

VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
KOMPIUTERIJOS KATEDRA

Baigiamasis magistro darbas

Bevieliai kompiuteriniai tinklai Wi-Fi. Jų panaudojimas ir optimizavimas

Atliko: 2 kurso,

Kompiuterinio modeliavimo studentas

Vitalijus Romualdas Andrijauskas (parašas)

Darbo vadovas:

a. Eduardas Kutka (parašas)

Vilnius

2007

TURINYS

Anotacija	4
Summary	5
1. Įvadas	6
2. Wi-Fi sisteminės platformos pasirinkimas	7
2.1 Routerboard platforma	7
2.2 PC-based platforma	8
2.3 Platformos pasirinkimo išvados	9
3. Įrenginio komplektuojančių dalių parinkimas ir suderinimas	10
3.1 Platforma ir papildomos dalys	10
3.2 Radijo modulis	11
3.3 Antena	12
4. Įrenginio operacinė sistema	14
4.1 Operacinės sistemos parinkimas	14
4.2 Operacinės sistemos optimizavimas, papildymai ir patobulinimai	14
5. Duomenų srauto apdorojimas	16
5.1 Srauto klasifikacija su I7-filter	16
5.2 Srauto markiravimas dscp pagalba	19
5.3 Srauto nukreipimas į virtualų interfeisą IMQ	20
5.4 Srautas yra nukreipiamas į klasę, ribojamas ir prioritetizuojamas	21
6. Sistemos paleidimas	23
7. Praktinis pritaikymas	24
8. Išvados ir rekomendacijos	28
8.1 Išvados	28
8.2 Rekomendacijos	29
9. Literatūra	30

Terminų žodynas

1. **Access point (Prieigos taškas)** - įrenginys, kuris jungia bevielio ryšio įrenginius prie kito tinklo - kito bevielio tinklo, laidinio tinklo.
2. **BSSID (Basic Service Set Identifier)** - unikalus adresas, kuris identifikuoja prieigos tašką (įrenginį)
3. **BGP (Border Gateway Protocol)** – pagrindinis interneto maršrutizavimo protokolas
4. **CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)** - principinis bevielio 802.11 tinklo priėjimo prie duomenų perdavimo terpės (erdvės) metodas, kurio pagalba stengiamasi išvengti duomenų kolizijų. Tai „klausymo prieš siuntimą“ metodas. Prieš siusdami duomenys, tinklo įrenginiai tikrina ar perdavimo kanalas laisvas.
5. **Bridge** – tinklo įrenginys skaidrus tinklų apjungimas
6. **DHCP (Dynamic Host Configuration Protocol)** – taisyklių rinkinys naudojamas tinklo įrenginių tokių kaip kompiuteris, maršrutizatorius arba tinklo adapteris, kuris suteikia galimybę užklausti ir gauti IP adresą iš serverio turinčio galimu priskirti adresų sąrašą.
7. **ESSID (Extended Service Set Identifier)** - bevielio tinklo, sudaryto iš keleto bevielių tinklų, vardas (identifikatorius)
8. **NAT (Network Address Translation)** – tinklo adresų interpretavimas
9. **POE (Power Over Ethernet)** - technologija leidžianti perdavinėti elektros srovę, kartu su duomenimis, nutolusiam įrenginiui standartiniu vytos poros kabeliu Ethernet tinkle.
10. **RADIUS (Remote Authentication Dial In User Service)** - tai [AAA \(autentikacijos, autorizacijos ir apskaičiavimo\) protokolas](#) tokiom aplikacijom kaip prisijungimas prie tinklo arba IP mobilumas. Jis skirtas dirbti abeiose lokatioje ir mobilioje situacijose.
11. **RISC (Reduced Instruction Set Computer)** – tam tikra kompiuterinė architektūra
12. **Router** – tinklo maršrutizatorius
13. **SSID (Service Set Identifier)** - unikalus 32 simbolių bevielio tinklo vardas (identifikatorius). Visi priėjimo taškai ir kliento bevielio tinklo įrenginiai, norėdami prisijungti prie tam tikro bevielio tinklo turi naudoti tą patį SSID.
14. **Traffic Shaping** – kompiuterinio tinklo srautų kontrolės, optimizavimas arba srauto charakteristikos kokybės garantija.
15. **WEP** - bevieliuose tinkluose naudojamas originalus saugumo standartas, skirtas perduodamų duomenų šifravimui.

Anotacija

Darbe nagrinėjami bevieliai kompiuteriniai tinklai Wi-Fi ir jų problemos. Nustatomos kelios iš pagrindinių bevielių tinklų problemų. Radijo modulio veikimo režimas yra halfduplex, nepakankamas naudingo srauto perdavimas, srauto klasifikacijos ir prioritizacijos nebuvimas mano manymu yra pagrindinės bevielio ryšio įrenginių problemos. Bandoma ieškoti problemų sprendimo variantus. Vienas iš galimų sprendimų yra sukurti bevielio ryšio įrenginį, kuris turės šių problemų realizaciją. Ieškoma įrenginiui sukurti būtinų detalių, tokių kaip platforma, radijo modulis, antena ir kitos būtinos detalės. Pirmiausia pasirenkama PC-based platforma dėl to kad turi didesnę produktyvumą ir yra universalesnė. Vienareikšmiškai pasirenkamas 5 GHz radijo dažnis, kadangi įrenginys bus testuojamas ir naudojamas realaus tinklo infrastruktūroje Vilniaus mieste. 2,4 GHz dažnio ruožo naudojimo buvo atsisakyta dėl stipraus užterštumo.

Kaip paaiškėjo analizuojamos problemos yra susijusios viena su kita ir reikalauja kompleksinio sprendimo. Buvo nustatyta problemų prigimtis ir jos sprendimas: bendro srauto ribojimas, srautų pagal paskirtį atskyrimas ir jų ribojimas. Ieškomos standartinės ir nestandartinės problemų sprendimo priemonės, tobulinamos, tarpusavyje suderintos ir pritaikytos kuriamai sistemai. Tik realioje tinklo infrastruktūroje su realiais vartotojų generuojamais srautais pavyko nustatyti ir pašalinti trukumus.

Summary

This work is an analysis of wireless computer networks Wi-Fi and their problems. Few main wireless networks problems established. Radio module working mode is halfduplex, insufficient transfers of useful data stream, absence of stream classification and prioritisation in my opinion is a main problems of wireless devices. Attempt to search solution of the problems. One of the possible solutions is making an own wireless device witch will have realisation of this problems. Searching for necessary parts to make a device, such as platform, radio module, antenna ant other necessary parts. First of all I have chosen PC-based platform because it has a good productivity ant is more universal. Unambiguous choice was 5 GHz radio frequency, because device will be tested and used in real network infrastructure of Vilnius city. The use of 2,4 GHz radio frequency was rejected because of high radio pollution.

It emerged that analysed problems are associated one with another and needs complex solution. Was found nature of this problems and its solutions: total bandwidth shaping, separation of different streams by purpose and their shaping. Searching for standard and nonstandard means to solve such problems, modifying, matching together and adjust to created system. Only in real network infrastructure with real user generated streams was able find and eliminate limitations.

1. Įvadas

Telekomunikacijų tinklai plečiasi dideliais tempais. Dar bent dešimtį metų numatoma didelė tinklų plėtra. Tinklai klojami ryšių kabelių kanalizacijose, kolektoriuose, grunte. Kabelio tiesimas oro linijomis trumpais atstumais galimas, tačiau jo buvo atsisakyta daugumoj atvejų dėl neestetinės išvaizdos. Telekomunikacijų tinklų įrengimui butini ilgai trunkantys ir daug investicijų reikalaujantys projektavimo, derinimo bei įrengimo darbai. Įrengimo kainų augimas pasiekė rekordinius skaičius ir nenustoja augti. Šiuolaikinėje situacijoje telekomunikacijų tinklai nebespėja plėstis tokiais pat tempais kaip naujų gyvenamųjų, švietimo, verslo, pramonės, ūkinės veiklos objektų statyba. Tam kad suteikti kokybiškesnes paslaugas, įdiegti naujas paslaugas, tokias kaip VoIP ir IPTV, tuo pačių pritraukti naujus klientus senų tinklų vietovėse būtina renovuoti pasenusius „varinius“ tinklus.

Ryšių Reguliavimo Tarnybos duomenimis interneto prieigą turinčių Lietuvoje gyventojų skaičius per pastaruosius metus išaugo apie 100%. Norinčių jungtis prie internet tinklo skaičius nemažėja. Atsiranda daugiau norinčių naudotis VoIP ir IPTV paslaugomis. Todėl atsiranda problema: telekomunikacijų tinklų įrengimo terminų bei kaštų mažinimas.

2. Wi-Fi sisteminės platformos pasirinkimas

Pagrindiniai vartotojų kriterijai yra ne kažkokie ypatingi testai, o interaktyvumas kurį jis patyria surinkęs naršyklėje pageidaujamą adresą ir paspaudęs mygtuką ir savo monitoriaus ekrane jis nori matyti kad jo užklausa jau vykdoma. Todėl didesnę dėmesį reikia atkreipti į interaktyvias paslaugas ir pagerinti jų veikimą norint pasiekti gerų rezultatų.

Yra du galimi Wi-Fi sprendimai: PC-based arba routerboard platforma. Prieš pasirenkant vieną iš dviejų platformų reikia tiksliai žinoti kokie yra šių platformų skirtumai, privalumai ir trukumai.

2.1 Routerboard platforma

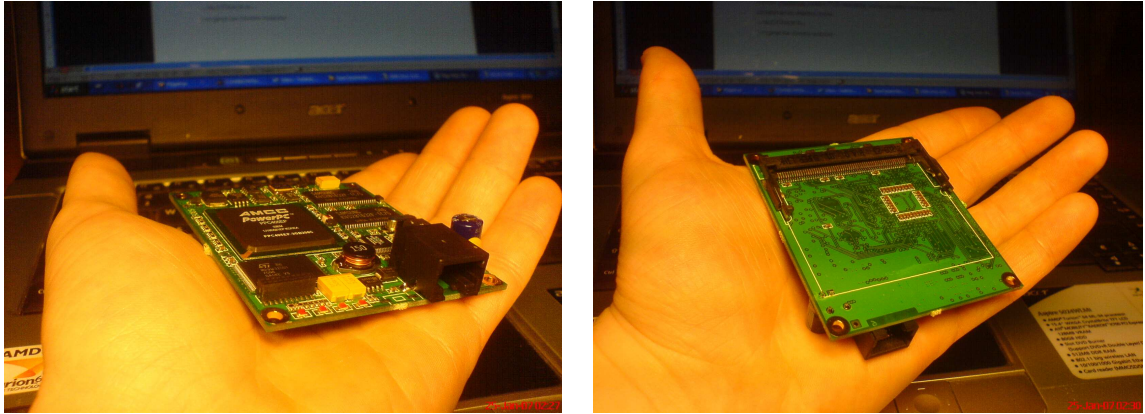
Privalumai:

- Akivaizdus skirtumas tai kad platformos išmatavimai yra tikrai labai maži. Šiai dienai mažiausios platformos kurią pavyko įsigyti atitinkančios projekto reikalavimams išmatavimai yra: 100x60x20 mm (PxIxA). Platformą galima įmontuoti į lauko anteną, užhermetizuoti ir sistema tampa pilnai lauko montavimo įrenginiu
- Platforma užsimaitina nuo 12-20V 0,5-1,5A elektros. Maitinimo blokas yra tai pat mažų išmatavimų 20x60x35 mm. Maitinimo bloko gali išvis nebūti, nes platformą galima užmaitinti per PoE (Power over Ethernet). Šis sprendimas labai patogus padeda sutaupyti daug laiko ir medžiagų
- Nereikalauja aktyvaus aušinimo

Trukumai:

- Mažas sistemos produktyvumas palyginus su PC-based sistemom
- Nesaugu palikti visos sistemos lauke
- Kadangi platforma turi tik viena minipci jungtį sistemos papildymas dar vienu radijo moduliu negalimas
- Dėl mažos elektros srovės nepavyks panaudoti galingo radijo modulio kad padidinti radijo spinduliavimą
- Sistema negali būti papildyta pastoviaja ir operatyviaja atmintimi
- Sistema negali būti papildyta tinklo interfeisu

- Labai didelė problema dėl mažos detalės gedimo, bet kokios detalės gedimo atveju visas įrenginys sugenda, kadangi negalima pakeisti operatyvios ir pastovios atminties, procesoriaus, tinklo interfeiso ir bet kokios kitos integruotos detalės



Pav. 1 Routerboard sistema

2.2 PC-based platforma

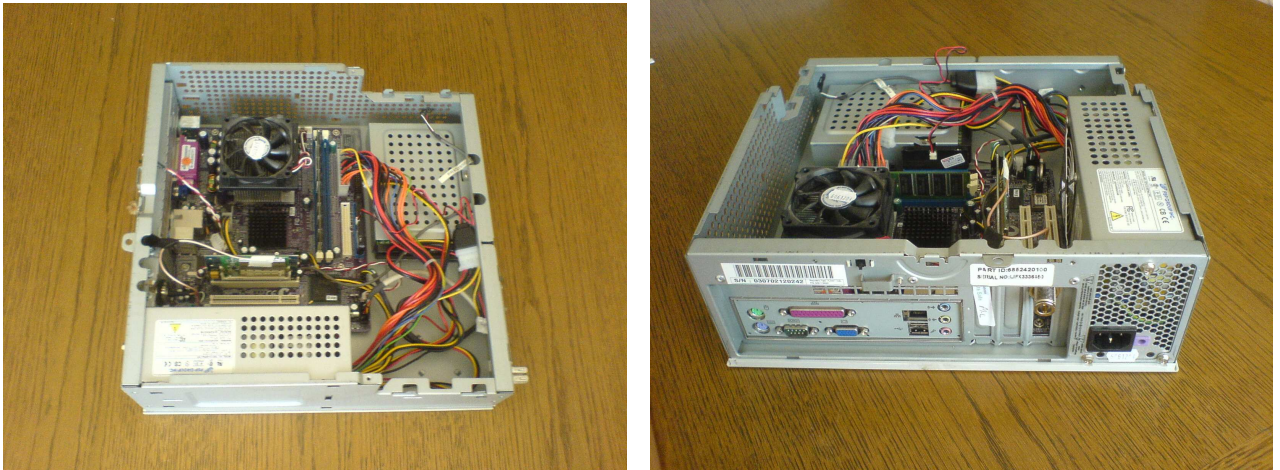
Privalumai:

- Kadangi platforma turi stalinio kompiuterio galingą procesorių labai padidėja jos produktyvumas, galima vykdyti papildomas užduotis tokias kaip DNS, BGP, VPN, cache, proxy serveris (squid) ir kitas, tai leidžia greičiau įvykdyti užklausas ir sutaupyti srautą iki nutolusių resursų
- Sistemoje gali būti sumontuotas ne vienas galingas radijo modulis (400mW), galima didinti modulių galingumus ir pasiekti labai didelį radijo spinduliavimą, tokias sistemas galima naudoti tolimų taškų apjungimui (net iki 100Km)
- Sistemą su tokia platforma labai universali, ją galima papildyti bet kokia reikiama detale: tinklo plokštė, operatyvioji ir ilgalaikė atmintis ir t.t.
- Sistemoje gali būti pakeista bet kokia detalė, netgi pagrindinė plokštė, todėl

Trūkumai:

- Platformos dideli išmatavimai sukelia papildomų problemų dėl įrangos patalpinimo vietos suradimo
- Sistema su tokia platforma yra sudėtingesnė maitinimo atžvilgiu. 220V elektros maitinimas sudaro papildomų išlaidų, ilgesnėms atstumams reikia tiesti galingus elektros kabelius, reikia papildomų elektros automatinių jungiklių ir kitų saugumo priemonių

- Dėl platformos didelio galingumo yra būtinas aktyvus aušinimas
- Dėl išvardintų priežasčių sistemą negali būti montuojama lauke
- Išorinės antenos montuojamos lauke o sistema patalpoje, reikia ilgesnių kabelių jungiančių anteną ir radijo modulį, dėl to sumažėja radijo signalo stiprumas



Pav. 2 Surinkta PC-based sistema

2.3 Platformos pasirinkimo išvados

Pasirinkome PC-based sistemą, nes ji yra labiau produktyvi ir yra universali. Ateityje sistemą galima bus papildyti keliais standartiniais arba galingesniais radijo moduliais ir įjungti kelis papildomus servisus.

Iš esmės didelio skirtumo nėra kokią platformą turės užbaigta ir veikianti sistema.

Problemos sprendimui platforma mums nėra svarbi, nes ir prie routerboard ir prie PC-based sistemos galima prisiderinti ir perkompiliuoti kodą. Opensource sprendimą galima pritaikyti vienai ir kitai sistemai.

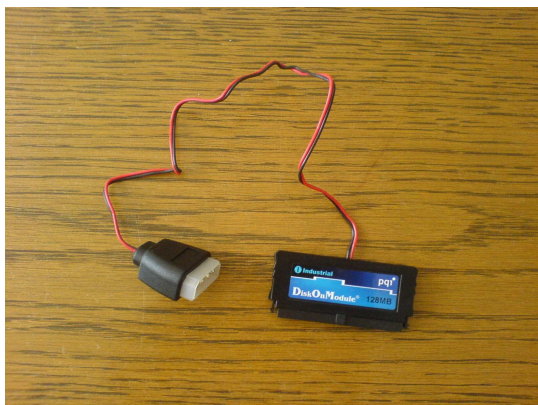
3. Įrenginio komplektuojančių dalių parinkimas ir suderinimas

3.1 Platforma ir papildomos dalys

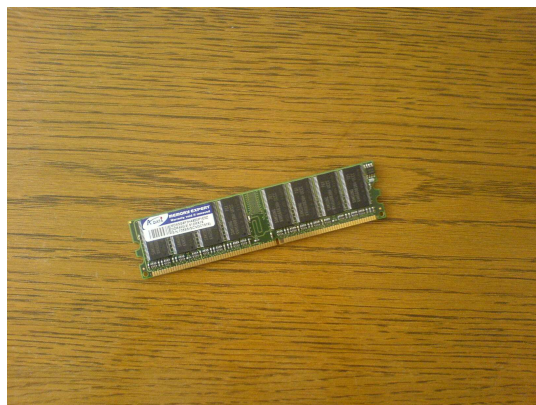
Pasirinkta PC-based platforma pagrinde dėl didesnio produktyvumo ir visos sistemos universalumo.

Platformos komplektuojančios dalys, charakteristika:

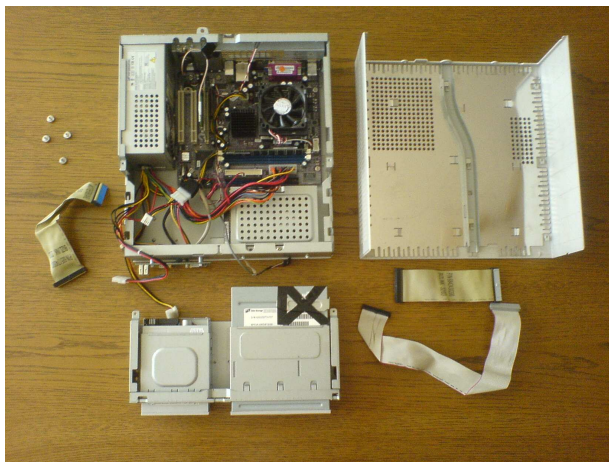
- RAM 512MB;
- CPU Intel 2,4GHz;
- IDEflash 256MB (ilgalaikė atmintis);
- 3xPCI jungtys;
- 1x10/100 Mbps Intel tinklo adapteris
- Maitinimo blokas 250W (ATX)
- Korpusas 350x350x90 mm (miniATX)
- ...



Pav. 3 IDE flash (ilgalaikė atmintis)



Pav. 4 RAM modulis (operatyvioji atmintis)

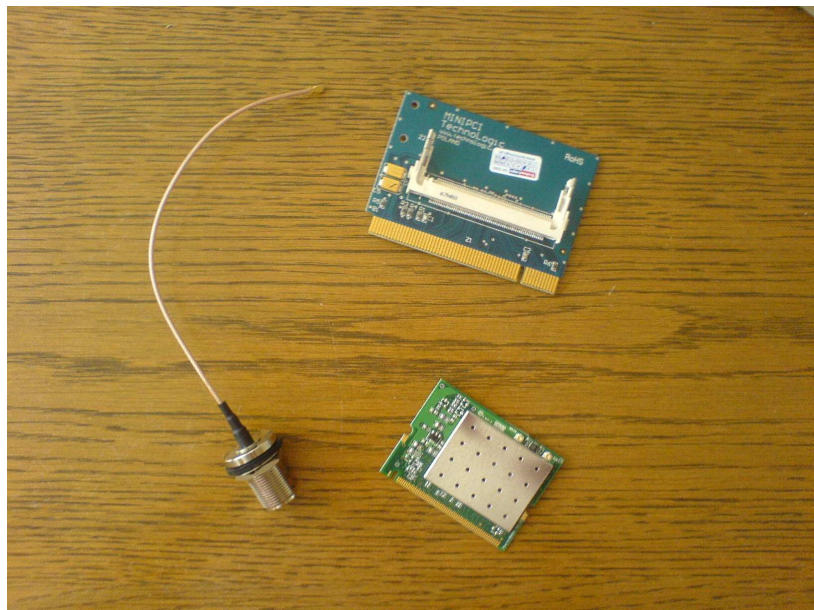


Pav. 5 PC-based platforma

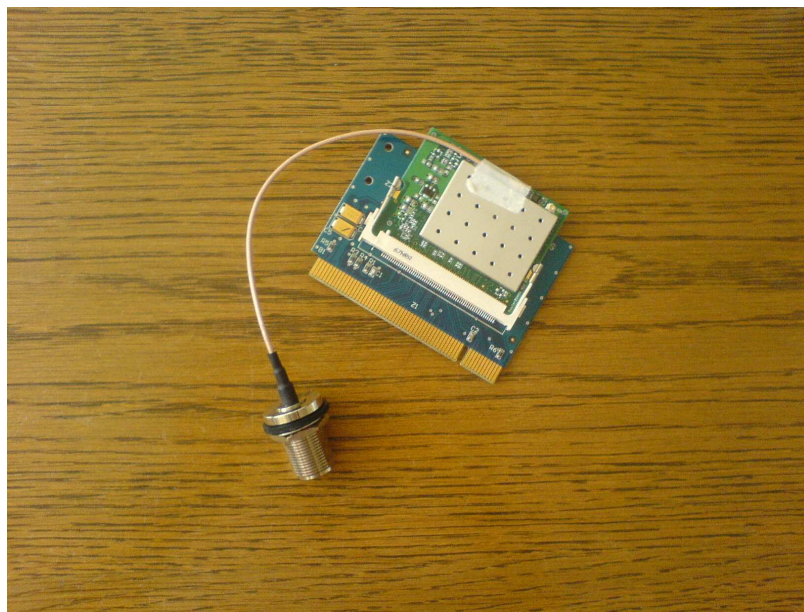
Intel procesorinė platforma pasirinkta dėl daugybės detalėms pritaikytu tvarkyklių, kurių gausa didesnė už AMD platformoms skirtas tvarkykles. Tai pat tvarkyklės geriau pritaikytos ir su jomis pasiekiamas didesnis produktyvumas.

3.2 Radijo modulis

Radijo modulio ilgai ieškoti nereikėjo, buvo užsakytas labiausiai užsirekomendavęs ir visų „pripažintas“ Atheros 5213 CM9 serijos radijo modulis palaikantis 802.11a/b/g standartus, kainavęs tik 39\$. Kartu su juo užsakytas 3\$ kainuojantis RG174 aukšto dažnio kabelis 15 cm ilgio su jungtimis, kurio pagal apskaičiavimus turi užtekti. Šio kabelio parametrai: vidinis laidininkas 7x0,16, dielektrikas PE 1,5mm, ekranas Cu+Sn, apvalkalas PVC 2,8mm. Kabelis nemažo slopinimo, todėl kuo trumpesnis tuo geriau, signalo atžvilgiu.



Pav. 6 Radijo modulis, pci perėjimas ir patchkabelis



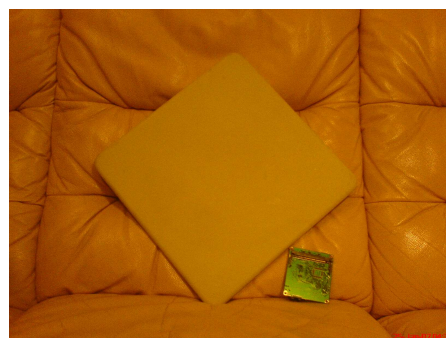
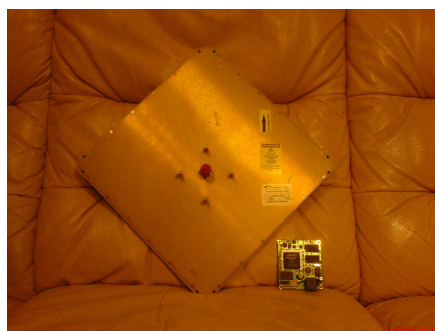
Pav. 7 Radijo modulis, pci perėjimas ir patchkabelis sujungti

Atheros radijo moduliai turi labai daug tvarkyklių opensource sistemoms, turi dideles galimybes. Šių modulių naudojimas padėjo išgauti daugiau tikslumo, produktyvumo, žemesniam lygmeny kreiptis prie sistemos, tiksliau susiderinti su radijo antena ir su visa sistema.

3.3 Antena

Pradiniame projekte radijo transmisija turėtų būti apie 5 km ir optimaliai parinkta antena MA-WA58-1X 5GHz Broadband Subscriber Antenna, kurios parametrai tokie:

- Dažnių ruožas 5,15-5,875 GHz
- Jautrumas 23 dBi min.
- Poliarizacija linijinė arba linijinė vertikali
- Spinduliavimo kampas 10,5 laipsnių



Pav. 8 Antena Mars 23dbi

Daromas projektas buvo pakoreguotas ir vienas iš radijo taškų buvo perkeltas. Dabar radijo transmisijos ilgis 1,5 km, todėl buvo pasirinktas kitas antenos modelis su tokiais parametrais:

- Dažnių ruožas 5,25-6,100 GHz
- Jautrumas 19 dBi min.
- Poliarizacija linijinė arba linijinė vertikali
- Spinduliavimo kampas 20,0 laipsnių



Pav. 9 Antena 19dbi

Praktika rodo kad 1,5 km atstumu keičiant anteną iš pirmos į antrą kokybiniai parametrai suprojektuotos radijo transmisijos nepablogės. Su silpnesne antena galima pasiekti net geresnius rezultatus, nes kai antena turi daugiau dbi, ji jautriai reaguoja į triukšmus kitų tokiu pat dažniu veikiančių antenų. Tokia tikimybė miesto sąlygom yra labai didelė, todėl ir buvo pakeista antena.

5GHz dažnio signalas labiau silpsta nei 2GHz, todėl jam reikia geresnio laidininko. Kad išvengtų signalo praradimo, reiktu kuo trumpesnio jungiamojo kabelio su mažesniu slopinimu. Antenai pajungti prie įrenginio reikia g400 5 metrų kabelio su SMA jungtimis galuose. Negalima stipriai perlenkti kabelio, todėl iš įrenginio pajungimo pusės naudosime SMA 90 laipsnių kampinį sujungimą o iš antenos pusės įprastą SMA jungtį.



Pav. 10 Antenos kabelis (90 laipsnių jungtis)



Pav. 11 Antenos kabelis (tiesioji jungtis)

4. Įrenginio operacinė sistema

4.1 Operacinės sistemos parinkimas

Programinės įrangos skeletas pradėtas kurti nuo bazinės sistemos parinkimo. Buvo išanalizuota open source operacinių sistemų įvairovė, tokių kaip FreeBSD, OpenBSD, Linux ir įvairių jų versijų. BSD operacinės sistemos daugiau tinka serveriams. Embedded produktams kurti dažniausiai naudojamos Linux operacinės sistemos. Atsižvelgiant į keliamus reikalavimus ir numatomą uždavinio sprendimo būdą pasirinkimas atiteko Linux Slackware operacinei sistemai.

Pasirinkimo priežastis, tai kad Slackware viena iš seniausių distribucijų GNU/Linux. Ji truputi skiriasi nuo kitų populiarių distribucijų (tokių kaip Debian, Gentoo, Mandrake, Fedora, SuSE) tuo, kad Slackware buvo ir lieka „pačiu Unix‘iausiu“ – stabilumas ir saugumas, taip pat diegimo, palaikymo ir naudojimo paprastumas.

4.2 Operacinės sistemos optimizavimas, papildymai ir patobulinimai

Naudojau perdarytus Linux Slackware ir dalinai Gentoo, darydamas testus, daug kartų juos perkompiliuodavau. Eksperimentuodamas su keliais branduoliais ir įvairiu saugumo, produktyvumo patchų rinkiniu mano pasirinkimas apsisusto ties 2.6.17 branduolio. Mano manymu šiam momentui šis branduolys maksimaliai atitinka visiems suformuluotos užduoties reikalavimams: visų įrenginio dalių palaikymas, stabilumas ir eilės būtinų patchų palaikymas:

- grsecurity <http://www.grsecurity.net> (tai pagrinde su saugumu susijęs patchas)
- patch-o-matic <http://www.netfilter.org> (tai maršrutizavimo, pažangaus tinklo ypatumai)
- imq <http://www.linuximq.net> (virtualūs interfeisai)
- l7-filter <http://www.l7-filter.sourceforge.net> (application layer packet classifier)
- nf-hipac <http://www.hi-pac.org> (didelio produktyvumo ugniasienė)
- esfq <http://www.fatooh.org/esfq-2.6/>
- ir kiti dėl papildomų dalių ir programų suderinamumų (papildomų šifravimo algoritmų palaikymas, įvairių šifravimo tunelių naudojimui, tokių kaip pptp, ipsec, ...)

Visą sistemos tobulinimo laiką naudoju internetą informacijos paieškai. Vienas iš naudingiausių šaltinių buvo: <http://www.lartc.org> (mailing list). LARTC bendruomenės dėka turėjau galimybę pabendrauti ir spręsti savo problemas tiesiogiai su žmonėmis kuriančiais programinę įrangą maršrutizavimo ir srauto kontrolės srityje. Čia gavau daug naudingos informacijos.

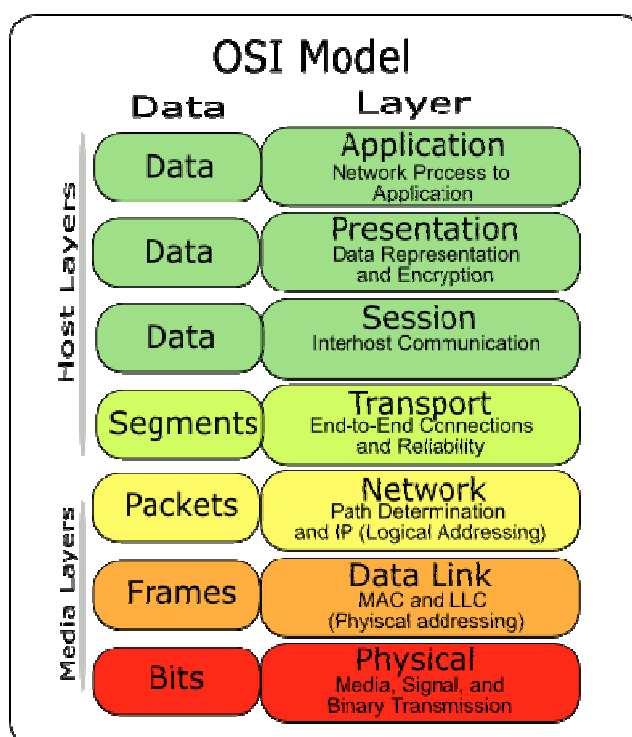
Gentoo bendruomenė <http://www.gentoo.org>. Yra pakankamai didelė bendruomenė orientuota ne tik į Gentoo Linux distribuciją bet iš esmės apčiuopia Linux'ą. Mailing listas tai visada labai „šviežios“ naujienos.

HTB HOME tai pat daug naudingos informacijos aktualia tema.

5. Duomenų srauto apdorojimas

5.1 Srauto klasifikacija su I7-filter

Srauto klasifikacija su I7-filter Srauto klasifikavimui buvo pasirinktas L7-filter todėl kad leidžia su minimaliu resursų išnaudojimu ir maksimaliai teisingai nustatyti srauto (sesijų) tipą. L7-filter – klasifikatorius kuris identifikuoja paketus aplikacijų lygmenyje (pagal OSI modelį septintas lygmuo).



Schema 1 OSI modelis






OSI Modelis – Atvirų sistemų apjungimo modelis (Open Systems Interconnect Basic Reference Model - OSI Reference Model arba sutrumpintai OSI Model)

L7-filter gali klasifikuoti srautą kaip Kazaa, HTTP, Bittorrent, FTP, eDonkey, VoIP, ir t.t. nepriklausomai nuo porto. Jis papildo egzistuojančius (pasenusius) klasifikatorius kurie ieško atitiktens pagal IP adresą, porto numerį ir t. t.





Šablonai skiriasi paskirtimi, kuri protokolą jie atpažįsta. Šablono kokybei nusakyti reikia kelių dalykų ir nepakanka bendrais bruožais apibudinti kaip gerai jis veikia. Šitie dalykai yra (1) kaip gerai atpažįstamas protokolai (2) kaip ilgai srautas pagal šabloną buvo testuojamas (3) keliose

situacijose šablonas buvo testuojamas ir (4) kokia dalis identifikuojamo srauto buvo identifikuota teisingai.








































Kokybė:













-  Puikiai: Veikia.
-  Gerai: Veikia kiek mums žinoma.
-  Na: Atrodo veikia.
-  Pakrašty: galbūt veikia, o gal ir ne.
-  Blogai: Atrodo neveikia.

Greitis:

-  Labai greitai: 0–0.3 sekundės.
-  greitai: 0.3–1.5 sekundės.
-  Ne per greičiausiai: 1.5–15 sekundžių.
-  Lėtai: >15 sekundžių.

L7-filter panaudotų šablonų ir jų techninės charakteristikos lentelė:

Šablonas	Greitis	Kokybė	Tipas	Protokolas
ventrilo				Ventrilo - VoIP – http://ventrilo.com
teamspeak				TeamSpeak – VoIP aplikacija - http://gotteamspeak.com
skypeout				Skype to phone - UDP balso skambutis (iš programos į POTS telefoną)- http://skype.com
skypetoskype				Skype to Skype - UDP balso skambutis (iš programos į programą) - http://skype.com
ssh				SSH – Secure Shell
telnet				Telnet – Neapsaugotas nutolęs prisijungimas (Insecure remote login) - RFC 854
dhcp				DHCP - Dynamic Host Configuration Protocol - RFC 1541
applejuice				Apple Juice - P2P apsikeitimas bylomis – http://www.applejuicenet.de
bittorrent				Bittorrent - P2P apsikeitimas bylomis / publikacijos priemonė- http://www.bittorrent.com
soulseek				Soulseek - P2P apsikeitimas bylomis – http://slsknet.org
mute				MUTE - P2P apsikeitimas bylomis - http://mute-net.sourceforge.net
napster				Napster - P2P apsikeitimas bylomis
imesh				iMesh - the native protocol of iMesh, a P2P aplikacijos - http://imesh.com

gnutella				Gnutella - P2P apsikeitimas bylomis
directconnect				Direct Connect – P2P apsikeitimas bylomis - http://www.neo-modus.com
fasttrack				FastTrack - P2P apsikeitimas bylomis (Kazaa, Morpheus, iMesh, Grokster, ir t.t.)
edonkey				eDonkey2000 – P2P apsikeitimas bylomis - http://edonkey2000.com ir kiti

Lentelė 1 L7-filter

Kokias klases naudosime ir kurioms iš jų suteiksime didžiausią prioritetą? Pagrindė toms srauto klasėms, kurių perdavimas reikalauja minimalaus vėlinimo. Pavyzdžiui video ir audio srautas (mūsų atveju audio – VoIP srautas) arba interaktyvus (SSH, telnet) srautas, kuris pagal savo prigimtį reikalauja momentinio srauto padidėjimo ir neturi didelės įtakos „kaimyniniam“ srautui.

Panaudotų šablonų pavyzdžiai:

Bittorrent

```
^(\\x13bittorrent protocol|azver\\x01$|get /scrape\\?info_hash=)|d1:ad2:id20:|\\x08'7P\\)[RP]
```

```
iptables -t mangle -A PREROUTING -m layer7 --l7proto bittorrent -j DSCP --set-dscp 0x01
```

VoIP

```
^\\xf4\\xbe\\x03.*teamspeak
```

```
iptables -t mangle -A PREROUTING -m layer7 --l7proto voip -j DSCP --set-dscp 0x02
```

SMTP

```
^220[\\x09-\\x0d -~]* (e?smtp|simple mail)
```

```
userspace pattern=^220[\\x09-\\x0d -~]* (E?SMTP|[Ss]imple [Mm]ail)
```

```
userspace flags=REG_NOSUB REG_EXTENDED
```

```
iptables -t mangle -A PREROUTING -m layer7 --l7proto smtp -j DSCP --set-dscp 0x03
```

ir kiti

Populiarus triukas kai norima parodyti komandos *ping* gerą atsakymo laiką netgi kai srautas pilnai užsikimšęs transmisiją – ICMP paketų prioriteto didinimas (suprantama, kad iš techninės pusės tai tikrai nepagerins sujungimo).

5.2 Srauto markiravimas DSCP pagalba

DSCP (Differentiated Services Code Point - Skirtingo Serviso Žymė) – tai laukas IP paketų antraštėje (header) skirtas paketų klasifikavimui.

Maršrutizatoriai tinklo pakrašty klasifikuoja paketus ir markiruoja juos pagal IP pirmumą arba DSCP reikšmę Diffserv (skirtingo serviso) tinkluose. Kiti įrenginiai tinklo centruose kurie palaiko Diffserv naudoja DSCP reikšmę IP antraštėje (header) tam kad pasirinkti tolimesnį elgesį su paketu ir pritaikyti tinkamą QoS veiksmą.

TOS paskirtis yra labai panaši, tačiau nėra plačiai naudojama. Dauguma senesnės įrangos nekreipia dėmesio į DSCP ir ToS reikšmes (nes neturi palaikymo). Šiuolaikiniai didesnio pralaidumo komutatoriai dažniausiai turi palaikymą, bet praktikoje tai dar nėra plačiai naudojama..

Schema žemiau parodo skirtumą tarp ToS baido apibrėžia RFC791 ir DiffServ lauko.

ToS Baitas (ToS Bite)

P2	P1	P0	T2	T1	T0	CU1	CU0
-----------	-----------	-----------	-----------	-----------	-----------	------------	------------

- IP pirmenybė — tris bitai (nuo P2 iki P0)
- Uždelsimas, Pralaidumas ir Patikimumas — tris bitai (nuo T2 iki T0)
- CU (Currently Unused - Nenaudojami) — du bitai (CU1-CU0)

DiffServ Laukas (DiffServ Field)

DS5	DS4	DS3	DS2	DS1	DS0	ECN	ECN
------------	------------	------------	------------	------------	------------	------------	------------

- DSCP — šeši bitai (nuo DS5 iki DS0)
- ECN — du bitai

6 bitai, tai reiškia kad gali būti pakankamai daug skirtingų reikšmių (64 variantai) pagal kuriuos gali būti prioritetuojamas srautas. DSCP dirba su žemesnio lygio įrenginiais, dauguma naujų komutatorių jau palaiko DSCP ir gali prioritetuoti srautą pagal DSCP reikšmes, kurios dažniausiai nustatomos tinklo centriniuose (core) maršrutizatoriuose. Tokia praktika yra labai naudinga, nes per visą paketų transmisiją kiti tinklo įrenginiai kurie palaiko DSCP gali prioritetuoti srautą pagal DSCP lauko reikšmes ir taupyti savo produktyvumą, gerinti serviso kokybę bei didinti duomenų srautus

Sukurta sistema turi DSCP palaikymą ir gali prioritetuoti srautą pagal šias reikšmes, tai pat sistema klasifikuoja srautą ir gali suteikti savo dscp reikšmes.

5.3 Srauto nukreipimas į virtualų interfeisą IMQ

Kam naudojamas IMQ?

IMQ įrenginys turi du įprastus panaudojimus::

- Įeinantis srauto apdorojimas (**Ingress shaping**) :
Linux sistemose galimas tik įeinančio srauto apdorojimas (išskyrus įeinančios eilės kuri gali atlikti tik greičio ribojimą). IMQ leidžia panaudoti išeinantį qdiscs tikram įeinančio srauto apdorojimui pasiekti.
- Srauto apdorojimas sudėtiniuose interfeisuose (**Shaping over multiple interfaces**) :
Qdiscs surišamas su įrenginiu. Dėl to vienas qdiscs gali valdyti srautą tik to interfeiso prie kurio jis yra pririštas. Kartais norima turėti globalius apribojimus per kelis interfeisus. Su IMQ galima naudoti iptables tiksliai apibrėžti kokius paketus mato qdiscs, tuomet globalūs apribojimai gali būti naudojami.

Uždavinio sprendimas reikalauja įdiegti virtualius interfeisus. Tai būtina daryti, nes fiziniu interfeisų gali būti daug, o valdyti srautą reikia vienoje vietoje tam kad pasiekti taip vadinamą „overbookingą“. Mūsų atveju buvo pasirinktas IMQ. Jau daugeli metų sėkmingai naudojamas Linux sprendimuose. Suteikia srauto valdymui papildomo lankstumo. Tai pat Wi-Fi įrenginių ypatumas, tai kad jie dirba halfduplex režime verčia naudoti IMQ.

Tam kad IMQ tvarkingai veiktų reikia papildyti kodu branduolį ir iptables, perkompiliuoti ir daryti testus.

Mūsų atveju visą srautą turėsime nukreipti į vieną IMQ dėl to kad įrenginys dirba halfduplex režimu:

```
iptables -t mangle -L POSTROUTING -j IMQ --to-dev 0
```

Kiti pavyzdžiai:

```
iptables -t mangle -A PREROUTING -i $wireless1 -j MARK --set-mark 0x1
```

PIC: [mag_iptables_veikimo_schema.jpg](#)

Kadangi bevielis įrenginys tai siaura vieta (bottleneck) iškarto viską nukreipinėjame į IMQ

```
iptables -t mangle -A PREROUTING -i $wireless1 -j IMQ --to-dev 0
```

\$wireless1 tai įrenginio radijo interfeisas

iptables -t mangle -A POSTROUTING -o \$wireless1 -j IMQ --todev 0

Tokiu atveju visas srautas patenka į IMQ

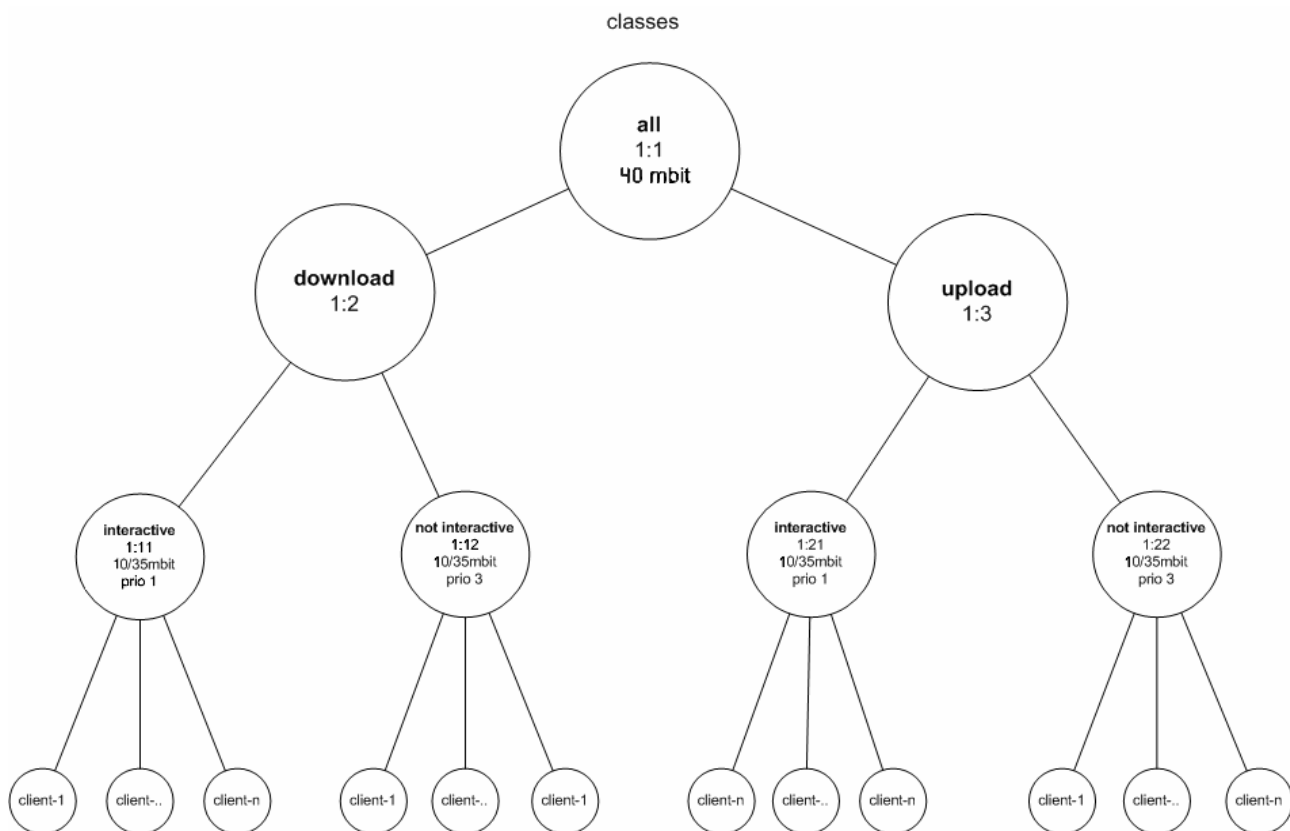
5.4 Srautas yra nukreipiamas į klases, ribojamas ir prioritetizuojamas

Šiame etape naudojame Netfilter palaikomą iptables projektą

Iptables – komandinės eilutės programa skirta Linux 2.4.x ir 2.6.x IPv4 paketų filtro taisyklių rinkiniui (packet filter rulset) sudaryti ir valdyti.

Iptables skirtas IP paketų taisyklių lentelės sudarymui, palaikymui ir inspektavimui Linux kernelyje. Gali būti apibrėžtos kelios lentelės. Kiekviena lentelė saugo įdiegtų grandinių numerį ir tai pat gali turėti vartotojo apibrėžtas grandines.

Kiekviena grandinė tai sąrašas taisyklių, kuri gali atitikti eilei paketų. Kiekviena taisyklė nusako ką daryti su paketu kuris atitinka. Tai vadinama „taikiniu“, kuris gali būti šuolis į vartotojo apibrėžtą grandinę toje pačioje lentelėje. Filtravimas vyksta pagal paketų DSCP reikšmes, paketas nukreipiamas į tam tikras HTB (Hierarchical Token Bucket) klases, ten jis ribojamas ir prioritetizuojamas. Sistemos HTB klasių medis atrodo taip:



Schema 2 Sistemos HTB klasių medis

Filtrų yra tiek kiek yra klientų kart keturi.

Kadangi klientų nėra daug mes galime sau leisti linijinę filtrų paiešką. Bet kai klientų skaičius yra didelis (≥ 100) reikės naudoti paieškos algoritmą (pvz. HASH), nes linijinė kiekvieno paketo kelio paieška išnaudoja sistemos resursus.

Jeigu darytume prioritizavimą tikrai interaktyviam srautui (neribotume kiekvieno kliento) galima būtų daryti tik vieną filtrą prioritizuotam srautui. Reiktu sukurti tik dvi klases, į vieną eitu prioritizuotas srautas ir į kitą klasę „default“ visas likęs srautas.

6. Sistemos paleidimas

Kraunamės iš bet kokios Linux sistemos (dažniausiai LiveCD) ir paruošiamė sekančius diskų skyrius (sukuriame ir formatuojame) distribucijos paleidimui. Pagal nutylėjimą PC-based sistemoje į /etc/fstab ir /etc/lilo.conf nurodyta:

```
/dev/hda1 – swap (swap 256Mb)
/dev/hda2 (boot flag) - /boot (mkfs.ext264Mb)
/dev/hda3 - /var/log (reiserfs) (256Mb)
/dev/hda4 - / (reiserfs all space left)
```

Pagal aukščiau nurodytą lentelę montuojame skyrius įrengimo direktorijoje, pavyzdžiui:

```
mkdir /mnt/install
mount /dev/hda4 /mnt/install/
cd /mnt/install
mkdir boot var var/log
mount /dev/hda2 /mnt/install/boot
mount /dev/hda3 /mnt/install/var/log
```

su scp (secure copy) pagalba arba kitaip kopijuojame į /mnt/install sistemos atvaizdą /image.tar.bz2 ir jį išpakuojame komanda:

```
tar xvjpf image.tar.bz2
```

po išpakavimo montuojame sistemą /proc ir naudodami komandą chroot diegiame „kroviklį“ LiLo į pakrovimo disko MBR:

```
mount -t proc none /mnt/install/proc
chroot /mnt/install /bin/bash
lilo -v
```

išmontuojame skyrius ir perkrauname sistemą, šį kartą pasikrauname iš skyriaus /boot

7. Praktinis pritaikymas

Sistema turi daugybę galimų pritaikymų realioje infrastruktūroje kurie gali būti labai naudingi. Paminėsiu keletą pritaikymo variantų ir aprašysiu jų veikimą.

- **DHCP relay (friendly DHCP server)**

Dažnai tinklo įrenginiai naudoja ne statinę IP konfigūraciją, o automatinį IP adresacijos priskyrimą. Tokiu atveju naudojamas DHCP serveris. Kai tinklo įrenginys, kurio adresacija yra ne statinė, o automatinio priskyrimo, siunčia broadcast IP adresacijos užklausimą visiems tinklo įrenginiams, DHCP serveris, esantis tam pačiam (dažniausiai) potinklyje, atsako ir siunčia IP nustatymus įrenginiui, laukiančiam atsakymo. Taip daroma dideliuose tinkluose, kai norima palengvinti tinklo administravimą. Naudojant automatinį IP adresacijos priskyrimą, pasitaiko ganėtinai didelė problema – svetimo DHCP serverio atsiradimas.

Sukurtas įrenginys turi originalų šios problemos sprendimą.

Su L7-filter pagalba DHCP paketai yra identifikuojami, toliau yra tikrinamos sąlygos siuntėjo IP adresas, mac adresas, ir t.t. Jeigu paketai neatitinka nustatytų sąlygų, jie yra blokuojami. Taip sprendžiama svetimo DHCP serverio problema.

- **Virusų plėtimo tinkle blokavimas**

Vienas iš labai naudingų ir aktualių pritaikymų yra virusų blokavimas. Analogiškai kaip ir su DHCP paketų identifikavimu L7-filter gali klasifikuoti virusus. Toliau įrenginys gali ne tik blokuoti virusų plėtimą, bet ir informuoti apie tai virusuotą vartotoją (kad yra virusuotas, kokių virusu, kaip jį išvalyti), nukreipiant tą vartotoją į jam sugeneruotą puslapį, kuris gali būti įrenginio WWW serveryje. Arba vartotojui gali būti tiesiog užblokuota tinklo prieiga.

Šis sistemos pritaikymas realizuojamas su PC-based platforma, nes reikalaujama labai didelių resursų, norint išsaugoti mažą vėlinimą ir gerą paslaugos kokybę.

Pateiksiu du schematiškus pavyzdžius:

- 1) Bridge
- 2) Router

Kaip jau minėjau sistema yra įdiegta realioje infrastruktūroje. Schemoje „Bridge“ vaizduojama, kur įdiegtas suprojektuotas įrenginys (bridge). Suprojektuotas bridge – tiltas, susideda

iš vienuodų įrenginių, kurie skaidriai perduoda duomenis iš vieno vielinio tinklo į kitą per radijo transmisiją bei gali klasifikuoti persiunčiamus duomenis ir atlikti su jais atitinkamus veiksmus:

- blokuoti nepageidautiną srautą

Virusai plinta tinkle, užkrečia kitus tinklo vartotojus ir apkrauna tinklą. Neakceptuoti vartotojai blokuojami nuo interneto prieigos taip tausojamas interneto bendras kanalas ir užtikrinamas didesnis saugumas. Broadcast paketai siunčiami kiekvienam tinklo vartotojui tai pat generuoja papildomą srautą. Visos išvardintos priežastis sudaro papildomą apkrovą ne tik vielinėje tinklo dalyje, bet ir bevielėje transmisijoje, kas yra labai skaudu, ypač kai radijo transmisijos ir taip trūksta. Įrenginys nepraleidžia išvardinto srauto iš vienos tinklo dalies į kitą per radijo transmisiją.

- prioritetizuoti siunčiamus duomenis

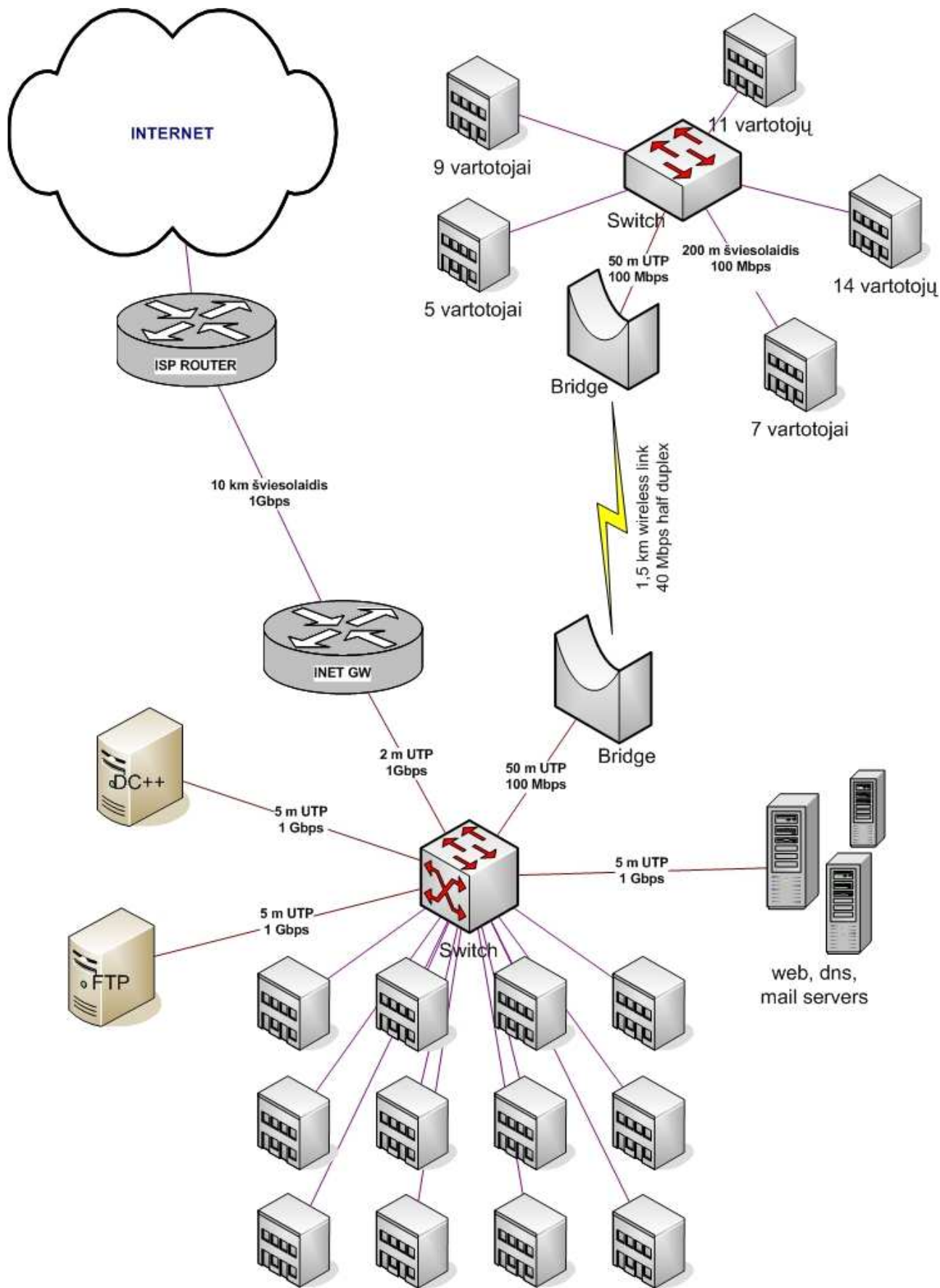
Įrenginys prioritetizuoja srautą (Telnet, SSH, VoIP ir kiti) einanti per radijo transmisiją ir taip pasiekiamas interaktyvumas.

Įrenginys gali atlikti maršrutizatoriaus (Router) veiksmus, jo tinklo interfeisai palaiko VLAN funkciją. Sudėtingesnė, tuo pačiu naudingesnė (produktyvesnė, saugesnė) schema, kaip gali būti naudojamas įrenginys pavaizduota „Router“ schemeje.

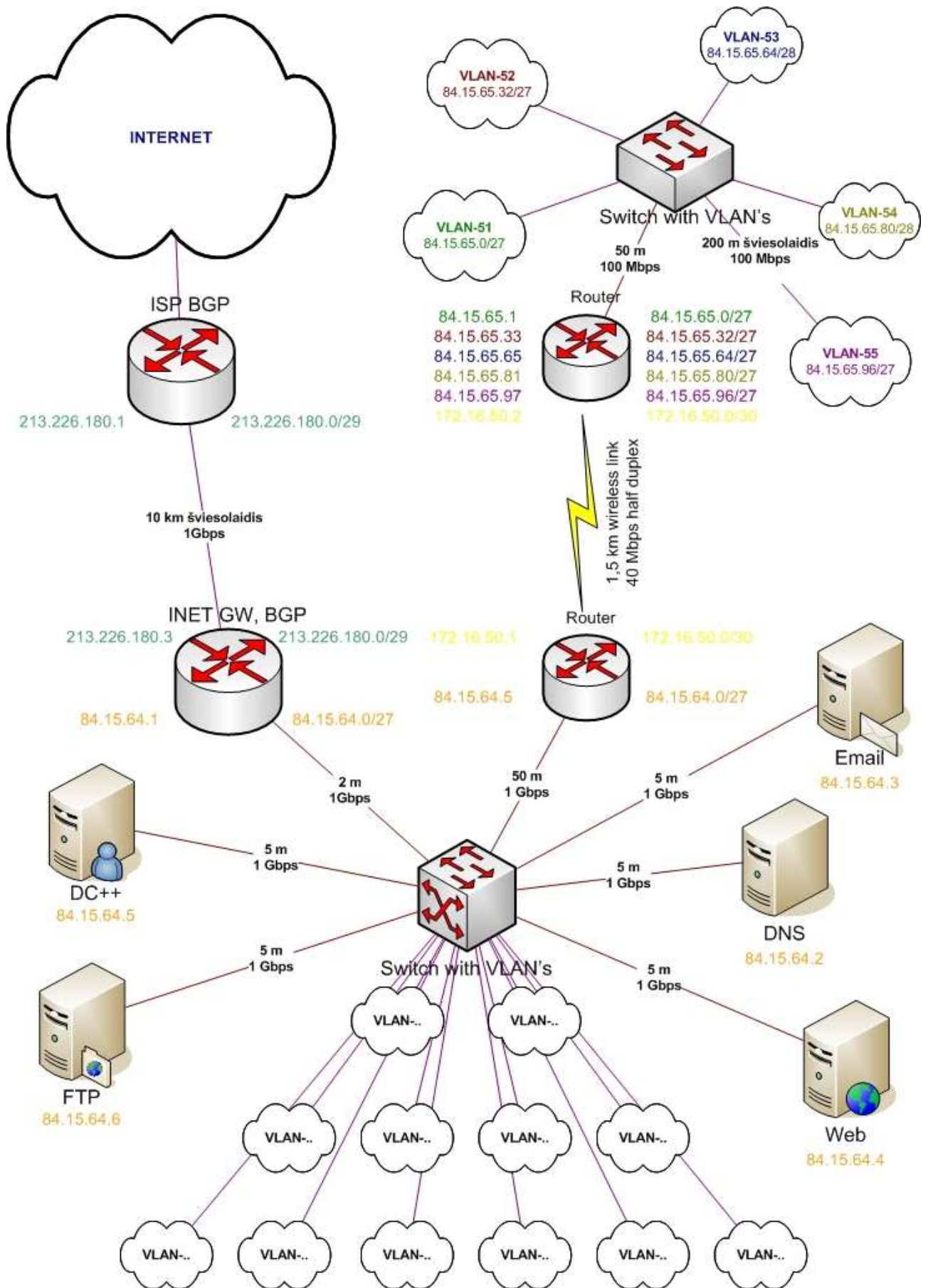
„Router“ tinklo topologijos pagrindiniai privalumai palyginus su „Bridge“ schemeje pavaizduota tinklo topologija yra:

- blokuoti nepageidautiną srautą,
- prioritetizuoti siunčiamus duomenis.

Įrenginys gali išnaudoti šiuos privalumus ne tik tarp dviejų potinklių, atskirtų radijo transmisija, bet ir tarp visų mažų potinklių (VLAN'ų). Tai leidžia pagerinti tinklo savybes ne tik radijo transmisijoje, bet ir visame vieliniame tinkle.



Schema 3 „Bridge“



Schema 4 „Router“

8. Išvados ir rekomendacijos

8.1 Išvados

Šiame darbe ištirtos Wi-Fi įrenginių problemos ir jų sprendimo variantai. Pasirinktas praktinis problemos sprendimas – sukurtas PC-based platformos bevielio ryšio įrenginys. Panaudoti srauto realiam laike analizavimo, klasifikavimo ir prioritetizavimo algoritmai. Papildyti savo kodo dalimi ir tarpusavyje suderinti jie sudaro vientisą užbaigta sistemą, kuri prioritetizuoja srautą pagal aukštą ir žemą prioritetą. Jautriai į vėlinimą reaguojančių interaktyvių aplikacijų, tokių kaip SSH, Telnet, VoIP, visas darbas su konsole, video realiu laiku ir t.t. po atlikto prioritetizavimo veikimas akivaizdžiai pagerėjo. Piko metu kai duomenų srautas siekia maksimumo prioritetizuotas srautas išstumia neprioritetizuotą srautą į antra vietą, bet nesustabdo jo visiškai, taip pasiekiamas interaktyvumas ir vartotojas dirbdamas pavyzdžiui prie konsolės nejaučia diskomforto.

Atliktas darbas padėjo įprastais įrenginiais ir programinės įrangos pagalba didinti Wi-Fi tinklų kokybę ir produktyvumą. Pavyzdžiui gali atlikti DHCP relay (snooping) funkcijas, kurias atlieka tik galingi komutatoriai rimtų gamintojų, kai ateina DHCP kliento užklausa dėl IP adreso, įrenginys gali ją iškart nukreipti į tam tikrą DHCP serverį, o ne siusti visiems kompiuteriams tinkle (broadcast) taip apkraudamas tinklą. Arba gali blokuoti paketus ne autorizuoto DHCP serverio. Tai pat įrenginys gali atlikti antivirus funkcijas su srautais realiam laike. Įrenginys gali būti papildytas radijo moduliu ir siusti duomenis per vieną radijo interfeisą, o gauti per kitą, taip galės pasiekti 40 Mbps Fullduplex režime.

Šio įrenginio potencialas yra tikrai labai didelis, jis yra labai universalus ir jį galima pritaikyti praktiškai prie bet kokios užduoties su duomenų srautais tinkle.

8.2 Rekomendacijos

Sukurta sistema galima naudoti pagal tiesioginę paskirtį: interaktyvių aplikacijų veikimo gerinimui, naudingo srauto padidimui, greito ir nebrangaus kokybiškos radijo transmisijos įrengimui.

Sukurta sistema yra labai universali, ją galima pritaikyti daugeliui užduočių spręsti, joje įdiegtas labai pažangus programinės įrangos paketas papildytas kodu kuris garantuoja įrangos stabilumą ir leidžia pasiekti geriausiai šiai dienai rezultatus, arti teorinių. Sistema be didelių pakeitimų gali atlikti Bridge, Router, Radius, Wi-Fi hot spot, Cache, DHCP, DNS, BGP funkcijas. Sistemą galima nesunkiai pritaikyti prie kitos platformos kadangi ji yra opensource.

9. Literatūra

- [IEE90] *An American National Standard* IEEE Standards for Local Area Networks:
Published by The Institute of Electrical and Electronics Engineers, Inc
Distributed in cooperation with Wiley-Interscience, a division of John Wiley &
Sons, Inc
- [MFP01] *Analysis of the Interference Between IEEE 802.11b and Bluetooth Systems*
Michael Fainberg, Pennie & Edmonds LLP, 1155 Avenue of Americas, New York,
NY 10036 fainbergm@pennie.com
David Goodman, Polytechnic University, Electrical Engineering, 6 Metrotech Center,
Brooklyn, NY 11201, USA, dgoodman@poly.edu
- [GB06] *Linux From Scratch*
1999-2006 Gerard Beekmans, gerard@linuxfromscratch.org
- [SC03] *802.11g CP: A Solution for IEEE 802.11g and 802.11b Inter-Working*
Sunghyun Choi, School of Electrical Engineering, Seoul National University, Seoul,
Korea schoi@snu.ac.kr
Javier dei Prado Pavon, Philips Research USA, Briarcliff Manor, New York, USA,
javier.delprado@philips.com
- [MGR06] *Stabilizing TCP Performance over Bursty Wireless Links Through the Combined
Use of Link-Layer Techniques*
Marta Garcia, Ramon Aguero, Luis Munoz, Member, IEEE, and Jose Angel Irastorza,
Member, IEEE
- [DYY06] *Performance Enhancement of Multirate IEEE 802.11 WLANs with Geographically
Scattered Stations*
Duck-Yong Yang, Tae-Jin Lee, Member, IEEE, Kyunghun Jang,
Jin-Bong Chang, and Sunghyun Choi, Senior Member, IEEE

- [WFE06] ***CISC, RISC architecture***
From Wikipedia, the free encyclopedia, <http://en.wikipedia.org/wiki/CISC>
<http://cse.stanford.edu/class/sophomore-college/projects-00/risc/>
- [WFE06] ***Wi-Fi***
From Wikipedia, the free encyclopedia,
http://en.wikipedia.org/wiki/Wi-fi#Origin_and_meaning_of_the_term_22Wi-Fi.22
- [DLD03] ***A Channel Condition Dependent QoS Enabling Scheme for IEEE802.11 Wireless LAN and Its Linux Based Implementation***
Dong Liu, Dimitrios Makrakis, Voicu Groza .
Broadband Wireless and Internetworking Research Laboratory
School of Information Technology and Engineering
University of Ottawa, Ottawa, Ontario, Canada, K1N 6N5