Assignment - 1

Probe based operations – Applied Network Management, ET2536

Samuel Sushanth Kolli
School of Computing
Blekinge Institute of Technology
Karlskrona, Sweden
sako15@student.bth.se

***Abstract*— This document is a report which describes the step by step method to install and configure Multi Router Traffic Grapher (MRTG). It also describes the comparison between MRTG and the Network Monitoring tool developed as a task for the assignment 1 for the course Applied Network Management (ET2536).**

I. INTRODUCTION

The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network links. MRTG generates HTML pages containing PNG images which provide a LIVE visual representation of this traffic. MRTG works on most UNIX platforms and Windows NT. MRTG is written in Perl and comes with full source. It uses a highly portable SNMP implementation written entirely in Perl. There is no need to install any external SNMP package. The router interfaces can be identified by IP address, description and Ethernet address, in addition to the normal interface number. MRTG has built-in hooks for using RRDtool. In addition to a detailed daily view, MRTG also creates visual representations of the traffic seen during the last seven days, the last five weeks and the last twelve months. The traffic is displayed in terms of Bytes per Second for both the incoming as well as an outgoing stream for each interface.

In this course, we develop a tool which is similar to MRTG and compare the results of the developed tool with that of MRTG.

II. INSTALLATION & CONFIGURATION OF MRTG

The following steps were followed to install and configure MRTG in Ubuntu 14.04 LTS operating system:

I. sudo apt-get install mrtg

J. sudo mkdir /etc/mrtg && sudo mv /etc/mrtg.cfg /etc/mrtg

K. sudo cfgmaker –output=/etc/mrtg/mrtg.cfg
   a. COMMUNITY@IP.

L. sudo indexmaker —output /var/www/mrtg/index.html /etc/mrtg/mrtg.cfg

M. sudo env LANG=C /usr/bin/mrtg /etc/mrtg/filename.cfg

In your .cfg file include RunAsDaemom:Yes and Interval:5 in global defaults section. Now, view in the browser with the URL as localhost/mrtg/. Make sure that “WorkDir: /var/www/html/mrtg” (under Debian) is uncommented.

III. REPLICATION OF MRTG - TOOL

A tool working similar to MRTG was developed as per the requirement for assignment 1 for this course. This tool uses SNMP and RRDtool. The source code for the backend part was written entirely in Perl. CPAN modules are available to interface with SNMP and RRD through Perl scripting. SNMP & Object Identifiers were used to filter the interfaces for the devices whose credentials were stored in a MySQL database as done by MRTG. RRDtool was used to store the inoctet and outoctet values for each device. MySQL database was used to store the device information and the interfaces that were filtered. The data stored in MySQL was used to display the device credentials in web dashboard. The front end was developed using PHP and HTML.

IV. COMPARISON BETWEEN MRTG & TOOL

The interfaces filtered by MRTG and the tool developed for each device are exactly the same. The traffic observed by MRTG and tool are not exactly the same, the variations can be seen in the screenshots given below for a device provided at the laboratory of the university with the IP address – demo.snmplabs.com ; Port – 1161, Community – public. Figure 1 shows the graph for interface 1 produced by the developed tool. Figure 2 shows the graph for the interface 1 produced by MRTG.

The variations can be seen because, basically the when the protocol exchange is marked blocking, the snmp messages return only when the protocol exchange is completed. But for the tool it’s non-blocking to remove the delays and for the mrtg it is blocking (by default), mrtg uses a blocking and the tool uses a non-blocking. The non-blocking does not cause the code to wait for the response so it is better to use a non-blocking,

The time we start the mrtg and tool are run are different, the time mrtg starts taking samples and tool starts taking samples is not parallel so this difference in start times of the tool and the mrtg can cause the variation in bit rate, to avoid this both should be run parallel at the same time.

The other reasons are bit counters, Basically, A rate is calculated by dividing the difference between the readings through the time interval between them (300 sec in our case). And all counters here are represented using 32 bit counters and SNMP standards has clearly stated that when a counter's maximum value is reached (2^32 - 1 in our case) it is wraped to zero and continues counting from there. In such cases, the Manager polls a counter and calculates a rate by adding a 2^32 to the binary value in next binary value and divides it with the time intervel. So when there is very high traffic so high that a counter is wraped more that once in between the samples (2^32 between samples) obviously the rate is under estimated by the manager. Hence there is a difference in values. And so the 64 bit counters must be used to rectify this issue.

The 64-bit equivalents of ifInOctets and ifOutOctets are used for interface capacities that are higher than 20 Mb/s (standard (RFC 2233)Rules).Counters in SNMP are never reset and there is not a defined starting value but the tool can be reset on interfaces as the SNMP restrictions are not present.

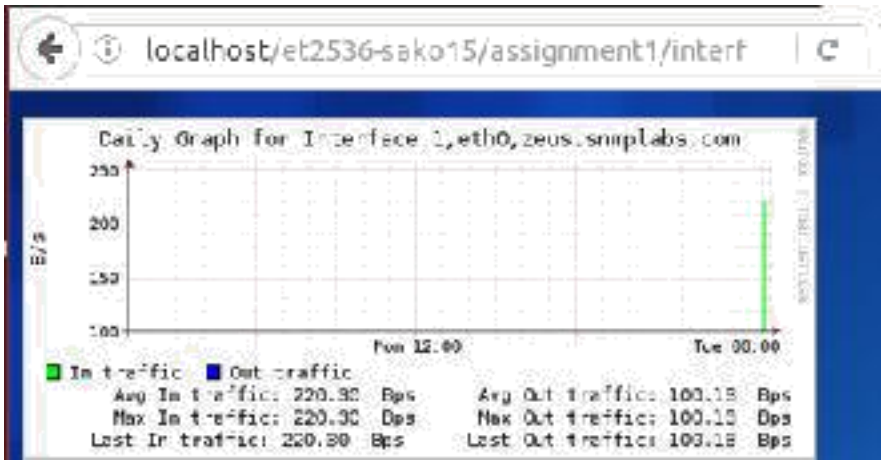
localhost/et2536-sako15/assignment1/interf
Daily Graph for Interface 1,eth0,zeus.snmplabs.com
B/s
200
Mon 12:00
Tue 00:00
In traffic
Out traffic
Avg In traffic: 220.30 Bps
Max In traffic: 220.30 Bps
Last In traffic: 220.30 Bps
Avg Out traffic: 100.15 Bps
Max Out traffic: 100.15 Bps
Last Out traffic: 100.15 Bps

Fig: 1

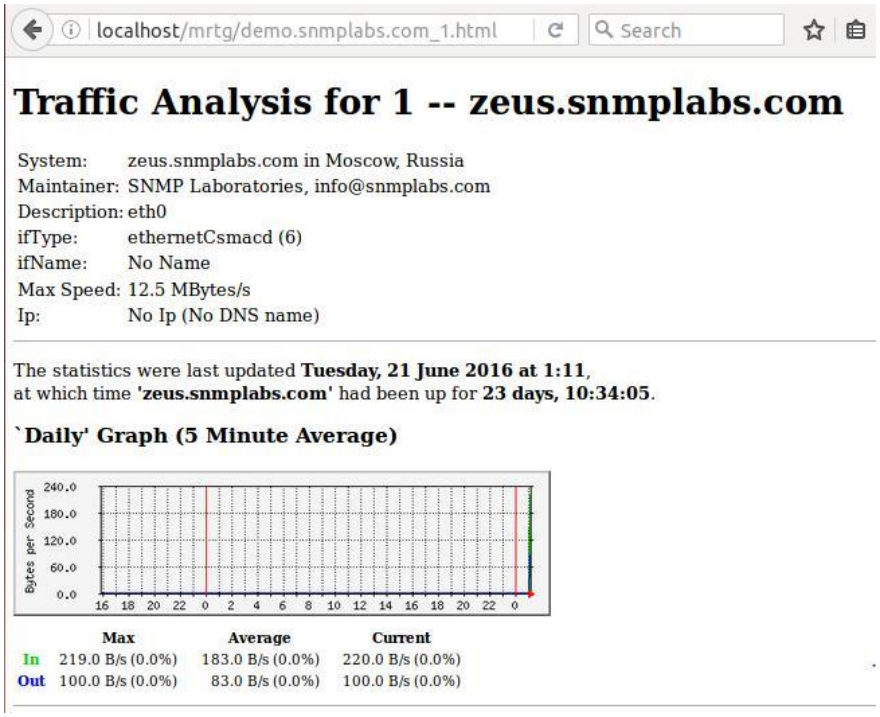
localhost/mrtg/demo.snmplabs.com_1.html
Search
Traffic Analysis for 1 -- zeus.snmplabs.com
System: zeus.snmplabs.com in Moscow, Russia
Maintainer: SNMP Laboratories, info@snmplabs.com
Description: eth0
ifType: ethernetCsmacd (6)
ifName: No Name
Max Speed: 12.5 MBytes/s
Ip: No Ip (No DNS name)
The statistics were last updated Tuesday, 21 June 2016 at 1:11,
at which time 'zeus.snmplabs.com' had been up for 23 days, 10:34:05.
`Daily' Graph (5 Minute Average)
Bytes per Second
240.0
180.0
120.0
60.0
0.0
16 18 20 22 0 2 4 6 8 10 12 14 16 18 20 22 0
Max
Average
Current
In 219.0 B/s (0.0%) 183.0 B/s (0.0%) 220.0 B/s (0.0%)
Out 100.0 B/s (0.0%) 83.0 B/s (0.0%) 100.0 B/s (0.0%)

Fig: 2