Unverza v Ljubljani
Fakulteta za računalništvo in informatiko

Damjan Maček

Nadzor dostopa v brezžičnih ISP omrežjih

diplomsko delo

visokošolski strokovni študijski program prve stopnje računalništvo in informatika

Mentor: dr. Andrej Brodnik

Ljubljana, 2013

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tržaška 25
1001 Ljubljana, Slovenija
telefon: 01 476 84 11
01 476 83 87
faks: 01 426 46 47
01 476 87 11
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 00335/2012
Datum: 04.09.2012

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **DAMJAN MAČEK**

Naslov: **NADZOR DOSTOPA V BREZŽIČNIH ISP OMREŽJIH**
ACCESS CONTROL IN WIRELESS ISP NETWORKS

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija prve stopnje

Tematika naloge:

V skladu z obstoječo zakonodajo Republike Slovenije, mora ponudnik internetnih storitev (ISP) zagotavljati organom pregona določene aktivnosti. Najbolj pogosto omenjana je možnost prisluha prometu določene stranke. Redkeje omenjana je zahteva po identifikaciji kdo je izvor oziroma ponor določenega prometa. Za zagotovitev obeh aktivnosti mora ISP natančno vedeti, kateri stranki je dodeljen nek IP naslov v določenem trenutku.
Poleg opisanega problema morajo ISP zagotoviti še različne funkcionalnosti za svoje naročnike. Slednje vključujejo varovanje dostopa, nudenje dovolj velikega IP naslovnega prostora in podobno.
V svoji diplomski raziskavi opišite in (so)implementirajte primer arhitekture, ki jo uporabljajo ISP dandanes. Pri tem se osredotočite na opis arhitekture in na potrebno programje, ki omogoča konfiguracijo omrežnih enot v takšnem omrežju

Mentor:

doc. dr. Andrej Brodnik

Fakulteta za računalništvo in informatiko
UNIVERZA V LJUBLJANI
2

Dekan:

prof. dr. Nikolaj Zimic

Izjava o avtorstvu diplomskega dela

Spodaj podpisani Damjan Maček, z vpisno številko **63070197**, sem avtor diplomskega dela z naslovom: *Nadzor dostopa v brezžičnih ISP omrežjih.*

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom dr. Andreja Brodnik,
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela
- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki »Dela FRI«.

V Ljubljani, dne 4. marca 2013 Podpis avtorja:

Zahvaljujem se mentorju dr. Andreju Brodnik za vse nasvete in pomoč pri izdelavi diplomske naloge.

Kazalo

Kazalo slik

Kazalo tabel

Povzetek

V diplomskem delu je opisano, kako v majhnem ISP-ju (ponudniku internetnih storitev) spremenimo infrastrukturo internetnega omrežja. To smo storili zaradi zahtev zakona o elektronskih komunikacijah v ISP-ju, ki je bil sprejet leta 2007. Da smo si postopek olajšali in pohitrili smo naredili program, ki spreminja odjemalčeve sprejemne naprave. Program je napisan v Microsoft Visual Studiu 2010 v jeziku C#. Njegova prednost je, da nam ni potrebno ročno spreminjati nastavitev vsake odjemalčeve sprejemne naprave. V program vnesemo IP naslove sprejemnih naprav ter željene nove nastavitve, ta pa nato dostopa do vsake naprave posebej preko IP naslova ter spremeni nastavitve. Ker je program narejen izključno za odjemalčeve naprave je potrebno ostalim usmerjevalnikom v omrežju nastavitve spremeniti ročno.

Na samem začetku smo spremenili nastavitve glavnega usmerjevalnika, ki je v omrežje priklučen preko optičnega voda. Za njim smo spremenili usmerjevalnike na oddajnikih. Sledilo je spreminjanje odjemalčevih naprav z uporabo programa, ki smo ga napisali. Istočasno so se spreminjale nastavitve uporabnikov, ki so povezani na isto oddajno napravo na oddajniku. Za tem smo spremenili še oddajno napravo. To smo ponavljali toliko časa, dokler nismo spremenili vseh oddajnikov.

Ugotovili smo, da omrežje po spremembi deluje hitreje, izboljšala se je tudi varnost v omrežju. Povezave med sprejemnimi ter oddajnimi napravami smo zaščitili z WPA2 zaščito. Do naprav v omrežju pa sedaj dostopamo preko HTTPS povezav. Zgradba omrežja je bolj enostavna, kar močno vpliva na

manjše število napak pri novih priklopih v sistem.

Ključne besede:

ISP, javni IP naslovi, sprememba omrežja v ISP, delovanje omrežja

Abstract

This thesis describes how the internet network infrastructure in a small ISP (internet service provider) can be changed to fulfill the requirements of the Electronic Communications Act which was adopted in 2007 by the Slovenian parliament. To simplify the process, we created a programme that changes client's reception device. The programme is written in C# language. Its advantage is that we do not need to manually change the settings of each client's reception device. Instead, we type into the programme the IP addresses of reception devices, along with desired preferences. The programme then accesses each device via the IP address and changes the settings. Since it was created for client's recipient devices only, other network router's settings need to be adjusted manually. First, we changed the settings of the main router that is connected to the network with an optical line. Second, we changed the routers on transmitters. We proceeded by changing the client's reception devices using the programme that we wrote. The settings of users connected to the same transmitting device on the transmitter were being changed simultaneously. Last, we changed the transmition device. We repeated the process until all transmitters were changed. What we found out was that after the change the network speed and security improved. Connections between transmitting and receiving devices were secured using WPA2 protection. Network devices are now being accessed through HTTPS links. And the network infrastructure itself became simpler, which exhibits in a smaller number of errors.

Keywords:

ISP, public IP addresses, modification network in ISP, network performance

Poglavje 1

Uvod

V ISP-ju se ukvarjamo z omogočanjem dostopa do medmrežja ter IP telefonije preko brezžičnih povezav do razdalje dvajsetih kilometrov, kot prikazuje slika 1.1. Te povezave uporabljajo standard 802.11n, ki je prišel v veljavo leta 2009. Razvoj brezžičnega omrežja ima veliko prednost v višje ležečih razgibanih reliefnih področjih saj nimamo nobenih stroškov z izkopavanjem in polaganjem kablov.

Slika 1.1: Primer brezžične povezave.

V podjetju je bilo potrebno prilagoditi infrastrukturo omrežja kakor zahteva »Zakon o elektronskih komunikacijah«. Zakon o elektronskih komunikacijah (uradno prečiščeno besedilo) (ZEKom-UPB1) [18].

Posebno je potrebno upoštevati 107. člen, ki govori o »zakonitem prestrezanju komunikacij«. Poleg tega člena je potrebno poskrbeti še za člena 107.a »splošne določbe o podatkih, ki se hranijo« ter 107.b »kategorije podatkov, ki se hranijo«. Člen 107. se glasi:

> *(1) Operater mora na svoje stroške zagotoviti ustrezno opremo v svojem omrežju in primerne vmesnike, ki v njegovem omrežju omogočajo zakonito prestrezanje komunikacij.*
>
> *(2) Operater je dolžan omogočiti zakonito prestrezanje komunikacij na določeni točki javnega komunikacijskega omrežja takoj, ko prejme prepis tistega dela izreka odredbe pristojnega organa, v katerem je navedba točke javnega komunikacijskega omrežja, na kateri naj se izvaja zakonito prestrezanje komunikacij, ter drugi podatki, povezani z načinom, obsegom in trajanjem tega ukrepa.*

(3) Prepis odredbe iz prejšnjega odstavka opravi organ, ki je odredbo izdal.

(4) Operater je dolžan omogočiti zakonito prestrezanje komunikacij na način, v obsegu in trajanju, kot je določeno v predpisu izreka odredbe.

(5) Operaterji morajo skupaj s pristojnimi organi, ki izvajajo nadzor komunikacij, zagotoviti neizbrisno registracijo zakonitega prestrezanja komunikacij. Pri tem morajo zbrane podatke hraniti trajno ter jih varovati v skladu z oznako stopnje tajnosti prepisa odredbe, vendar najmanj z oznako stopnje tajnosti »ZAUPNO« v skladu s predpisi o varovanju tajnih podatkov.

(6) Minister v soglasju z ministrom oziroma ministrico, pristojnim oziroma pristojno za notranje zadeve (v nadaljnjem besedilu: minister, pristojen za notranje zadeve), ministrom oziroma ministrico, pristojnim oziroma pristojno za obrambo (v nadaljnjem besedilu: minister, pristojen za obrambo), in direktorjem Slovensko obveščevalno-varnostne agencije predpiše funkcionalnost opreme in določi primerne vmesnike iz prvega odstavka tega člena.

Člen 107a:

(1) Operater mora za namene pridobivanja podatkov o prometu v elektronskem komunikacijskem omrežju, ki jih določa zakon, ki ureja kazenski postopek, za namene zagotavljanja nacionalne varnosti in ustavne ureditve ter varnostnih, političnih in gospodarskih interesov države, kot jih določa zakon, ki ureja Slovensko obveščevalno varnostno agencijo, in za namene obrambe države, kot jih določa zakon, ki ureja obrambo države, hraniti podatke iz 107.b člena.

(2) Obveznost iz prejšnjega odstavka vključuje tudi hranjenje podatkov o neuspešnih klicih, kjer jih operater ustvari ali obdela

ter hrani ali beleži pri zagotavljanju z njimi povezanih javnih komunikacijskih storitev, ne vključuje pa hrambe podatkov o povezavah, ki niso bile uspešno vzpostavljene, in vsebine komunikacij.

(3) Operaterji lahko hrambo podatkov iz 107.b člena.

(4) Operaterji zagotavljajo hrambo podatkov iz prvega, drugega in tretjega odstavka tega člena.

(5) Pristojni organ, ki odloča o dostopu do podatkov iz prvega odstavka tega člena.

(6) Operaterji morajo ob koncu obdobja hranjenja uničiti vse podatke, ki so jih hranili v skladu z določbami tega zakona, razen tistih, za katere je bila izdana odredba za dostop in so bili posredovanji pristojnemu organu.

Člen 107b:

(1) Podatki, ki se hranijo (v nadaljnjem besedilu: hranjeni podatki), so:
1. podatki, potrebni za odkritje in prepoznanje vira komunikacije, ki obsegajo:
– pri telefonskih storitvah v fiksnem in mobilnem omrežju telefonsko številko kličočega ter ime in naslov naročnika ali registriranega uporabnika;
– pri dostopu do interneta, elektronske pošte in uporabi internetne telefonije uporabniško ime in telefonsko številko, dodeljeno za vsako komunikacijo, s katero se vstopa v javno telefonsko omrežje, ime in naslov naročnika ali registriranega uporabnika, ki mu je bil v času komunikacije dodeljen naslov internetnega protokola, uporabniško ime ali telefonska številka;
2. podatki, potrebni za prepoznanje cilja komunikacije, ki obsegajo:
– pri telefonskih storitvah v fiksnem in mobilnem omrežju klicano telefonsko številko in v primerih, ki vključujejo dodatne storitve,

kot je preusmeritev ali predaja klica, številko ali številke, na katere je klic preusmerjen, ime in naslov naročnika ali registriranega uporabnika;
– pri dostopu do elektronske pošte in uporabi internetne telefonije uporabniško ime ali telefonsko številko prejemnika klica prek internetne telefonije, ime in naslov naročnika ali registriranega uporabnika in uporabniško ime namembnega prejemnika komunikacije;
3. podatki, potrebni za ugotovitev datuma, časa in trajanja komunikacije, ki obsegajo:
– pri telefonskih storitvah v fiksnem in mobilnem omrežju datum ter čas začetka in trajanje ali čas konca komunikacije;
– pri dostopu do interneta, elektronske pošte in uporabi internetne telefonije datum in čas prijave na internet in odjave z njega, pri čemer se upošteva določen časovni pas, skupaj z naslovom statičnega ali dinamičnega internetnega protokola, ki ga je ponudnik dostopa do interneta dodelil komunikaciji, in uporabniško ime naročnika ali registriranega uporabnika ter datum in čas prijave in odjave z internetnih storitev elektronske pošte ali internetne telefonije glede na določen časovni pas;
4. podatki, potrebni za ugotovitev vrste komunikacije, ki obsegajo:
– pri telefonskih storitvah v fiksnem in mobilnem omrežju vrsto uporabljene telefonske storitve;
– pri dostopu do elektronske pošte in uporabi internetne telefonije vrsto uporabljene storitve;
5. podatki, potrebni za razpoznavo komunikacijske opreme uporabnikov, ki obsegajo:
– pri telefonskih storitvah v fiksnem omrežju kličočo in klicano telefonsko številko;
– pri telefonskih storitvah v mobilnem omrežju kličočo in klicano telefonsko številko, mednarodno identiteto mobilnega naročnika

kličoče in klicane stranke, mednarodno identiteto mobilnega terminala kličoče in klicane stranke, v primeru predplačniških anonimnih storitev pa datum in čas začetka uporabe storitve ter ID celice, kjer je bila storitev izvedena;
– pri dostopu do interneta, elektronske pošte in uporabi internetne telefonije kličočo telefonsko številko za klicni dostop, digitalni naročniški vod ali drugo končno točko začetnika komunikacije, ID celice na začetku komunikacije, oziroma podatke, ki določajo zemljepisno lego med obdobjem, za katerega se hranijo podatki o komunikaciji.

Za prestrezanje komunikacij je potrebno poskrbeti, ker se lahko kdo od naročnikov ukvarja z nelegalno aktivnostjo. Te aktivnosti so lahko vdiranje v računalnike, spolne zlorabe, kraje denarja, osebnih podatkov, e-mail seznamov in podobno. Tako tisti, ki nadzirajo te aktivnosti, glede napadalčevega IP naslova locirajo kateremu internetnemu ponudniku pripada. Vsak od ISP ponudnikov pa mora vedeti, kateremu njegovemu odjemalcu ta IP naslov pripada. Lahko se zgodi, da je naročnik osumljenec kaznivega dejanja in oblasti zahtevajo od ISP-ja, nadzor nad njim. S tem lahko preko IP naslova spremljajo njegove spletne aktivnosti. Ker v podjetju do sedaj tega nimajo, je potrebno spremeniti celotno infrastrukturo omrežja obenem pa bomo povečali varnost v omrežju in pohitrili njegovo delovanje.

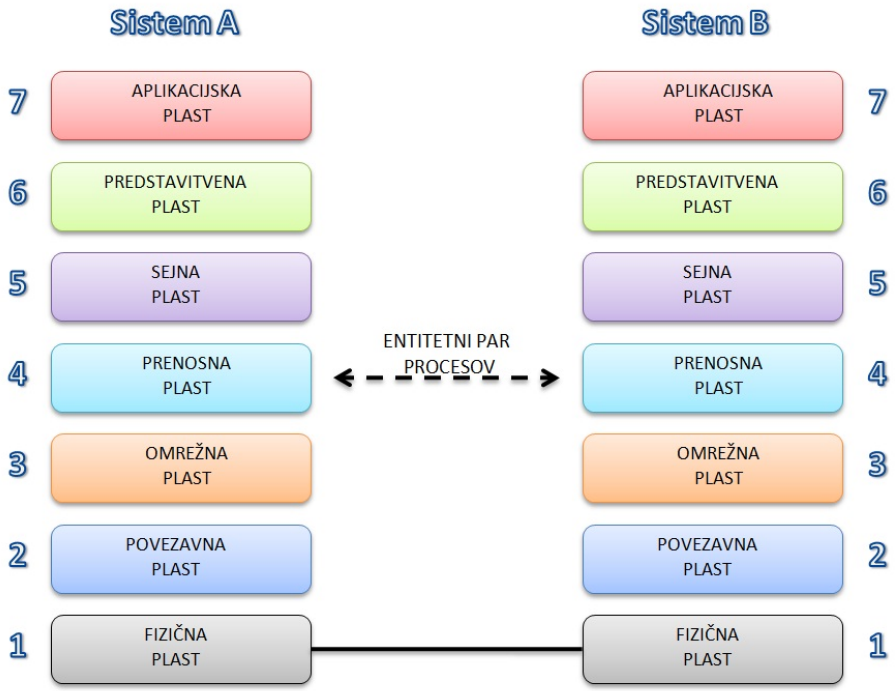
Poglavje 2

Osnovni pojmi računalniških omrežij

Za razumevanje diplomske naloge je potrebno poznati določene izraze o omrežju, ki so opisani v tem poglavju.

2.1 ISO/OSI model

Je 7 plastni referenčni model, ki predstavlja modularno zgradbo protokolov, kjer vsaka plast opravlja svojo nalogo, vsi skupaj pa delujejo kot celota. Vsaka plast nudi (streže) naslednji plasti ter vsaka plast zahteva storitve (odjema) od prejšnje plasti. Prednost večplastnega modela je, ko je potrebno model spremeniti saj se lahko spremeni katerakoli plast ne da bi s tem vplivali na ostale plasti, ki so med seboj neodvisne. Vsaka plast ima protokole, skupke pravil za delovanje omrežja oziroma jezik, s katerim se pogovarja istoležni entitetni par procesov [15]. To nam prikazuje slika 2.1.



Slika 2.1: Plasti v ISO/OSI modelu.

Aplikacijska plast

Je plast, ki je najbližja uporabniku, omogoča interakcijo aplikacije z omrežnimi storitvami. Njene standardne storitve so: telnet, FTP (*File Transfer Protocol*), SMTP (*Simple Mail Transfer Protocol*), SNMP (*Simple Network Management Protocol*), HTTP (*Hyper Text transfer Protocol*).

Predstavitvena plast

Je plast, ki določa pomen podatkov med entitetnima paroma aplikacijske plasti, določa kodiranje, kompresijo podatkov ter varnostne mehanizme. Prav tako pa skrbi za sintakso in semantiko.

Sejna plast

Je plast, ki nadzira dialog oziroma množice povezav med aplikacijama, skrbi za logično povezovanje med aplikacijami. Sejna plast je običajno vgrajena v aplikacije.

Transportna plast (enota: SEGMENT)

Skrbi za zanesljiv, učinkovit in transparenten prenos podatkov med uporabnikoma, te storitve zagotavlja višje ležečim plastem. Odgovorna je za kontrolo pretoka, kontrolo napak, segmentacijo in za povezavni oziroma nepovezavni način prenosa. Njene standardne storitve so: TCP (*Transmission Control Protocol*), UDP (*User Datagram Protocol*), GRE (*Generic Routing Encapsulation*).

Omrežna plast (enota: PAKET)

Skrbi za prenos paketov od izvornega do ciljnega računalnika in usmerjanje z uporabo usmerjevalnih algoritmov. Zagotavlja dostavo, fragmentacijo in izogibanje zamašitvam. Uporablja protokole IP (*Internet Protocol*), ICMP (*Internet Control Management Protocol*), IPSec (*IP Security*), IGMP (*Internet Group Management Protocol*), IPX (*Internetwork Packet Exchange*).

Povezavna plast (enota: OKVIR)

Skrbi za sinhrono oziroma asinhrono komunikacijo, fizično naslavljanje (MAC naslov), zaznavanje in odpravljanje napak (pariteta, CRC, chechsum), kontrolo pretoka, okvirjanje. Standardni protokoli so Ethernet, L2TP (*Layer 2 Tunnelling Protocol*), PPP (*Point to Point Protocol*) in Frame Relay.

Fizična plast

Je digitalni oziroma analogni medij, ki skrbi za prenos bitov po kanalu. Za prenos lahko uporablja UTP kabel, optični kabel, koaksialni kabel ali brezžična omrežja. Uporablja lahko serijski prenos RS-232, RJ45, T1, E1, 802.11b/g, USB.

2.2 Projekt 802

Spodnja dva sloja OSI referenčnega modela se nanašata na strojno opremo; omrežno kartico in omrežni medij. Nadalnje izpopolnjevanje zahtev za strojno opremo se določa znotraj teh slojev. Na IEEE (*Institute of Electrical and Electronics Engineers*) so razvili razširjene specifikacije namenjene posebej za različne omrežne kartice in medije. Ti standardi so poznani kot projekt

802 [13].

Model projekta 802

Ko so se lokalna omrežja začela pojavljati kot potencialna poslovna orodja v poznih sedemdesetih letih 20. stoletja, se je IEEE začel zavedati, da je potrebno določiti standarde za lokalna omrežja. Za dovršitev te naloge, je IEEE izdal Project 802, imenovan po letu in mesecu začetka (1980, februar).

Četudi so objavljeni standardi IEEE nastali malo pred standardi ISO (*International Organization for Standardization*), so bili vsi razviti skoraj hkrati. Oba modela posredujeta informacije, ki so imele za posledico nastanek dveh kompatibilnih modelov. Projekt 802 je določal omrežni standard za fizične komponente omrežja (omrežna kartica in mediji), ki se nanašajo na fizični sloj in sloj podatkovne povezave v referenčnemu modelu ISO/OSI.

Določbe 802 so postavile standard za:

- omrežne kartice (NIC angl. *network interface card*),
- komponente lokalnih omrežij,
- komponente za omrežja, ki uporabljajo sukane parice in koaksialne kable.

Standardi 802 določajo načine dostopa omrežnih kartic in prenos podatkov preko fizičnih medijev. Ti standardi vključujejo priključevanje, vzdrževanje in odklapljanje omrežnih naprav, ki jih prikazuje tabela 2.1.

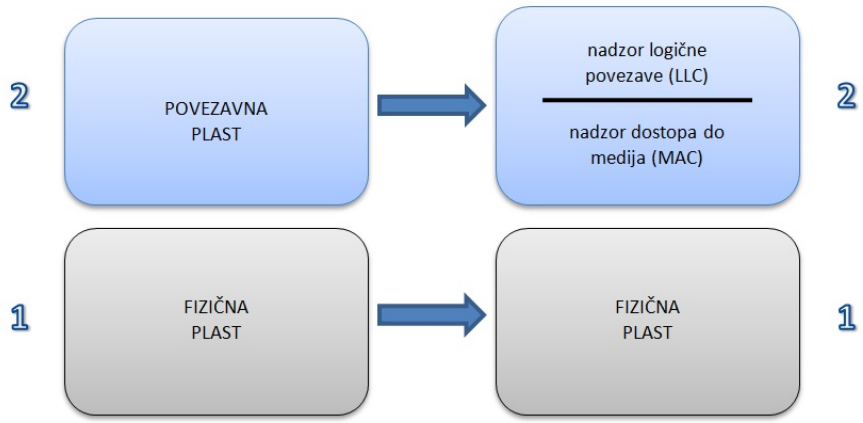
Oznaka	Opis
802.1	Standardi za medomreženje, ki so povezani z upravljanjem.
802.2	Splošna pravila za sloj podatkovne povezave IEEE. Sloj deli na dva podsloja in sicer na LLC (*link logical control*) in na MAC (*media access control*). Podsloj MAC je različen za različna omrežja in je določen z drugimi standardi.
802.3	Podsloj MAC za omrežno topologijo vodilo, ki uporablja CSMA/CD (*Carrier–Sense Multiple Access with Collision Detection*). To je praktično standard eternet.
802.4	Podsloj MAC za omrežno topologijo vodila z žetonom.
802.5	Podsloj MAC za obroč z žetonom.
802.6	Standardi za mestna omrežja (MAN angl. *Metropolitan Area Network*), kjer so podatkovna omrežja narejena za mesta. V geografski prostranosti je MAN večji od LAN (*Local Area Network*), je pa manjši od WAN (*Wide Area Network*). Za MAN je značilna uporaba optičnih kablov in prenos različnih digitalnih vsebin (podatki, video ...).
802.7	Uporabljeno pri tehnično svetovalni skupini za širokopasovno medomreževanje.
802.8	Uporabljeno pri tehnično svetovalni skupini za optične linije.
802.9	Govorno–podatkovna omrežja.
802.10	Pravila za omrežno varnost.
802.11	Standardi za brezžična omrežja.
802.12	Zahtevne prioritetne dostope za LAN, 100Base VG-AnyLAN.
802.13	Neuporabljeno, ker prinaša nesrečo.
802.14	Standardi za modeme.
802.15	Standard za WPAN (*Wireless Personal Area Network).*
802.16	Standardi za brezžična širokopasovna medomreževanja.

Tabela 2.1: Kategorije IEEE 802.

Razširitev referenčnega modela OSI

Spodnji plasti OSI, fizični sloj in sloj podatkovne povezave, določata, kako lahko več računalnikov hkrati uporablja omrežje brez vpliva na druge. Projekt IEEE 802 vsa pravila teh dveh slojev poveže tako, da izdela standarde za prevladujoča okolja lokalnih omrežij.

Projekt 802 je ugotovil, da sloj podatkovne povezave vsebuje več podrobnih razlag. Zato se je odločil, da se sloj podatkovne povezave razdeli v dva podsloja (slika 2.2), podsloj logične povezave (LLC, angl. *Logical Link Control*) in podsloj dostopa do medija (MAC, angl. *Media Access Control*).



Slika 2.2: Delitev povezavne plasti v IEEE 208.

Podsloj za nadzor logične povezave

Podsloj za nadzor logične povezave (LLC) upravlja podatkovno povezavo (vzpostavitev, vzdrževanje in prekinitev) in določa uporabo logičnih vmesnih točk, imenovanih SAP (*Service Access Points*). Ostali računalniki lahko prenesejo in uporabljajo SAP za prenos podatkov iz LLC v zgornji sloj OSI. Kategorija 802.2 določa te standarde. Nadzoruje prenos okvirjev, zaporedje okvirjev in njihove potrditve.

Podsloj za nadzor dostopa do medija

Podsloj za nadzor dostopa do medija (MAC) je nižji podsloj in zagotavlja skupen dostop do fizičnega sloja računalnikove omrežne kartice. Podsloj MAC komunicira neposredno z omrežno kartico in je odgovoren za dostavo podatkov brez napak med dvema računalnikoma v omrežju. Podsloj je zadolžen tudi za strojne naslove, določa in prepoznava naslove okvirjev.

2.3 Projekt 802.11

IEEE 802.11 je skupek standardov za implementacijo WLAN (*wireless local area network*) z brezžičnim oddajanjem v 2.4 GHz, 3.7 GHz in 5 GHz frekvenčnem pasu. Osnovna različica standarda 802.11 je bila kasneje še velikokrat spremenjena. Ti standardi so podlaga za brezžične izdelke omrežja z uporabo Wi-Fi blagovne znamke.

Protokol je bil izdan junija 1997, zametki pa so nastali že nekaj let prej. Podatki so se po zraku prenašali najprej z DSSS (*Direct-sequence spread spectrum*) in FHSS (*Frequency-hooping spread spectrum*) modulacijo, kasnejši protokoli pa z OFDM (*Orthogonal frequency-division multiplexing*) modulacijo. Prenos pa je bil izveden s *half-duplex* tehnologijo. To je tehnologija kjer sta dve napravi povezani s točka v točko protokolom (*Point to Point Protocol*) medtem ko ena naprava oddaja druga sprejema po določenem času pa se zamenjata. Začetna hitrost prenosa je bila največ 2 Mb/s. Brezžična omrežja so prišla v uporabo s protokoloma 802.11b in 802.11g, ki sta spremenjeni različici osnovnega protokola. Še višje hitosti so prišle s protokoloma 802.11n in 802.11ac s hitrostjo do nekaj 100 Mb/s [20]. Kako so se razvijali standardi lahko vidimo v tabeli 2.2.

802.11 standardi						
802.11 protokol	**izdaja**	**frekvenca (GHz)**	**pasovna širina (MHz)**	**hitrost (Mb/s)**	**MIMO tokovi**	**modulacija**
-	Jun 97	2.4	20	2	1	DSSS, FSSS
a	Sep 99	5, 3.7	20	54	1	OFDM
b	Sep 99	2.4	20	11	1	DSSS
g	Jun 03	2.4	20	54	1	OFDM, DSSS
n	Okt 09	2.4, 5	20	288,8	4	OFDM
			40	600		
ac	Nov 11	5	20	87.6	8	
			40	200		
			80	433.3		
			160	866.7		

Tabela 2.2: Standardi IEEE 802.11.

802.11a

Je standard, ki uporablja enako povezavno plast in enako obliko paketov kot osnovni standard, vendar uporablja OFDM modulacijo. Frekvenčni pas je 5 GHz, z maksimalnim prenosom podatkov do 54 Mb/s. V to pa je vključeno tudi popravljanje napak tako, da realna hitrost seže nekje do 25 Mb/s.

Njegova prednost je v tem, da deluje v 5 GHz frekvenčnem pasu namreč 2.4 GHz pas je zelo zaseden. Tako ne prihaja do motenj med signali, posredno s tem se zmanjša število ponovljenih paketov, posledično se zmanjša tudi njegovo območje delovanja. Predmeti, ki so na poti, absorbirajo krajše valove močneje kot daljše [11].

802.11b

Ta standard ima najvišjo hitrost 11 Mb/s in uporablja isto metodo dostopnega medija, kot je definirano v originalnem standardu. Zaradi velikega povečanja prenosa podatkov (v primerjavi z originalnim standardom) ter zaradi sprejemljive cene je bil ta standard sprejet kot dokončna tehnologija za brezžični LAN (WLAN). Naprave, ki uporabljajo 802.11b standard so lahko motene z ostalimi napravami, ki uporabljajo 2.4 Ghz frekvenčni pas. Te naprave so mikrovalovna pečica, brezžična povezava modri zob, brezžični telefoni in tako dalje.

802.11g

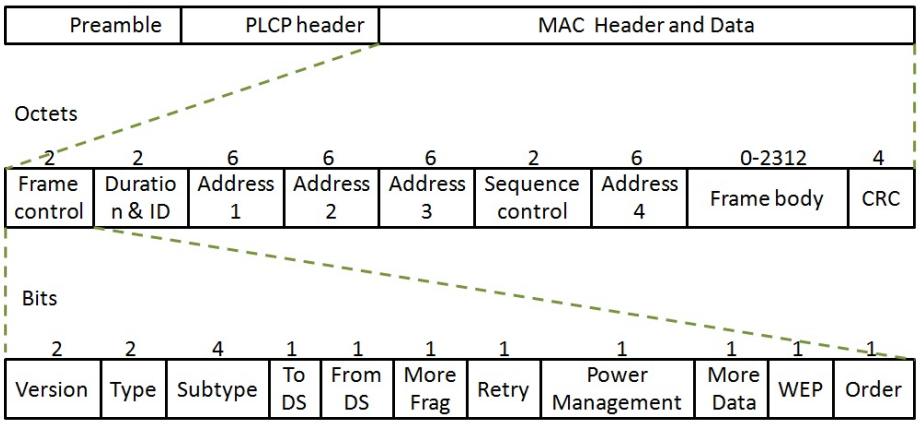
Deluje na 2.4 Ghz frekvenčnem pasu in uporablja OFDM ter DSSS modulacijo. Njegova največja hitrost prenosa podatkov seže do 54 Mb/s vključno z popravljanjem napak, povprečna realna hitrost pa je 22 Mb/s. Uporabljati se je začel zaradi potrebe po višjih hitrostih prenosa, 802.11b standard ga ima samo 11Mb/s. Njegova prednost je popolna združljivost strojne opreme s standardom 802.11b, na ta način so v primerjavi z 802.11a zmanjšali prepustnost podatkov tudi do 21 odstotkov. Njegova slabost je ista kot pri 802.11b standardu, motnje ostalih naprav v istem frekvenčnem pasu.

802.11n

Standard 802.11n je sprememba, ki izboljšuje vse dosedanje standarde z MIMO (*Multiple-Input Multiple-Output*) tehnologijo. To pomeni, da naenkrat pošilja in oddaja več anten hkrati. Deluje tako na 2.4 Ghz kot na 5 GHz frekvenčnem pasu, njegova hitrost podatkov seže do 600 Mb/s.

802.11ac

Je standard v razvoju, ki zagotavlja visoko prepustnost v 5 GHz frekvenčnem pasu. Uporablja MU-MIMO (*Multiple User MIMO*) tehnologijo.



Slika 2.3: Okvir 802.11.

Obstajajo tri glavne vrste 802.11 okvirjev, ti so podatkovni okvir (*data frame*), upravljalni okvir (*management frame*) in kontrolni okvir (*conrtol frame*) [3]. Osnovno sestavo okvirja prikazuje slika 2.3.

Version

Številka verzije protokola je vedno 0.

Type

Je dvobitno polje, ki opredeljuje ali je okvir podatkovni, upravljalni ali kontrolni. Če sta bita 00 je okvir upravljalni, če sta bita 01 je kontrolni, če sta 10 je podatkovni. Bita 11 sta rezervirana.

Subtype

Kontrolne, upravljalne in podatkovne pakete razdeli v podskupine.

To DS

Je polje, ki se nastavi, če se okvir pošlje v porazdeljeno omrežje (*distribution system*).

From DS

Je polje, ki se nastavi, če se okvir prejme iz porazdeljenega omrežja (*distribution system*).

More Frag

Se nastavi, ko je paket razdeljen v več okvirjev. Vsi okvirji razen zadnjega imajo ta bit nastavljen.

Retry

Včasih okvirji zahtevajo ponovno pošiljanje, zato obstaja »*retry*« bit, ki se nastavi na 1 kadar je to potrebno. S tem se izognemo podvojenim okvirjem.

Power Management

Kaže v katerem energijskem stanju je bila naprava, ko je poslala okvir. Stanja sta lahko »*save*« ali »*active*«.

WEP

Se nastavi, če je uporabljena WEP zaščita za šifriranje telesa (*body*) okvirja.

Order

Ta bit se nastavi le ko se uporablja »*strict ordering*« način dostave.

Sequence Control

Je razdeljen na »*Sequence Number*« (12 bitov) in »*Fragment Number*« (4 bite). Prvi označuje zaporedno številko posameznega okvirja. Zaporedna številka je enaka za vsak okvir poslan v razdrobljenem okvirju, z vsakim paketom se to število poveča za 1 dokler ne doseže 4095 potem se zopet prične pri 0. Druga je številka okvirja v razdrobljenem okvirju. Začetna vrednost je 0 z vsakim novim delcem pa se poveča za 1.

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	cilj	izvor	BSSID	ni na voljo
0	1	cilj	BSSID	izvor	ni na voljo
1	0	BSSID	izvor	cilj	ni na voljo
1	1	prejemnik	oddajnik	cilj	izvor

Tabela 2.3: Naslovi v 802.11 okvirju.

Address 1

Je vedno ciljni naslov če se ne pošilja v porazdeljeno omrežje. Če se pošilja v porazdeljeno omrežje je to naslov naprave, ki bo prejela ta okvir (tabela 2.3).

Address 2

Je vedno naslov oddajne naprave če se pošilja v porazdeljeno omrežje če se ne pa je to naslov prejemne naprave (tabela 2.3).

Address 3

Je v večini primerov manjkajoči naslov. Če je *From DS* nastavljen je to prvotni izvorni naslov. Če je nastavljen *To DS* je ta naslov ciljni naslov (tabela 2.3).

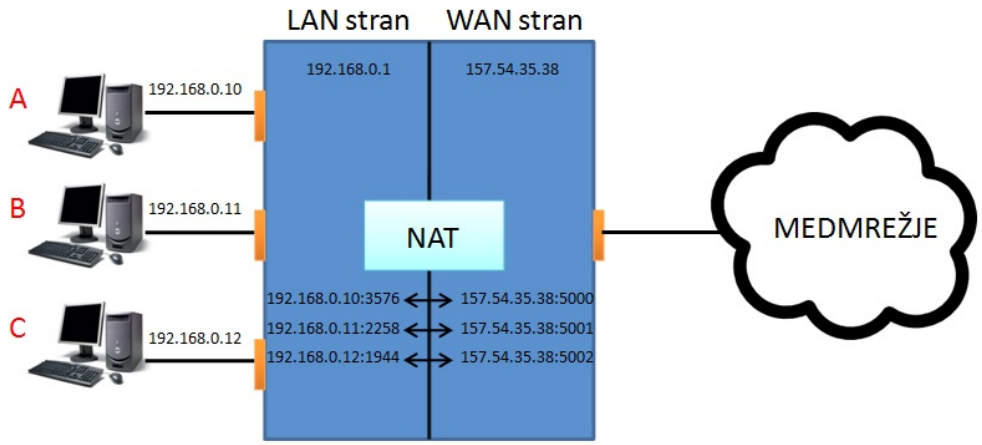
Address 4

Se uporabla v posebnih primerih ko je uporabljen WDS (*Wireles Distribution System*), ko je okvir poslan od ene dostopne točke k drugi. Oba *To Ds* in *From DS* sta nastavljena torej sta oba izvorni in ciljni naslov izgubljena (tabela 2.3) [4].

2.4 NAT

Pomemben izraz, ki ga bomo še velikokrat omenili je NAT (*network address translation*), ki pomeni spreminjanje IP naslovov in vrat.

Uporablja se predvsem zaradi dveh razlogov, na prvem mestu je varnost omrežja, ker NAT loči med javnim in privatnim omrežjem. Na LAN (*local area network*) strani naredi svoje podomrežje (slika 2.4), zato računalniki, ki so v privatnem omrežju, v zunanjem javnem omrežju (medmrežju) niso vidni. Tako so preprečeni vdori, hkrati pa je to slabost, saj računalniki niso javno dostopni [9, 2].



Slika 2.4: NAT ločevanje med privatnim in javnim omrežjem.

Drugi razlog je pomanjkanje javnih IP naslovov. Vsak IP naslov verzije štiri (IPv4) lahko zapišemo z dvaintridesetimi biti, vsak bit lahko vrednost nič ali ena. Iz tega sledi da lahko z IP naslovi verzije štiri zapišemo

$$2^{32} = 4.294.967.296$$

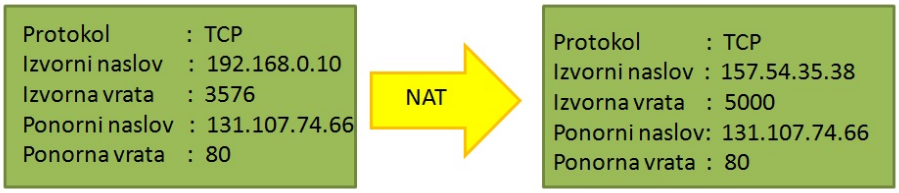
različnih naslovov.

Od teh naslovov jih je veliko gruč rezerviranih za posebno uporabo in nedostopnih za javno uporabo. Tako je recimo okoli 18 milijonov rezerviranih za privatna omrežja, 270 milijonov za razpošiljanje in še za ostale stvari.

Delovanje

Spreminjanje omrežnih naslovov bomo prikazali na primeru. Imamo tri računalnike, ki uporabljajo privatne IPv4 naslove v 192.168.0.0 omrežju z masko 255.255.255.0. Za delovanje uporabljamo usmerjevalnik, ki ima vključen NAT. Na WAN (*Wide Area Network*) strani usmerjevalnika imamo dva javna IP naslova, 157.54.35.38 in 157.54.35.39 [16, 5].

Uporabnik na računalniku A želi dostopati do spletne strani na medmrežju, računalnik A pošlje usmerjevalniku TCP paket. Aplikacija na računalniku (brskalnik) si sama določi izvorna vrata, v našem primeru 3576. Ko pride paket do usmerjevalnika mu spremeni izvorni IP naslov v enega od javnih IP naslovov in številko izvornih vrat, ki jo določi usmerjevalnik (slika 2.5). Spreminjaju izvornega IP naslova in vrat se imenuje NAPT (*Network Address and Port Translation*).



Slika 2.5: Preslikovanje paketa za računalnik A.

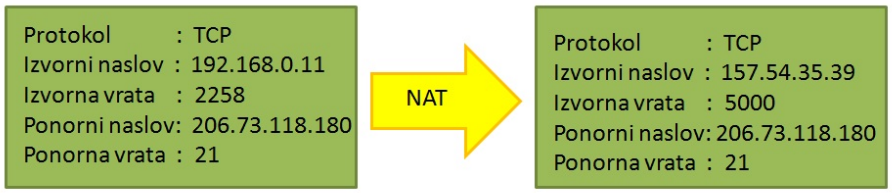
Ob spreminjanju paketa se spremenjene vrednosti shranijo na usmejevalnik v preslikovalno tabelo (slika 2.6). Ta tabela se ponovno uporabi ko usmerjevalnik prejme odgovor na poslani paket. Ta paket je naslovljen na javni IP usmerjevalnika v našem primeru 157.54.35.38 z vrati 5000. Usmerjevalnik pregleda če v preslikovalni tabeli ta vnos obstaja s tem pa tudi ve na kateri privatni IP naslov in vrata ga mora poslati. V primeru, da vnos v preslikovalni tabeli ne obstaja se paket zavrže.

NAT preslikovalna tabela
192.168.0.10 : 3576 ← TCP → 157.54.35.38 : 5000

Slika 2.6: Preslikovalna tabela za računalnik A z dinamičnim preslikovanjem naslova.

Uporabnik na računalniku B prične TCP (*Transmission Control Proto-*

col) sejo z gostovanjem v javnem omrežju. V tem primeru je brskalnik izbral številko vrat 2258. Prav tako kot pri računalniku A se rčunalniku B spremeni izvorni IP naslov v 157.54.35.39 in izvorna vrata v 5000 (slika 2.7). V preslikovalno tabelo pa se doda nova vnosna vrstica (slika 2.8).



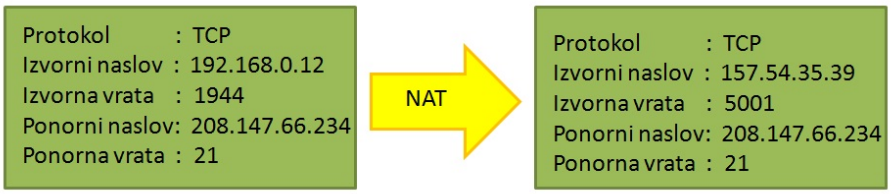
Slika 2.7: Preslikovanje paketa za računalnik B.

NAT preslikovalna tabela
192.168.0.10 : 3576 ← TCP → 157.54.35.38 : 5000
192.168.0.11 : 2258 ← TCP → 157.54.35.39 : 5000

Slika 2.8: Nov vnos v preslikovalni tabeli za računalnik B z dinamičnim preslikovanjem naslova.

Na koncu še uporabnik računalnika C pošlje paket iz privatnega v javno omrežje z privatnim IP naslovom 192.168.0.12 in vrati 1944. Ko paket prispe do usmerjevalnika vidimo, da sta oba javna IP naslova že zasedena od računalnika A in računalnika B. Zato uporabi enega od obstoječih javnih IP naslovov in spremeni izvorna vrata. Ta par (javni IP naslov:vrata) mora biti v preslikovalni tabeli unikaten. Če bi imelo več različnih naprav v podomrežju enak javni IP naslov in vrata usmerjevalnik nebi vedel, kateremu računalniku v privatnem omrežju paket poslati.

Paket se spremeni (slika 2.9), nov unikaten vnos se doda v preslikovalno tabelo (slika 2.10).



Slika 2.9: Preslikovanje paketa za računalnik C.

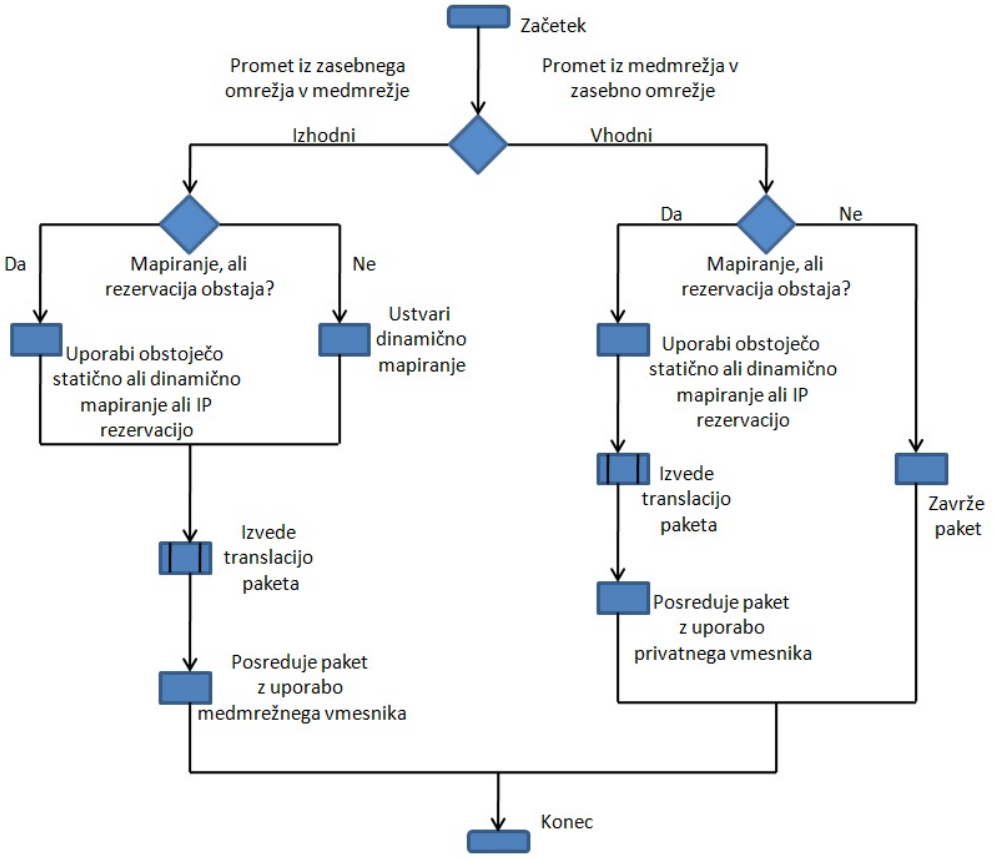
NAT preslikovalna tabela
192.168.0.10 : 3576 ← TCP → 157.54.35.38 : 5000
192.168.0.11 : 2258 ← TCP → 157.54.35.39 : 5000
192.168.0.12 : 1944 ← TCP → 157.54.35.39 : 5001

Slika 2.10: Nov vnos v preslikovalni tabeli za računalnik C z dinamičnim preslikovanjem naslova in vrat.

Obravnavanje vhodnih in izhodnih NAT paketov

Slika 2.11 prikazuje, kako NAT obravnava paket glede na to ali prihaja iz privatnega omrežja (uporabnikovi paketi) ali iz medmrežja (odgovori na uporabnikove zahteve). Paketi iz javnega omrežja so lahko tudi odvečni paketi (tisti, ki jih uporabnik ni zahteval), te pakete se zavrže.

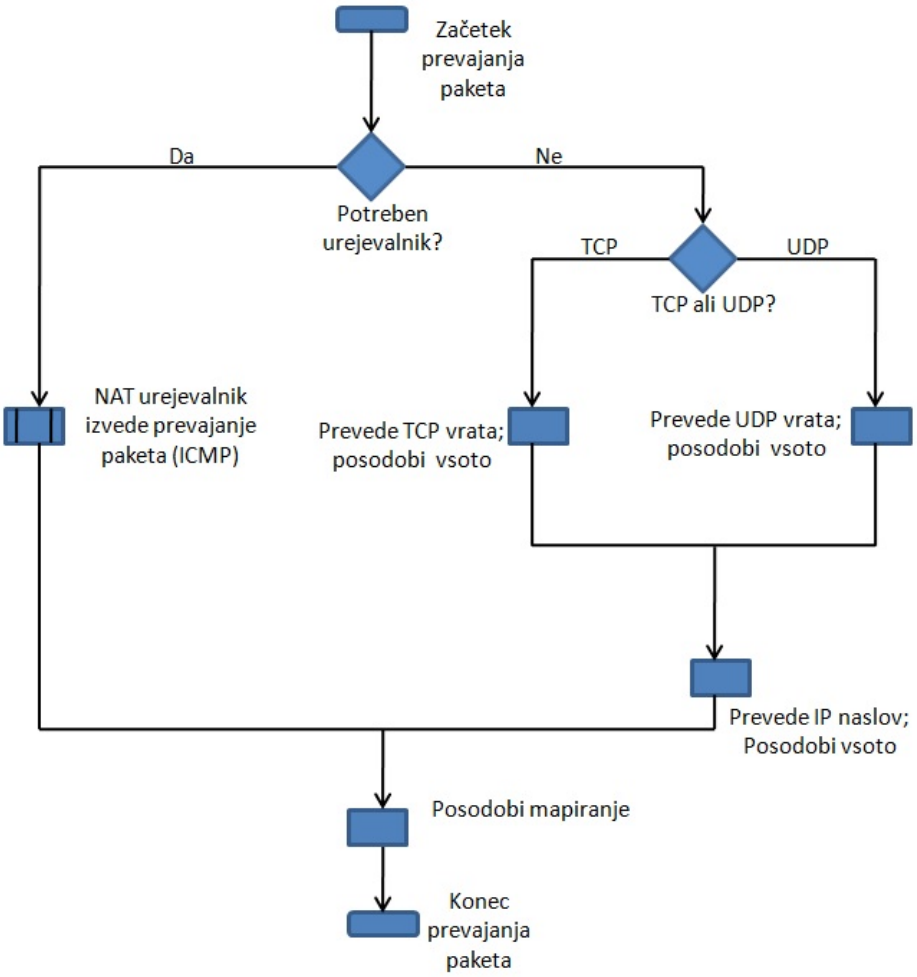
Ko pride paket iz privatnega omrežja (izhodni paket) se najprej preveri, če zanj obstaja zapis v preslikovalni tabeli, drugače se doda nov zapis. Zatem se izvede translacija paketa (spremeni se izvorni IP naslov in vrata) in paket potuje naprej v medmrežje. Pri potovanju paketa iz medmrežja se najprej preveri v preslikovalni tabeli, če obstaja zapis. Če ta obstaja se izvede translacija paketa in se pošlje naprej v privatno omrežje, drugače pa se paket zavrže.



Slika 2.11: NAT obravnava vhodnih in izhodnih paketov.

Obravnava preslikave paketa

Slika 2.12 nam prikazuje kaj se dogaja s paketom, ko potuje skozi postopek translacije (spreminjanja IP naslova ter vrat). Ta postopek je enak za vhodne in izhodne pakete. Če se IP naslov in vrata v paketu nahajata v IP in TCP ali UDP glavi, se paket prevede brez urejevalnika.(Desna stran slike 2.12).



Slika 2.12: Preslikava paketa.

Obstajata dva primera, ko NAT ne more izvesti prevajanja paketa brez pomoči urejevalnika, ki mu včasih rečemo tudi aplikacijski prehod. Če so IP naslov, TCP vrata ali UDP vrata shranjena v tovoru (*payload*) paketa. Nekatere aplikacije raje shranijo IP naslov in vrata znotraj podatkovnega dela paketa namesto v IP, UDP ali TCP glavo. Primer take aplikacije je FTP (*File Transfer Protocol*). Ta shrani IP naslov v glavo paketa. Poleg tega FTP shrani IP naslov v decimalnem zapisu s pikami, kar pomeni, da je lahko preveden IP naslov različnih velikosti. Zato je potrebno spremeniti

zaporedje številk TCP (*TCP sequence numbers*), da se zagotovi, da ni izgub podatkov. Primera takih aplikacij sta tudi *RealAudio* in *CUSeeMe*, ki uporabljata TCP povezavo z dinamičnim izbiranjem UDP vrat, po katerih so prenešeni podatki.

TCP ali UDP se ne uporablja za identifikacijo podatkovnega toka. Podatki, ki so tunelirani po medmrežju z uporabo PPTP *Point-to-Point Tunneling Protocol* ne uporabljajo TCP ali UDP glave. Namesto tega uporabljajo GRE (*Generic Routing Encapsulation*) glavo, *call ID*, ki je shranjen v glavi GRE opredeljuje podatkovni tok.

NAT urejevalniki so ALGs (*application level gateways*), ki so jih razvili za prenos paketov v teh dveh primerih. Urednik NAT razišče pakete, ki jih pošlje taka aplikacija in spremeni podatke kot je potrebno. Ker s s tem spremeni tudi velikost paketov mora urejevalnik spremeniti tudi zaporedne številke TCP paketov.

Na napravi je lahko več NAT urejevalnikov, eden od teh skrbi za podporo sporočil o napakah (*ICMP*).

2.5 Razdelitev IP naslovov v razrede

Razred	**Levi biti**	**Število omrežij**	**Število naprav v omrežju**	**Začetni naslov**	**Končni naslov**
A	0xxx	128 (2^7)	16.777.216 (2^{24})	0.0.0.0	127.255.255.255
B	10xx	16.384 (2^{14})	65.536 (2^{16})	128.0.0.0	191.255.255.255
C	110x	2.097.152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
D	1110	ni opredeljeno	ni opredeljeno	224.0.0.0	239.255.255.255
E	1111	ni opredeljeno	ni opredeljeno	240.0.0.0	255.255.255.255

Tabela 2.4: Vseh 5 razredov.

IPv4 naslovni prostor je razdeljen na pet razredov. To so A, B C D in E (tabela 2.4). Naslove iz prvih 3 razredov RIR (*Regional Internet Registry*)

dodeljuje internetnim ponudnikom. Razred D je uporabljen za razpošiljanje (*multicast*), razred E pa je rezerviran za bodočo uporabo.

A

Razred A je prepoznaven po prvem bitu z vrednostjo 0. Prvi IP naslov ki je na voljo je 0.0.0.0 zadnji pa 127.255.255.255. Je največji od vseh razredov saj zajema polovico vseh možnih IP naslovov. Vsak naslov je sestavljen iz 32-ih bitov, ker je prvi bit uporabljen za določitev razreda, jih ostane 31. Iz tega sledi da je v razredu A na voljo

$$2^{31} = 2.147.483.648 \text{ IP naslovov.}$$

Od teh naslovov jih $2^7 = 128$ predstavlja število omrežij v razredu, $2^{24} = 16.777.216$ pa največje število naprav v omrežju.

B

Razred B je prepoznaven po prvih dveh bitih 10. Njegov prvi IP naslov se začne z 128.0.0.0 konča pa z 191.255.255.255. Njegov razpon IP naslovov obsega četrtina vseh naslovov, ker sta prva dva bita rezervirana za določilo razreda jih ostane še 30. Na voljo imamo

$$2^{30} = 1.073.741.824 \text{ IP naslovov.}$$

Od teh naslovov jih $2^{14} = 16.384$ predstavlja število omrežij v razredu, $2^{16} = 65.536$ pa največje število naprav v omrežju.

C

Razred C je prepoznaven po prvih treh bitih 110. Njegov prvi IP naslov se začne z 192.0.0.0, zadnji pa je 223.255.255.255. Obsega osmino vseh IP naslovov, ker so prvi trije biti rezervirani za določilo razreda jih ostane 29 iz teh bitov lahko sestavimo

$$2^{29} = 536.870.912 \text{ IP naslovov.}$$

Od teh naslovov jih $2^{21} = 2.097.152$ predstavlja število omrežij v razredu, $2^8 = 256$ pa največje število naprav v omrežju.

D

Razred D je prepoznaven po prvih štirih bitih 1110. Prvi IP naslov se začne pri 224.0.0.0 zadnji se konča pri 239.255.255.255. Pokriva šestnajstino vseh naslovov, za naslove mu ostane 28 bitov, kar znaša

$$2^{28} = 268.435.456$$

IP naslovov, ki se uporabljajo za naslove razpošiljevalnih skupin.

E

Razred E je podoben razredu D in je prepoznaven po prvih štirih bitih, ki so 1111. Zajema šestnajstino vseh naslovov. Prvi naslov se prične pri 240.0.0.0 zadnji se konča pri 255.255.255.255. Za naslove mu ostane 28 bitov in tako kot razred D pokriva

$$2^{28} = 268.435.456 \text{ IP naslovov.}$$

2.6 Notacija CIDR

CIDR (*Classless Inter Domain Routing*) je metoda za dodeljevanje IP naslovov brez uporabe standardnih razredov kot so razred A, B, C, D in E.

V zapisu CIDR je IP naslov sestavljen kot X.Y.Z.Q/n, kjer n predstavlja omrežno predpono oziroma masko omrežja. Maska označuje število bitov, ki so uporabljeni za določitev omrežja. Maska je lahko največ 32

(255.255.255.255) ter najmanj 0 (0.0.0.0). X, Y, Z in Q so števila, katerih vrednost je lahko od 0 do 255.

Število naprav v podomrežju izračunamo po formuli

$$2^{32-n} - 2 \ ,$$

kjer je n število bitov v maski mreže. Na koncu odštejemo dva naslova, ker je prvi naslov v podomrežju naslov omrežja in zadnji naslov za oddajanje (*broadcast*).

2.7 Zasebni IP naslovi

Zasebno omrežje je omrežje, ki uporablja posebni IP naslovni prostor. Za svoje delovanje uporablja standarde, ki jih najdemo v [17, 12]. Ta naslovni prostor se pogosto uporablja za dom, pisarne ter lokalna omrežja podjetij.

V podjetjih, ki imajo večje število računalnikov, do večine od njih ni potrebno dostopati iz medmrežja temveč je dovolj, da so povezani med seboj. Izkazalo se je, da zasebni naslovni prostor močno pomaga pri upočasnitvi izčrpanja javnih naslovov. Z uporabo NAT-a ali vmesnega (*proxy*) strežnika je mogoče zasebno omrežje povezati z medmrežjem.

Ti naslovi so označeni kot zasebni, ker v medmrežju niso uporabljeni oziroma niso dodeljeni nobeni organizaciji. Paketov z IP naslovom zasebnega omrežja se ne sme usmerjati po medmrežju. Vsakdo lahko uporablja zasebne naslove brez dovoljenja RIR (*Regional Internet Registry*). To je organizacija, ki sodeluje z IANA (*Internet Assigned Numbers Authority*), in z upoštevanjem njihovih pravil dodeljujejo javni IP naslovni prostor internetnim ponudnikom.

Blok, maska, razred	Začetek	Konec	Št. naslovov
24-bitni (/8 maska, 1xA)	10.0.0.0	10.255.255.255	16.777.216
20-bitni (/12 maska, 16xB)	172.16.0.0	172.31.255.255	1.048.576
16-bitni (/16 maska, 256xC)	192.168.0.0	192.168.255.255	65.536

Tabela 2.5: Naslovni prostori zasebnih omrežij.

V tabeli 2.5 so zasebni naslovi rezervirani v razredu A, B in C. Pri prvem razredu ta prostor pokriva en A blok od 10.0.0.0 do 10.255.255.255. Osem bitov zasede omrežje, ostalih 24 bitov lahko uporabimo za naslavljanje omrežnih naprav. Tako imamo na voljo 2^{24} različnih IP naslovov. Pri drugem razredu prostor pokriva šestnajst B blokov od 172.16.0.0 do 172.31.255.255. Dvanajst bitov zasede omrežje in ostalih 20 bitov je na voljo za naslavljanje naprav. Na voljo imamo 2^{20} različnih IP naslovov. Pri tretjem razredu ta prostor pokriva 256 C blokov od 192.168.0.0 do 192.168.255.255. Šestnajst bitov zasede omrežje, medtem ko jih ostalih šestnajst ostane za naslavljanje naprav. Na voljo imamo 2^{16} različnih IP naslovov. Uporabnik lahko sam izbira v katerem razredu zasebnih naslovov bo gostoval, običajno pa je izbira odvisna od števila mrežnih naprav, ki bi jih radi imeli v uporabi.

2.8 Protokol DHCP

DHCP (*Dynamic Host Configuration Protocol*) je omrežni protokol, ki se uporablja za nastavitev omrežnih naprav, da se lahko priključijo v omrežje. Odjemalec s pomočjo protokola DHCP pridobi informacije o nastavitvah kot so IP naslov, privzeti prehod (*default gateway*), IP naslov imenskega strežnika in podobno. Ko je postopek končan, lahko odjemalec komunicira z napravami v svojem omrežju oziroma z zunanjim omrežjem.

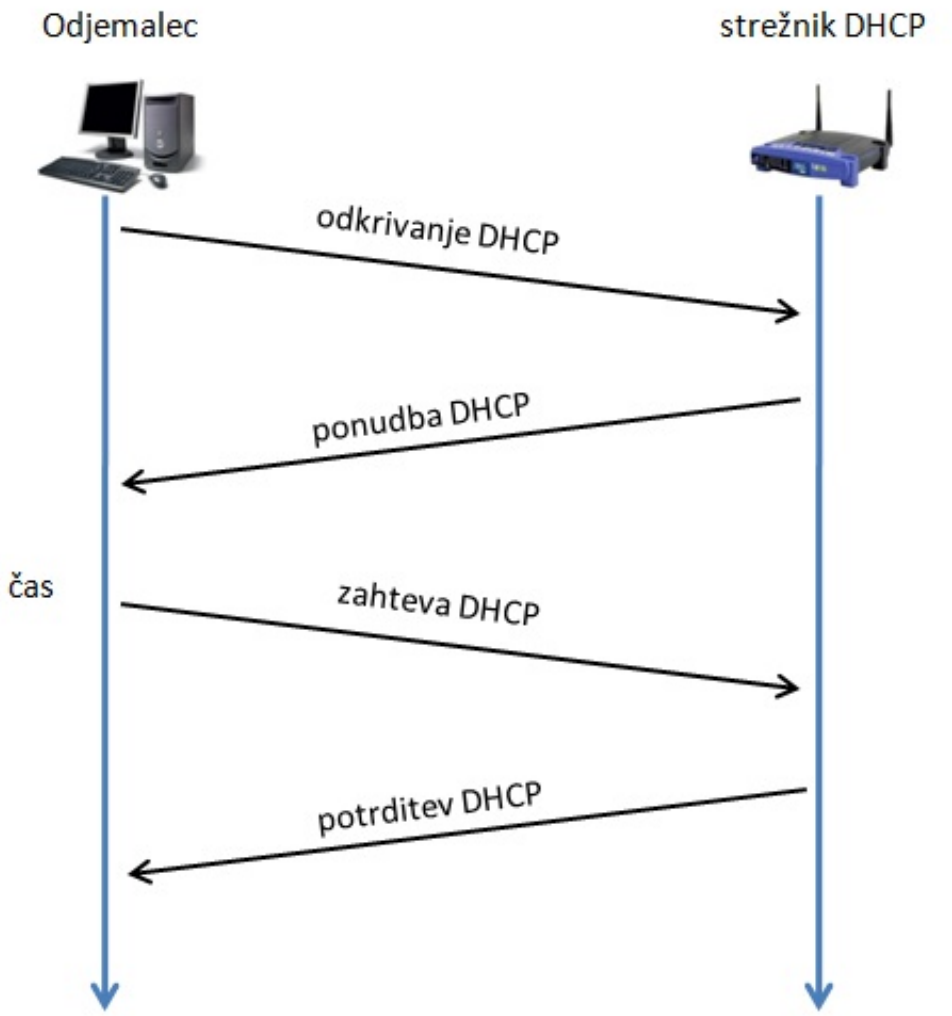
Naloga strežnika DHCP je, da vzdržuje bazo prostih IP naslovov in informacije nastavitev. Za vsakega odjemalca hrani ime naprave, dodeljen IP

naslov, naslov MAC in odpustitveni čas (*lease time*). Odjemalec mora sam poskrbeti za podaljšanje odpustitvenega časa. Ko ta čas preteče ga strežnik izbriše iz baze. Če se to ne bi zgodilo, bi se sčasoma polje praznih IP naslovov izpraznilo in posledično novi odjemalci ne bi dobili prostega IP naslova, s tem bi bil dostop do medmrežja onemogočen.

Protokol DHCP je bil prvič opredeljen kot standardni protokol v RFC 1531 [19] oktobra 1993, ki je razširjena različica BOOTP (*Bootstrap Protocol*) protokola (RFC 951) [6]. BOOTP zahteva ročno vnašanje nastavitev za vsakega odjemalca posebej in ne zagotavlja mehanizma za povrnitev zastarelih IP naslovov [1].

2.8.1 Vzpostavitev povezave

Za vzpostavitev povezave je potreben postopek izmenjavanja sporočil med uporabnikom in DHCP strežnikom, kot ga prikazuje slika 2.13. Če bi obstajal en sam DHCP strežnik bi se lahko korakoma ponudbi DHCP in zahtevi DHCP izognili [8, 7].



Slika 2.13: Potek vzpostavitve povezave.

odkrivanje DHCP (*discovery*)

Odjemalec odda (*broadcast*) sporočila po fizičnem podomrežju, da bi našel razpoložljive strežnike DHCP. Z odjemalčeve strani se tvori sporočilo UDP (*User datagram protocol*), ki je naslovljeno na 255.255.255.255 (oddajni na-

slov).

ponudba DHCP (*offer*)

Ko strežnik DHCP prejme odjemalčevo sporočilo, zanj rezervira IP naslov ter mu pošlje sporočilo z ponudbo DHCP. Ta vsebuje odjemalčev MAC naslov, rezervirani IP naslov, masko podomrežja, odpustitveni čas ter IP naslov strežnika. Strežnik določi nastavitve glede na odjemalčev fizični naslov.

zahteva DHCP (*request*)

Ker se na odjemalčevo zahtevo lahko oglasi več DHCP strežnikov, ki vsak pošlje svojo ponudbo, se mora odjemalec odločiti za samo eno ponudbo. To naredi tako, da pošlje izbranemu strežniku zahtevo, v kateri zaprosi za dodeljen IP naslov. Ostali strežniki so obveščeni, katero zahtevo je odjemalec sprejel.

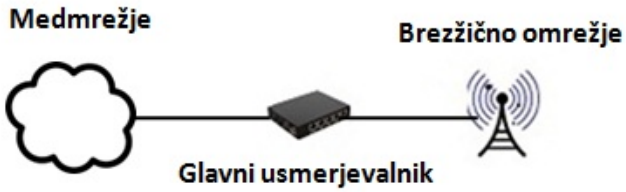
potrditev DHCP (*acknowledgement*)

Ko strežnik prejme zahtevo DHCP odjemalca se prične zadnji korak procesa. Ta vključuje pošiljanje sporočila potrditve DHCP odjemalcu. V tej točki je IP nastavitveni proces končan.

Poglavje 3

Model omrežja

V tem poglavju je opisano, kakšna je bila infrastruktura omrežja ISP-ja preden smo jo spremenili in kakšna po spremembi. Glavni razlog je bil prilagoditev omrežja zakonu o elektronskih komunikacijah. Med drugimi pa se je poenostavila zgradbo omrežja, razbremenil se je tudi glavni usmerjevalnik (slika 3.1), na katerem je bil NAT za celotno omrežje.



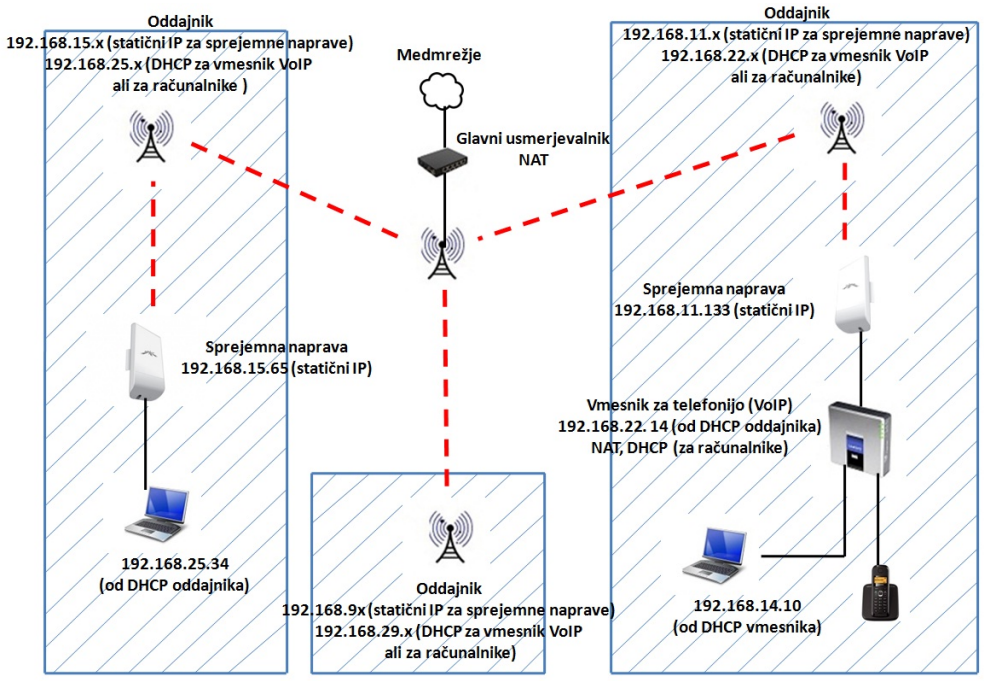
Slika 3.1: Najpomembnejši člen omrežja.

3.1 Prvotna zgradba omrežja

Prvotna zgradba omrežja je temeljila na privatnih statičnih IP naslovih. Vsi uporabniki ISP-omrežja so bili v medmrežje vidni preko enega javnega IP naslova, katerega je imel glavni usmerjevalnik, ki je v medmrežje povezan preko

optičnega vlakna. Na tem usmerjevalniku je bil NAT za celotno omrežje, ki je označeno na sliki 3.2 s šrafiranim področjem.

Od glavnega usmerjevalnika naprej potekajo povezave preko brezžičnega omrežja s standardom 802.11n do vseh oddajnikov v omrežju.



Slika 3.2: Označeno je lokalno omrežje 192.168.X.Y.

ISP je uporabljal zasebne IP naslove iz C razreda. Vsaki odjemalčevi sprejemni napravi je bil dodeljen statičen IP naslov 192.168.X.Y z masko 255.255.255.0 (24).

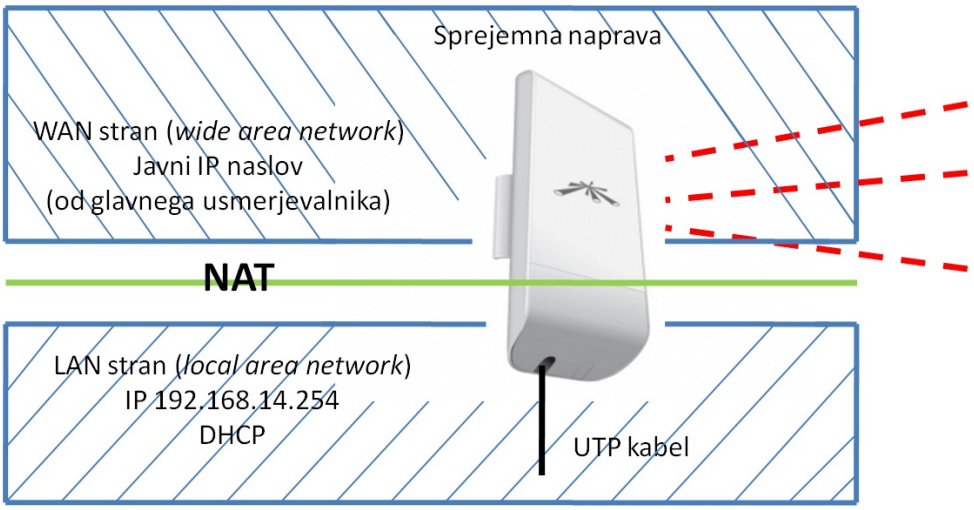
Pri tem je X oznaka za skupino odjemalcev, ki so povezani na isti oddajnik (podomrežje). Vsak oddajnik je imel svoj razred X, ter vsak odjemalec v razredu X svoj Y. Ta statičen IP naslov je bil vpisan v odjemalčevo sprejemno napravo, na kateri se nastavila tudi njegova pasovna širina. Na vsakem oddajniku je bilo poleg podomrežja za statične IP naslove sprejemnih naprav še podomrežje za naprave za njimi (računalniki, VoIP vmesniki, usmerjevalniki).

Vse sprejemne naprave so bile nastavljene v premostitveni način (*bridge mode*), kar pomeni, da gredo paketi skozi napravo brez da bi jih ta spremenila. Za sprejemnimi napravami so bili običajno priključeni računalniki, ki so dobili IP naslov od oddajnikovega strežnika DHCP. V primeru, da je odjemalec imel tudi telefonski priključek je bil za sprejemno napravo priključen VoIP (*Voice over Internet Protocol*) vmesnik, na katerem je bil NAT ter strežnik DHCP. S temi nastavitvami se je, ko je bil v uporabi telefon, samodejno rezerviralo 300 kb/s pasovne širine (*Quality of service*), da so se lahko nemoteno opravljali telefonski pogovori. Za VoIP vmesnikom pa so bili priključeni računalniki, ki so dobili IP naslov od VoIP vmesnika (slika 3.2).

3.2 Model posodobljenega omrežja

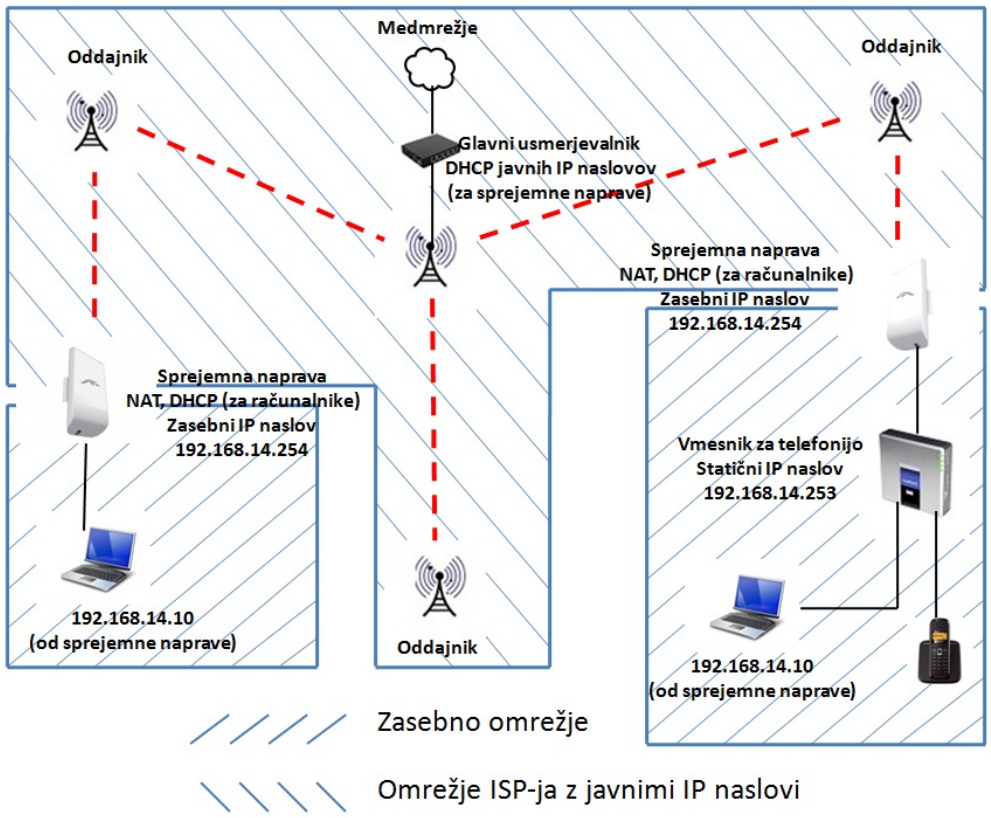
Na sliki 3.4 je prikazan posodobljeni model omrežja katerega zgradba se zelo razlikuje od prvotne zgradbe. Za posodobitev omrežja smo si najbolj pomagali s programom, ki smo ga napisali. Na glavnem usmerjevalniku je sedaj bazen (*pool*) javnih IP naslovov ter ne več NAT za celotno omrežje, kar usmerjevalnik močno razbremeni.

Vse naprave med glavnim usmerjevalnikom in sprejemnimi napravami so sedaj nastavljene v premostitveni način (*bridge mode*). Na sprejemnih odjemalčevih napravah je sedaj NAT in strežnik DHCP. Te naprave od glavnega usmerjevalnika prejmejo javni IP naslov, katerega odpustitveni čas (*lease time*) je 30 dni. Torej, če naprava v omrežje ni vključena več kot 30 dni, se njen IP naslov sprosti. Ob naslednjem priklopu v omrežje pa dobi drugega.



Slika 3.3: Delovanje sprejemne naprave.

Vsaka odjemalčeva sprejemna naprava ima svoje podomrežje (*local area network*) z IP naslovom 192.168.14.254 (slika 3.3), privzetim prehodom 192.168.14.254 in strežnikom DHCP z bazenom (*pool*) od 192.168.14.10 do 192.168.14.100. Za odjemalce, ki imajo telefonski priključek je za sprejemno napravo priključen vesnik VoIP s statičnim IP naslovom 192.168.14.253. Da lahko do njega dostopamo, je na sprejemni napravi vključeno posredovanje vrat (*port forwarding*). Omogočen je tudi DMZ (*demilitarized zone*), s katerim se lahko izognemo NAT-u s tem, da v mrežno napravo vpišemo statični IP naslov 192.168.14.1. Naprava avtomatsko dobi javni IP naslov sprejemne naprave in postane vidna v medmrežju.



Slika 3.4: Javno omrežje s svojim strežnikom DHCP in lokalna omrežja 192.168.14.Y s svojimi strežniki DHCP.

3.3 Prednosti in slabosti sistemov

Poglejmo si nekatere prednosti in slabosti novega sistema v primerjavi s starejšim.

Novejši sistem dela NAT na vsaki odjemalčevi sprejemni napravi in ne več samo na glavnem usmerjevalniku. Je bolj enostavno zgrajen sistem, ki omogoča sledljivost strank na enostaven način. Nastavitev odjemalčevih naprav je hitrejša, na napravo prenesemo nastavitveno datoteko ter nato nekaj malenkosti spremenimo. V omrežju se ne more zgoditi, da bi dve

sprejemni napravi imeli isti IP naslov saj za to skrbi strežnik DHCP na glavnem usmerjevalniku. Vsak odjemalec ima svoje podomrežje. Povezave med sprejemnimi napravami in oddajniki so zaščitene z WPA2 zaščito.

V starem sistemu ni bila možna sledljivost strank. Znotraj podomrežja (oddajnika) so bili vsi računalniki med seboj vidni. Navsezadnje je bilo možno, da sta dve sprejemni napravi imeli isti IP naslov saj smo jih vnašali ročno.

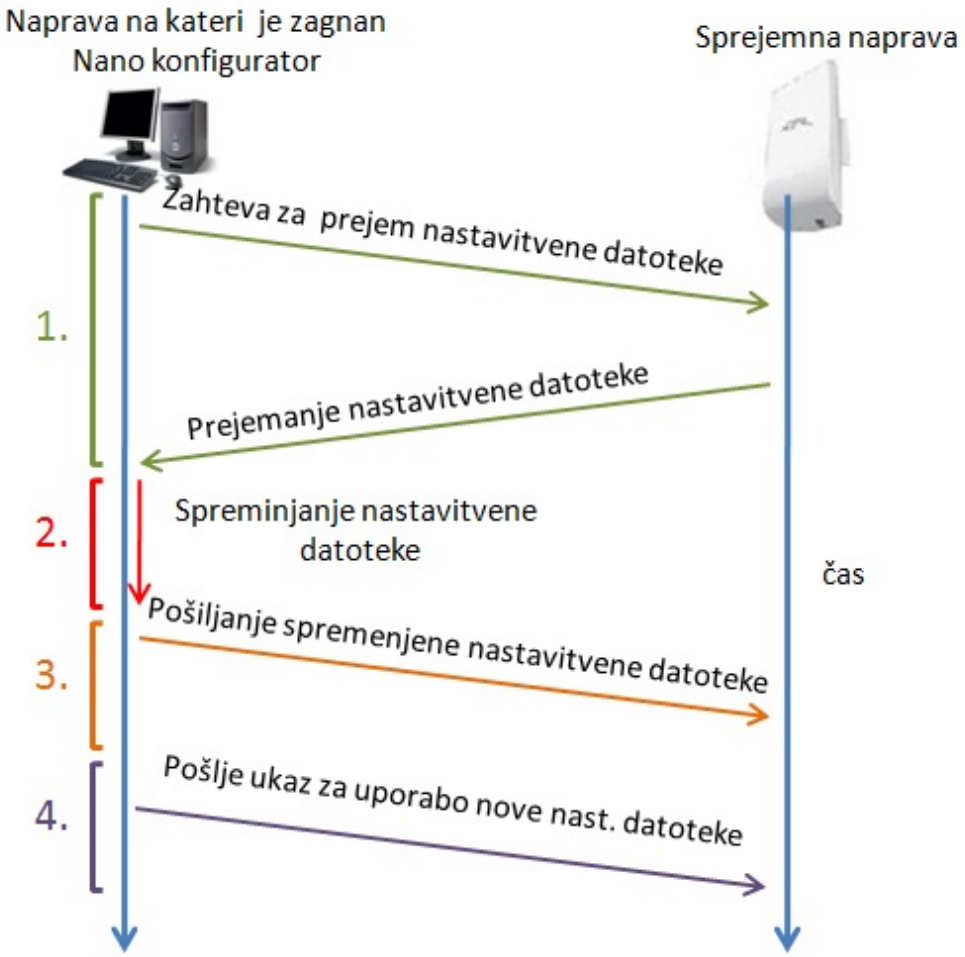
Poglavje 4

Konfiguracijski program

V tem poglavju je opisano izdelovanje programa za spreminjanje odjemalčevih sprejemnih naprav in težave, ki so nastale, ko smo z njegovo pomočjo spreminjali zgradbo omrežja. S pomočjo programa, ki smo ga poimenovali *Nano konfigurator* smo se izognili dolgotrajni ročni nastavitvi odjemalčevih sprejemnih naprav.

4.1 Izdelava programa

Program z imenom *Nano konfigurator* smo naredili v Microsoft Visual Studiu 2010 v jeziku C#. Njegova naloga je, da preko IP naslova dostopa do odjemalčeve sprejemne naprave in spremeni njene nastavitve. V program v vnosno vrstico vnesemo IP naslove odjemalčevih naprav, katerih nastavitve želimo spremeniti. Vnesemo lahko poljubno število IP naslovov.



Slika 4.1: Glavne aktivnosti programa.

Ko zaženemo postopek spreminjanja nastavitev naprav se najprej vsi IP naslovi, ki smo jih vnesli v vnosno vrstico vstavijo v tabelo. Glavna zanka iz te tabele posamično jemlje IP naslove. Za vsak IP naslov se izvedejo 4 glavne aktivnosti (slika 4.1). Glavna zanka pa se izvede za vse vnesene IP naslove. Glavne 4 aktivnosti so:

I. `sshScp(ip_naslov, sprejmi)`,

II. `spremeniKonf()`,

III. `sshScp(ip_naslov, poslji)`,

IV. `nano_konzola(ip_naslov)`.

Naloga prve aktivnosti je, da vzpostavi povezavo s sprejemno napravo in z nje prenese nastavitveno datoteko. To stori preko SSH povezave, ki uporablja programsko knjižnico Tamir.SharpSsh [10]. Prva aktivnost je definirana s funkcijo `sshScp(ip_naslov, sprejmi)`. Preko prvega parametra (ip_naslov) funkciji dodelimo IP naslov sprejemne naprave, z drugim parametrom (sprejmi) pa funkciji sporočimo, da želimo prejeti datoteko.

V funkciji deklariramo naslednje konstante:

- local: mesto v datotečnem sistemu kjer naj se shrani nastavitvena datoteka, ki jo prenesemo iz naprave,
- host: eden izmed IP naslovov, ki jih vnesemo v vnosno polje v aplikaciji,
- remote: mesto v datotečnem sistemu naprave kjer se nahaja nastavitvena datoteka,
- user: uporabniško ime za dostop do naprave,
- pass: geslo za dostop do naprave,
- port: SSH vrata za dostop do naprave.

Ker imamo v prvi funkciji drugi argument z imenom sprejmi, se v izvorni kodi kliče funkcija `scp.From(host, port, remote, user, pass, local)`. Po izvršitvi prve aktivnosti se v datoteki, kjer se nahaja program (*Nano konfigurator*), pojavi nastavitvena datoteka, ki smo jo prejeli od sprejemne naprave.

Naloga druge aktivnosti, ki je opredeljena v metodi `spremeniKonf()` je, da iz nastavitvene datoteke sprejemne naprave, ki smo jo dobili s prvo aktivnostjo pridobi podatke o odjemalcu, ki jih potrebujemo. V datoteki, kjer se

nahaja program imamo nastavitveno datoteko z imenom *koncne-nastavitve*, ki ustreza novim nastavitvam sistema. Podatke ki smo jih pridobili iz nastavitvene datoteke iz naprave vstavimo v datoteko z novimi nastavitvami, nekatere med njimi so (prim. tudi sliko 4.2):

- Država: različne države imajo različne frekvenčne pasove,
- Naziv: v nazivu se nahaja ime priimek ter naslov odjemalca,
- Ssid: ime brezžičnega omrežja na katerega se hočemo povezati,
- Channel shifting: je lahko vključen ali izključen,
- Distance: razdalja med sprejemno napravo in oddajnikom,
- Limita: ali ima uporabnik omejeno pasovno širino,
- Download: omejitev sprejemanja,
- Upload: omejitev oddajanja.

```
radio.1.countrycode=705
radio.countrycode=705
resolv.host.1.name=Damjan Maček, Želodkova ulica 7
wireless.1.ssid=gora-oselica
radio.1.chanshift=0
radio.1.ackdistance=12000
tshaper.in.rate=4126
tshaper.out.rate=1024
tshaper.status=enabled
```

Slika 4.2: Delček nastavitvene datoteke.

Pri tej aktivnosti smo imeli kar nekaj težav, saj smo morali podatke pridobiti iz nastavitvene datoteke. Slika 4.2 predstavlja delček te datoteke. Celotna datoteka vsebuje 362 različnih ključev. Ker ima vsaka sprejemna

naprava različen vrstni v nastavitveni datoteki se je pojavila težava branja te datoteke. Posledično smo se odločili, da nastavitveno datoteko preberemo kot podatkovni slovar. Podatkovni slovar je sestavljen iz ključa, katerega ime je unikatno ter neponovljivo in vrednosti, ki je lahko poljubne vrednosti. Na sliki 4.2, vidimo, da je v vsaki vrstici enačaj. Tako lahko besede, ki so na levi strani enačaja vzamemo kot ključ slovarja saj so neponovljive, besede na desni pa kot vrednost. V datoteki, kjer se nahaja program se nahaja nastavitvena datoteka, ki ustreza končnim nastavitvam (datoteka z imenom *koncne-nastavitve*). To pomeni, da je v njej že nastavljeno samodejno pridobivanje IP naslova in posredovanje vrat (*port forwarding*), ki je potreben da lahko dostopamo do vmesnika VOIP. Od sedaj naprej bodo namreč vse sprejemne naprave delale NAT. Tudi številka vrat za HTTP, SSH ter HTTPS so spremenjena. Nekatere nastavitve bo datoteka prejela preko polj in gumbov v programu na primer sprememba gesla, vklop HTTPS in zaščita brezžičnega omrežja z WPA2. Obe datoteki *koncne-nastavitve* in nastavitveno datoteko prejeto od naprave preberemo kot podatkovni slovar. Iz podatkovnega slovarja odjemalčeve nastavitvene datoteke izberemo ključe katerih vrednosti moramo prenesti v podatkovni slovar *koncne-nastavitve*. V slovarju *koncne-nastavitve* poiščemo istoimenske ključe ter vstavimo ustrezne vrednosti. Ko je postopek končan imamo datoteko *koncne-nastavitve* ustrezno spremenjeno.

Da to datoteko spravimo nazaj na sprejemno napravo, nam omogoča tretja aktivnost, ki uporablja isto funkcijo kot prva, samo da se kliče s spremenjenim drugim parametrom (poslji). Vse kar ta atribut spremeni je, da se namesto funkcije `scp.From(host, port, remote, user, pass, local)` kliče funkcijo `scp.To(local, host, port, remote, user, pass)`. S to funkcijo se spremenjena nastavitvena datoteka pošlje na sprejemno napravo.

Sledi še zadnja aktivnost ki se kliče z metodo `nanoKonzola()`. Njena naloga je, da se trenutno aktivna nastavitvena datoteka ne uporablja več, temveč pride v uporabo datoteka, ki smo jo na napravo poslali v tretji aktivnosti. Obenem se naredi ponoven zagon sprejemne naprave. Ta funkcija

naredi nov predmet razreda *SshStream*, odpre ukazno vrstico (konzolo) ter v njej izvede ustrezne ukaze.

V programu je zasnovano tudi poročilo o uspešnem oziroma neuspešnem poteku delovanja programa. Za vsako od štirih glavnih aktivnosti programa sporoči ali se je aktivnost izvedla uspešno ali ne. Po končanem spreminjanju odjemalčevih naprav se odpre novo okno, v katerem se izpiše poročilo. Ob zaprtju programa se poročilo shrani v datoteko POROČILA, ki se nahaja v datoteki programa.

4.2 Nastale težave

Ker nekateri odjemalci niso imeli vključene svoje sprejemne naprave v električno napajanje, nekaterim napravam ni bilo mogoče spremeniti nastavitvene datoteke. Tem napravam je bilo kasneje (ko je bila naprava vključena v električno omrežje) potrebno spremeniti nastavitve. Za dostop do naprav s predhodnimi nastavitvami je bilo potrebno izvesti naslednji postopek. Na oddajni napravi smo izključili WPA2 zaščito. Tedaj so se naprave, ki jih do tedaj še nismo spremenili povezale v omrežje. Ponovno smo zagnali program ter spremenili nastavitve teh naprav.

Naprave so dobile IP naslov (po strežniku DHCP) od usmerjevalnika na oddajniku in ne od glavnega usmerjevalnika (strežnik DHCP javnih IP naslovov). Strežnik DHCP na oddajniku je skrbel, da so računalniki, vmesniki VoIP in dostopne točke pri odjemalcih samodejno dobili IP naslov. V tem primeru bi moral predhodno na usmerjevalniku oddajnika izklopiti strežnik DHCP, s tem bi vse antene dobile IP naslov od glavnega usmerjevalnika. Ker se je zgodilo, da tega nismo naredili, so naprave dobile napačen IP naslov. Izpustitveni čas za te IP naslove je bil nekaj dni zato smo se morali ročno povezati na vsako napravo in obnoviti IP naslov.

Spremenili smo napravo, ne da bi prej spremenili nastavitve vmesnikov VoIP. V takem primeru smo se morali povezati na sprejemno napravo in vpisati novo posredovanje vrat (*port forwarding*) z IP naslovom 192.168.14.10.

Kajti vmesnik VoIP je dobil IP naslov preko strežnika DHCP sprejemne naprave, dobil je prvi naslov iz bazena naslovov 192.168.14.10. Sedaj smo lahko dostopali do vmesnika VoIP in mu ročno spremenili nastavitve.

Pri spreminjanju IP naslova na oddajni napravi je prišlo do napake in do naprave nismo mogli več dostopati. V tem primeru smo se morali fizično odpeljati do oddajnika ter napravo izključiti iz električnega omrežja in ponovno vključiti. Vožnjo bi si lahko prihranili s tem, da bi predhodno na napravi vključil agenta, ki bi redno oddajal ping pakete (*Ping Watchdog*) z IP naslovom enega od oddajnikov. *Ping Watchdog* preverja ali ima naprava stik z napravo z vpisanim IP naslovom. Če ga ni se naprava ponovno zažene.

Poglavje 5

Zaključek

V diplomskem delu je opisano, kako v majhnih brezžičnih ISP-jih poteka nadzor nad sledljivostjo strank ter postopek spremembe infrastrukture brezžičnega omrežja. Opisani so osnovni izrazi računalniških omrežij in delovanje omrežja.

Ker zakon o sledljivosti zahteva, da mora vsak ISP (*internet service provider*), poznati identiteto svojih strank je bilo potrebno spremeniti infrastrukturo omrežja. Prvotno omrežje je bilo zgrajeno na zasebnih statičnih IP naslovih. Da bi si olajšali sledljivost strank in povečali varnost v omrežju, je bilo potrebno spremeniti celotni sistem. Spremeniti je bilo potrebno napravo vsakega odjemalca.

Najprej smo zgradili program, ki je bil sposoben dostopati do več odjemalcev hkrati. Napisali smo ga v jeziku C#. Zgrajen je iz štirih glavnih stopenj: naloga prve stopnje je dostop do naprave in sprejem nastavitvene datoteke. V drugi stopnji se spremeni nastavitvena datoteka, v tej stopnji smo dali velik poudarek na zaščito celotnega sistema. Z WPA2 zaščito smo zaščitili brezžične povezave med oddajniki in odjemalci, dostop do omrežnih naprav pa poteka preko HTTPS povezave. Tretja stopnja nastavitveno datoteko naloži nazaj na napravo, četrta pa aktivira na novo naloženo nastavitveno datoteko.

Spreminjanje nastavitev sistema smo začeli pri odjemalcih in se pomikali

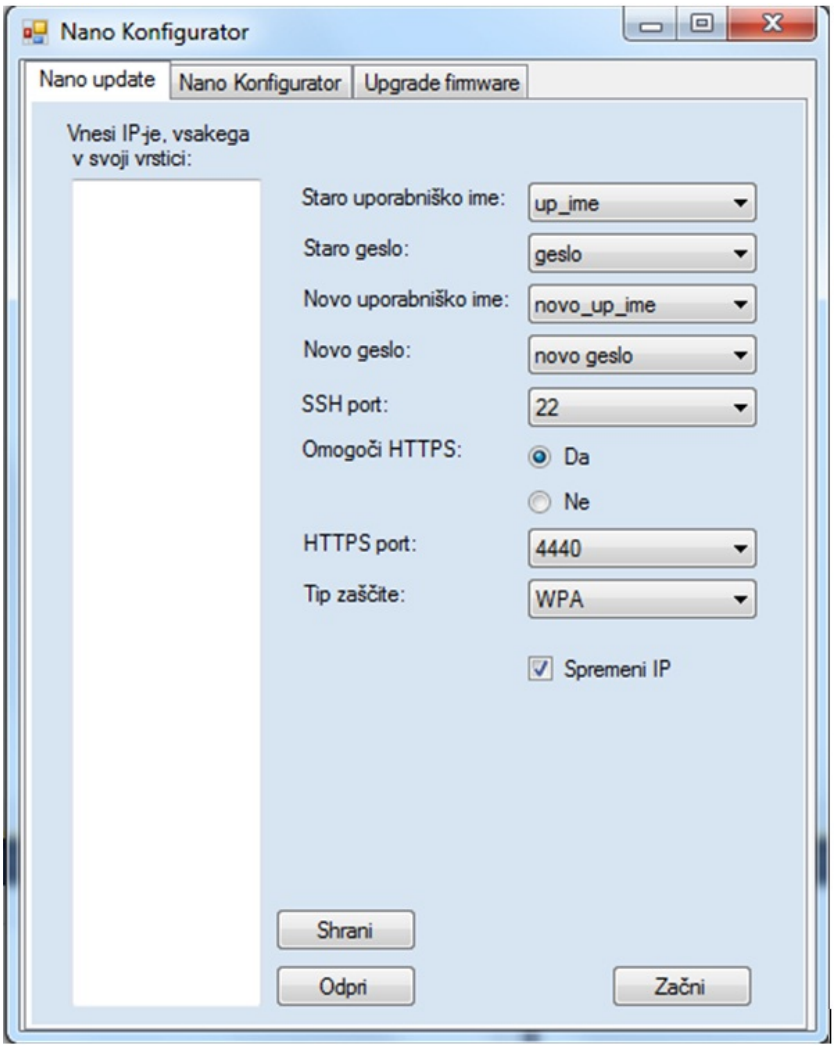
proti glavnemu usmerjevalniku. Tako smo imeli ves čas nadzor nad celotnim omrežjem. Paziti je bilo potrebno na naprave, ki niso bile vključene v omrežje saj do njih ni bilo mogoče dostopati. Te naprave smo nastavili kasneje, ko so bile vključene v omrežje. Sistem smo vedno spreminjali ponoči, ker je takrat aktivnih najmanj odjemalcev. Na ta način smo zmanjšali število pritožb zaradi nedelovanja sistema.

Na glavnem usmerjevalniku, na katerem je v času starega sistema deloval NAT, je sedaj namesto enega javnega IP naslova postavljen bazen javnih IP naslovov, ki jih dobijo odjemalčeve sprejemne naprave. Ker vemo, kateri IP pripada določeni stranki, sedaj ni več težav s sledljivostjo.

V prihodnje bo veljalo pomisliti o prehodu na IPv6. Slednje bo potrebno nekega dne brez dvoma storiti.

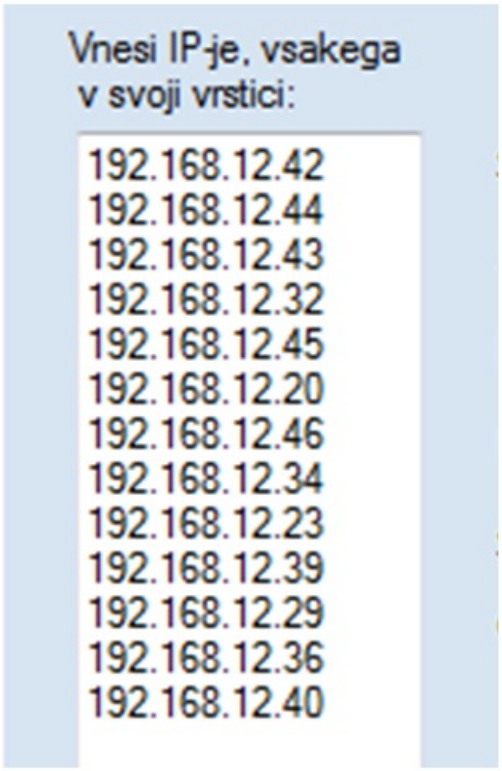
Dodatek A

Opis programa



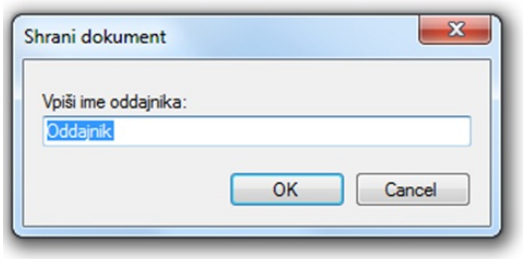
Slika A.1: Izgled programa.

Na sliki A.1 vidimo zunanji izgled programa. V vnosno polje na levi strani vpišemo IP naslove sprejemnih naprav, na katerih želimo spremeniti nastavitve. Poleg vnosnega polja imamo na spodnji strani še gumba »Shrani« in »Odpri«. S Klikom na gumb »Shrani«, se IP naslovi iz vnosnega polja shranijo v tekstovno datoteko. Gumb »Odpri« pa nam omogoča, da tekstovne datoteke, ki smo jih prvotno shranili, odpremo. S tem se nam IP naslovi prikažejo v vnosnem polju. Desno od vnosnega polja imamo gumbe in polja, s katerimi določamo dodatne nastavitve na sprejemnih napravah. Najprej uporabniško ime in geslo, ki omogočata, da lahko preko SSH (*secure shell*) povezave dostopamo do sprejemne naprave. Za dostop do naprave potrebujemo tudi SSH vrata, ki jih izberemo med lastnostmi malo nižje. Novo uporabniško ime in novo geslo nam služita, če želimo spremeniti uporabniško ime in geslo. Po želji lahko izberemo, zaščito sprejemnih anten s HTTPS (*Hypertext Transfer Protocol Secure*) zaščito. Če se odločimo za to zaščito, moramo izbrati še vrata s katerimi lahko dostopamo do sprejemne naprave preko HTTPS. Temu sledi zaščita, s katero lahko zaščitimo našo brezžično povezavo med sprejemnimi in oddajnimi napravami. V našem primeru je to WPA2 zaščita. S klikom na gumb »Začni« sprožimo spreminjanje sprejemnih naprav.



Slika A.2: Vnos IP naslovov v vnosno vrstico.

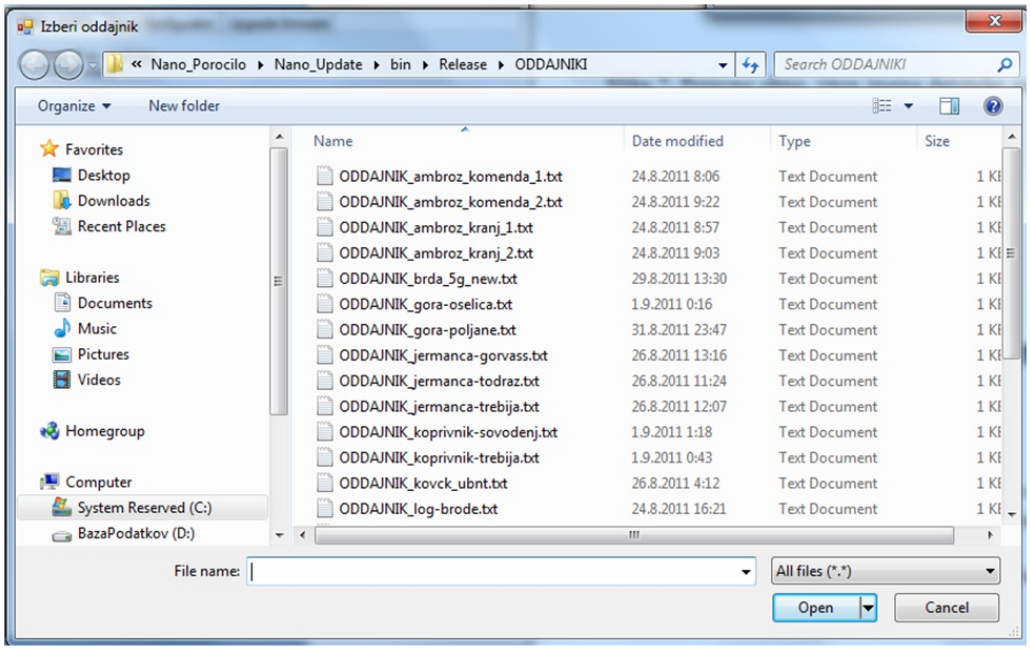
S programom naenkrat spremenimo vse sprejemne naprave odjemalcev, ki so povezani na oddajno napravo. Priporočljivo je, da se njihovi IP naslovi shranijo. To se nam obrestuje, ko želimo ponovno spremeniti nastavitve naprav. V programu nam gumb »Shrani« to omogoča. Vsi podatki (IP naslovi), ki se nahajajo v vnosni vrstici (slika A.2) se shranijo kot tekstovna datoteka v mapo »ODAJNIKI«, ki se nahaja v datoteki programa.



Slika A.3: Pojavno okno, vnos imena datoteke za IP naslove.

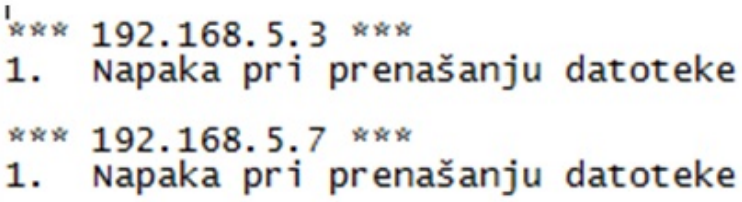
Preden se datoteka dokončno shrani, ji lahko spremenimo ime. Po kliku na gumb »Shrani« se nam prikaže okno (slika A.3), v katerem lahko vpišemo ime, pod katerim želimo datoteko shraniti, kar potrdimo s klikom »OK«.

Ko bomo naslednjič hoteli posodobiti sprejemne naprave, bomo kliknili na gumb »Odpri« in odprlo se nam bo pojavno okno (slika A.4). Tukaj izberemo željeno datoteko, jo odpremo in v vnosnem polju se nam izpišejo IP naslovi.



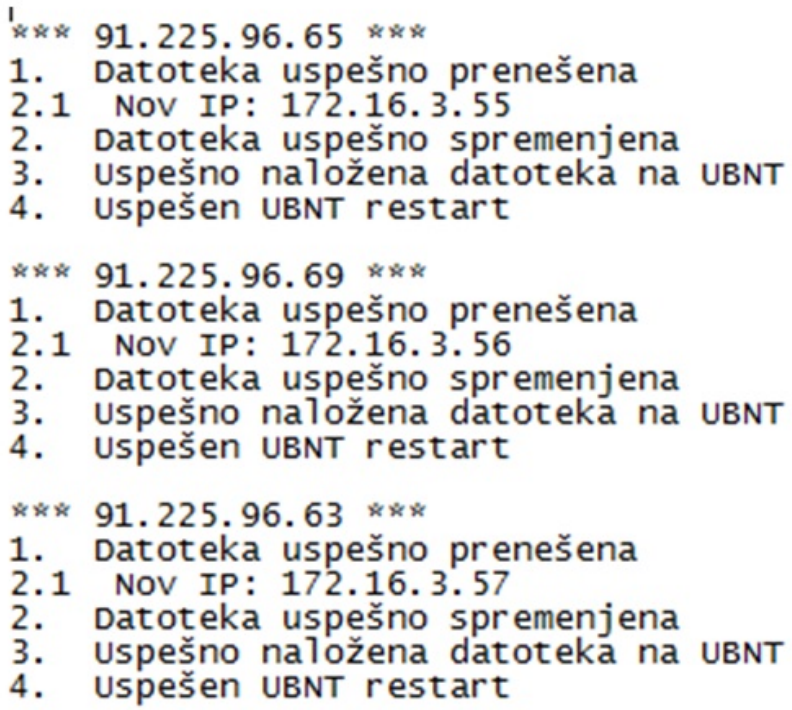
Slika A.4: Izbira oddajnika.

Z gumbom »Začni« zaženemo spreminjanje sprejemnih naprav. Vsaki spremenjeni napravi se nastavi tudi vrnitveni IP naslov (*fallback IP*), ki nam omogoča, da dostopamo do naprave v primeru, če naprava ne dobi IP naslova preko strežnika DHCP. Vrnitveni naslov se shrani v datoteko *koncne-nastavitve* v drugi aktivnosti na sliki 4.1. Da je to izvedljivo, se mora program povezati s strežnikom ISP-ja in iz podatkovne baze poiskati zadnji uporabljen vrnitveni IP naslov. Če je to na primer naslov 172.16.1.200, se ta naslov poveča za 1, torej na 172.16.1.201. Če je ta naslov 172.16.2.254, se naslov spremeni v 172.16.3.1 ter se ob zaprtju aplikacije posodobi v podatkovni bazi strežnika.

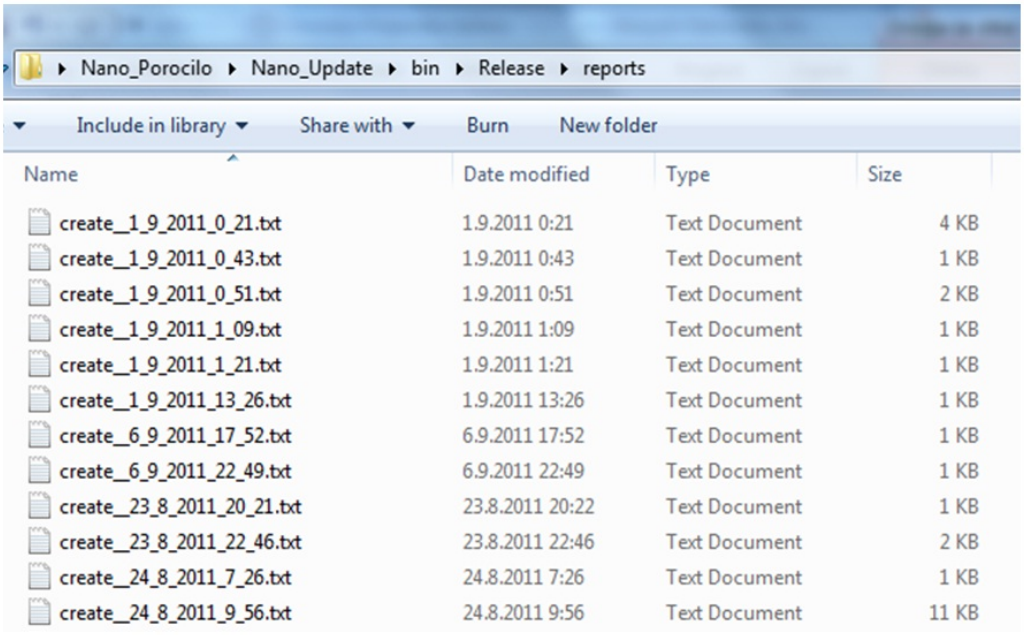


Slika A.5: Izpis poročila o neuspešno izvedeni akciji.

V programu je vključena tudi možnost izpisa poročila o uspešnem oziroma neuspešnem delovanju programa. Za vsako od štirih glavnih aktivnosti, ki so opisane na strani 38 na sliki 4.1, program javlja ali se je vsaka od njih izvedla uspešno (slika A.6) ali ne (slika A.5). Po končanem procesu se odpre novo okno, v katerem se izpiše poročilo. Ob zaprtju programa se poročilo shrani v datoteko »POROČILA«, ki se nahaja v datoteki programa. Kot ime poročila se uporabi datum in čas nastanka poročila (Slika A.7).



Slika A.6: Izpis poročila o uspešno izvedeni akciji.



Slika A.7: Mapa s poročili.

Literatura

[1] S. Alexander and R. Droms. DHCP Options and BOOTP Vendor Extensions. RFC 2132 (Draft Standard), March 1997. Updated by RFCs 3442, 3942, 4361, 4833, 5494.

[2] F. Audet and C. Jennings. Network Address Translation (NAT) Behavioral Requirements for Unicast UDP. RFC 4787 (Best Current Practice), January 2007.

[3] Pablo Brenner. A technical tutorial on the ieee 802.11 protocol. http://www.sss-mag.com/pdf/802_11tut.pdf, 1997.

[4] P. Calhoun, M. Montemurro, and D. Stanley. Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11. RFC 5416 (Proposed Standard), March 2009.

[5] Cisco. How NAT works. `http://www.cisco.com/en/US/tech/tk648/tk361/technologies\_tech\_note09186a0080094831.shtml`. Pogledano 2. 3. 2013.

[6] W.J. Croft and J. Gilmore. Bootstrap Protocol. RFC 951 (Draft Standard), September 1985. Updated by RFCs 1395, 1497, 1532, 1542, 5494.

[7] R. Droms. Dynamic Host Configuration Protocol. RFC 1531 (Proposed Standard), October 1993. Obsoleted by RFC 1541.

[8] R. Droms. Dynamic Host Configuration Protocol. RFC 2131 (Draft Standard), March 1997. Updated by RFCs 3396, 4361, 5494, 6842.

[9] K. Egevang and P. Francis. The IP Network Address Translator (NAT). RFC 1631 (Informational), May 1994. Obsoleted by RFC 3022.

[10] Tamir Gal. A secure shell (ssh) library for .net. http://www.tamirgal.com/blog/page/SharpSSH.aspx. Pogledano 2. 3. 2013.

[11] Rhys Haden. Wireless lan. http://www.rhyshaden.com/wireless.htm. Pogledano 2. 3. 2013.

[12] R. Hinden and B. Haberman. Unique Local IPv6 Unicast Addresses. RFC 4193 (Proposed Standard), October 2005.

[13] IEEE. Ieee 802 lan/man standards committee. http://www.ieee802.org/. Pogledano 2. 3. 2013.

[14] IEEE. Ieee 802.11 wireless local area networks. http://www.ieee802.org/11/. Pogledano 2. 3. 2013.

[15] Keith W. Ross James F. Kurose. *Computer Networking: a top-down approachn*. Addison-Wesley, 2009.

[16] Microsoft. How NAT works. http://technet.microsoft.com/en-us/library/cc756722(v=ws.10).aspx. Pogledano 2. 3. 2013.

[17] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. Address Allocation for Private Internets. RFC 1918 (Best Current Practice), February 1996.

[18] Republika Slovenija. Zakon o elektronskih komunikacijah, February 2007. Uradni list RS 13/2007.

[19] Wikipedia. Dynamic host configuration protocol. http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol. Pogledano 2. 3. 2013.

[20] Wikipedia. Ieee 802.11n. http://en.wikipedia.org/wiki/IEEE_802.11n-2009/. Pogledano 2. 3. 2013.