АНАЛИЗА НА ПЕРФОРМАНСИ НА КВАЛИТЕТ НА СЕРВИС ЗА VOIP И IPTV ВО IPV4 И IPV6 КОМПЈУТЕРСКИТЕ МРЕЖИ

Јелена Ѓорѓев, Александра Петкова, Сашо Гелев, Александар Соколовски
Европски Универзитет Република Македонија" – Скопје,
gjorgjev.jelena@live.eurm.edu.mk petkova.aleksandra@live.eurm.edu.mk
saso.gelev@eurm.edu.mk aleksandar.sokolovski@eurm.edu.mk

***Абстракт* – Области на истражување на овој труд се компјутерските мрежи и мултимедија, поточно IPTV / VoIP протоколите кои се користат за пренос на дигитални материјали во реално време.**
Во овој труд се анализираат двата споменати протоколи, и опциите кои ги нуди quality of service во IPv4 и IPv6 компјутерски мрежи.
Главната цел на овој труд е да се изврши анализа кои од постоечките комбинации и категории на quality of service е најсоодветен за кој тип на сообраќај во IPv4 и IPv6 компјутерски мрежи, а исто така да предложи некои нови, за нови типови на мултимедијалниот мрежен сообраќај .
Ова ќе се постигне со тестирање на ефикасноста и перформансите на различни сценарија, со цел да се најде оптимално решение за IPv4, IPv6 компјутерски мрежи.
Експериментот се изведува во строго контролирани лабораториски услови во вистинска реална средина за автентикација на резултатите.

Клучни зборови: QoS, quality of service, IP, IPv4, IPv6, VoIP, IPTV

I. Вовед

A. IP - интернет протокол

Интернет протокол (IP) е мрежен протокол за пренос на податоци кои се користат од страна на изворниот и одредишниот компјутер со цел да се воспостави податочна комуникација преку компјутерска мрежа. [8] Некои протоколи (како link протоколите) се дизајнирани за пренос на податоци во рамките на една локална мрежа, додека други протоколи се користат за транспорт на податоци меѓу соседни рутери во поширока мрежа. За разлика од ваквите линк протоколи интернет протоколите (IP) се користат за транспорт на податоци помеѓу арбитрарни компјутери во рамки на интернетот, т.е. низ многу LAN мрежи.

Обично, податоците се пренесуваат (рутираат) од испраќачот кон примачот преку повеќе рутери. Помеѓу испраќачот и примачот може да има еден или повеќе рутери. Секој рутер ја врши својата работа независно од друг и му ги пренесува податоците на рутерот до него, што значи дека податоците се пренесуваат од рутер на рутер.

IP е протокол кој овозможува конектирање на индивидуална (обично локална) мрежа на широко распространетиот интернет. Акронимот интернет протокол означува протокол кој конектира точно определени мрежи.

IP се состои од неколку индивидуални протоколи, и тие се:

- Самиот IP
- ICMP (Internet Control Message Protocol) – кој служи и е специфициран за одредени абнормални состојби
- IGMP (Internet Group Management Protocol) - служи за локално пренесување на MultiCast-ови
- ARP (Address Resolution Protocol) – и RARP (Reverse Address Resolution Protocol) – кои обично се среќаваат како независни протоколи бидејќи нивните паќети не се енкапсулирани во IP датаграмите.

Податоците во IP мрежата се праќаат во вид на блокови кои се нарекуваат пакети или датаграми.Специфично е тоа што при испраќањето на пакетите од изворот до одредишната адреса, однапред не се одредува точниот пат по кој податоците ке се испраќаат. Поради тоа IP мрежата функционира како пакетска мрежа.

Интернет протоколот е неконекциски ориентиран што значи дека патеката т.е. рутата од изворот до дестинацијата не треба да се воспостави пред пакетите (со податоците) да влезат во мрежата. Можно е секој пакет да си има своја различна независна рута од рутата на претходниот пакет кој има иста изворна и дестинациона IP адреса.

Интернет протоколот го познава секој логички домаќин (host) по неговиот број (IP адресата). На која

билодадена мрежа овој број мора да биде единствен за сите домашни корисници кои комуницираат низ таа мрежа. IP адресите на корисниците кои сурфаат по www се користат за да овозможат комуникација со сервверот на некој web site. Во зависност од интернет врската IP адресата при конектирањето (таканаречена статична IP адреса) или различна при секоја нова конекција (динамичка IP адреса). IP адресите обично се доделуваат преку сервисот наречен DHCP (Dynamic Hos Configuration Protocol).

IP протоколот нуди релативно несигурен пренос на податоци, што значи дека не постои никаква гаранција дека испратениот пакет навистина ќе стигне на одредиштето каде е испратен. Самиот пакет во процесот на пренесување може да се измени (на пр. да се измени редоследот на испратените пакети, може некој од пакетите да се дуплира или целосно да се изгуби). Интернет протоколот е протокол на третиот слој на OSI референтниот модел (мрежниот слој). Тој содржи информации за адресирањето, со што се постигнува секој мрежен уред (компјутер сервер, работна станица) кој е поврзан на интернет да има единствена адреса со која лесно ќе може да се идентификува во целата интернет мрежа. IP адресата претставува единствен број кој се користи од страна на машините (компјутерите) за меѓусебен сообрќај (комуникација) преку интернет со помош на интернет протоколи.

Додека еден рутер ги испраќа IP датаграминте тој не смее да ја измени нивната содржина. IP датаграмот претставуvа основната компонента на пренесен податок кај IP.

Засега постојат две верзии на IP протоколот, и тоа: IP version 4 (IPv4), која е опишана во RFC 791, и IP version 6 (IPv6), опишана во RFC 1883-1887. Описот на IP ги содржи следниве многу значајни елементи:

- IP ги дефинира основните податочни единици кои можат да се испратат преку Интернет т.е. IP дефинира формат на податочни единици (датаграми) кои се испраќаат;
- IP софтверот ги извршува рутирачките функции врз основа на IP адресите;
- Фрагментација и составување на датаграмите со цел да се обезбеди пренос на податоци со различни должини;
- IP содржи сет на правила за тоа како хостовите (крајните корисници) и рутерите да се справат со добиените датаграми, како и кога да се генерираат пораки за грешка и за тоа кога може датаграмите да се отстранат од мрежата.
-

Како што кај Link протоколите секој мрежен интерфејс има своја физичка адреса (Link), која за LAN мрежите е составена од 6 бајти, кај IP секој мрежен интерфејс има барем една IP адреса (каде за IPv4 содржи 4 бајти, а за IPv6 - 16 бајти.

Оригиналниот IPv4 , специфициран од страна на RFC760 во јануари 1980 бил заменет со RFC791 во септември 1981. IPv6 оригинално бил одреден од RFC1883 во декември 1995, Денес, IPv6 ја користи спецификацијата RFC2460 и бил наречен IP Next Generation. Иако IPv4 била доста моќен за неговото време.

Развојот на IPv6 главно бил мотивиран од малиот адресен простор во IPv4. Експанзијата на користењето на интернет услугите довела до потреба да се редефинира заглавјето со цел да се овозможи поефикасно рутирање и поголем адресен простор (т.е. поголем број IP адреси).

Интернет Протоколот (IP) е податочно ориентиран протокол кој се користи за пренос на податоци низ поврзани мрежи со користење на технологијата на комутација на пакети.

IP е протокол на мрежно ниво во пакетот на интернет протоколи кој е енкапсулиран во протоколите на податочно ниво (како што е на пример Етернет).
Како протокол на пониско ниво, IP обезбедува сервиси за комуникација помеѓу комјутерите со користење на единствени адреси.

1) IPv4

Интернет протокол верзија 4 е четврта итерација на IP и прва верзија на овој протокол која е пошироко прифатена и имплементирана. IPv4 е доминантен протокол на мрежно ниво на Интернет [8].

Овој протокол е опишан во IETF RFC 791 (Септември 1981) а претходно во RFC 760 (Јануари 1980). Департментот за одбрана на Соединетите Американски Држави го има прифатено и адаптирано овој стандард како MIL-STD-1777.

Целта на IP е да обезбеди систем на адресирање на компјутерите во мрежата со доделување на единствен идентификациски број.

IP датаграмот се состои од заглавие и информационо поле. Заглавието кај IPv4 е составено од фиксен дел со должина 20 бајти и опционен дел со променлива должина. Секој бајт од ваквата структура се праќа во мрежата во редослед од MSB (Most significant bit) кон LSB (Least significant bit) бит, па по тој редослед и се прима во дестинационата машина.

Кога не се спомнува верзијата на IP протоколот секогаш се подразбира IPv4, која е доминантен тип на Интернет протокол денес. Во продолжение ќе ги анализираме одделните полиња кои се составен дел на заглавието на IP пакетот.

Полето верзија (Version) укажува на верзијата на протоколот кој го генерирал тој датаграм (може да биде верзија 4 или 6, т.е. IPv4 или IPv6).

Бидејќи заглавието може да има променлива должина (зависно од тоа дали има и опции и колку), IHL (Internet Header Length) полето ја покажува должината на заглавието, изразена во 32 битни зборови (т.е. 1 збор = 4 бајти). Минималната должина е 5 збора (или 5 збора x 4 бајти = 20 бајти), што е случајот кога не е присутно опционо поле, а максималната е 60 зборови.
Полето тип на сервис (Type of Service – ToS) овозможува хостот да и каже на подмрежата каков сервис бара од неа, во смисла на доцнење, надежност и брзина на пренос. Овие побарувања се различни за различни типови сервиси. На пример, за дигитализиран говор малото доцнење е многу побитно од точната испорака (загубите на пакети), бидејќи во говорот може да се толерира по некој загубен датаграм, но не и варијација во доцнењето. При File Transfer, безгрешната трансмисија е многу побитна од доцнењето. Самото ToS поле се состои од 3 битно Precedence поле, а наредните 3 бита ја носат информацијата за: Delay, Throught, и Reliability. Користејќи ги овие битови, рутерите донесуваат одлука за тоа дали тој датаграм ќе го проследат користејќи некои сателитски врски или пак некоја изнајмена линија со голем проток (во bit/sec). Денес, под default, во рутерите се игнорира ова поле ако не се специфицира поинаку. Кога нема различни побарувања за различни типови сервиси (говор, веб сурфање, e-mail итн.), тогаш станува збор за еднакви сервиси за сите апликации од страна на мрежата, што е познато како best-effort. Затоа, често пати може да се сретне дека Интернет денес е во основа best-effort мрежа.

Полето вкупна должина на пакетот (Total Length) ја дава вкупната должина на датаграмот. Следствено, бидејќи полето има 16 бити, максимална должина на еден датаграм е 65535 бајти (64 kB), т.е. должината може да биде од 0 до 215 бајти.

Полето за идентификација на фрагмент (Fragment Identification) е потребно за да му овозможи на дестинациониот хост да изврши реасемблирање на помалите датаграми кои се фрагментирани некаде во мрежата, а притоа да не ги помеша со датаграмите кои припаѓале на некој друг поголем датаграм, наменет за иста дестинација, но кој потекнува од друг извор.

Полето знаменца (Flags) се состои од 3 бита од кои двата со најмало значење служат за контрола на фрагментацијата. Најмалку значајниот бит специфицира дали пакетот може да биде фрагментиран или не. Средниот бит специфицира дали пакетот е последен од серијата фрагментирани пакети или не. Третиот бит не е искористен.

Офсет на фрагментот (Fragment Offset) полето содржи информација за позицијата на фрагментираниот податок, кој се пренесува со IP пакетот, а е дел од еден датаграм, релативно во однос на почетокот на податоците во датаграмот. Оваа информација овозможува да се изврши правилна реконструкција на правилниот датаграм на приемната страна. Бидејќи полето се состои од 13 бити, можни се 8192 фрагменти по датаграм, но нивната вкупна должина не смее да надмине 64 kB.

Време на живот (Time to Live) полето е бројач со кој се ограничува животот на секој датаграм во мрежата. Повеќето рутери го идентификуваат ова поле како број на hop-ови кои му се дозволени на пакетот да ги помине во мрежата. Во секој рутер по патеката на пакетот вредноста на TTL полето се намалува за еден, независно од тоа колку датаграмот се задржал на линијата. Кога ќе стане 0, датаграмот се отфрла и рутерот кој го отфрлил праќа информација за тоа до изворот на пакетот. Ова поле оневозможува датаграмите бесконечно да шетаат низ мрежата, што лесно може да се случи ако рутерот на кој е поврзана дестинационата машина испадне од работа, така што тој датаграм бесцелно би патувал од рутер до рутер и непотребно би го оптоварувал сообраќајот.
Кога датаграмот е успешно и целосно примен во дестинацијата, IP нивото треба да знае на кој протокол над него да го проследи (на TCP, на UDP или пак до друг транспортен протокол). Таа информација ја носи тип на протокол (Protocol) полето.

IP адреса на изворот (Source Address) – ја дефинира IP адресата на изворот на датаграмот.
IP адреса на дестинацијата (Destination Address) – ја дефинира IP адресата на крајната дестинација, кон која е упатен IP пакетот.

Полето опции (Options) е предвидено за усовршување на протоколот, обезбедување на дополнителни сервиси како на крајниот корисник така и за потребите за одржување на самата мрежа. Со тоа што ова поле е опционо, се избегнува трајно алоцирање на бити во заглавието кои ретко би се користеле, а со тоа се намалува редундантната информација. Options полето е со променлива должина. Тоа почнува со код со кој се идентификува конкретната опција, потоа следи самата опциона информација.

2) IPv6

Интернет Прокол верзија 6 (IPv6) е протокол на мрежно ниво (англиски network layer протокол) за пакет-комутирани вмрежувања. Дизајниран е како наследник на IPv4 [9] и [10].

Главно подобрување кое го дава IPv6 (Интернет Протокол верзија 6) е зголемувањето на бројот на адреси на располање за вмрежените уреди. Тоа овозможува, например, секој мобилен телефон или кој и да е друг мобилен електронски уред да има сопствена адреса. IPv4 подржува околу 4,3 милијарди адреси, кои не се доволни согласно нараснатите потреби. IPv6 подржува околу $3{,}4\times10^{38}$ адреси или по околу 5×10^{28} адреси за секого од околу 6,5 милијарди денешни жители на земјата. На овој начин ќе се

надмине проблемот со недостаток на јавни IP адреси и најверојатно нема да има потреба од NAT (network address translation).

IPv6 не е директно компатибилна со IPv4. Адресната шема на IPv6 е нова и е базирана да им служи на демографски и модерни мрежи. Адресниот простор на IPv6 е долг 128 бити со кој е овозможено постоење на огромен број на адреси во споредба со 32 бити за адреси кај IPv4. Но, IPv6 не е развиена со цел да го разреши само проблемот со адресите бидејќи истиот може да биде решен со користење на јавни и приватни IP адреси.

Новитети кои ги внесува IPv6 ќе се согледаат преку разликите на IPv6 пакетите.

Како новитет во однос на IPv4, IPv6 поддржува QoS (Quality of Service) на мрежно ниво. Тоа значи дека квалитетот на сервисот (кој се дефинира преку загуби, доцнење на пакети, и проток во бити/сек) ќе може поедноставно да се имплементира во Интернет, посебно со премин на реалните комуникации (како говор) во IP средина. Ова е овозможено индиректно со користење на лабели за поток (flow labels) и приоритетна индикација, но притоа и во овој случај IP не дава гаранција за реалните end-to-end QoS како што нема и резервирање на мрежни ресурси.

Во поглед на безбедноста IPv6 подржува автентификација и приватност. Овозможува основни фукционалности на наплаќање на услугите како и наплаќање за идните видови сообраќај.

Со цел да се подобри рутирањето, (фалеше запирка) форматот на заглавјето е фиксен што овозможува хардверско процесирање на истото со што се овозможува побрзо рутирање во споредба со рутирањето со софтверското процесирање на заглавјето. Позначајни промени се направени во поглед на фрагментирањето на податоците. Кај IPv6 фрагментирањето на податоците се прави кај изворот а не како кај IPv4 каде истото се врши во рутерите.

Проверката на грешка на IP ниво е испуштена во IPv6 со цел да се намали процесирањето (додека кај IPv4 требаше секој рутер за секој пакет да ја пресметува одново Header Checksum, заради промена на TTL полето) и да се подобри рутирањето. Проверката на грешка само би одземала време и бити од заглавието а воедно ќе воведе и редундантност бидејќи и податочното и транспортното ниво вршат доверливи проверки на грешки.

IPv6 е следна генерација на IP верзија која има многу подобрувања во однос на верзијата 4 меѓу другите е и поголемиот адресен простор од 128 бити во однос на 32 битното адресно поле на IPv4.

Хоп (Hop) лимит е 8-битна вредност која ги нуди истите функции како и TTL полето во IPv4.

Но, од друга страна, IPv6 е нова IP верзија која не е радикално различна од моменталната IPv4. На мрежите се уште им се доделуваат мрежни адреси или префикси, IPv6 ги препраќа пакетите на истиот начин, неконекционо ориентирано по принципот скок по скок, IPv6 рутерите се уште ги користат рутирачките протоколи, мрежниот уред мора да биде исконфигуриран со IPv6 адреса итн. На IPv6 треба да се гледа како на поедноставна, поскалабилна и поефикасна верзија на IP.

Минималната должина на IPv6 заглаието е 40 бајти. Додека поголемиот адресен простор е позитивната страна на двапати поголемата минимална должина на IP заглавието кај IPv6 во споредба со IPv4 (таму е 20 бајти минималната должина на заглавието), редундантноста на ваквото заглавие е негативната страна. Имено, кај комуникациите во реално време кои користат помали пакети (како што е пример со говор преку IP) големиот број редундантни бајти во заглавието доведува до неефикасно искористување на расположливиот капацитет, односно до забележливо помал капацитет за пренос на корисните информации кај IPv6 во однос на IPv4.

3) Споредба на IPv4 и IPv6

Во [12] се објаснети подетално разликите помеѓу овие две верзии на Интернет протоколот.

Опис	IPv4	IPv6
Address	Адресата е долга 32 бита (4 бајти). Таа е составена од дел за мрежата и дел за хостот, а големината на таквите делови зависи од класата на адресата. Дефинирани се повеќе класи на адреси и тоа: A,B,C,D,E кои се разликуваат по првите неколку битови. Вкупниот број на IPv4 адреси е 4 294 967 296. Текст формата на IPv4 адресата е xxx.xxx.xxx.xxx, каде xxx се движи од 0 до 255 и секој таков број е составен од децимални (декадни цифри). Доколку на почетокот на адресата (кај првиот xxx имаме нули тие можеме да ги изоставиме и да не ги пишуваме. Максималниот број на карактери е 15, не вклучувајќи ја маската.	Адресата е дола 128 бита (16 бајти). Основната архитектура има 64 бита за мрежата и 64 бита за хостот. Често делот на хостот од IP адресата (или од дел од неа) се изведува од MAC адресата или друг интерфејс идентификатор. Во зависност од префиксот на подмрежата, IPv6 има покомплицирана архитектура од IPv4. Бројот на IPv6 адреси е 10^{28} (79 228 162 514 264 337 593 543 950 336) пати поголем од бројот на IPv4 адреси. Текст формата на IPv6 адреса е : xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, каде секој x е хексадецимална цифра, односно заменува 4 бита. Како и кај IPv4 нулите на почетокот на адресата можат да бидат изоставени. Дуплиот знак :: може да биде употребен еднаш во една текст форма на една IP адреса, што се користи за да се замени било кој број оф нула бити. На пр., ::ffff:10.120.78.40 е IPv4 адреса IPv6 мапирана.
Address allocation	Првобитно, адрсите биле распределувани според класата на мрежата. Како адресниот простор се намалувал се помали распределби биле правени користејќи classless inter-domain routing (CIDR), меѓутоа ваквото распределување не е балансирано помеѓу институциите и нацијата.	Алокацијата (распределбата) е во почетна фаза. Internet engineering task force (IETF) и internet architectura board (IAP) предложиле секоја организација, дом или субјект да се распределуваат на по должина од 48 подмрежен префикс. На овој начин на организацијата и остануваат 16 бита за подмрежување. Адресниот простор е доволно голем за на секоја личност во светот да му се овозможи подмрежен префикс со должина 48.
Address livetime	Генерално овој концепт не се применува, со исклучок на адресите доделени за користење на DHCP.	IPv6 адресите имаат два животи (livetimes) : посакуван и валиден, каде посакуван живот е секогаш помал или еднаков на валидниот. Откако посакуваниот живот ке се потроши, адресата не треба да се користи како изворна IP адреса за нови конекции, доколку постои еднакво добра

		посакувана адреса на располагање. Откако валидниот живот ќе се потроши адресата не може да се употребува (и не може да се препознае) како валидна дестинација – IP адреса за дојдовни пакети ниту да се користи како изворна IP адреса. Сепак некои IPv6 адреси, по дефиниција, имаат бесконечен посакуван и валиден живот.
Address mask	Се користат за определување на мрежата од хост делот	Не се користат
Address prefix	По некогаш се користат за да се определи мрежата од хост делот и понекогаш се запишува како /nn суфикс за презетираната форма на адресата.	Се користи за означување (оделување) на префиксот за подмрежата на една адреса. Се запишува како /nnn суфикс (достигнува до 3 децимални цифри и nnn бројот може да се движи од 0 до 128) по печатената форма. На пример fe80::982:2a5c/10, каде првите 10 битови го содржат подмрежниот префикс.
Address Resolution Protocol (ARP)	Address resolution протоколот се користи од страна на IPv4 за барање на физички адреси поврзани со IPv4 адреса како MAC или линк адреси.	IPv6 ги вградува овие функции во рамките на самиот IP како дел од алгоритмите за автоконфигурација без состојба и откривање на соседите користејќи internet control message протокол верзија 6 (ICMPv6). Оттука гледаме зошто не постои ARP6.
Address scope	За unicast адресите овој концепт не се преименува. Постојат одредени гарници за приватните адреси и повратна врска. Надвор од тоа адресите се претпоставува дека се глобални.	За IPv6 опсегот на адресата (address scope) е дел од архитектурата. Unicast адресите имаат два дефинира опсега, вклучувајќи локални врски и глобални; а multicast адресите имаат 14 опсега. Стандардната адреса за селекција и за изворот и за одредиштето го зема опсегот во предвид. Зоната на опсегот е негова инстанца во одредена мрежа.Како последица на тоа, IPv6 адресите понекогаш треба да се внесат или да се поврзат со идентификациониот број на зоната (zone ID). Синтаксата е %zid , каде zid е број (обично многу мал) или име. Идентификациониот број на зоната се пишува после адресата но пред префиксот. На пример, 2ba::1:2:14e:9a9b:c%3/48.
Address type	Unicast , multicast и broadcast	Unicast, Multicast и Anycast
Communications trase	Алатка за собирање на детални информации за патеката на TCP/IP (и други) пакети кои влегуваат или излегуваат од ситемот.	Се јавува и кај IPv6.
Configuration	Мора да го конфигурираме ново инсталираниот систем пред да можеме да комуницираме со други системи, односно IP адресите и рутите мора да бидат доделени.	Конфигурирањето не е задолжително и е опционално, во зависност од потребните функции. IPv6 може да се користи со било кој Ethernet адаптер и може да се стартува врз интерфејс со повратна врска. Ipv6 интерфејсите се само – конфигурирачки и ја користат IPv6 автоконфигурацијата без состојба. Можеме и рачно да го конфигурираме интерфејсот на IPv6. Значи системот ќе биде способен да комуницира со други IPv6 системи кои се локални или далечински, во зависност од типот на мрежата и дали има IPv6 рутер.
Domain Name System (DNS)	Апликациите ги прифаќаат хост имињата и потоа преку DNS ѓи добиваат IP адресите користејќи го API сокетот gethostbyname(). Апликациите исто така работат и обратно, ги прифаќаат IP адресите и потоа повторно преку DNS ѓи добиваат имињата на хостовите со користење на gethostbyaddr(). За IPv4 доменот за обратно пребарување се наоѓа во addr.arpa.	Истото важи и за IPv6. Подршката за IPv6 постои со користење на AAAA рекорд тип и обратно пребарување. Апликацијата може да избере да прифати IPv6 адреса од DNS (или не) и потоа да ја користи IPv6 за комуникација (или не). API сокетот gethostbyname() подржува само IPv4.За IPv6 доменот користи за обратно пребарување на ip6.arpa или ip6.int и се користи API сокетот getnameinfo(). За IPv6 се користи getaddrinfo() за да се добие (по избор на апликацијата) само IPv6, или и IPv4 и IPv6 адреси.
Dynamic Host Configuration Protocol (DHCP)	Се користи за динамочко добивање на IP адреса и други информации за конфигурацијата. i5/OS го поддржува DHCP серверот за IPv4.	i5/OS имплементацијата на DHCP не го подржува IPv6.
File Transfer Protocol (FTP)	File transfer protocol ни овозможува да праќаме и примаме фајлови преку мрежа	i5/OS имплементацијата на FTP не го подржува IPv6.
Fragments	Кога еден пакет е премногу голем за следниот линк преку кој треба да се испрати, може да биде фрагментиран од страна на испраќачот (host или router)	За IPv6, фрагментацијата може да се случи само кај изворниот јазол, и составувањето може да се направи само кај одредишниот јазол. Кај екстензијата на фрагментацијата насловот (заглавјето) се користи.
Host table	На iSeries Navigator, конфигурирачката табела ги поврзува интернет адресата со името на хостот.Оваа табела се користи од страна на sockets name resolver, или пред DNS пребарувањето или по неуспешното DNS пребарување (утврдени со приоритетот на пребарување на името на хостот).	Во моментов оваа табела не го подржува IPv6. Корисниците треба да го конфигурираат AAA рекордот во DNS за резолуцијата на IPv6 доменот. DNS може да се изврши локално на истиот систем како преведувач, или може да се користи на друг систем.
Interface	Концептуалниот или логичкиот ентитет го користи TCP/IP за да праќа и прима пакети и секогаш е тесно поврзан со IPv4 адреса, ако не е и именуван со IPv4 адреса. Понекогаш се нарекува логички интерфејс. Може да се стартува и да се прекине независно еден од друг и од TCP/IP користејќи STRTCPIFC и ENDTCPIFC команди и со користење на iSeries navigator.	Истиот концепт важи и за IPv6. Но може да се стартува или прекине независно еден од друг и од TCP/IP само со користење на iSeries navigator.
Internet Control Message Protocol (ICMP)	ICMP се користи од страна на IPv4 за комуникација со информации на мрежата.	Слично се користи и за IPv6 меѓутоа интернет протоколот за контрола на пораките со верзија 6 (ICMPv6) нуди некој нови атрибути. Основните видови на грешки остануваат како што се недостапна информација, ехо барање и одговор. Нови типови и кодови се додадени за подршка на откривањето на сосед и нејзините сродни функции.
Internet Group Management Protocol (IGMP)	IGMP се користи од страна на IPv4 рутери за да се најдат хостови кои сакаат сообраќај за одредена multicast група, и се користат од страна на IPv4 хост за да ги информира IPv4 рутерите за постоечките слушачи на multicast групи (на хостот).	За IPv6 се заменува со MLD протокол (multicast listener discovery). Во суштина го работи истото што IGMP го прави за IPv4, но користи ICMPv6 со додавање на неколку MLD специфични ICMPv6 типови на вредности (променливи).
IP header	Должината на променливите (варијаблите) се движи од 20 до 60 бити, во зависност од постоечките IP опции.	Има фиксна должина од 40 бајти. Во IP заглавјето нема опции. Општо земено, IPv6 заглавјето е поедноставно од IPv4 заглавјето.
IP header options	Постојат повеќе опции кои можат да го придружуваат IP заглавието (пред било кој транспорт на заглавието).	IPv6 заглавието нема опции. Наместот тоа, IPv6 додава дополнителни опционални екстензии (продолжувања) на заглавијата. Екстензиите на заглавијата се AH и ESP (кои се непроменети од IPv4), hop-by-hop, рутирање, фрагмент и дестинација.
IP header protocol byte	IP header protocol byte е кодот на протоколот на транспортниот слој или пакетниот товар, на пример ICMP.	IP header protocol byte е тип на заглавието кој се наоѓа веднаш до IPv6 заглавието. Ги користи истите вредности како кај IPv4 полето, но ефектот на архитектурата е да се овозможи тековно дефиниран спектар на следните заглавија, и лесно се проширува. Следното заглавје ќе биде транспортното заглавје, односно екстензија на заглавието (ICMPv6).
IP header type of service (TOS) byte	Се користи од страна на QoS и диференцираните сервиси за одредување на класата на сообраќајот.	Ја означува IPv6 класата на сообраќајот слично како кај IPv4, меѓутоа користи различни кодови, моментално IPv6 не го подржува TOS.
iSeries navigator support	iSeries navigator нуди целосно решение за конфигурација на TCP/IP.	Истото важи и за IPv6 но за IPv6 конфигурацијата нема достапни CL команди.
LAN conection	Се користи од страна на IP интерфејс за да се дојде до физичка мрежа. Постојат повеќе типови на пример token ring и ethernet. Понекогаш се нарекува физички интерфејс, линк или линија.	IPv6 може да се користи со било кои Ethernet адаптери, а исто така е подржан и преку виртуелен Ethernet меѓу логички партиции.
Layer 2 Tunnel Protocol (L2TP)	L2TP може да се смета за виртуелен PPP (Peer-To-Peer Protocol) и работи над било кој подржан тип на линија.	Во моментов i5/OS имплементацијата на L2TP не го подржува IPv6.
Loopback address	Интерфејс со адреса 127.*.*.* (обично 127.0.0.1) кој може да се користи од страна на еден јазол за испраќање пакети самиот на себе. Физичкиот интерфејс е именуван *LOOPBACK.	Концептот е ист како и кај Ipv4. Единствената повратна врска е со адреса 0000:0000:0000:0000:0000:0000:0000:0001 или скратено ::1. Виртуелниот физички интерфејс е именувана *LOOPBACK.
Maximum Transmission Unit (MTU)	MTU на линк е максималниот број на бајти што таков вид на врска (линк) го подржува, како на пример Ethernet или модем	Архитектурата на IPv6 има долна граница на MTU од 1280 бајти, што значи дека IPv6 не ги фрагментира пакетите под оваа граница. За да се испрати IPv6 преку линк со помалце од 1280 MTU, линк слојот мора транспарентно да ги фрагментира и дефрагментира IPv6 пакетите.

NETSTAT	Алатка која служи за преглед на статусот на TCP/IP конекциите, интерфејсите или рутите и достапна е со користење на iSeries navigator и 5250.	Истото важи и за IPv6 и IPv6 има подршка за 5250 и iSeries navigator.
Network Address Translation (NAT)	Основните firewall функции интегрирани во TCP/IP, конфигуриран е со користење на iSeries navigator.	Во моментов NAT не подржува IPv6 односно IPv6 не бара NAT. Проширениот адресен простор на IPv6 го елиминира проблемот на недостаток на адреса и овозможува полесно повторно нумерирање.
Network table	На iSeries navigator конфигурирачката табела ги поврзува името на мрежата и IP адресата без маска.	Во моментов кај IPv6 не се направени промени вр оваа табела.
Node info queru	Не постои	Едноставна и задоволувачка мрежна алатка која треба да работи како PING, но со содржина: еден IPv6 јазол може да пребарува друг IPv6 јазол преку DNS името, а IPv6 unicast адресата или IPv4 адресата, меѓутоа во моментов не е подржана.
Packet filtering	Основните firewall функции интегрирани во TCP/IP, конфигуриран е со користење на iSeries navigator.	Кај IPv6 не може да се користи филтрирање на пакетите.
Packet forwarding	I5/OS TCP/IP стекот може да биде конфигуриран да проследува IP пакети кој ги добива за нелокални IP адреси. Типично влезниот и излезниот интерфејс се поврзани со различни LAN мрежи.	IPv6 пакетите не се праќаат (проследуваат)
Ping	Основна TCP/IP алатка за тестирање на дострелот. Достапна е со користење iSeries navigator и 5250.	Истото важи и за IPv6 и IPv6 има подршка за 5250 и iSeries navigator.
Point-to-Point Protocol (PPP)	PPP подржува dial-up интерфејси преку различни модеми и типови на врски.	Во моментов i5/OS имплементацијата на PPP не го подржува IPv6.
Port restrictions	Овие i5/OS панели му дозволуваат на корисникот да го конфигурира бројот на селектираната порта или интервалот на броевите на портите за TCP или UDP , така што тие би станале достапни само за одреден профил.	Истото важи и за IPv6, а рестрикциите за портите за IPv6 се идентични со оние кое се на располагање во IPv4.
Ports	TCP и UDP имаат оддвоени простори за порти, секоја идентификувана на бројот на портата во интервал од 1 до 65535.	За IPv6 портите работат исто како и кај IPv4, затоа што тие се во новото адресно семејство каде во моментов има четри оделни простори за порти. На пример, има две TCP порти со 80 празни места на кои може да се врзе некоја апликација и еден AF_INET и еден AF_INET6.
Private and public addresses	Сите IPv4 адреси се јавни освен три адресни интервали кои се дизајнирани како приватни од страна на IETF RFC 1918 и тие се: 10.*.*.* (10/8) и од 172.16.0.0 до 172.31.255.255 (172.16/12) и 192.168.*.* (192.168/16). Домејните на приватните адреси обично се користат во склоп на организации и не можата да бидат рутирани преку интернет.	IPv6 има аналоген концепт со важни разлики. Адресите се јавни или привремени, претходно одредени како анонимни. За разлика од IPv4 приватните адреси, привремените адреси можат да бидат глобално рутирани. И мотивацијата е различна; IPv6 привремените адреси треба да го бранат идентитетот на клиентот кога воспоставува комуникација (од приватен интерес). Привремените адреси имаат привремен живот (lifetime), и не содржат идентификувач на интерфејсот што е линк (MAC) адреса. Генерално овие адреси можат да се разликуваат од јавните. IPv6 има идеја за ограничување на опсегот на адреси користејќи свој изграден опсег од знаци.
Protocol table	На iSeries navigatorot, конфигурирачката табела ги поврзува името на протоколот со неговиот доделен број на протокол на пример UDT,17.Системот е испратен со мал број на записи на влезови : IP, TCP, UDP и ICMP.	Табелата може да се користи со IPv6 без промени.
Quality Of Service (QOS)	Квалитетот на услугата овозможува да се побара приоритет на пакетот и пропусен опсег на TCP/IP апликации.	Во моментов, IP/OS имплементацијата за QOS не го подржува IPv6.
Renumbering	Се прави преку мануелна реконфигурација со можен исклучок на DHCP. Општо земено за сајт или организација еден тежок и проблематичен процес може да се избегне ако е тоа можно.	Е значаен елемент од архитектурана на IPv6 и во голема мера е автоматски, особено во рамките на /48 префикс.
Route	Логички гледано, претсавува мапирање на сет од IP адреси (може да содржи и само една) на физички интерфејс и единечна next-hop IP адреса. IP пакетите чија адресна дестинација е дефинирана како дел од сетот се пренасочуваат на следниот hop користејќи линија (врска). IPv4 рутите (правците) се поврзани со IPv4 интерфејс, а со тоа и со IPv4 адреса. Стандардната рута е *DFTROUTE.	Концептуално, слична е на IPv4, со една важна разлика: IPv6 рутите се поврзани со физички интерфејс (линк), како на пример ETH03. Една од причините за поврзаноста на рутата со физички интерфејс е разликата на функциите за избор на изворна адреса.
Routing Information Protocol (RIP)	RIP е рутирачки протокол подржан од страна на рутирачкиот демон (routed daemon).	Во моментов, RIP нема подршка за IPv6 и IPv6 рутирањето користи статички рути.
Services table	На i5/OS, конфигурачките табели го поврзуваат името на сервисот со порта или протокол. Голем број на добро познати услуги (сервиси) се наведени во табелата на сервиси. Многу апликации ја користат оваа табела за да одлучат која порта да ја користат.	Кај IPv6 врз оваа табела не се направени никакви измени.
Simple Network Management Protocol (SNMP)	SNMP е протокол за менаџирање (управување) со системот.	Во моментов, IP/OS имплементацијата за SNMP не го подржува IPv6.
Sockets API	Овие API се начин на кој апликациите го користат TCP/IP. Апликациите кои немаат потреба за IPv6 не се погодени од промените на сокетите за подршка на IPv6.	IPv6 ги подобрува сокетите, така што апликациите сега може да користат IPv6, со користење на ново адресно семејство AF_INET6. Подобрувањата се дизајнирани така што постоечките IPv4 апликации остануваат комплетно не променети од страна на IPv6 и API промените. Апликациите кои сакаат да подржат конкурентен IPv4 и IPv6 сообраќај, или само IPv6 сообраќај, а многу лесно се прилагодуваат со користење на IPv6 адреси кои се IPv4 мапирани во облик ::ffff:a.b.c.d, каде a.b.c.d е IPv4 адресата на клиентот. Новите API исто така вклучуваат подршка за конвертирање на IPv6 адреси од текс во бинарен формат и од бинарна форма во текст.
Source address selection	Апликација која може да го одреди изворниот IP (обично со користење на сокетите bind()).Ако се врзе со INADDR_ANY, изворниот IP се избира врз основа на рутата.	Како и со IPv4 апликацијата може да посочи на изворната IPv6 адреса со користење на BIND(). Слично на IPv4 може да му дозволи на системот да избере IPv6 изворна адреса со користење на IN6ADDR_ANY. Но бидејќи IPv6 врските имаат многу IPv6 адреси, внатрешниот метод за избор на IP извор е различен.
Starting and stopping	Користи STRTCP и ENDTCP за стартување и прекинување на TCP/IP.	Важи истото како за IPv4. IPv4 и IPv6 не се стартуваат и прекинуваат независно еден од друг или пак независно од TCP/IP. Тоа значи дека ги стартуваме или прекинуваме сите TCP/IP, не само IPv4 или IPv6. Секој IPv6 интерфејс автоматски се стартува ако AUTOSTART параметарот има вредност *YES (по default). IPv6 не може да се користи или конфигурира без IPv4. IPv6 интерфејсот на повратна врска, ::1, автоматски ќе биде дефиниран и ќе се активира кога IPv6 ќе стартува.
Telnet	Telnet овозможува користење и логирање оддалечен компјутер како да сме поврзани со него директно.	Во моментов, IP/OS имплементацијата за Telnet не го подржува IPv6.
Trace route	Основна TCP/IP алатка за определување на патеката. Достапна е со користење на iSeries navigator и 5250.	Истото важи и за IPv6 и IPv6 има подршка за 5250 и iSeries navigator.
Transport layers	TCP, UDP, RAW	Истите транспорти постојат и кај IPv6.
Unspecified address	Очигледно не се дефинираат како такви. Socket програмирањето користи 0.0.0.0 како INADDR_ANY.	Дефинирана како ::/128 (0/128). Се користи како IP извор во некои пакети за откривање на соседи, и во други различни контексти, како сокети. Socket програмирањето користи ::/128 како IN6ADDR_ANY.
Virtual Private Network (VPN)	Виртуелната приватна мрежа (со користење на IPsec) овозможува безбедно проширување на приватна мрежа врз постоечка јавна мрежа.	Во моментов, IP/OS имплементацијата за VPN не го подржува IPv6.

B. IPTV

Internet Protocol Television (IPTV) е систем каде услуга за дигитална телевизија е овозможена користејќи Интернет протокол, низ мрежна инфраструктура, која може да вклучува доставка преку мрежна конекција [5]. Генерална дефиниција би била телевизиска содржина која наместо да биде доставена низ традиционален медиум за пренос и формат за кабел, таа е примена од гледачот преку технологиите кои се користат за компјутерските мрежи. За домашните корисници, IPTV е најчесто овозможен заедно со video on demand и прикачен со интернет услуга како на пример web пристап и VoIP. IPTV е најчесто овозможен од сервис провајдер кој користи затворена мрежна инфраструктура. Овој пристап на затворена мрежа е во конкуренција со доставката на телевизиската содржина во јавниот интернет, наречена Интернет Телевизија. Во бизнисот, IPTV може да се користи телевизиската содржина во заедничка LAN мрежа.

IPTV го конвертира телевизискиот сигнал во мали пакети на податоци како било која друга форма на online сообраќај како на пример e-mail или web страна. IPTV се состои од три главни компоненти. Првата, содржината и телевизорот, каде што TB каналите се примени и кодирани, а исто така и друг вид на содржина како на пример видеа кои се предходно зачувани. Втората компонента е мрежата за доставка, која е широка, распространета мрежа овозможена од телеком операторите како на пример MTNL. Третата компонента е *set top box* или кутија која е потребна кај локацијата на купувачот. Пакетите се реасемблирани со програмирање од софтвер во set-top кутијата. Оваа кутија е поврзана помеѓу мрежата на модемот на операторот и телевизорот на корисникот.

C. VoIP

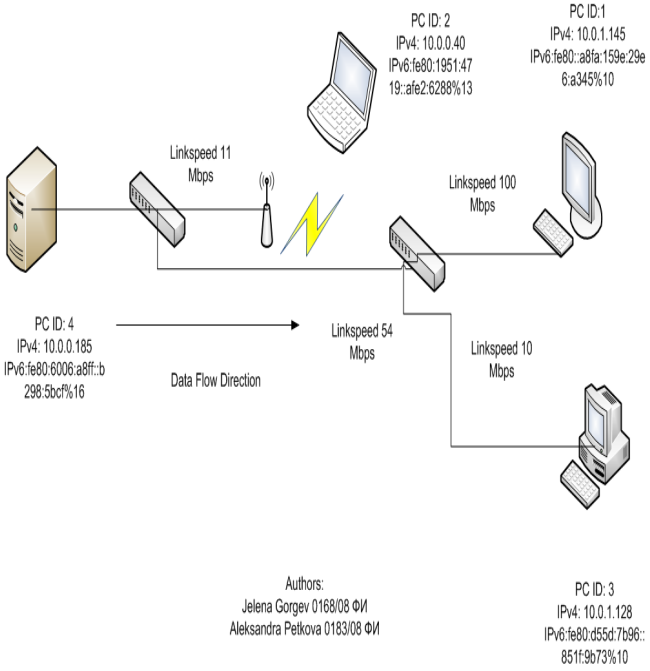
Voice over Internet Protocol, или VoIP, IP Телефонија, Интернет телефонија, Broadband телефонија, Broadband Телефон или Voice over Broadband претставува рутирање на говорна конверзација преку Интернет односно преку IP-базирани мрежи. Компаниите кои обезбедуваат VoIP услуги се нарекуваат провајдери, додека протоколите кои се користат за пренос на говорните сигнали преку IP мрежата се нарекуваат Voice over IP или VoIP протоколи.

VoIP - VoIP разговорите вообичаено се бесплатни додека за VoIP - PSTN разговорите најчесто се плаќа одредена надокнада. VoIP е апликација која аудиоинформацијата во реално време, како што е говорот, ја претвара на начин кој е конкурентен на класичната телефонија. Се врши дигитилизација на сигналот и се праќа да патува низ Интернет мрежата. VoIP може да се направи од компјутер, специјален VoIP телефон или по традиционален телефон со адаптер. Но за да се воспостави VoIP врска потребно е да се има Интернет конекција. VoIP се заснова на фундаменталните принципи на архитектурата на Интернетот така што секој компјутер кој има IP адреса може да праќа податоци до било кој друг компјутер со друга IP адреса. Многу од корисниците се запознаени со архитектурата на клиент/сервер мрежата каде клиентот испраќа барање до друг компјутер во мрежата наречен сервер. Иако VoIP може да работи на овој начин, VoIP е доста флексибилен и не е потребен клиент/сервер моделот. VoIP само бара поврзување со Интернет и програм кој може да ги кодира и трансмитира говорот.

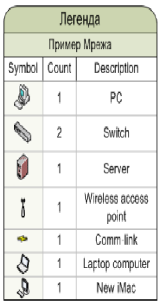
II. ЕКСПЕРИМЕНТ

Значи со нашиот експеримет кој што го извршувавме ние сакавме да увидиме всушност како настанува губењето на пакетите кога го зголемуваме бројот на уреди кон кои што праќаме а брзината да ни остане иста. За да може сите овие резултати да ги увидиме сите сценарија кои ги изведувавме го снимавме со Wireshark за да може подобро да увидеме како настанува губењето на пакетите.

Со цел да разгледаме повеќе аспекти и да добиеме различни резултати кои ќе не доведат до подобар заклучок, експериментиравме со повеќе различни сценариа. Експериментот главно се состои до video streaming на еден или повеќе филмови од еден кон друг или повеќе компјтери. За video streaming ја корисевме софтверската програма Windows Media Player, кој се покажа одлично при извршување на нашите барања. Со цел да добиеме пореални и поразлични резултати стримингот се вршеше помеѓу еден PC (со Windows 7 оперативен систем, кој всушност играше улога на сервер при изведување на експериментот), два Laptop-и (едниот со WIndows 7 операивен систем, а другиот со Mac OSX - Snow Leopard) и уште еден notebook (со WIndows XP оперативен систем). Исто така уредите беа поврзани на две различни мрежи, два од нив со Ethernet кабел, а два преку Wireless врска. Опсегот на брзината на протек на каблите го ограничивме на различна брзина. Сценаријата се состоеја од стримување на еден филм кон еден, два и три компјутери и три филма кон три различни компјутери, најпрво со користење IPv4 интернет протоколот, а потоа истите ги повторивме со употреба на IPv6 протоколот. Дополнителни комбинации се правеа при стриминг на еден и три филмови кон три компјутери и со двата интернет протоколи со тоа што QoS (quality of service) сервисот или го вклучувавме или го исклучувавме. На тој начин со секое сценарио, се добиваа различни резултати за процентот на загубата на пакети.



III. РЕЗУЛТАТИ



Data Loss in IPTV Traffic					
source	destination	No. of Stremas	Ip version	Qos	% of Loss
1	3	1	Ipv4	OFF	<1%
1	3,4	1	Ipv4	OFF	<1%
1	2,3,4	1	Ipv4	OFF	2-4%
1	2,3,4	1	Ipv4	ON	<2%
1	2,3,4	3	Ipv4	OFF	3-5%
1	2,3,4	3	Ipv4	ON	<2%
1	3	1	Ipv6	OFF	<0,25%
1	3,4	1	Ipv6	OFF	<0,5%
1	2,3,4	1	Ipv6	OFF	<1%
1	2,3,4	1	Ipv6	ON	<0,5%
1	2,3,4	3	Ipv6	OFF	<2%
1	2,3,4	3	Ipv6	ON	<1%

Како што можеме да забележиме од добиените резултати во врска со употребата на IPv4 и IPv6, доста очигледно е дека при користење на IPv6 интернет протоколот имаме многу помала загуба на пакети отколку при изведување на експериментот со употреба на IPv4 протоколот. Разликата при загубата на пакети е многу голема, согледувајќи дека со IPv6 таа загуба е скоро двојно помала. Оваа разлика особено се забележува при стримингот на еден филм кон три компјутери, каде од 2-4% со IPv4 се намалува на 1% со IPv6 и на три филма кон три компјутери, каде од 3-5% со IPv4 се намалува на 2% со IPv6. Исто така двојно помала загуба на пакети имаме кога употебуваме QoS, за разлика од истото сценарио кога не го употребуваме.

Според овие резултати лесно може да се согледа дека најмала загуба на пакети ни се јавува кога користиме комбинација на QoS со IPv6.

Ако ја погледнеме табелата ќе забележиме дека доколку употребуваме IPv6 протокол со добра интренет конекција тогаш од аспект на IPTV имаме многу помала загуба на пакети. Бидејќи знаеме дека IPTV се заснова на интернет протоколи, и тој е чуствителен на губење на пакети (пакети) и доцнење доколку IPTV конекцијата не е доволно брза. Значи од табелата ќе забележиме дека кога вршиме стриминг на видео кон три уреди загубата на пакетите ни се зголемува дури и до пет проценти бидејќи конекцијата е многу побавна и пооптеретена и затоа е намамален и квалитетот на сервисот. А додека пак кога имаме стриминг на видеото кон еден компјутер тогаш интеренет конекцијата ни е побрза нема толку голема оптеретеност и затоа губењето на пакети е до еден процент и квалитетот на сервис е далеку подобар.

IV. ЗАКЛУЧОК

Internet Protocol Television (IPTV) е дигитална телевизија која е достапна во вашиот дом, на вашиот телевизор или компјутер преку брза интернет конекција. Во овој тип на сервис, каналите се кодирани во IP формат и донесени до телевизијата преку сет на кутии. IP платформата нуди значителни предности, вклучувајќи ја способноста да интегрира телевизија со други IP сервери како интернет пристап и VoIP.Вклучената IP мрежа дозволува доставувањето да биде со повеќе содржини и функционалности.

Според направениот експеримент со употреба на IPv4 и IPv6 доста очигледно е дека со користење на IPv6 интернет протоколот има многу помала загуба на пакети отколку кај IPv4 интренет протоколот.Тоа и самите можеме да го утврдиме од резултати во табелата погоре кои ги добивме при стримингот на еден филм кон три компјутери. Но сепак треба да се нагласи и дека имаме и двојна помала загуба на пакети и при употреба на QoS.Значи со добра интернет конекција, според добиените резултати од табелата можеме да увидеме дека најмала загуба на пакети имаме кога користиме комбинација на QoS со IPv6 интренет протоколот.А најголема загуба на пакети имаме кога го зголемуваме бројот на уреди кон кои стримуваме бидејќи тогаш конекција е пооптеретена и затоа се намалува и квалитетот на сервис.Кон колку помалку уреди стримуваме подобра интернет конекција помала загуба на пакети и подобар квалитет на сервис.

V. БИБЛИОГРАФИЈА

[1] Сашо Гелев “Компјутерски Мрежи” 2011, ЕУРМ-ФИ
[2] Andrew S. Tanenbaum, Computer Networks, 4th Edition \
[3] William Stallings, Operating Systems Internals and Design Principles (5th Edition) , 2009
[4] Larry L. Peterson and Bruce S. Davie, Computer Networks, a System Approach, Edition 3
[5] The Economic Times: What is IP television?, http://articles.economictimes.indiatimes.com/2006-11-27/news/27425252_1_iptv-service-internet-protocol-television-boxes-with-broadband-internet , [06/18/2011]

[6] Guardian.co.uk: Broadcasters to launch joint VoD service, http://www.guardian.co.uk/media/2007/nov/27/bbc.itv , [03/21/2011]
[7] Inqurier.net: World 'running out of Internet addresses', http://technology.inquirer.net/infotech/infotech/view/20110121-315808/World-running-out-of-Internet-addresses , [14/07/2011]
[8] RFC 791: Internet Protocol, http://tools.ietf.org/html/rfc791 , [02/05/2011]
[9] Network World: IPv6 vs. Carrier-grade NAT http://www.networkworld.com/news/2010/060710-tech-argument-ipv6-nat.html , [03/04/2011]
[10] RFC 2460: Internet Protocol version 6 (IPv6) Specification, http://tools.ietf.org/html/rfc2460 , [03/14/2011]
[11] RFC 1752: The Recommendation for the IP Next Generation Protocol, http://tools.ietf.org/html/rfc1752 , [23/07/2011]
[12] IBM: i5/OS Information Center, Version 5 Release 4, http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=%2Frzai2%2Frzai2compipv4ipv6.htm, [11/08/2010]

Јелена Ѓорѓев е родена на 05/02/1990 во Ниш, Р. Србија. Живее и студира во Скопје. Студира Софтверско инжењерство на Факултетот за информатика при Европскиот Универзитет на Р. Македонија. Матурираше во државната гимназија "Орце Николов" во Скопје.

Александра Петкова е родена на 08/11/1989 во Гевгелија, Р. Македонија. Живее и студира во Скопје. Студира Софтверско инжењерство на Факултетот за информатика при Европскиот Универзитет на Р. Македонија. Матурираше во државната гимназија "Јосиф Јосифовски" во Гевгелија.

Performance Analysis of quality of service for VOIP and IPTV IPv4 and IPv6 computer networks

Jelena Gjorgjev[1], Aleksandra Petkova[1], Sasho Gelev[1], Aleksandar Sokolovski[1]
[1] "European University of Republic Of Macedoina" – Skopje,
gjorgjev.jelena@live.eurm.edu.mk petkova.aleksandra@live.eurm.edu.mk
saso.gelev@eurm.edu.mk aleksandar.sokolovski@eurm.edu.mk

Abstract –Areas of research of this paper are computer networks and multimedia, more precisely IPTV / VOIP protocols used for transmission of digital materials in real time.
In this paper are analyzed the two mentioned protocols, and the options that are offered by the quality of service in IPv4 and IPv6 computer networks.
The main objective of this paper is to perform analysis of which existing combinations and categories of the quality of service is most suitable for which type of traffic in IPv4 and IPv6 computer networks and also to propose some new, for the new types of multimedia network traffic.
This will be achieved by testing the performance of different scenarios in order to find the optimal solution for IPv4, IPv6 computer networks.
The experiment is performed in strictly controlled laboratory conditions in a real environment to authenticate results.

Keywords
QoS, quality of service, IP, IPv4, IPv6, VoIP, IPTV

Jelena Gjorgjev is born on 02/05/1990 in Nis, R.Serbia. Lives and studies in Skopje. Studies Software Engineering, part of the Faculty of Informatics, on European University of Republic of Macedonia. Graduated in the state high school "Orce Nikolov" in Skopje.

Aleksandra Petkova is born on 11/08/1989 in Gevgelija, R.Macedonia. Lives and studies in Skopje. Studies Software Engineering, part of the Faculty of Informatics, on European University of Republic of Macedonia. Graduated in the state high school "Josif Josifovski" in Gevgelija.