Practical Aspects Regarding Network Monitoring

CORINA SIMIAN
Faculty of Sciences
University “Lucian Blaga” Sibiu
Str. Dr. Ion Ratiu 5-7, 550012, Sibiu
ROMANIA

VLADISLAV GEORGIEV
University Computer Center
St. Kliment Ohridski University of Sofia
5, James Bourchier Ave., 1164 Sofia
BULGARIA

Abstract: - Monitoring the resources of a network is an important function of network management. One software dedicated to network monitoring can be used. In the case of big networks and in the case of some additional requirements this is not a simple problem. In order to assist people working with these tools, this paper makes a comparative analysis of some software for network monitoring used in Sofia University Network.

Key-Words: - Computer Network, Network Monitoring

1 Introduction

In the past, network management mainly consisted in monitoring devices. Now, network management is a complex process regarding the activities, methods and tools for operation, administration, maintenance and provisioning of networks. Operation includes monitoring the network, to spot problems as soon as possible. More than monitoring the devices, performance management and monitoring has become very important, especially for global organization of a network.

Data for network management is collected through many mechanisms: agents installed on infrastructure, synthetic monitoring that simulates transactions, logs of activities, sniffers and real user monitoring. Network management involves a variety of tools, applications and devices to assist human in monitoring and maintaining networks. A large number of access methods exist to support network and network device management: SNMP, Command Line Interfaces (CLIs), custom XML, CMIP, Windows Management Instrumentation, (WMI), Transaction Language 1, CORBA, netconf, and the Java Management Extensions - JMX

More details about network management can be found in [1].

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 via email, pager or other alarms. A network monitoring system monitors the network for problems caused by overloaded or crashed servers, network connections or other devices ([3]).

The monitoring process includes many activities; Server monitoring, switch monitoring, WAN monitoring, URL monitoring, application monitoring, CPU, memory and disk monitoring etc.

Another important part of network monitoring process is the network traffic measurement which represents the monitoring of performance of a network uplink. Usually, the results of traffic measurements are given using various types of diagrams and graphics.

In the case of a very big network, composed by many sub networks the management process becomes more complicated. If some characteristics for the tools used in management process are imposed (like free software, easy configuration, friendly interface) the choosing of the software products for network management is not very simple. This is the case of the big academic networks. The results obtained for some particular networks can help in choosing the appropriate product.

A search in Google of topics "network monitoring" gave us 21.100.000 results. Many of them refer to management or monitoring software: NetCrunch 5, Argus, MRTG, PRTG Network Monitoring Product Line, GroundWork Monitor, OpManager, Alchemy Network Monitor PRO.

The aim of this paper is to help network administrators of academic computer networks and not only, offering comparative analysis of many tools for network monitoring used in Sofia University Computer Network (SU). The main common characteristics of these tools are: free products, easy to install, work under Linux operating System.

2. Tools for network monitoring

Before making the comparative study of the software for monitoring used in SU, first we will make a short presentation of SU Computer network.
Sofia University has got many campuses in different places in the city. These campuses are connected by MAN, which uses Optical fiber. The SU is using 16 networks Class C, divided in 30 sub networks, counting more than 3000 different computers. SU uses star topology. The operating systems used are Windows and Linux (used only for servers). In SU there are 2 border routers. The routers are connecting in reflector scheme. If one of the routers is down the secondary router is taking the functions of the other router without down time.

We are looking for free license software. The network monitoring software tested in SU was MRTG and CACTI.

2.1 MRTG

The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network links. It monitors router traffic, CPU and RAM. MRTG is free software licensed under the GnuGPL. MRTG monitors SNMP network devices showing how much traffic has passed through each interface. It generates HTML pages containing PNG images which provide a live visual representation of the traffic. MRTG is not limited to monitoring traffic, though. It is possible to monitor any SNMP variable you choose. Even an external program can be used to gather the data which should be monitored via MRTG.

MRTG is written in Perl and works on Unix/Linux, Windows and Netware systems. The pearl script uses SNMP to read the traffic counters of the routers and a fast C program which logs the traffic data and creates graphs representing the traffic on the monitored network connection.

MRTG also creates visual representations of the traffic seen during a given period of time. This is possible because MRTG keeps a log of all the data it has pulled from the router. This log is automatically consolidated using an unique data consolidation algorithm, so that it does not grow over time, but still contains all the relevant data for all the traffic seen over the last two years.

SU tried to work with this soft, tested the soft around one month but renounced to use it be cause of many reasons that we present next. It can make monitoring only for one interface. It doesn't create the graphics dynamic. Only 2 parameters for what you want to combine (traffic in this case), can be given. The programme makes automatic the graphics. The actualization, to each interval of time imposed by the user, is made for all graphics for which MRTG has definition. This consumes many resources on the server: CPU usage, memory, disk usage. Only the scale, the name of the graphics and the colour can be changed. Some difficulties appeared in writing the scripts. Usually the examples for the scripts on the site are used and modified.

2.2 CACTI

CACTI software allows the surveying of the network traffic, CPU usage and memory. It offers information about the load average and the capacity of the processor, by means of graphic representation. It uses MySQL database to save the configuration. With this configuration makes graphics. Cacti uses agents for taking the information regarding the servers, switch, routers and put it in files with extension .rrd.

SU started to work with Cacti 5 years ago. To install the soft it was necessary one week (including the configuration for the network and the writing of scripts).

In the present SU uses Cacti for network monitoring. The web interface for CACTI is user friendly. It is easier to install and make basic preferences Cacti needs to make simpler scripts for graphics. The scripts take the information that is need from the .rrd files and use it to make graphics. It can be used basic script for creating and modifying the graphics. The graphics is created in the moment we want to see it. It takes the last data that is obtained. The program doesn’t use so many resources. The customizability is better than for MRTG. Many elements of the graphs can be customized. More values, not only 2 like for MRTG, can be composed.

We nest present some interpretation of the graphics obtained using CACTI. In these graphics, the inbound represents the information that is coming and the outbound represents the information that is sent.

1. Usually the outbound is bigger than the inbound. These happen because SU network has got many resources: data bases, clusters, mirrors on the open source distributions.

Fig. 1

2. The maximum is attended usually during the working hours, between 14 and 17 and also around the midnight. But this is not a rule because this depends on the amount of information that is discharged from computers all over the world. Usually the minimum for the inbound and for the outbound is attend in the same
3. The maximum is attend for a very short time

4. The traffic on the secondary router is smaller than on the other router.

5. The load average depends on the traffic. In the following graphics is presented the load average for the main and secondary router. The maximum of the load average is attending around 12.

8. Usually the minimum has the same value with the medium value.

2.3 Comparative study

A comparative study makes take into account many characteristics. Commonly measured metrics are response time and availability (or uptime), consistency, reliability, flexibility, customizability, portability.

Using the observation from SU computer network,
we give a comparative table for MRTG and CACTI from the point a view of a user. Because we compare only two products we will use a scale from 0 to 2. A better behaviour regarding a given criteria means a score 2 and the absence of the characteristics means a score 0.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>CACTI</th>
<th>MRTG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clarity of interface</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Reliability</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Response time</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Flexibility</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Customizability</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Graphics on demand</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Periodical update of graphics</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Portability</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Configuration</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Resources needed</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 1.

### 3. Conclusions

In this paper we have evaluated two computer network software monitoring: MRTG and CACTI, using the practical observation from SU computer network. Both are free license software. The main differences between them regard the configuration effort and the resources needed. We recommend CACTI which is more flexible, easier configurable and need less effort in writing the script for graphics. The customizability of graphics is better for CACTI then for MRTG.

### References:

5. [http://argus/tcp4me.com/](http://argus/tcp4me.com/)