2013 Third International Conference on Instrumentation, Measurement, Computer, Communication and Control

Research of Network Monitoring Based on SNMP

Yongqi Han
Jilin Agricultural University
College of Information Technology
Changchun 130118,China
jlauhyq@aliyun.com

Yun Zhang
Changchun University of Science and Technology
College of Information Engineering
Changchun 130600,China
z9y29@aliyun.com

Taihao Li
Jilin Agricultural University
Informatization Teaching and Management Center
Changchun 130118,China
lth@jlau.edu.cn

Liying Cao
Jilin Agricultural University
College of Information Technology
Changchun 130118,China
caoliying99@163.com

Abstract—**Network monitoring system is a collection about consisting of a set of tools for network monitoring and control, a combination of organic is used to manage networks and ensure the normal operation of the network software and hardware.It is not only to improve the efficiency of network management, but also continue to monitor the network, creating blogs, research and analysis of network status.**

Keywords-network monitoring;fault monitoring;performance monitoring

I. INTRODUCTION

With the development of computer networks, network has grown into a multi-network operating system, multi-topology, multi-vendor equipment mixed complex networks. So the daily management of maintenance work becomes increasingly heavy, but also more complex. Network monitoring system is to meet the needs of network users and network management development, it is no longer a passive network management. In this paper, network devices uses SNMP on the network key data indicators to monitor, analyze the current network conditions, so that managers real-time control network operations, detect or prevent network problems that may arise.

SNMP is based on the manager/agent model consisting of an SNMP manager, an SNMP agent, a database of management information, managed SNMP devices and the network protocol. The SNMP manager provides the interface between the human network manager and the management system. The SNMP agent provides the interface between the manager and the physical devices being managed[1]. Figure 1. is SNMP-based network management model details.

SNMP-based network model characteristics, this thesis researches network monitoring system consists of three major design:

1 Accessing to the monitored information: how to define monitoring information, and how to pass them to the network administrator.

2 Design of monitoring mechanisms: What is the best way for obtaining the information from the managed resources.

3 The application of the monitoring information: how to take full advantage of the various management functions to be monitored.

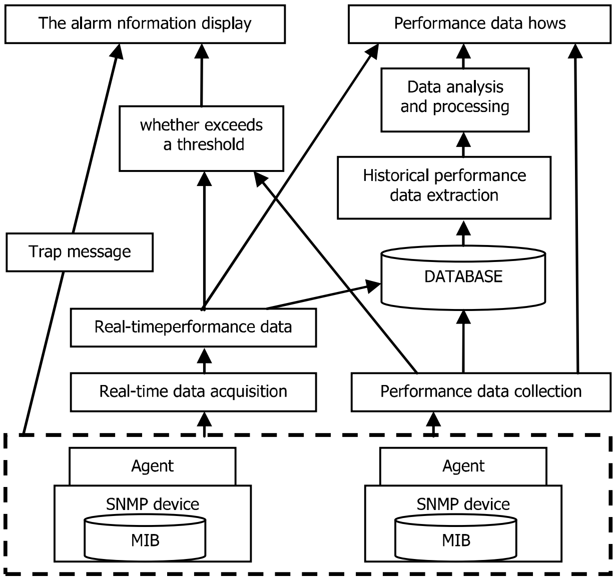

The alarm nformation display
Performance data hows
Data analysis and processing
whether exceeds a threshold
Historical performance data extraction
Trap message
DATABASE
Real-timeperformance data
Real-time data acquisition
Performance data collection
Agent
SNMP device
MIB
Agent
SNMP device
MIB

Figure1. SNMP-based network management model

II. SELECTING THE INFORMATION MONITORED

The management of a network to the network performance-measure,only in the performance of a system that can monitor the situation tomanage it. Managers face how to choose the right performance indicators, selection of network data indicators related to a variety of factors, but the most commonly used indicator of most network monitoring system is basically the same, such as throughput, utilization, packet loss rate.

A. Throughput capacity

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the A4 paper size. If you are using US letter-sized paper, please close this file and download the file for "MSW_USltr_format".

978-0-7695-5122-7/13 $26.00 © 2013 IEEE
DOI 10.1109/IMCCC.2013.94

Throughput refers to the rate of data sent over the network,that is an application-oriented indicators, usually represented as bits per second (bps), the number of bytes per second (Bps) or the number of packets per second (pps). The formula is:

Throughout = bytes/time

(The number of bytes transmitted / a interval time)

B. Utilization rate

The utilization rate is the use of network resources to the frequency of the dynamic parameters, is more refined than the throughput indicator. It is used to search for potential network bottlenecks and congestion area, also can know which resources have not been fully utilized. Through the analysis of network management may find that resource is over used or utilization rate is not high, adjust the network planning,load balancing, the effective use of resources. Refering the result managers can adjust the network planning, load balancing, the effective use of resources.

- The interface utilization

Interface utilization is the main indicator of network utilization. The operational status of the interface can be achieved by monitoring the utilization rate, utilization rate can be expressed in percentage relative to theinterface interface bandwidth as the number of bytes specified interface flowing. Calculations are performed using the collection of interfaces groupvariables, the formula is as follows:

$$IfUtilizationRate = \frac{(\Delta ifInOctets + \Delta ifOutOctets) \times 8 \times 100}{(\Delta t) \times ifSpeed}$$

Where: Δt is time interval, ΔifInOctets is the number of the input bytecollection,ΔifOutOctets is the number of output byte collection,ifSpeed is the transmission rate of interface.

Similarly, you can use the interface table, where the number of input bytes and the number of output bytes are calculated input utilization and output utilization.

- The utilization of cpu and memory

The CPU Utilization reflect equipment busy, and play an important role in the discovery of network congestion and balancing network load. However, The CPU Utilization is not defined in the public MIB, mostly vendor-defined private variables, Cicso defines CiccoProcessMIB (ID :1.3.6.1.4.1.9.9. 109) and ciscoMemoryPoolMIB(ID : 1.3.6.1.4.1.9.9.48) to manage the CPU and memory.

C. Packet Loss Rate

Packet loss sometimes adverse signs of abnormal network,so packet loss rate is another important indicator of network monitoring. Usually less than 15% above this value network is usually not available. Acquisition interfaces group variable calculate,the formula is as follows:

$$DropRate = \frac{(ifOutDiscard2 - ifOutDiscard1 + ifInDiscard2 - ifInDiscard1)}{(indrop + outdrop)}$$

$$Indrop = ifInUcastPkts2 + inInNUcastPkts2 - ifInUcastPkts1 - ifInNUcastPkts1$$

$$Outdrop = ifOutUcastPkts2 + inOutNUcastPkts2 - ifOutUcastPkts1 - ifOutNUcastPkts1$$

Among them,DropRate is the packet drop rate; IfInDiscard2 and ifInDiscard1 show two different times the value of the ifInDiscard variable; IfInDiscard said the message input direction discard number; ifInUcastPkts said the number of packets sent to the upper layer protocol subnet unicast communication; ifOutUcastPkts said upper layer protocol packet number of requests sent to the address of the subnet unicast communication; IfOutNUcastPkts said the upper layer protocol and message request to non - unicast address subnet number[2].

III. Monitoring mechanisms

Collect information from the network equipment can use two techniques: roll poling and event report.

Roll poling is a process requests and responses between the network manager and agent. Managers can query command and sent its agents within the scope of authorization and request of all kinds of information value, the agent will be the information in the MIB as a response. For real-time monitoring, managers must constantly go to polling agents and obtain data to evaluate the health of the network.

Event report is initiated by the agent, managers in a monitoring role wait to receive the information. Agent may be regular or pre-set cycle, is also possible when major events or abnormal events take the initiative to generate reports, which are very effective for real-time monitoring. For the state or value of relatively small changes in the monitored object can be more efficient than roll polling[3].

Roll polling and Event report is a network monitoring system adopted by the two kinds of the most effective methods, however, for different management systems, both have different emphases. Telecommunication management system uses more incident reports, and SNMP management does not depend on event report. The management of OSI system are more likely to find a balance point between the two ways, making the selection can be based on the following:

- Network data traffic generated by each method
- Reliability of critical case
- The required delay
- Supporting the network monitoring application

IV. Application of the monitoring information

Combined with the current network environment in our school, the analysis and design a network equipment monitoring system based on SNMP protocol on application testing, its basic features include:

1 The managed device to scan

By entering the managed device IP address and community name for the device connect status scanning.

2 Information data collection

Through SNMP data collection was carried out on the equipment (mainly equipment status, the port data traffic, utilization, CPU, memory utilization, etc parameters), and data storage.

3 The monitoring data processing

The collected data into a data file for system monitoring module is nalyzed, at the same time, after analyzing the result or fault information stored in the database.

4 Alarm Information Management

Read SMS alarm information or queries, while the alarms and logs sent information to search.

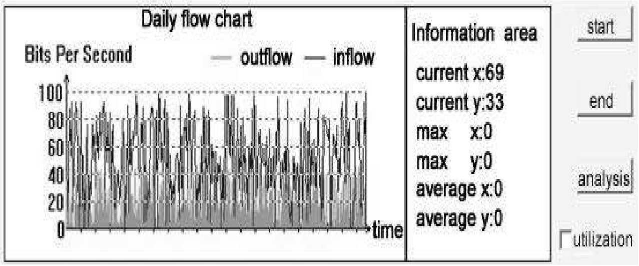
5 GSM SMS Operations Management

6 System Management

A. *Traffic data real-time display*

Curve, according to the real-time acquisition of data can be converted to realize the dynamic display function. A time point corresponding to the display data with inflow and outflow data, but also save the time of inflow and outflow of utilization data, the data structure stored in a variable of the type, all data to be displayed is stored in the structure type array[4].

This window has two states: the first is real-time data display state; the second data analysis states. The default is the first state. Generating object, a parameter passed is to display the horizontal axis and indicates the number of status data. with the passage of time, the previous data is discarded, only the display and hold the latest maximum horizontal display that data, while taking advantage of the aliquots axis 5, if the display data maximum is 1000, then each scale is 200, when more than the maximum, for example 1500, the maximum value is adjusted to 2000, each scale is 400. But when you click the button to switch to Data Analysis Data Analysis shaped body, the control reads the saved data collection files, with the location of the mouse movement data show the maximum, minimum, and other data. Interface as shown in Figure 2:



Information area
current x:69
current y:33
max x:0
max y:0
average x:0
average y:0

Figure2. Traffic monitoring of interface GigabitEthernet5/2

B. *CPU and memory utilization monitoring*

CPU and memory utilization of most devices in the MIB of the public is not in standard definition, as shown in figure 3 Cicso defines CiccoProcessMIB (identified as: 1.3.6.1.4. 1.9.9.109) and ciscoMemoryPoolMIB (identified as: 1.3.6.1.4 .1.9.9.48) to manage the CPU and memory.

CPU utilization and system memory available about network equipment reflect the degree of equipment in a certain period of busy time, that the discovery of network congestion and network load balance play a very important role. To implement the program network devices to monitor CPU and memory utilization, you must first know the device's manufacturer and model of the device, and then check the corresponding OID identifier for data acquisition and processing, and then set the threshold for monitoring. The figure 4 is to monitor the campus network the state of cpu and memory[5] .

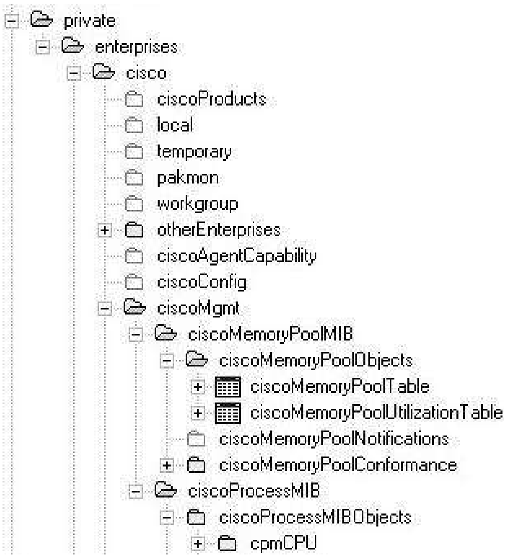
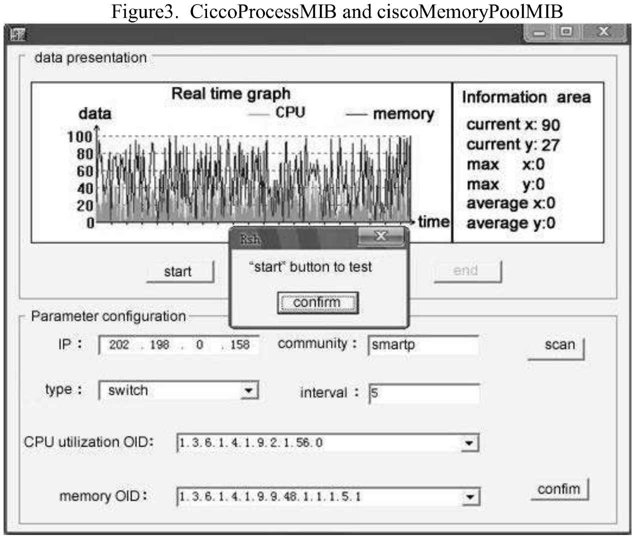


Figure3. CiccoProcessMIB and ciscoMemoryPoolMIB



Information area
current x: 90
current y: 27
max x:0
max y:0
average x:0
average y:0

"start" button to test

IP : 202 . 198 . 0 . 158

community : smartp

type : switch

interval : 5

CPU utilization OID: 1. 3. 6. 1. 4. 1. 9. 2. 1. 56. 0

memory OID : 1. 3. 6. 1. 4. 1. 9. 9. 48. 1. 1. 1. 5. 1

Figure 4. The campus network the state monitoring of cpu and memory

V. FAULT MONITORINGS

Fault monitoring goal is as far as possible, the timely discovery and find the fault reason to take measures to repair or warning trouble before the fault occurs. In a complex network environment, location and fault diagnosis is difficult. FOR failure observations, the following three related issues:

1 The fault can not be observed: some faults cannot be observed in the local.

2 Part of the observed fault: Fault may be able to observed, but only by observation might, you can not determine the cause of the problem.

3 Observation of uncertainty: that is able to fault careful observation, but the observation process may also be uncertainty even inconsistencies.

Observed failure, it is necessary to carry out the fault isolation investigation and positioning repaired. However, several problems still may be in this process:

1 Too many observations and potential causes.

2 The conflict between the diagnosis process and local recovery process .

3 The lack of automated testing tools.

Therefore, fault monitoring should have the following features:

1 Must be able to detect and report the failure. Management Agent can maintain the major event log management ,and system can use these logs. The system by roll polling rely on these logs. The monitor agent can take the initiative to report to the management station, but in order to avoid network overload, should be a reasonable limit fault report.

2 Best able to fault warning. This need to set the threshold value, when the monitored variables exceeds the threshold value reporting. If the threshold is set low, the network administrators can get timely notice and take measures to avoid more serious problems.

3 Fault isolation diagnostics. The management system should include test function such as some connectivity tests, integrity tests, diagnostic tests.

4 An effective user interface. Monitoring system with the close collaboration of the managers, the network can better achieve fault isolation, diagnostics and repair.

VI. CONCLUSIONS

After a pair of information collection methods, data, analysisand processing, alarms, etc. carried out a detailed study and analysis,system has implemented network devices MIB information collection, processing, monitoring, alarm and other basic functions. But in the actual application process has many limitations found in the SNMP protocol. For example, polling performance limitations, the trap can not confirmatory. It is not suitable for managing large networks and large amounts of data, and that the value of the basic SNMP standard authentication feature that makes it more suitable for monitoring rather than control. SNMP network management in the position,however, is still unable to shake by any other means and methods[6].

ACKNOWLEDGMENT

This work was funded by the Youth Foundation of Jilin Agricultural University under Grant No. 201326; The research and application of facilities for the safety of vegetables produ ction technology based on Internet of Things(2011-Z20)

REFERENCES

[1] Walter Goralski,"Simple Network Management Protocol",The Illustrated Network, 2009,Pages 609-630.

[2] Al Kovalick,"Systems Management and Monitoring ,"Video Systems in an IT Environment (Second Edition), 2009, Pages 345-372.

[3] Vijay K. Verma, Ramesh C. Joshi, Bin Xie."Agrawal Combating the bloated state problem in mobile agents based network monitoring applications",Computer Networks, Volume 52, Issue 17, 8 December 2008, Pages 3218-3228.

[4] Demetris Hoplaros, Zahir Tari, Ibrahim Khalil,"Data summarization for network traffic monitoring",Journal of Network and Computer Applications, In Press, Corrected Proof, Available online 27 April 2013.

[5] Ousmane Diallo, Joel J.P.C. Rodrigues, Mbaye Sene, "Real-time data management on wireless sensor networks: A survey",,Journal of Network and Computer Applications, Volume 35, Issue 3, May 2012, Pages 1013-1021.

[6] Kwang Sik Shin, Jin Ha Jung, Jin Young Cheon, Sang Bang Choi, "Real-time network monitoring scheme based on SNMP for dynamic information",Journal of Network and Computer Applications, Volume 30, Issue 1, January 2007, Pages 331-353.