실시간 트래픽 모니터링 시스템 설계 및 구현

(주)스마트넷 테크놀로지 김성호 · 조시훈

1. 서 론

최근 인터넷은 새로운 응용프로그램과 네트워크의 고속화로 인해 그 수요는 한층 더 폭발적으로 증가하고 있다. 이를 위한 정확한 트래픽 분석에 대한 요구가 현재 네트워크 관리 측면에서 중요한 이슈로 등장하고 있다. 분석된 데이터를 바탕으로 ISP입장에서는 SLA와 CRM이 가능하게 되며, IP Packet양을 얼마나 사용했는지에 대한 과금 즉 IP 종량제를 구축할 수도 있다. . 이런 트래픽 분석 방법에는 여러가지 기법들이 현재 존재하며, 각 방법의 기능에 대해서는 2장에서 설명하기로 한다. 본 고에서는 MPC 7450 즉. Motorola Power PC 계열의 H/W에 Embedded Linux 2.4.10 을 사용하여 트래픽 모니터링 시스템을 설계하고 구현하였으며, Embedded Linux 시스템을 선정하게 된 동기는 Time-Critical 한 패킷을 처리하기 위해서는 Kernel 내부를 건드려야 하는데 이를 위해서 Embedded Linux를 사용하는 것이 개발하기에 용이하며, 또한 기존 VxWork나 Nuclius등이 너무나 비싼 가격도 Embedded Linux를 선택하게 된 이유이기도 하다.. 3장에서는 H/W 설계 측면과 S/W적인 설계 및 구현에 대해 설명하며, 4장에서 결론에 대해 서술한다.

2. 동기 및 목표

패킷 모니터링은 네트워크 관리 측면에서 중요 이슈로 부각되고 있으며, 기존의 방식은 라우터에 빌드인 (Built in)하는 기법으로 SNMP, RMON, NetFlow 같은 기법을 사용해왔다. 이는 이들간에도 트래픽 관리 객체에 대한 차이도 있지만 이 기법은 현재의 트래픽 관리의 요구사항을 만족하지 못할뿐만 아니라, 새로운 요구사항을 수용할 수 있는 유용성을 제공하지 못하며, 가장 큰 문제점으로는 네트워크의 고속화와 상당히 많은 IP Packet을 캡쳐링하는데 라우터 베이스의 메커니즘은 패킷 손실이 많이 존재 할 수 밖에 없고, 또한 본래의 기능을 수행하는데 많은 오버헤드를 갖게 된다. 이러한 문제점으로 인해 트래픽만 전담하여 처리하는 프로브를 이용하는 것이 새로이 대두되고 있다 이를 Non - Router Based 기법 또는 STA (Semantic Traffic Analysis) 기법이라고도 한다. 프로브를 이용해 트래픽을 측정 밥법에는 크게 두가지 방식으로 나눌수 있다. 첫째는 능동적 측정 (Active Measurement) 방식이다. 이는 실시간으로 트래픽을 분석하는 장점은 있으나. 기존 트래픽에 부하를 가중시키며 또한 패킷 손실이 아닌 정보의 손실이 존재할 수 있다. 즉 정확한 데이터를 분석하는데 어려움이 존재한다.

둘째로 수동적 측정 (Passive measurement)방식은 off-line으로 트래픽을 분석하는 방식으로 기존 트래픽에는 영향을 주지는 않지만 단점으로는 데이터에 대한 분석이 off-line으로 이루진다는 것이다. 또한 상당한 많은 데이터를 나중에 분석할 때 오버헤드도 부담이 된다. 트래픽을 캡쳐링하는 방법은 오래전부터 연구되어 왔으며, 통상적으로 TCP - dump를 사용해왔다. TCP-dump는 Pcap 라이브러리를 이용하여 패킷을 캡쳐링한다. 최근의 방식으로는 미국 코넬대학에서 개발하고 있는 Cyclone이라는 방식이 있다. 이는 kernel 내부 프로그램의 여러 어려움점을 해결하기 위한 미들웨어 이다. 사용자 레벨 프로그램에서는 Cyclone에서 제공하는 여러 메커니즘을 이용하여 커널 프로그래밍이 가능하다.

TCP-dump는 pcap 라이브러리를 사용하는데 이는 socket Level의 recvfrom을 이용하는 것으로 드

* 정회원

라이버에서 패킷이 올라오면 IP stack, TCP stack, socket Stack을 통과하여 패킷을 사용자레벨로 전송하는 방식으로 고속의 패킷을 처리하는데 패킷 손실이 유발되며 Time-Critical한 패킷을 핸들링할 때 정보의 손실이 발생하게 된다. Cyclone을 이용한 방식은 편리함 잇점은 있으나 이는 또 하나의 미들웨어이므로 고속의 패킷을 처리하는데는 적합하지 않은 방식이다. 본 설계에서는 고속의 패킷을 처리하기 위해 Driver단에서 패킷을 처리하는 Kernel Level의 메커니즘을 구현한다. 이를 통해 고속의 패킷을 정보의 손실없이 처리하고자 한다.

이를 위해 전용 프로세서인 MPC7450을 설계하였으며 그 hardware Interface는 10/100/100M, T1,T3,OC-3,OC-48등을 디자인 하였다. 위에서 언급한 것처럼 Kernel Level 프로그램을 위해 Embedded Linux 2.4.10 및 각 네트워크 디바이스에 해당하는 드라이버을 수정하여 개발하였다.

Embedded Linux를 이용할 시 많은 드라이버 소스코드와 Kernel Source code가 Open되어 있어 커널 프로그래밍을 설계하고 구현하는 것이 용이하였다.. 본 트래픽 모니터링 시스템 설계의 궁극적인 목표는 첫째로 고속의 패킷을 처리하는데 time-critical한 부분을 드라이버와 커널 프로그래밍을 함으로써 정보의 손실을 없게 하는것이며, 둘째로 능동적 측정(Active Measurement)방식의 데이터 측정방법을 표준 트래픽 측정방식인RMON(Remote Monitoring)I, II의 스펙에 적용하는 것이며, 셋째로 프로브와 트래픽을 분석하는 메커니즘을 표준 NMS(Network Management System) 프로토콜인 SNMP(Simple Network Management Protocol) 프로토콜을 사용하여 기존의 NMS 서버와의 Integration이 될 수 있도록 구현하는 것을 주요 목표로 하였다.

3. 설계 및 구현

본 트래픽 모니터링 시스템은 전용 프로브를 만드는 것으로 H/W와 S/W로 구성되어 있다.

3.1 H/W 설계

3.1.1 기본구성

Main Processor는 MPC7450733Mhz, System Controller는 GT-64260이며 여기에는 SDRAM/PCI/Ethernet/Interrupt controller를 내장하고 있다. Main Memory는 DIMM Socket 2개, 즉 1GigaByte까지 지원하며, Flash Memory는 BootRom과 Kernel및 Ram용(Disk on Chip), 응용프로그램에 사용되며 PCI는 66Mhz/64bit 3개, 기타 Serial Port등으로 구성되어 있다.

3.1.2 블록도

CPU의 재활용(높은 가격대임)을 높이기 위해 CPU part를 분리하여 별도의 카드로 구성되어 있으며 차후 Dual CPU 구성 시 CPU card만 새로 구성할 수 있어 효율적이다.

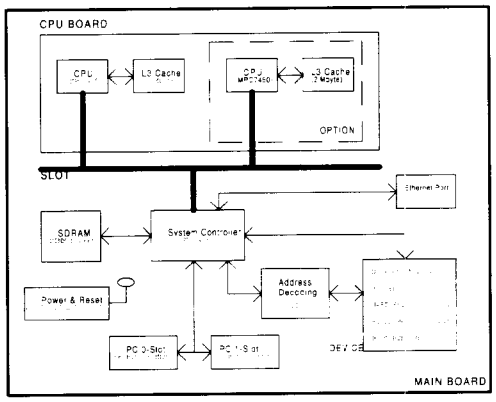


그림 1 메인보드 블록도

3.2 S/W 설계

3.2.1 S/W 구성도

트래픽 모니터링을 위한 S/W 구성도는 다음의 그림2와 같으며 패킷처리부분은 커널 내부에 존재하며, 사용자 영역에서는 처리된 결과는 SNMP Agent화 시켜서 관리 station에게 전달하게 된다. 커널 내부에서는 Time Critical한 패킷을 처리하게 되는데 내부적으로 보면 드라이버를 통해서 들어오는 패킷을 캡쳐링하여 분석하는 모듈이 있다. RMON II의 Almatrix라는 그룹을 처리하는 것이 시스템에 가장 부하를 많이 주게 된다. 이 관리 내용은 Source와 Destination이 Matrix로 존재하게 되며 분석된 데이터가 이 Matrix를 Searching 하거나 Update할때 시스템에 많은 부하가 존재한다. 이 부분의 성능이 전체 시스템의 성능을 좌우 하며 이 부하로 인해 패킷 손실 및 정보의 유실이 발생할 수 있다. 사용한 Hashing 알고리즘은 5-tuple (Source IP, Destination IP, Source Port, Destination Port, Protocol

Number)XOR Folding 메커니즘을 사용하여 hash table의 Size를 적당하게 설정하고, Collision을 가장 적게 발생하도록 유지하여, Hashing 처리로 인한 시스템의 부하를 최소화하고 정보의 손실이 없도록 설계하였다.. Hash table의 크기와 Collision rate의 관계는 다음의 공식을 이용하여 설정하였다.

$$Cr = 1 - \frac{N(1 - ((N-1)/N)^m}{m}$$

N : Hash table size, m : number of distinguished flows , Cr = Collision rate

처리된 데이터는 응용프로그램에서 관리 station으로 넘기게 되는데 이 메커니즘은 SNMP 프로토콜을 이용하여 전달하게 된다.

전달되는 메커니즘은 대부분의 분석된 데이터는 폴링에 의거하여 전달하며, 알람 임계값 경보(Threshold)등은 트랩을 이용하여 관리 station에게 보내게 된다.

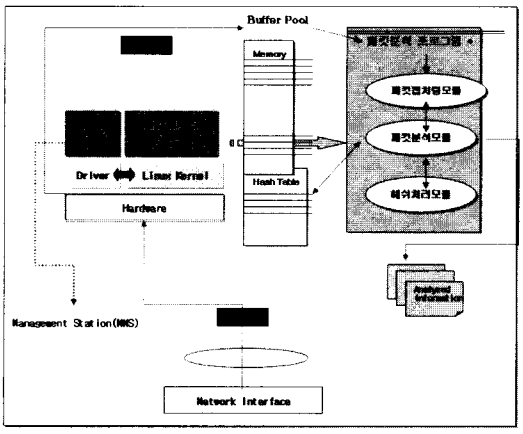


그림 2 소프트웨어 구성도

4. 결 론

향후 해야할 일은 본 시스템에 대한 실험결과를 바탕으로 이를 이용한 IDS, IP Billing, Worm Detection등을 구현하여 테스트 해볼 예정이다.

참고문헌

[1] K.G.Anagnostakis,S.Ioannidis, "Efficient Packet Monitoring for Network Management" May 2002 NOMS

[2] John Cleary, Ian Grahan, "High Precision Traffic Measurement", IEEE Com Magazine, March 2002-05-29

[3] G.Goldszmidt and Y.Yemni, "Distributed management by delegation", In Procedings of the 15th International Conference on Distributed Computing Systems, 1995

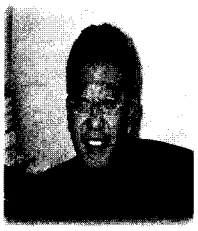
[4] J.D.Case, M.Fedor, "Simple Network Management Protocol(SNMP)", RFC1157, May 1990

[5] RFC1157

[6] RFC2025

[7] V.Paxson, J.Mahdavi, "An Architecture for large scale Internet Measurement", IEEE Com Magazine, august 1998

[8] S.Savage, D.Wetherall, "Practical Network support for IP traceback", In ACM SIGCOMM, August 2000



김 성 호

1990 울산공대 전산학과 졸
1994 한국과학기술원 정보및통신공학 석사 졸
2001~현재 고려대학교 전자공학과 박사과정
~ 현재. ㈜스마트넷 연구소장
관심분야:NMS, QoS, TE 등
E-mail:shkim@smartnet.co.kr

조 시 훈

1992 경북대 전산학과 졸업
1994 한국과학기술원 정보및통신공학 석사 졸업
1994~현재 한국과학기술원 전산학과 박사과정
현재 ㈜스마트넷 S / W 개발 팀장
관심분야:RealTime OS, NMS, Qos
E-mail:shcho@smartnet.co.kr