UVOD U IZGRADNJU RAČUNALNE MREŽE ZA PRISTUP INTERNETU ZA MALE I SREDNJE UREDE NA SUSTAVU OTVORENOG KÔDA

Kukec M.[1]
[1]Veleučilište u Varaždinu, Varaždin, Hrvatska

Sažetak: *Ovaj rad ne iznosi nikakve tehnološke novosti niti rezultate istraživanja, već mu je nakana bez dubljeg ulaženja u tehnologiju dati pregled osnovnih mogućnosti i tehnologija koje se mogu primijeniti pri spajanju lokalnih računalnih mreža na Internet. Tekst daje osnovni pregled mogućnosti i objašnjenja zašto i kako se pojedine tehnologije koriste. Nakana rada je približiti tematiku bez previše stručnih pojmova kako bi se dala početna točka i objasnilo koje korake je potrebno poduzeti pri planiranju ovakvih rješenja. Korisniku Interneta ovaj rad može dati poneki odgovor na pitanje na koji način njegovo računalo komunicira s ostalima u mreži.*

Abstract: *This paper does not provide any technology innovations or research results, but intents, with no deeper analysis of the technology, to present basic options and technologies which can be applied in connection local computer networks to the Internet. It presents the basic options and explains why and how some technologies are being used. The purpose is to introduce the topic without too much professional terminology in order to get a starting point and to explain which steps should be taken in planning such solutions. To an Internet user this paper may provide an answer to the question of how his computer communicates with other network computers.*

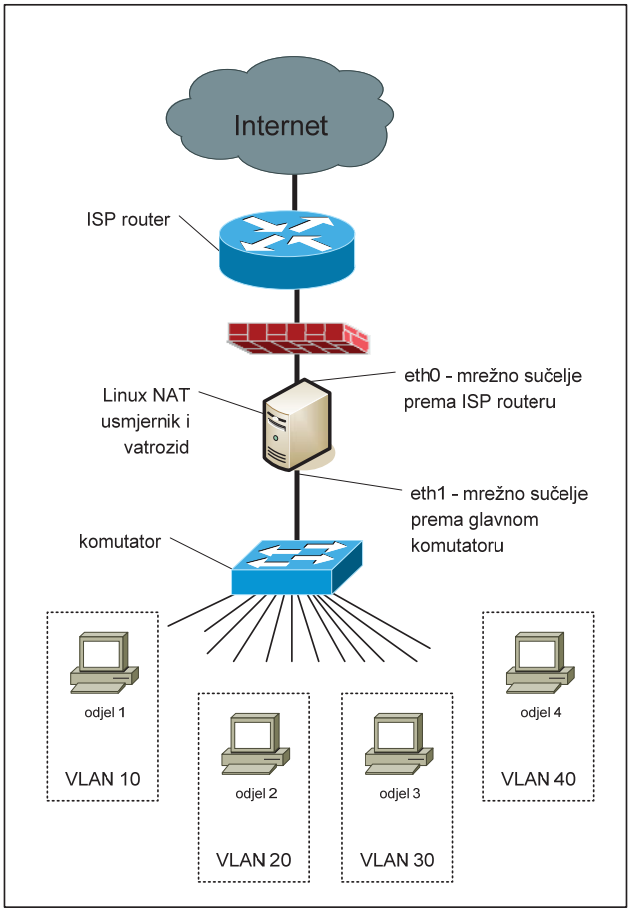
1. UVOD

Ovaj rad daje uvod u planiranje računalne mreže za male i srednje uvrede koja je izgrađena na otvorenim sustavima. Nakana rada je pokazati na koji način povezati i podesiti uređaje kako bi lokalna mreža većeg broja računala imala pristup Internetu uz uspostavljanje minimalne razine sigurnosti i kontrole. Na početku je potrebno dodatno objasniti naslov i namjeru ovog rada. Računalna mreža koja će ovdje biti razmatrana, izgrađena je na trenutno najrasprostranjenijim tehnologijama za izgradnju lokalnih računalnih mreža (LAN): TCP/IP protokolni stog s Ethernet protokolom u pristupnom sloju (engl. Network Access Layer). Sustav otvorenog kôda koji se spominje u naslovu, je bilo koji sustav izgrđen na Linux jezgri. Postoje i drugi operacijski sustavi otvorenog kôda koji mogu poslužiti istoj svrsi (npr. FreeBSD), no ovaj rad će se koncentrirati na Linux operacijski sustav. Doseg ovdje prikazanog rješenja je računalna mreža s do stotinu mrežnih priključaka kakvi se mogu nalaziti u malom ili uredu srednje veličine. Strukturno kabliranje izvedeno je kablovima kategorije 5 ili 6.

Rad je organiziran na sljedeći način. U drugom odjeljku daje se pregled infrastrukture koja mora postojati prije implementiranja ovakvih rješenja. Treći dio objašnjava na koji način su spojeni uređaji koji sudjeluju u prenošenju podataka između računala u lokalnoj mreži i onih izvan nje. Odabir i postavljanje Internet adresa objašnjava se u četvrtom dijelu ovog rada. Adresna translacija, mehanizam bez kojeg sve ovo ne bi bilo moguće, objašnjen je u petom poglavlju nakon kojeg slijedi zaključak.

2. STRUKTURNO KABLIRANJE

Prvi korak u izgradnji svake računalne mreže je strukturno kabliranje. Strukturno kabliranje je skup pravila i standarda koji određuju na koji način je potrebno izvesti postavljanje pasivne mrežne opreme koja uključuje kablove, utičnice u radnom prostoru na koje se spajaju računala, te prospojne točke u mrežnim ormarima na mjestu koncentracije svih mrežnih priključaka.



Sl. 1.Arhitektura mreže

Aktualni skup standarda za strukturno kabliranje telekomunikacijske opreme naziva se TIA/EIA-568-B. Navedeni skup standarda definira tipove kablova,

dopuštene udaljenosti, tj. dužine kablova, pravila za terminaciju kablova i tipove priključaka na kablovima. Osim pravila za planiranje i postavljanje pasivne mrežne opreme, standardi propisuju i minimalne zahtjeve koje kod postavljanja pasivna mrežna oprema mora zadovoljavati. Osnovna ograničenja se odnose na dopuštene dužine kablova, no standardi određuju i ograničenja koja se odnose na električne karakteristike postavljene instalacije. Kao primjer može se navesti jedan od parametara koji instalacija mora zadovoljavati. Standard propisuje tzv. "Insertion loss" koji je mjera gubitka signala, a koji nastaje u prijenosnom mediju između predajnika i prijemnika. Često se naziva "Atenuacija". Izražava se u dB relativno primljenoj razini signala. Mjeri se za sve parove kabla na 20 ± 3°C pri čemu je moguće uzeti korektivni faktor od 0.4%/°C na temperaturu od 20 °C.

Strukturno kabliranje je vrlo važan korak u izgradnji računalne mreže te mu je potrebno posvetiti posebnu pažnju prilikom implementacije. Polaganje mrežnih kablova, postavljanje ormara i priključnih mjesta u radnom prostoru često zahtijeva građevinske radove te je ovaj korak potrebno vrlo pažljivo planirati i kvalitetno implementirati. Eventualne greške i propusti koje se otkrivaju nakon implementacije tijekom ispitivanja instalacije i njezine usklađenosti sa standardima, mogu znatno produžiti rokove i podići cijenu izvedbe.

Ovaj rad neće se detaljnije baviti strukturnim kabliranjem. Smatra se da je strukturno kabliranje izvedeno te da je izvedena infrastruktura sukladna navedenim standardima. Kabliranje je izvedeno koristeći pasivnu mrežnu opremu kategorije 5e ili kategorije 6. Navedene kategorije kablova i općenito pasivne mrežne opreme omogućavaju korištenje 100BASE-TX Ethernet standarda i 1000BASE-T Ethernet standarda pri čemu je preporučljivo koristiti pasivnu mrežnu opremu kategorije 6. Brzine prijenosa podataka na mediju su 100 Mbit/s za 100BASE-TX i 1000 Mbit/s za 1000BASE-T.

3. ARHITEKTURA MREŽE

Slika 1 pokazuje arhitekturu mreže. Prikazane su osnovne komponente nužne za spajanje lokalne mreže računala na Internet.

ISP router na slici 1 je mrežni uređaj koji se nalazi u prostorijama korisnika a najbliže je davatelju usluga pristupa Internetu. Iako se nalazi u prostoru korisnika, često je taj uređaj u vlasništvu davatelja usluga i u njegovoj je nadležnosti, no to nije nužno pravilo i ovisi o samom davatelju usluga pristupa Internetu. Davatelj usluga taj uređaj podešava za korisnika te mu daje određeni broj javnih IP adresa na korištenje. Dodijeljeni broj IP adresa može se kretati od jedne do teoretski najviše 2^{24} što iznosi 16,777,216 IP adresa u slučaju kada je korisniku pridijeljena A klasa IP adresa što je u današnje vrijeme u praksi gotovo nemoguće. Razlog tome je iscrpljenost adresnog prostora. IP protokol verzije 4 (IPv4), predviđa IP adrese veličine 32 bita što ukupno daje 2^{32} mogućih IP adresa. Na prvi pogled se možda ova brojka čini velikom no potrebno je uzeti u obzir da svaki korisnik Interneta, svaki poslužitelj i općenito svaki uređaj koji se spaja na Internet mora imati jedinstvenu IP adresu. Iskoristivi broj IP adresa smanjuju mehanizmi i protokoli koji su nužni za njihovo korištenje. Upravo zbog tih razloga vrlo je vjerojatno da će korisnik imati na raspolaganju manji broj IP adresa u opsegu od 2^0 do 2^5 najviše. U ovom radu pretpostavljamo da korisnik ima jednu ili najviše osam javnih IP adresa za korištenje. Potrebno je napomenuti da od navedenih osam IP adresa ostaje zapravo samo pet na korištenje korisniku. Dvije su potrošene automatski kao adresa mreže i broadcast adresa za korisnikovu mrežu a treća je IP adresa koju koristi ISP usmjernik. Pitanje koje se postavlja ovdje je na koji način spojiti istovremeno 100 računala na Internet s samo 5 raspoloživih javnih IP adresa ako svako računalno mora imati jedinstvenu IP adresu? Odgovor na ovo pitanje iznesen je u narednim dijelovima.

Kako bi se riješio problem manjka IP adresa na ISP, na usmjernik s korisnikove strane može se spojiti još jedan usmjernik koji je u nadležnosti korisnika čija je zadaća da omogući računalima u lokalnoj mreži pristup Internetu i pored nedostatka IP adresa. Zadaću ovog, drugog, usmjernika može obavljati samo jedan usmjernik, npr. ISP usmjernik, no ovdje se razmatra slučaj kada to nije moguće ili iz nekog razloga nije poželjno. Jedan od mogućih slučajeva je uspostava demilitarizirane zone (DMZ) za poslužitelje. To je slučaj kada korisnik unutar svojeg adresnog prostora ima poslužitelje koji su direktno spojeni na ISP usmjernik. Poslužitelji se mogu postaviti i iza drugog usmjernika koji je podešen tako da se omogući pristup tim poslužiteljima s javnim IP adresama, no ovakva razmatranja prelaze okvire ovog rada.

Za drugi usmjernik, na slici 1 označen kao "Linux NAT usmjernik", koji se spaja na ISP usmjernik, može se iskoristiti PC računalo s dvije mrežne kartice. Ovakvo rješenje je financijski povoljnije od usmjernika, posebno ako se uzmu u obzir relativno male mogućnosti proširivanja nekih od hardverskih usmjernika i nadogradnje softvera. S PC računalom je situacija potpuno drugačija bez obzira razmatra li se hardverska ili softverska nadogradnja. Upravo u raznolikosti softvera za nadzor mreže koji se može instalirati na PC računalo, javlja se prednost ovog rješenja.

Prednosti korištenja PC računala kao usmjernika su ujedno i nedostatci navedenog rješenja. U širem kontekstu za računala možemo reći da je PC računalo stroj općenite namjene te kao takvo nije automatski pripremljeno za upravljanje mrežnim prometom za razliku od hardverskih usmjernika. Kako bi ga pripremili za upravljanje mrežnim prometom, na njega je potrebno instalirati operacijski sustav te dodatne alate koji to podržavaju. Primjer takvih operacijskih sustava su svi operacijski sustavi izgrađeni na Linux jezgri.

Posljednji mrežni uređaj na koji se spajaju računala je komutator. Komutator se s jedne strane spaja na Linux NAT usmjernik a s druge strane se na njega spajaju računala.

4. PODEŠAVANJE LINUX USMJERNIKA

Podešavanje Lunux usmjernika ključna je točka ovakvog postava mreže. Operacijski sustav instaliran na PC računalu koji će omogućiti njegovo pretvaranje u usmjernik kako je već navedeno, može biti bilo koji baziran na Linux jezgri. Uputno je pri tome koristiti poznatije distribucije, no nije nužno. Prednost poznatijih distribucija je u podršci, stabilnosti i lakoći korištenja što ih i čini poznatijima. Namjerno niti jedna distribucija

poimence nije nabrojena jer je nezahvalno odrediti preciznu granicu između poznatijih i manje poznatih distribucija dok će i gotovo sve manje poznatije distribucije poslužiti u ovom primjeru. Ovdje se neće razmatrati procedura instalacije operacijskog sustava. Smatra se da je na PC računalo instalirana neka od distribucija Linux baziranog operacijskog sustava.

Linux usmjernik je komponenta u mreži koji će preuzimati promet s ISP usmjernika te ga dostavljati računalima u mreži iza njega i obrnuto. Kako bi to mogao, potrebna su mu dva mrežna sučelja, tj. dvije mrežne kartice. Slika 1 pokazuje Linux usmjernik s dva mrežna sučelja pod nazivima eth0 i eth1. Prvo mrežno sučelje, eth0, spaja se na ISP usmjernik te se na njemu podešava javna IP adresa koju korisniku pridjeljuje davatelj usluga pristupa Internetu. Ova javna IP adresa Linux usmjerniku može se pridijeliti na dva načina: statički i dinamički. Statičko dodjeljivanje znači da korisnik sam podešava dodijeljenu mu IP adresu na Linux usmjernik te da ta adresa ostaje stalno pridijeljena mrežnom sučelju eth0. Dinamičko pridjeljivanje IP adrese obavlja se koristeći protokol za automatsku dodjelu mrežnih parametara (engl. Dynamic Host Configuration Protocol – DHCP).

Parametre automatski pridjeljuje davatelj usluga kroz DHCP poslužitelj. Karakteristika dinamičkog pridjeljivanja mrežnih parametara i IP adrese je njezina promjenjivost s vremenom. Dinamičko pridjeljivanje parametara davatelji usluga koriste kod ADSL tehnologije pristupa dok je statičko pridjeljivanje parametara češći slučaj pri zakupu stalne linije za prijenos podataka. U prvom slučaju korisnik će imati na raspolaganju samo jednu javnu IP adresu dok će u drugom slučaju imati na raspolaganju nekoliko ili više IP adresa. Davatelji usluga često podešavaju svoje DHCP poslužitelje da IP adrese dodjeljuju na određeni vremenski period nakon kojeg korisnik automatski dobiva neku drugu IP adresu. Razlog tome je pokušaj onemogućavanja korisnika u korištenju IP adrese u svrhe postavljanja poslužitelja za WEB, mail ili u neke druge svrhe. Ovaj primjer se ograničava na korištenje jedne, statički dodijeljene IP adrese.

Sl. 2. Podešavanje IP adresa na Linux usmjerniku

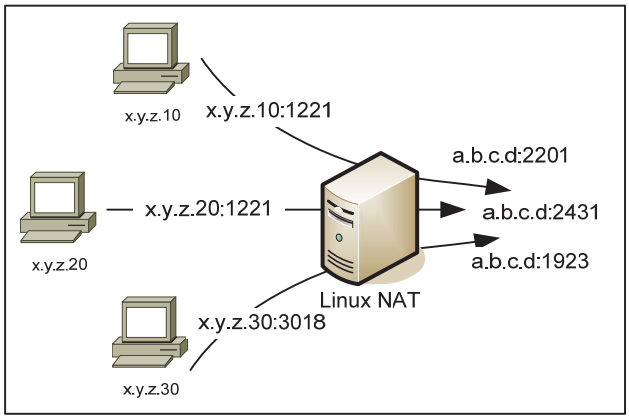
Slika 2 pokazuje postavljanje IP adresa na mrežna sučelja Linux usmjernika. Na eth0 mrežno sučelje postavljena je javna IP adresa 193.198.63.55[1] a na eth1 mrežno sučelje postavljena je IP adresa 192.168.0.1. Za razliku od IP adrese eth0 mrežnog sučelja koju dodjeljuje davatelj usluga, IP adresa koja se postavlja na eth1 mrežno sučelje Linux usmjernika, može se odabrati proizvoljno iz skupa privatnih IP adresa. Slika 3 pokazuje opseg IP adrese iz skupa privatnih IP adresa. [referenca prema RFC 1918] One se razlikuju od javnih IP adresa po tome što se one smiju koristiti samo unutar organizacije za njezine unutarnje potrebe. Organizacija ih može koristiti bez registriranja kako to njoj najbolje odgovara što nije slučaj s javnim IP adresama.

Privatne IP adrese su jedan od mehanizama koji smanjuje potrebu za velikim količinama javnih IP adresa. Kako je njihova namjena korištenje isključivo unutar organizacije ili unutar mreža nekoliko organizacija, svaka organizacija ih može koristiti. IP adrese neće biti jedinstvene, iste IP adrese će koristiti veliki broj organizacija, no ne postoji mogućnost zabune jer se te IP adrese koriste samo unutar organizacije.

```
10.0.0.0 - 10.255.255.255  (10/8)
172.16.0.0 - 172.31.255.255  (172.16/12)
192.168.0.0 - 192.168.255.255 (192.168/16)
```

Sl. 3. Privatne IP adrese prema RFC 1918

Privatnim IP adresama rješava se problem nedostatka javnih IP adresa. Organizacija, mali ili srednji ured iz ovog primjera, dobiva od svojeg davatelja usluga jednu ili mali broj javnih IP adresa. Broj računala kojima treba omogućiti pristup Internetu često je puno veći od broja dobivenih adresa te se na ta računala postavljaju adrese iz privatnog opsega. Njihova karakteristika je da se smiju koristiti samo unutar lokalne mreže organizacije što znači da se ne mogu koristiti kako bi se računala iz lokalne mreže povezala direktno na Internet. Mehanizam koji omogućava ovu vezu, naziva se NAT – Network address translation. Naredni odjeljak objašnjava kako NAT radi i kako ga podesiti.



Sl. 4. Adresna translacija

5. ADRESNA TRANSLACIJA

Adresna translacija (NAT) pojednostavljeno se može objasniti kao multipleksor koji omogućava mrežnom prometu s proizvoljnog broja IP adresa da izvana izgleda kao da dolazi samo s jedne javne IP adrese. Upravo je to učinak koji je potrebno u ovom primjeru postići. Slika 4 pokazuje kako radi jedna od vrsta adresne translacije koja se naziva PAT (Port Address Translation). Da bi se moglo

[1] IP adresa 193.198.63.55 samo je primjer i nalazi se u opsegu IP adresa Veleučilišta u Varaždinu te se ne može koristiti bilo gdje drugdje.

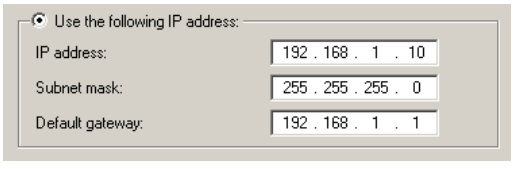
objasniti kako navedena metoda radi a bez dubljeg razmatranja TCP protokola, potrebno je reći da mrežni promet od točke A do točke B pronalazi put, tj. odredište pomoću IP adrese a kada stigne na odredište pomoću parametra koji određuje broj vrata (engl. port), dodjeljuje se određenoj vezi i pripadajućoj aplikaciji. Tako vrata 80 označavaju HTTP poslužitelja, vrata 53 DNS itd.

Na slici 4 prikazana su tri računala u lokalnoj mreži s IP adresama redom x.y.z.10, x.y.z.20 i x.y.z.30 kako pokušavaju pristupiti mrežnom sredstvu. Njihov mrežni promet prolazi kroz Linux usmjernik na kojem je aktivan PAT. U trenutku prosljeđivanja mrežnog prometa na vanjsko sučelje eth1, PAT će promijeniti izvorišne x.y.z adrese u vanjsku IP adresu a.b.c.d. Osim toga, kako bi se moglo odrediti koji mrežni promet je stigao s kojeg od x.y.z računala, PAT će promijeniti i izvorišna vrata s kojih je stigao promet te će sve te promjene zapisati u svoju tablicu. Kada stigne odgovor na zahtjeve računala iz lokalne mreže, odgovor će stići na IP adresu a.b.c.d Linux usmjernika. Pomoću prije stvorene tablice usmjernik će znati primljene podatke dostaviti računalima u lokalnoj mreži. Upravo zbog korištenja različitih vrata na jednoj IP adresi ova se vrsta NATa naziva Port Address Translation.

```
iptables -t nat -A POSTROUTING –s \
192.168.1.0/24 -o eth0 -j SNAT --to \
193.198.63.55
```

Sl. 5. Podešavanje PATa

Naredba sa slike 5 dovoljna je kako bi se uključila PAT funkcionalnost usmjernika. Vidljivo je da navedena naredba kombinira sve već rečeno. U prvom dijelu naredbe nakon prekidača "-s" navodi se skupina IP adrese za koje se omogućava adresna translacija. U ovom primjeru je adresna translacija omogućena za IP adrese iz lokalne mreže u opsegu od 192.168.1.1-192.168.1.254. Nakon označavanja adresa za koje se uključuje adresna translacija nakon opcije "-o", navodi se ime izlaznog mrežnog sučelja te nakon opcije "--to" javna IP adresa preko koje će mrežni promet prolaziti.



Sl. 6. Podešavanje računala u lokalnoj mreži

Pokretanjem naredbe sa slike 5 omogućava se adresna translacija na usmjerniku. Kako bi računala iz lokalne mreže mogla pristupiti Internetu koristeći Linux usmjernik, potrebno im je mrežne parametre podesiti kako je prikazano na slici 6., IP adresa usmjernika (Default gateway) koji će računalo koristiti, je IP adresa eth1 mrežnog sučelja Linux usmjernika. IP adresa računala se postavlja u opsegu 192.168.1.2-192.168.1.254 pazeći pri tome da svako računalo u lokalnoj mreži ima različitu IP adresu. Navedene parametre potrebno je upisati u svako računalo. U slučaju kada se radi o većem broju računala u lokalnoj mreži, uputno je na Linux usmjernik instalirati DHCP poslužitelja koji će mrežne parametre automatski proslijediti računalima.

6. ZAKLJUČAK

Rad sažeto i bez dubokog ulaženja u tehnologiju opisuje neke od metoda i postupaka koji se mogu primijeniti kako bi se računalima u manjem ili srednjem uredu omogućilo pristupanje Internetu. Iznesena rješenja izgrađena su na korištenju ograničenih sredstva što se očituje u vrlo malom broju dostupnih javnih IP adresa te korištenju PC računala kao zamjene za hardverski usmjernik.

Kako i naslov rada govori, prikazano rješenje samo je uvod u navedenu tematiku. Kroz nekoliko odjeljaka ovog rada prikazano je na koji način zaobići zapreke pri rješavanju ovog problema. Teme koje nisu dotaknute su zaštita računalne mreže od mogućih napada, uspostava vatrozida. Vrlo je važno razmotriti mehanizme koji će omogućiti da pojedino računalo ili skupina unutar lokalne računalne mreže ne onemogući druge u pristupu Interentu koristeći velik postotak propusnosti. Navedeni mehanizmi su vrlo važni za kvalitetno funkcioniranje lokalne mreže te ih je potrebno razmotriti u narednom radu.

7. LITERATURA

[1] Tanenbaum, A.S., "Computer Networks, 4th Edition", Prentice Hall, Upper Saddle River, New Jersey, March, 2003.

[2] Rodriguez, A., Gatrell, J., Karas, J., Peschke, R., "TCP/IP Tutorial and Technical Overview", IBM Corporation, International Technical Support Organization, New York, August 2001

[3] L. Gheorghe, *Designing and Implementing Linux Firewalls and QoS Using Netfilter, Iproute2, NAT and 17-filter*, Packt Publishing Limited, Birmingham, 2006.

Kontakt:
M. Kukec
Veleučilište u Varaždinu
Križanićeva bb, 42000 Varaždin
Telefon: 042-493 394
E-mail: mkukec@velv.hr