VII – Nadzor računarskih mreža

S A D R Ž A J

1. **Osnovni pojmovi**
2. **SNMP (*Simple Network Management Protocol*)**
3. **Alati za nadzor mreža**
   a. **Nagios**
   b. **WireShark**
   c. **Win Performace Monitor**

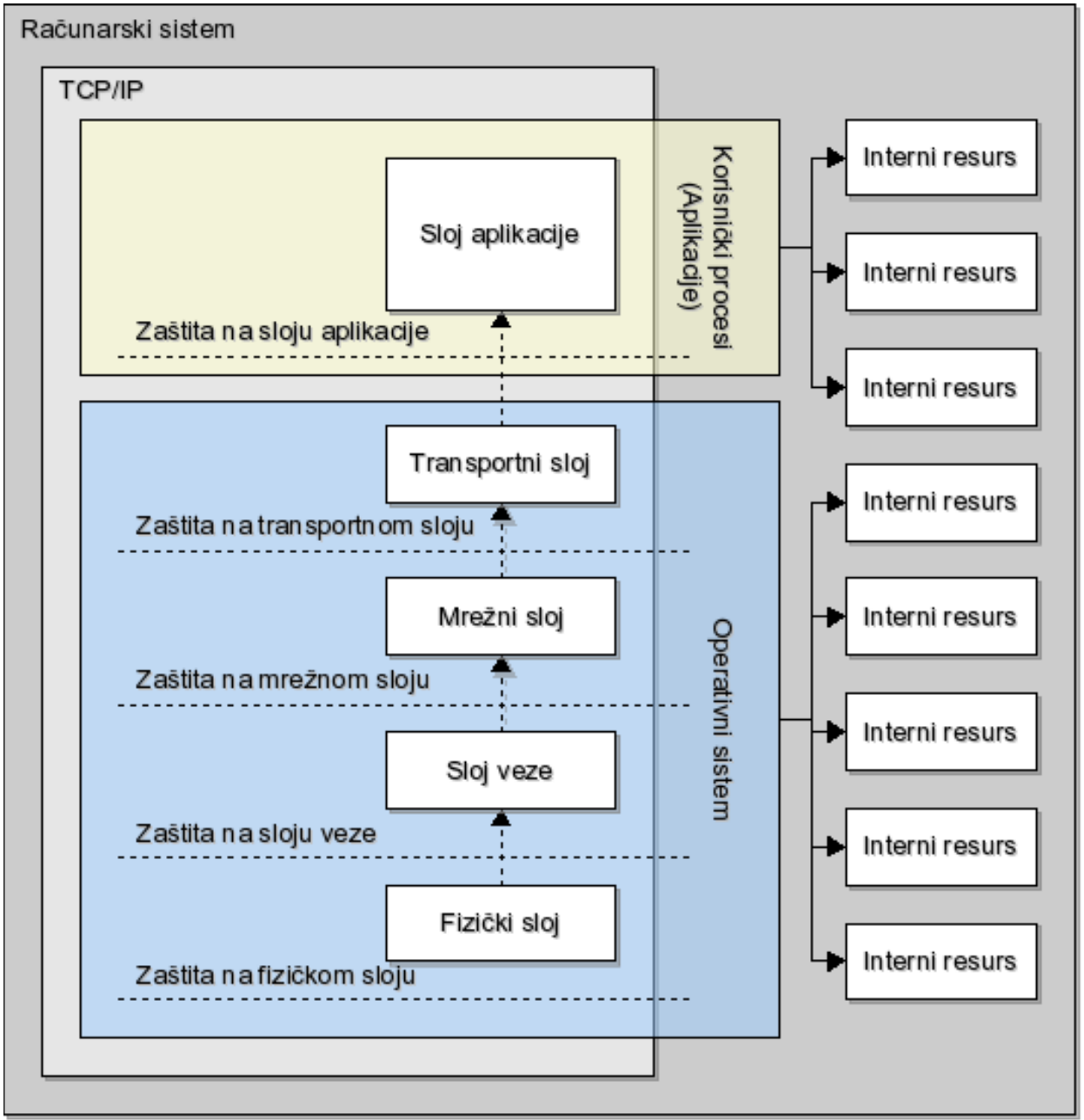
7 - Sigurnost i nadzor račun.mreža

- Širenje računarskih mreža i tehnologija doprinelo je da se više ne može zamisliti rad bez mogućnosti pristupa Internetu a E-biznis, Intranet i Ekstranet su neminovnost današnjeg poslovanja.
- Klijent/server tehnologija donosi mnoge prednosti, koje se ogledaju u lakšem pristupu i korišćenju podataka ali donosi i velike probleme
- Pouzdanost i raspoloživost računarskih sistema i mreža na kojima se temelje sve ove usluge postaje sve kritičniji aspekt, pa je veoma bitno da se obezbedi pouzdan skup **alata za kontrolu i nadzor mreža**.
- Sigurnost računara i mreža (*computer and network security*) je oblast koja se bavi nadzorom, praćenjem i sprečavanjem raznih opasnosti koje mogu prouzrokovati nestabilnost, prestanak rada ili bilo kakvu štetu na softveru i hardveru računara, tj. ugroziti normalan rad mreže.
- Pod pretpostavkom da je računar siguran od svih opasnosti (razne vrste infekcija i napada), korisnik bi trebao da uraditi ono što hoće na računaru, što nije slučaj ako je računar napadnut od strane nekog štetnog programa koji može da naškodi ili onemogući rad računara.

7.1 – Osnovni pojmovi

- U zavisnosti od uzroka pojavljivanja sve greške koje se javljaju na računarskim mrežama i mrežnim resursima možemo podeliti na:
  1. Greške koje se samoinicijativno pojavljuju usled propusta u definiciji hardverskih i softverskih komponenti računarskih mreža
  2. Greške koje se javljaju kao posledica neadekvatnog dizajniranja računarskih mreža i nenamenske upotrebe korišćenih komponenata
  3. Greške koje se javljaju usled neadekvatnog korišćenja računarskih mreža od strane korisnika nedovoljno obučenih za rad
  4. Greške koje se javljaju kao posledica iskorišćenja propusta u definiciji hardversko-softverskih komponenti računarskih mreža
- Za određivanje efikasnih metoda za zaštitu računarskih mreža potrebno je predhodno izvršiti analizu parametara koji karakterišu napade: izvore, nosioce i ciljeve napada kao i ponašanja u toku napada.
- Podatak o mogućim izvorima predstavlja i socijalnu i tehničku karakteristiku napada.
- Podaci o izvorima napada se najčešće dobijaju iterativnim kombinovanjem podataka dobijenih analizom.

7.1- Nivoi zaštite i pristupa



7.1 – Osnovni pojmovi

- Upravljanje mrežom (*network management*) je proces upravljanja složenom mrežom infrastrukturom sa ciljem da se maksimizira efikasnost i produktivnosti te mreže
- Veliki broj tehnika koje se primenjuju za stvaranje sigurnih sistema:
  1. **Kriptografija**, **jaka autentifikacija** i **kontrola pristupa**
  2. **Provereni softver** i **primena antivirusnog softvera**
  3. **Redovni backup**, **Firewall** i **bezbedne zone**
  4. **Uočavanje upada i preventiva**
- Korisnici očekuju sigurnu i pouzdanu mrežnu komunikaciju
- Postoje mnogi protokoli koji omogućavaju nadgledanje i upravljanje mrežnim resursima kao i praćenje mrežnog saobračaja
- Jedan od najpoznatijih je **SNMP** koji je postao mrežni standard
- Mnogi nezavisni proizvođači su razvili različite programske pakete sa velikim brojem migućnosti za nadgledanje mrežnog saobraćaja: **Nagios, WireShark, Win. performace Monitor, HP OpenView**

7.1 – Osnovni pojmovi

- Međunarodna organizacija za standarde (ISO) upravljanje mrežom podelila je u pet funkcionalnih domena:

1. ***Upravljanje kvarovima*** (*fault management*) daje mogućnost otkrivanja, izolovanja i otklanjanja neispravnih stanja u mreži.
2. ***Upravljanje obračunavanjem*** *troškova* (*accounting management*) daje mogućnost za naplatu troškova nastalih korišćenjem mrežnih resursa.
3. ***Upravljanje konfiguracijom*** (*configuration management*) služi za prikupljanje podataka od mrežnih objekata i za slanje podataka mrežnim objektima kojima se upravlja (konfiguracioni podaci).
4. ***Upravljanje performansama*** (*performance management*) služi za proračun i grafički prikaz ponašanja upravljanih mrežnih objekata i efikasnosti komunikacionih aktivnosti.
5. ***Upravljanje sigurnošću*** (*security management*) predstavlja one aspekte sigurnosti koji su važni za ispravan rad sistema upravljanja mrežom i za zaštitu mrežnih objekata.

7.2 - Upravljanje mrežom

1. Softver za predstavljanje upravljačkih podataka korisnicima (*user presentation software).* Interakcija korisnika i softvera za mrežno upravljanje odvija se kroz korisnčki interfejs koji treba da omogući nadzor i upravljanje mrežom. On treba da je bude isti (*unified)* na svim mrežnim čvorovima, nezavisno od proizvodača mrežne opreme.
2. Softver za upravljanje mrežom (*network management software).* Najviši sloj su aplikacije za upravljanje mrežom koje sadrže softverske module za obavljanje jednostavnih i opštih funkcija, kao što su npr. generisanje alarma, sistematizacija prikupljenih upravljačkih podataka i sl. Najniži sloj čini usluga transporta upravljačkih podataka (*network management data transport service)* koji sačinjavaju dve komponente: interfejs prema aplik.elementima i protokol upravljanja mrežom, koji je namenjen razmeni upravlj. informacija između upravljača i agenata
3. Softver za podršku aplikaciji mrežnog upravljanja (*network management support software).* Omogućava aplikaciji mrežnog upravljanja pristup bazi upravljačkih informacija (MIB - *Management Informat.Base*) i komunikaciju sa udaljenim agentima i upravljačima

7.2 - SNMP protokol

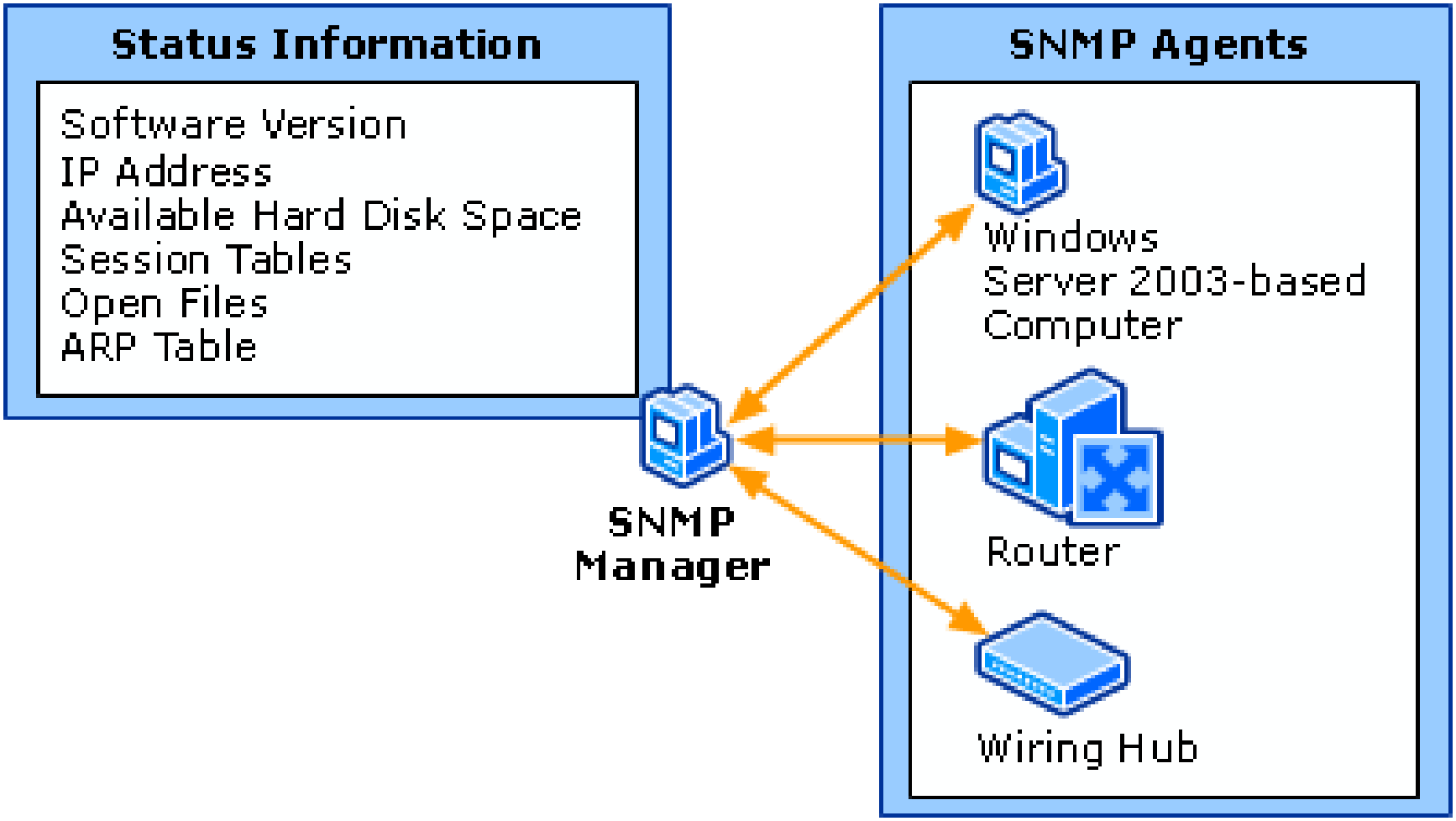
- Velike mreže sa stotinama ili hiljadama čvorova zahtevaju veliki broj IT stručnjaka koji bi trebalo da nadziru svaki računar kako bi se efikasno sproveo nadzor i upravljanje jednim ovakvim sistemom.
- Trenutno na tržištu postoje mnogi protokoli koji omogućavaju nadgledanje mrežnih resursa i upravljanje njima.
- **SNMP** (*Simple Network Management Protocol*) koji je nastao 1988, danas je postao dominantan mrežni standard u ovoj oblasti
- SNMP je upravljački protokol koji omogućava administratorima da nadgledaju rad mrežnih uređaja koristeći centralni server i softverske agente koji prate i prijavljuju rad SNMP uređaja.
- Može se reći da je SNMP standard za upravljanje i nadzor koji definiše strategiju upravljanja TCP/IP mrežama.
- SNMP obuhvata integrisanu kolekciju alata koji se naširoko koristi u LAN-u i omogućava nam da pratimo mrežne čvorove sa jednog hosta.
- Osim praćenja fizičkih uređaja (serveri, radne stanice, štampači, ruteri, mostovi, habovi), možemo pratiti i servise kao što su DHCP ili DNS.

7.2 – SNMP protokol

- Osnovne karakteristike SNMP-a su jedinstven operatorski interfejs i minimalna količina posebne opreme (sve je ugrađeno u opremu).
- Ključni elementi SNMP-a su integrisani skup alata za nadgledanje i kontrolu mreže, upravljačka stanica, upravljački agenti, upravljačka informaciona baza i protokol za upravljanje mrežom.
- Upravljanje mrežom može obuhvatati nekolilko skupova značajnih operacija, kao što su definisanje pojedinih parametara, preusmeravanje saobraćaja, rekonfigurisanje, distribuirani nadzor i upravljanje.
- Možemo koristiti SNMP za praćenje svih pokazivača performansi dostupnih u *System Monitor* TCP/IP, uključujući ICMP, IP, mrežne interfejse, TCP, UDP, DHCP, FTP, WINS, i IIS.
- Pored toga što prima statusne informacije, SNMP može poslati ***Set*** zahtev za konfigurisanje bilo kog objekta na kojem SNMP menadžer ima ***read/write*** dozvole.
- Koristeći SNMP softver za upravljanje (*SNMP management software*) možemo pratiti bilo koji uređaj na koji je instaliran SNMP klijent softver (*SNMP agent software*).

7.2 - SNMP protokol

- SNMP agent interaguje sa SNMP menadžerom kako bi omogućio deljenje informacija o statusu mreže između nagledanih uređaja i aplikacija sa jedne, i SNMP sistema za upravljanje koji vrši nadzor, sa druge strane.



7.2 – SNMP protokol

- Koristeći SNMP, možemo pratiti performanse i iskorišćenost mreže, detektovati greške na mreži ili nedozvoljene pristupe, i u nekim slučajevima konfigurisati udaljene uređaje.
- Dizajniran je da bude raspoređen na velikom broju mrežnih uređaja, da ima minimalan uticaj na praćeni uređaj, minimalne transportne zahteve, i da radi kada većina drugih mrežnih aplikacija otkaže.
- Jednostavan protokol jer se implementira sa relativno malo izvornog koda koji razdvaja upravljačku i hardversku arhitekturu uređaja
- SNMP menadžer prikazuje informacije koje prima u grafičkom korisničkom interfejsu.
- Na SNMP agentu se konfigurišu SNMP opcije, uključujući ***trap***, ali SNMP agent ne prikazuje informacije koje šalje ka menadžeru.
- Da bi omogućili komunikaciju između SNMP menadžera i SNMP agenata, oni moraju biti članovi iste SNMP zajednice.
- Ime zajednice funkcioniše kao lozinka za autentifikaciju komunikacije.
- SNMP zajednica je jedna SNMP definisana grupa; *nije grupa definisana u Aktivnom Direktorijumu.*

7.2 - SNMP arhitektura

- SNMP menadžer može zahtevati sledeće tipove informacija od agenta:
  - ✓**Identifikaciju mrežnog protokola i statistiku,**
  - ✓**Dinamičku identifikaciju uređaja priključenih na mrežu,**
  - ✓**Hardverske i softverske konfiguracione podatke,**
  - ✓**Performanse uređaja i statistiku korišćenja,**
  - ✓**Greške uređaja i poruke o događajima,**
  - ✓**Statistiku o korišćenju programa i aplikacija**.
- Da bi izvršio usluge monitoringa, koristi distribuiranu arhitekturu upravljačkih sistema i agenata, kao i nekoliko povezanih komponenti:
  - ✓ SNMP upravljački sistemi i agenti,
  - ✓ MIB baza,
  - ✓ SNMP poruke,
  - ✓ SNMP zajednica (*community*),
  - ✓ komunikacioni proces između SNMP menadžera i agenata.

7.2 - SNMP komunikacija

1.Menadžer,HostA, formira SNMP poruku koja sadrži zahtev za informacijom (*Get*) o broju aktivnih sesija, ime zajednice (MonitorInfo), i odredište poruke

5. Master agent komponenta SNMP agenta poziva odgovarajućeg agenta proširenja da preuzme zahtevanu informaciju o sesijama iz MIB baze

Host A
SNMP Manager

Host B
SNMP Agent

2.Menadžer šalje zahtev ka Hostu B koristeći SNMP bibliotečki servis

Community: MonitorInfo
IP Address: 131.107.7.29

From Host A to Host B:
Get Active Sessions
Community: MonitorInfo
Destination: 131.107.7.24

7. Host B šalje odgovor ka Hostu A
From Host B to Host A:
Number of Sessions: 2
Community: MonitorInfo
Destination: 131.107.7.29

Community: MonitorInfo
Community: TrapAlarm
IP Address: 131.107.7.24

6. Koristeći informaciju o sesijama koju je primio od agenta proširenja, SNMP servis formira povratnu SNMP poruku koja sadrži broj aktivnih sesija i odredište-IP adresu (131.107.7.29) SNMP menadžera, Hosta A

4. Ako je *community* ime Hosta A različito, Host B će poslati „*authentication failure*“ trap ka Hostu C

Community: TrapAlarm
IP Address: 131.107.7.15

Host C
SNMP Manager

3. Kada Host B primi poruku, proverava da li je ime zajednice (*MonitorInfo*) iz primljenog paketa na listi prihvatljivih *community* imena, procenjuje zahtev na osnovu dozvola pristupa iz agentove liste za tu zajednicu, i verifikuje izvornu IP adresu

7.2 – Komunikacioni proces menađer-agent

1. SNMP menadžer, Host A, formira SNMP poruku koja sadrži zahtev za informacijom (*Get*) o broju aktivnih sesija, ime zajednice (*community name*) kojoj SNMP menadžer pripada, i odredište poruke – IP adresa (131.107.7.24) SNMP agenta, Hosta B.
2. Menadžer šalje zahtev ka Hostu B koristeći SNMP bibliotečki servis.
3. Kada Host B primi poruku, proverava da li je ime zajednice (*MonitorInfo*) iz primljenog paketa na listi prihvatljivih *community* imena, procenjuje zahtev na osnovu dozvola pristupa iz agentove liste za tu zajednicu, i verifikuje izvornu IP adresu.
4. Ukoliko su *community* ime ili dozvole nekorektne, i SNMP servis je konfigurisan da šalje *authentication trap*, agent šalje jedan „*authentication failure*“ trap ka specificiranom trap odredištu,Hostu C.
5. Master agent komponenta SNMP agenta poziva odgovarajućeg agenta proširenja da preuzme zahtevanu informaciju o sesijama iz MIB.
6. Koristeći informaciju o sesijama koju je primio od agenta proširenja, SNMP servis formira povratnu SNMP poruku koja sadrži broj aktivnih sesija i odredište-IP adresu (131.107.7.29) SNMP menadžera, Hosta A.
7. Host B šalje odgovor ka Hostu A.

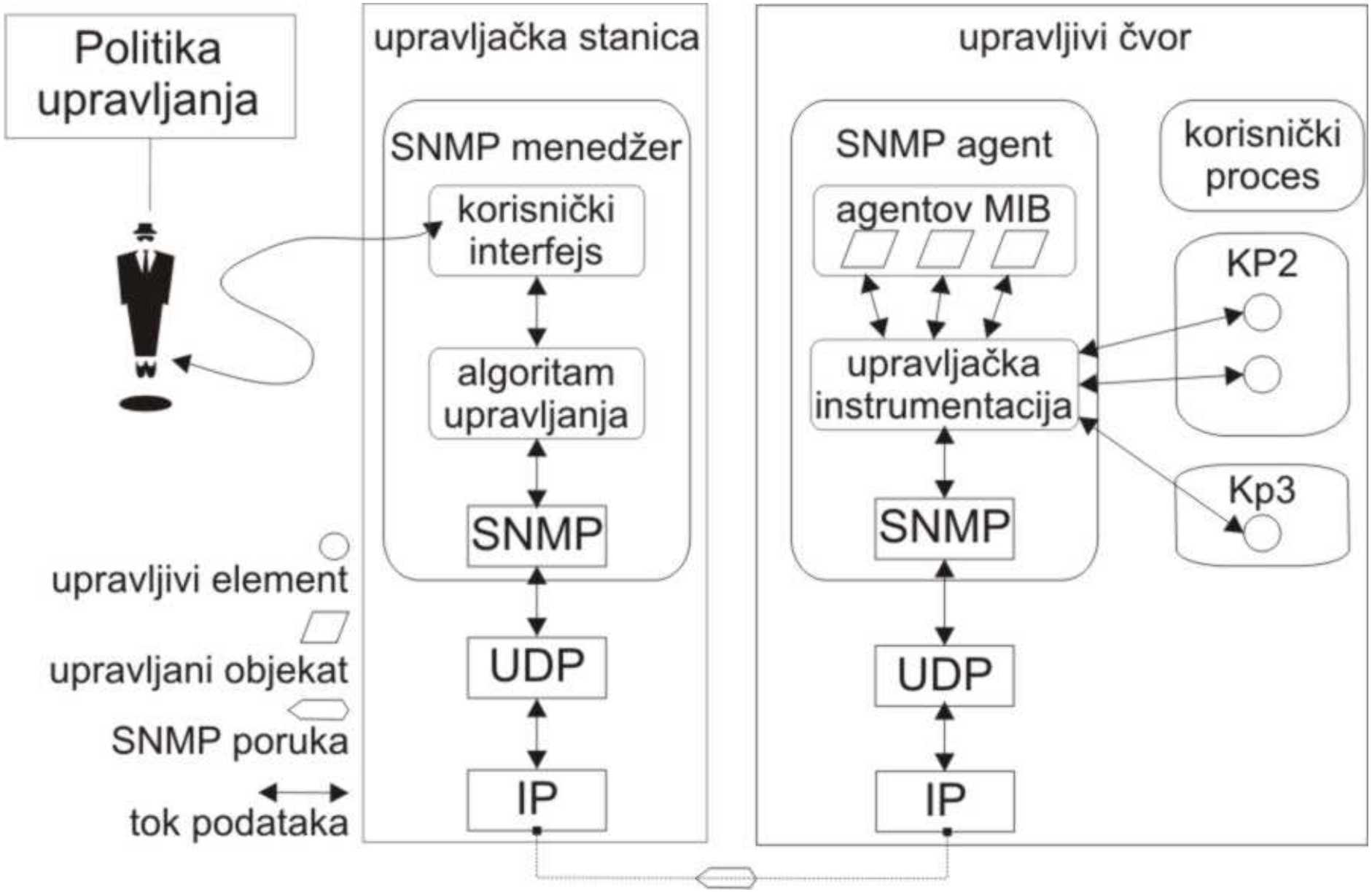
7.2 – Osnovni delovi SNMP sistema

1. **Upravljačka stanica** (*network management station*) jeste mrežni računar koji ima procesnu sposobnost dovoljnu za izvršavanje upravljačke aplikacije.
2. **Upravljačka aplikacija** (*management application*), koja se često naziva i SNMP menadžer (*SNMP manager*) ili samo menadžer, računarski je program koji nadgleda upravljane elemente na upravljanim čvorovima mreže i upravlja njima u skladu s politikom upravljanja (*management policy*) koju je definisao čovek - upravnik računarske mreže.
3. **Upravljački čvor** (*managed node*) mrežni je uređaj čijim se stanjima, ili stanjima nekih njegovih delova koje nazivamo upravljani elementi (*managed elements*), upravlja ili se ona samo nadgledaju. Prema složenosti i funkciji, upravljani čvorovi mogu biti vrlo raznovrsni; na primer, to mogu biti razne vrste mrežnih računara, servera, terminali, ruteri, modemi, mrežni štampači.

7.2 – Osnovni delovi SNMP sistema

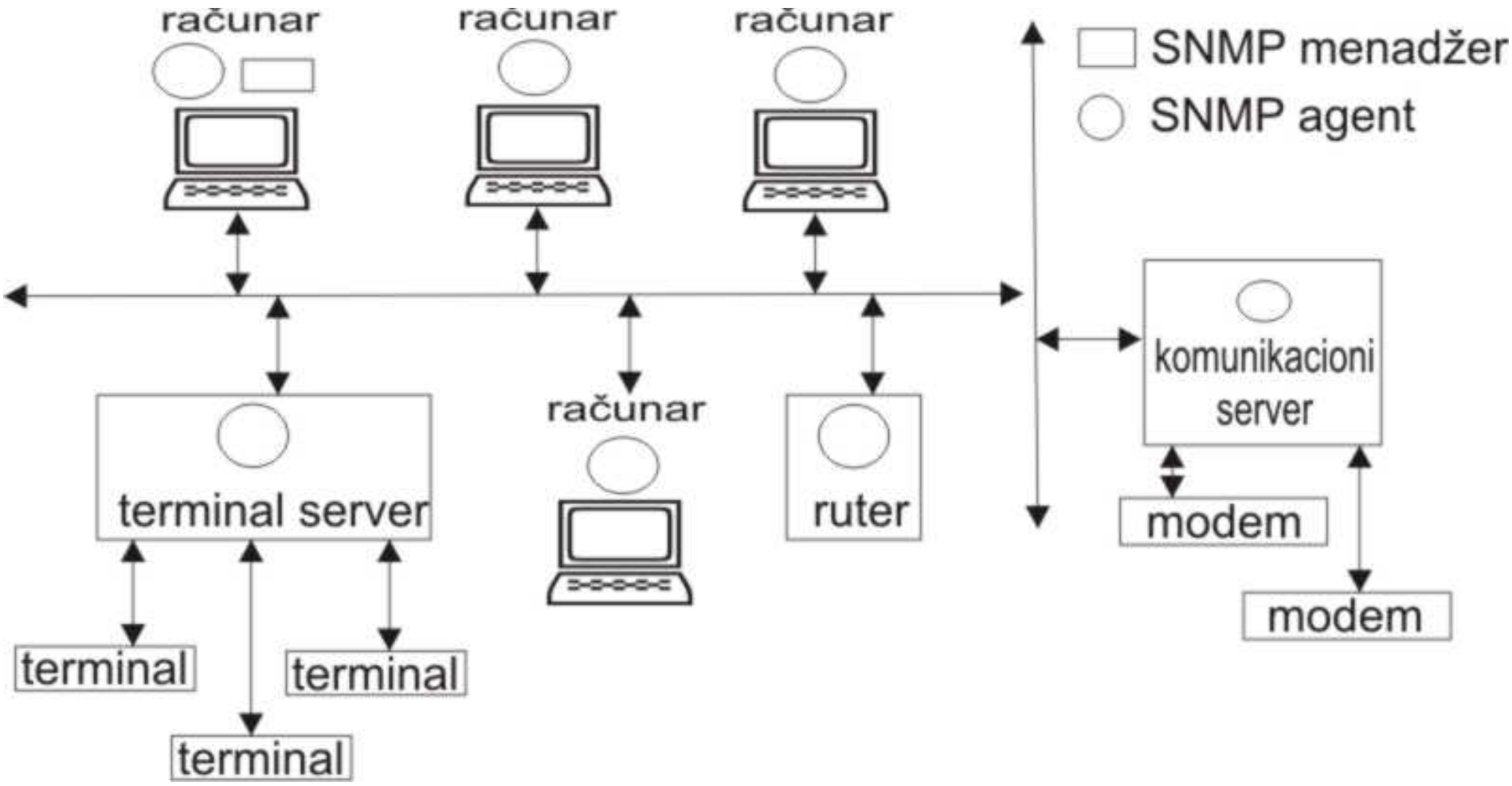
4. **Upravljački agent** ili SNMP agent je procesni entitet (program ili deo programa) koji se izvršava na upravljanom čvoru i ima potrebnu upravljačku instrumentaciju (*management instrumentation*) pomoću koje upravlja korisnim funkcijama elemenata u upravljanom čvoru. Upravljačka instrumentacija upravlja komunikacijom sa upravljanim elementima, tj. njihovim strukturama podataka i, s druge strane, predstavlja te strukture kao skup upravljanih objekata.
5. **Upravljačke informacije** (*management information*) predstavljaju podatke o stanjima upravljanih elemenata u upravljanom čvoru. SNMP menadžer nadgleda stanja tih elemenata, dok postavljanjem njihovih vrednosti menja ta stanja. Upravljačke informacije, koje su fizički smeštene u SNMP agentima, SNMP menadžer vidi kao skup upravljaniih objekata (*managed objects*) smeštenih u virtuelnom skladištu informacija koje se naziva baza upravljačkih informacija (*Management Information Base*, MIB).
6. **Protokol SNMP** po kojem se upravljačke informacije prenose izmedu upravljačkih aplikacija i agenata.

7.2 – SNMP upravljanje mrežom



7.2 – Komponente SNMP mreže

- Tri ključne komponente SNMP upravljačke mreže su: **upravljani uređaji, agent i NMS** (*Network Management System*):



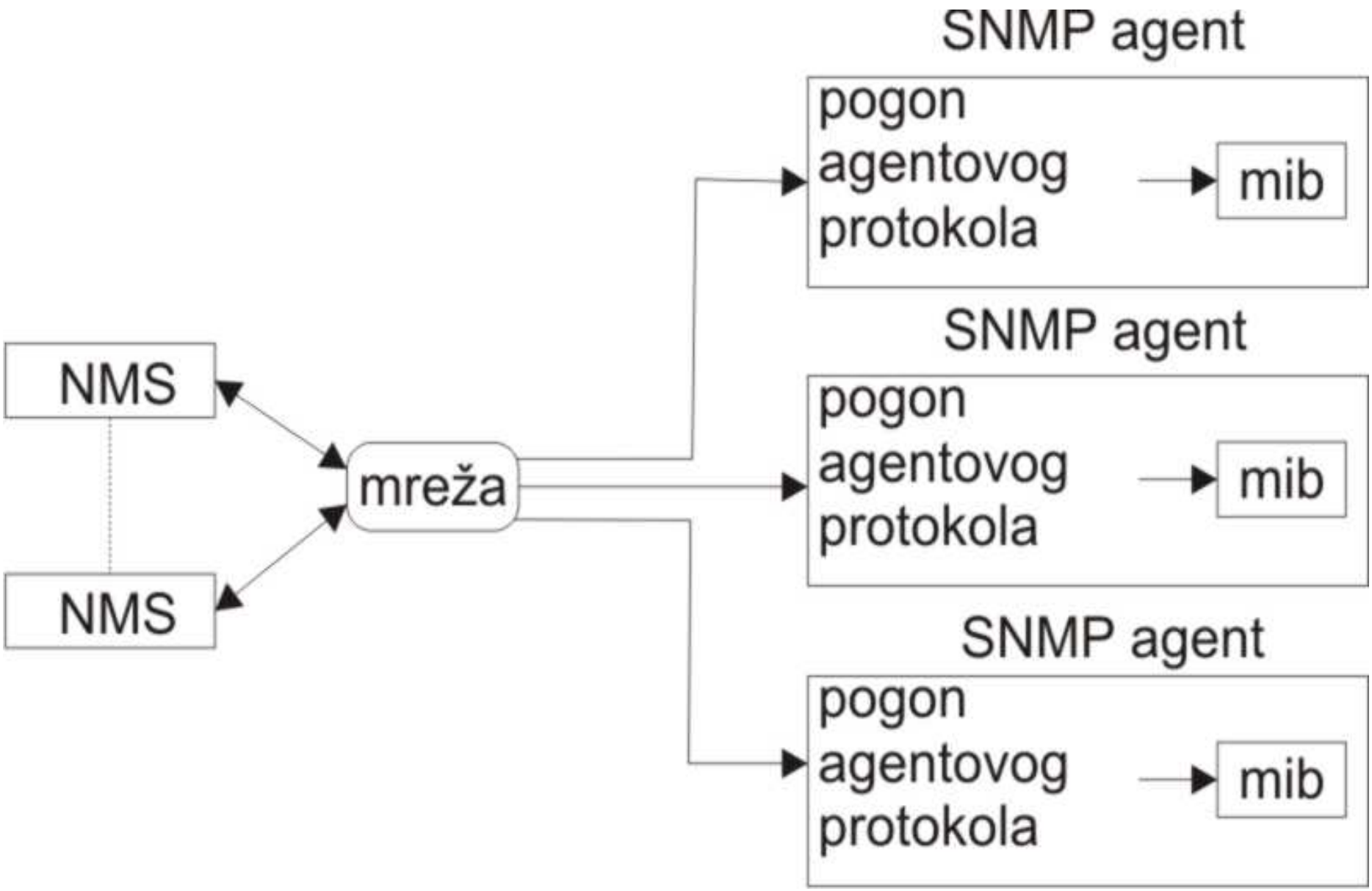
7.2 – Komponente SNMP

1. **Upravljani uređaj** je 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 mogu biti ruteri, serveri za daljinski pristup (*access server*), komutatori, štampači itd.

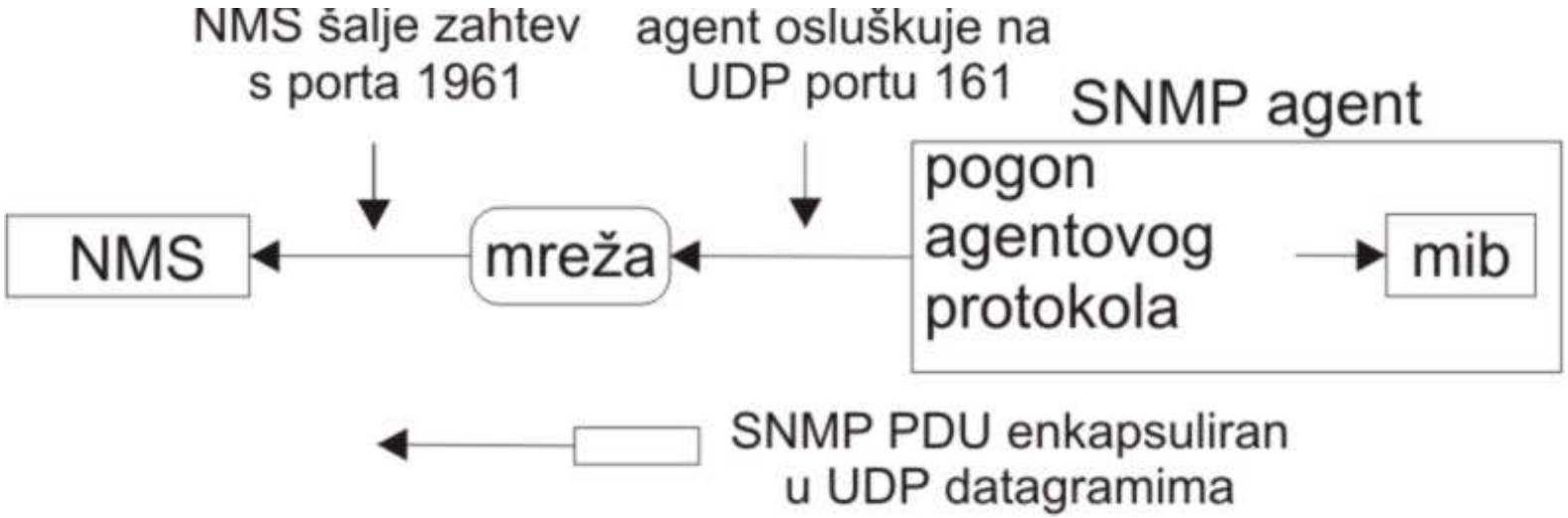
2. **Agent** je mrežno-upravljački softverski modul koji je smešten na uređaju za upravljanje. On ima lokalno znanje o upravljačkim informacijama i prevodi ih u oblik kompatibilan sa SNMP-om. Omogućava udaljeni pristup opremi za upravljanje.

3. **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.

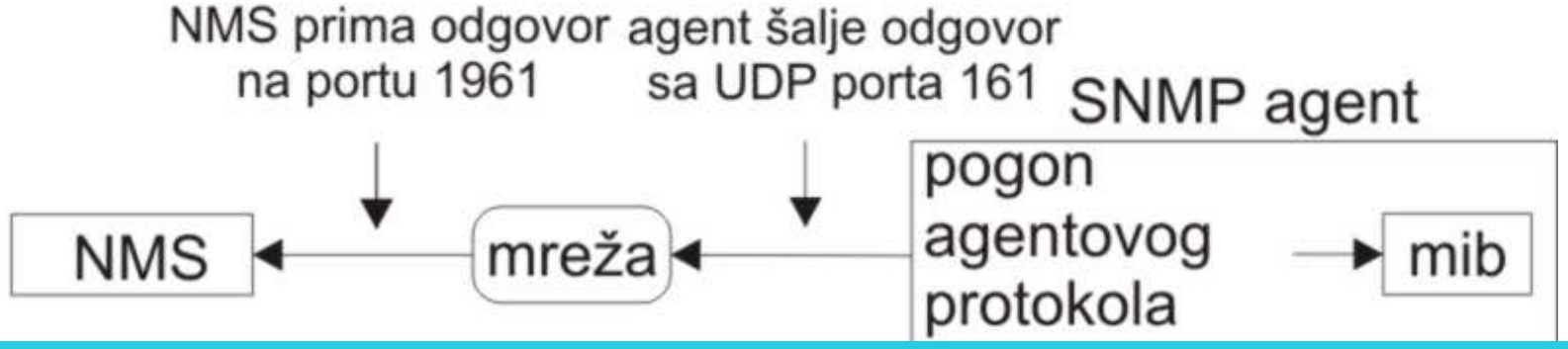
7.2-Model SNMP upravljačke mreže



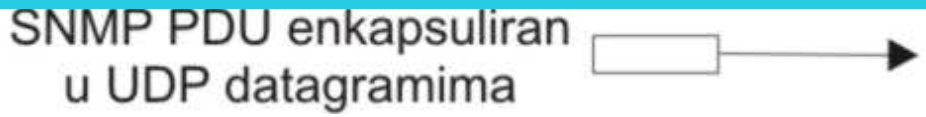
7.2 – Način rada SNMP protokola



Veličina SNMP poruke ograničena je max. veličinom UDP poruke a sve SNMP implementacije moraju primiti pakete min. dužine 484B

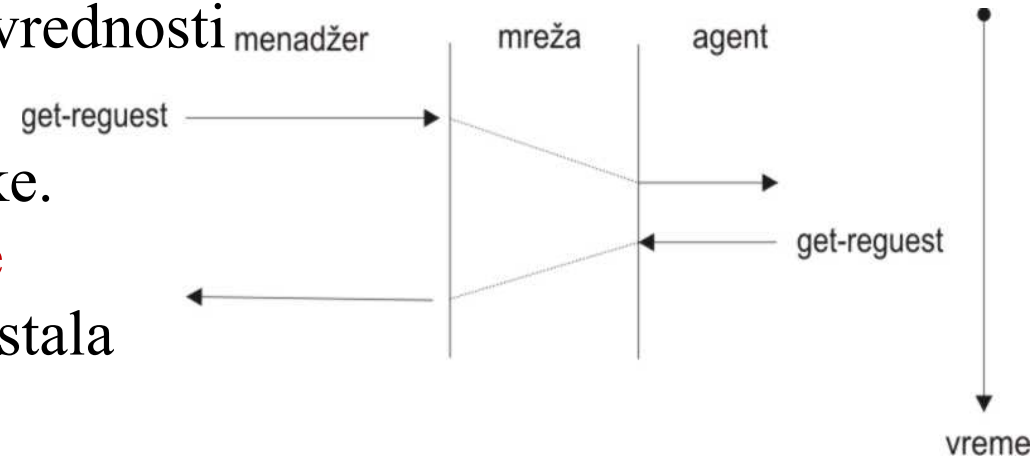


Ako nastane greška kod prenosa, prima se poruka na NMS portu 162.



7.2 – Način rada SNMP protokola

- Upravljačka konzola prikuplja podatke od SNMP agenata na svakom pojedinom upravljivom uređaju i čuva ih organizovane u bazi podataka koja se naziva *Management Information Base* (MIB).
- Zapisi u MIB bazi jedinstvenog su formata, tako da SNMP upravljačke jedinice mogu te informacije o upravljivim uređajima u mreži prezentovati administratoru sistema i to obično na upravljačkoj konzoli.
- SNMP se zasniva na modelu menadžer/agent
- SNMP je jednostavan jer agent zahteva minimalan softver.
- Da bi bio jednostavan, SNMP sadrži ograničen skup naredaba i odgovora: ***get***, ***get next*** i ***set*** za dobijanje pojedinačnih ili grupnih promenljivih ili za utvrđivanje vrednosti pojedinačnih promenljivih.
- Agent šalje odgovor na te poruke.
- Agent, takođe, šalje trap poruke upravljačkom sistemu ako je nastala greška.



7.2 – Vrste poruka u SNMP saobraćaju

➢Postoji pet osnovnih poruka tj. jedinica podataka SNMP protokola:

1. ***Get request*** - zahteva vrednost jedne ili više promenljivih u MIB bazi.
2. ***Get next request*** - omogućava menadžeru da dođe do narednih (sledećih u nizu) vrednosti. Koristi se za čitanje vrednosti narednih promenljivih u MIB bazi; često se koristi za čitanje redova tabele.
3. ***Set request*** - osvežava tj. ažurira (engl. *update*) MIB promenljive.
4. ***Get response*** - vraća odgovor na *get request*, *get next request* ili *set request*.
5. ***Trap*** - javlja da je nastao problem ili značajan događaj

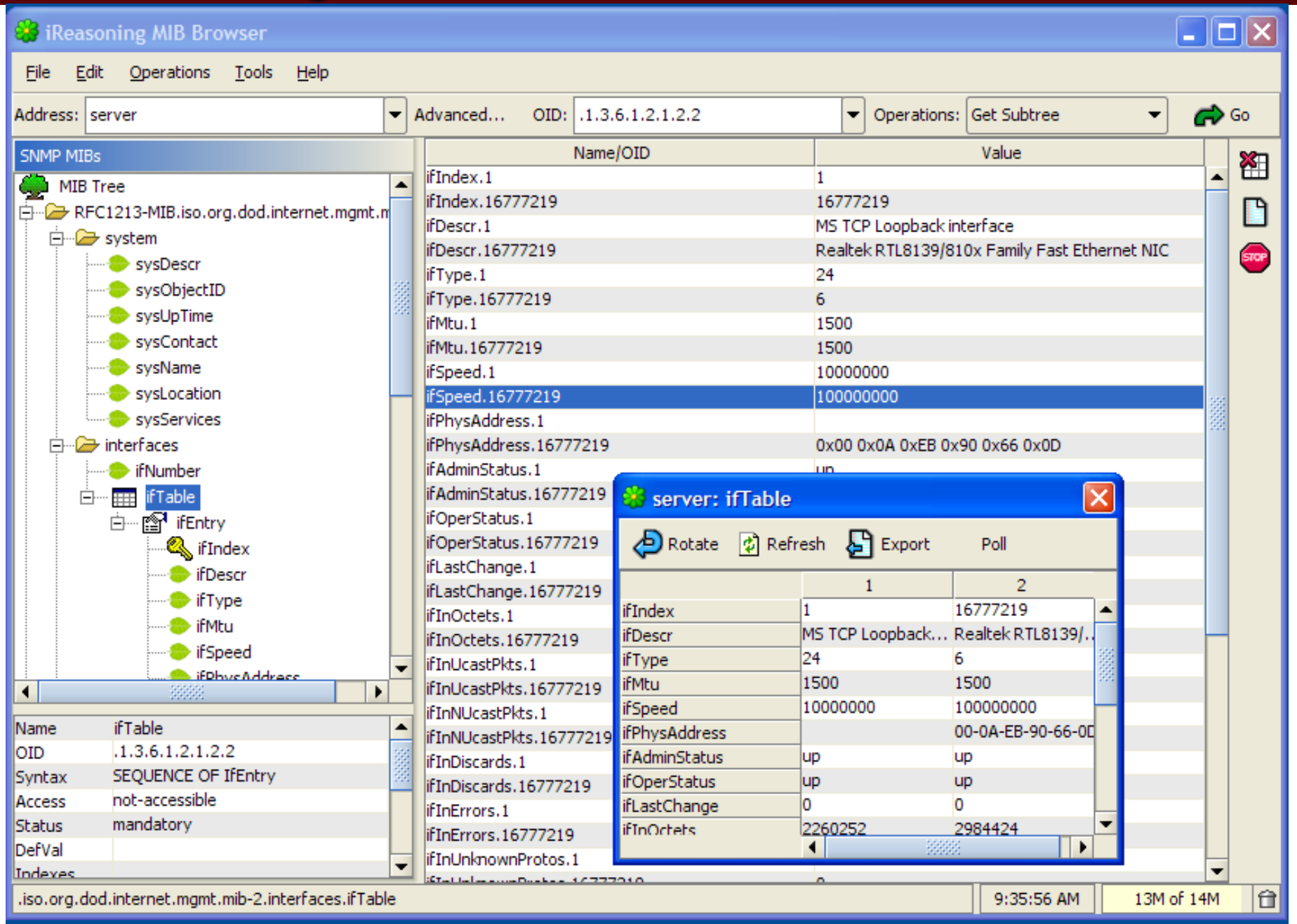
7.2 – Osnovne SNMP naredbe

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

7.2-Management Information Base (MIB)

- MIB baza sadrži informacije o komandama i ciljnim objektima - upravljivim entitetima ili potencijalnim izvorima informacija o statusu
- MIB baza predstavlja hijerarhijski organizovan skup informacija.
- To je logička baza upravljačkih informacija/definicija, napravljena na osnovu konfiguracije i statističkih informacija uskladištenih na uređaju
- MIB-u se pristupa preko mrežnog protokola kao što je SNMP.
- Sastoji se od upravljanih objekata i prepoznaje se na osnovu identifikatora objekata (*OID - Object Identifier*) koji jednoznačno obeležavaju upravljane objekte u MIB hijerarhiji.
- Svaki upravljani objekat ima bazu podataka, tj. vrednosti, za svaku definiciju zapisanu u MIB-u.
- Postoje dve vrste upravljanih objekata: skalarni i tabelarni.
- **Skalarni objekti** definišu pojedinačne instance objekata a **tablični** definišu više povezanih instanci objekata grupisanih u MIB tabelu
- Postoje brojni uslužni programi (otvorenog koda, besplatni ill komercijalni) za operativne sisteme Windows i Linux, koji služe za prevođenje i pregledanje MIB datoteka tj. baza.

7.2-Management Information Base (MIB)



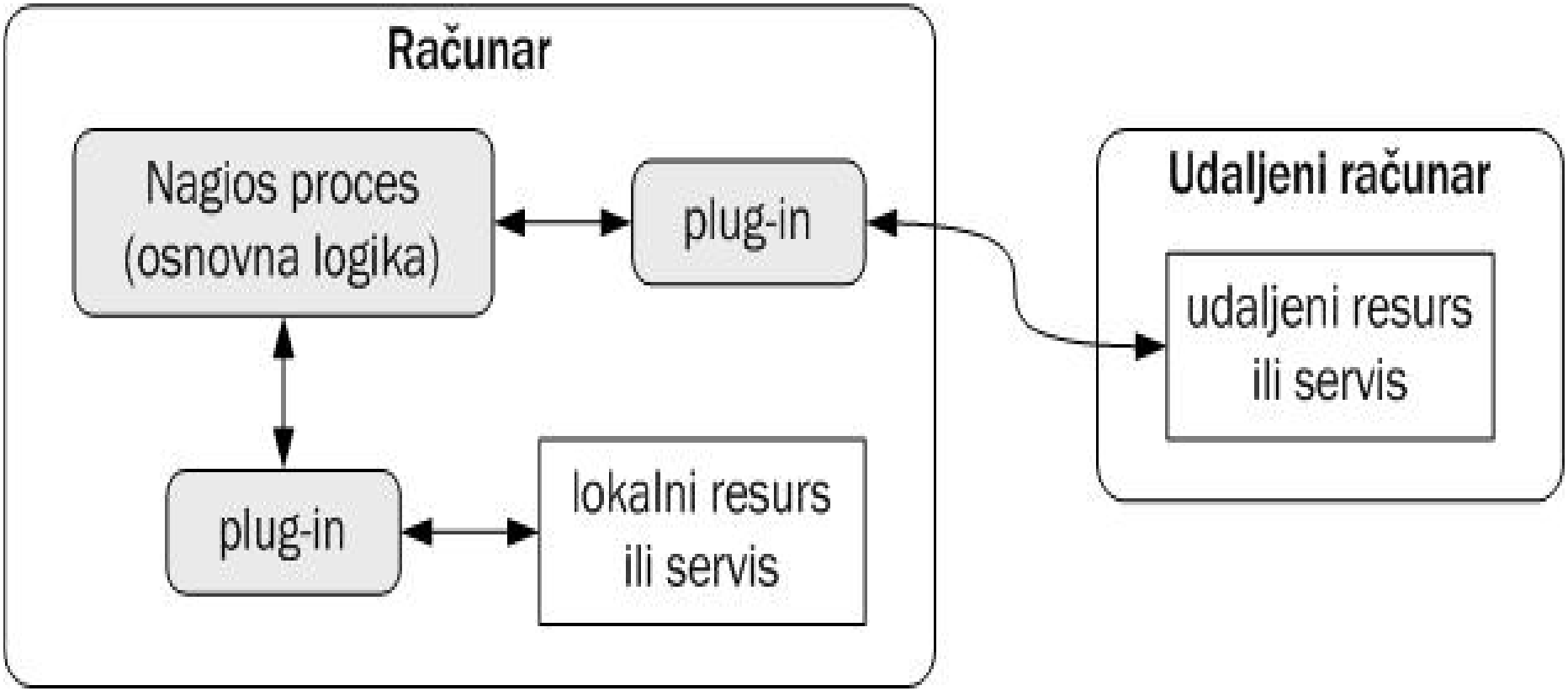
7.3 – Alati za nadgledanje rada mreže

- Trenutno je na tržištu prisutno mnogo komercijalnih alatki koje omogućavaju **nagledanje i upravljanje mrežnim resursima**.
- Primer jako dobrog alata je **HP OpenView** Network Node Manager, HP OpenView Network Configuration Manager.
- Postoje i paketi open source zajednice - **Nagios**, koji omogućava funkcionalno i pouzdano realizovanje sistema za praćenje mreže.
- Druga rešenje koja omogućavaju takođe open source analizatore paketa svakako ubrajaju **Wireshark** koji je korišćen za rešavanje problema u mreži, analizu komunikacionih protokola i portova.
- Od strane Microsoft-a imamo rešenje korišćenja **Servers Check Monitoring** alata za praćenje, izveštavanje i upozoravanje o mreži i dostupnosti stanja sistema.
- Možemo pratiti uređaje, korišćenjem bilo kog TCP porta (HTTP, HTTPS, FTP, NNTP, POP3, SMTP, VNC, DNS) kao i izvršavati proveru baza podataka (ODBC, Oracle, MySql), kao i hvatati SNMP vrednosti kao što su prostor na diskovima, dostupnost memorije, iskorišćenja procesora i drugih.

7.3 – Mogućnosti Nagios programa

1. nadgledanje dostupnosti svih mrežnih servisa (PING, DNS, HTTP, ...)
2. nadgledanje sistemskih resursa hostova (opterećenje procesora, iskorišćenost RAM memorije, opterećenje hard diskova, stanje mrežnih interfejsova, status vitalnih procesa, itd.)
3. Jednostavni *plug-in* koncept koji dozvoljava korisniku da lako razvija i implementira sopstvene *plagin*-ove za nadgledanje specifičnih servisa
4. paralelno nadgledanje servisa
5. otkrivanje i razlikovanje hostova koji su nedostupni od onih koji su pali pomoću ugrađenog koncepta roditeljskih hostova i mre.hijerarhije
6. obaveštavanje u slučaju pojave neregularnog rada hostova ili servisa i njihovog oporavka (putem e-maila, pejdžera, SMS-a)
7. mogućnost da se definišu *hendleri* događaja (*event handlers*) koji su aktivni za vreme izvršavanja servisa ili dešavanja događaja na hostu
8. automatsku rotaciju log-a
9. podršku za implementaciju redundantnih servera za nadgledanje mreže
10. podršku za implementaciju distribuiranog nadgledanja mreže
11. informativan web interfejs za uvid u tekući status mreže

7.3 Modularna arhitektura prog.paketa Nagios



7.3 Home Dashboard prog.paketa Nagios

Nagios XI | Home | Views | Dashboards | Reports | Configure | Tools | Help | Admin | nagiosadmin | Logout

Quick View
- Home Dashboard
- Tactical Overview
- Birdseye
- Operations Center
- Operations Screen
- Open Service Problems
- Open Host Problems
- All Service Problems
- All Host Problems
- Network Outages

Details
- Service Detail
- Host Detail
- Hostgroup Summary
- Hostgroup Overview
- Hostgroup Grid
- Servicegroup Summary
- Servicegroup Overview
- Servicegroup Grid
- BPI
- Metrics

Graphs
- Performance Graphs
- Graph Explorer

Maps
- BBmap
- Hypermap
- Minemap
- Nagvis
- Network Status Map
- Legacy Network Status Map

Incident Management
- Latest Alerts
- Acknowledgements
- Scheduled Downtime
- Mass Acknowledge
- Recurring Downtime
- Notifications

Monitoring Process
- Process Info
- Performance
- Event Log

Home Dashboard

Getting Started Guide

Common Tasks:

- Change your account settings
  Change your account password and general preferences.
- Change your notifications settings
  Change how and when you receive alert notifications.
- Configure your monitoring setup
  Add or modify items to be monitored with easy-to-use wizards.

Getting Started:

- Learn about XI
  Learn more about XI and its capabilities.
- Signup for XI news
  Stay informed on the latest updates and happenings for XI.

Administrative Tasks

Task
Initial Setup Tasks:

- Configure system settings
  Configure basic settings for your XI system.
- Reset security credentials
  Change the default credentials used by the XI system.
- Configure mail settings
  Configure email settings for your XI system.

Ongoing Tasks:

- Configure your monitoring setup
  Add or modify items to be monitored.
- Add new user accounts
  Setup new users with access to Nagios XI.

Host Status Summary

Up	Down	Unreachable	Pending
1	0	0	0

Unhandled	Problems	All
0	0	1

Last Updated: 2016-12-01 13:46:20

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
12	0	0	0	0

Unhandled	Problems	All
0	0	12

Last Updated: 2016-12-01 13:46:20

We're Here To Help!

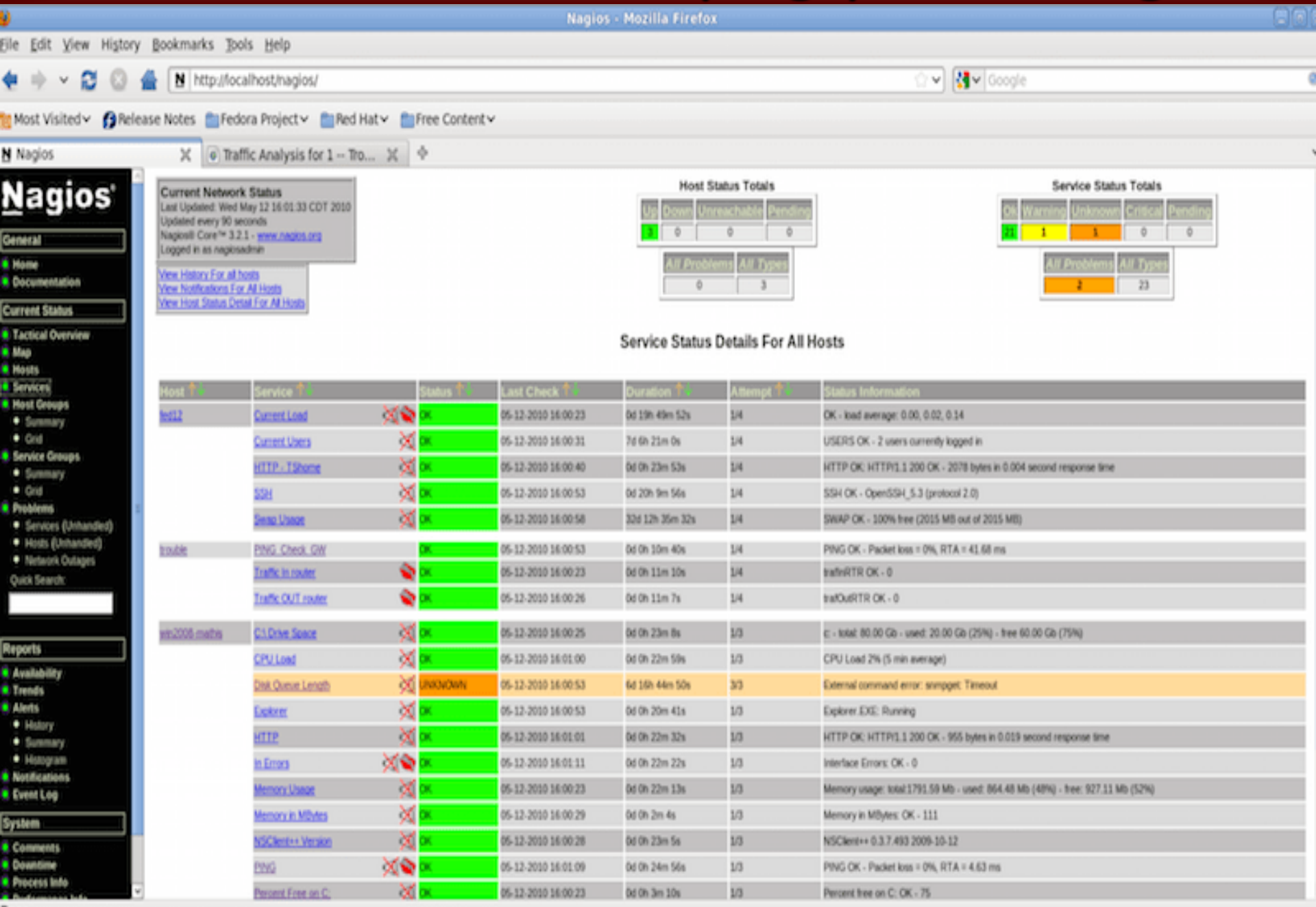
Our knowledgeable techs are happy to help you with any questions or problems you may have getting Nagios up and running.

- Support Forum / Customer Support Forum
- ? Help Resources
- Email Support: customersupport@nagios.com
- Phone Support: +1 651-204-9102 Ext. 4

Start Monitoring

Run a Config Wizard | Run Auto-Discovery | Advanced Config

7.3 Home Dashboard prog.paketa Nagios



7.3 Grafički prikaz performansi servisa

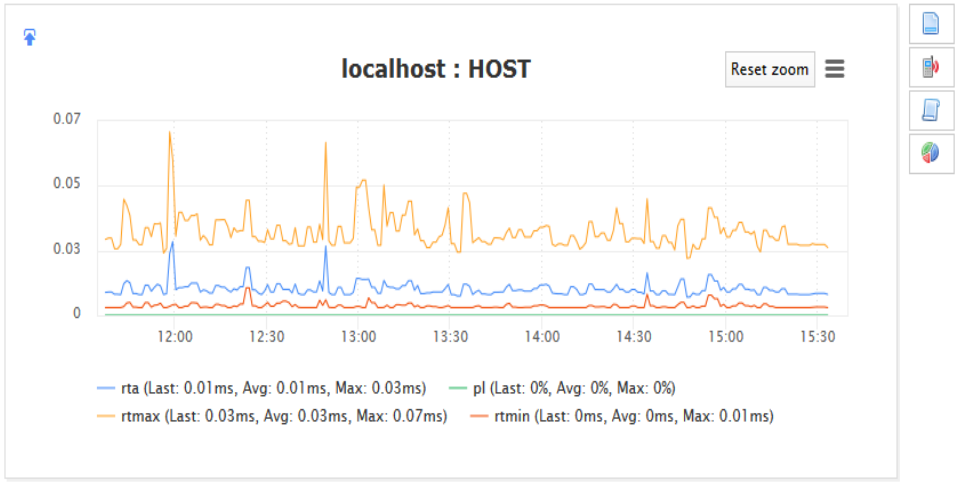
Time Period: Last 4 Hours | Host: localhost | Update | Search...

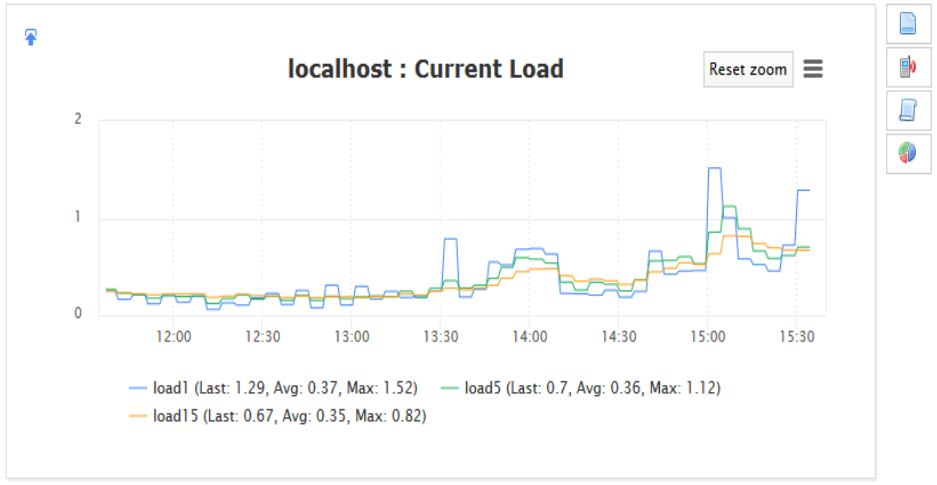
Performance Graphs

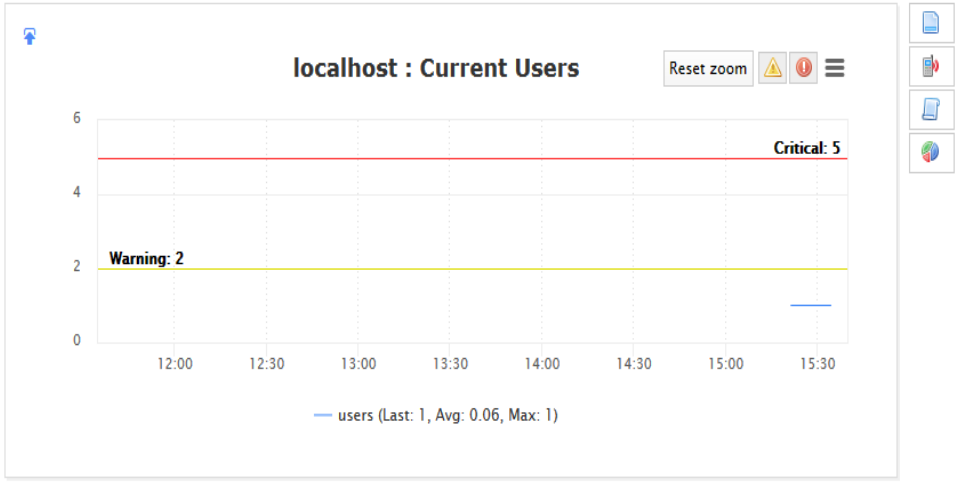
localhost Performance Graphs - 4 Hour View

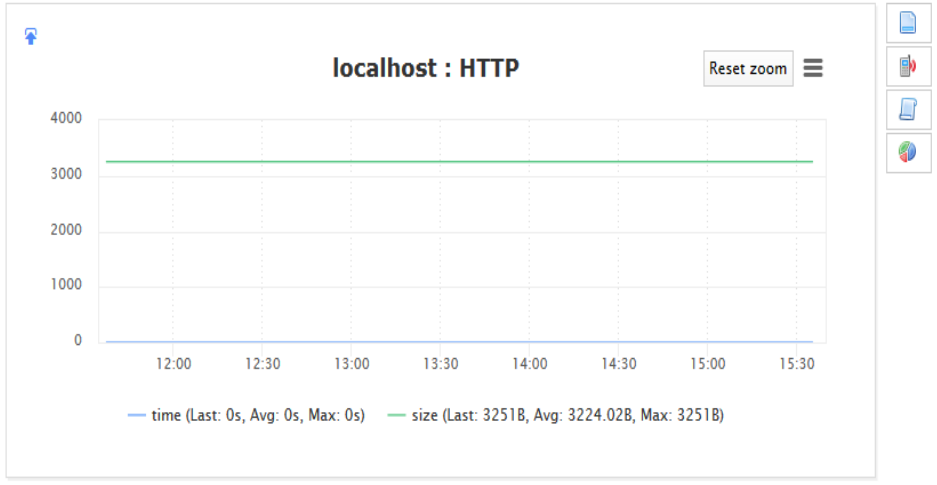
Showing 1-21 of 21 total records

Page 1 of 1 | 200 Per Page | Go







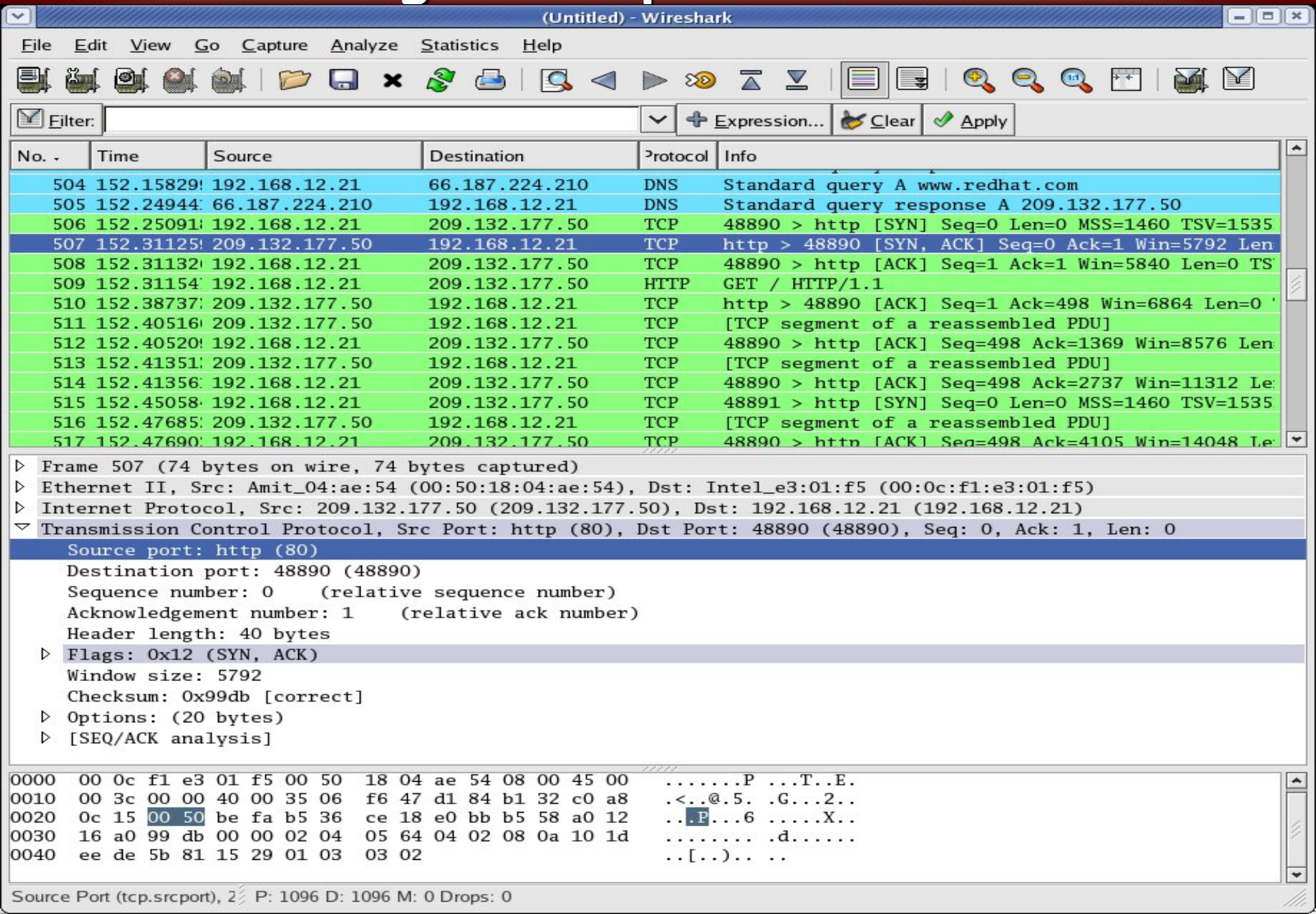


7.3 Programski paket WireShark

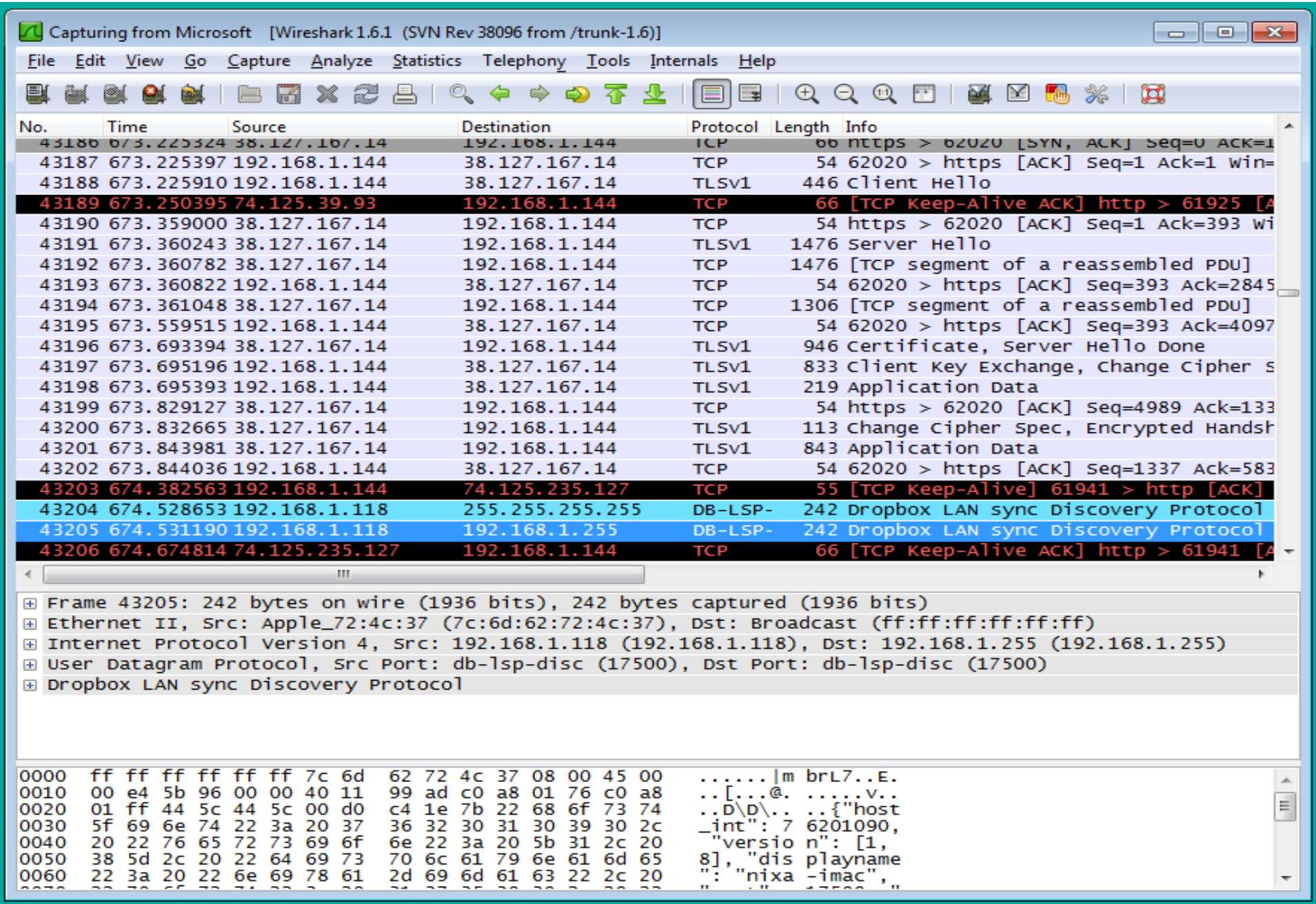
- Najpoznatiji prihvaćen program za analizu mrežnog saobraćaja
- Omogućuje nam da na "mikroskopskom nivou" vidimo šta se dešava na našoj mreži i ***de facto*** je (i često ***de jure***) postao je **standard**
- Poseduje jako bogat set funkcija koji uključuje sledeće:

✓ Detaljan pregled velikog broja protokola koji se stalno dopunjuju
✓ Trenutno snimanje mrežnog saobraćaja (***on-line***) i ***off-line*** analiza
✓ Radi na velikom broju OS: Windows, Linux, macOS, Solaris, i td.
✓ Snimljeni mrežni podaci mogu se pregledati putem GUI-ja ili putem uslužnog programa TShark
✓ Mogućnost postavljanja različitih filtera
✓ Bogata VoIP analiza
✓ Podrška za čitanje i upisivanja u različitim formatima datoteka
✓ Podaci uživo se mogu čitati sa Etherneta, IEEE 802.11, PPP / HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relai, FDDI i drugih
✓ Podrška za dešifrovanje mnogih protokola, uključujući IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, VEP i VPA / VPA2
✓ Pravila bojenja mogu se primeniti na listu paketa za intuitivnu analizu

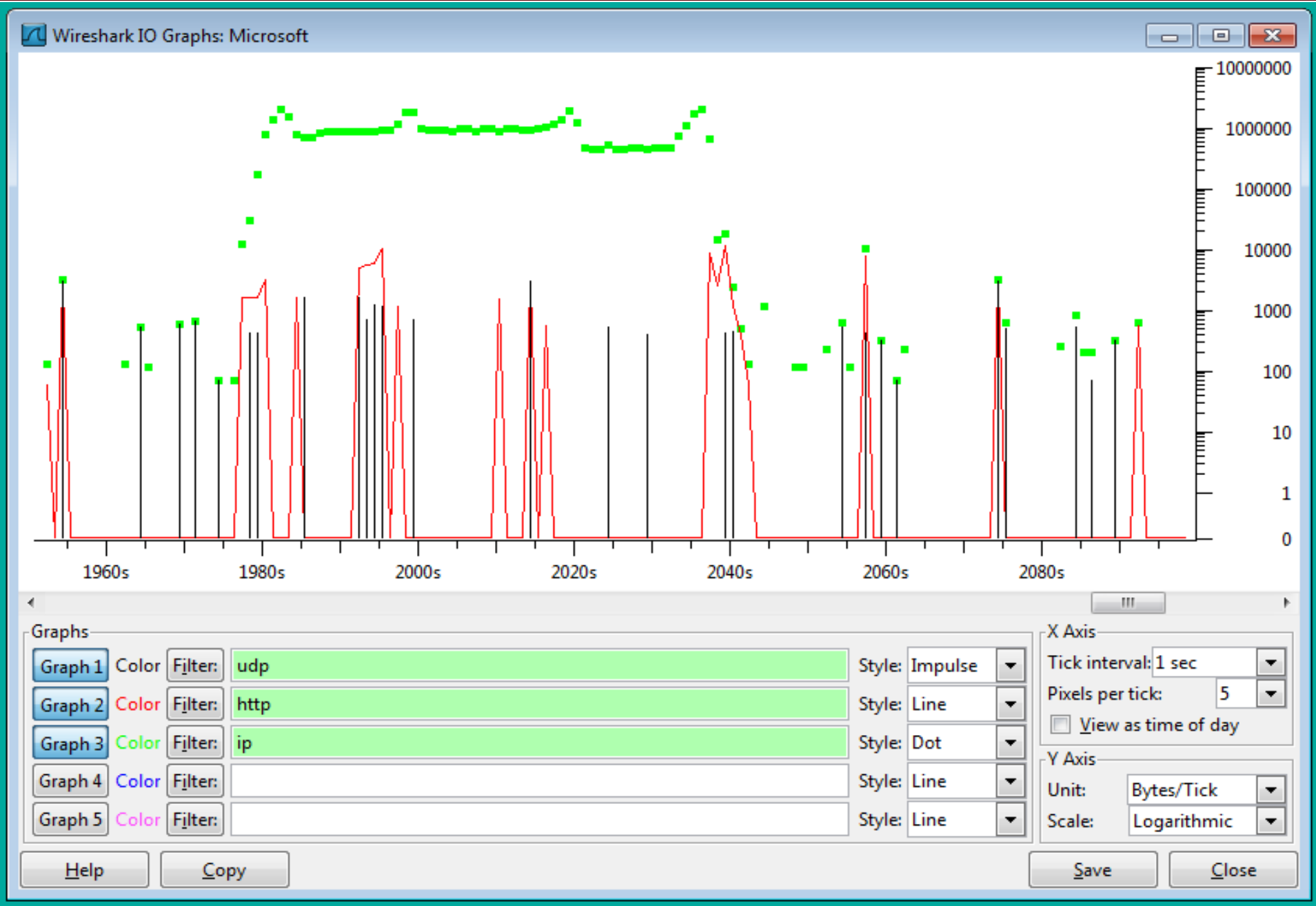
7.3 Programski paket WireShark



7.3 Programski paket WireShark



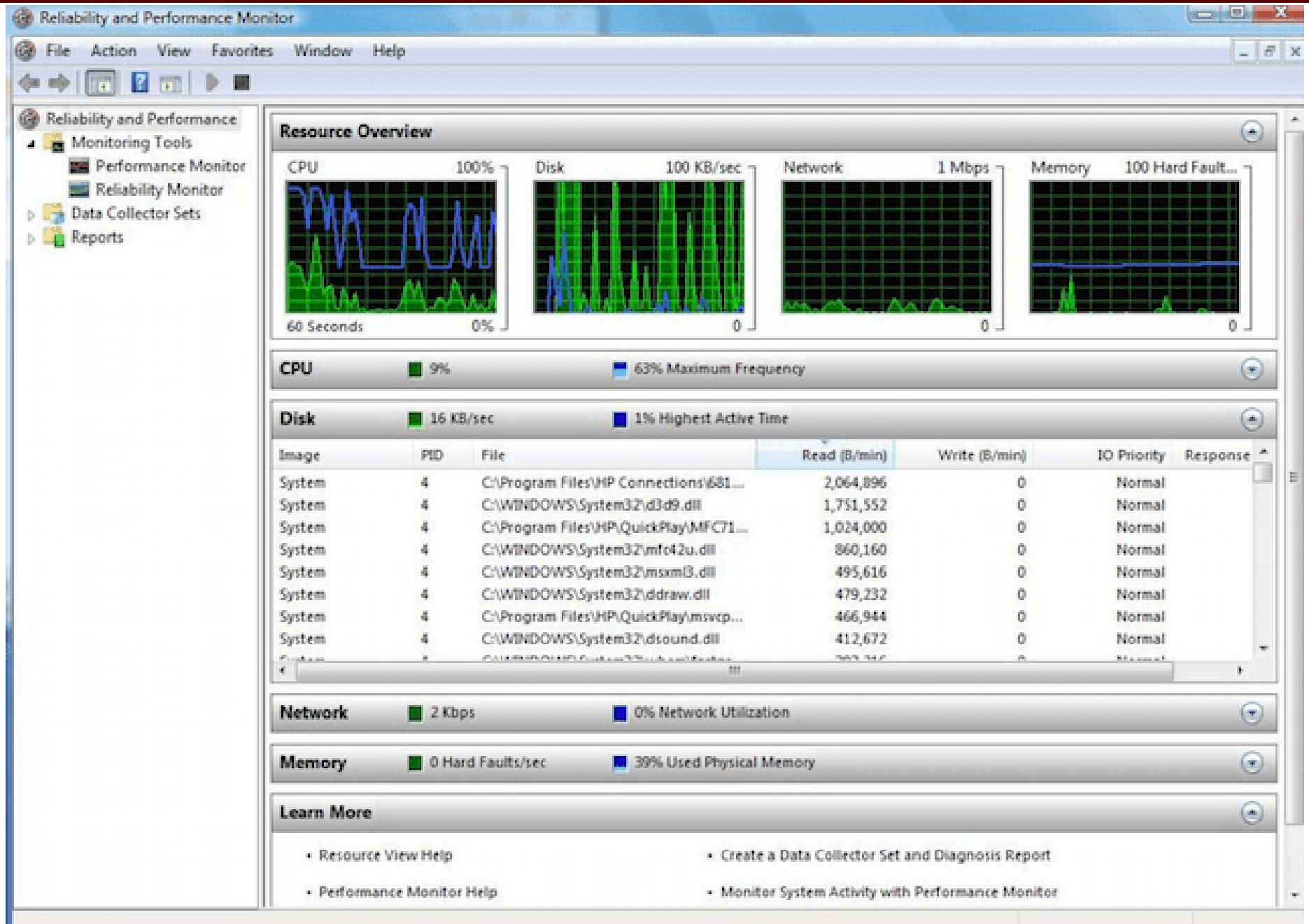
7.3 Programski paket WireShark



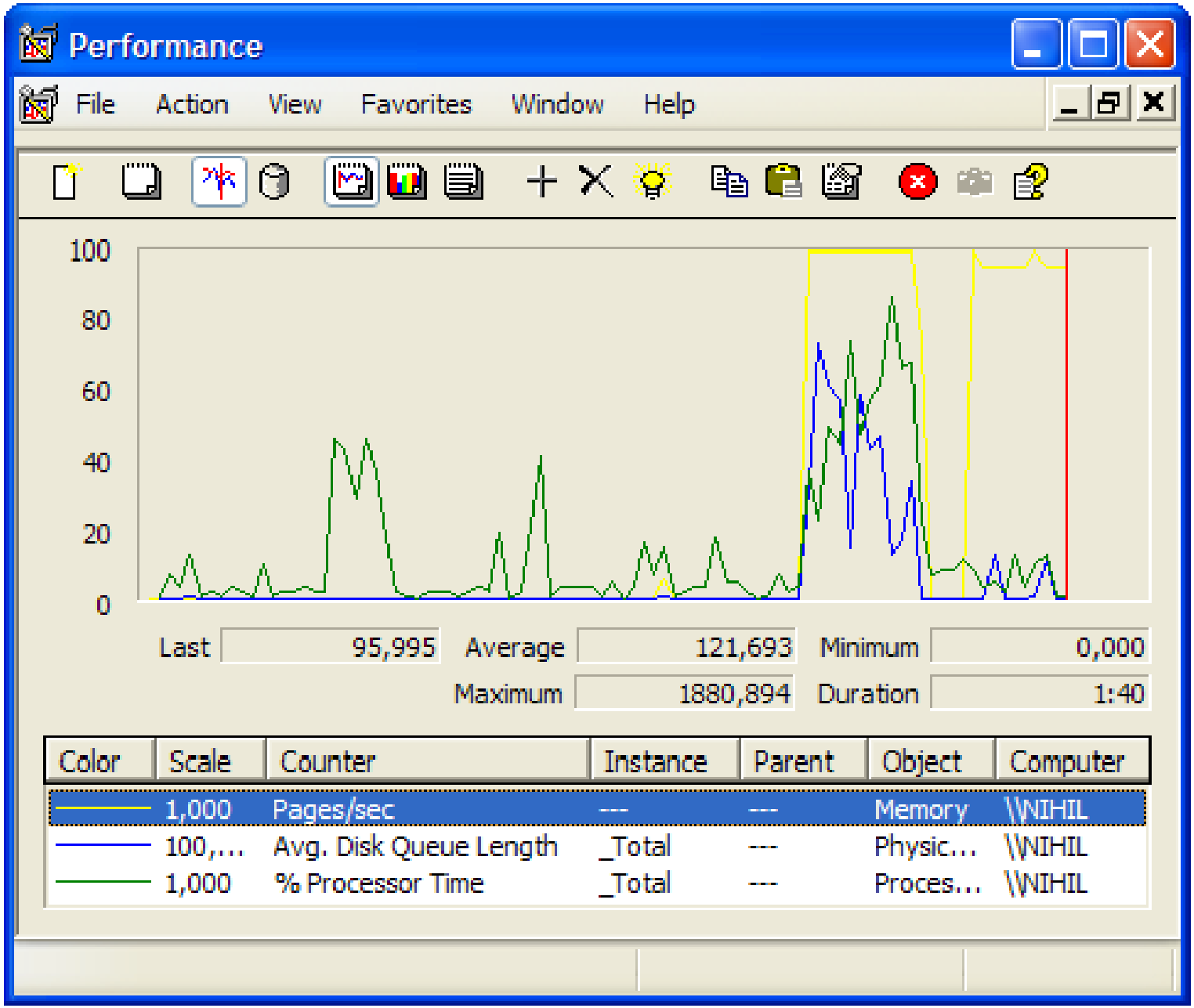
7.3 Monitor performansi kod WIN sistema

- **Glavni alat** za upravljanje brojačima performansi u OS Windows.
- Microsoft Windovs Performance Monitor je alat koji administratori mogu da koriste kako bi pregledali kako programi koji rade na matičnim računarima utiču na performanse tog računara.
- Alat se može koristiti u realnom vremenu, a može se koristiti i za prikupljanje informacija u log fajlu za kasniju analizu tih podataka
- Program koristi informacije o sistemskoj konfiguraciji, brojače performansi i trenutne podatke da bi u potpunosti dao performanse
- Sve informacije mogu se kombinovati u skupove sakupljača podataka.
- Brojači performansi vrše merenja aktivnosti sistema i stanja sistema u pojedinačnim aplikacijama ili u celom operativnom sistemu.
- Log podaci se prikupljaju sa komponentama davaoca praćenja u pojedinačnim aplikacijama ili sa komponentama operativnog sistema.
- Administratori mogu da kombinuju više pružaoca usluga praćenja u nešto što se naziva **sesija praćenja**.
- Mogu se snimati vrednosti u intervalima ili u određenim trenucima.
- Performance Monitor je dostupan u sistemima od Windows 7.

7.3 Monitor performansi kod WIN sistema



7.3 Monitor performansi kod WIN sistema



Hvala na pažnji !!!

Pitanja

? ? ?