

# 31. Капацитет канала - Никвистов опсег и Шенонова једначина за капацитет канала (документа 5\_6\_sajt.pdf, поглавље 5.4, једначине 5.6 и 5.7)

## 5.4 Капацитет канала

Видели смо да постоји више параметара који изобличавају или оштећују сигнал. За дигиталне сигнале поставља се питање до колико ова погоршања 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) којом се подаци могу размењивати;
- Опсег - односи се на опсег предајног сигнала који је ограничен предајником и природом трансмисионог медијума и изражава се у циклусима у секунди или херцима (Hz);
- Сметња - односи се на средњи ниво сметње на комуникационом путу;
- Вероватноћа грешке - односи се на учестаност појављивања грешака. Под грешком се сматра када се прими „1” а послато је „0” и обрнуто.

Проблем је следећи: комуникациона опрема је генерално скупа и што је њен пропусни опсег већи виша је цена. Поред тога сви доступни преносни канали су ограниченог пропусног опсега. Ограничења су полсецица 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 задати опсег. За дигиталне податке, ово значи да ми 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 сигнала. Никвист је формулисао да уколико се сигнал преноси брзином  $2B$  онда, сигнал учестаности која није већа од  $B$  је довољан да пренесе ову брзину. На други начин можемо се казати: за задати опсег  $B$ , највећа брзина која се може пренети је  $2B$ . Ова ограничења су последица међусимболске интерференције као што су изобличење услед кашњења.

У претходном параграфу користили смо термин  $1073$  брзина сигнала. Уколико је сигнал који треба пренети бинаран (два ж напонска нивоa), 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  $3100$ Hz. Онда је капацитет  $C$  канала  $2B = 6200$ b/s. Као што ћемо видети у поглављу ? могуће је користити сигнале са више од два напонска (струјна) нивоa; то значи да сваки сигнализациони елеменат може да представља више од једног бита. Са вишенивоском сигнализацијом Никвистова формула постаје:

$$C = 2B \log_2 M = 2B \ln M \quad (5.6)$$

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

За задату ширину (пропусни опсег) канала, брзина се може повећати са увећањем броја различитих сигнализационих ж 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 други погоршања на преносној линији ће ограничити стварне вредности броја  $M$  напонских нивоa.

## Шенонова једначина за капацитет канала

Никвистова формула указује да уколико је све друго једнако, удвостручавањем ширине опсега удвостручава се брзина података. Посматрајмо везу између брзине преноса података и шума и вероватноће грешке. Присуство шума може да оштети један или два бита. Уколико се брзина података повећава, трајање битског интервала се смањује па се повећава број битова на који сметња (шум) има утицај. То значи да за задати ниво сметње, што је већа брзина података то је већа вероватноћа грешке. Слика 5.9 графички приказује ову релацију. Уколико се брзина података повећава, онда се више битова појављује у интервалу када је шум великог интензитета (у шпигецима) и због тога се јавља више грешака. Сви претходно набројани параметри могу се повезати у формулу коју је развио математичар Клод Шенон. Као што смо видели, што је већа брзина података то више штете може да направи нежељена сметња. За задати ниво сметње, за очекивати је да ће

већа снага сигнала повећати способност да су пријемни подаци исправни у присуству шума. Кључни параметар у овој анализи су однос сигнала и сметње (S/N) који представља однос између снаге сигнала и снаге шума присутног у тој специфичној тачци у преносу.

Типично, однос се мери на пријемној страни, пошто се у тој тачци обрађује сигнал и из њега извлаче подаци. Уобичајено се овај однос (једначина 5.5) мери у децибелима (dB) и указује за колико је сигнал већи од шума. Већи однос S/N значи квалитетнији сигнал и потреба за мањим бројем рипитера. Однос сигнала и шума је важан за пренос дигиталних података пошто он поставља горњу границу брзине података која се може постићи. Шенон је показао да се максимални капацитет канала, изражен у битима у секунди, може исказати једначином:

$$C = B \log_2(1+S/N) = B \ln(1+S/N) \quad (5.7)$$

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 достићи. У пракси се може постићи много мањи капацитет. Један од разлога за то је што једначина претпоставља бели (термички) шум. Нису укључени ни импулсни шум, ни изобличење услед слабљења или кашњења. Капацитет дефинисан једначином (5.7) назива се капацитет без грешке. Може се још нека додатна анализа спровести. За задати ниво шума чини се да ће се брзина података повећати повећавањем снаге сигнала. У ствари повећавањем снаге сигнала ефекат нелинеарности система се повећава, што доводи до повећања интермодулационог шума. Такође, пошто је реч о белом шуму, што је пропусни опсег већи, то се више шума додаје систему. Тако са порастом B однос S/N се смањује.

## 32. AMI и технике скрембловања (докуменат 7\_06\_1\_d.pdf, поглавље 7.3, слика 7.6)

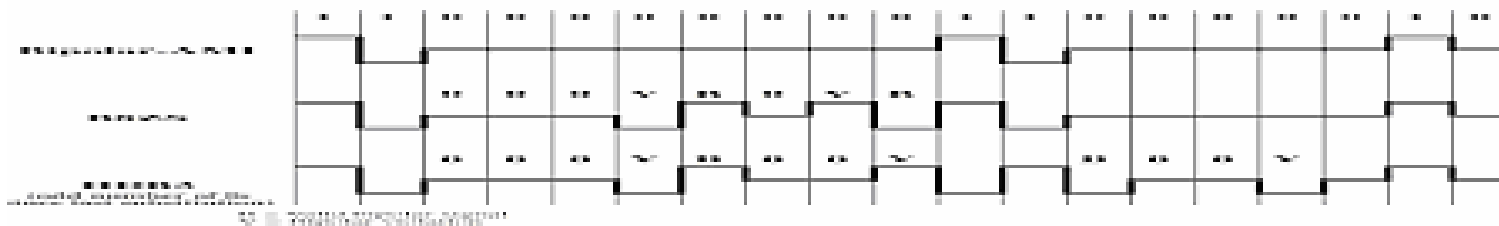
### 7.3 Технике уметања (скрембловања)

Иако су бифазне технике широко распрострањене у локалним рачунарским мрежама не користе се у комуникационим системима на већим удаљеностима. Основни разлог је велика сигнализациона брзина у односу на брзину података. У комуникационим системима на већим удаљеностима овакава неефикасност је значајна по цени.

Други приступ би био употреба неке од техника скрембловања. Идеја је следећа: секвенце које би довеле до константног напонског нивоа на линији се замењују секвенцама које ће обезбедити довољан број транзиција тако да пријемни такт сигнал задржи синхронизацију. Уметнуту секвенцу пријемник треба да препозна и замени је оригиналном секвенцом података. Захтеви који се постављају пред ову технику су следећи:

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

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



Слика 7.6 Технике кодирањ B8ZS, HDB3 и биполарна AMI

Техника B8ZS је заснована 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 два поремећаја кода, која не могу да буду проузрокована шумом или смањењем квалитета сигнала у преносу. Пријемник препознаје узорак и интерпретира октет као да се састоји од свих нула.

Кодна шема HDB3<sub>3</sub> (табела 7.3) је такође заснована на AMI коду. Поворка од четири нуле се замењује секвенцом од једног или два импулса. У сваком од случајева четврта нула је замењена „поремећајем код”.

<sup>1</sup> Биполарна са заменом 8 нула (*Bipolar with 8 zeros substitution*). уобичајено се користи у северној Америци.

<sup>2</sup> Узорак сигнала који није дозвољен код AMI кода.

<sup>3</sup> Биполарна високе густине са 3 нуле (*High Density Bipolar 3 Zeros*). Уобичајено се користи у Европи и Јапану.

Потребно је одређено правило које обезбеђује да су узастопни „поремећаји” различитог поларитета како се не би појавила једносмерна компонента. То значи да уколико је последњи поремећај 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.

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

Табела 7.2 Правило код HDB3 кода

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 спектар око учестаности која је једнака половини брзине података. Ови кодови су погодни за пренос података великих брзина .

## 33. Пример HDLC процедуре (докуменат **11\_06\_l\_d.pdf**, поглавље 10.4, слике 11.8 стр.180, слика 11.7 стр 187)

### 11.4 Бит оријентисани протоколи

Бит оријентисани протоколи направљени су да задовоље широк опсег захтева слоја везе које укључују:

- тачка - тачка и тачка више тачака везе,
- полудуплекс (наизменични двосмерни) и потпуни дуплекс (два смера симултане) операције,
- примарну, секундарну (нпр. станица<sup>2</sup> - 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 (а).

Задатак ових протокола је да обезбеде следеће циљеве:

- независност од кода - корисник би требало да буде у могућности да употреби било који код 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 подељена у поља, при чему свако поље има специфично значење. Позиција поља је фиксирана у односу на ограничавааче рама. Кодирано управљачко поље је оно у коме различита комбинација бита има специфично значење и у коме се користе потпоља чије значење зависи од његове позиције. Већи број сличних бит-оријентисаних протокола је достигло широку примену.

Најзначајнији међу њима су:

- Протокол HDLC<sub>1</sub> је развила ISO<sub>2</sub>;
- Протокол LAP-B<sub>3</sub> развила је ADCCP<sub>4</sub> - преузела CCITT као део X.25 стандарда за мреже са комутацијом пакета;

- Протокол SDLC<sup>5</sup> користи IBM. Није га стандардизовала ниједна од организација за стандардизацију али се доста користи.

Не постоји значајна разлика између HDLC и LAP-B. LAP-B је подскуп HDLC. Протокол SDLC је такође подскуп протокола HDLC. У следећем поглављу анализираћемо протокол HDLC.

<sup>1</sup>Data Link

<sup>2</sup>Користи се термин станица или хост

## 11.6 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 (линк). 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<sup>6</sup> 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<sup>7</sup> конфигурација. Користи само тачка -тачка начин рада. Ова конфигурација састоји се од две мешовите станице. Подржава и потпуни дуплекс и полудуплексни пренос.



а) Асиметрична конфигурација

б) Симетрична конфигурација  
Слика 11.7 HDLC конфигурација везе

Постоје три врсте начина рада HDLC протокола:

- Нормални начин са одговором NRM<sup>1</sup>. 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<sup>2</sup>. Ово је симетрична конфигурација. Било која комбинована станица може да иницира пренос без дозволе друге комбиноване станице.
- Асинхрони начин са одговором ARM<sup>3</sup>. 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. NRM се користи на линијама са више секундарних станица. Примарна станица шаље упит (полира) за сваку секундарну станицу. NRM се често користи у тачка-тачка везама, поготову ако је везан терминал или нека друге периферија за рачунар. Асинхрони балансни начин рада омогућава много ефикасније коришћење, потпуни дуплекс тачка- тачка везе. ARM се ретко користи.

### Пример HDLC процедуре

У овом поглављу дат је пример HDLC (LAP\_B) рада за пренос без грешке (слика 11.7) и случај када у току преноса дође до грешке (слика 11.8).

| Време          | →                |                |                                   |                                   |                          |                                   |                                   |                          |
|----------------|------------------|----------------|-----------------------------------|-----------------------------------|--------------------------|-----------------------------------|-----------------------------------|--------------------------|
|                | n                | n+1            | n+2                               | n+3                               | n+4                      | n+5                               | n+6                               | n+7                      |
| Станица А шаље | SABM<br>B<br>P=1 |                | I<br>B<br>P=0<br>N(S)=0<br>N(R)=0 | I<br>B<br>P=1<br>N(S)=1<br>N(R)=0 |                          |                                   |                                   | RR<br>A<br>F=1<br>N(R)=2 |
| Станица В шаље |                  | UA<br>B<br>F=1 |                                   |                                   | RR<br>B<br>F=1<br>N(R)=2 | I<br>A<br>P=0<br>N(S)=0<br>N(R)=2 | I<br>A<br>P=1<br>N(S)=1<br>N(R)=2 |                          |

Легенда:

| Ознака | Опис                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| I      | Информациона рам                                                                                                                                                                                                                                                                                                                                                                      |
| N      | Станица А шаље SABM команду са Р битом постављеним на 1                                                                                                                                                                                                                                                                                                                               |
| n+1    | Станица В одговара са UA рамом који се користи као одговор са F битом постављеним на 1.                                                                                                                                                                                                                                                                                               |
| n+2, 3 | Станица А шаље информациони рам са секвенцијским бројевим 0 (P=0) и 1 (P=1)                                                                                                                                                                                                                                                                                                           |
| n+4    | Станица В потврђује исправан пријем А слањем одговора RR, са 2 у пољу за пријемни секвенцијски број                                                                                                                                                                                                                                                                                   |
| n+5, 6 | Станица шаље В информациони рам са секвенцијским бројевим 0 (P=0) и 1 (P=1). У тренутку Р бит је био постављен на 0, што је указивало да то није последњи пакет и да В не треба још да шаље потврду. У n+2 тренутку Р бит је био постављен на 1. На тај начин се указује станици В да је то последњи информациони рам и да треба да пошаље потврду. Види се да се је отвор прозора 2. |
| n+7    | Станица А потврђује В рамове са секвенцијским бројевима 0 и 1 са N(R)=2 и F=1.                                                                                                                                                                                                                                                                                                        |

Слика 11.7 Асинхрони балансни начин рада ABM са полудуплексним протоком података (коришћењем P/F проверама) без грешке

| Време  | →                                 |                                   |                                   |                          |                                   |                                   |                                   |                          |
|--------|-----------------------------------|-----------------------------------|-----------------------------------|--------------------------|-----------------------------------|-----------------------------------|-----------------------------------|--------------------------|
|        | n                                 | n+1                               | n+2                               | n+3                      | n+4                               | n+5                               | n+6                               | n+7                      |
| А шаље | I<br>B<br>P=0<br>N(S)=6<br>N(R)=4 | I<br>B<br>P=0<br>N(S)=7<br>N(R)=4 | I<br>B<br>P=1<br>N(S)=0<br>N(R)=4 | RR<br>B<br>F=1<br>N(R)=4 | I<br>B<br>P=0<br>N(S)=7<br>N(R)=4 | I<br>B<br>P=0<br>N(S)=0<br>N(R)=4 | I<br>B<br>P=1<br>N(S)=1<br>N(R)=4 |                          |
| В шаље |                                   |                                   | REJ<br>A<br>P=1<br>N(R)=7         |                          |                                   |                                   |                                   | RR<br>A<br>F=1<br>N(R)=2 |

Легенда:

| Ознака    | Опис                                                                                                                                                                                                      |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| n, n+1, 2 | Станица А шаље информациони рам са секвенцијским бројевим 0, 1 (P=0) и 2 (P=1)                                                                                                                            |
| n+2       | Станица В детектује грешку у раму 7, и одмах шаље RR ( <i>Reject</i> ) рам са пријемним секвенцијским бројем 9. Уочимо коришћење адресног поља и Р бита да би се информациони рам употребио као командни. |
| n+4       | Станица А враћа RR                                                                                                                                                                                        |
| n+4, 5, 6 | Станица А поново шаље оштећени рам (секвенцијски број 7) и наставља са слањем                                                                                                                             |
| n+7       | Станица В потврђује исправан пријем рамове са секвенцијским бројевима 7, 0 и 1 са N(R)=2 и F=1.                                                                                                           |
| n+7       | Станица А потврђује В рамове са секвенцијским бројевима 0 и 1 са N(R)=2 и F=1.                                                                                                                            |

Слика 11.8 Опоравак од грешке код LAP\_B протокола.

## 34. Упоређивање статичког и динамичког метода (*arhitektura lokalnih racunarskih mreza.pdf* објашњење стр. 1,2, једначина 12.2)

### 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 архитектура 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<sub>1</sub> и TDM<sub>2</sub>) и динамички (ALOHA<sub>3</sub>, CSMA<sub>4</sub>, 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, додељени му фреквенцијски опсег је једноставно 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. Однос између саобраћаја највећег интензитета и просечног саобраћаја обично је 1000:1.

<sup>1</sup> FDM - фреквенцијски мултиплекс (8. поглавље)

<sup>2</sup> TDM - временски мултиплекс (8. поглавље)

<sup>3</sup> ALOHA (здро на Хавајском) - станица шаље када има пакет за слање.

<sup>4</sup> CSMA (*Carrier Sense Multiple Access*) - станица прво ослушкује преносни медиј, ако је слободан шаље.

<sup>5</sup> *Bursty*

Лоше карактеристике статичког FDM-а могу показати следећом анализом [1]. Пођимо од средњег времена  $u1082$  кашњења<sup>1</sup>, T, канала чији је капацитет Cb/s., са брзином пристизања  $\lambda$  рамова/сек. и са средњом дужином од 1/ $\mu$  битова/раму. Овим параметрима брзина пристизања пакета је  $\lambda$ , а брзина услуге (сервиса)  $\mu$ C. По теорији редова за случај Поасонове расподеле времена пристизања и сервисирања пакета добија се:

$$T = 1/(\mu C - \lambda) \quad (12.1)$$

На пример ако је C=100Mb/s, средња дужина пакета 1/ $\mu$  је 10000 битова, и брзина пристизања пакета  $\lambda$  је 5000 рамова/сек., 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 бита пренесе кроз рачунарску мрежу брзине 100Mb/s добијамо (нетачан) одговор од 100 $\mu$ s. Овај резултат се добија само под условом да нема „надметања” за приступ каналу.

Поделитемо сада канал на N независних делова (подканала). Капацитет сваког дела је C/N b/s. Средња брзина пакета података који су спремни (пристигли) за слање за сваки подканал је  $\lambda/N$ . Средње време кашњења постаје:

$$T_{FDM} = 1/[(\mu C/N) - (\lambda/N)] = N/(\mu C - \lambda) = NT \quad (12.2)$$

Средње кашњење T 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 200 $\mu$ s на 2ms.

Види се да ни једна 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 u1084 медијуму.

Генерално посматрано, постоје два механизма приступа: по унапред одређеном редоследу<sup>2</sup> и сукобљавањем<sup>3</sup>. У рачунарским мрежама саобраћај је неравномерно расподељен у времену великог интензитета и кратког трајања. Доказано је да је ефикасније користити један канал велике брзине коме се приступа међусобним сукобљавањем (релација 12.2).

<sup>1</sup> Дефинише се као време потребно да рачунарска мрежа обезбеди испоруку податка спремног за слање одредишту

<sup>2</sup> *Polling, token passing*

<sup>3</sup> *Contention*

## **35. Протокол за управљањем слојем везе (*arhitektura lokalnih racunarskih mreza.pdf* поглавље 12.12 слика 12.22)**

### **12.2 Стандард IEEE 802 за локалне рачунарске мреже**

Локалне рачунарске мреже по стандарду IEEE 802<sup>3</sup> 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<sup>4</sup> су оптимизоване за већа растојања, него локалне рачунарске мреже, нпр. неколико блокова зграда, до целих градова.

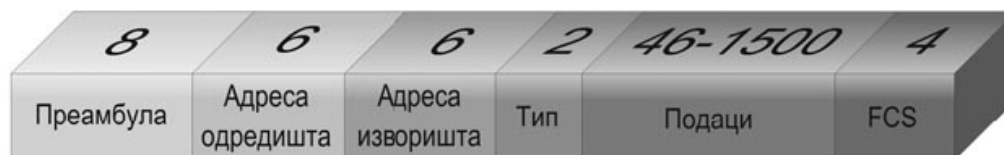
Слика 12.11 Однос архитектуре LAN&MAN/RM<sup>5</sup> и OSI/RM<sup>6</sup>.

Референтни модели IEEE802 направљени су после OSI референтног модела. С тандарди IEEE802 укључују функционалност најнижа два слоја (физички слој и слој везе) OSI

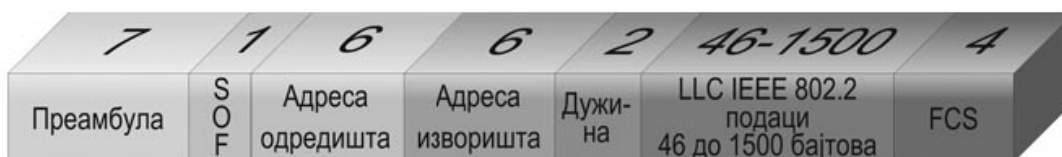
Локалне рачунарске мреже

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 и OSI/RM. Организација IEEE је објавила више стандарда за локалне рачунарске мреже познатих као серија<sup>1</sup> IEEE802. Стандарде које ћемо у овом уџбенику анализирати су:

- IEEE802.1Q - дефинише архитектуру за виртуелне локалне рачунарске мреже са премештавањем<sup>2</sup>.
- IEEE802.2 - управљање слојем везе<sup>3</sup>.
- IEEE802.3 - CSMA/CD метод приступа трансмисионом медијуму и спецификација физичког слоја.
- IEEE802.4 - магистрала са жетоном<sup>4</sup> као метод приступа трансмисионом медијуму и спецификација физичког слоја.
- IEEE802.5 - прстен са жетоном<sup>5</sup> као метод приступа трансмисионом медијуму и спецификација физичког слоја.
- IEEE802.11 - метод за приступ медијуму код бежични локалних рачунарских мрежа и спецификација физичког слоја.
- IEEE802.15 - метод за приступ медијуму код бежични локалних рачунарских мрежа<sup>6</sup> и спецификација физичког слоја.
- IEEE802.16 - стандардни интерфејс за широкопојасне бежичне системе градских подручја<sup>7</sup>.



Ethernet II рам одатака



802.3 рам података

Слика 12.12 Формати Етернет и IEEE 802.3 рамова

## 36. Временски интервали између рамова (*bezične racunarske mreze.pdf*, страна 12, сл. 13.10)

### Централизоване координационе функције

Други начин приступа медијуму код IEEE802.11 система је помоћу централизоване координационе функције PCF. Базна станица<sup>1</sup> шаље упит (полира) другим станицама 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<sup>2</sup> рам 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<sup>3</sup> 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

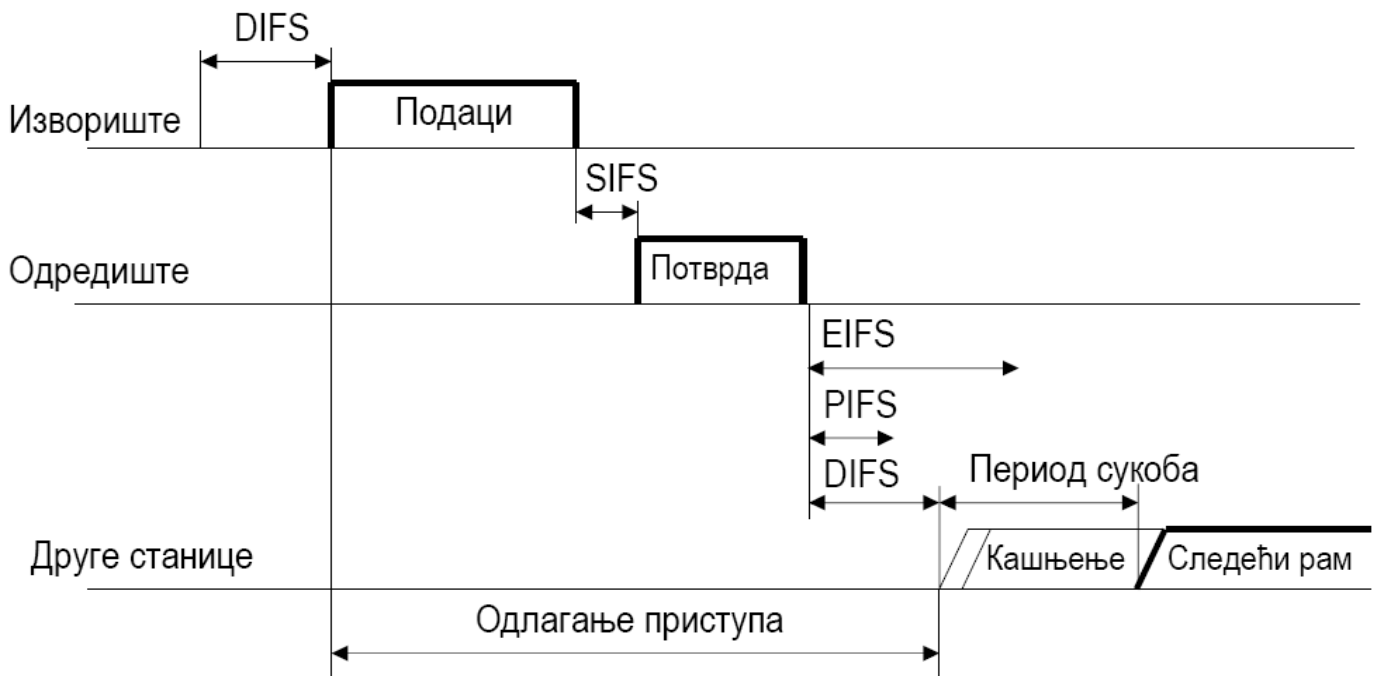
Стандард IEEE802.11 је предвидео коегзистенцију оба начина рада: централизованог PCF и дистрибуираног DCF у једној ћелији. Један од механизма су дефинисана времена између рамова. Пошто се један рам пошаље чека се одређени временски интервал пре него што било која станица може да пошаље следећи рам. Дефинисана су четири временска интервала (слика 13.10):

**1.** Најкраћи интервал између рамова SIFS<sup>4</sup> 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 податка. 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<sup>1</sup>. Овај механизам 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<sup>2</sup> 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<sup>3</sup> 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.



Слика 13.10 Временски интервали између рамова код 802.11

## 37. Скуп протокола код Bluetooth система (*bezicne racunarske mreze.pdf*, стр. 23, 24, сл. 13.14)

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 базе станице HSP и профил Fax Profile који су изнад серијског профила SPP. Навешћемо један пример: ако треба синхронизовати 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 2 код Bluetooth система

Језгро Bluetooth система обухвата четири најнижа слоја и одговарајуће протоколе који су у Bluetooth спецификацији, као и заједнички протокол за откривање услуга SDP3 и свеобухватни генерички профил приступа GAP4. 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 13.13. На слици су обележени слојеви са одговарајућим протоколима:

- нижи слојеви са одговарајућим протоколима: радио слој RF5, слој основног опсега BAW6, аудио слој, протокол за управљање везом LC7, протокол за надзор везе LM8, протокол за управљање и прилагођавање везе L2CAP9,
- виши слојеви: подаци DT10, слој са различитим протоколима везаним за различите интерфејсе (TCS11, RFCOMM12, SDP13) и апликације AP14, и
- управљање CN15.

1 Користи се и термин *Bluetooth Enabled*.

2 *Protocol stack*

3 *Service Discovery Protocol*

4 *Generic Access Profile*

5 *Radio*

6 *Baseband*

7 *Link Control Protocol*

8 *Link Manager*

9 *Logical Link Control and Adaptation Protocol*

10 *Data*

11 *Telephony Control Protocol Spec* - бит оријентисани протокол који дефинише сигнализацију при

успостави/раскидању позива између станица.

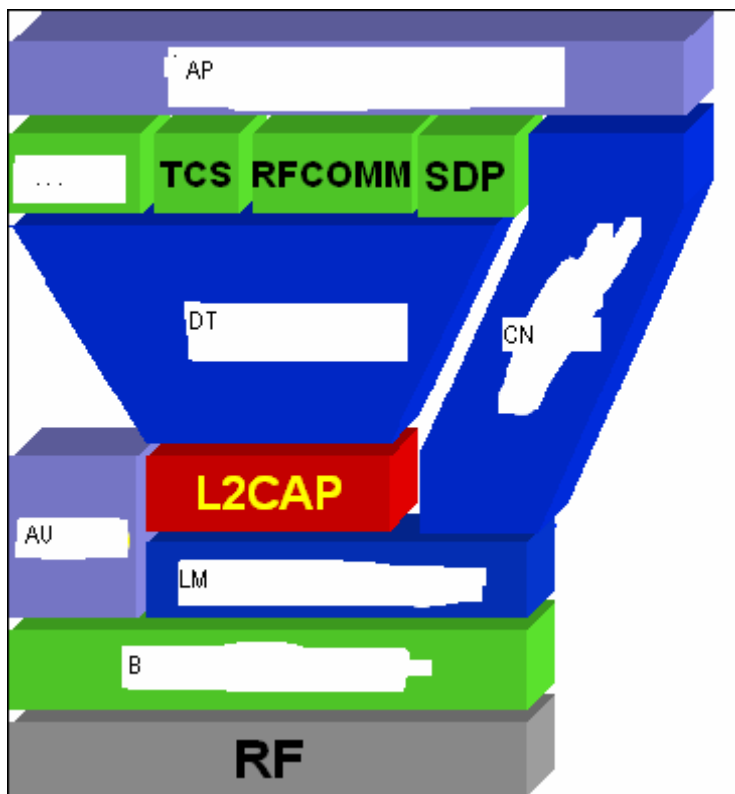
12 *Serial cable emulation protocol* - протокол за емулацију серијског кабла.

13 *Service Discovery Protocol* - протокол за откривање сервиса.

14 *Application*

15 *Control*

Бежичне рачунарске мреже



Слика 13.14 Поређење архитектуре OSI, IEEE802 и Bluetooth система

Детаљнија архитектура језгра Bluetooth система представљена је на слици 13.14. Најнижа три слоја груписана су у подсистем који се среће под називом Bluetooth контролер. Остатак система укључујући L2CAP1 сервис 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 SAP2. Услуге могу бити разврстане у две групе: управљачке, које се означавају као С3 раван, и корисничке које се означавају као U4 раван. Прва група води рачуна о успостављању и раскидању канала и веза, а друга о подацима који се том везом размењују.

Сервисни интерфејс 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 хост - контролер HCI5. Његове приступне тачке сервиса означене су на горњој ивици контролера подсистема. Имплементација ових стандардних интерфејса сервиса је опциона.

- 1 Logical Link Adaptation Protocol
- 2 Service Access Point
- 3 Control
- 4 User
- 5 Host to Controller Interface

## 38. Заглавље IPv4 пакета (*Internet\_protocol.doc*, поглавље 15.1, слика 15.1)

### 15.1 Заглавље IP пакета верзије 4

На слици 15.1 приказано је заглавље IP пакета верзије 4 (IPv4). IP пакет се састоји од дела за заглавље и дела за текст. Заглавље има фиксан део од 20 бајтова и део променљиве дужине као опциони. Формат заглавља приказан је на слици 15.1. Он се шаље следећим редоследом: слева надесно, са битом највеће тежине поља верзија на првом месту.



Слика 15.1 Формат IPv4 заглавља

Верзија<sup>1</sup> (4 бита). Текућа верзија протокола је 4, и означава се са IPv4. Постоји и нова верзија IPv6.

Дужина заглавља<sup>2</sup> (4 бита). Пошто дужина заглавља није константна, поље у заглављу, IHL, 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 превише мало чинећи опцију бескорисном.

Тип сервиса<sup>3</sup> (8 бита). Ово поље дозвољава хосту да укаже подмрежи коју врсту сервиса 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 TOS и данас DS/ECN. TOS садржи (слева надесно) следећа поља:

- *Precedence* тробитно поље, указује на приоритете од 0 (нормалан) до 7 (мрежни управљачки пакет);
- четири бита која дозвољавају хосту да специфицира шта му 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 нормалан сервис. 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, 1349). TOS већина новијих имплементација не користи.

Поље DS/ECN подељено је на следећи начин:

- првих 6 битова DS<sup>4</sup> одређује различите нивое квалитета сервиса (QoS). Могуће је дефинисати 64 (2<sup>6</sup>) класа саобраћаја (RFC 2474)
- друга 2 бита односе се на загушење саобраћај ECN<sup>5</sup>.

Укупна дужина<sup>6</sup> (16 бита). Укупна дужина укључује све у пакету и заглавље и податке. Максимална дужина је 65 535 бајтова. За сада горња граница је прихватљива, али са будућим гигабитским мрежама биће потребни већи пакети.

Идентификација<sup>7</sup> (16 бита). Поље је потребно да би омогућило удаљеном хосту 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 делим DF<sup>8</sup> (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. Постављем пакета са DF битом пошиљалац зна да ће пакет стићи на одредиште као једна целина, иако 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<sup>9</sup> (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<sup>10</sup>.

Време постојања<sup>11</sup> (8 бита). 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 га 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, изворишном хосту, шаље се ICMP пакет. Ова особина спречава кретање пакета у недоглед.

Протокол<sup>12</sup> (8 бита). Када мрежни слој споји цео пакет потребно му је да зна шта да ради са пакетом. Поље протокола указује који протокол је задужио IP да му пренесе податке. TCP је једна могућност, друга UDP, итд. Нумерисање протокола је глобално кроз цео Интернет и дефинисано је стандардом RFC1700.

Контролни збир заглавља<sup>13</sup> (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. ICMP, IGMP, UDP и TCP/IP користе исти алгоритам за прављење контролног збира (RFC 1071). 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 RFC 1141.

Адреса изворишта<sup>14</sup> (32 бита). Указује на адресу мреже и адресу хоста (слика 15.1).

Адреса одредишта<sup>15</sup> (32 бита). Указује на адресу мреже и адресу хоста (слика 15. 1).

Опције<sup>16</sup> (променљиве дужине). Ретко се користе и не подржавају их сви рутери и рачунари. У пољу опције за сада је дефинисана:

- сигурност и ограничења (за војне примене RFC1108),
- записивање руте (рутери уписују своје IP адресе),
- записивање времена (рутери уписују време и своју IP адресу),
- даје комплетан пут који пакет треба да следи,

---

<sup>1</sup> Version

<sup>2</sup> Internet Header Length

<sup>3</sup> Type Of Service

<sup>4</sup> Differentiated Services

<sup>5</sup> Explicit Congestion Notification

<sup>6</sup> Total Length

<sup>7</sup> Identification

<sup>8</sup> Don't Fragment

<sup>9</sup> More Fragments

<sup>10</sup> Total length Field

<sup>11</sup> Time to Live

<sup>12</sup> Protocol

<sup>13</sup> Header Checksum

<sup>14</sup> Source Address

<sup>15</sup> Destination Address

<sup>16</sup> Options

- даје листу рутера које пакет не треба да заобиђе.
- Додатак<sup>17</sup> (променљиве дужине). Користи се да обезбеди да је дужина заглавља умножак од 32 бита.

## 39. IPv6 (*Internet\_protocol.doc*, поглавље 15.1, поглавље 15.6 и 15.7, слика 15.13)

### 15.6 Интернет протокол верзије 6

Броја рачунара који је повезан на Интернет расте изузетно великом брзином. У јулу 2005. год Интернет је користило скоро 350000000 станица<sup>18</sup>. Са IPv4 величином адресног поља могло би да се обезбеди  $2^{32}$  различитих адреса што је десет пута више него број станица који тренутно користи Интернет. Разлог због којих IPv4 адресни простор постао неодговарајућа 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 те мреже може бити неискоришћен, али ако се посматра ефекат на IP адресни простор онда када се искористи број мреже искоришћене су и све адресе за станица у оквиру те мреже;
- Адресни простор верзије IPv4 подељен је у мреже класа А, В и С 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) повезане 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;
- Проширивање области у којима се користе TCP/IP протоколи као што су POS<sup>19</sup> терминали или кабловска телевизија доводе до повећања потражње за IP адресама;

Видимо је да су потребе за већим адресним простором довела 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 механизмима подршке у управљању саобраћајем. Проблеме које IPv4 протокола није мога да разреши су и:

- У чворовима (рутерима) Интернета (нарочито у окосницама) 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 сервиса и механизми приоритета. Код верзији IPv4 механизми који обезбеђују квалитет сервиса нису били јасно дефинисани и веома су се мало користили;

Организација IETF<sup>20</sup> је као одговор на постојеће пробелеме<sup>21</sup> 1992. год. започела процедуру за нову верзију Интернет протокола. До данас су објављени бројни документи међу којима су најважнији: RFC 1752<sup>22</sup>, RFC 2460<sup>23</sup>, RFC 2373<sup>24</sup>

---

<sup>17</sup> *Padding*

<sup>18</sup> *ISC Internet Domain Survey*, Jan 2004, <http://www.isic.org>

<sup>19</sup> *Point Of Sale*

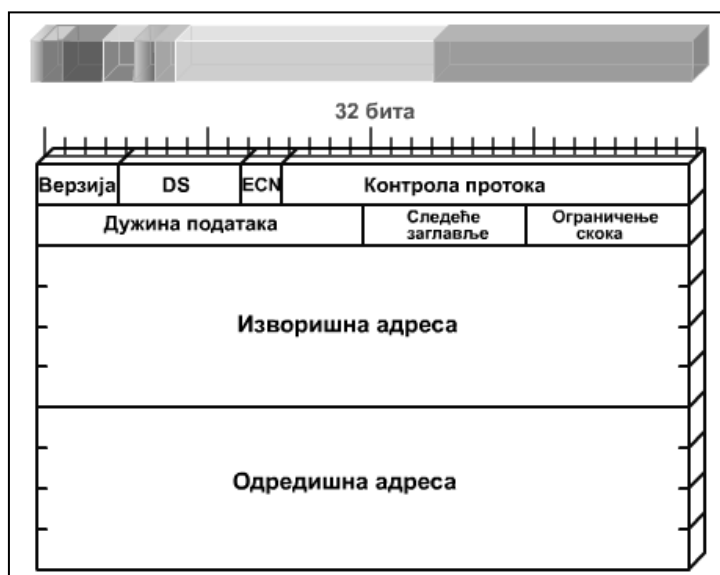
<sup>20</sup> *Internet Engineering Task Force*

Разлике између верзија IPv6 и верзије IPv4 су следеће:

- Дужина IPv6 је повећа на 40 бајтова (са 20 бајтова IPv4) и садржи две адресе од по 16 бајтова (изворишта и одредишта). Заглавље IPv4 (слика 4.22) садржи две адресе од по 4 бајта иза кога је 12 бајтова управљачих информација и обично опциони подаци. Проширење адресног простора је за фактор  $2^{96}$ . Израчунато је да ово омогућава  $6 \times 10^{23}$  јединствених адреса по квадратном метру површине Земље<sup>25</sup>. 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 смањењивањем броја управљачких информација и измештање опционих података из заглавља. Опције IPv6 смештене су у посебна заглавља која се постављено између заглавља IPv6 и заглавља транспортног слоја. Највећи број додатних заглавља рутери на путу који пакета прелази се не анализирају;
- Повећана флексибилност адресирања: IPv6 укључује и концепт адресе један ка једном од групе (еникаст) Пакет се испоручује само једним путем. Перформансе рутирања један ка групи (мултикаст) су унапређене тако што је додат опсег поља за мултикаст адресе;
- Подршка у додели ресурса: IPv6 омогућава означавање пакета за различите брзине проток ако то пошиљалац тражи. На располагању су и додатне услуге у саобраћају када се преноси видео сигнал<sup>26</sup>.

### 15.7 Формат заглавља протокола IPv6

Заглавље протокола IPv6 је поједностављено у односу на заглавље претходника IPv4. Формат заглавља IPv6 предствљен је на слици 15.13.



Слика 15.13 Формат IPv6 заглавља

Састоји се од следећих поља:

- Верзија (дужине 4 бита): верзија Интернет протокола, вредност је 6;
- DS/ECN<sup>27</sup> (дужине 8 бита): првих шест бита поља односно се на поље DS<sup>28</sup>, а остала 2 бита резервисана су за обавештења о загушењу ECN<sup>29</sup>;

<sup>21</sup> IP Address Exhaustion Problem

<sup>22</sup> Сматра се прекретницом у дефинисању новог протокола означеног са IPrng. (Recommendation for the IP Next Generation).

<sup>23</sup> Односи се на свеобухватну спецификацију протокола IPv6.

<sup>24</sup> Односи се на структуру адресирања IPv6.

<sup>25</sup> [Hind95]

<sup>26</sup> Real-time video

<sup>27</sup> 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.

<sup>28</sup> Differentiated services

<sup>29</sup> Explicit congestion notification

- Ознака тока (дужине 20 бита): може користити станица да обележи оне пакете са којима рутери треба да поступају на посебан начин у оквиру мреже;
- Дужина података (дужине 16 бита): дужина остатка IPv6 пакета који прати заглавље, у октетима. Другим речима, ово је комплетна дужина свих заглавља и јединице података транспортног слоја TPDU<sup>30</sup>;
- Следеће заглавље (дужине 8 бита): 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<sup>31</sup>,
  - 58 -ICMP пакет протокола IPv6,
  - 46 - протокол за резервисање ресурса<sup>32</sup>.

Вредности за додатна заглавља су следеће:

- 0 - заглавље опције корак по корак ,
- 43 - заглавље IPv6 рутирања ,
- 44 - заглавље IPv6 делова,
- 50 - заглавље сигурности податка,
- 51 - заглавље о IPv6 аутентификацију,
- 59- нема следећег заглавља<sup>33</sup>,
- 60 - заглавље одредишних опција.
- Ограничење скока (дужине 8 бита): колико је још скокова за овај пакет дозвољено. Ограничење скокова поставља извориште одговарајућу вредност. Декрементира се у сваком чвору који прослеђује пакет. Када вредност овог поља постане нула пакет се одбацује<sup>34</sup>;
- Изворишна адреса (дужине 128 бита): адреса оног који пакета формира;
- Одредишна адреса (дужине 128 бита): адреса оног који пакета прима. 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<sup>35</sup> 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 заглавље (40 према 20 бајтова) број поља је мањи (8 према 12). То значи да ће рутери имати мање посла око обраде заглавља чиме је процес рутирање значајно убрзан.

## Структура IPv6

Пакет IPv6 има општу структуру приказану сликом 15.14. Сваки IPv6 пакет започиње са 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<sup>36</sup> 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<sup>37</sup>

<sup>30</sup> TPDU (*Transport Protocol Data Unit*)

<sup>31</sup> *Interdomain Routing Protocol*

<sup>32</sup> *Resource Reservation Protocol*

<sup>33</sup> *No Next Header*

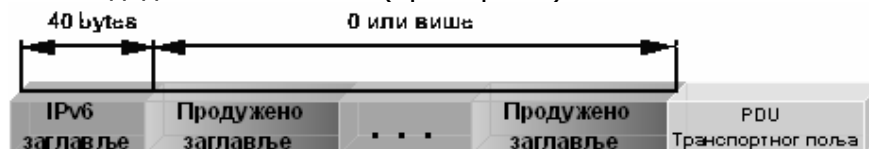
<sup>34</sup> Ово је поједностављен поступак у односу на поступак који би требало да се уради са TTL пољем код IPv4. Рад са временским интервалима код верзије IPv4 није донео никакву предност. Устvari рутери са IPv4 протоколом третирали су TTL поље само као ограничење у броју скокова.

<sup>35</sup> Код израчунавања контролне суме TCP и UDP користе псеудозаглавље у коме је садржана и IP адреса.

<sup>36</sup> Код верзије IPv4 тај задатак је обављало поље опција.

<sup>37</sup> *Next Header Field*

које означава који тип (врста) заглавља следи иза њега. Оваква структура омогућава уланчавање различитих додатних заглавља (проширења).



Слика 15.14 Форма пакета IPv6

Дефинисана су следећа додатна заглавља (проширења):

- заглавље опције корак по корак<sup>38</sup>: дефинише специјалне опције које захтевају обраду корак по корак,
- заглавље IPv6 рутирања<sup>39</sup>: обезбеђује проширење рутирања, слично изворишном рутирању у IPv4,
- заглавље IPv6 делова<sup>40</sup> (фрагмента) пакета: садржи информације о дељењу и поновном повезивању пакета,
- заглавље о IPv6 аутентификацију<sup>41</sup>: обезбеђује интегритет и аутентичност сваког пакета,
- заглавље о сигурности податка<sup>42</sup>: обезбеђује заштиту пакета,
- заглавље одредишних опција<sup>43</sup>: садржи опционе информације које ће одредишни чвор анализирати.

У случају када се користи више додатних заглавља 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 податка,
8. заглавље одредишних опција - за опције које ће бити обрађене само у крајњем одредишту пакета.

<sup>38</sup> Hop-by-Hop Options header

<sup>39</sup> Routing header

<sup>40</sup> Fragment header

<sup>41</sup> Authentication header

<sup>42</sup> Encapsulating Security Payload header

<sup>43</sup> Destination Option header



Слика 15.15 IPv6 пакет са продуженим заглављима

Слика 15.15 приказује пример једног IPv6 пакета који укључује део сваког заглавља осим оних која су повезана са сигурношћу. IPv6 заглавље и свако 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 15.15 као протокол вишег слоја је постављен TCP протокол. Подаци (виших слојева) које носи IPv6 пакет садрже заглавља TCP протокола и податке апликације.

#### Ознака тока<sup>44</sup>

IPv6 стандард дефинише ток као низ пакета који се шаљу од одређеног изворишта ка одређеном одредишту<sup>45</sup> и за које извориште захтева од рутера да на посебан начин поступа. Проток је јединствено дефинисан тако што се комбинују изворишна и одредишна адреса са ознаком тока (20-битни број различит од нуле). Извориште додељује исту "ознаку тока" свим пакетима који су део једног тока.

Посматрано са стране изворишта ток је низ пакета које је генерисала апликација изворишта а који захтева исти транспортни сервис. Ток може да обухвати једну или више TCP веза. Једна апликација може да генерише један или више токова. Пример два тока је мултимедијални састанак, коме је додељен један ток за звук а други за слику. Сваки од токова има различите захтеве код преноса података, кашњења или одступање у кашњењу.

Ако се погледа из угла рутера, ток је низ пакета који има исте атрибуте који утичу на то како ће се рутер понашати према пакетима тог тока. Ту спада: одабрана путања, додељени ресурси, критеријуми за одбацивања, алгоритам заштите итд. Рутер може да се понаша другачије према пакетима који нису из истог тока. На пример: доделом различитог меморијског простора (бафера), придруживањем различитог приоритета код прослеђивања пакета или различитим захтевом за квалитетом сервиса који се од мреже очекује .

Не постоји посебно значење било које ознаке тока. Уместо тога, да би се обезбедио специјални поступак ток 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 одговарајуће информације у једно од додатних заглавља пакета, као што је нпр. заглавље опције "корак по корак". Примери специјалног поступка су и захтеви за нестандартним квалитетом сервиса или неким од сервиса у реалном времену.

У начелу, сви кориснички захтеви за одређеним током могу бити дефинисани у додатним заглављима и укључени у сваки од пакета. Ако се жели оставити концепт тока потпуно отвореним за мноштво захтева, резултат би могао бити превелико заглавље пакета. Друга могућност, која је усвојена код протокол IPv6, је тзв. ознака тока код које су захтеви тока дефинисани на самом

<sup>44</sup> Flow label

<sup>45</sup> Уникаст (unicast) или мултикаст (multicast).

почетку а јединствена ознака тока додељена је сваком току. У овом случају рутер мора да чува информације о захтевима сваког тока.

Следећа правила важе за ознаке тока:

1. Станица или рутер који не подржавају поље "ознака тока" мора да када прави пакет постави поље на нулту вредност, када преусмерава пакет не мења његову вредност а игнорише га 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 тока у табели без испитивања осталих заглавља;
3. Извориште додељује току "ознаку тока". Нова ознака тока мора бити изабрана као случајни број из опсега 1 до  $2^{20} - 1$ . Услов је да извориште не може да додели ознаку новом току ако се она користи за ток који је још активан. Вредност нула указује да се ни једна од ознака тока не користи;

### Адресирање протокола IPv6

Код протокола IPv6 адресе су дужине 128 бита. Адресе се додељују сваком од интерфејсу чвора<sup>46</sup> а не самом чвору. Сваки интерфејс може да има више јединствених унікаст адреса. Било која од унікаст 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 потпоможе 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:

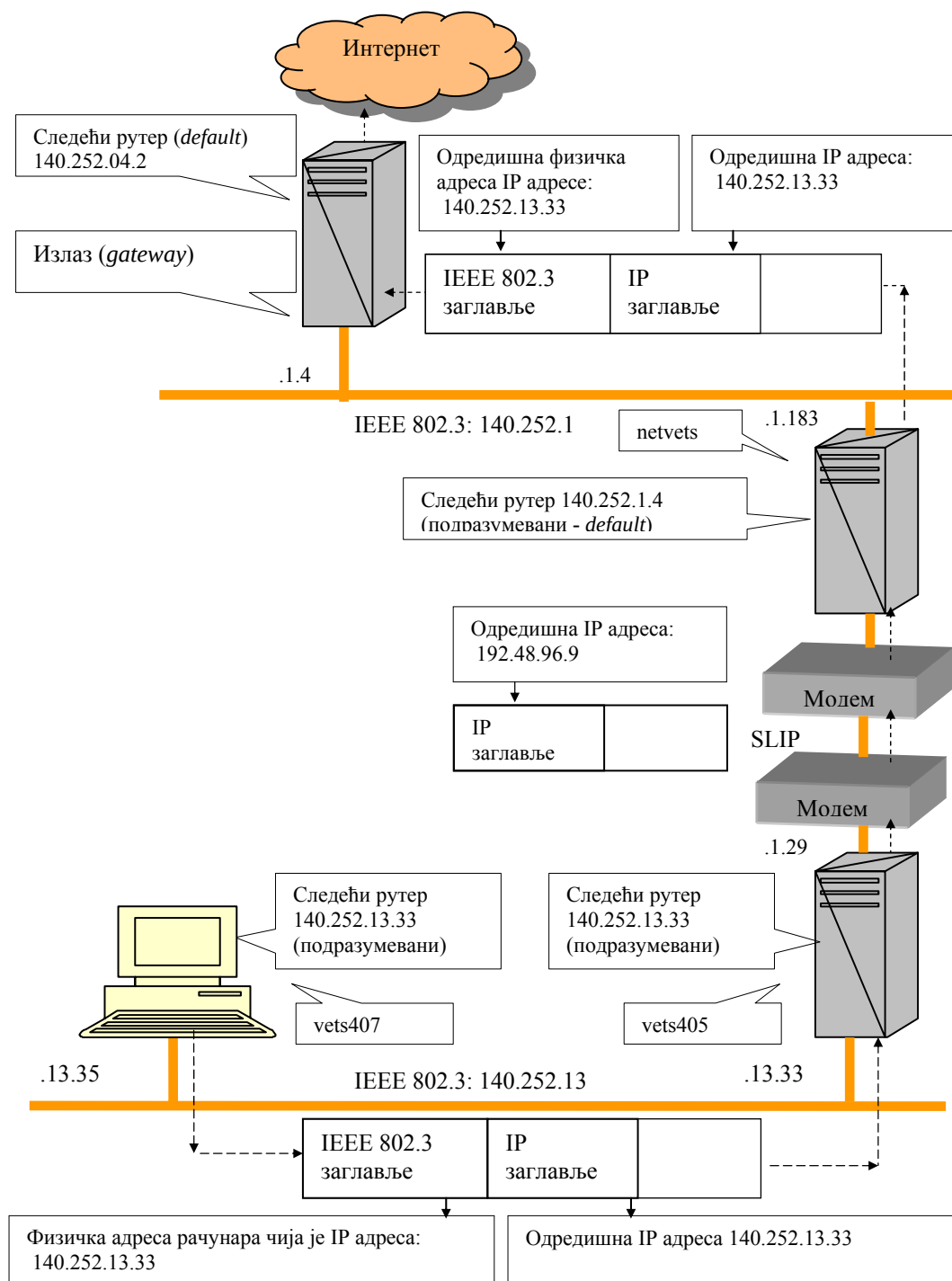
- Унікаст адреса је идентификатор једног интерфејса. Пакет послат унікаст адресом испоручује се интерфејсу који је одређен том адресом;
- Еникаст адреса је идентификатор за више интерфејса који припадају различитим чворовима. Пакет послат еникаст адресом испоручује се неком од интерфејса који је одређен том адресом (најближем, гледајући по протоколу за рутирање);
- Мултикаст адреса је идентификатор за групу интерфејса који припадају различитим чворовима. Пакет послат мултикаст адресом испоручује се свим интерфејсима који су одређени том адресом;

---

<sup>46</sup> Код протокола IPv6 термин чвор се односи и на рутер и на крајњу станицу. Односно на сваки уређај код кога је имплементиран IPv6 протокол.

## 40. Објашњење примера 16.2 (*rutiranje.doc*, слика 16.4)

Пример 16. 2: Рачунар *vets405* треба да пошаље пакет рачунару *ftp.hardsoft.com* чија је IP адреса 192.48.96.9. На слици 16.4 приказан је пут пакета кроз прва три рутера.



Слика 16.4. Испорука пакета од *vets407* ка [ftp.hardsoft.com](http://ftp.hardsoft.com)

Прво рачунар *vets407* претражује своју табелу рутирања и не налази одговарајуће записе (ни рачунара ни мреже). Користи се подразумевани запис који указује да треба послати пакет ка *vets405* следећем рутеру<sup>47</sup>. Када се пакет шаље од *vets407* ка *vets405* одредишна IP адреса је IP адреса крајњег одредишта (192.48.96.9).

Адреса слоја везе је 48 - битна IEEE802.3 адреса интерфејса рутера *vets405*. Упоредити овај пакет са оним где су одредишна IP адреса и адреса одредишног мрежног интефејса адресе рачунара *vets405*. Када *vets405* прими пакет он уочава да одредишна IP адреса у пакету није његова IP адреса. Пошто је рачунар *vets405*

<sup>47</sup> Next hop router

конфигуриран као рутер он преусмерава пакете, претражује табелу рутирања и користи подразумевани запис.

Подразумевани запис указује рутеру *vets405* да пошаље пакет ка следећем рутеру *netvets* чија IP адреса је 140.252.1.183. Пакет се шаље преко везе типа тачка -тачка са SLIP<sup>48</sup> протоколом. Пошто SLIP не додаје никакво заглавље на слици је представљен само IP пакет. Када *netvets* прими пакет поступа на исти начин као и рутер *vets405*: пакет није упућен ка некој од његових IP адреса па се усмерава даље пошто је *netvets* конфигуриран као рутер. Користи се подразумевана адреса рутирања и пакет се шаље ка следећем рутеру - међумрежном пролазу (140.252.1.4).

Рутер *netvets* користи ARP протокол за добијање MAC адресе која одговара 140.252.1.4 и та Етернет адреса је одредишна адреса у заглављу слоја везе.

Међумрежни пролаз<sup>49</sup> пролази кроз исту процедуру као и претходна два рутера а њихов подразумевани запис у табели рутирања указује на адресу 140.252.104.2 као свој следећи рутер. Уочимо следеће:

- сви рачунари и рутери у овом примеру користе подразумевану путању,
- одредишна IP адреса никада се не мења<sup>50</sup>,
- различита заглавља слоја везе се користе на свакој вези и одредишна адреса слоја везе, ако постоји, увек садржи адресу слоја везе следећег рутера (*next hope*). У нашем примеру и укалупљени IEEE802.3 рам садржи адресу следећег рутера, али не и SLIP рам. IEEE802.3 адресу обезбеђује ARP протокол.
- 

## 41. Статистички временски мултиплекс (*8\_06\_sajt.pdf*, слика 8.3, слика 8.19)

### 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 времене терминали били у употреби не постоји пренос података код сваког терминала.

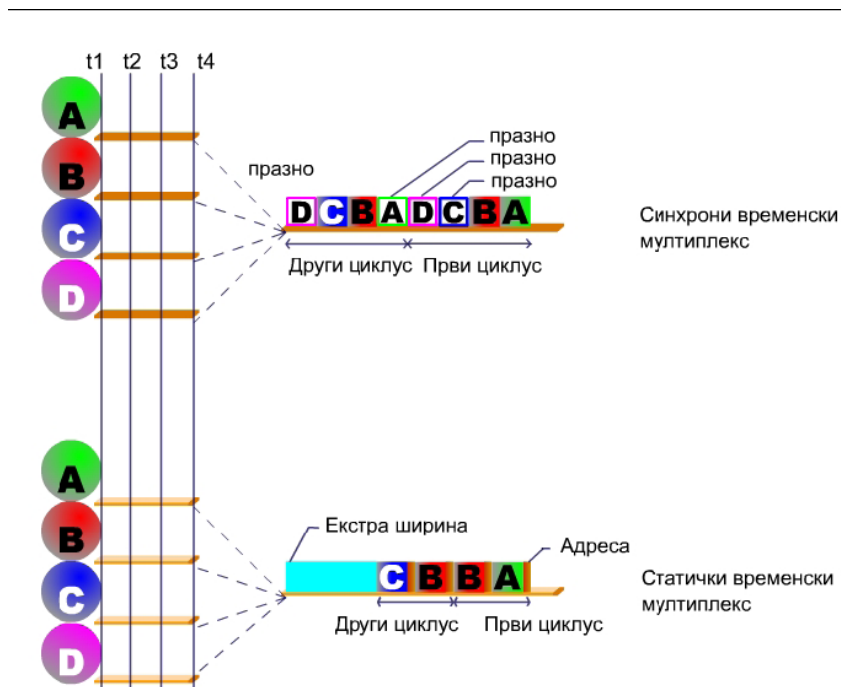
Друга врста временског мултиплекса је статистички мултиплекс. Статистички мултиплекс испитује карактеристике података који се преносе и динамички додељује временске слотове према захтевима. Као и код синхроног временског мултиплекса статистички мултиплекс има већи број улазно/излазних линија на једној 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 само  $k$  где је  $k < n$  временских слотова који су на располагању у временском мултиплексу. Са стране улаза задатак мултиплексера је да прегледа улазне бафере, читава јединице података из њих и шаље рам. На излазу мултиплексер прима рам и прослеђује податке из временских целина у одговарајући излазни меморијски простор (погледати слику. 8.9).

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 мултиплекса за исти број прикључених уређаја. На слици 8.19 приказана је разлика статистичког и синхроног временског мултиплекса. На слици су приказана четири извора података која 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 од тренутака  $t_1, t_2, t_3, t_4$  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 јединице да буду празне (без података).

<sup>48</sup> Serial Line IP, RFC1055- укалупљивање IP пакета на серијским линијама.

<sup>49</sup> Gateway

<sup>50</sup> За изворишно рутирања (*source routing*) које се ретко користи овај исказ није тачан.



Слика 8.19 Поређење статистичког и синхроног мултиплексирања

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 А и В. Види се да не постоји додељивање временских целина по њиховој позицији. Због тога је адреса за испоруку потребна да би се обезбедила правилна испорука података. На тај начин се уз корисне податке за сваки уређај морају додати и некорисни подаци (премашења) за адресирање.

Формат рама који користи статистички мултиплексер има утицаја на перформансе. Наравно пожељно је минимизирати премашење да би се пропусна моћ система побољшала. Уопште посматрано статистички мултиплексер ће користити неки од синхроних протокола као што је HDLC. У оквиру HDLC рама део за податке мора да садржи и управљачке битове за мултиплексирање. На слици 8.20 приказани су могући формати. У првом случају само један извор података је укључен у рам. Извор података је одређен адресом. Дужина поља података је променљива и његов крај је означен крајем целокупног рама. Овај начин може да ради 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.



а) Свеукупни рам



б) Део рама (подрам) са једним извором по раму



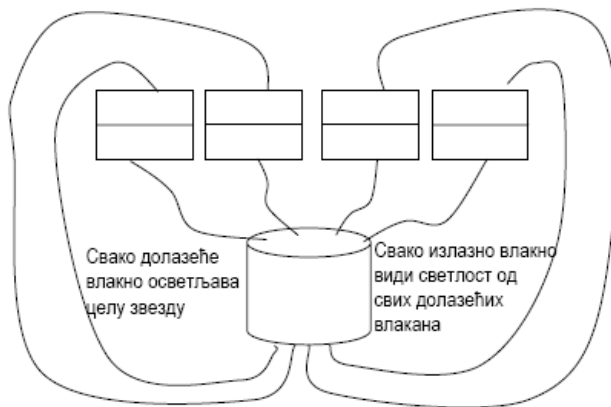
в) Део рама (подрам) са више извора по раму

Слика 8.20 Формат рама статистичког мултиплексера

## Локалне рачунарске мреже са оптичким кабловима

Код локалних мрежа са оптичким кабловима често се користи мултиплексирање по таласним дужинама. Више истовремених комуникационих веза остварује се на различитим таласним дужинама. У овом делу описаћемо један такав протокол.

Једноставан начин да се направи оптичка локална мрежа је употреба пасивне компоненте која их повезује. У ствари, два оптичка влакна из сваке станице су повезана 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 (слика 21).

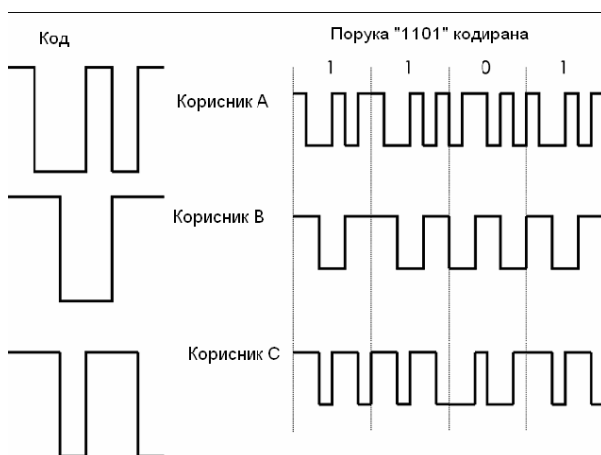


Слика 8.21 Пасивно повезивање у звезду у мрежи са оптичким влакнима

## 42. Кодномултиплексирање (8\_06\_sajt.pdf, слика 8.21, једначина 8.1)

### Кодно мултиплексирање

Кодно мултиплексирање<sup>2</sup> је техника која се користи код система са проширеним спектром<sup>3</sup>. Ради на следећи начин: полази се од сигнала података брзине  $D$  који означавамо битском брзином. Разбијамо сваки бит у  $k$  чипова према фиксним узорцима који су дефинисани за сваког корисника и који се означавају као кориснички код. Брзина чипова новог канала је  $k * D$  у секунди. Посматрајмо једноставан пример за  $k = 6$ . Најједноставније је окарактерисати код као секвенце од  $+1$  и  $-1$ . Слика 8.23 показује код за три корисника А, В и С. Свака од њих комуницира са истом базном станицом - пријемником R.



Слика 8.23 Пример CDMA

Код за корисника А је  $c_A = (1, -1, -1, 1, -1, 1)$ . Слично корисник В има код  $c_B = (1, 1, -1, -1, 1, 1)$ , а корисник С  $c_C = (1, 1, -1, 1, 1, -1)$ .

Посматрамо комуникацију корисника са базном станицом. Претпостављамо да базна станица познаје код станице А. једноставности ради претпостављамо да је комуникација већ синхронисана тако да базна станица зна где да пронађе код за А. Уколико А хоће да пошаље бит 1, шаље свој чип-узорак  $(1, -1, -1, 1, -1, 1)$ ;

уколико хоће да пошаље бит 0, шаље комплемент чип-узорка:  $(-1, 1, 1, -1, 1, -1)$ . Базна станица на пријему декодује чип-узорак. У нашем једноставном примеру уколико пријемник R прими чип-узорак  $d = (d_1, d_2, d_3, d_4, d_5, d_6)$  и пријемник тражи да комуницира са корисником  $u$  који има код  $(c_1, c_2, c_3, c_4, c_5, c_6)$  пријемник ће обавити следећу функцију декодавања:

$$S_u(d) = d_1 \times c_1 + d_2 \times c_2 + d_3 \times c_3 + d_4 \times c_4 + d_5 \times c_5 + d_6 \times c_6 \quad (8.1)$$

У нашој анализи посматраћемо корисника означеног са  $u$  и када је у питању корисник А видећемо шта се дешава. Уколико А шаље 1 бит онда је  $d: (1, -1, -1, 1, -1, 1)$  и једначине 8.1 постаје:

$$SA(1, -1, -1, 1, -1, 1) = 1 \times 1 + (-1) \times (-1) + (-1) \times (-1) + 1 \times 1 + (-1) \times (-1) + 1 \times 1 = 6$$

Уколико А пошаље бит 0 што одговара вредности за  $d: (1, -1, -1, 1, -1, 1)$  онда се за SA добија вредност:

$$SA(-1, 1, 1, -1, 1, -1) = (-1) \times 1 + 1 \times (-1) + 1 \times (-1) + (-1) \times 1 + 1 \times (-1) + (-1) \times 1 = -6$$

Треба уочити да се  $SA(d)$  увек налази у опсегу  $-6 \leq SA(d) \leq 6$  без обзира на секвенце -1 и 1. Вредност за коју се добија гранична вредност је код станице А и његов комплемент. Тако ако се израчунавањем добије +6 зна се да је од станице А примљен бит 1 а ако се добије -6 зна се да је примљен бит 0. У било ком другом случају претпоставља се да неко други шаље податке или да је дошло до грешке. Разлог зашто се ради на овај начин биће јасан уколико погледамо шта ће се десити уколико корисник В шаље а покушава се пријем са SA. односно са погрешним кодом (код корисника А). Уколико В шаље бит 1, онда је  $d: (1, 1, -1, -1, 1, 1)$  па се добија:

$$SA(1, 1, -1, -1, 1, 1) = 1 \times 1 + 1 \times (-1) + (-1) \times (-1) + (-1) \times 1 + 1 \times (-1) + 1 \times 1 = 0$$

Тако нежељени сигнал (од корисника В) се не појављује уопште. Може се једноставно проверити да ако корисник В пошаље бит 0 декодер ће добити поново  $SA = 0$ . Ово значи да уколико је декодере линеаран и уколико А и В шаљу сигнале  $s_A$  и  $s_B$  у исто време онда је  $SA(s_A + s_B) = SA(s_A) = SA(s_B) = SA(s_A)$  пошто декодер не узима у обзир В када декодује А. Код А и В имају особину да су међусобно ортогонални која се може изразити следећом једнакошћу:  $SA(c_B) = SB(c_A) = 0$ .

Веома је добро имати такве кодове али их нема много. Много је чешћи случај да је вредност  $SX(c_Y)$  мала по апсолутној вредности за случај када је  $X \neq Y$ . Тада је могуће направити разлику између случаја у када је  $X = Y$  и када је  $X \neq Y$ . У нашем примеру  $SA(cc) = SC(c_A) = 0$  али је  $SB(cc) = SC(c_B) = 2$ . У другом примеру С сигнал ће дати мали допринос декодујућем сигналу у односу на 0.

## 43. ADSL (докуменат [9\\_drajic\\_1.pdf](#), поглавље 9.3, слика 9.7, 9.8, 9.9)

### 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

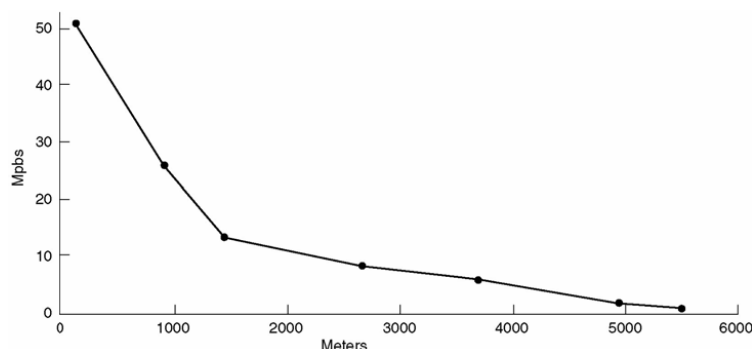
нуде дигитални приступ преко локалних петљи. Дигитални приступ даје могућност већег опсега од стандардног телефонског канала.

У самом почетку постојало је више међусобно преклапајућих решења која се сва могу означити општом ознаком xDSL1 (x означава различите системе). У следећем поглављу описаћемо различите системе међу којима најраспрострањенији постаје ADSL2 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 сигнал1 пролазе кроз филтере који ограничавају све учестаности испод 300Hz и изнад 3400Hz. Подаци који се преносе телефонским линијама су такође ограничени овим уским опсегом3.

Када претплатници користе xDSL системи 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.

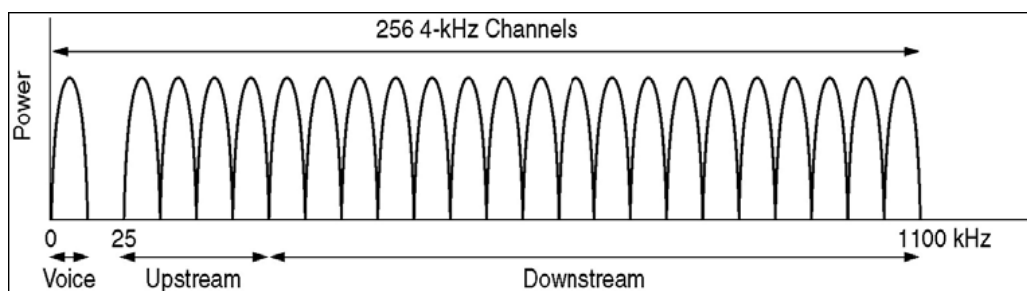
Капацитет локалне петље зависи од више фактора: дужине, дебљине жице и општег квалитета. На слици 9.5 је нацртана могућа ширина опсега у функцији од растојања под претпоставком да су сви остали фактори оптимални (нове жице, равномерна изолација, итд.)



Слика 9.5 Ширина опсега у зависности од растојања код упредених парица категорије 3 за xDSL системе.

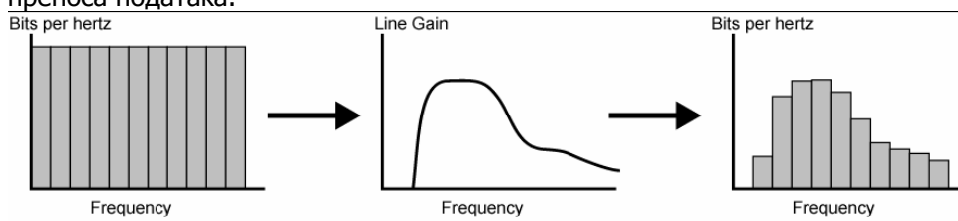
Последице слабљења приказане на слици 9.5 стварају проблеме оператерима телефонских мрежа. Када нуде услуге корисницима морају да имају у виду и растојања до корисника. То значи да удаљеним корисницима не могу да понуде исту услугу као онима који су ближи локалном чворишту. Што је понуђена брзина нижа 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 факса. Треће, морају да понуде брзине веће од 56kb/s. Четврто, морају бити стално прикључени што подразумева месечну претплату а не плаћање по минути. 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<sup>1</sup>, директни (одлазни) канал 2- од претплатника до локалног чворишта, повратни (долазни) канал - од локалног чворишта до корисника<sup>3</sup> (слика 9.8 а). Други приступ је систем са више дискретних тонова DMT<sup>4</sup> илустрован је на слици 9.6. DMT техника састоји се у коришћењу више носећих сигнала на различитим 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.



Слика 9.6 Распоред канала код ADSL система са DMT модулацијом

При иницијализацији DMT модем шаље тест сигнале у сваки од подканала 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 9.7 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.



### Слика 9.7. Додељивање брзине по каналу код DMT система

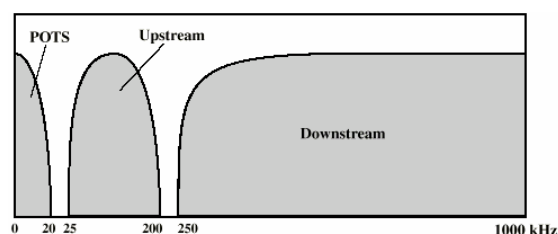
Канали су распоређени на следећи начин (слика 9.8):

- 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<sup>1</sup> или фреквенцијски мултиплекс за доделу два опсега: за одлазни и долазни саобраћај;
- По један канала користи се за управљање одлазним и долазним саобраћајем. Преосталих 248 канала могу се употребити за пренос података корисника.

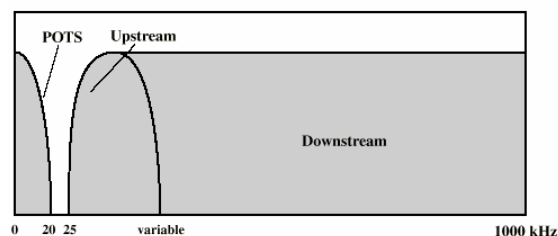
У принципу сваки од 248 канала за податке може се употребити за пренос података у потпуном дуплексу. Међутим хармоници, преслушавање итд. ограничавају брзину реалних система значајно испод теоретских граница. Задатак пружаоца Интернет услуга ISP2 је да одреди колико канала се користи за одлазни а колико 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 А код ADSL-а. Уобичајена подела је: 32 канала за одлазни саобраћај и остатак за долазни. 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 обезбедити. Оваква опција захтева додавање специјалних кола за одстрањивање еха.

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 256kb/s у одлазном каналу.



(a) Frequency-division multiplexing



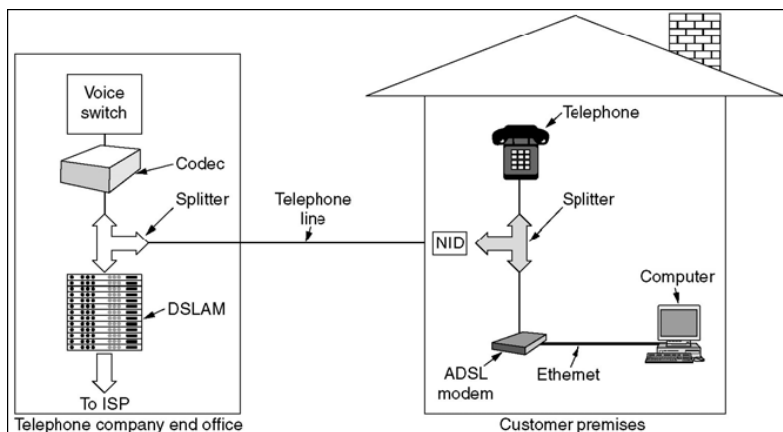
(b) Echo cancellation

Слика 9.8 Конфигурација ADSL канала

У оквиру сваког канала користи се модулативна 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 битоа по једном боду<sup>1</sup>.

Уобичајена организација ADSL система је приказна на слици 9.9. У овој шеми телефонска компанија треба да инсталира мрежни интерфејсни уређај NTD2 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<sup>3</sup>. То је аналогни филтер који раздваја фреквенцијски опсег од 0 до

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.



Слика 9.9 Уобичајена организација ADSL система

Већина данашњих ADSL модела 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 чворишту, инсталира се одговарајући уређај за раздвајање. На овом месту део сигнала који одговара говору издваја се и шаље комутатору за говорне сигнале. Сигнал изнад 26kHz усмерава се ка новој врсти уређаја - мултиплексеру за дигиталне претплатничке петље DSLAM1. Мултиплексери DSLAM садрже исту врсту процесора за обраду сигнала као и ADSL модем. Сигнал из ADSL модела подељен 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 9.9 је присуство уређаја NID 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. Систем би изгледао исто као на слици 9.9 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 модела и телефонске парице. Микрофилтер је нископропусни филтер који одстрањује

учестаности изнад 3400Hz; микрофилтер за ADSL модем је високопропусни филтер који одстрањује учестаности испод 26kHz. 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).

ADSL је стандард физичког слоја. Шта се налази изнад и како ради зависи од оператера. Често је то и ATM мрежа пошто она може да обезбеди квалитет сервиса а користи се за међусобно повезивање комутационих центара.

## 44. Динамичко рутирање (*rutiranje.doc*, поглавље 16.7, сл. 16.8)

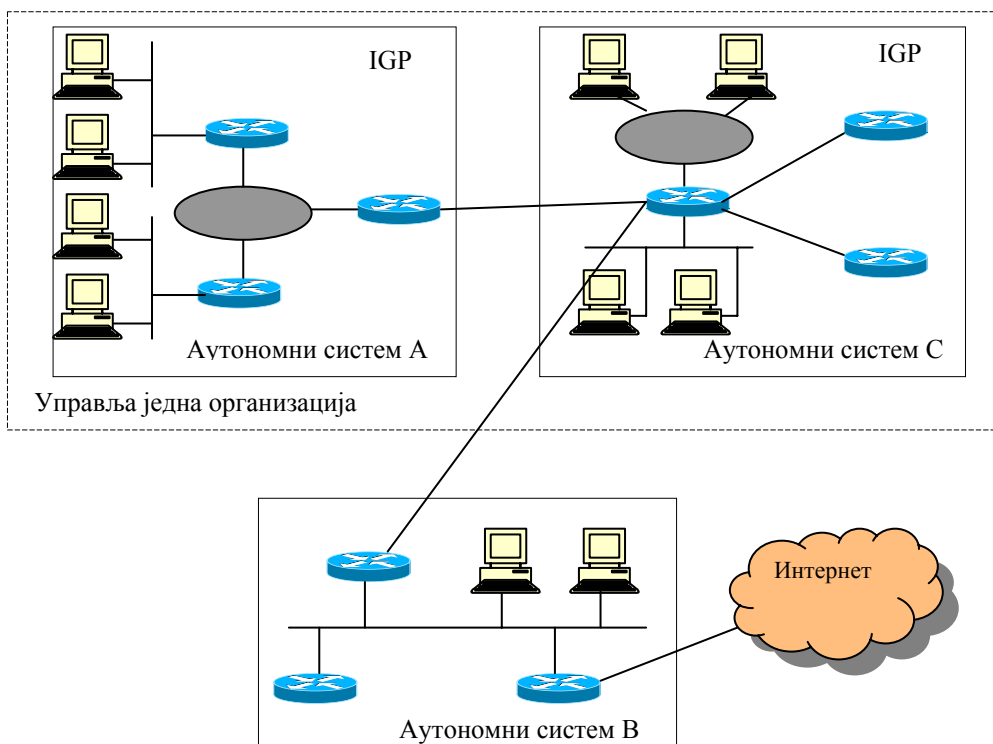
### 16.7 Рутирање између домена CIDR<sup>51</sup>

CIDR је начин да се спречи превелик раст табела рутирања. Описан је у RFC1518. Основни концепт у CIDR 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 се 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 могу 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;

<sup>51</sup> Classless Interdomain Routing

- 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. OSPF и RIP-2 могу да преносе и 32-битну маску.



Слика 16.8. Аутономни системи