DOI 10.7251/PMG0115046S COBISS.RS-ID 5446680 UDK 004.032.26: 681.324

UPRAVLJANJE MREŽOM U ISO-OSI OKRUŽENJU

Prof.dr Ilija Šušić

Rezime: *Danas broj računarskih mreža u okviru jedne organizacije raste zajedno sa raznorodnim sistemima koji omogućavaju njihovo međusobno povezivanje i povezivanje na Internet (ruteri različitih proizvođača, terminal server..). Sama mreža, njeni resusi i distribuirane aplikacije postaju od neprocenjive vrijednosti za organizaciju. Iz tih razloga upravljanje ovim sistemima je veoma značajno, jer velike mreže ne mogu biti grupisane i administrirane samo od strane ljudi. Kompleksnost takvih sistema diktira korišćenje aplikacija za automatizovano upravljanje računarskim mrežama. Potražnja za takvim aplikacijama stalno se povećava, ali takođe postaje i sve teže isporučiti takve aplikacije, pogotovu ako se mreža sastoji od opreme različitih proizvođača. Međutim, kod kompleksnih računarskih mreža koje čini veliki broj članova često je neophodno, a uz to i veoma komplikovano, predvidjeti moguće probleme, utvrditi da je do problema na mreži došlo i utvrditi njegovu lokaciju i uzrok. Uloga protokola za jednostavno upravljanje mrežom SNMP (engl. Simple Network Management Protocol) jeste da administratorima obezbjedi informacije vezane za rad računarske mreže, a koje je moguće iskoristiti za sprečavanje i rješavanje problema u njenom radu. Za korišćenje SNMP protokola u mreži potrebno je obezbjediti odgovarajuće karakteristike mreže. Protokol SNMP se u mrežama omogućava putem tri tipa komponenata: mrežnih uređaja sa podrškom za upravljanje SNMP-om (engl.managed device),SNMP agenata i sistema za upravljanje mrežom (engl. Network Management System, NMS). Mrežni uređaji sa podrškom za SNMP upravljanje su članovi mreže koji sadrže SNMP agente. Ovi uređaji kreiraju bazu podataka koja sadrži informacije o njihovom radu u proteklom periodu. Podaci iz ove baze su dostupni sistemu za upravljanje mrežom (NMS) putem SNMP protokola. Uloga SNMP agenata je da podatke iz baze podataka mrežnog uređaja prevede u oblikdefinisan SNMP protokolom kao i da kontrolne podatke dobijene od NMS sistema primeni na lokalnom uređaju. Zadatak NMS sistema jeste da informacije dobijene od SNMP agenata analiziraju kao i da kontrolišu mrežne uređaje. rotokol za upravljanje mrežom SNMP razvijen je kao alat za upravljanje mrežama i međusobno povezanim mrežama koje koriste TCP/IP protokol, a kasnije je njegova primjena proširena i na sva ostala mrežna okruženja.*

Ključne riječi:*.računarska mreža, protokol, administrator, agent, upravljanje, okruženje.*

MANAGING THE WEB IN ISO-AXIS ENVIRONMENT

Apstract: *Nowadays, number of computer webs in the field of one organization grows together with different systems that enable their interconnection and Internet connection (rooters of various producers, terminal server...).The web itself, its resources and distributed applications become invaluable for organization. Due to these reasons, managing these systems is very important because great webs cannot be grouped and administered only by people.Complexity of those systems dictates use of applications for automatized managing of computer webs. Requirement for that kind of applications is constantly growing but it is also becoming more and more difficult to deliver those applications especially if the web consists of equipment of various producers. However, when there are complex computer webs made of great number of members it is often necessary ,as well as very complicated , to predict possible problems , determine the problem and identify its location and cause. The role of protocol for simple managing of SNMP web (Simple Network Management Protocol) is to provide administrators with information on the work of computer web. It is possible to use it for preventing and dealing*

with problems in its work. If you want to use SNMP protocol in web it is necessary to provide appropriate web characteristics. Protocol SNMP in webs is provided by 3 types of components: web devices with backup for managing SNMP (managed device), SNMP agents and systems for managing the web (Network Management System, NMS).Web devices with backup for SNMP managing are members that contain SNMP agents. These devices create data base that contains information on their work in the past period. Data from this base are available to system for managing the web (NMS) via SNMP protocol. The role of SNMP agents is to take data from the base of web device and translate into the shape defined by SNMP protocol as well as to apply control data received from NMS system on a local device. The task of NMS system is to analyse information given from SNMP agents and to control web devices. Protocol for managing the web SNMP has been developed as a tool for managing webs and connected webs that use TCP/IP protocol. Later, its application has been widened on all the other web environment.

***Key words**: computer web, protocol, administratror, agent, management, environment*

UVOD

Upravljanje i kontrola moderne mrežne okoline izazovan je zadatak ponajprije zbog kompleksnosti i raznolikosti današnjih mrežnih arhitektura. Standardizacija strategije i tehnika upravljanja stoga je nužna kako bi se omogućilo uspješno kontrolisanje današnjih mreža. Većina arhitektura za upravljanje mrežom zasnovana je na istim principima. Arhitektura tipičnog sistema za upravljanje mrežom (eng. NMS – *Network Management System*) sastoji od entiteta za upravljanje, entiteta kojima se upravlja i skupa veza između njih. Entiteti kojima se upravlja često se nazivaju i krajnje tačke. Oni su obično računari, poslužioci i drugi mrežni uređaji (usmjerivači, preklopnici, vatrozidovi itd.) koji izvršavaju programe, tzv. agente, koji im omogućuju slanje obavijesti prilikom detekcije nekog problema (primjer, ako je zauzeće diskovnog prostora prešlo definisani kritiči nivo). Kada entitet za upravljanje ili više njih prime dojavu o problemu oni reaguju tako da izvedu jednu ili više akcija zavisno o prilagodivosti sistema za upravljanje mrežom. Entiteti za upravljanje pored primanja dojave mogu preuzimati određene podatke s nadziranih sistema. Preuzimanje može biti automatsko ili inicirano od strane korisnika. Programski agenti koji se nalaze na sistemima koji se prate predstavljaju vezu između fizičkog sistema i parametara koje je potrebno kontrolisati te samog sistema za kontrolu. Agenti prilikom prvog pokretanja stvaraju bazu podataka o parametrima koji se kontrolišu na sistemu, pohranjuju je u specijaliziranom obliku i po potrebi šalju potrebne podatke sistemu za kontrolu putem protokola za upravljanje mrežom.

Jedan od najrasprostranjenijih protokola za upravljanje mrežom je SNMP (eng. *Simple Network Management Protocol*). SNMP je mrežni upravljački protokol dizajniran tako da olakša upravljanje i kontrolu kompletne mreže te svih njenih entiteta. Funkcionalnost i implementacija SNMP protokola je relativno jednostavna no ipak dovoljno fleksibilna da pruži mogućnost kvalitetnog upravljanja velikim brojem različitih tipova uređaja u današnjoj distribuiranoj mrežnoj okolini (ISO-OSI okruženje).

Za korišćenje SNMP (Simple Network Management Protocol) protokola u mreži potrebno je obezbjediti odgovarajuće karakteristike mreže. Mreže sa omogućenim SNMP-om se čine tri tipa SNMP komponenti:

- Mrežni uređaji sa podrškom za SNMP upravljanje (eng. *Managed device*).
- SNMP agenti.
- Sistemi za upravljanje mrežom (eng. *Network Management System*, NMS).

Mrežni uređaji sa podrškom za SNMP upravljanje su članovi mreže koji sadrže SNMP agente. Ovi uređaji kreiraju bazu podataka koja sadrži informacije o njihovom radu u proteklom periodu. Podaci iz ove baze su dostupni sistemu za upravljanje mrežom (NMS) putem SNMP protokola. Uloga SNMP agenata je da podatke iz baze podataka mrežnog uređaja prevede u oblik definisan

SNMP protokolom kao i da kontrolne podatke dobijene od NMS sistema primjeni na lokalnom uređaju. Zadatak NMS sistema jeste da informacije dobijene od SNMP agenata analiziraju kao i da kontrolišu mrežne uređaje. U jednoj SNMP mreži se može nalaziti i više NMS sistema. Takođe, s obzirom na hijerarhijsku strukturu SNMP mreža, jedan mrežni uređaj može istovremeno funkcionisati i kao SNMP agent i kao NMS.

U radu će biti objašnjeni osnovni koncepti SNPA, arhitektura SNMP protokola, njegov istorijski razvoj, bezbjednost i budućnost.

1. OSNOVNI KONCEPTI SNMP PROTOKOLA

Za potrebe upravljanja aktivnim mrežnim uređajima u računarskim mrežama razvijen je aplikacijski protokol **SNMP (***Simple Network Management Protocol).* Njegova funkcija je prikupljanje i organiziranje primljenih informacija o stanju računarske mreže. SNMP protokol mrežnom administratoru omogućuje nadgledanje performansi te pronalaženje i rješavanje mrežnih problema. Protokol SNMP je dio sistema za upravljanje mrežom – NMS (eng. *network management system NMS*).

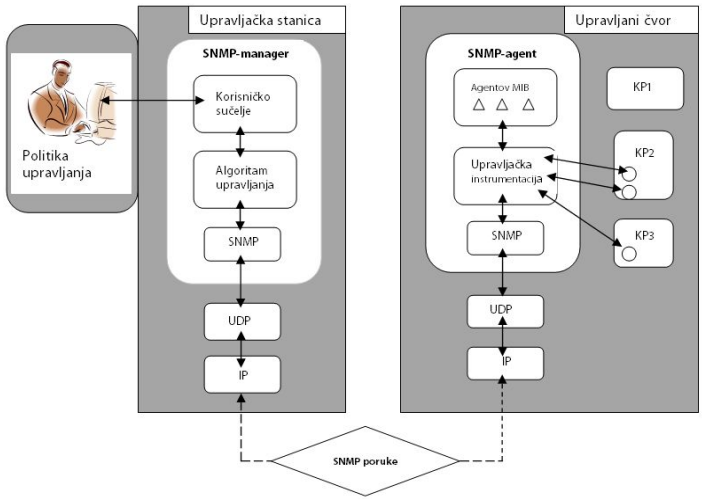
Network management system - NMS je sastavljen od jedne ili više upravljačkih stanica na kojima se izvode upravljačke aplikacije te od nekoliko upravljanih čvorova na kojima se izvode upravljački agenti. Prenos upravljačkih informacija između SNMP-agenata i SNMP *managera* obavlja se SNMP protokolom.

Navedeni odnosi između osnovnih dijelova upravljačkog sistema zasnovanog na protokolu SNMP prikazani su shemom na slici 1. [Douglas R. Mauro, Kevin J. Schmidt 2005.].

Sistem za upravljanje mrežom je kolekcija alata za nadgledanje i upravljanje mrežom:

- jedan interfejs sa moćnim, ali lakim za korišćenje skupom komandi za izvršavanje većine upravljačkih zadataka,
- minimalna količina dodatne opreme tj., većina hardvera i softvera potrebnog za upravljanje meržom uključeno je u postojeću korisničku opremu.

Sistem za upravljanje mrežom sastoji se od dodatnog hardvera i softvera implementiranih u postojaće mrežne komponente. Softver koji se koristi za izvršavanje zadataka upravljanja mrežom nalazi se u krajnjim stanicama i komunikacionim opremi (npr. komutatorima, ruterima..). Sistem za upravljanja mrežom projektovan je tako da vidi mrežu kao jedinstvenu arhitekturu sa adresama i oznakama koje su dodeljenih svakoj tački i specifičnim karakteristikama svakog elementa i svake veze za koju sistem zna. Aktivni elementi u mreži redovno obezbeđuju statusne informacije upravljačkom centru mreže.



Slika 1. Sistem za upravljanje mrežom u okviru SNMP protokola

Cijeli sistem funkcioniše pomoću niza upravljačkih naredbi. Upravljanje računarom mrežom može se definisati kao usluga koja se dodaje u postojeću računalnu mrežu da bi se olakšalo upravljanje pojedinim dijelovima mrežnog sistema i mrežom kao cjelinom na jednom od sledećih područja:

- upravljanje greškama, tj. otkrivanje i dojava grešaka u sistemu,
- upravljanje konfiguracijom,
- upravljanje performansama,
- upravljanje bezbjednošću,
- upravljanje uslugama i
- upravljanje obračunavanjem troškova.

Upravljačka stanica je računar sa primarnom namjenom za komunikaciju putem računarske mreže. Računarska mreža može biti organizovana lokalno kao LAN mreža ili globalna Internet mreža. Procesna sposobnost upravljačke stanice je dovoljna za izvođenje upravljačkih aplikacija. Upravljačka aplikacija **(**često se naziva i SNMP *manager)* je računarski program koji nadgleda ili upravlja elementima na upravljanim čvorovima mreže u skladu s politikom upravljanja koja je određena od strane rukovodioca računarske mreže (najčešće mrežnog administratora). Upravljani čvor (eng. *Managed node*) je mrežni uređaj čijim se stanjima upravlja ili ih se samo nadgleda. Zavisno o stanju mrežnog uređaja upravljačka stanica može s njim izvesti neku akciju na mreži ili joj to može biti onemogućeno. Prema složenosti i funkciji, upravljani čvorovi mogu biti vrlo raznorodni. Na primjer, to mogu biti razne vrste računara na mreži, mrežni poslužioci, usmjerivači, modemi ili mrežni pisači. Upravljački agent je procesni entitet (program ili dio programa) koji se izvodi na upravljanom čvoru i sadrži potrebnu instrumentaciju kojom upravlja funkcijama kontrolisanih elemenata u čvoru. Upravljačka instrumentacija diriguje komunikacijom s upravljanim elementima (eng. *managed elements*), tj. njihovim podatkovnim strukturama. S druge strane, ona predstavlja te podatkovne strukture kao skup upravljanih objekata. U daljnjem tekstu, za upravljački agent koristit će se uobičajeni naziv - SNMP-agent. Upravljačke informacije govore o stanjima upravljanih elemenata u upravljanom čvoru. Dohvatom tih informacija SNMP *manager* nadgleda stanja upravljanih elemenata, dok postavljanjem njihovih vrijednosti mijenja ta stanja. Upravljačke informacije, koje su fizički smještene u SNMP agentima, SNMP *manageri* vide kao skup upravljanih objekata smještenih u jednom virtualnom skladištu informacija koje se naziva baza upravljačkih informacija - MIB (eng. *Management Information Base*). MIB datoteka sadrži definiciju skupa objekata upravljanih SNMP-om.

2. ISTORIJSKI RAZVOJ SNMP PROTOKOLA

U aprilu 1988. objavljen je RFC 1052 (*Request For Comments*) - skup dokumenata koji sadrže Internet protokole i diskusije. Taj RFC je specifikacija za standardizovano mrežno upravljanje u kojoj su objašnjeni zahtjevi za mrežno upravljanje.

RFC dokumenti koji su inicijalno opisivali SNMP protokol (objavljeni 1988. godine) su:

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

Sedamdesetih godina i u prvoj polovini osamdesetih godina prošlog vijeka u mrežama koje koriste TCP/IP protokole nisu bili implementirani protokoli upravljanja mrežnom opremom. Za potrebe upravljanja bio je korišten protokol ICMP (eng. *Internet Control Message Protocol*). ICMP protokol omogućava prenos upravljačkih poruka između računara i upravljanih mrežnih uređaja (drugi računari, usmjerivači i dr.).

Koristeći ICMP i različita zaglavlja IP paketa moguće je razviti jednostavne i moćne alate za upravljanje mrežom (PING, i sl.), no čak ni ti alati ne pružaju dovoljno kvalitetnu funkcionalnost za upravljanje složenim mrežama. Iz tih razloga je 1987. godine razvijen protokol SGMP (eng. *Simple Gateway Monitoring protocol*), namijenjen kontroli usmjerivača. Rastući zahtjevi i brz razvoj tada već složenih TCP/IP mreža, otežavali su mrežno upravljanje. To sve je uslovilo daljnji razvoj i poboljšanje protokola SGMP te je time nastao protokol SNMP. Istorijski od 1988. godine do danas razvijene su tri varijante protokola SNMP.

2.1. VARIJANTE SNMP PROTOKOLA

Danas postoje tri verzije SNMP protokola koje su u upotrebi:

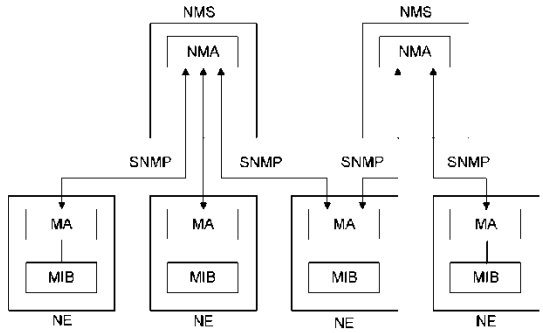
- **SNMPv1** - u upotrebi od 1988. godine → RFC 1157
- **SNMPv2** - u upotrebi od 1995. godine → RFC 1901 – 1908
- **SNMPv3** - u upotrebi od 1998. godine → RFC 2271 – 2275

2.1.1. PROTOKOL ZA UPRAVLJANJE MREŽOM VERZIJA SNMPV1

Protokol za upravljanje mrežom SNMP (Simple Network Management Protocol) razvijen je kao alat za upravljanje mrežama i međusobno povezanim mrežama koje koriste TCP/IP protokol. Kasnije je njegova primena proširena i na sva ostala mrežna okruženja. Naziv protokol za upravljanje mrežom ukazuje na skup specifikacija za upravljanje mrežom koja uključuje i sam protokol kao i definiciju i koncept baze podataka.

Model upravljanja mrežom prikazan na slika 2. obuhvata sledeće ključne elemente [Andrew S. Tanenbaum, David J. Wetherall. 2013.]:

- upravljačka stanica (menadžer - stanica),
- aplikacija za upravljanje,
- elemenat računarske mreže,
- agent,
- baza podataka za upravljanje,
- protokol za upravljanje mrežom.



Slika 2. SNMP - komponente sistema za upravljanje mrežom

NMS - *Network Management Station* *MA - Management Agent*

NMA - *Network Management Application* *MIB - Management Information Base*

NE - *Network Element*

Komunikacija može biti dvostrana:

- menadžer traži od agenta odgovor o specifičnoj promjenljivoj. Na primjer koliko je ICMP poruka tipa „port je nedostupan" je poslao;
- agent obavještava menadžera da se nešto važno desilo. Na primjer „mrežni interfejs" je u kvaru;
- menadžer može da očita ili postavi vrijednost neke promjenljive kod agenta Na primjer „promjeni podrazumjevanu vrijednost polja TTL u IP zaglavlju na 64".

Upravljačka stanica je obično poseban, samostalan uređaj ali se može realizavati i kao dio drugog sistema. U oba slučaja upravljačka stanica služi kao interfejs čovjeka-menadžera i upravljačkog sistema mreža. Upravljačka stanica treba da sadrži:

- skup upravljačkih aplikacija koje se koriste za analizu podataka, oporavak od grešaka itd.,
- interfejs preko koga menadžer nadzire i upravlja mrežom,
- mogućnost sprovođenja zahteva menadžera mreže u procesu nadzora i upravljanja udaljenih elemenata mrežne,
- bazu podataka sa informacijama o upravljanju mrežom dobijenih iz baza svih upravljivih cjelina u mreži.

SNMPv1 protokol je prihvaćen kao standard u TCP/IP mrežama od 1988. godine. Još i danas se dosta koristi iako ima određene bezbjedonosne nedostatke. Bezbjednost se kod SNMPv1 zasniva na korištenju takozvanih zajedničkih znakovnih nizova (eng. *community string*). *Community string* je u stvari niz tekstualnih ASCII znakova i podsjeća na tradicionalne lozinke koje se koriste u operativnim sistemima. Koristi se za autentikaciju SNMP poruka između upravljačke jedinice i upravljanog uređaja. Najveći problem je što se ne koristi nikaka**v** oblik enkripcije pa neovlašteni korisnici mogu snimanjem IP paketa koji se prenose mrežom pročitati sadržaj SNMP poruka, a samim time i *community string*. Poznavajući taj podatak, zlonamjerni korisnici mogu pristupiti upravljačkim informacijama nekog mrežnog uređaja i promijeniti njegovu konfiguraciju.

Varijanta 1.0, objavljena u maju 1991. godine, obuhvatala je sledeće RFC dokumente :

- RFC 1155 - struktura i identifikacija upravljačkih informacija za TCP/IP te struktura i identifikacija
- upravljačkih informacija za objekte,
- RFC 1212 - MIB definicije,
- RFC 1213 - baza upravljačkih informacija za mrežno upravljanje MIB-2 i

– RFC 1157 (*Simple Network Management Protocol*) - SNMP protokol, definiše: poruke koje se mogu razmjenjivati između upravljačkih entiteta i upravljačkih stanica (poruke omogućavaju čitanje i obnavljanje vrijednosti), alarm poruke (trap), format poruka i komunikacijski protokol.

Druga varijanta, SNMPv2, donijela je određena poboljšanja u odnosu na prvu, ali su problemi bezbjednosti ostali i dalje prisutni.

2.1.2. PROTOKOL ZA UPRAVLJANJE MREŽOM VERZIJA SNMPV2

U aprilu 1993. godine varijanta 2.0 postala je standard. Ta varijanta nudi dodatne mogućnosti kao što su bezbjednost i autentikacija. SNMP varijanta 2 je dokumentovana u nekoliko RFC dokumenata:

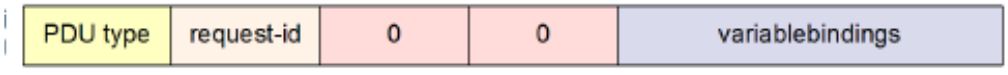
– RFC 1902 - MIB struktura,
– RFC 1903 - tekstualne konvencije (promjene i novosti u SNMP inačici 2),
– RFC 1904 - izjave sukladnosti s SNMPv1 (kooperativnost SNMP inačica 1 i 2),
– RFC 1905 - protokol operacija,
– RFC 1906 - transport, mapiranje i
– RFC 1907 - MIB.

SNMPv2 predstavlja proširenje protokola SNMPv1 te podržava tri načina pristupa upravljačkoj informaciji:

– **upravljač-agent zahtjev-odgovor:** SNMPv2 upravljač šalje zahtjev agentu, a agent odgovara slanjem traženih upravljačkih informacija. Koristi se za dohvatanje i modificiranje upravljačkih informacija;
– **upravljač-upravljač zahtjev-odgovor:** jedan SNMPv2 upravljač šalje zahtjev drugom upravljaču, a drugi odgovara slanjem traženih upravljačkih informacija;
– **agent-upravljač bez potvrde:** SNMPv2 agent šalje poruku „*Trap*“ upravljaču.

2.1.3. RAZLIKE IZMEĐU PROTOKOLA SNMPV1 I SNMPV2

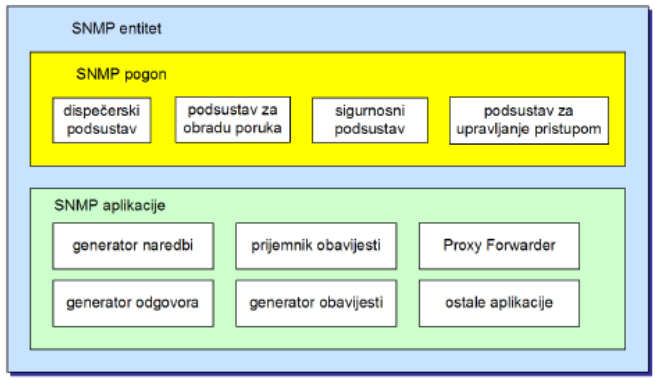
SNMPv1 podržava prvi i treći način pristupa upravljačkim informacijama. Samo je drugi način specifičan za SNMPv2. Komunikaciju između upravljača omogućava mehanizam informiranja. Porukom *Inform* jedan upravljač obavještava drugog o upravljačkoj informaciji koju posjeduje. Operaciju *Inform* pokreće upravljač pošiljalac slanjem *InformRequest* PDU-a (eng. *Packet Data Unit*) upravljaču primaocu. Na slici 3. prikazan je format poruke *InformRequest* PDU-a [SNMP protocol wiki]. Upravljač primalac potvrđuje prijem PDUa slanjem *Response* PDU-a upravljaču pošiljaoca. SNMPv2-Trap PDU ima drugačiji format od Trap PDU-a korištenog u SNMPv1. Format SNMPv2-Trap PDU je identičan formatu *GetRequest, GetNextRequest SetRequest i InformRequest* PDU-a korištenih u SNMPv2. Poruke *GetRequest, GetNextRequest i SetRequest* su zadržale isti format kao u prvoj varijanti protokola SNMP, no SNMPv2 predviđa i uvođenje *Report* PDU-a u upotrebu, ali njegov tačan način korištenja i semantika još nisu u potpunosti definisani. Saradnja i postojanje SNMPv1 i SNMPv2 unutar jednog NMS-a je moguća te za njihovu saradnju postoje jasna pravila unutar dvije kategorije: upravljačka informacija i protokol.



Slika 3.: SNMPv1 konfiguracija

2.1.4. PROTOKOL ZA UPRAVLJANJE MREŽOM VERZIJA SNMPV3

Protokol SNMPv3 posjeduje bitno poboljšane bezbjedonosne mehanizme. Posebno treba izdvojiti mehanizme za autentikaciju, tj. provjeru vjerodostojnosti korisnika i zaštitno kodiranje SNMP poruka, odnosno enkripciju. SNMPv3 može koristiti takozvanu korisničku (*user-based*) autentikaciju (autentikaciju na osnovu korisničkog imena i lozinke) ili se provjera vjerodostojnosti korisnika može obaviti bez slanja lozinki u čitljivom obliku. Takva provjera vjerodostojnosti se zasniva na upotrebi algoritama HMAC-MD5 (eng. *Hash-based Message Authentication Code- Message-Digest algorithm 5*) ili HMACSHA (eng. *Hash-based Message Authentication Code -Secure Hash Algorithm*). MD5 i njegov nasljednik SHA su algoritmi za provjeru autentičnosti datoteka ili poruke prilikom prenosa između pošiljaoca i primaoca. Zaštitna enkripcija koristi 56-bitni CBC-DES (eng. *Cipher Block Chaining-Data Encryption Standard*) algoritam za kodiranje i dekodiranje SNMP poruka. Najvažnija promjena u SNMPv3 je napuštanje koncepta NMS-a koji sezasniva na upravljačima i agentima. SNMPv3 NMS čine SNMP entiteti, prikazani na slici 4. [Douglas R. Mauro, Kevin J.Schmidt 2005.].



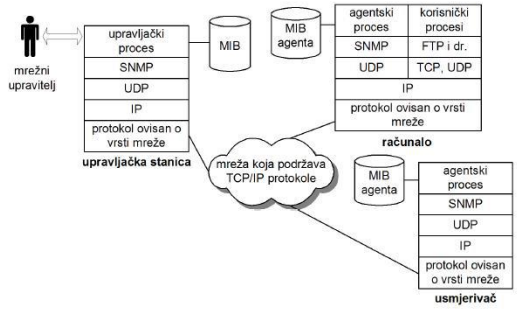
Slika 4. SNMP entitet

Novi koncept definiše arhitekturu NMS-a, a ne samo skup poruka kao ranije varijante. Svaki se entitet (slika 4.) sastoji od SNMP pogona (eng. *SNMP engine*) i SNMP aplikacija. SNMP pogon se sastoji od 4 podsistema. Dispečerski podsistem (eng. *Dispatcher Subsystem*) šalje i prima SNMP poruke (u prijemu određuje varijantu svake primljene poruke). Podsistem za obradu poruka (eng. *Message Processing Susbsystem*) priprema SNMP poruke za slanje drugim entitetima i obrađuje podatke iz SNMP poruka primljenih od drugih entiteta. Bezbjedonosni podsistem (eng. *Security Subsystem*) pruža usluge autentifikacije i zaštite privatnosti upravljačkih informacija (enkripcija). Autentifikacija koristi mehanizam zajedničkih znakovnih nizova (eng. *community string*), ako se radi o SNMPv1 ili SNMPv2 porukama, odnosno SNMPv3 korisničku autentikaciju (mehanizmi autentikacije navedeni iznad slike 4.). Podsistem za upravljanje pristupom (eng. *Access Control Subsystem*) je odgovoran za upravljanje pristupom objektima MIB-a. Pomoću tog podsistema moguće je upravljati pristupom korisnika pojedinim objektima (kojim objektima korisnik smije pristupiti i koje operacije smije nad pojedinim objektom izvoditi). Drugi dio entiteta su SNMP aplikacije:

- generator naredbi - generira **get**, **getnext**, **get-bulk** i **set** zahtjeve, te obrađuje odgovore (implementira se u upravljačkoj stanici);
- generator odgovora - šalje odgovore na **get**, **get-next**, **getbulk** i **set** zahtjeve (implementira se u upravljanim mrežnim uređajima);
- generator obavijesti - generira SNMP **trapove** i obavijesti,
- prijemnik obavijesti - prima **trap** i **inform** poruke, a **proxy forwarder** olakšava prosljeđivanje SNMP poruka između entiteta.

3. ARHITEKTURA SNMP NMS-A

Protokol SNMP je dizajniran kao protokol aplikacijskog sloja OSI modela [Wikipedia: OSI model,http://en.wikipedia.org/wiki/OSI_model]. Na transportnom sloju SNMP koristi transportnu uslugu protokola UDP (eng. *User Datagram Protocol*). UDP višim protokolnim slojevima pruža bespolnu (eng. *connectionless*) uslugu transporta informacija, jer uređaj koji primi UDP datagram ne potvrđuje prijem pošiljaocu. Na taj se način ubrzava prenos i smanjuje količina prenesene informacije. U slučaju SNMP-a to je izuzetno važno jer je osnovni cilj NMS-a utemeljenog na protokolu SNMP (SNMP NMS) bio taj da upravljački protokol svojim porukama što manje opterećuje mrežu. Prikaz arhitekture SNMP NMS-a dan je na slici 5. [William Stallings 2007.]. Na upravljačkoj stanici pokrenut je proces koji upravlja pristupom središnjem MIB-u instaliranom u SNMP *manageru*, te pruža interfejs prema mrežnom upravitelju, osobi koja je zadužena za obavljanje poslova vezanih uz upravljanje mrežom (najčešće mrežnom administratoru). Agentski proces interpretira primljene SNMP poruke i upravlja pristupom MIB-u agenta.



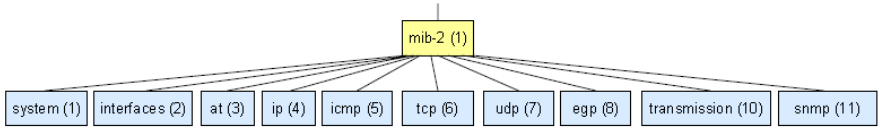
Slika 5. Arhitektura SNMP NMS-a

3.1. BAZA UPRAVLJAČKIH INFORMACIJA - MIB

Svaki SNMP agent sadrži popis svih svojih upravljanih objekata koji se naziva baza upravljačkih informacija. Baza sadrži sledeće zapise:

- ime,
- OID,
- tip podatka,
- dozvole čitanja i pisanja te
- kratki opis za svaki objekt SNMP agenta.

Pomoću informacija o objektu i vrijednosti pojedine instance – varijable, SNMP *manager* može slati SNMP poruke za dohvat ili postavljanje pojedine varijable SNMP agenta. Objekti namijenjeni upravljanju putem SNMP protokola grupirani su u deset grupa, od kojih svaka odgovara jednom čvoru u SMI stablu Navedenih deset čvorova su podstabla čvora *mib-2* data na slici 6. [Šušić, I 2014.].



Slika 6 : Čvor mib-2 SMI stabla

Mib-2 odgovara varijanti SNMPv2 i stoga objekt *cmot* čiji je OID jednak 9 nije više prisutan u SMI stablu. CMOT (CMIP over TCP/IP) je protokol koji se 1989. godine razvijao zajedno sa

SNMP protokolom, no zbog prevelike složenosti u implementaciji, IAB (*Internet Architecture Board*) je 1989. godine odlučio da se protokoli SNMP i CMOT nastave razvijati odvojeno s ciljem očuvanja jednostavne implementacije protokola SNMP. Spomenutih deset grupa upravljanih objekata predstavlja osnovni sadržaj koji bi svaka upravljačka stanica morala razumjeti. Grupa *system* omogućava upravljaču da odredi ime, lokaciju i opis mrežnog uređaja (naziv proizvođača, interfejs i programske pakete koje uređaj sadrži, namjena uređaja i dr.). Grupa *interfaces* odnosi se na mrežne interfejse i priključke na mrežnim uređajima (*ports)*. Grupa *at* pruža informacije o preslikavanju adresa (npr. Ethernet u IP adrese). Grupa *ip* je namijenjena prikupljanju informacija o IP prometu koji ulazi ili izlazi iz mrežnog čvora. Ova je grupa posebno važna za usmjerivače. Grupa *icmp* se odnosi na ICMP poruke o greškama u komunikaciji. Za svaku ICMP poruku definisana je posebna varijabla koja sadrži broj primljenih relevantnih ICMP poruka. Grupa *tcp* nadzire broj trenutno aktivnih TCP veza, kao i kumulativni broj TCP veza, broj primljenih i poslanih TCP segmenata te statistiku grešaka. Grupa *udp* je zadužena za praćenje broja primljenih i poslanih UDP datagrama i sličnih informacija. Grupa *egp* se primjenjuje u usmjerivačima koji podržavaju protokol EGP (*Exterior Gateway Protocol*). Grupa *transmission* je prazna grupa koja čuva mjesto u stablu za MIB-ove specifične za pojedinu vrstu mreže (npr. *Ethernet*). Grupa *snmp* je namijenjena prikupljanju statistike o djelovanju samog protokola SNMP (broj poslanih SNMP poruka, vrste poruka i sl.).

Struktura upravljačkih informacija SMI definiše opšti okvir unutar koga se definiše i konstruiše baza podataka MIB. SMI identifikuje tipove podataka koji se mogu koristiti u MIB bazi podataka kao i na koji način su resusrsi u njoj predstavljeni i označeni. Osnovna koncepcija strukture upravljačkih informacija SMI je jednostavnost i mogućnost proširivanja MIB baze podataka. Prema tome, MIB može da skladišti samo proste tipove podataka: skalare i dvodimenzione matrice (tabele). Struktura upravljačkih informacija SMI ne podržava stvaranje i pronalaženje kompleksnih struktura podataka. Ovakav princip nije u skladu sa onim koji se koristi kod sistema za upravljanje u okviru OSI okruženja kod koga se složena funkcionalnost postiže sa kompleksnim strukturama podataka i složenim pretraživanjem. SMI izbjegava kompleksne tipove podataka da bi se pojednostavila implementacije i rad sa drugim sistemima. MIB će svakako sadržati tipove podataka koje su kreirali sami proizvođači i dok se ne postave stroga pravila vezane za definisanje tipova podataka međusobno povezivanje sistema različitih proizvođača (interoperabilnost) neće biti moguća.

Tri ključna elementa se nalaze u SMI specifikaciji. Na najnižem nivou SMI određuje tipove podataka koji mogu da se skladište. Zatim SMI određuje tehniku za definisanje objekata i njihovih tabela. Konačno, SMI obezbjeđuje šemu za povezivanje jedinstvenih oznaka sa svakim stvarnim objektom u sistemu tako da podatke i agente mogu menadžeri referencirati.

U tabela 1. prikazuje tipove podataka koje SMI dozvoljava. To je prilično ograničen skup tipova. Na primjer, realni brojevi nisu podržani. Međutim, dovoljno je širok da podrži većinu zahtjeva u upravljanju računarskom mrežom.

Tip podatka	Opis
INTEGER	Cijeli brojevi u rasponu od 2^{31} do 2^{31} - 1.
Uinteger32	Cijeli borjevi u rasponu od 0 do 2^{32} - 1.
Counter32	Pozitivni cijeli brojevi koji mogu biti uvećani po modulu 2^{32}.
Counter64	Pozitivni cijeli brojevi koji mogu biti uvećani po modulu 2^{64}.
Gauge32	Pozitivni cijeli brojevi koji mogu biti uvećani ili umanjeni, ali ne smiju prekoračiti maksimalnu vrijednost. Maksimalna vrijednost ne može biti veća od 2^{32} - 1. MIB varijabla tcpCurrEstab je primjer: to je broj TCP veza koje su trenutno u stanju ESTABLISHED ili CLOSE_WAIT.
TimTicks	Pozitivni cijeli brojevi koji reprezentuju vrijeme po modulu 2^{32}. Na primjer varijabla sysUpTime pokazuje je vrijeme koloko dugo je agent podignut izraženo u stotinama sekundi.

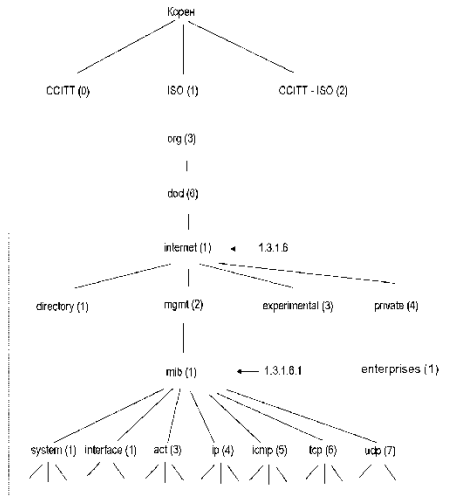
OCTET STRING	Nizovi okteta za proizvoljne binarne ili tekstualne podatke; mogu biti ograničeni na 255 okteta.
IPAddress	OCTET STRING dužine 4, Internet adresu.
PhysAddress	OCTET STRING određuje fizičku adresu (npr. 6 bajtova za Eternet adresu).
Opaque	Polje za proizvoljan bit.
BIT STRING	Spisak imenovanih bitova.

Tabela 1. Dozvoljeni tipovi podataka u SNMPv2 protokolu ***Identifikator objekta***

OBJECT IDENTIFIER - Identifikator objekta. Administrativno dodjeljeno ime (tip podatka) objektu ili drugom standardizovanom elementu. Vrijednost je niz veličine do 128 pozitivnih cijelih brojeva.

Identifikator objekta je niz cijelih brojeva odvojenih tačkom. Brojeve spaja razgranata struktura (stablo) slična DNS stablu. Na samom vrhu stabla je neimenovani korjen od koga identifikator objeata počinje. Na slici 7. data je struktura stabla koja se koristi za sisteme sa SNMP protokolom. Sve promjenljive u upravljačkoj bazi MIB započinju sa identifikatorom objekta koji počinje sa 1.3.6.1.2.1

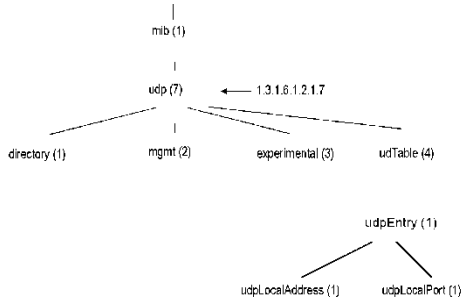
Na slici 7. je pored MIB identifikatora objekata predstavljen i jedan imenovani objekat: ***iso.org.dod.inemetprivate.enterprise*** **(1.3.6.1.4.1).** To je mjesto gdje se postavljaju MIB baze specifične za određenog proizvođača. Ovaj čvor sadrži listu od 400 registrovanih identifikatora koji su dodjeljeni odgovarajućim RFC dokumentom.



Slika 7.: Identifikatori objekata u bazi MIB

Baza podataka za informacijama za upravljanje MIB je baza podataka koju održava agent a iz koje menadžer može da dobije odgovor (upit) ili u raju menadžer može da postavi određene vrijednosti. U ovom dijelu rada biće dat kratak pregled baze podataka označene sa MIB-II i opisane u dokumentu RFC1213.

Kao što je na slici 8. predstavljeno MIB je podjeljena u grupe označene sa: system, interfaces, at, ip itd. Opisaćemo samo promjenljive iz grupe UDP. Ovo je jednostavna grupa sa malim brojem promjenljivih i jednom tabelom. Na slici 8. data je struktura stabla za tabelu za IP adresu.



Slika 8.: Struktura stabla za tabelu za IP adresu

3.2. ASN.1

Glavna bit modela SNMP NMS-a predstavlja skup objekata kojima upravljaju agenti, a čitaju ih i zapisuju upravljačke stanice. Postoje dva problema koja se javljaju pri komunikaciji mrežne opreme različitih proizvođača. SNMP poruke moraju riješiti te probleme ako se želi postići interoperabilnost, tj. da svi SNMP uređaji (različitih proizvođača) razumiju i znaju interpretirati primljene SNMP poruke.

Prvi problem nastaje zbog toga što različiti programski jezici imaju različite tipove podataka (cjelobrojne, znakove, nizove znakova, oktete itd.). Ukoliko SNMP upravljač pošalje poruku punu vrsta podataka iz jednog programskog jezika (npr. Jave) a SNMP agent je napisan u drugom programskom jeziku (npr.programskom jeziku C), oni se neće razumjeti. Da bi se riješio ovaj problem SNMP koristi ASN.1 (*Abstract Syntax Notation One*) notaciju za definiranje tipova podataka korištenih za konstrukciju SNMP poruke. Budući da je ASN.1 sintaksa nezavisna od izbora programskog jezika, SNMP agenti i upravljači mogu biti pisani u bilo kojem programskom jeziku.

Drugi problem nastaje kada komuniciraju dva krajnja sistema (komunikacija koja se odvija logički izravno između dva učesnika, u ovom slučaju na svakom kraju je jedan sudionik komunikacije), od kojih jedan, na primjer, zapisuje cjelobrojne vrijednosti u obliku 32-bitnih binarnih brojeva i u tehnici dvojnog komplementa, a drugi u obliku 16-bitnih binarnih brojeva u tehnici jednostrukog komplementa. Ni C niti Java ne zadiru u tu problematiku. To je još jedan od razloga za neophodno korištenje jezika za standardizovanu definiciju upravljanih objekata.

Dakle, svi tipovi podataka u SNMP poruci moraju biti ispravni ASN.1 tipovi podataka i moraju biti kodirani u skladu s osnovnim pravilima kodiranja. ASN.1 sintaksa je vrlo moćna i kompleksna ali zato pati od nedostatka učinkovitosti. Glavna snaga ASN.1 sintakse je u definisanju jednoznačnih pravila kodiranja na nivou bita. No, to je ujedno i slabost ASN.1 sintakse. Pravila kodiranja su takva da je cilj postići što manje bita na prenosnom mediju, a to se plaća vrlo slabom efikasnošću korištenja procesora na komunikacijskim krajevima prilikom kodiranja i dekodiranja poruka. ASN.1 je definisani standardom ISO 8824, a pravila kodiranja standardom ISO 8825.

Apstraktna sintaksa definira strukturu podataka neovisnu o načinu kodiranja korištenom za prikaz podataka. Kroz apstraktnu sintaksu je moguće definisati tipove podataka i vrijednosti istih. Tip podataka uključuje veći broj vrijednosti, a osnovna podjela je na jednostavni i složeni tip.

Neki od osnovnih tipova podataka za ASN.1 jezik dani su u tablici 2**.** [Nacionalni CERT, www.cert.hr]

Naziv tipa	Kod	Kratki opis
INTEGER	2	Cijeli broj proizvoljne duljine
BIT STRING	3	Niz koji sadrži 0 ili više bita
OCTET STRING	4	Niz koji sadrži 0 ili više okteta bez predznaka (*unsigned*)
NULL	5	*Place holder*
OBJECT IDENTIFIER	6	Tip za označavanje objekata

Tablica 2. Osnovni ASN.1 tipovi podataka

Kodiranjem se dobija niz okteta koji se koristi za prikaz podatkovnih vrijednosti. Pravila kodiranja definiraju način preslikavanja iz jedne u drugu sintaksu, tj. iz apstraktne sintakse u sintaksu prenosa, a što je prikazano na slici 9. [Nacionalni CERT, www.cert.hr].

Drugim riječima, pravilima kodiranja određen je način na koji će se skup podatkovnih vrijednosti iz apstraktne sintakse prikazati u sintaksi prenosa.

Slika 9. Kodiranjem iz apstraktne sintakse u sintaksu prelaza

3.3. SNMP PORUKE

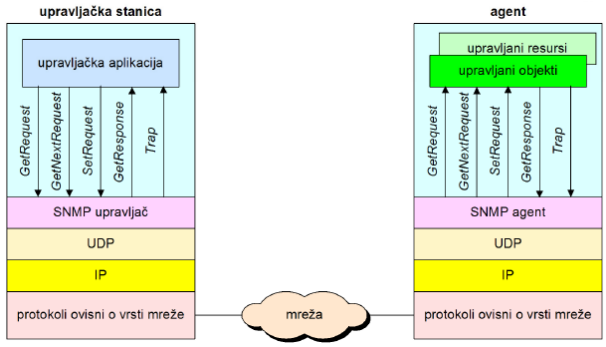
Tri osnovne funkcionalnosti koje protokol SNMP pruža sistemu upravljanja mrežom su mogućnost slanja *get, set* i *trap* poruka.

- ***Get (dohvati)*** upravljačkoj stanici omogućava dohvatanje vrijednosti upravljanih objekata sadržanih u MIB-ovima agenata. Slanje *get* poruka agentima naziva se prozivanje (*polling*). Upravljač agente najčešće proziva ciklički. Unutar nekog zadanog vremenskog intervala upravljač prozove redom sve agente i nakon toga započinje novi ciklus prozivanja. Frekvenciju prozivanja je moguće konfigurirati u SNMP *manageru*.
- ***Set*** **(postavi)** upravljačkoj stanici omogućava postavljanje vrijednosti upravljanih objekata u MIB-ovima agenata. Aplikacija obično vrši operaciju *set* tako da upravljačkoj stanici preda naziv agenta i jedan ili više OID oznaka zajedno s pripadajućim varijantama te novu vrijednost. Agent prosljeđuje zahtjev i dodjeljuje nove vrijednosti MIB varijabli. Ako dođe do greške nova vrijednost neće biti dodijeljena.
- ***Trap*** **(privuci pažnju)** omogućava agentu da obavijesti upravljačku stanicu o važnim događajima koji se zbivaju u komunikacijskoj okolini agenta.

Standardom nije određen broj upravljačkih stanica niti odnos broja upravljačkih stanica prema broju agenata u NMS-u. Praksa pokazuje da je u jednom NMS-u poželjno imati barem dvije upravljačke stanice (zbog pouzdanosti sistema), a broj agenata može iznositi i do nekoliko stotina. Na osnovu osnovnih mogućnosti protokola SNMP definisane su SNMP poruke. Upravljačka aplikacija (NMA) šalje agentima poruke *GetRequest, GetNextRequest* i *SetRequest*, a što je dato na slici 10.[William Stallings,2007]. Primitak bilo koje od tih poruka agent potvrđuje slanjem poruke *GetResponse* upravljačkoj stanici. Poruku *Trap* agent šalje upravljačkoj stanici kao reakciju na događaj koji utiče na sadržaj MIB-a agenta ili na njegove upravljane resurse u podlozi MIB-a. S obzirom da se SNMP oslanja na transportni protokol UDP, on je također bespojni protokol. Drugim riječima, prilikom komunikacije između upravljačke stanice i agenata ne uspostavljaju se veze. Svaka razmjena SNMP poruka predstavlja posebnu transakciju.

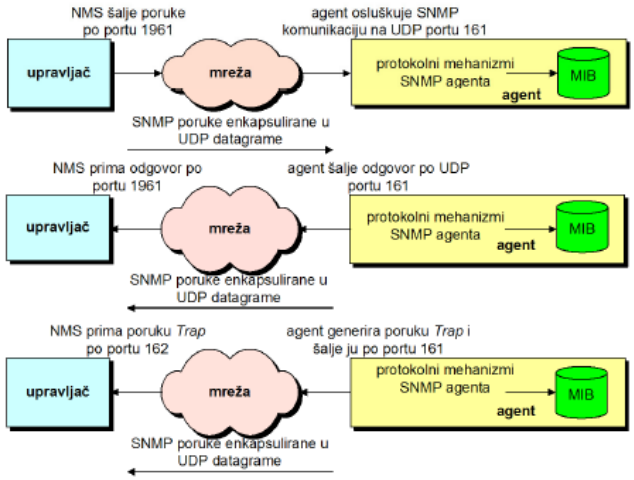
Sve se SNMP poruke enkapsuliraju se u UDP datagrame. Prilikom slanja SNMP poruke (*get ili set*), upravljač u zaglavlje UDP datagrama upisuje vrijednost izvorišnog porta. U primjeru na slici

11. [Douglas R. Mauro, Kevin J. Schmidt 2005.]. odabrana je proizvoljna vrijednost 1961. To je tzv. privremeni port kojeg upravljaču dodjeljuje operacijski sistem stanice na kojoj se izvodi NMA. Odredišni port je port 161 na kojem agent osluškuje SNMP komunikaciju i prima UDP datagrame. Kad agent stvara odgovor na primljenu SNMP poruku, u zaglavlje UDP datagrama upisuje u polje izvorišni port vrijednost 161, a u polje odredišni port u ovom slučaju vrijednost 1961.



Slika 10. Razmjena SNMP poruka

Prilikom slanja poruke *Trap* agent u polje izvorišni port upisuje vrijednost 161 (to je osnovna vrijednost no moguće je korištenje i drugih vrijednosti), a u polje odredišni port vrijednost 162. Upravljač prima poruke *Trap* na portu 162. Maksimalna duljina SNMP poruke je ograničena dozvoljenom duljinom UDP datagrama, i iznosi 65.507 okteta.



Slika 10. Razmjena SNMP poruka i asinkrono generiranje poruka Trap

3.4. VRIJEDNOSTI IDENTIFIKATORA

Svaka promejnljiva u MIB bazi mora biti indentifikovana kada se SNMP refernecira na nju, očitava ili postavlja njenu vrednost.Treba istaći da se samo čvorovi „listovi" referenciraju. SNMP ne radi sa odredišnim kolonama ili redovima tabela. Posmatrajući sliku 7. čvorovi „listovi" su oni koji su opisani na slici 8. Nisu čvorovi „listovi": ***mib, udp, udpTable* i *udpEntry***.

3.5. PROMJENLJIVE

Promjenljive se refernciraju dodavanjem "0" na identifikator objekta promjenljive. Na primjer brojač ***udpInDatagram*** iz tabele 2. čiji identifikator objekta je 1.3.6.2.1.7.1 se referencira sa 1.3.6.2.1.7.1.0. Tekstualno ime je: ***iso. org.internet.mgmt.mib. udp. udpInDatagrams.0***

Iako se ime sa kojim se referencira promejnljiva obično skraćuje na ***udpInDatagrams.0*** treba naglasiti da ime promjenljive koje se javlja u SNMP poruci je identifikator objekta 1.3.6.2.1.7.1.0.

3.6. RAD PROTOKOLA

Glavna komponenta SNMPv2 okvira je sam protokol. Protokol obezbjeđuje direktan, bazičan mehanizam za razmjenu upravljačkih informacija između menadžera i agenta. Osnovna jedinica koja se razmjenjuje je poruka koja je sastavljena od omotača i jedinice protokola PDU. Zaglavlje omotača je zaduženo za sigurnost. Jedinica podataka protokola PDU može prenijeti sedam vrsta SNMP poruka. Opšti format je prikazan na slici 8. Nekoliko polja je zajedničko za više jedinica podataka protokola PDU. Polje oznaka-zahtjeva je cio broj dodijeljen tako da je svaki zahtjev jedinstveno označen. To omogućava menadžeru da međusobno poveže dolazeće odgovore sa zahtjevima koji čekaju na odgovor.To takođe omogućava agentu da razrješi problem duplikata jedinica podataka protokola PDU nastao kao posljedica nepouzdanog mrežnog servisa (UDP). Polje povezivanje-promjenljivih sadrži listu oznaka objekata, zavisno od jedinice podataka protokola PDU. Lista može takođe da sadrži vrijednost za svaki objekat.

Jednica podataka protokola ***GetRequest*** PDU koju izdaje menadžer sadrži listu jednog ili više imena objekata za koje se traži vrijednost. Ako je operacija uspješna odgovarajući agent će poslati jedininicu podataka protokola ***Response.*** Lista ***Variable-bindings*** će sadržati oznake i vrijednosti svih traženih objekata. Za sve promjenljiva koje nisu relevantne za MIB, njihov oznaka i poruka o grešci vraćaju se u listi ***Variable-bindings***. Dakle SNMPv2 ne dozvoljava djelimičan odgovor na ***GetRequest***, što je bitno poboljšanje u odnosu na SNMPv1. U verziji SNMPv1 ako jedna ili više promjenljivih u jedinici podataka protokola ***GetRequest-PDU*** nije podržana agent će vratiti poruku o gešci koja glasi: „nema takvog imena ***(noSuchName)***". Da bi se izborio sa tom greškom, rukovodioc neće vratiti nikakvu vrjednost ili će uključiti takav algoritam koji će kada dođe do greške odstraniti nedostajuću promjenljivu ponovo šaljući zahtjev i prosleđujući aplikaciji nepotpun rezultat.

Jedinicu podataka *GetNextRequest* PDU se takođe izdaje menadžer i sadrži listu jednog ili više objekata. U ovom slučaju za svaki objekat imenovan u ***variable-bindings*** polju, vrijednost mora biti vraćena za objekat koji je sledeći po leksikografskom redu, tj. sledeći po redu u strukturi stabla oznaka objekata. Kao što je bilo i sa jedinicom podataka protokola *GetRequest* PDU, agent će vratiti vrijednosti za što je moguće više promjenljivih. Jedna od sposobnosti jedinicom podataka protokola *GetNextRequest* PDU je da omogući menadžeru da dinamički pretražuje strukturu MIB. Korisno je ako menadžer ne zna unaprijed skup objekata koji podržava agent ili koji je u određenoj bazi MIB.

Jedno od glavnih unapređenja u SNMPv2 je jedinica podataka protokola *GetBulkRequest* PDU. Svrha ovog jedinice podataka protokola PDU je da smanji broj razmjena u protokolu potrebnih da bi se pribavila velika količina upravljačkih informacija. *GetBulkRequest* PDU dozvoljava SNMPv2 menadžeru da zahtjeva da odgovor bude što je moguće obimniji poštujući ograničenje u veličini poruke.

Jedinicu podataka protokola *SetRequest* PDU izdaje menadžer kada zahtjeva da se vrijednosti jednog ili više objekata promjeni. SNMPv2 cjelina koja prima poruku sa jedinicom podataka protokola *Response* PDU koji sadrži istu oznaku zahtjeva. Kod *SetRequest* operacija je ili su sve promjenljive ažurirane ili nije ni jedna. Ako je cjelina koji odgovar u mogućnosti da postavi vrijednosti za sve promjenljive koje se nalaze u dolazećoj *variables-bindings* listi onda *Response* PDU postavlja odgovarajuća polja sa vrijednostima koje su za svaku od promjenljivih dobijene. Ako se samo jedna od vrijednosti promjenljive ne može dobiti ne šalje se natrag ni jedan

vrijednost i ni jedna vrijednost se ne ažurira. Onda statusni kbd o grešci ukazuje na razlog za grešku i polje indeks-greške ukazuje na promjenljivu u listi koja je dovela do greške.

Jedinicu podataka SNMPv2-Trap PDU pravi i šalje SNMPv2 cjelina koji ima ulogu agenta ukoliko dođe do neubičajenog događaja. Koristi se da bi upravljačka stanica se obavijestila (asinhrono) o nekim bitnim događajima. Lista se koristi da čuva informacije vezane za *Trap* poruke. Jedinice podataka protokola SNMPv2-trap-PDU za razliku od jedinica podataka protokola *GetRequest , GetNextRequest, GetBulkRequest, SerRequest* i *InformRequest* PDU ne zahtjeva odgovor od prijemnog cjeline.

Jedinicu podataka *InformRequest* PDU šalje SNMPv2 cjelina koja je u ulozi menadžera jedne aplikacije drugoj SNMPv2 cjelin koja je u ulozi mendžera da bi pribavio upravljačke informacije za aplikaciju koristeći ovu drugu cjelinu. Kao što je slučaj i sa jedinicom podataka SNMPv2-trap PDU, polje liste koristi se da prenese odgovarajuće informacije. Menadžer koji prima *InformRequest* potvrđuje prijem sa jedinicom podataka protokola *Response* PDU.

Za SNMPv2-*trap* i *InformRequest* važi da se različita stanja mogu odrediti koja ukazuju kada je obavještenje napravljeno; takođe je naznačeno i koja se informacija mogu poslati.

ZAKLJUČAK

SNMP protokol je jednostavan alat za upravljanje mrežom. On definiše ograničenu i lako primjenljivu bazu podataka o upravljanju mrežom MIB sastavljenu od skalarnih promjenljivih i dvo-dimenzionalnih tabela. Takođe definiše i automatizovan protokol koji omogućava menadžeru da pribavi i podesi MIB promjenljivu i da omogući agentu da pošalje obavještenje-zamku. Jednostavnost je jedan od najvećih aduta protokola SNMP. On se lako implementira i ne opterećuje mnogo procesor a ni mrežne resurse. Takođe struktura protokola i MIB je dovoljno otvorena, tako da nije teško postići kompatibilnost između upravljačkih stanica i agent softvera različitih proizvođača. Sa njegovim rasprostranjenim korišćenjem nedostaci SNMP su postali očigledniji. Nedostaci se odnose i na način rada i mehanizme zaštite. Posljedica je usavršena verzija poznata kao SNMPv2 koju su veoma brzo proizvođači opreme prihvatili i najavili uređaja sa novom verzijom protokola za upravljanje mrežom. Verzija SNMPv2 ne obezbjeđuje upravljanje mrežom već okvir u kome se aplikacije za upravljnjem mrežom može napraviti. Aplikacije, kao što su upravljanje greškama, nadgledanje performansi, naplata itd. su van obima ovog standarda. SNMPv2 obezbjeđuje infrastrukturu za upravljanje mrežom. Glavna komponenta SNMPv2 okvira je sam protokol. Protokol obezbjeđuje direktan, bazičan mehanizam za razmjenu upravljačkih informacija između menadžera i agenta. Osnovna jedinica koja se razmjenjuje je poruka koja je sastavljena od omotača i jedinice protokola PDU. Jedno od glavnih unapređenja u SNMPv2 je jedinica podataka protokola *GetBulkRequest* PDU. Svrha jedinice podataka protokola PDU je da smanji broj razmjena u protokolu potrebnih da bi se pribavila velika količina upravljačkih informacija. *GetBulkRequest* PDU dozvoljava SNMPv2 menadžeru da zahtjeva da odgovor bude što je moguće obimniji poštujući ograničenje u veličini poruke. Da bi se ispravili nedostatke SNMPv1 i SNMPv2 vezani za bezbjednost napravljena je nova verzija SNMPv3 koja se pojavila januara 1998. god. i koja je opisana je dokumentima RFC2570 do RFC2575. Skup ovih dokumenata ne prikazuje kompletne mogućnosti verzije SNMPv3 već definiše njegovu opštu arhitekturu i osobine vezane za bezbjednost.

Glavni aduti SNMP-a su jednostavnost i interoperabilnost. Njegova važna odlika SNMP je da mora efektivno raditi i kada mreža nije potpuno operabilna. To se odražava u izboru nespojnog transportnog protokola (UDP) koji dopušta upravljačkim aplikacijama potpunu kontrolu nad mehanizmom retransmisije. Gledajući današnje mrežne tehnologije i stvarnu upotrebu SNMP modela, očito je kako bi uređaji mogli obavljati još kompleksnije upravljačke operacije uz nisko opterećenje. Razumno je očekivati kako će uređaji, pogotovo novi usmjerivači i preklopnici, postati sve više programibilni i kako će postati moguće pokretanje sve snažnije kontrolne

programske podrške na tim uređajima. Budućnost se nazire u sve većem okretanju upravljanju računarskim sistemom zasnovanom na webu.

LITERATURA

1. *Douglas R. Mauro, Kevin J. Schmidt. 2005. Essential SNMP pdf ebook, Publisher: „O'Reilly Media".*
2. *Andrew S. Tanenbaum, David J. Wetherall. 2013. Računarske mreže - prevod petog izdanja, Beograd: Mikro knjiga.*
3. *Šušić, I. 2014. Računarske mreže – skripta sa predavanja, Banja Luka: PIM-Fakultet računarskih nauka.*
4. *William Stallings, 2007. Data and computer communications/ Network Management-SNMP , London: Cambridge University.*
5. *Veinović, M. Jevremović, A. 2008. Uvod u računarske mreže, Beograd: Univerzitet Singidunum-Fakultet za informatiku i menadžment.*
6. *SNMP (Simple Network Management Protocol):*
7. *http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol*
8. *MIB (Management Information Base):*
9. *http://en.wikipedia.org/wiki/Management_information_base*
10. *OID (Object Identifier): http://en.wikipedia.org/wiki/Object_identifier*
11. *RFC-1213 references: http://www.rfc-editor.org/rfc/rfc1213.txt*
12. *Wikipedia: OSI model,http://en.wikipedia.org/wiki/OSI_model*
13. *Nacionalni CERT, www.cert.hr*