Research on the Data Acquisition Resource Management Based on SNMP

Jing Wang

Computer Science and Technology Department, Zhuhai College of Jilin University, Zhuhai, Guangdong, 519041, China

312900384@qq.com

Keywords: Network management; Data acquisition; SNMP; Resource management

Abstract. With the increasing size of computer network, network information is changing. However, the devices from different vendors and the difference of equipment management means make network management more complex. So it is a great challenge to effectively maintain network and ensure the quality of network operation. The effective monitoring of the state of each part of the network is an important means to ensure the normal work of the network. This paper expounds how to effectively monitor the network and collect, process and analyze the SNMP data of the network accurately in real time. In this paper, a resource management architecture is proposed to make the overall performance of the network more reasonable by managing network resources.

Introduction

The rapid development of modern network system and information security technology has put forward higher requirements for the new generation of network equipment, and the network equipment is becoming more and more miniaturized and specialized. In view of the characteristics of many layers of network management, many kinds of devices and complex network structure, it is inevitable to set up and access managed network objects when managing the network. In the long-term network operation and management practice, a network management industrial standard network management protocol SNMP(Simple Network Management Protocol) that meets the requirements mentioned above is formed. This protocol standard has been widely supported by the industry circles, and many network management systems based on SNMP are introduced. The goal is to ensure that the network management information is transferred between the management entities supporting SNMP protocol and the managed devices arbitrarily, which is convenient for network management system to retrieve information from any node on the network and obtain network index parameters[1].

Based on the information characteristics of simple network management protocol(SNMP) and management information base(MIB), this paper puts forward the general framework of SNMP data acquisition system, and introduces the design idea and implementation mode of data acquisition system. Through the analysis of the data acquisition technology in the network management and the comparison of the collection methods, the concrete solution of the data acquisition based on SNMP is given. It effectively improves the speed of network information processing, and has a certain theoretical and practical value.

Analysis of Data Acquisition System Based on SNMP

Main Design Ideas of SNMP. SNMP is an application layer protocol in the TCP/IP protocol family, using the Client/Server model, that is the Manager/Agent model. The management and maintenance of the network are accomplished through the interaction between the management station and the agent. The basic functions of the SNMP protocol are to monitor network performance, detect and analyze network errors, and configure network devices. The protocol is simple. The system architecture of SNMP data acquisition is designed around the following four concepts and goals.

The first point is to keep the cost of managing agent software as low as possible.

The second point is to maximally maintain the function of remote management in order to make full use of the network resources of Internet.

The third point is that the architecture must be able to extend the room for future needs.

The fourth point is to maintain the independence of SNMP, not depending on the specific computer, gateway, and network transport protocol[2].

Functional Requirements of SNMP Data Acquisition System. Combined with the actual needs of the subject, the main functions of data acquisition system include: collection configuration, collection monitoring, rule configuration, collection and testing tools, collection log, system management and help. The functional requirements of the data acquisition system based on SNMP are divided into two parts: the network management work module and the managed device module. The function requirements of the network management work module are shown in Table 1. The functional requirements of the managed device module are shown in Table 2.

Table 1   Function requirement table of network management work module

Name	Network management work module			
Description	Request-response mode			
Trigger	The management process sends a request, the agent process replies and responds			
Operation sequence	1 Run the module 2 Display control interface 3 Select the type of operation by the user: collect data 4 Receive the related parameters and form a character stream 5 Wake up a remote agent, wait for a network connection 6 Put in a specified space to receive 7 Parse and print out the public part			
Input	Parameter name	Parameter type	Data length	Parameter description
	IP address	Character		IpAddress 4 byte length OCTER STRING. The network order is used to express the IP address. Each byte represents a field of the IP address
	Time count	Date		Time on equipment
	The number of retries	Character		
	Timeout period	Date		
	Community	Character		Attribute information
	UDP and TCP port number	Character	65535	
Output	Parameter name	Parameter type	Data length	Parameter description
	Enterprise Id	Character		Enterprise Id number
	IP address	Character		
	Physical address	Character		
	Time count	Date		The time of the original execution
	Value pairs	Character		Processing and searching for relevant instructions, detailed description of alarm / events

Table 2　The function requirements table of the managed device module

Name	The managed device module			
Description	The agent process notifies the management process			
Trigger	The agent process initiatively sends a message to inform the management process that something is happening			
Operation sequence	1 Run the module 2 Display control interface 3 Select the type of operation by the user: collect data 4 Receive the related parameters and form a character stream 5 The agent process initiatively sends a message to inform the management process 6 Put parameters in a specified space to receive 7 Parse and print out the public part			
Input	Parameter name	Parameter type	Data length	Parameter description
	IP address	Character		IpAddress 4 byte length OCTER STRING. The network order is used to express the IP address. Each byte represents a field of the IP address
	Time count	Date		Time on equipment
	The number of retries	Character		
	Timeout period	Date		
	UDP and TCP port number	Character	65535	
	community	Character		Attribute information
Output	Parameter name	Parameter type	Data length	Parameter description
	Enterprise Id	Character		Enterprise Id number
	IP address	Character		
	Physical address	Character		
	Time count	Date		The time of the original execution
	Value pairs	Character		Processing and searching for relevant instructions, detailed description of alarm / events

Management System Architecture Based on SNMP. The SNMP based management system architecture is shown in Fig.1. Network management applications in network management workstations are usually an independent device and can be implemented with a shared system. The manager, as the network administrator, is the entity that implements the network management and is the core of the whole network system. It can accomplish all functions of network management, such as monitoring network performance, eliminating network failures, and extracting information and data from the MIB of all managed devices on the network. It is generally located on a host node in the network.
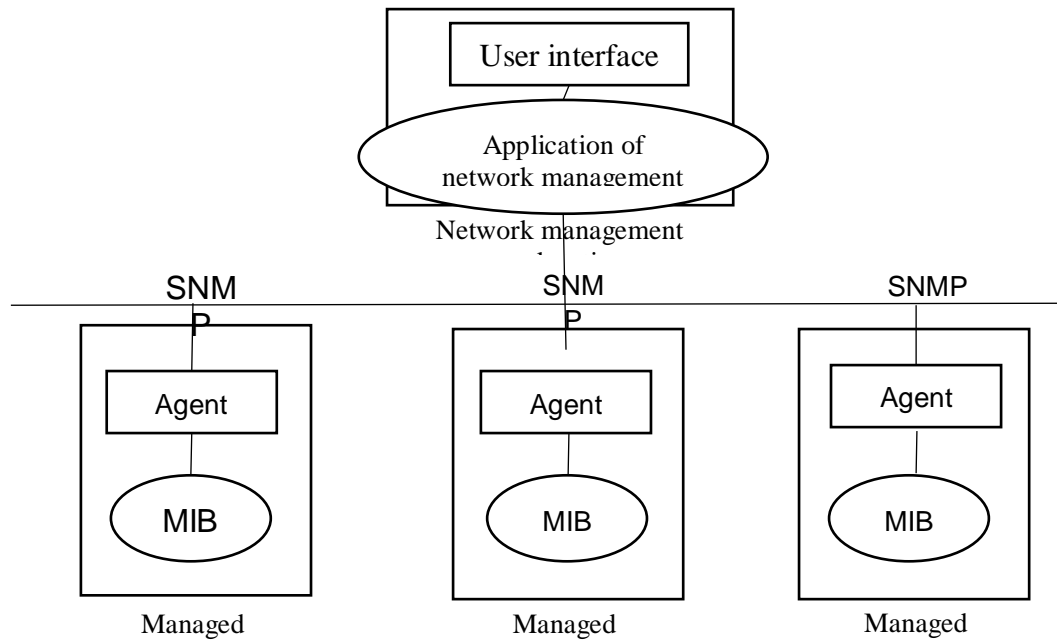
Figure 1   SNMP architecture

Another important element in the SNMP architecture is the agent. In a managed device, the host, bridge, router, and concentrator all can work as agents. The agent responds to requests from the management workstation and randomly reports some accidents for the management workstation.

The resources in the network are expressed in the form of objects, and the collection of objects is the management information base(MIB). The management workstation implements the monitoring function by getting the value of the MIB object and implements the action on the management agent by modifying the value of the special variable. MIB is stored in the managed device, and it is a dynamically refreshed database. It includes the configuration information of the device, the statistical information of data communication, the performance data of the port, the security information and the private information of the device, and the information forms the data source of the network management system.

The communication between the management workstation and the agent of the managed device is carried out through the SNMP protocol. SNMP describes the data communication mechanism between the management workstation and managed agent, defines the type and format of the SNMP protocol data unit PDU (Protocol Data Unit), defines the data message format between the management workstation and the managed agent, determines the main functions of the network management system and defines the format of the datagram of the management information base (MIB).

Implementation Mechanism of SNMP Data Acquisition

The Composition of Data Acquisition System Based on SNMP. The program architecture of the data acquisition system based on the SNMP is shown in Fig.2. Firstly, on the custom interface of the interface layer, the system modeler configures the class, object, and port, and then they send the configuration results to the database in data layer through the middle layer. When the user selects the "view real-time information" on the object of the interface layer, the corresponding real-time acquisition interface will be transferred. Through the middleware, the program gets the corresponding data in the data layer table based on the object ID and the class ID, and determines whether the port exists, and then returns the data obtained above to the corresponding program of the interface layer. The corresponding program of the interface layer will pass the data obtained in the last step to the acquisition program of the acquisition layer. After processing the data, the acquisition program collects the data in the corresponding equipment according to the parameters

and obtains the collected data. The collection program updates the related tables through the middleware. If this class contains the port class, the corresponding port class relational table should be updated and the port data collected should be also updated to the corresponding data table.

The overall solution of data acquisition based on SNMP makes remote important network devices more convenient for maintenance and monitoring under simple communication links.
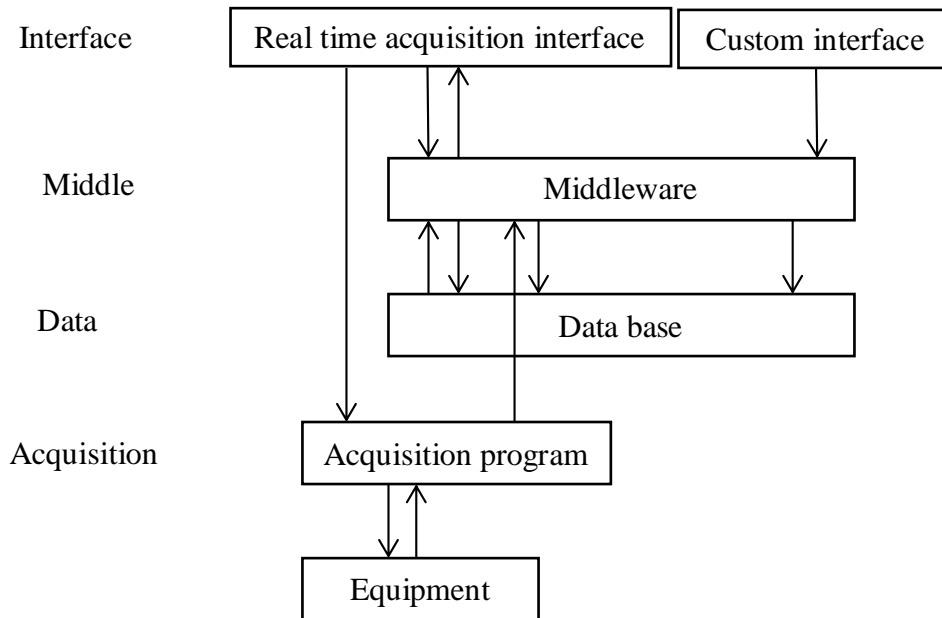

Figure 2.   The program architecture diagram of the data acquisition system based on SNMP

Data Acquisition Specific Process. The communication between the network management workstation and the agent in the SNMP is realized by the message exchange. The commands are sent from one end of the network management workstation to start the construction of SNMP datagram. The software system of the network management workstation will create a SNMP message and fill in the appropriate message heading in order to transmit the message to the destination agent process through the Internet. In the message, we need to specify the group name, version number and request ID, and insert the variable bound list into the message, and then transmit the SNMP message to the UDP transport layer[3]. When the message is sent out, the network management workstation must remember the Request ID in the request so as to match the response ID received later. The data acquisition process is shown in Fig.3.

When the initialization is completed, the agent process is waiting to receive the SNMP message on the UDP port 161 of the network device. When the agent process receives a message successfully, the syntax analyzer is invoked to decode the ASN.1 format. If the format of the message is not correct, the message will be lost, and no processing will be done, and then the agent process will return directly to the waiting state. If the format is correct, the agent process will start to verify the version number. After these two checks, the agent process calls the authentication function to verify the message. If the authentication fails, the agent process will lose the message and send out the authentication failure trap message. If the authentication is passed, the agent process will interpret the message and save the transmission information needed for the response message[4].

When the agent process decodes the message in the ASN.1 format, it can construct a message for the response. Any error that is generated after this will not discard the received message, but points out the reason for the failure of the operation in the response message.

The decoding function module checks all the fields in the message to confirm whether the order of the label, length, and value field is correct. If the format is valid, the command is executed, and the module operates the variables in the variable binding list. The agent process program determines

whether the variable instance exists, whether the network management station's request has access rights, and how to access the variables to be manipulated in the request. After the agent process constructs the Get Response-PDU, the message is encoded in the ASN.1 format with the basic encoding rule BER, and then the message is delivered to the UDP transport service. The agent process enters a circular wait state. All variables that the agent process is used to record the operation process are appropriately incremented so that the network management station will be checked.
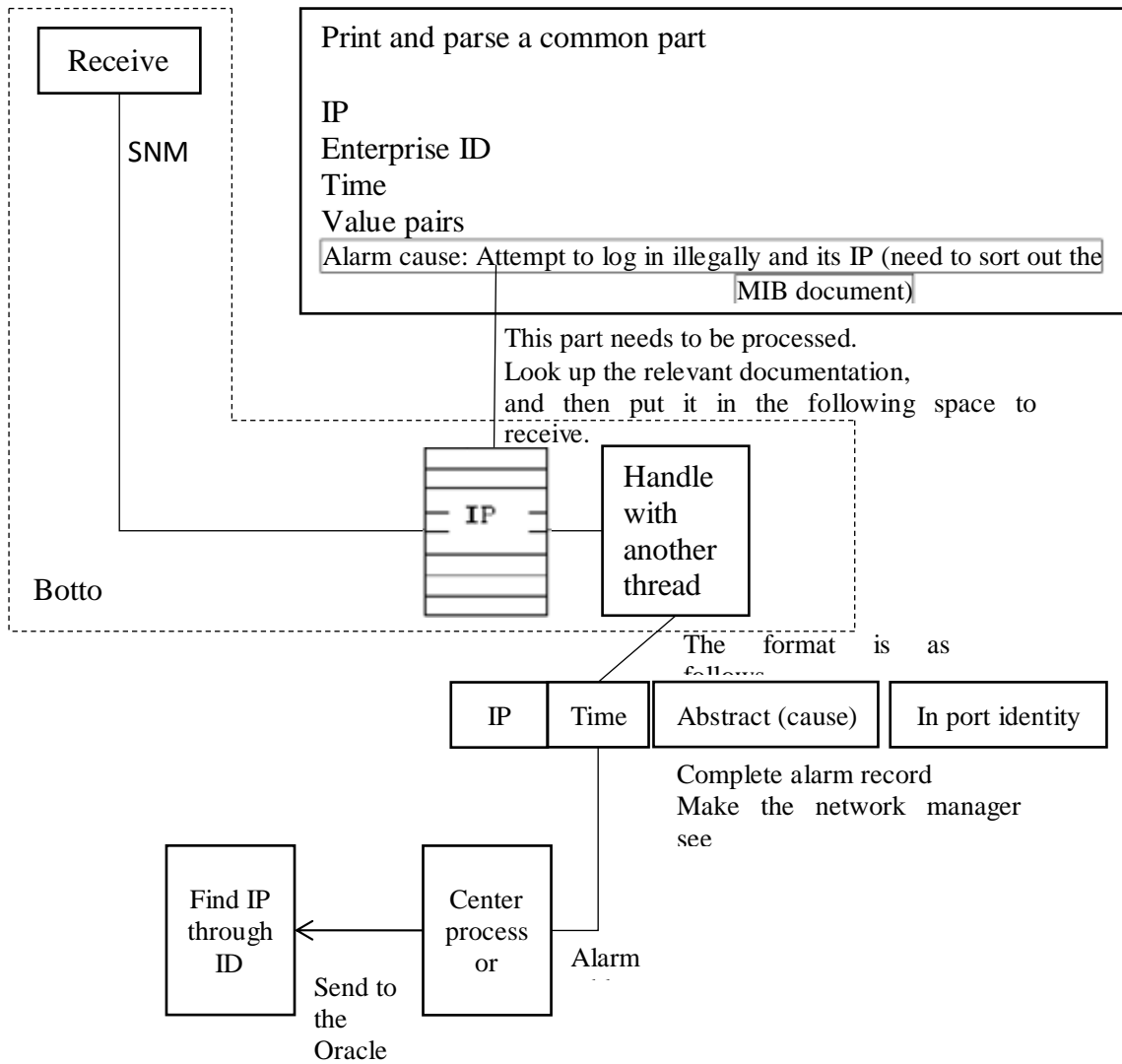

Figure 3   The diagram of the data acquisition process based on SNMP

Characteristics of Data Acquisition System Based on SNMP. SNMP is a network management protocol based on TCP/IP, and can also be extended to other types of network devices. Its monitoring and control activities are independent of TCP/IP. SNMP requires only TCP/IP to provide non-connected datagram transmission services. The data acquisition system based on SNMP is specially designed for the characteristics of the computer application of the telecommunication network. Based on the control standards in the field of telecommunications, the maximum modular and extensible capabilities are provided by simply inserting the corresponding templates and corresponding software modules. The open Linux operating system should be run, and the open and extensible running development environment of the system is provided[5].

Research on the Security of SNMP Collection Resources

The Security Mechanism of SNMP. The basis of failure and performance management is to collect data from various devices in the network. The data acquisition function is completed through the SNMP protocol, and then the mass data collected is processed. Network security testing is usually a tool for network security analysis. Its function is to scan and analyze network system with practical methods, check the weakness and loopholes in the reporting system, and suggest remedial measures and security strategies to enhance the network security[6].

The security of information resources is mainly embodied in the safety and protection of information resources. To ensure the security of information resources, from the content, it guarantees the confidentiality, integrity, reliability and availability of data. From the time and space, it is necessary to ensure the safety and reliability of information collection, storage, transmission and reception.

Implementation of Security Mechanism. Basic data networks use fixed or semi fixed connections to achieve point-to-point data transmission. The management of the data acquisition system mainly includes the user management, the authority management, the log management and the security authentication, which is mainly used to protect the security of the system and to manage the log of the system[8].

The user management is mainly to maintain the information of the users who use the system.

The authority management is mainly to manage the privileges of the users, which can give different privileges to the users, and also reclaim the privileges that have been given.

The log management mainly records the operation of the data acquisition system, and starts or stops the collection tasks configured by the user. The abnormal situations appearing during the data collection tasks and the handling experiences of the administrators for abnormal situations are recorded in the log system, so that users can have a clear track of the operation of the entire data acquisition system and can draw on the previous successful experience in dealing with similar anomalies[9].

The log entry mainly provides two functions: the manual input and automatic input. The user can record the running status of the system through this function, in order to check later[10]. Log queries provide users with the ability to view logs, and users can browse the logs in the system by setting up various query conditions. Log collation provides the user with the function of organizing the log, retaining the important system running information and successful exception handling cases.

Conclusions

This paper analyzes the characteristics of SNMP, further analyzes the network status, helps network planning, and achieves optimal network performance to ensure the high quality network services. This paper studies the method that improves the security of SNMP data acquisition system, in order to give the way to enhance the security of SNMP. Research shows that these technologies have strong practical significance, and can be used for network management conveniently and effectively, providing a good tool for network administrators to maintain the network. At the same time, the research also has a strong representation, which can be used for the management of the vast majority of telecommunication data network equipment.

Acknowledgements

University(JZ2017JZB305), Key Laboratory of the Symbolic Computing and Knowledge Engineering Ministry of Education.

References

[1] X.Li: Development of Network Management System Based on SNMP Technology[J], Mechanical Engineering & Automation, 2014,4:34-36.(In Chinese)

[2] P.H.Wen: Large Scale Network Running State Data Acquisition System Based on SNMP Protocol[D], Beijing: Beijing University of Posts and Telecommunications, 2013:15-16.(In Chinese)

[3] C.Lin, H.J.Wang and G.W.Chen: Data Acquisition Framework Based on SNMP[J], Computer Systems & Applications, 2016,5:55-59.(In Chinese)

[4] X.Y.Tao and L.Xu: Network Monitoring Data Acquisition Algorithm Based on Local Data Processing[J], Journal of Shenyang Institute of Aeronautical Engineering, 2016,3:84-87.(In Chinese)

[5] Y.J.Li: Research and Application of an Intelligent Data Acquisition Strategy[J], Software Guide, 2016,3:162-164.(In Chinese)

[6] X.G.Li: Improvement of SNMP Security Mechanism[J], Value Engineering, 2014,36:209-210.(In Chinese)

[7] B.Jiang, Z.X.Liu and H.Peng: Research on the Security Sharing Management of Government Information Resources in Guangdong[J], Electronic Product Reliability and Environment Test, 2017,3:55-59.(In Chinese)

[8] X.L.Wan: Design and Implementation of Log Analysis System of Information Management System[D], Jinan: Shandong University,2017,4:43-47.(In Chinese)

[9] F.Y.Yang and H.C.Liu: Research on Multi Platform Oriented Log Remote Acquisition System[J], Computer Technology and Development, 2014,7:149-152+15.(In Chinese)

[10] M.J.Luo and C.Jia: Discussion on Campus Network Log Based on Data Mining[J],Electronic Test, 2017,21:113-114.(In Chinese)