Aalto University

School of Electrical Engineering
Department of Communications and Networking

ELEC-E7330 Laboratory Course in Internet Technologies

32 – Network Monitoring

Student edition

Juha Järvinen, 5.1.2007
Matias Elo & Antti Kajander, 4.8.2010
Neela Shrestha, 30.8.2012
Riku-Antti Oinonen & Laura Tilli, 8.8.2013
Jitendra Kumar Pandit & Sunny Dutta, 30.7.2014
Abbas Waqar & Ogenda Dancun 20.07.2019

Contents

This laboratory work includes 35 questions. The total number of points is 90.

Answer the following questions shortly but clearly. You can answer in Finnish/Swedish or in English. It is also a good idea to examine the laboratory assignment beforehand. There is only 3 hours work time on your lab turn

1. Preliminary exercises

[P01] (2 points)
SNMPv1 (Simple Network Management Protocol) [1] isn't a perfect protocol for network management, but what is absolutely the most important and the biggest lack of the SNMPv1 protocol? How this lack is corrected in newer SNMP versions [2] or what has been done for correcting it? [3]

[P02] (2 points)
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 reaches the correct agent?

[P03] (5 points)
In SNMP objects are used for defining the hierarchical structure of the protocol. This is done with macros. Explain all the useful information in the code below. In addition mention the other possible values of the STATUS field.

```
sysLocation 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 6 }
```

[P04] (3 points)
The authentication mechanism of SNMPv1 is very simple. Tell more about it.

[P05] (5 points)
Describe the five functional areas of OSI Network Management (FCAPS). Use a couple sentences per an area.

[P06] (6 points)
Active and passive network monitoring.

(a). Define active and passive network monitoring.
(b). 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.

[P07] (3 points)

Describe situations when it is useful to use

(a) Active network monitoring.
(b) Passive network monitoring.
(c) Both active and passive network monitoring together.

[P08] (2 points)

What are Network Flows or Netflows? What are the usages of netflow data?

[P09] (4 points)

Here's the configuration of SNMPv3 for Juniper routers which you will slightly modify during your lab time. Explain briefly the most important parts and write down the commands of how to modify the passwords (with authentication MD5 and encryption DES) of snmpv3 user and how to add new view to include oid system only.

```
[edit snmp]
description <SERVER DESCRIPTION>;
location <SERVER LOCATION>;
contact <CONTACT INFORMATION>;

snmp {
    v3 {
        usm {
            local-engine {
                user <username> {
                    authentication-md5 {
                        authentication-key "<you Key here>";
                    }
                    privacy-des {
                        privacy-key " <you Key here> ";
                }
            }
        }
        vacm {
            security-to-group {
                security-model <usm> {
                    security-name <username> {
                        group <groupname>;
                    }
                }
            }
            access {
                group <groupname> {
                    default-context-prefix {
                        security-model <usm> {
                            security-level privacy {
                                read-view <view name>;
                                notify-view <view name>;
                            }
```

```
                }
            }
        }
    }
  }
}
engine-id {
    local 62;
}
view view-all {
    oid <oid number or name> include;
}
        }
```

[P10] (3 points)

Explain what are SNMP Traps and how to configure SNMP Traps on Juniper routers. Check Juniper manual [5].

2. Laboratory Exercise

2.1. Introduction

SNMP (Simple Network Management Protocol) is a very handy tool for getting all kinds 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, system temperature, processor load etc. After this laboratory you understand the basics of SNMP and how to gather traffic information from different sources. You familiarize yourself with different network management tools. You also know how to use SNMPv3. In addition, after the lab you should understand the basics of passive monitoring and somehow handle captured data

2.2. Environment

2.2.1 Network

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 Figure 1. Laboratory has one Juniper J2320 router (10.255.4.201), which is using SNMPv1 to share system information. Ohmi.noc.lab (IP 10.38.0.5) has also its own MIB (Management Information Base).

You will use ohmi as your workstation in this lab work. You can ssh into ohmi by using **lab** as username and password both.

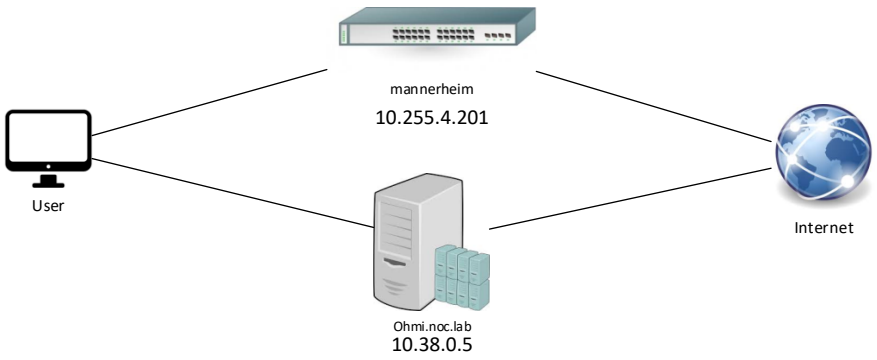

Figure 1 Topology

2.2.2 Software

A program called MRTG (Multi Router Traffic Grapher) [6] is installed on ohmi. It is a web-based analyzer program using the data of MIB. Ohmi has an Apache web server, so we can watch diagrams for example on the screen of remote computer. MRTG uses SNMP functions for gathering data.

Netflow Senser or NfSen [7] is useful software for network management and monitoring. It is a graphical web based front end for nfdump netflow tools. NfDump tools collect and process netflow data on command line. NfSen displays graphs of flows, packets and traffic of netflow activated interfaces.

In http://ohmi.noc.lab/ you will find all the web tools, which are used in this laboratory work.

2.3 Instructions

This laboratory work includes simple questions and calculations and some router configuration. In the final report you have to answer questions, but also include used commands and their outputs. 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!

Check if snmpd program [9] is running with the command *service snmpd status* in the terminal. If it is not running, start with *sudo service snmpd start*. More information about commands and snmpd program you get at http://netsnmp.sourceforge.net

2.4 Exercises and Questions

2.4.1 Comparing MRTG and NfSen

Open up MRTG and NfSen from http://ohmi.noc.lab/ in Firefox. You'll see a few graphs being drawn. Get back to this exercise at the end of the lab turn. Then save pictures (screen captures / graph images) of the two web pages. Compare the programs and their outputs in your final report, according to the questions below. You can answer to the questions at you own time after the lab. Remember to justify your opinions.

[Q01] (2 points)

In your opinion, which program is better:

(a) to get general view of traffic?

(b) if you would have to check what are active ips or protocols in the network during certain period.

[Q02] (2 points)

Could it be possible to manage with only one type of a network status program (e.g. MRTG) in big networks?

[Q03] (3 points)

Describe briefly

(a) the operational principles of these two programs.

(b) the pros and contras of these two programs.

[Q04] (2 points)

In NfSen, three types of graphs are shown -bits/s, packets/s and flows/s. Compare them and write briefly what information is shown by them.

[Q05] (2 points)

For what purposes you will consider using MRTG and NfSen?

2.4.2 Passive Monitoring

There is already a pre-captured file named netmon.pcap in home/lab. To perform passive monitoring first run the script pcap2tsv.py on the pre-captured file for parsing the dump to plain text in tab separated format, run it.

```
./pcap2tsv.py vlan netmon.pcap netmon_vlan.csv
./pcap2tsv.py proto netmon.pcap netmon_proto.csv
```

You will now have two text files (.csv) with tab separated values, one with VLAN ID information and one with transport layer protocol information. Use scp to transfer them to the desktop computer. Save these files, you will use them in your final report.

After the lab time, import these files in to a spreadsheet application such as OpenOffice.org Calc or Microsoft Excel (available at, e.g., the Maari house) to analyze the data in your final report. You are allowed to use any programs, tools or scripts you wish.

[Q06] (6 points)

In the final report you should include the following graphs:

(a) Bytes per transport layer protocol as a pie graph.
(b) Packets per transport layer protocol as a pie graph.
(c) The bits/second/VLAN bar graph of the four most visible VLAN IDs. Calculate the average bps over the capture time. You should have all four VLANs in the same graph.
(d) The total bits/second graph as a run chart.

In addition, you should tell briefly what you can say about the traffic (per a graph). Tell shortly how you made these graphs: which programs you used and so on. If you used scripts, programming languages or Matlab, please include the code to the final report. If you want, you can include these graphs as appendices. Remember to put correct titles etc. to your graphs.

2.4.3 SNMP

[Q07] (2 points)

Use snmpwalk to find out what is ohmi's uptime and what is its system name? Does the device work as a router now? Use snmpwalk command! You can check /etc/snmp/snmpd.conf file to find the community string for ohmi.

[Q08] (3 points)
How many physical network interfaces do you find in the device by using the snmpwalk? 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.

[Q09] (2 points)
Using SNMP, find the SNMP indexes of gigabit ethernet interfaces of Router mannerheim 10.255.4.201. Can you find if an interface is down due to missing link or is manually shut using snmp?

[Q10] (6 points)

Run sudo wireshark in the Terminal. Start a packet capture on the local loopback interface **lo**. Make inquiries using the snmpwalk command again. In the final report include a brief analysis about the structure of messages and answer to the following questions.

(a) Which command does SNMP use when inquiring; you can't see any snmpwalk messages.
(b) Explain why it's easier to use another command.
(c) What is the use of object identifier?

[Q11] (2 point)
Use snmpwalk command for host 10.255.4.201 to list values associated with following OID

.1.3.6.1.2.1.2.2.1.2
.1.3.6.1.2.1.1.3.0
.1.3.6.1.4.1.2636.3.1.13.1.5.9
.1.3.6.1.4.1.2636.3.1.13.1.7.9

Is SNMP client able to interpret all the OIDs?

[Q12] (2 points)

Access the file with /etc/snmp.conf with you favourite editor and uncomment the following line

#mibdir +/usr/share/snmp/mib/juniper

Now use the following command with OIDs given in Q 11.

snmpwalk 10.255.4.201 -v 2c -c <community> -m JUNIPER-MIB <OID>

What are OIDs? What is the difference in the result as compared to that above question? What can you comprehend from this? Remember to comment the mibdir line again in snmp.conf.

2.4.4 SNMPv3

SNMPv3 on linux host:

As already mentioned in the preliminary exercises, security is a major issue with SNMPv1/SNMPv2.

To overcome this problem, you should now configure linux host to use snmpv3 instead. The configuration file is /etc/snmp/snmpd.conf. Create new SNMPv3 user with authentication MD5 and encryption DES. Allow them to read only oid system. Restart snmpd with *service snmpd restart*.

Start Wireshark capture on lo0 on capture and use snmpwalk to fetch system information using SNMPv3

[Q13] (2 point)
Write the additional lines in configuration file for enabling SNMPv3.

[Q14] (2 points)
What was the used command and its output?

[Q15] (3 points)
Compare captured packets to the previously captured SNMP packets.

SNMPv3 in Juniper routers:

Router mannerheim has been configured for SNMPv2. When you use command show snmp, community name will be displayed. For SNMPv3, you have to configure on your own. For SNMPv3 minimum configuration, follow link
http://www.juniper.net/techpubs/en_US/junos13.3/topics/task/configuration/snmpv3-minimum-config-junos-nm.html and for more details,
http://www.juniper.net/techpubs/en_US/junos13.3/topics/example/snmpv3-configuration-junos-nm.html.

Login to the router using ssh with username **student** and password **Student**:

ssh student@10.255.4.201

Also add new view to include oid system only. Use the commands you found out for the preliminary report. Once you have the above configured, start a new Wireshark capture on ens192 (interface of virtual Ohmi server) for capture and use snmpwalk also on capture to fetch system information again now using SNMPv3.

[Q16] (2 points)
What was the used command and its output?

[Q17] (5 points)
Attach your configuration and briefly explain the components

Remember the MRTG vs NfSen (2.4.1) and passive monitoring (2.4.2) questions!
Remember to take a copy of every file needed for the final report. Then delete all files you have created during the assignment from the workstation

3. Final Report

In the final report answer the following questions marked with Q and the following final report questions. Stay to be point and present concise answers to the questions.

[F1] (3 points)

Let's plan a network analyzer program. Where should "one probe" (a place where traffic measurements should be taken from) be put in a network hierarchy, if we want to measure the traffic of? Measurements are used for billing. Please explain why you chose those places

(a) An individual user using an ADSL connection.
(b) A small company
(c) FUNET

[F2] (1 point)

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?

[F3] (1 point)

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

[F4] (2 points)

What are the advantages of using netflow based traffic monitoring over traditional SNMP based traffic monitoring? Write two scenarios where netflow can facilitate network administrators.

References

[1] J. Case, M. Fedor, M. Schoffstall, and J. Davin. A Simple Network Management Protocol (SNMP). http://tools.ietf.org/html/rfc1157. Checked July 24, 2019.

[2] J. Case, R. Mundy, D. Partain, and B. Stewart. Introduction and Applicability Statements for Internet Standard Management Framework. http://tools.ietf.org/html/rfc3410. Checked July 24, 2019.

[3] SNMP Research International, Inc. Security in SNMPv3 versus SNMPv1 or v2c. http://www.aethis.com/solutions/snmp_research/snmpv3_vs_wp.pdf. Checked July 30, 2014.

[4] Les Cottrel. Passive vs. Active Monitoring. http://www.slac.stanford.edu/comp/net/wan-mon/passive-vs-active.html. March 2001. Checked July 24, 2019.

[5] Juniper Networks, Inc. JUNOS 12.1 Network Management Configuration Guide. http://www.juniper.net/techpubs/en_US/junos12.1/information-products/topic-collections/config-guide-network-mgm/config-guide-network-mgm.pdf. Checked July 24, 2019.

[6] Tobi Oetiker. Tobi Oetiker's MRTG - The Multi Router Traffic Grapher. http://oss.oetiker.ch/mrtg/. Checked July 24, 2019.

[7] NfSen developers. NfSen - Netflow Sensor. http://nfsen.sourceforge.net/ Checked July 24, 2019.

[9] net-snmp developers. Net-SNMP. http://www.net-snmp.org/ Checked July 29, 2019.