분산 Lan 세그먼트관리를 위한 LAN 모니터링 시스템의 설계 및 구현

이원혁*, 조규억*, 최영수*, 정진욱*
*성균관 대학교 전기.전자 및 컴퓨터공학부
e-mail : livezone@unitel.co.kr

Design and Implementation of LAN Monitoring System for managing Distributed Lan Segment

Won-Hyuk Lee*, Kyu-Oak Joe*, Young-su Choi*, Jin-Wook Chung*
*School of Electrical and Computer engineering, Sungkyunkwan University

요 약

본 논문에서는 여러 개의 Lan 세그먼트를 관리하며 패킷의 분석과 이용현황 등을 비교, 분석하기 쉽게 해주는 Lan 모니터링 매니저 시스템과 각 세그먼트별로 패킷을 수집하는 LAN 모니터링 에이전트를 설계 및 구현하였다. 네트워크의 규모가 커지고 관리를 요하는 장비가 증가함에 따라 기존의 NMS 로는 관리에 있어 한계를 보여왔다. 이에 Lan 세그먼트단위의 관리를 하는 RMON 에이전트의 필요성이 대두되는데. 이또한 여러 Lan 세그먼트를 관리하기 위해 RMON 장비를 세그먼트마다 탑재해야 하는 등 비용과 관리의 어려움이 있다. 따라서 본 논문에서는 소프트웨어적으로 구현하여 간편하게 망 관리를 할 수 있는 Lan 모니터링 시스템을 제시한다.

1. 서 론

최근 네트워크의 규모가 점차 커지고, 관리를 요하는 장비가 증가함에 따라 기존의 NMS 로 네트워크를 관리하는데 있어서 한계를 보여왔다. 기존의 NMS 는 중앙집중적인 관리를 원칙으로 하고 있어 모든 장비들과의 정보교환을 위한 폴링으로 인해 네트워크에 많은 부하가 걸림에 따라 네트워크 전체의 성능이 떨어지게 된다. 이러한 현상은 네트워크의 규모가 커질수록 더 심하게 발생될 수 있다.

또한 기존의 NMS 에서 사용하는 MIB(Management Information Base)으로는 장비자신에 대한 정보 밖에 얻을 수 없기 때문에 보다 효율적인 관리를 위해서는 매니저가 처리해야 할 일이 많아져서 부담이 되게 된다.

현재 네트워크 관리를 위해 SNMP(Simple Network Management Protocol)와 CMIP(Common Management Information Protocol)등과 같은 표준 프로토콜들이 있으며, 관리 대상 장비로부터 정보를 얻어와 이 정보를 토대로 분석 결과를 제시하는 네트워크 관리도구들, 그리고 서브넷 단위로 네트워크 모니터링을 위한 RMON(Remote Network Monitoring)등이 존재한다.

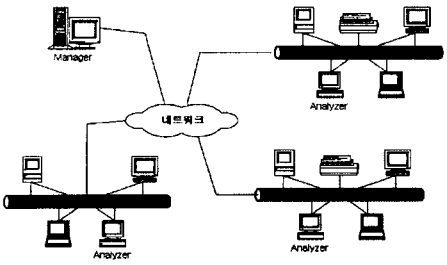
CMIP 은 ITU-T 와 ISO 에서 표준화하였으나 너무 복잡하고 방대하여 구현하기가 어렵고, 기능을 제공하는 장비도 많지않아 SNMP 를 대체하지 못하고 있다. 또한 중앙 집중적인 관리구조를 가지는 SNMP 보다, 분산관리를 통해 매니저의 부담을 줄이고 매니저의 폴링을 감소시킴으로써 네트워크의 성능을 향상시킬 수 있는 RMON 이 각광받게 되었다.

그러나 전체 Lan 세그먼트를 관리하기 위해서는 여러 대의 RMON 장비들이 모든 세그먼트에 존재해야 한다.

이에 이 논문에서는 소프트웨어로 구성된 LAN 모니터링 에이전트와 LAN 관리시스템을 개발하여 분산 LAN 세그먼트 관리를 위한 새 모델을 제시하고자 한다. 패킷을 분석할 수 있는 에이전트를 Lan 세그먼트마다 설치하여 매니저에서 각각의 패킷 입출력

현황과 프로토콜등의 분석을 통해 각 LAN 들의 이용 현황을 파악할 수 있는 자료로 이용할 수 있다.

이 시스템의 전체 구조는 다음 그림과 같다.



[그림 1] 전체 구조도

[그림1]과 같이 각 세그먼트의 PC에 설치된 에이전트를 통해 전체 LAN세그먼트의 트래픽 통계정보, 프로토콜 정보등을 관리할 수 있다. 여러 개의 세그먼트에 설치할 수 있으므로 복수개의 LAN관리도 가능하다.

2. Lan 모니터링 에이전트의 분석 항목

본 LAN모니터링 시스템에서는 다양한 분석 기능들을 제공하며 이를 위해 각 에이전트는 해당 정보를 수집하여 관리한다. 이와 같은 분석항목은 [표1]과 같다.

[표 1]

Segment 통계정보	단위시간당 패킷수	단위시간동안 입출력패킷의 누적,평균값
	총바이트량	총수신 패킷량과 단위시간당 수신 패킷수의 누적,평균값
	Layer별프로토콜	Ethernet/IEEE802.3등 link layer protocol의 갯수 및 백분율
		IP,ICMP,IGMP등의 프로토콜 갯수 및 백분율
		TCP/UDP의 갯수 및 백분율
		HTTP ,SMTP ,FTP ,TELNET등의 응용 프로토콜 갯수 및 백분율
	패킷유형별 분석	Broadcast,Multicast의 개수 및 백분율
	Frame별 분석	Ethernet/IEEE802.3의 Frame 종류 개수 및 백분율
Host간 통계정보	단위시간당 패킷수	특정 호스트간에 단위시간동안 주고받은 패킷의 누적,평균값
	총바이트량	특정 호스트간에 주고받은 패킷의 총바이트량 및 단위시간당 수신 패킷수의 누적,평균값
	응용 Protocol	특정 호스트간에 주고받은 응용 프로토콜의 종류 및 프로토콜당 백분율
단일 Host정보	입력패킷수	특정 호스트에서의 단위시간당 입력 패킷수의 누적,평균값
	출력패킷수	특정 호스트에서의 단위시간당 출력 패킷수의 누적,평균값
	총바이트량	특정 호스트에서 단위시간당 입출력하는 패킷수의 누적,평균값
	응용 Protocol	특정 호스트에서 사용한 응용 protocol의 종류와 프로토콜당 백분율

3. Lan모니터링 매니저 시스템의 설계

3.1 시스템 구조

이 시스템은 크게 세가지 기능으로 나뉘며, Socket 통신 모듈, 패킷 수신 및 분석 모듈, NIC 접근 제어 모듈로 구성된다.

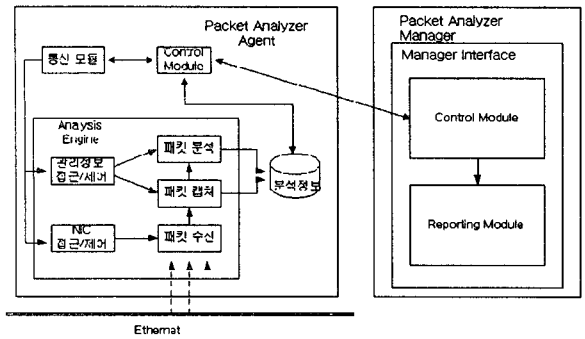
Socket통신 모듈은 Lan 모니터링 에이전트와 매니저가 통신 및 상호 제어하기 위한 이다

패킷수신 및 분석모듈은 패킷 수신,패킷 분석, 패킷 캡쳐로 이루어지며 매니저로부터의 요청이 들어오면 네트워크로부터 NIC 버퍼에 수신되는 모든 패킷을 읽어들여 각 프로토콜 계층에 따라 패킷을 분석하고 그 분석된 결과를 실시간 전송 및 관리정보 데이터베이스에 저장하는 핵심 모듈이다.

NIC접근 제어 모듈은 NIC로의 접근과 패킷 수신을 수행할 수 있도록 인터페이스 역할을 수행하는 packet.vxd와 이 드라이버의 서비스를 C 라이브러리로 구현한 packet.dll은 인터넷에 공개된 모듈을 사용했다.

위의 그림에서 보듯이 하나의 매니저는 여러 개의 Lan 세그먼트 상의 에이전트와 연결된다.

다음은 특정 Lan 세그먼트의 에이전트와 매니저와의 소켓 연결 상황을 나타낸 내부 구조이다.



[그림 2] 시스템 내부 구조

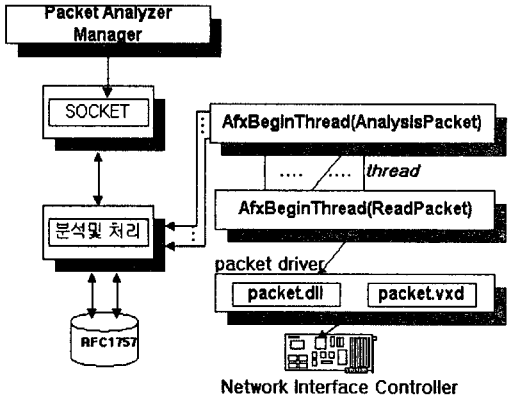
Lan 모니터링 에이전트와 매니저는 Control module 로 연결되며 이 모듈을 통해 매니저와 에이전트의 통신이 이루어진다. 각 모듈별 기능은 다음과 같다.

3.2 Lan 모니터링 에이전트

(1) 제어 모듈
매니저의 실행시 둘 사이는 소켓으로 연결되며 이후 패킷 수집에 대한 매니저의 요청이나 에이전트의 응답이 이를 통해 이루어진다.

(2) 패킷 수집 모듈
매니저로부터의 패킷 수집 요청이 오면 에이전트는 랜상에 흘러다니는 모든 패킷을 수집하기 시작한다. 이때 LAN 상에 흘러다니는 모든 패킷들을 상위 어플리케이션이 수집하고, 모니터링 할 수 있도록 하기 위해서 네트워크 카드는 특정 모드로 설정되어야 하며, 이 모드를 " promiscuous 모드" 라고 한다. 이 모드로 설정된 NIC 는 자신에게 수신된 패킷의 목적지 주소가 자신의 해당 주소가 아니더라도 모든 패킷을 자신의 내부 패킷 버퍼에 저장한다. 이로써 LAN 상의 모든 패킷을 수신하게 되는 것이다. 일단 수집이 시작된 모듈은 매니저로부터 중지 요청이 올때까지 계속 수집이 이루어지며 패킷 수신의 효율성을 위해 쓰레드로 구현되었다.

(3) 패킷 분석/ 저장 모듈
수집된 패킷은 일부 실시간 분석이 이루어 지며 일부는 데이터베이스에 저장된다. 모든 패킷을 실시간 분석하지 않는 이유는 한꺼번에 수십개의 패킷을 수집하고 분석하려면 패킷의 손실이 생길 수 있기 때문이며, 호스트의 성능을 고려하여 필요한 일부만 실시간으로 분석하여 매니저에게 전송되고 나머지는 저장되어 패킷 수집이 모두 끝난후에 분석이 이루어 진다.
다음은 NIC 로부터 흘러들어온 패킷을 수신하고 분석/저장하는 내부 동작의 구성도를 나타낸 것이다.



[그림 3] 패킷 수신 및 분석/저장 모듈

(4) 패킷 전송 모듈
매니저로부터의 패킷 수집중지 요청이 오면 에이전트는 즉시 패킷수집을 끝마치며 이와 함께 그때까지 수집했던 패킷들을 재분석하여 소켓을 통해 매니저에 전송된다.

3.3 Lan 모니터링 매니저 시스템

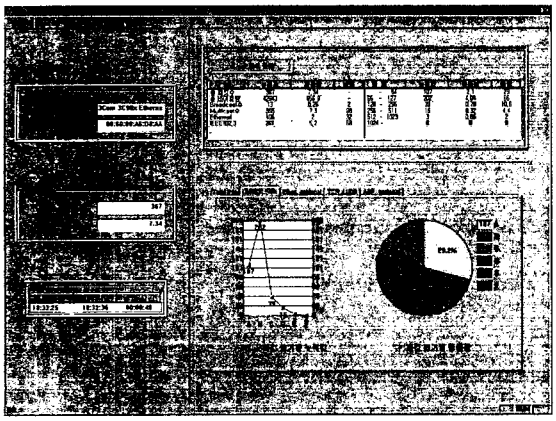
(1) 제어 모듈
에이전트가 소켓 서버로서 먼저 실행되면 매니저는 실행과 동시에 소켓 접속을 시도한다. 접속에 성공하면 매니저는 성공적인 실행과 함께 에이전트가 있는 호스트의 랜카드명과 Mac 주소를 전송받는다.

(2) 패킷 수집 요청
에이전트가 패킷을 수집하고 저장하는 등의 일을 수행하기 위해서는 매니저의 패킷수집 요청이 선행되어야 한다. 수집 요청이 받아들여지면 에이전트는 패킷의 수집과 일부의 실시간 분석을 통해 나온 결과를 주기적으로 소켓을 통해 전송하고 매니저는 이를 받아들여 주기적으로 화면을 갱신하여 관리자에게 보여준다.

(3) 결과 수신 모듈
패킷 수집 중지요청을 하면 에이전트는 패킷의 수집을 중지하고 저장된 데이터를 분석하여 그 결과를 매니저에 보내온다. 그러면 매니저는 그 결과를 받아들여 표와 차트로 관리자에게 분석결과를 보여준다.

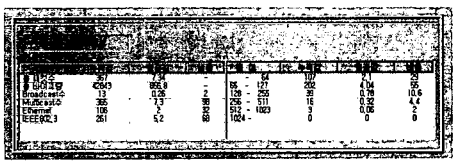
4. 시스템 구현

다음은 매니저툴의 전체적인 모습이다. 매니저의 시작과 함께 연결된 에이전트로부터 에이전트의 MAC 주소와 NIC 이름을 전송받는다. 이후 수집이 시작되면 실시간 정보창으로는 실시간으로 데이터가 업데이트되고, 수집을 마친 후에는 총 분석정보를 Tab 컨트롤로 표현한다.



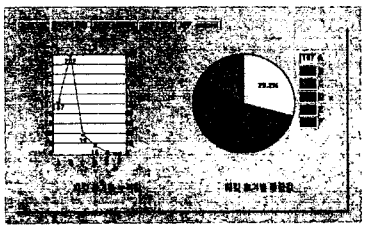
[그림 4] manager 툴의 전체모습

다음은 실시간으로 에이전트의 수집 현황을 보여주는 툴이다. 모든 분석을 실시간으로 보여주지 않은 이유는 분석모듈로 인해 패킷 수신의 성능이 저하될 우려가 있기 때문이다. 때문에 실시간 분석이 필요한 일부만 분석하고 나머지는 데이터 베이스에 저장함으로써 성능의 향상을 추구했다.



[그림 5] 실시간 분석정보 창

다음은 패킷 수집을 마친 후에 각 계층의 프로토콜과 전체 패킷 정보를 분석하고 보내온 정보를 나타낸다.



[그림 6] 패킷 분석 창

5. 결론

본 논문에서는 여러 개의 LAN 세그먼트를 관리하기위한 Lan 모니터링 관리시스템과 Lan 모니터링 에이전트를 구현하였다.

PC 상에서 Lan 모니터링 관리시스템이 동작하기 위한 전체 내부구조와 패킷 수신부터 분석까지의 일련과정을 정의하였으며, 데이터베이스 관리구조와 분석항목을 정의했다. 또한 구현된 이 시스템을 실제 네트워크 환경에 적용해 봄으로써 RMON 하드웨어 장비의 대체 가능성에 대해 검증해 보았다.

이를 통해 각각의 Lan 세그먼트의 트래픽 동향을 분석할 수 있고 특정 호스트간의 연결상태 및 Lan 이용율, 혹은 단일 호스트의 감시도 가능하다.

하드웨어 장비를 사용하지 않고 순수하게 소프트웨어적으로 만으로도 Lan 관리 시스템을 구현했다는 점과 RMON 에서 발전된 분산 LAN 세그먼트 관리 시스템의 새로운 모델 제시라는 측면에서 큰 성과가 있었다.

6. 참고 문헌

(1) 안신영,안성진,정진욱, "LAN 관리를 위한 Web 기반 가시화 시스템의 설계 및 구현", 한국통신학회 논문지, p.410-421, 제 24 권 제 3B 호,1999

(2) 김순철,최영수,정진욱, "Lan 세그먼트 관리를 위한 PC 기반의 RMON 에이전트 및 관리자시스템에 대한 연구", 한국정보처리학회 추계학술발표논문집 제 6 권 제 2 호 , 1999

(3) TCP/IP Illustrated, Volume I, W.Richard Stevens,1994

(4) Computer Networking, James F.Kurose, Addison Wesley, 2000

(5) William Stallings, "SNMP, SNMPv2 and RMON", Addsion Wesley, 1996

(6) Gilbert Held, "Lan Management with SNMP and RMON", WILEY, 1996

(7) Soon-Chul Kim, Young-su Choi, Jin-Wook Chung, "A Study on RMON Agent/Manager System for LAN Segment Management base on PC", 1999

(8)http://hometown.weppy.com/~alzzanom/network/network/basic/comm05/comm5.htm