Верица Васиљевић

Рачунарске мреже

Висока школа електротехнике и рачунарства
струковних студија
Београд, 2008.

Аутор: др Верица Васиљевић

Рецензенти: проф. др Душан Драјић, проф. др Зоран Петровић

Издавач: Висока школа електротехнике и рачунарства струковних студија

За издавача: др Драгољуб Мартиновић

Лектор: Анђелка Ковачевић

Техничка обрада: Верица Васиљевић, Ана Милетић, Веселин Илић, Никола Кајгана, Мирко Ступар

Дизајн: Мирко Ступар

Штампа: Грид, Београд

Тираж: 220

Наставно веће Високе школе електротехнике и рачунарства струковних студија у Београду, на седници одржаној 21.8.2007. године, одобрило је издавање и примену овог уџбеника у настави.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

004.7 (075.8)

ВАСИЉЕВИЋ, Верица
Рачунарске мреже / Верица Васиљевић. - Београд ; Висока школа електротехнике и рачунарства струковних студија, 2008. (Београд : Грид). - VIII, 347 стр. ; илустр. ; 24 cm

Тираж 220. - Напомене уз текст, -
Библиографија: стр. 350 - 354. - Регистар,
- - Рачунарске мреже [Електронски извор] / Верица Васиљевић. - 1 електронски оптички диск (CD-ROM) ; 12 cm

ISBN 978 - 86 - 85081 - 96 - 5

а) Рачунарске мреже
COBISS.SR - ID 143348748

Предговор

Уџбеник Рачунарске мреже првенствено је намењен студентима Високе школе електротехнике и рачунарства струковних студија у Београду. Настао је као резултат дугогодишњег рада на настави из предмета Рачунарске мреже.

Уџбеник се састоји од осамнаест целина, методички обрађених.

Да би се студентима омогућило да што квалитетније и са више мотива самостално уче припремљен је и мултимедијални уџбеник организован као хипертекст. Сви цртежи су анимирани и озвучени нарацијом.

Београд,
фебруар, 2008.

Аутор

Садржај

1. УВОД **1**
Коришћење рачунарских мрежа 2
Класификација рачунарских мрежа 4
Стандарди 7

2. КОМУТАЦИОНЕ ТЕХНИКЕ **9**
Комутација канала 13
Комутација порука 14
Комутација пакета 16
Поређење комутационих техника 19
Штафетни пренос рамова 20
Мреже са комутацијом ћелија 20

3. СЛОЈЕВИТА АРХИТЕКТУРА ПРОТОКОЛА **22**
OSI референтни модел 25
TCP/IP референтни модел 27
Референтни модел Novell Netware 32
ATM референтни модел 32

4. КОМУНИКАЦИОНИ МОДЕЛ **34**
Пренос података 35
Веза између брзине података и опсега 40
Снага сигнала 43

5. АНАЛОГНИ И ДИГИТАЛНИ ПРЕНОС ПОДАТАКА **46**
Подаци 46
Сигнали 47
Пренос 50
Трансмисиони параметри 51
Капацитет канала 55

6. ТРАНСМИСИОНИ МЕДИЈУМИ **58**
Жични медијуми 59
Упредене парице 60
Коаксијални каблови 62
Оптички каблови 64
Бежични пренос 68

Земаљске микроталасне везе 70
Сателитске микроталасне везе 71
Радио-везе 74
Пренос у инфрацрвеном опсегу 74
Бежично простирање 75

7. ПРЕТВАРАЊЕ (КОДИРАЊЕ) ПОДАТАКА 77
Дигитални подаци, дигитални сигнали 78
Модулациона брзина 84
Технике уношења прекршаја биполарности 84
Дигитални подаци, аналогни сигнали 86
Аналогни подаци, дигитални сигнали 91
Аналогни подаци, аналогни сигнали 94
Системи са проширеним спектром 100

8. МУЛТИПЛЕКСИРАЊЕ 105
Фреквенцијски мултиплекс 106
Аналогни системи за пренос 110
Мултиплексирање по таласним дужинама 110
Синхрони временски мултиплекс 112
Дигитални системи за пренос 114
Интерфејси за пренос оптичким влакнима 116
Статистички временски мултиплекс 117
Локалне рачунарске мреже са оптичким влакнима 120

9. МОДЕМИ 122
Телефонска мрежа 122
Модеми за телефонски канал 124
Асиметричне дигиталне претплатничке петље 132
Кабловски модеми 141

10.КОМУНИКАЦИОНЕ ТЕХНИКЕ ДИГИТАЛНИХ ПОДАТАКА 145
Синхронизација у преносу података 145
Типови грешака 149
Интерфејси 155
Стандард V.24/EIA-232-F 157
Интерфејс у дигиталној мрежи интегрисаних услуга 164

11. УПРАВЉАЊЕ СЛОЈЕМ ВЕЗЕ 166
Линијска конфигурација 166
Контрола тока 172
Контрола грешке 172

Бит оријентисани протоколи 176
Основне карактеристике протокола HDLC 177

12.АРХИТЕКТУРА ЛОКАЛНИХ РАЧУНАРСКИХ МРЕЖА 186
Методи приступа трансмисионом медијуму 186
Стандард IEEE 802 за локалне рачунарске мреже 196
Етернет 198
Стандард IEEE 802.3 199
Повезивање у IEEE 802.3 локалним рачунарским мрежама 201
Стандард IEEE 802.3u 202
Етернет брзине 1Gb/s 204
Етернет брзине 10Gb/s 206
Стандард IEEE 802.4 - магистрала са жетоном 208
Стандард IEEE 802.5 - прстен са жетоном 209
Протокол за управљање логичком везом 212

13. БЕЖИЧНЕ РАЧУНАРСКЕ МРЕЖЕ 215
Бежичне локалне рачунарске мреже 216
Топологије бежичних локалних рачунарских мрежа 216
Технологије бежичних локалних рачунарских мрежа 218
Стандарди серије IEEE 802.11 220
Архитектура IEEE 802.11 220
Протоколи MAC подслоја IEEE 802.11 222
Структура рама стандарда IEEE 802.11 226
Услуге IEEE 802.11 227
Физички слој стандарда IEEE 802.11 229
Бежичне персоналне мреже 232
Стандард Bluetooth 232
Стандарди за персоналне мреже IEEE организације 241
Стандарди за широкопојасне мреже 242
Међусобно упоређивање бежичних система 247

14. МЕЂУСОБНО ПОВЕЗИВАЊЕ РАЧУНАРСКИХ МРЕЖА 251
Комутиране локалне рачунарске мреже 251
Комутација на слоју везе 252
Локално, међусобно повезивање рачунарских мрежа 256
Принцип рада комутатора слоја 2 263
Комутатори слоја 3 265
Поређење мостова и рутера 266
Виртуелне локалне рачунарске мреже 267
Стандард IEEE 802.1Q 272

15. ИНТЕРНЕТ ПРОТОКОЛ **275**
Формат заглавља IP пакета верзије 4 275
Адресирање на Интернету 278
Адресирање подмрежа 280
Динамичко конфигурисање протокола 286
Интернет протокол верзије 6 288
Формат заглавља IP пакета верзије 6 290

16. РУТИРАЊЕ **296**
Процес рутирања 298
Протоколи за рутирање и аутономни системи 300
Алгоритми за рутирање 301
Динамичко рутирање 302
Протокол за рутирање између аутономних система 305
Бескласно рутирање између домена 306

17. ТРАНСПОРТНИ СЛОЈ TCP/IP РЕФЕРЕНТНОГ МОДЕЛА **308**
Услуге које пружа транспортни слој 309
Елементи транспортног протокола 312
Транспортни протокол и поуздана мрежна услуга 313
Транспортни протокол без успоставе везе 333

18. АПЛИКАЦИОНИ СЛОЈ TCP/IP РЕФЕРЕНТНОГ МОДЕЛА **334**
Систем имена домена 335

ИНДЕКС ПОЈМОВА **340**

ЛИТЕРАТУРА **348**

1. Увод

Сваки од претходна три века у развоју људске цивилизације био је доминантан по некој од технологија. 18. век познат је као индустријска револуција, 19. век је век парних машина. У 20. веку кључна технологија је сакупљање, обрада и дистрибуција информација, доминантна је и инсталација у целом свету распрострањене телефонске мреже, затим проналазак радија и телевизије, појава и изузетно ширење рачунарске индустрије и лансирање комуникационих сателита.

Као последица брзог технолошког прогреса ове области рапидно се међусобно приближавају и разлике између сакупљања, преношења, смештања и обраде информација брзо нестају. Организације са хиљадама пословница распрострањених на широком географском подручју очекују да притиском на дугме могу да добију податке и са најудаљенијих локација. Будући да способност сакупљања, обраде и дистрибуције информација расте повећавају се захтеви за софистицираном обрадом информација.

Иако је рачунарска индустрија млада у поређењу са осталим индустријама развој и примена рачунара достигли су спектакуларни напредак у кратком времену. У време прве две декаде постојања рачунарски системи били су високоцентрализовани, обично у оквиру једне велике просторије. Средње компаније, по величини, или универзитети могли су имати један или два рачунара, док су велике институције могле имати неколико рачунара. Идеја да ће за двадесет година рачунари једнаке моћи бити мањи од поштанске марке и да ће се масовно производити изгледала је као научна фантастика.

Повезивања рачунара и комуникација имало је дубоког утицаја на начин како су рачунарски системи организовани. Концепт рачунског центра као собе са великим рачунаром, где су корисници доносили податке на обраду, сада је потпуно застарео. Стари модел једног рачунара који опслужује целокупну рачунарску обраду у оквиру организација замењен је системом у коме велики број просторно раздвојених а међусобно повезаних рачунара обавља посао. Овај систем назива се рачунарска мрежа.

Користићемо термин „рачунарска мрежа" који означава међусобно повезани скуп аутономних рачунара. За два рачунара каже се да су повезани уколико су у могућности да размењују информације. Комуникација не мора да буде преко бакарних жица: могу да се користите и оптичка влакна, микроталаси и комуникациони сателити. Захтевајући да рачунар буде аутономан издвајамо га из господар/слуга релације [1]. Уколико неки рачунар укључује, искључује или њим управља други рачунар он није аутономан. Систем са једном управљачком целином и великим бројем „робова" није мрежа; није то ни рачунар са удаљеним штампачима и терминалима.

У литератури постоји конфузија између појма рачунарске мреже и појма дистрибуирани системи. Кључна разлика је у томе што за дистрибуирани систем постојање више аутономних рачунара није видљиво кориснику. Корисник може да откуца кома-

[1] Master/Slave

нду, да покрене програм и цео програм је покренут. Ствар је оперативног система да одабере најбољи процесор, пронађе и пренесе улазне програме ка том процесору и смести резултат на одговарајуће место.

Другим речима корисник није свестан да постоји више процесора. Цео систем изгледа као виртуелни једнопроцесорски систем. Функције као што су смештање извршних програма до процесора и датотека на дискове, померање датотека између места где су смештене и места на којима су потребне и све друге системске функције аутоматске су. Добро познат пример дистрибуираног система је *World Wide Web* у коме све изгледа као један документ[1].

У рачунарској мрежи корисник мора експлицитно да се пријави, експлицитно покрене удаљени програм, експлицитно помери датотеке и генерално сам води рачуна о управљању мрежом. Са дистрибуираним системом ништа не мора да буде експлицитно урађено, систем све уради сам, без увида корисника.

Дистрибуирани систем је софтверски систем који користи рачунарску мрежу. Софтвер даје висок степен кохезије и транспарентности. Тако граница између рачунарске мреже и дистрибуираног система лежи у софтверу (оперативном систему), а не у хардверу. У сваком случају, постоји значајно преклапање између ова два појма. На пример и дистрибуирани системи и рачунарске мреже захтевају померање датотека. Разлика лежи у томе ко захтева пренос, систем или корисник.

1.1 Коришћење рачунарских мрежа

Анализираћемо питање зашто су људи заинтересовани за рачунарске мреже и за шта се оне могу користити.

Дељење ресурса

Циљ је омогућити сваком у мрежи, независно од физичке локације ресурса и корисника, доступ свим програмима, опреми и подацима. То значи да ако је корисник удаљен 1000km од података, то га неће спречити да користи податке као да су локални.

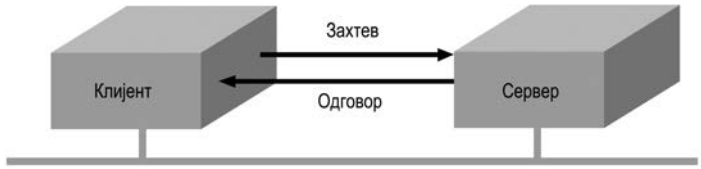
Висока поузданост

Сви програми могу да буду ископирани на више рачунара, тако да уколико један од њих није доступан (као последица хардверског проблема) могу се користити остале копије. Практично, присуство више централних процесорских јединица[2] значи да уколико једна откаже друга може да преузме посао, иако са мањим перформансама.

Уштеде

Мали рачунари имају бољи однос цена/карактеристике. То доводи до тога да многи пројектанти бирају системе који се састоје од персоналних рачунара, по један за сваког корисника, и са подацима који се чувају на једној или више централних машина, сервера. У овом моделу корисник се зове клијент а комплетна организација назива се клијент-сервер модел (илустровано је сликом 1.1).

[1] *Web page*
[2] CPU - *Central Processing Unit*



Слика 1.1 Клијент-сервер модел

У клијент-сервер моделу комуникација се генерално одвија у форми упита који клијент шаље серверу да он уради (изврши) неки посао за њега. По обављеном послу сервер шаље одговор натраг. Обично постоји велики број клијената који користе мали број сервера.

Још један циљ мреже је надоградивост, тј. способност да се побољшају перформансе система постепено, како се повећава обим посла, додавањем још процесора. У централизованом систему када се систем попуни он се мора заменити већим, који је обично скупљи и захтева промену у начину рада корисника. У клијент-сервер моделу могу се додавати и нови клијенти и нови сервери. Коришћењем рачунарске мреже могуће је да два корисника раде на истом документу, прате измене тренутно[1], а да су географски дислоцирани. Један од разлога који је допринео да од 1980. године нагло порасте умрежавање рачунара је чињеница да рачунари који нису међусобно повезани немају никаквог смисла. Више међусобно повезаних (умрежених) рачунара чине рачунарску мрежу.

Јавне рачунарске мреже

Од 1990. године рачунарске мреже почеле су да пружају сервисе приватним лицима код њихових кућа. Навешћемо четири најважнија:

- приступ удаљеним информацијама,
- комуникација личност-личност,
- интерактивна забава,
- електронска трговина.

Приступ удаљеним информацијама је у различитим формама. Једна од често коришћених је приступ информационим системима као што је WWW, који садржи разноразне информације (уметност, послови, кување, здравство, историја, наука, спорт, путовања ...).

Новине су доступне у реалном времену [2]. Други вид је дигитална библиотека (магазини, часописи). Многе професионалне организације као што је ACM[3] и IEEE[4] *Computer Society* имају своје дигиталне библиотеке са часописима и зборницима радова са конференција којима се може приступити преко Интернета. У зависности од цене и величине може се десити да штампане књиге постану застареле.

Следећа широка категорија је комуникација личност-личност, практично одговор 21. века на телефон 19. века. Електронску пошту[5], која може да садржи и звук и слику,

[1] *On- line*
[2] *Real time*
[3] *Association for Computing Machinery*, www.acm.org
[4] *Institute of Electrical and Electronics Engineers,* www.ieee.org, www.computer.org
[5] E-*mail*

користе милиони људи. Електронска пошта у реалном времену омогућила је удаљеним корисницима да комуницирају без кашњења, уз могућност да се и виде и чују. Могу се одржати и виртуелни састанци између просторно удаљених људи (тзв. видеоконференција).

Трећа категорија је забава којој се придаје значајна пажња. Поменућемо видео по жељи: ускоро ће бити могуће одабрати било који филм, било када снимљен, у било којој земљи и имати га тренутно на свом екрану .

Термин електронска трговина има широко значење. Куповина „од куће“ је веома популарна и омогућава корисницима да прегледају електронске каталоге великог броја произвођача.

Све значајнији је и приступ финансијским институцијама. Многи људи електронски плаћају рачуне и управљају својим банковним рачунима.

Рачунарске мреже од велике су важности људима који су географски удаљени од великих градова дајући им приступ услугама какав имају људи који живе у самом центру великог града. На пример:

- даљинско образовање (телеучење) може значајно да утиче на образовање,
- телемедицина (удаљено праћење пацијената) је у све већем развоју.

Укратко, способност стапања информација, комуникација и забаве резултовала је у новој, масовној индустрији заснованој на рачунарском умрежавању.

Мобилни корисници

Преносиви рачунари и PDA[1] системи део су рачунарске индустрије који се најбрже развија. Да би ови уређаји комуницирали међусобно а и са стационарним рачунарима потребне су бежичне рачунарске мреже. Бежичне мреже се користе за телефонске разговоре, електронску пошту, претраживање Интернета и приступ удаљеним датотекама. Користе их различите службе: таксисти, комуналне службе, војска. Бежичне технологије све су распрострањеније и бројне апликације их све више користе.

1.2 Класификација рачунарских мрежа

Генерално посматрано постоје два типа технологије преноса:

- од једног ка свима[2] (дифузно),
- од једног ка једном[3] (тачка-тачка).

Рачунарске мреже које користе технологију „један ка свима” имају један комуникациони канал који деле сви рачунари на мрежи. Кратку поруку (тзв. пакет) коју шаље било који рачунар примају сви остали. Адреса у адресном пољу специфицира коме је упућен пакет. После пријема пакета рачунар проверава адресно поље. Уколико је њему намењен, обрађује га, уколико није игнорише га.

С друге стране, рачунарске мреже које користе технологију „тачка-тачка” обезбеђују много веза појединих парова рачунара. Да би прешао од извора до одредишта пакет мора да пређе један или више међурачунара.

[1] *Personal Digital Assistant* - лични дигитални асистент
[2] *Broadcast*
[3] *Point to point*

Удаљеност	Смештени на (у) истом (ој)	Примери
1 m	Делу просторије	Личне мреже
10 m	Простор ији	Локалне рачунарске мреже
100 m	Згради	
1 km	Блоку зграда	
10 km	Граду	Мреже градског подручја
100 km	Држави	Мреже ширег подручја
1000 km	Континенту	
10 000 km	Планети	Интернет

Табела 1.1 Класификација међусобно повезаних рачунара (или делова) по величини

Један од начина класификације рачунарских мрежа је по њиховој величини. У табели 1.1 дата је класификација рачунарских мрежа поређаних по њиховој величини. На почетку табеле су мреже[1] које користи једна особа (личне мреже). На пример бежичне мреже[2] које повезују рачунар са мишем, тастатуром и штампачем су личне мреже. Иза њих су рачунарске мреже, рачунари који комуницирају разменом порука преко дужих каблова или бежичних система. Тако се мреже могу поделити на:

- личне мреже PAN[3],
- локалне рачунарске мреже LAN[4],
- рачунарске мреже градског подручја MAN[5] и
- рачунарске мреже ширег подручја WAN[6].

На крају веза две или више рачунарских мрежа назива се рачунарска мрежа међусобно повезаних мрежа[7]. Почетком 90-тих година констатовано је да постојање међусобно неповезаних мрежа нема никаквог смисла. Више мрежа које користе исти скуп протокола међусобно је повезано[8] и названо Интернет. То је најпознатији пример мреже међусобно повезаних рачунарских мрежа.

Локалне рачунарске мреже

Локалне рачунарске мреже су типа један ка свима и имају следеће карактеристике:

- податке које шаље једна станица прима више станица, често и све станице мреже,
- станице деле заједнички трансмисиони медијум и због тога су потребне технике за приступ заједничком трансмисионом медијуму.

[1] Термин рачунарска мрежа (*computer network*) користи се за системе у којима су међусобно повезани рачунари. Све је чешћа појава међусобног повезивања: рачунара, мобилних телефона, уређаја у домаћинству, алармних система, тако да је термин који се за све може употребити комуникациона мрежа, односно мрежа (*network*).
[2] *Wireless Network*
[3] *Personal Area Network*
[4] *Local Area Network*
[5] *Metropolitan Area Network*
[6] *Wide Area Network*
[7] *Internetworking*
[8] *Internetwork*

Локалне рачунарске мреже (LAN) су приватне мреже у оквиру једне зграде, блока зграда (кампуса) или у окружењу од пар километара раздаљине. Користе се за повезивање персоналних рачунара и радних станица у институцијама и омогућују дељење ресурса (нпр. штампача), размену података итд. Локалне рачунарске мреже разликују се међусобно по:

- величини,
- технологији (начину) преноса,
- топологији (начину физичке повезаности).

Рачунарске мреже градских подручја

Рачунарске мреже градских подручја (MAN) као што и само име указује обухватају подручје једног града. Најпознатији пример ове врсте је мрежа кабловске телевизије. Настала је као замена градског система антена, у коме је ваздушни пријем био лошег квалитета. Велике антене постављане су на неком од најближих узвишења, а одатле сигнали су се кабловским везама преносили до корисника.

Када је Интеренет почео масовно да се користи кабловски ТВ оператери су закључили да би и они могли да обезбеде двосмерни приступ Интернету са изменама у свом систему у делу спектра који се не користи. Од тог тренутка кабловски ТВ дистрибутивни системи постају и рачунарске мреже градских подручја.

Рачунарске мреже ширих подручја

Рачунарске мреже ширих подручја (WAN) обухватају: шира градска подручја, једну државу или континент. Садрже скуп рачунара (крајњих станица) који су међусобно повезани комуникационим мрежама[1]. Комуникациона мрежа се састоји од преносних (трансмисионих) линија и уређаја за преусмеравање (комутационих елемената) као што су различите врсте комутатора и рутера.

Данашње комуникационе мреже изузетно су сложени системи са линијама за пренос великог капацитета и уређајима за преусмеравања са имплементираним сложеним алгоритмима.

Бежичне рачунарске мреже

Бежичне рачунарске мреже нису нова идеја. Италијански физичар Маркони[2] 1901. године приказао је бежичну везу користећи Морзеов кôд. Савремени бежични системи знатно су сложенији али је основна идеја остала иста. Бежичне мреже могу се на једноставан начин систематизовати у три категорије:

- међусобно повезивање делова рачунарских система,
- бежичне локалне рачунарске мреже,
- бежичне мреже ширег подручја.

Међусобно повезивање делова рачунарских система може се реализовати помоћу радио-таласа. Група компанија развила је бежичну мрежу Bluetooth. Поред тастатуре, миша, монитора, штампача могуће је повезати и дигиталне камере, слушалице, скенере и друге уређаје.

[1] У 2. поглављу биће детаљније анализиране комуникационе мреже.
[2] *Gugliemo Marconi*

Следећа категорија јесу бежичне локалне рачунарске мреже. То су системи код којих сваки рачунар има радио-модем и антену преко које може да комуницира са другим рачунарима или уређајима у рачунарској мрежи. Доста се пажње поклања стандардизацији оваквих система[1].

Трећу категорију представљају бежичне мреже које се користе у ширим географским подручјима, односно на већим растојањима. Пример су ћелијски (мобилни) телефонски системи који припадају групи ускопојасних бежичних система. До сада су развијене три генерације ових система. Прва генерација су аналогни системи (само за пренос говора). Друга генерација су дигитални системи али претежно намењени за пренос говора. Трећа генерација су дигитални системи који су предвиђени и за пренос говора и за пренос података. Растојања између базне станице и рачунара или телефона може да буде и неколико километара.

Поред описаних ускопојасних система мањих брзина[2] све се више ради на развоју широкопојасних бежичних рачунарских мрежа[3]. Пажња је усмерена на бежични приступ Интернету великом брзином за резиденцијалне (кућне) и пословне кориснике. Ови системи заобилазе телефонску мрежу и загушења која због великог саобраћаја у њој постоје.

1.3 Стандарди

Процес стандардизације важан је за све оне који учествују у свету комуникација. Без стандарда пренос података био би скоро немогућ. Специфична решења једног произвођача била би ексклузивна за пренос кроз комуникационе системе без могућности подржавања уређаја другог произвођача. Стандард омогућава да више произвођача нуде производе који могу ефикасно заједно да раде. Корисници добијају системе који имају унапред дефинисане карактеристике и могу успешно да раде једни са другима. Стандарди имају велики утицај на економију. Производи који су стандардизовани масовно се производе, тиме се снижава њихова цена и то их чини економски прихватљивим.

Постоје две категорије стандарда:

- *de facto* (латински - на основу чињеница) су стандарди који се једноставно појаве, без икаквог плана. IBM персонални рачунар и његови следбеници су *de facto* стандард за рачунаре који се користе за послове мањег обима,
- *de jure* (латински - по закону) су легални стандарди које су прописале организације за стандардизацију.

Интернационалне организације за стандарде деле се у две групе: оне које су основане међудржавним уговором и друге, добровољне, које не обавезују своје чланове да донете стандарде примењују.

У табели 1.2 дат је списак организација које се баве стандардизацијом.

[1] Серија стандарда IEEE802.11. Биће детаљније описано у 13. поглављу.
[2] *Rate*. Јединица је бит у секунди (b/s). Користи се и термин проток.
[3] Серија стандарда IEEE802.16. Биће детаљније описано у 13. поглављу.

Име организације	Ознака	Карактер	Допринос/област
International Organization for Standardization	ISO	Интернационална/ добровољна	OSI слојевити модел
Comite Consultatif International Telegraphique et Telephonique	CCITT (више не постоји)	Интернацинална/ на основу повеље Уједињених нација.	Телекомуникациони стандарди
International Telecomunications Union	ITU-T	Интернационална/ на основу повеље Уједињених нација	Матична организација наследник CCITT-а
American National Standards Institute	ANSI	Представник владе САД у ISO	Стандарди у информационим технологијама
Institut of Electrical and Electronics Engineers	IEEE	Професионална организација	Стандарди у локалним рачунарским мрежама
Internet Engineering Task Force	IETF	Интернационална/отворена	Протоколи и други стандарди везани за Интернет
International Architecture Boarad	IAB	Интернационална/отворена	Надгледа стандарде које је развила IETF
Request for Comments	RFC	Технички извештаји	Доступна свима
International Industrial Association	EIA	Организација трговаца	Стандарди везани за електричне сигнале, ожичавање
European Telecommunication Stanadard Institute	ETSI	Европски институт	Стандарди у телекомуникацијама
Third Generation Partnership Project	3GPP	Организација произвођача	Стандарди у целуларним и мобилним системима треће генерације
Federal Communications Commission	FCC	Федерални комитет за комуникације САД-а	Регулаторно тело
Wireless Fidelity Alliance	Wi Fi Alliance	Организација произвођача	Издаје WiFi сертификат о усаглашености са стандардима серије IEEE802.11
Worldwide Interoperability for Microwave Access Forum	Wi Max [1] Forum	Организација произвођача	Издаје WiFi сертификат о усаглашености са стандардима серије IEEE802.16
Bluetooth Special Interest Group	Bluetooth SIG	Организација произвођача	Издаје Bluetooth сертификат
Internet Society	ISOC	Професионална организација	Подршка расту и развоју Интернета

Табела 1.2 Организације које се баве стандардизацијом

[1] *WiMax* није технологија већ сертификат (потврда) да је опрема прошла тестирање о усаглашености и могућности међусобног рада, а у складу са скупом стандарда IEEE802.16.

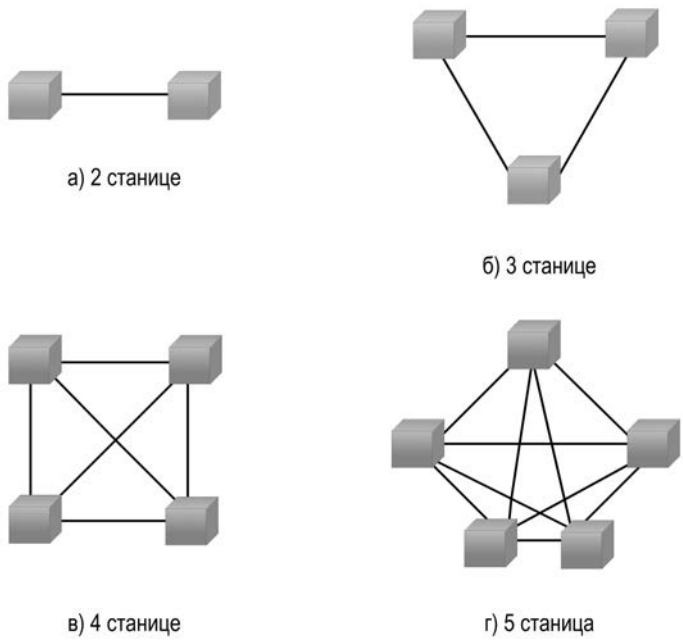
2. Комутационе технике

У најједноставнијем облику комуникације се обављају између два уређаја која су директно повезана неком врстом тачка-тачка трансмисионог медијума. Обично је непрактично за два уређаја да буду директно повезана тачка-тачка. Разлози су следећи:

- уређај је веома далеко. Било би превише скупо, на пример, доделити посебну линију између уређаја стотинама километара удаљених један од другог;
- постоји више уређаја и сваки од њих може да захтева везу са другима у различитим тренуцима времена. Пример су сви телефони или рачунари у свету, или некој организацији.

Да бисмо разјаснили проблем који се јавља као последица друге тачке посматраћемо појам топологије. Топологија се, у овом контексту, односи на начин на који је више уређаја међусобно повезано преко комуникационе везе (линка). Посматрајмо ситуацију са више уређаја који захтевају више веза. Зашто се не би обезбедила тачка-тачка веза између свих њих?

Проблем са оваквим приступом илустрован је на слици 2.1. Сваки уређај има тачка-тачка везу са сваким другим уређајем. Ово се назива потпуно повезана или „меш"[1] топологија. Уколико има *k* уређаја захтева се $k(k-1)/2$ потпуни дуплекс веза, и сваки уређај



Слика 2.1 Потпуно повезане станице

[1] *Mesh*

захтева *k-1* улазно/излазних (У/И) портова. Тако цена система посматрајући кабловску инсталацију и хардвер расте с квадратом броја уређаја.

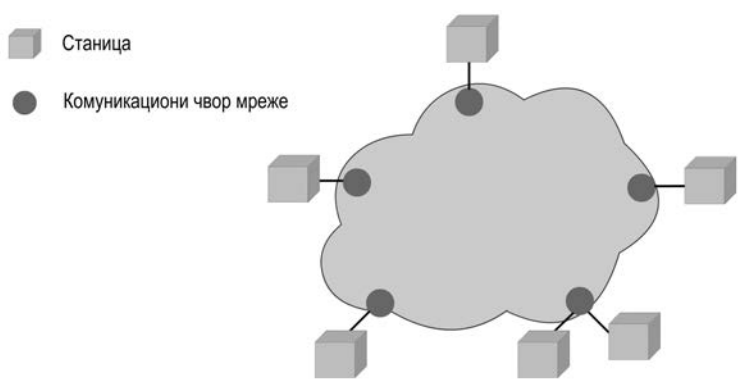
Мане оваквог решења су јасне. Решење овог проблема је повезивање уређаја на комуникациону мрежу. Слика 2.2 илуструје концепт на генералан начин. Имамо скуп уређаја који треба међу собом да комуницирају; уопштено ћемо их назвати станице [1]. Станице могу бити рачунари, терминали, телефони или други комуникациони уређаји. Свака станица се прикључује за мрежни чвор. Скуп чворова на који се прикључују станице је граница комуникационе мреже која је подесна за размену података између парова прикључених станица.

Комуникациона мрежа:

- не води рачуна о садржају података који се размењују између станица; намена је једноставно да пренесе податке од изворишта до одредишта,
- обезбеђује деобу трансмисионих уређаја између многих станица чиме се смањују трошкови које направи било који пар станица. Такође, један У/И порт је потребан свакој станици, а не *k-1*.

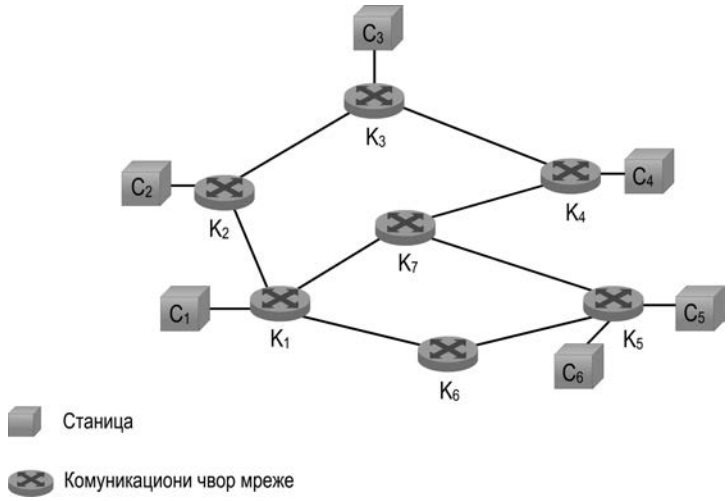
Комуникационе мреже могу бити категоризоване у зависности од архитектуре и технике које се користе за пренос података. Типови мрежа који су у употреби су:

- комутиране комуникационе мреже [2],
  - мреже са комутацијом канала[3],
  - мреже са комутацијом порука[4],
  - мреже са комутацијом пакета[5],
- комуникационе мреже један ка свима [6],
  - радио-мреже,
  - сателитске мреже,
  - локалне рачунарске мреже.



Слика 2.2 Повезивање преко комуникационе мреже.

[1] У литератури се користе и термини крајња станица или хост.
[2] *Switched communication network*
[3] *Circuit switching network.* Користе термини: комутација канала, линија, веза или кола. У овом уџбенику користићемо најчешће термин комутација канала.
[4] *Message switching network*
[5] *Packet switching network*
[6] *Broadcast communication network*



Слика 2.3 Комутирана комуникациона мрежа

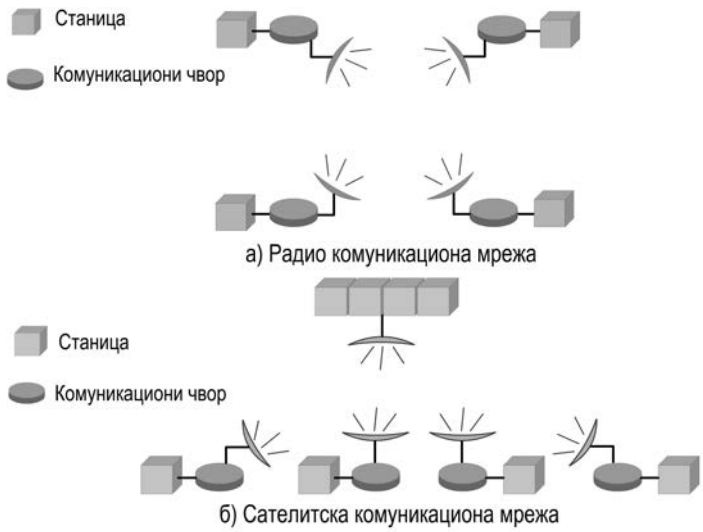
Комутирана комуникациона мрежа састоји се од међусобно повезаних скупова чворова, у којима се подаци преносе од изворишта до одредишта преусмеравањем кроз чворове. Слика 2.3 је илустрација тог концепта.

Чворови су везани преко трансмисионих (преносних) путева. Подаци који долазе у мрежу из станице усмеравају се (рутирају) ка одредишту комутацијом од чвора до чвора. На пример, подаци из станице 1 (C_1) који треба да дођу до станице 5 (C_5) шаљу се ка чвору K_1. Он затим може да пошаље податке преко чворова K_2, K_6 или K_7 ка чвору K_5 за који је везана одредишна станица C_5.

За комутиране комуникационе мреже са комутацијом канала, порука и пакета следећа опажања су битна:

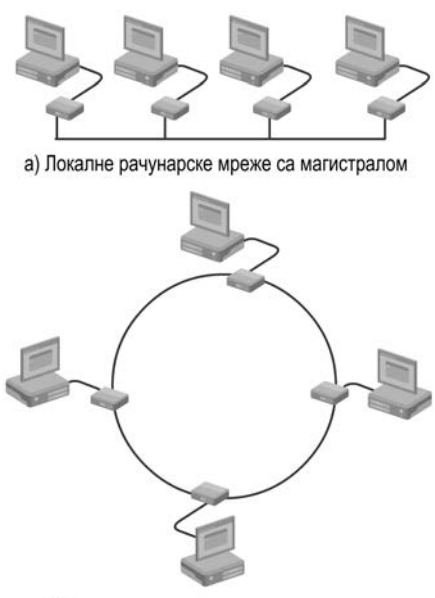
- Поједини чворови повезују само друге чворове (нпр. K_6 и K_7). Њихов задатак је да интерно (у мрежи) усмеравају (комутирају) податке. Други чворови имају прикључену једну (или више) станица. Поред комутирајућих функција такви чворови прихватају и прослеђују податке од и ка прикљученим станицама;
- Везе чвор-станица искључиво су намењене за повезивање тачака. Чвор-чвор везе су обично мултиплексиране везе које користе технике фреквенцијског мултиплекса (FDM[1]) или временског мултиплекса (TDM[2]). За чворове који су удаљени мултиплексирање значајно смањује цену преноса у поређењу са везом искључиво посвећеном сваком пару станица;
- Чворови комуникационе мреже могу да буде потпуно или делимично повезани. Ово друго је уобичајено за велике мреже. Увек је пожељно за сваки пар станица имати више од једног могућег пута кроз мрежу. На тај начин се обезбеђује поузданост комуникационе мреже;

[1] *Frequency Division Multiplexing*
[2] *Time Division Multiplexing*



Слика 2.4 Бежичне мреже

Код комуникационих мрежа један ка свима између крајњих станица не постоји комутациони чвор. Свака станица прикључена је за предајник/пријемник који комуницира преко медијума који дели са осталим станицама. То је најједноставнији начин; оно што пошаље било која станица прослеђује се тако да све станице могу то да приме. Једноставан пример је радио-систем у коме се слушаоци подешавају на исти канал (учестаност) тако да могу међусобно да комуницирају. Слике 2.4 и 2.5 илуструју комуникационе мреже.



Слика 2.5 Локалне рачунарске мреже

2.1 Комутација канала

Комутација канала подразумева технику комуницирања две удаљене станице тако да постоји комуникациони пут додељен само тим станицама. Пут је повезана секвенца комуникационих веза између чворова. Уобичајени пример мреже са комутацијом канала је телефонска мрежа. Комуникација у систему са комутацијом канала подразумева три фазе: фазу успоставе везе[1], фазу преноса порука[2] и фазу раскидања везе[3].

Фаза успоставе везе

Пре него што се било који сигнал пошаље мора се успоставити веза с краја-на-крај (станица-станица). На пример: станица C_1 шаље захтев чвору K_1 захтевајући везу са станицом C_5 (слика 2.3). Типично, веза између станице C_1 и чвора K_1 је линија намењена искључиво томе, тако да тај део везе већ постоји. Чвор K_1 мора да пронађе путању и она га води до чвора K_5. На основу информације о рутирању и мерењу доступности и вероватно цене, чвор K_1 бира везу ка чвору K_7, додељује слободан канал (користећи временски или фреквенцијски мултиплекс[4]) на том линку и шаље поруку да захтева везу са C_5. Тако додељени пут остварен је од станице C_1 преко чворова K_1 до K_7. Пошто више станица може да се прикључи на чвор K_1 он мора да буде у стању да оствари интерне путеве од више станица ка више чворова. Даље, чвор K_7 додељује канал ка чвору K_5 и интерно повезује тај канал са каналом од чвора K_1. Чвор K_5 завршава везу ка станици C_5 тако што испитује да ли је станица C_5 заузета или је спремна да прими везу.

Фаза преноса порука

Сигнали сада могу да се пренесу од станице C_1 преко мреже ка станици C_5. Сигнали могу да буду дигитални (рачунари), или аналогни (говор). У оба случаја путању чине: линија између станице C_1 и чвора K_1, интерна комутација у чвору K_1, канал између чворова K_1 и K_7, интерна комутација у чвору K_7, канал између чворова K_7 и K_5, интерна комутација у чвору K_7 и линија између чвора K_5 и станице C_5. Веза је обично таква да се сигнали могу слати у оба правца.

Фаза раскидања везе

После периода преноса података веза се прекида, обично захтевом једне од две станице. Сигнал се мора проследити кроз чворове K_1, K_7 и K_5 да би се ослободили додељени ресурси.

Уочимо да је путања успостављена пре него што је пренос порука започет. Тако капацитет канала мора бити резервисан између пара чворова на тој путањи, и сваки чвор мора да има расположиве интерне комутационе капацитете за одржавање захтеване везе. Комутатор мора да има способност да овим управља.

---

[1] *Circuit establishment* (успостављање везе). Користићемо термин успостава везе као генералнији приступ који се односи на све системе који у себи обједињује три фазе: успоставу, пренос и раскид везе. У случају система са комутацијом канала веза се користи у смислу физички додељеног канала или линије.

[2] *Data transfer (*пренос података). Треба истаћи да се подаци преносе у облику рамова или порука. Али за разлику од система са комутацијом порука успостављена путања, односно одговарајући канали који чине ту путању додељени су само тој вези.

[3] *Circuit disconnect*

[4] Коришћење истог трансмисионог медијума за више канала тако да не долази до преклапања у времену (временски мултиплекс) или по фреквенцији (фреквенцијски мултиплекс). У 8. поглављу биће детаљно објашњене ове технике.

Комутација канала је релативно неефикасна. Каналски капацитет је додељен за време трајања везе, без обзира да ли се поруке преносе. У говору постоје паузе тако да је канал заузет највише 50% времена. За рачунарске комуникације капацитет може да буде неискоришћен у великом делу трајања везе. У ствари, једном када се веза успостави мрежа је практично транспарентна за корисника.

Подаци се шаљу фиксном брзином без кашњења, осим времена пропагације тј. кашњења услед простирања преко преносних линија (линкова). Кашњење које је последица времена које је потребно да се подаци обраде у чворовима практично је занемарљиво.

2.2 Комутација порука

Комутација канала је приступ који одговара системима у којима је размена података везана за релативно континуалан проток података, као што су говор (телефон) и неки типови сензорских и телеметријских улаза. У ствари, комутација канала има два значајна ограничења:

- обе станице морају бити на располагању у исто време за размену података,
- ресурси кроз мрежу морају бити слободни и искључиво додељени двема станицама.

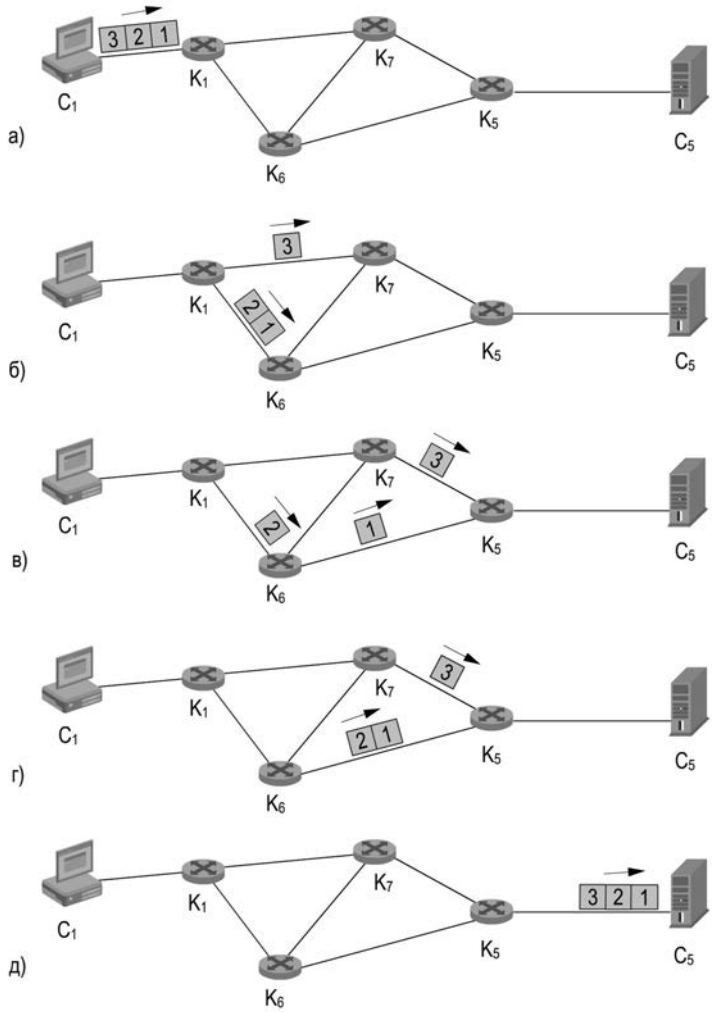
Други приступ, који генерално одговара преносу дигиталних сигнала, је размена логичких јединица које се називају поруке. Примери порука су телеграми, електронска пошта, рачунарски програми, трансакције са упитом и одговором. Уколико је потребно размењивати поруке у оба правца између станица користи се приступ познат под називом комутација порука. Са комутацијом порука није неопходно успоставити додељени пут између станица. Станица која шаље поруку додаје адресу одредишта поруци. Порука се затим прослеђује кроз мрежу од чвора до чвора. У сваком чвору цела порука се прими, смести на кратко и затим шаље ка следећем чвору.

На слици 2.6 илустрован је пример слања 3 поруке. Чвор сваку поруку независно анализира и може (као што је на слици 2.6 приказано) свака од њих да се шаље различитим путањама. Овај систем назива се систем „смести и проследи"[1]. У неким случајевима чвор за који је станица прикључена, или централни чвор, прави такође и сталну копију поруке (извештај).

Предност овог приступа у односу на комутацију канала је следећа:

- ефикасност линије је већа пошто у датом тренутку канал чвор-чвор може делити више порука. За исту количину саобраћаја потребни су мањи капацитети преносних канала;
- није неопходна истовремена расположивост и предајника и пријемника. Мрежа може да чува (смести) податке;
- када је саобраћај повећан мрежа са комутацијм канала блокира неке позиве, тј. мрежа одбија да их прими. Код система са комутацијом порука поруке се и даље примају, али прослеђивање касни;

[1] *Store and Forward*



Слика 2.6 Комутација порука

- систем са комутацијом порука може да шаље једну поруку ка многим одредиштима. Праве се дупликати поруке и свака се шаље ка једном од захтеваних одредишта. Ово се не може лако постићи системом са комутацијом канала;
- могуће је обезбедити приоритет порука. Тако, уколико чвор има већи број порука које чекају у реду за пренос, он може прво да шаље поруку са вишим приоритетом. Ове поруке ће стизати са мањим кашњењем него поруке са мањим приоритетом;
- контрола грешке и опоравак од грешке могу бити уграђени у мрежу. Поруке могу бити нумерисане и ископиране за касније, уколико оригинална не успе да стигне до одредишта;

- порука која се шаље ка станици која није у раду може се поново послати ка некој другој станици или задржати до даљњег;
- мрежа са комутацијом порука може обезбеди конверзију кôда и брзине. Две станице са различитим брзинама могу бити међусобно повезане. Мрежа са комутацијом порука може лако да конвертује формат (нпр. из ASCII формата у EDCIDIC формат).

Основни недостатак мреже са комутацијом порука је да није погодна за саобраћај у реалном времену[1]. Кашњење кроз мрежу може да буде релативно дугачко и има велике варијације[2].

2.3 Комутација пакета

Чињеница је да станица поруке изнад одређене величине прво мора да подели у мање јединице (пакете) и затим их шаље једну за другом.

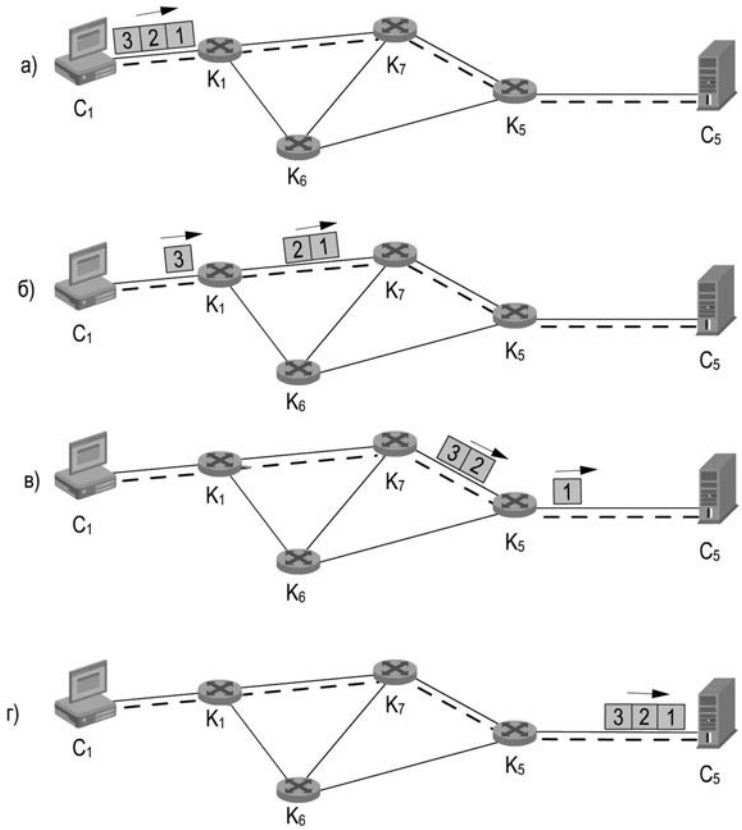
Посматрајмо пренос једног пакета на примеру слике 2.6. Пакет садржи податке и одредишну адресу. Станица C_1 шаље пакет ка чвору K_1, који га накратко смешта и затим прослеђује ка чвору K_7, који га затим прослеђује ка чвору K_5 и тако даље до станице C_5. На први поглед комутација пакета може да изгледа као да нема посебне предности у односу на на комутацију порука. Међутим, смањење величине поруке у пакет има значајан утицај на перформансе.

Проблем је у следећем: станица има поруку за слање која је већа од максималне величине пакета. Порука се дели у мање целине (пакете) који се шаљу ка чворовима (слика 2.7). Поставља се питање како ће мрежа водити рачуна о овој групи пакета? Постоје два приступа: датаграм (без успоставе везе) и виртуелни канал (са успоставом везе).

У датаграм приступу сваки пакет се третира независно, као што се и свака порука третира независно у мрежи са комутацијом порука. Анализираћемо последице оваквог приступа. Претпоставимо да станица C_1 има три пакета да пошаље ка станици C_5, као што је приказано на слици 2.6. Сматраћемо да је станица C_1 поделила поруку коју треба да пошаље станици C_5 у три пакета. Она шаље

Слика 2.7 Употреба пакета

[1] *Real time*
[2] *Jitter*



Слика 2.8 Комутација пакета: виртуелни канал

пакете напоље, 1-2-3 ка K_1. За сваки пакет чвор K_1 мора да направи одлуку о даљем прослеђивању (на пример K_6). Сваки чвор одабира као следећи чвор на путањи пакета на основу информација које добија од суседних чворова о саобраћају, линијама које не раде итд. Пакет 1 долази у чвор K_1 који види да је ред за чвор K_6 мањи него за чвор K_7 и ставља пакет у ред за чвор K_6. Исто је и за пакет 2. Али за пакет 3 чвор K_1 проналази да је његов ред за чвор K_7 краћи и ставља пакет 3 у тај ред. Тако пакети са истим одредишним адресама не иду по истим путањама. Могуће је да ће пакет 3 пре стићи до чвора K_5 од пакета 2. Тако је могуће да ће пакети бити испоручени станици C_5 различитим редоследом од оног у коме су послати. Станица C_5 је та која ће их правилно поређати. Пошто се сваки пакет третира независно ова техника се назива датаграм [1].

У приступу са виртуелним каналом успоставља се логичка (виртуелна) веза пре него што се било који пакет пошаље. На пример, претпоставимо да станица C_1 има једну или више порука да пошаље ка станици C_5 (слика 2.8). Она прво ка чвору K_5 шаље пакет „позив за успоставом везе"[2], захтевајући успоставу везе са станицом C_5. Чвор K_1

[1] Без успоставе везе - *connectionless.*
[2] *Call Request*

одлучује да усмери позив за успоставом везе (као и све остале податке) ка чвору K_5 који га прослеђује ка станици C_5. Уколико је станица C_5 спремна да прихвати везу она шаље пакет „позив је прихваћен"[1] ка чвору K_5. Овај пакет се шаље натраг преко истих чворова до станице C_1. Станице C_1 и C_5 могу сада да размењују податке преко логичке везе, односно виртуелног канала (кола) који је између њих успостављен.

Сваки пакет сада садржи ознаку (идентификатор) виртуелног канала и податке. Сваки чвор у претходно успостављеној путањи[2] зна где да усмери пристигле пакете; није потребно одлучивати о рути. Тако сваки пакет података из станице C_1 пролази кроз чворове K_1, K_7 и K_5; сваки пакет података из станице C_5 пролази кроз чворове K_5, K_7 и K_1. Једна од станица може да прекине везу са пакетом „захтев за брисањем везе"[3]. У било ком тренутку свака станица може да има више од једног виртуелног канала ка било којој станици и може да има виртуелни канал ка већем броју станица.

Главна карактеристика технике са виртуелним каналима је да се успоставља путања (рута) између станица пре преноса порука. Уочимо да ово не значи да постоји додељени пут, као у колима са комутацијом канала. Пакет података се и даље смешта (баферује) у сваком чвору, и ставља у ред ка свакој линији. Разлика у односу на датаграм приступ је да чвор нема потребе да одлучује о путањи (рути) за сваки пакет већ се то за сваку везу уради само једном.

Виртуелни канал може да обезбеди различите услуге као што су додела редних бројева (секвенционирање), контрола грешке и контрола тока. Пошто сви пакети иду истом путањом стижу редоследом којим су послати. Контрола грешке обезбеђује да су пакети исправног редоследа и да су тачно примљени. На пример, уколико један од пакета у реду (секвенци) не стигне до чвора K_5, или стигне са грешком, чвор K_5 може да захтева поновно слање (ретрансмисију) пакета из чвора K_1 користећи редни број тог пакета

Техника која обезбеђује да пошиљалац не „преоптерети" примаоца подацима је контрола тока. На пример уколико станица C_5 памти податке које је добила од станице C_1 и констатује да нема више простора за смештање нових података, она може да захтева да станица C_1 до даљњег одложи слање података.

Предност датаграма је да је прескочена фаза успоставе везе[4], зато станица жели да пошаље само неколико пакета датаграм пренос је бржи. Друга предност датаграм сервиса је што је много флексибилнији. Уколико дође до загушења у једном делу мреже долазећи датаграми могу се преусмерити (рутирати) на други део мреже, тј. комуникационој мрежи је много лакше да се прилагоди загушењу. Ако се користи техника са виртуелним каналом када чвор није у функцији (у квару је) подаци о свим виртуелним везама које пролазе кроз тај чвор изгубљени су и веза између изворишне и одредишне станице мора се поново успостављати. Са датаграмом, уколико је чвор ван функције, пакети могу да се усмере на другу путању (преко неког другог чвора).

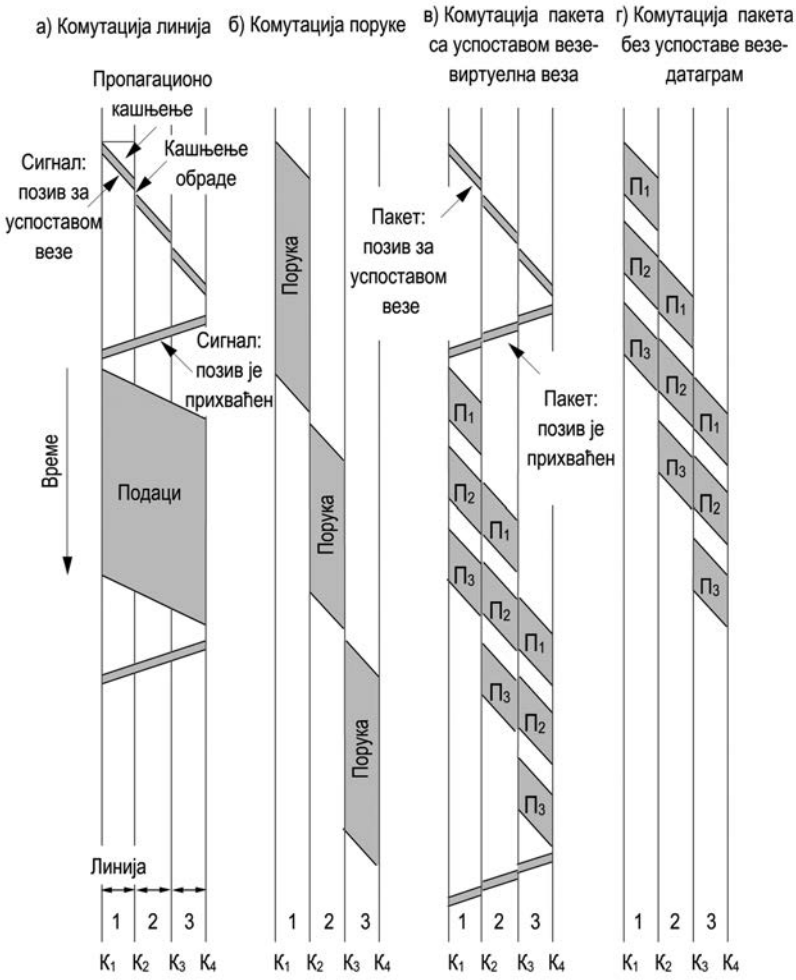
[1] *Call Accept*
[2] Користе се и термини пут или рута.
[3] *Clear Request*
[4] *Call setup*

2.4 Поређење комутационих техника

Три комутационе технике: комутација канала , порука и пакета приказана је на слици 2.9. На слици је скициран пренос порука кроз чворове K_1, K_2, K_3, K_4, од изворишне станице која је прикључена на чвор K_1 до одредишне станице прикључене на чвор K_4 преко међучворова K_2 и K_3.

У овом случају срећемо се са три типа кашњења:

- пропагационо кашњење је време потребно да се сигнал пренесе од једног чвора до првог следећег чвора. Ово време је занемарљиво код малих растојања али не и код великих као што су на пример трансконтиненталне везе. Брзина електромагнетског сигнала кроз жичне медијуме[1] је око $2*10^8$m/s;



Слика 2.9 Приказ комутационих техника

[1] *Hardwire*

- време слања (предаје) је време потребно предајнику да пошаље блок података ка линији. На пример, потребна је 1ms да би се послао блок од 1000 бита брзином 10Mb/s;
- кашњење обраде је време које је потребно чвору да обави неопходну обраду када врши комутацију података.

Перформансе комутационих система зависе од више фактора који укључују:

- број станица,
- саобраћај у систему,
- дужину (и у времену и у подацима) типичне размене између станица,
- време обраде чворова,
- величину пакета.

Детаљније о карактеристикама ових система биће речи у осталим поглављима овог уџбеника.

2.5 Штафетни пренос рамова

Пакетски пренос развијен је у време када је број грешака у пакету услед преноса дигиталним системима био већи него што је данас. Као резултат постоји значајан додатак[1] (сувишак) који се уноси у пакет код система са пакетском комутацијом, са циљем да компензују настале грешке у преносу. Додатак укључује битове који се придружују сваком пакету да би се помоћу њих обрадом у крајњим станицама и међучворовима откриле и по могућност исправиле грешке настале у преносу.

Са савременим телекомуникационим системима великих брзина дадаци су беспотребни и контрапродуктивни. Нису неопходна пошто је проценат грешака драстично смањен. Преостали број грешака може се једноставно открити у крајњим системима са одговарајућим механизмима.

Штафетни пренос рамова (FR[2]) пројектован је са намером да се искористе предности великих брзина преноса и малог процента грешака. Прве рачунарске мреже са пакетском комутацијом пројектоване су за брзине од око 64kb/s до крајњих корисника а мреже са штафетним преносом рамова пројектоване су да раде ефикасно са брзинама до 2Mb/s до крајњих корисника. Кључни потез који ово омогућава био је отклањање сложених механизама за контролу грешке.

2.6 Мреже са комутацијом ћелија

Мрежа са комутацијом ћелија (ATM[3]) представља сам врх у развоју система са комутацијом канала и пакета. Очигледна разлика између система са штафетним преносом (FR) и са комутацијом ћелија (ATM) је у томе што системи са штафетним преносом рамова користе целине променљиве дужине, које се називају рамови, а система са комутацијом ћелија целине фиксне величине које се називају ћелије. Као и системи са

[1] *Overhead*. Односи се на управљачке податке, тзв. некорисне податке. Користи се и термин премашење.
[2] *Frame Relay* (FR). Користи се и термин шафетни пренос оквира.
[3] *Asynchronous Transfer Mode* (ATM)

штафетним преносом, АТМ системи уносе мали додатак за контролу грешке: то препуштају вишим слојевима у крајњим системима. Користећи пакете фиксне дужине АТМ системи смањују време обраде у међучворовима. Резултат је да брзине које се постижу у АТМ мрежама иду и до реда Gb/s.

АТМ се такође може сматрати као систем који се развио из система са комутацијом канала. Код система са комутацијом канала крајњим системима су на располагању тачно одређене брзине података. АТМ системи омогућавају дефинисање више виртуелних канала са брзинама података које се дефинишу динамички у тренутку када се виртуелни канал успоставља. Користећи мале ћелије, тачно одређене величине (53 бајта) АТМ је тако ефикасан да може да понуди канале са константном брзином без обзира што користи пакетску комутацију. На тај начин АТМ проширује могућности система са комутацијом канала, тако да он омогућава постојање више канала у којима се брзина по захтеву динамички додељује.

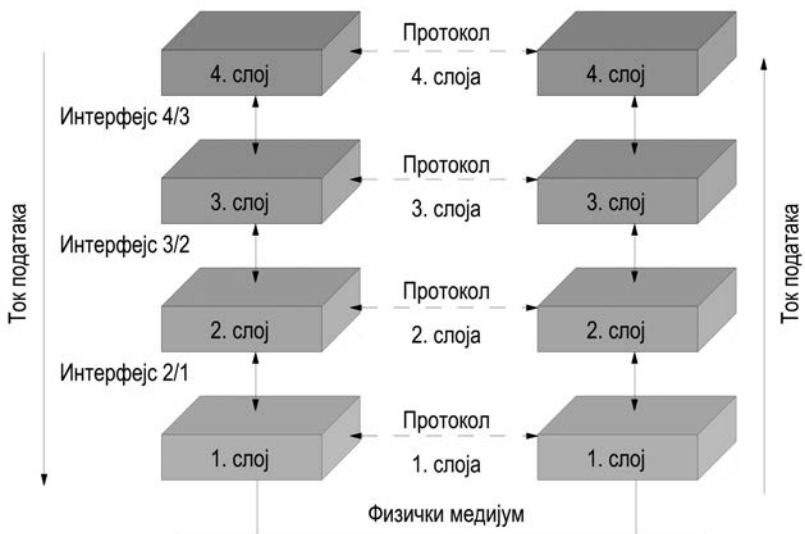
3. Слојевита архитектура протокола

Због комплексности у пројектовању рачунарских мрежа поступци за предају, пренос и пријем порука организовиани су као серија слојева или нивоа. Број слојева, као и њихова имена разликују се од мреже до мреже. У свим мрежама намена сваког слоја је да пружи одређену услугу[1] вишим слојевима, штитећи те слојеве од детаља (нпр. како се услуга реализује). Виртуелно слој *N* на једном рачунару води конверзацију са слојем *N* на другом рачунару. Правила и конвенције који се користе у овој конверзацији заједничке су и познате као протокол *N*-тог слоја. На слици 3.1 представљен је четворослојни модел.

У стварној комуникацији подаци се не шаљу директно из слоја *N* једног рачунара ка слоју *N* другог рачунара (осим у најнижем слоју). Уместо тога, сваки слој предаје податке и управљачке информације ка слоју који је одмах испод, докле год не стигне до најнижег слоја. На најнижем слоју постоји физичка комуникација са другим рачунаром, супротно од виртуелне комуникације коју користе протоколи виших слојева.

Између сваког пара суседних слојева постоји интерфејс[2]. Интерфејс дефинише које основне операције и услуге нижи слој нуди вишем слоју. Када пројектант мреже одлучи колико слојева ће укључити у мрежу и шта ће који од њих да ради најважније је јасно дефинисати интерфејсе између слојева.

Јасно дефинисање слојева, заузврат, захтева да сваки слој извршава специфични скуп јасно дефинисаних функција. Последица тога је да се један слој може заме-



Слика 3.1 Слојеви, протоколи и интерфејси

[1] Користи се и термин сервис.
[2] *Interface* (спрега).

нити потпуно другим слојем (нпр. телефонска линија може се заменити сателитском везом), пошто је све што се тражи од новог слоја да пружи исти скуп услуга слоју изнад себе, као што је претходна имплементација обезбеђивала.

Важна ствар за разумевање слике 3.1 јесте релација између виртуелне и стварне комуникације и разлика између протокола и интерфејса. Процес парњак[1] на 4. слоју, на пример, размишља о својој комуникацији као да је „хоризонтална", користећи протокол 4. слоја. Сваки од њих има процедуру која се назива „пошаљи на другу страну" и процедуру „узми са друге стране", иако ове процедуре стварно комуницирају са нижим слојевима преко 4/3 интерфејса а не са другом страном.

Скуп слојева и протокола назива се слојевита архитектура.

Спецификација архитектуре мора да садржи довољно информација да омогући ономе ко је имплементира писање програм за сваки слој, тако да програм коректно реализује одговарајући протокол. Ни детаљи имплементације, ни спецификација интерфејса нису делови архитектуре. У ствари чак ни сви интерфејси на свим рачунарима нису исти, а ипак је обезбеђено да сваки рачунар може коректно да користи протокол.

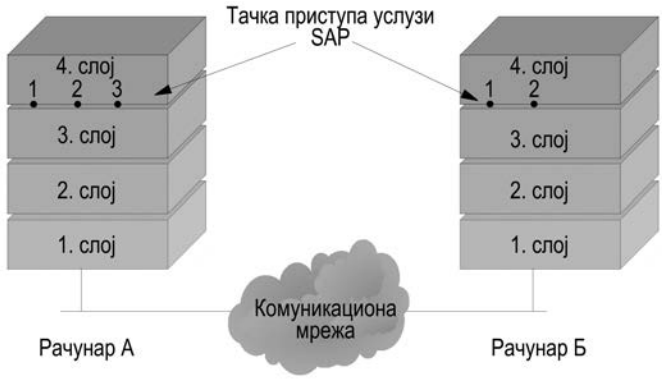
Пример вишеслојне архитектуре је следећи[2]: замислите да два истраживача (парњаци 3. слоја) од којих је један у Београду а други у Берлину, желе да комуницирају (слика 3.2).

Пошто немају заједнички језик они укључују преводиоце (парњак-процес 2. слоја), а сваки од њих контактира инжењере (парњак-процес 1. слоја). Истраживач А жели да пренесе своје закључке истраживачу Б (свом парњаку). Он шаље своје за-

Слика 3.2 Пример вишеслојне архитектуре: комуникација два истраживача

1 *Peer to peer process*

2 Пример преузет из [36].



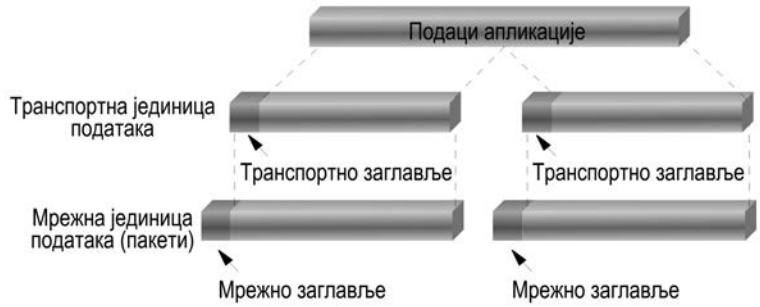
Слика 3.3 Комуникација преко тачке приступа услузи (SAP)

кључке на српском језику као поруке преко 2/3 интерфејса ка свом преводиоцу који их преводи на енглески или на француски језик, зависно од протокола 2. слоја. Преводилац затим даје поруку свом инжењеру који поруку преноси телеграмом, телефоном, рачунарском мрежом или неким другим средством, зависно како су се унапред договорили (протокол 1. слоја). Када порука стигне она се преводи на немачки и преноси преко 2/3 интерфејса истраживачу Б. Уочимо да је сваки протокол потпуно независан од других протокола докле год се интерфејс не мења. Преводилац може мењати језике са енглеског на француски подразумевајући да се оба слажу и да ни један не мења интерфејс ка 1. слоју или 3. слоју.

Посматрајмо технички пример: како обезбедити виртуелну везу ка највишем слоју четворослојне мреже. На слици 3.3 поруку M генерисао је процес који се одвија на 4. слоју. Порука се прослеђује са 4. до 3. слоја преко интерфејса 4/3 слоја који има јединствену адресу у оквиру тог система. Адреса интерфејсне тачке среће се и под називом тачка приступа услузи (SAP[1]). Са становишта апликационих процеса на 4. слоју комуникација рачунара А и Б изводи се преко тачака приступа 1, 2 и 3 рачунара А до тачака приступа 1 и 2 на рачунару Б.

Слика. 3.4. Пример протока података у четворослојном моделу

[1] *Service Access Point*



Слика 3.5 Јединице података протокола (PDU)

Као што смо истакли целине на истом слоју међусобно комуницирају користећи протокол тог слоја. Да би се реализовао протокол поред корисничких података морају се преносити и управљачке информације које се означавају као заглавље тог слоја. Комбинација података вишег слоја и управљачких информација чини јединицу података протокола PDU[1] (слика 3.4). Сваки слој додаје своје заглавље не залазећи у садржај јединице података коју је добио од вишег слоја. Овај процес назива се укалупљивање[2].

У нашем примеру, као и у другим стварним мрежама, не постоји ограничење у величини поруке коју може 4. слој да прими, али постоји ограничење које поставља 3. слој. Посматрајући даље, 4. слој мора да подели поруку у мање јединице додајући заглавље свакој јединици. Ово заглавље укључује управљачке информације, као што је нпр. редни број, да би се омогућило 4. слоју на одредишном рачунару да повеже делове у правилном редоследу.

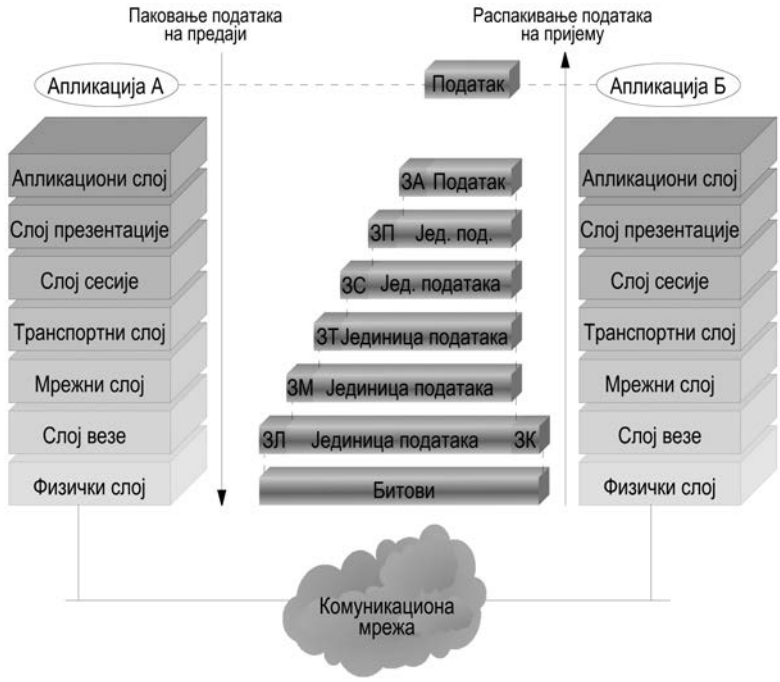
3.1 OSI референтни модел

На слици 3.6 приказан је OSI[3] референтни модел. Овај модел базиран је на препорукама које је развила интернационална организација ISO. Модел се назива ISO OSI референтни модел за међусобну комуникацију отворених система зато што се бави повезивањем отворених система - система који комуницирају са другим системима.

У овом делу објаснићемо укратко намену сваког од слојева:

- Физички слој је задужен за пренос преко физичке средине за пренос (трансмисионог медијума). Приликом приступа трансмисионом медијуму физики слој води рачуна о механичким, електричним, функционалним и процедуралним карактеристикама;
- Слој везе обезбеђује поуздан пренос података преко физичке везе. Шаље блокове података (рамове) са подацима потребним за синхронизацију, контролу тока, откривање и отклањање грешака;
- Мрежни слој одговоран је за успостављање, одржавање и раскидање везе. Омогућава да виши слојеви раде потпуно независно од врсте преноса или примењене комутационе технике;

[1] *Protocol Data Unit*
[2] *Encapsulation*
[3] *Open System Interconnection* - отворен систем за међусобну комуникацију.



Слика 3.6 OSI референтни модел

- Транспортни слој омогућава поуздан и транспарентан пренос података између крајњих тачака везе. Омогућава отклањање грешака[1] и контролу тока с краја на крај;
- Слој сесије обезбеђује управљачке структуре за међусобну комуникацију апликација. Омогућава успостављање, одржавање и раскидање везе (сесије) између одговарајућих апликација;
- Слој презентације обезбеђује да апликациони процеси не зависе од разлика у представљању података (синтакси);
- Слој апликације обезбеђује корисницима приступ OSI окружењу и такође обезбеђује дистрибуирану информациону услугу.

Слика 3.6 приказује и употребу јединице података у оквиру OSI референтног модела. Када апликација X има податке за апликацију Y она их шаље апликационој целини (процесу) на апликационом слоју. Подацима се додаје заглавље ЗА (тзв. процес укалупљивања) које садржи управљачке информације потребне парњаку, 7. слоју на одредиште. Оригинални подаци заједно са заглављем сада се прослеђују 6. слоју. Презентациони слој посматра јединицу података као јединствену целину и додаје своје заглавље ЗП (друго укалупљивање).

Овај процес наставља се све до слоја везе (линка) који додаје и ознаку о почетку (ЗЛ) и крају[2] (ЗК) јединици података. Јединица података 2. слоја, која се назива рам (оквир)

[1] Користи се и термин опоравак од грешака.
[2] *Trailer*

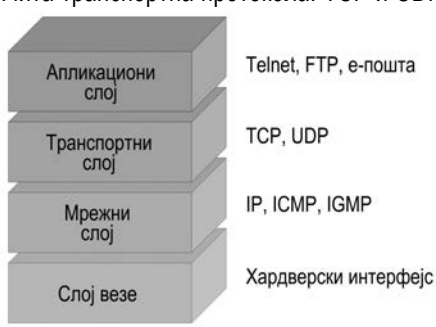
преко физичког слоја прослеђује се на трансмисиони медијум. Када рам стигне до одредишног система на њему се одвија процес обрнутог редоследа. Сваки слој примивши јединицу података уклања управљачке информације (заглавље) њему упућене а остатак прослеђује вишем слоју.

3.2 TCP/IP референтни модел

TCP/IP скуп протокола[1] омогућава рачунарима различитих величина и различитих произвођача који раде под различитим оперативним системима да међусобно комуницирају. Развила их је 1960. године агенција DARPA[2] за мрежу са комутацијом пакета. Од 1990. године то је начин за повезивање рачунара који се највише користи, тј. *de facto* стандард. TCP/IP протоколи су основа Интернета. Скуп TCP/IP протокола је комбинација различитих протокола са различитих слојева. TCP/IP је четворослојни систем као што је приказано на слици 3.7.

Сваки од слојева има различита задужења:

- Слој везе (среће се у литератури и под називом приступ мрежи) води рачуна о свим хардверским детаљима физичког медијума који се користи. Укључује софтверске модуле[3] оперативног система и одговарајуће хардверске интерфејсе[4] датог рачунара;
- Мрежни слој (среће се и под називом интернет слој) води рачуна о кретању пакета кроз мрежу. Преусмеравање (рутирање) пакета извршава се на овом слоју. Протоколи IP[5], ICMP[6] и IGMP[7] чине мрежни слој у TCP/IP скупу протокола;
- Транспортни слој апликационом слоју изнад себе обезбеђује проток података између две станице (рачунара). У TCP/IP скупу протокола постоје два потпуно различита транспортна протокола: TCP и UDP[8].



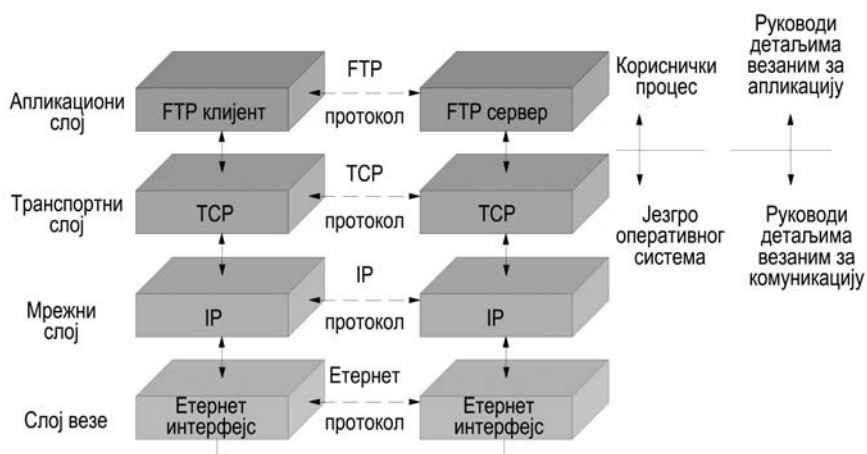
Слика 3.7 Четворослојни скуп TCP/IP протокола

[1] *Transmission Control Protocol /Internet Protocol* (*TCP/IP*)*protocol suite*
[2] *Defense Advanced Research Projects Agency, a* рачунарска мрежа је ARPANET.
[3] *Device driver*
[4] Користе се различити термини: физички интерфејс, мрежне картице, мрежни интерфејс.
[5] *Internet Protocol* (IP) - Интернет протокол. У овом уџбенику користићемо термин IP протокол. Правилније би било само IP пошто у скраћеници слово P већ потиче од протокола (*Protocol*).Ова примедба се односи и на остале протоколе и њихове скраћенице.
[6] *Internet Control Message Protocol*
[7] *Internet Group Management Protocol*
[8] *User Datagram Protocol*

- TCP обезбеђује поуздан проток података између рачунара. Од података које добија од апликације: формира целине (делове) које прослеђује мрежном слоју, шаље потврде о успешном пријему пакета од удаљених рачунара, поставља времена на часовницима[1], итд. Пошто транспортни слој обезбеђује поуздан пренос (ток) података апликациони слој је потпуно ослобођен од ових задатака.
- С друге стране UDP обезбеђује много једноставнију услугу (сервис) апликационом слоју. Он једноставно шаље од једног до другог рачунара пакете података (датаграме). Све захтеве за поузданошћу мора да преузме апликациони слој.

- Апликациони слој води рачуна о карактеристичним детаљима сваке апликације. У скоро свим имплементацијама обезбеђене су следеће апликације:
  - Telnet - удаљени приступ;
  - FTP[2] - пренос датотека;
  - SMTP[3]- електронска пошта;
  - SNMP[4] - надзор и управљање мрежом.

Уколико постоје две станице на једној локалној мрежи (нпр. Етернет) и на обе је покренут FTP који су протоколи укључени приказано је на слици 3.8. Једна апликација је означена као клијент а друга као сервер. Већина мрежних апликација је тако пројектована (клијент-сервер). Сервер обезбеђује одређене врсте услуга клијенту, у овом случају приступ фајловима на серверу. Апликације за удаљени приступ[5] пружају клијенту могућност да се пријави на сервер. Сваки слој има један или више протокола који му обезбеђују комуникацију са „парњаком"[6] на истом слоју. На пример TCP протокол обезбеђује комуника-



Слика 3.8 Две станице са FTP протоколом на локалној рачунарској мрежи Етернет типа

[1] Систем који се користи је следећи: часовници (*timer*) се постављају на одређену вредност, тј. време (*timeout*).
[2] *File Transfer Protcol*
[3] *Simple Mail Transfer Protocol*
[4] *Simple Network Management Protocol*
[5] *Telnet* - удаљени приступ.
[6] *Peer*

цију два транспортна слоја, а IP протокол обезбеђује комуникацију два мрежна слоја. На десној страни слике може се уочити да је уобичајено да је апликациони слој кориснички процес, док су нижа три слоја обично реализована као језгро оперативног система [1].

Постоји још једна битна разлика између највишег слоја и доња три слоја. Апликациони слој води рачуна само о детаљима везаним за апликацију а не о кретању података кроз мрежу. Нижи слојеви не знају ништа о апликацији али руководе кретањем података кроз мрежу.

На слици 3.8 приказана су четири различита протокола, сваки за различити слој: FTP за апликациони слој, TCP за транспортни слој, IP за мрежни слој и Етернет за слој везе. TCP/IP скуп протокола је комбинација више протокола. Без обзира што је назив TCP/IP, TCP и IP су само два протокола. Друго име које се користи је скуп протокола на Интернету [2].

Намена најнижег слоја који води рачуна о приступу мрежи и највишег апликационог слоја сасвим је јасна. Први води рачуна о свему што је везано за комуникациони медијум, као што су бежичне рачунарске мреже или локалне рачунарске мреже по стандарду IEEE802.x [3], док други води рачуна о свему што је везано за корисничку апликацију (FTP, Telnet, итд.). С друге стране разлика између мрежног и транспортног слоја није на први поглед јасно видљива. Да би се боље разумела разлика морамо посматрати не више само једну мрежу већ скуп мрежа.

Најједноставнији начин да се направе међусобно повезане мреже је повезати две мреже са уређајем за преусмеравање – рутером. Позитивна страна рутера је да омогућава везу са различитим типовима физичких мрежа – Етернет, прстен са жетоном, бежичне, тачка-тачка везе, итд. Слика 3.9 приказује разлику између крајњег система (два рачунара на крајевима) и међусистема (рутер у средини). Апликациони слој и транспортни слој користе протоколе с краја на крај [4]. Ови протоколи потребни су само крајњим системима. Мрежни слој обезбеђује протокол од једне станице до друге (скок по скок [5]) и користе га сви системи: и крајњи и међусистеми.

У скупу TCP/IP протокола мрежни слој не обезбеђује поуздану услугу. То значи прослеђује пакете од изворишта до коначног одредишта што је могуће боље, али не гарантује да је пакет и стигао на одредиште. TCP протокол с друге стране обезбеђује поуздану транспортну услугу користећи непоуздану IP услугу. Да би обезбедио поуздану услугу TCP употребљава часовнике, поновно слање пакета, шаље и прима потврде с краја на крај и сл. Рутер по својој дефиницији има два (или више) мрежна интерфејса[6] пошто повезује две (или више) мреже.

Један од циљева Интернета је да од апликације прикрије детаље физичког преноса.

---

[1] На овај начин је реализовано на UNIX оперативном систему.

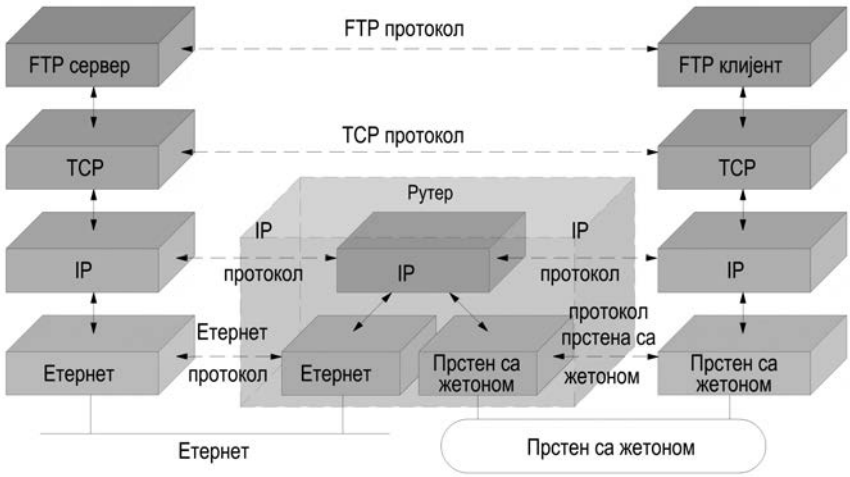
[2] *Internet protocol suite*

[3] У поглављу 12 биће детаљно анализирани протоколи за приступ трансмисионим медијумима у локалним рачунарским мрежама. Организација која се највише бави стандардизацијом локалних рачунарских мрежа је IEEE. Најпознатији стандарди који се односе на локалне рачунарске мреже носе ознаке IEEE802.3 (срећу се и под називом Етернет - енг. *Ethernet*), IEEE802.5 (срећу се под називом прстен са жетоном - енг. *token ring*) і IEEE802.11x (бежичне локалне рачунарске мреже - енг. *wireless*).

[4] *End to end*

[5] *Hop by hop*

[6] Крајња станица (хост) може такође да има више мрежних интерфејса (*multihomed*) али ако није конфигурисана да врши преусмеравање пакета онда се не може назвати рутер.



Слика 3.9 Две TCP/IP мреже међусобно повезане рутером

Као што се види на слици 3.9 (са два мреже) апликациони слојеви не морају да воде рачуна (и не воде рачуна) о томе да је једна станица на Етернет мрежи а друга на прстену са жетоном са рутером између њих. Апликација ће радити на исти начин чак и ако се између њих нађе 20 рутера са додатним врстама мрежних интерфејса. Прикривање ових детаља чини слојевити концепт протокола Интернета толико моћним и корисним решењем.

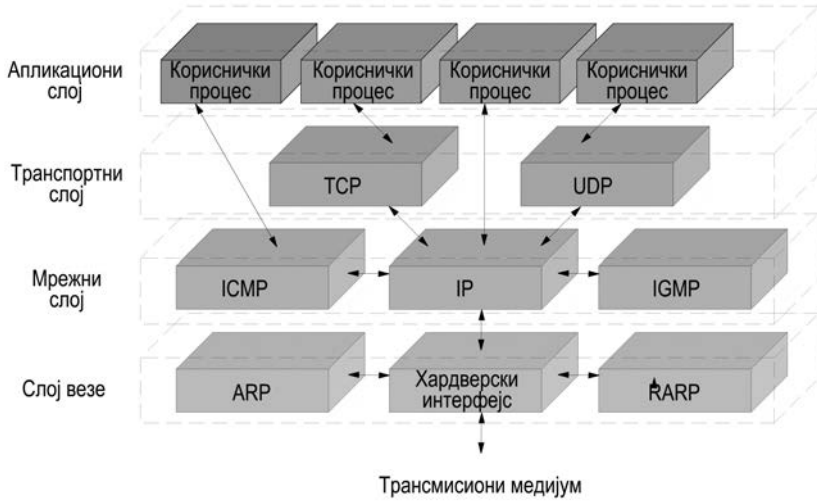
Као што је поменуто у скупу TCP/IP протокола постоји више протокола. На слици 3.10 приказане су њихове међусобне везе. TCP и UDP су доминантни протоколи транспортног слоја. Оба користе IP протокол на мрежном слоју. TCP обезбеђује поуздан пренос без обзира што сервис који користи IP није поуздан. Протокол UDP је за разлику од протокола TCP без успоставе везе (тј. непоуздан). Нема никаквих гаранција да јединица података протокола икада стигне на одредиште. Апликације као што су: систем имена домена DNS [1] или протокол за надзор и управљање у рачунарским мрежама SNMP [2], користе UDP протокол.

IP је главни протокол на мрежном слоју. Користе га и TCP и UDP протоколи. На слици 3.10 такође видимо да неке апликације директно користе IP протокол. Ово се ретко користи али је могуће.

Протокол ICMP [3] је додатак IP . Користе га IP слојеви за међусобну размену порука о грешци и других виталних информација. Апликациони процес такође може директно да користи ICMP протокол.

Протокол IGMP се користи код слања UDP пакета ка више рачунара (хостова). Специјална врста протокола су и ARP [4] и RARP [5]. Користе се да би претворили адресу коју користе IP слојеви у адресу која се користи на слоју везе (мрежни интерфејси као што је нпр. Етернет или прстен са жетоном).

[1] *Domain Name System*
[2] *Simple Management Transfer Protocol*
[3] Два популарна алата за дијагностику *Ping* и *Traceroute* користе ICMP протокол.
[4] *Adress Resolution Protocol*
[5] *Reverse Adress Resolution Protocol*



Слика 3.10 Протоколи на различитим слојевима TCP/IP референтног модела

Стандарди и TCP/IP

TCP/IP је постао популаран и међу онима који га развијају и међу онима који га користе. Разлог је његова отвореност и стално иновирање. Исто важи и за Интернет као отворену комуникациону мрежу. Ова отвореност брзо би постала велика мана уколико не би била контролисана. Не постоји државна организација која се бави правилима и прописима на Интернету. Контрола се највише заснива на међусобним договорима, а улогу стандардизационог тела Интернет комуне обавља организација ISOC (табела 1.2). Њом управља тело IAB. Тело IAB ослања се на две организације: IETF за издавање нових стандарда и IANA[1] за усаглашавање онога што користе различити протоколи.

Процес стандардизације на Интернету описан је у RFC 2026[2] који се бави свим протоколима, процедурама и конвенцијама које се користе на Интернету, независно од тога да ли јесу (или нису) део скупа TCP/IP протокола.

Скуп протокола на Интернету и даље се развија кроз механизам RFC. Нове протоколе (најчешће апликациони) истраживачи пројектују и имплементирају, представљају Интернет комуни у форми предлога[3]. Највећи извор предлога (ID[4]) потиче од организације IETF.

Два популарна интерфејса за апликације (API[5]) које користе TCP/IP протоколе називају се прикључци[6] и TLI[7].

---

[1] *Internet Assigned Number Authorities*

[2] *Internet Standard Process Revision 3*

[3] Неки од ових протокола, нарочито оних који се појављују 1. априла су најблаже речено неприменљиви. На пример RFC 1149 (од 1 априла 1990. год.) описује како голубови преносе IP пакете, а RFC 1437 (од 1. априла 1993. год.) описује пренос људи електронском поштом.

[4] *Internet Draft*

[5] *Application Programming Interface*

[6] *Socket*. Среће се и под називом - *Berkley socket* указујући на место где је првобитно развијен.

[7] *Transport Layer Interface*. Првобитно је развила AT&T и некада се назива XTI (*X/Open Transport Interface*) указујући да је везан за организацију X/Open, интернационалну групу произвођача рачунара који праве свој сопствени скуп стандарда.

3.3 Референтни модел Novell Netware

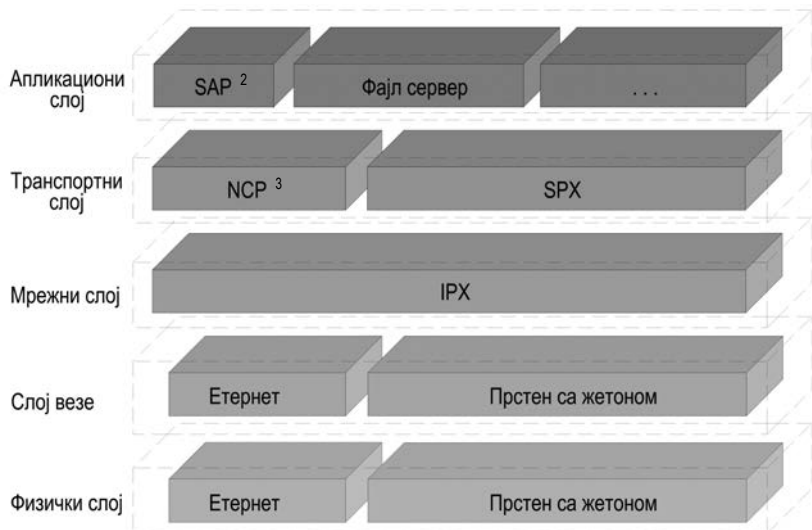
У једном периоду најпопуларнији мрежни оперативни систем за персоналне рачунаре био је Netware компаније Novell. Пројектован је за институције које су са великих рачунара[1] прешле на персоналне рачунаре. У таквим системима сваки корисник има на свом радном месту рачунар који ради као клијент а одговарајући број сервера обезбеђује потребне сервисе. Netware користи одговарајући скуп протокола који је илустрован сликом 3.11. Подсећа више на TCP/IP него на OSI референтни модел.

За физички и слој везе може се одабрати један од стандарда за локалне рачунарске мреже као што је Етернет, прстен са жетоном итд. Мрежни слој обезбеђује протокол без успоставе везе IPX. По својој функцији IPX протокол сличан је IP протоколу осим што користи десетобајтну уместо четворобајтне адресе.

Изнад IPX протокола налази се транспортни протокол са успоставом везе NCP. Протокол NCP поред преноса (транспорта) обезбеђује и друге сервисе. Суштински представља централну тачку Netware оперативног система. Други протокол, SPX такође је доступан али обезбеђује само пренос. Апликације могу да користе било који од поменутих протокола. Презентациони и слој сесије не постоје. На апликационом слоју присутни су различити апликациони протоколи.

3.4 ATM референтни модел

ATM је систем са комутацијом пакета који су тачно одређене величине, од 53 бајта (слика 3.12). Назива се и систем са комутацијом ћелија. Стандард је донела интернационална организација ITU-T а референтни модел се разликује и од OSI и од



Слика 3.11 Novell Netware референтни модел

[1] *Mainframe*
[2] *Service Advertising Protocol*
[3] *Network Core Protocol*

Слика 3.12 Формат ATM пакета (ћелије)

TCP/IP референтних модела. На слици 13.13 представљен је ATM референтни модел. Физички слој води рачуна о специфичностима трансмисионог медијума и техникама кодирања. Брзине података на физичком слоју крећу се од 25,6Mb/s до 622,08Mb/s. Могуће су и друге брзине: и више и ниже. Два слоја референтног модела односе се на ATM функције: ATM слој, заједнички за све услуге које омогућавају пренос и слој за прилагођавање на ATM слој (AAL[1]). ATM слој дефинише пренос података помоћу ћелија и дефинише начин коришћења виртуелних (логичких) веза. Намена слоја за прилагођавање на ATM слој је да обезбеди да и други протоколи (не само ATM) протоколи користе ATM системе. AAL слој повезује информације виших слојева у ATM ћелије (на изворишној страни), усмерава пренос ћелије преко ATM мреже и на одредишној страни преузима информације из ATM ћелија и испоручује их вишим слојевима.

Референтни модел је тродимензионалан и сачињавају га следеће одвојене равни:

- корисничка раван[2] - обезбеђује кориснику све информације потребне за пренос података заједно са управљачким информацијама као што су контрола тока, контрола грешке итд,
- контролна раван[3] - извршава све операције везане за управљање позивом и везом,
- управљање равнима[4] и управљање слојевима[5] - воде рачуна о функцијама везаним за надзор ресурса и координацију између слојева.

Слика 3.13 ATM референтни модел

[1] *ATM Adaptation Layer*
[2] *User plane*
[3] *Control plane*
[4] *Plane management*
[5] *Layer management*

4. Комуникациони модел

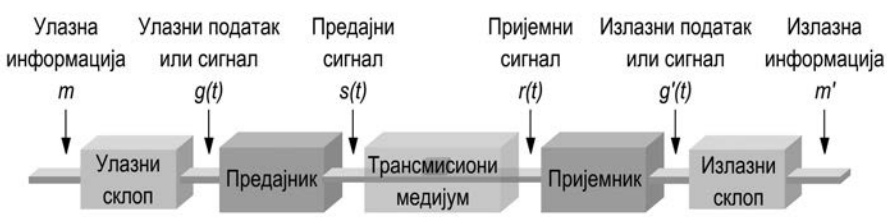
Блок дијаграм једноставног комуникационог модела дат је на слици 4.1. Основна намена преноса података је да преноси поруке између два корисника. На слици информација коју треба пренети садржана је у поруци означеној са *m*. Ова порука, која се преноси као податак, генерално је представљена предајнику као сигнал променљив у времену *g(t)*.

Појмови податак и информација често се користе и могу се дефинисати на следећи начин:

- податак је репрезентација чињеница, концепта или инструкција форматизованих на начин погодан за комуникацију и интерпретацију, обрађена од стране човека или неког средства за аутоматску обраду,
- информација је значење које човек додељује подацима преко конвенција које примењује на те податке.

Ове дефиниције могу да буду академске, али за ову намену може им се дати следећа интерпретација: подаци могу да буду идентификовани, подаци се могу описати; подаци не морају да представљају нешто физичко у смислу нечега што се може измерити. Али подаци могу и треба да се користе за стварање информација. Подаци за једну особу су информација за другу. Информација се стиче када се подаци интерпретирају. Да би се пренела информација потребан је приступ елементима података и могућност да се пренесу.

Вратимо се на слику 4.1; потребно је пренети сигнал *g(t)*. Ако сигнал није у форми погодној за пренос и он мора бити претворен (конвертован) у сигнал *s(t)* који је прилагођен карактеристикама трансмисионог медијума. Сигнал се, затим, преноси преко медијума. Друга страна прима сигнал *r(t)*, који због оштећења при преносу сигнала може да се разликује од *s(t)*. Овај сигнал пријемник конвертује у форму погодну за излаз. Конвертовани (претворени) сигнал *g ’t)* је апроксимација (процена) улазног сигнала *g(t)*. На крају, излазни модул предаје процењену поруку *m*’ одредишном кориснику. На слици 4.1 представљен је један смер везе, а исти модел се користи за други смер када је веза двосмерна. У том случају на обе стране комуникационог система налазе се примопредајници (модеми), односно улазно/излазни (У/И) склопови.



Слика 4.1 Комуникациони модел

Представићемо овај пример на коришћењу електронске поште. Претпоставимо да су улазни склоп и предајник компоненте персоналног рачунара. Корисник жели да пошаље поруку другом кориснику, на пример; „Почетак наставе је 16. фебруара." (*m*). Овај низ карактера садржи информацију. Корисник активира електронску пошту на персоналном рачунару и уноси поруку преко тастатуре (улазни склоп). Низ карактера (симбола) спакован је у меморију. Поруку можемо видети као секвенцу карактера *g* или као низ (секвенцу) битова (*g*) у меморији. Рачунар је везан за неки трансмисиони медијум, као што је телефонска линија или локална рачунарска мрежа преко У/И склопа као што је примопредајник локалне мреже или модем. Улазни подаци преносе се ка предајнику као секвенца битова (низ „0" и „1") *g(t)*, или као низ напонских (струјних) промена *g(t)* кроз неку комуникациону магистралу или кабл. Предајник је прикључен директно на медијум и претвара долазеће битове у сигнал *s(t)* погодан за пренос.

Предајни сигнал *s(t)* упућен на средину за пренос предмет је деловања бројних изобличења и сметњи пре него што дође до пријемника. Због тога примљени сигнал *r(t)* може да се разликује од *s(t)*. Пријемник може да процени природу *s(t)* засновану на *r(t)* и свом познавању медијума производећи секвенцу битова *g'(t)*. Битови се шаљу излазном рачунару и смештају у меморију као блок битова или карактера *g'(t)*. Одредишни систем покушаће да одреди да ли се појавила грешка. Ако се то деси сарађиваће са предајним системом да би евентуално добио комплетан, без грешке, блок података. Ове податке корисник може да прегледа преко неког од излазних уређаја као што је на пример монитор или штампач. Порука коју корисник може да прегледа (*m*') није потпуно идентична са послатом поруком *m*. У неким применама[1] то је довољно за успешан пренос. У другим применама[2] пренос се обавља док се не добије идентична порука.

4.1 Пренос података

Успешан пренос података зависи у принципу од два фактора:

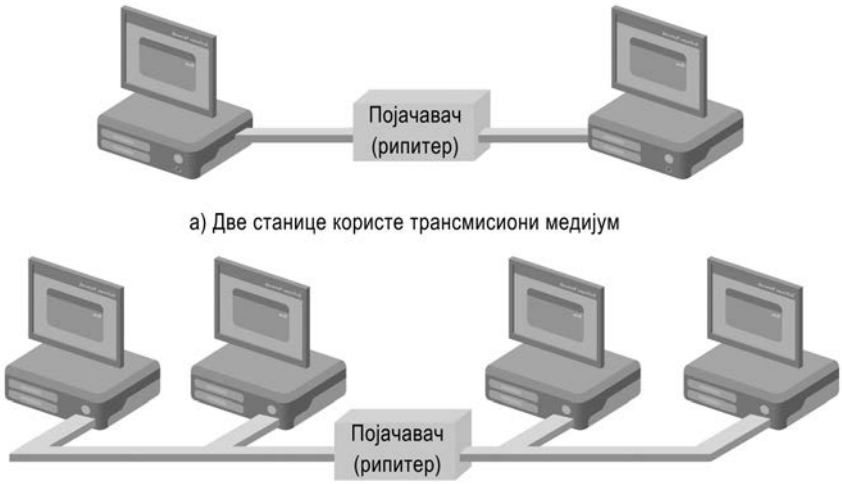
- квалитета сигнала који се преноси,
- карактеристика трансмисионог медијума.

Концепт и терминологија

Пренос података обавља се између предајника и пријемника преко трансмисионог медијума. Трансмисиони медијум може да буде жични[3] и бежични[4]. Жични медијум физички повезује крајње станице. Пример су упредена телефонска парица, коаксијални каблови и оптичка влакна. Са бежичним медијумом крајње станице нису физички повезане већ се сигнали преносе кроз нпр. ваздух, вакуум и море.

Термин директна веза (линк) користи се за преносни пут између два уређаја уколико се сигнал преноси директно од предајника ка пријемнику, без икаквих уређаја између њих осим појачавача и уређаја који обнављају сигнал[5]. На слици 4.2 приказана је директна

[1] Дигитализовани говор
[2] Банкарске трансакције
[3] *Hardwire*
[4] *Softwire*
[5] Користе се термини рипитер (енг. *repeat*) и регенератор.



Слика 4.2 Конфигурације а) тачка-тачка, б) више тачака

веза. Уочимо да се овај термин може искористити и за жичне и за бежичне медијуме.

Постоје два типа веза: тачка-тачка[1] и више тачака[2]. Када постоји директна веза између два уређаја (станице) и само они деле медијум, веза се назива тачка-тачка (слика 4.2а). У конфигурацији са више тачака више од два уређаја деле медијум (4.2б). У оба случаја канал или веза могу да буду симплекс , полу дуплекс, или потпуни дуплекс . У симплекс преносу сигнал се преноси само у једном правцу; једна станица је предајник а друга пријемник. У полудуплекс операцији обе станице могу да преносе сигнал, али само једна по једна. У потпуном дуплексу обе станице могу да шаљу сигнале истовремено.

Фреквенцијски домен

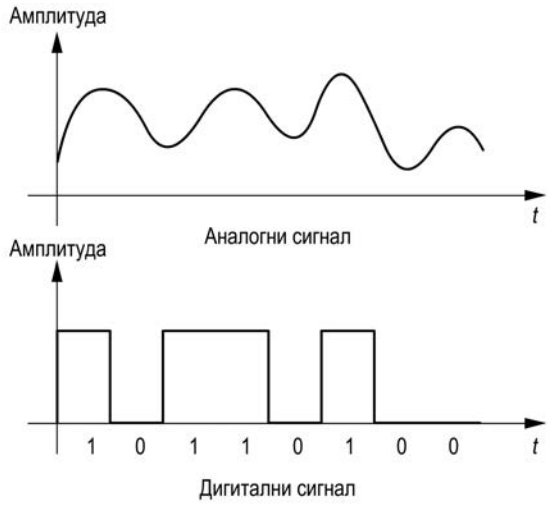
У анализама које следе бавићемо се електромагнетским сигналима као средством за пренос порука. На слици 4.3 сигнал који генерише предајник шаље се преко преносног медијума[3]. Сигнал је функција времена, али се такође може описати и као функција учестаности. Значи, сигнал се може представити сумом простопериодичних компоненти различите учестаности. Посматрање слике сигнала у фреквенцијском домену много је важније за разумевање преноса података од посматрања сигнала у временском домену.

Временски домен

Посматрано у функцији времена, електромагнетски сигнал може бити аналогни[4] или дигитални[5]. Аналогни сигнал је онај чији се интензитет мења континуално у времену.

Математичка дефиниција је: сигнал *s(t)* је континуалан уколико је за свако *a*:

[1] *Point to point*
[2] *Multipoint*
[3] Користе се термини: средина за пренос, преносни медијум и трансмисиони медијум.
[4] Математички континуалан
[5] Математички дискретан



Слика 4.3 Аналогни и дигитални сигнали

$$\lim_{t \to a} s(t) = s(a) \tag{4.1}$$

Другим речима, не постоје прекидне тачке или дисконтинуитети. Сигнал је дигиталан уколико је његов интензитет константног нивоа у одређеном периоду времена а затим се промени на други константан ниво [1]. Слика 4.3 показује пример обе врсте сигнала. Континуалан сигнал може да представља говор, а дигиталан сигнал може да репрезентује бинарно 1 или 0.

Најједноставнија врста сигнала је периодичан сигнал у коме се после одређеног временског интервала T понавља исти облик сигнала. Слика 4.4 показује пример периодичног континуалног сигнала (синусни сигнал) и периодичног дискретног сигнала (правоугаони сигнал). Математички сигнал $s(t)$ је периодичан ако и само ако је:

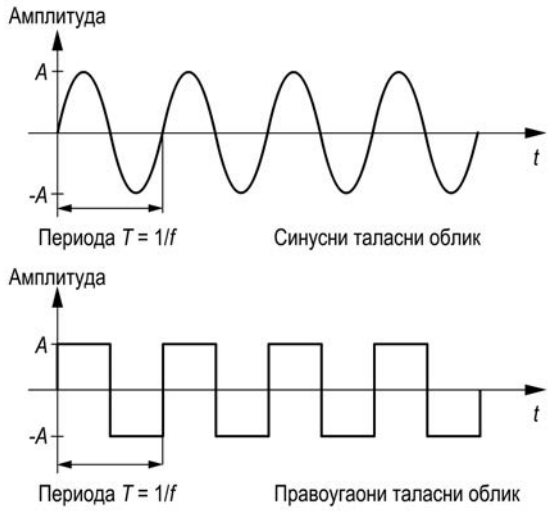
$$s(t + kT) = s(t) \quad -\infty < t < +\infty, \quad k = 1, 2... \tag{4.2}$$

Најједноставнији периодични сигнал је простопериодични сигнал. Три важне карактеристике простопериодичног сигнала су амплитуда (A), фреквенција (f_0) и фаза (θ). Амплитуда је максимална вредност сигнала и мери се у волтима (V). Фреквенција је инверзна периоди ($1/T_0$) и једнака је броју понављања периоде у секунди; изражава се у циклусима у секунди [2], или херцима (Hz). Фаза је мера релативне позиције у времену у оквиру једног периода сигнала. Као пример слика 4.5 показује два простопериодична сигнала која су фазно померена за $\pi/2$ радијана (2π радијана 360°= 1период). Тако можемо да представимо синусоиду као:

$$s(t) = A\sin(2\pi f_0 t + \theta) \tag{4.3}$$

[1] Ово је дефиниција идеалног случаја. У стварности, прелазак (транзиција) са једног напонског нивоа на други није тренутна, већ постоји одређени прелазни период.

[2] *Cps*



Слика 4.4 Пример периодичног сигнала: синусни и правоугаони таласни облик

где је A амплитуда, f_0 је учестаност, а θ је фаза. Уочимо да се синусни сигнал на слици 4.5 може представити као један од сигнала:

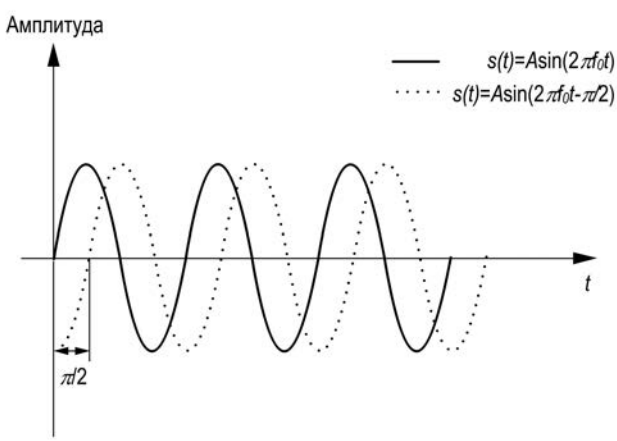
$$s(t) = A\sin(2\pi f_0 t) \tag{4.4}$$

$$s(t) = A\cos(2\pi f_0 t - \frac{\pi}{2}) \tag{4.5}$$

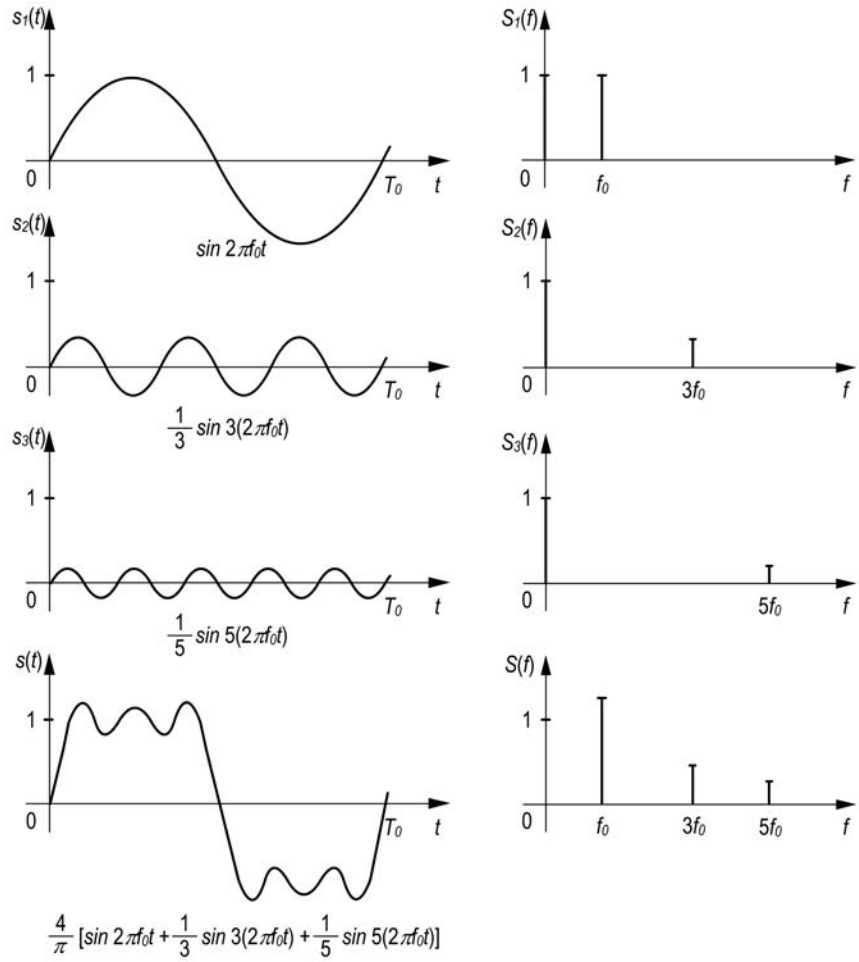
Концепт фреквенцијског домена

До сада смо сигнал посматрали као функцију времена. Сигнал се може посматрати и у функцији фреквенције (слика 4.6) тако што ће се представити сумом простопериодичних сигнала.

$$s(t) = \frac{4}{\pi}\left[\sin 2\pi f_0 t + \frac{1}{3}\sin 3(2\pi f_0)t + \frac{1}{5}\sin 5(2\pi f_0)t\right] \tag{4.6}$$



Слика 4.5 Пример разлике у фази синусног сигнала



Слика 4.6 Сигнал са три фреквенцијске компоненте у временском и фреквенцијском домену

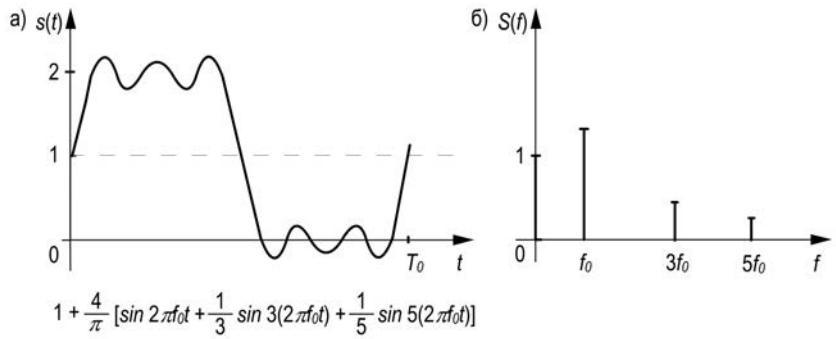
Посматрајући слику 4.6 можемо да уочимо следеће:

- компоненте овог сигнала су синусни таласи фреквенције f_0, $3f_0$ и $5f_0$,
- када су све фреквенцијске компоненте сигнала целобројни умножци једне одређене учестаности онда се она назива основна учестаност,
- период резултујућег сигнала *s(t)* једнак је периоди сигнала основне учестаности. Периода компоненте $sin\ 2\pi\ f_0 t$ је $T_0=1/f_0$, а периода сигнала *s(t)* је такође T_0.

Можемо показати, користећи дисциплину која се назива Фуријеова [1] анализа, да се било који електромагнетски сигнал може представити као скуп простопериодичних аналогних сигнала (синусоида) различите амплитуде, учестаности и фазе.

Можемо рећи да за сваки сигнал постоји функција у временском домену, *s(t),* којом је одређена вредност сигнала у сваком тренутку времена. Слично, постоји функци-

[1] Француски математичар *Jean-Baptiste Fourier*



Слика 4.7 Сигнал са једносмерном компонентом: а) у временском б) у фреквенцијском домену

ја у фреквенцијском домену, *S(f),* која специфицира амплитуду (максималну вредност) компоненти од којих се тај сигнал састоји. Та функција назива се амплитудски спектар. Слика 4.6б показује амплитудски спектар у фреквенцијском домену за сигнале на слици 4.6а. Уочимо да је у овом случају *S(f)* дискретна функција. Спектар сигнала заузима одређени опсег учестаности. За сигнал са слике 4.6а спектар се простире од f_0 до $5f_0$. У претходном случају ширина опсега спектра сигнала[1] је $4f_0$. Многи сигнали имају неограничен спектар. Међутим, највећи део снаге сигнала који представљају реалне поруке садржан је у релативно уском опсегу учестаности. Овај опсег учестаности назива се ефективни опсег спектра или само опсег спектра сигнала.

Термин који је потребно дефинисати је једносмерна[2] компонента. Уколико сигнал садржи и компоненту нулте учестаности та компонента је једносмерна или константна компонента. Без једносмерне компоненте сигнал има средњу вредност једнаку нули. Са једносмерном компонентом он има компоненту на *f=0*, и средњу вредност различиту од 0. На пример на слици 4.7 приказано је додавање једносмерне компоненте сигналу са слике 4.6а па једначина (4.6) сада гласи:

$$s(t) = 1 + \frac{4}{\pi}\left[\sin 2\pi f_0 t + \frac{1}{3}\sin 3(2\pi f_0)t + \frac{1}{5}\sin 5(2\pi f_0)t\right] \qquad (4.7)$$

На слици 4.8 представљен је импулс у времену који има вредност 1 између $-T/2$ и $+T/2$ и 0 за остале тренутке времена. Његова слика у фреквенцијском домену *S(f)* приказана је на слици 4.8б. Спектар овог сигнала *S(f)* је неограничена функција учестаности[3].

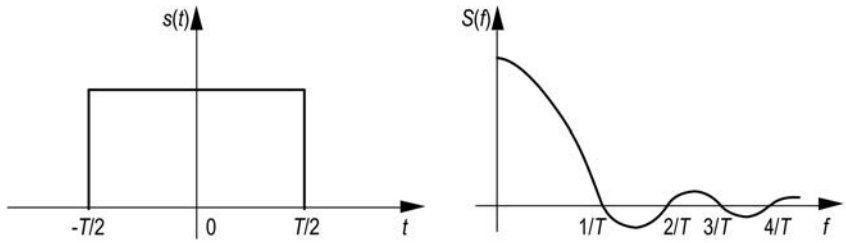
4.2 Веза између брзине података и опсега

Дефинисали смо да је ефективни опсег спектра сигнала онај опсег спектра у коме је сконцентрисан највећи део енергије сигнала. Термин „највећи" употребљен је прилично произвољно. Важно је уочити да иако задати таласни облик може да садржи учестаности из веома широког опсега, било који преносни систем (предајник, трансми-

[1] У литератури се среће и други начин дефинисања опсега: од 0 до $5f_0$.

[2] *Direct current*

[3] У ствари, функција *S(f)* у овом случају је симетрична у односу на $f = 0$, тако да садржи и вредности за негативне учестаности. Присуство негативне учестаности је математички део и објашњење је ван домена овог уџбеника.



Слика 4.8 Правоугаони импулс вредности 1, трајања од +T/2 до -T/2 у временском и фреквенцијском домену

сиони медијум и пријемник) може да прихвати само ограничени опсег учестаности. Ово као последицу даје ограничење у брзини података који могу да се пренесу тим трансмисионим системом.

У једноставном примеру, погледајмо правоугаони таласни облик на слици 4.9а. Претпоставимо да позитиван импулс представља бинарно 1 а негативни импулс бинарно 0. Сигнал тада представља бинарни низ 1010...па је периода овог сигнала T_0 једнака двоструком трајање импулса[1] T_b ($T_0 = 2T_b$). Ако је брзина података бинарне поворке импулса R (b/s), онда је трајање једног импулса $T_b = 1/R$, периода бинарног низа је $T_0 = 2/R$ а учестаност $f_0 = R/2$. Које су простопериодичне компоненте овог сигнала? Да бисмо одговорили на ово питање посматрајмо слику 4.6. Сабирањем синусних компонената учестаности f_0 и $3f_0$, па затим додавањем $5f_0$ видели смо да је добијени таласни облик све сличнији правоуганом таласном облику периоде f_0. Показаћемо да се правоугаони таласни облик са слике 4.9 може аналитички представити као:

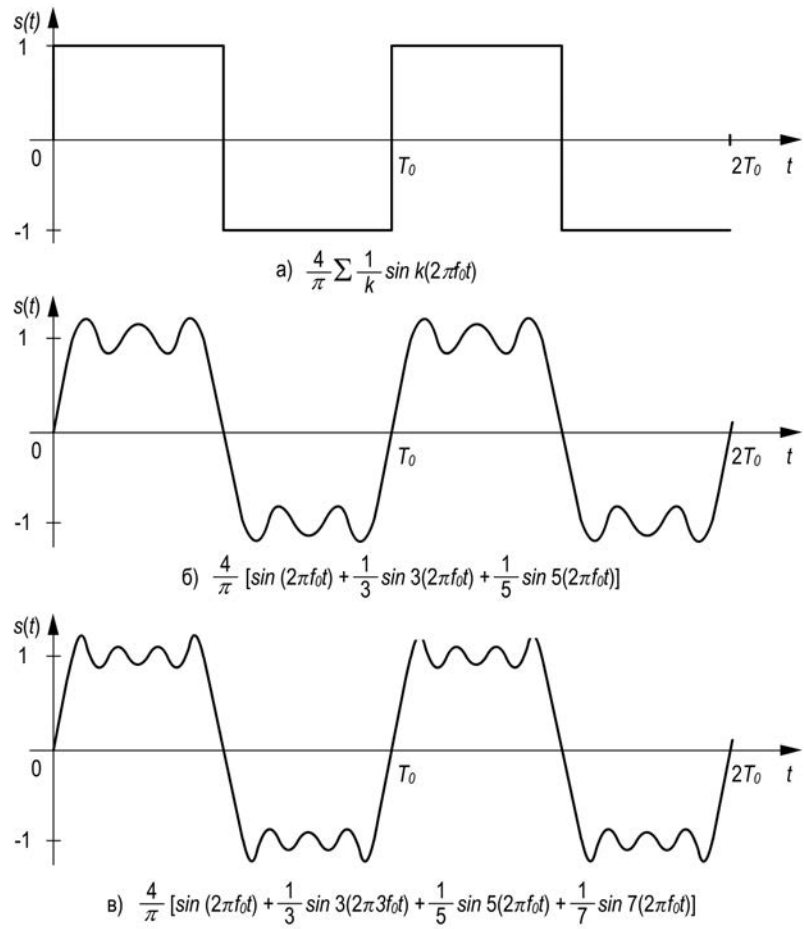
$$s(t) = \frac{4A}{\pi}\sum\frac{1}{k}\sin k(2\pi f_0 t) \quad \text{где је } k \text{ непаран број } \{1, \infty\} \tag{4.8}$$

Види се да максимална амплитуда синусних компонената опада, тако да је максимална амплитуда k-те фреквенцијске компоненте (учестаности kf_0) једнака $1/k$ од максималне амплитуде првог хармоника (учестаности f_0). Снага простопериодичног сигнала пропорционална је квадрату амплитуде тог простопериодичног сигнала.То значи да је снага сигнала сконцентрисана у првих неколико фреквенцијских компонената. Шта ће се десити уколико ограничимо опсег спектра сигнала на само прве три фреквенцијске компоненте? Такав сигнал приказан је на слици 4.9б, а упоређивањем видимо да је он веома сличан оригиналном правоугаоном сигналу (слика 4.9а). Додавањем синусне компоненте учестаности $7f_0$ таласни облик се значајно не мења (слика 4.9в).

Ову слику можемо употребити да бисмо илустровали везу између брзине података и опсега. Претпоставимо да користимо дигитални преносни систем који може да преноси сигнале чији спектар је опсега 4MHz. Послаћемо секвенцу бита која се састоји од наизменичних „1" и „0" (као што је правоугаони сигнал на сл. 4.9а).

Апроксимирајмо ову секвенцу бита сигналом на слици 4.9б. Иако је овај сигнал

[1] У овом примеру поворка 1010... је периодичан сигнал и његова периода једнака је двоструком трајању битског интервала. Ако бисмо посматрали неку другу периодичну поворку на пример 100100...њена периода била би једнака троструком трајању битског интервала итд.



Слика 4.9 Компоненте правоугаоног таласног облика

„изобличени" правоугаони сигнал, он је довољно сличан правоугаоном тако да ће пријемник моћи да направи разлику између бинарног „1" и бинарног „0". Уколико претпоставимо да је f_0=1MHz, онда је опсег спектра сигнала (слика 4.6б):

$$B^{1}=5f_0-f_0=5\text{MHz}-1\text{MHz}=4\text{MHz} \tag{4.9}$$

Уочимо да за f_0=1MHz, периода $T_0=1/10^6=10^{-6}$=1μs. Пошто смо претпоставили да се сигнал састоји од наизменичних „1" и „0", једна периода се састоји од једне „1" и једне „0". Трајање сваког бита је 0,5μs, а брзина (број бита у једној секунди) је $1/(0{,}5*10^{-6})=2*10^6=2$Mb/s. То значи да је за брзину од 2Mb/s довољно пренети опсег спектра сигнала од 4MHz, односно обезбедити ширину канала од 4MHz.

На основу претходне анализе можемо да закључимо следеће: дигитални сигнал генерално има спектар неограничене ширине (једначина 4.8). Уколико покушавамо да пошаљемо сигнал преко било каквог трансмисионог медијума преносни систем ће

[1] Разлика између највише и најниже компоненте у спектру.

ограничити опсег спектра сигнала који желимо да пошаљемо. С друге стране што је шири пропусни опсег трансмисионог медијума то је његова цена већа. Због тога економски и практични разлози налажу да се дигиталне информације шаљу сигналима ограниченог опсега спектра. Ограничење опсега спектра сигнала генерише изобличења која отежавају интерпретацију примљеног сигнала. Што се опсег спектра сигнала више ограничава то се повећава изобличење сигнала и повећава се могућност грешке на пријему.

На слици 4.10 графички је приказана претходно спроведена анализа за брзину података од 2000b/s. Посматрамо дигитални сигнал који пропуштамо кроз преносни систем различитог пропусног опсега: од 500Hz до 4000Hz. Са пропусним опсегом од 2500Hz или чак 1700Hz излазни сигнал довољно добро представља оригинални дигитални сигнал. Можемо да генерализујемо овај резултат: уколико је дигитални сигнал брзине *R* (b/s) онда се веома добро представљање сигнала може постићи опсегом спектра сигнала од 2**R* (Hz). Уколико шум није велики оригинални сигнал може се реконструисати мада је примљени (пренесени) сигнал мањег опсега спектра. Постоји директна веза између брзине сигнала и опсега спектра сигнала. Што је већа брзина сигнала већи је ефективни опсег спектра тог сигнала. Посматрано на други начин: што је већи пропусни опсег преносног система то је већа брзина података која се њиме може пренети.

4.3 Снага сигнала

Важан параметар у било ком систему преноса је снага сигнала који се преноси. Сигнал се преноси трансмисионим медијумом и долази до губитка или слабљење снаге сигнала. Да би се надокнадио губитак и повећала снага сигнала могу се у одређеним тачкама везе поставити појачавачи. Уобичајено је појачање [1] (*G*), слабљење [2] (*L*) и релативне нивое посматрати у децибелима пошто:

- снага сигнала обично опада експоненцијално са растојањем, тако да се губитак једноставно описује преко децибела који су логаритамска јединица,
- добитак и губитак у каскадном преносном путу могу се израчунати једноставним операцијама сабирања или одузимања.

Децибели су мера за разлику између нивоа два сигнала:

$$N_{dB} = 10\log\left(\frac{P_2}{P_1}\right) \tag{4.10}$$

где је:

N_{dB} - разлика у децибелима,

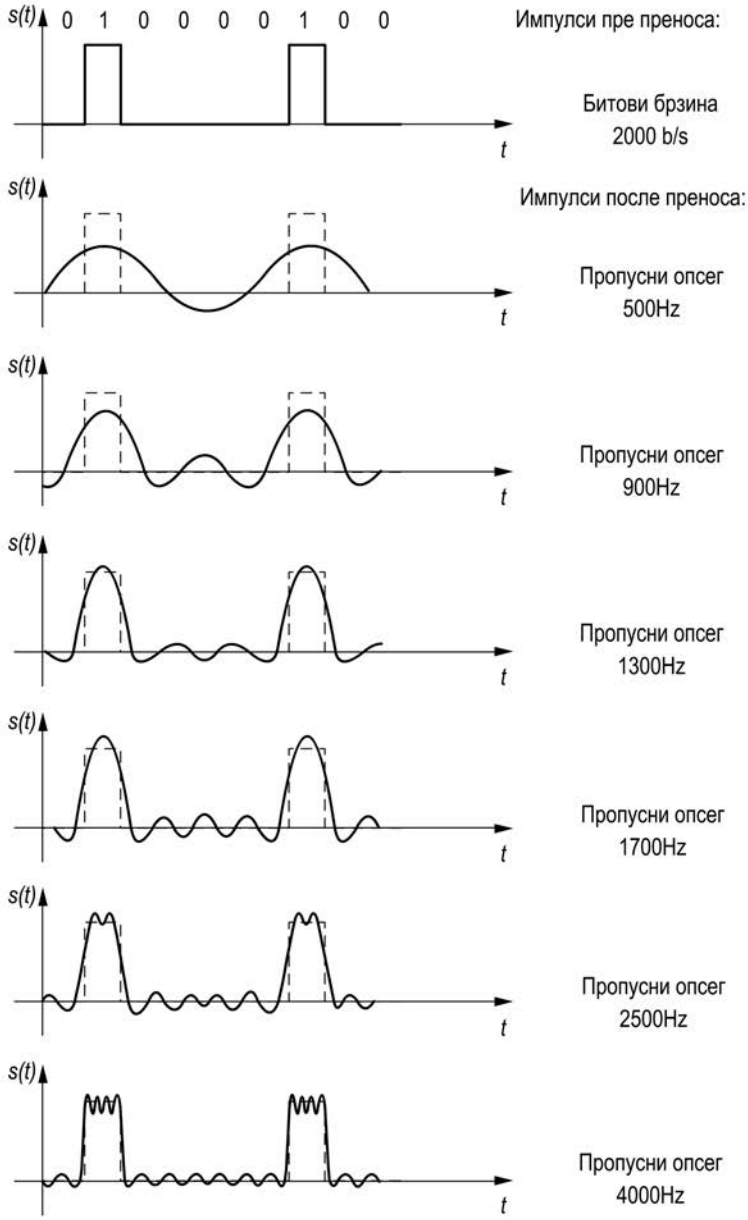
P_1 - снага сигнала на улазу система,

P_2 - снага сигнала на излазу система,

log x - логаритам за основу 10 ($\log_{10} x$).

Када је однос снага дефинисан као у једначини 4.10 онда појачање (*G*) има позитивну вредност а слабљење (*L*) негативну вредност. Слабљење се може дефи-

[1] *Gain*
[2] *Loss*



Слика 4.10 Утицај пропусног опсега канала

нисати као однос снаге сигнала на улазу и излазу система и тада је његова вредност позитивна а појачање је негативно.

На пример (користећи једначину 4.9), уколико треба пренети сигнал снаге 10mW и ако је после одређеног растојања снага тог сигнала 5mW његово слабљење може се изразити на следећи начин:

$$L = 10\log\left(\frac{5}{10}\right) = 10 * (-0.3) = -3\text{dB}$$

Уочимо да је децибел мера релативне (а не апсолутне) разлике. Смањење снаге са 1000W на 500W такође је губитак -3dB. Децибел се исто тако користи за мерење разлике у напону. Узимајући да је снага пропорционална квадрату напона:

$$P = \frac{U^2}{R} \tag{4.11}$$

где је:

P - снага која се дисипира преко отпорника *R*,

U - напон на отпорнику *R*

па је:

$$N_{dB} = 10\log\left(\frac{P_2}{P_1}\right) = 10\log\frac{U_2^{\,2}/R}{U_1^{\,2}/R} = 20\log\frac{U_2}{U_1} \tag{4.12}$$

Децибел је погодан за одређивање свеукупне разлике нивоа у преносном систему, који се састоји од преносних линија на којима долази до опадања снаге сигнала (слабљења) и појачавача који се постављају да би тај губитак надокнадили (појачања). Вредност у децибелима односи се на релативну величину или промене у величини, не на апсолутни ниво. Некада је потребно ослонити се на апсолутни ниво снаге или напона у децибелима. У употреби је неколико изведених јединица.

У микроталасним апликацијама користи се јединица dBW (децибел ват). Вредност од 1W изабрана је као референтна и означава 0dBW. Апсолутни ниво снаге у децибелима дефинише се као:

$$P_{dBW} = 10\log\left(\frac{P_W}{1\text{W}}\right) \tag{4.13}$$

На пример снага од 1000W може се представити као 30dBW, а снага од 1mW као -30dBW. У видео апликацијама користи се јединица dBmV (децибел миливолт). Вредност од 1mV изабрана је као референтна и означава 0dBmV. Апсолутна вредност напона у децибелима дефинисана је као:

$$U_{dBmV} = 20\log\frac{U_v}{1\text{mV}} \tag{4.14}$$

На пример, посматрајмо тачка-тачка везу две станице са слике 4.2а. Претпоставићемо да је слабљење на преносном путу од једне станице до појачавача 13dB, појачање појачавача 30dB, а слабљење на преносном путу од појачавача до друге станице 40dB. Свеукупна разлика је -13 + 30 - 40 = -23dB. Уколико је снага сигнала на улазу првог дела преносног пута -30dBW онда је снага излазног сигнала, тј. снага примљеног сигнала на месту друге станице -53dBW.

5. Аналогни и дигитални пренос података

У преносу података од извора до одредишта мора се водити рачуна о природи података, о уређајима који обезбеђују преношење података, о томе какво процесирање или прилагођавање се може захтевати дуж преносног пута, а које би обезбедило разумљиве пријемне податке. Сигнал је електрична или електромагнетска презентација података. За све анализе најважније је да ли се ради о аналогним или дигиталним сигналима. Термин аналогни или дигитални односи се, грубо посматрано, на континуални и дискретни сигнал, респективно. Ова два термина користе се често у преносу података у најмање три контекста:

- подаци,
- сигнализација,
- трансмисија.

Ми посматрамо податке који се разликују од информација. За сада дефинишемо податке као целине које садрже значење. Сигнализација је чин пропагације сигнала преко одговарајућег медијума. На крају, трансмисија је пренос података пропагацијом и процесирањем сигнала. Покушаћемо да разјаснимо ове апстрактне појмове анализирајући термине „аналогни" и „дигитални", сигнали или подаци.

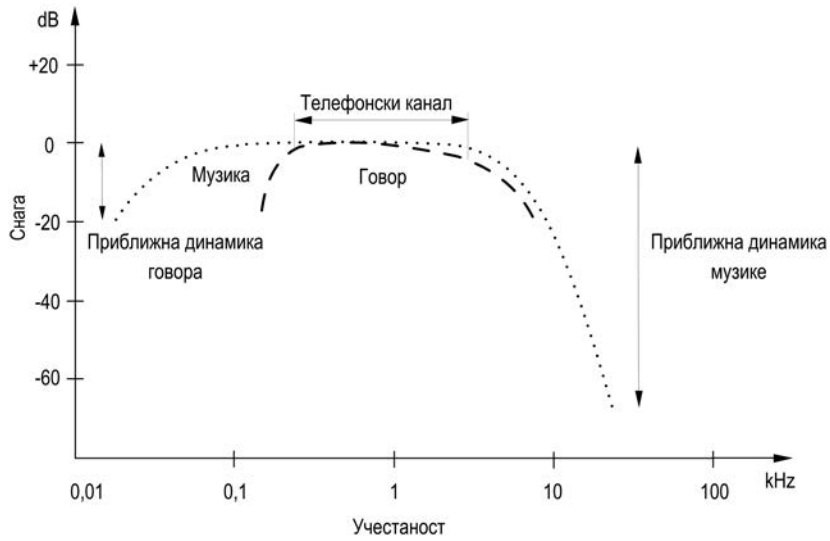
5.1 Подаци

Концепт аналогних и дигиталних података веома је једноставан. Аналогни подаци узимају континуалне вредности на неком интервалу. На пример, говор и видео су целине које су континуално променљиве по интензитету. Већина података које сакупљају сензори, као што су температура и притисак, су континуално променљиве. Дигитални подаци узимају дискретне вредности, пример су слова, карактери и цели бројеви.

Нама најближи појам аналогних података је звук (аудио податак) који људи могу у форми звучних таласа, директно примати. Слика 5.1 показује спектар говора и музике. Фреквенцијске компоненте говора могу се наћи између 100Hz и 8 - 9kHz. Много ужи опсег омогућиће прихватљиву репродукцију говора. Иако је доста енергије говора (слика 5.2) сконцентрисано на нижим учестаностима, тестови су показали да фреквенције до 600 и 700Hz додају веома мало разумљивости говору с обзиром на функционисање људског уха.

Испрекидана линија много тачније одражава разумљивост или емоционални садржај говора. Типично, говор је динамике 25dB. То значи да снага сигнала најјаче вике може да буде најмање 300 пута већа него најмањи шапат. Људско ухо чује учестаности које су у опсегу од 20Hz до 20kHz.

Нама најближи пример дигиталних података јесте текст или скуп карактера. Док су текстуални документи за човека уобичајени они се не могу у облику карактера једно-



Слика 5.1 Акустички спектар говора и музике

ставно запамтити или послати неким од система за обраду и пренос података. Ови системи пројектовани су за бинарне податке. Развијени су многи кодови који карактере представљају као скуп (секвенце) битова. Најстарији пример је Морзеов кôд. Данас се најчешће користи IRA [1] кôд. Сваки карактер у овом коду представља се јединственом комбинацијом од седам битова. На тај начин може се представити 128 различитих карактера. Ово је већи број од онога који је потребан и нека од комбинација предствља невидљиве контролне (управљачке) карактере. IRA карактери памте се у меморији и шаљу као комбинација од осам битова по карактеру. Осми бит назива се бит парности и користи се за детекцију грешке. Поставља се на такву вредност да је укупан број битова у карактеру, који имају вредност један, увек паран[2]. Грешке у преносу које доведу до промене једног бита, или непарног броја битова, могу се детектовати на пријему.

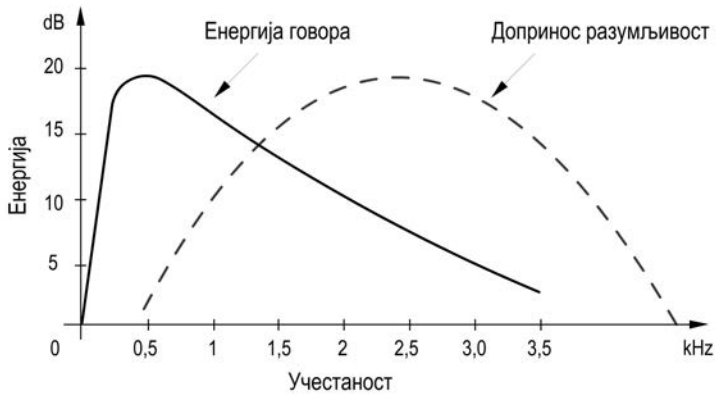
5.2 Сигнали

У комуникационом систему подаци се преносе из једне тачке у другу посредством електричних сигнала. Аналогни сигнал је континуални променљиви електромагнетски талас који се може простирати преко различитих медијума, зависно од његовог спектра; пример су жични медијуми као што су упредене парице и коаксијални каблови, оптички каблови и бежични - атмосфера и пропагација кроз ваздух.

Дигитални сигнал су секвенце напонских (струјних) импулса који се могу преносити преко жичног медијума; на пример константни позитивни напон може да представља бинарно 1, а константни негативни напон бинарно 0.

[1] IRA (*International Reference Alphabet*) је дефинисана у ITU-T препоруци T-50 и позната је као IA5 (*International Alphabet Number 5*). Верзија IRA која се користи у САД (а и шире) носи ознаку ASCII (*American Standard Code for Information Interchange*).

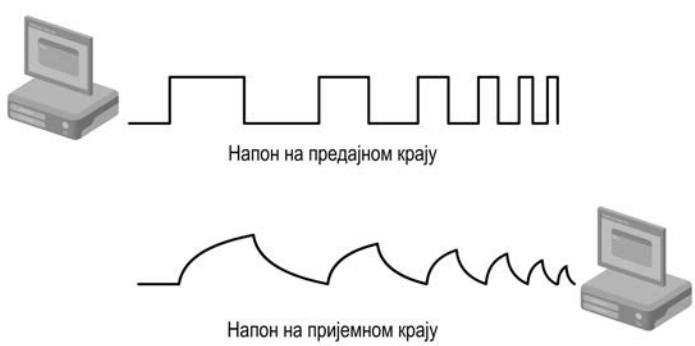
[2] Или непаран зависи од договора. Користе се термини „парна парност" и „непарна парност" који означавају да је свеукупни број јединица у осмобитном карактеру паран или непаран.



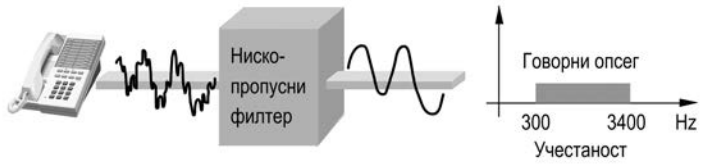
Слика 5.2 Спектар говора

Предност дигиталних сигнала је у томе што су њихово генерисање и пренос генерално јефтинији од аналогних сигнала, а мање су осетљиви на сметње. Мана им је што су на истом растојању значајније ослабљени од аналогних сигнала. На слици 5.3 приказана је секвенца напонских импулса коју је генерисао извор користећи два напонска нивоа и сигнал на пријемној страни. Због већег слабљења снаге сигнала на вишим учестаностима импулси су постали заобљени и смањени. Јасно је да ово слабљење брзо води до губитка информације која је садржана у сигналу који се простире кроз проводник.

Као пример аналогног података анализираћемо говор и предвидети ширину његовог спектра. Звук као податак може се представити директно преко електромагнетског сигнала који заузима исти опсег спектра. У ствари, указује се потреба да се направи компромис између квалитета говора који се преноси електричним путем и цене преноса која се повећава с повећањем пропусног опсега. Иако је, као што је поменуто, спектар говора приближно између 100Hz и 8-9kHz и мања ширина спектра обезбеђује прихватљиву репродукцију говора. Стандардни опсег за говорни канал за потребе телефоније је 300Hz до 3400Hz (слика 5.1). То је довољно за репродукцију говора (имајући у виду разумљивост), минимизира захтев за преносним капацитетом и омогућава упо-



Слика 5.3 Слабљење дигиталног сигнала



Слика 5.4 Ограничавање опсега спектра говорног сигнала на 300 - 3400Hz

требу телефона. Предајник на телефону претвара долазећи говорни (звучни) сигнал у електромагнетски сигнал, а нископропусни филтер слаби све компоненте сигнала изван опсега 300Hz-3400Hz (слика 5.4). Овај сигнал затим се преноси кроз телефонску мрежу ка пријемнику који репродукује звучни сигнал из долазећег електромагнетског сигнала.

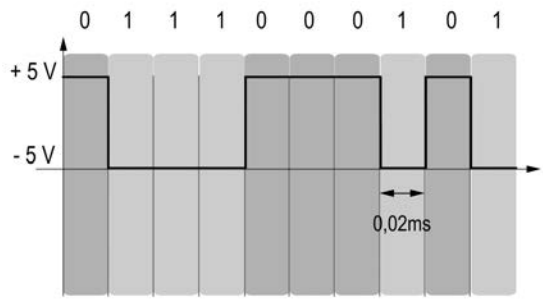
Други пример је генерални случај бинарног податка. Често коришћени сигнали за такве податке су два константна напонска нивоа, један ниво за бинарно „1" и један ниво за бинарно „0". На слици 5.5 представљен је један такав сигнал брзине 50kb/s.

Подаци и сигнали

Посматрајмо аналогне сигнале који се користе за представљање аналогних података и дигиталне сигнале који се користе за представљање дигиталних података. Генерално, аналогни подаци су континуалне функција времена и заузимају ограничени фреквенцијски опсег; такви подаци могу се представити електромагнетским сигналима, који заузимају исти фреквенцијски опсег. Дигитални подаци могу се представити преко дигиталних сигнала са различитим напонским нивоом за сваку од бинарних цифара.

Дигитални подаци могу се преносити аналогним сигналима коришћењем модема (модулатор/демодулатор). Модем [1] претвара дигиталне податке у аналогни сигнал[2] који заузима исти фреквенцијски опсег као и говорни сигнал. На тај начин се дигитални подаци могу преносити телефонским линијама. На другом крају линије модем демодулише аналогни сигнал да би поново добио оригиналне, дигиталне податке.

Аналогни подаци могу бити пренети дигиталним сигналима неком од одговарајућих техника кодирања (аналогно-дигиталном конверзијом). Уређај који извршава ову

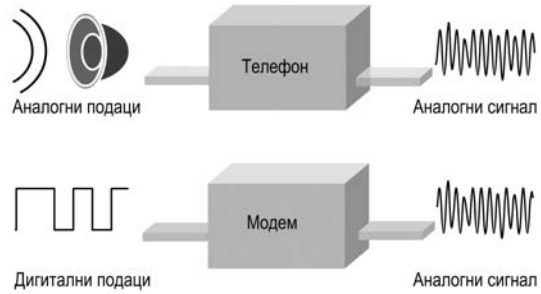


Слика 5.5 Пример дигиталног сигнала

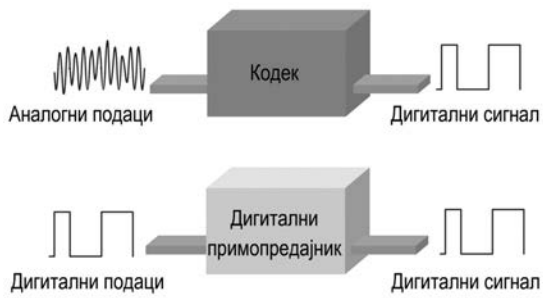
[1] Код система код којих је могућа комуникација у оба смера модулатор (за предају) и детектор (за пријем) смештени су физички у истом уређају који се зове модем (модулатор-демодулатор).

[2] Користи се простопериодични сигнал - носилац (*carrier*) у који се утискује дигитални податак који треба пренети неком од техника модулације (детаљније у 7. поглављу).

Аналогни сигнали	Преносе податке са континуално промењивим електромагнетским таласима



Дигитални сигнали	Преносе податке са секвенцама напонских импулса



Слика 5.6 Аналогни и дигитални пренос аналогних и дигиталних података

функцију назива се кодек[1]. Аналогни сигнал који директно репрезентује нпр. говор (или излаз сензора) кодер ће представити секвенцом битова. На пријемној страни та секвенца битова користи се да би се реконструисао оригинални аналогни податак (нпр. говор или излаз сензора).

5.3 Пренос

У овом поглављу биће анализирана разлика између аналогних и дигиталних сигнала. Обе врсте сигнала могу се преносити кроз одговарајући трансмисиони (преносни) медијум. Начин на који се ови сигнали третирају у зависности је од преносног система.

Аналогни пренос је начин на који се преноси аналогни сигнал, без залажења у његов садржај. Сигнал може да представља аналогне податке (нпр. говор) или дигиталне податке (нпр. подаци који пролазе кроз модем). У оба случаја аналогни сигнал ће постати слабији (ослабљен) после одређеног растојања.

Да би обезбедио већа растојања аналогни преносни систем укључује појачаваче који додају енергију сигналу. Нажалост, појачавач појачава и шум. Са појачавачима, каскадно везаним да би се обезбедило веће растојање, сигнал постаје све више и више изобличен. За аналогне сигнале као што је говор значајно изобличење може се толерисати тако да говор (податак) и даље остаје разумљив. Међутим код дигиталних података каскадно везани појачавачи уносе грешке.

[1] КОдер и ДЕКодер.

Дигитални пренос бави се садржајем сигнала. Дигитални сигнал може се преносити само на ограниченом растојању пре него што слабљење угрози могућност тачне реконструкције података. Да би се постигло веће растојање користе се „обнављивачи"[1]. Рипитер (обнављивач) прима дигитални сигнал, обнавља јединице и нуле, и шаље обновљени (нови) сигнал. Иста техника може се користити са аналогним сигналима, уколико се претпостави да сигнал носи дигиталне податке. На одговарајућим тачкама систем поставља рипитере а не појачаваче. Рипитер опоравља дигитални податак из аналогног сигнала и генерише нови, чист аналогни сигнал. Тако се спречава акумулирање шума.

Природно се јавља питање који је метод бољи за пренос? Одговор који се добија од телекомуникационе индустрије и њихових корисника је да је то дигитални, без обзира на огромна улагања у аналогна комуникациона средства. И удаљена телекомуникациона опрема, и опрема у оквиру једне зграде биће замењене дигиталним преносом и дигиталном сигнализационом техником где год је то могуће.

Најважнији разлози за то су:

- Дигитална технологија - напредак LSI [2] и VLSI [3] технологије проузроковао је смањење цене дигиталних кола;
- Целовитост података - коришћењем рипитера, а не појачавача ефекат шума и других утицаја на сигнал није кумулативан. Рипитер може да унесе грешку али се она може открити и исправити. Тако је могуће преносити податке на већа растојања а са мање квалитетним линијама, задржавајући целовитост података;
- Коришћење већих капацитета - постало је економично изградити преносне линије (линкове) врло великог пропусног опсега, укључујући сателитске канале и оптичка влакна. Да би се ефикасно искористио такав капацитет потребно је мултиплексирање, и то је много једноставније и јефтиније постићи дигиталном (временском) него аналогном (фреквенцијском) расподелом канала[4];
- Поузданост и приватност - технике шифрирања могу се применити на дигиталне податке и аналогне податке који су дигитализовани;
- Интеграција - третирањем и аналогних и дигиталних података дигитално, сви сигнали имају исту форму и могу се третирати слично. Значајне уштеде се могу постићи интеграцијом говора, видеа и дигиталних података.

5.4 Трансмисиони параметри

У било ком комуникационом систему сигнал на пријему може се разликовати од сигнала на предаји због различитих утицаја (погоршања) у преносу. Код аналогних сигнала ова погоршања могу да умање квалитет сигнала. Код дигиталних сигнала јављају се грешке; бинарна јединица се претвара у бинарну нулу и обрнуто. У овом делу анализираћемо различите параметре који утичу на погоршање сигнала и како они могу да утичу на информациони капацитет комуникационе везе. У поглављу 5.2 ана-

[1] *Repeaters*
[2] *Large Scale Integration* - висок степен интеграције
[3] *Very Large Scale Integration* - веома висок степен интеграције
[4] Детаљније о мултиплексирању биће речи у 8. поглављу.

лизирајући аналогни и дигитални сигнал посматрали смо опсег адекватан спектру сигнала. Такав опсег може да буде недовољан, или може да доведе до појаве грешке када покушамо да пренесемо сигнал. Док се сигнал преноси он је предмет великог броја утицаја од којих су најважнији:

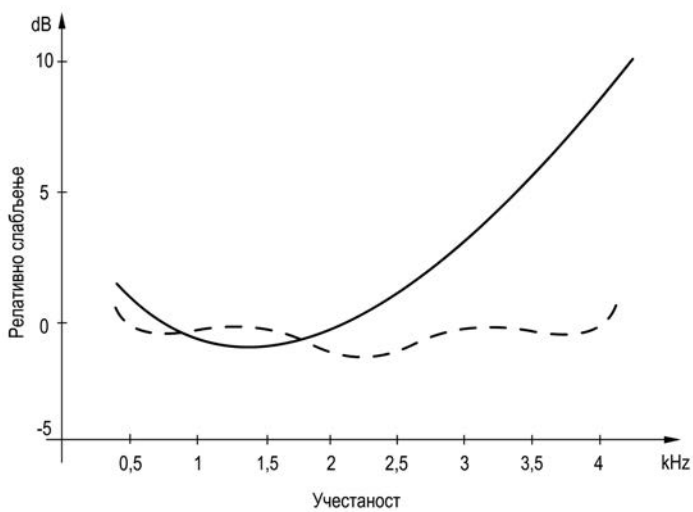
- слабљење и изобличења услед слабљења,
- изобличења услед кашњења,
- шум (сметње).

Слабљење

Снага сигнала опада са растојањем код било ког трансмисионог медијума. За жичне[1] медијуме смањење снаге, или слабљење, генерално се мења експоненцијално и зато је типично представљено константним бројем децибела по јединици раздаљине.

За бежичне[2] трансмисионе медијуме слабљење зависни од растојања и стања атмосфере. Слабљење укључује три аспекта важна за пројектанте. Прво, примљени сигнал мора да буде довољне снаге, тако да електронско коло у пријемнику може да детектује и интерпретира сигнал. Друго, сигнал се мора одржавати на нивоу довољно вишем од шума да би се могао примити без грешке. Треће, слабљење је функција која расте са учестаношћу.

Први и други проблем односе се на снагу сигнала и разрешавају се употребом појачавача и обнављивача. Трећи проблем је нарочито видљив за аналогне сигнале. Пошто се слабљење мења у функцији учестаности примљени сигнал је изобличен. Овај проблем превазилази се бројним техникама које уједначавају слабљење у одређеном опсегу учестаности. Уобичајено је да се код телефонских линија користе калемови[3] који мењају електричне карактеристике линије. Резултат је уједначавање ефекта слабљења. Други начин



Слика 5.7 Слабљење говорног канала

[1] *Hardwire*. Употребљава се и термин вођени (*guided*).
[2] *Softwire*. Употребљава се и термин невођени (*unguided*).
[3] Називају се Пупинови (Михајло) калемови, а телефонске парице пупинизоване.

је употреба појачавача који компоненте спектра на вишим учестаностима више појачавају од компонената спектра на нижим учестаностима. Пример на слици 5.7 приказује зависност слабљења од учестаности телефонске линије. На овој слици слабљење је мерено у односу на слабљење на 1000Hz. Тон од 1000Hz одређене снаге доводи се на улаз линије и мери се снага на излазу (P_{1000}). Процедура се понавља за сваку другу учестаност *f.* Релативно слабљење у децибелима је:

$$N_f = 10\log_{10}\left(\frac{P_f}{P_{1000}}\right) \tag{5.1}$$

Пуном линијом на слици 5.7 означена је крива слабљења без уједначавања (еквилизације). Види се да су у говорном опсегу компоненте спектра на вишим учестаностима значајно више ослабљене од компонената спектра на нижим учестаностима. Јасно је да ће то довести до изобличења примљеног говорног сигнала. Испрекидана линија показује ефекат уједначавања. Изобличење услед слабљења много је мањи проблем код дигиталних сигнала. Као што се види на сликама 4.9 и 4.10 снага дигиталног сигнала значајно опада са учестаношћу и њен највећи део је сконцентрисан око основног хармоника, односно битске брзине сигнала.

Изобличење услед кашњења

Изобличење услед кашњења је феномен посебно везан за жичане трансмисионе медијуме. Изобличење се јавља због тога што се брзина пропагације (простирања) сигнала мења кроз жичане медијуме у зависности од учестаности. За сигнале ограниченог опсега брзина је највећа близу централне учестаности и опада ка границама опсега. Изобличење услед кашњења сигнала говора или музике нема никаквог утицаја на репродукцију што није случај са телевизијским сигналом или сигналима који преносе дигиталне податке.

Шум (сметње)

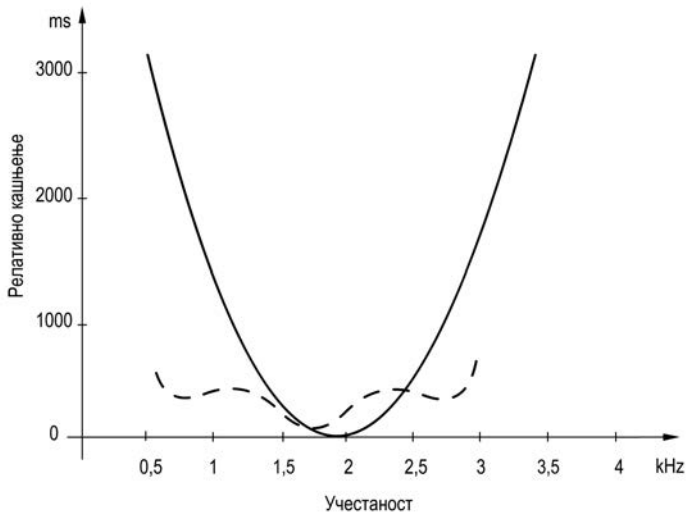
За сваки пренос примљени сигнал ће се састојати од:

- послатог сигнала модификованог различитим изобличењима које уноси преносни систем,
- додатног нежељеног сигнала који се уметнуо негде између предаје и пријема.

Тај нежељени уметнути сигнал назива се шум или сметња. Шум је тај који је највећи ограничавајући фактор у карактеристикама комуникационог система. Шум се може поделити у четири категорије:

- термички шум,
- интермодулациони шум,
- шум услед преслушавања,
- импулсни шум.

Термички шум представља појаву која је својствена свим системима чија је апсолутна температура *T* већа од 0^0 K. У сваком проводнику због термичке интеракције између слободних електрона и вибрирајућих молекула проводника, у условима термичке равнотеже, долази до сталног и нерегуларног кретања електрона. Термички шум је прису-



Слика 5.8 Изобличење услед кашњења за говорни канал

тан у свим уређајима и трансмисионим медијумима. Не може се елиминисати и због тога је ограничавајући фактор за перформансе комуникационих система.

За термички шум се каже да је равномерно расподељен у спектру и често се назива „равним" или „белим шумом" јер и белу светлост карактерише униформна расподела у видљивом делу спектра. Снага термичког шума (изражена у ватима) који је присутан у опсегу учестаности ширине *B* херца може се израчунати на следећи начин:

$$N = kTB \tag{5.2}$$

где је:

k - Болцманова константа 1,3803 *10^{-23} J/ ^{0}K,

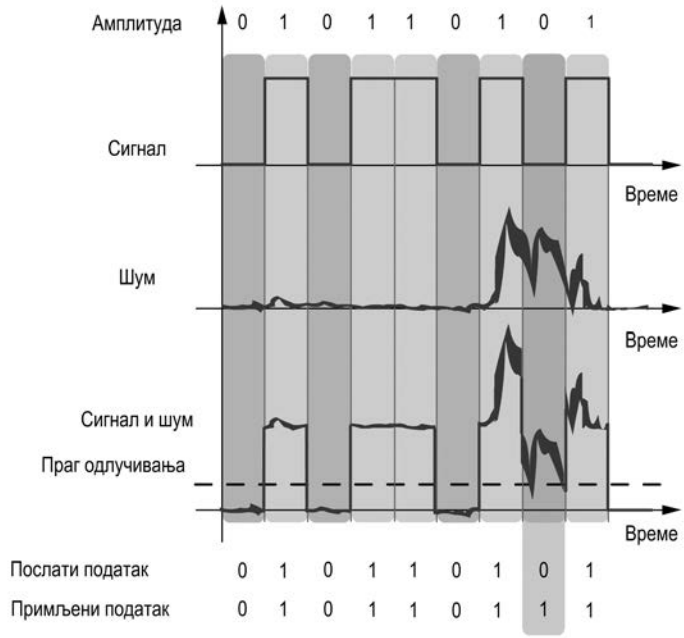
T - температура у Келвиновим степенима.

Када сигнали различите учестаности деле исти трансмисиони медијум резултат може да буде интермодулациони шум. Интермодулациони шум се ствара кад постоји нелинеарност у предајнику, пријемнику или преносном систему. Ефекат интермодулационог шума је да производи сигнале таквих учестаности које су сума, разлика или мултипл оригиналних учестаности. На пример, мешањем сигнала учестаности f_1 и f_2, могу да се добију сигнали на учестаностима $f_1 + f_2$.

Преслушавање су имали прилике да чују сви који користе телефонске везе - били су у стању да чују туђе разговоре. То је нежељена електромагнетска спрега комуникационих путева. Сви ови типови шума су предвидиви и релативно константне јачине.

Импулсни шум је дисконтинуалан извор грешака у дигиталним комуникацијама. Слика 5.9 пример је ефекта на дигитални сигнал. Шум се састоји од релативно скромног нивоа термичког шума и повремених шпицева импулсног шума.

Однос сигнала и шума S/N (сигнал/шум) је најважнији параметар који одређује перформансе трансмисионог система. Представља однос снаге сигнала према снази



Слика 5.9 Ефекат шума на дигитални сигнал

која се садржи у присутном шуму. Релација се обично мери на пријемној страни пошто је то тачка у којој се обрађује (процесира) сигнал и елиминише нежељени шум. Уобичајено је да се однос дефинише у децибелима:

$$\left(\frac{S}{N}\right)_{dB} = 10\log\cdot\frac{\text{снага сигнала}}{\text{снага шума}} \tag{5.3}$$

На слици 5.9 приказан је утицај шума на дигитални сигнал. При детекцији сигнала на пријему и поређења са прагом одлучивања може се уочити да се као последица шума појавила грешка у примљеном сигналу.

5.5 Капацитет канала

Видели смо да постоји више ефеката који изобличавају или оштећују сигнал. За дигиталне сигнале поставља се питање до колико ово погоршање ограничава брзину података која се може постићи. Максимална брзина којом се подаци могу преносити преко неког комуникационог пута, или канала, под датим условима назива се капацитет канала.

Постоје четири појма која су везана један са другим. То су:

- Брзина података - односи се на брзину у битима у секунди (b/s, bps[1]) којом се подаци могу размењивати;
- Опсег - односи се на опсег спектра предајног сигнала који је ограничен предајником и природом трансмисионог медијума и изражава се у циклусима у секунди или херцима (Hz);

[1] *Bit per second*

- Сметња - односи се на средњи ниво снаге сметње на комуникационом путу;
- Вероватноћа грешке - односи се на учестаност појављивања грешака. Под грешком се подразумева када се прогласи „1" а послато је „0" и обрнуто.

Проблем је следећи: комуникциона опрема генерално је скупа и што је њен пропусни опсег већи виша је цена. Поред тога сви доступни преносни канали су ограниченог пропусног опсега. Ограничења су последица физичких карактеристика трансмисионих медијума и намерног ограничавања ширине опсега предајника да би се спречила интерференција са другим изворима. Задатак је да се искористи што више за расположиви опсег. За дигиталне податке ово значи да бисмо волели да постигнемо што је могуће већу брзину података за задату вероватноћу грешке и понуђену ширину опсега.

Никвистов опсег

Започећемо анализу претпоставком да располажемо каналом без шума. У оваквом систему ограничење које се поставља је опсег спектра сигнала. Никвист је формулисао да је за расположиви опсег B највећа брзина која се може пренети $2B$. Ова ограничења последица су међусимболске интерференције као што је изобличење услед кашњења.

У претходном параграфу користили смо термин брзина сигнала. Уколико је сигнал који треба пренети бинаран (два напонска нивоа), онда брзина података која се може постићи са B (Hz) износи $2B$ (b/s). Као пример посматрајмо говорни канал који се користи за пренос дигиталних података. Претпоставимо да је његова ширина 3100Hz. Онда је капацитет C канала $2B = 6200$b/s. Као што ћемо видети у 7. поглављу могуће је користити сигнале са више од два напонска (струјна) нивоа; то значи да сваки сигнализациони елемент може да представља више од једног бита. Када нема фазних изобличења сигнал се шири у времену. Са вишенивоском сигнализацијом Никвистова формула постаје:

$$C = 2B\log_2 M = 2B\ln M \tag{5.4}$$

где је M број дискретних сигнала или напонских нивоа. Тако би за $M = 4$, која се користи код неких модема, капацитет канала C био 12400b/s за ширину од 3100Hz.

За задату ширину (пропусни опсег) канала брзина се може повећати са увећањем броја различитих сигнализационих елемената. Ово усложњава рад пријемника. Уместо да прави разлику између два могућа сигнализациона елемента за време трајања једног сигнализационог елемента треба да направи разлику M могућих елемената. Шум и друга погоршања на преносној линији ограничиће стварне вредности броја M напонских нивоа.

Шенонова једначина за капацитет канала

Никвистова формула указује да се, уколико је све друго једнако, удвостручавањем ширине опсега удвостручава брзина података. Посматрајмо везу између брзине преноса података, шума и вероватноће грешке. Присуство импулсног шума може да оштети један или два бита. Уколико се брзина података повећава трајање битског интервала се смањује али се повећава број битова на који сметња (шум) има утицај. То значи да је за задати ниво сметње већа вероватноћа грешке што је већа брзина података. Слика 5.9 графички приказује ову релацију. Уколико се брзина података повећава, више се

битова нађе у интервалу када је шум великог интензитета (у шпицевима). Сви претходно набројани параметри могу се повезати у формулу коју је развио математичар Клод Шенон. Као што смо видели, што је брзина података већа то нежељена сметња може да изазове већи број грешака. За задати ниво сметње већа снага сигнала повећава способност [1] да се на пријему добију подаци без грешке. Кључни параметар у овој анализи је однос сигнала и сметње (*S*/*N*). Он представља однос између средње снаге сигнала и средње снаге сметње (шума) присутан у тој специфичној тачки у преносу (једначина 5.3).

Однос сигнала и сметње важан је код преноса дигиталних података, пошто он поставља горњу границу брзине података која се може постићи у одређеном каналу. Шенон је показао да се максимални капацитет канала, изражен у битима у секунди, може исказати једначином:

$$C = B\log_2\left(1+\frac{S}{N}\right) = B\ln\left(1+\frac{S}{N}\right) \tag{5.5}$$

У овој релацији је:

C - капацитет канала изражен у битима у секунди (b/s), а

B - пропусни опсег канала изражен у херцима (Hz).

Шенонова једначина представља теоретску границу која се може постићи. На пример за канал од 3000Hz и односа сигнал шум од 30dB (типичан параметар за телефонски канал) не може да се пренесе више од 30000b/s без обзира која се техника модулације користи.

У пракси се може постићи мањи капацитет. Један од разлога за то је што једначина 5.5 претпоставља постојање само белог (термичког) шума. Нису укључени ни импулсни шум, ни изобличење услед слабљења или кашњења.

Капацитет дефинисан једначином 5.5 назива се капацитет без грешке[2]. Додатна анализа указује на следеће:

- За задати ниво шума чини се да ће се повећавањем снаге сигнала повећати и брзина података. Међутим, повећавањем снаге сигнала ефекат нелинеарности система се увећава, што доводи до повећања интермодулационог шума;
- Пошто је реч о термичком (белом шуму), што је пропусни опсег већи то се више шума додаје систему. Значи са порастом *B* однос *S*/*N* се смањује.

[1] Имуност на шум (сметње).

[2] Тачније грешка се може држати под контролом.

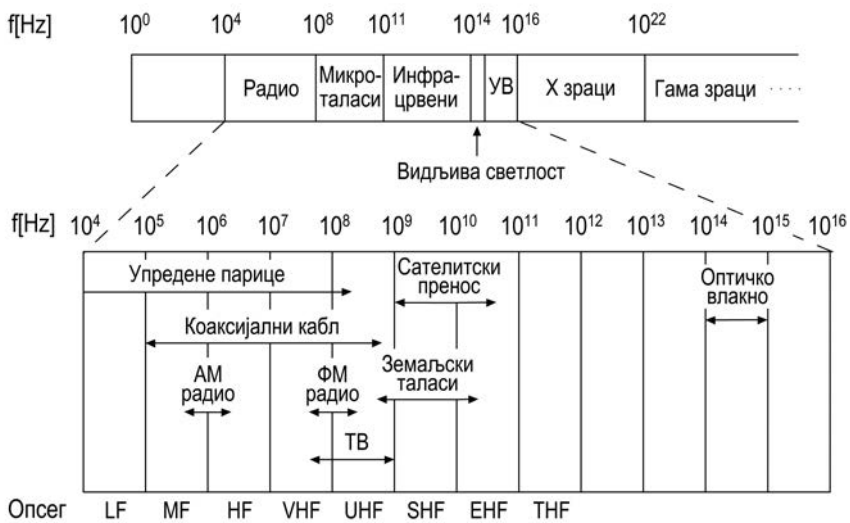
6. Трансмисиони медијуми

Трансмисиони медијум је физички пут између предајника и пријемника у систему за пренос података и може се класификовати као жични[1] и бежични[2] (слика 6.1). Пример жичних медијума су упредене парице, коаксијални каблови и оптичка влакна. Пример бежичних медијума су ваздух, вакуум или вода.

Карактеристике и квалитет преноса података одређени су и природом сигнала и природом медијума. У случају жичних медијума, медијум сам по себи важнији је у одређивању ограничења у преносу.

С друге стране за бежичне медијуме спектар сигнала који шаље антена много је важнији од медијума у одређивању преносних карактеристика. Код бежичних медијума битна је усмереност антена. Сигнали на нижим учестаностима су, генерално, вишедирекциони[3]; то значи да се сигнал који шаље (емитује) антена простире у свим правцима. На вишим учестаностима могуће је усмерити сигнал у одређеном правцу.

У анализи преносних система кључне особености су брзина преноса и домет (удаљеност). Што су постигнута брзина и домет већи то је преносни систем бољи. При пројектовању битни чиниоци који су везани за трансмисиони медијум и сигнал, а одређују брзину података и домет, су: опсег спектра сигнала, слабљење, интерференција и број пријемника.



Слика 6.1 Електромагнетски спектар и његова примена у комуникационим системима

[1] Користе се и термин вођени (*guided*) медијум и жични (*hardwire*) медијум.
[2] Користе се и термини невођени (*unguided*) медијум и бежични (*softwire*) медијум.
[3] Омнидирекциони (*omnidirectional*)

Опсег

Уколико су сви остали фактори константни што је већи опсег канала то се већа брзина тим каналом може постићи.

Слабљење

Један од параметара који умањује квалитет сигнала у преносу тј. ограничава његов домет је слабљење. Ако се посматрају жични медијуми онда је слабљење сигнала који се преносе упреденим парицама веће од слабљења при преносу коаксијалним кабловима а најмање је код преноса оптичким влакнима.

Интерференција

Међусобни утицаји сигнала у опсезима спектра који се међусобно преклапају могу да изобличе и умање снагу сигнала. Интерференција је нарочито изражена код бежичних медијума, али је такође и проблем код жичних медијума. На пример више упредених парица обично је смештено у једном каблу. Код жичних медијума овај проблем може се умањити оклопљавањем.

Број пријемника

Жични медијуми користе се или као једна веза (тачка-тачка) или као више веза (дељени медијум). Када исти медијум користи више прикључених уређаја онда свака прикључна тачка уноси неко слабљење и изобличење линије чиме се ограничавају домет и брзина преноса.

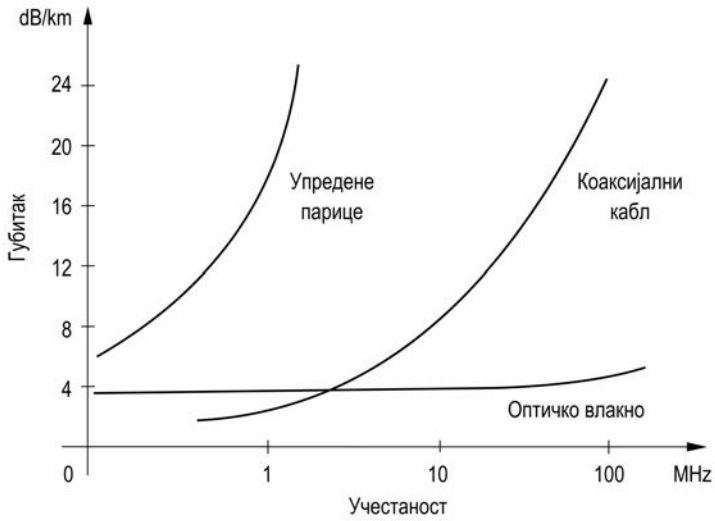
6.1 Жични медијуми

За жичне трансмисионе медијуме капацитет преноса, без обзира да ли се посматра кроз брзину преноса или ширину пропусног опсега, зависи од раздаљине и од тога да ли се медијум користи као једна веза (тачка-тачка) или као дељени (више тачака). Табела 6.1. садржи типичне карактеристике жичних медијума, укључујући граничну брзину података коју медијум може да подржи, пропусни опсег медијума и потребну раздаљину за рипитере.

Трансмисиони медијум	Типично слабљење	Типично кашњење	Пропусни опсег	Растојање рипитера
Упредене парице (са оптерећењем [1])	0,2dB/km -1kHz	50 μs/km	0 - 3,5kHz	2km
Упредене парице (вишепарични кабл)	3dB/km -1kHz	5 μs/km	0 - 1MHz	2km
Коаксијални кабл	7dB/km -1MHz	4 μs/km	0 - 500MHz	1 - 9km
Оптичко влакно	0,2 - 0,5dB/km	5 μs/km	180 - 370THz [2]	40km

Табела 6.1 Карактеристике жичаних медијума директне (тачка-тачка) везе

[1] Енг. *with loading*. Односи се на Пупинизоване парице.
[2] 1THz=10^{12}Hz



Слика 6.2 Слабљење жичних трансмисионих медијума

6.2 Упредене парице

Упредене парице су највише коришћени и најјефтинији трансмисиони медијум.

Физички опис

Упредене парице састоје се од две изоловане бакарне жице упредене равномерним кораком упредања. Жице се понашају као једна комуникациона веза. Упредањем се минимизира[1] електромагнетска интерференција између парова жица.

Када се жице упреду сигнали који су резултат преслушавања из упредених делова међусобно се потиру. Уобичајено је да се већи број ових парова смешта у кабл са заштитним омотачем.

Коришћење

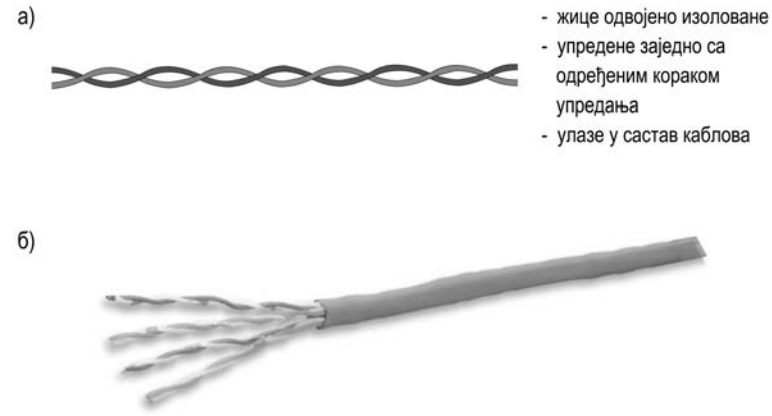
Упредене парице су трансмисиони медијум који се највише користи и за аналогни и за дигитални пренос. Користе се у телефонској мрежи за повезивање корисника и комутационих центара (тзв. претплатничка петља).

Такође се користе за скоро све комуникационе везе унутар објеката. Нарочито су нашле широку примену у локалним рачунарским мрежама за брзине од 100Mb/s и 1Gb/s.

Преносна (трансмисиона карактеристика)

Упредене парице се користе и за аналогни и за дигитални пренос. Код аналогних система преноса појачавачи су потребни на сваких 5km до 6km. Код дигиталних система преноса рипитере треба поставити на размаку од 2km до 3km. Слика 6.2 показује колико је слабљење код упредених парица зависно од фреквенције. У поређењу с другим жичним трансмисионим медијумима (коаксијални кабл, оптичко влакно) упредене парице су мањег домета, опсега и капацитета.

[1] Две паралелне жице понашају се као антена.



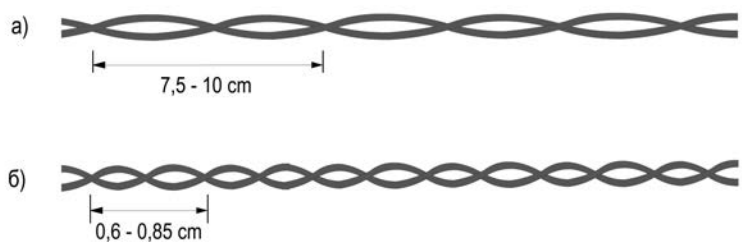
Слика 6.3 Упредене парице а) један пар б) кабл са 4 упредене парице

Оклопљене и неоклопљене упредене парице

Упредене парице се израђују у две варијанте: неоклопљене и оклопљене. Неоклопљене, без заштитног омотача, UTP[1] су стандардне телефонске жице (слика 6.3). Пословни објекти најчешће су ожичени неоклопљеним телефонским парицама што је више него довољно квалитетно за телефонске везе. Ово је најјефтинији трансмисиони медијум и уобичајено се користи и за локалне рачунарске мреже. Неоклопљене парице су подложне спољашњим електромагнетским сметњама. Начин да се побољшају карактеристике медијума је да се заштите металним омотачем или мрежом и на тај начин спрече нежељени утицаји (интреференција). Оклопљене упредене парице STP[2] бољих су особина (нарочито на већим брзинама), али су скупље.

Категорије каблова

Ожичавање са упреденим парицама постоји у неколико варијанти. Организација произвођача електронике EIA[3] 1995. године донела је стандард за ожичавање објеката[4] који специфицира коришћење упредених парица[5] (оклопљених - 150Ω и неокло-



Слика 6.4 Различите категорије упредених парица а) категорије 3 б) категорије 5

[1] *Unshielded Twisted Pair*
[2] *Shielded Twisted Pair*
[3] *Electronic Industries Association*
[4] *Commercial Building Telecommunication Standard*
[5] За каблове (па и упредене парице) дефинисана је карактеристична импеданса која се изражава у омима (Ω).

	Слабљење [dB / 100m]			Преслушавање на ближем крају [dB]		
f [MHz]	*Cat* 3 UTP	*Cat* 5 UTP	150Ω STP	*Cat* 3 UTP	*Cat* 5 UTP	150Ω STP
1	2,6	2,0	1,1	41	62	58
4	5,6	4,1	2,2	32	53	58
16	13,1	8,2	4,4	23	44	50,4
25	-	10,4	6,2	-	41	47,5
100	-	22,0	12,3	-	32	38,5
300	-	-	21,4	-	-	31,3

Табела 6.2 Особине различитих врста упредених парица

пљених - 100Ω) за инсталације унутар објеката и који носи ознаку EIA-588A. Осврнућемо се на оне које су (или су биле) значајне за рачунарске комуникације.

Категорија[1] 3 састоји се од две изоловане жице заједно упредене (слика 6.3а). Корак упредања је 7,5cm до 10cm. Четири упредене жице (парице) груписане су заједно и смештене у пластични заштитни омотач. Пропусни опсег ових каблова је до 16MHz.

Категорија[2] 5 разликује се од категорије 3 само по кораку упредања (слика 6.4б). Корак упредања је 0,6cm до 0,85cm. Пропусни опсег ових каблова је до 100MHz.

У табели 6.2 сумиране су особине различитих врста упредених парица. Први параметар за међусобно упоређивање је слабљење. Снага сигнала опада са растојањем код сваког преносног медијума. За жичне медијуме то опадање је експоненцијално и типично је изражено константним бројем децибела по јединици растојања.

Други параметар је преслушавање на ближем крају. У табели 6.3 побројани су нови системи каблирања и направљено је поређење са постојећим стандардом.

6.3 Коаксијални каблови

Физички опис

Коаксијални кабл, као и упредене парице, састоји се од два проводника, који су различито конструисани да би обезбедили рад у широком фреквенцијском опсегу.

	Cat 3 Класа C	Cat 3 Класа D	Cat 5E	Cat 6 Класа E	Cat 7 Класа F
f [MHz]	16	100	100	200	600
Тип кабла	UTP	UTP/FTP[3]	UTP/FTP	UTP/FTP	SSTP[4]
Цена везе	0,7	1	1,2	1,5	2,2

Табела 6.3 Нови системи каблирања

[1] UTP Cat *3*
[2] UTP Cat *5,* UTP Cat *5*E (*Enhanced)* - унапређена Cat *5*
[3] Упредене парице обмотане металном фолијом (*Foil Twisted Pair*)
[4] Сваки пар (од 4) је посебно заштићен и металном фолијом и металном мрежицом - SSTP (*Shielded Screen Twisted Pair*)

Слика 6.5 Изглед и попречни пресек коаксијалног кабла

Један од проводника је пуна проводна жица која је постављена у цев од изолационог материјала, око кога је обмотана цилиндрична проводна мрежа. Све заједно је смештено у заштитни, пластични омотач (слика 6.5).

Коришћење

Коаксијални кабл је трансмисиони медијум који се користи на најразноврсније начине. Најважнија примена је за:

- удаљени телефонски и телевизијски пренос,
- телевизијску мрежу,
- локалне рачунарске мреже.

Две врсте коаксијалних каблова налазиле су се у широј употреби. Једна од њих је 50Ω кабл који се користио у локалним рачунарским мрежама [1]. Други 75Ω уобичајено се користи за аналогни пренос и кабловску телевизију али постаје све значајнији и за приступ Интернету.

Коаксијални кабл је традиционално био важан део међуградске телефонске мреже. Данас се све више замењује оптичким кабловима, земаљским микроталасима и сателитским везама. Користећи фреквенцијску поделу опсега коаксијални кабл [2] може да обезбеди 10000 истовремених говорних канала.

Преносна карактеристика

Коаксијални каблови се користе и за аналогне и за дигиталне сигнале. Као што се може видети на слици 6.1 коаксијални кабл има бољу фреквенцијску карактеристику од упредених парица, тако да се може ефикасније користити на вишим учестаностима и при већим брзинама.

[1] На самом почетку у свим локалним рачунарским мрежама рачунари су били повезани дебелим (*thick*) а касније танким (*thin*) коаксијалним кабловима. Данас су ове инсталације замењене упреденим парицама и оптичким влакнима.

[2] Фреквенцијски мултиплекс FDM (*Frequency Division Multiplex*), детаљније у 8. поглављу.

Због заштитног омотача коаксијални кабл је мање подложан сметњама и преслушавању. Ограничавајући фактор је слабљење, термички шум и интермодулациони шум.

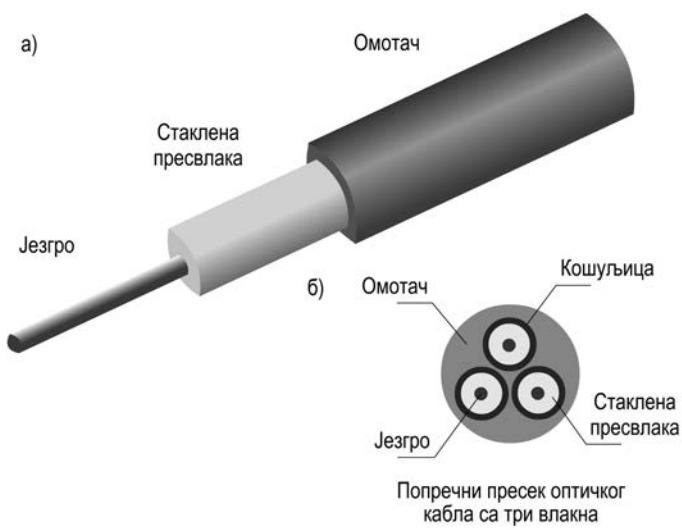
6.4 Оптички каблови

Пројектанти у рачунарској индустрији веома су поносни на брзину којом се развија рачунарска индустрија. Персонални рачунар (1981. год., IBM) радио је са такт сигналом од 4,77MHz. Двадесет година касније персонални рачунар ради са такт сигналом од 2GHz. Повећање брзине рада је двадесет пута по декади. У истом периоду пренос дигиталних података између географски удаљених локација је са 56kb/s (ARPANET[1]) дошао на 1Gb/s. Повећање је 125 пута по декади, а вероватноћа грешке је са 10^{-5} дошла скоро на нулу.

Са данашњом технологијом израде оптичких влакана пропусни опсег дозвољава брзину од 50000Gb/s (50Tb/s). Ограничења која тренутно постоје последица су немогућности да се на већим брзинама изврши конверзија електричног у оптички сигнал. С друге стране централна процесорска јединица достигла је своје границе. У трци између рачунарства и комуникација комуникације су за сада победиле. Последице суштински неограниченог опсега (али не и ниске цене) још није потпуно прихватила генерација пројектаната која је научила да размишља са ограничењима која су поставили Никвист и Шенон за жичне медијуме.

Физички опис

Оптичко влакно је танак (2 до 125μm), флексибилни медијум, кроз који може да се простире светлосни зрак. Праве се од стакла или пластике. Најмањи губици су код оптичких влакана која су направљена од силицијума[2]. Нижи по цени али и даље прихватљи-



Слика 6.6 Изглед: а) оптичког влакна б) оптичког кабла са три влакна

[1] Прва рачунарска мрежа коју је организација ARPA (*Advance Research Project Agency*) развила.
[2] Реч је о SiO_2 веома велике чистоће. Тешко је обезбедити производњу.

вих перформанси су стаклена оптичка влакна. Пластична оптичка влакна су најнижа по цени и могу се користити за краћа растојања и примене у којима су губици средњег нивоа прихватљиви.

Оптичка влакна имају цилиндрични облик и састоје се од три концентрична дела: језгра, пресвлаке и омотача (слика 6.6а). Језгро је од стакла или пластике пречника 8 до 100μm. Оптичко влакно је пресвучено материјалом који има различита оптичка својства од језгра (нижи индекс преламања). Спој између језгра и омотача за светлосни зрак понаша се као гранична, рефлектујућа површина. Трећи слој може да буде омотач једном или више оптичких влакана. Омотач је обично направљен од пластичног материјала и заштита је од влаге, механичких оштећења и других нежељених утицаја у окружењу.

Коришћење

Једна од најважнијих технолошких прекретница у преносу података је развој оптичких комуникационих система. Оптичка влакна су применљива у међуградским телефонским везама, локалним рачунарским мрежама и војним комуникацијама. Следеће карактеристике разликују оптичке каблове од упредених парица и коаксијалних каблова:

- већи пропусни опсег - могућа ширина опсега, а самим тим и брзина је значајно већа (10 и 100Gb/s);
- мање димензије и тежина - оптички каблови су значајно тањи и лакши од каблова са упреденим парицама и коаксијалних каблова[1]. Код инсталација нових уређаја за преусмеравање података (рутера) користе се оптичка влакна због значајно лакше инсталације, а самим тим и цене;
- мање слабљење - слабљење је значајно мање код оптичких влакана него код коаксијалних каблова и упредених парица и константно је у широком опсегу (слика 6.2);
- електромагнетска изолација - на системе са оптичким влакнима немају утицаја спољашња електромагнетска поља. То значи да систем није подложан интерференцији, импулсном шуму и преслушавању;
- већи размак између рипитера - као последица малог слабљења рипитери су потребни на сваких 40 до 50km. У поређењу са размаком рипитера од највише 5km код бакарних преносних медијума уштеде су значајне.

Оптичка влакна су нашла примену у следећим комуникационим системима:

- међуградским преносним системима,
- у градским преносним системима,
- претплатничким петљама,
- локалним рачунарским мрежама.

Постало је уобичајено да се међуградски преносни системи у телефонској мрежи реализују оптичким влакнима. Раздаљине у међуградским везама су и до 1500km и нуде велики капацитет (обично 20000 до 60000 говорних канала). Ови системи су по цени близу микроталасним системима. У градским подручјима преносни системи су просечне дужине од 12km и могу да садрже до 100000 говорних канала. Уобича-

[1] 1000 UTP каблова 1km дужине, тешко је 8000kg. Може се заменити (по капацитету) са 2 оптичка влакна. Дужине 1km она су тешка 100kg.

јено се постављају без рипитера. Оптичка влакна у претплатничким петљама повезују локалне телефонске централе са крајњим корисницима (претплатницима). Овакве везе могу да обезбеде услуге не само преноса говора већ и података, слике и видео сигнала. За сада су намењене пословним претплатницима али се сматра да ће се у блиској будућности користити и у домаћинствима. Важна примена оптичких влакана су локалне рачунарске мреже. Развијени су стандарди и појавила се опрема која омогућава брзине од 100Mb/s до 10Gb/s.

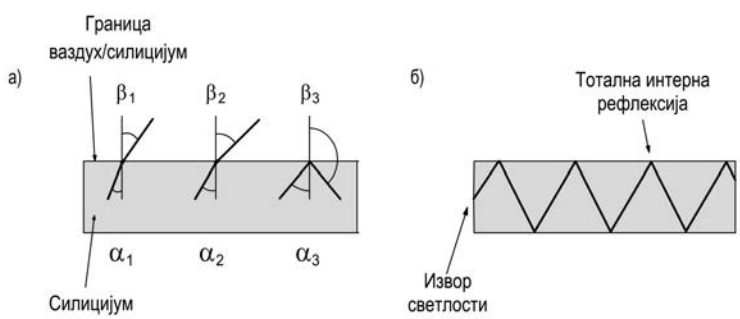
Преносна карактеристика

Оптички систем преноса има три компоненте: извор светлости, преносни медијум и детектор. Уобичајено (по конвенцији) импулс светлости представља бит „1", а одсуство светлости бит „0". Детектор генерише електрични импулс када светлост падне на њега. Довођењем извора светлости на један крај оптичког влакна и детектора на други крај добија се једносмерни (унидирекциони) преносни систем. Он прихвата електрични сигнал, претвара га у светлост и емитује као светлосни импулс. На пријемној страни светлосни импулс се поново претвара у електрични сигнал.

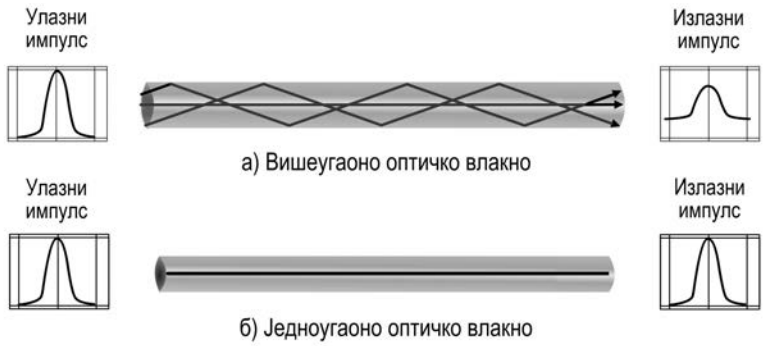
Преносни систем би расипао светлост и био би неупотребљив у пракси да није примењен принцип из физике. Када светлосни зрак прелази из једног медијума у други долази до промене његовог правца (рефракције) на самој граници између два медијума (нпр. стакленог влакна и ваздуха). На слици 6.7а види се да се светлосни зрак који пада на површину под углом α_1 појављује под углом β_1.

Величина рефракције зависи од карактеристика ова два медијума. За улазни угао изнад одређене критичне вредности светлост се прелама (рефрактује) у стаклено влакно. Тако светлосни зрак који пада под углом изнад одређене критичне вредности остаје у оптичком влакну (слика 6.7б). Може (теоретски гледано) да се простире на велике раздаљине практично без губитака. На слици је приказан један светлосни зрак, али се било који светлосни зрак који се појави под углом већим од критичног исто понаша - остаје „заробљен" у оптичком влакну.

На слици 6.7б приказан је један зрак, али било који зрак који пада под углом већим од граничног одбијаће се о граничну површину влакна (слика 6.8). Сваки од ових



Слика 6.7 а)Три примера светлосног зрака унутар оптичког влакна који падају на границу влакно/ваздух под различитим угловима,
б) Зрак који се простире потпуном рефракцијом



Слика 6.8 Начин преноса светлосног зрака кроз оптичко влакно: вишеугаоно и једноугаоно

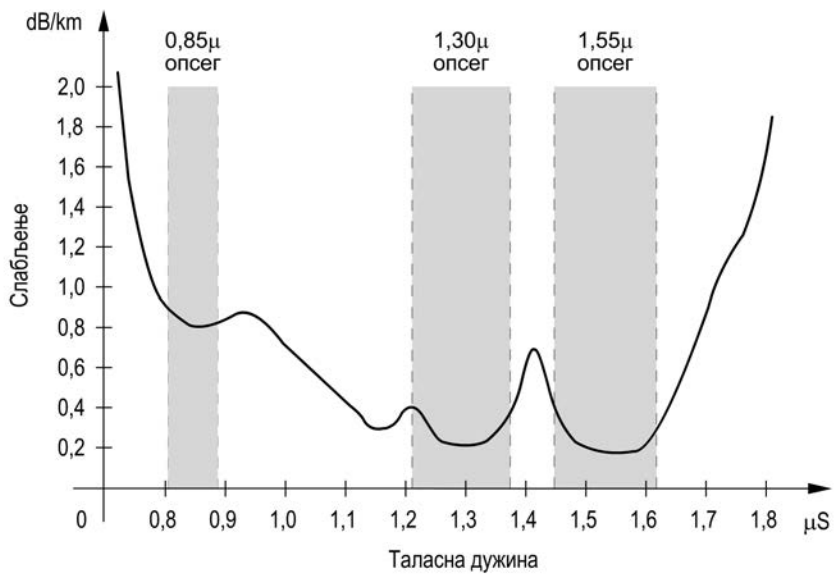
зрака има свој угао под којим се емитује и свој пут, односно начин [1] простирања, па се ова врста оптичких влакана назива вишеугаона [2] оптичка влакна (слика 6.8а).

Уколико се пречник влакна смањи на неколико таласних дужина светлости влакно „води" светлосни зрак. Могућ је један једини угао а самим тим и пут светлосног зрака па се ова врста влакана назива једноугаона [3] оптичка влакна (слика 6.8б).

У системима са оптичким влакнима користе се различити типови светлосног извора:

LED [4] - полупроводничка диода која емитује светлост када кроз њу пролази струја,

ILD [5] - полупроводничка диода која ради на принципу ласера.



Слика 6.9 Слабљење светлости инфрацрвеног дела спектра при проласку кроз оптичко влакно

[1] Користи се термин мод (енг. *mode* - начин).
[2] *Multimode*
[3] *Singlemode*
[4] *Light Emitting Diode*
[5] *Injection Laser Diode*

Слабљење светлости при простирању кроз оптичко влакно зависи од таласне дужине светлости и од физичких карактеристика оптичког влакна. За различите врсте стакла од којих се праве оптичка влакна слабљење (изражено у dB/km) приказано је на слици 6.9. Оптички комуникациони системи у раду користе три опсега таласних дужина (тзв. оптичка „прозора"). Они су центрирани [1] око таласних дужина 0,85; 1,30 или 1,55μm. Последње две имају добре карактеристике слабљења (мање од 5% по километру дужине). Сва три опсега таласних дужина су ширине од 25000 до 30000GHz.

6.5 Бежични пренос

Електромагнетски таласи могу се простирати кроз ваздух, чак и кроз вакуум. Број осцилација у секунди је учестаност таласа (*f*), а растојање између две узастопне максималне (или минималне) вредности назива се таласна дужина λ. У вакууму електромагнетски таласи простиру се брзином која не зависи од учестаности. Та брзина обично се назива брзина светлости (*c*) и приближно је $3*10^8$m/s. Код простирања електромагнетских таласа кроз бакарни кабл или оптичко влакно брзина се смањује и зависи од учестаности. Основна релација између *f,* λ, *c* је:

$$\lambda f = c \qquad (6.1)$$

Пошто је *c* константно уколико се зна *f* може се израчунати [2] λ. Електромагнетски спектар је приказан на слици 6.1. Опсези који су обележени на дну слике званичне су ознаке које користи ITU-T. Најнижи опсег од 30 до 300kHz означен је као низак фреквенцијски опсег, следе средњи, висок, веома висок итд. Ознаке су одговарајуће енглеске скраћенице [3]: LF, MF, VHF, UHF, SHF, EHF, THF.

За бежични пренос који ће бити анализиран у овој глави од интереса су три фреквенцијска опсега:микроталасни, радио и инфрацрвени. Фреквенције у опсегу од око 1GHz до 40GHz означавају се као микроталасне учестаности. На овим учестаностима могуће је емитовати веома усмерене зраке тако да су микроталаси подесни за тачка-тачка везе. Микроталаси се користе и за сателитске комуникације. Учестаности у опсегу 30MHz до 1GHz подесне су за омнидирекционе примене. Тај опсег се назива радио-опсег.

Трећи важан опсег учестаности је инфрацрвени део спектра. Он обухвата опсег учестаности од $3*10^{11}$ до $3*10^{14}$Hz (приближно). Инфрацрвени део спектра користи се за везе тачка-тачка и тачка-више тачака у оквиру ограниченог простора (нпр. једна просторија). Да би се обезбедио пренос бежичним медијумима на предајној и пријемној страни постављају се одговарајуће антене.

Антене

Антена се дефинише као електрични проводник или систем електричних проводника који се користи било за емитовање било за сакупљање електромагнетске енерги-

[1] Видљива светлост таласне дужине 0,4 до 0,7μm (микрона)
[2] Може се користити следеће правило: када је *f* у MHz а λ у метрима онда је λ *f* ~300.
[3] *Low, Medium, High Frequency; Very High, Ultra High, Supe Highr, Extremely High, Tremendeus High Frequency*

Слика 6.10 Параболична антена

је. За пренос сигнала електрична енергија из предајника посредством антене претвара се у електромагнетску енергију и емитује у средину која га окружује (атмосфера, вода, простор). За пријем сигнала електромагнетска енергија која доспе до антене претвара се у електричну енергију коју користи пријемник.

У двостраној комуникацији иста антена може се користити и за предају и за пријем. Ово је могуће зато што свака антена претвара енергију из средине која је окружује у улазни сигнал пријемног уређаја са истом ефикасношћу као што претвара улазни сигнал предајног уређаја у средину која је окружује, уз претпоставку да се користи иста учестаност у оба правца. Формулисаћемо на други начин: карактеристике антене су суштински исте без обзира да ли она шаље или прима електромагнетску енергију.

Антена ће емитовати енергију у свим правцима али обично не и једнако добро у свим правцима. Добар начин да се окарактеришу особине антене је дијаграм зрачења. Најједноставнији дијаграм зрачења добија се од идеалне антене која се назива изотропска антена. Изотропска антена је тачка у простору чија је снага емитовања подједнака у свим правцима. Дијаграм зрачења изотропске антене је сфера са антеном у њеном центру.

Параболична рефлектујућа антена

Важан тип антене је параболична рефлектујућа антена која се користи у земаљским микроталасним и сателитским везама. Параболична антена[1] има следећа својства: уколико се извор електромагнетске енергије налази у жижи параболичне антене а унутрашњост антене је направљена од рефлектујућег материјала, онда ће се електромагнетски таласи одбити о рефлектујућу површину у правцу паралелном оси антене (слика 6.10) .

По теорији на овај начин се формира паралелан млаз без икаквог расипања. У пракси постоји расипање (дисперзија) пошто извор зрачења заузима већи простор од једне тачке. Што је антена већа то је веће њено усмеравање. На пријему, уколико су долазећи таласи паралелни са осом рефлектујућег параболоида, резултујући сигнал ће бити усмерен (фокусиран) у жижу.

[1] Попречни пресек ове антене паралелан са осом је парабола, а попречни пресек нормалан на осу је круг.

Појачање антене

Појачање антене је мера усмерености антене. Дефинише се као однос снаге сигнала у одређеном правцу у поређењу са снагом сигнала у било ком правцу коју би произвела омнидирекциона (изотропска) антена. На пример, уколико нека антена има појачање 3dB та антена емитује два пута већу снагу у том правцу у односу на изотропску антену. Повећање радијације у једном правцу резултат је смањене радијације у неком од других праваца. Важно је напоменути да се појачање антене не односи на повећање излазне снаге већ на повећање њене усмерености. Дефинисаћемо и појам ефективне површине антене која је везана за физичку величину и облик антене. Веза између појачања антене (G) и ефективне површине описана је следећом једначином:

$$G = \frac{4\pi A_e}{\lambda^2} = \frac{4\pi f^2 A_e}{c^2} \qquad (6.2)$$

где је:

A_e - ефективна површина,

f - носећа учестаност,

c - брзина светлости (~ $3*10^8$m/s),

λ - таласна дужина носиоца.

6.6 Земаљске микроталасне везе

Физички опис

Као што је речено највише коришћени тип микроталасних антена је параболична. Уобичајена величина параболичног рефлектора је 3m у пречнику. Антена је фиксирана круто и усмерава узак сноп зрака да би обезбедила предају „у линији видљивости"[1] до пријемне антене. За пренос на великим удаљеностима користи се серија микроталасних релејних станица које омогућавају да се тачка-тачка микроталасне везе повезују на жељеној раздаљини.

Примена

Најважнија примена микроталасних система је у међуградским телефонским везама, као алтернативно решење коаксијалним кабловима и оптичким влакнима. Микроталасне везе захтевају мало мање појачавача него коаксијални каблови за исту раздаљину, али је потребна линија видљивости.

Друга, све већа примена микроталаса су кратке тачка-тачка везе између зграда. Могу се користити за телевизију или за повезивање локалних рачунарских мрежа. Важна примена микроталасних веза су и ћелијски (мобилни) системи.

Преносна карактеристика

Микроталасне везе заузимају значајан део електромагнетског спектра. Уобичајене учестаности које се користе су у опсегу од 1 до 40GHz. Што је виша учестаност

[1] *Line of sight (*LOS*)*

Опсег [GHz]	Ширина опсега [MHz]	Брзина [Mb/s]
2	7	12
6	30	90
11	40	135
18	220	274

Табела 6.4 Типичне особине дигиталних микроталасних система

која се користи већа је потенцијална ширина фреквенцијског опсега, а самим тим и потенцијална брзина. У табели 6.4 приказани су фреквенцијски опсези и брзине у неким од типичних примена.

Као код свих система преноса главни извор губитка је слабљење. За микроталасне везе (и радио-учестаности) губитак се може изразити једначином:

$$L_{dB} = 10\log\left(\frac{4\pi d}{\lambda}\right)^2 \qquad (6.3)$$

где је *d* растојање, а λ таласна дужина изражена у истим јединицама. Као што се види губитак се мења са квадратом растојања.

Код микроталасних система слабљење се повећава када је време кишовито. Ефекат кише је нарочито изражен на учестаностима већим од 10GHz. Још један узрок погоршања је и интерференција. Са повећаним интересовањем за микроталасни пренос опсези преноса се преклапају и интерференција је увек могућа. Због тога је додела фреквенцијских опсега веома строго регулисана.

Уобичајени опсег за међуградске телекомуникације је од 4GHz до 6GHz. Све се више користи опсег од 11GHz. Опсег на 12GHz користи се за кабловску телевизију. Микроталасни пренос се користи за довођење ТВ сигнала до локалне инсталације кабловске телевизије. Сигнал се затим преко коаксијалних каблова дистрибуира до корисника. Микроталаси на вишим учестаностима користе се за кратке тачка-тачка везе између зграда, типичног фреквенцијског опсега од 22GHz. Више учестаности мање се користе за веће раздаљине због значајног повећавања слабљења, али су веома погодне за кратка растојања. Треба истаћи да што је учестаност виша то је антена мања и њена цена је нижа.

6.7 Сателитске микроталасне везе

Физички опис

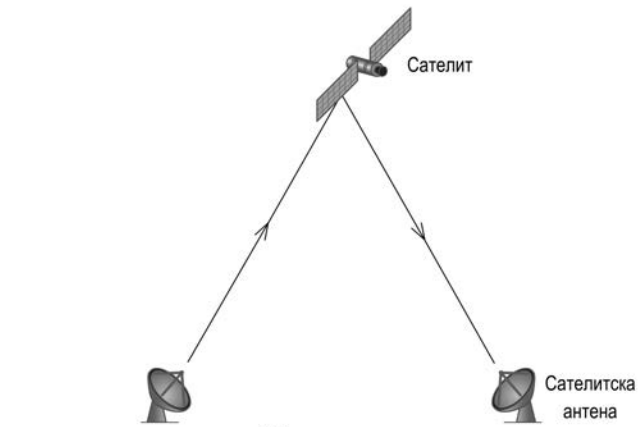
Комуникациони сателит је у ствари микроталасна релејна станица. Користи се за повезивање више земаљских микроталасних пријемника/предајника који се срећу под називом земаљске станице.

Сателит прима сигнал у једном опсегу учестаности (дирекни канал [1]), појачава га и шаље у другом опсегу учестаности (повратни канал [2]). Један сателит у орбити може да ради на неколико фреквенцијских опсега.

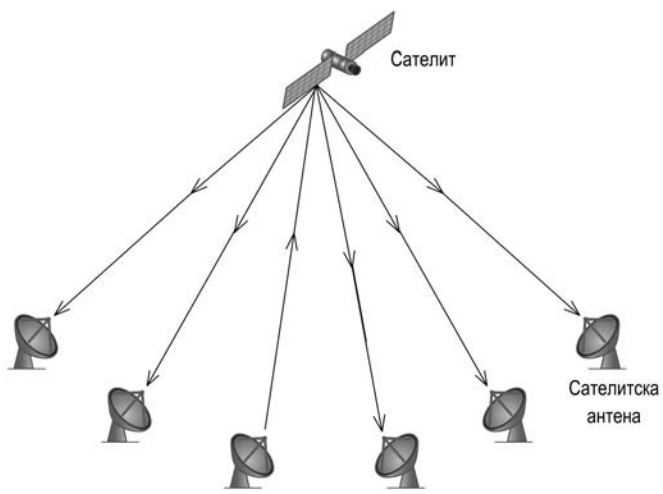
[1] *Uplink*
[2] *Downlink*

На слици 6.11 скициране су две уобичајене конфигурације у сателитским комуникацијама. У првој се сателит користи да обезбеди тачка-тачка везу између две удаљене земаљске антене. У другом случају сателит обезбеђује комуникацију земаљског предајника и групе земаљских пријемника. За комуникационе сателите да би ефикасно радили генерално се захтева да остају стационарни (релативно) посматрано у односу на Земљу. У супротном не би били стално у линији видљивости са својим земаљским станицама. Да би остао геостационаран сателит мора да има исти период ротације као Земља око своје осе. То се дешава у екваторијалној равни на висини од 35863km.

Два сателита која користе исти фреквенцијски опсег уколико су близу ометаће један другог. Да би се то спречило постојећи стандарди захтевају 4° размак [1] у опсегу 4/6GHz и



а) Веза тачка - тачка



б) Веза један ка свима

Слика 6.11 Конфигурација сателитских система

[1] Угао посматран са Земље

3° у опсегу 12/14GHz. Могући број сателита је ограничен. Постоје и сателити на ниским (LEO[1]) и средњим висинама (MEO[2]).

Примена

Комуникациони сателити су технолошка револуција једнако важна као и оптички каблови. Међу најзначајнијим применама су следеће:

- дистрибуција телевизијских програма,
- телефонска мрежа на великим растојањима,
- приватне пословне мреже.

Сателити се због своје могућности да шаљу свима користе у дистрибуцији телевизијског програма. Програм се шаље сателиту који га затим емитује великом броју сателитских станица на Земљи, које га даље дистрибуирају до корисника[3]. Новија примена сателитске технологије је да се видео сигнал емитује директно до корисника. Сателити се користе и код директних веза између телефонских централа у јавној телефонској мрежи.

У последње време повећан је број корисник микростаница (VSAT[4]). Ови мали терминали имају антену највише 1m у пречнику и снаге су око 1W. Директан канал је брзине 19,2kb/s, а повратни канал најмање 512kb/s. У многим VSAT системима микростанице немају довољно снаге да комуницирају директно једна са другом (наравно преко сателита). Уместо тога специјална земаљска станица (хаб[5]) са антеном великих димензија и великог појачања користи се за преусмеравање саобраћаја између VSAT система. У оваквом начину рада или предајник или пријемник имају велику антену и снажан појачавач. Негативан резулат уштеде на крајњим станицама је повећање кашњења.

Преносна карактеристика

Оптимални фреквенцијски опсег је 1 до 10GHz. У фреквенцијском опсегу испод 1GHz значајан је ниво природних извора шума као што су: галактички, соларни и атмосферски шум као и сметње од различитих електронских уређаја. Изнад 10GHz шум је значајно ослабљен апсорпцијом атмосфере и падавина. Већина сателита која омогућава тачка-тачка услуге данас користи фреквенцијски опсег од 5,925 до 6,425GHz за пренос од Земље до сателита (директан канал) и опсег 3,7 до 4,2GHz за пренос од сателита до Земље (повратни канал). Ова комбинација је позната као опсег 4/6GHz. Уочимо да се учестаности директног и повратног канала разликују. За континуирани рад без сметњи сателит не може да прима и шаље на истој учестаности. Тако се сигнал примљен од земаљске станице на једној учестаности мора послати натраг на другој учестаности. Фреквенцијски опсег 4/6GHz налази се у оквиру оптималне зоне од 1 до 10GHz али је попуњен. Друге учестаности се у овом опсегу не могу користити пошто су додељене земаљским микроталасима. Због тога се започело са слањем у опсегу[6] 12/14GHz. И овај опсег се такође попунио па се прешло на опсег[7] 20/30GHz.

[1] *Low Earth Orbit*
[2] *Medium Earth Orbit*
[3] DBS (*Direct Broadcast Satelite*)
[4] *Very Small Aperture Terminals*
[5] *Hub*
[6] Директан канал у опсегу од 14 до 14,5GHz а повратни канал у опсегу од 11,7 до 12,2 GHz.
[7] Директан канал у опсегу од 27,5 до 30,0 GHz а повратни канал у опсегу од 17,7 до 20,2 GHz.

Слабљења у фреквенцијским опсезима 12/14GHz и 20/30GHz су велика али омогућавају шире фреквенцијске опсеге у преносу, пријемнике мањих димензији и нижих цена.

Набројаћемо још неке од карактеристика сателитских комуникација. Прво, због великих удаљености постоји кашњење услед простирања између предајне и пријемне сателитске станице на Земљи, које је око четвртине секунде. Кашњење је уочљиво у телефонском разговору. Постоје такође и проблеми код детекције и корекције грешке. Сателитске комуникације су типа један ка свима[1]. Многе станице шаљу ка сателиту а оно што сателити шаљу може да прими више станица.

6.8 Радио-везе

Физички опис

Принципијелна разлика између радио и микроталасних веза је у томе што у радиовезама антене зраче у свим правцима (имају кружни дијаграм зрачења - омнидирекциони), а у земаљским и сателитским микроталасним везама антене су усмереног зрачења.

Примена

Радио-везе се генерално користе за фреквенцијски опсег од 30MHz до 1GHz. Користи се и термин „бродкаст радио" који покрива VHF[2] и део UHF[3] фреквенцијског опсега. Овај опсег покрива FM радио и UHF и VHF телевизију, а користи се и за мреже за пренос података.

Преносна карактеристика

Јоносфера је транспарентна у фреквенцијском опсегу преко 30MHz. На тај начин могућ је само директан пренос[4] и различити предајници неће ометати један другог. За разлику од микроталасне области радио-таласи су мање осетљиви на слабљења услед падавина (нпр. кише). Као и код микроталаса слабљење је изражено једначином 6.3. Најважнији узрок погоршања пријемног сигнала је интерференција због различито пређених путева[5]. Рефлексија од земље, воде и различите препреке могу да доведу до тога да таласи између две антене прелазе више различитих путања.

6.9 Пренос у инфрацрвеном опсегу

Пренос у инфрацрвеном опсегу постиже се коришћењем пријемника/предајника (примопредајника) који као носилац користи некохерентну инфрацрвену светлост. Примопредајници морају бити у линији видљивости један према другом или у правцу рефлектованих таласа. Разлика између микроталаса и инфрацрвеног преноса је та што инфрацрвени таласи не продиру кроз зидове. Тако је проблем заштите и интерференције разрешен. Додатна предност је та што за пренос у овом опсегу дозволе нису потребне.

[1] *Broadcasting*
[2] *Very High Frequency*
[3] *Ultra High Frequency*
[4] У линији видљивости (LOS -*Line of sight*).
[5] *Multipath interference*

Слика 6.12 Простирање површинских таласа

6.10 Бежично простирање

Сигнал који емитује антена простире се на један од три начина: површински таласи [1], ваздушни таласи [2] и директни таласи [3].

Површински таласи

Површински таласи при свом простирању прате закривљеност Земље и могу да достигну значајну раздаљину у опсегу видљивости (слика 6.12). Овакав ефекат може да се постигне са учестаностима до 2MHz. Најпознатији пример употребе површинских таласа је AM радио.

Ваздушни таласи

Ваздушни таласи се користе радио-аматерско емитовање, интернационално емитовање итд. С ваздушним таласима сигнал са станице на Земљи одбија се од јоносфере [4] натраг ка Земљи. Иако изгледа да се таласи одбијају од јоносфере као о подлогу са добром рефлексијом [5] ефекат је добијен рефракцијом [6] (слика 6.13). Ваздушни талас може се простирати великим бројем скокова [7], преламајући се наизменично између земљине површине и јоносфере. Са оваквим начином простирања сигнал се може примити километрима далеко од предајника.

Слика 6.13 Простирање ваздушних таласа

[1] *Ground wave*
[2] *Sky wave*
[3] У линији видљивости
[4] Јонизујући део атмосфере
[5] Одбијање таласа
[6] Преламање таласа
[7] *Hops*

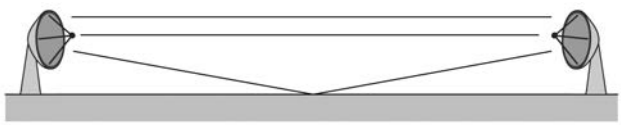
Слика 6.14 Простирање директних таласа

Директни таласи

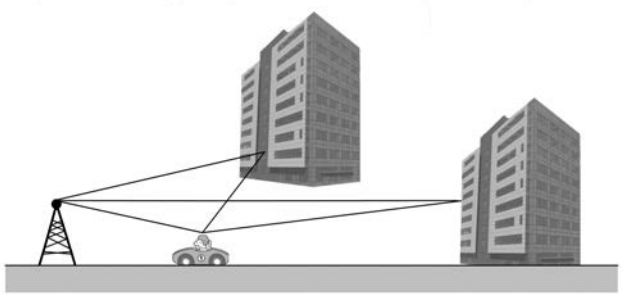
Изнад 30MHz не могу се користити ни површински таласи ни ваздушни таласи већ комуникација мора бити у директној видљивости (слика 6.14). За сателитске комуникације сигнал преко 30MHz се не рефлектује од јоносфере тако да се сигнал може пренети између земаљске станице и сателита, или између две станице које су у ефективној линији видљивости. Термин ефективна користи се пошто се микроталаси преламају или рефрактују о атмосферу. Количина па чак и правац преламања зависе од различитих услова, али се генерално микроталаси преламају тако да се простиру даље него што је директна оптичка видљивост.

Више путања[1]

За бежични пренос широке су могућности постављања антена тако да пријемник и предајник могу да буду у линији видљивости и на тај начин спрече могуће сметње због препрека. Ово се генерално односи само на сателитске и тачка-тачка микроталасне везе. У другим случајевима, као што је на пример мобилна телефонија, препреке су незаобилазне. Сигнал се може одбити од препреке тако да на место пријемника долази више копија сигнала са променљивим кашњењем. Може се чак догодити да не постоји директан сигнал. У зависности од разлике у пређеном путу директног и рефлектованог таласа композитни сигнал може да буде јачи или слабији од директног сигнала. На слици 6.15 приказан је генерални случај простирање таласа по више путања. Ова појава је типична за земаљске микроталасне и мобилне везе.



а) Микроталаси у линији видљивости предајника и пријемника



б) Мобилна телефонија

Слика 6.15 Пример интерференције услед више путања

[1] *Multipath*

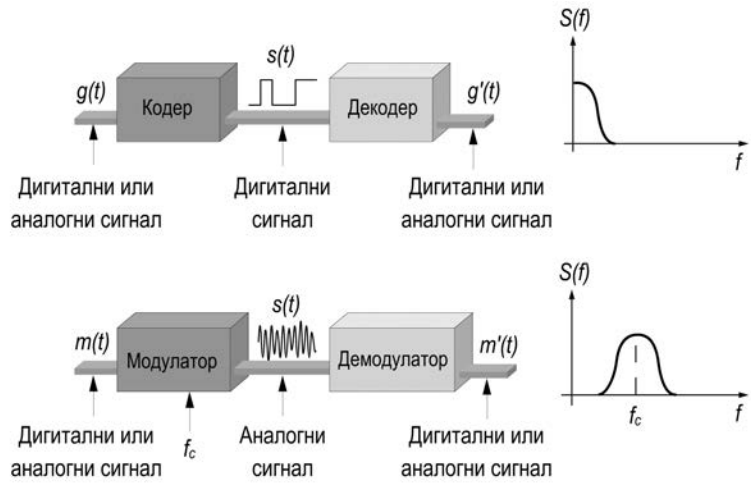
7. Претварање (кодирање) података

У 5. поглављу разматрали смо разлику између аналогних и дигиталних података и аналогних и дигиталних сигнала[1]. Слика 7.1 приказује процес кодирања. Код дигиталне сигнализације извор података *g(t)* (који може да буде било дигиталан било аналоган) претвара се[2] у дигитални сигнал *s(t)*. Стварна форма *s(t)* зависи од система кодирања и користи се да оптимизира употребу трансмисионог медијума. На пример, кодирањем се може сачувати опсег сигнала или се могу минимизирати грешке.

Основа за аналогну сигнализацију је континуални сигнал константне учестаности, познат као сигнал носилац[3]. Учестаност носиоца треба да буде усаглашена са трансмисионим медијумом. Подаци се могу преносити помоћу сигнала носиоца користећи модулације. Модулација је процес утискивања изворних података у носиоца учестаности f_c. Циљ у поступку модулације је да се сигнал обради тако да буде подесан за пренос. Све модулационе технике укључују операције над једним или више основних параметара сигнала носиоца:

- амплитудом,
- фреквенцијом,
- фазом.

Улазни сигнал *m(t)* може бити аналогни или дигитални и назива се модулишући сигнал, или сигнал у основном опсегу[4]. Резултат модулације носећег сигнала назива се модулисани сигнал. Као што се на слици 7.1 види *s(t)* је сигнал ограниченог спектра.



Слика 7.1 Кодирање и модулационе технике

[1] Погледати слику 5.5.
[2] *Encoded*
[3] *Carrier signal*
[4] *Baseband signal*

Локација спектра везана је за f_c (учестаност носиоца) и обично је центрирана око f_c. Свака од четири могуће комбинације скициране на слици 7.1 у широкој је употреби. Навешћемо неколико значајних разлога за коришћење неке комбинације:

- Дигитални подаци, дигитални сигнал. Генерално, опрема за кодирање дигиталних података у дигитални сигнал мање је комплексна и мање скупа него опрема за дигитално-аналогну модулацију.
- Аналогни подаци, дигитални сигнал. Конверзија аналогних података у дигиталну форму омогућава употребу модерне дигиталне преносне и комутационе технике. Предност дигиталног приступа анализирана је у 5. поглављу.
- Дигитални подаци, аналогни сигнал. Неки трансмисиони медијуми, као што су оптичка влакна и бежични медијуми, једино могу да преносе аналогне сигнале.
- Аналогни подаци, аналогни сигнал. Аналогни подаци у електричној форми могу се преносити као сигнали у основном опсегу једноставно и јефтино. Ово је случај са преносом говорног сигнала кроз говорни канал. Резултат модулације је померање опсега сигнала из основног опсега у неки други (транспоновани) део спектра. На овај начин више сигнала, сваки на различитој позицији у спектру, могу да деле исти трансмисиони медијум. То је познато као фреквенцијско дељење спектра или фреквенцијско мултиплексирање.

Испитаћемо технике које су укључене у сваку од ових комбинација.

7.1 Дигитални подаци, дигитални сигнали

Дигитални сигнал је секвенца дискретних, дисконтинуалних напонских (струјних) импулса. Сваки импулс је сигнализациони елемент (елементарни сигнал). Бинарни подаци преносе се кодирањем сваког бита података у сигнализациони елемент. У најједноставнијем случају постоји један према један кореспонденција између битова и сигнализационих елемената.

У примеру приказаном на слици 5.5, бинарно 0 репрезентује нижи напонски ниво, а бинарно 1 виши напонски ниво. Као што ћемо видети у овом одељку користе се и различите врсте других кодерских шема.

Термин	Јединице	Дефиниција
Елементарни податак	Бит	Бинарна јединица или нула
Брзина (проток) података	Бит у секунди [b/s]	Брзина којом се елементарни подаци шаљу
Сигнализациони елемент (елементарни сигнал)	Дигитални: напонски импулс константне амплитуде Аналогни: импулс константне амплитуде, фазе и учестаности	Онај део сигнала који заузима најмањи интервал сигнализационог кода
Сигнализациона брзина или модулациона брзина	Сигнализациони елемент у секунди	Брзина којом се сигнализациони елемент шаље

Табела 7.1 Термини и јединице

Прво ћемо дефинисати неке термине (табела 7.1). Уколико сви сигнализациони елементи имају исти алгебарски знак, односно ако су сви позитивни или су сви негативни, онда је сигнал униполаран. У поларној сигнализацији једно логичко стање представља се позитивним напонским нивоом, а друго стање негативним напонским нивоом.

Брзина података (проток) је брзина у битима у секунди којом (b/s) се подаци шаљу. Трајање или дужина бита је време које је потребно предајнику да пошаље бит; за брзину података *R,* трајање бита је 1/ *R*.

Модулациона брзина је брзина којом се сигнализациони ниво мења. Ово зависи од природе дигиталног кодовања, што ће бити објашњено у овом поглављу. Модулациона брзина је изражена у бодима и представља број сигнализационих елемената у секунди. Из традиционалних разлога користе се термини знак [1] и пауза [2] и односе се на 1 и 0, респективно.

Задатак који се поставља при интерпретацији дигиталних сигнала на пријемној страни може се сумирати на следећи начин (погледати слику 3.14): прво, пријемник мора да зна временске одреднице сваког бита [3]. То значи да пријемник мора да зна, са одређеном тачношћу, када бит почиње и када се завршава. Друго, пријемник мора да одреди да ли је ниво сигнала, за сваку битску позицију, висок (1) или низак (0). На слици 5.9 ови задаци извршавају се преко одмеравања сваке позиције у средини интервала и пореде се са вредношћу граничног напона. Због шума и других утицаја јављају се грешке тако да се 1 прогласи за 0 и/или обрнуто.

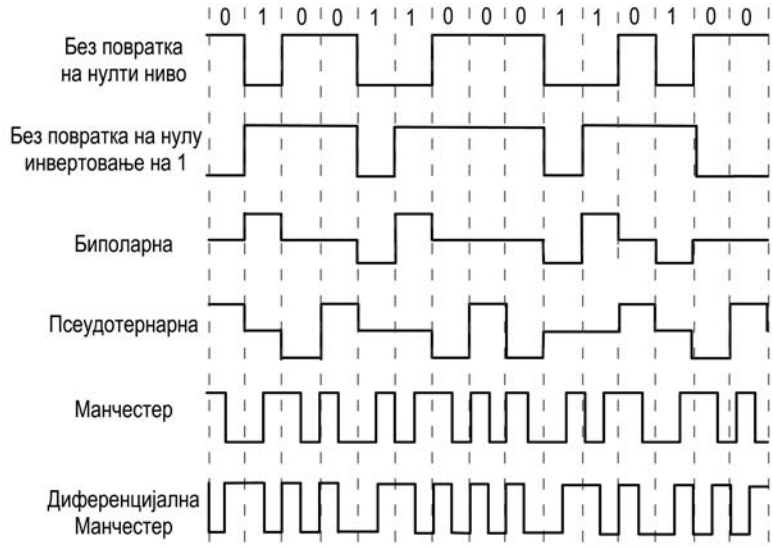
Који фактори одлучују колико ће пријемник бити успешан у интерпретирању долазећег сигнала? Видели смо у 3. поглављу да су важна три фактора: однос сигнал/шум, брзина података и опсег спектра сигнала. Тачно је и да:

- повећање брзине података повећава вероватноћу да је примљени бит погрешан [4],
- повећање односа сигнал/шум смањује вероватноћу грешке,
- повећање пропусног опсега дозвољава повећање брзине података.

Постоји још један фактор који се може употребити за побољшање перформанси - то су кодне шеме. Кодне шеме могу се интерпретирати као повезивање битова података и сигнализационих елемената. У даљем тексту биће описане (слика 7.2) неке од уобичајених метода које се могу категоризовати на следећи начин:

- без повратка на нулу (NRZ [5]) -
  - 0 - висок ниво,
  - 1 - низак ниво;
- биполарна (AMI [6]) -
  - 0 - нема линијског сигнала,
  - 1 - позитиван или негативан ниво, наизменично се мења када су узастопне јединице;

[1] *Mark*
[2] *Space*
[3] *Timing*
[4] Величина која се користи је вероватноћа грешке BER (*Bit Error Rate*).
[5] NRZ - *Non Return to Zero*
[6] Среће се под називом биполарна AMI (*Alternate Mark Inversion* - сваки следећи знак је инверзија).



Слика 7.2 Формати сигнала дигитално кодираних

- Манчестер (бифазна) -
  0 - прелазак са високог напонског нивоа на низак у средини интервала,
  1 - прелазак са ниског напонског нивоа на висок у средини интервала;
- диференцијална Манчестер - увек је прелазак у средини интервала
  0 - прелазак на почетку интервала,
  1 - нема преласка на почетку интервала;

Пре него што опишемо ове технике анализираћемо факторе којима се оне могу међусобно поредити.

Спектар сигнала

Неколико аспеката спектра је важно. Непостојање високих учестаности значи да је мањи пропусни опсег потребан за пренос. На другој страни, укидање једносмерне компоненте [1] такође је пожељно. Са једносмерном компонентом у сигналу мора да постоји директна физичка веза преносних уређаја; без једносмерне компоненте могуће је повезивање преко трансформатора. Ово обезбеђује изванредну електричну изолацију и редукује интерференцију.

Синхронизационе могућности сигнала

Напоменули [2] смо потребу да одредимо почетак и крај сваке битске позиције. Ово није лак задатак и може да захтева посебан такт који се доводи да синхронизује предајник и пријемник. Неке шеме кодирања превазилазе овај проблем.

Способност сигнала да детектује грешке

О техникама за детекцију грешака биће речи у 10. поглављу. Неке примитивне технике за детекцију грешака могу се обезбедити природом технике кодирања.

[1] DC (*Direct Current*)
[2] Пожељно је да у сигналу постоји доста транзиција (прелазака са једног напонског нивоа на други).

Интерференција сигнала и имуност на сметње

Одређени кодови обезбеђују добре карактеристике преноса у присуству сметњи. Уобичајено је да се квалитет преноса изражава преко вероватноће грешке битова BER.

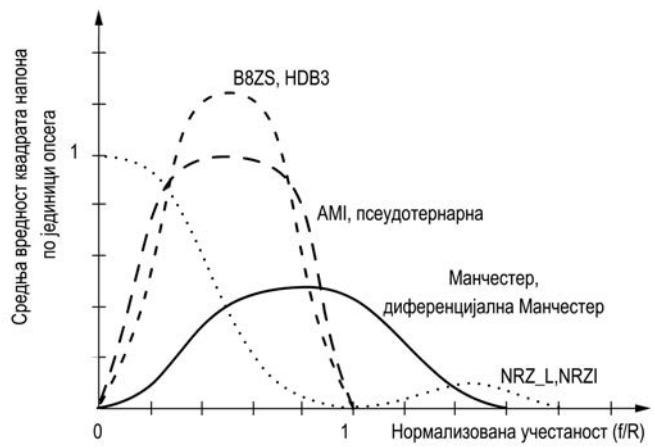
Цена и комплексност

Цена дигиталних кола у сталном је паду. Што је већа сигнализациона брзина (да би достигла захтевану битску брзину) то је цена већа. Неки кодови захтевају сигнализациону брзину која је већа од битске брзине. У одељцима који следе биће описане неке од техника кодирања.

Кодови без повратка на нулу

Кодови без повратка на нулу (NRZ[1]) имају карактеристику да је напонски ниво константан за време битског интервала (слика 7.2); не постоји транзиција (нема повратка на нулти напонски ниво). На пример константан позитиван напон представља бинарно 1, а одсуство напонског (струјног) нивоа представља бинарно 0. Много чешће негативан напон представља једну бинарну вредност а позитиван напон другу бинарну вредност и среће се под називом - без повратка на нулти ниво (NRZ_L[2]). Кодови NRZ су најједноставнији за реализацију и ефикасно користе фреквенцијски опсег. Ова последња особеност приказана је на слици 7.3. На овој слици учестаност је нормализована на брзину података (*R*). Као што се може видети највећи део енергије сконцентрисан је између једносмерне компоненте (нулта учестаност) и половине брзине сигнала.

Кôд NRZI[3] је пример диференцијалног кôда. У диференцијалном кодирању информација коју треба пренети представљена је променом узастопних сигнализационих елемената. Кодирање се обавља на следећи начин: уколико је бит бинарно 0, онда се он кодира истим сигналом којим је кодиран и претходни бит; уколико је бит бинарно 1 онда се он кодира сигналом различитим од оног којим је кодиран претходни бит.



Слика 7.3 Спектрална густина различитих техника кодирања сигнала[4]

[1] *Non Return to Zero*
[2] *Non Return to Zero Level*
[3] Без повратка на нулу, инвертовање код јединица NRZI (*Non Return to Zero Invert on ones*).
[4] HDB3 (*High Density Bipolar* 3 *Zeros*), B8Z8 (*Bipolar with* 8 *Zeros Substitution*).

Највеће ограничење NRZ кодова је присуство једносмерне компоненте и недостатак могућности за синхронизацију. Да бисмо илустровали поменути недостатак узмимо за пример дужу комбинацију јединица или нула. NRZ кодови даће као резултат константан напон у току дужег периода времена. Под овим условима било каква неусаглашена промена такт сигнала на пријемној или предајној страни довешће до њиховог губитка синхронизације.

Бинарни вишенивоски кодови

Бинарни вишенивоски кодови користе више од два нивоа сигнала. Примери ове технике представљени су на слици 7.2: биполарна[1] и псудотернарна техника кодирања.

У случају биполарне (AMI[2]) технике бинарно 0 представља се недостатком линијског сигнала, а бинарно 1 предствља се позитивним или негативним импулсом. Импулс бинарно један наизменично мења поларитет. Постоји неколико предности бинарних вишенивоских кодова. Прво, не може да дође до губитка синхронизације уколико се појави више узастопних јединица. Дуже комбинације нула и даље су проблем. Друго, пошто јединице мењају поларитет (позитиван и негативан напонски ниво) неће постојати једносмерна компонента. Треће, нарушавање промена поларитета напонског нивоа може послужити као једноставан начин за детекцију грешке.

Особености које су изложене у претходном параграфу могу се применити и на псеудотернарну технику. Код ње се бинарно 1 представља одсуством сигнала на линији, а бинарно 0 наизменично позитивним и негативним импулсима. Ова техника се на краћим растојањима користи код мрежа интегрисаних услуга (ISDN[3]).

Са вишенивоским бинарним кодирањем линијски сигнал може да добије вредност једног од три напонска (струјна) нивоа. Сваки сигнализациони елемент, који би могао да садржи $\log_2 3 = 1{,}58$ бита информације носи само један бит информације. То значи да вишенивоска техника кодирања није тако ефикасна као NRZ (за два напонска нивоа $\log_2 2 = 1$). Недостатак је и то што пријемник мора да направи разлику између три напонска нивоа (+A, -A, 0) уместо само два (као што је код NRZ). Последица је да вишенивоске бинарне технике кодирања за исту вероватноћу грешке захтевају 3dB више снаге сигнала у односу на оне са само два нивоа сигнала (слика 7.4). На други начин се може рећи: вероватноћа грешке код NRZ кодова, за задати однос сигнал/шум, значајно је мања него код вишенивоских бинарних кодова.

Бифазна техника кодирања

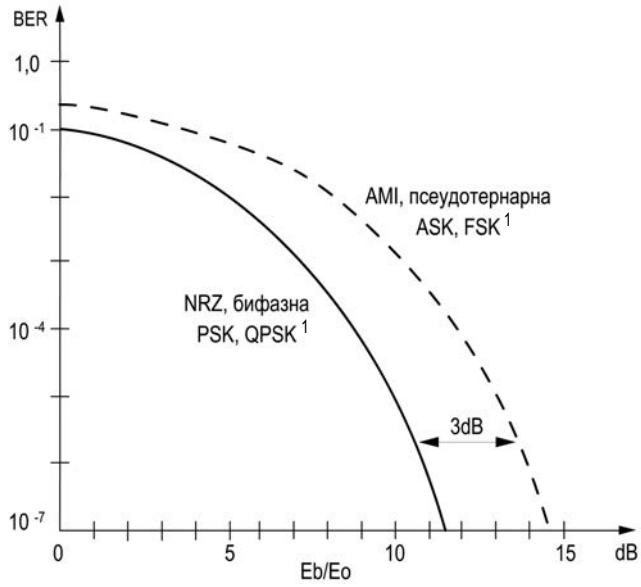
Постоји још једна група техника кодирања под заједничким називом бифазне технике од којих су Манчестер и диференцијални Манчестер кôд често у употреби.

---

[1] *Bipolar AMI*

[2] *Alternate Mark Inversion*

[3] *Integrated Service Digital Network* пројектована је као дигитална мрежа с краја на крај. Капацитет приступа корисника у мрежу повећан је применом:
- базног приступа (*Basic Rate Access*) са два B (*Bearer*) канала и једним D (*Data*) каналом. Сваки B канал има проток од 64kb/s и користи се за пренос корисничких информација (говора или података) док D канал служи за сигнализацију и има проток 16kb/s,
- примарни приступ (*Primary Rate Access*) са 30B канала за пренос корисничких информација и једним B каналом за сигнализацију са протоком 64kb/s.



Слика 7.4 Теоретска вероватноћа грешке по биту за различите шеме кодирања у зависности од односа снаге сигнала и шума [2]

У овој техници захтева се бар један прелазак са једног напонског нивоа на други (транзиција) у битском интервалу, а може да их има и више. Транзиција у средини интервала служи и као механизам за синхронизацију (такт) и као податак. Прелазак са ниског на висок ниво представља јединицу, а прелазак са високог на низак представља нулу [3]. У диференцијалном Манчестер коду транзиција у средини интервала користи се само за синхронизацију. Логичко 0 кодира се присуством транзиције на почетку битског интервала, а логичка 0 изостајањем транзиције на почетку битског интервала.

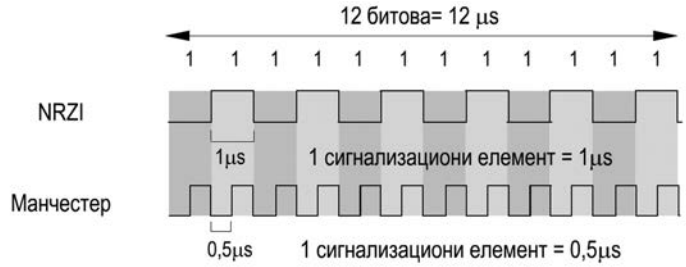
Обе бифазне технике захтевају најмање једну транзицију у току битског интервала. Због тога је модулациона брзина двоструко већа од NRZ. То значи да је и ширина опсега спектра сигнала већа. Предности бифазних техника су следеће:

- Синхронизација - пошто постоји (предвидљива) транзиција на средини синхронизационог интервала пријемник се може на њу синхронисати.
- Нема једносмерне компоненте - бифазни кодови не садрже једносмерну компоненту.
- Детекција грешке - изостајање транзиције може се искористити за детекцију грешке. Шум на линији нема такво својство да може у једном битском интервалу да изазове две различите промене и доведе до грешке која се не може детектовати.

[1] У другом делу овог поглавља детаљно ће бити објашњене шеме кодирања ASK, FSK, PSK, QPSK (комбинација аналогни подаци, дигитални сигнал).

[2] Релација је следећа $S/N = 2E_b/E_0$. Детаљније се може погледати у литератури [16].

[3] У литератури се среће супротна дефиниција - транзиција са ниског на висок напонски ниво представља бинарно 0, а транзиција са високог на низак ниво представља бинарно 1. Дефиниција која је овде изнета у складу је са стандардом IEEE802.3 за локалне рачунарске мреже.



Слика 7.5 Поворка бинарних јединица и нула код брзине од 1Mb/s

Као што се може уочити опсег спектра бифазних сигнала је прихватљиве ширине и не садржи једносмерну компоненту. Бифазне технике се доста користе. Манчестер кодови се користе код локалних рачунарских мрежа са коаксијалним кабловима и упреденим парицама (IEEE802.3 и IEEE802.5).

7.2 Модулациона брзина

Када се користи одређена техника кодирања мора се направити разлика између брзине података (која се изражава у битима у секунди) и модулационе брзине (која се изражава у бодима). Брзина података, или битска брзина, изражена је са $1/T_b$ где је T_b трајање једног бита. Модулациона брзина је брзина којом су сигнализациони елементи генерисани.

Посматрајмо на пример Манчестер кодирање: сигнализациони елемент је импулс трајања половине битског интервала. Од поворке која се састоји од бинарних јединица и/или нула, коју треба пренети, генерише се континуална поворка таквих импулса (слика 7.5). На тај начин је максимална модулациона брзина Манчестер кода $2/T_b$. Слика 7.5 приказује пренос поворке бинарних јединица брзином од 1Mb/s када се користе кодови NRZI и Манчестер. Генерално посматрано:

$$D = \frac{R}{L} = \frac{R}{\log_2 M} \tag{7.1}$$

где је:

D - модулациона брзина изражена у бодима,

R - брзина података изражена у битима у секунди,

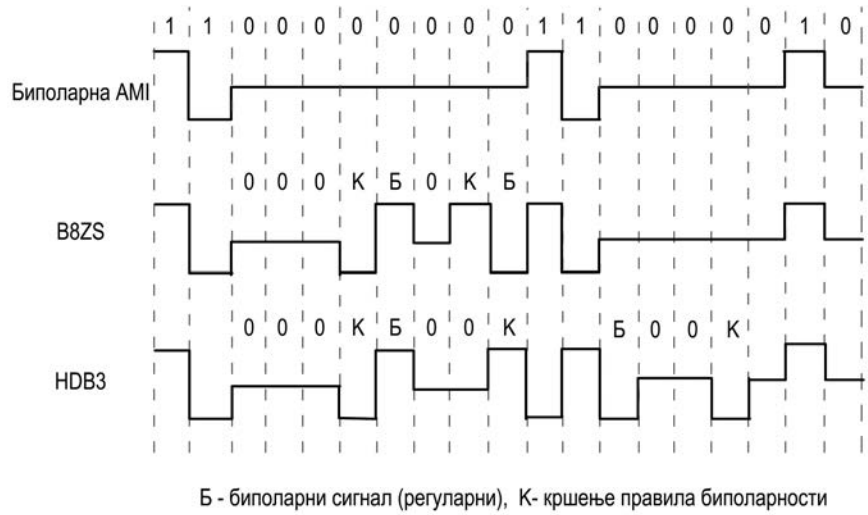
M - број различитих сигнализационих елемената $= 2^L$,

L - број битова по сигнализационом елементу.

Један од начина за описивање брзине модулације је одређивање просечног броја транзиција које се јављају у току битског интервала. Уопштено посматрајући то зависи од тачне секвенце битова која се шаље.

7.3 Технике уношења прекршаја биполарности

Иако су бифазне технике широко распрострањене у локалним рачунарским мрежама оне се не користе у комуникационим системима на већим удаљеностима.



Слика 7.6 Технике кодирања B8ZS, HDB3 и биполарна AMI

Разлог је већа сигнализациона брзина у односу на брзину података, што резултује значајним повећањем цене преноса.

Други приступ био би употреба неке од техника уношења прекршаја биполарности. Идеја је следећа: уместо секвенце података која би довела до константног напонског нивоа на линији, убацује се секвенца која ће обезбедити довољан број транзиција тако да пријемни такт сигнал задржи синхронизацију. Убачену секвенцу пријемник треба да препозна, одстрани је и обезбеди оригиналну секвенцу података. Захтеви који се постављају пред ову технику су следећи:

- да нема једносмерне компоненте,
- да нема дугих поворки сигнала нултог напонског нивоа,
- да нема смањења брзине података,
- способност да детектује грешке.

Две технике се уобичајено користе код удаљених веза и приказане су на слици 7.6.

Техника B8ZS [1] заснована је на биполарном AMI коду. Негативан ефекат биполарног AMI кода је дугачка поворка нула која може да доведе до губитка синхронизације. Овај проблем се превазилази на следећи начин:

- када се појави октет са свим нулама а последњи напонски импулс који је претходио октету је позитиван, онда ће се осам нула октета кодирати као 000 + - 0 - +;
- када се појави октет са свим нулама а последњи напонски импулс који је претходио октету је негативан, онда ће се осам нула октета кодирати као 000 - + 0 + -;

Ове технике доводе до нарушавања кода [2], које не може да буде проузроковано шумом или смањењем квалитета сигнала у преносу. Пријемник препознаје узорак и инте-

[1] Биполарна са заменом 8 нула (*Bipolar with 8 Zeros Substitution*). Уобичајено се користи у Северној Америци.
[2] Узорак сигнала који није дозвољен код AMI кода.

	Број импулса (јединица) пре последње замене	
Поларитет претходног импулса	Непаран	Паран
-	000 -	+ 00 +
+	000 +	- 00 -

Табела 7.2 Правило код HDB3 кода

рпретира октет као да се састоји од свих нула. Кодна шема HDB3[1] (табела 7.2) је такође заснована на AMI коду. Поворка од четири нуле замењује се секвенцом од једног или два импулса. У сваком од случајева четврта нула замењена је „прекршајем биполарности". Потребно је одређено правило које обезбеђује да су узастопни прекршаји (нарушавање) биполарности различитог поларитета како се не би појавила једносмерна компонента. То значи да уколико је последњи прекршај биполарности био позитиван, следећи треба да буде негативан и обрнуто. Табела 7.2 показује да се овај услов испитује на основу тога:

- да ли је број импулса после последње промене у коду био паран или непаран и
- какав је поларитет последњег импулса пре појаве четири нуле.

Слика 7.3 приказује карактеристике спектра ова два кода. Као што се види ни један од њих нема једносмерну компоненту. Већи део енергије је сконцентрисан у релативно малом делу спектра око учестаности која је једнака половини брзине података. Ови кодови погодни су за пренос података великих брзина.

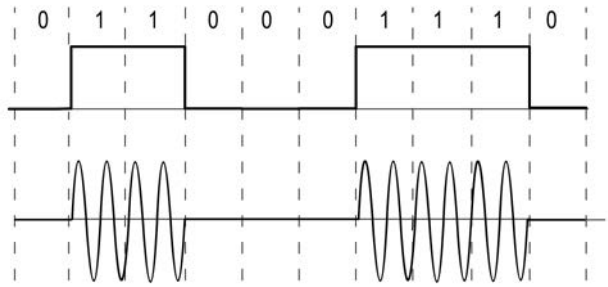
7.4 Дигитални подаци, аналогни сигнали

Анализираћемо слање дигиталних података аналогним сигналима. На пример овај начин користи се за трансформацију сигнала за пренос дигиталних података преко јавне телефонске мреже. Телефонска мрежа је пројектована да прима, комутира и преноси анологне сигнале у говорном опсегу (300 до 3400Hz). За сада није уобичајено да се може дигитални сигнал директно преносити претплатничким петљама[2]. Дигитални уређаји прикључени су на мрежу преко модема (модулатор-демодулатор) који конвертује дигиталне податке у аналогни сигнал, и обрнуто. У телефонској мрежи модеми дају сигнале у говорном опсегу. У основи иста техника користи се за модеме који раде на вишим учестаностима (на пример микроталаси).

Напоменули смо да модулација укључује операцију над једним (или више) параметром носећег простопериодичног сигнала: амплитудом, учестаношћу и фазом. Мењајући један од њих сразмерно дигиталном сигналу који треба пренети и задржавајући остала два константним добија се:

- амплитудска ASK[3] (слика 7.7),
- фреквенцијска FSK[4] (слика 7.8),
- фазна PSK[5] (слика 7.10).

[1] Биполарна високе густине са 3 нуле (*High Density Bipolar 3 Zeros*). Уобичајено се користи у Европи и Јапану.
[2] Део јавне телефонске мреже од комутационог центра до претплатника (*subscriber line*).
[3] *Amplitude Shift Keying*
[4] *Frequency Shift Keying*
[5] *Phase Shift Keying*



Слика 7.7 Шематски приказ ASK модулације

На првом месту модулација носиоца примењује се када се жели да се дигитални сигнал преноси бежичним трансмисионим медијумима (нпр. радио-везама). Исто тако примењује се и у жичним трансмисионим медијумима.Тада је основни циљ да се транслацијом спектра сигнала оствари вишеканални пренос, или да се побегне из области ниских учестаности где трансмисионе карактеристике канала нису увек најбоље. У свим овим случајевима опсег спектра резултујућег сигнала је транслиран и центриран око носеће учестаности f_c.

Амплитудска модулација

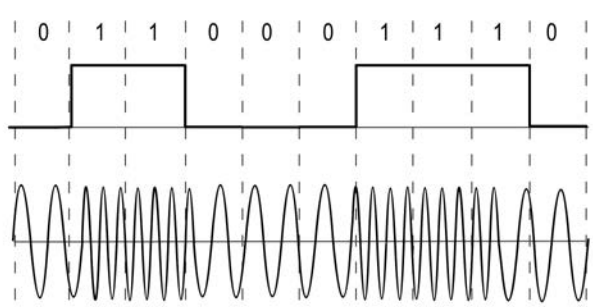
Код амплитудске модулације (ASK) две бинарне вредности су представљене различитим амплитудама носиоца. Уобичајено је једна амплтуда нула: то значи да је једна вредност дигиталног сигнала представља присуством носиоца, а друга одсуством носиоца. Резултујући сигнал који се шаље се може представити на следећи начин:

$$\text{ASK} \qquad s(t) = \begin{cases} A\cos\left(2\pi f_c t + \theta_c\right) & \text{бинарно 1} \\ 0 & \text{бинарно 0} \end{cases}$$

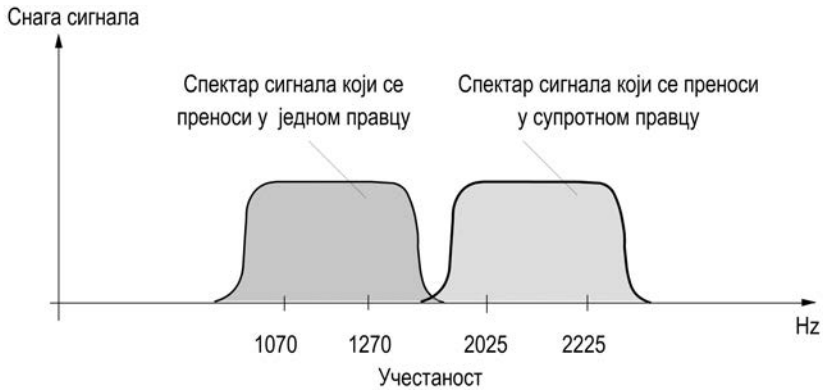
где је носилац $A\cos 2\pi f_c t$. Модулација ASK користи се за пренос дигиталних сигнала оптичким влакнима тако што један сигнализациони елемант представља присуство светлости а други сигнализациони елемент представља одсуство светлости.

Фреквенцијска модулација

Најчешћа врста фреквенцијске модулације (FSK) је бинарна (BFSK). Две бинарне вредности представљене су са две различите учестаности f_1 и f_2 носећег си-



Слика 7.8 Шематски приказ FSK технике модулације



Слика 7.9 Пренос у потпуном дуплексу у говорном каналу

гнала. Обично су учестаности померене у односу на носећу учестаност f_c за исти износ Δf тако да је $f_1 = f_c + \Delta f$ и $f_2 = f_c - \Delta f$.

FSK $$s(t) = \begin{cases} A\cos(2\pi f_1 t + \theta_c) & \text{бинарно 1} \\ A\cos(2\pi f_1 t + \theta_c) & \text{бинарно 0} \end{cases}$$

Слика 7.9 показује пример коришћења FSK у говорном каналу са потпуним дуплексом. Говорни канал пропушта учестаности приближно у опсегу 300 до 3400Hz, а потпуни дуплекс значи да се сигнал шаље у оба правца истовремено. Да би се постигао пренос у потпуном дуплексу овај пропусни опсег се раздваја на 1700Hz. Учестаност која се користи да би репрезентовала 1 или 0 у једном правцу (предајник или пријемник) центрирана је на 1170Hz, са померајем од 100Hz на обе стране. Ефекат смењивања ових двеју учестаности је сигнал чији је спектар на левој страни слике 7.9.

Слично, за друге правце (предајник или пријемник) користи се фреквенцијски померај од 100Hz на сваку страну од централне учестаности која је 2125Hz. Спектар овог сигнала приказан је на десној страни слике 7.9. Уочимо да постоји мало преклапање, а самим тим и интерференција. FSK модулација је мање осетљива на шум него ASK модулација. У говорним каналима уобичајено се користи брзина од 1200b/s.

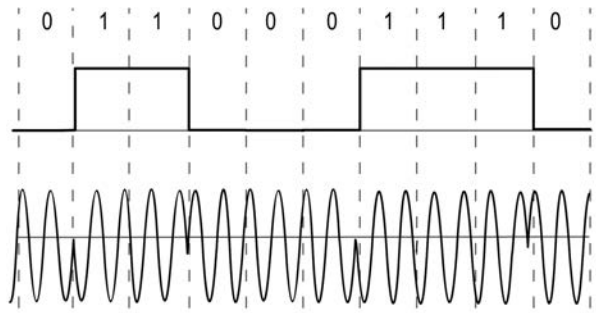
Фазна модулација

Код фазне модулације (PSK) фаза носиоца мења се у складу са променом дигиталног сигнала који треба пренети. На слици 7.10 нацртан је пример двофазне модулације (BPSK[1]). Види се да бинарном 0 одговара фаза $\theta = 0$, а бинарном 1 фаза $\theta = \pi = 180°$. Резултујући сигнал може се представити на следећи начин:

BPSK $$s(t) = \begin{cases} A\cos(2\pi f_c t + \pi) & \text{бинарно 1} \\ A\cos(2\pi f_c t) & \text{бинарно 0} \end{cases}$$

Поред BPSK користи се и диференцијална модулација (DPSK[2]). Код DBPSK бинарно 0 представља се слањем сигнала исте фазе, а бинарно 1 представља се слањем

[1] *Binary Phase Shift Keying*
[2] *Differential Phase Shift Keying*



Слика 7.10 Шематски приказ PSK технике модулације

сигнала супротне фазе од фазе сигнала послатог у претходном сигнализационом интервалу. То значи да фазни померај DBPSK сигнала зависи од претходног бита, а не од неког константног референтног сигнала.

Много ефикасније коришћење пропусног опсега система преноса може се постићи када сваки сигнализациони елемент представља више од једног бита.

На пример, уместо фазног помераја од $\theta = 180°$, као што је дозвољено у PSK, уобичајена техника модулације је кватернарна фазна модулација (QPSK[1]) која користи фазне помераје који су умножак од 45°.

QPSK

$$s(t) = \begin{cases} A\cos\left(2\pi f_c t + 45°\right) & 11 \\ A\cos\left(2\pi f_c t + 135°\right) & 10 \\ A\cos\left(2\pi f_c t + 225°\right) & 01 \\ A\cos\left(2\pi f_c t + 315°\right) & 00 \end{cases}$$

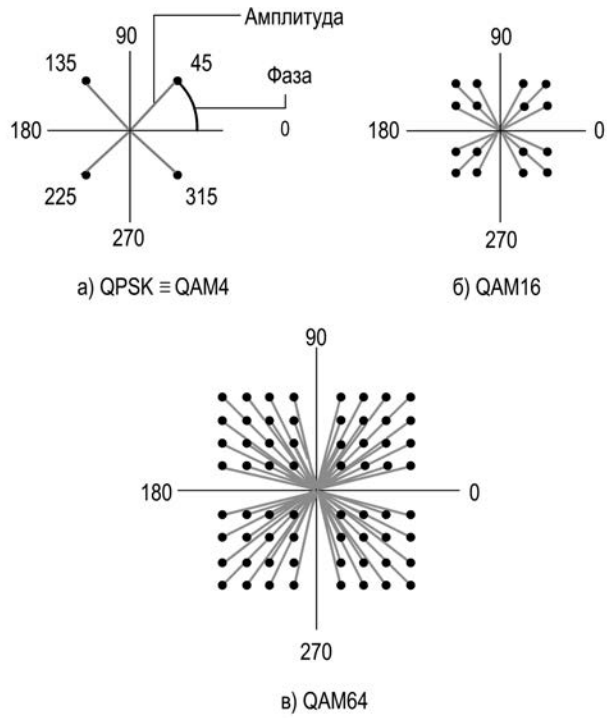
Модулације са више нивоа

Број сигнализационих елемената у секунди мери се у бодима (Bd[2]). За време сваког бода пошаље се један сигнализациони елемент[3]. То значи да *n* бодна линија шаље *n* сигнализационих елемената у секунди. На пример линија од 2400Bd пошаље један симбол сваких[4] 416667 μs. Уколико се симбол састоји од напонских (струјних) импулса нпр. позитивног за логичко 0 и негативног за логичко 1, брзина података је 2400b/s. Уколико се уместо два користе четири напонска нивоа сваки сигнализациони елемент представља (састоји се од) 2 бита.

Са четири могућа фазна помераја постоје 2 бита по сигнализационом елементу, тако да је брзина у битима (битска брзина) двоструко већа од брзине у бодима (бодска брзина[5]). Ова техника, кватернарна PSK (QPSK), доста се користи.

Концепт ширине опсега, бод, сигнализациони интервал и битска брзина често су збуњујући. Ширина опсега преносног система (трансмисионог медијума) је опсег

[1] *Quaternary Phase Shift Keying*
[2] *Baud* - одељак 7.2.
[3] Користе се и термини елементарни сигнал или симбол.
[4] 1/2400
[5] Пошто се ради о брзини на линији (трансмисионом медијуму) користи се и термин линијска брзина.



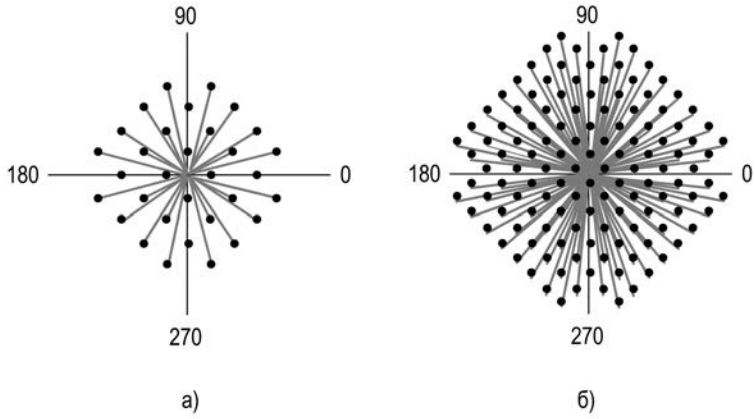
Слика 7.11 Констелациона раван а) QPSK б) QAM16 в) QAM64

учестаности који пролази кроз систем са минималним слабљењем. То је физичка карактеристика трансмисионог медијума и мери се у херцима (Hz). Брзина у бодима је број сигнализационих елемената у секунди. Сваки сигнализациони елемент шаље једну информацију, тј. један симбол. Брзина у бодима и сигнализациона брзина су исто. Модулациона техника нпр. (QPSK) одређује број битова по сигнализационом елементу. Брзина у битима је количина информација која се шаље каналом и једнака је производу броја сигнализационих елемената у секунди и броја битова у секунди.

Сви новији модеми користе комбинацију модулационих техника да би послали више битова по једном боду. Често се користи комбинација више амплитуда и више фазних помераја. На слици 7.11а означене су тачке од 45°, 135°, 225° и 315° са константном амплитудом која је представљена удаљеношћу тачака од координатног почетка. Фаза тачке одређена је углом који чини права провучена кроз координатни почетак и тачку са позитивним смером *x* осе.

Четири комбинације представљене на слици 7.11а могу се користити за слање 2 бита по симболу. На слици 7.11б приказана је друга модулациона шема у којој се користе четири амплитуде и четири фазе, свеукупно 16 различитих комбинација. Ова модулациона шема може се искористити за слање 4 бита по сигнализационом елементу. Назива се квадратурна амплитудска модулација[1] - QAM16 и представља комбинацију ASK и PSK модулација. Користи чињеницу да је могуће послати два

[1] *Quadrature Amplitude Modulation* (QPSK = QAM4)



а) б)

Слика 7.12 Констелациона раван за модеме по стандарду
а) V.32 за 9600b/s б) V.32bis за 14400b/s

различита сигнала истовремено на истој носећој учестаности користећи две копије носеће учестаности померене једна у односу на другу за 90°. Код QAM сваки носилац је ASK модулисан. Два независна сигнала истовремено се шаљу преко истог медијума. На пријему сигнали се демодулишу и резултат комбинује да би се добио оригинални бинарни улазни податак. На пример да би се пренело 9600b/s преко линије која може да пренесе 2400Bd користи се QAM16.

На слици 7.11в приказана је још једна модулациона шема која користи комбинацију различитих амплитуда и фаза. Видимо 64 различите комбинације тако да је могуће послати 6 битова по једном симболу. Ова модулациона шема означава се као QAM64. Могуће су и QAM[1] модулације још већег реда (256 чак и 1024).

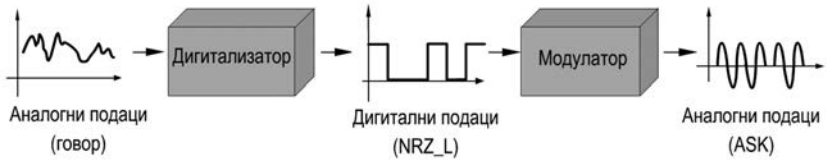
Дијаграми на слици 7.11, који показују комбинацију амплитуде и фазе називају се констелациони дијаграми. Сваки од модемских стандарда садржи свој сопствени констелациони узорак (комбинацију) и може да комуницира само са модемима који користе исти констелациони узорак. Са много тачака у констелационом узорку чак и мали шум ће при детекцији сигнала изазвати грешку која резултује у пријему највероватније већег броја погрешних битова.

За корекцију грешке код модеме већих брзина стандардизовано је да се дода још један бит у сваком сигнализационом елементу. Овај метод (шема) познат је као Трелис кôд (TCM[2]). На пример, модеми по стандарду V.32 (слика 7.12) користе 32 констелационе тачке за слање 4 бита података и 1 бит парности по симболу. На линији са 2400Bd обезбеђена је брзина од 9600b/s са детекцијом грешке.

7.5 Аналогни подаци, дигитални сигнали

У овом одељку анализираћемо процес трансформације аналогног података у дигитални сигнал. Тачније, биће много коректније указати да је то процес конвертовања

[1] Користи се код модема ADSL (*Asymmetric Digital Subscriber Line* - асиметрична дигитална претплатничка петља).
[2] *Trellis Code Modulation*

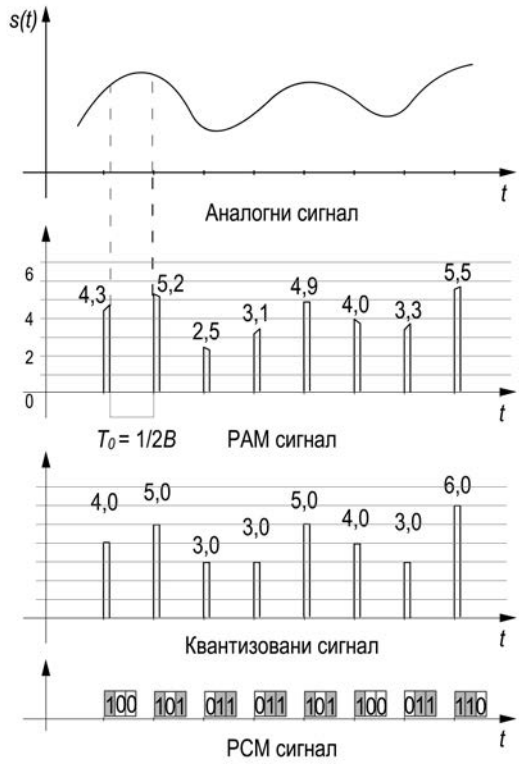


Слика 7.13 Дигитализовање аналогних података

аналогног податка у дигитални сигнал, и он је познат као дигитализација. Једном када је аналогни податак конвертован у дигитални податак, могу се:

- дигитални подаци преносити користећи NRZ_L. У овом случају пут од аналогног до дигиталног сигнала је директан,
- дигитални подаци кодирати као дигитални сигнал коришћењем другог кода (не само NRZ_L). У том случају захтевају се додатни кораци,
- дигитални подаци конвертовати у аналогни сигнал користећи једну од модулационих техника објашњену у одељку 7.1.

Ово последње илустровано је на слици 7.13, која показује да су говорни сигнали дигитализовани и затим конвертовани у аналогни ASK сигнал. На тај начин омогућен је дигитални пренос. Говорни подаци, пошто су дигитализовани, могу се третирати као дигитални подаци, иако преносни параметри (нпр. микроталаси) диктирају коришћење аналогних сигнала.



Слика 7.14 Импулсна кодна модулација

Склоп који се користи за конвертовање аналогних података у дигиталну форму за пренос и даље издвајање оригиналних аналогних података из дигиталних, назива се кодек (кодер-декодер). У овом одељку описаћемо једну од широко распрострањених техника[1]: импулсну кодну модулацију (PCM[2]).

Импулсна кодна модулација

Импулсна кодна модулација заснована је на теореми одмеравања која каже:

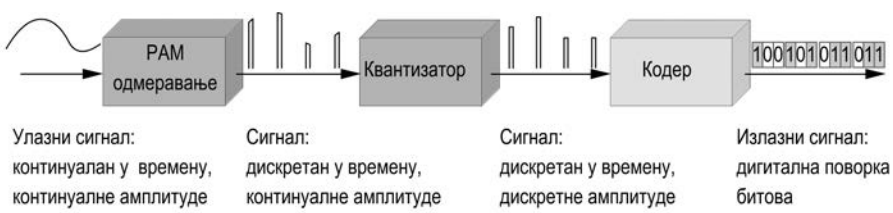
„Уколико је сигнал *f(t)* одмерен[3] у регуларним интервалима времена, брзином двоструко већом од највише значајне учестаности сигнала, онда одмерци садрже све информације оригиналног сигнала. Функција *f(t)* се може реконструисати коришћењем нископропусног филтра."

Уколико су говорни подаци ограничени на фреквенције испод 4000Hz, 8000 одмерака у секунди биће довољно да потпуно окарактерише говорни сигнал. Уочимо да су ово аналогни узорци (одмерци) као што је представљено на сликама 7.14а и 7.14б. Претпостављено је, да је оригинални сигнал ограниченог спектра *B* и највише учестаности f_M. Одмерци су узети брзином $2*f_M$, или сваке $1/(2*f_M)$ секунде. Ови узорци представљени су као уски импулси чија је амплитуда пропорционална вредности оригиналног сигнала. Овај процес познат је као импулсна амплитудска модулација (PAM[4]).

Важно је рећи да је импулсна амплитудска модулација (PAM) први корак ка импулсној кодној модулацији (PCM), као што представљено на слици 7.14б. Да би се произвео PCM сигнал, PAM одмерци се квантизују (дискретизују). То значи да се сваки PAM импулс апроксимира са *n*-битском целобројном вредношћу. На пример уколико је $n = 3$ онда ће се $8 = 2^3$ нивоа користити за апроксимирање PAM импулса. Ако се користи 8 битова по сваком одмерку, што даје 256 квантизационих нивоа квалитет реконструисаног говорног сигнала на пријему може се упоредити са аналогним преносом.

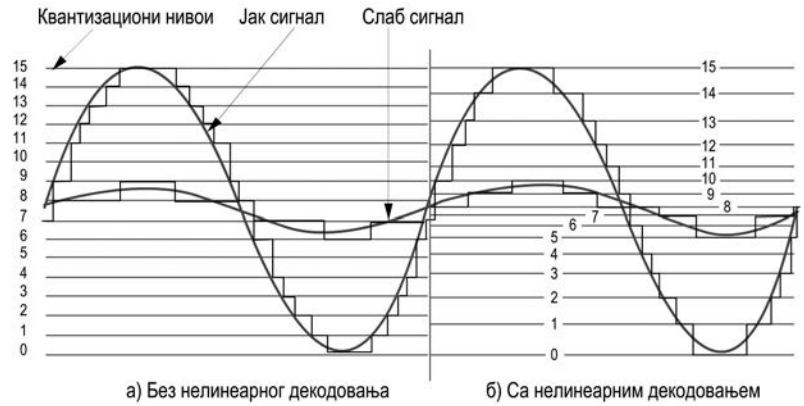
Треба уочити да када се број одмерака у секунди (8000) помножи с бројем битова по одмерку (8) добије брзина (64kb/s). Толико је потребно за један говорни сигнал. Слика 7.15 илуструје процес генерисања дигиталног сигнала почевши од временски континуалног и амплитудски континуалног (аналогног) сигнала.

Дигитални сигнал састоји се од група од по *n* битова, где је 2^n број амплитуда PCM импулса.



Слика 7.15 Аналогно-дигитална конверзија

[1] Друга техника је делта модулација
[2] *Pulse Code Modulation - PCM*
[3] Узети узорци - одмерци (*samples)*
[4] *Pulse Amplitude Modulation*



Слика 7.16 Нелинеарно кодовање

Квантизацијом PCM импулса, оригинални сигнал је само апроксимација и не може се тачно реконструисати. Ефекат је познат као грешка квантизације или шум квантизације.

Ефекат грешке квантизације може се умањити коришћењем технике познате као нелинеарно кодовање. Квантизациони нивои неравномерно се распоређују (слика 7.16): користи се већи број квантизационих нивоа за сигнал са малом амплитудом (слаб сигнал), а мањи број квантизационих нивоа за сигнал са већом амплитудом (јак сигнал).

7.6 Аналогни подаци, аналогни сигнали

Модулација је дефинисана као процес комбиновања улазног сигнала *m(t)* и сигнала носеће учестаности f_c. За дигиталне податке потреба за модулацијом је јасна: када су на располагању само аналогни системи преноса модулација је потребна за претварање дигиталних података у аналогне сигнале.

Када су подаци већ аналогни мање је јасна потреба за модулацијом. Сам говорни сигнал преноси се преко телефонских линија у свом оригиналном спектру (тј. пренос у основном опсегу спектра).

Навешћемо два разлога који могу да допринесу да се користи аналогни сигнал за пренос аналогних података:

- пренос сигнала је ефикаснији на вишим учестаностима. За бежични пренос немогуће је преносити сигнал у основном опсегу спектра; антена која би то омогућавала била би километар (или више) у пречнику,
- модулацијом се може обезбедити истовремени пренос више сигнала (тзв. фреквенцијски мултиплекс[1]).

У овом делу анализираћемо технике за модулацију користећи аналогне податке. Као што је већ поменуто, три основна параметра простопериодичног сигнала, носиоца, користе се за модулацију: амплитуда, фаза и фреквенција.

[1] Фреквенцијски мултиплекс биће детаљно описан у 8. поглављу.

Амплитудска модулација

Амплитудска модулација (AM) је најједноставнији тип модулације и скицирана је на сликама 7.17 и 7.18. Заснована је на принципу модификације амплитуде носиоца тако да она у процесу модулације постаје директно сразмерна модулишућем сигналу, оригиналном носиоцу поруке. Математички, процес може бити описан као:

$$s(t) = [1 + n_a m(t)] \cos 2\pi f_c t \tag{7.1}$$

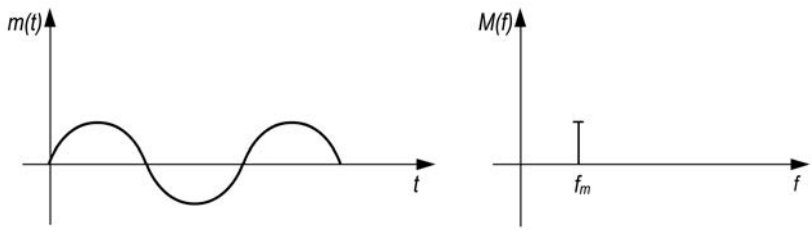
где је $\cos 2\pi f_c t$ носилац а $m(t)$ је модулишући сигнал. Параметар n_a назива се степен модулације и изражава максималну релативну амплитуду модулисаног сигнала. Вредност 1 је једносмерна компонента.

Из једначине 7.1 види се да AM сигнал представља множење [1+ n_a $m(t)$] са носиоцем, а [1+$n_a m(t)$] представља анвелопу (обвојницу) резултујућег сигнала. Посматрајући AM сигнал у временском домену види се да је за n_a < 1 анвелопа тачна репродукција оригиналног сигнала. За n_a > 1 анвелопа ће прећи временску осу и информација о оригиналном сигналу је изгубљена. Извешћемо израз за $s(t)$ уколико је $m(t)$ простопериодичан сигнал $\cos 2\pi f_m t$ (слика 7.17):

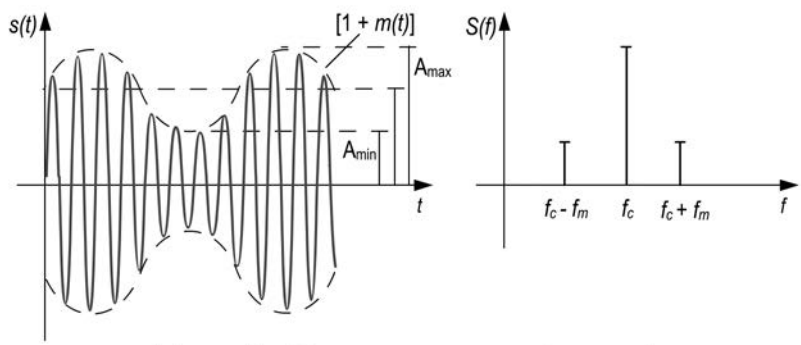
$$s(t) = [1 + n_a \cos 2\pi f_m t] \cos 2\pi f_c t \tag{7.2}$$

Користећи тригонометријске једнакости једначина се може проширити на:

$$s(t) = \cos 2\pi f_c t + \frac{n_a}{2} \cos 2\pi (f_c - f_m) t + \frac{n_a}{2} \cos 2\pi (f_c + f_m) t \tag{7.3}$$

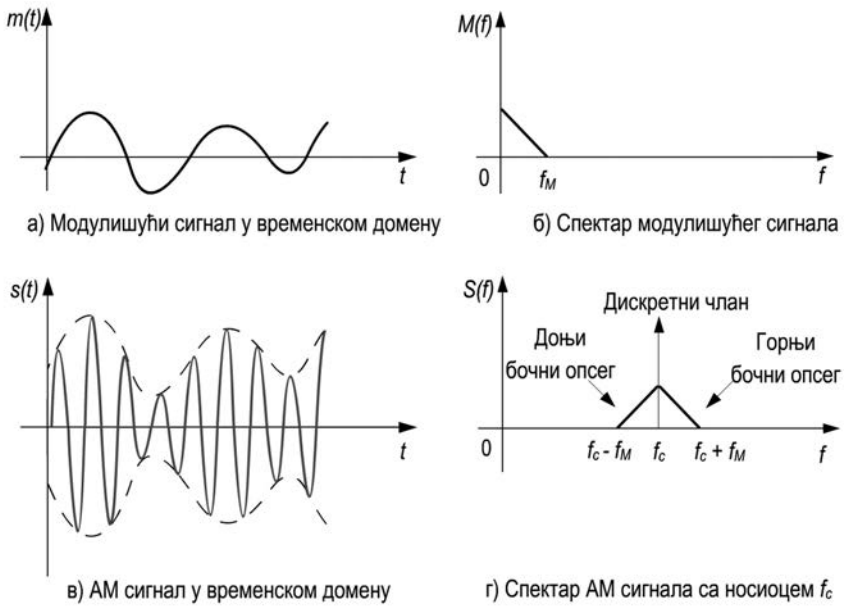


а) Синусоидални модулациони сигнал у временском и фреквенцијском домену



б) Резултујући AM сигнал у временском и фреквенцијском домену

Слика 7.17 Амплитудски модулисан сигнал у временском и фреквенцијском домену



Слика 7.18 Спектар АМ сигнала

Резултујући АМ сигнал састоји се од простопериодичне компоненте носеће учестаности f_c и две простопериодичне компоненте учестаности f_c+f_m и $f_c- f_m$ симетричне у односу на носећу учестаност (слика 7.17). Видимо да је множење у временском домену резултовало у двема транслацијама у спектру: f_c+f_m и $f_c - f_m$. Поред тога се појавила и компонента сигнала на носећој учестаности (дискретан члан) која је последица присуства једносмерне компоненте у једначини 7.1.

Погледајмо пример АМ сигнала када је модулишући сигнал апериодичан сигнал *m(t)* који има спектар ограничен учестаношћу f_M (слика 7.18а). Резултат множења је не само транслација спектра модулишућег сигнала за величину f_c већ и појава њему симетричног спектра $f_M - f_c$ у односу на f_c. Значи спектар се проширио. Спектар који се налази у опсегу учестаности од f_c до $f_c + f_M$ назива се вишим (горњим) бочним опсегом а њему симетричан спектар у опсегу учестаности од $f_c - f_M$ до f_c нижим (доњим) бочним опсегом.

Оригинални сигнал у свом основном опсегу учестаности има спектар који заузима опсег учестаности:

$$B_0 = f_M - 0 = f_M \tag{7.4}$$

Модулисани сигнал, носилац поруке, заузима два пута шири опсег учестаности:

$$B_T = (f_C + f_M) - (f_C - f_M) = 2 f_M = 2B_0 \tag{7.5}$$

Пошто модулисани сигнал има два бочна опсега (АМ-2БО) са слике 7.18в види се да оба опсега (и горњи и доњи) имају облик спектра модулишућег сигнала. За пренос оригиналне поруке довољно је преносити само један од бочних опсега. Такав амплитудски модулисан сигнал назива се АМ сигнал са једним бочним опсегом (АМ-1БО).

Угаона модулација

У поступку угаоне модулације амплитуда носиоца (синусоидалног таласног облика) остаје непромењена, а његов угао се мења модулишућим сигналом и постаје карактеристичан параметар у коме је садржан податак који се преноси. Одатле за овај поступак и потиче назив угаона модулација. Специјални случајеви угаоне модулације: фреквенцијска (FM) и фазна модулација (PM) нашле су у преносу сигнала широку примену. Пођимо од таласног облика носиоца који је дат изразом:

$$s(t) = A_c \cos\Omega(t) = A_c \cos[2\pi f_c t + \varphi(t)] \tag{7.6}$$

Претпоставимо да модулишући сигнал *m(t),* носилац оригиналне поруке, има спектар ограничен учестаношћу f_M. У поступку угаоне модулације амплитуда A_c остаје константна, а угао $\Omega(t)$ биће зависан од модулишућег сигнала *m(t).* У процесу угаоне модулације модификује се фазни став φ тако да он постане функција модулишућег сигнала:

$$\varphi = \varphi(t) = \gamma[m(t)] \tag{7.7}$$

На тај начин општи израз за угаоно модулисани сигнал гласи:

$$s(t) = A_c \cos\Omega(t) = A_c \cos\{2\pi f_c t + \gamma[m(t)]\} \tag{7.8}$$

У зависности од тога какав ће бити аналитички облик функције $\varphi = \varphi(t) = \gamma\,[m(t)]$ разликоваће се две врсте угаоне модулације: фреквенцијска модулација (FM) и фазна модулација (PM).

Угао Ω *(t)* из једначине (7.8) назива се тренутном фазом:

$$\Omega_i = \Omega(t) = 2\pi f_c t + \varphi(t) = 2\pi f_c t + \gamma[m(t)] = \Omega_c + \gamma[m(t)] \tag{7.9}$$

Величина $\varphi(t)$ представља одступање тренутне фазе Ω_i од вредности $\Omega_c = 2\pi f_c t$ и назива се тренутном девијацијом фазе:

$$\varphi(t) = \gamma[m(t)] = \Delta\Omega_i \tag{7.10}$$

Извод тренутне фазе по времену из израза 7.9 дефинише се као тренутна учестаност угаоно модулисаног сигнала и може се представити на следећи начин:

$$2\pi f_i(t) = \frac{d[2\pi f_c t + \varphi(t)]}{dt} = 2\pi f_c + \frac{d[\varphi(t)]}{dt}$$
$$f_i(t) = f_c + \frac{1}{2\pi}\varphi`(t) \tag{7.11}$$

Одступање тренутне учестаности f_i од учестаности носиоца f_c назива се тренутном девијацијом учестаности угаоно модулисаног сигнала:

$$\frac{1}{2\pi}\frac{d[\varphi(t)]}{dt} = f_i - f_c = \Delta f_i \tag{7.12}$$

Две врсте угаоне модулације, фазна и фреквенцијска, међусобно се разликују по начину на који се остварује зависност фазе $\varphi(t)$ од модулишућег сигнала *m(t).*

Фазном модулацијом означава се угаона модулација у којој је тренутна девијација фазе $\Delta\Omega_i$ директно сразмерна модулишућем сигналу.

$$\Delta\Omega_i = \varphi(t) = n_p m(t) \tag{7.13}$$

где је n_p константа која се назива индекс фазне модулације.

Модулишући сигнал можемо да представимо у облику:

$$m(t) = A_m x(t) \tag{7.14}$$

где је A_m максимална вредност модулишућег сигнала фазне модулације $m(t)$.

Временски променљиви модулишући сигнал $m(t)$ представљен је преко нормализоване функције $x(t)$ која задовољава услов да је $|x(t)| < 1$, при чему је $|x(t)|_{max} = 1$. Максимална девијација фазе $\Delta\Omega_c$ (или само девијација фазе) је:

$$|\Delta\Omega_i|_{\max} = |\varphi(t)|_{\max} = |n_p m(t)|_{\max} = n_p |A_m x(t)|_{\max} = n_p A_m = \Delta\Omega_c \tag{7.15}$$

Израз за тренутну фазу може се представити на следећи начин:

$$\Omega_i = \Omega_i(t) = 2\pi f_c t + n_p m(t) = 2\pi f_c t + \Delta\Omega_c x(t) \tag{7.16}$$

Израз за фазно модулисани сигнал постаје:

$$s(t) = A_c \cos\Omega(t) = A_c \cos[2\pi f_c t + n_p m(t)] = A_c \cos[2\pi f_c t + \Delta\Omega_c x(t)] \tag{7.17}$$

Да поновимо: фазна модулација је угаона модулација у којој је промена фазе (тренутна девијација) директно сразмерна модулишућем сигналу. Објаснимо сада фреквенцијску модулацију: фреквенцијском модулацијом називамо угаону модулацију у којој је тренутна девијација учестаности (једначина 7.11) директно сразмерна модулишућем сигналу:

$$\Delta f_i = \frac{1}{2\pi}\frac{d\varphi(t)}{dt} = \frac{1}{2\pi} n_f m(t) \tag{7.18}$$

Максимална девијација учестаности или само девијација учестаности је:

$$|\Delta f_i|_{\max} = \frac{1}{2\pi}\left|\frac{d\varphi(t)}{dt}\right|_{\max} = \frac{n_f}{2\pi}|m(t)|_{\max} = \frac{n_f}{2\pi}|A_m x(t)|_{\max} = \frac{n_f A_m}{2\pi} = \Delta f_c \tag{7.19}$$

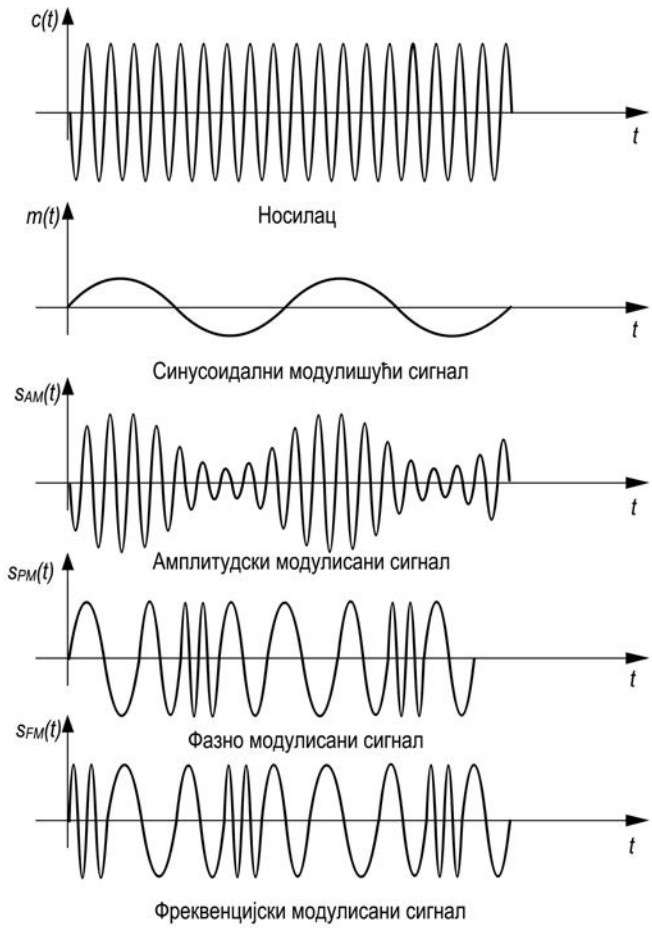
Израз за тренутну учестаност може се представити на следећи начин:

$$f_i = f_i(t) = f_c + \frac{1}{2\pi}\frac{d\varphi(t)}{dt} = f_c + \frac{1}{2\pi} n_f A_m x(t) = f_c + \Delta f_c x(t) \tag{7.20}$$

Израз за фреквенцијски модулисани сигнал постаје:

$$s(t) = A_c \cos\left[2\pi f_c t + n_f \int m(t)dt\right] = A_c \cos\left[2\pi f_c t + \Delta f_c \int x(t)dt\right] \tag{7.21}$$

Из претходне анализе види се да је фреквенцијска модулација угаона модулација у којој је промена учестаности (тренутна девијација) директно сразмерна модулишућем сигналу. Слика 7.19 илуструје амплитудску, фазну и фреквенцијску моду-



Слика 7.19 Амплитудска, фазна и фреквенцијска модулација

лацију када је модулишући сигнал синусоидална функција. Изглед фреквенцијског сигнала веома је сличан изгледу фазног сигнала. Заиста, немогуће је уочити каква је разлика без познавања модулационе функције.

Сумираћемо запажања о процесу фреквенцијске модулације. Види се да повећање јачине модулишућег сигнала повећава максимална девијација $\Delta\Omega$ (једначина 7.14) што доводи до повећања опсега спектра фазно модулисаног сигнала B_T. Као што се може видети на слици 7.19, ово неће повећати просечни ниво снаге FM сигнала која је $A_c^2 / 2$. То је значајно различито од AM, где ниво модулације утиче на снагу AM сигнала, али не утиче на ширину опсега спектра сигнала. Фреквенцијска и фазна модулација као резултат дају сигнал чији је спектар центриран око f_c (као код амплитудске модулације). Амплитудска модулација је линеаран процес и даје фреквенције које су једнаке збиру и разлици носећег сигнала и компонената модулационог сигнала. Видели смо да је опсег спектра AM сигнала је $B_T = B_{AM} = 2f_M$ (једначина 7.5).

Угаона модулација садржи чланове типа $cos\ddot{o}(t)$ који су нелинеарни и који као резултат дају широк опсег учестаности. У општем случају за слање FM и PM сигнала захтева се неограничен спектар сигнала. У пракси се може применити приближан начин израчунавања опсега спектра угаоно модулисаних сигнала[1]:

$$B_T = 2(\beta+1)B_0 = 2(\beta+1)f_M \tag{7.22}$$

где је:

$\beta = n_p A_m$ за фазну модулацију а,

$\beta = \dfrac{\Delta f_c}{B_0} = \dfrac{n_f A_m}{2\pi f_M}$ за фреквенцијску модулацију.

Једначину за опсег спектра FM сигнала можемо поново написати на следећи начин:

$$B_T = 2\Delta f_c + 2B = 2\Delta f_c + 2B_0 = 2\Delta f_c + 2f_m \tag{7.23}$$

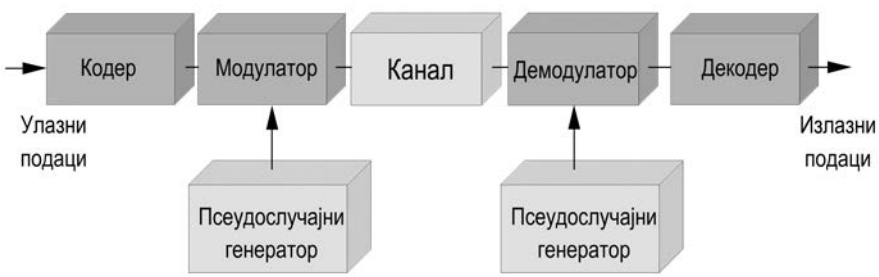
Као што се види опсег спектра FM и PM сигнала већи је од опсега спектра AM сигнала.

7.7 Системи са проширеним спектром

Проширивање спектра важна је техника за бежичне комуникационе системе. У самом почетку техника проширеног спектра искључиво се користила у војним системима. Основна је идеја да се опсег спектра сигнала на предаји прошири и на тај начин ометање и пресретање учини много сложенијим. Прво је развијен систем са фреквенцијским скакањем (FHSS[2]) а касније са директном секвенцом (DSSS[3]).

На слици 7.20 представљени су најбитнији елементи система са проширеним спектром. Улазни сигнал доводи се до кодера који формира аналогни сигнал релативно уског опсега спектра око носеће учестаности. Сигнал се даље модулише секвенцом битова која се означава као кôд проширења или секвенца проширења.

Типично, али не и увек, кôд проширења прави се помоћу псеудослучајног генератора. Као резулатат модулације добија се значајно проширен опсег спектра сигнала. Такав сигнал преноси се кроз трансмисиони медијум тј. канал. На пријемној страни ис-



Слика 7.20 Општи модел дигиталног комуникационог система са проширеним спектром

[1] Познато као Карсоново (*Carson*) правило [32], [34].

[2] *Frequency Hoping Spread Spectrum* - проширени спектар са фреквенцијским скакањем

[3] *Direct Sequency Spread Spectrum Technology* - проширени спектар са директном секвенцом

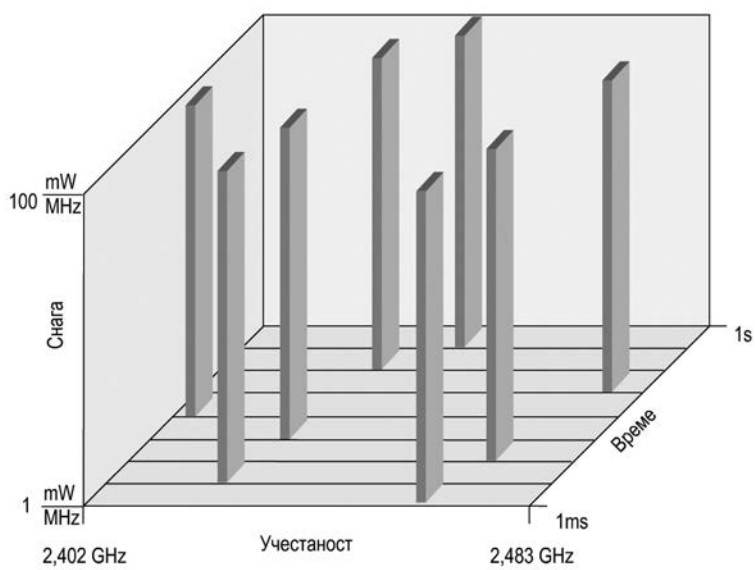
та псеудослучајна битска секвенца користи се за демодулацију сигнала проширеног спектра. Пропуштањем сигнала кроз декодер добијају се оригинални подаци. Набројаћемо неке од предности система са проширеним спектром:

- постже се већа имуност на сметње од различитих врста шума и мултипутног изобличења. Првобитна примена проширеног спектра била је у војним системима па је ово био начин да се заштите од ометања;
- може се искористити за прикривање и шифрирање сигнала. Само пријемник који зна кôд проширења може да извуче кодирану информацију;
- више корисника може независно да користи фреквенцијски опсег са незнатном међусобном интерференцијом. Ова особина искоришћена је код система са кодним мултиплексирањем (CDM[1]).

Помоћу псеудослучајног генератора добијају се псеудослучајни бројеви, тј. бројеви који „као да су случајни". Користи се и термин псеудослучајни шум. Спектар секвенце псеудослучајних бројева сличан је спектру белог шума. Бројеви се генеришу помоћу алгоритама који користе иницијалну вредност тзв. семе[2]. Алгоритам је детерминистички и као резултат даје секвенце бројева које нису статистички случајне. Важно је напоменути да уколико се не познају алгоритам и иницијална секвенца практично је немогуће предвидети секвенцу. На тај начин само пријемник који има исте информације као и предајник биће у могућности да успешно декодује сигнал.

Проширивање спектра методом фреквенцијског скакања

Код система са проширивањем спектра фреквенцијским скакањем (FHSS) сигнал



7.21 Пример расподеле канала код система са фреквенцијским скакањем

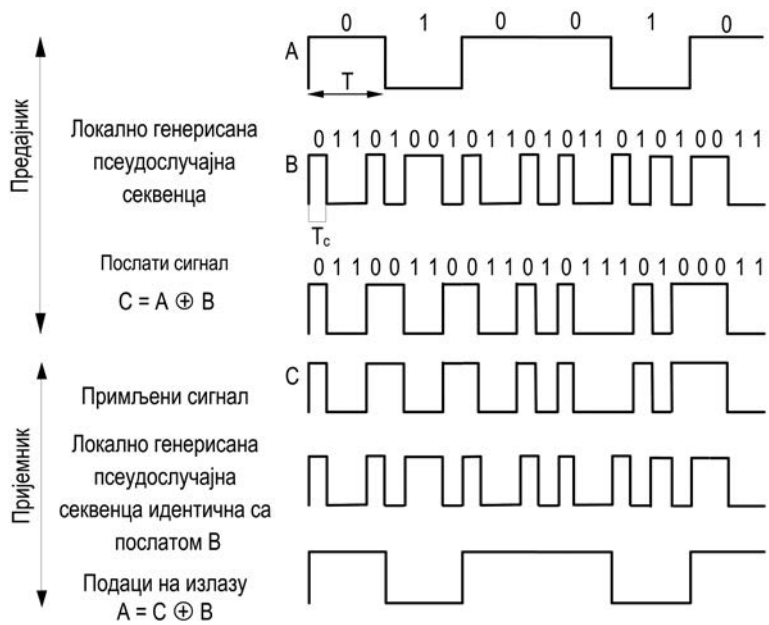
[1] *Code Division Multiplexing* (8. поглавље), или приступ са кодним мултиплексирањем CDMA *(Code Division Multiple Access).*

[2] *Seed*

се емитује (на први поглед) на случајној серији радио-учестаности (слика 7.21). Растојање између носећих учестаности обично одговара опсегу спектра улазног ускопојасног сигнала.

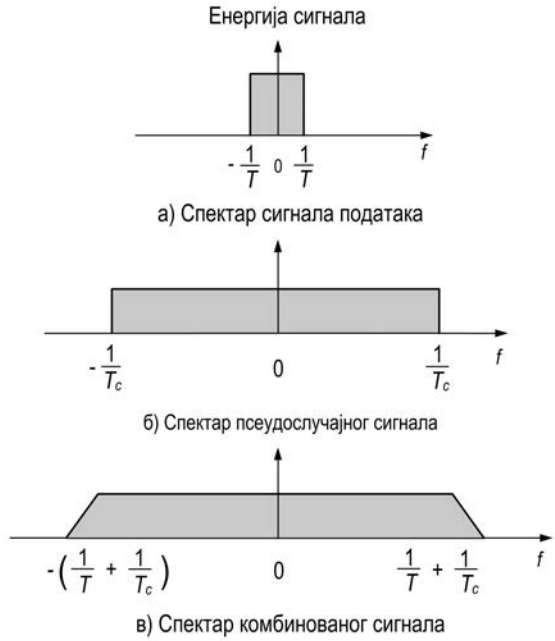
Промена учестаности одвија се после тачно одређеног интервала времена (нпр. код стандарда IEEE802.11 је мањи 400ms). За време тог интервала шаље се одређени број битова уз употребу неке од техника кодирања. На пријемној страни промена[1] носеће учестаности синхронисана је са предајником. Ако дође до ометања сигнала онда се то дешава само на једној од учестаности и утиче само на неколико битова који се том учестаношћу преносе.Носилац је ускопојасни, али се његова фреквенција мења у времену по псеудослучајном правилу, и на тај начин долази до ширења спектра. Спектар добијеног сигнала знатно је шири од минимално потребног за пренос истог податка. Пријемник детектује користан сигнал захваљујући томе што познаје његове параметре, односно образац скакања (промене) носеће фреквенције.

У случају да није тако овај сигнал се манифестује као краткотрајни импулсни шум чиме је постигнута тајност преноса код ових система. Брзина скакања зависи од земље у којој се користи ова техника, тако да постоје FHSS системи са брзим и са спорим скакањем. Код ових система није изражен проблем близу-далеко и они имају кратко време аквизиције синхронизације, али захтевају сложен синтетизатор учестаности и неопходно је FEC[2] кодирање. Домети који се могу постићи овом техником мањи су него применом DSSS система, али је зато могућ истовремени рад (коегзистенција) већег броја FHSS система на истом географском простору.



Слика 7.22 Пример проширивања спектра директном секвенцом

[1] За промене с једне на другу учестаност користи се и термин фреквенцијско скакање (*frequency hopping*).
[2] *Forward Error Correction*



Слика 7.23 Апроксимација спектра DSSS сигнала

Проширивање спектра методом директне секвенце

Код система са проширивањем спектра директном секвенцом (DSSS) сваки бит оригиналног сигнала представљен је са више битова у предајном сигналу уз коришћење кôда проширења. Проширивање спектра предајног сигнала у директној је зависности од броја употребљених битова. То значи да 10-битни кôд проширења увећава фреквенцијски опсег 10 пута више од 1-битног кôда проширења.

Један од начина који се користи код DSSS система је следећи: операција ексклузивно или примењује се између оригиналне секвенцу битова и кôда проширења. Назив за такав бит је чип [1], јер он не носи никакву информацију. Као што је познато за операцију ексклузивно или (ЕИЛИ [2]) важи следеће правило:

$$0 \otimes 0 = 0 \qquad 0 \otimes 1 = 1 \qquad 1 \otimes 0 = 1 \qquad 1 \otimes 1 = 0$$

На слици 7.22 приказан је један пример. Треба уочити да информациони бит 1 инвертује кôд проширења док информациони бит 0 доводи до његовог слања без инверзије. Брзина секвенци битова која се добија једнака је брзини кôда проширења тј. псеудослучајне секвенце. Као резултат добија се знатно шири спектар од минималне ширине потребне за пренос исте поруке (слика 7.23).

Да би пријемник могао да прими емитовани податак неопходно је да и он познаје коришћене псеудослучајне секвенце, иначе неће бити у стању да разликује информацију од шума. Тиме се постиже да потенцијални пријемници, који желе да прислу-

[1] *Chip*
[2] XOR (*Exclusive OR*)

шкују комуникацију, нису у стању да примете да она постоји. У случају да дође до оштећења једног или више чипова могуће је помоћу одређених статистичких техника реконструисати сигнал на пријему, без захтева за поновним слањем. Ови системи су отпорнији на покушај ометања од FHSS, имају врло малу вероватноћу пресретања сигнала, велику отпорност на вишепутни пренос, али знатно дуже време аквизиције синхронизације, и захтевају контролу и управљање снагом.

8. Мултиплексирање

Поставља се следећи проблем: две станице међусобно комуницирају и није им потребан целокупни капацитет трансмисионог медијума. Ефикасности ради потребно је изнаћи начин како тај капацитет може да се дели. Термин који се за такву поделу користи је мултиплексирање. Уобичајена примена мултиплексирања јесу међуградске[1], међудржавне и међуконтиненталне линије. Трансмисиони медијуми на овим правцима великог су капацитета, то су оптичка влакна, коаксијални каблови као и микроталасне везе. Користећи мултиплексирање ове линије могу да се користе за истовремени пренос великог броја веза говора и података.

Да би се ефикасно искористиле телекомуникационе линије великих брзина потребно је користити неку од врста мултиплексирања. Мултиплексирање дозвољава да подаци из више извора деле (истовремено користе) велики преносни (трансмисиони) капацитет. Два најчешће коришћена начина су фреквенцијско мултиплексирање[2] (FDM)и временско мултиплексирање[3] (TDM).

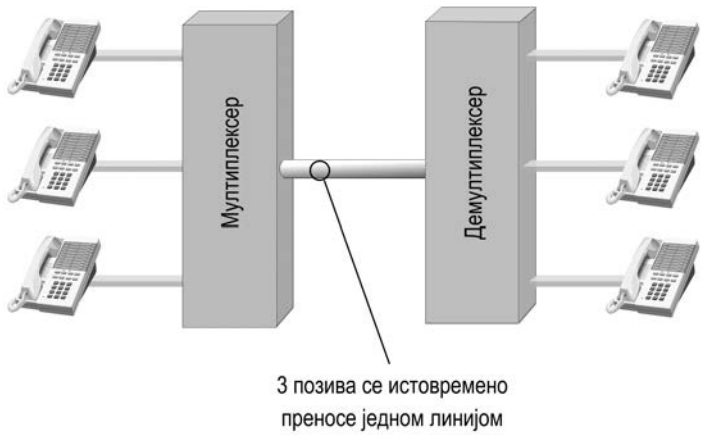
Фреквенцијски мултиплекс користи се за аналогне сигнале. Већи број сигнала преноси се истовремено истим медијумом. Сваком од сигнала додељен је други фреквенцијски опсег. Да би се фреквенцијски опсег сигнала из основног опсега померио у захтевани фреквенцијски опсег потребне су модулационе технике и уређаји за мултиплексирање који ће комбиновати модулисане сигнале.

Синхрони временски мултиплекс може се користити са дигиталним сигналима или аналогним сигналима који преносе дигиталне податке. У овој врсти мултиплексирања подаци из различитих извора преносе се у понављајућим рамовима. Сваки рам састоји се од скупа временских делова (слотова). Сваком извору додељује се један или више временских делова у оквиру рама. Ефекат који се постиже је да се из различитих извора умеђу битови података у једну целину.

Статистички временски мултиплекс омогућава генерално много ефикаснију услугу од синхроног временског мултиплекса. Код статистичког временског мултиплекса временски делови нису унапред додељени одређеним изворима података. Кориснички подаци прво се смештају у меморијски простор (бафер) а затим шаљу максималном могућом брзином користећи све неискоришћене временске делове (слотове).

На слици 8.1 приказана је функција мултиплексирања у свом најједноставнијем облику. Постоји више улаза у мултиплексер. Мултиплексер је повезан једном линијом за демултиплексер. Овом једном линијом могуће је преносити више независних канала говора и/или података. Мултиплексер комбинује (мултиплексира) сигнале из више линија и преноси их кроз линију већег капацитета. Демултиплексер прихвата мултиплексиране сигнале, одваја (демултиплексира) их за сваки од канала и испоручу-

[1] *Long distance*
[2] *Frequency Division Multiplexing*
[3] *Time Division Multiplexing*



Слика 8.1 Мултиплексирање

је ка одговарајућим излазним линијама. Широка распрострањеност мултиплексирања у преносу података може се објаснити већом ефикасношћу трансмисионих система великог капацитета, а самим тим и смањењем цене преноса података и/или говора.

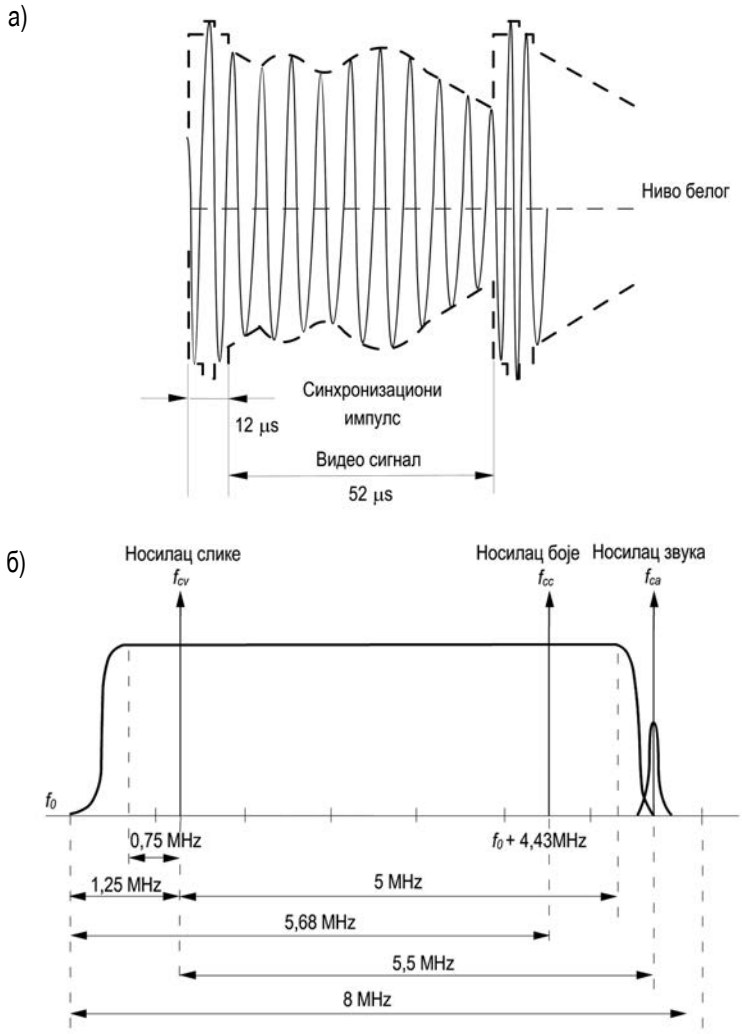
У овом поглављу анализираћемо четири врсте техника за мултиплексирање. Прва врста, фреквенцијски мултиплекс (FDM), највише се користи и најближа је онима који користе радио или телевизијске уређаје. Друга врста је временски мултиплекс (TDM) који се означава и као синхрони временски мултиплекс. Трећа врста је покушај да се побољша ефикасност синхроног TDM-а и среће се под називом статистички TDM, асинхрони TDM и интелигентни TDM. У овој књизи користићемо термин статистички TDM. Четврта врста је мултиплексирање по таласним дужинама са вишеструким приступом [1] (WDMA).

8.1 Фреквенцијски мултиплекс

Фреквенцијски мултиплекс могућ је када пропусни опсег трансмисионог медијума, који је на располагању, премашује потребе сигнала који треба да пренесемо. Велики број сигнала може се пренети истовремено уколико сваки сигнал модулише различиту носећу учестаност [2]. Носеће учестаности бирају се са међусобно довољно великим размаком, тако да не може да дође до значајног преклапања опсега сигнала. Сваки модулисани сигнал захвата одређени опсег центриран око своје носеће учестаности и он се назива канал. Да би се спречила интерференција канали су раздвојени неискоришћеним деловима спектра (чуварима).

Композитни сигнал који се преноси трансмисионим медијумом је аналогни. Треба имати на уму да улазни сигнали могу бити и дигитални и аналогни. У случају када је улазни сигнал дигиталан он мора прво да прође кроз модем [3] да би се конвертовао (претворио) у аналогни сигнал. У оба случаја сваки улазни сигнал мора се затим модулисати да би се пребацио у одговарајући фреквенцијски опсег.

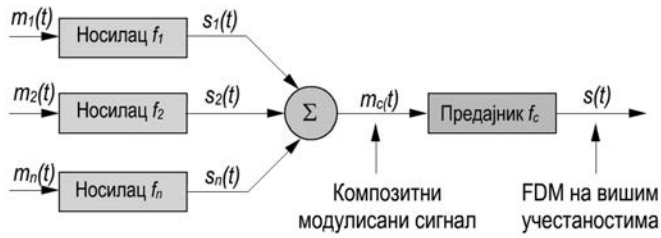
[1] *Wavelength Division Multiple Access Protocols*
[2] Погледати слику 7.16.
[3] Уређај за модулацију и демодулацију (МОдулатор - ДЕМодулатор).



Слика 8.2 ТВ сигнал: а) у временском домену б) у фреквенцијском домену

Пример фреквенцијског мултиплекса са којим се често срећемо је телевизијски сигнал. За телевизијски сигнал довољан је фреквенцијски опсег од 8MHz. На слици 8.2 представљен је ТВ сигнал у временском и фреквенцијском домену.

Црно-бели видео сигнал амплитудски модулише носилац f_{cv}. Спектар видео сигнала у основном опсегу је ширине 5MHz, а спектар АМ видео сигнала са два бочна опсега је ширине 10MHz и центриран је око учестаности f_{cv}. Да би се преносио што мањи фреквенцијски опсег АМ видео сигнала пропушта се кроз филтар, пропусник опсега, тако да је већи део доњег бочног опсега значајно ослабљен (потиснут). Спектар видео сигнала (на излазу из филтра) налази се у опсегу учестаности од f_{cv} - 1,25MHz до f_{cv}+5MHz. Посебан подносилац боје учестаности f_{cc} користи се за пренос информације о боји.



Слика 8.3 Фреквенцијски мултиплекс - предаја

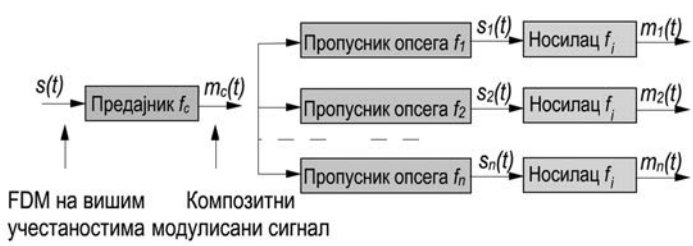
Он је довољно удаљен од учестаности носиоца сигнала слике f_{cv} да практично нема интерференције. Носилац учестаности f_{ca} је фреквенцијски модулисан аудио (тонским) сигналом и смешта се ван спектра сигнала слике. Носилац тона удаљен је од носиоца слике за 5,5MHz.

Код кабловских дистрибутивних система (КДС) од више ТВ сигнала може се направити фреквенцијски мултиплекс: сваком ТВ сигналу додељен је фреквенцијски опсег ширине 8MHz. Пошто је пропусни опсег коаксијалног кабла веома велики (до 500MHz) може се истовремено преносити велики број ТВ сигнала.

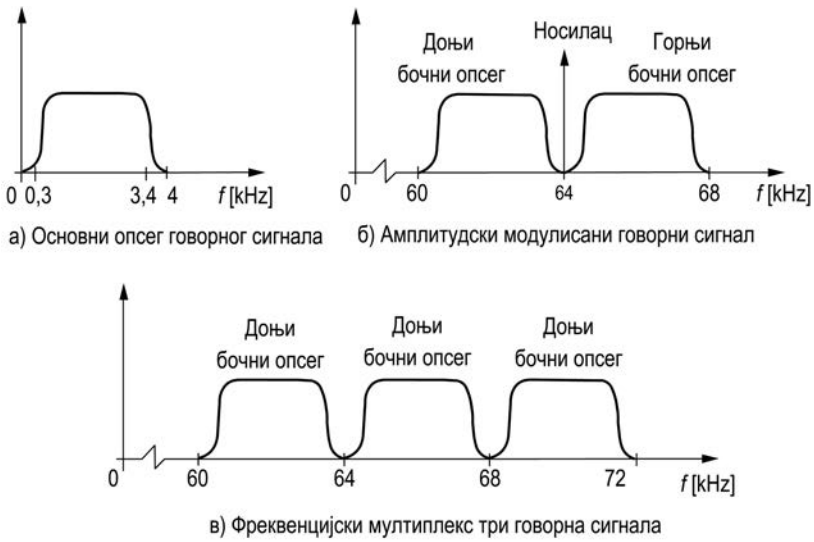
Ако се користе радио таласи може се такође направити фреквенцијски мултиплекс. Општа блок шема система за прављење фреквенцијски мултиплексираног сигнала приказана је на слици 8.3.

Уколико већи број аналогних или дигиталних сигнала [$m_j(t)$, $j = 1, n$] треба да се преноси преко истог трансмисионог медијума (мултиплексира) онда сваки од сигнала $m_i(t)$ модулише сопственог носиоца учестаности f_i. Пошто се користи више носилаца они се називају подносиоци. Може се употребити амплитудска, фазна или фреквенцијска модулација. Резултујући аналогни, модулисани, сигнали сабирају се и добија се композитни сигнал $m_c(t)$. На слици 8.5в приказан је резултантни (композитни сигнал) у фреквенцијском домену за три говорна сигнала. Спектар сигнала $m_i(t)$ померен је и центриран око учестаности носиоца f_i (слика 8.5б). Да би овај систем радио правилно учестаност носиоца f_i се мора одабрати тако да се спектри сигнала $m_i(t)$ значајно не преклапају (слика 8.5б). У противном било би немогуће извршити издвајање оригиналног сигнала. Композитни сигнал може се померати као целина користећи другу носећу учестаност.

Сигнал који се добија на излазу из фреквенцијског мултиплексера $s(t)$ има опсег B који је $B > \Sigma B_i$ (8.5б) Овај аналогни сигнал може се преносити одговарајућим трансми-



Слика 8.4 Фреквенцијски мултиплекс - пријем



Слика 8.5 Фреквенцијски мултиплекс за три говорна канала

сионим медијумом. На пријемном крају фреквенцијски модулисан сигнал се демодулише у $m_c(t)$ сигнал који се затим пропушта кроз n (на слици 8.4) филтера пропусника опсега од којих је сваки центриран око учестаности f_i и чији је пропусни опсег B_i за $1 \leq i \leq n$. На овај начин сигнал је поново раздвојен на своје компоненте. Свака од компонената се затим демодулише да би се добио оригинални сигнал.

Претпоставимо једноставан случај истовременог преноса три говорна сигнала. Као што је поменуто у претходном поглављу, узима се да је опсег говорног сигнала 4kHz при чему је његов спектар од 0,3 до 3,4kHz (слика 8.5а). Уколико се такав сигнал користи да се амплитудски модулише носилац учестаности 64kHz добија се сигнал чији је спектар приказан на слици 8.5б.

Модулисани сигнал има спектар ширине 8kHz који се простире од учестаности 60kHz до 68kHz. Да би се ефикасно искористио преносни опсег система опредељујемо се за пренос само доњег бочног опсега. Ако треба пренети три говорна сигнала, а на располагању су носиоци учестаности 64kHz, 68kHz и 72kHz добија се композитни сигнал чији је спектар приказан на слици 8.5в.

На слици се могу уочити два потенцијална проблема са којима системи са фреквенцијским мултиплексом морају да се носе. Први је преслушавање које се може појавити у спектрима суседних канала који се значајно преклапају. У случају говорног сигнала са ефективним опсегом спектра од 3,1kHz (0,3 до 3,4kHz) фреквенцијски опсег од 4kHz је задовољавајући. Спектру сигнала на излазу модема за пренос у говорном опсегу такође одговара ширина од 4kHz. Други потенцијални проблем представља интермодулациони шум (настаје због нелинеарности). На пример на дужим релацијама ефекат нелинеарности појачавача у једном каналу може да произведе фреквенцијске компоненте сигнала које одговарају неком другом каналу.

Аналогни системи за пренос

Системи за пренос сигнала у говорном опсегу у међуградском саобраћају великог су капацитета. Најстарија и за сада најчешће коришћена техника за искоришћење веза великог капацитета је фреквенцијски мултиплекс. Да би се прилагодили преносним системима великог капацитета у САД је AT&T пројектовала хијерархијску шему фреквенцијског мултиплекса. Сличан, али не и идентичан, систем у осталим земљама предложила је ITU-T (табела 8.1).

На првом нивоу хијерархије 12 говорних канала се комбинује и производи групни сигнал ширине спектра од 12*4kHz = 48kHz, који заузима фреквенцијски опсег од 60 - 108kHz. Носеће учестаности су од 64 -108kHz са размаком од 4kHz. Група за даљу надоградњу је супергрупа од 60 канала која се прави као фреквенцијски мултиплекс од пет група сигнала. У овом кораку свака група се посматра као један сигнал чији је спектар ширине 48kHz. Композитни сигнал обухвата фреквенцијски опсег од 312 - 552kHz. Остали нивои хијерархије праве се на сличан начин.

Уочимо да се сигналима говорног опсега (говор или подаци) могу вршити модулације неколико пута. На пример сигнал података може се кодирати користећи QPSK да би се добио аналогни сигнал. Добијеним сигналом се затим аналогно модулише носилац (нпр. 76kHz) и на тај начин постаје део једне групе фреквенцијског мултиплекса. Цела група модулише носилац (нпр. 516kHz) и постаје део супергрупе. Сваки од корака може да допринесе изобличењу оригиналног сигнала података.

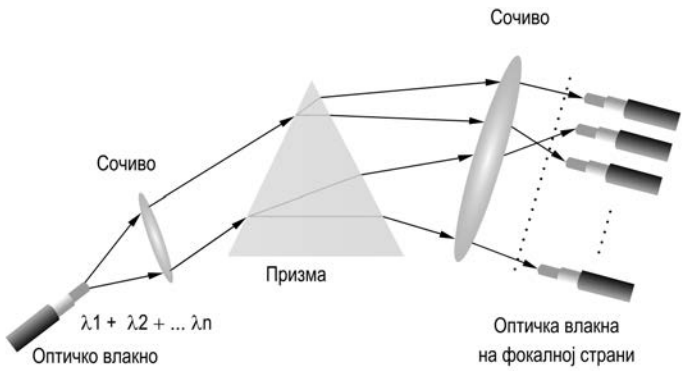
Мултиплексирање по таласним дужинама

Прави потенцијал оптичких влакана потпуно је искоришћен када је више светлосних млазева на различитим учестаностима (таласним дужинама) послато кроз исто оптичко влакно. Ово представља једну врсту фреквенцијског мултиплекса али се уобичајено назива мултиплексирање по таласним дужинама (WDMA [1]). Код мултиплексирања по таласним дужинама светлосни млаз састоји се од више боја, од којих је свака различите таласне дужине и свака носи посебан канал података.

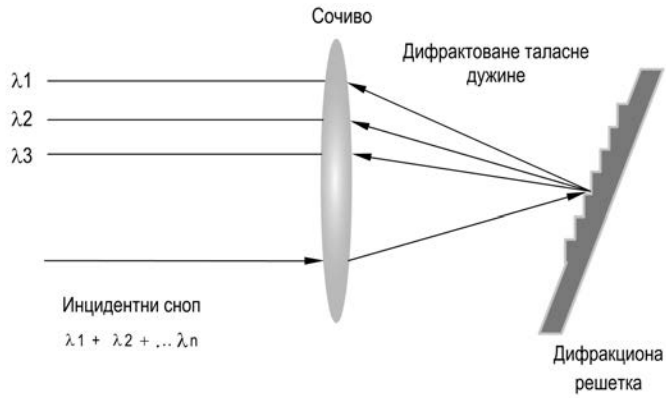
Број говорних канала	Опсег	Спектар	AT&T	ITU-T
12	48 kHz	60 - 108 kHz	Група	Група
60	240 kHz	312 - 552 kHz	Супергрупа	Супергрупа
300	1,232 MHz	812 - 2044 kHz	-	Мастергрупа
600	2,52 MHz	564 - 3084 kHz	Мастергрупа	-
900	3,872 MHz	8,516 - 12,388 MHz	-	Супермастер група
N * 600	-	-	Мултиплекс мастергрупе	-
3 600	16,984 MHz	0,564 - 17,548 MHz	Џамбогрупа	-
10 800	57,422 MHz	3,124 - 60, 566 MHz	Мултиплекс мастергрупе	-

Табела 8.1 Стандарди за фреквенцијски мултиплекс у преносним системима

[1] *Wavelength Division Multiple Access Protocols*



а) Оптички демултиплексер са призмом



б) Оптички демултиплексер са дифракционом решетком

Слика 8.6 Оптички демултиплексери

Први лабораторијски систем са мултиплексирањем по таласним дужинама је 1997. године демонстриран у Беловим лабораторијама. Представљен је са 100 светлосних млазева од којих је сваки радио на брзини од 10Gb/s са укупном брзином од 1Tb/s [1]. Данас је расположив комерцијални систем са 160 канала и сваки је брзине 10Gb/s.

Типични систем са мултиплексирањем таласне дужине има општу архитектуру сличну фреквенцијском мултиплексу. Више извора светлости формира ласерски млаз различите таласне дужине. Шаље се на мултиплексер који формира композитни млаз кроз једно влакно. Појачавачи оптичких сигнала постављени су на размаку од око десетак километара и појачавају истовремено све таласне дужине. На одредишту композитни сигнал стиже до демултиплексера где се компоненте канала одвајају и шаљу одговарајућим пријемницима (слика 8.6).

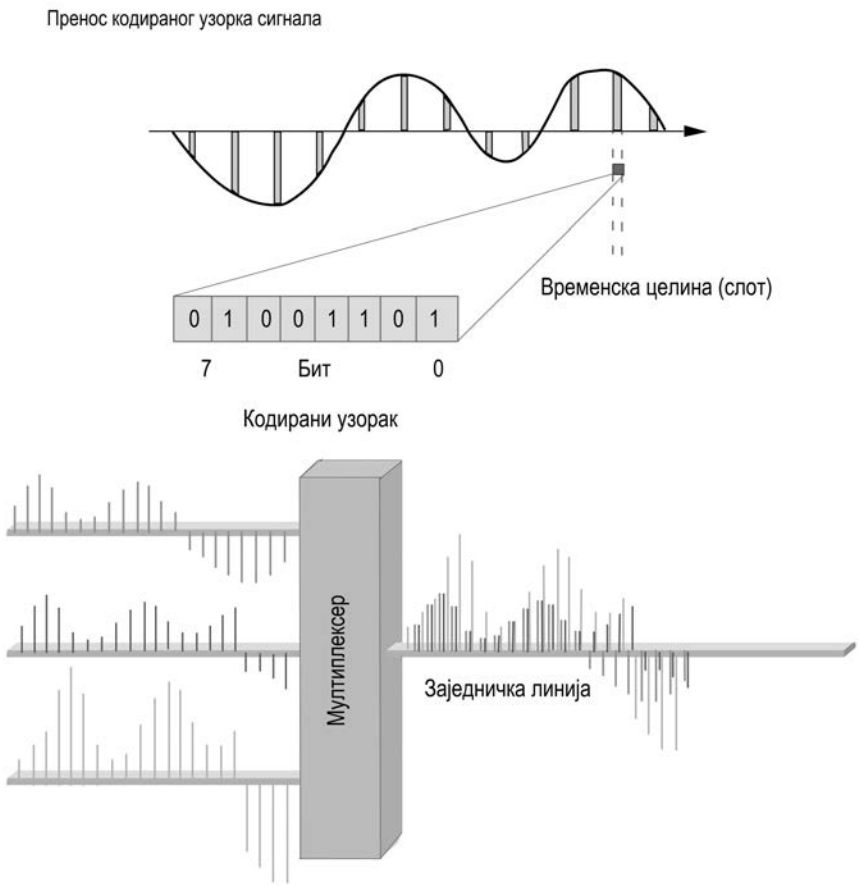
На слици 8.6а видимо систем са сочивима и призмом, а на сл. 8.6б сочиво и дифракциону решетку. Оба система на основу различитих индекса преламања и дифракције коју различите таласне дужине λ_i имају обезбеђују њихово издвајање из композитног сигнала.

[1] 1Tb/s = 10^{12}b/s

8.2 Синхрони временски мултиплекс

Синхрони временски мултиплекс користи се када брзина која се може достићи [1] преносним медијумом превазилази брзину дигиталног сигнала који треба тим медијумом пренети. Више дигиталних сигнала (или аналогних сигнала који носе дигиталне податке) може се пренети једним трансмисионим медијумом уметањем сигнала у временски слободне делове у преносу другог сигнала (слика 8.7).

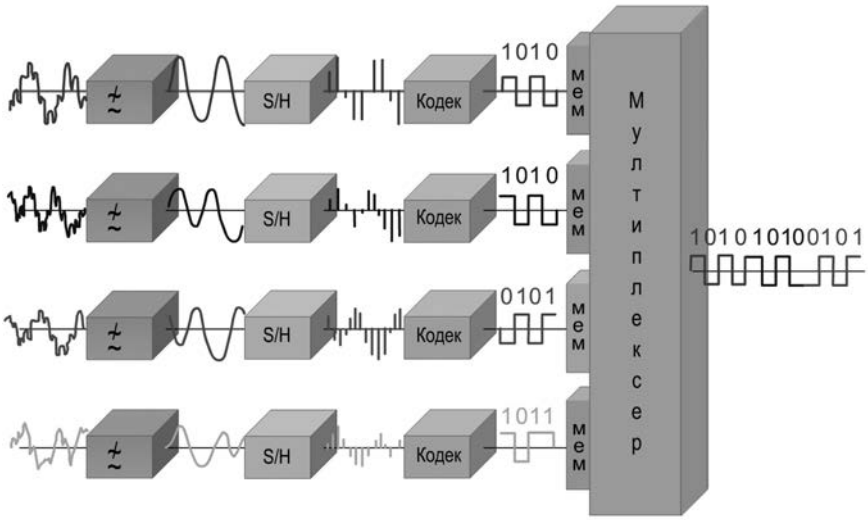
Синхрони временски мултиплекс представљен је на слици 8.8. Има четири улаза и сваки је брзине 14,4kb/s. Линија је брзине 57,6kb/s (треба додати и премашење [2]). Долазећи подаци из сваког од четири извора краткотрајно се памте у меморијском простору. Меморијски простор се секвенцијално очитава и формира композитни ди-



Слика 8.7 Пример дигитализовања сигнала и формирања временског мултиплекса

[1] Максимална брзина која се може остварити на трансмисионом медијуму је директно везна за фреквенцијски, тј. пропусни опсег тог медијума. Када посматрамо сигнале које преносимо у временском домену онда посматрамо капацитет трансмисионог медијума. Када сигнал који преносимо посматрамо у фреквенцијском домену онда говоримо о пропусном тј. фреквенцијском опсегу трансмисионог медијума.

[2] *Overhead* - поред корисних дигитални података потребни су и додатни подаци о синхронизацији, раздвајању итд. Ти додатни „некорисни" подаци називају се премашење.



Слика 8.8 Синхрони временски мултиплекс: филтрирање, одмеравање, кодирање, и мултиплексирање

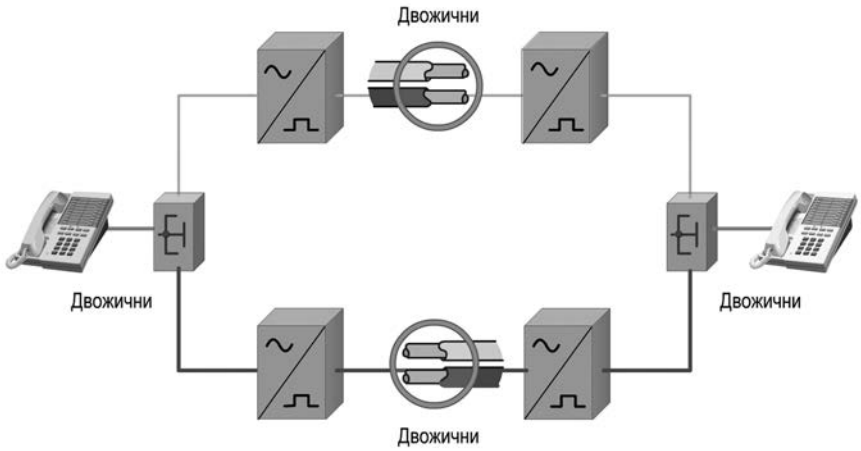
гитални сигнал. Операција ишчитавања треба да буде довољно брза да би меморијски простор био испражњен (очитан) пре него што се нови подаци појаве. Брзина композитног сигнала мора да је најмање једнака брзини збира појединачних сигнала. Дигитални сигнал се преноси директно или преко модема као аналогни сигнал.

Подаци су организовани у рамове. Сваки рам садржи циклусе временских целина (слотова). У сваком раму једна или више временских целина додељена је одговарајућем извору података. Секвенца временских целина која припада једном извору назива се канал. Подаци из сваког канала пре прослеђивања на линију привремено се складиште у меморијском простору мултиплексера.

Синхрони временски мултиплекс назива се „синхрони" због тога што су канали (секвенце временских целина) унапред додељене појединим изворима података и не мењају се у току рада. Уколико извор података нема шта да пошаље канал је њему и даље додељен али неискоришћен. Овај принцип примењен је и код фреквенцијског мултиплексирања.

ITU-T			AT&T		
Ниво	**Број говорних канала**	**Брзина [Mb/s]**	**Ниво**	**Број. говорних канала**	**Брзина [Mb/s]**
E-1	30	2048	DS-1	24	1,544
E-2	120	8,448	DS-1C	48	3,152
E-3	480	34,368	DS-2	96	6312
E-4	1920	139,264	DS-3	672	44,736
E-5	7680	565,148	DS-4	4032	274,176

Табела 8.2 Стандарди за временски мултиплекс



Слика 8.9 Четворожични PCM преносни систем

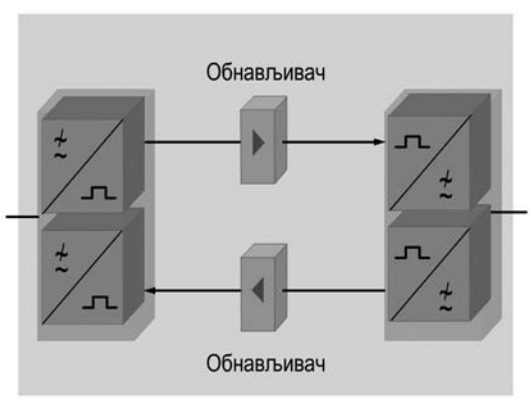
Дигитални системи за пренос

Системи за пренос дигиталних сигнала на великим растојањима пројектовани су тако да преносе сигнале говорног опсега преко преносних линија великог капацитета, као што су оптичка влакна, коаксијални каблови и микроталаси. Део прелаза телекомуникационих система ка дигиталним системима последица је примене и прилагођавања структуре синхроних временских мултиплекса.

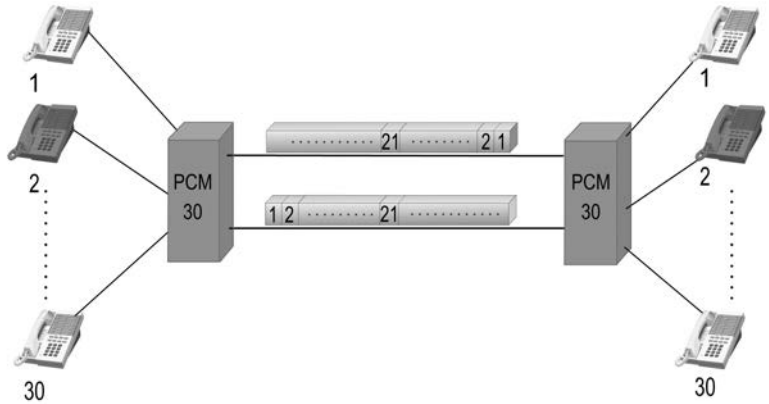
У САД, Канади и Јапану примењена је хијерархијска шема коју је развила AT&T. Остале државе користе ITU-T предлог који је сличан али не и идентичан. У табели 8.2 приказане су обе хијерархијске шеме.

У преносним системима са временским мултиплексом (нпр. E1 типа) за сваки од праваца постоји посебан канал (нпр. пар жица). То значи да припадају четворожичним преносним системима (слика 8.9).

На сваком од крајева дигиталних преносних система налазе се јединице за мултиплексирање/демултиплексирање. Оне се састоје од предајника и пријемника. Предајник формира осмобитну дигиталну PCM кодирану поворку за пренос. Прије-



Слика 8.10 Општи модел дигиталног преносног система

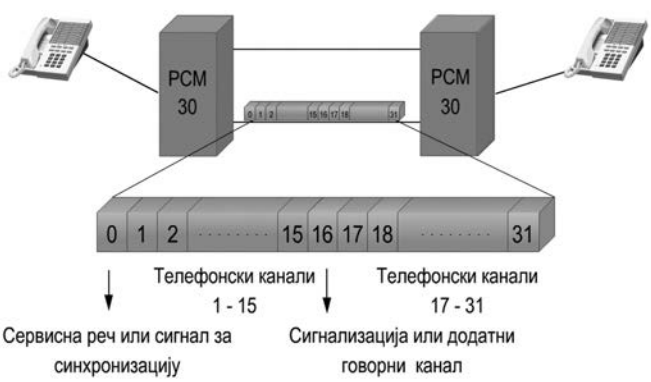


Слика 8.11 Преносни систем E1

мник претвара примљену дигиталну поворку у аналогни сигнал. У преносу долази до изобличења сигнала па се обнављивачи постављају на одређеном растојању[1] (слика 8.10).

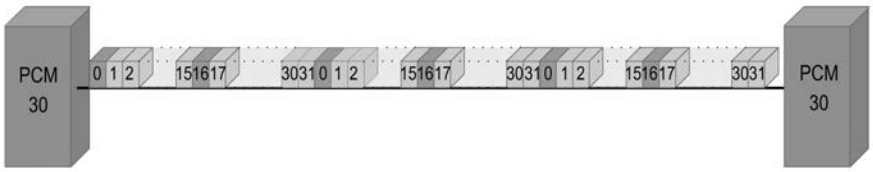
Основ временске хијерархије у Европи је E1 систем[2]. Он обезбеђује истовремени пренос 30 говорних позива, синхронизацију и сигнализацију[3]. Као што је већ наглашено, потребан је по један пар жица за сваки правац. Позив између два корисника захтева по једну временску целину у сваком правцу. Долазећи и одлазећи позиви увек користе исти број временске целине (слика 8.11). Рам E1 (PCM30) састоји се од 32 временске целине, од којих се за пренос говора користе 1-15 и 17-31 (слика 8.12).

У временској целини 0 наизменично се преносе сервисна реч (SW[4]) и сигнал за синхронизацију (FAS[5]). Временска целина 16 користи се за сигнализацију или као до-



Слика 8.12 Рам E1 система

[1] Међусобни размак рипитера (обнављивача) зависи од врсте употребљеног трансмисионог медијума - бакарних парица, коаксијалних каблова, оптичких влакана или микроталаса.
[2] Среће се и под ознаком PCM30 у Европи, односно PCM24 у САД.
[3] Укупно то чини 32 канала, тако да се 30 у ознаци PCM30 односи на број говорних канала, а не на укупан број канала.
[4] *Service Word*
[5] *Frame Alignment Signal*



Слика 8.13 Пренос E1 рамова

датни говорни канал. Рамови се преносе један за другим (слика 8.13). Сигнал који се користи за синхронизацију предајника и пријемника увек има исти распоред битова (слика 8.14).

Распоред битова у сервисној речи приказан је на слици 8.15. У сервисној речи се на пример трећи бит поставља на 1 у случају хитног упозорења.

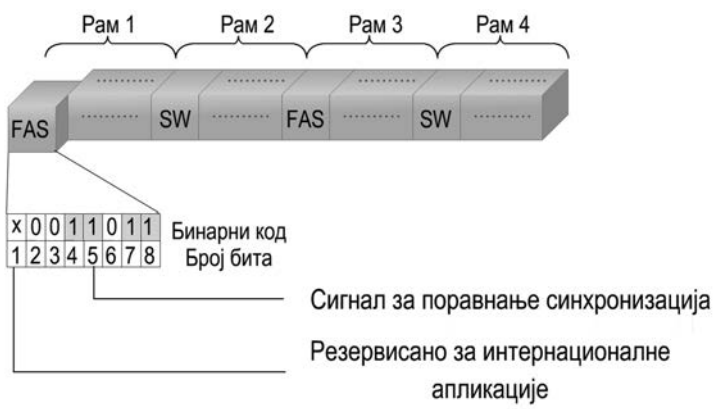
Из табеле 8.2 види се да се дигитални преносни системи великог капацитета добијају комбиновањем дигиталних система мањег капацитета (слика 8.16).

У меморију мултиплексера циклично се уписују подаци из 32-каналног система (2Mb/s). Четири канала уписују се брзином од 2MHz а ишчитавају брзином од 8MHz (слика 8.17).

Интерфејси за пренос оптичким влакнима

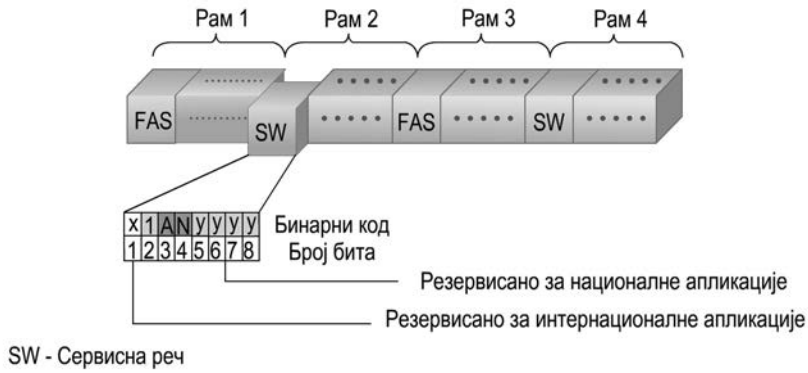
Синхрону оптичку мрежу (SONET[1]) је прво предложио BellCore а касније је стандардизовала организација ANSI. Одговарајућа верзија коју је предложила организација ITU-T[2] је синхрона дигитална хијерархија (SDH[3]). Интерфејси за пренос оптичким влакнима (SDH, SONET) имају за циљ да обезбеде коришћење свих предности дигиталних преносних система са оптичким влакнима.

Спецификација SONET дефинише хијерархију за стандардизоване брзине дигиталних података (табела 8.3). Најнижи ниво, означен са STS-1[4] или OC-1[5], је бр-



Слика 8.14 Сигнал за синхронизацију (FAS)

[1] *Synchronous Optical Network*
[2] Препорука - *Recommendation G.707*
[3] *Synchronous Digital Network*
[4] *Synchronous Transport Signal level 1*
[5] *Optical Carrier level*



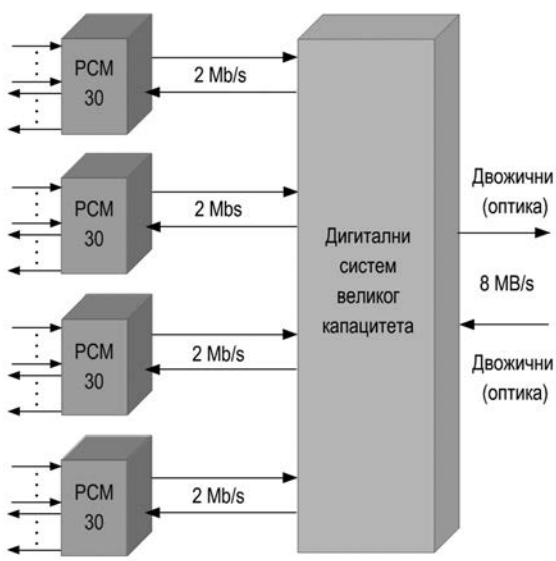
Слика 8.15 Сервисна реч (SW) у E1 систему

зине 51,84Mb/s. Ова брзина може се користити за пренос једног DS3 сигнала или групе сигнала нижег нивоа хијерархије као што су DS-1, DS-1C, DS-2 или брзине ITU-T (2,048Mb/s). Више STS-1 (односно STM-0) сигнала може се комбиновати да сачини STS-N (тј. сигнал STM-N).

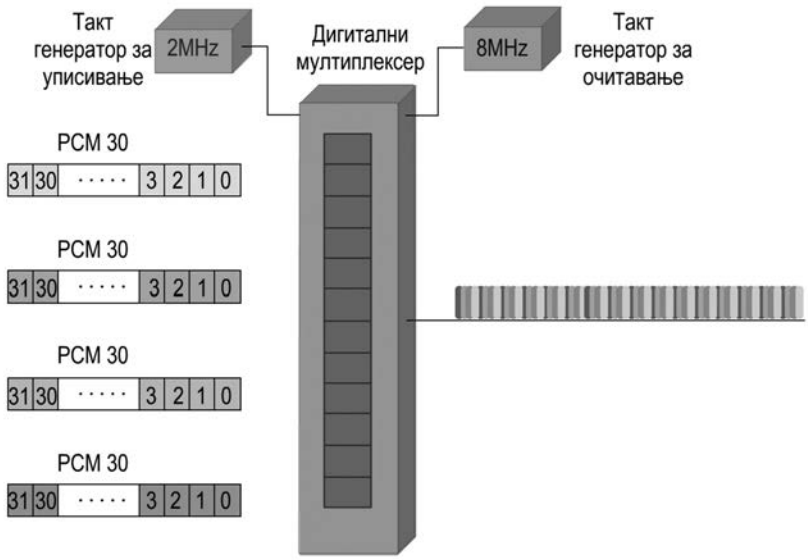
8.3 Статистички временски мултиплекс

Код синхроног временског мултиплекса може се десити у општем случају да су многе временске целине неискоришћене. Типична примена временског мултиплекса била би веза терминала са дељеним рачунарским портом. Иако би већи део времена терминали били у употреби не постоји пренос података код сваког терминала.

Друга врста временског мултиплекса је статистички мултиплекс. Статистички мултиплекс испитује карактеристике података који се преносе и динамички додељује вре-



Слика 8.16 Формирање сигнала код E2 дигиталног преносног система

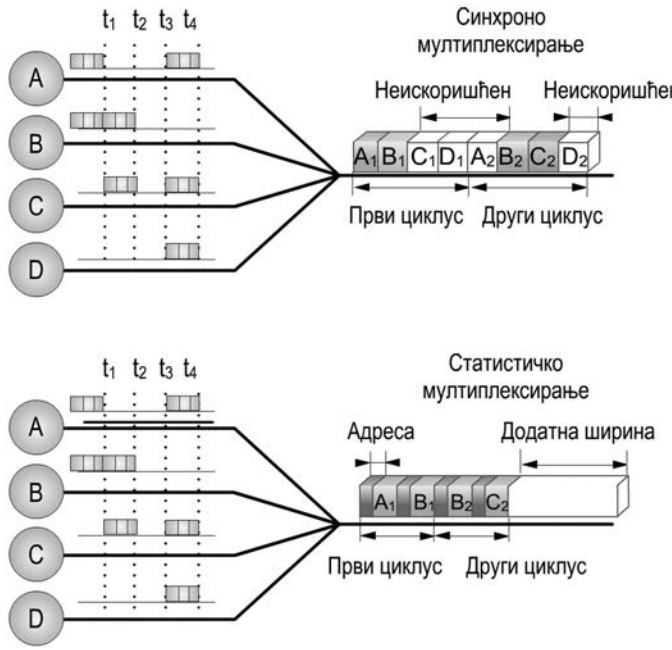


Слика 8.17 Уписивање и очитавање у E2 систему

менске целине само ако се захтева пренос. Као и код синхроног временског мултиплекса статистички мултиплекс има већи број улазно/излазних линија на једној страни и мултиплексирану линију велике брзине на другој страни. Свака од линија има свој меморијски простор - бафер. У случају статистичког мултиплексера постоји n улазно/излазних линија али је само k временских целина где је $k < n$ на располагању временском мултиплексу. Са стране улаза задатак мултиплексера је да прегледа улазни меморијски простор и очитава јединице података. На излазу мултиплексер прима рам и про-

ITU-T	SONET	Брзина података	Брзина корисних података
STM - 0	STS-1/OC-1	51,84 Mb/s	50,112 Mb/s
STM - 1	STS-3/OC-3	155,52 Mb/s	150,336 Mb/s
	STS-9/OC-9	466,56 Mb/s	451,008 Mb/s
STM -4	STS-12/OC-12	622,08 Mb/s	601,344 Mb/s
	STS-18/OC-18	933,12 Mb/s	902,01 Mb/s
	STS-24/OC-24	1,24416 Gb/s	1,202688 Gb/s
	STS-36/OC-36	1,86624 Gb/s	1,804032 Gb/s
STM -16	STS-48/OC-48	2,48832 Gb/s	2,405376 Gb/s
	STS-96/OC-96	4,87664 Gb/s	4,810752 Gb/s
STM - 64	STS-192/OC-192	9,95328 Gb/s	9,621504 Gb/s
STM - 256	STS-768	39,81312 Gb/s	38,486016 Gb/s
STM - 3072		159,25248 Gb/s	153,944064 Gb/s

Табела 8.3 Хијерархија SDH/SONET



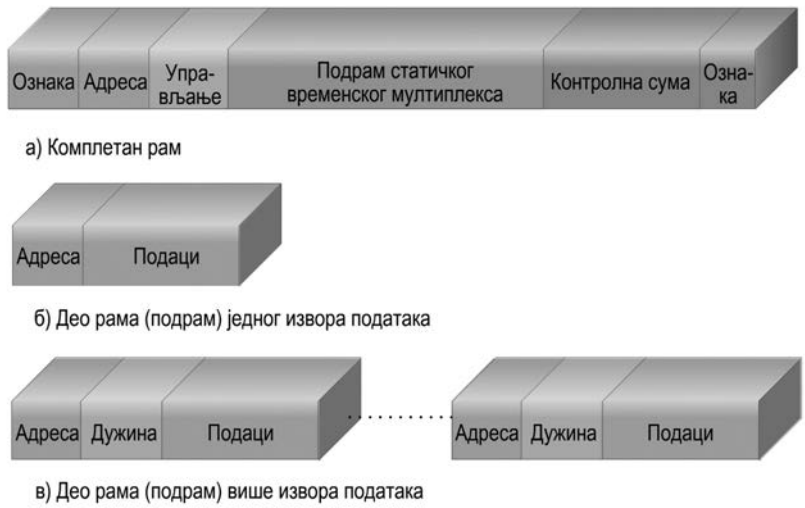
Слика 8.18 Поређење статистичког и синхроног мултиплексирања

слеђује податке из временских целина у одговарајући излазни меморијски простор (погледати слику 8.8).

Пошто статистички временски мултиплекс користи чињеницу да прикључени уређаји не шаљу податке све време, брзина на преносној линији је мања него збир брзина прикључених уређаја. Тако статистички мултиплексер може да користи мању брзину података на мултиплексираној линији од синхроног временског мултиплексера за исти број прикључених уређаја. На слици 8.18 приказана је разлика статистичког и синхроног временског мултиплексирања. На слици су приказана четири извора података који шаљу јединице података у времену t_1, t_2, t_3, t_4. У случају синхроног мултиплексирања на излазу из мултиплексера брзина ће бити једнака четворострукој брзини улазних уређаја. У сваком тренутку t_1, t_2, t_3, t_4 подаци се узимају са улазних уређаја и шаљу на линију. На пример може да се деси да уређаји C и D немају податке за слање. Онда ће две од четири временске целине да буду неискоришћене (празне, без података).

С друге стране статистички мултиплексер не шаље празне временске целине ако било који од улазних уређаја има податке за слање. У првом тренутку шаљу се само подаци у временским целинама A и B. Види се да не постоји додељивање временских целина по њиховој позицији. Због тога је потребно увести адресирање да би се обезбедила правилна испорука података. На тај начин се корисним подацима морају додати и некорисни подаци (премашења) намењени адресирању.

Формат рама који користи статистички мултиплексер има утицаја на перформансе система. Наравно пожељно је минимизирати премашење да би се пропусна моћ



Слика 8.19 Формат рама статистичког мултиплексера

система побољшала. Статистички мултиплексер користиће синхрони протокол као што је HDLC [1]. У оквиру HDLC рама део за податке мора да садржи и управљачке битове за мултиплексирање. На слици 8.19 приказани су могући формати. У првом случају само један извор података укључен је у рам. Извор података је одређен адресом. Дужина поља података је променљива и његов крај је означен крајем комплетног рама. Овај начин може се применити када саобраћај није великог интензитета, али је неефикасан при саобраћају већег интензитета.

Начин да се повећа ефикасност је да се дозволи да се подаци из више извора смештају (пакују) у један рам. У том случају потребна је ознака да би указала на дужину података сваког од извора. Тако се део статистичког рама (подрам) састоји од секвенце поља за податке. Свако од поља означено је својом адресом и дужином.

Локалне рачунарске мреже са оптичким влакнима

Код локалних рачунарских мрежа са оптичким влакнима често се користи мултиплексирање по таласним дужинама. Више комуникационих веза остварује се истовремено на различитим таласним дужинама.

Једноставан начин да се направи локална рачунарска мрежа са оптичким влакнима јесте употреба пасивне компоненте која повезује станице. У ствари, два оптичка влакна из сваке станице повезана су у стаклени цилиндар. Једно оптичко влакно је улаз цилиндра, а друго излаз из цилиндра. Светлосни излаз било које станице осветљава цилиндар, и то могу детектовати све остале станице. Да би се омогућио истовремени вишеструки пренос спектар је подељен у канале (опсеге таласних дужина [2]), као што је приказано на слици 8.20. У овом протоколу (WDMA [3]), свакој станици додељују се два канала. Ускопојасни ка-

[1] Протокол слоја везе HDLC (*High Level Data Link Control)* развила је интернационална организцаија ISO (*International Stanadard Organisation).*

[2] Ово је у ствари такође фреквенцијски мултиплекс. У оптици се говори о таласним дужинама.

[3] *Wavelength Division Multiplex Access* - приступ са мултиплексирањем по таласним дужинама.

Слика 8.20 Приступ са мултиплексирањем по таласним дужинама (WDMA)

нал се користи као управљачки канал за обавештавање станице, а широкопојасни канал се користи за слање података (рамова).

Сваки канал је подељен на групе временских целина, као што је приказано на слици 8.20. Сви су канали синхронисани заједничким такт сигналом.

Протокол подржава три класе:

- саобраћај са успоставом везе са константном брзином података,
- саобраћај са успоставом везе променљивог интензитета,
- саобраћај без успоставе везе (датаграм типа).

У случају протокола са успоставом везе идеја је да када станица 1 (C_1) хоће да комуницира са станицом 2 (C_2), мора прво да пошаље рам „захтев за успоставом везе"[1] у слободан временски сегмент управљачког канала станице C_2. Уколико станица C_2 прихвата везу комуникација може да се одвија у оквиру канала података станице C_1. Свака станица има два предајника и два пријемника:

- пријемник фиксне таласне дужине за пријем са сопственог управљачког канала,
- променљиви предајник који може да мења предајну таласну дужину за слање по управљачком каналу других станица,
- предајник фиксне таласне дужине за слање података,
- променљиви пријемник који може да се прилагоди таласној дужини различитих предајника канала података.

Свака станица ослушкује сопствени канал за долазеће позиве и потребно је да се подеси на таласну дужину предајника. Данас се користи велики број WDMA протокола. Неки од њих имају само један управљачки канал, неки имају више управљачких канала. Неки укључују време пропагације, други не, итд. Када је велика густина носилаца различитих таласних дужина систем се означава као DWDM[2] .

[1] *Connection Request*

[2] *Dense Wavelength Division Multiplexing* - мултиплексирање са великом густином таласних дужина

9. Модеми

Уређаји који су се до сада највише користили за међусобно повезивање рачунара јесу модеми. У овом поглављу обрадићемо модеме за телефонски канал, модеме за дигиталне претплатничке петље и кабловске модеме.

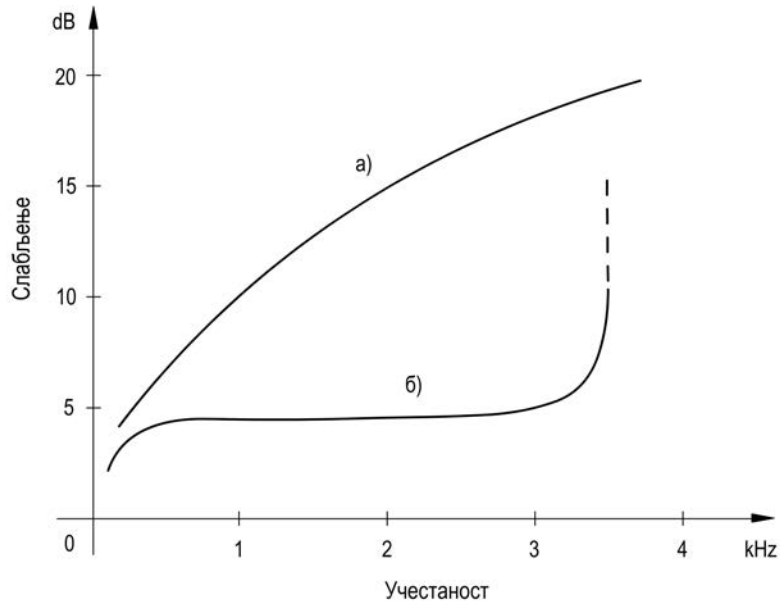
9.1 Телефонска мрежа

Телефонија је стара више од једног века али млађа од телеграфије, тако да би се могло рећи и да је аналогни пренос млађи од дигиталног. У телефонској мрежи[1] претплатници су повезивани са телефонским централама бакарним парицама а и локалне централе међусобно су повезане на исти начин (слика 9.1). Средишње и међуградске централе биле су повезиване, уз коришћење фреквенцијског мултиплекса, коаксијалним кабловима или радио-релејним везама, а данас махом оптичким влакнима. Главне компоненте јавне телефонске мреже представљају:

- локална претплатничка петља (ЛП) која је веза између крајњег корисника и локалног комутационог центра,

Слика 9.1 Основна инфраструктура јавне телефонске мреже (JTM)

[1] Код нас се користи термин јавна телефонска мрежа а у САД се означава са PSTN (*Public Switched Telephone Network*).
[2] ISP (*Internet Service Provider*)



Слика 9.2. Слабљење а) непупинизоване б) пупинизоване парице

- локални комутациони центар ЛК који омогућава успостављање телефонских позива корисницима који су за њега повезани преко локалне претплатничке петље. Пошто локалне петље у највећем делу још увек преносе аналогне сигнале, и релативно су мале раздаљине међу њима, често се у литератури називају „последња миља" телефонског система;
- комутациони центри за међуградски саобраћај, или за саобраћај између локалних комутационих центара (тандем), који омогућавају преусмеравање (комутацију) позива који није у области локалног комутационог центра.

Да би се повећао домет у оквиру градских мрежа често је вршена „пупинизација", тј. уметање концентрисаних индуктивности (калемова) на одређеним растојањима.

Стандардизовани, фреквенцијски опсег телефонског канала је на учестаности од 0,3 до 3,4kHz, довољан да се на пријему добије разумљив говор [1]. При филтрирању говора није се водило рачуна о фазним изобличењима, јер је ухо на њих практично неосетљиво. Иако застарела, постојећа инфраструктура и даље је широм света у употреби. Телефонски канал је и данас нека врста стандардне јединице, па се може казати „капацитет је 900 телефонских канала". Развој дигиталних телекомуникација омогућио је економичну употребу дигиталних комутационих центара („централа") у којима би аналогни говорни сигнал најпре био дигитализован, па онда комутиран и након тога опет евентуално враћен у аналогни облик. На тај начин једна телефонска веза успостављена бирањем (комутирањем [2]) може да се састоји од низа аналогних и дигиталних деоница од којих свака има своје посебне карактеристике.

[1] Одељак 3.1.
[2] Друга варијанта била би изнајмљена линија.

9.2 Модеми за телефонски канал

Пошто је опсег телефонског канала почевши од комутационог центра ограничен, за пренос података потребно је спектар преношеног сигнала сместити у тај опсег. Због тога се мора користити нека врста модулације, а за то користимо модеме. Подаци које треба пренети дигитални су по својој природи. Телефонска мрежа је пројектована за пренос говорног сигнала. Користи се дигитална модулација и генерише еквивалентан аналогни сигнал који се у оквиру преноса кроз телефонску мрежу третира као аналогни. У комутационим центрима и при преносу овај се модемски сигнал дигитализује вршећи А/Д [1] и Д/А конверзије једанпут или више пута. На крају се, у аналогном облику, враћа пријемном модему који га сада демодулише и дигиталне податке доставља кориснику. Узимајући у обзир да је ширина опсега говорног канала од 3 до 3,5kHz добија се да је капацитет [2] у опсегу од 30 до 33kb/s за однос сигнал-шум 30dB, односно у опсегу од 35 до 38,5kb/s за однос сигнал/шум 33dB. Парице у приступној мрежи (локалној претплатничкој петљи) имају далеко већи капацитет од телефонског канала. Ту је однос сигнал-основни шум око 50 до 60dB. Расположиви опсег веома је широк али слабљење у њему није константно, као што је претпостављено при одређивању капацитета телефонског канала. Ови капацитети могу се користити када се примењују xDSL [3] технологије.

Развој модема зависио је у великој мери од расположиве технологије а најбоље се може пратити кроз одговарајуће ITU-T препоруке серије V [4]. Да бисмо остварили компатибилност модема различитих произвођача неопходно је било стандардизовати саме протоколе. Тако су развијени стандарди који дефинишу модулацију, компресију података, корекцију грешке и компатибилност са ранијим стандардима.

Кратак опис неких од стандарда:

- Стандард V.32 - обезбеђује синхрони/асинхрони пренос података, дуплексни пренос преко двожичних комутираних или изнајмљених телефонских линија са бинарним протоком до 9600b/s, 7200b/s и 4800b/s. Први универзални стандард за модеме бинарног протока до 9600b/s на комутираним и изнајмљеним телефонским линијама је V.32. Модеми „типа V.32" раде тако што покушавају да успоставе везу на 9600b/s, ако се појаве грешке враћају се и раде на 2400b/s. Могу користити протоколе за компресију података и контролу грешака. Овај стандард компатибилан је са стандардом V.22bis организације ITU-T;
- Стандард V.32bis - модеми који одговарају овом стандарду омогућавају синхрони/асинхрони дуплексни пренос података преко двожичних комутираних или изнајмљених линија, бинарно протока 14400b/s, 12000b/s, 9600b/s, 7200b/s, 4800b/s. Модеми V.32bis интензивније анализирају везу да би од-

[1] А/Д - аналогно/дигитална конверзија

[2] Према Шенноновој теореми о каналном кодовању капацитет је максимална брзина преноса (проток) при којој се вероватноћа грешке може држати под контролом. Она зависи од расположивог фреквенцијског опсега и односа сигнал-шум (погледати одељак 3.4).

[3] *Digital Subscriber Line* - дигитална претплатничка петља. У одељку 9.3 биће детаљније речи о овој технологији.

[4] Пренос података телефонском мрежом.

Стандард	Бинарни проток [b/s]	Линијска брзина [Bd]	Компресија података	Модулација	Тип везе	Остале карактеристике
V.90	56000[1] 28800[2]	3200, 3000, 2400, 2743, 2800, 3429	V.42bis MNP5	2^9QAM[3] TCM[4,5]	Комутирана, двожична изнајмљена	Дуплекс или полудуплекс, раздвајање канала поништавањем еха, адаптивна техника за аутоматско одређивање једног од протока, помоћни канал 200b/s
V.34	28800 33600	3200, 3000, 2400, 2743, 2800, 3429	V.42bis MNP5	2^9QAM TCM	Комутирана, двожична изнајмљена	Дуплекс или полудуплекс, раздвајање канала поништавањем еха, адаптивна техника за аутоматско одређивање једног од протока, помоћни канал 200b/s
V.32ter[6]	19 200	2400	V.42bis MNP5	2^8QAM TCM	Комутирана, двожична изнајмљена	Дуплекс, раздвајање канала поништавањем еха, скрембловање, адаптивни еквализатор
V.32bis[7]	14400	2400	V.42bis MNP5	2^6QAM TCM	Комутирана, двожична изнајмљена	Дуплекс, раздвајање канала поништавањем еха, скрембловање, адаптивни еквализатор
V.32	9600	2400	V.42bis MNP5	2^4QAM TCM	Комутирана, двожична изнајмљена	Дуплекс, раздвајање канала поништавањем еха, скрембловање, адаптивни еквализатор, смањење протока на 4800b/s
V.29	9600	2400	V.42bis MNP5	Комбиација AM и DPSK	Изнајмљена четворожична	Смањење протока на 7200 и 4800b/s, аутоматски адаптивни еквализатор, мултиплексирање сигнала мањих протока, скрембловање
V.27ter	4800 2400	1200 600	V.42bis MNP5	8DPSK	Комутирана	Повратни канал за контролу грешака - 75Bd, аутоматски адаптивни еквализатор
V.27bis	4800 2400	1200 600	V.42bis MNP5	8DPSK	Изнајмљена четворожична или двожична	Дуплекс или полудуплекс, повратни канал за контролу грешака 75Bd, аутоматски адаптивни еквализатор

[1] Брзина у директном каналу (*Up Link*)
[2] Брзина у повратном каналу (*Down Link*)
[3] Модулација у директном каналу
[4] Трелис кодирање (*Trellis Coded Modulation*)
[5] Модулација у повратном каналу
[6] Наставак „ter" обележава трећи стандард објављен од стране истог одбора.
[7] Наставак „bis" обележава други стандард објављен од стране тог одбора.

Стандард	Бинарни проток [b/s]	Линијска брзина [Bd]	Компресија података	Модулација	Тип везе	Остале карактеристике
V.26ter[1]	2400	2400	V.42bis MNP5	DPSK	Комутирана, двожична изнајмљена	Дуплекс, раздвајање канала поништавањем еха, скрембловање, адаптивни или компромисни еквализатор
V.26bis[2]	2400 1200	600	V.42bis MNP5	4DPSK	Комутирана	Повратни канал за контролу грешака 75Bd
V.23	600/1200	600 1200	V.42bis MNP5	FSK	Комутирана	Синхроно и асинхроно, повратни канал за контролу грешака 75Bd
V.22bis	2400	600	V.42bis MNP5	4QAM TCM		Повратни канал за контролу грешака 75Bd
V.22	1200	1200		DPSK	Комутирана, двожична изнајмљена	Дуплекс, скрембловање, синхроно и асинхроно
V.21	<300	300		FSK	Комутирана	Дуплекс, асинхроно

Табела 9.1 Модемски стандарди

мах установили највећу могућу брзину модулације (линијску брзину). Могу користити протоколе за компресију података и контролу грешака;

- Стандард V.33 - модеми који одговарају овом стандарду омогућавају синхрони дуплексни пренос података преко четворожичних изнајмљених линија брзинама 14400b/s, 12000b/s и 9600b/s;
- Стандард V.FASAT - модеми који одговарају овом стандарду омогућавају синхрони пренос података брзинама од 19200b/s са могућношћу рада и конфигурисања брзине.

Стандард V.34

Један од новијих стандарда за аналогне модеме је V.34. Омогућава синхрони/асинхрони дуплексни пренос података преко двожичних комутираних линија и двожичних или четворожичних изнајмљених линија брзином од 33600b/s. Важно је напоменути - да би се повећала брзина преноса стандарди за модулацију су се мењали, али су стандарди за компресију података и корекцију грешке остали исти.

Да би се добила оваква брзина преноса преко комутираних линија променљивог квалитета стандард V.34 увео је велики број техничких иновација. Укупан ефект техничке иновације је тај да је V.34 модем способнији од било ког старијег стандарда да се прилагоди променљивим условима линија да би се оптимизовао пренос података.

Табела 9.2 резимира техничке иновације које су уведене са V.34 стандардом и њихов значај и примену (утицај). Иако се све иновације наведене у табели сматрају делом стандарда V.34, не треба претпоставити да су све од њих укључене у сваки V.34 модем. Још неколико опција које могу, а не морају, бити подржане у неком

[1] Наставак „ter" обележава трећи стандард објављен од стране истог одбора.
[2] Наставак „bis" обележава други стандард објављен од стране тог одбора

V.34 модему су следеће:

- подршка изнајмљених као и комутираних линија,
- четворожичне и двожичне линије,
- заштита употребом шифре и повратна заштита,
- могућност повезивања fax уређаја преко V.17FAX стандарда,
- могућност аутоматског бирања преко V.25bis стандарда.

Стандард V.90

Велики део телефонске мреже је дигитализован имајући у виду пренос говорног сигнала. Уведена је PCM уз одговарајућу μ или A карактеристику компресије са 8000 узорака у секунди, где је сваки узорак представљен кодном речи од 8 бита, па је ка-

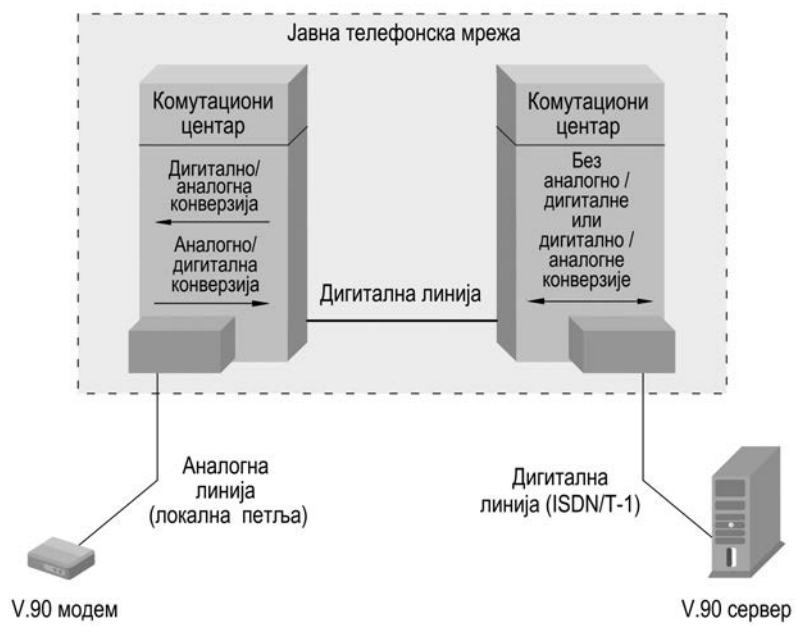
V.34 техничка иновација	Значај/ Примена
Вишеструке линијске брзине[1] / фреквенције носиоца[2]	V.34 стандард прописује три неопходне линијске брзине (3200, 3000, 2400) и три опционе (3429, 2800, 2743). Ово повећава прилагодљивост V.34 модема различитим условима линија. Свака брзина подржава две различите носеће учестаности да би се оптимизовала брзина преноса на комутираним линијама променљивог квалитета.
Линијска брзина је већа од 2400	V.34 стандард је први покушај да се достигне линијска брзина која је већа од 2400. Бинарни проток од 28,8 kb/s добијена је тако што линијска брзине 320Bd „носи" 9 бита, док је бинарни проток од 33,6 kb/s добијен тако што сигнал линијске брзине 2800Bd „носи" 12 бита.
Помоћни канал за управљање	Помоћни канал, који је одвојен од канала за пренос података, намењен је за пренос управљачких података или за конфигурисање система. Овај канал посебно је значајан у случајевима када је V.34 модем повезан са рутером или неким сличним уређајем за међуповезивање који може захтевати надгледање или управљање, без ометања преноса података.
Асиметричан пренос	Неке апликације као што су упити база података или учитавање са Интернет страница могу захтевати већи пропусни опсег само у једном правцу. V.34 одређује метод за доделу података са већим пропусним опсегом у једном правцу него у другом.
Испитивање прилагодљивости линија	Испитивање прилагодљивости линија тестира особине линија за пренос не само за време успостављања везе, већ и за време преноса. Брзина преноса сигнала, фреквенција носиоца и други параметри могу се мењати да би се оптимизовала бинарни проток.
Поновно кодирање и нелинеарно кодирање	Смањује високофреквентни линијски шум и повећава отпорност на сметње које настају током A/Д конверзије.
Промена брзине смањење[3] / повећање[4]	Иако многи стандарди за модеме подржавају смањење брзине, V.34 подржава и повећање брзине преноса са побољшањем линијских услова.
Трелис кодирање	Методологија FEC[5] исправљања грешке која омогућава веће брзине преноса сигнала телефонским линијама са шумом.
V.8	Омогућава да модеми који подржавају V.8 брже поставе и иницијализују позив, у односу на модеме који не подржавају V.8.

Табела 9.2 Техничке иновације V.34

[1] *Baud rate*
[2] *Carrier frequencies*
[3] *Fallback*
[4] *Fallforward*
[5] *Forward Error Correction* - корекција грешке унапред (детаљније у 10. поглављу).

нални проток 64kb/s. И комутациони центри су дигитални па се аналогни пренос врши углавном још само бакарним парицама од комутационог центра до претплатника. Изгледало је да је у преносу података кроз телефонске канале достигнут врхунац и да је V.34 последњи модем из серије модема. Међутим, појавио се још један тзв. 56k модем. Говорни сигнал је континуални сигнал. Због тога се у већини случајева у комутационом центру користи одговарајући PCM сигнал бинарног протока 64kb/s по каналу. Он представља или дигитализовани говор или дигитализовани модемски сигнал, при чему је максимални бинарни проток са V.34 модемом 33,6kb/s. Познато је да парице [1] у приступној мрежи имају далеко већи капацитет. Претплатник може да закупи ISDN [2] везу (144kb/s) или да инсталира xDSL [3] модем. На први поглед изгледа једноставно доставити претплатнику 64kb/s који већ постоје у комутационом центру.

Проблем је следећи: на излазу из комутационог центра према претплатнику као и на улазу од претплатника у комутациони центар постоје филтри који ограничавају спектар улазног сигнала на опсег телефонског канала. Они су неопходни и због Д/А конверзије (од комутационог центра ка претплатнику) и А/Д конверзије (од претплатника ка комутационом центру). То значи да се претплатнику доставља аналогни сигнал добијен Д/А конверзијом као да је то реконструисан говорни сигнал. Поменути филтри се не могу уклонити. Пошто се у телефонској мрежи ништа не може мењати,



Слика 9.3 Примена V.90 стандарда

[1] Погледати поглавље о жичним трансмисионим медијумима.
[2] Мрежа интегрисаних услуга ISDN (*Integrated Service Digital Network*). Два корисничка канала од 64kb/s и један сигнализациони од 16kb/s.
[3] Дигитална претплатничка петља (*Digital Subscriber Line*).

преостаје једино да се промени модем. Тако је настао 56k модем.

Основна идеја је следећа:

- Сервер (везан дигиталном линијом за комутациони центар) шаље станици А (везаној аналогном линијом за комутациони центар) осмобитне бајтове података брзином 64kb/s; Д/А конвертор у кодеку ове бајтове претвара у одговарајуће амплитуде као да се ради о говорном сигналу. Том приликом врши се и одговарајућа експанзија сигнала на основу коришћене карактеристике компресије. Добијен сигнал личи на импулсну амплитудску модулацију.
- Задатак модема је да на основу одговарајућих примљених амплитуда правилно одреди бајтове података на основу којих су те амплитуде генерисане и преда их кориснику. Да би се ово могло успешно урадити у почетку се користи тест секвенца за одређивање одговарајућих амплитудских нивоа у пријемнику. Овај процес илустрован је на слици 9.3.

Коришћењем ове технике теоријски пренос од 56kb/s може бити постигнут од сервера до модема. Треба напоменути да је ово теоријска брзина. Физичка ограничења у локалној мрежи, укључујући удаљеност модема од телефонске централе, број веза или чворова у локалној мрежи, и укупан квалитет локалне мреже могу додатно ограничити брзину преноса. Ближе посматрање слике 9.3 показује да је увећање брзине понуђене од стране V.90 ограничено на половину везе: од сервера ка модему. Друга половина везе, од модема до сервера, мора да прође А/Д конверзију, због чега се појављује шум и брзина смањује на V.34 ниво. Брзина је другачија у сваком правцу па се за V.90 каже да је несиметрична технологија преноса. Несиметричне особине V.90 одговарају несиметричној природи најчешће употребе модема, а то је приступ Интернету. Уобичајено је да корисник шаље кратак упит ка серверу. Сервер шаље кориснику одговор са већом количином података, чинећи стандард V.90 потпуно прилагођен за приступ Интернету. Као и са свим осталим стандардима за модеме V.90 компатибилни модеми су у сагласности са свим ранијим стандардима. Када се веза успоставља модем покушава да се повеже на највећој могућој брзини. Уколико не успе, брзина се смањује на ниже V.90 нивое, па на V.34 ниво, затим V.32 ниво итд. све док се веза не успостави.

Стандард V.92 (унапређена верзија V.90) омогућава: бржу успоставу везе, прихватања позива за време трајања Интернет везе[1], повећање брзине са 33,6kb/s на 48kb/s и копмресију података по V.44 стандарду. Не подржавају га сви добављачи Интернету услуга.

Стандарди за компресију података

Протокол MNP[2] развила је компанија која се бавила производњом модема *Microcom*. Класе или групе MNP протокола одлични су примери *de facto* стандарда. Они су подржани у већини модема иако их није прогласила обавезним ниједна од званичних организација за стандардизацију. Међутим, MNP класа често представља основу за званично потврђене међународне стандарде. На пример стандард V.42 за корекцију

[1] *Modem on Hold (MOH)*
[2] *Microcom Networking Protocol*

MNP класа	Објашњење / Значај
1	Протокол за откривање грешака замењен каснијим класама.
2	Дефинише метод за асинхрони бајт-оријентисани пренос података у потпуном дуплексу.
3	Дефинише метод за синхронизовану бит-оријентисану комуникацију између модема, иако је комуникација између персоналних рачунара несинхронизована. Укида старт и стоп битове да би се ефикасност повећала и до 8%.
4	Прилагодљива величина пакета података: величина пакета података прилагођава се квалитету линије да би се избегле грешке или поновни пренос. Имплементација MNP протокола класе 4 може повећати ефикасност преноса и до 20%.
5	Протокол за компресију података који може повећати проток и до 200%.
6	Омогућава модемима који подржавају различите стандарде да комуницирају брзинама од 50 до 19,2kb/s. Елиминише некомпатибилност између Bell и V серије стандарда. Омогућава модемима у полудуплекс раду већу брзину пребацивања на основу тога који правац има више података за пренос.
7	Побољшана компресија података која повећава проток до 300%.
8	Комбинује MNP класу 7 са V.29 протоколом (9600 b/s, полудуплекс).
9	Комбинује MNP класу 7 и V.32 (9600 b/s, полудуплекс). Омогућава MNP и модемима који немају уграђен MNP стандард комуникацију са оптималним перформансама.
10	Састоји се од четири протокола ACE[1] који су оригинално намењени целуларним модемима и сателитским линијама и омогућава бољи рад у условима лоших веза, компензацију шума на линији и проблеме еха у појасу ограничене ширине. Вишеструки покушаји успостављања везе на највећем заједничком нивоу протокола. Величина пакета брзо се и динамично мења променама линијских услова. Бинарни проток и модулационе технике варирају са променама линијских услова. Комуникација се одвија брзином која омогућава највећу поузданост. Ако се линијски услови поправе већа брзина биће подржана.

Табела 9.3 Различите MNP класе

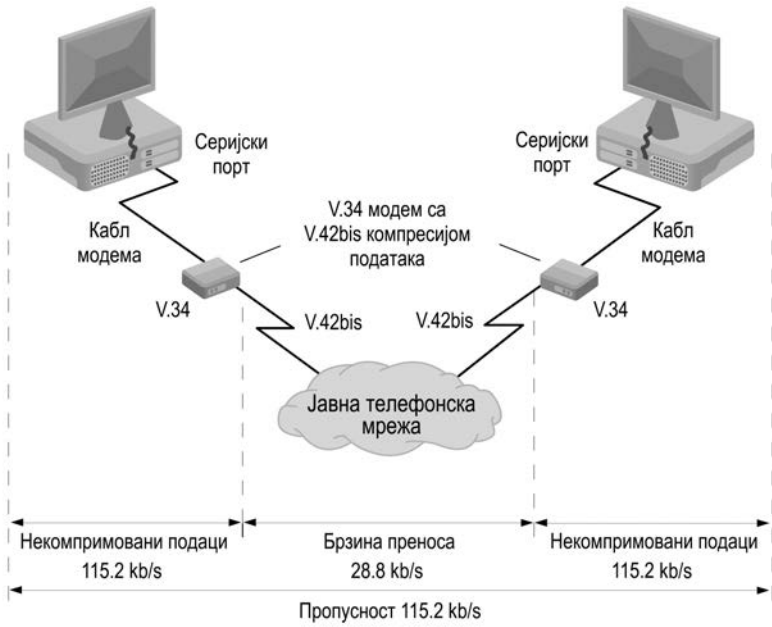
грешака организације ITU спаја MNP класе 2, 3 и 4. У табели 9.3 дат је преглед MNP класа које су у употреби.

Иако неколико чинилаца може довести до повећања ефикасности модема компресија података може имати значајан утицај у количини података стварно испоручених од стране модема у датом времену. Компресија података замењује велике низове карактера који се понављају специјалним кодом који представља узорак. Кôд се шаље другом модему. Од те тачке надаље модем пошиљалац шаље кôд уместо оригиналног узорка. Пошто је кôд значајно мањи од узорка кога представља, количина података која се шаље између два модема смањује се у оптималним условима и до 400%. Коришћењем компресије података за модеме бинарног протока 28,8kb/s (V.34 стандард) преко комутиране телефонске линије оптимално се може пренети 115,2kb/s података[2]. У овом случају 115,2kb/s назива се пропусност док бинарни проток остаје на, или испод максимума од 28,8kb/s за стандард V.34. Слика 9.4 илуструје разлику између пропусности и бинарног протока.

Важно је разумети како компресија података ради и чињеницу да се свих 115,2kb/s не преноси стварно телефонском мрежом. Једнако је важно разумети да компресија података једино ради ако оба модема на вези подржавају исти стандард за компресију по-

[1] *Adverse Channel Enhancement*

[2] Бинарни проток 28,8 kb/s фактор компресије 4:1.



Слика 9.4 Компресија података: линијска брзина према пропусној моћи

датака. Податке које је компримовао модем пошиљаоца мора декомпримовати модем примаоца истом методологијом и алгоритмом.

У случају уобичајеног стандарда за компресију V.42bis софтвер за компресију, пре него што пошаље податке, прегледа сирове податке које је добио од пошиљаоца трагајући за карактерима или узорцима који се понављају. Пошто открије узорке дужине до 32 карактера који се понављају два модема снимају (складиште) ове узорке заједно са 11-битним кôдом или кључем у библиотеку која се стално обнавља. Следећи пут када такав узорак података треба да буде послат модем пошиљаоц шаље 11-битни кôд који представља 32-бајтни узорак уместо да шаље целокупне низове. Модем прималац консултује своју библиотеку да види који некомпримовани узорак је представљен кôдом карактера који је примљен. Наравно, што је више узорака који се понављају, које софтвер за компресије може да пронађе међу подацима, већи степен компресије се може очекивати. Такође, неки низови података могу се боље компримовати од осталих низова података и то може довести до већег степена компресије.

У датом преносу компримованих података у ком се један карактер може декомпримовати у више карактера, важност спречавања грешака, откривање и исправка је очигледна. Погрешно пренесен карактер може бити препоручен библиотеци модема примаоца као узорак који се понавља, и онда да се декомпримује у погрешан низ података.

Стандарди V.42bis и MNP5

Два доминирајућа стандарда за компресију су V.42bis и MNP5. Већина модема покушава да се после иницијализације међусобно договори о коришћењу V.42bis компре-

сије. Мање ефикасан MNP5 протокол често се користи као друга могућност. V.42bis користи алгоритам за компресију података који је познатији као Лемпел Зив алгоритам.

Произвођачи могу побољшати овај алгоритам на два начина:

1. Повећањем количине меморије која се користи за библиотеку. Стандард је 1,5kB али је код неких модема величине 6kB;
2. Повећањем величине узорка карактера који може бити сачуван у библиотеци. Стандард је 32 бајта али неки модеми подржавају низ и до 256 бајтова.

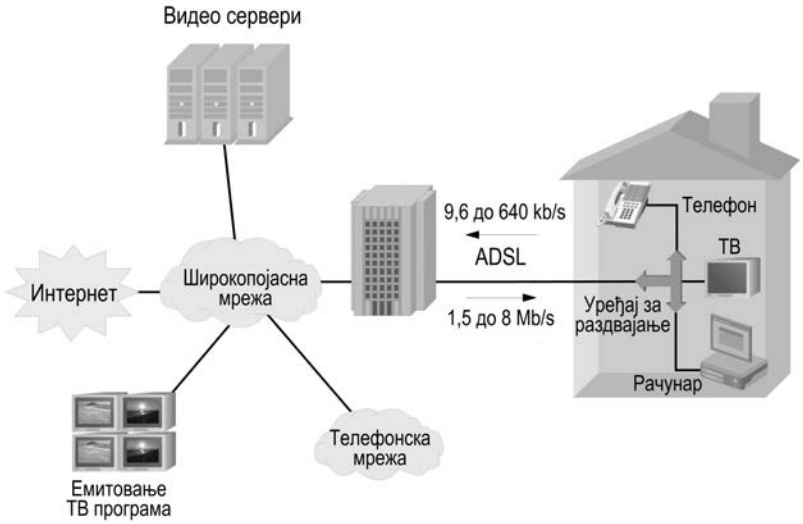
Побољшање особина стандарда као што је V.42bis ефикасно је једино ако су оба модема који учествују у преносу идентична. Нови стандард V.44 обезбеђује повећање компресије од 20% до 60 % а за неке апликације и до 200%.

Класе MNP омогућавају компресију података између 1,31:1 и 2: 1. Стандард MNP5 користи два алгоритма за компресију:

1. Хафманово кодирање заснива се на чињеници да се неки ASCII знакови појављују чешће од осталих. У типичној комуникацији без компресије података сваки знак се кодира помоћу 7 или 8-битних кодова. Софтвер који следи стратегију Хафмановог кодирања шаље слова која се најчешће користе у четворобитним групама; знакове који се ређе појављују кодира са 11 битова. Иако ређи знакови могу да захтевају више битова од некомпримованих знакова уз Хафманово кодирање се ипак штеди време јер се знакови који се чешће понављају шаљу са мање битова. Када се датотека пренесе софтвер за компресију прво укључује информацију о дужини кодираног знака а затим сам знак. Пошто се неки знакови сувише често понављају низ података који их садржи много је краћи по извршеној компресији него што би био да је употребљено више коришћено ASCII кодирање;
2. Кодирање по дужини заснива се на лакој идентификацији низа знакова који се често понављају, укључујући знакове који се не штампају као нпр. нов ред, нов пренос и размак. Када алгоритам примењен у стандарду MNP5 уочи најмање три иста знака у низу примењује кодирање по дужини. На линију ће послати овај знак и број који означава колико се пута он понавља. Описана техника обезбеђује одличну компресију за неке врсте датотека као што су датотеке програма за унакрсно израчунавање, које за форматирање користе велики број знакова који се не штампају.

9.3 Асиметричне дигиталне претплатничке петље

Када се у телефонској мрежи коначно достигла брзина преноса података од 56kb/s сматрало се да је посао добро обављен. У међувремену компаније које се баве развојем кабловске телевизије нудиле су брзине до 10Mb/s, а сателитске компаније планирале су да понуде у одлазном саобраћају 50Mb/s. Приступ Интернету постаје све важнија услуга која се поставља пред телефонске оператере. Као свој одговор телефонски оператери нуде дигитални приступ преко локалних петљи. Дигитални приступ даје могућност већег опсега од стандардног телефонског канала



Слика 9.5 Данашња ADSL мрежа

(слика 9.5) па су могуће следеће апликације:

- приступ Интернету,
- обављање посла са удаљених места[1],
- преузимање видео садржаја: емитовање ТВ програма или видеа по захтеву[2],
- пренос говора преко IP протокола[3],
- телемедицина,
- даљинско образовање и куповина,
- игрице[4].

У самом почетку постојало је више међусобно преклапајућих решења која се сва могу означити општом ознаком xDSL[5] (x означава различите системе). Преглед постојећих xDSL дат је у табели 9.4. У овом поглављу описаћемо различите системе међу којима најраспрострањенији постаје ADSL[6] систем. Пошто се ADSL системи још развијају и нису донети сви стандарди, треба имати у виду да ће се неки од описаних детаља временом променити, али сигурно не и основни концепт.

Разлог због ког су модеми спори је тај што они користе телефонске линије које су намењене преносу сигнала говора и цео систем је прилагођен говору. Пренос података дошао је тек касније. У тачки где се локална петља завршава у локалном чворишту (централи) телефонски сигнали[7] пролазе кроз филтре који ограничавају све учестаности испод 300Hz и изнад 3400Hz[8]. Подаци који се преносе телефонским ли-

[1] *Teleworking*
[2] *Video on Demand*
[3] *VoIP (Voice over IP)*
[4] *On line gaming*
[5] *Digital Subscriber Line*
[6] *Asymetric* DSL
[7] Може се формулисати и на следећи начин: телефонске парице претплатника завршавају на нископропусним филтрима опсега од 300 до 3400Hz.
[8] Ограничавање није тренутно (оштро) па се сматра да је опсег телефонског сигнала 4000Hz.

Група	Правац	Максимална брзина [Mb/s]	Ознака ITU	Година доношења стандарда
ADSL	Директни	7	G.992.1	1999.
	Повратни	0,8		
ADSL2	Директни	8	G.992.3	2002.
	Повратни	1		
ADSL2plus	Директни	24	G.992.5	2003.
	Повратни	1		
ADSL2-RE	Директни	8	G.992.3	2003.
	Повратни	1		
SHDSL	Директни	5,6	G.991.2	2001. (иновиран 2003.)
	Повратни	5,6		
VDSL	Директни	15	G.993.1	2004.
	Повратни	55		
VDSL2 12MHz, великог домета	Директни	30	G.993.2	2005.
	Повратни	55		
VDSL2 30MHz, кратког домета	Директни	100	G.993.2	2005.
	Повратни	100		

Табела 9.4 Опције DSL технологије

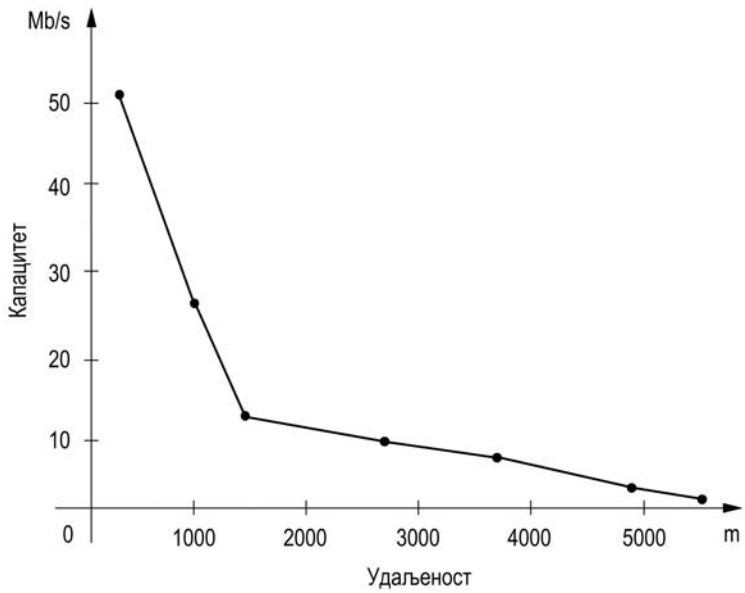
нијама такође су ограничени овим уским опсегом [1].

Када претплатници користе xDSL системе онда се линија која стиже од претплатника до локалног чвора (централе) везује на другу врсту комутатора. Он не садржи филтер па се цео капацитет локалне петље даје на располагање претплатнику. Ограничавајући фактор постају физичке карактеристике локалне петље а не граница коју филтер поставља.

Капацитет локалне петље зависи од више фактора: дужине, дебљине жице и општег квалитета. На слици 9.6 нацртана је могућа ширина опсега у функцији од растојања под претпоставком да су сви остали фактори оптимални (нове жице, равномерна изолација, итд.)

Последице слабљења приказане на слици 9.6 стварају проблеме оператерима телефонских мрежа. Када нуде услуге корисницима морају да имају у виду и растојања до корисника. То значи да удаљеним корисницима не могу да понуде исту услугу као онима који су ближи локалном чворишту. Што је понуђена брзина нижа то је већа удаљеност на којој се она може остварити. Смањивање брзине умањује шансе да ће корисник пожелети да плати за ту услугу. Могуће, мада веома скупо решење, било би прављење малих локалних чворишта. Услуге xDSL система пројектоване су са одређеним циљем. Прво, систем треба да ради користећи каблове категорије 3 у постојећим претплатничким петљама. Друго, xDSL системи не смеју да поремете рад постојећих уређаја: телефона и

[1] Погледати одељак: Модеми за телефонски канал.

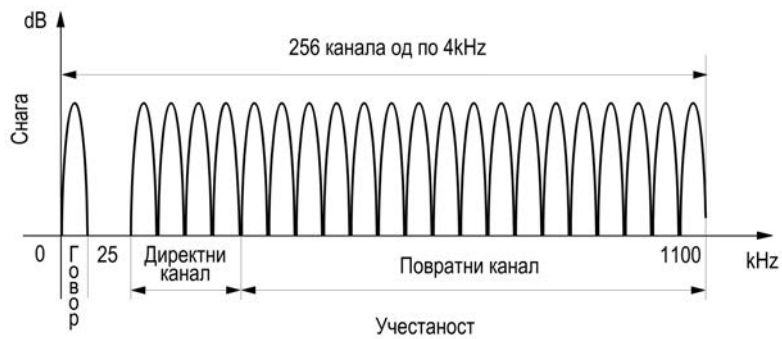


Слика 9.6 Ширина опсега у зависности од растојања код упредених парица категорије 3 за xDSL системе

факса. Треће, морају да понуде брзине веће од 56kb/s. Четврто, морају бити стално прикључени, што подразумева месечну претплату, а не плаћање по минуту.

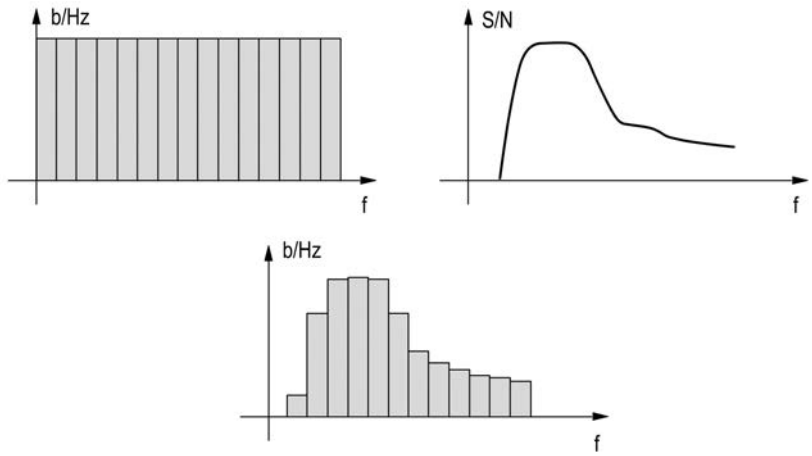
Иницијална понуда стигла је од AT&T. Фреквенцијски опсег од 1,1MHz који одговара претплатничкој петљи подељен је у три дела: опсег стандардног телефонског канала [1], директни (одлазни) канал [2] - од претплатника до локалног чворишта, повратни (долазни) канал [3] - од локалног чворишта до корисника (слика 9.9а).

Други приступ је систем са више дискретних тонова DMT [4] (илустрован је на слици 9.7). DMT техника састоји се у коришћењу више носећих сигнала на различитим



Слика 9.7 Распоред канала код ADSL система са DMT модулацијом

[1] POTS (*Pllain Old Telephone Network*) - јавна телефонска мрежа (JTM).
[2] *Upstream*
[3] *Downstream.*
[4] *Discret MultiTone*



Слика 9.8 Додељивање брзине (b/Hz) по каналу код DMT система

учестаностима, и слању дигиталних података кроз канал. Фреквенцијски опсег од 1,1MHz подељен је у 256 независних канала од којих је сваки широк 4312,5Hz.

При иницијализацији DMT модем шаље тест сигнале у сваки од потканала да би одредио однос сигнала и шума. На основу тог податка модем додељује већу битску брзину каналу са бољим преносним карактеристикама. Сваки потканал може да преноси од 0 до 60kb/s. На слици 9.8 приказана је уобичајена ситуација у говорном каналу где слабљење расте са учестаношћу. Последица је смањење односа сигнала и шума на већим учестаностима, а самим тим и смањење капацитета, односно максималне могуће брзине преноса података.

Канали су распоређени на следећи начин (слика 9.9):

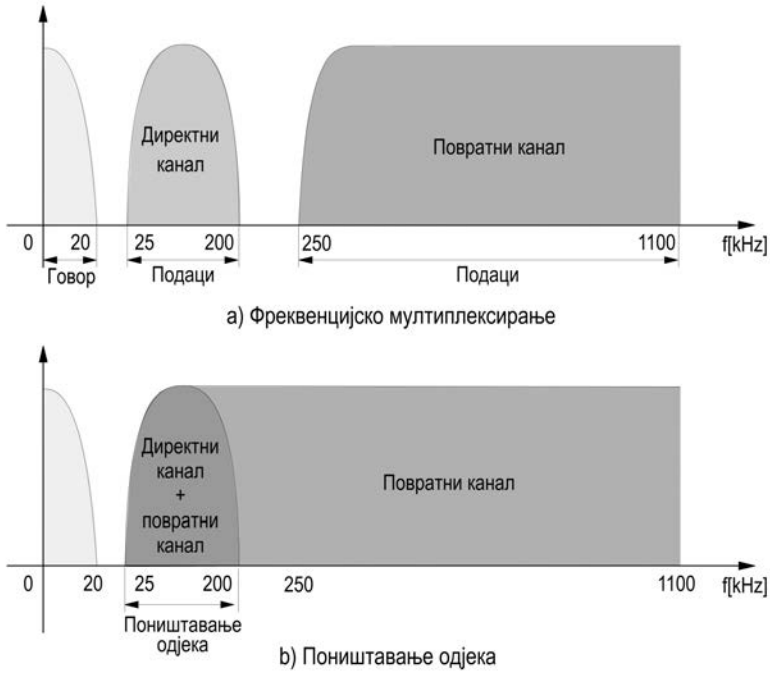
- канал означен са 0 користи телефонска мрежа. Да би се спречила међусобна интерференција сигнала говора и података за говор је резервисано првих 25kHz;
- користи се или поништавање одјека [1] или фреквенцијски мултиплекс за доделу два опсега: за одлазни и долазни саобраћај,
- по један канал користи се за управљање одлазним и долазним саобраћајем. Преосталих 248 канала могу се употребити за пренос података корисника.

У принципу сваки од 248 канала за податке може се употребити за пренос података у потпуном дуплексу. Међутим хармоници, преслушавање итд. ограничавају брзину реалних система значајно испод теоретских граница. Задатак пружаоца Интернет услуга (ISP [2]) је да одреди колико канала се користи за одлазни а колико за долазни саобраћај. Технички је могуће обезбедити однос 50% - 50% али већина пружаоца Интернет услуга бира однос од око 80% - 90% опсега за долазни саобраћај. Разлог је једноставан: већина корисника више користи долазни од одлазног канала. Овакав избор даје ознаку A [3] код ADSL-а.

[1] Поништавање одјека (енг. *echo cancellation*) је техника обраде сигнала која омогућава пренос дигиталног сигнала у оба правца истовремено у једној линији за пренос. Да би исправно примио долазећи сигнал предајник мора да од пријемног (долазећег) сигнала одузме одјек (ехо) своје сопствене предаје.

[2] *Internet Service Provider*

[3] *Asymetric*



Слика 9.9 Конфигурација ADSL канала од претплатника до локалног чворишта

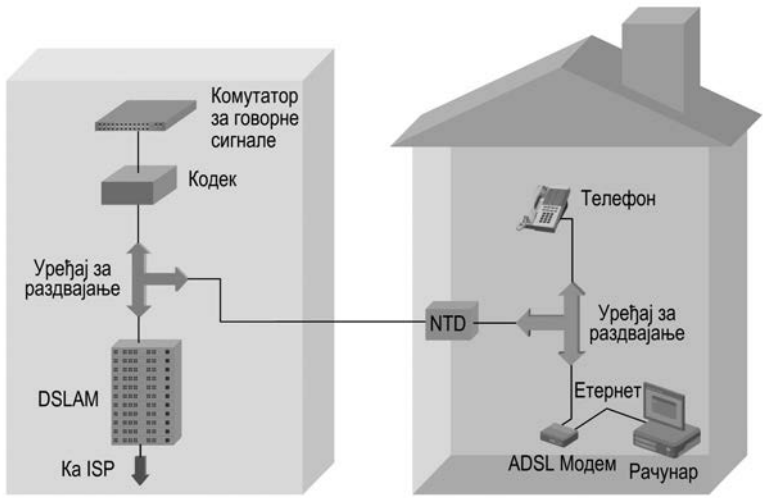
Уобичајена подела је: 32 канала за долазни саобраћај и остатак за одлазни. Такође је могуће подесити да су неки од одлазних канала бидирекциони да би се у случају потребе за повећањем опсега у неком од праваца то могло и обезебедити. Оваква опција захтева додавање специјалних кола за одстрањивање одјека (eха).

Стандарди за ADSL модеме (ANSI T1.413 и ITU G.992.1) дозвољавају брзине до 8Mb/s у долазном каналу и 1Mb/s у одлазном каналу. Ипак само мали број пружаоца Интернет услуга нуди ове брзине. Уобичајено се нуде брзине 512kb/s у долазном и 64kb/s у одлазном каналу и 1Mb/s у долазном и 512kb/s у одлазном каналу.

У оквиру сваког канала користи се модулациона шема слична оној по стандарду V.34. Разлика је у сигнализационој брзини која је код ADSL модема 4000Bd а код V.34 модема 2400Bd. Квалитет сигнала у сваком каналу стално се надгледа и брзина, уколико је то потребно, континуално прилагођава. На тај начин различити канали могу да имају различите брзине. Брзина се постиже са QAM модулацијом са 15 битова по једном боду[1].

Уобичајена организација ADSL система приказана је на слици 9.10. У овој шеми телефонска компанија треба да инсталира мрежни интерфејсни уређај (NTD[2]) на локацији корисника. Интерфејсни уређај представља крајњу тачку надлежности телефонског оператера и почетак надлежности корисника. До интерфејсног уређаја (а некада заједно с њим) је уређај за раздвајање[3]. То је аналогни филтер који раздваја фреквенцијски опсег од 0 до

[1] 15 битова по једном сигнализационом елементу. Брзина (линијска, модулациона) дефинише се као број сигнализационих елемената у секунди и јединица је бод (Bd - *baud*).
[2] *Network Telephone Device*
[3] *Splitter*



Слика 9.10 Уобичајена организација ADSL система

4000Hz, који телефонски оператери користе за говор, од фреквенцијског опсега који се користи за податке. Телефонски сигнал усмерава се ка телефону и факсу, а сигнал података усмерава се ка ADSL модему. ADSL модем је уређај за дигиталну обраду сигнала који ради као 250 паралелних модема на различитим учестаностима, а са QAM модулацијом.

Већина данашњих ADSL модема су спољашњи (екстерни) уређаји и рачунари треба да буду повезани са њима великом брзином. Често се то обезбеђује постављањем Етернет мреже са два међусобно блиска чвора: ADSL модем и рачунар опремљен Етернет картицом. Понекад се уместо Етернет мреже користи USB порт. Очекује се да ће се ускоро појавити интерни ADSL модеми. На другој страни телефонске парице, у локалном чвориште, инсталира се одговарајући уређај за раздвајање. На овом месту део сигнала који одговара говору издваја се и шаље комутатору за говорне сигнале. Сигнал изнад 25kHz усмерава се ка новој врсти уређаја - мултиплексеру за дигиталне претплатничке петље DSLAM[1]. Мултиплексери DSLAM садрже исту врсту процесора за обраду сигнала као и ADSL модем. Сигнал из ADSL модема додељен подацима претвара се у поворку битова од којих се праве пакети података и шаљу пружаоцима Интернет услуга.

Пошто описани систем обезбеђује потпуно раздвајање телефонске мреже и ADSL система оператерима телефонске мреже једноставно је да га примене. Све што треба да ураде је да набаве мултиплексер DSLAM, уређај за раздвајање, и повежу ADSL корисника на уређај за раздвајање. Други системи (нпр. ISDN) захтевају значајније измене у постојећој комутационој опреми.

Мана у пројектовању система на слици 9.10 је присуство уређаја NTD и уређаја за раздвајање на страни корисника. Постављање ових уређаја захтева рад специјализованих лица, телефонских оператера, што значајно повећава трошкове инсталације. Због тога је стандардизована друга врста система без уређаја за раздвајање. Неформално се означава као G.lite, али званична ознака ITU стандарда је G992.2.

[1] *Digital Subscriber Line Access Multiplexer*

Систем би изгледао исто као на слици 9.10 само без уређаја за раздвајање. Телефонска линија се користи на исти начин. Разлика је у следећем: микрофилтер треба да се постави у сваки телефонски прикључак између телефона или ADSL модема и телефонске парице. Микрофилтер је нискропропусни филтер који одстрањује учестаности изнад 3400Hz; микрофилтер за ADSL модем је високопропусни филтер који одстрањује учестаности испод 25kHz. Овакав систем није поуздан као систем са уређајем за раздвајање. Због тога се G.lite систем може користити за брзине до 1,5Mb/s, а ADSL систем са уређајем за раздвајање за брзине до 8Mb/s. Новије верзије ADSL2, ADSL2plus, ADSL2-RE[1] обезбеђују веће максималне брзине.

ADSL је стандард физичког слоја. Шта се налази изнад и како ради зависи од оператера. За међусобно повезивање комутационих центара користе се Етернет или ATM рачунарске мреже пошто оне могу да обезбеде захтеве за квалитетом услуге.

Дигиталне претплатничке петље великих брзина

Системе који се срећу под називом дигиталне претплатничке петље великих брзина HDSL[2] развила је компанија BellCore при крају 1980. године да би обезбедила ефикаснији начин за дистрибуцију брзине података од 1,544Mb/s[3]. Линије T1 (E1) користе стандардне AMI кодове и заузимају опсег око 1,5MHz (2MHz). Пошто је реч о преносу високих учестаности слабљење ограничава домет на T1 (E1) линијама. Тако је за велики број претплатничких петљи потребан један или више обнављивача што представља значајно финансијско улагање.

Обележја HDSL система су:

- 2B1Q линијски кôд[4],
- обезбеђују брзине до 2Mb/s преко упредених парица,
- фреквенцијски опсег је око 196kHz,
- домет је до 4km.

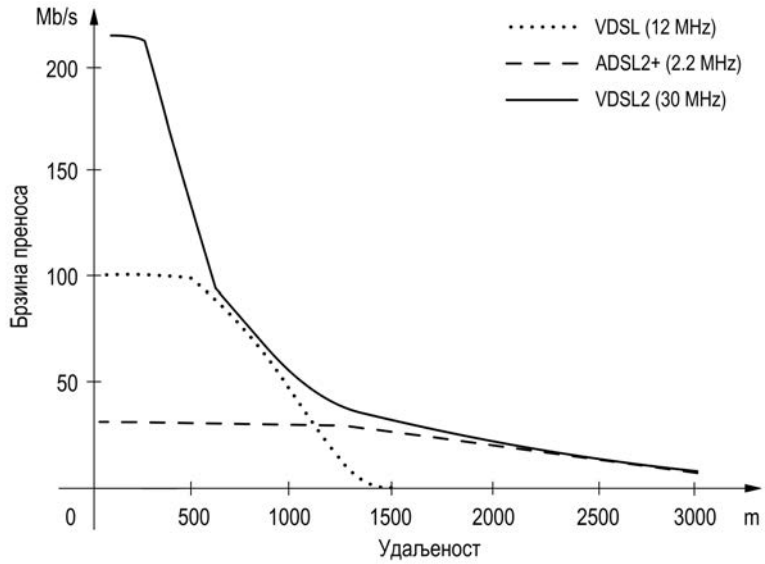
Симетрична дигитална претплатничка петља

Без обзира што је HDSL веома примамљив за замену постојећих T1 (E1) линија није погодан за обичне кориснике[5] пошто захтева две парице. Обичан корисник поседује само једну парицу. Систем који је развијен, а који се среће под називом дигитална претплатничка петља са једном линијом SHDSL[6], обезбеђује исту врсту услуге као и HDSL системи, али преко једне телефонске парице. Користи се 2B1Q кодирање, а техником поништавање одјека обезбеђује се рад у потпуном дуплексу.

Дигиталне претплатничке петље веома велике брзине

Једна од најновијих xDSL технологија је дигитална претплатничка петља изузетно велике брзине VDSL[7]. Намена ове технологије је да обезбеди систем сличан ADSL си-

[1] *Asymetric Digital Subscriiber Line Reach Extended*
[2] *High Data Rate Digital Subscriber Line*
[3] T1 стандард је у САД, а E1 стандард је у Европи (2,048Mb/s).
[4] Два бита се представљају са једним од четири могућа напонска нивоа.
[5] Користи се и термин приватно лице (резиденцијални корисник) за разлику од правног лица (корисника).
[6] *Symetric Digital Subscriber Line*
[7] *Very High Data Rate Digital Subscriber Line*



Слика 9.11 Дијаграм протока података (брзине) ADSL2+,VDSL1 и VDSL2 системи у зависности од растојања (дужине кабла)

стему на много већим брзинама уз смањење домета (слика 9.11). Максимални фреквенцијски опсег који се користи за пренос сигнала:

- 1,1MHz код ADSL система,
- 2,2MHz код ADSL2+ система,
- 12MHz код VDSL система и
- 30MHz код VDSL2 система кратког домета.

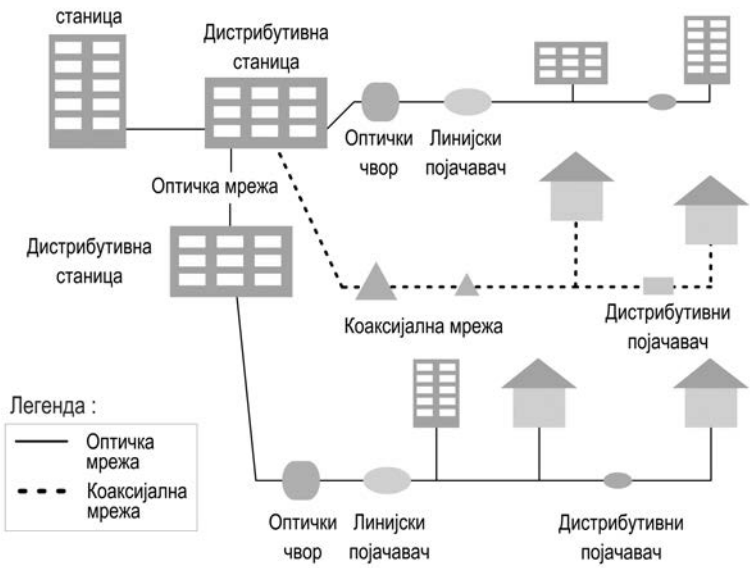
Брзине које су нудили системи ADSL2 и SHDSL нису довољне за истовремени пренос говора, слике и података[1]. Захтеви који се постављају пред VDSL системе су: истовремени пренос говора, слике и података, могућност пријема 3 дигитална телевизијска канала, пренос говора преко пакетских мрежа (VoIP)и пренос података брзином од 5Mb/s.

		ADSL	HDSL	SHDSL	VDSL
Брзина канала	Директни	1,5 - 8Mb/s	1,544 - 2,048Mb/s	192kb/s - 5,6Mb/s	13 - 52Mb/s
	Повратни	9,6 - 640kb/s			1,5 - 2,3Mb/s
Начин рада		Асиметрични	Симетрични	Симетрични	Асиметрични
Број тел. парица		1	2	1	1
Домет (24 AWG)		3,7 - 5,5km	3,7km	3 km	1,4km
Сигнализација		Аналогна	Дигитална	Дигитална	Аналогна
Линијски кôд		CAP[2]/DMT	2B1Q	2B1Q	DMT
Учестаност		1 - 5MHz	196kHz	196kHz	≥10MHz
Битова / циклусу		Мења се	4	4	Мења се

Табела 9.5 Поређење xDSL система

[1] *Triple Play*

[2] Амплитудска и фазна модулација без носиоца (*Carrierless Amplitude and Phase*) је верзија QAM где се долазећи подаци модулишу појединачним носиоцима и затим преносе телефонском линијом. Сам носилац је потиснут пре слања па одатле у називу „без носиоца“.



Слика 9.12 Архитектура КДС система

Сва предвиђања су да они то могу да обезбеде корисницима. У табели 9.5 дате су упоредне карактеристике различитих xDSL система.

Кабловски модеми

Један од све чешће коришћених начина приступа Интернету је преко система чија је основна намена била дистрибуција телевизијске слике (КДС[1]). Најчешће се користи ситем каблирања који користи и оптичка влакна и коаксијалне каблове (HFC[2]). Архитектура система HFC шематски је приказана на слици 9.12.

Слика 9.13 Фреквенцијски распоред КДС система

[1] Кабловски дистрибутивни систем. Среће се и под називом кабловска телевизија (*Cable TV*).
[2] *Hybrid Fiber Coax*

Карактеристика	DOCSIS 1.1	Euro-DOCSIS	DVB-RC
Пренос у повратном каналу	64QAM: 27Mb/s 256QAM: 42Mb/s ITU J.83B 6MHz канал	64QAM: 38Mb/s 256-QAM: 52Mb/s ITU J.83A 8MHz канал	64QAM: 38Mb/s 256QAM: 52Mb/s ITU J83B 6MHz канал
Пренос у директном каналу	QPSK: 0,320; 0,640; 1,280; 2,560 и 5,120b/s 16QAM : 0,640; 1,280; 2,560; 5,120 и 10,24Mb/s 5 - 42MHz	QPSK: 0,320; 0,640; 1,.280; 2,560 и 5,120Mb/s 16QAM: 0,640; 1,280; 2,560; 5,120 и 10,24Mb/s 5 - 65MHz	DQPSK: 1,544Mb/s; 3,088Mb/s 5 - 65MHz
Перформансе	Ефикасност >80% код преноса говора и података брзине до 10,24Mb/s за ширину канала од 3,2MHz	Ефикасност >80% код преноса говора и података брзине до 10,24Mb/s за ширину канала од 3,2MHz	50-72% ефикасност за брзине до 3,088Mb/s за ширину канала од 2MHz
Сервиси	Приступ Интернету, пренос говора преко Интернета[1], видео на захтев[2].	Приступ Интернету, пренос говора преко Интернета, видео на захтев.	Приступ Интернету, видео на захтев
Комерцијална употреба	У употреби	У употреби	Раније DAVIC 1.2, сада се испитује DVB-RC
Базни протокол	IP са QoS	IP са QoS	Пренос ATM ћелија са прилагођавањем на IP протокол
Сигурност	Услуга приватности са алгоритмом DES 56-битни кључ који ради у режиму уланчавања CBC[3]	Услуга приватности са алгоритмом DES 56-битни кључ који ради у режиму уланчавања CBC	Није укључена
QoS	8 - 16 бита	8 - 16 бита	53 бита + заглавље физичког слоја

Табела 9.6 Поређење стандарда DOCSIS1.1, Euro-DOCSIS1.1 и DVB-RC

На слици 9.13 представљена је расподела фреквенцијског опсега КДС система. Као што видимо:

- за пренос ТВ слике (од главне станице до претплатника) користи се фреквенцијски опсег од 110MHz до 862MHz,
- за пренос FM радио-сигнала користи се фреквенцијски опсег од 87,6MHz до 110MHz,
- за повратни смер (од претплатника до главне станице) користи се опсег од 5MHz до 65MHz,
- у опсегу од 110MHz до 862MHz користе се стандардни канали ширине 8MHz[4]

Постоје три стандарда за пренос података по КДС-у и њихове основне карактеристике су дате у табели 9.6. Треба напоменути да је стандард Euro-DOCSIS1.1 европска варијанта стандарда DOCSIS1.1[5] који се користи у САД. Основна група стандарда за дигитални пренос слике су DVB[6] стандарди који су дефинисани за сателитске системе, кабловске, радио-дифузне итд. У табели је стандард DVB-RC[7] који користи ATM AAL5

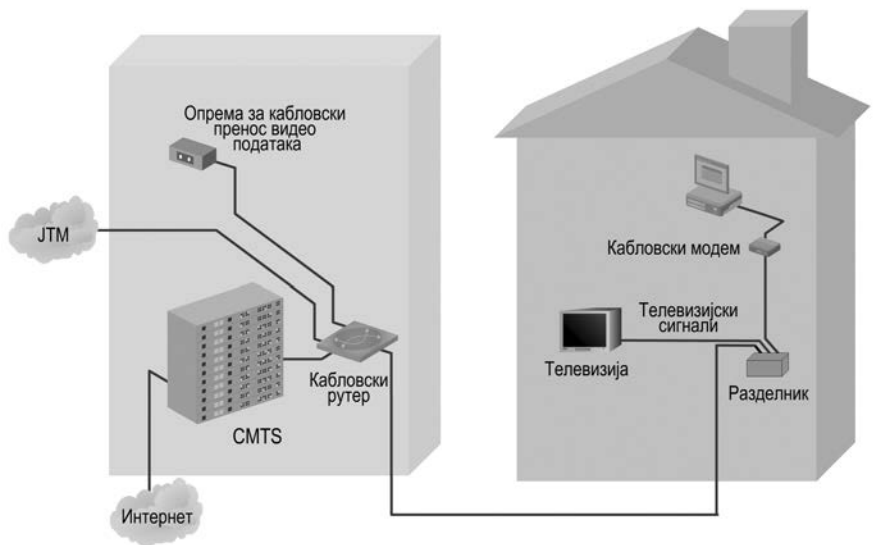
[1] *Vioice over IP*
[2] *Interactive Set top Box* - уређај који се повезује на телевизор и омогућава видео на захтев тј. лични видео рекордер.
[3] *Cipher Block Chaining*
[4] У САД-у постоје незнатне разлике: стандардни канал је ширине 6MHz, горња граница повратног смера је 54MHz и горња граница директног смера је 750MHz.
[5] *Data Over Cable Service Specification*
[6] *Digital Video Broadcast*
[7] *DVB Returned Channel*

OSI	DOCSIS (Пренос података КДС системом)	
Виши слојеви	Апликације	DOCSIS Управљачке поруке
Транспортни слој	TCP или UDP	
Мрежни слој	IP	
Слој везе	IEEE802.2	
	DOCSIS MAC	
Физички слој	Директни канал TDMA[1] (мале временске целине)	Повратни канал TDM (MPEG[2])
	5-65 MHz	8 MHz ITU-T J.83 A
	HFC	

Табела 9.7 Поређење OSI референтног модела и DOCSIS протокола

протокол за пренос података. Као што је уобичајено свака од архитектура протокола пореди се са OSI референтним моделом што је и приказано у табели 9.7. Неки системи за кабловску телевизију били су предвиђени само за једносмерно емитовање, односно поседовали су само долазни (повратни)[3] канал ка кориснику. Већина данашњих система омогућава саобраћај у оба правца. Осим дистрибуције ТВ слике у КДС системима све остале услуге реализују се као пренос података.

У овом делу анализираћемо приступ Интернету преко КДС система. Овај приступ захтева кабловски модем, уређај који мора да има два интерфејса: један код рачунара корисника и други у главној станици[4] (слика 9.14). Интерфејс између рачунара и модема је



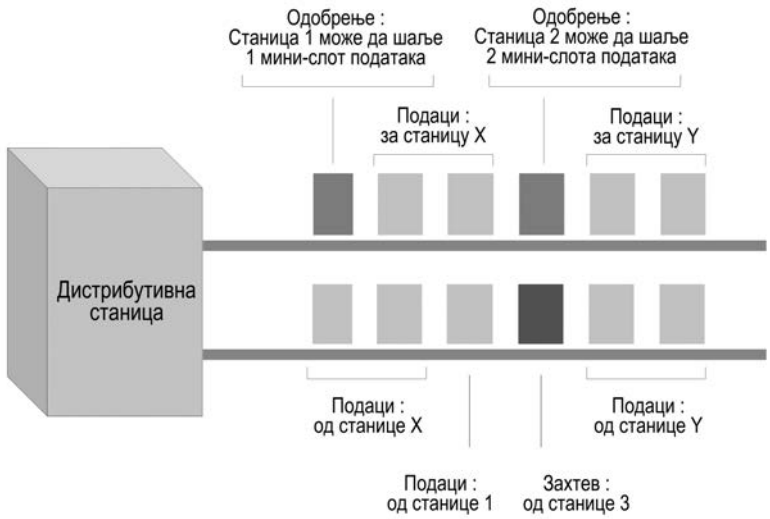
Слика 9.14 Инсталација са кабловским модемом

[1] TDMA (*Time Division Multiplex Access)*

[2] *Motion Picture Expert Group* - експертска група за покретне слике. У питању су алгоритми који се користе за компресију видео сигнала и представљају међународни стандад од 1993. године.

[3] *Downstream*

[4] Део који се налази у главној станици а односи се на приступ Интернету срећете се у литератури [15] под називом завршни систем кабловских модема и означава са CMTS (*Cable Modem Termination System*).



Слика 9.15 Расподела временских целина код кабловских модема

или преко локалне рачунарске мреже (Етернет интерфејс) или USB порта. Шта се дешава када се кабловски модем прикључи? Модем тражи у долазним каналима специјалан пакет који се периодично шаље из главне станице са системским параметрима за оне модеме који су се тек прикључили на мрежу. Пошто пронађе тај пакет управо прикључени модем оглашава своје присуство у неком од одлазних (директних) канала[1]. Главна станица одговара додељивањем два канала за сваки правац (одлазног и долазног).

Канале дели више корисника па је неопходно применити неку од техника за доделу капацитета у оквиру канала. Најчешће се користи једна врста статистичког временског мултиплекса (слика 9.15).

У долазном саобраћају (од главне станице до корисника) подаци се испоручују у виду пакета. Уколико канал дели више претплатника и више од једног је и укључено (активно) сваки претплатник добија само део долазног капацитета. У долазном и одлазном саобраћају сваком од претплатника се такође додељују тачно одређени временски делови (слотови) .

[1] *Upstream*

10. Комуникационе технике дигиталних података

За два уређаја повезана трансмисионим медијумом, који треба да размењују податаке, потребан је висок степен међусобне кооперације. Подаци се обично преко медијума шаљу један по један сигнализациони елемент у току времена.

Брзина, трајање и размак сигнализационих елемената морају да буду усаглашени на пријемној и предајној страни. Користе се две технике: асинхрона и синхрона. Као што смо видели пренос података није процес без грешака и потребни су механизми за заштиту од њих.

10.1 Синхронизација у преносу података

У даљем тексту подразумеваћемо серијски пренос података; тј. пренос података преко једног комуникационог пута, а не преко паралелног скупа линија. Код серијске комуникације сигнализациони елеменат шаље се на линију један по један. Сваки сигнализациони елемент може да буде:

- мањи од једног бита - пример је Манчестер кодирање,
- један бит - пример је NRZ и FSK (дигитални и аналогни),
- више од једног бита - пример је QPSK.

Због једноставности, у даљем објашњавању претпоставићемо случај од једног бита по сигнализационом елементу (уколико није другачије наглашено). Синхронизација је један од кључних задатака преноса података. Пријемник треба да:

- препозна почетак и крај блока битова,
- зна трајање сваког бита,
- узима узорак (одмерак) у тачним тренуцима времена и на тај начин очитава сваки бит.

Типична ситуација је она у којој пријемник одмерава линију у средини сигнализационог (битског интервала). Уколико постоји разлика у времену, рецимо за 5% између предајника и пријемника, прво одмеравање ће бити померено 0,05 битског времена у односу на центар бита. На крају десетог одмеравања пријемник може да погреши. За мању разлику у времену пријемник неће погрешити, али докле год они нису на неки начин синхронизовани пријемник неће бити у кораку са предајником.

За синхронизацију су уобичајна два приступа. Први се назива асинхрони пренос. У овој шеми се шаље један по један карактер, а карактери су пет до осам битова дугачки. Синхронизација се мора постићи само у оквиру сваког карактера. На почетку сваког карактера пријемник има прилику да се поново синхронише. Алтернатива је синхрони пренос. Велики блокови података шаљу се као јединице или нуле и пријемник мора дужи период времена да буде синхронисан са предајником.

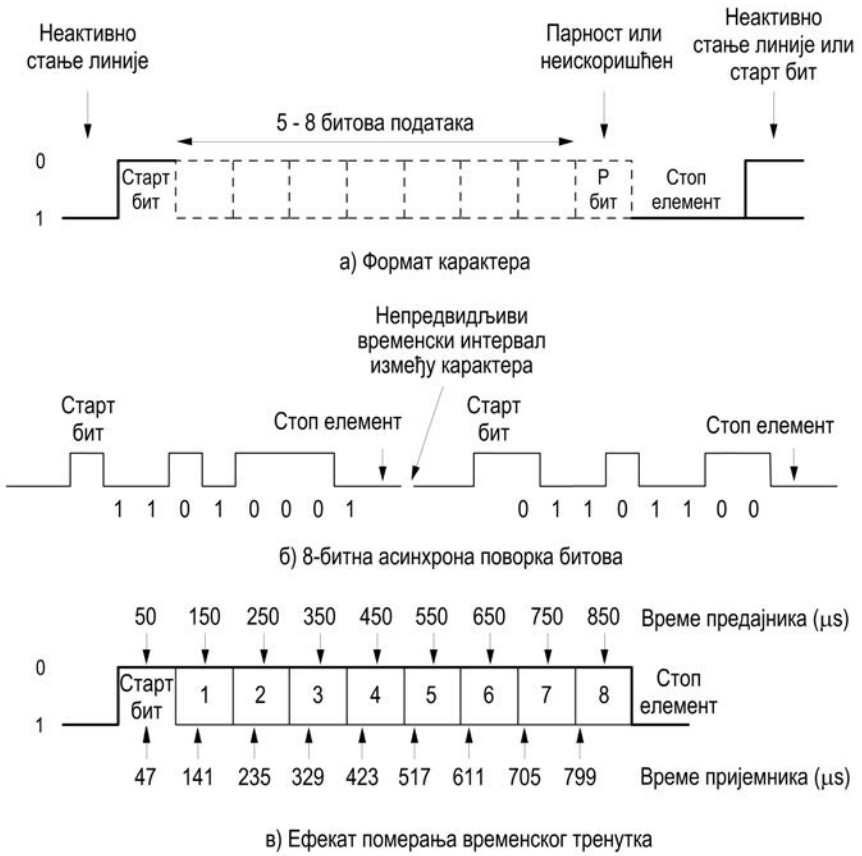
Постоји хијерархија у задацима који се постављају пред синхронизацију:

- битска синхронизација - препознаје почетак и крај сваког бита,
- синхронизација карактера или речи - препознаје почетак и крај сваког карактера или друге мале јединице података,
- синхронизација блокова или порука - препознаје почетак и крај великих јединица података.

Асинхрони пренос

Један начин за решавање проблема синхронизације је слање мањих блокова битова на почетку сваког блока за поновну синхронизацију (ресинхронизацију). Стара техника позната као старт-стоп или асинхрони пренос ради управо то. Асинхрони пренос заснован је на слању карактера [1] дужине 5 - 8 битова (слика 10.1).

Када се не преносе карактери линија између предајника и пријемника је неактивна [2]. Дефиниција неактивног стања на линији је конвенција и типично је еквивалентна сигна-



Слика 10.1 Асинхрони пренос

[1] Користи се и термин карактер оријентисан.
[2] *Idle state* - јалово стање

лизационом елементу за бинарно 1. Пријемник испитује када долази до транзиције са 1 на 0 (старт) што указује на почетак карактера, затим узима узорак сигнала у једном битском интервалу и то понавља за свих осам интервала. Крај карактера (стоп) означава се једном до две битске позиције вредности бинарно 1. Затим очекује нову транзицију са 1 на 0. На пример ASCII карактер се обично шаље као целина од 8 битова, узимајући у обзир и бит парности. Уколико је пријемник 5% бржи или спорији од предајника 10. информациони бит ће се одмеравати са 45% померајем и још увек ће бити коректно идентификован (слика 10.1в). Посматрајмо на пример пренос брзином од 10kb/s, па је сваки бит ширине 100μs. Претпоставимо да је пријемник бржи 6% по битском интервалу од предајника, односно 6μs по битском интервалу. Грешка као што је ова резултује у две грешке. Прво, последњи одабрани бит је неисправно примљен. Друго, бројач битова неисправно одбројава (осмо одбројавање у време седмог бита). Уколико је бит 7 јединица, а бит 8 је нула, бит 8 може да буде погрешно интерпретиран као да је старт бит. Ово се назива грешка рама, пошто се карактер заједно са старт и стоп елементима назива рам [1]. Такође, уколико за време неактивног стања шум проузрокује лажно појављивање старт бита може да наступи грешка рама [2]. Слика 10.1 показује да што је већи рам то је и кумулативана грешка већа.

Асинхрона комуникација је једноставна и јефтина, али захтева 2 - 3 бита више по карактеру. На пример за седмобитни кôд, користећи једнобитни стоп елемент, на сваких девет битова два не носе никакву информацију, тако да је премашење [3] 2/9=0,22. Наравно, слањем великих блокова између старт и стоп елемената проценат премашења се може смањивати.

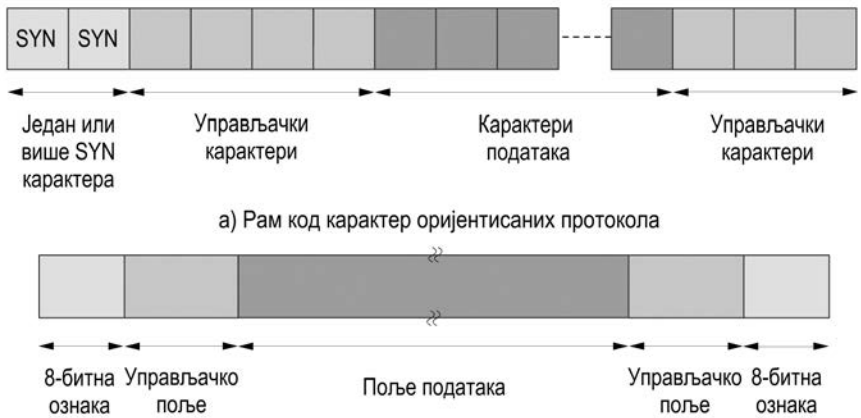
Као што се на слици 10.1 види што је већи блок битова то је акумулирана грешка већа. За велике блокове битова користи се друга врста синхронизације, која се зове синхрони пренос.

Синхрони пренос

Синхрони пренос је значајно ефикаснији начин комуникације. У овом начину рада блокови битова шаљу се без старт и стоп елемената. Могуће је предвидети тачно време које је потребно да стигне бит. Да би се спречио временски померај између предајника и пријемника њихов такт мора да буде међусобно синхронисан. Једна могућност је да се обезбеди посебна линија за такт између предајника и пријемника. Други начин је да такт сигнал буде убачен [4] у сигнал података. Код дигиталних сигнала синхронизација се може постићи Мачестер (или диференцијалним Манчестер) кодирањем. Када се преносе аналогни сигнали могу се користити бројне технике: једна од њих је синхронизација пријемника на основу фазе сигнала носеће учестаности.

Са синхроним преносом захтева се и други ниво синхронизације који обезбеђује пријемнику да одреди почетак и крај блока података. Да би се то обезбедило сваки блок започиње са преамбулом (битска комбинација која означава почетак) и заврша-

[1] *Frame*
[2] Зато постоји стоп елеменат.
[3] *Overhead*
[4] *Embeded*



Слика 10.2 Синхрони пренос

ва се са постамбулом (битском комбинацијом која означава крај). Ова комбинација битова је управљачка информација, а не подаци. Подаци, заједно са управљачком информацијом називају се рам. Тачан изглед рама зависи од тога да ли је трансмисиона шема карактер оријентисана или бит оријентисана.

Са карактер оријентисаном преносом блок података се третира као секвенца карактера (обично 10-битна). Све управљачке информације су у форми карактера. Рам започиње са једним или више синхронизационих карактера. Синхронизациони карактер (обично означен са SYN) је јединствена комбинација битова која сигнализира пријемнику да је то почетак блока. Постамбула је други јединствен карактер који се користи у истој шеми. Пријемник се поставља на блок података преко SYN карактера и прима податаке докле год се детектује карактер постамбуле. Пријемник даље може да очекује нову SYN комбинацију битова. Други приступ био би да се укључи дужина рама као део управљачких информација. Пријемник затим гледа у SYN карактер, одређује дужину рама, очитава означени број карактера, гледа када ће да се појави нови SYN карактер да би започео нови рам.

Са бит оријентисаним преносом, блок података се третира као секвенца битова. Ни податке, ни управљачке информације није потребно интерпретирати као 10-битне јединице, тј. карактере. Као и са карактер оријентисаном шемом, специјална комбинација битова сигнализира почетак блока. У бит оријентисаном преносу преамбула је 8 битова дугачка и назива се ознака о почетку рама или застава [1].

Иста ознака (флег) користи се за крај рама (постамбула). Да би сигнализирао почетак рама пријемник чека појављивање комбинације битова која означава почетак. Ово је праћено одређеним бројем управљачких поља, затим пољем података променљиве дужине, па са више управљачких поља и на крају пољем које означава крај.

За велике блокове података, синхрони пренос је ефикаснији него асинхрони. Асинхрони пренос захтева 20% премашења. У синхроном преносу поље за управљачке ин-

[1] Застава (*flag*)

формације је обично мање од 100 битова. На пример, једна од често коришћених шема бит оријентисаних протокола је HDLC[1] која садржи 48 битова управљачких информација заједно са ознакама за почетак и крај рама. За поруку од 1000 битова, премашење је само 48/1000 = 4,8%.

10.2 Типови грешака

У дигиталним системима грешке наступају када се промени бит у преносу; то значи да је послато бинарно 1 а примљена бинарна 0 и обрнуто. Две врсте грешака могу да наступе: погрешно примљен један бит и погрешно примљена група (пакет) битова.

Грешка једног бита су услови у којима је погрешан само један бит а грешка се не простире на суседне битове. Грешке могу да буду груписане и у блокове при чему су први и последњи бит погрешни а могуће је да нису сви битови у блоку погрешни.

Грешка једног бита може се јавити у присуству белог шума када мали, случајни поремећај односа сигнал-шум доведе да пријемник погрешно интерпретира један бит. Пакетске грешке су учесталије и сложеније за разрешавање. Код бежичних система пакетске грешке може да изазове импулсни шум или фединг[2].

Технике за детекцију грешке

У претходним поглављима разматрали смо пренос и ефекат односа сигнала и шума (S/N) на вероватноћу грешке (BER). Независно од пројектовања преносног система, грешке ће постојати. Уколико се чак и постигне да се термички шум значајно минимизира постоји и импулсни шум који може да генерише значајне грешке. Претпоставићемо да се подаци преносе као поворка битова груписана у рамове. Дефинисаћемо вероватноћу грешке (табела 10.1) посматрајући број грешака у примљеном раму.

Анализираћемо случај када не постоји начин да се грешке открију. Вероватноћа да се грешака открије P_3 ће бити једнака нули. Да би изразили остале вероватноће претпоставимо да је вероватноћа, да је било који бит погрешан P_b, константна и независна од битске позиције. Онда ће бити:

$$P_1 = (1 - P_b)^{N_f} \tag{10.1}$$

$$P_2 = 1 - P_1 \tag{10.2}$$

где је N_f број битова у раму.

Претходне једначине можемо речима описати на следећи начин:

- вероватноћа да се рам прими без погрешних битова смањује се што се вероватноћа грешке да се бит погрешно прими повећава (што је и за очекивати),
- вероватноћа да рам прими без погрешних битова смањује се што је рам дужи; дужи рам садржи већи број битова па је и вероватноћа да је неки од њих погрешан већа.

[1] *High-Level Data Link Control*. У 11. поглављу биће детаљно описан начин рада овог протокола.

[2] Фединг (*fading*) је слабљење сигнала на пријему које је последица суперпонирања сигнала који прелазе различите путеве (*multipath propagation*).

Ознака вероватноће	Опис
P_b	Вероватноћа да је бит погрешно примљен (BER).
P_1	Вероватноћа да рам стиже без грешке.
P_2	Вероватноћа да са примењеним алгоритмом за детекцију грешке рама стиже са једном или више недетектованих грешака.
P_3	Вероватноћа да са примењеним алгоритмом за детекцију грешке рама стиже са једном или више детектованих грешака и ниједном недетектованом грешком.

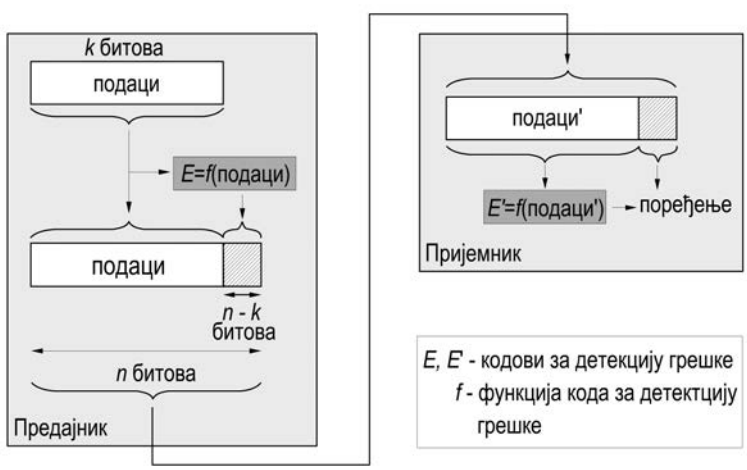
Табела 10.1 Ознаке и опис вероватноћа

Ово је врста резултата која мотивише да се користе технике за детекцију грешке. Свака од ових техника ради на следећем принципу: секвенци битова (раму података) додају се на предајној страни битови који чине кôд за детекцију грешака (слика 10.3). Кôд се израчунава као функција других осталих битова који се шаљу. Уобичајено за групу (блок) од k битова, алгоритам за детекцију грешака производи кôд за детекцију грешке од n-k битова, где је $(n-k) < k$.

Кôд за детекцију грешке се често појављује под називом и „бити за проверу". Додаје се блоку битова тако да се добија рам од n битова који се шаље. На пријемној страни раздваја се долазећи рам у k битова података и n-k битова кôда за детекцију грешке. Пријемник извршава исту операцију над битовима података и упоређује добијене вредности са пристиглом вредношћу кôда за детекцију грешке. Детектована грешка се јавља ако и само ако се појави разлика примљеног и израчунатог кода за детекцију грешке.

P_3 је вероватноћа да рам садржи грешку и да ће шема за детекцију грешке то и установити. P_2 је позната као резидуална вероватноћа грешке и представља вероватноћу да ће грешка остати неоткривена без обзира на употребу шеме за детекцију грешке.

Анализирајмо конкретан пример, једну ISDN везу. Дефинисани циљ ISDN везе је да BER у 64kb/s каналу треба да буде мања од 10^{-6} у најмање 90% посматраног једноминутног интервала.



Слика 10.3 Процес детекције грешке

Претпоставимо да имамо релативно умерене захтеве корисника:

- један рам са неоткривеном битском грешком појавиће се дневно у 64kb/s каналу који се непрекидно користи,
- рам је дужине 1000 битова.

Број рамова који се може дневно послати је $5,529*10^6$ што даје вероватноћу грешке рама:

$$P_2 = 1/ (5,529* 10^6) = 0,18*10^{-6}$$

Уколико претпоставимо да је вероватноћа грешке $P_b = 10^{-6}$ онда је $P_1 = (0,999999)^{1000} = 0,999$ и зато $P_2 = 10^{-3}$, што је за три реда величине веће од вредности која задовољава наше захтеве.

Контрола парности

Најједноставнија техника за детекцију грешке је поступак у коме се додаје бит парности на крају сваке речи у раму. Типичан пример је пренос ASCII[1] карактера, у коме се бит парности додаје сваком 7 битном ASCII карактеру. Вредност овог бита бира се тако да целина (ASCII карактер и бит парности) садржи паран[2], или непаран[3] број јединица. Побољшање се може постићи коришћењем скупа битова парности, као што је илустровано сликом 10.4. Рам је представљен као блок карактера распоређен у две димензије. Сваком карактеру (K_i) додат је бит парности (y_i) као и раније. Поред тога, бит парности се генерише за сваку битску позицију кроз све карактере. Тако се генерише додатни карактер (Z), у коме је *i*-ти бит додатног карактера бит парности свих *i*-тих битова свих карактера у блоку.

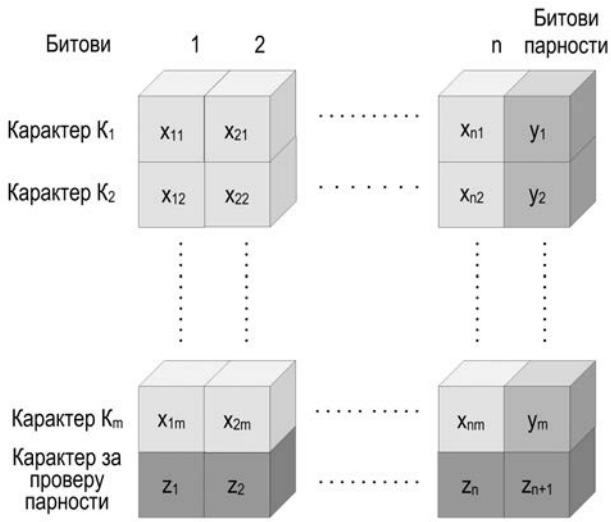
Циклична провера

Да би се достигла даља побољшања, може се користити врло моћан, али једноставан полиноминални кôд који се среће и под називом циклична редундантна провера (CRC[4]). Полиноминални кôд третира поворку битова као полином са коефицијентима 0 и 1. Рам од *k* битова се сматра листом коефицијената полинома са *k* чланова почевши од x^{k-1} до x^0. За такав полином се каже да је степена *k-1*. Бит највеће тежине (крајње леви) је коефицијенат члана x^{k-1}; следећи бит је коефицијенат од x^{k-1} и тако даље. На пример, 110001 има 6 битова и представља шесточлани полином са коефицијентима 1, 1, 0, 0, 0 и 1: $x^5 + x^4 + x^0$.

За дељење полинома користи се аритметика по модулу 2. Не постоји пренос за операцију сабирања или позајмљивање за операцију одузимања. И сабирање и одузимање су идентични логичкој операцији ексклузивно ИЛИ. На пример:

```
  1111        1111          11001
+ 1011      - 0101        x    11
------      ------        -----
  0101        1010          11001
                          11001
                          ------
                          101011
```

[1] IRA
[2] *Even parity*
[3] *Odd parity*
[4] *Cyclic Redundancy Check*



Слика 10.4 Вертикална и хоризонтална (лонгитудинална) провера

Дугачка дељења остварују се на исти начин као и бинарна с тим што је одузимање по модулу 2, као у претходном примеру. За делилац се каже да „одговара" дељенику ако дељеник има исти број битова као и делилац.

Када се користи метод са полиноминалним кôдом предајник и пријемник се морају договорити унапред око полинома *P(x)*. Битови највишег и најнижег реда морају бити јединице. Да би се израчунао контролни збир за неку поруку *D* од *k* битова који одговарају полиному *M(x)* полином мора да буде дужи од полинома *P(x)*. Идеја је да се дода контролни збир[1] (сума) на крај рама на такав начин да је полином који је представљен рамом са контролним збиром дељив са *P(x)*. Када пријемник добије рам са контролним збиром он га дели са *P(x)*. Уколико постоји остатак при дељењу то значи да је дошло до грешке у преносу. Уколико желимо да нема остатка при дељењу *T/ P* онда је јасно да је:

$$T = 2^{n-k} D + F \tag{10.3}$$

Тако смо множењем *D* са 2^{n-k} извршили померање за $n-k$ места и проширили резултат са нулама. Желимо да *T* буде тачно дељив са *P*. Претпоставимо да делимо $2^{n-k} D$ са *P*:

$$\frac{2^{n-k} D}{P} = Q + \frac{R}{P} \tag{10.4}$$

Пошто је реч о дељењу по модулу 2, остатак је увек најмање један бит краћи од делиоца. Остатак користимо као контролну суму:

$$T = 2^{n-k} D + R \tag{10.5}$$

Поставља се питање да ли количник *T/ P* нема остатка?

[1] *Checksum*

$$\frac{T}{P} = \frac{2^{n-k}D + R}{P} = \frac{2^{n-k}D}{P} + \frac{R}{P} \tag{10.6}$$

Користећи једначину 10.4 добијамо:

$$\frac{T}{R} = Q + \frac{R}{P} + \frac{R}{P} = Q + \frac{R+R}{P} = Q \tag{10.7}$$

Види се да нема остатка и да је *T* дељиво са *P*. Алгоритам за израчунавање контролне суме је следећи:

1. Нека је *n-k* степена полинома *P(x)*. Додаје се *n-k* битова нулте вредности као битови мање тежине тако да новонастали рам садржи *n* битова. Проширивање рама за *n-k* битова одговара полиному $x^{n-k}\ M(x)$.
2. Поделити поворку битова која одговара полиному $x^{n-k}\ M(x)$ поворком битова која одговара полиному *P(*(x) користећи дељење по модулу 2.
3. Одузети остатак (који је највише *n-k* битова) од поворке битова који одговарају $x^{n-k}\ M(x)$ користећи одузимање по модулу 2. Резултат је рам T са контролном сумом, који се може послати.

Слика 10.4 илуструје израчунавање контролне суме рама 1010001101 користећи делитељ $P(x)=x^5 + x^4 + x^2 + 1$. Јасно је да је *T(x)* дељиво (по модулу 2) са *P(x)*. Уколико се дељеник умањи за остатак при дељењу оно што преостане јдељиво е са делиоцем. На пример код дељења у декадном бројном систему[1] када број 378 поделимо са 135, остатак је 8. Ако од 378 одузмемо 8 оно што је преостало (370) је дељиво са 135.

Анализирајмо овај метод. Која врста грешака се може детектовати? Замислимо да се јављају грешке у преносу и да уместо поворке битова *T(x)* стиже поворка *T(x)* + *E(x)*. Сваки бит 1 у *E(x)* одговара биту који је оригиналној поворци *T(x*) инвертован. Уколико у поворци *E(x)* постоји *k* јединица (битова са вредношћу 1), појавиће се *k* битских грешака у поворци *T(x)*. Једна пакетска грешка је карактерисана са иницијалном[2], комбинацијом 0 и 1, на крају 1, са свим осталим битовима ван те целине који су 0.

На пријемној страни рам са контролном сумом се дели са *P(x).* Значи да се израчунава [*T(x)* + *E(x)*] /*P(x)*. Количник *T(x)* / *P(x)* има вредност 0, па се резултат израчунавања своди само на количник *E(x)* / *P(x)*. Оне грешке које се појаве у полиному који садржи *P(x)* као чинилац остаће неоткривене; остале грешке биће откривене.

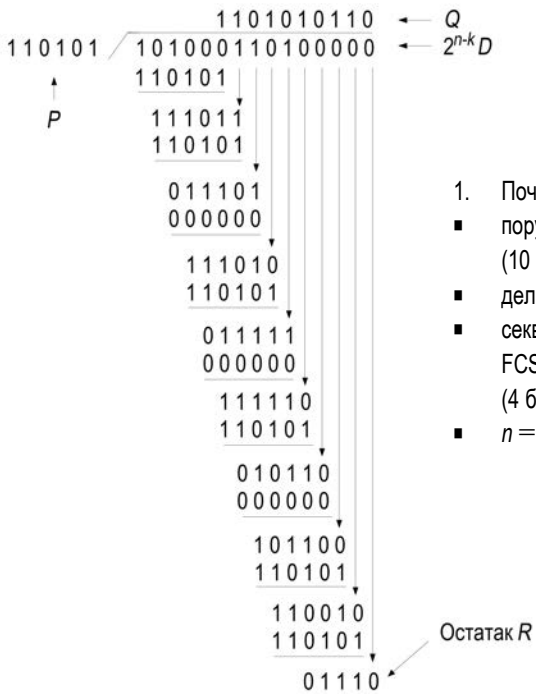
Уколико постоји грешка у једном биту онда је $E(x)=x^i$, где и дефинише који бит је погрешан. Уколико *P(x)* садржи два или више члана, *E(x)* неће бити дељив тако да ће све грешке једном биту бити откривене.

Уколико су се појавиле две изоловане грешке по једном биту, $E(x)=x^i + x^j$ где је $j < i$. Ово се може написати и на други начин: $E(x)=x^j\ (x^{i-j} + 1)$. Уколико претпоставимо да *P(x)* није дељив са *x* довољан услов да се све двоструке грешке открију је да x^{k+1} није дељив са *P(x)* за *k* све до максималне вредности *i-j* (максималне дужине рама).

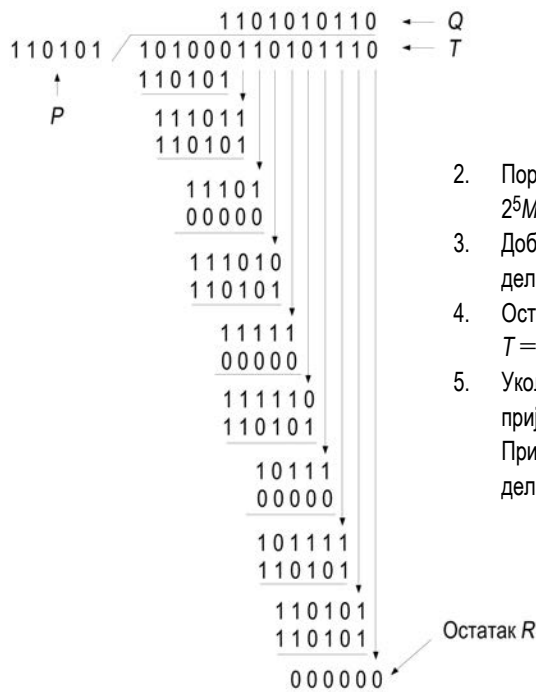
Уколико постоји непаран број битова који су погрешни, *E(x)* садржи непаран број чланова (на пример $x^5 + x^2 + 1$, али не $x^2 + 1$). Интересантно је да не постоји полино-

[1] Основа је 10

[2] Уколико је у поворци *T(x)* нека битска позиција имала вредност 1 сабирањем са 1 одговарајуће битске позиције у поворци *E(x)* добије се 0. Уколико је вредност била 0 постаје 1.



1. Почетни услови:
   - порука $M = 1\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 1$ (10 битова),
   - делитељ $P = 1\ 1\ 0\ 1\ 0\ 1$ (6 битова),
   - секвенца P за проверу поруке (рама) FCS[1] = која ће бити израчуната (4 бита)
   - $n = 15$, $k = 10$ и $(n - k) = 5$



2. Порука се множи са 2^5 и добија се $2^5M = 11010110110000$
3. Добијени производ дели се са делитељом $P = 110101$
4. Остатак се додаје 2^5M и добија се $T = 1011000110101110$
5. Уколико нема никакве грешке пријемник прима неизмењену поруку. Пријемна порука се дели са делитељем $P = 110101$

Слика 10.5 Израчунавање контролне суме за полиноминални кôд

[1] *Frame Check Sequence*

ма са непарним бројем чланова који има $x+1$ као чинилац (у аритметици по модулу 2). Обезбеђујући да је $x+1$ један од чинилаца $P(x)$, можемо пронаћи све грешке које се састоје од непарног броја инвертованих битова.

Да бисмо видели да је полином са непарним бројем чланова дељив са $x+1$ претпоставимо да $E(x)$ садржи непаран број чланова и дељив је са $x+1$. Раставићемо $E(x)$ на чиниоце: $(x+1)J(x)$. Израчунаћемо $E(1)=(1+1)J(1)$. Пошто је $1+1=0$ (по модулу 2), $E(1)$ мора да буде нула. Уколико $E(x)$ има непаран број чланова, замена сваког x са 1 као резултат увек ће дати 1. Тако, ниједан полином са непарним бројем чланова није дељив са $x+1$.

На крају, и најважније, полиноминални кôд са r контролних битова детектоваће све пакетске грешке дужине $\leq r$. Пакетска грешка дужине k може се представити са $x^i (x^{k-1}+...+1)$, где и одређује колико далеко од крајње десне позиције је лоцирана пакетска грешка. Уколико $P(x)$ садржи члан x^0, онда неће имати x^i као чинилац. Ако је степен израза у загради мањи од степена $P(x)$, остатак не може никада да буде нула.

Уколико је пакетска грешка дужине $r+1$, остатак при дељењу са $P(x)$ биће нула ако и само ако је пакетска грешка идентична са $P(x)$. По дефиницији пакетске грешке први и последњи бит морају да буду 1, тако да ли одговарају зависи од $r-1$ међубитова. Уколико се све комбинације сматрају једнако вероватним, вероватноћа да се прихвати погрешан рам као важећи је $(1/2)^{r-1}$. Може се такође показати да када се појави пакетска грешка дужа од $r+1$ битова, или када се појави више краћих пакетских грешака, вероватноћа да промакне рам са неоткривеним грешкама је $(1/2)^r$ уз претпоставку да су сви узорци битова једнако могући. Неки од полинома постали су интернационални стандар. Један од њих који користи IEEE802 стандард је полином:

$$x^{32}+x^{26}+x^{22}+x^{32}+x^{16}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x^1+1$$

Овај полином између осталог има особину да може да открије све пакетске грешке дужине 32 или мање и све грешке које су деловале на непаран број битова.

Иако захтевано израчунавање контролне суме изгледа компликовано, Петерсон и Браун [1] показали су да се једноставан померачки регистар може искористити за хардверско израчунавање и проверу контролне суме. У пракси се овај хардвер готово увек и користи и то у свим локалним рачунарским мрежама као и тачка-тачка везама.

Деценијама се претпостављало да рамови за које треба израчунати контролну суму садрже случајне битове. Све анализе алгоритама за израчунавање контролних сума полазиле су од ове претпоставке. Посматрањем стварних података констатовало се да је ова претпоставка потпуно погрешна. Последица тога је да су под одређеним условима недетектоване грешке много чешћа појава него што се то до сада сматрало.

10.3. Интерфејси

Већина дигиталних модула има ограничену способност преноса. Типично, они генеришу једноставне дигиталне сигнале, који су обично типа NRZI а растојање преко којих могу да преносе податке је ограничено. Ретко је да се таква опрема везује директно за преносни систем.

[1] *Peterson, Brown* (1961)

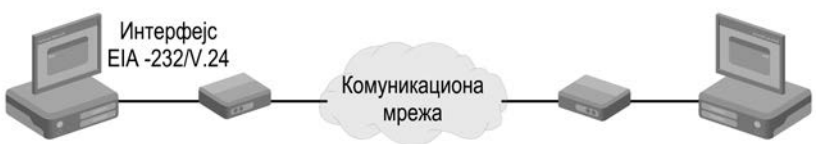
Уобичајена ситуација приказана је на слици 10.6. Опрема коју анализирамо укључује терминале и рачунаре и означава се DTE[1]. Она користи преносни систем посредством DCE[2]. Као пример последњег је модем. На једној страни DCE је одговоран за предавање и примање битова са преносног медијума. На другој страни DCE мора да буде у вези са DTE. Да би се то остварило потребан је пренос и података и управљачких информација преко скупа линија које се називају кола за размену[3]. Два DCE морају да разумеју један другог, што значи да пријемник једног DCE-а мора да користи исту шему кодирања (на пример Манчестер или PSK) као предајник другог DCE-а. Поред тога сваки пар DTE-DCE мора да буде пројектован тако да ефикасно обави интеракцију. Да би се поједноставио овај процес развијени су стандарди који специфицирају тачну природу интерфејса DTE-DCE. Ови стандарди су познати и као протоколи физичког слоја и обухватају први слој OSI референтног модела.

У овом делу анализираћемо природу и функционалност овог интерфејса. Интерфејс има четири битне карактеристике:

- механичке,
- електричне,
- функционалне,
- процедуралне.

Механичке карактеристике односе се на стварну физичку везу DTE-DCE. Типично, сигнал и управљање воде се каблом који се завршава утичницама[4]. На сваком крају се DTE и DCE морају физички повезати преко каблова и утичница супротног типа. Електричне карактеристике односе се на напонске нивое и тренутке времена у којима долази до

а) Општи модели интерфејса ка трансмисионом медијум



б) Уобичајена конфигурација

Слика 10.6 Интерфејс ка трансмисионом медијуму

[1] *Data Terminal Equipment* - опрема терминала података
[2] *Data Circuit Termination Equipment* - опрема за завршетак кола података
[3] *Interchange Circuit*
[4] Конектори, тзв. мушки и женски

промене напона. И DTE и DCE морају користити исти кôд (нпр. NRZI), морају користити исте напонске нивое и морају користити исто трајање сигнализационих елемената. Ове карактеристике одређују брзину преноса података и растојање које се може остварити.

Функционалне карактеристике специфицирају функције које се извршавају доделом значења колима за међусобну размену сигнала. Функције се могу класификовати у следеће категорије:

- подаци,
- управљање,
- временски распоред и
- уземљење.

Процедуралне карактеристике дефинишу редослед догађаја за слање података заснован на функционалним карактеристикама интерфејса. Постоји велики број стандарда који се односе на интерфејсе. У овом поглављу описаћемо један од њих: V.24/EIA-232-F.

10.4 Стандард V.24/EIA-232-F

Највише коришћени стандард за интерфејсе је ITU-T стандард V.24. У ствари стандард само специфицира функционални и процедурални део интерфејса. Стандард V.24 се референцира на друге стандарде када су у питању електрични и механички део интерфејса. У САД постоји спецификација EIA-232-F која одговара V.24 стандарду. Стандарди на које се V.24 ослања су следећи:

- механички - ISO 2110,
- електрични -V.28,
- функционални -V.24,
- процедурални -V.24.

Прву верзију спецификацију EIA-232 је 1962. године издала организација EIA [1] под ознаком RS-232. Најновија верзија чија је ознака EIA-232-F појавила се 1997. године. Текуће верзије стандарда V.24 и V.28 појавиле су се 1998. и 1993. године. Овај интерфејс користи се за прикључивање DTE опреме за модеме телефонских канала [2]. Такође се користи и за друге врсте међусобног повезивања.

Механичка спецификација

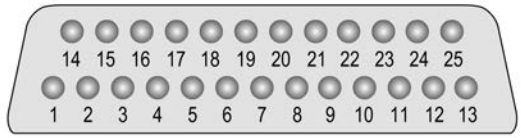
Механичка спецификација EIA-232-F је представљена на слици 10.7. То је 25-пински конектор дефинисан у стандарду ISO2110. Овај конектор је прикључак 25-жичног кабла који се може користити да би се повезали DTE (терминал) и DCE (нпр. модем). У пракси се користи кабл са мање жица.

Електрична спецификација

Електричне карактеристике означавају сигнализацију између DTE и DCE опреме. У свим колима за размену користи се дигитална сигнализција. Конвенција је да се (уз изузетак заједничког уземљења) напон негативнији од -3V интерпретира као бинарно

[1] *Electronic Industries Alliance*

[2] Када се каже телефонски канал, или говорни канал, мисли се на канал за говор који се користи у јавним телефонским мрежама.



Слика 10.7 V.24 / EIA-232 конектор

1, а напон позитивнији од +3V интерпретира као бинарно 0. Брзина на интерфејсу мања је од 20kb/s и раздаљина од 15m. Исти напонски нивои користе се за управљачке сигнале: напон негативнији од - 3V интерпретира се као искључење, а напон позитивнији од +3V интерпретира се као укључење.

Функционална спецификација

Функционални спецификација најважнијих кола за размену дата су у табели 10.2. Кола се могу груписати у следеће категорије: подаци, управљање, временски редослед и уземљење. Постоји по једно коло за податке у сваком правцу тако да је могућ потпуни дуплекс. Када уређај ради у полудуплексу постоји и додатно секундарно коло за податке. У датом тренутку је у полудуплексном раду размена података између два DTE-а (преко DCE-а и одговарајућих комуникационих веза) само у једном правцу. Постоји потреба да се ка уређају који шаље податке пошаљу поруке о контроли тока или о прекиду рада. Због тога се обезбеђује повратни канал обично много мање брзине података. На DTE-DCE интерфејсу повратни канал се води посебним паром линија за податке.

Постоји 16 управљачких кола од којих је првих 10 везано за пренос података преко примарног канала (табела 10.2). За асинхрони пренос користи се шест кола (105, 106, 107, 108.2, 125, 109). Њихова намена биће касније објашњена.

У синхроном преносу се поред ових шест кола користе и три додатна управљачка кола. Коло детектор „квалитета сигнала"[1] поставља (укључује) DCE опрема да би показала да ли је квалитет телефонске линије опао испод дефинисаног прага. Модеми подржавају пренос на различитим брзинама тако да када дође до повећања сметњи у телефонској линији могу да пређу на пренос мањом брзином. За промену брзине користи се коло за одабир брзине преноса[2]. Било који крај везе и DTE и DCE може да иницира промену. Коло 133 омогућава пријемнику да проток података у колу 104 искључи или укључи. Три управљачка кола (120, 121, 122) користе се за управљање секундарним каналом. Он се може користи као повратни канал или за неку другу намену.

Последња група управљачких сигнала користи се за тестирање у затвореној петљи и омогућава DTE крају везе да преко DCE краја везе изврше тестирање. Ова кола су од великог значаја код модема или других DCE уређаја који подржавају тестирање у затвореној петљи. У раду са затвореном петљом предајни излаз модема везује се за пријемни улаз, тако да је модем одвојен (откачен) са линије. Подаци које генерише кориснички уређај шаљу се модему и враћају корисничком уређају. Код удаљене затворене петље локални модем повезан је за преносни систем на уобичајени начин, а при-

[1] *Signal Quality Detector*
[2] *Data Signal Rate Selector*

јемни излаз удаљеног модема повезан је на предајни улаз. За време оба теста DCE укључује коло за тестирање [1]. Слика 10.8 илуструје употребу кола која су везана за тестирање у затвореној петљи. Тестирање у затвореној петљи веома је корисно за проналажење грешака.

Временски сигнали обезбеђују такт импулсе за синхрони пренос. Када DCE шаље синхроне податке преко кола за пријем података RD [2] (104) он шаље и транзи-

V24	EIA-232	Име	Усмерен ка	
Сигнали података				
103	BA	Слање података *Transmitted data*	DCE	Шаље DTE
104	BB	Пријем података *Received data*	DTE	Прима DTE
118	SBA	Секундарно слање података *Secondary transmitted data*	DCE	Шаље DTE
119	SBB	Секундарни пријем података *Secondary received data*	DTE	Прима DTE
Управљачки сигнали				
105	CA	Захтев за слањем *Request to send*	DCE	DTE жели да шаље
106	CB	Спреман за слање *Clear to send*	DTE	DTE је спреман да прима, одговара на RTS
107	CC	DCE је спреман DCE *Ready*	DCE	DCE је спреман за рад
108.2	CD	DTE је спреман DTE *Ready*	DTE	DTE је спреман за рад
125	CE	Индикатор звоњења *Ring Indicator*	DTE	DCE прима сигнал звоњења
109	CF	Детектор сигнала на пријемној линији *Received Line Signal Detector*	DTE	DCE прима сигнал са одговарајућим ограничењима у каналу
110	CG	Детектор квалитета сигнала *Signal quality detector*	DTE	Указује да постоји велика вероватноћа грешке у примљеним подацима
111	CH	Селектор брзине података *Data Signal Rate Selector*	DCE	Селектује једно од две брзине података
112	CI	Селектор брзине података *Data Signal rate selector*	DTE	Селектује једно од две брзине података
133	CJ	Спреман за слање *Ready for receiving*	DCE	Укључена/искључена контрола тока
120	SCA	Секундарни захтев за слањем *Secondary request to send*	DCE	DTE жели да шаље преко повратног канала
121	SCB	Секундарни спреман за слање *Secondary clear to send*	DTE	DCE жели да прима преко повратног канала
122	SCF	Детектор сигнала на секундарној пријемној линији *Secondary received line signal detector*	DTE	Исто као 109, за повратни канал
140	RL	Удаљена затворена петља Remote loopback	DCE	Указује удаљеном DCE да направи затворену петљу
141	LL	Локална затворена петља *Local loopback*	DCE	Указује DCE-у да направи затворену петљу за сигнал
142	TM	Врста рада - тестирање *Test mode*	DTE	Локални DCE је у стању тестирања

[1] *Test Mode*
[2] *Received Data*

V24	EIA-232	Име	Усмерен ка	
Временски сигнали				
113	DA	Временски распоред предајних сигнализационих елемената *Transmitter signal element timing*	DCE	Такт сигнал; транзиција на укључено (ON) и искључено (OFF) се јавља у средини сваког сигнализационог елемента
114	DB	Временски распоред предајних сигнализационих елемената *Transmit signal element timing*	DTE	Такт сигнал; и 113 и 114 се односе на сигнале у колу 103
115	DD	Временски распоред предајних сигнализационих елемената *Receiver signal element timing*	DTE	Такт сигнал за коло 104
Уземљење				
102	AV	Уземљење / заједничка маса *Signal ground/common return*	DCE	Заједничко уземљење се односи на сва кола

Табела 10.2 Кола за размену V.24 / EIA-232-F

цију са 1-0 и 0-1 по колу REST[1] (115). Транзиција је постављена на средини сваког RD сигнализационог елемента. Када DTE шаље синхроне податке, у зависности од услова, било DTE или DCE могу да обезбеде временске импулсе.

На крају сигнал уземљење/сигнална маса (102) служи као повратно коло за све линије података. Тако, пренос је асиметричан[2] са само једном активном жицом.

Спецификација процедура

Спецификација процедура дефинише секвенце догађаја у којима се користе различита кола за одређену намену. У овом делу биће описано неколико примера. Први пример је веома уобичајен код повезивања два уређаја на кратким растојањима у оквиру једног објекта (зграде). Познат је као асинхрони линијски модем или модем ограниченог растојања. Асинхрони модем прихвата сигнале од DTE-а, као што су терминал или рачунар, претвара их у аналогне сигнале и шаље преко преносног медија као што је на пример упредена парица.

На другом крају линије асинхрони модем прихвата долазећи аналогни сигнал, претвара га у дигитални и прослеђује терминалу или рачунару на свом крају. Наравно размена података је двострана. У овом једноставном примеру потребна су следећа кола за размену (табела 10.2):

- Сигнал уземљења (102);
- Предајни подаци (103);
- Пријемни подаци[3] (104);
- Захтев за слањем[4] (105);
- Спреман за слање[5] (106);

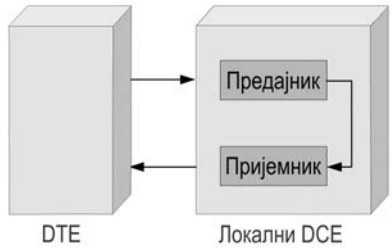
[1] *Receiver Element Signal Timing*

[2] Користи се и термин небалансиран. Балансиран (симетричан пренос) подразумева да се користе две линије за вођење сигнала. Пријемник посматра разлику сигнала између те две линије. На тај начин се резултати сметњи које се при преносу јављају у обе жице међусобно потиру.

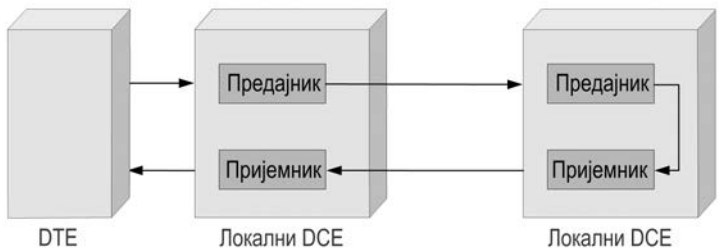
[3] *Received Data* - RD

[4] *Request to Send* - RTS

[5] *Clear to Send* - CTS



а) Тестирање у локалној затвореној петљи



б) Тестирање у удаљеној затвореној петљи

Слика 10.8 Локална и удаљена затворена петља

- DCE је спреман (107);
- Детектор пријемног линијског сигнала [1] RLSD (109).

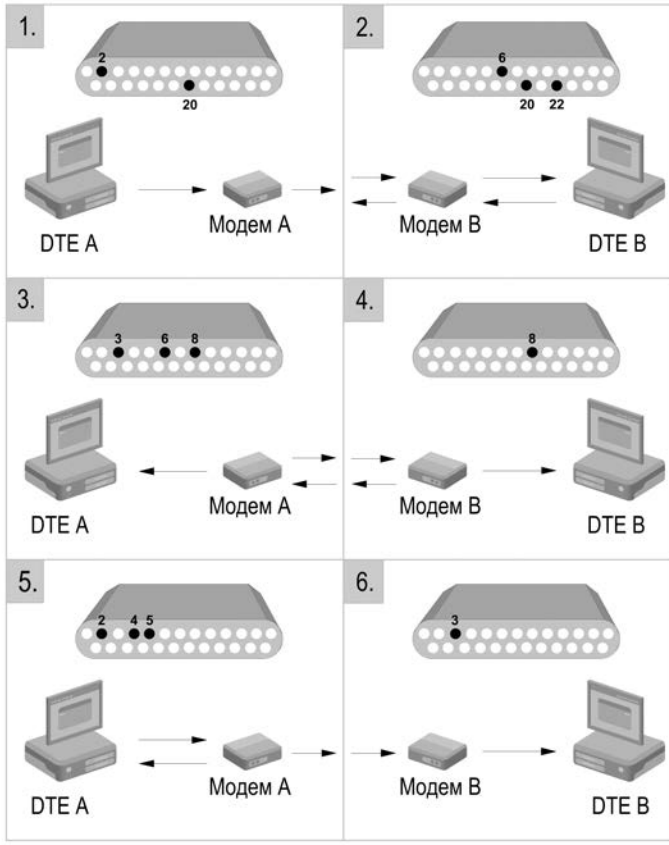
Када је модем (DCE) укључен и спреман за рад, он то потврђује постављањем константног негативног напона на линији „DCE је спреман". Када је DTE спреман да шаље податке (корисник терминала је послао карактер) активира RTS. Модем, када је спреман, одговара активирањем CTS указујући да се подаци могу послати преко линије за слање података (TD). Уколико је договорен полудуплексни начин рада онда RTS спречава пријем. Сада DTE може да шаље податке преко линије за слање података (TD). Када подаци стигну од удаљеног модема локални модем активира линију RLSD да би указао да удаљени модем испоручује податке по пријемној линији RD. Треба уочити да није неопходно користити коло за синхронизацију [2] пошто је у питању асинхрони пренос.

Кола која су поменута довољна су за рад модема на изнајмљеним тачка-тачка линијама. Када се модеми користе за пренос преко јавне телефонске мреже захтевају се додатна кола. Иницијатор везе мора, користећи јавну телефонску мрежу, прво да позове одредишни уређај. Користе се следеће линије:

- DTE је спреман [3] (108.2);
- Индикација звоњења [4] (125).

Користећи ове две додатне линије, систем DTE-модем може ефикасно да користи јавну телефонску мрежу на начин сличан ономе како се користи за телефонске разговоре.

[1] *Received Line Signal Detector* - RLSD
[2] *Timing Circuit*
[3] DTE *Ready* - DTER
[4] *Ring Indicator* - RI



Слика 10.9 Рад V.24 / EIA-232-F интерфејса преко комутиране линије

На слици 10.9 представљени су кораци у случају комутиране [1] полудуплекс везе. Када се започне позив, било ручно или аутоматски, телефонска централа шаље сигнал звоњења. Телефон се оглашава звоњењем, модем одговара постављањем индикатора звоњења RI. Особа одговара на позив подизањем слушалице; DTE реагује активирањем DTE спреман (DTER). Особа која је одговорила очекује глас онога ко је позвао и ако ништа не чује прекида везу. DTE ће пратити да ли је постављен RLSD чиме модем указује да је сигнал присутан. Уколико линија није активна DTE ће оборити DTER. Како може ова последња ситуација да се догоди? Један једноставан начин је да особа случајно бира број модема. То активира DTE модема, али када се не појави носилац DTER се укида.

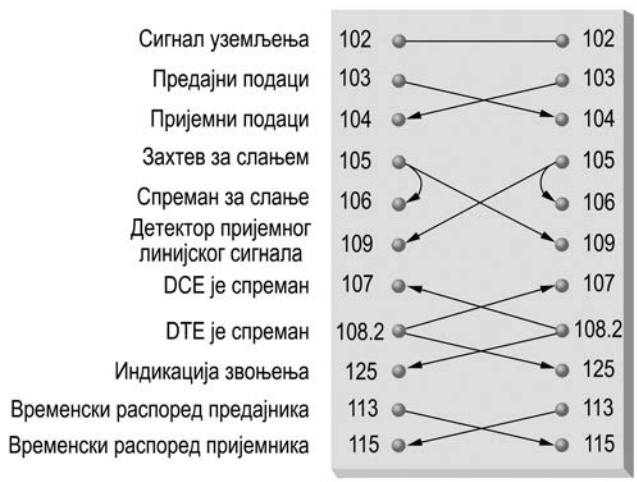
Кораци у комуникацији представљеној на слици 10.9 су следећи:

1. DTE A активира прикључак DTER [2] (20) да би наговестио модему да хоће да започне размену података. Док је овај сигнал подигнут DTE A шаље телефонски број преко линије на прикључак TD [3] (2) ка модему A који ће бирати тај број.

[1] *Dial up*
[2] *Data Terminal Ready* - DTE спреман
[3] *Transmit Data*

2. Када модем B обавести свој DTE о долазећем позиву преко прикључка звоњења RI[1] (22), DTE B активира DTER (20). Модем B затим генерише носећи сигнал, који ће се користити у међусобној размени и активира сигнал на прикључку (6) да укаже на своју спремност да прими податке.
3. Када модем A детектује носећи сигнал, он обавештава DTE A преко прикључка 8. Модем такође указује DTE-у да је успостављена линија (6) и да је дозвољено слање. Модем ће послати поруку ка DTE-у преко пријема података RD[2] (3) (ако је тако програмиран).
4. Модем A генерише свој сопствени носећи сигнал ка модему B, и поставља обавештење (8)[3].
5. Када жели да пошаље податке DTE A активира захтев за слањем RTS[4] (4). Модем A одговара активирањем прикључка спреман за слање CTS[5] (5). DTE A шаље податке (импулсе који представљају 1 и 0) ка модему A преко прикључка за слање података TD[6] (2). Модем A импулсе претвара у аналогно модулисани сигнал и шаље га на линију.
6. Модем B претвара примљени аналогни сигнал у дигитални и шаље га преко прикључка за пријема података RD[7] (3) ка DTE B.

Потребно би било размотрити ситуацију у којој је раздаљина између два DTE толико мала да могу директно да комуницирају. У том случају кола за размену V.24/EIA-232-F могу се и даље користити, али не постоји потреба за DCE опремом. Да би такав



Слика 10.10 Пример нул модема

[1] *Ring Indicator*
[2] *Received Data*
[3] Пошто не добија сигнал носиоца од B (као у 3) због полудуплексне везе модем A „лаже" свој DTE да DTE није „послао", да нема сигнала на линији.
[4] *Request To Send*
[5] *Clear To Send*
[6] *Transmit Data*
[7] *Received Data*

систем могао да ради, потребан је нул модем [1] који повезује линије на такав начин да је сваком DTE-у представљено као да је везан на модем (слика 10.10).

10.5 Интерфејс у дигиталним мрежама интегрисаних услуга

Велика разноликост функција које обезбеђује V.24/EIA-232-F интерфејс су последица употребе великог броја кола за размену што је скуп начин да се дође до решења. Друга могућност је обезбедити само неколико кола али додати више логике на DTE и DCE интерфејсима. Падом цена логичких кола овакав приступ могуће је реализовати. Овај приступ је прихваћен код X.21 стандарда као интерфејс ка јавној телефонској мрежи и направљена је спецификација за конектор са 15 прикључака [2]. За дигиталну мрежу интегрисаних услуга (ISDN [3]) специфициран је конектор са 8 прикључака (контакта). У овом одељку анализираћемо физички интерфејс дефинисан за ISDN мрежу.

Физичке везе

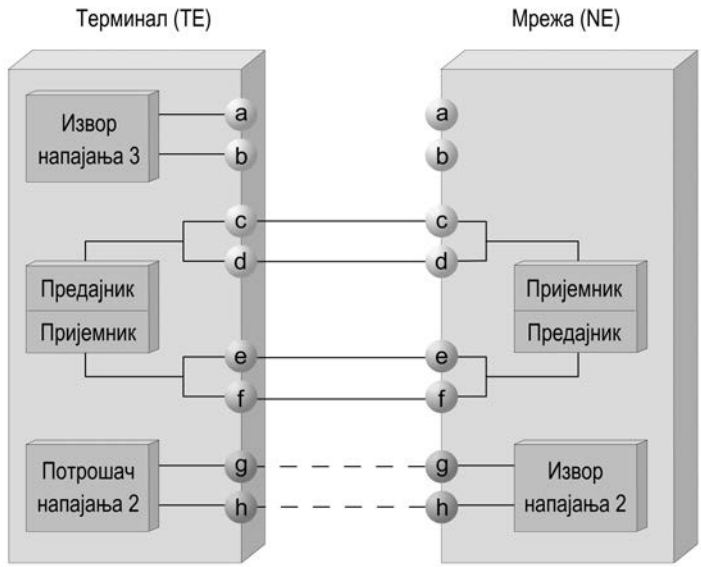
У дигиталној мрежи интегрисаних услуга физичка веза се остварује између терминалске опреме (TE [3]) и опреме мрежних завршетака (NT [4]). Физичке везе, описане у ISO8877, специфицирају како се NT и TE каблови завршавају на одговарајућим конекторима.

Слика 10.11 приказује распоред прикључака за осам линија на оба краја NT-TE везе. Два прикључка се користе за пренос података у оба правца. Ови прикључци се користе да повежу упредене парице које долазе од NT и TE уређаја. Пошто не постоје специфична функционална кола онда се кола предаја/пријем користе за пренос података и управљачких сигнала. Управљачке информације шаљу се у форми порука. Спецификацијом је предвиђена могућност преноса напајања преко интерфејса. Правац преноса напајања зависи од примене. Уобичајена примена је да мрежа обезбеђује напајање терминалу за основне телефонске услуге када на страни терминала дође до нестанка напајања. Пренос напајања може се остварити преко истих приступних тачака као и пренос дигиталних сигнала (*c*, *d*, *e*, *f*) или додатних проводника користећи приступне тачке *g* и *h*. У дигиталној мрежи интегрисаних услуга преостала два проводника се не користе, али могу бити корисна у другим конфигурацијама.

Електрична спецификација

Електрична спецификација за дигиталне мреже интегрисаних услуга захтева употребу симетричног (балансираног [5]) преноса. Сигнал се преноси по линији (као што су на пример упредене парице) која се састоји од два проводника. Када је реч о дигиталним сигналима ова техника се назива диференцијална сигнализација пошто бинарну вредност одређује знак напонске разлике сигнала из два проводника. Асиметрични (небалансирани [6]) пренос који се користи код EIA-232-F користи један проводник за вођење сигнала и масу [7].

[1] *Null Modem*
[2] *Terminal Equipment*
[3] *Integrated Services Digital Network*
[4] *Network Terminating Equipment*
[5] *Balanced*
[6] *Unbalanced*
[7] *Ground*



Слика 10.11 ISDN интерфејс

Симетричан начин може да толерише већи и производи мањи шум. Идеално посматрано интерференције на симетричној линији делују на исти начин на оба проводника и неће утицати на напонску (струјну) разлику. Пошто асиметрични пренос нема овакву предност он се обично користи само код коаксијалних каблова. Када се користи код кола за размену као што је EIA-232-F, ограниченог је домета.

Техника кодирање која се користи на физичком интерфејса у ISDN мрежама зависи од брзине података. За базни приступ [1] (192kb/s) стандард специфицира употребу псеудотернарних кодова (слика 5.6). Бинарно 1 је представљено одсуством напона, а бинарно 0 је представљено позитивним или негативним импулсом 750mV ± 10%. За примарни ISDN [2] постоје две верзије: 1,544Mb/s са кôдом B8ZS и 2,048Mb/s са кôдом HDB3.

[2] *BISDN Basic rate ISDN*
[3] *PISDN Primary rate ISDN*

11. Управљање слојем везе

У претходним поглављима разматрали смо слање сигнала преко трансмисионог медијума. За ефикасни дигитални пренос података потребни су и надзор и управљање разменом података. У овом поглављу анализираћемо слање података преко комуникационе везе. Да би се то постигло потребно је поред физичког интерфејса додати целину која се означава као слој за управљање везом и представља се као 2. слој у OSI референтном моделу. Протокол који се користи за комуникацију ових целина назива се протокол за управљање везом [1]. Да бисмо уочили потребу за управљањем везом набројаћемо неке захтеве и поставке за ефикасну комуникацију између две директно повезане предајно-пријемне станице:

- Синхронизација рама: подаци се шаљу у блоковима који се називају рамови. Почетак и крај сваког рама мора да буде идентификован. Користе се различите линијске конфигурације.
- Контрола тока: станица која шаље рамове не сме то да ради брже него што пријемна станица може да их прими.
- Контрола грешака: битске грешке које уносе трансмисиони системи треба да буду детектоване а ако је могуће и исправљене.
- Адресирање: на линији са више станица идентитет станице која учествује у комуникацији мора да буде познат.
- Управљање и подаци на истој вези: обично није препоручљиво имати одвојене комуникационе путеве за управљачке сигнале. Као последица тога важно је да пријемник мора да буде у могућности да разликује управљачке информације од података који се преносе.

Иницирање, одржавање и завршетак подржаног преноса података захтева значајну координацију и кооперацију између станица. Потребне су процедуре управљања. Ниједна од ових карактеристика није задовољена физичким интерфејсом који су до сада анализирани.

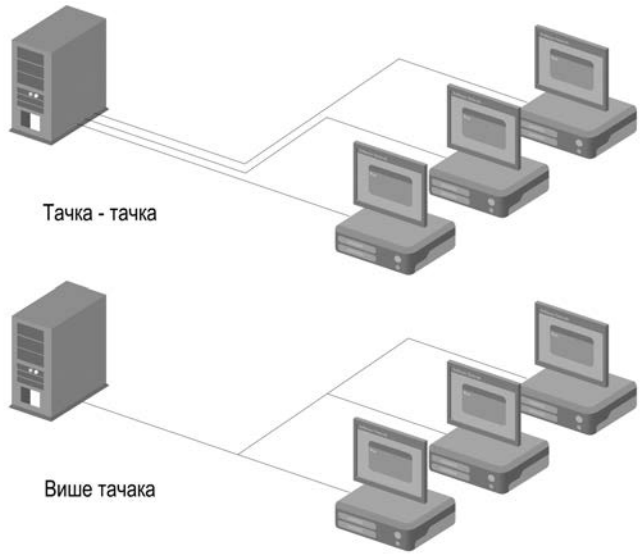
11.1 Линијска конфигурација

Три особине су карактеристичне за различите линијске конфигурације и то су: топологија, дуплексност и линијска дисциплина.

Топологија и дуплексност

Топологија везе односи се на физичко организовање станица на вези. Уколико постоје само две станице које користе исти трансмисиони медијум онда је то тачка-тачка [2] топологија. Уколико постоји више станица назива се топологија више тачака [3] (слика 11.1).

[1] *Data Link Control*
[2] *Point to point*
[3] *Multiple point*



Слика 11.1 Различите топологије: тачка-тачка и више тачака

Дуплексност везе односи се на правац и време једног тока података. У симплекс преносу један ток је увек у једном правцу. На пример улазни модул као што је тастатура, или удаљени сензор, може да буде прикључен на рачунар тако да само прима податке. Симплекс се не употребљава много пошто није у могућности да шаље повратне управљачке сигнале ка извору података. Симплекс је исто као једна трака у саобраћају, или као мост у једном правцу.

Полудуплекс[1] веза може да предаје и прима али не истовремено. Ово се назива двосмерно-наизменично пропуштање саобраћаја. Потпуни дуплекс[2] веза је она у којој станице могу истовремено да примају и да предају податке једна другој. Ова врста рада назива се „двосмерно симултано", и може се поредити са две траке у саобраћају или двосмерним мостом.

Са дигиталном сигнализацијом, која захтева хардверски пренос, потпуни дуплекс обично захтева два одвојена трансмисиона пута (нпр. две упредене парице), док полудуплекс захтева само једну.

За аналогну сигнализцију дуплексност зависи од носеће фреквенције, било да се користи жични или бежични пренос. Уколико станица предаје и прима на истој учестаности она мора да ради у полу-дуплексном начину рада (изузетак је жични пренос који користи два независно изолована проводника; ретко се овако ради). Уколико станице шаљу на једној учестаности и примају на другој могу да раде у потпуном дуплексу[3].

Могућ је велики број комбинација топологије и дуплексности. Слика 11.2 скицира уобичајне комбинације: једну примарну станицу (П) и једну или више секундарних станица (С).

[1] *Half-duplex*
[2] *Full-duplex*
[3] Могу да раде и са поништавањем еха.

Слика 11.2 Комбинације примарних (П) и секундарних станица (С)

За тачка-тачка [1] везе постоје само две могућности. За везе са више тачака [2] постоје три могућности:

- примарна - потпуни дуплекс, секундарна - полудуплекс,
- обе, примарна и секундарна - полудуплекс, и
- примарна и секундарана - потпуни дуплекс.

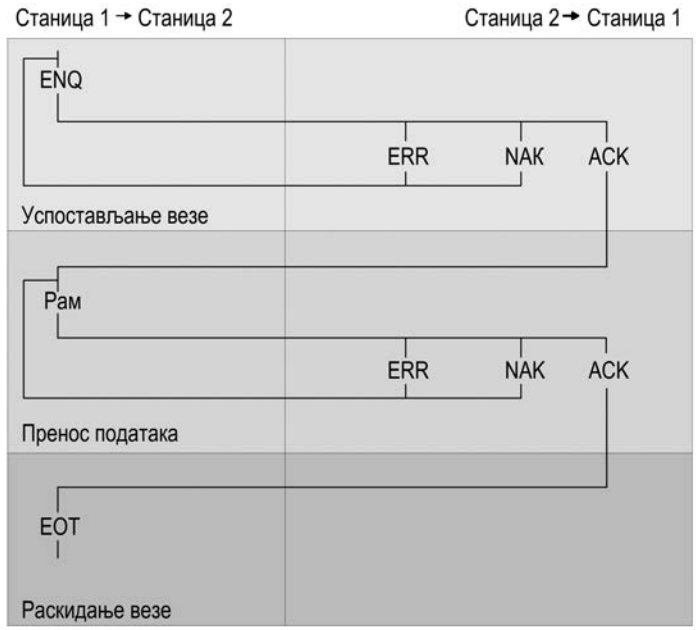
Процедуре у преносу

Постоји више типова процедура у коришћењу везе за пренос. На полудуплекс линији требало би да само једна станица у датом тренутку предаје. Без обзира да ли је у питању полудуплекс или потпуни дуплекс станица ће слати само уколико зна да је пријемник, коме је намењена порука, спреман да поруку и прими.

Тачка-тачка везе

Процедура је једноставна са тачка-тачка везама. Посматрајмо прво полудуплексну везу у којој обе станице могу да иницирају размену. Пример размена скициран је на слици 11.3.

[1] *Point to point*
[2] *Multipoint*



Слика 11.3 Управљање тачка-тачка везом

Уколико било која станица жели да шаље податке другој станицом она прво шаље упит (ENQ[1]) другој станици да би се видело да ли је спремна да прима податке. Друга станица одговара позитивном потврдом (ACK[2]) да би показала да је спремна. Прва станица затим шаље податке, који су на слици 11.3 означени као рам.

У асинхроној комуникацији подаци би били послати асинхроно. У сваком случају, пошто се нека количина података пошаље прва станица паузира да би сачекала одговор о успешном или неуспешном пријему. Друга станица потврђује успешан пријем података слањем потврде (ACK). Прва станица шаље поруку за крај трансмисије (EOT[3]) која окончава размену и враћа систем у његово иницијално стање. Да би се обезбедио рад у случају грешака додате су поруке: негативна потврда (NAK[4]) и грешка (ERR[5]). Негативна потврда (NAK) користи се да би се показало да станица није спремна да прима, или када прима да прима са грешком. Станица може да не одговори или да одговори са погрешном поруком. Оваква стања су уцртана тањим линијама на слици 11.3; пуњијом линијом представљена је нормална секвенца комуникационих догађаја.

Уколико се деси неочекиван догађај, као што је NAK, или погрешан одговор, станица може да понови своју последњу активност, или може да захтева неке процедуре за опоравак од грешке (ERR). Постоје три различите фазе у процедури управљања комуникацијом:

[1] *Enquiry*
[2] *Positive Acknowledgment*
[3] *End of Transmission*
[4] *Negative acknowledgment*
[5] *Error*

- Успостављање: одређује која станица треба да шаље а која да прима, и да је пријемник спреман да прима;
- Пренос података: подаци се преносе у једном или више блокова са потврдом;
- Завршетак : окончава логичку везу (предајник-пријемник).

Ове три фазе у некој форми део су свих линијских дисциплина, и за везе тачка-тачка и за везе са више тачака.

Претходно објашњена релација је равноправна; то значи да свака станица може да иницира пренос. Уобичајена ситуација је да се једна станица назива примарном а друга секундарном. Примарна је одговорна за иницирање размене података. Ово је уобичајена ситуација када је једна станица рачунар, а друга је терминал (секундарна). Слика скицира секвенце у којима примарна станица има податке које шаље секундарној. Уколико секундарна станица има податке да пошаље примарној мора да сачека да примарна захтева податке и само тада да уђе у фазу преноса података.

Уколико је веза потпуни дуплекс подаци и управљачке поруке могу се слати у оба правца истовремено. Видећемо предности оваквог механизма када будемо разматрали дијаграм тока и контролу грешака.

Више веза

Избор процедуре у преносу за више веза зависи првенствено од тога да ли постоји одређена примарна станица или не. Када постоји примарна станица подаци се размењују само између примарне и секундарне станице а не између две секундарне. Уобичајена процедура која се користи у овој ситуацији су све варијанте шеме „упитај и одабери[1]":

- упит - примарна станица захтева податке од секундарне,
- селектовање - примарна станица има податке за слање и информише секундарну да долазе подаци.

Слика 11.4 илуструје овај концепт. На слици 11.4а примарна станица проверава[2] секундарну слањем кратке поруке упита. У овом случају секундарна нема ништа да пошаље и одговара NAK поруком. Укупно време t_n може се представити на следећи начин:

$$t_n = t_{prop} + t_{pol} + t_{proc} + t_{nak} + t_{prop} \qquad (11.1)$$

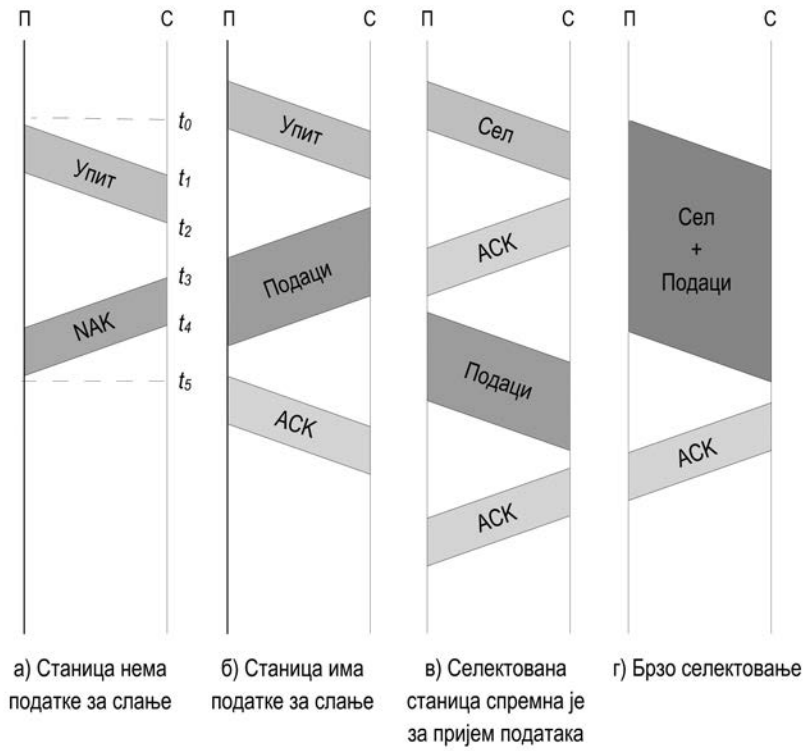
где је:

t_n - укупно време упита станице која нема шта да пошаље,
t_{prop} - време пропагације $t_1 - t_0 = t_5 - t_4$
t_{pol} - време потребно да се пошаље упит,
t_{proc} - време потребно да се обради упит пре потврде,
t_{nak} - $t_3 - t_2$
t_{prop} - време потребно за пренос негативне потврде = $t_4 - t_3$

Време t_p (слика 11.4б) осликава ситуацију успешног упита и може се израчунати на следећи начин:

$$t_p = 3_{tprop} + t_{prol} + t_{ack} + t_{data} + 2_{tproc} = t_n = t_{prop} + t_d + t_{proc} \qquad (11.2)$$

[1] *Roll call polling*
[2] *Poll*



Слика 11.4 Селектовање и слање података

Због једноставности претпостављамо да је потребно време обраде (процесирања) одговора за било коју поруку константно.

Уобичајена форма упита је она у којој примарна станица селективно шаље упит свакој секундарној станици по унапред утврђеном редоследу. У најједноставнијем случају примарна станица шаље упит за *n* секундарних станица C_1, C_2,...C_n и затим понавља секвенце. Време може да се опише на следећи начин:

$$t_n = nt_c + kt_d \tag{11.3}$$

t_c - време за један комплетан циклус слања упита,

t_n - средње време да се пошаље упит секундарној станици искључиво за пренос података,

t_d - време преноса података = $t_{prop} + t_d + t_{proc}$,

n - број секундарне станице,

k - број секундарне станице са подацима за слање за време циклуса.

Могуће је и слање упита са приоритетима. На пример слање више упита једној станици више пута у току једног циклуса.

Функција селектовања приказана је на слици 11.4в. Уочимо да се четири независне трансмисије захтевају за пренос података од примарне до секундарне станице.

Алтернативна техника је „брзо селектовање". У овом случају селектована порука укључује податке које треба пренети. Први одговор секундарне станице је потврда која указује да је станица припремљена да прима, и да успешно прима податке. Брзо селектовање је погодно код апликација код којих се кратке поруке учестало преносе, и време преноса порука није приметно дуже од времена одговора. У случају тачка-више тачака (слика 11.2в) примарна станица шаље упит једној секундарној у исто време када прима управљачку поруку од друге. За више тачака примарна може да обезбеди конверзацију у потпуном дуплексу са било којом од секундарних станица.

Јасно је на основу једначине (11.3) да премашење код сваке станице може значајно да повећа време одзива уколико постоји велики број станица или дугачка линија (велико t_{prop}).

11.2 Контрола тока

Контрола тока је техника која обезбеђује да предајна станица „не загуши" пријемну станицу подацима. Прималац ће обично резервисати меморијски простор (бафер) са неком максималном дужином. Када се подаци приме потребно је одређено време да би пријемник обрадио податке, и тек после тога може да испразни меморијски простор и припреми се за пријем нових података.

Најједноставнији начин контроле тока, познат као „заустави се и чекај", ради на следећи начин: прималац показује „спремност" да прихвати податке слањем упита или одговара на селектовање. Пошиљалац шаље податке. По пријему прималац мора поново да покаже спремност да прими нове податке. Ова процедура је погодна када се порука шаље као једна целина или један рам података. У ствари, уобичајено је да пошиљалац разбија велику поруку у мање делове (целине) и шаље их један за другим. Ово се ради из следећих разлога:

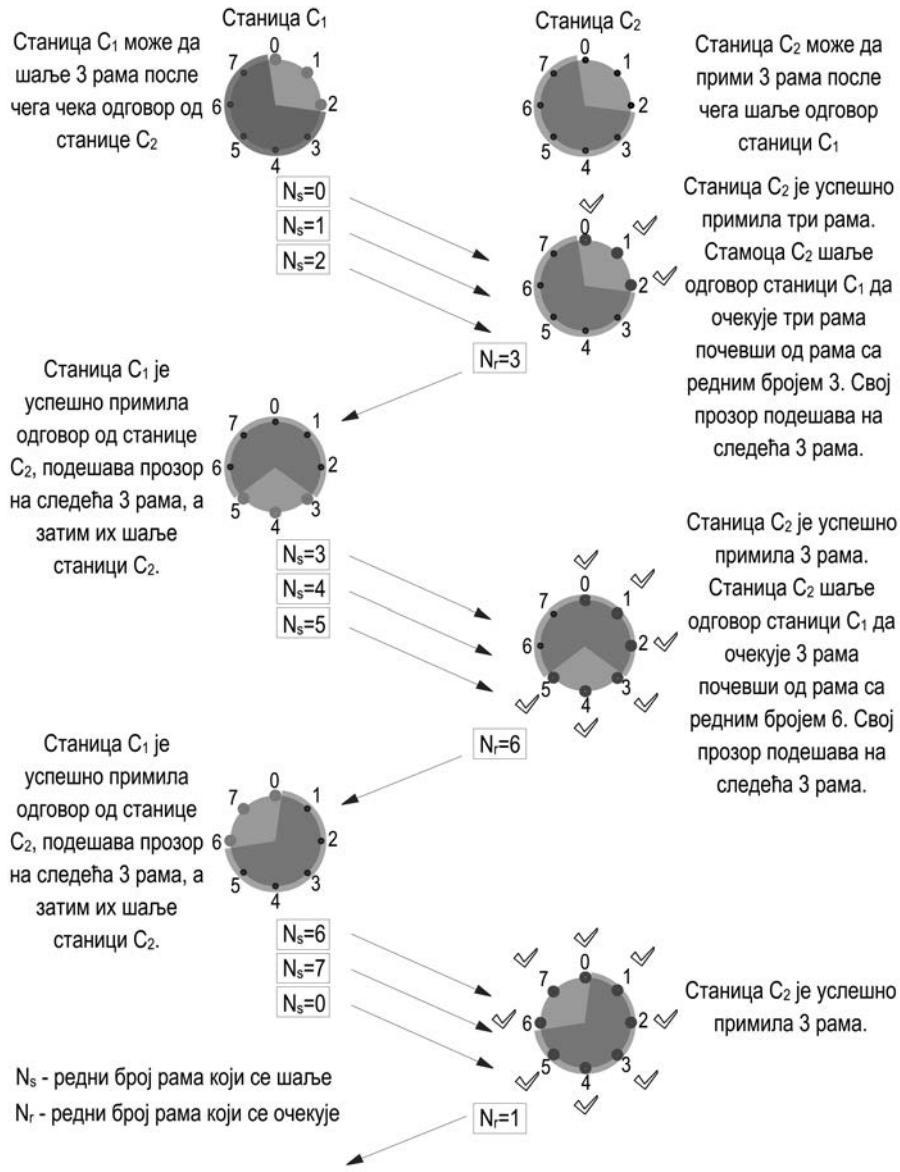
- што је дужи пренос већа је вероватноћа да ће доћи до грешке, што доводи до потребе за поновним слањем (ретрансмисијом) те целине. Када су целине мање, мања је вероватноћа грешке, и мање података треба поново послати,
- на линији са више тачака пожељно је не дозволити станици да заузима линију дуго и тиме изазове велика кашњења другим станицама,
- величина меморијског простора пријемника може да буде ограничена.

Када се користи више целина (рамова) за једну поруку једноставна процедура „заустави се и сачекај потврду" не обезбеђује добру искоришћеност линија. Зато се користи процедура, опште прихваћена, која се назива протокол клизајућег прозора (слика 11.5).

11.3 Контрола грешке

Најчешће коришћена техника за контролу грешака је базирана на две функције:

- детекцији грешака (обично се користи циклични кôд),
- захтеву за аутоматским понављањем. Када се детектује грешка пријемник захтева да се податак-рам понови.



Слика 11.5 Пример употребе протокола клизајућег прозора

Захтев за аутоматским понављањем

Верзије захтева за аутоматским понављањем (ARQ[1]) које се користе су:

- заустави се и чекај[2] ARQ,
- иди натраг *n* пута континуално[3] ARQ,
- селективно понављање[4].

[1] *Automatic Request*
[2] *Stop and Wait*
[3] *Go back n*
[4] *Selective Repeat*

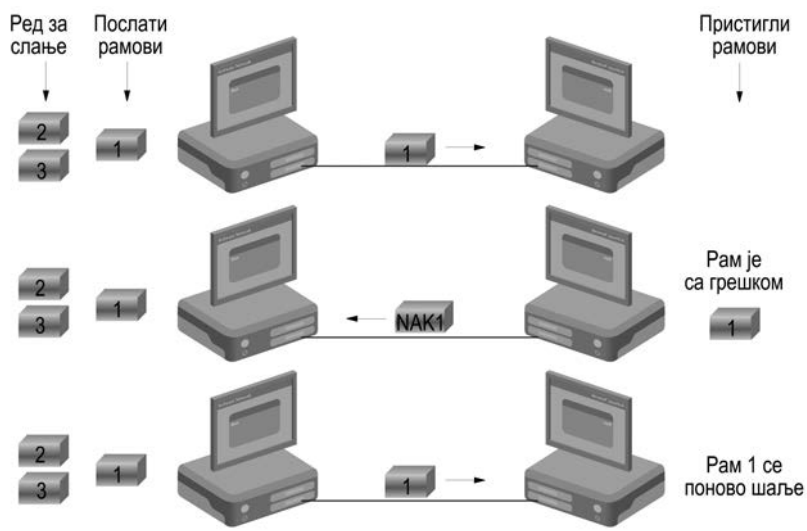
Заустави се и чекај ARQ користи једноставну „заустави се и чекај" шему за потврђивање која је већ описана. Станица шаље један рам а затим мора да чека потврду. Други рамови не могу да буду послати док се не добије одговор пријемне станице. Пријемник шаље позитивну потврду (ACK) уколико је рам коректан и негативну потврду (NAK) у осталим случајевима:

- предајник чека NAK или ACK,
- уколико истекне одређено време поново пошаљи пакет,
- чува копију док се не добије ACK,
- негативна страна је велико кашњење, а то значи неефикасан протокол.

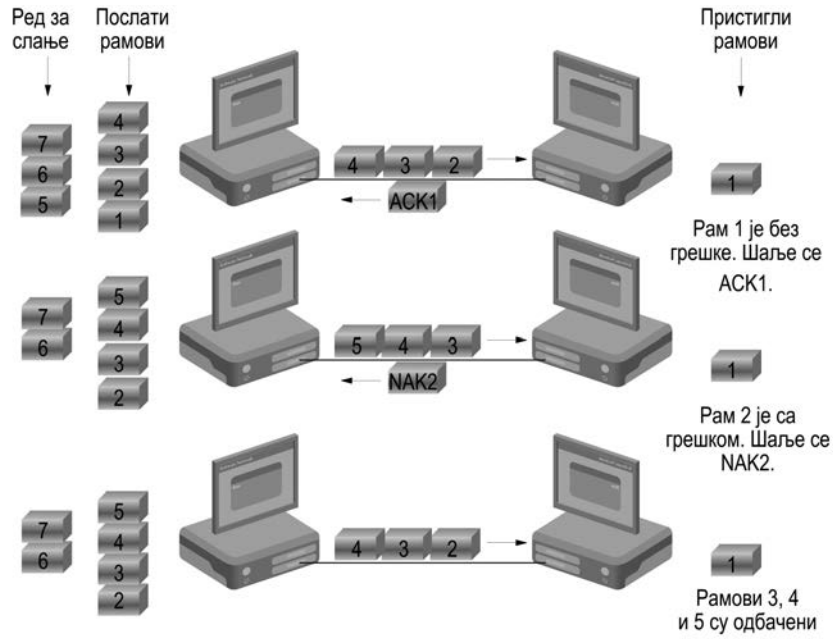
Предност заустави се и чекај ARQ је у једноставности, негативна страна у великом кашњењу. Техника клизајућег прозора омогућава веће искоришћење линије. Варијанта континуалног ARQ је иди натраг *n* пута ARQ. У овој техници станица може да пошаље серију рамова (до максималног отвора прозора). Уколико пријемна станица детектује грешку рама шаље NAK за тај рам. Пријемна станица ће одбацити све рамове који долазе после тог докле год се рам са грешком не прими исправно. Када предајна станица прими NAK мора поново да шаље рам са грешком и остале рамове (3,4).

Селективно понављање даје финији приступ него иди натраг *n*. Једини рам који се поново шаље је онај за који је примљена негативна потврда (NAK). Недостатак је што прималац треба да има простора за чување осталих рамова (3, 4, 5) док се не добије рам који је примљен са грешком (2). Пошиљалац мора да има много сложенији систем да би могао да шаље рамове ван редоследа.

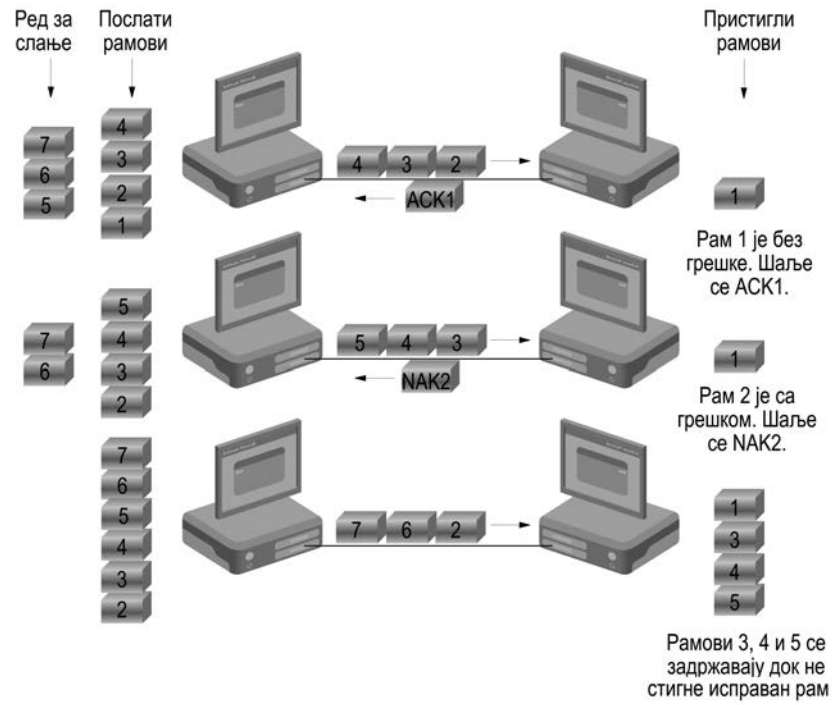
Захтев за величином отвора прозора је много рестриктивнији за селективно понављање него за „иди натраг *n* пута". Видели смо да за 2^n редних (секвенцијских) бројева код „иди натраг *n*" можемо користити прозор од 2^n -1. Сада посматрајмо случај са 3-битним пољем (број секвенцијских бројева је 8) и погледајмо сценарио:



а) Заустави се и чекај ARQ



б) Иди натраг *n* пута ARQ



в) ARQ са селективним понављањем

Слика 11.6 Шематски приказ различитих начина потврде успешног пријема рамова

1. станица C_1 шаље рамове са редним бројевима од 0 до 6 станици C_2,
2. станица C_2 прима (потврђује свих шест рамова),
3. потврда за свих шест рамова је изгубљена (нпр. велики импулсни шум),
4. на месту станице C_1 активира се часовник који указује да је протекло довољно времена од када је послат последњи рам потврда још није стигла. То значи да станица C_1 треба поново да пошаље рамове почев од оног са редним бројем 0,
5. станица C_2 је после успешног пријема свих шест рамова већ померила свој пријемни прозор да би се припремила за пријем рамова са редним бројевима 7, 0, 1, 2, 3, 4, 5. Претпоставља да је пристигли рам нов са редним бројем 0 и долази до грешке.

Да би се превазишао описани проблем максимална величина прозора не сме бити већа од половине опсега редних бројева. У претходном примеру до грешке не би дошло да су била послата само четири рама.

11.4 Бит оријентисани протоколи

Бит оријентисани протоколи направљени су да задовоље широк опсег захтева слоја везе [1] које укључују:

- тачка-тачка и тачка-више тачака везе,
- полудуплекс (наизменични двосмерни) и потпуни дуплекс (два смера симултане) операције,
- примарну, секундарну (нпр. станица [2] - терминал) и парњак (станица - станица) интеракцију,
- везе са великим (нпр. сателитском) и малим (на кратким растојањима - директна веза) односом између времена пропагација и времена слања.

Задатак ових протокола је да обезбеде следеће циљеве:

- независност од кода - корисник би требало да буде у могућности да употреби било који кôд или скуп битова у подацима које шаље,
- адаптивност - формат би требало да подржава различите варијанте типа линка,
- висока ефикасност - формат би требало да минимизира битове премашења и обезбеди ефикасну контролу грешке и контролу тока,
- висока поузданост - протокол би требало да има моћан скуп процедура за детекцију и опоравак од грешака.

Кључ да се задовоље постављени захтеви је ослањање на значење позиције и кодирање управљачких поља. Структура рама са значењем позиције је када је рам подељен у поља, при чему свако поље има специфично значење. Позиција поља је фиксирана у односу на ограничаваче рама. Кодирано управљачко поље је оно у коме различита комбинација битова има специфично значење и у коме се користе потпоља чије значење зависи од њихове позиције. Већи број сличних бит-оријентисаних протокола је достигао широку примену.

[1] *Data Link*
[2] Користи се термин станица или хост.

Најзначајнији међу њима су:

- Протокол HDLC[1] је развила ISO[2];
- Протокол LAP-B[3] развила је ADCCP[4] - преузела CCITT као део X.25 стандарда за мреже са комутацијом пакета;
- Протокол SDLC[5] користи IBM. Није га стандардизовала ниједна од организација за стандардизацију, али се доста користи.

Не постоји значајна разлика између протокола HDLC и LAP-B. Протокол LAP-B је подскуп протокола HDLC. Протокол SDLC је такође подскуп протокола HDLC. У следећем одељку анализираћемо протокол HDLC .

11.5 Основне карактеристике протокола HDLC

Да би задовољио већи број захтева који су набројани HDLC протокол дефинише три типа станица, две конфигурације везе и три врсте рада. Три типа су :

- Примарна станица одговара за управљање радом везе (линка). Рамови које захтева примарна станица називају се команде.
- Секундарна станица ради под контролом примарне станице. Рамови који се траже од секундарне станице називају се одговори. Примарна станица одржава посебан логички линк (везу) са сваком секундарном станицом на линији.
- Комбинована станица може да захтева и команде и одговоре. Комбинује карактеристике примарне и секундарне станице.

Две конфигурације везе су (слика 11.13):

- Асиметрична[6] конфигурација. Користи се тачка-тачка и више тачака врста рада. Ова конфигурација састоји се од примарне и више секундарних станица. Обезбеђује и потпуни дуплекс и полудуплекс пренос.
- Симетрична[7] конфигурација. Користи само тачка-тачка начин рада. Ова конфигурација састоји се од две мешовите станице. Подржава и потпуни дуплекс и полудуплексни пренос.

Постоје три врсте начина рада HDLC протокола:

- Нормални начин са одговором (NRM[8]). Ово је асиметрична конфигурација. Примарна станица може да иницира пренос података ка секундарној, али секундарна може само да шаље податке као одговор на упит примарне станице.
- Асинхрони балансни начин (ABM[9]). Ово је симетрична конфигурација. Било која комбинована станица може да иницира пренос без дозволе друге комбиноване станице.

---

1 *High Level Data Link Control*
2 *International Stanadard Organisation*
3 *Link Access Procedure Balanced*
4 *Advanced Data Communication Control Procedures*
5 *Synchronous Data Link Control*
6 Користи се и термин небалансирана конфигурација.
7 Балансирана конфигурација
8 *Normal Response Mode*
9 *Asynchronous Balance Mode*

а) Асиметрична конфигурација

б) Симетрична конфигурација

Слика 11.7 HDLC конфигурација везе: асиметрична и симетрична

- Асинхрони начин са одговором (ARM[1]). Ово је асиметрична конфигурација. У овој врсти рада секундарна станица може да иницира пренос без експлицитне дозволе примарне станице (нпр. шаље одговор без чекања команде). Примарна станица и даље је одговорна за линију, укључујући иницијализацију, опоравак од грешке и логичко раскидање.

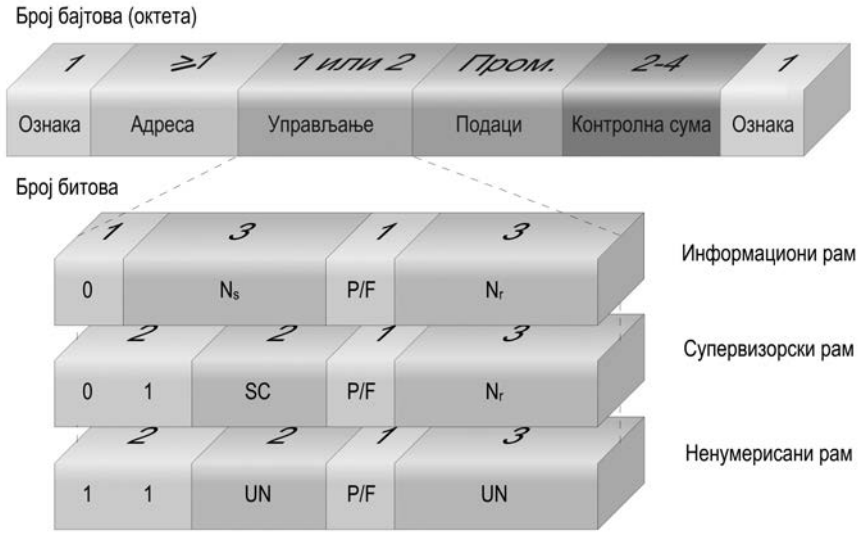
Врста рада NRM користи се на линијама са више секундарних станица. Примарна станица шаље упит (полира) за сваку секундарну станицу. Често се NRM врста рада користи у тачка-тачка везама, поготову ако је за рачунар везан терминал или нека друга периферија. Асинхрони балансни начин рада омогућава много ефикасније коришћење, потпуни дуплекс тачка-тачка везе. Врста рада ARM ретко се користи.

Структура рама протокола HDLC

Протокол HDLC користи синхрони пренос. Све што се преноси је у рамовима, и један формат је довољан за размену свих података и управљачких информација.На слици 11.8 приказан је рам који користи протокол HDLC. Рам има следећа поља:

- ознака за почетак рама (флег): 8 битова,
- адреса: један или више бајтова (октета),
- управљање (контрола): 8 или 16 битова,
- подаци: променљиви,
- секвенца за детекцију грешке (FCS[2]), контролна сума: 16 или 32 бита,
- ознака за крај рама (флег): 8 битова.

[1] *Asynchronous Response Mode*
[2] *Frame Check Sequence*



Слика 11.8 Формат рама код HDLC протокола

SC[1] = супервизорски кôд,
UN[2] = ненумерисани кôд,
P/F[3] = бит који означава упит/одговор,
N_s = предајни редни број,
N_r = пријемни редни број.

Ознака за почетак рама (флег), адреса и управљачко поље често се називају заглавље[4]. Контролна сума (FCS[5]) и ознака о крају рама који се појављује иза поља података називају се приколица, или ознака краја рама[6]. Поље које означава почетак и крај рама ограничава рам са оба краја јединственом комбинацијом битова 01111110. Сама ознака може се користити као ознака о крају једног рама и почететку другог рама. Све активне станице повезане за линк континуално „лове" секвенцу ознаке да би се синхронизовале на почетак рама. Док примају рам станице настављају да траже секвенцу која одређује крај рама. У ствари, пошто су у HDLC раму дозвољене све комбинације битова, није сигурно да се неће појавити комбинација 01111110 негде унутар рама, чиме би се уништила синхро-

Оригинални рам:

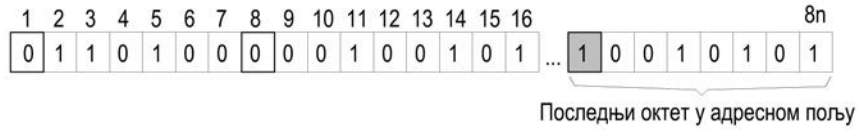
1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 0 1 1 1 1 1 1 0

После уметања битова:

1 1 1 1 1 **0** 1 1 1 1 1 **0** 1 1 0 1 1 1 1 1 **0** 1 0 1 1 1 1 1 **0** 1

Слика 11.9 Пример уметања битова

[1] *Supervisory*
[2] *UNnumbered*
[3] *Poll/Final*
[4] *Header*
[5] *Frame Check Sequence* - секвенца за проверу рама.
[6] *Trailer*



Слика 11.10 Проширени формат адресирања код HDLC протокола

низација на нивоу рама. Да би се спречио овај проблем користи се процедура позната као уметање битова[1]. Предајник ће увек после појаве пет узастопних битова 1 убацити додатни бит 0. Пријемник после пет узастопних јединица испитује шести бит. Уколико је бит 0 он се брише. Уколико је шести бит 1 и седми бит 0, комбинација се прихвата као ознака о почетку рама. Уколико су шести и седми бит 1 станици која шаље сигнализира се стање прекида. Коришћењем уметања битова поље података HDLC рама може да садржи било коју комбинацију битова. Ова особина назива се транспарентност података.

Адресно поље се користи за идентификовање секундарне станице која шаље или треба да прими рам. Ово поље није потребно за тачка-тачка везе, али је увек укључено због униформности. Адреса је нормално дугачка 8 битова. По претходном договору може се користити проширени формат у коме је адресно поље мултипл од седам битова. Осми бит у сваком октету је 1 или 0 у зависности од тога да ли јесте или није последњи октет у адресном пољу. Један октет адресе 11111111 интерпретира се као адреса свих станица, у основном и проширеном формату. Користи се да омогући примарној станици да пошаље рам свим секундарним станицама[2].

Управљачко поље код HDLC протокола дефинише три типа рамова, сваки са различитим управљачким пољем:

- Информациони рам[3] (I) преноси податке који станици треба да се пренесу и који се називају кориснички подаци. Додатно преноси и податке о контроли тока и грешци, коришћењем ARQ механизма када се не користи део информационог рама за потврду[4];
- Супервизорски рам[5] (S) обезбеђује ARQ механизам када се не користи информациони рам за потврду;
- Ненумерисани рам[6] (U) обезбеђује додатне управљачке функције везе. Остале битске позиције су организоване у потполја, као што је показано на слици 11.8.

Уочимо да базична управљачка поља супервизорских (S) и информационих (I) рамова користе 3-битни редни (секвенцијски) број. Са одговарајућом командом за постављање начина рада проширено управљачко поље може се користити за супервизорске и информационе рамове који укључују 7-битни редни број.

Поље података се јавља само у информационим и ненумерисаним рамовима. Поље може да садржи било коју комбинацију битова. Његова дужина није дефинисана

[1] *Bit staffing*
[2] *Broadcast*
[3] *Information*
[4] *Piggyback*
[5] *Supervisory*
[6] *Unnumbered*

стандардом, али је обично ограничено у зависности од примене на неку, унапред дефинисану, максималну вредност. Најчешће се захтева да је величина поља података мултипл од осам битова.

Секвенца за проверу рама (FCS[1]) примењује се на део рама без ознака о почетку и крају рама. Уобичајено се као секвенца користи 16-битни циклични кôд (CRC-16) који је дефинисала организација ITU-T. Уколико величина рама или поузданост линије то захтевају може се користити и 32-битна секвенца за проверу која се добија као 32-битни циклични кôд (CRC-32).

Начин рада HDLC протокола

HDLC протокол се извршава тако што се размењују I рамови, S рамови и U рамови између примарне и секундарне или између две примарне станице. Различите команде и одговори дефинисани за ове типове рамова дефинисани су у табели 11.1. Да би се описао начин рада HDLC протокола потребно је прво дефинисати три типа рамова.

Основни начин рада HDLC протокола укључује размену информационих рамова (I-рамова) који садрже корисничке податке. Сваки I рам садржи редни број послатог рама као и потврду о успешно примљеном раму. Потврда о позитивном пријему је редни број следећег рама који се очекује. Максимални број редних бројева (ширина прозора) је 7 или 127. Информациони рам такође садржи P/F бит. Постављен P бит указује да је рам - команда коју шаље примарна станица а постављен F бит указује на рам - одговор који шаље секундарна станица.

Супервизорски рам се користи за контролу тока и контролу грешке. Метод иди натраг *n* пута ARQ (REJ) и метод ARQ са селективним понављањем (SREJ) су дозвољени. Последњи се ређе примењује због потребе за већим меморијским простором (за чување података које треба поново послати). Поред I рама за потврду о успешном пријему може се користити RR рам.

P/F бит у супервизорском раму може се користити на следећи начин. Примарна станица може да шаље упит (полира) секундарној станици слањем RR рама са битом P=1 када нема I рамова са којима може да потврди упит. Секундарна одговара слањем I рама уколико има бар један рам за слање. У супротном, шаље RR рам са F=0 да би показала да нема података за слање. Примарна/комбинована станица може да постави P бит (P=1) у RNR команди и да на тај начин тражи пријемни статус секундарне/комбиноване станице. Одговор ће бити RR са F=1 уколико станица може да прими I рамове, и RNR са F=0 уколико је станица заузета.

Ненумерисани рамови се користе за различите управљачке функције. Као што и само име каже, рамови не носе редне бројеве и не мењају редослед или ток нумерисаних I-рамова. Рамови се могу груписати у следеће категорије:

- команде и одговори за постављање начина рада,
- команде и одговори о преносу информација,
- команде и одговори за опоравак,
- разноврсне команде и одговори.

[1] *Frame Check Sequence*

Назив	Функција	Опис
Информација (I)	Команда/Одговор[1]	Размена корисничких података
Супервизорски (S)		
Пријемник спреман (RR) *Receiver Ready*	Команда/Одговор	Позитивна потврда: спреман за пријем I рамова
Пријемник није спреман (RNR) *Receiver Not Ready*	Команда/Одговор	Позитивна потврда: није спреман за пријем
Одбацивање (REJ) *Reject*	Команда/Одговор	Негативна потврда: иди натраг N пута
Селективно одбацивање (SRJ) *Selective Reject*	Команда/Одговор	Негативна потврда: селективно понављање
Ненумерисан (U) *Unnumbered*		
Постављање NRM врсте рада/ проширени начин (SNR/SNRE) *Set Normal Response/Extended Mode*	Команда	За постављање проширеног начина рада = управљачко поље је два октета
Постављање ARM врсте рада/ проширени начин (SABM/SABME) *Set Asynchronous Response/ Extended Mode*	Команда	За постављаље проширеног начина рада = управљачко поље је два октета
Постављање иницијализационог начина рада (SIM) *Set Initialization Mode*	Команда	Иницијализује управљачке функције на адресираној станици
Раскид (DISC) *Disconnection*	Команда	Прекида логичку везу на линку
Ненумерисана потврда (UA) *Unnumbered Acknowledge*	Одговор	Потврђује пријем једне од команди за постављање начина рада
Раскидајући начин рада (DM) *Disconnection Mode*	Одговор	Секундарна станица је логички раскинута
Захтев за раскидом (RD) *Request Disconnect*	Одговор	Захтев за DISC командом
Начин рада у коме се иницијализује захтев (RIM) *Request Initialization Mode*	Одговор	Потребна је иницијализација: захтев за SIM командом
Ненумерисана информација (UI) *Unnumbered Information*	Команда/Одговор	Користи се за размену управљачких информација
Ненумерисани упит (UP) *Unnumbered Poll*	Команда	Користи се за тражење управљачких информација
Поновно укључивање *Reset*	Команда	Користи се за опоравак: ресетује N_r, N_s
Размена идентификатора (XID) *Excange Identification*	Команда/Одговор	Користи се за идентификацију захтева/извештаја и статуса
Test	Команда/Одговор	Размењује идентична поља за тестирање
Одбацивање рама (FRMR) *Freame Reject*	Команда	Обавештава о пријему неприхватљивог рама

Табела 11.1 HDLC команде и одговори

[1] *Command*/*Response* - Команда/Одговор

Команде за постављање начина рада шаље примарна/комбинована станица да би иницијализовала или променила начин рада секундарне/комбиноване станице. Секундарна/комбинована станица потврђује пријем одговарајући ненумерисаном потврдом (UA). Рам UA има F бит постављен на исту вредност као примљени P бит. Једном успостављен начин рада остаје на снази докле год се не прими нова команда за постављање начина рада.

Команде SNRM, SARM, SABM и SABME саме себе објашњавају. По пријему команде редни број I рама (N_r., N_s.) се у оба правца поставља на 0. Команда SIM користи се да би адресирана секундарна/комбинована станица иницирала специфичне процедуре за иницијализацију управљачких функција (нпр. пријем нових програма или иновирање радних параметара). У овој врсти рада информације које су биле захтеване шаљу се коришћењем ненумерисаних информационих (UI) рамова.

Команда за раскид (DISC) користи се као обавештење да станица која је била у фази слања обуставља рад.

Поред UA рама постоје и други рамови - одговори који су везани за постављање начина рада. На пример DM рам шаље се као одговор на све команде које указују да се станица која шаље одговор логички „откачила". Када се шаље као одговор на команду за постављање начина рада DM рам одбија захтевани начин рада.

Захтев за иницијализацијом начина рада (RIM одговор) користи се као одговор када станица жели да иницира начин рада. Захтев за раскидом (RD одговор) користи се као захтев за раскидом логичке везе.

Команде и одговор за пренос информација користе се за размену информација између станица. Ово се најчешће ради са ненумерисаним информационим рамовима (UI). Команда ненумерисани упит (UP рам) користи се за тражење ненумерисаних одговора, као начин успостављања статуса адресираних станица.

Команде и одговори за опоравак од грешке користе се када се ARQ механизам не примењује или не ради добро. Одговор да је рам одбачен (FRMR рам) користи се да би обавестио да је дошло до грешке у пријемном раму. Могуће грешке су:

- погрешно управљачко поље,
- поље података предугачко,
- поље података није дозвољено са типом рама који се прима,
- погрешан пријемни бројач (нпр. рам је потврђен иако још није послат).

Команда RSET користи се за брисање FRMR стања. RSET рам је обавештење станици која шаље да треба да ресетује свој редни број за слање и адресираној станици да треба да ресетује свој пријемни редни број. Команда/одговор XID користи се да би две станице размениле идентификације и карактеристике.

Стварна размена информација је у зависности од примене. TEST команда/одговор је једноставан начин за тестирање да веза и адресиране станице заиста раде.

Часовници код HDLC протокола

HDLC дефинише два часовника[1] T_1 и T_2. Користе се на следећи начин:

- T_1 часовник - примарна станица поставља P бит и тестира да ли је одговор

[1] Тајмера (*timer*)

Активност	Разлог
Укључује (стартује) T_1 од 0	Када је команда послата са P = 1
Поново укључује (ресетује) T_1 на 0	Када је одговор примљен са F = 1
Поново шаље команду са P = 1	Време на које је постављен T_1 истиче

Табела 11.3 Активности часовника T_1 на примарној станици

примљен у одређеном времену. Ову функцију контролише часовник T_1 и назива се „чекај на F".

- T_2 часовник - станица која шаље I рамове тестира да ли је потврда примљена у одређеном временском периоду. Ову функцију контролише часовник T_2 и назива се „чекање на N_r".

У табели 11.3 објашњено је коришћење часовника за NRM врсту рада.

Пример HDLC процедуре

У овом одељку дат је пример HDLC (LAP_B) рада за пренос без грешке (слика 11.11)

Време								
	n	*n*+1	*n*+2	*n*+3	*n*+4	*n*+5	*n*+6	*n*+7
Станица C_1 шаље	SABM A_2 P=1		I A_2 P=0 N_s=0 N_r=0	I A_2 P=1 N_s=1 N_r=0				RR A_1 F=1 N_r=2
Станица C_2 шаље		UA A_2 F=1			RR A_2 F=1 N_r=2	I A_1 P=0 N_s=0 N_r=2	I A_1 P=1 N_s=1 N_r=2	

Легенда:

Ознака	Опис
I	Информациони рам
n	Станица C_1 шаље SABM команду са P битом постављеним на 1, и адресом станице C_2 (A_2).
n+1	Станица C_2 одговара са UA рамом који се користи као одговор са F битом постављеним на 1.
n+2, 3	Станица C_1 шаље информациони рам са редним бројевима 0 (P=0) и 1 (P=1).
n+4	Станица C_2 потврђује исправан пријем C_1 слањем одговора RR, са 2 у пољу за пријемни редни број.
n+5, 6	Станица шаље C_2 информациони рам са редним бројевима 0 (P=0) и 1 (P=1), и адресом станице C_1 (A_1). У *n*+1 тренутку P бит је био постављен на 0, што је указивало да то није последњи пакет и да C_1 не треба још да шаље потврду. У *n*+2 тренутку P бит је био постављен на 1. На тај начин се указује станици C_1 да је то последњи информациони рам и да треба да пошаље потврду. Види се да је отвор прозора 2.
n+7	Станица C_1 потврђује C_2 рамове са редним бројевима 0 и 1 са N_r=2 и F=1.

Слика 11.11 Асинхрони балансни начин рада ABM са полудуплексним протоком података (коришћењем P/F провера) без грешке

и случај када у току преноса дође до грешке (слика 11.12).

Време								
	n	*n*+1	*n*+2	*n*+3	*n*+4	*n*+5	*n*+6	*n*+7
Станица C_1 шаље	I A_2 P=0 N_s=6 N_r=4	I A_2 P=0 N_s=7 N_r=4 грешка	I A_2 P=1 N_s=0 N_r=4	RR A_2 F=1 N_r=4	I A_2 P=0 N_s=7 N_r=4	I A_2 P=0 N_s=0 N_r=4	I A_2 P=1 N_s=1 N_r=4	
Станица C_2 шаље			REJ A_2 P=1 N_r=7					RR B F=1 N_r=2

Легенда:

Ознака	**Опис**
n, *n* + 1, 2	Станица C_1 шаље информациони рам са редним бројевим 0, 1 (P=0) и 2 (P=1)
n + 2	Станица C_2 детектује грешку у раму 7 и одмах шаље RR (Reject) рам са пријемним редним бројем 7. Уочимо коришћење адресног поља и P бита да би се информациони рам употребио као командни
n + 4	Станица C_1 враћа RR
n + 4, 5, 6	Станица C_1 поново шаље оштећени рам (редни број 7) и наставља са слањем
n + 7	Станица C_2 потврђује исправан пријем рамове са редним бројевима 7, 0 и 1 са N_r=2 и F=1
n + 7	Станица C_1 потврђује C_2 рамове са редним бројевима 0 и 1 са N_r=2 и F=1

Слика 11.12 Опоравак од грешке код LAP_B протокола

12. Архитектура локалних рачунарских мрежа

Без обзира што нису све архитектуре локалних рачунарских мрежа стандардизоване од стране различитих тела за стандардизацију (ISO, IEEE, ANSI...), оне су састављене од истих логичких компонената. Када се описује одређена архитектуре локалне рачунарске мреже потребно је познавати следеће:

- методологију (метод) приступа трансмисионом медијуму,
- логичку и физичку топологију,
- врсту трансмисионог медијума.

12.1 Методи приступа трансмисионом медијуму

Уколико исти медијум треба да користи (дели) више радних станица неопходно је да постоји начин који регулише приступ више станица трансмисионом медијуму. Анализираћемо два приступа: статички (FDM[1] и TDM[2]) и динамички (Aloha[3], CSMA[4], мреже са жетоном...).

Упоређивање статичких и динамичких метода

Традиционалан начин дељења преносног медијума (канала) између више корисника је фреквенцијски мултиплекс. Уколико има *n* корисника фреквенцијски опсег се дели на *n* једнаких делова. Сваком кориснику се додељује одговарајући део фреквенцијског опсега. Пошто сваки корисник има свој фреквенцијски опсег не постоји преклапање између корисника. Уколико постоји само мали и константан број корисника FDM је једноставан и ефикасан метод. Уколико је број корисника велики и мења се, онда FDM није најбоље решење. Када је корисник неактиван, њему додељен фреквенцијски опсег једноставно је неискоришћен. Неактивни корисник га не користи, а није га могуће ни доделити неком другом кориснику. У већини рачунарских система саобраћај је великог интензитета а кратког трајања[5]. Однос између саобраћаја највећег интензитета и просечног саобраћаја обично је 1000:1. Лоше карактеристике статичког FDM-а могу се показати следећом анализом. Пођимо од средњег времена кашњења[6], *T*, канала чији је капацитет *C* b/s, са брзином пристизања λ рамова/секунди и са средњом дужином од $1/\mu$ битова/раму. Са овим параметрима: брзином пристизања пакета λ и брзином услуге (сервиса) μC, а по теорији редова за случај Поасонове расподеле времена пристизања и обраде пакета добија се:

$$T = \frac{1}{\mu C - \lambda} \tag{12.1}$$

[1] FDM - фреквенцијски мултиплекс (детаљно је обрађено у 8. поглављу).
[2] TDM - временски мултиплекс (детаљно је обрађено у 8. поглављу).
[3] Aloha (здраво на Хавајском) - станица шаље када има пакет за слање.
[4] CSMA (*Carrier Sense Multiple Access*) - станица прво ослушкује преносни медијум, ако је слободан шаље.
[5] *Bursty*
[6] Дефинише се као време потребно да рачунарска мрежа обезбеди испоруку података спремног за слање одредишту.

На пример ако је $C = 100$Mb/s, средња дужина пакета $1/\mu$ је 10000 битова, и брзина пристизања пакета λ је 5000 рамова/секунди, онда је $T = 200\mu$s. Ако не узмемо у обзир кашњење у реду за приступ заједничком преносном медијуму и израчунамо потребно време да се рам од 10000 битова пренесе кроз рачунарску мрежу брзине 100Mb/s добијамо (нетачан) одговор од 100μs. Овај резултат се добија само под условом да нема „надметања" за приступ каналу.

Поделимо сада канал на n независних делова (потканала). Капацитет сваког дела је C/n b/s. Средња брзина пакета података који су спремни (пристигли) за слање за сваки потканал је λ/n. Средње време кашњења постаје:

$$T_{FDM} = \frac{1}{\frac{\mu C}{n} - \frac{\lambda}{n}} = \frac{n}{\mu C - \lambda} = nT \tag{12.2}$$

Средње кашњење T_{FDM} у мрежама са фреквенцијским мултиплексирањем је n пута веће од средњег кашњења T хипотетичке мреже у којој би n корисника било у јединственом реду за приступ каналу.

Код временског мултиплекса ситуација је идентична. Сваки корисник је статички расподељен тако да је n-ти временски сегмент (слот) додељен n-том кориснику. Уколико корисник нема податке за слање временски сегмент је неискоришћен. Иста је ситуација уколико физички раздвојимо мрежу. Користећи претходни пример, уколико заменимо мрежу од 100Mb/s на 10 мрежа од по 10Mb/s, и статички сваком кориснику доделимо по једну од њих, средње време кашњења ће порасти са 200μs на 2ms.

Види се да ниједна од традиционалних метода статичког додељивања канала корисницима није погодна за саобраћај великог интензитета и кратког трајања.

Када више корисника треба да шаље податке на заједнички медијум потребно је јасно дефинисати ко може да пошаље податак, а ко не. Методе за дељење трансмисионог медијума познате су као методе приступа трансмисионом медијуму.

Генерално посматрано, постоје два механизма приступа: по унапред одређеном редоследу[1] и сукобљавањем[2]. У рачунарским мрежама саобраћај је неравномерно расподељен у времену, великог је интензитета и кратког трајања. Доказано је да је ефикасније користити један канал велике брзине коме се приступа међусобним сукобљавањем (релација 12.2).

Динамички методи приступа трансмисионом медијуму

Најстарији и најједноставнији представник динамичких метода приступа трансмисионом медијуму је Aloha. Овај метод развијен је за пакетске радио-преносе. Сваки корисник приступа каналу када има податке спремне за слање, не испитујући да ли је канал већ заузет. Уколико је канал већ био заузет доћи ће до сукоба (колизије) и сви подаци ће бити оштећени. После одређеног времена[3] уколико не добије потврду о успе-

[1] *Polling, token passing*
[2] *Contention*
[3] Обично се ово време поставља на вредност двоструко већу од максималног времена пропагације две најудаљеније станице.

Слика 12.1 Временски периоди у слању код CSMA/CD метода

шном пријему података од одредишне станице предајна станица ће поново послати податке. Као последица великог броја сукобљавања и понављања пакета [1] Aloha је неприменљива за локалне рачунарске мреже. Постоји и верзија са тачно дефинисаним тренуцима времена у коме станице у Aloha [2] мрежама могу да шаљу податке са бољим искоришћењем трансмисионог медијума [3].

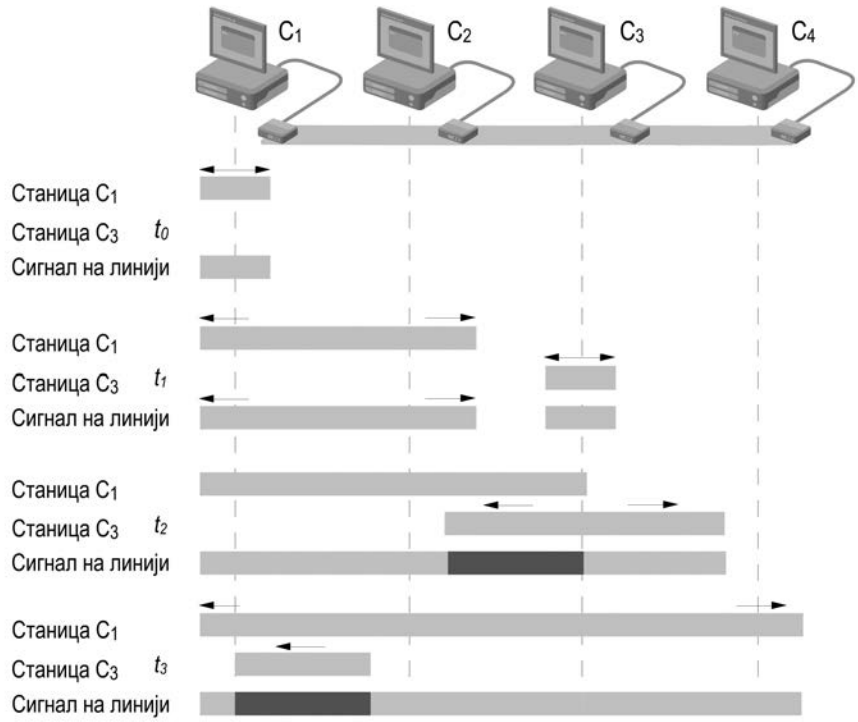
CSMA [4] (вишеструки приступ са ослушкивањем носиоца) је метод приступа каналу који се користи да би се умањила могућност сукоба. Идеја је да када станице желе да шаљу податак испитује (ослушкују) да ли је неко заузео трансмисиони медијум (кабл). Ако је трансмисиони медијум заузет, станица чека да се он ослободи. Ако је слободан одмах започиње слање. Уколико две или више станица истовремено почну да шаљу преко слободног трансмисиони медијум, долази до сукоба. Могућност конфликта (судара) постоји у кратком временском интервалу који се назива време рањавања[5] и једнак је максималном времену пропагације између најудаљенијих корисника.

Метод CSMA/CD [6] (ослушкивање носиоца, вишеструки приступ и откривање судара) широко је распрострањен у локалним рачунарским мрежама. Припада подслоју за приступ трансмисионом медијуму (MAC [7]). Као и многи други протоколи у локалним рачунарским мрежама користе модел који се може објаснити помоћу слике 12.1. У тренутку означеном са t_0 станица завршава слање свог рама. Било која друга станица која има рам за слање може сада да покуша да то уради. Уколико две или више станица покушају то даураде, доћи ће до колизије. По детектовању колизије станица прекида слање, чека случајни период времена и поново покушава са слањем. То значи да модел CSMA/CD чине периоди слања, сукобљавања и неактивни периоди.

Потребна је одређена процедура која специфицира шта станица треба да уради ако је трансмисиони медијум заузет и шта треба да уради ако је медијум слободан:

1. Ако је медијум слободан, послати рам, у супротном прећи на 2. тачку;
2. Уколико је медијум заузет наставити са ослушкивањем док се канал не ослободи, а онда одмах послати рам;
3. Уколико се детектује колизија за време слања, треба послати кратак сигнал „упозорења" [8];

[1] Максимална искоришћеност не прелази 18%.
[2] *Slotterd* Aloha
[3] Максимална искоришћеност не прелази 37%.
[4] *Carrier Sense Multiple Access*
[5] *Vulnerable time*
[6] *Carrier Sense Multiple Access with Collission Detection*
[7] Управљање приступа медијуму - *Medium Access Control.*
[8] *Jamming*



Слика 12.2 Активности станица код CSMA/CD метода

4. После слања сигнала упозорења треба сачекати произвољно време које се израчунава помоћу алгоритма за кашњење [1]. Затим треба поново пробати са слањем рама.

Слика 12.2 илуструје описану процедуру. Горњи део слике показује локалну рачунарску мрежу типа магистрале. Испод слике је скицирана активност на магистрали у тренуцима када су се десила четири узастопна догађаја. У тренутку t_0 станица C_1 започиње са слањем рама упућеног станици C_4. У тренутку t_1 и станица C_2 и C_3 су спремне да започну слање. Станица C_2 детектује да је канал заузет (у току је слање) и одлаже своје слање. Пошто станица C_3 није детектовала да станица C_1 већ шаље свој рам и она започиње са слањем. Када подаци које је станица C_1 послала стигну до станице C_3, у тренутку t_2, станица C_3 открива да је дошло до колизије и престаје са слањем. Ефекат колизије се простире натраг до станице C_1 која га открива у тренутку t_3 и обуставља слање свог рама.

Да би се обезбедила стабилност, величина кашњења која се примењује у 4. тачци обезбеђена је механизмом који се назива метод бинарног експоненцијалног кашњења [2]. Станица ће покушавати да шаље упркос поновљеним колизијам. У првих десет покушаја време кашњења се дуплира а у следећих шест покушаја се не мења. После шеснаест неуспелих покушаја да пошаље рам станица одустаје и обавешта-

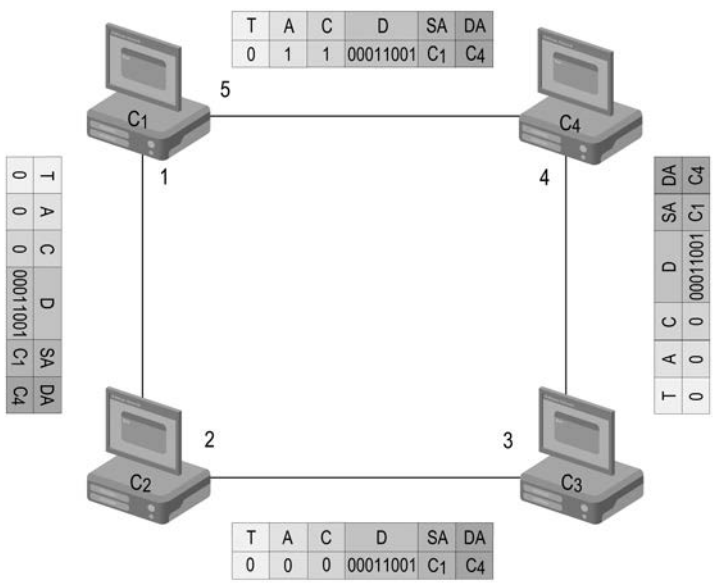
[1] *Backoff*
[2] *Binary exponential backoff*

ва више слојеве о грешци. Види се да што је загушење у саобраћају веће станице повећавају своје кашњење како би се могућности колизије умањиле.

Јасно је да је метод CSMA/CD ефикасан када је релативно мало сукобљавања станица. Способност да станица (најчешће рачунар) приступа мрежи једноставно, без много дозвола, побољшава искоришћеност мреже код саобраћаја слабијег интензитета. Како се саобраћај у мрежи повећава број судара (колизија) пакета се такође повећава. Њихово поновно слање може негативно да утиче на свеукупне перформансе мреже.

Пролазак жетона[1] је механизам приступа са унапред одређеним редоследом. Принцип је следећи: станица не може да приступи трансмисионом медијуму док није на њу ред. Знак станици да има право да шаље своје податке на медијум је пријем одговарајућег жетона. Пролазак жетона обезбеђује да свака станица када шаље податке има 100% канала на располагању. Процедура која одговара слици 12.3 је следећа:

1. Станица C_1: прихвата 24-битни жетон и поставља бит T[2] са 1 на 0 (из слободног статуса у заузети); шаље рам података на мрежу; поставља одредишну адресу[3] (DA) станица C_4; а своју као изворишну адресу[4] (SA); налази се у стању предаје[5].
2. Станица C_2: прима рам и очитава одредишну адресу; пошто је одредиште станица C_4 прослеђује рам; налази се у стању ослушкивања[6].



Слика 12.3 Локалне рачунарске мреже са проласком жетона

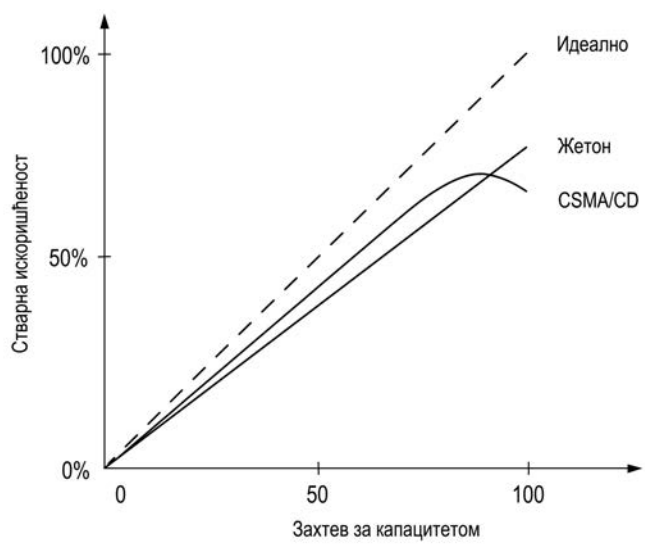
[1] *Token passing*
[2] *Busy status* - заузети статус
[3] DA *(Destination Address),*
[4] SA *(Source Address)*
[5] *Transmit mode*
[6] *Listen mode*

3. Станица C_3: искључена је па се саобраћај преко ње одвија без њене обраде; налази се у стању заобилажења [1].
4. Станица C_4: прима рам и види да је њој намењен; смешта податке из рама у своју меморију; мења ознаке о статусу чиме потврђује успешну испоруку података.
5. Станица C_1: прима рам који је она послала; испитује ознаке о статусу рама које указују да је адреса препозната (A=1) и да је одредишна станица успешно ископирала податке (C=1); не врши поновно слање рама; поставља T бит жетона на 1 (слободан); ослобађа жетон.

Прстен са жетоном [2], брзине до 16Mb/s, је модификована форма локалне рачунарске мреже са прослеђивањем жетона. Жетон изворишна станица ослобађа, тј. поставља га у статус слободног жетона одмах по завршетку слања свог рама података. Овакав механизам се среће под називом рано ослобађање жетона. Софтвер и протоколи који воде рачуна о прослеђивању и регенерацији жетона у случају губитка жетона су обично смештени у чиповима на мрежној картици станице (рачунара).

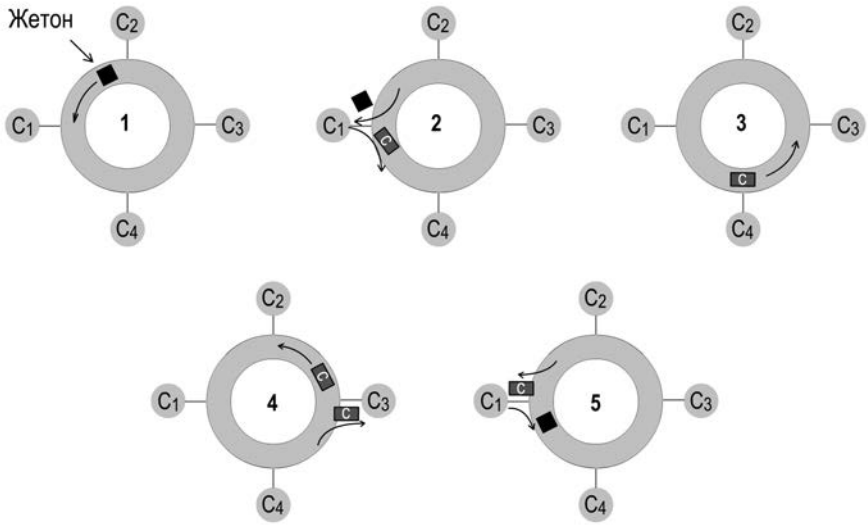
Упоређивање метода са прослеђивањем жетона и са детекцијом носиоца

Постоји стварна разлика у карактеристикама локалних рачунарских мрежа које користе претходно описане механизме за приступ трансмисионом медијуму. Метод са детекцијом носиоца (CSMA/CD) има мање додатних података [3] и ефикаснији је од приступа са прослеђивањем жетона код саобраћаја малог интензитета. Када је саобраћај већег интензитета повећан број судара и поновно слања података доприноси да су мреже са жетоном ефикасније. Стварна тачка у којој долази до разлике у ефикасности зависи од више фактора као што су величина рама, дужина сегмента и брзина слања.



Слика 12.4 Упоређивање метода CSMA/CD и са прослеђивањем жетона

[1] *Bypass mode*
[2] *Token ring*
[3] *Overhead*



Слика 12.5 Секвенцијална логичка топологија

На слици 12.4 хоризонтална оса представља захтевани капацитет у процентима. Вертикална оса представља стварни, ипоручени капацитет који је постигнут механизмом за приступ трансмисионом медијуму. Идеалан однос би био 1:1. Графички приказано била би то права са нагибом од 45°. Додатни подаци и поступци придружени сваком од механизама приступа чине овај идеалан однос неизводљивим.

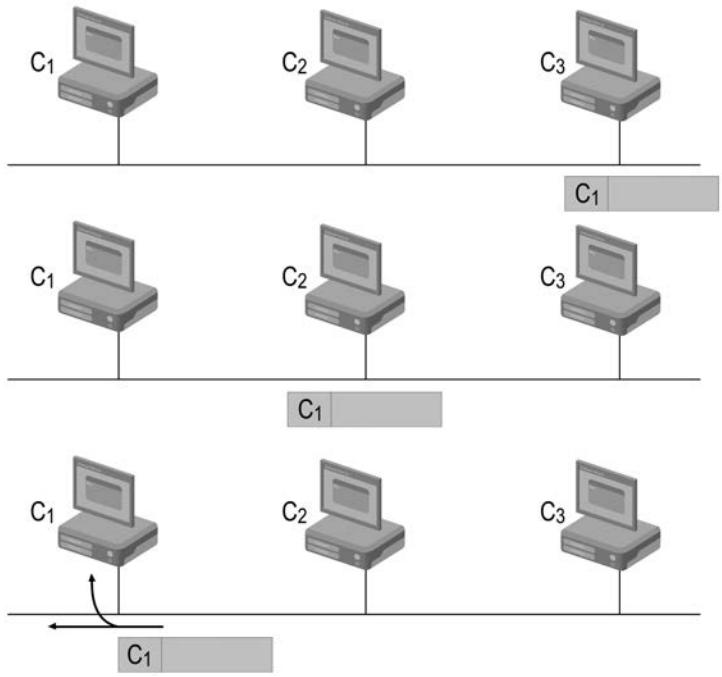
Као што се види на слици CSMA/CD обезбеђује скоро потпуну ефикасност, док је број судара и поновног слања не умање. Ова појава почиње озбиљно да утиче на перформансе на око 60% захтева за капацитетом, и увећава се док се перформансе значајно не погоршају додатним захтевом за капацитетом. Једноставно, број судара почиње да премашује број успешно послатих пакета.

Код структуираног механизма приступа уз помоћ жетона не долази до судара. Пошто је слање потпуно контролисано, перформансе се могу предвидети док не достигну 100% захтеваног опсега. Премашење (жетон као додатни податак) утиче да је механизам са жетоном мање ефикасан од CSMA/CD код слабијег саобраћаја. Графички приказ на слици 12.4 добро описује свеукупни однос ових механизама приступа.

Логичка топологија

Када се порука нађе на локалној рачунарској мрежи која користи заједнички (дељени) медијум, за који је прикључено више станица, мора се одредити како ће порука на свом путу до одредишне станице бити прослеђена од једне до друге станице. Методологија прослеђивања поруке назива се логичка топологија локалне рачунарске мреже.

Секвенцијална логичка топологија, позната као топологија прстена (слика 12.5), је метод у коме се подаци шаљу од једне до друге станице (чвора). Сваки чвор испитује



Слика 12.6 Логичка топологија један ка свима

одредишну адресу пакета података да би установио да ли је пакет баш њему упућен. Уколико пакет није адресиран том чвору, прослеђује се следећем чвору прстена. Од једног ка свима [1] је други тип логичке топологије (слика 12.6), или метод испоруке пакета података. Код овог типа логичке топологије подаци се шаљу истовремено свим чворовима на мрежи. Сваки чвор одлучује појединачно да ли је пакет података упућен баш њему. Уколико није, порука се једноставно игнорише. Не постоји потреба да се порука проследи суседном чвору. Сви чворови добијају поруке истовремено.

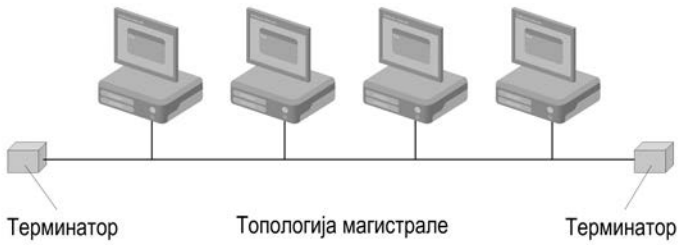
Да закључимо шта је кључна разлика између секвенцијалног и од једног ка свима метода? Главна тачка је одговорност међустанице ка којој порука није адресирана. У секвенцијалном методу међустаница има активну улогу - мора да проследи поруку свом следећем суседу. У случају логичке топологије од једног ка свима, станица која није одредишна игнорише примљену поруку.

Физичка топологија

Станице морају бити физички међусобно повезане медијумом који деле по некој од конфигурација. Физичка реализација конфигурације мреже може да има значајан утицај на карактеристике локалне рачунарске мреже и дефинише се као физичка топологија локалне рачунарске мреже.

Топологија магистрале [2] је организација на линији са терминаторима на сваком од крајева (слика 12.7). Станице се везују на магистралу преко прикључка и/или при-

[1] *Broadcast*
[2] *Bus*



Слика 12.7 Физичка топологија магистрале

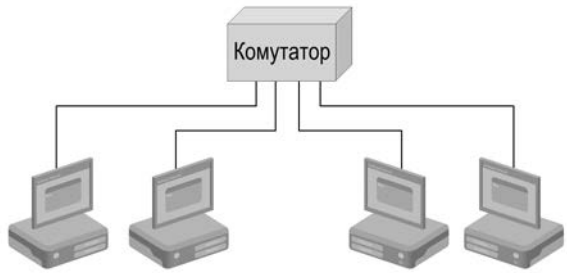
мопредајника (трансивера). Слаба тачка топологије магистрале је у томе што прекид било где на магистрали доводи до прекида рада целе мреже.

Код топологије прстена[1] прекид у једном делу угрожава целу локалну рачунарску мрежу (слика 12.8). Свака станица повезана топологијом прстена је практично активна карика прстена, која прослеђује пакете података у секвенцијалном редоследу кроз прстен. Уколико је нека од станица у квару (сама станица или мрежна картица) веза између њој суседних станица је раскинута, жетон је изгубљен и локална рачунарска мрежа је ван употребе. Такође било који прекид кабла доводи до прекида рада целе мреже.

Код топологија звезде[2] избегнут је прекид у раду читавог система услед прекида у неком делу локалне рачунарске мреже увођењем одређеног централизованог управљачког уређаја (слика 12.9). У зависности од архитектуре мреже овај уређај има различиту функцију и назив као што је комутатор[3], концентратор[4] и јединица за вишеструки приступ (MAU[5]). Уколико се ова централизована станица поквари, цела мрежа је

Слика 12.8 Физичка топологија прстена

[1] *Ring*
[2] *Star*
[3] *Switch*
[4] *Hub*
[5] *Multiple Access Unit*



Слика 12.9 Физичка топологија звезде

ван функције. С друге стране, уколико је било који чвор (тј. станица) ван функције, то нема утицаја на рад осталих делова мреже.

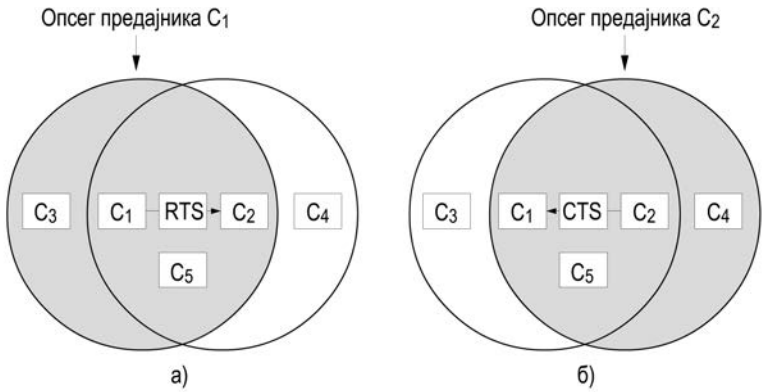
Протокол за бежичне локалне рачунарске мреже

Број мобилних корисника који користе и телефоне и рачунаре у сталном је порасту. Да би се постигла потпуна мобилност покретни рачунари треба да користе радио или инфрацрвени сигнал за комуникацију. Систем са покретним рачунаром који комуницира радио-путем сматра се бежичном локалном рачунарском мрежом. Ове локалне мреже имају различите особине у односу на стандардне локалне мреже и захтевају специјалан подслој [1] (MAC).

Стандардна конфигурација за бежичне мреже је са базним станицама (назива се и приступна тачка [2]) распоређеним по згради. Све базне станице су повезане међусобно оптичким влакнима или бакарним кабловима. Уколико је предајна снага базне станице предвиђена да покрива раздаљину од 3 до 4m, свака соба постаје једна ћелија. Зграда постаје велики ћелијски [3] систем, као што је стандардни систем мобилне телефонске (целуларне) мреже.

Вишеструки приступ са избегавањем колизије (MACA [4]) први је протокол пројектован за бежичне локалне рачунарске мреже. Основна идеја је да пошиљалац шаље примаоцу кратак рам, тако да га станице које су у близини могу да детектују и „избегну" слање за време слања долазећег, великог рама података. Протокол MACA је илустрована на слици 12.10. Посматрајмо како станица C_1 шаље рам ка станици C_2. Започиње слањем рама „захтев за слањем" (RTS [5]) ка станици C_2 (приказано је на слици 12.10а). Овај кратак рам (30 бајтова) садржи дужину рама података који треба да буде послат. Станица C_2 одговара рамом „спреман за пријем" (CTS [6]). У раму CTS налази се дужина рама података (ископираног из рама RTS). По пријему рама CTS, станица C_1 започиње слање података. Како станице које „чују" рамове RTS и CTS реагују? Свака станица која чује рам RTS довољно је близу станице C_1 и мора да остане „мирна" толико дуго да може рам CTS да стигне до станице C_1 без конфликта. Свака станица која „чује" рам CTS је близу станице C_2 и мора да остане „мирна" док се не заврши слање података

[1] *Medium Access Control*
[2] *Access point*
[3] *Cell*
[4] *Multiple Access with Collision Avoidance*
[5] *Request To Send*
[6] *Clear To Send*



Слика 12.10 MACA протокол: а) C_1 шаље RTS ка C_2 б) C_2 одговара са CTS ка C_1

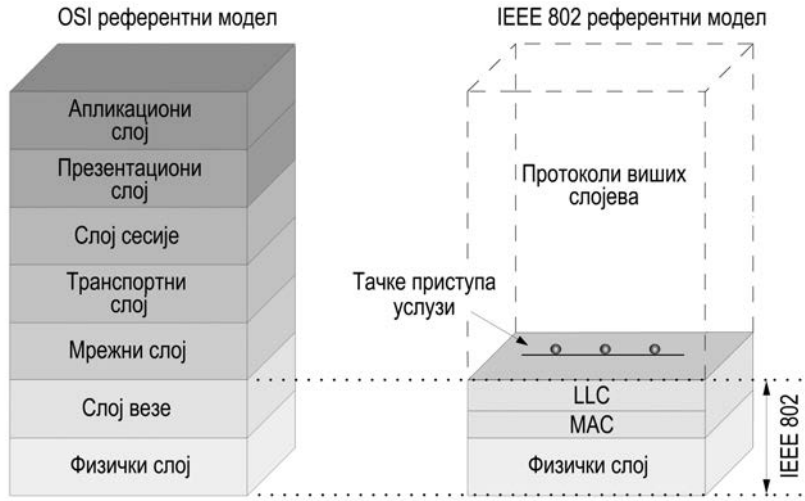
дужине која се може видети из рама CTS. На слици 12.10 станица C_3 је у опсегу станице C_1 али није у опсегу станице C_2. Због тога чује рам RTS од станице C_1 али не и рам CTS од станице C_2. Док год се не преклапа са рамом CTS, може да шаље за време слања рама података. С друге стране станица C_4 је у опсегу станице C_2 али не и станице C_1. Она не чује рам RTS али чује рам CTS. Њој пријем рама CTS указује да је близу станице која треба да прими рам, тако да одлаже слање било чега за време трајања рама података. Станица C_5 чује обе управљачке поруке, и као и станица C_4 остаје „мирна" док се се не заврши слање рама података. И поред свих мера предострожности до колизије може да дође. На пример станице C_2 и C_3 могу да пошаљу истовремено рам RTS ка станици C_1. Доћи ће до судара рамова (колизије). У случају колизије пошиљалац рама RTS (онај који не добије одговор - рам CTS после одређеног времена) чека одређени временски интервал одабран по случајној расподели и покушава касније. Алгоритам који се користи је бинарни експоненцијални [1].

Протокол MACAW [2] представља побољшану варијанту протокола MACA. Уочено је да пошто слој везе не шаље потврду о исправно примљеним пакетима, изгубљени пакети се не шаљу поново док то не утврди са значајним кашњењем транспортни слој. Да би се овај проблем разрешио шаље се рам потврде ACK по успешном пријему рама података. Такође је укључен и метод CSMA да би се спречила станица да шаље рам RTS у исто време док нека од блиских станица то ради.

12.2 Стандард IEEE 802 за локалне рачунарске мреже

Локалне рачунарске мреже по стандарду IEEE802 [3] су рачунарске мреже са заједничким медијумом кроз који се преносе подаци које могу да приме све станице у тој мрежи. Рачунарска мрежа је генерално власништво једне организације и користи је једна организација. Мреже градског подручја[4] су оптимизоване за већа растојања него локалне рачунарске мреже, нпр. неколико блокова зграда, до целих градова. Референтни модели

[1] Детаљније објашњење биће дато у поглављу IEEE 802.3.
[2] MACW-MACA *for Wireless*
[3] Користићемо термин IEEE 802 локалне мреже.
[4] MAN - *Metropolitan Area Network*



Слика 12.11 Однос архитектуре LAN&MAN/RM[1] и OSI/RM[2]

IEEE802 направљени су после OSI референтног модела. Стандарди IEEE802 укључују функционалност најнижа два слоја (физички слој и слој везе) OSI референтног модела. Дефинисана је веза са вишим слојевима и како се они односе на међусобно повезивање и управљање у локалним рачунарским мрежама.

Референтни модел IEEE802 сличан је OSI референтном моделу у дефинисању слојева и граница сервиса. Пошто су у свим IEEE802 локалним мрежама медијуми дељиви, увек је присутан MAC слој. Слика 12.11 приказује поређење архитектуре референтних модела LAN&MAN/RM[1] и OSI/RM[2]. Организација IEEE објавила је више стандарда за локалне рачунарске мреже познатих као серија[3] IEEE802. Стандарди који ће се у овом уџбенику анализирати су:

- IEEE802.1Q - дефинише архитектуру за виртуелне локалне рачунарске мреже са премошћавањем[4].
- IEEE802.2 - управљање слојем везе[5].
- IEEE802.3 - CSMA/CD метод приступа трансмисионом медијуму и спецификација физичког слоја.
- IEEE802.4 - магистрала са жетоном[6] као метод приступа трансмисионом медијуму и спецификација физичког слоја.
- IEEE802.5 - прстен са жетоном[7] као метод приступа трансмисионом медијуму и спецификација физичког слоја.
- IEEE802.11 - метод за приступ медијуму код бежичних локалних рачунарских мрежа и спецификација физичког слоја.

[1] *Local Area Network & Metropolitan Area Network/Reference Model*
[2] *Open System Interconnection/Reference Model*
[3] Списак стандарда дат је у табели 12.3 на крају овог поглавља.
[4] *Virtual Bridged Local Area Network*
[5] *Logical Link Control*
[6] *Token Bus*
[7] *Token Ring*

- IEEE802.15 - метод за приступ медијуму код бежичних локалних рачунарских мрежа[1] и спецификација физичког слоја.
- IEEE802.16 - стандардни интерфејс за широкопојасне бежичне системе градских подручја[2].

12.3 Етернет

Без обзира што Етернет и IEEE802.3 стандард нису идентични, термин Етернет се користи за мреже које подржавају стандард IEEE802.3. тј. локалне рачунарске мреже са протоколом CSMA/CD. Користећи описану терминологију архитектура локалне рачунарске мреже је:

- метод приступа: CSMA/CD,
- логичка топологија: један ка свима (бродкастинг),
- физичка топологија: традиционално магистрала, данас најчешће звезда.

Стандард IEEE802.3 има интересантну историју. Почетак је био Aloha систем пројектован да омогући радио-комуникацију између рачунара раштрканих по Хавајским острвима. Касније је реализована идеја за спајање преко 100 рачунара на 1km дугом каблу CSMA/CD система брзином 2,94Mb/s. Тај систем је назван Етернет[3]. Назив је добио по етру за који се некад сматрало да испуњава простор и да се кроз њега преноси електромагнетско зрачење.

XEROX Ethernet је био толико успешан да су XEROX, DEC, INTEL скицирали стандард за 10Mb/s локалну рачунарску мрежу познату у литератури као Етернет I. Овај стандард је 1982. године потиснут новим стандардом који је познат као Етернет II.

Објављени IEEE802.3 стандард разликује се од Етернет спецификације (слика 12.12) у томе што описује целу фамилију CSMA/CD система који раде на брзинама од 10 до 100Mb/s на различитим медијумима. Такође, једно од поља заглавља се међу њима разликује (IEEE802.3 дужина поља је коришћена за тип пакета у Етернету). Иницијални стандард даје параметре за 10Mb/s систем у основном опсегу који користи 50Ω коаксијални кабл. Скуп параметара за остале медијуме и брзине долази касније.

У раму за Етернет II поља имају следеће значење:

- преамбула од 8 октета има за циљ да обавести и омогући синхронизацију мрежне картице са долазећим подацима;
- одредишна и изворишна адреса (од по 6 октета) називају се адресе MAC слоја. Ове адресе су уписане у ROM меморији која се налази на картици. Прва три октета указују на произвођача мрежне картице и додељује их организација IEEE. Остала три октета додељује сам произвођач;
- поље тип указује на то који је протокол имплементиран на вишим слојевима. На пример поље података садржи IPX/SPX[4] пакете, у поље тип ће бити уписан број 8137_{16} Уколико се у пољу налази TCP/IP рам, поље тип ће садржати вредност

[1] *Bluetooth*
[2] *Standard Air Interface for Fixed Broadband Wireless Access Systems*
[3] *Ethernet*
[4] *Novell*

Етернет II рам података

IEEE 802.3 рам података

Слика 12.12 Формати Етернет и IEEE 802.3 рамова

0800_{16}. Ове вредности додељује организација IEEE. На овај начин омогућено је да различити протоколи виших слојева могу да користе исту мрежну картицу;

- поље за податке су укалупљени (енкапсулирани) пакети протокола виших слојева, од мрежног до апликационог. Дужина може да им буде најмање 46, а највише 1500 бајтова;
- FCS[1] је секвенца која омогућава детекцију грешака. Користи се тридесетдвобитни (32) циклични кôд CRC[2], који се генерише над пољима адресе, типа и података. Пријемна мрежна картица може да генерише идентичан циклични кôд над пољима адресе, типа и података и упоређује их са предајним циклични кôдом. Уколико су идентични пренос је обављен без грешке. Са циклични кодом од 32 бита може да се детектује импулсна сметња од 31 бита са 100% тачношћу.

12.4 Стандард IEEE802.3

Структура рама по стандарду IEEE802.3 приказана је на слици 12.13. Сваки рам почиње уводним делом[3] од седам бајтова а сваки садржи комбинацију 10101010. Код Манчестер кодовање ова комбинација даје правоугаони талас од 10MHz у трајању од 5,6μs да би омогућио да се пријемник синхронизује са пошиљаоцем. Следећи је почетак рама[4], бајт који садржи 10101011 чиме је означен почетак самог рама.

Рам садржи две адресе, једну одредишта[5] а другу извориште[6]. Стандард допушта двобајтне и шестобајтне адресе, али параметри дефинисани за 10Mb/s стандард користе шестобајтне адресе. Бит највеће тежине одредишне адресе је 0 за обичне адресе, а 1 за групне адресе. Кад је рам послат на групну адресу све станице у групи га примају. Слање групи станица назива се вишеструко емитовање[7]. Адреса која садржи све 1

[1] *Frame Check Sequence*
[2] *Cyclic Redundancy Check*
[3] *Preamble*
[4] *Start of frame*
[5] *Destination*
[6] *Source*
[7] *Multicast* - једна станица шаље групи станица.

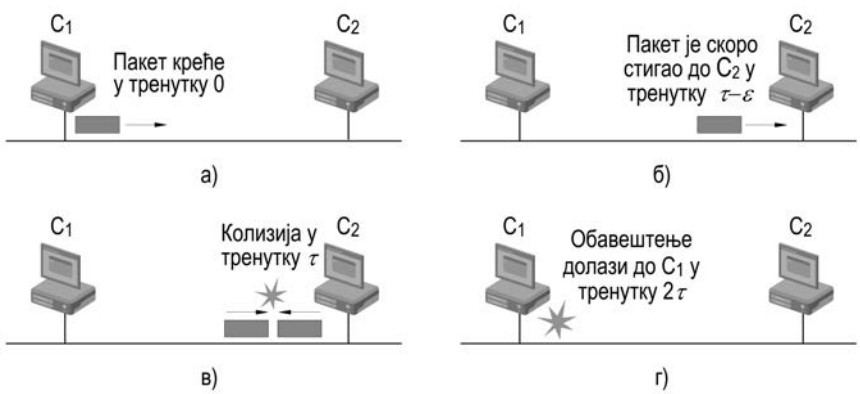
Слика 12.13 Формат рама по стандарду IEEE 802.3

је резервисана за слање свима [1]. Рам који садржи све јединице у пољу одредишне адресе биће послат свим станицама у мрежи. Још једна интересантна особина адресирања је коришћење 46. бита (суседног биту највеће тежине) за разликовање локалне од глобалне адресе. Локалне адресе додељују администратори локалне мреже и немају никакв значај изван локалне мреже. Глобалне адресе додељује IEEE тако да две станице нигде на свету немају исту глобалну адресу. Са 46 битова [2] доступно је $7x10^{13}$ глобалних адреса. Идеја је да било која станица јединствено адресира било коју другу станицу дајући тачан 46-битни број. На мрежном слоју је да лоцира одредиште.

Поље дужина [3] показује колико бајтова је присутно у пољу података, од минималних 0 до максималних 1500. Вредност поља података од 0 бајтова је дозвољена, али ствара проблем кад предајник детектује колизију, прекида слање текућег рама, што значи да се лутајући битови и делови рамова појављују у каблу све време. Да би се омогућило да се једноставније разликују важећи рамови од неважећих 802.3 захтева да је важећи рам дугачак најмање 64 бајта почевши од заглавља до контролне суме. Ако је дужина података мања од 46 бајтова користе се додатна [4] поља да попуне рам до минималне величине.

Постоји још један разлог за одређивање минималне дужине рама. Посматрајмо пример на слици 12.14:

а) станица C_1 је завршила успешно слање свог рама;
б) најудаљенија станица [5] C_2 (удаљена за τ секунди) констатовала је да је трансмисиони медијум слободан и започела са слањем у тренутку $\tau - \varepsilon$;



Слика 12.14 Детекција колизије између два удаљена краја локалне рачунарске мреже

[1] *Broadcast*- једна станица шаље свим станицама.
[2] 48-2 = 46
[3] *Length*
[4] Пад (*pad*)
[5] Време пропагације између две најудаљеније станице мреже.

в) долази до колизије коју станица C_2 детектује и шаље обавештење;
г) станица C_1 је завршила са слањем и не може да закључи да је дошло до колизије или да открије рам обавештења који је станица C_2 послала.

Ако би станица C_1 слала рам у трајању најмање 2τ она би успешно примила обавештење о колизији. Значи да минимална дужина рама треба да износи 2τ. Како се повећава брзина мреже минимална дужина рама (изражена у бајтовима) мора да расте или да се пропорционално смањи максимална дужина кабла. За локалну рачунарску мрежу дужине 2500m која ради на брзини од 1Gb/s, минимална дужина рама мора бити 6400 бајтова. Алтернатива је да дужина буде 640 бајтова а максимална дужина између било које две станице да буде 250m. Ова ограничења постају тешко савладива како се иде у правцу гигабитних рачунарских мрежа.

Последње поље рама IEEE802.3 је контролни збир [1]. То је ефективно 32-битна комбинација кода података. Ако се неки подаци приме с грешком (услед сметњи у каблу), контролни збир ће скоро сигурно бити погрешан, па ће грешка бити и детектована.

12.5 Повезивање у IEEE 802.3 локалним рачунарским мрежама

У употреби су четири начина повезивања (каблирања) као што је представљено у табели 12.1. Историјскио 10Base5 повезивање, популарно названо дебео Етернет прво је било у употреби. Повезивање на њега генерално се прави помоћу тзв. вампирских прикључница које су уметнуте у средиште коаксијалног кабла. Ознака 10Base5 значи да ради брзином 10Mb/s, користи сигнализацију у основном опсегу и може да подржи 100 рачунара по сегменту дужине до 500m.

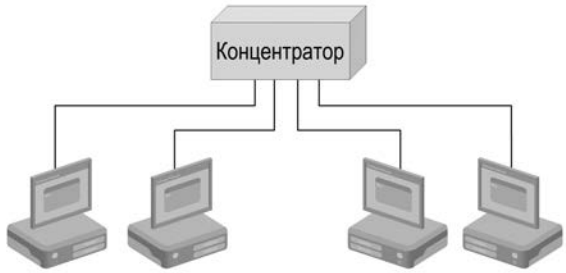
Други по редоследу појављивања је 10Base2, или танки Етернет. Повезивање се врши коришћењем индустријски стандардних BNC[2] конектора за формирање T споја. Конектори BNC су лакши за употребу и поузданији. Танки Етернет може да ради са сегментима дужине 200m и може да подржи само 30 рачунара по сегменту.

Детектовање прекида кабла, прикључница конектора био је главни проблем за оба медијума. Проблем везан за проналажење прекида каблова довео је до новог начина повезивања (слика 12.15). Све станице су каблом повезане на централни активни уре-

Име	Кабл	Максимална дужина сегмената	Број чворова по сегменту	Предности
10Base5	Дебели коаксијални (50Ω)	500m	100	Више се не користи
10Base2	Танак коаксијални (50Ω)	200m	30	Више се не користи
10BaseT	Упредене парице	100m	1024	Лако одржавање
10BaseF	Оптичко влакно	2000m	1024	Најбољи за повезивање ван зграда

Табела 12.1 Најчешће коришћене врсте повезивања у IEEE 802.3 локалним мрежама

[1] *Checksum*
[2] *Bayonet Neill -Concelman.* Конектор је добио име по проналазачима *Paul Neill* и *Carl Concelman.*



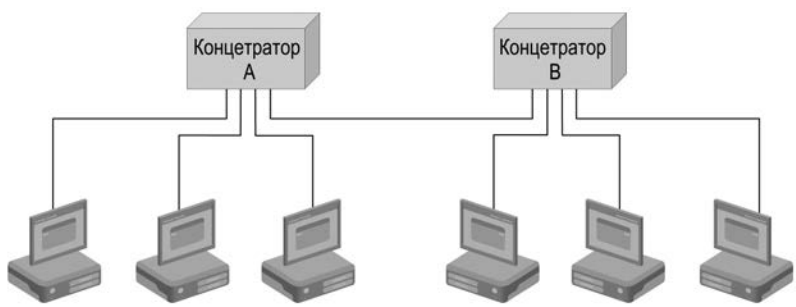
Слика 12.15 Повезивање станица помоћу активног уређаја - концентратора

ћај - концентратор (хаб)[1]. Каблови су телефонске упредене парице, пошто у већини пословних зграда постоји инсталација, и слободне парице. Овакав начин повезивања (шема) назива се 10BaseT.

Када се користи 10BaseT не постоји више дељени медијум (кабл) већ само активни елемент. Свака станица је повезана са концентратором сопственим (не дељеним) каблом. Концентратор прихвата рам који му једна од прикључених станица шаље и прослеђује га свим осталим станицама. Због тога се концентратор назива и вишеулазни обнављивач[2]. Додавање или издвајање станице у (из) мреже је једноставно, а прекид каблова лако се открива. Негативна страна 10BaseT је што максимална дужина кабла од концентратора до станице не сме да пређе 100m. Проширивање локалне рачунарске мреже постиже се додавањем и међусобним повезивањем концентратора (слика 12.16). За повећање брзине рада уместо концентратора користе се комутациони уређаји - комутатори[3]. Четврти систем каблирања - 10BaseF користи оптичка влакна. Веома је скупо решење, због високе цене конектора и терминатора, али пружа одличну заштиту од сметњи.

12.6 Стандард IEEE 802.3u

Многе инсталације захтевале су веће брзине (већи пропусни опсег). Због тога је 1992. године IEEE захтевао од 802.3 комитета да размотри могућност нових стандарда за локалне рачунарске мреже. Један од предлога био је да се задржи досадашњи



Слика 12.16 Међусобно повезивање концентратора

[1] *Hub*
[2] Вишепортни обнављивач (*multiport repeater*).
[3] Свич (*switch*). Детаљно ће бити објашњени у 14. поглављу.

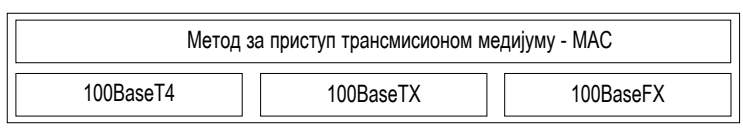
IEEE802.3 тачно какав јесте, али да се само убрза. Нови стандард је брзо направљен и потврђен од стране IEEE 1995. године као IEEE802.3u. Среће се и под називом брзи Етернет[1] и носи заједничку ознаку 100BaseT. Други предлог био је да се направи потпуно нови концепт са саобраћајем у реалном времену (нпр. за дигитализовани говор). Као резултат настао је стандард IEEE802.12[2].

Основна идеја стандарда IEEE802.3u је једноставна: задржати стари формат рама, метод за приступ трансмисионом медијуму и количину података коју рам може да пренесе. Само повећати брзину, тј. смањити време трајања бита са 100ms на 10ns. Задржане су предности 10BaseT каблирања и брзи Етернет је заснован на таквом решењу. Сви системи базирани на брзом Етернету користи активне елементе (концентраторе и комутаторе). Спецификација за брзи Етернет је предвидела и могућност аутоматског прилагођавања брзине. То значи да интерфејсни уређаји могу да раде на брзинама и 10Mb/s и 100Mb/s.

Постоје три различите спецификације у зависности од физичког медијума који се користи (слика 12.17). Стандарди 100BaseTX и 100BaseFX (заједнички се означавају са 100BaseX) представљају прилагођен стандард за физички слој који је коришћен у FDDI[3] рачунарским мрежама. Користе се две физичке везе између станица: једна за предају а друга за пријем. У табели 12.2 систематизоване су основне карактеристике ових стандарда.

Појавила се идеја да се за овај систем користе упредене парице категорије 3. Разлог је једноставан: сваки пословни објекат има најмање 4 упредене парице категорије 3 које не прелазе дужину од 100m. Значи, користећи упредене парице категорије 3 могуће је повезати рачунаре брзим Етернетом без додатног провлачења каблова. Мана упредених парица категорије 3 је немогућност да пренесу сигнале од 200MBd[4] на раздаљини од 100m (што је максимална раздаљина рачунара и активног елемента специфицирана са 10BaseT). Проблем је решен тако што се за пренос користе све четири парице и то истовремено три у једном правцу[5]. Два пара се конфигуришу као бидирекционе. Ток података је подељен у три дела: сваки од по 33,3Mb/s. Линијски сигнал је тронивоски. Техника кодирања је 8B/6T: 8 битова података се претвара у кодну групу од 6 тронивоских симбола.

100BaseFX је систем који користи оптичка влакна. Ова опција је скупља због високе цене конектора и терминатора. Има одличну имуност на сметње и користи се за ве-



Слика 12.17 Три различите спецификације физичког слоја брзог Етернета

[1] *Fast Ethernet (*IEEE 802.3u)

[2] Среће се и као 100VG-AnyLAN. Може да користи 100Mb/s Етернет преко телефонских парица категорије 3 (*Voice Grade)*. Може да преноси IEEE 802.3 и IEEE 802.5 рамове (Any).

[3] *Fiber Distributed Data Interface*. Стандард ANSI X3-T9. Користи: оптичка влакна, двоструки прстен и IEEE 802.5 протокол. Брзина по прстену је100Mb/s. Покрива раздаљине до 200km али појавом гигабитног Етернета губи на значају.

[4] 100Mb/s са Манчестер кодирањем.

[5] Наравно, уколико се користе каблови категорије 5 и навише, овај проблем не постоји.

	100BaseT4	100BaseTX	100BaseSX
Трнасмисиони медијум	4 пара UTP категорије 3, 4 и 5	2 пара: UTP категорије 5 или STP	2 оптичка влакна
Линијски кôд	8B/6T, NRZ	MLT-3	4B/5B, NRZI
Битска брзина	100Mb/s	100Mb/s	100Mb/s
Максимална дужина сегмента	100m	100m	100m
Максимални домет	200m	200m	400m

Табела 12.2 Карактеристике три различите спецификације физичког слоја стандарда IEEE 802.3u

зе између зграда или између активних елемената који се налазе на великом међусобно растојању. Користи технику кодирања 4B/5B-NRZI: 4 бита података се претвара у симбол од 5 битова који се даље кодира техником без повратка на нулу (NRZI).

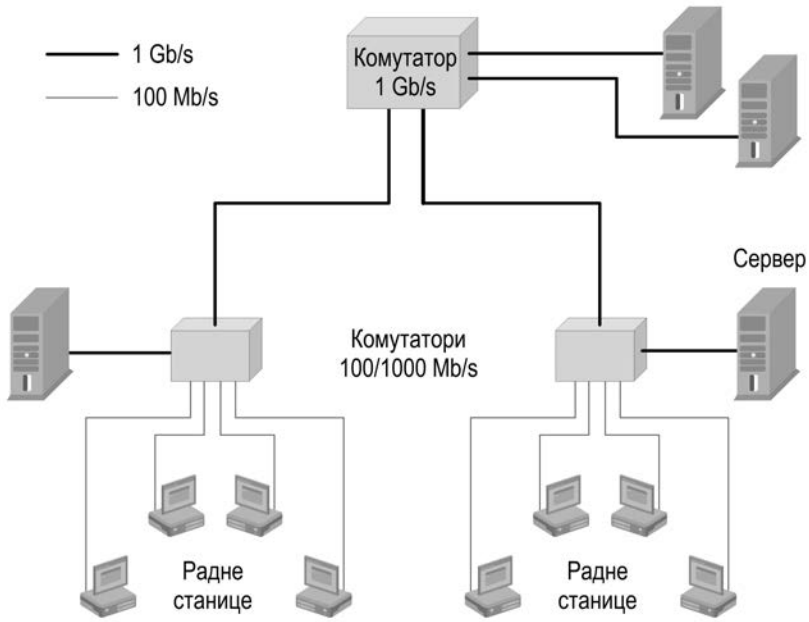
Без обзира што је техника кодирања 4B/5B-NRZI ефикасна за оптичка влакна није погодна за пренос преко упредених парица. Због тога је за 100BaseTX система предвиђена тронивоска техника кодирања MLT-3 [1].

12.7 Етернет брзине 1Gb/s

Локална рачунарска мрежа велике брзине од 1Gb/s (гигабитни Етернет) је иновиран стандард за брзи Етернет [2], који је организација IEEE стандардизовала 1998. године. Постоје две верзије: IEEE802.3z за оптичка влакна и STP каблове и IEEE802.3ab за UTP каблове категорије 5. Стандарди дефинишу следеће конфигурације:

- 1000BaseSX - користе се вишеугаона оптичка влакна, извор светлости је ласер таласне дужине 850nm [3]. Највише се користи за спратни развод. У зависности од дебљине влакна (62,5μ или 50μ) максимална раздаљина се креће од 200m до 500m.
- 1000BaseLX - користе се оптичка влакна, извор светлости је ласер таласне дужине 1310nm [4]. Употребљавају се једноугаона оптичка влакна (10μ) или вишеугаона оптичка влакна (50μ и 62,5μ). Најчешће се користи као брза окосница [5] у оквиру блиских објеката [6]. Максимална раздаљина је до 5000m.
- 1000BaseCX - користи оклопљене бакарне каблове и примопредајнике (трансивере) за раздаљине од само 25m. Најчешће служи за повезивање сервера или за повезивање брзих мрежних уређаја у оквиру ормана. Верзија 1000BaseT је практично потиснула употребу 1000BaseCX.
- 1000BaseT - Овај стандард користи сва четири пара UTP каблова категорије 5. Максимална раздаљина је 100m.

[1] Детаљније о техникама кодирања MLT-3 (*Multilevel Treshold - 3*), 4B/5T и 8B/6B може се наћи у литератури [1] и [2].
[2] *Fast Ethernet* брзине 100Mb/s
[3] Користи се ознака S (*Short*).
[4] Користи се ознака L (*Long*).
[5] Кичма - *backbone*
[6] Кампуса



Слика 12.18 Пример локалне рачунарске мреже са гигабитним Етернетом

На слици 12.18 представљена је типична примена локалне рачунарске мреже са брзинама од 100Mb/s и 1Gb/s. Комутатор окоснице мреже је брзине 1Gb/s и обезбеђује везу [1] између централног сервера и комутатора радних група брзине 100Mb/s. Сваки комутатор радне групе обезбеђује везу брзине 1Gb/s са комутатором окоснице и локалним серверима, а 100Mb/s са сервером и радним станицама.

Стратегија гигабитног Етернета идентична је са стратегијом брзог Етернета. Дефинисањем нове спецификације задржан је CSMA/CD протокол и формат IEEE802.3 рама за брзине 10Mb/s и 100Mb/s. Компатибилан је са 10BaseT и 100BaseTX системима. Постоје два побољшања у односу на CSMA/CD протокол а то су:

- проширивање величине рама на минимум 4096 битова [2],
- могућност слања групе кратких рамова [3] (један за другим) без поновне примене CSMA/CD протокола.

Гигабитни Етернет са оптичким влакнима користи 8B/10B кодирање. Сваки бајт се кодира са 10 битова. Број кодних речи је 1024 [4] тако да се у избору кодних речи користи следеће правило:

- ниједна кодна реч не треба да има више од четири идентична бита у низу,
- ниједна кодна реч не треба да има више од шест идентичних нивоа (нула или јединица).

[1] Окосницу локалне рачунарске мреже.
[2] За брзине 10 и 100 је то износило 512 битова односно 64 бајта. Овим се постиже да је време потребно да се пошаље рам дуже од времена простиарања за 1Gb/s.
[3] *Frame bursting*
[4] 2^{10}, а 2^8 је потребно за кодирање улазних података.

Кôд омогућава довољно транзиција у току података тако да пријемник остаје у синхронизацији са предајником. Због равномерног броја јединица и нула једносмерна компонента је приближно 0. Гигабитни Етернет са UTP кабловима категорије 5 (1000 BaseT) користи технику кодирања 4D/PAM5. По свакој парици кабла (има их 4) истовремено се шаље по један симбол брзином од 250Mb/s. Сваки симбол кôдира се са једним од 5 напонских нивоа: +1, -1, 0, +0,5, -0,5V. За корекцију грешака насталих због преслушавања и сметњи користи се Трелис кôд [1].

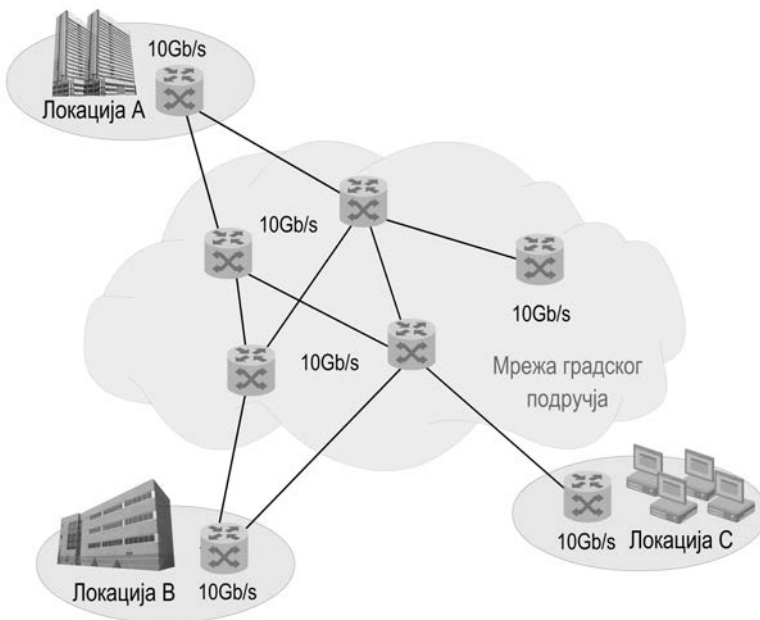
12.8 Етернет брзине 10Gb/s

Све већи саобраћај на Интернету и интранету довео је до захтева да се брзина Етернета повећа на 10Gb/s.

Стандард IEEE 802.3ae

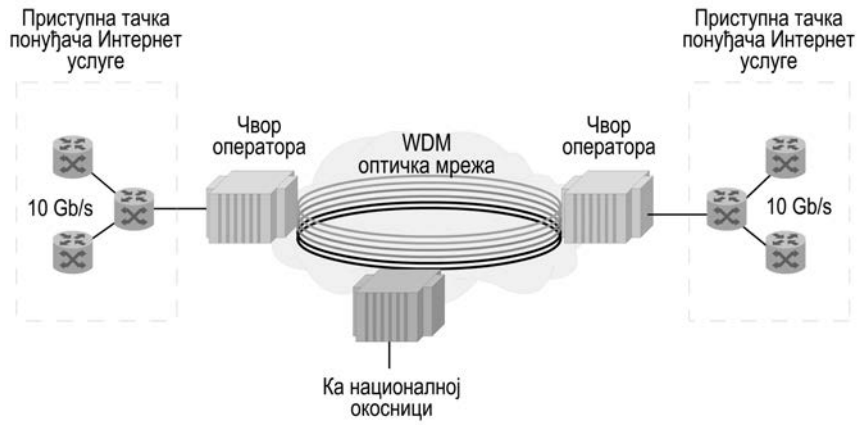
Организација IEEE је 2002. године донела нови стандард IEEE802.3ae. Основни критеријум је испоштован: користи MAC протокол, формат, минималну и максималну величину рама као оригинална 802.3 верзија.

Иницијално се предвиђало да ће се Етернет брзине 10Gb/s користити за повезивање комутатора великих капацитета (слика 12.18). Међутим, ова технологија омогућила је везе великих брзина између понуђача и корисника Интернет услуга у мрежама градских (MAN) и ширих географских подручја (WAN) (слика 12.19). Тако је Етернет технологија постала озбиљна конкуренција ATM [2] и другим технологијама



Слика 2.19 Пример употребе Етернета брзине 10Gb/s

[1] *4 Dimension 8 State Trellis Forward Error Correction*
[2] *Asynchronous Transfer Mode*



Слика 12.20 Пример Етернета брзине 10Gb/s у мрежи ширих географских подручја (WAN)

које се користе у мрежама ширег географског подручја. Максимална растојања која се могу постићи са Етернетом брзине 10Gb/s су од 300m до 40km. Као трансмисиони медијум користе се различите врсте оптичких влакана, тако да се постојеће оптичке мреже (SONET, SDH) могу искористити (слика 12.20). Начин рада је искључиво потпуни дуплекс тако да је протокол за детекцију колизије сувишан. На физичком слоју дефинисане су следеће спецификације:

- 10GBaseS - пројектована је за вишеугаона оптичка влакна са ласерима таласне дужине 850nm. Домет је 300m.
- 10GBaseL - пројектована је за једноугаона оптичка влакна са ласерима таласне дужине 1310nm. Домет је 10km.
- 10GBaseE - пројектована је за једноугаона оптичка влакна са ласерима таласне дужине 1550nm. Домет је 40km.
- 10GBaseLX4 - пројектована је за једноугаона или вишеугаона оптичка влакна са ласерима таласне дужине 1310nm. Домет је 10km. Користи се WDM[1] мултиплексирање за слање тока битова помоћу четири носиоца различите таласне дужине.

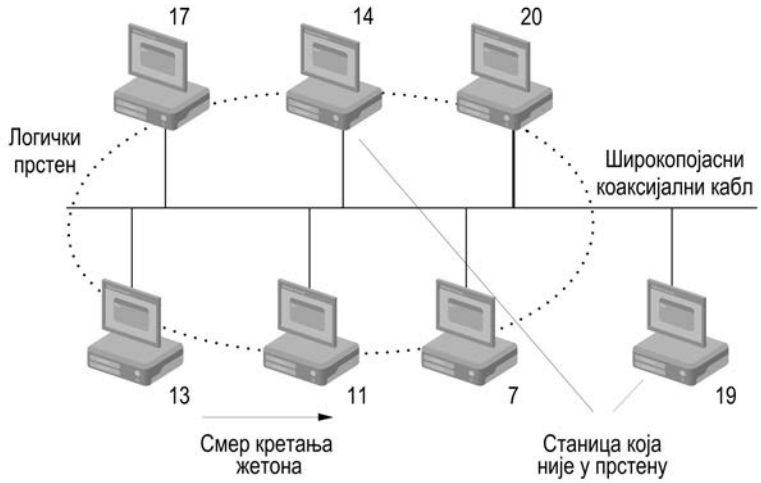
Стандард IEEE 802.3an

У јуну 2006. године објављен је стандард IEEE802.3an за Етернет рачунарске мреже брзине 10Gb/s преко упредених парица. Стандард специфицира захтеве за 10GBaseT каблирањем упреденим парицама. Организације EIA/TIA, ISO/IEC донеле су нови стандарди (2007. године) за каблирање Cat. 6A и Class EA који су усаглашени са 10GBaseT спецификацијом.

Стандард IEEE 802.3af

Енергетско напајање преко Етернета (PoE[2]) је технологија која обезбеђује напајање за системе као што су IP телефони, приступне тачке, (AP) Web камере исл.

[1] *Wavelength division Multiplexing* - мултиплексирање са различитим таласним дужинама.
[2] *Power over Ethernet*



Слика 12.21 Логички прстен

преко упредених парица Етернет мреже. Организација IEEE донела је 2003. год. стандард за овакве системе који носи ознаку IEEE802.3af. Стандард дефинише две врсте система: уређаје који се користе као извор напајања (PSE[1]) и уређаје којима се напајање обезбеђује (PD[2]).

12.9 Стандард IEEE 802.4 - магистрала са жетоном

Архитектура локалне рачунарске мреже IEEE802.4 је:

- метод приступа: са прослеђивањем жетона,
- логичка топологија: секвенцијална,
- физичка топологија: магистрала, данас уобичајено звезда.

Иако се стандард IEEE802.3 највише користи током израде IEEE802 стандарда компаније заинтересоване за аутоматизацију фабрика имале су озбиљну резервисаност у вези овог стандарда. Због равноправног приступа трансмисионом медијуму станице са мање среће могу чекати доста дуго док не успеју да пошаљу рам. Друго, IEEE802.3 рамови немају приоритете што их чини неприкладним за системе за рад у реалном времену[3], у којима важни рамови не би требало да чекају више од мање важних рамова.

Једноставан систем је прстен у коме станице чекају на ред за слање рамова. Ако има n станица и потребно је T секунди за слање рама, ниједан рам никада неће чекати више од nT секунди да би био послат. Инжењерима који раде на аутоматизацији фабрика[4], у IEEE802 комитету, свидела се идеја, али им се није свидела физичка имплементација, јер би прекид у каблу прстена оборио читаву мрежу. Даље, приметили су да је прстен лоше поклапање са линеарном топологијом са највише спојених линија. Као резултат, развијен је нови стандард, који има робусност IEEE802.3 а превазишао је лоше карактеристике пр-

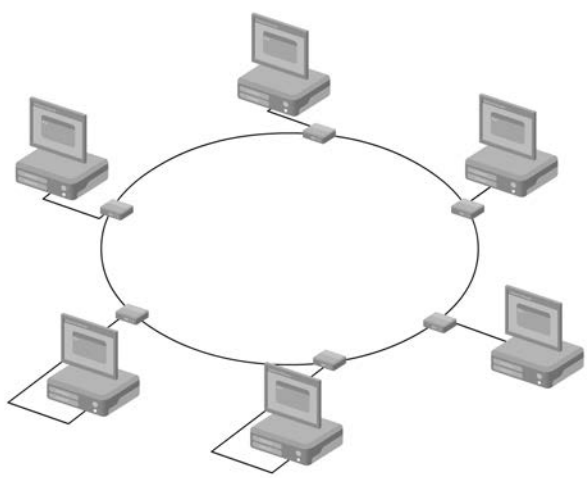
[1] *Power Sourcing Equipment*
[2] *Powered Devices*
[3] *Real time*
[4] У производним погонима *General Motorsa* користила се 802.4.

Слика 12.22 Формат рама IEEE 802.4

стена: прекид у каблу прстена обара читаву мрежу. Овај стандард носи ознаку IEEE802.4 и назив магистрала са жетоном [1]. Станице су логички организоване у прстен (слика 12.21), где свака станица зна адресе станица до ње (лево и десно - суседних). Кад се логички прстен иницира станица нумерисана највећим бројем може да пошаље први рам. Када она заврши додаје дозволу њеном непосредном суседу дајући му специјални контролни рам - жетон. Жетон пролази кроз логички прстен а власнику жетона је једино дозвољено да емитује рамове. Пошто само једна станица поседује жетон не долази до колизија. Физички распоред станица повезаних на каблу није важан. Кабл има функцију заједничке магистрале, а слање је један ка свима. Свака станица прима сваки рам, одбацујући оне који нису адресирани на њу. Кад станица дода жетон она шаље рам жетон специфично адресиран њеном логичком суседу у прстену, независно од тога где је станица физички лоцирана на каблу. Магистрала са жетоном користи 75Ω широкопојасни коаксијални кабл. Системи са појединачним и двоструким каблом дозвољени су, са или без челних завршетака. Формат рама за магистралу са жетоном приказан је на слици 12.22.

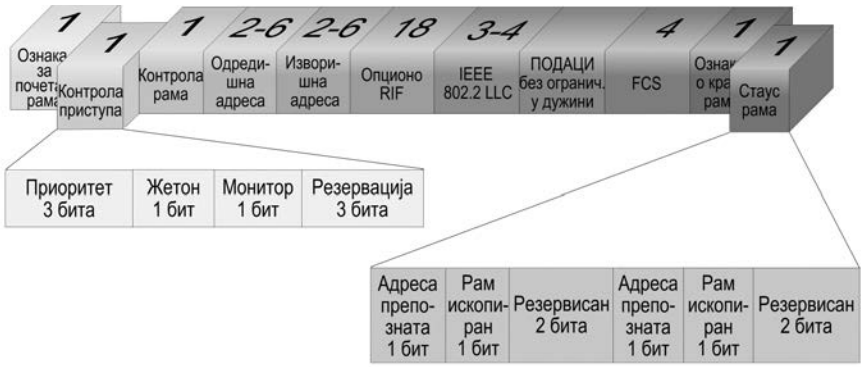
12.10 Стандард IEEE 802.5 - прстен са жетоном

Мреже у облику прстена присутне су већ доста година и дуго се користе за локалне рачунарске мреже и мреже градских подручја. Архитектура локалне рачунарске мреже је:



Слика 12.23 Прстен са интерфејсима

[1] *Token bus*



Слика 12.24 Формат IEEE 802.5 рама

- метод приступа: са прослеђивањем жетона,
- логичка топологија: секвенцијална,
- физичка топологија: традиционално прстен, данас уобичајено звезда.

Секвенцијалне (тачка-тачка везе) могу да раде на: упређеним парицама, коаксијалним кабловима или оптичким влакнима. Технологија прстена је скоро у потпуности дигитална, док IEEE802.3 има компоненту аналогног сигнала за детекцију колизије.

Прстен је јасан и има дефинисану границу приступа каналу. Из тих разлога IBM је усвојио прстен као свој стандард и IEEE прстен са жетоном стандард означио као стандард IEEE802.5. Прстен са интерфејсима је приказан на слици 12.23.

Жетон IEEE802.5 састоји се од више поља и анализираћемо намену сваког од њих (слика 12.24). Ознака о почетку рама активира мрежну интерфејсну картицу у радној станици указујући да рам жетона стиже. Уочимо да и рам жетона и рам података имају исту ознаку о почетку рама. Када прими „контролу приступа" станица може да направи разлику између рама жетона и рама података. Уколико је бит „жетон" у оквиру „контроле приступа" постављен на 0, онда примљени рам представља слободан жетон у ком случају одмах иза поља за контролу приступа следи ознака о крају рама. Станица може, примивши цео рам жетона, да у њему промени бит жетона са 0 на 1 и тиме га претвори у заузети жетон. Примљена ознака о почетку рама заједно са пољем за контролу приступа, у коме је бит жетона постављен на 1, сачињавају прва два поља IEEE802.5 рама података. Станица још додаје адресу, податке и остала поља рама података и шаље га на прстен. Уколико је бит жетона у примљеном раму био постављен на 1, онда следеће поље указује да ли овај рам садржи податке или су специјални управљачки рамови.

Иза управљачког поља су поља адресе изворишта и одредишта. Пријемна мрежна картица ће очитати одредишну адресу да би видела да ли је рам њој намењен. Уколико јесте станица ће рам учитати у своју меморију. Уколико није једноставно ће проследити рам дуж прстена без учитавања.

Поље „информације о рутирању" (RIF [1]) користи се код уређаја који носе назив „мостови са изворишним рутирањем" [2]. Намењени су међусобном повезивању више IEEE802.5 локалних рачунарских мрежа.

[1] *Routing Information Field*
[2] *Source Routing Bridge*

Брзина података [Mb/s]	4	16	100	100	1000
Трансмисиони медијум	UTP, STP, оптичка влакна	UTP, STP, оптичка влакна	UTP, STP	Оптичка влакна	Оптичка влакна
Линијски кôд	Диференцијални Манчестер	Диференцијални Манчестер	MLT-3	4B/5B, NRZI	8B/10B
Максимална величина сегмента	4550	18200	18200	18200	18200
Метод приступа	TP[1] или DTR[2]	TP или DTR	DTR	DTR	DTR

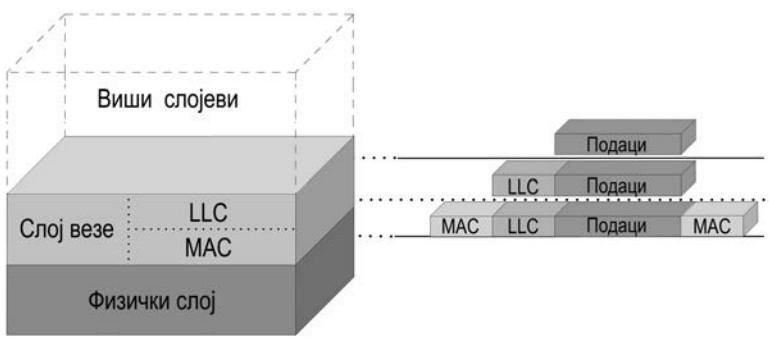
Табела 12.3 Различите варијанте физичког медијума стандарда IEEE 802.5

Заглавље IEEE802.2 се користи на исти начин као код IEEE802.3. То значи да је IEEE802.2 SNAP такође укључен у рам IEEE802.5.

Поље података садржи податке протокола виших слојева. Поље података није ограничено на фиксну максималну величину као код Етернета али може да постоји ограничење у времену колико нека станица може да задржи жетон. На пример последица временског ограничења од 10ms даје ограничење од 4500 бајтова за мрежу брзине 4Mb/s и 16000 до 18000 бајтова за мреже брзине 16Mb/s.

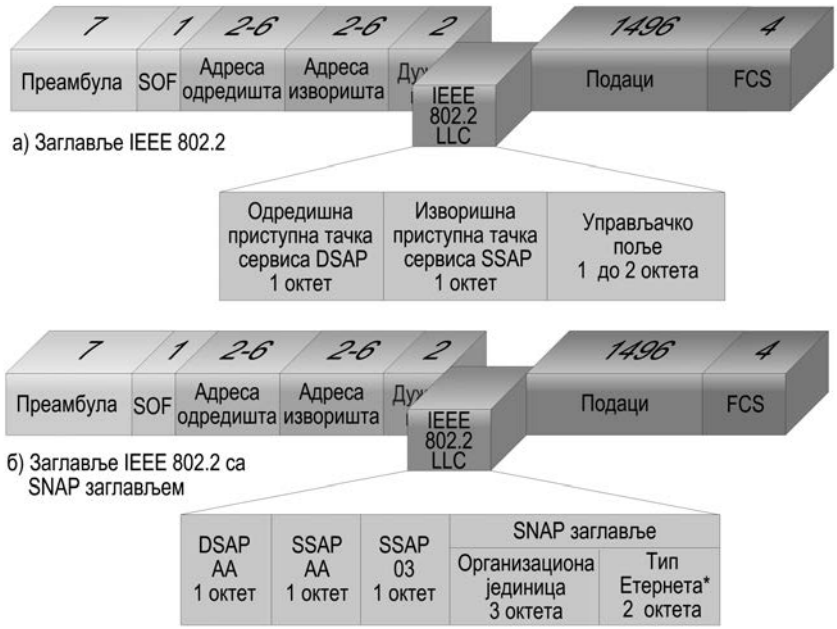
Поље FCS[3] је секвенца цикличног кода од 32 бита (као и код IEEE802.3). Ознака о крају рама значи завршетак рама, али може да значи и да је то међурам иза кога следе додатни подаци. Ознака о крају такође може да укаже да уколико је друга станица пронашла грешку у раму рам треба само проследити дуж прстена да би га изворишна станица уклонила.

Статус рама користи изворишна станица да би имала информацију о томе да ли је рам успешно испоручен. Уколико је одредишна станица препознала адресу онда се бит[4] A поставља на 1. Уколико је рам успешно ископиран у меморију одредишне станице онда се поставља бит[5] C на 1. Због сигурности постоје по два A и C бита.



Слика 12.25 Укалупљивање на LLC (*Logical Lnk control)* подслоју за управљаање логичком везом

[1] *Token Passing* - прослеђивање жетона
[2] *Dedicated Token Ring* - наменски прстен са жетоном
[3] *Frame Check Sequence*
[4] *Adress recognized*
[5] *Frame Copied*



Слика 12.26 Формат LLC рама

Стандард за IEEE802.5 иновиран је 1997. године. Предложен је нови метод за приступ трансмисионом медијуму: наменски прстен са жетоном (DTR). Користи се топологија звезде и метод са прослеђивањем жетона (TP). Могуће је користити централизовани комутатор који омогућава станицама рад у потпуном дуплексу. Овај стандард предвиђа различите брзине, различите величине рамова и различите трансмисионе медијуме као што се може видети у табели 12.3.

12.11 Протокол за управљање логичком везом

У одељку 11.6 анализирано је како станице могу да комуницирају поуздано преко непоузданих веза, користећи HDLC протокол слоја везе. Овај протокол обезбеђује контролу грешака (користећи механизам потврде) и контролу тока (користећи клизајући прозор). У анализи протокола који се користе у локалним рачунарским мрежама није било речи о поузданој комуникацији. Протоколи у IEEE802.3, 4, 5... локалним мрежама као и IP протокол нуде „најбољу могућу" услугу. Постоје системи код којих су и у локалним мрежама пожељни протоколи на слоју везе, који имају механизам за контролу тока и грешке. Организација IEEE је дефинисала протокол за управљање логичком везом (LLC[1]) који је постављен изнад IEEE802.3 и осталих IEEE802 протокола (слика 12.13). Формат, интерфејс и протокол засновани су на HDLC протоколу и описани су стандардом IEEE802.2.

Типична примена услуга LLC подслоја је следећа: мрежни слој на предајној станици предаје пакет LLC подслоју користећи LLC примитиве. LLC подслој додаје загла-

[1] *Logical Link Control*

Стандард	Опис
IEEE 802.1	Протоколи за међусобно повезивање локалних мрежа и мрежа градског подручја, сигурност, управљање, архитектура и протоколи виших слојева (*Internetworking among 802 LANs, MANs, link security, network management, protocol layers above the MAC& LLC layers*)
IEEE 802.1D	Мостови (*MAC Bridges*)
IEEE 802.1O	Виртуелне локалне рачунарске мреже (*Virtual LANs*)
IEEE 802.1X	Управљање приступом мрежи (*Port Based Network Access Control*)
IEEE 802.1AB	Протокол за препознавање на мрежи [1] (*Station and Media Access Control Connectivity Discovery*)
IEEE 802.2	Управљање логичком везом (*Logical Link Control*)
IEEE 802.3	Вишеструки приступ са детекцијом колизије (*CSMA/CD*)
IEEE 802.4	Магистрала са жетоном (*Token bus*) - не користи се
IEEE 802.5	Прстен са жетоном (*Token ring*)
IEEE 802.6	Мреже градских подручја (*Metropolitan Area Network*) - не користи се
IEEE 802.7	Широкопојасне локалне рачунарске мреже са коаксијалним кабловима (*Broadband LAN using Coaxial Cabel*) - не користи се
IEEE 802.8	Оптичке мреже (*Fibre optic Technical Advisory Group*) - не користе се
IEEE 802.9	Локалне рачунарске мреже интегрисаних услуга (*Integrated Service LAN*) - не користи се
IEEE 802.10	Сигурност локалних мрежа (*Interoperable LAN Security*) - не користи се
IEEE 802.11	Бежичне локалне рачунарске мреже [2] (*Wireless LAN*)
IEEE 802.12	Приоритети по захтеву (*Demand priority*)
IEEE 802.13	Не користи се
IEEE 802.14	Кабловски модеми (*Cable modems*)
IEEE 802.15	Бежичне личне мреже (*Wireless PAN*)
IEEE 802.15.1	*Bluetooth* [3]
IEEE 802.16	Бежични широкопојасни приступ [4] (*Broadband Wireless Access*)
IEEE 802.16e	Мобилни бежични широкопојасни приступ (*Mobile Broadband Wireless Access*)
IEEE 802.17	Прстен са пакетском комутацијом (*Resilient packet ring*)
IEEE 802.18	Група за усаглашавање радио IEEE 802 пројеката (*Radio Regulatory Technical Advisory Group*)
IEEE 802.19	Група води рачуна о коегзистенцији IEEE 802 пројекта (*Coexistence TAG*)
IEEE 802.20	Мобилни широкопојасни бежични приступ (*Mobile Broadband Wireless Access*)
IEEE 802.21	Преузимање независно од врсте мреже (*Media Independent Handoff*)
IEEE 802.22	Бежичне регионалне мреже (*Wireless Regional Area Network*)

Табела 12.4 Стандарди организације IEEE

[1] Практично је ратификован протокол *LLDP (Link Layer Discovery Protocol)* који омогућава станици да на мрежи објави свој идентитет.
[2] *Wi Fi* сертификат
[3] *Bluetooth* сертификат
[4] *Wi MAX* сертификат

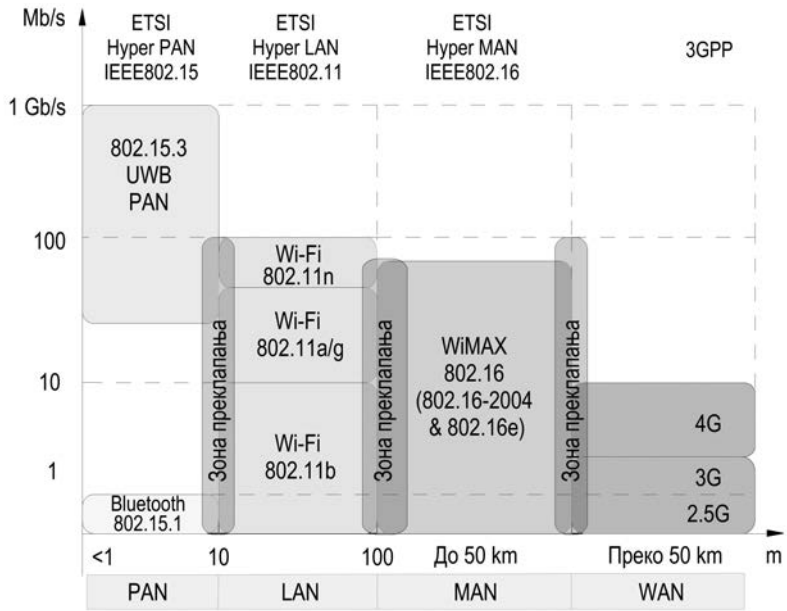
ваће, добијена целина се убацује у поље за податке рама IEEE802 и шаље преко трансмисионог медијума. На одредишној страни одвија се обрнути процес (слика 12.25). Подслој LLC подржава три типа услуга: непоуздану без успоставе везе (датаграм), без успоставе везе са потврдом и поуздану са успоставом везе. На слици 12.26 илустрована су поља која садржи јединица података LLC подслоја.

Тип протокола који је укључен у јединицу података одређен је приступним тачкама сервиса - одредишном (DSAP[1]) и изворишном (SSAP[2]). Овим пољима одговарају поља „врста"[3] у IEEE802.3 раму. Кôд SAP-а означава протокол који су произвођачи усагласили са организацијом IEEE. На пример, SAP кôд E0 указује на протокол произвођача *Novel*l, кôд 06 на TCP/IP протоколе. Рамови који се формирају и размењују у локалним рачунарским мрежама под *Netware*[4] оперативним системом се означавају као *Netware* IEEE802.2. Некада није лако обезбедити да је протокол усаглашен са IEEE, па је за такав случај развијен протокол SNAP[5]. Сваки протокол може да користи SNAP са IEEE802.2 и на тај начин се појављује као усаглашени протокол.

[1] *Destination Service Access Point*
[2] *Source Service Access Point*
[3] *Type*
[4] Произвођач *Novell*
[5] S*ubnetwork Access Protocol*

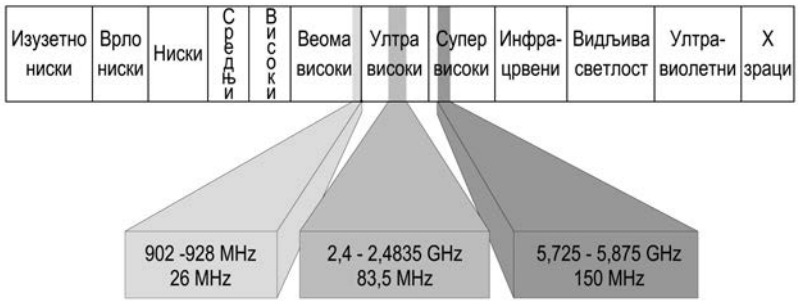
13. Бежичне рачунарске мреже

Бежичне рачунарске мреже предмет су великог интересовања произвођача, организација које се баве стандардизацијом и корисника. У зависности од растојања (као што је и код кабловских мрежа случај) оне су категоризоване у четири групе: бежичне личне мреже (WPAN[1]), бежичне локалне рачунарске мреже (WLAN[2]), бежичне рачунарске мреже градских подручја (WMAN[3]) и бежичне рачунарске мреже ширих географских подручја (WWAN[4]). Многе организације баве се стандардизацијом рачунарских мрежа нпр.: IEEE, ETSI, ANSI, ISO, 3GPP... Другу групу представљају регулаторна тела (нпр. FCC, ETSI) која дефинишу стандарде везане за коришћење радио-медијума. Трећу групу представљају асоцијације произвођача као што су на пример WiFi Alliance, WiMax Forum и Bluetooth SIG. Намена ових асоцијација је да промовишу и сертификују могућност међусобног рада производа који су добили њихове сертификате. На слици 13.1 дат је приказ опсега брзина и растојања која покривају производи по стандардима, за које ове оргнизације дају одговарајуће сертификате.



Слика 13.1 Домет и брзине стандарда у бежичним комуникационим мрежама: ETSI Hyper PAN, LAN, MAN[5]; IEEE802.11, 15, 16 и 3GPP (2.5, 3 и 4G)

[1] *Wireless Personal Area Network* - бежичне личне рачунарске мреже
[2] *Wireless Local Area Network* - бежичне локалне рачунарске мреже
[3] *Wireless Metropolitan Area Network* - бежичне градске рачунарске мреже
[4] *Wireless Wide Area Network* - бежичне рачунарске мреже ширих подручја
[5] Европски стандарди (ETSI) за персоналне мреже, локалне рачунарске мреже и градске мреже. Одговарају IEEE серији стандарда.



Слика 13.2 ISM опсега који се користи за бежичне локалне рачунарске мреже

13.1 Бежичне локалне рачунарске мреже

Први експеримент бежичног повезивања рачунара реализован је 1970. године у лабораторијама IBM-а у Швајцарској. Та рачунарска мрежа заснивала се на преносу у инфрацрвеном [1] делу спектра. Исте године и Hewlett-Packard оформио је своју бежичну рачунарску мрежу користећи радио-таласе. Брзине које су достигнуте биле су 100kb/s, али ниједан од тих производа није доживео комерцијалну примену.

Развој бежичних мрежа наставља се 1985. године пошто је FCC одобрио коришћење опсега радио-фреквенцијског спектра без посебних дозвола за потребе индустрије, научних истраживања и медицине (ISM [2]). Овај фреквенцијски опсег обухвата три групе фреквенција: 902 - 928MHz; 2,4 - 2,4835GHz и 5,725 - 5,875GHz (слика 13.2).

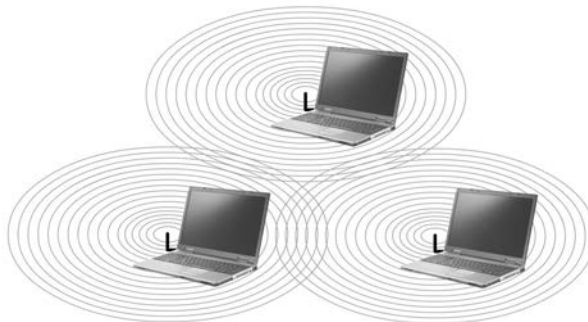
Модуларност и флексибилност бежичних локалних рачунарских мрежа чини их добрим решењем за поједине објекте као на пример: повезивање рачунара на сајмовима, у болницама, библиотекама, повезивање зграда које су раздвојене прометним саобраћајницама или реком, у зградама од историјске вредности у којима није дозвољена промена изгледа зграде, али и као допуна или проширење кабловских мрежа.

Бежичне мреже пружају велику флексибилност и могућност комбиновања различитих начина повезивања. Искристалисале су се следеће топологије: само за ову прилику (*ad hoc*), инфраструктурна и тачка-тачка.

13.2 Топологије бежичних локалних рачунарских мрежа

Ad hoc локалне рачунарске мреже (слика 13.3) омогућавају корисницима успостављање везе „свако са сваким" без уређаја за приступ (AP [3]). Као такве погодне су за комуникацију између мањих група корисника на малом растојању и углавном се примењују тамо где је потребно брзо успоставити привремену мрежу [4]. Да би могла да се оствари међусобна комуникација потребно је да сваки рачунар буде у домету свих осталих рачунара, што ограничава покретљивост корисника на релативно мали простор.

[1] *Infra Red*
[2] *Industrial Scientific Medical*
[3] *Access Point*
[4] Нпр. састанци, скупови, сајмови.

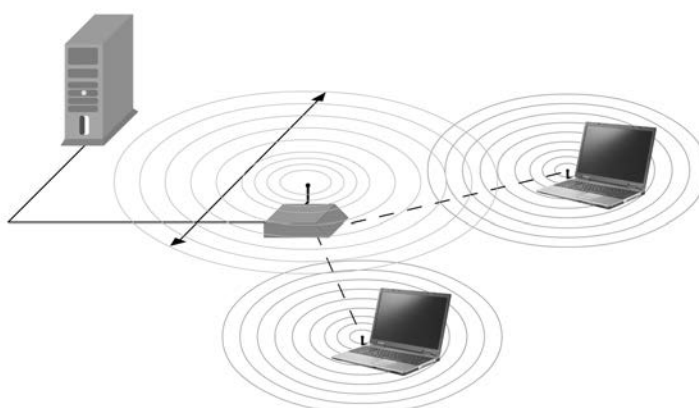


Слика 13.3 *Ad hoc* начин међусобног повезивања рачунара

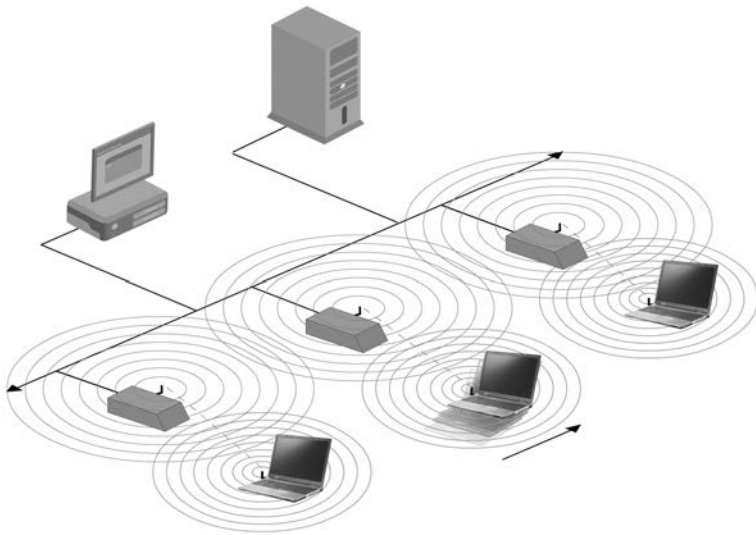
Уколико станице нису у стању да комуницирају без посредства уређаја за приступ AP онда се примењује начин рада који захтева одговарајућу инфраструктуру (слика 13.4). Све станице које се налазе у зони покривања уређаја за приступ међусобно комуницирају преко њега.

Домет једног уређаја за приступ зависи од примене и креће се од 100m у затвореним просторима до 300m на отвореном. Број корисника које може да опслужи један уређај за приступ зависи од произвођача и креће се од 15 до 50.

У случају да се жели повећати покривеност може се инсталирати више уређаја за приступ и формирати ћелијска (целуларна) мрежа (слика 13.5). У таквој мрежи станице не могу да комуницирају директно међу собом већ искључиво посредством уређаја за приступ, међусобно повезаних кабловима у рачунарску мрежу. Одређеним бројем приступних станица може се покрити одређено подручје, при чему се зоне покривања појединих станица, тзв. ћелије, могу међусобно делимично и преклапати. У случају да је у одређеној ћелији велика густина саобраћаја могуће је исту површину покрити са више приступних станица, које међусобно деле мрежни саобраћај и на тај начин омогућавају опслуживање већег броја корисника.



Слика 13.4 Међусобно повезивање рачунара помоћу уређаја за приступ (инфраструктурни начин)



Слика 13.5 Ћелијски начин међусобног повезивања рачунара

Карактеристика ћелијских мрежа је да корисници могу бити покретљиви у току рада, мењајући приступне станице преко којих комуницирају са остатком мреже. Уређаји за приступ AP везују се на ожичену мрежу[1]. Такође се по потреби могу и бежичним путем повезати на остатак мреже.

У одређеним ситуацијама погодне су и мреже типа тачка-тачка, на пример за повезивање две удаљене локалне мреже. Најчешће се изводе коришћењем усмерених радио-веза ако су ван објеката, или употребом инфрацрвене технологије ако су везе унутар једне просторије. Ове везе најчешће су фиксног карактера, односно њихови корисници не могу бити мобилни.

13.3 Технологије бежичних локалних рачунарских мрежа

Бежичне локалне рачунарске мреже WLAN према техници преноса генерално се могу поделити на следеће категорије:

- технике преноса у инфрацрвеном делу спектра (IR[2]),
- технике проширеног спектра (SS[3]) и
- ускопојасне микроталасне технике[4].

Пренос у инфрацрвеном делу спектра

Инфрацрвени системи IR за пренос података користе веома високе фреквенције, нешто ниже од видљивог дела спектра. До сада су се користили за даљинско управљање уређаја у домаћинству. У скорије време користе се за повезивање у бежичним локалним рачунарским мрежама. Као и светлост, IR таласи не могу да прођу кроз саме

[1] Кичму - *backbone*
[2] *Infrared Technology*
[3] *Spread Spectrum*
[4] *Narrowband Microwave*

објекте, тако да разликујемо усмерену (директну) и дифузну[1] технологију IR преноса. Усмерени системи (јефтинији) захтевају директну линију видљивости, тако да се користе углавном за личне локалне рачунарске мреже (PAN[2]). Дифузни IR WLAN системи не захтевају линију видљивости, али је величина ћелије одређена просторијом у којој систем ради. Због области покривености (једна просторија):

- обезбеђена је једноставна заштита од прислушкивања,
- не постоји интерференција између суседних ћелија.

Технике проширеног спектра

Тренутно најпопуларније врсте бежичних локалних рачунарских мрежа користе технике проширеног спектра[3]. У зависности од начина ширења спектра технике су подељене на системе са директном секвенцом (DSSS[4]) и на системе са фреквенцијским скакањем (FHSS[5]). Међусобно поређење ових система дато је у табели 13.1.

Ускопојасни системи

Ускопојасни радио-системи користе се за пренос података од раних 80-их. Корисницима се додељују уски фреквенцијски опсези, о чему воде рачуна посебна тела на

Бежични системи / Карактеристике	IR системи		Системи са проширеним спектром		Радио системи
	Дифузни IR системи	Усмерени IR системи	FSSS системи	DSSS системи	Ускопојасни микроталаси
Брзина података [Mb/s]	1 до 4	1 до 10	1 до 3	2 до 50	10 до 20
Мобилност	Стационарни/ мобилни	Стационарни у линији видљивости	Мобилни	Стационарни / мобилни	
Домет [m]	15 до 60	25	30 до 100	30 до 250	10 до 100
Таласна дужина/ фреквенцијски опсег	Од 850 до 950nm		902 до 928MHz 2,4 до 2,4835GHz 5,725 до 5,85GHz		902 до 928MHz 5,2 до 5,725GHz 18,825 до 19,205GHz
Модулациона техника	ASK		FSK	QPSK	FS / QPSK
Снага зрачења	-		< 1W		25mW
Метод приступа	CSMA	Прстен са жетоном/ CSMA	CSMA		Aloha, CSMA
Да ли се захтева лиценца?[6]	НЕ		НЕ		Да ако не користе ISM

Табела 13.1 Поређење технологија бежичних локалних рачунарских мрежа WLAN

[1] Инфрацрвена светлост се дифузно рефлектује од светло обојених површина. Због тога је могуће искористити рефлексију да би се постигла покривеност целе просторије.
[2] *Personal Area Network*
[3] Детаљно су обрађене у 7. поглављу.
[4] *Direct Sequency Spread Spectrum Technology* - проширени спектар са директном секвенцом
[4] *Frequency Hoping Spread Spectrum* - проширени спектар са фреквенцијским скакањем
[6] Лиценца подразумева да се држави плаћа коришћење одговарајућег фреквенцијског опсега.

нивоу државе. Корисници шаљу и примају податке на тачно одређеној учестаности. Ширина фреквенцијског опсега је што је могуће ужа.

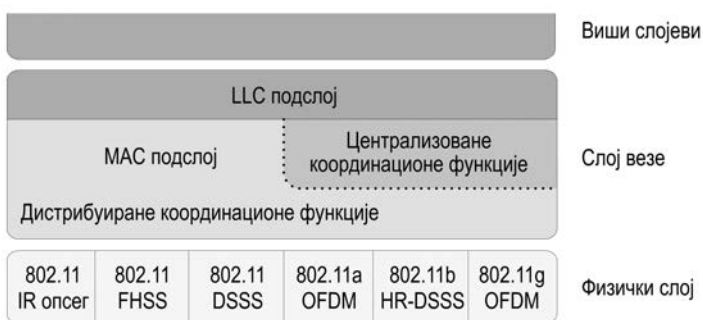
Нежељена преслушавања између канала избегавају се фреквенцијским планирањем, а сигурност и избегавање интерференције постижу се употребом посебних радио-фреквенција. Филтер на пријемнику одстрањује све сигнале осим жељеног. Први произвођач који је направио ускопојасну бежичну рачунарску мрежу у нелиценцираном фреквенцијском опсегу је RadioLAN 1995. године.

13.4 Стандарди серије IEEE 802.11

Стандард IEEE802.11 (објављен 1997. год.) тренутно је најпопуларнији стандард у области WLAN мрежа. Локалне рачунарске мреже могу да раде у једном од два режима: са базном станицом и без базне станице (слике 13.3 и 13.4). Стандард IEEE802.11 узео је то у обзир. У овом поглављу биће анализирани скуп протокола [1] IEEE802.11, бежичне технике преноса физичког слоја, протоколи MAC подслоја, формат рама и понуђене услуге. Организација IEEE је од 1997. године до данас издала бројне стандарде [2] за бежичне локалне рачунарске мреже. Стандарди који су до сада нашли широку примену су: IEEE802.11, IEEE802.11a, IEEE802.11b и IEEE802.11g. Стандарди за које се сматра да ће се користити у будућности су: IEEE802.11i (сигурност [3]), IEEE802.11e (квалитет услуга [4]), IEEE802.11s (покретна возила [5]), IEEE802.11p и IEEE802.11n (велике брзине [6]).

13.5 Архитектура IEEE 802.11

Протоколи који се користе у серији IEEE802 имају заједничку структуру (слика 13.6). Стандард се односи на прва два слоја OSI архитектуре: физички слој и слој везе. Подслој MAC (слоја везе) одређује начин доделе канала. А подслој LLC (слоја везе) има задатак да заштити више слојеве од различитости техника IEEE802 серије.



Слика 13.6 Слојевита архитектура протокола у бежичним локалним рачунарским мрежама

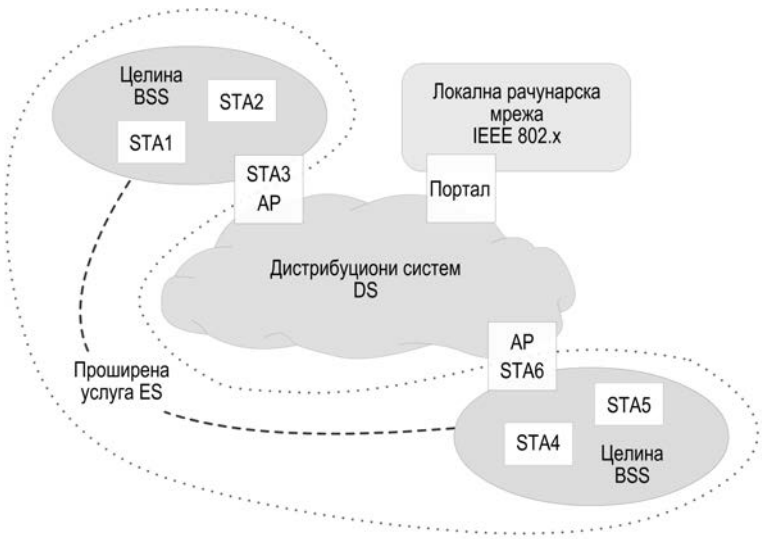
[1] *Protocol stack*
[2] У табели 13.5 (на крају поглавља) дат је списак проширења IEEE802.11 стандарда. Један је стандард IEEE802.11 али се користи термин стандард и за проширење стандарда.
[3] *Enhanced Security*
[4] QoS (*Quality of Service*)
[5] WAVE (*Wireless Access for the Vehicular Environment*) - на пример амбулантна возила.
[6] *High Speed*

У општем случају мрежа IEEE802.11 састоји се од једне или више целина са основном (базном) услугом (BSS[1]), које су повезане са дистрибуционим системом (DS[2]). Обично је дистрибуциони систем ожичена локална рачунарска мрежа која има функцију окоснице али може да буде и било која друга комуникациона мрежа. Целина са базном услугом (BSS) основна је градивна целина архитектуре IEEE802.11. Група станица (STA[3]) која је под директним управљањем једне координационе функције формира целину са основном услугом (BSS).

Координационе функције могу да буду: дистрибуиране координационе функције (DCF[4]) и централизоване координационе функције (PCF[5]). Област коју покрива BSS целина означава се као област базном услугом (BSA[6]) и одговара ћелији у целуларним комуникационим мрежама. Све станице у BSS целини могу међусобно директно да комуницирају. Може се десити да неке станице постану невидљиве због слабљења сигнала, као последице мултипутног фединга или због интерференције суседних станица.

Ад хок мрежа представља груписање станица у једну целину са основном услугом (BSS). Стандард IEEE802.11 користи назив независна BSS целина (IBSS[7]). Било која станица у целини са основном услугом може да комуницира са било којом другом станицом без уређаја за приступ (AP).

Када се за комуникацију између станица користи уређај за приступ (AP) онда стандард IEEE802.11 за такву мрежу користи термин инфраструктурна мрежа. Уређај за при-



Слика 13.7 Архитектура IEEE802.11

[1] *Basic Service Sets*
[2] *Distribution System*
[3] *Stations*
[4] *Distributed Coordination Function*
[5] *Point Coordination Function*
[6] *Basic Service Area*
[7] *Indipendent Basic Service Area*

ступ омогућава проширење опсега и могућност комуникације више целина са основном услугом. Проширена услуга (ESS[1]) састоји се од две или више целина са основном услугом, међусобно повезаних дистрибуционим системом. Проширена услуга појављује се као једна логичка локална рачунарска мрежа на подслоју слоја везе (LLC).

На слици 13.17 уређај за приступ (AP) представљен је као део станице; представља логику у оквиру станице која омогућава и приступ дистрибуционом систему (DS) и саму станицу. Дистрибуциони систем (дефинисан стандардом IEEE802.11) је независан од имплементације. То значи да дистрибуциони систем може да буде кабловска IEEE802.3 локална рачунарска мрежа, или магистрала са жетоном IEEE802.4, или прстен са жетоном IEEE802.5, или неки други IEEE802.11 медијум.

За интеграцију IEEE802.11 архитектуре са традиционалним локалним рачунарским мрежама са жичаним трансмисионим медијумима[2], или за повезивање на Интернет, користи се портал. Логика портала се уграђује у уређаје као што су мостови или рутери који су део кабловске рачунарске мреже и који су прикључени на дистрибуциони систем (DS).

13.6 Протоколи MAC подслоја IEEE 802.11

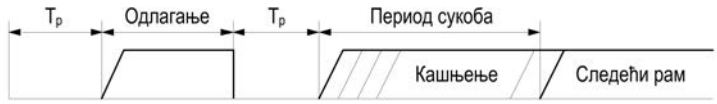
Протокол на MAC подслоју стандарда IEEE802.11 значајно се разликује од протокола на MAC подслоју стандарда IEEE802.3, због веће сложености бежичних у односу на кабловске системе. Код IEEE802.3 система станица чека док се трансмисиони медијум не ослободи и тек онда започиње са слањем. Уколико не прими ометајући сигнал[3] (који указује да је дошло до колизије) скоро је сигурно да је рам успешно испоручен одредишту. Код бежичних система ситуација је мало другачија.

Постоји проблем невидљиве станице[4]: све станице нису једна другој у радио-домету па се може десити да се предаја у једном делу ћелије не може детектовати у другом делу исте ћелије. У примеру на слици 12.10 станица C_1 шаље податке ка станици C_2. Станица C_1 испитује канал и пошто је ван домета станице C_3 погрешно ће закључити да је канал слободан и да може да започне са слањем података ка станици C_2.

Постоји и други проблем: станица C_2 жели да пошаље податке станици C_4 и испитује канал. Кад открије да постоји неки сигнал погрешно ће закључити да не може да започне са слањем ка станици C_4 пошто станица C_1 шаље податке ка станици C_4. Многи радио-системи су полудуплексни што значи да не могу истовремено и да шаљу и да испитују (ослушкују) медијум на истој радио-учестаности. Последица тога је да IEEE802.11 системи не могу да користе CSMA/CD протокол који се користи код IEEE802.3 система. Да би разрешио овај проблем IEEE802.11 је предвидео два начина рада:

- рад са дистрибуираним координационим функцијама (DCF), код кога се не користи централизовано управљање,
- рад са централизованим координационим функцијама (PCF), код кога базна станица управља свим активностима у ћелији.

[1] *Extended Service Set*
[2] Користи се и термин не-IEEE802.11.
[3] После 64 бајта за брзине од 10Mb/s (12.2 одељак).
[4] Одељак 12.1.



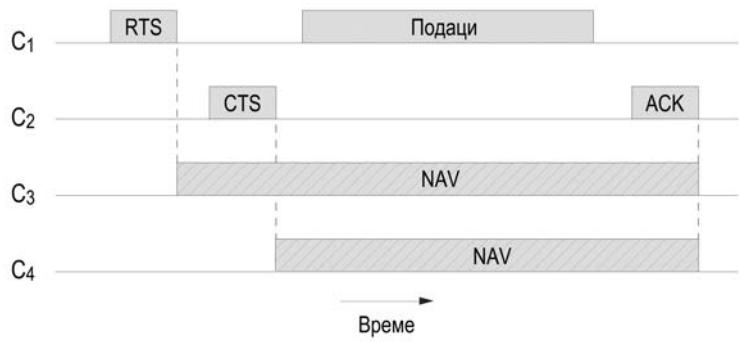
Слика 13.8 Протокол CSMA/CA

Дистрибуиране координационе функције

Системи који примењују дистрибуирану координациону функцију користе протокол са избегавањем колизије (CSMA/CA [1]). Протокол се састоји у следећем (графички приказано на слици 13.8):

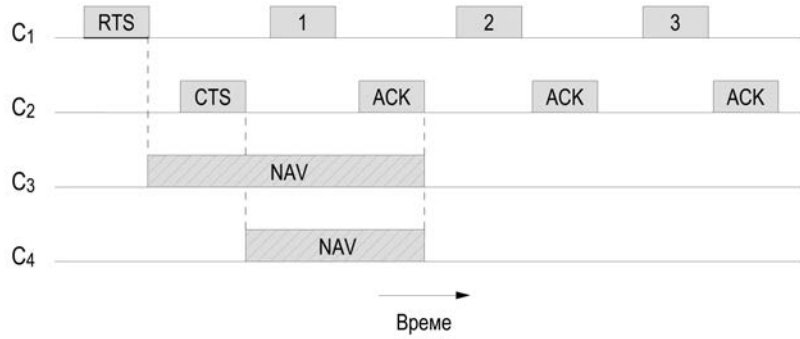
1. Станица која жели да шаље податке прво испитује трансмисиони медијум. Ако је слободан чека одређено време [2] T_P да види да ли ће и даље бити слободан. Уколико је и по истеку T_P времена медијум и даље слободан започиње са слањем;
2. Уколико је трансмисиони медијум заузет, било зато што је већ био заузет, било зато што је постао заузет после T_P времена, станица одлаже слање, чека да се заврши слање и да се медијум ослободи;
3. Када се текуће слање заврши станица чека још T_P времена. Уколико је медијум и тада слободан станица чека још неко случајно време [3]. Ово је период сукоба [4] у коме станице могу да се „боре" за медијум. Ако по истеку случајног времена нико није заузео медијум станица може да започне са слањем података.

Кашњење (случајно време) које се користи је бинарно експоненцијално и користи се код саобраћаја великог интензитета. Понављање неуспелих покушаја слања података доводи до све дужих одлагања слања, што помаже да се саобраћај развуче у времену. Ако се не би користило случајно кашњење догодило би се следеће: две станице које покушају истовремено да шаљу податке дошле би у колизију. Уколико би без међусобно различитог кашњења покушале поново да шаљу поново би дошло до колизије.



Слика 13.9 Употреба испитивања виртуелног канала са протоколом CSMA/CA

[1] *CSMA with Collision Avoidance* - CSMA са избегавањем колизије.
[2] Ово време се означава као време између рамова.
[3] Користи се исти алгоритам са бинарним експоненцијалним кашњењем као код IEEE802.3.
[4] *Contention time*



Слика 13.10 Слање фрагмената

Други начин који се користи код система са дистрибуираном координационом функцијом је заснован на протоколу MACAW и користи испитивање виртуелног канала као што је приказано на слици 13.9.

Анализирајмо опет пример станице C_1 која жели да пошаље податке станици C_2. Она прво шаље RTS рам којим тражи дозволу од станице C_2 да јој пошаље податке. Када станица C_2 добије захтев RTS станице C_1, и ако жели да прими податке од ње, она шаље натраг дозволу - рам CTS. По пријему CTS рама станица C_1 шаље рам са подацима и поставља на одређено време часовник за потврду ACK. Када станица C_2 прими рам података она шаље рам потврде ACK и размена је окончана. Уколико време на које је часовник ACK постављен истекне пре него што стигне рам потврде ACK цела процедура се понавља.

Посматрајмо како размену података виде станице C_3 и C_4. Станица C_3 је у домету станице C_1 и може да прими RTS рам. Уколико га је примила она може на основу података из рама RTS да закључи да ће станица C_1 бити заузета одређено време. На основу тога станица C_3 поставља на одређену вредност индикатор заузетости канала (NAV[1]). Рам RTS не може да допре до станице C_4 али може рам CTS, пошто је станица C_4 у домету станице C_2. Станица C_1 поставља на одређену вредност своју ознаку заузетости канала (NAV). Треба уочити да ознаке о заузетости канала (NAV) нису рамови који се шаљу; они су само интерни показатељи који указују колико дуго станица не треба ништа да шаље.

За разлику од кабловских локалних рачунарских мрежа бежичне рачунарске мреже су непоуздане и са великим сметњама. Због тога је у IEEE802.11 рачунарским мрежама предвиђено дељење рамова у мање целине - фрагменте. Сваки фрагмент садржи свој контролни збир. Фрагменти су нумерисани и потврђују се помоћу протокола заустави се и чекај[2]. Фрагменти се шаљу један за другим (слика 13.10).

Централизоване координационе функције

Други начин приступа медијуму код IEEE802.11 система је помоћу централизоване координационе функције (PCF). Базна станица[3] шаље упит (полира) другим стани-

[1] *Network Allocation Vector*
[2] Поглавље 7.
[3] Централизовани координатор.

цама у ћелији да би видела да ли имају податке за слање. Пошто редослед слања потпуно одређује базна станица до колизије не може да дође. Стандард прописује механизам полирања али не и учестаности, редослед или приоритете полирања.

Основни механизам састоји се у томе да базна станица шаље посебан рам [1] периодично (10 до 100 пута у секунди). Посебан рам садржи параметре система као што су учестаност скакања и такт за синхронизацију. Такође се позивају нове станице да се пријаве.

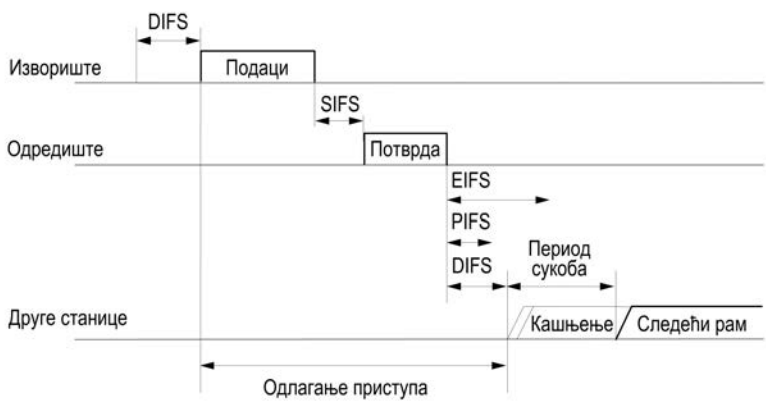
Пошто је трајање батерија значајно за бежичне системе стандард IEEE802.11 је понудио решење које води рачуна о томе. Базна станица може да обавести мобилну станицу да је у стању мировања [2] све док је она или корисник експлицитно не активирају. Ово има за последицу да базна станица преузима на себе смештање свих података који се упућују ка станици која је у стању мировања. Станица у мировању податке може да покупи касније.

Временски интервали између рамова

Стандард IEEE802.11 је предвидео коегзистенцију оба начина рада: централизованог PCF и дистрибуираног DCF у једној ћелији. Један од механизама су дефинисана времена између рамова. Пошто се један рам пошаље чека се одређени временски интервал пре него што било која станица може да пошаље следећи рам.

Дефинисана су четири временска интервала (слика 13.11):

1. Најкраћи интервал између рамова (SIFS [3]) користи се код станица које су већ у међусобној вези. То значи да ће по истеку SIFS времена: бити послат рам CTS као одговор на пријем рама RTS, или рам ACK као одговор на фрагмент или цео рам података. Постоји само једна станица која би требало да шаље по истеку времена SIFS.
2. Уколико станица не искористи канал у том временском интервалу (SIFS) базна станица може да пошаље свој посебан рам или упит (PIFS [4]). Овај меха-



Слика 13.11 Временски интервали између рамова код IEEE802.11

[1] *Beacon* - фар
[2] *Sleep state* - стање успаваности
[3] *Short Interframe Spacing*
[4] *Point Coordination Function Inter Frame Spacing* - PCF размак између рамова

низам дозвољава да станица која шаље податке или секвенцу фрагмената заврши започето слање.

3. Уколико базна станица нема шта да пошаље по истеку временског интервала DIFS[1] било која станица може да покуша да приступи каналу и пошаље нови рам. Примењује се уобичајен начин за приступање каналу и бинарни експоненцијални алгоритми за кашњења уколико дође до колизије.
4. Последњи временски интервал EIFS[2] користи станица која је управо добила рам са грешком или рам који није очекивала. Она шаље обавештење о грешци. Идеја да се додели најнижи приоритет овом обавештењу произлази из чињенице да треба дати времена предајнику који не зна да је дошло до грешке и да се на тај начин спречи интерференција.

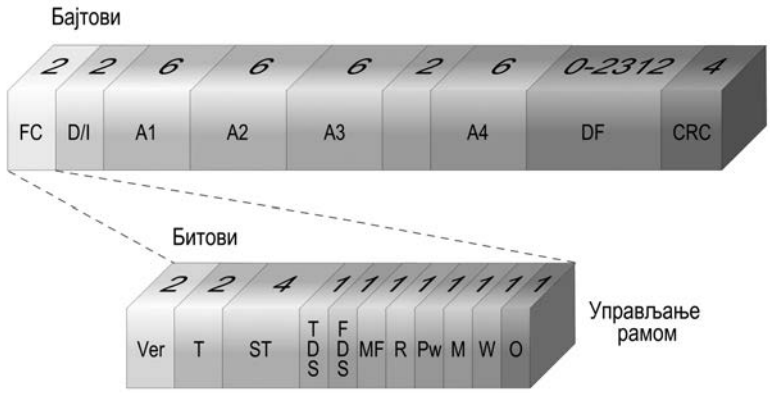
13.7 Структура рама стандарда IEEE 802.11

Стандард IEEE802.11 дефинише 3 различите класе рамова: податак, управљање и надзор. За сваки од ових рамова дефинисана су поља унутар MAC подслоја. Формат рама података приказан је на слици 13.12.

Прво поље за управљање рамом (FC[1]) садржи 11 потпоља:

- верзија протокола Ver[2] - дозвољава истовремени рад две верзије протокола у истој ћелији,
- тип (T[3]) - указује да ли је рам података, управљања или надзора,
- подтип (ST[4])- указује да ли је рам RTS или CTS,
- ка DS (TDS[5]) и од DS (FDS[6]) - указује да ли рам одлази ка или долази од дистрибуционог система,
- бит MF[7] - указује да постоји више фрагмената,
- бит поновни покушај R[8] - означава ретрансмисију рамова који су већ раније послати,
- бит управљање напајањем Pw[9] - користи базна станица за постављање мобилне станице у мирно или активно стање,
- бит M[10] - указује да пошиљалац планира да пошаље још рамова примаоцу,
- бит W - указује да је садржај рама шифрован користећи WEP[11] алгоритме,
- бит O[12] - указује примаоцу да рамови са постављеним битом на 1 треба да буду обрађени редоследом којим су и примљени.

[1] *Distributed Coordination Function Inter Frame Spacing* - DCF размак између рамова
[2] *Extended Inter Frame Spacing* - проширени размак између рамова
[1] *Frame control field*
[2] *Version*
[3] *Type field*
[4] *Subtype*
[5] *To DS*
[6] *From DS*
[7] *More fragment*
[8] *Retry*
[9] *Power management*
[10] *More*
[11] *Wired Equivalent Privacy*
[12] *Order*



Слика 13.12 Рам података IEEE802.11

Поље трајања (D/I [1]) указује на то колико ће дуго (изражено у микросекундама) рам и његова потврда заузимати канал. Ово поље постоји и у управљачким рамовима тако да на основу њега станице могу да поставе своје индикаторе NAV.

Заглавље рама садржи четири адресе (A_1 - A_4). Све адресе су стандардног IEEE802 формата. Две адресе су изворишна и одредишна адреса мобилних станица. Преостале две адресе су изворишна и одредишна адреса базних станица када се саобраћај одвија између ћелија.

Поље за секвенцне бројеве (SC [2]) користи се за обележавање фрагмената. Од 16 битова који су на располагању 12 битова се користи за обележавање рамова а 4 бита за обележавање делова рама (фрагмената).

Поље података (DF [3]) садржи корисне податке [4] од 0 до 2312 бајтова.

Поље контролног збира (CRC [5]) има уобичајену намену да открије грешке у преносу.

Рамови за надзор имају формат сличан формату рама података осим броја адреса. Пошто се рамови надзора размењују искључиво унутар једне ћелије адреса базне станице није потребна.

Управљачки рамови су краћи и имају само једну или две адресе. Не садрже поље за податке ни поље за секвенцне бројеве. Кључне информације у овим рамовима налазе се у потпољу подтип које указује да ли је рам захтев за успоставом везе (RTS), потврда о успостави везе (CTS) или потврда о успешном пријему рама података (ACK).

13.8 Услуге IEEE 802.11

Стандард IEEE802.11 дефинише девет услуга које треба да пружи бежична локална рачунарска мрежа да би обезбедила функционалност еквивалентну оној која постоји у кабловским локалним рачунарским мрежама. Табела 13.2 приказује списак услуга и два начина на које оне могу да се систематизују.

[1] *Duration/Connection ID*
[2] *Sequence Control*
[3] *Data Field*
[4] *Pay load*
[5] 32-битни циклични кôд (*Cyclic Redundancy Check*)

Услуга	Ко обезбеђује	За шта се користи
Приступање (*Association*)	Дистрибуциони систем	MSDU[1] испорука
Одступање (*Dissassociation*)	Дистрибуциони систем	MSDU испорука
Дистрибуција (*Distribution*)	Дистрибуциони систем	MSDU испорука
Поновно приступање (*Reassociation*)	Дистрибуциони систем	MSDU испорука
Интеграција (*Integration*)	Дистрибуциони систем	MSDU испорука
Пријава (*Authentication*)	Станица	Приступ и безбедност локалне рачунарске мреже
Одјава (*Deauthentication*)	Станица	Приступ и безбедност локалне рачунарске мреже
Приватност (*Privacy*)	Станица	Приступ и безбедност локалне рачунарске мреже
Испорука јединица података MAC подслоја (MSDU *dilevery*)	Станица	MSDU испорука

Табела 13.2 Услуге IEEE802.11

Као што се у табели види пет дистрибуционих услуга, које обезбеђује базна станица, односе се на мобилност станице када она улази и напушта ћелију и повезује се и раскида везу са базном станицом:

- Услугу приступања користи мобилна станица да би се повезала са базном станицом. Уобичајено се обавља одмах пошто станица уђе у радио-домет базне станице. По доласку она објављује свој идентитет;
- Услугу одступања користи или мобилна или базна станица. Мобилна станица користи ову услугу када престаје са радом (искључује се) или када напушта ћелију. Ову услугу може да користи и базна станица када због текућег одржавања престаје са радом;
- Да би променила базну станицу мобилна станица може да користи услугу поновног приступања. Ова услуга користи се и при преласку мобилне станице из једне у другу ћелију. Уколико се правилно примењује неће доћи до губитка података код преузимања (хендовера);
- Услуга дистрибуције одређује како треба преусмеравати рамове који су послати базној станици. Уколико је одредиште у истој ћелији (локално) онда се рамови директно емитују кроз ваздух. Уколико одредиште није у истој ћелији онда се рамови усмеравају преко кабловског дела рачунарске мреже;
- Услуга интеграције обезбеђује пренос података између станица које су повезане бежичном локалном рачунарском мрежом IEEE802.11 са станицом која је на кабловској мрежи[2]. Ова услуга води рачуна о превођењу адреса и других карактеристика које су везане за промену трансмисионог медијума.

[1] MAC *Service Data Unit*

[2] Станице које не користе стандард IEEE802.11 (non IEEE802.11).

Преостале услуге из табеле 13.2 су унутарћелијске:

- Услуга пријављивања је битна за бежичне рачунарске мреже да би се спречиле неауторизоване станице да шаљу податке. Пошто мобилна станица приступи ћелији базна станица јој шаље специјалан рам да би видела да ли мобилна станица зна шифру (сигурносни кључ) која јој је додељена. Станица шифрира специјалан рам и враћа га базној станици. Уколико је то добро урадила мобилна станица је потпуно прихваћена у ћелији;
- Услугу одјављивања користи мобилна станица (претходно пријављена) када жели да напусти мрежу. После одјављивања она не може да користи мрежу.

За информације које се размењују бежичном мрежом користи се RC4[1] алгоритам за шифровање.

13.9 Физички слој стандарда IEEE 802.11

Као што се може видети из табеле 13.2 велика пажња поклања се побољшању свих карактеристика система са бежичним преносом. У овом одељку биће дата кратка анализа физичких слојева оригиналног стандарда IEEE802.11 и каснијих, побољшаних верзија IEEE802.11a, IEEE802.11b и IEEE802.11.g.

Оригинални стандард IEEE 802.11

Предвиђена су три начина реализације физичког слоја стандарда IEEE802.11. Први користи пренос сигнала у инфрацрвеном опсегу спектра а друга два омогућавају радио-пренос података употребом техника проширеног спектра[2], у фреквенцијском опсегу од 2,4GHz до 2,4835GHz.

Први начин реализације стандарда IEEE802.11 користи дифузну инфрацрвену технологију преноса. Таласне дужине су од 850 до 950nm. Користи се импулсна позициона модулација (PPM[3]) са 4 и 16 нивоа. Подржава пренос на брзинама од 1Mb/s и 2Mb/s. Може се користити на растојањима до 20m.

Други начин реализације стандарда IEEE802.11 користи пренос података техником проширеног спектра, употребом директне, Баркерове, секвенце. Број канала зависи од фреквенцијског опсега који одређују национална регулаторска тела. Распон је од дванаест канала колико се користи у САД, девет у већини европских земаља до само једног у Јапану. Сваки канал је ширине 5MHz. Примењују се диференцијалне фазне модулације и то: DBPSK[4] за проток од 1Mb/s и DQPSK[5] за проток од 2Mb/s.

Трећи начин реализације стандарда IEEE802.11 користи пренос података техником проширеног спектра са фреквенцијским скакањем. Сигнал носиоца мења учестаност у зависности од псеудослучајне секвенце. Дефинисано је 78 секвенци за скакање. Растојање између учестаности два узастопна скока је 6MHz у САД и већини

[1] Аутор је Роналд Ривст са MIT (*Massachusetts Institute of Technology*).
[2] Одељак 7.11
[3] *Pulse Position Modulation* - позиција импулса носи информацију
[4] *Differential Binary Phase Shift Keying*
[5] *Differential Quaternary Phase Shift Keying*

европских земаља, а 5MHz у Јапану. Коришћени фреквенцијски опсег подељен је на 79 потканала ширине 1MHz чиме је брзина ограничена на 2Mb/s.

Стандард IEEE 802.11a

Први у низу стандарда већих брзина у бежичним системима је IEEE802.11a. Користи се ISM фреквенцијски опсег 5,8GHz и ортогонални фреквенцијски мултиплекс OFDM[1]. Не користи се техника проширивања спектра већ потканали са носиоцима на различитим међусобно ортогоналним учестаностима. Подаци се деле у више токова а сваки се преноси помоћу свог подносиоца, кроз свој потканал. Могуће брзине су: 6, 9, 12, 18, 24, 36, 48 и 54Mb/s. Користе се до 52 носиоца који су модулисани са BPSK, QPSK, 16QAM, 64QAM у зависности од брзине која се захтева.

Стандард IEEE 802.11b

Циљ је био понудити стандард IEEE802.11b који подржава брзине преноса података као и (тадашњи) IEEE802.3 стандард. Понуђене су брзине 5,5Mb/s и 11Mb/s и рад у ISM фреквенцијском опсегу од 2,4GHz до 2,4835GHz. Само повећање брзине преноса на 11Mb/s омогућено је употребом CCK[2] модулације, или такозване модулације са комплементарним кодовима. CCK се користе као кодна секвенца при процесу ширења спектра DSSS техником. Улазни подаци се посматрају као блокови од по 8[3] (односно 4 бита) брзине 1,375MHz. Шест од осам битова повезује се једном од 64 кодне секвенце и модулише са QPSK. Да ли ће проток бити 11Mb/s или 5,5Mb/s зависи од стања у каналу, а уређај се сам томе прилагођава.

Стандард IEEE 802.11g

Стандард IEEE802.11g је побољшана верзија 802.11b. Користи OFDM модулацију али ради у 2,4GHz фреквенцијском опсегу. Теоретски може да достигне брзине од 54Mb/s.

Стандард IEEE 802.11e

У стандарду IEEE802.11e унапређене су координационе функције MAC подслоја (дистрибуиране DCF и централизоване PCF) увођењем нове хибридне координационе функције (HCF[4]). У оквиру хибридне координационе функције дефинисана су два метода за приступ каналу (слична оригиналном IEEE802.11 MAC стандарду): побољшани дистрибуирани приступ (EDCA[5]) и контролисани приступ (HCCA[6]). Оба метода дефинишу класе саобраћаја, тако да се на пример е-пошти може доделити најнижи приоритет, а говору[7] највиши.

Код метода са побољшаним дистрибуираним приступом (EDCA) станица са већим приоритетом у просеку чека мало мање, пре него што пошаље свој рам, од ста-

[1] *Orthogonal Frequency Division Multiplexing.* Среће се и под називом дискретна вишетонска DMT *(Discrete Multitone)* и модулација са више носиоца MCM (*MultiCarrier Modulation*).
[2] *Complementary Code Keying*
[3] (8b/sym * 1,375MHz) = 11Mb/s
[4] *Hybrid Coordination Function*
[5] *Enhanced DCF Channel Access*
[6] *HCF Controlled Channel Access*
[7] VoWIP (*Voice over Wireless*). Говор захтева пренос у реалном времену, тј. мања и равномерна кашњења.

нице нижег приоритета (слика 13.8). Сваком од нивоа приоритета додељен је период времена (TXOP[1]) у коме станица или уређај за приступ могу да пошаљу одједном[2] више рамова. Уређаји за приступ са WMM[3] сертификатом морају да имају ову опцију (остале не морају).

Код начина рада са контролисаним приступом (HCCA) интервал између рамова - фарова, које PCF шаље станицама, подељен је у два дела. У првом делу користе се централизоване координационе функције. У другом делу може се користити побољшани дистрибуирани приступ (EDCA). У зависности од приоритета неким станицама може се доделити чешћи приступ медијуму. Станицама се у зависности од класе услуга додељује и различита дужина њиховог приступа.

Квалитет услуга (QoS) може се подешавати према захтевима корисника. На тај начин су обезбеђени услови за квалитетан пренос говора и видеа.

Стандард IEEE 802.11i

IEEE802.11i (познат и као WPA2[4]) је проширење IEEE802.11 стандарда који специфицира сигурност у W-iFi мрежама. Претходна спецификација (WEP) показала се недовољно сигурном. Спецификација WPA2 примењује AES[5] стандард за шифрирање. Поред тога могућа је и примена других метода заштите као што су провера приступа на основу портова[6], RADIUS или виртуелне приватне мреже.

Стандард IEEE 802.11n

У јануару 2004. године IEEE је формирао радну групу 802.11TG[7] чији је задатак да развије проширење IEEE802.11 стандарда за бежичне локалне рачунарске мреже. Очекује се да ће се достићи брзине веће од 600Mb/s. Предвиђа се коришћење OFDM и MIMO[8] преноса.

Технологија MIMO користи више антена (просторно распоређених) и мултипутно простирање сигнала. Користи QAM са 64 и 256 констелационих тачака. Потканали су ширине 40MHz у односу на садашњих 20MHz (у државама у којима регулаторска тела то дозвољавају).

Стандард IEEE 802.11p

Стандард IEEE802.11p означава се и као стандард за бежични приступ покретних возила WAVE[9]. Намена му је да обезбеди бежичну везу између возила у покрету и уређаја на путевима. Возила могу добити информације о условима на друму (метеоролошки преглед, саобраћај) или неку од напредних услуга нпр. интелигентно навођење возила. Домет је око 300m и ради у лиценцираном фреквенцијском опсегу од 5,96GHz, а брзине је 6Mb/s. Реализација је сложена пошто се возила брзо крећу.

---

1 *Transmit Opportunity*
2 Блок (*burst*)
3 *Wi-Fi Multimedia*
4 *Wi-FI Protected Access*
5 *Advanced Encription Standard*
6 802.1x
7 *Task Group*
8 *Multiple Input - Multiple Otput*
9 *Wireless Access for the Vehicular Environment*

Слика 13.13 Међусобно повезане мреже

Стандард IEEE 802.11s

Међусобно повезане мреже [1] постају све популарније у великим градовима пошто је могуће повезати локалне рачунарске мреже без постављања додатних каблова. Да би се испоручио саобраћај који је на другом крају мреже предлаже се рутирање и на MAC и на IP слоју.

13.10 Бежичне персоналне мреже

Под појмом персоналне мреже (PAN [2]) подразумева се повезивање рачунара, телефона и дигиталних персоналних уређаја (PDA [3]) које користи једна особа (лично). За повезивање ових уређаја могу се користити и радио или инфрацрвени таласи па је онда реч о бежичној персоналној мрежи (WPAN [4]). Велики број технологија и произвођача присутан је на тржишту бежичних персоналних мрежа. У овом поглављу биће детаљно анализиран стандард Bluetooth SIG.

13.11 Стандард Bluetooth

Bluetooth [5] је стандард за бежичне везе, који је 1994. године промовисао Ericsson. Првобитно је био намењен за бежично повезивање мобилних телефона и уређаја, као нпр. PDA, а тек касније за међусобно повезивање рачунара. Организација произвођача која развија и унапређује ову технологију позната је под називом Bluetooth SIG [6].

---

[1] *Mesh Network*

[2] *Personal Area Network*

[3] *Personal Digital Assistent*

[4] *Wireless Personal Area Network*

[5] Добила је име по викиншком краљу Харалду II Блатану (Blatann Harald), који је у X веку ујединио зарађена викиншка племена. Значење имена Блатан су плави зуби (енг. *bluetooth*).

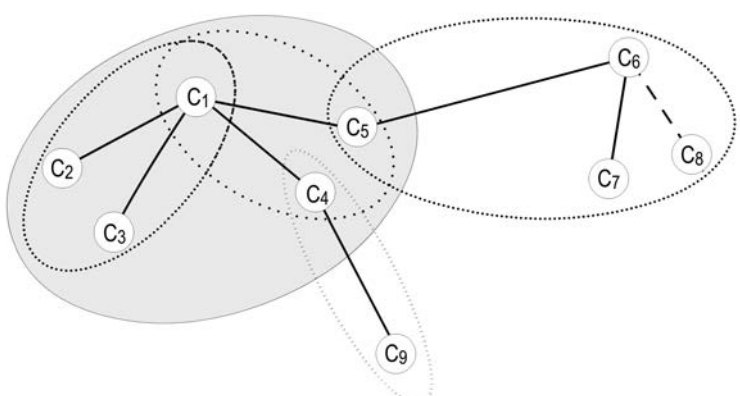
[6] *Special Interest Group* - Ericsson, IBM, Nokia, Toshiba и Intel. Од када је 1998. године ова група издала проглас о званичном почетку развоја ове технологије преко 2000 компанија је потписало споразум који им даје за право да развијају, производе и продају Bluetooth уређаје.

Архитектура Bluetooth мрежа

Основна јединица Bluetooth система је пиконет[1] мрежа. Пиконет мрежа састоји се од две или више станице (уређаја) које користе исти физички канал, што значи да су синхронизоване на заједнички такт сигнал и да користе исту секвенцу скакања. Заједнички такт пиконета је идентичан такт сигналу главне станице (уређаја)[2]. Све остале станице (уређаји) које се синхронизују са главном станицом су пратеће станице (уређаји)[3]. Само једна станица може да буде главна а све остале су пратеће. Комуникација се одвија само између главне и пратећих станица. Директна комуникација између пратећих станица није могућа у оквиру канала пиконета.

На једној локацији може да постоји више независних пиконет мрежа. Свака од тих пиконет мрежа ради на различитим физичким каналима (различита главна станица, независни такт пиконет мреже и секвенца скакања). Bluetooth станица може да буде главна само у једној пиконет мрежи. Разлог је следећи: пошто је пиконет мрежа дефинисана преко синхронизације са главним Bluetooth тактом није могуће бити главна станица у више од једне пиконет мреже. Bluetooth станица може да буде пратећа станица у више независних пиконет мрежа користећи временски мултиплекс.

Bluetooth станица која је члан више пиконет мрежа укључена је у разбацану мрежу[4]. Укључење у разбацану мрежу не значи да је омогућено и преусмеравање саобраћаја. Језгро Bluetooth протокола не нуди такву опцију већ се сматра да је то у надлежности протокола виших слојева и ван је Bluetooth спецификације. На слици 13.14 приказан је пример топологије. Станица C_1 је главна станица у пиконету (осенчена област и означена као пиконет мрежа C_1) са станицама C_2, C_3, C_4 и C_5 као пратећим станицама. Пиконет мрежа C_1 за рад користи два канала: један за везу са станицама C_2 и C_3 и други за везу са станицама C_4 и C_5. Приказане су и две друге пиконет мреже: једна са станицом C_6 као главном (означена као пиконет мрежа C_6) и ста-



Слика 13.14 Пример Bluetooth технологије

[1] *Piconet*
[2] *Master*
[3] *Slave*
[4] *Scatternet*

ницама C_5, C_7 и C_8 као пратећим и друга са станицом C_4 (означена као пиконет мрежа C_4) као главном и станицом C_9 као пратећом.

Поред активних станица (главне и пратеће) Bluetooth дефинише и неактивну станицу[1]. Када пратећа станица нема потребе да ради (учествује у пиконет каналу), а још увек је синхронизована са тим каналом, она улази у неактивно стање. Повремено, када јој главна станица пошаље одговарајући сигнал (фар[2]) неактивна станица се због синхронизације укључује. Неактивно стање омогућава уштеду напајања (батерије) и могућност да је у пиконет мрежи присутно више од седам пратећих станица.

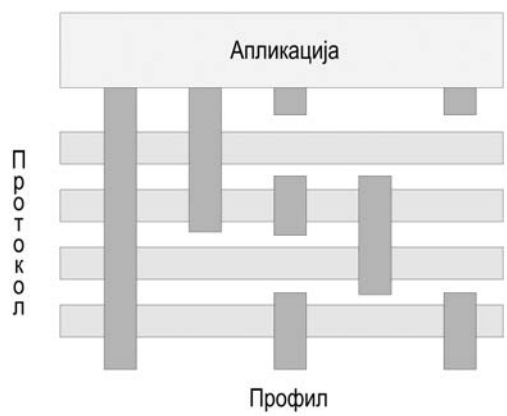
Начин функционисања пратеће станице веома је једноставан па су једноставни и ниске цене чипови који те функције реализују.

Примена Bluetooth мрежа

Да би станица користила Bluetooth мрежу мора бити у стању да интерпретира одређене дефинисане профиле. Профили представљају специфичне апликације од којих свака подржава различит скуп протокола[3] (слика 13.15). У табели 13.3 приказано је 13 профила[4].

Профил за генерички приступ (GAP) у ствари није апликација већ основа на којој су све апликације направљене и од које зависе. Њен основни задатак је да обезбеди процедуре за откривање Bluetooth станица, успостављање и одржавање сигурне везе (канал) између станица.

Поред GAP профила и профили SPP, SDAP и GOEP сматрају се генеричким. Изнад профила за генерички приступ (GAP) налазе се серијски профил (SPP), профил за генеричку размену објеката (GOEP) и профил за синхронизацију (SP). Многи често коришћени профили су: приступ фиксној локалној мрежи (LAP), профил за везу слушалице и базне станице (HSP) и профил за факс (Fax Profile) који су изнад серијског профила (SPP). Навешћемо један пример: ако треба синхронизовати[5] дигита-



Слика 13.15 Веза апликације протокола и профила код Bluetooth система

[1] *Parked*
[2] *Beacon*
[3] *Protocol stack*
[4] За сада (2006. год.) су дефинисана 33 профила.
[5] Користи се и термин *Bluetoth Enabled*.

Ознака профила	Опис
GAP (*Generic Access*)	Процедуре за надзор везе
SDAP (*Service Discovery Application Profile*)	Протокол за откривање понуђене услуге
CTP (*Cordeless Telephone Profile*)	Повезује слушалицу са локалном базном станицом
IP (*Intercom Profile*)	Дигитални воки-токи
SPP (*Serial Port Profile*)	Замена за кабл за серијски порт
HSP (*Headset Profile*)	Омогућава употребу телефона без држања апарата у руци
DUNP (*Dial Up Networking Profile*)	Омогућава да се преносиви рачунар повезује преко мобилног телефона
Fax Profile	Омогућава да се преносиви факс уређај повезује преко мобилног телефона
LAP (*LAN Access Profile*)	Протокол између мобилног рачунара и кабловске локалне рачунарске мреже
GOEP (*Generice Object Exchange Profile*)	Дефинише клијент-сервер релације између објеката у покрету
OPP (*Object Push Profile*)	Обезбеђује начин за размену једноставних објеката
FTP (*File Transfer Profile*)	Обезбеђује пренос датотека
SP (*Synchronization Profile*)	Дозвољава PDA уређају да се синхронизује са другим рачунаром

Табела 13.3 Неки од профила Bluetooth мрежа

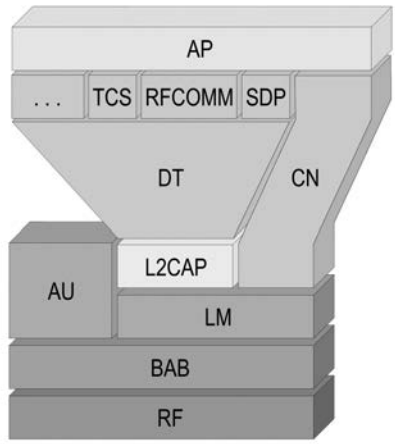
лни лични уређај (PDA) и рачунар да би преко серијског порта размењивали податке онда оба уређаја морају да подржавају профиле GAP, SPP, GOEP и SP. Остали профили нису потребни.

Скуп протокола[1] код Bluetooth система

Језгро Bluetooth система обухвата четири најнижа слоја и одговарајуће протоколе који су део Bluetooth спецификације, као и заједнички протокол за откривање услуга (SDP[2]) и свеобухватни генерички профил приступа (GAP[3]). Комплетна Bluetooth апликација захтева додатне услуге и протоколе виших слојева који су дефинисани али превазилазе обим овог уџбеника. Општи дијаграм Bluetooth система може се представити сликом 13.16. На слици су обележени слојеви са одговарајућим протоколима:

- нижи слојеви са одговарајућим протоколима: радио слој (RF[4]), слој основног опсега (BAB[5]), аудио слој (AU[6]), слој за надзор везе (LM[7]), слој за управљање и прилагођавање везе (L2CAP[8]),

[1] *Protocol stack*
[2] *Service Discovery Protocol*
[3] *Generic Access Profile*
[4] *Radio Frequency*
[5] *Baseband*
[6] *Audio*
[7] *Link Manager*
[8] *Logical Link Control and Adaptation Layer Protocol* (L2CAP)



Слика 13.16 Архитектура Bluetooth система

- виши слојеви: подаци (DT[1]), слој са различитим протоколима везаним за различите интерфејсе (TCS[2], RFCOMM[3], SDP[4]) и апликације (AP[5]), и
- управљање (CN[6]).

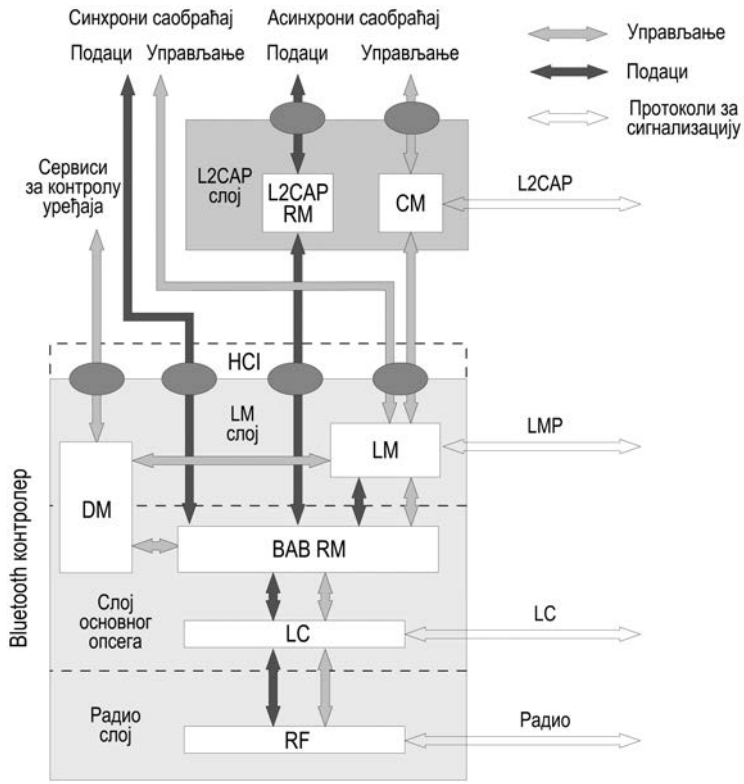
Детаљнија архитектура језгра Bluetooth система представљена је на слици 13.17. Најнижа три слоја груписана су у подсистем који се среће под називом Bluetooth контролер. Остатак система укључујући услугу L2CAP[7] и више слојеве означава се као Bluetooth хост.

Станице комуницирају користећи протоколе дефинисане Bluetooth спецификацијом. Језгро протокола чини: језгро система које нуди услуге преко бројних тачака приступа (SAP[8]). Услуге могу бити разврстане у две групе: управљачке, које се означавају као C[9] раван, и корисничке које се означавају као U[10] раван. Прва група води рачуна о успостављању и раскидању канала и веза, а друга о подацима који се том везом размењују.

Интерфејс услуга ка подсистему контролера дефинисан је на такав начин да се Bluetooth контролер може сматрати стандардним делом. У оваквој конфигурацији контролер ради на најнижа три слоја, а L2CAP слој садржи остатак апликације хост система. Стандардни интерфејс назива се интерфејс станица - контролер (HCI[11]). Његове приступне тачке означене су на горњој ивици контролера подсистема. Имплементација ових стандардних интерфејса ка услугама је опциона.

---

1 *Data*
2 *Telephony Control Protocol Spec* - бит оријентисани протокол који дефинише сигнализацију при успостави/раскидању позива између станица.
3 *Serial cable emulation protocol* - протокол за емулацију серијског кабла
4 *Service Discovery Protocol* - протокол за откривање услуге
5 *Aplication*
6 *Control*
7 *Logical Link Control and Adaptation Layer Protocol*
8 *Service Access Point*
9 *Control*
10 *User*
11 *Host to Controller Interface*



Слика 13.17 Архитектура језгра Bluetooth система

Слој основног опсега (BAB[1]) на неки начин је сличан MAC подслоју али садржи и елементе физичког слоја. Води рачуна о томе како главна станица управља временским целинама и како су оне груписане у рамове.

Слој L2CAP може опционо да обезбеди додатну детекцију грешке и поновљено слање јединица протокола (L2CAP PDU[2]). Ова опција препоручује се апликацијама које у корисничким подацима захтевају малу вероватноћу неоткривених грешака. Следећа опција слоја L2CAP је контрола тока применом механизма клизајућег прозора[3].

У тексту који следи биће укратко објашњена функција сваког од модула са слике:

- модул за надзор канала (CM[4]) задужен је за успостављање, управљање и раскидање L2CAP канала укључујући управљање напајањем, проверу идентитета и квалитет услуге. Протокол између парњак целина је L2CAP;
- модул за управљање ресурсима (L2CAP_RM[5]) води рачуна о редоследу пријема сегмената. Такође води рачуна и о томе да ли апликације примају податке у складу са договореним квалитетом услуга QoS;

[1] *Baseband Layer*
[2] *Protocol Data Unit* (3. поглавље)
[3] Детаљније у 7. поглављу.
[4] *Channel Manager*
[5] *L2CAP Resource Manager*

- модул за надзор станице (DM[1]) управља општим радом Bluetooth станице. Задужен је за све операције које нису директно везане за пренос података као што су испитивање присуства суседних станица, повезивање са тим станицама итд.;
- модул за надзор везе (LM[2]) задужен је за успостављање, модификовање, раскидање логичке везе и иновирање параметара везаних за физичку везу између уређаја. За комуникацију са модулом за управљање везом и удаљеном станицом користи се протокол за управљање везом (LMP[3]);
- модул за управљање везом (LC[4]) задужен је за кодирање и декодирање Bluetooth корисних података као и параметара везаних за физички канал,
- модул за управљање ресурсима основног опсега (BAB_RM[5]) одговоран је за приступ медијуму;
- радио модул (RF) задужен је за предају и пријем рамова на физичком каналу.

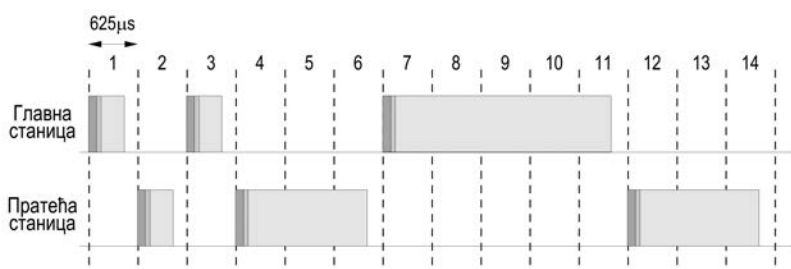
Радио-слој Bluetooth система

Радио-слој преноси битове од главне станице до пратеће и обрнуто. Систем ради у 2,4GHz фреквенцијског опсегу (ISM) као и IEEE802.11 системи тако да се међусобно преклапају. Фреквенцијски опсег је подељен на 79 канала ширине 1MHz а модулација је GFSK[6]. Користи се фреквенцијско скакање са 1600 скокова у секунди. Време између два скока је 625μs.

Домет Bluetooth везе је 1m са предајником снаге 0dBm, 10m са предајником снаге 4dBm и 100m са предајником снаге 20dBm. Могу се достићи брзине од 723,1kb/s код верзија 1.1 и 1.2 и 2,1Mb/s код верзије 2.0. Bluetooth SIG је објавила (март 2006. год) да је одабрала вишеканални OFDM (MB-OFDM[7]) верзију UWB система WiMedia Alliance за интеграцију са садашњом верзијом Bluetooth технологије.

Слој основног опсега Bluetooth система

Овај слој претвара ток битова у рамове и дефинише формате од значаја. У најједноставнијем облику главна станица у свакој пиконет мрежи дефинише серију временских целина величине 625μs. Главна станица шаље у непарним временским целина-



Слика 13.18 Размена пакета између главне и пратеће станице

[1] *Device Manager*
[2] *Link Manager*
[3] *Link Management Protocol*
[4] *Link Controller*
[5] *Baseband Resource Manager*
[6] *Gaussian Frequency Shift Keying*
[7] *Multi-Band Orthogonal Frequency Division Multiplexing*

ма, а пратећа станица у парним. Ово је традиционалан временски мултиплекс у коме је главној станици додељена половина временских целина а пратеће станице деле другу половину. Рамови могу бити дугачки 1, 3 и 5 временских целина (слика 13.18).

Сваки од рамова шаље се преко логичког канала - везе [1]. Постоје две врсте везе:

- асинхрона без успоставе везе (ACL [2]), и
- синхрона са успоставом везе (SCO [3]).

Код ACL врсте користи се пакетска комутација и примењује се на податке који пристижу у неравномерним временским интервалима. Подаци пристижу са L2CAP слоја на предајној страни и предају се L2CAP слоју на пријемној страни. Саобраћај се испоручује на најбољи могући [4] начин али не постоји гаранција да су подаци успешно стигли на одредиште. Пратећа станица може са главном станицом да успостави само једну ACL везу.

Друга врста - SCO везе користи се за апликације у реалном времену, као што су телефонске везе. За овакав тип канала додељују се тачно одређене временске целине у оба правца. Због природе апликација у реалном времену - критична су временска кашњења - не користе се поновна слања већ корекција грешака унапред (FEC [5]). Пратећа станица може да има до три SCO везе са главном станицом. Свака SCO веза може да пошаље 64000b/s кодирани PCM аудио сигнал.

Слој L2CAP

Слој L2CAP има три важне функције:

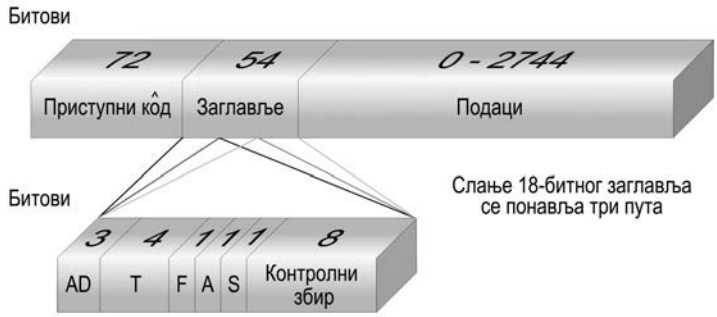
- прво, прима пакете до величине од 64kB од виших слојева и дели их на рамове погодне за пренос. На одредишту рамови се поново повезују у пакете;
- друго, води рачуна о мултиплексирању и демултиплексирању пакета из различитих извора. Када се пакети поново повезују L2CAP указује коме од виших слојева су упућени;
- треће, L2CAP руководи захтевима за квалитет услуге и у фази успоставе везе и за време нормалног тока података. Такође води рачуна и о усаглашавању величине пакета између станица. Ово је важно пошто нису све станице у могућности да раде са пакетима величине 64kB.

Структура рама у Bluetooth системима

Постоји неколико формата рамова. Један од њих приказан је на слици 13.19 и чине га:

- приступни кôд који идентификује главну станицу тако да пратеће станице које се налазе у радио-опсегу две главне станице могу да одреде који од саобраћаја је за њих,
- заглавље дужине 54 бита које садржи поља типична за MAC подслој,
- поље корисничких података величине до 2744 бита. Ова величина одговара трајању од пет временских целина.

[1] Линк
[2] *Asynchronous ConnectionLess*
[3] *Synchronous Connection Oriented*
[4] *Best effort* - термин који се користи код система без успоставе везе као што су Интернет слој, Етернет и сл.
[5] *Forward Error Correction*



Слика 13.19 Карактеристичан рам података у Bluetooth системима

Заглавља сачињавају следећа поља:

- поље адресе A (дужине 3 бита) - указује којој од осам активних станица је рам упућен;
- поље типа T (дужине 4 бита) - указује на врсту рама (ACL, SCO...), врсту корекције грешке која се користи и на то колико временских целина је рам дугачак;
- поље тока F [1] (дужине 1 бит) - поставља пратећа станица када је њен меморијски простор попуњен и не може да прими више података;
- поље потврде A (дужине 1 бит) - користи се да се пошаље потврда преко рама података [2];
- поље секвенце S [3] (дужине 1 бит) - користи се за обележавање рамова. Пошто се користи протокол заустави се и чекај [4] довољан је један бит;
- поље контролног збира [5] (дужине 8 битова) - користи се за детекцију грешке.

Дужина заглавља од 54 бита постиже се троструким слањем 18-битне целине која се састоји од претходно описаних поља. Вишеструким слањем повећава се поузданост преноса у радио-медијуму.

Код ACL веза за поље података користе се различити формати. Формати рамова у SCO везама су једноставнији: поље података је увек дужине 240 битова. Постоје три верзије: 80, 160 и 240 стварне дужине података. Остатак се користи за корекцију грешке. У најпоузданијој верзији (80 битова података) садржај се три пута шаље.

Пратећа станица може да користи само непарне временске целине, тј. 800 временских целина у секунди. Са 80-битним подацима капацитет канала пратеће и главне станице је по 64000b/s што одговара капацитету PCM говорног канала. То и јесте био разлог да се одабере брзина скакања од 1600. Уколико се користи мање поуздана варијанта (без редундансе) могуће је реализовати истовремено три говорне везе што и представља максимум за SCO пратеће станице.

[1] *Flow control*
[2] *Piggy back*
[3] *Sequence*
[4] *Stop and wait* - 11. поглавље.
[5] CRC

13.12 Стандарди за персоналне мреже IEEE организације

Организација IEEE формирала је радне групе које се баве бежичним персоналним мрежама. Прва радна група радила је на прилагођавању стандарда Bluetooth SIG и издала 2002. године стандард IEEE802.15.1 који се односи само на физички слој и слој везе (слика 13.16). Као што смо видели у претходним поглављима Bluetooth [1] спецификација обухвата цео систем, од физичког слоја до апликационог (слика 13.20). Без обзира што ове верзије нису идентичне оне конвергирају ка истом стандарду. Стандард IEEE802.15 односи се на бежичну комуникацију уређаја малих димензија на релативно кратким растојањима као што су PDA, преносиви рачунари, мобилни телефони, MP3 уређаји...

Рад друге групе (IEEE802.15.2) односи се на могућност истовременог рада бежичних персоналних мрежа по стандардима серије IEEE802.15 и бежичних локалних рачунарских мрежа по стандардима серије IEEE802.11.

Генерално, пошто и бежичне персоналне мреже и бежичне локалне рачунарске мреже користе ISM фреквенцијски опсег 2,4GHz може да дође до интерфернције у раду уређаја ових мржа. Да би се разрешио овај проблем радна група је предложила механизам за истовремени рад [2].

Трећа радна група ради на стандарду IEEE802.15.3 за рад персоналних уређаја на релативно великим брзинама (већим од 20Мб/с) као и дефиницију нових карактеристика као што су мала потрошња и квалитет услуга који одговара мултимедијалним апликацијама.

Постоји више радних група: IEEE802.15.3a се бави преносом у изузетно широком опсегу спектра UWB[3] (опсег од 3,1GHz до 10,6GHz, ширине 500MHz, брзине до 480Mb/s), IEEE802.15.3b се бави међусобним радом и IEEE802.15.3c се бави физичком спецификацијом преноса са милиметарским таласима (опсег од 57GHz до 64GHz, брзине преко 2Gb/s).

Слика 13.20 Стандард IEEE802.15.1

[1] По верзији 1.1.
[2] *Coexistence Mechanism*
[3] *Multi-Band OFDM (MB-OFDM)* подржава *WiMedia Alliance, Direct Sequence - Ultra Wide Band* подржава *UWB Forum*

Четврта радна група издала је стандард IEEE802.15.4-2006 за релативно мале брзине (испод 250kb/s). Минимизирањем потрошње батерије у овим уређајима могу дуго да трају. Овај стандард развијен је за мреже са сензорима, за даљинско управљање и аутоматизацију у домаћинствима итд. ZigBee Alliance има исту улогу у односу на стандард IEEE802.15.4 као Wi-Fi Alliance у односу на стандард IEEE802.11.

13.13 Стандарди за широкопојасне мреже

Радна група за стандардизацију широкопојасних мрежа у оквиру IEEE организације издала је 2002. године стандард[1] који носи ознаку IEEE802.16 и предвиђа рад у широкопојасном фреквенцијском опсегу. Области које покривају спадају у категорију мрежа градског подручја (MAN). Сматра се да су алтернатива xDSL системима у делу претплатничке петље[2]. Радна група је проширила стандард и упоредна анализа је дата у табели 13.4. Стандард је рађен по угледу на OSI модел (слојеви, примитиве, терминологија) и веома је сложен.

Скуп протокола стандарда IEEE 802.16

Скуп протокола IEEE802.16 представљен је на слици 13.21 и види се да је сличан општем моделу IEEE802 архитектуре протокола са мало више подслојева.

Најнижи подслој се односи на сам пренос. Ускопојасни радио-систем користи модулационе шеме QPSK, 16QAM и 64QAM. Изнад трансмисионог подслоја налази се подслој[3] чији је задатак да заштити слој везе од различитости технологија преноса.

	IEEE802.16	IEE802.16d	IEEE802.16e
Завршена	2001. год.	2004. год.	2005. год.
Фреквенцијски опсег	10-66GHz	2-11GHz	2-6GHz
Намена	*Backhoul*	Бежични DSL и *Backhoul*	Мобилни Интернет
Услови	Линија видљивост LOS[4]	Није потребна линија видљивости NLOS[5]	Није потребна линија видљивости NLOS
Брзина	32-150Mb/s у каналу ширине 28MHz	До 75Mb/s у каналу ширине 20MHz	До 15Mb/s у каналу ширине 5MHz
Модулација	QPSK, 16QAM, 64QAM	OFDM 256, QPSK, 16QAM, 64QAM	SOFDM[6], 16QAM, 64QAM
Ширина канала	20, 25 и 28MHz	Бира се ширина канала између 1,5 и 20MHz	Исто као и IEE802.16d
Типичан домет	2 до 5km	7 до 10km максималан 50km	1 до 5km

Табела 13.4 Упоредни преглед стандарда IEE802.16, IEE802.16d и IEE802.16e

[1] WiMAX Forum је идустријска асоцијација од 320 компанија међу којима су и Intel, Samsung, Cisco, Nokia и Motorola. WiMAX Alliance промовише и потврђује међусобни рад производа за широкопојасне бежичне системе који користе IEEE802.16 и ETSI *HiperMAN* спецификације.

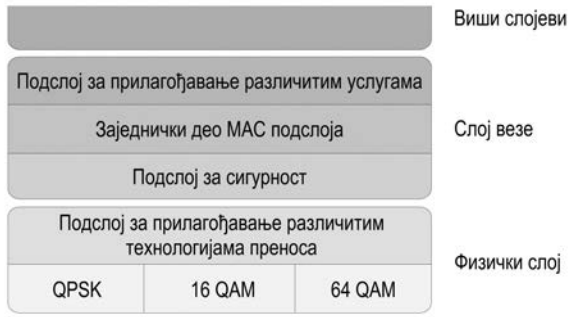
[2] Последњи километар (*Last mile*)

[3] *Transmission Convergence Sublayer*

[4] *Line Of Site*

[5] *Non Line Of Site*

[6] *Scalable OFDM*



Слика 13.21 Скуп протокола стандарда IEEE802.16

Слој везе чине три подслоја. Најнижи се бави сигурношћу [1] која је веома значајна за системе ван затворених објеката. Овај подслој води рачуна о шифровању, дешифровању и заштитним кључевима.

Средњи подслој се означава као заједнички MAC део [2]. У овом делу налази се главни протокол за надзор канала. Модел је конципиран тако да главна станица управља целим системом. Она може да одреди када се шаљу подаци од главне станице ка кориснику и од корисника ка главној станици. Неуобичајено у односу на остале MAC подслојеве је да подржава рад са успоставом везе да би се обезбедила квалитетна услуга за телефонски саобраћај и мултимедијални саобраћај.

Подслој који зависи од услуга [3] има исту функцију као и LLC подслој код осталих IEEE802 архитектура: његова функција је да заштити мрежни слој од различитих имплементација нижих слојева. IEEE802.16 је пројектован тако да подржава рад и протокола без успоставе везе (IP, Етернет, PPP [4]) и са успоставом везе ATM [5].

Физички слој стандарда IEEE 802.16

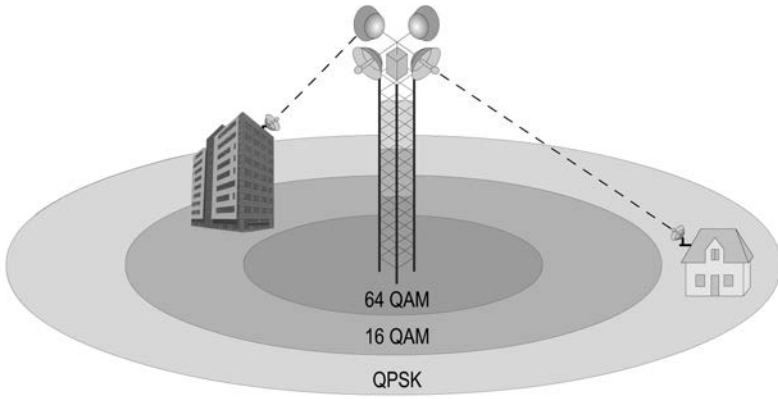
Као што и сам назив указује широкопојасне бежичне мреже захтевају широк фреквенцијски опсег за свој рад. Одабран је фреквенцијски опсег од 10GHz до 66GHz. Ови таласи се простиру праволинијски па главна станица може да има више антена од којих је свака усмерена у одређеном правцу који покрива једну групу корисника.

Због мале таласне дужине снага сигнала значајно опада са удаљеношћу а самим тим и однос сигнала и шума. Имајући то у виду IEEE802.16 стандард је предвидео, у зависности од растојања, три различите кодне шеме и три различите брзине (слика 13.22) и то:

- за најближе кориснике кодну шему 64QAM и брзину од 150Mb/s,
- за средње удаљене кориснике кодну шему 16QAM и брзину до 100Mb/s и
- за најудаљеније кодну шему QPSK и брзину до 50Mb/s.

Да би се постојећи спектар искористио што ефикасније предвиђена су два метода: фреквенцијско дуплирање (FDD [6]) и временско дуплирање (TDD [7]). Код TDD систе-

[1] *Security sublayer*
[2] *MAC sublayer common part*
[3] *Service specific convergence sublayer*
[4] *Point To Point* - тачка тачка протокол.
[5] Мрежа са комутацијом ћелија (*Asynchronous Transfer Mode*).
[6] *Frequency Divisin Multiplexing*
[7] *Time Division Duplexing*



Слика 13.22 Преносни системи стандарда IEEE802.16

ма рамови се шаљу у временским целинама. Прва група временских целина резервисана је за директни саобраћај, тј. од базне станице до корисника. Намена друге групе временских целина је да омогуће пребацивање са једног правца на други. Трећа група временских целина је за одлазни правац. Број временских целина који се додељују сваком од праваца може се динамички мењати у зависности од потреба.

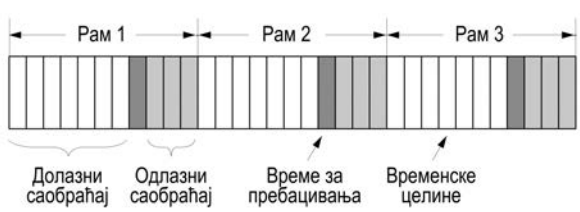
Протоколи на слоју везе IEEE 802.16

Као што је на слици 13.21 приказано слој везе је подељен у три подслоја. Први подслој - за сигурност обезбеђу шифрирање података користећи алгоритме 3DES, AES и SHA-1 а за аутентификацију корисника са базном станицом користи се RSA шифрирање са јавним кључем.

Други слој је заједнички MAC подслој. Као што се види на слици 13.23 сваки рам заузима одређени број временских целина на физичком слоју. Сваки рам се састоји од подрамова. Прва два подрама садрже информације о томе која од временских целина је слободна, параметре система (када се нови корисник укључује у мрежу)...

Долазни канал је једноставан. Базна станица одлучује о томе шта и у који подрам поставља. Одлазни канал је много сложенији и због различитих потреба различитих корисника. Дефинисане су четири класе:

- услуга са константном битском брзином,
- услуге битским брзинама које задовољавају системе у реалном времену,



Слика 13.23 Додељивање временских целина рамовима код система са временским дуплирањем

- услуге битским брзинама за системе који не раде у реалном времену и
- најбоља могућа услуга[1].

Услуге са константном битском брзином предвиђене су за некомпримован говор као што је онај који се преноси преко E1/T1 система. За овакве системе потребно је послати унапред одређену количину података у унапред дефинисаним интервалима времена.

Услуге брзинама које задовољавају системе у реалном времену односе се на компримоване мултимедијалне апликације и апликације у реалном времену. Базна станица шаље упит кориснику у тачно одређеним интервалима да би сазнала колики фреквенцијски опсег му је потребан.

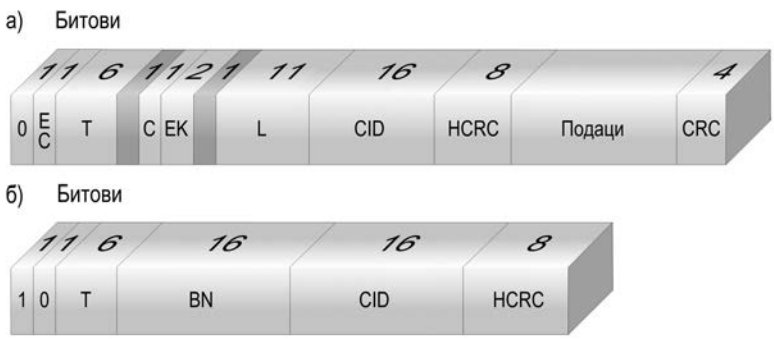
Услуге за системе који не раде у реалном времену односе се на пренос велике количине података. Базна станица шаље упит кориснику, али није неопходно да то буде у тачно одређеним интервалима времена.

Најбоља могућа услуга се односи на све друге ситуације осим ових које су описане. Станице надмећући се у слободним временским целинама за приступ могу да дођу у колизију. Да би се колизија минимизирала користи се кашњење по бинарно експоненцијалном алгоритму.

Структура рама IEEE 802.16

Постоје две врсте рамова на MAC подслоју IEEE802.16: генерички и захтев за фреквенцијским опсегом. Генерички рам састоји се од заглавља, корисничких података и контролног збира (слика 13.24а). Заглавље чине следећа поља:

- прво поље има вредност 0 што указује да је то генерички рам,
- поље о шифрирању EC[2] (дужине 1 бит) - указује да ли су (или нису) подаци шифрирани
- поље тип T (дужине 6 битова) - одређује врсту рама,
- поље C[3] (дужине 1 бит) - указује да ли постоји поље контролног збира,
- поље EK[4] (дужине 2 бита) - указује који кључ за шифрирање се користи (ако се користи било који),



Слика 13.24 Структура IEEE802.16 рамова: а) генерички б) захтев за опсегом

[1] *Best effort*
[2] *Encrypted* - шифриран
[3] *Checksum* - цикични кôд (CRC), али је опционо пошто се не врши поновно слање.
[4] *Encryption Key* - кључ за шифрирање

- поље о дужини рама L (дужине 11 битова) - указује на укупну дужину рама укључујући заглавље,
- поље CI[1] (дужине 16 битова) - указује којој вези рам припада,
- поље HCRC[2] (дужине 8 битова) - контролни збир заглавља користећи полином: $x^8 + x^2 + x + 1$,
- поље D - поље података,
- поље CRC[3] (поље дужине 4 бита) - поље за контролни збир целог рама.

Рам којим се захтева фреквенцијски опсег не садржи корисничке податке. Његово заглавље (слика 13.24б) састоји се од следећих поља:

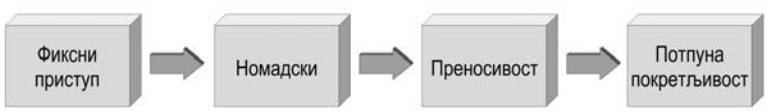
- прво поље има вредност 1 што указује да је реч о захтеву за фреквенцијским опсегом,
- поље тип T (дужине 6 битова) - одређује врсту рама,
- поље BN[4] (дужине 16 битова) - колики фреквенцијски опсег је потребан за пренос одговарајућег броја бајтова,
- поље CI[5] (дужине 16 битова) - указује којој вези рам припада,
- поље HCRC[6] (дужине 8 битова) - контролни збир заглавља.

Правци развоја IEEE 802.16x

Правци даљег развоја IEEE802.16x, односно коришћења WiMax система, могу се представити блок дијаграмом на слици 13.25.

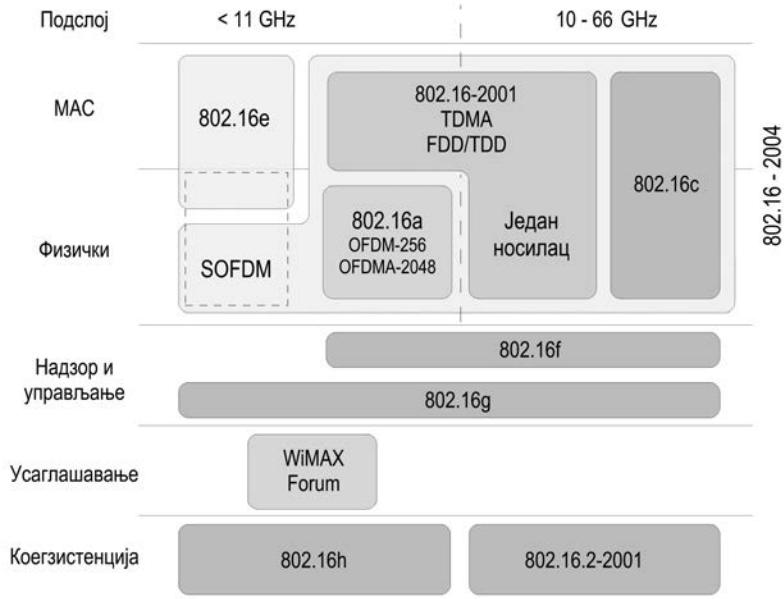
Карактеристике система представљених на слици 13.25 су следеће:

- фиксног приступа:
  - могућност приступа у оквиру објеката и између објеката,
  - услуге које се пружају одговарају услугама DSL система,
  - базна станица може да обезбеди равномерно оптерећење али не и хендовер[7],
  - ауторизација је могућа само на нивоу уређаја,
  - могућ је пренос говора IP протоколом (VoIP[8]);
- номадског[9] приступа:
  - услуге сличне услугама DSL система са различитих тачака прикључивања,



Слика 13.25 Развој IEEE802.16x

[1] *Connection identifier* - ознака везе
[2] *Header CRC* - циклични кôд заглавља
[3] *Cyclic Redundancy Check*
[4] *Bytes needed* - потребно број бајтова
[5] *Connection identifier* - ознака везе
[6] *Header CRC* - циклични кôд заглавља
[7] *Handover* - преузимање. Термин који се користи у мобилним, вишећелијским системима.
[8] *Voice over Internet Protocol*
[9] *Nomadicity*



Слика 13.26 Протоколи IEEE802.16x

- базна станица не обезбеђује хендовер,
- могућа је ауторизација корисника.

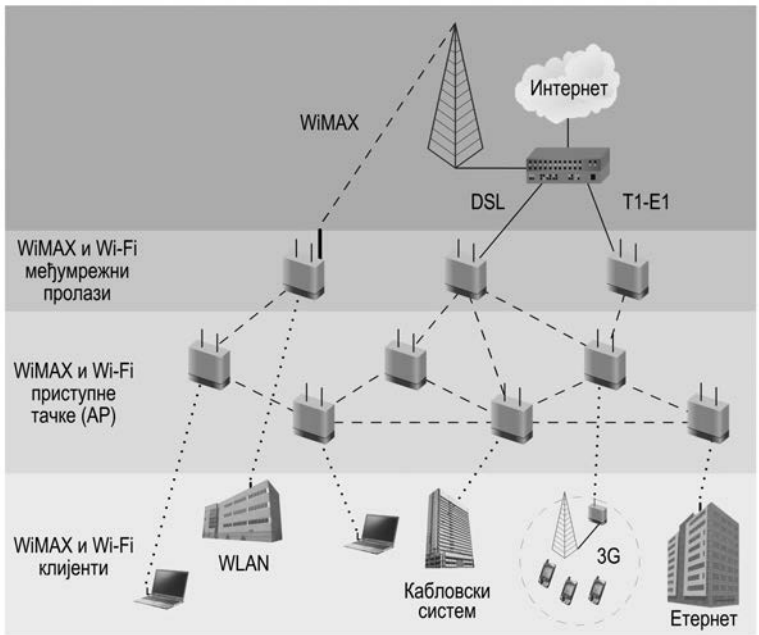
- приступа који омогућава преносивост су [1]:
  - могућа је аутентификација корисника,
  - стационарна или ограничена покретљивост,
  - мора се раскинути веза пре него што се пређе у другу ћелију,
  - квалитет услуге се умањује за време преласка из једне ћелије у другу,
  - могућ је пренос говора IP протоколом (VoIP).
- приступа потпуне покретљивости [2] су следеће:
  - извршено је прилагођење система да се пре прекида везе са једном базном станицом сачувају подаци и да се не умањи кавалитет услуге (QoS),
  - могућ је међусобни рад са сличним системима,
  - прилагођен је раду са малом потрошњом,
  - могућ је пренос говора IP протоколом (VoIP).

На слици 13.26 приказани су протоколи из серије IEEE802.16x.

13.14 Међусобно упоређивање бежичних система

Као што смо видели, постојећи стандарди и они чије је усвајање у току односе се на различите фреквенцијске опсеге и покривају различита растојања, што је систематизовано у табели 13.4. У табели је назначен још један параметар, а то је покретљивост [3] о којој

[1] *Portability*
[2] *Full Mobility*
[3] *Mobility*



Слика 13.27 Међусобно повезани системи: WiMAX, WiFi, 3G и кабловски

се све више води рачуна. Мобилни системи друге (2G) и треће генерације (3G) превазилазе оквире овог уџбеника али су битни за међусобно упоређивање система па су зато приказани у табели 13.4.

Мрежа	Стандард	Брзина	Фреквенцијски опсег	Покретљивост
WLAN	IEEE802.11b	1; 2; 5,5; 11Mb/s	ISM 2,4GHz	Мала
	IEEE802.11a	До 54Mb/s	ISM/UNI 5GHz	Мала
	IEEE802.11g	До 54Mb/s	ISM 2,4GHz	Мала
Bluetooth	IEEE802.15.1	1Mb/s	ISM 2,4GHz	Мала
WMAN	IEEE802.16	134Mb/s	10-66GHz	-
	IEEE802.16d	75Mb/s	2-11GHz	Мала
	IEEE802.16e	15Mb/s		Велика
2G	GSM[1]	9,6 / 57,6 kb/s	900/1800/ 1900MHz	Велика
	GPRS[2]	115kb/s		Велика
	EDGE[3]	384kb/s		Велика

[1] *Global System For Mobile Communications* - користи се у већини земаља осим САД.
[2] *General Packet Radio Service* - пакетска мрежа на врху GSM-а.
[3] *Enhanced Data Rates for GSM Evolution* - назива се и 2,5G.

Мрежа	Стандард	Брзина	Фреквенцијски опсег	Покретљивост
3G	UMTS [1] / WCDMA [2]	До 2Mb/s	1900-2025MHz	Велика
UWB	IEEE802.15.3a или неки де факто	До 400Mb/s	3,1-10,6GHz [3]	-
Сензори	IEEE802.15.4	5 - 200kb/s	433; 866; 916MHz 2,4 GHz (ISM)	Велика
Нова генерација WLAN		До GHz (у просторији) и 150 - 250MHz (напољу)	-	Велика

Табела 13.4 Бежичне технологије, постојеће и оне које долазе

Бежични системи се међусобно укрштају и повезују са постојећим кабловским системима (слика 13.27).

Стандард	Опис
IEEE802.11	Оригинални стандард опсег 2,4GHz, брзина 1Mb/s и 2Mb/s (1999)
IEEE802.11a	Брзина 54Mb/s, опсег 5,8GHz стандард (2001)
IEEE802.11b	Опсег 2,4GHz, брзина 5,5 и 11 Mb/s (1999)
IEEE802.11c	Премошћавање, укључен је у стандард IEEE802.1D (2001)
IEEE802.11d	Интернационални: роминг држава - дражава (2001)
IEEE802.11e	Побољшање квалитета услуга QoS [4] (2005)
IEEE802.11F	Протокол између приступних тачака различитих произвођача (2003) -повучен (2006)
IEEE802.11g	Опсег 2,4GHz, брзина 54 Mb/s (2003)
IEEE802.11h	Прилагођавање IEEE802.11a за европски стандард радио-канала (2004)
IEEE802.11i	Побољшање сигурности (2004)
IEEE802.11j	Проширење за Јапан (2004)
IEEE802.11k	Побољшања у мерењу радио-ресурса
IEEE802.11l	Резервисан и неће се користити
IEEE802.11m	Одржавање стандарда
IEEE802.11n	Побољшања протока
IEEE802.11o	Резервисан и неће се користити
IEEE802.11p	Приступ возила у покрету WAVE - (*Wireless Access for the Vehicular Environment)*
IEEE802.11q	Резервисан и неће се користити
IEEE802.11r	Брзи роминг (*Fast roaming*)

[1] *Universal Mobile Telecommunication System* - ETSI стандард за 3G у Европи
[2] *Wideband Code Division Multiple Access* - широкопојасни приступ са кодним мултиплексирањем (један од UMTS стандарда).
[3] FCC
[4] *Quality of Service*

Стандард	Опис
IEEE802.11s	Међусобно повезане мреже
IEEE802.11T	Бежичне перформансе и предвиђања
IEEE802.11u	Рад са не 802 мрежама
IEEE802.11v	Надзор бежичних мрежа
IEEE802.11w	Заштићени рамови за надзор
IEEE802.11x	Резервисан и неће се користити
IEEE802.11y	*3650-3700* рад у САД-у

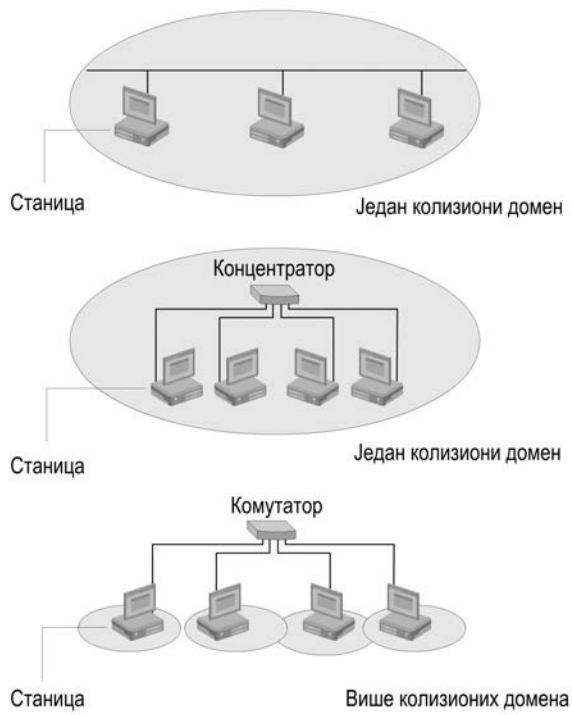
Табела 13.5 Проширење стандарда IEEE802.11

14. Међусобно повезивање рачунарских мрежа

Уводном поглављу је наглашено да рачунарска мрежа која није повезана са другим рачунарским мрежама више нема никаквог смисла. У овом поглављу анализираћемо концепт и уређаје за међусобно повезивање локалних рачунарских мрежа.

14.1 Комутиране локалне рачунарске мреже

Идеја о грађењу локалних мрежа[1] на моделу слања једног ка свима и дељеним медијумима имала је смисла само док саобраћај у локалним мрежама није значајно порастао. Од организације IEEE тражило се да понуди решење које би превазишло проблем загушења саобраћаја. Руковођен искуством из локалних рачунарских мрежа са жетоном, IEEE је 1990. године донео стандард за локалне рачунарске мреже са концентратором[2], заснован на стандарду IEEE802.3 и упређеним парицама. Локалне рачунарске мреже које раде са овим уређајем означавају се и као друга генерација локалних рачунарских мрежа.



Слика 14.1 Три генерације локалних рачунарских мрежа

[1] Идеју реализовали R. Metcalfe и D.L. Boggs у Xerox Co. 1972 године.
[2] *Hub* - хаб.

Проблем загушења у саобраћају је и даље остао неразрешен иако су проблеми поузданости и прекида у инсталацији (каблирању) превазиђени. Проблем загушења у саобраћају превазилази тзв. трећа генерација рачунарских мрежа. Конципиране су као да раде са засебним трансмисионим медијумом и са засебном ширином опсега. Такво својство обезбеђује уређај који називамо комутатор локалне рачунарске мреже [1].

Комутатор је отишао један корак даље од локалне мреже са концентратором. Он прави од сваког свог порта посебну локалну рачунарску мрежу. Такве мреже се називају комутиране локалне рачунарске мреже. Поменуте три генерације локалних рачунарских мрежа приказане су на слици 14.1.

У поглављу о уређајима за међусобно повезивање рачунарских мрежа детаљније ће бити описани концентратори и комутатори. Као што ћемо видети, комутатори другог и трећег слоја у суштини раде на исти начин као мостови и рутери.

14.2 Комутација на слоју везе

Мноштво организација поседује више локалних рачунарских мрежа и желе да их повежу (обједине). Локалне рачунарске мреже могу бити повезане уређајима који се називају мостови [2] и који раде на слоју везе. Да би обавили преусмеравање мостови испитују адресу слоја везе. Будући да се од њих не очекује да испитују садржај дела за податке [3] у рамовима које преусмеравају, могу преносити и IPv4 [4], IPv6 [5], ATM, OSI, или ма који други тип пакета. Насупрот томе рутери испитују адресе у пакетима и путању заснивају на њима.

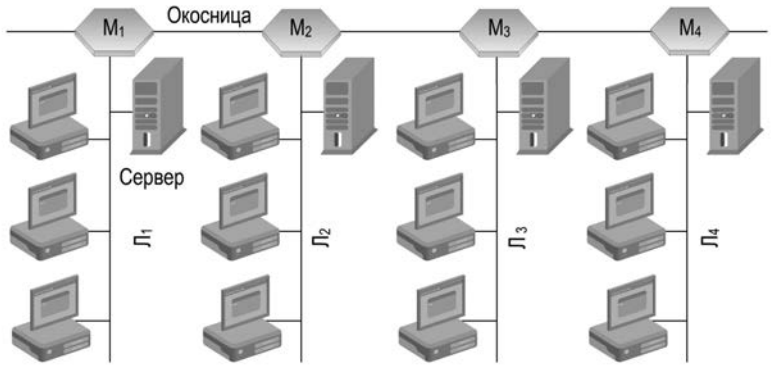
На први поглед изгледа као да постоји јасна разлика између мостова и рутера, али појавом новијих уређаја у комутираним локалним рачунарским мрежама ова разлика је доведена у питање.

У наредним одељцима осврнућемо се на мостове и комутаторе, нарочито при повезивању различитих локалних рачунарских мрежа. Пре залажења у технологију мостова корисно је начинити осврт на неке ситуације у којима је уобичајена употреба мостова. Постоје бројни разлози зашто јединствена организација има сложену локалну рачунарску мрежу.

Као прво, мноштво универзитета и делова организација поседује своје локалне рачунарске мреже, првенствено да би повезали сопствене рачунаре (радне станице) и сервере. Разни одсеци су се одлучивали за различите врсте локалних рачунарских мрежа, без увида у опредељења осталих одсека. Пре или касније јавила се потреба за међусобним повезивањем и мостовима који би то обезбедили.

Као друго, организација може бити просторно раздвојена у неколико зграда на значајној међусобној удаљености. Некада је јефтиније имати одвојене локалне рачунарске мреже у свакој од зграда и повезати их помоћу мостова и бежичних веза него постављати каблове преко читавог подручја.

[1] *Switch* - свич
[2] *Bridge*
[3] *Payload*
[4] *Internet Protocol version* 4 - највише се тренутно користи на Интернету.
[5] *Internet Protocol version* 6 - планира се коришћење на Интернету.



Слика 14.2 Локалне рачунарске мреже ($Л_1$ - $Л_4$) повезане мостовима ($М_1$, $М_2$) и окосницом

Треће, може бити неопходно да се раздвоји једна логичка рачунарска мрежа у више локалних рачунарских мрежа да би се саобраћај равномерно расподелио. На многим универзитетима хиљаде радних станица могу да користе и студенти и особље. Различити софтвери се држе на серверима и по потреби учитавају на радне станице. Уколико би све радне станице биле на једној локалној рачунарској мрежи укупан опсег који би био потребан је превелик. Уместо тога користи се више локалних рачунарских мрежа повезаних мостовима као што је приказано на слици 14.2. Свака локална рачунарска мрежа садржи свој сервер тако да се највећи део саобраћаја обавља у оквиру ње, а само мали део преко кичме рачунарске мреже. Локалне рачунарске мреже често се цртају као да су рачунари међусобно повезани једним каблом [1] (као на слици 14.2). Познато је да се оне данас [2] остварују помоћу концентратора [3] и комутатора [4]. Дугачак кабл и концентратор са више рачунара функционално су идентични. У оба случаја сви рачунари припадају истој области сукобљавања (колизије) и сви користе CSMA/CD протокол за слање рамова. Локалне рачунарске мреже са комутатором значајно се разликују од локалних рачунарских мрежа са заједничким каблом или са концентратором.

Као четврто, у неким ситуацијама јединствена локална рачунарска мрежа би била добро решење у односу на оптерећења али је физичко растојање између најудаљенијих рачунара превелико (нпр. веће од 2,5km за Етернет). Ако је и могуће поставити кабл постоји могућност да локална рачунарска мрежа, због великог времена пропагације између најудаљенијих станица, не би добро радила [5]. Решење је раздвајање локалне рачунарске мреже у сегменте. Један од начина за међусобно повезивање сегмената су мостови који омогућавају да се максимална физичка удаљеност између станица може увећати.

Пето, мостови могу допринети сигурности организације. Већина мрежних интерфејса прихвата све рамове а не само оне адресиране на њих. Уметањем мостова на одре-

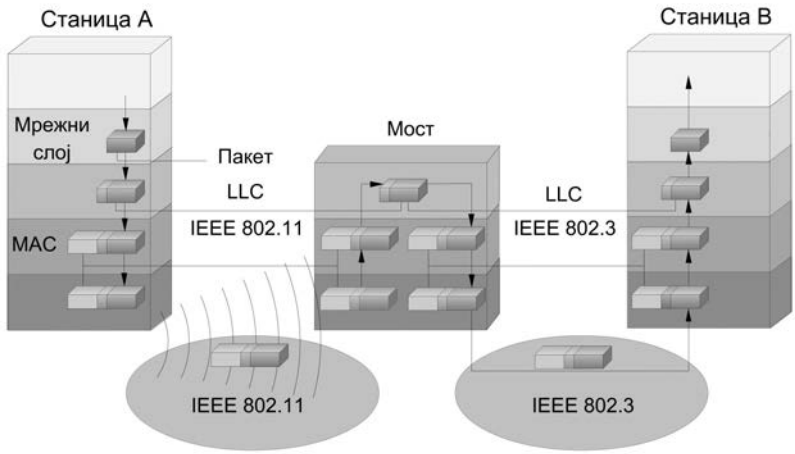
[1] Локалне рачунарске мреже прве генерације
[2] Поглавље 12
[3] Локалне рачунарске мреже друге генерације
[4] Локалне рачунарске мреже треће генерације
[5] Слика 12.4

ђеним местима у локалној рачунарској мрежи може се подесити да се саобраћај од важности задржава само у сигурним деловима рачунарске мреже.

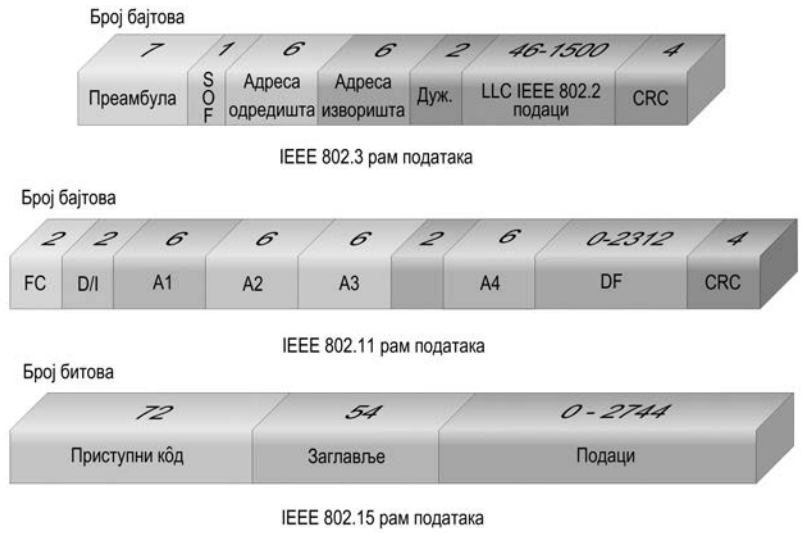
У идеалном случају мостови би требало да су потпуно транспарентни. То значи да је могуће премештати станице (рачунаре) из једног сегмента у други без измена у хардверу, софтверу или табелама за конфигурацију. Такође би требало да је могуће да станица на једном сегменту комуницира са станицом на другом сегменту, без обзира на врсту локалне рачунарске мреже која се користи. Некада је то могуће постићи али не увек.

Мостови за превођење из стандарда IEEE 802.x у IEEE 802.y

На слици 14.3 приказан је рад са двопортним мостом. Станица 1 је у бежичној локалној рачунарској мрежи по стандарду IEEE802.11 и треба да пошаље пакет података станици 2. Она се налази на локалној рачунарској мрежи (кабловској) по стандарду IEEE802.3 на коју је бежична локална рачунарска мрежа везана. Подслој LLC станице 1 прихвата пакет података и додаје своје заглавље. Затим MAC подслој станице 1 формира рам додајући 802.11 заглавље и контролни збир. Рам се шаље радио-таласима ка уређају за приступ (AP) који на основу одредишне адресе види да је рам упућен станици на IEEE802.3 мрежи. Уређај за приступ ради као мост који повезује IEEE802.11 локалну рачунарску мрежу са IEEE802.3 локалном рачунарском мрежом: прихвата рам на физичком слоју и прослеђује га подслојевима изнад себе. На MAC подслоју моста заглавље IEEE802.11 се уклања. Пакет са LLC заглављем прослеђује се LLC подслоју моста. Пошто је пакет усмерен ка IEEE802.3 локалној рачунарској мрежи он се преко IEEE802.3 стране моста шаље на IEEE802.3 мрежу. Треба уочити да би мост који повезује *n* различитих врста локалних рачунарских мрежа имао *n* различитих MAC подслојева и *n* различитих физичких слојева, за сваку врсту по један. Прослеђивање рамова из једне локалне рачунарске мреже у другу је на први поглед веома једноставно. У поглављима која следе биће анализирани проблеми који се јављају код повезивања различитих врста локалних рачунарских



Слика 14.3 Повезивање локалних рачунарских мрежа по стандардима IEEE802.11 и IEEE802.3



Слика 14.4 Формати рамова из серије IEEE802 стандарда

мрежа и рачунарских мрежа градских подручја. Полазимо од чињенице да различите врсте локалних рачунарских мрежа користе различит формат рама података (погледати слику 14.4).

Разлике локалних рачунарских мрежа по стандарду IEEE802.3 (Етернет) и IEEE802.5 (прстен са жетоном) последице су историјске и организационе природе. У односу на стандард IEEE802.11 та разлика је суштинске природе.

На пример, поље „трајање" у раму по стандарду IEEE802.11 је неопходно за протокол за заобилажење колизије [1] и нема никаквог смисла у раму по стандарду IEEE802.3 и протоколу са детекцијом колизије. Последица је да ма каква била повезаност између различитих локалних рачунарских мрежа она захтева поновно формирање рамова и заузимање времена централне процесорске јединице моста.

Други проблем је што међусобно повезане локалне рачунарске мреже не преносе податке истом брзином. Током прослеђивања рамова из брзе у спорију локалну рачунарску мрежу мост не може да проследи рамове брзином којом они пристижу. На пример, уколико се подаци из локалне рачунарске мреже по стандарду IEEE802.3 брзине 1Gb/s шаљу преко бежичне локалне рачунарске мреже по стандарду IEEE802.11b (брзине 11Mb/s) мост ће морати да привремено сместити податке у своју локалну меморију, надајући се да неће доћи у ситуацију да нема довољно меморијског простора.

Трећи проблем, потенцијално најозбиљнији од свих, јесте да локалне рачунарске мреже по различитимIEEE802 стандардима имају различите максималне дужине рамова. Јасно је да проблем настаје када рамове веће дужине треба проследити ка локалној рачунарској мрежи која користи мање рамове. Стандардима није предвиђено да се деоба рамова обавља на слоју везе па мостови рамове који су превелики за прослеђивање одбацују.

[1] CSMA/CA, код врсте рада са дистрибуираним координационим функцијама DCF (13. поглавље).

У бежичним локалним рачунарским мрежама веома је важна сигурност. Стандарди IEEE802.11 и IEEE802.16 на слоју везе користе различите алгоритме за шифрирање, а стандард IEEE802.3 не. Ово значи да се услуга шифрирања, која је на слоју везе могућа, у бежичним рачунарским мрежама губи када се саобраћај одвија преко IEEE802.3 локалне рачунарске мреже. Уколико сама радио-станица не користи шифрирање њени ће подаци при слању ваздушним путем бити незаштићени.

Једно решење проблема сигурности је да се шифрирање обавља на неком од виших слојева. Тада 802.11 станица мора да зна да ли комуницира са другом станицом само преко 802.11 мреже (што подразумева употребу шифрирања на слоју везе), или не (што условљава изостављање шифрирања). Условљавање да станициаправи избор нарушава појам транспарентности међусобно повезаних локалних рачунарских мрежа.

Важна карактеристика је квалитет услуге. И IEEE802.11 и IEEE802.16 обезбеђују квалитет услуге на различите начине. Локалне рачунарске мреже IEEE802.11 могу да раде са централизованом координационом функцијом[1] а локалне рачунарске мреже IEEE802.16 могу да користе везе са константном брзином преноса. Локалне рачунарске мреже IEEE802.3 не подржавају концепт квалитета услуге[2] тако да ће подаци који се преносе преко тих мрежа изгубити дефинисани квалитет услуге.

14.3 Локално, међусобно повезивање рачунарских мрежа

У претходном поглављу анализирали смо проблеме који се појављују при повезивању мостом локалних рачунарских мрежа са различитим IEEE802 стандардима. У великим организацијама, са много локалних рачунарских мрежа, њиховим међусобним повезивањем отвара се читав низ питања, чак и у случају да су све исте врсте нпр. IEEE802.3.

Теоретски посматрано требало би да буде могуће да се набаве мостови по одговарајућем IEEE стандарду, поставе на предвиђена места у рачунарској мрежи и раде без икаквих проблема. Другим речима мостови би требало да буду у потпуности транспарентни (невидљиви и за хардвер и за софтвер).

У свом најједноставнијем облику транспарентни мост прихвата сваки рам који се преноси било којом од локалних рачунарских мрежа на коју је он повезан. На пример посматрајмо конфигурацију на слици 14.5: мост $М_1$ је повезан са локалним рачунарским мрежама $Л_1$ и $Л_2$, а мост $М_2$ је повезан са $Л_2$, $Л_3$ и $Л_4$. Рам који долази на мост $М_1$ са локалне рачунарске мреже $Л_1$ намењен станици $С_1$ може одмах бити одбачен зато што је он већ у одговарајућој локалној рачунарској мрежи. Рам који долази са локалне рачунарске мреже $Л_1$ а намењен је станицама $С_3$ или $С_4$ мора се проследити.

Када рам стигне, мост мора донети одлуку да ли да га одбаци или да га проследити. Ако мост треба да проследити рам онда мора да одлучи ка којој локалној рачунарској мрежи га прослеђује. Мост одлуку доноси на основу резултата претраживања табеле са адресама станица (коју сваки мост има). У табели се налазе адре-

[1] PCF

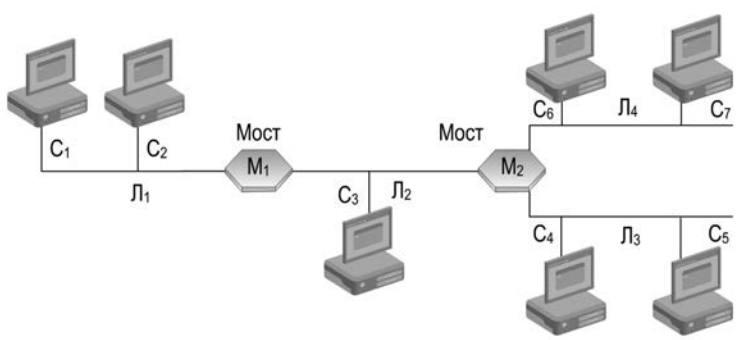
[2] IEEE802.3 (Етернет) је мрежа без успоставе везе и не користи се мехнизам потврде.

се могућих одредишних станица и локалне рачунарске мреже којој станице припадају. На пример, у табели моста $М_2$ би се видело да станица $С_1$ припада локалној рачунарској мрежи $Л_1$. Како ће се после тога преусмеравање одвијати мост $М_2$ не води рачуна.

У тренутку када се мостови први пут прикључе све табеле са записима су празне. Ниједан од мостова не зна где су одредишта тако да се за попуњавање табела користи алгоритам плављења[1]. Овај алгоритам се реализује тако што мост сваки добијени рам са непознатом адресом одредишта прослеђује на све локалне рачунарске мреже на које је повезан, осим оне са које је рам дошао. Како време одмиче табеле са записима мостова се попуњавају[2] па мост зна где се које одредиште налази. Једном када се открије одредиште рамови се усмеравају само ка одговарајућој локалној рачунарској мрежи.

Алгоритам који се користи код транспарентних мостова је учење уназад[3]. Пошто мост види сваки рам који се преноси било којом од локалних рачунарских мрежа са којом је повезан, онда он може на основу изворишне адресе да укаже преко које локалне рачунарске мреже се може доћи до ког рачунара. На пример уколико мост $М_1$ на слици 14.5 види рам на локалној рачунарској мрежи $Л_2$, који долази од станице $С_3$, он зна да станица $С_3$ мора бити доступна преко локалне рачунарске мреже $Л_2$.Тако да ће мост $М_1$ приступити својој табели, и направити запис да рамови који иду ка станици $С_3$ треба да користе локалну рачунарску мрежу $Л_2$. Сваки следећи рам адресиран на станицу $С_3$ који долази са локалне рачунарске мреже $Л_1$ биће прослеђен, али рам за станицу $С_3$ који долази са локалне рачунарске мреже $Л_2$ биће одбачен.

Топологија се може мењати у складу с тим како су рачунари и мостови укључени или искључени, као и померани с једног места на друго. Да би се задржала динамика у топологији у табели се бележи време доласка рамова. Уколико већ постоји запис у табели о времену доласка за изворишну адресу пристиглог рама, он се иновира текућим временом.



Слика 14.5 Међусобно повезане локалне рачунарске мреже ($Л_1$ - $Л_4$) са два моста ($М_1$, $М_2$)

[1] *Flooding*
[2] Користи се израз да мостови уче.
[3] *Backward learning*

Периодично се табеле у мостовима прегледају и уклања старији записи. На овај начин, уколико се станица премести у оквиру зграде са једне на другу локалну рачунарску мрежу и све се то одради у року од неколико минута, радиће нормално без додатних ручних интервенција администратора. Овај алгоритам такође значи да уколико је станица неактивна неколико минута сваки саобраћај ка њој ће се прослеђивати алгоритмом плављења све док она не пошаље рам.

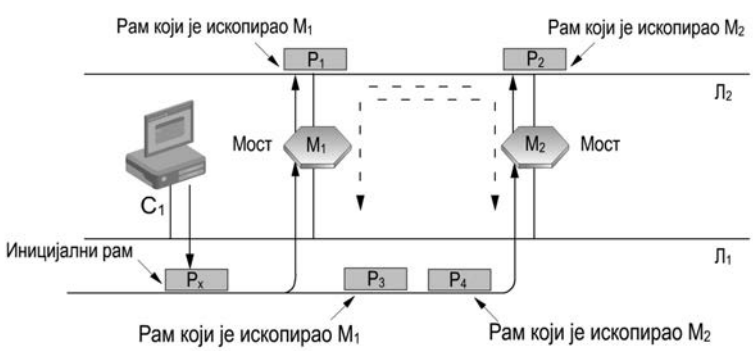
Процедура преусмеравања за долазећи рам зависи од локалне рачунарске мреже са које долази (изворишна локална рачунарска мрежа) и локалне рачунарске мреже ка којој се прослеђује (одредишна локална рачунарска мрежа) при чему:

- уколико је одредишна и изворишна локална рачунарска мрежа иста мрежа, рам се одбацује,
- уколико се одредишна и изворишна локална рачунарска мрежа разликују рам се прослеђује,
- уколико је одредишна локална рачунарска мрежа непозната користи се алгоритам плављења.

Мостови у рачунарским мрежама са топологијом разгранатог стабла

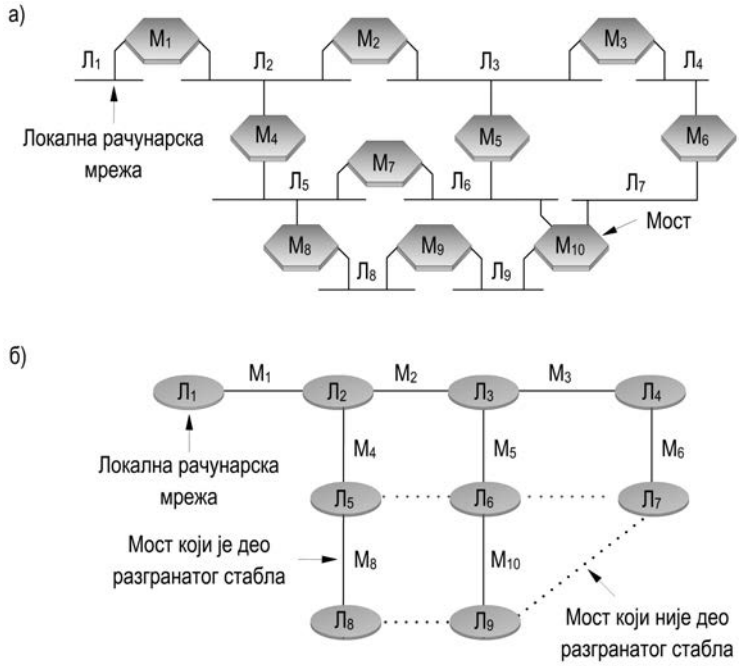
Да би се увећала поузданост на неким местима користе се два или више мостова и везују паралелно између две локалне рачунарске мреже, као што је приказано на слици 14.6. Анализираћемо пример како се рам P_x са непознатом одредишном адресом преноси кроз рачунарску мрежу. Мостови M_1 и M_2, следећи уобичајену процедуру за одређивање непознатих одредишта, користе алгоритам плављења који у овом примеру значи само копирање рама P_x у рамове P_1 и P_2 ка локалној рачунарској мрежи $Л_2$. Убрзо затим, мост M_1 види P_2, рам непознатог одредишта, који копира у рам P_3 ка локалној рачунарској мрежи $Л_1$. Слично томе, мост M_2 копира рам P_1 у P_4. Мост M_1 сада прослеђује рам P_4 даље а мост M_2 рам P_3. Овај процесе се може наставити у недоглед.

Решење је да се у локалним рачунарским мрежама међусобно повезаним мостовима обезбеди топологија разгранатог стабла [1]. То се постиже тако што се неке од веза између локалних рачунарских мрежа изостављају да би се обезбедила топологија без затворених петљи. На пример, на слици 14.7а видимо 9 локалних рачунарских мре-



Слика 14.6 Два паралелна транспарентна моста

[1] *Spanning Tree Bridges*



Слика 14.7 а) Међусобно повезане локалне рачунарске мреже
б) разгранато стабло - испрекидане линије нису део разгранатог стабла

жа међусобно повезаних са 10 мостова. Овај скуп међусобно повезаних локалних рачунарских мрежа може се нацртати као граф у коме чворови представљају локалне рачунарске мреже а лук везује оне локалне рачунарске мреже које су повезане мостом. Добијени граф може се претворити у разгранато стабло изостављањем лукова означених испрекиданим линијама (слика 14.7б).

Посматрајући добијено разгранато стабло види се да постоји само један пут који води од једне локалне рачунарске мреже до било које друге локалне рачунарске мреже. Тако су онемогућене затворене петље.

Да би се направило разгранато стабло треба да се одабере мост који ће бити корен стабла. Сваки мост има свој, на свету јединствени серијски број [1], који се добија од произвођача. Мостови шаљу један другом свој серијски број. Мост са најмањим серијским бројем постаје корен. Затим се прави стабло са најкраћом путањом до сваког моста и локалне рачунарске мреже. Овако направљено стабло је разгранато стабло. Уколико дође до отказа у раду локалне рачунарске мреже или моста прави се нова путања. Без обзира што је успостављено разгранато стабло, а да би могао аутоматски да открије промене у топологији и према томе иновира стабло, алгоритам наставља да се примењује и за време нормалног рада.

Дистрибуирани алгоритам за прављење разгранатог стабла описан је у стандарду IEEE802.1D. Информације о серијском броју моста и друге информације потребне

[1] BID (*Bridge Identification*)

за примену протокола разгранатог стабла размењују се специјалном врстом рамова (BPDU [1]) после одређеног времена.

Време потребно да се реконфигурише локална рачунарска мрежа због промене у њој назива се време опоравка. Брзо разгранато стабло [2] је алгоритам који је време опоравка, које се кретало од 30s до 60s, смањио на 10s. Организација IEEE је 2004. год. издала нову верзију IEEE802.1D са алгоритмом брзог разгранатог стабла.

Порт моста може да:

- ослушкује[3] - уређај обрађује јединицу података моста (BPDU),
- учи[4] - уређај прави табелу са записима којој MAC адреси одговара који порт,
- преусмерава[5] - на једном порту се примају подаци а на другом шаљу (нормалан рад),
- буде заустављен [6] - ка порту који проузрокује петљу нити се шаљу подаци нити са њега примају. Уколико нека од веза откаже овај порт се може укључити у рад,
- буде онемогућен [7] - није део алгоритма разгранатог стабла. Дата је могућност администратору да онемогући (искључи из употребе) одређени порт.

Када се примењује алгоритам брзог разгранатог стабла побољшање је постигнуто на тај начин што се дозвољава да када се прикључи нови уређај порт може одмах да пређе у стање преусмеравања.

Мостови који повезују удаљене локалне рачунарске мреже

Уобичајена употреба мостова је у повезивању две (или више) удаљене локалне рачунарске мреже. На пример једна институција може да има пословнице у неколико градова, сваку са својом сопственом локалном рачунарском мрежом. У идеалном случају све локалне рачунарске мреже би требало да су међусобно повезане тако да се читав систем понаша као јединствена локална рачунарска мрежа. Ово се може постићи постављањем мостова на сваку од локалних рачунарских мрежа и међусобним повезивањем мостова помоћу веза тачка-тачка (на пример изнајмљеним линијама или бежичним везама).

Једноставан систем, са две локалне рачунарске мреже, илустрован је на слици 14.8. У везама тачка-тачка могу се користити различити протоколи. Једна могућност је да се

Слика 14.8 Удаљени мостови могу се користити за повезивање географски удаљених локалних рачунарских мрежа

[1] BPDU (*Bridge Protocol Data Units*)
[2] RSTP (*Rapid Spannig Tree Protocol*). Објављен у стандарду IEEE802.1w.
[3] *Listening*
[4] *Learning*
[5] *Forwarding*
[6] *Blocking*
[7] *Disabled*

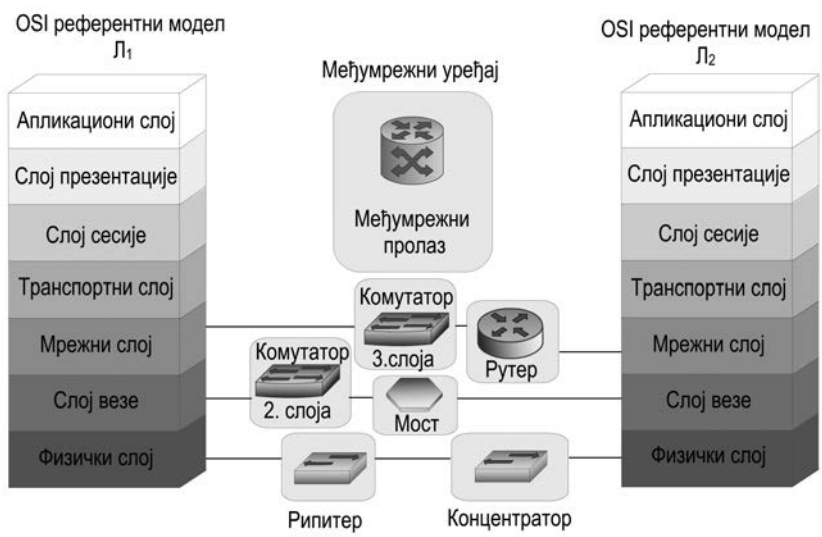
изабере неки од протокола слоја везе, као што је на пример протокол тачка-тачка (PPP[1]). Овај протокол цео MAC рам смешта у своје поље за податке и тако га преноси. Други начин био би да се из рама уклоне заглавље и контролни збир. Оно што је преостало од рама смешта се у поље за податке протокола тачка-тачка. Ново MAC заглавље и контролни збир могу се поново додати на одредиште.

Слојевита архитектура и уређаји за повезивање

Постоје различити начини да се рам усмери са једног сегмента локалне рачунарске мреже на други. Уређаји који то омогућавају су: обнављивачи[2], концентратори, мостови, комутатори, рутери и међумрежни пролази[3]. У овом одељку биће анализиране њихове сличности и разлике.

Као што се види на слици 14.9 поменути уређаји раде на различитим слојевима OSI референтног модела. Слој је од значаја зато што различити уређаји користе различите информације на основу којих обављају преусмеравање. Уобичајено је да корисник има неке податке које жели да пошаље ка удаљеној станици. Ови подаци се преносе од слоја до слоја. Сваки од слојева додаје своје заглавље, осим слоја везе који додаје и крај (контролни збир). Тако формиран рам прослеђује се ка одредишту где се извршава обрнут процес: сваки слој уклања своје заглавље а преостали део[4] прослеђује слоју изнад себе. Овај процес се назива процес паковања и распакивања[5].

Анализираћемо везу уређаја за преусмеравање и слојева OSI референтног модела. На самом дну референтног модела на физичком слоју, налазимо обнављиваче (рипитере).



Слика 14.9 Слојеви OSI референтног модела и уређаји за међусобно повезивање рачунарских мрежа

[1] *Point to Point Protocol*
[2] *Repeater*
[3] *Gateway*
[4] *Payload*
[5] *Encapsulation, decapsulation.* 3. поглавље.

Рипитер

Рипитер (обнављивач) је уређај који сигнал који је долази на његов улаз обнавља и шаље га на свој излаз. Рипитери не познају (и не залазе) у структуру рамова и не анализирају садржај заглавља. Они познају само напонске или струјне нивое и о њима воде рачуна.

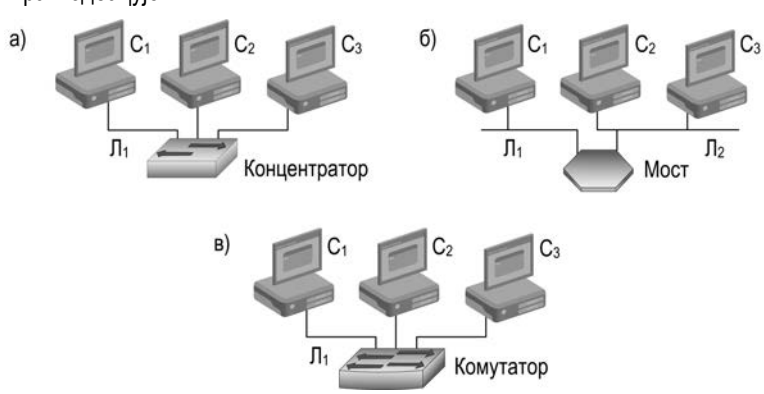
Концентратор

Концентратор је уређај који има већи број улазних линија (портова) преко којих су везане станице. Рам који пристигне са било које од улазних линија шаље се на све остале линије, тј. ка свим осталим станицама. Уколико концентратору два рама стигну у исто време доћи ће до међусобног сукобљавања, као да су станице повезне коаксијалним каблом. Другим речима, концентратор представља јединствену област (домен) за сукобљавање [1]. Брзина на свим линијама концентратора мора да буде иста. Као и обнављивачи, концентратори не анализирају адресна поља рама (MAC адресу) нити их на било који други начин користе (14.10).

Мостови и комутатори

Мост повезује две или више локалних рачунарских мрежа, (слика 14.10б). Када мост прими рам из заглавља рама издваја адресу одредишта и упоређује са записима у табели, и на основу тога се врши преусмеравање. За IEEE802.3 локалне рачунарске мреже ова адреса је 48-битна адреса одредишта [2]. Мост може да има различите мрежне (линијске картице) за различите врсте локалних рачунарских мрежа и различите брзине. За мост је свака линија посебна област сукобљавања, што није случај са концентратором. На слици 14.11 приказана су поља рама која су од значаја за преусмеравање.

Комутатори су слични мостовима по томе што и један и други уређај усмеравају рамове на основу њихове адресе. Суштинска разлика је у томе што се комутатор најчешће користи за повезивање станица, као што је приказано на слици 14.10в. Последица тога је да када станица C_2 са слике 14.10б хоће да пошаље рам ка станици C_3, мост такав рам одбацује.



Слика 14.10 Уређаји за међусобно повезивање а) концентратор б) мост в) комутатор

[1] Колизиони домен
[2] Слика 12.13

Слика 14.11 Рам на слоју везе

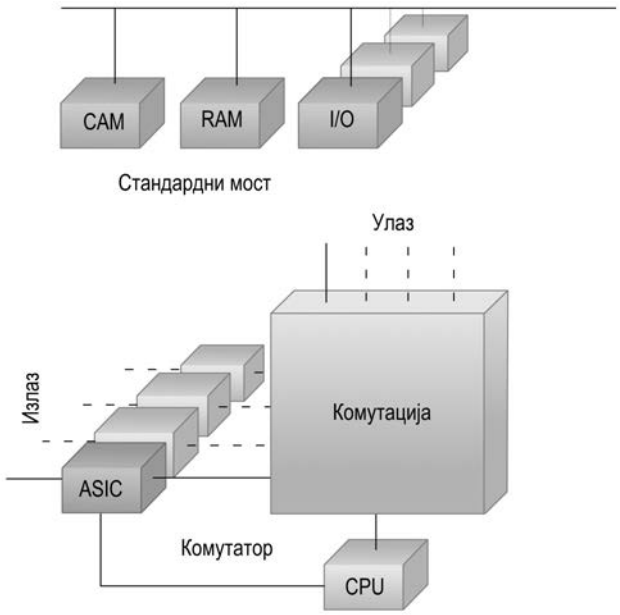
Насупрот томе, слика 14.10в, комутатор мора активно да проследи рам од станице C_1 ка станици C_2, зато што не постоји други начин да рам стигне до станице C_2. Како сваки порт комутатора уобичајено иде на један рачунар, комутатори морају да имају простора за много више линијских (мрежних) картица, него мостови чија је искључива намена повезивање локалних рачунарских мрежа. Свака мрежна картица садржи меморијски простор за смештање рамова који пристижу на њен улаз (порт). Будући да сваки порт представља сопствену област сукобљавања (колизиони домен), комутатори никада не губе рамове као последицу сукобљавања.

14.4 Принцип рада комутатора слоја 2

Комутатор слоја 2 је уређај који може да очита MAC адресе станице и запамти која је станица прикључена на који његов улаз (порт). Када комутатор прими рам са било ког улаза он очитава одредишну MAC адресу и рам шаље на улаз за који је станица са одредишном MAC адресом прикључена. Ако је одредишна адреса „један ка свима" онда ће рам бити послат на све портове комутатора. Када је одредишни порт заузет комутатор ће сместити [1] рам док се одредишни порт не ослободи.

Предности овог приступа су да се побољшање пропусне моћи може постићи једноставном изменом комутатора и да је сваки прикључени систем посебан колизиони домен. Локална рачунарска мрежа са оваквим уређајем назива се комутирана локална рачунарска мрежа. Пројектанти првог комутатора [2] успели су да споје два концепта: мост и концентратор. Комутатор има физички изглед и конфигурацију концентратора а интерно примењује комутацију. Модул за комутацију је најчешће дељена меморија или унакрсни [3] комутатор, иако су могуће и друге технологије. Такође је уобичајено да се за сваки од интерфејса на комутатору угради једно специјализовано интегрисано коло (ASIC [4]) које одлучује о филтрирању, прослеђивању и убацивању

[1] Баферовати
[2] Фирма *Kalpana* коју је касније купио *Cisco Systems.*
[3] *Cross point*
[4] *Application Specific Integrated Circuit* - интегрисана кола специфичне намене.



Слика 14.12 Комутатори и стандардни мост

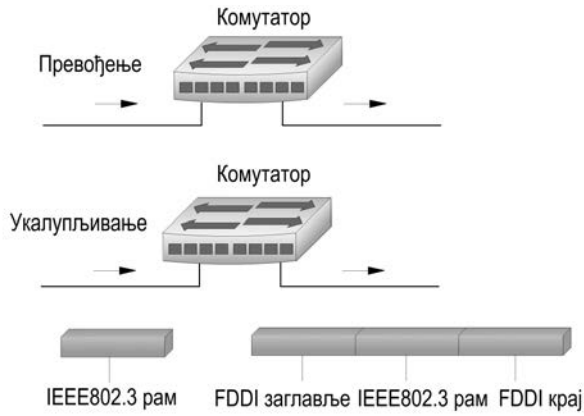
рамова у уређај за комутацију. Стандардни мост, је ради поређења, суштински фон Нојманов рачунар оптимизован за функције премошћавања (слика 14.12).

Увођење комутатора отворило је врата новом концепту - локалним мрежама са потпуним дуплексом. У локалним рачунарским мрежама стандардни начин рада био је полудуплекс (само једна станица може да буде присутна на трансмисионом медијуму). Комутатори могу да формирају приватну локалну рачунарску мрежу са само две прикључене станице. Рад у потпуном дуплексу омогућава дуплирање пропусне моћи система.

Комутатори имају и мало време кашњења. Због своје архитектуре мостови прихватају цео рам и затим га прослеђују [1]. Једна од предности овог приступа је што било који рам који је откривен са грешком може бити одбачен пре прослеђивања. Недостатак овог приступа је повећано време кашњења. Са брзином од 10Mb/s рам дужине 1500 бајтова изгуби бар 1,2ms времена пролазећи кроз стандардни мост [2].

Комутатор може да започне са прослеђивањем рама пре него што је он потпуно примљен. Тако се у преносу рама уноси само кашњење које је једнако времену потребном да се прочита одредишна адреса, која је на самом почетку рама. Са брзином 10Mb/s, рам дужине 1500 бајтова касни [3] само 0,0048ms. Рамови са грешком, нажалост, могу бити откривени само када је рам потпуно примљен, па се прослеђивањем рамова са грешком пропусна моћ система безразложно троши. Ако је одредишни порт заузет комутатор ради као и мост - прихвата комплетан рам и касније га прослеђује.

[1] *Store and forward bridging*
[2] Један бит би могао да за то време пређе 350km.
[3] Један бит за то време може да пређе око 1,5km.



Слика. 14.13 Превођење и укалупљивање

Битна особина комутатора је њихова способност да уче MAC адресе. Комутатор може да научи адресу станице везане за порт, али и других прикључених уређаја који могу бити рутери, други комутатор, концентратори или мостови. Комутатори обично објављују адресну способност по порту и укупну адресну способност.

Комутатор може да подржава различите брзине по портовима. На пример брзина коју захтева сервер, рутер или веза ка другом комутатору обично је већа од оне коју захтева станица. Ако је формат рама исти за сваку локалну мрежу комутатор ће сместити рам у меморију да би усагласио различите брзине преноса. На пример, IEEE802.3 комутатор може имати неколико портова типа 100BaseT и један или два порта типа 1000BaseT (слика 12.18).

Као и са свим уређајима за међусобно повезивање у рачунарским мрежама комутатори морају да разрешавају проблем преоптерећења. Један од механизама који се користи је повратни притисак[1]. Када комутатор почне да прима рам намењен преоптерећеном порту он је у стању да генерише ометајући сигнал на пријемном порту. Пошиљалац везан за тај порт престаје са слањем, зауставља се и касније покушава поново. Треба напоменути да о преоптерећењу могу да воде рачуна и виши слојеви механизмима који су им на располагању, као што је на пример контрола тока[2].

Код поступка превођења (транслације) комутатори претварају рам из једног формата у други, на пример: IEEE802.3 у IEEE80211. Док се код поступка паковањ[3] један рам ставља у други. На слици 14.13 приказан је поступак паковање IEEE802.3 рама у FDDI рам. Могуће су и разне друге комбинације.

14.5 Комутатори слоја 3

Од проналаска комутатора води се велика расправа између произвођача рутера и комутатора. Први тврде да комутаторима недостаје комплексност да би задовољили захтеве великих рачунарских мрежа. Други тврде да њихови производи има-

[1] *Backpresure*
[2] Поглавље 11
[3] *Tunneling*

ју нижу цену по порту, веће брзине и мања кашњења што је важно за уградњу у окоснице [1] рачунарских мрежа.

Данас се развој преусмеравања (комутације) на трећем слоју креће у два правца: произвођачи комутатора локалних рачунарских мрежа укључују преусмеравање на бази IP и IPX протокола. Истовремено, произвођачи рутера примењују и комутирајућу технику у своје производе.

Један од најбитнијих чинилаца који су довеле до потребе за повећањем брзина преноса података и за мањим кашњењем у рутирању, су велике брзине података у рачунарским мрежама (на пример ATM, гигабитни Етернет). Код тако великих брзина примена метода „прихвати и проследи" захтевала је велики меморијски простор за смештање рамова и велику процесну моћ рутера. Један гигабитни Етернет адаптер могао би слати рутеру преко 200000 рамова у секунди. Већ са малим бројем портова била би преоптерећена чак и најбржа централна процесорска јединица [2].

Видели смо да су обнављивачи и концентратори слични, као и што су мостови и комутатори. Анализираћемо рутере који се од претходно описаних уређаја значајно разликују. Када рам стигне у рутер (уређај за преусмеравање) заглавље и контролни збир се уклањају и део који се налази у пољу за податке (пакет) препушта се софтверу рутера (слика 14.11). Софтвер ће заглавље пакета искористити да би одабрао линију за даљи пут пакета. Заглавље IP пакета, садржи адресе од 32 или 128 битова, али не и 48-битну MAC [3] адресу. Софтвер рутера не види адресу рама (MAC адресу) и не зна да ли је пакет стигао локалном рачунарском мрежом или везом тачка-тачка. Детаљније ћемо анализирати рутере и рутирање у 16 поглављу.

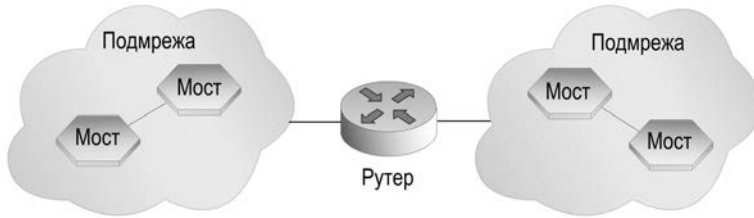
На четвртом слоју (изнад мрежног слоја) уређаји који се за сада користе су транспортни међумрежни пролази (гејтвеји). Транспортни пролази могу да повежу 2 рачунара који користе различите протоколе са успоставом везе на транспортном слоју. На пример, претпоставимо да рачунар који користи TCP/IP протокол са успоставом везе треба да комуницира са рачунаром који користи ATM транспортни протокол са успоставом везе. Транспортни међумрежни пролаз може да копира пакете из једне везе у другу, и ако је потребно поново их форматира.

На крају уређаји на апликационом слоју - апликациони међумрежни пролаз познаје формат и садржај података и може да преведе поруке из једнога формата у други. На пример апликациони међумрежни пролаз може да претвори електронско писмо са Интернета у SMS поруку за мобилни телефон.

14.6 Поређење мостова и рутера

Мостови раде на слоју везе. Каже се да они изолују колизиони домен прослеђујући само оне рамове који треба да пређу из једне локалне мреже у другу. Мостови анализирају MAC адресе (директно или индиректно). Софтвер мостова мора бити спосо-

[1] *Backbone*
[2] CPU
[3] Користи се и термин IEEE802 адреса. Под тим се подразумева скуп свих IEEE802.x стандарда којим су одређена заглавља, а самим тим и адресе рамова за различите типове локалних рачунарских мрежа.



Слика 14.14 Поређење мостова и рутера

бан да чува запис (траг) до сваке потенцијалне крајње станице у мрежи са мостовима.

Рутери раде на мрежном слоју усмеравајући пакете од једне крајње станице ка другој преко међусобно повезаних мрежа[1]. Рутери повезују подмреже. Подмреже могу бити локалне рачунарске мреже, група локалних рачунарских мрежа повезаних мостовима или чак и мреже ширег географског подручја[2]. Без обзира шта је, свака подмрежа је јединствено одређена бројем подмреже. Сваки уређај има адресу мрежног слоја која одређује подмрежу на коју је прикључен и јединствено га одређује унутар те подмреже. Посматрајмо ова два уређаја и упоредимо њихове позиције: мост повезује унутар подмреже док рутер повезује две подмреже (слика 14.14).

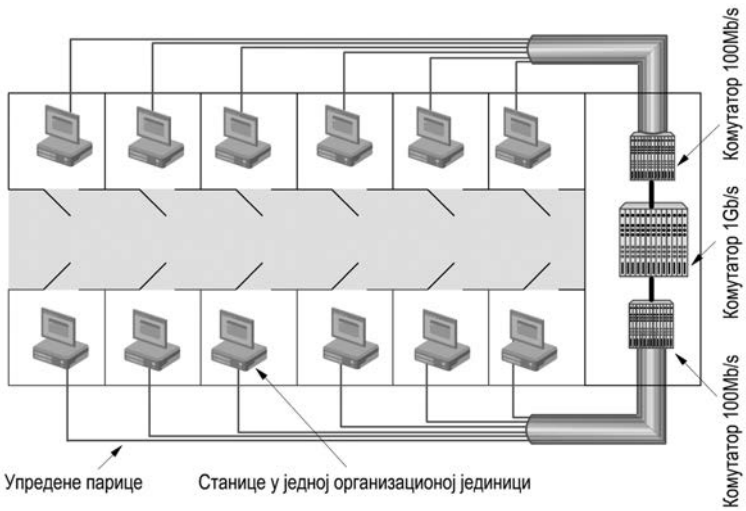
14.7 Виртуелне локалне рачунарске мреже

Некада су се у пословним зградама за међусобно повезивање рачунара у локалну рачунарску мрежу провлачили каблови (дебели или танки Етернет). Сваки рачунар поред кога је кабл пролазио обично је био и прикључен на њега. Други начин ожичавања (каблирања) је повезивање сваког рачунара каблом са централном окосницом рачунарске мреже (слика 14.2), или са централним концентратором. Никакав значај се није придавао томе који рачунар би требало да припада којој рачунарској мрежи. Све особе у суседним канцеларијама биле су повезане на исту локалну рачунарску мрежу, независно од тога да ли су у истој радној групи. Просторни распоред био је изнад организационог.

Појавом 10baseT и концентратора деведесетих година се све то променило. Зграде су поново ожичене упреденим парицама које су се завршавале у специјалним орманима на крају сваке целине или у централној просторији, као што је приказано на слици 14.15.

Помоћу Етернета са концентратором и комутатором било је могуће извршити конфигурацију локалних рачунарских мрежа логички а не физички. Уколико нека институција жели *n* локалних рачунарских мрежа она набавља *n* концентратора или комутатора. Пажљиво бирајући које везе се прикључују за које концентраторе корисници локалне рачунарске мреже могу се одабрати тако да чине организациону целину, без превише утицаја просторног распореда. Наравно, у случају да двоје људи из исте групе раде у различитим зградама они ће вероватно бити на различитим концентраторима а самим тим и на различитим локалним рачунарским мрежама.

[1] *Internetwork*
[2] *Wide Area Network*



Слика 14.15 Зграда са централизованим ожичавањем и употребом концентратора и комутатора

Да ли је од значаја ко је на којој локалној рачунарској мрежи? Често јесте од значаја. Практично све институције имају међусобно повезане локалне рачунарске мреже. Администратори рачунарске мреже из много разлога групишу кориснике тако да се пресликава организациона структура а не њихов физички распоред у згради. Једно је питање сигурности. Било који мрежни интерфејс може бити постављен да ради у помешаном начину[1], копирајући сав долазни саобраћај. Многи одсеци, као што је на пример студентска служба или рачуноводство поседују информације за које не желе да доспеју изван њихових организационих јединица. У таквој ситуацији има смисла обезбедити да су сви сарадници из једног одсека у јединственој локалној рачунарској мрежи. Такође је важно не дозволити да ма који део тог саобраћаја изађе ван оквира те локалне рачунарске мреже. То некада и није једноставно остварити.

Друго тежиште је стављено на питање оптерећења. Неке локалне рачунарске мреже се више користе од других и пожељно је одвојити их.

Трећи проблем представља слање одређених рамова свим станицама[2]. Већина локалних рачунарских мрежа подржава слање свима, а и протоколи виших слојева га користе[3]. Као последица слања рамова свим станицама код више међусобно повезаних локалних рачунарских мрежа лако може да дође до емисионе олује[4]. То значи да је капацитет локалне рачунарске мреже заузет рамовима упућеним свим станицама, а да саме станице велики део свог времена посвећују обради и одбацивању тих рамова.

На први поглед се чини да је решење раздвајање локалних рачунарских мрежа мостовима и комутаторима. Пошто је основно обележје повезаних локалних рачунарских мрежа транспарентност (рачунар се може преместити из једне локалне ра-

[1] *Promiscuous*
[2] *Broadcast frame*
[3] Пример је ARP (*Adress Resolution Protocol*) протокол за разрешавање IP у MAC адреси
[4] *Broadcast storm*

чунарске мреже у другу а да се то не примети) мостови морају да усмеравају и рамове упућене свим станицама тј. не могу да спрече појаву емисионих олуја.

Пошто смо видели зашто институцијама треба више локалних рачунарских мрежа ограниченог домета, размотрићемо проблем раздвајања логичке од физичке топологије. Претпоставимо да је корисник премештен у оквиру институције из једне канцеларије у другу без промене организационе јединице. Са инсталираним концентраторима премештање корисника на одговарајућу локалну рачунарску мрежу значи да администратор из централног ормана премести кабл који повезује корисников рачунар са једног концентратора на други концентратор. У многим институцијама организационе измене су учестале, што значи да администратори система треба да посвете доста времена премештању каблова. Некада измене нису ни могуће зато што је прикључак корисничког рачунара сувише удаљен од одговарајућег концентратора.

Реагујући на захтев за већу флексибилност произвођачи и пројектанти локалних рачунарских мрежа отпочињу рад тако што праве нову софтверску инсталацију (оживчавање) целе зграде. Резултујући концепт назива се виртуелна локална рачунарска мрежа и означава се са ВЛ (VLAN [1]). Удружење IEEE802 е стандардизовало концепт и носи ознаку IEEE802.1Q.

Виртуелне локалне рачунарске мреже су засноване на специјално пројектованим ВЛ комутаторима. Да би се подесила мрежа базирана на виртуелним локалним рачунарским мрежама, администратор мреже мора да прецизира:

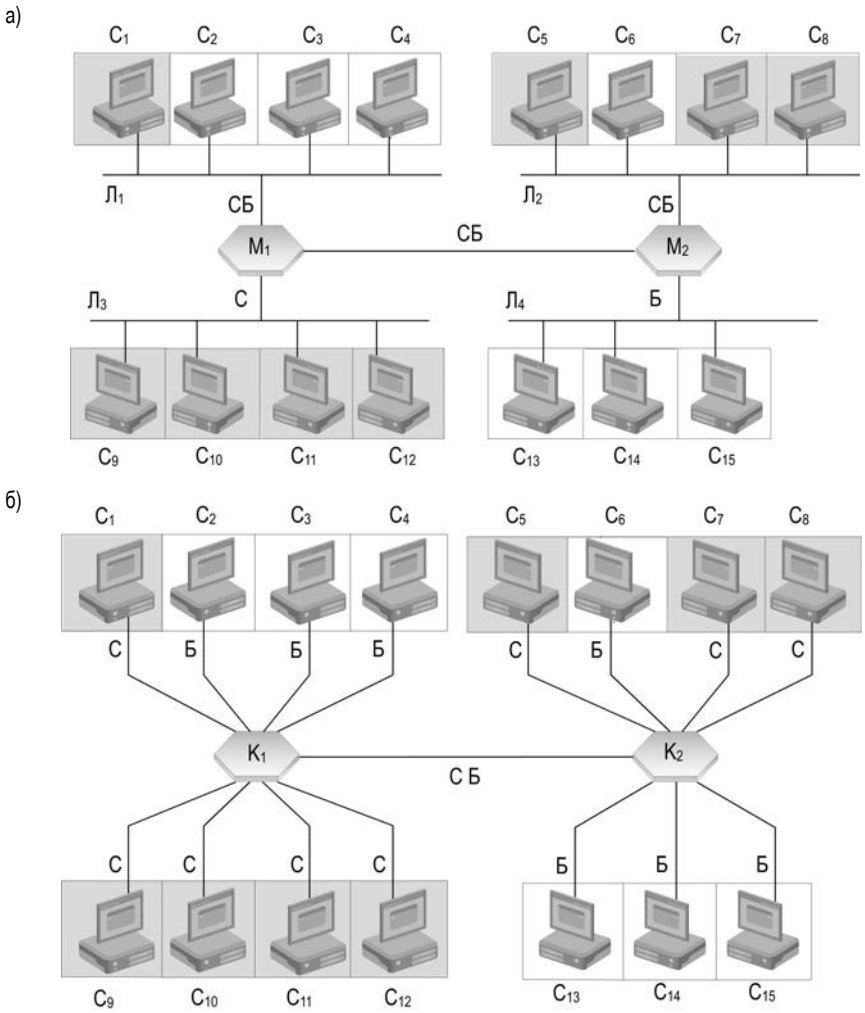
- број виртуелних мрежа,
- распоред - који ће се рачунар налазити на којој виртуелној мрежи,
- величину виртуелних мрежа.

Често се виртуелне локалне рачунарске мреже (неформално) означавају по бојама, будући да је тада могуће да се одштампају обојени дијаграми који приказују стварни положај рачунара. На пример, сви рачунари који припадају црвеној виртуелној мрежи обојени су црвеном бојом, рачунари који припадају зеленој виртуелној мрежи обојени су у зелено итд. На овај начин су и физички и логички распоред видљиви на јединственом цртежу.

Као пример анализираћемо 4 локалне рачунарске мреже као на слици 14.16 на којој 8 рачунара припада сивој виртуелној мрежи (С), 7 од њих припада белој виртуелној мрежи (Б). Четири физичке локалне рачунарске мреже повезане су помоћу два моста, $М_1$ и $М_2$. Уколико се користи централизована инсталација са упређеним парицама могу да се поставе и 4 концентратора (нису приказани на слици). Као што је познато логички кабл са више станица и концентратор раде на исти начи. Цртање на овај начин чини слику прегледнијом. Мост се данас углавном користи када је више рачунара везано на сваки од портова (слика 4.16). Јасно је да су мост и комутатор међусобно заменљиви. Слика 14.16б приказује исте рачунаре и исте виртуелне мреже са комутаторима, код којих је за сваки порт везан по један рачунар.

Да би виртуелне мреже правилно радиле табеле са записима треба да буду формиране на мосту или на комутатору. Ове табеле указују која виртуелна мрежа је до-

[1] *Virtual Local Area Network*



Слика 14.16 а) Четири физичке локалне рачунарске мреже организоване у две виртуелне мреже, сиву (С) и белу (Б)
б) истих 15 рачунара је организовано у две виртуелне мреже повезане комутаторима

ступна на ком порту. Када рам долази са сиве виртуелне мреже он се мора проследити ка свим портовима означеним сивом бојом. Ово је уобичајено и за саобраћај ка једној станици [1], ка више станица [2] и ка свим станицама [3]. Порт може бити означен са више боја што се најбоље види на слици 4.16а. Претпоставимо да станица C_1 шаље рам ка свим станицама. Мост M_1 прима рам и види да је он пристигао са рачунара на сивој виртуелној мрежи, тако да га прослеђује на све портове означене са С. Будући да M_1 има само два сива порта и да су оба означена са С, рам је послат на оба.

[1] *Unicast* - уникаст
[2] *Multicast* - мултикаст
[3] *Broadcast* - бродкаст

Са мостом $М_2$ ситуација је другачија. Овде мост зна да нема сивих рачунара на локалној рачунарској мрежи $Л_4$, тако да се рам тамо и не прослеђује. Рам се прослеђује на локалну рачунарску мрежу $Л_2$. Уколико један од корисника на локалној рачунарској мрежи $Л_4$ треба да промени организациону јединицу и буде пребачен у сиву виртуелну мрежу, онда у табели записа моста $М_2$ порт на који је корисник везан и који је био означен као бели (Б) треба да се сада означи са СБ (сиво-бели). Уколико рачунар 9 постане сив онда и порт за који је везан у локалној рачунарској мрежи $Л_2$ треба да буде сив (С) уместо сиво-бели (СБ).

Претпоставимо да сви рачунари на локалним рачунарским мрежама $Л_2$ и $Л_4$ постану сиви. Портови моста $М_2$ на локалним рачунарским мрежама $Л_2$ и $Л_4$ постају сиве боје (С) а такође и портови моста $М_1$ ка мосту $М_2$ морају да промене боју од сивобеле (СБ) у сиву (С). Бели рамови који долазе до моста $М_1$ са локалних рачунарских мрежа $Л_1$ и $Л_3$ не треба више да буду прослеђивани ка мосту $М_2$.

До сада смо закључили да мостови и комутатори некако знају које је боје долазећи рам. Како они то знају? Користе се следећа три метода:

1. сваком порту је додељена боја виртуелне локалне рачунарске мреже,
2. свакој MAC адреси је додељена боја виртуелне локалне рачунарске мреже,
3. сваком протоколу слоја 3 или IP адреси је додељена боја виртуелне локалне рачунарске мреже.

У оквиру првог метода, сваки порт је означен бојом виртуелне мреже. Овај метод добро ради само ако сви рачунари на порту припадају истој виртуелној мрежи. Као што се види на слици 14.16а, ово важи за мост $М_1$ и порт ка локалној рачунарској мрежи $Л_3$, али не и за порт ка локалној рачунарској мрежи $Л_1$.

У оквиру другог метода мост или комутатор поседује у табели записе о MAC адреси сваког рачунара који је повезан на њих и запис о виртуелној мрежи којој тај рачунар припада. На тај начин могуће је поставити више виртуелних мрежа на стварној виртуелној мрежи као што је случај у мрежи $Л_1$, на слици 14.16а. Када рам стигне до моста или комутатора, да би они видели са које виртуелне мреже је рам дошао, треба да издвоје MAC адресу из заглавља рама и потраже у табели запис о њој.

Код трећег метода мост и комутатор испитују садржај поља за податке рамова. На основу тога врше груписање свих рачунара са IP протоколом као да припадају једној виртуелној мрежи и свих рачунара са IPX[1] протоколом као да припадају некој другој виртуелној мрежи.

Проблем са оваквим приступом је нарушавање основног правила умрежавања - независност слојева. Задатак слоја везе није да задире у садржај поља за податке рама. Слој везе не би требало да испитује поље за податке, а још мање да доноси одлуке које се заснивају на њиховом садржају.

Последица употребе оваквог приступа била је да комутатор неће моћи да ради ако дође до измена у протоколу на 3. слоју (нпр. пређе се са верзије IPv4 на верзију IPv6).

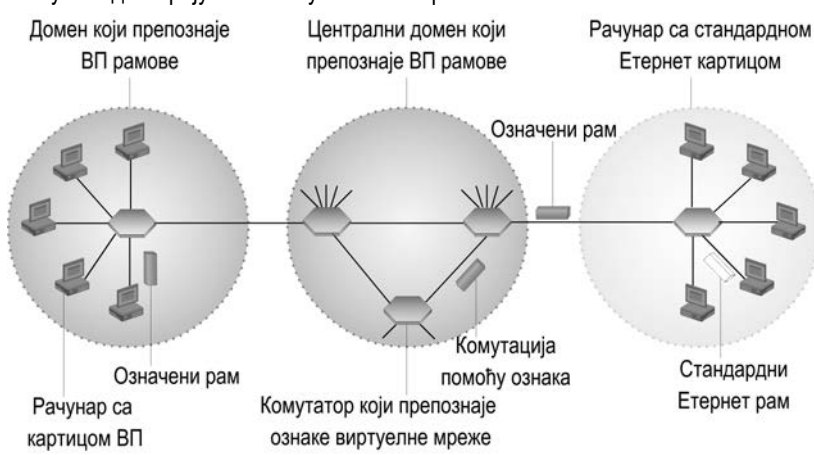
[1] Протокол мрежног слоја мрежног опертивног система *Netware* произвођача *Novell.*

14.8 Стандард IEEE 802.1Q

Од највећег значаја за виртуелне локалне рачунарске мреже је рам који се у њима преноси. Уколико би било начина да са виртуелна мрежа означи у заглављу рама онда би потреба да се анализира поље за податке нестала. За новије локалне рачунарске мреже, као што су IEEE802.11 или IEEE802.16, довољно би било додати у заглавље рама поље за виртуелну мрежу. У ствари за поље[1] „ознака везе" у раму IEEE802.16 може се казати да је слично ономе што јесте ознака виртуелне мреже. Поставља се питање како разрешити проблем у IEEE802.3 (Етернет) мрежи, која је најраспрострањенија локална рачунарска мрежа, када у њеном раму не постоји ниједно слободно поље које би могло да се искористи као ознака виртуелне мреже? Решење је измена Етернет заглавља. Нови формат рама објављен је у оквиру стандарда[2] IEEE802.1Q . Максимална дужина рама по стандарду IEEE802.3 је 1518 бајтова. Стандард IEEE802.1Q је ту границу повећао на 1522 бајтова.

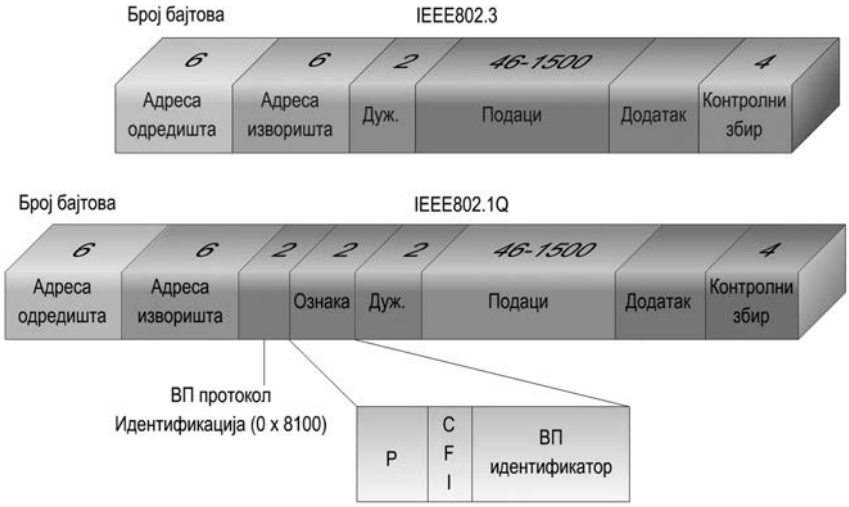
Ознаке виртуелних мрежа (тзв. ВЛ поља) користе само мостови и комутатори, а не и крајње станице (рачунари). Посматрајући слику 14.16 видимо да је најважније да ознаке постоје у линијама између мостова и комутатора. Затим, да би се виртуелне мреже користиле мора да постоје мостови и комутатори који знају за постојање виртуелних мрежа[3].

Током процеса преласка многе инсталације ће имати и рачунаре који још увек имају картице (класични или брзи Етернет) које нису пројектоване тако да могу да препознају ознаке виртуелних мрежа и друге (типичне гигабитни Етернет) које то могу. Ово је илустровано на слици 14.17: засенчени су рачунари који препознају ознаке, а нису они који их не препознају. Претпоставићемо да сви комутатори могу да препознају ознаке виртуелних мрежа. Уколико то није случај први комутатор на који рам наиђе, а који може да препозна ознаке виртуелне мреже моћи ће да на основу MAC или IP адресе дода ознаку на одговарајуће место у заглавље рама.



Слика 14.17 Прелаз на локалне рачунарске мреже по IEEE802.1Q стандарду

[1] *Connection identifier*
[2] Прва верзија је донета, 1998. год. иновиран је 2003. год.
[3] *VLAN aware* - свестан постојања виртуелних рачунарских мрежа, тј. ознака које се на њих односе.



Слика 14.18 Формати рамова по стандардима IEEE802.3 и IEEE802.1Q

На слици 14.17 мрежне картице по IEEE802.1Q стандарду формирају означене рамове и надаље у комутацији се те ознаке користе. Да би се комутација обавила комутатори морају да знају која се виртуелна мрежа налази на ком порту, као што смо у анализи уз слику 14.16 већ објаснили. То што зна да рам припада сивој виртуелној мрежи није од значаја уколико комутатор не зна и на које су портове повезани рачунари на сивој виртуелној мрежи. Тако комутатори треба у табели да имају записе о портовима које треба да користе као и о томе да ли они препознају ознаке виртуелних мрежа или не.

Када рачунар (не по IEEE802.1Q стандарду) пошаље рам ка IEEE802.1Q комутатору он формира означени рам користећи запис о виртуелној мрежи на којој је одредиште а користећи ознаку порта, MAC или IP адресу. Одатле па надаље нема више значаја то што пошиљалац није по IEEE802.1Q стандарду. С друге стране комутатор који треба да испоручи означени IEEE802.1Q рам ка рачунару који је по IEEE802.3 стандарду мора да га преформатира у одговарајући рам.

На слици 14.18 приказан је формат рама по стандарду IEEE802.1Q. Измена у односу на IEEE802.3 рам састоји се у додавању поља од четири бајта. Прво поље је ознака протокола[1]. Оно увек мора да има вредност 0x8100. Будући да је овај број већи од 1500 (максимална дужина IEEE802.3 рама), све IEEE802.3 картице интерпретирају га радије као тип протокола него као дужину рама.

Друго двобајтно поље садржи 3 потпоља. Најзначајнија је ознака виртуелне мреже[2], која заузима 12 битова (крајње десно). Поставља се питање којој виртуелној мрежи овај рам припада? Тробитно поље за приоритет[3] не односи се на виртуелне мреже. Ово поље даје могућност да се саобраћају у реалном времену да одговарајући приоритет и побољша квалитет услуге IEEE802.3 мрежа.

[1] *Protocol ID*
[2] *VLAN Identifier*
[3] *Priority*

Последњи бит је канонични идентификатор формата (CFI [1]). Он се такође не односи на виртуелне мреже: одступило се од почетне идеје да направи разлику између неких MAC адреса већ се користи код преноса IEEE802.5 рамова преко IEEE802.3 мрежа.

Као што смо у претходном излагању нагласили, означени рамови долазе на комутатор који те ознаке може да очита. Комутатор на основу ознаке виртуелне мреже у табели записа проналази порт на који рам треба да пошаље.

Како се табела записа прави? Један од начина био би да администратор то одради ручно. Међутим, највећа предност транспарентних мостова је у томе што се једноставно укључе и раде [2] и не захтевају ручно подешавање. Мостови који могу да очитавају ознаке о виртуелним мрежама у рамовима могу на основу тих ознака сами себе да подешавају. Уколико рам са ознаком виртуелне мреже $ВЛ_4$ дође на порт 3, онда је очигледно да рачунар везан за порт 3 припада виртуелној мрежи $ВЛ_4$. Стандард IEEE802.1Q описује како да се динамички направе табеле а на основу алгоритма [3] описаног у стандарду IEEE802.1D.

[1] *Canonical Format Identificator*
[2] *Plug and play*
[3] Аутор Радиа Перлман

15. Интернет протокол

У 3. поглављу анализиране су уопштене карактеристике TCP/IP референтног модела док ће у овом поглављу бити детаљније описан IP[1] протокол. Интернет протокол IP је главна карика у скупу TCP/IP[2] протокола. Све што одраде TCP, UDP, ICMP и IGMP протоколи налази се у, и преноси се IP пакетом (слика 3.10). IP протокол[3] обезбеђује непоуздану, без успоставе везе[4] испоруку пакета. Појам непоуздан значи да се не гарантује да ће IP пакет успешно стићи на одредиште. За IP протокол се каже да обезбеђује најбољу могућу услугу. Када дође до неког проблема (нпр. рутер нема више слободног меморијског простора) IP протокол покреће једноставан алгоритам: одбацује пакет и шаље ICMP поруку изворишту. Захтевану поузданост морају да обезбеде виши слојеви (тј. TCP). Термин без успоставе везе значи да IP протокол не чува никакве информације о међусобној позицији узастопних пакета. Сваки пакет посматра се независно од свих осталих пакета. Ово значи да се IP пакети могу испоручивати ван редоследа. Уколико изворište шаље два узастопна пакета (нпр. 1 и 2) ка истом одредишту и ако се они усмеравају (рутирају) независно један од другог[5] онда се преносе различитим путањама (рутама) тако да пакет 2 може да стигне пре пакета 1.

15.1 Формат заглавља IP пакета верзије 4

На слици 15.1 приказан је формат заглавља IP пакета верзије 4 (IPv4). IP пакет се

Слика 15.1 Формат заглавља IPv4 пакета

[1] *Internet protocol*
[2] *Protocol suite*
[3] Стандард који описује IP је STD 5. Стандард такође описује и протоколе ICMP и IGMP. Спецификација за IP може се наћи у RFC 791, 950, 919, 922 и 2474.
[4] *Connectionless*
[5] 2. поглавље.

састоји од дела за заглавље и дела за податке. Заглавље чини део непроменљиве дужине од 20 бајтова и део променљиве дужине који је опциони. Шаље се редоследом: слева надесно, са битом највеће тежине поља на првом месту. Врста, величина и намена сваког од поља заглавља биће објашњене у тексту који следи.

Верзија[1] (4 бита). Текућа верзија протокола је 4, и означава се са IPv4. Постоји и нова верзија IPv6.

Дужина заглавља IHL[2] (4 битова). Пошто дужина заглавља није константна поље у заглављу, обезбеђује информацију колико је заглавље дугачко, изражено у броју тридесетдвобитних речи. Када не постоји поље опција нормална вредност је 5. Максимална вредност заглавља је 60 бајтова, тако да је поље опција 40 бајтова. За неке опције, као што су оне које праве запис о рути коју пакет пређе, 40 бајтова је изузетно мало и чини опцију бескорисном.

Тип услуге TOS[3] (8 бита). Ово поље дозвољава станици да укаже подмрежи коју врсту услуге жели. Могуће су различите комбинације поузданости и брзине. За дигитализовани говор брза испорука пакета је важнија од тачне испоруке. За пренос датотека важнији је пренос без грешке него брз пренос. Објаснићемо раније имплементиран тип услуге и данашњи (DS[4]/ECN[5]). Тип услуге садржи (слева надесно) следећа поља:

- тробитно поље[6] које указује на приоритете од 0 (нормалан) до 7 (мрежни управљачки пакет);
- четири бита која дозвољавају станици да специфицира шта јој је најважније за подешавање: што мање кашњење, што већа пропусна моћ, што већа поузданост или што нижа цена. Само један од битова треба да буде постављен на један. Уколико су сва четири постављена на нулу у питању је нормална услуга. По теорији ово поље дозвољава рутерима да направе избор између, на пример сателитског линка са великом пропусношћу и великим кашњењем и изнајмљених линија са малом пропусношћу и малим кашњењем (RFC1340, RFC1349). Тип услуге већина новијих имплементација не користи.

Поље DS/ECN подељено је на следећи начин:

- првих 6 битова (DS) одређује различите нивое квалитета услуге (QoS). Могуће је дефинисати 64 (2^6) класа саобраћаја (RFC2474);
- друга 2 бита односе се на загушење саобраћаја (ECN).

Укупна дужина[7] (16 битова). Укупна дужина укључује све у пакету и заглавље и податке. Максимална дужина је 65535 бајтова. За сада горња граница је прихватљива, али са будућим гигабитским мрежама биће потребни већи пакети.

Идентификација[8] (16 битова). Поље је потребно да би омогућило удаљеној стани-

[1] *Version*
[2] *Internet Header Length*
[3] *Type Of Service*
[4] *Differentiated Services*
[5] *Explicite Congestin Notification*
[6] *Precedence*
[7] *Total Length*
[8] *Identification*

ци да одреди ком пакету управо доспели део (фрагмент) припада. Нормално се инкрементира за један при сваком слању пакета. Сви делови истог пакета садрже исту идентификациону вредност.

Не делити DF[1] (1 бит). DF има вредност 1 (постављен је) да би указао да не треба делити пакет. То је команда рутеру да не врши деобу пакета пошто одредиште није у могућности да делове спаја у целину. Постављањем пакета са DF битом пошиљалац зна да ће пакет стићи на одредиште као једна целина, иако ће пакет морати да заобиђе мреже са малим пакетима и одабере мање оптималну путању (руту). Захтева се од свих машина да прихватају фрагменте од 576 бајтова или мање.

Још делова MF[2] (1 бит). MF означава још фрагмената. Сви фрагменти осим последњег имају постављен овај бит. Потребно је знати да су сви фрагменти пакета стигли. Одступање фрагмента указује где у текућем пакету фрагмент припада. Сви фрагменти осим последњег морају бити мултипл од 8 бајтова, што је елементарна јединица фрагмента. Пошто је обезбеђено 13 битова постоји максимално 8192 фрагмената по пакету, па је максимална дужина пакета 65536, за један већа од поља укупне дужине[3].

Време постојања TTL[4] (8 битова). Ово поље је бројач који се користи да би се ограничило време постојања пакета. Поставља се горња граница за број рутера кроз који пакет пролази. Поставља је пошиљалац на неку вредност (најчешће 32 или 64) и умањује се за један при проласку кроз сваки рутер. Када ова вредност стигне до нуле пакет се одбацује, а натраг, изворишној станици, шаље се ICMP пакет. На тај начин спречава се кружење пакета у недоглед.

Протокол[5] (8 битова). Када мрежни слој спои цео пакет потребно му је да зна шта да ради са пакетом. Поље протокола указује који протокол је задужио IP протокол да му пренесе податке: TCP протокол или UDP протокол, итд. Нумерисање протокола је глобално кроз цео Интернет и дефинисано је документом RFC1700.

Контролни збир заглавља[6] (16 битова). Контролни збир се израчунава само за заглавље. Израчунавање се обавља тако што се прво у поље за контролни збир упишу све нуле. Затим се израчуна први комплемент од 16-то битних целина (као да се заглавље састоји од 16-то битних речи). Од добијеног збира (16-то битни број) направи се први комплемент и упише у поље за контролни збир. На пријему се понови операција над целим заглављем. Ако у преносу није дошло до грешке добиће се 16-то битни број са свим јединицама. Ако је дошло до грешке пакет се једноставно одбацује. Протоколи IP, ICMP, IGMP, UDP и TCP користе исти алгоритам за прављење контролног збира дефинисан у документу RFC1071. Уочимо да се збир мора израчунавати на сваком рутеру пошто се мења најмање једно поље (нпр. TTL). Постоји и ефикаснији начин и описан је у документу RFC1141.

Адреса изворишта[7] (32 бита). Указује на адресу мреже и адресу станице (слика 15.1).

[1] *Don' t Fragment*
[2] *More Fragments*
[3] *Total length Field*
[4] *Time to Live*
[5] *Protocol*
[6] *Header Checksum*
[7] *Source Address*

Адреса одредишта [1] (32 бита). Указује на адресу мреже и адресу станице (слика 15. 1).

Опције [2] (променљиве дужине). Ретко се користе и не подржавају их сви рутери и рачунари.

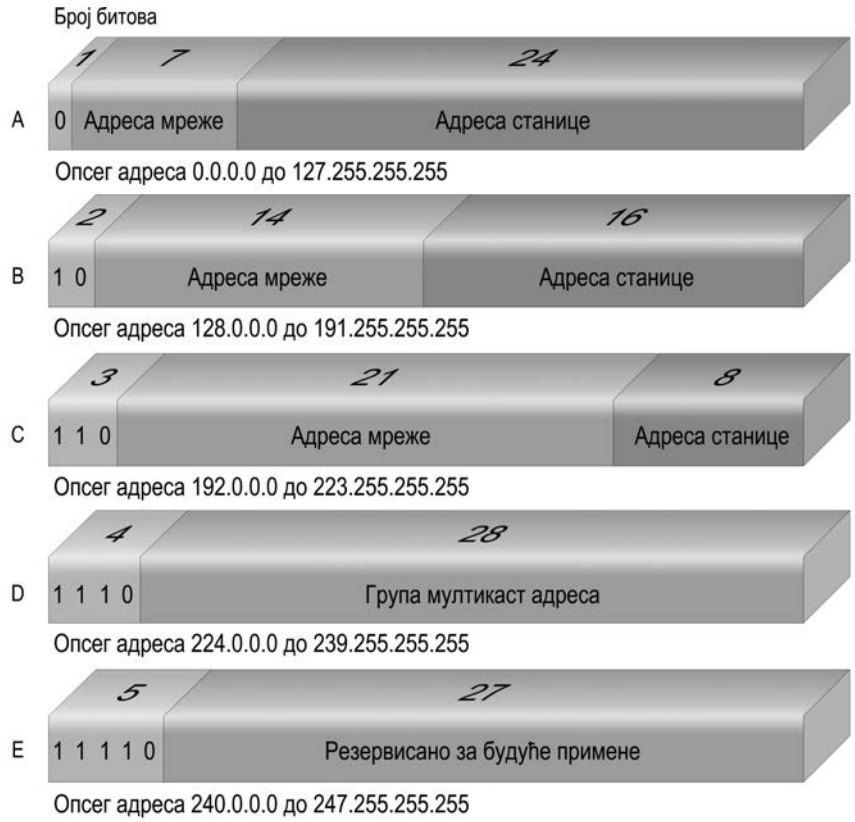
У пољу опције за сада је дефинисано:

- сигурност и ограничења (за војне примене RFC1108),
- записивање руте (рутери уписују своје IP адресе),
- записивање времена (рутери уписују време и своју IP адресу),
- комплетан пут који пакет треба да следи,
- листа рутера које пакет не треба да заобиђе.

Додатак [3] (променљиве дужине). Користи се да обезбеди да је дужина заглавља умножак од 32 бита.

15.2 Адресирање на Интернету

Сваки мрежни интерфејс на Интернету мора да има јединствену Интернет адресу (тзв. IP адресу) која је 32-битни број. Уместо равног адресног простора (нпр. 1, 2, 3,...)



Слика 15.2 Класе IPv4 адреса

[1] *Destination Address*
[2] *Options*
[3] *Padding*

користи се структура приказана на слици 15.2. Уобичајено је да се ова тридесетдвобитна адреса представља са четири децимална броја (један децимални број за један бајт). Први битови указују на који начин је остали део адресе расподељен између дела адресе додељеног мрежи (адреса мреже) и дела адресе додељеног станици (адреса станице). Постоје три типа IP адреса:

- додељена једном рачунару [1] (станици),
- намењена свим станицама [2] (бродкаст) на мрежи,
- намењена групи станица [3] (мултикаст).

На слици 15.2 види се да:

- Класа A адреса:
  - користи 7 битова за адресу мреже и 24 бита за адресу станица. На овај начин може се адресирати $2^7 - 2 = 126$ мрежа. У свакој мрежи може да буде $2^{24} - 2 = 1677721$ станица,
  - опсег адреса је од 0. 0. 0. 0 до 127. 255. 255. 255,
  - одговара мрежама са изузетно великим бројем станица.
- Класа B:
  - користи 14 битова за адресу мреже и 16 битова за адресе станица (хостова). На овај начин може се адресирати $2^{14} - 2 = 16382$ мрежа. У свакој мрежи може да буде $2^{16} - 2 = 65534$ станица,
  - опсег адреса класе B је од 128. 0. 0. 0 до 191. 255. 255. 255,
  - одговара мрежама са релативно великим бројем станица.
- Класа C:
  - користи 21 бит за адресу мреже и 8 битова за адресе станица (хостова). На овај начин може се адресирати $2^{21} - 2$ (2097150) мрежа. У свакој мрежи може да буде $2^8 - 2 = 254$ станица,
  - опсег адреса класе C је од 192. 0. 0. 0 до 223. 255. 255. 255,
  - одговара мрежама са малим бројем станица.
- Класа D:
  - користи се за мултикаст (врста бродкаста) али за ограничене области и једино за станице који користе исту класу D адреса,
  - опсег адреса је од 224. 0. 0. 0 до 239. 255. 255. 255.
- Класа E:
  - резервисана је за примене у будућности,
  - опсег адреса класе E је од 240. 0. 0. 0 до 247. 255. 255. 255.

Разлика између адреса различитих класа најједноставније се уочава на основу првог броја децималне презентације адресе. Посебне (резервисане) IP адресе добијају се постављањем свих битова на 0 или свих битова на 1 и значења су следећа:

- сви битови 0:
  - у адресном делу станице интерпретира се као „ова станица“,
  - у адресном делу мреже интерпретира се као „ова мрежа“. Када станица

[1] *Unicast*
[2] *Broadcast*
[3] *Multicast*

хоће да комуницира преко мреже, али још увек не зна мрежни део IP адресе, може да пошаље пакет са <netID=0> који значи „ова мрежа“. Одговори садрже важећу адресу мреже [1];

- сви битови 1:
  - адреса са свим битовима постављеним на један интерпретира се као све мреже или све станице. На пример адреса 128.2.255.255 значи све станице на мрежи 128.2 (класа B). Ово се назива директни бродкаст пошто садржи важећу адресу мреже и бродкаст адресу станице;
- затворена петља [2]:
  - адреса 127.0.0.1 у класи A је дефинисана као адреса затворене петље. Додељује се мрежном интерфејсу за обраду на локалном систему и нема приступ физичкој мрежи.

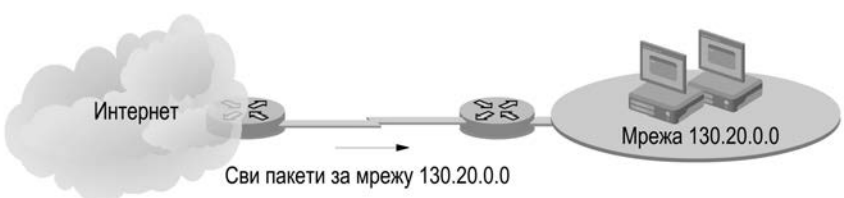
Станица са више интерфејсних модула имаће више IP адреса: за сваки интерфејс по једну. Пошто сваки интерфејс на Интернету мора да има јединствену јавну IP адресу постоји централно место (InterNIC [3]) задужено за додељивање адреса мрежама које су везане за Интернет. Додељивање адреса станицама је надлежност администратора система.

Поред јавних IP адреса постоје тзв. приватне адресе. Приватне адресе су адресе које нису ником званично додељене, не могу се користити на Интернету и не гарантује се да су јединствене. Оне су намењене за мреже које нису директно повезане на Интернет (већ нпр. преко заштитних баријера [4], специјалних сервера [5]...). Приватне адресе су на пример:

- 10.0.0.0/8;
- 172.16.0.0/12;
- 192.168.0.0/16.

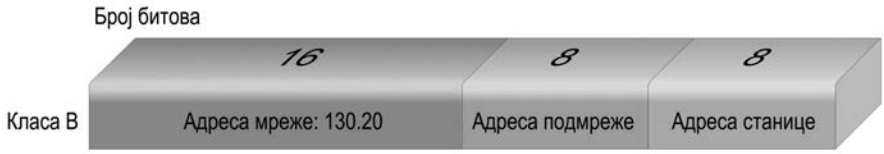
15.3 Адресирање подмрежа

Као последица наглог развоја Интернета принцип додељивања IP адресе постао је превише сложен да би омогућио брзе промене конфигурација локалних мрежа.



Слика 15.3 Мрежа у класи B

[1] *Fully qualified network adress*
[2] *Loopback*
[3] *Internet Network Information Center*. Сервис за регистрацију на Интернету (као што су IP адреса и DNS домен) је раније био у надлежности NIC. 1993. год. формиран је InterNIC за све кориснике осим DDN (*Defense Data Network*) на адреси *rs.internic.net*. Регионалне организације су: ARIN (*American Registry for Internet Numbers*) задужена за Северну и Јужну Америку; RIPE (*Reseaux IP Europeens*), задужена за Европу, Блиски Исток и део Африке; APNIC (*Asia Pacific Network Information Centre*) задужена за Далеки Исток ;
[4] *Firewall*
[5] *Proxy*



Слика 15.4 Прављење подмрежа за адресе класе B

До промене може да дође када се:

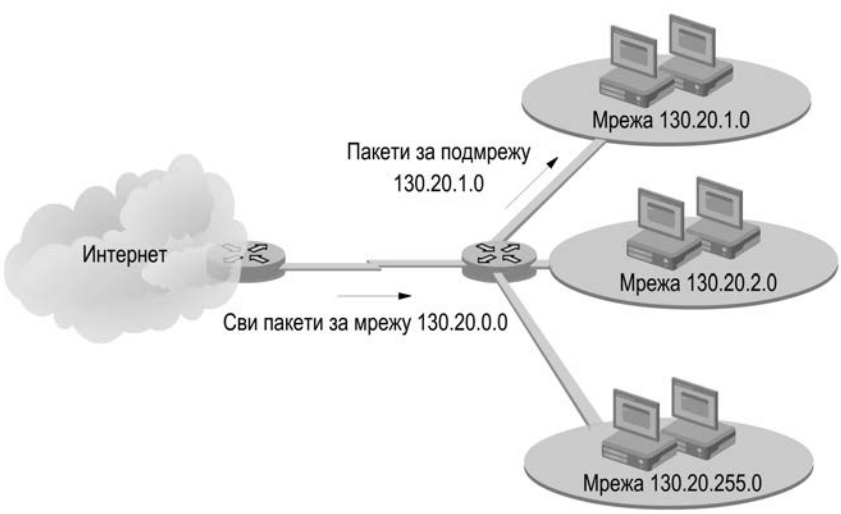
- нови тип физичке мреже инсталира на тој локацији,
- значајно повећа број станица, па се захтева деоба локалне мреже у две или више одвојених мрежа,
- повећање раздаљине које захтева деобу мреже у више мањих мрежа, које су повезане уређајима за међусобно повезивање.

Да би се спречило додавање мрежа са новим IP адресама од свих рачунара захтева се да подржавају адресирање подмрежа дефинисано у документу RFC950. Додељивање адреса подмрежа је локално. Мрежа са подмрежама је споља виђена и даље као једна IP мрежа. Уместо да се посматра само адреса мреже и адресе станице (у оквиру IP адреса) део адресе станице се дели у два дела: у адресу подмреже и адресу станице. Ова идеја има смисла пошто адресе у класи A и класи B имају превише битова додељених адресама станица: 2^{24} - 2 (A); 2^{16}- 2 (B).

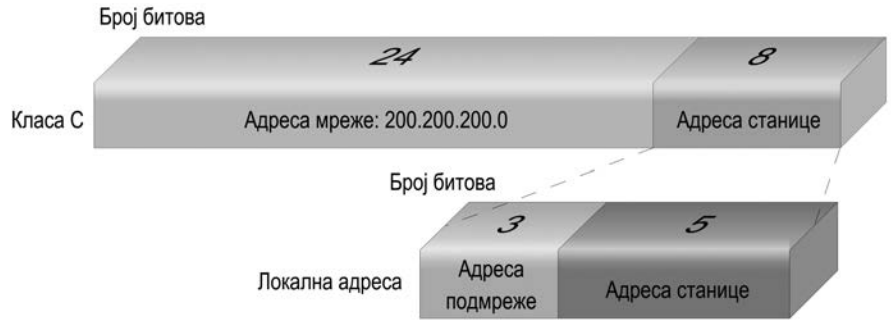
У пракси није уобичајено да се толико рачунара повезује у једну мрежу. На слици 15.2. приказани су формати различитих класа IP адреса. По добијању IP адресе за мрежу од овлашћене организације, ствар је локалног администратора система да ли да прави подмреже или не. Уколико прави подмреже онда је питање колико битова се додељује за адресирање подмреже а колико за адресирање станица.

Пример 15.1: Прављење подмрежа у класи B.

Посматраћемо мрежу у класи B (слика 15.3) чија је мрежна адреса 130.20.0.0.



Слика 15.5 Пример подмреже у класи B



Слика 15.6 Прављење подмрежа за адресе класе С

Од 16 битова додељених адреси станице (хоста) за адресу подмреже додељено је 8 битова (слика 15.4).

На овај начин омогућено је 256 (2^8) подмрежа [1] са 254 (2^8-2) рачунара у свакој подмрежи. Креиране су следеће подмреже (сегменти):

130. 20. 0. 0
130. 20. 1. 0
130. 20. 2. 0
...
130 .20. 255.0

Комбинација броја подмреже и броја станица назива се и локална адреса или локални део IP адресе. Подмрежавање се примењује тако да је невидљиво (транспарентно) за удаљене мреже (сл. 15.5). Структура подмреже станици у оквиру мреже, која је подмрежена, је позната. Станици друге мреже структура подмреже је непозната. Она и даље третира локални део IP адресе као адресу станице. Деобу локалног дела IP адресе на адресу подмреже и адресу станице одређује локални администратор. Било који битови у локалном делу могу се користити за прављење подмрежа.

Пример 15.2: Прављење подмрежа у класи С.

Потребно је мрежу 200.200.200.0 поделити на 7 подмрежа. Позајмићемо три бита

Бинарна вредност 4. бајта (последњег октета)	Адреса подмреже
0 0 0 0 0 0 0 0	200.200.200.0
0 0 1 0 0 0 0 0	200.200.200.32
0 1 0 0 0 0 0 0	200.200.200.64
0 1 1 0 0 0 0 0	200.200.200.96
1 0 0 0 0 0 0 0	200.200.200.128
1 0 1 0 0 0 0 0	200.200.200.160
1 1 0 0 0 0 0 0	200.200.200.192
1 1 1 0 0 0 0 0	200.200.200.224

Табела 15.1 Бинарна вредност и адреса подмреже за пример 15.2

[1] У мрежама са старијим рутерима (старијим протоколима за рутирање) нису дозвољене подмреже са чије су адресе све нуле или све јединице па је у тим случајевима укупан број подмрежа 2^n -2.

Адреса подмреже	Опсег адреса станица	Бродкаст адреса
200.200.200.0	200.200.200.1 - 200.200.200.30	200.200.200.31
200.200.200.32	200.200.200.33 - 200.200.200.62	200.200.200.63
200.200.200.64	200.200.200.65 - 200. 200.200.94	200.200.200.95
200.200.200.96	200.200.200.97 - 200.200.200.126	200.200.200.127
200.200.200.128	200. 200.200.129 - 200.200.200.168	200.200.200.169
200.200.200.160	200. 200.200.161 - 200.200.200.190	200.200.200.191
200.200.200.192	200. 200. 200.193 - 200.200.200.222	200.200.200.223
200.200.200.224	200. 200. 200.225 - 200.200.200.254	200.200.200.255

Табела 15.2 Адресе из примера 15.2

од последњег октета: добићемо $2^3 = 8$ подмрежа. У табели 15.1 дате су бинаране вредност 4. бајта и адреса подмреже.

Број станица у оквиру подмреже (сегмента) може да буде највише $2^5 - 2 = 30$. Све нуле у делу за адресу станице означавају саму подмрежу.

Све јединице у делу за адресу станице означавају све станице у подмрежи. Рам са овом адресом намењен је свим станицама у подмрежи [1].

Пример 15.3: Прављење 7 подмрежа у класи C са старијим протоколима за рутирање.

Старији протоколи за рутирање не дозвољавају да адреса подмреже има све нуле или све јединице. У случају да се одвоје три бита за адресу подмреже добијамо $2^3 - 2 = 6$ подмрежа.

Маска подмреже

Када се користи подмрежавање сама класа IP адресе не може да одреди који део адресе представља адресу мреже а који адресу хоста. Да би се одредило који

Бинарна вредност 4. бајта	Адреса подмреже за новије протоколе	Адреса подмреже за старије протоколе
0 0 0 0 0 0 0 0	200.200.200.0	Не користи се
0 0 1 0 0 0 0 0	200.200.200.32	200.200.200.32
0 1 0 0 0 0 0 0	200.200.200.64	200.200.200.64
0 1 1 0 0 0 0 0	200.200.200.96	200.200.200.96
1 0 0 0 0 0 0 0	200.200.200.128	200.200.200.128
1 0 1 0 0 0 0 0	200.200.200.160	200.200.200.160
1 1 0 0 0 0 0 0	200.200.200.192	200.200.200.192
1 1 1 0 0 0 0 0	200.200.200.224	Не користи се

Табела 15.3 Адресе подмрежа из примера 15.2 и 15.3

[1] *Broadcast*

	16 битова		8 битова	8 битова
Класа B	Адреса мреже		Адреса подмеже	Адреса станице
Маска подмреже	11111111	11111111	11111111	00000000
Децимално	255.255.255.0			
Хексадец.	ffffff00			
	16 битова		10 битова	6 битова
Класа B	Адреса мреже		Адреса подмеже	Адреса станице
Маска подмреже	11111111	11111111	1111111111	000000
Децимално	255.255.255.192			
Хексадец.	ffffff00			

Слика 15.7 Подмреже у класи B са подмрежама од 8 и 10 битова

део IP адресе представља адресу мреже а који адресу станице користи се маска подмреже[1]. Маска је тридесет двобитна вредност у којој су:

- на 1 постављене све позиције у мрежном делу адресе[2],
- на 1 постављене све позиције у подмрежном делу адресе[3],
- на 0 постављене све позиције у делу адресе станице[4].

На слици 15.7 приказане су маске подмреже у класи B када је за подмрежу одвојено 8 и 10 битова. Врло често се маска подмреже пише у префиксној нотацији уз адресу мреже. На пример 192.168.1.0/24, где /24 означава број битова у масци подмреже.

Када станица поседује IP адресу и маску подмреже она може да закључи да ли је пакет упућен ка:

- станици у истој мрежи у којој је и она,
- станици на другој подмрежи у оквиру исте мреже,
- станици на другој мрежи.

Познавање сопствене IP адресе указује да ли је у питању класа A, B или C (на основу битова највеће тежине), што указује где је граница између мрежног и подмрежног дела адресе. Маска подмреже указује где се налази граница између дела адресе подмреже и дела адресе рачунара.

Пример 15.4: Претпоставимо да је адреса рачунара 130.20.1.1 (класа B) и маска подмреже 255.255.255.0 (8 битова за адресу подмреже и 8 битова за адресу рачунара).

На слици 15.8 приказано је како се употребом маске подмреже обавља упоређивање две IP адресе. Уколико је одредишна IP адреса 130.20.5.1 видимо да је мрежни део адресе исти (130.20), али је део за подмрежу различит (1 и 5). Уколико је одредишна IP адреса 130.20.1.22 мрежни део адресе исти (130.20) и део адресе

[1] *Subnet mask*
[2] *NetID*
[3] *Subbnet ID*
[4] *Host ID*

	16 битова		8 битова	8 битова
Класа B	130	20	5	1
Маска подмреже	11111111	11111111	11111111	00000000
Децимално	255	255	255	0
	Адреса мреже		Аресе подмрежа	
	исте		нису исте	
Класа B	130	20	1	1

Слика 15.8 Поређење две адресе класе B

за подмрежу је исти (1). Део адресе за станице је наравно различит (5 и 22). Уколико је одредишна IP адреса 200.168.5.225 (адреса из класе C) мрежни делови адреса су различити. Даља поређења нису потребна.

Пример 15.5: Станица са адресом 200.200.200.65 и маском подмреже 255.255.255.224 треба да пошаље пакет на адресу 200.200.200.91.

Одредиште је на истој мрежи као и станица (рачунар) који шаље пакет.

Моја адреса	11001000	11001000	11001000	01000001
Маска	11111111	11111111	11111111	11100000
И (AND)				
Моја мрежа	11000000	10101000	00000001	01000000
Одредишна адреса	11001000	11001000	11001000	01011011
Маска	11111111	11111111	11111111	11100000
И (AND)				
Одредишна мрежа	11000000	10101000	00000001	01000000

Пример 15.6: Станица са адресом 200.200.200.65 и маском подмреже 255.255.255.224 треба да пошаље пакет на адресу 200.200.200.97.

Одредиште није на истој мрежи као и станица (рачунар) који шаље пакет.

Моја адреса	11001000	11001000	11001000	01000001
Маска	11111111	11111111	11111111	11100000
И (AND)				
Моја мрежа	11000000	10101000	00000001	01000000
Одредишна адреса	11001000	11001000	11001000	01100001
Маска	11111111	11111111	11111111	11100000
И (AND)				
Одредишна мрежа	11000000	10101000	00000001	01100000

Подмреже са променљивом дужином дела за подмрежу

Оригинална имплементација подмрежа подразумева да се мрежа подели на сегменте исте величине. Овакав начин поделе адресног простора не одговара увек стварним потребама. Подмрежа са променљивом дужином дела за подмрежу (VLSM[1]) омогућава креирање сегмената различите величине. У суштини врши се даље подмрежавање подмрежа на претходно описан начин. VLSM треба да буде подржан од стране протокола за динамичко рутирање. Већина нових рутера има подршку за VLSM.

Пример 15.7: Посматрајмо корпорацијску мрежу којој је додељена адреса из класе C 195.214.32.0. Захтева се да се адресни простор раздвоји у пет независних мрежа таквих да:

- подмрежа број 1 има 50 станица,
- подмрежа број 2 има 50 станица,
- подмрежа број 3 има 50 станица,
- подмрежа број 4 има 30 станица,
- подмрежа број 5 има 30 станица.

Овај задатак не може се разрешити подмрежавањем без VLSM-а. У овом примеру прављење подмрежа без VLSM-а дало би четири подмреже (22) од којих свака може да има 62 (2^6 – 2) станице или 8 (2^3) подмрежа од којих би свака имала по 30 станица (2^5 – 2). Ниједно од понуђених решења не задовољава тражене захтеве. Да би се мрежа поделила у пет подмрежа треба дефинисати две различите маске подмрежа:

- маском 255.255.255.192 мрежу можемо поделити у четири подмреже са по 62 станице:
  - 195.214.32.0 маском 255.255.255.192 (подмрежа број 1),
  - 195.214.32.64 маском 255.255.255.192 (подмрежа број 2),
  - 195.214.32.128 маском 255.255.255.192 (подмрежа број 3),
  - 195.214.32.192 маском 255.255.255.192,
- четврту подмрежу можемо даље да поделимо у две подмреже са по 30 станица користећи маску 255.255.255.224:
  - 195.214.32.192 маском 255.255.255.224 (подмрежа број 4),
  - 195.214.32.224 маском 255.255.255.224 (подмрежа број 5).

Добили смо три мреже са по 62 станице и две мреже са по 30 станица. Ово решење задовољава постављене захтеве.

15.4 Динамичко конфигурисање протокола

Протокол за динамичко конфигурисање (DHCP[2]) аутоматски додељује IP адресе станицама и превазилази на тај начин проблеме који наступају када се додељивање обавља ручно.

Као што је на слици 15.9 приказано сваки пут када се покрену DHCP клијенти захтевају информације о IP адресама од DHCP сервера, укључујући и IP адресу, маску

[1] *Variable Length subnetting*
[2] *Dinamic Host Configuration Protocol*

подмреже и друге опционе вредности. Опционе вредности могу да укључе подразумевану адресу међумрежног пролаза[1], адресу сервера имена домена (DNS[2]) итд. Када DHCP сервер добије захтев он селектује информације о IP адресама из заједничког скупа адреса дефинисаних у његовој бази података и нуди их својим клијентима. Уколико клијенти прихвате понуду, информација о IP адресама се за одређени период времена издаје клијентима. Уколико не постоје доступне адресе у заједничком скупу, које могу да се издају клијенту, клијент не може да иницијализује TCP/IP везу.

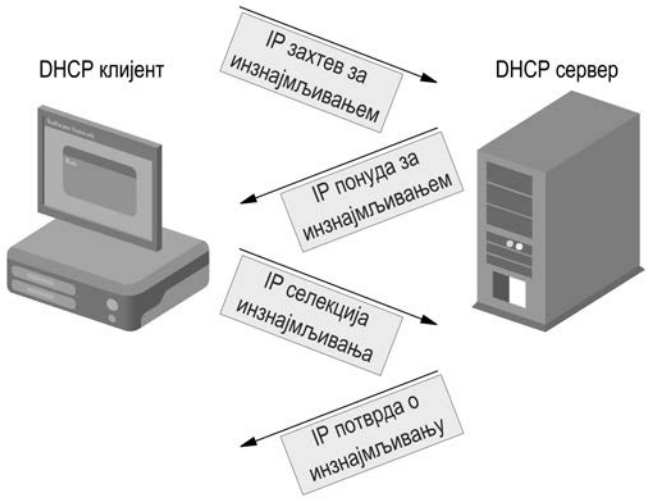
Да би се разумело каква је предност коришћења DHCP протокола за конфигурисање скупа TCP/IP протокола на клијент рачунарима, корисно је описати разлику између ручног (мануелног) метода конфигурисања и аутоматског метода коришћењем протокола DHCP. Ручно конфигурисање скупа TCP/IP протокола значи да корисник може да изабере неку (произвољну) IP адресу уместо да од администратора мреже добије важећу адресу. Коришћење нетачне адресе доводи до проблема у мрежи које је тешко пратити и пронаћи узрок. Уношење некоректне IP адресе, маске подмреже или адресе међумрежног пролаза, доводи до проблема који се крећу од проблема у комуникацији (ако су подразумеване маска подмреже и излаза погрешне) до дуплицираних IP адреса.

Коришћењем DHCP протокола за аутоматско конфигурисање информације о адреси показује се да корисник нема више потребе да информацију о IP адреси, потребној за конфигурисање TCP/IP протокола, добија од администратора. DHCP сервер обезбеђује све потребне конфигурационе информације о свим DHCP клијентима. Већина проблема у мрежи које је тешко пратити елиминишу се коришћењем DHCP протокола. DHCP користи четворофазни процес за конфигурисање DHCP клијената као што је приказано у табели 15.4 и на слици 15.9. Уколико станица има више мрежних интерфејса (адаптера) процес се обавља независно, преко сваког појединачног интерфејса. Сваком интерфејсу станице додељује се јединствена IP адреса. Комплетна DHCP комуни-

Фаза	Опис
IP захтев за изнајмљивање (*IP lease request*)	Клијент иницијализује ограничену верзију TCP/IP и шаље свима захтев за лоцирањем DHCP сервера и IP информације о адреси.
IP понуда за изнајмљивање (*IP lease offer*)	Сви DHCP сервери који имају на располагању важеће IP информације о адресирању шаљу понуду клијентима.
IP селекција изнајмљивања (*IP lease selection*)	Клијент бира IP адресну информацију на основу прве понуде коју добије и шаље свима поруку захтевајући да изнајми IP адресну информацију у понуди.
IP потврда о изнајмљивању (*IP lease acknowledgement*)	DHCP сервер који даје понуду одговара на поруку, и сви остали DHCP сервери повлаче своје понуде. IP адресне информације додељују се клијентима и шаљу се потврде. Клијент завршава иницијализацију и везивање на TCP/IP протокол. Једном када је процес аутоматског конфигурисања завршен, клијент може да користи TCP/IP услуге и оквиру комуникационе мреже и комуницира са другим IP станицама.

Табела 15.4 DHCP конфигурације

[1] *Gateway*
[2] *Domain Name System*



Слика 15.9 Размена DHCP порука између клијента и сервера

кација урађена је преко UDP портова 67 и 68. Већина DHCP порука се шаље свима. За DHCP клијенте који комуницирају са DHCP сервером на удаљеној мрежи рутери морају да обезбеде прослеђивање порука намењених свим. Фазе DHCP конфигурација приказане су у табели 15.4.

15.5 Интернет протокол верзије 6

Број рачунара који је повезан на Интернет расте изузетно великом брзином. У јулу 2005. године Интернет је користило скоро 350000000 станица [1]. Са IPv4 величином адресног поља могло би да се обезбеди 2^{32} различитих адреса, што је десет пута више него број станица које тренутно користи Интернет.

Разлози због којих је IPv4 адресни простор постао неодговарајући су следећи:

- Двослојна структура IP адреса (број мреже и број станице) је добро решење, али је и непотребно трошење адресног простора. Када се број мреже једном додели одређеној мрежи све станица на тој мрежи аутоматски добијају свој број (адресу). Адресни простор мреже може бити неискоришћен, али ако се посматра IP адресни простор онда када се искористи број мреже искоришћене су и све адресе за станице у оквиру те мреже;
- Адресни простор верзије IPv4 подељен је у мреже класа A, B и C различитих величина. Потребно је посебно анализирати адресни простор сваке од њих;
- Модел IP адресирања генерално захтева да јединствен мрежни број буде додељен свакој IP мрежи без обзира да ли јесте (или није) повезана на Интернет;
- Број рачунарских мрежа расте великом брзином. Многе организације без икакве потребе користе уместо једне више локалних рачунарских мрежа. Бежичне мреже добијају на значају;

[1] *ISC Internet Domain Survey,Jan 2004, http://www. isic.org*

- Проширивање области у којима се користе TCP/IP протоколи као што су POS [1] терминали или кабловска телевизија доводе до повећања потражње за IP адресама.

Видимо да су потребе за већим адресним простором довеле до потребе за новом верзијом IP протокола. Протокол IP је дуго у употреби а у међувремену су се појавили нови захтеви везани за конфигурацију адреса, рутирања и механизме подршке у управљању саобраћајем. Проблеми које IPv4 протокол није могао да разреши су и:

- у чворовима (рутерима) Интернета (нарочито у окосницам)а табеле рутирања су постале превелике да би се могле одржавати, без обзира на примену CIDR рутирања;
- апликације у реалном времену (које се све више користе) захтевају да постоје класе услуга и механизми приоритета. Код верзија IPv4 механизми који обезбеђују квалитет услуге нису били јасно дефинисани и веома су се мало користили.

Организација IETF [2] да би разрешила постојеће проблеме [3] 1992. године започела је процедуру за нову верзију Интернет протокола. До данас су објављени бројни документи међу којима су најважнији: RFC1752 [4], RFC2460 [5], RFC2373 [6]

Разлике између верзије IPv6 и верзије IPv4 су следеће:

- Дужина IPv6 је повећана на 40 бајтова (са 20 бајтова IPv4) и садржи две адресе од по 16 бајтова (изворишта и одредишта). Заглавље IPv4 (слика 15.1) садржи две адресе од по 4 бајта иза којих је 12 бајтова управљачких информација и обично опциони подаци. Проширење адресног простора је за фактор 2^{26}. Израчунато је да ово омогућава $6*10^{23}$ јединствених адреса по квадратном метру површине Земље [7]. Како год се адресе додељују овај адресни простор је довољно велики. Предвиђања су да ће бити довољан за следећих 30 година;
- Намера пројектаната верзије IPv6 је да се смањи време обраде пакета у рутерима смањивањем броја управљачких информација и измештањем опционих података из заглавља. Опције IPv6 смештене су у посебна заглавља која су постављена између заглавља IPv6 и заглавља транспортног слоја. Највећи број додатних заглавља рутери на путу који пакет прелази не анализирају;
- Повећана флексибилност адресирања: IPv6 укључује и концепт адресе један ка једном од групе [8]. Пакет се испоручује само једним путем. Перформансе рутирања један ка групи (мултикаст) унапређене су тако што је додат опсег поља за мултикаст адресе;
- Подршка у додели ресурса: IPv6 омогућава означавање пакета за различите брзине протока ако то пошиљалац тражи. На располагању су и додатне услуге у саобраћају када се преноси видео сигнал [9].

[1] *Point Of Sale*
[2] *Internet Engineering Task Force*
[3] *IP Address Exhaustion Problem*
[4] Сматра се прекретницом у дефинисању новог протокола означеног са IPng. (*Recommendation for the IP Next Generation*).
[5] Односи се на свеобухватну спецификацију протокола IPv6.
[6] Односи се на структуру адресирања IPv6.
[7] Литература [3]
[8] Еникаст *(Anycast)*
[9] *Real-time video*

Слика 15.10 Формат заглавља IPv6 пакета

15.6 Формат заглавља IP пакета верзије 6

Заглавље протокола IPv6 је поједностављено у односу на заглавље претходне верзије протокола IPv4. Формат заглавља IPv6 пакета предствљен је на слици 15.10.

Састоји се од следећих поља:

- Верзија (4 бита): верзија Интернет протокола, вредност је 6;
- DS/ECN [1] (8 битова): првих шест битова поља односи се на поље DS [2], а остала 2 бита резервисана су за обавештења о загушењу (ECN [3]);
- Ознака протока (20 битова): може користити станица да обележи оне пакете са којима рутери треба да поступају на посебан начин у оквиру мреже;
- Дужина података (16 битова): дужина оног дела IPv6 пакета који прати заглавље, у октетима. Другим речима, ово је комплетна дужина свих заглавља и јединице података протокола транспортног слоја (TPDU [4]);
- Следеће заглавље (8 битова): идентификује тип заглавља које прати IPv6 заглавље. Ово може бити неко од IPv6 додатних заглавља или заглавље вишег слоја, као што су заглавља TCP или UDP протокола. Поред оних вредности које су идентичне са верзијом IPv4 ово поље може да има следеће вредности:
  - 41- IPv6 заглавље,
  - 45 - међудоменски протокол за рутирање [5],
  - 58 - ICMP пакет протокола IPv6,
  - 46 - протокол за резервисање ресурса [6].

  Вредности за додатна заглавља су следеће:
  - 0 - заглавље опције корак по корак ,
  - 43 - заглавље IPv6 рутирања ,
  - 44 - заглавље IPv6 делова,

[1] У првим документима ово поље је означавано као „класе саобраћаја" (*Traffic Class*). Његова употреба је резервисано за почетне чворова и/или прослеђујуће рутере да би се направила разлика између различитих класа приоритета IPv6 пакета.
[2] *Differentiated services.*
[3] *Explicit congestion notification*
[4] TPDU (*Transport Protocol Data Unit*)
[5] *Interdomain Routing Protocol*
[6] *Resource Reservation Protocol*

- 50 - заглавље сигурности податка,
- 51 - заглавље о IPv6 аутентификацији,
- 59 - нема следећег заглавља [1],
- 60 - заглавље одредишних опција.

- Ограничење корака (8 битова): колико је још корака за овај пакет дозвољено. Ограничење корака поставља извориште на жељену максималну вредност. Декрементира се у сваком чвору који прослеђује пакет. Када вредност овог поља постане нула пакет се одбацује [2];
- Изворишна адреса (128 битова): адреса станице која формира пакет;
- Одредишна адреса (128 битова): адреса станице која који прима пакет. Ово не мора да буде крајња одредишна адреса ако је присутно заглавље рутирања;
- Контролна сума: протокол IPv6 не израчунава контролну суму зато што транспортни протоколи [3] то већ раде и зато што постоји опција за аутентификацију која може да обезбеди интегритет података.

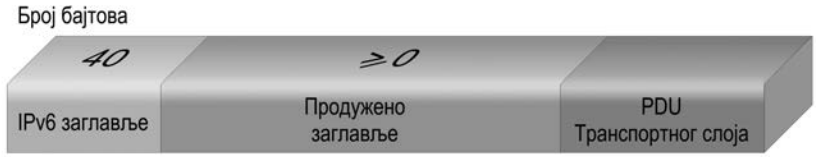
Иако је IPv6 заглавље дуже него обавезни део IPv4 заглавља (40 према 20 бајтова) број поља је мањи (8 према 12). То значи да ће рутери имати мање посла око обраде IPv6 заглавља, чиме је процес рутирања значајно убрзан.

Структура пакета IPv6

Пакет IPv6 има општу структуру приказану сликом 15.11. Сваки IPv6 пакет започиње основним заглављем. У многим случајевима ово ће бити и једино заглавље које је потребно да би се пакет испоручио одредишту. Некада је потребно пренети и још неке податке [4] одредишту или рутерима на путу до одредишта. Додатна заглавља се користе у ту сврху а постављају се одмах иза IPv6 заглавља. Свако додатно заглавље (осим оног које носи број 59) има своје поље [5] које означава који тип (врста) заглавља следи иза њега. Оваква структура омогућава уланчавање различитих додатних заглавља (проширења).

Дефинисана су следећа додатна заглавља (проширења):

- заглавље опције корак по корак [6]: дефинише специјалне опције које захтевају обраду у сваком рутеру,



Слика 15.11 Форма пакета IPv6

[1] *No Next Header*

[2] Ово је поједностављен поступак у односу на поступак који би требало да се уради са TTL пољем код IPv4. Рад са временским интервалима код верзије IPv4 није донео никакву предност. У ствари рутери са IPv4 протоколом третирали су TTL поље само као ограничење у броју корака.

[3] Код израчунавања контролне суме TCP и UDP користе псеудозаглавље у коме је садржана и IP адреса.

[4] Код верзије IPv4 тај задатак је реализован преко поља опција.

[5] *Next Header Field*

[6] *Hop-by-Hop Options Header.* Поред термина корак, користи се и термин скок.

- заглавље IPv6 рутирања[1]: обезбеђује проширење рутирања, слично изворишном рутирању у IPv4,
- заглавље IPv6 делова[2] (фрагмената) пакета: садржи информације о дељењу и поновном повезивању пакета,
- заглавље о IPv6 аутентификацији[3]: обезбеђује интегритет и аутентичност сваког пакета,
- заглавље о сигурности података[4]: обезбеђује заштиту пакета,
- заглавље одредишних опција[5]: садржи опционе информације које ће одредишни чвор анализирати.

У случају када се користи више додатних заглавља стандард IPv6 препоручује да се заглавља појављују следећим редоследом:

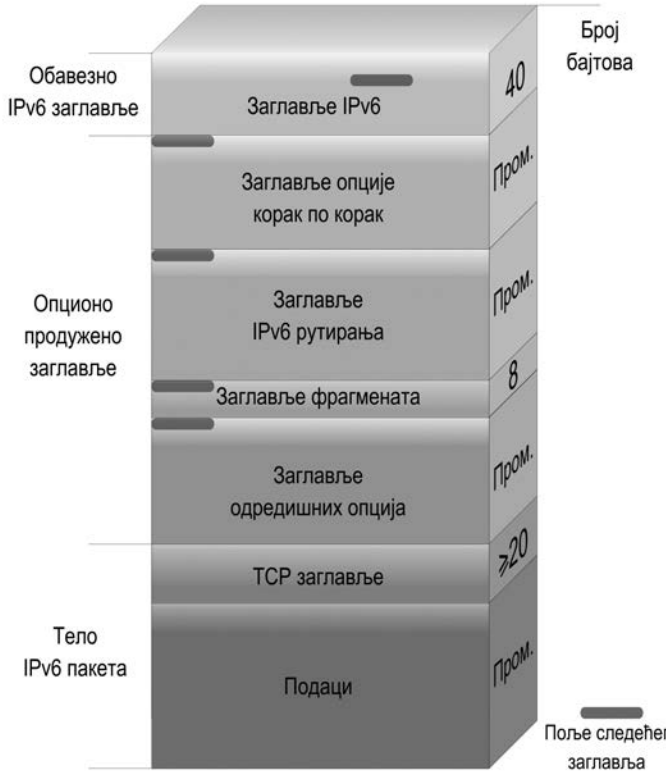
1. заглавље IPv6 (обавезно мора да буде прво),
2. заглавље опције корак по корак,
3. заглавље одредишних опција - за опције које ће бити обрађене од стране првог одредишта које се појављује у пољу IPv6. Одредишне адресе и накнадна одредишта која су набројана у заглављу рутирања,
4. заглавље IPv6 рутирања,
5. заглавље IPv6 делова,
6. заглавље аутентификације,
7. заглавље сигурности података,
8. заглавље одредишних опција - за опције које ће бити обрађене само у крајњем одредишту пакета.

Слика 15.12 приказује пример једног IPv6 пакета који укључује део сваког заглавља осим оних која се односе на сигурност. IPv6 заглавље и свако додатно (продужено) заглавље садрже поље „следеће заглавље". Ово поље идентификује тип следећег заглавља. Ако је следеће заглавље једно од продужених заглавља онда ово поље садржи идентификатор типа тог заглавља. У противном, ово поље садржи идентификатор протокола вишег слоја који користи IPv6 (обично протокол транспортног слоја). На слици 15.12 као протокол вишег слоја постављен је TCP протокол. Подаци (виших слојева) које носи IPv6 пакет садрже заглавља TCP протокола и податке апликације.

Ознака протока[6]

IPv6 стандард дефинише проток као низ пакета који се шаљу од одређеног извориштa ка одређеном одредишту[7] и за које изворište захтева од рутера да на посебан начин поступа. Проток је јединствено дефинисан тако што се комбинују изворишна и одредишна адреса са ознаком протока (20-битни број различит од нуле). Изворište додељује исту ознаку протока свим пакетима који су део једног протока.

[1] *Routing header*
[2] *Fragment header*
[3] *Authentication header*
[4] *Encapsulating Security Payload header*
[5] *Destination Option header*
[6] *Flow label*
[7] Уникаст (*unicast*) или мултикаст (*multicast*).



Слика 15.12 IPv6 пакет са продуженим заглављима

Посматрано са стране изворишта ток је низ пакета које је генерисала апликација изворишта а који захтева исту услугу транспортног слоја. Ток може да обухвати једну или више TCP веза. Једна апликација може да генерише један или више протокола. Пример два протока је мултимедијални састанак коме је додељен један проток за звук а други за слику. Сваки проток има различите захтеве код преноса података, кашњења или одступање у кашњењу.

Ако се погледа из угла рутера проток је низ пакета који има исте атрибуте који утичу на то како ће се рутер понашати према пакетима тог протока. Ту спада: одабрана путања, додељени ресурси, критеријуми за одбацивања, алгоритам заштите итд. Рутер може да се понаша другачије према пакетима који нису из истог протока. На пример: доделом различитог меморијског простора (бафера), придруживањем различитог приоритета код прослеђивања пакета или различитим захтевом за квалитетом услуге који се од мреже очекује .

Не постоји посебно значење било које ознаке протока. Уместо тога, да би се обезбедио специјални поступак проток се мора обележити на неки други начин. На пример, извориште може да затражи од рутера специјални поступак везан за обраду времена помоћу протокола за управљање, или времена преноса, тако што ће поставити одгова-

рајуће информације у једно од додатних заглавља пакета, као што је нпр. заглавље опције „корак по корак". Примери специјалног поступка су и захтеви за нестандардним квалитетом услуге или неком од услуга у реалном времену.

У начелу, сви кориснички захтеви за одређени проток могу бити дефинисани у додатним заглављима и укључени у сваки од пакета. Ако се жели оставити концепт протока потпуно отвореним за мноштво захтева резултат би могао бити превелико заглавље пакета. Друга могућност, која је усвојена код протокола IPv6, је тзв. ознака протока код које су захтеви протока дефинисани на самом почетку а јединствена ознака протока додељена је сваком протоку. У овом случају рутер мора да чува информације о захтевима сваког протока.

Следећа правила важе за ознаке протока:

1. станица или рутер који не подржавају „ознаку протока" морају да: када праве пакет поставе поље на нулту вредност; када преусмеравају пакет не мењају вредност поља и да га игноришу на пријему,
2. сви пакети који су направљени у истом изворишту морају имати исту: вредност поља „ознака протока", одредишну адресу, изворишну адресу, садржај заглавља опције „корак по корак" (ако постоји) и садржај заглавља „рутирање" (ако постоји). Рутер може да обрађује пакет тако што ће једноставно погледати ознаку протока у табели без испитивања осталих заглавља,
3. извориште додељује протоку „ознаку протока". Нова ознака протока мора бити изабрана као случајни број из опсега 1 до 2^{20} -1. Услов је да извориште не може да додели ознаку новом протоку ако се она користи за проток који је још активан. Вредност нула указује да се ни једна од ознака протока не користи.

Адресирање у протоколу IPv6

Код протокола IPv6 поље додељено адресама је дужине по 128 бита. Адресе се додељују сваком од интерфејса чвора [1] а не самом чвору. Сваки интерфејс може да има више јединствених уникаст адреса. Било која од уникаст адреса додељена интерфејсу чвора може се искористити да јединствено идентификује тај чвор. Комбинација адреса велике дужине и више адреса додељених интерфејсу омогућава ефикасније рутирање у поређењу са верзијом IPv4. Код IPv4 протокола адреса није направљена тако да потпомаже процес рутирања. Због тога рутер је морао да води рачуна о великим табелама путања (рутирања). Дуже Интернет адресе дозвољавају повезивање већег броја адреса према: хијерархијама рачунарских мрежа, добављачима Интернет услуга преко којих се приступа Интернету, географској локацији, предузећу итд. Такав број би требало да учини да табеле рутирања буду мање, а преглед табела бржи. Претплатнику је омогућено да приступа Интернету преко више добављача Интернет услуга а да за то користи исти интерфејс.

IPv6 дозвољава три типа адреса:

- уникаст [2] адреса је идентификатор једног интерфејса. Пакет послат уникаст адресом испоручује се интерфејсу који је одређен том адресом;

[1] Код протокола IPv6 термин чвор се односи и на рутер и на крајњу станицу. Односно на сваки уређај код кога је имплементиран IPv6 протокол.

[2] *Unicast*

- еникаст[1] адреса је идентификатор за више интерфејса који припадају различитим чворовима. Пакет послат еникаст адресом испоручује се неком од интерфејса који је одређен том адресом (на пример најближем, гледајући по протоколу за рутирање),
- мултикаст[2] адреса је идентификатор за групу интерфејса који припадају различитим чворовима. Пакет послат мултикаст адресом испоручује се свим интерфејсима који су одређени том адресом.

[1] *Anycast*
[2] *Multicast*

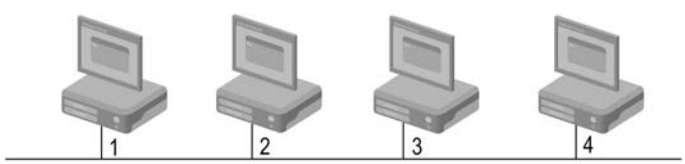
16. Рутирање

Уколико су одредишна и изворишна станица директно везане (тачка-тачка веза) или се налазе на некој од рачунарских мрежа за дељење заједничког медијума (нпр. IEEE802.3) онда се IP пакет шаље директно ка одредишној станици. IP пакет се укалупљује у IEEE802.3 рам и шаље ка другој станици користећи физичке (MAC) адресе (слика 16.1). Уколико се изворишна и одредишна станица не налазе на истој локалној рачунарској мрежи (или подмрежи) онда је испорука IP пакета индиректна. Прво се IP пакет шаље ка подразумеваном [1] рутеру и њему препушта даље усмеравање или испорука одредишту (слика 16.2). Изворишни рачунар укалупљује IP пакет у одговарајући рам (нпр. IEEE802.3) у коме је као физичка (MAC) адреса одредишта постављена физичка адреса рутера. Рутер преусмерава пакете до одредишне станице или другог рутера. Разлика између станице са више мрежних интерфејса и рутера је у томе што станица не преусмерава пакете са једног свог интерфејса на други а рутер их преусмерава.

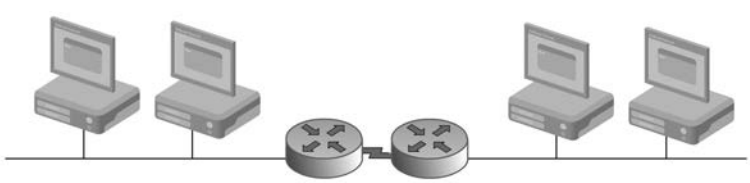
Уопштено посматрајући IP протокол може да прими пакете:

- од TCP, UDP, ICMP и IGMP протокола (тј. локално генерисане пакете) да би их послао даље,
- од мрежног интерфејса да би их преусмерио.

IP слој у својој меморији садржи табелу рутирања која се претражује сваки пут када слој добије пакет за слање. Када станица добије IP пакет од мрежног интерфејса проверава да ли је одредишна IP адреса његова адреса или је реч о пакету који је упућен свим станицама на мрежи [2]. Уколико је тако онда се пакет испоручује модулу протокола који је специфициран у пољу за протокол у заглављу IP пакета. Уколико пакет није намењен том IP слоју преусмерава се даље под условом да је



Слика 16.1 Директна испорука пакета



Слика 16.2 Индиректна испорука пакета

[1] *Default*
[2] *Broadcast*

станица конфигурисана као рутер; у супротном пакет се одбацује [1].

Сваки запис у табели рутирања садржи информације о:

- одредишној IP адреси која може да буде или потпуна адреса рачунара (крајње станице) или адреса мреже;
- IP адреси следећег рутера [2] или IP адреси мреже за коју је директно везана. Под следећим рутером сматра се онај рутер са којим се станица може директно повезати и коме ће послати пакете за даље прослеђивање. Следећи рутер није крајње одредиште већ међустаница која прихвата пакете које је крајња станица послала и преусмерава их ка крајњем одредишту;
- ознакама које указују да ли је одредишна IP адреса адреса мреже или адреса станице. Друга ознака указује да ли је следећи рутер заиста следећи рутер или директно повезан интерфејс;
- мрежном интерфејсу преко кога ће пакет бити послат.

IP рутирање одвија се корак по корак [3]. Као што се види из табеле рутирања (табела 16.1) IP целина не зна комплетну путању (руту) ка било ком одредишту, осим оних одредишта која су директно везана за изворишну станицу. Све што IP протокол обезбеђује је адреса следећег рутера [4] ка коме се пакет шаље. Претпоставља се да је следећи рутер заиста ближи одредишту од предајне станице и да је следећи рутер директно везан за одредишну станицу. IP рутирање се састоји од следећих активности:

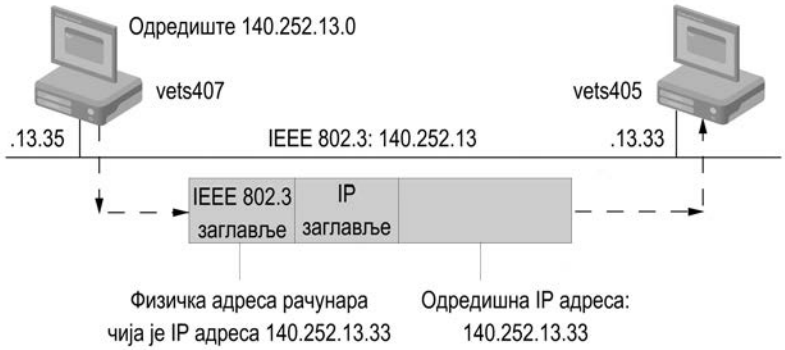
- тражења записа у табели рутирања која одговара комплетној одредишној IP адреси (и адреси мреже и адреси станице). Уколико се пронађе запис пакет се шаље или ка следећем рутеру или ка директно везаном интерфејсу (у зависности од ознаке);
- тражења записа у табели рутирања која одговара само мрежном делу адресе одредишне станице. Уколико се пронађе запис пакет се шаље или ка следећем рутеру или ка директно везаном интерфејсу (у зависности од ознаке). За све станице одредишне мреже то се може обезбедити преко једног записа у табели рутирања. Сви записи о станицама из локалне рачунарске мреже (нпр. IEEE802.3) реализовани су на овај начин;
- тражења записа у табели рутирања означеног као „подразумевани". Уколико се пронађе шаље се пакет ка рутеру означеном као следећи.

Уколико се не добије резултат ни једног од поменутих претраживања сматра се да пакет не може да се испоручи. Ако је пакет формиран на тој станици апликацији се шаље порука: „мрежа је недоступна" или „станица је недоступна".

Пример 16.1: Станица vets407 има IP пакет који треба да пошаље станици vets405. Обе станице су на истој локалној рачунарској мрежи типа IEEE802.3.

На слици 16.3 представљена је испорука пакета. Изворишни рачунар vets407: када IP прими пакет од једног од виших слојева он претражује табеле рутирања и проналази да се одредишна адреса 140.252.13.33 налази на истој мрежи (IEEE802.3

[1] *Silent discard*
[2] *Next hope router*
[3] *Hop to hop*
[4] *Next hope router*



Слика 16.3 Испорука пакета рачунара vets407 рачунару vets405

140.252.13.0). Одговарајућа адреса мреже проналази се у табели рутирања. Пакет се прослеђује софтверском модулу (Етернет драјвер) и затим шаље као IEEE802.3 рам ка станици vets405. Одредишна IP адреса је IP адреса станице vets405. Одредишна 48-битна физичка [1] адреса је адреса мрежног интерфејса станице vets405. Ова адреса добија се коришћењем протокола ARP [2].

16.1 Процес рутирања

Рутирање је процес који се одвија на IP слоју и састоји се од одређивања најбоље путање и преусмеравања пакета. Одређивање најбоље путање своди се на преглед табеле рутирања, и одређивања следећег рутера на путањи пакета као и сопственог мрежног интерфејса преко којег ће се извршти испорука.

IP протокол на свакој станици аутоматски креира запис у табели рутирања на основу IP адреса. Записи описују путању за саобраћај којој је одредиште друга станица на директно прикљученој мрежи, усмерено и ограничено слање свим станицама, групи станица, локална петља и сопствена IP адреса.

У табели рутирања могу постојати и додатни записи који представљају путање до појединих удаљених мрежа. Записи могу бити специфични за поједине удаљене мреже или уопштени; најчешће један (или више) записа представљају упутство за усмеравање пакета за све остале не-директно прикључене мреже. Додатни записи у табели рутирања могу се унети ручно или их динамички уноси демон [3] (услуга) за рутирање реализована као софтверски процес покренут на рутеру. Услуга рутирања користи протоколе за рутирање да би са осталим рутерима разменила информације о тренутној топологији мреже, и одговарајући алгоритам да би на основу тих информација динамички изменила табелу рутирања.

Информације које се налазе у табели рутирања утичу на све одлуке које о рутирању доноси алгоритам за рутирање. Пример табеле рутирања дат је у табели 16.1.

[1] IEEE802.3, Етернет

[2] *Adress Resolution Protocol.* Протокол који проналази (разрешава) физичку (MAC) адресу одредишне станице за коју је позната IP адреса.

[3] Термин демон користи се за процесе који су невидљиви, раде у позадини и воде рачуна о раду целог система. *Deamon* (дух, демон) нормално се покреће при подизању система. Користи се и израз услуга или сервис.

Одредишна мрежа	Маска	Међумрежни пролаз	Мрежни интерфејс	Удаљеност	Намена
0.0.0.0	0.0.0.0	157.55.16.1	157.55.27.90	1	Подразумевана путања
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1	Затворена петља
157.55.16.0	255.255.240.0	157.55.27.90	157.55.27.90	1	Директно прикључена мрежа
157.55.27.90	255.255.255.255	127.0.0.1	127.0.0.1	1	Локална станица
157.55.255.255	255.255.255.255	157.55.27.90	157.55.27.90	1	Слање свима на мрежи
224.0.0.0	224.0.0.0	157.55.27.90	157.55.27.90	1	Слање појединим станицама на мрежи
255.255.255.255	255.255.255.255	157.55.27.90	157.55.27.90	1	Ограничено слање свима

Табела 16.1 Табела рутирања

Намена појединих поља је следећа:

- подразумевана путања[1] - у овој табели је 0.0.0.0 са маском 0.0.0.0. Било који пакет који је послат на подразумевану путању, тј. онај за који није пронађена бољa путања у табели, биће преусмерен на међумрежни пролаз;
- затворена петља[2] - сви пакети који се пошаљу на 127.x.y.z преусмераваују се на 127.0.0.1;
- директно прикључена мрежа[3] - пакети који су намењени за мрежу на којој је станица не преусмеравају се на рутер;
- локална станица[4] - адреса локалног рачунара. Сви пакети који иду на ову адресу преусмераваују се на затворену петљу;
- пакети „слање свима на мрежи"[5] шаљу се свим рачунарима на мрежи;
- слање појединим станицама на мрежи[6] користи се за слање порука одређеним корисницима;
- ограничено слање свима[7] - пакети намењени свима шаљу се у складу са овом путањом преко 157.55.27.90;
- метрика је приказана целобројном вредношћу у интервалу од 1 до 9999 и може представљати број прелазака преко рутера до одредишта, брзину везе, поузданост или неко друго својство.
  Уколико до истог одредишта постоји више путања бира се она са најмањом метриком.

[1] *Default route*
[2] *Loopback network*
[3] *Directly Attached Network*
[4] *Local host*
[5] *Network Broadcast*
[6] *Multicast*
[7] *Limited Broadcast*

Записи у табели рутирања су:

- адреса одредишта, станице или мреже [1],
- адреса рутера [2] ако није подешен користи се знак " * ",
- маска подмреже за одредишта [3],
- број прелазака[4] преко рутера до одредишта [5],
- број референци [6] на путању,
- број колико је пута употребљена путања [7],
- мрежни интерфејс на који се шаљу пакети за ову путању [8].

Могуће опције[9]:

- *U* - путања је успостављена,
- *H* - одредиште је крајња станица,
- *G* - користи се међумрежни пролаз [10],
- *!* - путања је у прекиду.

Сличне табеле рутирања праве и рутери са основном разликом што такве табеле имају много већи број записа - за сваку мрежу на коју су повезани.

16.2 Протоколи за рутирање и аутономни системи

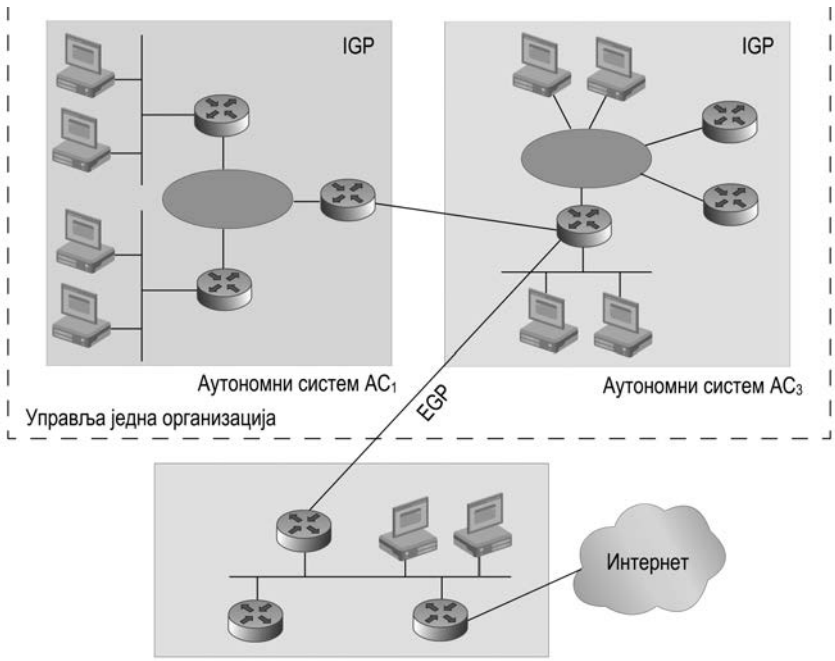
Протоколи за рутирање омогућавају да се динамички прикупљају и одржавају информације у табелама рутирања. Како се мења топологија мреже табеле рутирања се иновирају.

Аутономни систем представља целину која се састоји од међусобно повезаних мрежа. Аутономним системом може да управља једна организација и једна организација може да има више аутономних система. Као што се на слици 16.4 види аутономни системи могу се међусобно повезивати са другим приватним или јавним рачунарским мрежама.

Протоколи за рутирање деле се на:

- унутрашње протоколе за рутирање IGP [11] који омогућавају размену информација у оквиру аутономног система. Пример IGP протокола су OSPF [12] и RIP [13];
- спољашње протоколе за рутирање EGP [14] који омогућавају размену здружених информација између аутономних система. Пример EGP протокола је BGP [15].

[1] *Destination*
[2] *Gateway*
[3] *Genmask*
[4] *Metric*
[5] *Hops*
[6] *Ref*
[7] *Use*
[8] *Iface*
[9] *Flags*
[10] *Gateway*
[11] *Interior Gateway Protocol*
[12] *Open Shortest Path First*
[13] *Routing Information Protocol*
[14] *Exterior Gateway Protocols*
[15] *Border Gateway Protocol*



Слика 16.4 Међусобно повезивање аутономних система

16.3 Алгоритми за рутирање

Алгоритми за рутирање користе се за формирање и одржавање табеле рутирања. Постоје два основна метода која се користе за прављење табела рутирања:

- статичко рутирање,
- динамичко рутирање.

Табела рутирања се код статичког рутирања формира обично када се конфигурише мрежни интерфејс (код директно повезаних интерфејса) користећи *route* команду или користећи ICMP *redirect* (када је одабрана погрешна подразумевана путања). Овај начин је добар ако је мрежа мала, ако постоји само једна веза са осталим мрежама и ако не постоје редундантне путање које би могле да се користе ако би главна путања отказала. Уколико било који од поменутих услова није испуњен уобичајено се користе динамички протоколи за рутирање.

Динамичко рутирање ослања се на динамичке алгоритме за рутирање који аутоматски откривају и одржавају своје податке о путањама кроз мрежу. Аутоматско откривање може да користи различите динамичке протоколе за рутирање. Разлика између ових протокола је у начину на који се откривају и прерачунавају путање ка одредишним мрежама. Могу се класификовати у три категорије:

- протокол вектора удаљености [1],
- протокол стања везе [2],
- хибридни протокол.

[1] *Distance vector protocol*
[2] *Link state protocol*

16.4 Динамичко рутирање

Када рутер размењује информације са суседним рутером обавештавајући га са којим је мрежама повезан реч је о динамичком рутирању. Рутер мора да комуницира користећи протоколе за рутирање. У систему као што је Интернет користе се различити протоколи за рутирање. Интернет је организован као скуп аутономних система (слика 16.4). На пример NSFNET, кичма Интернета, чини један аутономни систем пошто су сви рутери под надзором једне организације. Сваки аутономни систем може да одабере сопствени протокол за рутирање за комуникацију између рутера аутономног система (унутрашњи протоколи за рутирање).

Протокол RIP[1] је дуго времена био најпопуларнији протокол за рутирарање. Данас га је увелико заменио OSPF протокол[2]. Протокол OSPF нуди неколико значајних предности у односу на RIP протокол, укључујући способност да ради у много већим мрежама, а да измене у табелама рутирања имају много мањи утицај на мрежни саобраћај. Главна разлика између протокола за рутирање је у начину или алгоритму којим рутери прикупљају ажурне информације о рутирању. На пример, RIP протокол користи алгоритам вектора раздаљине[3], који мери само број скокова (максимално 16) до удаљеног рутера, док OSPF протокол користи много напреднији алгоритам стања везе[4], који врши избор између алтернативних путања не само на основу броја скокова, већ и кашњења, капацитета, протока и поузданости линија које повезују рутере. И што је можда још важније, за одржавање ажурних табела рутирања OSPF протокол захтева много мањи проток.

Рутирање вектором раздаљине захтева да сваки рутер одржава табелу са бројем скокова, који се понекад назива и трошак линка[5], између себе и сваког другог доступног рутера. Ове раздаљине се израчунавају коришћењем садржаја табела рутирања суседних рутера, и додавањем раздаљине од себе до рутера од кога је преузета табела са информацијама. Табеле рутирања морају у свако доба бити ажурне да би приказале сваку промену у мрежи.

Кључни проблем са вектором раздаљине је што сви рутери не сазнају одмах да је дошло до промене на мрежи (на пример прекид у раду рутера или неке од веза). Узрок је кашњење до кога долази јер сваки рутер мора да прерачуна сопствене табеле рутирања пре него што их проследи суседним рутерима. Ово кашњење, тј. прелазак у стабилно стање после неких промена назива се спора конвергенција.

Протоколи стања везе, као што је OSPF протокол , у могућности су да превазиђу спору конвергенцију и понуде још нека унапређења перформанси. Једна од важних разлика између ове две врсте протокола је што протоколи вектора раздаљине могу да користе само информације од рутера са којима су непосредно повезани, док протоколи рутирања стања везе користе информације о мрежи примљене од свих рутера у датој мрежи.

[1] *Routing Information Protocol*
[2] *Open Shortest Path First*
[3] *Distance vector*
[4] *Link state*
[5] *Link cost*

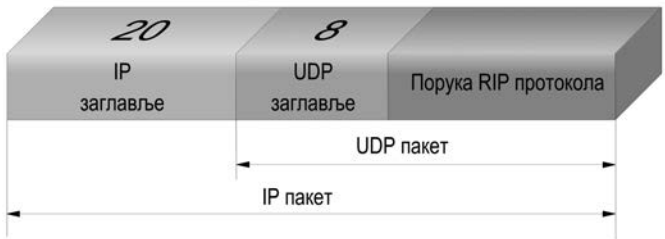
	Вектор раздаљине	Стање везе
Примери	RIPv1, RIPv2, IGRP, EIGRP	OSPF, NLSP, ISIS
Ажурирање	Обично се цела табела рутирања размењује са суседима сваких 30-90s. (RIPv1, RIPv2, IGRP)	Ажуриране путање шаљу се само по потреби.
Обрада	Када прими табелу од суседа сваки рутер прерачунава све раздаљине.	Пакети стања везе одмах се обрађују. Информације садржане у њима користе се за ажурирање погледа на мрежу.
Искоришћеност опсега	Већа	Мања
Искоришћеност CPU[1] и RAM[2]	Мања	Већа
Метрика	RIP: број скокова. IGRP, EIGRP: опсег, кашњење, оптерећење, поузданост, максимална јединица преноса (MTU[3])	Трошак, алгоритам најкраћег пута.
Предности	Мали захтеви за меморијом и процесорском снагом. Једноставнији за имплементацију.	Нема размене табела рутирања. Нема ограничења броја скокова. Опсег везе и кашњење узимају се у обзир. Брза конвергенција. Подршка за VLSM и CIDR. Хијерархијски поглед на мрежу боље скалира у великим међумрежама.
Мане	Не узимају у обзир пропусни опсег када доносе одлуку о рутирању. Спора конвергенција Ограничење броја скокова на 15. (RIPv1, RIPv2) Размена комплетних табела рутирања је неефикасна Не подржавају VLSM[4] и CIDR[5] (RIPv1) Нема хијерархије мреже, слабо скалирање у великим мрежама.	Већи захтеви за обрадом и меморијским простором. Сложенији за реализацију.

Табела 16.2 Разлика између протокола вектора раздаљине (RIP) и стања везе (OSPF)

Протоколи за рутирање стања везе могу да имају комплетнији и ажурнији поглед на целу мрежу него протоколи за рутирање вектора раздаљине, придржавајући се следећих основних процедура:

- рутери стања везе користе специјализоване пакете познате као пакети стања везе (LSP[6]) за одређивање назива и раздаљине до суседних рутера и повезаних мрежа;
- све информације које се о мрежи науче шаљу се свим познатим рутерима, а не само суседним, коришћењем LSP пакета;

[1] *Central Processsing Unit*
[2] *Random Access Memory*
[3] *Maximum Transmission Unit.* Када су две станице у истој мрежи максимална јединица преноса (MTU) дефинисана је у тој мрежи. Када станице комуницирају преко различитих мрежа сваки линк може да има различиту максималну јединицу преноса. Важна величина је и максимална јединици преноса на комплетном путу (*Path* MTU).
[4] *Variable Length Subnetting Mask* (подмреже са маскама променљивих дужина је објашњено у 15. поглављу).
[5] *Classless Interdomain Routing* (рутирање са груписањем IP адреса које нису засноване на класама A, B,..).
[6] *Link state packets*



Слика 16.5 RIP порука је укалупљена у UDP пакет

- сваки рутер је одговоран за обраду информација садржаних у свим најскорије примљеним LSP пакетима и на тај начин прављење ажурног погледа на стање целе мреже. Из овог комплетног сагледавања протокол за рутирање стања везе је у могућности да одреди најбољу путању до одредишне мреже, као и алтернативне путање са различитим трошковима;
- новопримљени LSP пакети одмах се прослеђују даље, за разлику од протокола вектора раздаљине код којих се прво мора прерачунати сопствена табела рутирања пре него што се ажуриране информације проследе суседним рутерима. Брзо прослеђивање LSP пакета омогућава бржу конвергенцију у случају прекида везе или додавања нових чворова.

Званична спецификација за RIP протокол је документ RFC1058 али је овај документ написан много касније него што је протокол почео да се имплементира. Порука RIP протокола преноси се UDP пакетом као што је то приказано на слици 16.5.

Протокол OSPF пројектован је као унутрашњи протокол за рутирање, алтернатива RIP протоколу. Превазишао је сва ограничења RIP протокола. Верзија 2 OSPF протокола описана је у документу RFC1247. Протокол OSPF различит је од RIP (и многих других протокола) по томе што користи директно IP пакет. То значи не користи UDP или TCP протоколе. Протокол OSPF има своју сопствену вредност за поље протокола [1]. Набројаћемо још неке од предности OSPF у односу на RIP протокол:

- OSPF протокол може да прорачуна посебан скуп путања за сваки тип услуге. То значи да за свако одредиште може да постоји неколико записа у табели рутирања за сваку од врста услуга;
- Интерфејсу се додељује цена. Она се може доделити на основу пропусне моћи система, времена које порука пређе до одредишта и натраг [2], поузданости и сл. Различите цене могу да се доделе свакој услузи;
- Када постоји више путања до одредишта са истом ценом онда OSPF може да расподели саобраћај између рутера. Ово се назива расподела оптерећења [3];
- OSPF протокол подржава подмреже. Маска подмреже је придружена свакој путањи. Путања до станице (хоста) оглашава се поруком у којој су постављене све јединице у пољу за маску подмреже. Подразумевана путања оглашава се као IP адреса 0.0.0.0 са маском подмреже постављеном на све нуле;

[1] *Protocol field*
[2] *Round trip delay*
[3] *Load balansing*

- Везама тачка-тачка између рутера нису потребне IP адресе за сваки од крајева. Ово се назива ненумерисана мрежа. На овај начин могу се приштедети IP адресе;
- Може се користити текстуална или MD5 аутентификација;
- OSPF може да шаље поруке појединим станицама [1] уместо да их шаље свим станицама [2] и на тај начин смањи саобраћај на мрежи.

16.5 Протокол за рутирање између аутономних система

Намена протокол за рутирање између аутономних система (BGP [3]) је да обезбеди комуникацију између рутера у различитим аутономним системима. Протокол BGP је замена за протокол EGP [4] који се користио у ARPANET мрежи. Документ RFC1268 описује коришћење протокола BGP на Интернету. Систем са BGP протоколом размењује информације о мрежи са другим системима који користе BGP протокол. Ове информације омогућавају формирање графа повезаности аутономног система. Петље у путањама могу се уклонити и може се применити нека од метода одабира путања.

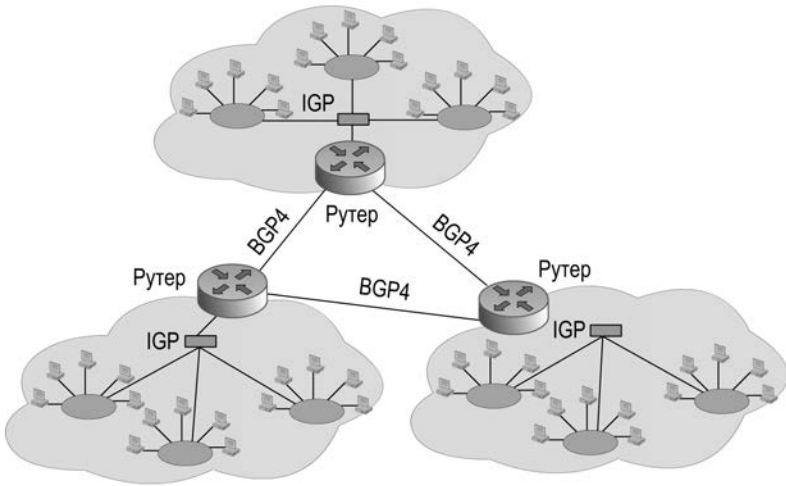
У аутономном систему пренос IP пакета може се посматрати као локални саобраћај или пролазак (транзит). Локални саобраћај може да буде изворишни или одредишни (започиње или се завршава у аутономном систему). Ако је саобраћај локални онда је или изворишна IP адреса или одредишна IP адреса адреса станице у том аутономном систему. Све остало сматра се пролазећим (транзитним) саобраћајем. Најважнији допринос употреби BGP је у смањењу транзитног саобраћаја. Аутономни системи могу се категоризовати на следећи начин:

- аутономни систем који има само једну везу са другим аутономним системима [5] и може да преноси само локални саобраћај;
- аутономни систем повезан је са више од једне везе са другим аутономним системима [6] али не прихвата транзитни саобраћај;
- транзитни аутономни систем повезан је са више аутономних система и може уз одређена ограничења да прихвата и локални и транзитни саобраћај.

Свеукупна топологија Интернета је таква да се састоји од све три врсте аутономних система [7].

Протокол BGP разликује се од RIP и OSPF протокола по томе што BGP користи TCP протокол. Стриктно говорећи, BGP је протокол вектора путање [8] што значи да рутери који користе BGP протокол (BGP рутери) међусобно размењују информације о путањи. Аутономни систем одређен је 16-битним бројем. Правила рутирања код BGP протокола могу се врло прецизно поставити изменом BGP атрибута и подешавањем филтрирања рута. Слика 16.6 представља једноставан дијаграм који илуструје овај процес.

[1] *Multicasting*
[2] *Broadcasting*
[3] *Border Gateway Protocol*
[4] *Exterior Gateway Protocol*
[5] *Stub*
[6] *Multihomed*
[7] *Stub, multihomed и transit.*
[8] *Path vector protocol*



Слика 16.6 Аутономни системи и екстерни протоколи за рутирање

Пошто BGP протокол користи TCP протокол за испоруку информација о векторима путања сматра се поузданим протоколом. Протокол BGP користи принцип суседних аутономних система. Када се открије суседни аутономни систем специјалне поруке [1] се непрестано размењују да би се осигурала видљивост оглашених путања. На тај начин BGP рутери знају да је дошло до отказа суседног рутера и да су информације о вези постале неважеће. Сваки BGP рутер у аутономном систему конфигурише се да оглашава скуп мрежа унутар тог аутономног система, и да дефинише са којим ће се рутерима на суседним аутономним системима размењивати информације о векторима путања. Различита тежина може се доделити појединим путањама тако да се једна путања учини атрактивнијом од друге.

У случају аутономних система статичко рутирање може бити пожељније од динамичког. Пошто се информације о рутирању не деле преко веза које повезују различите аутономне системе, знатно се смањује опасност да један лоше подешен рутер из другог аутономног система негативно утиче на рутере датог аутономног система.

16.6 Бескласно рутирање између домена

Бескласно рутирање између домена (CIDR [2]) је начин да се спречи превелик раст табела рутирања. Описан је у документу RFC1518. Основни концепт рутирања између домена је да додели више IP адреса тако да се као последица смањи број записа у табелама рутирања. На пример, уколико је једној локацији додељено 16 адреса класе C али се њих 16 може здружити тако да се на свих 16 може указати преко једног записа у табели рутирања на Интернету. Такође, уколико је осам различитих локација повезано са истим Интернет понуђачем услуга преко исте тачке за повезивање и ако је за тих осам локација додељено осам различитих IP адреса које се мо-

[1] *Keepalive* - порука којом указује да је у радном стању
[2] *Classless Interdomain Routing*

гу здружити (сумирати), онда је само један запис у табели рутирања довољан за свих осам локација. Карактеристике које су потребне да би до здруживања могло да дође су:

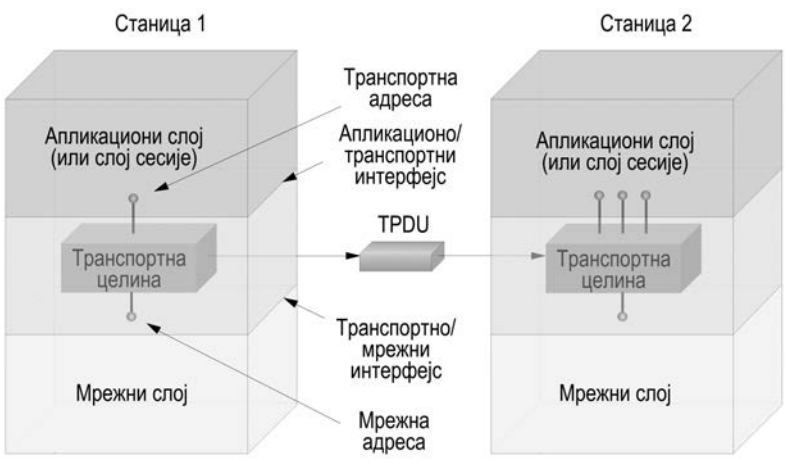
- више IP адреса које треба здружити треба да имају у својој адреси исте битове највеће тежине;
- табеле рутирања и алгоритми за рутирања треба да се прошире за одлучивање о путањи и на 32-битну IP адресу и на 32-битну маску;
- протокол за рутирање који се користи мора се проширити да поред 32-битне адресе преноси и 32-битну маску. Протоколи OSPF и RIP-2 могу да преносе и 32-битну маску.

17. Транспортни слој TCP/IP референтног модела

Транспортни слој је кључна карика у целокупном концепту архитектуре протокола. Протоколи нижих слојева су лакши за разумевање и мање сложени од транспортног протокола. Транспортни протокол обезбеђује услугу преноса података између крајњих корисника (с краја на крај). Свака апликација се може пројектовати тако да користи директно услугу транспортног слоја без посредства слоја сесије и презентације. У овом поглављу анализираћемо детаљно транспортни слој TCP/IP референтног модела.

Најважнији циљ транспортног слоја је да обезбеди ефикасну, поуздану и економичну услугу својим корисницима, обично процесима на апликационом слоју[1]. Да би достигао овај циљ траснпортни слој користи услуге које му обезбеђује мрежни слој. Хардвер и/или софтвер у оквиру транспортног слоја који обавља те задатке назива се транспортна целина. Транспортна целина може бити реализована као део језгра оперативног система, као посебан кориснички процес у библиотеци повезаној са мрежном апликацијом или на мрежној интерфејсној картици. Повезаност (логичка) мрежног, транспортног и апликационог слоја приказана је на слици 17.1.

Услуга коју пружа транспортни слој веома је слична услузи коју пружа мрежни слој. Поставља се питање ако је то тако зашто постоје и користе се два различита слоја? Зашто није довољан само један слој[2]. Разлог је једноставан. Софтвер који реализује услуге транспортног слоја налази се на рачунару самог корисника, док се софтвер који реализује услуге мрежног слоја најчешће налази на рутерима који су код рачунарских мрежа ширих географских подручја део опреме оператера. Тиме је из-



Слика 17.1 Веза мрежног, транспортног и виших слојева (сесија или слој апликације)

[1] Или слоју сесије ако је реч о OSI референтном моделу.
[2] WAN - *Wide Area Network*

над мрежног слоја постављен још један слој - транспортни који, може да побољша квалитет мрежног сервиса на месту и према захтеву крајњег корисника (апликације).

Као што је у 3. поглављу истакнуто TCP и UDP су доминантни протоколи транспортног слоја. Оба користе IP протокол на мрежном слоју. TCP је протокол са успоставом везе и на тај начин обезбеђује поуздан пренос без обзира што сервис који користи IP није поуздан. Протокол UDP је без успоставе везе и, за разлику од TCP протокола, нема никаквих гаранција да су подаци стигли на одредиште. Апликације као што су систем имена домена (DNS [1]), или протокол за надзор и управљање (SNMP [2]) користе UDP протокол.

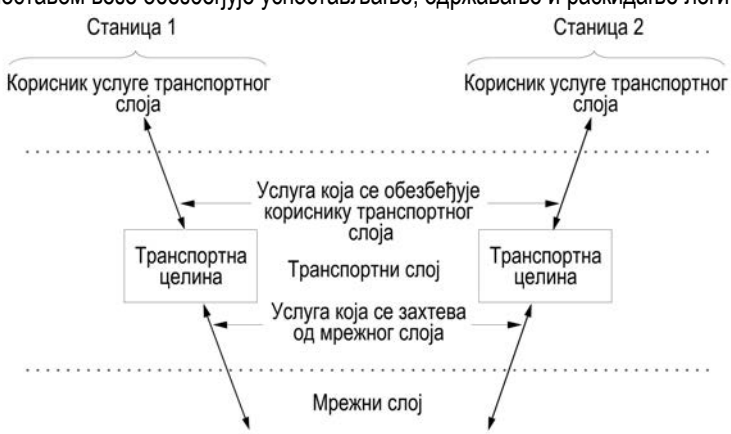
17.1 Услуге које пружа транспортни слој

Услуге које обезбеђује транспортни протокол је пренос података с краја на крај на такав начин да се штите корисници од детаља везаних за комуникациони систем који користе (слика 17.2). Категорије услуга које се користе у описивању услуга транспортног слоја су:

- тип услуге,
- степен услуге,
- пренос података,
- кориснички интерфејси,
- надзор везе,
- убрзана испорука података,
- извештај о статусу,
- безбедност.

Тип услуге

Могућа су два основна типа услуге: са успоставом везе [3] и без успоставе везе [4]. Услуга са успоставом везе обезбеђује успостављање, одржавање и раскидање логичке везе



Слика 17.2 Транспортна целина и њено место у односу на суседне слојеве

[1] *Domain Name System*
[2] *Simple Network Management Protocol*
[3] *Connection oriented*
[4] *Connectionless*

између транспортних корисника. Оваква услуга генерално је поуздана и садржи механизме као што су: контрола тока, контрола грешке и испорука у правилном редоследу.

Степен услуге

Протокол транспортне целине дозвољава кориснику да специфицира степен услуге или квалитет услуге који очекује. Транспортна целина ће покушати да оптимизира употребу мреже и везе. Примери услуга које се могу захтевати су:

- прихватљив ниво погрешних и изгубљених података,
- пожељно и максимално прихватљиво кашњење,
- пожељна и минимална пропусност[1],
- нивои приоритета.

Јасно је да су могућности транспортне целине да обезбеди захтеване услуге ограничене могућностима услуга које нуде нижи слојеви. Навешћемо неке од апликација које захтевају специфични степен услуге:

- протокол за пренос датотека (FTP[2]) може да захтева велику пропусну моћ система и високу поузданост да би спречио поновно слање,
- трансакциони протоколи (упити база података) могу да захтевају мала кашњења,
- електронска пошта може да захтева више нивоа приоритета.

Постоје четири категорије транспортног протокола:

- поуздан протокол са успоставом везе,
- мање поуздан протокол без успоставе везе,
- протокол за пренос говора који захтева благовремени пренос и пренос исправног редоследа,
- протокол за пренос у реалном времену који захтева високу поузданост и минимална кашњења.

Пренос података

Намена транспортног протокола је да обезбеди пренос података између транспортних целина. Подаци и управљачке информације могу се преносити истим или различитим каналом. Могући је: потпуни дуплекс, полудуплекс и симплекс начин рада.

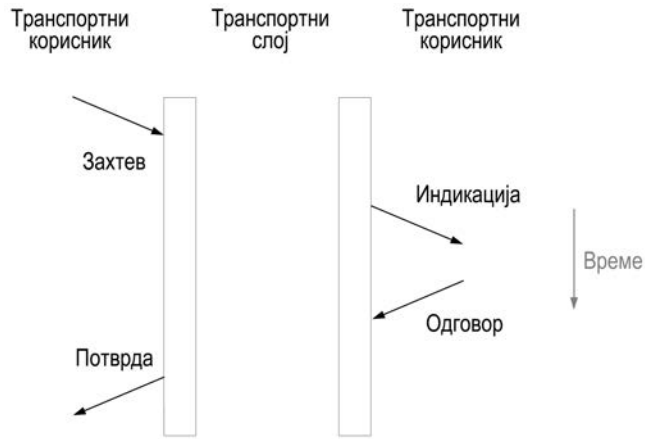
Кориснички интерфејс

Прецизно дефинисан кориснички интерфејс нема потребе да буде стандардизован. Боље је да се у реализацији прилагоди специфичностима окружења у коме се реа-

Примитиве	Значење
Request - Захтев	Захтева за одређеном услугом
Indication - Индикација	Индикација о покретању активности за реализацију услуге
Response - Одговор	Одговор на примитиву индикације
Confirm - Потврда	Потврда иницијатору о реализацији одређене услуге

Табела 17.1 Четири класе примитива

[1] *Throughput*
[2] *File Transfer Protocol*



Слика 17.3 Временски редослед примитива

лизује. Веза између транспортне целине и корисника посматра се преко примитива (операција) и параметара који се размењују. Ове примитиве налажу целини да изврши неку активност, или да извести о некој активности коју су парњак целине обавиле. Један од начина да се класификују примитиве је да их групишемо у четири класе (табела 17.1). Примитиве које се користе су:

- захтев који иницира транспортни корисник да би покренуо одређену услугу,
- индикација коју обезбеђује транспортна целина да би обавестила о покретању активности за остваривање одређене услуге,
- одговор који обезбеђује транспортни корисник као одзив на примитиву индикација,
- потврда која се враћа транспортном кориснику по реализацији тражене услуге.

На слици 17.3 приказан је временски редослед ових догађаја.

Надзор везе

Када је обезбеђена услуга са успоставом везе транспортна целина је одговорна за успостављање и раскидање (окончање) везе. Када је симетрична процедура обезбеђена корисници са оба краја везе могу да иницирају комуникацију. Асиметричне процедуре омогућавају реализацију симплекс веза.

Раскид везе може да буде тренутан или одложен. Када је тренутан раскид везе онда подаци који су послати, а још нису стигли на одредиште, могу бити изгубљени. Одложен раскид спречава било коју страну да прекине везу док сви послати подаци не стигну на своје одредиште.

Убрзана испорука

Представља услугу која одговара механизму прекида и користи се за пренос повремено хитних података (нпр. аларм). Разликује се од услуге са приоритетом која додељује виши приоритет одређеним ресурсима. Подаци са тих ресурса се прослеђују брже од осталих података.

Извештај о стању

Извештај о стању и параметрима је услуга која даје могућност транспортном кориснику да обезбеди или да сам добије информације које се односе на услове транспортне целине или везе. Примери статусних информација су:

- карактеристике везе (нпр. пропусна моћ, средње кашњење...),
- адресе (мрежна, транспортна),
- класа протокола која је у употреби,
- текуће стање часовника,
- стање протокола (у контексту дијаграма стања),
- деградација у односу на захтевани степен услуге.

Сигурност

Транспортна целина може да обезбеди различите услуге везане за сигурност као што су:

- управљање приступом које се реализује на локалном и удаљеном крају,
- шифровање/ дешифровање података,
- рутирање преко поузданих веза и чворова уколико су на располагању.

17.2 Елементи транспортног протокола

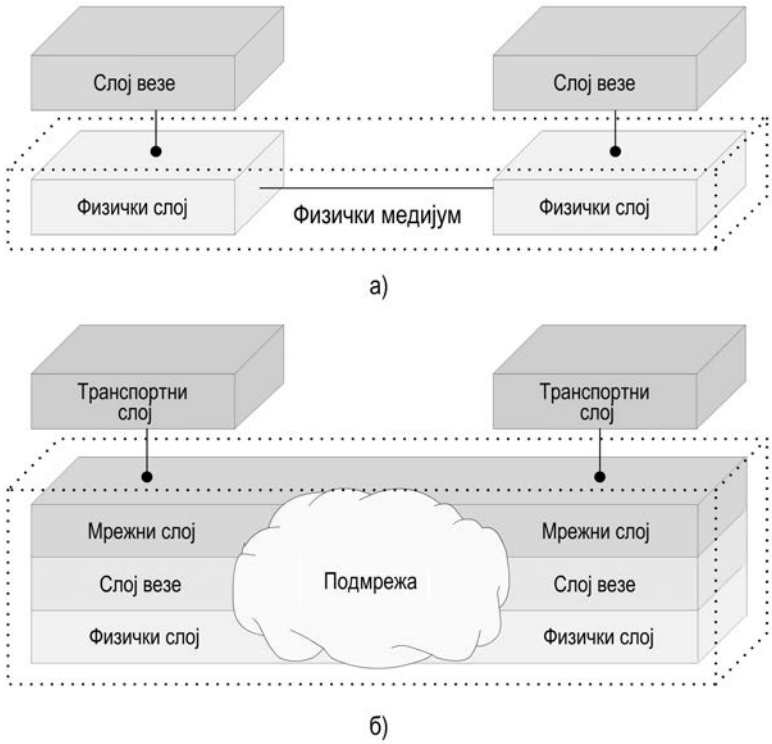
Услуга транспортног слоја (транспортна услуга) имеђу две транспортне целине реализује се помоћу транспортног протокола.Транспортни протокол сличан је протоколу слоја везе описаном у 11. поглављу. Код оба протокола, поред осталог, имплементирани су механизми за контролу грешке, секвенционирање и контролу тока. Постоје и значајне разлике које ћемо објаснити у овом одељку (слика 17.4).

Разлике које су на први поглед видљиве су следеће:

- два слоја везе комуницирају преко физичког канала док транспортни слојеви комуницирају преко подмрежа,
- успостављање везе преко физичког канала је једноставно, док је успостављање везе преко подмрежа знатно сложеније,
- подмрежа може да задржава податке и да их испоручи са значајним кашњењем,
- контрола тока и додељивање меморијског простора за чување пакета (баферовање) присутни су и код транспортног и код слоја везе. На слоју везе обично се резервише меморијски простор одређене величине за сваку од веза. Када рам стигне, меморијски простор за његово смештање је расположив. Пошто на транспортном слоју постоји велики број веза које треба опслужити принцип са наменским меморијским простором је практично неприхватљив.

Сложеност транспортног протокола зависи у значајној мери од услуга мрежног слоја. Организација ISO је дефинисала три типа услуга:

- тип А за мрежне везе са прихватљивим степеном погрешних пакета и прихватљивим степеном сигнализираних грешака,



Слика 17.4 Аналогија протокола а) слоја везе б) транспортног слоја

- тип B за мрежне везе са прихватљивим степеном погрешних пакета и неприхватљивим степеном сигнализираних грешака,
- тип C за мрежне везе са неприхватљивим степеном погрешних пакета.

Под погрешним пакетима подразумевају се изгубљени или дуплицирани мрежни пакети - NPDU[1]. Уколико грешку уочи и исправи целина на мрежном слоју на такав начин да је невидљива за транспортног корисника проблем је успешно разрешен. Уколико мрежна целина детектује грешку, не може да је отклони него обавести (сигнализира) транспортну целину, онда се то назива сигнализирана грешка. У овом поглављу анализираћемо транспортни протокол за случај поуздане и непоуздане услуге мрежног слоја (мрежне услуге).

17.3 Транспортни протокол и поуздана мрежна услуга

Претпоставка је да целина на мрежном слоју прихвата поруке произвољне дужине и да их са вероватноћом од 100% испоручује у правилном редоследу. Ова претпоставка доприноси примени једноставног транспортног протокола. Примери комуникационих мрежа које обезбеђују овакву услугу су:

- X.25 мрежа са комутацијом пакета високе поузданости,
- мрежа са штафетним преносом рамова (F R) која користи LAPF[2] протокол,

[1] *Network Protocol Data Unit*
[2] *Link Access Procedure for Frame Mode Bearer Services*

- локалне рачунарске мреже по стандарду IEEE802.3 и LLC услугом са успостављањем везе.

Анализираћемо:

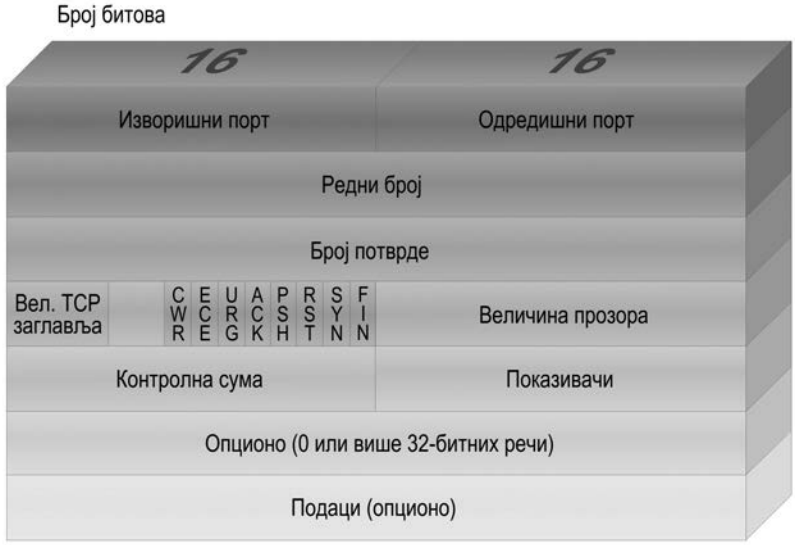
- формат заглавља јединице података транспортног слоја (TCP сегмента),
- адресирање,
- мултиплексирање,
- контролу тока и
- успостављање и раскидање везе.

Формат заглавља TCP сегмента

Слика 17.5 показује изглед TCP сегмента. Сваки сегмент почиње заглављем од 20 бајтова тачно дефинисаног формата. Заглавље може бити праћено опционим делом. После опционог дела може се послати 65535-4[1] = 65515 бајтова података. Сегмент без података је могућ и обично се користи као потврда или управљање.

TCP заглавље чине следећа поља:

- Изворишни и одредишни порт[2] (величине по 16 бита) - идентификују крајње тачке везе. Сваки TCP корисник може одлучити како да распореди сопствене портове почевши од 1024 па навише;
- Редни број[3] (величине 32 бита) - представља редни број првог бајта података у том сегменту осим у случају да је постављен на јединицу SYN бит. Тада поље редни број означава иницијални редни број ISN[4], а први бајт података има редни број ISN+1.



Слика 17.5 Заглавље TCP сегмента

[1] Фиксно заглавље (20) + поље опција (20).
[2] *Source port, destination port*
[3] *Sequnce number*
[4] *Initial Sequence Number*

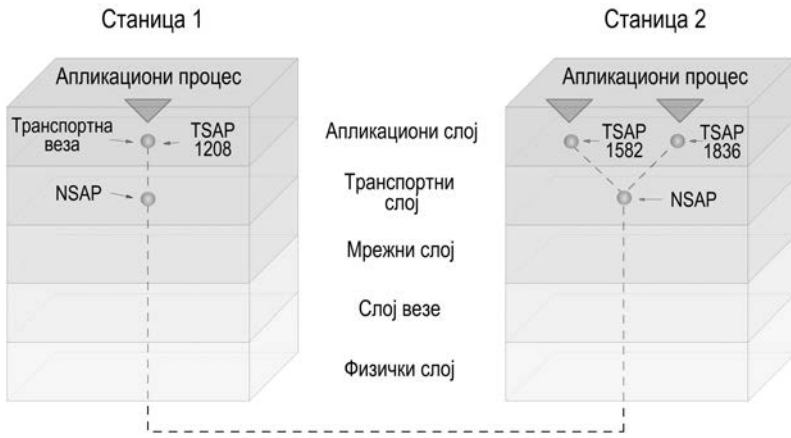
- Број потврде [1] (величине 32 бита) - означава редни број следећег податка који TCP целина очекује да прими;
- Дужина TCP заглавља (величине 6 битова) - носи информацију колико речи дужине 32 бита има у заглављу. Ово поље је неопходно пошто је поље опције променљиве величине;
- Резервисано (величине 4 бита) - намењено је за будућу употребу и тренутно се не користи;
- Ознака (флег) (величине 8 битова) - сваки бит у овом пољу има неку функцију:
  - CWR [2] постављен на 1 указује да је прозор загушења смањен,
  - ECE [3] - битови ECE и CWR дефинисани су у документу RFC3168. Користе се за обавештавање о загушењу које ће бити објашњено у следећем поглављу,
  - URG [4] постављен на 1 означава да је поље које указује [5] на место „хитних" података од значаја и у употреби. Функција која обезбеђује испоруку хитних података [6] служи да би се указало апликацији да су стигли хитни подаци и да одмах треба да јој се испоруче,
  - ACK постављен на 1 означава да је поље број потврде важеће и у употреби (*Ack* сегмент). Ако је ACK=0 сегмент не садржи потврду. У том случају поље „потврдни број" се игнорише,
  - PSH постављен на 1 од TCP целине - примаоца захтева да испоручује податке апликацији одмах по њиховом доласку и да их не складишти (што би он урадио због ефикасности),
  - RST постављен на 1 користи се за ресетовање везе (*Rst* сегмент). Такође се користи да би се одбацио неочекивани сегмент или одбио захтев за отварање нове везе,
  - SYN постављен на 1 користи се при успостављању везе (*Syn* сегмент). Када се шаље захтев за успоставу везе поља SYN и ACK имају вредности 1 и 0 респективно [7]. Када се шаље потврда на захтев за успоставу везе оба поља имају вредност 1 [8],
  - FIN постављен на 1 користи се при ослобађању везе (*Fin* сегмент). Указује да пошиљалац нема више података за слање,
- Отвор прозора [9] (величине 16 битова) - користисе се за контролу тока. Садржи број бајтова података, почев од редног броја који је наведен у пољу „потврдни број" које прималац може да прихвати. Када је вредност овог поља једнака 0 указује да прималац не може да прихвати више података.

[1] *Acknowledgement number TCP header lenght*
[2] *Congestion Window Reduced*
[3] *Explicit Congestion Notification - Exho*
[4] *Urgent function*
[5] *Urgent Pointer*
[6] Са постављеним URG битом на вредност 1 и одговарајућом вредношћу у пољу *Urgent Pointer*.
[7] SYN=1, ACK=0
[8] SYN=1, ACK=1
[9] *Window size*

- Контролни збир [1] (величине 16 битова) - користи се да би се избегао пријем сегмената који су оштећени при преносу. Када пошиљалац шаље сегмент он израчуна контролни збир и упише га у ово поље.
  Када прималац прими сегмент он израчуна контролни збир и ако је вредност коју добије иста као и вредност поља контролног збира, значи да при преносу није дошло до грешке и сегмент се прихвата;
- Указивач „хитних" података [2] (величине 16 бита). Када се ова вредност дода на редни број сегмента добија се вредност последњег бајта у секвенци података које треба хитно испоручити апликацији;
- Опције [3] (променљиве величине) - користи се за додатне услуге које нису укључене у регуларно заглавље. Једна од опција је, на пример, величина сегмента која се користи при преносу.
  Требало би користити што веће сегменте [4] јер се на тај начин преноси више података а заглавље од 20 бајтова се лакше амортизује. Као и у случају IP датаграма у пољу опције може бити један бајт или више бајтова.

Адресирање

Када апликациони процес (тј. корисник) жели да успостави везу са другим апликационим процесом потребно је да означи који је то процес, тј. потребно је да дефинише његову транспортну адресу. Термин који се користи (дефинисан је у 3. поглављу) је приступна тачка услуге транспортног слоја (TSAP [5]). На Интернету се ове крајње тачке - TSAP називају портови. На мрежном слоју се ове тачке (адресе мрежног слоја) називају приступне тачке услуге мрежног слоја NSAP (IP адресе су пример NSAP-а). На слици 17.6 приказана је веза између NSAP, TSAP и транспортне везе.



Слика 17.6 Транспортна веза, TSAP и NSAP

[1] *Checksum*
[2] *Urgent Pointer*
[3] *Options*
[4] Онолико велики колико дозвољавају станице који учествују у размени података.
[5] *Transport Service Access Point*

Апликациони процеси на страни клијента и сервера могу да се прикључе на приступну тачку транспортне услуге (TSAP) да би успоставили везу са удаљеном приступном тачком транспортне услуге. Ове везе се реализују преко приступних тачака мрежне услуге (NSAP) на страни сваке станице.

Значи адреса корисника је одређена паром (станица, порт). Порт је променљив и представља одређеног корисника. Идентификација транспортне целине није потребна пошто обично постоји само једна целина за одређени тип протокола. Касније ћемо видети да адреса треба да укључи тип транспортног протокола (нпр. TCP, UDP).

У случају једне одвојене мреже станица (хост) представља уређај повезан на рачунарску мрежу. Када је реч о Интернету станица (хост) представља глобалну Интернет адресу.

Рутирање није у надлежности транспортног слоја, тако да он само прослеђује део адресе која се односи на станицу (хост) мрежној целини. Порт се налази у транспортном заглављу и на одредишту га може употребити одредишни транспортни слој.

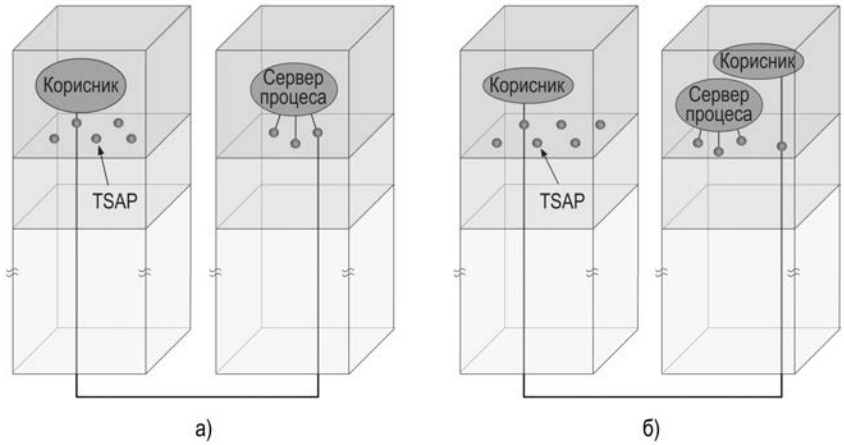
Поставља се питање како иницијатор транспортне везе зна адресу одредишног транспортног корисника? Одговор се може категоризовати на следећи начин:

- Корисник зна унапред одредишну адресу. У основи то је функција конфигурисања система. На пример, постоји процес који се искључиво бави прикупљањем статистичких података за одређени број транспортних корисника. С времена на време, са централног места систем за надзор рачунарске мреже скупља податке од осталих процеса да би обезбедио статистичке податке. Овај процес је важан за правилан рад, и не треба да буде приступачан свима;
- Неке од опште коришћених услуга проглашене су „познатим адресама"[1] (табела 17.2). На пример то су серверске стране протокола FTP, SMTP и неки други стандардни протоколи;
- Обезбеђени су сервери имена. Корисник захтева услугу користећи неко генеричко или глобално име. Захтев се шаље ка серверу имена који садржи базу адреса. На основу имена проналази тражену адресу и шаље је кориснику. Добивши тражену адресу транспортна целина успоставља везу са одредиштем. Ова услуга је корисна за апликације које се често користе али повремено мењају своју локацију. На пример неки процес може се пребацити са једног

Порт	Протокол	Намена
21	FTP	Пренос датотека
23	Telnet	Удаљени терминал
25	SMTP	Електронска пошта
80	HTTP	*Word Wide Web*
110	POP-3	Удаљени приступ електронске поште
53	DNS	Сервер имена домена

Табела 17.2 Најчешће коришћени портови

[1] *Well-known address.* Листа се може наћи на www.iana.org



Слика 17.7 Како корисник успоставља везу са:
а) сервером имена (процеса) б) покренутим процесом

рачунара на други у оквир локалне рачунарске мреже да би се обезебедило равномерно оптерећење;

- У неким случајевима одредишни корисник је процес који се по захтеву треба покренути, односно изазвати [1]. Корисник иницијатор шаље захтев ка познатим адресама. Процес – сервер на тим адресама покреће нове процесе и шаље иницијатору адресу новопокренутог процеса. На слици 17.7а приказана је комуникација са сервером процеса, на слици 17.7б комуникација са траженим корисником (изазваним процесом).

Мултиплексирање

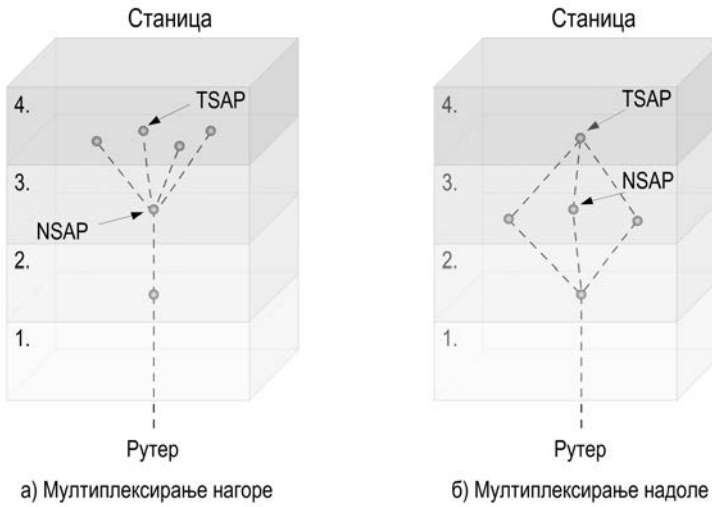
На транспортном слоју мултиплексирање је приказано на слици 17.8 и дефинишемо га као:

- мултиплексирање нагоре [2] уколико више транспортних корисника дели једну виртуелну везу успостављену између мрежних целина,
- мултиплексирање надоле [3] уколико једна транспортна веза користи више веза на мрежном слоју.

Навешћемо ситуације у којима се мултиплексирање користи. Узмимо за пример да је станици на располагању само једна мрежна адреса тако да све транспортне везе на тој станици морају ту адресу да користе.

Претпоставимо да подмрежа користи виртуелне везе и намеће ограничење у максималној брзини података по једној вези. Уколико је кориснику потребна већа брзина од брзине једног виртуелног кола може да отвори више мрежних веза и подели саобраћај између њих. Уобичајени пример мултиплексирања надоле је коришћење две ISDN везе од по 64kb/s за повезивање са пружаоца Интернет услуга, брзином од 128kb/s.

[1] *Spawned*
[2] *Upward multiplexing*
[3] *Downward multiplexing*



Слика 17.8 Мултиплексирање нагоре и надоле

Контрола тока

Ово је једноставан механизам на слоју везе а сложен механизам на транспортном слоју из следећих разлога:

- контрола тока на транспортном слоју укључује међусобну интеракцију транспортних корисника, транспортних целина и услуге мрежног слоја,
- кашњење у преносу између транспортних целина може бити велико. То значи да постоји прилично кашњење у размени информација везаних за контролу тока,
- кашњење у преносу пакета између транспортних целина је у општем случају знатно дуже од времена потребног за његово слање,
- с обзиром на то да транспортни слој функционише преко нижих слојева кашњење може да буде веома променљиво. Ово доприноси томе да је прилично отежано коришћење часовника за поновно слање изгубљених података.

Основна сличност контроле тока на слоју везе (на пример код HDLC протокола), на мрежном слоју (на пример X.25 протокол) и на транспортном слоју (на пример TCP протокол) настаје из потребе да се спречи да брзи пошиљалац загуши спори пријемник. Код слоја везе пошиљалац чува рамове (баферује их) и на пријемној и на предајној страни. Када подмрежа обезбеђује непоуздану услугу транспортна целина - пошиљалац чува све јединице података (TPDU) док не добије потврду за њих. Пријемна транспортна целина може на пример да резервише меморијски простор [1] за све везе заједно, а не за сваку појединачно.

Свака транспортна целина има одређену количину простора за чување пристиглих података, односно величину бафера. TPDU (у даљем тексту сегменти [2]) који

[1] *Buffer pool*

[2] Јединице података PDU (*Protocol Data Unit*) које међусобно размењују транспортне целине називају се сегменти.

пристижу смештају се у бафер. Сваки сегмент се анализира, нпр. TPDU заглавље, и по завршетку анализе шаље се одређеном транспортном кориснику. Ако пријемна транспортна целина не може да одржи корак са дотоком сегмената, бафери бивају препуњени [1] и може да дође до губитка података.

Да би се спречила појава „препуњених бафера" пријемна транспортна целина мора да предузме кораке за заустављање или успоравање дотока сегмената, да би могла да обради већ пристигле сегменте. Овај задатак није једноставно реализовати с обзиром на могућу удаљеност (временску и просторну) транспортних целина. Изложићемо четири начина за разрешавање захтева који се постављају пред механизмом за контролу тока.

Пријемна транспортна целина може:

- да не реагује ни на који начин,
- да одбије да надаље прима сегменте (TPDU) од мрежног слоја,
- да користи протокол клизајућег прозора са фиксним отвором прозора,
- да користи механизам кредита.

Друга варијанта значи да ће пријемна целина одбацити пакете у недостатку простора за њихово чување. Пошто не добије потврду за њих пошиљалац их поново шаље. Овај приступ није пожељно користити, јер долази до ретрансмисије. Предност мреже са успоставом везе је та да не би требало да постоји ретрансмисија (или бар да се сведе на минимум). Трећа варијанта је она која је примењена код протокола HDLC [2]. Кључни параметри су:

- свака јединица података добија редни број,
- отвор прозора је фиксан,
- користи се потврда која доводи до померања (клизања) прозора.

Са поузданом услугом мрежног слоја техника клизајућег прозора ради сасвим добро.

У четвртој варијанти пријемна транспортна целина поред потврде о пакетима које је успешно примила шаље нови параметар - кредит. Он представља отвор прозора али може да се мења у току трајање везе.

Успостава и завршетак везе

Да бисмо боље објаснили како се операције (примитиве) могу употребити у фазама успоставе и раскида везе посматраћемо апликацију са сервером и већим бројем удаљених клијената. У табели 17.3 дат је преглед примитива и њихово значење.

На почетку сервер извршава примитиву Passive Open обично системским позивом који блокира сервер док се не појави захтев клијента.

Када клијент жели да комуницира са сервером извршава примитиву Active Open. Транспортна целина извршава примитиву тако што блокира позивајућег корисника и шаље серверу јединицу података „захтев за успоставом везе" [3] (*Syn* сегмент). Порука транспортног слоја клијента упућеног транспортном слоју сервера спакована (учаурена) [4] је у део за податке [5] пакета мрежног слоја. Пакет мрежног слоја спакован је у рам

[1] *Buffer overflow*
[2] Описано је у 11. поглављу
[3] *Connection Request* TPDU
[4] *Encapsulated* - укалупљена.
[5] *Payload*

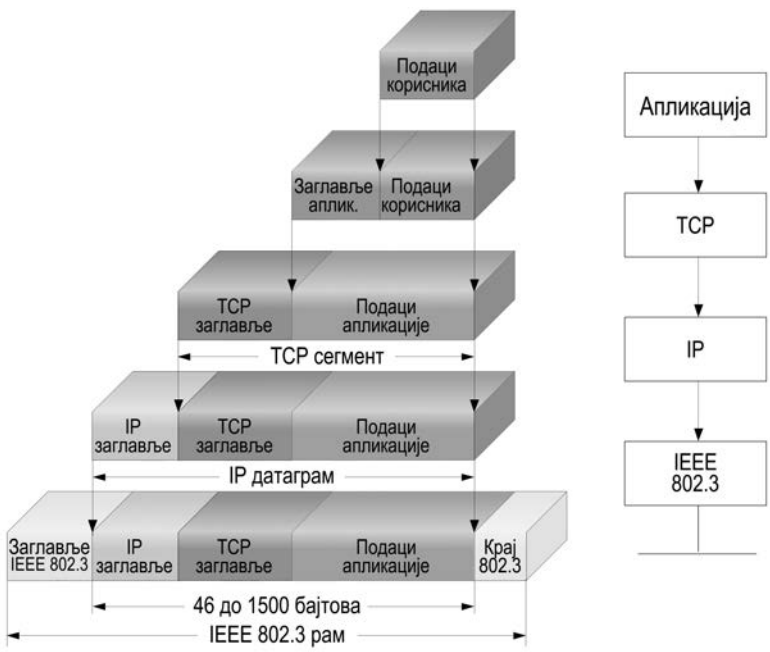
Примитива	Послата јединица података TPDU	Значење
Passive Open [1]	Не шаље се ништа	Блокиран је док неки од процеса не покуша да се повеже са њим.
Active Open [2]	Шаље захтев за успоставом везе	Активно покушава да успостави везу.
Send	Подаци	Шаљу се информације.
Receive	Не шаље се ништа	Блокиран је док не пристигну *Data* пакети.
Close	Шаље захтев за раскидом везе	Ова страна жели да оконча везу.

Табела 17.3 Примитиве и њихово значење

слоја везе. Када рам дође до сервера одвија се обрнут процес - распакивање на сваком слоју. Повезивање (укалупљивање) јединица података приказано је на слици 17.9.

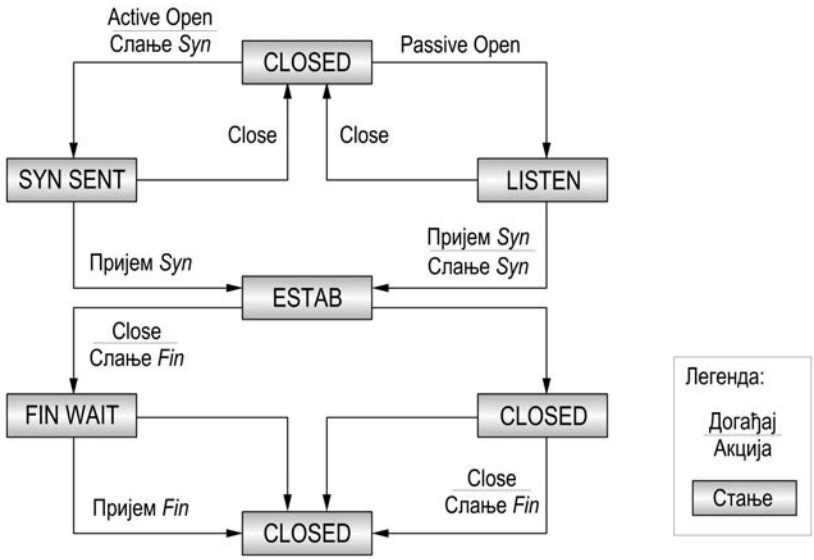
За реализацију услуге са успоставом везе неопходне су процедуре за успоставу и завршетак везе. Три битне функције успоставе везе су:

- омогућавање сваком учеснику да се увери да је други учесник присутан,
- дозвољавање договора око опционих параметара као што су на пример: максимална величина сегмента (TPDU), максимална величина отвора прозора, квалитет услуге,
- покретање додељивања ресурса потребних транспортној целини као што су меморијски простор за смештање података (бафер) и формирање табеле [3].



Слика 17.9 Повезивање јединица података (PDU [4])

[1] У литератури се пасивно отварање везе [Таненбаум] означава и као *Listen* (ослушкуј).
[2] TCB (*Transmission Control Block*) - запис о вези. Садржи све променљиве потребне за одржавање везе.
[3] У литератури се активно отварање везе [Таненбаум] означава и као *Connect* (повежи се).
[4] *Protocol Data Unit*



Слика 17.10 Једноставан дијаграм стања везе

Успостава везе је међусобни договор корисника и може се остварити разменом различитих команди и управљачким сегментима, као што је приказано на дијаграму стања на слици 17.10. Имена и опис 11 стања која су дефинисана у RFC793 дати су у табели 17.4. Стање CLOSED у ствари је имагинарно стање када не постоји TCB запис, а самим тим ни веза.

На почетку корисник је у неактивном стању - CLOSE[1], нема успостављену ни једну везу. Корисник командом (примитивом) Passive Open чека на захтев за успостављање везе. После издавања ове команде транспортна целина креира објекат везе (нпр. запис у табели) која се налази у стању LISTEN[2]. Ако се транспортни корисник у међувремену предомислио и жели да се врати у CLOSE стање, може то једноставно да реализује извршавањем команде Close.

Уколико стигне сегмент *Syn* (*Cr*)[3] који је адресиран на корисника који је у стању пасивног чекања, веза је отворена и транспортна целина ће:

- сигнализирати кориснику да је веза отворена,
- послати *Ack_Syn* (*Cs*)[4] сегмент као потврду удаљеној транспортној целини,
- поставити објекат везе у стање ESTABLISHED.

Корисник може да успоставља (отвара) везу користећи команду Active Open[5] која покреће транспортну целину да пошаље сегмент *Syn*. Пријем одговарајућег *Syn* сегмента успоставља везу.

[1] Указује да је веза затворена.
[2] Указује да је процес на страни сервера у стању ослушкивања позива клијента.
[3] TPDU захтев за успоставом везе *Cr* (*Connction request*). Код TCP протокола означава се са *Syn*.
[4] *Cs* (*Connection confirm*) - уобичајено је да се исти TPDU користи и као захтев за успоставом везе и као потврда о успостави везе и означава као *Ack Syn*.
[5] Назива се и захтев за успоставом везе (*Connect*).

Стање	Опис
CLOSED	Указује да не постоји TCB запис а самим тим ни веза.
LISTEN	Представља ишчекивање (ослушкивање) захтева за успоставу везе од удаљеног TCP процеса или порта.
SYN-SENT	Представља стање ишчекивања одговарајућег захтева за успоставу везе после слања захтева за успоставом везе (*Syn* сегмента).
SYN-RCVD	Представља стање ишчекивања пријема потврде захтева за успоставу везе (*Ack* сегмента) после и слања и пријема захтева за успоставом везе.
ESTABLISHED	Представља успостављену везу. Подаци који се добијају могу се испоручити кориснику. Ово је нормално стање за фазу преноса података у вези.
FIN-WAIT1	Представља стање ишчекивања захтева за окончање везе од удаљеног TCP процеса, или потврду на захтев за окончање везе који је претходно послат.
FIN-WAIT2	Представља ишчекивање захтева за окончање везе од удаљеног TCP процеса.
TIME-WAIT	Представља чекање да протекне довољно времена да би били сигурни да је удаљени TCP процес примио потврду свог захтева за окончање везе.
CLOSING	Представља ишчекивање потврде захтева за окончање везе.
CLOSE-WAIT	Представља ишчекивање захтева за окончање везе од локалног корисника.
LAST-ACK	Представља ишчекивање потврде захтева за окончање везе претходно послатог удаљеном TCP процесу (што укључује потврду свих његових захтева за окончање везе).

Табела 17.4 Стања везе и њихов опис

Када страна која је иницирала отварање везе прими *Syn* сегмент, може да пређе у ESTABLISHED стање. У случају да било који транспортни корисник изврши *Close* команду веза се одмах прекида. Било која страна може да иницира успостављање везе. У случају да обе стране иницирају везу у исто време, веза се без икаквих проблема успоставља. Разлог је то што се *Syn* сегменти посматрају и као захтеви за успоставу везе и као потврда о успостављеној вези. Веза се превремено прекида када локални корисник пошаље Close команду или када удаљена транспортна целина одбије везу слањем транспортне јединице података за окончање везе сегмент *Fin* (*Dr*)[1].

Шта се дешава уколико је корисник који би требало да се налази у стању пасивног чекања (LISTEN) неактиван (CLOSE)?

Може да се деси:

- да транспортни слој одбаци захтев слањем сегмента *Fin*,
- да се захтев ставља у ред за чекање док корисник не пошаље команду Active Open,
- да транспортна целина сигнализира кориснику да постоји нерешен захтев за успоставу везе са њим.

У случају да транспортна целина реагује на трећи од наведених начина, Active Open команда није неопходна и може бити замењена командом Accept, која представља сигнал који шаље транспортни корисник транспортној целини да прихвати захтев за успоставу везе.

[1] *Dr* (*Disconnect request*) - код TCP протокола означава се са *Fin*

Раскид везе извршава се на сличан начин. Било која страна, или обе, могу да иницирају окончање, тј. затварање (Close). Веза се затвара обостраном сагласношћу. Постоје два начина да се прекине веза а то су: изненадан прекид, када једна страна покрене иницијативу за прекид везе не сачекавши да то друга страна одобри, или прекид везе који настаје као резултат договора обе стране. Ако се веза изненада прекине подаци који се у том тренутку налазе на путу између две станице могу бити изгубљени.

Прекид везе уз међусобни договор обавезује обе стране да не прекидају везу док се сви подаци не испоруче. Да би се то постигло веза у стању FIN WAIT треба да настави да прима податке све док не добије *Fin* сегмент.

Слика 17.10 илуструје процедуру правилног прекида везе. Прво је неопходно уочити страну која иницира прекид везе:

- Као одговор на примитиву Close транспортног корисника транспортна целина шаље *Fin* сегмент другој страни, захтевајући прекид везе.
- Када пошаље *Fin* сегмент транспортна целина ставља конекцију у FIN WAIT стање. Када је веза у овом стању транспортна целина мора да настави да прихвата податке који стижу с друге стране и да испоручи податке кориснику.
- Када *Fin* сегмент стигне као одговор транспортна целина затвара везу и о томе обавештава корисника.

С тачке гледишта стране која није иницирала прекид ситуација је следећа:

- Када страна која није иницирала прекид прими *Fin* сегмент, транпортна целина информише корисника да је иницран прекид везе и ставља везу у CLOSE WAIT стање. Када се веза налази у овом стању, транспортна целина мора да настави да прима податке од свог корисника и да их прослеђује ка другој страни.
- Када корисник изврши *Close* примитиву, транспортна целина шаље одговарајући *Fin* сегмент другој страни и затвара везе.

Ова процедура обезбеђује да се обе стране сложе око затварња везе и да приме податке који се налазе на линији, пре самог затварања везе, да не би дошло до губљења података.

Транспортни протокол и непоуздана услуга мрежног слоја

Сложенији случај транспортног протокола је када је услуга мрежног слоја непоуздана.

Примери мрежа које користе овакве услуге су:

- мреже које користе Интернет протокол (IP),
- мреже са штафетним преносом које користе само LAPF протокол,
- локалне рачунарске мреже типа IEEE802.3. које користе LLC услугу без успоставе везе и без потврде.

Проблеми су:

- повремени губитак сегмената,
- њихово пристизање ван послатог редоследа као последица променљивог кашњења кроз мрежу.

Потребно је анализирати:

- стратегију поновног слања,
- детекцију дуплих пакета,
- контролу тока,
- успоставу везе,
- окончање везе,
- опоравак после испада из рада.

Стратегија поновног слања (ретрансмисија)

Два догађаја указују да је потребна стратегија за поновно слање сегмената. Прво сегмент може да буде оштећен при проласку кроз мрежу али и поред тога стиже на одредиште. Уколико је контрола грешке укључена у сегмент пријемна транспортна целина може да детектује грешку и одбаци сегмент. Друга непредвиђена ситуација је да сегмент не стигне на одредиште. Транспортна целина која је послала сегмент не зна да је слање неуспешно. Да би се овакви проблеми разрешили уводи се потврда (сегмент *Ack*). Пријемник мора да потврди сваки успешно примљени сегмент. Због ефикасности не користи се један *Ack* по једном сегменту података већ кумулативна потврда – један *Ack* за више сегмената. Значи пријемник прима сегменте података означене бројевима (редни бројеви) 1, 2 и 3 али враћа натраг само *Ack* 3. Уколико сегмент није успешно примљен неће бити послата потврда (*Ack*) и предајна страна мора сегмент поново да шаље. За свако слање сегмената мора да постоји часовник[1] који се поставља на одређено време. Ако то време истекне а сегмент није потврђен пошиљалац мора поново да шаље пакет.

Увођење часовника донекле разрешава проблем. Поставља се питање на коју вредност треба поставити часовник? Уколико је вредност превише мала постојаће много беспотребних ретрансмисија. Уколико је вредност превелика протокол ће бити инертан у реаговању на изгубљене сегменте. Часовник треба да буде постављен на вредност мало већу од укупног кашњења кроз мрежу[2] које је једнако збиру времена потребног да сегмент стигне на одредиште и да се врати његова потврда. Кашњење је променљиво и код мрежа са константним саобраћајем а нарочито код мрежа са променљивим карактеристикама.

Постоје два метода: са тачном (фиксном) вредношћу и са променљивом (адаптивном) вредношћу. Тачно одређена вредност на коју се часовник подешава заснована је на уобичајеном стању мреже. Проблем са овим методом је што не одговара мрежама чије се стање мења. Уколико је вредност превише велика услуга ће увек бити инертна. Уколико је вредност превише ниска јавља се позитивна повратна спрега - загушење мреже које доводи до више ретрансмисија које повећавају саобраћај у мрежи и још веће загушење.

Адаптивна шема има својих ограничења. Претпоставимо да транспортни слој прати колико времена је потребно да би се потврдио сегмент и подешава часовник према праћеној средњеној вредности.

[1] *Timer*
[2] *Round trip delay*

Часовник	Намена
За ретрансмисију [1]	Поново шаље сегмент који није потврђен
За поновну успоставу везе [2]	Минимално време између затварања једне везе и отварања друге везе са истом одредишном адресом
За отвор клизајућег прозора [3]	Максимално време између два сегмента ACK/CREDIT
За ретрансмисију *Syn* сегмента [4]	Време између два покушаја да се веза успостави (отвори)
За прекид [5]	Прекида везу пошто ниједан сегмент није потврђен

Табела 17.5 Часовници који се користе на транспортном слоју

Може се десити да:

- одредиште не шаље потврду одмах (нпр. користи се кумулативна потврда),
- сегмент се шаље поново али пошиљалац не зна да ли је примљена потврда (*Ack*) за првобитно слање или за ретрансмисију,
- услови у мрежи могу се нагло променити.

Сваки од ових проблема се може разрешити на неки начин али свако од решења оставља одређени степен неодређености. Часовник за ретрансмисију је веома важан за исправан рад транспортног протокола. У табели 17.5 описани су часовници које транспортни протокол користи.

Откривање (детекција) дупликата

Уколико се деси да је сегмент изгубљен и поново послат не може да дође до грешке. Уколико је *Ack* изгубљен један или више сегмената ће бити поново послати и уколико стигну успешно биће дупликати претходно послатих сегмената. Потребно је пронаћи начин да пријемник препозна дупликате. Постоје два случаја:

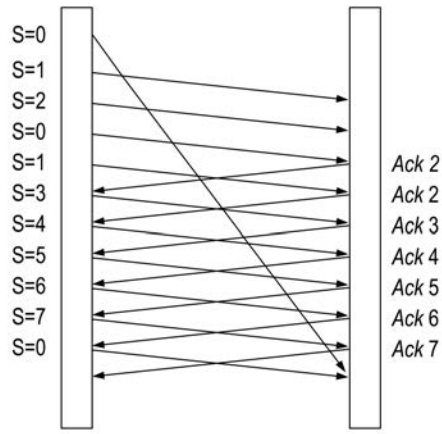
- дупликат је примљен пре затварања везе,
- дупликат је примљен по затварању везе.

Може да се деси да дупликат стигне пре оригиналног сегмента. Уколико се деси да дупликат стигне пре затварања везе онда:

- пријемник треба да претпостави да је потврда изгубљена и да је потребно да пошаље потврду за дупликат,
- простор редних бројева (број редних бројева) треба подесити да је довољно велики.

Слика 17.11 приказује разлог за захтеве који следе. У овом примеру простор редних бројева је 8. Због једноставности претпостављамо да је отвор клизајућег прозора величине 3 сегмента. Нека је станица 1 послала сегменте са редним бројевима 0, 1, 2 (на слици 17.11 означених као S=0,...) и није добила потврду о њиховом успешном пријему. Оглашава се часовник за ретрансмисију (пошто је време истекло). Станица 1 поново шаље сегмент 0. Станица 2 прима сегменте 1, 2 али је при проласку кроз мрежу сегмент

[1] *Retransmission timer*
[2] *Reconnection timer*
[3] *Window timer*
[4] *Retransmit Syn timer*
[5] *Give up timer*



Слика 17.11 Пример погрешне детекције дупликата

0 закашњен. Када дупликат сегмента 0 стигне станица 2 потврђује 0, 1 и 2. У међувремену истекло је и време за пакет са редним бројем 1 па га станица 1 поново шаље. Станица 2 га потврђује новим *Ack2*. Када је простор редних бројева потпуно искоришћен станица 1 се поново враћа на редни број 0 и наставља даље. Али у међувремену стиже стари сегмент 0 пре него што је стигао нови сегмент 0.

Јасно је да пристизање старог сегмента 0 „у невреме" не би изазвало никакве проблеме да није кренуо нови круг редних бројева. Питање је колико треба да буде велики простор редних бројева? Ово зависи, између осталог, од тога да ли мрежа подржава максимално „време живота" пакета и брзину којом се сегменти поново шаљу. Додавањем само једног бита у поље редних бројева може се удвостручити простор редних бројева. Стандардни транспортни протокол омогућава огроман простор редних бројева.

Анализираћемо други проблем: сегмент кружи мрежом по затварању транспортне везе. Ако је следећа веза отворена између истих транспортних целина сегмент из старе везе може да се појави и да буде прихваћен. Такође закаснела потврда може да се појави у новој транспортној вези и изазове проблеме.

Постоји неколико метода који могу да разреше ове проблеме. Анализираћемо неке од њих. Први метод се састоји у следећем: транспортна целина памти последњи редни број који је употребљен у завршеној транспортној вези. Када се нова веза успоставља *Syn* садржи редни број са којим треба да се започне пренос података.

Други приступ је увођење посебног идентификатора транспортне везе и употреба новог идентификатора са сваком новом везом.

Описана процедура ради добро докле год не дође до пада система, па се информација о идентификатору последње везе губи. Алтернатива је да се једноставно сачека довољно дуго између две транспортне везе да би осигурали да су сви сегменти испоручени. Уколико дође до пада система на једној страни друга страна може да одбије успостављање везе све док време на које је часовник за поновну успоставу везе постављен не прође. Ово наравно може да изазове беспотребна кашњења.

Контрола тока са механизмом кредита

Побољшања са механизмом кредита представља добро решење за мреже са непоузданом услугом мрежног слоја. Механизам са доделом кредита и механизам потврде повезани су тако да пријемна транспортна целина шаље управљачки сегмент који садржи:

- потврду о успешном пријему сегмента закључно са редним бројем *N* (означава се са *AckN*),
- дозволу да предајник пошаље сегмент почевши од редног броја *N*+1 до редног броја *N*+*M* (означава се са *Credit M* - отвор прозора).

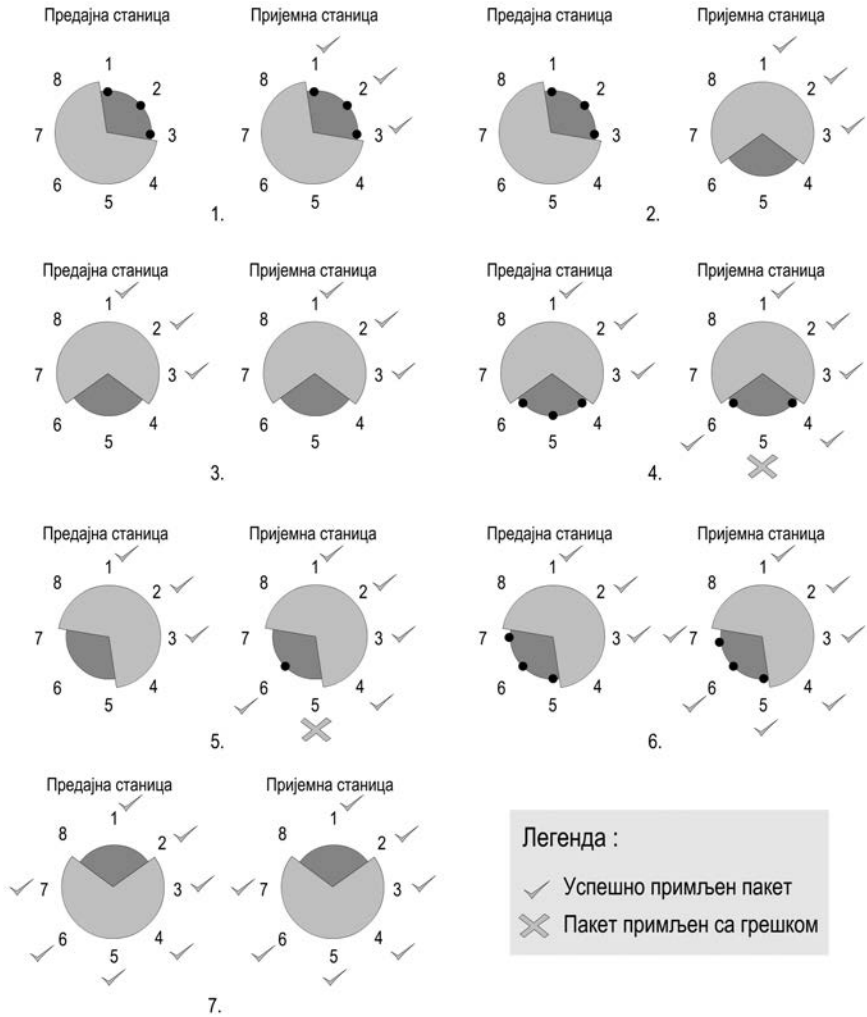
Уколико се деси да потврда не стигне на време часовник за ретрансмисију ће то сигнализирати и предајник ће поново послати сегменте који захтевају нову потврду. Грешка је и даље могућа али се може превазићи што ћемо видети у следећем примеру:

- предајна станица шаље сегмент са параметрима (*AckN, Credit M*) и привремено затвара прозор,
- затим шаље сегмент са параметрима (*AckN, Credit0*) али овај сегмент је изгубљен,
- предајна станица чека дозволу да пошаље податке, пријемна станица зна да је дозвола послата,
- часовник за отвор прозора (активира се при слању сваког сегмента *Ack/Credit*) сигнализира да је време истекло,
- понавља се последњи *Ack/Credit* сегмент и указује пошиљаоцу да је одредиште и даље активно.

На слици 17.12 илустрован је пример употребе клизајућег прозора. Види се да се доња граница отвора прозора поставља када се сегмент пошаље а горња граница када се добије кредит. У тексту који следи објашњен је пример са слике 17.12:

1. отвор прозора је подешен на 3 и код предајне и код пријемне станице. Предајна станица шаље три сегмента пријемној станици;
2. пријемна станица је успешно примила сва три сегмента и подешава свој отвор прозора за следећа три сегмента; шаље предајној станици сегмент потврде [1] означен као *Ack4* и кредит који је 3. Број 4 указује да је секвенцни број првог следећег пакета који очекује 4;
3. на основу примљеног *Ack4* сегмента, предајна станица зна да су прва три пакета испоручена а на основу кредита (3) подешава отвор прозора за следећа три сегмента: сегменте са секвенцним бројевима 4, 5 и 6 које затим шаље;
4. пријемна станица прима сва три сегмента али 5. сегмент је са грешком. Пријемна станица помера свој отвор прозора за један и шаље предајној станици сегмент *Ack5* и кредит који је 3. На тај начин обавештава предајну станицу да је примила 4. сегмент, и да поново пошаље 5, 6. и 7. сегмент;
5. предајна станица прима *Ack5* сегмент и прилагођава свој отвор прозора. Затим шаље сегменте са редним бројевима 5, 6 и 7;

[1] Потврда о успешном пријему означава се са *Ack* (*Positive Acknowledge* - позитивна потврда). Уколико је примљен пакет са грешком онда одредиште шаље пакет који указује да је примљени пакет са грешком *NAK* (*Negativ Acknowledge* - негативна потврда).



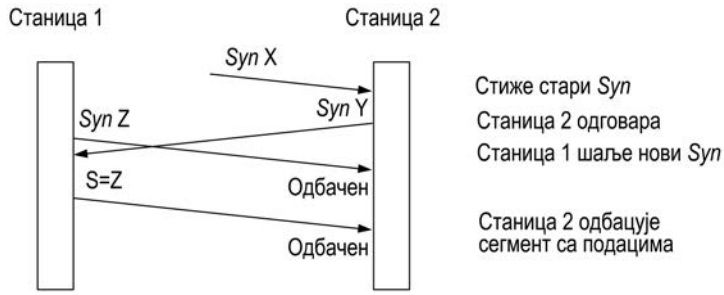
Слика 17.12 Пример технике клизајућег прозора са кредитом

6. пријемна станица успешно прима 5, 6. и 7. сегмент, подешава свој отвор прозора на нову вредност, а затим предајној станици шаље потврду да је успешно примила сегменте и нови кредит;
7. предајна станица добија потврду о пријему сегмената и подешава свој отвор прозора на нову вредност.

Успостављање везе

Успостављање везе као и остали механизми протокола треба да узму у обзир непоузданост мрежне услуге. Размена *Syn*[1] сегмената некада се назива двострана процедура[2]. Претпоставимо да станица 1 шаље *Syn* сегмент ка станици 2. Очекује да добије

[1] Код TCP протокола означава се са *Syn*. Користи се и ознака CR TPDU (*Connection Request Transport Protocol Data Unit*).
[2] *Two-way handshake*



Слика 17.13 Пример двостране процедуре

натраг *Syn* сегмент као потврду да је веза успостављена. Две ствари могу да изазову погрешан ток: *Syn* сегмент који шаље станица 1 је изгубљен или је *Syn* сегмент који као одговор шаље станица 2 изгубљен. Оба случаја могу се превазићи са часовницима за поновно слање (ретрансмисију).

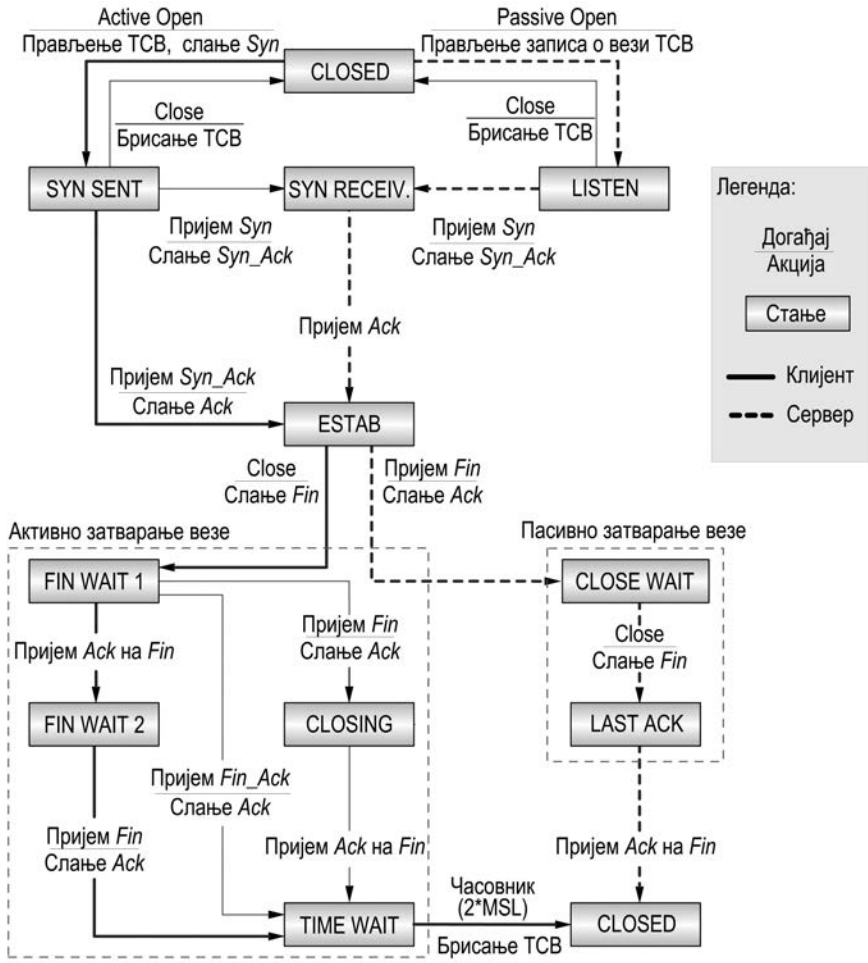
Поновна слања могу довести до дуплицирања *Syn* сегмената. Када је веза успостављена станице 1 и 2 могу једноставно да игноришу дупликате.

Шта се дешава уколико дупликати *Syn* сегмената опстану по завршетку везе? На слици 17.13 приказан је проблем који може да се појави. Стари *Syn* сегмент (захтев за успоставом везе, редни број почиње са X) стиже до станице 2 пошто је веза окончана. Станица 2 претпоставља да је ово нови захтев и одговара са сегментом *SynY*. У међувремену станица 1 је одлучила да успостави нову везу са станицом 2 и шаље сегмент *SynZ*. Станица 2 га одбацује као дупликат. Станица 1 започиње пренос података сегментом са редним бројем *Z*. Станица 2 га одбацује као сегмент ван очекиваног опсега редних бројева.

Начин за превазилажење овог проблема је да свака од страна потврди пријем *Syn* сегмента. Процедура се назива тространa [1] . На измењеном дијаграму стања (горњи део слике 17.14) додато је ново стање - *Syn* примљен (SYN RCVD). У овом стању транспортна целина чека да добије потврду да је послати *Syn* сегмент и примљен и тек тада се веза сматра успостављеном (отвореном). Поред новог стања додат је и нови управљачки сегмент (*Rst*). Његова функција је да када се открије дупликат *Syn* пакета раскине везу на другој страни. Слика 17.14 илуструје типични начин рада са тространом процедуром. У нормалним околностима станица 1 (нпр. клијент) шаље *Syn* сегмент који садржи предајни редни број. Ова вредност представља иницијални редни број станице 1. Станица 2 (нпр. сервер) шаље као одговор *Syn* сегмент који садржи потврду примљеног редног броја и свој иницијални редни број. Станица 1 првим сегментом података потврђује пријем *Syn/Ack* сегмента станице 2.

Примером који је приказан на слици 17.15 представљен је случај у коме станици 2 стиже стари *SynX* сегмент после окончања везе. Станица 2 претпоставља да је ово захтев за успоставом нове везе и одговара са *SynY*, *AckX*. Када станица 1 добије овај сегмент, и види да није захтевала ову везу, шаље сегмент *Rst*, *AckY*. Уочимо да је део *AckY* у *Rst* сегменту суштински веома значајан, тако да стари *Rst* не може да прекида

[1] *Three - way handshake*



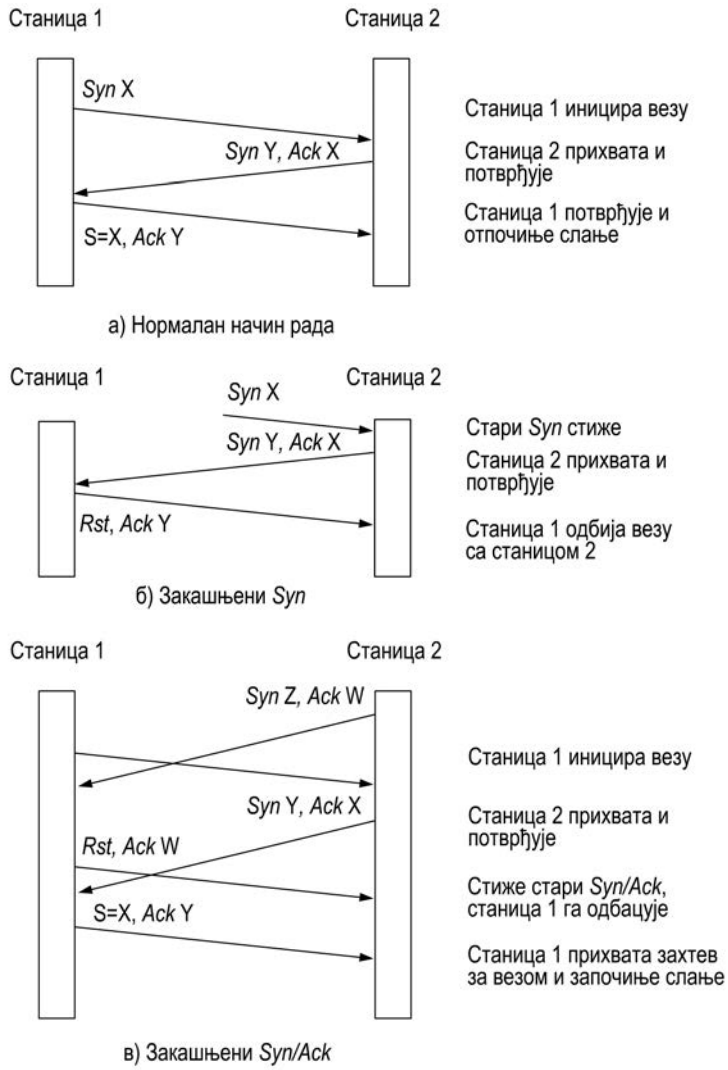
Слика 17.14 Измењени дијаграм стања

регуларну успоставу везе. На крају пример на слици 7.15в указује на случај када стари *Syn_Ack* сегмент стиже у току успоставе нове везе. Због употребе редних бројева у потврди овај догађај неће изазвати никакав проблем.

Горњи део слике 17.14 не садржи транзицију у којој је *Rst* сегмент послат, једноставности ради. Основно правило гласи: послати *Rst* сегмент уколико веза није још увек у стању ESTABLISHED и уколико је примљен погрешан *Ack* (који се не односи на оно што је послато).

Окончавање везе

Као и у случају успоставе везе процедура за окончавање везе мора да се бави старим и изгубљеним управљачким сегментима. На слици 17.14 види се да је примењено слично решење. Свака страна мора експлицитно да потврди *Fin* сегмент друге стране користећи у *Ack* сегменту редни броја који одговара *Fin* сегменту који треба да по-



Слика 17.15 Пример тростране процедуре у нормалном начину рада, са кашњењем *Syn* и *Syn/Ack* сегмената

тврди. Да би се спречила неусаглашеност користе се редни бројеви на следећи начин:

- *Fin* садржи редни број последњег сегмента увећан за један,
- *Ack* садржи редни број примљеног *Fin* сегмента.

Процедуре које се покрећу када истекне време на које су часовници подешени користе се за затварање везе када друга страна везе не ради исправно.

Опоравак после отказа[1]

Када систем на коме ради посматрана транспортна целина престане са радом (падне) и после се поново покрене, информације о стању свих веза су изгубљене. Ве-

[1] *Crash recovery*

зе се сматрају полуотвореним пошто друга страна (код које није дошло до грешке) није још сагледала проблем.

Још увек активна страна полуотворене везе може да је затвори користећи часовник за прекид [1]. Часовник мери време које истекне после максималног броја ретрансмисија. По истицању тог времена транспортна целина претпоставља да је друга транспортна целина у квару и обавештава транспортног корисника о нерегуларном окончању везе.

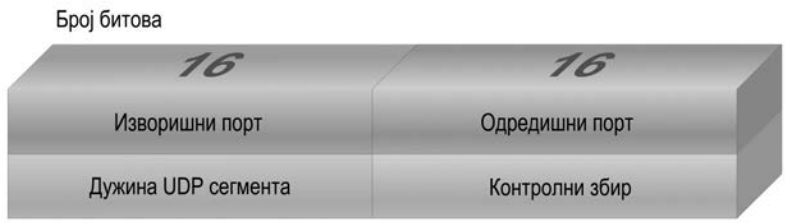
У случају да је транспортна целина кратко време у квару па убрзо поново почне да ради, полуотворена веза се може окончати употребом *Rst* сегмента. Страна која је у квару шаље *RstX* за сваки сегмент података редног броја *X* који прими. Када *Rst X* сегмент стигне на другу страну мора се проверити на основу редног броја *X* пошто *Rst* може да буде одговор на стари сегмент. Уколико је прекид важећи транспортна целина ће извршити нерегуларно окончање везе.

17.4 Транспортни протокол без успоставе везе UDP

Интернет подржава и транспортни протокол без успоставе везе UDP [2]. Многе клијент-сервер апликације радије за упит и одговор користе UDP него TCP протокол.

Протокол UDP описан је у документу RFC768. Сегмент UDP састоји се од заглавља (величине 8 бајтова) и поља података. UDP заглавље (приказано на слици 17.16) састоји се од:

- поља изворишног и одредишног порта (величине по 2 бајта) - намена изворишног [3] и одредишног [4] порта иста је као и у TCP заглављу - идентификација прикључних тачака изворишног и одредишног рачунара,
- поља дужине (величине 2 бајта) - указује на укупну дужину UDP сегмента укључујући и UDP заглавље,
- контролни збир (величине 2 бајта) - контолни збир се односи на псеудозаглавље које се користи и код TCP протокола. Опционо је, и уколко се оно не користи његова вредност поставља се на 0.



Слика 17.16 Заглавље UDP сегмента

[1] *Give up timer*
[2] *User Datagram Protocol*
[3] *Source port*
[4] *Destination port*

18. Апликациони слој TCP/IP референтног модела

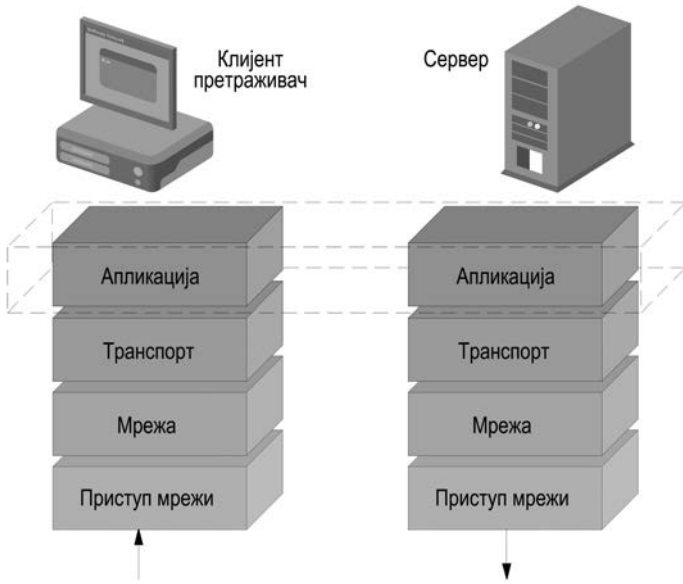
Како се број корисника на Интернету повећавао и захтеви за различитим апликацијама су се повећавали пратећи све сложеније захтеве корисника. Један од начина на који се апликације, које се данас користе, могу категоризовати је на традиционалне апликације и на савремене апликације.

У овом поглављу биће дат кратак преглед неких од највише коришћених апликација, а детаљније ће бити обрађен систем имена домена (DNS[1]). У традиционалне апликације могу се сврстати: удаљени терминал, пренос датотека и електронска пошта, а у савремене: Web, систем имена домена, апликација које захтевју пренос у реалном времену и надзор и управљање рачунарским мрежама. Поменуте апликације користе одговарајуће протоколе:

- Удаљени терминал користии Telnet протокол. Омогућава кориснику терминала или персоналног рачунара да се пријави на удаљени рачунар и ради на њему као да је директно повезан са њим.
- За пренос датотека са једног на други систем користи се FTP[2] протокол. Могу се слати датотеке бинарног и текстуалног типа.
- Систем имена домена (DNS) омогућава повезивање између имена станице на Интернету и његове нумеричке адресе.
- Протокол SMTP[3] обезбеђује размену електронских писама, тј. омогућава механизам за размену порука између различитих корисника.
- Протокол HTTP[4] подржава размену захтева и одговора између Web претраживача и Web сервера.
- Протоколи H323[5] и SIP[6] воде рачуна о успостављању, модификовању и раскидању веза апликација које раде у реалном времену као што је телефонија[7] или видео, а користе IP протокол.
- Протокол за управљање мрежом (SNMP[8]) развијен је као средство за надзор и управљање рачунарским мрежама и међусобно повезаним рачунарским мрежама које користе скуп TCP/IP протокола. Назив указује на скуп спецификација за надзор и управљање рачунарским мрежама која укључује протокол, дефиницију базе података и одговарајуће концепте.

---

1 *Domain Name System*
2 *File Transfer Protocol*
3 *Simple Mail Transfer Protocol*
4 *Hypertext Transfer Protocol*
5 Серија стандарда организације ITU-T која се односи на повезивање јавних телофонских мрежа преко Интернета (тзв. Интернет телефонија).
6 *Session Initiation Protocol* - једноставнији протокол од H323 за пренос говора преко Интернета. Усвојила га је организација IETF а описан је у документу RFC3261.
7 *VoIP* - гпренос говор преко Интернета.
8 *Simple Network Management Protocol*



Слика 18.1 Место система имена домена (DNS)

18.1 Систем имена домена

Без обзира што се станице [1] на мрежи (односно њихови мрежни интерфејси) препознају по IP адресама корисницима је лакше да користе име рачунара (хоста) уместо IP адресе (нпр. *www.vets.edu.yu* = 195.252.117.130). У TCP/IP окружењу систем имена домена (DNS [2]) представља дистрибуирану базу података која обезбеђује везу (мапирање) између IP адресе и имена рачунара. Свака од апликација може да приступи стандардној бази података.

Систем имена домена (DNS) је дистрибуирана база података коју користе апликације TCP/IP архитектуре. Задатак јој је да изврши повезивање имена рачунара и њихових IP адреса, као и да обезбеди информације потребне појединим услугама (нпр. информације потребне за усмеравање електронске поште). Свака страна (факултет, смер, институција, организациона јединица...) одржава сопствену базу података и на серверу коме други системи (клијенти) преко Интернета могу да приступе. Систем имена домена (DNS) обезбеђује протоколе који омогућавају клијентима и серверима да међусобно комуницирају.

Са стране апликације приступ DNS бази је преко претраживача [3]. Апликација мора да претвори име рачунара у IP адресу пре него што постави захтев транспортној целини да успостави TCP везу или пошаље датаграм користећи UDP протокол. TCP/IP у оквиру оперативног система не зна ништа о систему имена домена (DNS). На почетку за разрешавање имена рачунара у IP адресу користила се *hosts*-

[1] Користе се термини станица, рачунар или хост.
[2] RFC1034 специфицира концепт, *а* RFC1035 специфицира детаље примене.
[3] *Resolver*

текстуална датотека у којој су се налазила повезивања (мапирања) између имена рачунара и његове IP адресе. То су датотеке:

- /etc/hosts, на Linux, UNIX и сличним оперативним системима,
- \%SystemRoot%\System32\Drivers\Etc. на оперативном систему Windows.

Сви рачунари на Интернету морали су са централног места да пренесу и користе *hosts* датотеку. *Hosts* датотека је централизована „равна" база.

Простор имена

Простор имена домена је хијерархијска структура (слика 18.2). Сваки чвор има ознаку (лабелу). У стаблу чвор може бити јединствено идентификован на основу свог потпуно квалификованог имена (FQDN[1]). Ознака може да има највише 63 карактера. Корен стабла је специјалан чвор без ознаке. Име домена сваког чвора стабла је скуп ознака које почињу од тог чвора идући ка корену, са тачком која раздваја ознаке. Домени на нивоу врха[2] подељени су у три категорије:

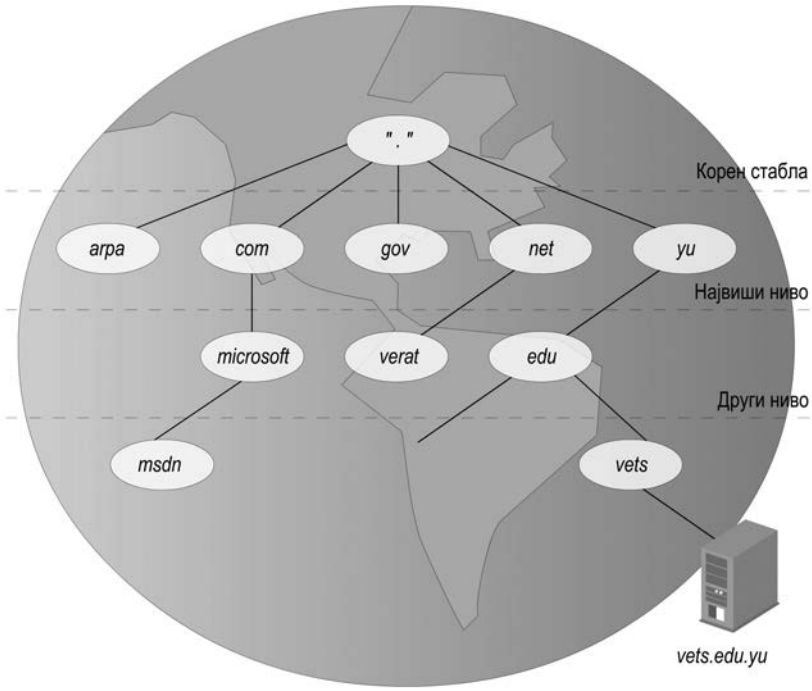
- *arpa* је специјалан домен који се користи за повезивање адресе и имена,
- седам домена означених са три карактера називају се генерички или организацијски домени,
- домени означени са два карактера називају се домени држава или географски домени. Ознаке одговарају коду државе и могу се наћи у стандарду ISO3166.

У табели 18.1 наведено је седам организацијских домена Свака грана стабла представља један DNS домен. Треба истаћи једну битну чињеницу а то је додељивање (делегирање) одговорности у оквиру система имена домена (DNS). Ниједна од целина није задужена за све ознаке у стаблу. Уместо тога једна целина води рачуна о делу стабла (доменима на нивоу врха) и делегира одговорност другима за одређену зону. Зона је део DNS стабла који се администрира независно. Многи домени другог нивоа деле своје зоне у мање. На пример високошколске установе се деле у зоне које се односе на одређене делове високошколске установе (слика 18.3). Једном када се додели[3] надлежност[4] ствар је администратора зоне да обезбеди сервер

Домен	Опис
com	Комерцијална организација
edu	Образовна институција
gov	Владине организације у САД
int	Међународне организације
mil	Војне организације у САД
net	Мреже
org	Друге организације

Табела 18.1 Ознаке за генеричке домене

[1] *Fully Qualified Domain Name*
[2] *Top level domains*
[3] *Delegated*
[4] *Authority*



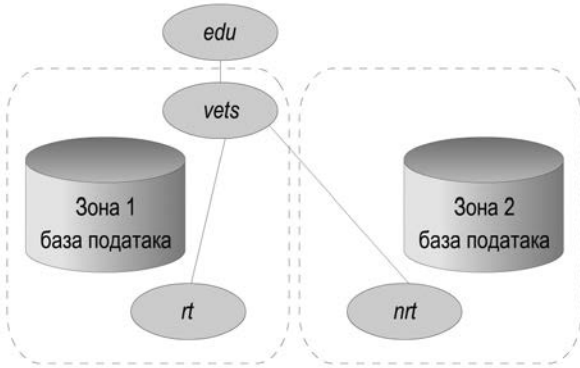
Слика 18.2 Простор имена домена

имена за ту зону. Када се нови систем инсталира у одређеној зони DNS администратор те зоне додељује му име и IP адресу и убацује ове податке у базу података сервера имена. Овде се види потреба за делегирањем. За малу организацију као што је на пример ВЕТШ једна особа може да обавља овај посао, али за Београдски универзитет то би било немогуће.

Сервер имена може да буде надлежан за једну или више зона. Особа која је задужена за зону мора да обезбеди примарни сервер имена за ту зону и један или више секундарних сервера имена. Примарни и секундарни сервери морају да буду међусобно независни и редундантни сервери тако да услуга коју пружа та зона није угрожена ако је један од система (примарни или секундарни) у квару. Разлика примарног и секундарног сервера имена је у томе што примарни сервер скупља и складишти информације а секундарни их добија од примарног. Све промене – додавање домена или рачунара обављају се на нивоу примарног сервера. Пребацивање информација од примарног сервера ка секундарном серверу назива се пренос зоне [1].

Шта ради сервер када нема информације које се од њега траже? Он мора да потражи информације од другог сервера имена. Ово је пример дистрибуираности DNS-а. Сваки сервер имена не мора да зна како да ступи у везу са свим осталим серверима имена. Уместо тога сваки сервер имена мора да зна како да ступи у везу са сервером имена корена стабла [2].

[1] *Zone transfer*
[2] *Root name servers*



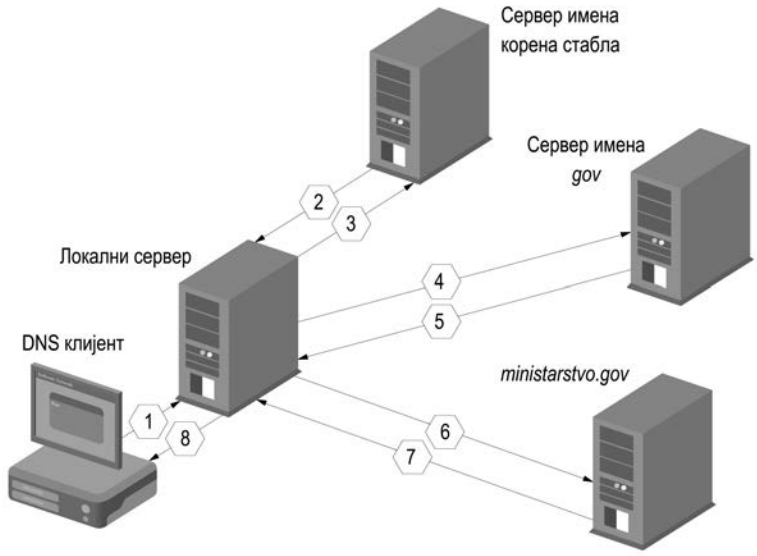
Слика 18. 3 Зоне ауторитета

Од 1993. године постоји осам сервера имена корена стабла и примарни сервери имена морају да знају IP адресе сваког од њих (не њихова DNS имена). Сервер корена стабла зна име и локацију (тј. IP адресу) надлежних сервера имена за домене другог нивоа. Ово доводи до итеративног процеса, тако да сервер коме је упућен захтев мора да ступи у везу са сервером у корену стабла.

Пример 18.1: Клијент шаље упит о *www.ministarstvo.org* локалном серверу (слика 18.4).

У итеративном упиту сервер имена коме је упит упућен враћа најбољи могући одговор. То може да буде разрешено име или референца на други сервер имена, који може да одговори на оригиналан клијентов захтев. На слици је пример итеративног упита. На овом примеру клијент у оквиру институције шаље упит локалном DNS серверу тражећи IP адресу за *www.ministarstvo.gov*.

1. Претраживач шаље упит ка свом локалном DNS серверу тражећи IP адресу за *www.ministarstvo.gov*. Локални сервер имена одговоран је за разрешавање имена и не може да у одговору клијенту укаже на други сервер имена.
2. Локални сервер имена проверава своје зоне и не проналази зону која одговара траженом имену домена. Шаље итеративни упит ка кореном (.) серверу имена .
3. Корени сервер имена надлежан је за корени домен и одговориће IP адресом сервера имена за врх *.gov* домена.
4. Локални сервер имена шаље итеративни упит за *www.ministarstvo.gov* ка серверу имена за *.gov* домен.
5. *.gov* сервер имена одговара IP адресом сервера имена који опслужује домен *ministarstvo.gov*.
6. Локални сервер имена шаље итеративни упит за *www.ministarstvo.gov* ка серверу имена одговорном за домен *ministarstvo.gov*.
7. Сервер имена за домен *ministarstvo.gov*. одговара са IP адресом која одговара рачунару *www.ministarstvo.gov*.
8. Локални сервер имена шаље IP адресу станице (рачунара) *www.ministarstvo.gov* натраг ка оригиналном претраживачу.



Слика 18.4 Итеративни упит за пример 18.1

Инверзни упити

Претраживач шаље инверзни упит, захтев серверу имена са задатком да нађе (разреши) име рачунара за познату IP адресу. У DNS простору имена не постоји веза између имена рачунара и IP адреса. Само претраживање свих домена гарантовало би коректан одговор. Да би се ово избегло направљен је специјалан домен '*in-addr-arpa*'.

Памћење времена трајања

Када сервер имена обрађује рекурзивни упит то може захтевати слање неколико упита док се не пронађе одговор. Сервер имена памти [1] све информације (IP адресе) добијене у том процесу за једно одређено време. Ово време се назива време трајања и означава се са TTL[2]. Информација о времену трајања (TTL) садржана је у повратним подацима. Када DNS сервер запамти податке, запамти и њихово време трајања и мора да започне смањивање тог времена да би знао када да податке избрише из своје меморије.

[1] *Cache*
[2] *Time To Live* - време трајања пакета (15. поглавље).

Индекс појмова

A

AAL (ATM *Adaptation Layer*), 33

ad hoc мреже, 216, 217

А/Д аналогно дигитална конвезија, 93, 124

адресирање:
- IEEE 802.3, 199
- IEEE 802.4, 208
- IEEE 802.5, 209
- IEEE 802.11, 209
- IEEE 802.16, 209
- IPv4, 277, 278
- подмрежа, 279
- IPv6, 289, 291
- на транспортном слоју, 316
- HDLC, 178, 180

ADSL (*Asymetric Digital Subscriber Line*), 132

акустички спектар
- говора, 46, 47
- музике, 46, 47

Aloha, 186,187

AMI (*Alternate Mark Inversion*) кодирање 79, 82, 185

амплитудска модулација (AM), 87, 95

амплитудски спектар, 96

аналогни сигнал, 36, 47, 60, 86

аналогни податак, 46, 48, 91-94

аналогни системи преноса, 50, 110

анвелопа, 95

ANSI (*American Natinal Standard Institute*), 8

антене
- дијаграм зрачења, 69
- изотропска антена, 69
- параболична рефлектујућа антена, 69
- појачање, 70

API (*Application Programming Interface*), 31

апликациони слој
- OSI референтног модела, 26
- TCP/IP референтног модела, 28, 334-339

апсолутни опсег нивоа снаге, 45

ARP (*Address Resolution Protoco*l), 30

ARPA (*Advance Research Project Agency*), 65

ARPANET, 27

ARQ (*Automatic Repeat Request*), 173

асинхрони пренос, 145, 146-147

ASK (*Amplitude Shift Keying*), 86, 87

ASCII (*American Standard Code of Information Interchange*), 132, 147, 151

ATM (*Asynchronous Transfer Mode*), 20, 32

ATM ћелија, 33

аудио, 46, 108

аутономни систем, 300, 302

ACK (*Acknowledge*), 169

ACL (*Asynchronous ConnectionLess*), 239-240

Б

B8ZS (*Bipolar with 8 Zero Substitution*), 85,165

BAB (*Baseband Layer),* 235

базна станица, 222, 224

балансирани пренос, 164

Баркерова (*Barker*) секвенца, 229

BGP (*Border Gateway Protocol*),

300, 305-306

Bd (*Baud*), 84

бели шум, 54

BER (*Bit Error Rate*), 83, 150

best effort, 239, 260

бинарна PSK (BPSK), 88

бинарни сигнал
- без повратка на нулу,79, 81
- биполарни, 79, 82
- диференцијално кодирани, 80, 82

бинарног експоненцијалног кашњења, 189, 245

биполарна AMI, 79, 82

Blatann Harald, 232

Bluetooth,
- архитектура, 233
- асинхроне везе (ACL), 239
- историјат, 232
- пиконет, 233-234
- примена, 234
- профил, 234
- разбацана мрежа (*scatternet*), 233
- сигурност, 243, 244
- синхроне везе (SCO), 239
- синхрони линк са успоставом везе,
- скуп протокола, 235-237
- слој основног опсега, 235, 238-239

Bluetooth SIG, 8, 215, 232

бочни опсег
- виши, 96
- нижи, 96

бод, 84

Болцманова константа, 54

BPSK (*Binary Phase Shift Keying*), 88

BPDU (*Bridge Protocol Data Units),* 260

брзина података, 78-79, 84

бродкаст (*broadcast) ,* 4,10, 74, 198

бродкаст (слање једног ка свима):
- адреса, 200, 279
- Етернет, 198
- комуникационе мреже, 10
- олуја, 269
- радио, 74

В

VDSL (*Very High Data Rate Digital Subscriber Line*), 140

веза, слој везе,
- комутација на слоју везе, 263
- уметање битова, 180
- HDLC, 177

вероватноћа грешке, 83, 150

виртуелна веза, 33, 24, 318
- двожична, 124, 140
- четворожична, 114, 125, 140

видео сигнал, 107

виртуелни канал, 16

VHF (*Very High Frequency*), 68

Г

говор,
- динамика, 47
- канал, 48
- мултиплексирање, 108-110, 114-116

- одмеравање, 93
- спектар, 48 - 50

Д

DARPA,
(*Advanced Research Project Agency*), 27
датаграм, 16-19, 28, 212, 316
dBm, 45
dBW, 45
dBV, 45
DVP (*Distance Vector Protocol),* 301
девијација,
- максимална учестаност, 98
- максимална фаза, 98
- тренутна учестаност, 98
- тренутна фаза,98

декодер, 93, 100-101
de jure стандард, 7
демодулација, 100-101
демодулатор, 86
демултиплексер, 105, 111, 114
детекција грешке, 93
de facto стандард, 7
децибел (*dB),* 43-45
дигитална претплатичка петља
- асимтрична, 132-139
- симетрична, 139

дигитални подаци, 78
дигитални сигнал, 78
- без повратка на нулу, 79, 81-82
- бинарни вишенивоски, 82
- биполарни, 79
- бифазни, 80, 82-84
- с повратком на нулу, 79
- поларни,79
- униполарни, 79

дигитални системи преноса, 114
дијаграм зрачења, 69, 74
динамика говора, 46
дискретизовање континуланих сигнала по:
- амплитуди, 95
- времену, 93

диференцијална
- Манчестер, 80
- фазна модулација (DPSK), 88-89

DIFS (*DCF Inter Frame Spacing),* 226
DM (*Discret Multitone*), 135-136
DNS (*Domain Name System*), 335-339
домен на нивоу врха (*root)*, 336
DOCSIS (*Data Over Cable Service Specification*),
142-143
DSLAM (*Digital Subscriber Line AccessMultiplexer*),
138
DSSS (*Direct Sequency Spread Spectrum),*
100, 102-103
дуплекс, 9, 36, 125, 207
DHCP (*Dynamic Host Configuration Protocol*)
286-288
DCF*(Distributed Coordination Functions*)
221-225

Е

електронска пошта, 28, 334
енкапсулација (укалупљивање), 25
EURODOCSIS, 142-143
ефективни опсег спектра, 40

Ж

жични трансмисиони медијуми, 58-68

З

захтев за аутоматским понављањем (ARQ), 173
- заустави се и чекај, 174
- иди натраг N пута, 174
- селективно понављање, 174

И

изобличење, 35-36, 52-53, 56-57

импулсна амплитудска модулација (PAM), 93

импулсна кодна модулација (PCM), 93-94

индекс фазне модулације, 98

интерференција
- електромагнетска, 60
- међусимболска (интерсимболска), 56

интерфејс, 22-25, 29, 155-165, 310

информација, 34

IRA (*International Reference Alphabet*) 47

J

јединица података,
- моста (BPDU), 260
- протокола (PDU), 25, 237
- транспортног протокола (TPDU), 319-321

јоносфера, 74

К

кабловски,
- модем, 144
- ТВ слика, 142-143

кабловски дистрибутивни систем (КДС), 141-144

Карсоново правило, 100

кашњење обраде, 20

квадратурна АМ, 90

квантизација,
- грешка, 94
- ниво, 93
- неравномерна, 94
- равномерна, 94
- шум, 94

кватернарна РМ, 89

класе A, B, C, D адреса, 278-280

клизајући прозор, 172-174, 320-321, 328-329

клијент-сервер модел, 2-3

коаксијални кабл, 59, 62-64

кôд,
- за детекцију грешке, 150
- полиноминални (CRC), 151-155

кодек, 93

кодер, 50, 93, 100

кодни мултиплекс, 101

колизија, 188-189, 245

колизиони домен, 266

кодирање, 49, 101, 78-84

комуникациони модел, 34

комутатор слоја 2, 194, 202, 205, 212, 253, 261-265

комутатор слоја 3, 265-266

комутација,
- канала, 10, 13-14, 19
- пакета, 10, 16-18, 19
- порука, 10, 14-16, 19
- рамова (FR), 20
- ћелија (ATM), 20-21

контрола грешке, 172-175

контрола тока,
- на слоју везе, 166, 172
- на транспортном слоју, 319, 328-329

контролна сума (збир), 152-155

Л

L2CAP *(Logical Link Control and Adaptation Layer Protocol), 235*-236

LLC (*Logical Level Control),* 235-237

LM (*Link Manager), 235-237*

LC (*Link Control Protocol),* 235-237

М

магистрала (*bus), 1*89, 193-194, 198, 208

максимална учестаност видео сигнала, 107

M - арни сигнал,, 56

микроталасне везе,
- земаљске, 70-71
- сателитске, 71-74

модем, 34, 49, 90-91
- за дигиталну претплатничку петљу 132-141
- за телефонски канал, 124-132
- кабловски, 141-144

модулација,
- амплитудска, 87, 95-96
- фазна,88-91, 97-100
- фреквенцијска, 87-88, 97-100
- импулсна кодна, 93
- угаона 9, 7-100

модулација са више нивоа, 89-91

модулациона брзина, 78-79, 84

модулисани сигнал, 96

модулишући сигнал, 96

мост
- алгоритам разгранатог стабла, 258-260
- изворишно рутирање, 211
- транспарентни, 256
- удаљени, 260
- учење адресе, 257
- учење уназад, 257

музика, 47

мултиплексер,
- са временском расподелом канала, 112, 117-18
- са фреквенцијском расподелом канала, 106-109

мултиплексирање по таласним дужинама, 110

Н

нелинеарна изобличења, 54

неоклопљене упредене парице, 61

нижи бочни опсег, 96

Никвистов опсег, 56

О

обнављање сигнала, 35, 51, 261-262

одабирање,
- периода, 93
- теорема, 93

одмерак (узорак, одбирак), 93

одмерци, квантизовани, 93

однос сигнала и шума, 54-55

оклопљене упредене парице, 61

оптичка влакна, 58, 59, 64-68

ортогонална фреквенцијска модулација

(OFDM), 230

OFDM (*Orthogonal Frequency Division Multiplexing),* 230

П

пакет, 16-19, 28-30, 32, 275-295

PAM (*Pulse Amplitude Modulation*), 93

површински таласи, 75

подаци, 34-35

поништавање еха (одјека), 28, 137

порука, 5, 10, 13

потврда (ACK), 169

предајник, 34-36

премашење, 20

пренос,
- аналогни, 50, 110
- дигитални, 50-51, 114-118

пренос података
- бод и бит, 78
- брзина модулације, 78 -79
- грешка (BER), 83, 150
- стандардизоване брзине, 124-126

преслушавање,53-54

пропагационо кашњење,19

пропусни опсег ,

пропусник, филтар ниских учестаности, 93

простор имена домена, 335-336

проток, 79

протокол између аутономних система (BGP), 300, 305-306

проширивање спектра директном секвенцом, 100, 102-103

проширивање фреквенцијским скакањем, 100-102

PCM (*Pulse Code Modulation*), 93

Р

равни шум, 54

радио,
- везе, 74
- опсег, 68
- радио слој (RF), 235-236
- таласи, 232

разумљивост говора, 46-47

расподела амплитуда термичког шума, 54

рачунарске мреже,
- ATM, 20, 32-33
- бежичне, 215-250
- IEEE 802, 187-214
- слојевита архитектура протокола, 22-25, 197
- стандардизација, 7-8, 213, 215, 249-250
- штафетни пренос рамова, 20

референтни модели,
- ATM, 32-33
- Novell Netware, 32
- OSI, 25-26
- TCP/IP, 27-28

рефлексија, 66, 74

рипитер (обнављивач), 35, 51, 261-262

RIF (*Routing Information Field),* 210

рутирање
- помоћу стања везе (LS), 301-303
- вектора удаљености (DV), 301-303

С

сателитске везе, 63, 69, 71-74

серијски подаци, 145

сигнализациони интервал, 89

симбол, 35, 90-91, 203-204, 206

симплекс, 36

синхронизација, 145-146

синхрони пренос, 147-149

систем имена домена, 334-335
- зона, 336-337
- простор имена, 335-336
- сервер имена, 336-337

слабљење, 43-45, 58-59

слабљење трансмисионих медијума
- бежични, 71, 74, 76
- коаксијални каблови, 64
- оптички каблови, 65, 68
- упредене парице, 61-62

слој везе,
- контрола грешке, 172, 178, 199, 206, 211, 212, 26, 227, 237, 240
- контрола тока, 166, 172
- протокол клизајућег прозора, 172-173
- HDLC протокол, 177-185

слојевита архитектура, 22-24

слој основног опсега (BAB), 235

спектар,
- амплитудски, 40
- видео сигнала, 107-108
- говора, 46-48
- дискретан, 40
- музике, 46-47

старт- стоп системи, 146-147

степен модулације, 95

SSTP (*Shielded Screen Twisted Pair*), 62

STP (*Shielded Twisted Pair*), 61- 62

SCO (*Synchronous Connection Oriented)* 239-240

Т

талас, 68-69
- ваздушни, 75
- директни, 76
- површински, 75

таласна дужина, 68-70

тачка приступа, 216

TDM (*Time Division Multiplex*), 105, 112-120

телевизија,
- учестаност носиоца слике, 107-108
- учестаност носиоца тона, 107-108
- ширина опсега, 107

телевизијски сигнал, 107

телефонска мрежа, 122

теорема одмеравања, 93

термички шум, 53-54

У

укалупљивање, 325, 321

угаона модулација
- фазна и фреквенцијска, 97-100
- индекс, 96

уметање битова (*bit stuffing),* 180

упредене парице, 60-62

услуга без успоставе везе, 121, 214, 239, 304, 309

услуга са успоставом везе, 121, 239, 309-324

успостављање везе, 13-14, 216, 227, 234, 315

UTP (*Unshielded Twisted Pair*), 61

учестаност,
- основна, 39
- тренутна, 97-98
- тренутна девијација, 97-98

Ф

фаза,
- преноса порука, 13, 322
- прекида везе, 13, 323
- успоставе везе, 13, 322

фазна модулација аналогним сигналом, 96

фазна модулација дигиталним сигналом,
- бинарна, 88
- диференцијална, 88
- кватернарна, 89

фединг, 149

фреквенцијска модулација аналогним сигналом, 98

фреквенцијска модулација дигиталним сигналом, 87

фреквенцијски померај, 88

FTP (*Foil Twisted Pair*), 62

Фуријеова трансформација, 39

FHSS (*Frequency Hoping Spread Spectrum),* 100-102

Х

Херц (Hz*), 37*

Ц

Cat 3 (ожичавање категорије 3), 62

Cat 5 (ожичавање категорије 5), 62

Cat 5E (ожичавање категорије 5E), 62

Cat 6 (ожичавање категорије 6), 62

CDM (*Code Division Multiplexing*), 101

CDMA (*Code Division Multiple Access*),101

CIDR (*Classless Inter Domain Routing*), 289, 306

CM (*Channel Manager), 237*

CRC (*Cyclic Redundancy Check*), 151-155

CSMA (*Carrier Sense Multiple Access*), 186, 188

CSMA/CA (CSMA *with Collision Avoidance*), 195-196

CSMA/CD (CSMA *with Collision Detection*), 188-195, 197

CCITT (*Comite Consultif International Telegraphique et Telephonique),* 8

Ч

чвор, 10

четворожична веза, 144, 140

чип секвенца (*chip),* 103

Ш

ширина канала, 59, 124

ширина пропусног опсега, 43

ширина спектра сигнала,
- видеа, 107-108
- говора, 46-48
- музике, 46-47

широкопојасне бежичне мреже,

(IEEE 802.16), 242-247

широкопојасне мреже, 32, 242

шум,
- импулсни, 53, 54
- квантизације, 94
- случајни, 53, 54
- термички, 53, 54

Литература

[1] Борковић В., Његован М., Темелковски М., Зафировић М.
Локалне рачунарске мреже, Научна књига,
Београд, 1986.

[2] Bradner S.,
Key words for use in RFCs to Indicate Requirement Levels,
RFC 2119, March 1997.

[3] Bound J., Carpenter B., Harrington D., Houldsworth J., Lloyd A.,
OSI NSAPs and IPv6,Ð
RFC 1888, August 1996.

[4] Васиљевић В., Гавриловић П.,
Рачунарске мреже - практикум,
ВЕТШ, Београд, 1998.

[5] Васиљевић В., Гавриловић П., Крнета Б.,
Администрација рачунарских мрежа,
ВЕТШ, Београд, 2002.

[6] Васиљевић В., Гавриловић П., Крнета Б., Мачек Н., Крстанови М.,
Приручник за администрацију рачунарских мрежа, 2. издање,
ВЕТШ, Београд, 2006.

[7] Васиљевић В., Гавриловић П., Крнета Б., Мачек Н., Крстанови М., Богојевић Б.,
Протоколи у рачунарским мрежама - приручник за лабораторијске вежбе,
2. издање,
ВЕТШ, Београд, 2006.

[8] Vasiljevic V., Krneta B., Gavrilovic P., Kuk K., Petkovic V.
Choosing the best education method - from drawing animation to cable making,
Proceedings of Hawaii International Conference on Education,
Honolulu, January 2007.

[9] Vasiljevic V., Ginic K., Petkovic V., Vasiljevic M., Miletic A., Kajgana N., Ilic V.
Difference in Students Learning Styles of Traditional and Multimedia Instructional Environment, *Proceedings of Hawaii International Conference on Education,*
Honolulu, January 2007.

[11] Gilligan, R., Nordmark E.,
Transition Mechanisms for IPv6 Hosts and Routers,
RFC 1993, April 1996.

[12] Goldman J., Rawles T.,
Applied Data Communications,
John Wiley &Sons, Inc., New York, 2001.

[13] Goralski W.,
ADSL and DSL Techologies,
McGraw-Hill, New York, 2001.Ђ

[14] Deering, S., Hinden R., Editors,
I*nternet Protocol, Version 6 (IPv6) Specification,*
RFC 1883, December 1995.

[15] Dodd A.,
The Essential Guide to Telecommunications,
Prentice Hall Professional Technical Reference,
Upper Saddle River, NJ, 2006.

[16] Драјић Д.,
Увод у статистичку теорију телекомуникација,
Академска мисао, Београд, 2003.

[17] Ilčev S.,
Global Mobile Satellite Communications,
Springer, Dordrecht, The Netherlands, 2005.

[18] Jacobson V.,
Congestion Avoidance and Control, Proceedings of SIGCOMM'88,
Computer Communication Rewiew, Vol.18, No.4, pp 314-329 (Aug), 1988.

[19] Khader M., Barns W.,
Telecommunications System and Technology,
Prentice Hall PTR, Upper Saddle River, New Jersey, 2000.

[20] Крајновић Н.,
Мултисервисне приступне мреже,
Електротехнички факултет, Београд, 2004.

[21] Couch, L.
Digital and Analog Communication Systems,
Prentice Hall, Upper Saddle River, NJ, 2001.

[22] Kurose J., Ross K.,
Computer Networking: A Top Down Approach Featuring The Internet,
Pearson Education Inc., New York, New York, 2005.

[23] Максимовић А., Шћепановић Љ., Јовановић М., Аврамовић Б.,
Карактеристике кабловског дистрибутивног система ПТТ-а "Тошин бунар"- Пилот пројекат,
Јавно предузеће ПТТ Србија, 2002.

[24] Марков Ж.,
Савремена телефонска техника,
ИРИТЕЛ, Београд, 2005.

[25] Metz C., Sackett G.,
ATM and Multiprotocol Networking,
McGraw-Hill, New York, 1996.

[26] Papadopulous C., Parlkar G. M.,
Experimental Evaluation of SunOS IPC and TCP/IP Protocol Implementation, IEEE/ACM Transaction on Networking,
Vol.1, No.2, 199-216. (Apt), 1993.

[27] Perlman R.,
Interconnections: Bridges, Routers, Swiches and Internetworking Protocols,
Addison - Wesley, Reading, Massachusec, 1999.

[28] Peterson W., Brown D.,
Cyclic codes for error detection,
Proceedings of the IRE, Volume 49, pp 228-235,1961.

[29] Петровић З.,
Енглеско-српски појмови из телекомуникација
Електротехнички факултет, Београд, 2002.

[30] Santamaria A., Lopez-Hernandez F., (Ed),
Wireless LAN Standards and Applications,
Artech House, Norwood, MA, 2001.

[31] Stallings W.,
Data and Computer Communication,
Macmillan Publishing Company, New York, 1985.

[32] Stallings W.,
Computer Network with Internet Protocol and Technology,
Pearson Education, Inc., Prentice Hall, Upper Saddle River, New Jersey, 2004.

[33] Stallings W.,
Data and Computer Communication, Pearson Education, Inc.,
Pearson Prentice Hall, Upper Saddle River, New Jersey, 2004.

[34] Стојановић И.,
Основи телекомуникација,
Грађевинска књига, Београд, 1977.

[35] Fuller V., Li T., Yu J., Varadhan K.,
Classles Inter-Domain Routing (CIDR): An Address Assignment and Aggregation Strategy,
RFC 1519, September 1993.

[36] Tanenbaum A.,
Computer Networks,
Pearson Education, Inc., Pearson Prentice Hall,Upper Saddle River,
New Jersey, 2003.

[37] Halonen T., Romero J., Melero J.,
GSM, GPRS and EDGE Performance,
John Wiley & Sons, Chichester, England, 2003.

[38] Haykin S.,
Communication Systems,
Jon Wiley & Sons, New York, 1994.

[39] Hinden R.,
IP Next generation Overview,
Connexions, March 1995.

[40] Hinden, R., Deering S.,
IPv6 Multicast Address Assignments,
RFC 2375, July 1998.

[41] Webb W.,
The Complete Wireless Communications Professional: A Guide for Engineers and Managers,
Artech House, Norwood, MA, 1999.

[42] Webb W.,
The Future of Wireless Communications,
Artech House, Norwood, MA, 2001.

ISBN 978-86-85081-96-5

Висока школа електротехнике и рачунарства
струковних студија