Helsinki University of Technology

Department of Electrical and Communications Engineering
Networking Laboratory

S-38.3133 - Networking Technology, laboratory course
Spring 2007
Work number 32: SNMP

Instructions, preliminary exercises and questions for final report

5.1.2007
Juha Järvinen
Juha.Jarvinen@netlab.tkk.fi

Updated by Juha Järvinen
Juha.Jarvinen@netlab.tkk.fi

SNMP Laboratory Work

Preliminary Exercises

Add the cover page according to the example to your answers. Answer the following questions shortly **but clearly**. Answer questions in Finnish if you are Finnish, others in English. Make sure you understand the basics of SNMP before entering the lab. It could also be a good idea to examine laboratory assignment beforehand. Return the preliminary report three days before coming to the laboratory.

1. SNMP (Simple Network Management Protocol) isn't a perfect protocol for network management, it has some little bugs. What is absolutely the most important and the biggest lack of the SNMP protocol? How is this lack corrected or what has been done for correcting it?

2. Because of SNMP is based on UDP, the SNMP is not a reliable protocol. Let's say you did the SNMP SET operation. How do we guarantee that the SNMP SET packet reached the agent?

3. In the SNMP objects are used to define the hierarchical structure of the protocol. This is done with macros. Explain all the useful information on a code below. In addition mention the other values of the STATUS field.

```
sysContact OBJECT-TYPE
   SYNTAX DisplayString (SIZE (0..255))
   ACCESS read-write
   STATUS mandatory
   DESCRIPTION
     "The textual identification of the contact person
     for this managed node, together with information
     on how to contact this person."
   ::= { system 4 }
```

4. An authentication mechanism of the SNMP protocol is very simple. Tell more about it.

5. Describe the 5 functional areas of OSI Network Management (FCAPS). Use a couple sentences per an area.

6. Active and passive network monitoring.
    a. Define active and passive network monitoring.
    b. In addition mention pros and contras of these two methods.
    c. Mention (and draw) different ways to connect a measurement computer to the network, when capturing data passively.

7. Describe situations when it is useful to use
    a. Active network monitoring.
    b. Passive network monitoring.
    c. Both active and passive network monitoring together.

SNMP Laboratory Assignment

1.Introduction

SNMP (Simple Network Management Protocol) is a very handy tool for getting all kind of information from different communication devices. You can get information for example of the speed of data stream in a router or a radio link.

You have three hours to do this lab work and this time should be sufficient. But if the time is too short for you, reserve more time. The written documents play a big role in grading, so make the final report carefully. If you have appendices, remember to refer to them in your text, too!

Any comments and questions concerning this work should be addressed to Juha.Jarvinen@netlab.tkk.fi in the spring 2007.

2.Goals of this laboratory work

After this laboratory you understand the basics of SNMP and how to gather traffic information from different sources, for example from different interfaces. You familiarize yourself with different network management tools. In addition after the lab you should understand the basics of passive monitoring and somehow handle captured data.

3.Environment

In this laboratory work we use one part of the laboratory network, which is also connected to the Internet. The structure of the network is shown below in fig 1. *Ohmi.noc.lab* (IP 10.38.0.5) includes a MIB (Management Information Base) and it works as a management station.

A program called MRTG (Multi Router Traffic Grapher) is installed on *ohmi*. It is a web-based analyzation program using data of MIB. *Ohmi* has an Apache web server, so we can watch diagrams for example on the screen of Delta computer. MRTG uses SNMP functions for gathering data. More information about this program you will find at http://people.ee.ethz.ch/~oetiker/webtools/mrtg.

Ifmonitor program is installed on *Ohmi* and uses MySQL database. More information about this program can be found at http://ifmonitor.preteritoimperfeito.com/. Ifmonitor doesn't use SNMP functions.

Ohmi has Debian OS with a window system. At http://10.38.0.5/snmp/ you will find all the programs which are used in this laboratory works.

In passive network monitoring we use a method to capture data from the network: port mirroring. There are a couple of scripts made to parse the data to plain text.

4.Instructions

This laboratory work only includes simple questions and calculations. In the final report you have to answer questions, but also include used commands (questions 3 – 9). For example if a command is

```
snmpget localhost -Of -v 1 -c public system.sysContact.0
```

You have to include `system.sysContact.0` or two last objects `sysContact.0`. This only relates to exercises where snmpd program is used. If you don't do it this way, you will lose 50 % of your points per exercise!

If snmpd program is not running or it timeouts, type `/etc/init.d/snmpd` restart on the command line. More information about commands and snmpd program you get at http://net-snmp.sourceforge.net/.

5.Exercises & Questions

Q1. The State of the Network –tools: Comparing MRTG and Ifmonitor

You have to run some commands at ohmi to make diagrams to a website:
First clean the www directory: /var/www/mrtg/

Then give the command:

```
cfgmaker --global 'WorkDir: /var/www/mrtg/' --output /home/mrtg.cfg
public@ohmi.noc.lab
```

You find an analyzation site at http://10.38.0.5/snmp/.

Now you have started these two programs to draw bps diagrams of Ohmi. Back to this exercise at the end of the lab.

Then save the pictures of programs. At the final report you should compare these two programs and their outputs:

Outputs

1. In your opinion which program is better to get general view of traffic?
2. If you would have to check what it has happened in the network at time between 5:48pm and 5:50pm.
3. Could it possible to make out only with one type network status program (e.g. MRTG) in big networks.

   Remember to justify your opinions!

Programs

4. Desribe briefly operational principle of these two programs.
5. Pros and contras of these two programs
6. In your opinion which program is better?

Q2. Passive monitoring

- Go to first http://switchcontrol.noc.lab -> Port Mirroring. Then enable all the ports apart from the Labroom Trunk port from D-link.
- Then login to the Capture computer as a capture user: *ssh capture@capture.noc.lab*
- There login as root (do not use the *su* command): *ssh root@localhost*
- Now start capturing with tcpdump: we want to capture 1000 packets from the eth1 interface: *tcpdump -c 1000 -ni eth1 -w snmp.pcap*

Capturing takes a while, you can continue to the next exercises and back to this at the end of lab time (however before the question 1). Then you will have a dump of network traffic. Now we want to parse it to plain text.

- Run *sh snmp_vlan.sh*
    - it produces a snmp_vlan.txt file. The form is

```
timestamp bytes VLAN_id
```

- Run *sh snmp_proto.sh*
    - it produces a snmp_proto.txt file. The form is

```
timestamp bytes transport_layer_protocol
```

At final report you should show the graphs of

1. The distribution of transport layer protocols of bytes (a pie graph)
2. The distribution of transport layer protocols of number of occurrence (a pie graph)
3. The bits/second/VLAN id graph of the four most visible VLAN ids. Use one second time block to calculate bps. So you should have four graphs in the same graph.
4. The timestamp/bytes graph.

In addition you should tell briefly what you can say about the traffic (per a graph).

If you want you can include these graphs as appendixes. Remember to put correct titles etc. to your graphs. You can you whatever programs to make graphs: different scripts, program languages, spreadsheets, mathematics programs and so.

In addition tell shortly how you have managed to do these graphs: which programs you used and so on. If you have used scripts, programming languages or Matlab, please include programming files to the final report.

Do the next seven exercises by using *Ohmi.*

Q3. SnmpWalk

What is the device's uptime and what is its system name? Does the device work as a router now? Use snmpwalk command!

Q4.

How many physical network interfaces do you find in the device by using the snmp program? How fast are they and what type are they? What is the maximum packet size of interfaces when transmitting data? Find also their IP-addresses.

Q5.

Calculate the proportion of error packets to all transmitted packets. Do the same for received packets. You need to do calculations from two first physical interfaces only! Mention them. Give results as percentages.

Q6. SnmpGet

Calculate average received and transmitted data traffic of interfaces [bit/s]. Make two charts (one for received and one for transmitted). Fill them with ten values and then calculate mean value and deviation.

Q7.

Calculate utilization of two physical network interfaces.

Q8.

Make inquiries from *Ohmi* computer by using snmpwalk command. Capture messages and include a brief analysis for example about the structure of messages. Which command does snmp use when inquiring; you can't see any snmpwalk messages. Explain why it's easier to use another command. What is object identifier? Tell more about it!

Q9.

Do the next exercise by using the ***ohmi*** computer again. Let's surf in the Internet. Go to the main site of TKK (www.tkk.fi) and surf them for a while (for example 120s). Calculate the used bandwidth. Compare this value to the site of MTV3 (www.mtv3.fi). Try to think, based on these results and practice, can you easily surf the site of MTV3 with a computer with a 56kbit/s modem. Can you get SNMP information from a normal computer phone modem (V.90)? Why/why not?

Remember back to questions 2 and 1!

The next three exercises you don't have to do under your laboratory time! But of course, answers must be written in the final report.

Q10.

Let's plan a network analyzation program. Where should "one probe" (a place where traffic measurements should be taken from = SNMP management agent) be put in a network hierarchy, if we want to measure traffic of

a. An individual user using a modem (V.90).

b. A small company

c. FUNET

Measurements are used for billing. Give explanations, too, why you chose those places.

Q11.

Why shouldn't you put a probe to a backbone network, when you want to get some information about the traffic of an individual user? Isn't it easier to put it there, when you only need a probe to the whole network? Why don't operators use SNMP in billing if we would like to charge customers for transmitted traffic?

Q12.

What kind of things (e.g. meters) can you observe with passive network monitoring?

6.Final Report

Answer the questions. Add the cover page according to the example (shown at course's homepage) to your answers. Return the final report in three weeks.