Laborator 1
SNMP

Introducere

SNMP (*Simple Network Management Protocol)* este un protocol de nivel aplicaţie, bazat pe UDP, cu rol în transmiterea de mesaje administrative între echipamentele de reţea (*agenţi SNMP*) şi unul sau mai multe *servere*.
Serverul este, tipic, un PC care rulează un soft de management (*NMS – Network Monitoring System*). Mesajele principale sînt:

- GET, dinspre server spre agent (cu varianta GET-NEXT), prin care se interoghează valoarea unei variabile. Tipic, în variabilele de pe agenţi se memorează valorile unor contoare care reprezintă traficul prin interfeţe, încărcarea, numărul de erori, etc
- GET-RESPONSE: Răspunsul la GET
- SET, dinspre server spre agent, pentru actualizarea unor informaţii de management şi chiar de configurare
- TRAP (cu varianta INFORM), mesaj "de urgenţă" dinspre agent spre server, prin care tipic acesta din urmă este informat despre apariţia unei schimbări sau, mai ales, a unei erori. Mesajele TRAP sînt unidirecţionale şi nu primesc răspuns de la server, de aceea agentul nu ştie dacă mesajul a ajuns sau nu. Mesajele INFORM sînt de acelaşi tip cu TRAP doar că serverul le confirmă (ceea ce este pozitiv din punct de vedere al siguranţei şi negativ din punct de vedere al traficului generat).

Schimbul de mesaje se face pe portul 161/UDP, cu excepţia mesajelor TRAP care se trimit pe 162/UDP.
Variabilele de pe agent, împreună cu o "hartă" ierarhică a acestora şi modul de acces la fiecare, formează un MIB *(Management Information Base*).

Alte aspecte SNMP:

- *SNMP community*: prezintă similitudini cu un domeniu Windows; toţi agenţii care sînt configuraţi în aceeaşi comunitate cu serverul pot fi interogaţi de către serverul respectiv (sau îi trimit mesaje TRAP). Ţine loc şi de parolă de acces. Exemple de comunităţi predefinite: *public, private*.
- Se pot întîlni următoarele versiuni de SNMP: v1, v2c, v3. Cea din urmă suportă şi autentificare prin metode mai avansate decît simpla parolă dată de *community*.

Desfăşurare; configurare; exerciţii

- Linux PC va avea rol de NMS (*Network Monitoring System)* folosind pachetul Net-SNMP (sau UCD-SNMP); de asemenea, pe PC va rula un agent care să informeze asupra traficului prin interfeţe.

- Ruterul Cisco va avea rol de *SNMP Agent*

Faza 1: Configurarea SNMP pe Linux

Se instalează şi configurează serverul şi clientul local de SNMP ca în [1]

```
sudo apt-get install snmpd
```

```
sudo apt-get install snmp
```

se modifică /etc/snmp/snmpd.conf
se comenteaza
com2sec paranoid default public
se decomenteza
com2sec readonly default public
com2sec readwrite default private

şi se restartează snmpd
sudo service snmpd restart

Cu acestea s-au instalat componentele SNMP.

Faza 2: Configurarea SNMP pe ruterul Cisco

Se configurează pe ruter numele acestuia, adresa interfeței care se conectează la PC, precum şi faptul că ruterul nu va ieşi automat din modul *enable* datorită timpului de inactivitate:

```
Router> enable
Router# conf t
Router(config)# hostname R0
R0(config)# line con 0
R0(config-line)# no exec-timeout

R0(config)# interface E0
R0(config-if)# ip address 192.168.1.1 255.255.255.0
R0(config-if)# no shutdown
```

OBSERVAȚIE: reamintim că pentru a întrerupe o comandă *ping, traceroute* etc care nu funcționează se va folosi secvența **CTRL-SHIFT-6**

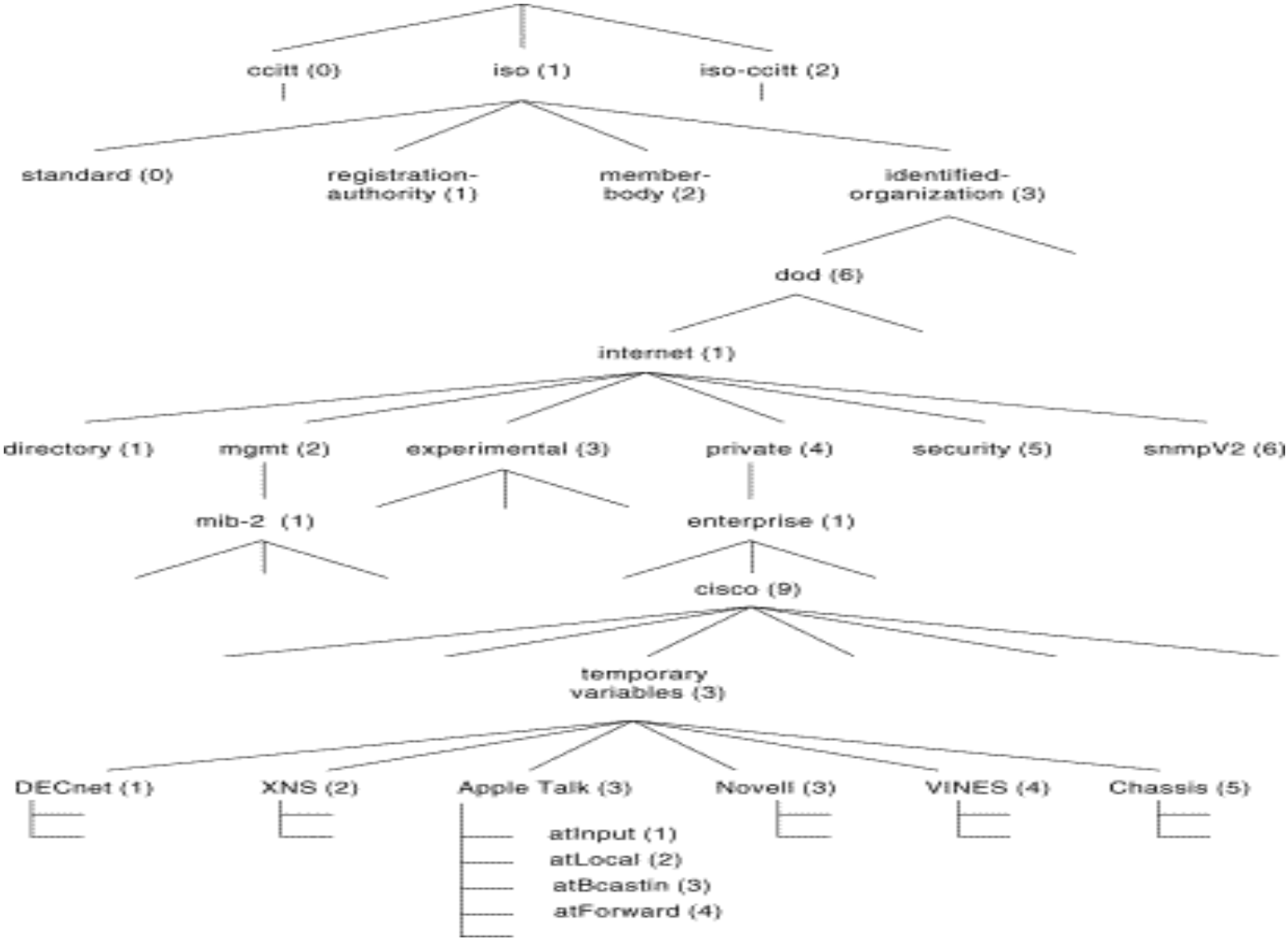
Se configurează cine va fi serverul SNMP (keyword *host*) şi comunitatea folosită:

```
R0(config)#snmp-server host 192.168.1.2 public tty config
snmp
R0(config)#snmp-server contact gigel
R0(config)#snmp-server chassis-id Cisco2500-1234

R0(config)#snmp-server community public ro
R0(config)#snmp-server community private rw
```

“public” şi “private” sînt comunitățile, cu rol de parole; pot fi înlocuite cu orice, acestea sînt valorile implicite (şi nerecomandate dacă se doreşte securitate). Aceleaşi parole trebuie scrise şi în /etc/snmpd/snmpd.conf, deci, în cazul nostru, nu se vor schimba !
RO/RW se referă la drepturi: *Read-Only* / *Read-Write*. Comunitatea *private* va fi folosită mai tîrziu (permite modificări pe ruterul Cisco prin SNMP).

Se va examina valoarea pentru diferite OID (Object Identifiers) din MIB. Denumirea acestora este standardizată la nivel global, ca în figură; fiecare producător îşi defineşte OID-urile în categoria 1.3.6.1.4 (private).



De pe PC se va folosi *snmpwalk* pentru inspectarea variabilelor OID:

snmpwalk –v1 –c public 192.168.1.1 1.3.6.1.4.1.9.2.1 pt un grup de variabile
snmpwalk –v1 –c public 192.168.1.1 1.3.6.1.4.1.9.2.1.73 pt numele imaginii
snmpwalk –v1 –c public 192.168.1.1 1.3.6.1.4.1.9.2.1.8 pt free RAM
snmpwalk –v1 –c public 192.168.1.1 1.3.6.1.4.1.9.2.1.57 pt CPU use

De pe ruter:

```
R0# show snmp
```

arată toate pachetele SNMP trimise de ruter, precum şi tipul acestora.

Faza 3 configurarea MRTG pe Linux

Se instalează o variantă populară de software NMS cu reprezentare grafică, numită MRTG (*Multi Router Traffic Grapher*).

```
Sudo apt-get install mrtg
```

se creaza directorul radacina web al MRTG:
sudo mkdir /var/www/mrtg
se genereaza fisierul de configurare pentru mrtg (se completeaza adresa ip a routerului Cisco):
sudo cfgmaker --global 'WorkDir: /var/www/mrtg' --output /etc/mrtg.cfg public@141.85.43.5
se genereaza fisiserul index ce contine toate interfetele:
indexmaker /etc/mrtg.cfg --columns=1 --output /var/www/mrtg/index.html

Se va lansa mrtg, se va deschide pagina de web în care scrie acesta (tipic, http://127.0.0.1/mrtg) şi se vor urmări statisticile. Tipic, durează cam 10-15 minute ca să se strîngă suficiente statistici. Se recomandă să se pornească un ping între PC şi ruter pentru a genera trafic pe interfaţa ruterului.

Faza 4: Activarea SNMP Traps pe ruterul Cisco

```
snmp-server host 192.168.1.2 traps public tty config snmp
```

unde după numele comunităţii se specifică acele categorii de *traps* care se doresc.
Se activează manual trimiterea de *traps*:

```
snmp-server enable traps
```

Pe PC:

Se activează (dacă nu e activ deja) serverul care recepţionează traps: snmptrapd. Poate fi necesară editarea fişierului de configurare /etc/snmp/snmptrapd.conf

Se vizualizează în continuu, din alt terminal, fişierul de log (unde se scriu diverse evenimente, inclusiv SNMP traps)

```
tail –f /var/log/syslog
```

Faza 5: Modificarea de informaţii pe ruter folosind SNMP

Pînă acum, SNMP a fost folosit doar pentru interogare. Comunitatea *public* fiind read-only, nici nu poate fi folosită în alt scop. Pentru a modifica valori se foloseşte comunitatea read-write pe care am numit-o *private*.
Vom experimenta resetarea ruterului de la PC, scriind o valoare specifică Cisco în MIB.

Pe Cisco se definesc următoarele:

```
R0(config)#snmp-server host 192.168.1.2 private
R0(config)#snmp-server system-shutdown
```

Se salvează configuraţia folosind `copy run start`, căci ruterul se va reseta !

Pentru a transmite comanda de resetare de pe PC, se dă următoarea comandă (-v 2c specifică versiunea 2c de SNMP; -c specifică numele comunităţii):

```
snmpset -v 2c -c private 129.174.3.10 .1.3.6.1.4.1.9.2.9.9.0 i 2
```

Ruterul ar trebui să se reseteze (*reload*). În terminalul care rulează tail –f /var/log/syslog se pot vedea mesajele *trap* pe care ruterul le trimite cînd se iniţializează.

Bibliografie

[1] www.debian-administration.org/articles/366
[2] http://www.aboutdebian.com/monitor.htm
[3] informaţie configurare SNMP pe Cisco: se găseşte direct pe www.cisco.com