

SVEUCILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RACUNARSTVA

SEMINARSKI RAD IZ PREDMETA
SUSTAVI ZA PRACENJE I VOĐENJE PROCESA

SNMP (Simple Network Management Protocol)

Violeta Đurdek
0036389292

Zagreb, 03.06.2005.

Sadržaj

1. Uvod	2
2. Razvoj SNMP-a	3
3. Dijelovi sustava za upravljanje mrežom.....	5
4. Osnovne naredbe SNMP-a.....	11
5. SNMP MIB	12
6. Opis rada SNMP-a.....	15
7. Prednosti SNMP-a.....	21

1. Uvod

Danas kada racunarske mreže i tehnologije doživljavaju veliku ekspanziju, više se ne može zamisliti rad bez mogucnosti pristupa internetu. Klijent-poslužitelj revolucija donijela je mnoge dobitke, uključujući lakši pristup podacima, brže odgovore na nove poslovne inicijative i veliku lakocu korištenja. No, s druge strane, ova revolucija donijela je i niz problema. Pouzdanost i raspoloživost racunarskih sustava i mreža na kojima se temelje svi ovi servisi, postaje sve kriticnija te je od životnog interesa osigurati pouzdan alat za njihovu kontrolu i nadzor.

Trenutno je na tržištu prisutno mnogo protokola koji omogucavaju nadgledanje i upravljanje mrežnim resursima. Jedan od njih je SNMP protokol (eng. *Simple Network Management Protocol*) koji je, otkad je razvijen 1988., postao dominantan mrežni standard.

SNMP je mrežni upravljacki protokol koji omogucava kompanijama da nadgledaju operacije mrežnih uređaja koristeci centralni poslužitelj i softverske agente koji prate i prijavljuju rad SNMP-prijateljskih uređaja. Ili pak možemo reci da je SNMP protokol standard za upravljanje i nadzor mreže koji definira strategiju upravljanja TCP/IP mreža.

SNMP je jednostavan, zahtijeva malo koda za implementaciju, razdvaja upravljacku arhitekturu od arhitekture hardware uređaja i možda najvažnije, SNMP više nije samo specifikacija na papiru već implementacija koja je dostupna svakome danas.

2. Razvoj SNMP-a

Glavni ljudi odgovorni za razvoj SNMP-a su:

- Keith McCLOGHRIE
- Marshall ROSE
- Jeffrey D.CASE
- Mark FEDOR
- Martin LEE SCHOFFSTALL
- James R.DAVIN.

U travnju 1988. objavljen je RFC (Request For Comments → skup dokumenata koji sadrže Internet protokole i diskusije) 1052. Taj RFC je zahtjevna specifikacija za standardizirano mrežno upravljanje u kojoj se objašnjava što sve mora mrežno upravljanje:

- Biti što je veće moguće.
- Imati što je više moguće razlicitosti u administraciji/upravljanju.
- Pokrivati što je više moguće raznih protokola.

Sljedeci RFC-ovi su prvi dokumenti koji su objavljeni sa SNMP-om 1988.:

- RFC 1065 – Struktura i identifikacija upravljačkih informacija za TCP/IP
- RFC 1066 – Baza upravljačkih informacija za mrežno upravljanje
- RFC 1067 - Simple Network Management Protocol

Postoje 2 verzije: SNMPv1 i SNMPv2. Obje verzije imaju mnogo zajednickih osobina, no SNMPv2 nudi više mogućnosti, kao npr. dodatne protokol operacije. Postoji i SNMPv3 koji je još u razvoju.

Verzija 1.0 u svibnju 1991. obuhvacala je sljedeće RFC dokumente :

RFC 1155 -

Struktura i identifikacija upravljačkih informacija za TCP/IP te struktura i identifikacija upravljačkih informacija za objekte

RFC 1212 -

Sadrži MIB definicije

RFC 1213 -

Baza upravljačkih informacija za mrežno upravljanje -MIB-II

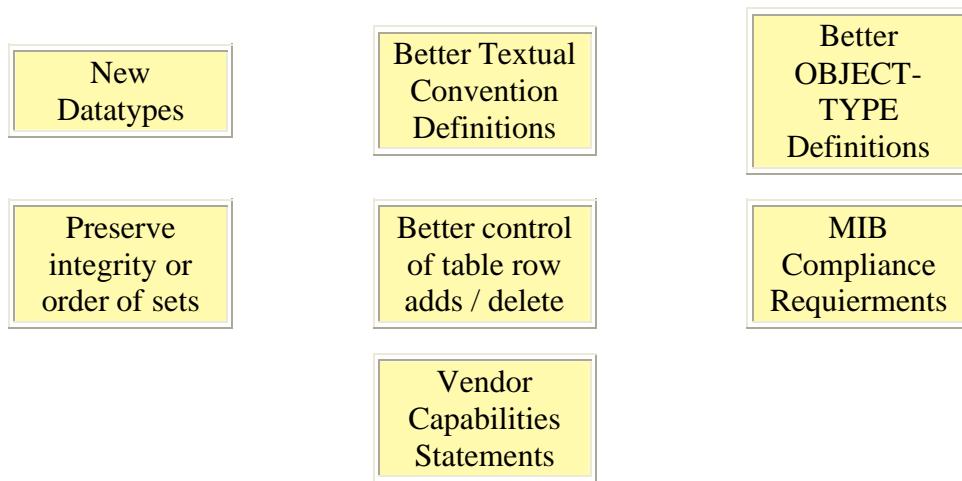
RFC 1157

- Simple Network Management Protocol (SNMP)
- Definira poruke koje se mogu razmjenjivati izmedu upravljačkih entiteta i upravljačkih stanica koje omogucavaju citanje i updatiranje vrijednosti.
- Definira alarm poruke (*trap*).
- Definira format poruka i komunikacijski protokol.

U travnju 1993. verzija 2.0 postala je standard. Ta verzija nudi dodatne mogućnosti kao npr. sigurnost i autentikaciju. SNMP verzija 2 je dokumentirana u nekoliko RFC-a:

- RFC 1902 (MIB struktura)
- RFC 1903 (Tekstualne konvencije)
- RFC 1904 (Conformance Statements)
- RFC 1905 (Protokol operacija)
- RFC 1906 (Transport mapiranje)
- RFC 1907 (MIB)

Neka poboljšanja SNMPv2:



Konačno 1997. sastavljena je grupa ciji je glavni cilj razviti SNMPv3 te prilagoditi multimedija protokol za mrežno upravljanje.

Treća verzija SNMP-a (SNMPv3) objavljena u RFC 2271 do RFC 2275 u siječnju 1998.

3. Dijelovi sustava za upravljanje mrežom

Upravljanje racunalnom mrežom (engl. *network management*) može se definirati kao usluga koja se dodaje u postojecu racunalsku mrežu da bi se olakšalo upravljanje pojedinim dijelovima mrežnog sustava i mrežom kao cjelinom na jednom od slijedeciih područja:

- *upravljanje greškama, tj. otkrivanje i dojava grešaka u sustavu;*
- *upravljanje konfiguracijom;*
- *upravljanje performansom;*
- *upravljanje sigurnošcu;*
- *upravljanje uslugama;*
- *upravljanje obracunavanjem troškova.*

U racunalskoj mreži vrste **internet** za izvođenje usluge upravljanja mrežom razvijen je aplikacijski protokol **SNMP**. Protokol SNMP dio je **sustava za upravljanje mrežom** (engl. *network management system*) sastavljenog od slijedecihi dijelova:

- *jedne ili više upravljackih stanica na kojima se izvode upravljacke aplikacije;*
- *jednog ili više upravljenih cvorova na kojima se izvode upravljacki agenti;*
- *upravljackih informacija;*
- *protokola SNMP po kojem se prenose upravljacke informacije između upravljackih aplikacija i agenata.*

Upravljacka stanica (engl. *network management stations*) je mrežno racunalo koje ima procesnu sposobnost dovoljnu za izvođenje upravljacke aplikacije.

Upravljacka aplikacija (engl. *management application*), koja se cesto naziva i SNMP-mNger ili samo manager, je racunalni program koji izvodi nadgledanje ili upravljanje upravljenih elemenata na upravljenim cvorovima mreže u skladu s **politikom upravljanja** (engl. *management policy*) koja je odredena od strane covjeka - upravitelja racunalne mreže.

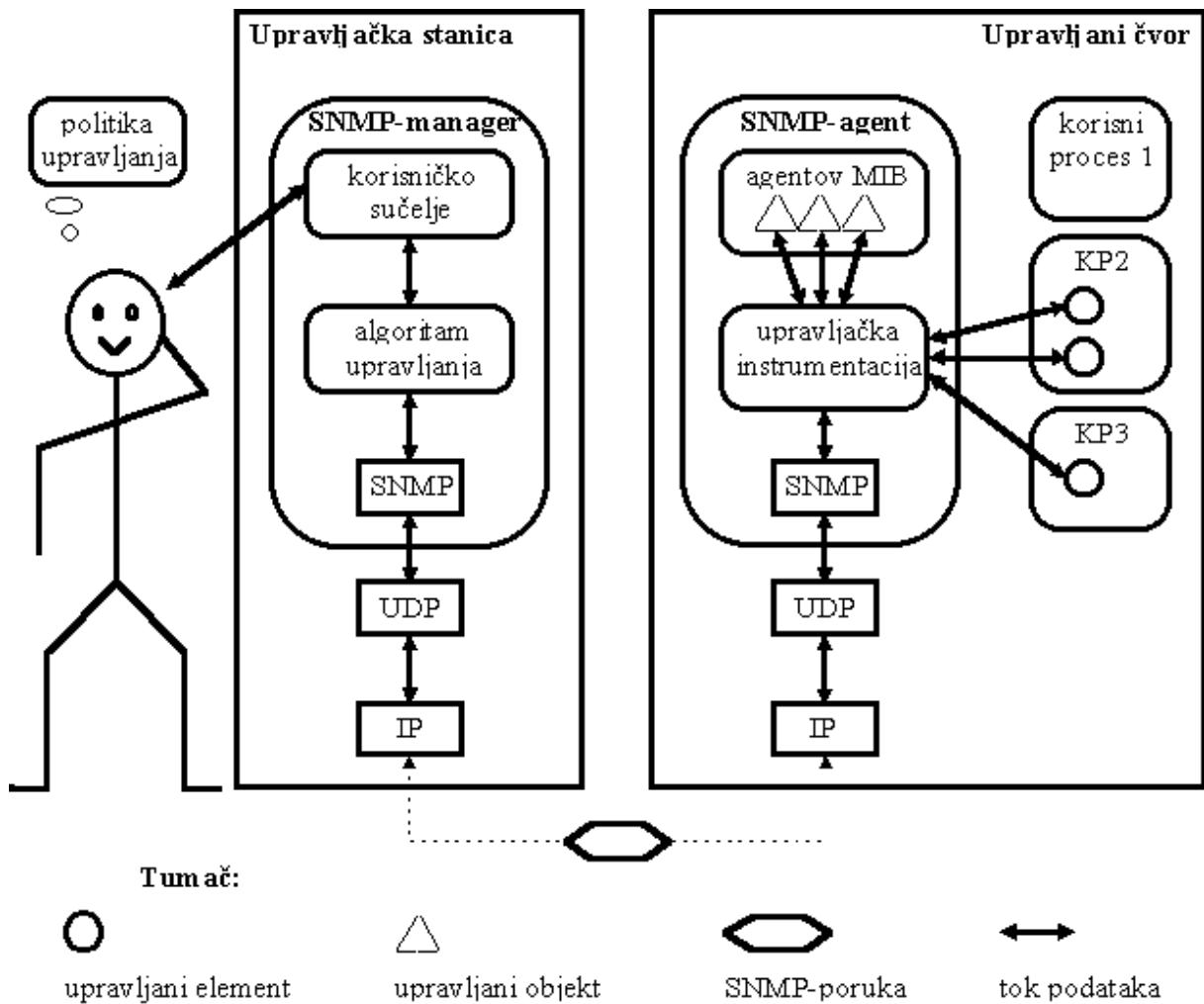
Upravljeni cvor (engl. *managed node*) je mrežni uredaj cija se stanja, ili stanja nekih njegovih dijelova koje nazivamo **upravljeni elementi** (engl. *managed elements*), upravljaju, ili samo nadgledaju. Prema složenosti i funkciji, upravljeni cvorovi mogu biti vrlo raznorodni,

npr. to mogu biti razne vrste mrežnih racunala, poslužioci terminala, ruteri, modemi, mrežni pisaci (engl. *hosts, terminal servers, routers, modems, network printers*).

Upravljacki agent (engl. *agent*) je procesni entitet (program ili dio programa) koji se izvodi na upravljanom cvoru i ima potrebnu **upravljacku instrumentaciju** (engl. *management instrumentation*) kojom može upravljati korisnim funkcijama upravljenih elemenata u upravljanom cvoru. Upravljacka instrumentacija obavlja to upravljanje komunikacijom s upravljanim elementima, tj. njihovim podatkovnim strukturama, i s druge strane predstavlja te podatkovne strukture kao skup upravljenih objekata (vidi niže). U dalnjem tekstu, za upravljacki agent koristit će se naziv SNMP-agent, ili samo agent.

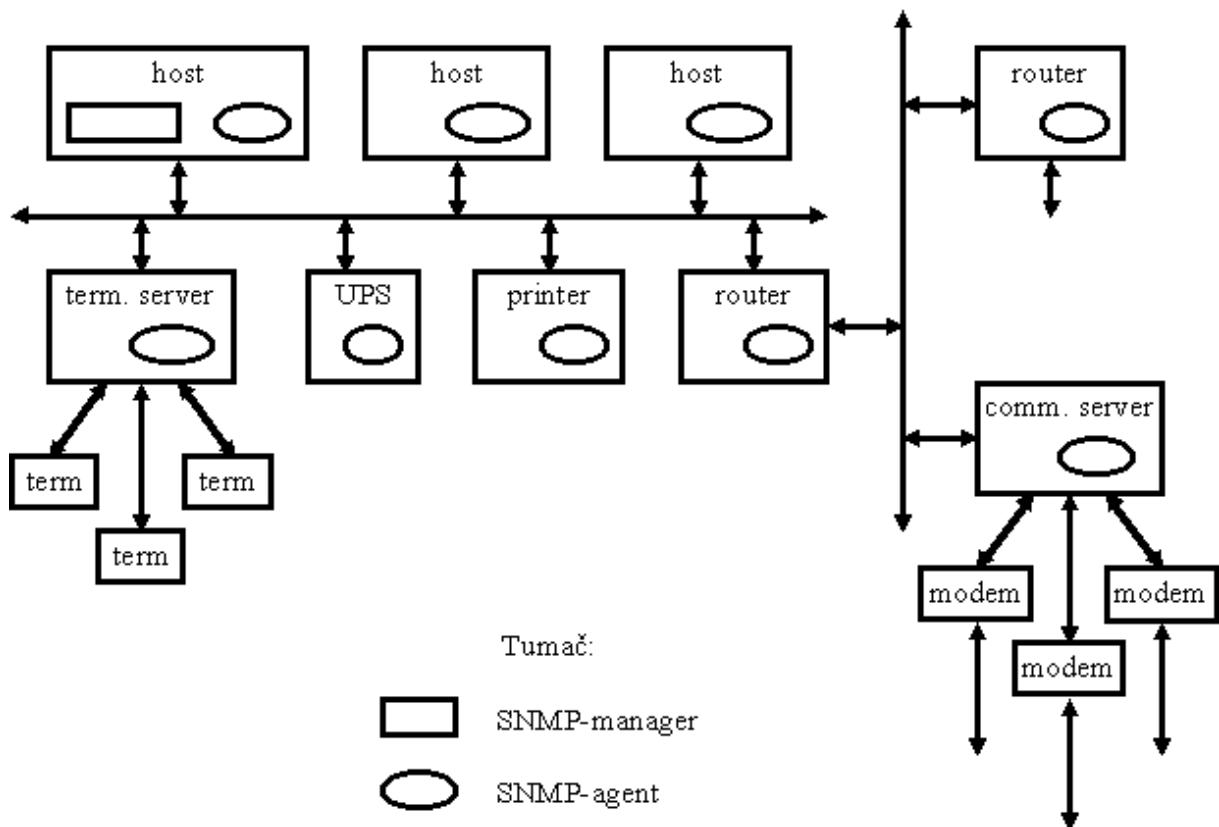
Upravljacke informacije (engl. *management information*) govore o stanjima upravljenih elemenata u upravljanom cvoru. Dohvatom tih informacija SNMP-manager nadgleda stanja upravljenih elemenata, dok postavljanjem njihovih vrijednosti mijenja ta stanja. Upravljacke informacije, koje su fizicki smještene u SNMP-agentima, SNMP-manager vide kao skup **upravljenih objekata** (engl. *managed objects*) smještenih u jednom virtualnom spremištu informacija koje se naziva **baza upravljackih informacija** (engl. *Management Information Base, MIB*). Prijenos upravljackih informacija između SNMP-agenata i managera obavlja se protokolom SNMP.

Navedeni odnosi između osnovnih dijelova jednog upravljackog sustava zasnovanog na protokolu SNMP mogu se prikazati shemom na slici 1.



Slika 1. Sustav za upravljanje mrežom u okviru protokola SNMP

Medutim, jedan stvarni raspored tih dijelova u jednoj lokalnoj racunalskoj mreži vrste internet, mogao bi izgledati kao na slici 2.



Slika 2. Primjer rasporeda dijelova sustava za upravljanje mrežom u jednoj lokalnoj mreži

Na slici 2. važno je uociti da je obično broj SNMP-agenata mnogo veci od broja SNMP-menadžera jer je broj upravljenih cvorova obično mnogo veci od broja upravljackih stanica, tj. cilj je da jedan SNMP- manager upravlja s više upravljenih cvorova.

Dakle, 3 ključne komponente SNMP upravljacke mreže su: upravljeni uredaji, agent i NMS.

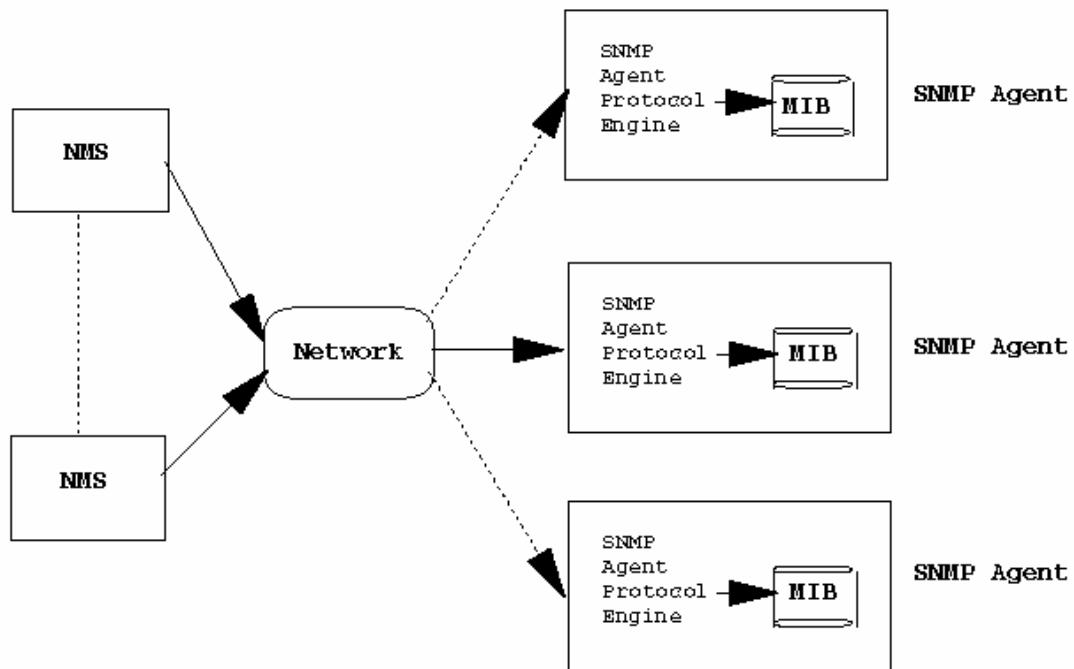
Upravljeni uredaj je mrežni cvor koji sadrži SNMP agenta i koji je smješten na upravljackoj mreži. Uredaj za upravljanje sakuplja i pohranjuje upravljacke informacije i cini ih dostupnima NMS-u preko SNMP protokola. Ti uredaji, ponekad se nazivaju mrežni elementi, mogu biti routers i acces poslužitelji, switchevi i mostovi, hubs, host ili printeri.

Agent je mrežno-upravljacki software modul koji je smješten na uredaju za upravljanje. On ima lokalno znanje o upravljackim informacijama i prevodi te informacije u oblik kompatibilan s SNMP. Omogucava udaljeni pristup opremi za upravljanje.

NMS (eng. *Network Management System*) izvršava aplikacije koje prate i kontroliraju uredajima za upravljanje. NMS osigurava mnoštvo procesnih i memorijskih resursa opremljenih za mrežno upravljanje. Jedan ili više NMS-a moraju postojati na upravljackoj mreži.

Model upravljacke mrežne arhitekture prikazan je na slici 3.

Architecture



Slika 3. Model upravljačke mrežne arhitekture

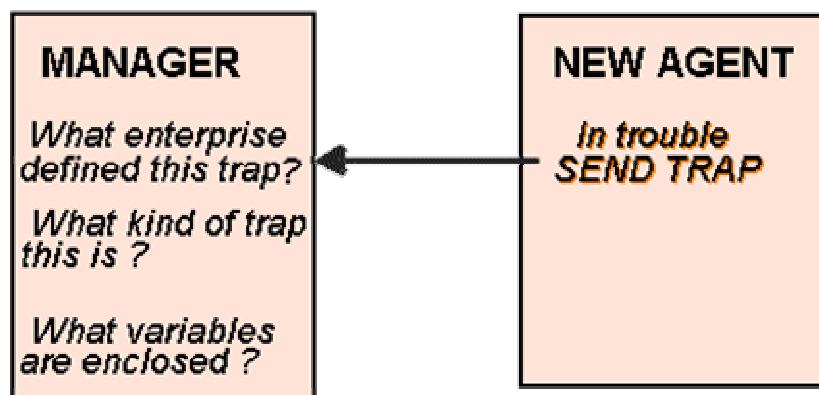
4. Osnovne naredbe SNMP-a

Upravljacki uredaji se nadziru i kontroliraju korištenjem 4 osnovne SNMP naredbe: read, write, trap i traversal operacija.

Read naredba se koristi preko NMS za pracenje upravljackih uredaja. NMS ispituje razlike variable koje se podržavaju preko upravljackih uredaja.

Write naredbu koristi NMS za kontroliranje upravljackih uredaja. NMS mijenja vrijednosti varijablama spremnjanim unutar upravljackih uredaja.

Trap naredbu (tj. alarm poruka koja prijavljuje problem ili znacajniji dogadaj) koriste upravljacki uredaji za izvještavanje NMS-a o asinkronim dogadajima. Kada se dogodi određeni tip dogadaja, upravljacki uredaj pošalje *trap* NMS-u.



Manager dobiva trap poruku

Traversal operacije koristi NMS da bi utvrdio koje variable upravljacki uredaj podržava i da bi sekvenčno sabrao informacije u tablicu kao npr. routing tablica.

5. SNMP Management Information Base

MIB (eng. *Management Information Base*) je skup informacija koji je organiziran hijerarhijski. To je logicka baza upravljackih informacija (tj.definicija) napravljena na temelju konfiguracije i statistickih informacija spremiljenih na uredaju. MIB-u se pristupa preko mrežnog protokola kao što je SNMP. Sastoji se od upravljanih objekata i prepoznaće se pomocu objekt identifikatora .

Svaki upravljeni objekt ima bazu podataka tj vrijednosti za svaku definiciju zapisanu u MIB-u. Postoje dvije vrste upravljanih objekata: skalarni i tablicni. Skalarni objekti definiraju pojedini objekt instance. Tablicni definiraju više povezanih objekt instanci koje su grupirane u MIB tablicu.

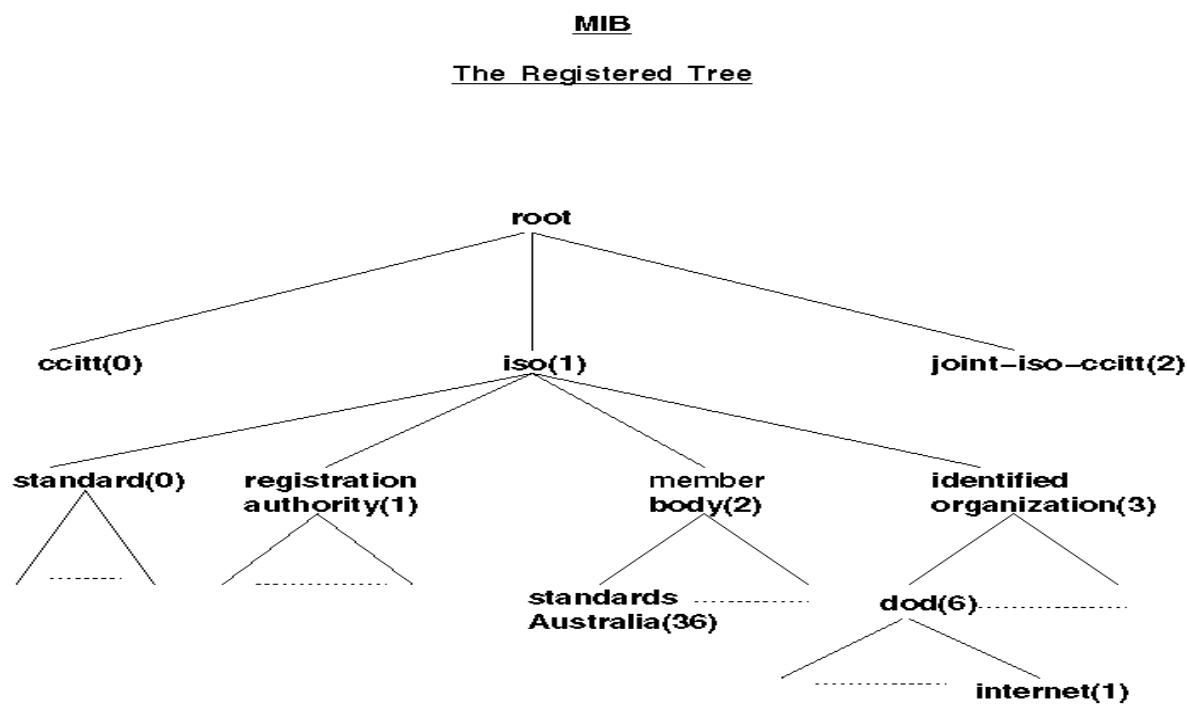
Jedan primjer upravljanih objekata je atInput- to je skalarni objekt koji sadrži pojedinacne objekt instance, integer vrijednost koja pokazuje ukupan broj inputa AppleTalk paketa na router sucelju.

Objekt identifikatori jednoznačno određuju upravljane objekte u MIB hijerarhiji. MIB hijerarhija se može prikazati kao stablo (slika 4.). Djeca i roditelji ne mogu imati iste cjelobrojne vrijednosti. Djeca mogu dalje biti roditelji cineći tako podstablo.

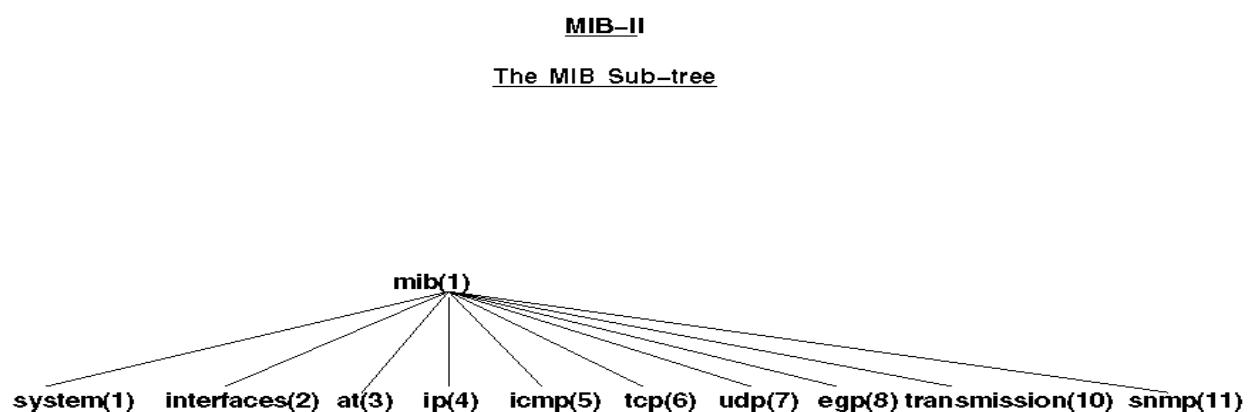
MIB-II standars Internet MIB

MIB-II (RFC 1213) (slika 5.) je trenutna standardna definicija virtualnih datoteka spremiljenih za SNMP upravljane objekte. Ima 10 osnovnih grupa: system, interfaces, at, ip, acmp, tcp, udp, egp, transmission, snmp.

MIB-I i MIB-II imaju istu poziciju na internet podstablu prikazanom na slici 6.



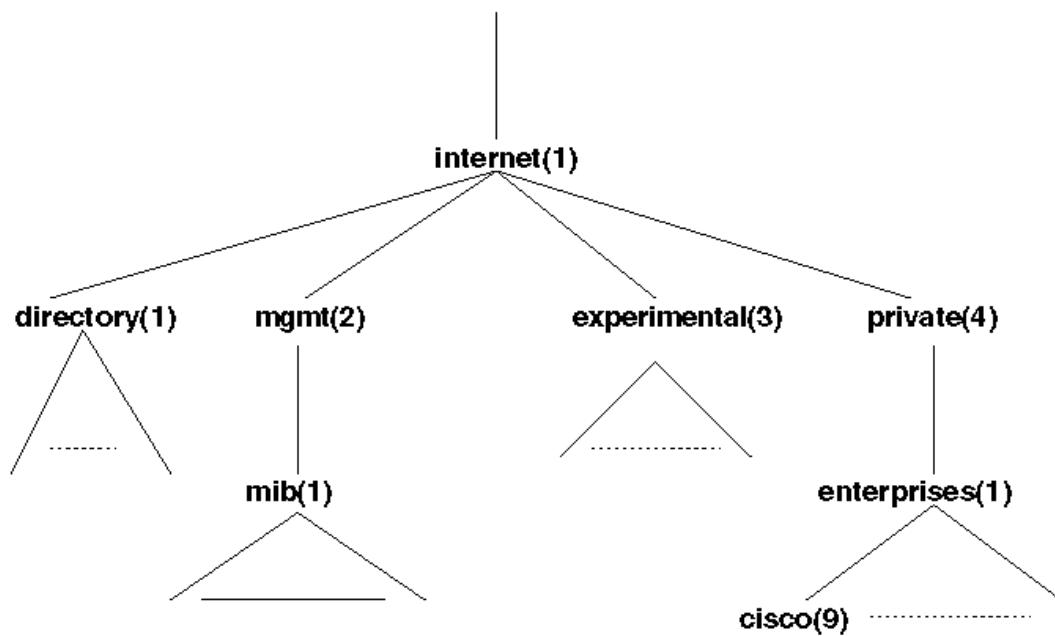
Slika 4. MIB stablo



Note: There is an object **cmot(9)** under the **mib** but it has become almost superfluous and for all intents and purposes is not one of the SNMP manageable groups within **mib**.

Slika 5. MIB-II stablo

The Internet Sub-tree



Slika 6. Internet sub-tree

6. Opis rada

Simple Network Management Protokol SNMP - (RFC 1157/1158) je standardni i vrlo raširen protokol za upravljanje i administriranje mreže koji služi za prikupljanje informacija o subjektima na mreži i šalje ih administratoru. SNMP se naslanja na User Datagram Protocol , UDP (slika 7.). UDP prijenos možemo opisati po sljedecim koracima:

- Agent sluša na UDP portu 161
- Odgovori se šalju na NMS port (neki koristi isti port 161)
- Max velicina SNMP poruke ogranicena je max velicinom UDP poruke
- Sve SNMP implementacije moraju primiti pakete najmanje duljine 484 byte-a
- Ako dođe do greške prilikom prijenosa, prima se poruka na NMS portu 162

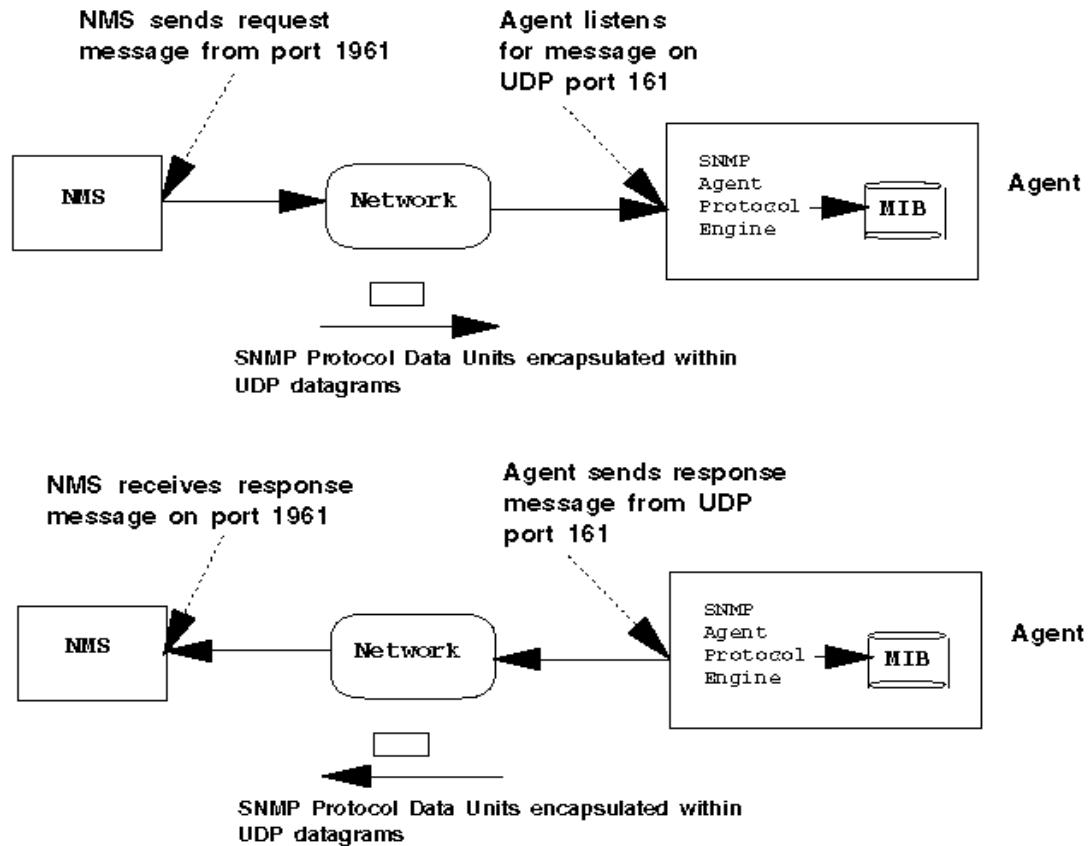
Svaki uredaj u mreži implementira SNMP agenta, točnije programski modul koji prikuplja informacije o tom uredaju u mreži, njegovim karakteristikama, o prometnom opterecenju, grešakama, protoku podataka i sличno.

Upravljacka konzola prikuplja podatke od SNMP agenata na svakom pojedinom upravljivom uredaju i pohranjuje ih na organizirani nacin u bazu podataka koja se naziva Management Information Base (MIB). Zapisi u MIB bazi su jedinstvenog formata tako da SNMP upravljacke jedinice mogu te informacije o upravljivim uredajima u mreži prezentirati sistem administratoru na upravljackoj konzoli.

Neki mrežni uredaji ne raspolažu resursima za odvijanje SNMP agentskog programa pa zbog toga postoje tzv. Proxy agenti tj. uredaji koji obavljaju monitoriranje uredaja i opskrbljuju ga sa SNMP funkcijama (slika 8.).

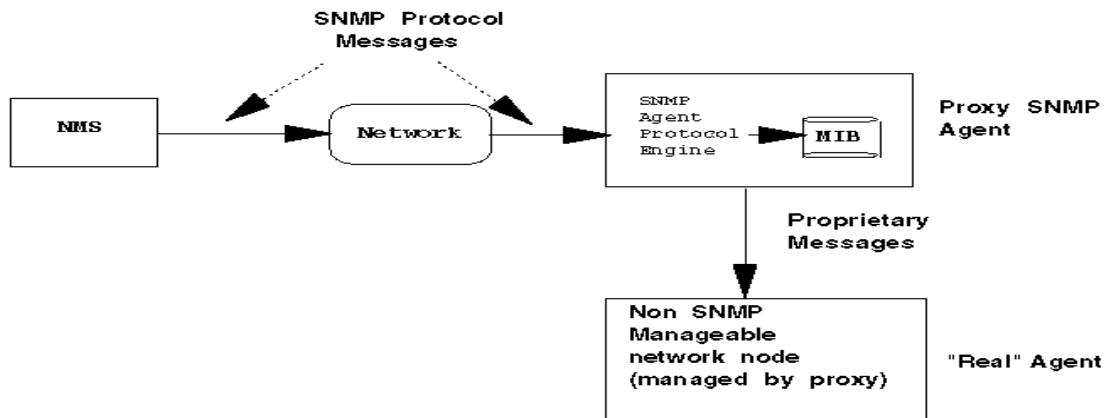
UDP Transport

Normal Send – Response Exchange



Slika 7. Arhitektura UDP prijenosa

Proxy Management of Agent



MIB in Proxy Agent reflects the current management information on the "real" agent, and not the proxy

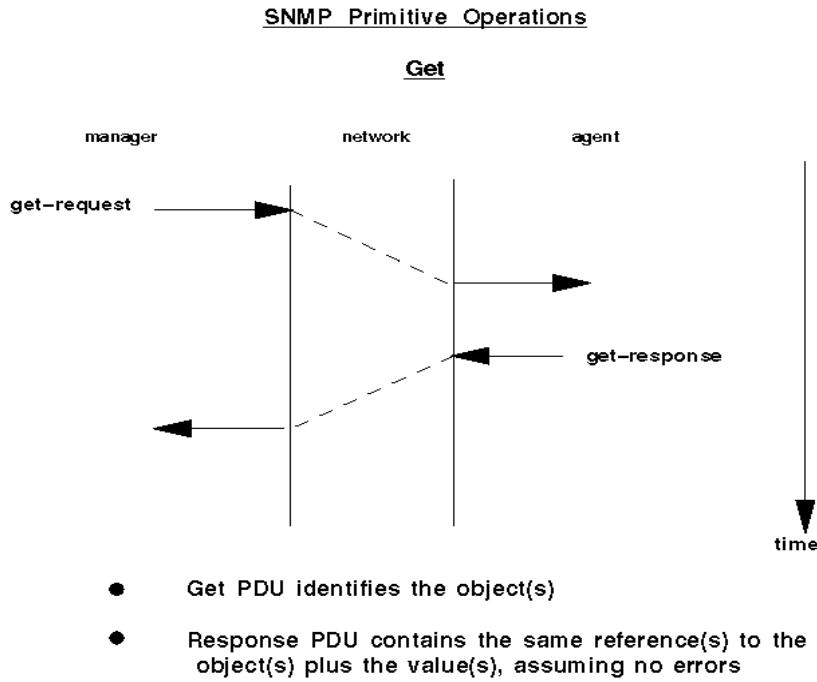
Slika 8. Proxy agent

SNMP se temelji na modelu manager/agent (slika 9.). SNMP je jednostavan jer agent zahtjeva minimalan software. Da bi bio jednostavan, SNMP uključuje ogranicen skup naredbi i odgovora: get, get next, set za dobivanje pojedinačnih ili grupnih varijabli ili za utvrđivanje vrijednosti pojedinačnih varijabli. Agent šalje odgovor na te poruke. Agent također šalje trap poruke upravljačkom sustavu ako je došlo do neke greške.

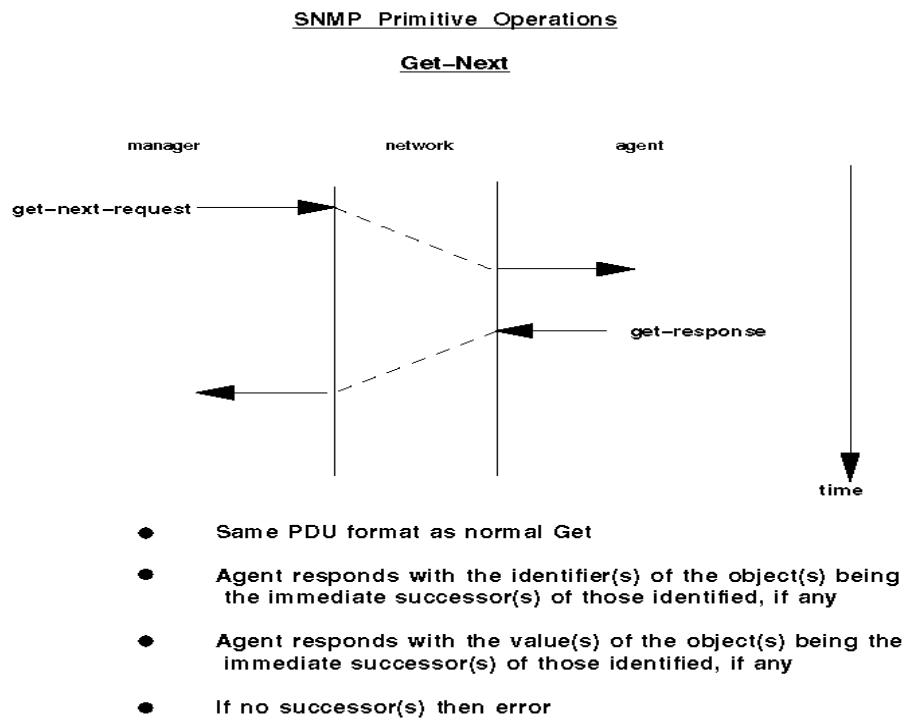
Pet je osnovnih poruka tj. SNMP protokol podatkovnih jedinica (Protocol Data Units):

- **Get request** → poruka koja zahtjeva vrijednost jedne ili više MIB varijabli
- **Get next request** → omogućava manageru da dode do vrijednosti sljедnih vrijednosti. Koristi se za citanje vrijednosti MIB sljednih varijabli; cesto se koristi za citanje redova tablice.
- **Set request** → poruka koja osvježava (update) MIB varijable
- **Get response** → vraca odgovor na get request, get next request ili set request
- **Trap** → poruka koja javlja problem ili znacajan

get (retrieve operation)

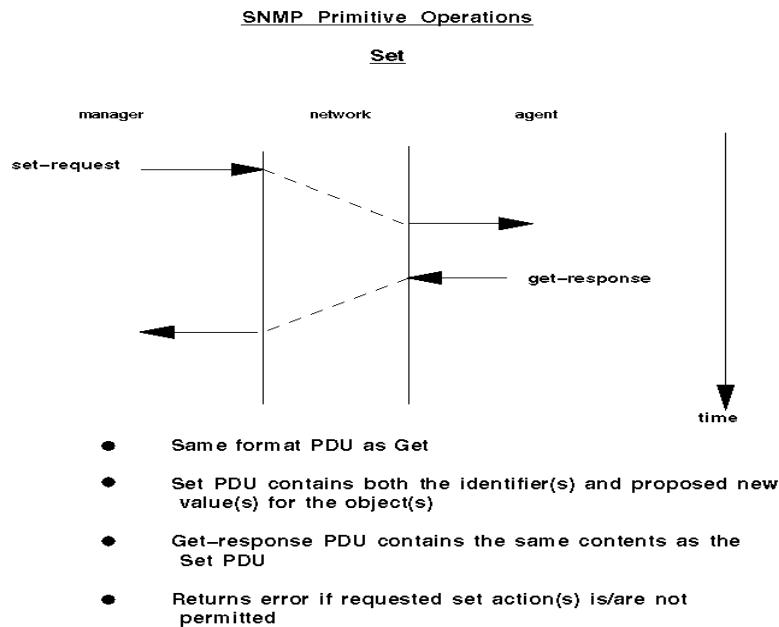


get next (traversal operation)

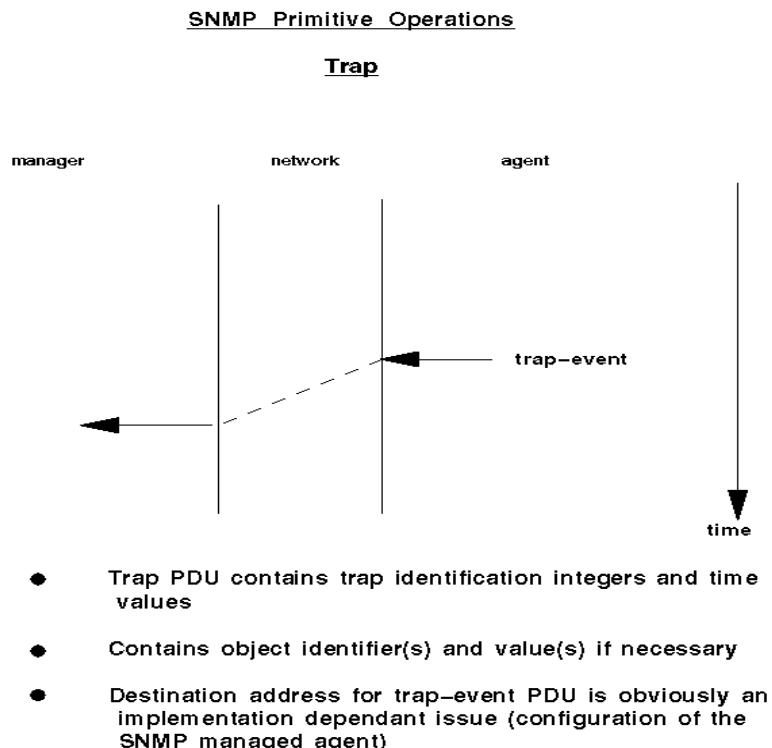


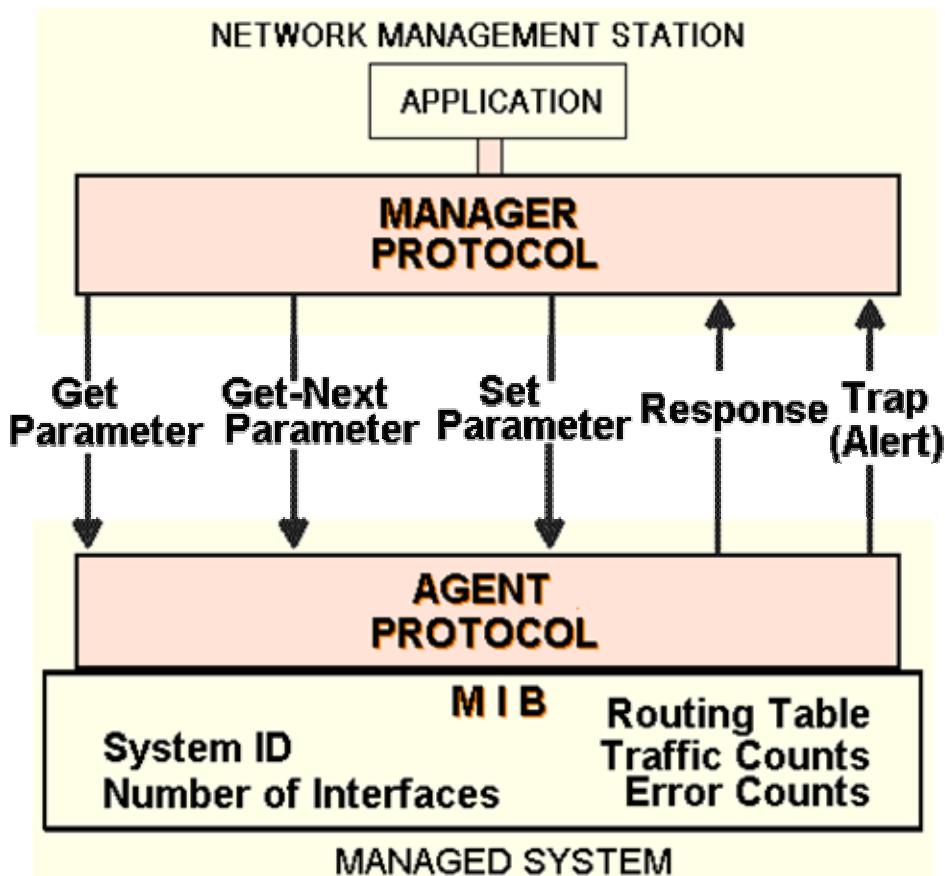
get response (indicative operation)

set (alter operation)



trap (asynchronous trap operation)





Slika 9. Slanje poruke izmedu managera i agenta

Svaka SNMP poruka ima ovakav format:

- Broj verzije
- Password
- Jedan ili više SNMP PDU-autentifikaciju

7. Prednosti SNMP-a

- **Minimalni dizajn.** SNMP je dizajniran da bude mali, jednostavan i da ima najmanje dodira s mrežnom opremom, to je upravljanje.
- **Datagram protokol.** Kad mreža ima problema, najviše trebamo mrežnu upravljivost. Pod ovim uvjetima SNMP nije koneksijski orijentirani protokol jer se bolje ponaša nego koneksijsko orijentirani protokol koji više vremena troši na ponovno uspostavljanje izgubljenih veza nego na prebacivanje podataka.
- **Mogućnost dijagnosticiranja mreže:** SNMP skuplja podatke iz mreže periodično i gleda treba li se nečemu pokloniti pažnja. Ako se zahtjev za odgovorom izgubio, on se s dovoljno znanja nosi sa situacijom.
- **Postavljanje zamke.** Kada nešto krene po zlu, SNMP agent šalje poruku, poznatu kao «zamka» (eng. *trap*), mrežnom manageru da riješi pravi problem.
- **Sigurnost.** SNMP ima sigurnosni mehanizam gdje svaki paket ima oznaku koja označava nivo upravljačke kontrole mrežnog Managera nad mrežnim uređajem. Za nadzor sustava potreban je samo read community right odnosno podaci se samo citaju, a na vecini uređaja SNMP protokol je po default-u enabled
- **Network Management Services.** SNMP odreduje NMS, uključujući instalaciju, održavanje, konfiguraciju, izvođenje i fault management. Korištenjem SNMP protokola, korisnikova mreža se ne zagušuje prometom za potrebe nadzora i upravljanja jer ja kao osnovna namjena protokola upravo NMS.
- **Proxy** može biti SNMP agent koji održava informacije u korist jednog ili više non-SNMP uređaja.