네트워크 디스커버링을 통한 윈도 NT 서버 모니터링 시스템

조 현 영 · 김 성 조
중앙대학교 컴퓨터공학과

Windows NT Server Monitoring System through Network Discovering

Hyun-Young Cho, Sung-Jo Kim
Dept. of Computer Science & Engineering, Chung-Ang University

요 약

인터넷 사용자의 급격한 증가로 인해 사용자들은 더욱 다양한 인터넷 서비스들을 제공받기를 원하고 있다. 사용자들의 다양한 요구를 원활히 충족시켜주기 위하여 인터넷 서버의 성능은 날로 증대되고 있으나 서버의 관리는 네트워크의 크기가 증대될수록 점점 더 어려워지고 있다. 또한 기존의 인터넷 서버 시장은 유닉스 계열의 서버가 우위를 차지하고 있었지만, 최근 개인 PC 서버의 증가로 인해 윈도 NT 서버가 전체 서버 시장에서 차지하는 비율이 커지고 있다. 본 논문은 유닉스 서버에 비해 상대적으로 연구가 미약했던 윈도 NT 서버를 관리할 수 있는 모니터링 도구를 제시한다. 순간적으로 변화하는 네트워크 상황에 적응하기 위하여 윈도 NT 서버를 탐지할 수 있는 네트워크 디스커버리 기법을 접목함으로써 관리 대상 서버의 선택을 손쉽게 하고자 하였고, PDH 라이브러리를 사용하여 윈도 NT 서버의 관리를 보다 효율적으로 수행하였다.

1. 서론

인터넷 사용자가 급격히 증가함에 따라 이를 수용하기 위해 네트워크의 속도가 더욱 고속화되어가고 있고, 사용자들에게 다양한 정보를 제공해줄 수 있는 서버의 수도 증가하고 있다. 사용자들은 인터넷 서버들이 웹이나 FTP 등 하나의 서비스만을 제공해주던 상황에서 벗어나 웹과 전자 메일, FTP, DNS, 뉴스, Proxy 등 다양한 서비스들을 함께 제공해주기를 요구하고 있다. 이를 위해 서버의 성능은 날로 증대되고 있으나, 서버의 관리는 네트워크의 크기가 커져감에 따라 점점 더 복잡해지고 있는 상황이다[1]. 또한, 네트워크 상황은 끊임없이 변하고 있어 이의 구조를 정확하게 파악하는 일은 중요하다. 최신의 네트워크 구조를 파악하고 인터넷 토폴로지(topology)를 구축하기 위해 네트워크 디스커버리(discovery) 기법이 사용되는데, 이를 통해 액티브(active)한 서버와 네트워크 장비를 발견함으로써 변화하고 있는 네트워크 상태를 자동으로 탐지할 수가 있다[2][3].

인터넷 서버 시장은 윈도 NT 서버의 등장으로 인해 조금씩 그 상황이 변하고 있다. 가트너그룹의 조사에 의하면 97년도에 전체 서버 시장의 10% 정도만을 차지했던 NT 시장이 올해엔 41%, 2005년도엔 50%까지 차지할 것으로 예측하고 있다. 서버 시장에서 NT가 차지하는 비율이 높아져가고 있지만, 아직까지 NT 서버 시스템의 모니터링이나 관리 시스템은 부족한 상황이다. 본 논문에서는 네트워크 상태를 자동으로 탐지할 수 있는 디스커버링 기법을 바탕으로 관리 대상인 NT 서버를 찾아내고 이를 효율적으로 관리할 수 있는 시스템을 개발하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문의 기반이 되는 네트워크 디스커버링 기법과 인터넷 서버 관리 기법에 대하여 살펴본다. 3장에서는 본 논문에서 제안하고자 하는 NT 서버 성능 모니터링 시스템에 대하여 설명하고, 4장에서는 이의 구현 상황에 대해서 기술한다. 마지막으로 5장에서는 결론과 향후 연구 과제에 대해 논의하고자 한다.

2. 관련 연구

2.1 네트워크 디스커버링

네트워크 상태는 끊임없이 변화하므로, 최신의 네트워크 상태를 유지하기 위해 이의 상태 변화를 지속적으로 갱신시켜주어야 한다. 이와 같이, 최신의 네트워크 구조를 파악하고 인터넷 토폴로지를 구축하기 위한 네트워크 디스커버리(discovery) 기법이 요구되어 다음과 같은 다양한 디스커버리 기법들이 제안되었다[2][3][4].

첫째, ping 명령어를 이용하여 이에 대한 응답 여부를 가지고서 서버의 동작 여부를 알아내는 방법이다. 이 중 aaa.bbb.ccc.0이나 aaa.bbb.ccc.255의 주소로 명령어를 보내는 broadcast ping 방식이 많이 사용되는데, 이는 해당 서브넷에 속해 있는 모든 호스트들로부터 응답을 받게 된다. 어떤 네트워크에서는 라우터만이 응답을 하기도 하고, 또 다른 네트워크는 서비스 거부(denial-of-service) 공격을 막기 위해 broadcast ping에 대해서 전혀 응답을 하지 않는 문제점이 있다.

둘째, 특정 주소까지의 경로를 알아보기 위한 traceroute 명령어를 사용하는 방법이다. 이 방식은 호스트까지의 패스상에 있는 라우터에게 두 번의 probe 메시지를 보내야하기 때문에, ping을 이용하는 방법에 비해 오버헤드도 더 크고, 네트워크 부하를 최소화하기 위해 일정 간격을 두고 probe 메시지를 보내기 때문에 시간도 더 오래 걸리는 단점이 있다.

셋째, 도메인 네임 서버에 저장되어 있는 호스트 이름과 IP 쌍의 정보를 이용하는 방법이다. 도메인 네임 서버에 "zone transfer" 명령어를 내리면 해당 도메인에 속해 있는 모든 호스트의 이름을 반환하게 되어 특정 도메인 내에 있는 호스트와 라우터의 이름을 알아내는데 유용하게 사용될 수 있다. 이 방법은 도메인 네임 서버에 등록된 호스트만을 탐지할 수 있다는 문제점이 존재한다.

마지막으로, 어느 도메인에서나 사용할 수 있는 가장 간단한 방법으로 SNMP(Simple Network Management Protocol)를 이용하는 방법이 있다. SNMP 데몬이 설치되어 있는 라우터의 MIB(Management Information Base) 정보 중에서 ARP

(Address Resolution Protocol) 테이블을 통해 해당 라우터에 연결되어 있는 호스트들을 알아낼 수 있고, ipRoute 테이블을 통해서는 근처 라우터의 정보를 획득할 수 있다. 이 방법은 다른 방식에 비해 효율적이고 빠르며 정확하지만, SNMP 데몬이 설치되어 있는 곳에서만 사용할 수 있다는 단점이 있다.

2.2 분산 환경에서의 NT 서버 모니터링

인터넷 서버 관리와 모니터링 기술은 효율적이고 원활한 인터넷 서비스를 제공하는데 필수적이다. 현재 서버나 네트워크를 관리하기 위한 방식은 대부분 분산 환경을 이용하는 원격(remote) 관리 방식이 사용되고 있어, 네트워크의 복잡성이 증가하고 이질성이 커질수록 이를 통합하여 지속적으로 네트워크를 관리할 수 있는 방향으로 나아가고 있는 추세이다[1].

NT 서버의 여러 시스템 정보들을 얻기에 가장 좋은 방법은 시스템 레지스트리(registry)에서 필요한 값을 얻어내는 것이다. 그러나, 레지스트리로부터 직접 추출하는 정보들은 가공이 덜 된 저급 정보이기 때문에 판독하기 쉬운 자료로 변환을 시켜주어야 하는 어려움이 있다. NT 서버의 시스템 정보를 좀 더 편하고 효율적으로 살펴볼 수 있도록 만든 것이 PDH (Performance Data Helper) 라이브러리(library)로, 이는 새로운 기능이 추가된 것이 아니라 기존에 존재하던 NT 서버의 성능 모니터링 기반 위에 구축된 것이다[5].

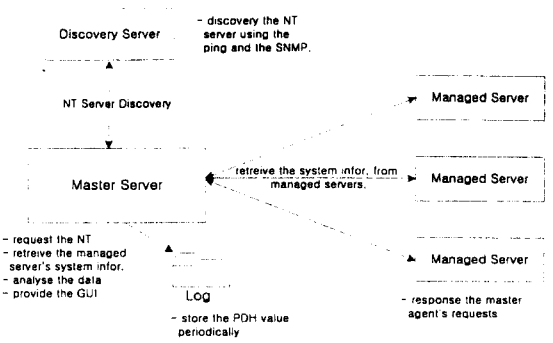
PDH 라이브러리를 이해하기 위해서 몇 가지 핵심 단어를 살펴볼 필요가 있다. 우선, 카운터(counter)는 성능 유닛을 나타내는 것으로 관리 대상 서버에서 추출할 수 있는 단일 아이템에 관련된 데이터를 제공해 준다. 오브젝트(object)는 측정 가능한 엔티티(entity)를 지칭할 때 쓰이는 단어로, Memory나 Process, Processor, System, Thread 등이 이에 속한다. 각각의 오브젝트는 서로 다른 카운터 집합을 가지고서 동작한다. 쿼리(query)는 카운터들을 모아놓은 것으로, 이 쿼리를 실행시키면 카운터에 속한 모든 정보가 갱신된다. 또 다른 중요한 키워드로서 패스(path)가 있는데, 이는 텍스트 문자열로 이루어져서 특정 카운터의 위치 정보를 나타낸다[5][6].

PDH 라이브러리를 사용하게 되면 NT 서버에서 기본으로 제공하는 시스템 레지스트리의 정보를 얻게된다. 따라서, 관리 대상 서버에 새로운 관리 프로그램을 설치해야 하는 등의 추가 작업은 하지 않아도 된다.

3. 시스템 제안

본 논문에서 제안하고 있는 NT 서버 모니터링 시스템은 <그림 1>과 같이 마스터 서버, 디스커버리 서버, 관리 대상 서버로 구성되어 있다. 마스터 서버에는 PDH 라이브러리를 작동시킬 수 있는 환경이 구축되어 있어야 하며, 디스커버리 서버는 네트워크 디스커버리를 수행하는데 필요한 SNMP 에이전트가 탑재되어 있어야 한다. 앞 절에서 살펴본 각각의 디스커버리 방식들은 모두 장단점을 가지고 있기 때문에 한가지 방법만을 사용하여서는 정확한 네트워크 상태를 알아내기가 힘들다. 또한, 네트워크 디스커버리 작업은 작업의 특성상 시간이 많이 소요되기 때문에 별도의 서버를 두어서 전체 시스템의 효율을 높이고자 하였다. 본 시스템에서 수행하게 되는 네트워크 디스커버리 방법은 가장 널리 사용되는 ping 명령어를 이용한 방식과 네트워크 환경에서 NT 서버를 정확히 탐지해낼 수 있는 SNMP를 이용한 방식을 접목시켜 사용한다.

각 서버의 역할은 다음과 같다.



[그림 1] NT 서버 모니터링 시스템

3.1 마스터 서버

마스터 서버는 디스커버리 서버를 통해 사용자가 정의한 전체 서브 네트워크 상에서 관리 대상 NT 서버를 탐지한다. 네트워크 디스커버리 작업은 부하와 시간이 많이 소요되는 작업이기 때문에, 사용자의 요청이 발생했을 때 작업을 수행하게 된다. 마스터 서버는 디스커버리 서버로부터 관리 대상 서버를 넘겨받은 후, 이들 관리 대상 서버의 동작 상황을 체크하게 된다. 마스터 서버는 각 관리 대상 서버마다 쓰레드를 하나씩 생성하여 관리 대상 서버의 시스템 정보를 획득한다. 관리 대상 서버마다 쓰레드를 생성함으로써 발생되는 이점 중 하나가 시스템 정보를 추출하는 작업을 백그라운드로 처리할 수 있다는 것이다. 쓰레드를 통해 지속적으로 관리 대상 서버의 정보를 얻어와 이를 로그화 시켜서 저장하고, 사용자의 요청이 있을 때 즉시 정보를 출력시켜준다. 로그를 기록하는 것은 분석 작업에 도움이 된다. 저장된 로그 기록을 살펴봄으로써 과거의 시스템 상황과 현재의 시스템 상황을 비교할 수 있고 시스템의 변화 상태라든가 추가 자원의 필요성을 파악하기에도 용이한 이점이 있다. 사용자들은 마스터 서버에서 제공하는 GUI 기능을 통해 시스템 정보에 대한 이해력을 높일 수 있고 관리 시스템의 상태를 편리하고 쉽게 살펴볼 수 있다.

마스터 서버는 일반 NT 서버에서 기본적으로 제공해주는 기능 외에 PDH 라이브러리를 사용해야 하므로, 이를 미리 설치해야 한다.

3.2 디스커버리 서버

디스커버리 서버는 시간과 부하가 많이 걸리는 네트워크 디스커버리 작업을 따로 수행함으로써 전체 시스템의 효율을 높이고자 한 것이다. 본 시스템에서는 ping을 이용한 방법과 SNMP를 이용한 방법을 같이 사용하여 좀 더 정확히 NT 서버를 탐지를 할 수 있도록 하였다. broadcast ping을 사용하지 않고 사용자가 지정한 서브넷에 있는 모든 호스트에 ping 메시지를 보내어 서버의 구동 상태를 검사하는데, 이는 broadcast ping의 단점을 보완하고자 한 것이다. 액티브(active)한 서버라 판명이 되면 SNMP를 사용하여 각 호스트가 NT 서버인지를 판단하게 된다. 이는 각 호스트에 설치되어 있는 SNMP 데몬을 이용함으로써 사용되고 있는 OS의 종류를 정확히 파악해낼 수 있기 때문이다. 네트워크 디스커버리 작업은 사용자의 요청이 생겼을 때 마스터 서버가 디스커버리 서버에게 요구를 하여 수행하게 된다.

3.3 관리 대상 서버

여러 가지 인터넷 서비스들이 동작되고 있는 관리 대상 서버들은 디스커버리 기능을 통해 발견되어 관리 대상 서버 목록

에 포함된다. 관리 대상 서버들은 마스터 서버로부터 시스템 정보에 대한 요청이 들어오면 응답을 해준다. 각각의 관리 대상 서버는 프로그램이 종료할 때까지 마스터 서버가 요청한 PDH 카운터들에 대한 정보를 지속적으로 제공해준다.

4. 시스템 구현

본 절에서는 앞 절에서 제안하였던 NT 서버 모니터링 시스템에 대해 모니터링 방법을 중심으로 기술한다.

4.1 인터넷 서비스

네트워크의 속도가 빨라지고 사용자들의 요구가 다양해짐에 따라 웹과 FTP, 이메일 등 현재 많은 인터넷 서비스가 제공되고 있다. 본 시스템에서는 <표 1>과 같이 많이 사용되고 있는 핵심적인 인터넷 서비스의 이상 유무를 검사한다. 여러 인터넷 서비스의 정상적인 작동 여부를 검사함으로써 관리 대상 서버가 제공하는 서비스에 문제가 발생했는지를 쉽게 발견할 수 있다.

<표 1> 관리 대상 인터넷 서비스

서비스	내 용
HTTP	웹 서비스 프로토콜
FTP	파일 전송 프로토콜
DNS	도메인 네임 서비스 프로토콜
SMTP	메일 전송 프로토콜
POP3	외부 메일 수신 프로토콜
NNTP	뉴스 서비스 프로토콜

<표 2 > 관리 대상 서버의 시스템 정보

PDH 카운터	카운터 정보
System : Processor Queue Length	현재 CPU의 부하
Memory : Committed Bytes	관리대상서버에서 현재 사용중인 메모리
Memory : Commit Limit	관리대상서버의 전체 메모리
Network Interface : Current Bandwidth	사용자가 정의한 네트워크 I/F 사용율의 경고 수치
Network Interface : Packet outbound Errors	사용자가 정의한 네트워크 I/F 에러율의 경고 수치
Network Interface : Packet Received Errors	네트워크 전송 패킷 에러 수
Network Interface : Packets/Sec	초당 평균 네트워크 전송 패킷 수
Process : Thread Count	웹 서버의 쓰레드 개수
Process : Virtual Bytes	웹 서버의 프로세스 크기
Web Service : Total Method Requests	웹서비스의 평균 요구량
Web Service : Total Not Found Errors	제공되지 않은 평균 웹서비스 회수

4.2 시스템 정보

PDH 라이브러리를 사용하여 획득할 수 있는 시스템 정보는 매우 다양하지만, 이 정보를 모두 사용하는 것은 오버헤드가 크다. 본 시스템에서는 이러한 정보들 중에서 인터넷 서버를 관리하는데 필요한 핵심 정보만을 사용한다[7][8]. PDH 라이브러리를 사용하여 관리 대상 서버로부터 획득하는 시스템 정보는 <표 2>와 같다. 관리 대상 서버로부터 얻어오는 시스템 정보 중 웹서버에 관련된 정보가 많이 포함되어 있는데, 이는 많은 인터넷 서비스 중 웹 서비스를 제공하는 서버의 수가 상대적으로 많고 또한 이들 웹 서버의 관리가 더욱 중요하기 때문이다. 이렇게 획득된 정보를 마스터 서버에서는 로그로 기록해 두고, 사용자에게 GUI 기능을 제공할 때 저장된 정보를 분석하여 사용한다. 분석 기능과 함께 많이 사용되는 기능으로 장애 관리 기능이 있다. 본 시스템에서도 사용자가 미리 정의해 놓은 임계값과 관리 대상 서버로부터 획득한 정보를 비교하여 문제가 발생되기 전에 조치를 취할 수 있도록 하고 있다.

5. 결론 및 향후 연구 과제

본 논문에서는 네트워크 디스커버리를 통해 윈도 NT 서버를 탐지하고, 이를 통해 발견된 NT 서버를 관리하는 모니터링 시스템을 제시하였다. 윈도 NT 서버의 관리는 PDH 라이브러리를 사용함으로써 관리 대상 서버에 특정 프로그램을 설치하지 않고서도 CPU의 부하나 메모리의 사용량, 네트워크의 사용률 등을 모니터링하고 관리할 수 있는 특징이 있다. 인터넷 사용자와 서비스의 증가로 인해 인터넷 서비스를 제공해주고 있는 NT 서버가 증가되고 있는 상황에서 본 모니터링 시스템의 사용은 인터넷 서비스의 작동 유무뿐만 아니라 서버의 원활한 동작 상황까지 살펴 볼 수 있어 NT 서버를 효율적으로 관리하는데 도움이 될 것이다.

향후 본 연구에서 제안된 시스템은 윈도 2000 시스템을 모니터링 할 수 있는 기능이 추가되어야 한다.

참고 문헌

[1] Luca Deri, "Network Management for 90s", *Proceeding of ECOOP'96 Workshop*, July, 1996.

[2] R. Siamwalla, R. Sharma, and S. Keshav, "Discovering Internet Topology", http://www.cs.cornell.edu/skeshav/papers/discovery.pdf, July, 1998.

[3] J. Schonwalder and H. Langendorfer, "How to Keep Track of Your Network Configuration", *LISA*, November 1993.

[4] Ramesh Govindan, Hongsuda Tangmunarunkit, "Heuristics for Internet Map Discovery", Technical Report 99-717, Computer Science Department, University of Southern California.

[5] Allen Denver, "Using the Performance Data Helper Library", http://msdn/microsoft.com/library/techart/msdn_pdhlib.htm, March, 1997.

[6] Matt Pietrek, "Under The Hood", http://msdn.microsoft.com/library/periodic/period98/msj0598hood.htm, May, 1998.

[7] Scott B. Suhy, "Performance Tuning Windows NT", http://www2.slac.stanford.edu/comp/winnt/perftune.htm, April, 1999.

[8] Michael D. Relly, "More Windows NT Performance Monitor", http://www.windntmag.com, April, 1997.