그림 1)과 같다. 인터넷 분석 파라미터 추출 시스템은 외부 인터페이스(External Interface)로부터 수집요구나 분석요구를 입력받아 수집이나 분석을 수행한다. 외부 인터페이스로부터 어떤 요구가 들어오면 요구제어 모듈(Request Controller)이 동작하고, 수집요구이면 수집 요구 모듈

(Collection Handling Module)을 호출하고 분석요구이면 분석 요구 모듈(Analysis Handling Module)을 호출한다. 수집요구 모듈은 분석을 하기 위해 일정 기간동안 지정된 피관리 시스템으로부터 관리 정보를 수집하는 모듈이고, 분석 요구 모듈은 수집 요구 모듈을 통해 수집된 데이터를 인터넷 분석 파라미터를 이용하여 분석하는 모듈이다.



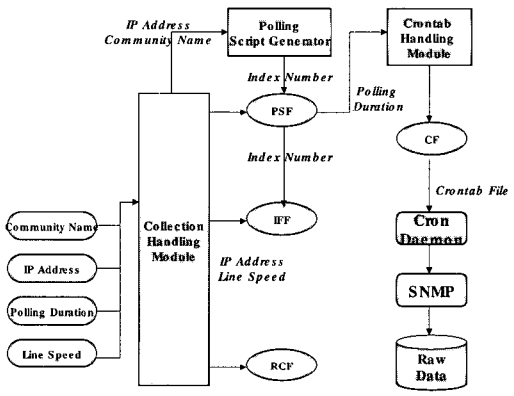
(그림 1) 인터넷 분석 파라미터 추출 시스템의 전체 구조
(Fig. 1) The implementation model of parameter extraction system for analyzing Internet

(1) 요구 제어 모듈 (Request Control Module)

외부 인터페이스로부터 인터넷 성능 파라미터 추출 시스템으로 어떤 요구가 들어오면 요구제어 모듈(Request Control Module)이 동작한다. 요구제어 모듈에서는 외부 인터페이스로부터 들어온 요구 메시지를 분석하고 이를 프로그램에서 정의된 구조체에 저장을 한다. 그리고, 수집 요구와 분석 요구를 구분하여 수집 요구(Collection Request)이면 수집 모듈(Collection Handling Module)을 호출하고 분석 요구(Analysis Request)이면 분석 모듈(Analysis Handling Module)을 호출하는 역할을 수행한다.

(2) 수집 요구 모듈 (Collection Handling Module)

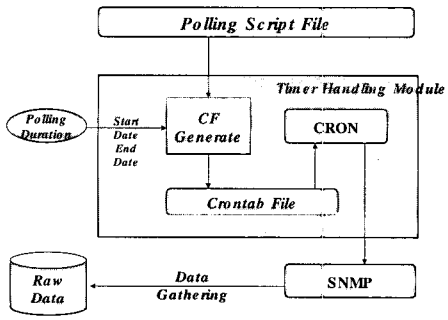
수집요구 모듈은 분석을 하기 위해서 일정기간 동안 자료를 수집해주는 모듈이다. 이 모듈에서는 자료를 수집하는 기간, 분석하고자 하는 피관리 시스템, 수집하고자 하는 MIB-II 오브젝트와 같은 것들을 정의하고 있다. 수집요구가 들어오면 수집요구 모듈은 이 요구가 이전 요구와 중복되는 것인지 아닌지를 확인하고 중복되지 않았으면 RCF(Request Control File)에 등록한다. 그리고, 이후에 분석요구시에 필요한 피관리 시스템의 특성을 IFF(InterFace File)에 이러한 특성을 정의하고, 폴링 스크립트 생성기(Polling Script Generator)에 시스템 정보와 폴링할 MIB-II 오브젝트 등의 정보를 입력하여 폴링 스크립트를 작성한다. 폴링 스크립트의 작성이 완료되면 Crontab 처리 모듈(Crontab Handling Module)을 호출한다.



(그림 2) 수집 요구 모듈
(Fig. 2) Collection Handling Module

(3) 타이머 처리 모듈(Timer Handling Module)

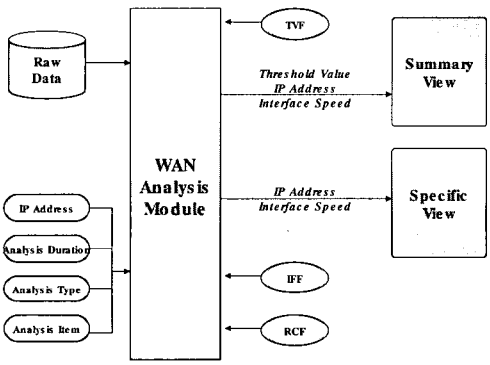
이 모듈에서는 유닉스의 시간 데몬(Timing Daemon)인 cron에 폴링 스크립트와 폴링 기간의 정보를 입력으로 받아 CF(Crontab File)을 생성하고, 이를 cron에 넘겨 일정기간동안 폴링 스크립트를 수행시켜 분석에 필요한 자료를 수집해온다. 수집 시에는 SNMP을 이용하여 피관리 시스템으로부터 관련된 MIB-II 객체들을 폴링해온다.



(그림 3) 타이머 처리 모듈
(Fig. 3) Timer Handling Module

(4) 분석 요구 모듈 (Analysis Handling Module)

분석 요구 모듈은 관리자가 수집 요구 모듈을 통해 수집한 데이터를 분석해주는 모듈이다. 분석 요구는 크게 두가지로 나뉘는데 하나는 기본 분석(Summary View)이고, 다른 하나는 심화 분석(Specific View)이다. 기본 분석은 관리자가 문제가 있는 시스템을 구분할 경우 판단자료가 될 수 있도록 기본적인 항목만으로 전체 피관리 시스템에 대하여 분석하는 경우 사용된다. 심화 분석은 관리자가 문제가 있다고 판단한 시스템에 대해서 더 자세히 분석하기 위해서 제공되는 것으로 2장에 정의된 분석 파라미터들에 대한 정보를 얻을 수 있다.



(그림 4) 분석 요구 모듈
(Fig. 4) Analysis Handling Module

(5) 폴링 스크립트 생성기(Polling Script Generator)

수집 요구 모듈에서 받은 정보를 이용하여 폴링 스크립트를 생성하는 부분이다. 생성된 폴링 스크립트에는 수집하고자 하는 MIB 변수가 정의되어 있고 분석에 필요한 부가 정보도 함께 수집하도록 정의되어 있다.

(6) 환경 파일

인터페이스 파일(IFF : interface file)은 관리하고자 하는 시스템에 대한 인터페이스를 저장하고 있는 파일이다. 이 파일은 수집 요구시에 생성되며 분석 요구 모듈이 참조한다. 이 파일에는 피관리 시스템의 IP 주소, 인터페이스 속도, 인터페이스 번호가 저장되어 있다.

폴링 스크립트 파일(PSF : Polling Script File)은 수집 요구시에 폴링 스크립트 생성기에 의해서 생성되는 파일로 분석에 필요한 부가 정보 - 시간 정보, 분석 시작/종료 시점 - 와 수집하고자 하는 MIB 변수를 폴링하는 SNMP 명령으로 구성되어 있다.

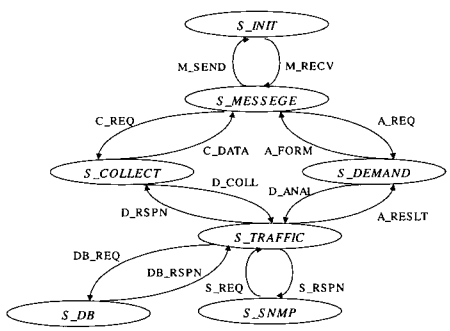
요구 제어 파일(RCF : Request Control File)은 복수개의 수집 요구를 수행할 경우 이를 구분하기 위해 사용되는 수집요구 식별자(request control identifier)와 수집요구 정보를 기록하고 있는 파일이다.

CF 파일(CF : Crontab File)은 유닉스의 시간 데몬인 cron에 입력되는 시간 정보에 대해 정의되어 있는 파일이다. 이 파일의 내용은 crontab 명령의 형식에 따른다.

임계치 파일(TVF : Threshold Value File)은 기본 분석(Summary View)에 필요한 파일로 이용률, 가동률, 다운 횟수에 대한 임계치가 저장되어 있는 파일이다.

3.2 상태 흐름 및 동작

인터넷 분석 파라미터 추출 시스템은 S_INIT, S_MESSAGE, S_COLLECT, S_DEMAND, S_TRAFFIC, S_DB, S_SNMP 등의 상태를 가진다(그림 5). S_INIT 상태에서는 시스템의 초기 상태를 설정하고 외부 인터페이스와의 통신을 위해 준비하는 작업을 수행한다. 그리고, 외부 인터페이스에서 입력되는 메시지를 처리하기 위해 S_MESSAGE로 상태가 천이된다. S_MESSAGE 상태에서는 입력된 메시지를 분석하게 되고, 분석된 각 결과에 의해 각 요구에 맞는 상태로 천이하게 된다. 즉, S_COLLECT와 S_DEMAND 등의 상태로 천이하게 된다. 먼저 S_COLLECT에서는 외부 인터페이스에 의한 수집 요구에 대한 처리를 하고, 인터넷 분석 파라미터 추출 시스템에게 미리 정의된 MIB 변수의 값을 수집하도록 S_TRAFFIC 상태로 천이하게 된다. 다음은 S_DEMAND로 외부 인터페이스에서 요구한 기본 분석 요구와 심화 분석 요구에 대한 처리가 행해지며 해당 분석 항목에 관



(그림 5) 인터넷 분석 파라미터 추출 시스템의 상태 천이도
(Fig. 5) The state transition diagram of parameter extraction system for analyzing Internet

련된 MIB 검색에 대한 결과를 요청한다. S_TRAFFIC 상태에서는 수집 요구에 대해서는 SNMP를 호출하기 위해 S_SNMP 상태로 천이하게 되고 이렇게 받아온 결과를 데이터베이스에 저장하는 S_DB 상태로 천이하게 된다. 분석 요구에 대해서는 저장된 결과를 데이터베이스에서 검색하기 위해 S_DB 상태로 천이하게 된다.

다음은 S_SNMP 상태로서 해당 MIB에 대한 값을 폴링하기 위한 상태이다. 마지막으로 S_DB는 폴링한 MIB 변수값을 저장하기 위한 상태이다. 상태 천이에 따른 자세한 동작을 (그림 5)와 <표 3>에 요약하여 설명한다.

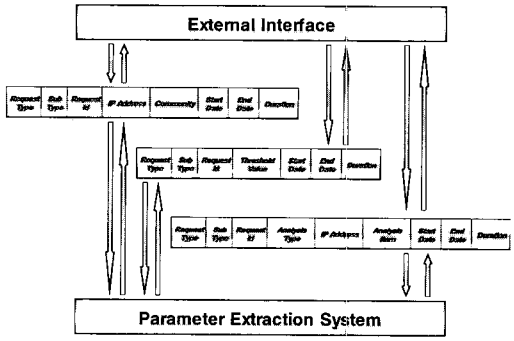
〈표 3〉 인터넷 분석 파라미터 추출 시스템을 위한 상태 천이 테이블

〈Table 3〉 The state transition table of parameter extraction system for analyzing Internet

현재 상태	사 건	행 위	다음 상태
S_INIT	M_RECV	시스템 초기상태 설정 후, 외부 인터페이스로부터 수신한 메시지를 분석한다.	S_MESSAGE
S_MESSAGE	M_SEND	결과 정보를 외부 인터페이스로 전달하기 위한 작업을 수행한다.	S_INIT
	C_REQ	수집 요구를 위해 필요한 정보를 분석한다.	S_COLLECT
	A_REQ	분석 요구를 위해 필요한 정보를 분석한다.	S_DEMAND
S_COLLECT	D_COLL	수집 요구를 수행한다.	S_TRAFFIC
	C_DATA	수집 요구의 결과에 대한 메시지를 형성한다.	S_MESSAGE
S_DEMAND	D_ANAL	기본/심화 분석을 요구한다.	S_TRAFFIC
	A_FORM	기본/심화 분석 요구의 결과에 대한 메시지를 형성한다.	S_MESSAGE
S_TRAFFIC	D_RSPN	수집 요구에 대한 결과를 전달한다.	S_COLLECT
	A_RESLT	분석 요구에 대한 결과를 전달한다.	S_DEMAND
	DB_REQ	데이터베이스에 분석한 정보를 저장한다.	S_DB
	S_REQ	SNMP를 이용해 MIB 객체를 폴링한다.	S_SNMP
S_DB	DB_RSPN	데이터베이스에서 검색한 정보를 전달한다.	S_TRAFFIC
S_SNMP	S_RSPN	폴링한 결과 데이터를 전달한다.	S_TRAFFIC

3.3 메시지 형식

인터넷 분석 파라미터 추출 시스템은 클라이언트와의 통신을 위하여 MATP(Management Application Transfer Protocol) 프로토콜을 정의하여 사용한다. MATP 프로토콜의 메시지 형식은 (그림 6)과 같다. MATP 메시지 형식은 크게 하나의 형식으로 통일되어져 있지만, 사용자가 요구하는 서비스에 따라서 수집 요구 메시지(Collection Demand Message)와 기본 분석 요구 메시지(Summary-View Demand Message) 그리고, 심화 분석 요구 메시지(Specific-View Demand Message)로 구분되어진다. 다음은 기본적인 형태의 메시지 필드들에 대한 설명이다.



(그림 6) MATP의 메시지 형식

(Fig. 6) The message formats of MATP

(1) 요구 형식(Request Type)

인터넷 분석 파라미터 추출 시스템에 사용자가 요청하는 서비스를 구분해주는 필드로써 수집 요구, 기본 분석 요구, 심화 분석 요구 등으로 요청된다. 다음의 테이블은 그 메시지 형식과 각 형식에 대한 값을 보여준다.

〈표 4〉 요구 형식과 값

〈Table 4〉 Request types and its values

메시지 형식	값
COLLECT_DEMAND	1
BASIC_ANALYSIS	2
ADVANCE_ANALYSIS	3

(2) 세부 형식(Sub Type)

요구 형식에서 설정된 수집 요구에 대해 세부적으로

요청을 하기 위한 형식으로 요청을 추가하는 것인지 삭제하는 것인지 변경하는 것인지 알려준다.

〈표 5〉 세부 형식과 값
〈Table 5〉 Sub-types and its values

메시지 형식	값
ADD	1
MOD	2
DEL	3

(3) 요청 식별자 (Request Identifier)

인터넷 분석 시스템에서 수집 요구나 분석 요구를 할 때 인터넷 분석 시스템이 어떤 요구인지 식별하기 위해서 사용한다.

(4) IFF와 파라미터

이 필드는 수집 요구와 기본 분석 요구, 심화 분석 요구에 따라 다른 기능을 갖는 필드이다.

가. 수집 요구

WAN 분석 시스템에서 수집 요구와 관련해서 필요한 피관리 시스템의 정보를 정의한다.

- IP 주소
  피관리 시스템의 IP 주소를 명시한다.
- 커뮤니티 이름(Community Name)
  피관리 시스템에서 사용하는 커뮤니티 이름을 명시한다.
- 선로 속도(Line Speed)
  피관리 시스템의 선로 속도를 명시한다.

나. 기본 분석 요구

기본 분석 요구에서는 각각의 임계치 정보에 대해서 정의하고 있다. 임계치 정보는 다음과 같이 구성된다.

- 이용률 임계치 정보(Utilization Threshold Value)
  피관리 시스템의 이용률에 대한 임계치 정보를 정의한다.
- 다운 횟수 임계치 정보(Down Count Threshold Value)
  피관리 시스템의 다운 횟수에 대한 임계치 정보를 정의한다.
- 가동률 임계치 정보(Availability Threshold Value)
  피관리 시스템의 가동률에 대한 임계치 정보를 정의한다.

다. 심화 분석 요구

분석 형식(Analysis Type)과 분석 항목(Analysis Item), 분석하고자 하는 시스템의 IP 어드레스에 대하여 정의하는 필드이다. 분석 형식과 분석 항목의 타입과 값은 아래의 테이블에 정의된다.

〈표 6〉 분석 형식의 타입과 값
〈Table 6〉 Analysis types and its values

메시지 형식	값
TIME_ANALYSIS	1
DAY_ANALYSIS	2
WEEK_ANALYSIS	3
MONTH_ANALYSIS	4
TOTAL_ANALYSIS	5

〈표 7〉 분석 항목의 타입과 값
〈Table 7〉 Analysis items and its values

메시지 형식	값	메시지 형식	값
UTILIZATION	0	OUT_SYSTEM_PACKET	9
IN_ERROR_RATE	1	IN_SYSTEM_LOST	10
IN_PACKET_RATE	2	OUT_SYSTEM_LOST	11
OUT_PACKET_RATE	3	SYSTEM_MEM_LOAD	12
PACKET_LOST	4	PACKET_RATE	13
IN_OCTET_RATE	5	LOST_PACKET_RATE	14
OUT_OCTET_RATE	6	ROUTING_ERROR	15
BROADCAST_TRAFFIC	7	SNMP_TRAFFIC	16
IN_SYSTEM_PACKET	8		

(5) 시작 시간(start time)

수집 요구 시에 수집 기간을 설정하는 필드로 수집을 시작하는 시간을 입력 받아 설정한다. 이 필드는 년, 월, 일, 시, 분의 세부 필드로 구성된다. 이 필드는 수집 요구 시에만 사용되고 다른 요구 시에는 NULL로 설정된다.

(6) 종료 시간(end time)

수집 요구 시에 수집 기간을 설정하는 필드로 수집을 종료하는 시간을 입력 받아 설정한다. 이 필드 역시 시작 시간과 마찬가지로 년, 월, 일, 시, 분의 세부 필드로 구성된다. 이 필드 역시 수집 요구 시에만 사용

되고 다른 요구 시에는 NULL로 설정된다.

(7) 주기(interval)

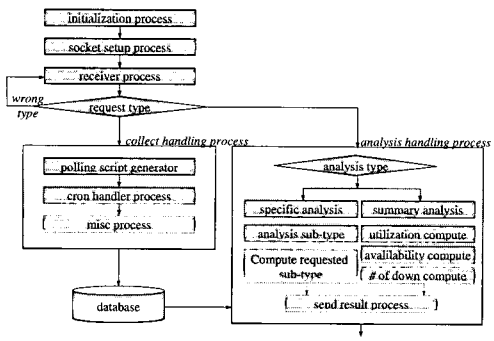
수집 요구 시에 시작 시간과 종료 시간사이에 얼마만큼의 주기를 가지고 데이터를 폴링해서 저장할 것인가를 설정하는 필드로 1분부터 4시간까지 설정하는 것이 가능하다.

(8) 모드(mode)

모드는 분석 요구 시에 사용되는 필드로 설정된 분석 파라미터에 대하여 시간대별 분석, 일일 분석, 주간 분석, 월간 분석, 총괄 분석 등으로 구분된다.

3.4 프로그램 구조

인터넷 분석 파라미터 추출 시스템의 전체 프로그램 구조는 (그림 7)과 같다. 외부 인터페이스로부터 요구 정보를 수신하기 전에 우선 필요한 변수를 초기화하고(initialization process), 외부 인터페이스와 통신하기 위한 소켓을 설정하는 과정을 거친다(socket setup process). 이러한 초기화 과정을 거친 후 외부 인터페이스와 송수신 절차를 수행할 수 있다. 외부 인터페이스로부터 어떤 요구가 입력되면 요구 형식을 감지하여 수집 요구 처리 프로세스나 분석 요구 처리 프로세스로 제어를 넘긴다. 수집 요구 프로세스에서는 주기적으로 관리 정보를 수집하기 위해 폴링 스크립트를 작성하고 분석에 필요한 정보들을 저장하는 작업을 수행한다. 분석 요구 처리 프로세스에서는 분석 요구가 기본 분석인지 심화 분석인지 구별하여 각각에 상응하는 처리 절차를 수행한다.



(그림 7) 전체 프로그램 구조
(Fig. 7) The program structure

(1) 초기화 모듈

가. 초기화 프로세스 (initialization process)

인터넷 분석 파라미터 추출 시스템의 동작을 위해 필요한 변수 및 함수들을 정의하는 부분이다.

나. 소켓 설정 프로세스 (socket setup process)

인터넷 분석 파라미터 추출 시스템은 수집 및 분석 시스템으로 외부 인터페이스로부터 수집이나 분석 요구가 있을 경우에 이를 처리해서 그 결과를 외부 인터페이스로 전송한다. 외부 인터페이스와의 통신을 위해 소켓을 사용한다. 소켓을 사용함으로써 인터넷 분석 파라미터 추출 시스템은 자체 시스템에서의 요구만이 아니라 원격지에서의 요구도 처리할 수 있기 때문에 효과적으로 분산 망 관리를 수행할 수 있다. 소켓 설정 프로세스(socket setup process)는 이러한 소켓에 대한 설정을 하는 부분으로 외부 인터페이스와 안정적으로 접속을 하기 위해 TCP 소켓을 설정해서 사용한다.

다. 수신 프로세스 (receiver process)

이 프로세스는 외부 인터페이스로부터 요구를 전달 받아서 이 요구가 수집 요구인지 분석 요구인지 판별을 하고 각 요구를 실제로 처리하는 부분으로 입력 메시지를 전달한다.

(2) 수집 요구 처리 모듈

가. 폴링 스크립트 생성 프로세스 (polling script generator)

폴링 스크립트 생성 프로세스는 폴링 스크립트를 생성하는 부분이다. 폴링 스크립트를 생성하기 위해 폴링 스크립트 생성 프로세스는 피관리 시스템의 주소, 커뮤니티 이름을 입력으로 받는다. 폴링 스크립트 생성기는 피관리 시스템의 주소를 이용하여 IP 그룹의 ipAdEntIndex 번호를 추출해낸다. ipAdEntIndex 값은 인터페이스 그룹의 관리 정보를 얻어오는데 필요한 정보이다. 폴링 스크립트 생성 프로세스에서 생성한 폴링 스크립트의 예를 들면 다음과 같다.

```
Echo "START" >> /lan/pjt/kdc97/poll/soft.dat
date >> /lan/pjt/kdc97/poll/soft.dat
echo "203.252.36.2" >> /lan/pjt/kdc97/poll/soft.dat
/lan/pjt/kdc97/bin/poll.ksh 203.252.36.2 3 public >>
/lan/pjt/kdc97/poll/soft.dat
echo "203.233.12.54" >> /lan/pjt/kdc97/poll/soft.dat
/lan/pjt/kdc97/bin/poll.ksh 203.233.12.54 6 public >>
/lan/pjt/kdc97/poll/soft.dat
echo "134.75.62.2" >> /lan/pjt/kdc97/poll/soft.dat
/lan/pjt/kdc97/bin/poll.ksh 134.75.62.2 1 public >>
/lan/pjt/kdc97/poll/soft.dat
echo "END" >> /lan/pjt/kdc97/poll/soft.dat
date >> /lan/pjt/kdc97/poll/soft.da
```

[폴링 스크립트 생성기를 통해 생성된 폴링 스크립트]

위 예에서는 203.252.36.2, 203.233.12.54, 134.75.62.2를 주소에 대한 입력으로 받고, SNMP와의 인증 절차를 위한 커뮤니티 이름은 모두 "public"으로 입력 받았을 경우 생성된 폴링 스크립트이다. 폴링 스크립트에는 각 수집 시점의 시간 정보와 분석 시작 및 종료 시점에 대한 정보는 분석을 위해 첨가되는 정보이다. 폴링 스크립트에 존재하는 poll.ksh에는 피관리 시스템으로부터 수집할 MIB 변수가 정의되어 있는데 다음과 같다.

```
/usr/local/bin/snmpget -v 1 $1 $2 2.2.1.10.$3 2.2.1.16.$3
2.2.1.5.$3  2.2.1.3.$3  2.2.1.11.$3  2.2.1.12.$3  2.2.1.13.$3
2.2.1.14.$3  2.2.1.15.$3  2.2.1.17.$3  2.2.1.18.$3  2.2.1.19.$3
2.2.1.20.$3 1.3.0
```

[poll.ksh]

나. 시간 처리 프로세스 (cron handler process)

시간 처리 프로세스는 사용자로부터 입력받은 수집 정보를 바탕으로 주기적으로 피관리 시스템의 관리 정보를 수집하기 위한 처리를 해주는 프로세스이다. 이 프로세스에서는 사용자로부터 수집 시작 및 종료 시간과 폴링 주기를 입력받아 주기적인 관리 정보 수집을 위한 스크립트를 생성한다. 이렇게 생성된 스크립트는 유닉스의 시간 데몬인 cron에 입력되고 cron에서는 이 스크립트에 설정된 시간 정보를 바탕으로 주기적으로 스크립트에서 지정된 명령을 사용하여 관리 정보를 수집하여 저장한다.

다. 기타 프로세스 (misc process)

기타 프로세스에서는 수집 요구시에 추가적으로 생성되는 파일이나 처리 절차를 수행한다. 이 기타 프로세스에는 수집 요구 중복 여부 판별, 기본분석을 위한 임계치 설정, 수집 요구 로그 파일 처리, 수집 요구 삭제시 관련 파일 삭제 등의 기능을 수행한다.

또, 기타 프로세스에는 시스템 구성 관리를 위한 구성 정보를 수집하는 기능도 가지고 있다. 구성 정보는 그 특성상 주기적으로 수집해야 하는 정보가 아니기 때문에 수집 요구 설정을 할 때 한번만 수집하는 정보이다.

(3) 분석 요구 처리 모듈

가. 기본 분석 프로세스 (summary analysis process)

기본 분석 프로세스는 분석할 피관리 시스템이 많을 경우 이들 피관리 시스템들 중에서 이상이 있는 피관리 시스템을 분리해내고자 할 때 유용한 분석이다. 기본 분석 프로세스에서는 수집된 정보를 이용하여 피관리 시스템의 이용률(utilization), 가동률(availability), 다운 횟수(# of down)를 계산한다. 시스템의 이용률은 2장에 정의된 수식을 이용해서 구하고, 가동률은 전체 수집 시간과 실제 피관리 시스템의 동작시간 - 시스템 그룹의 sysUpTime을 이용 - 을 비교해서 구할 수 있다. 다운 횟수도 마찬가지로 시스템 그룹의 sysUpTime을 이용해서 구할 수 있다. 기본 분석 프로세스에서는 수집 요구시에 설정한 모든 피관리 시스템에 대해서 선로 이용률, 가동률, 다운 횟수를 계산해서 사용자에게 전달한다. 사용자는 수집 요구시에 이들 항목에 대해 임계치를 설정할 수 있는데, 이 임계치를 바탕으로 피관리 시스템에 이상 여부를 추측할 수 있다.

나. 심화 분석 프로세스 (specific analysis process)

심화 분석 프로세스는 사용자로부터 하나의 특정 피관리 시스템에 대해서 분석하는 프로세스이다. 분석 항목은 사용자가 직접 설정할 수 있으며 2장에 정의된 모든 항목이 심화 분석 프로세스에서 분석하는 내용이다. 분석은 크게 전체 피관리 시스템 통계 정보 분석, 피관리 시스템 상태 정보 분석, 월별/주별/일별/시간대별 특정 항목 분석으로 나뉘어진다.

이 절에서 설명한 기본 분석 프로세스와 심화 분석 프로세스의 처리 결과는 4장 실험 및 고찰에서 자세히 다루겠다.

4. 실험 및 고찰

이번 장에서는 본 논문에서 설계 및 구현한 인터넷 분석 파라미터 추출 시스템을 이용하여 실제로 인터넷 망에 대하여 관리 정보를 수집하고 이를 분석하였다. 이때, 설정된 실험 환경은 다음과 같다.

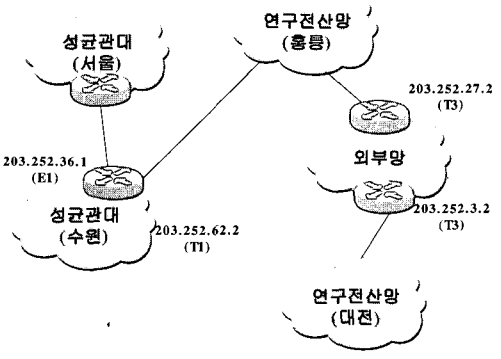
(1) 실험을 위해 사용된 성균관대학교 인터넷 망의 구성은 (그림 8)과 같다.

성균관대학교 내부망은 서울과 수원 사이의 선로이며 속도는 E1이다. 성균관대는 연구 전산망을 통해 인터넷 망에 접속하며 속도는 T1이다. 홍릉의 연구전산망은 외부망을 통해 대전의 연구전산망과 접속하며 속도는 T3이다.

(2) 수집 주기(Polling Interval)는 30분이다.

분석을 위한 데이터의 수집 기간은 1998년 6월 10일

10시부터 1998년 06월 20일 20시까지이다.



(그림 8) 실험 대상 망 구성도
(Fig. 8) Network environments for experiments

(그림 8)의 피관리 시스템들에 대해서 기본 분석을 한 결과는 <표 8>과 같다. 기본분석은 여러 피관리 시스템 중에서 이상이 있는 시스템을 분리하기 위해 사용될 수 있다. <표 9>의 결과를 보면 전체적으로 피관리 시스템들이 안정적으로 동작하고 있음을 확인할 수 있다. 그러나 선로의 이용률을 보면 피관리 시스템인 134.75.62.2의 경우 이용률이 다른 피관리 시스템에 비해 상당히 높은 것을 확인할 수 있다. 일반적으로 WAN 선로의 경우 선로 이용률이 90% 이상일 경우 선로의 이용률이 높다고 할 수 있는데[10], 피관리 시스템 134.75.62.2의 경우 망 사용자가 추가되거나 선로의 대역폭을 추가로 필요로 하는 응용을 설치했을 경우 선로의 대역폭을 증속하거나 망의 구성을 효율적으로 변경해야 할 가능성이 있다.

〈표 8〉 기본 분석 결과
〈Table 8〉 The Results of Summary-View

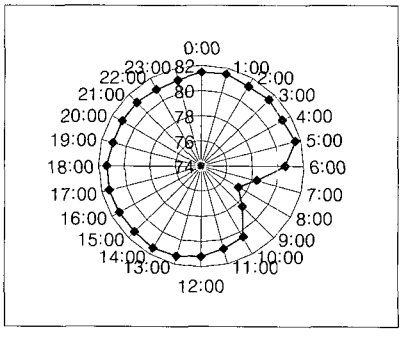
피관리 시스템의 IP 주소	다운 횟수	가동률 (%)	선로 이용률 (%)	속도
203.252.36.1	0	100	8.52	E1
134.75.62.2	0	100	80.54	T1
134.75.27.2	0	100	7.32	T3
134.75.3.2	0	100	23.54	T3

<표 9>는 기본분석을 바탕으로 하여 선로의 이용률이 다른 피관리 시스템에 비하여 상당히 높은 134.75.62.2를 대상으로 하여 심화 분석을 수행한 결과이다.

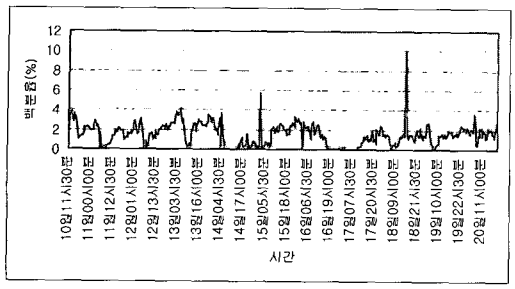
〈표 9〉 심화 분석 결과 (134.75.62.2)
〈Table 9〉 The Results of Specific-View (134.75.62.2)

유통 트래픽 분석		
선로 이용률	80.5453%	
입출력 트래픽률	49.5686% (출력)	50.4314% (입력)
가동률	100%	
인터페이스 유통 패킷 분석		
인터페이스 패킷 송수신율	49.4199% (송신)	52.1271% (수신)
방송형 송수신 트래픽 비율	0.0816%	
인터페이스 패킷 송수신 손실률	1.5539%	
에러 수신율	0.0603%	
시스템 현황 분석		
시스템 패킷 입출력률	1.0795% (출력)	98.9205% (입력)
패킷 전달률	99.7071%	
시스템 패킷 송수신 손실률	0.0010% (출력)	0.0024% (입력)
시스템 자원 부하율	0.0005%	
경로 설정 실패율	0.0010%	
관리 트래픽 이용률	0.0943%	

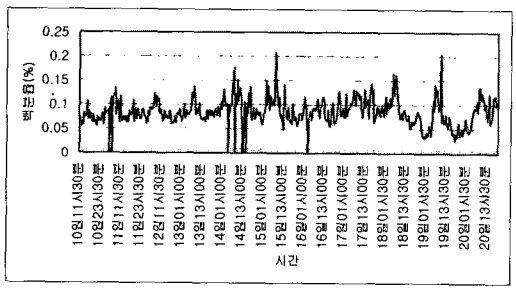
(그림 9)는 피관리 시스템 134.75.62.2에 대하여 심화 분석을 수행한 결과이다. 분석 항목은 선로 이용률이며 분석 방법은 일일 분석으로 각 시간대별로 평균 선로 이용률을 계산하여 보여주는 분석 방법이다. (그림 9)를 보면 134.75.62.2가 07시부터 09시를 제외하고는 모두 80%이상의 선로 이용률을 보이는 것을 알 수 있다.



(그림 9) 심화 분석 예 - 일일 분석 (134.75.62.2)
(Fig. 9) The radar diagram of hourly utilization (134.75.62.2)



(그림 10) 심화 분석 예 - 에러율 (134.75.62.2)
(Fig. 10) The line graph of error rate (134.75.62.2)



(그림 11) 심화 분석 예 - 비방송형 패킷 비율 (134.75.62.2)
(Fig. 11) The line graph of non-unicast packet rate (134.75.62.2)

(그림 10)과 (그림 11)은 각각 134.75.62.2에 대한 정상 패킷에 대한 이상 패킷의 비율, 전체 패킷에 대한 비방송형 패킷에 대한 비율을 표시하는 분석 결과 그래프이다. (그림 10)을 보면 전체적으로 이상이 있는 패킷의 비율이 높다는 것을 알 수 있다. 이상 패킷은 경로 설정 에러 패킷, 에러 패킷, 폐기 패킷으로 되어 있으므로 경로 설정에 문제가 있거나 선로에 문제가 있거나 피관리 시스템의 메모리가 부족할 가능성이 있다. (그림 11)은 전체 패킷에 대한 비방송형 패킷의 비율로 전체 패킷에서 비방송형 패킷이 비율이 많은 것을 알 수 있다.

5. 결 론

본 논문에서는 인터넷 상에서 효율적인 망 관리를 지원하기 위해 기존의 분석 항목들을 이용하여 인터넷 분석 파라미터 추출 시스템을 설계하고 구현하였다. 인터넷 분석 파라미터 추출 시스템에서는 기본 분석과 심화 분석으로 분석 단계를 나누어 관리자들이 쉽게 관리 행위를 수행하도록 하였으며, 월별/주별/일별/시간별 분석을 통하여 일정기간 수집된 데이터에 대해 체계적인 분석이 가능하도록 설계하였다. 분석을 위해 사용하는 인터넷 분석 파라미터는 크게 유통 트래픽 분석 파라미터와 인터페이스 유통 패킷 분석 파라미터, 패킷 트래픽 및 관리 트래픽 분석 파라미터, 구성 관리 파라미터로 구분된다. 이들 파라미터를 추출하기 위한 인터넷 분석 파라미터 추출 시스템은 크게 수집 요구 처리 모듈과 분석 요구 처리 모듈로 나뉜다.

수집 요구 처리 모듈은 인터넷 상의 여러 피관리 시스템들로부터 주기적으로 관리 정보를 추출하는 부분이다. 피관리 시스템으로부터 분석에 필요한 관리 정보를 자동적으로 추출하기 위해 폴링 스크립트 생성기를 통해 폴링 스크립트를 생성한다. 그리고, 사용자로부터 시작, 종료 시간을 입력 받아서 이를 시간 처리 모듈에서 처리하여 주기적으로 관리 정보를 수집할 수 있다. 수집을 위한 프로토콜로는 TCP/IP 망 관리 표준인 SNMP를 사용하고 있다.

분석 요구 처리 모듈은 수집 요구 처리 모듈에서 수집한 관리 정보를 입력으로 하여 인터넷 분석 파라미터를 추출하는 부분이다. 인터넷 분석 파라미터 추출 시스템은 기본적으로 하나의 피관리 시스템만 분석하는 것이 아니라 다수의 피관리 시스템을 분석하도록 설계 및 구현되었다. 그러므로 관리자들은 다수의 피관리 시스템을 분석할 경우 모든 피관리 시스템을 분석하는 것이 아니라 각 피관리 시스템에 대한 기본적인 항목을 검사해서 문제가 있는 피관리 시스템을 판별해내야 한다. 이를 위해 인터넷 분석 파라미터 추출 시스템에서는 기본 분석을 제공한다. 기본 분석에서는 피관리 시스템의 선로 이용률, 가동률, 다운 횟수 등을 분석하여 이상이 있다고 판단되는 시스템을 분리해낼 수 있다. 기본 분석외에도 심화 분석을 통해서 관리자는 특정 피관리 시스템에 대해 자세히 분석할 수 있다. 심화 분석에서 제공되는 분석 항목들은 2장에 정의된 분석 파라미터들이며 이를 일별/주별/월별/시간대별로 세분화하여 분석할 수 있도록 구현되었다.

SNMP는 단순 MIB 변수들에 대한 정의와 이들 정보의 송수신에 관련된 프로토콜이므로 관리자가 이들 정보를 실제 관리에 도움이 되는 정보로 변환하고자 한다면 우선 이들 변수들 중 추출하고자 하는 정보를 가지고 있는 MIB 변수들을 알아내야 한다. 또한 SNMP는 정보를 누적하여 저장하고 있지 않으므로 관리자는 이를 일정 기간동안 주기적으로 수집하는 과정을 거쳐야 한

다. 이렇게 저장된 정보를 조합하여 계산하는 과정을 통해 비로소 관리자는 관리에 도움이 되는 정보를 도출해 낼 수 있다. 관리자들이 이러한 사항을 모두 파악하여 분석 정보를 도출해내는 것은 쉬운 일이 아니다. 본 논문에서 설계 및 구현한 인터넷 분석 파라미터 추출 시스템은 복잡한 수집, 분석 과정들을 분석 시스템 내부에서 처리하도록 설계 및 구현하여 관리자가 최소한의 정보만으로 다양한 분석 정보를 도출해 낼 수 있다. 망 관리자들은 인터넷 분석 파라미터 추출 시스템을 통해 추출된 분석 파라미터를 이용해서 인터넷 망에 대해 분석 파라미터 별로 체계적으로 분석 결과를 도출할 수 있고, 피관리 시스템의 관리 정보를 일정기간 주기적으로 수집하여 보다 장기적인 인터넷 망 관리를 할 수 있을 것이다. 또한 선로의 증속이나 망 구축 및 설비 확장시에 도움이 되는 유용한 지표로 사용할 수 있을 것이다.

참 고 문 헌

[1] H.J.Kang, J.W.Chung, J.H.Ahn, S.J.Ahn, "The Design and Implementation of MIT for Management Information Base," Proceedings of 7th International Joint Workshop on Computer Communications, pp.357-364, 1992.

[2] Olga Havel, Ahmed Patel, "Design and Implementation of a Composite Performance Evaluation Model for Heterogeneous Network Management Applications," International Journal of Network Management, Vol.5, No.3, pp.25-46, 1995.

[3] J. Case, M. Fedor, M. Schoffstall, "Simple Network Management (SNMP)," RFC 1157, 1990.

[4] 한정수, 안성진, 정진욱, 박형우, "웹 응용 서비스 관리를 위한 성능 관리자 시스템의 설계 및 구현", 정보처리논문지, 제1권, 제5호, pp.161-171, 1998.

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

[6] Allan Leinwand, "Accomplishing Performance Management with SNMP," INET'93, pp.CEA-1~CEA-5, 1993.

[7] J. Case, Craig Partridge, "Case Diagram: A first step to Diagrammed Management Information Bases," ACM Computer Communication Review, 1989.

[8] 신상철, "SNMP를 기반으로 하는 인터넷 성능 파라미터 추출 시스템의 설계 및 구현", 석사학위논문, 성균관대학교, 1998.

[9] 안성진, "TCP/IP 망 관리를 위한 시스템 분석 파라미터 계산 알고리즘", 박사학위논문, 성균관대학교, 1998.

[10] John Blommers, "Practical Planning for Network Growth," Hewlett-Packard Professional Books, 1996.

신 상 철

e-mail : july4th@maru.comtec.re.kr

1996년 성균관대학교 정보공학과 졸업(학사)

1998년 성균관대학교 대학원 정보공학과 졸업(석사)

1998년~현재 콤텍시스템 기술연구소 연구원

관심분야 : 네트워크 관리, 트래픽 분석, 유닉스 네트워킹

안 성 진

e-mail : sjahn@songgang.skku.ac.kr

1988년 성균관대학교 정보공학과 졸업(학사)

1990년 성균관대학교 대학원 정보공학과 졸업(석사)

1998년 성균관대학교 대학원 정보공학과 졸업(박사)

1990년~1995년 시스템공학연구소 연구원

1999년~현재 성균관대학교 컴퓨터교육학과 교수

관심분야 : 네트워크 관리, 분산 시스템, 고속 통신

정 진 욱

e-mail : jwchung@songgang.skku.ac.kr

1974년 성균관대학교 전기공학과 졸업(학사)

1979년 성균관대학교 대학원 전자공학과 졸업(석사)

1991년 서울대학교 대학원 계산통계학과 졸업(박사)

1982년~1985년 한국과학기술 연구소 실장

1981년~1982년 Racal Milgo Co. 객원연구원

1985년~현재 성균관대학교 전기전자 및 컴퓨터공학부 교수

관심분야 : 네트워크 관리, 네트워크 보안, 고속 및 무선 통신 프로토콜