The Design and Implementation of a Network Traffic Monitor

Luo Wanming  
Computer Network Information Center,  
Chinese Academy of Sciences  
Beijing, P.R.China, 100080  
lwm@cnic.ac.cn

Yan Baoping  
Computer Network Information Center,  
Chinese Academy of Sciences  
Beijing, P.R.China, 100080  
ybp@mimi.cnc.ac.cn

Abstract
Network measurement is a key technology for network performance analysis and is becoming more and more important in the Internet research fields. In this paper a network traffic monitor for collecting and analyzing network information is presented, which is based on passive measurement. The system architecture and hardware/software modules are designed and several key technical issues are also investigated. Finally the implementation of this monitor is given too.

Keywords
network monitor, passive measurement, architecture.

1. Introduction
As the Internet has grown, so has the expending and complexity of the Internet traffic. People find that it becomes more and more difficult to investigate the Internet and network performance analysis also become more and more important. In order to study network characteristics what to do at first is to capture and analyze the network traffic information.

Network measurement is a key technology to complete the above tasks. IETF Working Group named IPPM (Internet Protocol Performance Metrics [1]) has designed a series of methods and metrics for network measurement. Generally all measurement technologies can be classified into two types: active and passive measurement. With active measurement network performance statistics can be get by using some tools such as ping, traceroute and so on. AMP (NLANR Active Measurement Project [2]) funded by American NSF use above methods to measure vBNS performance. However this mode of measurement may affect the relevant network due to sending packets to the network. With passive measurement traffic can be captured ‘silently’ without affecting any networks. In this paper we will introduce a network traffic monitor which we have developed and has a lot of functionalities.

The rest of the paper is organized as follows. In section 2, we present the system architecture of the network traffic monitor. In section 3 we give the software architecture and functionality of this monitor. In section 4 several key technical issues will be analyzed in order to archive functionality we needed. Implementation of the prototype will be demonstrated in Section 5. Finally, Section 6 concludes the paper.

2. System Architecture
This system primarily includes three parts, collecting point, Storage site and analysis&statistic part. Figure 1 gives the system architecture of the monitor, which is discussed later, and shows how the components interact. The monitor is a real time system. Collecting point reads/captures raw packets from network interface directly, and generate flow data. The capture of packets can be implemented base upon libpcap. Storage site is in charge of storing the traffic data from collecting point. Analysis&Statistic part includes web-based service interface and interactive management. They are offline, using data collected by the storage site, and generating report.

1 This paper is funded by Chinese national high technology Research and Development Program (863 Program)(NO. 2001AA112040 and NO.2001AA112136)
3. Software Architecture and Functionality

The figure 2 below depicts software architecture and functionality of the system. At the lowest level are the different network interface modules that perform basic functions such as packet/cell header extraction. For high speed interfaces, these modules are typically implemented by dedicated interface cards. For low speed interfaces, they are usually implemented by the respective interface chipset with code as part of the operating systems. Above the network interface level are various software modules for traffic analysis and management functions.

The second is how to store massive raw data collected by the monitor. There are two formats to store data. One is to use text files and the other is to use database system. Text file may give us some flexibility for defining and storing data. But database system is more feasible and mature to use. Furthermore database system can provide record operations (such as insert, delete, etc) faster than text file. The characteristic that database system is a distributed system in nature is very important too. In our monitor we adopt database system to store raw data.

4 Analysis of the key technical issues

To get the above functionality several technical issues should be considered carefully.

The first one is how to capture all packets through network at high speed. We adopt some special network interface cards. For 10/100M Ethernet network we use one 100M fast Ethernet interface card which is set to promiscuous mode to get packets going in or out the network. For POS/ATM networks we use special high-speed interface card to capture cells or packets. Within Operating System we make use of BPF (Berly Packet Filter [3]) as a data link interface. figure 3 shows the principle of BPF.

5 Implementation of the monitor’s prototype

According to the above design we have developed a prototype of network traffic monitor. This prototype integrates a series of advanced computer technologies such as Oracle database, JAVA, JSP, JDBC and so on. Following list shows main data structure used in the monitor.

- Collecting point ID
- Destination and source address of data link level
- Network protocol types
- Destination and source address of network level
- Port numbers of network level
- Transport protocol types
- Port numbers of Transport level
- Number of packets
For analysis of network traffic information the taxonomy is as follows:

- **Protocol-based**
  - TCP
  - UDP
  - ICMP
  - GRE
  - IPSEC-ESP
  - IGMP
  - ….

- **Application-based**
  - WWW
  - TELNET
  - FTP
  - STMP
  - ….

- **Flow-based**
- **Host-based**
  - Destination host
  - Source host

Three formats of visualization are designed and implemented: table, pie picture and plot picture.

Figure 3 and figure 4 demonstrate implementation of this monitor within one network selected to be monitored.

**6 Conclusions**

With the rapid increase in the volume and complexity of traffic on the Internet, it is both more difficult and more important to understand what happened in the network. The network traffic monitor introduced in this paper provides a strong tool for us to study network.

**7 Reference**


