Adaptive Network Monitoring System in Multi-domain Networks

Selma Aneer
Department of Computer Science and Engineering
Calicut University,India

Abstract

Monitoring must be conducted across domains and layers to fully grasp the details of overall network performance. However, when conducting monitoring, it takes too long to analyze the monitoring data because the monitoring system gathers massive sets of data from multiple locations. Furthermore, it is expensive to install the monitoring equipment in multiple locations. To realize faster analysis and lower cost, this paper proposes an adaptive monitoring system which troubleshoots service troubles automatically by creating and running monitoring scenarios; it can reconfigure the monitoring equipment and program dynamically at runtime. This paper surveys all possible networks monitoring system in multi-domain networks. I hope this paper will enable people working on computer networks to choose appropriate network monitoring system to meet their goals.

1. Introduction

Network monitoring describes the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator in case of outages. It is a subset of the functions involved in network management. A network monitoring system is capable of detecting and reporting failures of devices or connections. It normally measures the processor (CPU) utilization of hosts, the network bandwidth utilization of links, and other aspects of operation. It will often send messages over the network to each host to verify it is responsive to requests. When failures, unacceptably slow response, or other unexpected behavior is detected, these systems send additional messages called alerts to designated locations to notify system administrators.

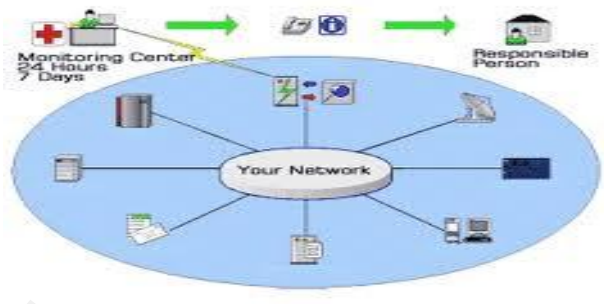

Figure 1: Network Monitoring System

In the real time streaming service[1], when packet loss or reorder occurs, the video is distorted or stopped which degrades the QoE (Quality of Experience). In order to hold QoE acceptable, monitoring should be conducted across multiple domain and multiple layers to grasp the details of overall network performance and troubleshoot any network troubles discovered. By implementing monitoring across multiple domains, networks in different locations administered by different organizations, the network operator identifies troubles more easily. In addition, monitoring across multiple layers, such as application layer and network layer, the network operator can understand the relationship between service quality and the possible causes of trouble. For example, delay varies significantly and traffic is bursty, packet loss maybe caused by buffer overflow of a switch somewhere in the network. The network operator must monitor the network in detail such as delay, inter-packet gap and jitter for this reason. In addition, in order to monitor each packet in a 10-Gbps network[2], network monitoring must have the resolution of micro or sub-micro second.

In order to ensure adequate service quality, monitoring should be conducted across multiple domains and multiple layers to grasp the details of overall network performance and troubleshoot network trouble as rapidly as possible. However, in such monitoring, it takes too long to analyze network performance because multiples sets of data, each of which is very large, must be gathered. Furthermore, it

is expensive to install monitoring sets in multiple locations because each set needs a high-end CPU and large memory. This paper proposes an adaptive network monitoring system, which changes monitoring location and layer dynamically at runtime and can watch multiple domains and multiple layers as necessary. This monitoring system was designed to reduce the time taken from fault detection to cause analysis and reducing system-wide cost.

2. Lierature Survey

Recently several domain networks in different parts of the world have been connected and streaming services are being provided through them. In order to identify where packet loss occurs or where the jitter characteristics are deteriorating, it is important that the monitoring system cover the entire service area and grasp overall network quality. Wide-area deployment of the monitoring system enables us to evaluate the service stability more reliably because the network quality indicators such as delay and jitter can be determined. Because monitoring is performed at many sites and layers in the network as suggested above, there are two issues. The first is the long time need to analyze the monitoring data and the second is the high cost of monitoring.

a. Analysis time

Each monitoring set gathers and presents monitoring data to the network operator, who identifies the location or cause of failure by analyzing the data. Many attributes must be monitored such as jitter and delay characteristics, the number of erroneous packets, and the statistical data of the application layer. When performing failure analysis using these monitoring data, the network operator troubleshoots by rule of thumb because the relationship between cause of fault and monitoring data is not clear yet. The network operator has difficulty in analyzing monitoring data promptly.

b. Monitoring cost

Each monitoring set needs many functions such as application layer monitoring, packet capture and analysis of collected packets in order to monitor the network in detail. Furthermore, to grasp overall network quality in detail, we need to install monitoring sets in as many locations as possible. Monitoring cost is high because many functions are implemented in each monitoring set, including high-end CPU, a large amount of memory and storage.

2.1 VERMONT, a versatile monitoring toolkit

In this paper, Vermont[3], a monitoring probe for IPFIX/PSAMP compliant flow monitoring and packet sampling. Vermont has fulfilled its design goal of providing a versatile high-speed monitoring toolkit consisting of a modular, reusable, and freely configurable architecture. The performance on state-of-the-art PC systems is satisfactory. Nevertheless, optimizations are possible if used for standard flow accounting not requiring the flexible, rule-based aggregation scheme. Excellent compatibility and high robustness have been proven in interoperability tests. Vermont is available as an open-source package It can change the packet sampling rate and filter configuration and perform flow accounting based on rules set at runtime. A rule is characterized by sensor-actor system, and VERMONT executes actor as triggered by a change in the value of sensor. By using VERMONT's sensor-actor system, the monitoring manager can remotely triggered the next operation in accordance with changes in the statistical data. We extended VERMONT so that sensor-actor system can execute programs and implement scenarios at remote sites. The main criteria in the development of VERMONT are Standardized accounting (IPFIX/PSAMP), Policy-based data aggregation, Data collection using libpcap (HW abstraction layer), Efficient, decoupled data processing, Multiprocessor support, High-performance based on optimized hash tables.

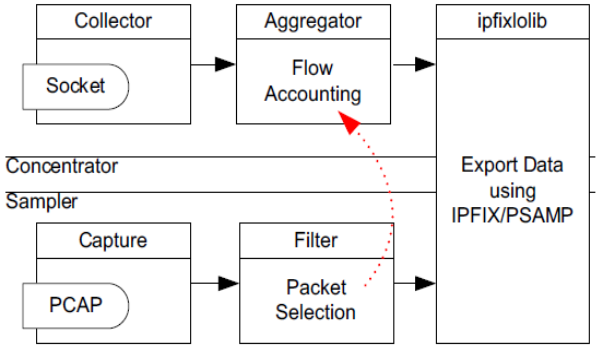

Figure 2.1 Vermont Architecture

2.2 GFI Network Server Monitor

GFI Network Server Monitor[4][GFI04] monitors network for failures or irregularities. It maximizes

network availability by monitoring all aspects of Windows and Linux servers, workstations and devices such as routers. When it detects a failure, GFI Network Server Monitor can send alerts via SMS, pager, email or a network message. GFI Network Server Monitor consists of a network monitoring service and a separate management interface. No agent software needs to be installed on the machines you wish to monitor. The Network Monitor Engine is multi-threaded and can run 40 checks at a time. This software architecture allows for high reliability and scalability to monitor both large and small networks. GFI Network Server Monitor can check the status of a terminal server by actually performing a complete login and checking if the session is established correctly. GFI Network Server Monitor can check the availability of all leading database applications. GFI Network Server Monitor includes extensive checks for monitoring Linux servers. All CPU usage, printer availability, file existence, process running, folder size, file size, users and groups membership, disk partition check and disk space can be monitored by GFI Network Serve. GFI Network Server Monitor allows you to store monitoring data to either an SQL Server or MS Access database backend. SQL Server is more appropriate for users with higher monitoring level requirements as well as those who need to centralize the monitoring results of multiple GFI Network Server Monitor installations in one place, such as backups, remote accessing as well as report generation by third party tools such as Crystal Reports or MS Reporting Services. You can check rule status from any location using GFI Network Server Monitor's remote web monitor. You can check critical processes and services on local and remote computers using GFI Network Server Monitor. You can also monitor the CPU usage of a machine.

2.3 BBMonitor

BBMonitor[5][BBMonitor06] is a commercial tool for Windows. It monitors bandwidth usage and internet connection speed test. BBMonitor displays all bandwidth going in and out of the computer, so you can know that all the internet usage is done by you and not either harmful software or hacker. It can test bandwidth easily and efficiently and stores test data into database. You can improve your bandwidth using database result. Also you can create charts using the data in the database. Internet connection behavior can be seen in the display graph. It will display upload and download speed real in time. Figure 2.2 from [BBMonitor06] shows display graph of BBMonitor.

Figure 2.2 Screen shot of BBMonitor

2.4 Argus

Argus[6] is a fixed-model Real Time Flow Monitor designed to track and report the status and performance of all network transactions seen in a data network traffic stream [Argus03]. Argus runs on Linux, Solaris, FreeBSD, OpenBSD, NetBSD, and MAC OS X and its client programs have also been ported to Cygwin. Argus provides a common data format for reporting flow metrics such as connectivity, capacity, demand, loss, delay, and jitter on a per transaction basis. The record format that Argus uses is flexible and extensible, supporting generic flow identifiers and metrics, as well as application/protocol specific information.

Argus can analyze and report on the contents of packet capture files and it can run as a continuous monitor, examining data from a live interface, generating an audit log of all the network activity seen in the packet stream, providing both push pull data handling models and allowing flexible strategies for collecting network audit data. Argus can be used to monitor individual end-systems, or an entire enterprises network activity. Argus data clients support a range of operations, such as sorting, aggregation, archival and reporting. The network transaction audit data that Argus generates has been used for a wide range of tasks including Security Management, Network Billing and Accounting, Network Operations Management and Performance Analysis.

2.5 CommView

CommView[7] [CommView02] is a commercial tool that runs on any Windows. It monitors Internet and Local Area network activity and captures and analyzes network packet. It collects information about data that passing through the dial-up connection or Ethernet and

decodes them. It lists all network connections, local IP and remote IP and examines all individual packets. Figure 2.3 shows result produced CommiView program.

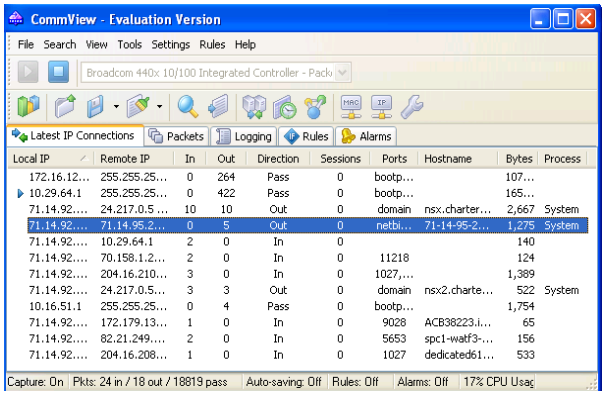

Figure 2.3 Result of CommView

2.6 SmokePing

SmokePing[8] [SmokePing02]is a free-open source tool that works on all Unix platforms. It s measures, stores and displays latency, latency distribution and packet loss. It supports dynamic IP. Using RRD tool it maintains a long term data-store and presents them into graphs, so we can easily get information of each network connection. SmokePing has a smart alarm system. We can define latency or loss pattern. This pattern will trigger alarms. Figure 2.4 [SmokePing 02] shows graph created by SmokePing.

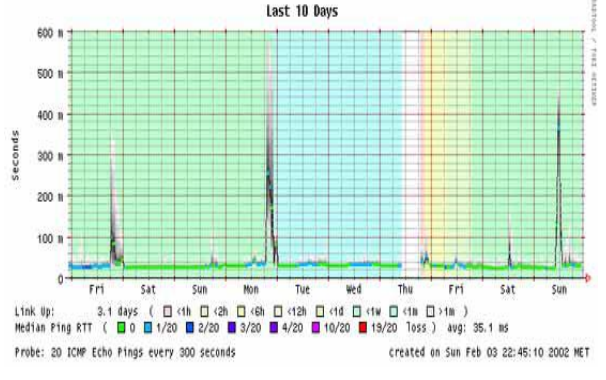

Figure 2.4 (Open source tools) Graph of SmokePing

2.7 Advanced HostMonitor

HostMonitor[9] [HostMonitor05] is a network administrator software. It monitors network traffic, Web, FTP, Mail, DNS servers, and file/folder size. It also checks TCP services, disk space, CPU usage, SQL servers and many other things. It put test result in log files and reports. Figure 2.5 shows a result produced by HostMonitor.

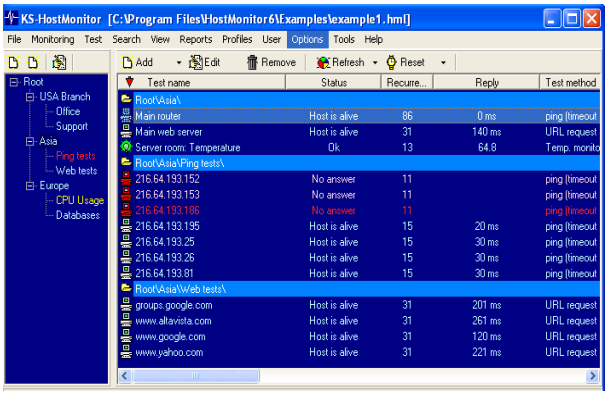

Figure 2.5 Screen shorts of HostMonitor

2.8 Axence NetVision

NetVision[10] [NetVision06] is a commercial tool developed in 2006. It is supported on all operating systems. It monitors servers, applications, TCP/IP services and SNMP devices. Once it runs, in a minute it automatically detects all hosts in the entire network and scans services on them. It present hosts on interactive maps which display all critical information such as service response time, services and host down time, alerts and so on. So problems can be detected and focused easily. It also provides alerts and report about when hosts go down. Figure 2.6 shows an interactive map of NetVision.

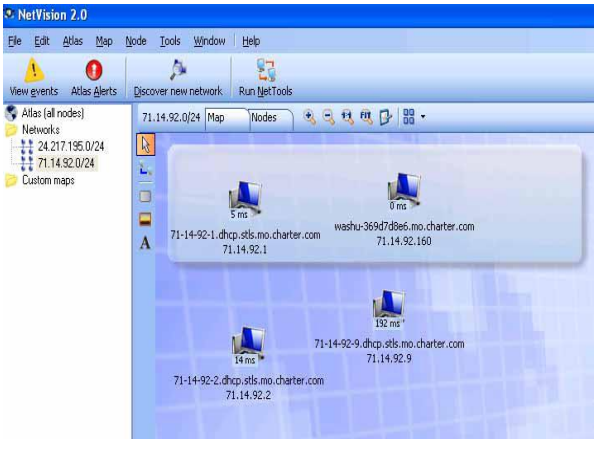

Figure 2.6 Interactive map of NetVision

Table 1. Comparison table

Name	Type	Performance Matrics
Vermont	Flow Monitoring and Packet Sampling	Packet loss
BBMonitor	Application Monitor	Bandwidth usage and speed
CommView	Analyzer	Internet and LAN activity
Advanced Monitoring	Application Monitoring	Network traffic and server's availability
GFI Network Server Monitor	Application Monitor	CPU usage
Argus	Flow Monitoring	Track and report network transaction
SmokePing	Path Characterization	Latency, packet loss
Axence NetVision	Application Monitoring	Applications, TCP/IP services and SNMP devices
Adaptive Network Monitoring System	Multi-domain Monitoring	Packet loss, delay, jitter, CPU usage, load average, data volume, bandwidth, etc

3. Adaptive Network Monitoring System

To realize faster analysis and lower cost, to propose an adaptive monitoring system which troubleshoots service troubles automatically by creating and running monitoring scenarios; it can reconfigure the monitoring equipment and program dynamically at runtime. An adaptive monitoring system that achieves an efficient monitoring and prompt data analysis. First, to increase in speed of analyzing the statistical data obtained from monitoring, we introduce the monitoring scenario which is a predefined troubleshooting procedure of the network operator and the method of cooperating with other monitoring equipment. Next, to reduce the cost of monitoring, we propose a dynamic reconfiguration method of monitoring resources. Figure 3 illustrates the overview of our proposal. This system is composed of three major components: monitoring scenario, monitoring manager and monitoring sets. Each monitoring scenario describes an accumulation of operator's knowledge describing what data to focus on, how to analyze the data, and how to identify trouble location, and understand why the troubles occurred. The monitoring manager manages all monitoring sets on paths crossing several networks. It changes the location or layer of monitoring on the basis of the monitoring scenario selected. A monitoring set executes a monitoring program for each layer, gathers and stores statistical data, and then analyzes the statistical data based on the monitoring scenario. An adaptive network monitoring system works as follows.

1) The monitoring set monitors the network using the default scenario.
2) The statistical data gathered exceeds or drops below a threshold, and the monitoring set notifies that event to the monitoring manager.
3) Based on the notification, the monitoring manager selects the most suitable scenario.
4) The monitoring manager relocates the monitoring set to move the monitoring location or changes execution program according to the scenario.
5) The monitoring manager identifies where and why the trouble occurred by combining and analyzing the statistical data come from the monitoring sets.

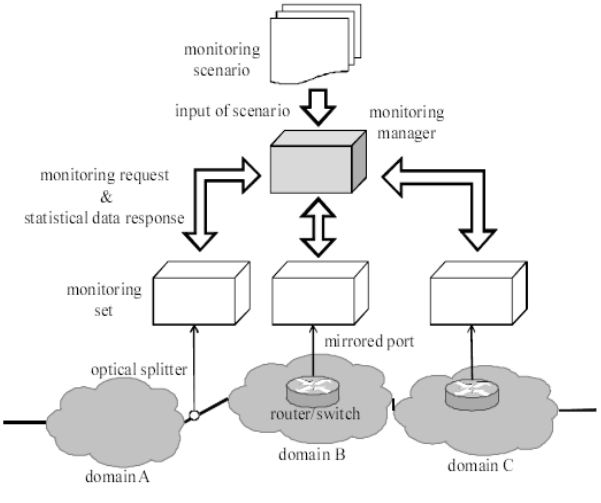

Figure 3: Adaptive network monitoring system

4. Advantages

a. Analysis time

By following a predetermined monitoring procedure and capturing a wide variety of data, monitoring and troubleshooting are performed automatically. Because we automate the monitoring and troubleshooting procedure, the network operator is freed from manual analysis and the time needed for analysis is shortened.

b. Monitoring cost

Each monitoring set changes monitoring layer or location dynamically, monitoring equipment monitors network quality with necessary and sufficient resource. These functions help monitoring equipment save resources, we realize reducing required performance of monitoring.

5. Conclusion

From this paper got the detailed survey of adaptive monitoring system for large-volume streaming services which identify where and why troubles have occurred by using accumulated operator's knowledge, and dynamically allocate network monitoring resources by narrowing down the monitoring network range and layers. The adaptive network monitoring system is composed of the three components of monitoring scenarios, monitoring manager and monitoring sets. An experiment on resource consumption showed that our system could control monitoring programs and reduce resource requirements.

6. References

[1] D. Shirai, T. Yamaguchi, T. Shimizu, T. Murooka, and T. Fujii, "4K SHD Real-Time Video Stremaing System with JPEG 2000 Parallel Codec," in *Proceedings of IEEE Asia Pacific Conference on Circuites and System (APCCAS 2006)*, Singapore, pp. 1855–1858, April 2006.

[2] K. Shimizu, T. Ogura, T. Kawano, H. Kimiyama, and M. Maruyama, "Application-coexistent wire-rate network monitor for 10 gigabit-persecond network," *IEICE Trans. Inf. and Syst.*, vol. E89-D, pp. 2875–2885, December 2006.

[3] R. T. Lampert, C. Sommer, G. Munz, and F. Dressler, "VERMON – A Versatile Monitoring Toolkit for IPFIX and PSAMP," *in Proceedings of Workshop on Monitoring, Attack Detection and Mitigation (MonAM 2006)*, Tubingen, Germany, pp. 20-32, September 2006.

[4] [GFI 2004] http://www.gfi.com/nsm/nsmfeatures.-html and http:// www.gfi.com/nsm/ nsmfeatures.html

[5] [BBMonitor06] http://www.absolutefuturity.com /BBMonitor.html Network Monitoring Tool developed in 06, http://www.Absolute-futurity.com /BBMonitor-.html

[6] [Argus03] http://www.qosient.com/argus and http: //www.Qosient.com /argus

[7] [CommView02] http://www.tamos.com/products/commview/ Network Monitoring Tools developed in 2002 http://www.tam- os.com/products/commview

[8] [SmokePing02] http://oss.oetiker.ch/smokeping/and http://oss.- oetiker.ch /smokeping

[9] [HostMonitoring05] http://www.kssoft.net/hostm-on.eng/index.html. Network Monit- oring Tools developed in 2005 http://www.kssoft.net/hostmon-.eng/ index.html

[10] [Netvision06] http://www.axencesoftware.com.Network Monitoring Tools Developed in 2006 http://www.axencesoftware.com