Libpcap를 이용한 Cacti기반 네트워크 트래픽 모니터링 시스템

초황 · 반태학 · 함종완 · 정선철 · 정회경

배재대학교 컴퓨터공학과

A Study on the Cacti-based Network Traffic Monitoring System Using Libpcap

xiao-huang · Tae-hak Ban · Jong-wan Ham · Sun-chul Jeong · Heo-kyung Jung

Dept. of Computer Engineering, Paichai University

E-mail : {xiaohuang, banth, jongwanham, harrison, hkjung}@pcu.ac.kr

요 약

네트워크 기술이 빠르게 성장함에 따라 네트워크 환경도 복잡해지고 있다. 이에 따라, 네트워크 트래픽이나 정보를 이용하여 실시간으로 자원을 모니터링 하는 기술들이 발전하고 있다. 대표적인 모니터링 툴은 Cacti이다. Cacti는 RRDTool(Round Robin Database tool), SNMP(Simple Network Management Protocol)를 기반으로 한 모니터링 툴 이다. 본 논문에서는 Cacti와 Libpcap 기반으로 시스템을 개발하여 실시간으로 대상을 모니터링 할 수 있다. 본 시스템은 Libpcap으로 포착한 네트워크 트래픽 패킷을 분석하고 그래프 형식으로 Cacti에서 표현되어 모니터링을 할 수 있다. 본 시스템은 높은 효율성을 가지며 관리가 간편하고 정확성을 가지므로, 향후 널리 활용될 것으로 보인다.

ABSTRACT

For network is growing at a rapid rate, network environment is more complex. The technology of using network traffic to monitor our network in real-time is developed. Cacti is a representative monitoring tool which based on RRDTool(Round Robin Database tool), SNMP(Simple Network Management Protocol). In this paper, it show you how to develop a system which based on Cacti and Libpcap to monitor our monitored objects. At this system, using Libpcap to capture network traffic packets, analyze these packets and then turn out in Cacti in graphical form. So as to achieve monitoring system. This system's execution is efficient and the management is easy and the results are accurate, so it can be widely utilized in the future.

키워드

Cacti, Libpcap, network traffic, 트래픽, 모니터링

Ⅰ. 서론

사회정보화가 발전하고 네트워크 영역이 점점 더 넓어지고 네트워크 기술도 빠르고 혁신적으로 변화하고 있고, 네트워크 구조 역시 복잡해지고 있다. 네트워크에서 트래픽은 작은 변화에도 네트워크 안전과 애플리케이션에 큰 영향을 끼친다. 이를 통해 네트워크의 동작 상태를 전체적으로 분석하여 네트워크의 안정적 운영, 관리를 함으로써, 큰 도움을 줄 것이다[1].

본 시스템은 1분마다 네트워크 카드에서 패킷을 캡처하고 캡처 한 데이터가 쉘 프로그램을 통하여 패킷들의 정보들을 통계해 분석한다. 그 다음에 이 데이터를 이용하여 Cacti에서 그래프가 나타난다. 만약에 어떤 패킷의 수량은 미리 설정된 값보다 크면 이 시스템은 자동적으로 관리자에게 알림 이메일을 보낸다.

본 논문의 구성은 다음과 같다. 2장에서는 Cacti과Libpcap를 기술한다. 3장에서는 시스템 환경, 원리 및 구조를 어떻게 설계한다. 4장에서는 실험에서 나타난 결과를 분석하고 결론 및 향후 연구과제는 5장에서 기술한다.

Ⅱ. 관련 연구

2.1 Cacti 개요

RRD(Round Robin Database)는 네트워크 대역폭, 기계실 온도, 서버의 평균 부하 등과 같은 시간대별 데이터를 저장하고 표시하기 위한 시스템

이다. RRD는 매우 간결한 방법으로 데이터를 저장하므로, 시간이 흐름에 따라 양이 그리 크게 늘어나지 않는다. RRD는 항상 일정한 데이터 밀도를 강제로 유지하기 위해 데이터를 처리함으로써, 유용한 그래프를 제공한다. 이를 위해서는 쉘이나 펄 등으로부터 만들어진 단순한 래퍼 스크립트나, 또는 네트워크 장비에 주기적으로 질문을 던지고 편리한 인터페이스를 제공하는 프론트엔드의 이용 등 어떤 방식이라도 이용할 수 있다[2]. Cacti는 RRDTool의 데이터베이스를 이용한 웹 그래픽 생성엔진이다. Cacti는 각종 데이터를 MySQL등의 데이터베이스에 시스템 상황 등의 데이터 값을 저장하고 시간단위로 저장된 데이터를 분석하여 웹상에서 그래프를 생성하여 보여주는 매우 유용한 시스템 모니터링 도구이다[3]. 그림 1은 Cacti의 작업 원리를 표현한다.

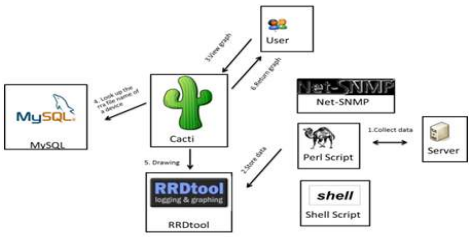

그림 1. Cacti 실행 원리

2.2 Libpcap 개요

패킷 캡쳐란 네트워크를 돌아다니는 패킷정보를 보는 것이다. 일반적인 인터넷 환경에서 라우터는 내부 네트워크로 향하는 패킷을 브로드캐스팅하게 되고 각 컴퓨터들은 자신의 인터페이스로 들어오는 패킷 중 목적지가 자신인 경우에만 받아들여 이를 운영체제가 처리한다. 패킷 캡쳐는 이처럼 자신에게 전달되는 패킷을 받아들여 패킷의 내용을 확인할 수 있음을 의미한다. 이러한 패킷 캡쳐는 네트워크의 사용에 대한 통계나 보안을 목적으로 하는 모니터링, 네트워크를 디버깅하기 위한 목적, 스니퍼링 등 다양한 형태로 응용이 가능하다[4][5].

Libpcap은 이러한 패킷 캡쳐를 용이하게 해주는 라이브러리이다. 각 운영체제 벤더들이 각각의 패킷 캡쳐 도구들을 제공하고 있어 개발이나 포팅 등에 어려움이 있기 때문에 각 도구들의 기능을 포함하면서 시스템에 독립적인 Libpcap이 등장하게 되었다. 그림 2는 Libpcap를 이용하고 네트워크 카트가 패킷을 잡은 과정이다.

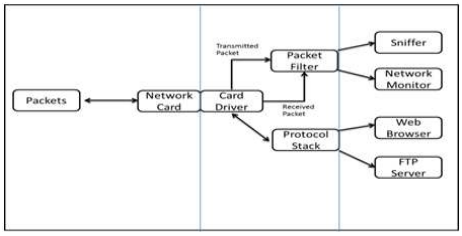

그림 2. 패킷을 처리 과정

Ⅲ. 시스템 설계

3.1 시스템 설계 원리

본 시스템 설계 원리를 여러 가지 호스트가 모니터링 대상을 방문하고 1분마다 이 방문수량을 기록하고 이 방문수량은 어떤 처리 방식을 이용하여 같지 않은 데이터 정보를 얻을 수 있다. 이 데이터 정보를 통계하여 그 다음에 이 데이터를 이용하고 그래픽 형태로 Cacti에서 나타난다. 만약에 어떤 패킷의 수량은 미리 설정된 값보다 크면 이 시스템은 관리자에게 이메일로 보내고 경고를 나타나서 실시간으로 목적 대상을 모니터링하기를 성취한다. 이 설계 원리가 그림 3과 같다.

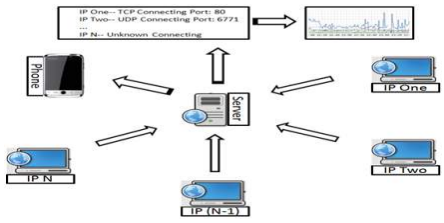

그림 3. 시스템 설계 원리

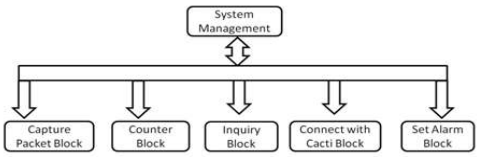

그림 4. 시스템 구조

3.2 시스템 구조

본 시스템은 그림 4와 같은 다섯 부분으로 구성되어 있다. 첫 번째 부분은 패킷을 캡쳐된 부분이며, 두 번째 부분은 패킷의 통계 부분이며, 셋 번째 부분은 데이터 쿼리 부분이며, 넷 번째 부분은 Cacti를 연결하는 부분이며, 경고하는 부분은 마지막 부분에 나타난다. 패킷을 캡쳐하는 부분은 네트워크 카트에 모든 지난 패킷을 캡쳐 하는 과정이다. 이 과정에서 생긴 데이터 흐름은 두 번째 부분에서 통계 처리하고 셋 번째 부분에서는 지난 데이터 흐름은 하루 동안 파일에 백업한다. Cacti로 연결 부분은 DB, Perl Script를 만들고

Cacti에서 data input method를 설치한 후에 모니터닝 대상이 추가 된다. 경고부분은 Cacti의 'Alerting/Thold'을 이용하고 이메일을 보내는 것이다.

Ⅳ. 실험 결과 및 분석

4.1 실험 결과

PuTTy는 telnet, rlogin, SSH(Secure SHell)프로토콜을 이용하며 윈도우에서 리눅스 서버로 로그인할 수 있는 원격 터미널 프로그램이다. 본 실험은 시스템을 자극하여 데이터를 생긴다. 그림 5는 1분마 DB안에 있는 데이터 업데이트 하고 있다. 그림 6은 Cacti가 15초마다 DB에서 데이터를 취득하고 그래프 한 과정화면 이다. 그림 7은 로그파일 내용이고 그림 8은 알림 이메일이고 그림 9는 점시 후에 나타난 그래프이다.

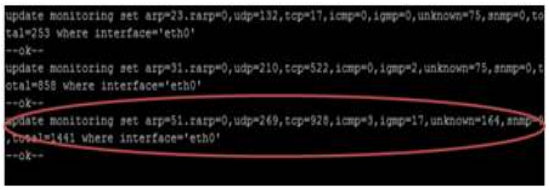

그림 5. DB 데이터 업데이트

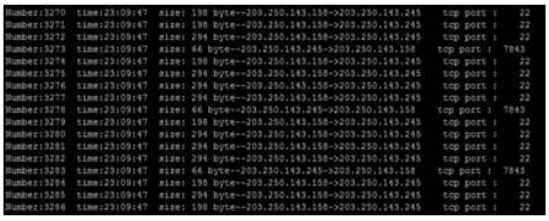

그림 6. 로그 파일

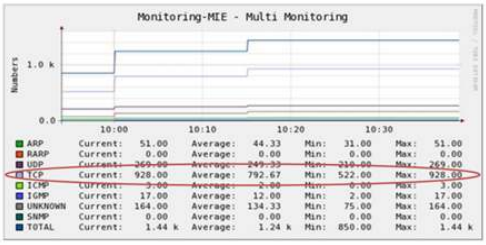

그림 7. 그래프

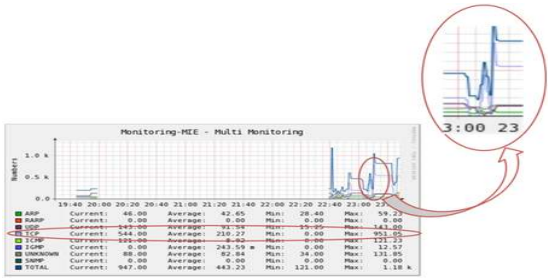

그림 8. 경향 그래프


From: **admin** <xiaodongyixin@qq.com>
Date: 2011/5/19
Subject: Monitoring-MIE - Multi Monitoring [TCP] went above threshold of 100 with 109
To: xiao58588395@gmail.com

An alert has been issued that requires your attention.

Host: Monitoring-MIE (203.250.143.158)
203.250.143.158: http://203.250.143.158///graph.php?local_graph_id=101&rra_id=1
Message: Monitoring-MIE - Multi Monitoring [TCP] went above threshold of 800 with 928

그림 9. 알림 이메일

4.2 실험 분석

PuTTy가 신뢰할 수 있는 TCP 프로토콜 기반 신뢰성 있는 클라이언트 터미널 프로그램이고 SSH 프로토콜은 통신 포트는 22이다. 그리고 위에 있는 정보들을 조차해보고 본 시스템의 신뢰성, 정확성 및 실시간성 다 확인 할 수 있다.

Ⅴ. 결론 및 향후 연구 과제

본 시스템은 오픈 소스 Cacti 기반으로 설계된다. 이 시스템은 사용이 쉽고 또한, 데이터를 저장 방식은 RRD방식을 사용한다. 가장 중요한 것은 결과의 정확성, 그래픽의 직관성, 안전의 실시간성을 가지고 있다, 하지만 이 시스템은 몇 개 부적한 점이 있다. 첫 번째는 쿼리 부분이다. 로그 파일을 확인하기 불편하다. 두 번째는 이 시스템은 Ethernet 유형만을 고려한다. 이런 복잡한 네트워크 환경은 더 많이 유형을 고려해 야 한다.

참고 문헌

[1] Myung-Sup Kim, Yong J.Won, and James Won-Ki Hong, "Application-Level Traffic Monitoring and an Analysis on IP Networks", ETRI Journal, Volume 27, Number 1, February 2005
[2] http://www.mrtg.org/rrdtoo
[3] http://www.cact.net/features.php
[4] 노광민 "리눅스에서 pcap library를 사용하여 패킷을 잡아보기 v0.3" 2000.09.14
[5] 강승일 "Packet Capture using Libpcap" 2006.03.10