TECHNISCHE UNIVERSITÄT BERLIN

Fakultät IV – Elektrotechnik und Informatik
Fachgebiet Intelligente Netze und Management verteilter Systeme
Prof. Anja Feldmann, Ph.D.
A. Mehmood, W. Mühlbauer, H. Schiöberg, A. Wundsam

Praktikum RouterLab SS 2008
Work Sheet 10: A glimpse of SNMP

Extra-Credit Worksheet   Info 10.1

Note that this worksheet is a *short extra credit worksheet*. That means

- It is worth 50 points

- These 50 points will not add up to the official total score of the course. The official total score of the course is thus 885 points. You will need 663 points to pass the course, and at least 840 points for a straight 1.0. This worksheet can help you earn those few last points.

- It is not completely optional though – you still may only complete one worksheet with below 25% (including this one). That is, if you already missed that mark once, you have to complete this one. Otherwise feel free to earn the extra points or enjoy your holidays!

Network operators need be able to monitor the state of the components in their network. Especially, in a large scale, complex environment, maintaining a high level of reliability without a good system monitoring is next to impossible.

Table 1: Assignment of devices to groups

Gruppe	Ham-Cloud	Muc-Cloud
Switch	ham-sc1	muc-sc1
Router	ham-rc1, ham-rj1	muc-rc1, muc-rj1
Host A	loadgen104	loadgen102
IP range	10.1.0.0/16	10.2.0.0/16

Question 1: (5 Points) *The same procedure as last worksheet...*
The same procedure as every worksheet. Set up your infrastructure. This time, we will stick with a very simple setup: One loadgen, one switch(`sc1`), one Cisco router (`rc1`), and one Juniper router (`rj1`). Establish IP connectivity between the loadgen and the routers. No VLANs needed this time! (Actually anyone who sets up an unnecessary trunk port in this assignment will have to pay for one round at the beergarden tutorial next week).

But now, let's get down to business. Business today is SNMP!

The management protocol SNMP   Info 10.2

SNMP is the protocol most commonly used to exchange management information between components on the Internet.

The communication model follows the Client-Server paradigm. The following parties participate in the protocol: One *Manager* (oder *Management Station*) and several *Management Agents*, which are located inside of the monitored component (also called *Managed Node*). The Manager acts as

---

a client and requests pieces of information from the Agent (acting as the server), using the *get-request*. Alternatively, it can also transfer information there (*set-reqest*). Access to the information is protected using a simple shared secret, the *community string*[1].

The information is structured based on an information model: the *Structure of Managed Information, SMI*. According to the SMI, the agents in the managed nodes have a characteristic *Management Information Base (MIB)*, a structure of variables. The Agent-MIB represents a subtree of the standardized Internet-MIB tree.

Question 2: (40 Points) *Network management with SNMP*

Info 2 provides an overview of network management using SNMP. Accomodate yourself in the following questions about any necessary details on the SNMP management, and about the invocation and functionality of the tools involved.

In this question, we take the first steps with the protocol SNMP and the associated tools, and we examine the information and communication model.

(a) The command line programs `snmpget`, `snmpset` and `snmpwalk` (All present on the loadgens) are useful tools to perform simple management tasks. Read up on their functionality and basic invocation syntax in the `man` pages. Hint: Use the option `-v1` the avoid conflicts with different versions of SNMP, and use `-Of` to always output full OIDs.

(b) Enable SNMP on the two routers. Some hints on the required communication commands can be found in Info 3.

(c) Make sure IP connectivity between your lg-monitor and the rc1 and rj2 routers in your cloud is established. Both routers have to reachable via *ping* from your loadgen. Now request the value of the Agent MIB object with the OID `iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0`.

> ### Enabling on Ciscos and Junipers
> Info 10.3
>
> On Cisco routers, the commands to activate and configure an SNMP agent in configuration mode are initiated with `snmp-server`. Type `snmp-server ?` to request a list of available configuration commands and a short description.
>
> On Juniper, there is a configuration section called `snmp`. This section provides essentially the same options as available with Cisco. Navigate through the `set` and `edit` commands using `?`.

(d) SNMP is based on UDP. What consequences does this have for different error situations? E.g., what behaviour did you observe when there was no SNMP agent running on the router? What happens in case of packet loss? What happens if you pass a wrong community string?

(e) Analyze the SNMP packets using `Wireshark`. What pieces of information are transmitted in the packets, which protocol fields are present?
How does the OID look? Does `snmpget` show it in the same way? Can you also provide the numeric OID to `snmpget`?
Can you think of anything you would have done differently when designing the procotol?
Include your tracefile with your answer.

(f) Set the router MIB variables for *system contact* and *system location* to arbitrary values.
Do an `snmpwalk` on `iso.org.dod.internet.mgmt.mib-2.system`.
Capture the packet exchange, like in exercise (e). What types of request do you see now? The same ones as before? Explain how *snmpwalk* works!

(g) Do an `snmpwalk` on `iso.org.dod.internet.mgmt.mib-3.interfaces.ifTable` on a router of your choice. Orient yourself in the table, and note down the table for two interfaces (sensibly, FastEthernet0/0, 0/1, or ge-0/0/0, ge-0/0/1). Note down all columns!

(h) The definition of the *Structure of Management Information (SMI)* is done via the MIBs. Take a look into `/usr/share/snmp/mibs`.
Lookup the definition of the column `ifAdminStatus` in the interface table you just analyzed. What is defined here? In which way does it differ from the defintion of the column `ifOperStatus`?

(i) Use `snmptable` to output the entire interface table

(j) `snmpset` allows to change the value of specific MIB variables using SNMP. Try to change the `sysLocation` of the subtree `system`. Does it work? Validate, e.g., using `snmpget`! If it did not work, which error message did you get (compare to your findings from question d)?

For the router to allow MIB variables to be set using SNMP, you have to enable specific permissions. By default, only *Read* permissions are granted. See info 4.

> **Enabling write access for SNMP** Info 10.4
>
> On Cisco, you can grant write permissions to communities by appending `rw` to the `snmp-server community` command after the community string.
>
> On Juniper, you have to change two things: You have to add `authorization read-write` to the `community` section, and you have to add a `view`. The view is defined in the `snmp`-section and limits the range of the permission to a subtree (given by a OID). E.g., by giving the OID `1`, you can define that the entire `iso` tree should be part of the view. As always, you can use `?` in the get and set commands to orient yourself.

Enable write access to the MIB variables by adjusting the access permissions in the SNMP configuration.

Now check the `sysLocation` on both routers. Validate using `snmpget`! Look at the router configuration and observe the change.

(k) Can you change the `ifAdminStatus` of `FastEthernet0/0` using `snmpset` on a Cisco? Does it work for Juniper, e.g., on `ge-0/0/0`? Compare with the MIB definitions you observed in h. Would it make sense to shut down an interface using SNMP?

Question 3: (5 Points) *And finally...*

We would like to know how you liked this lab course. What should be improved next time? Which worksheet was particularly hard or way too easy?

Of course, we will *not* rate the content of your comments. You can hand in a completed evaluation form at the Debriefing session next week, and claim your 5 points. The evaluation will then be carried out anonymously by a blind deaf monkey sitting in a black box locked away on a distant island... or something similar. We definitely won't hold your comments against you.

Thanks for participating and have a nice semester break!

For submission details please check the FAQ:
`http://www.net.t-labs.tu-berlin.de/teaching/ss08/RL_labcourse/`
Submit the following:

- All configuration inputs on routers, switches and loadgens (no trials, only the final ones)

- The outputs of all commands such as `ping`, `tcpdump`, `ifconfig` etc.

- The completed evaluation form (extra sheet)

Due Date: Friday, July 18th, 2008, 08:00 am