Monitoring mrežnih ure?aja pomo?u SNMP protokola

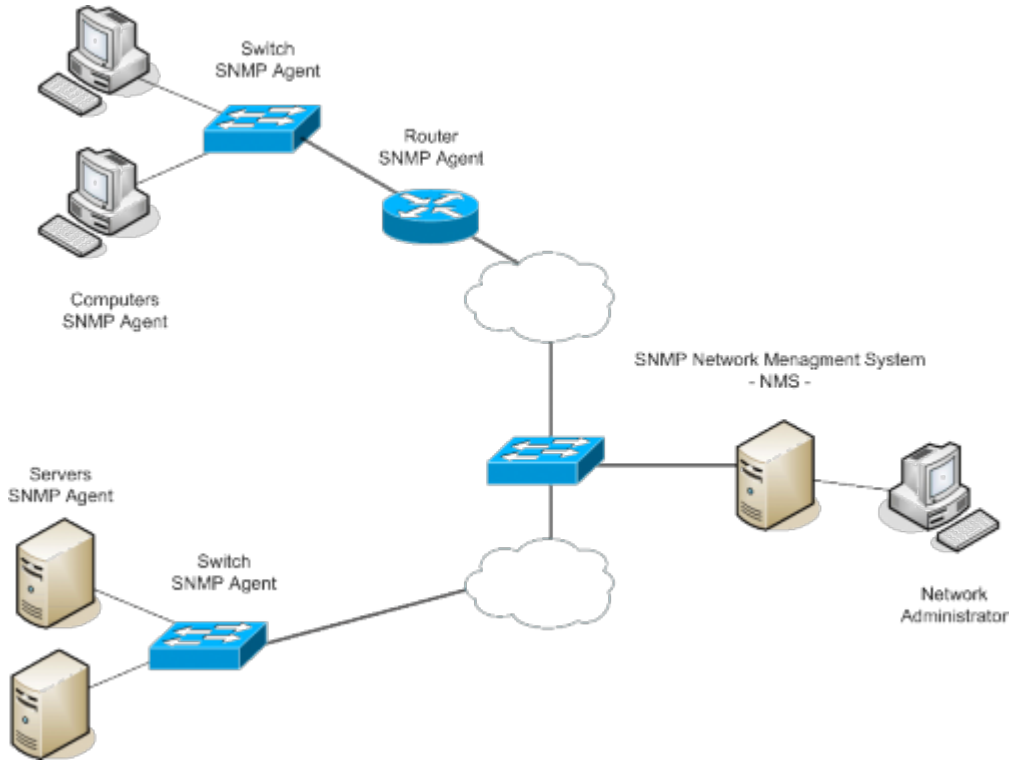
Uvod:

Cilj ovog dokumenta je da uputi ?itaoca u osnovne mehanizme funkcionisanja monitoring-a mreže pomo?u SNMP-a kao i u ispravan na?in 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 ure?ajima. Opisani su razni primeri o?itavanja parametara sa udaljenih ure?aja pomo?u programa koji se koriste za testiranje SNMP agenata. Ovaj dokument je namenjen svim administratorima koji žele na ispravan na?in da pokrenu SNMP protokol u mreži a žele da o?uvaju privatnost i sigurnost mreže koju nadgledaju.

SNMP protokol

Opšte karakteristike SNMP-a

Razvoj mrežnih ure?aja 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 pomo?u SNMP protokola. Sam SNMP protokol je dizajniran tako da veoma malo optere?uje 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: na?in upravljanja mrežom, baze podataka za ?uvanje informacija i strukture koriš?enih podataka. Oslanja se na UDP, mada je mogu?e podesiti i rad preko TCP-a, što nije preporu?ljivo u velikim mrežama.
Monitoring mrežnih ure?aja pomo?u SNMP-a se obi?no vrši tako što se na mrežnom ure?aju pokrene SNMP agent i to tako da odgovara na periodi?ne zahteve koje dobija od servera koji prikuplja podatke (NMS Server). SNMP agent saznaje od ure?aja informacije neophodne za upravljanje, prevodi ih u oblik koji propisuje SNMP, u tom obliku ih prosle?uje NMS-u. U slu?aju kada do?e do neke bitne promene na ure?aju SNMP agent generiše SNMP Trap poruku i na taj na?in se brzo, bez ?ekanja 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 omogu?i komunikacija izmedu mrežnih uredaja i NMS servera po ovim portovima (access lists, IP tables ….).



Slika 1 - Monitoring pomo?u SNMP-a

Tipovi Podataka

Informacije koje se mogu o?itati sa udaljenog ure?aja su definisane u MIB (Management Information Base) bazi podataka. U MIB bazi su varijable hijerarhijski definisane u formi stabla, i te varijable sam proizvo?a? ure?aja kreira. Svaka od ovih varijabli u MIB bazi je jednozna?no odre?ena svojim OID (Object Identifier) identifikatorom. Postoje i univerzalne varijable koje su definisane na svim mrežnim ure?ajima. Rad sa ovim varijablama ?e biti opisan pojedina?no za svaki ure?aj.

Tipovi podataka su podeljeni u dve grupe:

- Prosti tipovi podataka
- Aplikativni tipovi podataka

Tipovi podataka su nasle?eni od SNMP V1 i za V2c i V3 su samo dodati novi tipovi.

- Prosti tipovi podataka
  - Celobrojni tip - (-2^{31}~2^{31}-1)
  - String okteta - (0~65535)
  - ObjectID - (OID vrednost)

- Aplikativni tipovi podataka
  - Adrese mreže - IPv4 i IPv6 adrese mreže
  - Broja?i - (V2c i V3 podržavaju 64-bitne broja?e dok V1 samo 32-bitne) Broja?i vrše inkrement svog stanja sve dok ne do?u do maksimalne vrednosti kada se resetuju u po?etno nulto stanje.

- Mera?i - (Mogu menjati stanje u okviru nenegativne minimalne i maksimalne vrednosti) U slu?aju da prekora?e grani?ne vrednosti mera?i se zadržavaju u tom grani?nom stanju.
- Zabeleženi trenutak - Predstavlja trenutak od odigravanja nekog doga?aja izražen u stotim delovima sekunde.
- Pokrivanje - Predstavlja proizvoljno kodiranje koje pruža fleksibilnost zato što omogu?uje prosle?ivanje tipova podataka u formi stringa koji nisu striktno definisani u SMI.
- Celobrojne ozna?ene vrednosti
- Celobrojne neozna?ene vrednosti (Nenegativne)

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

- Read (Varijabla se može samo o?itati)
- Read-Write (Varijabla se može o?itati ali joj se može i promeniti vrednost)

Veoma je bitno prou?iti tip vrednosti koju SNMP agent vra?a. 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 V 2c. 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 pomo?u community stringa i on se šalje u ?istom tekstu preko mreže. U slucaju da neko “uhvati” ovaj saobra?aj pomo?u neke sniffing aplikacije, može vrlo lako otkriti community string i na taj na?in biti u mogu?nosti 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), spre?ava mogu?nost izmene paketa prilikom prenosa
2. Autentifikacija, potvrda da je poruka stigla sa pravog izvorišta
3. Kriptovanje paketa, spre?avanje ?itanja 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. Omogu?uje 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 ce biti opisana implementaija SNMP V2c i SNMP V3 na raznim mrežnim uredajima.

Pokretanje SNMP-a na raznim tipovima ure?aja

CISCO Ruter

Pomo?u slede?e komande,koja se koristi u konfiguracionom modu, pokre?e 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 ?e ruter odgovoriti samo onom ure?aju koji mu pošalje zahtev koji sadrži baš ovaj string. Opcija ro na naglašava da je mogu?e samo o?itati podatke a ne i menjati ih (ro-read only). Tako?e je mogu?e 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 ograni?e samo na mogu?nost o?itavanja a ne i menjanja varijabli. Kona?no na kraju komande je definisana access lista acl10 pomo?u koje se može definisati pristup SNMP agentu na ure?aju samo sa odre?enih 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 ?e 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. Pomo?u slede?ih komanda se pokre?e SNMP V3 protokol na Cisco ure?ajima.

```
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 o?itani sa ure?aja. U ovom slu?aju je omogu?eno o?itavanje OID-a (interface) koji opisuju stanje interfejsa na ure?aju. Ako se ne definiše ovakva grupa predpostavlja 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 mogu?nost o?itavanja podataka iz MIB baze i to samo onih koji su definisani u "pogledu" MYGROUPV. Tre?a komanda definiše korisnika peraperic koji pripada grupi MYGROUP koji koristi SNMP V3, autentifikaciju pomo?u md5 algoritma i ima password perapass. Poslednjom opcijom u komandi 3 "pera1234" se definiše passphrase koja se koristi za enkripciju SNMP saobra?aja. ?etvrta komanda pokre?e SNMP Trap mod rada. Peta komanda definiše NMS server koji ?e prikupljati trap poruke. U ovom slu?aju prilikom komunikacije izme?u NMS i Cisco ure?aja koristi?e se SNMP V3 i pravila koja su definisana pomo?u grupe MYGROUP. Provera izvršavanja SNMP upita se može uraditi direktno sa NMS servera. U slu?aju Linuxa to je mogu?e uraditi slede?om komandom.

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

Kao rezultat ove komande dobi?e se tabela koja opisuje stanje interfejsa na Cisco ure?aju.

Koriš?enje enkripcije saobra?aja dosta optere?uje resurse ure?aja (Procesor i Memoriju) tako da pojedini ure?aji nemaju implementiran modul za enkripciju. Takvi ure?aji ne podržavaju SNMP V3. U slede?oj 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 naj?ešce monitorišu OID vrednosti koje opisuju stanje interfejsa na ure?aju i OID vrednosti koje opisuju stanje memorije i procesora ure?aja, mada je mogu? monitoring i ostalih parametara od interesa. Obi?no svaki proizvo?a? opreme definiše svoje OID vrednosti koje opisuju ove parametare. U *Tabeli 1* je dat primer o?itavanja ifTable (.1.3.6.1.2.1.2.2) OID tabele. Ove OID vrednosti se ?esto koriste i svi tipovi mrežnih ure?aja ih moraju podržavati.

ifTable - Tabela koja opisuje trenutno stanje svih interfejsa			
ifType	6	6	1

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

Tabela 1 - ifXTable

U Cisco menadžment modulu .1.3.6.1.4.1.9.9 mogu se naci OID-ovi od intersa za nadzor nad Cisco uredajima.

SERVERI

Linux Server

LINUX Server (SNMP V2c)

U slu?aju podešavanja SNMP protokola na Linux operativnim sistemima prvo je potrebno instalirati SNMP deamona na server. U slede?em primeru bi?e opisana instalacija na CentOS 5.3 operativnom sistemu pomo?u YUM komande. Slede?a komanda omogu?uje automatizovanu instalaciju SNMP deamona i korisnih komandi za kontrolu rada SNMP-a.

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

Slede?i korak je podešavanje servisa da se automatski pokre?e prilikom startovanja servera. Potrebno je uneti slede?u komandu.

```
chkconfig snmpd on
```

Slede?a stavka je podešavanje community stringa i OID objekata koji mogu biti o?itani sa servera.

Potrebno je editovati fajl snmpd.conf koji se obi?no nalazi u direktorijumu /etc/snmp/ i izmeniti slede?e 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 de su uklju?eni svi OID-ovi koji se nalaze ispod ?vora .1.3.6.1.2.1.1 u MIB drvetu. Pomo?u komande excluded mogu?e je isklju?iti pojedine OID vrednosti, odnosno uvesti ograni?enja u prikazu MIB baze. Ovde je potrebno definisati OID vrednosti koje ?e server vra?ati kao odgovor na SNMP upite. Ako NMS zatraži OID koji nije ovde definisan server ne?e odgovoriti NMS-u. U slu?aju da želimo da omogu?imo o?itavanje svih OID vrednosti potrebno je uneti slede?i red:

```
view systemview included .1
```

Na taj nacin su uklju?ene sve vrednosti koje se nalaze ispod cvora .1 u MIB stablu, odnosno celo stablo.

Sada je potrebno pokrenuti servis slede?om komandom:

```
service snmpd start
```

Proveru je mogu?e uraditi pomo?u slede?e komande:

```
snmpwalk –v 2c –c mojcommunity 127.0.0.1
```

Kao rezultat ?e se prikazati cela MIB tabela (drvo), ili deo MIB tabele, koji je definisan prethodnim komandama za ograni?enje prilikom o?itavanja 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 slede?e 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 mojpogled
```

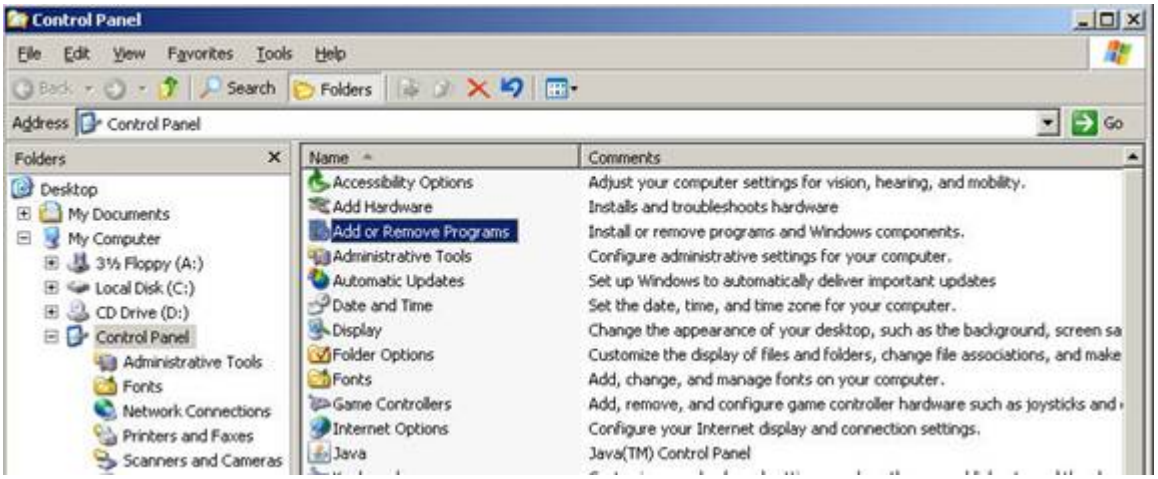
Prva dva parametra, *syslocation* i *syscontact* su podaci koji služe da daju opšte informacije o serveru. Oni nisu zna?ajni za ispravan rad SNMP protokola ali su bitni za administratore servera koji ?e imati pored osnovnih informacija o stanju servera i informaciju o lokaciji servera i kontakt osobi kojoj se mogu obratiti u slu?aju pojave problema. *Syslocation* i *Syscontact* su neki od parametara koji se mogu na?i na svim ure?ajima koji podržavaju SNMP protokol. Tre?i red definiše pogled, odnosno skup OID vrednosti iz MIB stabla. U ovom slu?aju je definisana tabela interfejsa servera. Mogu?e je dodati više tabela ili pomo?u komande *exclude* iskljuciti neke OID vrednosti. Ova ograni?enja su veoma bitna zato što je pomocu SNMP–a mogu?e i postaviti neke parametre a to direktno može uticati na ispravan rad uredaja. ?etvrta komanda kreira *user*-a john ?iji je *password* john1234. Prlikom autentifikacije koristi se MD5 algoritam, a saobra?aj je enkriptovan pomocu DES algoritma. Passphrase koji se koristi prilikom enkripcije je john5678. Peta komanda user-u john daje read only (rouser) privilegije i to samo nad mojpogled pogledom na MIB bazu koji je definasn u tre?oj komandi. Provera podešavanja SNMP V3 na serveru je mogu?a pomo?u komande:

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

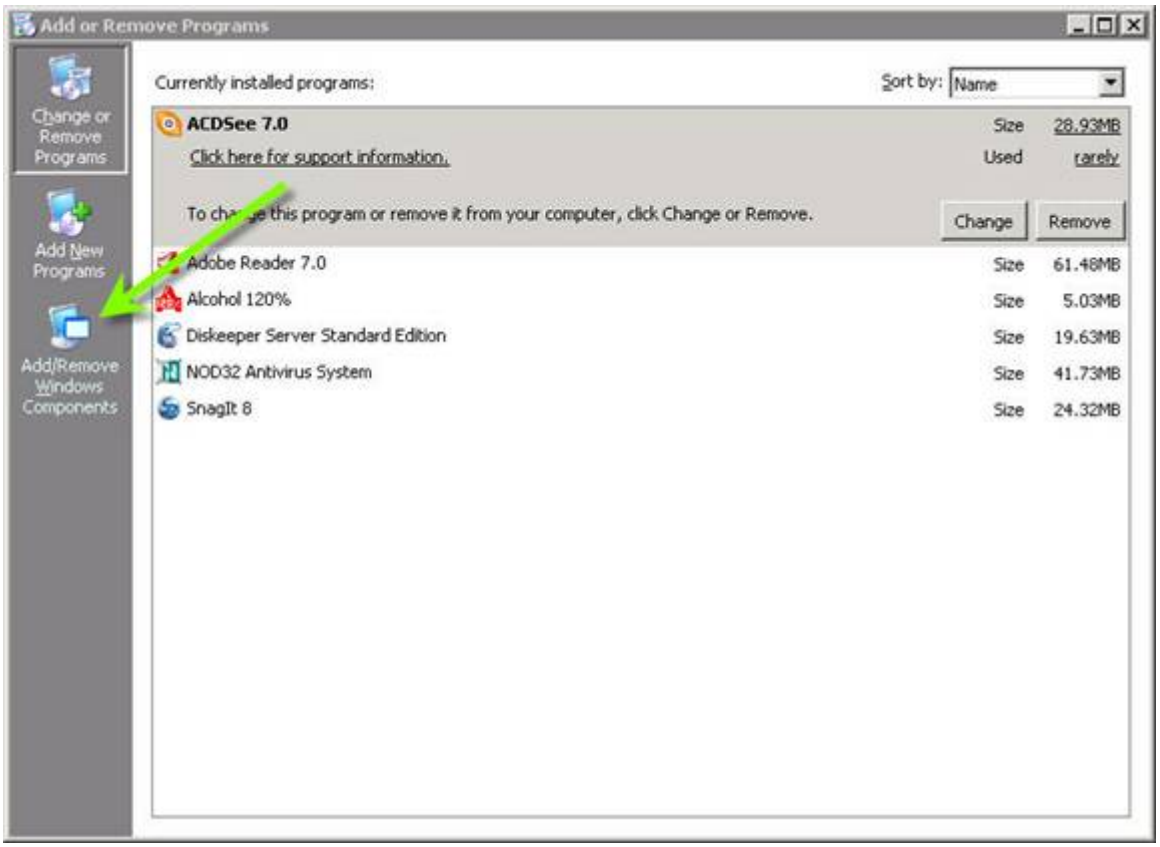
Windows 2000 Server

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

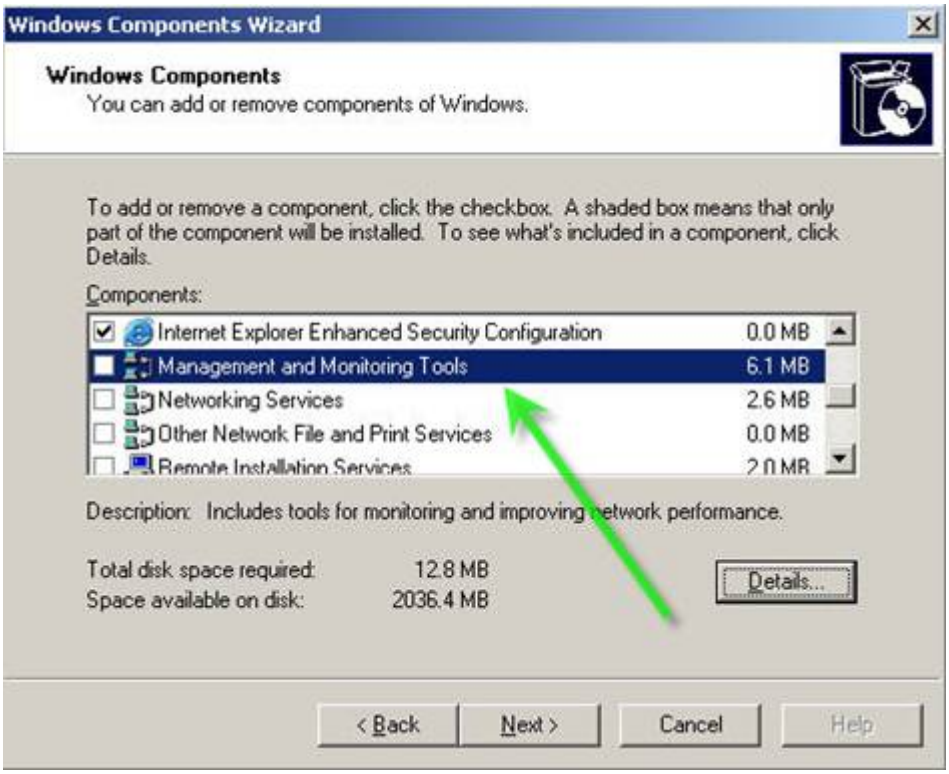
1. Kliknuti na **Start**, zatim **Control Panel** pa **Add or Remove programs**.



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

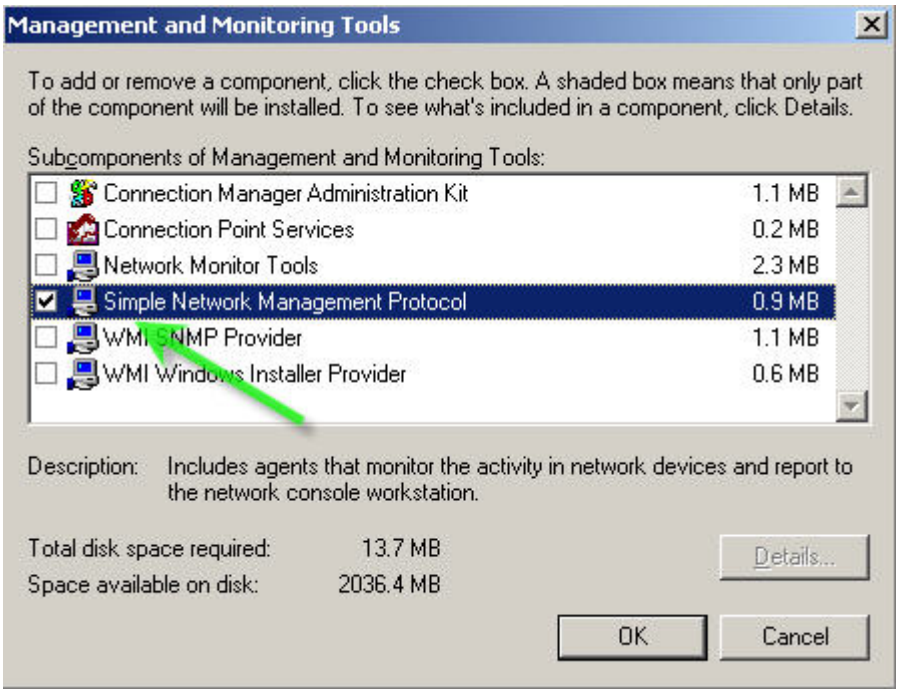


1. U otvorenom prozoru **Windows Components wizard**-a selektovati (ne štiklirati) **Management and Monitoring Tools,** a zatim na **Details** (dok je **Management and Monitoring Tools** selektovan plavom bojom).



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

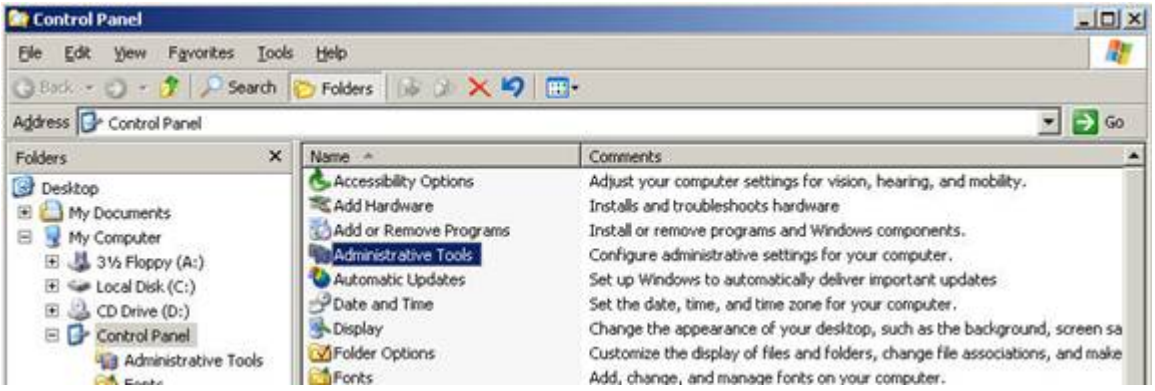
Management Protocol pa **OK.**



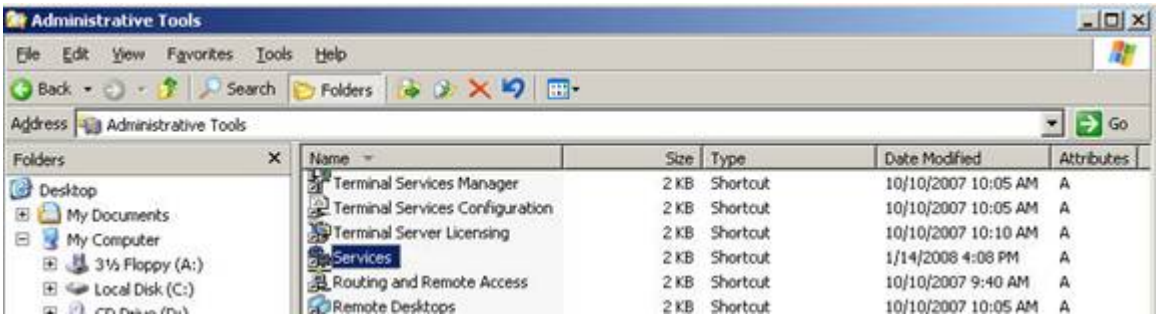
Za ispravnu instalaciju SNMP protokola potreban je instalacioni disk instalirane verzije Windows server 2003 koga treba staviti u CD citac. Zatim u prozoru **Windows Components wizard**-a kliknuti na **Next** i pratiti korake instalacije.

Konfiguracija SNMP Agenta

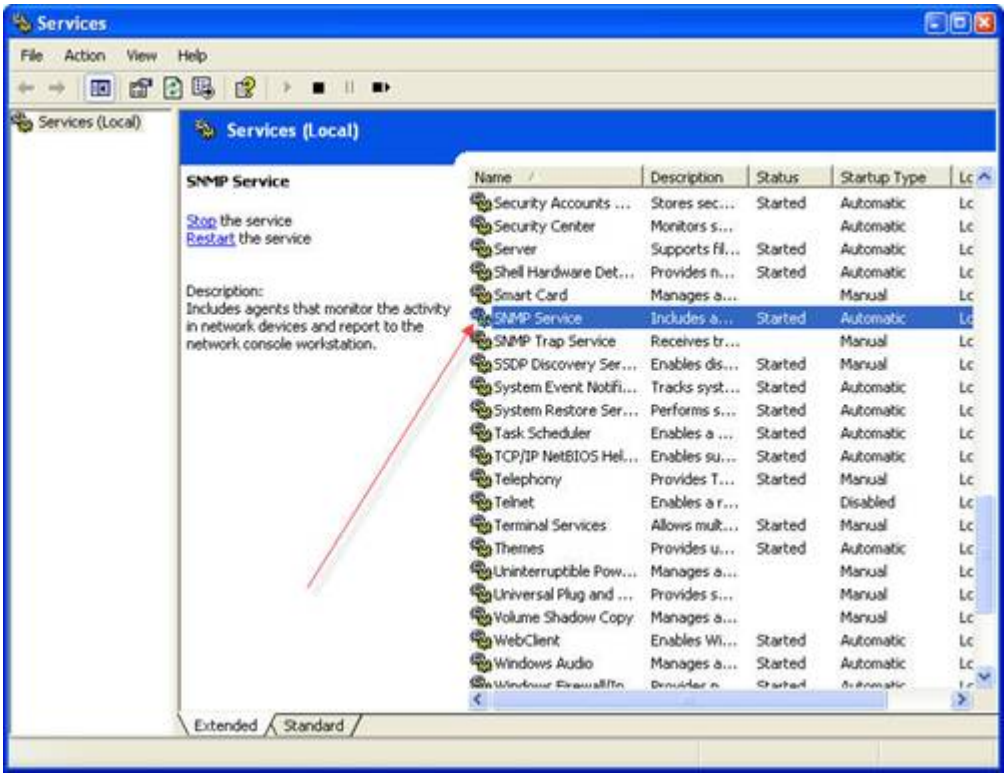
1. Otvoriti **Control Panel**, pa kliknuti na **Administrative Tools**

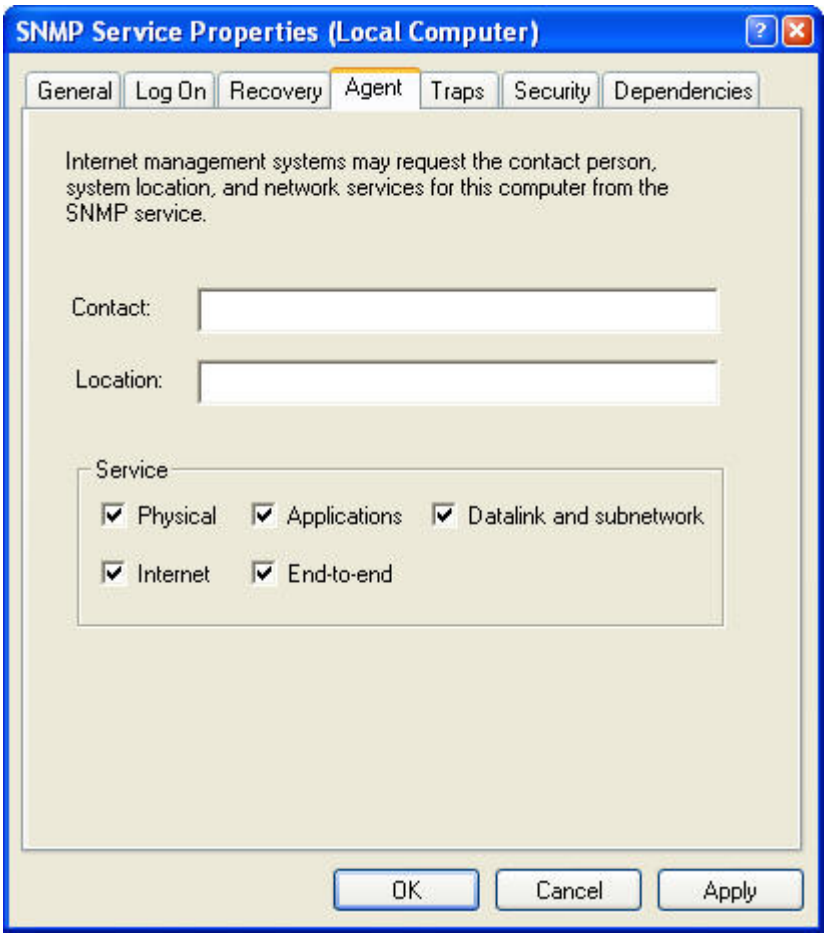


1. Otvoriti polje **Services**



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



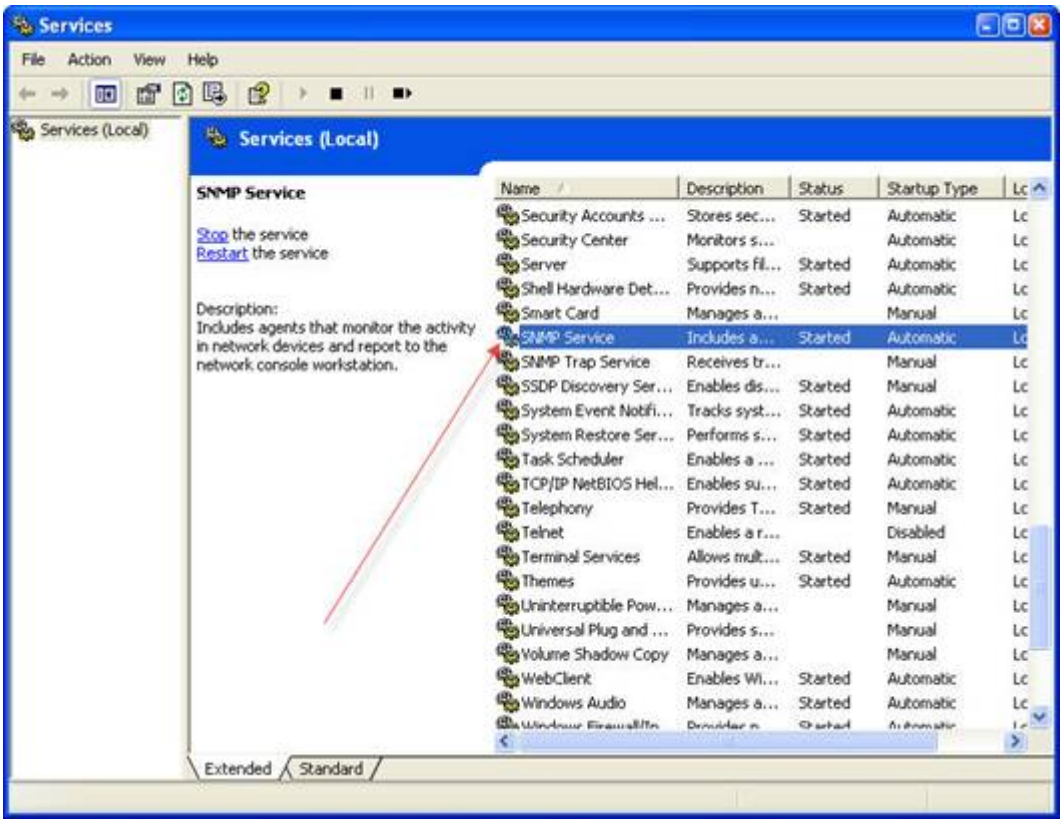


1. Upisati u polju **Contact** e-mail adresu administratora zaduženog za održavanje servera, a u polju **Location** fizicku lokaciju racunara ili kontakta.
2. U polju **Service** treba štiklirati sve servise kao na slici prikazanoj gore. To su:

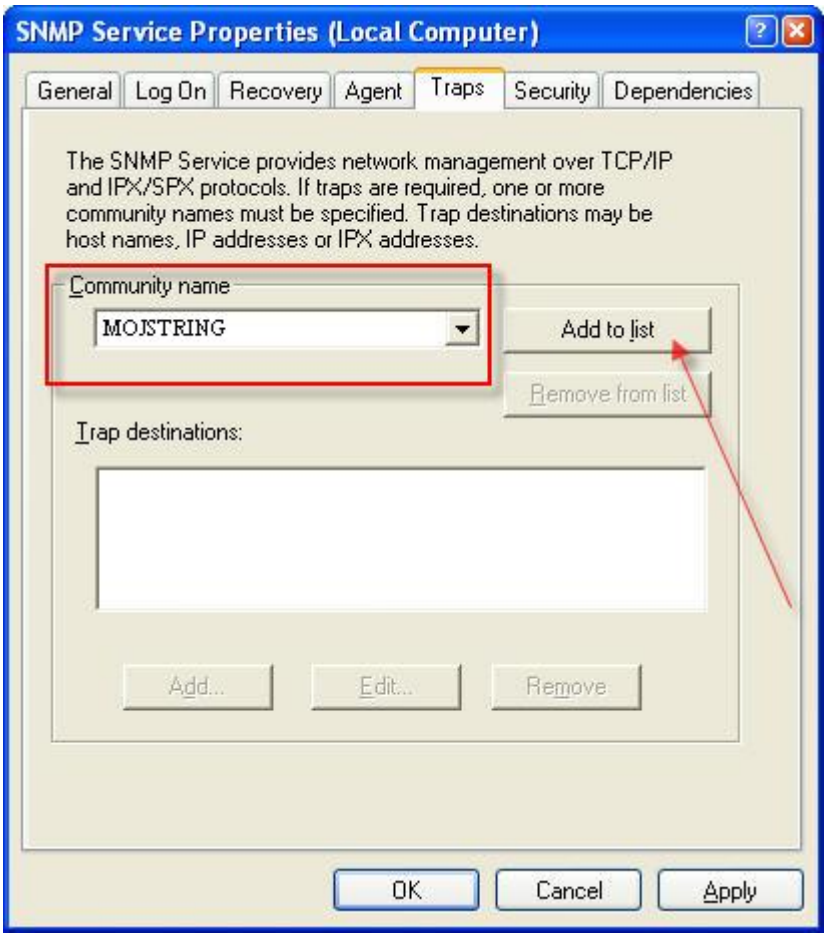
Po konfigurisanju kliknuti na OK.

Konfigurisanje Community grupe i Trap-ova

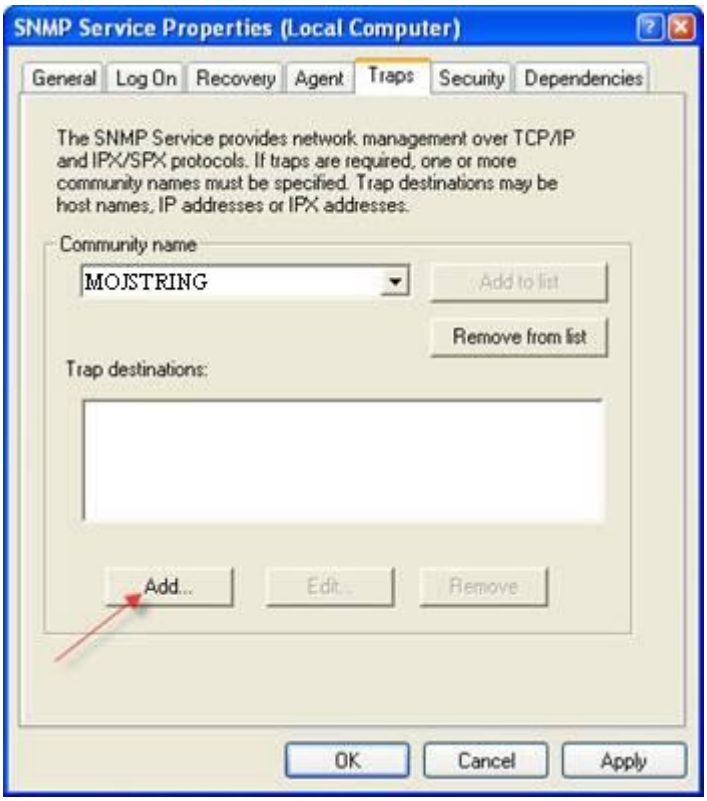
1. Otvoriti **Control Panel**, pa kliknuti na **Administrative Tools** .



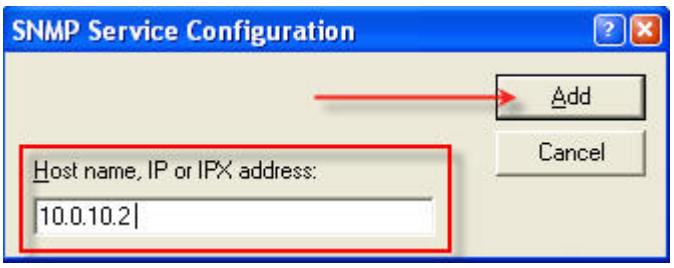
1. Otovoriti polje **Services**.



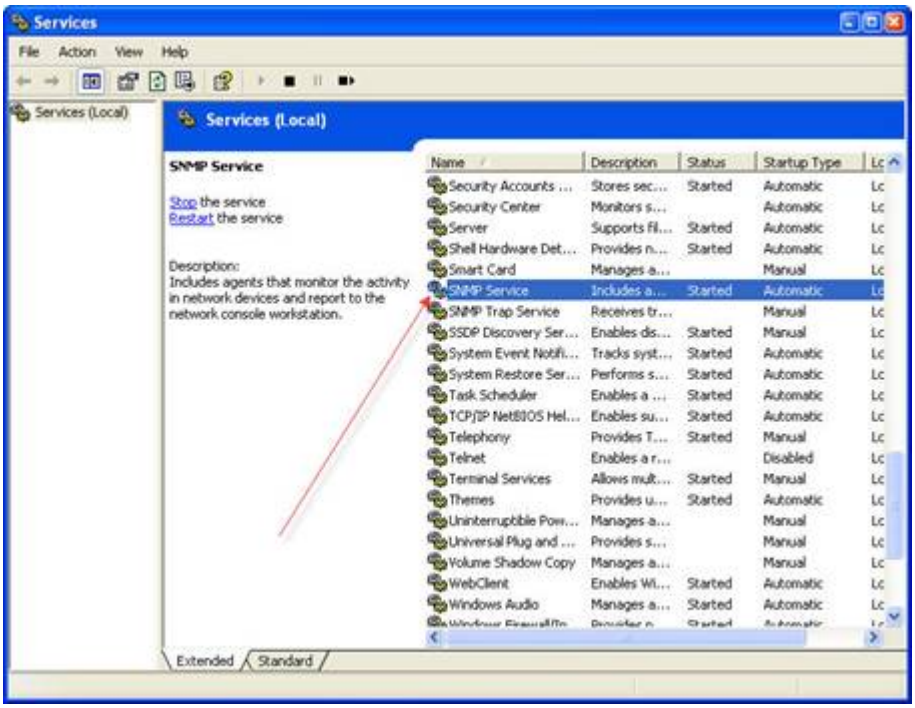
1. U desnom panelu dva puta kliknuti na **SNMP Service**.



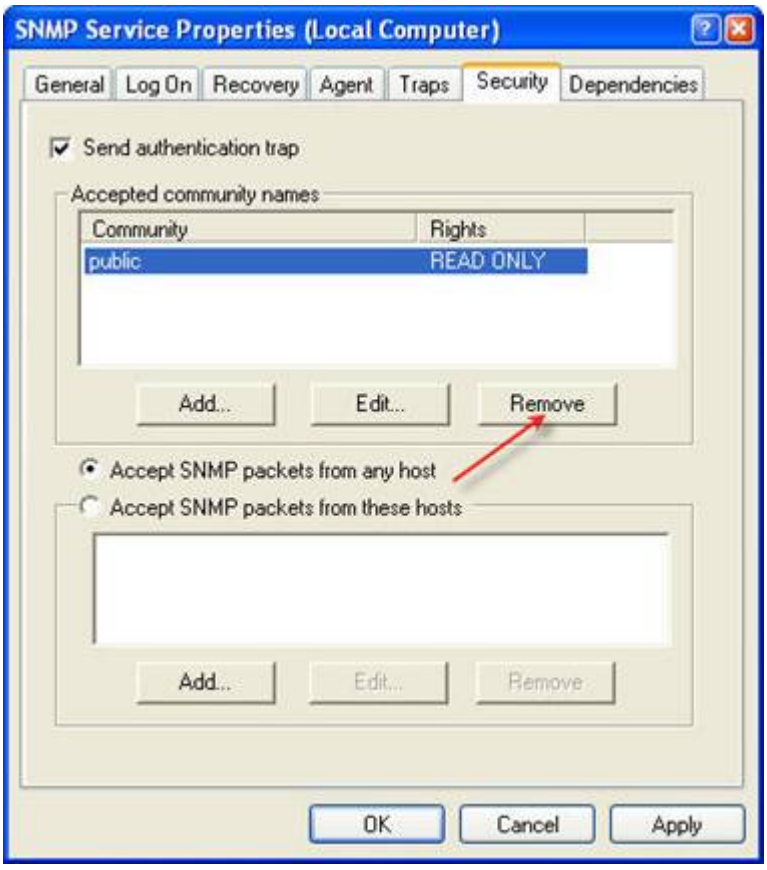
1. Posle otvaranja na kartice **Traps**, u polju **Community name upisati Community string, koji ce biti naknadno dostavljen administratorima (Community string "MOJSTRING" je primer i ne treba ga koristiti), a zatim kliknuti na Add to List**



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



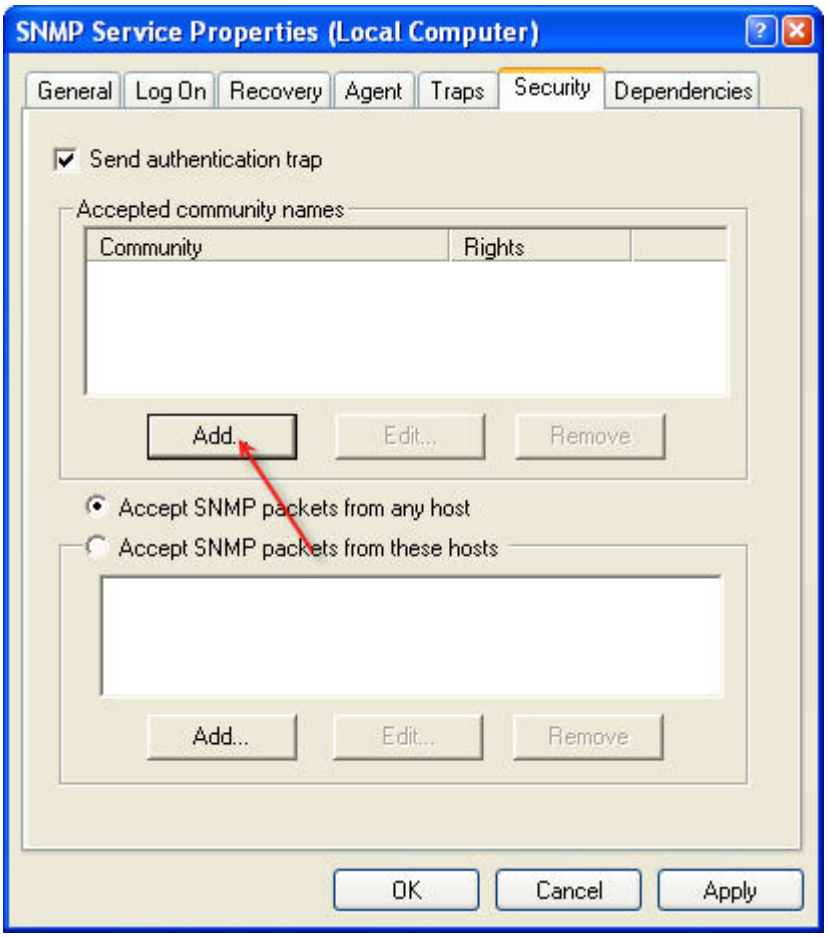
- U polju Host name, IP or IPX address upisati IP adresu 10.0.10.2 kliknuti Add.



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

Konfiguracija SNMP bezbednosti na serverima

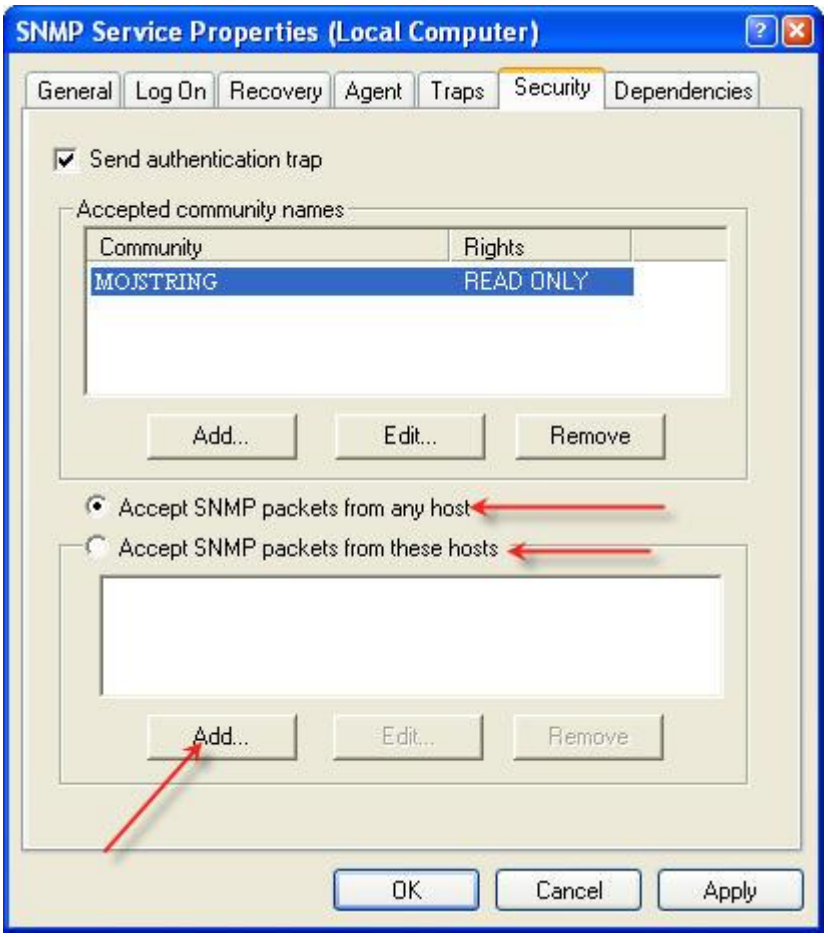
1. Otvoriti **Control Panel**, pa kliknuti na **Administrative Tools** .



- Kliknuti na **Services**.



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



1. Zatim otvoriti **Security** karticu, i štiklirati (ako vec nije) **Send authenntication 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 obraduje 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 slu?aju potrebe za SNMP V3 na Windows server je potrebno instalirati SNMP V3 agenta nekog drugog proizvo?a?a, ta rešenja se mogu na?i na internetu i besplatna su.

Preporu?ene varijable za monitoring mrežnih ure?aja

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

Parametri koji se naj?eš?e prate kod mrežnih ure?aja kao što su router-i i switc-evi su:

- Stanje Interfejsa (L2 i L3 veza)
- Protok na interfejsu (dobija se indirektno)
  - Standardan In/Out saobra?aj(bits/sec)
  - Odba?en In/Out saobra?aj(bits/sec)
  - Protok po In/Out paketima(packets/sec)
- Optere?enje procesora
- Optere?enje memorije
  - I/O memorija
  - CPU memorija

U slu?aju potrebe za pra?enjem funkcija koje se ne sre?u na svim ure?ajima odnosno koje su karakteristi?ne za pojedine proizvo?a?e potrebno je ispitati MIB baze proizvo?a?a koji je napravio taj ure?aj.

OID promenjive koje se mogu o?itavati kod servera zavise od operativnog sistema. U opštem slu?aju svi operativni sistemi podržavaju standardne IETF MIB baza, tako da je dosta OID vrednosti univerzalno za sve ure?aje koji podržavaju SNMP. Preporu?ene su slede?e vrednosti:

- Stanje Interfejsa (L2 i L3 veza)
- Statistika interfejsa (dobija se indirektno)
  - Standardan In/Out saobra?aj (bits/sec)
  - Odba?en In/Out saobra?aj(bits/sec)
  - Protok po In/Out paketima(packets/sec)
  - Koliko dugo je interfejs aktivan
- Optere?enje procesora
- Optere?enje 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 slu?aju pra?enja SNMP promenjivih UPS ure?aja, ve?ina OID vrednosti se mora na?i u MIB bazama proizvo?a?a. Preporu?ene varijable su:

- Trentno stanje UPS-a, odnosno mod rada (battery mod, online mod, malfunction…..)
- Kapacitet batrije UPS-a
- Koliko dugo UPS može da radi u battrery modu.
- Temperatura baterije
- Izlazno optere?enje UPS-a
- Ulazni napon
- Izlazni napon

Ostali mrežni ure?aji:

- Klima Ure?aji
  - Temperatura
  - Vlažnost vazduha
  - Status kompresora
- Senzorski ure?aji
  - Senzor za buku
  - Senzor za temperaturu
  - Senzor za vlažnost
  - Senzor za vibracije
  - Senzor za pokret
  - Senzor za dim
  - Senzor za detekciju te?nosti

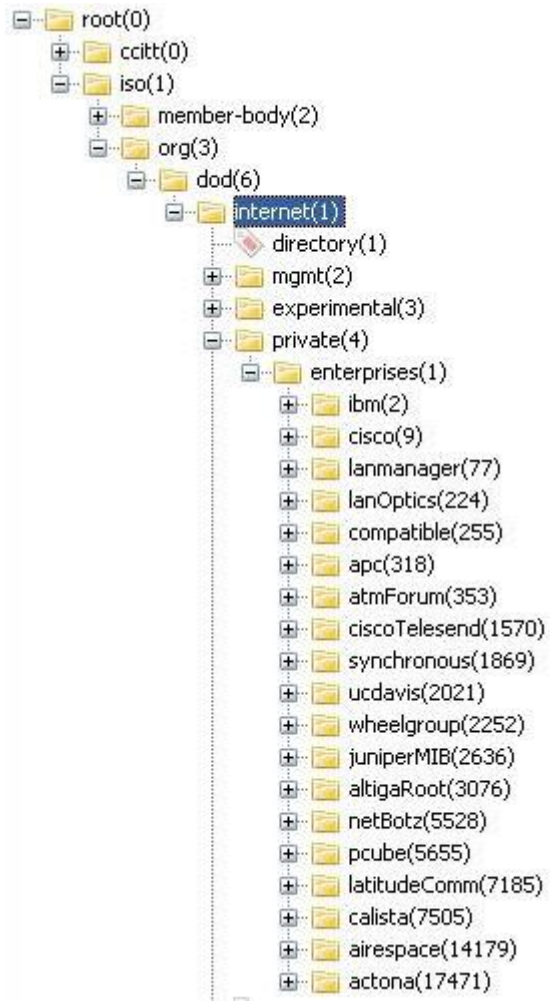
Standardne IETF MIB baze se nalaze pod MIB-2 (.1.3.6.1.2.1) ?vorom u MIB drvetu.

- interfaces (.1.3.6.1.2.1.2) - Ovde se nalaze sve informacije o stanju interfejsa na ure?aju.
- ifMIB (.1.3.6.1.2.1.31) - ifMIB Predstavlja proširenje interfaces MIB baze sa 32bit-nih broja?a na 64bit-ne broja?e.
- 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) ?vorom.

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

Sve ostale varijable koje su karakteristi?ne za pojedine proizvo?a?e mrežnih ure?aja (Cisco, Juniper, HP…..) se nalaze pod private(.1.3.6.1.4) ?vorom u MIB bazi, kao što je prikazano na slede?oj slici.



Aplikacije za rad sa SNMP protokolom

Linux

Instalacija SNMP-a koja se naj?eš?e koristi kod linux operativnih sistema je net-snmp paket aplikacija. Programi koji služe za testiranje SNMP agenta na udaljenom ure?aju se nalaze u net-snmp-utils paketu. Instalacija paketa se vrši pomo?u slede?e komande:

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

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

Primer 1:

Verzija 2c
snmpwalk -v 2c -c 192.168.10.5 .1.3.6.1.2.1.31.1.1.1.1

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 dobi?e se tabela *ifXName* interfejsa koji postoje na ure?aju. 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 mogu?e je koristiti i skra?enu verziju *ifXTable.1.1.1*.

Kao rezultat dobija se:

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

Iz ove tabele se vidi gde se može javiti problem prilikom o?itavanja SNMP vrednosti. Pošto ure?aji mogu imati razli?it broj interfejsa SNMP agent sam dodaje indekse na kraju tabele *IF-MIB::ifName.**INDEX***. U ovom slu?aju postoji devet interfejsa i indeksi uzimaju vrednost od 1 do 9. U nekim slu?ajevima ?e se desiti da indeksi uzimaju neke druga?ije vrednosti (recimo od 101 do 109), i tada se mora voditi ra?una o vrednostima indeksa. To se ?esto sre?e kod o?itavanja memorije na Linux i Windows serverima. Tako?e se može na?i primer gde se indeksi dinami?ki menjaju. Primer je CDP tabela kod Cisco ure?aja. Kada do?e 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

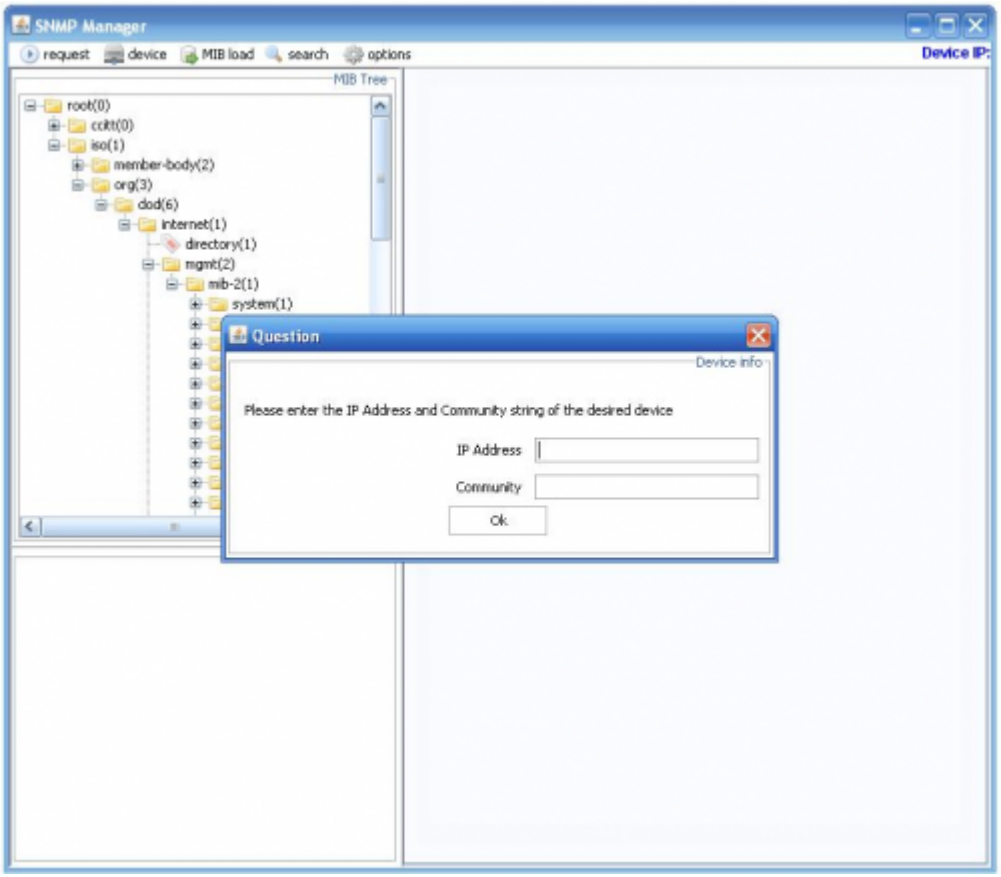
Pomo?u *snmpget* komande mogli bi samo da o?itamo samo jednu vrednost recimo naziv prvog interfejsa u tabeli.
Kao rezultat dobija se:

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

Windows

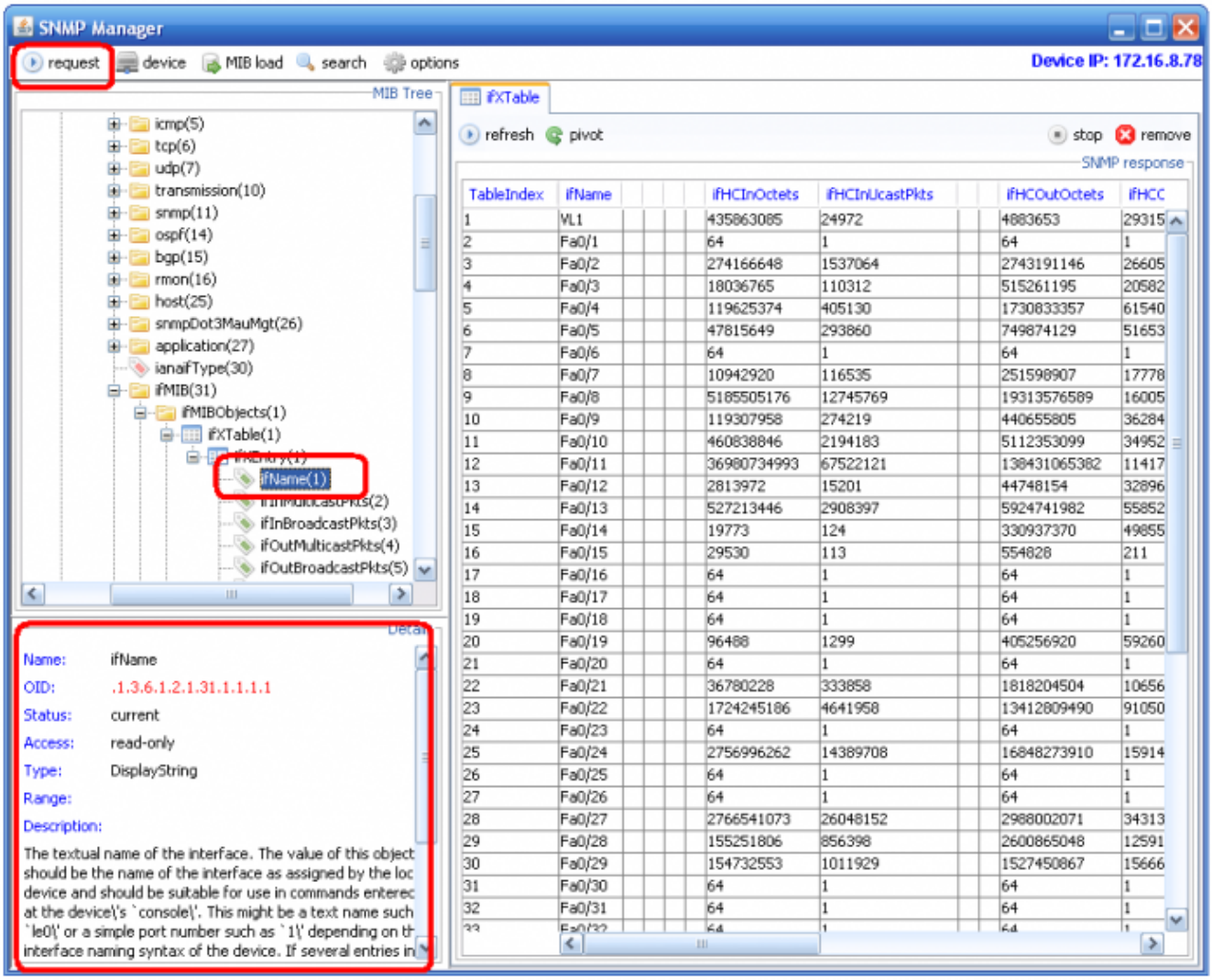
Kod Windows operativnih sistema razvijen je veliki broj aplikacija koje se koriste za testiranje SNMP protokola. RCUB je razvio java aplikaciju (*SNMPManager*) koja se može pokretati na svim operativnim sistemima i koristi se za o?itavanje SNMP vrednosti sa udaljenih ure?aja. U daljem radu je objašnjen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

Prilikom startovanja aplikacije otvara se prozor u kome se zahteva od korisnika da unese ip adresu udaljenog ure?aja 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 ?e se dobiti SNMP odgovor udeljenog ure?aja za izabranu OID vrednost u drvetu. Ispod MIB drveta se nalazi *description* panel u kome se može videti opis selektovane OID vrednosti.



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

Last update: **2009/11/09 09:47**