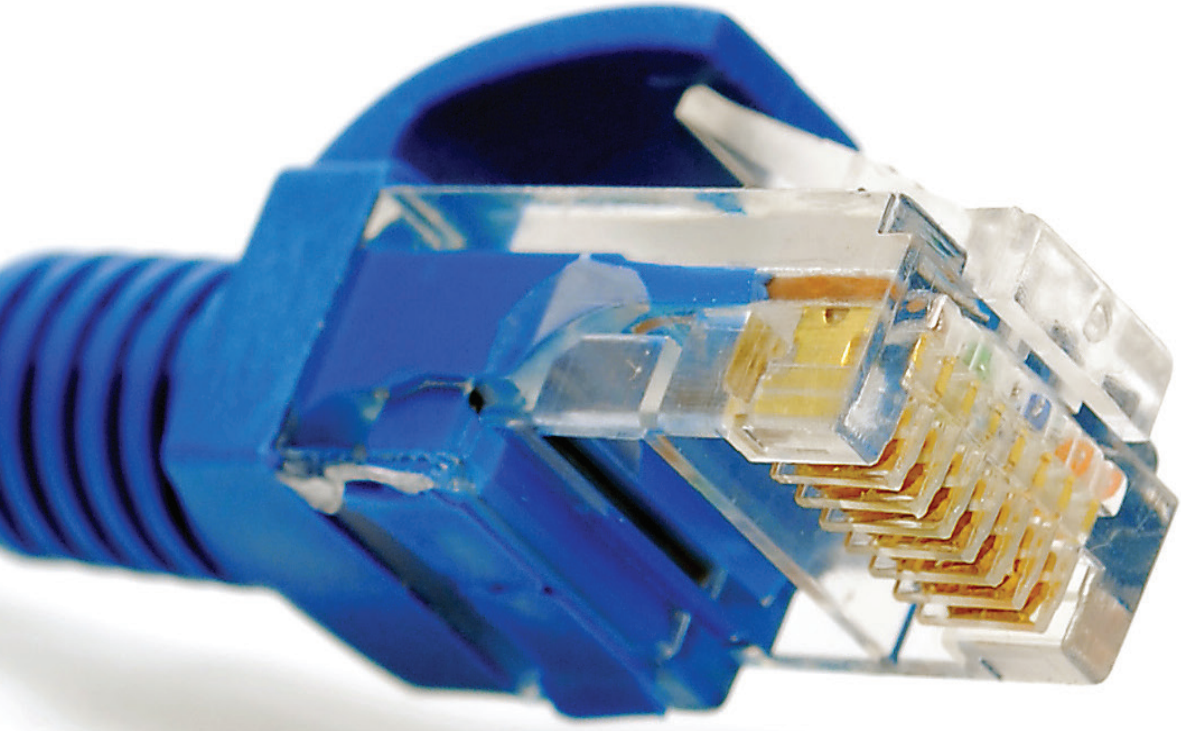
Универзитет
Сингидунум

Младен Веиновић
Александар Јевремовић

РАЧУНАРСКЕ МРЕЖЕ



Београд, 2020.

УНИВЕРЗИТЕТ СИНГИДУНУМ

Факултет за информатику и рачунарство

Младен Веиновић

Александар Јевремовић

РАЧУНАРСКЕ МРЕЖЕ

Седмо издање

Београд, 2020.

РАЧУНАРСКЕ МРЕЖЕ

Аутори:
др Младен Веиновић
др Александар Јевремовић

Рецензенти:
др Милан Милосављевић
др Бранко Ковачевић

Издавач:
УНИВЕРЗИТЕТ СИНГИДУНУМ
Београд, Данијелова 32
www.singidunum.ac.rs

За издавача:
др Милован Станишић

Лектор:
Данило Јевремовић

Техничка обрада:
Александар Јевремовић

Дизајн корица:
Александар Михајловић

Година издања:
2020.

Тираж:
1500 примерака

Штампа:
Бирограф, Београд

ISBN: 978-86-7912-626-9

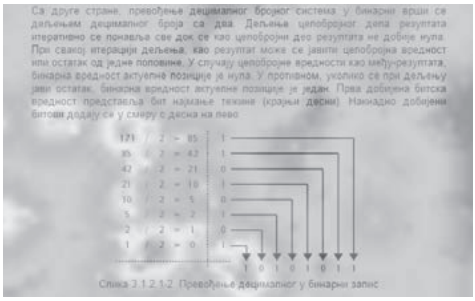
Садржај

Предговор другом издању

Поштоване колеге,

пред вама је друго, значајно измењено издање уџбеника „Рачунарске мреже“. Разлози за измене у овом издању су вишеструки. Као прво, у обзир су узете све сугестије читалаца - студената, професора и професионалаца који се баве рачунарским мрежама. Ове сугестије су нам достављене на различите начине - неке на предавањима, неке у разговорима са колегама на стручним и научним скуповима, а неке путем Веб сајта *www.racunarskemreze.com*, на ком је претходно издање уџбеника објављено у целини, као интерактиван материјал.

На основу претходног издања уџбеника извели смо једно, не баш уобичајено мерење. На поменутом Веб сајту уџбеника инсталирали смо компоненту за праћење курсора миша читалаца, метод који је алтернатива праћењу погледа. На основу података добијених овим методом утврдили смо који делови уџбеника су читаоцима занимљиви, а које делове прескачу. Ови налази су интензивно коришћени у измени постојећих и изради нових делова за ово издање.



Слика 3.1.2.1-2 Превођење децималног у бинарни запис

Следеће што је утицало на измене у овом издању је и издавање два нова уџбеника из ове области од стране Универзитета Сингидунум. То су уџбеници „Интернет технологије“ и „Заштита у рачунарским мрежама“. Појављивањем ових уџбеника неки делови претходног издања су постали сувишни, имајући у виду да тамо далеко детаљније обрађени.

Искрено се надамо да ће вам и ово издање бити корисно, барем колико и претходно. Такође, и надаље очекујемо сарадњу са вама, у виду указивања на евентуалне уочене грешке, предлога за даља унапређивања, као и препоручивања уџбеника другим потенцијалним читаоцима.

Београд, 2016. године Аутори

Предговор првом издању

Уџбеник „Рачунарске мреже“ намењен је студентима Факултета за информатику и рачунарство Универзитета Сингидунум за припрему испита из предмета „Рачунарске мреже“, а може се користити и као уводни материјал за савладавање градива из предмета који се односе на Интернет технологије и Веб сервисе. Резултат је вишегодишњег искуства аутора у областима умрежавања, мрежног и Интернет програмирања, комуникација и заштите података у рачунарима и рачунарским мрежама. Поред своје основне намене уџбеник може да буде од користи свим инжењерима који се у пракси сусрећу са умрежавањем, пројектовањем, инсталацијом и администрирањем рачунарских мрежа.

Читаоци ће у овом уџбенику наћи основне концепте и принципе умрежавања, опис слојевите архитектуре и функције појединих слојева као и њихове протоколе, али и детаљне приказе најважнијих Интернет протокола и Веб сервиса на апликативном нивоу. Програмерима ће бити од користи за боље разумевање различитих технологија за развој мрежних апликација које се ослањају на системске позиве и наменске библиотеке чијом применом се поштују строго дефинисани стандарди у савременим рачунарским мрежама.

У уводном делу уџбеника дати су основни појмови о умрежавању и анализиране су главне комуникационе функције које постоје код свих мрежа, независно од њихове величине. Уводи се појам рачунарских протокола и прецизније се разматрају два основна принципа у њима која се односе на пренос података са успоставом и без успоставе везе. Разматрају се реални комуникациони канали у којима постоје различите врсте сметњи и које морају на адекватан начин да буду третиране (технике за спречавање, откривање и исправљање грешака насталих током преноса). Затим се представљају најважније организације и модели за стандардизацију у овој области.

Подела рачунарских мрежа се може извршити на више начина, а у овој књизи су разматране поделе у односу на комуникационе медијуме, топологију, величину и функционални однос чланова у мрежи. У наставку се преко *OSI* и *TCP/IP* модела обрађује слој приступа мрежи, мрежни и транспортни слој и слој апликација. На физичком слоју анализирају се и жичне и бежичне комуникације, а на слоју везе података основне технике за приступ комуникационом медијуму као и технике за управљање током преноса података. У оквиру мрежног слоја детаљно су приказане технике адресовања по стандардима *IPv4* и *IPv6*, као и карактеристични протоколи на овом слоју: *ICMP* и *IGMP*. Од читаоца се захтева да добро разуме различите врсте *IP* адреса (приватне, јавне, статичке, динамичке) до нивоа да може правилно да изврши додељивање валидних *IP* адреса појединим сегментима (подмрежама)

једне рачунарске мреже. Посебно детаљно су разматрани протоколи рутирања *IP* пакета кроз чворове рачунарске мреже и дискутовани су релевантни проблеми за постизање ефикасности и правичности у рутирању. У оквиру транспортног слоја, који је одговоран за испоруку пакета са краја на крај мреже, разматрана су два основна протокола - *TCP* и *UDP*. Дискутоване су услуге које се дају апликативном слоју, а у њиховој основи су поузданост, перформансе, контрола загушења и брзине преноса датаграма.

Слој апликације је детаљно обрађен. Приказани су најпопуларнији сервиси на овом слоју као што су електронска пошта, Интернет телефонија и други. Указујемо на детаљно објашњено функционисање *DNS* и Веб сервиса као данас најшире прихваћених сервиса на Интернету. Ослањајући се на претходна разматрања рачунарских мрежа приказане су серверска и клијентска страна Веб сервиса, технике јединственог адресовања докумената на Интернету и пратећи протоколи. Књига обухвата и основе безбедности и доступности ресурса у мрежи кроз анализу могућих напада, улогу фајервола и система за откривање и спречавање напада. На крају је дат приказ мрежне подршке за Линукс оперативни систем.

Специфичности овог издања чине избор ћирилице за основно писмо при његовој изради и инсистирање на превођењу страних израза. За овакав приступ одлучили смо се из два разлога. Први је жеља да студенти знање стечено путем овог уџбеника што јасније увежу са разумевањем комуникације и да разграниче њене суштинске принципе од конвенција. Други разлог је омогућавање читаоцима исправног спеловања страних израза кроз њихово јасно визуелно издвајање и упућивање на језик коме припадају. У том циљу смо увели правило писања страних израза курзивом, уз навођење језика при њиховом првом појављивању у тексту.

Овај уџбеник је логичан наставак претходног, под називом „Увод у рачунарске мреже“. На основу повратних информација од шире стручне јавности, позитивних критика читалаца штампаног и електронског издања, као и чињенице да се претходни текст интензивно користио и изван Универзитета Сингидунум као помоћни уџбеник за припрему испита везаних за област рачунарских телекомуникација, аутори су покушали да допуне материјал и да га још боље прикажу. Због тога је књига значајно реорганизована. Неки наслови су изостављени, други су појачани и исправљени, а поједини су потпуно нови. За евентуалне недостатке у овом уџбенику сугестије читалаца биће добродошле. Аутори ће се потрудити да се комуникација са читаоцима појача јавним објављивањем текста овог уџбеника и остављањем простора за предлоге и допуне, а све у циљу што квалитетнијег и приступачнијег савладавања ове тешке и сложене гране рачунарства.

Београд, 2011. године Аутори

1. Принципи рачунарских телекомуникација

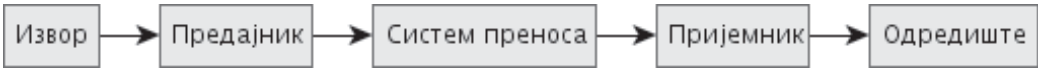
Рачунарске телекомуникације представљају један од облика комуникација, односно комуникацију на даљину остварену путем коришћења рачунара. Иако се често узимају за један од најсавременијих резултата развоја цивилизације, оне не решавају ни један од суштинских проблема везаних за комуникацију, већ представљају строго технолошки напредак. Ипак, такав напредак је посредно довео до многих напредака у областима невезаним за рачунарске технологије, као и до одређених социолишких, културолошких и других феномена.

Основни принципи рачунарских телекомуникација условљени су принципима везаним за комуникацију уопште и принципима везаним за рачунарство уопште. У овом поглављу су представљени основни принципи рачунарских телекомуникација, првенствено са аспекта принципа рачунарских система и технологија за комуникацију на даљину.

1.1. Пренос података

Рачунарска мрежа се може посматрати као комуникациони систем, где се информација генерисана на предајној страни (извориште поруке) доставља жељеном одредишту. Основни елементи комуникационог система су:

- Извор (*source*) – генерише податаке за пренос.
- Предајник (*transmitter*) – трансформише генерисане податке у облик погодан за пренос (нпр. модем дигиталне податке из рачунара трансформише у аналогни сигнал који се може пренети преко јавне телефонске мреже).
- Преносни систем (*tramission sistem*) – може бити једноставна линија или комплексна мрежа која спаја извор и одредиште.
- Пријемник (*receiver*) – прихвата сигнал из преносног система и трансформише га у облик погодан за одредиште.
- Одредиште (*destination*) – прихвата пренете податке.



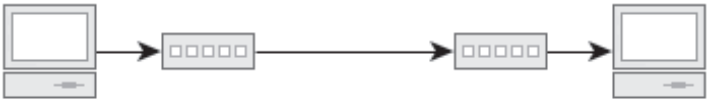
Слика 1. Модел комуникационог система.

Описани модел представља општи модел комуникације и може се, поред на комуникације у рачунарским мрежама, применити на било коју комуникацију. На пример, у разговору двоје људи, извор информације је ум говорника. Он

информацију кодује у гласовну поруку коју шаље коришћењем гласних жица. Систем преноса је ваздух који осцилује, а пријемник је уво слушаоца. Одредиште послате поруке је њена реконструкција у уму слушаоца.

Слика 2. Модел гласовне комуникације.

Једноставан пример реализације описаног модела у рачунарским мрежама јесте повезивање два рачунара путем јавне телефонске мреже и модема. При преносу података у том случају један рачунар је њихов извор. Подаци се прослеђују предајнику - модем у овом случају - који их припрема за слање а затим и шаље.



Слика 3. Модел модемске рачунарске комуникације.

Систем којим се подаци преносе јесте јавна телефонска мрежа, односно њени канали. Модем на другој страни представља пријемника података. Подаци се након пријема и декодовања прослеђују одредишту - пријемном рачунару.

1.1.1. Кодовање података, сигнали и медији

Комуникациони системи служе за пренос порука од изворишта до одредишта преко одређеног комуникационог медијума. Поруке се састоје од података, а подаци се кодују (представљају) сигналима који одговарају датом комуникационом медијуму. У реалним условима преноса на комуникационом медијуму постоји шум који утиче на сигнале којима се врши пренос података. Сигнали којима се преносе подаци су реални физички сигнали (струја, светлост, електромагнетни радио сигнали итд.), који имају одговарајуће слабљење са растојањем, брзину и самим тим уносе одговарајуће кашњење од изворишта до одредишта. Циљ комуникације је да се у задатим временским условима информација пренесе у неизмењеном облику, са што мањим кашњењем.

Информације које се преносе могу бити у аналогном (говор, музика, видео) или дигиталном облику (рачунарски подаци). Такође, сигнали којима се преносе

подаци могу бити аналогни или дигитални. Постоје четири могућа случаја: пренос аналогних података аналогним и дигиталним сигналима и пренос дигиталних података аналогним и дигиталним сигналима.

Аналогни подаци аналогни сигнали. Код овог типа преноса ради се модулација аналогних сигнала из два разлога:

1. Сигнали виших фреквенција имају боље карактеристике у преносу кроз одговарајући комуникациони медијум
2. Омогућава се фреквенцијско мултиплексирање различитих података кроз исти комуникациони медијум

Аналогни подаци се модулишу сигналом носиоцем који је обично више фреквенције. Типови модулације су амплитудска, фазна и фреквенцијска .

Аналогни подаци дигитални сигнали. Код ове врсте преноса врши се тзв. аналогно дигитална конверзија. Најпознатији кодери овог типа су PCM (*pulse code moduzlation*), DM (*delta modulation*) и други који се још зову и кодери таласног облика. Заснивају се на дискретизацији, квантизацији и кодирању добијених вредности. Поред ових техника познате су и технике дигитализације које улазе у природу произвођења сигнала који се кодује, а њихов циљ поред дигитализације је компресија сигнала. Наиме, таласни кодери говорног сигнала као резултат дају дигитални сигнал одговарајуће битске брзине која често превазилази могућности комуникационог канала (канал са ограниченим фреквенцијским опсегом). На пример, за пренос говора кроз мобилну телефонију се не користе кодери говорног сигнала који се заснивају на таласном облику (PCM, 64kb/s) већ се користе вокодери говора (IMBE *vocoder*, 13,6 kb/s). У нашем окружењу су углавном аналогни сигнали (температура, притисак, електрична струја, говор, музика, видео и сл.) и за потребе рада у реалном времену неопходна је аналогно дигитална конверзија.

Дигитални подаци аналогни сигнали. Класичан пример је пренос рачунарских података преко јавне телфонске комутиране мреже (PSTN). Ради се о преносу дигиталних података путем аналогних сигнала. За пренос се користе модеми (уређаји који врше модулацију на предаји и демодулацију на пријему). Позната су три типа модулације, зависно од тога на коју карактеристику синусоидалног носиоца се утиче: амплитудска (*amplitude shift keying,* ASK), фреквенцијска (*frequency shift keying,* FSK) и фазна (*phase shift keying* PK) .

Дигитални подаци дигитални сигнали. Постоје различите технике којима се дигитални подаци кодирају дигиталним сигналима. Циљ свих ових техника је да се постигне боље искоришћење комуникациуоног канала (пренос што веће

количине података кроз ограничен комуникациони канал), да се постигне већа отпорност у преносу на утицај шума на комуникационом каналу, да се омогући битска синхронизација на пријемној страни и сл. Познате технике кодирања овог типа су: *Nonreturn to Zero-Level* (NRZ-L), *Nonreturn to Zero Inverted* (NRZI), *Bipolar –AMI*, *Pseudoternary*, *Manchester*, *Differential Manchester*, B8ZS, HDB3 .

Медијуми преко којих се преносе сигнали могу бити жични (електрични и оптички каблови) или бежични (ваздух, вода, вакум и сл.). Сваки од медијума се карактерише пре свега пропусним опсегом (ширином фреквенцијског опсега канала) који ограничава максималну брзину преноса сигнала. Пропусни опсег медијума може бити у основном опсегу (од 0 Hz до максималне горње граничне учестаности) или у неком вишем опсегу (карактерише га доња и горња гранична учестаност). Код преноса сигнала се у овим случајевима говори о преносу у основном опсегу (baseband) или неком другом (транспонованом) опсегу, а устаљени термин је тзв. рад у проширеном спектру.

Важна карктеристика медијума је слабљење сигнала са растојањем. Ако се за пренос података користе аналогни сигнали, на одређеном растојању је неопходно да постоје појачивачи сигнала. Њихова основна мана је да са сигналом појачавају и шум, те после неколико деоница шум постаје јачи од сигнала. Код преноса дигиталних сигнала на одређеном растојању се врши регенерација сигнала (препознавање, обнављање и поновно генереисање) што практично омогућава пренос дигиталног сигнала без ограничења растојања.

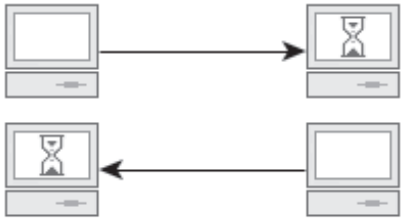
1.1.2. Усмереност комуникације

Са аспекта усмерености комуникације (могућих смерова у којима се преносе подаци) она се може поделити на једносмерну, полу-двосмерну и потпуно двосмерну. Једносмерна комуникација или симплекс (енгл. *simplex*) подразумева постојање предајника на једној страни комуникације и пријемника на другој.

Слика 1. Једносмерна комуникација - симплекс

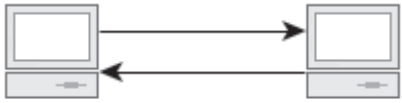
Код двосмерне комуникације обе њене стране су опремљене примопредајником, односно и предајником и пријемником. Уколико примопредајници могу у једном тренутку да раде само као пријемници или

само као предајници, односно или да примају или да шаљу податке, таква комуникација се назива полу-дуплексом (енгл. *half-duplex*).



Слика 2. Полу-двосмерна комуникација - полу-дуплекс

Насупрот томе, уколико примопредајници могу истовремено да раде и као предајници и као пријемници, односно да истовремено и шаљу и примају податке, таква веза се назива пуним дуплексом (енгл. *full duplex*).



Слика 3. Потпуна двосмерна комуникација - фул-дуплекс

Савремене рачунарске телекомуникационе технологије углавном нуде неку врсту двосмерне комуникације. Међутим, постоје и занимљиви савремени приступи (нпр. *Li-Fi*) за масовно коришћење једносмерних комуникација (на пример, за синхронизацију уређаја).

1.1.3. Комутација веза и пакета

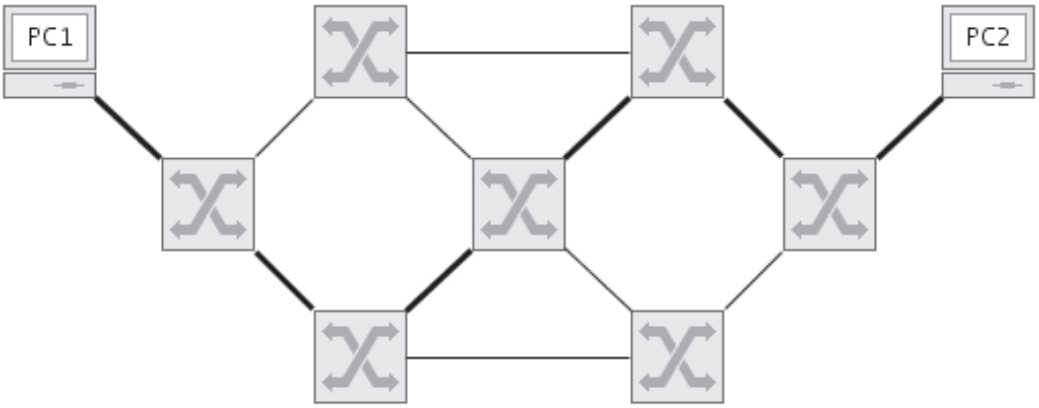
У рачунарским мрежама постоје два основна начина преноса података. Код првог начина, који је старији, веза између изворишта поруке и одредишта успоставља се кроз чворове мреже, на начин да се заузима комплетан спојни пут. Карактеристичан пример је јавна телефонска комутирана мрежа.

Други тип је пакетски начин преноса, где се порука дели у мање целине – пакете (оквире), а кроз мрежу се пакети могу преусмеравати по различитим спојним путевима. Овакав начин преноса је карактеристичан код Интернета. Постоји и трећи начин преноса података, а односи се на пакетски пренос података где сви пакети пролазе исти спојни пут.

1.1.3.1. Пренос података са комутацијом веза

Код преноса података са комутацијом веза (енгл. circuit switched) између два

учесника у комуникацији успоставља се чврста директна веза, а укупна информација се преноси путањом која је утврђена у току успоставе везе. На пример, ако рачунар PC1 жели да комуницира са рачунаром PC2 прво се успоставља веза између ова два рачунара и та веза постоји само за дати пренос података.



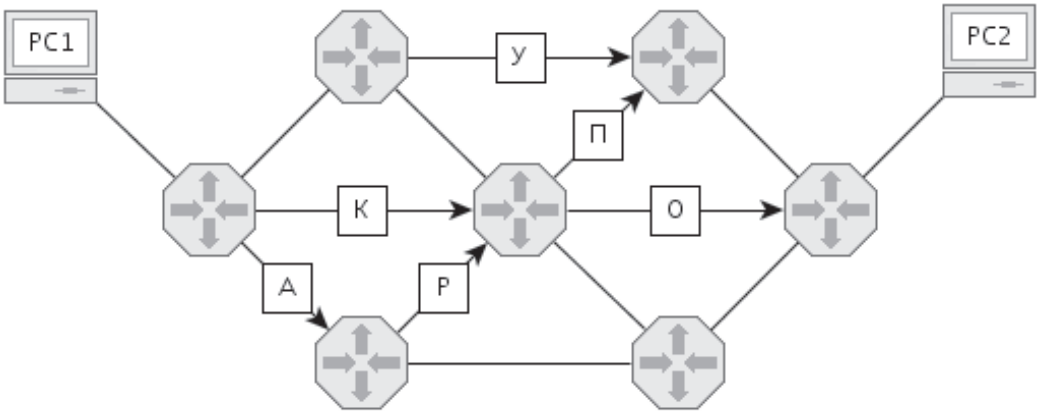
Слика 1. Пренос података са комутацијом веза

Ако неки трећи рачунар пожели да комуницира са рачунаром PC2 у том тренутку, то неће бити могуће по истом спојном путу. Такође, комуникација било која друга два учесника не може да се одвија заузетим спојним путем. Основна карактеристика оваквог начина преноса података је да се подаци могу преносити успостављеном везом максималном брзином која је могућа, тј. у потпуности се може користити комплетан фреквенцијски опсег успостављеног спојног пута (комуникационог канала) за пренос података.

1.1.3.2. Пренос података са комутацијом пакета

Код преноса података са комутацијом пакета (енгл. packet switched) између два учесника, прво се информација која се размењује дели у пакете чија структура (дужина пакета, редни број, адреса одредишта, приоритет и сл.) одговара носећим протоколима. Пакети се упућују до првог чвора у мрежи (рутера), а у сваком рутеру се врши независно усмеравање пакета. Избор путање у рутерима се врши на основу више критеријума који важе у датом тренутку. Пакети пролазе различите путање од изворишта до одредишта. На одредишту се врши слагање пакета у првобитан редослед да би се добила потпуна информација. Овакав начин преноса података је карактеристичан за рачунарске мреже где већину мрежног саобраћаја чине кратки налети података са празним простором између и који су обично временски дужи од "попуњених". Суштина оваквог

начина преноса података је да се у празним просторима могу слати пакети које шаље неки трећи учесник. Дакле, подаци од различитих извориштa могу пролазити истим спојним путем.



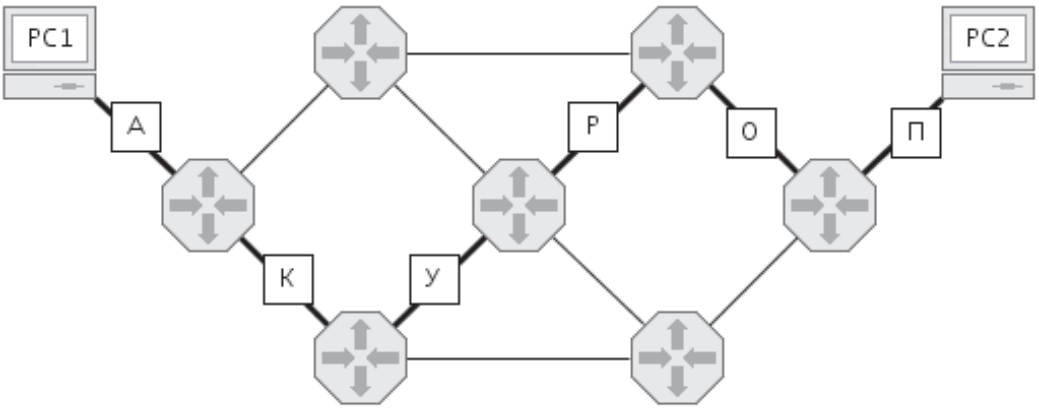
Слика 1. Пренос података са комутацијом пакета

Ово је далеко „жилавији“ начин преноса, зато што пакети најчешће могу да нађу бар један слободан спојни пут. Мана је што је ефективна брзина слања података на овај начин мања од максималне коју дозвољава пропусни опсег канала, зато што га користе више учесника у комуникацији.

1.1.3.3. Пренос података виртуалном везом

Пренос података виртуалном везом (енгл. virtual circuit) такође се односи на пакетски пренос. Међутим, пакети се усмеравају на исти спојни пут између два рачунара. Виртуелна кола су перманентног типа што значи да када се једном дефинишу путање, ретко или никада се не мењају. Ово је заправо софтверска замена за хардверска решења овог типа. Подаци и даље путују кроз мрежу (повезани чворови) али тачно одређеном путањом. Сваки пакет, поред карактеристичних поља које носи, има и обележје које указује на дату виртуелну везу. Скоро све мреже које имају интензиван саобраћај на мрежи користе ову методу дефинисања путање.

Предност оваквог начина преноса пакета је да се крајњим апликацијама може обезбедити одговарајући квалитет услуге. На пример, код интерактивног преноса говора кроз мрежу, важно је обезбедити да пакети података, којима је кодован говор, до пријемника стижу истом брзином, тј. да не постоји варијација у кашњењу.



Слика 1. Пренос података виртуалном везом

У мрежама са комутацијом пакета, поједини пакети могу да проналазе драстично различите путање (различито време преноса), што може довести до проблема на пријему – неразумљив говор. Само виртуелним колима се може обезбедити захтевани квалитет услуге. Због преноса кроз мрежу постоји кашњење, али је оно идентично за све пакете и за дати сигнал није од интереса.

1.1.4. Адресовање у рачунарским мрежама

Адресовање у рачунарским мрежама се одвија на више нивоа. На пример, адресовање на физичком нивоу се користи за одређивање ком уређају треба упутити одређене сигнале, односно који уређај треба да обради примљене сигнале. Затим, постоји логичко адресовање које се користи у међумрежној комуникацији, за утврђивање којом путањом је оптимално доћи до мреже у којој се одредиште налази. Коначно, овакви системи адресовања нису интуитивни за људску употребу, тако да се на највишем нивоу налази симболичко адресовање.

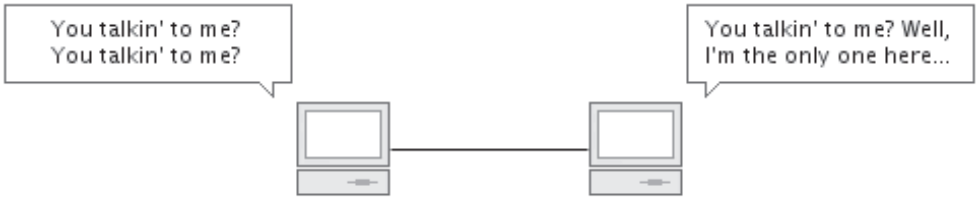
Замислимо да се у рачунарској мрежи, повезаној са Интернетом, налази рачунар који ради као сервер. Физика адреса тог рачунара је F4:6D:04:03:3D:FF, њему је додељена IP адреса 212.62.45.222 а домен www.singidunum.ac.rs води на ту IP адресу. Дакле, корисници ће за приступ ресурсима и сервисима на овом рачунару користити симболичку адресу - www.singidunum.ac.rs - као најједноставнију за људску употребу и памћење. Ова адреса ће на рачунарима корисника аутоматски бити преведена у логичку адресу 212.62.45.222 да би се могла утврдити путања Интернет мреже преко које се може доћи до мреже у којој се налази сервер са том адресом. Када захтеви корисника стигну до мреже у којој се сервер налази, они ће серверу бити испоручени коришћењем физичке

адресе F4:6D:04:03:3D:FF и технологије на којој се та мрежа заснива (нпр. Етернет).

Наведена три основна типа адресовања се такође могу назвати и хоризонталним адресовањем (односно хијерархијским у случају симболичког адресовања) јер се на основу њихових адреса умрежени рачунарски системи и уређаји раздвајају једни од других. Са друге стране, постоји велики број параметара у рачунарским комуникацијама који служе за усмеравање података током преноса. На пример, у заглављу Етернет оквира дефинисан је протокол вишег нивоа коме треба проследити садржај на обраду, у пакетима Интернет протокола су дефинисани порт и транспортни протокол, итд.

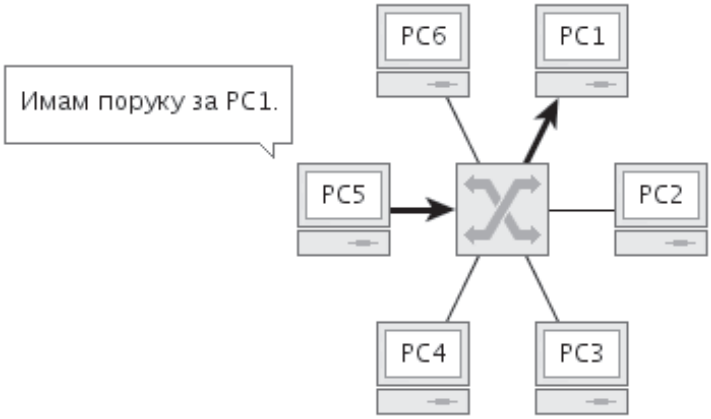
1.1.4.1. Број прималаца

Проблем адресовања прималаца не постоји у једноставним мрежама, типа тачка-тачка, које се састоје од само два члана. У таквим мрежама сви подаци, послати од стране једног учесника, стижу до другог члана, као и обрнуто. Међутим, код комуникација у мрежама са сложенијим топологијама, постоји више модела комуникације са аспекта броја прималаца.



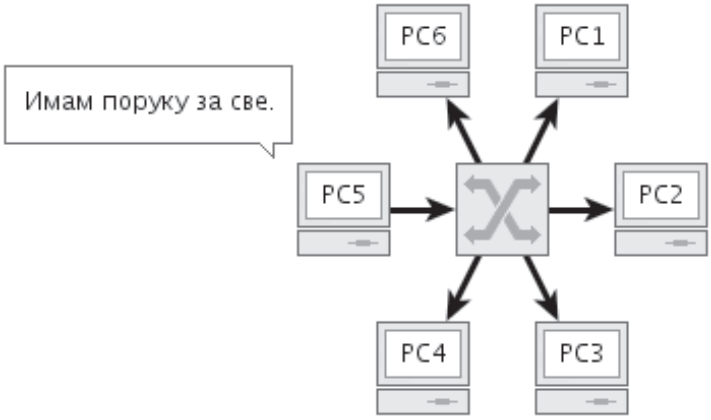
Слика 1. Код мрежа типа тачка-тачка адресовање је једноставно.

Подразумевани модел слања података у рачунарским мрежама је уникаст, односно слање података само једном примаоцу у мрежи. Иако овај модел делује најједноставније, он то, у принципу, није. Углавном је захтевно, а често и немогуће (на пример, у бежичним мрежама), податке усмерити само до једног члана мреже. Из тог разлога неке технологије (на пример, Етернет) у својим ранијим и једноставнијим варијантама користе дифузно слање, а тек са увођењем напреднијих уређаја имају могућност усмереног слања, појединачним примаоцима.



Слика 2. Слање података јединственом примаоцу.

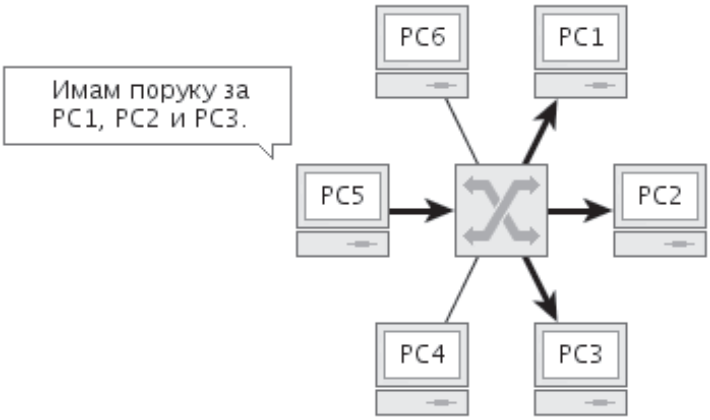
Дифузно или емисионо слање података (енгл. *broadcast*) је слање код кога сви чланови мреже добијају по једну, идентичну копију послатих података. Овај тип слања се углавном користи код испитивања, односно упита на које потенцијално може да одговори било који члан мреже. Неке мрежне технологије симулирају усмерену комуникацију путем дифузног слања података на физичком нивоу и филтрирања на страни примаоца, што у главном има негативан утицај на перформансе и приватност.



Слика 3. Слање података свим члановима локалне мреже.

У рачунарским телекомуникацијама често постоји потреба да се иста порука пошаље вишеструким, али не и свим примаоцима у мрежи. Овакав начин слања података назива се мултикастинг (енгл. *multicast*) и углавном се реализује додатним протоколима (за управљање чланством у групама прималаца) и коришћењем специјалних адреса које се односе на групе, пре него на

појединачне примаоце. Коначно, исти ефекат као и слање вишеструким примаоцима може се постићи и вишеструким слањем исте поруке појединачним примаоцима. Међутим, на такав начин се вишеструко заузима комуникациони канал, повећава кашњење и додатно десинхронизује комуникација, те је такав приступ углавном пожељно или чак неопходно избећи.

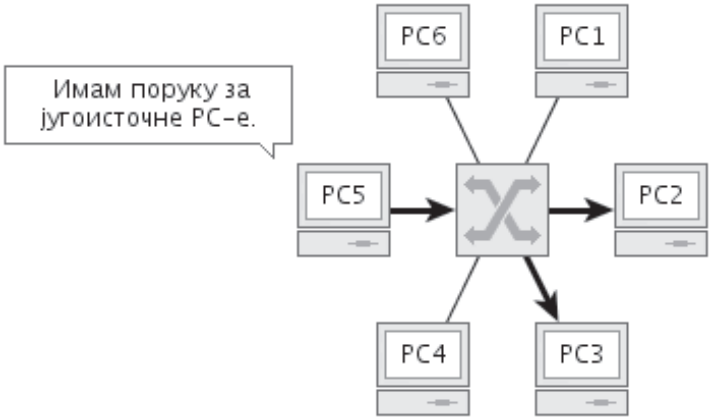


Слика 4. Слање података вишеструким примаоцима.

Још један посебан начин слања порука је слање код кога је потребно да послате податке прими један, и то било који, прималац из групе прималаца (енгл. *anycast*). Такав приступ се често користи у ситуацијама када, најчешће услед великог оптерећења, на истом задатку ради већи број чланова мреже (на пример, већи број Веб сервера је ангажован за испоруку сервиса које нуди компанија Гугл). Овај модел се углавном не реализује на нивоу пошиљаоца, већ на некој тачки која посредује у комуникацији (на пример, *DNS* сервер који клијенте усмерава на један сервер из дефинисане групе).

Слика 5. Слање података било ком из групе примаоца.

Интернет, као глобална рачунарска мрежа, омогућава комуникацију између било која два њена члана, без обзира на то где се они географски налазе. Међутим, у ситуацијама када је то могуће, комуникација између географски ближих тачака углавном има боље перформансе (бржи пренос, мање кашњење, нижи трошкови и слично). Из тог разлога, компаније чије Веб сервисе користи велики број клијената из свих делова света, често поседују сервере у дата-центрима у различитим деловима света, а клијенти се усмеравају на њима најближе. Оваква комуникација, која у обзир узима и географску локацију њених учесника, назива се гео-кастинг (енгл. *geocast*).



Слика 6. Слање података географски одређеној групи прималаца.

Ипак, треба имати у виду да са аспекта класичне рачунарске мреже и њених чланова географска компонента не постоји - постоји само логичка топологија, број посредника и подужно слабљење сигнала. У складу са тим, геокастинг је изведени тип скупа прималаца који се на вишем нивоу реализује додатним протоколима, а нижем нивоу, на пример, мултикастингом.

1.1.5. Протоколи

Пренос података кроз мрежу обавља се по протоколима – утврђеним правилима која су позната свим учесницима у комуницирању. Протокол представља стандард (конвенцију) за остваривање и контролу везе и пренос података између две крајње тачке. Комуникациони протокол је скуп стандардизованих правила за представљање података, сигнализацију, проверу аутентичности и контролу грешака, неопходних за пренос информација комуникационим каналом.

Кључни елементи протокола којим се договара спремност за слање, спремност

за пријем, формат података и сл. су:

1. синтакса - формат података и нивои сигнала,
2. семантика – контролне информације у преносу и контрола грешака,
3. тајминг – брзина преноса.

Размена података у рачунарској мрежи је изузетно сложена. Са повећањем броја умрежених рачунара који комуницирају и са повећањем захтева за све савршенијим услугама (сервисима) неопходно је и усавршавање протокола. Посао комуницирања је толико сложен да је било неопходно развити протоколе у више слојева. Сваки слој је намењен за један одговарајући посао. Код првобитних рачунарских мрежа умрежавање се вршило зависно од произвођача рачунарске опреме. Сав хардвер и софтвер су били везани за једног произвођача тако да је било веома тешко вршити измене, унапређивања мреже, и све је било изузетно скупо. Увођењем стандарда за комуницирање по логички јасно дефинисаним слојевима, појавило се више произвођача софтверске опреме. Стандардима се омогућило комбиновање хардвера и софтвера од различитих произвођача, што је све заједно довело до пада цена опреме и софтвера за умрежавање и до повећања квалитета услуга у мрежама.

Једна од најбитнијих ствари код умрежавања је адресовање. Ако се посматрају само два рачунара, нема потребе за адресовањем, јер све што се пошаље са једног рачунара намењено је другом. Већ када мрежу чине три рачунара, појављује се потреба за адресовањем. Послати подаци са једног рачунара могу бити намењени једном од преостала два рачунара. Додатно усложњавање настаје ако се посматра више апликација на једном рачунару, које могу да комуницирају са више апликација на другом рачунару. Овде није довољно само адресовати рачунар, већ и апликацију са којом се комуницира.

Кораци протокола морају да се спроведу у складу са редоследом који је исти за сваки рачунар у мрежи. У предајном рачунару ови кораци се извршавају од врха ка дну. У пријемном рачунару ови кораци морају да се спроведу у обрнутом редоследу. На предајном рачунару протокол:

- дели податке у мање целине, назване пакети, које може да обрађује,
- пакетима додаје адресне информације тако да одредишни рачунар на мрежи може да одлучи да ли они припадају њему, и
- припрема податке за пренос кроз мрежну картицу и даље кроз мрежни кабл.

На пријемном рачунару протоколи спроводе исти низ корака, али обрнутим редоследом:

- преузимају се подаци са кабла,
- кроз мрежну картицу уносе се пакети података у рачунар,
- из пакета података уклањају се све информације о преносу које је додао предајни рачунар,
- копирају се подаци из пакета у прихватну меморију (бафер) која служи за поновно склапање и
- поновно склопљени подаци прослеђују се апликацији у облику који она може да користи.

Основни принципи у дизајну протокола су ефикасност, поузданост (робустност) и прилагодљивост. Потребно је да оба рачунара, предајни и пријемни, сваки корак изведу на исти начин како би примљени подаци имали исту структуру какву су имали пре слања. У мрежи, више протокола мора да ради заједно. Њихов заједнички рад обезбеђује исправну припрему података, пренос до жељеног одредишта, пријем и извршавање. Рад више протокола мора да буде усаглашен како се не би догађали конфликти или некомплетне операције, односно некомплетан пренос информација. Резултат тог усаглашавања назива се слојевитост (*layering*).

Успостављање везе, пренос података и раскид везе одређени су сетом протокола од којих је сваки надлежан за један од следећих послова:

- *Handshaking* - успостављање везе;
- Преговарање о различитим карактеристикама везе;
- Дефинисање почетка и краја поруке;
- Дефинисање формата поруке.
- Дефинисање правила за обраду оштећених или неправилно форматираних порука (исправка грешака);
- Утврђивање неочекиваног прекида везе и дефинисање даљих корака у том случају;
- Прекид везе.

1.1.5.1. Протоколи без успостављања везе

При коришћењу протокола без успостављања везе иницијални корак при преносу података јесте само слање података. Овом кораку не претходи процедура везана за успостављање везе као што је то случај код протокола са успостављањем везе. Иако је успостављање везе најчешће особина протокола са поузданим преносом, постоје протоколи који омогућавају поуздан пренос без успостављања везе као и протоколи који не гарантују безбедан пренос иако користе успостављање везе.

1.1.5.2. Протоколи са успостављањем везе

При коришћењу протокола са успостављањем везе две стране морају да успоставе везу између себе као предуслов за размену података. Процес успостављања везе може се поредити са позивањем телефонског броја:

1. Страна која позива иницијализује линију (подизањем слушалице) и уноси одредишни број.
2. Након позива броја успоставља се веза која још увек није адекватна за пренос података и чека се на примаоца позива да подигне слушалицу.
3. Након подизања слушалице прималац позива обавештава позиваоца да је спреман за размену података сигналом "хало".
4. Након примања сигнала "хало" веза адекватна за пренос података је успостављена и размена може да почне.

Јасно је да процедура потребна за успостављање везе захтева одређено време и ангажовање обе стране. Међутим, она обезбеђује поузданији (али не и потпуно поуздан) пренос података и умањује могућност грешке. Успостављање везе се практикује код протокола који имају за циљ да осигурају поуздан пренос података. Пример протокола који ради са успостављањем везе је *TCP* (*Transmission Control Protocol*). Протоколи сервиса код којих су перформансе битније од поузданог преноса података најчешће не укључују успостављање везе.

1.2. Управљање грешкама

Управљање грешкама односи се на механизме који откривају и исправљају грешке које се јављају током преноса података. Постоји могућност појављивања два типа грешака и то: промењен податак и изгубљен податак. Грешке на комуникационом каналу су неминовне код реалних комуникација и настају због различитих врста шумова или проблема у преносу.

Ниједна мрежа не може у потпуности да одстрани грешке, али већина грешака може бити спречена, откривена и евентуално исправљена. Ниво грешке представља један погрешан бит на *n* послатих битова (нпр. 1 на 500.000). Грешке се обично појављују у групама. У групним грешкама, више битова је нарушено у исто време и грешке нису униформно распоређене. Основне функције контроле грешака су спречавање и откривање њиховог настајања, као и њихово исправљање.

1.2.1. Извори грешака

Основни узроци грешака су шум на линији и деградација сигнала. Код жичних мрежа шум је непожељан електрични сигнал који се јавља на комуникационом каналу. Може се очекивати на електричним медијима где се појављује као неочекиван електрични сигнал. Манифестује се на два начина и то: додатни битови – уметање или недостајући битови – брисање.

Постоји више врста извора грешака:

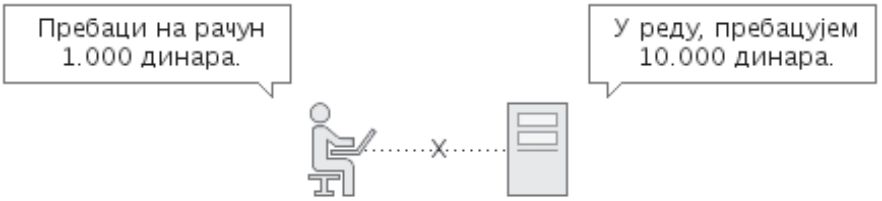
- Прекид линије; катастрофалан узрок грешке који онемогућава пренос. Често се прекиди дешавају на кратко време. Овај тип грешке могу да узрокују грешке уређаја, спољног прекида, губитак носећег сигнала, проблем са конекторима и сл.
- Бели Гаусов шум; настаје код свих електричних сигнала. Он не представља проблем све док не постане толико јак да надвлада процес преноса података. Као превенција повећава се снага сигнала којим се преносе подаци.
- Импулсни шум; основни узрок грешака приликом преноса података. Обично кратко траје, али је великог интензитета. Узрокују га нагле промене струје, а као превенција се врши оклопљивање каблова и евентуално њихово измештање.
- Преслушавање; узрокују га блиски каблови и недовољно размакнути опсези фреквенција. Као превенција, повећава се фреквенцијски опсег сигнала и врши се измештање каблова.
- Ехо; узрокују га лоше везе где се сигнал рефлектује (враћа) до извориште. Као превенција проверавају се конектори или подешавају уређаји.
- Слабљење; губитак јачине сигнала док се преноси од пријемника до предајника. Слабљење се повећава са растојањем, а као превенција се

употребљавају рипитери или појачивачи.

- Интермодулациони шум; у њему се сигнали из два независна тока података комбинују и стварају нов сигнал који упада у фреквенцију која је резервисана за други сигнал. Узрокује га сигнал настао комбинацијом из више преносних система, а као превенција употребљавају се оклопљени каблови и врши се њихово измештање.
- Џитер; узрокује промена аналогних сигнала (амплитуда, фреквенција, фаза) а као превенција се врши подешавање уређаја.
- Хармонијска изобличења; узрок су појачивачи који мењају фазу (некоректно појачање улазног сигнала), а као превенција се такође врши подешавање уређаја.

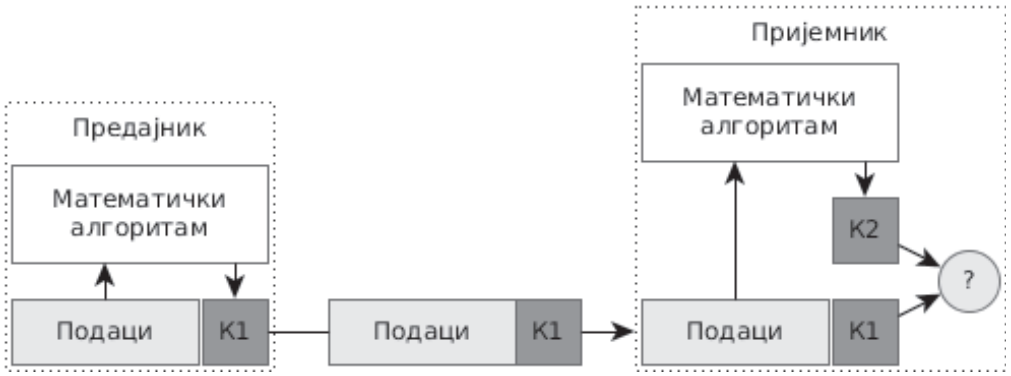
1.2.2. Откривање грешака

Један од кључних задатака у рачунарским телекомуникацијама је провера да ли су примљени подаци идентични послатима, односно да ли је током преноса дошло до њихове измене. Другим речима, потребно је утврдити да ли примљени податак садржи грешку, односно разлику у односу на послати податак. Отежавајућу околност за откривање грешака представља чињеница да прималац не поседује изворну поруку са којом би упоредио примљену поруку.



Слика 1. Утицај грешке код електронског банкарства

За потребе откривања грешака пошиљалац израчунава додатне битове и шаље их заједно са корисним подацима. Што се већи број битова користи као додатак корисним подацима, боље је откривање грешке али је и мања ефикасност преноса. Прималац из добијених корисних података израчунава додатак и пореди га са добијеним. Ако је додатак исти као што га је пошаљилац израчунао, нема грешке у преносу, а ако је различит, постоји грешка у преносу.

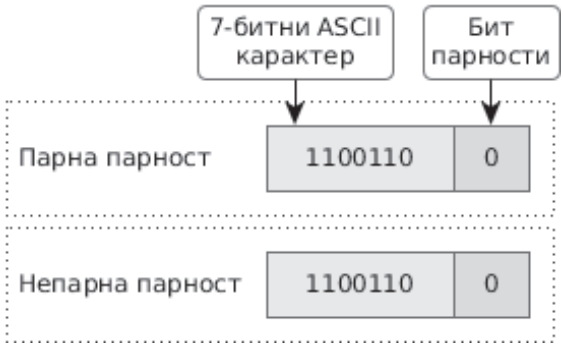


Слика 2. Техника откривања грешке

У технике за откривање грешака спадају провера парности, лонгитудинална редудантна провера (*Longitudinal Redundancy Checking, LRC*), и полиномијална провера (*Checksum, Cyclic Redundancy Check , CRC*).

1.2.2.1. Провера парности

Провера парности представља најстарији и најједноставнији метод детекције грешке где се један бит додаје сваком карактеру. Ако у карактеру који се преноси постоји паран број јединица и бит који је додат има вредност 0 то се назива парна парност (*even parity*). Ако у карактеру постоји паран број јединица и додаје се 1 то се назива непарна парност (*odd parity*).Пријемник прима карактер, поново рачуна бит и пореди га са добијеним битом парности. На овај начин се може уочити непаран број погрешних битова.



Слика 3. Пример провере парности

Овај једноставни метод детектује 50% грешака. Примена провере парности није ефикасна у присуству јаког шума.

1.2.2.2. Полиномијална редундантна провера

Код полиномијалне редундантне провере на крај поруке се додаје један или више карактера одређених математичким алгоритмом. У основне типове овакве провере спадају контролна сума (*Checksum*) и циклична редундантна провера (*Cyclic Redundancy Check, CR*C).

Контролна сума представља кôд детекције грешке заснован на операцији сабирања која се врши над карактерима који требају да се провере. Блок података над којим се рачуна контролна сума може да буде различите дужине, а сама контролна сума је увек исте дужине. Добар алгоритам за израчунавање контролне суме за мале промене у блоку података даје потпуно различите вредности контролне суме. Код најједноставнијег алгоритма контролна сума се израчунава сабирањем децималних вредности сваког карактера у поруци, укупна вредност се затим дели са 255 а остатак дељења (1 бајт) је контролна сума. Ефикасност контролне суме је 95%. Код *TCP/IP* модела контролна сума се примењује у протоколима *TCP* и *UDP* и дужине је 16 битова.

Циклична провера редундансе - (*Cyclic Redundancy Check, CRC*) резултат је математичког израчунавања. Она додаје поруци 8, 16, 24 или 32 бита. Порука се третира као један дуг бинаран број *P*. Пре преноса, слој везе података дели *P* фиксним бинарним бројем *G* и као резултат даје цео број *Q* и остатак *R/G*. Израчунава се и на полазном и на одредишном рачунару. Дакле, циклична провера редундансе се одређује израчунавањем следећег остатка:

$$P / G = Q + R / G$$

Остатак *R* додаје се поруци као карактер за проверу грешке при преносу. Пријемник дели примљену поруку са истим *G*, што за резултат даје *R*. Пријемник проверава да ли се примљено *R* слаже са стварним *R*. Ако се не слажу, сматра се да је дошло до грешке. *CRC* представља најјачу и највише употребљавану проверу и са њом се детектује 100% грешака ако је број грешака мањи или једнак од величине *R*. Наведена техника за детекцију грешке користи се на слоју везе података.

1.2.3. Исправљање грешака

Када се у примљеним оквирима детектује грешка она мора да се исправи или се такав оквир одбацује. Једноставан, ефикасан, јефтин и најчешће коришћени метод за корекцију грешке је ретрансмисија. Код овог поступка пријемник, када детектује грешку, тражи од предајника да поново пошаље поруку све док се порука не прими без грешке. Чест назив је аутоматски захтев за понављање

(*Automatic Repeat Request, ARQ*). Постоје два типа *ARQ* а то су: стани и чекај и континуални *ARQ*.

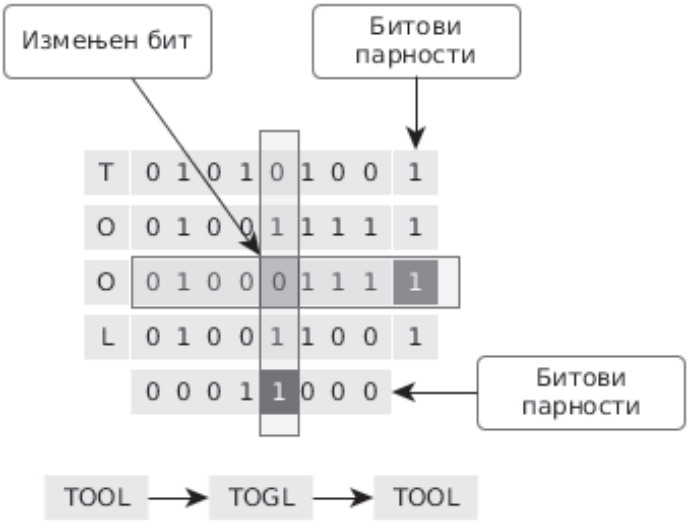
Корекција грешке унапред (*Forward Error Correction*) користи кодове који садрже довољно редудансе да се грешке на комуникационом каналу могу на пријему детектовати и исправити, без поновног слања. Додатни битови варирају од малог процента екстра битова до 100% редудансе. Кодови за корекцију грешке унапред, због додатних битова, смањују ефикасност преноса. Са друге стране, избегава се потреба за ретрансмисијом података. Обично се користи за сателитске комуникације. Пример за корекцију грешке унапред је Хамингов код. Кодови који се користе су ефикасни уколико грешка на комуникационом каналу не прелази услове под којима су дати кодови конструисани.

Постоје примери где се не врши корекција грешке иако се грешка детектује. Такав случај је код већине локалних рачунарских мрежа, где се исправљање евентуалних грешака препушта вишим слојевима *OSI* или *TCP/IP* модела. Захтеви за ретрансмисијом погрешно примљених података би захтевали увођење протокола који на сваки примљени оквир одговарају *ACK* или *NACK* поруком. Овакви компликовани протоколи би били веома неефикасни у жичним локалним рачунарским мрежама, где се претпоставља да су услови преноса добри и да је низак ниво евентуалног шума на комуникационим каналима, тј. мали је ниво очекиване грешке. Исти случај је код преноса података оптичким кабловима, где грешке практично и не постоје.

Насупрот томе, у бежичним системима је неопходно да се користе *ACK* или *NACK* потврде на сваки оквир, зато што су услови преноса података такви да је висок ниво грешке на комуникационом каналу (пренос електромагнетних таласа кроз ваздух). Ниво грешке у бежичним системима је такав да се унапред зна да је 10 до 20% оквира сигурно погрешно. Кад би се исправљање грешака препуштало нпр. транспортном слоју, вероватно да се пренос података никада не би завршио.

1.2.3.1. Дводимензионална провера парности

Код дводимензиналне провере парности додаје се бит парности на сваки карактер, а на крају блока података додаје се нови карактер, који се рачуна уздужно. Уколико се на преносном путу деси грешка, односно промена неког бита у поруци, та се грешка манифестује на једну врсту и на једну колону. Ово омогућава прецизно откривање погрешног бита, а затим и његово исправљање.



Слика 4. Откривање измењеног бита дводимензионалном провером парности

На овај начин је могуће открити и исправити вишеструке грешке, али се оне не смеју јављати у истим врстама и колонама. Као и код сваке провере парности, могуће је открити само непаран број промењених битова у једној колони или врсти. Наведена дводимензиона шема има слабе карактеристике ако се ради о импулсним сметњама и грешкама које су сконцентрисане на једном интервалу.

1.3. Категоризације рачунарских мрежа

Данас постоји велики број различитих технологија за повезивање рачунара у рачунарске мреже, односно технологија на физичком слоју и слоју везе података *OSI* референтног модела. Ове технологије се могу груписати по различитим критеријумима, а основне поделе се праве по типу медија који се користи за пренос података и по географској површини коју покривају.

Основна подела рачунарских телекомуникационих технологија по типу медија који користе је на бежичне и жичне. Унутар ове поделе даља подела се врши по носиоцу сигнала: електрични импулси, светлосни импулси, радио-таласи.

Следећа значајна карактеристика рачунарских телекомуникационих технологија односи се на величину простора на коме се путем њих може извршити повезивање рачунарских система. Нивое који се јављају у оквиру ове поделе чине:

- личне рачунарске мреже (енгл. *Personal Area Network, PAN*)
- локалне рачунарске мреже (енгл. *Local Area Network, LAN*)

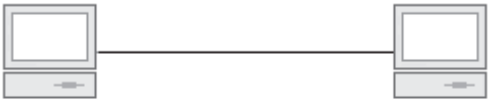
- мреже на подручју града (енгл. *Metropolitan Area Network, MAN*)
- мреже на ширем подручју (енгл. *Wide Area Network, WAN*)
- глобална мрежа, Интернет

Коришћењем ових технологија формирају се сталне или привремене рачунарске мреже које пружају телекомуникациону функционалност на другом слоју *OSI* модела. Интернет, као глобална мрежа, подразумева повезивање рачунарских мрежа наведених величина на мрежном слоју *OSI* модела.

1.3.1. Топологија

Једна од основних категоризација рачунарских мрежа прави се на основу њихове топологије, односно начина на који су мрежни чворови међусобно повезани. Топологија може бити физичка и логичка, односно може се правити на основу физичког распореда и начина повезивања чланова и на основу њиховог логичког односа.

За потпуно разумевање топологија рачунарских мрежа треба направити разлику између посредујућих и крајњих мрежних уређаја. У посредујуће мрежне уређаје спадају сви уређаји чија је улога омогућавање мрежне комуникације, односно повезивање осталих уређаја. У ту групу спадају разводници, комутатори, модеми, рутери... Са друге стране, у крајње мрежне уређаје спадају управо уређаји због којих се рачунарске мреже и формирају - рачунари, телефони, штампачи и други.

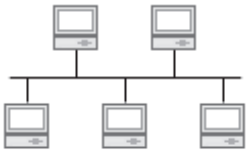


Слика 1. Најједноставнија топологија - тачка-тачка

Једна од најједноставнијих топологија у рачунарским мрежама је топологија тачка-тачка (енгл. *point-to-point*). Ова топологија подразумева постојање само два мрежна члана која су директно повезана, без посредника. Топологија тачка-тачка се најчешће користи код повезивања удаљених чворова, односно у ситуацијама када се (најчешће серијском) везом премошћава велика удаљеност између два телекомуникациона уређаја.

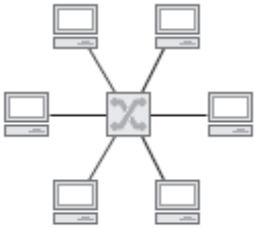
Следећа најједноставнија топологија је топологија магистрале (енгл. *bus*). Код ове топологије су сви чланови повезани на једну линијску магистралу и путем ње шаљу поруке осталим члановима. Ова топологија, као сложенија од топологије тачка-тачка, уводи потребу за адресовањем, односно одређивањем

ко од прималаца треба да обради примљену поруку. Све поруке се на физичком нивоу шаљу дифузно, тј. испоручују се свим члановима мреже. Један од главних недостатака топологије магистрале је тај што прекид у једној тачки најчешће блокира рад целе мреже, или макар онемогућава комуникацију између раскинутих сегмената.



Слика 2. Топологија магистрале

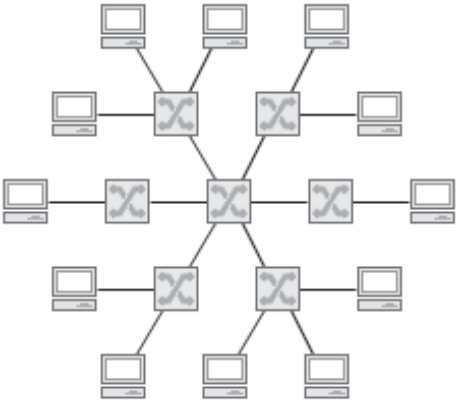
Код топологије звезде (енгл. *star*) су сви чланови мреже повезани са једном, централном тачком. Ова тачка је задужена да примљене податке прослеђује осталим члановима мреже. Уколико је ниво рада централне тачке такав да она примљене податке прослеђује свим осталим чворовима, у том случају логичка топологија такве мреже остаје магистрала. У противном, уколико централна тачка може да усмерава податке само оним члановима на које су ти подаци адресовани, у том случају је и логичка топологија мреже звезда.



Слика 3. Топологија звезде

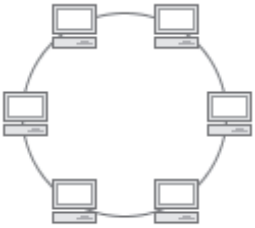
Једна од главних предности топологије звезде у односу на топологију магистрале је већа робусност, односно отпорност на отказивање. Уколико се у мрежи са топологијом звезде пресече један комуникациони канал, комуникација ће бити онемогућена само за једног члана мреже, односно члана кога тај канал повезује са остатком мреже.

Напреднију варијанту топологије звезде чини топологија стабла (енгл. *tree*). Код ове топологије се чланови повезују на исти начин као код звезде, с тим што се на један централни уређај може повезати исти такав уређај и на тај начин мрежа ширити теоријски готово бесконачно. Додавањем посредујућих уређаја се повећава кашњење те је препорука да се свака комуникација у једној мрежи омогући у највише 6-7 скокова, односно са не више од 5-6 посредујућих уређаја.



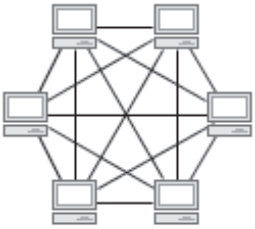
Слика 4. Топологија стабла

Топологија прстена представља ватијанту топологије магистрале код које су крајеви магистрале повезани. На тај начин су у одређеној мери побољшане перформансе, као и (делимично) приватност у комуникацијама.



Слика 5. Топологија прстена

Са друге стране, већина проблема везаних за топологију магистрале се задржала - отказивање једне тачке онемогућава рад целе мреже, као и додавање нових чланова - а уведено је и повећање кашњења у зависности од броја чланова.



Слика 6. Меш топологија

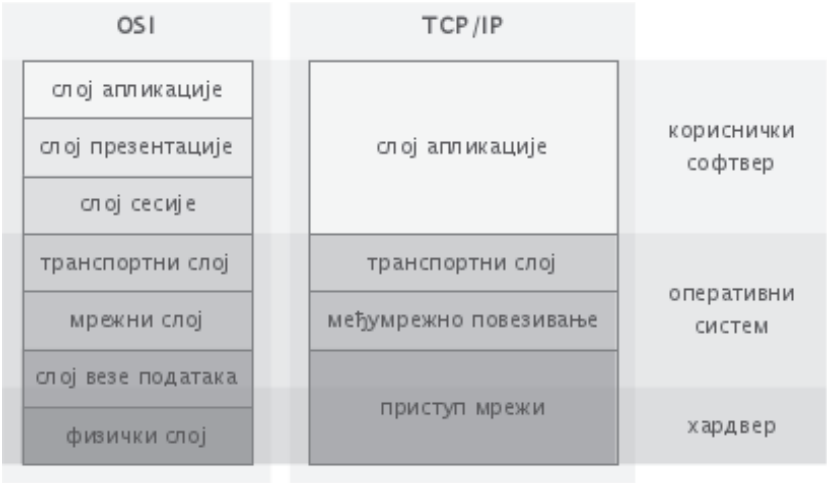
Код меш (енгл. *mesh*) топологије сваки чвор има директну везу ка сваком од осталих чворова у мрежи. Таква топологија нуди највише перформансе (нема

дељења канала, као ни кашњења због посредника) али је веома сложена и скупа за реализацију, тако да се ретко користи у жичним мрежама.

1.4. Модели рачунарских комуникација

Свака комуникација - не само рачунарска - може се посматрати у виду слојева. На пример, уколико једна особа жели да нешто саопшти другој, она на највишем нивоу има апстрактну поруку, ближу потреби за саопштењем нечега него уобличеној поруци. Она, затим, бира одговарајући облик за формулисање поруке - вербални, музички, сликовни... Након формулисања поруке изабира се најприкладнији начин кодовања поруке и медиј за њен пренос - на пример кодовање музичке поруке у нотном систему и запис на папиру или њено извођење на одређеном музичком инструменту.

Слојевитост код комуникације у рачунарским мрежама је стандардизована. Формални стандард за рачунарске телекомуникације дефинисала је Међународна организација за стандардизацију (енгл. *International Organization for Standardization, ISO*) у виду референтног модела за отворено повезивање система (енгл. *Open Systems Interconnection, OSI*). Овај модел дели рачунарску мрежну комуникацију на седам слојева у зависности од специфичног задатка који се обавља: физички слој, слој везе података, мрежни слој, транспортни слој, слој сесије, слој презентације и слој апликације.

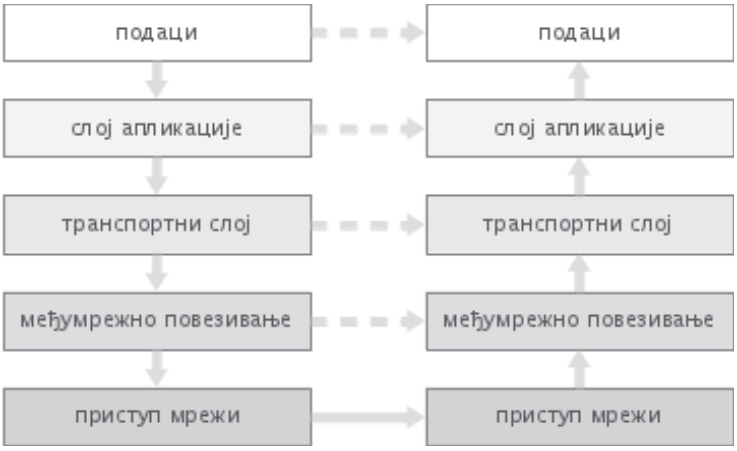


Слика 1. Референтни комуникациони модели и нивои имплементације

С обзиром да детаљност коју нуди, подела *OSI* модела најчешће није потребна. У пракси се за опис комункације често користи једноставнији модел, познат под називом ***TCP/IP* скуп протокола** (енгл. *TCP/IP Protocol Suite*) или **Интернет**

модел. Овај модел не залази у детаље комуникације унутар корисничког сервиса (апликације), те слојеве сесије и презентације интегрише у сам слој апликације. Додатно, унутар њега се не врши подела телекомуникационе инфраструктуре на физички слој и слој везе података већ су они обједињени у функционалну целину задужену за приступ рачунарској мрежи.

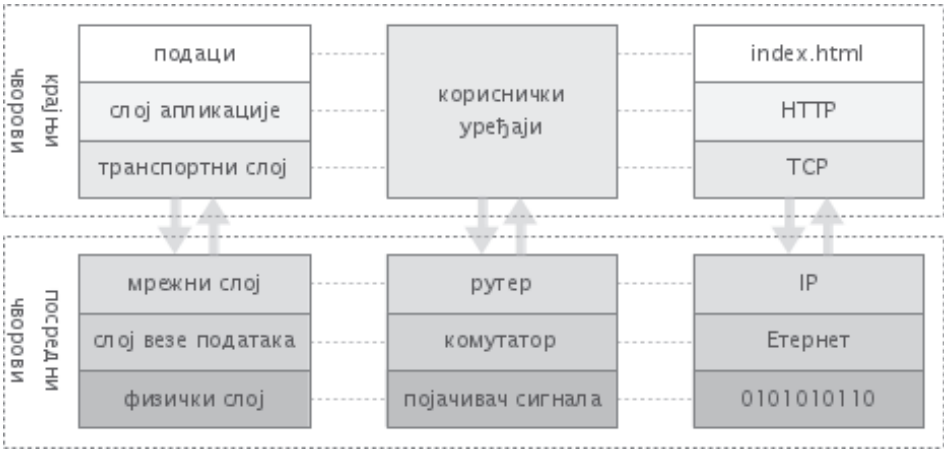
Подела рачунарске комуникације на слојеве омогућава фокусирање на издвојени задатак слоја при развоју телекомуникационог протокола или медија, односно изузимање из вида детаља осталих слојева и апстракцију до нивоа комуникације са имплементацијом решења на другој комуникационој страни. Оваква комуникација, комуникација између страна које комуницирају, назива се **хоризонтална комуникација**.



Слика 2. Вертикална и хоризонтална комуникација слојева

Са друге стране, сваки слој добија задатке (податке које треба пренети) од слојева виших нивоа, а за њихово извршавање користи услуге слојева нижих нивоа. Оваква комуникација - комуникација између различитих слојева унутар једног рачунара - назива се **вертикална комуникација**. Вертикална комуникација је неодвојива од принципа инкапсулације и декапсулације пакета.

Подела рачунарске комуникације на више нивоа омогућава виши ниво специјализације при развоју мрежних уређаја, односно уређаја који омогућавају рачунарске телекомуникације. За одређивање нивоа на коме ради одређени уређај узима се највиши слој *OSI* модела чије је јединице података уређај у стању да разуме, уз подразумевање чињенице да разуме и све ниже слојеве.



Слика 3. Паралела између комуникационих слојева, уређаја и протокола

На пример, у уређаје који раде на првом, физичком слоју (тзв. *L1* уређаји) спадају појачивачи дигиталних сигнала (разводници и рипитери), у уређаје који раде на слоју везе (тзв. *L2* уређаји) комутатори, а у уређаје који раде на трећем, мрежном слоју (тзв. *L3* уређаји) рутери. Размевање протокола транспортног слоја је обично директно повезано са њиховом употребом од стране протокола на слоју апликације а у уређаје виших слојева углавном спадају крајњи, кориснички уређаји или специјализовани мрежни уређаји.

1.4.1. Нивои рада мрежних уређаја

У пракси се често користе ознаке *L1*, *L2* и *L3* за означавање нивоа рада мрежних уређаја. Ове ознаке се односе на највиши слој (ниво) *OSI* референтног модела који уређај разуме. У складу са тим, на првом, физичком нивоу (*L1*) функционишу рипитери и разводници. На слоју везе података (*L2*) функционишу мрежни мост, комутатор и модем. На мрежном слоју (*L3*) функционишу сви виши уређаји - рутер, рачунар, заштитни зид...

Треба имати у виду да се мрежни слој - *L3* - често узима за највиши слој при одређивању нивоа на коме ради уређај, а да у пракси велики број *L3* уређаја има подршку и за протоколе виших слојева. На пример, већина рутера има могућност коришћења протокола за динамичко рутирање који функционишу на апликативном, седмом нивоу. Рачунари такође подразумевано користе сервисе на апликативном слоју. Постоје заштитни зидови који заиста разумеју само протоколе мрежног нивоа, али и заштитни зидови који могу да анализирају и протоколе транспортног и апликативног нивоа (прокси сервери).

Слика 1. Нивои рада мрежних уређаја.

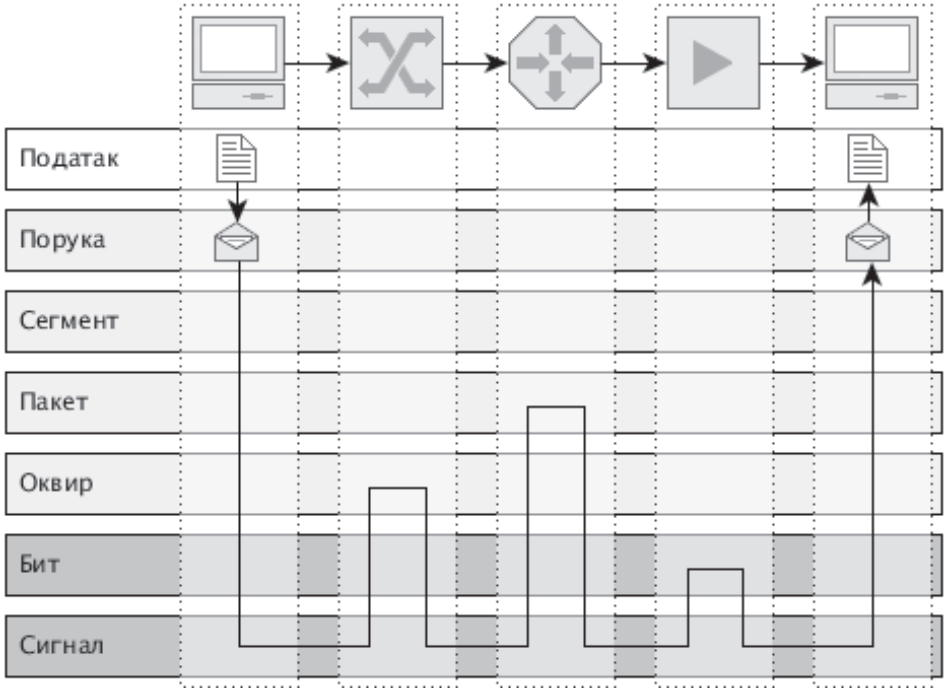
Такође, постоје и комутатори који подржавају одређене функције мрежног слоја. У њих првенствено спадају основне функције рутирања за потребе повезивања различитих виртуалних локалних мрежа. Такви комутатори се називају *L3* комутаторима (енгл. *L3 switch*).

1.4.2. Принцип инкапсулирања

Подаци у рачунарским мрежама реализованим по Интернет моделу размењују се кроз пакетски пренос. Пакетски пренос података подразумева поделу веће количине података у мање јединице (пакете) које се засебно преносе у оквиру комуникације. Пакети представљају основне јединице података протокола а у зависности од слоја на коме се протокол налази називају се оквирима (слој везе), пакетима (мрежни слој) или сегментима (транспортни слој).

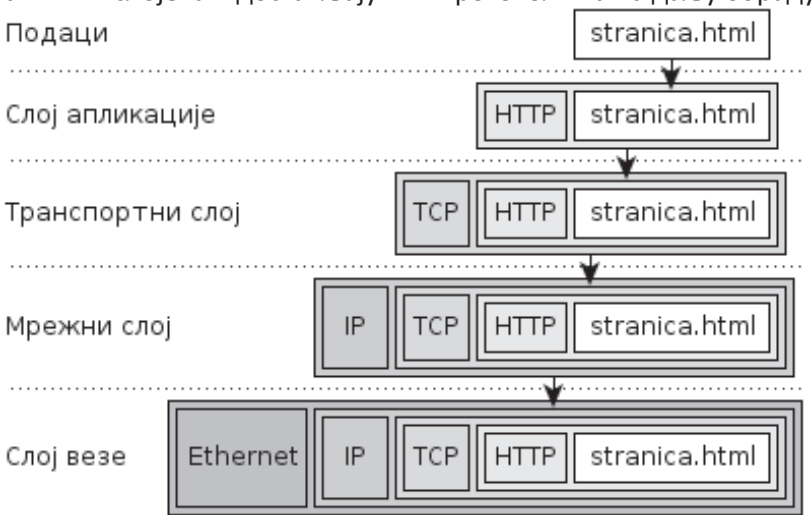
Хоризонтална пакетска комуникација подразумева превођење битова пакета у одговарајуће сигнале коришћене технологије за повезивање и на такав начин њихов пренос до коначног одредишта или првог следећег посредника у комуникацији. Уколико је у питању комуникација путем посредника, пакети се могу једноставно прослеђивати следећем посреднику/одредишту или преводити у пакете различите телекомуникационе технологије.

Када је у питању вертикална комуникација, односно комуникација између различитих протокола на различитим комуникационим слојевима, неодвојив део пакетског преноса је и процес **инкапсулације**. Процес инкапсулације подразумева прављење пакета протокола на одређеном слоју чији садржај чини пакет добијен од протокола вишег нивоа. Овај процес се понавља за сваки комуникациони слој чији се протоколи користе.



Слика 1. Нивои инкапсулације/декапсулације током преноса

Процес инкапсулације пакета се извршава на страни пошиљаоца, а њему инверзан процес је процес **декапсулације.** Декапсулација се извршава на страни примаоца а њоме се из пакета протокола нижих слојева издвајају пакети протокола виших слојева и достављају тим протоколима на даљу обраду.



Слика 2. Инкапсулација у пакете протокола различитих слојева

Комплетан процес инкапсулације одвија се на страни пошиљаоца а комплетан процес декапсулације на страни примаоца података. Међутим, оба процеса се делимично могу извршавати и на посредницима у комуникацији, у зависности од тога на којим нивоима ти посредници функционишу. На пример, рутер ће из примљених оквира издвојити пакете мрежног слоја (декапсулација) да би на основу података у њиховом заглављу донео одлуку о прослеђивању. Након доношења те одлуке, рутер ће пакет мрежног слоја упаковати у одговарајући оквир (инкапсулација) за преношење до следећег посредника или коначног одредишта.

1.4.3. Стандарди, референтна тела и организације

Данас, доминантну улогу на пољу рачунарске безбедности и њене стандардизације имају САД. Водеће организације на пољу стандардизације безбедносних система функционишу као агенције владе САД. Такође, и значајне организације које имају утицаја на глобалне трендове у развоју информационих технологија лоциране су на северноамеричком континенту.

1.4.3.1. Међународне организације

Интернет корпорација за додељивање назива и бројева (енгл. *Internet Corporation for Assigned Names and Numbers, ICANN*) задужена је за управљање адресама на Интернету, одређивање аутономних система, администрацију кореног система доменских имена, одређивање бројева за протоколе и сл. Пре формирања ове корпорације при америчком министарству трговине, њене функције су вршене на Институту за информатичке науке при Универзитету Јужна Калифорнија, на основу уговора са америчким министарством одбране. При овој корпорацији функционише и *IANA (Internet Assigned Numbers Authority*).

Специјална комисија за развој интернета (енгл. *Internet Engineering Task Force, IETF*) задужена је за развој и промовисање Интернет стандарда. Учесници ове организације су волонтери, с тим да је њихов рад плаћен од стране њихових послодаваца или спонзора (тренутног председавајућег ове организације спонзоришу компанија *VeriSign* и америчка Национална безбедносна агенција).

Међународна телекомуникациона унија (енгл. *International Telecommunication Union ITU*) је агенција при Уједињеним нацијама, са седиштем у Женеви. Основни циљ ове агенције је развој телекомуникационе инфраструктуре и успостављање међународних стандарда.

Европски институт за телекомуникационе стандарде (енгл. *European Telecommunications Standards Institute, ETSI*) је независна, непрофитна

организација, призната од стране европске комисије, а основана 1988. године од стране европске конференције за поштанску и телекомуникациону администрацију. Основни допринос ове организације је у развоју стандарда за мобилну комуникацију.

Фондација за слободан софтвер (енгл. *Free Software Foundation, FSF*) непрофитна је организација основана са циљем да промовише слободу у коришћењу рачунарског софтвера, као и да заштити права корисника тог софтвера. Један од главних доприноса ове фондације је развој *GNU* оперативног система и допринос развоју софтвера са отвореним изворним кодом, првенствено Линукс оперативног система.

1.4.3.2. Националне организације

Једна од најзначајнијих организација за стандардизацију на пољу рачунарске безбедности је америчка Национална безбедносна агенција (енгл. *National Security Agency, NSA*). Ова агенција је основана 1952. године са циљем да пружи услуге надгледања комуникација страних обавештајних служби и заштиту комуникација владе САД. Од 2008. године ова агенција је задужена и за заштиту владиних рачунарских система и мрежа. Ова агенција је чланица обавештајне заједнице САД (енгл. *U.S. Intelligence Community*). Координацију између Националне безбедносне агенције и војске САД обавља Централна безбедносна служба (енгл. *Central security service*). Национална безбедносна агенција је имала значајан утицај на развој актуелних шифарских алгоритама *AES* и *DES*, Клипер криптографског чипа и сл. Ова агенција је инвестирала милионе долара у академски развој на пољу безбедности, али су познати и примери у којима је она утицала и на забрану објављивања одређених резултата (нпр. шифарски алгоритми *Khufu* и *Khafre*).

Амерички Национални институт за стандардизацију и технологију (енгл. *National Institute of Standards and Technology, NIST*), раније познат под именом Национални биро за стандардизацију (енгл. *National Bureau of Standards, NBS*), основан је 1901. године као агенција департмана за трговину владе САД. Као званична мисија института наведена је промоција иновативности и индустријске компетитивности САД путем унапређивања науке, стандарда и технологије. Овај институт је учествовао у стандардизацији популарних шифарских алгоритама *AES* и *DES*.

2. Приватне рачунарске мреже

У групу приватних рачунарских мрежа спадају све рачунарске мреже које су комплетно у власништву једног лица или огранизације. Ту се првенствено мисли на мреже на локалном подручју (енгл. *Local Area Network, LAN*), а затим и на мреже на подручју града (енгл. *Metropolitan Area Network*). Додатно, у ову групу спадају и личне рачунарске мреже (енгл. *Personal Area Network*) и рачунарске мреже на подручју тела (енгл. *Body Area Network*).

> **Напомена:** у српском језику се термин *Local Area Network* често преводи као „локална мрежа“. Овај превод није исправан с обзиром на то да се тај термин (енгл. *local network*) првенствено користи у међумрежној комуникацији, за одређивање мреже у којој се одређени уређај налази, насупрот удаљених мрежа, суседних или несуседних.

Мреже на локалном подручју су мреже којима су повезана два рачунара, рачунари у једној просторији, згради или кампусу и у власништву су једног лица или организације. Мреже на подручју града чине инфраструктуру за повезивање и у власништву су града у ком се налазе. У оба случаја важна карактеристика ових мрежа је да се у потпуности налазе у власништву једног власника, односно да се ни један део њих не изнајмљује.

Једна посебна врста приватних рачунарских мрежа су тзв. **виртуалне рачунарске мреже** (енгл. *Virtual Private Network, VPN*). Ове мреже имају више сегмената који се налазе на удаљеним локацијама, а који су међусобно повезани мрежама које се простиру на ширем подручју - Интернетом, изнајмљеним линијама и сл. Дакле, назив „виртуалне“ у овом случају потиче отуд што ове мреже нису заиста у приватном власништву већ се један њихов део изнајмљује.

За потребе приватних рачунарских мрежа IEEE асоцијација је дефинисала групу стандарда под бројем 802. Два најважнија стандарда и ове групе се односе на технологије за формирање жичних (Етернет, 802.3) и бежичних (Wi-Fi, 802.11) мрежа на локалном подручју.

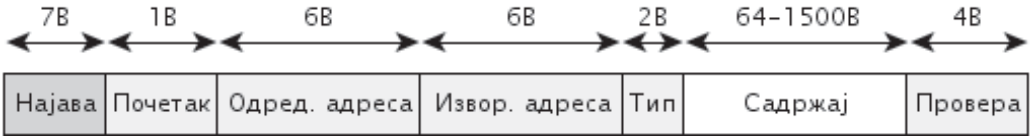
2.1. Етернет

Етернет (*IEEE 802.3* или *ISO 80802-2*) представља најчешће коришћени протокол за приватне рачунарске мреже. То је стандард којим се дефинише физички слој и *MAC* подслој везе података. Развијен је од стране компанија *DEC*, *Xerox* и *Intel* а касније је формализован од стране *IEEE* као *IEEE 802.3*. То је протокол који је оријентисан на бројање бајтова (садржи поље које одређује дужину поруке оквира). Приступ медијуму се врши на основу садржаја.

На слоју везе података *OSI* модела Етернет користи метод *CSMA/CD*. *Multiple Access* значи да су сви рачунари повезани на један заједнички медијум коме приступа више рачунара. *Carrier Sense* означава да пре емитовања података рачунар проверава - ослушкује медијум да би утврдио да ли неки други рачунар већ емитује податке. Ако у медијуму влада тишина (не емитује нека друга станица) тек тада рачунар почиње да шаље податке. *Collision Detection* значи да у случајевима када две станице почну истовремено да емитују податке и дође до судара (колизије) постоје механизми за отпочињање поновног слања истих података.

2.1.1. Поруке и адресовање у Етернет мрежама

Етернет технологија подразумева пакетски пренос података. Пакети Етернета се називају оквирима (енгл. *Ethernet frame*). Ови оквири се адресују, и то адресом пошиљаоца и адресом примаоца. Ове адресе представљају физичке адресе Етернет интерфејса који је оквир послао, односно коме је оквир намењен. Дужина адреса које користи Етернет је 48 битова и њих у мрежне интерфејсе уписују произвођачи у процесу производње. Сваки Етернет интерфејс би требало да има јединствену физичку адресу.



Слика 1. Формат Етернет оквира

Етернет оквир на почетку има преамбулу дужине 7 бајтова и обично је облика „10101010...“. Овакав почетак помаже пријемнику да се боље припреми за долазак самог оквира, омогућава бољи рад екстрактора такта у пријемнику и смањење евентуалних грешака због непрецизног очитавања бита. Поред тога, пријемник се обавештава да иза тога следи карактеристичан бајт који означава почетак оквира. Одредишна адреса одређује адресу примаоца, а изворишна адреса означава адресу пошаљиоца. *VLAN* се користи за виртуалне *LAN*-ове; ако нема *VLAN*-а, поље се изоставља, а ако се користи прва 2 бајта имају вредност 24,832 (8100X). Дужина, која се одређује са два бајта, означава број бајтова у оквиру или се се ово поље користи за размену контролних информација, нпр. тип протокола на мрежном нивоу (*TCP/IP, IPX/SPX*). Максимална дужина поља за податке је 1.500 бајтова. Да би се лакше разликовао Етернет оквир од случајних података који могу да лутају рачунарском мрежом, минимална дужина података у оквиру је 64 бајтова. Ако су подаци из горњих слојева, који се енкапсулирају у оквир, краћи од ове дужине, врши се допуна до минималних 64. Оквир се

завршава *CRC-32* кодом за откривање грешака на комуникационом каналу.

2.1.2. Етернет преко коаксијалних каблова

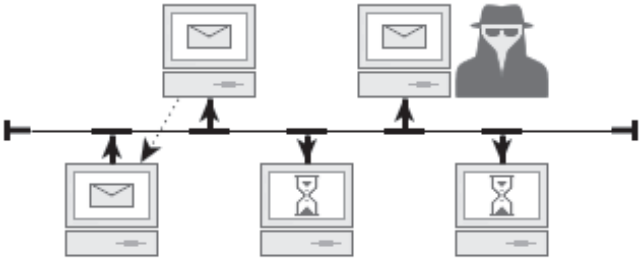
Прву комерцијално доступну варијанту Етернет технологије (1985. година) чинио је тзв. дебели Етернет (енгл. *thick Ethernet*), познат и под ознаком 10BASE5. Ова варијанта Етернета користила је коаксијалне каблове пречника 9,5mm. Највећа дозвољена дужина кабла код дебелог Етернета износила је 500 метара а у једном сегменту је било могуће повезати до 100 рачунара.

Следећи стандард Етернета заснован на коришћењу коаксијалних каблова објављен 1985. године под ознаком 10BASE2 а у јавности је познат под називом танки Етернет (енгл. *thin Ethernet*).

Слика 1. Компоненте за повезивање

Код ових мрежа слање података се одвија дифузно (енгл. *broadcast*). То значи да се послати подаци испоручују свим члановима мреже. Члан коме су подаци намењени то утврђује на основу поклапања одредишне адресе окрвира са својом физичком адресом. Остали чланови примљене оквире одбацују јер нема поклапања одредишне са локалном адресом.

Описани начин рада поседује два главна недостатка: низак ниво безбедности и ниске перформансе. У мрежама са дифузним слањем података прислушкивање, односно снимање саобраћаја је веома једноставно. Довољно је да један рачунар постави свој мрежни адаптер у промискуитетни режим рада и одмах је у могућности да сними све размене података између свих чланова мреже.



Слика 2. Прислушкивање је једноставно код дифузионог слања

Са друге стране, перфомансе мрежа са дифузним слањем података су ниже него код мрежа истих карактеристика код којих се подаци шаљу усмерено. Разлог томе је могућност да само један члан мреже шаље податке у једном тренутку, односно функционисање целе мреже у полу-дуплексном режиму. Остали чланови који у том тренутку желе да шаљу податке морају сачекати да се тренутно слање података заврши.

Слика 3. У мрежи само један члан може да шаље податке у једном тренутку

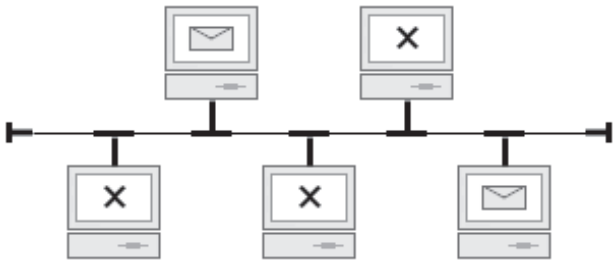
Постоји велики број проблема везаних за рад мрежа које користе коаксијалне каблове, првенствено на пољу доступности и перформанси. На пример, код додавања новог рачунара у такву мрежу неопходно је њен рад прекинути за време потребно за физичко прикључивање новог члана и поновно успостављање протокола.

Слика 4. Пад целе мреже због једног прекида

Код Етернет мрежа које користе коаксијалне каблове и физичка и логичка топологија су магистрале. С обзиром на то да је са овим типом физичке топологије отежано радити, као и на проблеме везане за доступност мрежа заснованих на коаксијалним кабловима, они су 1990. године замењени кабловима са упреденим парицама који и данас чине стандард када су у питању приватне рачунарске мреже.

2.1.2.1. Контрола приступа медију

С обзиром на то да су прва и друга генерација Етернета користиле логичку топологију магистрале (полу-дуплекс режим рада), било је неопходно решити проблем коришћења дељеног медија од стране вишеструких чланова. У ту сврху је развијен метод под називом *ослушкивање медија код вишеструког приступа са откривањем судара* (енгл. *Carrier sense multiple access with collision detection , CSMA/CD*). Овај метод је подразумевао да свака Етернет станица пре слања оквира ослушкује медиј да би проверила да ли је он заузет (да ли нека друга станица у том тренутку већ шаље свој оквир). Уколико је то случај, станица би сачекала да се тренутно слање заврши и тек тада би започела слање свог оквира.



Слика 1. Истовремено слање оквира изазива блокаду мреже

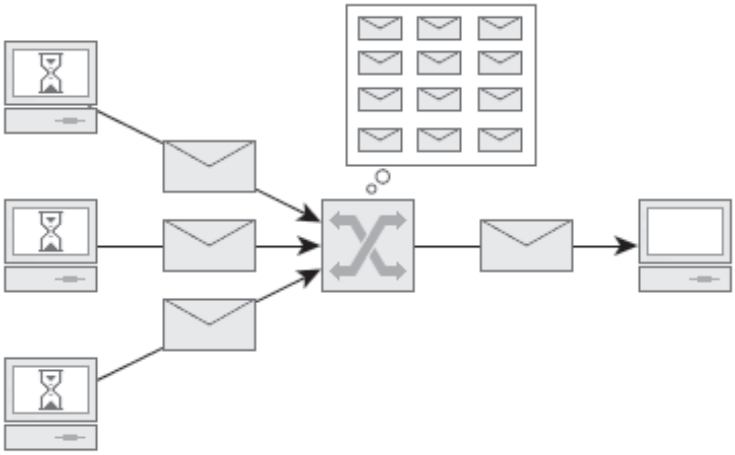
Иако наведени метод делује као потпуно решење, постоје два случаја у којима ће ипак доћи до „сударања“ два или више оквира, односно колизије:

1. Две или више станица истовремено провере да ли је медиј заузет и, добијајући негативан одговор, истовремено започну слање.
2. Две или више станица у току заузећа медија сачекају да се он ослободи, а затим истовремено започну слање.

Дакле, колизије се у полу-дуплекс Етернет мрежама ипак могу јавити, те је било потребно допунити метод могућношћу да се настала колизија открије (*collision detection*) и отклони на одговарајући начин. Са тим циљем је у метод уведено сигнализирање застоја (енгл. *jam signal*) који су станице слале у случају

откривања колизије. Подразумевана реакција на овај сигнал је тренутан прекид слања свих оквира у мрежи.

Сам прекид слања у случају колизије није коначан корак у CSMA/CD методу јер је након прекида потребно омогућити и поновно слање, односно наставак нормалног рада. То је решено на такав начин да све станице које желе да понове слање пре тога чекају случајно изабран временски период. У случају да је овај период фиксно одређен, станице би се заглавиле у бесконачној петљи, односно мрежа би престала са радом.

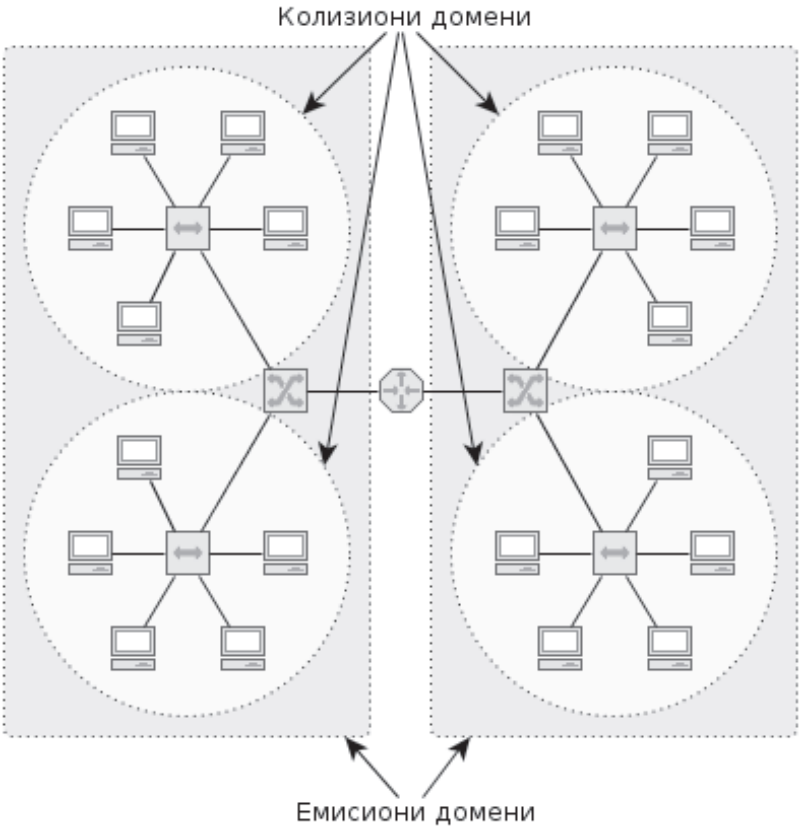


Слика 2. Затрпавање комутатора оквирима

Проблем колизија у Етернет мрежама решен је напуштањем логичке топологије магистрале, односно увођењем пуног дуплекс режима рада (комутатори). У таквим мрежама „сударање“ оквира није могуће, али је могуће њихово „сустизање“, односно нагомилавање у меморији комутатора у ситуацијама када оквири брже пристижу него што их је могуће проследити. У таквим ситуацијама комутатор станицама са којих долазе оквири шаље сигнал застоја и на тај начин успорава њихово слање.

2.1.2.2. Колизиони и емисиони домени

Колизиони домени (енгл. *collision domain*) у етернет мрежама представљају подручја у којима се могу јавити колизије - сударања оквира. Код првих генерација Етернета (засноване на коаксијалним кабловима, као и на разводницима) цела мрежа је представљала један колизиони домен. Ови домени су, евентуално, дељени додавањем мрежних мостова.

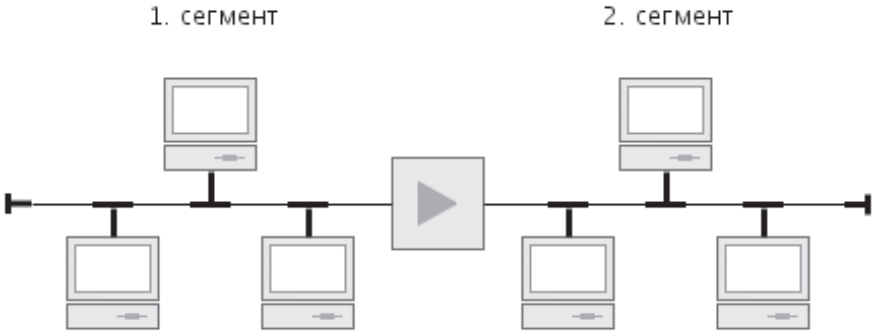


Слика 1. Колизиони и емисиони домени

У савременим Етернет мрежама, заснованим на комутаторима, свака веза представља засебан колизиони домен, тако да колизије нису могуће. Са друге стране, целокупна Етернет мрежа представља један емисиони, дифузни домен (енгл. *broadcast domain*). Овај домен обухвата све чланове мреже који ће примити дифузно послате поруке. Рутери деле емисионе домене.

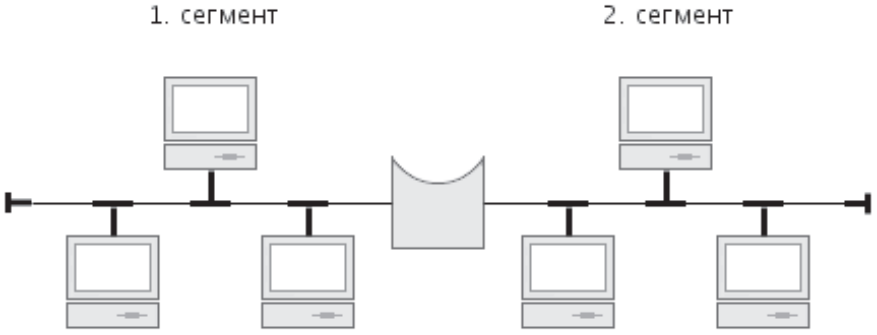
2.1.2.3. Појачивачи сигнала и мостови

Јачина и квалитет сигнала у коаксијалним кабловима опадају у складу са раздаљином (подужно слабљење). Из тог разлога је, када је потребно премостити веће раздаљине, потребно користити појачиваче сигнала. Појачивачи који се користе код Етернет мрежа заснованих на коаксијалним кабловима јесу дигитални појачивачи сигнала или рипитери (енгл. *repeater*). Они подразумевано поседују два порта и омогућавају повезивање два сегмента мреже. Кашњење које се уводи применом рипитера је занемарљиво.



Слика 1. Вишеструки сегменти се повезују рипитером.

За разлику од рипитера који логички не раздвајају сегменте, мрежни мостови (енгл. *bridge*) од сегмената које повезују праве логички одвојене целине. То значи да је могућа паралелна, истовремена комуникација између једног пара у једном сегменту и једног пара у другом сегменту. То се постиже тако што мост онемогућава пролаз оквира из једног сегмента у други уколико то није потребно. Са друге стране, уколико се јави потреба за комуникацијом између чланова различитих сегмената, мрежни мост дозвољава пролаз оквира те комуникације. Због оваквог начина рада Етернет мостови се називају и филтерима оквира.



Слика 2. Мостови омогућавају паралелну комуникацију у сегментима

Јасно је да су Етернет мостови далеко сложенији уређаји од рипитера. Они, за разлику од рипитера који раде на нивоу бита, раде на нивоу оквира, односно користе одредишну адресу оквира за доношење одлуке о пропуштању или одбацивању. Такав рад захтева постојање меморијских и процесорских капацитета, а он уједно уводи и одређено кашњење при испоруци оквира. Меморија на мрежном мосту је, осим за чување оквира о коме се одлучује,

потребна и за складиштење листи које повезују припадност одређене физичке адресе неком од сегмената. Дакле, мрежни мостови поседују и напредну функцију учења физичких адреса мреже у којој раде.

2.1.3. Етернет преко каблова са упреденим парицама

Један од најзначајнијих еволутивних скокова Етернет технологије догодио се 1986. године када је стандардизована употреба каблова са упреденим парицама (енгл. *twisted pair cable*). Увођењем ових каблова са физичке топологије магистрале прешло се на топологију звезде (тзв. *Star LAN*) и отклоњени су бројни проблеми везани за расположивост мреже. Касније, увођењем комутатора, напуштена је и логичка топологија магистрале чиме су драстично повећане перформансе Етернет мрежа.

Кабл са упреденим парицама (енгл. *twisted pair cable*) састоји се од парова изолованих бакарних жица које су обмотане (упредене) једна око друге. Упредање се врши у циљу отклањања електромагнетних сметњи и ефекта преслушавања који потиче од суседних парица. Број увртаја по метру чини део спецификације кабла (корак упредања). Што је број увртаја по метру већи, већа је отпорност кабла на електромагнетне сметње. На слици 2. приказана су два типа овог кабла: кабл са неоклопљеним (*Unshielded Twisted-Pair, UTP*) и оклопљеним (*Shielded Twisted-Pair, STP*) парицама.

Слика 2.1.3-1. Каблови са неоклопљеним и оклопљеним парицама

UTP кабл се користи у телефонским системима као и у Етернет мрежама. Најчешће се састоји од четири пара упредених парица у изолационом омотачу. Групе парица се обично налазе у заштитном *PVC* омотачу и заједно са њим чине кабл. Оклопљене парице пружају знатно бољу заштиту од електромагнетних сметњи. Скупљи су од обичних каблова и мање су флексибилни тако да их је теже монтирати. Такође, оклопљени каблови имају већи попречни пресек од

обичних каблова, што значи да треба рачунати на веће канале за уградњу оваквих каблова. У пракси постоје три типа оклопљених каблова: *FTP*, *S-FTP* и *STP*.

FTP кабл је направљен тако да су четири парице потпуно обавијене танком металном фолијом. Ова фолија своју заштитну функцију обавља тако што, захваљујући високој импеданси, рефлектује спољне електромагнетне сигнале (шум) на учестаностима већим од 5MHz и тако им онемогућава продор до самих парица.

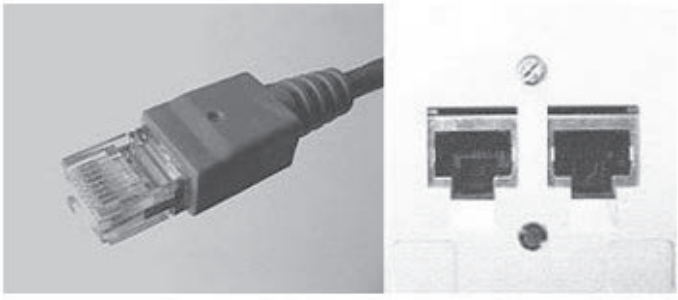
По односу цена/перформансе у пракси су се најбоље показали *FTP* каблови, тако да се они најчешће и користе. *STP* каблови имају заштиту за сваку парицу, а *S-FTP* каблови поред заштите појединачних парица имају још једну заједничку заштиту.

Слика 2.1.3-2. Пресек: каблови са неоклопљеним и оклопљеним парицама

Бакарне жице каблова са уврнутим парицама повезују се са хардверским мрежним интерфејсом рачунара (на пример мрежном Етернет картицом) путем одговарајућих конектора. Најчешће коришћени тип конектора је *RJ* (*Registered Jack*) и он се, у више варијанти, користи код телефонских (*RJ11*) и рачунарских мрежа (*RJ45*).

Упредене парице могу бити пуног попречног пресека и лицнасте без обзира да ли је кабл оклопљен или не. Кабл пуног пресека се користи за повезивање разводних панела са утичницама на радним местима. Може се срести и под називом *wall* (зидни) зато што се користи за инсталације у зидовима. Код оваквих каблова треба избегавати увртање, велика савијања и упредања. Каблови са пуним пресеком проузрокују мање слабљење него лицнасти каблови. Лицнасти кабл се користи за повезивање разводних панела, као и за повезивање радних станица са утичницама. Знатно су флексибилнији од каблова са пуним попречним пресеком. Ипак, слабљење које овакви каблови уносе веће је, тако да укупна дужина лицнастих каблова у једном сегмену

мреже не би требало да прелази 10 метара.



Слика 2.1.3-3. Конектор RJ45 и утичница

PVC - поливинил-хлорид се користи као изолациони омотач каблова свих врста. Каблови су савитљивији, лако се постављају али су и лако запаљиви и ослобађају отрован гас када горе. *Plenum* (зидни) каблови се постављају у међупросторе, чвршћи су од каблова са *PVC* изолацијом али не испуштају отрован гас у случају да се запале.

Каблови са упреденим парицама за повезивање са рачунарима користе *RJ-45* конекторе. За повезивање бакарних жица са конекторима користи се посебан тип алата - тзв. клешта за кримповање. Распоред жица при повезивању је одређен стандардима *568A* и *568B*.

Како је потреба за повећањем пропусног опсега стално расла, због употребе све захтевнијих мрежних апликација, квалитет каблова са упреденим парицама је такође морао да се повећава. *TIA/EIA-568B* стандард спецификује категорије каблова са упреденим парицама. *ISO/IEC* специфицира категорије мрежних компонената, док каблове специфицира по класама (*class*).

Категорија 3 (*CAT3*/Class *C*) кабла са упреденим парицама се користила у мрежема са брзинама до 10Mb/s, са максималним пропусним опсегом од 16MHz. Ова категорија кабла је била у употреби почетком деведесетих година прошлог века.

Категорија 4 је коришћена у мрежама са жетоном и омогућавала је брзине до 16Mb/s.

Категорија 5 (*CAT5*) каблова се користи у локалним рачунарским мрежама са брзинама до 100Mb/s и са максималним сегментом мреже од 100 метара.

Побољшана категорија 5 (*CAT5e/Class D*) каблова је дизајнирана да омогући пропусни опсег од 100MHz и потпуни дуплекс. Са овом категоријом каблова се уводе додатни параметри перформанси *Power-Sum Near-End Crosstalk* (*PS-NEXT*),

Equal-Level Far-End Crosstalk (*EL-FEXT*), и Power-Sum Equal-Level *Far-End Crosstalk (PS-ELFEXT)*. И поред стриктних спецификација које кабл категорије 5е мора да задовољи он ипак не омогућава дуже мрежне сегменте од 100 метара.

Категорија 6 (*CAT6/Class E*) представља категорију каблова који имају пропусни опсег од 250MHz и подржавају гигабитни пренос података. Ова категорија каблова има још строжије параметре перформанси од каблова категорије *CAT5e*. *CAT6* компоненте морају бити компатибилне са компонентама нижих категорија.

Категорија 6а (*CAT6a/Class EA*) је дизајниран да подржи захтеве за 10-гигабитним Етернетом преко упредених парица до 100 метара дужине. Пропусни опсег је проширен са 250MHz на 500MHz. Такође, уводи се и нови параметар *Alien Crosstalk* (*ANEXT*) и представља мерење преслушавања које долази са околних-суседних каблова. За категорију *CAT6a* се могу употребљавати *UTP* и *FTP* врсте каблова.

Категорија 7 (*CAT7/Class F*) дизајниран је да подржи захтеве 10-гигабитног Етернета. Стандард специфицира фреквенције од 1-600MHz преко потпуно оклопљених упредених парица дужине до 100 метара. Са оваквим карактеристикама каблови категорије 7 су идеални у просторијама где постоји висок степен електромагнетних сметњи. Завршавају се *GG45* конекторима (*GigaGate*) или модулима. *GG45* конектор има 4 додатна пина у односу на *RJ45* конектор. Ови додатни пинови ће се користити у будућности за још 2 парице за пренос података при брзинама од 10Gb/s.

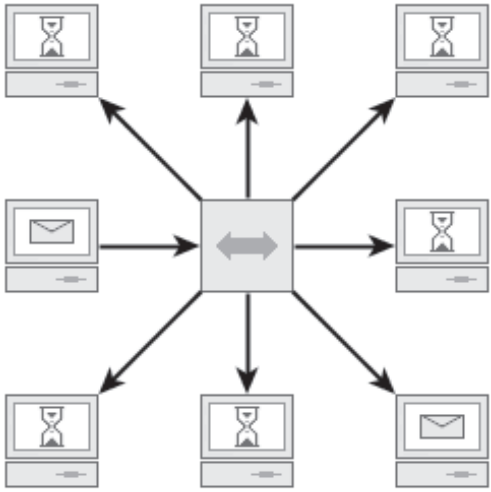
2.1.3.1. Разводници

Први мрежни уређај који се јавио код преласка Етернет технологије на каблове са упреденим парицама је разводник (енгл. *hub*). Ово је уређај једноставне конструкције и може се посматрати као **вишепортни дигитални појачивач сигнала**. Другим речима, улога разводника је да сваки примљени бит проследи кроз све сопствене портове (осим кроз порт са кога је бит примљен).

Разводници, као и дигитални појачивачи сигнала, раде на нивоу битова. То уједно значи и да се уметањем сваког новог разводника у комуникацију кашњење повећава за један бит, односно за време потребно да се тај бит пренесе.

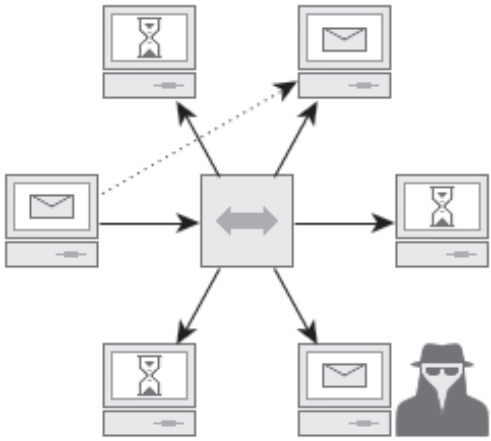
Увођењем разводника физичка топологија Етернет мрежа је од магистрале прешла на топологију звезде, односно стабла у случају коришћења више разводника. Логичка топологија се увођењем разводника није мењала пошто сви чланови мреже добијају све податке који се њоме преносе.

Гледано са аспекта перформанси само увођење разводника није довело до побољшања перформанси Етернет мрежа. Разлог томе је што је са употребом разводника омогућена само једна комуникација у целој мрежи у једном тренутку.



Слика 1. Разводници се понашају као вишепортни појачивачи сигнала

Са аспекта безбедности, односно приватности, нема побољшања код употребе разводника уместо топологије магистрале код прве генерације Етернета. С обзиром да разводници добијене оквире прослеђују свим члановима мреже, довољно је да се нападач прикључи мрежи па да може да чита садржај свих комуникација које се у тој мрежи обављају.

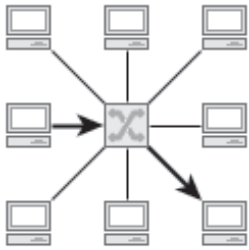


Слика 2. Приватност остаје проблем и код употребе разводника

Иако преласком на каблове са упреденим парицама и разводнике није дошло до промене логичке топологије магистрале, на тај начин су ипак постигнута одређена побољшања - омогућено је додавање нових чланова без прекида у функционисању мреже, а прекид везе једног рачунара са мрежом није угрожавао рад осталих чланова.

2.1.3.2. Комутатори

На исти начин на који Етернет разводник представља вишепортни дигитални појачивач сигнала, комутатор представља вишепортни мост. За разлику од Етернет мостова, који имају само два порта и који су првенствено предвиђени за повезивање мрежних сегмената, Етернет комутатори имају више портова (5,8,16,24,48...) и углавном се сви крајњи уређаји директно повезују са њима.



Слика 1. Комутатори прослеђују оквир само станици на коју је адресован

Следећа разлика између Етернет разводника и комутатора је ниво на ком они раде. Разводници раде на нивоу битова, док комутатори раде на нивоу оквира. То значи да комутатори прихватају комплетан оквир и, након тога, прослеђују га кроз одређени порт, на основу одредишне адресе. Оваквим начином рада су постигнута бројна и значајна побољшања:

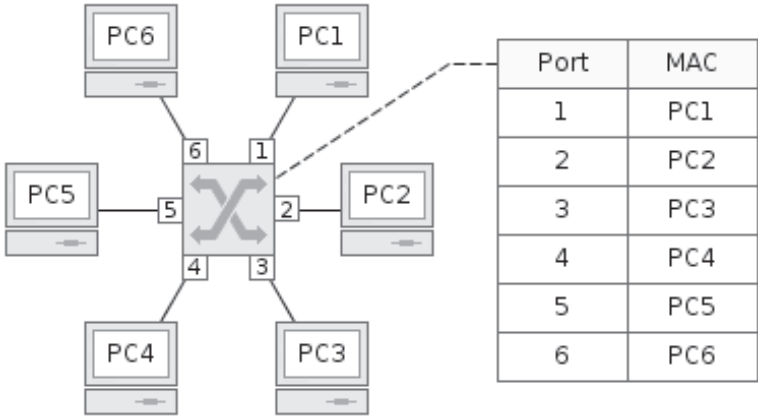
- Омогућен је потпуни дуплекс, односно паралелно слање и пријем оквира.
- Избегнуте су колизије оквира.
- Омогућена је паралелна комуникација између различитих станица у мрежи.
- Значајно је подигнута безбедност у мрежи с обзиром да подаци више не стижу до свих чланова мреже.
- Омогућено је увођење нових, напредних функција у Етернет мреже.

Са друге стране, постоје два главна недостатка комутатора у односу на

разводнике:

- Значајно је повећана сложеност уређаја, чиме је повећана и њихова цена, као и могућност отказивања.
- Кашњење је подигнуто са нивоа бита на ниво оквира (или заглавља оквира у одређеним режимима рада).

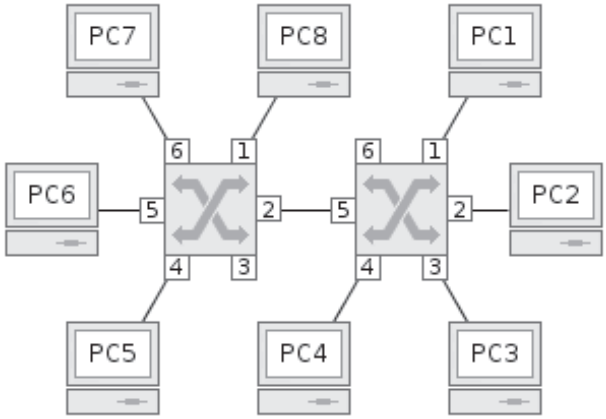
Да би комутатори могли да прослеђују оквире само станицама на које су адресовани, они користе одредишну адресу оквира. У меморији комутатора се налази табела која садржи информације на ком порту се налази која Етернет станица (одредишна адреса) и на основу те информације се одређује кроз који порт ће оквир бити прослеђен.



Слика 2. Комутатори користе табелу која повезује адресе и портове

Посебна карактеристика комутатора односи се на начин на који се ове информације, које повезују адресе и портове, формирају у табелама комутатора. Уместо да се оне уносе ручно, од стране администратора, оне се аутоматски ту формирају на основу могућности комутатора да „учи“. Овај процес се одвија тако што комутатор за сваки примљени оквир анализира порт путем кога је оквир примљен и изворишну адресу оквира. Овај пар података се, уколико већ тамо не постоји, уноси у табелу адреса. На тај начин се будући оквири, адресовани на поменуту адресу, прослеђују кроз наведени порт.

Port	MAC
1	PC8
2	**PC1**
2	**PC2**
2	**PC3**
2	**PC4**
4	PC5
5	PC6
6	PC7



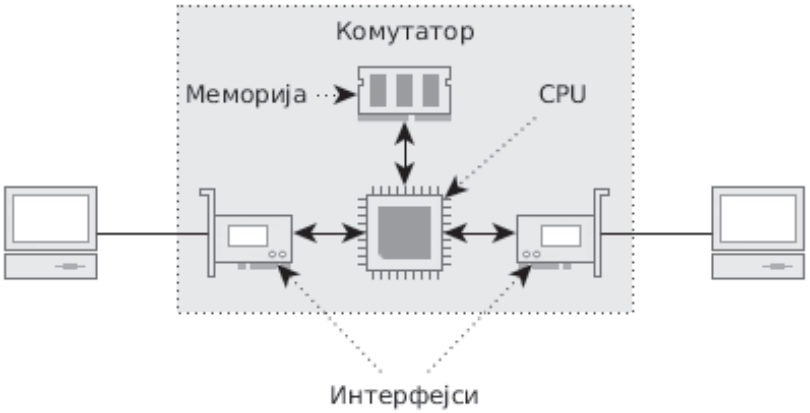
Port	MAC
1	PC1
2	PC2
3	PC3
4	PC4
5	**PC5**
5	**PC6**
5	**PC7**
5	**PC8**

Слика 3. Код сложенијих мрежа могуће су вишеструке асоцијације

Комутатори данас представљају подразумеване уређаје за формирање Етернет мрежа. Њихова цена се креће од 10-ак, па до неколико стотина хиљада долара.У складу са тим, и њихове могућности, пропусна моћ, број портова и напредне функције се драстично разликују.

2.1.3.2.1. Архитектура комутатора

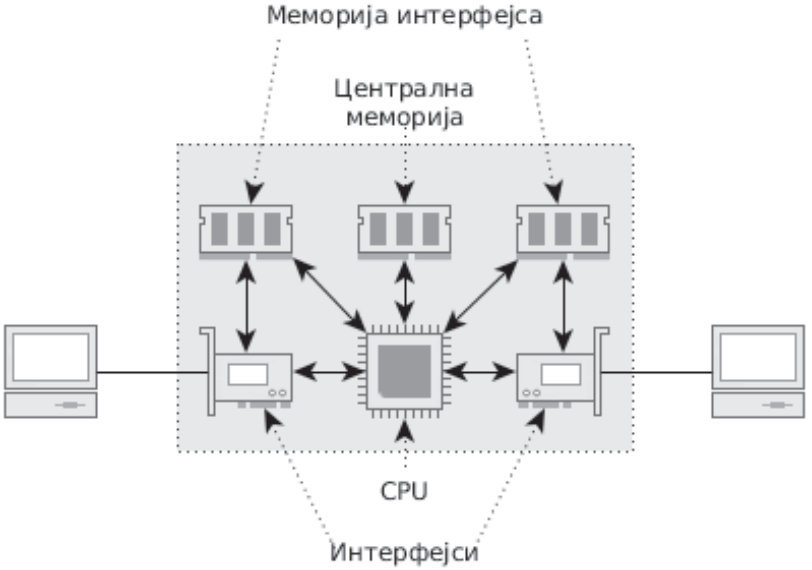
У складу са сложеним функцијама које обављају комутатори су уређаји са сложеном архитектуром. У питању су прави мали рачунари чији је хардвер и софтвер прилагођен обављању уско-специјализованог задатка - прослеђивању оквира.



Слика 1. Архитектура комутатора

У основне компоненте комутатора спадају централни процесор, меморија, мрежни интерфејси и софтвер (оперативни систем, фирмвер). Улога централног процесора је да извршава системски софтвер комутатора, односно да извршава

функције потребне за прослеђивање оквира. Улога меморије је двојака. У меморији се налазе подаци потребни за одлучивање приликом прослеђивања оквира (табела са паровима адреса-порт). Додатно, у меморији се привремено складиште пристигли оквири - до тренутка доношења одлуке кроз који порт их треба проследити и до ослобађања везе на том порту (уколико је, евентуално, заузета).



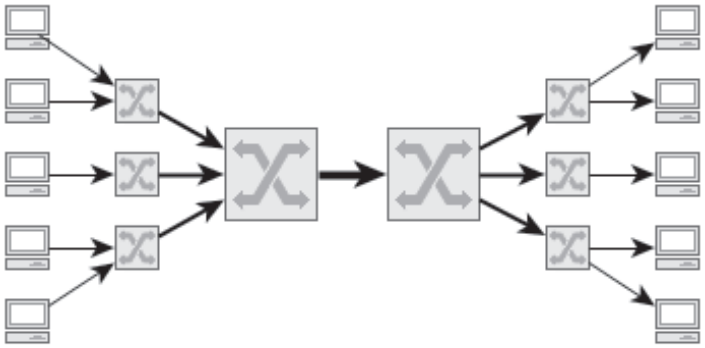
Слика 2. Архитектура комутатора са посебним меморијама

Неки комутатори имају обједињену меморију, док код неких постоје посебне меморије за сваки порт. Таква архитектура онемогућава да преоптерећење на једном порту утиче на остале портове. Међутим, иста функционалност се може постићи и додатним инструкцијама код обједињене меморије. Додатно, засебне меморије захтевају додатно време за копирање (из меморије улазног порта у меморију излазног).

2.1.3.2.2. Пропусна моћ

Пропусна моћ комутатора је једна од његових основних карактеристика. При том, пропусна моћ комутатора постоји на два нивоа - као пропусна моћ појединачних портова и као укупна пропусна моћ комутатора. Пропусне моћи по портовима углавном износе између 100Mb/s и 10Gb/s. Са друге стране, укупна моћ комутатора који има 48 портова, од којих сваки има пропусну моћ 1Gb/s би требало да буде 48Gb/s. У пракси, само напреднији (и скупљи) комутатори имају такав однос пропусних моћи. Код јефтинијих комутатора се

полази од претпоставке да неће сви портови истовремено бити коришћени у максималном капацитету, тако да се укупна пропусна моћ поставља на 10-50 процената оне која је теоретски потребна.



Слика 1. Различите позиције захтевају различите пропусне моћи

У правилно пројектованој рачунарској мрежи комутатори који се налазе у језгру мреже имаће већу пропусну моћ од комутатора који се налазе на рубу мреже. Потребна пропусна моћ може се оквирно израчунати множењем броја канала са очекиваном употребом.

2.1.3.2.3. Напредне функције комутатора

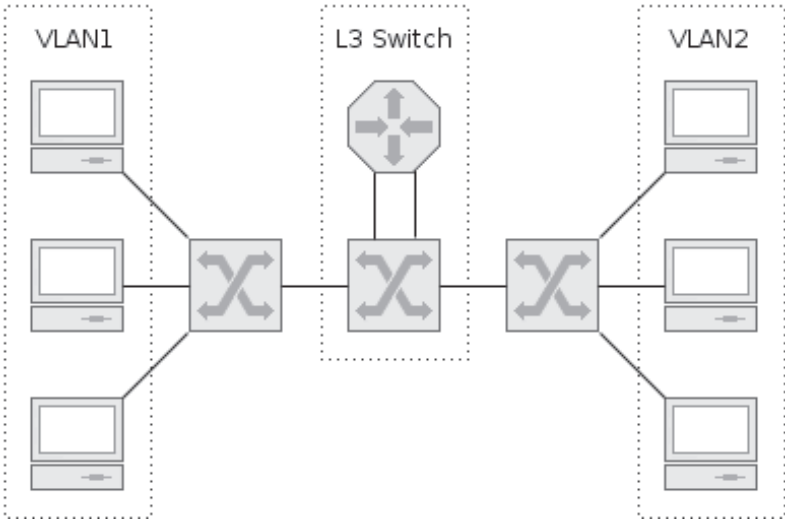
Осим по пропусној моћи, броју портова и типу подржаног медија, комутатори се разликују и по томе да ли поседују напредне функције или не. У напредне функције, пре свега, спада да ли је комутатор управљив или не. Комутатори који нису управљиви имају подржане основне функције и измена њиховог начина рада није могућа.

Слика 1. Управљиви комутатори дозвољавају промену њиховогначина рада

Насупрот томе, управљиви комутатори нуде могућност да се њихово понашање измени. На пример, могуће је мењати режиме и брзине рада портова, њихово искључивање/укључивање, управљање додатним протоколима... Управљање комутаторима се обавља кроз одређени интерфејс (конзолни, Веб и сл.).

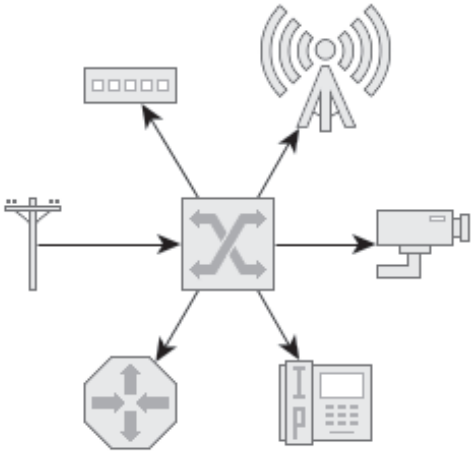
У великим рачунарским мрежама постоји могућност за изоловање одређених

група чланова у тзв. виртуалне мреже на локалном подручју (енгл. *Virtual Local Area Network, VLAN*). Ове мреже деле исту физичку инфраструктуру, али се понашају као физички потпуно одвојене мреже. Да би се то омогућило комутатори морају да имају подршку за VLAN мреже, односно за IEEE 802.1Q протокол.



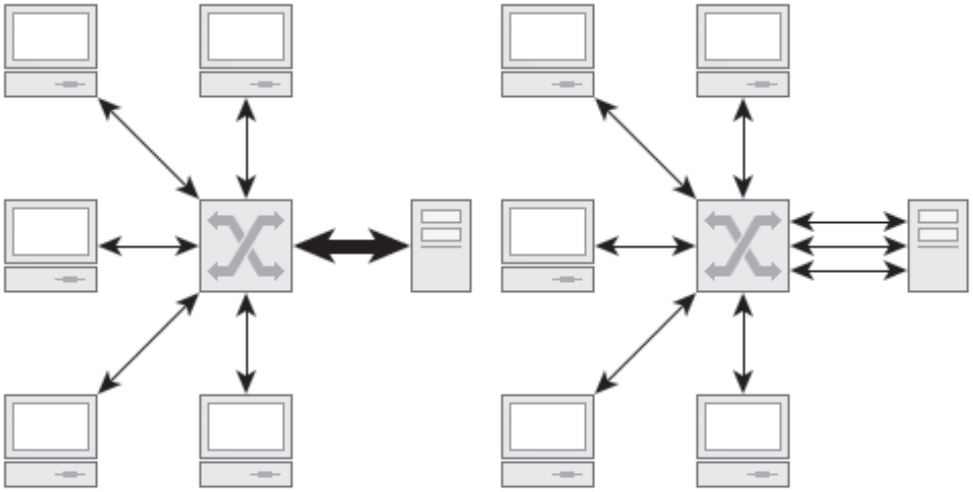
Слика 2. Комутатори 3. нивоа се понашају као рутери

Посебну врсту подршке за VLAN мреже имају такозвани L3 комутатори, односно комутатори који раде на 3. нивоу OSI модела. Такви комутатори се понашају као рутери, односно омогућавају међумрежну комуникацију, односно комуникацију између чланова различитих VLAN-ова.



Слика 3. Напајање уређаја електричном енергијом кроз мрежни кабл

Једна од веома корисник карактеристика комутатора је и могућност напајања крајњих уређаја електричном енергијом кроз мрежни кабл. Та функција је веома корисна за мање уређаје - камере, телефоне, бежичне приступне тачке и слично.



Слика 4. Асиметрични комутатори и агрегација канала

У пракси, комутатори веома често немају потребу за симетричним радом, односно за истом пропусном моћи на свим портовима. На пример, у мрежи у којој клијенти комуницирају са сервером очекује се далеко веће оптерећење порта на који је привезан сервер од оптерећења на портовима на које су повезани клијенти. Из тог разлога комутатори често имају један или два порта веће брзине (обично 10 пута веће брзине од осталих портова). Такви портови се често користе и за повезивање са осталим комутаторима.

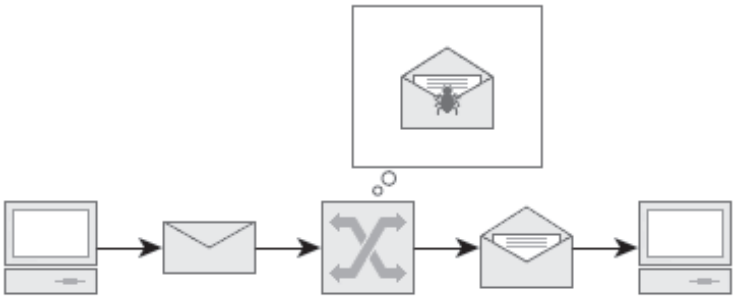
2.1.3.2.4. Режими рада комутатора

Комутатори подразумевано прихватају цео оквир, проверавају да ли се десило оштећење током преноса и прослеђују га даље на основу одредишне адресе у заглављу. Овакав начин рада се назива „складишти и проследи“ (енгл. *store and forward*).

Режим рада са преузимањем комплетног оквира пре прослеђивања је ефикасан у том погледу да ће се пренос оштећених оквира спречити на првом комутатору на који оквир наиђе након оштећења. Другим речима, оштећени оквири неће оптерећивати остатак мреже већ ће се одмах искључити из саобраћаја.

У основне недостатке режима рада са складиштењем комплетних оквира

спадају повећано кашњење током преноса и додатно оптерећивање меморије и процесора комутатора. Из тог разлога одређени комутатори имају подршку и за алтернативни начин рада, познат под називом „просецање“ (енгл. *cut throught*). Код овог режима рада комутатор прослеђује примљене битове већ након пријема одредишне адресе у заглављу оквира, односно након пријема информације коме треба прослеђивати примљене битове.



Слика 1. Комутатор у режиму рада складиштења и прослеђивања

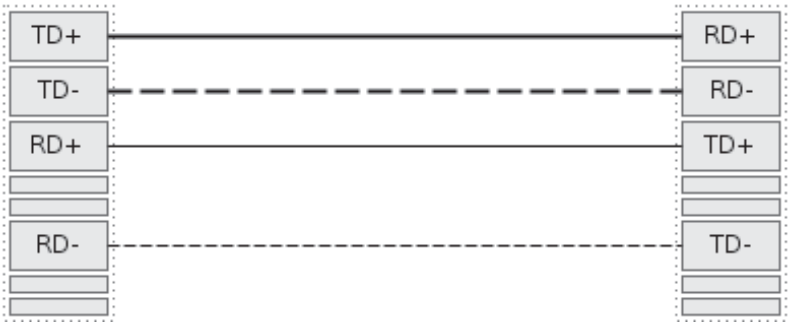
Режим рада са просецањем може значајно да смањи кашњење током преноса података. На примеру оквира којим се преноси 1.500 бајтова садржаја, кашњење у режиму складиштења и прослеђивања износи 1.522 бајта (укупна дужина оквира), док кашњење у режиму просецања износи свега 6 бајтова. Преведено у временске јединице, на примеру гигабитне Етернет мреже са једним комутатором као посредником, ова кашњења износе приближно 48 наносекунди код просецања, односно 12 микросекунди код складиштења и прослеђивања. Кашњење се умножава са сваким додатним комутатором као посредником, а приликом рачунања није узето у обзир време које је потребно комутатору да провери исправност оквира у режиму складиштења и прослеђивања.

Слика 2. Комутатор у режиму рада „просецања“

Због значајног смањивања кашњења режим просецања често се користи у мрежама заснованим на оптичким кабловима (мала вероватноћа грешке), односно у мрежама код којих смањивање кашњења има висок значај (мреже за складиштење података које користе *iSCSI*, мреже за повезивање чворова суперрачунара и слично).

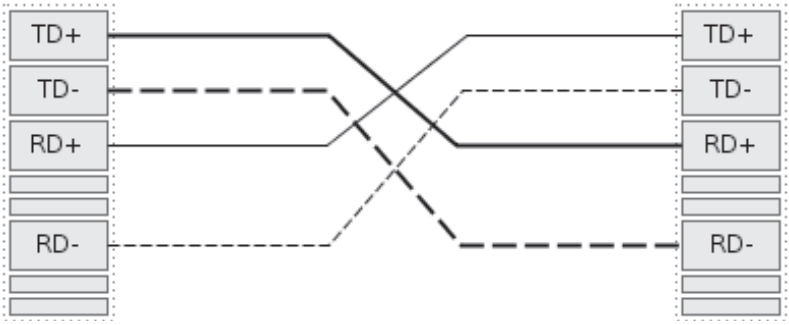
2.1.3.2.5. Типови веза у Етернет мрежама

Каблови са упреденим парицама који се користе код Етернет мрежа имају 4 пара жица у себи. Постоје два основна распореда ових жица на крајевима кабла, у конекторима (RJ45). То су 568A и 568B. У суштини нема значајне разлике између ова два стандарда за распоређивање жица у конекторима. Међутим, оно што прави разлику јесте то да ли је на оба краја кабла коришћен исти или различит распоред.



Слика 1. Исти распоред жица на оба краја користи се за директно повезивање

Уколико се на оба краја кабла користи исти распоред жица, такав кабл се назива каблом за директно повезивање (енгл. *strait-through*). Овакав кабл се користи за повезивање уређаја који раде на различитим нивоима OSI модела, пре свега за повезивање крајњих уређаја са комутаторима. Насупрот томе, уколико се на крајевима кабла користи различит распоред жица, такав кабл се назива каблом за премошћавање (енгл. *crossover*). Овакав кабл се користи за повезивање уређаја који раде на истом нивоу OSI модела, првенствено за међусобно повезивање комутатора.



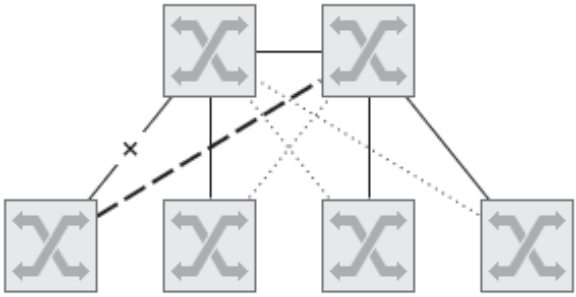
Слика 2. Различит распоред жица на крајевима користи се за међусобно повезивање комутатора

Захваљујући Auto MDI-X (auto medium dependent interface crossover) функцији

већина савремених Етернет уређаја има могућност да се аутоматски прилагоди било ком типу кабла. Међутим, за коришћење напреднијих функција комутатора веома је важно користити исправне типове каблова јер комутатори на основу тога могу да утврде да ли су повезани са другим комутатором или крајњим уређајем.

2.1.4. Перформансе и расположивост

С обзиром да рачунарске мреже имају све критичнију улогу у пословним системима, све више расте потреба да се повећају њихова расположивост (робусност, отпорност на отказивање) и перформансе. Повећање расположивости се у главном постиже додавањем редундантних компонената, односно компонената које ће преузети радну улогу у случају отказивања примарних компонената. У правилно пројектованој Етернет мрежи постоји алтернатива за све критичне комутаторе и канале.

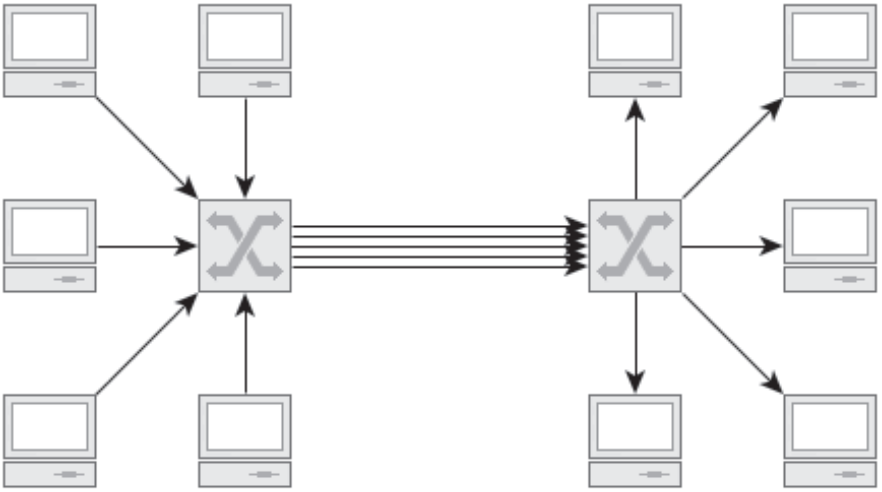


Слика 1. Редундантни канали улазе у употребу у случају отказивања примарних

Када је у питању подизање перформанси рачунарске мреже, оно се до одређене границе може постићи вертикалним скалирањем, односно коришћењем напреднијих медија (на пример, оптика уместо бакарних каблова) и комитатора са бољим перформансама. Међутим, након достизања те границе потребно је применити хоризонтално скалирање, односно додавање више ентитета (комутатора, каблова...) који ће радити паралелно.

Да би вишеструки каблови између два комутатора служили сврси, односно да би паралелено учествовали у преносу података, потребно је да комутатори имају подршку за такво њихово коришћење, односно за **агрегацију**. Агрегација је могућност комутатора да на више портова гледа као на један. Наравно, потребно је да комутатори са обе стране вишеструких канала имају одговарајућу подршку, односно да поседују могућност агрегације и да буду исправно подешени. Осим између комутатора, агрегација се може искористити и за

повезивање комутатора са крајњим уређајима високог оптерећења (нпр. сервером) чији мрежни интерфејс има подршку за агрегацију.



Слика 2. Агрегација вишеструких канала у циљу подизања перформанси

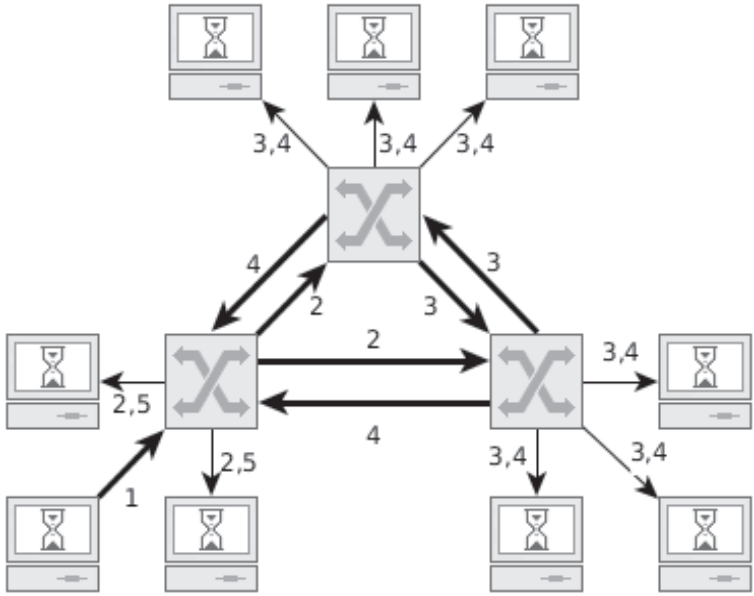
При свему наведеном треба имати у виду да комутатори морају да имају подршку за агрегацију да би додавање вишеструких канала довело до жељеног резултата. У противном, могу се јавити два исхода:

1. Комутатори који имају подршку за протокол разгранатог стабла елиминисаће све вишеструке канале осим примарног и на њих ће гледати као на резерве у случају његовог отказивања.
2. Комутатори који немају подршку за протокол разгранатог стабла ући ће у бесконачне петље код прослеђивања оквира и цела мрежа ће на крају бити оборена.

Дакле, може се закључити да је протокол разгранатог стабла критична компонента у Етернет мрежама за њихов несметан рад у случајевима када се јаве вишеструке путање, односно када се угрози топологија стабла.

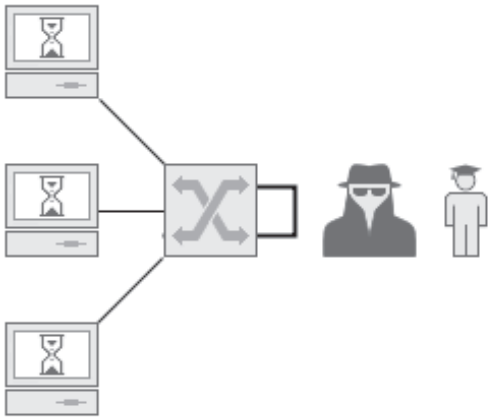
2.1.4.1. Протокол разгранатог стабла

У случају када се у Етернет мрежама наруши топологија (разгранатог) стабла, односно када се јаве вишеструке путање којима се може стићи до истог одредишта, таква мрежа ће подразумевано почети да бесконачно понавља прослеђивање оквира упућених свим члановима мреже. Првих пет цикулса тог бесконачног понављања илустрован је на следећи начин:



Слика 1. Бесконачно кружење оквира упућених свим члановима мреже

Треба имати у виду да се приказана кружења оквира бесконачно понављају (односно, док год се мрежа не искључи или петља отклони), а да се постојећим оквирима додају и сви нови оквири који су послати свим члановима мреже. Код сложенијих топологија - код којих постоји више вишеструких путања - оквири не само да бесконачно круже, већ се и умножавају у свакој итерацији. Коначан исход у оваквим ситуацијама је пораст оптерећења мреже и смањивање брзине преноса корисних података до потпуне неупотребљивости.

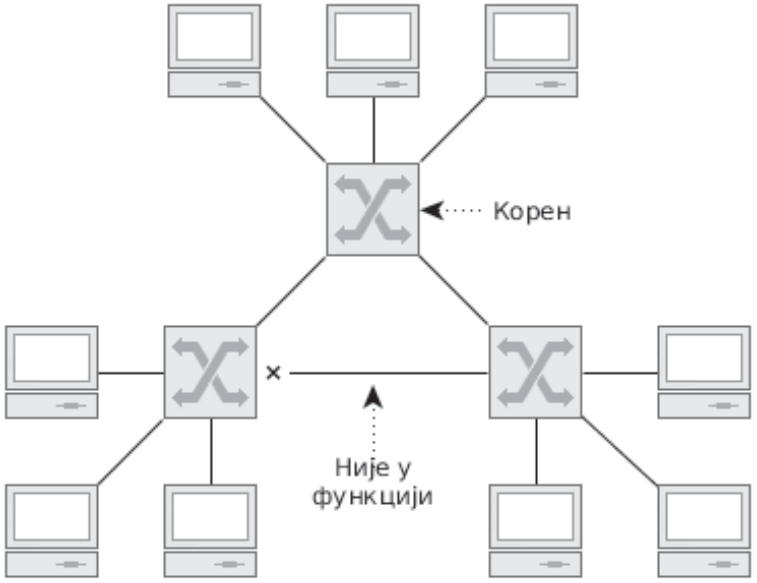


Слика 2. Узроци петљи могу бити намерна/ненамерна додавања каблова

Узроци настајања вишеструких путања у мрежама, које доводе до престанка

њиховог рада, могу бити различити, односно ненамерна или намерна додавања каблова. У првом случају то могу бити грешке проузроковане непажњом, недостатком документације и слично. У другом случају то могу бити нападачи који имају физички приступ комутаторима (довољно је свега неколико секунди за утакање два краја једног кабла у два порта на једном комутатору).

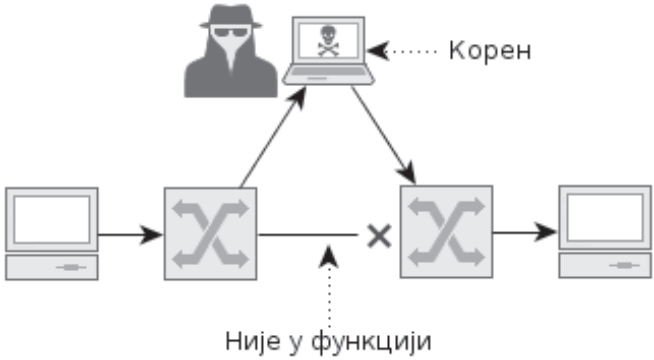
Улога **протокола разгранатог стабла** (енгл. *Spanning Tree Protocol, STP*) је да у Етернет мрежи са вишеструким путањама те путање открије и елиминише их. Са аспекта топологије мреже, улога STP протокола је да топологију мреже преведе у топологију разгранатог стабла.



Слика 3. Пример резултата примене STP протокола

Да би протокол разгранатог стабла имао ефекта сви комутатори у мрежи морају да га подржавају. Његов принцип рада се своди на то да комутатори приликом сваке промене топологије, односно приликом сваког додавања или уклањања неке од веза, изврше проверу да ли је негде направљена петља. Уколико се утврди да је до тога дошло, дупле везе се уклањају путем деактивирања једног од портова које оне повезују. Везе и портови који ће бити деактивирани одређују на основу удаљености од **кореног комутатора** (енгл. *root bridge*) који се аутоматски одређује у првој фази извршавања протокола.

Процес избора кореног комутатора је могуће у одређеној мери контролисати. При том, треба имати у виду да је STP протокол могуће злоупотребити за нападе на рачунарске мреже.



Слика 4. Могућа злоупотреба STP протокола

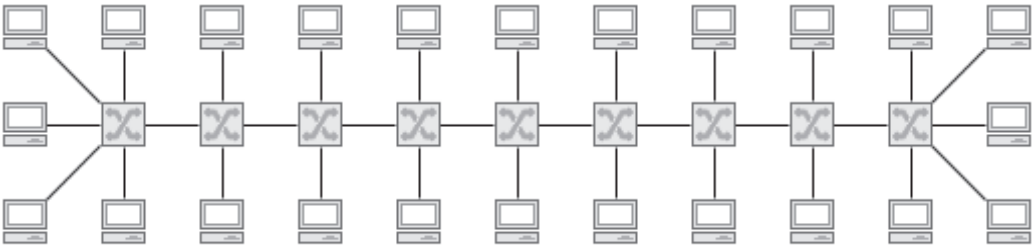
На пример, нападач може свој уређај да повеже са постојећим комутаторима у и да их натера да сав саобраћај преусмере на његов уређај. На тај начин је могуће напасти сва три аспекта безбедности - поверљивост, веродостојност и расположивост.

2.1.5. Организација и архитектура мреже

Иако сама Етернет технологија омогућава различито распоређивање опреме и организацију мреже, различити начини се могу драстично разликовати по расположивости и перформанси. Два основна приступа која треба узети у обзир код пројектовања мреже су хијерархијски модел и структурно каблирање.

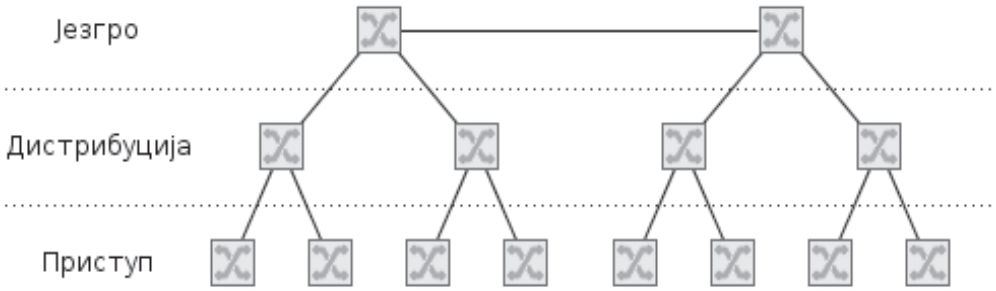
2.1.5.1. Хијерархијски модел мреже

Комутаторе у Етернет мрежи могуће је распоредити на различите начине. На пример, могуће их је линијски повезати, односно сваки комутатор повезати са два суседна комутатора. Мрежа која би се правила на такав начин имала би веома ограничен простор за ширење, кашњење током преноса података би било велико, а перформансе комуникација између удаљених чланова тежиле нули.



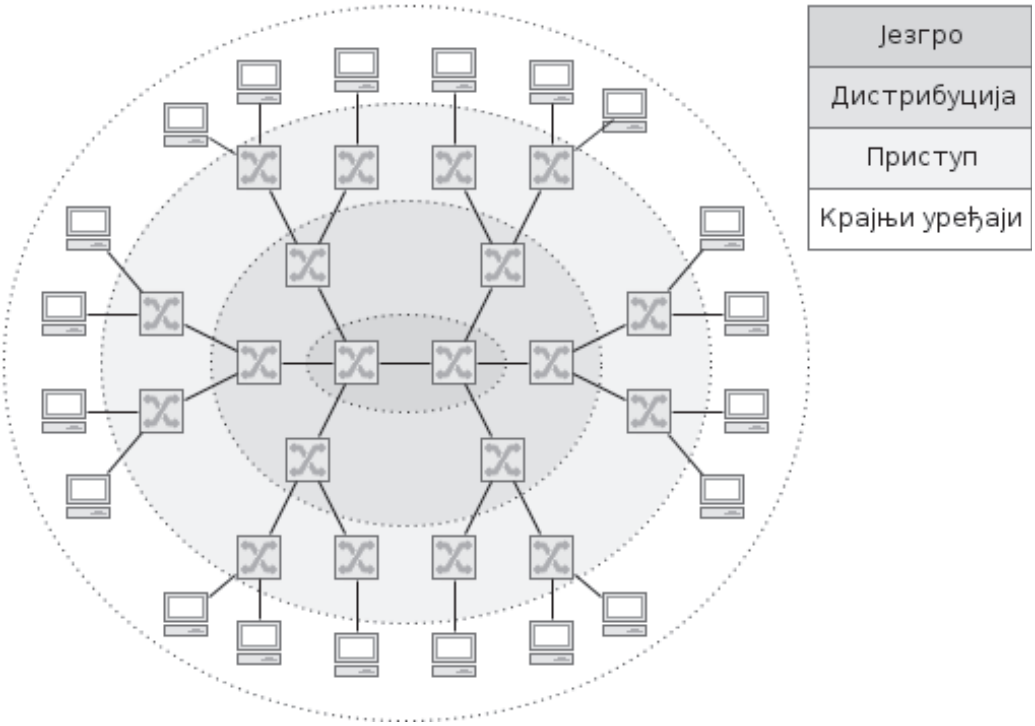
Слика 1. Линијска организација - велико кашњење и ниске перформансе

Хијерархијски модел мреже дефинише начин на који је оптимално повезивати комутаторе, односно начин на који ће се у великим мрежама омогућити даља проширивања, минимално кашњење и максималне перформансе. Три основна слоја код хијерархијског мрежног модела су језгро, дистрибуција и приступ.



Слика 2. Слојеви хијерархијског мрежног модела

Слој језгра представља кичму рачунарске мреће и задужен је да повеже њене критичне центре везама са високом расположивошћу и перформансама. Овај слој најчешће чини мањи број комутатора, високог квалитета израде, високих перформанси, подршком за медије високих перформанси (каблове са оптичким влакнима) и напредним функцијама као што је агрегација портова и редунданса.



Слика 3. Повезивање крајњих уређаја путем хијерархијског модела

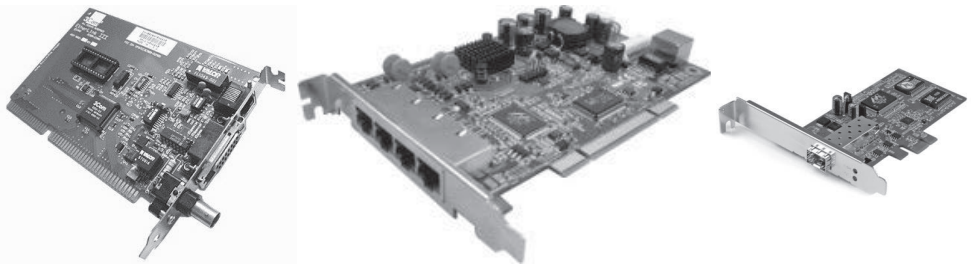
Слој дистрибуције хијерархијског модела је задужен да језгро мреже повеже са слојем приступа, односно да комутаторе на које су везани крајњи уређаји повеже са комутаторима у језгру. Комутатори дистрибутивног слоја имају средње перформансе, али такође треба да поседују подршку за функције као што су агрегација портова и редунданса.

Слој приступа хијерархијског модела задужен је да крајњим уређајима омогући приступ рачунарској мрежи, односно да их повеже са мрежом. Комутатори на овом слоју обично имају ниже перформансе и квалитет израде, али се код њих очекује велики број портова и функције као што су напајање електричном енергијом кроз мрежни кабл.

Једна од важних ствари у рачунарским мрежама, на коју одговор даје хијерархијски модел, јесте пречник мреже. Пречник мреже представља највећи могући број посредујућих уређаја кроз које оквири могу да прођу на путу кроз мрежу. Што је пречник мреже већи, то је веће кашњење и потенцијални пад перформанси. Код мрежа урађених по хијерархијском моделу пречник мреже је највише 6.

2.1.6. Рачунарски интерфејси за Етернет мреже

Етернет, као основни стандард за жичне приватне мреже, изузетно добро је подржан од стране произвођача хардвера и софтвера корисничких рачунара и сервера. Етернет интерфејси се данас подразумевано уграђују на матичне плоче стоних и преносивих рачунара.



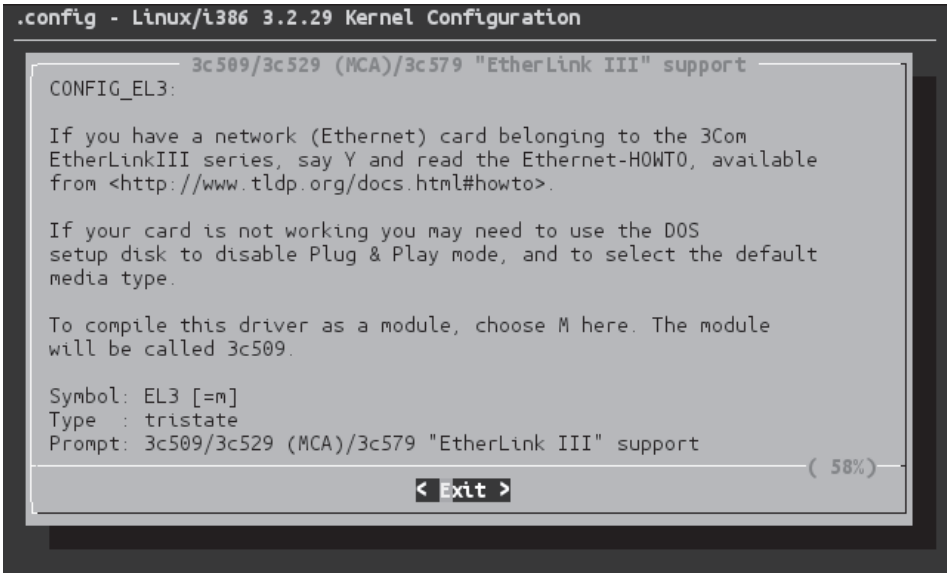
Слика 1. Различити рачунарски интерфејси за различите Етернет медије

С обзиром на разноврсност Етернет стандарда (пре свега медија за пренос података), као и на разноврсност интерфејса савремених рачунара (PCI, USB...) постоји велики број варијација и у погледу додатног хардвера за Етернет повезивање. Неки мрежни интерфејси су прављени тако да подрже више различитих медија (на пример, коаксијалне каблове и каблове са упреденим парицама на истој картици), док су неки интерфејси пројектовани тако да

омогуће високе перформансе и вишеструко паралелно повезивање (најчешће код сервера).

Слика 2. Гигабитни Етернет адаптер са USB 3.0 интерфејсом

Препреке за интегрисање Етернет интерфејса на преносиве уређаје (таблети, мобилни телефони и слично) су, пре свега, смањена преносивост уређаја жичним умрежавањем, као и величина Етернет порта наспрам величине (дебљине) самог уређаја. Међутим, и за ове уређаје постоје интерфејси, најчшће намењени за повезивање путем *USB* порта.



Слика 3. Подршка за одређени Етернет адаптер у Линукс ОС

Да би одређени рачунарски систем могао да се повеже са Етернет мрежом потребно је да, осим поседовања одговарајућег хардверског интерфејса, његов оперативни систем има подршку за тај интерфејс. Ова подршка се остварује

путем драјвера за одређени оперативни систем а углавном сви популарни интерфејси су подржани и на *MS Windows* и Линукс оперативним системима.

2.2. WiFi - IEEE 802.11

Wi-Fi - Wireless-Fidelity је популарни назив за бежичне технологије средњег домета где се пренос података имеђу два или више рачунара врши путем радио таласа уз примену одговарајућих антена. *Wi-Fi* технологија се користи у бежичним *LAN* мрежама (*WLAN*), али и за бежични приступ Интернету. Основни стандарди којима се дефинише ова технологија су *IEEE* 802.11a, 802.11b, 80.11g и 802.11n. Први стандарди су дефинисани половином деведесетих година XX века и подржавали су ниске брзине преноса података (1-2 Mb/s).

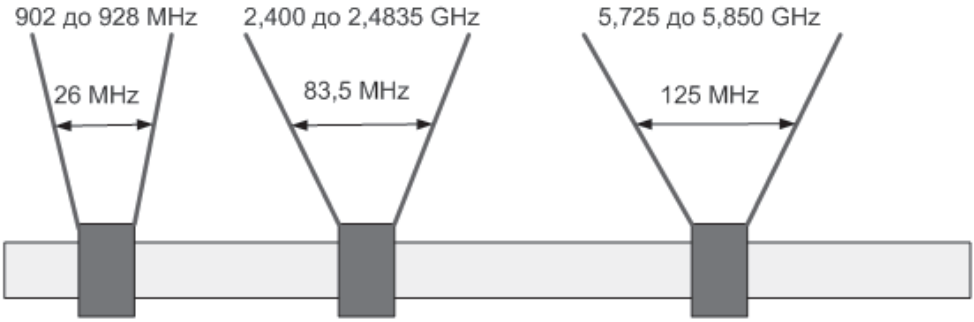
Стандарди *Wi-Fi* су:

- 802.11a стандард из 2002. године подржава максималну теоријску брзину преноса података од 54Mb/s, али она најчешће износи око 30Mb/s. Ради на 5*GHz*.
- 802.11b стандард представљен је 1999. Брзина протока података је до 11Mb/s, али уз велике препреке и сметње брзина може спасти на минималних 1 до 2 Mb/s. Ово је уједно и најјефтинија варијанта *WiFi* мреже.
- 802.11g је представљен 2003. године и објединио је претходна два стандарда. Ради на 2,4GHz, али има скоро исту брзину као и 802.11a стандард.
- 802.11n ради на 2,4GHz или на 5GHz, са максималном брзином преноса података до 150Mb/s.

Радио комуникација код *WLAN*-ова се обавља у тзв. *ISM* (*Industrial, Scientific & Medical*) опсегу фреквенција који је свуда у свету прихваћен као опсег за чије коришћење није потребна лиценца тзв. *FTA* (*free to air spektar*).

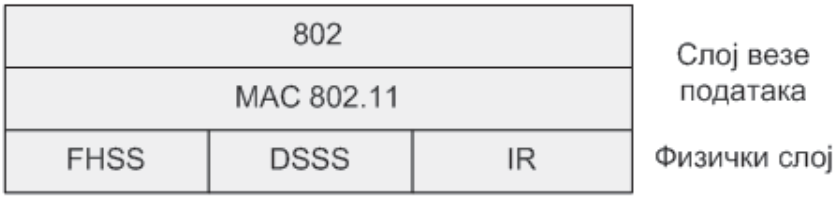
ISM чине три опсега фреквенција: 902 - 928MHz, 2.400 - 2483,5MHz и 5.728 – 5.750MHz. У овом тренутку најчешће се користи опсег око 2,4GHz. *WLAN*-ови користе технику рада у проширеном спектру (*Spread Spectrum*). Добро познате технике су фреквенцијско скакање (*FHSS – Frequency-Hopping Spread Spectrum*), рад са директним секвенцама (*DSSS – Direct-Sequence Spread Spectrum)* и коришћење тзв. Ортогоналних фреквенција (O*FDM – Orthogonal Frequency Division Multiplexing*). Наиме, више корисника истовремено деле исти фреквенцијски опсег без међусобне интерференције и пружају много већу

отпорност на сметње и прислушкивање у односу на рад са фиксним фреквенцијама. Ова технологија је развијена још пре око 50 година и то за војне примене са циљем да буде максимално отпорна на ометања, интерференцију и прислушкивање.



Слика 1. ISM опсези фреквенција

IEEE 802.11 спецификација обухвата начин рада протокола физичког слоја и слоја везе података. У односу на кабловске системе овде се издваја *MAC* (*Media Access Control*) подслој који дефинише карактеристике и услуге за бежичне технологије. Физичким слојем (*Phisycal Layer*) утврђују се електричне и физичке карактеристике уређаја. *MAC* је нижи подслој слоја веза података (*Data Link Layer*) којим се утврђује почетак и крај емитованих пакета приликом примања и слања, додељује се *MAC* адреса, врши се провера грешака у преносу оквира и дефинишу се права приступа физичком слоју.



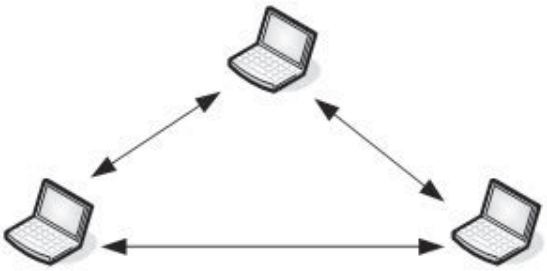
Слика 2. Приказ физичких слојева 802.11 стандарда

Три физичка слоја унутар *IEEE* 802.11 стандарда укључују рад са инфрацрвеним таласима, фреквенцијско скакање или рад са директном секвенцом.

Бежично умрежавање је вероватно најједноставнији начин умрежавања који нуди средњу брзину и не захтева додатне каблове. *WiFi* технологија обухвата *WiFi* картице (интерне или екстерне) уз које се обично испоручују и одговарајуће антене. На овај начин могуће је формирати мање мреже (мреже до 30 m). За већа растојања користе се екстерне антене које врше додатно појачање сигнала. Бежичне локалне рачунарске мреже по стандарду *IEEE* 802.11 су по дизајну

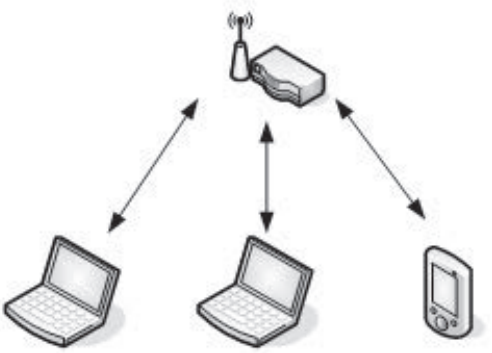
флексибилне. Постоје три типа *WLAN* топологија које се могу имплементирати.

Независан начин повезивања, често се назива и *AD-HOC* (*IBSS – Independed Basic Service Set*) а састоји се од групе 802.11 станица које комуницирају директно једна са другом. Може се посматрати и као *peer-to-peer WLAN* мрежа. За функционисање се не користи приступна тачка (*AP- Acces Point*). Обично су мале и трају све док постоји потреба за комуницирањем. Пошто је сваки уређај клијент, у комуникацији могу настати проблеми због тзв. скривеног чвора (*hidden node*).



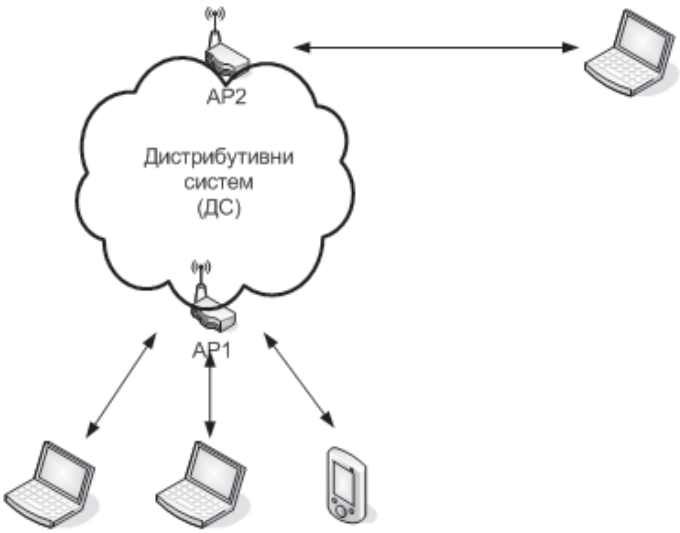
Слика 3. Ad-hoc режим рада (IBSS WLAN)

Инфраструктурни режим повезивања (*BSS – Basic Service Set*) захтева специјализовану станицу тј. тачку приступа (*AP – Access Point*). *AP* нуди покривеност од око 30 метара, док је уз разне појачиваче могуће битно проширити домет. Клијентске станице не комуницирају директно једна са другом, као у предходном случају, већ са тачком приступа. Тачка приступа прослеђује оквире одредишним станицама. Она може имати и *uplink* порт за повезивање на жичну мрежу.



Слика 4. Инфраструктурни режим рада (BSS WLAN)

Повезивање *BSS* мрежа преко жичних дистрибутивних система често носи ознаку *ESS* (*Extended Service Set*).



Слика 5. Проширени начин повезивања (ESS WLAN)

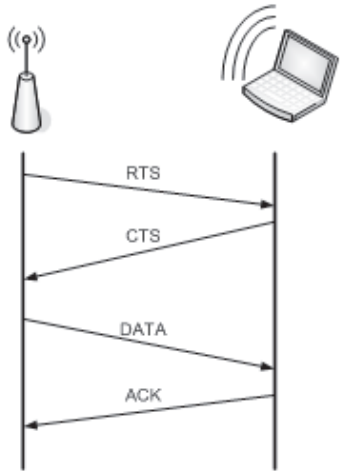
802.11 бежичне мреже користе *CSMA/CA* (*Carrier Sense Multiple Access With Collision Avoidance*) у чијој основи је принцип „слушај пре него што почнеш да говориш“ (*LBT– listen before talk*). Станица која жели да емитује прво проверава да ли постоји сигнал носиоца и чека док се канал не ослободи. *CSMA/CA* садржи правила ради спречавања колизије. Кључне компоненте *CSMA/CA* су:

1. Детекција носиоца (*carrier sense*) - Станица која жели да емитује мора да провери да ли је медијум у употеби. Уколико јесте станица ће одложити слање оквира све док медијум не постане слободан.
2. *DCF* (*distributed coordination function*) - Станица која жели да пошаље оквир мора да сачека одређени период времена након ослобађања медијума. Постоји велика вероватноћа да ће две станице покушати да шаљу када медијум постане слободан, и да ће доћи до колизије. Да би се ово избегло користи се тајмер са случајно генерисаном вредношћу (*random backoff timer*).

Да би се спречила колизија која настаје истовременим емитовањем два уређаја, према стандарду *IEEE* 802.11 примењује се *RTS/CTS* механизам.

Уколико је на неки *AP* стигао податак који је адресован на неког бежичног клијента, *AP* ће послати *RTS* оквир том клијенту, тражећи време за предају података. Клијент одговара са дифузним *CTS* оквиром, чиме саопштава *AP*-у да је спреман да прими његове податке и да у том временском периоду неће

одржавати комуникацију са другим станицама све док *AP* не заврши пренос. Други бежични клијенти "чују" овај договор па се суздржавају од комуникације. На овај начин подаци се преносе са минималном могућношћу доласка до колизије. Истовремено, овако се решава проблем тзв. "скривеног чвора". Пријемници потврђују пријем оквира без грешака слањем *ACK* оквира (потврда пријема). Уколико предајник не прими очекивани *ACK*, знаће да оквир није испоручен и извршиће ретрансмисију. Све се ово одвија у *MAC* подслоју чиме предајник, након што установи да није примио *ACK*, може заузети радио канал пре свих осталих и поновити слање. Овакав начин пружа транспарентан начин корекције преноса, односно крајњи корисник и не зна да је дошло до било каквих проблема приликом слања података.



Слика 6. Пример RTS/CTS комуникације

Неопходан предуслов за функционисање бежичних мрежа је мала потрошња електричне енергије бежичних клијената, тј. одговарајући капацитет њихових батерија. *IEEE* 802.11 је у стандард уградио начине управљања потрошњом електричне енергије на начин да бежични клијент одлази у начин рада са ниском потрошњом енергије, а без губитака везе са бежичном инфраструктуром. Како би клијент најавио одлазак у штедљиви мод рада, он *AP*-у шаље 20-битни *PS-Poll* (*Power Save*) оквир. *AP* све податке који су намењени том клијенту чува у својој меморији све време док је клијент у штедљивом режиму рада. Бежични клијент се периодично пребацује из штедљивог начина рада у нормални, како би проверио да ли постоје подаци за њега. Након провере и евентуалног пријема истих, клијент поново шаље *PS-Poll* оквир и враћа се у штедљиви начин рада. Предности овог приступа су у томе што је

време трајања батеријских извора енергије клијента продужено, а самим тим продужена је и аутономија рада.

Још једна од могућности код бежичног *LAN*-а (*WLAN*) је да се бежични клијент може кретати без потребе да мења своје мрежне параметре. Ово је важна карактеристика зато што се тиме повећава физички домет бежичних мрежа. Бежични уређаји имају могућност да одреде квалитет сигнала према било ком *AP*-у у чијем се подручју покривености налазе, те на основу тога одлучују да се пребаце са једног на други. Ова могућност се заснива на односу сигнал-шум примљеног сигнала. Како би бежични уређај могао одредити однос сигнал-шум за сваки *AP* у мрежи, *AP*-ови шаљу тзв. *beacon* поруку у којој се садрже информације о *AP*-у, као и подаци о квалитету везе. Бежични уређај ослушкује те поруке и одређује који *AP* има најбољи сигнал. Након што одреди најоптималнији сигнал, клијент шаље информацију о аутентификацији и шаље захтев за повезивањем. Током овог процеса, нови *AP* одређује са ког *AP*-а клијент долази те проверава евентуалне заостале пакете на старом АП-у који клијенту морају бити пренесени. Након тога нови *AP* шаље поруку старом да више не треба сакупљати податке за тог одређеног клијента.

Процедура преласка на други *AP* је најједноставнија ако су два посматрана *AP*-а повезана хаб уређајем, а сложенија је ако се за повезивање користи свич (због упарености интерфејса на свичу и *MAC* адресе клијента). Посебан протокол за комуникацију између *AP*-ова се користи када су они повезани преко рутера. Ако су *AP*-ови у истој подмрежи задржава се текућа *IP* адреса, а ако нису или долази до промене адресе или се примењује посебан протокол.

2.3. Протокол за разрешавање мрежних адреса

Један од главних задатака мрежног слоја јесте логичко адресовање рачунара док је слој везе задужен за пренос података. Међутим, адресовање мрежног слоја путем *IP* адреса није могуће употребити на нивоу слоја везе. Поред тога, и на овом слоју је у неким ситуацијама неопходно обезбедити систем адресовања да би се остварила веза са одређеним чланом мреже. На пример, при коришћењу Етернет технологије за директно повезивање два рачунара или за повезивање више рачунара путем хаб уређаја адресовање на слоју везе није неопходно јер у првом случају не постоје опције, а у другом сви чланови мреже добијају све поруке а затим их прихватају или одбацују у зависности од адресе мрежног слоја. Са друге стране, у већим рачунарским мрежама, које се нпр. базирају на свич уређајима, потребно је одредити и адресовање на слоју везе да би се утврдило са којим уређајем у мрежи треба успоставити везу и доставити му податке. Одређивање уређаја се, наравно, врши у складу са адресом

мрежног слоја. За адресовање на слоју везе задужен је *Address Resolution Protocol* (*ARP*) који је описан у документу *RFC 826*.

Протокол за разрешавање адресе (енгл. *Address Resolution Protocol*, *ARP*) је протокол задужен за проналажење хардверске адресе одредишта путем његове *IP* адресе. Резултат се записује у привремену меморију која се назива *ARP* кеш табела. У случају Етернет мрежа, *ARP* прокол се користи за утврђивање *MAC* адресе путем *IP* адресе. *ARP* протокол обезбеђује динамичко превођење у смислу да се превођење одвија аутоматски без потребе за доделом хардверских адреса од стране корисника.

Када се у оквир података на слоју везе података енкапсулира *IP* пакет, у њему је дефинисана *IP* одредишна адреса. На слоју везе података неопходно је да се у односу на одредишну *IP* адресу дефинише одредишна *MAC* адреса следећег чвора у мрежи. Да би се ово разрешило, у првом кораку гледа се *ARP* кеш табела изворишног рачунара и тражи се одговарајућа *MAC* адреса одредишта (мапирана преко *IP* адресе одредишног рачунара). Ако не постоји тражени запис у *ARP* табели, шаље се дифузни *ARP* пакет (датаграм), који у суштини представља питање "да ли постоји рачунар са датом одредишном *IP* адресом?" Ако постоји, дати рачунар шаље одговор са својом *MAC* адресом, ова адреса се записује на изворишном рачунару у *ARP* кеш табелу и после овог је могуће фомирати на слоју везе података оквир са прецизном *MAC* адресом следећег чвора у мрежи. Због ефикасности, и рачунар који је формирао одговор, такође врши мапирање *IP* адресе и *MAC* адресе изворишног рачунара. Ово је из разлога, што најчешће рачунар који је примао податке после тога треба да формира свој одговор.

Слика 1. Конвертовање адреса путем ARP и RARP протокола

Разматрани случај се односи на ситуацију када је рачунар са одредишном *IP* адресом био члан мреже, тј. прецизније, налазио се у сегменту пре рутера. Ако је тај рачунар (са жељеном одредишном *IP* адресом) удаљени рачунар, иза првог рутера, он није могао да одговори на постављени *broadcast* упит за разрешавање *IP* и *MAC* адресе (рутери не пропуштају *broadcast* адресе на слоју везе података). У таквом случају изворишни рачунар енкапулира свој пакет са

жељеном *IP* адресом у оквир у коме је дестинациона *MAC* адреса у ствари адреса гејтвеја који ће у следећем кораку спровести сличан протокол. До дестинационе *MAC* адресе гејтвеја се такође долази преко *ARP* протокола. Дакле, када се подаци преносе од једног до другог рачунара, а рачунари су удаљени, *IP* адресе се никада не мењају од изворишта до одредишта, а мењају се *MAC* адресе од чвора до чвора мреже. *ARP* табела садржи три параметра: *IP* адресу, *MAC* адресу и *TTL* (*Time-to-Live*), који се стандардно поставља на вредност од 20 минута.

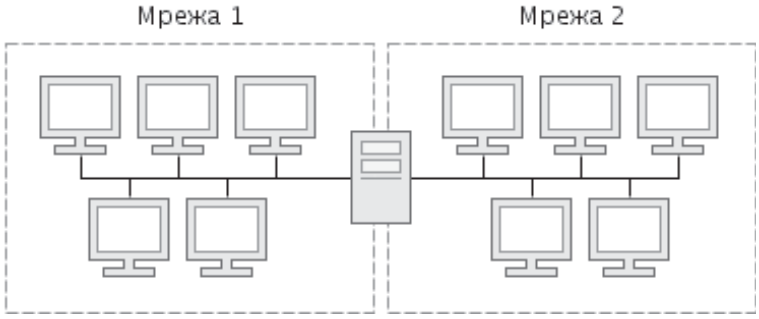
Reverse Address Resolution Protocol (*RARP*) представља инверзан протокол у односу на *ARP*. Овај протокол служи за одређивање адресе мрежног слоја (логичке *IP* адресе) путем хардверске адресе уређаја. На пример, у радним станицама које немају хард диск (*diskless workstation*) не постоји начин да се логичка *IP* адреса негде сачува, тако да се сваки пут она разрешава протоколом. За функционисање *RARP* протокола неопходно је да у локалној рачунарској мрежи постоји *RARP* сервер у коме су мапиране физичке и *IP* адресе рачунара. Наведено мапирање се врши мануелним активностима администратора мреже. *RARP* протокол започиње броадцаст захтевом (на слоју везе података) за откривање *RARP* сервера. Након добијања *MAC* адресе *RARP* сервера следи *RARP* захтев са питањем „која је моја *IP* адреса?“). *RARP* сервер формира одговор и упућује га на *MAC* адресу рачунара који је започео комуникацију.

3. Међумрежна комуникација

Технологије на физичком слоју и слоју везе података *OSI* комуникационог модела, односно на слоју приступа мрежи *TCP/IP* модела, омогућавају успостављање везе и пренос података између чланова једне рачунарске мреже. Ове технологије поседују сопствене начине адресовања чланова у циљу достављања послатих података предвиђеном примаоцу. Међутим, систем адресовања на том нивоу није у стању да омогући комуникацију између чланова различитих рачунарских мрежа.

Слика 1. Међусобно повезане различите рачунарске мреже

Задатак мрежног слоја *OSI* комуникационог модела, односно међумрежног слоја *TCP/IP* модела, јесте да кроз одговарајући систем адресовања омогући проналажење оптималних путања између учесника у комуникацији који се налазе у различитим и међусобно директно или посредно повезаним рачунарским мрежама.

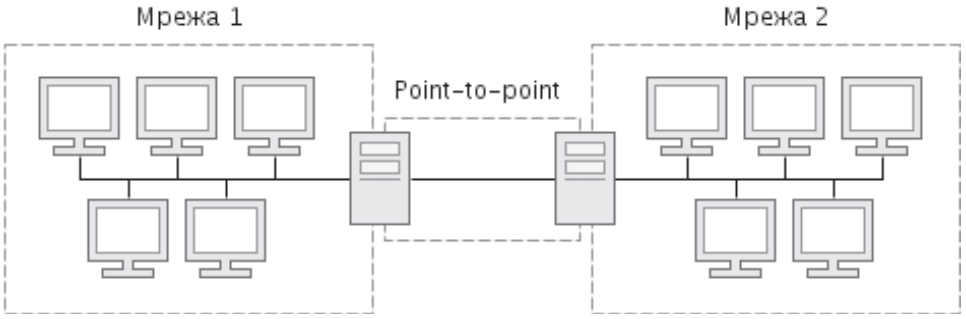


Слика 2. Вишеструко удомљавање чланова мреже

Међумрежно повезивање се заснива на постојању **пролаза** (енгл. *gateway*) између две или више мрежа, односно на **вишеструком удомљавању** (енгл. *multihoming*) чланова мреже способних да усмеравају мрежни саобраћај. Вишеструко удомљени чланови поседују онолико мрежних интерфејса са колико су мрежа повезани. Ови интерфејси могу бити међусобно различити, у

зависности од примењене технологије у мрежи са којом су повезани.

Две географски суседне рачунарске мреже је лако повезати кроз вишеструко удомљавање њиховог заједничког члана. Међутим, у ситуацијама када се две мреже које треба повезати налазе на великој географској удаљености, технологије које омогућавају рад локалних рачунарских мрежа обично нису у стању да то омогуће. Најчешће решење тада представља уметање нове међу-мреже засноване на технологијама које омогућавају повезивање на већим удаљеностима (изнајмљене линије, фрејм-релеј и сл.) а обично подразумевају тачка-тачка (енгл. *point-to-point*) тип комуникације.



Слика 3. Повезивање мрежа уметањем међу-мреже

Треба имати у виду да се самим вишеструким удомљавањем чланова у различитим мрежама не добија могућност међусобне комуникације њихових чланова, већ да је за то потребно укључити наменску функционалност. Основна функционалност мрежних пролаза за омогућавање комуникације између чланова различитих мрежа јесте **рутирање**, односно усмеравање саобраћаја. Из тог разлога се уређаји који имају улогу мрежног пролаза који усмерава саобраћај називају рутерима. У неким ситуацијама је једноставно усмеравање саобраћаја недовољно па се уместо њега користи **превођење мрежних адреса** (енгл. *Network Address Translation, NAT*) заглављима пакета који путују кроз мрежни пролаз.

Коначно, целокупна Интернет мрежа се може посматрати као универзална, глобална међу-мрежа (енгл. *inter-network, inter-net*), односно мрежа која повезује приватне рачунарске мреже широм света.

3.1. Мреже на ширем подручју

Регионалне мреже или мреже на ширем подручју (енгл. *Wide Area Network, WAN*), како им и сам назив каже, простиру се на ширем простору - међуградском, државном, међудржавном. У неким случајевима ове мреже се

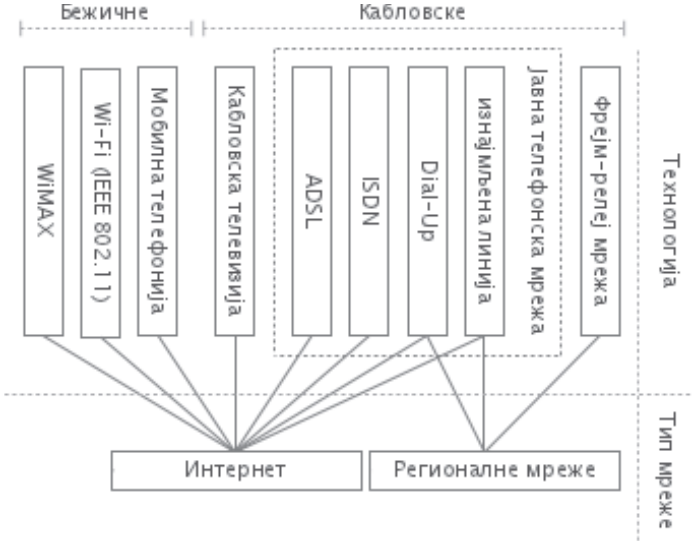
налазе у власништву само једне компаније или државе, док је у неким случајевима њихова инфраструктура сачињена од сегмената који припадају различитим власницима.

Мреже на ширем подручју могу бити рачунарске мреже, мада су чешће у питању традиционалне телекомуникационе мреже са вишеструким наменама (на пример, јавна телефонска мрежа), између осталог и за рачунарске телекомуникације. Такође, ове мреже се могу користити и за потребе Интернет мреже, најчешће за повезивање крајњих корисника са Интернет провајдерима.

Развојем Интернета, као универзалне и глобалне телекомуникационе инфраструктуре, мреже на ширем подручју све више губе своју основну намену и значај. Такође, еволуцијом традиционалних телекомуникационих сервиса (фиксна и мобилна телефонија, телевизија и слично), односно њиховом трансформацијом у сервисе Интернет мреже, у будућности се може очекивати потпуни прелазак на Интернет инфраструктуру.

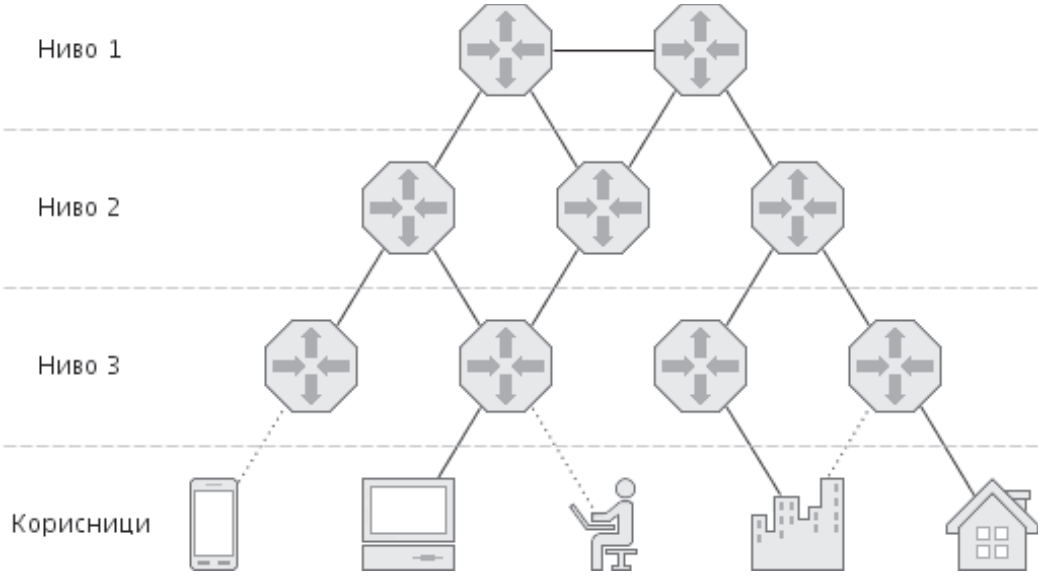
3.1.1. Технологије за приступ Интернету

Интернет мрежа има своју, наменску инфраструктуру - комуникационе водове и чворишта. Комуникациони канали Интернета имају велику пропусну моћ, а често повезују и веома удаљена чворишта, чак и она на различитим континентима. Међутим, за повезивање крајњих корисника са Интернетом често се користи постојећа, ненаменска телекомуникациона инфраструктура.



Слика 1. Популарне технологије за приступ Интернету и WAN повезивање

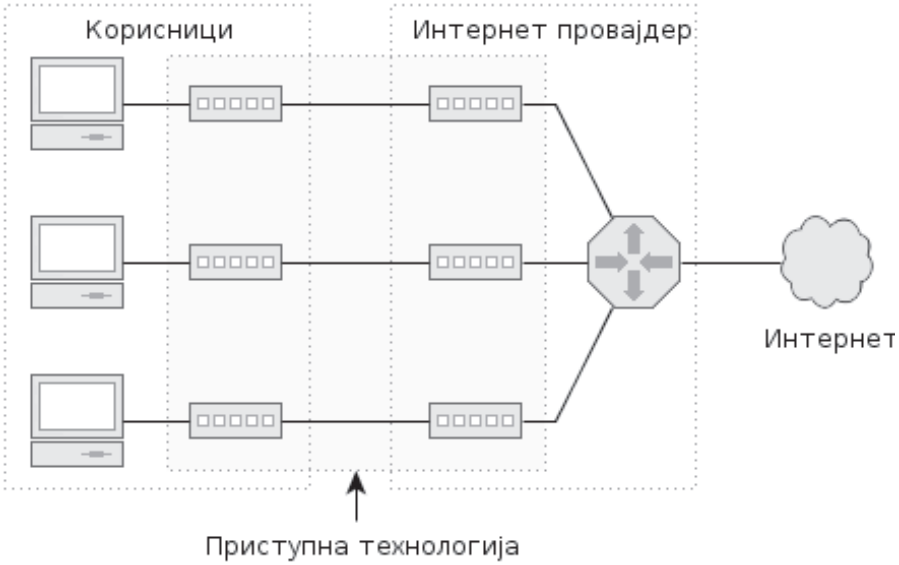
Основу рада Интернет мреже, као и њене приступне тачке, чине Интернет провајдери. Интернет провајдери су организације које успостављају и одржавају примарне телекомуникационе канале Интернет мреже, а уједно, у зависности од нивоа свог функционисања, омогућавају и повезивање крајњих корисника и њихових мрежа на Интернет мрежу.



Слика 2. Интернет провајдери и приступ корисника Интернету

Рачунарске мреже, првенствено оне на већим географским просторима, често се успостављају и путем коришћења већ постојећих телекомуникационих инфраструктура, односно инфраструктура које нису развијане са идејом да се користе за рачунарске телекомуникације. Ове инфраструктуре се данас најчешће користе за повезивање крајњих корисника и мрежа са Интернет провајдерима. На пример, за остваривање везе са Интернет провајдерима данас се често користи инфраструктура јавне телефонске мреже (кроз модемско повезивање, *ISDN* и *ADSL* сервисе) или кабловске телевизије.

Још једно важно питање приликом повезивања на Интернет мрежу путем Интернет провајдера је и питање границе између Интернет провајдера и клијента, односно тачке у којој престаје надлежност провајдера а почиње надлежност клијента. Та тачка се назива тачком разграничења (енгл. *demarcation point*) и у Европи је углавном чини телекомуникациони уређај на страни клијента.



Слика 3. Шема приступа Интернету путем Интернет провајдера

На пример, последња тачка за коју је одговоран провајдер приступа Интернету путем *ADSL* технологије, углавном је сам *ADSL* адаптер који се физички налази у просторијама корисника али се налази у власништву провајдера. Питање тачке разграничења је поред функционалних значајно и због безбедносних разлога.

3.1.2. Јавна телефонска мрежа

Јавна телефонска мрежа једна је од још увек најмасовније коришћених инфраструктура за комуникацију. Ова инфраструктура је реализована углавном жичним комуникационим каналима, увезаним преко локалних, регионалних, националних и интернационалних централа. Такође, пословни системи могу имати интерну телефонску мрежу која је повезана са јавном телефонском мрежом. Основни уређај за коришћење јавне телефонске мреже јесте телефон, уређај за основну двосмерну аудио-комуникацију, али се она може користити и код (разних) других уређаја - факс уређај, модем, и сл.

Јавна телефонска мрежа је, поред своје основне намене, у великом проценту служила и за повезивање корисника са Интернет мрежом, односно, за њихово повезивање са Интернет провајдерима путем модема. Ова мрежа се, због своје распрострањености, и данас користи за приступ корисника Интернету, првенствено путем *xDSL* технологија.

За стандардизацију јавне телефонске мреже задужена је организација под

називом Међународна Телекомуникациона Унија (енгл. *International Telecommunication Union, ITU*). Ова организација има седиште у Женеви и представља агенцију Уједињених нација а чини је 191 земља чланица. Циљ организације је развој и имплементација јавне телефонске мреже и пратећих технологија. Последња препорука *E.164* ове организације, објављена 1997. године под називом „Јавни међународни план за нумерисање телекомуникација“, дефинисала је следећа правила за одређивање телефонских бројева:

1. телефонски број може имати највише 15 цифара;
2. прве цифре (једна до три) телефонског броја одређују земљу којој он припада;
3. средишње цифре телефонског броја чине национални одредишни код (енгл. *national destination code, NDC*);
4. остале цифре телефонског броја представљају број претплатника (енгл. *subscriber number, SN*);
5. национални одредишни код и број претплатника представљају део телефонског броја са националним значајем.

Интеграција сопственог система заштите комуникације у јавну телефонску мрежу првенствено се може извести на нивоу комуникационих уређаја, првенствено телефонских апарата. Међутим, тренд преласка са класичне на Интернет телефонију указује на то да је оптималнији избор вршити интеграцију сопственог система заштите кроз технологије које се у њој користе. Када је у питању модемско коришћење јавне телефонске мреже, оно подлеже истим правилима и структури комуникације као и када су у питању рачунарске комуникације путем Интернет мреже. Из наведених разлога сматрамо оптималнијим решењем фокусирање интеграције система заштите кроз Интернет технологије.

Телефонија се често назива и јавна телефонска комутирана мрежа (*Public Switched Telephone Network, PSTN*). Ова мрежа је пројектована давно са основним циљем да се успешно пренесе говорни сигнал. Карактеристика комутационе мреже је да се у фази успоставе везе бира један од могућих путева преноса, а за време одржавања везе информација се преноси успостављеним физичким путем. Сасвим је могуће да се за две узастопне успоставе везе са истих локација изабере потпуно различит физички пут преноса информације. Често се каже да су ово примери чврсте директне везе. Телефонија је од изузетног интереса за *WAN* мреже зато што је широко распрострањена. Што се

тиче преноса података, систем телефоније нуди више начина преноса. То су комутиране везе, закупљене линије и разне технологије са пакетском комутацијом.

Да би се овом мрежом могли преносити подаци потребно је да се на оба краја везе поставе модеми, уређаје који врше модулацију и демодулацију дигиталног сигнала из рачунара. Сигнали у рачунару су дигитални, а телефонске линије су аналогне тако да модем на излазу врши конверзију дигиталног сигнала у аналогни, а на улазу у рачунар преводи аналогни сигнал у дигитални. Пошто је телефонска мрежа пројектована за пренос говора, њен пропусни опсег је мали - до 3,4kHz – из чега следи да су брзине преноса података килобитског, а не мегабитског реда величине. Аналогни пренос података и примена модемске технологије достиже максималну брзину од 56Kb/s применом савремених модулационих техника (*TCM - Trellis Coded Modulatiori*), као и техника компресије. Што је проток већи, већи је и утицај шума. Осим тога, шум се јавља и при Д/А и А/Д конверзији. Такође, брзине преноса чак и при условима блиским идеалним не постижу максималне номиноване вредности. На пример, модем од 56Kb/s при најбољим условима може постићи брзину између 45 и 50Kb/s (и то ако је централа дигитална). Имајући у виду ове предности и недостатке, *dial-up* аналогна веза налази примену у повезивању кућног рачунара са Интернетом, кућног рачунара са *LAN* мрежом на послу, као и *backup* веза у *WAN* мрежи када сервис преко којег је *WAN* мрежа примарно реализована откаже.

Ова технологија омогућава пренос дигиталних података преко постојећих телефонских линија и због тога је врло брзо постала прихватљиво решење за кућне кориснике и мала предузећа која су желела релативно брзу везу са Интернетом, а нису имали довољно средстава за неку другу технологију. Да би се извршило повезивање на одређену мрежу, корисник је одговоран за део опреме и инсталације које се налазе у његовим просторијама, док је за инсталације ван корисникових просторија одговорна телефонска компанија.

Рачунарски модеми могу бити интерни и екстерни. Интерни модем се поставља у слот на матичној плочи рачунара. На полеђини постоји утичница *RJ-11* (четворожични телефонски прикључак) помоћу које се модем, односно рачунар, прикључује на стандардну телефонску утичницу на зиду.

Екстерни модем је засебан уређај са засебним напајањем. Са рачунаром је повезан серијским каблом (*RS-232*) или путем *USB* магистрале. Екстерни модеми имају утичницу *RJ-11* за повезивање на линију и сигналне диоде које означавају разне режиме рада и стања модема. Екстерни модеми имају једну предност над

интерним - могу се ресетовати независно од рачунара, могу се искључити и поново укључити, а да се при томе не мора искључивати или ресетовати рачунар.

3.1.3. *ISDN* (*Integrated Services Digital Network*)

ISDN (*Integrated Services Digital Network*) је, према *ITU-T*, сет комуникационих стандарда за дигитални пренос говора, видеа и података преко јавне телефонске комутиране мреже (*PSTN*). Представља дигитални еквивалент аналогне телефонске мреже, а у односу на њу обезбеђује бољи квалитет и већу брзину преноса. Почетком 70-их година XX века први пут се јавила идеја о интегрисаним сервисима тј. идеја да се преко једне јединствене мреже корисницима понуде различити сервиси. Први пакет препорука за реализацију и примену *ISDN*-а донет је 1984. године. *ISDN* се може посматрати и као сет протокола за успостављање и раскидање дигиталне везе. Пример је мреже са комутацијом веза (*circuit switched connections*).

Термин „мрежа интегрисаних сервиса која обезбеђује дигиталну везу“ односи се на три битне ствари:

1. Интегрисани сервиси. *ISDN* омогућава најмање две истовремене везе (било која комбинација преноса података, говора, видеа или факса) преко само једне физичке линије. На *ISDN* се могу повезати различити уређаји, како би се задовољиле различите човекове потребе за комуникацијом. Није потребно обезбеђивати вишетруке аналогне телефонске линије, а омогућена је далеко већа брзина преноса.

2. Дигитална веза. Мисли се на дигитални пренос насупрот аналогном преносу код стандардних телефонских линија. Ако се на Интернет повезује стандардном аналогном телефонском линијом, модем код Интернет провајдера врши Д/А конверзију посећеног сајта пре слања података. Локални модем врши А/Д конверзију. Овакве конверзије се дешавају за потребе сваког преноса података. Ако се повезивање врши преко ISDN-а не постоје Д/А и А/Д конверзије. Подаци се преносе дигитално а добро су познате предности дигиталног преноса.

3. Мрежа. *ISDN* није једноставна дигитална веза од тачке до тачке, као што је нпр. изнајмљена линија. *ISDN* мрежа се протеже од локалне телефонске централе све до удаљеног корисника укључујући све телекомуникационе уређаје и централе на преносном путу.

ISDN представља надградњу, односно виши степен постојеће јавне комутиране

телефонске мреже. Већи део комутационих система (телефонских централа) и преносних система између централа дигитализован је, како у свету тако и код нас. Међутим, претплатнички део мреже је остао аналоган. Увођењем *ISDN*-а и претплатнички део мреже постаје дигиталан, и то коришћењем постојећих бакарних парица. Ово је свакако најбитнија чињеница - дигитална веза од краја до краја преко постојеће телефонске мреже без додатних улагања у инфраструктуру.

Слика 1. ISDN обезбеђује дигитални пренос података целом путањом

Постоје два типа *ISDN* приступа: базни (*BRI – Basic Rate Interface*) и примарни (*PRI – Primary Rate Interface*). Базни приступ подразумева два Б канала (канали по којима се преноси информација) од по 64Kb/s и један Д канал (канал по коме се преносе информације неопходне за синхронизацију и корисничку сигнализацију) од 16Kb/s, што је укупно 144Kb/s. Често се означава са 2Б+Д. Намењен је кућним корисницима. Примарни приступ *PRI* (30Б+Д) садржи тридесет Б канала протока 64Kb/s за говор и пренос података и један Д канал протока 64Kb/s за синхронизацију, сигнализацију и пренос података (укупно 2Mb/s), и углавном је намењен за пословне кориснике. По истој бакарној парици по којој је реализован аналогни телефонски прикључак реализује се и базни прикључак *BRI* (2Б+Д), док је за примарни прикључак *PRI* (30Б+Д) потребно две бакарне парице. Једна од главних примена *ISDN*-а је приступ Интернету, где *ISDN* омогућава 128Mb/s пренос података за *upsteram* и *downstream* смер.

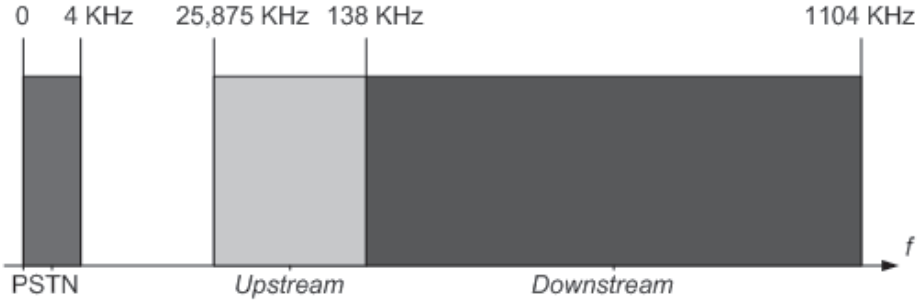
На *ISDN* линију се могу прикључити различити терминални уређаји:

1. *ISDN* телефон
2. Терминални адаптер (TA) за прикључење постојећих аналогних уређаја
3. *ISDN* картице (за пренос података потребна је *ISDN* картица у рачунару или екстерни *ISDN* адаптер)
4. *ISDN LAN router* или *bridge*
5. *ISDN* мултиплексери
6. *ISDN PABX* – претплатничке (кућне) централе *ISDN* типа.

3.1.4. Дигитална претплатничка линија

Дигитална претплатничка линија (*Digital Subscriber Line DSL*) представља начин преноса дигиталних података по бакарним парицама већим брзинама (у распону од 144Kb/s па све до 50Mb/s). *DSL* омогућава пружаоцима услуга (*service providers*), као што су нпр. локалне телефонске компаније, да обезбеде брзу Интернет везу корисницима. Често се каже да је ово технологија која се користи за потребе "задње миље" (растојање од телефонске централе до куће). То је широкопојасна технологија где се поступцима мултиплексирања и модулације омогућава дигитални пренос података високим брзинама по постојећим бакарним парицама, које су у својој основи намењене класичној телефонији. У класичној телефонији преноси се говорни сигнал који у фреквенцијском спектру доминантно заузима опсег фреквенција од 300 до 4.000Hz. Сама бакарна парица својим физичким карактеристикама омогућава боље искоришћење фреквенција, тј. омогућава пренос података далеко већим брзинама.

Постоји више *DSL* технологија које раде на сличном принципу и заједнички се називају *xDSL*. Иницијално *DSL* је настао кроз коришћење већ усвојене предности начина преноса из *ISDN*-а. *DSL* подржава и симетричне и асиметричне сервисе, што зависи од пропусности података у једном и другом смеру. Асиметрични сервиси имају већу пропусност у једном смеру преноса у односу на други. Конкретније, већа брзина преноса је по *downstream* каналу (од централе ка кориснику), а мања по *upstream* каналу (од претплатника ка централи). Асиметрични сервиси су погодни за Интернет из разлога што се фајлови већег обима *download*-ују, а фајлови мањег обима, какви су *e-mail*-ови, *upload*-ују.



Слика 1. Принцип ADSL-а – подела фреквенцијског опсега

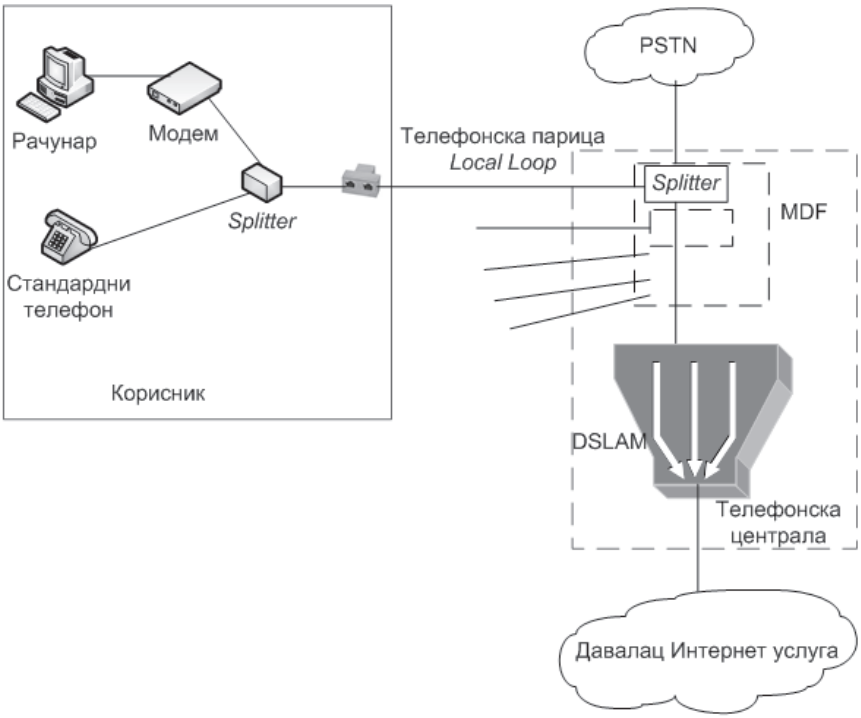
Постоје различите варијанте *DSL*-а: Асиметрични (*ADSL*), *High-bit rate* (*HDSL*), *Single Line* (*SDSL*), *Very-High-Data-Rate* (*VDSL)* и сл. Свака од њих захтева

идентичне уређаје (технологије) на страни корисника и на страни провајдера и карактерише је максимална физичка удаљеност између корисника и провајдера, као и одговарајуће брзине преноса података у оба смера.

У технологији *DSL*-а постоји неколико подврста. Међутим, она која се данас најчешће користи је такозвана асиметрична дигитална претплатничка линија (*ADSL-Asymetric Digital Subscriber Line*). Као што јој и само име каже, основна карактеристика ове врсте *DSL* реализације је асиметричност. Управо она је и чини најзанимљивијом *DSL* реализацијом за приватне и пословне кориснике. Већина најзанимљивијих апликација за кориснике на мрежи су асиметичне (видео на захтев, приступ удаљеним локалним мрежама, приступ Интернету, мултимедијални приступ, *home shopping*, итд.), где значајно више информација корисник узима са мреже него што их у њу шаље. Та асиметричност чини *ADSL* идеалним за ове апликације. *ADSL* дели укупан расположиви фреквенцијски опсег на три дела поступцима фреквенцијске модулације. У најнижем делу спектра се задржава опсег фреквенција за пренос говорног сигнала и тиме се ништа не ремети у односу на стандардан рад телефоније (*PSTN Public Switch Telephone Network*).

ADSL услуга је базирана на сталном и брзом приступу Интернету по већ постојећој телефонској линији (парици) без њеног заузећа или промене телефонског броја. Може се реализовати преко обичне телефонске линије или базног *ISDN* прикључка. Приликом пуштања *ADSL* сервиса на постојећу обичну или *ISDN* линију на располагању су истовремено обе везе тј. обична или *ISDN* и *ADSL* веза. Захтевани технички услови су да постоји слободна парица и да има слободних ресурса на уређају у реонској телефонској централи. Проток се дефинише посебно за долазни а посебно за одлазни саобраћај с тим да се већи проток одређује за долазни саобраћај.

Код *ADSL*-а претплатничка опрема се повезује на телефонску компанију преко стандардног прикључка. Основна компонента уређаја код корисника је *splitter*, кога чине два филтра који фреквенцијски раздвајају говорни сигнал од модемског сигнала *ADSL*-а. Један излаз из сплитера се повезује на телефон тако да се овом везом задржава сервис говорне комуникације (стандардни телефон), а други се повезује на *ADSL* модем и задужен је да обезбеди подршку *ADSL* услугама. На телефонској парици (*Local Loop*) преносе се мултиплексирани говорни и модемски сигнали. Пошто су фреквенцијски одвојени нема међусобних сметњи, тако да се *ADSL*-ом могу истовремено преносити и говор и подаци.



Слика 2. Блок шема повезивања ADSL-а

Сплитери постоје и на страни корисника и на страни телефонске централе. На страни телефонске централе постоји банка сплитера. Један сплитер има два излаза. Први излаз се води према јавној телефонској мрежи (*PSTN*), а други се повезује на *DSL* модем. Из разлога ефикасности, а због подршке за више корисника, на страни телефонске централе постоји јединствен уређај *DSL access multiplexers* (*DSLAM*) који се повезује на даваоца Интернет услуга.

3.1.5. Изнајмљена линија

Изнајмљене линије су телекомуникационе (аналогне или дигиталне) везе које међусобно спајају две удаљене локације. Често се назива и стална веза. Насупрот традиционалним телефонским везама, непотребан је телефонски број учесника, зато што је свака страна у комуникацији у сталној вези са другом страном. Користе се за телефонију, пренос података и Интернет сервисе. Преко изнајмљених линија остварују се брзине од 56Kb/s, 64Kb/s, 128Kb/s, 256Kb/s, 512Kb/s или 2Mb/s. Плаћају се паушално - на одређени временски период, без обзира на степен коришћења. Одговара организацијама које имају потребу за преносом велике количине података. Највећи недостатак овакве везе је

изузетно висока цена која расте са захтевом за већом брзином преноса података. То су везе типа тачка-тачка где се не може мењати дестинација као код *dial-up* везе. Најчешће служе за повезивање удаљених географских локација, и то на два начина:

1. изнајмљена линија се простире целом дужином између две локације и
2. изнајмљена линија иде до локалног телеком оператера, а веза од њега је реализована неком другом технологијом, као што је на пример *frame relay*. Крајњем кориснику се гарантује квалитет услуге.

3.1.6. WiMAX

WiMAX (*Worldwide Interoperability for Microwave Access*) је бежична технологија за високе брзина преноса података према стандарду *IEEE* 802.16. Користи се техника рада у проширеном спектру. Омогућава фиксним и мобилним корисницима приступ Интернету. Може се посматрати као алтернатива *DSL* кабловским технологијама. Стандардом је обезбеђена интероперабилност између опреме различитих произвођача. Иако може да служи као подршка за *WiFi* 802.11, корисници путем наменских уређаја могу директно да приступају *WiMAX*-у. Омогућава брзи бежични приступ на раздаљинама од 50Km за фиксне станице и 5-15Km за покретне станице, за разлику од *WiFi* 802.11 чији је домет ограничен на 30-100 метара. Текући стандард омогућава брзине преноса података до 40Mb/s, а очекује се да ће развојем стандарда *IEEE* 802.16м бити омогућена брзина преноса података од 1Gb/s.

Овом технологијом могуће је поставити мрежу на подручјима којима недостаје традиционални приступ Интернету путем каблова. Поред тога може се користити када је потребно поставити мрежу у ванредним околностима. Користи се често као подршка кабловским мрежама када дође до хаварије или једноставно као појачање постојећој жичаној инфраструктури. *WiMAX* омогућава квалитет сервиса који пружају *VoIP*, *streaming*, пренос података итд.

Постоје два типа *WiMAX*-а: фиксни (802.16д) и мобилни (802.16е). Фиксни је *point-to-multipoint* технологија док је мобилни *multipoint-to-multipoint* технологија, слично инфраструктури за мобилну телефонију.

3.2. Интернет протокол

И након сто година, ова прича је још увек застрашујућа.
Не због убице у локалној мрежи, већ зато што се користи IPv4.
Рендал Монро, www.xkcd.com

Тренутно, највећи број чланова Интернет мреже, као и већина локалних рачунарских мрежа, адресован је Интернет протоколом четврте верзије (енгл. *Internet Protocol version 4, IPv4, IP*). Управо једна од најзначајнијих карактеристика овог протокола је та да се њиме могу адресовати мреже величине од два члана до више милијарди чланова – Интернет. Овај протокол је и основа одређених софтверских система који се извршавају у оквиру једног рачунара (на пример, *X Window System* графички интерфејс на *UNIX* оперативном систему).

Две основне функције Интернет протокола јесу адресовање рачунарских мрежа и њихових чланова и фрагментовање података. Процес адресовања, као примарна функција Интернет протокола, започиње већ при системском позиву модула оперативног система у коме је имплементиран Интернет протокол. У оквиру тог позива, модулу Интернет протокола прослеђује се одредишна адреса, односно коме треба доставити податке. На основу одредишне адресе модул Интернет протокола израчунава да ли је у питању адреса у локалној или удаљеној мрежи, као и мрежни интерфејс путем кога ће слање бити извршено. У зависности од одредишне адресе Интернет протокол одређује и да ли ће се слање извршити директно или путем одговарајућег мрежног пролаза.

Подаци се смештају у пакете који се у називају датаграмима. У заглавља пакета уписују се изворишна и одредишна адреса, односно адреса мрежног интерфејса путем кога је извршено слање и адреса мрежног интерфејса на коме одредиште треба да прихвати податке. На пријемној страни улога Интернет протокола је да анализира податке заглавља примљених пакета и донесе одлуку о томе да ли примљене пакете треба проследити следећем мрежном чвору, локалном протоколу вишег нивоа, или их треба одбацити.

Фрагментовање података следећа је битна функција Интернет протокола јер омогућава да се пакети Интернет протокола преносе посредством мрежа које имају различита ограничења у погледу највеће могуће дужине јединице података. У току овог процеса датаграми се деле на фрагменте који поседују исту структуру као и оригинални датаграми али су мање величине. На пријемној страни Интернет протокол од добијених фрагмената поново формира оригинални датаграм и наставља са његовим прослеђивањем ка коначном одредишту.

Значајна карактеристика Интернет протокола је та да он функционише без успостављања везе. То значи да се сваки од пакета које треба пренети прослеђује засебно, односно независно од осталих пакета и ван контекста у виду успостављене везе. Такође, Интернет протокол не поседује механизме као што су поновно слање изгубљених пакета и контрола тока података, а који обезбеђују поуздан пренос између крајњих или посредних тачака комуникације. У случајевима када има потребе да се извор обавести о немогућности испоруке пакета, то се врши путем Интернет протокола за контролне поруке (енгл. *Internet Control Message Protocol, ICMP*) као проширења самог Интернет протокола.

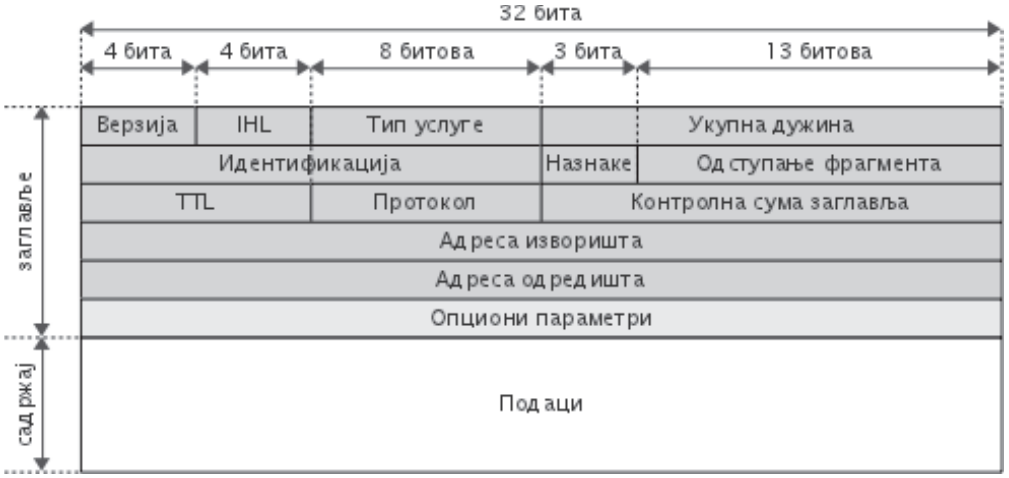
За разумевање и рад са Интернет протоколом четврте верзије, неопходно је познавање бинарног бројног система јер он представља основу свих израчунавања везаних за овај протокол. Знања везана за четврту верзију Интернет протокола од великог су значаја и за разумевање и рад са шестом верзијом овог протокола, посебно што ове две верзије у пракси често коегзистирају. Додатно, функционалности и карактеристике шесте верзије Интернет протокола често се представљају у виду разлика у односу на функционалности и карактеристике четврте верзије.

Последњих пет блокова слободних адреса Интернет протокола четврте верзије расподељено је регионалним регистрима Интернета трећег фебруара 2011. године. Иако је исцрпљивање слободних адреса овог протокола у прошлости више пута наговештавано а превентиван прелазак на шесту верзију Интернет

протокола био могућ више година уназад, након наведеног датума се очекује интензивнија миграција на коришћење нове верзије.

3.2.1. Структура пакета Интернет протокола

Пакети Интернет протокола – датаграми – састоје се од два основна дела: заглавља пакета и података који се њиме преносе. Битска дужина пакета није фиксна а у њу улазе битови заглавља и битови података.



Слика 1. Структура датаграма Интернет протокола

Заглавље пакета омогућава функционисање Интернет протокола. Његова минимална битска дужина је 160 битова у које улази 96 битова основних параметра (тип сервиса, преостало време постојања, опције, контролна сума заглавља, итд) и 64 бита изворишне и одредишне адресе. Додатно, заглавље може садржати и допунске параметре (опције) који повећавају битску дужину заглавља у јединицама од 32 бита. Основна поља заглавља чине:

- **Верзија** (енгл. *Version*) – вредност овог поља означава верзију Интернет протокола на који се пакет односи. За пакете Интернет протокола четврте генерације децимална вредност овог поља је 4.
- **Дужина Интернет заглавља** (енгл. *Internet Header Length, IHL*) – битска дужина заглавља у јединицама од по тридесет два бита. Користи се за утврђивање битске позиције на којој се заглавље завршава, односно на којој почињу подаци. Најмања исправна вредност је пет, а највећа могућа шеснаест.
- **Тип услуге** (енгл. *Type of Service, ToS*) – садржи параметре на основу

којих се одређује жељени квалитет услуге, односно, приоритет под којим ће се пакет обрађивати и представља однос између минималног кашњења, високе поузданости и високе пропусне моћи. Прва три бита овог параметра одређују редослед приоритета (који се у посредним мрежама може разликовати од жељене конфигурације), четврти бит се односи на кашњење, пети на потребну пропусну моћ, шести на поузданост, а последња два бита су резервисана за будућу употребу. С обзиром на то да се у већини мрежа једна карактеристика остварује на рачун осталих, препоручено је укључивање највише две опције.

- **Укупна дужина** (енгл. *Total Length*) – садржи податак о укупној дужини пакета (укључујући и заглавље и податке), израженој у октетима (бајтовима). Највећа могућа дужина пакета Интернет протокола је 65.536 бајтова, мада се у пракси пакети дужине веће од 576 бајтова (64 бајтова за заглавље и 512 бајтова за податке) користе само уколико се са сигурношћу зна да је одредиште способно да прихвати такве пакете.

- **Идентификација** (енгл. *Identification*), назнаке (енгл. *Flags*), и одступање фрагмента (енгл. *Fragment Offset*) – ова три параметра, укупне дужине 32 бита, користе се за потребе фрагментовања датаграма. Први параметар, идентификација, има за задатак да одреди текући датаграм, односно, датаграм коме фрагмент припада. За назнаке су резервисана три бита од којих је први резервисан за будућу употребу, други означава да ли се забрањује фрагментовање датаграма, док трећи бит означава да ли је он последњи у низу фрагмената одређеног датаграма, односно, да ли након њега следи још фрагмената. Због могућности да редослед пријема датаграма буде различит од редоследа слања, заједно са фрагментом се прослеђује и његово одступање од почетка (у јединицама од по 64 бита), односно, позиција на којој он чини садржај фрагментованог датаграма.

- **Преостало време постојања** (енгл. *Time to Live*) – ова опција ограничава време које пакет може да проведе у путовању кроз мреже. Иако је основна замисао да се овај параметар односи баш на време, он у пракси означава број скокова, односно број посредних уређаја (који раде на мрежном нивоу, нпр. рутера) кроз које пакет може да прође. Сваки посредни уређај пре прослеђивања смањује вредност овог поља пакета за један. У случају да се вредност поља смањи на нулу, уређај на коме се то догоди неће даље прослеђивати пакет већ ће га одбацити. Пошиљаоцу се у том случају може послати *ICMP* пакет са назнаком да је путовање пакета прекорачило дозвољени број скокова. Ограничавање

броја скокова пакета веома је значајно јер постоје ситуације у којима би пакет могао бесконачно да оптерећује одређене комуникационе канале и уређаје, а да никада не стигне на одредиште. У шестој верзији Интернет протокола назив овог поља промењен је у ограничење броја скокова (енгл. *Hop Limit*).

- **Протокол** (енгл. *Protocol*) – садржај овог поља одређује који је протокол транспортног слоја иницирао слање података, односно ком протоколу транспортног слоја ће подаци на одредишту бити испоручени. На пример, уколико је децимална вредност овог поља 1, подаци ће бити испоручени ICMP протоколу, вредност 6 указује на *TCP* протокол, итд. Везе између вредности овог поља и протокола транспортног слоја одређене су у RFC 790 документу.

- **Контролна сума заглавља** (енгл. *Header Checksum*) – ово поље омогућава да се на пријемној страни одреди да ли је током преноса дошло до оштећења заглавља, односно до измене битова који њему припадају. Ова провера се врши не само на коначном одредишту већ на сваком уређају који посредује у преносу пакета. Уколико се утврди да је дошло до оштећења заглавља, престаје прослеђивање пакета и он се одбацује. С обзиром на то да је ово поље такође саставни део заглавља, за вредности његових битова се код израчунавања контролне суме узимају нуле.

- **Адреса извора** (енгл. *Source Address*) – у ово поље се уписује адреса мрежног интерфејса изворишта са кога је пакет послат. У случају да на неком од посредника у комуникацији дође до превођења мрежне адресе извора, вредност овог поља се мења, као и контролна сума заглавља.

- **Адреса одредишта** (енгл. *Destination Address*) – у ово поље се уписује мрежна адреса одредишта са кога је пакет послат. У случају да на неком од посредника у комуникацији дође до превођења мрежне адресе одредишта вредност овог поља се мења, као и контролна сума заглавља.

Осим наведених основних параметара заглавља у њему се могу појавити и додатни, опциони параметри. Атрибут »опциони« односи се на то да ли ће параметри бити постављени или не. Уколико су додатни параметри постављени, они морају, осим од стране пошиљаоца, бити подржани и од стране примаоца, као и од стране свих посредника у комуникацији.

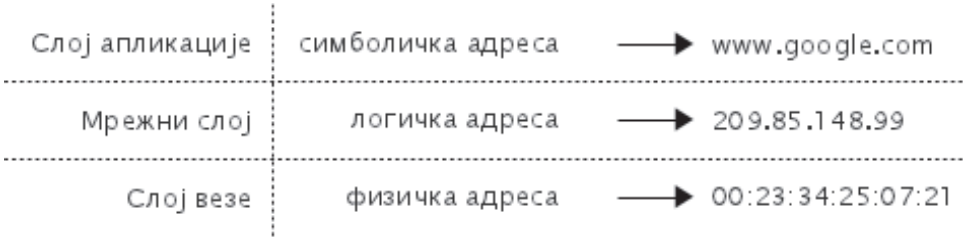
```
▸ Frame 75: 212 bytes on wire (1696 bits), 212 bytes captured (1696 bits)
▸ Ethernet II, Src: Cisco-Li_b4:a8:32 (00:1d:7e:b4:a8:32), Dst: AsustekC_35:07:22 (00:23:54:35:07:22)
▾ Internet Protocol, Src: 209.85.148.104 (209.85.148.104), Dst: 192.168.60.238 (192.168.60.238)
    Version: 4
    Header length: 20 bytes
  ▸ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 198
    Identification: 0xc9a4 (51620)
  ▸ Flags: 0x00
    Fragment offset: 0
    Time to live: 55
    Protocol: TCP (6)
  ▸ Header checksum: 0x5639 [correct]
    Source: 209.85.148.104 (209.85.148.104)
    Destination: 192.168.60.238 (192.168.60.238)
```

Слика 2. Пакет Интернет протокола, забележен Wireshark алатом

Опциони параметри се најчешће односе на захтеване руте којима пакет треба да стигне до одредишта, безбедност током преноса и слично.

3.2.2. Адресовање чланова мреже

Једна од основних функција Интернет протокола јесте адресовање мрежа и њихових чланова. Под овим адресовањем подразумева се **логичко адресовање**, док су физичко и симболичко адресовање (слика 1.) задаци протокола других комуникационих слојева и системских модула.



Слика 1. Адресе по слојевима

Симболичка адреса члана мреже (мрежни назив) углавном се користи на слоју апликације. Ова адреса, иако најчешће хијерархијски структуирана, пре употребе мора се превести у логичку адресу, односно у адресу Интернет протокола. Превођење симболичких адреса у логичке није задатак Интернет протокола већ системске компоненте *resolver* и *Domain Name System* сервиса.

Физичка адреса, са друге стране, локално одређује примаоца података који се преносе мрежом. Локални карактер овог типа адреса ограничава њихову употребу на оквире једне рачунарске мреже. У комуникацији два рачунара из две удаљене мреже, локалне адресе пакета ће се више пута мењати, односно, прилагођавати посредничким рачунарским мрежама. Превођење логичких

адреса у физичке такође није задатак Интернет протокола већ одвојених наменских протокола слоја везе (нпр. *Address Resolution Protocol*-а).

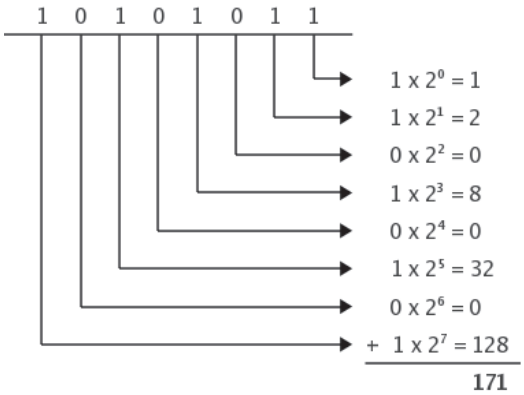
Која је онда улога Интернет протокола и логичких адреса? Интернет протокол, као и остали протоколи мрежног слоја, има задатак да обезбеди систем логичког адресовања на основу кога се могу одредити мрежне руте – путање комуникације било која два члана мрежа који су посредно или непосредно повезани. У том циљу, четврта верзија Интернет протокола користи логичке мрежне адресе, мрежне маске, класе мрежних адреса, приватне, јавне и специјалне опсеге мрежних адреса, превођење мрежних адреса, статички задате руте и протоколе за рутирање.

У складу са битском дужином адреса, Интернет протокол нуди укупно 2^{32} (односно 4.294.967.296) јединствених мрежних адреса. Овај број адреса се ауторима четврте верзије Интернет протокола, у тренутку пројектовања - 1974. године - чинио сасвим довољним за све будуће потребе. Данас, међутим, број расположивих адреса представља главно уско грло овог протокола.

3.2.2.1. Бинарни бројни систем, логичке операције и рачун

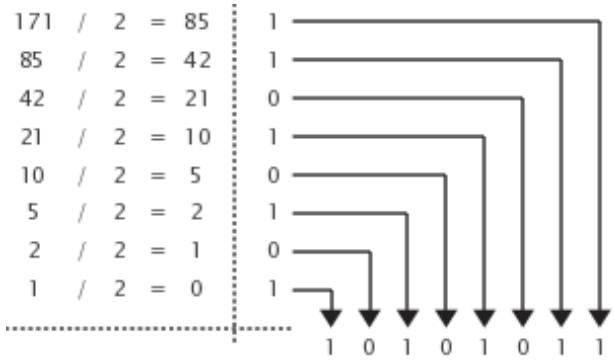
За потребе коришћења бинарног бројног система у рачунарским мрежама потребно је познавање његовог превођења у децимални бројни систем, и познавање логичке операције под називом искључива дијсункција (енгл. *exclusive dijsunction, exclusive OR, XOR*). С обзиром на то да се *IP* адресе најчешће представљају у децималном облику, а да се све мрежне операције врше над њиховим бинарним обликом, познавање превођења ова два бројна система је неопходно. Са друге стране, већина мрежних операција захтева бинарно упоређивање одређених делова *IP* адреса, тако да је познавање искључиве дисјункције такође неопходно.

Превођење података из бинарног бројног система у децимални врши се одговарајућим сумирањем основа (број два) степенованим на позиције. Као бит најмање тежине узима се крајњи десни бит а његова позиција се означава нултом. Позиције осталих битова се, затим, увећавају за један, са десна на лево. Децимална вредност сваког бита јесте број два степенован на позицију бита. Уколико је бит укључен – има вредност један – његова децимална вредност се укључује у коначну суму. У противном, уколико је његова бинарна вредност нула, његова децимална вредност се не укључује у коначну суму. Коначна сума представља децималну вредност бинарног низа.



Слика 1. Превођење бинарног у децимални запис

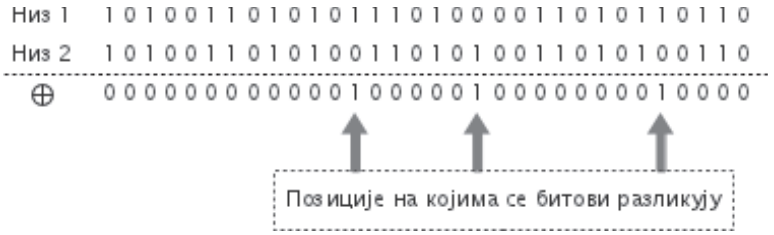
Са друге стране, превођење децималног бројног система у бинарни врши се дељењем децималног броја са два. Дељење целобројног дела резултата итеративно се понавља све док се као целобројни део резултата не добије нула. При свакој итерацији дељења, као резултат може се јавити целобројна вредност или остатак од једне половине. У случају целобројне вредности као међурезултата, бинарна вредност актуелне позиције је нула. У противном, уколико се при дељењу јави остатак, бинарна вредност актуелне позиције је један. Прва добијена битска вредност представља бит најмање тежине (крајњи десни). Накнадно добијени битови додају се у смеру с десна на лево.



Слика 2. Превођење децималног у бинарни запис

Коришћењем искључиве дисјункције може се утврдити да ли су два низа битова идентична, односно на којим позицијама се битови разликују. Ова логичка операција као улаз подразумева два бита. Уколико се вредности улазних битова разилкују – вредност првог бита је јединица а вредност другог нула, или обрунуто – резултат операције је бит са вредношћу један. У противном, уколико

су вредности улазних битова једнаке – обе нуле или обе јединице – резултат је бит са вредношћу нула.



Слика 3. Поређење низова битова искључивом дисјункцијом

Када је у питању поређење низова битова овом логичком операцијом, оно се врши са по једним паром битова – узима се по један бит са исте позиције из првог и другог низа. Подразумева се поређење низова исте битске дужине, која је уједно и дужина резултујућег низа. Уколико су низови који се пореде идентични добијени низ је сачињен искључиво од нула. У противном, уколико на одређеним позицијама постоје разлике, резултујући низ ће на тим позицијама садржати јединице. Смер поређења битова не утиче на резултат, а зависи од конкретне потребе.

3.2.2.2. Мрежна адреса и мрежна маска

Интернет протокол четврте генерације користи адресе фиксне дужине од 32 бита (четири октета). Ове адресе садрже почетни део - део који одређује мрежу којој адреса припада - и остатак - део који одређује конкретног члана те мреже. Адресе могу бити специјалне адресе или адресе намењене адресовању чланова мреже. На основу мрежне адресе чланови мреже израчунавају да ли се одредиште налази у истој мрежи, или не.

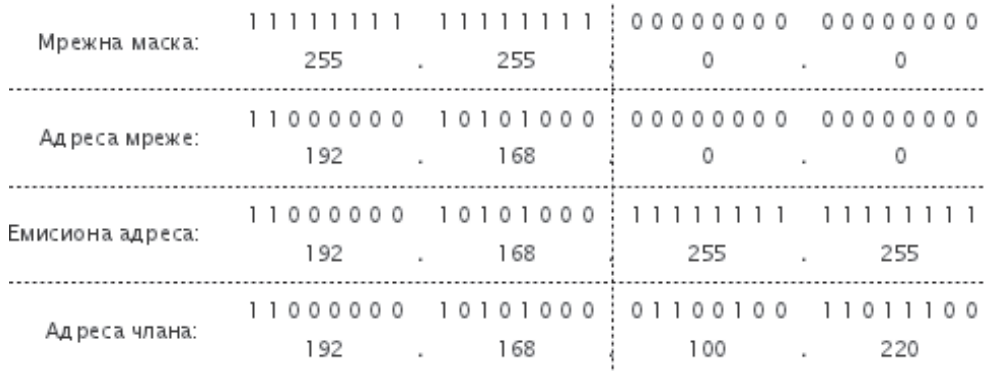
Слика 1. Записи и структура адресе Интернет протокола

За потребе обављања основних мрежних операција, сваки адресовани члан мреже мора имати дефинисану и мрежну маску. Мрежна маска дефинише границе одређене мреже, односно опсег мрежних адреса које припадају тој мрежи. На основу мрежне маске утврђује се који битови мрежне адресе

одређују мрежу, а који конкретног члана те мреже.

Слика 2. Однос мрежне маске и мрежне адресе

Две специјалне адресе у мрежама адресованим Интернет протоколом јесу адреса саме мреже (енгл. *network address*) и емисиона адреса (енгл. *broadcast address*). Адреса мреже представља прву адресу из додељеног опсега мрежних адреса. Код ове адресе сви битови који одређују мрежног члана су нуле. Емисиона адреса је последња адреса у опсегу мрежних адреса. Код ове адресе сви битови који одређују мрежног члана су јединице. Подаци упућени на емисиону адресу прослеђују се свим члановима мреже. Адреса мреже и емисиона адреса не могу се користити за адресовање чланова.



Слика 3. Мрежна маска, адреса мреже и емисиона адреса

На основу мрежне адресе и мрежне маске, сваки члан мреже, пре слања података, израчунава да ли се одредишна мрежна адреса налази у локалној мрежи или не. Ово израчунавање врши се коришћењем искључиве дисјункције над првих *n* битова локалне и одредишне адресе. Број првих битова који ће бити упоређени одређује мрежна маска. Уколико резултат упоређивања покаже да су поменути низови битова идентични, закључује се да је одредишна адреса у локалној мрежи и, у складу са тим, слање се врши директно. У противном, уколико поменути низови нису идентични, закључује се да се одредишна адреса

налази у удаљеној мрежи и подаци се ка њој упућују путем специфичног или подразумеваног мрежног пролаза.

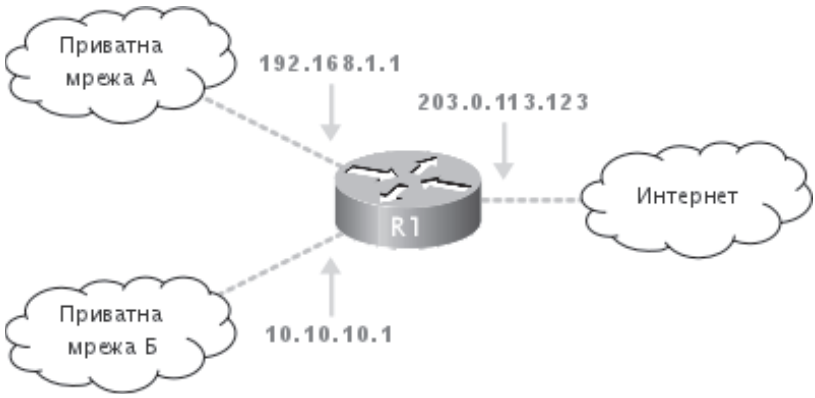
	Део који се пореди			
Мрежна маска:	11111111	11111111	00000000	00000000
Адреса изворишта:	11000000	10101000	11010100	10010110
Адреса одредишта:	11000000	10101000	01100010	11011100
⊕	00000000	00000000		

Слика 4. Примена искључиве дисјункције за проверу одредишне адресе

Подразумевани мрежни пролаз (енгл. *default gateway*) мрежни је уређај или рачунар који је члан две или више рачунарских мрежа, а оспособљен је да врши функцију рутирања или превођења мрежних адреса. Једна рачунарска мрежа може имати више мрежних пролаза а њени чланови могу их користити за различите дестинације, давати им различите приоритете, а један од њих прогласити подразумеваним.

Слика 5. Мрежни пролази омогућавају комуникацију између мрежа

Могућност припадања једног рачунара, или мрежног уређаја, вишеструким рачунарским мрежама назива се вишеструко удомљавање (енгл. *multihoming*). Ова могућност, међутим, отвара ново питање: уколико је рачунар Р члан мрежа А и Б, да ли је његова мрежна адреса А/Р или Б/Р? Одговор на ово питање лежи у чињеници да се не адресује сам мрежни члан већ његов одређени мрежни интерфејс (физички или логички). У складу са тим, рачунар Р из претходног примера, са мрежом А био би повезан путем мрежног интерфејса ИФ1, а са мрежом Б путем мрежног интерфејса ИФ2. Дакле, рачунар Р имао би адресу А/Р на мрежном интерфејсу ИФ1, а адресу Б/Р на мрежном интерфејсу ИФ2.

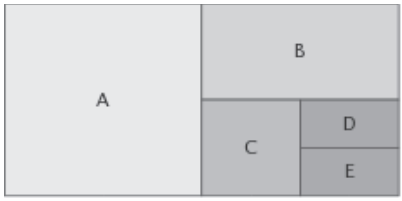


Слика 6. Пример вишеструког удомљавања рутера

Мрежна адреса и мрежна маска параметри су који се односе на појединачни мрежни интерфејс, а подразумевани мрежни пролаз, руте и адресе *DNS* сервера општи су мрежни параметри. Вишеструко удомљени мрежни члан може обављати функцију рутирања или превођења мрежних адреса, али то није подразумевана функционалност.

3.2.2.3. Класе мрежних адреса

У основној спецификацији четврте верзије Интернет протокола адресни простор био је подељен у 254 мреже (2^8 – 2) које су могле садржати по 16.777.214 чланова (2^{24} – 2). Ова подела одређена је правилом да првих осам битова, односно осам најзначајнијих битова, представља адресу мреже, док преостала двадесет четири бита чине адресу члана мреже. Оваква подела је функционисала у раним фазама Интернета када је њега чинио релативно мали број рачунара. Са порастом броја рачунара на Интернету, као и броја локалних рачунарских мрежа, увидело се да оваква подела није оптимална. Нови модел поделе адресног простора на мреже представљен је 1981. године у *RFC* 791 документу у коме су дефинисане мреже различитих величина – **класе мрежа**.



Слика 1. Подела адресног простора у опсеге за различите класе

У самом *RFC* 791 документу дефинисане су три основне класе мрежних адреса – *A*, *B* и *C* – као и две додатне класе – *D* и *E* – за специјалне намене. За потребе

увођења класа мрежних адреса комплетан адресни простор подељен је у више опсега различитих величина, у складу са величином предвиђених мрежа.

Први бит мрежних адреса класе *A* фиксиран је на вредност један. На основу тога, *A* класи мрежних адреса додељена је половина укупног адресног простора Интернет протокола четврте генерације. У рачунарским мрежама класе *A* првих осам битова одређује мрежу а преостала двадесет четири одређују члана те мреже. Постоји укупно 127 рачунарских мрежа класе *A* од којих свака поседује 16.777.216 адреса.

Мрежна маска:	11111111	00000000	00000000	00000000
	255	0	0	0
Прва адреса:	**0**0000000	00000000	00000000	00000000
	0	0	0	0
Последња адреса:	**0**1111111	11111111	11111111	11111111
	127	255	255	255

Слика 2. A класа и опсег мрежних адреса

Прва два бита мрежних адреса класе *B* фиксирана су на вредност „10“. На основу тога, за рачунарске мреже класе *B* резервисана је четвртина укупног адресног простора Интернет протокола четврте генерације. У рачунарским мрежама класе *B* првих шеснаест битова одређује мрежу а преосталих шеснаест одређује члана те мреже. Постоје укупно 16.384 рачунарске мреже класе *B* од којих свака поседује 65.536 адреса.

Мрежна маска:	11111111	11111111	00000000	00000000
	255	255	0	0
Прва адреса:	**10**000000	00000000	00000000	00000000
	128	0	0	0
Последња адреса:	**10**111111	11111111	11111111	11111111
	191	255	255	255

Слика 3. B класа и опсег мрежних адреса

Прва три бита мрежних адреса класе *C* фиксирана су на вредност „110“. На основу тога, за рачунарске мреже класе *C* резервисана је једна осмина укупног адресног простора Интернет протокола четврте генерације. У рачунарским мрежама класе *C* прва двадесет четири бита одређују мрежу а преосталих осам битова одређује члана те мреже. Постоје укупно 2.097.152 рачунарске мрежа класе *C* од којих свака поседује 256 адреса.

Мрежна маска:	11111111	11111111	11111111	00000000
	255	255	255	0
Прва адреса:	**110**00000	00000000	00000000	00000000
	192	0	0	0
Последња адреса:	**110**11111	11111111	11111111	11111111
	223	255	255	255

Слика 4. C класа и опсег мрежних адреса

Прва четири бита мрежних адреса класе *D* фиксирана су на вредност „1110“. На основу тога, за адресе класе *D* резервисана је једна шеснаестина укупног адресног простора Интернет протокола четврте генерације. Рачунарске адресе из овог опсега не служе за адресовања конкретних рачунарских мрежа, већ се користе за подребе адресовања вишеструких примаоца послатих података (енгл *multicast*). *D* класа мрежних адреса дефинисана је у *RFC* 1112 документу.

Прва адреса:	**1110**0000	00000000	00000000	00000000
	224	0	0	0
Последња адреса:	**1110**1111	11111111	11111111	11111111
	239	255	255	255

Слика 5. D класа и опсег мрежних адреса

Прва четири бита мрежних адреса класе *E* фиксирана су на вредност „1111“. На основу тога, за адресе класе *E* резервисана је последња шеснаестина укупног адресног простора Интернет протокола четврте генерације. Рачунарске адресе из овог опсега не служе за адресовања конкретних рачунарских мрежа, већ се користе у експерименталне сврхе.

Прва адреса:	**1111**0000	00000000	00000000	00000000
	240	0	0	0
Последња адреса:	**1111**1111	11111111	11111111	11111111
	255	255	255	255

Слика 6. E класа и опсег мрежних адреса

Увођење класа мрежних адреса још увек није захтевало експлицитно навођење мрежне маске јер се она могла утврдити на основу прва четири бита адресе. Резултат увођења класа мрежних адреса био је прецизније одређивање величине рачунарских мрежа, што је омогућило економичније коришћење адресног опсега четврте верзије Интернет протокола у периоду од 1981. до 1993. године. Међутим, пораст броја рачунара на Интернету довео је до превазилажења могућности које је донело класно одређивање мрежних адреса.

Класе мрежних адреса су 1993. године замењене бескласним одређивањем величине мрежа Интернет протокола четврте верзије. Данас се углавном

користи бескласно одређивање величине мреже, а класа мрежа се подразумева само у теоријским случајевима када је мрежна маска изостављена.

3.2.2.4. Бескласно адресовање и подмрежавање

Нагли пораст броја корисника Интернет прокола четврте генерације, у последње две деценије, указао је на то да класе IP адреса представљају превише грубу поделу адресног простора. Најмања класа адреса – класа C – показала се неоптималном за адресовање (у пракси све чешћих) мрежа од свега неколико чланова, јер се на тај начин непотребно заузимало и до 252 од 256 мрежних адреса. Такође, овом класом нису могле да се адресују ни мреже које су бројале нешто преко 254 члана. У тим случајевима морала се користити класа Б са којом се јављало непотребно заузимање и до 65.279 од 65.536 мрежних адреса. Због оваквог, неоптималног трошења адреса Интернет протокола, 1993. године, у RFC 1519 документу, представљен је модел бескласног међудоменског рутирања, односно бескласног одређивања величине мреже – *Classless Inter-Domain Routing, CIDR*.

Основна маска:	11111111	11111111	11111111	00000000
	255	255	255	0
Основна мрежа:	11000000	10101000	00000001	00000000
	192	168	1	0
Маска подмреже:	11111111	11111111	11111111	**1**0000000
	255	255	255	**128**
1. подмрежа:	11000000	10101000	00000001	**0**0000000
(адреса мреже)	192	168	1	0
1. подмрежа:	11000000	10101000	00000001	**0**1111111
(емисиона адреса)	192	168	1	127
2. подмрежа:	11000000	10101000	00000001	**1**0000000
(адреса мреже)	192	168	1	128
2. подмрежа:	11000000	10101000	00000001	**1**1111111
(емисиона адреса)	192	168	1	255

Слика 1. Подела мреже класе C на две подмреже

Бескласно одређивање величине мреже пружа прецизност одређивања величине мреже на нивоу бита, за разлику од прецизности на нивоу октета што је био случај код класног одређивања величине. За разлику од класног одређивања величине мреже, где су се величина мреже и мрежна маска подразумевале на основу класног опсега у коме се адреса налази, код бескласног одређивања величине мреже мрежну маску је потребно

експлицитно дефинисати. Децималне вредности октета маски подељених мрежних опсега могу имати вредности 0, 128, 192, 224, 240, 248, 252, 254 и 255.

Подмрежавање рачунарских мрежа врши се у оквиру одређеног мрежног опсега, који може, али и не мора бити класно одређен. На пример, као основа за подмрежавање може се узети мрежа класе *C* – 192.168.1.0 – са мрежном маском од 24 бита – 255.255.255.0. Уколико ову мрежу желимо да поделимо на две мање подмреже, за део мрежне адресе који одређује мрежу заузећемо још један бит. У складу са тим, прва половина адреса из мрежног опсега мреже 192.168.1.0-255 припашће првој новодобијеној подмрежи, док ће друга половина опсега припасти другој мрежи. Мрежна маска ове две новодобијене подмреже имаће 25 битова који одређују мрежу и 7 битова који одређују члана. Децимални приказ овакве мрежне маске је 255.255.255.128 али се у пракси често користи и децимални запис броја битова који одређују мрежу. У поменутом случају би се адреса прве подмреже записала као 192.168.1.0/25 а адреса друге подмреже као 192.168.1.128/25. Сваку од новодобијених подмрежа из претходног примера можемо даље делити на мање подмреже.

3.2.2.4.1. Пример подмрежавања мреже *C* класе

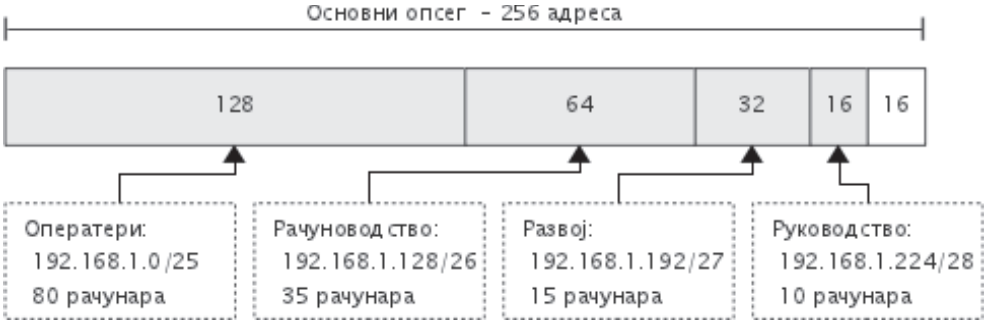
Узмимо за пример дељење мрежног опсега класе *C*, 192.168.1.0/24, за потребе организације која има 140 рачунара подељених у четири одељења:

1. оператери: 80 рачунара
2. рачуноводство: 35 рачунара
3. развој: 15 рачунара
4. руководство: 10 рачунара

Уколико желимо да рачунаре сваког од одељења изолујемо у засебну мрежу, биће нам потребне четири мреже одговарајуће величине. Могуће величине рачунарских мрежа јесу *n*-ти степени броја 2 адреса - од чега за два мањи број њихових чланова, због изузимање прве и последње адресе из опсега, односно адресе мреже и емисионе адресе. У циљу економичног коришћења ограниченог расположивог опсега адреса (256 мрежних адреса), за свако одељење биће узет најмањи могући одговарајући опсег: за 80 оператерских рачунара то је опсег од 128 адреса (2^7), за 35 рачуноводствених рачунара то је опсег од 64 адресе (2^6), за 15 рачунара развојног одељење то је опсег од 32 адресе (2^5), док је за 10 рачунара руководства то опсег од 16 адреса (2^4).

На слици 1. приказан је резултат правилне поделе расположивог опсега адреса на мање мреже, у складу са датом спецификацијом потреба. За потребе оператерског одељења одређена је мрежа од 128 адресних места. Адреса ове

мреже је 192.168.1.0/25, емисиона адреса 192.168.1.127, опсег за адресовање чланова од 192.168.1.1 до 192.168.1.126, а децимални запис мрежне маске 255.255.255.128.



Слика 1. Пример поделе мреже класе C на више подмрежа

За потребе рачуноводственог одељења одређена је мрежа од 64 адресе. Адреса ове мреже је 192.168.1.128/26, емисиона адреса 192.168.1.191, опсег за адресовање чланова од 192.168.1.129 до 192.168.1.190, а децимални запис мрежне маске 255.255.255.192.

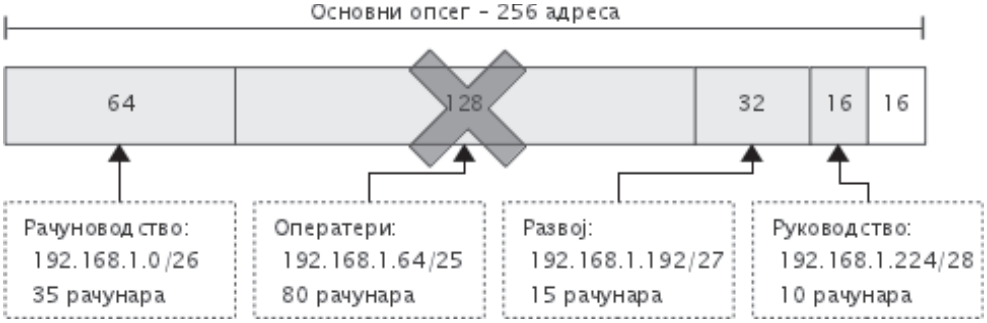
За потребе развојног одељења одређена је мрежа од 32 адресе. Адреса ове мреже је 192.168.1.192/27, емисиона адреса 192.168.1.223, опсег за адресовање чланова од 192.168.1.193 до 192.168.1.222, а децимални запис мрежне маске 255.255.255.224.

За потребе руководственог одељења одређена је мрежа од 16 адреса. Адреса ове мреже је 192.168.1.224/28, емисиона адреса 192.168.1.239, опсег за адресовање чланова од 192.168.1.225 до 192.168.1.239, а децимални запис мрежне маске 255.255.255.240.

Након описане поделе мреже *C* класе може се уочити да је последњи четворобитни опсег адреса – 192.168.1.240/28 – остао неискоришћен. Овај опсег, у описаној ситуацији, може се разматрати за коришћење на два начина. Прва ствар коју би требало размотрити јесте да ли постоји потреба за постојањем једне или више међумрежа, односно, мрежа које би чинили рутери задужени за омогућавање комуникације између дефинисаних мрежа наведених одељења. Овакав сценарио је реалан, пре свега у ситуацијама када се одељења налазе на већим географским удаљеностима. На пример, овај опсег било би могуће поделити на четири подмреже од по четири адресе, односно, са по две адресе којима се могу адресовати чланови. Такви опсези су погодни за повезивање рутера у посредне мреже.

Друга могућност искоришћавања преосталих адреса јесте њихово придодавање неком од опсега у коме се планира повећавање броја чланова (водећи при томе рачуна о правилима условљеним бинарном структуром адреса). У ситуацијама где постоји потреба за крајње економичном поделом опсега, увек треба имати у виду могућа будућа повећања броја чланова у неком од подопсега. У противном, лако се може десити да додавање једног прекобројног члана захтева реорганизацију већег броја, или чак свих дефинисаних подопсега.

Важна напомена при подели одређеног опсега мрежних адреса на мање подопсеге је да та се она мора извршити у складу са бинарном структуром мрежних адреса Интернет протокола четврте генерације. На пример, уколико бисмо заменили редослед мрежа за оператере и рачуноводство добили бисмо одређене грешке у међусобној комуникацији између чланова оператерске мреже, као и у комуникацији чланова те мреже са члановима осталих мрежа.



Слика 2. Пример неправилне поделе мреже класе C на више подмрежа

У таквој ситуацији (приказаној на слици 2.) покушај да дефинишемо опсег мрежних адреса од 192.168.1.64 до 192.168.1.192 не би био у складу са њиховом бинарном основом. Као последица јавила би се ситуација у којој би рачунари адресовани адресама мањим од 192.168.1.127 сматрали да се налазе у мрежи 192.168.1.0/25, а рачунари адресовани адресама већим од 192.168.1.128 сматрали да се налазе у мрежи 192.168.1.128/25. Покушаји да се рачунарима доделе адресе 192.168.1.127/25 и 192.168.1.128/25 резултовали би системском грешком њихових оперативних система јер би те адресе биле сматране емисионом адресом и адресом мреже. Додатно, рачунари из ова два опсега покушавали би да међусобно комуницирају путем подразумеваног мрежног пролаза, док би чланове осталих мрежа погрешно сматрали локалним.

3.2.2.5. Јавне и приватне адресе, специјални опсези

За располагање адресама Интернет протокола одговорност је дата организацији *Internet Assigned Numbers Authority, IANA*. Ова организација је задужена за

поделу адреса Интернет протокола у опсеге за одређене намене (јавну, приватну или специјалну употребу) и делегирање надлежности над опсезима јавних адреса регионалним регистрима. Регионални регистри су задужени за расподелу добијених опсега јавних адреса операторима у свом региону.

Поред опсега за јавну употребу на Интернету постоје и посебни опсези адреса Интернет протокола који су резервисани за употребу у приватним мрежама и за специјалну употребу. Опсези адреса за приватну употребу намењени су адресовању приватних рачунарских мрежа и за коришћење адреса из тих опсега није потребно одобрење локалног Интернет провајдера или регионалног регистра. Док свака адреса из јавних опсега мора бити јединствена на Интернету, адресе намењене за приватну употребу морају бити јединствене само унутар саме приватне мреже, али се могу понављати у различитим приватним мрежама. Адресе из опсега резервисаних за употребу у приватним мрежама не могу се појављивати нити користити на Интернет мрежи. Из тог разлога рачунари адресовани адресама из ових опсега не могу директно комуницирати са рачунарима на Интернету већ за то морају користити посреднике – мрежне пролазе адресоване јединственом јавном Интернет адресом.

У наставку текста дати су параметри и намена специјалних опсега адреса Интернет протокола четврте генерације:

- **Опсег 0.0.0.0/8** има специјалну намену да означи део локалне мрежне адресе. На пример, адреса 0.0.0.0/32 представља везу ка потпуној реалној локалној адреси. Безбедносно правило „0.0.0.0/24 TCP 22 ALLOW“ дозвољава комуникацију *TCP* протокола по порту 22 само члановима локалне мреже *C* класе, док правило „0.0.0.0/32 TCP 110 ALLOW“ омогућава употребу *POP3* протокола само на рачунару на коме је примењено. Дакле, адреса 0.0.0.0 је симболичка веза са локалном адресом мрежног интерфејса док је /XX број почетних битова који се од ње узима. Коришћењем ове адресе могу се направити правила која се могу преносити на различите мрежне уређаје, без потребе да се за сваки од њих ажурирају адресе.
- **Опсег 10.0.0.0/8** је намењен за приватну употребу. Он уједно представља и највећи блок адреса Интернет протокола четврте генерације резервисан за приватну употребу (класа *A*). С обзиром на то да би из одређених разлога било неефикасно стављање 16.777.216 чланова у исту мрежу, овај опсег се најчешће дели на више мањих опсега у складу са структуром и потребама организације која га користи.

- **Опсег 127.0.0.0/8** назива се и опсегом повратних адреса (енгл. *loopback address*) а намењен је за локалну употребу, унутар једног рачунара. Адресе из овог опсега не користе се ни на Интернету, нити у локалним мрежама, јер оне нису намењене адресовању физичких већ логичких мрежних интерфејса. За потребе локалних мрежних комуникација, односно комуникација унутар једног рачунара, најчешће се користи адреса 127.0.0.1/32 с тим да су све адресе из овог опсега резервисане за исту намену.

- **Опсег 169.254.0.0/16** назива се и блоком адреса за локалне везе (енгл. *link local addresses*). Адресе из овог опсега нису намењене за јавно коришћење на Интернету, нити за регуларно коришћење у локалним мрежама, већ се користе као специјалне адресе за рачунаре у локалној мрежи. У случају да активном мрежном интерфејсу рачунара није статички додељена адреса, нити ју је добио путем *DHCP* протокола, оперативни систем може за адресовање тог интерфејса случајним избором одабрати једну од адреса из овог опсега. На тај начин два рачунара чији су мрежни интерфејси адресовани на описани начин имају велике шансе да остваре комуникацију. Рачунари адресовани на овај начин имају само могућност локалне комуникације.

- **Опсег 172.16.0.0/12** је, као и блокови 10.0.0.0/8 и 192.168.0.0/16, резервисан за употребу у приватним мрежама. Овај опсег дефинише 1.048.576 адреса за локалну употребу. Међутим, због своје бескласне структуре ређе се среће у пракси од остала два опсега локалних адреса.

- **Опсег 192.0.0.0/24** представља прву мрежу из опсега резервисаног за мреже *C* класе. Овај опсег је резервисан за експерименталне потребе *IANA* и *IETF* организација. Адресе из овог опсега нису намењене коришћењу у јавној и приватним мрежама.

- **Опсег 192.0.2.0/24** носи назив *TEST-NET-1* и његове адресе су намењене за коришћење у документацији и литератури. Адресе из овог опсега најчешће се користе у пару са *example.com* Интернет доменом и нису намењене коришћењу у јавној и приватним мрежама. Аутори различите документације (књига, упутстава и сл.) могу користити ове адресе за одређене демонстрације, без бојазни да ће случајно указати на већ резервисану адресу неке организације и тиме јој, евентуално, нанети штету.

- **Опсег 192.88.99.0/24** намењен је за превођење адреса Интернет

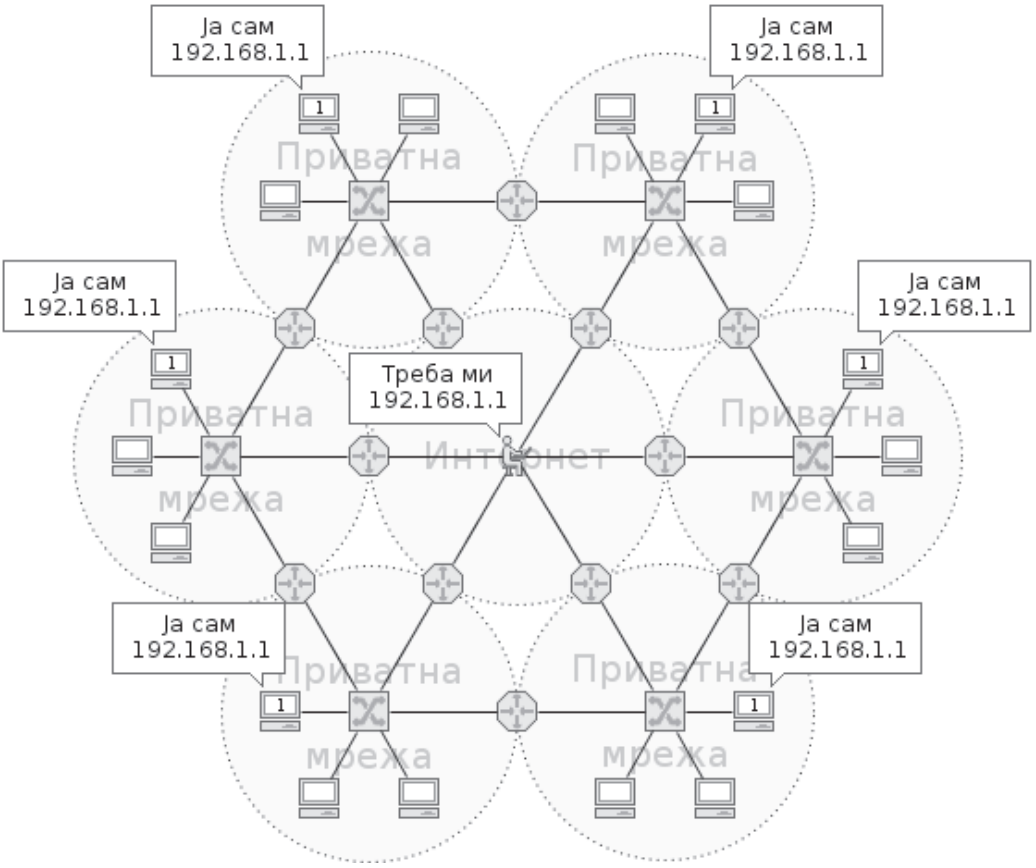
протокола шесте генерације у адресе Интернет протокола четврте генерације. Адресе из овог опсега сматрају се јавним адресама, односно адресама којима се адресују регуларни чланови Интернета (најчешће рутери са подршком за обе генерације Интернет протокола).

- **Опсег 192.168.0.0/16** је последњи опсег адреса Интернет протокола четврте генерације, резервисаних за употребу у приватним мрежама. Овај опсег садржи 65.536 адреса, односно, 256 мрежа класе *C*. У пракси, употреба овог мрежног опсега за адресовање приватних мрежа веома је честа.
- **Опсег 198.18.0.0/15** садржи адресе резервисане за коришћење код мерења перформанси – брзине комуникације – између одређених уређаја на Интернету. За те потребе изабран је посебан опсег да би се избегла евентуална загушења канала резервисаних за регуларне комуникације. Из тог разлога рутери не врше прослеђивање пакета код којих изворна адреса припада овом опсегу.
- **Опсег 198.51.100.0/24** носи назив *TEST-NET-2* и његове адресе су, као и адресе опсега 192.0.2.0/24 намењене за коришћење у документацији и литератури. Адресе из овог опсега нису намењене коришћењу у јавној и приватним мрежама.
- **Опсег 203.0.113.0/24** носи назив *TEST-NET-3* и његове адресе су, као и адресе опсега 192.0.2.0/24 и 198.51.100.0/24, намењене за коришћење у документацији и литератури. Адресе из овог опсега нису намењене коришћењу у јавној и приватним мрежама.
- **Опсег 224.0.0.0/4** раније је представљао опсег адреса резервисан за мреже *D* класе. Користи се за адресовање вишеструких одредишта (енгл. *multicast*).
- **Опсег 240.0.0.0/4** раније је представљао опсег адреса резервисан за мреже *E* класе а данас је резервисан за будућу употребу.

Наведени опсези адреса Интернет протокола четврте генерације у прошлости су више пута реорганизовани у складу са уочаваним потребама и проблемима. Историјат ових измена може се наћи у *RFC* документима. Са друге стране, може се очекивати још измена с обзиром на то да су неки опсези резервисани за потребе које ће накнадно бити уочене, као и да ће се у блиској будућности јавити изражен дефицит адреса Интернет протокола четврте генерације, чиме ће се убрзати прелазак на шесту генерацију тог протокола.

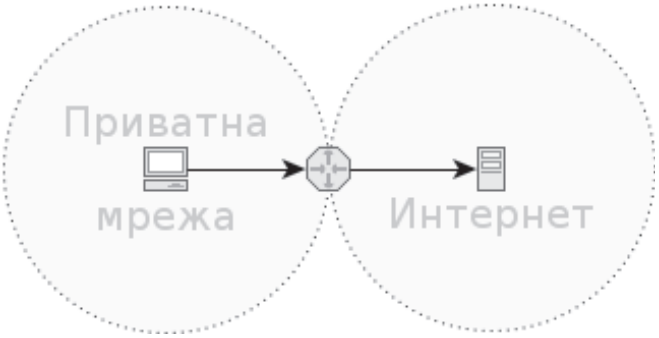
3.3. Комуникација приватних мрежа и Интернета

Приватне мреже користе посебне опсеге адреса, односно опсеге који се слободно могу користити и понављати у приватним мрежама, али се не смеју користити за адресовање комуникација на Интернету. Из тог разлога комуникација приватних мрежа са Интернетом није могућа без додатних механизама.



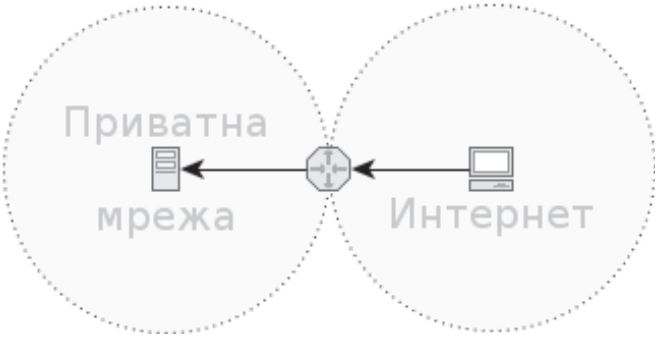
Слика 1. Немогућа је комуникација на Интернету са приватним адресама

Први механизам за омогућавање комуникације између чланова приватних мрежа и чланова Интернета је превођење мрежних адреса. Овај механизам омогућава да се успостави комуникација коју је иницирао члан приватне мреже. Успостављање комуникације у обрнутом смеру, од стране члана Интернета, овим механизмом није омогућено.



Слика 2. Превођење мрежних адреса

Механизам који омогућава комуникацију иницирану од стране чланова Интернета назива се **прослеђивање портова**. Код овог механизма се на рутеру дефинише ком члану приватне мреже треба проследити одређене податке.



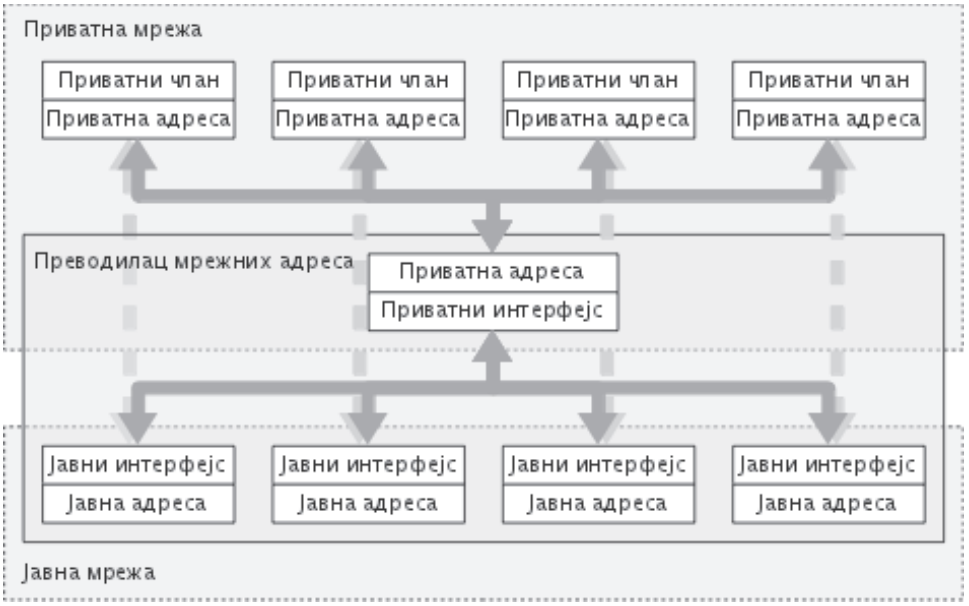
Слика 3. Прослеђивање портова

У оба случаја, и код превођења мрежних адреса, и код прослеђивања портова, страна комуникације која се налази у Интернет мрежи има утисак да разговара са рутером који повезује приватну мрежу са Интернетом.

3.3.1. Превођење мрежних адреса

Превођење мрежних адреса (енгл. *Network Address Translation, NAT*) неопходан је процес за омогућавање комуникације рачунара из приватних мрежа, адресованих адресама резервисаним за коришћење у приватним мрежама, са рачунарима на Интернету. Овај процес подразумева постојање преводиоца мрежних адреса - посредника између приватне рачунарске мреже и Интернета. Иако поседују неке заједничке елементе, улогу преводиоца мрежних адреса не треба поистовећивати са улогом рутера јер је превођење мрежних адреса знатно сложенији процес.

Потреба за превођењем мрежних адреса јавила се услед недостатка слободних IP адреса, односно услед потребе да се већем броју рачунара из приватне мреже омогући приступ Интернет мрежи путем једне јавне адресе Интернет протокола. Из тог разлога се рачунари у приватним мрежама адресују за њих резервисаним адресама које нису јединствене на глобалном нивоу већ се могу понављати у различитим приватним мрежама. Преводилац мрежних адреса је уређај који је најчешће подразумевани мрежни пролаз рачунара у приватној мрежи, а поседује и једну или више јавних адреса путем којих се врши размена података са рачунарима на Интернету.



Слика 1. Архитектура превођења мрежних адреса

Код превођења мрежних адреса преводилац замењује своју јавну адресу адресом члана у приватној мрежи или обрнуто. Уколико члан из приватне мреже шаље пакет члану јавне мреже преводилац ће изворишну адресу пакета заменити одговарајућом јавном локалном адресом. Након добијања одговора на послати пакет преводилац одредишну адресу пакета замењује адресом члана приватне мреже који је послао захтев. У случају да комуникацију иницира члан јавне мреже извршава се исти процес али обрнутим редоследом. У одређеним случајевима се поред адреса замењују и изворишни, односно одредишни портови пакета.

Основа рада преводиоца мрежних адреса јесте поседовање по најмање једног мрежног интерфејса у две или више рачунарских мрежа. Ове мреже се називају

унутрашњом и спољашњом, а најчешће подразумевају приватну и Интернет мрежу. Преводиоци располажу једном или више адреса спољашње мреже које користе за потребе комуникације чланова локалне мреже са члановима спољашње мреже.

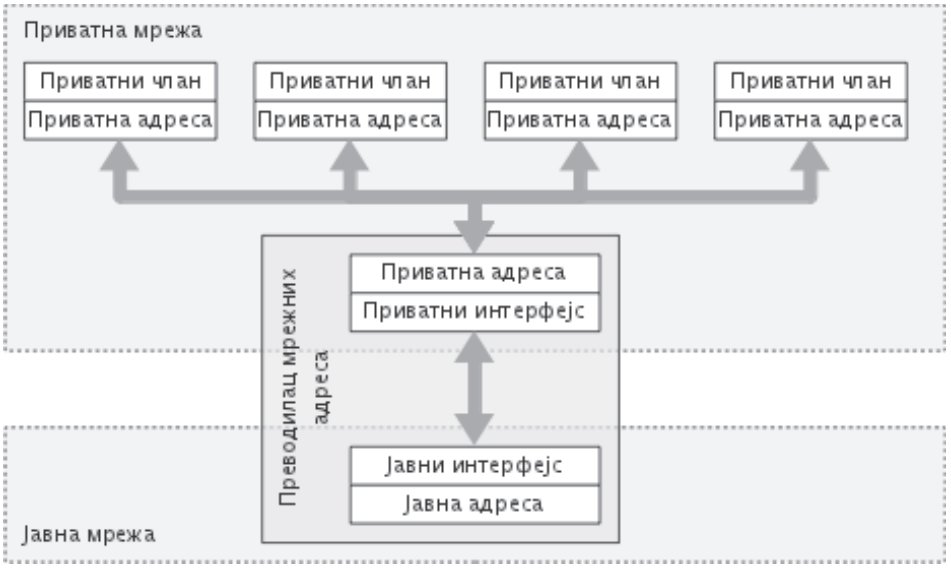
Код директног превођења мрежних адреса, при слању података од стране рачунара из приватне мреже, мрежни преводилац, пре прослеђивања пакета у јавну мрежу, замењује приватну адресу пошиљаоца одговарајућом јавном адресом. Након замене (превођења, пресликавања) изворне адресе преводилац шаље пакет кроз одговарајући интерфејс на јавној мрежи. Са друге стране, при пријему пакета адресованих на јавну адресу (за коју је дефинисано превођење у одређену адресу приватне мреже), преводилац ту адресу замењује одговарајућом приватном адресом. Након замене, преводилац прослеђује пакет у приватну мрежу којом се он прослеђује до примаоца. Код директног превођења мрежних адреса није значајно ко је иницијатор комуникације, односно веза се може успоставити и од стране члана приватне мреже, и од члана јавне мреже.

Један од главних недостатака директног превођења јавних у приватне мрежне адресе јесте потреба за истим бројем јавних адреса у односу на број рачунара у приватној мрежи који ће приступати јавној мрежи. Из тог разлога се, у ситуацијама када је број доступних јавних адреса мањи од броја рачунара из приватне мреже, користи превођење адреса путем портова (енгл. *Network Address Port Translation, NAPT*).

Превођење адреса путем портова (енгл. *Port Address Translation*) подразумева поседовање једне или неколико јавних мрежних адреса од стране преводиоца. Пошто се на овај начин не може извршити директно мапирање (број јавних адреса је мањи од броја чланова у приватној мрежи) преводиоци захтеве добијене од чланова приватне мреже везују за један од слободних портова јавне адресе. На тај начин се приватна адреса и изворишни порт замењују јавном адресом и неким од на њој слободних портова. С обзиром на то да се мапирање код оваквог превођења врши динамички, код њега није могуће иницирати комуникацију од стране рачунара који се налазе у јавној мрежи. Због тога се овим приступом уједно подиже ниво безбедности рачунара у приватној мрежи, али се њиме и онемогућава нормално функционисање сервиса који подразумевају захтевање успостављања везе са спољне мреже.

На слици 3. дат је пример мрежне топологије која за приступ чланова приватне мреже јавној мрежи користи превођење мрежних адреса путем портова. Чланови приватне мреже адресовани су приватним опсегом мрежних адреса,

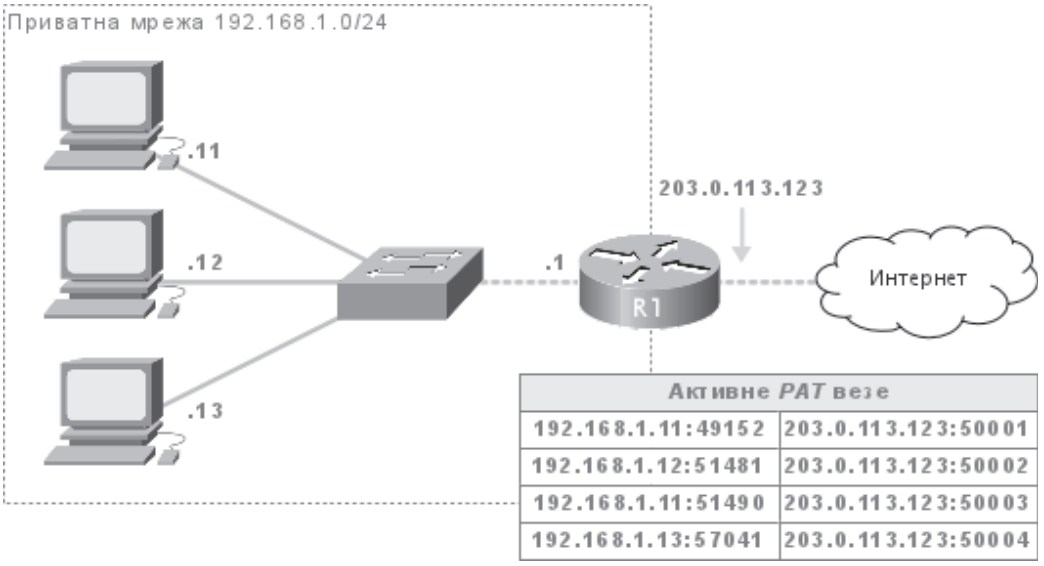
као и унутрашњи интерфејс рутера који чини пролаз између приватне и Интернет мреже. На слици је дата и табела тренутно активних *PAT* асоцијација које чине адреса и порт члана локалне мреже, као и адреса и порт рачунара на Интернету са којим он комуницира. Ова табела се формира и ажурира динамички, у складу са успостављањем и раскидањем веза. У зависности од потреба и могућности уређаја који врши превођење мрежних адреса, табела активних *PAT* веза може садржати и додатне параметре (сопствена адреса и интерфејс у приватној мрежи, адреса удаљеног рачунара и сл.).



Слика 2. Архитектура превођења мрежних адреса путем портова

У сваком пакету који напушта приватну мрежу рутер замењује изворну адресу и порт одговарајућим вредностима из десне колоне. Такође, у сваком пакету који долази са Интернет мреже, а који долази на неки од портова из десне колоне, одредишна адреса и порт се замењују одговарајућом вредношћу из леве колоне и он се прослеђује одговарајућем члану приватне мреже.

Превођење мрежних адреса је специфична функционалност која омогућава далеко ефикасније повезивање великог броја рачунара из приватне рачунарске мреже са Интернетом када је у питању број употребљених јавних адреса. Његовим коришћењем штеде се јавне адресе Интернет протокола, а уједно се код превођења путем портова повећава и ниво безбедности приватне мреже јер се онемогућава захтевање успостављања везе од стране рачунара који се не налазе у приватној мрежи.



Слика 3. Пример топологије са NAPT/PAT превођењем адреса

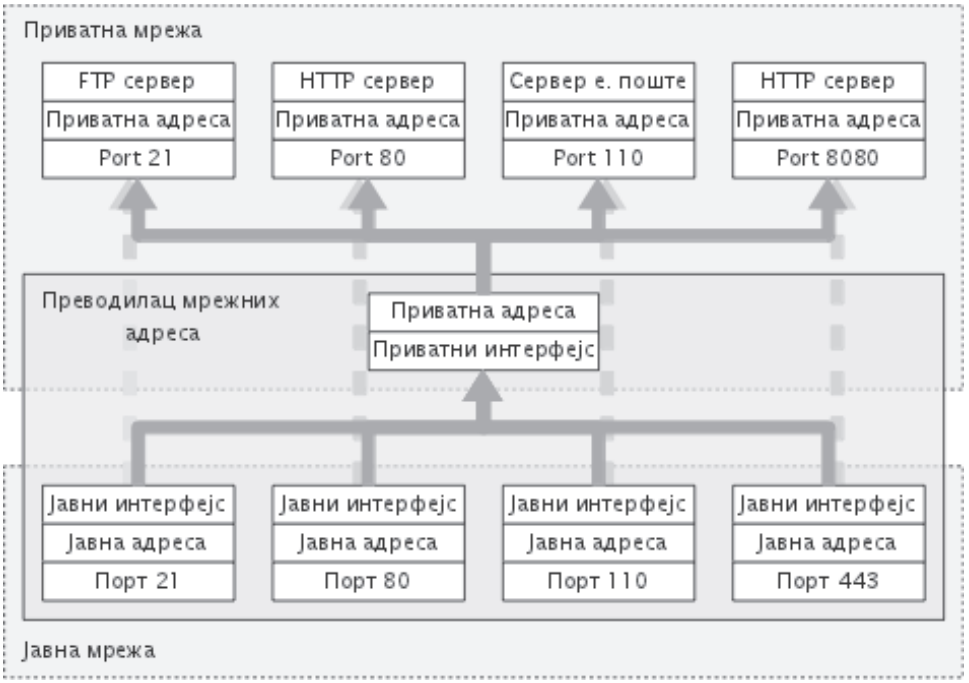
Са друге стране, превођење мрежних адреса, у случајевима ограничене процесорске снаге преводиоца, може негативно утицати на перформансе преноса података, првенствено у виду повећања кашњења испоруке. Додатно, одређени мрежни протоколи (нпр. *IPsec*) забрањују било какву измену података током преноса тако да се код њих морају користити додатни механизми тунеловања или је њихов рад у потпуности онемогућен.

3.3.2. Прослеђивање портова

Код директног превођења мрежних адреса сви захтеви упућени на јавну адресу прослеђују се одговарајућој приватној адреси, односно, рачунару или уређају који је користи. На тај начин је могуће омогућити успостављање везе са чланом приватне рачунарске мреже на захтев чланова јавне рачунарске мреже. То је посебно значајно у случајевима када члановима јавне мреже треба омогућити приступ мрежним сервисима које обезбеђују чланови приватне рачунарске мреже. На пример, организација може имати Веб сервер у оквиру своје локалне, приватне рачунарске мреже, а да се тај сервер користи за испоруку Веб презентације клијентима који приступају са Интернет мреже.

Са друге стране, у ситуацијама када се не користи директно превођење мрежних адреса, већ је у питању превођење адреса путем портова, преусмеравање саобраћаја се не може извршити директно. На самим преводиоцима мрежних адреса морају се дефинисати правила на основу којих

се одређује ком члану приватне мреже треба доставити одређени захтев који потиче са јавне мреже. Сам процес прослеђивања захтева назива се прослеђивањем портова (енгл. *port forwarding*).

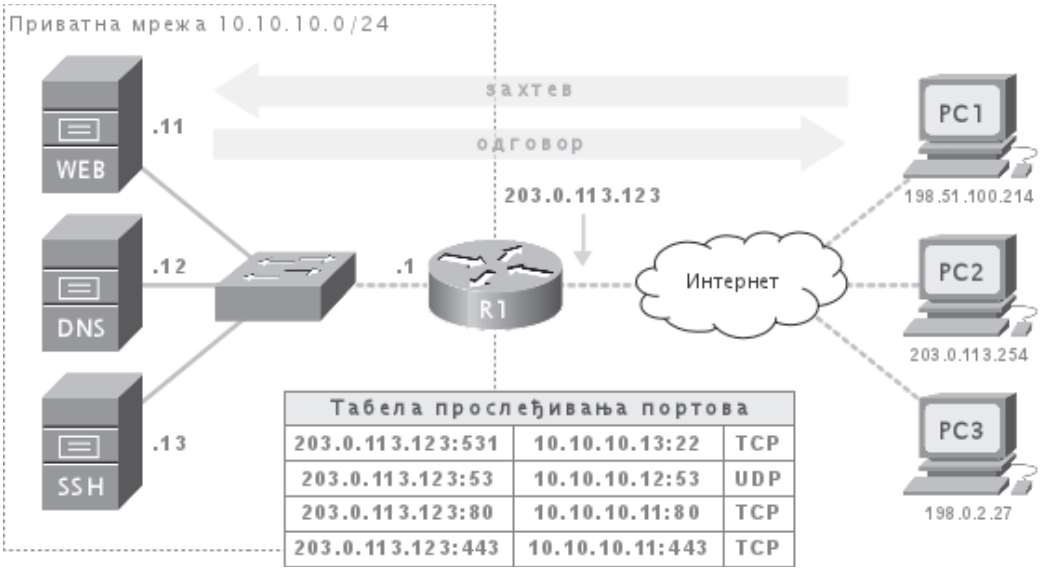


Слика 1. Прослеђивање портова код NAPT превођења мрежних адреса

На слици 2. дат је пример приватне мреже која садржи сервере чијим је услугама могуће приступити са спољне, Интернет мреже. Сервери у приватној мрежи користе адресе из приватног опсега 10.10.10.0/24 а на њима су доступни *SSH*, *DNS*, *HTTP* и *HTTPS* сервиси. Ови сервиси су мапирани у виду асоцијација приказаних у табели прослеђивања портова. Ова табела се налази на рутеру *R1* чија је улога омогућавање комуникације између чланова приватне и Интернет мреже.

Клијенти на Интернету сервисима у приватној мрежи приступају коришћењем јавне адресе преводиоца (рутера) - 203.0.113.123. Након добијања захтева за сервисом од стране клијента из Интернет мреже рутер проверава да ли је у табели дефинисано прослеђивање за захтевани порт. Уколико јесте, рутер замењује одредишну адресу пакета одговарајућим адресом приватне мреже и прослеђује захтев члану локалне мреже. Сервер у локалној мрежи резултат обраде захтева упућује на изворишну адресу - адресу члана јавне мреже који је захтевао услугу. Рутер, као посредник у овој комуникацији, замењује изворишну

адресу (адреса сервера у приватној мрежи) својом јавном адресом и прослеђује одговор на јавну адресу са које је клијент упутио захтев.



Слика 2. Пример топологије са функцијом прослеђивања портова

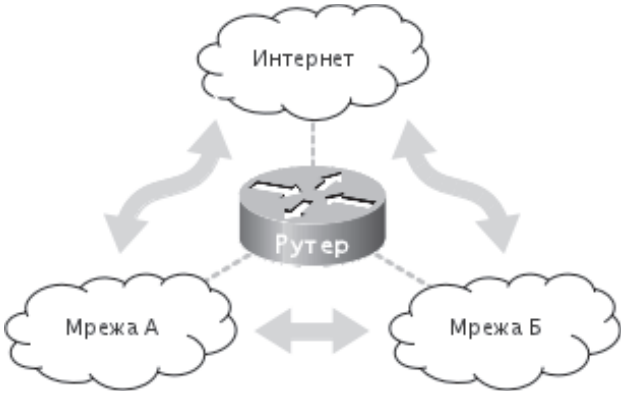
Приликом описаног процеса комуникације клијент из јавне мреже сматра да је непосредан испоручилац сервиса заправо уређај који се налази на јавној Интернет адреси приватне мреже. У неким случајевима се приликом прослеђивања захтева серверу у локалној мрежи не врши замена одредишне адресе, а у неким случајевима се поред замене одредишне врши и замена изворишне адресе. Ове варијације су првенствено везане за коришћење безбедносних протокола и топологија које омогућавају анонимност.

У зависности од карактеристика преводиоца мрежних адреса могуће је дефинисати више критеријума на основу којих ће се одредити прималац прослеђеног саобраћаја. Основни критеријуми за прослеђивање захтева су одредишна јавна адреса и одредишни порт на јавној адреси.

У случајевима када преводилац поседује одговарајуће могућности, као додатни параметри за прослеђивање могу се користити и изворишна јавна адреса, временски период, оптерећење комуникационог канала, оптерећење примаоца, и сл. Такође, у правилима за прослеђивање за једну јавну или приватну адресу може се везати више портова а пријемни порт на јавној адреси не мора бити идентичан пријемном порту на приватној адреси.

3.4. Рутирање и протоколи рутирања

Једно од основних задужења мрежног слоја, односно уређаја и протокола који на њему функционишу, јесте одређивање руте којом ће подаци путовати до коначног одредишта. Унутар једне мреже за испоруку пакета података одредишној адреси задужени су протоколи слоја везе. Пакете из једне мреже у другу преусмеравају рутери - уређаји који имају улогу мрежних пролаза. Подразумевана улога рутера јесте повезивање две или више рачунарских мрежа кроз преусмеравање пакета података. Процес у коме рутери преусмеравају пакете ка посредним мрежама или коначном одредишту назива се рутирање.



Слика 1. Рутери прослеђују податке између различитих мрежа

Након пријема пакета на одређеном мрежном интерфејсу, рутер врши распакивање до слоја мреже и узима параметре из заглавља пакета. За одређивање руте пакета најважнији параметар заглавља је одредишна адреса која се упоређује са записима из табеле рутирања.

Табела рутирања чини основу рада рутера и самог процеса рутирања. У табели рутирања налазе се информације на основу којих рутер одређује куда треба послати одређени пакет. Основна информација коју носи сваки од записа у табели рутирања јесте до које се одредишне мреже може доћи прослеђивањем пакета одређеном мрежном пролазу.

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.55.0	192.168.60.10	255.255.255.0	UG	0	0	0	eth0
192.168.60.0	*	255.255.255.0	U	0	0	0	eth0
loopback	*	255.0.0.0	U	0	0	0	lo
default	192.168.60.12	0.0.0.0	UG	0	0	0	eth0

Слика 2. Једноставна табела рутирања на Линукс оперативном систему

За сваки од примљених пакета рутер његову одредишну адресу упоређује са

свим записима табеле рутирања тражећи мрежу којој одредишна адреса пакета припада. У случају да не постоји посебно дефинисана одредишна мрежа пакет се прослеђује подразумеваном мрежном пролазу (уколико је дефинисан). У случају да је у табели рутирања дефинисано више мрежа којима одредишна адреса припада (на пример, одредишна адреса је 192.168.12.34 а постоје записи за мреже 192.168.0.0/16 и 192.168.12.0/24) искористиће се мрежни пролаз оне мреже код које је веће поклапање почетних битова адресе. Са друге стране, уколико се код вишеструких рута јави идентично поклапање почетних битова, односно, за једну одредишну мрежу постоји више мрежних пролаза, избор се врши у зависности од метрике, односно приоритета путање. Постојање вишеструких мрежних пролаза ка истој одредишној мрежи и са истом метриком најчешће указује на балансирање оптерећења наизменичним коришћењем доступних рута.

Метрика руте одређује приоритет руте у односу на остале дефинисане руте којима се може доћи до одредишта. Њена вредност се може задати статички од стране администратора, а може се и динамички израчунати коришћењем различитих параметара комуникационих канала: број скокова - број рутера који посредују у комуникацији, пропусна моћ, оптерећеност, кашњење, и сл. Динамичко одређивање метрике руте врше протоколи за динамичко рутирање а администратор може да зада формуле у које ће се укључити поменути параметри, у зависности од конкретне ситуације.

Формирање исправне табеле рутирања један је од главних задатака код успостављања рутирања у рачунарским мрежама. Записи табеле рутирања се додају на три основна начина:

1. директним повезивањем рутера са одређеном рачунарском мрежом,
2. статичким додавањем рута од стране администратора и
3. динамичким утврђивањем могућих рута коришћењем протокола за динамичко рутирање.

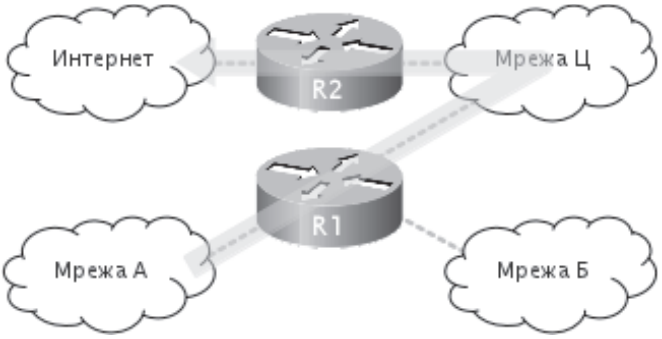
Директно повезивање рутера са одређеном рачунарском мрежом подразумева физичко повезивање мрежног интерфејса и његово адресовање на мрежном слоју. Већина савремених рутера и мрежних оперативних система након описаних корака аутоматски додаје одговарајући запис у табелу рутирања а испорука пакета адресованих на чланове тих мрежа врши се директно - коришћењем адресовања протокола слоја везе и без посредовања мрежних пролаза.

Статичко рутирање подразумева ручни унос записа табеле рутирања од стране

администратора мреже. Овакав приступ је ефикасан код мањих и једноставнијих рачунарских мрежа где нема потребе за великим бројем рута и њиховим честим изменама. Такође, статички унете руте је тешко заобићи што их чини погодним и са безбедносног аспекта. Са друге стране, статичко дефинисање табеле рутирања је неефикасно код сложених рачунарских мрежа које имају велики број могућих рута и код којих се руте (или њихова метрика) често мењају.

Динамичко рутирање подразумева коришћење одговарајућих протокола. Постоји више различитих протокола за динамичко рутирање али је њихова основна улога заједничка: размена информација између рутера у циљу формирања табела рутирања на основу којих ће се подаци између различитих мрежа прослеђивати коришћењем оптималних рута. За коришћење динамичког рутирања од администратора се очекује да на рутерима укључи одређени протокол за динамичко рутирање и зада параметре његовог коришћења. У складу са тим, време потребно за подешавање рутирања у сложенијим мрежама, коришћењем динамичких протокола, може бити далеко краће у односу на статички унос рута али се од администратора захтева виши ниво знања.

Не треба мешати **протоколе за рутирање** (енгл. *routing protocol*) и **протоколе који се рутирају** (енгл. *routed protocol*). Протоколи за рутирање обезбеђују рутерима информације потребне да би се успешно извршило рутирање пакета протокола који се рутирају. Такође, протоколи за рутирање најчешће раде на апликативном а протоколи који се рутирају на мрежном слоју.



Слика 3. Рутер R1 нема директну везу са Интернет мрежом

На слици 3. приказана је реална ситуација у којој не постоји само један рутер који повезује различите мреже, односно, у којој немају сви рутери директну везу са свим рачунарским мрежама. У приказаној ситуацији рутер *R1* би у своју табелу рутирања додао записе о мрежама A, B и C самим прикључивањем на

њих. Са друге стране, рутер *R1* иницијално нема информацију о могућности изласка на удаљене мреже, у овом случају на Интернет мрежу, већ би такав запис морао да се у његову табелу дода као статичан унос или путем протокола за рутирање. Најпогоднији облик за додавање овог записа јесте **подразумевана рута** (енгл. *default route*) која ће се користити уколико одредишна адреса пакета не припада ни једној од осталих мрежа дефинисаних у табели рутирања.

Рутер *R2* из приказане ситуације нема информацију о мрежама А и Б јер са њима није директно повезан. Подразумевана рута на рутеру *R2* би требало да пакете адресоване на мреже којих нема у табели рутирања усмери ка Интернету. Очигледно је да је таква одлука погрешна, односно да она неће довести до испоруке пакета жељеним примаоцима. Из тог разлога у табелу рутирања рутера *R2* морају се додати одговарајући записи о мрежама А и Б, да се до њих стиже посредством рутера *R1* (његовог интерфејса у мрежи Ц). Такви записи се могу додати статички, или их могу формирати протоколи за динамичко рутирање на основу информација добијених од рутера *R1*.

Постоје четири основна случаја у којима рутер доноси различите одлуке о томе шта ће урадити са примљеним пакетом. У првом случају је одредишна адреса пакета придружена једном од локалних мрежних интерфејса. Тада се даље прослеђивање пакета прекида а његов садржај се прослеђује одговарајућем протоколу вишег (најчешће транспортног) нивоа.

У другом случају одредишна адреса примљеног пакета припада једној од мрежа на које је рутер директно повезан. У том случају се прекида даље рутирање пакета и он се испоручује одредишту коришћењем физичке инфраструктуре и протокола на слоју везе.

Трећи случај подразумева да се одредишна адреса налази у удаљеној мрежи којој рутер има приступ путем суседног рутера. У том случају се пакет мрежног слоја у добијеном облику прослеђује суседном рутеру коришћењем посредне физичке инфраструктуре и протокола на слоју везе.

Четврти случај подразумева да се одредишна адреса пакета налази у мрежи за коју рутер нема податке у својој табели рутирања. У том случају се пакет одбацује а извориште се шаље порука о томе да није могуће доћи до одредишта.

3.4.1. Протоколи за динамичко рутирање

Основни начин за дефинисање рута представља њихово ручно уношење у табелу рутирања од стране администратора. У случајевима једноставних и

статичних рачунарских мрежа такав начин дефинисања правила рутирања може се сматрати оптималним. Међутим, код сложених рачунарских мрежа - мрежа које садрже велики број рутера и путања - ручно попуњавање табела рутирања на рутерима може захтевати огромно време и ангажовање администратора. Додатно, у динамичним мрежама - мрежама код којих су честе измене комуникационих водова и њихових стања - ручно прилагођавање насталим промена обично подразумева дуге периоде неоптималног или онемогућеног коришћења комуникационе инфраструктуре. Из тог разлога су развијени и користе се протоколи за динамичко рутирање.

Протоколи за динамичко рутирање омогућавају аутоматизовано попуњавање табела рутирања на основу информација размењених између рутера. Коришћењем ових протокола рутери размењују информације о томе који од њих имају приступ којим мрежама. На основу размењених информација се израчунавају могуће и оптималне руте. За одређивање приоритета рута, односно оптималне и алтернативних путања, узимају се различити параметри као што су број посредних рутера, капацитет и заузеће комуникационих канала, кашњење и сл.

Данас у употреби постоји више протокола за динамичко рутирање. С обзиром на њихову исту основну намену - израчунавање оптималних путања комуникације - постојање вишеструких решења проузроковано је различитим приступима у реализацији, потребом да се решења прилагоде специфичностима различитих мрежа и жељом произвођача мрежних уређаја да своје производе пласирају на тржиште у што већем броју. У складу са наведним, избор протокола за рутирање у пракси најчешће зависи од следећих параметара:

- знања администратора рачунарске мреже,
- величине рачунарске мреже и специфичности реализације и
- скупа протокола које постојећа мрежна опрема подржава.

Постоји више критеријума за класификацију протокола за рутирање. Старији протоколи за рутирање развијани су у периоду када су још увек биле у употреби класе мрежних адреса. Са тог аспекта се протоколи за рутирање деле на оне који су засновани на класама и оне који подржавају подмрежавање. Данас се у пракси све ређе може срести примена протокола за рутирање који свој рад заснивају на класама мрежних адреса, а као пример за њих могу се узети прва верзија *RIP* протокола, *EGP* протокол и старије верзије *BGP* протокола. Протоколи засновани на класама у оквиру порука размењују само адресу мреже, односно не размењују мрежну маску. Мрежну маску прималац

израчунава на основу класе у коју адреса мреже спада. Протоколи који подржавају подмрежавање у порукама поред адресе мреже шаљу и мрежну маску. У ту групу спадају друга верзија *RIP* протокола, *OSPF*, *IS-IS* и други.

Са аспекта величине и типа мреже за коју су намењени протоколи за рутирање деле се на интерне - *Interior Gateway Protocol* - и екстерне - *Exterior Gateway Protocol*. С обзиром на величину Интернет мреже утврђивање њене комплетне топологије би било немогуће, чак и путем коришћења протокола за рутирање. Из тог разлога је ова мрежа подељена на аутономне системе. **Аутономни систем** (енгл. *Autonomus System*) представља скуп мрежа које користе јавне адресе Интернет протокола, а чије је администрирање поверено једној организацији. Сваки аутономни систем је од стране организације *IANA* означен јединственим бројем. У интерне протоколе за рутирање спадају *RIP*, *OSPF*, *IS-IS* и више других. За потребе рутирања између аутономних система раније је коришћен *EGP* који је касније замењен тренутно актуелним *BGP* протоколом.

Једна од најважнијих категоризација протокола за рутирање односи се на тип информација које они размењују, односно на који начин одређују могуће руте. У оквиру ове категоризације протоколи за рутирање деле се на протоколе који користе векторе удаљености (енгл. *distance vector*) и који користе стање веза (енгл. *link state*). **Протоколи базирани на векторима удаљености** комуницирају само са суседним рутерима, односно рутерима који се налазе у истим мрежама. У складу са тим, ови протоколи обезбеђују информацију који рутер је први следећи посредник у путању до коначног одредишта, али не и структуру целе мреже и руте. Метрику ових протокола најчешће чини број скокова, односно број рутера који ће посредовати у испоруци пакета у одредишну мрежу. Као представник ове групе протокола могу се узети протоколи *RIP* и *EIGRP*. Протоколи који користе векторе удаљености обично размењују мање количине података (за потребе конвергенције) од протокола који користе стање веза.

Насупрот протоколима заснованим на векторима удаљености стоје **протоколи који користе стање веза**. Они се још називају и протоколима базираним на *SPF* алгоритму, као и протоколима са дистрибуираним базама. Карактеристика ових протокола је да сваки рутер одржава базу података која описује целу топологију аутономног система коме рутер припада. Ова база се назива базом стања веза (енгл. *link-state database*) и идентична је код свих рутера у аутономном систему. На основу базе стања веза сваки рутер одређује оптималне путање између себе и осталих делова аутономног система.

У пракси се често јавља разумевање да разлика између протокола за рутирање који користе векторе удаљености и оних који користе стање веза лежи у врсти

података који се користе за одређивање метрике, односно да протоколи који користе векторе удаљености за израчунавање метрике користе искључиво број скокова док протоколи који користе стање веза користе пропусну моћ и заузеће комуникационих канала. Такво разумевање је погрешно јер основну разлику чини то да ли коришћењем одређеног протокола рутер формира комплетну топологију мреже у којој се налази или само долази до информације до којих све мрежа може доћи преко својих суседних рутера. На пример, EIGRP протокол за рутирање заснован је на векторима удаљености а за израчунавање метрике користи пропусну моћ комуникационих канала, њихово заузеће, кашњење и поузданост.

Када су у питању протоколи за динамичко рутирање, **конвергенција** означава усклађеност информација свих рутера у мрежи, односно поседовање свих потребних информација на основу којих су формиране исправне табеле рутирања на свим рутерима. У конвергентним мрежама нема грешака у рутирању као што су бесконачне петље, губитак пакета и слично. Протокол за динамичко рутирање може се сматрати исправним уколико се њиме у разумном временском року (након укључивања свих рутера) може постићи стање конвергенције. Након постизања, стање конвергенције остаје активно док се год не деси нека измена у топологији. Настанак измене у топологији је окидач за размену нових информација протоколима за динамичко рутирање и поновно постизање стања конвергенције. Што је време за постизање конвергенције по укључивању свих рутера, или настанку измене у топологији краће, то се протокол за динамичко рутирање може сматрати оптималнијим по том питању.

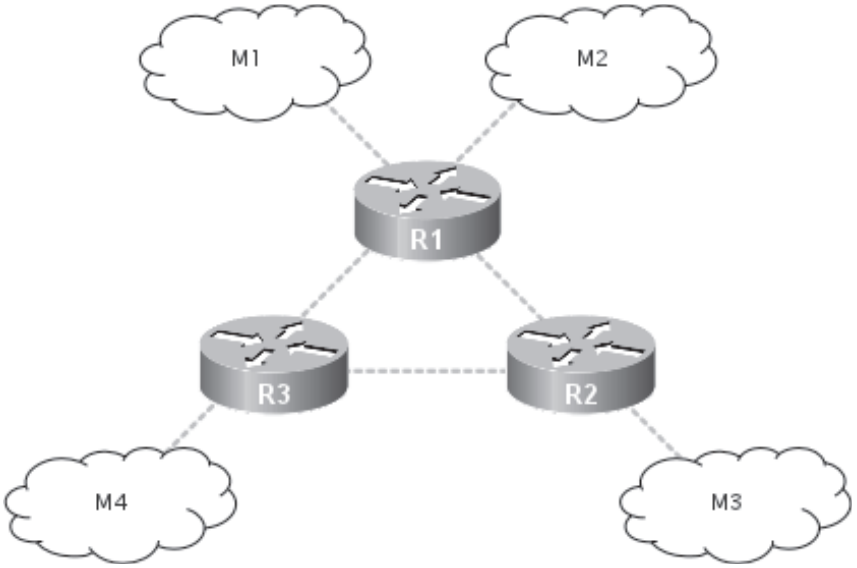
3.4.1.1. RIP - протокол информација за рутирање

Један од најпопуларнијих протокола за рутирање који користе векторе удаљености је протокол информација за рутирање (енгл. *Routing Information Protocol, RIP*). Корени овог протокола налазе се у програму *routed* који се користио на *BSD UNIX* оперативном систему, а чији је формат порука за размену информација за рутирање био *de facto* стандард у том периоду. Спецификација протокола иницијално је дата 1988. године а од тада се појавило неколико проширења везаних за подршку бескласних мрежа и шесту верзију Интернет Протокола. Основе алгоритма који користи *RIP* протокол датирају још из 1969. године из *ARPANET* мреже.

Протокол информација за рутирање намењен је за коришћење у мрежама које користе Интернет протокол на мрежном слоју (протокол који се рутира) и које користе једноставне (тачка-тачка) или сложене топологије (*Token-ring, Ethternet*).

У погледу величине мрежа у којима се може користити, овај протокол је ограничен на мреже чији је мрежни пречник - најкраћа путања по броју коришћених рутера између две најудаљеније интерне мреже - мањи од 16. То значи да се коришћењем овог протокола не може достићи конвергентно стање у мрежама где у најкраћој рути комуникације између две интерне мреже посредује више од 15 рутера.

Основни принцип рада протокола информација за рутирање подразумева оглашавање доступних мрежа, односно обавештавање суседних рутера о записима у локалној табели рутирања. Након пријема обавештења рутери ажурирају своје табеле рутирања новодобијеним информацијама. Процес обавештавања суседних рутера се затим понавља, односно информације из локалне табеле рутирања шаљу се суседним рутерима (који понављају процес ажурирања локалних табела рутирања и обавештавања суседних рутера). На овај начин се након одређеног броја итерација постиже стање конвергентне мреже.



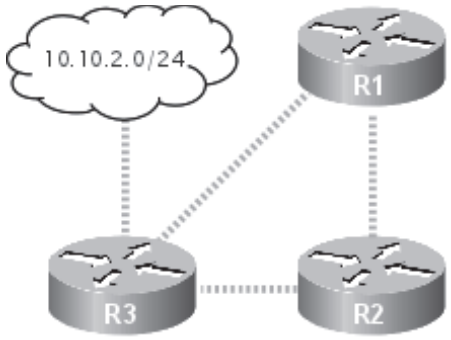
Слика 1. Топологија за илустрацију принципа рада RIP протокола

На слици 1. приказана је поједностављена топологија у којој рутер *R1* има ексклузиван приступ мрежама *M1* и *M2*, рутер *R2* има ексклузиван приступ мрежи *M3*, а рутер *R3* има ексклузиван приступ мрежи *M4*. Оваква мрежа ће постати конвергентна након две итерације обавештавања суседних протокола. У првој итерацији ће рутер *R1* рутере *R2* и *R3* обавестити о мрежама *M1* и *M2*, рутер *R2* ће обавестити рутере *R1* и *R3* о мрежи *M3* а рутер *R3* обавестити рутере

R1 и *R2* о мрежи *M4*. У овако једноставној топологији овом једном итерацијом је размењено довољно информација да сви рутери могу доћи до свих мрежа које у њој постоје. Међутим, добијање нових информација, односно измене у табелама рутирања, окидач су за нову итерацију обавештавања.

У другој итерацији ће рутер *R1* обавестити рутер *R2* о доступности мреже *M4* и рутер *R3* о доступности мреже *M3*, рутер *R2* ће обавестити рутер *R1* о доступности мреже *M4* и рутер *R3* о доступности мрежа *M1* и *M2*, а рутер *R3* ће обавестити рутер *R1* о доступности мреже *M3* и рутер *R2* о доступности мрежа *M1* и *M2*. На овај начин су рутери, поред основних рута (успостављених у првој итерацији), информисани и о алтернативним рутама које се могу користити у случају прекида примарних рута. На пример, уколико дође до прекида везе између рутера *R1* и *R2* рутер *R1* ће мрежи *M3* приступати посредством рутера *R3* јер је од њега добио информацију о тој могућности на начин описан у другој итерацији размене информација. Које ће се руте користити као примарне а које чувати као алтернативне одређује њихова метрика.

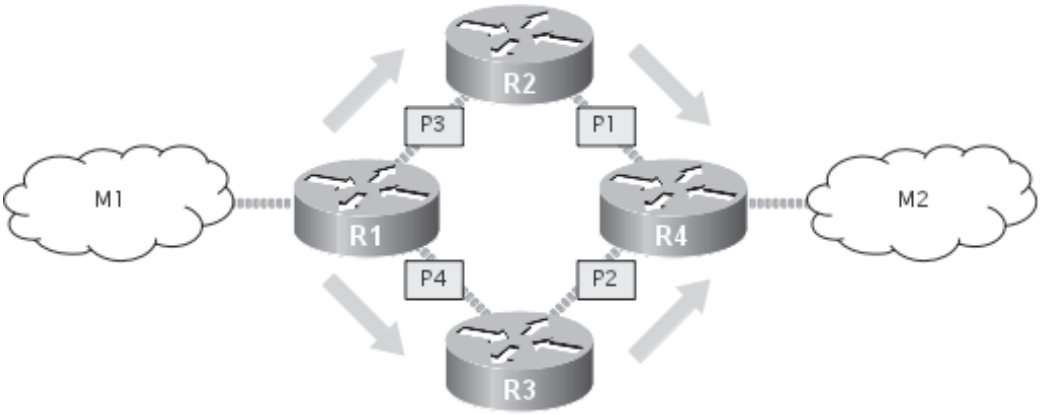
Метрика се код протокола информација за рутирање изражава кроз удаљеност одређене мреже, односно кроз број рутера који посредују у достављању података. На слици 2. приказана је топологија у којој рутер *R1* има могућност приступа мрежи 10.10.2.0/24 коришћењем две различите руте - посредством рутера *R3* и посредством рутера *R2* и *R3*. Примарна рута која ће се користити јесте директно посредством рутера *R3* јер је метрика те руте (број скокова) један док је метрика руте у којој се користе рутери *R2* и *R3* два. У случају прекида везе између рутера *R1* и *R3* алтернативна рута ће бити коришћена.



Слика 2. Топологија за илустрацију метрике код RIP протокола

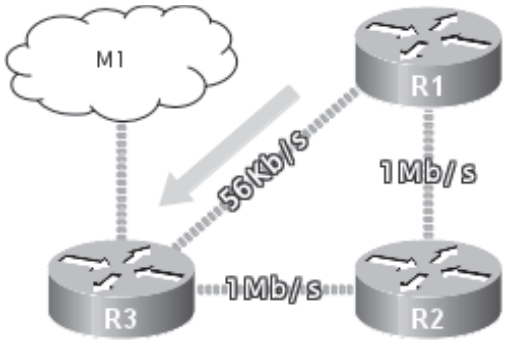
Следећа ситуација која се може јавити је та да се за долазак до одређене мреже могу користити различите руте које имају исту метрику. Пример такве мреже дат је на слици 3. где рутер *R1* поседује информацију о две руте за доставу пакета у мрежу *M2* које имају исту метрику. Подразумевано понашање рутера у оваквој

ситуацији јесте балансирање оптерећења (енгл. *load balancing*), односно наизменично слање пакета свим рутама које имају исту метрику.



Слика 3. Вишеструке руте са истом метриком омогућавају балансирање оптерећења

Избор броја скокова за основу метрике код *RIP* протокола омогућава веома једноставно формирање топологије и давање приоритета рутама. Међутим, сам број скокова не мора увек да означава оптималну путању. Метрика која користи само број скокова неће моћи да искористи путање са већим бројем скокова чији комуникациони канали имају већи број скокова или су растерећенији.



Слика 4. Метрика RIP протокола не гарантује оптимално коришћење веза

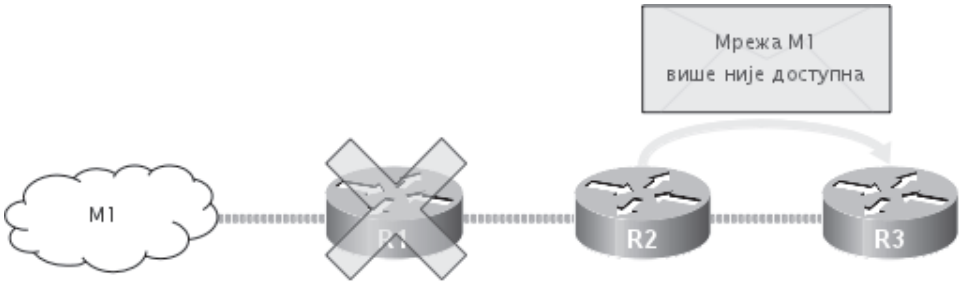
На слици 4. приказана је ситуација у којој рутер *R1* као оптималну руту ка мрежи *M1* види кроз директно посредовање рутера *R3*, наспрам руте у којој постоји један скок више (посредством рутера *R2*) али чији комуникациони канали имају готово двадесет пута већу пропусни моћ. У оваквим ситуацијама је неопходна интервенција администратора мреже да би се постигло оптимално искоришћавање доступних комуникационих канала.

Метрика *RIP* протокола се назива још и „фиксном метриком“ јер укључује само број скокова. Метрике неких од савремених протокола за рутирање поред фиксних параметара мрежа (број скокова, пропусна моћ комуникационих канала и сл.) укључују и њихове динамичне параметре, односно параметре чија се вредност мења током времена (заузеће комуникационих канала, њихова поузданост, утврђено кашњење и сл.).

3.4.1.1.1. Прилагођавање променама у топологији

До сада разматране топологије нису подразумевале никакве накнадне измене. Међутим, једна од главних предности протокола за рутирање (наспрам коришћења статичних рута) огледа се баш у могућности аутоматског прилагођавања променама у топологији. Промене у топологији могу имати различите узроке - додавање нових рутера и канала, физичко отказивање или искључивање канала, отказивање или намерно гашење рутера и слично. *RIP* протокол поседује више механизама који омогућавају аутоматско прилагођавање насталим изменама у топологији и спречавање постојања петљи у коначном броју итеративних измена, односно у коначном и прихватљивом временском периоду.

Основни начин прилагођавања насталим изменама у топологији подразумева обавештавање суседних рутера о измени топологије од стране рутера на чијим је комуникационим каналима дошло до измене. У овом случају измена у табели рутирања представља окидач за размену података између рутера у циљу синхронизације. Период од тренутка настанка измене до њеног подржавања у свим табелама на које та измена има утицаја представља период у коме мрежа рутера није конвергентна, односно могући су губици пакета података и јављање петљи рутирања.



Слика 1. Проглашавање рута недоступним

Поруке *RIP* протокола изазване настанком одређене измене шаљу се у кратком периоду након настанка саме измене. Овај период представља случајно одабрано време између једне и пет секунди. Уколико се у периоду чекања дође

до дотаних измена, све оне се шаљу у оквиру једне поруке. У оквиру ових порука се шаљу само информације о рутама код којих је дошло до измене, а не и целокупна табела рутирања.

Једна од ситуација у којима није могуће обавештавање суседних рутера о новонасталој измени у топологији мреже јесте отказивање самог рутера - његовог хардвера, софтвера, саме имплементације *RIP* или неког од носећих протокола и слично - или комуникационог канала којим би се обавештавање извршило. У таквој ситуацији задржавање постојећих записа у табелама рутирања (о рутама које користе сада недоступни рутер) доводи до губитка њему послатих пакета података. За потребе препознавања и прилагођавања оваквим ситуацијама *RIP* протокол користи периодично слање контролних порука између суседних рутера на сваких 30 секунди. У случају да рутер не добије овакву контролну поруку од суседног рутера у току 180 секунди, односно суседни рутер се не јави шест пута узастопно, он из своје табеле рутирања уклања све записе који укључују тај рутер. Додатно, он о насталој измени обавештава себи суседне рутере. Овакве измене имају посебан карактер јер се њима не оглашавају доступне већ недоступне руте.

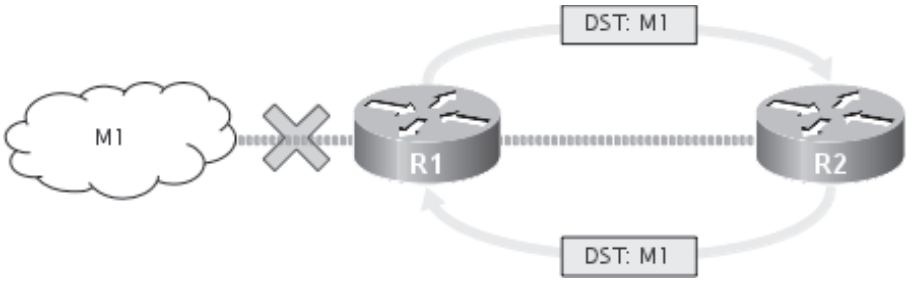
Насупрот логици да се недоступна рута једноставно изузме из даљег оглашавања, *RIP* протокол такву руту оглашава својим суседима као недоступну. Недоступна рута се оглашава у истом формату као и регуларне, али са том разликом што је њен број скокова постављен на 16. На овај начин се суседни и даљи рутери информишу да ту руту не треба користити.

3.4.1.1.2. Подела хоризонта и тровање рута

На слици 1. приказана је топологија у којој је рутер *R1* директно или посредно повезан са мрежом *M1* (метрика 1 у случају директне везе). У првој итерацији ће рутер *R1* огласити рутеру *R2* мрежу *M1* тако да ће рутер *R2* у своју табелу рутирања додати мрежу *M1* са вредношћу метрике 2. У другој итерацији ће рутер *R2* огласити мрежу *M1* свим суседима, међу којима је и рутер *R1*. Након пријема ове информације рутер *R1* неће додати запис о доступности мреже *M1* путем рутера *R2* јер таква рута има метрику 3 а у табели рутирања тренутно постоји рута са метриком 1.

Претпоставимо да након описане сихнронизације табела рутирања рутера *R1* и *R2* дође до отказивања везе рутера *R1* са мрежом *M1*. Рутер *R1* ће у том случају уклонити запис о доступности мреже *M1* из своје табеле рутирања. Међутим, у наредној итерацији ће од рутера *R2* добити информацију о доступности мреже *M1* са метриком 3 (што је застарела информација која подразумева

посредовање рутера *R1* у достављању пакета података у мрежу *M1*). У овом случају ће рутер *R1* додати мрежу *M1* у своју табелу рутирања јер у њој сада не постоји рута са бољом метриком.



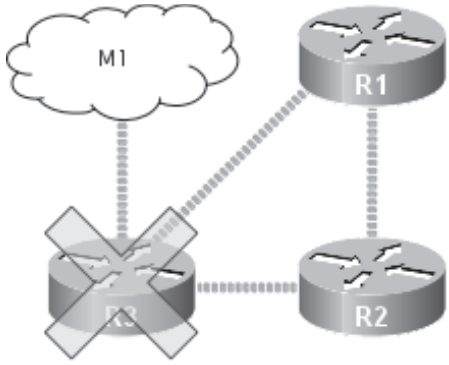
Слика 1. Подела хоризонта спречава стварање петљи у једноставним топологијама

Резултат описане ситуације био би стварање петље рутирања у којој ће се пакети података адресовани на чланове мреже *M1* непрестано шетати између рутера *R1* и *R2* - рутер *R2* ће пакете слати рутеру *R1* који ће их враћати назад рутеру *R2*... Овакво кружење пакета би се бесконачно понављало (а њихов број вероватно повећавао новим пакетима намењеним мрежи *M1*) да није *TTL* механизма Интернет протокола. Овај механизам подразумева одбацивање пакета у тренутку када он направи 255 скокова између рутера. Међутим, овај механизам само ублажује проблем петљи рутирања а њиховим стварањем се непотребно заузимају комуникациони канали преносом пакета података који никада неће стићи до одредишта.

Један од механизама којим ће се горе наведени проблем разрешити јесте тзв. **бесконачно бројање**. Последњи описани корак било је додавање мреже *M1* у табелу рутера *R1* путем рутера *R2* са метриком 3. Овим се, међутим, процес сихнронизације рутера неће завршити, већ ће рутер *R1* о насталој измени обавестити суседне рутере, међу којима и рутер *R2*. Рутер R2 ће на основу ове измене повећати метрику ка мрежи *M1* на вредност 4 и о томе обавестити рутер *R1*. Овај процес ће се понављати док год се не достигне вредност метрике 16, након чега ће се рута прогласити недоступном и избацити из табела рутирања на оба рутера.

Основни механизам протокола информација за рутирање за спречавање стварања петљи рутирања из описаног разлога јесте **подела хоризонта** (енгл. *split horizon*). Овај једноставни механизам подразумева да се руте научене од једног суседа не оглашавају том истом суседу. У једноставним линеарним топологијама, каква је и топологија представљена на слици 1, подела хоризонта

спречава стварања петљи рутирања. Међутим, код сложенијих топологија овакав начин избегавања петљи рутирања није довољан. Из тог разлога се користи нешто сложенији механизам **поделе хоризонта са затрованим повратним рутама** (енгл. *split horizon with poisoned reverse*). Код овог механизма се руте добијене од једног суседа њему повратно оглашавају али са метриком 16. Предност овог механизма је што се петље рутирања уклањају у много краћем временском периоду.



Слика 2. Подела хоризонта није довољна у сложеним топологијама

Код топологије приказане на слици 2. сама подела хоризонта не би спречила стварање петље, односно за њено разрешавање би било потребно много времена. У случају коришћења подељеног хоризонта са затрованим повратним рутама стање конвергенције постиже се у далеко мањем временском периоду. Негативна страна коришћења затрованих повратних рута огледа се у повећању количине саобраћаја самог *RIP* протокола.

3.4.1.1.3. RIPng - протокол информација за рутирање следеће генерације

Протокол информација за рутирање следеће генерације (*Routing Information Protocol next generation, RIPng*) представља варијанту оригиналног *RIP* протокола намењену за коришћење у мрежама адресованим шестом верзијом Интернет протокола. Као и претходне верзије, и *RIPng* је заснован на коришћењу вектора удаљености. Записе у табели рутирања овог протокола чине следећи параметри:

- IPv6 префикс одредишта.
- Метрика која представља укупан трошак за достављање пакета од рутера до одредишне мреже.
- IPv6 адреса суседног рутера као првог посредника у достављању података на одредиште. Овај параметар може бити изостављен уколико

се запис односи на неку од мрежа на које је рутер директно повезан.

- Индикатор да ли је рута мењана у скоријем периоду.
- Различити временски параметри.

С обзиром на то да протокол информација за рутирање следеће генерације ради на апликативном слоју, он користи услуге *UDP* транспортног протокола.

3.5. Остали значајни протоколи мрежног слоја

Последњих пет блокова слободних адреса Интернет протокола четврте верзије расподељено је регионалним регистрима Интернета трећег фебруара 2011. године. То у пракси значи да ће крајњи корисници све теже моћи да добију адресе тог протокола од стране Интернет провајдера, док ће сами Интернет провајдери за даље ширење морати да пређу на шесту верзију Интернет протокола. У складу са тим, **Интернет протокол шесте верзије** треба имати у виду као будући носећи протокол Интернет мреже.

Један од основних недостатака Интернет протокола представља непостојање механизама за контролу и потврду успешности достављања пакета одредишту, односно утврђивања настанка и узрока проблема у комуникацији. За те потребе је развијен посебан **протокол контролних порука Интернета** који надомешћује поменути недостатак самог Интернет протокола, а за који је подршка подразумевано укључена у свим популарним оперативним системима и мрежним уређајима који функционишу на мрежном слоју.

Следећи значајан недостатак Интернет протокола јесте немогућност испоруке једног датаграма на више различитих одредишних адреса. Ово ограничење намеће оптерећивање комуникационих канала вишеструким слањем пакета са идентичним садржајем на слоју апликације. Протокол који нуди решење за наведени проблем јесте **протокол за управљање групама на Интернету** - IGMP.

3.5.1. ICMP - протокол контролних порука Интернета

Сам Интернет протокол функционише без успостављања везе и не поседује механизме за обавештавање извора о неуспешној достави послатих датаграма. Из тог разлога, за потребе информисања пошиљаоца о проблемима при слању датаграма развијено је проширење Интернет протокола у виду засебног протокола. Овај протокол је познат под називом протокол контролних порука Интернета (енгл. *Internet Control Message Protocol*).

Протокол контролних порука Интернета је веома једноставан протокол који

нуди свега неколико функционалности. Поруке овог протокола углавном се односе на грешке у обради датаграма а инкапсулирају се у датаграме Интернет протокола.

У основне типове порука које користи овај протокол спадају поруке везане за следеће грешке запажене у обради датаграма на одредишту или на посредним уређајима. Ове поруке су описане у наставку текста.

```
▷ Frame 9: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▷ Ethernet II, Src: AsustekC_35:07:22 (00:23:54:35:07:22), Dst: Microsof_6e:6b:00 (00:15:5d:6e:6b:00)
▷ Internet Protocol, Src: 192.168.55.238 (192.168.55.238), Dst: 192.168.55.10 (192.168.55.10)
▽ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4fc5 [correct]
    Identifier: 0x2ce5
    Sequence number: 2 (0x0002)
    Sequence number (LE): 512 (0x0200)
  ▽ Data (56 bytes)
      Data: 7136084e0ccc0a0008090a0b0c0d0e0f1011121314151617...
      [Length: 56]
```

Слика 1. Реалан ICMP пакет, забележен помоћу Wireshark алата

Поруке везане за недоступност одредишта (енгл. *Destination Unreachable Messages*) углавном указују на ситуацију у којој један од посредних рутера у својој табели рутирања није успео да пронађе руту ка захтеваној мрежи или на ситуацију у којој је датаграм стигао до одредишне мреже али није успело његово достављање примаоцу. Додатно, поруке овог типа су могуће и у ситуацијама када је фрагментовање датаграма неопходно али је у његовом заглављу фрагментовање забрањено.

Слика 2. Посредник информише пошиљаоца да одредиште није доступно

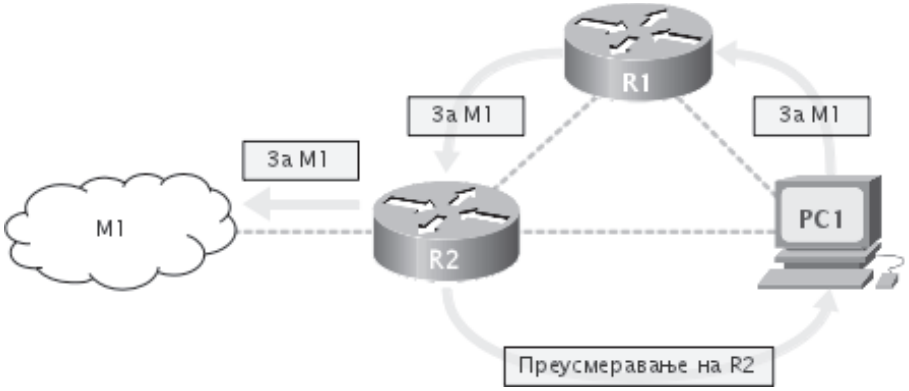
Поруке везане за прекорачено време обраде (енгл. *Time Exceeded Messages*) углавном се односе на прекорачен дозвољен број скокова током преноса (поље *Time to live* у заглављу Интернет протокола, али могу указивати и на прекорачење дозвољеног времена за склапање изворног датаграма у

ситуацијама када је коришћено фрагментовање.

Поруке везане за проблем са одређеним параметром (енгл. *Parameter Problem Messages*) указују на то да неки од посредника није био у могућности да обради неки од додатних параметара заглавља датаграма Интернет протокола. Показивач унутар контролне поруке упућује на октет у заглављу изворног датаграма који је изазвао грешку.

Поруке везане за смањење брзине слања (енгл. *Source Quench Messages*) указују на то да неки од посредника није у стању да обрађује датаграме брзином којом они пристижу, односно да ју је потребно смањити. Ове поруке се шаљу пре достизања загушења са циљем избегавања губљења датаграма услед немогућности прихватања у долазни бафер.

Поруке везане за преусмеравање (енгл. *Redirect Messages*) се користе у случајевима када постоји боља рута ка између посредника и извора поруке.



Слика 3. Преусмеравање пошиљаоца протоколом контролних порука

Ехо поруке са захтевом и одговором (енгл. *Echo and Echo Reply Messages*) служе за проверу могућности комуникације са одредиштем. Прималац ехо поруке дужан је да на њу одговори, осим уколико није другачије подешен из безбедносних разлога. Осим за утврђивање могућности остваривања комуникације са удаљеним рачунаром ове поруке се користе и за мерење времена потребног да датаграм дође до одредишта и одговор се врати назад до извора.

Поруке са временским ознакама (енгл. *Timestamp Messages*) се користе за утврђивање одступања часовника страна које комуницирају. У оквиру ових порука се преносе три типа временских ознака: време на часовнику пошиљаоца, непосредно пре слања, време на часовнику примаоца непосредно након пријема и време на часовнику примаоца непосредно пре слања одговора.

Поруке за добијање информација о мрежи (енгл. *Information Request or Information Reply Messages*) се користе од стране чланова мреже за добијање њене адресе. Поруке овог типа које представљају захтев садрже све нуле као вредности битова у пољима за изворишну и одредишну адресу у заглављу датаграма Интернет протокола.

Протокол контролних порука Интернета омогућава обавештавање извора и посредника о насталим проблемима у комуникацији, али не даје предлоге на који начин се они могу превазићи. Након пријема информације да је дошло до грешке у току преноса, пошиљалац сам доноси одлуку које ће измене применити на процес слања.

Једно од правила везаних за протокол контролних порука Интернета је да се он никада не примењује на себе самог, односно да се никада не шаљу контролне поруке везане за контролне поруке. Разлог за то је избегавање бесконачних петљи које би се у противном могле јавити. Додатно, у случају фрагментовања датаграма Интернет протокола контролне поруке се шаљу само у вези са првим фрагментом.

3.5.1.1. Апликације које користе ICMP

ICMP је у основи системски протокол и није намењен за употребу од стране крајњих корисника. Међутим, коришћење овог протокола може администраторима мрежа знатно олакшати администрирање рачунарских мрежа, првенствено када је у питању дијагностиковање проблема. Два основна корисничка алата за коришћење *ICMP* протокола су *ping* и *traceroute*.

Алат *ping* служи за утврђивање могућности и перформанси комуникације са удаљеним рачунаром. Рад овог алата заснива се на слању *IP/ICMP* датаграма и мерењу времена потребног да се он достави до одредишта, заједно са временом потребним да одредиште пошаље назад одговарајући датаграм.

```
$ ping -c5 192.168.55.10
PING 192.168.55.10 (192.168.55.10) 56(84) bytes of data.
64 bytes from 192.168.55.10: icmp_req=1 ttl=128 time=0.302 ms
64 bytes from 192.168.55.10: icmp_req=2 ttl=128 time=0.366 ms
64 bytes from 192.168.55.10: icmp_req=3 ttl=128 time=0.295 ms
64 bytes from 192.168.55.10: icmp_req=4 ttl=128 time=0.313 ms
64 bytes from 192.168.55.10: icmp_req=5 ttl=128 time=0.487 ms

--- 192.168.55.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.295/0.352/0.487/0.074 ms
```

Листинг 1. Пример коришћења алата *ping*

Коришћењем ping алата могу се једноставно прикупити основни подаци везани за проходност и перформансе комуникационих канала између локалног и удаљеног рачунара. Уколико послати датаграм успе да стигне до одредишта, то углавном представља потврду да је могуће остварити комуникацију протоколима до мрежног слоја а највероватније и протоколима транспортног и апликативног слоја. Са друге стране, немогућност комуникације на овом нивоу обично указује на то да неће бити могуће остварити везу коришћењем протокола на апликативном слоју. Ипак, ово не мора да буде правило с обзиром на то да поруке *ICMP* протокола често одбацују *firewall* посредници због безбедносних разлога.

Осим за проверу везе са удаљеном адресом алат *ping* се може ефикасно користити и за дијагностиковање осталих проблема у мрежи. На пример, уколико се као удаљена адреса наведе симболичка адреса (листинг 2.) аутоматски ће се извршити њено превођење у логичку адресу - адресу Интернет протокола.

```
$ ping www.google.com
PING www.google.com (209.85.148.103) 56(84) bytes of data.
64 bytes from www.google.com (209.85.148.103): icmp_req=1 ttl=53 time=42.8
ms
```

Листинг 2. Коришћење *ping* алата за проверу разрешавања адреса

Следећи значајан случај представља немогућност превођења симболичке у логичку адресу, задате као аргумент *ping* алата (листинг 3.). Најчешћи узрок томе је погрешно унета симболичка адреса, односно непостојећа симболичка адреса, или грешка у раду коришћених *DNS* сервера.

```
$ ping www.google.com
ping: unknown host www.google.com
```

Листинг 3. Коришћење *ping* алата за проверу разрешавања адреса

Алат *traceroute* користи се за утврђивање путање којом пакети путују од изворишне до одредишне адресе, односно од локалног до удаљеног рачунара. Овај алат је нешто сложенији од *ping* алата а њихова заједничка карактеристика је да користе *ICMP* протокол као основу свог рада.

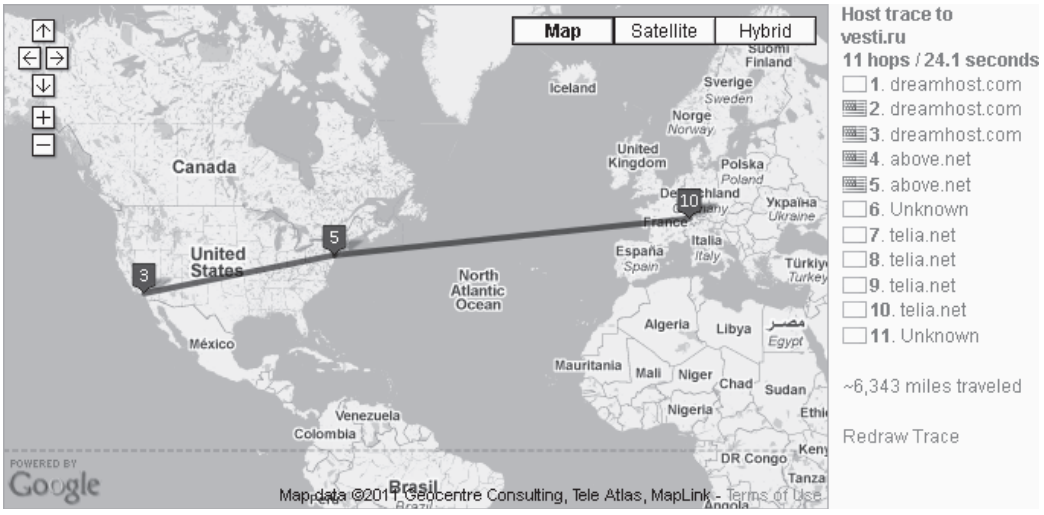
У оквиру листинга 4. дат је пример коришћења конзолног *traceroute* програма за утврђивање руте и посредника између локалног рачунара и сервера на адреси *www.google.com*. На основу резултата извршавања овог програма може се

закључити да између локалног и удаљеног рачунара постоји 6 посредника.

```
$ traceroute www.google.com
traceroute to www.google.com (209.85.148.103), 30 hops max, 60 byte packets
1  192.168.60.12 (192.168.60.12)  0.419 ms  0.813 ms  0.972 ms
2  79-101-159-1.isp.telekom.rs (79.101.159.1)  7.641 ms  9.040 ms  9.957 ms
3  212.200.15.221 (212.200.15.221)  11.424 ms  12.343 ms  13.793 ms
4  212.200.6.238 (212.200.6.238)  14.789 ms  16.188 ms  17.430 ms
5  79.101.106.2 (79.101.106.2)  25.807 ms  26.674 ms  28.063 ms
6  209.85.242.228 (209.85.242.228)  29.042 ms  23.735 ms  13.664 ms
7  72.14.232.102 (72.14.232.102)  30.110 ms  31.517 ms  37.913 ms
8  www.google.com (209.85.148.103)  38.252 ms  39.190 ms  40.196 ms
```

Листинг 4. Пример коришћења *traceroute* алата

Поред основног, конзолног алата за утврђивање руте комуникације између локалног и удаљеног рачунара постоје и графички алати ове намене. Ови алати су допуњени функцијама за коришћење *GeoIP* сервиса и у њима се добијене адресе посредника преводе у њихове приближне географске координате, тако да се целокупна путања комуникације графички представља на карти света.



Слика 1. Пример коришћења traceroute алата са графичким интерфејсом

Још један значајан софтверски алат чији се велики број функција ослања на коришћење *ICMP* протокола јесте мрежни мапер *Nmap*. Овај алат се користи за откривање активних чланова мреже, утврђивање типа и верзије оперативног система удаљеног рачунара, скенирање отворених портова, итд. Овај алат се у пракси веома често користи од стране мрежних администратора.

```
# nmap -O 192.168.1.1

Starting Nmap 5.51 ( http://nmap.org ) at 2011-06-25 09:20 CEST
Nmap scan report for 192.168.1.1
Host is up (0.0028s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
80/tcp open  http
MAC Address: 00:1E:E3:7A:98:B7 (T&W Electronics (ShenZhen) Co.)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.13 - 2.6.31
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.81 seconds
```

Листинг 5. Пример коришћења *nmap* алата за утврђивање отворених портова и оперативног система на удаљеном рачунару

Поред наведених постоји и велики број других софтверских алата чији се рад у мањој или већој мери заснива на коришћењу *ICMP* протокола за потребе утврђивања стања комуникационих канала и удаљених рачунара.

3.5.1.2. Злоупотреба ICMP протокола

ICMP протокол представља одличну основу за проверу рада рачунарске мреже, доступности удаљених рачунара, актуелних рута, перформанси и т.д. Међутим, веома често је у пракси скуп функционалности које овај протокол може да понуди намерно ограничен из безбедносних разлога. Два основна типа безбедносних проблема везаних за овај протокол су:

1. *ICMP* протокол се може злоупотребити за прикупљање података неопходних за извршавање напада на удаљени рачунар или рачунарску мрежу;
2. *ICMP* протокол се може злоупотребити за онемогућавање нормалног рада удаљених рачунара и комуникационих канала;

Са тачке гледишта нападача *ICMP* протокол представља драгоцен алат за прикупљање података о удаљеном рачунару или рачунарској мрежи. У оквиру листинга 1. дат је пример коришћења *ICMP* протокола за утврђивање које адресе мреже 192.168.1.0/24 су заузете од стране чланова. За потребе овог скенирања коришћен је алат nmap, скенирање 256 адреса је укупно трајало око

3 секунде, а њиме је утврђено да се на адресама 192.168.1.12, 192.168.1.15 и 192.168.1.20 налазе активни чланови. Информацију о заузетим адресама нападач може искористити на различите начине - даља анализа њихових карактеристика, заузимање неке од слободних адреса, преотимање неке од заузетих адреса и т.д.

```
$ nmap -sP 192.168.1.*
Starting Nmap 5.51 ( http://nmap.org ) at 2011-06-24 11:00 CEST
Nmap scan report for 192.168.1.12
Host is up (0.0020s latency).
Nmap scan report for 192.168.1.15
Host is up (0.00079s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.07 seconds
```

Листинг 1. Пример коришћења *nmap*-а за откривање активних чланова мреже

У оквиру листинга 2. приказана је злоупотреба *ICMP* протокола у циљу онемогућавања нормалног рада удаљеног рачунара. У односу на подразумевано коришћење *ping* алата уведене су следеће измене: 1) укључен је режим преплављивања (опција *-f*) у коме се је избегнута пауза од 1 секунде између слања пакета; 2) подразумевана величина пакета од 64 бајта повећана је на највећу могућу вредност од 65.535 бајтова; 3) захтевано је слање 10.000 пакета задате величине. Наведене измене су начињене у циљу онемогућавања нормалног рада удаљеног рачунара путем оптерећивања његовог комуникационог канала и централног процесора.

Статистика дата на крају листинга 2. показује да на послатих 10.000 захтева одредишни рачунар није успео да одговори на њих 4.736, а да је цео процес трајао 147,658 секунди. У том периоду слање података је вршено брзином од 33,5Mb/s, а пријем брзином од 17,8Mb/s. Губитак 47 процената пакета, односно разлика од 15,7Mb/s између просечних брзина слања и пријема пакета, последица је превеликог оптерећења неког сегмента комуникационог канала између пошиљаоца и примаоца, или је у питању ограничење капацитетом централног процесора примаоца.

```
# ping -f -s 65507 -c 10000 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 65507(65535) bytes of data.
.....................................................................
.........................................................
--- 192.168.1.12 ping statistics ---
10000 packets transmitted, 5264 received, 47% packet loss, time 147658ms
rtt min/avg/max/mdev = 36.779/578.688/882.137/124.448 ms, pipe 63, ipg/ewma
14.767/433.750 ms
```

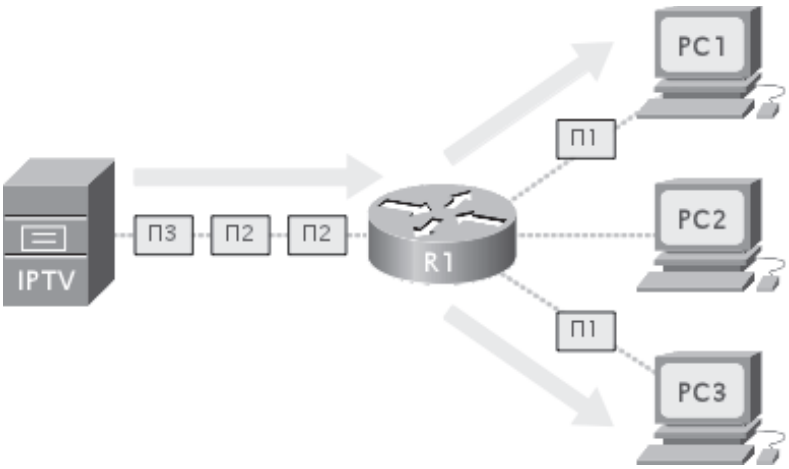
Листинг 2. Коришћење *ping* алата за преплављивање одредишта

У сваком случају, очекивана последица овог напада на удаљени рачунар јесте отежана или потпуно онемогућена његова комуникација са осталим рачунарима у мрежи. Овај тип напада спада у категорију напада чији је циљ ускраћивање услуге (енгл. *denial of service*) а често се извршава и у дистрибуираној варијанти у којој се већи број рачунара користи на описани начин за напад на један рачунар или комуникациони канал.

3.5.2. IGMP - протокол за управљање групама на Интернету

Два најједноставнија начина слања података у рачунарским мрежама јесу слање појединачном примаоцу (енгл. *unicast*) и емисионо слање (енгл. *broadcast*). Ови начини слања су подржани у самом Интернет протоколу, као и у популарним технологијама на слоју везе података (Етернет технологија на пример). Сам Интернет протокол не дозвољава постојање више од једне одредишне адресе у заглављу пакета.

Постоје, међутим, ситуације у којима је потребно исту поруку доставити вишеструким, али не и свим члановима локалне мреже као и ситуације у којима се примаоци не налазе унутар једне исте мреже. У таквим ситуацијама потребно је користити систем за слање једне поруке вишеструким примаоцима (енгл. *multicast*), на нивоу мрежног протокола. Такав систем за потребе Интернет протокола обезбеђује **протокол за управљање групама на Интернету** (енгл. *Internet Group Management Protocol, IGMP*).



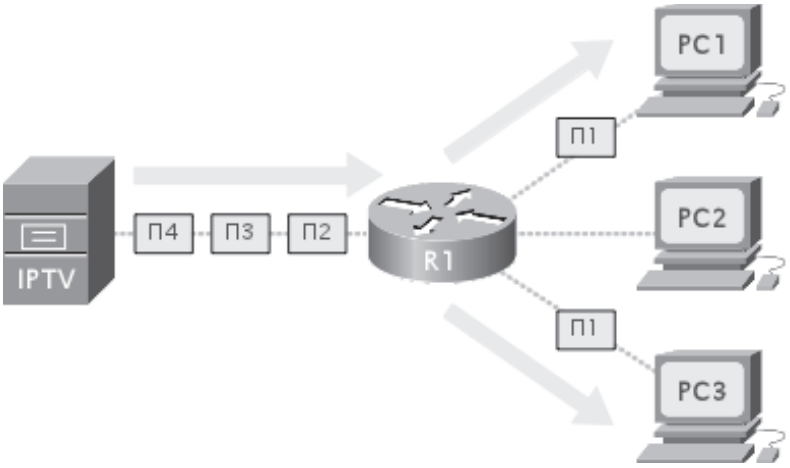
Слика 1. Вишеструка испорука поновљеним слањем

Поједностављено гледано, функцију слања једне исте поруке вишеструким примаоцима могуће је постићи и вишеструким слањем те поруке, у свакој

итерацији адресованом за наредног примаоца (слика 1.).

Наведени приступ, међутим, поседује значајна ограничења. Његов основни недостатак односи се на вишеструко оптерећење пошиљаоца и посредујућих комуникационих канала и уређаја. Довољно је за пример узети ситуацију у којој сервер видео-стриминга опслужује неколико стотина клијената, па да се одмах увиди немогућност постизања жељеног резултата вишеструким слањем услед ограничења пропусном моћи првих сегмената комуникационог канала.

Коришћењем Интернет протокола за управљање групама могуће је решавање описаног проблема на такав начин да се један комуникациони канал никада не оптерети више пута једном истом поруком. Кључну улогу у овом решењу играју рутери са подршком за протокол за управљање групама на Интернету и *D* класа адреса четврте верзије Интернет протокола.



Слика 2. Вишеструка испорука адресовањем на вишеструке примаоце

Две основне улоге код протокола за управљање групама на Интернету јесу улога члана групе и улога рутера који подржава овај протокол. Обавезе члана укључују управљање својим чланством у одређеној групи. Насупрот томе, задатак рутера са подршком за овај протокол је да ажурира информације о активним групама и њиховим члановима у локалној мрежи и да посредује између њих и извора саобраћаја.

Рад протокола за управљање групама на Интернету заснован је на коришћењу три типа порука:

1. поруке са захтевом учлањивања у одређену групу,
2. поруке са потврђивањем чланства у одређеној групи и

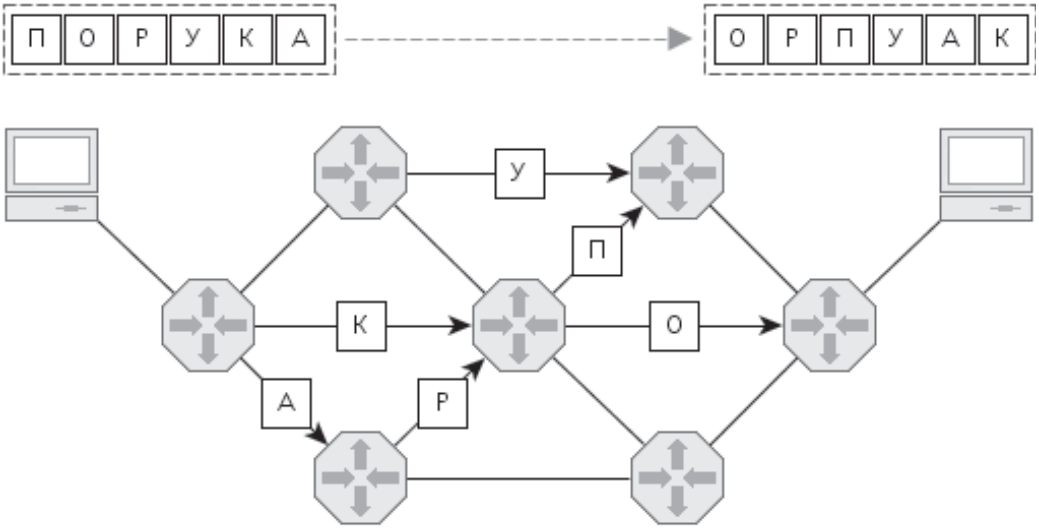
3. поруке са информацијом о изласку из одређене групе (у претходним верзијама).

Поруке протокола за управљање групама на Интернету се инкапсулирају у поруке Интернет протокола. С обзиром на вредност параметра *TTL* један, ове поруке служе за комуникацију унутар локалне мреже. Тренутно актуелна верзија протокола за управљање групама на Интернету је три а она нуди одређени ниво компатибилности и са претходним верзијама.

4. Транспорт података

Нижи комуникациони слојеви имају за задатак да омогуће комуникацију између чланова једне рачунарске мреже, као и између чланова више рачунарских мрежа које су међусобно повезане. Технологије и протоколи на овим слојевима омогућавају усмеравање и пренос послатих података до одредишта. Њихов задатак, међутим, није и брига о интегритету података који се преносе, као ни гарантована испорука у неизмењеном облику. Ове функционалности спадају у домен задатака протокола на транспортном слоју.

Оно што се на нивоу међумрежног повезивања или самог приступа мрежи може сматрати успешном комуникацијом не мора задовољавати комуникационе потребе корисничких сервиса. Са аспекта корисничког мрежног сервиса могу се јавити различити проблеми у комуникацији: оштећење послатих података, немогућност испоруке делова садржаја, испорука садржаја у измењеном редоследу његових сегмената, затрпавање одредишта превеликом количином података и слично. Решавање наведених проблема, односно брига о успешном преносу података корисничких сервиса, представља основни задатак протокола транспортног слоја а уједно и разлог његовог постојања.



Слика 1. Испорука пакета у измењеном редоследу

Сви телекомуникациони сервиси засновани на рачунарским мрежама могу се, у зависности од критичне карактеристике преноса података, сврстати у две основне категорије:

1. сервиси код којих је критично важан пренос без грешака и
2. сервиси код којих је критично важно мало кашњење.

Као пример сервиса код којих је критично важно да примљени подаци буду идентични послатим, односно да током преноса не дође до грешке, јесте електронско банкарство. Сама брзина преноса података и кашњење код овог сервиса су у другом плану. Другим речима, далеко ја важније да се по налогу клијента изврши трансфер са **исправним** износом, на **исправан** рачун, од тога да се захтев клијента до сервера банке пренесе за 2 или 3 секунде краће време.

Насупрот сервисима код којих је критично важан пренос без грешака стоје сервиси код којих је критично важна брзина преноса података, односно што мање кашњење. Као пример овог типа сервиса могу се узети видео-конференције. Наиме, код такве услуге много је значајније да се подаци преузети са улазних уређаја (видео-камере и микрофона) пошиљаоца што пре доставе излазним уређајима (монитору и звучницима) примаоца. Уколико се у томе не успе, односно уколико се јави кашњење веће од неколико десетих делова секунде, коришћење сервиса ће бити знатно отежано или потпуно немогуће. Оштећења пренешених података, манифестована у виду краткотрајних замућења слике или звука, у овом случају су далеко прихватљивија.

Критично важан пренос без грешака	Критично важно мало кашњење
- Електронско банкарство - Пренос фајлова - Веб - Електронска пошта	- Видео-конференције - IP телефонија - Стримовање видео садржаја - Рачунарске игре

Табела 1. Примери сервиса са критичним карактеристикама преноса

За потребе преноса података осетљивих на грешке најчешће се користи **протокол за контролу преноса** (енгл. *Transmission Control Protocol, TCP*). За потребе преноса података осетљивих на кашњење најчешће се користи **протокол корисничких датаграма** (енгл. *User Datagram Protocol*).

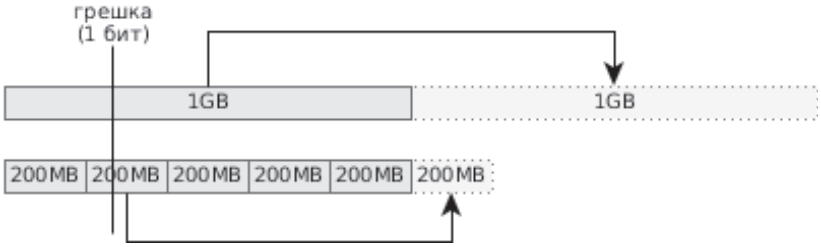
4.1. Сегментација података

Једна од основних функција транспортног слоја је **сегментација података**. Сегментација података подразумева поделу података које треба пренети на мање делове (сегменте) који ће се преносити појединачно. Сегментација је неопходан процес с обзиром да рачунарске мреже користе пакетски пренос података.

Дужине (величине) сегмената варирају из више разлога. Као прво, с обзиром на то да се сегменти састоје од два дела - заглавља и података - дужина сегмента зависи од дужине заглавља, односно од транспортног протокола који се користи. Уколико је у употреби TCP протокол, дужина заглавља сегмента ће бити 20 или више бајтова. Са друге стране, UDP протокол има фиксно заглавље дужине 8 бајтова.

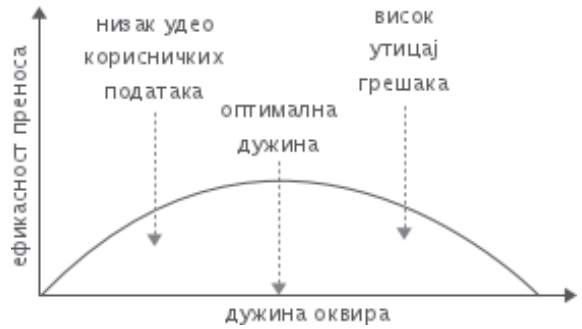
Слика 1. Дужина сегмента одређује удео корисничких података

Имајући у виду готово фиксну дужину заглавља сегмената, јасно је да ће код веће дужине сегмената удео корисничких података бити мањи, односно да ће практична искоришћеност комуникационог канала бити мања. У случају идеалне инфраструктуре, највећа искоришћеност би била код целокупног преноса у једном сегменту.



Слика 2. Превелики пакети умањују ефикасност преноса код грешака

Са друге стране, код преноса са понављањем у случају грешке, употреба већих сегмената даје лошије резултате јер је потребно поновити слање велике количине података, често због свега неколико битова. Дакле, оптимална величина сегмента зависи од више фактора.

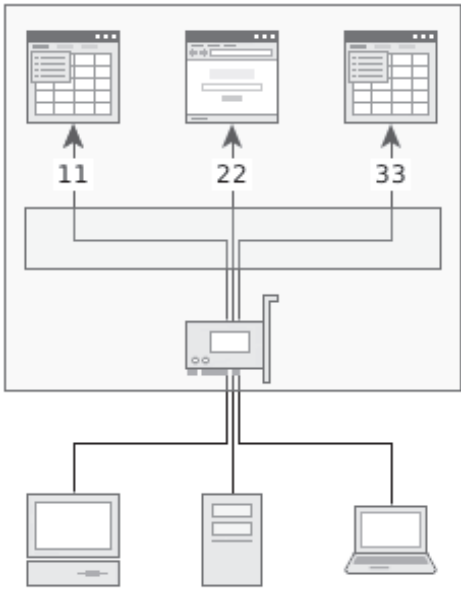


Слика 3. Оптимална величина сегмента

Још једна ствар која има утицај на величину сегмента је и то да ли су подаци унапред спремни за слање или тек пристижу. На пример, када се преко рачунарске мреже преноси велики фајл, његов садржај је у потпуности познат пошиљаоцу пре почетка слања. Са друге стране, код видео-конференције, подаци које треба послати пристижу из микрофона и камере одређеном брзином. Да би се смањило кашњење, транспортни слој шаље сегменте периодично, без обзира да ли су максимално попуњени или не.

4.2. Портови и утичнице

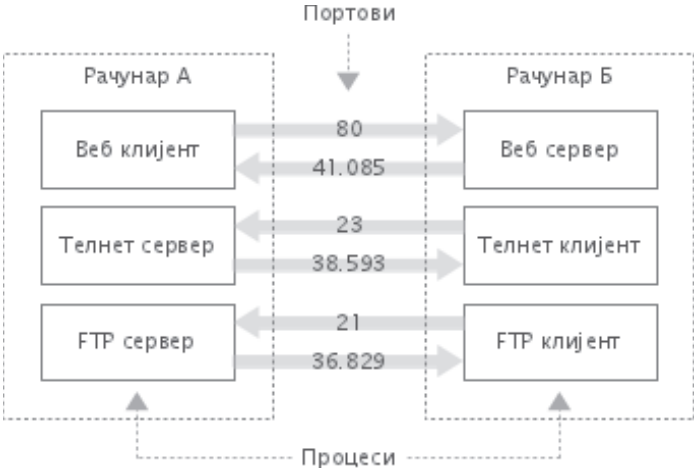
Иако је адресовање подразумевана улога мрежног слоја, транспортни слој поседује интерни систем адресовања чија је адресна јединица порт. Порт је одређен 16-битним нумеричким параметром и његова је улога да одреди изворни/одредишни ентитет апликативног слоја (апликацију) од кога потичу подаци, односно коме треба испоручити податке.



Слика 1. Портовима се одређује којој апликацији проследити податке

Портови се могу поделити на привилеговане, регистроване и динамичке (или краткотрајне). Привилеговани портови се налазе у опсегу бројева од 0 до 1023 и право на њихово отварање углавном има само оперативни систем или процеси које је покренуо администратор система. На привилегованим портовима се налазе најчешће коришћени сервиси (*FTP, SSH, Telnet, DNS* и други). Регистровани портови се крећу у опсегу од 1024 до 49151 и на њима се

подразумевано користе сервиси новијег датума. Динамички или краткотрајни портови крећу се у опсегу од 49152 до 65535 и њих није могуће регистровати а углавном служе за клијентске компоненте клијент/сервер софтвера.



Слика 2. Портовима се подаци усмеравају на процесе

Појам и функционалност утичница (енгл. *socket*) први пут се појављују у верзији 4.2 *BSD UNIX* оперативног система, а данас су оне де факто стандард за све популарне оперативне системе који подржавају мрежне функционалности. Утичнице представљају композитне адресне јединице на нивоу транспортног и мрежног слоја. Саставни делови утичница су:

1. *IP* адреса изворишта
2. Порт изворишта
3. Протокол транспортног слоја
4. Порт одредишта
5. *IP* адреса одредишта

Подршка за утичнице у оперативним системима најчешће се реализује помоћу готових системских библиотека. Неке од најпопуларнијих библиотека овог типа су *Berkeley socket* за *UNIX* оперативне системе и *Winsock* за оперативне системе компаније Мајкрософт.

Осим употребе у рачунарским мрежама утичнице се могу користити и код апликација које се извршавају на локалном рачунару. На пример, *X Window System* графички систем на *UNIX* платформи захтева коришћење утичница да би функционисао.

Слика 3. Утичница је сачињена од IP адресе и порта

4.3. Протокол за контролу преноса

Протокол за контролу преноса (енгл. *Transmission Control Protocol, TCP*) један је од најважнијих протокола, како на транспортном слоју, тако и у рачунарским мрежама уопште. Овај протокол обезбеђује поуздан пренос података и отпоран је на грешке које се могу јавити током преноса.

Слика 1. Структура сегмената протокола за контролу преноса

Функције које нуди протокол за контролу преноса су управљање везом, откривање грешака, исправљање грешака поновним преносом оштећених сегмената и прилагођавање брзине преноса могућностима комуникационог канала и примаоца.

4.3.1. Управљање везом

Протокол за контролу преноса је протокол који користи виртуалну везу за пренос података. То значи да станице које размењују податке пре размене успостављају везу, а након размене ту везу раскидају. Веза се успоставља и раскида у оба смера, односно за сваки смер преноса се успоставља и раскида независна веза.

Слика 2. Успостављање и раскид везе се обавља у три корака

Да би се успоставила или раскинула веза у једном смеру потребно је пренети два сегмента - један којим се захтева успостава везе (сегмент са укљученом SYN, односно FIN заставицом у заглављу) и један којим се тај захтев одобрава (ACK заставица). Пошто се веза готово увек успоставља и раскида у оба смера, наведени процес је оптимизован на такав начин да се потврда првог захтева и други захтев обједињују у један сегмент, односно цео процес се завршава преко три уместо четири сегмента. Овај процес се назива и *Three-Way Handshake*.

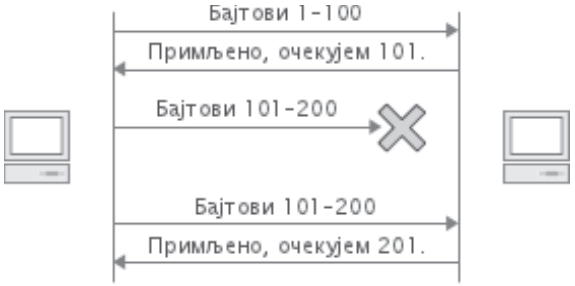
Осим регуларно, захтевом, веза TCP протокола се може раскинути и услед неактивности у одређеном периоду. Додатно, постоји и временско ограничење у ком друга страна мора да одговори на захтев за успостављање/раскид везе. Овај период се разликује на различитим оперативним системима, а на Линуксу износи 20 секунди.

4.3.2. Управљање грешкама

Једна од основних особина протокола за контролу преноса је његова могућност да отклони грешке које су се јавиле током преноса. Ове грешке се могу јавити из различитих разлога и у различитим облицима: оштећени сегменти, изгубљени сегменти, вишеструко примљени сегменти и сегменти примљени у другачијем редоследу. Протокол за контролу преноса поседује потребне механизме да исправи све наведене грешке.

Први механизам заштите од грешака код протокола за контролу преноса заснива се на потврђивању пријема сегмента. Дакле, пошиљалац за сваки

послати сегмент захтева потврду да је он примљен без грешака. Уколико у одређеном временском року не добије такву потврду, пошиљалац ће поново послати исти сегмент.



Слика 3. За послате сегменте се захтева потврда пријема

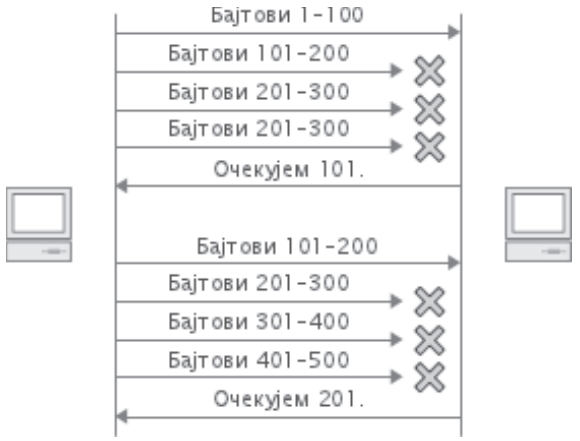
Прималац неће послати потврду о пријему уколико сегмент није добио, нити уколико је сегмент оштећен (што се утврђује упоређивањем контролне суме израчунате на одредишту са контролном сумом израчунатом на страни пошиљаоца и послатом у оквиру заглавља сегмента).

Оно што се може десити је да потврда пријема касно стигне до пошиљаоца сегмента, те да он поново пошаље исти сегмент, односно сегмент који је већ успешно примљен. Такви, вишеструко примљени сегменти се лако откривају и одбацују с обзиром на то да су сви сегменти нумерисани у редоследу којим су послати. Додатно, нумерисање сегмената омогућава и да се исправи евентуално нарушен редослед пријема, што је могуће с обзиром на то да сегменти у сложеним мрежама могу путовати различитим путањама.

4.3.3. Управљање загушењем

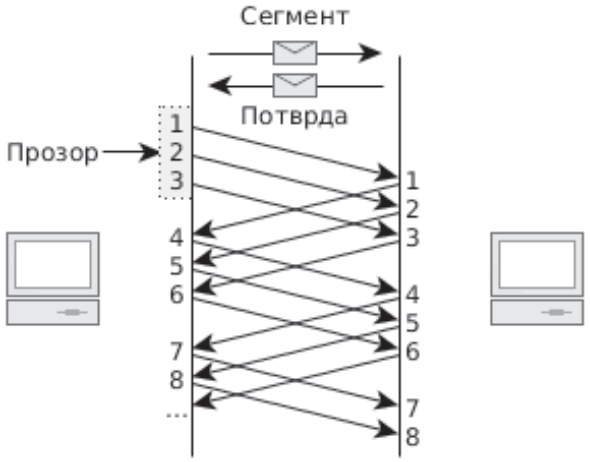
Још једна важна карактеристика протокола за контролу преноса је та да он прилагођава брзину слања података актуелним могућностима примаоца и стању на комуникационом каналу. На пример, уколико рачунар најновије генерације шаље пуном брзином податке рачунару старом десетак година, лако се може десити да пријемник успе да обради свега неколико посто примљених података а да остале, услед превеликог оптерећења, одбаци.

Други разлог за промену могуће брзине слања може се јавити због оптерећења на комуникационим каналима који се користе. На пример, уколико један рачунар са Интернета преузима три фајла истовремено, путем везе капацитета 10Mb/s, сваки од фајлова ће се преносити брзином од 3,3Mb/s. Уколико се преузимање једног фајла заврши, постаје могуће подићи брзину преноса за преостала два фајла на 5Mb/s.



Слика 1. Прималац нема могућност да обради све пристигле сегменте

Протокол за контролу преноса поседује наменски механизам за прилагођавање брзине слања актуелном стању везе и капацитету примаоца. Овај механизам се назива клизним прозором (енгл. *sliding window*).



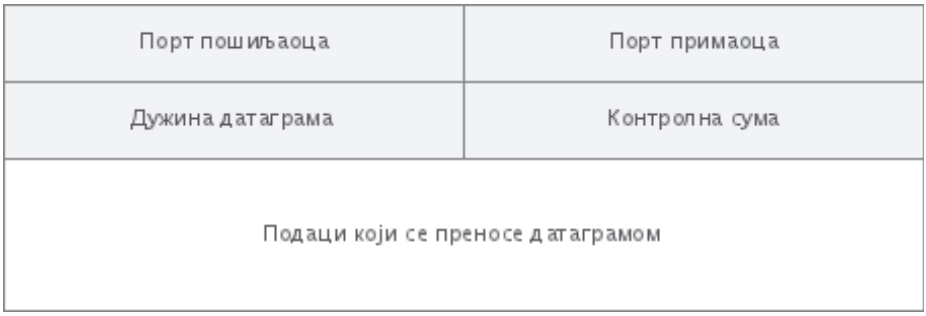
Слика 2. Број послатих сегмената за које није добијена потврда

Механизам клизног прозора функционише тако што се ограничава број сегмената који могу бити послати док није добијена потврда да је претходно послати сегмент успешно примљен. Уколико је величина прозора 1, то значи да ће се наредни сегмент слати тек након добијања потврде да је његов претходник успешно примљен. Такво понашање, међутим, доводи до неоптималног коришћења комуникационог канала, посебно у случајевима са великим бројем посредујућих уређаја.

Оно што је посебно важно је то да је величина прозора динамична величина, односно њена вредност се мења у складу са актуелним процентом поновно послатих сегмената. Дакле, уколико се сегменти успешно достављају и нема потребе за поновним слањем, пошиљалац ће покушати да повећа величину прозора (наравно, уколико са његове стране има простора за то). И супротно, уколико се утврди велики број оквира које је потребно поново слати, пошиљалац ће смањити величину прозора.

4.4. Протокол корисничких датаграма

Протокол корисничких датаграма (енгл. *User Datagram Protocol, UDP*) поред протокола за контролу преноса, представља један од најчешће коришћених транспортних протокола Интернета и локалних рачунарских мрежа. Насупрот протоколу за контролу преноса, протокол корисничких датаграма не омогућава поуздан пренос података путем остваривања виртуелне везе, контроле грешака, контроле редоследа сегмената и не прилагођава брзину слања података пријемној моћи одредишта. Недостатак ових функционалности чини протокол корисничких датаграма једноставнијим протокола за контролу преноса, али и протоколом који не гарантује поуздан пренос података.



Слика 1. Структура датаграма протокола корисничких датаграма

Међутим, намена протокола корисничких датаграма није поуздан пренос података, већ пренос са што мањим временским неслагањима између генерисања података на страни извориштa и пријема података на одредишту. Главне примене овог протокола су код проточног преноса гласа и видео материјала (Интернет телефонија, видео конференције, рачунарске игрице и слично). Предност протокола корисничких датаграма у односу на протокол за контролу преноса је могућност емисионог слања података, односно истовременог слања података свим члановима мреже. Јединица за пренос података протокола корисничких датаграма је датаграм. Структура датаграма овог протокола је знатно једноставнија од структуре сегмената протокола за

контролу преноса јер је у њима изостављена већина контролних информација.

Недостатак контролних информација чини *UDP* протокол знатно ефикаснијим у смислу мањег оптерећења комуникационог канала контролним подацима и мањег оптерећења примаоца датаграма у смислу његове једноставније обраде.

Сва поља у заглављу датаграма *UDP* протокола имају дужину од 16 битова а у њих спадају:

- Број порта на изворишту (енгл. *Source port number*) - одређује порт преко кога се комуникација врши на страни пошиљаоца.
- Број порта на одредишту (енгл. *Destination port number*) - одређује порт преко кога се комуникација врши на страни примаца.
- Дужина (енгл. *Length*) - битска дужина података које датаграм носи.
- Контролна сума (енгл. *Checksum*) - контролна сума заглавља и пакета.

Датаграми код којих се, на основу контролне суме, утврди оштећење током преноса, одбацују се. Неотпорност *UDP* протокола на вишеструко достављање истих датаграма или губитак података, достављање података у измењеном редоследу и слично могуће је надоместити функционалностима у апликативном слоју. Неке апликације које користе *UDP* протокол примењују овакав приступ (на пример *TFTP* сервис). Међутим, коришћењем *UDP* протокола апликације угавном очекују максималне перформансе преноса без обзира на грешке и додатни системи за исправљање грешака би угрозили нормалан рад поменутих апликација.

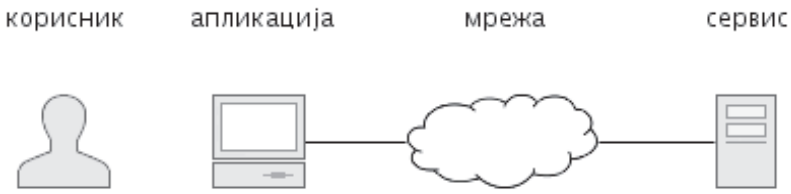
5. Корисничке апликације и сервиси

Целокупан комуникациони модел Интернет мреже је развијен са циљем да омогући функционисање корисничких сервиса. Задатак слоја за приступ мрежи је да омогући коришћење различитих телекомуникационих технологија на инфраструктурном нивоу, задатак међумрежног слоја да кроз одговарајући систем адресовања омогући проналажење удаљеног одредишта, задатак транспортног слоја да брине о испоруци података, а све у циљу несметаног коришћења мреже од стране корисника.

Са аспекта корисничког сервиса, односно компоненте на слоју апликације, она (компонента) се кроз захтев транспортном слоју (оперативном систему) за отварање сокета, директно обраћа компоненти на слоју апликације друге стране. Нижи слојеви омогућавају пренос података између две стране а протокол апликације брине о остваривању сервиса за корисника.

Слика 1. Апликације представљају интерфејс између корисника и мреже

Кориснички сервиси се по *OSI* и *TCP/IP* комуникационим моделима реализују на највишем слоју, слоју апликације. Овај слој је најближи кориснику и у виду апликације чини интерфејс корисника ка рачунарској мрежи. Апликације представљају облик реализације софтвера намењен за непосредно коришћење од стране корисника. У складу са тим апликације поседују одговарајући (графички, алфа-нумерички или неки други) кориснички интерфејс.



Слика 2. Клијентске апликације често размењују податке са сервисима

Сервиси, насупрот апликацијама, представљају реализацију код које се софтверски процеси извршавају „у позадини“ рачунарског система, односно не поседују кориснички интерфејс. Корисник се о овим процесима може

информисати само посредно (на пример, коришћењем наредбе *top* на Линукс оперативном систему) а њихова улога јесте подршка осталим софтверским процесима на локалном или удаљеним рачунарима. На пример, Веб сервис подразумева постојање корисничке апликације (Веб браузер) и серверског софтвера (Веб сервер).

Популарно име за сервисе на *UNIX* оперативним системима је **демони** (енгл. *daemon*). Овај термин се у рачунарству први пут појавио 1963. године, а употребили су га учесници на пројекту *MAC* компаније *IBM*. Као инспирацију за увођење овог термина учесници пројекта наводе Максвелове демоне из области физике и термодинамике. Називи сервисних процеса на *UNIX* системима се најчешће завршавају словом *d,* на пример *httpd*, *mysqld*...

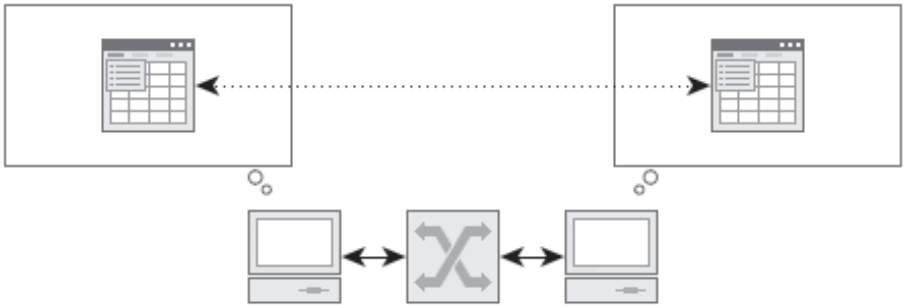
```
$ ps -A
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME CMD
...
root      2146  0.0  0.0   6060  1484 ?        Ss   Jun19   0:11 cupsd
root      2151  0.0  0.0   2076   416 ?        Ss   Jun19   0:00 crond
root      2175  0.0  0.0   2840   184 ?        S    Jun19   0:00 mysqld
root      2325  0.0  0.0  64836   564 ?        Ss   Jun19   0:13 httpd
...
```

Листинг 1. Сервисни процеси као извод из листе активних процеса

У пракси се често инфицирајући део „тројанских коња“ (тип малициозног софтвера) реализује у виду сервиса који од клијентске компоненте - апликације коју користи нападач - добија инструкције. *Rootkit* алати на *UNIX* оперативном систему пример су наведеног софтвера а тешко се откривају јер се на специфичан начин скривају од системских алата за листање активних процеса.

5.1. Мрежно програмирање

Различити механизми за међупроцесну комуникацију (дељена меморија, фајлови и сл.) омогућавају да одвојени процеси на истом рачунарском систему комуницирају, односно размењују податке. Међутим, када се процеси налазе на удаљеним рачунарским системима, омогућавање комуникације између њих је знатно сложеније и захтева коришћење мрежних протокола и физичке инфраструктуре. Са тог аспекта се целокупна рачунарско-телекомуникациона инфраструктура може гледати као подршка комуникацији између процеса који се налазе на различитим рачунарима.



Слика 1. Рачунарска мрежа омогућава комуникацију између удаљених процеса

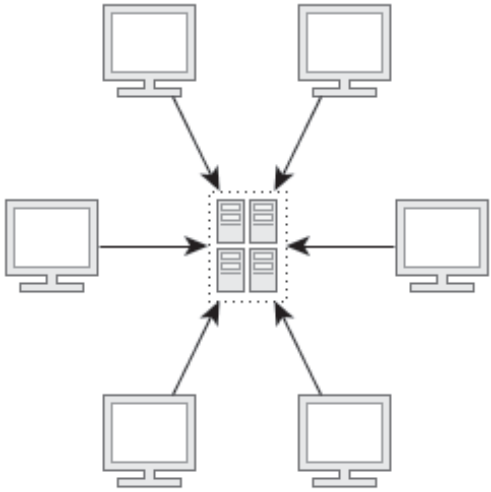
Савремени оперативни системи најчешће одрађују сав посао везан за коришћење протокола на транспортном и нижим комуникационим слојевима, па се мрежно програмирање своди на избор одговарајуће софтверске архитектуре и развој протокола на слоју апликације уз коришћења услуга повезивања које нуди оперативни систем - тзв. програмирање сокета (енгл. *socket programming*). Додатно, Веб програмирање, као један од данас најпопуларнијих облика реализације мрежног софтвера, омогућава коришћење већ постојећих протокола на слоју апликације (*HTTP*, *HTTPS*, *SOAP*...) што знатно поједностављује и убрзава развој мрежног софтвера.

5.1.1. Софтверске архитектуре

Софтверске архитектуре дефинишу на који начин се организују функције софтвера за дистрибуирану обраду података. За потребе одговарања на различите потребе корисника рачунарских мрежа развијено је више софтверских архитектура које пружају одговарајуће функционалности.

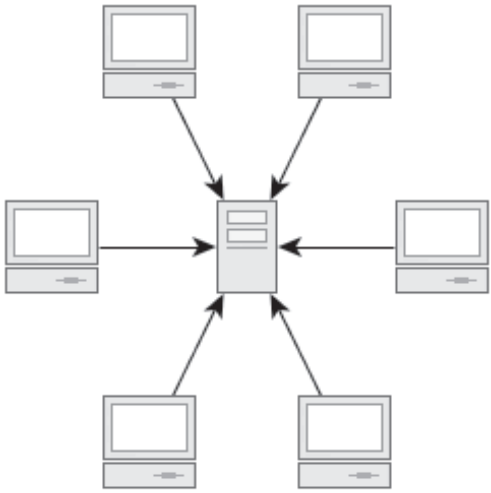
Прва мрежна сотфверско-хардверска архитектура јесте тзв. *host-based* архитектура коју су чинили мејн-фрејм рачунари и на њих прикључени терминали. Код ове архитектуре је целокупну обраду података извршавао мејн-фрејм рачунар а терминали су чинили интерфејс између мејн-фрејм рачунара и крајњих корисника. Данас одређени елементи ове архитектуре постају поново актуелни кроз Веб апликације и оперативне системе, као и рачунарство у облаку (енгл. *cloud computing*).

Вероватно најпопуларнија мрежна софтверска архитектура данас јесте клијент-сервер архитектура. Ова архитектура представља корак од мејн-фрејм архитектуре ка обради података на клијентима, али са одређеном централизованом обрадом на серверу.



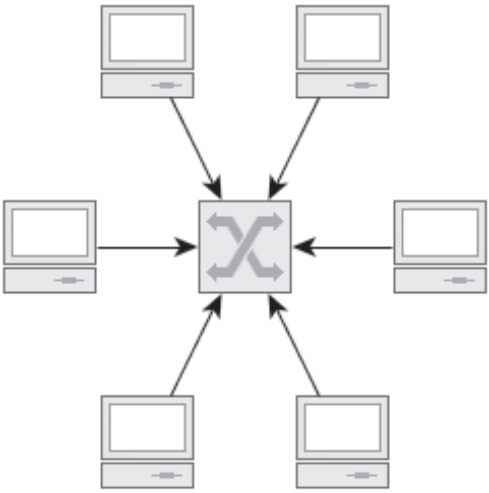
Слика 1. Топологија мејн-фрејм архитектуре

Оваквим приступом је омогућено растерећивање сервера кроз измештање одређених функција на клијенте, уз задржавање могућности централизовања одређених функција за потребе безбедности и стабилности система. Реализација ове архитектуре подразумева постојање упарених софтверских компонената - клијентске и серверске. Клијент-сервер архитектура може бити реализована у два или више слојева.



Слика 2. Топологија клијент-сервер архитектуре

Архитектура равноправних чланова (енгл. *peer-to-peer*) је софтверска архитектура са највишим нивоом аутономије у дистрибурираној обради података. Код ове архитектуре нема хијерархијске поделе чланова, већ сви чланови обављају локалну обраду података, уз могућност обраћања осталим члановима за функције и ресурсе који нису локално доступни. Основни недостатак архитектуре равноправних чланова односи се на отежану администрацију и контролу чланова.



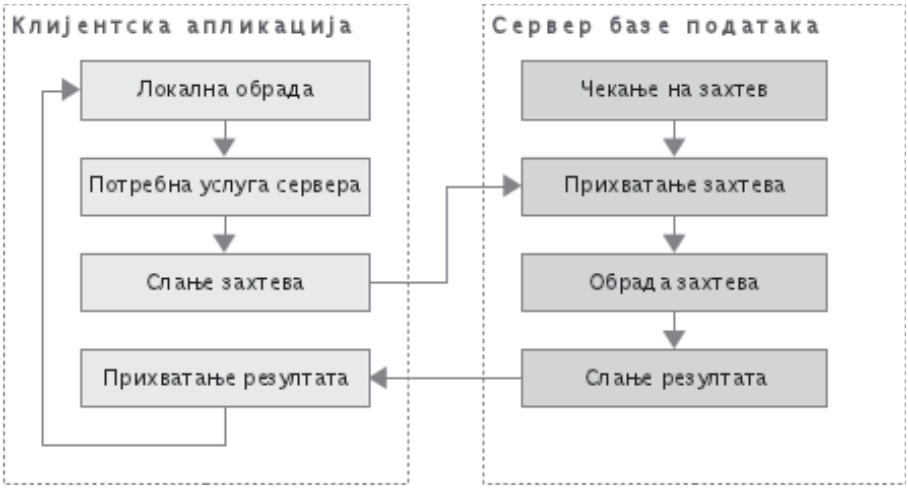
Слика 3. Топологија архитектуре равноправних чланова

Сервисно оријентисана архитектура један је од савремених приступа у дистрибуираном рачунарству. Основна идеја код ове архитектуре јесте омогућавање лакшег развоја и одржавања информационих система кроз мрежно коришћење софтверских функција доступних на осталим рачунарима. Данас постоји велики број затворених и отворених технологија којима се реализују системи засновани на овој архитектури.

5.1.1.1. Клијент-сервер архитектура

Клијент-сервер архитектура представља један од данас најчешће коришћених приступа код дистрибуиране обраде података. Корени ове архитектуре налазе се код мејн-фрејм рачунара и на њих прикључених терминала. Сличност са мејн-фрејм архитектуром јесте постојање једног члана способног за извршавање задатака који су ван могућности осталих чланова мреже. Постоје, међутим, битне разлике између ове две архитектуре. Код мејн-фрејм архитектуре терминали немају никакву могућност обраде података, док код клијент-сервер

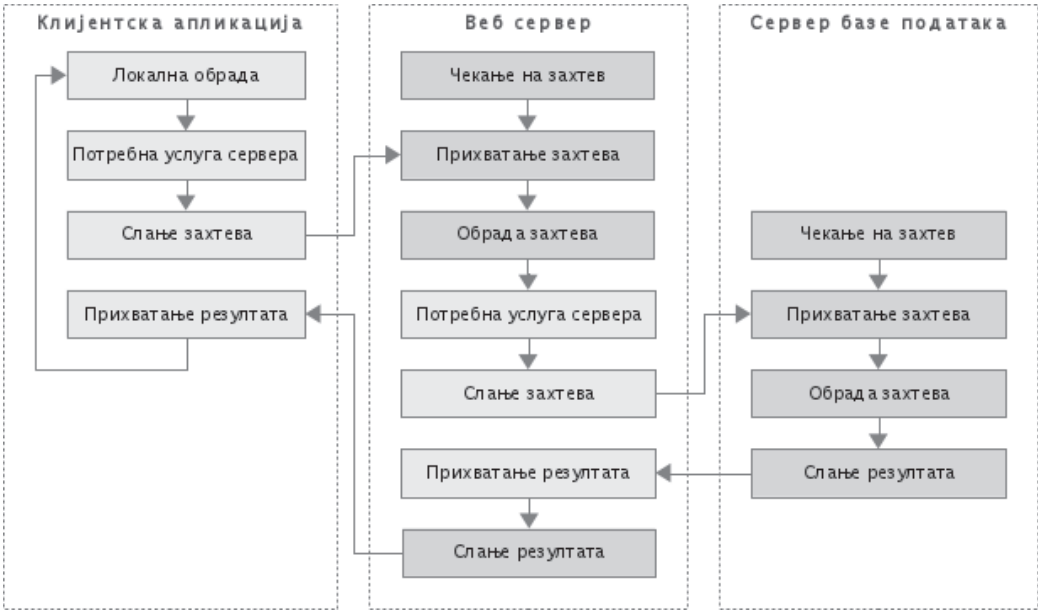
архитектуре клијенти од сервера добијају податке које, затим, користе у локалном процесу обраде. Затим, мејн-фрејм рачунари представљају аутономне чланове мреже који за процес обраде података користе локалне ресурсе. Насупрот томе, сервер се у виду клијента може обратити другим серверима у мрежи за одређени ресурс или дистрибуирану обраду.



Слика 1. Двослојна клијент-сервер архитектура

Основна клијент-сервер архитектура подразумева постојање два слоја - слоја клијента и слоја сервера (слика 1). Код двослојне клијент-сервер архитектуре софтверско решење се разлаже на једну искључиво клијентску, и једну искључиво серверску компоненту. Пример основне, двослојне клијент-сервер архитектуре јесте мрежа у којој корисници путем апликација на својим рачунарима приступају централној бази података.

У пракси су честе и клијент-сервер архитектуре са три слоја јер се њима лакше решавају питања заштите података и контроле приступа. На пример, Веб апликације најчешће користе трослојну клијент-сервер архитектуру на такав начин да основни клијентски део чини Веб браузер, средњи слој чини апликативни Веб сервер, а сервер базе података чини трећи, серверски слој (слика 2). У таквој организацији средњи слој је реализован као серверска компонента, гледано са аспекта Веб браузера, односно као клијентска компонента, гледано са аспекта сервера базе података.



Слика 2. Трослојна клијент-сервер архитектура

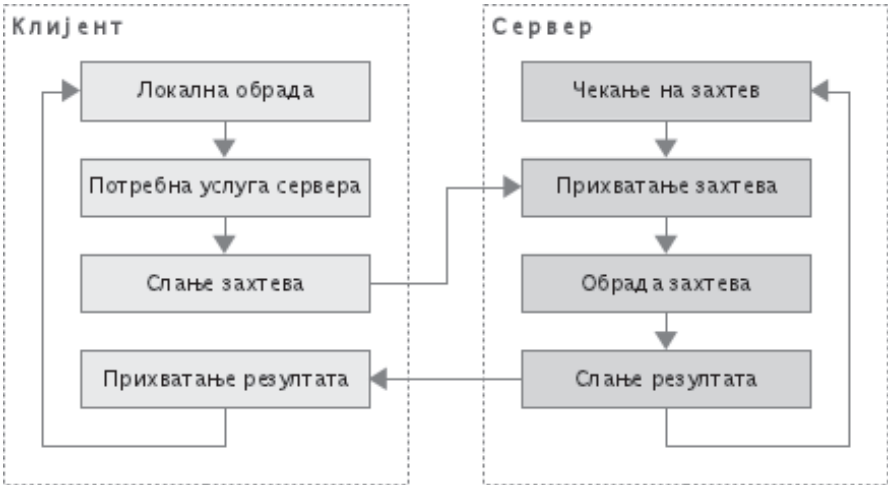
На примеру трослојне архитектуре јасно се може стећи увид да се појмови „клијент" и „сервер" не односе на хардверске карактеристике рачунара, већ на типове процеса, или чак њихове процедуре, који се на тим рачунарима извршавају. Уколико неки процес, или један његов део, захтева услугу од другог процеса (било на локалном или на удаљеном рачунару) његово понашање спада у клијентски део клијент-сервер архитектуре. И обрнуто, уколико неки процес чека на захтеве других процеса, његово понашање спада у серверски део клијент-сервер архитектуре. Опште правило за одређивање улоге код клијент-сервер архитектуре дефинише да је клијентска страна она која од друге стране захтева услугу, а да је серверска страна она која чека на захтев од друге стране и испоручује одговор на њега.

5.1.1.1.1. Итеративна и конкурентна обрада захтева

Постоји велики број различитих стратегија за оптимално искоришћавање процесорских, меморијских и комуникационих капацитета рачунарских система и мрежа. Сервери се, у зависности од начина на који распоређују обраду вишеструких захтева, деле на:

1. сервере са итеративном обрадом захтева и
2. сервере са конкурентном обрадом захтева.

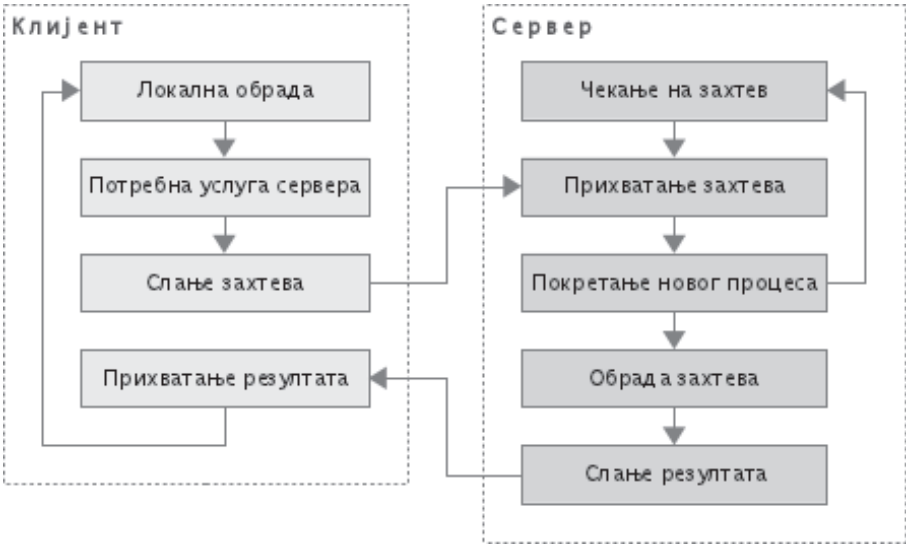
Сервери са итеративном обрадом захтева ослушкују на додељеном порту чекајући на захтев клијента. Након прихватања захтева клијента захтеви осталих клијената се одбацују или чекају у улазном баферу све док се прихваћени захтев не обради и резултати његове обраде пошаљу натраг клијенту.



Слика 1. Итеративна обрада захтева

Мана итеративне обраде захтева је у томе што такав приступ може знатно утицати на перформансе у смислу броја обрађених захтева по јединици времена. Уколико обрада једног захтева у току свог извршења заузме све ресурсе сервера, перформансе се могу сматрати оптималним. Међутим, уколико обрада захтева одузме додатно време услед чекања на ресурс (који није потребан за обраду осталих захтева, одбачених или који чекају у улазном баферу), итеративни приступ показује лошије перформансе од конкурентног. Главна предност итеративног приступа јесте елиминисање проблема конкурентног приступа интерним ресурсима сервера.

Конкурентна обрада захтева је приступ који нуди боље перформансе од итеративног приступа у ситуацијама у којима сервер обрађује велики број захтева од стране више клијената. Побољшање пефроманси произилази из могућности обраде више захтева паралелно. Паралелна обрада се постиже покретањем новог процеса (или нити процеса, у зависности од самог софтвера и од оперативног система) за обраду сваког клијентског захтева.



Слика 2. Конкурентна обрада захтева

За овакав приступ је потребан комплекснији серверски софтвер који се састоји од диспечерског дела (дела који је задужен за прихватање захтева и покретање процеса њихове обраде) и дела који је задужен за обраду захтева. Конкурентна обрада захтева може у одређеним ситуацијама показати слабије перформансе од итеративне обраде услед трошења процесорског времена на покретање нових процеса за обраду захтева. Такође, софтвер који омогућава конкурентну обраду је комплекснији јер интерно решава конкурентни приступ системским ресурснима. Софтвер за конкурентну обраду најчешће унапред покреће одређен број процеса за обраду захтева а по потреби тај број повећава до конфигурационе вредности или ограничења системским ресурсима.

5.1.1.2. Архитектура равноправних чланова

Архитектура равноправних чланова (енгл. *peer-to-peer, P2P*) представља вид диструбуираног рачунарства у коме сваки чвор (енгл. node) има двоструку улогу. Сваки чвор мреже равноправних чланова комуникацију са осталим члановима P2P мреже обавља путем софтвера који се може понашати и као клијент (захтевајући податке или услуге од осталих чворова) и као сервер (одговарајући на захтеве осталих чворова). На овај начин архитектура равноправних чланова омогућава већу аутономију чланова мреже. Архитектура равноправних чланова се углавном примењује код потреба у којима постоји већа толеранција грешке код дистрибуиране одбраде. Главне примене су размена фајлова, директна комуникација, дистрибуирана обрада велике количине података, хеш табеле,

софтвер за забаву...

Главни недостатак архитектуре равноправних чланова односи се на адресовање чланова мреже. Док је код клијент-сервер мрежа потребно само да клијенти имају информацију о томе који сервери су доступни на мрежи (и која је њихова адреса) код архитектуре равноправних чланова потребно је да сваки члан има информације о доступности осталих чланова. Из тог разлога постоји више различитих варијација унутар архитектуре равноправних чланова:

1. децентрализована архитектура равноправних чланова
2. централизована архитектура равноправних чланова
3. хибридна архитектура равноправних чланова

Децентрализована архитектура равноправних чланова представља архитектуру најближу основном моделу. Она је сачињена искључиво од peer чворова који међусобно комуницирају директно.

Код децентрализоване архитектуре равноправних чланова не постоји централни регистар чланова већ се откривање осталих чланова врши преко интерног протокола (најчешће у виду *broadcast* захтева).

Централизована архитектура равноправних чланова представља мешавину архитектуре равноправних чланова и клијент-сервер архитектуре. Као и код децентрализоване архитектуре равноправних чланова мрежу чине чворови који међусобно размењују податке директно, са том разликом што постоји централни сервер чији је задатак евидентирање чланова мреже.

Хибридна архитектура равноправних чланова представља варијанту централизоване архитектуре равноправних чланова која се користи у случајевима када се мрежа састоји од великог броја чворова, а улога сервера подразумева и додатне операције сем евидентирања чланова.

Код хибридне архитектуре равноправних чланова улогу сервера преузима већи број тзв. „супер чворова". Ове чворове најближи чворови користе као сервере док адресне информације везане за остале чворове супер чворови међусобно размењују.

5.2. Систем доменских имена

Систем доменских имена (енгл. *Domain Name System, DNS*) је систем који чува информације везане за имена домена у виду дистрибуиране базе података, а реализован је као клијент-сервер сервис. Најважнија функционалност *DNS*-а је превођење доменских имена у адресе Интернет протокола и обрнуто.

Већина осталих мрежних сервиса (Веб, електронска пошта, пренос фајлова итд.) користи или има могућност да користи *DNS* сервис. На пример, једна од функционалности *DNS*-а је и обезбеђивање информације о томе који сервери су задужени за размену електронске поште за одређени домен. Без ове функционалности *DNS*-а сервис за размену електронске поште не би могао да функционише.

5.2.1. Историјат проблема и решења

Систем доменских имена развијен је као одговор на пораст величине рачунарских мрежа, пораст броја рачунарских мрежа (и појаве Интернета) и на потребу за једноставнијим адресовањем рачунара на мрежи. Под једноставнијим адресовањем се мисли на прилагођавање мрежног адресовања особини људи да лакше памте симболичка имена од бројева (на пример, лакше је запамтити *www.dir.singidunum.ac.rs* од 212.62.45.222). Проблем је у почетку био решен путем *hosts* фајлова на сваком од рачунара на мрежи. Међутим, порастом броја рачунара у рачунарским мрежама недостаци оваквог решења су постајали све озбиљнији проблем:

Узмимо за пример рачунарску мрежу од *N* чланова. *N* рачунара чува информацију о *N* чланова те мреже у локалним *hosts* фајловима:

```
192.168.1.1 рачунар1.локална-мрежа
192.168.1.2 рачунар2.локална-мрежа
192.168.1.N рачунарN.локална-мрежа
```

Проблем 1: додавањем новог рачунара у мрежу потребно је на *N* рачунара додати нови запис у *hosts* фајл и на новом рачунару унети комплетан *hosts* фајл.

Проблем 2: изменом постојећег рачунара у мрежи потребно је на *N* рачунара изменити постојећи запис у *hosts* фајлу.

Проблем 3: уклањањем постојећег рачунара из мреже потребно је на *N*-1 рачунара додати или уклонити запис из *hosts* фајла.

Из наведеног се јасно види да код малих мрежа *hosts* фајлови могу бити једноставније решење од *DNS*-а јер нема потребе за постављањем *DNS* сервера. Међутим, код великих мрежа администрација се знатно отежава јер се при свакој измени мреже она односи на све рачунаре у мрежи. Први корак ка решавању наведених проблема био је дистрибуирани *hosts* фајл (један *hosts* фајл у мрежи коме могу да приступају сви чланови мреже) а проблем је у

потпуности решен 1983. године када је Пол Мокапетрис изумео систем доменских имена.

```
#
# hosts This file describes a number of hostnametoaddress
# mappings for the TCP/IP subsystem. It is mostly
# used at boot time, when no name servers are running.
# On small systems, this file can be used instead of a
# "named" name server. Just add the names, addresses
# and any aliases to this file...
#
# By the way, Arnt Gulbrandsen <agulbra@nvg.unit.no> says that 127.0.0.1
# should NEVER be named with the name of the machine.
# It causes problems
# for some (stupid) programs, irc and reputedly talk. :^)
#
# For loopbacking.
127.0.0.1     localhost
192.168.1.1   tool.local tool
# End of hosts.
```

Листинг 1. Пример hosts фајла на Линукс оперативном систему

Hosts фајлови се могу користити у комбинацији са *DNS*-ом. У том случају они имају приоритет над *DNS*-ом тј. при разрешавању неког имена прво се проверава садржај hosts фајла а тек уколико он не садржи информацију о траженом имену упит се шаље *DNS* серверу. Овакав редослед у разрешавању имена има своје добре стране. На пример, могуће је "заобићи" *DNS* тј. могуће је заменити адресу неког рачунара при локалном разрешавању имена - уносом записа:

```
0.0.0.0       ad.doubleclick.net
```

у *hosts* фајл локалног рачунара он неће бити у могућности да приступи стварној адреси *ad.doubleclick.net*. Последица овога је да при сурфовању Интернетом ниједан садржај са поменуте адресе неће бити доступан. Међутим, како са поменуте адресе најчешће долазе само рекламе, оне неће бити досупне тако да ће се то одразити већом брзином учитавања осталих садржаја у којима се оне

приказују. Са друге стране, заобилажење *DNS*-а могуће је као последица инфицирања система малициозним софтвером. На пример:

1. Нападач креира Веб страницу на сопственој адреси Интернет протокола - X.X.X.X - која је различита од адресе на којој се налази домен *www.google.com* - Y.Y.Y.Y.
2. Веб страница на адреси X.X.X.X је таква да визуелно у потпуности одговара оригиналној страници на *www.google.com* али су логика и база података претраживача који стоји иза те странице потпуно другачије од оних на стварној адреси претраживача *www.google.com*.
3. Лажни *www.google.com* на адреси X.X.X.X намењен је за промоцију клијената који нападачу за узврат дају новчану надокнаду.
4. Нападач затим креира малициозни софтвер који се шири путем Интернета и у hosts фајл заражених рачунара уноси запис: X.X.X.X *www.google.com*.

На овај начин, сваки од заражених рачунара при захтеву за страницом *www.google.com* приступа лажној адреси X.X.X.X уместо Y.Y.Y.Y а корисници добијају погрешне информације у корист нападача.

5.2.2. Теорија рада система доменских имена

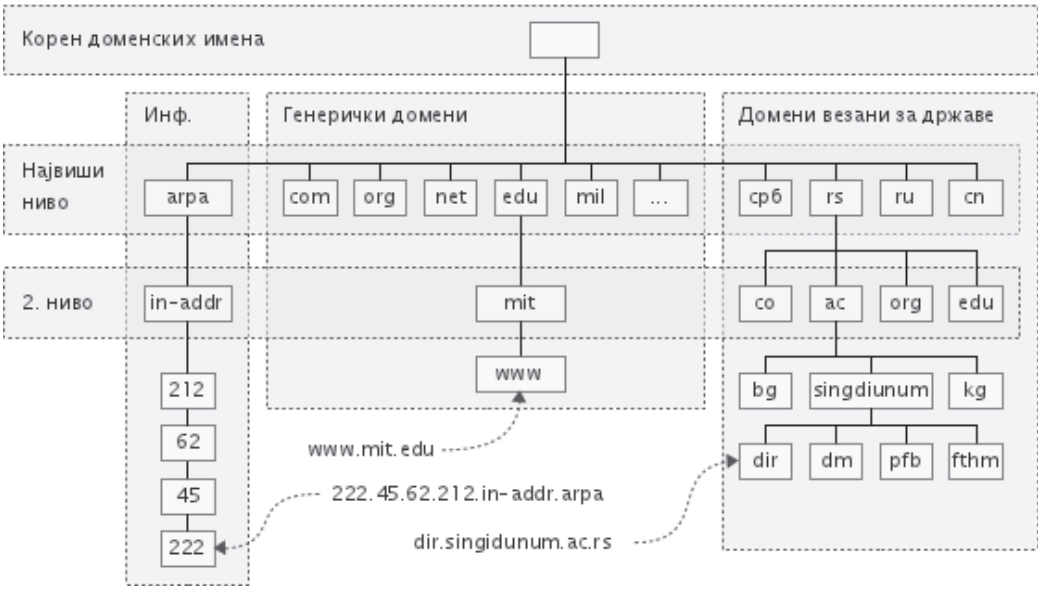
Простор доменских имена је стабло за чији сваки чвор постоји запис у *DNS*-у надлежном за ту зону. У надлежном *DNS* серверу (енгл. *authoritative DNS nameserver*) могуће је за одређену зону декларисати подзоне путем декларисања одговарајућих *DNS* под-сервера.

За разумевање система доменских имена и начина његовог функционисања потребно је разумети саму структуру имена домена (енгл. *domain name*). Назив домена се састоји од два или више делова раздвојених тачкама. Узмимо за пример домен *dir.singidunum.ac.rs*:

Прва ознака са десне стране представља домен највишег нивоа (енгл. *Top Level Domain, TLD*), у овом случају *rs.* Свака наредна ознака гледано са десне стране - *ac*, *singidunum* и *dir* - представља поддомен. Максималан број поддомена је 127 а сваки од чланова може имати максималну дужину од 63 карактера, с тим да целокупна дужина назива (укључујући све поддомене и тачке којим су раздвојени) не сме прећи 255 карактера.

Домен може имати једно или више дефинисаних имена домаћина (енгл. hostname) којима су придружене адресе Интернет протокола. У наведеном

случају, домен је *dir.singidunum.ac.rs* а име домаћина би могло да буде *www.dir.singidunum.ac.rs* са одговарајућом адресом Интернет протокола 212.62.45.222.



Слика 1. Хијерархијска организација система доменских имена

Сервис система доменских имена чине хијерархијски повезани сервери. За сваки од домена мора да буде декларисан један или више надлежних *DNS* сервера који су задужени за чување и давање информација о њему. Један *DNS* сервер може бити задужен и за већи број потпуно независних домена. У корену стабла постоје специјални *DNS* сервери који се зову корени сервери (енгл. *root servers*) и они су задужени за домене највишег нивоа - домене на самом корену стабла. Без поменутих корених сервера рад Интернета не би био могућ јер они чине основу сваког доменског именовања на њему. Тренутно постоји 13 корених сервера и њихова имена су *[A-M]. root-servers.net*.

Домен највишег нивоа је прва ознака с десна у сваком имену домена - у домену *dir.singidunum.ac.rs* домен највишег нивоа је *rs.* Постоје три категорије домена највишег нивоа:

1. домени највишег нивоа везани за државе - домени дужине два слова везани за земљу или одређени географски простор: *rs* - Република Србија, *ru* - Руска Федерација, *cn* - Народна Република Кина и тако даље;
2. генерички домени највишег нивоа - домени који се користе за одређену

класу организација: *com* - комерцијални системи, *org* - непрофитне организације, *edu* - образовне установе и тако даље;

3. инфраструктурни домени највишег нивоа - једини у овој групи је *arpa* домен.

За нашу државу, као и за све државе чије писмо садржи и друге знакове сем енглеског алфабета, значајна је од скора доступна могућност коришћења и међународних знакова у називу домена. У складу са њом, дефинисано је и више домена највишег домена за наведени тип држава. Када су у питању ћирилични домени највишег нивоа, Република Србија је, првенствено захваљујући професионалном и ефикасном раду РНИДС-а, обезбедила срб домен највишег нивоа, одмах након Руске федерације. Почетак јавне употребе овог домена десио се крајем 2011. године.

Клијентска компонента *DNS* система назива се разрешивач (енгл. *resolver*). Ова компонента се обраћа *DNS* серверу да би од њега добила адресу Интернет протокола за задато име домена. Разрешивач је системска компонента која се користи посредно, односно путем програма којима је ова услуга потребна. Разрешивачи доменских имена користе системске мрежне параметре који најчешће садрже логичку адресу једног или два *DNS* сервера.

Пример коришћења *DNS* услуге:

1. Апликација (на пример, Веб браузер) добија униформни локатор ресурса *http://www.dir.singidunum.ac.rs/index.php* од стране корисника и рашчлањује га на протокол (*http*), име домаћина (*www.dir.singidunum.ac.rs*) и локалну адресу ресурса (*/index.php*).

2. Апликација се обраћа разрешивачу доменских имена у циљу добијања адреса Интерент протокола за тражено име домаћина.

3. Разрешивач доменских имена обраћа се *DNS* серверу из мрежне конфигурације рачунара питањем: "Да ли знаш која је адреса Интернет протокола доменског имена *www.dir.singidunum.ac.rs*?"

4. Уколико *DNS* коме се разрешивач обратио није надлежан за домен у коме се тражени домаћин налази (*dir.singidunum.ac.rs*) он се обраћа једном од корених *DNS* сервера питањем: "Који је DNS сервер надлежан за rs домен?"

5. Корени сервер враћа одговор: "147.91.8.6".

6. DNS сервер се обраћа серверу 147.91.8.6 питањем: "Који је *DNS* сервер

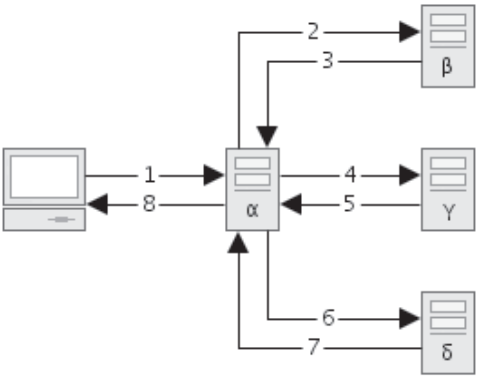
надлежан за *ac.rs* домен?".

7. *DNS* сервер на адреси 147.91.8.6 враћа одговор: "147.91.8.21".
8. *DNS* сервер се обраћа серверу на адреси 147.91.8.21 питањем: "Који је *DNS* сервер надлежан за домен *singidunum.ac.rs*?"
9. Сервер на адреси 147.91.8.21 враћа одговор: "212.62.48.42".
10. *DNS* сервер се обраћа серверу на адреси 212.62.48.42 питањем: "Који је *DNS* сервер надлежан за домен *dir.singidunum.ac.rs*?".
11. Сервер на адреси 212.62.48.42 враћа одговор: "212.62.45.222".
12. *DNS* сервер се обраћа серверу на адреси 212.62.45.222 питањем: "Која је адреса домаћина *www.dir.singidunum.ac.rs*?".
13. Сервер на адреси 212.62.48.222 враћа одговор: "212.62.45.222"
14. *DNS* сервер враћа одговор клијенту чији му се разрешивач обратио: "адреса Интернет протокола за домаћина *www.dir.singidunum.ac.rs* је 212.62.45.222".

На овај начин апликација на клијентском рачунару добија адресу Интернет протокола Веб сервера и путем те адресе прослеђује захтев за Веб страницом */index.php*. Овај пример објашњава рекурзију у раду *DNS*-а. Треба имати у виду да један *DNS* сервер може чувати информације о више различитих домена као и да више *DNS* сервера могу пружати информацију о једном домену.

5.2.3. Кеширање код система доменских имена

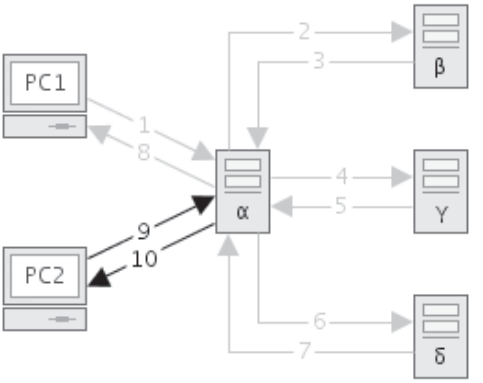
У примеру рекурзивног *DNS* разрешавања, датог у делу „Теорија рада система доменских имена", приказан је скуп корака који је теоретски неопходно проћи да би клијент добио информацију од сервера. У пракси би, међутим, овакав начин рада код сваког *DNS* упита за сваки Интернет домен створио огромно оптерећење свих *DNS* сервера који учествују у разрешавању одређеног домена. Ово се пре свега односи на корене *DNS* сервере и *DNS* сервере којима клијент директно приступа. Да би се избегло поменуто оптерећење уведено је кеширање резултата.



1	A	singidunum.ac.rs?
2	A	singidunum.ac.rs?
3	NS	ac.rs -> 147.91.173.4 (γ)
4	A	singidunum.ac.rs?
5	NS	singidunum.ac.rs -> 212.62.48.42 (δ)
6	A	singidunum.ac.rs?
7	A	singidunum.ac.rs -> 212.62.45.222
8	A	singidunum.ac.rs -> 212.62.45.222

Слика 1. Рекурзивно разрешавање адресе

Кеширање код *DNS*-а има за циљ да омогући сваком од *DNS* сервера смањење броја упита које он поставља осталим *DNS* серверима при разрешавању упита везаног за домене из зоне за коју он није надлежан. Уколико је кеширање укључено на *DNS* серверу, он у својој интерној бази чува резултате свих успешно обављених разрешавања, тако да, уколико се исти упит понови, сервер не мора да тражи поново све информације од осталих *DNS* сервера већ користи потојећу информацију из базе.



1	A	singidunum.ac.rs?
2	A	singidunum.ac.rs?
3	NS	ac.rs -> 147.91.173.4 (γ)
4	A	singidunum.ac.rs?
5	NS	singidunum.ac.rs -> 212.62.48.42 (δ)
6	A	singidunum.ac.rs?
7	A	singidunum.ac.rs -> 212.62.45.222
8	A	singidunum.ac.rs -> 212.62.45.222
9	A	singidunum.ac.rs?
10	A	singidunum.ac.rs -> 212.62.45.222

Слика 2. Претходно добијени резултати се чувају за наредне упите

Овакав начин рада штеди процесорске ресурсе и комуникационе канале *DNS* сервера али отвара и ново питање - уколико се информација о домену на за њега надлежном *DNS* серверу измени, како ће се то одразити на клијенте који

врше упит за тај домен посредством других сервера који у својој бази имају забележену претходну информацију? Одговор на ово питање лежи у ограничењу периода важења (енгл. *Time To Live, TTL*) информација које је надлежни сервер дао. Овај параметар одређује након ког времена ће посреднички *DNS* сервери обновити информацију у својој бази везану за тај домен. Период важења се изражава у секундама и најчешће је постављен на 86.400 секунди, односно један дан. То у пракси значи да је максимално време (након измене домена на надлежном *DNS* серверу) током кога ће клијенти добијати застарелу информацију од посредничких *DNS* сервера један дан.

Остали системски параметри сваке информације о имену домена су:

- *Serial*: серијски број зоне који се увећава при свакој измени података, а служи осталим серверима за утврђивање да ли се информација изменила на главном серверу.
- *Refresh*: број секунди након кога ће *slave* и *secondary* сервери освежити своје податке за зону.
- *Retry*: број секунди након кога ће *slave* и *secondary* сервери поново покушати освежавање података са *master* сервера уколико претходни покушај не успе.
- *Expire*: број секунди након кога ће *slave* и и *secondary* сервери одустати од покушаја да освеже своју базу са *master* сервера уколико претходни покушаји не успеју.

5.2.4. Типови записа

У основне типове записа у бази DNS сервера спадају:

- A - *Address* - запис који садржи IPv4 адресу домаћина.
- CNAME - *Canonical Name* - симболичка веза (линк) ка другом домаћину.
- MX - *Mail Exchange* - адреса сервера електронске поште за домен.
- NS - *Name Server* - адреса надлежног *DNS* сервера за домен.
- SOA - *Start Of Authority* - дефиниција почетка надлежности за одређени домен.

У наставку је дат пример зонског *DNS* фајла за домен *racunarskemreze.com*:

```
$ORIGIN racunarskemreze.com.
$TTL 300
@ SOA ns1.loopia.se. registry.loopia.se. (
        1372896000
        3H  ; Refresh after three hours
        1H  ; Retry after one hour
        1W  ; Expire after one week
        1D )  ; Minimum one day TTL

@       IN  NS  ns1.loopia.se.
@       IN  NS  ns2.loopia.se.
        IN  MX 10  88.198.75.150
        IN  MX 20  192.168.1.1
@       IN  A  88.198.75.150
*       IN  A  88.198.75.150
www     IN  A  88.198.75.150
ww2     IN  A  88.198.75.150
```

5.2.5. Процес регистрације домена

Процес регистрације домена је, у основи, процес уношења записа о домену у базе *DNS* сервера надлежних за наддомен чији ће домен који региструјемо бити поддомен. На пример, за регистровање домена *dir.singidunum.ac.rs* потребно је у базу *DNS* сервера надлежних за домен *singidunum.ac.rs* унети *IP* адресе *DNS* сервера који ће бити надлежни за домен *dir.singidunum.ac.rs*.

Када је у питању регистровање комерцијалних домена, као поддомена Интернет домена највишег нивоа, процес регистрације се обавља преко за то овлашћених регистара. Регистри Интернет домена су комерцијалне или некомерцијалне организације које су овлашћене да клијентима изнајме одређени Интернет домен на временски период од једне или више година.

Приликом подношења захтева за изнајмљивање одређеног домена клијент је дужан да обезбеди два или више *DNS* сервера са јавним *IP* адресама који ће бити надлежни за тај домен. Један *DNS* сервер се може користити као надлежни за више различитих домена. Та услуга (тзв. *DNS hosting*) се може и закупити. Додатно, многи регистри ову услугу нуде бесплатно.

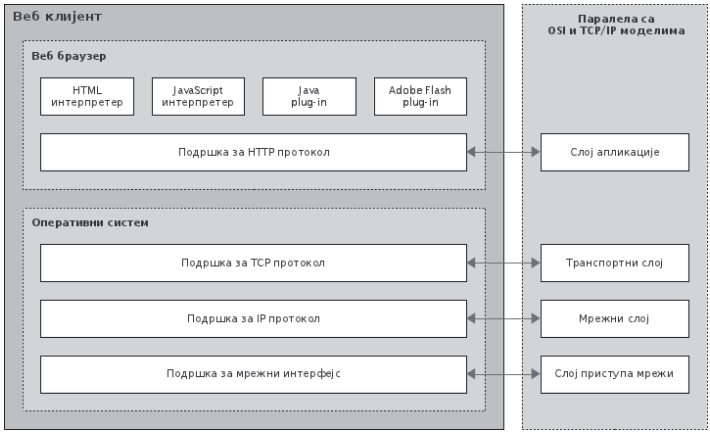
5.3. Веб сервис

Веб (енгл. *World Wide Web, Web*) је данас најпопуларнији сервис Интернет мреже. Развијен је почетком 90-их година прошлога века, паралелно са развојем *HTML* језика и *HyperText Transfer Protocol*-а, развијеним од стране Тим Бернерс-Лија, физичара из Европске организације за нуклеарно истраживање. Назив је добио по првом Веб браузеру који је поседовао графички кориснички интерфејс.

Веб је инцијално развијен да омогући приступ хипертекстуалним документима који су се налазили на различитим серверима. Временом су се појавили програмски језици на страни сервера који су омогућили креирање динамичких докумената као одговора на специфичне захтеве клијента, затим технологије за развој активних компонената на страни клијента (*JavaScript, Macromedia/Adobe Flash, Microsoft Silverlight* и друге), протоколи за сервисно оријентисану архитектуру засновани на Вебу и слично. Тиме је Веб све више постајао платформа за развој мрежних апликација тако да данас прети да у потпуности замени традиционалне десктоп апликације.

5.3.1. Клијент-сервер Веб модел

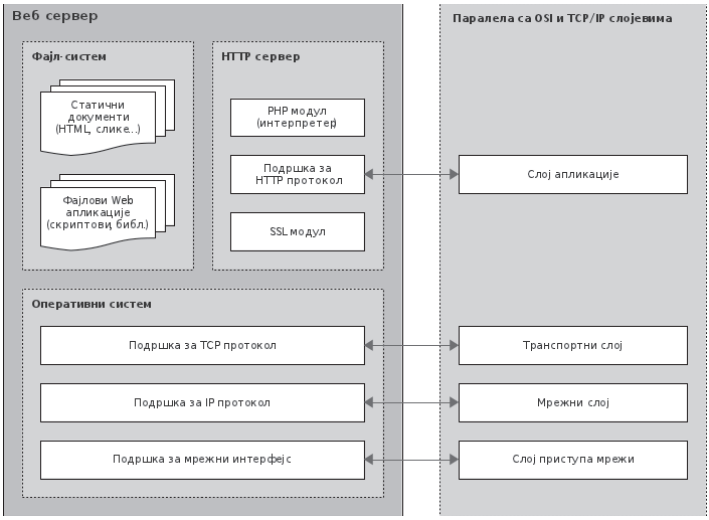
Архитектура Веба је заснована на класичном клијент-сервер моделу. Клијентску компоненту подразумевано представља Веб браузер у виду десктоп апликације, мада данас ресурсима и сервисима на Вебу приступају и друге софтверске компоненте (Веб апликације, апликације на мобилним телефонима и слично).



Слика 1. Архитектура Веб клијента и паралела са комуникационим слојевима

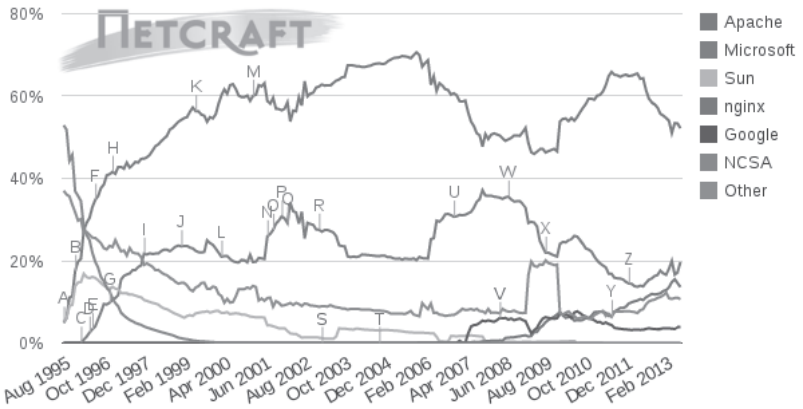
На серверској страни Веба налази се тзв. Веб или *HTTP* сервер чија је иницијална улога била да са фајл-система учита тражени статични документ. Данас Веб

сервери имају далеко веће могућности с обзиром да представљају основну платформу за извршавање Веб апликација.



Слика 2. Архитектура Веб сервера и паралела са комуникационим слојевима

Најпопуларнији сервер данас, а готово и током целог постојања Веба је тзв. Апач (енгл. *Apache HTTP server*) који је 1995. године развијен као наставак обустављеног пројекта у америчком националном центру за супер-рачунарство.

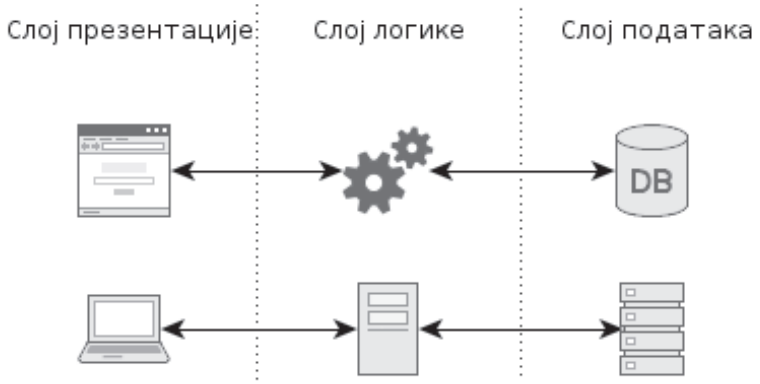


Слика 3. Учешће најпопуларнијих Веб сервера на Вебу (извор: неткрафт)

Поред Апача, данас се често користи и *nginx* код сајтова који имају велики број посета, као и *Microsoft IIS* код сајтова заснованих на технологијама те компаније.

5.3.2. Трослојна архитектура

Веб апликације се углавном могу посматрати подељене на три слоја: слој презентације, слој логике и слој података. Слој презентације обухвата резултате обраде захтева које сервер шаље клијенту и који се интерпретира у Веб браузеру клијента. Овај резултат може бити ресурс било ког типа (слика, скрипт и сл.), с тим да је то углавном *HTML* документ или формулар који садржи контроле за слање нових захтева слоју логике. Поједностављено речено, слој презентације обухвата све компоненте које чине интерфејс ка кориснику.



Слика 1. Трослојна архитектура Веб апликација

Основни задатак слоја логике је обрада корисничких захтева и слање добијених резултата. У типичне кораке обраде захтева спадају нормализација и интерпретација захтева, преузимање потребних података из слоја података, кодовање података у *HTML* или други тражени облик и слање тако добијеног резултата. За дефинисање логике за обраду захтева користе се програмски језици чији се програми извршавају на страни сервера, односно на слоју логике.

Слика 2. Циклус комуникације између слојева трослојне архитектуре

На слоју података се чувају подаци који се користе при креирању одговора на захтеве клијента. На пример, на Веб сајту за преглед најновијих вести, сам садржај вести се мора чувати на некој локацији која је доступна слоју логике. За складиштење и рад са подацима углавном се користе системи за управљање базама података (СУБП) или системи фајлова.

Код статичних Веб сајтова слојеви логике и података нису присутни јер се садржај чува у свом коначном облику, као статичан скуп *HTML* страница, *JavaScript* скриптова, *CSS* стилова, слика... Из тог разлога се статични Веб сајтови често називају и Веб презентацијама. Данас, услед веће доступности *CMS* система, као и све нижег нивоа потребног знања за рад са њима, корисници све чешће користе ове системе (који су, у суштини, Веб апликације) за развој Веб презентација. У складу са тим, данас се термин „Веб презентација" првенствено користи да означи низак ниво интерактивности Веб сајта, пре него за дефинисање структуре и технологија који се користе за његов развој и испоруку.

5.3.3. Униформни локатори ресурса

Униформни локатор ресурса (енгл. *Uniform Resource Locator, URL*) дефинише начин кодовања информација за лоцирање и приступ ресурсима на Интернету. У питању је Интернет стандард који се због погодности које нуди, осим за ресурсе на Интернету, често користи и у локалним мрежама, као и у софтверским системима који не подразумевају дистрибуирану обраду података. Типови ресурса који се овим начином адресовања лоцирају нису ограничени, а могу бити електронски документи, њихове графичке и мултимедијалне компоненте, софтверске компоненте и стања апликација, и т.д.

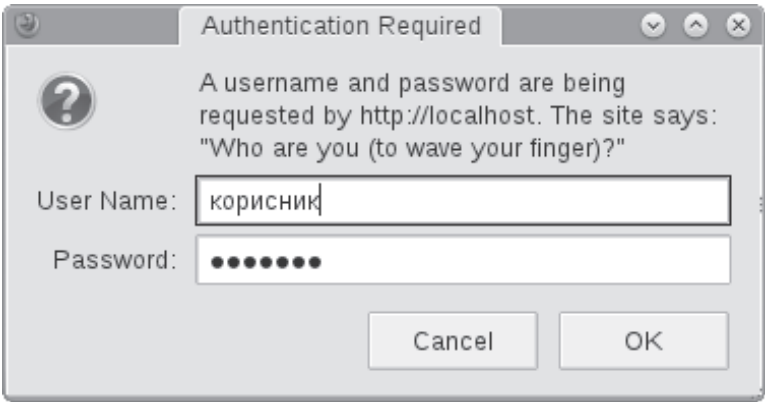
За потребе приступа различитим ресурсима дефинисано је више шема за описивање локације. Сама шема представља први део локатора и најчешће се односи на апликативни протокол којим се приступа ресурсу. Остали део локатора чини адреса специфична за ту шему и од ње је одвојена са две тачке. Спецификација шема које се користе на Интернету подразумева постојање две косе црте након сепаратора између шеме и за њу специфичне адресе. Поред овог, локатор ресурса може поседовати и више сепаратора који одређују његове различите делове.

Слика 1. Структура униформног локатора ресурса HTTP протокола

Када је у питању Веб, захтевани делови униформног локатора ресурса на њему су шема (*HTTP* или *HTTPS* протокол) и адреса домаћина (симболичка или логичка). Овако једноставни локатори се углавном користе за иницијални приступ Веб сајтовима. Порт је такође неопходан део униформног локатора

ресурса али се он у савременим Веб браузерима не приказује уколико се користе подразумеване вредности за протокол (порт 80 за *HTTP* протокол и порт 443 за *HTTPS* протокол).

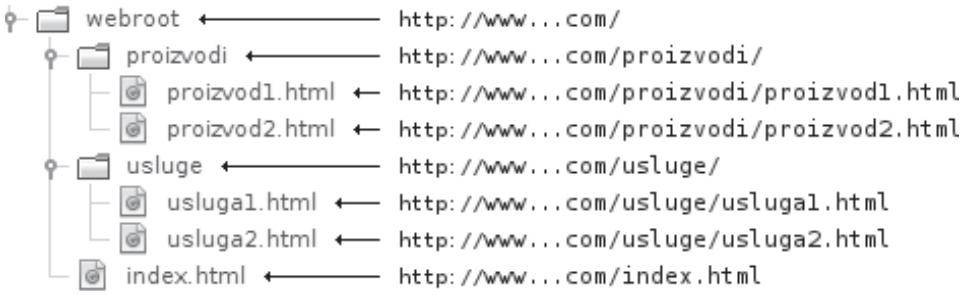
Осим захтеваних делова у пракси се често користи и путања, упит и идентификатор фрагмента. Под путањом се подразумева хијерархијска путања до ресурса на самом домаћину а она може бити путања на фајл-систему или се може динамички обрађивати од стране Веб сервера (пример: *mod_rewrite* модул *Apache* Веб сервера). Упит, као део локатора, најчешће се користи код Веб апликација за прослеђивање параметара серверу путем *GET* метода *HTTP* протокола. Подразумевана улога идентификатора фрагмента је скакање на одређени део документа након његовог учитавања, с тим да одређене Веб технологије на страни клијента могу искористити овај параметар и за друге функционалности. Иначе, сам идентификатор фрагмента се не шаље серверу већ искључиво служи за локалну употребу унутар Веб браузера.



Слика 2. Дијалог за аутентификацију код HTTP протокола

Неки ресурси на Интернету и у осталим рачунарским мрежама јавно су доступни, док се за приступ некима захтева потврђивање идентитета корисника коме је приступ одобрен. Различити протоколи нуде различите системе за утврђивање идентитета корисника а сам *HTTP* протокол нуди једноставан систем за ауторизацију коришћењем корисничког имена и лозинке (слика 2.). Ови приступни параметри се такође могу укључити у униформни локатор заштићеног ресурса, од домаћина одвојени знаком „@", а међусобно одвојени двема тачкама (корисник:лозинка@домаћин). При коришћењу система за аутентификацију *HTTP* протокола треба имати у виду да он самостално не нуди озбиљан ниво заштите, а да укључивање корисничког имена и лозинке у униформни локатор ресурса такође може довести до безбедносних проблема.

У пракси, документи на Вебу често садрже везе ка својим издвојеним садржајима и другим документима у облику релативних путања које прате ову хијерархијску организацију. При учитавању таквих веза Веб браузер израчунава њихове комплетне униформне локаторе на основу њихових релативних путања и униформног локатора документа у оквиру кога су оне дефинисане.



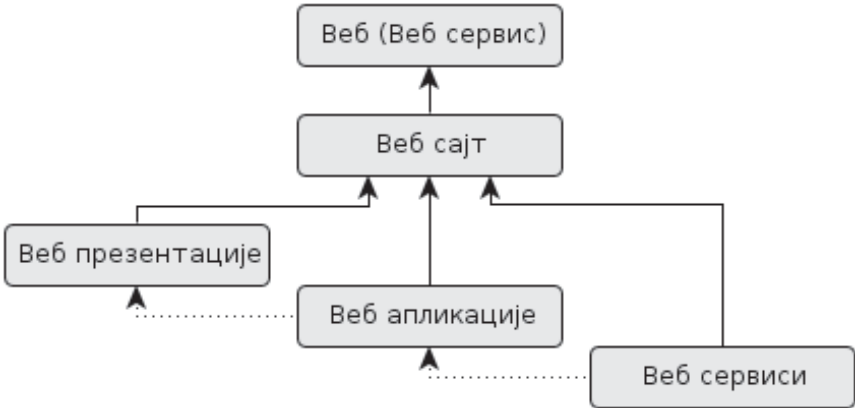
Слика 3. Однос путања фајл-система и URL-а

Униформни локатор ресурса дефинише локацију ресурса али не садржи информацију о томе да ли је ресурс тренутно доступан, нити гарантује да му се (у сваком или у било ком тренутку, као и са сваке или са било које локације) може приступити. Локација ресурса представља једну од његових могућих идентификација, док је униформни локатор ресурса један од типова униформног идентификатора ресурса (енгл. *Uniform Resource Identifier, URI*). Други популарни тип униформног идентификатора ресурса јесте униформни назив ресурса (енгл. *Uniform Resource Name, URN*).

5.3.4. Сајтови, презентације, апликације и сервиси

У пракси се често јавља терминолошка нејасноћа када су у питању Веб презентације, апликације и сервиси. Најчешће се не прави одговарајућа разлика између Веба и Веб сервиса, као ни између Веб сајтова, Веб апликација и Веб презентација.

Сам Веб представља један од сервиса Интернета. У том смислу, израз **Веб сервис** означава један тип услуге за кориснике Интернет мреже, мада се у пракси реч **сервис** све више изоставља и поприма исто значење као и када се користи у множини. Када се користи у множини, овај израз - Веб сервиси (енгл. *Web services*) - не односи се на сам Веб већ на специфичан тип ресурса доступног путем Веба. Веб сервиси нису намењени непосредној употреби од стране људи већ се користе за комуникацију између Веб апликација или њихових компонената.



Слика 1. Хијерархијски однос израза везаних за Веб

Веб сајтови (енгл. *Web site, website*) представљају основну јединицу за организовање садржаја на Вебу. Најчешће се под термином Веб сајт мисли на одређени Интернет домен (нпр. *www.racunarskemreze.com*) мада се Веб сајт пре односи на скуп сродних и међусобно повезаних садржаја који чине једну садржајну целину. У складу са тим, могуће је да се садржај једног Веб сајта налази на више Интернет домена, као и да се на једном Интернет домену налази више Веб сајтова.

У раним фазама Веба садржаје на њему су углавном чинили статични садржаји који су презентовани корисницима. Интеракција са оваквим садржајима је била на минималном нивоу а на основу њих се усталио израз **Веб презентација** (енгл. *Web presentation*). Временом, почели су да се појављују скрипт језици који су омогућавали динамичко креирање Веб садржаја те се за њих све чешће користио израз **Веб апликације**.

Почетком XXI века започео је и убрзан развој система за управљање саржајем на Вебу (енгл. *Content Management System, CMS*). Коришћењем ових система све већи број корисника Интернета дошао је у могућност да брзо и једноставно креира и одржава своје Веб сајтове, чак и они који нису имали никакво техничко познавање *HTML*-а и осталих Веб технологија. С обзиром да је интерактивност оваквих сајтова остала на минималном нивоу, као и да је њихова сврха и даље била презентовање одређеног садржаја, израз Веб презентације је наставио да се користи и за њих, без обира на то што је сам садржај добијен коришћењем Веб апликације

Данас, дакле, израз Веб презентација описује Веб садржаје са ниским нивоом интерактивности. Са друге стране, израз Веб апликација се користи за интерактивне Веб садржаје, односно сајтове чија улога није једносмерно информисање корисника већ пружање одређене услуге.

5.3.5. Развојна и продукциона окружења

Два основна окружења Веб апликација су развојно и продукционо. **Развојно окружење**, како му и само име каже, служи за развој Веб апликација од стране једне особе или развојног тима (програмера, дизајнера, администатора...). Развојно окружење симулира планирано продукционо окружење по присутним компонентама (Веб сервер, сервер базе података, модули за коришћене програмске језике...) али углавном има знатно мањи капацитет. Још једна карактеристика развојног окружења је и то да је оно подешено да одмах прикаже све грешке и недостатке Веб апликације која се развија.

Продукционо окружење служи за стварно извршавање развијене Веб апликације и њено коришћење од стране крајњих корисника. Обично има далеко веће ресурсе на располагању од развојног окружења, што значи да је у могућности да подржи већи број клијената који паралелно шаљу захтеве. Насупрот развојном окружењу, код продукционог окружења се информације о грешкама из безбедносних разлога не приказују, мада се складиште у дневнике догађаја за потребе анализе од стране развојног тима.

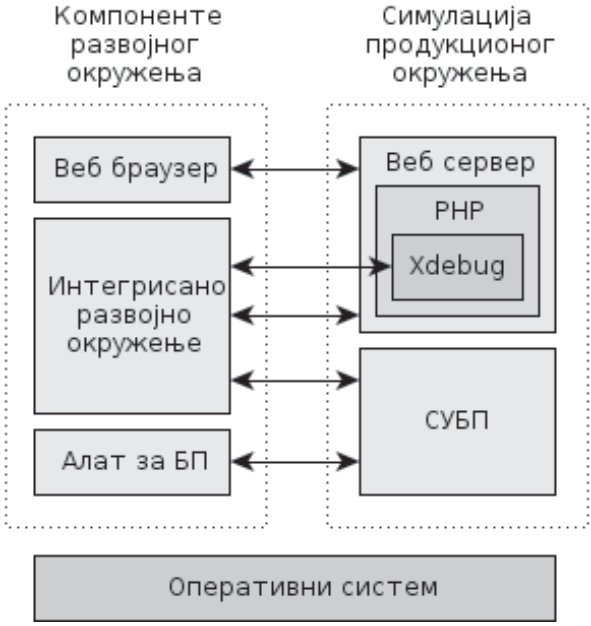
Слика 1. Однос развојног и продукционог окружења

Код великих и сложених пројеката најчешће није могуће, или макар није безбедно, развијене измене Веб апликације из развојног окружења директно применити у продукционо. У таквим ситуацијама се између развојног и продукционог окружења користи и међуокружење (енгл. *staging environment*) у

коме се проверава како ће се развијене измене одразити на активно продукционо окружење. Другим речима, задатак овог окружења је да се у њему тестирају измене и отклоне све неисправности.

5.3.5.1. Развојно окружење

Развојно окружење за Веб је софтверско окружење које се састоји од компонената које омогућавају развој и тестирање Веб апликације или презентације на којој се ради и компонената које симулирају продукционо окружење у коме је могуће извршавање Веб апликација. С обзиром да је у развојном окружењу циљ да се све грешке које постоје у апликацији прикажу одмах, компоненте које симулирају продукционо окружење су тако и подешене, а често садрже и додатке који у томе помажу (какав је, на пример, *Xdebug* додатак за *PHP* интерпретер).



Слика 1. Архитектура развојног окружења за Веб

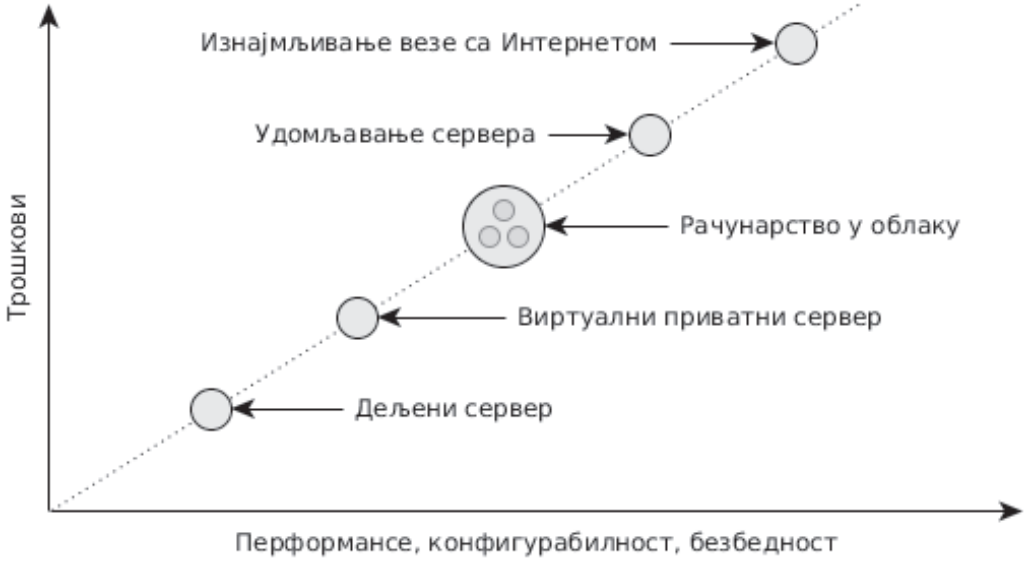
У компоненте које служе за развој спадају интегрисано развојно окружење, алат за рад са базама података (који се често налази у интегрисаном развојном окружењу) и Веб браузер (који служи за тестирање урађеног). **Интегрисано развојно окружење** (енгл. *Integrated Development Environment, IDE*) је софтверски алат који у себи садржи више компонената, као што су уређивач текста, односно програмских кодова, алат за отклањање грешака, алат за моделовање база података и рад са подацима у њима, и слично. Савремена

интегрисана развојна окружења су углавном модуларна па се њихов скуп подржаних функционалности може проширивати.

Развојно окружење се може налазити на једном рачунару (физичком или виртуалном) када су у питању мањи пројекти на којима ради само једна особа. Са друге стране, код већих пројеката се развојно окружење налази на више рачунара, што рачунара које користе програмери и дизајнери, што сервера који симулирају продукционо окружење. У тим случајевима се подаци на различитим рачунарима синхронизују коришћењем *FTP* протокола или напреднијим алатима за управљање верзијама, као што су *Git* и *Subversion*.

5.3.5.2. Продукционо окружење

Продукционо окружење за Веб је софтверско окружење које омогућава извршавање Веб апликација у циљу одговарања на захтеве клијената. У односу на развојно окружење за Веб, продукционо окружење је једноставније јер не садржи развојне алате а и сами сервери у њему садрже само компоненте неопходне за рад, тако да често немају инсталиран ни графички кориснички интерфејс. Са друге стране, продукциона окружења често имају инсталиране додатне компоненте које омогућавају повећање перформанси (нпр. алати за кеширање) и нивоа безбедности.



Слика 1. Однос цене и карактеристика различитих продукционих окружења

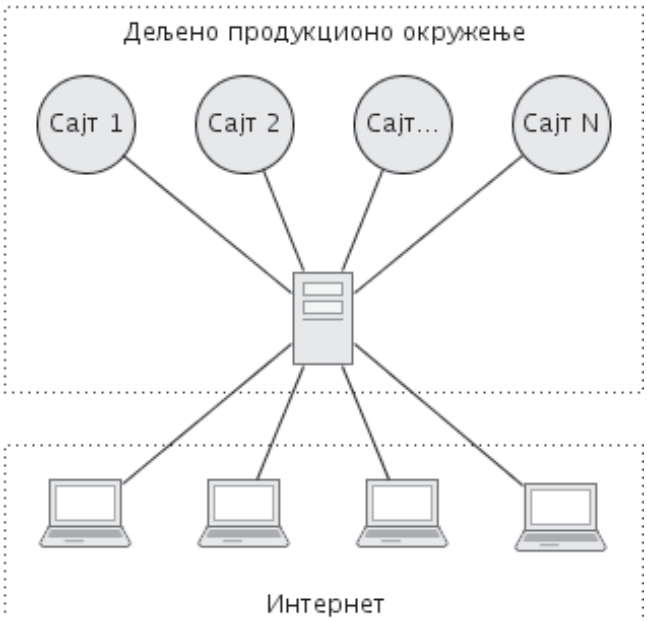
Постоји више решења за обезбеђивање продукционог окружења за сопствену Веб апликацију, односно за њено објављивање на Интернету. Најјефтиније, али

уједно и најскромније продукционо окружење чини дељени Веб сервер. Затим следи изнајмљивање виртуалног приватног сервера и коришћење услуга рачунарства у облаку. Најјефтинија опција за коришћење сопственог хардвера је постављање сервера код Интернет провајдера. Коначно, најмоћнија, али уједно и најскупља опција је развој сопственог дата-центра и измнајмљивање брзе везе са Интернет мрежом.

Компоненте продукционог окружења су тако подешене да о евентуалним грешкама и проблемима у раду Веб апликације клијентима дају што мање информација. Ово се ради из безбедносних разлога, јер је циљ да потенцијални нападач о Веб апликацији зна што мање и да му се на тај начин смањи простор за напад. Са друге стране, поменуте информације о поменутим грешкама и проблемима се складиште у дневнике догађаја и касније користе за отклањање грешака из Веб апликације и анализу покушаних напада.

5.3.5.2.1. Дељени сервер

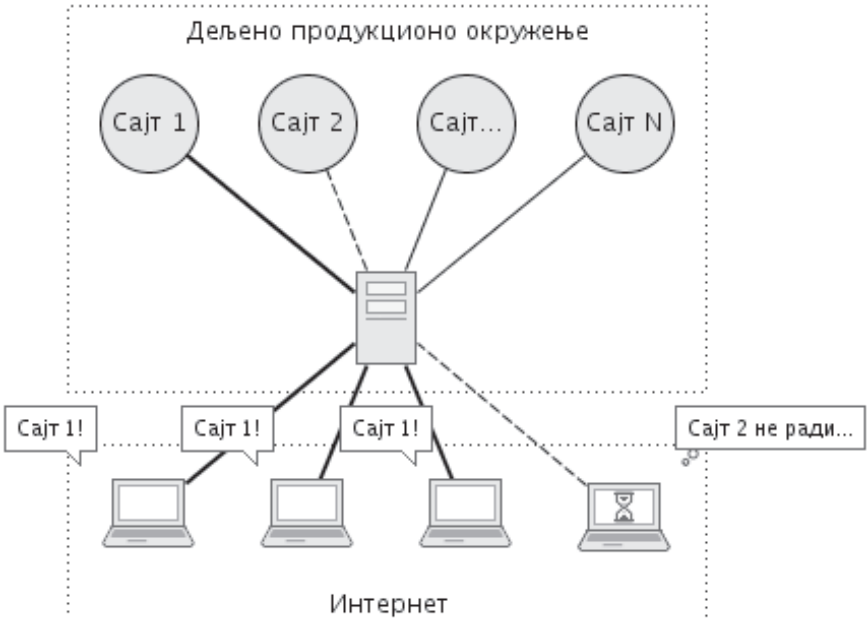
Једна од најјефтинијих, а самим тим и најпопуларнијих опција за објављивање Веб сајтова на Интернету је коришћење дељеног продукционог окружења у виду дељења сервера (енгл. *shared hosting*).



Слика 1. Код дељеног сервера више сајтова се испоручује са истог сервера

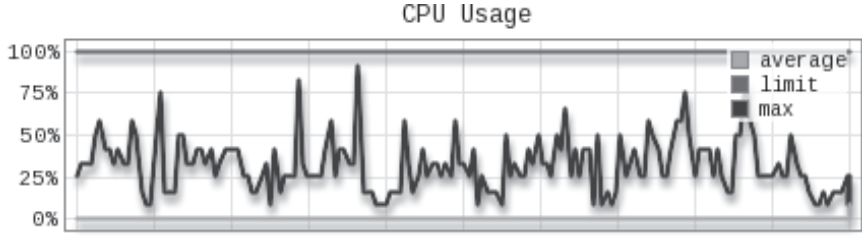
Осим због ниске цене, ова опција је популарна и из тог разлога што корисник не мора да брине о администрацији и одржавању сервера, у шта спадају хардвер, софтвер и мрежни линк, већ је то задатак компаније која нуди услугу.

Једна од главних мана коришћења дељеног сервера јесте ограничена количина ресурса (централни процесор, меморија, комуникациони канал) која је на располагању сваком од сајтова, с обзиром да се ресурси деле на више сајтова. Из тог разлога дељени сервер није добар избор за популарне Веб сајтове код којих су битне висока доступност и високе перформансе.



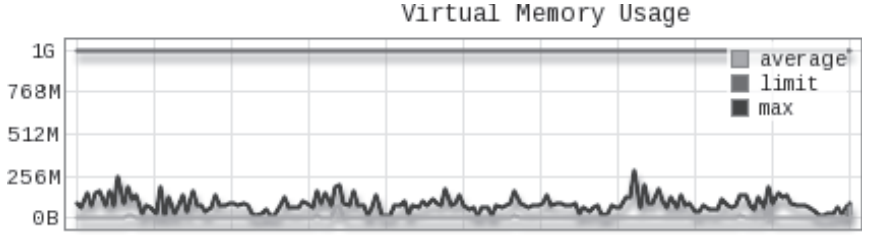
Слика 2. Код дељеног сервера може се јавити недоступност услед преоптерећења

У случају када се у једном тренутку појави велики број посетилаца за неки од сајтова, у зависности од подешавања сервера, може се догодити да се захтеви једног дела клијената одбаце или да се сви захтеви обраде али да због тога трпе остали сајтови. У пракси се углавном за сваког од корисника дефинишу ограничења везана за употребу централног процесора, радне меморије, броја конекција и заузеће комуникационог канала.



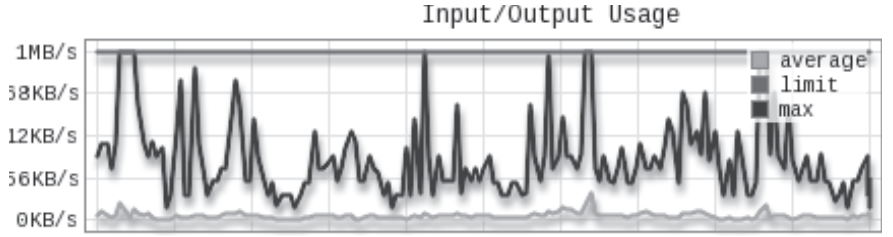
Слика 3. Дијаграм искоришћења додељеног времена централног процесора

На слици 3. је приказан пример дијаграма искоришћења додељеног времена централног процесора. На дијаграму се може видети да ово време углавном задовољава потребе сајтова чији се скриптови извршавају у оквиру једног налога. Добра страна ограничења у погледу времена централног процесора је да се захтеви углавном неће одбацивати, већ ће бити потребно више времена за њихово извршавање. Са друге стране, спор одзив сајтова има негативан утицај на њихову ефикасност, позиционирање на претраживачима...



Слика 4. Дијаграм искоришћења додељене радне меморије

Достизање ограничења у заузећу додељене радне меморије, за разлику од достизања ограничења у погледу времена централног процесора, доводи до насилног прекида обраде захтева. У том случају се, на пример, могу јавити оштећења база података. Заузеће радне меморије зависи од тога колико су скриптови Веб апликације оптимизовани, као и од тога колики је број паралелних захтева.

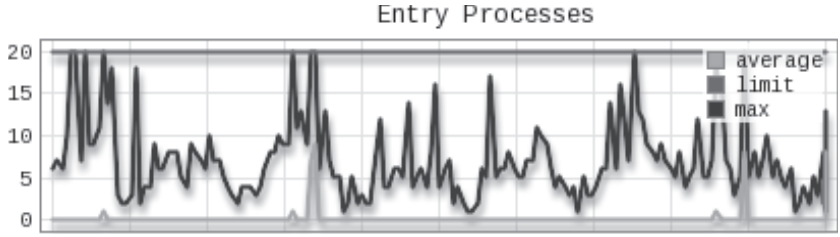


Слика 5. Дијаграм коришћења капацитета комуникационог канала

С обзиром на то да је ограничен и капацитет комуникационих канала којима су сервери дељеног продукционог окружења повезани на Интернет, то ограничење се преноси и на кориснике. На слици 5. се може видети да је администратор ограничио брзину преноса података на 1MB/s, као и да је то ограничње неколико пута достигнуто у посматраном периоду.

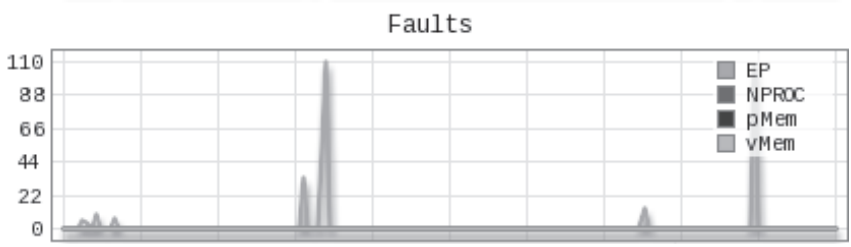
Поред ограничења у тренутној брзини преноса података, у пракси је често присутно и ограничење у количини пренетих података, најчешће на месечном нивоу (на пример, од неколико десетина GB па до неколико TB). Стратегије пружаоца услуга у случају достизања овог ограничења могу бити различите али

се углавном своде на смањење брзине преноса података на минималну или на одбијање захтева ка сајтовима који се налазе на том налогу.



Слика 6. Дијаграм броја паралелних захтева

Као што је раније речено, утрошак процесорског времена, заузеће радне меморије и заузеће комункационог канала зависе од два фактора: степена оптимизације скриптова који се извршавају на серверу и броја паралелних захтева. С обзиром на то да је први фактор у надлежности корисника, администратори често ограничавају и број паралелних захтева ка ресурсима који припадају једном налогу. На слици 6. је дат пример броја паралелних захтева (процеса) а са истог дијаграма се може уочити и да је ограничење од 20 паралелних захтева достигнуто неколико пута у посматраном периоду. Након достизања ограничења сервер одбија даље захтеве све док се не заврши извршавање неког од постојећих процеса.



Слика 7. Дијаграм коришћења централног процесора

О свим наведеним ограничењима треба водити рачуна с обзиром да она доводе до успореног одговарања на захтеве посетилаца или чак до њиховог одбијања. На слици 7. је приказан дијаграм проблема у извршавању захтева са кога се види да су се у одређеним периодима јављале грешке као последица ограничења у броју обрада паралелних захтева. Занимљиво је и да је у овом конкретном случају узрок великог броја паралелних процеса било њихово успорено извршавање услед отказивања хардверских компонената сервера.

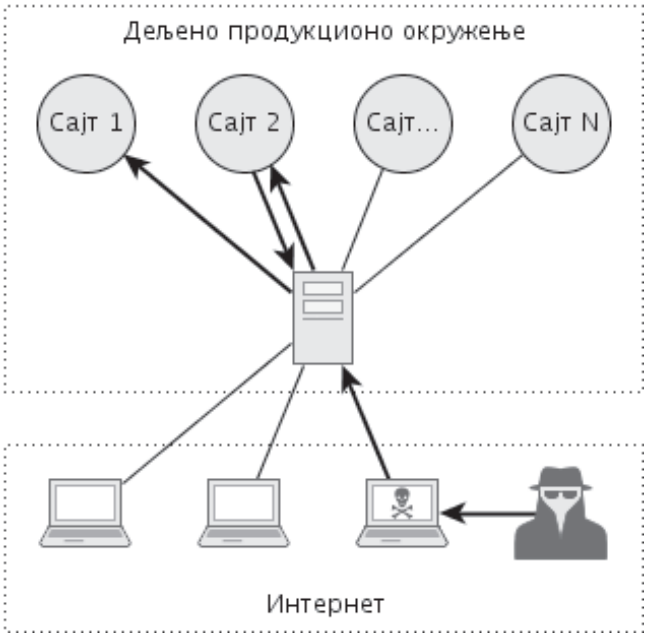
Није редак случај ни да компанија која пружа услугу дељеног сервера одређени сајт једноставно искључи уколико примети да се за обраду захтева ка њему троши далеко више ресурса од очекиваног просека. Логика иза тога је да је

боље изгубити једног клијента уместо више других чијих је чување сајтова исплативо, а који би били угрожени недостатком ресурса за нормалан рад.

Ограничење које у неким случајевима може бити значајно је и смањена могућност за специфично подешавање сервера за потребе неке Веб апликације која се на њему извршава. Администратори често не желе да врше сложеније измене из страха да се не угрози стабилност или безбедност сервера, односно осталих сајтова који се на њему држе. Није редак случај да сами администратори не поседују потребно знање из области у којој се захтева измена, те да из тог разлога не желе да начине чак ни мање измене у подешавањима.

5.3.5.2.1.1 Безбедносни аспекат

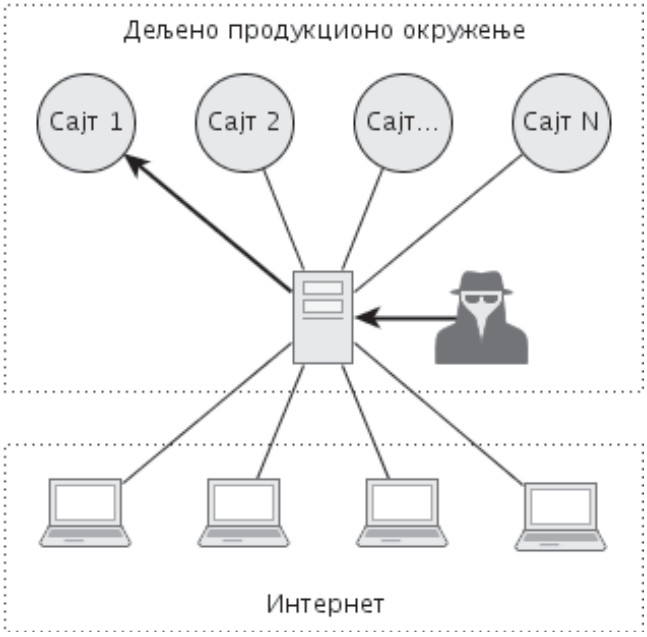
Још један недостатак дељеног продукционог окружења је и низак ниво безбедности апликације и података. С обзиром да се на истом серверу извршавају програми великог броја корисника, потенцијални нападачи до могућности за извршавање својих програма на серверу могу доћи кроз улогу регуларног корисника.



Слика 3. Код дељеног окружења пропусти у једном сајту могу угрозити остале

На пример, уколико сервер није правилно подешен, скриптови једног корисника

могу из конфигурационих фајлова другог корисника ишчитати параметре за приступ серверу базе података, а затим и преузети целокупну базу података у којој се налазе поверљиви подаци (лозинке уредника, приватне поруке, адресе за електронску пошту и друго). Често се дешава и да неки од корисника у дељеном окружењу користе застареле верзије бесплатних Веб апликација које садрже пропусте чијим се искоришћавањем може компромитовати цео сервер.

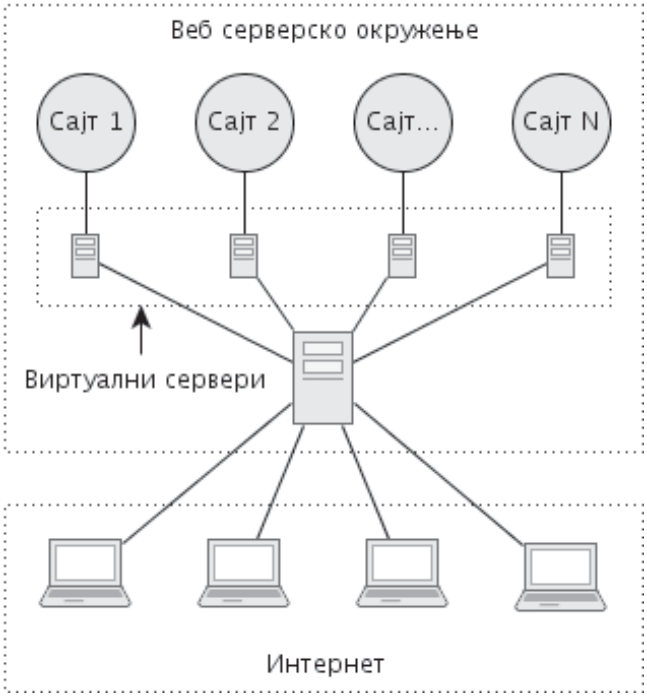


Слика 4. Администратор дељеног продукционог окружења има приступ свим подацима и фајловима апликације

Следеће о чему треба водити рачуна код дељеног продукционог окружења, када су безбедност и поверљивост у питању, јесте ниво поверења у самог администратора система. Треба имати у виду да администратор има приступ свим подацима везаним за Веб сајтове који се налазе на серверима које он одржава. У те податке спадају фајлови апликација, базе података, статистике коришћења и слично. Са друге стране, у уговорима које корисник дељеног продукционог окружења потписује са пружаоцем услуга ово питање се обично не поставља, нити корисник има икакву информацију ко је администратор сервера на коме се његов сервер налази.

5.3.5.2.2. Виртуални приватни сервери

Виртуални приватни сервери (енгл. *Virtual Private Server, VPS*) представљају напреднију варијанту дељеног продукционог окружења, односно јефтинију варијанту удомљавања сервера. У овом случају корисници од хостинг компанија закупљују једну или више виртуалних машина на којима ће се чувати и извршавати њихови Веб сајтови.

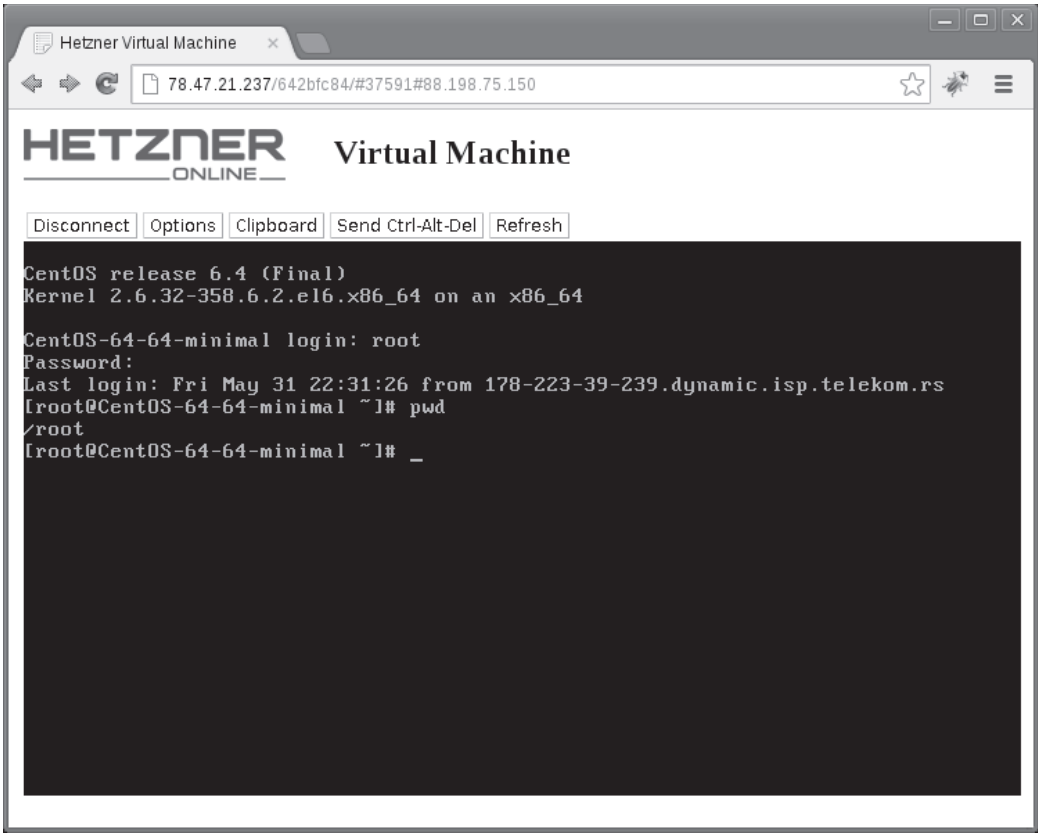


Слика 1. На једном виртуалном приватном серверу се налазе сајтови једног корисника

У предности код коришћења виртуалних приватних сервера, у односу на дељено продукционо окружење, спадају виши ниво заштите, гарантовани ниво ресурса резервисан за корисника и могућност подешавања свих параметара сервера у складу са сопственим потребама, укључујући и инсталацију додатног софтвера. Са друге стране, цена ове услуге је и преко десет пута виша у односу на дељено продукционо окружење. Додатно, корисник подразумевано преузима на себе задатак администрирања сервера - освежавање верзија софтвера, прављење резервних копија и друго.

И у случају коришћења виртуалног приватног сервера значајно је питање поверења у администратора физичког сервера пошто он и даље може да

приступи свим подацима који се налазе на виртуалном серверу, подацима које он размењује са клијентима, као и статистикама коришћења.



Слика 2. Приступ серверу коришћењем SSH протокола и Јава аплета

Хостинг компаније најчешће имају предефинисане виртуалне машине са инсталираним одређеним оперативним системом (углавном нека од популарних дистрибуција Линукса) и основним софтвером потребним зарад Веб сервера. С обзиром да је у том случају процес прављења нове инстанце веома једноставан, време потребно за активирање ове услуге мери се у минутима. Уколико се на виртуалну машину инсталира додатни софтвер за који се плаћа лиценца (на пример *CPanel* или *MS Windows* као оперативни систем), њену цену је потребно додати на основну цену услуге.

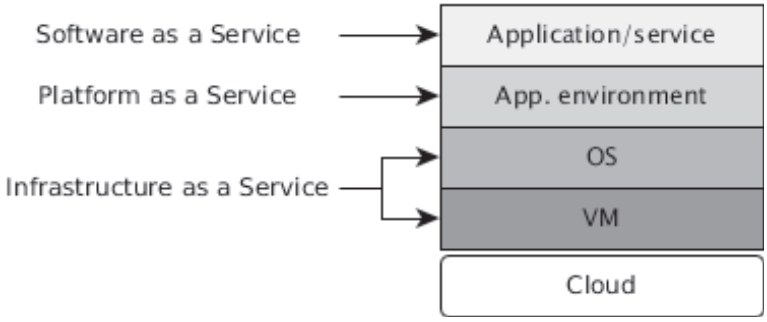
5.3.5.2.3. Рачунарски облак

Рачунарство у облаку (енгл. *Cloud computing*), по дефиницији америчког Националног института за стандарде и технологију (енгл. *National Instutute for*

Standards and Technology) представља *„модел за омогућавање општеприсутног, погодног, по потреби доступног мрежног приступа дељеном резервоару подесивих рачунарских ресурса (на пример, мрежама, серверима, складиштима података, апликацијама и сервисима) који се могу брзо прибавити и ослободити, уз минималне напоре у погледу управљања, као и минималну интеракцију са пружаоцем услуге“*[1].

У зависности од типа услуге, односно нивоа на ком се кориснику пружа услуга из рачунарског облака, постоје следећи модели рачунарства у облаку:

Софтвер као услуга (енгл. *Software as a Service, SaaS*) је модел код кога корисник користи апликацију или сервис који нуди пружалац услуга. При том се комплетна апликација извршава у рачунарском облаку који одржава пружалац услуге. **Платформа као услуга** (енгл. *Platform as a Service*) је модел код кога корисник изнајмљује окружење у ком ће се извршавати његова апликација. На пример, корисник изнајмљује Веб окружење са подршком за *PHP* језик и *MySQL* базом података, и у то окружење поставља своју апликацију која ће се у њему извршавати.



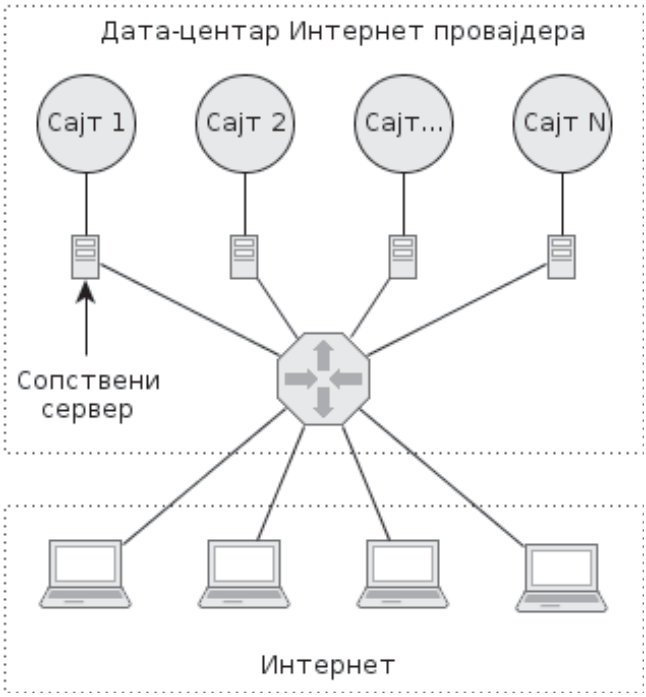
Слика 1. Различити модели коришћења рачунарства у облаку

Инфраструктура као услуга (енгл. *Infrastructure as a Service*) је најнижи ниво коришћења услуга рачунарског облака и подразумева изнајмљивање инфраструктуре у виду процесорских, складишних и мрежних ресурса, односно виртуалне машине са одређеним карактеристикама и, евентуално, инсталираним оперативним системом. У првом моделу (*SaaS*) корисник има најмању могућност за измену окружења, али и најмање обавезе око његовог одржавања. Са друге стране, код изнајмљивања инфраструктуре (*IaaS*) корисник може да мења готово све параметре изнајмљеног окружења, али је он дужан и да обезбеди инсталацију, подешавање и одржавање инсталираних компонената.

1 NIST SP 800-145, The NIST Definition of Cloud Computing

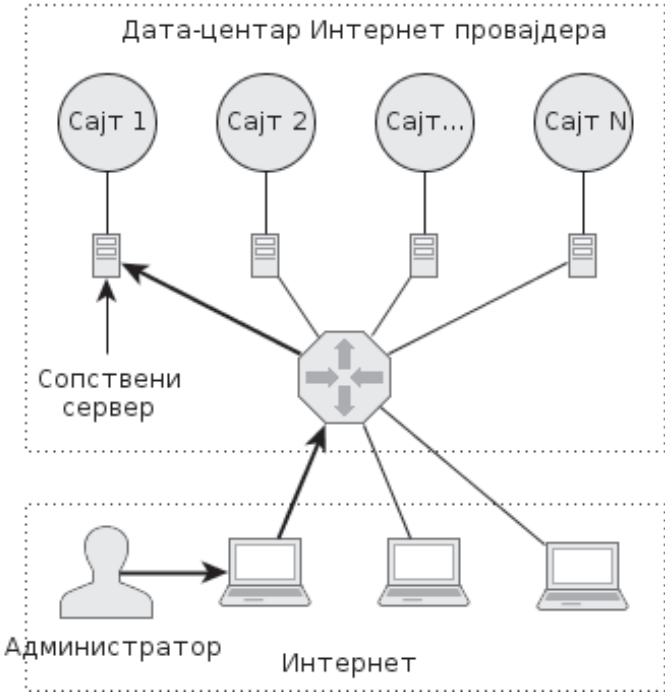
5.3.5.2.4. Удомљавање сервера

Удомљавање сервера (енгл. *server housing*) је приступ код кога корисник сам обезбеђује хардвер сервера, на њега инсталира жељени софтвер и поставља Веб сајт, а затим такав сервер односи до Интернет провајдера. Провајдер сервер односи у своју серверску салу и тамо га прикључује на мрежни кабл и кабл за напајање електричном енергијом. У серверској сали су обезбеђени потребни услови за несметан рад сервера (температура, влажност ваздуха, непрекидно напајање и слично).



Слика 1. Сопствени сервер се поставља у дата-центар Интернет провајдера

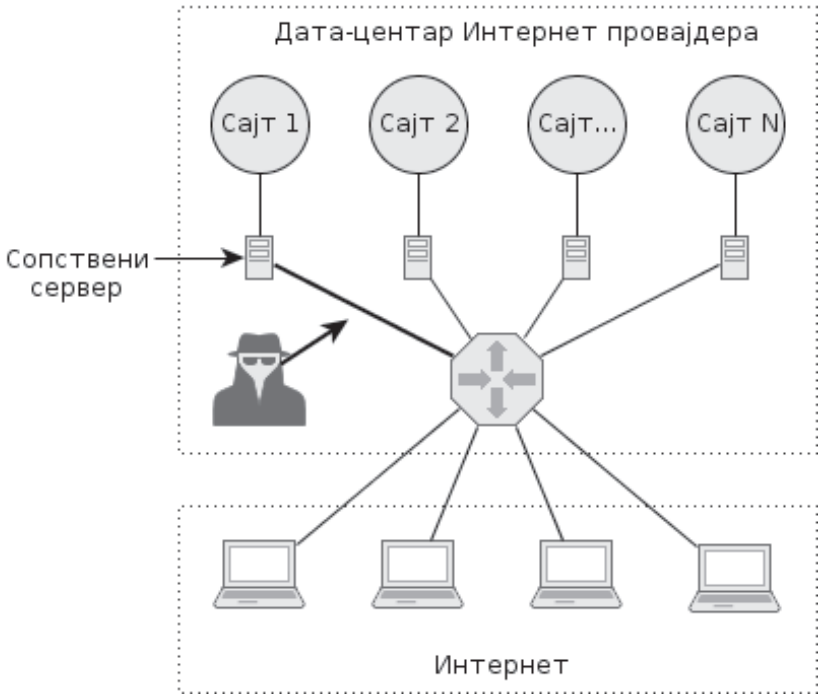
Администрирање сервера је код његовог удомљавања углавном задатак самог корисника услуге. То значи да је корисник задужен да пре одношења сервера код Интернет провајдера на њега инсталира одговарајући оперативни систем и подеси мрежне интерфејсе у складу са параметрима које је добио од провајдера. Одржавање сервера - накнадна подешавања сервиса, освежавање верзија софтвера, прављење резервних копија и слично - обавља се путем Интернета. У случају да постоји потреба за физичком интервенцијом на серверу (блокада оперативног система, надоградња...) сервер се преузима од провајдера и враћа након интервенције.



Слика 2. Одржавање сервера се обавља путем Интернета

Када је безбедносни аспекат у питању удомљавање физичког сервера нуди виши ниво безбедности од изнајмљивања виртуалног приватног сервера и коришћења дељеног окружења. Међутим, основни ризик који овде остаје (када је у питању неповерење у администраторе Интернет провајдера) је надгледање комуникационог канала. Дакле, администратори Интернет провајдера могу да читају све поруке које нису шифроване, као и да добију статистичке податке за посматрани период (број захтева, пренета количина података и слично).

Додатни ризик који постоји је и искључивање сервера од стране администатора Интернет провајдера (насилно или регуларно) и копирање садржаја са извађених хард-дискова. Овакав догађај, након враћања дискова и поновног укључивања сервера, може проћи неопажено или се заменити са краткотрајним прекидом рада комуникационог канала, као и правдати разлозима као што су проблеми на електричној мрежи и слично. Да би се заштитили подаци од оваквих напада потребно је користити шифроване фајл-системе на серверима који су физички доступни потенцијалним нападачима.

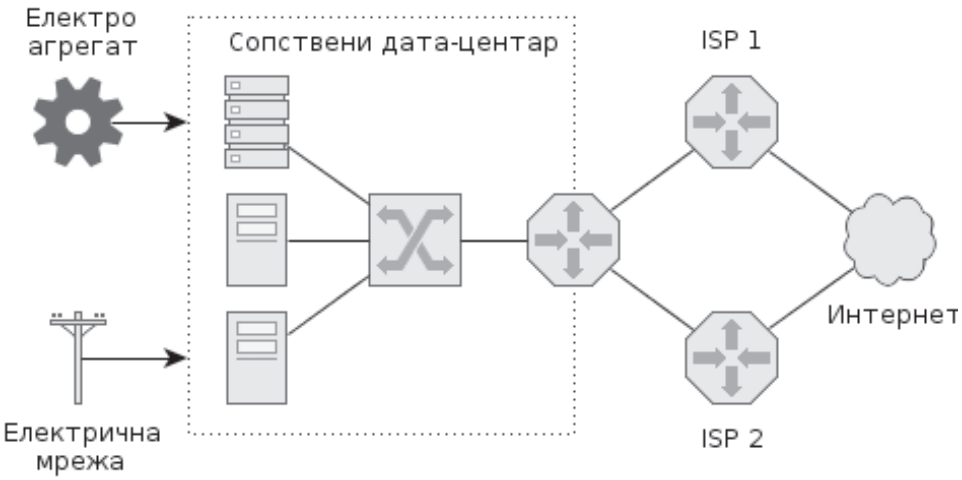


Слика 3. Администратор Интернет провајдера има приступ ком. каналу

5.3.5.2.5. Изнајмљивање брзе везе са Интернетом

Најфлексибилније и најбезбедније решење за продукционо Веб окружење, са потенцијално највишим перформансама, јесте повезивање сопственог дата-центра са Интернет мрежом и испорука Веб апликација са сопствених Веб сервера. Овакав тип решења је посебно згодан за кориснике који имају потребу да њихове јавно доступне Веб апликације комуницирају са интерним системима и базама података (на пример, портал за електронско банкарство).

При развоју оваквог решења треба обезбедити брзу и поуздану везу са Интернет мрежом. Везе треба да буду засноване на технологијама које нуде мало кашњење и брз пренос података у оба смера. Препоручљиво је коришћење вишеструких веза ка Интернету (по могућству преко различитих Интернет провајдера) и система који омогућавају несметан рад уколико нека од веза постане недоступна.



Слика 1. Сопствени дата-центар са Интернет везом

Иако развој сопственог решења нуди највиши степен безбедности и флексибилности, само корисници са највећим потребама и могућностима одлучују се за њега. Разлог томе су високе цене Интернет веза које се овде користе, али и додатни трошкови који се односе на куповину и одржавање рачунарских система, обезбеђивање сталног и поузданог напајања електричном енергијом, обезбеђивање одговарајуће температуре и влажности ваздуха у дата-центру и слично.

5.3.5.2.6. Мреже за испоруку садржаја

Код Веб сајтова који имају велики број посетилаца широм света превелика удаљеност између посетилаца и сервера на којима се налазе садржаји Веб сајта може бити узрок ниских перформанси. Додатно, на превише велики број захтева често није могуће одговорити са једне локације, коришћењем једног комуникационог канала ка Интернету. Да би се на овакве изазове одговорило у тим случајевима користе се мреже за испоруку садржаја.

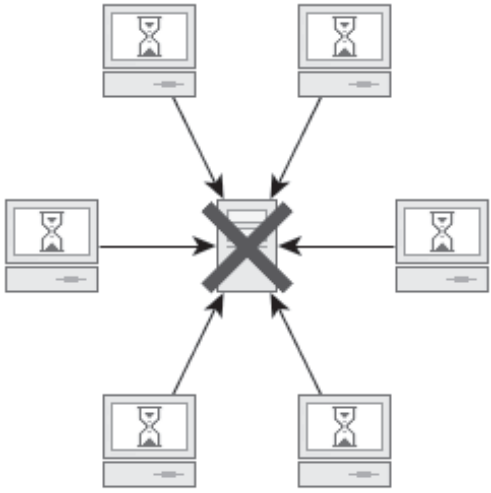
Мреже за испоруку садржаја (енгл. *Content Delivery Network, CDN*) су системи који имају сопствене сервере у чвориштима Интернет провајдера на различитим географским локацијама. Клијенти који закупе коришћење мреже за испоруку података статичне садржаје сајта (слике, *JavaScript* и *CSS* кодове и слично) снимају на њене сервере. Након тога, будући захтеви клијената за тим садржајима се преусмеравају на најближи сервер мреже за испоруку који их садржи.

5.3.5.3. Доступност

Доступност (расположивост) неког ресурса или услуге најчешће се израчунава као однос времена у коме је исте могуће користити и укупног времена које се посматра. На пример, Веб сервер који се годишње искључује шест пута на по сат времена, због одржавања хардвера и софтвера или нестанка струје, има доступност 8.754 од 8.760 сати, односно 99,931507 процената на годишњем нивоу.

У пракси се за означавање доступности неког система често користи и метрика „деветки", односно број деветки у проценту доступности (на пример, у претходном случају је то „три деветке"). Данас се често захтева доступност система на нивоу „пет деветки" (око 5 минута недоступности годишње) или чак „шест деветки" (око 30 секунди недоступности годишње).

Недоступност се може јавити услед отказивања система, али и услед његовог преоптерећивања - добијања већег броја захтева него што је у стању да обради. Такође, у дељеним продукционим окружењима сам сервер често има довољно ресурса да одговори на велики број захтева али је капацитет ограничен софтверски, у складу са количином ресурса које је корисник закупио.



Слика 1. Недоступност сервера онемогућава коришћење сервиса и података

Оно што треба имати у виду је и то да иако је систем укључен и оперативни систем се извршава (енгл. *uptime*) не подразумева да су сервиси и подаци на њему доступни. На пример, за одржавање већине софтверских сервиса није потребно ресетовати рачунар, али је саме сервисе потребно привремено

искључити. Такође, код већине система је након физичког укључивања рачунара потребно знатно време док се не покрену сви његови делови (оперативни систем, мрежни интерфејси, сервиси...) и достигне потпуна оперативност.

У извештају IBM-а[2] се процењује да је 1996. године недоступност рачунарских система коштала америчку привреду преко 4,5 милијарде америчких долара, а тај износ је за 1999. годину процењен на око 6,6 милијарди. Висине савремених губитака је тешко проценити али се може проценити да су оне потенцијално далеко веће од наведених с обзиром на то да све већи број пословних система уопште није у стању да функционише без информационе подршке и везе са Интернетом.

Једноставан пример губитака услед недоступности Веб сајта јесу плаћене рекламе на Гугл претраживачу. Ове рекламе се плаћају по клику на њих (енгл. *Cost Per Click, CPC*), без обзира на то да ли је Веб страница ка којој води линк у реклами доступна или не. То значи да би једнодневна недоступност Веб сајта чији је дневни рекламни буџет €100 створила губитак раван трогодишњој цени услуге дељеног продукционог окружења. При том не треба заборавити ни негативне ефекте као што су стварање лоше слике код потрошача, лошије позиционирање на претраживачима и слично.

5.3.5.4. Управљање оптерећењем и скалабилност

Једна од веома значајних карактеристика технологија које се бирају за развој одређеног Веб решења је скалабилност. **Скалабилност** представља могућност да се постојеће решење прошири у циљу одговарања на новонастале потребе, односно да није потребно да се због њих развија ново решење.

Често се димензије продукционог окружења више пута мењају током животног века апликације. На пример, одређени Веб сајт може почети као једноставна апликација у дељеном продукционом окружењу али због пораста популарности убрзо захтевати прелазак на издвојени виртуални приватни сервер, а потом и на неколико физичких наменских сервера.

Потреба за унапређивањем продукционог окружења Веб апликације углавном се јавља због пораста оптерећења - последице повећаног броја захтева клијената. Међутим, она се може јавити и због пораста вредности података у њему, односно потребе да се они боље заштите. На пример, Веб сајт на коме се уведе плаћање путем платних картица углавном је препоручљиво изместити из дељеног продукционог окружења на сопствени сервер.

2 IBM Global Services, Improving Systems Availability, http://www.cs.cmu.edu/~priya/hawht.pdf

Слика 1. Хоризонтално и вертикално скалирање серверске инфраструктуре

Скалирање може бити хоризонтално и вертикално. **Вертикално скалирање** сервера подразумева појачавање постојећих сервера, примарно кроз додавање нових и јачих процесора и радне меморије.

Слика 2. Хоризонтално и вертикално скалирање комуникационих канала

Хоризонтално скалирање подразумева додавање нових сервера и распоређивање функција на њих. При том треба имати у виду да коришћене софтверске технологије морају имати могућност да искористе више процесора/сервера, мада је то код Веб апликација углавном случај.

Оно што треба имати у виду је да се скалабилност не односи само на серверску инфраструктуру, већ и на комуникационе канале, коришћене технологије, софтверску архитектуру и друго. Скалирање комуникационих канала такође може бити хоризонтално и вертикално, где се код вертикалног скалирања повећава пропусна моћ постојећих канала а код хоризонталног се додају нови.

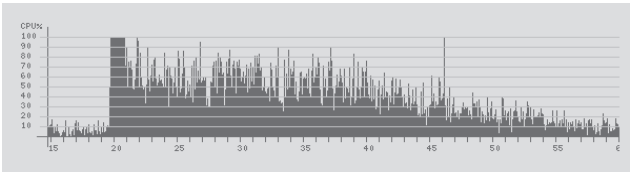
5.3.5.4.1. Пример вертикалног скалирања

У наставку је дат пример вертикалног скалирања Веб платформе, описан у раду под називом „Развој система за проверу знања студената у оквирима постојећег ИС универзитета“[3].

Прва коришћења система реализована су на хардверској платформи *Intel P4* процесор 2.4GHz, 1GB RAM, 1Gb/s мрежним линком. Уско грло се појавило приликом приступања провери од стране већег броја студената истовремено (~50 студената), када се брзина одзива драматично смањила (~120 секунди). Систем је дизајниран да за сваког студента у провери врши рандомизацију редоследа питања и понуђених одговора. Максимално оптерећење процесора у тренутку приступа провери могло се изразити на следећи начин:

$$O_{\max} = Ns * Np * (\frac{No}{Np} + 1)$$

при чему *Ns* представља број студента, *Np* је број питања у провери и *No* представља укупан број одговора у провери.



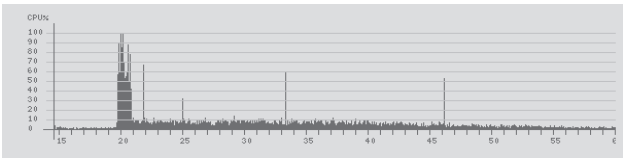
Слика 1. Оптерећење апликативног сервера са Intel P4 2,4GHz процесором

На горњој слици представљено је оптерећење серверског процесора током релизације провере над 63 студента који су одговарали на 100 питања и бирали између 400 одговора. Уочава се да се вршно оптерећење појавило на почетку

3 Шимић Г., Јевремовић А., „Развој система за проверу знања студената у оквирима постојећег ИС универзитета“, 15. телекомуникациони форум Телфор 2007., Београд, 2007., CD издање

периода проверавања, тј. у тренутку преузимања питања и одговора.

У следећој верзији хардверске платформе, наведене компоненте су замењене бољим: процесор са 8 језгара типа *Intel Xeon* 3,2GHz и 8GB радне меморије (ECC).



Слика 2. Оптерећење процесора апликативног сервера са 8 језгара типа Intel Xeon 3,2GHz

Овом променом, уз додатно оптимизовање кода апликације (екстракција и енкапсулација учестало коришћених метода у статичке методе посебне класе, редукција позива брокерских класа према БП коришћењем унапред припремљених и парсираних *SQL* наредби), добијени су задовољавајући резултати, сликовито представљени на претходној слици. Достигнута је планирана брзина одзива система (на клијентској страни, у интранет окружењу) – боља од 5 секунди, са преко 100 студената, преко 500 питања и преко 2.000 одговора. Евентуална уска грла у будућој експлоатацији могу се јавити услед ограничене пропусне моћи комуникационих канала, што се може решити додавањем нових мрежних адаптера и оптимизацијом конфигурације диспечерске компоненте система.

5.4. Сервис електронске поште

Сервис електронске поште, поред Веб сервиса, представља најпопуларнији сервис на Интернету. Корени овог сервиса налазе се још у шездесетим годинама прошлога века (у *host-based* периоду рачунарства), у програмима који су омогућавали размену порука између различитих терминалских корисника једног мејн-фрејм рачунара. Касније су овакви изоловани системи умрежавани а софтвер за електронску пошту проширивани функцијама за размену порука између система различитих организација.

Процењује се[4] да је у току 2010. године сервис електронске поште користило око 1,88 милијарде људи, да је свакога дана у просеку слато око 294 милијарди електронских писама, односно да их је у току те године укупно послато око 107 хиљада милијарди. Такође се процењује да су три четвртине налога за електронску пошту намењене за личну, а само једна четвртина за пословну

4 Извор: www.pingdom.com, *Internet 2010 in numbers*

употребу. Данас сервис електронске поште представља моћан пословни и маркетиншки алат који се, међутим, често ненаменски користи - 89,1 процената електронских писама у 2010. години препознато је као спем (енгл. *spam*).

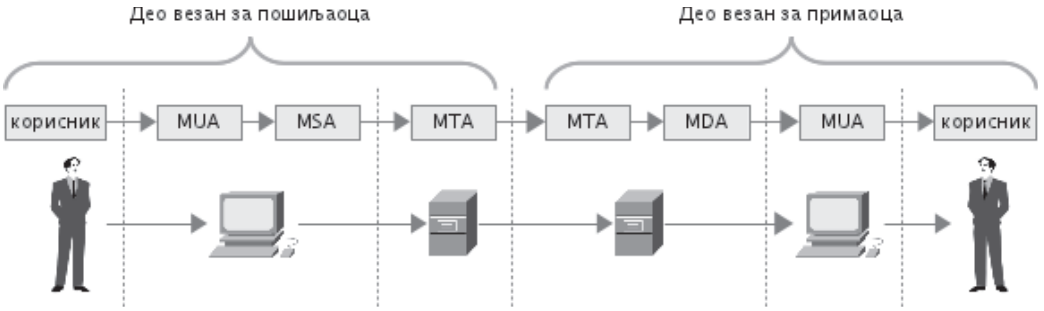
5.4.1. Архитектура сервиса електронске поште

Сервис електронске поште данас је у потпуности дефинисан одговарајућим софтверским компонентама и протоколима. Сам сервис електронске поште је организован по клијент-сервер архитектури унутар које постоје следећи типови агената у виду софтверских компонената:

- кориснички агент,
- агент за подношење порука,
- агент за пренос порука и
- агент за испоруку порука.

Поред наведених помпонената значајну улогу код овог сервиса игра и складиште порука (енгл. *Message Store, MS*) као компонента корисничког агента. Задатак ове компоненте је да прави архивске копије порука која се шаљу или преузимају у циљу омогућавања накнадног приступа корисника њима. Код већине популарних клијената за електронску пошту поруке су организоване у директоријуме.

Кориснички агент за електронску пошту (енгл. *Message User Agent, MUA*) је интерфејс између корисника и осталог дела сервиса електронске поште. Најчешће реализације овог софтвера су у виду десктоп или Веб апликације. Задатак корисничког агента је да кориснику омогући слање електронских порука другим корисницима, као и преглед електронских порука послатих од стране њих.



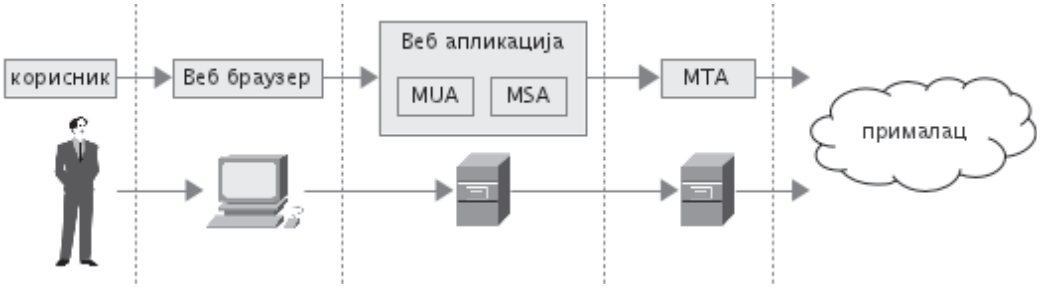
Слика 1. Архитектура и компоненте сервиса електронске поште

Агент за подношење порука (енгл. *Message Submission Agent, MSA*) прихвата поруку од корисничког агента, ставља је у формат прописан одговарајућим стандардима и прослеђује агенту за пренос порука. Овај процес обавља клијентску улогу протокола за пренос порука електронске поште.

Агент за пренос порука (енгл. *Message Transfer Agent*) представља серверску имплементацију протокола за пренос порука електронске поште. Овај процес прихвата поруке од стране корисничких агената за подношење порука или од других агената за пренос порука. У зависности од да ли представља коначно одредиште примљене поруке овај агент поруке прослеђује локалном агенту за испоруку порука или наредном агенту за пренос порука.

Агент за испоруку порука (енгл. *Message Delivery Agent*) задужен је за смештање поруке, примљене од последњег агента за пренос порука, у електронско поштанско сандуче примаоца (које може бити реализовано путем фајл-система, СУБП-а или на неки други начин). Испорука поруке у сандуче корисника не значи да је корисник њу истог тренутка прочитао, већ да је његовом корисничком агенту омогућен приступ поруци.

Два основна типа протокола које користи сервис електронске поште јесу протоколи за слање порука и протокол за приступ порукама у сандучету. Када су у питању протоколи за слање електронске поште, у пракси се готово увек користи једноставан протокол за пренос електронске поште (енгл. *Simple Mail Transfer Protocol, SMTP*). Са друге стране, када је у питању приступ корисничког агента сандучету са електронском поштом у пракси се користе релативно једноставан протокол за електронску пошту треће верзије (енгл. *Post Office Protocol version 3, POP3*) и нешто сложенији Интернет протокол за приступ порукама (енгл. *Internet Message Access Protocol, IMAP*).



Слика 2. Коришћење Веб апликације као клијента електронске поште

Неке од основних функција сервиса електронске поште директно зависе од система доменских имена. У ове функције спадају проналажење назива домаћина задуженог за размену електронске поште са одређеном

организацијом и превођење тог назива у одговарајућу адресу Интернет протокола. У случају да сервер доменских назива задужен за одређени Интернет домен не поседује информацију о томе који сервер је задужен за пријем и слање електронске поште, њена размена са адресама при том домену неће бити могућа.

У последњих неколико година знатно се популаризовало коришћење електронске поште путем клијената у виду Веб апликација (енгл. *Webmail*). Разлог томе је једноставније коришћење кроз елиминисање процеса инсталације десктоп апликације за електронску пошту, као и могућност коришћења апликације и порука са било ког рачунара који има приступ Вебу. Углавном најквалитетнији клијенти за електронску пошту у виду Веб апликација се корисницима нуде заједно са комплетном услугом електронске поште (*Google Mail, Hotmail, Yahoo*), с тим да постоји и велики број бесплатних Веб апликација ове намене (*Roundcube, Horde/IMP, Squirrel Mail, AtMail* и друге).

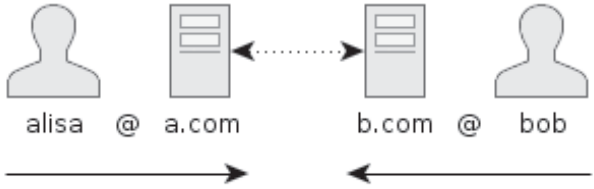
5.4.2. Адресовање електронске поште

Корени сервиса електронске поште везују се за размену порука између корисника мејнфрејм рачунара који су радили под *CTSS* (*Compatible Time-Sharing System*) оперативним системом (1961. година), развијеним на *MIT* универзитету. Ова размена порука првобитно је обављана путем фајл-система, складиштењем поруке у фајл назван по имену примаоца - на пример, „*to bob*" за корисника са именом Боб. Касније је у ту сврху развијен програм *mail* који је од 1971. године доступан и на *UNIX* оперативном систему. При свему томе треба имати у виду да су се сви корисници овакве размене порука, дакле и пошиљаоци и примаоци, налазили на истом рачунарском систему.

Слика 1. Корени електронске поште у размени порука на мејнфрејм системима

Од 1968. године активно је рађено на омогућавању слања порука између корисника рачунарских система повезаних на *ARPA* мрежу, а то је већ почетком 1972. године омогућено. Примаоца поруке је било потребно одредити у облику „корисник -at систем" а 1973. године је симбол „@" стандардизован[5] као сепаратор у адреси електронске поште.

5 RFC 469 - Network Mail Meeting Summary



Слика 2. Принцип адресовања електронске поште

Стандард за адресовање порука електронске поште данас[6] дефинише највише 64 *ASCII* карактера за идентификовање корисника (тзв. локални део, односно део пре знака @), с тим да је 2012. године стандард допуњен у циљу омогућавања коришћења међународних карактера[7].

Занимљив приступ у идентификовању примаоца има и Гугл провајдер сервиса електронске поште - тачка у адреси примаоца се не узима у обзир, тако да је власнику адресе:

```
racunarskemrezenet@gmail.com
```

могуће послати поруку и на адресу:

```
r.a.c.u.n.a.r.s.k.e.m.r.e.z.e.n.e.t@gmail.com
```

На овај начин семоже класификовати долазна пошта а одређене комбинације се могу користити на местима код којих се адреса лако може наћи на некој спем листи.

5.4.3. Поруке и протоколи

Структуру порука сервиса електронске поште чини омотач (енгл. *envelope*) у оквиру кога се налазе заглавље и садржај поруке. У заглављу поруке наслазе се описни параметри као што су адреса примаоца, наслов и слично. У телу поруке се налази њен садржај а оно може бити издељено у више делова. Тело поруке је подељено у јединице типа линије чија највећа дозвољена дужина износи 1.000 бајтова, укључујући и два бајта за крај линије.

Поруке сервиса електронске поште иницијало су могле бити састављене од првих 127 *ASCII* карактера, што је било погодно једино за енглеско говорно подручје. Додатно, није постојала ни могућност слања другачије кодованих фајлова у оквиру њих. Ова ограничења су довела до развоја Интернет стандарда

6 RFC 5322 - Internet Message Format

7 RFC 6531 - SMTP Extension for Internationalized Email

под називом **Вишенаменска проширења Интернет поште** (енгл. *Multipurpose Internet Mail Extensions, MIME*). Основна побољшања која нуди овај стандард односе се на коришћење симбола различитих језика у заглављу и телу порука и могућност придруживања различито кодованих фајлова.

5.4.3.1. SMTP - једноставан протокол за пренос електронске поште

Основни задатак једноставног протокола за пренос електронске поште (енгл. *Simple Mail Transfer Protocol, SMTP*) јесте да омогући поуздан и ефикасан пренос порука овог сервиса. Иако овај протокол није директно везан за протоколе нижег нивоа већ само захтева поуздан канал за пренос података, он се углавном користи у комбинацији са протоколом за контролу преноса, *TCP*.

Пре самог слања електронске поште потребно је успоставити двосмерни комуникациони канал између клијента и сервера. У случају да је порука адресована на вишеструке примаоце који се налазе на различитим доменима, задатак је клијента да успостави везе са серверима за електронску пошту сваког од њих. У случају да је једна порука адресована на вишеструке примаоце за чије је домене задужен исти сервер, клијент само један пут врши слање поруке.

Након успостављања везе са сервером клијент врши слање поруке путем низа наредби. Након што је пренос поруке извршен клијент може захтевати раскид успостављене везе или започети слање наредне поруке. Осим за слање поруке, веза са сервером електронске може се успостављати и за друге потребе, као што су провера исправности адресе примаоца или преузимање адреса чланова листе за електронску пошту.

```
MAIL FROM: "Adam Jones" <adam@jones.tld>
RCPT TO: "Danny Carrey" <danny@carrey.tld>
DATE: Fri 18 Feb 2005 16:27:01 GMT
SUBJECT: New song
Message-ID: 000a01c76701$b2a25600$f601f0d5@server
DATA
Danny, I believe that two notes would be enugh for entire song.

QUIT
```

Листинг 1. Наредбе *SMTP* протокола за пренос порука

Значајну карактеристику *SMTP* протокола представља и његова могућност да преноси поруке кроз вишеструке мреже. То значи да сервер који прима поруку може бити њено коначно одредиште или само посредник (релеј) у достављању поруке до њега, односно да достављање поруке примаоцу може бити извршено унутар једне директне везе или путем више веза између различитих сервера.

5.4.3.2. POP3 - протокол за електронску пошту

Протокол за електронску пошту (енгл. *Post Office Protocol version 3, POP3*) намењен је да корисничким апликацијама омогући преузимање и управљање порукама у сандучету електронске поште на серверу. У питању је једноставан, али и веома популаран протокол наведене намене.

Протокол за електронску пошту дефинише три стања везе: стање ауторизације, стање трансакција и стање ажурирања. Стање ауторизације почиње одмах након успостављања везе са сервером. У оквиру овог стања врши се утврђивање идентитета корисника на основу корисничког имена и лозинке које он доставља. Две основне наредбе у стању ауторизације су *USER* и *PASS* којима клијент задаје своје корисничко име и лозинку.

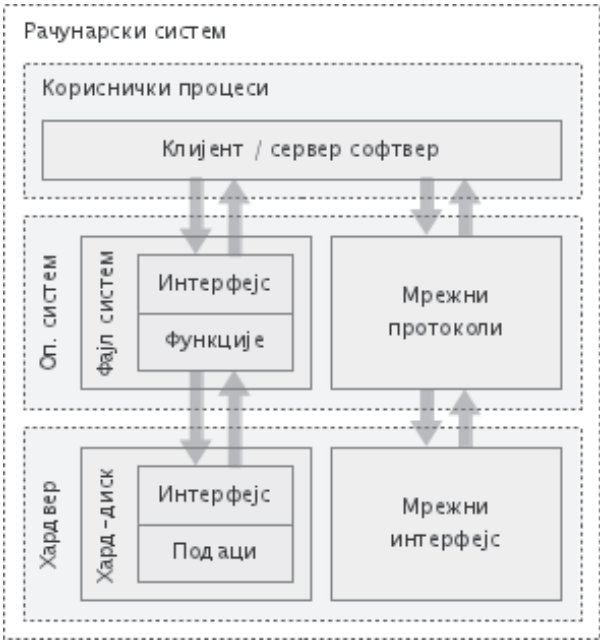
Након успешног утврђивања идентитета корисника прелази се у стање трансакција. Преласком у ово стање закључава се поштанско сандуче идентификованог корисника, односно онемогућава му се приступ из паралелних сесија. Унутар стања трансакције клијент може задавати следеће наредбе:

- *STAT* - захтева се исписивање тренутног статуса поштанског сандучета, односно броја порука у њему и њихове величине у бајтовима;
- *LIST* - захтева се преузимање заглавља порука у поштанском сандучету;
- *RETR* - захтева се преузимање комплетне поруке чији је редни број наведен након наредбе;
- *DELE* - захтева се означавање за уклањање поруке чији је редни број наведен након наредбе; овако означене поруке се уклањају након преласка везе у стање ажурирања;
- *RSET* - захтева се поништавање означавања порука за уклањање;
- *NOOP* - ова наредба нема никакву другу намену осим да се потврди веза између клијента и сервера да не би дошло до њеног аутоматског прекида након одређеног периода некативности;
- *QUIT* - захтева се прекид сесије, односно прелазак у стање ажурирања.

Веза прелази у стање ажурирања само уколико је у стању трансакција регуларно захтеван прекид везе. У току овог стања се уклањају за то означене поруке, искључава се поштанско сандуче и прекида се веза.

5.5. Сервиси за пренос фајлова

Основна улога рачунарских мрежа јесте размена података између (корисника) удаљених рачунарских система. Један од основних начина за складиштење података на рачунарским системима јесте у виду фајлова, односно коришћењем фајл-система. Фајл-системи се најчешће користе за складиштење података на екстерној меморији, мада се због једноставне употребе понекад користе и за рад са подацима у радној меморији, или као интерфејс за одређена стања и функције оперативног система. Две основне компоненте фајл-система су формат записа података на екстерној меморији и имплементација функција за рад са фајловима унутар оперативног система.



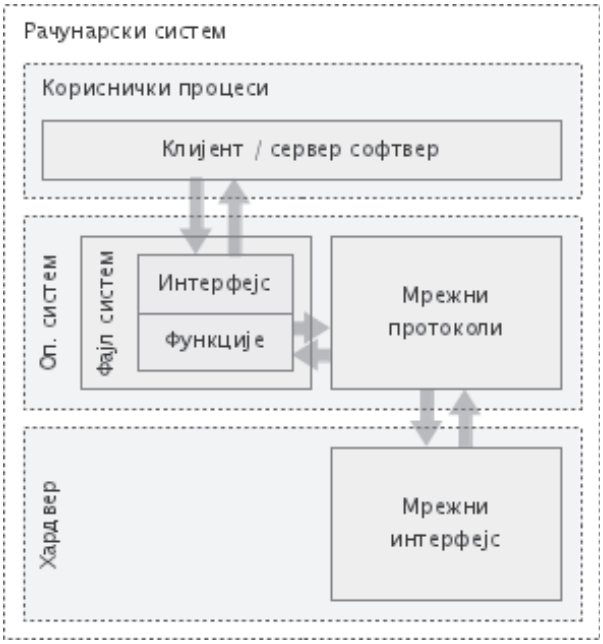
Слика 1. Пренос фајлова путем протокола у корисничком софтверу

Током историје развоја рачунара развијен је велики број различитих фајл-система. Неки од њих су заштићени и комерцијално доступни, док су неки отворени и јавно доступни. У пракси је могуће премештати податке са једног фајл-система на други али се тиме губе сви атрибути фајлова које одредишни фајл-систем не подржава. Најпопуларнији фајл-системи данас су *Extented*

filesysem (верзије 2, 3 и 4), *Reiserfs*, *XFS*, *JFS*, *Btrfs*, *NTFS*, *VFAT*, као и *ISO 9660* фајл-систем за компакт и дигиталне видео дискове.

За пренос фајлова путем рачунарских мрежа углавном се користе два приступа. Први подразумева коришћење клијент-сервер архитектуре, односно софтверских компонената које на захтев корисника шаљу фајлове серверу, преузимају их са њега или над њима извршавају неку другу операцију (уклањање, премештање у други директоријум и слично).

Други приступ за пренос фајлова путем мреже подразумева реализацију једног дела фајл-система у виду мрежног протокола. Код овог приступа се интерфејс фајл-система ка остатку локалног рачунарског окружења реализује као и када су у питању локални фајл-системи али се складиштење података са локалне екстерне меморије измешта на удаљени рачунарски систем, доступан коришћењем одговарајућих мержних протокола.



Слика 2. Пренос фајлова путем мрежног фајл-система

У овом поглављу обрађено је неколико типичних протокола за пренос фајлова путем рачунарских мрежа. Као свакако најпопуларнији протокол те намене обрађен је пороткол за пренос фајова (*FTP*). Затим, обрађени су мрежни фајл-системи који се користе на данас популарним оперативним системима - мрежни фајл-систем (*NFS*) на *UNIX* оперативним системима и општи Интернет фајл-систем на оперативним системима компаније Мајкрософт.

5.5.1. FTP - протокол за пренос фајлова

Протокол за пренос фајлова (енгл. *File Transfer Protocol, FTP*) је протокол намењен размени фајлова између рачунара који имају подршку за *TCP/IP* протокол. *FTP* је клијент-сервер протокол што значи да се његова примена врши путем серверског програма на серверу и клијентске апликације на клијенту. Постоји велики број серверских и клијентских реализација за различите оперативне системе и углавном су бесплатне.

Основни циљеви *FTP* протокола су:

- омогућавање размене фајлова између рачунара
- омогућавање индиректног коришћења удаљених рачунара
- заштита корисника од различитих варијација код складиштења фајлова на различитим системима поуздан и ефикасан пренос фајлова

Основне мане *FTP* протокола су:

- Приступне лозинке и садржај фајлова се мрежом преносе у изворном облику што га чини небезбедним.
- За сваку операцију (повезивање, преузимање фајлова, листање садржаја, постављање фајлова) се користи засебна *TCP/IP* конекција што може изазвати проблеме уколико се пренос обавља посредством рачунара са *firewall*-ом.
- Постоји могућност "узнемиравања" 3. рачунара при одређеним захтевима преко проху сервера.
- *FTP* је веома латентан протокол услед великог броја команди потребних за иницирање трансфера.
- Не постоји уграђена могућност провере интегритета пренешеног фајла тако да се ово најчешће обавља засебно преко *md5* фајла.

5.5.1.1. Сигурни *FTP*

Главни безбедносни недостаци *FTP* протокола су:

1. Корисничко име и лозинка се преко мреже преносе у изворном облику.
2. Подаци који се преносе протоколом преносе се у изворном облику.

Ови недостаци не представљају проблем код локалних мрежа чији се

комуникациони канали најчешће сматрају безбедним. Међутим, коришћење *FTP* протокола путем мреже чије је канале могуће прислушкивати (нпр. Интернет) отвара следеће безбедносне ризике:

1. Нападач може утврдити које операције је корисник извео на серверу.
2. Нападач може утврдити садржај фајлова који су пренешени *FTP* прокотоколом (у оба смера).
3. Нападач може утврдити корисничко име и лозинку корисника.

Услед поменутих безбедносних ризика при коришћењу *FTP*-а, појавиле су се две различите имплементације сигурног *FTP*-а:

1. *SFTP* (*SSH File Transfer Protocol*) - *FTP* базиран на *SSH* (*Secure SHell*) протоколу.
2. *FTPS* (*File Transfer Protocol over SSL*) - *FTP* са коришћењем *SSL* или *TLS* енкрипције.

5.5.2. NFS - мрежни фајл-систем

Мрежни фајл-систем (енгл. *Network File System, NFS*) најчешће је коришћени фајл-систем овог типа на *UNIX* оперативним системима. Развила га је компанија Сан Мајкросистемс.

Мрежни фајл-систем је реализован на клијент-сервер архитектури. То значи да рачунар на коме се налазе путем мреже доступни фајлови поседује серверску софтверску компоненту, а рачунари који тим фајловима приступају путем мреже клијентске софтверске компоненте.

5.5.3. CIFS - општи Интернет фајл-систем

SMB (*Server Messages Block*) је протокол апликативног слоја *OSI* модела и најчешће се користи за размену фајлова, дељење штампача и серијских портова између рачунара на мрежи. Углавном се користи на рачунарима под *MS Windows* оперативним системима. *SMB* је оригинално представљен од стране *IBM*-а са циљем да од *DOS*-овог "*Interrupt 33*" локалног приступа фајловима направи мрежни фајл систем. Међутим, опште распрострањена варијанта *SMB*-а је прилично измењена од стране компаније Мајкрософт. Ова компанија је 1998. године лансирала иницијативу за промену имена *SMB*-а у *CIFS* (*Common Internet File System*) јер је у *SMB* додато мноштво нових могућности: симболички и тврди линкови, већа величина фајлова и покушај да се комуникација остварује директно, без коришћења *NetBios*-а.

SMB је оригинално дизајниран да ради на *NetBios* протоколу (који ради на *NetBEUI*, *IPX/SPX* или *NBT* протоколу) а од *MS Windows* 2000 оперативног система *SMB* може да ради и на *TCP/IP* протоколу. Услед неопходности за комуникацијом са системима под *MS Windows* оперативним системима, *SMB* је портован и на *Unix* оперативне системе у оквиру *Samba* пројекта. Такође, постоје и друге, мање популарне имплементације *SMB* протокола намењене различитим оперативним системима.

CIFS (*Common Internet File System*) представља новију верзију *SMB*-а која подржава меко и тврдо линковање, нуди функционалности које нису доступне у *SMB*-у и ради на *TCP/IP* уместо *NetBios* протоколу. Компанија Мајкрософт је 1996. године након увођења поменутих новина у *SMB* протокол покренула иницијативу за преименовање *SMB* протокола у *CIFS*. Спецификација 1.0 верзије *CIFS* протокола је достављена *IETF* групи за стандардизацију а Мајкрософт такође сарађује на примени овог протокола и са осталим заинтересованим странама. Превођење са *NetBios* на *TCP/IP* протокол омогућава *CIFS* протоколу рад на Интернет мрежи уз коришћење *DNS* система за адресовање чланова. У мрежама са више клијената проблем конкурентног приступа фајловима *CIFS* решава интерним системима закључавања.

5.6. Сервиси за администрацију мреже

На исти начин као што се „бирократија шири да би одговорила на потребе бирократије која се шири“ тако се и на пољу рачунарских мрежа појављују нови сервиси који имају за циљ да олакшају одржавање и развој рачунарских мрежа. Постоји велики број специјализованих административних сервиса произвођача комерцијалних решења на пољу рачунарских система и мрежа. За такве сервисе њихови произвођачи обично дају обимну документацију која покрива све детаље који су значајни за њихово коришћење. У овом поглављу обрађена су два честа и отворена инфраструктурна сервиса рачунарских мрежа: протокол мрежног времена и протокол за једноставно управљање мрежом.

5.6.1. NTP - протокол мрежног времена

У рачунарским мрежама које чине сервери различитог типа (апликативни, комуникациони, базе података) или кластери сервера, често је потребно остварити прецизну временску синхронизацију између свих чланова мреже. На пример, уколико у серверској мрежи једне банке постоје два сервера за базе података од којих је један задужен за евидентирање уплата на рачуне клијената а други за евидентирање исплата са истих рачуна, временска несинхронизованост ова два сервера касније може условити нетачне

информације везане за редослед уплата и исплата. Иако на први поглед временска синхронизација не представља велики проблем за њено остваривање је потребно:

1. обезбедити систем за тачан пренос времена пакетским преносом, без утицаја променљивог времена потребног за пренос пакета,
2. иницијално синхронизовати време на часовницима свих рачунара у мрежи и
3. прериодично вршити синхронизацију да би се неутралисале разлике настале у међувремену.

Задатак протокола мрежног времена (енгл. *Network Time Protocol, NTP*) јесте да омогући синхронизацију времена на часовницима рачунара у мрежи.

```
bash3.1# /usr/sbin/ntpdate ntp.nasa.gov
15 Mar 12:02:46 ntpdate[]: step time server 198.123.30.132 offset 1.914867
sec
bash3.1# /sbin/hwclock systohc
```

Листинг 1. Пример синхронизације локалног часовника

Протокол мрежног времена је протокол апликативног нивоа који за рад користи услуге *UDP* протокола транспортног нивоа, подразумевано на порту 123. Један од главних проблема везан за синхронизацију времена путем рачунарских мрежа јесте варијабилност времена потребног да се подаци са *NTP* сервера пренесу до клијента. За решавање овог проблема у *NTP* протоколу користи се алгоритам који је Кејт Марцуло представио 1984. године у оквиру своје докторске дисертације. Више информација о овом алгоритму се може наћи на Веб сајту аутора[8].

За коришћење *NTP* протокола је потребно имати *NTP* сервер у локалној мрежи или користити неки од јавно доступних *NTP* сервера на Интернету (на пример, *ntp.nasa.gov*). Такође, један од најбољих приступа јесте подешавање аутоматске периодичне синхронизације часовника на свим клијентима. С обзиром на то да процес синхронизације не захтева значајне мрежне, процесорске и меморијске ресурсе период између синхронизација се може поставити и веома кратким, посебно у ситуацијама код којих је веома прецизна синхронизација времена неопходна, или код којих интерни часовници рачунара показују знатна одступања у кратком временском периоду. Међутим, у случају таквих знатних

8 http://www.cse.ucsd.edu/users/marzullo

одступања потребно је проверити исправност самог хардвера, као и подешавања оперативног система.

```
bash3.1# ls /sys/devices/system/clocksource/clocksource0/
available_clocksource  current_clocksource
bash3.1# cat /sys/devices/system/clocksource/clocksource0/
current_clocksource
hpet
```

Листинг 2. Утврђивање хардверског извора времена на Линукс систему

Треба имати у виду и то да неки сложени софтверски сервиси свој рад заснивају на вођењу дневника у којима се за сваку акцију евидентира време њеног извршења у секундама или милисекундама. Проблем који се код таквих сервиса може јавити потиче из ситуације у којој се синхронизацијом времена време на интерном часовнику рачунара (на коме се поменути процес извршава) „враћа уназад“. Таква синхронизација може резултовати тиме да накнадне акције имају забележено раније време извршавања од претходно евидентираних акција, што даље може довести до неисправног рада сервиса или његовог потпуног отказивања.

5.6.2. SNMP - протокол за једноставно управљање мрежом

од једноставних рачунарских мрежа са малим бројем чланова углавном није тешко утврдити да се јавио проблем и шта је узрок проблема. Међутим, код комплексних рачунарских мрежа које чини велики број чланова често је неопходно, а уз то и веома компликовано, предвидети могуће проблеме, утврдити да је до проблема на мрежи дошло и утврдити његову локацију и узрок. Улога протокола за једноставно управљање мрежом (енгл. *Simple Network Management Protocol*) јесте да администраторима обезбеди информације везане за рад рачунарске мреже, а које је могуће искористити за спречавање и решавање проблема у њеном раду.

За коришћење *SNMP* протокола у мрежи потребно је обезбедити одговарајуће карактеристике мреже. Протокол *SNMP* се у мрежама омогућава путем три типа компонената: мрежних уређаја са подршком за управљање *SNMP*-ом (енгл. *managed device*), *SNMP* агената и система за управљање мрежом (енгл. *Network Management System, NMS*).

Мрежни уређаји са подршком за *SNMP* управљање су чланови мреже који садрже *SNMP* агенте. Ови уређаји креирају базу података која садржи

информације о њиховом раду у протеклом периоду. Подаци из ове базе су доступни систему за управљање мрежом (*NMS*) путем *SNMP* протокола. Улога *SNMP* агената је да податке из базе података мрежног уређаја преведе у облик дефинисан *SNMP* протоколом као и да контролне податке добијене од *NMS* система примени на локалном уређају. Задатак *NMS* система јесте да информације добијене од *SNMP* агената анализирају као и да контролишу мрежне уређаје. У једној *SNMP* мрежи се може налазити и више *NMS* система. Такође, с обзиром на хијерархијску структуру *SNMP* мрежа, један мрежни уређај може истовремено функционисати и као *SNMP* агент и као *NMS*.

Један од главних проблема везаних за *SNMP* протокол јесте недостатак провере аутентичности у оба смера. Из тог разлога већина произвођача мрежне опреме у уређаје уграђује само могућност давања *SNMP* информација без могућности подешавања рада уређаја путем *SNMP*-а.

5.7. Сервиси за рад на удаљеном рачунару

Једно од наслеђа од мејнфрејм периода рачунарских телекомуникација је и потреба за коришћење услуга удаљених рачунарских система путем основног корисничког интерфејса, алфанумеричког или графичког. Један од првих сервиса ове намене био је Телнет, сервис који је омогућавао конзолни рад на удаљеном рачунару, а који је касније унапређен у виду *Secure Shell* сервиса. Један од првих сервиса који је омогућавао дистрибуирани графички кориснички интерфејс јесте *X Window System* на *UNIX* оперативним системима. У овом поглављу је поред наведених конзолних сервиса обрађен и сервис виртуалног мрежног рачунарства (енгл. *Virtual Network Computing, VNC*).

5.7.1. Телнет

Основна улога телнет сервиса јесте да омогући рад корисника на удаљеним рачунарима (најчешће под *UNIX* оперативним системом). Овај сервис је изграђен на клијент-сервер архитектури што значи да захтева од корисника поседовање клијентске апликације и да на рачунару на који корисник жели да се повеже буде инсталирана серверска компонента сервиса. Након успостављања иницијалне везе телнет протокола овај сервис поприма карактеристике хост-басед архитектуре. То значи да свака операција од стране клијента (нпр. притисак тастера на тастатури) се истовремено прослеђује серверу. На тај начин корисник може обављати операције на удаљеном рачунару на исти начин као да седи директно испред рачунара и користи локалну тастатуру и монитор.

Један од главних разлога зашто се данас телнет ретко користи за удаљени приступ рачунарима јесте појава графичког корисничког интерфејса за који овај протокол није дизаниран. Додатни разлог пада популарности овог сервиса јесте безбедност. Телнет протокол све акције корисника (укључујући и слање корисничког имена и лозинке) и резултате инструкција шаље у изворном облику што га чини небезбедним за коришћење на мрежама чије је канале могуће прислушкивати.

Без обзира на све ређу употребу телнет сервиса за рад на удаљеним рачунарима већина модерних оперативних система данас се испоручује са укљученом клијентском компонентом. Разлог овоме јесте могућност коришћења телнет клијента за приступ серверским компонентама осталих сервиса.

5.7.2. SSH - безбедна љуска

SSH (*Secure Shell*) протокол омогућава безбедан приступ и рад на удаљеним рачунарским системима [RFC4251]. Првенствено се користи на *UNIX* базираним оперативним системима. Три основне компоненте овог протокола чине протокол транспортног слоја, протокол за проверу аутентичности и протокол везе.

Протокол транспортног слоја који обезбеђује аутентичност, интегритет и поверљивост најчешће користи услуге *TCP/IP* протокола али се могу искористити и остали протоколи који омогућавају поуздан пренос података. Улога овог протокола је да омогући безбедан канал користећи небезбедну инфраструктуру. Овај протокол обезбеђује и јединствени идентификатор сесије који се може користити од стране протокола вишег нивоа.

Протокол за проверу аутентичности корисника на клијентској страни такође функционише на транспортном нивоу. Механизми овог протокола користе поменути идентификатор сесије који обезбеђује протокол транспортног слоја.

Протокол везе који мултиплексује шифровани тунел у више логичких канала лежи на протоколу за аутентичност.

Протокол везе који обезбеђује канале који се могу користити за различите примене, најчешће за сесије алфануемеричког корисничког интерфејса и тунеловање *X11* протокола. У оквиру *SSH* протокола алгоритми и методи за шифровање, проверу интегритета, израчунавање хеш вредности, компресију и размену кључева дефинисани су по називу. Неки од алгоритама су обавезни за све имплементације. У оквиру спецификације алгоритма подразумевана је

могућност проширивања скупа алгоритама одређене намене сопственим алгоритмом.

Сесијски кључеви се код *SSH* протокола генеришу коришћењем (псеудо)случајног генератора. Квалитет овог генератора један је од пресудних фактора безбедности коју нуди *SSH* протокол.

SSH протокол може бити рањив нападима ускраћивања услуге. Релативно захтевне процедуре на серверу нападач може искористити за заузимање меморијских и процесорских ресурса сервера. Ово питање првенствено зависи од конкретне имплементације проткола.

5.7.3. Дистрибуирано превођење *C* програмског језика

Један од интересантних примера коришћења рачунарских мрежа за дистрибуирану обраду података је и компајлер за дистрибуирано превођење *C* програмског језика - *DISTCC* (*Distributed C Compiler*). Овај програм подразумева инсталирање агената на свим или одабраним рачунарима у мрежи. Ти агенти ослушкују на додељеном порту и, када добију захтев, започињу локално превођење кода у *C* програмском језику на машински језик. Друга компонента овог решења јесте локални диспечер, односно програм који на захтев за превођењем дели изворни код, прослеђује га осталим рачунарима у мрежи и склапа добијене резултате. У случајевима рачунарских мрежа са доста чланова овакав приступ може убрзати превођење обимних програма и неколико стотина пута.

5.8. Мултимедијални сервиси

Убрзан развој рачунарских технологија довео је до могућности коришћења и обраде мултимедијалних садржаја на рачунарима. Додатно, паралелан развој рачунарских и телекомуникационих технологија омогућио је капацитете комуникационих канала довољне за пренос мултимедијалних садржаја високе резолуције, чак и у реалном времену. У овом поглављу су представљена два основна сервиса за удаљену комуникацију коришћењем рачунарских мрежа - Интернет телефонија и видео конференције.

5.8.1. Интернет телефонија

Интернет телефонија представља један од сервиса који се могу користити путем Интернет мреже и мрежа заснованих на Интернет технологијама. Овај сервис се

често среће и под називом „глас преко Интернет протокола“ (енгл. *Voice over IP, VoIP*). Основни задатак Интернет телефоније је да омогући миграцију популарних сервиса са јавне телефонске мреже (пренос гласа и факсимила) на Интернет технологије.

Интернет телефонија се реализује коришћењем више различитих затворених и отворених протокола. Историјски најзначајнији сет протокола за реализацију Интернет телефоније је *H.323*, као *ITU-T* препорука из 1996. године. Овај сет протокола омогућују пренос гласа и видео сигнала а подржан је у већини система за Интернет телефонију и видео-конференције. Поред *H.323* протокола у пракси се све чешће среће и *Session Initiation Protocol (SIP)* као протокол за успостављање и контролу сесија Интернет телефоније.

Једна од за овај рад најзначајнијих карактеристика Интернет телефоније је коришћење *IP* протокола од стране протокола који се користе за њену реализацију. То значи да се реализацијом система заштите на нивоу *IP* протокола могу штитити и подаци комуникационих сесија Интернет телефоније.

5.8.2. Видео конференција

Сервис видео-конференција омогућава пренос аудио и видео материјала у реалном времену са циљем омогућавања одржавања састанака између особа које се налазе на две или више удаљених локација. Сви учесници видео-конференција су опремљени дисплејима са звучницима за репрезентовање материјала који друга страна шаље као и камерама са микрофонима за слање порука другој страни. Учесници видео конференција могу бити појединци са личном опремом али и групе у специјално опремљеним салама. Опрема и софтвер који се користе за видеоконференције крећу се у распону од испод сто па до неколико хиљада долара у зависности од квалитета и могућности које нуде. Највећу корист од видео конференција имају пословне организације које на овај начин могу остварити значајну уштеду штедећи новац и време потребно за путовање на локацију на којој би се одржала стандардна конференција.

За коришћење услуге видео конференције је осим адекватног хадвера и софтвера потребно имати и везу са другом страном (или другим странама) која поседује капацитет потребан за пренос аудио и видео порука у реалном времену. Софтвер и уређаји који се користе код видео конференција углавном подржавају компресовање и декомпресовање аудио и видео материјала у циљу што ефикаснијег искоришћења комуникационог канала. Код комуникационих канала мале пропусне моћи углавном се прибегава компромису у погледу квалитета аудио/видео порука.

Већина производа који се користе за одржавање видео конференција базира се на интерним стандардима произвођача тако да комбиновање решења различитих произвођача најчешће није могуће. Тренутно најчешће коришћени јавни стандарди за кодирање аудио/видео порука су: *H.320*, *X.323* и *MPEG-2*. Ови стандарди међусобно нису компатибилни али постоје апликације које омогућавају коришћење више од једног стандарда.

Посебан вид видео конференција јесте *Webcasting*. Он омогућава једносмерни пренос аудио/видео материјала, од сервера ка клијентима. Аудио/видео материјал се креира и поставља на сервер а клијенти затим приступају материјалу. За овај вид видео-конференција тренутно не постоје формални стандарди али на тржишту постоји већи број решења базираних на де-факто стандардима.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

004.7(075.8)

ВЕИНОВИЋ, Младен, 1962-
Рачунарске мреже / Младен Веиновић, Александар Јевремовић. - 7. изд.
- Београд : Универзитет Сингидунум, 2020 (Београд : Бирограф). - IX, 212
стр. : илустр. ; 24 cm

На врху насл. стр.: Факултет за информатику и рачунарство. - Тираж 1.500.

ISBN 978-86-7912-626-9

1. Јевремовић, Александар, 1983- [autor]

а) Рачунарске мреже

COBISS.SR-ID 282670860

www.singidunum.ac.rs

9 788679 126269

Младен Веиновић
Александар Јевремовић

РАЧУНАРСКЕ МРЕЖЕ

Уџбеник „Рачунарске мреже" намењен је студентима Факултета за информатику и рачунарство Универзитета Сингидунум за припрему испита из предмета „Рачунарске мреже", а може се користити и као уводни материјал за савладавање градива из предмета који се односе на Интернет технологије и Веб сервисе. Резултат је вишегодишњег искуства аутора у областима умрежавања, мрежног и Интернет програмирања, комуникација и заштите података у рачунарима и рачунарским мрежама. Поред своје основне намене уџбеник може да буде од користи свим инжењерима који се у пракси сусрећу са умрежавањем, пројектовањем, инсталацијом и администрирањем рачунарских мрежа.

Читаоци ће у овом уџбенику наћи основне концепте и принципе умрежавања, опис слојевите архитектуре и функције појединих слојева као и њихове протоколе, али и детаљне приказе најважнијих Интернет протокола и Веб сервиса на апликативном нивоу. Програмерима ће бити од користи за боље разумевање различитих технологија за развој мрежних апликација које се ослањају на системске позиве и наменске библиотеке чијом применом се поштују строго дефинисани стандарди у савременим рачунарским мрежама.

Универзитет Сингидунум