SIGURNOST RAČUNARSKIH MREŽA (SRM)

Tema 13:

Nadzor računarskih mreža

URLs:

- Zvanična Web strana: www.viser.edu.rs/predmeti.php?id=122
- Dodatni resursi: www.conwex.info/draganp/teaching.html
- Knjige:

  www.conwex.info/draganp/books.html
- Teme za seminarske radove:

  www.conwex.info/draganp/SRM_seminarski_radovi.html

Napomena

- Ovo je skraćena verzija prezentacije / predavanja na temu **“Nadzor računarskih mreža”**

Nadzor računarskih mreža

- Sadržaj poglavlja i predavanja:
  - 13.1 Uvodne napomene
  - 13.2 Simple Network Management Protocol (SNMP)
  - 13.3 Alati za nadzor mreža

Quote

"The secret of all victory lies in the organization of the non-obvious."

–Marcus Aurelius – Roman Emperor

Potrebna predznanja

- Programiranje
- Za primenu:
  - Računarske mreže i protokoli
  - Operativni sistemi
  - Sistemsko programiranje
  - Strukture i modeli podataka, baze podataka

13.1 Uvodne napomene

- Jedna od definicija upravljanja mrežom glasi:
  - „**Upravljanje mrežom** (engl. *network management*) je proces upravljanja složenom komunikacionom mrežom čiji je cilj maksimiranje efikasnosti i produktivnosti mreže“.

ISO – pet funkcionalnih domena

- **Upravljanje kvarovima** (engl. *fault management*) omogućava otkrivanje, izolovanje i otklanjanje neispravnih stanja u mreži.
- **Upravljanje obračunavanjem troškova** (engl. *accounting management*) omogućava obračun i naplatu troškova nastalih korišćenjem mrežnih resursa.
- **Upravljanje konfiguracijom** (engl. *configuration management*) služi za prikupljanje podataka od upravljanih mrežnih objekata i za slanje podataka upravljanim mrežnim objektima. Ti podaci se odnose na konfiguraciju upravljanog objekta, i neophodni su za kontinuirani rad mreže.
- **Upravljanje performansama** (engl. *performance management*) služi za proračun i grafički prikaz ponašanja upravljanih mrežnih objekata i efikasnosti komunikacionih aktivnosti.
- **Upravljanje sigurnošću** (engl. *security management*) odnosi se na one aspekte sigurnosti koji su bitni za ispravan rad sistema upravljanja mrežom i za zaštitu upravljanih mrežnih objekata.

13.2 Simple Network Management Protocol (SNMP)

- Softver za upravljanje mrežom (engl. *network management software*) moguće je podeliti u tri kategorije:
  - Softver za predstavljanje upravljačkih podataka korisnicima (engl. *user presentation software*)
  - Softver za upravljanje mrežom (engl. *network management software*)
  - Softver za podršku aplikaciji mrežnog upravljanja (engl. *network management support software*)

Razvoj protokola SNMP

- U aprilu 1988. objavljen je RFC 1052. Taj RFC je zahtevna specifikacija za standardizovano mrežno upravljanje u kojoj se objašnjava šta sve mora da obezbedi mrežno upravljanje. Prva verzija protokola opisana je u dokumentu RFC 1157 (IETF standard) 1991. godine. Ovim dokumentom su definisani formati poruka i komunikacioni protokol, poruke koje se mogu razmenjivati između upravljačkih entiteta i upravljačke stanice koje omogućavaju čitanje i ažuriranje vrednosti, poruke za upozoravanje (tj. alarmiranje – *trap*).

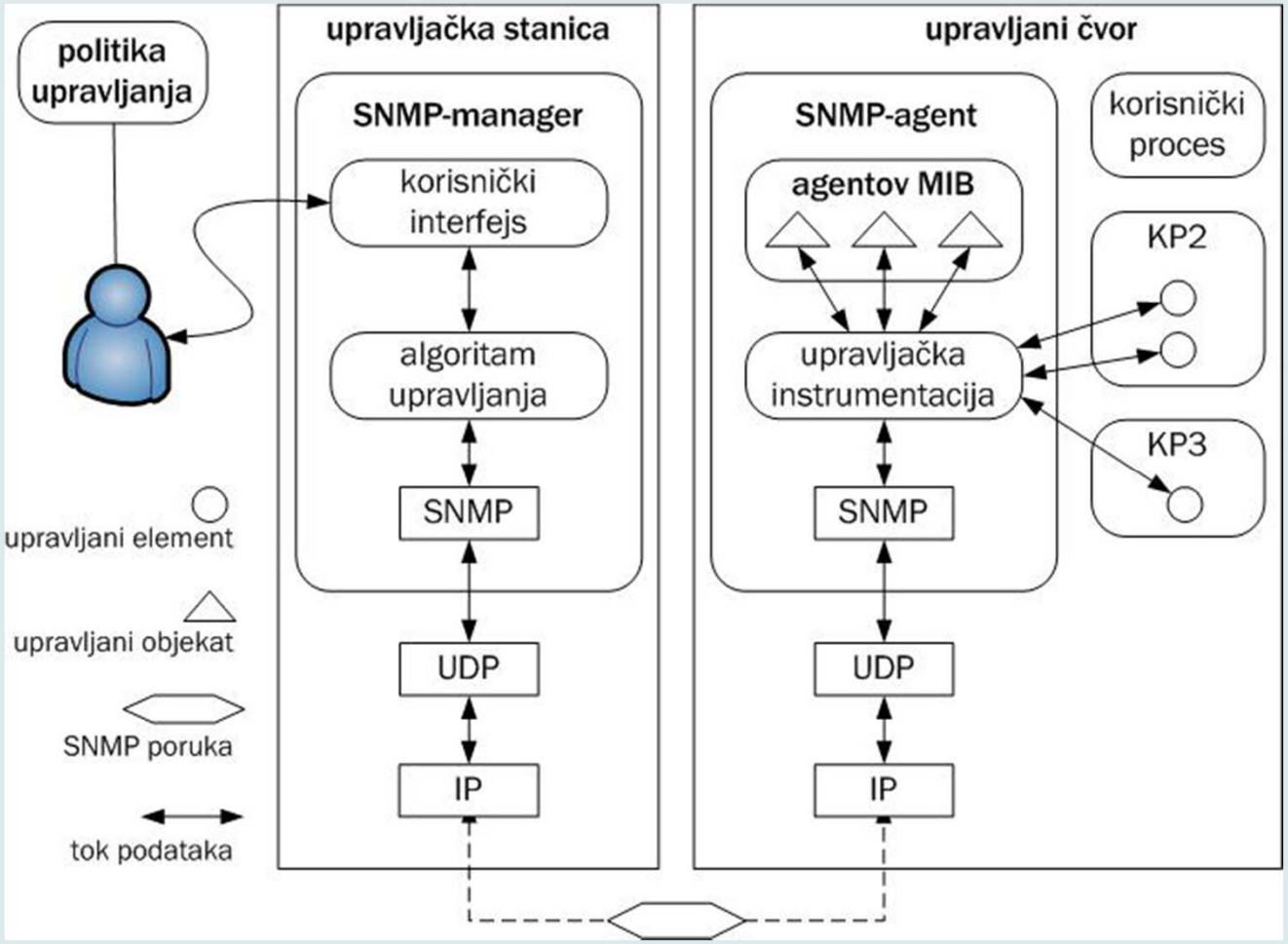
Verzije SNMP protokola

- SNMPv1 – 1988., 1991. (na bazi RFC-ova počevši od 1988.)
- SNMPv2 – 1993.
- SNMPv3 – 1997.

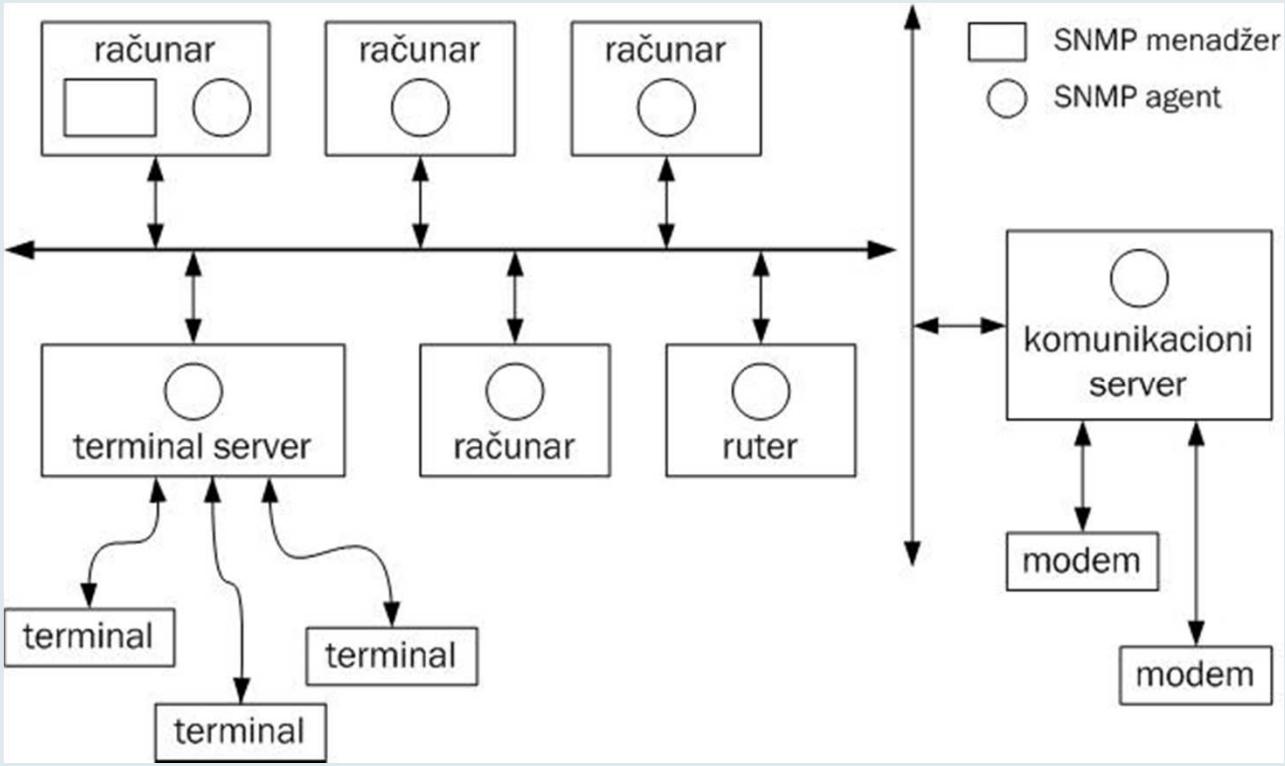
Delovi sistema za upravljanje mrežom

- Protokol SNMP je deo sistema za upravljanje mrežom (engl. *network management system*), sačinjenog od nekoliko delova. To su:
  - Jedna ili više upravljačkih stanica (engl. *network management station*) na kojima se izvršavaju upravljačke aplikacije (engl. *management application*)
  - Jedan ili više upravljanih čvorova engl. *managed node*) na kojima se izvršavaju upravljački agenti (engl. *managed elements*)
  - Upravljačke informacije (engl. *management information*)
  - Protokol SNMP po kojem se upravljačke informacije prenose između upravljačkih aplikacija i agenata

Sistem za upravljanje mrežom u okviru protokola SNMP



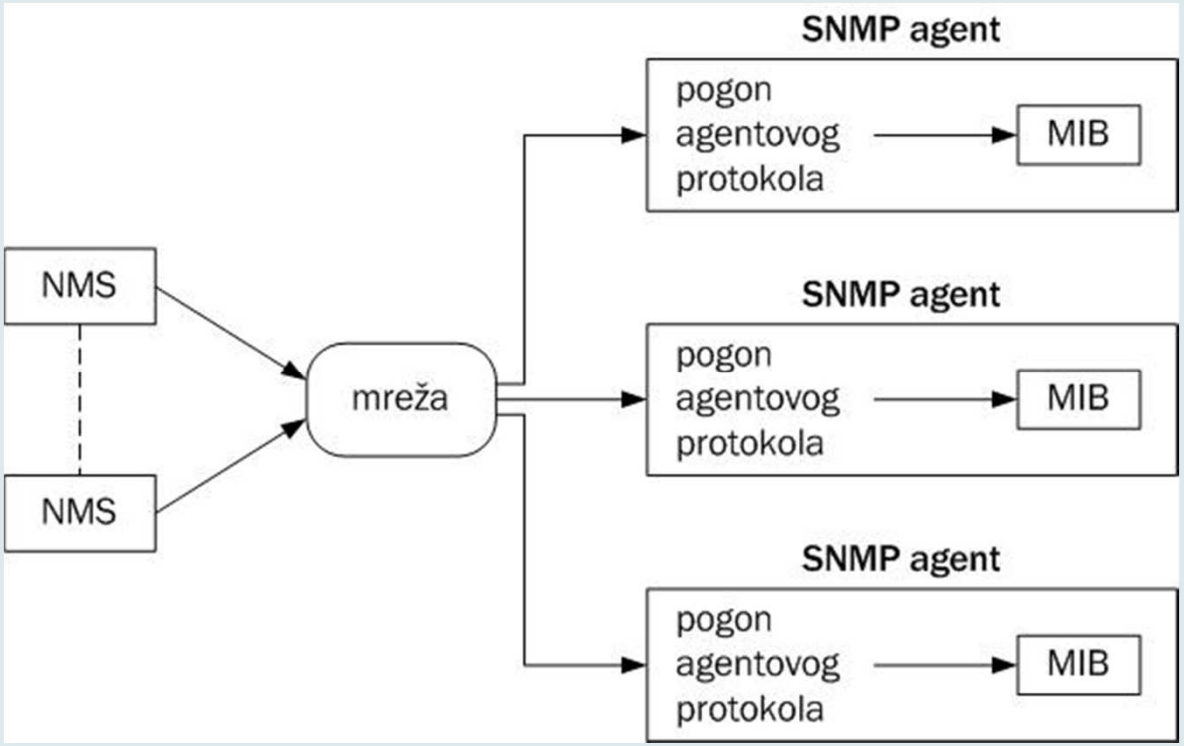
Primer rasporeda delova sistema za upravljanje mrežom u jednoj lokalnoj mreži



Komponente SNMP

- **Upravljani uređaj** - mrežni čvor koji sadrži SNMP agenta i koji se nalazi u upravljačkoj mreži. Uređaj za upravljanje sakuplja i čuva upravljačke informacije i čini ih dostupnima NMS-u preko protokola SNMP. Ti uređaji (ponekad se nazivaju mrežni elementi) mogu biti ruteri, serveri za udaljeni pristup (engl. *access server*), komutatori, štampači itd.
- **Agent** - mrežno-upravljački softverski modul koji je smešten na uređaju za upravljanje. On ima lokalno znanje o upravljačkim informacijama i prevodi ih u oblik kompatibilan sa SNMP. Omogućava udaljeni pristup opremi za upravljanje.
- **NMS** (*Network Management System*) - izvršava aplikacije koje prate i kontrolišu uređaje za upravljanje. NMS osigurava mnoštvo procesnih i memorijskih resursa, opremljenih za mrežno upravljanje. Na upravljačkoj mreži mora postojati jedan NMS ili više njih.

Model upravljačke mrežne arhitekture



Osnovne naredbe SNMP-a

- Naredba `Read` NMS koristi za praćenje upravljačkih uređaja. NMS ispituje različite promenljive koje se podržavaju preko upravljačkih uređaja.
- Naredbu `Write` NMS koristi za kontrolisanje upravljačkih uređaja. NMS menja vrednosti promenljivih koje su smeštene u upravljačkim uređajima.
- Naredbu `Trap` koriste upravljački uređaji za izveštavanje NMS-a o asinhronim događajima. Naredba `Trap` je poruka koja prijavljuje problem ili značajniji događaj. Kada se dogodi određeni tip dogadaja, upravljački uređaj pošalje trap NMS-u.
- Operacije `Traversal` NMS koristi da bi utvrdio koje promenljive upravljački uređaj podržava i da bi sekvencijalno sabrao informacije u tabelu.

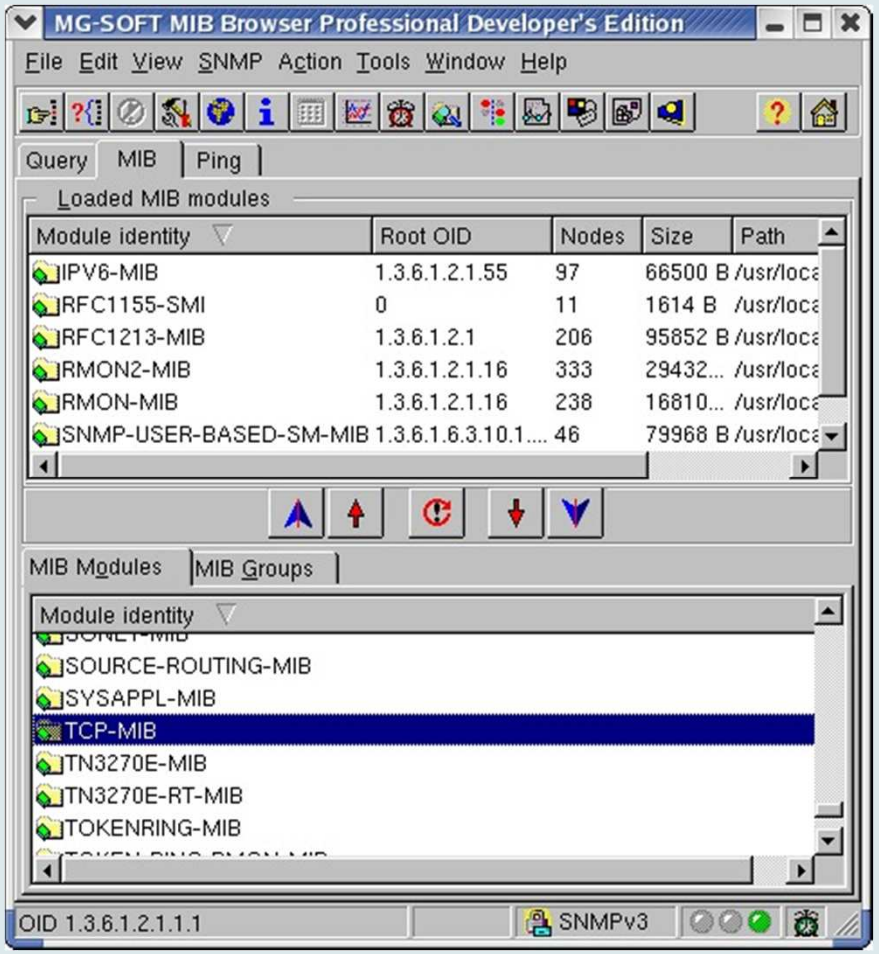
Management Information Base (MIB)

- MIB (*Management Information Base*) predstavlja hijerarhijski organizovan skup informacija.
- To je logička baza upravljačkih informacija (tj. definicija), napravljena na osnovu konfiguracije i statističkih informacija uskladištenih na uredaju.
- MIB-u se pristupa preko mrežnog protokola kao što je SNMP.
- Sastoji se od upravljanih objekata i prepoznaje se pomoću identifikatora objekata.
- Identifikatori objekata (engl. *Object Identifier, OID*) jednoznačno identifikuju upravljane objekte u MIB hijerarhiji.
- MIB hijerarhija se može prikazati kao stablo. Deca i roditelji ne mogu imati iste celobrojne vrednosti. Deca mogu dalje biti roditelji, čineći tako podstablo.

Primer – grana koja se odnosi na sigurnost

- Roditeljski identifikator objekta sa brojem: 1.3.6.1 ima svoje „dete“, tj. sledbenika za sigurnost, čiji je OID 1.3.6.1.5. Dalje se ovaj identifikator grana na sledeći način:
  - 1.3.6.1.5.1 – kerberosV4
  - 1.3.6.1.5.2 – kerberosV5
  - 1.3.6.1.5.3 – integrity
  - 1.3.6.1.5.4 – confide
  - 1.3.6.1.5.5 – mechanisms
  - 1.3.6.1.5.6 – nametypes
  - 1.3.6.1.5.7 – services

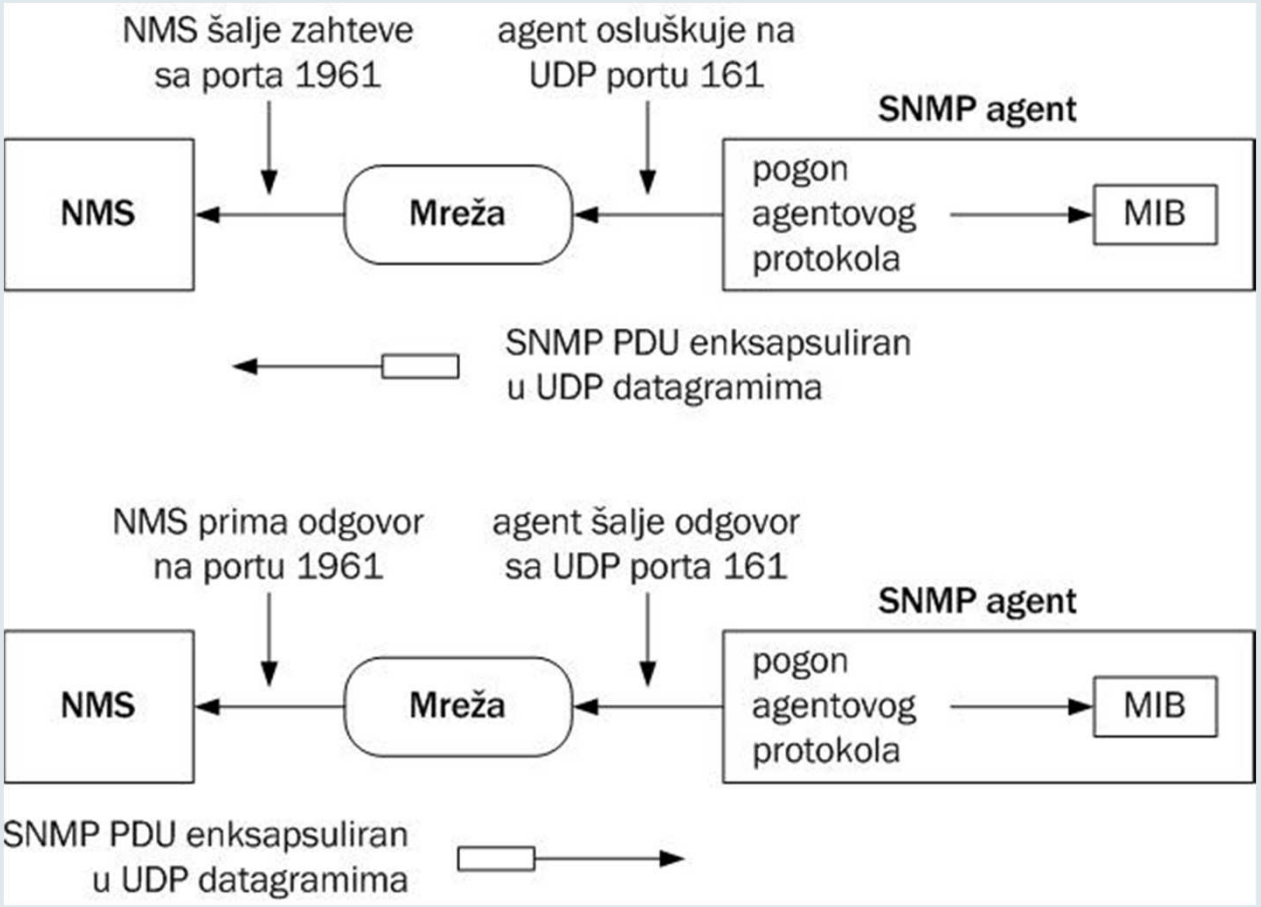
MG-SOFT MIB Explorer (Linux verzija)



Opis rada protokola SNMP

- SNMP je standardni i vrlo raširen protokol za upravljanje i administriranje mreže koji služi za prikupljanje informacija o subjektima na mreži i njihovo slanje administratoru. SNMP se naslanja na UDP (*User Datagram Protocol*). UDP prenos možemo opisati prema sledećim koracima:
  - agent sluša na UDP portu 161,
  - odgovori se šalju na NMS port (1961),
  - maksimalna veličina SNMP poruke ograničena je maksimalnom veličinom UDP poruke,
  - sve SNMP implementacije moraju primiti pakete najmanje dužine 484 bajta,
  - ako dođe do greške prilikom prenosa, prima se poruka na NMS portu 162.

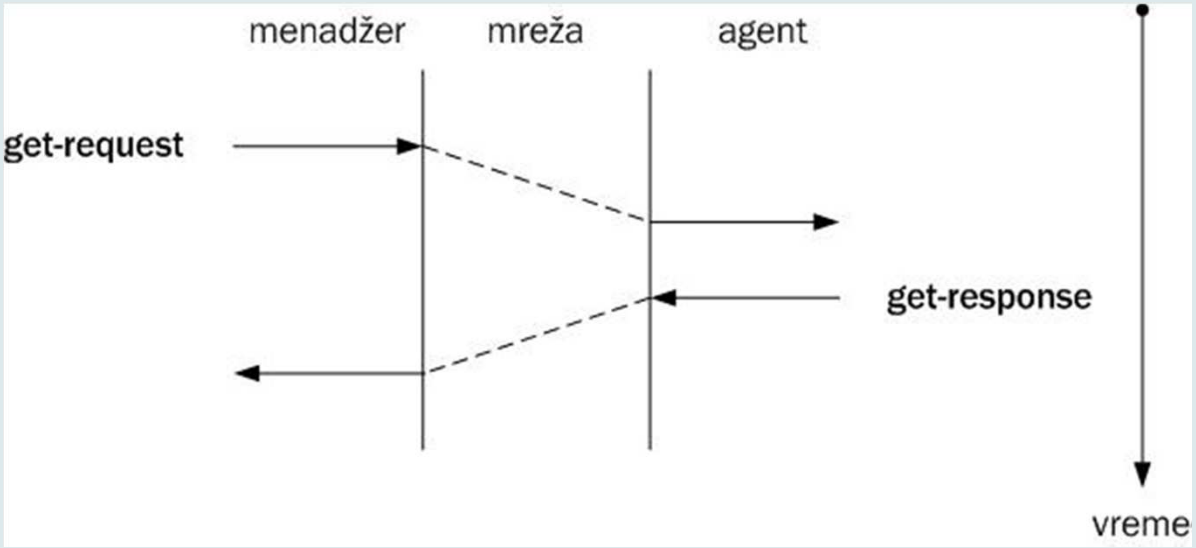
UDP prenos (standardna razmena zahtev-odgovor)



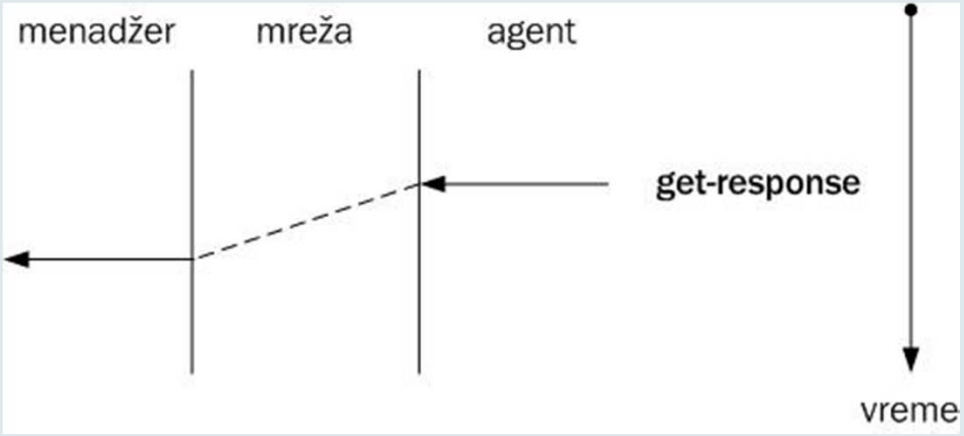
SNMP Protocol Data Units

- Postoji pet osnovnih poruka tj. podatkovnih jednica SNMP protokola (*Protocol Data Units*):
  - `Get request` – poruka koja zahteva vrednost jedne ili više MIB promenljivih,
  - `Get next request` – omogućava menadžeru da dođe do narednih (sledećih u nizu) vrednosti. Koristi se za čitanje vrednosti MIB narednih promenljivih; često se koristi za čitanje redova tabele,
  - `Set request` – poruka koja osvežava tj. ažurira (engl. *update*) MIB promenljive,
  - `Get response` – vraća odgovor na `get request`, `get next request` ili `set request`
  - `Trap` – poruka koja javlja problem ili značajan događaj

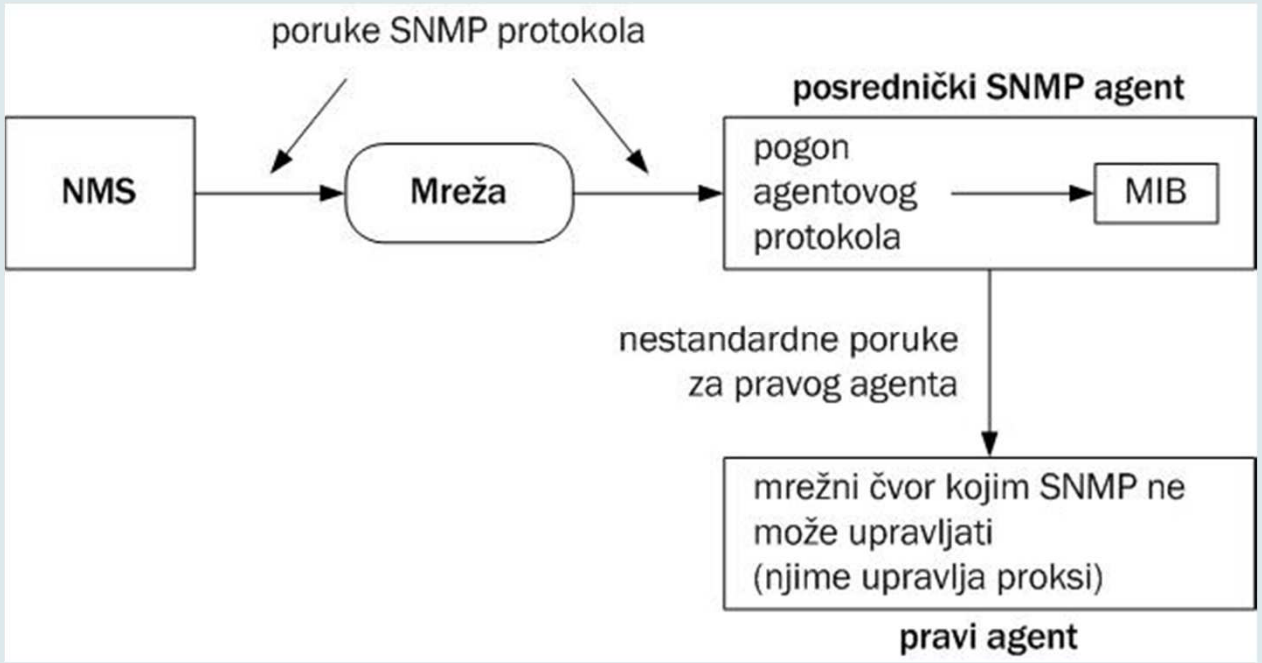
Model menadžer/agent (operacija get request)



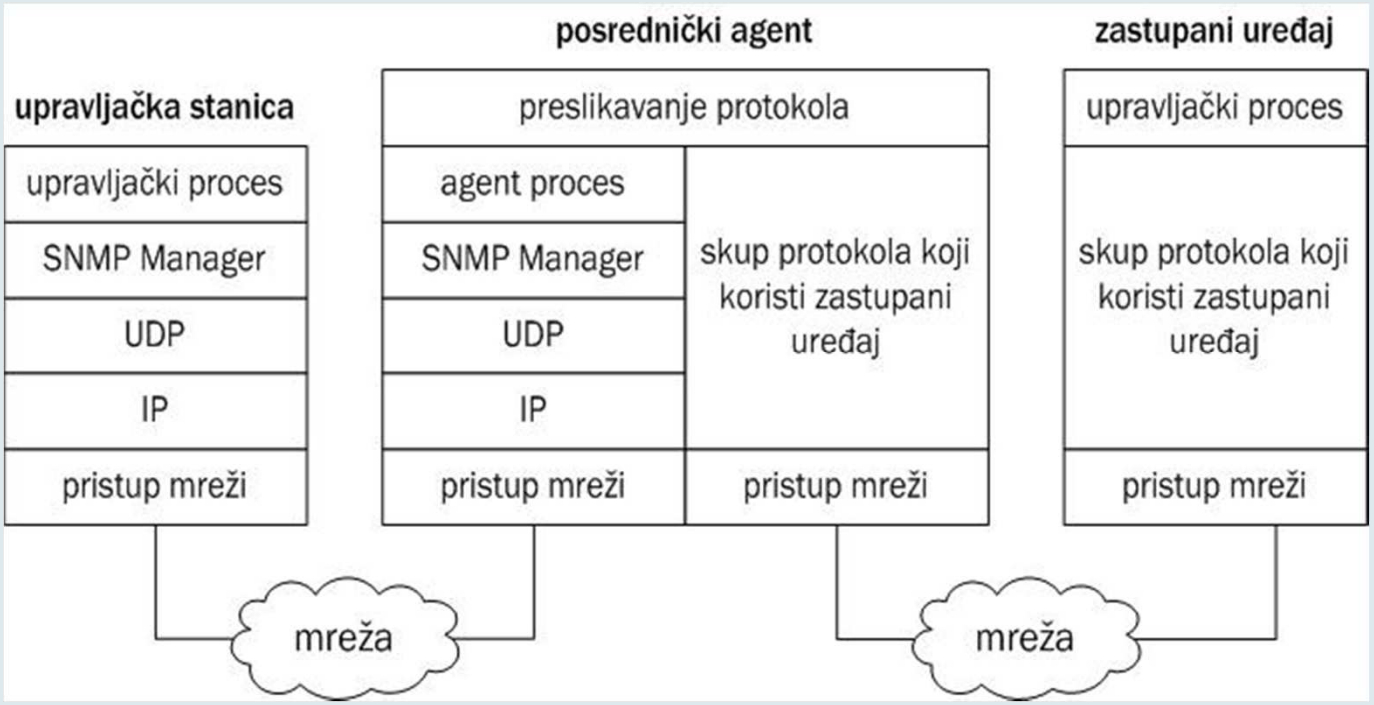
Model menadžer/agent (operacija trap)



Proksi agent



Posrednički SNMP agent



SNMPv3

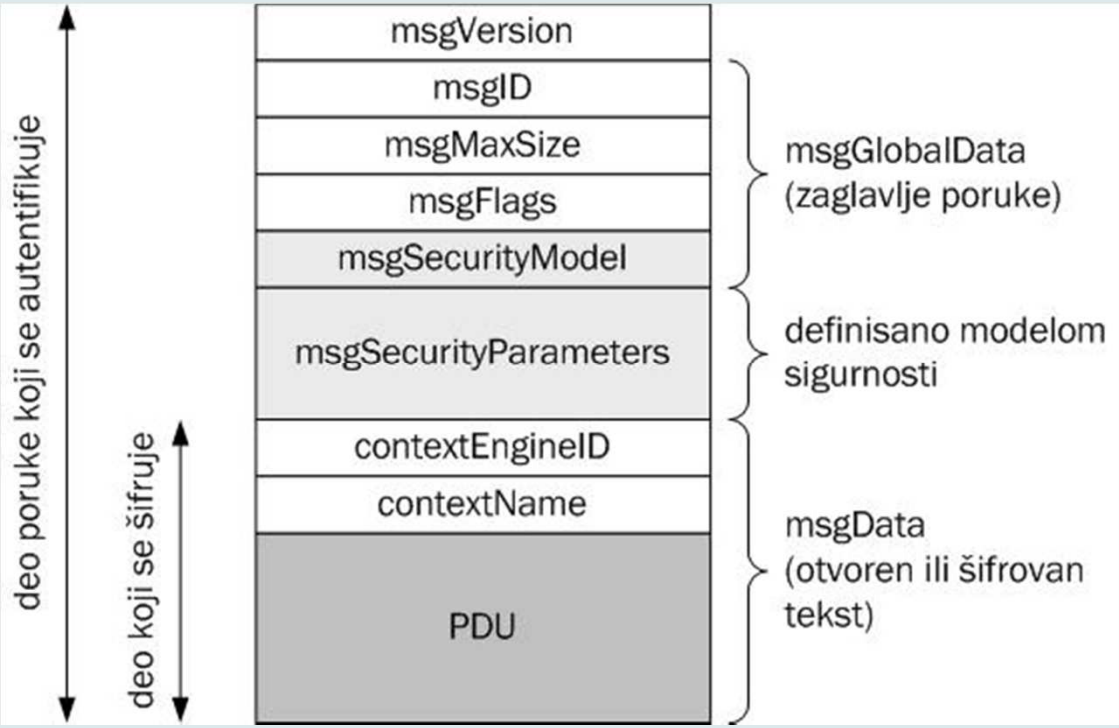
- Treća verzija, SNMPv31, konačno je otvorila put prema rešavanju problema sigurnosti NMS-a zasnovanog na protokolu SNMP. U SNMPv3 ugrađeni su ozbiljni mehanizmi za proveru identiteta korisnika i šifrovanje SNMP poruka. Nažalost, danas (2006. godina) još uvek veliki broj uređaja ne podržava SNMPv3. Cisco je ugradio podršku za SNMPv3 u operativni sistem IOS koji implementira u mrežne uređaje.

- Najvažnija promena u SNMPv3 jeste napuštanje koncepta NMS-a koji se zasniva na upravljačima i agentima. SNMPv3 NMS čine SNMP entiteti (engl. *entities*). Novi koncept definiše arhitekturu NMS-a, a ne samo skup poruka kao ranije verzije.

- Najvažniji RFC-ovi vezani za SNMPv3 su RFC 1905, RFC 1906, RFC 1907, RFC 2271, RFC 2272, RFC 2573, RFC 2274 i RFC 2275.

SNMPv3 entitet

Format SNMPv3 poruke



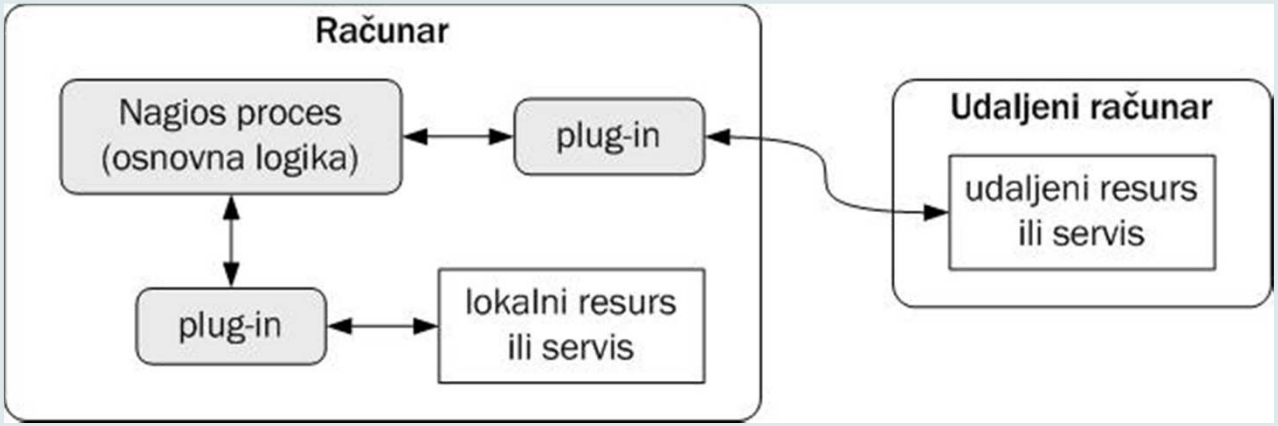
13.3 Alati za nadzor mreža

- Dve kategorije srodnih alata:
  - alati za nadzor računarskih sistema i mreža (engl. *network monitoring tools*)
  - alati za upravljanje računarskim mrežama (engl. *network management tools*)

Nagios

- Nagios je besplatan Linux softver otvorenog koda, namenjen za nadgledanje i analizu stanja mrežnih resursa i komponenata. Razvija ga i održava Ethan Galstad.
- Originalni projekat je započet pod imenom *Netsaint*, a njegova poslednja zvanična verzija je 0.0.7. Dalji razvoj projekta nastavljen je pod novim registrovanim imenom, *Nagios*™, čime su izbegnuti potencijalni pravni problemi oko korišćenja prethodnog imena *Netsaint*. Inače, novo ime je u istom duhu, pošto potiče od grčke reči *agios* (ΑΓΙΟΣ) koja znači svetac (takođe, engl. *saint* = svetac) i prefiksa „n“ koje je prvo slovo engleske reči *network* (mreža).

Modularna arhitektura



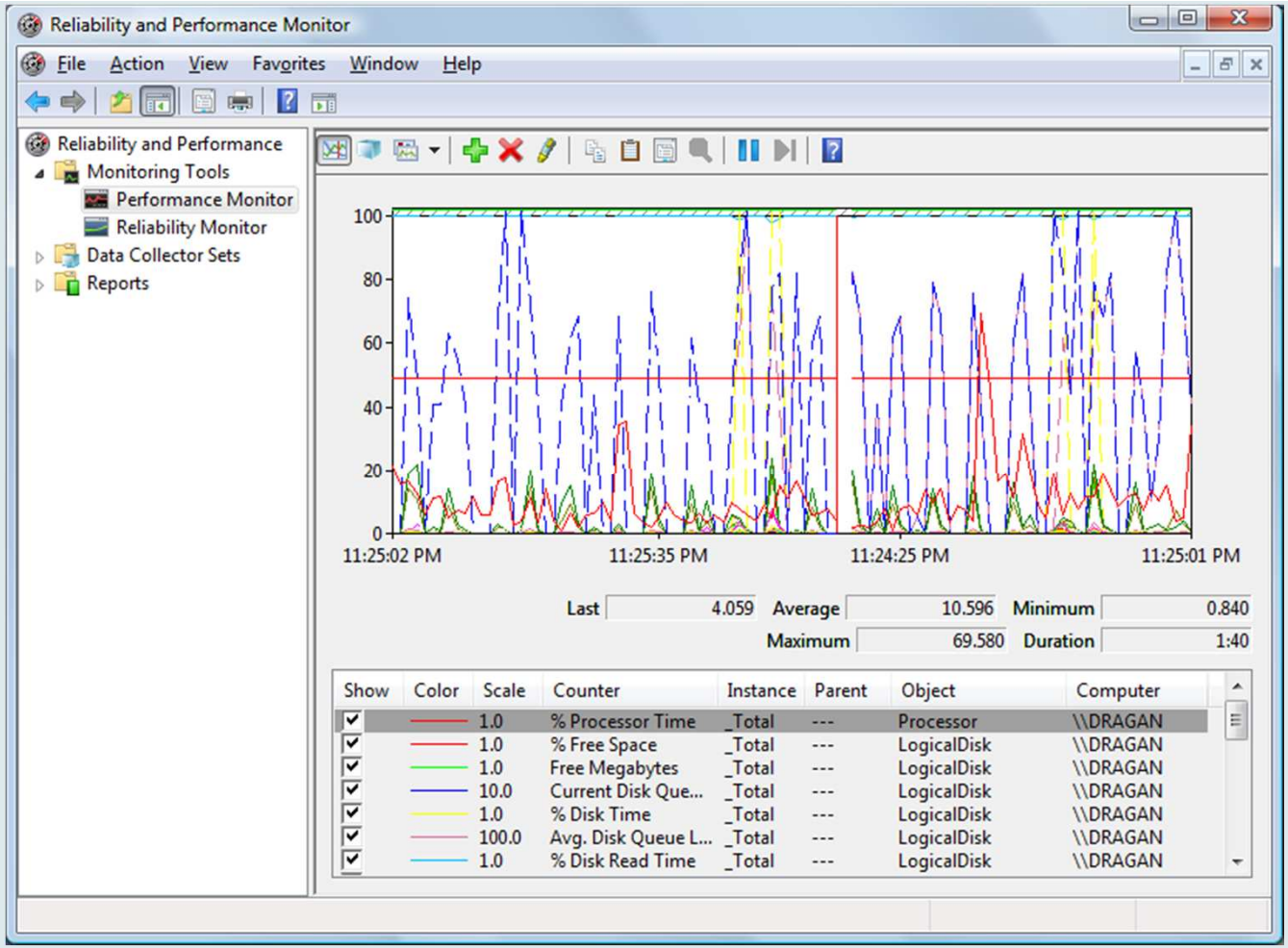
Više o alatu Nagios

- Dodatni podaci o programskom paketu Nagios, uključujući preuzimanje programskog paketa i dokumentacije, mogu se naći na Web lokacijama
  - www.nagios.org
  - http://nagiosplug.sourceforge.net/
- Ukoliko ste zainteresovani da učestvujete u daljem razvoju ovog programskog alata, možete na gore pomenutoj Web lokaciji videti i načine kako da se pridružite timu.

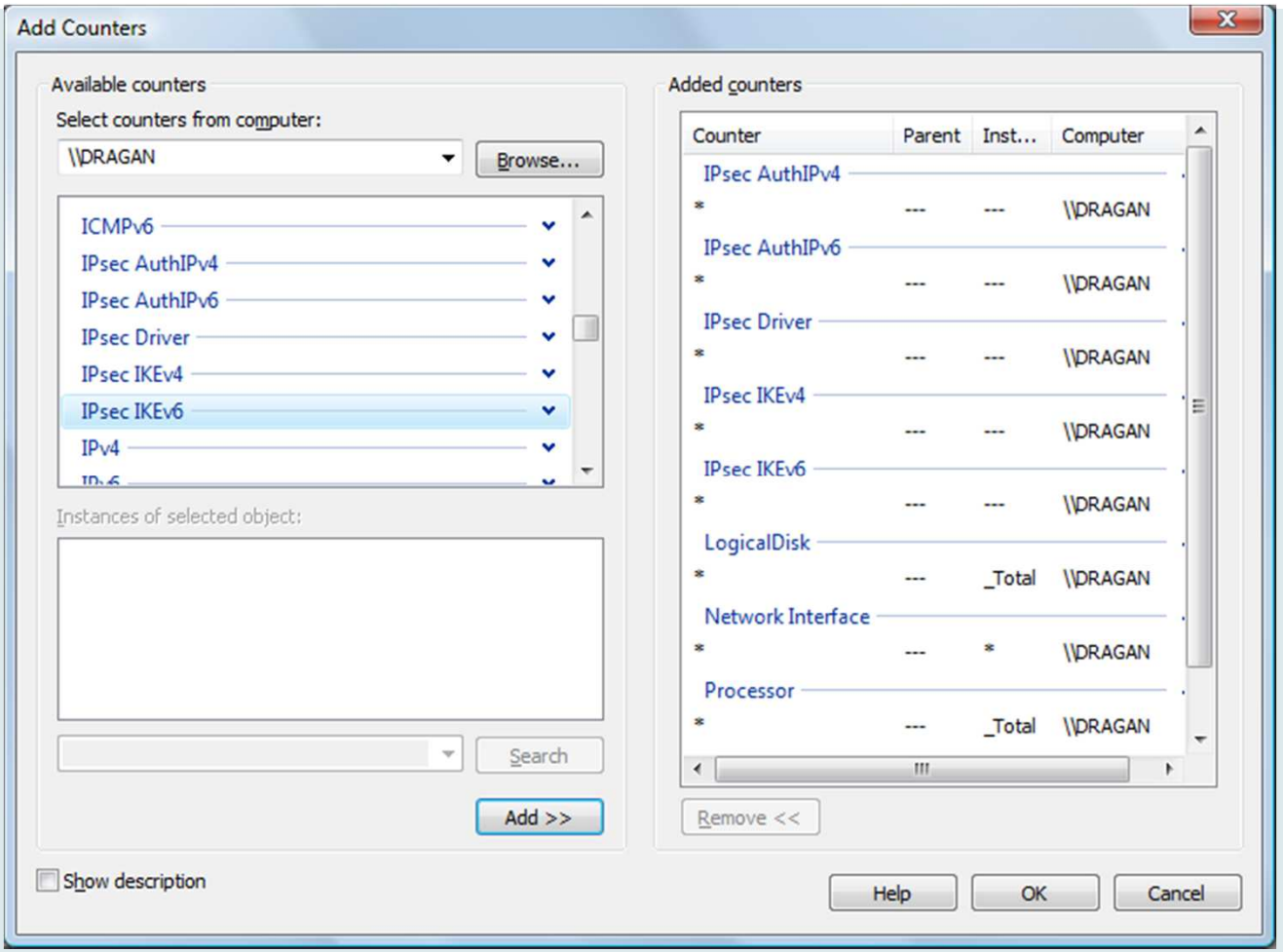
Nadzor na operativnim sistemima Windows

- Microsoft Windows počevši od Windowsa NT - dodavanje mogućnosti za nadzor operativnog sistema, performansi, kao i podršku za SNMP, MIB, OID i slično.
- Uveden je monitor performansi (*Performance Monitor*), koji se može pokrenuti naredbom `perfmon` ili iz upravljačke konzole (*Microsoft Management Console, MMC*) kao poseban dodatak (*snap-in*).
- Pri ovome se nude sledeće mogućnosti:
  - nadzor sistema (engl. *system monitoring*)
  - beleženje performansi (engl. *performance logs*) i sistemi dojavljivanja uzbuna (engl. *alerts*)
- Start → Run → unesite komandu `perfmon`.
- Start → Run → unesite komandu `mmc`, a zatim iz padajućeg menija MMC konzole odaberite opciju File → Add/Remove Snap-in i dodajte odgovarajući Snap-in.

Monitor performansi



Dodavanje brojača



Literatura

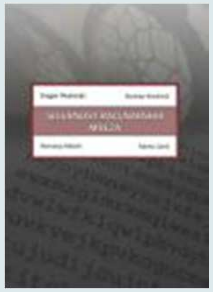
- D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: **"Sigurnost računarskih sistema i mreža"**, Mikro knjiga, Beograd, 2007., ISBN: 978-86-7555-305-2, knjiga – udžbenik
- www.conwex.info/draganp/books_SRSiM.html
- www.mikroknjiga.rs/store/prikaz.php?ref=978-86-7555-305-2

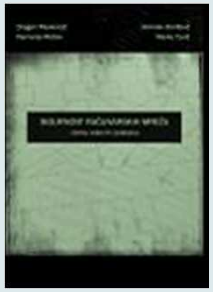
- Za predavanje 13:
  - Poglavlje 13: Nadzor računarskih mreža

Literatura - nastavak

- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-16-5, knjiga - udžbenik
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - priručnik za laboratorijske vežbe"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-49-1
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - zbirka rešenih zadataka"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-55-6

www.conwex.info/draganp/books.html





Dodatna literatura

- **Applied Cryptography**
  Bruce Schneier
  John Wiley & Sons, 1995

- **Cryptography and Network Security**
  William Stallings
  Prentice Hall, 1998

- **The CISSP Prep Guide – Mastering the Ten Domains of Computer Security**
  Ronald L. Krutz, Russell Dean Vines
  John Wiley & Sons, 2001

  Druge knjige i razni *online* resursi

- ***Napomena:*** tokom predavanja će biti naglašena dodatna literatura, po potrebi.

Pitanja

?