

# Monitoring mrežnih uređaja pomoću SNMP protokola

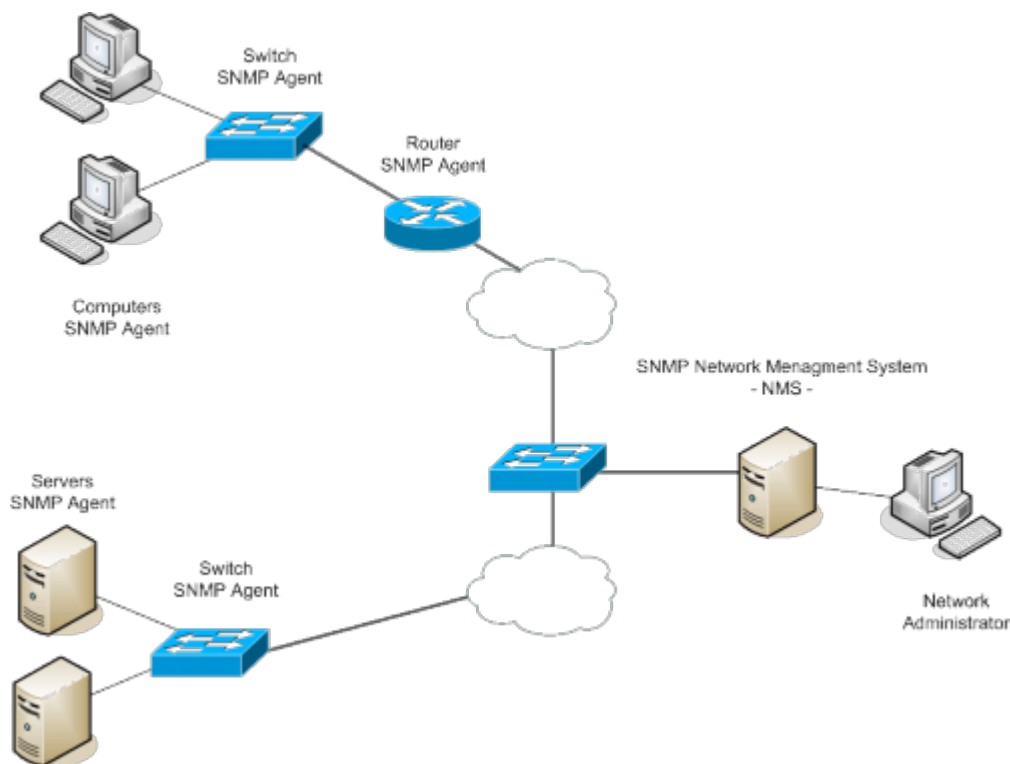
## Uvod:

Cilj ovog dokumenta je da uputi čitaoca u osnovne mehanizme funkcionisanja monitoring-a mreže pomoću SNMP-a kao i u ispravan način podešavanja SNMP-a u mreži sa stanovišta sigurnosti. Opisan je opšti princip rada sa SNMP promenjivim vrednostima kao i tipovi promenjivih sa kojima se korisnici mogu susretati. U dokumentu su dati primeri pokretanja SNMP-a verzije V2c i V3 na raznim mrežnim uređajima. Opisani su razni primeri očitavanja parametara sa udaljenih uređaja pomoću programa koji se koriste za testiranje SNMP agenata. Ovaj dokument je namenjen svim administratorima koji žele na ispravan način da pokrenu SNMP protokol u mreži a žele da očuvaju privatnost i sigurnost mreže koju nadgledaju.

## SNMP protokol

### Opšte karakteristike SNMP-a

Razvoj mrežnih uređaja i novih kompleksnih protokola doveo je do toga da se današnji mrežni sistemi ne mogu održavati bez dobrog programa za nadzor, kontrolu i konfigurisanje mreže. Dosta današnjih mrežnih sistema se oslanja na monitoring pomoću SNMP protokola. Sam SNMP protokol je dizajniran tako da veoma malo opterećuje mrežu. Naziva se prostim protokolom zato što koristi proste (nestrukturirane) tipove podataka. Ovaj protokol aplikativnog nivoa OSI modela sastavni je deo TCP/IP steka protokola. Sastoji se od skupa standarda kojima se definišu: način upravljanja mrežom, baze podataka za čuvanje informacija i strukture korišćenih podataka. Oslanja se na UDP, mada je moguće podesiti i rad preko TCP-a, što nije preporučljivo u velikim mrežama. Monitoring mrežnih uređaja pomoću SNMP-a se obično vrši tako što se na mrežnom uređaju pokrene SNMP agent i to tako da odgovara na periodične zahteve koje dobija od servera koji prikuplja podatke (NMS Server). SNMP agent saznaje od uređaja informacije neophodne za upravljanje, prevodi ih u oblik koji propisuje SNMP, u tom obliku ih prosleđuje NMS-u. U slučaju kada dođe do neke bitne promene na uređaju SNMP agent generiše SNMP Trap poruku i na taj način se brzo, bez čekanja na upit od NMS-a, obaveštava NMS o promeni u mreži. SNMP agent osluškuje upite po UDP portu 161, a Trap-ove šalje po UDP portu 162, tako da prilikom pokretanja monitoringa u mreži potrebno je da se omogući komunikacija između mrežnih uređaja i NMS servera po ovim portovima (access lists, IP tables ....).



Slika 1 - Monitoring pomoću SNMP-a

## Tipovi Podataka

Informacije koje se mogu očitati sa udaljenog uređaja su definisane u MIB (Management Information Base) bazi podataka. U MIB bazi su varijable hijerarhijski definisane u formi stabla, i te varijable sam proizvođač uređaja kreira. Svaka od ovih varijabli u MIB bazi je jednoznačno određena svojim OID (Object Identifier) identifikatorom. Postoje i univerzalne varijable koje su definisane na svim mrežnim uređajima. Rad sa ovim varijablama će biti opisan pojedinačno za svaki uređaj.

Tipovi podataka su podeljeni u dve grupe:

- Prosti tipovi podataka
- Aplikativni tipovi podataka

Tipovi podataka su nasleđeni od SNMP V1 i za V2c i V3 su samo dodati novi tipovi.

- Prosti tipovi podataka
  - Celobrojni tip - ( $-2^{31} \sim 2^{31}-1$ )
  - String okteta - (0~65535)
  - ObjectID - (OID vrednost)
- Aplikativni tipovi podataka
  - Adrese mreže - IPv4 i IPv6 adrese mreže
  - Brojači - (V2c i V3 podržavaju 64-bitne brojače dok V1 samo 32-bitne) Brojači vrše inkrement svog stanja sve dok ne dođu do maksimalne vrednosti kada se resetuju u početno nulto stanje.

- Meraži - (Mogu menjati stanje u okviru nenegativne minimalne i maksimalne vrednosti) U slučaju da prekorače granične vrednosti meraži se zadržavaju u tom graničnom stanju.
- Zabeleženi trenutak - Predstavlja trenutak od odigravanja nekog događaja izražen u stotim delovima sekunde.
- Pokrivanje - Predstavlja proizvoljno kodiranje koje pruža fleksibilnost zato što omogućuje proširivanje tipova podataka u formi stringa koji nisu striktno definisani u SMI.
- Celobrojne označene vrednosti
- Celobrojne neoznačene vrednosti (Nenegativne)

Za svaku OID vrednost se definiše tip dostupnosti i tip može biti:

- Read (Varijabla se može samo očitati)
- Read-Write (Varijabla se može očitati ali joj se može i promeniti vrednost)

Veoma je bitno proučiti tip vrednosti koju SNMP agent vraća. Zato je u MIB bazi podataka za svaku OID vrednost definisan tip podatka kao i opis tog tipa podatka, odnosno šta on predstavlja.

## Razvoj SNMP-a

Razvoj SNMP protokola se ogleda kroz tri verzije i danas je najzastupljenija druga verzija, SNMP V2c. Usled potrebe za implementaciju sigurnosti u mreži razvijena je SNMP V3 koja uvodi autentifikaciju i enkripciju.

SNMP V2c (RFC 1901-1908) Kod verzije 2c se autentifikacija vrši pomoću community stringa i on se šalje u istom tekstu preko mreže. U slučaju da neko "uhvati" ovaj saobraćaj pomoću neke sniffing aplikacije, može vrlo lako otkriti community string i na taj način biti u mogućnosti da ugrozi ispravan rad mreže.

SNMP V3(RFC 3411-3418) SNMPv3 pruža tri važna servisa: autentifikaciju, privatnost i kontrolu pristupa. SNMPv3 uvodi važne bezbednosne aspekte:

1. Integritet poruke (Message integrity), sprečava mogućnost izmene paketa prilikom prenosa
2. Autentifikacija, potvrda da je poruka stigla sa pravog izvorista
3. Kriptovanje paketa, sprečavanje čitanja poruka od strane neautorizovanog izvora

U tabeli 1 je dat prikaz verzija SNMP-a sa stanovišta sigurnosti u mreži.

SNMP Security modeli i nivoi				
Model	Nivo	Autentifikacija	Enkripcija	Princip rada
v1	noAuthNoPriv	Community String	-	Koristi Community string za autentifikaciju.
v2c	noAuthNoPriv	Community String	-	Koristi Community string za autentifikaciju.
v3	noAuthNoPriv	Username	-	Koristi Username za autentifikaciju.
v3	authNoPriv	MD5 ili SHA	-	Autentifikacija se bazira na HMAC-MD5 ili HMAC-SHA algoritmu. Umesto password-a se šalje MD5 ili SHA hash

v3	authPriv	MD5 ili SHA	DES	Autentifikacija se bazira na HMAC-MD5 ili HMAC-SHA algoritmu. Omogućuje DES 56-bitnu enkripciju u okviru autentifikacije baziranu na CBC-DES (DES-56) standardu.
----	----------	-------------	-----	--

Tabela 1 - Prikaz verzija SNMP-a sa stanovišta sigurnosti u mreži.

Iz tabele se vidi fleksibilnost SNMP V3 protokola u izboru nivoa sigurnosti u mreži. U daljem tekstu će biti opisana implementacija SNMP V2c i SNMP V3 na raznim mrežnim uređajima.

## Pokretanje SNMP-a na raznim tipovima uređaja

### CISCO Ruter

Pomoću sledeće komande, koja se koristi u konfiguracionom modu, pokreće se SNMP agent na ruteru.

```
SNMPTEST(config)#snmp-server community publicro ro acl10
```

String koji se koristi kao autentifikacija publicro predstavlja vid zaštite tako da će ruter odgovoriti samo onom uređaju koji mu pošalje zahtev koji sadrži baš ovaj string. Opcija ro na naglašava da je moguće samo očitati podatke a ne i menjati ih (ro-read only). Takođe je moguće i menjati pojedine varijable (wr-write komanda) što može dovesti do promene rada rutera (restart rutera), zato je veoma bitno da se ne koriste default-ne vrednosti za community string i da se SNMP upiti ograniče samo na mogućnost očitavanja a ne i menjanja varijabli. Konačno na kraju komande je definisana access lista acl10 pomoću koje se može definisati pristup SNMP agentu na uređaju samo sa određenih ip adresa.

Da bi se ispravno podesio i snmp trap mod rada potrebno je definisati community string za trap mod, pokrenuti SNMP-trap i definisati destination adresu na koju će se slati trap poruke.

```
1.SNMPTEST(config)#snmp-server enable traps
```

```
2.SNMPTEST(config)#snmp-server host myNMSserver.com version 2c publicro
```

U ovom primeru je definisana verzija 2c SNMP protokola. Da bi se uvela sigurnost u monitoring mreže koristi se SNMP V3 protokol. Pomoću sledećih komanda se pokreće SNMP V3 protokol na Cisco uređajima.

```
1.SNMPTEST(config)#snmp-server view MYGROUPV interfaces included
```

```
2.SNMPTEST(config)#snmp-server group MYGROUP v3 auth read MYGROUPV
```

```
3.SNMPTEST(config)#snmp-server user peraperic MYGROUP v3 auth md5 perapass priv  
des56 pera1234
```

```
4.SNMPTEST(config)#snmp-server enable traps
```

```
5.SNMPTEST(config)#snmp-server host 192.168.10.1 version 3 auth MYGROUP
```

U prvoj komandi se definišu vrednosti u MIB bazi OID-ova koji mogu biti očitani sa uređaja. U ovom slučaju je omogućeno očitavanje OID-a (interface) koji opisuju stanje interfejsa na uređaju. Ako se ne definiše ovakva grupa pretpostavlja se da je dozvoljen pogled na sve vrednosti u MIB bazi. Druga komanda definiše grupu MYGROUP koja koristi SNMP V3 protokola i koja koristi autentifikaciju. Ova grupa ima mogućnost očitavanja podataka iz MIB baze i to samo onih koji su definisani u "pogledu" MYGROUPV. Treća komanda definiše korisnika peraperic koji pripada grupi MYGROUP koji koristi SNMP V3, autentifikaciju pomoću md5 algoritma i ima password perapass. Poslednjom opcijom u komandi 3 "pera1234" se definiše passphrase koja se koristi za enkripciju SNMP saobraćaja. Četvrta komanda pokreće SNMP Trap mod rada. Peta komanda definiše NMS server koji će prikupljati trap poruke. U ovom slučaju prilikom komunikacije između NMS i Cisco uređaja koristi se SNMP V3 i pravila koja su definisana pomoću grupe MYGROUP. Provera izvršavanja SNMP upita se može uraditi direktno sa NMS servera. U slučaju Linuxa to je moguće uraditi sledećom komandom.

```
snmpwalk -v 3 -u peraperic -l authPriv -a MD5 -A perapass -x DES -X pera1234 CiscoIPadd
```

Kao rezultat ove komande dobije se tabela koja opisuje stanje interfejsa na Cisco uređaju.

Korišćenje enkripcije saobraćaja dosta opterećuje resurse uređaja (Procesor i Memoriju) tako da pojedini uređaji nemaju implementiran modul za enkripciju. Takvi uređaji ne podržavaju SNMP V3. U sledećoj listi je dat spisak Cisco platformi koje podržavaju SNMP V3.

•Cisco 700 series
•Cisco 1000 series
•Cisco 1600 series
•Cisco 2500 series
•Cisco 2500 series access servers
•Cisco 3600 series
•Cisco 3800 series
•Cisco 4000 series
•Cisco 4500 series
•Cisco AS5100 access server
•Cisco AS5200 universal access server
•Cisco AS5300 access server
•Cisco 7000 series
•Cisco 7200 series
•Cisco 7500 series

Preko SNMP-a se najčešće monitorišu OID vrednosti koje opisuju stanje interfejsa na uređaju i OID vrednosti koje opisuju stanje memorije i procesora uređaja, mada je moguće monitoring i ostalih parametara od interesa. Obično svaki proizvođač opreme definiše svoje OID vrednosti koje opisuju ove parametre. U Tabeli 1 je dat primer očitavanja ifTable (.1.3.6.1.2.1.2.2 ) OID tabele. Ove OID vrednosti se često koriste i svi tipovi mrežnih uređaja ih moraju podržavati.

<b>ifTable - Tabela koja opisuje trenutno stanje svih interfejsa</b>			
<b>ifType</b>	6	6	1

<b>ifMtu</b>	1500	1500	1500
<b>ifSpeed</b>	100000000	100000000	4294967295
<b>ifPhysAddress</b>	c8 00 08 c4 00 00	c8 00 08 c4 00 01	-
<b>ifAdminStatus</b>	up(1)	down(2)	up(1)
<b>ifOperStatus</b>	up(1)	down(2)	up(1)
<b>ifLastChange</b>	0 hours, 4 minutes, 17 seconds.	0 hours, 0 minutes, 9 seconds.	0 hours, 0 minutes, 0 seconds.
<b>ifInOctets</b>	939	0	0
<b>ifInUcastPkts</b>	3	0	0
<b>ifInNUcastPkts</b>	8	0	0
<b>ifInDiscards</b>	0	0	0
<b>ifInErrors</b>	0	0	0
<b>ifInUnknownProtos</b>	0	0	0
<b>ifOutOctets</b>	5525	0	0
<b>ifOutUcastPkts</b>	25	0	0
<b>ifOutNUcastPkts</b>	12	0	0
<b>ifOutDiscards</b>	0	0	0
<b>ifOutErrors</b>	0	0	0
<b>ifOutQLen</b>	0	0	0
<b>ifSpecific</b>	.0.0	.0.0	.0.0

Tabela 1 - ifXTable

U Cisco menadžment modulu .1.3.6.1.4.1.9.9 mogu se naći OID-ovi od interesa za nadzor nad Cisco uređajima.

## SERVERI

### Linux Server

#### LINUX Server (SNMP V2c)

U slučaju podešavanja SNMP protokola na Linux operativnim sistemima prvo je potrebno instalirati SNMP deamona na server. U sledećem primeru biće opisana instalacija na CentOS 5.3 operativnom sistemu pomoću YUM komande. Sledeća komanda omogućuje automatizovanu instalaciju SNMP deamona i korisnih komandi za kontrolu rada SNMP-a.

```
yum install net-snmp net-snmp-utils
```

Sledeći korak je podešavanje servisa da se automatski pokrene prilikom startovanja servera. Potrebno je uneti sledeću komandu.

```
chkconfig snmpd on
```

Sledeća stavka je podešavanje community stringa i OID objekata koji mogu biti očitani sa servera.

Potrebno je editovati fajl `snmpd.conf` koji se obično nalazi u direktorijumu `/etc/snmp/` i izmeniti sledeće redove. U redu

```
com2sec notConfigUser default public
```

potrebno je promeniti defaultni community string `public` u željeni community string.

U redu:

```
view systemview included .1.3.6.1.2.1.1
```

se vidi da su uključeni svi OID-ovi koji se nalaze ispod čvora `.1.3.6.1.2.1.1` u MIB drvetu. Pomoću komande `excluded` moguće je isključiti pojedine OID vrednosti, odnosno uvesti ograničenja u prikazu MIB baze. Ovde je potrebno definisati OID vrednosti koje će server vraćati kao odgovor na SNMP upite. Ako NMS zatraži OID koji nije ovde definisan server neće odgovoriti NMS-u. U slučaju da želimo da omogućimo očitavanje svih OID vrednosti potrebno je uneti sledeći red:

```
view systemview included .1
```

Na taj način su uključene sve vrednosti koje se nalaze ispod čvora `.1` u MIB stablu, odnosno celo stablo.

Sada je potrebno pokrenuti servis sledećom komandom:

```
service snmpd start
```

Proveru je moguće uraditi pomoću sledeće komande:

```
snmpwalk -v 2c -c mojcommunity 127.0.0.1
```

Kao rezultat će se prikazati cela MIB tabela (drvo), ili deo MIB tabele, koji je definisan prethodnim komandama za ograničenje prilikom očitavanja MIB baze.

### LINUX Server (SNMP V3)

Instalacija SNMP V3 agenta je ista kao za prethodnu verziju 2c, samo je sada potrebno pokrenuti verziju SNMP V3. Potrebno je editovati fajl `snmpd.conf`, i dodati sledeće komande.

```
syslocation MojGradiliLokacija  
syscontact mojemail@provajder.com  
view mojpogled included .1.3.6.1.2.1.2.2  
createUser john MD5 john1234 DES john5678
```

**rouser john priv -V moj pogled**

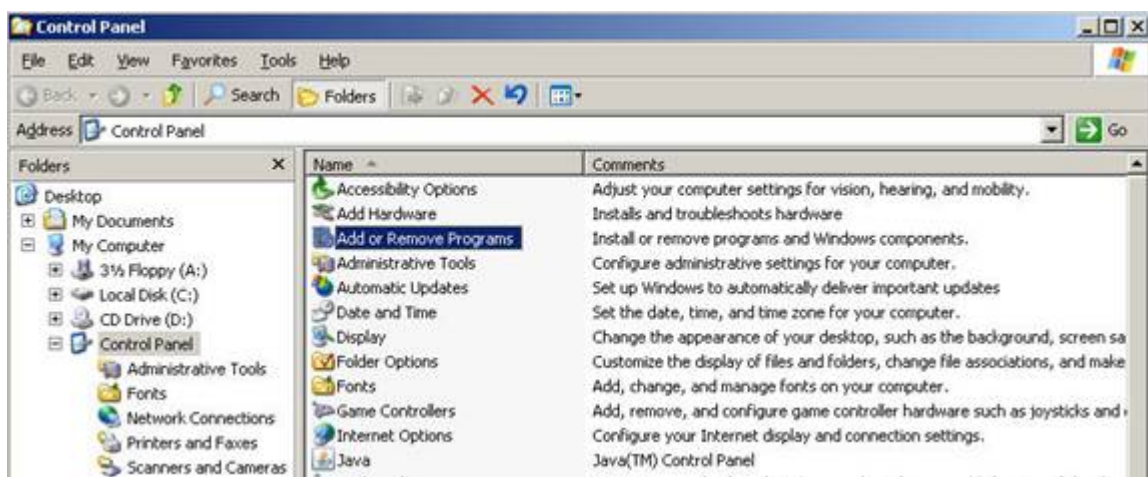
Prva dva parametra, *syslocation* i *syscontact* su podaci koji služe da daju opšte informacije o serveru. Oni nisu značajni za ispravan rad SNMP protokola ali su bitni za administratore servera koji će imati pored osnovnih informacija o stanju servera i informaciju o lokaciji servera i kontakt osobi kojoj se mogu obratiti u slučaju pojave problema. *Syslocation* i *Syscontact* su neki od parametara koji se mogu naći na svim uređajima koji podržavaju SNMP protokol. Treći red definiše pogled, odnosno skup OID vrednosti iz MIB stabla. U ovom slučaju je definisana tabela interfejsa servera. Moguće je dodati više tabela ili pomoću komande *exclude* isključiti neke OID vrednosti. Ova ograničenja su veoma bitna zato što je pomoću SNMP-a moguće i postaviti neke parametre a to direktno može uticati na ispravan rad uređaja. Četvrta komanda kreira user-a john čiji je password john1234. Prilikom autentifikacije koristi se MD5 algoritam, a saobraćaj je enkriptovan pomoću DES algoritma. Passphrase koji se koristi prilikom enkripcije je john5678. Peta komanda user-u john daje read only (rouser) privilegije i to samo nad moj pogled pogledom na MIB bazu koji je definisan u trećoj komandi. Provera podešavanja SNMP V3 na serveru je moguća pomoću komande:

```
snmpwalk -v 3 -u john -l authPriv -a MD5 -A john1234 -x DES -X john5678 serveripaddr
```

**Windows 2000 Server**

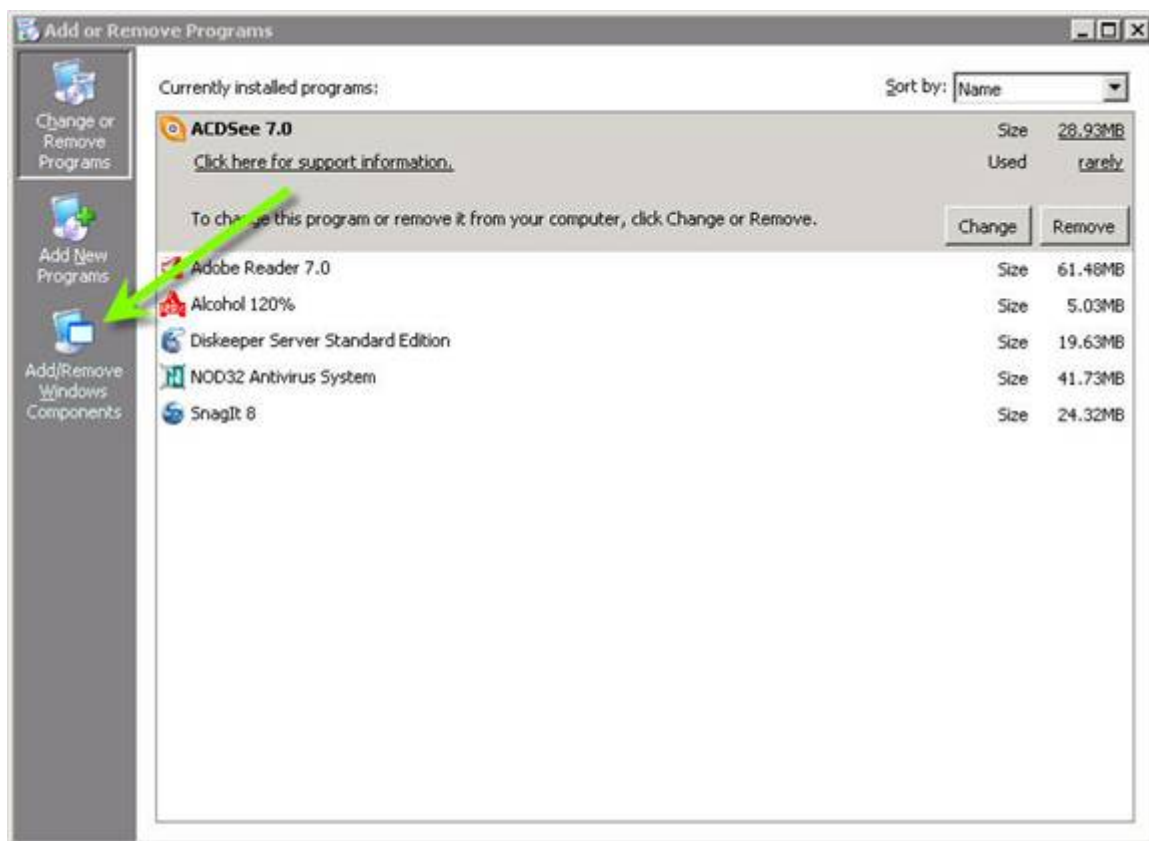
1. Potrebno je biti ulogovan kao Administrator na računaru na kom se instalira SMTP.

1. Kliknuti na **Start**, zatim **Control Panel** pa **Add or Remove programs**.

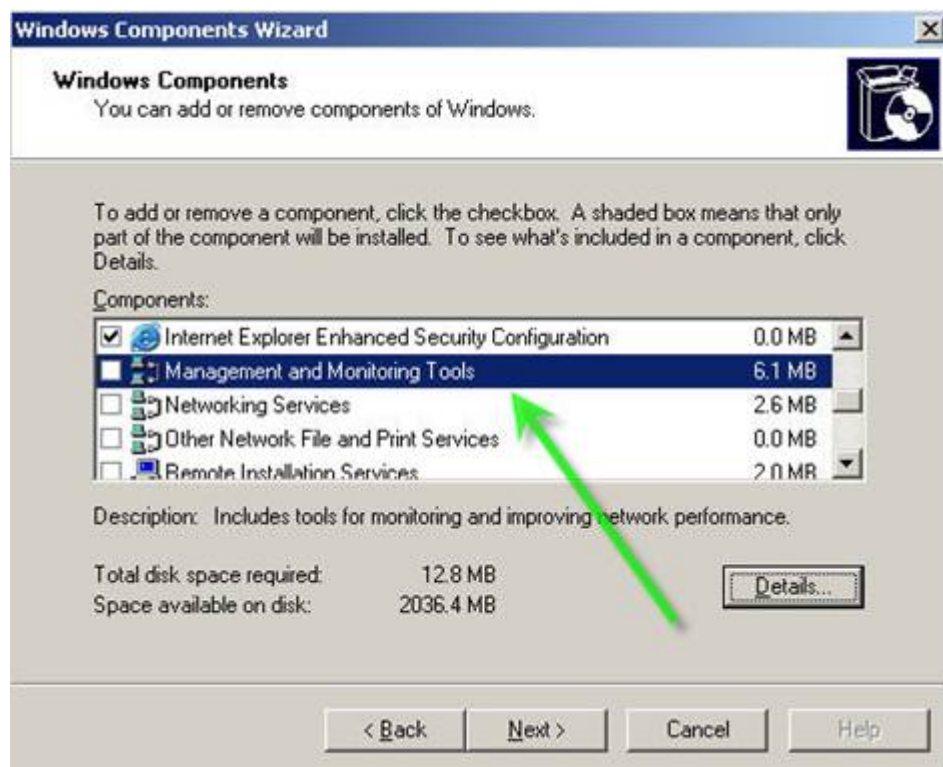


1. Zatim izabrati **Add or Remove Windows Components**.



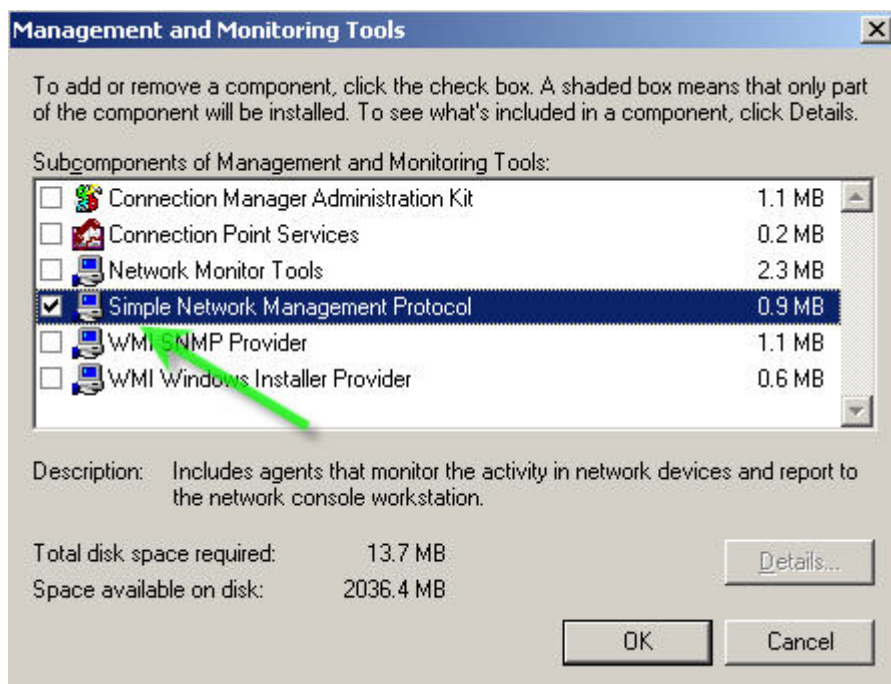


1. U otvorenom prozoru **Windows Components wizard**-a selektovati (ne štiklirati) **Management and Monitoring Tools**, a zatim na **Details** (dok je **Management and Monitoring Tools** selektovan plavom bojom).



1. U otvorenom prozoru **Management and Monitoring Tools** štiklirati **Simple Network**

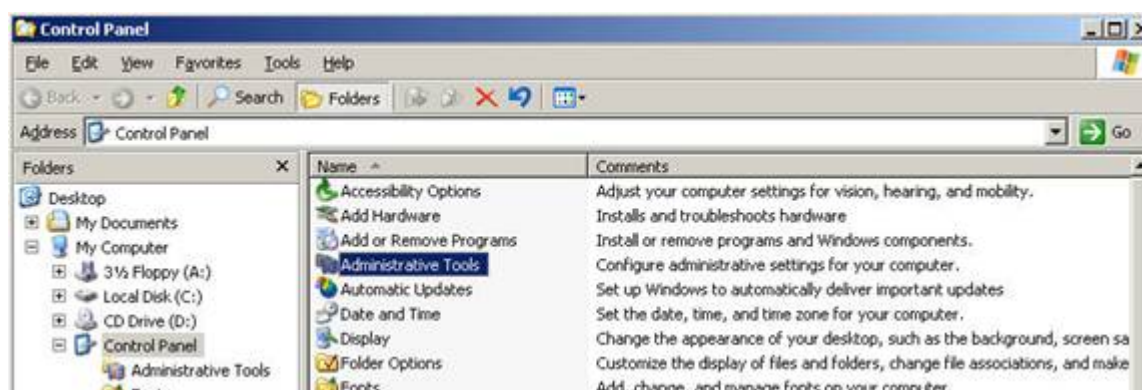
## Management Protocol pa OK.



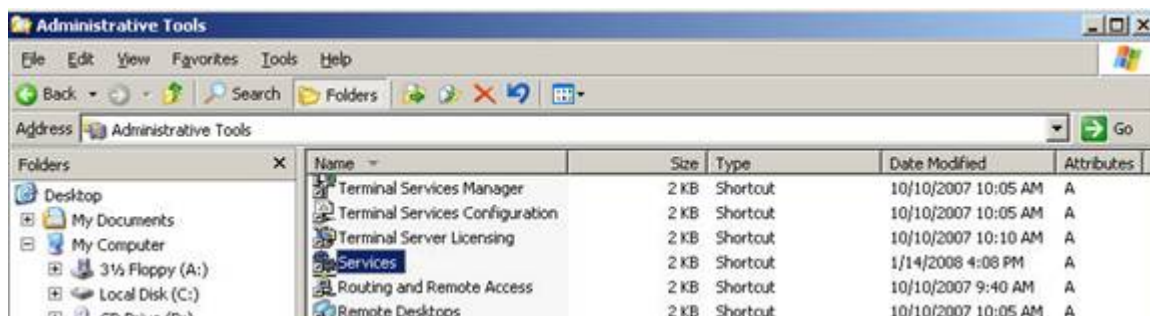
Za ispravnu instalaciju SNMP protokola potreban je instalacioni disk instalirane verzije Windows server 2003 koga treba staviti u CD citac. Zatim u prozoru **Windows Components wizard**-a kliknuti na **Next** i pratiti korake instalacije.

## Konfiguracija SNMP Agenta

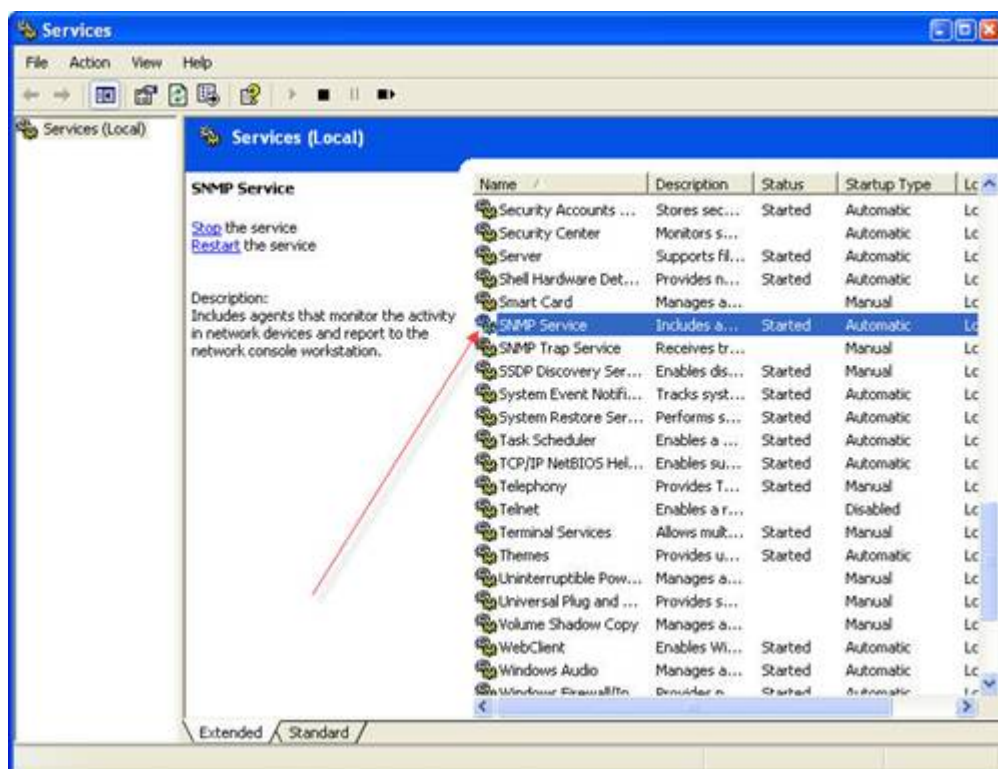
1. Otvoriti **Control Panel**, pa kliknuti na **Administrative Tools**

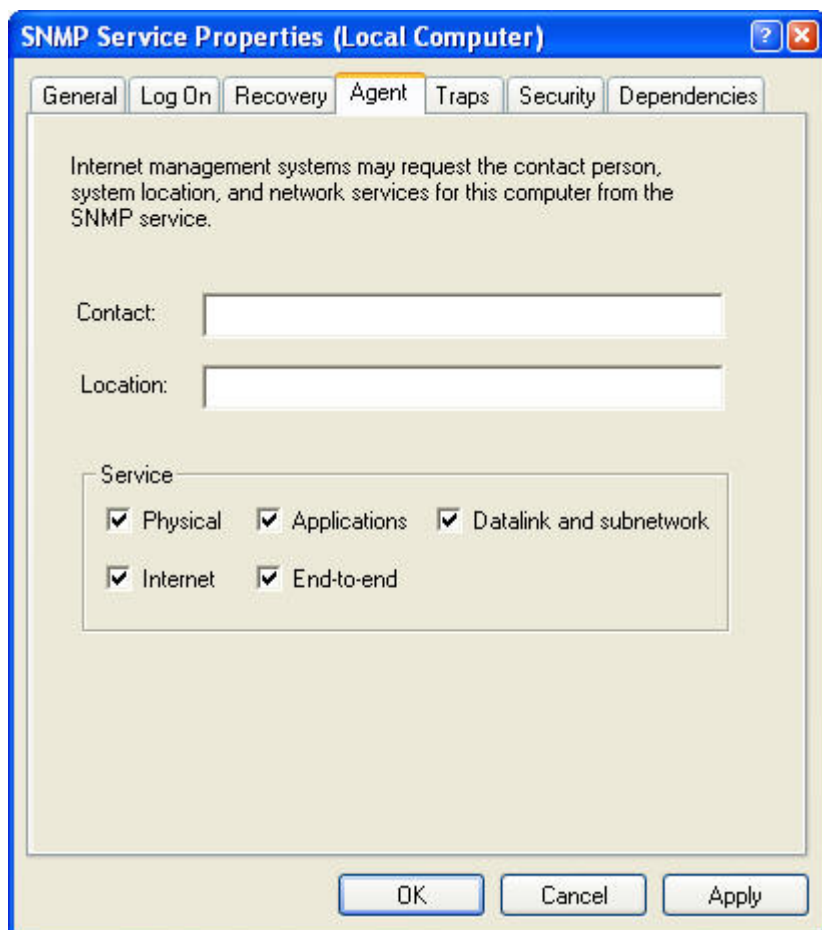


1. Otvoriti polje **Services**



1. U desnom panelu dva puta kliknuti na **SNMP Service** a posle otvoriti karticu **Agent**.



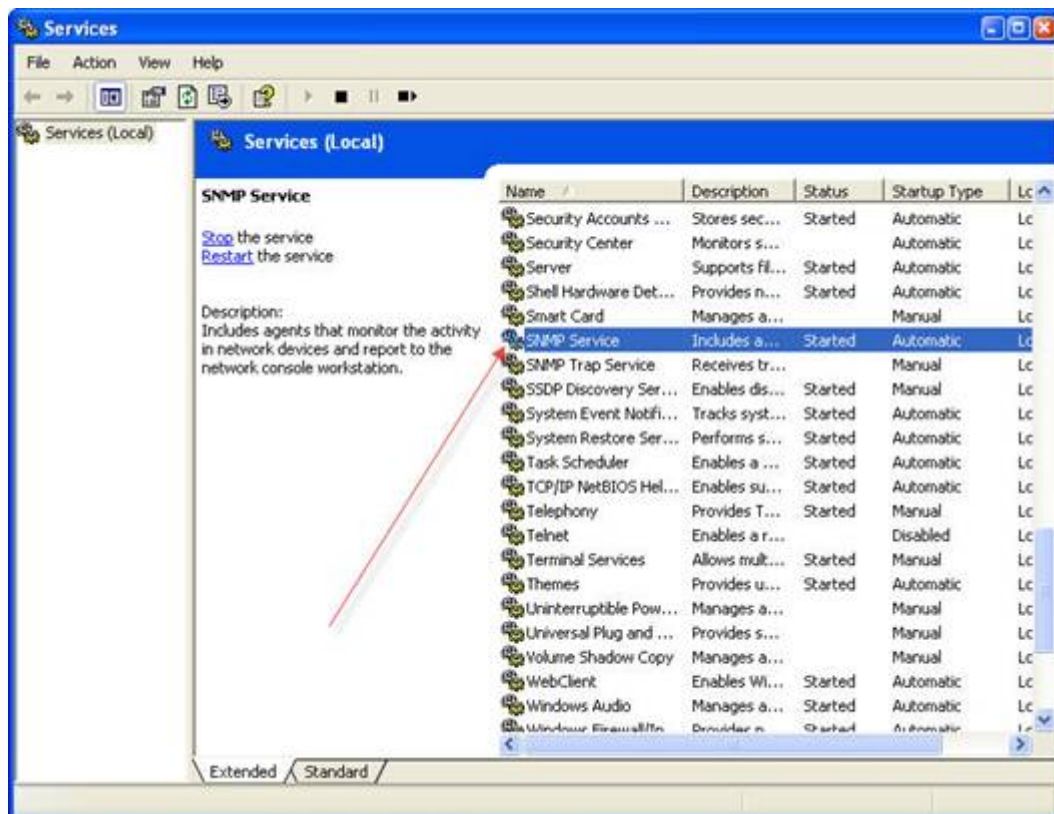


1. Upisati u polju **Contact** e-mail adresu administratora zaduženog za održavanje servera, a u polju **Location** fizicku lokaciju racunara ili kontakta.
2. U polju **Service** treba štiklirati sve servise kao na slici prikazanoj gore. To su:

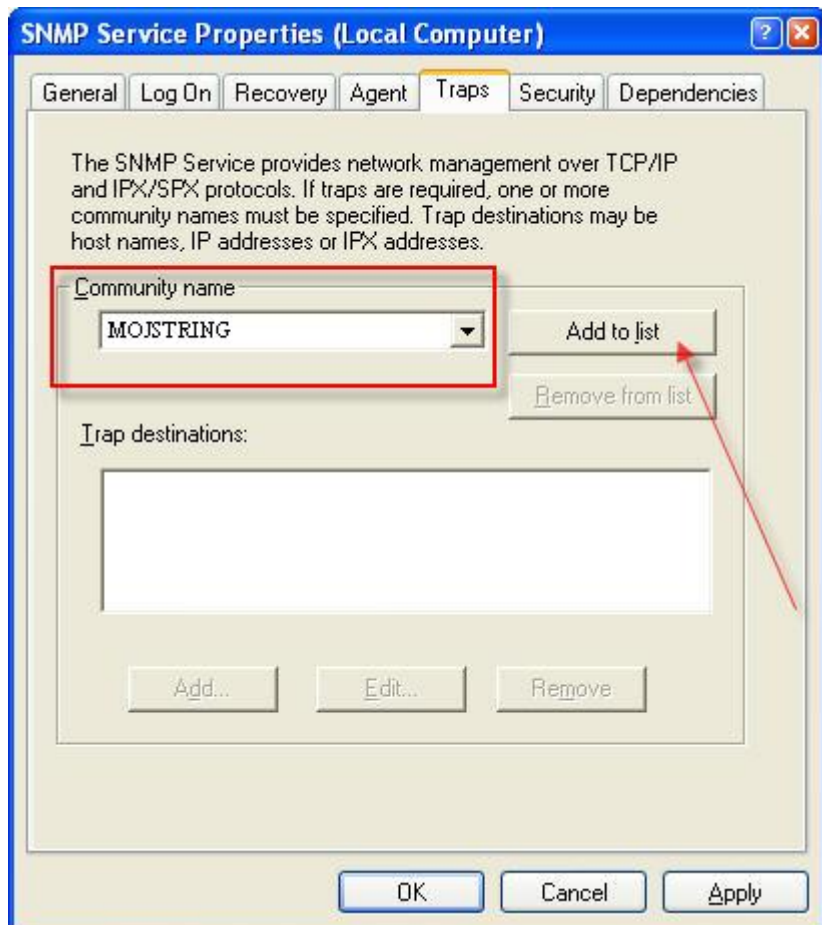
**Po konfigurisanju kliknuti na OK.**

#### **Konfigurisanje Community grupe i Trap-ova**

1. Otvoriti **Control Panel**, pa kliknuti na **Administrative Tools** .

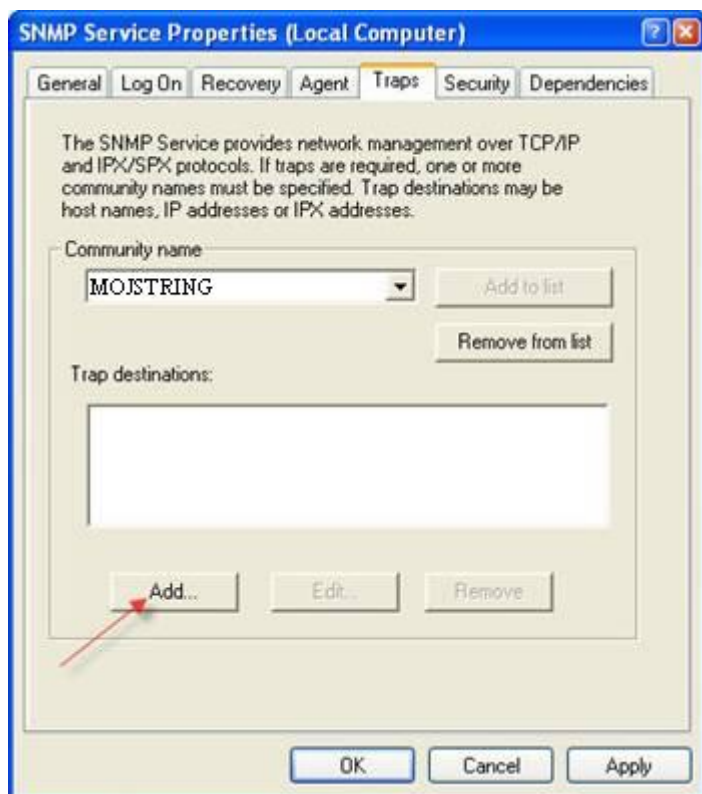


# 1. Otvoriti polje **Services**.

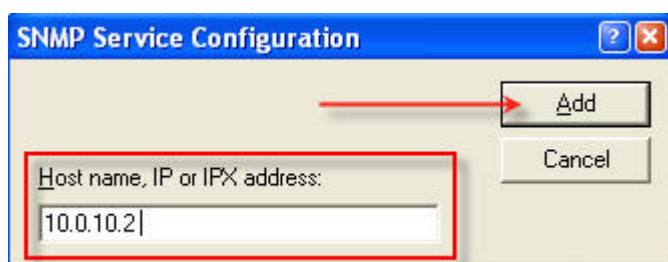




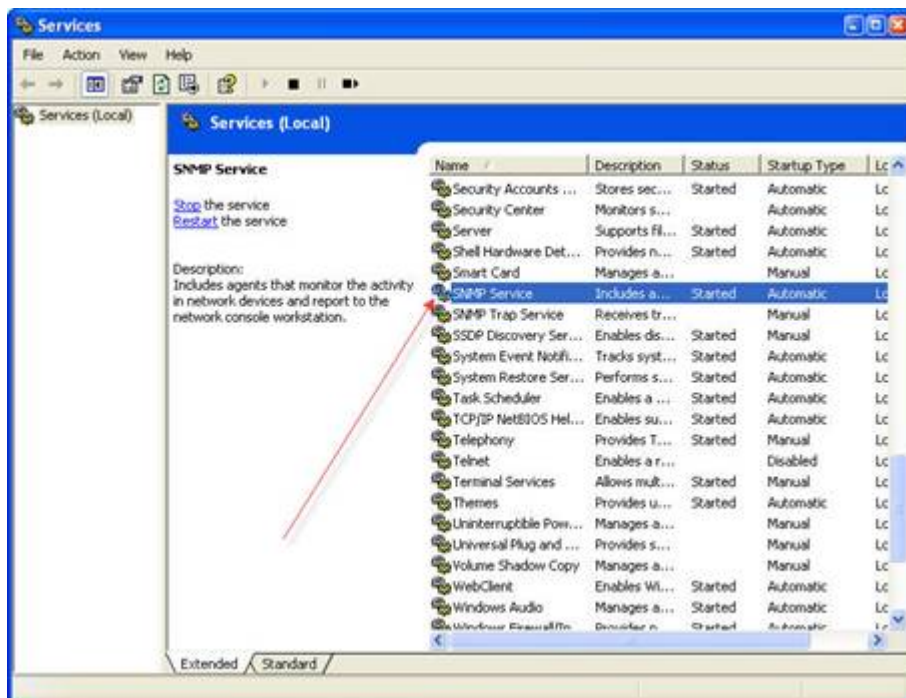
1. U desnom panelu dva puta kliknuti na **SNMP Service**.



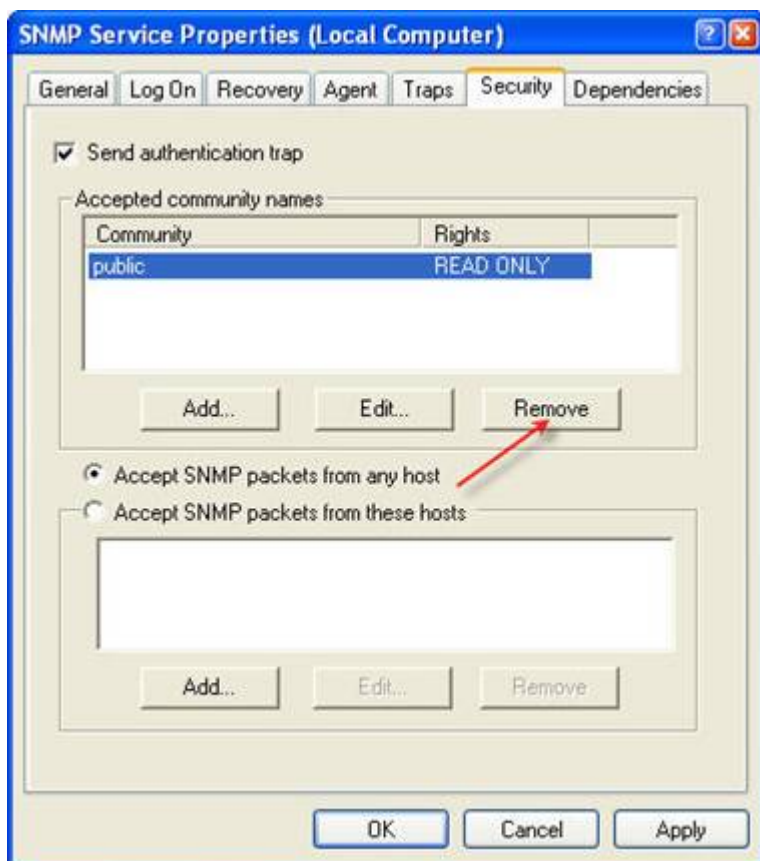
1. Posle otvaranja na kartice **Traps**, u polju **Community name** upisati **Community string**, koji će biti naknadno dostavljen administratorima (Community string "MOJSTRING" je primer i ne treba ga koristiti), a zatim kliknuti na **Add to List**



- Zatim kliknuti na **Add**, u odeljku **Trap destinations**.



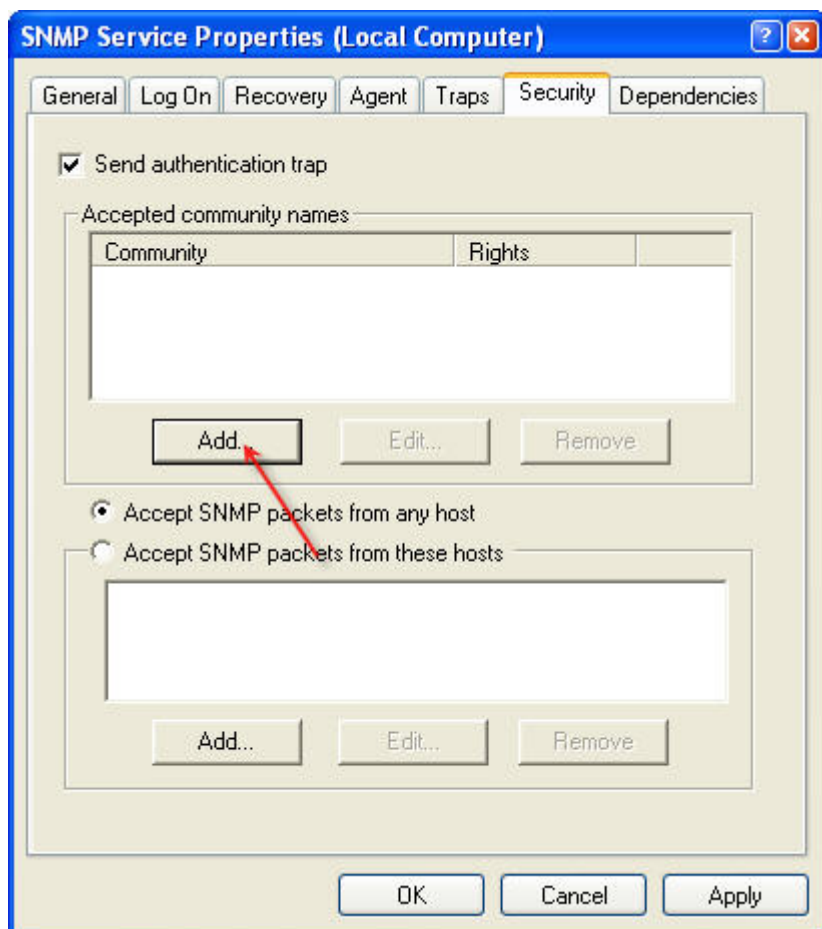
- U polju Host name, IP or IPX address upisati IP adresu 10.0.10.2 kliknuti Add.



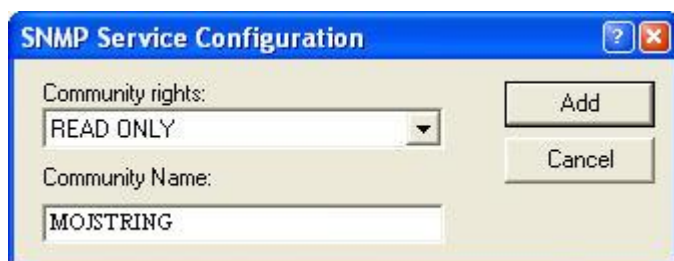
Upisano ime ili adresa hosta pojaviće se u Trap destinations listi. - Kliknuti OK na kraju..

Konfiguracija SNMP bezbednosti na serverima

1. Otvoriti **Control Panel**, pa kliknuti na **Administrative Tools** .

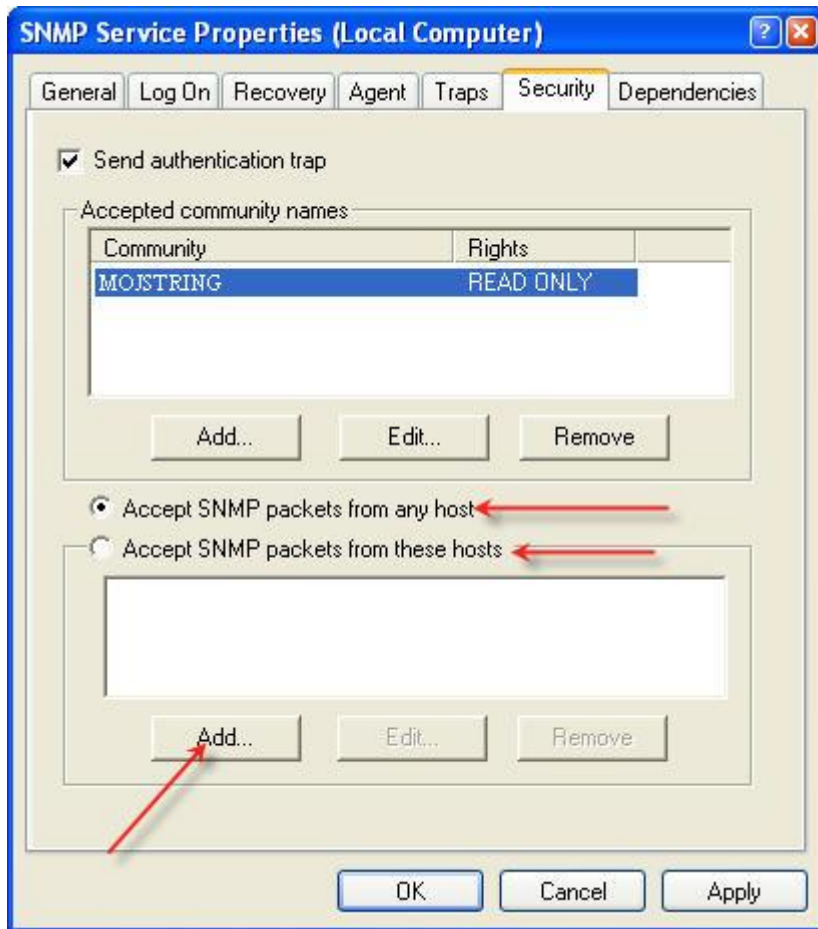


- Kliknuti na **Services**.



1. U desnom panelu dva puta kliknuti na **SNMP Service**





1. Zatim otvoriti **Security** karticu, i štiklirati (ako vec nije) **Send authentication trap**. Prvo je potrebno izbrisati **Community-grupu public**, tako što se selektuje pod **Accepted community names** i kliknuti na **Remove**. Zatim pod **Accepted community names** kliknuti **Add**.
2. Za definisanje kako host obrađuje SNMP zahteve selektovane **Community** grupe, izabrati nivo dozvole u polju **Community Rights READ ONLY**. U polju **Community Name**, upisati **case sensitive** ime **Community** grupe koji je dostavljen administratorima (MOJSTRING je primer i ne treba ga koristiti), a zatim kliknuti na **Add**.
3. Za definisanje hostova od koji ce se primati SNMP zahtevi kliknuti na (dok je selektovana željena **Community** grupa, u ovom primeru MOJSTRING)
4. **Accept SNMP packets from these hosts**, kliknuti na **Add**.
5. Upisati sledecu IP adresu **10.0.10.2**.
6. Kliknuti na **Add**, zatim na **Apply**.

Intersantno je primetiti da windows 2000 ne podržava SNMP V3. U slučaja potrebe za SNMP V3 na Windows server je potrebno instalirati SNMP V3 agenta nekog drugog proizvođača, ta rešenja se mogu naći na internetu i besplatna su.

## Preporučene varijable za monitoring mrežnih uređaja

Pre implementacije monitoring sistema u mrežu potrebno je definisati parametre koji će se nadgledati. MIB baza pruža veliki broj OID parametara i pitanje je kako odabrati vrednosti koje nam pružaju najbitnije informacije o stanju mrežnih uređaja i linkova. Tendencija u IT svetu je da se koriste standardne IETF MIB baze koje treba svaki proizvođač uređaja treba da podržava.

Parametri koji se najčešće prate kod mrežnih uređaja kao što su router-i i switch-ovi su:

- Stanje Interfejsa (L2 i L3 veza)
- Protok na interfejsu (dobija se indirektno)
  - Standardan In/Out saobraćaj(bits/sec)
  - Odbačen In/Out saobraćaj(bits/sec)
  - Protok po In/Out paketima(packets/sec)
- Opterećenje procesora
- Opterećenje memorije
  - I/O memorija
  - CPU memorija

U slučaju potrebe za praćenjem funkcija koje se ne sreću na svim uređajima odnosno koje su karakteristične za pojedine proizvođače potrebno je ispitati MIB baze proizvođača koji je napravio taj uređaj.

OID promenjive koje se mogu očitavati kod servera zavise od operativnog sistema. U opštem slučaju svi operativni sistemi podržavaju standardne IETF MIB baza, tako da je dosta OID vrednosti univerzalno za sve uređaje koji podržavaju SNMP. Preporučene su sledeće vrednosti:

- Stanje Interfejsa (L2 i L3 veza)
- Statistika interfejsa (dobija se indirektno)
  - Standardan In/Out saobraćaj (bits/sec)
  - Odbačen In/Out saobraćaj(bits/sec)
  - Protok po In/Out paketima(packets/sec)
  - Koliko dugo je interfejs aktivan
- Opterećenje procesora
- Opterećenje memorije
  - HDD memorija
  - RAM memorija
  - Swap space memorija
- Broj sistemskih procesa
- Lista pokrenutih servisa na serveru
- Broj uspostavljenih TCP konekcija
- Broj trenutno ulogovanih sistemskih korisnika

U slučaju praćenja SNMP promenljivih UPS uređaja, većina OID vrednosti se mora naći u MIB bazama proizvođača. Preporučene varijable su:

- Trenutno stanje UPS-a, odnosno mod rada (battery mod, online mod, malfunction.....)
- Kapacitet baterije UPS-a
- Koliko dugo UPS može da radi u battery modu.
- Temperatura baterije
- Izlazno opterećenje UPS-a
- Ulazni napon
- Izlazni napon

Ostali mrežni uređaji:

- Klima Uređaji
  - Temperatura
  - Vlažnost vazduha
  - Status kompresora
- Senzorski uređaji
  - Senzor za buku
  - Senzor za temperaturu
  - Senzor za vlažnost
  - Senzor za vibracije
  - Senzor za pokret
  - Senzor za dim
  - Senzor za detekciju tečnosti

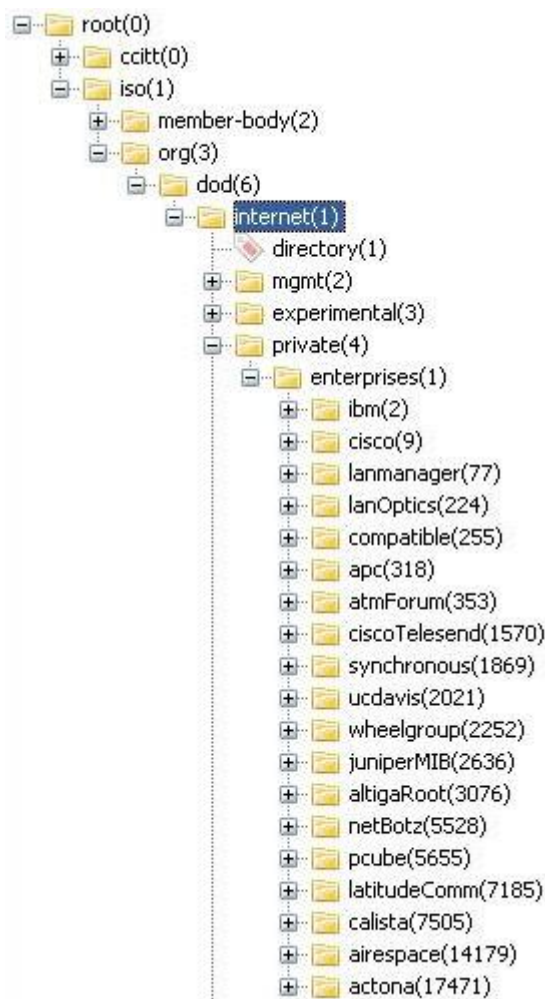
Standardne IETF MIB baze se nalaze pod MIB-2 (.1.3.6.1.2.1) prostorom u MIB drvetu.

- interfaces (.1.3.6.1.2.1.2) - Ovde se nalaze sve informacije o stanju interfejsa na uređaju.
- ifMIB (.1.3.6.1.2.1.31) - ifMIB Predstavlja proširenje interfaces MIB baze sa 32bit-nih brojeva na 64bit-ne brojeve.
- tcp (.1.3.6.1.2.1.6) - Ovde se nalaze parametri koji opisuju tcp konekcije.
- host (.1.3.6.1.2.1.25) - Host tabela sadrži informacije o stanju procesora i memorije na serverima.

Sve prethodne tabele se mogu koristiti i na Linux serverima. Postoji još jedna MIB baza koja služi za monitoring Linux servera i nalazi se pod private(.1.3.6.1.4) prostorom.

- ucdavis(.1.3.6.1.4.1.2021) - Sadrži informacije o stanju procesora i memorije na Linux serverima.

Sve ostale varijable koje su karakteristične za pojedine proizvođače mrežnih uređaja (Cisco, Juniper, HP.....) se nalaze pod private(.1.3.6.1.4) prostorom u MIB bazi, kao što je prikazano na sledećoj slici.



## Aplikacije za rad sa SNMP protokolom

### Linux

Instalacija SNMP-a koja se najčešće koristi kod linux operativnih sistema je net-snmp paket aplikacija. Programi koji služe za testiranje SNMP agenta na udaljenom uređaju se nalaze u net-snmp-utils paketu. Instalacija paketa se vrši pomoću sledeće komande:

```
yum install net-snmp-utils
```

Tom komandom se instalira niz aplikacija od kojih su za testiranje najbitnije *snmpget* i *snmpwalk*. Razlika između ove dve komande je u tome što *snmpget* kao vrednost vraća samo OID vrednost koja je zadata u komandi dok *snmpwalk* uzima zadatu OID vrednost i kao rezultat vraća sve OID vrednosti koje se nalaze ispod nje u drvetu u MIB bazi.

Primer 1:

Verzija 2c
<code>snmpwalk -v 2c -c 192.168.10.5 .1.3.6.1.2.1.31.1.1.1.1</code>

**Verzija 3**

```
snmpwalk -v 3 -u peraperic -l authPriv -a MD5 -A perapass -x DES -X pera1234 192.168.10.5
.1.3.6.1.2.1.31.1.1.1.1
```

Verzija 2c kao autentifikaciju koristi samo community string, dok verzija tri koristi i autentifikaciju i enkripciju. Kao rezultat dobije se tabela *ifXName* interfejsa koji postoje na uređaju. OID koji je zadat u komandi *.1.3.6.1.2.1.31.1.1.1.1* predstavlja prvu kolonu u *ifXTable* tabeli. Umesto cele OID vrednosti moguće je koristiti i skraćenu verziju *ifXTable.1.1.1*.

Kao rezultat dobija se:

<b>IF-MIB::ifName.1 = STRING: VL1</b>
<b>IF-MIB::ifName.2 = STRING: Fa0/1</b>
<b>IF-MIB::ifName.3 = STRING: Fa0/2</b>
<b>IF-MIB::ifName.4 = STRING: Fa0/3</b>
<b>IF-MIB::ifName.5 = STRING: Fa0/4</b>
<b>IF-MIB::ifName.6 = STRING: Fa0/5</b>
<b>IF-MIB::ifName.7 = STRING: Fa0/6</b>
<b>IF-MIB::ifName.8 = STRING: Fa0/7</b>
<b>IF-MIB::ifName.9 = STRING: Fa0/8</b>

Iz ove tabele se vidi gde se može javiti problem prilikom očitavanja SNMP vrednosti. Pošto uređaji mogu imati različit broj interfejsa SNMP agent sam dodaje indekse na kraju tabele *IF-MIB::ifName*. **INDEX**. U ovom slučaju postoji devet interfejsa i indeksi uzimaju vrednost od 1 do 9. U nekim slučajevima može se desiti da indeksi uzimaju neke drugačije vrednosti (recimo od 101 do 109), i tada se mora voditi računa o vrednostima indeksa. To se često sreće kod očitavanja memorije na Linux i Windows serverima. Takođe se može naći primer gde se indeksi dinamički menjaju. Primer je CDP tabela kod Cisco uređaja. Kada dođe do promene u CDP tabeli (link padne, izgubi se neighbour, pa se link vrati) u CDP-SNMP tabeli se prvo izbriše neighbour pa kada se ponovo uspostavi veza neighbour se vrati u CDP-SNMP tabelu ali sa novim indeksom.

Primer 2:

**Verzija 2c**

```
snmpget -v 2c -c 192.168.10.5 ifXTable.1.1.1
```

**Verzija 3**

```
snmpget -v 3 -u peraperic -l authPriv -a MD5 -A perapass -x DES -X pera1234 192.168.10.5
ifXTable.1.1.1
```

Pomoću *snmpget* komande mogli bi samo da očitamo samo jednu vrednost recimo naziv prvog interfejsa u tabeli.

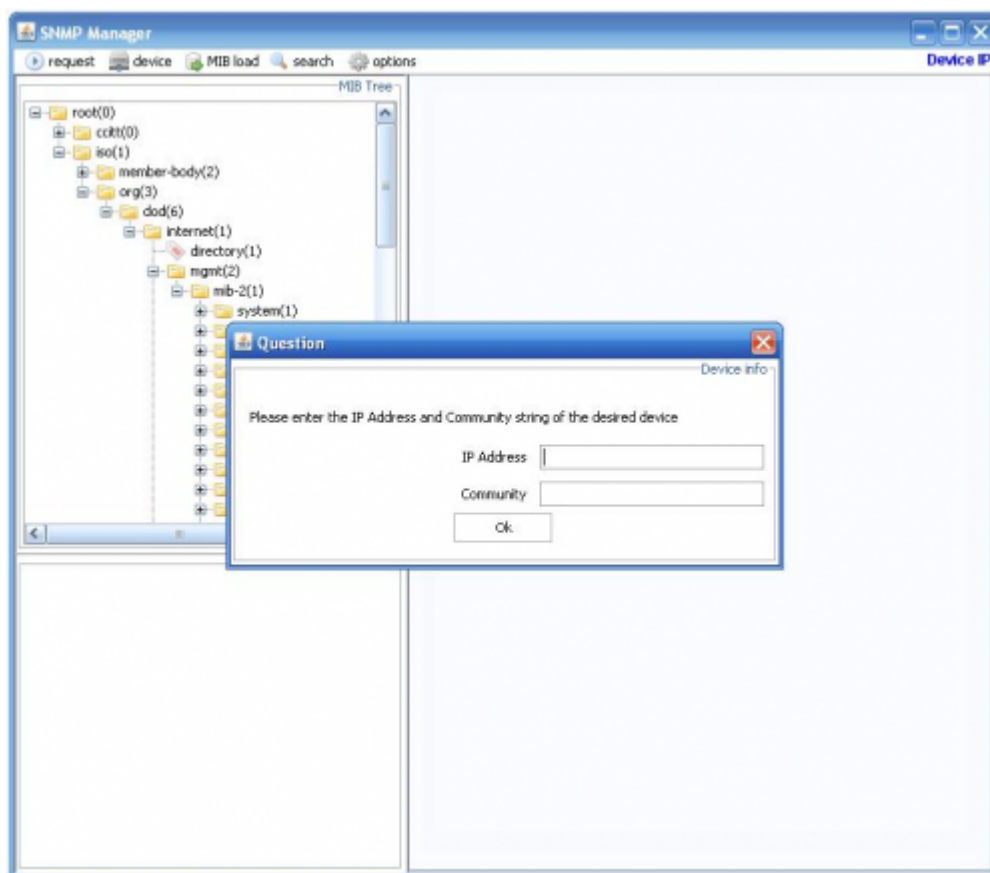
Kao rezultat dobija se:

```
IF-MIB::ifName.1 = STRING: Fa0/1
```

## Windows

Kod Windows operativnih sistema razvijen je veliki broj aplikacija koje se koriste za testiranje SNMP protokola. RCUB je razvio java aplikaciju (*SNMPManager*) koja se može pokretati na svim operativnim sistemima i koristi se za očitavanje SNMP vrednosti sa udaljenih uređaja. U daljem radu je objašnjen rad sa *SNMPManager* aplikacijom.

Prilikom startovanja aplikacije otvara se prozor u kome se zahteva od korisnika da unese ip adresu udaljenog uređaja i community string koji je konfigurisan na njemu. (Za sada aplikacija podržava samo V1 i V2c).



Slika 1 - SNMP Manager

Aplikacija se koristi tako što se u MIB drvetu sa leve strane izabere željeni element i selektuje opcija *request* kao što je prikazano na Slici 2. U desnom panelu će se dobiti SNMP odgovor udeljenog uređaja za izabranu OID vrednost u drvetu. Ispod MIB drveta se nalazi *description* panel u kome se može videti opis selektovane OID vrednosti.

The screenshot shows the SNMP Manager interface. On the left, the MIB Tree displays the hierarchy of MIBs, with the ifMIB(31) expanded to show ifName(1). The main window displays the ifXTable table, which lists interface statistics. The table has columns: TableIndex, ifName, ifHCInOctets, ifHCInUcastPkts, ifHCOutOctets, and ifHCC. The table contains 32 rows of data for various interfaces (Fa0/1 to Fa0/31). A red box highlights the ifName(1) object in the MIB Tree, and another red box highlights the details of this object in the bottom panel.

**ifName(1) Details:**

- Name: ifName
- OID: .1.3.6.1.2.1.31.1.1.1.1
- Status: current
- Access: read-only
- Type: DisplayString
- Range:
- Description: The textual name of the interface. The value of this object should be the name of the interface as assigned by the local device and should be suitable for use in commands entered at the device's console. This might be a text name such 'le0' or a simple port number such as '1' depending on the interface naming syntax of the device. If several entries in

Slika 2 - Primer O?itavanja ifXTable tabele stanja interfejsa sa udaljenog ure?aja

From:

<http://www.bpd.amres.ac.rs/> - AMRES wiki

Permanent link:

[http://www.bpd.amres.ac.rs/doku.php?id=glava\\_2](http://www.bpd.amres.ac.rs/doku.php?id=glava_2)

Last update: 2009/11/09 09:47