Research and Design of Network Servers Monitoring System Based on SNMP

Zhen-qi WANG, Yue WANG, Guangqiang SHAO
Information and Network Management Center
North China Electric Power University
Baoding, China
w-zhenqi@ncepu.edu.cn, bdqy071100@163.com, 153181483@qq.com

Abstract----**As the Internet continues to grow; it becomes more and more apparent that the network is playing a more and more vital role. The traditional network managements just monitor the network movements and the network devices. But the network servers occupy to the core status in the network. Aiming at the network server monitor and management, we proposed a server monitor solution which is based on the SNMP protocol. Survey the research and development work under way to develop a function formidable intelligence monitor system for network servers, via the SNMP protocol, MIB-II and host resources MIB. This paper introduces analyzes the system requirement and proposes data-collecting strategy based on data type, in order to enhance the colleting efficiency. Moreover, we present the architecture and the implementation of the system.**

Keywords–network management; SNMP; server monitoring; MIB

I. INTRODUCTION

Network management refers to monitoring, organizing and controlling the network communicating services as well as the status of the network devices. The goal is guaranteeing the computer network continuing normal movement.

The standard management framework currently used in the Internet is named after its main building block: the Simple Network Management Protocol (SNMP) [1].It was devised in the late 1980s and is widely supported by network devices. The original version, now known as SNMPv1, is widely deployed. SNMPv2 adds functionality to the original version but has not achieved much acceptance. Now SNMPv3 makes additional minor functional changes and incorporates a new security approach. Although SNMP technology is now well understood and widely deployed, it is still confined to network devices and rarely used for managing systems (PCs, servers) or applications. In this paper, we present the development of monitoring system for network servers, via the SNMP protocol, MIB-Ⅱ [2] and host resource MIB.

This paper is organized into five sections: in the next section we briefly introduce the related theories, including the management model and the MIB; in section 3 we research the network servers' anomaly analysis, specify the system requirements and define the related parameters, in section 4 we present the system development in detail; in the last section we give the conclusions of the paper.

II. RELATED WORKS

This section briefly describes the network management model in section *A* and the host resources MIB in section *B*.

A. SNMP-based Network Management

The model of network management that is used for SNMP includes the following key elements [3], shown in Fig.1:

(1) Management station
(2) Management agent
(3) Management information base (MIB)
(4) Network management protocol (SNMP)

The management station serves as the interface for the human network manager into the network management system. The management station will have, at minimum: a set of management applications for data analysis, fault recovery, and so on; an interface by which the network manager may monitor and control the network; a protocol by which the management station and the managed entities exchange control and management information; a database of information extracted from the management databases of all the managed entities in the network.. Only the last two elements are the subject of SNMP standardization.

The management agent responds to requests for information from a management station, responds to requests for actions from the management station, and may asynchronously provide the management station with important but unsolicited information.

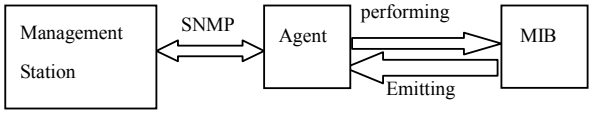

Figure 1. The manager-agent model

In order to manage the resources in a network, these resources are represented as objects. Each object is, essentially, a data variable that represents one aspect of the managed system. The collection of objects is referred to as management information bases (MIB), which are written in a language called Structure of Management Information (SMI) [4]. SMI is a data-oriented language based on Abstract Syntax Notation 1 (ASN.1).The MIB functions as a collection of access points at the agent for

978-0-7695-3557-9/09 $25.00 © 2009 IEEE
DOI 10.1109/ETCS.2009.728

the management station; the agent software maintains the MIB. A management station performs the monitoring function by retrieving the value of MIB objects.

The management station and agents are linked by a network management protocol, which includes five SNMP messages: GetRequest, GetNextRequest, SetRequest, GetResponse and trap. All the first three messages enables the management station to retrieve or set the values of objects at the agent, are acknowledged by the agent in the form of GetResponse message. In addition, an agent may issue a trap message in response to an event that affects the MIB and the underlying managed resources.

B. The Host Resources MIB & MIB-II

The host resources MIB (hr-MIB) [5] defines objects for the management of host computers – computers that communicate with other similar computers attached to the internet. Information about the hardware devices attached to hosts, software running or available on the host, along with other information such as total memory, load of the system, etc. is stored.

The hr-MIB objects are divided into six groups, including the hrSystem, hrStorage, hrDevice, hrSWRun, hrSWRunPerf, and hrSWInstalled groups. In addition, there are objects in MIB-Ⅱ which also provide host management functionality, such as the System and Interfaces groups.

In the next section, we analyze the common anomaly of network servers in detail, and introduce the method how to use the host resources MIB.

III. SYSTEM REQUIREMENTS ANALYSIS

In order to make the network severs move under an optimum performance condition, we introduced the monitored parameters and their simple implementation from 3 aspects.

SNMP protocol collects host parameters extremely abroad. But it is impossible to collect the objects in all MIBs for a perfect monitoring system. So we analyzed the normal exceptions of the network server as it is working, and then we determine which critical parameter should be monitored and its technology implementation.

(1) Server connectivity Anomaly

This exception usually occurs at the server's network interfaces, and the firewall's wrong configuration may also result in valid users can not access the server. We examine the linkage to the server by using Ping command in ICMP protocol.

(2) Server Traffic Anomaly

There are many reasons for the traffic anomaly. Such as: virus attack; system's vulnerability being used; flooding attack; the number of users proliferating during normal using time, and so on. We monitored the total number of octets, which were received on the interface and transmitted out of the interface. The Interfaces group in MIB-Ⅱ provided ifInOctets and ifOutOctets objects to describe real-time traffic. The OIDs for the two objects are 1.3.6.1.2.1.2.2.1.10 and 1.3.6.1.2.1.2.2.1.16.

(3) Server CPU Load and Memory Anomaly

The virus infection may lead server CPU load to a high level. But the services provided by the operating system back door can also lead to CPU load anomaly. If memory utilization is too high, the programs will make use of buffer substantively. Therefore, the system runs very slowly. The host.hrDevice.hrProcessorTable shows the table of processors contained by the host. We use this table to examine the whole server's CPU utilization. The host.hrStorage.hrStorageTable will be used to examine the whole memory utilization. We use the host.hrSWRun.hrSWRunPerfTable table to examine the CPU and memory utilizations of each running software.

(4) Server Buffer Blocking Anomaly

When server received a great lot of request information, the queue buffer will be full, and then the network packets will be discarded. If the server's network interface is not stable, a lot of error packets will be produced. We use ifInDiscards and ifOutDiscards objects to examine the number of inbound packets and the number of outbound packets. These two kinds of packets were chosen to be discarded by the server. The two objects come from Interfaces group in MIB-Ⅱ.

(5) Sever Network Interfaces Anomaly

We can monitor the real-time data of the number of error packets which the server discarded to examine whether server network interface appear anomaly. We use the ifInErrors and ifOutErrors objects belonging to Interfaces group in MIB-Ⅱ to describe the number of inbound packets containing errors preventing them from being deliverable to a higher-layer protocol, and the number of outbound packets that could not be transmitted because of errors.

(6) Server Disk Anomaly

Many application procedures will save some middle-results in the disk when they running, in the end they need save the end-result in the disk; operating system can also produce many temporary documents, all above situations may make the useable space of the disks being much smaller. With the useable space of disks decreasing, it will take more and more time for head seeking. Therefore, the system will run at very slow speed. Generally speaking, system's performance became bad, if disk's utilization is over 90%.A useful performance monitoring tool for tracking disk usage is host.hrStorage.hrStorageTable. The structure of the table [6] is as follows:

HrStorageEntry: = SEQUENCE {
hrStorageIndex "the index of the storage"
hrStorageType "the type of the storage"
hrStorageDescr "a description of the type and instance of the storage"
hrStorageAllocationUnits "the size, in bytes, of the data objects allocated from this pool"
hrStorageSize "the size of the storage"
hrStorageUsed "the amount of the storage represented by this entry that is allocated, in units of hrStorageAllocationUnits"
hrStorageAllocationFailures "the number of request for storage represented by this entry that could not be honored due to not enough storage"
}

We can calculate each disk's utilization using formula (1), and calculate the remainder space of each disk by formula (2).

hrStorageUsed/hrStorageSize*100% (1)

(hrStorageSize–hrStorageUsed)*hrStorageAllocation Units (2)

There are some other related parameters besides the above critical ones, such as description of the system's hardware type, software operating-system, and networking software; the physical location of the network server; the amount of physical memory. We can also monitor the state of running software through the hrSWRun group.

Above all introduced the defined-server's parameters, as the data-colleting will take up network bandwidth, we propose a data-collecting strategy in order to improve the efficient use of bandwidth.

We divided the parameters into two groups: one is static parameters, such as description of system and the software etc.; the other is dynamic parameters, such as CPU utilization, and so on.

We design deferent threads for the two categories. One static-parameters collecting thread is designed to acquire static parameters. It will run under the condition that the system is set by people. And a dynamic-parameters collecting thread is designed for the second. We use the multi-threading technology in order to avoid the long acquainting time problem caused by serial operation. Each sub-thread runs to access the relative monitored system. Then the timely collection will be ensured.

IV. DEVELOPMENT OF SYSTEM

A. Architecture of System

The aim of designation is to monitor the main parameters of the network servers initiatively, and then analyzes the parameters. If there is any anomaly of the network servers, it can give an alarm to the manager. The system includes user-interface module, fault-diagnosis module, statistic& display module, database module, data analysis module, and data acquisition module, shown in Fig. 2.

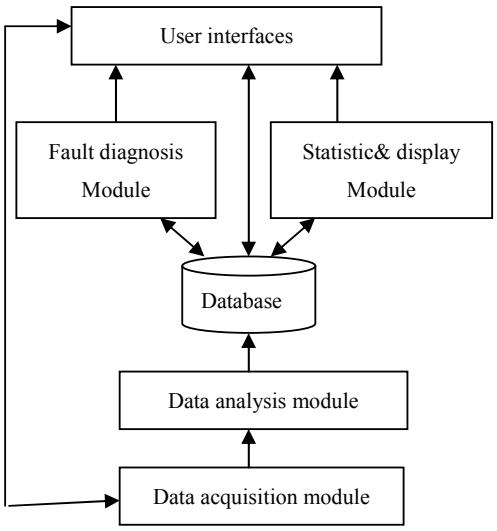

Figure 2. Framework of monitor and control system

(1) Data Acquisition Module

This module requests the list of monitored network servers from the database retrieve the value of MIB objects by sending SNMP Request messages to the monitored server, and accept SNMP Response messages responded by the monitored network server. The requested data has been introduced in section 2.

(2) Data Analysis Module

This module is to deal with the original data from the acquisition, transform the original data into the data form easily to read by users, and then store these data to the database.

(3) Database Module

Database stores the list of network server, answers for reading and writing the database, and provides the uniform database interfaces for other modules. Data are updated in every specified time which can be adjusted to adapt specific requirement.

(4) Fault Diagnosis Module

The fault diagnosis module includes warning processing, fault detecting and fault locating. Warning information has highest rank of privilege which should by processed previously. It can give an alarm (by TRAP, E-mail, SMS, or sound) to the manager, when there is any anomaly. Such as network connectivity alarming; disk, CPU, or memory's threshold anomaly; the running-service processors anomaly, such as whether the http service, for the WWW server, is started, or running normally.

(5) Statistic & Display Module

This module is to process data recorded in database and makes statistics. Then it displays the result in graph form. The users can also see the architectures and server distributions.

B. Implementation of System

The development environment is windows2000 server; which encapsulates the implementation of the SNMP protocol, and provides a set of interfaces for developing network management programs based on SNMP, called WinSNMP API [7]. WinSNMP encapsulates the each part of the SNMP protocol in function form (incarnated wsnmp32.dll, wsnmp32.lib, and winsnmp.h in the development environment of Visual C++).We use the SQL sever 2000 as our database and choose VC++ as the programming language to develop the system.

The SNMP agent must be implemented at the monitored server. In fact, many kinds of operating systems have realized the SNMP agent. The operating systems of network servers mostly are windows 2003, UNIX, windows 2000. The Windows system has realized the MIB- Ⅱ and hr-MIB, can provide sufficient management information; but for the UNIX system, but the MIB they supported can't satisfy the management requirement. So we choose Net-SNMP software as the agent. It can provide the whole SNMP service, and support the SNMPv1, SNMPv2, and SNMPv3 protocols.

Installing and configuring the agent, and then starting them, they will collect the monitored server's parameters.

Fig 3 shows the system running result. It displays the description of software installed in one monitored server.

名称索引		名称	安装ID	安装类型
1	1	Microsoft SQL Server 2000	0.0	4
2	2	Windows Server 2003 Service Pack 1	0.0	4
3	3	WinRAR 压缩文件管理器	0.0	4
4	4	J2SE Runtime Environment 5.0 Update 11	0.0	4
5	5	J2SE Development Kit 5.0 Update 11	0.0	4
6	6	Java 2 SDK, SE v1.4.2_03	0.0	4
7	7	Java 2 Runtime Environment, SE v1.4.2_03	0.0	4
8	8	Intel(R) Graphics Media Accelerator Driver	0.0	4
9	9	VMware Workstation	0.0	4
10	10	REALTEK GbE & FE Ethernet PCI NIC Driver	0.0	4
11	11	Realtek High Definition Audio Driver	0.0	4

Figure 3. Running result of monitor and control system

V. CONCLUSIONS

Considering the soul of the network, network servers, we design this system. This system can monitor the movement of network servers comprehensively by the agent. The design suits the network management actual demand, and has a higher practical significance. It is possible to develop a function formidable intelligence management system by integrating the server monitor system. Therefore we can monitor the whole network including the network servers, network devices and network link, in order to guaranty that the network can provide normal services.

REFERNCES

[1] J.Case et al.,"The Simple Network Management Protocol (SNMP)", RFC 1157, May 1990.Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] K. McCloghrie,M T Rose. Management information base of network management of TCP/IP-based Internets, MIB-Ⅱ RFC 1213,1991.

[3] Cen Xiandao,An Changqing. Network Management Protocol and Development [M].Beijing: Tsinghua University Press,1998.

[4] M. Rose and K. McCloghrie, Structure and identification of management information for TCP/IP-based Internets, RFC 1155, May 1990.

[5] RFC 2790-2000,Host Resources MIB[S].

[6] P. Grillo and S. Waldbusser (editors), Host Resources MIB, RFC 1514,September 1993.

[7] Bob Natale. Windows SNMP Manager API Specification (Version 1.1) [M].New Jersery.Prentice Hall,1994.

[8] Sun Dewen,Tian Xiaopeng. Acess Implementation of MIB Based on SNMP Network Management [J].Journal of Shanghai JiaotongUniversity,1996,30(6):59-64.