Телекомуникации

Основна задача – надеждно предаване на информация на разстояние

Информация – съвкупност от сведения за каквито и да са събития, явления и предмети.

Съобщение – начин на предаване на информацията. То се предава с помощта на сигнал.

Сигнал – изменяща се физическа величина (електрически ток, звукова вълна и т.н.), еднозначно изобразяваща съобщението. Делят се на два вида:

- ***аналогови*** – има безкраен брой значения за ограничен интервал от време.
- ***цифрови*** - има краен брой значения за ограничен интервал от време.

Сигнал

Превръщането на съобщението в сигнал се състои от три операции, които могат да бъдат независими или съвместни. Това са :

- ***преобразуване*** – превръщане на не електрическите величини, съответстващи на първоначалното съобщение, в електрически сигнал

- ***кодиране*** – построяване на сигнала по определен принцип, имащ някакъв математически израз (ASCII, EBCDIC)

- ***модулация*** – въздействие върху някой параметър на електрическия ток (амплитуда, честота,фаза), благодарение на което в изменението на този параметър се оказва заложен предавания сигнал.

За да се предаде едно съобщение на разстояние е необходима комуникационна система.

Комуникационна система – съвкупност от технически средства, необходими за предаване на съобщения от източника към получателя.

Това са : ***предавател***, ***комуникационна линия*** и ***приемник***.

Според вида на предаваните съобщения комуникационните системи се делят на:

- ***телефонни*** (за предаване на глас)
- ***телеграфни и телетексни*** (за предаване на текст)
- ***факсимилни*** (за предаване на неподвигни изображения)
- ***телевизионни и видеотелефонни*** (за предаване на подвижни изображения)
- ***телеизмервателни*** (за предаване на данни от измервания на разтояние)
- ***системи за предаване на данни***

Единицата за измерване на количеството информация е ***бит*** (***b***).

Количеството информация, което може да се предаде по дадена комуникационна система за единица време определя нейната ***пропускателна способност***.

Единицата за измерване на пропускателната способност е ***бит за секунда*** (***b/s***).

Комуникационна линия – физическа среда, която се използва за предаване на сигналите от предавателя към приемника. Комуникационната линия е физическо понятие

Комуникационен канал – съвкупност от средства, осигуряващи предаване на сигнал от някаква точка А на комуникационната система до друга нейна точка Б.

Комуникационният канал е логическо понятие.

В зависимост от вида на сигналите (цифрови или аналогови), постъпващи на входа и излизащи на изхода на канала, каналите се делят на:

- ***аналогови***
- ***цифрови***
- ***аналогово-цифрови***
- ***цифрово-аналогови***

Най-често под канал се разбира логическа част от използваната физическа комуникационна линия, осигуряваща предаването на отделен сигнал.

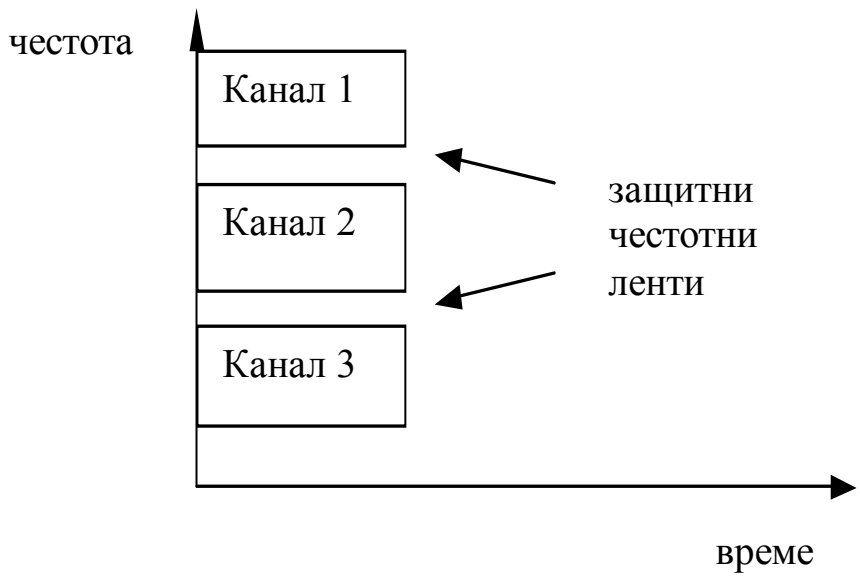
Комуникационните канали притежават следните черти:

- ***наличие на шум в канала*** даже при отсъствие на полезен сигнал в него
- ***линейност***
- ***закъснение на сигналите***
- ***затихване на сигналите***
- ***деформиране на сигналите***

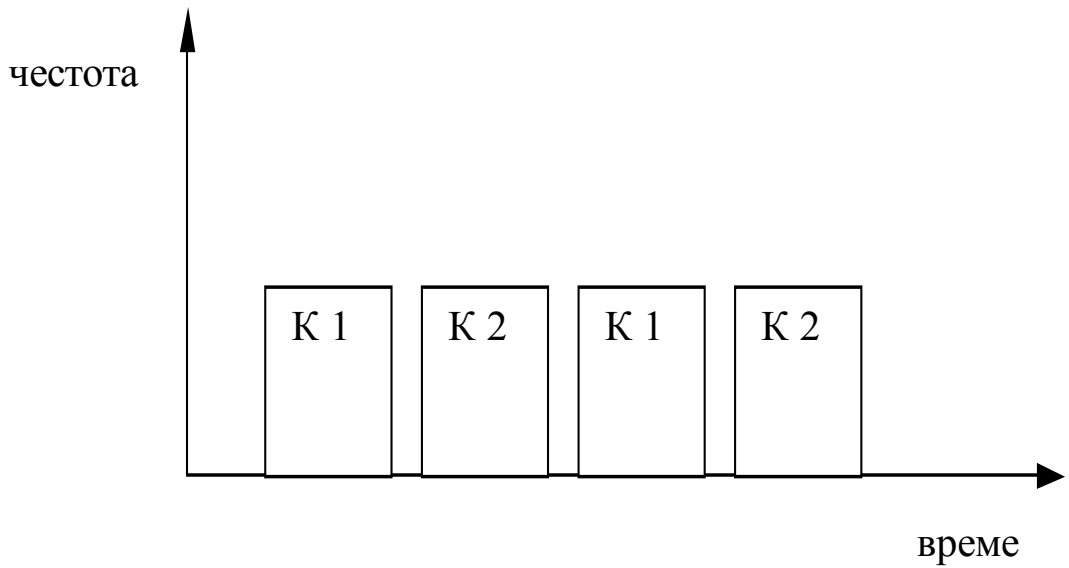
Една комуникационна система се нарича многоканална, ако осигурява няколко паралелни канала за предаване по една обща комуникационна линия.
Използвани устройства:
•***мултиплексор***
•***демултиплексор***

При многоканалните комуникации се използват няколко способа за разделяне на каналите:

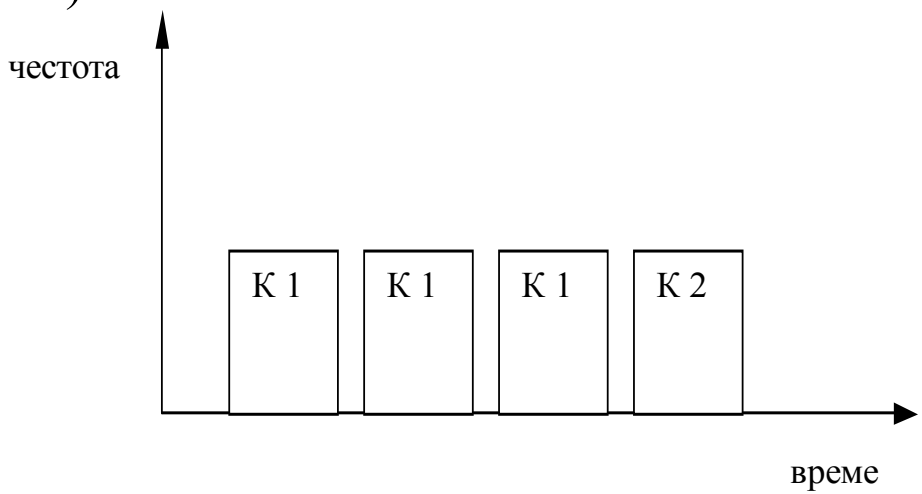
-честотно деление (FDM)



- ***времеделение (TDM)***



- ***статистическо деление*** (SM)



Комуникационна мрежа – съвкупност от различни комуникиращи устройства свързани помежду си чрез комуникационни линии.

Комуникационна подмрежа – съвкупност от комуникационни линии и междинни мрежови възли (***комутатори/маршрутизатори***), осигуряващи предаването на информация между крайните възли. Крайните възли не се включват в подмрежата.

Компютърна мрежа – частен случай на комуникационната мрежа, чиито крайни възли са главно компютърни системи.

Комуникационна интермрежа – съвкупност от взаимосвързани комуникационни мрежи.
За правилното предаване на съобщение по мрежата се грижат междинните мрежови възли (***маршрутизатори/комутатори***), изпълняващи две основни функции: маршрутизация и комутация.

Маршрутизация – процесът на намиране на оптимален маршрут за преминаване на дадено съобщение по мрежата.

Комутация – процесът на пренасочване на съобщението от даден входен порт на междинния мрежов възел към определен негов изходен порт, водещ към следващия междинен възел от избрания маршрут.

Различните мрежи използват различни методи за комутация:

- ***комутация на канали*** - комутацията се извършва на три етапа: установяване на временен канал между източника и получателя, обмен на съобщения, разпадане на канала

- ***комутация на съобщения*** - съобщението се предава по различните участъци на мрежата с натрупване в междинните й възли

-***комутация на пакети*** – при възела подател съобщението се разделя на по-малки части (пакети), всеки със своята адресна и информационна част.Отделните пакети се предават между комутаторите на подмрежата, докато накрая достигнат до възела-получател. Съществуват различни режими на работа :

•***дейтаграмен режим*** – при този режим пакетите (дейтаграми) се снабдяват с пълни адресни заглавия, по които комутаторите на пакети определят по-нататъшния им маршрут. Отделните дейтаграми се предават независимо една от друга, затова маршрутите им могат да са различни и може да бъде нарушен техния първоначален ред. За целта на отделните дейтаграми се дават номера, по които в крайния визел-получател се извършва подреждане в първоначалния им ред.

- ***режим на виртуално съединение*** – при този режим между взаимодействащите крайни възли предварително се изгражда логическо съединение, по което след това се предават всички пакети на съобщението един след друг по реда на следване, след което съединението се разпада.

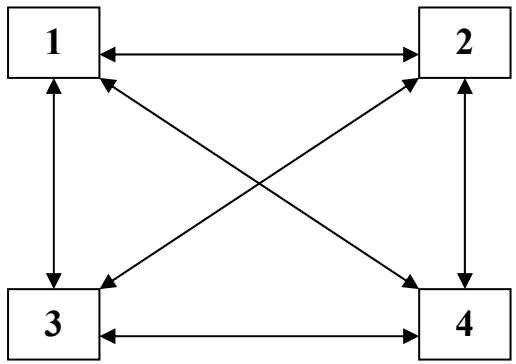
Услуги, предоставяни от комуникационната мрежа

1. ***Обществени услуги***
   - достъп до финансови институции
   - достъп до ”on-line” вестници и списания
   - ”on-line” цифрови библиотеки
   - достъп до WWW
2. ***Услуги, осигуряващи възможности за междуличностни комуникации***
   - електронна поща
   - средства за провеждане на интерактивен разговор в реално време
   - провеждане на видеоконференции
   - провеждане на дистанционно обучение
   - провеждане на дискусии в друпа по интереси в Internet
3. ***Услуги, осигуряващи интерактивни комуникации***
   - интерактивни бизнес-операции (електронна търговия)
   - участие в игри в мрежа
   - гледане по мрежата на интерактивни филми и интерактивна телевизия
   - гледане по мрежата на видеофилми по поръчка

Комуникационен модел OSI за съединение на отворени системи

Необходимост от комуникационния модел OSI (Open System Interconnection) - за ефективно свързване на различни отворени системи /компютри, комуникиращи устройства и др./, произведени от различни фирми, което изисква стандартизирани процедури за обмена на информация.

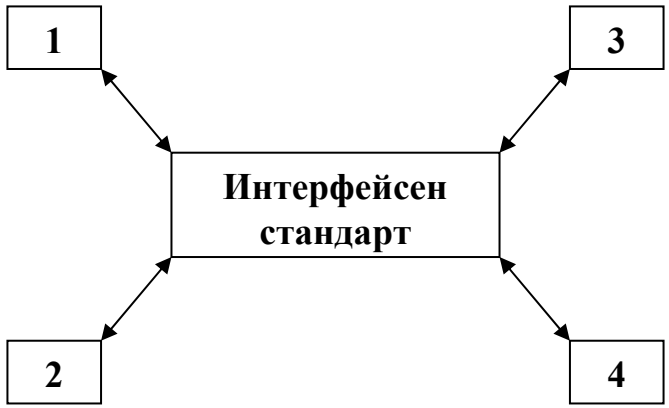
Нека допуснем, че имаме системи произведени от 4 различни фирми и трябва да комуникират помежду си.



Без интерфейсен стандарт - ***12 интерфейсни програми за комуникация между отделните системи***

За общия случай с ***n*** възли - ***n(n-1)*** на брой.

При общ интерфейсен стандарт – **4 програмите за комуникация :**



Стандартът OSI е създаден през 1978 година от две международни организации:

- ***Международна организация по стандартите ISO*** (International Standards Organization)
- ***Международен телекомуникационен съюз ITU*** (International Telecommunication Union)

Основната идея на OSI-стандарта - ***разделянето на комуникационните функции /на всяка една система/ на слоеве***.

OSI включва следните слоеве: ***физически***, ***канален***, ***мрежов***, ***транспортен***, ***сесиен***, ***представителен***, ***приложен***.

Всички слоеве могат да се разделят на две групи:

1. ***Долни слоеве***, свързани с транспортиране и доставка на информация между различни системи /***физически***, ***канален***, ***мрежов*** и ***транспортен*** слой/

2. ***Горни слоеве***, свързани с обработка и доставка на информация в рамките на една и съща система /***сесиен***, ***представителен*** и ***приложен*** слой/.

Най-долните три слоя са силно зависими от вида и структурата на подмрежата, към която непосредствено е свързана комуникиращата система. **Транспортният слой** осигурява /за слоевете над него/ независим сервиз за обмен на съобщения. **Най-горните три слоя** /*сесиен, представителен и приложен*/ са тясно свързани с процесите, изпълнявани в крайните мрежови възли под управлението на операционните им системи.
Най-долните слоеве /физически и канален/ на OSI модела се реализират **хардуерн**о, а **горните** – **софтуерно**.

OSI-моделът се базира на три основни понятия:

- ***услуга***
- ***интерфейс***
- ***протокол***

Всеки OSI слой се състои от обекти, изпълнява определена логическа функция и осигурява дадени услуги за по-горния слой. Всеки слой предлага функции, необходими за комуникиране с друга система, използващи услугите на по-долен слой. Съвкупността от правила за взаимодействие на обекти от едноименни слоеве се нарича ***протокол.*** А правилата за взаимодействие на обектите от съседни слоеве на една и съща система се нарича ***интерфейс.***

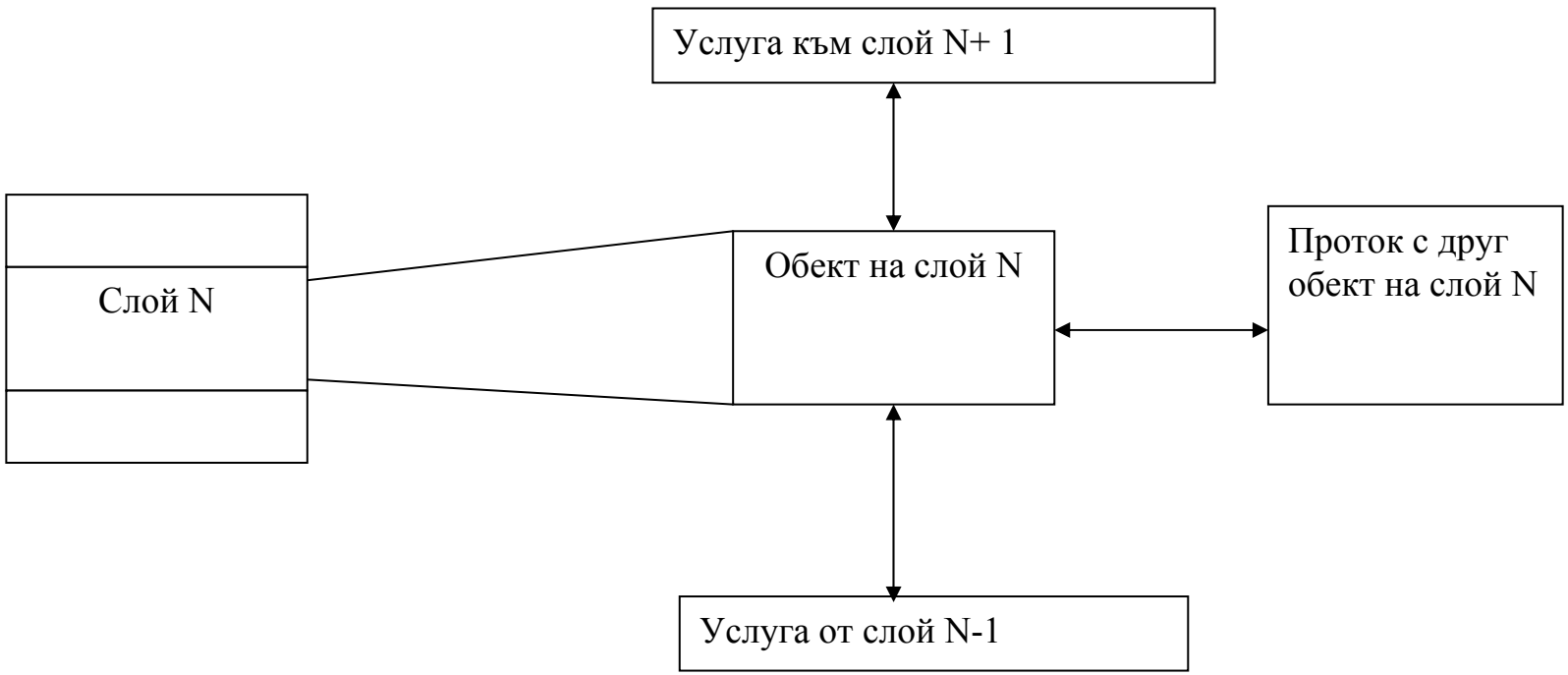
Услугата - определя какво прави даден слой.

Интерфейсът - определя как обектите на по-горния слой могат да осъществяват достъп до услугата от долния слой.

Протоколът - определя как работи даденият слой, за да осигури дадената услуга.

OOSI слоят може да използва всеки протокол, стига той да осъществява нужната услуга.

Във всеки случай може да бъдат разработени един или няколко стандарта. OSI моделът определя функциите, които трябва да бъдат представени във всеки слой. Те са ясно дефинирани, затова въвеждането на нови стандарти няма да се окаже проблем за вече написания софтуер за останалите слоеве.



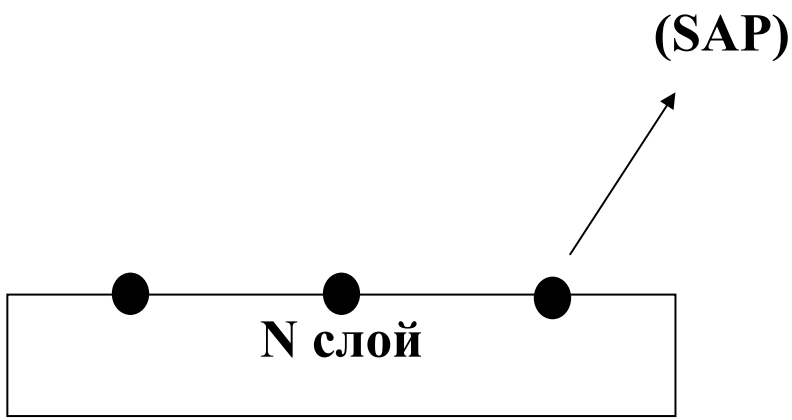
Във всеки слой има три елемента за стандартизация:

- ***спецификация на протокола***
- ***дефиниция на услугата***
- ***адресация***

Спецификацията на протокола се състои в определяне на формата на неговата единица за данни (PDU), семантиката на всички полета на тази единица и т.н.

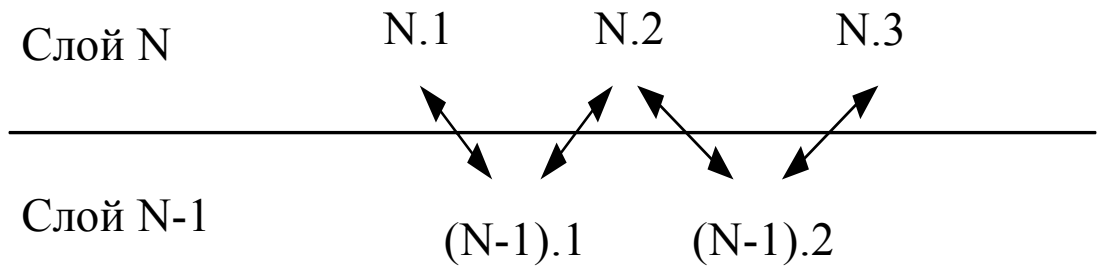
Дефиницията на услугата за по-горния слой определя какви услуги да му се предоставят, а не как.

Адресацията – указва на обектите от по-горния слой точките (SAP – Service Access Point), чрез които могат да се получи достъп до услугите на по-долния слой.



Протоколи

Протоколите помагат на два обекта от едноименни слоеве да комуникират помежду си.



Обектите от слой N си взаимодействат помежду си чрез *съединения,* създавани от слой N-1. По тези съединения се предават масиви информация, наречени *протоколни единици за данни* на слой N. Така всеки слой N-1 осигурява услуги за обектите от слой N във вид на изпълнение на задания, свързани с обмена на информация между тези обекти. На всеки обект може да се предостави едновременно едно или няколко съединения с обекти от същия слой.

Съществуват три типа съединения:

- **симплекс**
- **полудуплекс**
- **дуплекс**

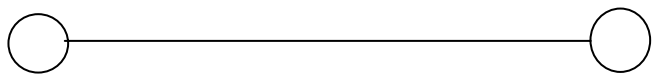
При **симплекса** информацията по всяко време се предава само в едната посока. При **полудуплекса** – в даден момент само в едно направление /но и в двете посоки/. При **дуплекса** – в двете посоки едновременно.

Елементи на протоколите:

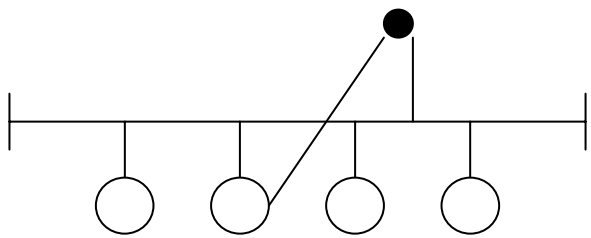
- ***синтаксис*** – включва формата на данните, кодирането им и т.н.
- ***семантика*** – включва управляващата информация за координиране на обмена, допълнителна информация за контрол на грешките, възникнали при предаването им.
- ***синхронизация*** – включва изравняване на скоростта и определяне на последователността на предаване.

Видове съединения, поддържани от различните протоколи

1. ***“точка – точка”***

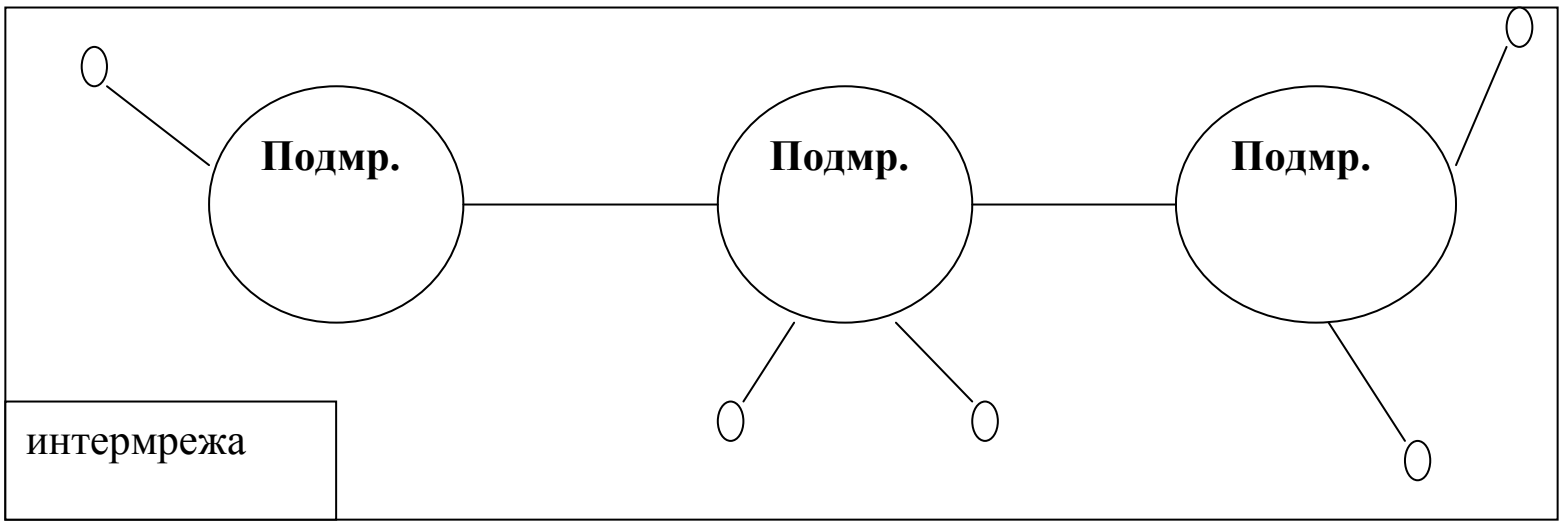


2. ***многоточково***



3. ***чрез подмрежа взаимодействие***

4. ***взаимодействие чрез интермрежа***



Характеристика на протоколите:

- ***директност или индиректност*** – директност при съединения от тип ***1*** и ***2***; индиректност – ***3*** и ***4***.

- ***монолитност или структурираност*** – монолигност е налице, ако комуникационните функции се изпълняват от един единствен протокол. Структурираността е налице, ако комуникационните функции се изпълняват от набор от протоколи, разпределени йерархично по слоеве /както при OSI модела/

- ***симетричност или асиметричност*** – симетричността е при локални мрежи с равноправен достъп /всеки възел конфигурира като клиен или сървър или и двете/. Асиметричността – при локални мрежи с отделен сървър.

- ***стандартност или нестандартност*** – стандартността е при тези протоколи, които са одобрени от международните стандартизиращи организации. Такива протоколи са протоколите на OSI модела.

Функции на протоколите:

1. Фрагментация и дефрагментация

Обикновено трансферът на данни се състои в предаване на отделни последователни блокове с определена дължина. Протоколите трябва да разделят данните на блокове. Този процес е известен като *фрагментация /сегментация/*. Блоковете се наричат PDU (Protocol Data Unit) – **протоколни единици за данни**. Всеки протокол има PDU със съответна дължина, като за някои е фиксирана, за други има **max** допустима стойност.

Пример:

стандартът X.25 – променлива дължина */максимум 4096 байта и 128 байта по подразбиране/*

Ethernet – променлива дължина */максимум 1526 байта/*.

В приемания край фрагментираните данни трябва да бъдат обединени, за да се възстанови съобщението. Този процес се нарича *дефрагментация /десегментация/*

Капсулация – процес, при който протоколната единица на по-горен слой се вмъква в полето <данни> на протоколната единица на по-долен слой, след което към него се допълна служебна информация, необходима за извършване на предаването.

Служебната информация се дели на:

- ***Адресна -*** нужна за правилното доставяне на протоколната единица до крайния адресант

- ***Управляваща -*** нужна за правилното функциониране на протокола

- ***Контролна -*** нужна за откриване и/или коригиране на грешки, възникнали при предаването на протоколната единица.

Управление на съаединението – два режима на работа:

- без установяване на логическо съединение
- с установяване на логическо съединение

При логическото съединение има три фази:

- *установяване на съединение*
- *предаване на данни*
- *разпадане на съединението*

Доставка на протоколни единици в правилен ред – протоколните единици се номерират.

Управление на потока данни – функция на приемника да ограничава големината и скоростта на протоколните единици, изпращани от предавателя.

Съществуват главно два метода:

- ***старт-стоп метод***
- ***метод на "плъзгащия се прозорец"***

При първият от тях се изпраща пакет и се чака квитанция за неговото получаване, след което се продължава с втория. При следващия метод – предават се *N* кадъра един след друг. *N*-размер на прозореца. След което се чака квитанция за тях.

6. ***Контрол на грешките*** **–** свързана е с откриването и/или коригирането на грешки при предаването на протоколните единици.

Повечето протоколи използват само режими за откриване на грешки, след което очакват повторение на сгрешените протоколни единици. Този режим е по-прост и евтин за реализиране. Режимът за корекции на грешки се използва по-рядко и само, ако не съществува възможност за обратна връзка /комуникационен канал/, по-който приемникът да сигнализира за получени сгрешени протоколни единици.

Съществува и хибриден режим, при който се извършва частично коригиране с откриване на останалите грешки.

7. *Адресация*

- *ниво на адресация* – всеки слой на комуникационния модел да има свой адрес т.е. имаме 7 нива за адресация на OSI модела.

Пример:

мрежовият слой използва ***IP*** адреси /мрежови адреси/

каналния слой използва канални адреси /***MAC*** адреси в локалните компютърни мрежи/

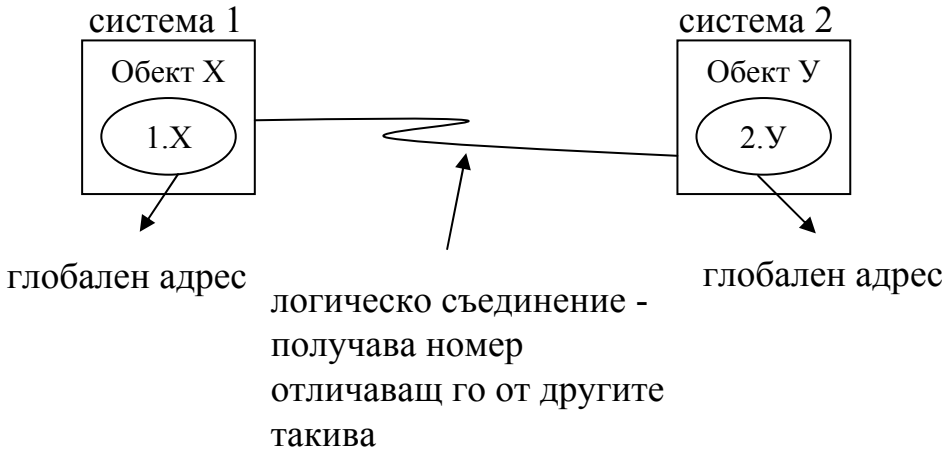
- *обхват* – два вида адреси:
  - локални
  - глобални

Пример:

локални – MAC адресите и X.25 адресите

глобални /неповторими, уникални/ – Internet адресите.

- *идентификатори на съединението*



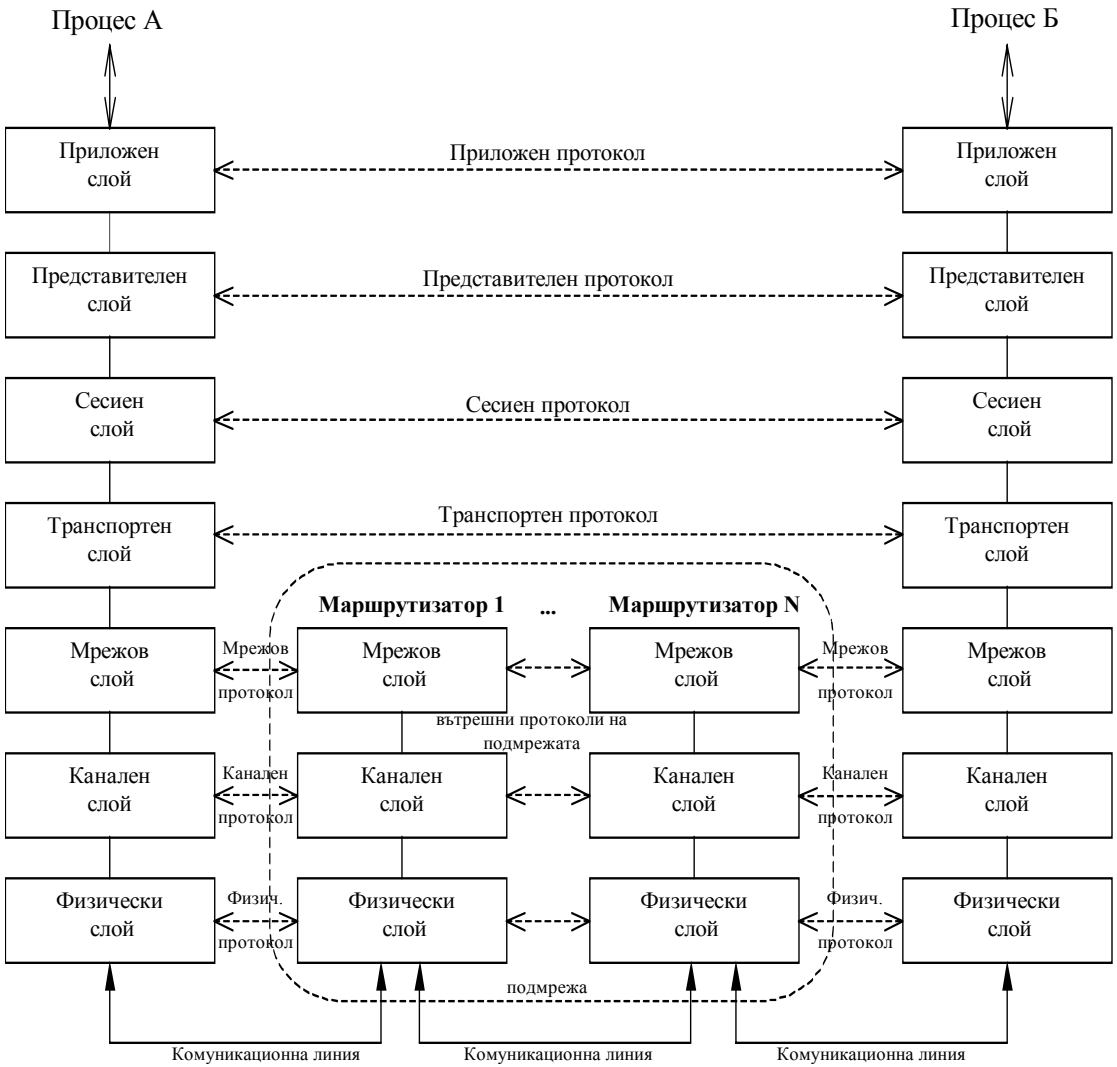
- *режим на адресация* – три типа адреси :
  - ***индивидуален адрес /unicast/*** - съобщенията се предават само към един възел
  - ***групов адрес /multicast/*** - използва се за адресиране на група възли с цел предаване на едно съобщение на всички от групата едновременно
  - ***общодостъпен адрес /broadcast/*** - предаване до всички възли в мрежата или област.

8. ***Мултиплексиране –*** процес на изграждане на много едновременни съединения в една система.

9. ***Услуги на предаването*** – съществуват следните услуги:
   - *приоритетност* – по-високи приоритети се присвояват на тези съобщения, които трябва да бъдат предадени с минимално закъснение, напр. управляващите съобщения.
   - *праг на закъснението* – дефинира се за данни, чувствителни към закъснение
   - *сигурност на данните* – за целта се използват методи като: шифриране на данните, ограничаване на достъпа до информацията с пароли и права на потребителите.
   - м*ах производителност* на процесорите на мрежовите възли

Комуникационен сценарий на модела OSI

Нека имаме два процеса (A и B), изпълнявани в две различни компютърни системи (1 и 2), свързани чрез комуникационна подмрежа:



система 1

система 2

Представителен слой – едно входно съобщение идващо от приложния слой се представя в удобен за транспортиране вид т.е. преобразува се кода, съгласува се формата, след което съобщението се предава надолу към сесийния слой. А при другата страна той представя съобщението във вид, съответстващ на приложния слой на другата система.

В **сесийния слой** се организира сесия за предаване на съобщенито, т.е. установява се съединение между комуникиращите процеси А и В. Освен това протоколът осигурява:

- *поддържане на съединението със зададено качество*
- *идентификация на съединението*
- *управление на диалога*
- *разпадане на съединението*

В **транспортния слой** съобщението се транспортира по комуникационната подмрежа от "край до край", т.е. от 1 до 2. За тази цел се организира двупосочно съединение, чието състояние непрекъснато се контролира от използвания транспортен протокол. От "край до край" – програмите за взаимодействие се реализират само в крайните възли.

В **мрежовия слой** се организират съединения между съседните междинни възли /маршрутизаторите/, извършва се маршрутизация, комутация, управление на натоварването. Съобщенията се предават във вид на отделни пакети.

В **каналния слой** се организират канала за предаване на данни между всеки два съседни възела в мрежата. Информацията се представя във вид на кадри.

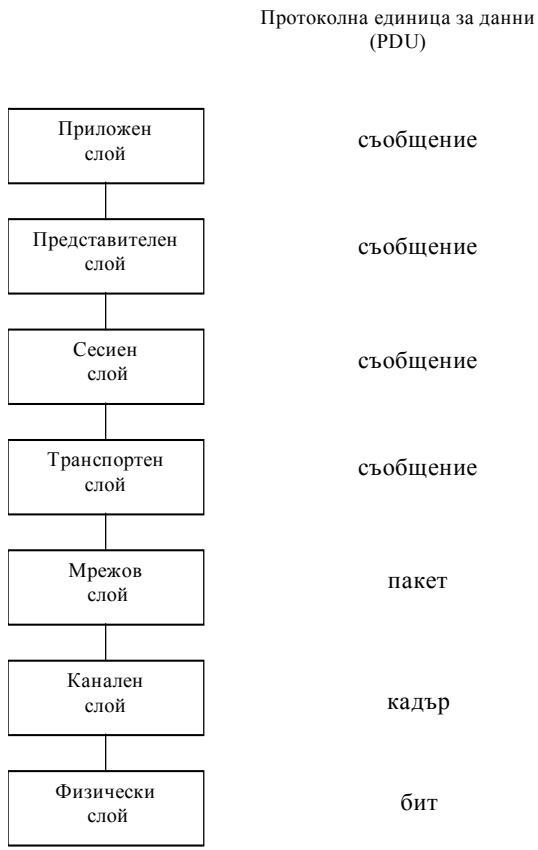
Във **физическия слой** се използва комуникационна линия /физическа среда/ за предаване на неструктуриран поток от битове, като при това може да се извърши и уплътнение на линията за едновременно предаване на няколко съобщениея по нея. Контрол на комуникационната линия.

Между равностойните слоеве на линията няма директна /физическа/ комуникация с изключение на физическите слоеве.

Във всеки слой *N* на предаващата система към протоколната единица за данни (PDU), получена от по-горния слой *N+1* се добавя собствена заглавна част *ЗЧ (header)*. Така получения блок представлява протоколна единица за данни на слой N, която се предава по-надолу към слой *N-1*.

Изключение – **<u>каналния слой</u>**, който добавя и *КЧ (крайна част)*. В приемащата система се извършват обратни преобразувания. Всеки слой освен това може да фрагментира протоколната единица с цел удовлетворение на собствените си изисквания за дължина на предавания блок данни. Съответния слой в приемащата система трябва да дефагментира данните.

Как се наричат протоколните единици за всеки слой е показано на фигурата по-долу.



I. **Физически слой** – най-долният слой на модела OSI. Той е непосредствено свързан с комуникационната линия.

Основна функция: Предаване на неструктуриран поток от битове по комуникационната линия и то по такъв начин, че когато предавателят генерира двоична единица, приемникът да я възпреме наистина като такава, а не като двоична нула. Единствено *протоколите* на физическия слой се наричат още *интерфейси*. Те реализират следните **съгласувания:**

- **механично –** задава броя и дължината на проводниците между устройствата, формите и размерите на конекторите и др.
- **електрическо** – определя формите, продължителността и нивата на сигналите /импулсите/.
- **функционално** – обуславя смисловото значение на електрическите сигнали, които си разменят съседни системи
- **процедурно** – специфицира последователността от събития, чрез която се обменя потокът от битове между мдва обекта на физическия слой.

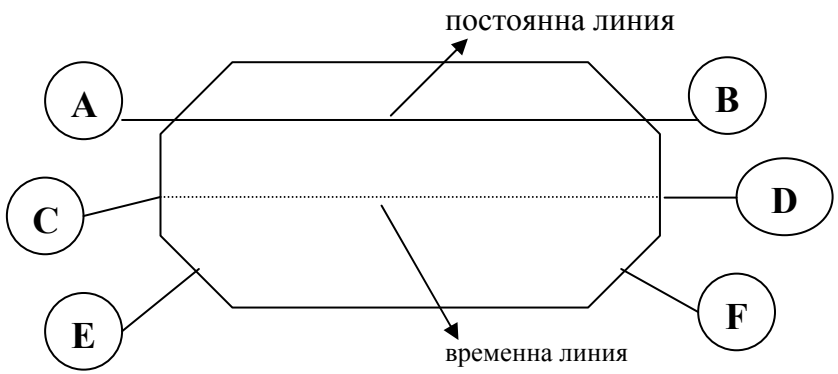
Функции на физическия слой:

1. *изграждане и разпадане на физически съединения* – тази функция е необходима поради отсъствието на физическо съединение във всеки момент между комуникиращите крайни възли /отнася се за мрежа с комутация на канали/. Физическите съединения могат да осигуряват както последователно, така и паралелно предаване на данни.

   Последователно – побитово

   Паралелно – побайтово

   Физическите съединения могат да са *постоянни* /наети линии/ или *временни* /комутируеми/.



2. *преобразуване на съобщенията в сигнали* – тази функция е свързана с необходимостта от преобразуване на предаваните съобщения в определен вид сигнали, съответстващи на изискванията на използваната физическа среда.

Съществуват 4 възможности:

- *аналогово съобщение в цифров сигнал*
- *цифрово съобщение в цифров сигнал*
- *цифрово съобщение в аналогов сигнал*
- *аналогово съобщение в аналогов сигнал*

Първите два вида преобразувания се наричат с общо име кодиране /устройството е кодер/, а обратните преобразувания /от цифров сигнал в съобщение/ се извършват от декодер. Много често кодерът и декодерът са обединени в едно устройство, наречено кодек.

Последните два вида се наричат с общото име модулация и се извършват от специално устройство, наречено модулатор, а обратните преобразувания /демодулация/ от устройство – демодулатор. Много често модулаторът и демодулаторът са обединени в едно устройство наречено модем.

3. *физическо предаване на битове* – основна функция на този слой. Тя се състои в предаване на битове без да бъдат анализирани смислово /извършава се от по-горните слоеве/. Основно изискване – предавателят и премникът да са синхронизирани помежду си по фаза и да работят с една и съща честота.
4. *синхронизация по битове* – необходима за синхронизация на приемника с предавателя по отношение на честота на предаване на импулсите. Липсата на синхронизация по битове би довела до неправилно тълкуване на предаваните импулси, а оттам – и до приемане на грешна информация. Използва се специален синхронизиращ знак, който се предава от предавателя към приемника с цел установяване на сихронизъм или за поддържане на този синхронизъм през времето, когато не се предават данни. При предаването на данни приемникът извлича тактовата честота от самите данни.

5. *реализиране на физическия интерфейс* – реализира се в зависимост от определения състав и структура на управляваните сигнали и данните, и в съответствие с препоръките на международния телекомуникационен съюз (ITU).

Примери:

- свързване на терминали към обществена телефонна мрежа чрез аналогови модеми се използва препоръка V.24
- свързване на терминали към обществена мрежа за предаване на данни са разработени препоръките X.20 и X.21

6. *диагностика на определен клас неизправности* – служи за определяне на прости неизправности от рода на: прекъсване на захранването, прекъсване на проводник.

II. Канален слой – използва услугите на физическия слой, разширява техните възможности и ги предоставя на мрежовия слой.

Основна функция: Осигуряването на надежден канал за предаване на данни /между два съседни мрежови възли/ с отсъствието на каквито и да е грешки. За тази цел данните, които трябва да се предадат, предварително се разделят на блокова, наречени кадри /frames/, с дължина обикновено от няколко стотин до няколко хиляди байта.

Готовите кадри се предават последователно в канала. Обикновено след всеки кадър, получен от приемника се очаква разписка от него към предавателя. За откриването на грешки всеки кадър се кодира с шумоустойчив код. На това ниво се генерират и флагове /поредица от битове/ към всеки кадър. Те се поставят като заглавна и крайна част с цел разпознаване на границите му. Каналният слой синхронизира скоростите на обработка на кадрите от страна на приемника и предавателя. Тябва да отбележим, че тази функция се среща и при някои по-горни слоеве от OSI модела.

В мрежите /напр. локалните/, които използват общ канал, този слой трябва допълнително да управлява достъпа до този канал. За тази цел каналният слой се разделя на **два подслоя,** по-долният, от които /MAC – подслоят/ се занимава именно с този проблем.

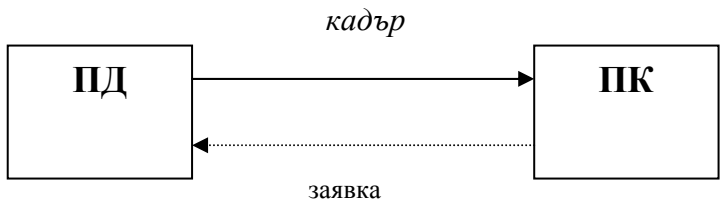
Протоколите на каналния слой се разделят на две големи групи:

- *протоколи с използване на обратна връзка*
- *протоколи без използването на обратна връзк*а

Използването или не на обратната връзка зависи от това какви канали използваме двупосочни или не.

Има три вида обратни връзки /ОВ/:

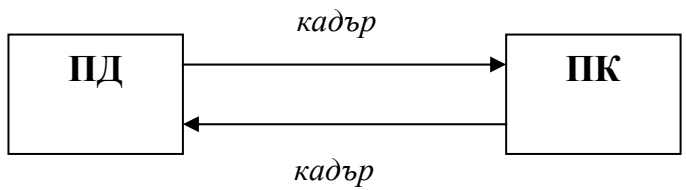
- *Решаваща обратна връзка /РОВ/* - при този вид приемникът използва шумоустойчив код, за да определи дали поредният приет кадър съдържа грешки или не. Ако кадърът е без грешка, то приемникът изпраща по канала за обратна връзка потвърждание /квитанция/ за неговото правилно приемане. Ако има грешки, то приемникът изпраща заявка за неговото повторно предаване.



2. *Информационна ОВ /ИОВ/* - при него приемникът връща обратно кадъра към предавателя, който все още пази този предаден кадър, с цел да ги сравни. Това служи за преценка дали да го изпрати отново или не.

Недостатък: всеки кадър се изпраща два пъти.

Проблем: при предаването обратно могат да възникнат грешки и предавателят да реши, че полученият от приемника кадър е грешен /съответно верен/.



Разновидности на сигнала РОВ:

- **Квитанции на РОВ** – делят се на 3 вида:
  - *частна квитанция* – с номер К указва, че кадър е номер n=К е приет правилно
  - *групова квитанция* – с номер К указва, че всички кадри с номера n ≤ К са приети правилно.

    Недостатък: при грешка се предават всички кадри от групата /дори верните/.
  - *псевдоквитанция* – с номер К указва, че кадърът е с номер n=К е приет правилно, но поради препълване на буфера трябва да се повтори отново /не е бил съхранен/.
- **Заявки за повторно предаване на кадри** /отрицателни квитанции/ - три вида:
  - *адресна заявка* N – иска повторение на кадъра с номер N
  - *групова заявка* N – иска повторение на кадри с номера n>N
  - *квазиадресна заявка* N – частен случай на груповата заявка и изисква повторение само на L на брой кадри с номера (N+1…N+L)

Формат на кадъра

флаг	адрес	управление	Данни /пакет на мреж. слой/	Контролно поле /FCS/	флаг

Форматът на кадъра зависи от протокола. Всеки протокол си има формат. По принцип, всеки кадър съдържа данни и служебна информация.

Полето <данни> съдържа пакета на мрежовия слой. Всички останали полета съдържат служебна информация, необходима за правилното предаване на кадъра.

Полетата <флаг> служат за означаване на границите на кадъра. Използват се от приемника за установяване на началото и края на кадъра.

Полето <адрес> е възела на когото го изпращаме.

Полето <управление> е за записване на служебна информация, номериране на кадрите.

Контролното поле <FCS> се използва за откриване и/или коригиране на грешки, възникнали в кадъра при предаването му по канала. При повечето канални протоколи полето <FCS> не обхваща флаговете.

За предпочитане е за всеки тип канал да се използват кадри с оптимална дължина.

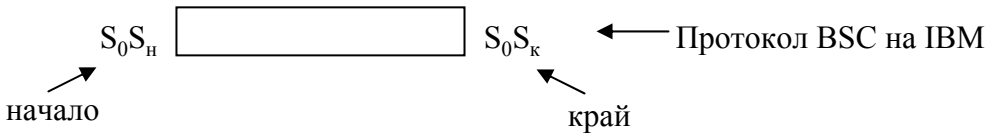
Причина: при предаване на дълги кадри /по канал с шум/ вероятността за грешка е много по-голяма. Ако дължината на кадъра се намали, вероятността за грешка се намалява, но с това и ефективната скорост на предаване, тъй като се предава повече служебна информация.

В зависимост от полетата на кадъра протолите можем да ги разделим на два вида:

- *байтово-ориентирани* - минималната смислова единица е байт и всички полета са кратни на един байт
- *битово-ориентирани* **-** дължината на кадъра може да бъде равна на произволен брой битове

Определяне на границите на кадрите – съществуват 3 метода:

- *чрез преброяване на символите в кадъра* – използват се байтово-ориентираните протоколи. В служебната информация в началото на всеки кадър се посочва броят на символите в кадъра. От другата страна приемателят разграничава кадрите чрез броене на символите
- *чрез вмъкване на служебни символи* – използва се при байтово-ориентираните протоколи. Вмъква се символ S_0. Ако се окаже, че има символ S_0, то той се дублира S_0S_0. Приемникът при два S_0S_0 премахва първия.



- *чрез добавяне/премахване на битове* – използва се при битово-ориентираните протоколи

флаг за начало - **01111110**

Във всяко поле от кадъра описан по-горе, ако се срещнат 5 единици след тях се добавя нула.

111111 ⟶ 1111101
111110 ⟶ 1111100

Действие на приемника:

III. Мрежов слой – осигурява обмяната на информация между обектите на транспортния слой.

Протоколите на първите два слоя /физически и канален/ могат да се считат за локални, защото се отнасят само за едно от ребрата на графа. За разлика от тях протоколите на мрежовия слой са глобални, защото се реализират в подмрежата като цяло и са тясно свързани с нейната топология.

Мрежовият слой управляла функционирането на подмрежата. Главна негова задача е да определи как блоковете от данни /пакети/ да се насочват правилно /маршрутизиране/ по пътя до получателя. За тази цел в междинните възли /маршрутизаторите/ на подмрежата се използват алгоритми за оптимално маршрутизиране на базата на някакъв критерий. В мрежите с общ поделен канал за предаване /напр. локалните мрежи/ маршрутизирането е просто и затова мрежовият слой е по-тънък или просто липсва. В същото време, ако твърде много пакети постъпят в един и същ момент за предаване в подмрежата, това би довело до евентуалното й задръстване. Затова мрежовият слой трябва да се занимава с това.

В общия случай мрежовият слой на възела подател формира пакет на базата от полученото от транспортния слой съобщение. Ако това съобщение е прекалено голямо, мрежовият слой го разделя /фрагментира/ на части, като всяка част постава в полето <данни> на поредния кадър. С помощта на физическия слой този кадър се изпраща като неструктуриран поток от битове към първия междинен възел /маршрутизатор/ на подмрежата. В този маршрутизатор кадъра се извлича, проверява се за грешки и ако всичко е наред, от него се извлича капсулирания пакет, който се предава нагоре към мрежовия слой на маршрутизатора. В него /по служебната информация/ се извършва определяне на по-нататъшното направление за преминаване на пакета през подмрежата. След това пакетът отново се капсулира в кадър, който се изпраща към следващия маршрутизатор. Тези действия се повтарят, докато пакетът стигне до крайния възел получател.

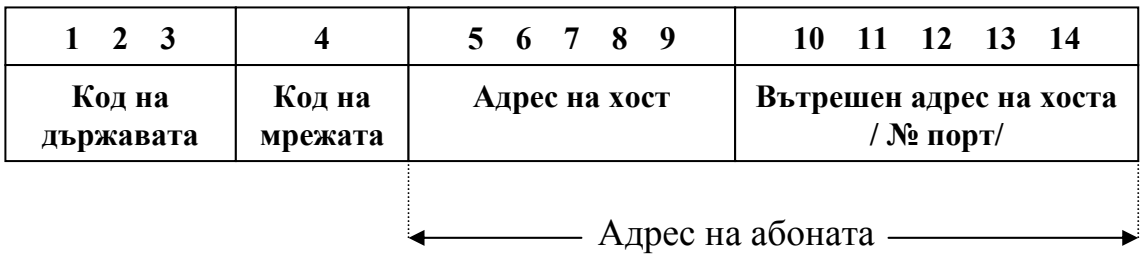
OSI моделът определя *два вида услуги* на мрежовия слой:

- *мрежови услуги с установяване на логическо съединение* – осигуряват надеждно предаване на данни по предварително изградено логическо съединение
- *мрежови услуги без установяване на логическо съединение* – използват се дейтаграми, които се предават независимо един от друг. Мрежови протоколи без установяване на съединения: IPX на фирмата Novell, IP от протоколния стек TCP/IP

Основни функции на мрежовия слой:

- *адресация* – необходима е еднозначна идентификация на адресираните обекти на мрежовия слой. Обикновено се използва йерархичен принцип на адресация, при който пълният адрес се състои от няколко степени, като първата от тях специфицира адреса на мрежата, втората – адреса на крайния възел /хоста/, третата – идентификатора на виканата програма /порта/.

Пример :



Формат на мрежовия адрес, използван от протокола X.25 (по препоръка X.121)

Пример :

IPv.4 – използва 4 байтов адрес. Йерархията е по-проста. Състои се от две степени:

- *адрес на мрежата* /**Net ID**/
- *адрес на хоста в нея* /**Host ID**/

Границата между тях се определя от т.нар. “подмрежова маска”.

- *маршрутизация* – най-важната функция на мрежовия слой. Свързана е с избиране на оптимален маршрут за преминаване на пакетите през подмрежата на базата на предварително зададен критерий. Методите на маршрутизация се разделят на две големи групи:

- **Фиксирани методи** – при тези методи изборът на направление не зависи от моментното състояние на мрежата. Използват се за мрежи с проста топология.
- **Адаптивни методи** – при тях се използва текущата информация за състоянието и натоварването на подмрежата. Потоците от пакети се преразпределят в зависимост от създадената конкретна ситуация. Междинните мрежови възли /маршрутизаторите/ обменят помежду си служебна информация за дължината на опашките и за натоварването на процесорите си, за наличието на подмрежи в мрежата.

Адаптивните методи се делят на:

- *Дистанционно-векторни алгоритми* – при този вид алгоритми всеки маршрутизатор поддържа таблица /вектор/, съдържаща най-кратки разстояния по различните направления в подмрежата /до всеки друг маршрутизатор/. Всеки маршрутизатор периодично обновява таблицата си чрез обмен на информация със своите съседни маршрутизатори. Разстоянието – в скокове /hops/ т.е. чрез броя на междинните маршрутизатори, през които трябва да премине пакетът.

Метрики:

- *Скокове*
- *Общата дължина на опашките от чакащи пакети по маршрута, чакащи на изходните портове*
- *Натоварване на процесора на маршрутиза*
- *Време за закъснение на пакетите – всеки маршрутизатор измерва закъснението за доставка на пакетите чрез специални ехо-пакети, които му се връщат "подпечатани" от съседите му*

Дистанционно-векторните алгоритми работят добре само в неголеми подмрежи /необходим е голям брой итерации/. Примерни протоколи RIP и IGRP използващи се в Internet

- *Алгоритми на състоянието на каналите* – при този вид алгоритми всеки маршрутизатор изпраща на всички останали маршрутизатори в подмрежата не цялата си маршрутна таблица, а само тази нейна част, описваща състоянието на неговите собствени канали /към съседните маршрутизатори/. С други думи, при тези алгоритми се изпращат неголеми корекции, но до всички маршрутизатори, докато дистанционно-векторните алгоритми изпращат големи корекции, но само до съседите.

Работа на маршрутизатора:

1. Открива съседите си чрез изпращане на специални пакети Hello и научава мрежовите им адреси /от пакета отговори/
2. Измерва закъснението /чрез ехо-пакети/ и цената на предаване на всеки свой съсед
3. Констуира и изпраща пакета до всечки маршрутизатори, съдържащ току-що научената информация.
4. Изчислява най-късия път до всеки друг маршрутизатор в подмрежата.

В резултат на тези действия всеки маршрутизатор получава достатъчна информация за постояване на точен граф на подмрежата.

!!! *По-трудно се реализира. Изисква по-мощни процесори от страна на маршрутизаторите.*

От друга страна методите на маршрутизация се делят на:

- *Децентрализирани* – при тях маршрута за предаване на пакета се преценява от всеки възел в зависимост от неговата преценка т.е. във всеки момент мрежата представлява един притегателен граф.
- *Централизирани* – всяка мрежа си има управляващ възел, който решава маршрута на пакета. С цел да не се блокира подмрежата при случайна негова повреда, той се дублира.

- *комутация* – използва се главно при глобални компютърни мрежи (WAN). Сега намира приложение и при LAN /извършва се в каналния слой/. Тя е функция на междинните мрежови възли, която е наложителна поради липсата във всеки момент на пряко съединение между всеки два крайни възела на подмрежата /с цел – икономия на средства.

Функцията му е да пренасочи съобщението от даден канал на входна линия към определен канал на изходна линия, определена от алгоритъма, който се използва за маршрутизация.

- *управление на натоварването* – свързано е с избягването на задръствания на подмрежата, при което рядко се влошават нейните характеристики. Претоварването може да има:
  - *Локален характер* – обхващащ част от подмрежата
  - *Глобален характер* – пълно блокиране на всички информационни потоци в подмрежата

Причини за претоварването:

- Увеличаване на броя на генерираните в подмрежата пакети
- Наличието на тесни места в подмрежата /комуникационни линии с малък капацитет, или комутатори/маршрутизатори с бавни процесори/
- Грешки в механизма за управление на потока данни

Управлението на натоварването се различава от управлението на потока данни. *Управлението на натоварването* – глобално понятие, свързано е с възможността на подмрежата да пренесе целия, предложен от крайните възли, трафик. *Управлението на потока данни* – отнася се не за целия трафик в подмрежата, а само за трафика между две точки. Основна негова задача е да се избегнат ситуации, при които една точка /предавателят/ работи непрекъснато с по-голяма скорост от другата точка /приемника/.

IV. Транспортен слой – осигурява обмен на данни между компонентите на сесийния слой с необходимото качество на обслужване.

Главна задача: Приемане на данни от сесийния слой, да ги раздели /при необходимост/ на по-малки единици и да ги предаде към мрежовия слой, като гарантира, че те ще пристигнат в същия правилен ред в другия край на комуникацията.

Транспортните протоколи осигуряват доставка на съобщения между крайните възли на мрежата, т.е. те работят "от край до край". Казано иначе, програмите осъществяващи функциите на транспортния слой се стартират в двата крайни възела и взаимодействат непосредствено една с друга /използват заглавната част на протоколните единици/. За разлика от транспортните протоколи протоколите от по-долните слоеве /физически, канален, мрежов/ не работят "от край до край", а осигуряват доставка на информация по отделните участъци на подмрежата /т.е. реализират се между всеки два съседни мрежови възела/. С други думи транспортните протоколи, и всички над тях, се реализират само в крайните възли, а протоколите на по-долните слоеве се реализират и в междинните мрежови възли. Всеки мрежов възел /междинен/ има мрежов модул и по два канални и физически модула. Следователно, транспортният слой осигурява отдалечен информационен обмен между крайни възли /хостове/. Приложните процеси в един и същи хост използват сесийния слой за взаимодействие. Така за тях най-ниския слой е сесийният.

Услуги – два вида:

- *услуга с установяване на логическото съединение* – при нея предварително се изгражда логическо съединение между транспортните модули в двата крайни възела. Комуникационният процес се състои от три фази:
  - *установяване на съединение*
  - *предаване на данни*
  - *възстановяване на системата*
- *услуги без установяване на логическо съединение* – при нея имаме предаване на транспортните блокове без установяване на съединение и без предварително споразумение. Този вид услуги се използват, когато не се изисква голяма надеждност при предаването, тъй като при тях е възможно загубата на блок или разбъркване на реда на следване на отделните блокове. Възстановяването на този тип грешки е функция на протоколите от по-горните слоеве.

По принцип няма пряка зависимост между транспортните и мрежовите услуги от двата вида. Всеки от двата вида транспортни услуги може да бъде използван с всеки от двата вида мрежови услуги. Когато се използва транспортен протокол с установяване на съединение над мрежов протокол от същия вид подреждането на пакетите, проверката за грешки и издаването на квитанции се извършва от мрежовия слой и след това се повтаря от транспортния слой.

При използване на транспортен протокол с установяване на съединение /напр. TCP/ над мрежов протокол без установяване на съединение /напр.IP/, транспортният протокол разделя потока данни, идващ от горния слой, на отделни блокове, които в мрежовия слой се капсулират в IP-дейтаграми, всяка от които се предава независимо от другите /преминават през различни маршрути – възможно/. Транспортният слой от друга страна се грижи за правилното подреждане на сегментите. Потвърждава блокове, приема нови.

Функции на транспортния слой:

- *изграждане и разпадане на транспортни съединения, свързващи крайните възли* – най-използваният тип транспортно съединение е тип "от край до край" без грешки при предаването, което гарантира получаването на съобщенията в същия ред, по който са били изпратени.
- *обединяване на няколко съединения в едно мрежово /мултиплексиране нагоре/ и обратно – осъществяване на едно транспортно съединение по няколко мрежови съединения едновременно /мултиплексиране надолу/* - при нормални условия транспортният слой изисква отделно мрежово съединение за всяко транспортно съединение, искано от сесийния слой.

  Ако обаче се налага транспортното съединение да се с висока производителност, транспортният слой може да изиска няколко мрежови съединения, разпределяйки данните за едновременно предаване по тях с цел повишаване на производителността.

  Ако създаването на такова мрежово съединение е скъпо, транспортният слой може да мултиплексира няколко транспортни съединения за предаване на едно и също мрежово съединение с цел намаляване на цената.
- *управление на последователността и цялостта на транспортните блокове (PDU), предавани през транспортното съединение*
- *откриване на процедурни грешки, извършване на тяхното частично коригиране; издаване на съобщения за некоригирани грешки*

- *управление на покота транспортни блокове* – старт-стоп медодът – нежелателен. Използва се процедура с плъзгащ се и достатъчно широк прозорец

- *потвърждаване на правилно приетите транспортни блокове*

- *предоставяне на приоритет при предаване на транспортните блокове*

- *съответствие между мрежови адреси и транспортни одреси на доставянето* – транспортните адреси се използват за изграждане и идентифициране на транспортните съединения. Много от крайните възли /хостовете/, участващи в комуникацията се свързват с множество транспортни съединения.

!!! Транспортния слой /и всички слоеве над него/ се реализират софтуерно чрез програмни модули.

V. **Сесиен слой** – осигурява съединения /сесии/ непосредствено между конкретна двойка приложни процеси /свърза портовете им/.

Два вида функции:

- *Обслужване на сесиите*
- *Диалогова форма на предаване на данните*

Сесия – последователността от процедури на диалога на обектите от представителния слой, извършван по съединения на сесийния слой. Сесията позволява предаване на данни, както транспортното съединение, но с подобрено обслужване. Напр. сесия се установява при предаване на файлове между два компютъра.

Понеже с транспортни адреси се борави трудно, сесийният слой трябва да допусне работа със символни имена, които да се изобразяват в транспортни адреси.

При изграждане на дадена сесия могат да бъдат установени някои съглашения за нея:

- използване на полудуплекс или дуплекс /съглашения за диалогова дисциплина/
- размер на прозореца
- наличие на шифриране или не

Основни функции на сесийният слой:

- установяване на сесия, определяща началото на диалога между обектите на представителния слой
- избор на процедури за сесията, подбор на параметри, идентификация на сесии

Основни функции на сесийният слой:

- установяване на сесия, определяща началото на диалога между обектите на представителния слой
- избор на процедури за сесията, подбор на параметри, идентификация на сесии
- управление на диалога – поддръжка на дуплекс или полудуплекс при предаването. Сесийният слой се грижи за редуването при предаване при полудуплекс
- възстановяване на сесията при поява на грешка от различен вид /чрез синхронизационни точки/ - сесийният слой поставя т.нар. синхронизационни точки, за да може при грешка при предаването на ниво транспортен слой да се връща към последната достигната синхронизационна точка

Пример:

При трансфер на файлове не е задължително всеки път да се започва отначало при прекъсването му.

- обмен на данни между представителния слой
- прекратяване на сесията при край на диалога
- работа с пароли за потребителите на локални компютърни мрежи /LAN/, а също и проверката им – в частност.
- осигуряване на статистическа информация за работата на LAN – кой предава, колко често, колко дълго и кога.

Сесийният слой предлага услуги само с установаване на съединение. Преминава се през познатите 3 фази:

- *установяване на съединението*
- *предаване на данни*
- *възстановяване на системата*

VI. **Представителен слой** – свързан е със синтаксиса и семантиката на предаваната информация. Предназначението на този слой е да преобразува данните /предавани от приложния слой към сесийния и обратно/, свързано с определянето на техните формати, кодове и структури. При предаване на данните към приложния слой представителният слой подготвя няколко форми на представяне, от които приложният слой избира най-подходящия. При необходимост представителният слой извършва компресиране и шифриране на данните.

Основни функции:

- преобразуване на данните
- управление на форматите
- разкриване на семантиката на данните
- форматиране на текстовете /разделяне на страници, отделяне на броя на редовете на екрана, преместване на курсора/
- кодиране на данните – ASCII – за обмен на информация в персоналните компютри, EBCDIC – разширен двоично-десетичен код за обмен на информация, използван в големите компютри на IBM
- съединение на приложните процеси с логически съединения, представени от по-долни слоеве.
- защита на информацията в мрежата от неоторизиран достъп чрез шифриране.

Представителният слой предлага услуги само с установяване на съединение .

Фази:

- *изграждане на сесия* – подава се команда към сесийният слой за изграждането на такава
- *управление вида на представянето* – избира се един от видовете представяния и се определят параметрите му
- *фаза на предаване на данни между приложние процеси* – при необходимост се извършват: преобразуване на данните, идентификация, компенсиране, шифриране.
- *завършване на процедурата на представяне на данните*

Една от основните функции на представителния слой е кодирането на данните по предварително съгласуван /стандартизиран/ начин.

Пример:

Различните видове компютри използват различни кодове за представяне на символи – ASCII, Unicode, EBCDIC и начини за представяне на числа. Затова е необходимо за комуникацията между различни видове машини структурите от данни да бъдат дефинирани по абстрактен начин. Представителният слой борави именно с тези абстрактни структури от данни, като извършва преобразуване от представянето в компютрите, към стандартното представяне в мрежата и обратно.

VII. **Приложен слой** – осигурява средства за достъп на приложните процеси до OSI обкръжението. Този слой е основен в OSI модела, защото всички останали се грижат за неговото функциониране. Той осигурява взаимодействието между приложните процеси, разположени както в един хост, така и в различни хостове.

Приложен процес – елемент на системата, който извършва съдържателна обработка на информация в съответствие с основната целева функция на системата.

Примери:

- работата на оператор на пулта на терминал или компютър
- изпълнение на програма, опериращa с данни, в някакъв компютър.

Най-важни приложни протоколи:

- *File Transfer, Access and Management (FTAM)* – необходим за преодоляване на различни файлови системи при предаване на файлове между тях. Осигурява следния комплект услуги за предаване на файлове между две системи:
  - създаване и изтриване на файлове
  - четене и запис на файлове
  - четене и промяна на файлови атрибути
  - изтриване на съдържанието на файл и др.

FTAM услугите се използват между следните видове файлове:

- *текстови и двоични*
- *с последователен и произволен достъп*
- *с иденксиране по един ключ*
- *файлове от директории*

- *Virtual Terminal (VT)* – емулира терминал, необходим за преодоляване на несъвместимостта при взаимодействие на терминали от различен вид.

Възможен начин – дефиниране на абстрактно звено при взаимодействието на различните по тип терминали. За всеки тип терминал трябва да се напише програма, която да преобразува функциите на мрежовия виртуален терминал в съответните функции на реалния терминал.

- *Протокол MOTIS (Message Text Interchange Standard)* – позволява на потребителите да обменят помежду си пощенски съобщения, като използват механизма за междинно съхранение и препредаване. Всяко съобщение се състои от плик и съдържание. Пликът съдържа служебна информация, необходима за доставка на съобщението до получателя.

Примери:

OSI – MOTIS
TCP/IP – SMTP

- *Протокол CMIP за управление на мрежата* – позволява задаването и конфигурирането на мрежовите ресурси, контролирането и отстраняване на грешки и проблеми.

ISO определя пет области за управлението на мрежата:

- *управление на конфигурацията на мрежата* - включва първоначално инсталиране на хардуера и софтуера на мрежата и определяне на параметрите й.
- *управление на производителността* – включва събиране, съхранение и обработка на информацията за работа с мрежата.
- у*правление на грешките и неизправностите, възникнали по комуникационните линии по време на работа*

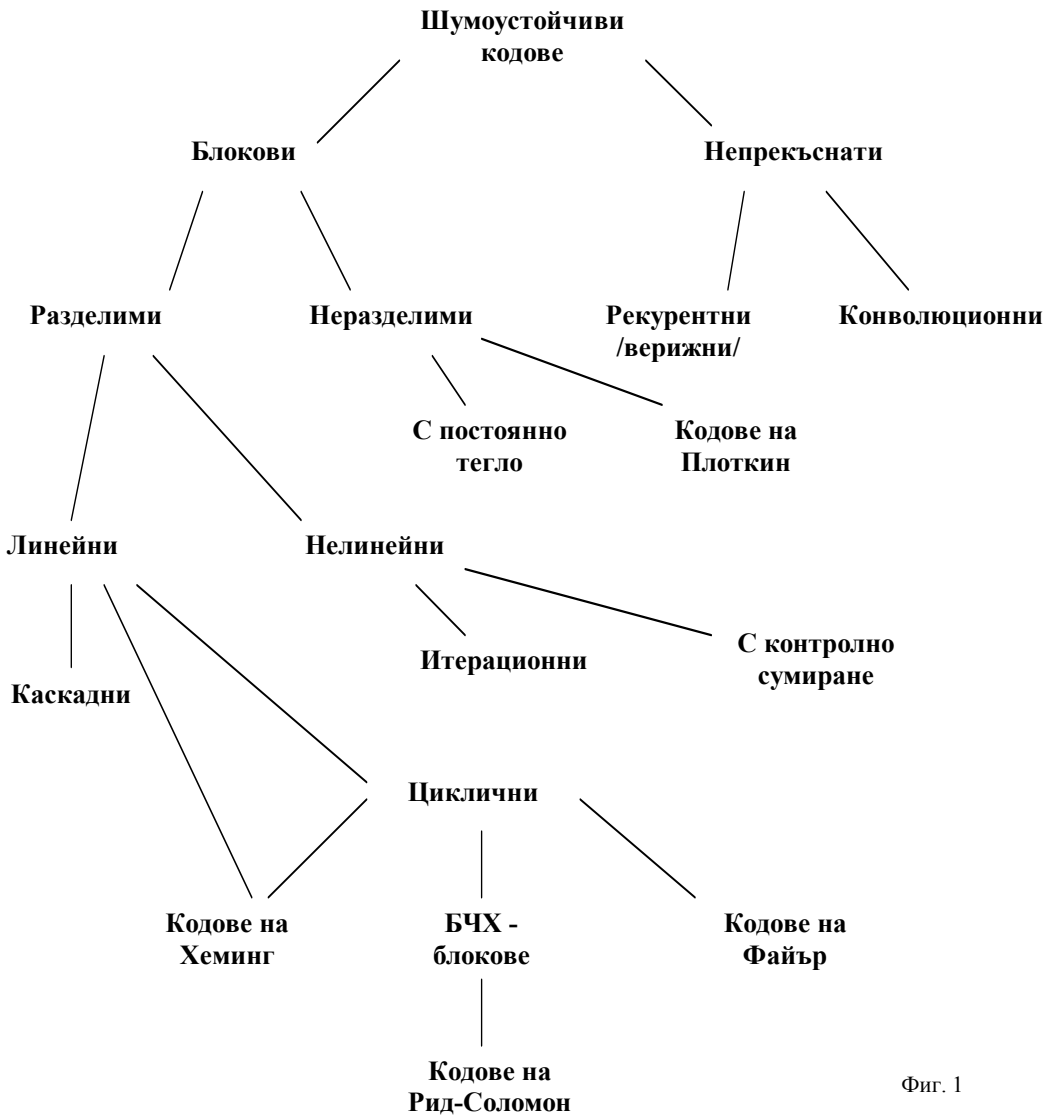
- у*правление на грешките и неизправностите, възникнали по комуникационните линии по време на работа*
- *управление на отчетността и използването* – включва средства за натрупване на отчетна информация за използването на мрежовите ресурси.
- *управление на достъпа и сигурността на информацията* – включва средства за управление на достъпа на потребителите до мрежовите ресурси.

- *Протокол X.500 за обслужване на директории* – осигурява достъп до хранилище на информация за набора от налични мрежови обекти:
  - *потребители на мрежата*
  - *ресурси на мрежата*
  - *мрежови приложения*

Предлага глобален сигурен достъп цо имформационното хранилище (наречено директория). Директорията може да е съставена от една или няколко отворени системи, които управляват базата данни на мрежовите обекти т.е. базата данни може да се намира на един компютър или да е разпределена на много такива.

Шумоустойчиво кодиране цифрови съобщения

Класификация на шумоустойчивите кодове

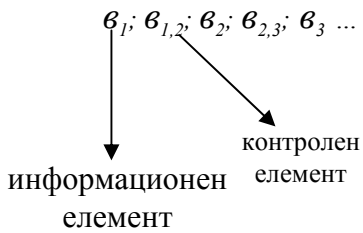


Фиг. 1

Шумоустойчивите кодове се делят на две големи групи: **непрекъснати** и **блокови** кодове.

Непрекъснати кодове – не разделя предаваната информация, а разполага контролните елементи в определен ред между информационните. Процесите "кодиране" и "декодиране" също имат непрекъснат характер. Тези кодове са подходящи за откриване и коригиране на пакетни грешки. Делят се на:

- *рекурентни кодове* – вид непрекъснати кодове. В най-простия вариант информационният елемент се редува с контролен елемент



$\oplus$, *XOR*

000
101
011
110

където $в_i \in \{0,1\}$

$в_{i,i+1} = в_i \oplus в_{i+1}$ *– контролен елемент*

Ако:
n – общ брой елементи,
k – брой информационни елементи,
то (k/n) *код е този код - за случая* (1/2) *код.*

При този код грешката в елемент b_i ще доведе до грешка в равенството за двата съседни контролни елемента $b_{i-1,i}$ и $b_{i,i+1}$. За да действа кодът е необходимо между два грешно приети елемента да има поне три вярно приети.

В общия случай контролните елементи се формират чрез събиране по *mod 2* (*XOR*) на два информационни елемента, намиращи се на разстояние *i* един от друг.

i – *стъпка на събирането*. Стъпката се определя на базата на статискическата информация за използвания канал, зависи от "паметта" на канала.

- *конволюционни кодове* – заложен е принципа на формиране на поредицата от контролни елементи чрез линейна комбинация на елементите от информационната поредица, които постъпват непрекъснато на входа на кодера. Той има *k* входа и *n* изхода. Във всеки дискретен момент на входовете на кодера постъпват *к* информационни елемента, а от изходите му излизат $n=k+r$ елемента, от които ***r*** са контролните.

Блокови кодове – информационната поредица се разбива на отделни блокове , които се кодират и декодират независимо една от друга. Те се делят на *разделими* и *неразделими*.

- *разделими кодове* – информационните и контролните елемети заемат едни и същи места във всички кодови комбинации. Обозначават се, като *(n, k)* – кодове, където *n* – общия брой на елементите в блоковата комбинация, *k* – брой на информационните елементи, $r=n-k$ – броят на контролните елементи в комбинацията.
- *неразделими кодове* – отсъства деление на информационни и контролни елементи.

Останалата част от йерархията в класификацията на шумоустойчивите кодове са показани на фиг. 1.

Основни понятия

Разстояние на Хеминг – броят на елементите, по които две кодови комбинации се различават една от друга. Използва се $\oplus$ *(XOR – сумиране по mod2)*

Пример:

$$\begin{array}{l} \oplus\ 101001 \\ \underline{\quad 100000} \\ \quad 001001 \end{array}$$

разлики

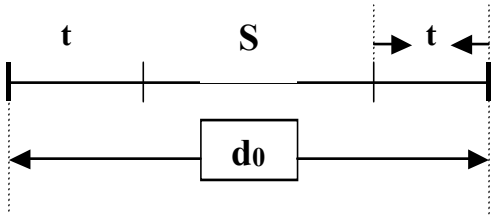
Кодово разстояние: min от всички разстояния на Хеминг за дадения код. Ще го означаваме с d_0.
Тегло на кодовата комбинация – броят на едничните елементи (двоичните единици) в нея.
Вектор на грешката (**e**) - комбинация от същия брой елементи (битове), като дадена кодова комбинация, но съдържа единични елементи (двоични единици) в местата на грешките при предаването на комбинацията, а нули – където няма грешки.
Спектър на кода – списък на разрешените кодови комбинации, разпределени по тегла, т.е. колко разрешени кодови комбинации на дадения код съответстват на всяко тегло.

Режими на използване на шумоустойчивите кодове

За повишаване на верността на предаването на цифрови съобщения шумоустойчивите кодове се използват в следните режими :

1. **Режим на откриване на грешки –** най-често използвания режим, тъй като излишеството, което е необходимо за откриване на грешките, е по-малко от излишеството необходимо за тяхното коригиране. Повишаването на верността се осъществява чрез използване на обратна връзка (квитанции или заявки). Използват се главно два вида кодове: циклични и итерационни. Обяснява се с простотата на реализиране на кодека. Код с кодово разтояние d_0, работещ в режим на откриване на грешки, може гарантирано да открива всякакви конфигурации от не повече от d_0-*1* грешки във всяка своя кодова комбинация.
2. **Режим на коригиране на грешки –** този режим се използва по-рядко и само ако обратната връзка е невъзможна или нецелесъобразна. В тези случаи се използват рекурентни, итерационни или каскадни кодове. Код с кодово разстояние d_0, работещ в режим на коригиране на грешки, може гарантирано да коригира $[(d_0-1)/2]$ грешки във всяка своя кодова комбинация (*[a] – цялата част на числото a*).
3. **Режим на частично коригиране с частично откриване на грешки**

   В някои случаи се оказва по-ефективно коригирането на грешки с малка кратност в съчетание с откриване на останалите грешки /с по-голяма кратност/. В този режим код с кодово разстояние d_0 може да коригира t грешки включително ($0 \le t \le [(d_0-1)/2]$) и да открива конфигурации от s грешки ($t < s < d_0-t$), във всяка своя кодова комбинация.



Обобщение за шумоустойчив код с кодово разтояние d_0 :

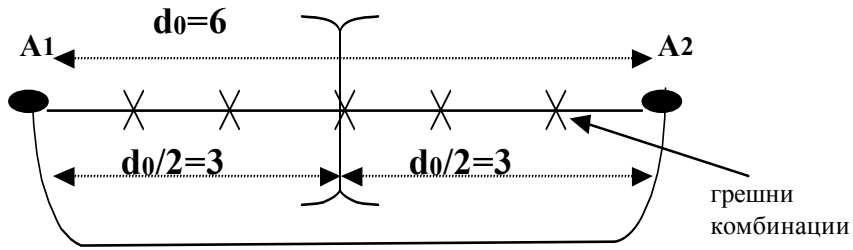
- откриване на грешки до d_0-*1*;
- коригиране до *[(d_0-1)/2]* грешки;
- коригира до *t* грешки включително $0 \le t \le [(d_0-1)/2]$, открива до *s* грешки ($t < s < d_0 - t$);

Пример:

При шумоустойчив код с кодово разтояние $d_0=6$ в зависимост от режима на използване:

- или открива всякакви конфигурации от не повече от 5 грешки.
- или коригира 1 или 2 грешки.
- или коригирайки до 1 грешка, да открива 2, 3, 4 грешки.
- или коригирайки до 2 грешки включително да открива 3 кратна грешка.

Нека A_1 и A_2 са две разширени кодови комбинации на шумоустойчив код с разстояние d_0, намиращи се една от друга на най-малкото възможно разстояние за дадения код, т.е. на разстояние d_0.



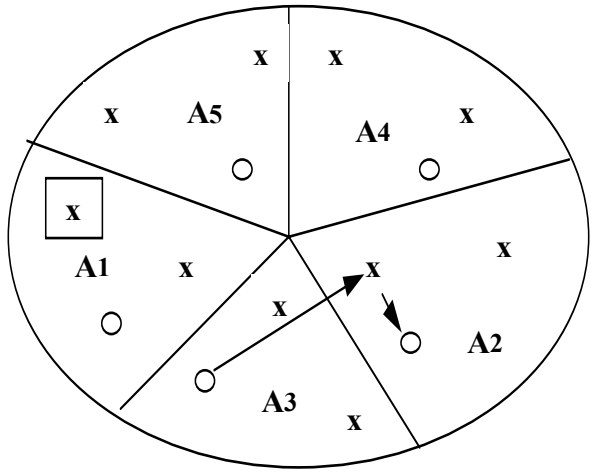
всяка грешка с кратност до d0-1 попада вътре

Най-вероятни са грешките с малка кратност. Това означава, че ако бъде приета кодова комбинация, попадаща в лявата половина на A_1A_2, то тя ще се възприеме от декодера на приемника като разрешената комбинация A_1 . Ако приетата комбинация попадне в дясната половина на A_1A_2, то декодерът взема решение, че това е повредена разрешена кодова комбинация A_2. Така всяка забранена комбинация се възприема от декодера като най-близо разположената до нея разрешена комбинация.

Ако $d_0 = 2k$, то средата не е ясно към кой край принадлежи, затова декодерът може да коригира грешки с кратност по-малка или равна на $(d_0/2)-1$;

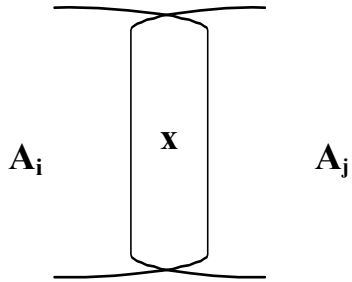
Ако $d_0 = 2k+1$, то грешката е с кратност по-малка или равна на $(d_0-1)/2$;

Можем да обединим двете неравенства в едно, където грешката е с кратност по-малка или равна на $[(d_0-1)/2]$, където $[в]$ е цялата част на $в$.



Всички комбинации се разделят на подмножества M_i, $i = 2k$. Около всяка разрешена комбинация се разпределят няколко неразрешени.

Желателно е подмножествата да не се пресичат, но не е задължително. Ако приетата кодова комбинация попадне в M_i, то декодерът взема решение, че е предадена разрешена кодова комбинация A_i. Понякога коригирането на грешки не е правилно /*виж фигурата горе*/. Ако множествата се пресичат и приетата кодова комбинация попадне в сечение на няколко подмножества M_i, то декодерът я бракува и подава заявка за нейното повторно предаване.



Алгоритъм на декодиране с корекция на грешките по принципа на максималното правдоподобие:

- *приетата комбинация Y се събира по mod2, последователно и поотделно с всички разрешени кодови комбинации A_i и се изчислява $e_i=A_i \oplus Y$*
- *определя се e_s с минимално теглото t_s*
- *$e_s \oplus Y = A_s$*

Основни задачи за генериране на шумоустойчив код

- **Задача за намиране на максимален код** – при даден брой разрешени кодови комбинация $N_0=2k$ и дадена дължина на кода n да се намери код с най-голямо разстояние d_0, т.е. код, осигуряващ максимална шумоустойчивост при зададено излишество.
- **Задача за намиране на код с минимално излишество** – при дадени N_0 и d_0 да се намери код с минимална дължина n, т.е. код, осигуряващ минимално излишество при зададена шумоустойчивост.
- **Задача за намиране на оптимален код** – При дадени n и d_0 да се намери код с максимално N_0, т.е. осигуряващ максимална ефективност при зададена шумоустойчивост.

Примери за кодове

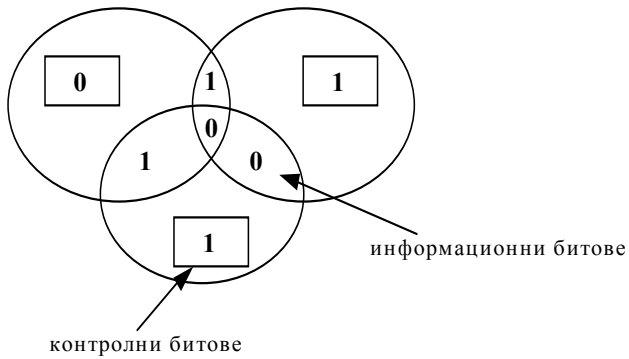
Линейни кодове

Линейно кодиране с една проверка по четност

Отбелязваме *(n,n-1)*. При него към всеки *n-1* информационни елемента се добавя един контролен елемент (бит), който е равен на сумата им по *mod2***.** По този начин, ако броят на единичните информационни елементи е четен, се добавя нулев контролен елемент. И обратно, ако броят на единичните информационни елементи е нечетен, се добавя единичен контролен елемент. Тогава всяка кодова комбинация ще съдържа винаги четен брой единични елементи. Кодово разстояние е $d_0 = 2$ – едно за информационния бит и едно за контролния бит. Този код да открива грешки с нечетна кратност, т.е. еднократна, трикратна, петкратна.

Код на Хеминг с кодово разстояние 3

Коригира всички еднократни грешки. По принцип, за такива линейни кодове броят на синдромите трябва да бъде *n+1*. а броят на контролните битове трябва да е $r \geq \log_2(n+1) \Rightarrow 2^r \geq (n+1) \Rightarrow 2^k \leq 2^n/(n+1)$. Това неравенство ни дава възможност при зададен брой *k* на информационните битове в кодовата комбинация да подберем нужната й дължина *n*. Такъв е кодът е *(7,4)*. Пояснява се с теоретична интерпретация:



Цел: Запазване на четността на двоичните единици във всеки кръг.

Получената по този начин кодова комбинация се изпраща към приемника, който от своя страна извършва проверка по четност във всеки от мислените кръгове.

Ако и трите проверки се окажат правилни, значи няма грешки.

Ако само една от проверките е грешна, значи при предаването е бил сгрешен съответният контролен бит на кръга с нарушена четност.

Ако две от проверките са грешни, значи е бил сгрешен информационния бит, намиращ се в сечението на съответните два кръга.

Поправка: инвентира сгрешеният информационен блок.

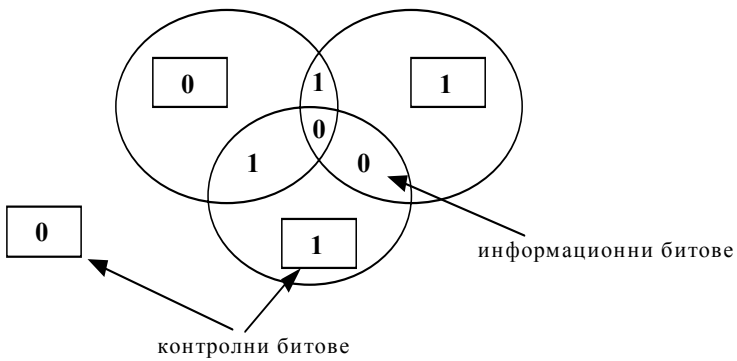
Ако и трите проверки се окажат грешни, значи е бил сгрешен информационния бит, намиращ се в сечението на трите кръга.

Поправка: инвентира сгрешеният информационен бит.

Код на Хеминг с кодово разстояние 4

Този код коригира еднократни грешки и открива всички двукратни грешки в кодовата комбинация. Такъв е кодът *(8,4)*, подобен на *(7,4)*.

Разлика: Един контролен бит с проверка по четност и обхваща всичките битове на кодовата комбинация.



Приемникът извършва по четност проверка за всеки от трите кръга плюс обща поверка по четност на битовете. При наличие на едно кратна грешка в комбинацията, това се констатира чрез нарушена обща проверка по четност плюс грешка в проверката на един или повече кръгове /както при горния алгоритъм, тук добавяме – ако е сгрешена общата проверка, без да е засегнат някой от кръговете, значи е сгрешен общият контролен бит/. При наличие на двукратна грешка в кодовата комбинация, нейното присъствие се констатира по нарушената проверка в един или повече кръгове, съчетана с правилна обща проверка по четност на битовете на комбинацията. Такава комбинация мсе бракува и приемника изисква повторението и от предавателя.

Код с просто повторение на кодовата комбинация

Всяка кодова комбинация се предава два пъти последователно, като втората част играе ролята на контролна спрямо първата. Позволява откриването на всички видове грешки с изключение на грешките в двойка елементи, заемащи една и съща позиция в първата и втората част на комбинацията.

Циклични (CRC) кодове

Намират широко приложение. Името им произлиза от основното им свойство: ако кодовата комбинация $\mathbf{a}_1$, $\mathbf{a}_2$ … **a**n, принадлежи на цикличен код, то и **a**n, **a**1 … **a**n-1 и т.н. също принадлежат на дадения цикличен код.

Друго свойство: Всички кодови комбинации разрешени за даден цикличен код се делят без остатък на един специален полином *P(x)*. Забранените комбинации на кода дават остатък при деление на *P(x)*. Всяка кодова комбинация може да се представи като полином, като всеки неин елемент се разглежда като коефициент пред степен на променливата *x*, съответстваща на мястото на дадения елемент в комбинацията.

Пример:

11011 $x^4 + x^3 + x + 1$

Множеството от всички полиноми отговарящи на допустимите кодови комбинации на даден цикличен код – поле на Галоа *GF(x)*, в което действията над коефициентите на полиномите /събиране, умножение, деление/ се извършват по *mod2*.

P(x) на *(n,k)* цикличен код трябва да удовлетворява следните условия:

- да е неразложим
- да дели без остатък полинома x^n-1
- степента му да се равна на броя на контролните елементи $r = n-k$ в кодовата комбинация
- да е примитивен, т.е. да дава максимален брой остатъци, по които да могат да се коригират различни грешки

Алгоритъм на кодера на CRC код

- полиномът *A(x)*, съответстващ на информационната поредица, която трябва да се кодира, се умножава с x^{n-k}.
- полученият полином *A(x)*. x^{n-k} се дели на образуващия полином *P(x)* и се намира остатъка от делението *R(x)***.**
- полиномът *R(x)* се прибавя (по *mod2*) към делимото *A(x)*. x^{n-k}. $F(x) = R(x) \oplus A(x)$. x^{n-k} – съответства на информационната поредица, която се предава по канала.

Кодерът от този вид може да се реализира хардуерно и софтуерно, като хардуерното е по-бързо.
При $n >> 100$ е необходимо използването на специализирани микропроцесорни чипове.

Пример:

информационна поредица – *1011*
цикличен код - *(8,4)*
образуващ полином – $P(x) = x^4 + x + 1$

Стъпка 1:

Стъпка 2:

$$\begin{array}{r} 10110000 \quad \vert\, 10011 \\ \oplus\ 10011 \\ \hline 10100 \\ \oplus\ 10011 \\ \hline 1110 \end{array} \longrightarrow \text{остатък}$$

Стъпка 3:

$$\begin{array}{r} 10110000 \\ \oplus\ 1110 \\ \hline 10111110 \end{array}$$

CRC – декодиране

При декодиране на кодови комбинации на циклични кодове се използва същото деление на образуващия полином на кода. Всяка пристигнала в приемника комбинация се дели на образуващия полином, при което се определя остатъка от делението

F`(x): P(x) → S(x) – синдром на цикличния код – показва дали в приетата комбинация има грешка или не. Ако получената комбинация се дели без остатък на *P(x)*, означава че тя принадлежи на множеството от разрешени кодови комбинации.

Алгоритъм на декодера /в режим на коригиране само на еднократни грешки/:

1. определя се полиномът *F`(x)*, съответстващ на приетата кодова комбинация
2. *F`(x)* се разделя на образуващия полином *P(x)* на кода. Определя се остатъка от това деление – *S(x)*.
3. ако $S(x) = 0$, се счита, че в приетата кодова комбинация няма грешки и се преминава към декодиране на следващата трета кодова комбинация. При $S(x) \neq 0$, към 4.
4. определя се теглото *t* на единичните елементи в комбинацията, съответстваща на *S(x)*.
5. ако *t* е по-малко от коригиращата способност на кода /кратността на грешката, която може да коригира дадения код/, т.е. $t \leq 1$, то коригирането се извършава чрез ⊕ на приетата кодова комбинация и остатъка *S(x)*, т.е. *F`(x)* +*S(x)* при $t > 1$ – към 6.

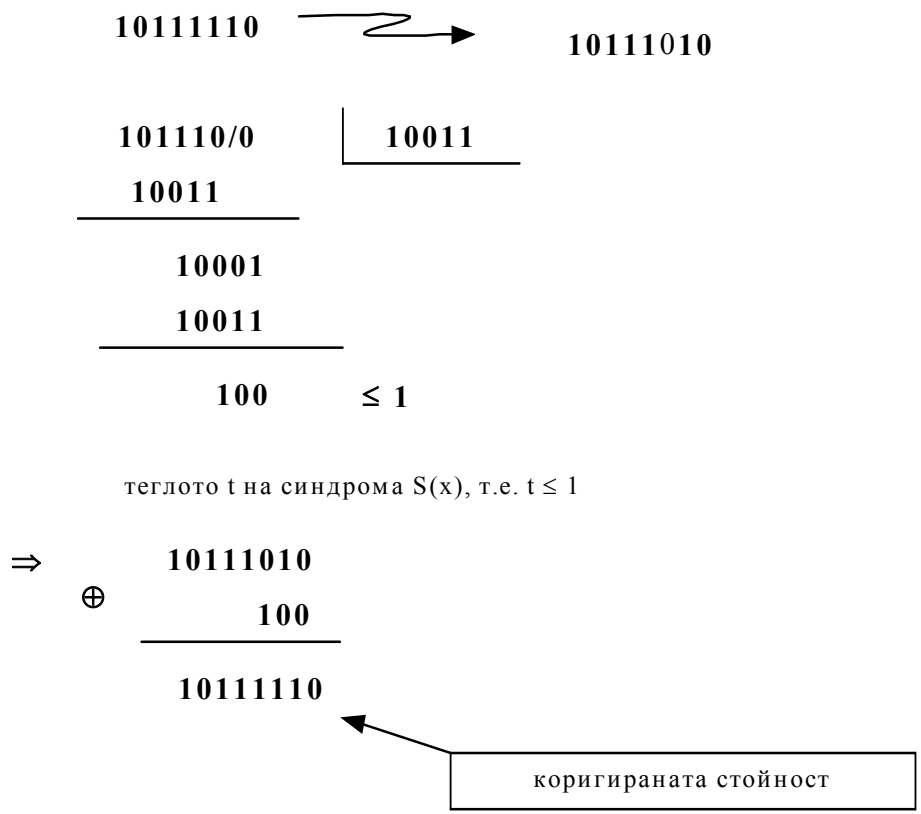
6. извършва се циклично преместване на една позиция на приетата кодова комбинация, след което новополученият полином се дели на *P(x)*. Определя се теглото *t`* на новополучения синдром *S`(x)*.

7. ако *t` ≤ 1*, то *S`(x) ⊕ делимото*, след което се извършва циклично преместване на резултата, в посока, обратна на предишните премествания. Крайният резултат представлява коригирана кодова комбинация /разрешена/. С това приключва декодирането и се преминава към декодиране на следваща такава. Ако *t`>1* – към 8.

8. извършва се циклично преместване на делимото още една позиция в същата посока, след което се повтаря делението на *P(x)* и се определя *t`* за новия остатък.

9. преход към точка 7.

Пример:



Шифриране

Изисквания към сигурността на информацията и възможни атаки срещу нея

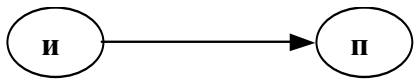
Има четири основни изисквания:

- *секретност* – информацията да бъде достъпна за четене само от оторизирани лица.
- *неприкосновеност* – информацията да бъде модифицирана само от оторизирани лица.
- *достъпност* – изисква активите на компютърните системи да бъдат достъпни само за оторизираните лица.
- *автентичност* – т.е. че информацията е генерирана именно от указания в нея източник и не е фалшифицирана.

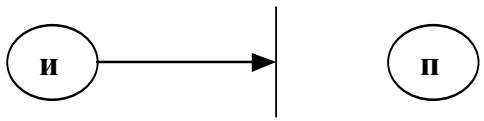
Атаки срещу сигурността – 4 типа:

- *прекъсване* – изразява се в разрушаване на активите на системата /напр. прекъсване на комуникационната линия или повреден твърд диск/. Това е атака против *достъпността*.

Нормална ситуация:

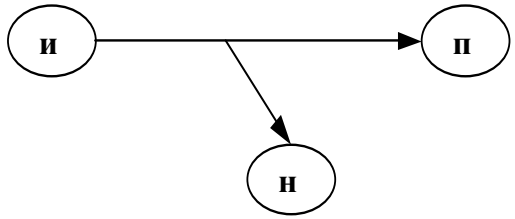


Пример:

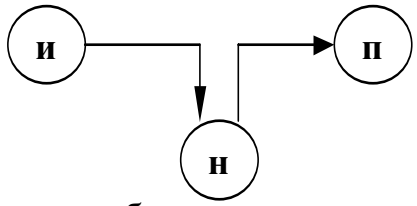


Задръстване на мрежата с пакети, “бомбандиране” на мрежов възел с пакети с цел изваждането му от строя.

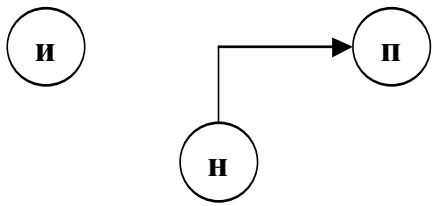
- *прихващане* – налице е когато неоторизиран обект /Н/ придобива достъп до системата. Това е атака срещу сигурността.



- *модифициране* – неоторициран обект /Н/ не само прехваща информацията, но и я модифицира. Това е атака срещу непрекосновеността.



- *фабрикуване* – вмъкване на фалшаиви обекти в системата от страна на неоторизиран обект /Н/. Това е атака срещу автентичността. Появява се, когато един обект претендира, че е друг /пр. web-сървър се "маскира" като друг и извършва неговата работа/



Атаките биват още: активни и пасивни.

Към *пасивните атаки* спада *прихващането*.

Основна цел: Определяне на съдържанието и анализ на трафика.

Противодействие на тези атаки – шифриране и генериране на трафик, част от който не се изпозва.

Цел: Невъзможност да се прочете информацията, заблуда за дължината на съобщението.

Пасивните атаки са много трудни за улавяне, тъй като те не променят данните, а само ги анализират. Стремеж към предотвратяването им, отколкото към откриването им.

Към *активните атаки* спадат *прекъсването*, *модифоицирането* и *фабрикуването*. При тях се цели модифициране или спиране на информационния поток или до генериране на фалшив такъв.

Борбата против тях е откриване и възстановяване на щетите.

Шифриране

Симетрично шифриране

Ключът е един и същ и е известен само на двете страни.
Слабото място**:** *ключът*.
Има пет начина за разпространение на ключа:

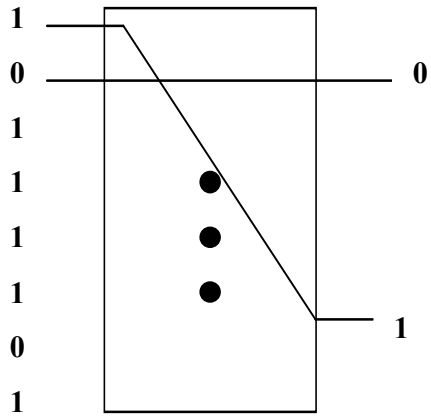
1) ключът се избира от едната страна и физически се доставя на другата. Най-добре е той да се разбие на части и всяка част да се изпрати по различен път.
   Недостатък – *разстоянието*.
2) едната страна създава новия ключ и го изпраща на другата страна шифриран с другия ключ.
   Недостатък – *губи се смисъла*.
3) ключът се създава от трета страна и физически се изпраща на съответните две страни.
4) едната страна използва публичния ключ на другата за шифриране на новия ключ /най-разпространен/.
5) физически се изпраща, както при 3), но ключът се доставя по електронен път.

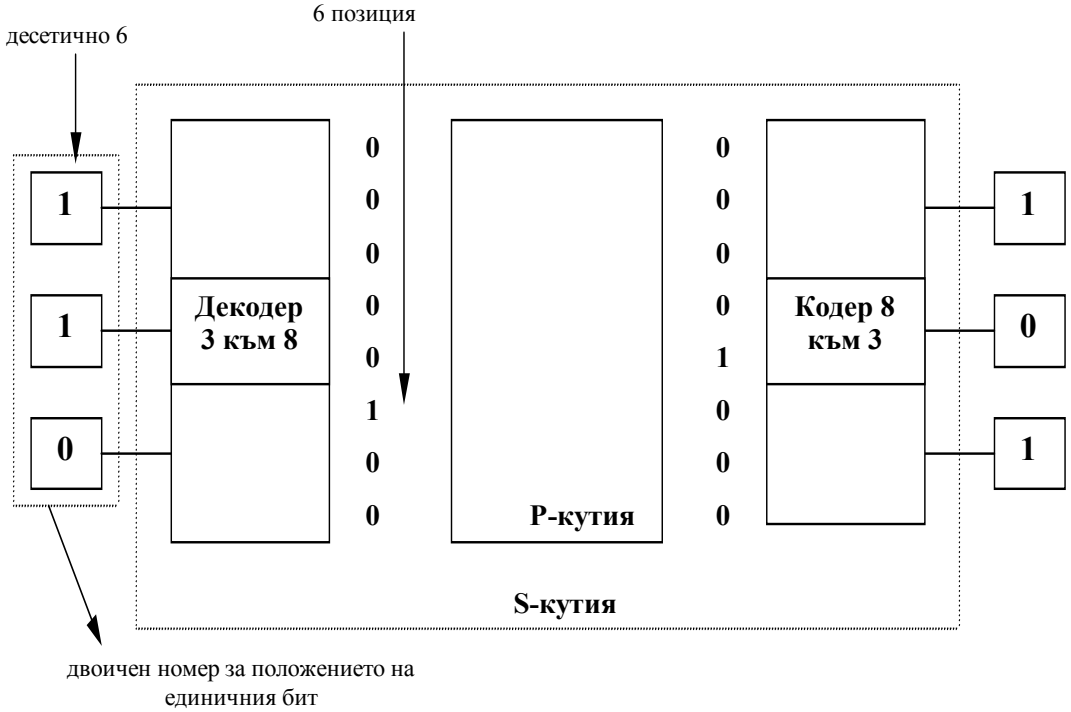
Шифрирането – безсмислена поредица от символи.
Най-често използвани варианти:

- прост алгоритъм с дълъг ключ
- сложен алгоритъм с къс ключ

Основни понятия

Пермутация /разместване/ - разместване на битове. Реализира се с P-кутии (Permutation box).





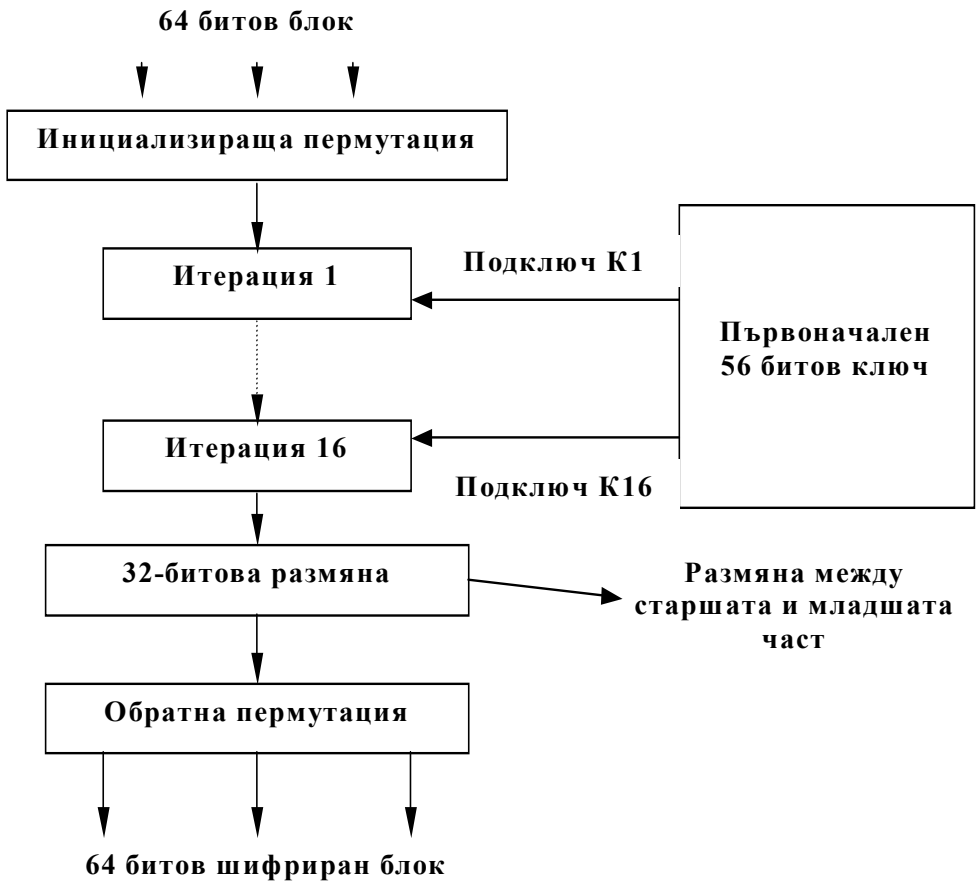
Субституция /заместване/ - чрез устройства наречени S-кутии (Substitution box).

Най-често използваните алгоритми за конвенционално шифриране са тези с блокови шифри – изходното съобщение се разделя предварително на блокове с фиксирана дължина.

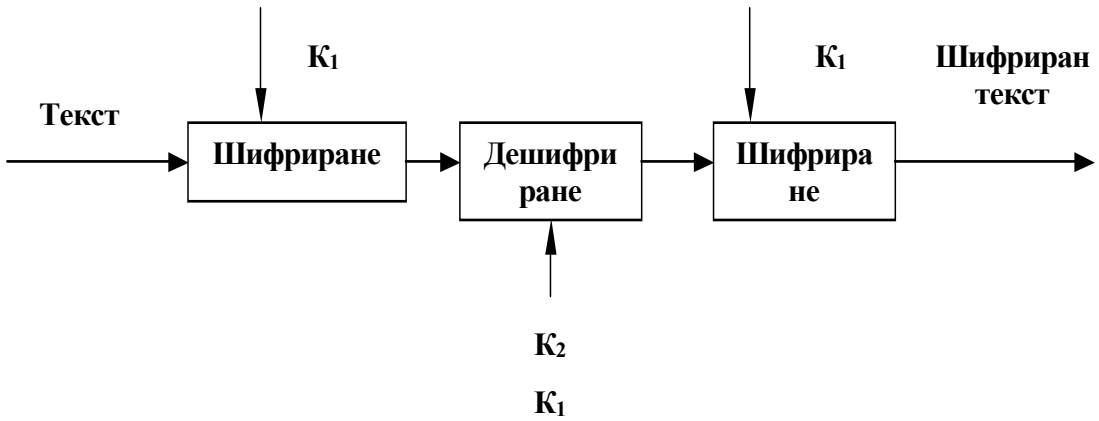
DES (Data Encryption Standard) – от 1977 г. Изходния текст се разделя на блокове по 64 бита. Дължината на ключа е 56 бита. 2,56 бита. Процесът на шифриране се състои от три фази:

- *инициализираща пермутация* – т.е. предварително разбъркване на битовете.
- *16 последователни идентични итерации,* които са функции на изходния текстов блок и ключа. Всяка итерация извършва една и съща функция, само че с различен подключ.
- о*братна пермутация* – действие обратно на инициализиращата пермутация, чийто резултат е 64-битов блок шифриран текст.

Днес DES се използва предимно за персонални приложения. Необходими средства за разбиване(теоритично)- **устройство –** 100 000$; **чипове** - 5760; **машинно време** – 1 млн.$; **време за разбиване** 3,5 часа; **последен рекорд** – 22 часа.


64 битов блок
Инициализираща пермутация
Итерация 1
Подключ К1
Първоначален
56 битов ключ
Итерация 16
Подключ К16
32-битова размяна
Размяна между
старшата и младшата
част
Обратна пермутация
64 битов шифриран блок

Троен DES – създаден 1979 г. Използва се за шифриране на финансови операции. Все още не е разбит. Използват се два ключа и трикратно използване на DES. Общата дължина на ключа е 112 бита. Шифрирането е в три фази.



З*ащо дешифриране?*

- да може потребители, използващи DES да дешифрират данни и обратно. Тогава се използва $\mathbf{K_1}$.
- дешифраторът е обратен на шифратора.

Разположение на устройствата за шифриране

Съществуват три възможности за шифриране в мрежа с комутация на пакети:

- **<u>шифриране в линията</u>** – при този метод всяка комуникационна линия е оборудвана в двата края с шифриращи устройства. Затова целият предаван по линията трафик е сигурен.

Недостатък: Необходимост от много шифриращи устройства в голяма мрежа. Всеки мрежов възел трябва да дешифрира съобщението, за да може да го маршрутизира. Това означава, че съобщенията са уязвими в междунните възли.

- **<u>шифриране "от край до край"</u>** – при този метод единият краен възел шифрира данните. Те преминават по мрежата в такъв вид до получателя, който ги дешифри ра.

Недостатък: заглавната част на пакетите трябва да се остави нешифрирана, за да може междинните възли да четат маршрутизиращата информация.

- **комбиниран метод** – осигурява най-добрата защитна комбинация на двата метода. Комбинираният метод шифрира само потребителските данни, използвайки **шифриране "от край до край"**, а след това целият пакет /заедно с маршрутизиращата информация/ се шифрира като се използва **шифриране в линията**.

Асиметрично шифриране (шифриране с публични ключове)

Базира се повече на математически функции. Не е по-сигурно, отколкото симетричното шифриране.

Асиметрично, защото един ключ се използва за шифриране, а друг ключ за дешифриране. Единият ключ се нарича *частен* и е напълно секретен. Другият ключ – *публичен*, защото е известен на много други потребители.

- **Схема "конфиденциалност" при асиметрично ширирane** – използва се за изпращане на секретни съобщения.

$К_{пп}$ – публичен ключ на получателя

$К_{чп}$ – частен ключ на получателя

- **Схема "цифров подпис" при асиметрично шифриране** – използва се за потвърждаване на автентичността на съобщенията.

$К_{чи}$ – частен ключ на изпращача
$К_{пи}$ – публичен ключ на изпращача

- **Алгоритъм RSA за асиметрично шифриране** – създаден е през 1978 г. Дължина на ключовете – 1024 и 2048 бита. Блоков алгоритъм. Използва факта, че произведението на две много големи числа p и q не може да се разложи на множители /за числата 10^{100}/.

Използване на асиметрично шифриране за доставка на ключ за симетрично шифриране.

Това е едно от приложенията на асиметричното шифриране, тъй като при симетричното шифриране слабото място е в това, че и двете страни трябва да разполагат с един и същ секретен ключ.

Сценарии:

- страната **A** подготвя съобщение за предаване към **B**.
- **A** шифрира съобщението с ключ за симетрично шифриране.
- **A** шифрира сесийния ключ с публичния ключ за асиметрично шифриране на **B**.
- **A** изпраща съобщението, заедно с присъединения към него шифриран сесиен ключ към **B**.
- **B** дешифрира сесийния ключ, използвайки свой частен ключ за асиметрично шифриране.
- **B** използва дешифрирания сесиен ключ за дешифриране на основното съобщенение.

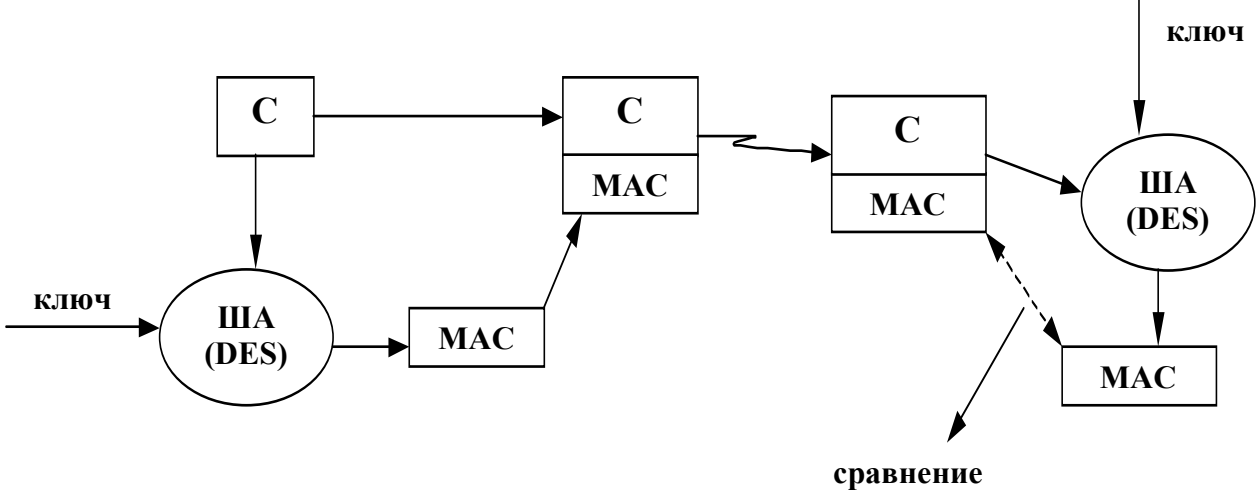
Въпрос: Как може да се докаже, че полученото съобщение е действително изпратено от страната **A?**

Потвърждаване на автентичността на съобщенията

Шифрирането предпазва от пасивни атаки. Защитата от активни атаки се реализира чрез потвърждаване на автентичността. Този процес включва проверка, че съдържанието на съобщението не е променено и че източника е автентичен, че съобщението не е задържано или предадено повторно.

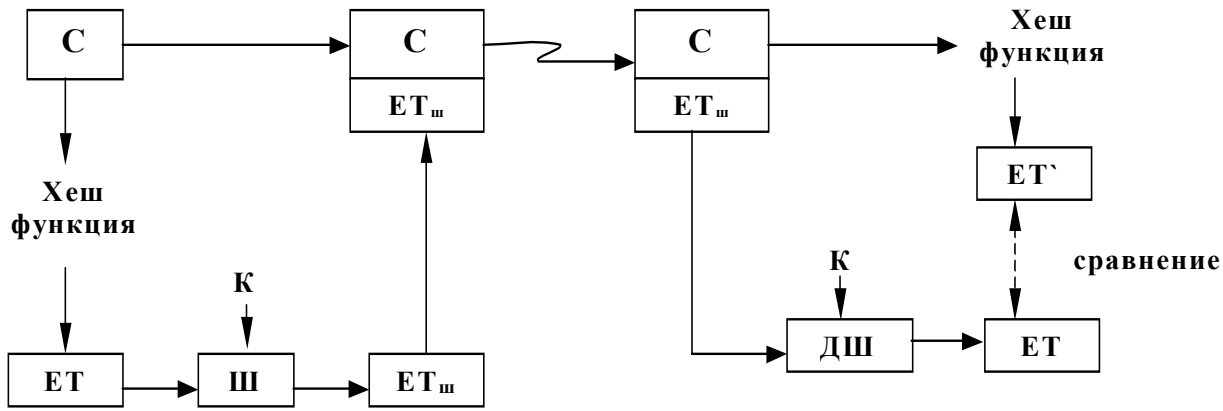
Съществуват няколко метода за потвърждаване на автентичността на съобщенията:

- *използване на автентичен код на съобщението* – При този метод двете страни използват секретен ключ, който заедно със съобщението се използва за създаването на малък блок данни, който се прикрепя към съобщението. Този блок се нарича MAC /Message Authentication Codde/.

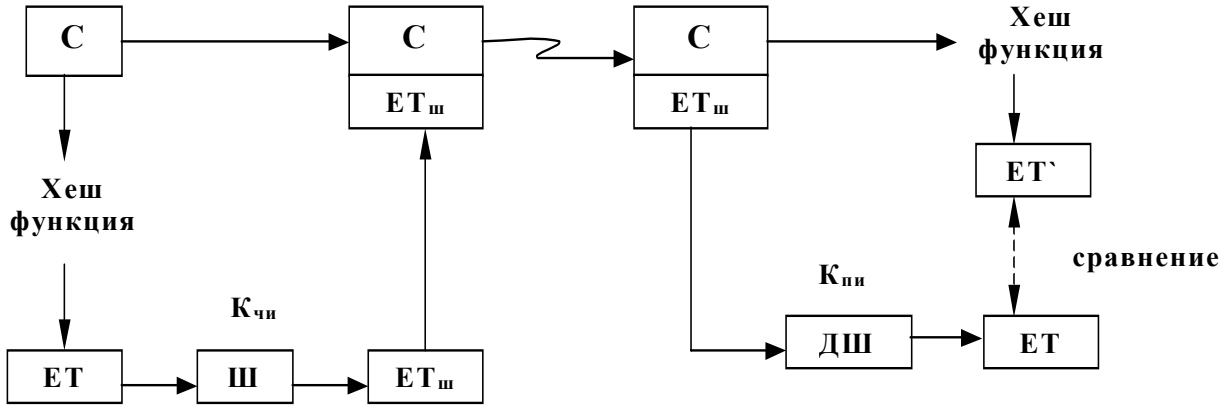


- *използване на хеш-функции за генериране на етикет на съобщението* – при този метод от съобщението с помощта на хеш-функция се получава етикет с фиксиран размер, който се прикрепя към съобщението. За защита на етикетите:

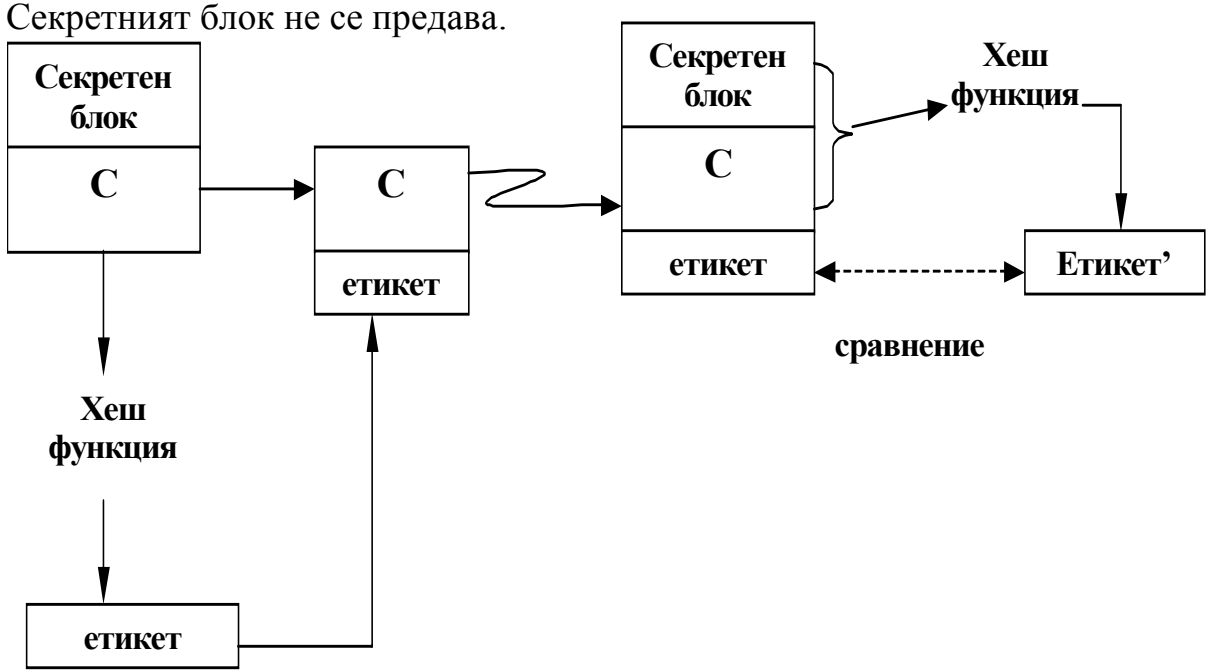
  - *конвенционално шифриране на етикет* /симетрично/ - един и същ ключ *К* и за двете страни



- *асиметрично шифриране на етикета* – при този метод се използва частния ключ на изпращача за шифроване на етикета, а получателят използва публичния ключ на изпращача.



- *използване на общ секретен блок за генериране на етикета* – тук не се използва шифриране на етикета, а вместо това се използва общ секретен блок за генериране на етикета. Секретният блок не се предава.



Локални компютърни мрежи

Определение – LAN е система, която дава възможност на независими цифрови устройства да комуникират помежду си на малки разстояния /до няколко километра/ и да използват общи мрежови ресурси.

Ресурсите се разделят на две групи:

- *локални*
- *мрежови*

Локалните ресурси се използват само от съответния компютър, на който принадлежат. **Мрежовите ресурси –** за общо ползване, поделят се между отделните потребители, имащи право на достъп до тях.

Четири вида ресурси:

- *процесорно време*
- *памет*
- *файлове с данни и програми*
- *входно-изходни устройства /принтери, плотери и др./*

Основна характеристика на LAN – възможност за групово /multicast/ и общодостъпно /broadcast/ предаване, малка вероятност за грешки при предаването.

Според функциите, които изпълняват, крайните възли на една локална мрежа са:

- *работна станция*
- *сървър*

Имаме и междунни мрежови възли – повторители, концентратори, комутатори, мостове, маршрутизатори.

Работна станция – произволен компютър или терминал, чрез който се осъществява достъп до мрежовите ресурси.

Сървър – компютър, осигуряващ мрежовите ресурси, както и тези които обслужват мрежата.

Един компютър да изпълнява едновременно функциите на сървър и работна станция (равноправен достъп “peer-to-peer”). При мрежи с усилено използване на даден ресурс е желателно компютърът, предоставящ този ресурс, да се използва единствено и само като сървър.

Под “сървър” се разбира приложен процес /програма/, реализиращ дадена мрежова услуга.
Едновременно – няколко сървъра в един компютър.
Видове сървъри:

- **Файлов** – програма, позволяваща достъп до файловата система на компютъра за съхранение и извличане на файлове и програми.
- **Сървъри за печат** – програма, осигуряваща достъп до принтера на компютъра, на който е стартирана.
- **Сървър за асинхронни комуникации –** програма стартирана на компютър с няколко модема, позволяващи използването им от всички потребители.
- **Сървър за отдалечен достъп (RAS) –** програма, стартирана на компютър, осигуряваща достъп до локалната мрежа от отдалечен компютър чрез модем и телефонна линия.
- **Сървър за електронна поща –** програма, управляваща електорнните пощенски кутии на потребителите.
- **Факс-сървър –** програма, управляваща изпращането и получаването на факс съобщения
- **Сървър за бази данни –** програма, реализираща функциите на ядрото на системата за управление на БД.
- **Сървър за приложни програми –** подава копие на проложната програма до работната станция по мрежата.

Основни предимства на LAN:

- Осигурява общи ресурси – намаляване на разходите за скъп хардуер.
- Повишаване на ефективността на сравнително непроизводителни компютри /пример – повечето дискова памет от сървъра/.
- Възможност за използване на обща база данни
- По-удобна колективна работа при разработването на проекти в група.
- Възможност за електронна комуникация /да комуникират без да напускат работното си място/.
- Възможност за свързване към други LAN/WAN.

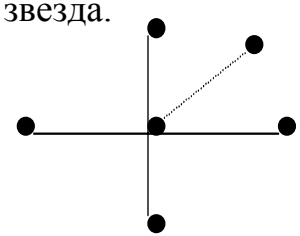
Физически слой в LAN – физическият слой на OSI модела извършва функции, като:

- Синхронизация по битове
- Кодиране в линията
- Предаване-приемане на битове

При LAN тези функции се осъществяват от мрежовия адаптер. Като допълнение към този слой в LAN се включват и спецификации на топологията и кабелната система.

Топология – начинът на разполагане и свързване на отделните й възли.

- **тип "звезда"** – тук крайните мрежови възли /работни станции, сървъри/ са свързани към централен възел /комутатор/ във вид на звезда.

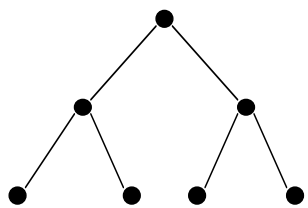


Предимство: лесно добавяне на нов възел.

Недостатък: повреда в централния възел – разпад на мрежата.

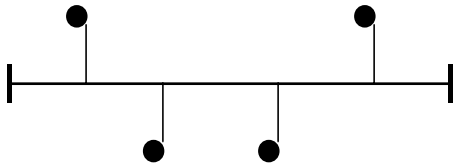
Стандарт: 10 Base T

- **тип "дърво"** – дърво с корен /главен концентратор/, към който са свързани крайни възли и концентратори, разположени на различни нива.



Предимство: повреда в концентратор от второ или по-долно ниво – само определен участък от мрежата.
Стандарти: 10 Base T, IEEE 802.12

- **тип "пасивна шина"** – една шина за данни /кабел/, към която са свързани отделните мрежови възли.

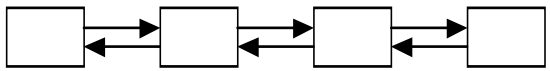


Предимства:
- лесно добавяне на нови възли
- повреда на един възел не указва влияние върху другите

Недостатъци:
- ограничено разстояние
- слаба диагностика на мрежата
- прекъсване на шината води до разпадане на мрежата

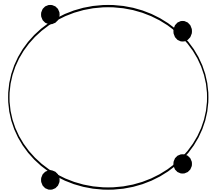
Стандарти: 10 Base5, 10 Base2.

- **тип "активна шина" –** изходът на всеки възел към входа на следващия. За комутиране в две различни посоки са необходими две активни шини. Всеки възел действа, като регенератор и усилвател.



Стандарти: IEEE 802.6 /за регионална мрежа/

- тип "кръг" – възлите в мрежата са свързани в кръг.



Предимства:

- възможност за покриване на големи разстояния
- удобство при използване на оптични влакна

Недостатък: трудно се добавят нови възли

Стандарти: IEEE 802.5, FDDI

Кабелна система на LAN

Основни видове кабели:

- кабели с усукана двойка проводници – състоят се от няколко /обикновено 4/ двойки медни проводници. Двата проводника на всяка двойка са изолирани и взаимно усукани. Усукването – за намаляване на външните шумове. Предназначени са за малки разстояния.

В зависимост от категорията:

скорост: 10 mb/s ;100 mb/s

максимална дължина: 100 m

- коаксиални кабели – вътрешен проводник обвит с изолационен материал, медна оплетка, външна обвивка. Оплетката – роля на предпазен екран. Ако съществува първи изолационен слой от фолио и втори от метална оплетка, то той е двойно екраниран. Покриват се по-големи разстояния и се поддържат по-големи скорости, защото имат по-добра защита от електромагнитни смущения.

- коаксиални кабели – вътрешен проводник обвит с изолационен материал, медна оплетка, външна обвивка. Оплетката – роля на предпазен екран. Ако съществува първи изолационен слой от фолио и втори от метална оплетка, то той е двойно екраниран. Покриват се по-големи разстояния и се поддържат по-големи скорости, защото имат по-добра защита от електромагнитни смущения.

Деление:

I.

- тънки – d = 0,5 см
- дебели – d = 1 см

II.

- широколентови /високоскоростни/ - 75Ω
- нискочестотни – 50 Ω

- влакнестооптични кабели – състоят се от отделни влакна, всяко от които се състои от тънка цилиндрична кварцова сърцевина облицована със стъклена обвивка, която е защитена от външна обвивка. Сигналите се пренасят по сърцевината под формата на модулирани светлинни импулси, които не се влияят от външни електромагнитни смущения.

Характеристики - на големи растояния; големи скорости; най-скъпи; използват се предимно за кръгови топологии.

Каналeн слой в LAN – разделен е на два подслоя:

- горен подслой за управление на логическите канали /LLC – Logic Link Control/
- долен подслой за управление на достъпа до комуникационната среда /MAC – Media Access Control/

Функциите на каналния слой се осъществяват от мрежовия адаптер.

MAC подслой

Този подслой управлява заемането и разпределението между мрежовите възли на комуникационната среда, по която се извършва предаването на физическите сигнали, осъществява адресацията, формира кадри със съответните полета. При предаване MAC-подслоя (изпращащият) получава от LLC подслоя съответен LLC – блок данни, който включва в полето <данни> на съответния кадър, добавя към него адресна информация, след което кодира тези полета с шумоустойчив код и записва полученото контролно значение в контролното поле.

След това завършва формирането на кадъра с полетата <встъпителна част>, <начален ограничител>, <краен ограничител>. После кадърът се предава към физическия слой, който го доставя във вид на неструктуриран поток от битове до възела-получател. Неговият MAC-подслой, осигурява разпознаване на MAC-адреса, открива грешките в кадъра, възникнали при предаването му, отделя данните от кадъра и ги предава към горния LLC слой.

LLC подслой

LLC получава пакети от мрежовия слой, формира и предава номерирани LLC блокове, контролира грешките и допълнително може да определя последователността на кадрите и да коригира грешки получени при предаването. LLC подслоят е независим от MAC-подслоя и от комуникационната среда. Функционирането на LLC подслоя е описано в стандарта IEEE 802.2. Според него имаме три типа услуги:

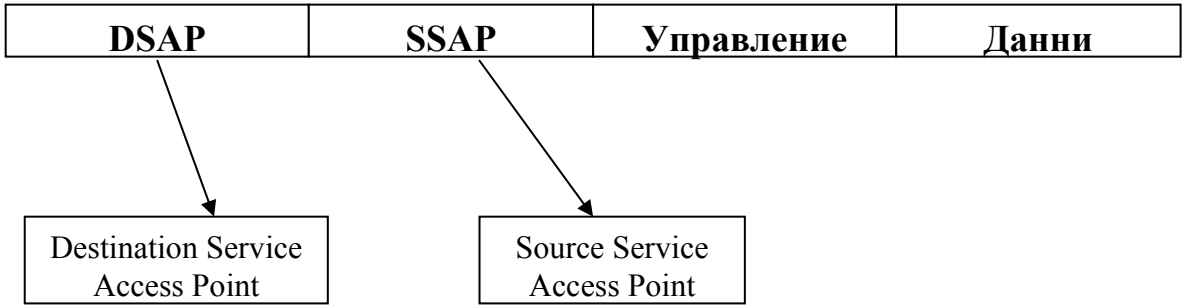
- тип 1/LLC1/ - осигурява предаването на данни между два мрежови възела без установяване на логическо съединение и без потвърждаване на предаването – дейтаграмен режим без потвърждаване. Коригирането на грешките и номерирането на пакетите се извършва от протоколите на по-горните слоеве.

- тип 2 /LLC2/ - осигурява предаването на данни между два мрежови възела с установяване на логическо съединение – режим на виртуално съединение. Използва се методът на плъзгащият се прозорец с N = 8 или 128 кадъра.

- тип 3 /LLC3/ - осигурява предаване на данни между два мрежови възела без установяване на логическо съединение, но с потвърждение – дейтаграмен режим с потвърждение. Стандартът 802.2 групира тези типове услуги в 4 класа:

- *клас 1* – тип 1
- *клас 2* – тип 1 и 2
- *клас 3* – тип 1 и 3
- *клас 4* – тип 1, 2 и 3

Формат на LLC-блок:



SSAP идентифицират протокола на по-горния слой, като по този начин позволяват в една и съща мрежа да бъдат използвани различни протоколни стекове.

Международни стандарти за физическия и каналния слоеве на LAN

Стандарт IEEE 802.3 (Ethernet) – описва LAN с логическа топология тип “шина”. Скоростта на предаване е 10 Mb/s, а в последните версии на стандарта - 100 Mb/s, 1Gb/s, 10 Gb/s

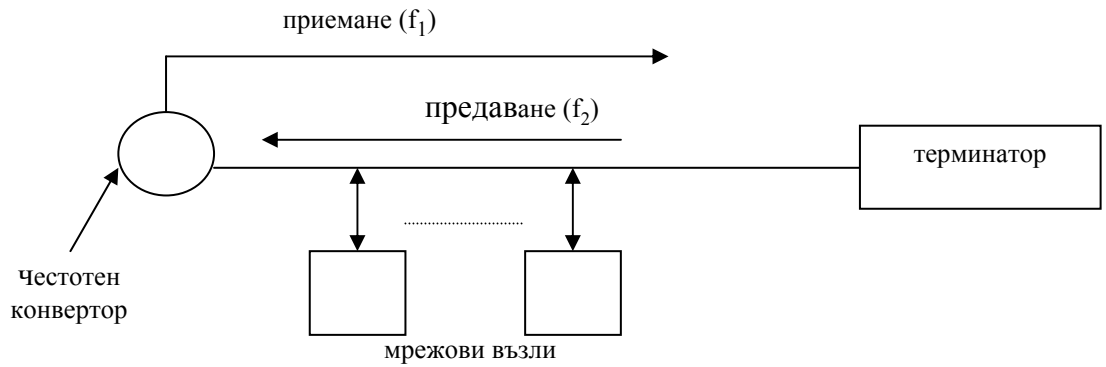
Два метода на предаване:

- *директно цифрово предаване*
- *модулирано аналогово предаване*

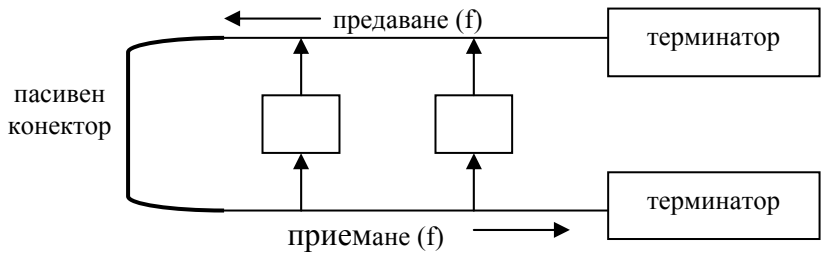
При *директното предаване* се използва цялата честотна лента на кабела, като по този начин се осигурява само един канал за предаване по него.сигналът е цифров, кодиран най-често с манчестърски код.

При *модулираното предаване* се осигуряват повече от един канал за предаване по кабела. По каналите се предават аналогови сигнали от различните възли.

I вариант:



II вариант: с два кабела



Означение за IEEE 802.3:

общо – *vMetodL*, където:

v – скоростта на предаване на сигнала изразена в MB/S.

Metod – методът на предаване. Има две значения:

- **Base** – за директно предаване
- **Broad** – за модулирано предаване

L – дължината на сегмента /кабела между два съседни терминатора/ в стотици метри.

При *L = {T, TX, T4}* – използва се кабел с усукани двойки проводници.

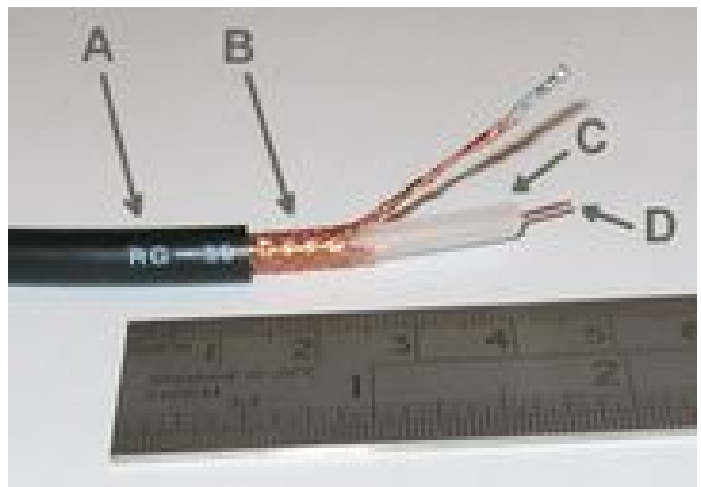
При *L = {F, FX}* – използва влакнестооптичен кабел

Най-предпочитани стандарти: 10 Base2, 10 BaseT

10 Base2 – минимална дължина между два възела 0,5 см /при 10 Base5 – 2,5 м и кратна на нея/; максимален сегмент /между терминаторите/ - 185м; брой възли – 30; конектор BNC; коаксиален кабел; максимално покриващо разстояние 925 м; максимално 4 повторителя.

Условие: между всеки два крайни възела трябва да има не повече от два повторителя.

10 BaseT – имаме концентратор (hub); физическа топология "звезда", логическа "шина"; свързване с усукана двойка проводници (два за предаване, два за приемане).



Разширение на стандарта:

•Fast Ethernet (100 Mb/s)

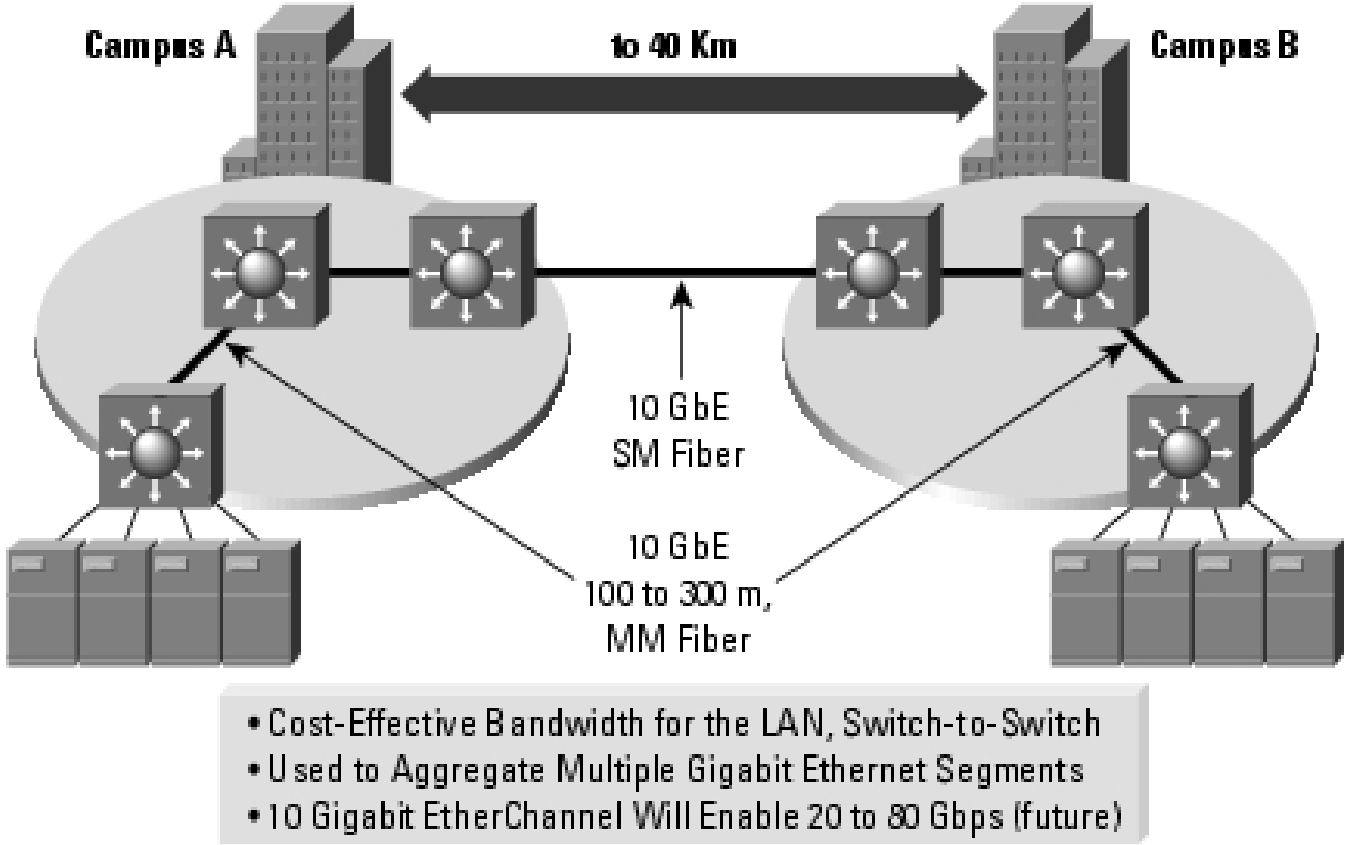
•Gigabit Ethernet (1 Gb/s)

•10 Gigabit Ethernet (10 Gb/s) - ратифициран като IEEE 802.3 Ethernet стандарт юни 2002г.

Комбинират висока скорост на предаване и интелигентни услуги.

Използва пълен дуплекс.

Означаване 10GBASE-X.



- Връзка между комутатори от различни обекти
- Обединяване на сегменти от тип Gigabit Ethernet

За покриване на регионални разтояния (до 100км) се използват приемо-предавателни устройства наречени *gigabit interface converters* (GBICs).

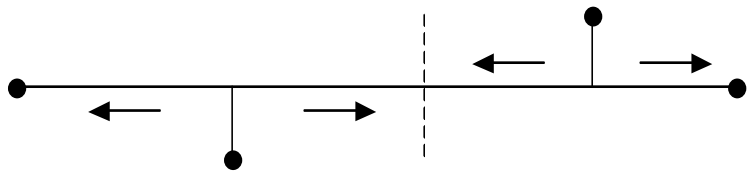
За достигане на разтояния до 100 км се използва метода single-mode и така нареченото „тъмно влакно” (dark fiber).

"Тъмно влакно" се наричат неизползваемите все още оптичните връзки.

MAC-подслой на стандарта IEEE 802.3

В този подслой на каналния слой стандартът IEEE 802.3 използва протокол с името CSMA/CD (**Carrier Sense Multiple Access With Collision Detection**)

Този протокол допуска, че всички възли в мрежата са равноправни, като им позволява да предават по общата комуникационна среда /шина/, създавайки се помежду си. Методът се основава на възможността всеки възел да разпознава кога шината е заета или свободна. След получаване на заявка за предаване от протоколите на горните слоеве, протоколът CSMA/CD формира кадър, който се предава в двете посоки по шината. В същото време друг възел може също да изпрати кадър в шината. Възниква конфликт между двата кадъра.



конфликт

Следствие: деформация на сигнала.

Извод: мрежовите адаптерни платки – да “подслушват” канала и докато предават съобщението.

При възникване на конфликт по мрежата се предава специален заглушаващ сигнал. Всеки възел, участвал в конфликта, изисква различен интервал от време преди да изпрати отново кадъра си. След 16 неуспешни опита контролерът на мрежовата платка предава към към компютъра сигнал за грешка.

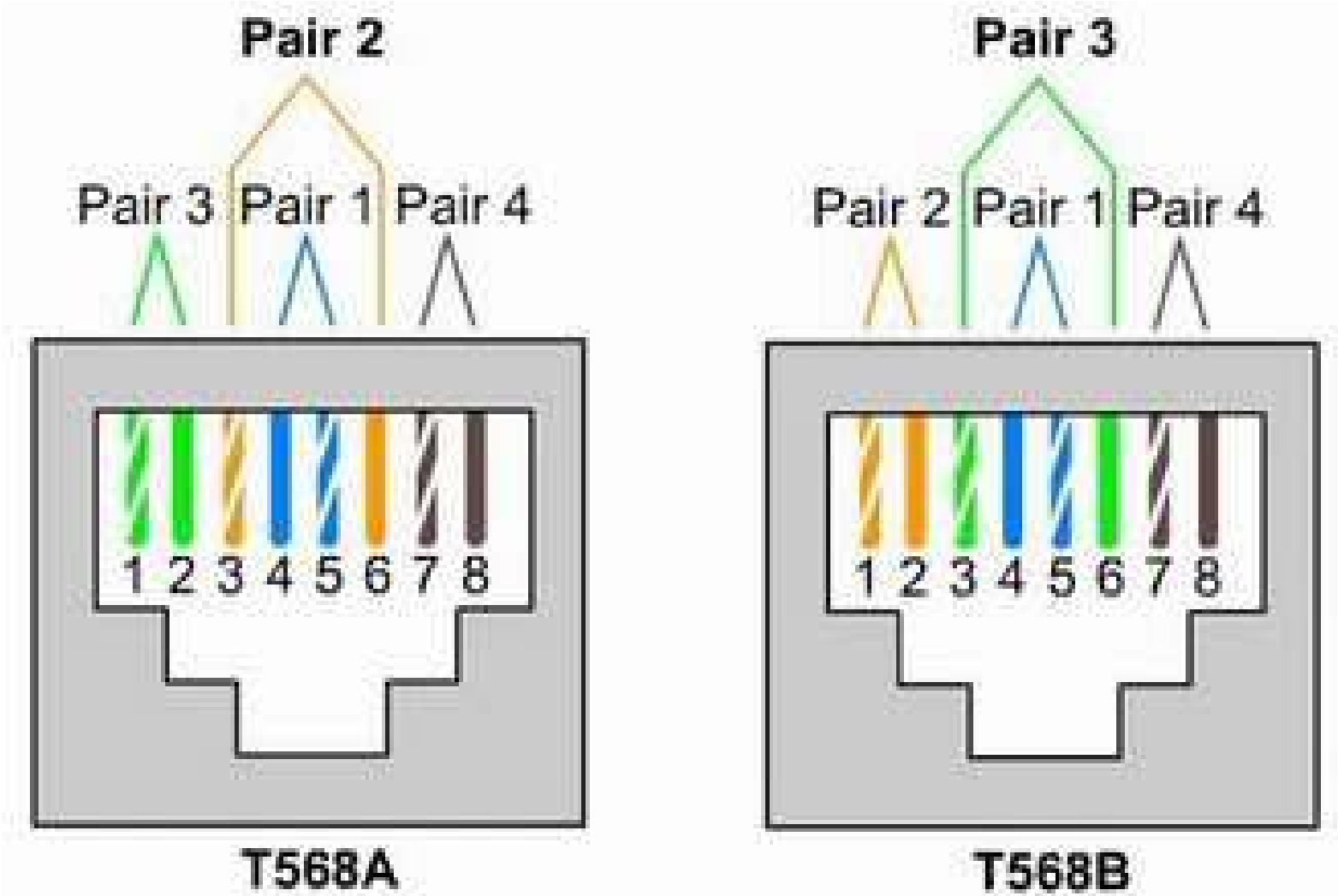
Извод: при увеличаване на възлите в мрежата конфликтите се увеличават и средната скорост намалява.

Главна Процедура

1. Кадърът е готов за предаване
2. Свободна ли е средата? Ако не, изчаква се до нейното освобождаване
3. Предаване
4. Има ли колозия? Ако да, преминаване към втората процедура
5. Успешно предаване

Колизионна процедура

1. Продължаване на опита за предаването
2. Достигнат ли е максималния брой опити? Ако да, неуспех на предаването
3. Случайно генериран период на изчакване
4. Преминаване към процедура 1



Свързва еднакви устройства

Следствие: деформация на сигнала.

Извод: мрежовите адаптерни платки – да “подслушват” канала и докато предават съобщението.

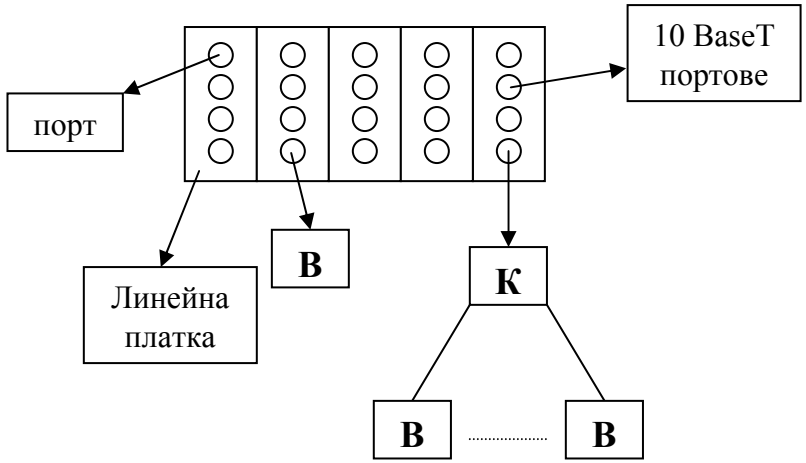
При възникване на конфликт по мрежата се предава специален заглушаващ сигнал. Всеки възел, участвал в конфликта, изисква различен интервал от време преди да изпрати отново кадъра си. След 16 неуспешни опита контролерът на мрежовата платка предава към компютъра сигнал за грешка.

Извод: при увеличаване на възлите в мрежата конфликтите се увеличават и средната скорост намалява.

Комутирани локални мрежи, изградени по стандарта IEEE 802.3

Локалните мрежи по стандарта 802.3 могат да бъдат комутирани. В този случай комуникационната среда престава да бъде обща. Използват се устройства – комутатори, които се инсталират на местото на концентраторите.

Комутатор – устройство с високоскоростна комутационна матрица, състояща се обикновено от 4 до 32 линейни платки, всяка с 1 до 8 порта за свързване на отделни крайни възли и концентратори.



Действие: при постъпване на сигнал на някой от портовете на съответната линейна платка, комутаторът най-напред проверява дали той е предназначен за възлите към същата линейна платка. Ако това е така, то кадърът се копира /предава/ директно към съответния порт на платката без да се използва матрицата. В противен случай кадърът се предава чрез нея към съответната линейна платка, а тя го предава към нужния порт.

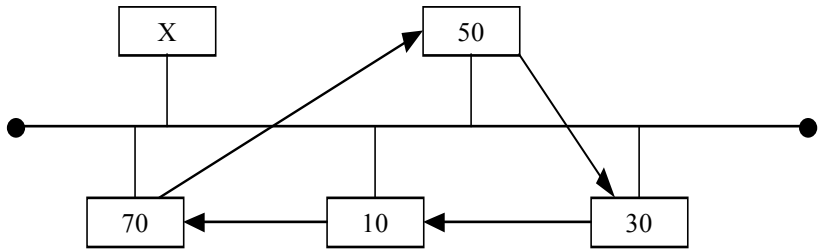
Стандарт 802.4 (Token Bus)
Използва се по-рядко от стандартите IEEE 802.3,802.5. По-сложен е.

Физически слой на стандарта IEEE 802.4
- физическа топология тип “шина”
- коаксиален кабел

Използва два режима на предаване:
- немодулирано аналогово предаване
- модулирано аналогово предаване

MAC-подслой на стандарта IEEE 802.4

Използва протокол Token Bus. При него достъпът до комуникационната линия се използва управляващ маркар /token/. Това е специален кадър, разрешаващ предаването по шината, който се предава от възел към възел. Единствено възел, в който е маркерът, има право да предава, като по този начин се премахва възможността за конфликт. Всеки възел знае MAC адреса на съседа си отляво и отдясно. При инициализиране на мрежата право да предава получава възелът с най- голям адрес. Той изпраща своя кадър, след което предава маркера към възела със следващия по-малък адрес. На практика маркерът достига до всички възли по шината, но само възелът с MAC-адрес указан в маркера, го прехваща.



Всеки възел да владее маркера само за определен период от време, през което изпраща кадрите си /зависи от дължината им/. Ако някой възел няма данни за предаването той препредава маркера.

Физическа топология – "шина"

Логическа топология – "кръг"

При изпращане на маркера към следващ възел се очаква потвърждение за получаването му. Ако не се получи такова, възелът изпращач предава маркера отново. Ако пак не получи потвърждение изпраща в шината кадър-запитване "търся заместник", като очаква адреса на произволен възел, готов да приеме маркера, за да изпрати кадъра.

При протокола **Token Bus** може да се изключва от логическия кръг някои крайни възли, като в този случай те могат да получават кадри, но не и да изпращат.

Стандарт 802.5 (Token Ring) – на базата на стандарта Token Ring на фирмата IBM

Физическа топология – най-често “свързани звезди”

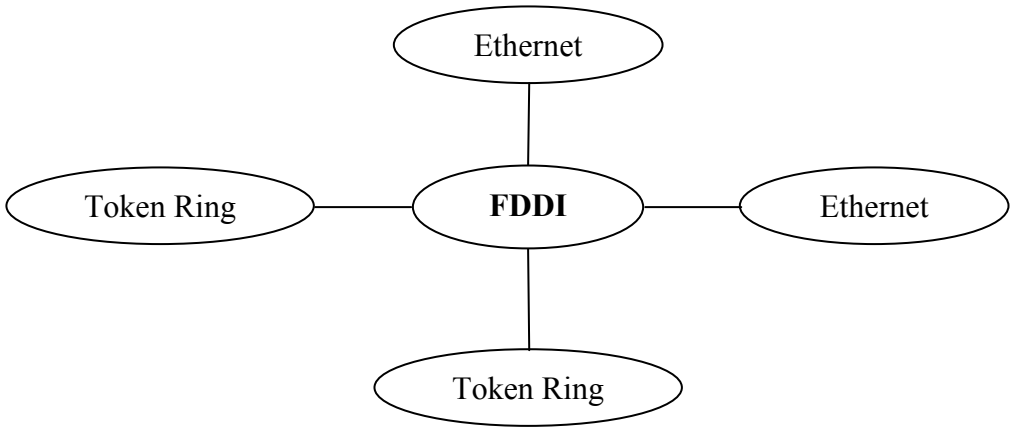
Логическа топология – тип “кръг”.

Сигналът обхожда последователно в кръг всички нейни възли. Разстоянията, които се покриват са по-големи от тези в стандартите IEEE 802.3, 802.4, тъй като всеки възел, през който преминава сигнала действа като усилвател за него. Могат да се използват и трите типа кабели.

MAC-подслой на стандарта IEEE 802.5

На това ниво се използва протокола Token Ring. Той използва маркер, както при Token Bus. Маркерът се генерира при инициализиация на мрежата, след което започва да циркулира в кръг само в една посока. Право за предаване има само този възел, който притежава маркер,. Когато А предава променя бит в маркера и допълва информацията, която иска да предаде, след което пуска маркера. Във възел А се пуска и таймер. Кадърът преминава през всички възли последователно в кръга, но само възелът В /получателят/ го прехваща в паметта си. Маркерът продължава до пристигането във възела А /подателя/. А премахва съобщението си, и предава освободения маркер в кръга. За правилното изпълнение на тази процедура при ненормални ситуации се грижи специална мониторна станция /един от крайните възли на мрежата/. Тя премахва забравени кадри, оставени да циркулират многократно по кръга и възстановява загубени маркери.

Стандарт FDDI (Fibre Distributed Data Interface) – 100 Mbs стандарт за разтегнати локални мрежи (Extended LAN) с MAC – протокол, базиран на протокола Token Ring.



Използване на FDDI като 100 Mbs опорна мрежа за свързане на няколко LAN помежду им базирани на Ethernet и Token Ring.

CDDI (Copper Distributed Data Interface) – подобно на FDDI, но използващ усукана двойка проводници.

Физически слой на FDDI

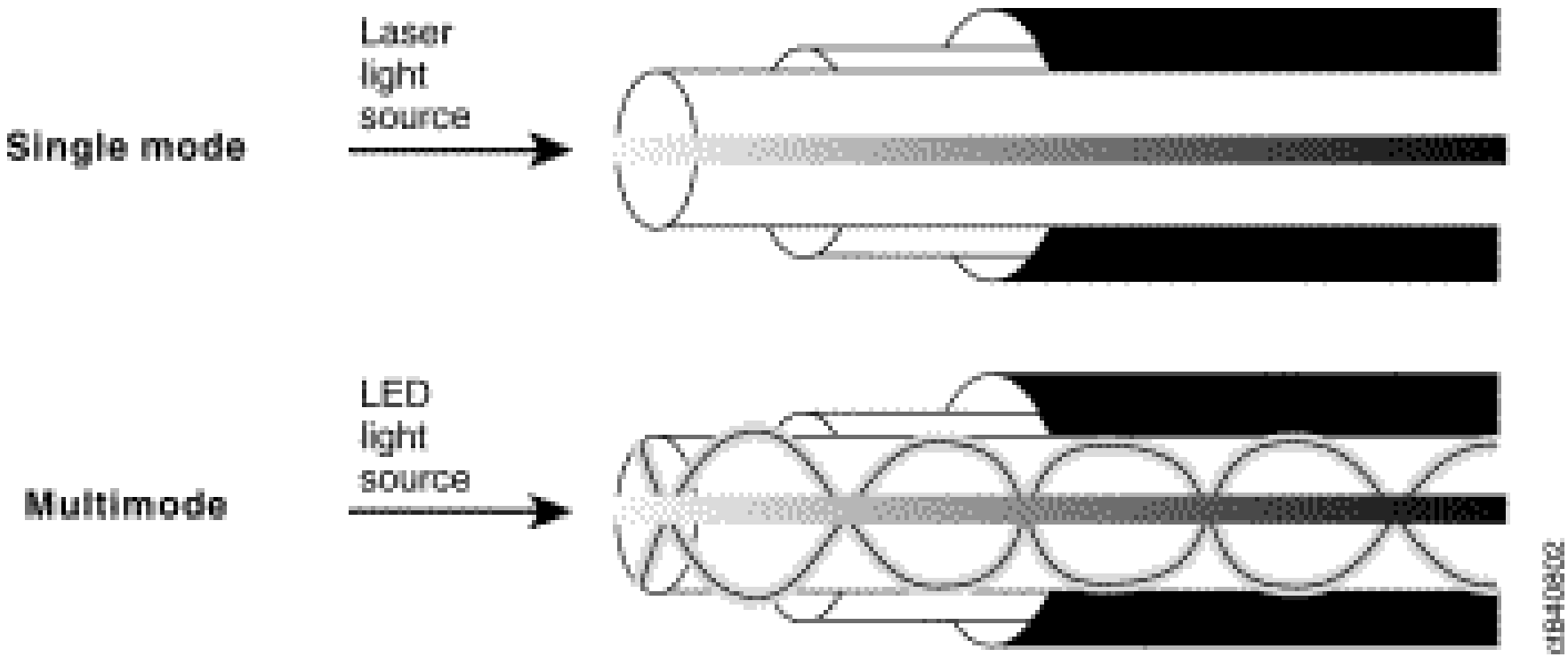
Топология – “двоен кръг”. Единият кръг е основен за предаването /първичен/, а другият – резервен. Посоката на предаване е различна за двата кръга.

Свързване - усукана двойка при CDDI;
опричен кабел при FDDI

Съществува два типа оптичен кабел:

- single mode – използва се лазер като източник на светлина. Предава се единствен сигнал.Покрива по-големи разтояния .

- multimode – използва се диод за източник на лъча, който разпръсква светлината под различни ъгли.Това ограничава дистанцията на предаване на сигнала.


Single mode
Laser
light
source
Multimode
LED
light
source
dB4092

Типове станции:

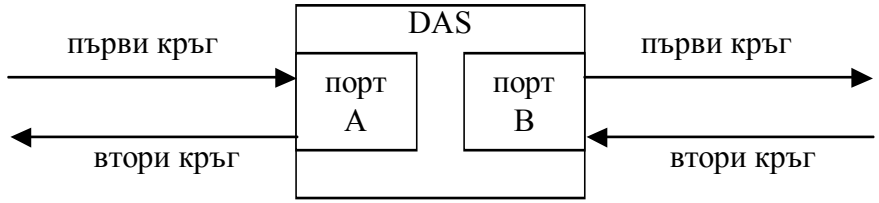
- възли, свързани към двата кръга (*DAS – dual-attachment station*)
- възли свързани само с първичния кръг (*SAS – single-attachment station*)
- единичен концентратор (*SAC – single-attachment concentrator*)
- двоен концентратор (*DAC – dual-attachment concentrator*)

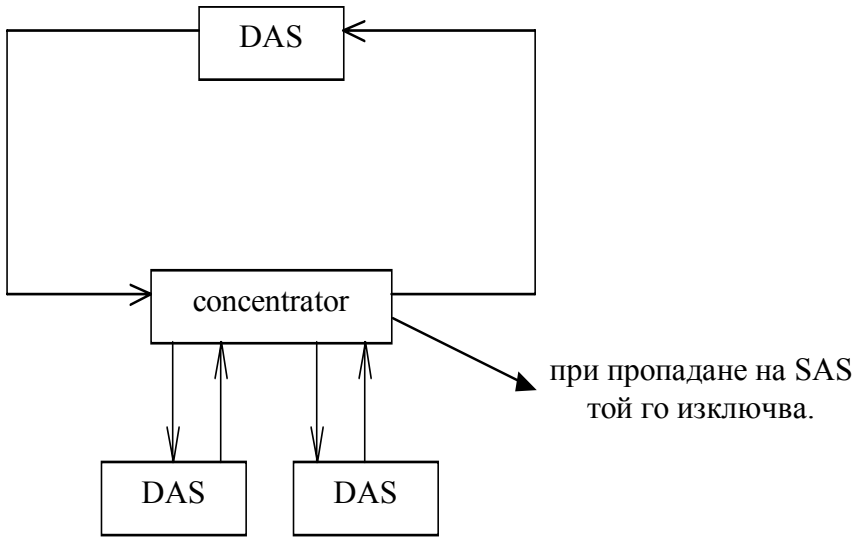
SAS-възлите трябва да бъдат свързани към кръга чрез концентратор. Всеки DAS има два порта. Вторичен кръг при нормални условия не се използва. При прекъсване на кабелите в дадена отсечка, в зависимост от това къде се намира повредата, може да очакваме :

- DAS устройството да затвари кръга
- концентраторът да изолира портовете на съответното SAS – устройство.

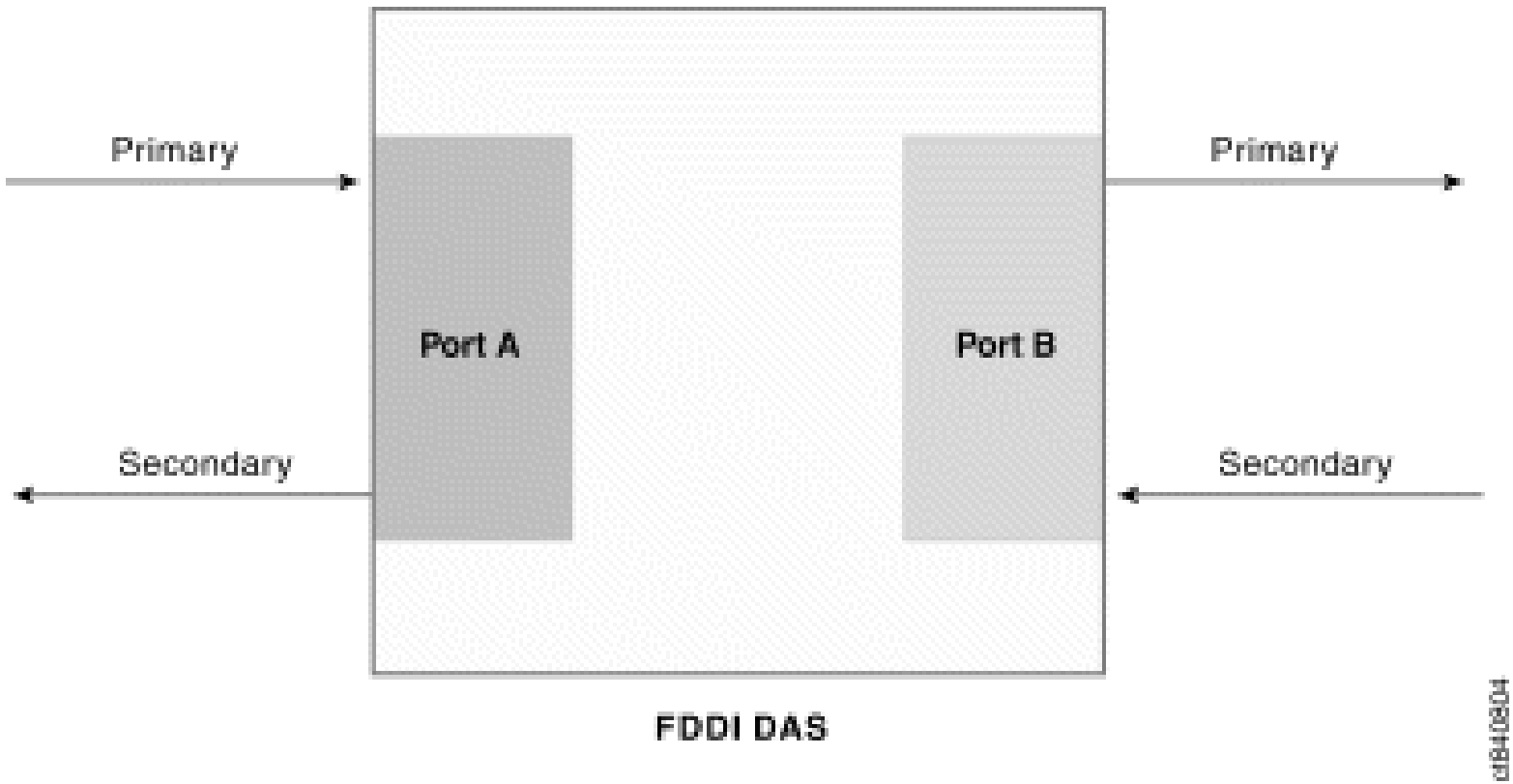
MAC-подслой

Използва се протокола Token Ring с някои изменения.

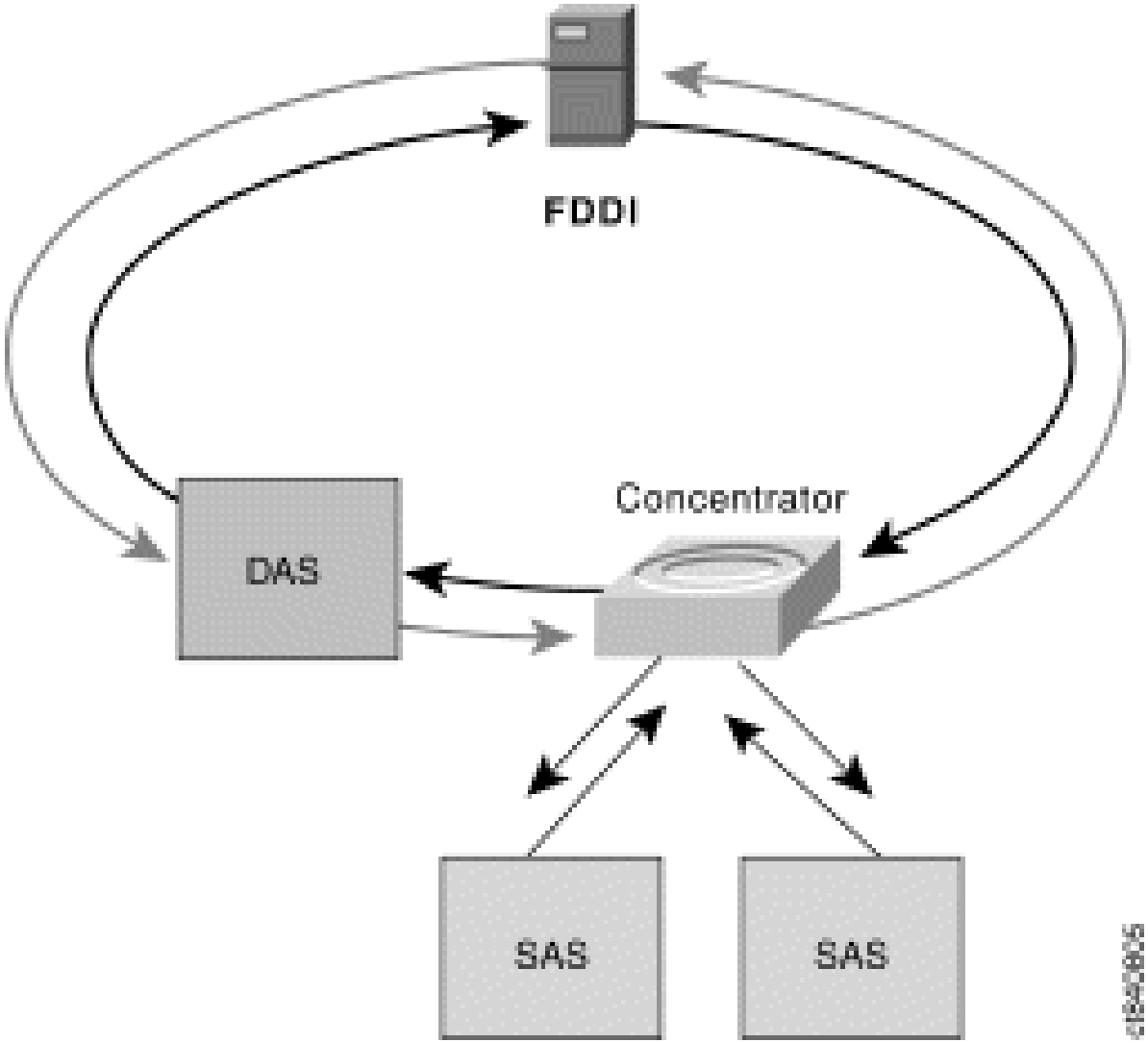

DAS
първи кръг
порт
A
порт
B
първи кръг
втори кръг
втори кръг


DAS
concentrator
при пропадане на SAS
той го изключва.
DAS
DAS

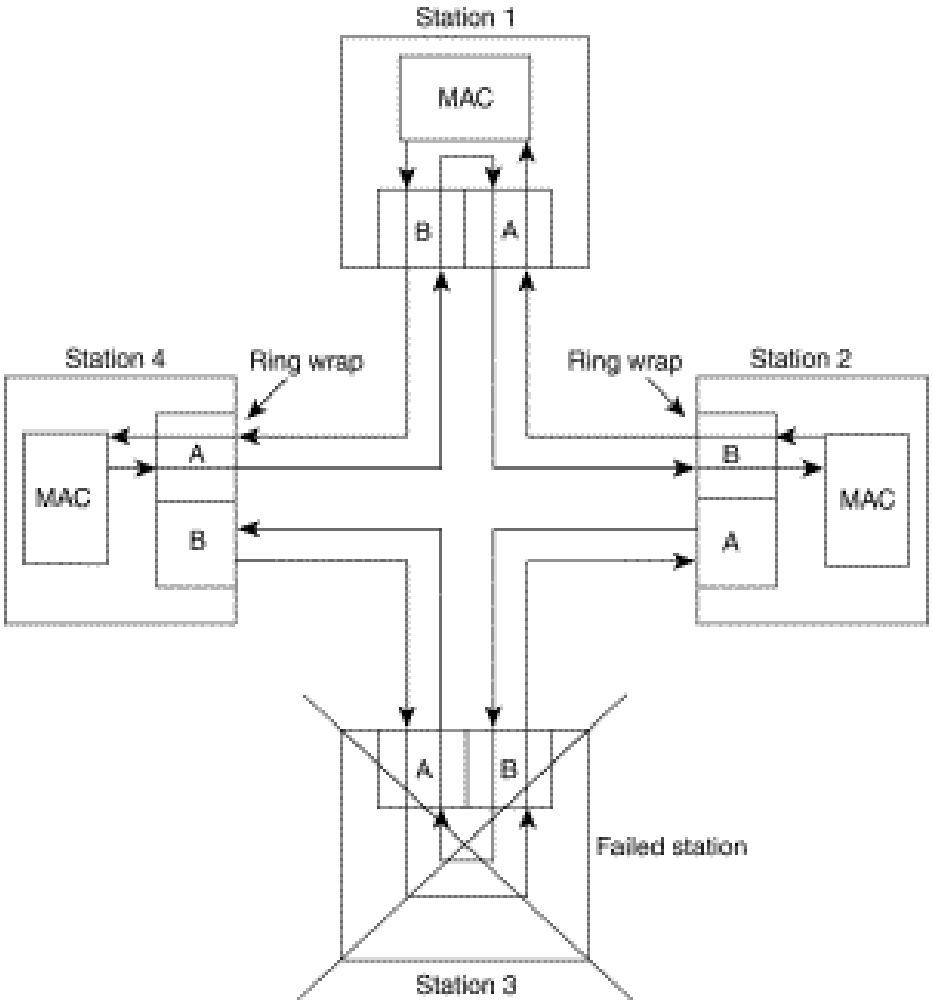
FDDI DAS Ports Attach to the Primary and Secondary Rings

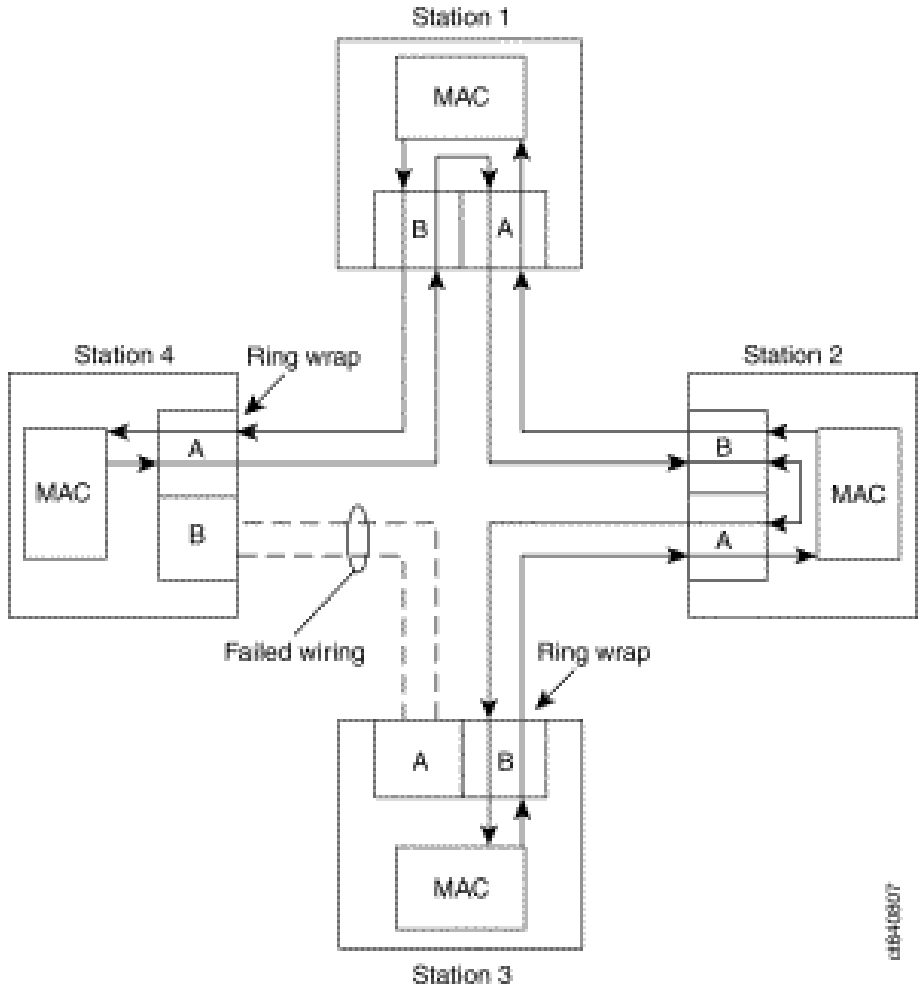


A Concentrator Attaches to Both the Primary and Secondary Rings

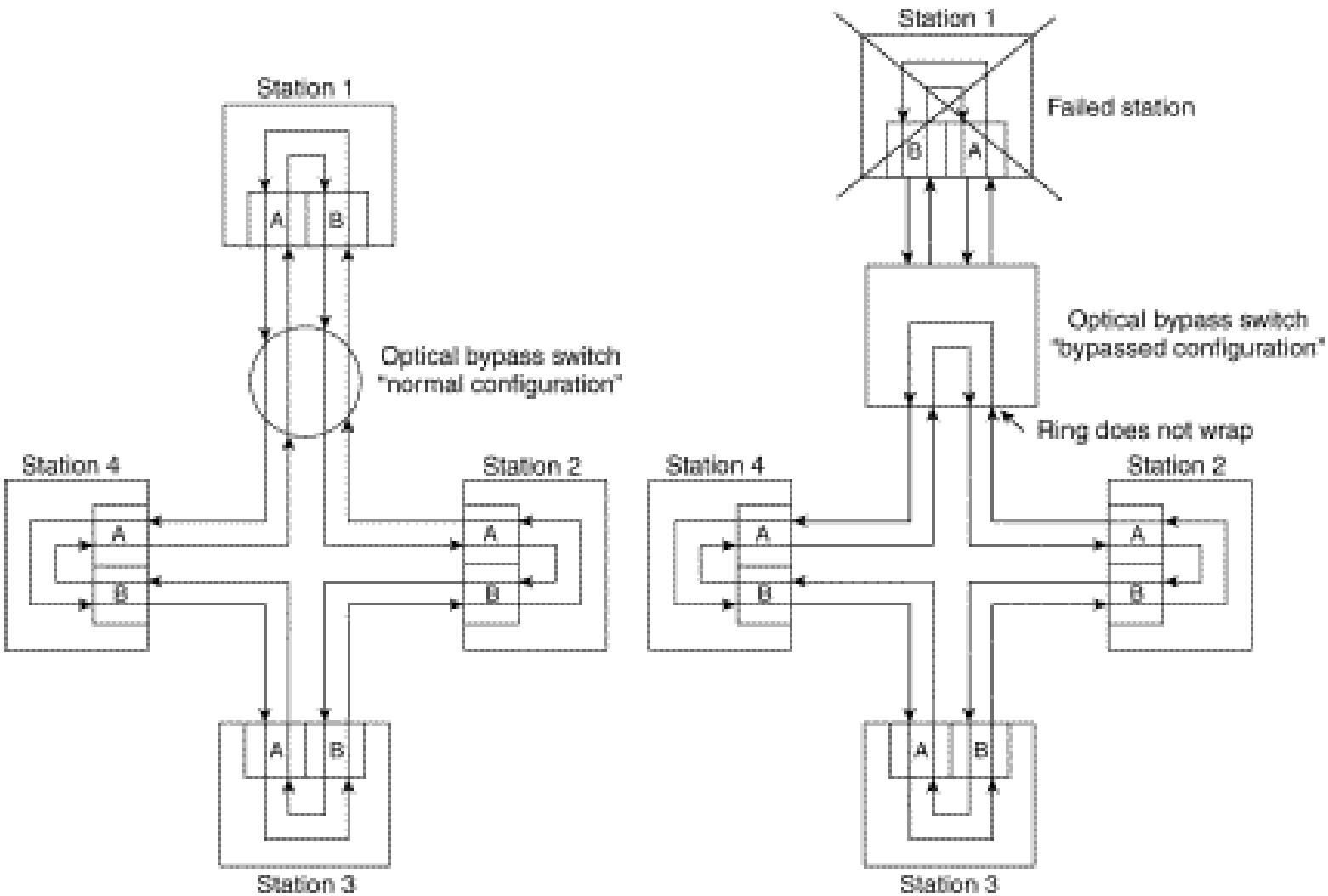


Повреда на станция или кабел

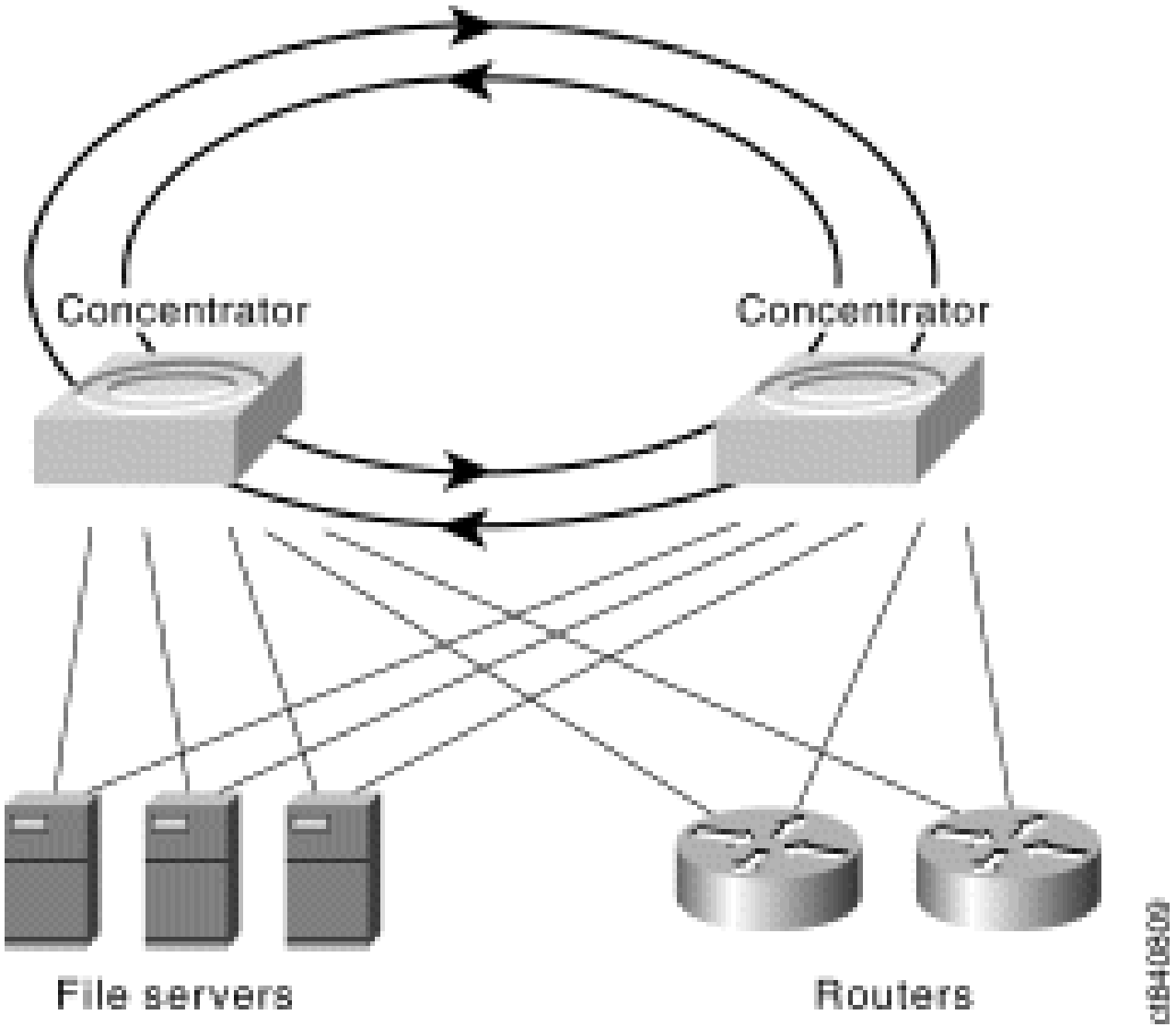




The Optical Bypass Switch Uses Internal Mirrors to Maintain a Network



A Dual-Homed Configuration Guarantees Operation



Стандарт 802.12 (100 VG – Any LAN) – 100 MB/S

Физически слой

Физическа топология тип “дърво” /както при 10 BaseT/. Мрежата включва главен концентратор /от първо ниво/. Влагане на концентратори до 5 нива. Всеки концентратор 100 VG – Any LAN може да бъде конфигуриран да поддържа или кадри 802.3 (Ethernet) или кадри 802.5 (Token Ring).

Условие: всички концентратори, разположени в един логически сегмент, т.е. неразделени с мост, комутатор или маршрутизатор, трябва да бъдат конфигурирани да поддържат кадри от един тип.

MAC-подслой

Използва протокола “приоритетен достъп по заявка” и се базира на предоставянето на концентратора на функции на арбитър, решаващ проблема с достъп до общата поделена мрежа. Използва се метод за разделяне на средата на две нива на приоритетност:

- нисък – на обикновените приложения
- висок – за мултимедийните приложения

IEEE 802.11

802.11	2.4 gigahertz (GHz) band	DSSS (Direct-sequence spread spectrum) modulation technique	1 and 2 Mbit/s
802.11a	5 gigahertz (GHz) band	OFDM (orthogonal frequency-division multiplexing)	54 Mbit/s
802.11b	2.4 gigahertz (GHz) band	FHSS (Frequency Hopping Spread Spectrum)	11 Mbit/s
802.11g	2.4 gigahertz (GHz) band	OFDM for the data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s	54 Mbit/s

Технологии за пренос

- с широк радиоспектър
  - *скачаща честота* (FHSS) – разделя честотната лента на подканали. В даден момент използва само един канал. Сигналът скача според предварително уговорен ред и честота
  - *директна поредица* (DSSS)– използва различните подканали в пореден ред
  - *ортогонална честота* (OFDM) – радиосигнала се разделя на множество подсигнали и едновременно се излъчва на съвсем леко различаваща се честота в общия канал

- с тесен или еднолентов радиоспектър – използват само един канал (микровълнов обхват). До 42м – открито, 12м – закрито. 15Mb/s

- инфрачервени – директна(разпространява се в една посока), дифузна(разпръсква във всички посоки). До 30м.

- лазерни – като директната инфрачервена комуникация

Точки за достъп (*Access Points*) - състоят се от радио модул, *Ethernet* интерфейси бриджинг софтуер.

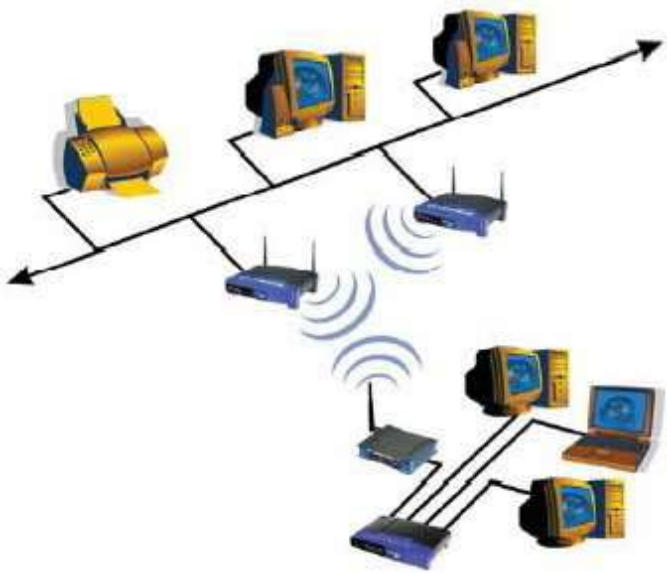
Клиентски устройства -*Wireless LAN* карти на *PCI*, *PCMCIA* или *USB* интерфейс

Типове безжични мрежи

Wireless мрежите имат два различни режима,на които могат да бъдат настройвани да работят:

infrastructure- - представлява *WLAN* и *LAN* мрежа, комуникиращи една с друга чрез *Access Point*

Ad-Hoc - конфигурация от компютри, екипирани с *Wireless* устройства, комуникиращи директно един с друг



Режими на работа на Access Point устройствата

•*Access Point* (*AP*) – това е първоначалният режим, който е бил създаден. Към устройството могат да се свързват компютри с *Wireless Lan* карти или *AP* устройства в клиентски режим, предоставящи свързаност на един или няколко компютъра.

•*AP Client* – този режим позволява на *AP* устройство да работи като клиент на друго *AP* устройство по същия начин както работи една *Wireless Lan* карта. Предимството е, че зад клиентското *AP* могат да бъдат свързани посредством *Switch* няколко компютъра, а не само един.Налични са всички услуги на безжичната мрежа, включително аутентикация на клиенти и т. н.

•*Wireless Bridge* – позволява свързването на няколко *LAN* мрежи чрез *Wireless* връзка. Много мощна алтернатива по отношение на дългите кабели и скоростта на изграждане на мрежата. Не се поддържа аутентикация на клиентски устройства, а само свързване между 2 или повече бриджа.

•*Point To Point Bridge (P2P Bridge)* – използва се в случай, че връзката е само между две устройства – всяко се свързва с другото и се осъществява връзка от точка до точка. Позволява свързването на бриджа само към един друг бридж

•*Point To Multipoint Bridge (P2MP Bridge)* – позволява към устройството да се закачат няколко устройства в бридж режим, като се осъществява връзка от тип една централна точка към много точки. Самото централно устройство поема целия трафик между отделните мрежи и ги свързва една с друга.

•*Ad-Hoc Bridge* – Много интересна разновидност на Bridge режима, използвана от някои производители (Linksys и др.) - при тях те работят в Ad-Hoc mode Мрежата е аналогична на горната с разликата, че не съществува едно централно устройство, а всеки бридж може да се свързва с другите.

•*Wireless Repeater* или *WDS* (*Wireless Distribution System*) – позволява на *AP* устройство да разширява областта на покритие на друго *AP*, като се свързва към него и същевременно обслужва клиентски устройства, нямащи връзка до отдалечения *AP*, но намираши се близо.

Покривни разтояния

•в затворени пространства (жилищни помещения, офиси, сгради и др.) е гарантирано покритие до 100 м

•на открито и при пряка видимост между устройствата се постигат разстояния на свързаност 300 – 400 м

•за да бъдат постигнати големи области на покритие и висока скорост на голямо разстояние, съществуват няколко начина – допълнителни антени, модифициран фърмуер и използването на усилватели

Сигурност при Wireless мрежите

•*SSID* (*Service Set Identifier*) - основен механизъм за разграничаване на две различни безжични мрежи, използващи едно и също физическо пространство, дори един и същ канал. Всички устройства в една *WLAN* трябва да имат един и същ *SSID.* Представлява последователност от символи, които обозначават една *WLAN* мрежа, и дължината му е от 1 до 32 знака (байта).

•*WEP* (*Wired Equivalent Privacy*) - протокол за сигурност, създаден да предложи защита на данните, съпоставима с тази на една кабелна мрежа. Открит пробив в сигурността на стандарта, които го правят уязвим за атаки.

•може да се извършва допускане до мрежата в зависимост от *MAC* адреса на клиентското устройство

Те могат да бъдат единствено допълнение към други, по-надеждни методи, като използването на ***VPN*** и *IEEE 802.1X* аутентикация. Тези технологии са първоначално разработени за стандартните *LAN* мрежи, но могат да бъдат приложени и тук и оперират на слой 3 от *OSI Layer* модела.

Края на 2002 г. *Wi-Fi Alliance* и *802.11i* групата на *IEEE* публикуват стандарт с подобрено криптиране на данните и проста, но сигурна аутентикация. Наречен е ***WPA*** (*Wi-Fi Protected Access*).

Metropolitan Area Network (MAN)

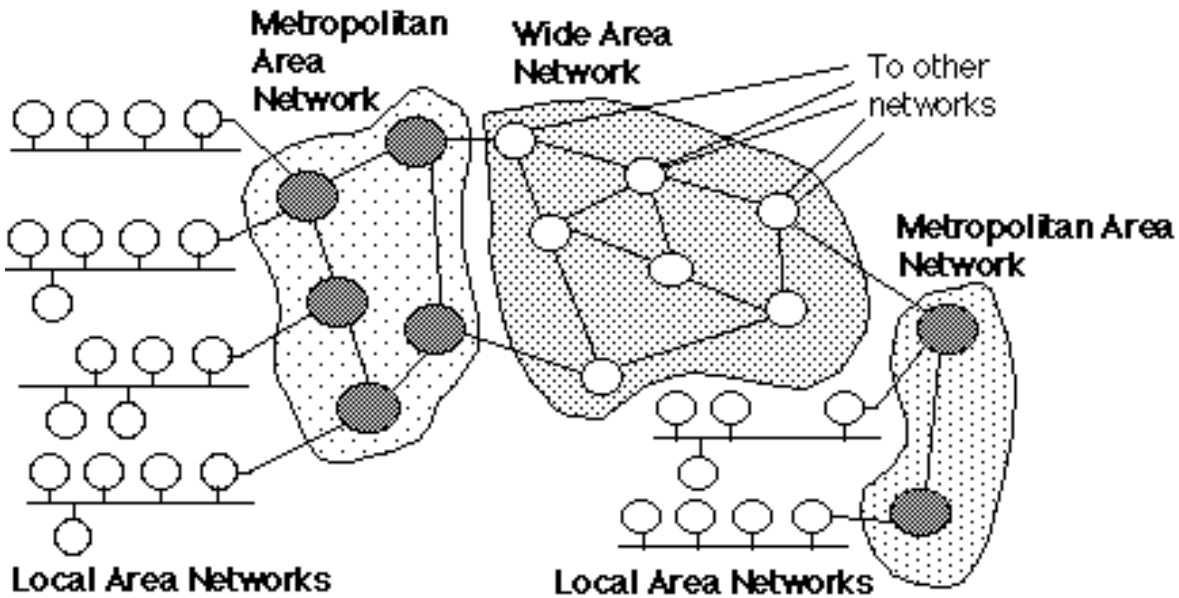
- Попадат между LAN и WAN (между 5 и 50 км диаметър)
- Поддържането на изохронен трафик (видео, глас)
- Висока производителност, поддържаща високоскоростни услуги
- Възможност за използване на съществуващите цифрови линии на обществените мрежи за пренос (например, телефонни мрежи)

Използване на MAN

•За взаимно свързване на няколко LAN

•Директно свързване на сървъри и високопроизводителни работни станции

• няколко MAN могат да бъдат свързани чрез WAN (между 5 и 50 км диаметър)



Топологии

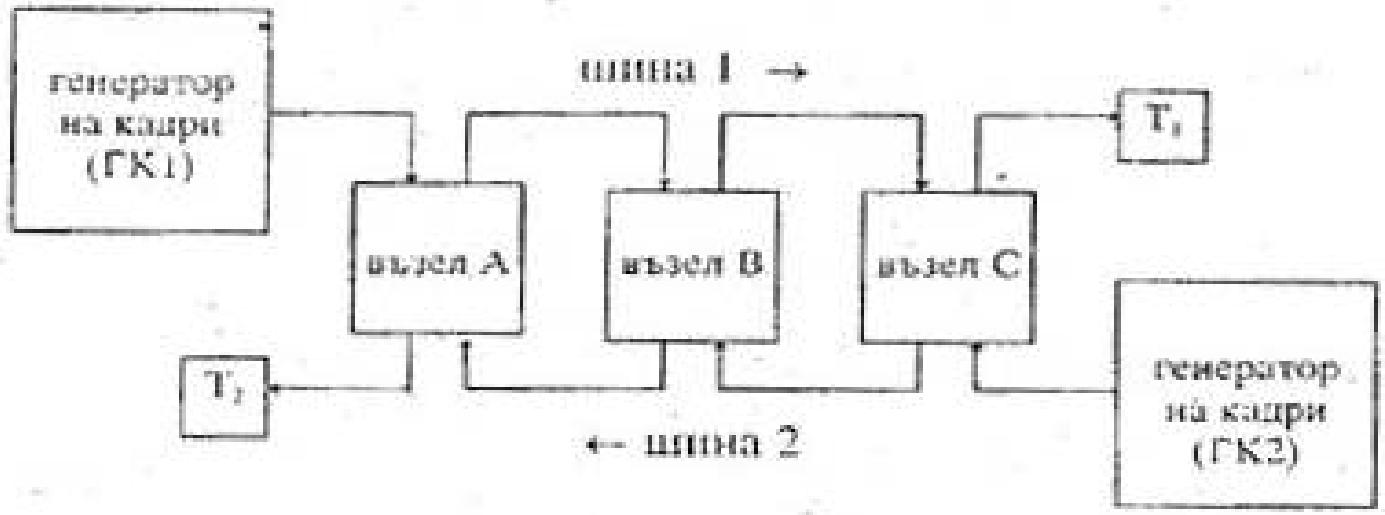
- Звезда, шина, кръг и техните комбинации

Услуги

- С установяване на логическо съединение
- Без установяване на логическо съединение
- Изохронни услуги (предаване на глас и видео)
- Broadcast
- Multicast

Физически слой на IEEE 802.6

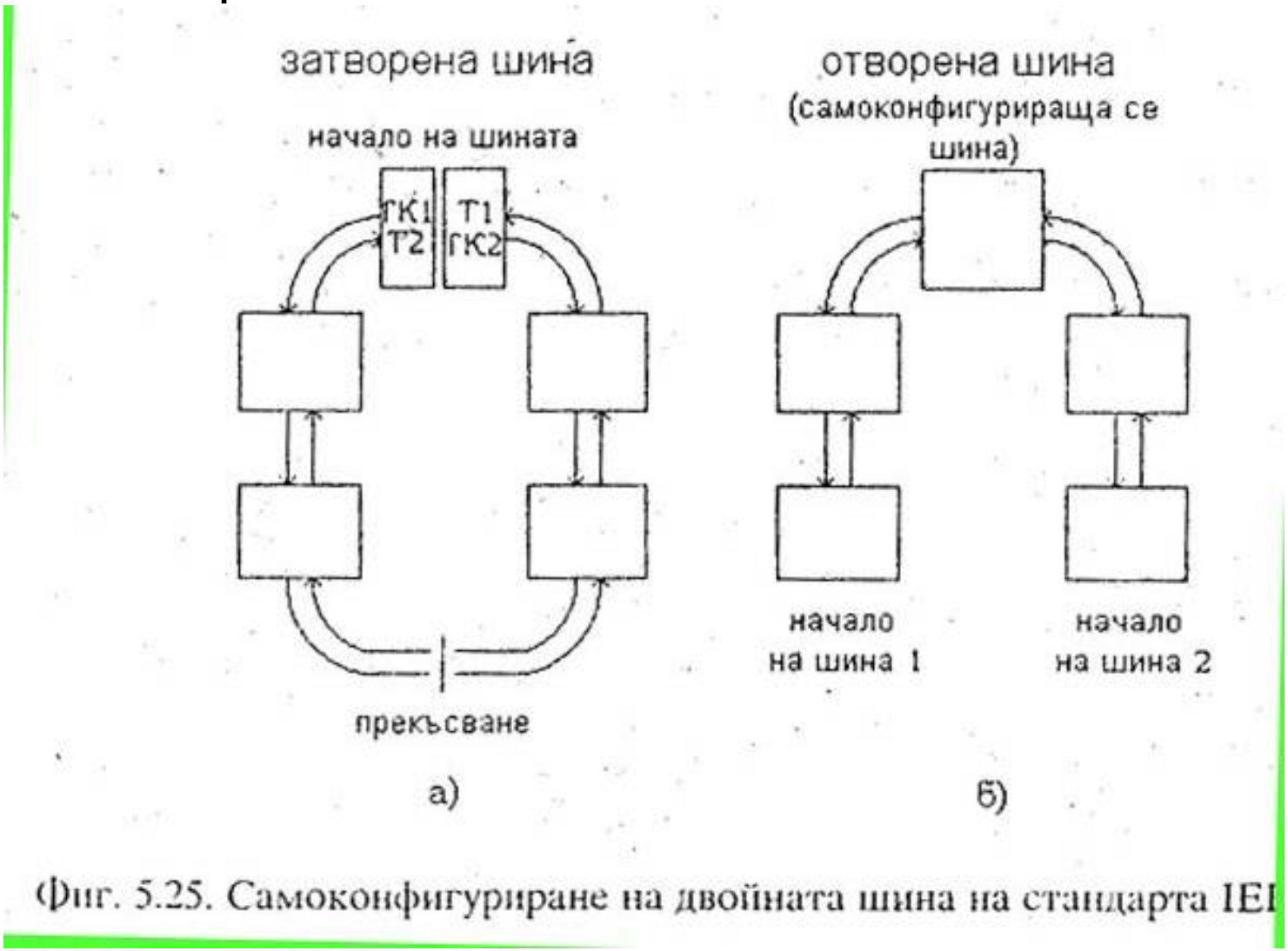
- Използва двойна шина (dual bus)
- Посоките на предаване са противоположни



Фиг. 5.24. Физическа топология тип „двойна шина" на MAN-стандарта IEEE 802.6.

- Генераторът генерира кадри на всеки 125мс

•Всеки възел може да генерира кадри – самоконфигурира не в отворена шина при прекъсване на кабел и запазване на двойната връзка



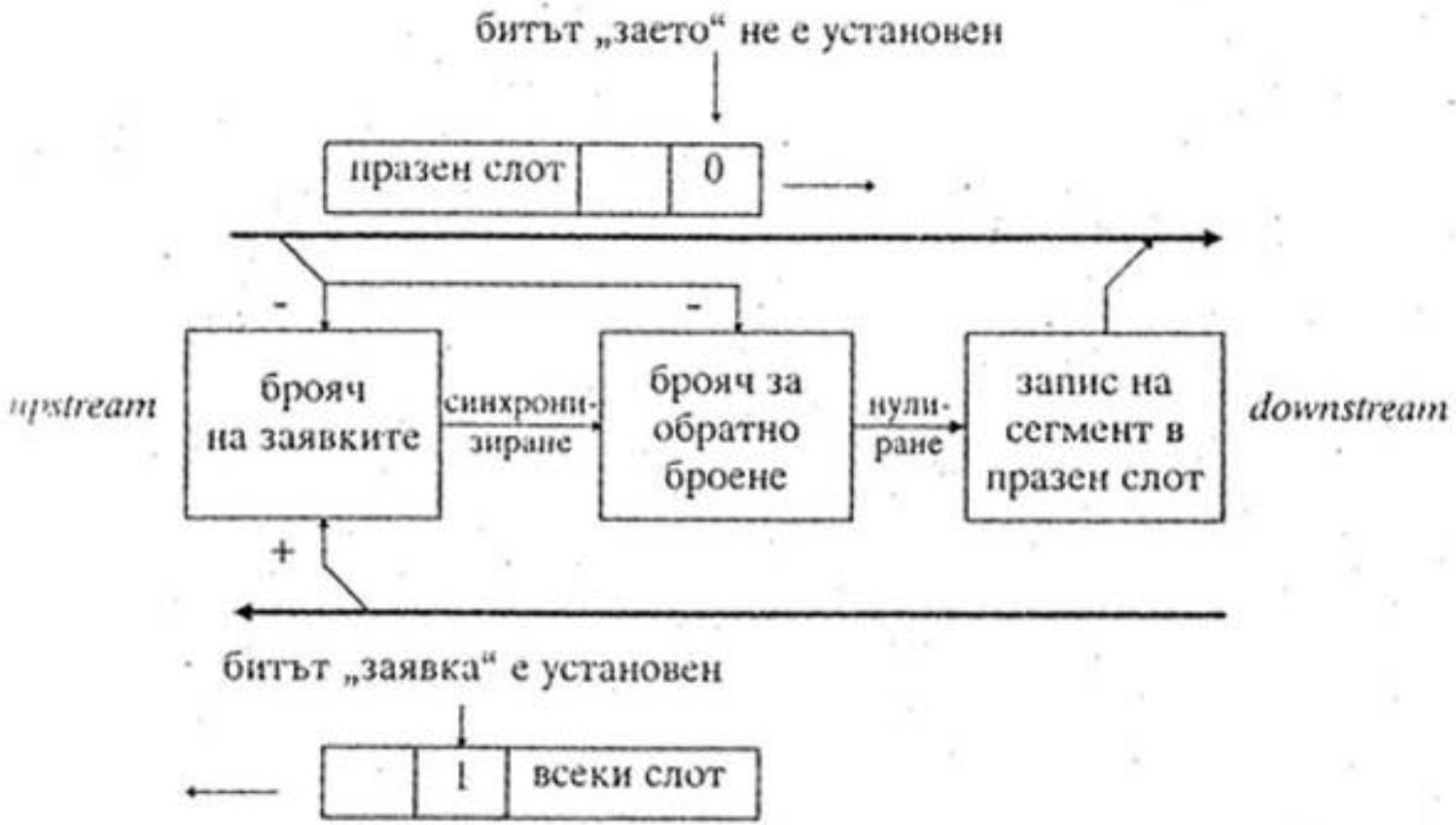
Фиг. 5.25. Самоконфигуриране на двойната шина на стандарта IE

MAC подслой на стандрта

•Протокол: DQDB (Distributed Queue Dual Bus)

•Използват се слотове – DQDB клетки (загл. част, данни). Структурата зависи от метода, който се използва.

•QA(Queue-Arbitrated) слотът (за анизохронните данни) съдържа два бита в заглавната част: ”заето”-дали слотът е зает и “заявка”-за резервация на място в опашката



Фиг. 5.26. Разпределена опашка в MAC-протокола DQDB

WAN стандарти
Стандарт X.25

- най-известен и използван при WAN с комутация на пакети
- скорост 2 Mb/s
- специфицира интерфейса между крайния възел и глобална подмрежа

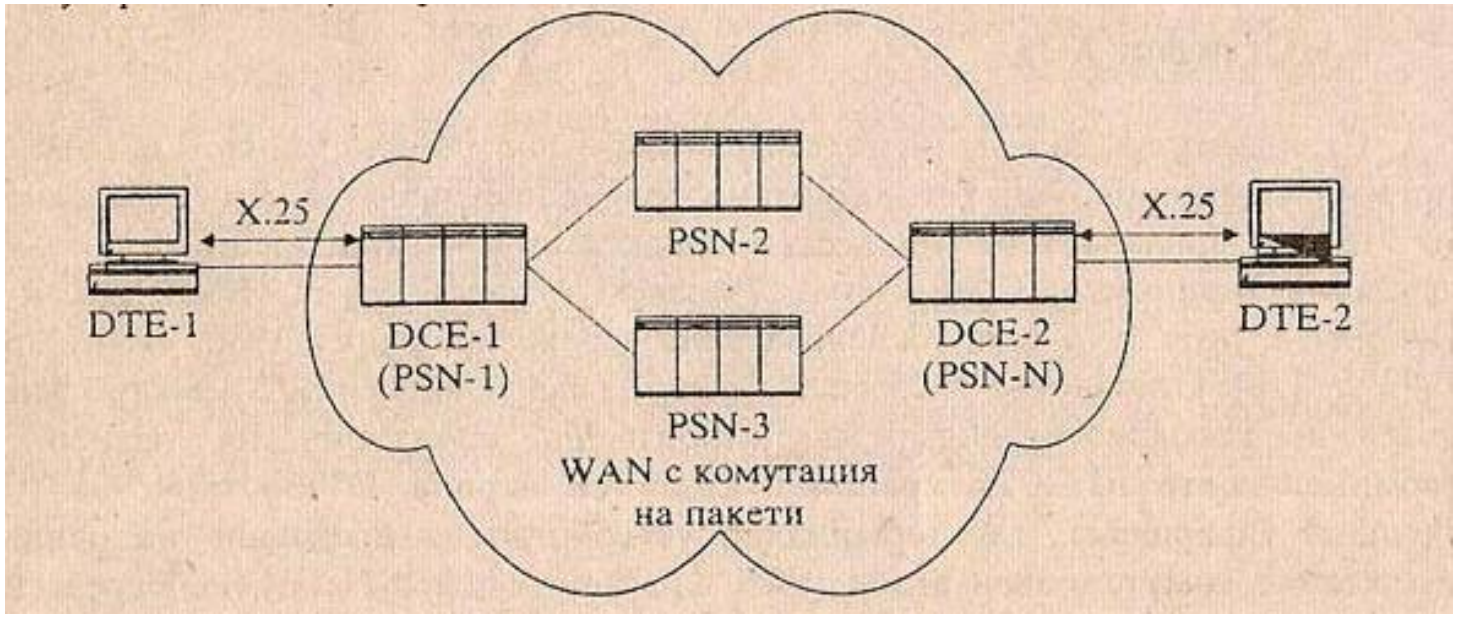
Термини

DTE (Data terminal Equipment) – клиентско у-во

PSN (Packet Switched Node) – междинен мрежов възел

DCE (Data Circuit – terminating Equipment) – PSN непосредствено свързан с DTE

X.25 – по-скоро стандарт за достъп до глобалната мрежа



Предаването става без нарушаване на последователността и без грешки. Използва отрицателни квитанции за лошите кадри.

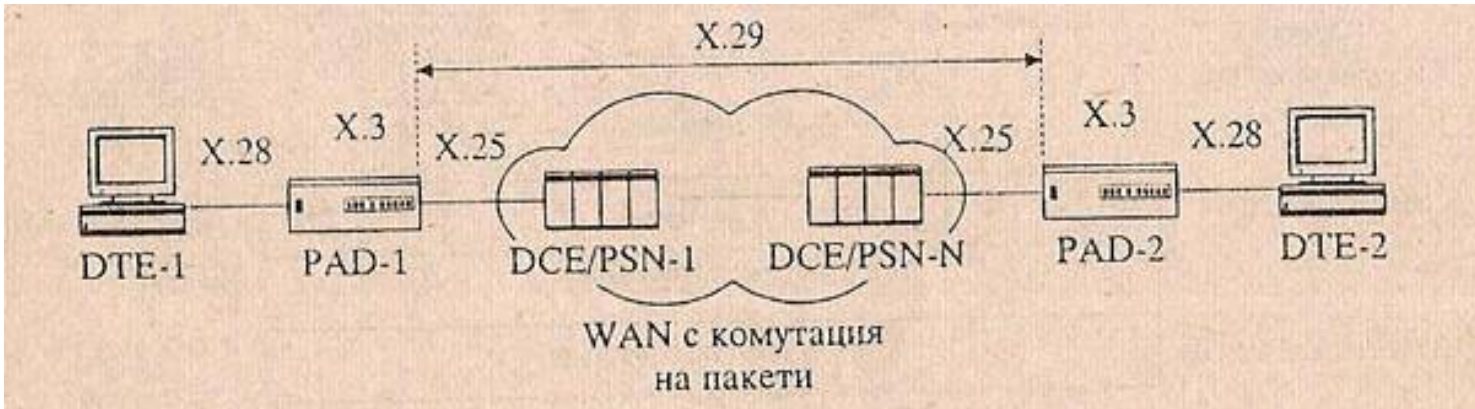
DTE – специален пакетен терминал. При обикновен компютър или терминал се поставя PAD (Packet Assembler/Disassembled) у-во, изпълняващо функциите на мрежовия слой(слепване, разделяне на пакети)

PAD работи на нивото на мрежовия слой, изпълнява и концентриращи функции.
За неговото функциониране се използват препоръките “Triple X”:

X.28 – определя интерфейса между DTE и PAD

• X.3 – определя услугите на PAD

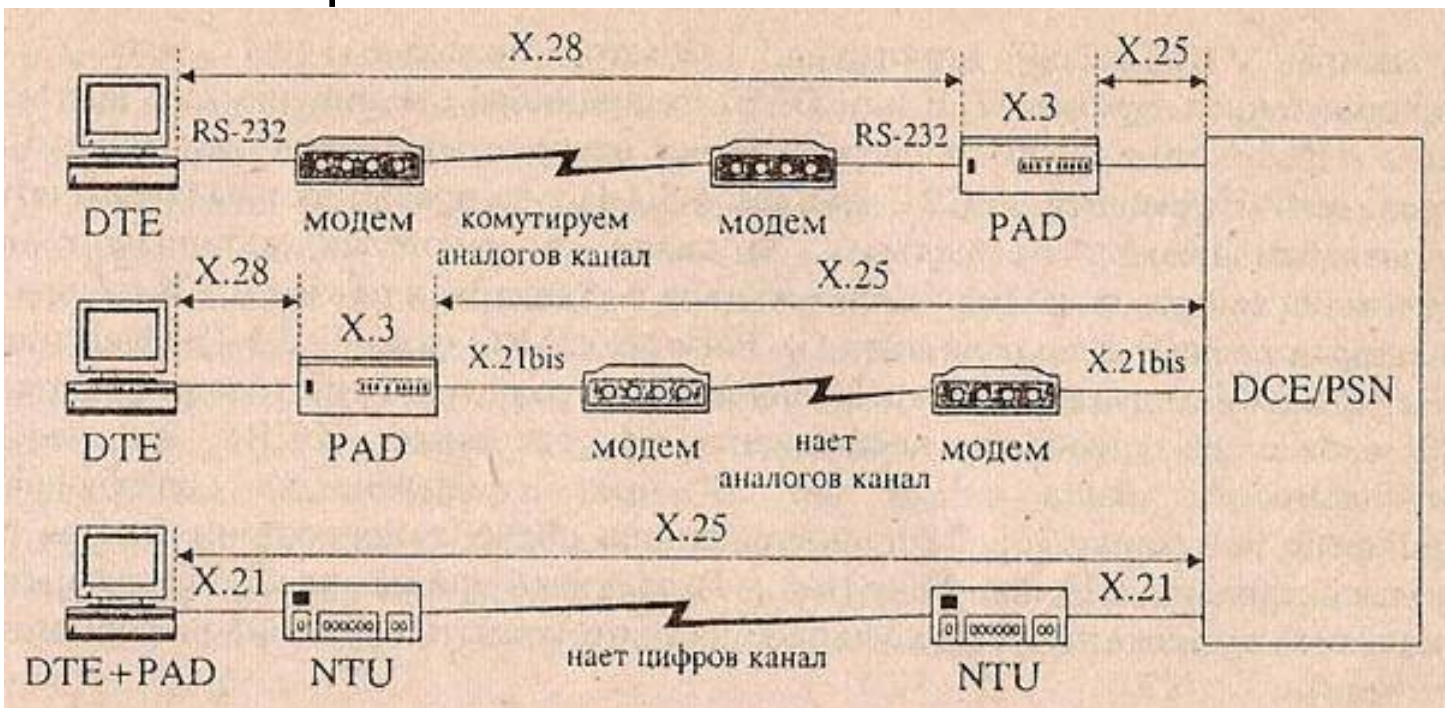
• X.29 – описва взаимодействието между две PAD устройства



Фиг. 6.3. Използване на PAD-устройство за достъп на непакетен терминал до WAN с комутация на пакети

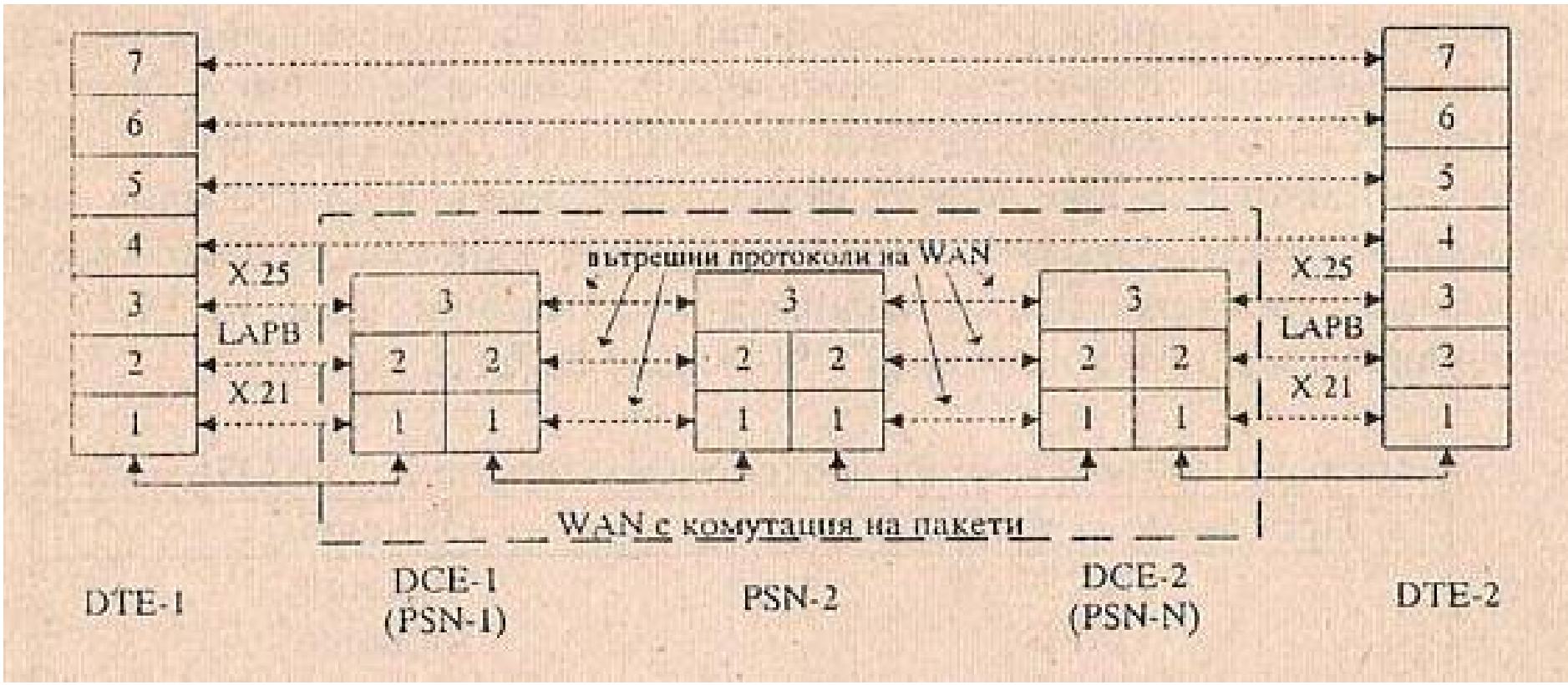
Разположение спрямо DTE:

- обществен PAD – DTE се свързва чрез модем
- външен PAD – непосредствено до DTE
- вътрешен PAD – разположен в DTE



Фиг. 6.4. Видове PAD и начини на свързване към DTE-устройство

Протоколен стек X.25	OSI
X.25	мрежов
LAPB	канален
x.21,x21 bis	физически



Физически слой на X.25

Използва протоколите:
• x.21- при наета цифрова линия

• x.21 bis – за работа със смесени канали (аналогови и цифрови)

Приличат на RS – 232C(V.24) – за комуникация по сериен порт на компютъра

Канален слой на X.25

Използва протокол LAPB (Link Access Protocol - Balanced).
Balanced – позволява на съединение и от към двете страни.
Следи за грешки в кадрите и спазване на последователността им.
Използва метода на “плъзгащия се прозорец” (8 кадъра в стандартен и 128 в разширен режим)

LAPB използва 3 вида кадри:

• информационни (I-кадри) – пренасят информацията на горния слой

•Супервайзорни (S-кадри) – управляват основните функции на LAPB протокола

•Неномерирани (У-кадри) – изпълняват допълнителни управляващи функции (преминаване между разширен и стандартен режим, генериране на съобщения за протоколни грешки)

Мрежов слой на X.25

Протокол X.25 – използва режим на виртуално съединение.

Съществуват два вида съединения:

• PVC (Permanent Virtual Circuits) – постоянни

•SVC (Switched Virtual Circuits) – комутируеми – протичащи на три фази: установяване, предаване и разпадане на логическо съединение

Стандарт Frame Relay

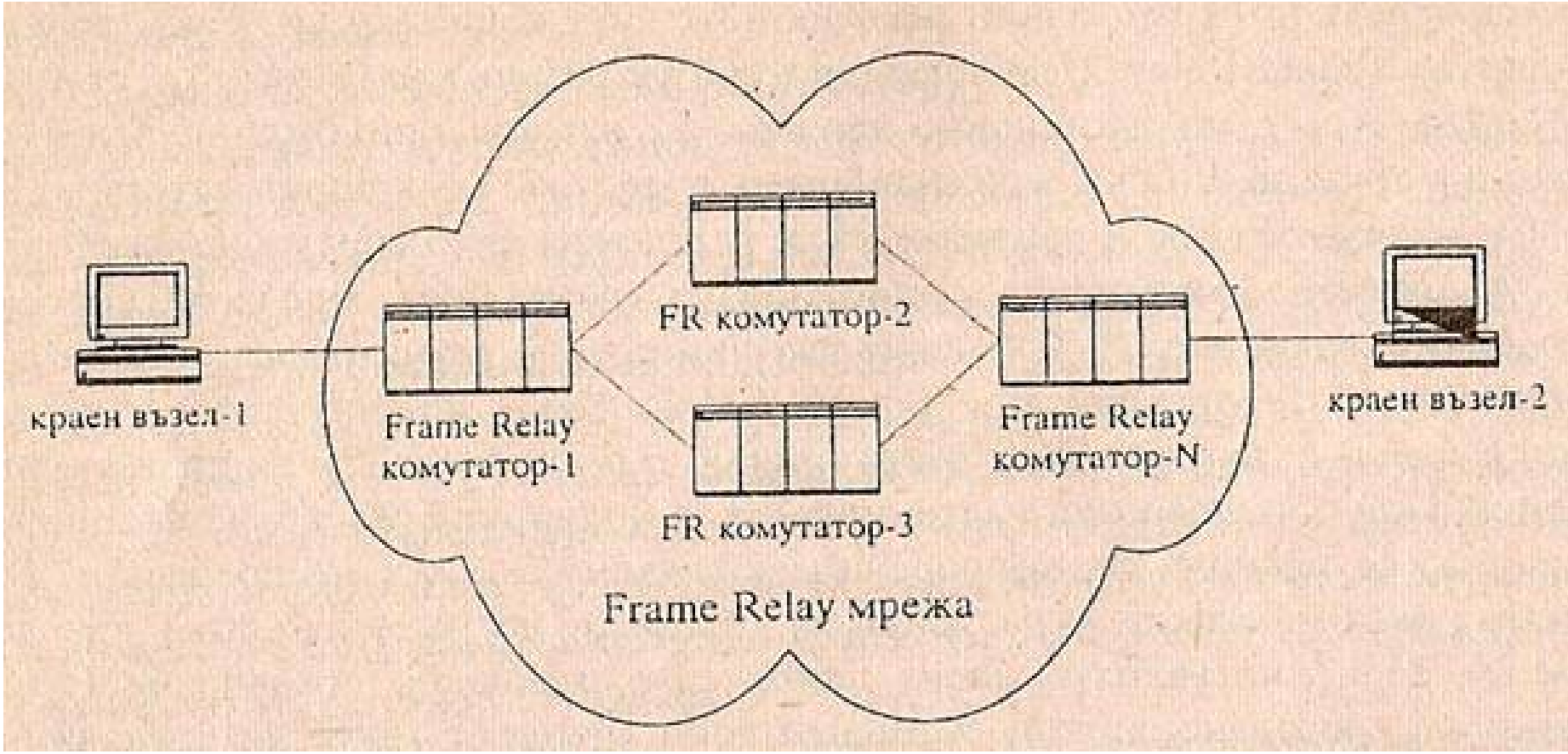
Подобен на X.25 за достъп до глобална мрежа с комутация на пакети.

X.25 по-бавен – проверка на всички пакети във всеки PSN възел (допълнителна управляваща информация), което утежнява тяхната работа – дължи се на тогавашните слаби компютри и ненадеждни аналогови телефонни линии.

Frame Relay – опростяване на протоколите, като по-голямата част от обработката се предоставя на крайните възли – разчита на надеждните цифрови линии+бързи компютри

Frame Relay – като виртуална наета линия.

Абонатите наемат PVC. Предават се Frame Relay кадри.



Скорост – 34 Mb/s (Европа), 45 Mb/s (САЩ)

Разлика между наетите линии:

•Обикновенна – заплаща се договорената максимална скоростна предаване (дори да не се използва)

•Виртуална – заплаща се договорената средна скорост на предаване

Междинните мрежови възли с опростени функции, свързани главно с определяне на границите на кадрите и откриване на грешки в тях.

Сгрешените кадри се “бракуват”. Възтановяването им – зависи от трафика:

•*При изохронен* – няма смисъл сгрешените кадри да се предават, защото са чувствителни към закъснение. Ефект – мигновенно пропадане на гласа при гласово предаване

•*При анизохронен* – не е чувствителен към закъснение, а към грешки – се искат наново сгрешените кадри.

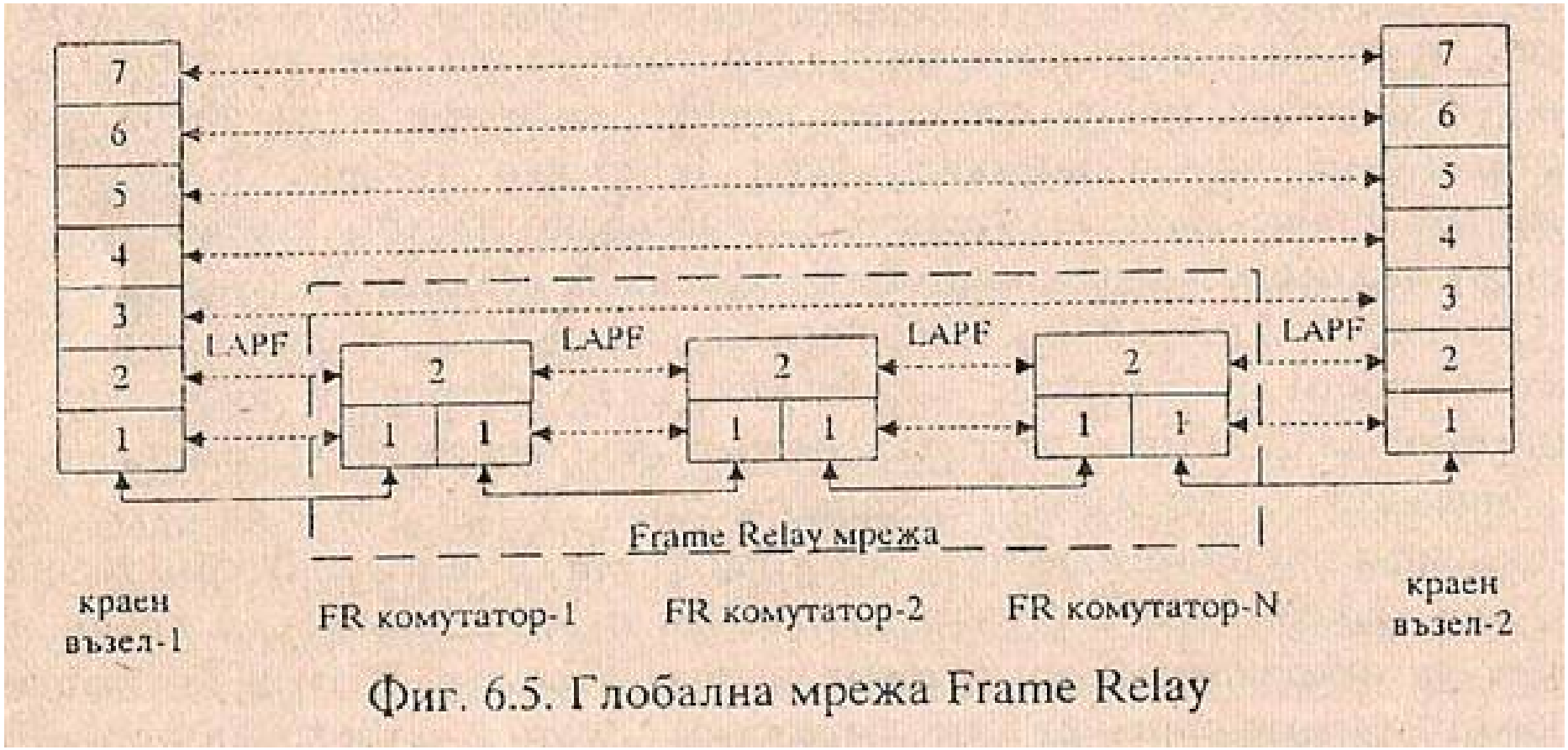
Frame Relay не потвърждава правилно приетите кадри за междинните мрежови възли (повишава се бързодействието)

Комутаторите “бракуват” кадрите в два случая:

•ако ги приемат с грешка

•ако не могат да ги съхранят поради препълване на буферите си – комутаторът известява за това крайните възли на всички активни PVC към него

Frame Relay използва протокола LAPF (LAP for Frame – mode bearer services)



Фиг. 6.5. Глобална мрежа Frame Relay

При PVC съединението доставчикът и абонатът се договарят за 3 параметъра (T_c, B_c, B_e)

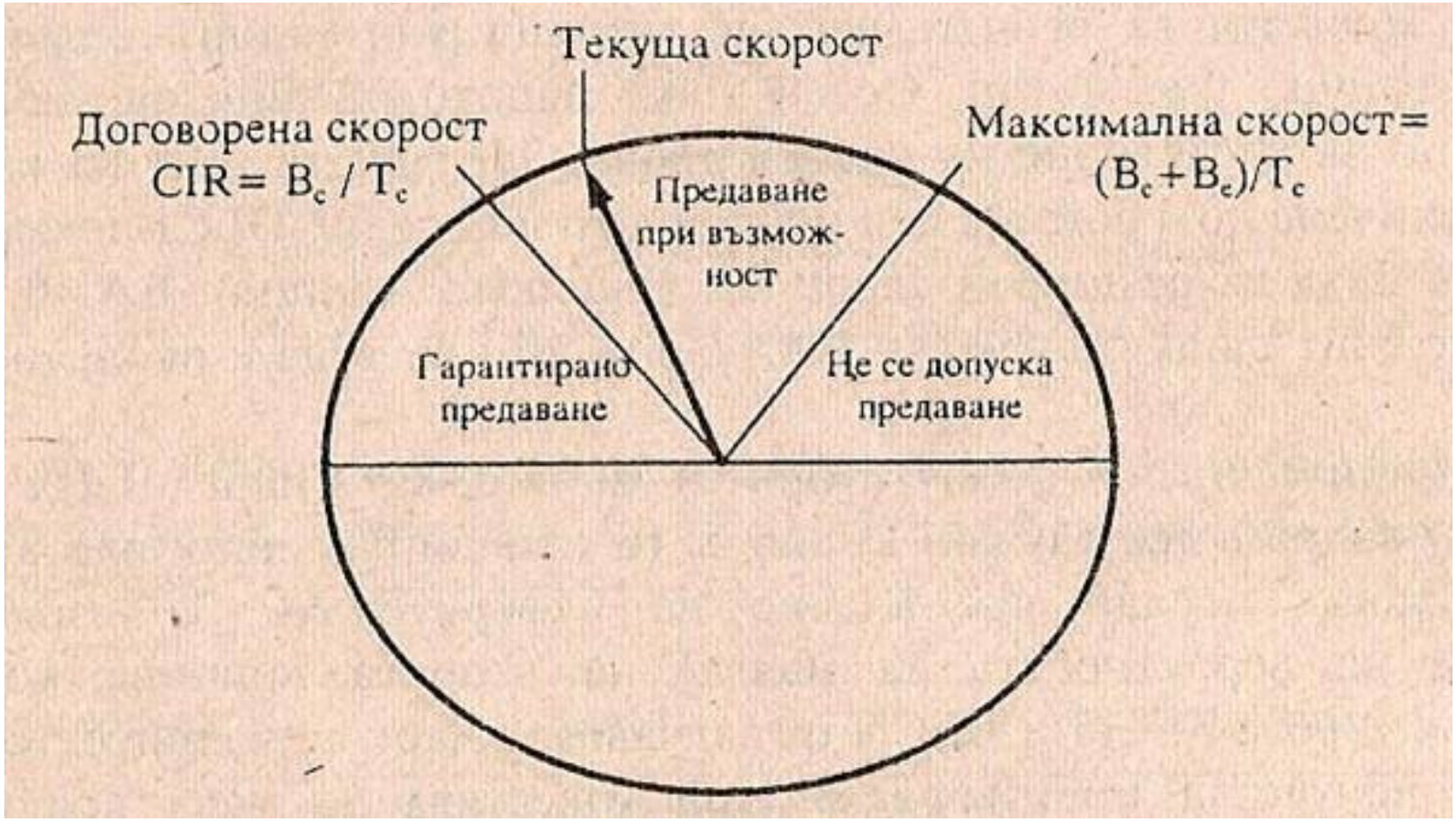
T_c - времетраене на интервалите, на които се разделя времето

B_c – гарантирани байтове за клиента от доставчика за T_c

CIR= B_c / T_c– договорена скорост, (Committed Information Rate), явява се средна скорост

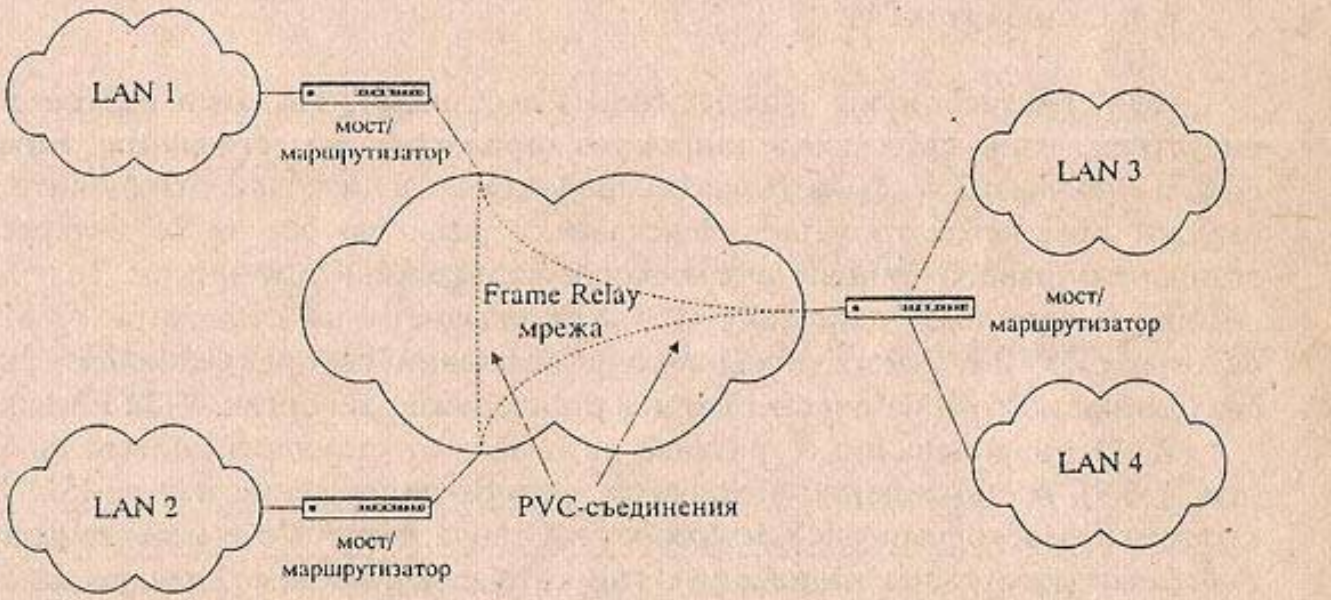
B_e – байтове в повече от B_c, като само B_e се приемат за T_c, но се маркират като нископриоритетни

(B_c + B_e)/ T_c – максималната скорост, с която абонатът може да предава

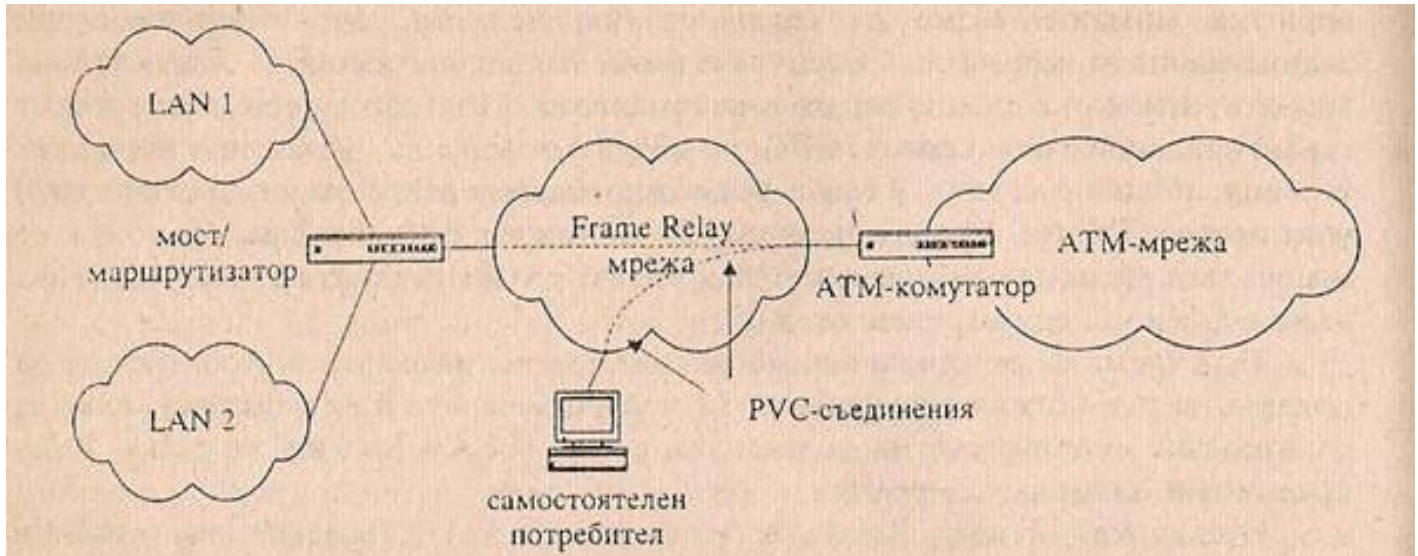


Използване на стандарта:

- за свързване на локални мрежи
- като глобална мрежа за анизохронни данни
- като средство за достъп до АТМ мрежи



Фиг. 6.8. Използване на Frame Relay мрежа за свързване на локални (LAN) мрежи помежду им



Фиг. 6.9. Използване на Frame Relay мрежа за достъп до ATM-мрежа

Стандарт ATM
(Asynchronous Transfer Mode)

ATM – още като Cell Relay (комутация на клетки) – използва блокове с фиксирана дължина (53 байта)

5 байта за заглавна част, 48 байта за данни

Съществуват два вида клетки:

UNI – използват се при интерфейса “потребител-мрежа”

NNI – между междинните мрежови възли

Използва комутация на пакети и мултиплексиране на няколко логически съединения по един физически интерфейс (до 1024 за физическа линия)

Използва предимството на новопоявилите се цифрови линии.

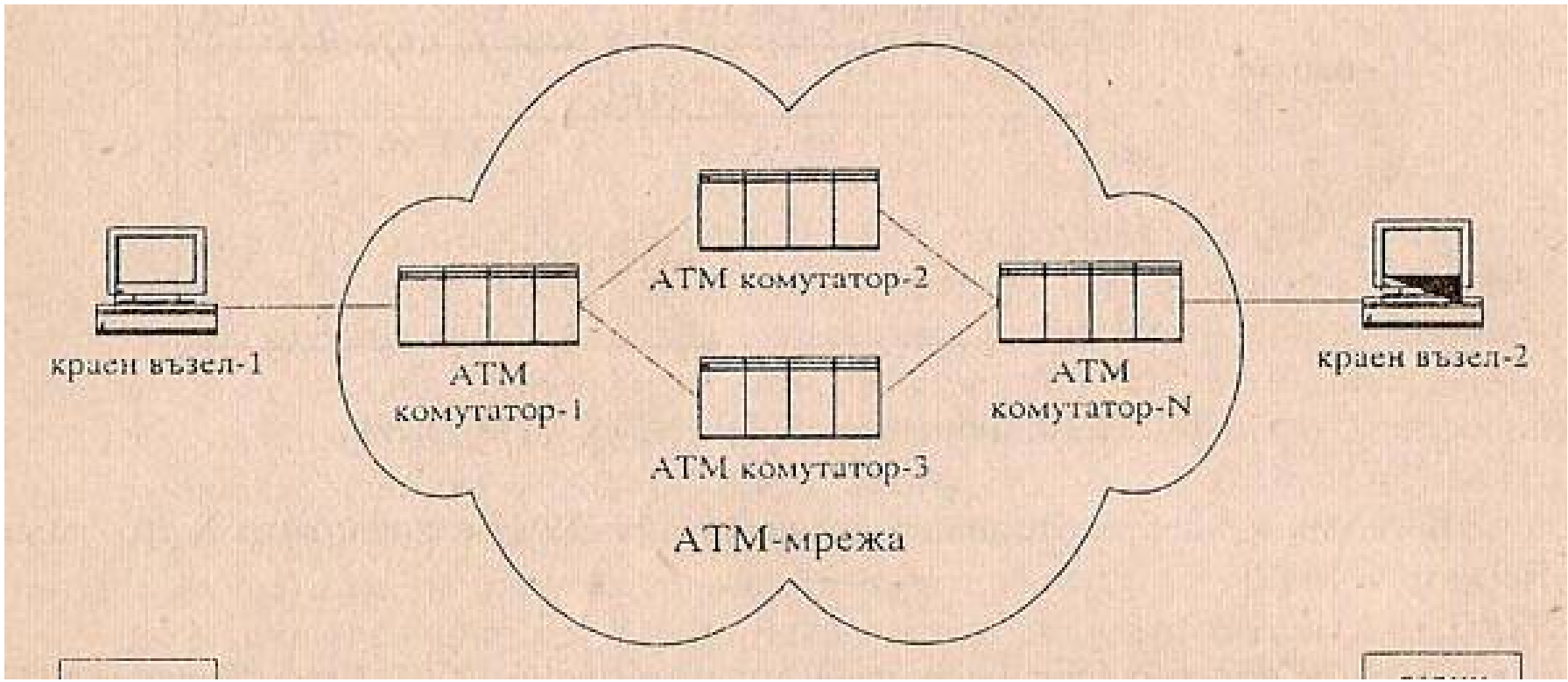
ATM използва скорости с наколко пъти по-високи от Frame Relay – следва от :

•използването на минимални средства за контрол на грешки и за управление на потока данни

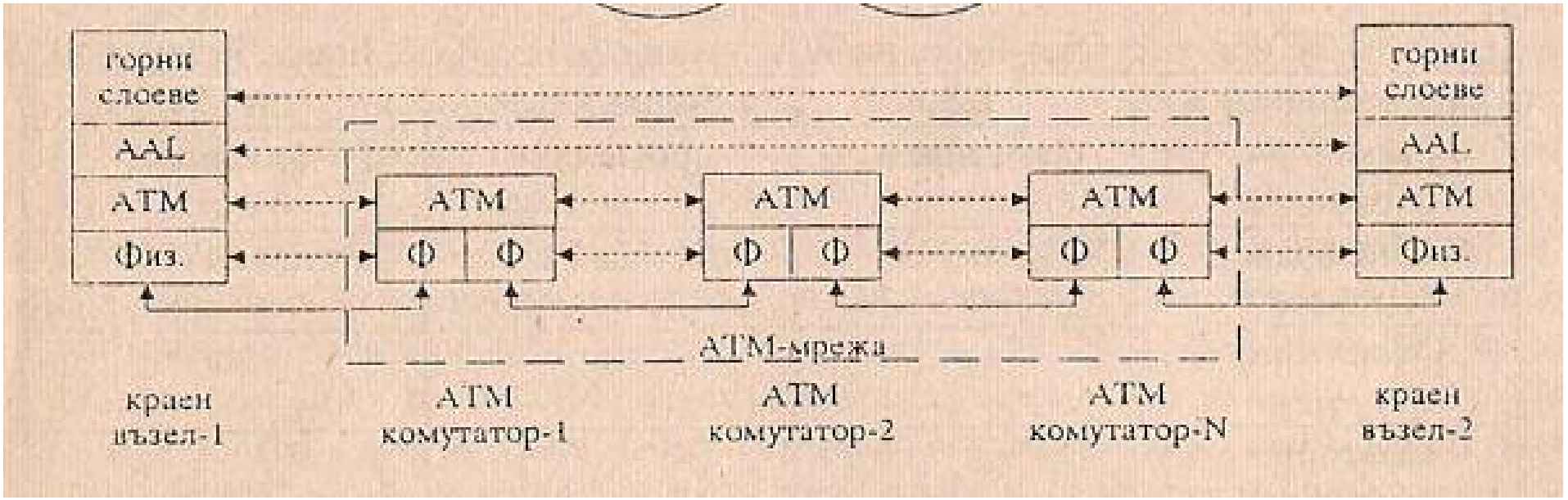
•фиксиран размер на клетките

Характеристика	X.25	Frame Relay	ATM
Размер на блоковете	променлив	променлив	фиксиран
Използване на флаг	да	да	не
Откриване на грешки	да	да	да
Повторно предаване на сгрешени блокове	Извършва се от мрежата	Извършва се от крайните възли	Извършва се от крайните възли
Контрол на натоварването на мрежата	не	да	да
Скорост на предаване	64 Kb/s – 2Mb/s	До 34 (45) Mb/s	25 Mb/s – 622 Mb/s (до 2.5 Gb/s в бъдеще)
Трафик	Анизохронен	Главно анизохронен	Всякакъв вид
OSI слоеве	1 2 3	2 и част от 3	1 2 3 и част от 4
Приложение	За достъп до глобална мрежа с комутация на пакети	За свързване на локални мрежи, за достъп до ATM мрежи	Като глобална мрежа за свързване на локални и регионални мрежи

Общ вид на ATM мрежа



Слоеве



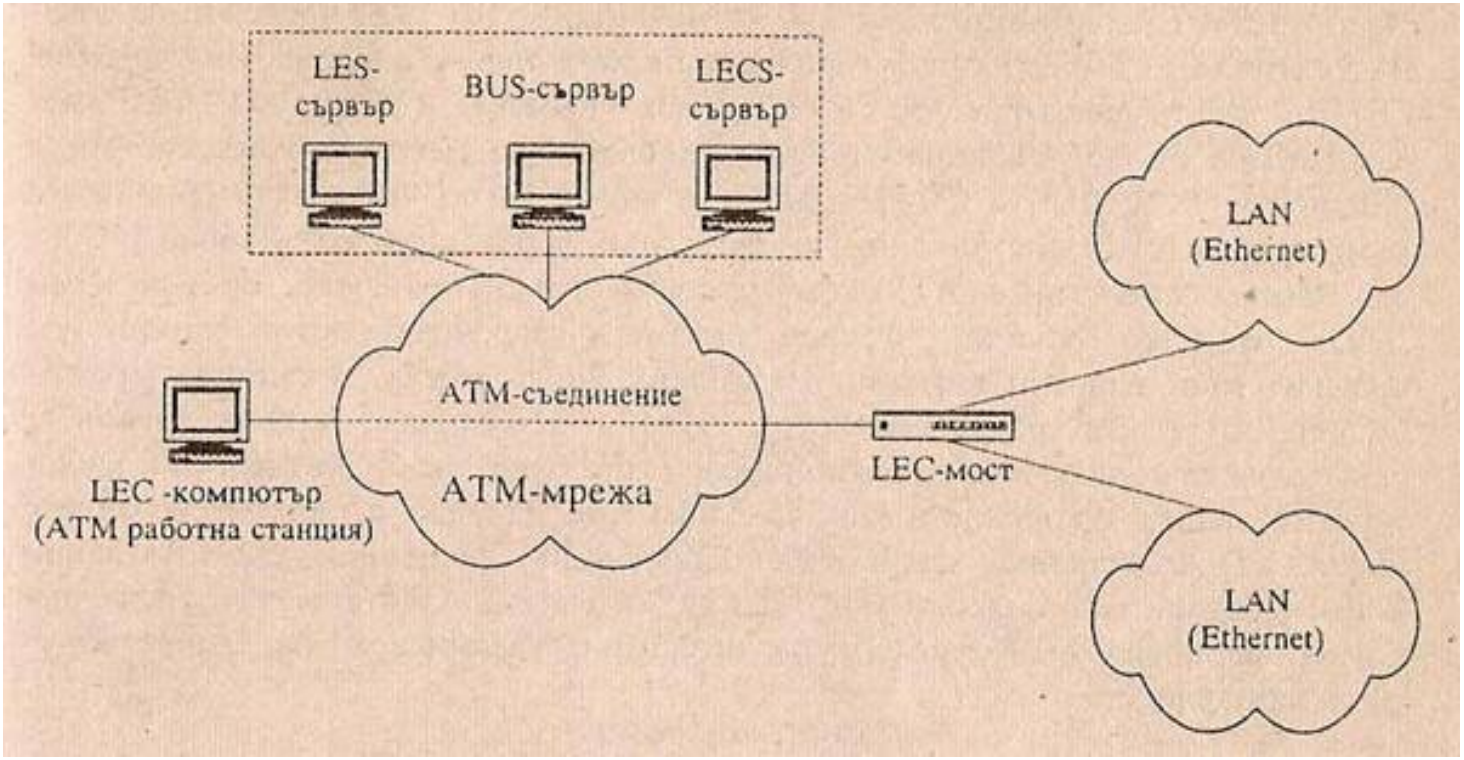
- Физически слой – съставен от два подслоя:
  - Долен – зависещ от физическата среда
  - Горен – конвертира ATM клетките в поток от битове

•ATM слой – независим от физическата среда

Едни от основните функции:

- •мултиплексиране (демултиплексиране) на ATM клетки от различни логически съединения в един поток от ATM клетки предавани към физическия слой
- •извършване на комутация на ATM клетки в междинните възли на мрежата

•AAL (ATM Adaptation Layer) – подобрява обслужването, предоставено от ATM слоя, до изискванията на следващия по-горен



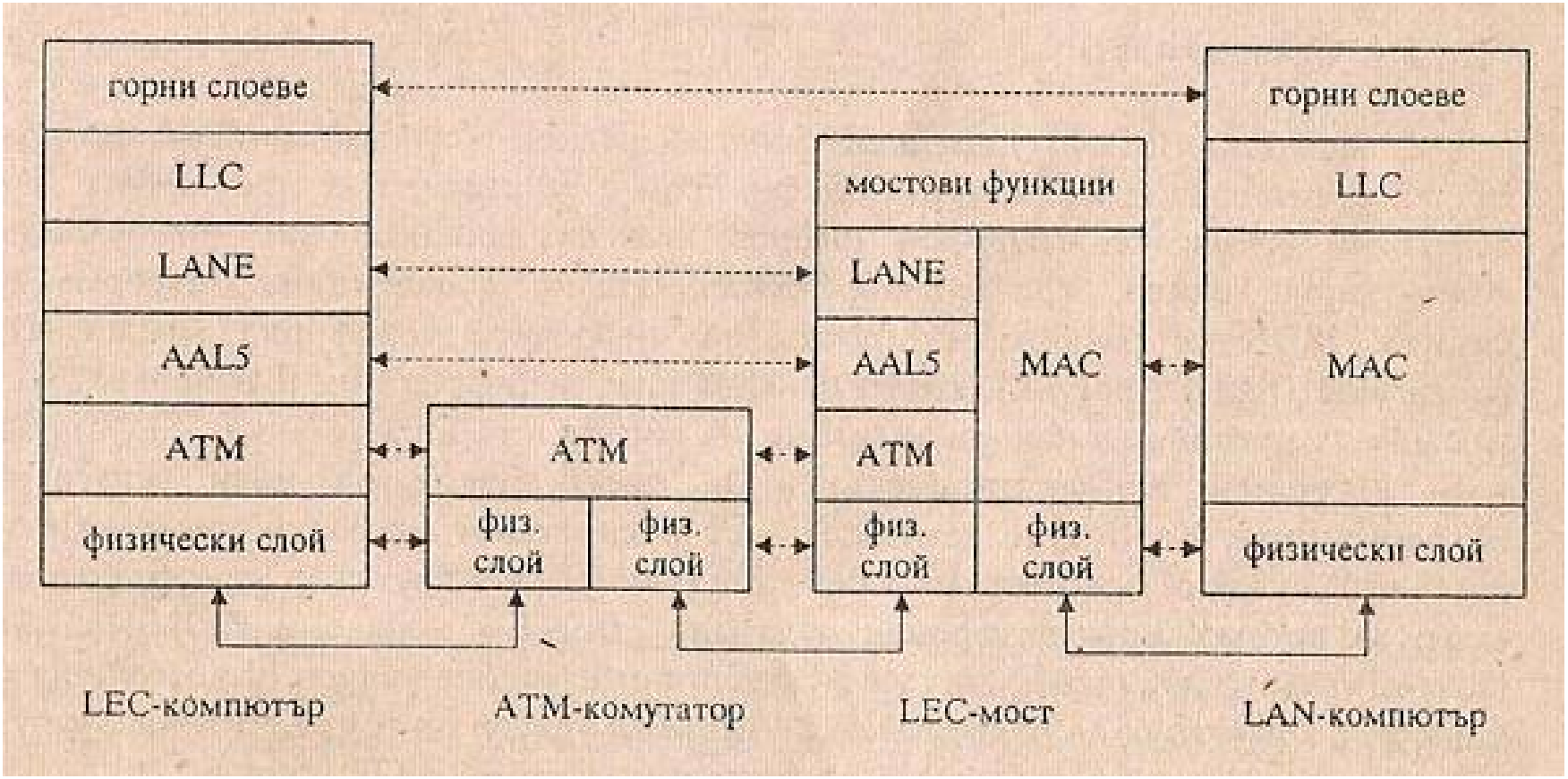
LEC – LAN Client

LES – LAN Server, подава адреса на LEC получателя, ако го знае, иначе запитване към BUS. Поддържа мрежата.

BUS – broadcast сървър, необходим защото LAN използва този тип съобщения, изпращат се към него

LECS – (LANE Configuration Server) – връща към LEC (при първоначалното му включване) адресите на LES и BUS сървърите. След тази процедура LEC иска разрешение от LES за присъединяването на неговата локална мрежа.

LES, BUS, LECS сървърите могат да бъдат на един или различни компютри.



LANE – LAN Emulation, реализира се софтуерно (чрез драйвер) в MAC – подслоя на каналния слой.

Протокол AAL5 – за трафик на IP диаграми и Frame Relay кадри

Стандарт ISDN

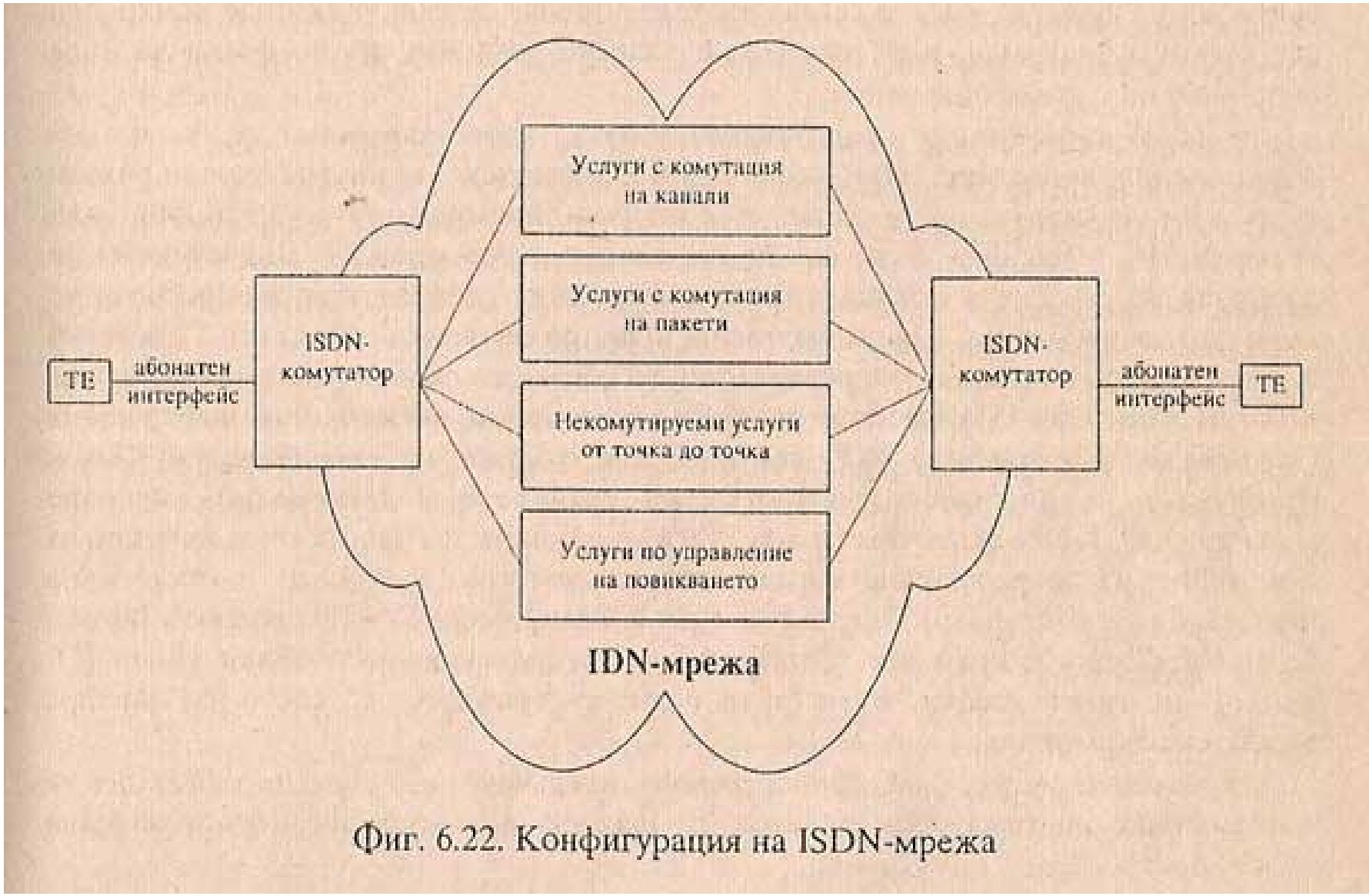
ISDN (Integrated Services Digital Network) – цифрова мрежа с интеграция на услугите (1984 г.).

Идея: Осъществяване на достъп до всички видове комуникационни услуги през една точка и през единствен абонатен номер

Осигурява пренасяне в единен цифров вид на всякакъв вид информация:

- компютърни данни
- глас
- изображения
- видео
- факсимилна информация
- музика

ISDN се развива на базата на телефонната мрежа *IDN (Integrated Digital Network)*



Фиг. 6.22. Конфигурация на ISDN-мрежа

ISDN комутаторът позволява различните услуги предоставяни от различни мрежи да бъдат достъпни за потребителите

ISDN комутатор – цифрова автоматична телефонна централа с добавени ISDN модули

Съществуват 3 вида услуги:

•*преносни* - покриват функциите и протоколите на долните три слоя от OSI модела:
✓ за пренасяне на глас и аудио-информация по комутируеми канали със скорост 64 Kb/s (B - канали)
✓предоставяне на цифрови комутируеми канали с висока скорост на предаване (H - канали), кратна на 64 Kb/s.
✓пренасяне на данни по виртуални съединения с X.25 комутация на пакети
✓пренасяне на данни във вид на дейтаграми

•*телеуслуги* – комуникация “от абонат до абонат”. Обхващат седемте слоя на OSI модела:

✓ ISDN-телефон – повишено качество, оптимално затихване, подобрено отношение “сигнал/шум”

✓ ISDN-телетекс – за предаване на буквено-цифрова информация

✓ ISDN-телефакс – усъвършенстване на обикновения факс

Пример:

А4 – 15-20 сек – обикновен факс

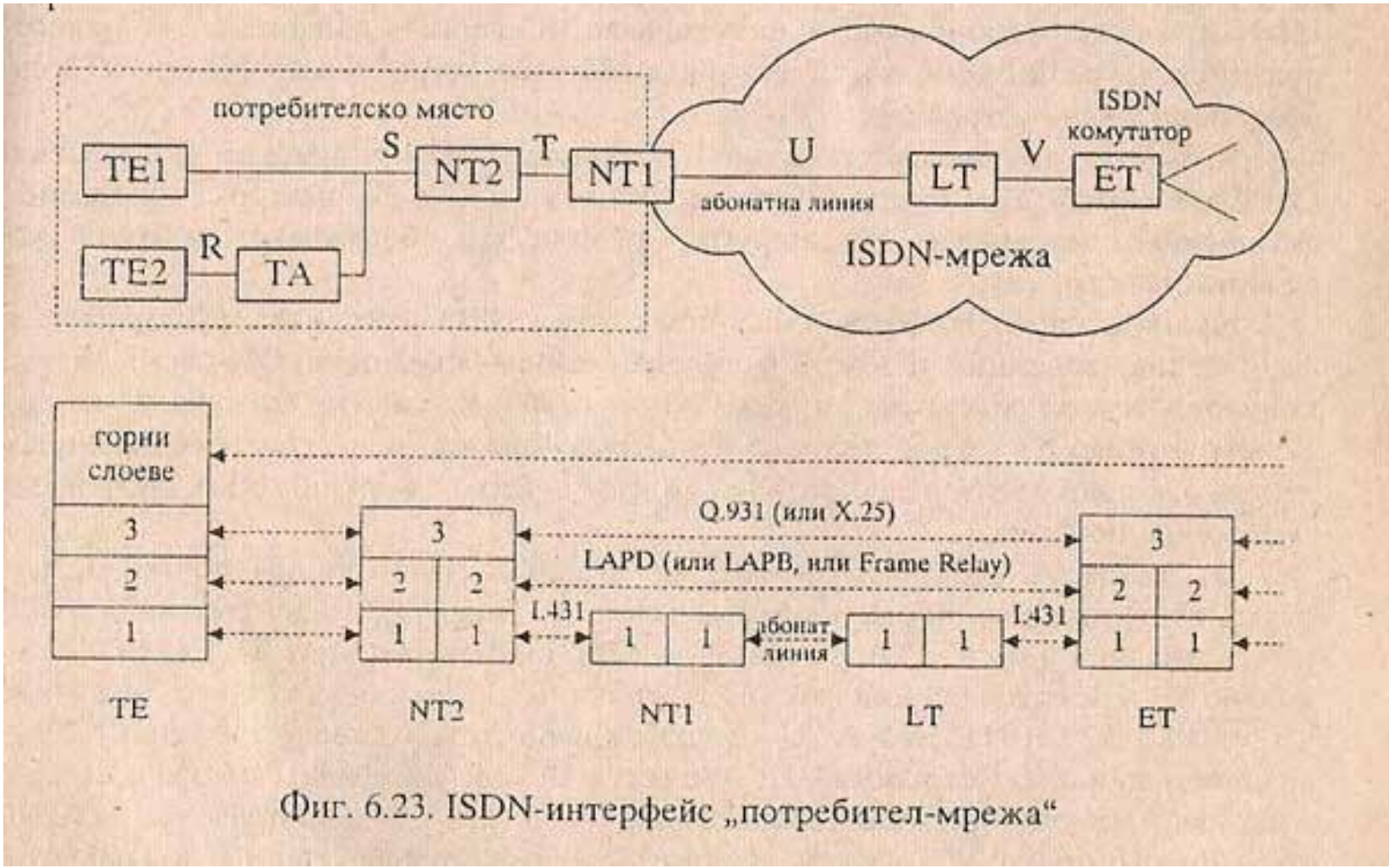
А4 – 3 сек – ISDN

✓ ISDN-видеотекс – получава се текстова и графична информация.Подобрява скоростта. Използва се за обучение в домашни условия, игри, пазаруване по каталог и доставка на място

✓ видеотелефон – глас и движещо се изображение

•*ДВУ* – допълнителни видове услуги – не съществуват самостоятелно, а като допълнение към някои от основните

- ✓ изчакване на зает абонат
- ✓ показване на номер
- ✓ прехвърляне на повикванията и т.н.



Фиг. 6.23. ISDN-интерфейс „потребител-мрежа“

Устройства:
TE – Terminal equipment - абонатни терминали
TA – Terminal Adapter – терминални адаптери
NT – Network Termination – крайни мрежови устройства
LT – Line termination – крайни линейни устройства

TE1 – специализиран абонатен терминал (ISDN телефон, цифров факс от група 4 и т.н.)

TE2 – неспециялизирани терминали (компютър, аналогов телефон, X.25 PAD) (интерфейс RS 232C/v.24)

NT2 – интелигентно устройство, работи на 3 ниво на OSI (учрежденска автоматична телефонна централа – УАТЦ; ISDN маршрутизатор за LAN) – може да липсва

NT1 – работи на физическия слой на модела OSI. Контролира се от доставчика. Формира границата на ISDN мрежата.

Може NT1 и NT2 да са обединени в едно – NT1/2

LT – работи на физическия слой на OSI модела – предаване, активиране, захранване на линията, контрол на качеството и др.

ET – изпълнява функциите на физическия, каналния и мрежовия слой на OSI, като: контрол, мултиплексиране, работа с канали и др.

ET – предимно във вид на платки, обединени в ISDN модули, монтирани към цифрова телефонна централа

В ISDN са определени контролни точки между отделните функционални компоненти (виж фиг. по-горе)

ISDN дефинира два вида абонатен интерфейс:

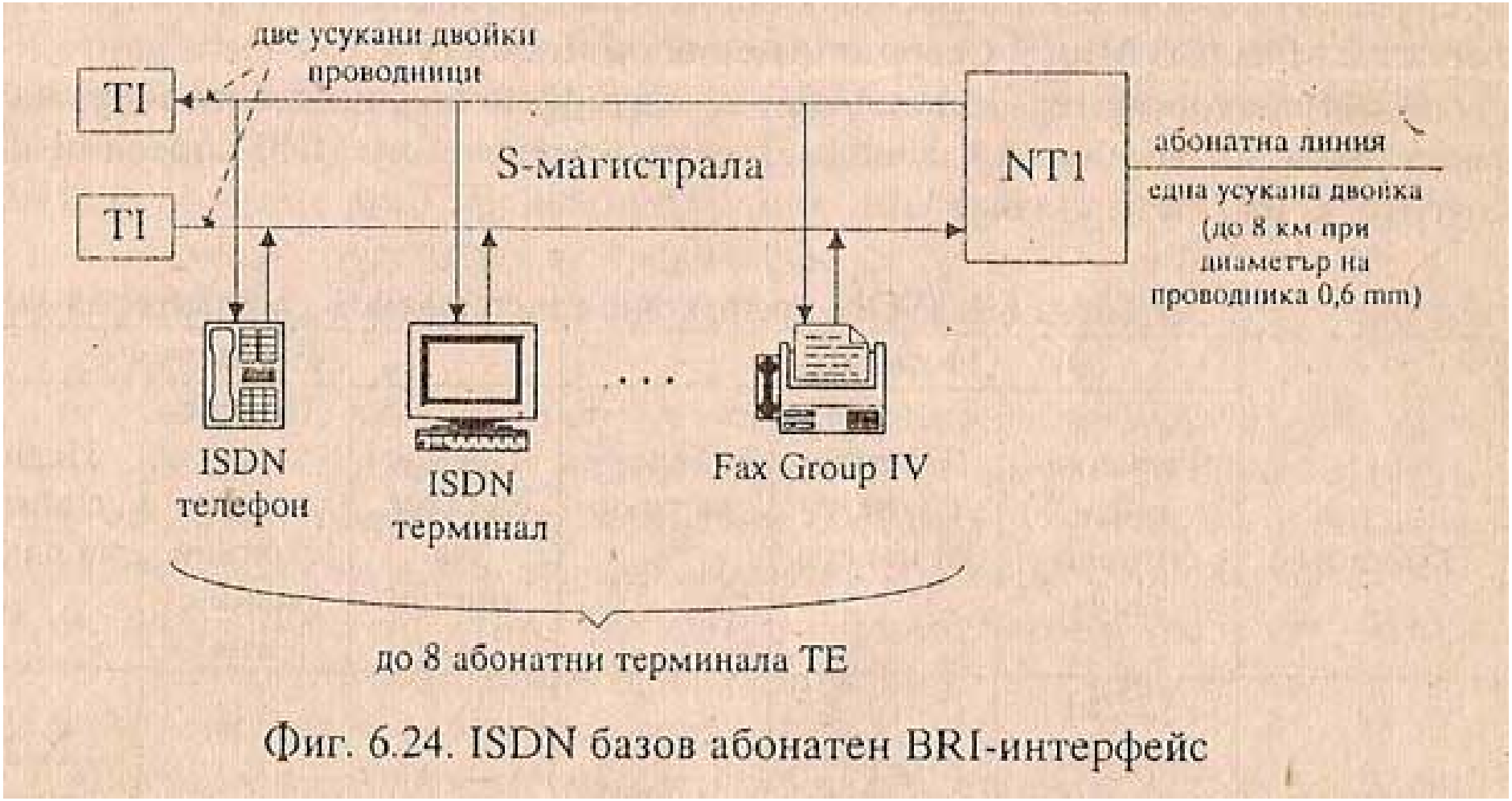
•BRI (Basic Rate Interface) – базов

•PRI (Primary Rate Interface) – първичен

BRI – още като 2B+D – предоставя на абонатите два канала от тип B (по 64 Kb/s) и един от тип D (по 16 Kb/s).

B-каналите се използват за услуги с комутация на канали.

D-каналът изпълнява главно служебни функции – по него се предават сигналите за повикването, номерата на двата абоната, извеждане на информация за номера



Фиг. 6.24. ISDN базов абонатен BRI-интерфейс

S–магистрала – общо 8 проводника (2 x 2 усукани двойки).

Всеки терминал е включен към S–магистралата с 8-проводен кабел (4 усукани двойки проводници).

PRI – още като 30B+D – предоставя 30 B-канали и един D-канал

Протоколи:

Табл. 6.4. ISDN-протоколи в интерфейса „потребител-мрежа“

OSI-слоеве ↓	D-канал			B-канал		
	Управление и сигнализация	Пренос с комут. на пакети	Телеметрия	Пренос с комут. на канали	Пренос по полупостоянни съединения	Пренос с комут. на пакети
Мрежов	Q.931 (Управление на повикването)	X.25 (пакетен слой)	за бъдещо изучаване			X.25 (пакетен слой)
Каналeн	LAPD (Q.921)			Frame Relay		LAPB
Физически	I.430 (BRI-интерфейс) + I.431 (PRI-интерфейс)					

Нов протокол за D-канала – LAPD (Link Access Protocol, D-channel)

Стандартът ISDN намира приложение за:

- достъ до интернет
- провеждане на видеоконференции
- отдалечен достъп до малка локална компютърна мрежа
- централизиран достъп до БД

Стандарт B-ISDN

B-ISDN (Broadband ISDN) – дефинира широколентов ISDN.

Предоставя услуги, изискващи скорости на предаване по-големи от тези на обикновения ISDN.

B-ISDN – поддържа скорости на предаване до 622 Mb/s.

B-ISDN – състои се от абонатно оборудване и множество междинни възли (B-ISDN централи)

Разлика с ISDN:

• оптика до абоната при B-ISDN

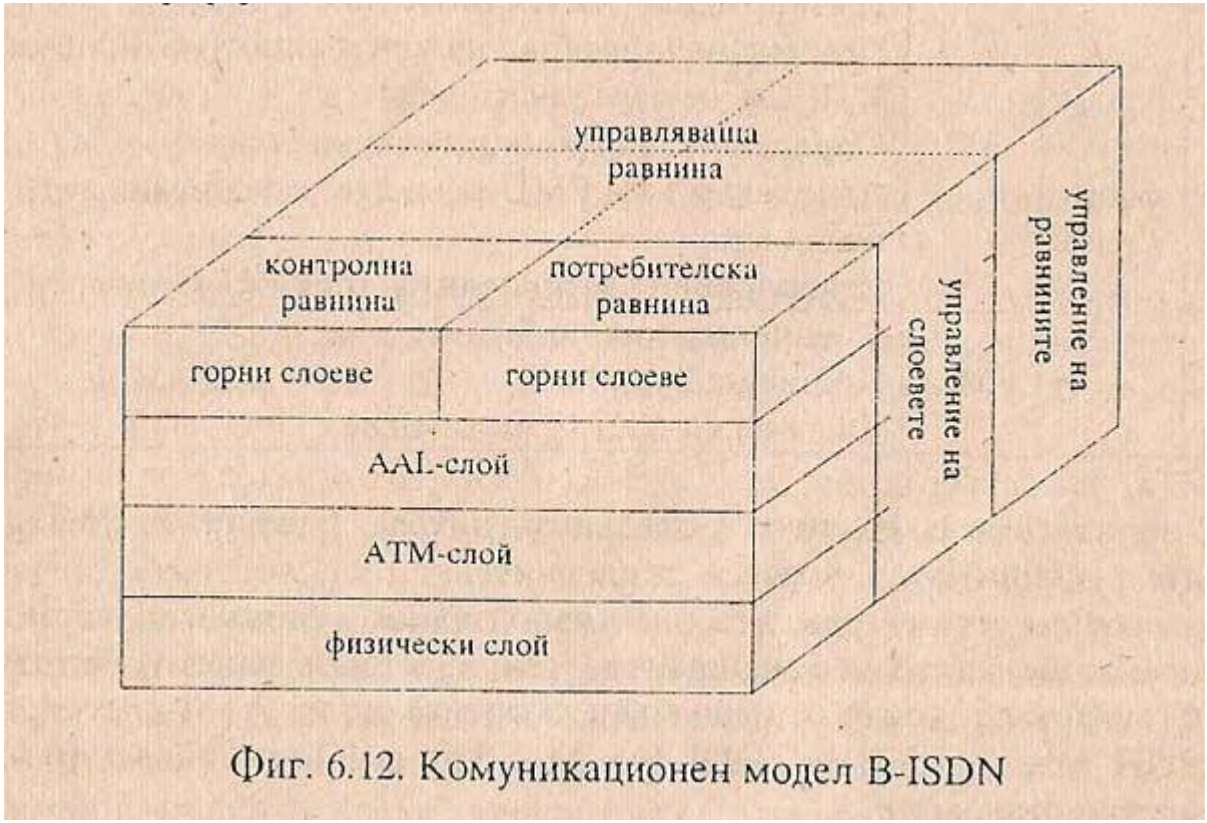
• B-ISDN се базира на ATM-мрежи и бърза комутация на пакети, докато ISDN на IDN и комутация на канали

От гледна точка на скоростта B-ISDN предлага 3 вида услуги:

1. пълнодуплексна – 155.52 Mb/s

2. асиметрична - 155.52 Mb/s от абоната към мрежата и 622.08 Mb/s - в обратна посока

3. пълнодуплексна – 622.08 Mb/s – за видеодоставчици



Фиг. 6.12. Комуникационен модел B-ISDN

ATM заема долните три слоя на модела B-ISDN

Потребителска равнина (user plane) – осигурява трансфер на потребителска информация + необходимото управление на предаването

Контролна равнина (control plane) – управление на повикването и управление на виртуалното съединение

Управляваща равнина (plane management) – функции, отнасящи се до системата като цяло (управление на равнините, управление на слоевете)

КОНКУРЕНТНИ ТЕХНОЛОГИИ

1. Аналогови модеми за комутируема връзка – използват V.90 технологията, която предоставя скорост до 56,6 Kbit/s. Ниска цена и съвместимостта им с телефонните линии.

2. ISDN и xDSL технологиите - сродни технологии по отношение използването на медни двупроводни линии, цифровото качество на услугите, ниското ниво на смущения и шумове при преноса на глас, сигурността.

ISDN - комутируема технология и изисква изграждане и разпадане на връзката (тарифиране на услугата по време); ISDN модемите се нуждаят от допълнително токозахранване и за телефонните услуги;

xDSL – достъпът е "от пункт до пункт" с постоянно активна връзка (тарифирането обикновено зависи от заявената модемна скорост); при липса на захранването преноса на данни се преустановява, телефонната линия-използваема

3. Кабелни модеми - високоскоростен Интернет достъп по кабелни телевизионни линии.

Кабелни модеми – предимно споделен достъп

xDSL – достъп заделен лично за абоната

xDSL технологии

HDSL(High-bit-rate Digital Subscriber Line) - симетрична технология, адресирана по-скоро към бизнес приложения (в момента се предлага от БТК под формата на цифрова наета линия). Тя е по-добър метод за осигуряване на T1 или E1 услуги по медни двупроводни кабели (усукана двойка). Тя използва по-малка широчина на честотната лента и не изисква разполагането на усилватели. Скорост до 1,544 Mbit/s или 2,048 Mbit/s по абонатни линии с дължина до около 3,6 км. При използването на усилватели, тази дължина може да бъде увеличена.

HDSL II (High-bit-rate Digital Subscriber Line II) - същите възможности като HDSL, но по един меден чифт, т.е. двупроводна линия.

SDSL (S-HDSL) (Single-line Digital Subscriber Line) - технология за симетричен пренос, работеща при същите скорости като HDSL

IDSL (ISDN Digital Subscriber Line) - хибрид между xDSL и ISDN технологиите; предоставя скорост до 144 Kbit/s в двете посоки

ADSL - пренася асиметричен поток информация, с много по-голяма скорост от централата на мрежовия оператор към абоната и много по-малка в обратна посока към мрежата. Модеми - от минимум 1,544/2,048 Mbit/s към абоната и 16 Kbit/s към мрежата до дори 10 Mbit/s към абоната и 768 Kbit/s към мрежата. Използва се splitter за разделянето на гласа от данните (използват различни честотни ленти)

RADSL (Rate-Adaptive Digital Subscriber Line) – поддържа ADSL скорости на предаване, но предлага допълнително възможност за динамично адаптиране на скоростта към качеството на абонатната линия (функция на модемите).

ADSL Light (Assymetric Digital Subscriber Line Light) - асиметрична xDSL технология, която е насочена предимно към домашните абонати, тъй като поддържа максимална скорост 1,544 Mbit/s към абоната и 512 Kbit/s обратно към мрежата. При нея не е необходим splitter.

VDSL Light (Very high-bit-rate Digital Subscriber Line Light) – в момента VDSL е разработвана само във варианти, адресирани към ATM мрежи с комутация на клетки

Цифровите преносни системи се делят на две големи групи:

• PDH-системи (Plesiochronous Digital Hierarchy) – по-стария вид

•SDH-системи (Synchronous Digital Hierarchy) – по-новия вид

В Европа PDH (5 степени):

• E1 – при нея в един групов канал (2.048 Mb/s) са мултиплексирани 30 телефонни канала (с използване на времеделение)
•E2 – при нея в един групов канал (8.448 Mb/s) са мултиплексирани 120 телефонни канала
•E3 – при нея в един групов канал (34.368 Mb/s) са мултиплексирани 480 телефонни канала
•E4 – при нея в един групов канал (139.264 Mb/s) са мултиплексирани 1920 телефонни канала

•E5 – при нея в един групов канал (565.148 Mb/s) са мултиплексирани 7680 телефонни канала

В САЩ и Канада PDH (4 степени):

• T1 – при нея в един групов канал (1.544 Mb/s) са мултиплексирани 24 телефонни канала
• T2 – при нея в един групов канал (6.312 Mb/s) са мултиплексирани 96 телефонни канала
• T3 – при нея в един групов канал (44.736 Mb/s) са мултиплексирани 672 телефонни канала
• T4 – при нея в един групов канал (274.176 Mb/s) са мултиплексирани 4032 телефонни канала

Взаимодействието между PDH-системите на Европа и Северна Америка – по трансатлантически подводни кабели със скорост 139.264 Mb/s чрез специално преобразуване на E4 в три T3 сигнала.

SDH-системите (SONET) имат 3 степени:

- STM1 – при нея в един групов канал (155.52 Mb/s) са мултиплексирани 1920 телефонни канала
- STM4 – при нея в един групов канал (622.08 Mb/s) са мултиплексирани 7680 телефонни канала
- STM16 – при нея в един групов канал (2488.32 Mb/s) са мултиплексирани 30720 телефонни канала

Горни слоеве в LAN. Мрежови операционни системи

Горните слоеве на LAN се реализират софтуерно от мрежовата операционна система (МОС). Горни слове – от мрежовия слой нагоре. Най-елементарно казано МОС – операционна система на отделен компютър, която му дава възможност да работи в мрежа с други компютри. В по-широк смисъл – съвкупността от операционни системи на отделните компютри, които взаимодействат помежду си по единни правила (протоколи) с цел обмяна на съобщения и поделяне на ресурси.

МОС на компютъра:

ЛОС – представлява средствата за управление на локалните ресурси на компютъра /управлението на процесите и разпределяне на операционните системи между тях, управление на многопроцесорни компютърни системи/.

Сървърна част – представя собствените ресурси на компютъра за общо ползване от страна на останалите компютри в мрежата.

Функции:

- заключване на файлове и записи при използване от различни процеси /чрез семафори, монитори и др./
- поддържане на директории с имената на мрежовите ресурси
- обслужване на заявки за отдалечен достъп към локалните файлови система или база данни
- управление на опашките на заявките на отдалечени потребители към локалните входно-изходни устройства

Клиентска част – осигурява средства за достъп до отдалечени ресурси и тяхното използване.

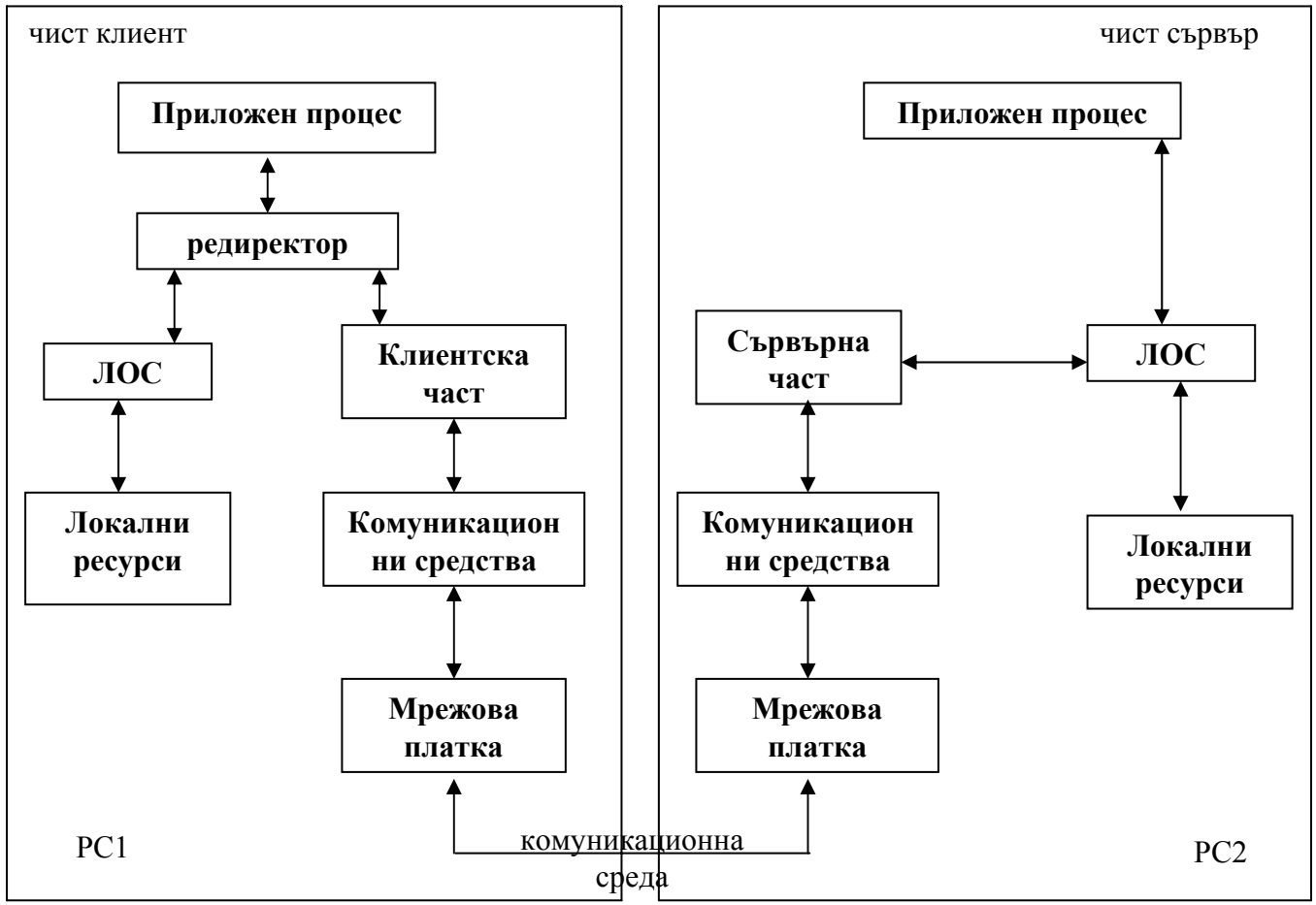
Редиректор – част от клиентския модул, която прихваща, анализира, пренасочва заявките, постъпващи от приложните процеси на компютъра клиент. Съвкупността от функции, чрез които приложните процеси се обръщат към редиректора, се нарича приложен интерфейс (API) на редиректора. Редиректорът има различни имена за различните фирми производители на МОС: *Redirector – Microsoft; LAN Requester – IBM.*

При постъпване на заявка от приложен процес за локален ресурс на дадения компютър, то тя се пренасочва от редиректора към локалната операционна система на компютъра, която я обработва по-нататък.

При заявка за отдалечен ресурс, тя се насочва от редиректора към клиентската част на МОС, която я преобразува от локална форма в мрежова форма. По този начин се постига прозрачност, т.е. изпълнението на заявки за локални и отдалечени ресурси е едно и също за приложните процеси.

Комуникационни средства – чрез тях се извършва обмяната на съобщения в мрежата. По принцип, това не са програмни модули, разпределени по комуникационните слоеве на протоколния стек, използван от дадената операционна система, и изпълняват функции като: адресиране и буфериране на съобщенията, избор на маршрута за предаване по мрежата, осигуряване на надеждност на предаването

В зависимост от функциите, които изпълнява даден компютър, в неговата МОС може да отсъства или клиентската част, или сървърната част, или да присъстват и двете.



В практиката същетвуват два подхода за създаване на мрежова операционна система:

- при първия подход мрежовата операционна система представлява съвкупност от съществуващата ЛОС /има минимални мрежови възможности/ и надстроената около нея мрежова обвивка, която изпълнява основните мрежови функции. Такъв подход използват следните МОС: LAN Manager (над OS/2), Personal Ware (над DOS7), клиентската част на мрежовата операционна система NetWare.

- при вторият подход мрежовата операционна система представлява операционна система с мрежови функции, вградени в нейните основни модули. Този подход се използва от – Widows NT Workstation, Windows NT Server, сървърната част на МОС NetWare.

В зависимост от това как са разпределени функциите между компютрите на локалната мрежа, мрежовите операционни системи се делят на два класа:

- *МОС с равноправен достъп (peer-to-peer)*
- *МОС с отделни сървъри (dedicated servers)*

Ако изпълнението на определени сървърни функции е основното предназначение на даден компютър, то той се нарича отделен сървър. На такива сървъри се инсталира операционна система, която е оптимизирана за изпълнение на дадените сървърни функции. Такива МОС са: Windows NT, NetWare и др.

Прието е отдалеченият сървър да не се използва за изпълнение на други задачи, несвързани с неговото основно предназначение, за да не се намалява производителността му. Обикновено за отделните компютри се използват най-мощните компютри в мрежата.

При МОС с равноправен достъп всички компютри са равноправни по отношение на предоставянето и използването на мрежови ресурси. Всеки компютър може да се настори, като "клиент", "сървър" или и двете. За всички компютри в такава мрежа се използва една и съща операционна система – LANtastic, Windows 95/98 и т.н. Използват се при малки групи /до 10 потребителя/, с ниска защита на информацията.

Междумрежови комуникации

Основен проблем, възникващ при междумрежовите комуникации – съгласуването на хетерогенни мрежи.

Ако съществуваше само един протоколен стек, крайните възли щяха да се разбират помежду си и нямаше да съществува този проблем. На практика съществяват няколко протоколни стека, които са широко използвани – напр. TCP/IP, NetWare на Novell. Общи протоколи в тези стекове се използват само в най-долните слоеве /физически и канален/. Това са международните стандарти 802.3, 802.4, 802.5.

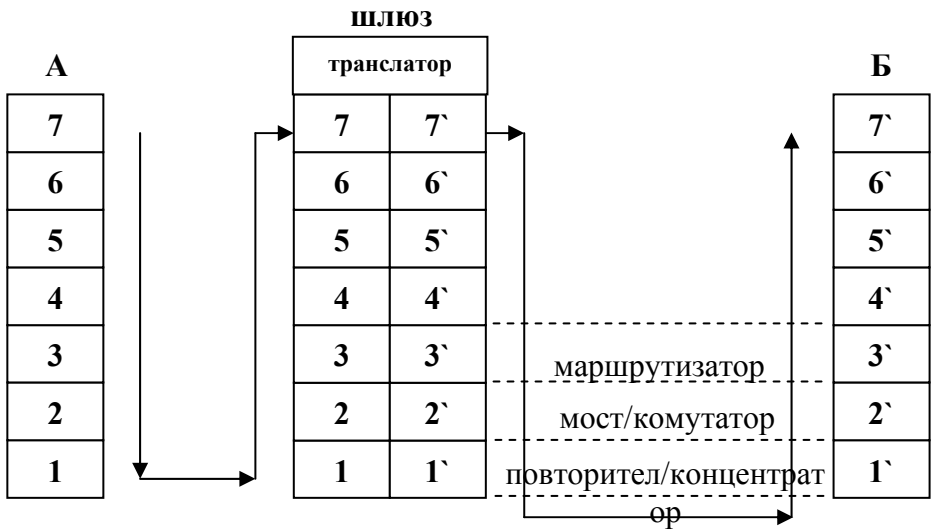
При разглеждането на въпроса за междумрежовите комуникации обръщаме внимание на два типа съгласуване:

- съгласуване на мрежите на нивото на долните слоеве на OSI
- съгласуване на горните слоеве на стековете на комуникационните протоколи, реализирани от операционните системи на крайните възли. Съществуват две главни решения:
- чрез транслация на протоколите – извършвано от отделно устройство, наречено шлюз
- чрез мултипрексиране на проток в крайните възли

Устройства за междумрежови комуникации

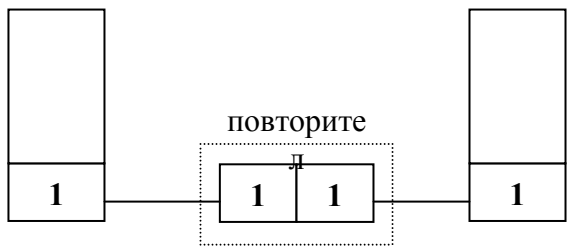
Съгласуването на две мрежи, използващи в горните слоеве еднакви протоколи и различни в долните, се извършва с помощта на допълнителни устройства поставени между тях.

Обща схема:



Повторител (Repeater)

- за възстановяване и усилване на сигнала
- удължава покривното разстояние
- съгласуваност между сегментите във физическия слой.



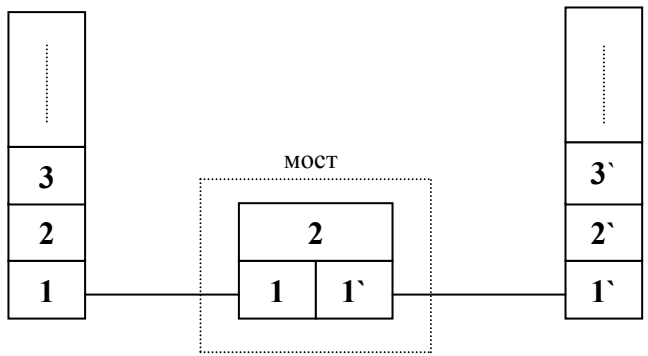
Концентратори (hubs) – осигуряват възможност за лесно включване на допълнителни възли в локалната компютърна мрежа.

Два типа концентратори:

- *пасивни* – само разделят сигналите за включване на допълнителни мрежови възли
- *активни* – допълнително усилват сигнала с цел компенсиране на тяхното затихване при удължаване на кабелните линии. Могат да се разглеждат допълнително като множество повторители.

Концентраторите имат фиксирани брой портове: 4, 8, 12, 16, 24. Действат на физическото ниво на OSI модела. Могат да се свързат йерархично.

Мостове (bridges) – работят в първия и втория слой на OSI модела. Състои се от хардуерни и/или софтуерни продукти



Основно предназначение – препредаване и филтриране на кадрите, използвайки указаните в тях MAC адреси на възлите получатели. Използват се най-често за сегментиране на големи и претоварени локални мрежи на по-малки мрежи.

В зависимост от разстоянието, на което са отдалечени двете локални мрежи, мостовете биват два вида:

- локални мостове – за свързване на LAN на близки разстояния.

- отдалечени мостове – за свързване на LAN на големи разстояния /най-често чрез наета линия/ и модеми. Много от модемите за наети линии се доставят с допълнителен модул – отдалечен мост.

- отдалечени мостове – за свързване на LAN на големи разстояния /най-често чрез наета линия/ и модеми. Много от модемите за наети линии се доставят с допълнителен модул – отдалечен мост.

В зависимост от това на нивото на кой подслой на каналния слой (MAC или LLC), те се делят на два вида:

- **MAC мостове** – използват се за свързване на еднотипни локални мрежи с еднакъв формат на кадрите.

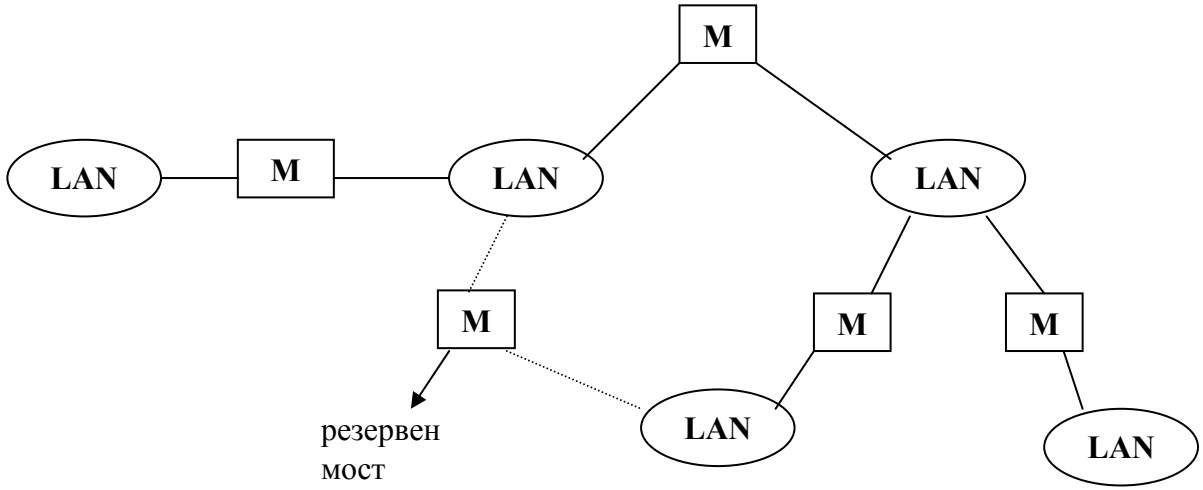
Пример: 802.3 – 802.3; 802.5 – 802.5

- **LLC мостове** – използват се за свързване на различни типове локални мрежи с различен формат на кадъра.

Пример: 802.3 – 802.5

Деление на MAC-мостовете:

- *Интервални мостове* – още “обучени” мостове, защото научават MAC-адресите на свързаните към тях крайни мрежови възли чрез самообучение на базата на преминаващите през тях кадри. Мрежите се конфигурират /софтуерно/ в дървовидна топология по такъв начин, че да има само един път между съседните мрежи. Може да има и резервни връзки, които се използват само при повреда на основните.

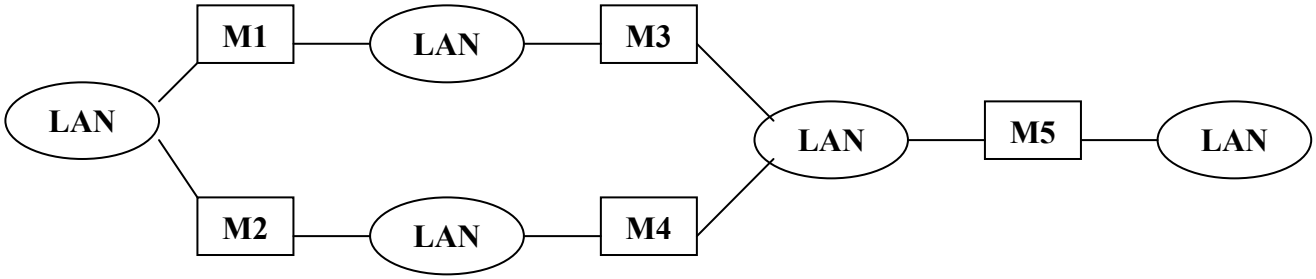


Ако мостът разполага с информация за съществуването на получателя, той препредава кадъра към него; ако пък получателят му е неизвестен мостът “разпръсква” кадъра към всички останали свои портове.

Интервалните мостове не се интересуват от точния маршрут на преминаване на кадрите, а само от номера на порта си, към който да пренасочат конкретния кадър.

- *Мостове, маршрутизиращи от източника* – използват се за свързване на 802.5 локални мрежи. Всяка от локалните мрежи Token Ring се означава с определен номер.

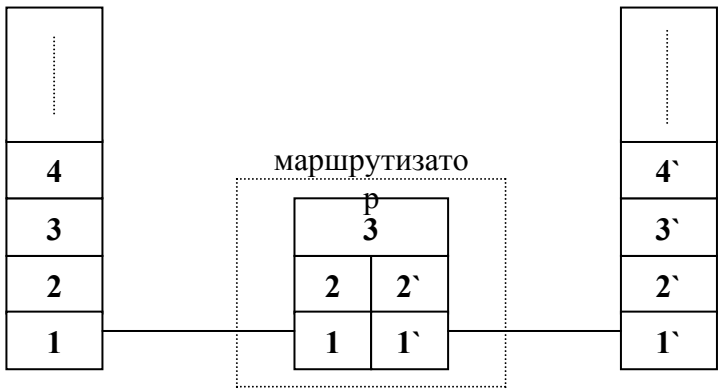
Всеки краен възел, готов да изпрати съобщение до друг краен възел-получател, предава общодостъпен кадър “до всички”, като чака отговор за маршрута до възела получател. Всеки мост добавя към този кадър номера на локалната мрежа. В зависимост от конфигурацията на интермрежата е възможно до крайния възел-получател да пристигнат няколко различни копия на такъв разузнавателен кадър. Взема се първото копие пристигнало през подателя.



Двата типа мостове по-горе са несъвместими помежду си. При смесени конфигурации се използват LLC-мостове. Мостовете (особено MAC-мостовете) обработват кадрите много бързо, тъй като не ги преформатират. Те само четат MAC-адреса на получателя и вземат решение дали да филтрират кадъра или да го препредадат.

Маршрутизатори (routers) – многопротоколни устройства, които свързат хетерогенни мрежи на нивото на мрежовия слой на OSI-модела.

Маршрутизатори се наричат и междинните възли на някои глобални компютърни мрежи, при които маршрутизиращата функция доминира над комутиращата /при IP мрежите/



Те маршрутизират пакета, откриват грешки и актуализират таблицата на мрежовите топологии, която се използва при маршрутизиране. Представляват отделен възел със собствен адрес /отнася се за всеки негов порт/. Те са по-сложни и скъпи устройства от мостовете. Могат да се реализират и софтуерно.

Основен недостатък – по-ниска скорост на обработване на пакетите.

Маршрутизаторите за разлика от мостовете изграждат "защитна преграда" за дадена мрежа срещу пакети, генерирани в друга мрежа. По този начин се намалява трафика и предпазва интермрежата от претоварване /"съобщителна буря"/.

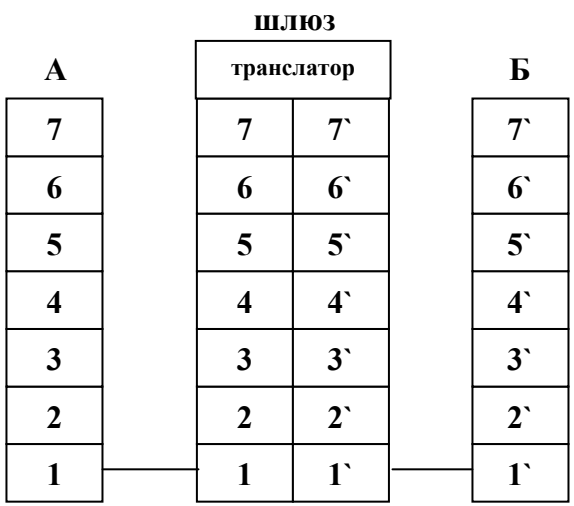
Не всички протоколи допускат маршрутизиране:

- допускат – *IPX, IP, XNS, DDP*
- не допускат – *NetBEUI (Microsoft), LAT (DEC)*

Комутатор (switches) – концентратор с възможност за комутация на кадри в каналния слой. Използва се за намаляване на вероятността от конфликти в 802.3 мрежи с интервален трафик.

Съгласуване на мрежи в горните слове

- *шлюзове (gateways)* – софтуер, инсталиран на възел-посредник между две мрежи, който осигурява съгласуване в един от горните слоеве /от транспортния до приложния слой включително/



На схемата е шлюз, функциониращ на гория слой на модела OSI, осигуряващ взаимодействието между две мрежи с напълно различни стекове на протоколите. За целта в шлюза са реализирани и двата протоколни стека с допълнителен транслатор на протоколите в най-горния слой. Шлюзовете са специализирани за връзка между два конкретни протоколни стека.

Пример:

NetWare – SNA, *SMTP – X.400* – шлюз за електронна поща.

- *мултиплексиране на протоколите* – при този вариант протоколните стекове се инсталират на всеки компютър поотделно.

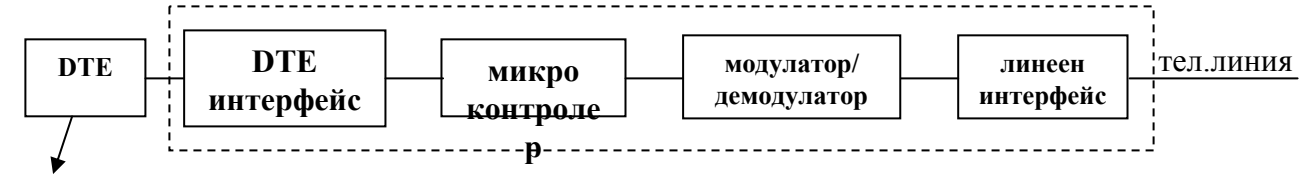
Основен недостатък – излишество на софтуер.

Модем (модулатор/демодулатор) – специализирано комуникационно устройство за предаване на данни през аналогови /най-често телефонни/ мрежи. Използват се най-често за отдалечен достъп на единични потребители до локална или глобална мрежа. Отдалечен достъп в локална мрежа се контролира от RAS-сървър (Remote Access Server), осигуряващ едновременно включване на множество отдалечени потребители към локалната мрежа.

I вариант:

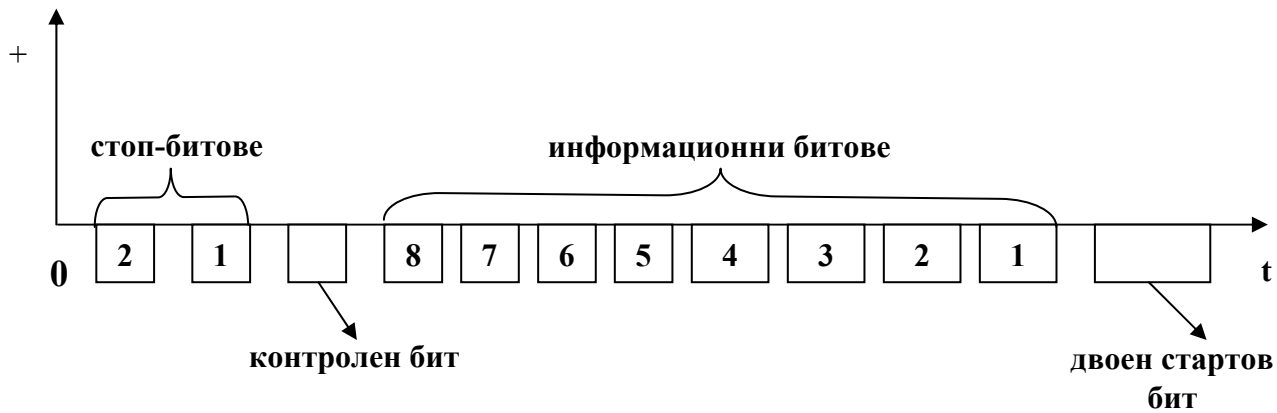
II вариант:

Устройство на модема:



DTE- интерфейс – това са средствата за свързване на модема с крайното DTE устройство. Ако модемът е външен, то той се свързва с един от серийните портове (COM 1, COM 2). Стандартът за DTE-DCE интерфейси – RS – 232C/V.24 – най-използваният. При него:

- всички битове “1” – като отрицателни импулси
- всички битове “0” – като липса на импулс
- разстоянието от модема до компютъра е ограничено до 15м
- данните се разделят на отделни блокове с дължина от 5 до 8 бита



Проверка:

проверка по четност (Е – Even parity**)** – контролният бит приема стойност единица или нула в зависимост от общия брой на двоичните единици, така че броя им + контролния бит да бъде четен. Операцията е mod2.

Резултат: при 0 – няма грешка

при 1 – има грешка /думата се повтаря отново/

проверка по нечетност (О - Odd parity**)** – както по-горе само, че резултатът е нечетен.

Резултат: при 1 – няма грешка

при 0 – има грешка, предава се отново думата

маркираща проверка (М – Mark parity**)** – контролният бит е винаги 1

разделяща проверка (S – Space parity**) –** контролният бит винаги е 0

липсваща проверка (N – No parity**)** – несъществува контролен бит

Пример:

DOS-системите – схемата 8-1-N, където 8 е броя на информационните битове; 1 – на стоп битове; N е вида на поверката. UNIX-системите – схемата е 7-1-E

Микроконтролер за подготовка на данните – анализира входещия поток от битове, компенсира го, извършва шумоустойчиво кодиране на данните. При приемане на данни микроконтролерът изпълнява същите функции в обратен ред.

Почти всички модеми имат собствени хардуерни методи за откриване и/или коригиране на грешки. Освен хардуерни методите за откриване и/или корекция могат да бъдат и софтуерни. Те са по-бавни.

Модулатор/демодулатор – преобразува цифровите сигнали, идващи от контролера, в аналогови сигнали, съвместими с телефонната мрежа. Съществуват два сигнала:

- *модулиращ цифров сигнал* – сигналът, съдържащ полезната информация /цифровият сигнал/
- *модулиран цифров сигнал*

Модулиращият цифров сигнал въздейства върху модулирания аналогов сигнал /носещ сигнал/, в резултат на което в един от неговите параметри /амплитуда, честота, фаза/ се оказва заложена полазната информация на модулиращия сигнал.

Класификация на модемите:

- *В зависимост от вида на използваните линии:*
  - модеми за комутируеми линии – използват се при по-малък трафик. Комуникационен канал се изгражда само при необходимост от комуникация.
  - модеми за арендовани линии – непрекъснато са включени към предварително прокарана линия. Модемите използват двупроводна, четирипроводна и шестпроводна линия.

  Пример:
  При четирипроводна линия – единият чифт за предаване, а другият за приемане.

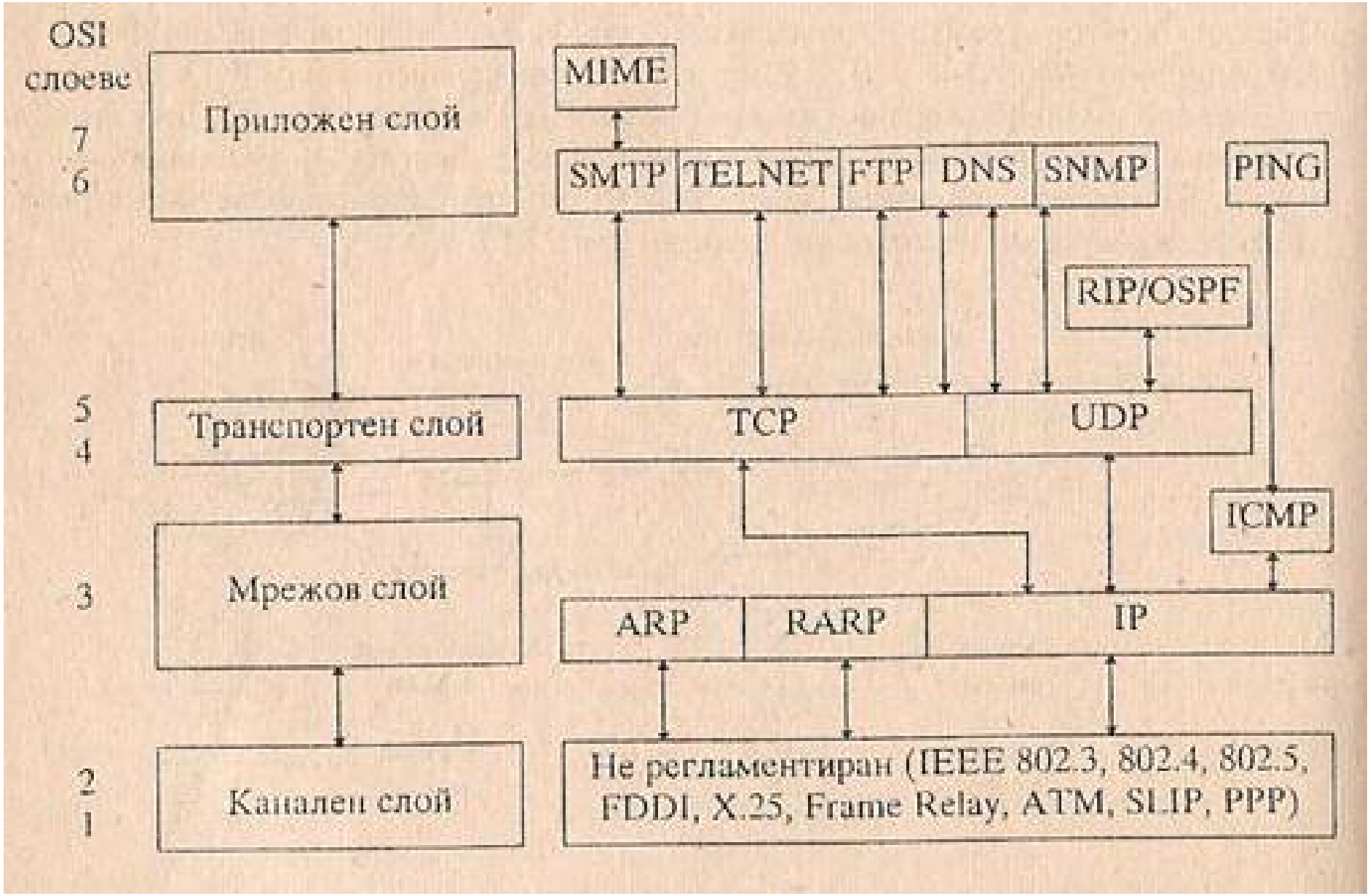
  При повреда се използва само едната двойка, която е изправна. Може да се използва и резервна комутируема линия в случай на авария или прекалено спадане на скоростта на предаване по наетата линия. Модемът автоматично превключва при нарушаване на условията на предаване.
- *В зависимост от режима на работа:*
  - модеми с асинхронен режим на работа – данните се разделят предварително на отделни блокове с определена дължина. Всеки блок има начало и край. Те се предават един след друг и ако има грешка в тях се повтарят.
  - модеми със синхронен режим на работа – модемите в двата края на канала са синхронизирани по време, като работят на една и съща честота и се поддържат непрекъснато в правилна фазова зависимост.
- *В зависимост от режима на предаване и приемане:*
  - пълнодуплексни – във всеки момент предават и приемат информация едновременно. Използват разделяне на честотната лента (FDM) на две отделни ленти – горна и долна. Единият предава по-горната, а другият приема по долната.
  - полудуплексни – в даден момент могат само да предават или да приемат. Алтернативно сменят двата режима на работа.
  - симплексни – конфигурирани са или само за предаване или само за приемане. Използват се за предаване на информация от датчици към централа.

- *В зависимост от режима на предаване и приемане:*
  - пълнодуплексни – във всеки момент предават и приемат информация едновременно. Използват разделяне на честотната лента (FDM) на две отделни ленти – горна и долна. Единият предава по-горната, а другият приема по долната.
  - полудуплексни – в даден момент могат само да предават или да приемат. Алтернативно сменят двата режима на работа.
  - симплексни – конфигурирани са или само за предаване или само за приемане. Използват се за предаване на информация от датчици към централа.
- *В зависимост от разположението на модемите:*
  - външни – отделно устройство, включено към един от серийните портове на компютъра.
  - вътрешни – поставят се в слот на компютъра.
- *По начина на свързване на модемите:*
  - модеми с модулно свързване – чрез RJ-11 конектор

Скоростта, с която модемът може да предава информация, се измерва с единицата “бит в секунда”. Това е информационната скорост. Тя е скоростта на предаване на информационните битове на модулация /цифров/ сигнал. Скоростта на модулация се измерва в бодове.

Комуникационен модел TCP/IP. Световна компютърна мрежа Internet

TCP/IP (*Transmission Control Protocol/Internet Protocol*) е комуникационен модел, разработен по инициатива на Министерството на отбраната на САЩ преди повече от 20 години, като набор от общи протоколи за разнородна изчислителна среда, по-специално за мрежата ARPA. ARPA е била глобална военна мрежа с пакетна комутация и динамична маршрутизация, разработена за поддържане на военното командване на САЩ при противников ядрен удар. При нея връзката между два компютъра се осъществявала по протокола IP, който и днес е един от основните протоколи на модела TCP/IP. След разрастването на ARPA, през 1983 г. тя е разделена на два сегмента: MILNET (мрежа, обединяваща военните сайтове) и ARPANET (гражданска мрежа). В началото на 80-те години ARPA се превръща в гръбнак на зараждащата се мрежа Internet.


OSI
слоеве
7
6
5
4
3
2
1
Приложен слой
Транспортен слой
Мрежов слой
Канален слой
MIME
SMTP
TELNET
FTP
DNS
SNMP
PING
RIP/OSPF
TCP
UDP
ICMP
ARP
RARP
IP
Не регламентиран (IEEE 802.3, 802.4, 802.5,
FDDI, X.25, Frame Relay, ATM, SLIP, PPP)

През юли 1986 г. се създава нова мрежа NSFNET, която постепенно се превръща в новия гръбнак на Internet. Мрежата ARPA официално прекратява съществуването си през 1990 г. ARPA изиграва ролята на опитен полигон за усъвършенстване на протоколите на модела TCP/IP.

Най-голям принос в развитието на модела TCP/IP има университета в Бъркли, който вгражда протоколите на модела в своя версия (BSD) на операционната система UNIX. Широкото разпространение на UNIX довежда и до широко разпространение на протоколите от модела, и като резултат, до възникване на световната компютърна мрежа Internet, функционираща на базата на комуникационния модел TCP/IP. Internet представлява колекция от множество йерархично подредени мрежи.

В горната част на тази йерархия се намират няколко опорни мрежи (гръбнака), по една за Северна Америка, Европа и Азия. Те се състоят от високоскоростни линии и бързи маршрутизатори. Към опорните мрежи са свързани мрежите (национални или щатски) от средно ниво на йерархията, а към тях са свързани мрежите от долното ниво – локални мрежи на университети, фирми, организации и доставчици на Internet. В някои случаи локалните мрежи (например, на Internet-доставчици) са свързани директно към някоя от опорните мрежи чрез нает сателитен канал.

Протоколния стек TCP/IP служи за основа и при създаването на Internet-корпоративна мрежа, използваща транспортни услуги на Internet и хипертекстовата технология WWW. Днес TCP/IP се поддържа стандартно от всички модерни операционни системи (UNIX, Windows NT, Windows 98, NetWare и др.).

Адресация в модела TCP/IP

В модела TCP/IP се използват 4 вида адреси /колкото са слоевете на модела/.

- **локален адрес**

Този адрес се използва в каналния слой. Определя се от технологията на мрежата, в която се намира съответния хост. За LAN това е MAC-адресът на мрежовия адаптер на хост или на порта на IP-маршрутизатор, например 10-B1-06-2C-E1-11 (6 байта). MAC-адресите се назначават от фирмата-производителка на мрежовия адептер и са уникални. Старшите 3 байта представляват идентификатор на фирмата-производителка, а младшите 3 байта – се назначават уникално от самата фирма.

Локалните адреси на възлите на глобални мрежи WAN (X.25, Frame Relay, ATM) се назначават от администраторите на глобалната мрежа.

- IP-адрес

Този вид адреси се използва в мрежовия слой. IP-адресът е уникален (неповторим) и представлява адрес на компютър-краен възел (хост) или на порт на междинен възел (IP-маршрутизатор). IP-адресите се назначават от администраторите на мрежи при конфигуриране на техните компютри и маршрутизатори. Всеки IP-адрес се състои от две части: *адрес на мрежата* (Net ID) и *адрес на хоста* (Host ID). Адресът на мрежата може да бъде избран от администратора произволно, или да му бъде даден от специален център (INTERNIC – за Северна Америка, RIPE NCC – за Европа, AP-NIC – за Азия) на Internet в САЩ, за да може мрежата да работи като съставна част на Internet. -IP-адресът на хоста е независим от локалния му адрес. Делението на IP-адреса на Net ID и Host ID е гъвкаво, като границата между тях може да се разполага напълно произволно с помощта на т.нар. "подмрежова маска" (subnetwork mask).

Даден възел може да влиза в състава на няколко IP-мрежи. Тогава той трябва да има и съответния брой IP-адреси. По този начин, IP- адресът характеризира мрежово съединение, а не отделен компютър или маршрутизатор.

В протокола IP съществуват няколко съглашения за специални адреси (тип broadcast и loopback). Ако Host ID или Net ID на даден IP-адрес са съставени само от двоични нули, то това се използва за означаване на самия хост или самата мрежа, а ако са съставени само от двоични единици – за broadcast-предаване.

Пример:

- ако целият IP-адрес се състои само от двоични нули, то той указва хоста, който е генерирал дадения пакет;

- ако само Net ID от IP-адреса на хоста-получател се състои от двоични нули, то хостът-получател се намира в една и съща подмрежа с поста-подател;

- ако целият IP-адрес на хоста-получател се състои от двоични единици, то той указва, че дадената IP-дейтаграма е предназначена за всички хостове, намиращи се в подмрежата на хоста-подател. Това предаване се нарича ограничено общодостъпно предаване "до всички" (limited broadcast);

- ако само Host ID от IP-адреса на хоста-получател се състои от двоични единици, това означава, че дадената IP-дейтаграма е предназначена за всички хостове на подмрежата с посочения Net ID. Това е т.нар. общодостъпно предаване “до всички” (broadcast);

- ако само Host ID от IP-адреса на хоста-получател се състои от двоични нули, то IP-адресът указва подмрежата със зададения Net ID.

IP-адресът 127.0.0.1 се използва за loopback-тестване на протоколния стек TCP/IP, реализиран в дадения хост.

IP-адресите са 4 байтови и се записват с 4 десетични числа, разделени с точки (например, 192.168.2.100). Съществуват 5 класа IP-адреси /по четвъртата версия на протокола IP – IPv.4/

Class A

Първият байт на тези адреси започва с двоична нула, т.е. IP-адресите от клас А започват с десетично число от 1 до 126 включително. Адресът на мрежата (Net ID) заема един байт, а останалите три байта представляват адрес на хост (Host ID) в нея. Този клас адреси се използва за големи мрежи /мрежи на големи доставчици на услуги/ с много крайни възли /например, адресите, започващи с 9, са на фирмата IBM, а адресите, започващи с 12 – на фирмата AT&T/. Десетичната нула не се използва като първо число на IP-адрес, а IP- адрес, започващ с числото 127, се използва само за специални цели /например, адрес 127.0.0.1 се използва за организиране на обратна връзка /loopback/ за тестване на работата на TCP/IP-софтуера на дадения възел, без реално да се изпращат пакети в мрежата, т.е. генерираните от възела данни се предават обратно към горните слоеве все едно, че току-що са приети от мрежата/;

Class B

Първият байт на тези адреси започва с двоичната комбинация 10, т.е. IP-адресите от клас B започват с десетично число от 128 до 191 включително. Този клас адреси се използва за мрежи със среден размер, като тези на големите западни университети и компании (например, FORD). Адресите на мрежата (Net ID) и хоста (Host ID) заемат по два байта

class B network to contain 2^{16} or *65,536* addresses.

The number of class B networks - *16,384*.

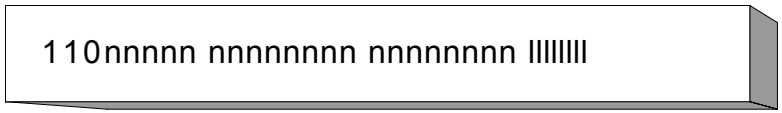
Пример:

137.55.0.0

129.33.0.0

Notice that these network numbers range between 128.0.0.0 and 191.255.0.0, the minimum and maximum numbers, respectively. And remember that the first two dotted decimal numbers are included in the network number since the network number in a class B address is 16 bits long.

Class C



Първият байт на тези адреси започва с двоичната комбинация 110, т.е. IP-адресите от клас C започват с десетично число от 192 до 223 включително. Използват се за малки локални мрежи. Адресът на мрежата (Net ID) заема три байта, а адресът на хоста (Host ID) – един байт /т.е. в една такава мрежа могат да се адресират най-много 254 хоста/;

class C network to contain 2^8 or *256* addresses.

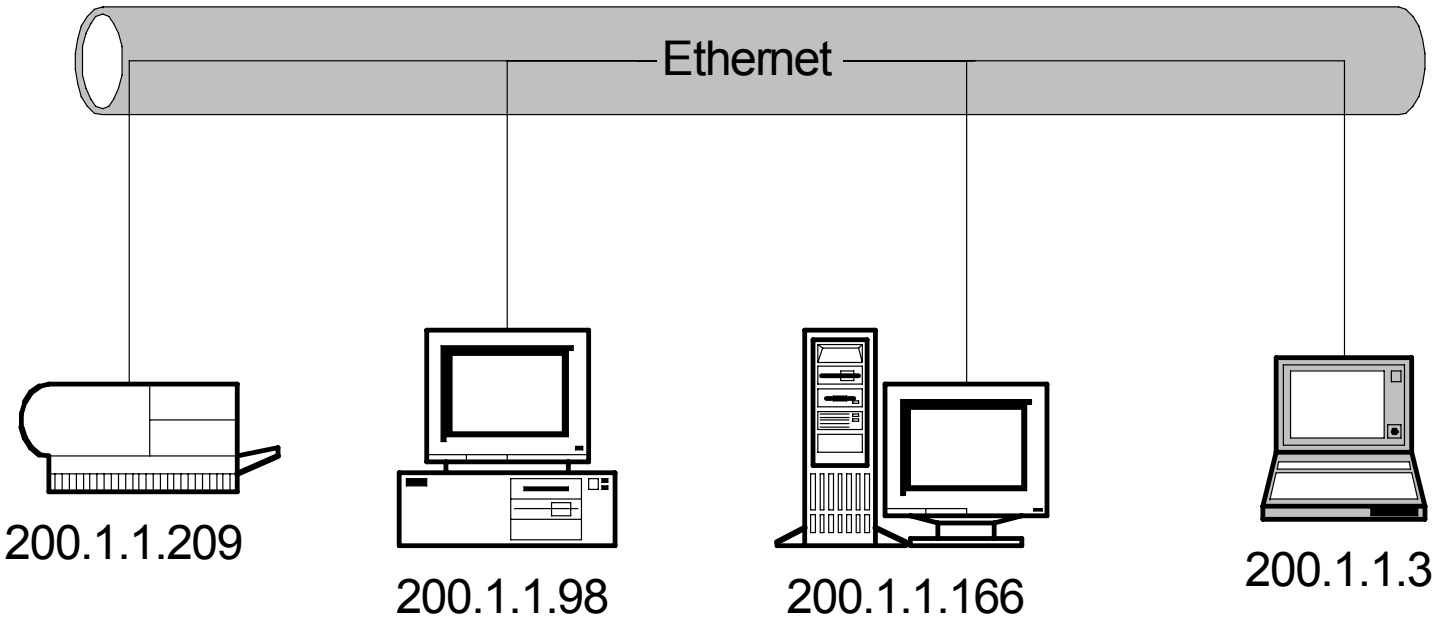
The number of class C networks - *2,097,152*.

Пример:

204.238.7.0
191.0.0.0
222.222.31.0

Notice that these network numbers range between 192.0.0.0 and 223.255.255.0, the minimum and maximum numbers, respectively. And remember that the first three dotted decimal numbers are included in the network number since the network number in a class C address is 24 bits long.

Class	Network Bits	Host Bits	Total Networks	Total Addresses
A	8	24	127	16,777,216
B	16	16	16,384	65,536
C	24	8	2,097,152	256



- клас D

Първият байт на тези адреси започва с двоичната комбинация 1110, т.е. IP-адресите от клас D започват с десетично число от 224 до 239 включително. Използват се за изпращане на multicast-съобщения до определена група хостове, на която е присвоен указаният адрес. Multicast-адресът не се дели на Net ID и Host ID;

- клас E

Първият байт на тези адреси започва с двоичната комбинация 11110, т.е. IP-адресите от клас E започват с десетично число от 240 до 254 включително. Този клас адреси е запазен за бъдещи приложения.

При IP-адресацията се използват и т.нар. “подмрежови маски”. Много често на мрежовите администратори не им достигат дадените им адреси Net ID, за да структурират мрежите си както трябва /например, за да разположат слабо взаимодействащите помежду си компютри в различни мрежи /. За разрешаването на дадения проблем администраторите могат да постъпят по два начина: 1) да получат съответно от INTERNIC, RIPE NCC или AP-NIC допълнителни адреси; 2) за да използват подмрежови маски (subnetwork mask). Маската представлява 4-байтово число, двоичния запис на което съдържа единици в битовете, които трябва да се интерпретират като мрежов адрес (Net ID), и нули – в битовете, представляващи адреса на хоста (Host ID). Например, за мрежите със стандартни IP-класове маските са следните: за клас A – 255.0.0.0, за клас B – 255.255.0.0, за клас C - 255.255.255.0. Но в маските, които се използват от администраторите, за увеличаване числото на мрежите, броят на единиците, определящи границата на Net ID, не е обезателно да е кратен на 8.

Например, нека маската е 255.255.192.0 (11111111 11111111 11000000 00000000), а адресът на мрежата е 130.168.0.0 /от клас B/. След налагане на маската върху мрежовия адрес, броят на битовете, които се интерпретират като Net ID, се увеличава от 16 на 18, т.е. администраторът придобива възможност вместо един /даден му, например, от RIPE NCC/ адрес на мрежа, да използва четири такива (130.168.0.0, 130.168.64.0, 130.168.128.0, 130.168.192.0), т.е. да организира логически четири отделни подмрежи. Тогава адресът 130.168.1400.0, който по IP-стандарта задава номер на мрежата 130.168.0.0 и номер на хоста 0.0.100.0, сега при използване на маска ще се интерпретира като: 130.168.64.0 – номер на мрежи, и 0.0.36.0 – номер на хоста в нея.

- порт

Този вид адреси се използва в транспортния слой. Портовете се използват от протоколите TCP и UDP за връзка с приложните процеси. Портът представлява 16-битово число. Някои от портовете са стандартно резервирани (например порт 21 – за протокола FTP, вж. § 8.9.3.1, порт 23 – за прокола Telnet, вж. §8.9.2), а по-неизвестните приложни протоколи използват свободно избрани номера на портове.

Портът и IP-адресът съвместно образуват сокет (socket), например: 193.68.180.5:21. Двойка сокети (един в предаващия край и един – в приемния край) еднозначно идентифицира едно TCP-съединение. Един сокет може да участвава в няколко съединиения едновременно.

- DNS-символно име

DNS-имената са имена (на хостове), които се използват в приложния слой. Въведени са за удобство на потребителите, които по принцип помнят по-добре имена, отколкото цифри (IP-адресите на хостовете). DNS-имената се назначават от мрежовите администратори. Състоят се от няколко части (домейни, области), разделени с точки, като старшият домейн се намира най-вдясно. Домейнът (domain) в Internet представлява логическо обединение на хостовете, възможно дори от различни физически мрежи. Всеки домейн се състои от поддомейни (subdomains) с цел по-лесното му администриране. Поддомейните, от своя страна, също могат да имат свои поддомейни и т.н.

Синтаксисът на DNS-имената е следния:

поддомейн_N.поддомейн_N-1. … .поддомейн_1.домейн

Пример за DSN-име е името www.fmi.uni-plovdiv.bg, което описва хоста www от домейна fmi (Факултет по математика и информатика), който е поддомейн на домейна uni-plovdiv (Пловдивски университет), който пък е поддомейн на домейна bg (България). Имената са част от разпределена база данни, наречена DSN /Domain Name System/. Тя поддържа йерархична система от имена за идентифициране на възлите и ресурсите в Internet. Основното предназначение на DNS е автоматично търсене на IP-адрес по съответното му DSN-име. За тази цел се използва протоколът DSN за приложния слой. Спецификацията на DSN се определя от документите RFC 1034 и RFC1035.