A Design and Implementation of Network Traffic Monitoring System for PC-room Management

Yonghak Ahn, Oksam Chae

Dept. of Computer Engineering, Kyunghee University,
Sochen-ri, Giheung-eup, Yongin-si, Gyeonggi-do 449-701, Republic of Korea
yohan@vision.khu.ac.kr, oschae@khu.ac.kr

Abstract. This study proposes a network traffic monitoring system that will support the operation, management, expansion and design of a network system for its users through an analysis and diagnosis of the network-related equipments and lines in the PC-room. The proposed monitoring system is lightweight for its uses under the wireless environment and applies a web-based technology using JAVA to overcome the limits to managerial space, inconveniences and platform dependency and to raise its applicability to and usability on the real network based on performances, fault analyses and their calculation algorithm. The traffic monitoring system implemented in this study will allow users to effectively fulfill the network management including network diagnoses, fault detection, network configuration and design through the web, as well as to help users with their managements by presenting how to apply a simple network.

1 Introduction

With the surprising developments in Internet, the users on network have rapidly increased so that the traffic on network leads to an explosive increase in many companies, schools and public institutions. Along with the developments in network technologies and the uses of various applications, network traffic includes not only data but also voice, picture, image and multimedia traffic. Those increases in network users and traffic have raised a need for a massive network line and the resulting equipment investments and made network configuration more gigantic and complicated[1-2]. However, such trends escape the managerial scope of a manager, leading to a more need for managements of performance and fault on network. To help the managers with their managements, and accordingly, various management tools have been developed. Since those tools, however, had such fundamental limits as limited management functions, inconveniences, their insufficient expansion into large-scale network and problematic applications of analytic results, the managements of managers had to be restrictively fulfilled[3]. The solution to problems in the existing management technologies and tools is being pursued by applying such new Internet based technologies as web related technologies or JAVA to such fields as managements of networks, systems or applications[4-5]. This approach is called the web based management technology, by which the limits to managerial space and inconveniences can be overcome through their application to the web platform for an increase in effi-

H. Jin et al. (Eds.): NPC 2004, LNCS 3222, pp. 644-652, 2004.

ciency. Web based network management products typically include MRTG (Multi Router Traffic Grapher) that collects management information through SNMP, stores traffic data into GIF and outputs the results in the form of HTML containing GIF files, N-Vision developed through JAVA interface of HP OpenView management platform, IntraSpection using JAVA SNMP-Applet, EnterprisePRO with WAN and LAN management functions, ANACAPA SOFTWARE tracking and providing user response time, and HP NetMetrix/UX Reporter[6-7]. Though an attempt to apply network management technology to the web using the platform has been made, many tools are for WAN management or monitor segments as well as the communications of all nodes within those segment for the management satisfying LAN environment, not including a function to analyze management information. On top of that, they carry problems with them that it is difficult to know the analytic result by providing static information without processing the extracted management information and that they do not provide the cumulative analysis function of long-term traffic statistics and trends through accumulation of management information [8-9].

In this study, RMON MIB, the extension of standard MIB-II together with web based management technology to solve these problems, is applied. It analyzes RMON MIB and MIB-II suitable for the network management, deriving relevant MIB objects and defining significant network performance and fault analyses in the position of the managers. It also attempts to apply JAVA and web related technology to the network management, and implements web based network traffic monitoring system to solve problems with the existing management tools, made it lightweight for its convenient use. Finally, it covers a simple application of network management to help managers optimize their managements.

2 Design and Implementation of Traffic Monitoring System

The whole structure of network traffic monitoring system proposed in this study is shown in Fig.1. The system consists of analysis server that will collect pieces of management information by monitoring network activities of systems managed on network to analyze their results and client system that will provide graphic data to raise an application of analysis result.

While the monitoring system comprises Internet server, intranet server and database existing on the web, HTML documents and JAVA bite codes on the web server are transferred to the client server for its operation. The client is implemented in applet, transferred to the server via new connection as requested by managers and answers the user in the graphic form. At this time is used a message form defined in MATP (Management Application Transfer Protocol) to receive and transfer message [10].

In the case of the real-time analyses subject to each analyzing item of its client, the server answers real-time requests to collect, analyze and show its response to information on a real-time base. In a cumulative analysis, the server polls the data on database to answer the request from the client.

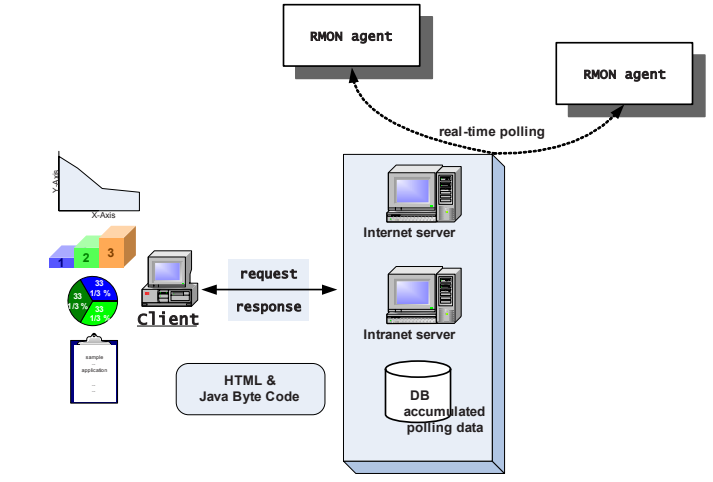

Fig. 1. The whole structure of network traffic monitoring system

2.1 Client System

The whole structure of client system is shown in Fig. 2. Client system is implemented on the web browser of its user client, which comprises such functions as user entry interface for the management request from user, real-time monitoring in which responses to the request are given, information collection requests/suspensions, accumulative analysis monitoring and graphic outputs of traffic results received from an analysis server and shows a simple application of network management.

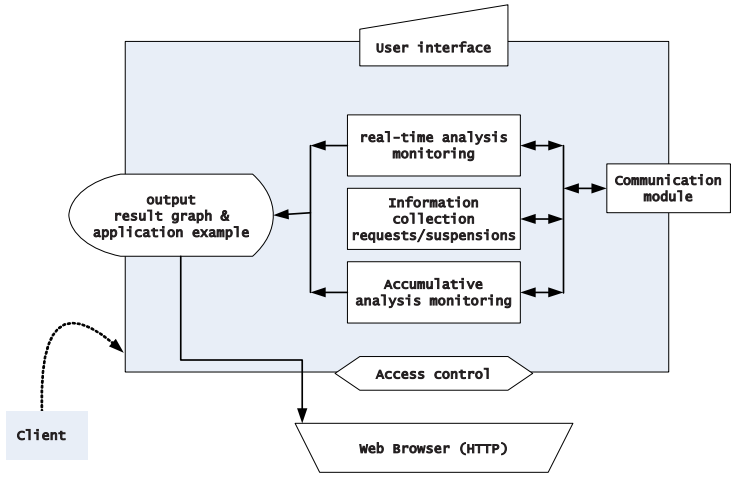

Fig. 2. The whole structure of client system

Function of real-time analysis monitoring. A user must enter the equipment name of the managed system, IP address, port number, community, network speed and polling time to analyze the conditions for the current traffic and fault of LAN. Specifically, such name and IP address are used to show the type of the analyzed equipment in output its results. The function of real-time monitoring is a user interface that receives a request to analyze the condition for the current traffic of LAN from a user, showing the analytic result via the graphic outputs, real-time. Table 1. shows items of analyzing the function of real-time monitoring:

Table 1. Items of analyzing real-time monitoring

type	analysis items	contents
internet	network utilization	rate of utilization of network per unit time
	input/output traffic	amount of input or output traffic
	network error	rate of error packet
	packet loss	rate of input and output error packet
	packet analysis	amount of broadcast packet
intranet	segment utilization	rate of segment utilization in use
	segment collision	rate of segment collision
	segment error	rate of segment error packet

Function of information collection requests/suspensions. It is required for a user to collect traffic statistics on segment and analyze its flows and trends to fulfill such managerial activities as for increasing its network performance & design and diagnosing a fault. In accordance with such collection requests from a user, traffic management information is periodically collected to save it on database up to the point of suspension requests.

Function of accumulative analysis monitoring. The function of accumulative analyses monitoring is required to enter Request ID, IP address and polling time to analyze the condition for traffic and faults during a specified period. Accumulative analyses show the analytic result of traffic data collected in response to a collection request to a user in the form of graph. The analyzing items of accumulative analyses monitoring are the same with that of real-time monitoring as shown in Table 1.

Function of outputting result graph & application example. In this function, the analytic results in response to a real-time monitoring request and accumulative analyses request are output to a user in the form of a graph. Graphic outputs include line graph, bar graph, and pie graph appropriate for the resulting outputs from an analysis of LAN performances & faults. And users make use of a simple application example on the result.

2.2 Analysis Server

Analysis server should go through daemon processes because it must provide services for a specific port to respond to the request from a client system. The server can be largely divided into Internet server and Intranet server.

Internet server. Internet server processes responses to the analysis request from the client, that is, the user interface and the connection setting for such process, message generation, or data processing and transferring by each item for their analyses. It is installed to operate in a place where the web server is installed. In receiving a message for the analysis request, the analysis module transfers it to the processor of analyzing items, acquires management information through the call from a SNMP user implemented in JAVA to poll the relevant management information according to each analyzing item, generates and transfers the analyzed information to the client system on a real-time base.

SNMP Manager. SNMP manager system performs the relevant MIB information polling so that the internet server can derive analysis information with respect to a message for real-time analysis request.

Message Processing Module. Message Processing Module processes the received message according to the mode requested by a user, analyzes the requested message and transfers the relevant processing module. The module interacting with this processing module provides a user with the processed results to the analyzing item requested by the analysis module and the graph generator module in the form of graph.

Analysis Module. It processes real-time responses to a request from a user to analyze the current internet status. This module calls SNMP manager system for the relevant MIB information polling to derive the request message from the client and the value of the current analyzing item from the data, delivers the obtained information to its processor and transfers the analysis information to the client every polls.

Analyzing Item Processor. It serves as a function that derives the analyzed results from the management information polled to each analyzing item by the analysis module. SNMP manager collects the polled management information form network devices in accordance with a request of the real-time analysis module, calculating the analyzed results at a specific point using different analysis methods according to the type of each analyzing item and delivering them to the real time analysis module.

Intranet server. Each module in intranet server has its own function form LAN analysis as user request control, RMON setting module, RMON check module, analysis management module.

User Request Control. It receives and analyzes a message transferred from the client and delivers it to process its appropriate requests. This system saves the message from the client in the message structure, and then analyzes its header to transfer a control to the relevant module corresponding to each analyzing item.

RMON Setting Module. This module is an RMON control module that sets RMON for its validity or invalidity, controlling RMON in a place where this module is required in accordance with the analyzing items.

RMON Check Module. This module inspects the managed system imported form a request of a user, that is, RMON, checks the function of RMON probe, and investigates whether there is no fault in collecting management information. It polls all the managed systems, respectively, imported from the requests of users for its identification of their functions and status.

Analysis Management Module. This module calculates the analyzed results by entering the managed information files real-time collected and accumulated to transfer them to the client module.

The proposed system comprises the client system and the analysis server. To give and receive a request from a user and its response within the system, each component requires a relevant message exchange procedure.

The client system that a user interfaces itself with sets TCP connection to the analysis server to transfer a requested message as a user requests a management, when the requested data may be transferred to the server together with the requested message, and the server transfers ACK to check the receipt. The server receiving the request from the client makes connection to RMON Agent to start polling. RMON Agent responds to the processed result to the server, which returns it to its client by using the responding message.

3 Results & Analysis

Network traffic monitoring system includes such functions as real-time analysis, collection request/suspension and accumulative analysis according to the request of user. To process these functions on the web, the client system and the analysis server contains their relevant processing module. Fig. 3 shows item setting required in conducting the function of tree structure interface and relevant processing of analyzing items as shown in the client system. In setting each item, the same interface structure is involved for the convenience of users, so that items alone requested in selecting the analyzing items could be set.

Fig. 3. user interface in client system

In the function of real-time analysis, the conditions for the current uses and fault of LAN are analyzed to provide a dynamic graphic view to help a user easily understand the network diagnosis. The result display of this real-time monitoring is shown in Fig. 4, which shows examples of graphs demonstrating line availability rate on LAN, real-time, and input and output traffic rate. Such setting helps optimize the management by presenting a simple application to the network management

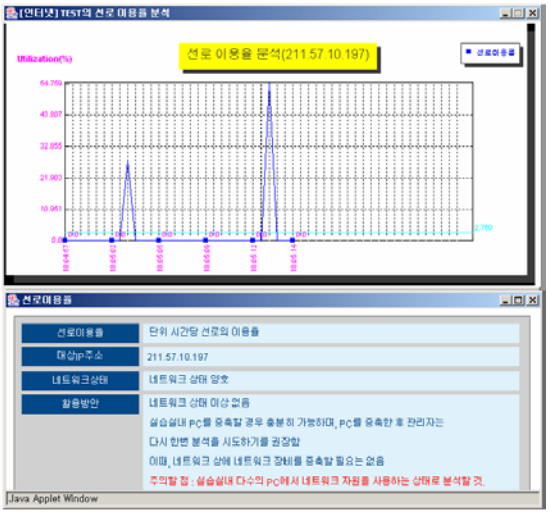

Fig. 4. Results of real-time analysis

In the function of collection request/suspension, LAN is monitored including its requests for the collection of management information to cumulate and analyze the management information of LAN. To fulfill this function, a user must enter RMON agent IP address, community, segment speed, management information of the managed segment, based on which the analysis server collects the management information. When such function of the collection request/suspension is fulfilled, the relevant message is displayed before a user.

The function of accumulative analysis involves analyzing the basic management considerations on the web. This function is implemented to facilitate the understand-

ing of user by providing information about the analyzed results calculated on a basis of the cumulated information during a certain period through a graphic view of various types. During the collected period, a user can compare pieces of information such as line availability rate, error rate and collision rate through various graphic views to identify the abnormality of LAN. Fig. 5 shows the result of this function.

Fig. 5. Results of accumulative analysis

And the proposed system can manage to PC-room without an expert skill by offering a variety application example. That is, a manager can check a managing status showing currently information and a simple application on each items. Fig. 6 shows the result of internet information analyses, which can to help managers perform network management.

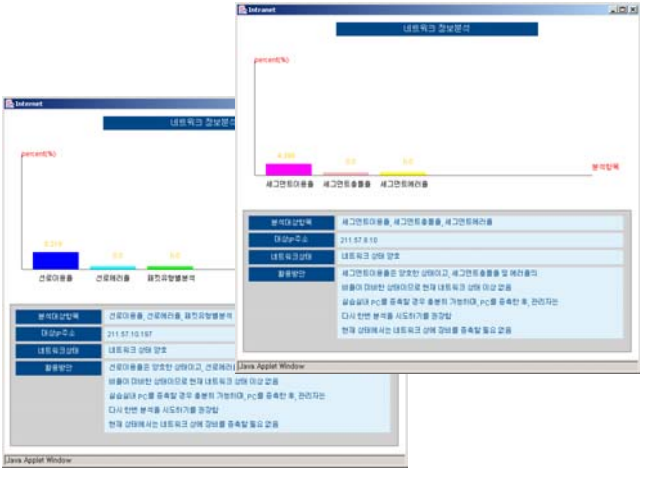

Fig. 6. Results of internet/intranet information analysis

4 Conclusions

In this study, we proposed the web-based network traffic monitoring system aimed to eliminate the constraints in managements, along with providing more user-friendly management tools. The proposed network traffic monitoring system is composed of client system and server system to provide management efficiency and distributed management function: The client system is implemented under JAVA and web related technology to provide the graphic function of clearly and dynamically demonstrating the user interface and the analyzed results on the web, while the client provides such the functions as real-time analysis, collection request/suspension, and cumulative analysis in which a request from a user is received. The analysis server analyzes and processes requests from a user transferred from the client to return their result to the client. Accordingly, the analysis server involves the function in which each request can be simultaneously processed through thread.

The network traffic monitoring system proposed in this study diagnoses the quality of and the conditions for network in the view of network manager to provide optimal performance, failure recovery and the management information that are measures of network configuration. So, it is expected to help effectively fulfill the managements on the complicated LAN where the manager has difficulty in handling such managements.

References

1. Nathan Kalowski,, “Applying the RMON Standard to Switched Environments”, International Journal of Network Management Vol.7, Wiley, 1997.
2. Willian Stallings, “SNMP, SNMPv2 and RMON: Practical Network Management”, Addison-Wesley Publishing Compan, 1996.
3. Gilbert Held, “LAN Management with SNMP and RMON”, John Wildy & Sons Inc, 1996.
4. Nathan J. Muller, “Web-accessible Network Management Tools”, International Journal of Network Management Vol.7, Wiley, 1997.
5. Wilco Kasteleijn, “Web based Management”, M.Sc Thesis University of Twente Department of Computer Science & Department of Electrical Engineering Tele-Informatics and Open System Group 13-20 63-65, 1997.
6. Allan Leinwand, Karen Fang Conroy, “Network Management”, Addison-Wesley Publishing Commpany, 1996.
7. Rechard E.Caruso, “Network Management: A Ttorial Overview”, IEEE Comm. Magazine, March 1990.
8. Allan Leinwand, “Accomplish Performance Mangement with SNMP”, INET’93, 1993.
9. John Blommers, “Practical for Planning for Network Growth”, Prentice Hall PTR, 1996.
10. Snag-Chul Shin, Seong Jin Ahn, Jin Wook Chung, “Design and Implementation of SNMP-based Performance Extraction System”, APNOMS, 1997.