HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Look@LAN programskog paketa

CCERT-PUBDOC-2007-09-204

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

***LS&S*, www.lss.hr -** laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Svakodnevno korištenje računala bilo bi nezamislivo bez lokalnih računalnih mreža (eng. *LAN – Local Area Network*). Računalne mreže su prisutne u svim segmentima društvenog života, počevši od banaka i financijskih institucija, bolnica pa sve do različitih edukacijskih ustanova poput fakulteta. Također, sve više privatnih korisnika koristi manje lokalne mreže u okviru svojih domova. Zbog svega navedenog, potreba za računalnim mrežama je neupitna. Ispravnost rada mreže kritična je za ispravan rad čitavog sustava koji ju koristi, a svaki prestanak rada može donijeti značajne štete.

Ta činjenica uvjetovala je nastavak odgovarajuće programske podrške koja se koristiti za neprekidan nadzor računalne mreže (eng. *Network Monitor*). Zadatak takvog alata je upozoriti administratora na usporen, djelomičan ili potpuno neispravan rad mreže odnosno usluga na mreži. Tu je uključena potencijalna neispravnost uzrokovana zagušenjem poslužitelja, mrežnih kanala, usmjerivača i ostalih mrežnih uređaja.

Jedan od alata koji se ističe mnogim karakteristikama nad konkurencijom je i Look@LAN. Intuitivan i jednostavan alat namijenjen je svim korisnicima bez obzira na veličinu i složenost nadgledane računalne mreže.

Dokument daje kratak osvrt na samu aplikaciju te opisuje njeno korištenje počevši od preuzimanja i instalacije. Slijedi opis naprednijeg korištenja ovog mrežnog nadglednika te savjeti za interpretaciju dobivenih rezultata.

2. Look@LAN programski paket

Autor Look@LAN paketa je Carlo Medas, a paket je namijenjen za korištenje na Windows operacijskim sustavima. Temeljna zamisao je bila razviti alat koji će pomoći korisnicima u instalaciji, podešavanju, nadgledanju i upravljanju mrežama. Paket je zamišljen kao pomoćni alat kod svih opsega mreža: od lokalnih računalnih mreža (eng. *LAN - Local Area Network*) do globalnih mreža (eng. *WAN – Wide Area Network*).

Look@LAN paket je besplatno rješenje namijenjeno osobnoj, ali i komercijalnoj uporabi. Radi se o naprednom mrežnom nadgledniku kojeg je moguće podesiti za rad doslovno u nekoliko klikova mišem. Neke od značajnijih karakteristika uključuju:

- automatsko detektiranje mrežnih postavki,
- kontinuirani nadzor,
- mehanizam za stvaranje preglednih izvješća,
- statističke podatke i grafove,
- pregled mreže u obliku stabla,
- mrežni dnevnik,
- temeljiti pregled pojedinog računala s mreže,
- detekcija operacijskog sustava i td.

Ovim alatom moguće je nadzirati i primarne čvorove mreže koji obuhvaćaju

- usmjerivače (eng. *router*),
- vatrozide (eng. *firewall*),
- prevoditelje adresa (eng. *NAT – Network Address Translation*),
- preklopnike (eng. *swtich*) i
- mrežne sabirne uređaje (eng. *HUB, concentrator*).

Look@LAN nadzorni alat uz komercijalan paket istog proizvođača Medas VNS (eng. *Visual Network Statistics*), korisniku omogućava potpuni uvid u detalje svakog mrežnog elementa koji podržava SNMP (eng. *Simple Network Management Protocol*). Na ovaj način moguće je prikupiti statističke podatke mrežnih sučelja, podatke protokola o proizvoljnom segmentu TCP/IP arhitekture, informacije o aktivnim TCP (eng. *Transmission Control Protocol*) i UDP (eng. *User Datagram Protocol*) priključcima te popis dostupnih TCP/IP mreža.

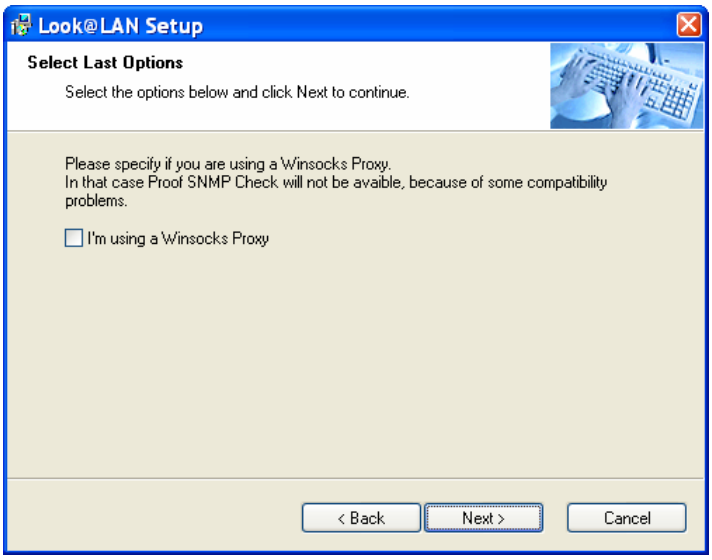
3. Preuzimanje i instalacija paketa

3.1. Preuzimanje

Postupak preuzimanja paketa vrlo je jednostavan. Pristupom web stranici proizvođača, http://www.lookatlan.com/ uočava se pregledan izbornik s kojeg treba odabrati poveznicu *Download*. Tekuća inačica paketa nosi oznaku Look@LAN 2.50 build 35, a datira još od siječnja 2006. godine. Veličina instalacijske datoteke je nešto veća od 2 MB. Radi se o inačici namijenjenoj Microsoft Windows operacijskim sustavima, ali to ne uključuje nove Windows Vista sustave.

3.2. Instalacija

Instalacija paketa je prilično jednostavna te uključuje samo odabir nekoliko osnovnih opcija (jezik: engleski ili talijanski; instalacijski direktorij), te prihvaćanje nekomercijalne licence pod kojom se paket distribuira. Jedino nestandardno pitanje tijekom instalacije je ono vezano uz korištenje *Winsocks Proxy* vatrozida / proxy poslužitelja, prikazano na slici 1. Korištenje *Winsocks Proxy* paketa uzrokuje probleme u radu Look@LAN alata te se korisnik obavještava da je posljedica toga nedostupnost usluge „*Proof SNMP Check*" Look@LAN programskog paketa.



Slika 1. Pitanje vezano uz Winsocks Proxy

Nakon instalacije korisniku su dostupna 2 alata:

- Look@LAN alat za analizu LAN mreže
- Look@Host alat za analizu određenog host računala unutar mreže

Prilikom pokretanja bilo kojeg od alata, ukoliko je uključen *Windows* vatrozid sa standardnim postavkama, pojavit će se *Windows* sigurnosno upozorenje (Slika 2) kod kojeg je potrebno odabrati opciju „*Unblock*" da se omogući rad oba alata.

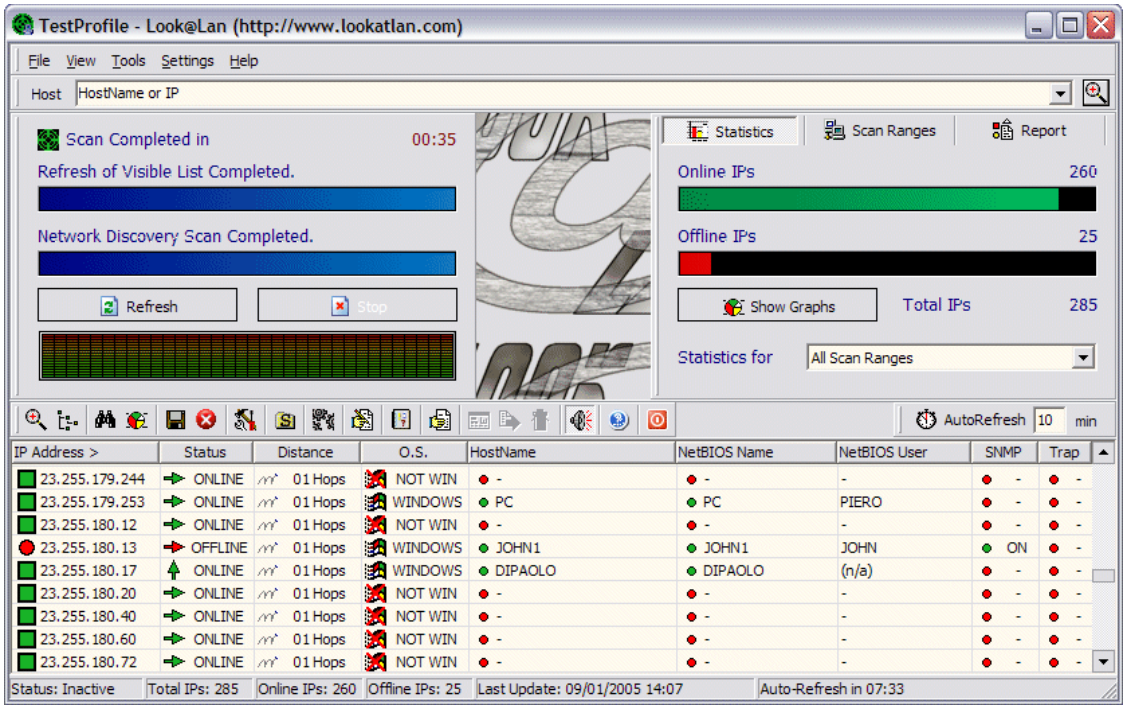
Slika 2. Windows sigurnosna upozorenja prilikom prvog pokretanja Look@LAN i Look@Host alata

4. Sučelje i funkcionalnosti

4.1. Osnovni podaci

Look@LAN alat se pokreće iz *Windows Start* izbornika nakon čega se pojavljuje prozor za izbor korisničkog profila, odnosno profila korisnikove mreže. U profilu se pohranjuju podaci o učinjenoj analizi mreže koji sadrže informacije o svim pronađenim računalima i njihovim atributima. Budući da se alat koristi za analizu mreža moguće je za svaku analiziranu mrežu nakon analize pohraniti njen profil te prilikom sljedeće analize pomoću postojećeg profila, otkriti izmjene koje su se dogodile između dvije analize.

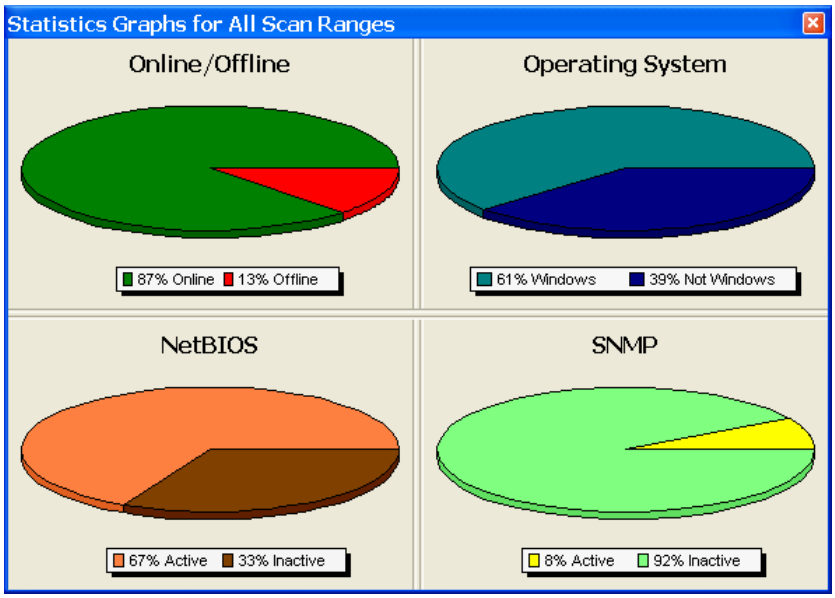
Kod prvog pokretanja alata korisnik mora kreirati novi profil, a nakon kreiranja profila alat provodi inicijalnu analizu mreže i prezentira rezultate analize kao na slici 3.



Slika 3. Prikaz rezultata analize mreže alatom Look@LAN

Kao što je vidljivo iz slike 3 rezultati uključuju sljedeće podatke:

- Popis svih aktivnih računala unutar korisnikove LAN mreže i njihove sljedeće karakteristike:
  - IP adresu ispitivanog računala,
  - status ispitivanog računala (aktivan ili neaktivan) – neaktivna računala su računala koja su detektirana nekom prethodnom analizom u toj mreži, ali prilikom zadnje analize nisu bila aktivna,
  - udaljenost – udaljenost ispitivanog računala od računala s kojeg se obavlja analiza,
  - operacijski sustav ispitivanog računala – alat ne detektira sve operacijske sustave već samo prijavljuje da li je na nekom računalu instaliran Windows operacijski sustav ili neki drugi,
  - naziv ispitivanog računala,
  - NetBIOS naziv ispitivanog računala,
  - NetBIOS naziv korisnika ispitivanog računala,
  - SNMP podršku – podatak da li ispitivano računalo podržava SNMP protokol i
  - *Trap* – podatak da li ispitivano računalo podržava SNMP *Trap* poruke.
- Statistiku analize mreže koja daje podatke o broju aktivnih odnosno neaktivnih računala u mreži u vrijeme analize. Statistiku je moguće vidjeti i u grafičkom formatu kao što je prikazano na slici 4.



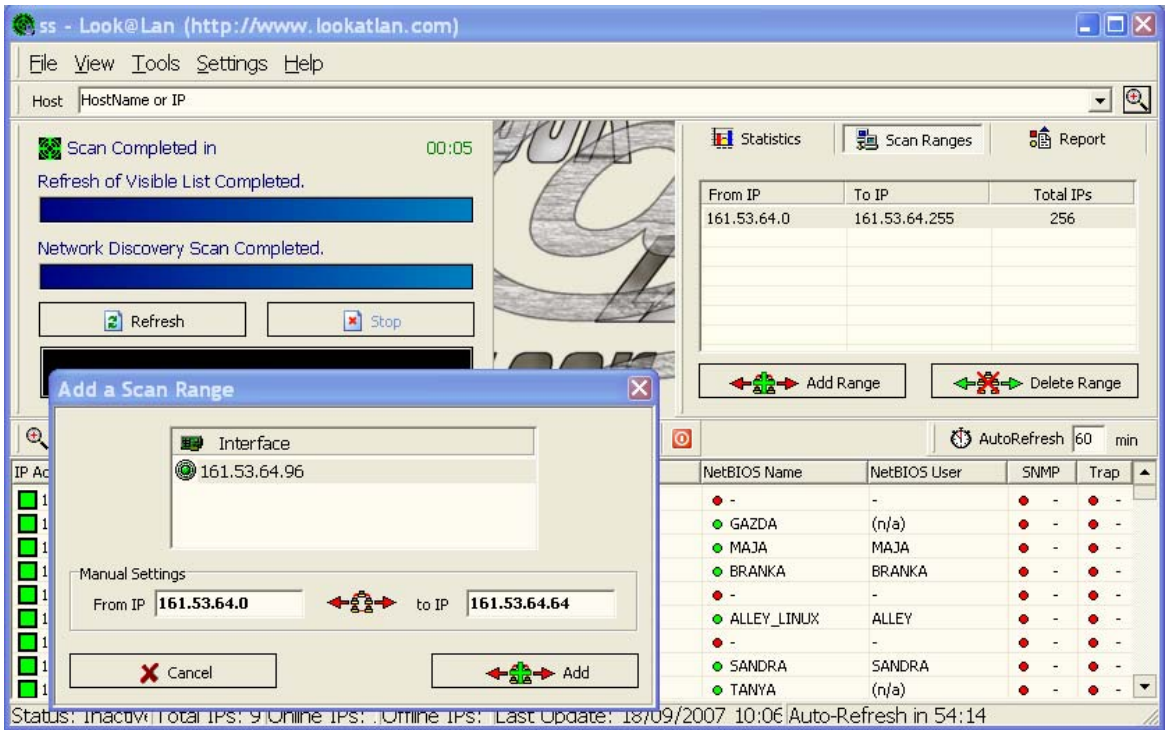
Slika 4. Grafički prikaz statistike analize mreže

Dobivene rezultate moguće je pohraniti u profil ili u neki od sljedećih formata pogodnih za pregled drugim aplikacijama:

- ANSI datoteka,
- CVS datoteka,
- jednostavna HTML datoteka,
- HTML datoteka s grafičkim prikazima,
- XML datoteka,
- Word datoteka, odnosno
- Excel datoteka.

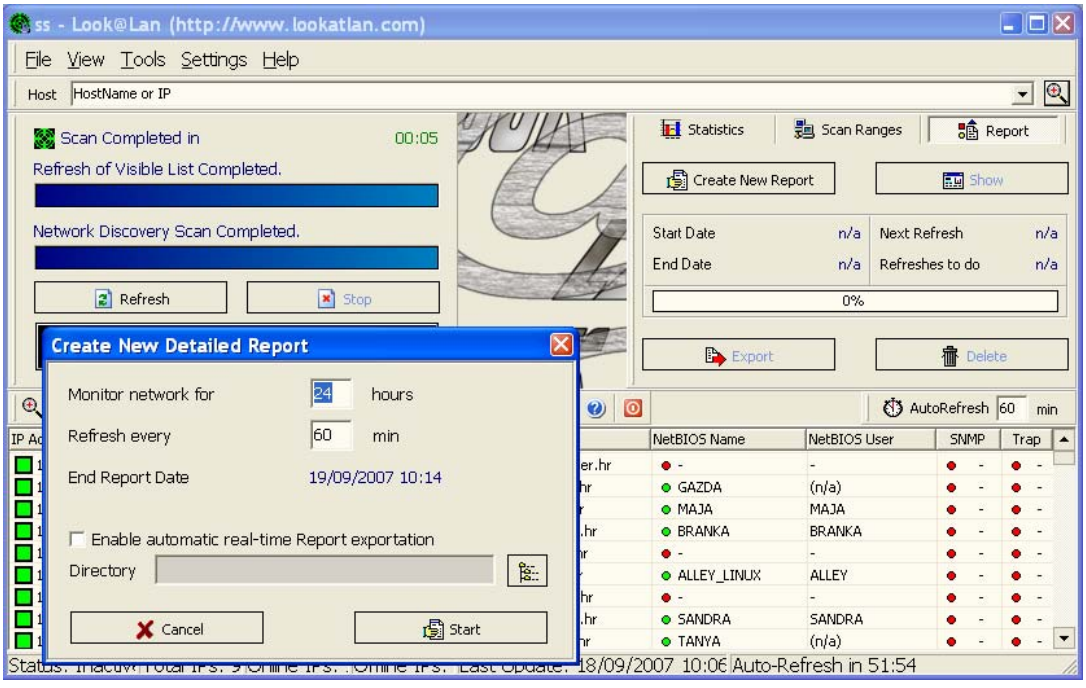
4.2. Analiza rezultata

Za detaljniju analizu programski paket Look@LAN korisniku daje mogućnost provedbe analize i pregleda rezultata prema njegovim specifičnim zahtjevima. Tako je moguće ograničiti analizu samo na dobivene rezultate za dio mreže. To se postiže odabirom opcije „*Scan Ranges*“ (slika 5) i zadavanjem ciljnog adresnog opsega. Kao rezultat se dobiva prikaz rezultata i statistika samo za računala unutar adresnog opsega.



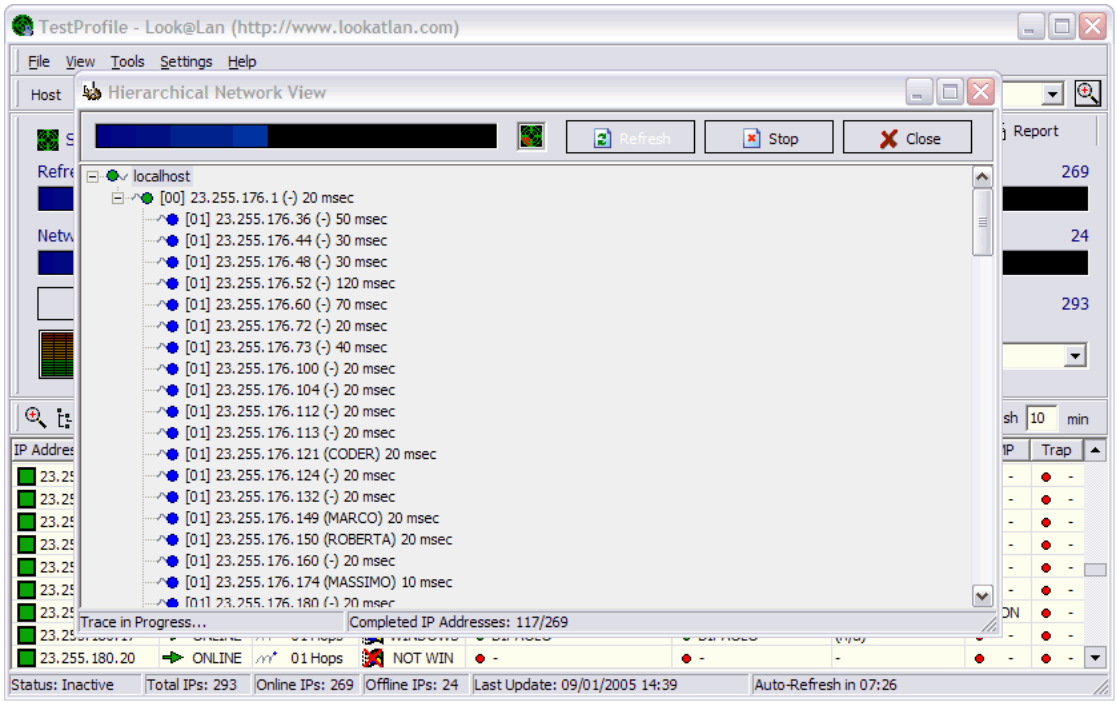
Slika 5. Ograničavanje područja analize mreže

Također je moguće obaviti i dugotrajnu analizu u svrhu promatranja aktivnosti unutar mreže u nekom vremenskom periodu. Takva analiza zadaje se odabirom opcije *„Report"*, gdje je moguće odabrati vremensko trajanje analize i specificirati mjesto pohranjivanja rezultata analize (slika 6). Nakon odabira program će periodički obavljati analize mreže i upisivati rezultate i sve promjene u zasebnu datoteku.



Slika 6. Specificiranje dugotrajne analize mreže

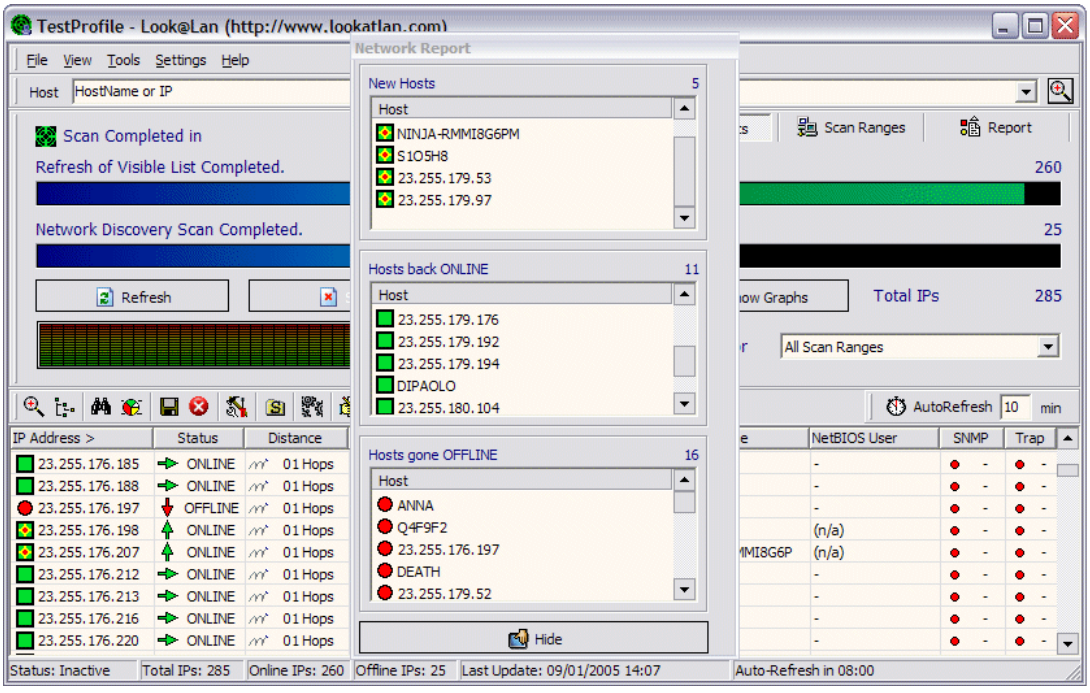
Isto tako, program omogućava i vizualizaciju rezultata prikazujući korisniku hijerarhiju analizirane mreže kao na slici 7.



Slika 7. Hijerarhijski prikaz analizirane mreže

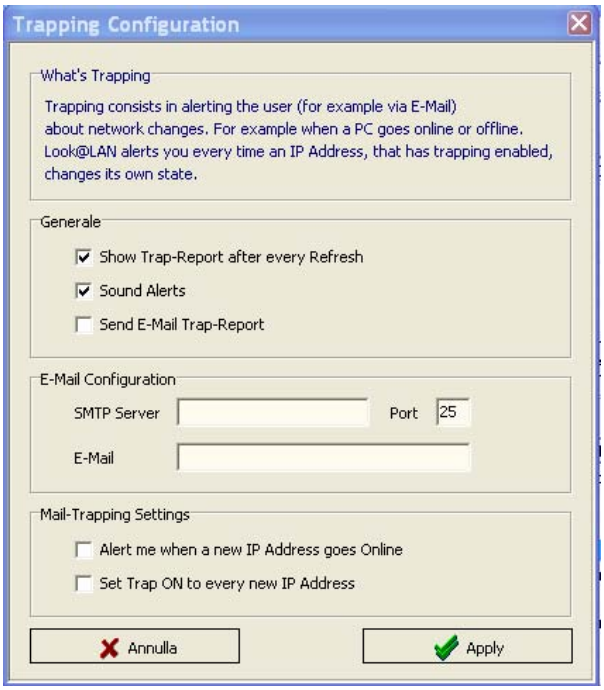
4.3. Periodička analiza

Programski paket Look@LAN obavlja automatske periodičke analize mreže dok god je aktivan te signalizira korisniku eventualne promjene u mreži u odnosu na prethodnu analizu (slika 8). Period automatske analize moguće je mijenjati u rasponu od 1 do 999 minuta.



Slika 8. Obavijest o promjenama u mreži između dvije analize

Vezano uz periodičku analizu mreže, Look@LAN programski paket daje mogućnost obavještavanja korisnika o otkrivenim promjenama putem poruka elektroničke pošte. Da bi se ova funkcionalnost aktivirala potrebno je u konfiguraciju programskog paketa, osim adrese primatelja, unijeti i podatke o SMTP poslužitelju s kojeg se mogu slati *e-mail* poruke (slika 9). Na taj način administrator mreže može ostaviti program aktivan kao proces u pozadini i dobivati obavijesti o svakoj promjeni.

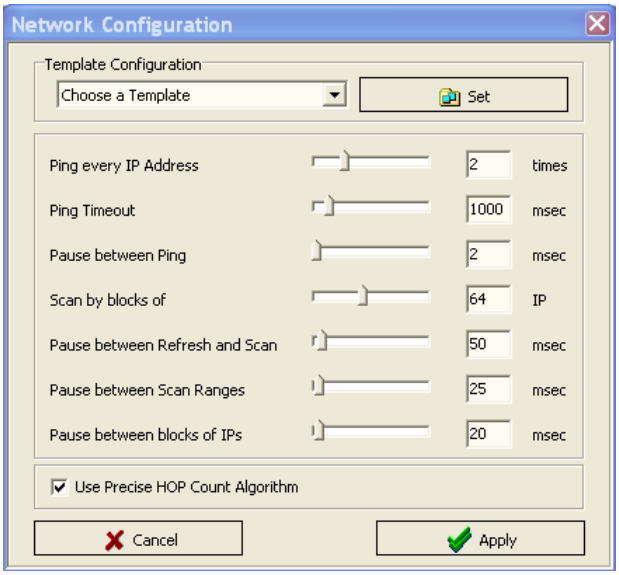


Slika 9. Konfiguracija e-mail izvješćivanja o promjenama u mreži

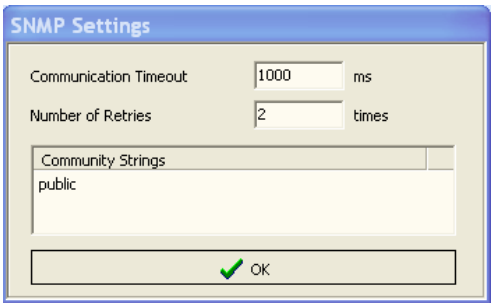
4.4. Postavke programskog paketa

Programski paket obavlja analizu mreže prema preddefiniranim standardnim postavkama, ali ostavlja naprednim korisnicima mogućnost izmjene tih postavki. Tako je unutar „Settings" izbornika moguće mijenjati:

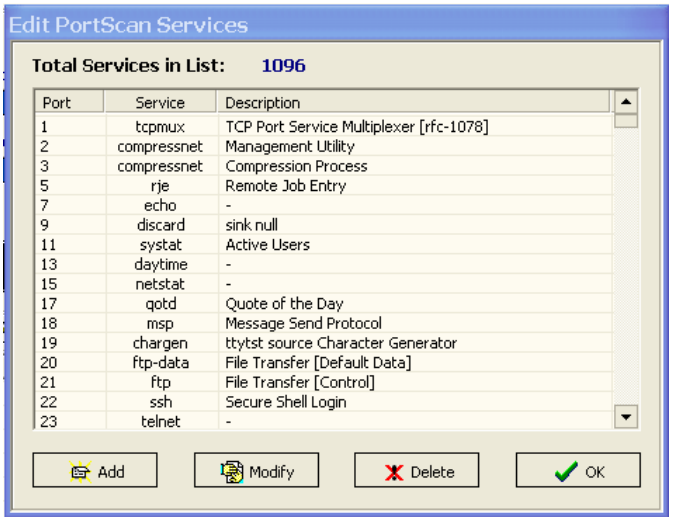
- postavke mrežnog ispitivanja (*ping* i *IP blocks* postavke) – slika 10,
- postavke SNMP ispitivanja – slika 11 i
- postavke veza usluga i priključaka – slika 12.



Slika 10. Postavke mrežnog ispitivanja



Slika 11. Postavke SNMP ispitivanja

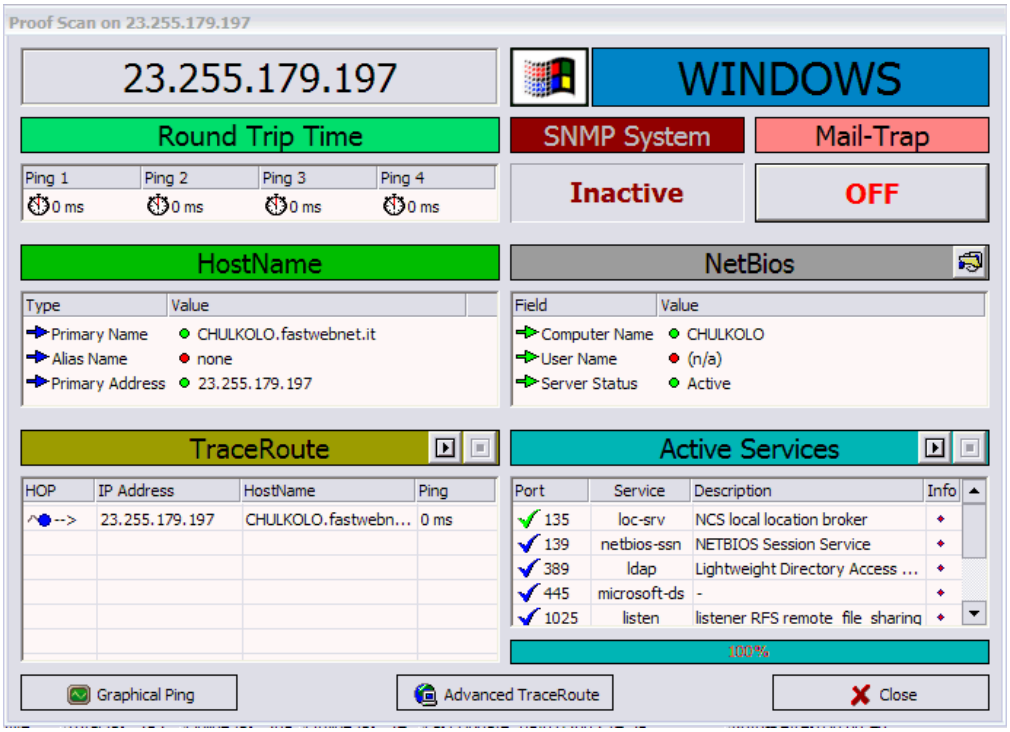


Slika 12. Postavke veza između usluga i priključaka

4.5. Look@Host - detaljna analiza računala

Unutar Look@LAN programskog paketa dostupna je i funkcionalnost Look@Host kojom se omogućava provedba detaljne analize pojedinog računala. Funkcionalnost je dostupna odabirom opcije *„Tools ->*

Quick Host Scan..." kojom se otvara prozor za unos IP adrese računala koje se želi analizirati. Nakon unosa adrese obavlja se analiza čiji rezultat izgledaju kao na slici 13.

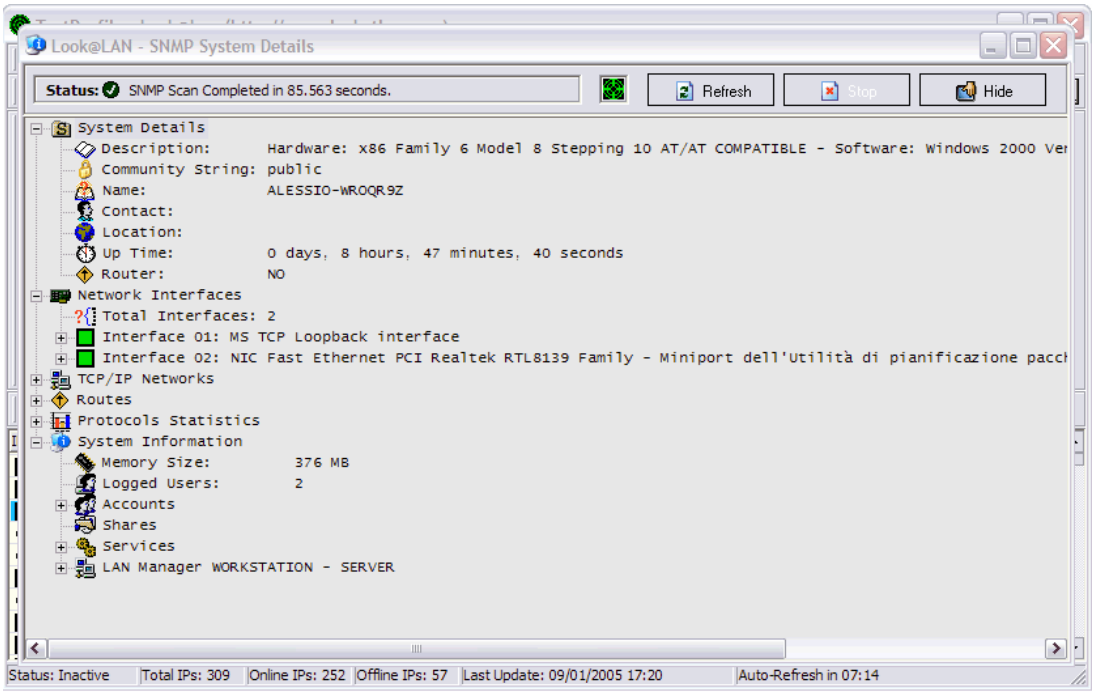


Slika 13. Prikaz rezultata analize računala

Kao što je vidljivo iz slike analizom se dobivaju detaljniji podaci o provedenim ispitivanjima koji uključuju:

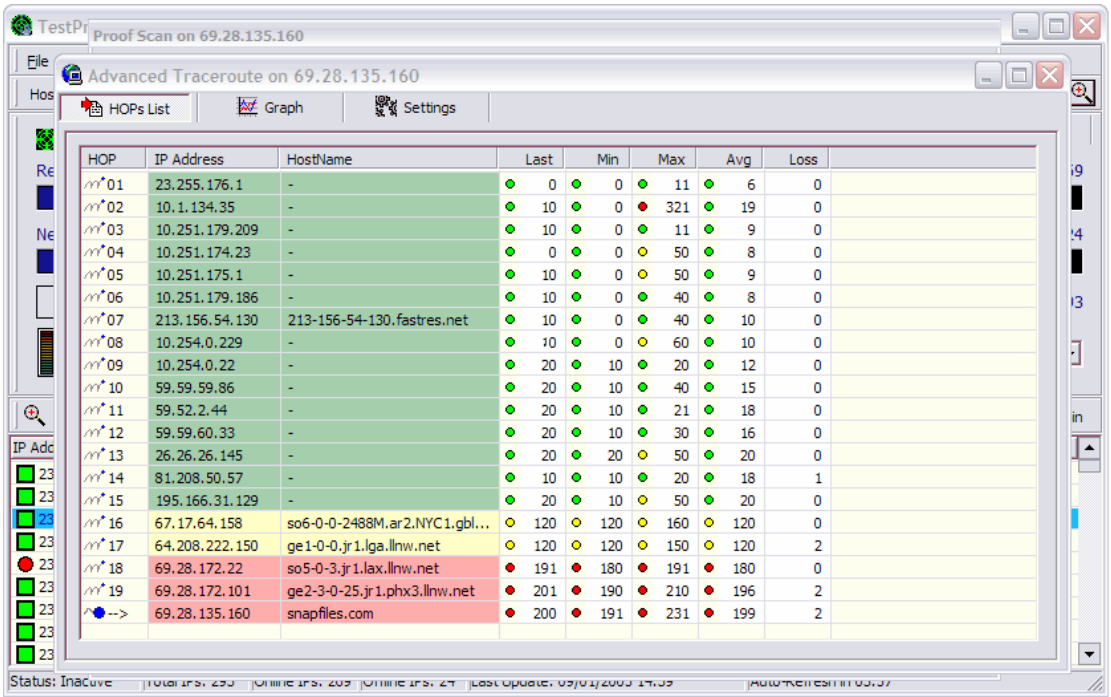
- statistiku *Ping* odziva,
- detalje NetBIOS podataka,
- podatke o putanji do ispitivanog računala i
- podatke o dostupnim uslugama na ispitivanom računalu.

Ukoliko ispitivano računalo podržava SNMP protokol onda se tijekom detaljne analize dobivaju i detaljni rezultati dobiveni SNMP komunikacijom kao na slici 14.



Slika 14. Rezultati detaljne analize računala koje podržava SNMP protokol

Detaljna se analiza računala može provesti i za računalo koje nije dio lokalne LAN mreže ukoliko se zna njegova IP adresa. Za takva računala mogu se dobiti korisne informacije odabirom opcije *„Advanced Traceroute"* koja prikazuje cjelokupan put do ispitivanog računala (slika 15).



Slika 15. Prikaz rezultata dobivenih odabirom "Advanced Traceroute" opcije

5. Zaključak

Look@LAN programski paket je jednostavan i intuitivan alat koji daje funkcionalnost koja se od njega očekuje. Prema podacima sa službene stranice paket ima više od 300 000 korisnika u svijetu što je samo po sebi dovoljna mjera kvalitete. Budući da se nakon analize Look@LAN alatom dobivaju gotovo svi uobičajeno potrebni podaci o mreži i računalima u mreži, programski paket nije doživio novije inačice od 2006. godine, unatoč najavama na službenoj stranici. Za zahtjevnije korisnike isti proizvođač nudi i Medas VNS programski paket kojim se mogu obaviti još detaljnije analize mreže i komponenti unutar mreže pa je time poprilično pokriven prostor analize LAN mreža i teško je očekivati neka drastična poboljšanja. Treba napomenuti da uz Look@LAN programski paket ne dolazi nikakva korisnička dokumentacija niti unutar samog paketa postoji pomoć za korištenje programa što unatoč oglašavanoj jednostavnosti i intuitivnosti programa ipak predstavlja ozbiljan nedostatak.

6. Reference

[1.] Službene stranice programskog paketa Look@LAN - http://www.lookatlan.com/ ,