

네트워크 통합관리와 리눅스를 이용한 NMS구현

황규홍 · 여현

순천대학교 정보통신학과

Network Unified Management and Implementation of Linux NMS

Kyu-hong Hwang, Hyun Yoe

Sunchon National University

E-mail : hkh91@mail.posdata.co.kr

요 약

초고속 통신망이 발달함에 따라 대기업은 물론, 학교와 중소기업에도 네트워크로 연결되어 업무 및 학습과 행정업무를 처리하고 있다. 인터넷을 이용한 재택근무, 재택교육 등이 발달하고 있는 시점에서 안정적이고 효율적인 네트워크환경을 제공하기 위해서는 네트워크상에 존재하는 다양한 자원들을 모니터링하고 제어하는 네트워크의 관리의 개념이 필요하게 되었다. 하지만, 대부분의 기업체나 학교에서는 구축비용측면에서 이를 투자하기를 꺼려하고 있다.

이에 본 논문에서는 중소기업 및 학교업무에서 일반적으로 사용되고 있는 MRTG(Multi Graphic Roter Grapher)를 연계하여 웹을 이용한 손쉽게 망을 관리할 수 있는 툴을 perl을 이용하여 구현하였다. 장애의 대부분이 네트워크 자원관리와 실시간 로그관리를 이용할 경우 대부분의 장애를 미연에 방지할 수 있다는 점에 착안하여 텍스트를 처리함에 있는 탁월한 기능을 가진 perl을 이용하여 로그처리 데몬프로그램을 작성하였고, 자원관리와 이력관리를 위해서는 MySQL을 이용하였다.

키워드

NMS,LINUX,PERL,MRTG

I. 서 론

최근 e-business의 급속한 부상으로 인해, 네트워크가 기업의 핵심 인프라로 자리 매김함에 따라 네트워크의 마비가 곧 업무의 마비로 이어질 정도로 기업에 직접적인 영향을 미치게 되었다. 매년 네트워크 다운으로인해 발생하는 손실이 100만달러를 넘어서 계속 증가추세에 있으며 각 가정마다 초고속 통신망의 확산으로 인해 네트워크 사용이 계속 증가하는 것은 당연한 일일 것이다. 또한 멀티미디어 데이터 처리의 증가로 대용량의 데이터를 처리하기 위해서는 초고속·대용량의 네트워크가 필요할뿐 아니라 개방형 환경하에서는 각각 상이한 정보통신 구성요소들을 통합관리해야 하는 어려움에 처해 있다.[1]

이러한 이유로 본 논문에서는 많은 네트워크장애들이 자원관리와 실시간 로그관리를 통해 많은 장애를 사전

에 미연에 방지할 수 있다는 점에 착안하여 많은 중소기업에서 사용하는 MRTG(Multi Router Traffic Grapher)를 MySQL과 연동하여 환경설정 및 설정 화면등을 웹으로 구현하여 굳이 많은 비용을 들이지 않고도 손쉽게 네트워크 망을 관리할 수 있는 NMS를 구현해 보았다. 또한 오픈소스의 장점인 소스공유를 통해 온라인상의 많은 사람들과 기능에 대한 개선을 용이하게 할수 있다.

II. 본 론

2.1 perl

Perl은 더구나 HTML이나 사용자입력과 같은 텍스트를 다루는데 아주 강력한 기능을 가지고 있으므로 문자열 위주의 데이터를 다루기에는 최적의 언어라 할

수 있으며, UN*X, MVS, VMS, MS-DOS, Macintosh, OS/2, Amiga, Windows NT 등 여러 가지 Operating system에 Porting되어 있으므로 소스파일의 이식성이 뛰어나다. perl 이라는 언어는 C와 C++이 가지는 문자열과 메모리관리에 있어 복잡난해한 개념들보다는 언어 자체의 유용성에 중점을 둔 언어이다. 즉 프로그래머가 표현하고자 하는데 있어 여러 가지 제약이 없이 자유롭게 서술할 수 있는 언어이다.[5]

2.2 SNMP의 구조와 동작

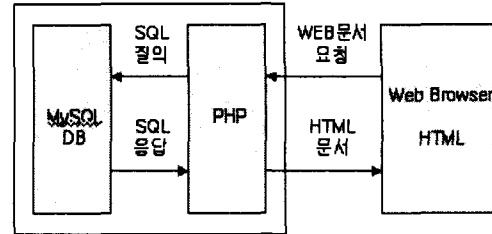
SNMP는 망관리자가 위치하는 매니저의 영역인 관리국(Management Station), 매니저의 요청에 대해 적절한 행동을 취하고, 매니저에게 응답을 하는 피관리 에이전트(Managed Agent), 망관리 대상에 개념적 구조체인 MIB, 매니저와 에이전트 사이의 통신을 위한 프로토콜인 SNMP등 4개의 요소를 가지고 동작하게 된다.[2,3], SNMP 버전은 1,2,3으로 크게 분류된다. 버전1은 SNMP의 기본동작인 GET,SET,TRAP을 지원한다.[3,7] 버전 1은 두가지 큰 문제점을 가지고 있는데, 이는 보안문제를 다루지 않는다는점과, 라우팅 테이블의 정보를 요청할 때 반복적인 정보의 요청으로 인해 과도한 대역폭의 낭비라는 문제점을 가지고 있다. 이를 개선한 버전2는 송신할 때 DES(Data Encryption Standard)알고리즘을 사용하고, 사용자 인증시에는 MD5(Message Digest 5)알고리즘을 사용함으로써 보안 문제를 다루게 된다. 또한 과도한 대역폭의 낭비를 방지하기 위해 bulk 요청을 한다. 또한 버전 1에서 에이전트가 트랩을 발생시켰을 때 매니저가 트랩을 받았음을 알리는 Inform메시지를 모범으로서 트랩의 효율성을 높인다. 또한 버전 3에서는 버전2의 기능에 사용자인증, 보안, 접근제어를 강화한다. [6]

2.3 PHP와 데이터베이스

PHP(Hypertext PreProcessor)는 서버 스크립트로써 리눅스에서 돌아가는 아파치 서버와 가장 잘 맞는 스크립트로 알려져 있다. 또한 Windows 환경인 Windows 2000에서의 IIS(Internet Information Server)나 Windows 95/98의 PWS(Personal Web Server)상에서 지원되는 솔루션이다. 즉 클라이언트로부터 웹문서의 요청이 왔을 때 서버는 해당요구사항을 분석한후 이를 HTML문서로 만들어 클라이언트로 보내게 된다. 아래의 <그림 1>은 PHP를 이용한 서버와 클라이언트 사이의 동적인 구성을 나타낸다.

PHP를 이용하여 웹화면에 접속하여 정보를 조회할 경우 실시간 데이터만 텍스트 파일 형태로 조회가 가능하도록 하며 나머지 데이터의 경우에는 5분단위를 주기로 해서 데이터베이스에 각 장치별 로그로 해서

저장되게 된다. 이후 모든 장치에 대한 조회는 직접 그 장치에 질의하는 것이 아닌 데이터베이스에 조회하도록 되어있어 장치에 대한 부하를 줄일 수 있다.



<그림 1> PHP를 이용한 동적 구동원리

PHP는 C로 만든 CGI와 달리 서버에 독립적인 프로세스를 생성시키지 않으므로 실행파일을 통한 CGI 구동방식보다 서버에 대한 자원 부담을 줄여주므로 빠른 속도로 구동할수 있다. 이것은 apache 웹서버의 기능에서 필요한 기능들을 모듈식으로 런타임 라이브러리로 작동하기 때문에 가능한 것이다.[8]

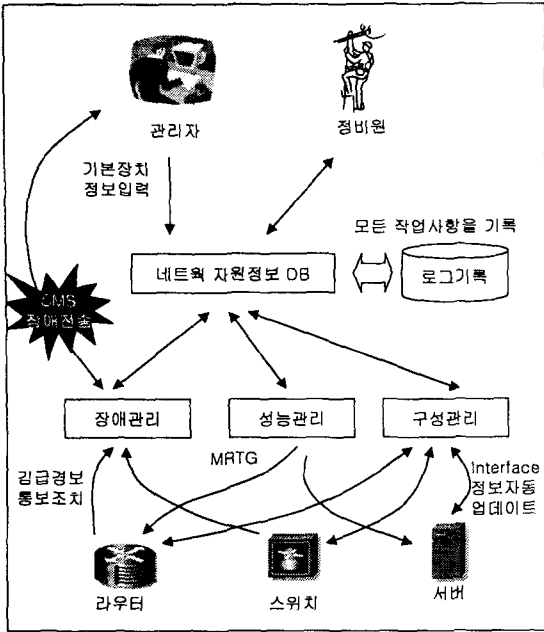
3. 시스템 분석 및 설계

효율적인 이력관리와 자원관리를 위해서 먼저 데이터를 수집방법과 조회방법을 분석하였다. 실시간으로 관리할 데이터와 데이터베이스에서 질의할 부분을 나누어 실시간으로 분석하는 경우 처리의 신속성을 위해 텍스트 형태로 저장하였다가 주기적으로 데이터베이스에 값을 입력하도록 하였다. <그림 2>는 NMS의 전체 구성도를 나타낸 것이다.

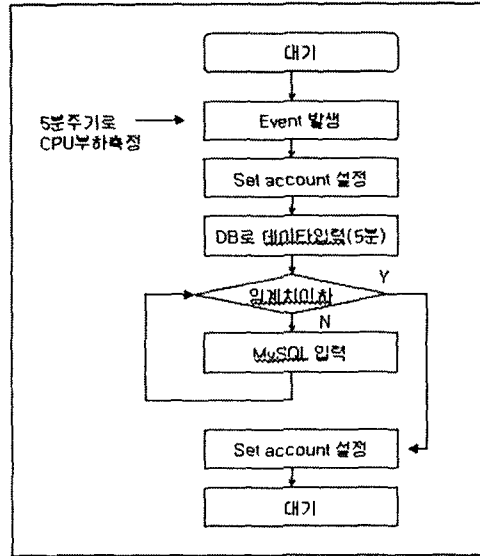
본 NMS의 주요 기능인 실시간 로그기능의 순차도는 아래 <그림 3>과 같이 나타내며, <그림 4>는 부하발생시 ip accounting 정보를 수집하는 순서도이다.

실시간 로그란 각 장치에서 발생하는 로그들을 각 장치마다 로그인하여 확인하는 것이 아닌 NMS로 로그인하도록 하여 사용자가 이를 실시간으로 확인하는 것이다. 이때 로깅시 미리 입력되어 있는 장치관련 정보를 키값으로 하여 해당로그를 장치명과 대조하여 사용자에게 해당지역 장치명으로 디스플레이 한다. 여러 장치들의 로그파일이 하나의 파일로 로그인시 파일의 크기가 커지므로 이를 5분단위로 DB에 저장한다. 이후 이전에 관련된 데이터값들은 DB에 쿼리하여 조회할 수 있다.

현재까지 대부분의 NMS가 없는 중소기업 및 학교에서는 콘솔로 로그인하거나 텔넷으로 매번 접속해 로그를 확인하고 있다. 네트워크 장치와 장치가 연결되어 서로간의 정보를 교환하고 갱신하는 과정에 한 장치의 에러는 다른 장치에 영향을 미칠 수 있다. 또한 장치의

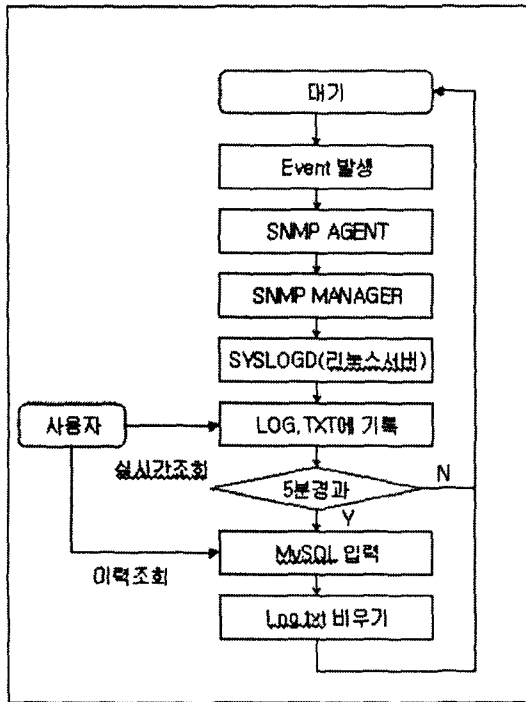


<그림 2> NMS 전체 구성도



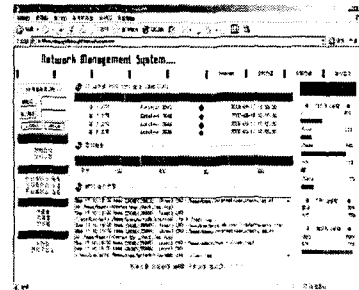
<그림 4> ip accounting 정보수집 순서도

특정 부하 발생시 자원에 대한 상태모니터만을 할 뿐 원인을 찾는 데는 어려움이 많다. 이에 이벤트 발생 시 ip accounting의 mib을 이용하여 장치에 셋팅을 한 후 발생하는 정보를 DB로 수합한 후 이벤트 종료시 mib값을 리셋시켜 데이터 수집을 종료한다. 이후 분석된 값을 이용하여 원인을 찾을 수 있다.



<그림 3> 실시간 로그기능의 순서도

이벤트를 등급을 설정하여 이벤트 발생시 관리자에게 SMS전송 내지는 메일을 발송하여 빠른 시간 내에 장애조치를 할 수 있다. 이렇게 함으로써 사용자에게 장애신고를 받기 전에 운영자가 먼저 이를 조치함으로써 장애파급효과와 downtime을 줄일 수 있다.



<그림 5> 장치관리화면

<그림 5>는 장치관리 화면으로 화면 왼쪽에 있는 로그인의 경우 작업시 작업자의 이름을 작성내역과 같이 이력관리하여 환경변경으로 장애발생시 작업자에게 문의해 볼 수 있다. 그러므로 작업자는 꼭 환경변경시 로그인을 해야만 작업할 수 있다.

4. 비교

상용 NMS의 경우 관리자가 손쉽게 작업할 수 있도록 GUI방식의 도입과 여러 가지 다양한 기능들을 제시하고 있다. 하지만, 대부분의 경우 전체 기능을 이용하는 것보다 일부 기능만을 이용하는 경우가 대부분

이며, 환경의 변경시 사용자가 변경하여 적용할 수 있는 부분이 극히 한정되어 쓰지 않고 두는 경우가 대부분이다. 본 논문에서 제공하는 NMS의 경우 오픈소스로 되어 있어 누구나 수정하여 기능을 추가할 수 있으며, 또한 널리 쓰이는 SNMP의 MIB값을 바탕으로 제작되어 있기 때문에 장치가 변경된다 하더라도 MIB값만 설정해 주면 기본적인 기능은 대부분 문제없이 작동된다.

또한 perl을 사용하여 기존의 사용 NMS가 가져와 데이터를 가공하는 시간이 줄어들어 데이터 gathering time을 줄일 수 있으며, 그러므로 좀더 많은 장치들을 관리할 수 있다.

III. 결 론

본 시스템은 상용 NMS에 비해 많은 기능들이 부족하지만, 꼭 필요한 기능만 사용자가 추가하여 사용하면 상용 NMS 못지 않은 효과를 볼 수 있다. 웹으로 화면 등이 구성되어 있으므로 작업자가 작업내역을 장소에 구애받지 않고 조회 및 입력이 가능하다.

앞으로 보안이 필요로 하는 부분은 자바로 개발이 필요하며, 사용자가 mib값을 설정하는 것도 가능하지만, 별도 장치 db를 구축하여 auto scanning 기능을 추가하는 것도 필요하다.

참고문헌

- [1] 김현성 “공공부문 정보통신망의 효율적 관리방안-네트워크관리시스템을중심으로-” 한국행정학회, 1999년도 하계학술대회 논문 발표집.
- [2] RFC1155 Structure of Management Information.
- [3] RFC1157 Simple Nerwork Management Protocol (SNMP).
- [4] RFC1212 Consise MIB definitions.
- [5] “Programming Perl, 3rd Edition” Larry Wall, Tom Christiansen & Jon Orwant, 2000.
- [6] “The OSI Management Architecture: an Overview” S.M. Klerer, IEEE Network, 1988.
- [7] “Essential SNMP” Douglas Mauro & Kevin Schmidt, 2001.
- [8] “Professional PHP Programming” Harish Rawat, Jon Parise, James Moore.