Design of College Network Security Management System Based on SNMP Management Model

Yongxin Cheng

Guangdong Mechanical & Electrical Polytechnic, Guangdong, Guangzhou, 510000

Keywords: SNMP, Network Security, MIB

Abstract: With the development of the application of computer network in teaching and scientific research activities, the problem of network security has become increasingly prominent, which has a direct impact on the application of campus network. By analyzing the current situation of college network security management, this paper focuses on the design of network security management system based on SNMP management model, and elaborates the design of network device topology management module, network equipment operation information collection module, network status monitoring module and network traffic monitoring module, as well as some major system processes.

1. Introduction

With the development of network application, the expansion of network scale and the increase of data storage, the requirement of network security is higher and higher. The school's teaching and scientific research activities all depend on the computer network to carry out, and the problem of network security is gradually emerging. Data loss, system paralysis, virus invasion, network blocking, information transmission interruption and other problems all have an impact on the healthy development of campus network, and also have a great impact on the teaching, management, scientific research and other activities in colleges. Running an effective management and maintenance system of campus network security is the practical need of campus network security management and maintenance personnel.

The network security management system should be able to realize the unified management and centralized monitoring of various devices in the network, as well as the interaction between various security function modules. Such a system can effectively simplify the network security management and improve the manageability, controllability and security management level of the network. As a mainstream general network management protocol, Simple network management protocol (SNMP) can collect relevant management and status information from network devices. The SNMP protocol allows network and device administrators to collect and classify this information in the management information base. Therefore, this paper focuses on the design of network security management system based on SNMP management model, to dynamically monitor the attribute parameters of computer network and regulate its network behavior, so as to ensure the smooth and stable operation of network and application system.

2. Overview of SNMP Management Model

SNMP is an application layer protocol, which can manage the equipment through this protocol network management station. SNMP as the fact standard of computer network management, network management station can read and write the management objects in the agent process through the protocol, which can realize the functions of statistics, configuration and testing network, as well as various error detection and recovery functions.

SNMP management model consists of four parts: manager, agent, communication protocol between manager and agent, and management information base (MIB), as shown in Figure 1.

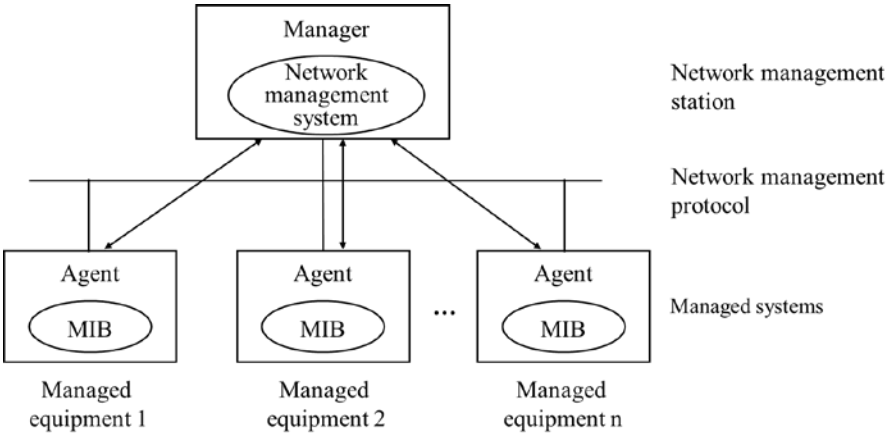

Figure 1. SNMP management model

2.1 Manager

Manager is the core of the whole network management system, which is usually a high-performance workstation with a good graphical interface and is directly operated and controlled by the network administrator. As the interface between the network administrator and the network management system, it is the entity implementing the network management. It resides on the management workstation and can complete all functions of the network management, generally located on a host in the network operation center.

2.2 Anent

Agent is another important element in the network management system, which resides in the managed device. The agent constantly listens for requests or commands from the management station, and once found, it immediately returns the information required by the management station, or performs an action. It can also report important accidents to managers at random.

2.3 MIB

Management information refers to the collection of managed objects. The managed object must maintain a number of control and status information that can be read and written by the management program. These managed objects form a virtual information storage called management information base (MIB). MIB includes the following information: device configuration information, data communication statistics, port performance data, security information and device private information.

2.4 SNMP

SNMP describes the data communication mechanism between the manager and the managed agent. SNMP network management consists of three parts: SNMP itself, management information structure and management information base. SNMP defines the packet format exchanged between the management station and the agent. The exchanged packet contains the object name and its status in this agent, and SNMP is responsible for reading and changing these values.

3. Current Situation of College Network Security Management

Campus network provides convenience for teachers and students, but it also provides the fastest way for virus spreading and Trojan attack. The crazy invasion of Trojan horse and the rampant virus represented by worm directly lead to the paralysis of network or the leakage of user privacy and important data. Colleges are the most active areas of network technology, and also the areas where the network population is relatively concentrated. There are various potential threats hidden in the network. In such a network environment, there is an urgent need for network monitoring and security management. At present, the following problems generally exist in the campus network security.

3.1 Network Administrators Lack Professional Skills

In Colleges, most network administrators have no systematic professional training before working, and lack of network security management experience. So, many network administrators are not competent for their jobs. Many systems do not set system administrator password, or password setting is too simple, or do not install firewall and anti-virus software in the system, etc. In addition, some network administrators even perfunctorily ignore the system failure.

3.2 Weak Awareness of Network Security

The security awareness of most university campus network users is very weak. Its specific performance includes: password setting is too simple; not used to scanning and processing viruses with antivirus software; do not update antivirus software and firewall software in time; not willing to scan and patch system vulnerabilities; do not scan with antivirus software in advance when using removable storage media; run or open files or messages with unknown calendar without any precautions; often intentionally or unintentionally browse pornographic websites or malicious websites, etc. There is no doubt that these operations will bring great hidden danger to network security.

3.3 Weak Defense against External Attacks

Although the functions and security of the operating system are improving day by day, many loopholes still exist. Some vulnerabilities even allow intruders to enhance user rights and execute code remotely. At the same time, desktop applications also have security risks.

In short, the security problems of campus network mainly focuses on the protection of devices in the network, anti-virus and malicious attacks, isolation of internal and external networks and broadcast information, important data backup and recovery, etc.

4. Design of College Network Security Management System Based on SNMP

4.1 Network Device Topology Management Module

Firstly, the system Ping devices in the network according to SNMP configuration parameters. If it is possible to Ping, the device information in the database will be obtained according to the returned device ID information and added to the topology map. If the data not in the database is found, the device information request message is sent to the device, and the information returned by the device is stored in the database, thus realizing the automatic discovery of devices in the network. If it can't Ping, the device has been removed or the device can't work normally. At this time, the system will send an error alarm message to the administrator.

After receiving the request of adding manually by the administrator device, the system judges whether the IP address entered by the administrator is legal. After verification, the system continues to check whether the device already exists in the campus network. If so, then the system will return a response message to the user that failed to create, otherwise, equipment node and equipment resource data will be added to MIB. After adding, send the device creation success message, and display the successfully added devices in the topology map.

In order to facilitate the administrator to manage the network equipment in the campus network, the system will automatically search the network equipment in the campus network every five minutes. Automatic discovery of campus network topology is a basic function of network equipment topology management. The algorithm flow of topology auto discovery is shown in Figure 2.

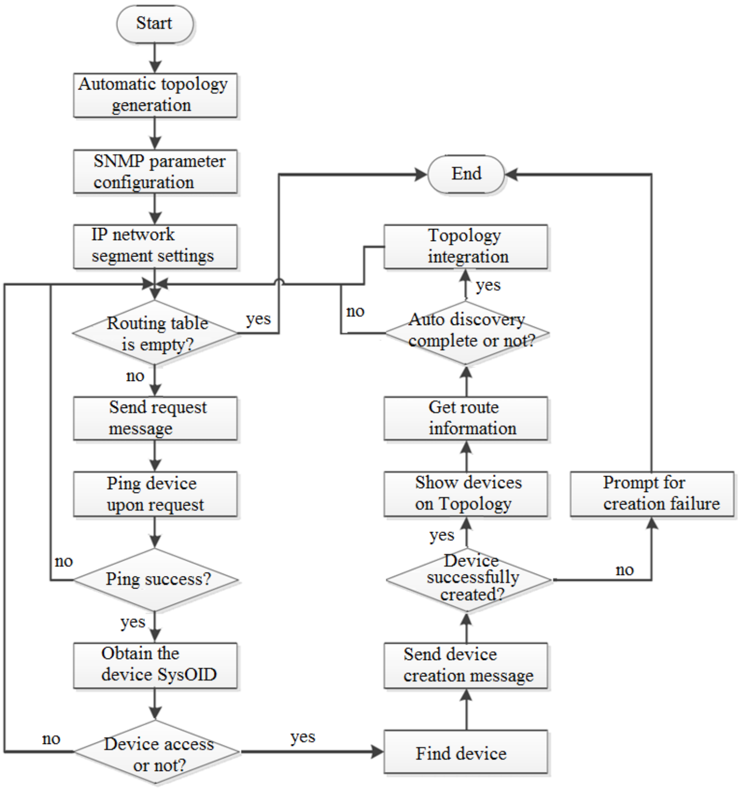

Figure 2. Algorithm flow of topology auto discovery

4.2 Network Equipment Operation Information Collection

The device operation information collecting process using SNMP is shown in Figure 3.

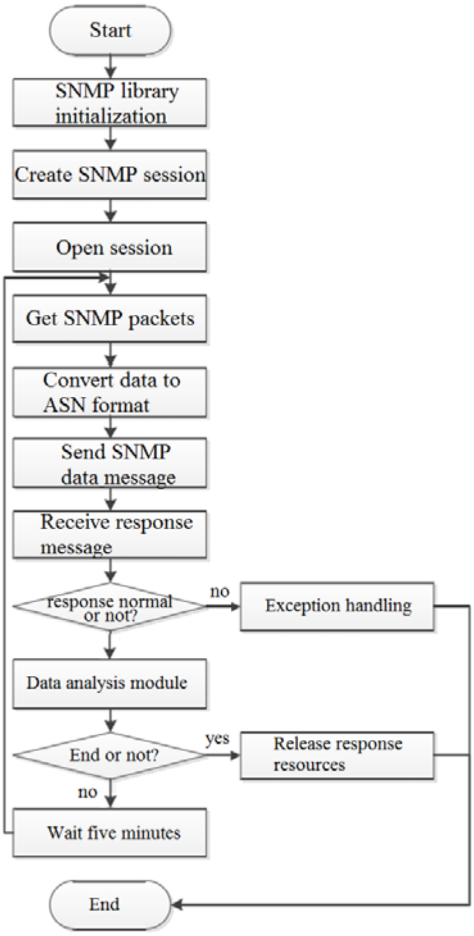

Figure 3. Device operation information collecting process

In the network management system based on SNMP, the steps of data collection are as follows:

1) Get SNMP packets: set community name, request ID, SNMP version number, variable list, message label and other data items required by SNMP message with common data format.

2) Data communication: the controlled site receives the monitoring data request message from the monitoring site using port 161, and transmits the request message to the SNMP message processing module for analysis, and then processes and packs the data generated by the message processing module, and sends it to the monitoring workstation.

3) Receive response: the monitoring station receive the SNMP message information of the controlled station by synchronous or asynchronous mode. In asynchronous mode, after sending a SNMP monitoring data request message, the monitoring station no longer waits for a response from the controlled station, but returns immediately. When the monitoring station receives the SNMP response message returned by the controlled station, it can proceed with further operations.

4.3 Network Status Monitoring Module

Both the two parameters of deviceStatus and deviceAdmiSet have two statuses: up (normal or on) and down (abnormal or off). The Operation parameters of network equipment status is shown in Table 1.

Table 1. Operation parameters of network equipment status

deviceStatus	deviceAdmiSet	Description
up	up	Device is operating normally
down	up	The administrator turned on the device, but the device runs abnormally
down	down	Administrator shut down the device

The system polls the devices that need to be monitored in the campus network at a fixed interval, and first determines whether the administrator has turned on the device normally. If the administrator shuts down the device, the system directly monitors the status of the next device, otherwise, the ping operation is used to determine whether the device is running. And according to the two parameters of deviceStatus and deviceAdmiSet, determine whether the device is operating normally.

4.4 Network Traffic Monitoring Module

Network traffic scanning is essentially monitoring the traffic of data transfer devices such as switches and routers in the network. Network traffic monitoring, on the one hand, allows administrators to understand the current status of network bandwidth allocation, thereby providing a basis for network bandwidth allocation; on the other hand, allows administrators to handle network traffic abnormally in a timely manner. Traffic management allows network administrators to gather information about the traffic on the switch to get a real-time understanding of the current bandwidth distribution in the network, and adjust it automatically or manually according to the specific bandwidth allocation status. The network traffic monitoring process is shown in Figure 4.

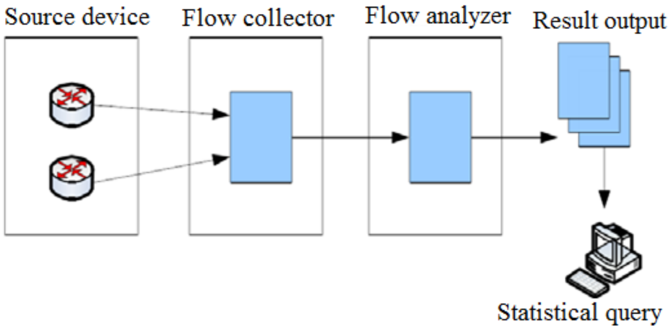

Figure 4. Network traffic monitoring process

5. Conclusion

Based on the campus network in colleges, this paper studies the design of network management system based on the SNMP. Firstly, this paper analyzes the current situation of college network security management, from the perspective of administrators' professional skills, network security awareness and defense against external attacks, and summed up the specific needs of college network security management system. And then, this paper describes the overall design of the network security management system based on SNMP. The system consists of four modules: network device topology management module, network equipment operation information collection module, network status monitoring module and network traffic monitoring module. And this paper focuses on the design of algorithm flow of topology auto discovery, device operation information collecting process and network traffic monitoring process, etc.

References

[1] Zhang W W , Chen S Y . Design and Implementation of SNMP-Based Web Network Management System[J]. Advanced Materials Research, 2011, 341-342:705-709.

[2] Liu BH, Tian YL, Chen DY. Development and Realization of the snmp-based distributed network management system[J]. Software, 2012, 033(006):135-138.

[3] Qing-Qing M A , Hong-Tao Y U , Juan-Juan L . Design and implementation of network management system based on ExtJS[J]. electronic design engineering, 2016, 43(003):119-135.

[4] Deng JA, Jin S. Network User Management System Based on Web and SNMP[J]. Computer and network, 2014, 000(023):58-60.

[5] Han J , Oh S . A study of IoT home network management system using SNMP[J]. International Journal of Control & Automation, 2018, 11(5):163-172.

[6] Shu-Qian F , Ti-Hong L I . Application of snmp communication protocol in communication network management system database[J]. Ship Science and Technology, 2019, 25(007):63-98.