통신망 트래픽 측정용 통합 시스템 구조

정연기
경일대학교 컴퓨터공학부

Architecture of an Integrated System for Traffic Measurement of Computer Networks

Youn-Ky Chung
School of Computer Engineering, KyungIl University

요 약

통신망의 규모가 커지고 구조가 복잡해짐에 따라, 통신망의 성능을 최적화하여 사용자들이 요구하는 서비스 품질을 보장해 주는 성능관리의 기능이 절실히 요구되고 있다. 현재 성능관리의 주요 기능이 되는 트래픽에 대한 분석을 위해서 넷플로우(NetFlow), RMON, 그리고 패킷을 캡처하는 방법이 쓰이고 있지만 통합적인 관점의 해결책은 되지 못한다. 본 논문에서는 다양한 전송기술(Multi-technology), 다양한 장치 제조사(Multi-vender) 장비들의 성능관리를 가능케 할 수 있도록 통합적인 통신망 성능관리 구조를 제시하고, 그에 따라 성능관리 시스템을 설계하고 구현하였다.

1. 서론

현대의 통신망은 점점 그 규모가 거대해지고 구조가 복잡해지고 있다. 그러나 현재 통신망에 설치되는 장비들은 서로 다른 관리 체계로 관리되고 있기 때문에 관리 기술의 이질성의 문제로 사람의 손에 의한 수동관리가 한계에 달하고 있으며, 이질적인 장치들간의 효율적인 통합관리 기술에 대한 요구가 높아지고 있다.

네트워크 관리는 ITU-T의 표준안에서 제시된 FCAPS(Fault, Configuration, Account, Performance, Security)의 5대 영역으로 나뉜다[1-2]. 이 중에서도 성능관리(Performance management)는 네트워크에 과부하가 걸리는 것을 사전에 찾아내어 적극적으로 장애를 회피하도록 하는 중요한 역할을 하고 있다. 이러한 성능관리가 제대로 이루어지기 위해서는 네트워크가 폭주에 빠지지 않았는지, 각 프로토콜별 대역폭은 알맞은지, 각 사용자별 대역폭 점유는 정상인지와 같은 네트워크의 트래픽 상황을 종합적으로 파악할 필요가 있다[3].

이러한 기능은 트래픽 현황을 탐지하는 기술을 기반으로 하는데, 트래픽 정보를 수집하는 기존의 기술로는 CISCO의 Netflow[4], IETF(Internet Engineering Task Force)의 RMON(Remote Monitoring)[5], 그리고 패킷을 직접 캡처하는 방법[6-7]이 대표적이다. 그러나 기존의 어느 한 기술로는 종합적인 네트워크 트래픽 측정이 불가능하다.

본 논문에서는 기존의 트래픽 현황을 탐지하는 기술의 여러 단점을 극복하여 통합 망관리 기능을 제공할 수 있도록, 하나의 정보 모델로 여러 트래픽 측정 기술들을 통합하는 구조를 제시한다. 본 논문에서 제안하는 통합 트래픽 정보 검출 구조는, 기존의 성능관리 제품들이 관리할 수 없었던 다양한 전송기술(Multi-technology), 다양한 장치 제조사(Multi-vender) 장비들의 성능관리를 가능케 하게 된다.

본 논문의 Ⅱ장에서는 기존의 국내외 트래픽 측정 기술 현황에 대해서 설명하고, Ⅲ장에서는 본 논문에서 제안하는 성능 관리시스템의 구조에 대해서 설명한다. Ⅳ장에서 성능관리 시스템 구현과 성능을 분석하고 Ⅴ장에서 결론을 맺는다.

2. 기존의 트래픽 측정기술 현황

트래픽 정보를 수집하는 기존의 기술로는 CISCO의 Netflow[4], IETF의 RMON(Remote Monitoring)[5], SNMP(Simple Network Management Protocol)[8], 그리고 패킷을 직접 캡처하는 방법[6-7]

이 대표적이다.

2.1 Netflow

NetFlow는 CISCO사에서 라우터나 스위치에서 장비를 통과하는 트래픽에 대한 방대한 양의 통계 자료들을 실시간으로 획득하기 위한 IP 스위칭 기능으로 구성되어 있다[4].

CISCO의 인터넷 장비는 네트워크 시장에서 높은 점유율을 보이고 있고, 데이터 수집 및 저장을 위한 서버만 설치하면 네트워크 트래픽 현황에 대한 정보를 획득할 수 있으므로 NetFlow를 통한 인터넷 성능 관리가 각광받고 있다. 그러나 NetFlow는 타 회사 인터넷 장비와의 호환성이 없고, CISCO의 NetFlow 기능을 지원하는 장비에 국한되어 있다는 약점이 있다.

2.2 RMON

RMON은 SNMP[8]의 확장판으로서, RFC 1757[5]에 정의된 MIB의 일부로 정의되어 있다. RMON은 네트워크를 효율적으로 이용하기 위해서 현재의 네트워크 상태를 측정하고 과거의 기록을 토대로 향후 네트워크 문제를 사전에 예견하는 기능을 갖는다. 현재 인터넷 장비 업체의 대부분은 RMON 서비스를 지원하지 않거나 부분적으로 지원하고 있으며, 고가의 장비에 국한되어 RMON 서비스를 지원하고 있다.

2.3 패킷 캡처

패킷 캡처 기술은 별도의 하드웨어 없이 소프트웨어만으로도 구현이 가능하다는 장점이 있으나, 스위치로 분할된 네트워크라면 LAN 세그먼트마다 모두 적용되어야 하는 제약이 있어 다수의 LAN 세그먼트로 분할되어 있는 현대의 네트워크에는 적용하기 힘들다.

2.4 SNMP

SNMP는 TCP/IP 프로토콜 기반의 인터넷에서 장치들을 관리하기 위한 기본 구조이며, 인터넷을 감시하고 유지, 보수하기 위한 기본적인 동작들의 조합을 제공한다[9,10]. SNMP는 TCP/IP를 기반으로, 보편적으로 사용하기 위하여 간단하게 설계되어 물리계층의 단위 망 구성 장치를 관리하기에 적합하다. 그러나 망 관점의 트래픽 정보를 관리하기에는 부적합하며 규모가 크고 다양한 장비로 구성된 망에서는 관리의 한계를 보이고 있다.

3. 성능관리시스템 설계 및 구현

한 가지 트래픽 측정 기술만으로는 종합적인 네트워크 트래픽 측정이 불가능하다. 앞에서 살펴 본 별개의 트래픽 측정 기술들을 하나로 통합하여, 현대의 다양한 기술과 다양한 제조회사 제품으로 구성된 네트워크에 대해 트래픽을 측정할 수 있도록 본 논문에서는 통합 시스템 구조를 제시한다.

3.1 전체 시스템 구조

그림 1은 전체 시스템의 구조를 나타낸다. ITU-T의 TMN 체계로부터 관리계층 개념을 받아 들여 NMS(Network Management System), EMS(Element Management System), Gateway, 그리고 NE(Network Element)에 탑재된 에이전트로 구성된다[11]. 각각의 에이전트들은 자신이 수집한 정보를 Gateway 모듈에게 전송한다. 이 때 Gateway 모듈은 기능별 에이전트에 대한 매니저(Manager)가 된다.

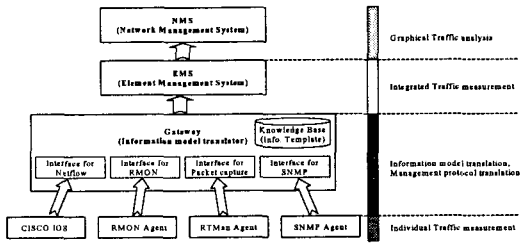

그림 1. 전체 시스템 구조

이종의 에이전트는 서로 다른 데이터 포맷과 내용, 다른 프로토콜을 이용하여 데이터를 전달하므로 Gateway가 데이터를 수신하기 위해서는 에이전트 종류별 인터페이스를 필요로 한다. 따라서 Gateway는 Netflow와 RMON, 패킷캡처와 SNMP를 지원하기 위한 각각의 인터페이스를 가지고 있으며, 에이전트로부터 수집된 정보를 가공하여 통일된 정보모델의 변화를 위한 Translation Template를 가진다. 또한 NMS의 관리 명령은 다시 Gateway를 통하여 하부의 각 기술들에 적합하도록 변환되어 전달된다.

Gateway는 하부의 이종 에이전트로부터 각각의 인터페이스로 네트워크 트래픽 통계에 대한 정보를 수집하고, 수집된 정보를 모델링하여 Knowledge Base(Database)에 저장한다. 이렇게 수집된 정보는 EMS(Element Management System)의 요청에 의해 보고된다. EMS는 세그먼트, 혹은 LAN을 단위로 서브넷의 통계 정보 및 서브넷 내의 호스트에 대한 모니터링 정보를 수집한다. 그러므로 여러 개의 세그먼트로 구성된 망에서는 세그먼트 단위로 하나의 EMS를 가진다. EMS는 다시 상위 NMS로 수집한 정보를 전달한다. NMS는 여러 개의 세그먼트 단위의 수집된

정보를 EMS를 통해 통합적으로 확인 및 분석 하고, EMS로부터 데이터 수집뿐만 아니라 장애나 알람 정보를 수신하여 네트워크 변화에 즉각적으로 반응할 수 있도록 한다.

이러한 계층별 기능 분산은 방대한 양의 트래픽이 전달되는 네트워크에서 트래픽 관리 기능의 부하를 줄이고, 다양한 트래픽 정보의 가공을 기능별로 명확하게 구별할 수 있어서 최종 관리자가 네트워크 부하 정보를 더욱 용이하게 확인할 수 있다는 장점이 있다.

패킷캡처 에이전트인 RTMan(Remote Traffic Management) 에이전트는 세그먼트 단위의 트래픽을 수집하여 네트워크 성능 분석을 수행하는 에이전트이다. 그러므로 RTMan 에이전트가 존재하는 세그먼트에 지나가는 모든 패킷을 캡처하여 트래픽량을 측정한다. 캡처된 정보는 소켓 인터페이스를 통하여 매니저에게 전달된다.

3.2 패킷 캡처

본 논문에서 구현한 시스템에서는 표 1과 같이 19개의 프로토콜을 캡처하여 분석할 수 있다.

표 1. 분석 가능한 프로토콜

	항목	상위 프로토콜	구분
1	EthernetII		Lenth/Type 필드에 2바이트 값이 십진 1514보다 큰 경우
2	802.3/802.2		Length/Type 필드 값이 십진 1514보다 작은 경우
3	IP	Ethernet2	Ethernet Type (2048, 0x0800)
4	IPX	Ethernet2	Ethernet Type (33079, 0x8137)
5	IPX	802.3	DSAP = E0, SSAP = E0
6	IPX	802.3	IPX Header의 CheckSum = 0xFFFF
7	IPX	802.3 SNAP	DSAP = AA, SSAP = AA, (Control = 03)
8	ARP	Ethernet2	Ethernet Type (2054, 0x0806)
9	ICMP	IP	IP Protocol 필드 = 1 (0x01)
10	TCP	IP	IP Protocol 필드 = 6 (0x06)
11	UDP	IP	IP Protocol 필드 = 17 (0x11)
12	HTTP	TCP	포트 : 80
13	POP	TCP	POP2 포트 : 109, POP3 포트 : 110
14	SMTP	TCP	포트 : 25
15	Telnet	TCP	포트 : 23
16	FTP	TCP	컨트롤 포트 : 21, 데이터 포트 : 20
17	DNS	UDP, TCP	포트 : 53
18	SNMP	UDP	SNMP 포트 : 161, SNMP Trap 포트 : 162
19	RIP	UDP	포트 : 520

그림 2는 패킷캡처 에이전트의 구조를 나타낸다. Main 쓰레드는 필요한 정보들을 획득하여 에이전트 환경을 초기화하고, 필요한 쓰레드를 생성한다. 쓰레드는 요청 수신 쓰레드, 네트워크 모니터링 쓰레드, 모니터링 결과 저장 쓰레드로 구성된다.

요청 수신 쓰레드는 성능관리 시스템 GUI로부터 모니터링을 시작할 것인지 아닌지에 대한 정보를 수신하고, 모니터링 시작 종료 명령을 네트워크 모니터링 쓰레드로 전달한다. 네트워크 모니터링 쓰레드는 모니터링 시작 정보를 요청 수신 쓰레드로부터 수신하면 네트워크 디바이스를 통과하는 트래픽을 모두 캡처한다. 캡처한 정보는 1초에 한번씩 모니터링 결과 저장 쓰레드로 전달하고, 모니터링 결과 저장 쓰레드는 수신한 트래픽 정보를 데이터베이스에 저장한다.

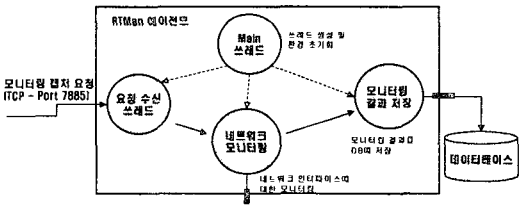

그림 2. RTMan 에이전트의 구조

네트워크를 통과하는 트래픽을 수신하여 다양한 통계 정보로 가공하여 저장하게 된다. 가공된 데이터는 다음 표2와 같다.

표 2. 캡처된 데이터의 가공 정보

정보	설명
전체 트래픽(bps)	초당 전달된 트래픽량을 bps로 확인
전체 트래픽(pps)	초당 전달된 트래픽량을 pps로 확인
인터넷 트래픽	외부에서 내부, 내부에서 외부로 전달되는 데이터를 인터넷 트래픽으로 구별하여 수집
서브넷 트래픽	세그먼트 내부 트래픽과 인터넷 트래픽을 구별한다.
프레임 사이즈별 분석	프레임 사이즈를 <= 64, 65-84, 85-128, 129-512, 513-1024, > 1024 범위로 구별하여 트래픽을 수집한다.
프로토콜별 분석	프로토콜 종류에 따라 1초간 누적된 데이터 정보를 전달한다.
호스트Top10	호스트별 트래픽 누적 양을 출력한다.
IP Matrix	IP 쌍별(근원지-목적지) 트래픽 누적 양을 출력한다.
MAC Matrix	MAC 주소 쌍별(근원지-목적지) 트래픽 누적 양을 출력한다.

4. 실행 및 분석

본 논문에서 구현한 성능관리 시스템은 Microsoft Windows 2000환경에서 Microsoft Visual C++ 6.0 컴

파일러를 사용하고, NetGroup의 WinPcap 3.0 패킷캡처 라이브러리와 MySQL 3.23 데이터베이스를 이용했다.

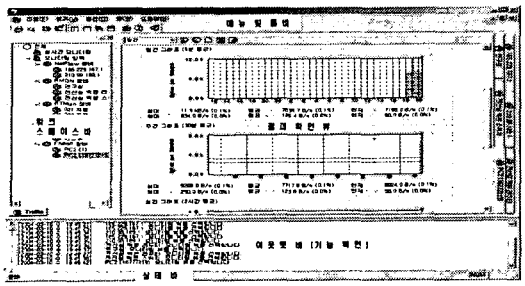

그림 3. 통합 성능관리 시스템 GUI

그림 3은 본 논문에서 구현한 통신망 성능관리 시스템 GUI를 나타낸다. 원격지의 에이전트로부터 수집된 정보를 하나의 통합 화면으로 출력한다. 워크 스페이스 바에서 등록된 EMS 항목을 확인할 수 있으며, 하위 그룹에 NetFlow 장비, RMON 장비, RTMan 장비, SNMP 장비별로 구성할 수 있다.

5. 결론

기존의 어느 한 기술로는 종합적인 네트워크 트래픽 측정이 불가능하다. 본 논문에서는 트래픽 현황을 탐지하는 기존 기술의 여러 단점을 극복하여 통합 망관리 관점을 제공할 수 있도록, 하나의 정보 모델로 여러 트래픽 측정 기술들을 통합하는 구조를 제시하고 패킷캡처를 담당하기 위한 트래픽 캡처 에이전트(RTMan 에이전트)의 구조를 제시하였다. 또 제시한 구조에 따라 성능관리 시스템을 구현하였다.

본 논문에서 제안한 통합적인 트래픽 정보 검출 구조는, 기존의 성능관리 제품들이 다양한 전송기술(Multi-technology)과 다양한 장치 제조사(Multi-vender) 장비들로 구성된 현실적인 통신망에서 성능관리를 제대로 할 수 없다는 문제점을 해결하였다.

RMON, Netflow 및 패킷 캡처와 같은 이종의 트래픽 측정 기술들을 하나로 통합하여 현대의 다양한 전송기술과 다양한 장치제조사 기반의 네트워크에 적합한 차세대 통합 트래픽 측정 기술을 개발하고, 그 응용으로 전사적인 네트워크를 포괄하는 프로토콜별 및 사용자별 트래픽 분석(Traffic analysis) 시스템을 개발하였다.

[참고문헌]

[1] ITU-T Rec. M.3010, "Principles for a telecommunications Management Network", 1992.

[2] ITU-T Rec. M.3400, "TMN Management Functions", 1997.

[3] J. W. Hong, J. Y. Kong, J. S. Kim, J. T. Park and J. W. Baek, "Web-based Intranet Services and Network Management", IEEE Communications Magazine, Vol. 35, No. 10, pp.100-110, 1997.

[4] Cisco Systems, "NetFlow Performance Analysis", 2002.

[5] IETF RFC 1757, "Remote Network Monitoring Management Information Base", 1995.

[6] Fulvio Risso and Loris, "An Architecture for High Performance Network Analysis", 2000.

[7] Steven McCanney and Van Jacobsony, "The BSD Packet Filter: A New Architecture for User-level Packet Capture", 1995.

[8] IETF RFC 1157, "A Simple Network Management Protocol (SNMP)", 1990.

[9] IETF RFC 1155, "Structure and Identification of management information for TCP/IP-based Internets", 1990.

[10] IETF RFC 1066, "Management Information Base for Network Management of TCP/IP-based internets", 1988.

[11] George Pavlou, "Telecommunication Management Network: A Novel Approach Towards its Architecture and Realization Through Object-Oriented Software", Thesis of the degree of Doctor, 1998.