

## SNMP를 이용한 원격 모니터링 및 제어 시스템의 설계 및 구현

안성진

성균관대학교 사범대학 컴퓨터교육과

### 요 약

본 논문에서는 SNMP를 이용하여 Window나 NT환경에서 동작하는 PC시스템을 관리하기 위하여 MIB를 정의하고 이를 모니터링 및 제어하는 관리 시스템을 설계 및 구현하였다. 제안된 시스템은 피관리 시스템의 상태를 제어하는 제어 시스템과 실시간 모니터링 및 프로세스 제어를 담당하는 모니터링시스템으로 구성되어 있다. 제어 시스템은 피관리 시스템의 구성정보 제어 및 설정과 피관리 시스템의 장애발생시 이를 제어하기 위한 백업 및 복구를 담당한다. 모니터링 시스템은 피관리 시스템의 현재의 동작 상태를 모니터링하고 실시간으로 실행중인 프로세스를 제어 및 새로운 작업을 실행시키는 기능을 담당하는 부분이다. 본 논문에서는 전체적인 관리 시스템과 피관리 시스템사이의 구조 및 동작과정을 규정하고 스크린 분할 및 분석 기법을 사용하여 모니터링의 성능을 향상시키는 방안을 제시하고 있다.

## Design and Implementation of Remote Monitoring and Controlling System using SNMP

Seong-jin Ahn

### ABSTRACT

In this paper, it is designed and implemented the management system to monitor and control PCs running on MS Windows or NT and define some MIBs using SNMP. The proposed system has controlling functions to control the status of PC and monitoring functions to have real-time monitoring and control processes. The controlling system supports update and setting of the configuration information of managed systems and backup/restore the information when it happens to be some faults. The monitoring system has some functions such as monitoring the processes of the PC, controlling the process on PC, and invoking a new job. This paper proposes a way of enhancing the performance of monitoring capabilities by screen partitioning and analysis techniques.

## I. 서 론

컴퓨터를 마치 자기 앞에 있는 컴퓨터처럼 관리 및 제어할 수 있는 기술의 필요성이 점점 대되고 있다. 정보화 사회로 접어들면서 컴퓨터 통신기술이 급속히 발전되었으며 이에 발맞추어 컴퓨터 네트워크를 이용하는 사용자들의 요구사항이 점점 복잡, 다양화되어 가고 있는 추세이다.[1][2] 또한 초고속 네트워크 환경에서 제공되는 대부분의 응용 서비스들은 대용량의 데이터와 실시간 처리를 요구하는 멀티미디어 서비스로 변해가고 있다. 이를 위해서는 기존의 자원 관리 방식에서 벗어나 응용 서비스를 대상으로 하는 새로운 관리 방식이 필요하게 된다.[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 단순 네트워크 관리 프로토콜 (SNMP : Simple Network Management Protocol)를 이용한 관리 시스템의 필요성이 대두되고 있는 실정이다.[4]

TCP/IP프로토콜을 기반으로 운영되는 네트워크에서 트래픽 분석을 위한 관리 표준으로 사용되는 SNMP는 호스트, 라우터, 허브, 스위치, 게이트웨이 등의 네트워크 구성 요소에 대한 관리 정보가 논리적으로 네트워크를 통해 원격지 관리자들에 의해 조사되거나 변경될 수 있게 지원하는 간단한 프로토콜을 정의한다. 특히, MIB(Management Information Base)과 함께 관리 정보의 구조를 기술하는 관련 표준들과 같이 본 표준은 TCP/IP를 기반으로 하는 네트워크들을 관리하고 운영 가능한 구조와 시스템을 제공한

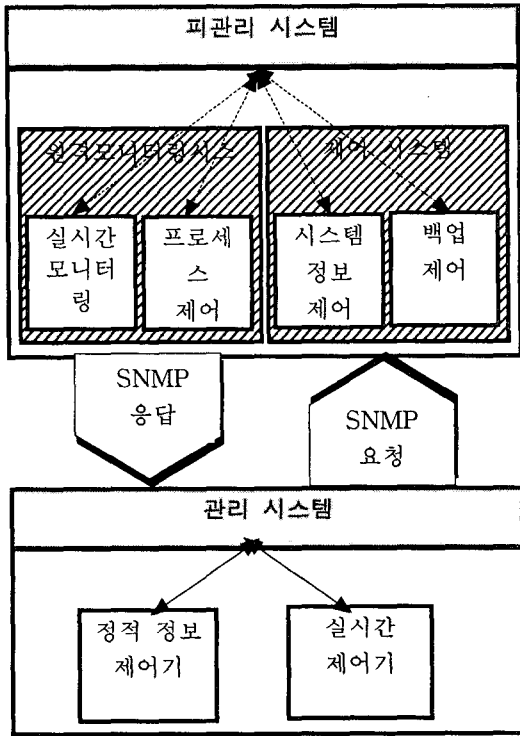
다.[5][6]

TCP/IP를 기반으로 하는 인터넷의 전산망관리를 위한 MIB는 관리객체를 기술한다. NT시스템의 경우 NT의 DHCP서버나 WINS서버, FTP서버, Gopher서버, HTTP서버와 관련된 정보를 제공하는 MIB로 입출력 패킷이나 해당 장비의 로그인 정보를 보여주는 항목을 갖고 있다. 본 논문에서 구성정보나 백업, 복구, 모니터링을 위한 정보를 관리하기 위하여 추가적인 MIB 변수를 설정하였다.

## II. 원격 모니터링 및 관리 시스템

원격 모니터링 및 관리 시스템은 그림1과 같이 크게 피관리국의 시스템관련정보를 조회 및 설정할 수 있는 제어시스템과 피관리국의 화면을 실시간으로 모니터링 및 원격지에서 피관리국의 프로세스를 제어하는 원격 모니터링 시스템, 그리고 피관리국의 상태를 분석하고 이를 이용하여 백업 및 복구를 하는 시스템으로 분류할 수 있다.

먼저, 제어 시스템은 피관리 시스템의 시스템, 운영체제, 네트워크 정보 및 백업/복구를 위한 정보를 관리하게 된다. 이 정보들은 정적인 구성 정보로서 피관리 시스템 초기화 시에 MIB 트리로 구성되며 관리국에서 이 정보들을 조회하거나 설정할 수 있는 시스템 관리 기능과 주기적으로 피관리 시스템의 상태를 수집하고 이를 분석하여 피관리 시스템의 상태가 불안정할 경우 백업을 실행하는 기능을 제공한다. 원격 모니터링 시스템의 경우 관리 시스템은 피관리 시스템의 화면을 실시간으로 모니터링 하는 기능과 실행 프로세스를 실시간으로 실행시키고 이를 직접 원격지에서 모니터링하는 기능을 제공한다.



(그림 1) 원격 모니터링 및 관리시스템 구조

(Figure 1) Structure of Remote Monitoring and Management System

관리 시스템으로부터 화면 모니터링 요청이 올 경우 피관리 시스템은 현재의 화면 정보를 수집하여 제공을 하게 되며 원격 프로세스 제어 요청이 올 경우 피관리 시스템의 프로세스 정보를 추출하여 이를 기반으로 하여 프로세스제어를 하게 된다.

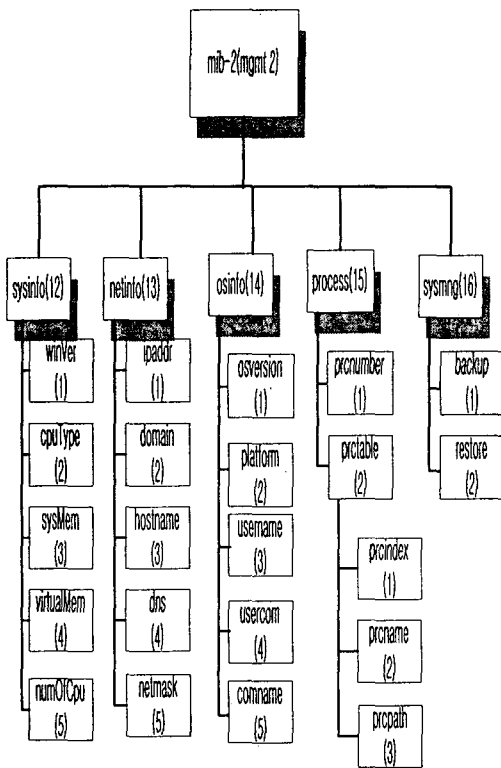
## 2.1 제어 시스템

제어 시스템의 기능은 크게 피관리 시스템 정보 조회와 피관리 시스템 설정, 그리고 장애에 대처하기 위한 백업과 복구로 크게 나누어 볼 수 있다.

제어 시스템은 원격지의 피관리 시스템 관련 정보들을 조회 및 수정을 할 수 있는데 해당 정보로는 시스템 관련 정보와 네트워크 관련 정보, 운영체제와 관련된 정보가 있다. 또한, 피관리 시스템의 구성정보를 주기적으로 수집 및 분석하여 장애에 대한 대처를 하는 백업 및 복구 기능이 있다. 피관리 시스템은 주기적으로 시스템 정보를 수집하여 분석하게 되며 누적 정보가 임계값을 넘을 경우 이를 시스템이 불안정한 상태로 인식하고 백업을 수행하게 된다. 백업 대상으로는 레지스트리, 시스템 구성 그리고 사용자 구성이 있다. 복구는 피관리 시스템의 상태가 불안정할 경우 백업해 놓았던 백업 정보를 이용하여 수행된다. 이와 같이 백업 및 복구 기능은 피관리 시스템의 레지스트리 정보 및 일반적인 시스템 정보를 백업하고 장애 발생시 이를 복구할 수 있는 기능으로 관리 시스템에서 해당 피관리 시스템에 백업 및 복구 명령만 내리면 해당 피관리 시스템에서 백업 및 복구가 수행된다.

TCP/IP망에서 네트워크관리 표준프로토콜인 SNMP를 이용하여 네트워크를 관리하기 위해서는 MIB가 필요하게 된다. 그러므로 SNMP를 이용하여 피관리 시스템을 관리하기 위해서 본 시스템에서는 표준 MIB에 추가적으로 MIB변수를 추가시켰다.

그림 2에서 보는 바와 같이 시스템 관련정보를 위한 MIB와 네트워크 정보를 위한 MIB, 운영체제의 정보를 위한 MIB, 현재 실행중인 프로세스들을 관리하기 위한 MIB, 그리고 시스템의 상태를 모니터링하여 백업이나 복구를 하기 위한 MIB 변수그룹을 표준 MIB그룹인 mib-2에 추가시켰으며 본 관리시스템의 관리 행위는 이 MIB 변수들을 중심으로 이루어지게 된다.

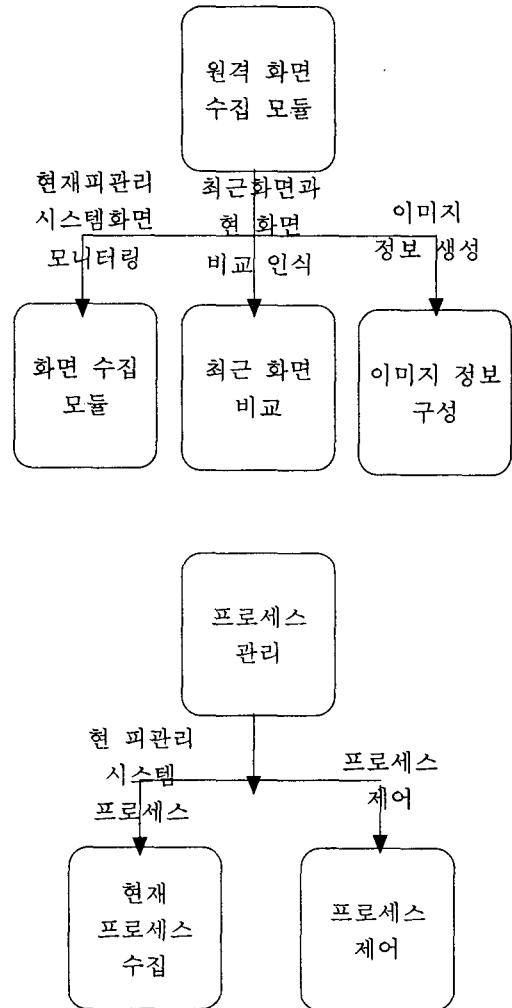


(그림 2) 추가된 MIB 트리의 구조

(Figure 2) Structure of Added MIB Tree

## 2.2 원격 모니터링 시스템

원격 모니터링시스템의 기능은 크게 관리자가 현재 관리 대상 시스템의 화면을 실시간으로 모니터링할 수 있는 기능과 현재 피관리시스템에서 수행중인 프로세스의 기본 우선순위나 쓰레드의 수, 형태, 실행 경로명 등의 정보조회 및 실행중인 프로세스의 작업 중단, 새로운 프로세스 실행 등의 작업을 원격지에서 수행을 하고 이를 피관리 시스템의 화면을 모니터링 함으로써 확인할 수 있는 기능을 제공한다. 전체적인 원격 모니터링 시스템의 구조는 아래 그림 3과 같다.



(그림 3) 원격 모니터링 시스템의 처리 구조

(Figure 3) Structure of Remote Monitoring Processing System

그림 3에서 보듯이 원격모니터링 시스템은 원격 화면 수집 모듈과 프로세스 제어 모듈로 나누어지며 각 모듈의 기능은 아래와 같다.

### 2.2.1 원격 화면 수집 모듈

이 모듈은 현재 시스템의 화면을 수집하는 화면

수집 모듈과 가장 최근에 이 모듈이 호출되었을 때의 이미지 정보와 현재 수집한 이미지 정보를 비교하는 최근 화면 비교 모듈 그리고 이 두가지 정보를 이용하여 패킷을 구성하는 이미지 정보 구성 모듈로 구성된다. 화면 수집 모듈의 경우 주기적으로 호출이 되며, 이때 화면 정보를 모두 관리시스템으로 전송을 할 경우 많은 성능저하가 발생하게 되며 이를 최소화하기 위하여 화면 분할 기법을 이용한다. 피관리 시스템의 화면을 여러 개의 영역으로 분할하여 최근 이미지와 비교하여 변화한 부분의 정보만을 전송하고 또, 설정 주기에 따라 분할 영역의 크기를 변화시킴으로써 성능저하를 최소화한다.

### 2.2.2 프로세스 제어

이 모듈은 현재 실행중인 프로세스의 정보를 수집하는 현재 프로세스 수집 모듈과 실행중인 프로세스의 작업을 중단하거나 새로운 응용 프로그램을 실행하는 프로세스 제어 모듈로 구성되어 있는데, 실행중인 프로세스의 경우 프로세스 현 정보 수집을 이용하여 파악을 하게 된다.

## III. 모니터링 및 제어 시스템 설계

### 3.1 피관리 시스템의 추가 MIB와 분석항목

피관리 시스템의 관리를 위해서 추가된 MIB는 sysinfo, netinfo, osinfo, process, sysmng 등으로 구성된다. 이들 MIB 정보는 시스템 구성 정보 파일과 SDK에서 제공되는 함수를 통해서 저장된다.

〈표 1〉 추가 MIB 변수

〈Table 1〉 Added MIB Variables

객체명	객체식별자	설명
sysInfo	1.3.6.1.2.1.12.1	윈도우 버전 정보
cpuType	1.3.6.1.2.1.12.2	CPU 형태 정보
sysMenu	1.3.6.1.2.1.12.3	메모리 양 정보
virtualMem	1.3.6.1.2.1.12.4	가상 메모리 양 정보
numOfCpu	1.3.6.1.2.1.12.5	CPU 수
ipAddr	1.3.6.1.2.1.13.1	IP 주소
domain	1.3.6.1.2.1.13.2	도메인 이름
hostname	1.3.6.1.2.1.13.3	호스트 이름
dns	1.3.6.1.2.1.13.4	DNS의 IP 주소
netmask	1.3.6.1.2.1.13.5	네트워크 마스크
dsVersion	1.3.6.1.2.1.14.1	운영체제 버전 정보
platform	1.3.6.1.2.1.14.2	플랫폼 정보
username	1.3.6.1.2.1.14.3	접속한 사용자 이름
userCom	1.3.6.1.2.1.14.4	접속한 컴퓨터 이름
comName	1.3.6.1.2.1.14.5	컴퓨터 이름
apNumber	1.3.6.1.2.1.15.1	수행중인 프로세스 수
apName	1.3.6.1.2.1.15.2.1	수행중인 프로세스 이름
apPath	1.3.6.1.2.1.15.2.2	수행중인 프로세스 경로명
backup	1.3.6.1.2.1.16.1	시스템과 레지스트리의 백업 정보
restore	1.3.6.1.2.1.16.2	복구 정보

#### (1) sysinfo MIB

피관리 시스템과 관련된 정보로서 윈도우 버전, CPU 형태 등의 정적인 정보와 관련된 MIB이다.

#### (2) netinfo MIB

피관리 시스템의 네트워크와 관련된 정보로서 IP 주소, 도메인 이름, DNS 서버 등이 들어가며 관리 시스템에서 이를 설정할 수 있다.

### (3) osinfo MIB

피관리 시스템의 운영체제와 관련된 정보로 하드웨어 플랫폼, 운영체제 버전 등의 정보와 관련된 MIB이다.

### (4) process MIB

실시간으로 수집한 현재 피관리 시스템에 실행중인 프로세스 정보나 원격 실행과 관련된 MIB이다.

### (5) sysmng MIB

피 관리 시스템 장애 발생 시 이를 복구하기 위한 복구/백업 정보와 관련된 MIB이다.

## 3.2 원격 모니터링 및 제어 시스템의 상태 흐름 및 동작

그림 4는 서버 시스템의 전체적인 상태 천이도를 보여주고 있다. 원격 모니터링 및 제어 시스템을 위한 서버 시스템의 상태는

S\_INITIAL, S\_MESSAGE, S\_SYSMON, S\_CONFIG, S\_BACKUP, S\_MONITOR, S\_REALTIME, S\_CAPTURING, S\_PROCESS로 구성되어 있다. S\_INITIAL상태

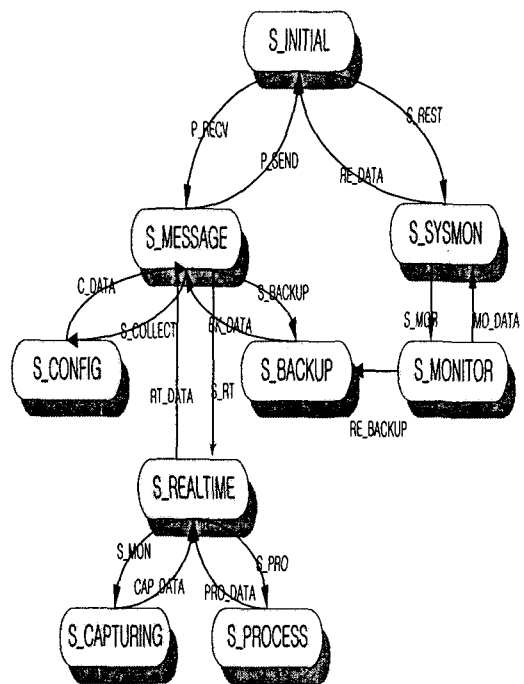
는 사스택의 초기 상태를 설정하고

S\_SYSMON의 상태로 이동하여 시스템의 상태를 주기적으로 감시하는 S\_MONITOR의 상태로 이동하게 된다. S\_MONITOR의 상태에서는 주기적으로 CPU 사용량이나 메모리 사용량, 쓰레드의 수 등을 이용하여 시스템의 상태를 파악한다. 만약 분석 결과 클라이언트의 상태가 불안정한 상태로 판단이 되면,

S\_BACKUP 상태로 전이하여 시스템의 백업을 요청하게 된다. 또한, 클라이언트로부터 패킷을

받았을 경우, S\_MESSAGE의 상태로 이동을 하게 되며 패킷을 분석하여 구성정보의 설정과 관련된 정보라면 S\_CONFIG의 상태로 이동하게 된다. 만약 실시간과 관련된 화면 수집이나 프로세스 제어와 관련된 메시지라면

S\_REALTIME으로 이동을 하게 되며 여기서 각 요구사항에 해당하는 S\_CAPTURING이나 S\_PROCESS의 상태로 이동을 하게 된다.



(그림 4) 서버의 상태 천이도

(Figure 4) State Transition Diagram of Server

## Ⅳ. 모니터링 및 제어 시스템 구현

### 4.1 구현 환경

시스템을 구현한 환경은 크게 운영체제, 사용언어, 사용프로토콜로 나눌 수 있다. 먼저 운영체제

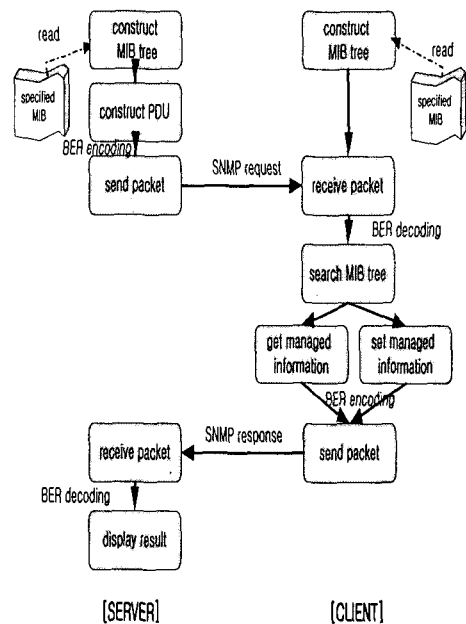
에 대해 살펴보면 관리 시스템과 피관리 시스템 모두 Win95이상이나 NT4.0 이상의 win32환경에서 동작하도록 구현되었으며 Windows SDK를 이용하여 구현하였기 때문에 이를 지원하는 어떠한 win32환경에서도 동작할 수 있다.[7] 사용언어로는 원격 모니터링 및 관리 시스템과 관리시스템 모두 Windows SDK를 이용하여 구현하였으며 사용프로토콜은 TCP/IP망의 네트워크 관리 프로토콜인 SNMP를 이용하여 관리 시스템과 피관리 시스템간의 통신이 이루어진다.

#### 4.2 관리 시스템의 구현

전체 관리시스템의 관리 구조는 그림 5와 같다. 관리 시스템은 기존의 표준 MIB에 추가적으로 피관리 시스템의 정보와 프로세스 관련 정보 복구를 위한 정보 및 모니터링을 위한 정보를 갖고 있는 MIB를 추가하여 피관리 시스템은 이를 읽어 들여 새로운 MIB 트리를 구성한다. 관리 시스템은 관리하고자 하는 시스템에 SNMP를 이용하여 피관리 시스템으로 관리하고자 하는 정보를 요청하거나 피관리 시스템의 설정을 요청을 하게 된다.

관리 시스템은 피관리 시스템으로부터 받은 정보들을 기반으로 하여 피관리 시스템의 상태를 분석하게 되며 만약 피관리 시스템의 상태가 관리 시스템에서 설정한 안전기준치(threshold)를 초과할 경우 피관리 시스템의 백업을 요청하게 된다.

시스템의 상태가 불안정할 경우 주기적으로 백업을 함으로써 피관리 시스템에 장애가 발생하였을 경우 이 백업정보들을 이용하여 가장 최근의 시스템의 상태로 복구시킴으로서 관리 대상들의 상태를 효과적으로 관리 할 수 있게 된다.

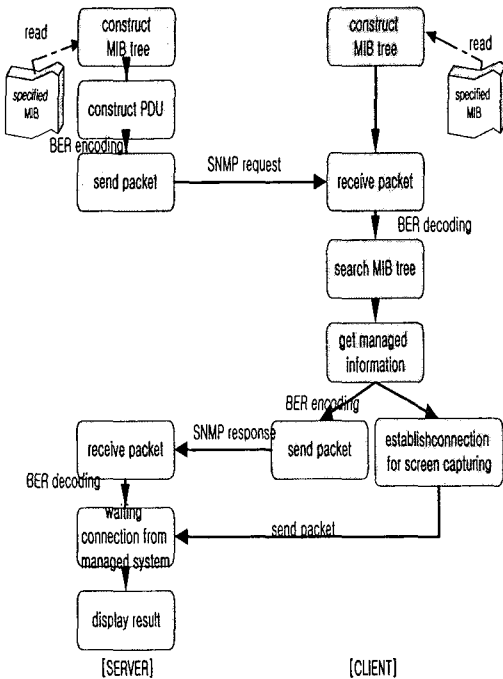


(그림 5) 관리 시스템의 구현 구조  
(Figure 5) Implementation Structure of Management System

#### 4.3 모니터링 시스템의 구현

원격모니터링 시스템의 전체 관리 구조는 그림 6과 같다.

원격모니터링 시스템은 과관리 시스템으로부터 모니터링을 요청하는 SNMP패킷이 도착했을 경우 현재의 화면 정보를 수집하고 이를 스크린 분할 및 분석 기법을 이용하여 이전의 스크린 정보와 비교하여 변화된 부분만을 전송하게 된다. 스크린 분할 및 분석 기법이란 매우 빠른 주기로 스크린 수집 요청이 도착할 경우 전체 화면 이미지 모두를 관리 시스템으로 전송하는 것이 아니라 이전의 화면 정보와 비교하여 변화된 부분의 정보만을 전송하는 방식을 말한다. 즉, 전송되는 정보



(그림 6) 원격 모니터링 시스템의 구현 구조  
(Figure 6) Implementation Structure of Remote Monitoring System

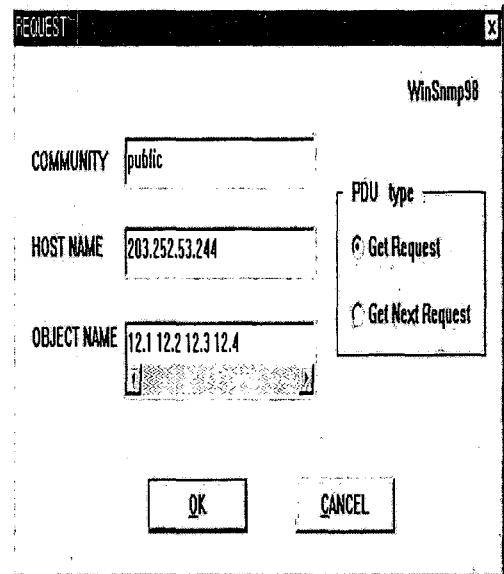
는 변위 부분만이 전송되어 지는 것이다. 이러한 방법을 사용함으로써 큰 용량을 차지하는 이미지 정보의 전송량을 최소화하고 관리 시스템에서 정보의 전송 지연 시간을 최소화하게 된다.

프로세스 제어 기법의 경우 피관리 시스템은 화면 추출(snapshot)기법을 이용하여 현재 실행 중인 프로세스의 정보를 관리 시스템으로 전송하게 되며 이 정보를 이용하여 전체 관리 시스템의 요구를 제어하게 된다.

#### 4.4 결과화면

피관리 시스템의 시스템 정보에는 윈도우 버전, CPU 타입, 시스템 메모리, 가상 메모리, 사용자

이름, PC에 등록된 사용자 이름 등이 있으며, 프로세스 정보에는 현재 실행 중인 프로세스의 수, 현재 실행 중인 프로세스의 이름, 현재 실행 중인 프로세스의 경로 등이 있다. 또한 장애 복구를 위한 백업, 및 복구 수행을 위한 정보도 있다. 그림 7은 관리자 시스템에서 관리 정보를 피관리 시스템으로 요구하는 화면을 보여주고 있다.

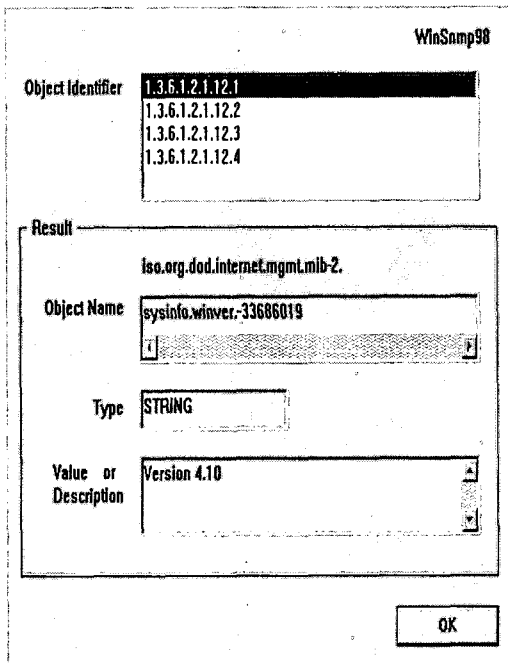


(그림 7) 관리 정보 요구 화면  
(Figure 7) Screen for Management Information Request

관리자로부터의 요청을 수신한 피관리 시스템은 자신에게 설정된 정보를 반환해야 한다. MIB 객체의 ID 형태로 요구한 정보에 대해서 반환된 값은 그림 8과 같은 형태로 관리자 화면에 보이게 된다.

그림 8에서는 피관리 시스템에서 보내온 시스템 정보를 출력하고 있다. 객체에 대한 내용을 더블 클릭하면 시스템 정보를 "Value or Description" 필드에서 출력한다.





(그림 8) 관리 정보에 대한 응답 화면

(Figure 8) Screen for Management Information Response

## V. 결 론

본 논문은 TCP/IP 표준 네트워크 관리 프로토콜인 SNMP의 기능 확장으로, SNMP프로토콜을 사용하여 피관리 시스템의 구성정보를 제어하고 주기적으로 피관리 시스템의 상태를 모니터링, 장애 발생 시 자동적인 백업 및 복구를 지원하는 시스템을 설계하고 구현하였다. 또한, 실시간으로 관리하고자 하는 시스템의 상태를 파악 및 프로세스를 제어함으로써 효율적으로 관리시스템을 구현하였다. MIB 관리를 위한 MIB 변수를 추가하여 트리 형태의 구성도로 제시하였고, 주기적인 백업이 아닌 시스템의 상태를 반영한 백업 기법을 소

개하였다. 또한 효율적인 화면 수집을 위한 화면 분할 및 분석 기법을 이용하여 전송 지연 시간을 최소화하였으며 관리 시스템과 피관리 시스템사이의 구조를 제시하고 그에 대한 동작 과정을 보였다. 구현된 모델은 SNMP표준 프로토콜을 사용하여 구현함으로써 TCP/IP 기반으로 설계된 어떠한 네트워크에서도 이용이 가능하며 피관리 시스템 대부분의 설정 정보를 관리시스템을 통하여 제어할 수 있으므로 대규모의 네트워크 관리에 있어서 적합한 모델로 사용되어 질 수 있다.

## 참 고 문 헌

- [1] John Blommers, Practical Planning for Network Growth, Prentice Hall, 1996
- [2] Jung Soo Han, Seong Jin Ahn, Jin Wook Chung, Hyung Woo Park, Web Based Performance Manager for a Web Server, APCC97, pp.272-276, 1997
- [3] 조규억, 안성진, 정진욱, "SNMP를 이용한 PC 관리 시스템의 설계 및 구현", 한국정보교육학회, 제3권, 제1호, pp. 86~93, 1999
- [4] J. Case, M. Fedor, M. Schoffstall, J. Davin, Simple Network Managment Protocol, RFC1157, 1990
- [5] K. McCloghrie, M. Rose, Management Information Base for Network Management of TCP/IP-based Internets : MIB-II, RFC1213, 1991
- [6] Alexander Clemm, Adding Value to MIBs : Relationship Layer for Management Platforms, International

Journal of Network Management, Vol.  
5, No. 3, pp.127-137, 1995

[7] Charles Petzold, Programming  
Windows, Microsoft Press, 1999



### 안 성 진

1988년 성균관대학교 정보공  
학과 (공학사)

1990년 성균관대학교 정보공  
학과 (공학석사)

1998년 성균관대학교 정보공  
학과 (공학박사)

1990~1995년 시스템공학연구소 연구원

1999~현재 성균관대학교 컴퓨터교육과 교수

관심분야 : 인터넷 관리, 전자상거래 시스템, 네  
트워크 보안