Александър Петров Милев

КОМПЮТЪРНИ МРЕЖИ И КОМУНИКАЦИИ

Учебник за дистанционно обучение

Рецензенти:
доц. д-р инж. Станимир Стоянов Станев
доц. д-р инж. Станислав Денчев Симеонов

ВЪВЕДЕНИЕ

Целта на създаване на учебника е студентите да натрупат знания по основните принципи на построение на съвременните компютърни мрежи и приетите международни стандарти за тяхното изграждане.

Учебникът е представен с два модула. Заедно те представляват въвеждащ курс, необходим при овладяване на теоретичните знания в предметната област. Той е съобразен с актуалната учебна програма по дисциплината „Компютърни мрежи и комуникации", предвидена в учебните планове на отделните специалности. Учебното съдържание се структурира в девет раздела на двата модула.

В първия модул са обосновани някои от основните понятия в комуникациите, необходими за по-лесното усвояване на изложения материал. Изяснени са някои множество елементи и параметри в компютърните комуникации. Изяснени са функциите на слоевете на отворения модел и са обосновани трите основни понятия услуга, интерфейс и протокол. Разгледани са локалните компютърни мрежи (LAN). Направена е обосновка и класификация на тези мрежи и са представени различните топологии за изграждане. Разгледани са различните стандарти за изграждане на LAN и са описани в голяма степен физическите и каналните им слоеве.

Във втория модул са разгледани глобалните компютърни мрежи (WAN). Направени са обосновка и описание на стандартите за изграждане на WAN. Представени са редица стандарти за глобални мрежи. Тук са разгледани приложените в различните стандарти методи за избор на маршрута на протоколните единици през комуникационната среда.

Разгледани са междумрежовите съгласувания на отделните слоеве на отворения модел за комуникации. Показани са различните видовете адресации в Internet и различните класове мрежи от йерархията на глобалната мрежа Internet.

Описано е действието на основните протоколи за различните нива на модела TCP/IP. Разгледани са особеностите на безжичните комуникации. Направена е обосновка на виртуалните частни мрежи, изградени в средата на Internet, както и на вируални локални мрежи и някои тяхни специфични особености. Специално внимание е обърнато на основни въпроси в сферата на сигурността на мрежите и данните .

Въпросите за самоподготовка в края на всяка глава, цитираната литература и списъка с литературни източници, може да подпомогнат читателите с по-задълбочени интереси в проблематиката. Посочените в текста търговски марки и наименования са собственост на съответните фирми и са включени само като учебни примери.

Настоящият електронен учебник по дисциплината „Компютърни мрежи и комуникации" е предназначен за дистанционно обучение на студентите от специалности „Информатика" в ШУ „Епископ Константин Преславски". Той може с успех да се използва и от студентите от Факултета по технически науки и от останалите специалности в Университета, както и от всички желаещи да се запознаят с основите на компютърните мрежи.

Разбира се, съществуват много варианти на поднасянето на подобен материал. В представения му вид в настоящия електронен вариант, той отговаря на изискванията на учебните програми за студентите по Информатика в Шуменския университет.

Структурата на учебника се определя от разбирането на автора и от практиката на преподаването на компютърните мрежи в редица водещи университети, че за изучаване на конкретни компютърни мрежи е целесъобразно първоначално да се разглеждат по-елементарни по структура примери и принципи за тяхното изграждане.

Учебникът се състои от 2 модула:

Модул 1 „Организация на компютърни мрежи".

Всеки раздел започва с основните ключови думи и съкращения в него, те са като „пътни маркери", по които студентите по-лесно ще се ориентират при усвояване и възпроизвеждане на съответната информация. В краят на всеки раздел има контролни въпроси за самопроверка на знанията.

Модул 2 „Глобални мрежи. Рутиране. Безжични мрежи. Виртуални мрежи”.

За информация се обръщайте към автора на адрес **al_milev@fmi.shu-bg.net**.

СЪДЪРЖАНИЕ НА УЧЕБНИКА ЗА ДИСТАНЦИОННО ОБУЧЕНИЕ „КОМПЮТЪРНИ МРЕЖИ И КОМУНИКАЦИИ”

Съдържание на Модул 1

Организация на компютърни мрежи

Раздели:

1. Основни понятия в комуникациите. Модели и класификация на комуникационните мрежи и системи
2. Компютърни мрежи. Устройства в компютърните мрежи. Класификация на компютърните мрежи.
3. Мрежови модели и стандарти. Отворен модел OSI.
4. Мрежови протоколен стек TCP/IP. Мрежови услуги .

Съдържание на Модул 2

Глобални мрежи. Рутиращи протоколи.

Раздели:

1. Глобални мрежи. Методи на комутация. Протоколи за глобални мрежи .
2. Рутиращи протоколи.
3. Безжични мрежи.
4. Виртуални частни мрежи. Виртуални локални мрежи
5. Сигурност в мрежите

ОСНОВНА ЛИТЕРАТУРА

1. Ганчев И., Компютърни мрежи и комуникации, Пловдив, 1999
2. Комър Брайън, TCP/IP мрежи и администриране, София, изд. „ИнфоДар” 1999
3. Милев Ал., Ръководство за лабораторни упражнения по компютърни мрежи и комуникации, Шумен, 2010
4. Нортън П., Пълно ръководство за работа с мрежи, Инфодар 1999 г.
5. Симеонов Ст., Катъров П., Съвременни компютърни комуникации – принципи и реализация. АПН, Бургас, 2001.
6. Станев С., Смит П., Захариев Ф., Компютърни системи и мрежи. Ш., 2002
7. Тужарав, Христо. Компютърни мрежи, ПИК, В. Търново, 2000
8. Хедър Остерло TCP/IP пълно ръководство, София, Изд. „СофтПрес”2002
9. Цонев И., Компютърни мрежи и комуникации, Шумен, 2008
10. Шиндър Дебора, Компютърни мрежи, София, Изд. „СофтПрес”2003

ДОПЪЛНИТЕЛНА ЛИТЕРАТУРА

1. Бакърджиева, Т. Електронен бизнес-технологии и мрежи. ВСУ „Черноризец Храбър”, 2006
2. Станев, Ст., Железов Ст. Компютърна и мрежова сигурност, Университетско издателство „Еп. К. Преславски” 2005
3. Каео, Мерике. Проектиране на мрежова сигурност. СофтПрес, 2006
4. Компютърни мрежи в лесни стъпки (колектив). СофтПрес, 2005
5. Крейг Хънт, LINUX мрежови сървъри, София, Изд. „СофтПрес” 2003
6. Начев А. И., Станков Г., Проектиране на компютърни мрежи, Камея, София, 2005.
7. Nader F. Mir, Computer And Communication Networks, Prentice Hall 2006
8. Tanenbaum Andrew S. Computer Networks 4th Ed Prentice Hall 2003
9. http://www.zapiski.info/view.php?id=153 (презентация)
10. http://dhstudio.eu/articles/wireless_bluetooth/wireless_bluetooth.doc
11. http://www.webopedia.com/
12. http://www.tuj.asenevtsi.com/CN/indexN.htm
13. http://www.phis.uni-sofia.bg/~burova

Информация:

1. Оценката от теоретичният семестриален изпит е средно аритметична от оценките от двата модула. Оценките по модулите са независими, всеки студент в рамките на изпитните сесии трябва да получи положителни 2 оценки, за да се формира обща оценка от изпита.
2. Оценката за модул 1 включва оценката от входния тест на изпита по целия материал и отговорите на два теоретични въпроса от конспекта за модул 1 на семестриалния изпит.
3. Оценката за модул 2 включва оценката от входния тест на изпита по целия материал и отговорите на два теоретични въпроса от конспекта за модул 2 на семестриалния изпит.
4. За подготовка към изпита, освен пуликуваните от автора материали, е желателно ползването на материали от Интернет, например сайта на Cisco – www.cisco.com, и на водещи университети у нас и в чужбина, които публикуват на своите сайтове различни учебни материали- лекции, упражнения и др.

На изпита студентите представят курсова работа – кратък теоретичен реферат по зададен от лектора проблем, оформена съгласно следните изисквания:

1. Разпечатана едностранно- формат А4 , обем- 6-7 страници без титулната страница, шрифт Times new Roman, височина на буквите от основния текст 12, на заглавията

14, нормален интервал между редовете . Листовете се подвързват в мека папка с машинка. Допуска се предаването им в джоб.

2. Титулната страница да е оформена съгласно изискванията във факултета- лого на университета и названието на факултета; название на катедрата- „ Компютърни системи и технологии”; тема на курсовата работа; данни за студента, разработил проекта- трите имена, специалността и факултетния номер и личен подпис; фамилията на лектора, проверил работата с място за подписа му; дата на разработването на работата.
3. Чертежите в работата се изготвят чрез Microsoft Visio, Word или се сканират.
4. На последната страница да се посочи списък на източниците (литературни и от Интернет), използвани при разработване на курсовата работа. В него те се подреждат по реда на цитирането им в работата. Техните номера в текста на работата се посочват в квадратни скоби.
5. Заедно с книжното тяло на работата се предава и **електронен носител с нейния текст.**

Съставил:.....

Доц.д-р инж. Александър Милев

Раздел 1

Основни понятия в комуникациите. Модели и класификация на комуникационните мрежи и системи

Ключови думи и съкращения

Комуникационна система	**Честотна лента**
Източник, съобщение	**Пропускателна способност**
Информация	**Шум, грешки, защита от грешки**
Комуникационна среда	**Отношение сигнал/шум**
Сигнал, аналогов и цифров	**Скорост на предаване**

1.1. Модели на комуникационни системи

Система за предаване на информация или система за свръзка или комуникационна система е съвкупност от технически средства за предаване на съобщения от източника до получателя на съобщения. За осъществяването на тази функция трябва да са налице три елемента - **източник на съобщението** и **преносна среда**, чрез която съобщението достига **приемника**. Това е най-малкият брой елементи, необходими за всеки съобщителен процес, и ако някой от тях отсъства, съобщителната връзка не може да се осъществи. Предвид на това следва да се отбележи, че думата комуникация има латински произход и значи предавам.

Системите за свръзка, предназначени за предаване на дискретни съобщения, се наричат дискретни системи или системи за предаване на дискретна информация (СПДИ). Част от СПДИ са и системите за предаване на данни. Формирането на сигналите предавани в дискретните системи за свръзка основно се извършва чрез операциите кодиране и модулация в устройството за кодиране и декодиране, модулация и демодулация.

1.1.1 Структурна схема на системите за предаване на дискретна информация.

Структурната схема на системата за предаване на дискретна информация е представена на фиг. 1.1.

Фиг. 1. 1 Структурната схема на системата на СПДИ

В качеството на източник, изработващ предназначените за предаване съобщения (ИС), могат да се използват компютри, факс-апарати, телекс-машини, телеграфни апарати, автоматизирани датчици и др. (DTE-Data Terminal Equipment).

За осъществяване на електрическо съгласуване на източника и получателя на информация с канала за свръзка и преобразуване на информация във вид удобна за последващо кодиране се използва апаратура за съгласуване (АС). Тя е съставна част на източника и получателя на информация.

От АС съобщението във вид на кодова дума постъпва в предавателя на апаратура за предаване на дискретна информация (АПДИ), (DCE-Data Communication Equipment). За да се осигури съвместна работа на ИС и ПС с различни типове АПД съединенията между тях се стандартизират.

Описанието (списъка) на веригите, сигналите и алгоритмите на взаимодействие по веригите на АПДИ са получили наименование интерфейс (DTE-DCE interface). Обменът на съобщения между УЗГ и ИС (ПС) може да се осъществи както последователно (побитно) - последователен интерфейс, така и паралелно (по байтово) - паралелен интерфейс.

Устройството за защита от грешки (УЗГ) е предназначено да защитава от грешки предаваната информация и повишава нейната достоверност. Исканата достоверност се осигурява от предаващата и приемащата апаратура за повишаване на достоверността. УЗГ се различават едно от друго при различните системи за предаване на дискретна информация. Когато не се предявяват високи изисквания към достоверността, УЗГ може и да отсъства. Тези устройства се наричат още кодери и декодери. Трябва да се отбележи, че когато източник на съобщение е компютър, същият кодира съобщението, представляващо набор от символи в двоични сигнали на първичен (информационен) код, който обикновено е без излишък. Кодерът на УЗГ в този случай е "канален кодер" и има за цел систематично

внасяне на излишък в информационните кодови комбинации, постъпващи от кодера на източника на съобщения с цел получаване на шумоустойчив код.

Последователността от импулси, образуващи кодовата дума, от изхода на УЗГ постъпва на входа на устройството за преобразуване на сигналите (УПС). То е предназначено за преобразуване на постоянно токовите импулси в модулиран сигнал и за съгласуване на параметрите, на предаващата и приемащата апаратура с параметрите на аналоговия канал.

При телеграфните канали и при канали с предаване в основната лента честоти (0 - FB) такова преобразуване не е задължително. При използуване на проводни канали с тонална честота, радиоканали, оптически канали или широколентови канали такова преобразуване е задължително.

УПС се отличават едно от друго по използвания вид модулация и скоростта на предаване. Тези устройства се наричат още модулатори, демодулатори или общо (модеми).

Съвкупността от устройствата, включваща устройства от входа на преобразуващото УЗГ до изхода на УЗГ на приемника на АПДИ образуват канал за предаване на дискретни информация (данни) (КПДИ). Той се характеризира с определена производителност, осигуряваща необходимата достоверност.

Съвкупността от паралелно функциониращи КПДИ образуват тракта за предаване на данни (ТПД). Трактът за предаване на данни е съвкупност от резервирани канали за предаване на данни, осигуряващи надеждност на предаването на данни.

Участъкът между УПС на предаващата страна и изхода на УПС на приемащата страна се нарича дискретен канал за свръзка. Той се състои от УПС и аналогов канал за свръзка.

Аналогов канал за свръзка (АКС) се нарича канал, сигналите на входа на който x(t) и на изхода му y(t) са непрекъсната функция на времето. В техническо отношение това е линията за свръзка и апаратурата за управление на канала, в това число комутатори, мултиплексори и др. Линиите за свръзка биват: проводни, оптически и радиолинии.

Проводните линии за свръзка се делят на кабелни и въздушни.

Радиолиниите за свръзка (радиоканали) биват: радиорелейни, късовълнови (КВ) канали, ултракъсовълнови канали (УКВ), радиоканали с дециметрови вълни (ДЦВ), тропосферни, космически и др.

Оптическите канали за свръзка се делят според диапазона на оптическите вълни: в диапазона на видимите оптически вълни, в инфрачервения диапазон и др.

Дискретният (цифров) канал за свръзка е предназначен за приемане и предаване на дискретни съобщения. Той се характеризира със скорост на предаване на информацията в бодове (Bd).

Две СПДИ могат да обменят данни при наличие на "общ език", а така също и общ набор от процедури и правила за ползване на езика. Наборът от правила за обмен на данни между два кореспондента (устройства, програми, хора) и съглашенията (конвенциите) по формата и семантиката на предаваните данни се нарича протокол.

Процесът на предаване на съобщенията по канала за предаване на данни се състои от няколко последователни етапа. Източникът на съобщение изработва данните, имащи завършен вид като дейтаграми, телеграми и т.н.. Елементите на дискретното съобщение(цифри, знаци, символи) се преобразуват в УЗГ (кодер) в кодирана (с код с излишък) последователност от двоични (или М-ични) цифрови сигнали, формирани по определени правила (кодове). Тази последователност се преобразува с помощта на УПС (модулатора) в последователност от манипулирани (дискретно модулирани) сигнали, в които е осъществено изменение на параметрите на носещо сигнала трептение (звуково, радиочестотно или оптическо) в съответствие с определена модулираща функция. В канала за свръзка електрическите (оптическите, радиочестотните) сигнали се разпространяват от предавателя на АПД към приемника на АПД, като се подлагат на различни външни въздействия (смущения). Приемникът осигурява преобразуване (желателно оптимално) на сместа от сигнал и смущение в дискретно съобщение, максимално съответстващо на предаденото. При това се изпълняват редица операции по преобразуването на сигналите: филтрация, усилване, демодулация и декодиране на дискретната последователност. Приетото съобщение е съвкупност от данни, предварително неизвестни за получателя на съобщението.

1.1.2 Основни характеристики на СПДИ

Към основните качествени показатели на дискретните системи за свръзки се отнасят: достоверност, пропускателна способност и скорост за предаване, шумозащитеност, надеждност, своевременност (оперативност) и ефективност.

- **Достоверност**

Известно е, че СПДИ трябва да бъде шумоустойчива, т.е. да притежава способността да възстановява с достатъчна вероятност предаваното съобщение при приемането на сигнала, намиращ се под въздействие на смущения.

На практика непрекъснатото съобщение се счита за правилно прието, ако неговите амплитудни, честотни и фазови отклонения не превишават определени норми.

Верността на предаването на дискретни съобщения определя степента на съответствие между приетото съобщение и предаденото.

При приемане на предаваното дискретно съобщение се регистрира последователността от импулси, съставляващи кодовата дума на предаваните символи. Ако всички разряди на кодовата дума са приети правилно, то след декодирането приетото съобщение точно ще съответства на предаденото.

За оценка качеството на предаденото дискретно съобщение се използва понятието достоверност, което се определя от съотношението на правилно приетите символи към общия брой предадени символи за определен интервал от време.

На практика обаче се използва понятието загуба на достоверност, което определя отношението на неправилно приетите (сгрешени) символи $n_{гр}$ към общия брой на предадените символи $n_{общ}$ (1). С понятието загуба на достоверност се дава оценка на честотата на грешките, $\eta_{гр}$.

$$\eta_{гр} = \frac{n_{гр}}{n_{общ}} \qquad (1)$$

Ясно е, че честотата на грешките е случайна величина и зависи от продължителността на измерването и условията при провеждането на измерването. При достатъчно дълго по време измерване или многократни измервания $\eta_{гр}$ се доближава с незначителни отклонения до една средна стойност, която представлява вероятност за поява на грешка в един символ (разряд). Отчитайки това условие израза за вероятността за грешка може да се запише във вида:

$$P_{гр} = \lim_{n_{гр}\to\infty} \eta_{гр} = \lim_{n_{гр}\to\infty} \frac{n_{гр}}{n_{общ}} \qquad (2)$$

Понякога се използува и обратната величина вероятност за правилно приемане $P_{пр} = q$, която се определя като:

$$q = 1 - P_{гр} \qquad (3)$$

Между вероятността за грешка на разряд и вероятността за грешка на символ (кодова дума) има съответствие, но не е еднозначно. Втората зависи не само от първата, но и от избрания код, дължината на кодовата комбинация, разпределение на грешките в канала и др. Счита се, че за достоверно приемане на дискретна информация е допустимо вероятността за грешка по разряд (двоичен символ) да бъде в границите 10^{-6}-10^{-9}. В реалните свързочни канали и в частност например телефонните вероятността за грешка на разряд е в порядъка 10^{-3}-10^{-5}. За постигане на желаната висока достоверност по кодова дума се използуват устройства за защита от грешки

- **Пропускателна способност и скорост за предаване на дискретна информация**

Известно е, че пропускателната способност на дискретния канал е най-голямото количество информация, което може да бъде предадено от системата за единица време и се определя по формулата:

$$C_k = \nu_{max}.\left[H(X) - H\left(\frac{X}{Y}\right)\right], бит/сек \quad (4)$$

където:

- $H(X)$ - начална неопределеност, ентропия на източника на съобщение;
- $H(X/Y)$ - остатъчна неопределеност, ненадеждност на канала;
- ν_{max} -максимален брой символи, които могат да бъдат предадени по канала за единица време.

При предаване на данни по реален двоичен канал със смущения при определено отношение на мощностите на сигнала P_S и на шума P_N в него при оптимален избор на вида на модулацията максималната пропускателна способност на СПДИ съгласно Шенон е:

$$C_{max} = \Delta F.\log_2(1 - \frac{P_S}{P_N}), бит/сек \quad (5)$$

Изчисленията по тази формула за съвременни телефонни канали с лента на пропускане $\Delta F = 3100$ Hz и отношение сигнал/шум 25-35 dB теоретически определя една пропускна способност на телефонните канали от 25,000 до 40,000 bit/s. За целта следва да бъдат идеално коригирани нелинейните характеристики на канала. Това в определен смисъл показва възможности за повишаване на реалната пропускателна способност до теоретичната.

Носител на информация в СПДИ е дискретен сигнал, представляващ последователност от импулси. Ако продължителността на един единичен импулс (разряд) е $\tau_{\hat{\imath}}$, параметърът

$$\hat{A} = \frac{1}{\tau_{\hat{\imath}}}, \text{Bd} \qquad (6)$$

се нарича манипулационна скорост на предаване на символите, или скорост на манипулацията. За разлика от скоростта за предаване на информация в канала C_k, [bit/s] тази скорост се измерва в бодове [Bd], като един бод съответства на предаването на един елементарен символ за една секунда. За двоични СПДИ където в предаваното съобщение има излишък скоростта за предаване на информация е по-малка от скоростта на манипулация.

Максимално възможната скорост за предаване на елементарни символи (разряди) по канал без смущения е

$B_{max} = 2.\Delta F,$

където ΔF - широчина на честотната лента на канала за свръзка.

Скоростта на манипулация е важен параметър на дискретните системи за свръзка. Той обаче не определя обема на предаваната информация в канала за свръзка. Количеството информация, която може да бъде предадена за единица време, се определя от скоростта на предаване на данните. Скоростта за предаване на данните е броя на информационните битове предадени за 1 секунда.

Въвеждането на понятията скорост на предаване на информация и скорост на манипулация се налага, тъй като при предаване на информацията почти винаги има излишък от коригиращи, служебни и синхронни импулси, които намаляват пропускателната способност на канала, за полезната информация и $C_k < B$.

За да се оцени ефективността на използуване на канала се въвежда коефициент на използуване на канала по скорост $K_C = C_k/B$, който за съвременните СПДИ е в границите $K_C = 0{,}7 - 0{,}9$.

- **Шумозащитеност**

Под шумозащитеност на СПДИ се разбира нейната способност да изпълнява своите задачи в условията на определени смущения. Очевидно е че шумозащитеността на системата зависи от нейните технически характеристики, от взаимното разположение на

СПДИ и апаратурата за разузнаване и подавяне, от тактиката на използване на СПДИ и т.н. Съчетаването на всички тези характеристики и условия носи случаен характер и затова шумозащитеността математически се описва като случайна величина.

Ако се обозначи с $P_р$ вероятността да бъдат разузнати параметрите на системата, необходими за организация на радиопротиводействие, а с $P_н$ - вероятността да бъде нарушена работата на системата в резултат на радиопротиводействието, то вероятността Ршз системата да може да изпълнява своите задачи ще бъде:

$$P_{из} = 1 - P_р . P_н . \quad (7)$$

Способността на системата да бъде устойчива и неподатлива на атака от противодействаща система, събираща информация, се нарича скритост. Вероятността $P_р$ описва количествено скритостта на системата.

Способността на системата да изпълнява своите задачи се нарича шумоустойчивост. Очевидно е че шумоустойчивостта количествено се описва с вероятността:

$$P_{иу} = 1 - P_н . \quad (8)$$

Скритостта на една система може да бъде три вида: енергетическа, структурна и информационна (т.е. криптоустойчивост).

Енергетическата скритост се характеризира със способността системата да остане незабелязана от разузнавателните приемни устройства.

Структурната скритост характеризира способността на системата да затрудни максимално разкриването на принципите на модулация на сигнала, неговите честотни и временни параметри. Следователно за увеличаване на структурната скритост е необходимо в системата да могат да се използват голям брой сигнали, както и да е възможно достатъчно бързо да се изменя формата на сигналите.

Информационната скритост се характеризира със способността на системата да противостои на мерките, насочени към разкриване на смисъла на предаваната с помощта на сигнали информация. Информационната скритост се нарича още криптоустойчивост и представлява важен самостоятелен научен проблем.

Енергетическата скритост се описва количествено с вероятността $P_{откр}$ да бъдат открити сигналите на системата, структурната скритост се описва количествено с вероятността $P_{стр}$ да бъде разкрита структурата на сигнала, а информационната скритост -

с вероятността $P_{инф}$ да бъде дешифриран смисълът на предаваната информация. От всичко до тук се вижда, че:

$$P_р = P_{откр}.P_{стр}.P_{инф}. \quad (9)$$

Шумоустойчивостта, както и скритостта, зависи от много параметри. Вероятността $P_н$ да бъде сринато правилното изпълнение на задачите от системата, физически означава, че отношението сигнал/шум γ ще стане по-малко от някакво критично значение $\gamma_{кр}$ (характерно за дадения вид смущение), т.е.:

$$P = P(\gamma \le \gamma_{кр}). \quad (10)$$

Следователно шумозащитеността на системата зависи от съчетаването на голям брой фактори: вида и формата на смущението, неговата интензивност, формата на полезния сигнал, структурата на приемника, антената, прилаганите методи за борба със смущения и др.

- **Надеждност**

Надеждността зависи, както от техническото състояние на апаратурата за предаване на дискретна информация (апаратурна надеждност), така и от състоянието на канала за свръзка. Вследствие на действието на различни смущения предаването на дискретна информация може да е ненадеждно даже и при пълна надеждност на апаратурата за предаване.

Повишаване на надеждността на СПДИ се постига чрез резервиране на апаратурата и на каналите за свръзка и чрез редица експлоатационно-технически мероприятия. Това изисква допълнително оборудване, което усложнява и оскъпява системата.

- **Ефективност на СПДИ**

Ефективността на СПДИ се оценява от две гледни точки:

- ✓ изразходваната лента за пропускане на канала ΔF за предаване на дадено количество информация с по висока скорост и със зададена достоверност;
- ✓ осигуряване на минимален разход на енергия за предаване на информацията по канала с шумове.

Ефективността зависи основно от:

- ✓ методите за кодиране,

- ✓ типа и интензитета на смущенията,
- ✓ зададената достоверност,
- ✓ време за предаване на информацията и др.

1.2 Класификация на комуникационите системите и компютърни комуникации.

1.2.1 Класификация по вида на предаваните дискретни съобщения

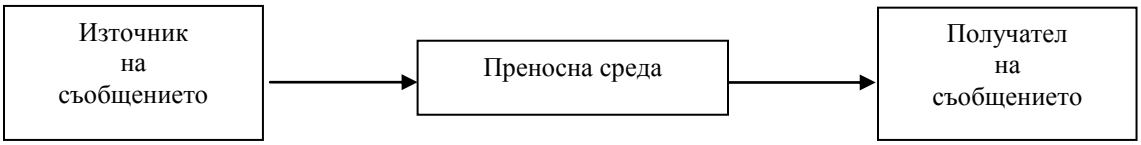
По вида на предаваните дискретни съобщения СПДИ биват:

- системи за предаване на данни (СПД) – това са СПДИ, в които кодовите думи се формират от автоматизиран източник на съобщения (ЕИМ и др.);
- системи за предаване на текст (СПТ) – това са СПДИ, в които информацията от източника постъпва във вид на m-разрядни кодови думи всяка от които съответства на определен знак от буквено-цифров текст. Към този вид СПДИ се отнасят телетекстните системи за предаване на символна информация;
- системи за предаване на изображения (СПИ) – това са СПДИ за предаване на факсимилни изображения (телефаксни системи);
- интегрирани системи (цифрови системи с интеграция на службите (услугите) – ISDN, DSL, Internet – те реализират предаване на данни, текстова информация, факсимилни изображения и др. по цифрови канали.

1.2.2 Класификация по вида на комуникационния канал

- с еднопосочно предаване (симплексни, simplex)
- с последователно двупосочно предаване (полудуплексни, half duplex)
- с едновременно двупосочно предаване (пълнодуплексни, full duplex)

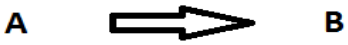
На фиг. 1.2 е показана комуникационна система в най-общ вид с трите й основни елемента.



Фиг. 1.2. Общ вид на съобщителна (комуникационна) система

Показаната на фиг. 1.2 съобщителна (комуникационна) система, всъщност осъществява така нареченото еднопосочно предаване, тъй като каналът за връзка се определя като средство за еднопосочно предаване. Той може да пренася информация в която и да е посока, но това трябва да става в различни интервали от време. Посоката на информационния поток зависи от характеристиките на устройствата във всеки край на линията.

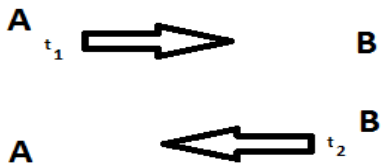
Радио- и телевизионните предавания са също примери за еднопосочно предаване (фиг 1.3). Сигналите от предавателните станции се приемат от приемниците в нашите домове. Радио и телевизионните приемници обаче не могат да предават обратно информация, тъй като не са конструирани за това, както предавателните станции не са пригодени за приемане на информация.



Фиг.1.3

Чрез използуване на подходящи устройства е възможно последователно да се променя посоката на потока от съобщения в канала, в резултат на което се получава двупосочно последователно (полудуплексно) предаване. Първоначално може А да предава към В в момент t_1. В края на съобщението системата се преобразува чрез прключване като и В може да стане предавател, а А - приемник, т.е възможно е изпращането на информация и в обратната посока - от В към А в момент t_2. Предвид на наличието на две възможности за посоката на потока от съобщения системата се нарича двупосочна комуникационна система или по-общо полудуплексна система (означава се като HDX – half duplex). Радиосигналите, които се използуват в полицейските коли и такситата, са полудуплексни. Когато шофьорът на таксито натисне бутона на микротелефона си, той

може да говори с диспечерския пункт, но не може да го чува. При отпускане на бутона той вече чува диспечерския пункт, но не може да говори с него.

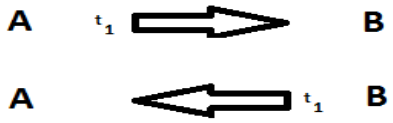


Фиг. 1.4. Полудуплексна съобщителна система

Необходимо е да се акцентира върху два основни момента, характерни за полудуплексната съобщителна система. Първо - за свързване на А и В се използват само два проводника.

Вторият момент, който следва да бъде отбелязан, е, че смяната на посоката на потока от данни заема определен, ограничен интервал от време. По-конкретно, операторите трябва да преценят колко време е необходимо, за да се опознае краят на съобщението за да превключат приемно-предавателните ключове, така че те да са готови за предаване в обратна посока. Времето за изменение на състоянието на системата е сума от времето за реакция, през което операторът разпознава края на предаването, и времето за физическо превключване на ключовете и създаване на готовност за предаване в обратна посока. Повечето съобщителни системи имат ограничено време за превключване и е необходимо да се определи неговата продължителност за всеки конкретен случай.

Чрез допълнително усложняване на схемата е възможно да се предават съобщения едновременно в двете посоки, в резултат на което се получава двупосочно едновременно (пълнодуплексно) предаване. За тази цел следва да се построи съобщителна линия с два канала, при което може да се изпраща информация и в двете посоки по едно и също време. Обикновено единият канал пренася информацията в едната посока, а другият канал - в другата посока. С други думи, ако съоръженията във всеки край на линията дават възможност за едновременно предаване и приемане, тогава системата е пригодна за едновременно предаване в двете посоки на потока от съобщения. Такава система се нарича двупосочна система или още пълнодуплексна система (означава се с FDX – full duplex). Например, двупосочните пътища представляват пълнодуплексни системи.



Фиг. 1.5. Пълнодуплексна съобщителна система

Така се получава система от вида, показан на фиг. 1.5, позволяваща едновременно предаване на данни в две (противоположни) посоки в един и същ момент от време t_1.

1.2.3 Класификация по вида на честотната лента и модулацията

- С предаване в основната лента (немодулирани) СПДИ – Тези системи използват цифрово-цифрово предаване на последователности от електрически или светлинни импулси кодирани с линеен код (например Манчестърско кодиране). Това обикновено се използва в серийните линии, кабелните локални мрежи като например Ethernet и в оптичните комуникации;
- Лентови (модулирани) СПДИ – Тези системи използват цифрово-аналогово предаване: Модулиран синусоидален сигнал представлява цифровия поток. Понякога това се счита като аналогово предаване. Сигнала се получава по различни методи за модулация като например фазова модулация (Phase-shift keying ,PSK), амплитудна квадратурна модулация (Quadrature amplitude modulation, QAM) или честотна модулация (Frequency-shift keying, FSK). Модулирането и демодулирането се осъществява от специални модеми. Този вид предаване се използва при безжичните комуникации, кабелните телевизионни мрежи и други.

1.2.4 Класификация по начина на предаване на елементарните сигнали

- със серийно (последователно) предаване – последователно предаване на елементарните сигнали от групата представляващи отделен символ или някакво множество от символи. При цифровото серийно предаване битовете се предават по една линия, честота, или оптичен канал последователно. Тъй като вид предаване изисква по-малко сигнална обработка и от там по-малко възможности за грешки спрямо паралелното предаване, скоростите за предаване по всяка отделна линия могат да са доста високи. Използва се при предаване на големи разстояния;

- с паралелно предаване – едновременно се предават елементите на един символ или множество символи. Елементите на един символ се предават едновременно по две или повече линии. Използват се многопроводни линии, което позволява достигане на високи скорости за предаване на няколко бита едновременно. Този вид предаване главно се използва в компютрите, например вътрешните шини, паралелните връзки с принтери и други периферни устройства. Паралелното предаване не е надеждно за големи разстояния поради разликата в свойствата на всяка линия и някои битове пристигат с различно закъснение.

1.2.5 Класификация по способа на поддържане на синфазност

- синхронни, при които се поддържа пълна синхронност между предаващата апаратура и приемащата апаратура – При тях не се използват начални и крайни битове, а се поддържа синхронизация на тактовата честота на приемника и предавателя. Поради липсата на стар и стоп битове скоростите са малко по-високи, но пък се получават повече грешки при разсинхронизирането
- асинхронни СПДИ, при които не се поддържа синхронност между предаващата апаратура и приемащата апаратура. – При тях се използват старт и стоп битове за обозначаването на началото и края на предаването на един символ. Например един ASCII символ ще се предаде с 10 бита: Например символ A "0100 0001" ще се предаде като "1 0100 0001 0". Допълнителната единица или нула (в зависимост от бита за четност) в началото и края на предаването казва на приемника, че идва и свършва предаването на един символ. http://halowave.webs.com/

1.2.6 Класификация по скоростта на предаване на информация

По скоростта на предаване на информация СПДИ са:

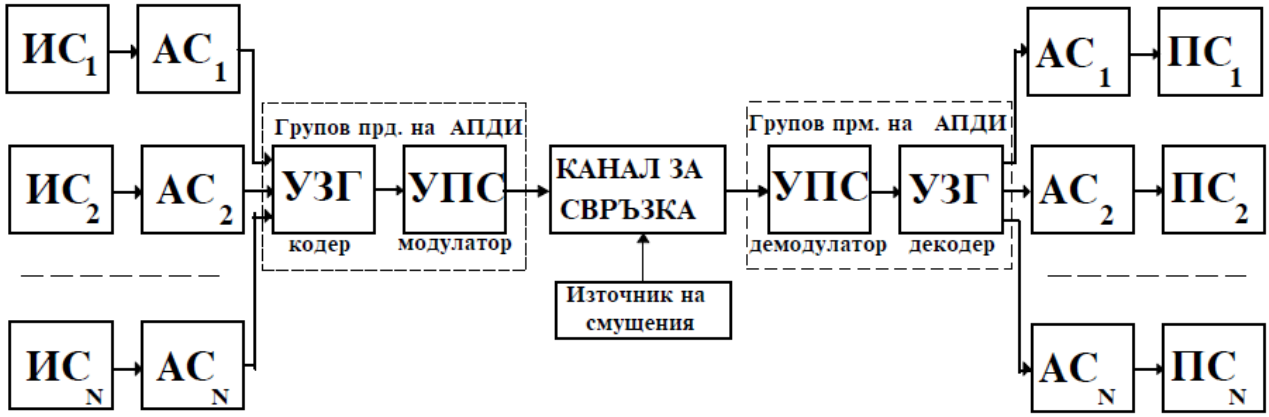
- нискоскоростни, в които информацията се предава по телеграфни канали с B<200 [Bd];
- средноскоростни, в които информацията се предава по телефонни канали с тонална честота на манипулацията със скорост B=600-19,200 [Bd];
- висикоскоростни СПДИ със скорост на предаване B>19,200 [Bd].

http://en.wikipedia.org/wiki/Data_rate_units

1.2.7 Класификация по броя на използваните канали

По броя на използваните канали СПДИ биват: едноканални и многоканални.

- Едноканални СПДИ са тези системи, които имат само един канал за предаване на дискретни съобщения (схемата аналогична на фиг. 1.1). В такива системи се предава дискретна информация от един източник.
- Когато е необходимо да се осигури предаване на дискретна информация от няколко източника за няколко получателя се използуват многоканални СПДИ, фиг.1.6.



Фиг.1.6. Структурна схема на СПДИ за N абоната

В този случай всяко дискретно съобщение се предава по свой информационен канал. На предаващата страна на СПДИ всички информационни канали се обединяват и образуват групов канал, който предава групов сигнал в канала за свръзка.

На приемната страна на СПДИ, сигналите на всеки информационен канал се отделят от груповия и се преобразуват в отделни съобщения, всяко от които постъпва към съответния получател.

Използуват се честотен, временен, кодов способи за структуриране на многоканални системи.

1.3 Основни понятия от теорията на информацията.

Приложната теория на информацията може да се определи като наука за рационалните методи за предаване на информацията по канали за свръзка. При това терминът "предаване на информация" трябва да разбира в разширен смисъл, имайки пред вид, че в процеса на движение на информацията от източника към получателя с нея може да се извършат различни преобразования и че съхраняването на информацията е частен

случай на нейното движение. В практиката под информация се разбират всякакви сведения, представляващи интерес за кореспондентите, поради което на този термин трябва да се предаде по-точен смисъл. По-нататък е целесъобразно да не се разглежда семантичният (смисловият) аспект на информацията, а да се съсредоточи внимание на техническите въпроси на измерването и, предаването и преобразуването на информацията от една форма в друга.

Съобщенията имат изключително важна роля и за възникването и развитието на човешката цивилизация. Всъщност хората непрекъснато участват в някаква форма на информационна връзка като например:

- разговор между две или повече лица директно, по телефона или по Интернет;
- четене на книга;
- гледане на филм, телевизия, театър, опера или балет;
- изпращане или получаване на писмо;
- разглеждане на картини в художествени галерии;
- слушане на радио, лекция и т.н.

Могат да се дадат хиляди други примери на съобщителни връзки в животинския свят или в сферата на човешкото общество. Все пак от посочените примери се вижда, че конкретният процес на предаване и получаване на съобщения може да протича в твърде различни форми, но въпреки това той има свойства, които са общи за всички случаи.

Съобщенията могат да има различна форма. Те могат да бъдат както някакви конкретни факти, съдържащи се в добре подготвена лекция, така и емоционалният заряд в художествено произведение или в откъс от музикална творба. Въпреки различията, общо за всички форми на съобщения е пренасянето на някаква информация.

Понятието информация произхожда от латинския термин “informatio”, който означава разяснение, изложение. От най-общи позиции може да се каже, че информацията са сведенията, предавани между хората устно, писмено или по друг начин (например с помощта на условни сигнали, технически средства и т.н.). Информацията увеличава знанията на този, който я притежава. Информацията е значението, което е приписано на данните по определени правила. Информацията най-общо е съвкупност от данни, които са съчетани в категории и квалификационни схеми.

В средата на XX век се оформи разбирането, че информацията е общонаучно понятие, което освен размяната на сведения между хората включва и предаването на сведения между човек и автомат, автомат и автомат, обмяната на сигнали в животинския и растителния свят, като например признаци от клетка към клетка, от организъм към организъм и т.н. Следователно, връзката "съобщение – информация" е от типа "форма – съдържание" като съобщенията са материалният носител на информацията, а информацията е смисълът на съобщенията. Съобщенията и информацията са двете страни на един и същ процес, защото предаването на съобщения има практическа стойност само ако те могат да бъдат правилно разбрани. Така например, ако по време на лекция се употребят думи, които са непознати на студентите, възгледите на преподавателя няма да стигнат до аудиторията. Също така, ако някой човек не знае японски език, вероятно той не ще може да разбере и осмисли японския вариант на дадена книга независимо от това колко добре е представен материалът в нея.

Досега не е дадено изчерпателно научно определение на информацията, но такива са направени за някои тесни научни области, като например общата теория на комуникационните системи. По-конкретно, американският теоретик К. Шенон със своята книга "Математическа теория на свръзките", издадена през 1949г., слага началото на теорията на информацията, чиито предмет и задачи са следните.

Предметът на теорията на информацията са: понятието информация и неговото измерване, принципите на кодиране и модулация, възприятието, предаването, представянето и преработка на информацията.

Задачата на теорията на информацията е да изучава своя предмет и на тази база да даде възможност на хората да преобразуват заобикалящата ги природна среда съобразно с техните потребности.

Теорията на информацията се състои от няколко основни клона:

- математическа теория на свръзките (възниква на базата на работите на К. Шенон и Н. Котелников);
- логически основи на компютърната техника (води своето начало от проекта на първия цифров компютър, разработен от Дж. Атанасов);
- теория на програмирането;
- теория на възприемането на сигналите от човека;

- теория на игрите (създадена от Дж. Наш);
- теория на управлението.

В тесен смисъл под теория на информацията се разбира математическата теория на свръзките.

Конкретно в рамките на теорията на информацията се използват следните понятия:

Информация – това е съвкупност от сведения, получаването и осмислянето на които, отстранява непълнотата, неточността и неопределеността в нашето познаване на някакво явление или предмет.

Информацията е сложно и многопланово понятие. Теорията на информацията насочва своето внимание за изследването и главно в три направления:

- количество на информацията;
- смисъл (съдържание) на информацията;
- полезност (ценност) на информацията.

Това съответства на три равнища за изучаване на информацията: синтактично, семантично и прагматично.

Важни характеристики на информацията са: достоверност, изчерпателност, достъпност, еднозначност, своевременност, направление, скорост за движение, принадлежност, форма на представяне и др.

Съобщение – това е материалната форма на информацията. Чрез него се предава абстрактната същност на информацията. Това е информация в определена материална форма – реч, текст, данни, изображение.

Съобщението е съвкупност от сведения за дадена материална система предавана от мястото на разположението и до пространствена отдалечена точка, от която тя не може непосредствено да се наблюдава. Това са сведения, които се предават от човек или устройство наблюдаващи тази система на друг човек или устройство, които нямат възможност да получават тези сведения от непосредствено наблюдение. Тази материална система заедно с наблюдателя представлява източник на съобщението. Ако тази материална система може да заеме няколко състояния, то тя представлява източник с крайно множество състояния.

Множеството възможни съобщения и техните вероятностни характеристики образуват **ансамбъл от съобщения**. Степента на разнообразие на възможните състояния на източника характеризира ентропията на системата.

Между ***информацията*** и ***съобщението*** няма еднозначно съответствие. Една и съща информация може да бъде предадена чрез различни, но еднакви по смисъл съобщения. Тя може да се разгледа като начин на осмисляне на съобщенията. Установяване на еднозначност между информация и съобщения става благодарение на договорността между предаващия и приемащия съобщението. Това изисква сложна преработка на информацията и от двете страни.

Трябва да се отбележи, че свойствата на системите за предаване на информация зависят от свойствата на предаваните съобщения. В теорията на информацията обаче не е необходимо детайлно описание на съобщенията. Поради това ще се разгледа само делението на съобщенията на дискретни и непрекъснати (аналогови).

Дискретните съобщения приемат само краен брой възможни стойности. Реално те представляват последователност от елементарни символи, съставящи една или друга азбука, например двоична. Затова такива съобщения често се наричат цифрови. Типични области на използването на такива съобщения са: предаването на данни, предаване на факсимилни изображения, телеграфията и др.

Непрекъснатите съобщения могат да приемат всякакво значение от множество с плътно разположени точки. Те могат да бъдат определени в дискретно и непрекъснато време.

Материален носител на информацията е сигналът (от латинската дума *signum-знак).* Това е физически процес, който протича във времето и пространството. В широк смисъл сигналът това е съобщение, предназначено за предаване на голямо разстояние, а в тесен смисъл под сигнал се разбират само електромагнитните съобщения.

Според веществено-енергетичното си проявление сигналите биват: светлинни, електрически, електромагнитни, звукови, ултразвукови и др., а според временно-пространствената си характеристика биват: статични и динамични.

От физическа гледна точка сигналът е процес или обект, природата, на който въобще не зависи от информацията, която той носи. Физическата среда, по която се

извършва предаване на сигналите от предаващата информацията страна към приемащата информацията страна, се нарича канал за свръзка.

Свойствата на сигналите, оказващи съществено влияние върху условията за предаване на информацията са:

- интензивност – H - степен на концентрация, разпространение или действие на светлина, звук и др. за единица време върху единица повърхност; сила;
- широчина на честотния спектър – F - съвкупност от електромагнитните вълни в природата, разделени пространствено и подредени по дължина или честота;
- продължителност - T.

За характеризиране на свързочните канали и качеството на сигналите се въвеждат понятията обем на канала - Vк и обем на сигнала – Vc.

$$Vc=H.F.T \qquad (11)$$

Необходимо е Vк > Vc.

Свързвайки понятията сигнал и съобщение, може да се каже, че под съобщение се разбира сигнал или последователност от сигнали с ясно очертано начало и край, съдържащи някакви смислени сведения.

1.4 Статистически методи на изследване в теорията на информацията.

В реалните канали за свръзка винаги има смущения. Под смущения се разбират всички пречещи на полезния сигнал външни въздействия (атмосферни шумове, влияние на други източници на сигнали, а така също и изкривяванията на сигналите в самата апаратура- апаратурни шумове, предизвикващи случайни отклонения на приетия сигнал от предавания). Освен това самите съобщения трябва да се отчита, че са също случайни. Например, летецът, чийто самолет се насочва по команди от земята, предварително знае всички възможни команди, но каква именно команда ще бъде подадена при поредния сеанс за свръзка, не му е известно. Примери подобни на приведения показват, че за получателя на информацията приемането на какво и да е частно съобщение винаги представлява случаен избор от някаква зададена съвкупност от съобщения.

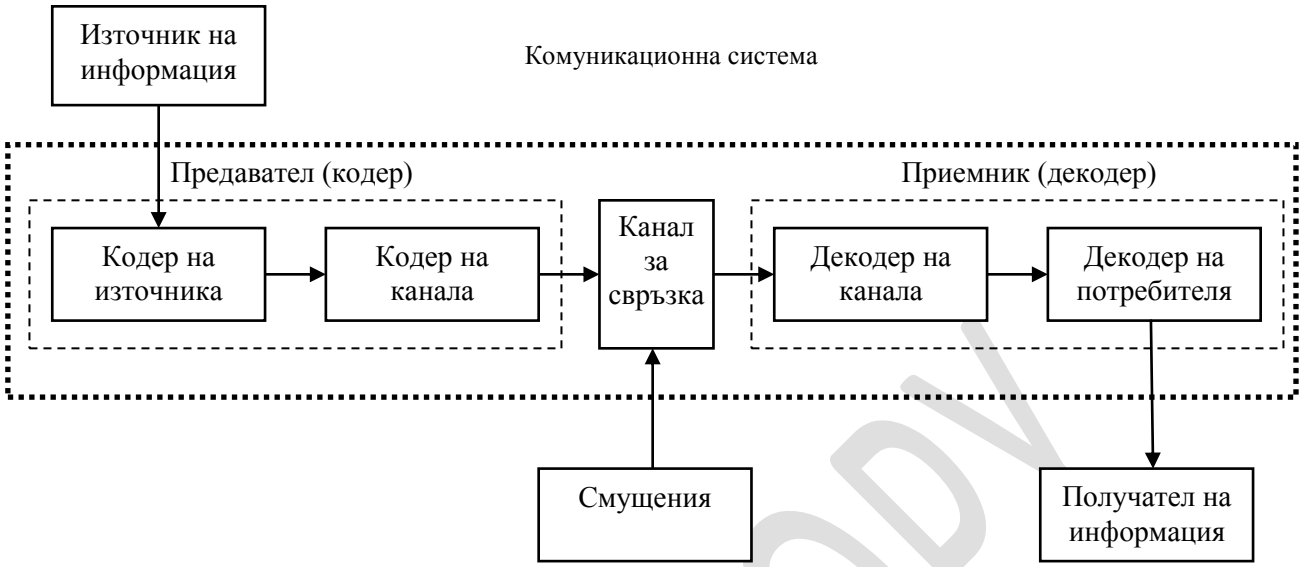
Сигналите, постъпващи от източниците на съобщения (микрофон, предаващи телевизионни тръби, датчици за измерване на топлина, налягане, влажност и т.н.) много често не могат да бъдат предадени незабавно по канала за свръзка по две причини. Първо, амплитудата на сигналите е недостатъчна. Второ, спектърът на сигналите е разположен в

диапазон, където затихването в канала за свръзка е голямо. Последната причина е по-съществена и почти винаги за да се осъществи ефективно предаване на сигналите в произволна преносна среда е необходимо да се пренесе спектъра на тези сигнали от нискочестотната област в диапазона на достатъчно високи честоти.

Съществени ограничения на структурата и свойствата на всяка система за предаване на информация налагат физическите свойства на канала за свръзка. Например: аналоговият телефонен канал не допуска непосредствено предаване на цифрови сигнали, радиотехническият и оптическият канал за свръзка не допускат непосредствено предаване по тях на аналогови или цифрови сигнали. Поради това в схемата на обобщената система за предаване на съобщения, фиг.1.7, трябва да има устройства, преобразуващи съобщението в сигнал, предаван по канала за свръзка и обратно, преобразуване на сигнала в съобщение на приемната страна. Тази процедура, получила в комуникационната техника названието модулация, винаги се осъществява така, че да се съхранени пренасяната от сигналите информация.

Както се вижда от фиг. 1.7, сигналите съдържащи полезната информация, не се изпращат директно в канала за връзка, а постъпват в специално техническо устройство, наречено предавател. Там те се преобразуват в други сигнали, наречени условно транспортни, които могат да преминат през канала за свръзка с най-висока скорост и с минимални изкривявания. Това преобразуване на информационните сигнали в транспортни се нарича кодиране. Следва да се има предвид, че много често на практика кодирането се извършва двукратно като се използват така наречените кодер на източника съобщението и канален кодер.

Следва дебело да се подчертае, че всички характеристики на съобщителната система се определят и ограничават от индивидуалните характеристики на източника, преносната среда и приемника. На свой ред типът на източника, средата и приемникът, които ще се използуват в съобщителната система, съществено зависят от вида на пренасяната информация. Така например прожектирането на цветен филм за конно състезание дава визуална и звукова информация за състезанието. От филма може да се разбере дали небето е ясно или облачно, в какъв цвят са облечени жокеите, кой печели състезанието. Но вследствие ограниченията, наложени от съобщителната система, не е възможно да се усети миризмата от тренировъчната площадка на конете.



Фиг.1.7: Кодиране и декодиране на сигналите в комуникационните системи

Така например в класическите радио системи, най-напред акустичните вълни, носещи съобщението на радио - говорителя, чрез кодера на източника на съобщението, представляващ микрофон, се преобразуват в нискочестотен електрически сигнал, чиито спектър е в честотната лента 300 [Hz]-10000 [Hz]. След това каналният кодер, наричан още модулатор, преобразува нискочестотните сигнали във високочестотни сигнали със спектър (например) в честотната лента 1,20 [MHz] – 1,21 [MHz]. Необходимостта от двукратно преобразуване на сигналите произтича от следните обстоятелства. Първо, акустичните вълни, носещи съобщението на радио - говорителя, бързо затихват в атмосферата и в най-добрия случай могат да бъдат чути на разстояние 20 [m]-30 [m]. Същевременно радиосигналите с честоти от порядъка на 1,20 [MHz] – 1,21 [MHz] могат да бъдат уверено приети на разстояния от порядъка на 100 [km]-1000 [km]. Второ, директното преобразуване на акустичните сигнали във високочестотни електрически сигнали без междинна трансформация в нискочестотни електрически сигнали е сложно или дори невъзможно.

Следва да се отбележи, че предавателят обединява кодерите на източника на съобщението и на канала.

Към канала за свръзка на фиг. 1.7 е включен източник на смущения. Математически това е некоректно, тъй като смущенията влияят на сигналите във всички елементи от системата за свръзка. Смисълът на показаното включване е в това, че от всички смущения

действащи в системата, най-непредсказуеми и следователно най-опасни са смущенията в канала за свръзка.

На другия край на канала за свръзка сигналът се преобразува във вид удобен за възприемане от получателя на информация чрез устройство, наречено приемник. Всъщност приемникът изпълнява функциите на предавателя в обратен ред. В разглеждания пример на класически радио системи на първия етап сигналите се демодулират, т.е. високочестотните електрически сигнали се преобразуват в нискочестотни, а на втория етап нискочестотните електрически сигнали посредством говорители (тон-колони) се трансформират в акустични вълни, които могат да бъдат възприети от слуховия апарат на радио слушателите.

Предвид на изложеното, следва да се отбележи, че основната задача на математическата теория на свръзките е да разработва оптимални методи за кодиране и декодиране на съобщенията, позволяващи информацията да достига получателя с максимална пълнота и точност.

За да се предаде определено количество информация, тя трябва да бъде подложена на ефективно преобразуване във вид на специални символи или сигнали т.е. да се закодира. Ето защо една от задачите на теорията на информацията е да се намерят най-икономични и най-ефективни методи за кодиране, позволяващи да се предаде дадена информация с минимално количество символи. Тази задача се решава за канал със и без шум. По същество това е задача за максимизация на средната скорост на предаване на информацията.

Друга задача е определяне пропускателната способност на даден канал такава, че той да е в състояние да предаде цялата постъпила информация без задръжки и изкривявания. По принцип това са въпросите свързани с определяне възможностите на канала и достоверността на предадената информация.

За да се решат успешно тези задачи, трябва да се определи количеството на предаваната и съхраняваната информация, да се изучат свойствата на информацията, способите за нейното предаване и системите за предаването и.

В заключение може да се формулират следните основни задачи, възникващи в теорията на информацията:

♦ Какво най-голямо количество достоверна информация може да се предаде по канала за свръзка, притежаващ зададени свойства, за единица време?

♦ Какви преобразувания на информацията трябва да се извършат, за да се предаде по канала за свръзка със смущения известно количество информация при зададено ниво на грешките?

Основно внимание в теорията на информацията се отделя на ограниченията, които се налагат на процеса на предаване на информацията от канала за свръзка.

Като обобщение, в теорията на информацията се установяват количествените характеристики на информацията, определят се физическите и статистическите параметри на каналите за свръзка, формулират се условията за съгласуване на източниците на информация с каналите за свръзка, развива се идеята за използуване на кодирането за повишаване на шумоустойчивостта на предаването на информация по каналите за свръзка с шум и построяването на оптимални кодове за предаване на информация в канали с отсъствие на смущения.

Теорията на информацията е сравнително млада наука. Нейното създаване е свързано с името на американския учен К. Шенон, публикувал своите основни изследвания в 1945 г. Съществени приноси в развитието на отделни раздели от теория на информацията и предаване на данни и сигнали са внесли ***А.Н. Колмогоров, В.А. Котелников, Н. Винер, Д. Мидлтон, Р.М. Фано, Р.Л. Стратонович, Джеймс Мартин*** и др.

Моля, отговорете на контролните въпроси:

1. *Каква е разликата между понятията - съобщение и сигнал ?*

2. *С какво понятие се указва измервато на скоростта в една комуникационна система?*

3. *Кой метод за обмен е по-добър - дуплекс или полудуплекс и защо?*

4. *Каква е целта на кодирането в комуникационните системи?:*

5. *Каква е разликата достоверност и шумозащитеност?.*

Раздел 2

Компютърни мрежи

Устройства в компютърните мрежи.

Класификация на компютърните мрежи.

Ключови думи и съкращения

Компюгтърна мрежа	**Мрежова карта**
Клиент	**Коаксиален кабел**
Сървър	**Концентратор**
Топология	**Комутатор**
Оптичен кабел	**Мрежова услуга**

2.1. История на компютърните мрежи

В началото на 19-ти век французите създават първата оптична телеграфна мрежа със скорост на предаване 20 знака в секунда. Малко по-късно Самюъл Морз демонстрира своя електрически телеграф, с което се слага началото на телефонните комуникации. В края на 19-ти век започва изграждане на големите телефонни мрежи. Към 1960 г. различните телефонни мрежи биват свързани, образувайки световна комуникационна мрежа.

През 60-те години, по време на Студената война, правителството на САЩ взема решение за разработване на компютърна мрежа, която да обслужва комуникационните връзки във военната система на САЩ. Тя се разработва под мониторинга на Министерството на отбраната на САЩ, като в нейното изграждане вземат участие и големи университети, между които Калифорнийският университет и Масачусетския технологичен институт. В резултат, в края на 60-те години възниква първата компютърна мрежа, наречена ARPAnet (Advanced Research Projects Agency network). През 1969 г. мрежата бива отворена за невоенни организации. Първи към нея се свързва Калифорнийския университет. След три години мрежата вече обхваща почти всички университети и научни институции в САЩ, а след още две достига и до Европа. Така възниква първата *глобална компютърна мрежа* (WAN – Wide Area Network). По-късно, през 80-те години, ARPAnet бива разделена на две мрежи – Defense Data Network (военна мрежа) и NSFNet (мрежа на Националната научна асоциация). За кратко време NSFNet се разраства, образувайки днешната мрежа Интернет.

Историята на компютърни мрежи не започва с ARPAnet. Отначало мрежите включваха един мейнфрейм (компютър с големи габаритни размери и с висока за времето си производителност) и множество терминали, свързани към него. Посредством терминалите

потребителите осъществяваха колективен достъп до данни и приложения, съхранявани в мейнфрейма. Терминалите са устройства, които не притежават памет и изчислителна способност. Те не са компютри. Изградени са от клавиатура и видеомонитор. Недостатък на този тип мрежи бе високата им цена, а излизането от строя на мейнфрейма водеше до отпадане на цялата мрежа.

Появата на персоналните компютри промени коренно нещата. Освен ниската си цена, те осигуриха на организациите и по-висока надеждност (отказоустойчивост) на системите им за обработка на информация. Например, ако един от компютрите излезе от строя, това не нарушава работоспособността на останалите. Нуждата от общо използване на информация и ресурси (принтери, скенери и др.) в едно предприятие наложи свързване на персоналните компютри в мрежа. Така възникнаха първите компютърни мрежи, наричани *локални мрежи* (LAN – Local Area Network). Те са локални, понеже свързаните компютри са разположени териториално близо един до друг, най-често в една обща стая или сграда. Днес под компютърна мрежа се разбира група от свързани помежду си компютри и други устройства (принтери, скенери и/или др.), които могат да комуникират помежду си и да споделят общи информационни ресурси. Мрежите могат да бъдат малки или големи, свързани постоянно (чрез кабели) или временно (чрез телефонни линии или безжична комуникация).

Телефонните мрежи се различават от компютърните по това, че използват технология, известна като *комутиране на електрически вериги* (circuit switching). Свързването на един телефон с друг (посредством поредица от комутации) води до възникване на електрическа верига, по която се извършва комуникацията. Връзката е *постоянна* и трае докато комуникацията приключи. Ако връзката бъде прекъсната и след това повторно създадена, най-често възниква друга постоянна връзка (друга електрическа верига), представляваща друг път за комуникация.

При компютърните мрежи се използва друга технология, използваща комутиране на пакети (packet switching). Тук данните биват разбивани и изпращани в мрежата под формата на пакети, като всеки един от тях може да пътува по различен път в мрежата и да достигне до крайната точка на комуникация в различно време. След като всички пакети достигнат крайния пункт, те биват подреждани в първоначалния им ред така, че да образуват отново тяхното общо цяло. За разлика от телефонните мрежи тук не се ползва една единствена връзка, оставаща постоянна за цялото времетраене на комуникация. Тук пакетите пътуват по различни пътища.

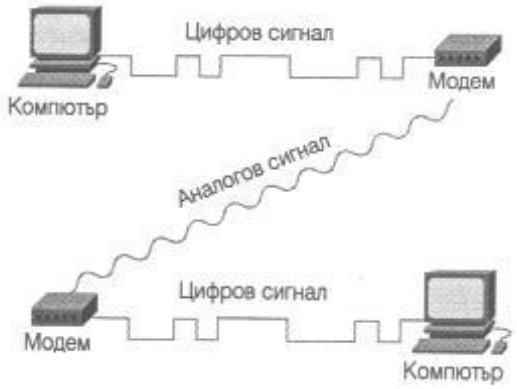
През 90-те години започна масово свързване на LAN-мрежите в по-големи мрежи. В резултат възникна и глобалната Интернет мрежа. Развитието на мрежите доведе до възникване на нови информационни технологии, немислими до преди 20 години

2.2 Принципи на компютърната мрежа

Компютърните мрежи представляват свързани помежду се **компютри**, **периферни устройства** и **софтуер** за съвместното им използване. Мрежата е механизма, позволяващ на разпръснатите компютри и техните потребители да комуникират помежду си и да споделят ресурси. Компютърните мрежи се организират за да се създаде възможност за :

- обмен на данни между потребителите на различни компютри
- съвместно ползване на общи ресурси/апаратни, софтуерни и информационни/
- разпределена обработка на данни, т. е. обработка чрез различни компютри на данни, части от които се съхраняват в паметта на различни компютри

Най – проста физическа система за съвместна работа на два отдалечени помежду си компютъра е възможна чрез осигуряване на комуникация по телефоннатата линия, като в двата и края се разполагат модеми (устройства, които могат да преобразуват компютърно представени данни в сигнали за изпращане по телефонни линии и обратно) фиг.2.1



фиг.2.1

Физическото свързване на компютрите в мрежата не означава, те ще могат да работят заедно. Затова е необходима подходяща мрежова операционна система, която да осигурява взаимодействието между различните устройства и програмни системи.

Предаването на данни в мрежата се регламентира от специални правила, наречени мрежови протоколи. Мрежата Интернет например се основава на протокол

наречен TCP/IP (Transmission Control Protocol / Internet Protocol) – протокол за управление на предаването / междумрежов протокол.

2.3 Видове мрежи

Според обхвата

- ✓ LAN (Local Area Network) – локална компютърна мрежа, която обслужва една организация и е разположена в една сграда.
- ✓ MAN (Metropolitan Area Network) – обхваща територия на едно населено място или голяма сграда с много разположени в нея организации.
- ✓ WAN (Wide Area Network) – глобална компютърна мрежа, която използва високоскоростни, далечни комуникации или спътници, за да свърже компютри, намиращи се в различни географски точки.
- ✓ SAN (Storage Area Network) – мрежа за съхранение на данни, която се използва за свързване на големи масиви от данни към групирани сървъри.

Собственост

- ✓ Обществена – открита за ползване от всички потребители мрежа. Може да обхваща даден регион, държава или целия свят.
- ✓ Корпоративна – затворена мрежа, която се ползва само от служители на корпорацията.
- ✓ Домашна – свързани в мрежа уреди с вградени компютри, които формират инфраструктурата на дома.

Интернет технология /класификация според приложението/

- ✓ Интернет – интегрирана световна мрежа.
- ✓ Интранет – частна корпоративна мрежа, в която се използват продукти и технологии от Интернет.
- ✓ Екстранет – Интранет мрежа, която е "отворена за приятели" - партньори и клиенти.

Тип

- ✓ Хетерогенна мрежа – мрежа, в която работят разнотипни системи от различни производители.
- ✓ Хомогенна мрежа – мрежа, в която работят системи от един и същ тип.
- ✓ Универсални – реализират разнообразни приложни процеси.

- ✓ Специализирани – реализират еднотипни приложни процеси.

Предаването на данни в мрежата се регламентира от специални правила, наречени **мрежови протоколи**. Съвкупността от определена група мрежови протоколи формира така наречения **протоколен стек** Например Internet мрежата се основава на протоколен стек, наречен TCP/IP (Transmission control protocol/Internet protocol).

http://en.wikipedia.org/wiki/Internet_protocol_suite

Съществуват и други протоколни стекове като IPX/SPX и AppleTalk

http://en.wikipedia.org/wiki/IPX/SPX

http://en.wikipedia.org/wiki/AppleTalk

2.4 Локални комютърни мрежи

Локална компютърна мрежа (Local Area Network, LAN) може да се образува от два или повече компютъра, които са свързани помежду си с помощта на някакво физическо средство (коаксиален кабел, кабел с усукани двойки проводници и др.). Свързаните по този начин компютри могат да обменят своите данни и да използват общи периферни устройства, като скоростта при на преноса на данни е обикновено висока, поне 100Mb/сек. Свързаните компютри са разположени върху ограничена площ, например в рамките на един етаж. Всяка компютърна мрежа включва няколко основни компонента:

- ✓ Компютри
- ✓ Съобщителна среда
- ✓ Мрежови карти
- ✓ Свързващо устройство в зависимост от типа на мрежата
- ✓ Мрежов софтуер

Съобщителната среда осигурява прехвърлянето на данните между различните устройства..Обикновено се изгражда чрез: коаксиален кабел, кабел тип усукана двойка, оптичен кабел или чрез радиопредавател

Мрежовата карта (Network interface card, NIC) осигурява връзката на компютъра с локалната мрежа (фиг.2.2).

фиг.2.2

Мрежовият софтуер играе управляваща роля. Той задава режима на работа на компютъра в мрежата, определя различната роля на компютрите в мрежата. Така два напълно еднакви компютъра могат да работят по различен начин в мрежата

В зависимост от предназначението и функциите, които изпълняват, компютрите в мрежата се делят на:

Сървър (server) – компютър, който предлага на другите включени в мрежата компютри някои свои услуги и периферни устройства, като по този начин се осигурява функционирането на мрежата като такава.

Клиент (client) – използва услугите, които се предоставят в една мрежа. Това може да бъде както компютър, така и отделна програма.

Чести използван термин е „**работна станция**” (Workstation) – потребителски компютър, свързан към мрежата. Разликата между работната станция и несвързания в мрежата персонален компютър е в това, че работната станция използува различни услуги, предлагани и от локалната мрежа, в които е включена.

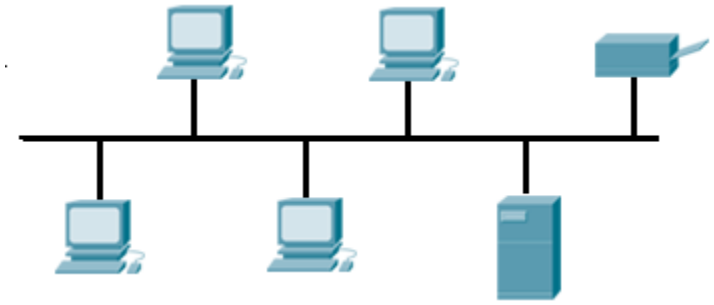
Сървърите се класифицират обикновено в зависимост от услугата, която предоставят. Те могат да бъдат:

- ✓ Файлов сървър – предоставя достъп до файлове с данни
- ✓ Принт-сървър – предоставя достъп до печатащи устройства
- ✓ Комуникационен сървър – предоставя достъп до средства за връзка
- ✓ Други

2.4.1 Топологии на локалните мрежи

Една от основните характеристики на всяка компютърна мрежа е нейната топология. Топологията определя начина за разположение и връзка между устройствата в мрежата. Основните типове топология на мрежите са линейна, звездообразна и кръгова.

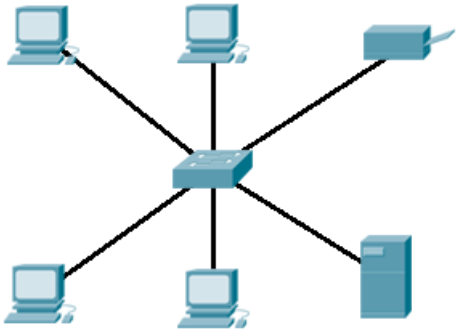
При линейната топология (фиг.2.3) мрежовите устройства се свързват последователно към кабел.



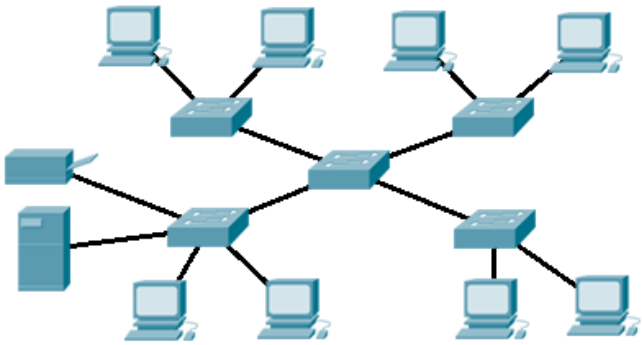
фиг.2.3.

Този кабел се нарича шина (BUS). Сигналът от кое да е устройство достига до всички останали. Ако кабелът се повреди някъде по средата на опорната магистрала, мрежата престава да работи и в двете й части.

При звездообразната топология (фиг.2.4) и топология разширена звезда (фиг.2.5) всеки възел от мрежата е свързан към устройство, наречено концентратор/хъб (hub) или комутатор(switch), което разпределя сигналите между отделните компютри



фиг.2.4 Топология звезда



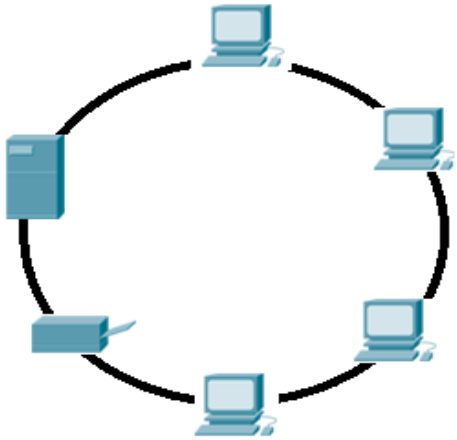
фиг.2.5 Топология Разширена звезда

Ако връзката между едно от устройствата и HUB-а бъде нарушена, това няма да попречи на цялостната работа на мрежата. При дефект обаче в концентратора (хъба) цялата мрежа спира да работи.

С използването на комутатор (switch) някой недостатъци се преодоляват, тъй като той осигурява микро-сегментиране на мрежата, на чиято основа евентуален срив в определен участък (сегмент) не оказва съществено влияние на работата в мрежата (фиг.2.5). От друга страна този мрежов елемент осигурява и по-голяма производителност.

Съвременните мрежи със скорост от порядъка на 100 Mbit/1 Gbit се изграждат с помощта на комутатор и с използването именно на тази топология.

При кръговата технология (фиг.2.6) отделните устройства са свързани в мрежа, в която връзките, условно казано, имат формата на кръг.



фиг.2.6

Всеки един възел от мрежата има по две връзки-по една към всеки съседен възел. Когато мрежата е малка (примерно, 4-5 възела), закъснението, което се получава докато данните пропътуват по кръга до намирането на получателя им е относително малко. Ако мрежата е съставена от около десетина възела, времето нараства значително. Този тип топология неефикасна за по-големи мрежи.

2.4.2 Видове мрежови преносни среди

Мрежовата преносна среда служи за пренасяне на сигнали от едно мрежово устройство към друго. Физическите компоненти необходими за свързването на компютрите в мрежа са мрежовите карти и определен вид кабел. Най-използваната мрежова преносна среда е кабелна, но съществуват и други форми на безжични връзки като инфрачервени и лазерни лъчи, радиовълни, микровълни, сателитни връзки.

Най-използваемите кабели използвани в мрежовите среди са следните:.

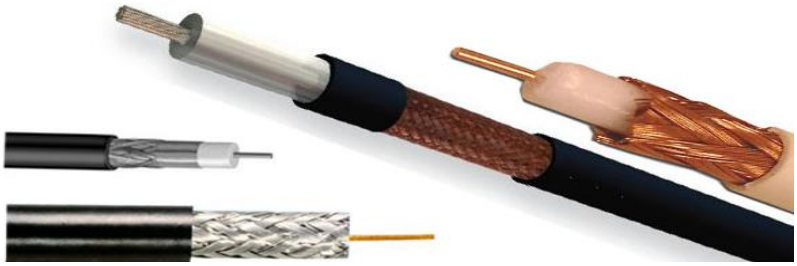
Коаксиален кабел – този тип кабели се използват както в мрежи с директно предаване, така и в радиочестотно.

- Коаксиален кабел за директно предаване – този тип коаксиален кабел осигурява съобщителен канал, по който в определен момент може да се предава само едно съобщение, но с много голяма скорост. Цифровата информация се предава серийно - бит

по бит в основната честотна лента на съобщителния канал, т.е. предаването е директно, без модулация. Предимство на кабелните системи от този вид е, че към кабела се монтират лесно съединители, позволяващи свързване на нови работни станции, без да се нарушава действието на мрежата.

Фиг.2.7 Коаксиален кабел

- Кабели за радиочестотно предаване – чрез радиочестотно предаване могат да се разпространяват интегрирани звукови, цифрови и видеосигнали. Често заедно с тях се използват усилватели, по този начин се осигурява покритие на по-големи разстояния в сравнение с коаксиалните кабели за директно предаване. При използване на коаксиалните кабели за радиочестотно предаване могат да се разпространяват едновременно няколко сигнала с различни честоти (кабелна телевизия, при която се използва радиочестотен коаксиален кабел с характеристичен импеданс 75 Ohm.) Всички системи за радиочестотно предаване са изградени с единичен кабел и двупосочни усилватели, или имат двукабелна конфигурация. И в двата случая носещите сигнали се изпращат до една централна точка, наречена главен възел, от където те се предават обратно до всички точки на мрежата.



Фиг.2.8 Кабел за кабелна телевизия

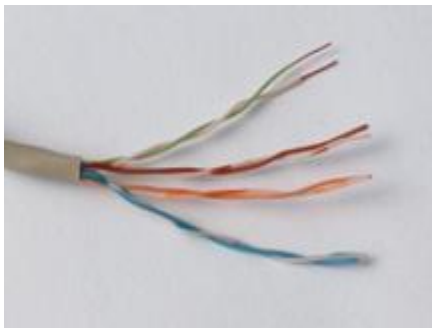
Кабели с усукани двойки проводници – основното предимство на кабелите с усукани двойки проводници е, че са евтини и се инсталират лесно. За предпочитане са, когато външните смущения не са най-важния фактор за мрежата. Кабелите с усукани двойки проводници са най-евтината съобщителна среда за локалните мрежи. Те се състоят

от двойки изолирани и взаимно усукани проводници, така че във всеки проводник попадат еднакви по интензивност външни смущения. Този внесен шум става част от предавания сигнал. Усукването на проводниците намалява, но не елиминира шума. Съществуват два основни типа усукани двойки проводници: екранирана (STP – shielded twisted pair) и неекранирана (UTP – unshielded twisted pair). Когато се добави екраниране към усуканата двойка проводници се намалява наличието на външните електромагнитни смущения, но по този начин се увеличава затихването на сигнала това от своя страна може да повлияе върху съпротивлението на проводника и да доведе до загуба на данни.

Екранирана усукана двойка (STP кабел) – екранирането се реализира чрез използване на медна оплетка или фолио, които обвиват изолираните медни двойки вътре в най-външната обвивка. Чрез използването на този метод се намалява въздействието на електромагнитните смущения за сметка на оскъпяването на кабела и загубата на данни. Най-често този тип кабели се използват в мрежите от тип AppleTalk и Token Ring.

Фиг.2.9 STP кабел

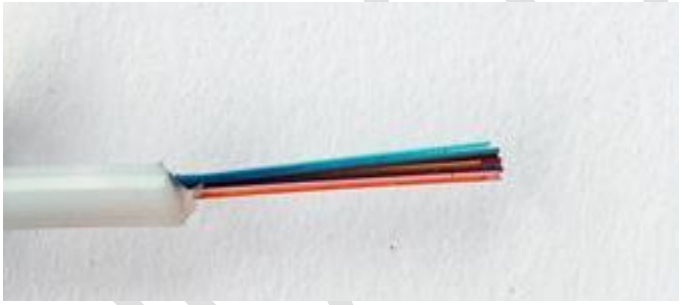
Неекранирана усукана двойка (UTP кабел) – е най-популярния тип кабел поради следните причини: евтин, гъвкав и лесен за употреба, използва RJ-45 конектор, използва се в топология звезда.



Фиг.2.10 UTP кабел Cat.5

Влакнесто оптичен – този вид технология осигурява шумоустойчивост на сигналите и безпогрешно предаване надалечни разстояния при най-високо ниво на защита на информацията в мрежата. Този вид кабели са най-скъпата съобщителна среда за локалната мрежа. Този метод за предаване на информация има редица предимства в сравнение с възможностите на усуканите двойки проводници и коаксиалните кабели. Осигуряват много по-висока скорост на предаване, влакнесто оптичните кабели са защитени от електромагнитни и радиочестотни смущения и пренасят сигнали без загуби на далечни разстояния. Влакнесто оптичният кабел е направен от чисто стъкло, изтеглено в тънко влакно образуващо сърцевината на кабела, около влакното има обвивка, състояща се от стъклен слой с по-малък показател на пречупване от този на сърцевината.

Влакнесто оптичния кабел работи в два режима: единичен режим (single mode) при него светлината се движи по оста на кабела и множествен режим (multi mode)



Фиг.2.11 Оптически кабел

Безжична преносна среда – използването на кабели не винаги е желателно, а понякога е и невъзможно. Използването на безжичната технология като алтернатива на мрежите става все по-популярна. Безжичната мрежа включва безжични устройства, които комуникират с традиционната кабелна мрежа. Точките за достъп (access points - приемо-предавателните устройства) се използват за предаване и приемане на данни между безжично устройство/ва и кабелната мрежа.

Безжичната комуникация включва различни методи за предаване като: инфрачервени лъчи (infrared), с използване на радио честоти, чрез използване на лазер (laser), Bluetooth.

Фиг.2.12 Bluetooth

Моля, отговорете на контролните въпроси:

1. *Кога е създадена първата мрежа ?*
2. *Какви видове мрежи познавате?*
3. *Кое не е вид кабел? :*

а) UTP; б) FTP; в) STP; г) UDP.

4. *Кое е най-използваното устройство в една мрежа?:*
5. *Каква е разликата между понятията клиент и сървър в мрежите?.*

Раздел 3

Мрежови модели и стандарти. Отворен модел OSI

Ключови думи и съкращения

Мрежов модел OSI	**Капсулация**
Протоколен стек	**Порт**
TCP/IP	**Сокет**
UDP	**RFC**

3.1. Мрежови модели

Мрежовите модели са основата на стандартизацията; ако един и същ модел се използва от производителите на мрежови продукти, тези продукти могат да бъдат сравнени с едни с други. Моделите описват начина, по който се извършват комуникациите на данни. Ако даден производител, произвеждащ продукти за изграждане на мрежи, съблюдава стандартите на всеки слой, мрежовите компоненти трябва да работят с тези, произведени от други производители.

Най-използваният модел в мрежите е моделът Open System Interconnection (OSI), който е разработен от Международната организация за стандартизация (ISO). Моделът OSI е изграден от седем слоя, всеки от които представлява една стъпка в процеса на мрежовите комуникации. Седемте слоя на OSI модела са показани на фиг.3.1

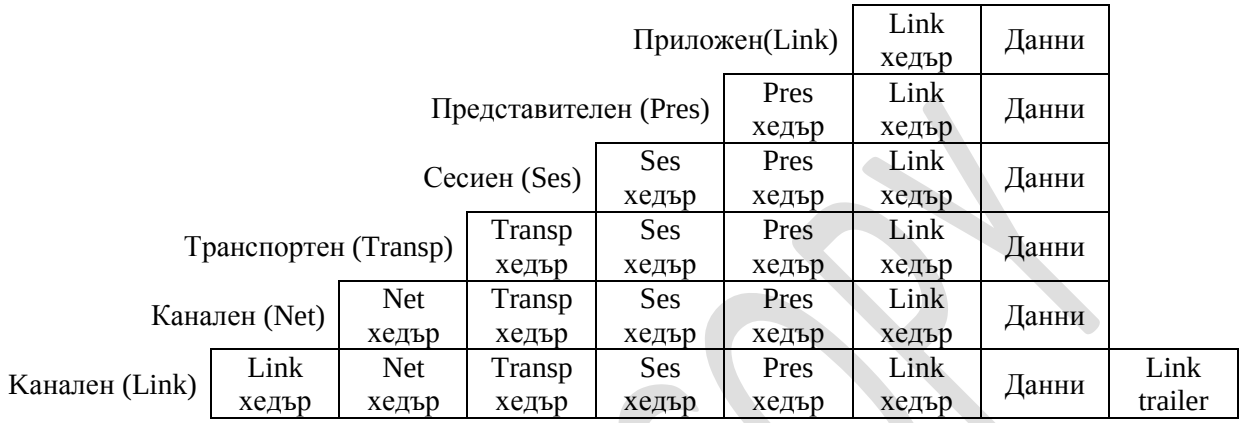
Application	Приложен
Presentation	Представителен
Session	Сесиен
Transport	Транспортен
Network	Мрежов
Data link	Канален
Phisical	Физически

фиг.3.1

Протоколите, които изграждат ***комплекта от протоколи (protocol suit),*** работят на различни слоеве.

Всеки слой на OSI модела изпълнява конкретна задача в процеса на мрежовата комуникация и след това предава данните нагоре или надолу към следващия слой (в

зависимост от това дали слоят функционира в предаващия или приемащия компютър). Тъй като данните се предават през слоевете, всеки слой добавя своя собствена информация под формата на хедъри, които биват добавяни пред оригиналните данни (фиг.3.2)



фигг.3.2

Трябва да се обърне внимание, че физическият слой не добавя хедър информация. Неговата функция не изисква подобно добавяне, защото той се занимава главно с мрежовия хардуер и създаването на сигналите по съобщителната среда

Процесът на мрежова комуникация работи по следния начин: от изпращащата страна дадено приложение създава данни, които трябва да бъдат предадени по мрежата. След това той ги предава на приложния слой от мрежовия компонент на операционната система.

Когато данните преминават през слоевете, те биват ***капсулирани*** или затваряни в рамките на по-голяма единица, тъй като всеки слой добавя хедърна информация. Когато данните достигнат приемащият компютър, процесът се извършва в обратния ред; информацията се предава нагоре през всеки слой и докато става това, капсулиращата информация постепенно бива премахвана, слой по слой, в ред, обратен на реда, в който е била добавяна.

Каналният слой (data link layer) в приемния край чете и снема хедъра, добавен от каналния слой на изпращащата страна. След това мрежовият слой на приемащата страна обработва информацията в хедъра, добавен от съответния слой на изпращащия компютър, и т.н. Всъщност всеки слой комуникира със слоя, който носи същото име от другата страна.

Когато данните преминат целия си път през слоевете на приемащия компютър, цялата хедър информация бива премахната и данните се възстановяват в тяхната оригинална форма, т.е. както са създадени от приложната програма на изпращащия. В тази форма те се представят на приложението на приемника под формата на информация.

3.1.1 Фуникции на отделните слоеве

Приложният слой

Първото и най-важно нещо, което трябва да бъде разбрано за приложеният слой, е, че това не е потребителското приложение, създаващо съобщението. Този слой осигурява взаимодействие между приложната програма и мрежата. Протоколите, функциониращи в приложния слой, изпълняват функции като услуги за трансфер на файлове, достъп за печат и обмен на съобщения.

По важни протоколи, които функционират в приложния слой, са следните:

File Transfer Protocol (FTP) - FTP се използва за трансфер на файлове между компютри, които не е задължително да работят под една и съща операционна система или платформа. Софтуерът на FTP сървъра се изпълнява на компютъра, който хоства файловете, а FTP *клиентската програма* се използва за свързване към, качване на или сваляне от сървъра. В повечето реализации на комплекта протоколи TCP/IP е включен FTP клиент, който работи от командния ред. Съществуват множество популярни графични FTP клиенти, като WSFTP, CuteFTP и FTP Voyager. Множество Web браузъри включват вградени възможности за трансфер на файлове.

Telnet - Telnet се използва за терминална емулация и за осъществяване на достъп до приложения и файлове на друг компютър. За разлика от FTP, той не може да бъде използван за копиране на файлове от един компютър на друг, а само за тяхното четене или изпълнение от отдалечения хост. Telnet софтуерът включва сървърния Telnet софтуер, изпълняващ се на отдалечения компютър, до който се осъществява достъп, и Telnet клиента, който се изпълнява на осъществяващия достъпа компютър.

Simple Mail Transfer Protocol (SMTP) - SMTP е независим от производителя, прост ASCII протокол, използван за изпращане на електронна поща по Интернет. Много популярни програми за e-mail използват SMTP за изпращане на поща; за сваляне се използва и протоколът Post Office Protocol (текущата версия е POP3) или протоколът Internet Message Access Protocol (IMAP).

Simple Network Management Protocol (SNMP) - SNMP събира информация за мрежата. SNMP може да бъде използван с различни платформи и операционни системи. Често той се приема за TCP/IP протокол, но може да бъде изпълняван и върху Internet Packet Exchange (IPX) и OSI. Протоколът SNMP използва база с управляваща информация (Management Information Base - MIB), представляваща база данни, която съдържа информация за работещ в мрежата компютър. SNMP има две части: ***агентски*** софтуер, който се изпълнява на наблюдавания компютър, и ***управленски*** софтуер, изпълняващ се на компютъра, който провежда наблюдението.

Необходимо е да се спомене, че не трябва да се бъркат самите приложни програми с протоколите със същото име, на които са базирани програмите. Например съществуват разнообразни приложни програми, наречени FTP клиенти. Тези програми използват протокола FTP за трансфер на файлове, но приложенията включват също и възможности като графични интерфейси (които се различават между различните реализации) или допълнителни функции, като например машини за търсене на файлове.

Представителен слой

Протоколът от приложния слой приема данните от потребителското приложение и ги предава надолу в стека към представителния слой. Този слой изпълнява действията, свързани с пакетирането или представянето на данните. Тези действия са следните:

Компресиране на данни - Представлява редуциране на размера на данните с цел способстване на по-бързото им предаване по мрежата. Различните типове данни могат да бъдат компресирани в различна степен.

Криптиране на данни - Представлява преобразуване на данните в кодирана форма, която не може да бъде прочетена от неоторизирани лица.

Транслация на протоколи - Конвертиране на данните от един протокол в друг с цел осъществяване на техния трансфер между разнородни платформи или операционни системи.

Представителният слой на приемащия компютър отговаря за декомпресирането, декриптирането и всички други транслации на данни в разбираем за приложението формат и тяхното представяне на приложния слой.

В представителния слой работят много шлюзове (gateways). ***Шлюзът*** представлява устройство или софтуер, което служи като точка на свързване между две различни мрежи. Популярните шлюзове са следните:

Gateway Services for Netware (GSNW) - софтуер, който дава възможност на клиентите на даден сървър да осъществяват достъп до неговите файлове. Софтуерът извършва транслиране между протокола Server Message Block (SMB), използван в софтуера на Microsoft, и протокола Netware Core Protocol (NCP), който е протоколът за поделяне на файлове, използван от Netware.

E-mail шлюз - софтуер, който транслира съобщения от разнородни и несъвместими e-mail системи в общоприет Интернет формат, какъвт е SMTP. Това позволява изпращането на електронни съобщения от копютър Macintosh, използващ клиента за електронна поща Eudora, до получател, използващ например Lotus Notes в NetWare мрежа. Независимо от разликата в системите за електронна поща, съобщението преминава успешно и може да бъде прочетено.

• **Systems Network Architecture (SNA)** шлюз - SNA представлява собствена архитектура на IBM, която се използва в мейнфрейм компютърни системи като AS/400. Софтуерът на SNA шлюза позволява на PC компютри от локална мрежа да осъществяват достъп до файлове и приложения на мейнфрейм компютър от своите десктопи.

Редиректорът (redirector) представлява софтуер, който определя дали дадена заявка трябва да бъде обработена от локалния компютър или от мрежово устройство, като пренасочват (преадресират) входно/изходните заявки по подходящ начин и по правило действат в представителния слой.

Сесиен слой

Протоколите, които работят в този слой, отговарят за изграждането на директна сесия между изпращащия и приемащия компютър. Сесийният слой установява и прекратява диалозите приложение-приложение. Той осигурява също така нареченото ***поставяне на контролни точки (checkpointing)*** за синхронизиране на потока от данни за приложенията. Това включва поставяне на маркери в потока от данни. При пропадане на комуникацията трябва да бъдат предадени отново само данните с най-скорошен маркер (контролна точка).

Друга функция на сесийния слой е да контролира дали предаването се изпраща като ***полудуплекс*** или като ***пълен дуплекс.***

Сесийният слой отговаря за много неща, например за установяването на правила за обмен на данни между приложенията по време на сесията. Това донякъде наподобява работата на рефер или посредник, който гарантира, че и двете страни знаят правилата на играта и са съгласни да ги спазват - поне за времето на тази сесия.

Сесийният слой осигурява експедиране на данните, клас на услугата и докладване на проблемите в самия слой и в слоевете над него в мрежовия модел.

Протоколите от сесийния слой включват следното:

Network Basic Input/Output System (NetBIOS) интерфейс - В сесиен режим NetBIOS позволява два компютъра да установяват връзка, позволява обработката на големи съобщения и осигурява откриване на грешки и тяхното коригиране. Също така този интерфейс освобождава приложението от необходимостта да е наясно с детайлите на мрежата.

Windows Sockets (Winsock) интерфейс - Този интерфейс управлява входно/изходните заявки за Интернет приложения в среда на Windows. Winsock произлиза от интерфейса Berkeley UNIX sockets, който се използва за установяване на конекции със и обмен на данни между два програмни процеса в рамките на един и същ компютър или по мрежа.

Сесийният слой може също да изпълнява функции на сигурността и преобразуване на имена.

Транспортен слой

Транспортният слой изпълнява няколко важни функции и е важен елемент в мрежовите комуникации. Основното предназначение на този слой е да осигури надежден контрол на грешките и потока при пряката комуникация. Протоколите от транспортния слой осъществяват структурирането на съобщенията.

Транспортният слой следи за такива неща, като валидността на пакетите с данни, реда на следване и управлението, както и за обработката на дублирани пакети. Транспортният слой на приемащия край може да изпраща обратно потвърждение до изпращащия компютър, за да съобщи на изпращача, че пакетът е пристигнал. Това става

само ако транспортният слой използва ***ориентиран към връзката*** протокол за изпращане на съобщението.

Съществуват два типа протоколи, използвани от транспортния слой - връзково-ориентирани (с установяване на връзка, TCP) и безвръзково-ориентиран (без установяване на връзка, UDP).

Други важни концепции на транспортния слой са ***преобразуването на имена*** и ***портовете и сокетите.***

Транспортни протоколи TCP е ориентиран към връзката протокол, който работи в транспортния слой като част от протоколния стек TCP/IP. Услугите на този протокол изграждат връзка преди изпращането на данните и използват потвърждения за удостоверяване, че данните са пристигнали успешно до своето местоназначение.

Изпращането на пакет по куриерска поща с изискване за връщане на обратна разписка е пример за неговото действие.

Протоколът UDP (User Datagram Protocol), който също е член на комплекта TCP/IP, е не-ориентиран към връзката транспортен протокол. Безвръзково-ориентираните протоколи работят подобно на обикновената пощенска услуга. Поставянето на марка на писмото и неговото изпращане по пощата е пример, но в този случай не сигурно дали то ще достигне по получателя.

Безвръзково-ориентираните транспортни услуги се използват за изпращане на съобщения, които не са критично важни или които са къси и прости, и лесно могат да бъдат изпратени отново, ако бъдат изгубени. Например бродкастните съобщения, които се изпращат до всички компютри в една подмрежа, използват UDP. Предимството в случая се явява тяхната скорост; простотата и малкото натоварване, които водят до по-висока производителност.

Преобразуването на имената на компютрите (хостовете) в логически мрежови адреси е друга задача на транспортния слой. Както TCP/IP, така и IPX/SPX (Internet Package Exchange/Sequenced Packet Exchange) задават логически имена на мрежовите компютри и използват зададените логически адреси за идентифициране на компютрите в мрежата.

Портове и сокети

Многозадачността в мрежовите приложения е предимство, което модерните операционни системи имат пред по-старите такива (например MS-DOS); многозадачността позволява на потребителя в даден момент да изпълнява повече от една мрежова програма. Например можете да използвате Web браузър за достъп до Web сайт и в същото време софтуерът за електронна поща да сваля вашите e-mail съобщения.

Транспортният слой включва механизъм за разделяне на вашата входяща поща и отговора на заявката от страна на вашия браузър, когато и двете пристигат на един и същ мрежов адрес. За да осъществят това разделяне, протоколите от транспортния слой, като TCP и UDP, използват портове.

Протоколите от транспортния слой (TCP и UDP) задават номера на портове на всяко приложение. Това гарантира, че данните, предназначени за Web браузъра в един компютър, няма да бъдат изпратени на друго място.

Мрежов слой

Мрежовият слой е отговорен за доставяне на пакетите до техните местоназначения. Този слой управлява ***маршрутизирането (routing).***

Този слой също така управлява приоритетите на типовете данни (основата на QoS [Quality of Service]), което осигурява някакво ниво на гаранция за достатъчно мрежови ресурси за приложения, изискващи висока пропускателна способност - например за видео на живо.

Устройствата, които работят в мрежовия слой, включват маршрутизатори и Layer 3 суичове.

Канален слой

Layer 2 бе дефиниран като канален слой (data link layer) в оригиналните спецификации на OSI. Този слой е разделен допълнително на два подслоя:

- Контрол за достъп до преносната среда (Media Access Control - MAC)
- Контрол на логическите връзки (Logical Link Control - LLC)

MAC подслоят обработва въпросите по физическото адресиране. Реално физическият адрес, който в една Ethernet или Token Ring мрежа представлява

шестнадесетично число, постоянно записано в чипа на мрежовата интерфейсна карта (NIC), се нарича MAC адрес.

MAC адресът се записва като 12 шестнадесетични цифри, подредени по двойки, като всяка двойка е отделена с двоеточие (например 17:A4:2C:43:2F:09).

Тези 12 цифри в шестнадесетична бройна система представят 48-битови (т.е. 6-байтови) двоични числа. Първите 3 байта съдържат кода на производителя, който се задава от Института на инженерите по електроника и електротехника (IEEE). Последните 3 байта се задават от производителя и идентифицират конкретната карта.

MAC адресът, или физическият адрес, се означава също като хардуерен адрес. Той се различава от логическите адреси (т.е. от IP адреса в TCP/IP мрежа) по това, че не може да бъде променян. Логическият адрес се задава с помощта на софтуер и лесно може да бъде модифициран. И двата идентифицират местоположението на компютъра в мрежата.

На теория никога не трябва да има две карти с едни и същи MAC адреси. Но н практика производителите допускат грешки, като създават карти с дублиращи се адреси. Освен това някои производители започнаха да рециклират (използват отново) своите номера. Дублираните MAC адреси предизвикват проблеми ако две карти с един и същ адрес се намират в една и съща мрежа.

Методът за контрол на достъпа до преносната среда разпределя достъпа на компютрите до мрежата. Контролът на достъпа до преносната среда се извършва в MAC подслоя..

LLC слоят и логическата топология В LLC подслоя се дефинира логическата топология на мрежата. В редица случаи логическата топология може да не е същата като физическата.

Този подслой отговаря също за осигуряване на връзка или интерфейс между MAC подслоя, който следва след него, и мрежовия слой над него.

Физически слой

Това е мястото, където данните и хедърите добавени от другите по-горни слоеве, биват транслирани в сигнали, които могат да бъдат предавани и прехвърляни в кабела, за да започнат пътуването си по мрежата (или в случай на безжична преносна среда,

изпращани като радиовълни или по други начини). Протоколите от физическия слой превръщат всички тези 0-ли и 1-ци в електрически импулси или светлинни импулси.

Физическият слой се занимава с проблемите, свързани с ***предаването на сигнали,*** а именно:

- Аналогово или цифрово предаване на сигнали
- Теснолентова или широколентова технология на предаване
- Асинхронно или синхронно предаване
- Мултиплексиране

Друг проблем, решаван от физическия слой, е мрежовата топология. Във физическия слой това се отнася за физическото разположение на мрежата, за разлика от логическата топология, която се определя в каналния слой.

Устройствата от физическия слой са тези, които осъществяват основното предаване на сигнали. Мрежовите интерфейсни карти работят във физическия слой както повторителите и хъбовете. Тези хъбове са хъб за мрежа Token Ring, който се означава като ***устройство за множествен достъп*** (MSAU), и пасивните, активните и интелигентните хъбове. Тук не влизат ***комутиращите хъбове,*** които действат в каналния слой. (Понякога „MSAU“ се записва като „MAU“).

Мрежови интерфейсни карти (NIC) Мрежовата интерфейсна карта (NIC) е основен компонент, който най-общо се използва за изграждане на комуникация между компютри. Казвам „най-общо“, защото има ситуации, при които даден компютър може да участва в мрежа и без NIC. Такива случаи са ***отдаленият достъп (remote access),*** в който се използват модем и телефонни линии за свързване към мрежата, и простата връзка между два компютъра с помощта на специален сериен кабел, наречен ***нулев модем.*** Мрежовите карти отговорят за подготвяне на данните, които трябва да бъдат предадени по мрежовата преносна среда.

Мрежовите интерфейсни карти се разпространяват в множество различни типове и избирането на правилната карта може да бъде предизвикателство. Изборът на мрежова карта зависи от:

Архитектура на мрежата - мрежовата артата трябва да бъде предназначена за работа с архитектурата, която се използва в определена мрежа. Например една Token Ring карта не може да работи в Ethernet мрежа.

Тип на преносната среда (медията) - Ethernet мрежите могат да използват тънък коаксиален кабел, кабел с усукана двойка и дори кабел с оптично влакно. Мрежовата карта трябва да има правилен тип конектор, за да може да бъде свързана към преносната среда на конкретна мрежа. (Ако е налична безжична конекция, картата трябва да бъде предназначена за съответния тип безжична комуникация - **инфрачервена, лазерна** или **радио**.)

Архитектура на шината - Картата трябва да бъде предназначена за работа с архитектурата, използвана на определен компютър. Трябва да се има предвид съответния тип шина и интерфейс за да може картата да работи в компютъра.

Скорост - Ethernet мрежа, работеща по кабел Cat 5 с неекранирана усукана двойка, може да бъде пусната на скорости 10 Mbps или 100 Mbps. Token Ring мрежа, използваща IBM кабел, може да бъде пусната на 4 Mbps или на 16 Mbps. Трябва да се поддържа съответствие между скоростта на картата и останалите мрежови компоненти.

Мрежови приемопредаватели

Приемопредавателят (трансивърът) се наричан така, защото е устройство, което предава и приема. Мрежата 10Base5 (thicknet) използва ***външен приемопредавател,*** представляващ устройство, свързано към мрежовата интерфейсна карта чрез AUI конектор (наричан също DIX конектор). AUI конекторът, който е от 15-изводен DIN тип, позволява конвертирането на различните типове преносни среди чрез свързване на външния приемопредавател за желания тип кабел.

Всички мрежови карти използват приемопредавател, който се вгражда в картите, предназначени за използване в мрежи 10Base2, lOBaseT или 100BaseT.

Повторители Повторителят свързва две дължини (два сегмента) на мрежовия кабел и усилва сигнала, предавайки го от първия към втория кабелен сегмент. Повторителят ви позволява да увеличите дължината на мрежовия кабел повече, отколкото е възможно по друг начин, като решите проблема със затихването (загубата на сигнала), което възниква при увеличаване на разстоянието.

Повторителите не филтрират сигналите. Те предават както данните, така и шума. Ето защо могат да бъдат използвани само ограничен брой повторители; в противен случай възникват проблеми в комуникацията. Използването на повторители в мрежа с коаксиален кабел се установява с помощта на правилото 5-4-3.

Хъбове или така наречените ***концентратори,*** служат като точка на централна точка на свързване. Повечето хъбове реално представляват ***множествени повторители.*** Докато един повторител обикновено има само два порта, хъбът най-общо има от четири до двадесет и повече порта. Хъбовете се използват най-масово в мрежите Ethernet, lOBaseT или 100BaseT, макара че има и други мрежови архитектури, които ги използват.

Хъбовете се разпространяват в три основни типа:

Пасивни - Пасивният хъб служи само като точка за физическо свързване. Той не се нуждае от електрическо захранване, защото той не усилва и не изчиства сигнала, а просто го препредава. Днес пасивните хъбове не са много разпространени.

Активни - Активният хъб трябва да бъде включен към електрическо захранване, защото използва енергия за усилване на входния сигнал, преди да го предаде обратно до другите портове. Активният хъб е мно- гопортов повторител и е най-често срещания тип хъб. Обърнете внимание, че всички Ethernet хъбове изискват електрическо захранване и поради това се класифицират като активни хъбове.

Интелигентни или „smart“ - Тези устройства функционират като активни хъбове, но включват също микропроцесорен чип и диагностични възможности. Те са по-скъпи от активните хъбове (без допълнителни възможности), но могат да бъдат полезни в ситуации на отстраняване на неизправности.

Друго специално устройство, което често се означава като Token Ring хъб, реално е устройството за множествен достъп - MSAU. Уникалната възможност на MSAU е логическата кръгова топология, която то създава благодарение на връзките вътре в самото устройство. Няколко MSAU устройства могат да бъдат свързани за осигуряване на непрекъснат кръгов път, по който да пътува сигналът

3.2 Мрежови стандарти и документи

Моделите не са единствените стандарти и спецификации, по които се разработват мрежови компоненти. Множество организации за стандартизация публикуват спецификации за свързан с мрежите хардуер и софтуер. Разбира се, тези спецификации не са ***закон.*** Организациите по стандартизация не са правителствени институции и не могат да налагат задължително съответствие към дадени стандарти. Производителят е свободен да се отклонява от стандартите толкова колкото желае, но не е в негов интерес да прави

това. Нестандартни продукти, които работят само с други продукти, произведени от същия производител, по принцип са непопулярни.

В ранните дни на компютърните мрежи производителите безнаказано създаваха такива продукти, но днешната мрежова индустрия изисква съвместимост.

ISO дефинира стандартите като „документирани споразумения, съдържащи технически спецификации или други точни критерии, които трябв да бъдат използвани задължително като правила, указания или дефиниции на характеристики, за да гарантират, че дадени материали, продукти, процеси и услуги отговарят на целта, за която са предназначени“.

Пазарът е една от причините производителите да спазват стандартите, но има и други предимства. Например стандартите осигуряват указания, които улесняват проектирането и производството на продукти, а от гледна точка на потребителя стандартизацията осигурява надеждност на продуктите и услугите.

Организации за стандартизация

ISO съществува от дълго време и е добре позната организация за стандартизация, но тя не е единствената организация, която осигурява стандартизирани спецификации за компютърни и мрежови компоненти.

Някои от главните международни организации за стандартизация са следните:

- ISO - http://www.iso.ch
- ITU - http//www.itu.int
- IETF - http://www.ietf.org/home.html
- IEEE - http://standards.ieee.org

Стандартите са описани в специализирани документ наречени RFC (Request for comment).

Моля, отговорете на контролните въпроси:

1. *Какво представлява процеса на декапсулация?*
2. *Кои нива извършват кодиране? Знаете ли някакъв код, използван в мрежите?*
3. *В кои нива на модела OSI се извърва определен вид преобразуване и какво е то?*
4. *Каква е целта на правилото 5-4-3?*
5. *Какво е предназначението на RFC1700?*

Раздел 4

Мрежови протоколен стек TCP/IP. Мрежови услуги .

Ключови думи и съкращения

Протоколен стек	**Протокол**
Мрежова услуга	**TCP**
FTP	**UDP**
DNS	**IP**
SMTP	**ICMP**
ARP	**RARP**

4.1. Протоколен стек TCP/IP

Съкращението TCP/IP (Transmission Control Protocol/Internet Protocol) е общо наименование на съвкупност от протоколи.

Основната цел на тази съвкупност от протоколи е да се зададе възможност за осъществяване на връзки в компютърните мрежи, предлагащи универсални мрежови услуги. В зависимост от технологията на изпълнение всяка комуникационна мрежа притежава собствен мрежов интерфейс, представен под формата на програмен интерфейс и поддържащ базови комуникационни функции, наречени примитиви. Комуникационните услуги се изграждат на основата на софтуер, който осъществява връзката между физическата мрежа и съответното приложение. По този начин сервизните функции (услугите) поддържат дефиниран интерфейс за мрежовите приложения, който е независим от намиращата се на по-ниско ниво физическа структура на мрежата. По същество архитектурата на физическото ниво е скрита за потребителя.

Друга задача, която се поставя за комуникацията между отделните системи е връзката между системи с различна физическа структура да се представи на потребителя като съвкупност от една единна мрежа. За да се даде възможност да се свържат две мрежи, е необходима компютърна система, притежаваща интерфейс и в двете. Такава система се нарича маршрутизатор (рутер, router). Терминът IP маршрутизатор (IP рутер) указва, че устройството, осъществяващо връзката между двете мрежи, е част от IP слоя на протоколния стек TCP/IP.

Маршрутизаторът се характеризира със следните особености:

- от гледна точка на мрежата, той е обикновена компютърна станция – хост;

- от гледна точка на потребителя, рутера е невидим. Потребителят забелязва единствено работата между крайните точки в мрежата.

Компютърна система, която е включена към мрежата се обозначава като хост. За да се идентифицира еднозначно в мрежата, на всеки хост се присъединява адрес, наречен IP адрес. Ако даден хост притежава множество мрежови интерфейсни адаптери, т.е. той участва в няколко мрежи, всеки един от тях притежава свой собствен уникален адрес. Всеки IP адрес се състои от две части – мрежов номер и адрес на отделния хост в рамката на мрежата. Мрежовият номер е част от IP адреса и се разпределя централно. Отговорността за разпределяне на отделните адреси на компютрите е в самата организация, която притежава съответната IP мрежа.

4.1.1 Модел на TCP/IP

Моделът TCP/IP се изгражда в съответствие с еталонния модел на слоеве. На фиг.1.1 е показано съответсвието на еталонния модел с модела на TCP/IP.

Всеки един протоколен слой представлява съвкупност от мрежови функции:

Потребителски слой – предоставя интерфейс за потребителските приложения, използващи TCP/IP за комуникация. Приложението представлява потребителски процес, който работи съвместно с друг процес на същия или на различен хост. Пример за такива приложения са TELNET, FTP, SMTP и др. Интерфейсът между отделните приложения и транспортния слой е дефиниран чрез комуникационни портове и сокети;

Транспортен слой – реализира връзки от тип крайна точка – крайна точка, като множество приложения се обслужват едновременно. Транспортният слой отговаря за осъществяване на сигурен обмен на информация. Наличните два протокола за осигуряване на преноса са TCP и UDP (User datagram protocol). Протоколът UDP поддържа отделните мрежови услуги чрез несвързани с информационния поток комуникации. По този начин, приложенията използващи UDP като транспотен протокол, могат да реализират собствен контрол на потока от информация. Обикновено UDP се използва при приложения, които се нуждаят от бърз транспортен механизъм.

Мрежов слой – този слой поддържа виртуално изображение на мрежата. Той представлява най-горният слой на физическата мрежова архитектура. IP (Internet protocol) е основният и най-важен протокол на този слой. Той не е свързан с отделния информационен поток. Протоколът не поддържа механизми за осигуряване на надеждни

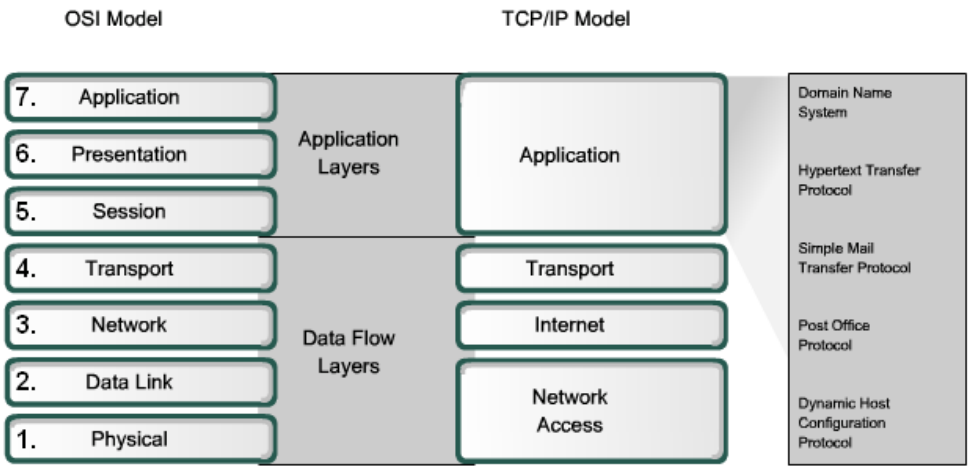
комуникации, контрол на потока данни и възстановяване при грешки. Тези функции е необходимо да се реализират на по-високо ниво на комуникация. Част от информацията, обменяна между отделните компютри, е информация за маршрутизиране. Тази информация дава възможност отделните съобщения да бъдат правилно разпределени към тяхното предназначение. Тези функции за маршрутизиране се осигуряват от IP протокола. Други по-важни протоколи на мрежово ниво са ICMP, ARP и RARP.

Слой на мрежовия интерфейс – той съответства на каналния слой в еталонния модел. Дава възможност за връзка към съответната мрежова апаратна част. Мрежовият интерфейс, в зависимост от изпълнението си, може да поддържа, или не, механизми за надеждно разпределение на информационния поток. Реализацията му може да бъде пакетно-ориентирана или поточно-ориентирана. На практика TCP/IP не дефинира определен протокол за това ниво, което дава възможност за по-голяма гъвкавост на изградената система. Примери за изпълнение на този слой са IEEE 802.2, ATM, FDDI и др.

Най-високото ниво при модела TCP/IP са приложните протоколи. Те комуникират с приложения на друг мрежов хост и представляват видимите за потребителите интерфейси от съвкупността на TCP/IP протоколите.

Потребителските протоколи притежават някои общи характеристики: могат да бъдат създадени от отделни потребители, или могат да представляват стандартизирани приложения.

- TCP/IP приложно ниво притежава приложни програми като:
- TELNET – осигуряващ интерактивен достъп до отдалечения хост;
- FTP (File Transfer Protocol) – осигуряващ високоскоростен трансфер на файлове от дисково устройство към друго подобно;
- SMTP (Simple Mail Transfer Protocol) – използва се като мрежова пощенска система.



Фиг. 4.1 Съответствие на модели и протоколни стекове

Това са само някои от разпространените протоколи на потребителско ниво, но съществуват и много други. Всяко отделно изпълнение на TCP/IP включва в себе си по-голяма или по-малка съвкупност от потребителски протоколи. Те използват или TCP или UDP като транспортен механизъм. Важна особеност е, че UDP е ненадежден протокол и не поддържа механизми за контрол на потока данни. В такива случаи приложението трябва да реализира собствени механизми за възстановяване при грешки и за реализация на контрол на информационния поток. В много случаи е по-лесно да се създават приложения, използващи вградения в TCP механизъм за контрол на информационния поток. Повечето приложения използват този подход, но трябва да се спомене, че използването на UDP като транспортен протокол дава възможност за по-висока производителност при осъществяване на комуникацията в следствие на редуцираната управляваща информация.

Както беше споменато TCP/IP представлява свързан с информационния поток протокол от типа крайна точка – крайна точка. Мрежовите приложения, изградени на базата на протоколния стек TCP/IP използват много често модела клиент/сървър (фиг.4.2) за комуникационен модел. Сървърът трябва да се разглежда като приложение, което предлага определени мрежови услуги (сервизни функции) на потребителите на мрежата. Клиентът е тази част от потребителската програма, която е реализирала определени заявки за обслужване от страна на сървърното приложение. Възможно е едно приложение да притежава и двете части. Тези две части могат да бъдат изпълнявани на една и съща компютърна система (хост) или на две различни системи.

Фиг. 4.2 Схема на мрежа тип клиент - сървър

Потребителите използват обикновено клиентската част на приложението, която прави заявки за отделни услуги или изпраща към сървър информация, използвайки протокола TCP/IP като транспортно средство.

Сървърното приложение се явява програма, която получава заявка, изпълнява заявените услуги (сервизни функции) и изпраща обратно резултатите като отговор. Сървърът може да обслужва множество заявки по едно и също време.

Някои от сървърите очакват заявки на общо познатите портове, като по този начин клиентът знае предварително сокета (комбинацията IP адрес и порт за връзка), към който трябва да се отпрати заявката. От страна на клиента се използват произволно избрани портове за комуникация, докато за заявената услуга се включва нужния за целта порт в сокета. Клиент, който желае да реализира комуникация със сървър, но не познава общо известните портове, трябва да притежава допълнителен механизъм за определяне към кой точно да бъде отправена заявката. Такъв механизъм може да се реализира посредством регистрирана карта на комуникационните портове, използваща общо познати такива.

Както беше изяснено формирането на комуникационна мрежа чрез свързването на съвкупност от мрежи (повече от две) е възможно чрез маршрутизатор (рутер). Тук е необходимо да се разбере разликата между различните типове маршрутизатори – рутери (routers), мостове (bridges) и шлюзове (gateways).

Мостове (bridge) – Тези устройства свързват отделни сегменти на локални компютърни мрежи на ниво мрежов интерфейс. Всеки bridge изпълнява функция за пренасочване на кадрите от подниво MAC (Media Access Control) и е независим от протоколите на по-високо йерархично ниво, включително и подниво LLC (Logical Link Control). Всеки bridge може да бъде прозрачен за IP. Това се получава в случаите, когато

даден мост използва IP като комуникационен протокол, за да комуникира с друг, намиращ се на мрежов сегмент, свързан с bridge посредством изпращане на дайтаграми.

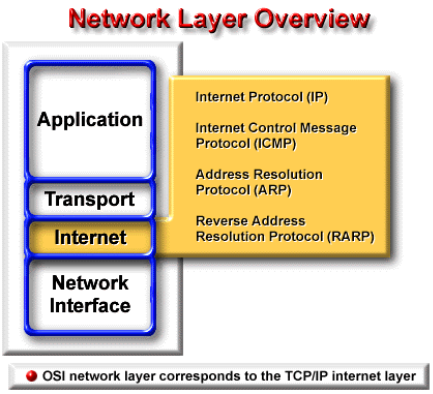
Рутери (router) – Устройствата свързват отделни сегменти на мрежово ниво и маршрутизират отделни пакети между тях. Всеки рутер трябва да може да разбере адресната структура, асоциирана с мрежовия протокол, да поддържа и взема решения как да маршрутизира съответния пакет или да го пренасочва. Рутерите имат възможност да определят най-добрия път за трансфер на информация и оптималната големина на пакета. Базовите рутиращи функции са реализирани в IP протокола. Съвременните рутери могат да изпълняват доста по-сложни функции от тези, които са дефинирани в IP.

Шлюзове (gateways) – Понятието gateway много често се смесва с входно/изходната точка при IP рутиране. В много случаи понятието gateway трябва да се употребява за реализация на входно/изходна точка на по-високо ниво за комуникация от рутер. Понякога такива устройства се използват за адресно преобразуване между отделни комуникационни мрежи. Използването на такива входно/изходни точки обикновено ограничава броя на конекциите между приложения, използващи ги за комуникация. Gateway е непрозрачен за IP комуникации. Ако определен хост изпрати дайтаграма през gateway, обикновено се реализира комуникация само до него, но не и прозрачно през него. Много често с това понятие се свързва и защитата, реализирана посредством „огнена стена" (firewall). Тя дава възможност за частично или пълно ограничаване на достъпа от една мрежа или група мрежи към друга такава.

4.1.2 Мрежово ниво

Протоколният стек IPv4 е в основата на изграждането на глобалната мрежова среда INTERNET, както и за проектирането на IP-базирани ведомствени мрежови конфигурации - INTRANET мрежови среди.

Мрежовото ниво на протоколния стек TPC/IP включва протоколите, предствени на фиг.4.3:



Фиг. 4.3 Протоколи на мрежово ниво

IP (Internet Protocol) е дейтаграмен мрежов протокол, осигуряващ несвързано мрежово обслужване. IP е протокол, който осигурява маршрутизирането на дейтаграмите от адреса-източник до целевия адрес, без да носи отговорност за достоверността на преноса на информацията и отстраняването на възникнали при предаването грешки. Протоколът поддържа йерархична адресна логика и осигурява глобален обмен на еднопосочни съобщения (дейтаграми).

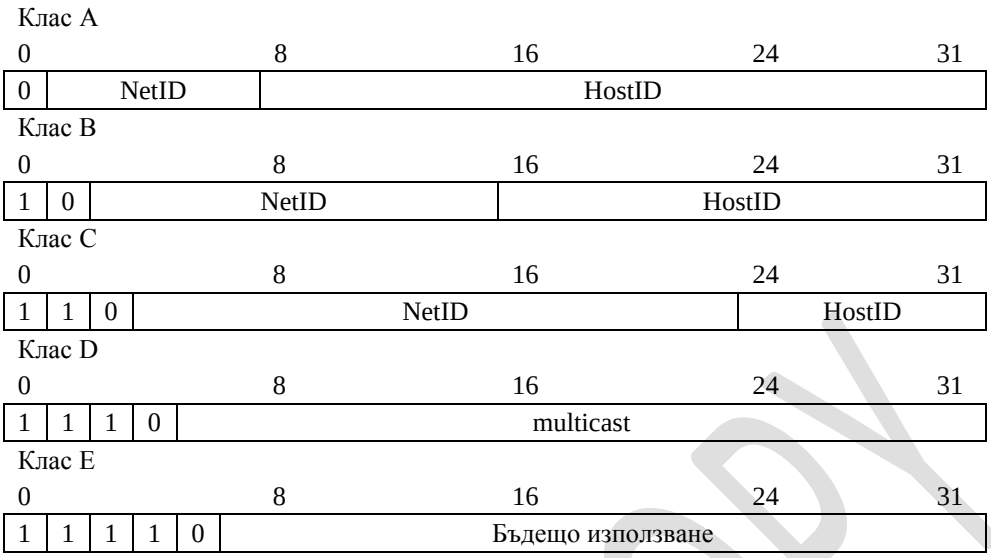
ICMP (Internet Control Message Protocol) е протокол за обмен на служебни съобщения на мрежово ниво. Използва се за управление и диагностика на състоянието на мрежовите съединения и обработване на аварийни ситуации.

ARP (Address Resolution Protocol) е протокол за намиране на адресно съответствие по валиден IP адрес. Той съпоставя IP (мрежовия адрес) на системата с нейния канален (физически) адрес (MAC-адрес).

RARP (Reverse Address Resolution Protocol) е протокол за намиране на адресно съответствие по валиден MAC адрес. Този протокол извежда съответствието между известен канален (физически) адрес (MAC-адрес) и присвоения на системата IP-адрес (мрежов адрес).

Структура на IP адреси

Адресната логика на протокол IP е йерархична. Адресното поле на протоколната спецификация е 32-битово като са дефинирани 3 базови формата (класове) адреси A, B, и C. Всеки клас се интерпретира и използва за адресиране в условията на различни по структура и размерност мрежови конфигурации - фиг.4.4



Фиг.4.4 Класове IP адреси

Първите 4 бита от адреса определят класа на мрежа. Останалите 24 бита се разделят на две части: мрежов идентификатор (network identifier - netid) и идентификатор на краен компютър (host identifier - hostid).

Адресите от клас A са със 7-битово поле на netid и 24-битово поле за hostid.

Адресите от клас B са с 14-битово поле на netid и 16-битово поле за hostid.

Адресите от клас C са с 21-битово поле на netid и 8-битово поле за hostid.

Клас A-адресите се използват при мрежови конфигурации с голям брой крайни компютри (до 224), докато клас C-адресите позволяват идентификация на голям брой подмрежи с относително малко крайни компютри във всяка от подмрежите (до 256). Един типичен пример за клас A мрежа е ARPANET, а пример за клас C мрежа е една малка корпоративна мрежа в завод, училище, общинска администрация и т.н.

Когато полето hostid е нула, то адреса се нарича адрес на мрежа (подмрежа). Когато полето hostid е запълнено с 1, то адреса, който се формира адресира едновременно всички крайни компютри в текущата мрежа. Такъв адрес се нарича общ или групов адрес (broadcast address).

За целите на по-ефективното и разбираемо представяне на IP адресите, 32-битовия адрес е разделен на 4 октета, като стойността на всеки октет се представя с десетичния си еквивалент.

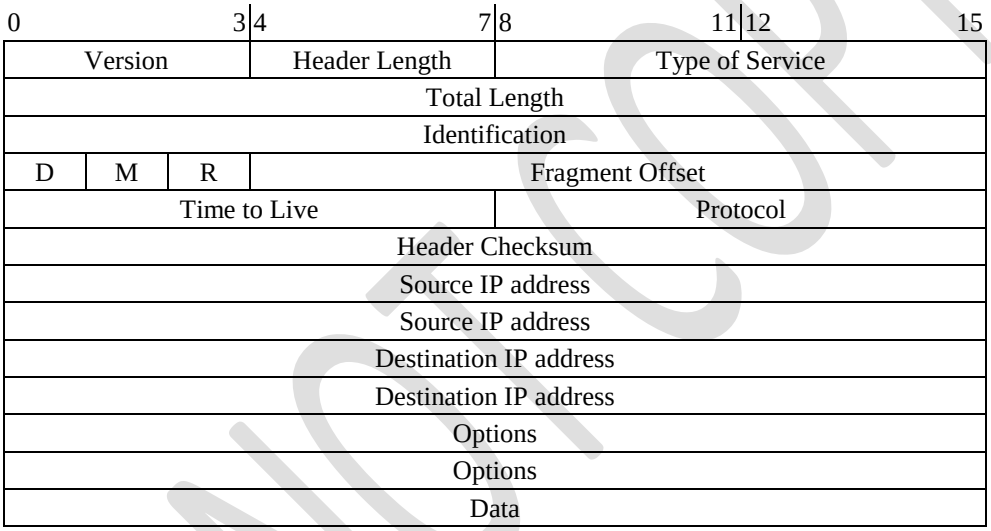
Октетите се разделят с точка, например

00001010 00000000 00000000 00000000 = 10.0.0.0 = Клас A : netid = 10
(ARPANET)
10000000 00000010 00000011 00000011 = 128.2.3.3 = Клас B : netid=128.2
hostid=3.3
11000001 00000000 00000101 11111111 = 193.0.5.256 = Клас C : netid= 193.0.5
Hostid = до всички крайни компютри в мрежа 193.0.5

Формат на IP дейтаграмите

Мрежовият протокол IP поддържа формат на пакетите (дейтаграмите), предствен на фиг.4.5

Формат на IP пакета – битова последователност 0 – 15



Фиг. 4.5 Формат на IP пакета

Описание на полетата на IP пакета (**datagram**):

1) Version – версия;
2) Header Length – дължина на заглавната част;
3) Type of Service – тип на услугата;
4) Total Length – обща дължина;
5) Identification – идентификация;
6) Fragment Offset – отместване на фрагмента;
7) Time to Live – време на живот;
8) Protocol – протокол;
9) Header Checksum – контролна сума на заглавната част;
10) Source IP address – IP адрес на източника;
11) Destination IP address – IP адрес на получателя;
12) Options – допълнение;

13) Data – потребителски данни.

1) ***Version*** – версия съдържаща текуща версия на IP протокола. Текущата версия е 4-та - IP v.4
2) ***Header Length*** – дължина на заглавната част – съдържа действителния размер на заглавието на пакета, представен като брой 32-битови думи. Минималната дължина на пакета, ако не се използват допълнителните полета, е пет 32-битови думи.
3) ***Type of Service*** – тип на услугата – поле, в което компютърът-източник заявява тип на мрежовата услугата за текущата приложна сесия: висока надеждност; минимално времезакъснение; висока пропускателна способност; прилагане на схема с приоритети.
4) ***Total Length*** – пълна дължина на пакета (заглавната част и потребителските данни). Максимално допустимия размер на пакета е 65 535 бита
5) ***Identification*** – идентификация – обикновено едно съобщение се предава под формата на поредица от няколко пакета. Това поле служи за идентификация за принадлежност на пакетите към едно и също приложно съобщение.

Битове D,M и R – свързани са с т.нар. фрагментация на данните.

D – ***Don't Fragment*** – не фрагментирай този пакет. Ако този флаг е усановен в "1" при достигане на мрежа с по-малък размер на пакета, текущия пакет няма да бъде фрагментиран, а ще бъде отхвърлен от тази мрежа. Налага се маршрутизиране по друг път.

M – ***More Fragments*** – когато бит M е установен в "1", то текущия пакет е част (един фрагмент) от по-голям пакет и след него следват още фрагменти.

R – ***Reserved*** – резервиран флаг.

6) ***Fragment Offset*** – отместване на сегмента. Записва се информация за позицията на полето за данни от текущия фрагмент в оригиналния пакет. Отместването от началото на съобщението се представя като число кратно на 8 октета.
7) ***Time to Live*** – време на живот. Стойността се установява във възела-източник и се намалява при преминаването през всеки следващ мрежов възел. След достигане на стойност 0, пакетът се унищожава.
8) ***Protocol*** – записва се типа на протокола от по-"високо" ниво, който се съдържа в тялото на пакета. Използва се за протоколна идентификация в целевия възел.
9) ***Header Check sum*** – контролна сума.
10) ***Source IP address*** – IP адрес на източника (32 битово число).
11) ***Destination IP address*** – IP адрес на получателя (32 битово число).

1 – 11 са задължителни полета.

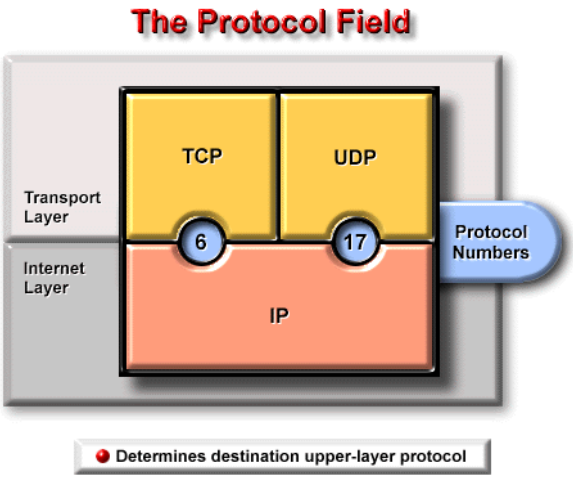
12) ***Options*** – допълнителни възможности. Формата им зависи от приложението:
    - за сигурност (Security) – полето за DATA от пакета е възможно да се криптографира. В Options се специфицира типа на кодирането.
    - Source Routing – маршрутизиране от източника. В Options се описва маршрута и по този начин се изключва маршрутизиращата логика във възлите.

- Route Recording – запис на маршрута. В Options се записва информация за маршрута (трасиране на маршрута).
- Time Stamp – маркер за време – при желание да проверим времето за транспорт на пакета

Първият байт на полето Options определя текущо използваната допълнителна възможност.

Протоколно взаимодействие

На фиг.4.6 е представено взаимодействието на базовия мрежов протокол IP и свързаните с него транспортни протоколи, осигуряващи свързано мрежово обслужване за приложните заявки.



фиг. 4.6 Номера на транспортни протоколи

Осигуряването на ориентирано към връзката мрежово обслужване се реализира в този протоколен стек на транспортно ниво, тъй като базовият мрежов протокол е дейтаграмен, т.е. неориентиран към връзката. Във взаимодействието участват два основни транспортни протокола:

TCP (Transmission Control Protocol) е ориентиран към връзката транспортен поротокол с две основни функции:

- да осъществява управление на предаването на информационни потоци като открива грешки, получени или неполучени пакети и осигурява тяхното повторно предаване;
- мултиплексиране на точките на достъп до мрежово обслужване при поддържането на приложните заявки.

Протоколът IP осигурява еднопосочното предаване на дейтаграми от адреса-източник до целевия адрес. Транспортният протокол TCP осигурява управлението на потока кадри и отстраняване на грешки.

На транспортното ниво в разглеждания протоколен стек, освен TCP, оперира и протокол за обмен на потребителски пакети UDP (User Datagram Protocol). Този транспортен протокол е дейтаграмен, т.е. не предоставя механизъм за установяване на връзка и се използва за услуги, свързани с управление на мрежовите устройства и обмен на служебни съобщения.

Протокол ICMP

На мрежово ниво в разглеждания протоколен стек функционира протокола ICMP (Internet Control Message Protocol)

Протоколните съобщения на ICMP се пренасят в DATA-полето на IP-дейтаграмите и се използват за обмен на информация за грешки и управляваща информация.

Протоколът използва множество от командни примитиви, които дават информация за състоянието на мрежовото съединение:

- Destination Unreachable (недостижим IP адрес);
- Time to Live Exceeded (изтекло време на "живот");
- Parameter Problem (проблеми при съставянето на дейтаграмите);
- Redirect (пренасочване на дейтаграми);
- Echo (заявка тест на IP адрес);
- Echo Reply (потвърждение за тест на IP адрес);
- Timestamp (заявка за времеви маркер);
- Timestamp Reply (потвърждение на времеви маркер)
- Information Request (заявка за информация за състояние);
- Information Reply (потвърждение за информация за състояние);
- Address Request (заявка за адресна информация);
- Address Reply (потвърждение за адресна информация).

Тази служебна информация се използва от приложенията за целите на анализ на състоянието на мрежовото съединение и обработване на ситуации на отказ.

Протоколи ARP и RARP

Един от основните проблеми при реализирането на мрежови съединения между компютри, включени в локални мрежови конфигурации, е проблема за взаимодействието между мрежови и физически адреси. Глобалният пренос се осъществява по мрежов адрес,

докато мрежовия пакет, се транспортира в локалната мрежа в съответствие с конкретния протокол от канално ниво.

ARP се използва за построяване на необходимата за мрежовото съединение таблица на съответствието между присвоените на компютрите от локалната мрежа IP-адреси и MAC-адресите. Тази таблица позволява установяването на мрежови съединения, основани на преносната среда в локалната мрежа, например IEEE 802.3 Ethernet. При известен целеви IP адрес, за установяване на съединението е необходимо да се извлече от ARP-таблицата, съответстващия му MAC-адрес. Ако в ARP таблицата няма информация за това съответвествие, то се изпраща IP-дейтаграма с целеви адрес, търсения целеви адрес, която се пакетира в broadcast MAC-кадър. Този кадър достига до всички MAC-адреси в локалната мрежа, т.е достига и до компютъра, чийто IP адрес е целевия IP адрес. Компютърът потвърждава дейтаграмата, като на канално ниво се формира кадър с физически адрес на получател, адреса на инициатора на мрежовото съединение и канален адрес-източник – търсения MAC-адрес. След пристигане на потвърждението в иницииращия компютър, неговата ARP-таблица се актуализира с липсващия MAC-адрес и са осигурени условията за установяване на мрежово съединение в MAC-преносната среда.

Протоколът RARP (Reverse Address Resolution Protocol) е "обратен" по функционалност на ARP. При този протокол се решава обратната задача, по известен MAC-адрес да се получи информация за съответстващия му IP-адрес. Използва се аналогичен подход, като се изпраща broadcast IP-дейтаграма, която достига мрежовото ниво и в потвърждението се съдържа търсения IP адрес.

4.2 Транспорни протоколи

Транспортното ниво се явява ниво за синхронизация, докато мрежовото ниво е нивото на информационния пренос, определен от ограниченията на комуникационната подсистема.

Транспортното ниво поддържа приложните заявки за обмен на информация и в средата на ограниченията на мрежовото ниво, осигурява заявеното качество на обслужване на приложните процеси. Транспортното ниво има за задача да осъществи прозрачен обмен на данни между сеансовите обекти и да ги освободи от изпълнението на функции по организиране на ефективното и надеждно предаване на данни.

Транспортният слой определя параметрите на качеството на мрежовото обслужване при предаването на данни, производителността на мрежата, подходящо мултиплексиране на мрежовите съединения и др. Тези параметри отчитат заявеното от обектите на сеансовото ниво качество на обслужване, от една страна, и от друга, отчитат реалните характеристики и възможности на комутационната подсистема, управлявана от мрежовия слой.

Функционалността на транспортното ниво е свързана с:

- мултиплексиране на точките на достъп до мрежовото съединение – установяване на няколко транспортни съединения на база на едно мрежово съединение;
- контрол на качеството на обслужване – следи за достоверното предаване на информацията, управлението на потока кадри, буфериране, откриване и корекция на грешки, контрол на времевите характеристики на информационния пренос и запълването на пропускателната способност на мрежовите съединения;
- установяване, поддържане и разпадане на транспортните съединения.

Транспортното ниво има синхронизиращи функции при използването на услугите на мрежовите съединения при зададено качество на обмена, зададено от сеансовото ниво.

“Високите” нива са част от операционната система, под управлението на която работи компютъра, или са приложение за операционната система, докато транспортното ниво е относително независимо от локалната операционна система, тъй като при него функционалността се определя от комуникационната подсистема (първите три нива от еталонния модел). Транспортното ниво се организира в локалната архитектура като самостоятелен елемент в състава на мрежовото системно програмно осигуряване.

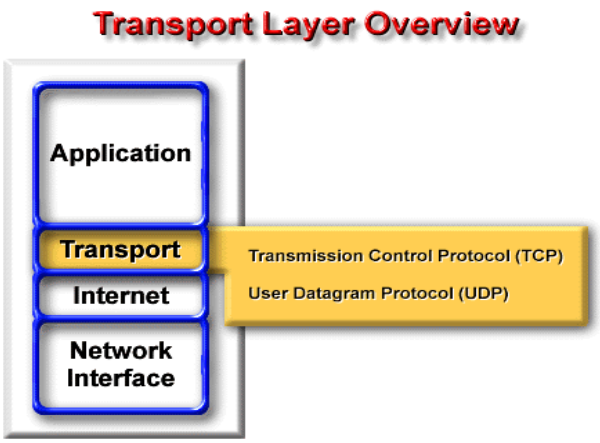
От архитектурен аспект транспортното ниво е първото от нивата, което реализира съединение точка – точка (Point to Point), от гледна точка на приложенията.

Съединението между приложните процеси се реализира на базата на транспортното ниво. На приложенията се предоставя за използване виртуално съединение, като комуникацията в “ниските” нива остава прозрачна. Независимо от разстоянието между двата крайни компютъра, функционалността на транспортния протокол е една и съща.

Всички приложно-ориентирани нива от еталонния модел се основават на транспортното, като достоверна комуникационна среда.

Транспортното ниво трябва да осигурява баланса между изискванията за комуникационни услуги на приложните нива и реалните възможности на мрежата.

В TCP/IP - протоколния стек, транспортният слой е изграден от два протокола TCP (Transport Control Protocol) и UDP (User Datagram Protocol) – фиг.4.7.



фиг. 4.7 Транспортни протоколи

4.2.1 Транспортен протокол TCP (Transport Control Protocol)

Интерфейсът между приложните програми (ПП) и TCP/IP услугата за надеждна доставка може да се характеризира с 5 основни свойства:

Ориентираност към потока - когато две ПП (потребителски процеси) си обменят големи обеми данни, данните се разглеждат като потоци от битове, разпределени в 8-битови октети, наричани обикновено байтове. Услугата за доставка на поток от страна на получаващата машина предава на получателя точно същата последователност от октети, които подателят е предал на предаващата машина;

Виртуална връзка - осъществяването на пренос на поток е аналогично на осигуряването на телефонен разговор. Преди да започне преноса, двете ПП се свързват със своите операционни системи (ОС) и ги информират за желанието си да осъществят пренос на поток. По принцип, едната ПП прави "повикване", което трябва да бъде прието от другата ПП. Софтуерът на протоколите в двете ОС се свързват чрез обмен на съобщения през мрежата, като проверяват и дават разрешение (authorization), след което двете страни

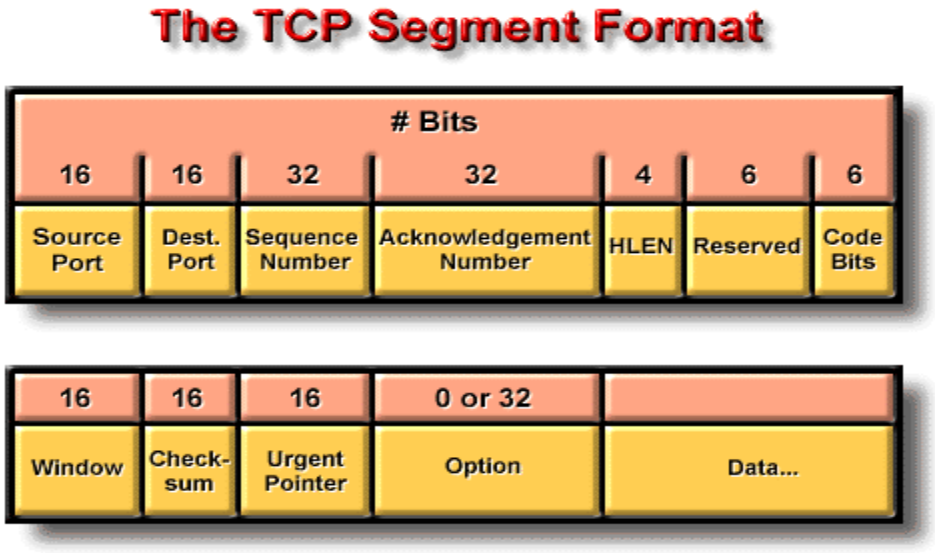
са готови. Щом подробностите бъдат уточнени, софтуерът на протокола информира ПП, че връзката е осъществена и следователно преносът може да започне. По време на преноса протоколният софтуер на двете машини продължава да поддържа връзка помежду им и проверява за коректното пристигане на данните. Ако по някаква причина връзката отпадне (напр. повреда в хардуера някъде по маршрута), двете машини отчитат това и го съобщават на съответните ПП. В такава ситуация, в рамките на изложението ще се използва термина виртуална верига за тези връзки, защото въпреки че ПП виждат връзката като налична хардуерна връзка, тя е виртуална връзка, предоставена от услугата за надеждна доставка;

Буфериран пренос - ПП изпращат потоци от данни по виртуалната верига чрез непрекъснато изпращане на октети към протоколния софтуер. При предаването на данни всяка ПП използва произволни по големина сегменти от данни, които могат да съдържат и само един октет. След проверка за коректност от страна на получателя, протоколният софтуер незабавно предава на получаващата ПП октетите точно в същия ред, в който те са били изпратени. Протоколният софтуер може да разделя потока в пакети с размери, нямащи нищо общо с получаваните от ПП парчета. За повишаване на ефективността и намаляване на мрежовия трафик, различните реализации на протокола за пренос обикновено набират от потока достатъчно данни до запълването на разумна по големина дайтаграма, която изпращат по мрежата. Така, даже ПП да изпраща периодично по един октет, преносът по мрежата може да бъде достатъчно ефективен. По същия начин, ако ПП реши да генерира много голям блок от данни, протоколният софтуер го разделя на по-малки части преди да го предаде по мрежата. За тези приложения, при които данните трябва да се пренесат, даже и да са много малко, услугата осигурява push механизъм, който ПП използват, за да предизвикат незабавен трансфер. От страна на подателя, това принуждава протокола да изпрати всички генерирани данни без да изчаква запълването на буфера. Когато тези данни пристигнат при получаващата машина, push принуждава TCP да предаде данните на получателя без забавяне. Трябва да се има предвид, че push механизмът гарантира само преноса на всички данни, но няма ограничение за обема. Така че, даже при такова принудително пренасяне, протоколът пак може да раздели потока по избран от него начин;

Неструктуриран поток - важно е да се разбере, че TCP/IP услугата за пренос на поток не различава структурираните данни. Не е предвиден начин програма за изплащане на заплати да принуди услугата да постави граници между записите за отделни служители, или да идентифицира съдържанието като ведомост за изплащане на заплати. Приложните програми са тези, които трябва да разбират съдържанието на потока и да договорят формата на данните преди да инициират връзка;

Пълно-дуплексна връзка - връзките, осигурявани от TCP/IP услугата за пренос на поток, дават възможност за едновременен пренос в двете посоки. Такива връзки се наричат пълно-дуплексни. От гледна точка на приложния процес, пълно-дуплексната връзка се състои от два напълно независими потока, течащи в противоположни направления, без явна връзка между тях. Пренасящата услуга позволява на даден приложен процес да спре потока по едното направление, докато данните продължават да се пренасят по другото, при което връзката става полу-дуплексна. Предимството на пълно-дуплексната връзка е, че протоколният софтуер може да изпраща контролираща информация за единия поток обратно до източника в рамките на потока дайтаграми, пренасяни в обратното направление. Това намалява мрежовия трафик.

На фиг.4.8 е представена формата на TCP-протоколната спецификация.



фиг. 4.8 Структура на заглавната част на TCP сегмент

Предназначението на полетата на TCP-сегмента е:

- ***Source Port*** – Идентификатор на порта-инициатор на транспортното съединение;
- ***Destination Port*** – Идентификатор на порт получател;

- ***Sequence Number*** – Последователен номер на сегмента;
- ***Acknowledgment Number*** – Номер за потвърждение;
- ***HLEN*** – Размер на пакета в 32-битови думи;
- ***Reserved*** – Не се използва;
- ***Code Bits*** – Използва се като указател за край на сесията на обмен;
- ***Window*** – Размер на прозореца, брой октети предадени без потвърждение;
- ***Checksum*** – Контролна сума на заглавната част и данните;
- ***Urgent Pointer*** – Указател за спешни данни;
- ***Option*** – Максимален размер на TCP сегмента;
- ***Data*** – Приложно съобщение, данни за TCP- протокола.

И двата протокола TCP и UDP използват идентификатори за номер на порт (socket) за целите на достоверния обмен на информацията с протоколите и услугите от "високите" нива. Портовете се използват за целите на мултиплексирането на мрежовото съединение.

Мрежовите приложения се разработват в условията на известна схема за разпределение на портовете, дефинирана в препоръка RFC 1700. Сесиите на обмен, за които няма предвиден стандартно номер се реализират на базата на случайно присвояване на номер на порт при постъпване на заявката от множеството на незаетите портове.

Приложните услуги, основани на базата на IP-протоколния стек, са представени на фиг. 4.9.

<table>
<tr><td colspan="8">ПРИЛОЖНИ УСЛУГИ</td></tr>
<tr><td>HTTP</td><td>SMTP</td><td>FTP</td><td>TELNET</td><td>SNMP</td><td>UDTP</td><td colspan="2">и т.н.</td></tr>
<tr><td colspan="3"><u>TCP</u></td><td></td><td colspan="2"><u>UDP</u></td><td></td><td></td></tr>
<tr><td colspan="8"><u>Internet IP v 4.0</u></td></tr>
</table>

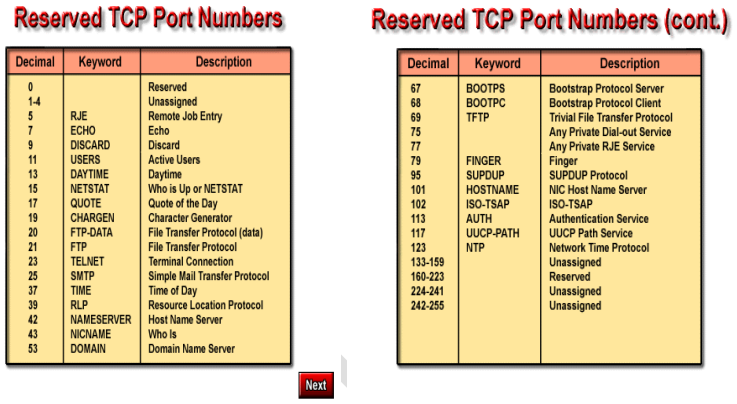
Фиг. 4.9 Услуги на приложно ниво

Една част от услугите изискват ориентирано към връзката мрежово съединение и се поддържат на транспортно ниво от протокол TCP:

- World Wide Web – HTTP (Hiper Text Transfer Protocol) протокол;
- Електронна поща (MAIL) – поддържа се от протокол SMTP (Simple Massage Transport Protocol);

- Обмен на файлове – FTP (File Transfer Protocol) протокол.
- Втора група приложни услуги не поставят изискването на свързано мрежово обслужване. Тогава на транспортно ниво се използва протокола UDP:
- Отдалечено администриране на устройства – SNMP (Simple Network Management Protocol) протокол;
- UDTP (User Define Transport Protocol) – този протокол позволява допълнително дефиниране на протоколна спецификация на приложно ниво.

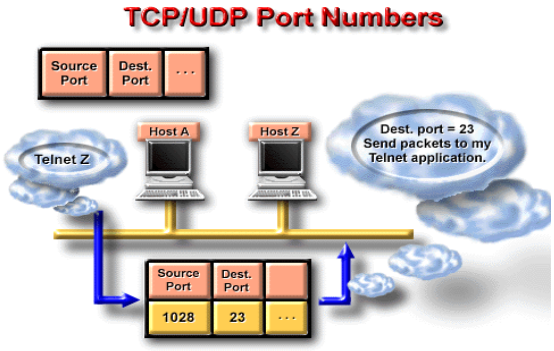
Разпределение на някои TCP портове е представено на фиг. 4.10.



фиг. 4.10 Портове на добре известни услуги

Някои от портовете са резервирани от двата протокола и приложенията не могат да използват тези портове. Принципът на разпределение на портовете е следния:

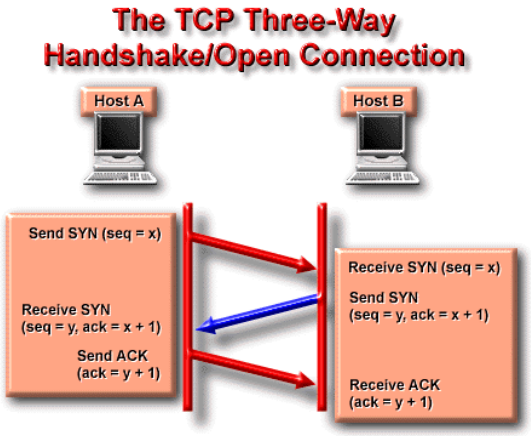
- портове с номера до 255 са предоставени за общо използване;
- портове с номера от 256 до 1023 са за системни приложения;
- портове с номера над 1023 са недефинирани.



фиг. 4.11 Разпределение на портове в процес на връзка

Крайните компютри използват портовете, за да достигнат до желаното приложение, като в полето за порт на получател (Dest. port) се указва номера на порта, с който се адресира на транспортно ниво приложението – номер 23 – приложение TELNET – фиг. 4.11.

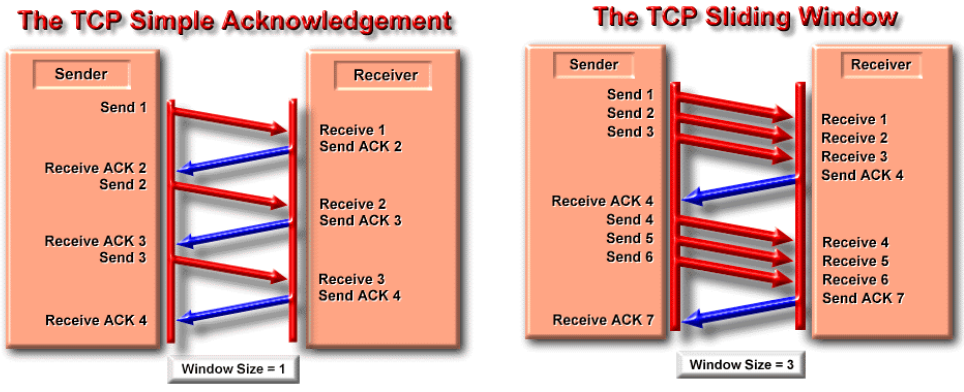
Установяването на TCP съединението в двете крайни точки (компютри) се реализира на три стъпки по последователността, показана на фиг. 4.12.



Фиг. 4.12 „Трипътно ръкостискане” при TCP протокол

Процедурата е фактически тест на логиката за потвърждение на протокола, като се обменя един празен сегмент в двете посоки и се изчаква двупосочно потвърждение за него преди да стартира обмена на реална информация.

Протоколът TCP поддържа два механизма за потвърждение, които се различават по размера на прозореца. При размер на прозореца =1, се реализира единично потвърждение; при размер на прозореца по-голям от единица потвърждението е от тип “пълзящ” прозорец – фиг.4.13.



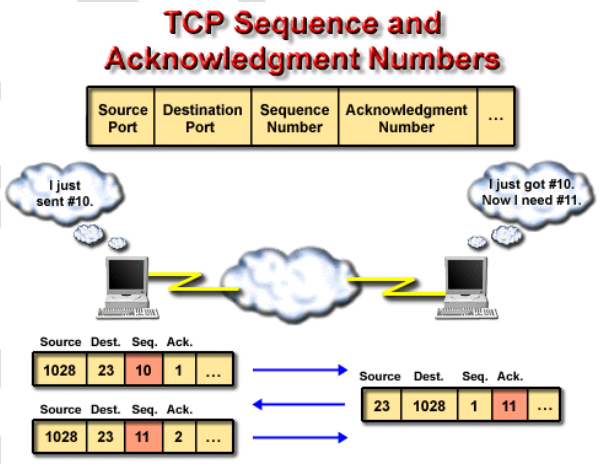
фиг. 4.13 Схема на потвърждение при „пълзящ прозорец”

Двата подхода се прилагат в зависимост от типа на приложната сесия, качеството на мрежовото обслужване и допълнителни системни изисквания за надеждност и вид на транспортното съединение.

Повечето надеждни протоколи използват един и същ фундаментален метод, наречен "потвърждение с повторно предаване". Методът изисква получаващата машина да се свърже с предаващата, като изпрати съобщение за потвърждение (АСК - acknowledge) при всяко получаване на данни. Подателят пази копие от всеки изпратен пакет и изчаква потвърждението преди да изпрати следващия. Освен това, изпращащата машина стартира таймер в момента на изпращането на пакет и изпраща пакета повторно, ако таймерът изтече преди да се получи потвърждение за получаването на пакета.

В случай, че даден пакет е загубен или повреден, подателят стартира таймер при изпращането на пакета. Когато таймерът изтече, той приема, че пакетът е загубен или не е получен и го изпраща отново.

Една примерна процедурна последователност за дуплексно управление на потока сегменти при TCP е представена на фиг.4.14



фиг. 4.14 Последователни стъпки на връзката (трипътно ръкостискане) при TCP протокол

В полето за номер на сегмента се записва номера на текущо изпратения сегмент, а в полето за потвърждение се указва номера на сегмента, който се очаква да бъде предаден, с което се потвърждава текущо предавания сегмент.

Проблем по отношение на надеждността може да възникне, когато доставящата система от по-нисък протоколен слой дублира пакет. Дублирани пакети възникват и когато в мрежата има големи закъснения, предизвикващи повторно изпращане на пакети.

Решаването на този проблем изисква сериозен размисъл, тъй като е възможно да се дублират не само пакети, но и потвърждаващи съобщения. Обикновено надеждните протоколи откриват дублираните пакети чрез присвояване на последователен номер на всеки пакет, като изискват от получателя да помни кои номера от последователността е получил. За избягване на объркването от закъснели или дублирани потвърждения, те също съдържат номера на потвърдения пакет.

Методът на "пълзящия прозорец" е по-сложен. Протоколите, които използват пълзящия прозорец", по-добре използват пропускателната способност на мрежата, защото дават възможност на подателя да изпраща множество пакети преди да изчака за тяхното потвърждение.

Даден пакет се нарича непотвърден, ако е бил изпратен, но все още не е получено потвърждение, че е получен. Броят на непотвърдените пакети технически е ограничен от размера на прозореца, който обикновено е някакво малко число.

Както е изобразено на фиг. 4.13, когато подателят получи потвърждение за първия пакет в даден прозорец, той "плъзва" прозореца и изпраща следващия пакет. Прозорецът продължава да пълзи при всяко получаване на потвърждение.

Работата на протоколите "пълзящ прозорец" зависи от размера на прозореца и скоростта, с която мрежата поема пакетите.

Фиг. 4.13 показва пример на пълзящ прозорец при изпращане на три пакета. В указания случай, подателят изпраща всичките три пакета преди да получи каквото и да е потвърждение.

Добре настроеният протокол "пълзящ прозорец" поддържа мрежата напълно наситена с пакети и той получава значително по-висока пропускателна способност, отколкото простия протокол с потвърждения.

По принцип протоколът "пълзящ прозорец" винаги помни кои пакети са потвърдени и поддържа отделни таймери за всеки непотвърден пакет. Ако даден пакет се загуби, таймерът изтича и подателят изпраща пакета повторно. Подателят премества своя прозорец след потвърдените пакети. При получателя се поддържа аналогичен прозорец, чрез който се приемат и потвърждават пристигащите пакети. По този начин прозорецът разделя последователността от пакети на три вида: отгоре на прозореца са успешно изпратените, получени и потвърдени, отдолу на прозореца - все още не са изпратени, а

тези в прозореца - са в процес на изпращане. Пакетът с най-малък номер в прозореца е първият пакет в последователността, който не е потвърден.

Услугата за надежден пренос се осигурява от пакета протоколи TCP/IP и е дефинирана в TCP. Надеждният пренос е толкова важен, че целият пакет протоколи обикновено се нарича TCP/IP. Важно е да се разбере, че:

TCP е комуникационен протокол, а не част от софтуер.

Разликата между протокола и софтуера, който го реализира, е аналогична на разликата между дефиницията на даден програмен език и компилатора.

4.2.2 Транспортен протокол UDP (User Datagram Protocol)

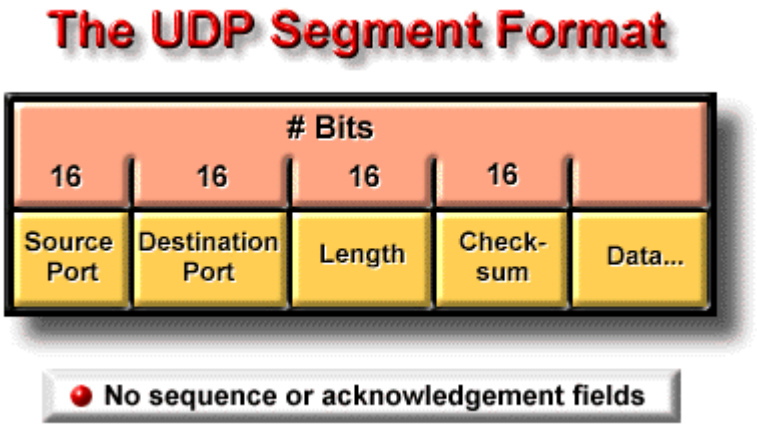
В пакета протоколи TCP/IP този протокол осигурява първичния механизъм, който използват приложните програми за изпращане на датаграми до други приложни програми (ПП). UDP осигурява портове, които служат за различаване на множеството-програми, изпълнявани на съответната машина. Т.е., освен самите данни, UDP съобщението съдържа номерата на порта-получател и порта-подател, така че UDP софтуера да може да изпрати съобщението на правилния получател, който пък има възможност да върне отговор.

UDP използва намиращият се под него протокол IP за транспортиране на съобщението от една машина до друга, като осигурява същата ненадеждна несвързана с потока данни семантика на изпращането на дайтаграмата, както IP. Той не използва опознаване (acknowledge) за да проверява дали съобщенията пристигат, не подрежда идващите съобщения, не дава обратна връзка за контрол на скоростта, с която се предава информацията между двете машини. Така UDP съобщенията могат да се загубят, дублират или да пристигат в непоследователен порядък. Още повече пакетите могат да пристигат с по-голяма скорост, отколкото получателя може да ги обработва. Протоколът UDP осигурява ненадеждна услуга с използване на IP за транспортиране на съобщенията между машините. Той използва IP като носител, но добавя способността да се различават множество получатели в рамките на един компютър.

ПП, която използва UDP, поема пълната отговорност за обработка и справяне с проблемите на надеждността, включително загуба на съобщения, дублиране, закъснение, разбъркан порядък и загуба на връзка. За съжаление, приложните програмисти често пренебрегват тези проблеми при проектирането на софтуер. При това, тъй като

приложните програмисти често тестват мрежовия софтуер върху бързи, надеждни и ниски закъснения локални мрежи, тестовете може да не покажат слабостите и потенциалните проблеми. Така много ПП, които се опират на UDP, работят добре в локални мрежи, но пропадат в големи TCP/IP мрежи.

На фиг.4.15 е представен формата на UDP-сегмента



фиг. 4.15 Формат на заглвана част в UDP дейтаграма

Сравнявайки този формат с формата на TCP сегмента се наблюдава отсъствие на полета за контрол на потока и корекция на грешки. Това е характерно за дейтаграмните протоколи. Във функционалността на сегмента е съхранена възможността за мултиплексиране на мрежовите съединения

Полетата SOURCE PORT (порт подател) и DESTINATION PORT (порт получател) съдържат в 16-битово представяне номерата на UDP портовете, които се използват за де мултиплексиране на датаграмите между процесите, които очакват да ги получат. Портът подател може да не се попълва. Ако това поле бъде използвано, то възможните отговори ще бъдат изпратени са указания номер на порт. Ако не се използва, стойността трябва да бъде 0.

Полето LENGTH (дължина) съдържа общия брой на октетите в дайтаграмата, включително заглавната част и данните. Следователно, минималната стойност в това поле ще бъде 8, колкото е броя на октетите в заглавната част.

Полето за контролната сума се използва по избор. Стойност 0 в това поле означава, че не е пресмятана контролна сума. Възможността да не се пресмята контролна сума е оставена за случаите, когато UDP се използва във високонадеждна локална мрежа и не е необходимо да се губи време за пресмятането и. Нека не забравяме, все пак, че IP не

пресмята контролна сума за данните в дайтаграмата. Така че контролната сума на UDP дава единствената възможност за гарантиране на точността на данните, пристигащи при получателя, и би трябвало да се използва.

Много от потребителите често се чудят какво става с UDP съобщенията, за които е пресметната контролна сума е 0. Това е възможно, защото UDP използва същия алгоритъм за пресмятане на контролната сума, както IP: той разделя данните на 16-битови стойности и пресмята допълнението към допълнената сума от отделните битове. Оказва се, че нулата не е проблем, тъй като в тази "допълнителна" аритметика нулата може да се представи по два начина: всички битове са 0 или всички битове са 1. Когато пресметнатата контролна сума е 0, UDP използва представянето с единици.

Контролната сума на UDP покрива повече информация, отколкото се съдържа в UDP дайтаграмата. За пресмятането на контролната сума UDP наставя псевдо-заглавна част към дайтаграмата, добавя октет от нули за да формира дайтаграма от цяло число 16-битови фрагменти и пресмята контролна сума за целия получен обект. Добавените псевдо-заглавна част и октета от нули не се изпращат с дайтаграмата, нито пък се вземат предвид при пресмятането на дължината и. За пресмятането на контролна сума софтуерът най-напред записва 0 в полето за контролна сума, после прави пресмятането за целия обект заедно с псевдо-заглавната част, истинската заглавна част и данните.

Псевдо-заглавната част се използва за проверка дали UDP дайтаграмата е пристигнала при получателя. Важно е тук ясно да се разбира, че адресът на получателя се състои от адреса на машината и номера на порта в тази машина. Заглавната част на UDP определя само номера на порта. Тогава, за да се гарантира получаването, UDP в машината на подателя пресмята контролна сума, която обхваща UDP дайтаграмата и IP адреса на получателя. В машината на получателя UDP проверява контролната сума като използва IP адреса на получателя, записан в заглавната част на IP дайтаграмата, която пренася UDP съобщението. Ако контролните суми съвпадат, то дайтаграмата е пристигнала точно по местоназначението и на правилния порт.

При пристигането си, най-долният слой от мрежовия софтуер приема пакета и той започва да се изкачва по слоевете. Всеки слой премахва съответната заглавна част и предава остатъка на горния слой, така че най-горният слой предава данните на очакващия ги процес без заглавна част. Така най-външната заглавна част съответства на най-ниския

мрежов протокол. При разглеждането на добавянето и премахването на заглавни части трябва да имаме предвид принципа на слоевете. В частност този принцип се прилага при UDP, така че UDP дайтаграмата, получена от IP на машината-получател, е идентична с дайтаграмата, която UDP е предал на IP в машината-подател. По същия начин данните, които UDP предава на потребителския процес в машината-получател, ще бъдат точно данните, които друг процес е предат на UDP в машината-подател.

Разпределението на задълженията между различните слоеве протоколи е точно и ясно:

- IP слоят отговаря само за преноса на данни между двойка хостове през мрежата;
- UDP отговаря само за разпределянето между многото възможни податели и получатели в рамките на тези хостове.

По този начин само IP заглавната част идентифицира машините подател и получател; само UDP идентифицира портовете в рамките на един хост.

Тук възниква въпроса: Как се присвоява номер на порт?

Проблемът е важен, тъй като два компютъра трябва да съгласуват номерата на портовете си преди да започнат обмен.

Например, когато компютър А иска да получи файл от компютър В, той трябва да знае кой порт използва компютър В за трансфер на файлове. Има два фундаментални подхода при присвояването на номера на портове. При първия подход се използва централизирано определяне. Всички останали се съгласяват и позволяват на "централната власт" да дава номера на портове и да публикува техния списък. Тогава софтуерът се изгражда според този списък. Този подход се нарича понякога "универсално присвояване" и присвоените номера на портове се наричат "известни номера на портове".

Вторият подход използва динамично свързване. При него номерата не са глобално известни. Вместо това, когато дадена програма поиска порт, мрежовият софтуер го дава.

За да се види моментното състояние на портовете на друг компютър ще трябва да се изпрати заявка с въпрос от вида "Кой порт се използва за трансфер на файлове?" Отговорът съдържа номера та порта, който трябва да се използва в този случай.

Примерен набор от стандартни номера за UDP портове, като са показани техните имена и UNIX еквивалент е показан на талица 4.1.

Таблица 4.1

	ключова дума	UNIX	Описание
0	-	-	Запазен
7	echo	echo	Exo
9	discard	discard	Отхвърляне
11	users	systat	Активни потребители
13	daytime	daytime	Дата и час
15		netstat	Статус на мрежата
17	quote	qotd	Цитат на деня
19	chargen	chargen	Знаков генератор
37	time	timserver	Сървър за време
42	nameserver	name	Сървър на имена
43	whois	nickname	Кой е
53	domain	nameserver	Сървър на имена в домейна
67	bootps	# BOOTP server	BOOTP Сървър
68	bootpc	# BOOTP client	BOOTP клиент
111	sunrpc		RPC за Sun
123	ntp	ntp	Сървър за време
525		timed	Демон за време в мрежата

Доколкото е възможно, други транспортни протоколи, които предлагат същите услуги, използват същите номера на портове.

Създателите на TCP/IP са използвали хибриден подход, при който някои от портовете имат предварително зададени номера, а останалите се управляват динамично от локалните ОС или ПП. Предварително зададените и еднакви за всички номера използват ниски стойности, като по-високите номера са оставени за динамично присвояване.

Обобщение

Протоколът за контрол на преноса TCP дефинира ключова услуга в междумрежовата среда, а именно надеждния пренос на поток от данни. TCP осигурява пълнодуплексна връзка между две машини, като им дава възможност да обменят ефективно големи обеми данни.

Тъй като използва протокол за пълзящ прозорец, TCP може ефективно да използва мрежата. Освен това, той малко зависи от разположената под него системи за доставка и поради това е достатъчно гъвкав, за да може да работи с голямо разнообразие от системи за доставка. Тъй като осигурява контрол на потока, TCP дава възможност за комуникация между системи с много различни бързодействия.

Основната единица, в която TCP пренася данни, е сегмент. Сегментите се използват за обмен на данни и контролна информация (например, за да даде възможност на TCP

софтуера на две машини да установява връзка и да я прекратява). Форматът на сегмента позволява на една машина да вмъкне потвържденията за данни пристигнали от едната посока в заглавните части на сегменти с данни, изпратени в обратната посока.

TCP осъществява контрол на потока посредством съобщение от страна на получателя за това колко данни може да приеме. Освен това той поддържа и съобщения извън пренасяния поток чрез специално средство за спешно изпращане на данни и предизвиква доставянето чрез механизъм push.

Съвременния стандарт за TCP дефинира експоненциално увеличаване на таймерите за повторно изпращане и алгоритми за избягване на задръстване, ката бавен старт, степенно намаляване и стъпково нарастване. В допълнение, TCP използва специални методики за избягване на изпращането на малки пакети

Моля, отговорете на контролните въпроси:

1. *Какво представлява понятието протоколен стек ?*
2. *Каква е разликата между протоколите TCP и UDP?*
3. *Кои протоколи не спадат към приложния слой на модела? :*

а)ICMP; б) FTP; в) STP; г) UDP.

4. *Какво е предназначението на протокола ICMP?:*
5. *Какво е предназначението на протокола ARP?.*
6. *Кой е протоколния стек на мрежа Novel и мрежа Decnet?*

Раздел 5

Интернет мрежа. Глобални мрежи. Методи за комутация

Ключови думи и съкращения

WAN	**ОС**
Frame Relay	**Отдалечени връзки**
ATM	**Комутация на пакети и канали**
Модем	**DSL**
ISDN	**X.25**
CATV	**OC-SONET**

5.1 История на Интернет

Първата мрежа е разработена от Агенцията за прогресивно научни проекти (Advanced Research Projects Agency) на американската армия, която е наречена ARPAnet. Поради растящия брой научни институти и университети, присъединили се в мрежата, ARPAnetостава да се занимава само с изследвания, докато една друга, втора мрежа MILnet се ориентира към военните комуникации. През 1980г. Националната научна фондация (NSF) основава NSFnet, свързвайки половин дозина суперкомпютри при изключително висока скорост, която в момента продължава да се увеличава. Накрая, NSFnet пое Интернет от ARPAnet и през 1991г. са създадени основите на Националната научна и образователна мрежа (NREN). Целите на NREN са да осъществява и поддържа високи скорости, научни и образователни мрежи с огромен капацитет, а също така и да развива търговското присъствие в Интернет. Този момент е изключително важен за WWW (Word Wide Web), която бързо бе възприета като среда за търговска дейност не само в Северна Америка, но и по целия свят. При това търговците не се включват в мрежата само за проучване или електронна поща; те са там защото Интернет предлага огромен търговски потенциал. Със сигурност Интернет е предимно научна и академична мрежа поне от гледна точка на творческата дейност и обхвата на използуване. Съществува огромна активност в сферата на образованието, включени са много общности и некомерсиални издания.

През 1995г. Федералният съвет за мрежи (FNC), приема резолюция, дефинираща термина Интернет:

Интернет е мрежа, обхващаща земното кълбо. Тя се основава на световната комуникационна мрежа, включваща кабелните телефонни линни, спътникови, оптични и др. връзки. Към Интернет са свързани десетки хиляди компютърни мрежи.

5.2 Глобални мрежи (WAN)

Глобалните мрежи (Wide Area Network, WAN) не е просто голяма LAN, а представлява сбор от повече LAN мрежи, свързани помежду си с отдалечени връзки.

Най-простата топология, използвана в глобалните мрежи (WAN) е простата връзка от точка до точка. WAN мрежата, подобно на LAN, може да използва също традиционни мрежови топологии, например кръг или звезда.

В традиционните LAN мрежи компютрите са разположени близко, поради което затихването на изпращаният сигнал при преминаването му по кабел е незначително. При по- големи разстояния директната кабелна връзка става неподходяща, което налага използване на други технически решения. Отдалечените мрежови връзки се осъществяват с помощта на допълнителни устройства, като преносната среда може да бъде жична или безжична. Мрежовите връзки с отдалечен достъп, макар и с ограничено времетраене, позволяват на потребителите да установяват връзка и да работят с LAN така, като че ли са свързани с мрежата директно посредством кабел.

Използването на телефонна линия и модем (***dialup networking***) представлява един пример за изграждане на отдалечена връзка. Тук ролята на мрежова карта изпълнява модема, а тази на Ethernet кабела телефонната линия. Разликата между този вид отдалечена връзка и директната кабелната връзка е в скоростта. По принцип отдалечените връзки отстъпват по скорост на директните кабелни връзки. Така например най-производителните модеми работят със скорост 56 Kbps, докато най-бавната Ethernet връзка постига 10 Mbps. Най- високоскоростните ADSL адаптери, използвани за отдалечени връзки по цифрови абонатни телефонни линии, постигат скорости максимум до 6 Mbps. Както е видно, дори и те отстъпват по скорост на най-бавната Ethernet връзка.

Множество от концепциите на LAN топологиите се прилагат и към WAN мрежите. Но в контекста на WAN мрежите топологията описва подреждането на включените в глобалната мрежа предаващи и приемащи устройства.

За реаализация на глобални мрежи се използват множество отдалечени връзки, при които се прилагат различни методи на комутация.

Компютърните мрежи използва следните методи за комутация:

- Комутация на каналите;
- Комутация на съобщенията;
- Комутация на пакетите.

При мрежите с ***комутация на каналите*** предаването на съобщенията се извършва на три етапа:

- установяване през мрежата на временен канал между източника и получателя;
- предаване (обмен) на съобщенията;
- разпадане на канала.

Недостатък на компютърната мрежа използваща комутацияна каналите е, че при заетост на краен възел и комутируем канал се налага изчакване на тяхното освобождаване, за да се изгради канала за предаване на съобщението.

Независимо от този недостатък методът на комутация на каналите се използва за предаване на съобщения в телеграфните, телефонните и ***ISDN*** мрежите.

При мрежите с ***комутация на съобщението***, цялото съобщение се предава по различните участъци на мрежата с натрупване в междинните й възли, които се наричат комутатори на съобщението.

В този случай всяко съобщение гтрябва да съдържа адресна и информационна част. Комутаторите на съобщенията са мощни компютърни системи с голямо бързодействие, към които са включени множество от канали за приемане и предаване на съобщения. Междинните възли работят с голяма скорост и притежават голяма по обем запомняща система (дискова памет).

Недостатък на този метод е, че при големи натоварвания на мрежите съобщенията закъсняват, изчаквайки на големи опашки в комутаторите на съобщенията.

Комуникационни мрежи с комутация на съобщенията се използва при доставката на електронната поща (E-mail) през комуникационните мрежите и интермрежи.

Мрежите, използващи ***комутация на пакети*** позволява намаляване на времето за доставка на дългите съобщения. В крайните възли съобщението се разделя на пакети,

всеки с адресна и информационна част. Пакетите се предават по мрежата и когато достигнат до получателя се събират за да се възстанови съобщението. Обикновено пакетите достигат до крайния получател по различни маршрути.

Компютърната мрежа с комутация на съобщението използва два режима на работа:

- режим "**Дейтаграмен**";
- режим "**Виртуално съединение**".

Всеки пакет има пълен адрес, по който се определя по-нататъшния му маршрут. Отделните дейтаграми се предават независимо една от друга и маршрутът им е различен. Възможно е редът на пристигане да е различен от реда, по който са изпратени. За да не се загуби реда на пакетите всяка дейтаграма се номерира и получателя ги подрежда в първоначалния ред.

Предимствата на дейтаграмния режим са следните:

- Съкращава се общото време за предаване на съобщенията;
- Постига се висока надеждност на предаване при отказ на част от мрежата;
- Динамична маршрутизация на дейтаграмите в зависимост от състоянието на мрежата.

Недостатък на този режим е липсата на потвърждение за правилното приемане на отделните дейтаграми и възможността за нарушаване на правилния ред на следване. Това налага допълнителни мерки при възстановяване на съобщението от страна на получателя.

При режима на предаване на съобщения по виртуално съединение съществуват следните обособени състояния:

- Изграждане на логическо (виртуално) съединение между крайните възли;
- Предаване на пакетите един след друг;
- Разпадане на съединението.

Предимствата на режим "Виртуално съединение" са следните:

- Маршрутът на съединението се избира само един път и междинните възли и комутатори на пакети по време на предаването не вземат решение за избор на маршрута на предаване на пакетите;
- Съхранява се редът за следване на пакетите
- Извършва се пълен контрол на грешките в пакетите.

Недостатъците на този метод са следните:

- Липсва гъвкава маршрутизация;
- Наличие на време за установяване на логическа връзка;
- Ниска надеждност при отказ на междинните възли.

За да се ускори предаването на съобшенията при комутацията на пакетите в междинните възли се използва основно оперативната памет на комутаторите на пакети. При препълване се прилагат механизми за забавяне на пакетите чрез управление на натоварването на мрежата. Метода за комутацията на пакети се използва от стандарта за глобални компютърни мрежи изградени по стандарта X.25 и световната компютърна мрежа Internet.

Мрежите с ***бърза комутация на пакетите*** представляват комбинация между комутация на каналите и комутация на пакетите.

При тези мрежи се намалява времето за обработка на пакетите в комутаторите. В междинните възли се използват самомаршрутизиращи се комутационни матрици. Не се извършва повторно предаване на сгрешени пакети в междинните възли, а възстановяването на такива пакети е функция на крайните възли. Интелигентността на компютърната мрежа е насочена към крайните възли.

Методът на бърза комутация на пакетите приложим за комуникационни линии с малка вероятност за грешки – каквито са оптическите. Прилага се се в съвременните стандарти за изграждане на глобални компютърни мрежи – Frame Relay и ATM.

Комуникационните мрежи предоставят услуги на потребителите разпределени в три категории:

Услуги за достъп до отдалечена информация:

- Достъп до информационни системи, WWW;
- Достъп до библиотеки on-line;
- Достъп до ежедневната преса;
- Електронна търговия;
- Достъп до банки , борси.

Услуги за междуличностна комуникация:

- Електронна поща – текст, видео, гласова поща;
- Интерактивни разговори в реално време ICQ, TRQ;
- Видеоконферентни връзки, дискусии;

- Дистанционно обучение.

Услуги за интерактивни комуникации:

- Участие във виртуални видеоигри;
- Интерактивни филми и телевизия;
- Гледане на видеофилми по поръчка.

Основните недостатъци с използването на глобалните мрежи са свързани с:

- разпространяване на лъжлива информация;
- извършване на финансови и други измами;
- предлагане на порнография;
- анонимност при използване на комуникационни услуги.

При отдалечените връзки за предаване на данни се използват два типа технологии на комутиране:

Комутиране на вериги (circuit switching) - връзката се изгражда посредством поредица от комутации, в резултат на които възниква електрическа верига, по която се осъществява комуникацията. Връзката е временна. Трае докато комуникацията приключи. Ако същата бъде прекъсната и след това повторно създадена, в резултат от нови комутации в общия случай възниква друга връзка (друга електрическа верига), представляваща друг път за комуникация. Пример за мрежа с комутиране на вериги е телефонната мрежа.

Комутиране на пакети (packet switching). Тук данните биват разбивани и изпращани в линията под формата на пакети, като всеки един от тях може да пътува по различен път в мрежата и да достигне до крайната точка на комуникация в различно време. След като всички пакети достигнат крайния пункт, те биват подреждани в първоначалния им ред така, че да образуват отново тяхното общо цяло. За разлика от комутацията на вериги тук не се ползва една единствена връзка за цялото времетраене на комуникацията. Тук пакетите пътуват по различни пътища. Пример за мрежа с комутиране на пакети е Интернет.

Отдалечени връзки с комутиране на вериги

Мрежите с комутиране на вериги използват както dialup връзки, осъществявани по стандартни телефонни линии чрез избиране на телефонен номер, така и наети линии, които представляват фиксирани телефонни връзки.

Устройствата, използвани за изграждане на мрежи с комутиране на вериги, са следните:

Модеми

С помощта на модеми се реализира популярният тип отдалечена връзка, известна като dialup връзка. Връзките от този тип се осъществяват по стандартните аналогови телефонни линии, инсталирани в повечето предприятия и организации. Технологията е позната със съкращението PSTN (Packed Switched Data Network).

Процесът на конвертиране на цифровите сигнали в аналогови и обратно се нарича модулация/демодулация. Модемът е устройство, което може да извършва двата вида конвертиране, откъдето произхожда и неговото название. Той преобразува цифровите данни, идващи от предаващия компютър, в аналогов сигнал, който след това се предава в стандартна телефонна линия. Процесът се нарича модулация. На другия край на линията пристигащият аналогов сигнал се възприема от друг модем, който извършва обратното преобразуване - конвертира аналоговия сигнал в цифров. Процесът се нарича демодулация.

Когато предаващият модем предприеме инициатива за осъществяване на връзка с друг модем, отначало той излъчва тонален сигнал, състоящ се от два периодично сменящи се тона с различна височина. Ако отсрещният модем отговори с подобни два тона (с други звукови честоти), това ще означава, че връзката е създадена. Двата модема са си „подали ръка", осъществявайки ръкостискане (handshaking) и вече може да започне предаването на данни. В случай, че отсрещният модем не поеме „подадената ръка", предаващият модем понижава честотите на двата тона и отново „подава ръка". Процесът се нарича fallback. Той се повтаря, докато се създаде връзка, а при невъзможност за осъществяване на такава (телефонната линия е лоша или зашумена или пък отсрещният модем не се отзовава) инициативата на предаващия модем се прекратява окончателно.

Модемите работят на най-долният слой на OSI-модела. Те са свързани непосредствено с комуникационната линия. Използват се за създаване на WAN-връзка към доставчик на Интернет услуги или за осъществяване на връзка с dial-up сървър в частна мрежа.

Според конструктивното им оформяне модемите се разделят на външни и вътрешни.

Външният модем е отделно устройство със собствено електрозахранване, което традиционно бива включвано към един от серийните портове (COM входове) на компютъра. Съвременните модеми позволяват включване в USB порт на компютъра или в хъб (концентратор). Предимството на външните модеми в сравнение с вътрешните е в това, че отпада необходимостта от инсталация на същите в компютъра и нуждата от конфигуриране на същите (задаване на прекъсването IRQ и на I/O адреса на серийния порт). Външните модеми имат индикаторни панели за състоянието си, което позволява визуално наблюдаване на процеса на комуникацията.

Вътрешните модеми биват поставяни под формата на интерфейсна карта в разширителен слот на компютъра - в ISA или в PCI слот на настолните компютри, респективно в PCMCA слот на преносимите компютри. В двата случая се изисква конфигуриране на модема, освен когато той е от типа Plug and Play (PnP) и BIOS и операционната система поддържат PnP.

Съвременните модеми извършват компресия/декомпресия на данните и са в състояние да осъществяват защита от грешки. Скоростта им на работа зависи от качеството на телефонната линия. Съвременните модеми могат да приемат/предават със скорост от 14.4 до 56 Kbps. Това е така наречената информационна скорост, от която се интересуват потребителите на мрежи. Съществува и друга скорост, измервана в бодове, която изразява качеството на модулация на цифровия сигнал. Един бод би могъл да съдържа един или повече бита. В числено изражение скоростта на модулация обикновено бива по-ниска от информационната скорост.

По скорост на комуникация модемите отстъпват на ISDN и ADSL адаптерите. Последните често биват неправилно наричани модеми. Те не извършват модулация и демодулация на цифровия сигнал. ISDN и ADSL линиите са цифрови, за разлика от стандартните комутируеми аналогови телефонни линии.

ISDN адаптери

ISDN (Integrated Services Digital Network – цифрова мрежа за интегрирани услуги) служи за трансфер на данни, включително аудио и видео информация, по цифрови или по обикновени телефонни линии. ISDN адаптерите притежават един или повече канали за пренасяне на данни, наричани B-канали (bearer, носещи канали) и един канал за

управление, наричан D-канал (Delta канал). Всеки B-канал е с пропускателна способност 64 Kbps, а D- каналът с 16 или 64 Kbps в зависимост от конкретната реализация на адаптера.

ISDN адаптерите се предлагат в два варианта:

- Basic Rate ISDN (BRI). Състои се от два B-канала. Всеки един от тях работи със скорост 64 Kbps. Адаптерите могат да бъдат конфигурирани така, че по време на комуникацията да се използват двата канала едновременно (multilink конфигурация), в резултат на което пропускателна способност става 128 Kbps. Двата канала са снабдени с различаващи се един от друг телефонни номера, макар че кабелът им за връзка с телефонната линия е общ. BRI се използва от телефонните компании за високоскоростен трансфер на данни в жилищни райони или между малки бизнес организации.
- Primary Rate ISDN (PRI). Състои се от 23 B-канала със скорост 64 Kbps, които взети заедно осигуряват пропускателна способност от 1472 Mbps. PRI се използва за цифрово предаване на глас, както и за реализация на частни телефонни мрежи от типа PBX (private branch exchange), използвани в предприятия и организации.

Подобно на модемите, ISDN адаптерите биват вътрешни и външни. Външните се свързват към мрежовите Ethernet карти на компютрите.

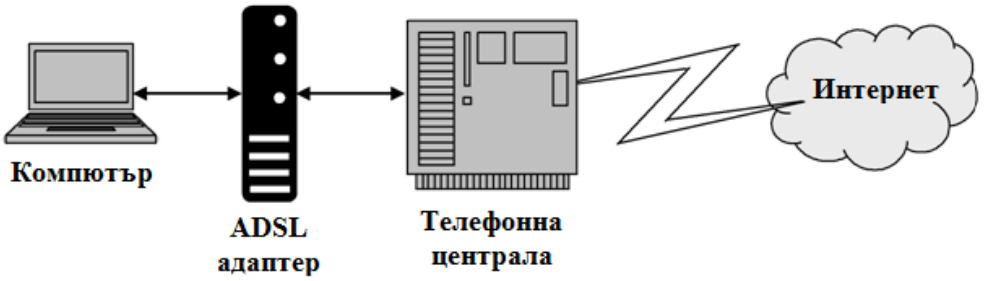
ISDN адаптерите позволяват свързване към тях на аналогови телефони, предназначени за извършване на разговори. В този случай те могат да бъдат конфигурирани така, че да осъществяват връзка с Интернет със скорост 128 Kbps. Ако по телефона постъпи повикване и започне провеждане на разговор, докато той трае скоростта на връзката с Интернет спада автоматично на 64 Kbps. След затваряне на телефона B-каналът, използван до тогава за провеждане на разговора, автоматично се превключва към Интернет, като скоростта се покачва отново на 128 Kbps.

DSL адаптери

DSL (Digital Subscriber Lines) технологията е по-съвременна технология от ISDN. Телефонните компании я предлагат на потребителите като допълнителна услуга върху

съществуващите телефонни линии. По една и съща линия могат едновременно да бъдат предавани глас и данни. При по-ниска цена от ISDN DSL предлага скорости близки до тези на наетите телефонни линии.

За установяване на връзка DSL технологията не изисква избиране на телефонен номер. Тя се намира постоянно на разположение (постоянно е включена).



фиг. 5.1

DSL се среща в 5 варианта. Универсалният начин за тяхното означаване е xDSL. Те са следните:

- ADSL (Asymmetric DSL). Това е най-разпространения и сравнително най-евтин вариант на DSL (фиг 5.1). Осигурява скорост на низходящия трафик (download stream) в диапазона от 384 Kbps до 6 Mbps. Скоростта на възходящия трафик (upload stream) е около 4 пъти по-ниска от тази на възходящия. Българска телекомуникационна компания (бТК) предлага ADSL с низходяща скорост, достигаща до 4 Mbps. Недостатък на ADSL е ограничението по отношение на разстоянието между потребителя и телефонната централа, което не може да надхвърля 5 км. ADSL адаптерите биват вътрешни и външни. Външните се свързват към мрежовата Ethernet карта на компютъра.
- SDL (Symmetric DSL). Осигуряват една и съща скорост на низходящия и възходящ трафик, която достига до 3 Mbps. Технологията отстъпва по скорост на ADSL и е по- скъпа.
- HSDL (High DSL). Осигурява в двете посоки скорост от 768 Kbps. Технологията не получи широко разпространение.
- VDSL (Very High Data Rate DSL). За сметка на високата цена позволява постигане на изключително високи скорости на трансфер между 13 Mbps и

52 Mbps, подходящи за предаване на живо на видео и на аудио. Това е най-скъпата DSL технология.

- IDSL. Това е DSL технология, осъществявана по ISDN линии. Максимална скорост на предаване е 144 Kbps. Технологията е по-скъпа и е с по-ниска скорост от ADSL. Предимството й е, че може да бъде използвана за реализации, при които поради големите разстоянията предходните четири DSL технологии не са подходящи.

T-носещи

За отдалечени връзки с висока пропускателна способност и надеждност се използват наети линии – линии, които биват вземани под наем от телефонни компании, обикновено за частно ползване. Наетите линии осигуряват постоянна връзка от една точка до друга, например от една LAN мрежа до някакъв Интернет доставчик или от един филиал на една фирма до друг нейн такъв.

Една от първите цифрови услуги по наети линии бе DDS, осигуряваща скорост на трансфер 56 Kbps. Не след дълго тя трябваше да отстъпи на технологията, наричана T- носещи, която се оказа по-евтина и по-производителна от DDS. Буквата T в названието указва характера на предавателния канал. Разпространени реализации на T-носещи са следните:

- T-1 със скорост на трансфер 1.544 Mbps;
- T-2 със скорост на трансфер 6.132 Mbps;
- T-3 със скорост на трансфер 44.736 Mbps;
- T-4 със скорост на трансфер 274.760 Mbps.

T-носещите линии се състоят от множество канали, всеки един от които със скорост 64 Kbps. Потребителите биха могли да наемат всички канали или само част от тях. Пропускателната способност на линията представлява сума от скоростите на наетите канали.

T-носещите представляват специализирани вериги за трансфер на данни, глас и видео от точка до точка. Те могат да бъдат безжични или жични с използване на обикновен меден, оптичен или коаксиален кабел. В двата крайща на веригата се включват CSU/DSU устройства (CSU/DSU – Channel Service Unit/Data Service Unit,

устройство за обслужване на канал/устройство за обслужване на данни), които биват свързвани към стандартен RS-232 интерфейс (COM порт на компютър). CSU защитава линията от електрически смущения, а DSU управлява трансфера на данните (обработва грешките и преобразува данните в сигнали, подходящи за изпращане в линията).

Т-1 услугата е най-евтина сред Т-носещите, но тя е по-скъпа от получилата напоследък популярност ADSL услуга, осигуряваща същата и дори по-висока скорост. Организациите предпочитат Т-1, когато се нуждаят от гарантирана скорост на предаване. При ADSL скоростта не е гарантирана. Тя би могла да се окаже по-ниска от максималната, докато при Т-1 това не е възможно. Гарантираната скорост е най-важното съображение за наемане на Т-1 линия, особено когато организациите се нуждаят от постоянна производителност на мрежата.

Отдалечени връзки с комутиране на пакети

Технологиите на комутиране на пакети са следните:

- X.25;
- Frame Relay;
- ATM.

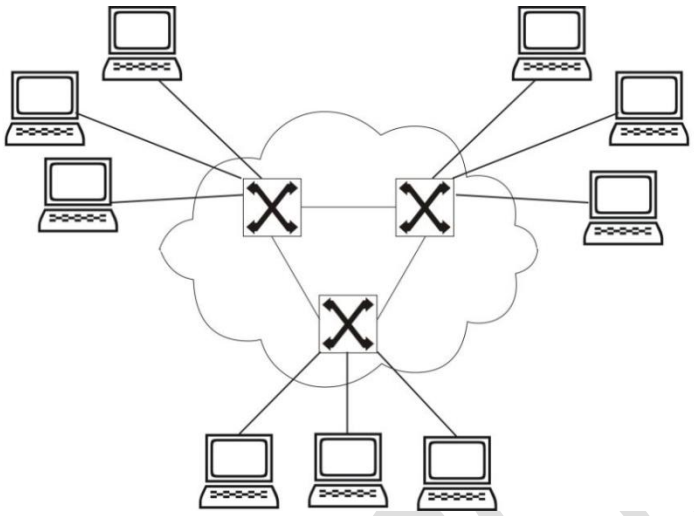
Първа се появи технологията X.25, известна още като PSDN (Packet Switched Data Network). Тя бе проектирана да работи с мейнфрейм компютрите на IBM. Frame Relay е усъвършенствана X.25 технология, която може да работи със скоростите на Т-1 и Т-3.

ATM

ATM (Asynchronous Transfer Mode) е модерна цифрова мрежова технология, предназначена за висикоскоростни приложения, каквито са например поточните аудио и видео.

Вместо стандартните и многобройни мрежи за предаване на данни, всяка от които осигурява само определен вид услуги, в ATM се реализира концепцията за построяване на единна цифрова мрежа базирана на единен метод за транспортиране на всички видове информация. ATM осигурява еднотипно представяне на потребителската информация чрез къси пакети с фиксирана дължина, наричани клетки, които по виртуален канал се доставят до местоназначението си в режим на бърза комутация. Благодарение на ATM цялото комутационно оборудване става еднородно (фиг.5.2), със способност да реализира всички

видове трафик посредством бърза комутация на клетки и асинхронно разпределяне на ресурсите.



фиг.5.2

АТМ съчетава предимствата както на метода "комутация на вериги" (константно закъснение при предаването и гарантирана пропускателна способност), така и на метода "комутация на пакети" (постигане на висока ефективност при нерегулярен трафик). При АТМ множество виртуални канали асинхронно се мултиплексират върху един физически цифров канал.

АТМ мрежите се характеризират с:

- висока гъвкавост и адаптируемост към изменящите се изисквания на потребителите по отношение на обема, скоростта и качеството на доставената информация;
- висока ефективност при използването на ресурсите благодарение на статистическото мултиплексиране на множество източници;
- ниски разходи за проектиране, строителство и експлоатация.

Класическите мрежи използват пакети, съдържанието на които не зависи от характера на връзката. Пакетите съдържат константна адресна информация за изпращача и получателя на съобщението. Тук мрежата отговаря за това как пакетите да достигнат до получателя. Работните станции (компютрите) са освободени от това задължение, което позволява те да бъдат относително прости.

При АТМ съществува следната особеност. Последната станция отговаря за установяване на виртуален път между отделните станции. Ролята на комутаторите при

АТМ режима, е да комутират клетки по продължение на един виртуален канал на базата на информация, съдържаща се в хедъра. Тук мрежата се освобождава от отговорността за пренасяне на данните, което опростява мрежовото оборудване.

При АТМ се използват два типа виртуални връзки - виртуален кръг и виртуален път.

Виртуалният кръг представлява логическата връзка (логическа верига) между две крайни устройства, осъществявана през комутационна мрежа. Двете устройства си обменят информация, като си изпращат клетки с данни по логическата верига.

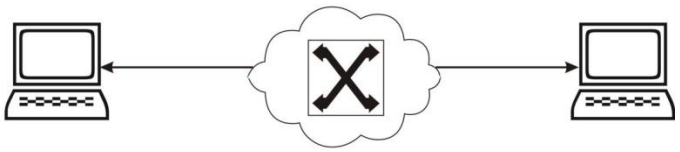
Виртуалният път представлява логическа група от тези логически вериги. Разпознаването на такива групи позволява на АТМ комутаторите да изпълняват операциите общо за цялата група вериги, а не поотделно за всяка една виртуална верига. Всяка АТМ клетка съдържа информация за виртуалния път (VPI - Virtual Path Information) и информация за виртуалната верига (VCI - Virtual Circuit Information). АТМ комутаторът използва тази информация, за да изпрати получените клетки към подходящото устройство.

Връзката при АТМ е ориентирана. В контекста на логическата връзка, това дава възможност за поддържане на протоколи, като TCP/IP и IPX/SPX.

АТМ може да поддържа два типа връзки:

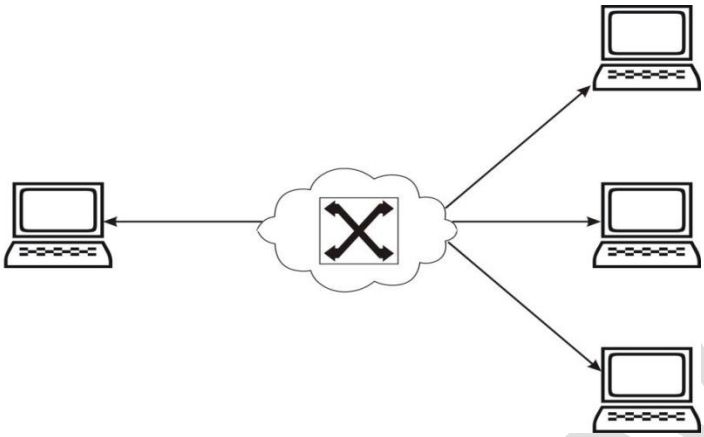
- връзки от типа точка до точка;
- връзка от типа точка да много точки;

При първия тип връзки (фиг.5.3) две устройства се свързват с виртуална връзка през един АТМ комутатор. Такива връзки могат да се използват за еднопосочен или двупосочен трансфер на данни.



Фиг.5.3

Вторият тип връзки- от точка до много точки (фиг.5.4), са малко по-сложни. Те могат да се използват само за еднопосочно предаване от една станция към много получатели.



Фиг.5.4

Увеличаването на Интернет трафика и възможността за неговата интеграция с трафик от другите видове услуги в рамките на единна мултисервизна мрежа правят ATM по същество най-перспективната концепция за развитие на телекомуникациите в света. Вече започналия преход към широколентови гигабитови мрежи съществено разширява областта на приложение на ATM.

ATM е за сега сравнително скъпа мрежова технология, изискваща използване на специализиран ATM хардуер (мрежови карти, хъбове и др.). Независимо от това тя успя да си пробие път и да се наложи като популярна технология. Днес много експерти предричат, че в бъдеще ATM ще се превърне в масова технология за изграждане както на LAN, така и на WAN мрежи.

Международният съюз по телекомуникации препоръчва при изграждането на такива мрежи да се прилага концепцията за широколентова мрежа с интеграция на услугите B-ISDN , представляваща сама по себе си мрежа с пакетна комутация по виртуални канали. Идеята за създаване на B-ISDN посредством ATM технологията възниква като принципно нова парадигма за построяване на телекомуникационни мрежи.

Перспективни WAN технологии

Развитието на комуникационното оборудване постоянно води до появата на нови, по-бързи и по-ефикасни WAN технологии. Много от тях взаимодействат една с друга за осигуряване на поддръжка на приложения, изискващи висока пропускателна способност, като тези, които се използват днес, и тези, които се очакват в бъдеще.

OC-SONET

OC означава optical carrier (оптична носеща), а SONET означава Synchronous Optical Network (синхронна оптична мрежа). SONET е протокол от физическия слой, който осигурява високоскоростно предаване с използване на оптичен кабел. SONET има възможност за скорости на предаване почти до 20 Gbps, а ATM може да се изпълнява по SONET за постигане на много високи скорости на трансфер на данни.

Скоростта на SONET се измерва по стандартите на OC. Достъпните скорости на предаване (наречени OC нива) са следните:

- OC-1 (базова скорост) - 51,84 Mbps
- OC-3 - 155,52 Mbps
- OC 12 - 622,08 Mbps
- OC -48 - 2,488 Gbps

Широколентов ISDN

Широколентовият ISDN (BISDN) представлява перспективна технология, предназначена за използване на оптичен кабел и радиовълни за предаване на данни на високи скорости по SONET, FDDI (Fiber Distributed Data Interface) и Frame Relay.

Широколентовите технологии, които могат да изпращат множество канали с данни, видео и глас по един и същ кабел или друга преносна среда, нарастват по популярност с нарастването на връзките към Интернет и други мрежи с изисквания за висока пропускателна способност. Други широколентови технологии са DSL и кабелните модеми.

CATV

Компаниите за кабелна телевизия (CATV) усетиха страхотна възможност: Те вече притежаваха развита инфраструктура от коаксиален кабел в повечето големи градове и много селски райони. Този кабел можеше да бъде използван не само за предаване на телевизионни сигнали, а също за предаване на компютърни данни. Множество кабелни оператори днес предлагат акаунти за достъп до Интернет.

Кабелът не е основна WAN технология. Първоначално той бе предназначен да ви позволи да комуникирате само със сървъра на кабелната компания (под формата на приемане на входящи телевизионни канали). Макар че всички клиенти бяха свързани към

една и съща мрежа с коаксиален кабел, преминаващ през техните съседи, мрежата не беше предназначена за комуникация между самите крайни абонати. Реално мрежата изобщо не беше проектирана да дава на потребителите възможност да си предават данни, а само да ги приемат. Кабелният модем промени всичко това.

Достъпът до Интернет по кабел изисква кабелен модем, който се свързва както към входящия коаксиален кабел, така и към мрежовата интерфейсна карта на компютъра на потребителя (обикновено това е lOBaseT Ethernet карта).

В този сценарий кабелната компания играе ролята на ISP за потребителя. Няма възможност за отделяне на физическата линия от услугата за достъп, както при достъпа по телефонни линии. С други думи, не можете да наемете линията от кабелната компания и да я използвате за свързване към сървъра на някой друг ISP.

От друга страна, когато плащате телефонна такса за използване на телефонна линия (независимо дали линията е PSTN или специализирана T-1), можете да закупите Интернет акаунт от всеки ISP, който изберете (включително от телефонната компания, която предоставя линията). Макар че същият този метод е технически възможен при кабела, кабелните компании пакетираха двете услуги заедно и условията на техните договори за услугата изискват да използвате единствено кабелната компания като ваш ISP (доставчик на Интернет).

Кабелната инфраструктура може да поддържа или еднопосочни, или двупосочни предавания. Еднопосочният кабел осигурява предаване по коаксиалния кабел само на низходящия поток (downstream). Качването трябва да бъде извършено по обикновена аналогова телефонна линия, която също се включва в кабелния модем. При еднопосочния кабел скоростите на качване са ограничени до стандартните нива, които могат да бъдат постигнати по PSTN, т.е. по-малко от 56 kbps. Скоростите на сваляне варират от 364 kbps до 1,5 Mbps.

Двупосочният кабел осигурява както качване, така и сваляне по коаксиален кабел. Независимо от това много кабелни компании ограничават скоростта на възходящия поток до 128 kbps, за да откажат клиентите от пускане на сървъри (което често се забранява и от условията на договора с кабелната телевизия).

Кабелът е постоянно включена технология, но еднопосочният кабел пак изисква от вас да изберете изграждане на връзка. Голямо предимство на CATV е нейната ниска цена;

но в много области потребителите се сблъскват с проблеми на надеждността. Тъй като кабелът е технология със „споделена честотна лента“ (т.е. цялата честотна лента или пропускателна способност се разделя между всички потребители, които в даден момент се намират в даден кабелен сегмент), производителността може да спадне, когато множество хора в съседство влязат в мрежата. Съществуват също проблеми със сигурността, които в момента правят CATV по-подходяща за жилищните райони, отколкото за бизнеса.

SMDS

Switched Multimegabit Data Service (SMDS) е нова технология с комутиране на пакети, която е предназначена специално за WAN връзки, подложени на голямо количество „пиков“ трафик. (Пиков означава предаване, което се извършва на пикове, а не в постоянен равномерен поток.)

SMDS е безвръзково-ориентиран; т.е. няма изискване преди да започне предаването на данните да бъде установена връзка или верига. Тя използва сравнително големи пакети, с дължина до 7168 байта. SMDS адресите, които представляват десетцифрени номера (като телефонни номера), се използват за идентифициране на SMDS подмрежата. SMDS връзките се свързват към SMDS суич по гръбнака на мрежата на телефонната компания, обикновено по множество връзки от типа OC-3 SONET. SMDS беше разработена като обществена мрежа за осигуряване на услуги, подобни на тези на LAN, с изключение на това, че обхваща голяма градска област. Скоростите на трансфер на данни обикновено варират от 1,544 Mbps до 45 Mbps. Технологията е мащабируема и може да бъде използвана заедно с ATM. Но SDMS не е широко достъпна като Frame Relay и други услуги, а SMDS оборудването може да бъде намерено трудно.

Безжични WAN мрежи

В много случаи е невъзможно - или най-малкото неудобно или скъпо - да се прокара кабелна линия за свързване на WAN сайтове. Безжичните решения са особено подходящи, когато е важно данните да бъдат комуникирани в реално време, или когато потребителите са в движение. Безжичните WAN работят най- добре при комуникация на малки количества данни.

Безжичните технологии, използвани за WAN, са следните:

- **Радиочестотни (RF) технологии** - Specialized Mobile Radio (SMR) осигурява скорости за предаване на данни от 1200 bps до 19 200 bps. Разширеният SMR (ESMR) е цифровата реализация на SMR.
- **Сателитни технологии** - Тази технология използва както услуги с комутиране на вериги, така и услуги с комутиране на пакети на скорости от 4800 до 9600 bps.
- **Микровълнови технологии** - Тази технология използва клетъчни техники на микровълнови честоти за осигуряване на висока скорост и капацитет (безжична широка лента).
- **Клетъчни технологии** - Това осигурява връзка с комутиране на вериги по аналогови или цифрови клетъчни връзки.
- **Технологии за мрежи с пакети от данни** - Тази технология осигурява WAN с комутиране на пакети без настройка на обаждането.

Характерна особеност на безжичните комуникации е че те са по-скъпи и относително бавни. Например, аналоговите клетъчни системи обикновено осигуряват скорости на трансфер не повече от 14 000 докато цифровите клетъчни системи осигуряват до 64 kbps.

5.3 Връзки между LAN и WAN

В наши дни нито една LAN не е самостоятелен остров. Почти всяка LAN е свързана с някаква друга мрежа, най-често с корпоративна WAN или с Интернет или с двете едновременно. Съществуват няколко начина за свързване на LAN с външния свят. Най-очевидният, но и най-примитивен начин, е да снабдим всеки един от компютрите с модем, ADSL адаптер или с ISDN адаптер и посредством телефонна линия да осъществим връзка с Интернет доставчик (ISP – Internet Service Provider) или отдалечен сървър. Освен за хардуер (модеми и/или адаптери), този начин изисква заплащане и за ползване на телефонните линии, а при връзка с Интернет доставчик (ISP) и за ISP акаунт за всеки един от компютрите. Контролът върху такъв вид връзка на LAN с външния свят е слаб, което крие сериозни рискове за сигурността, ако данните в LAN имат конфиденциален характер.

Съществуват по-добри алтернативи за връзка на LAN с WAN. Всяка една от тях има своите предимства и недостатъци пред останалите. Те биват реализирани чрез използване на:

- транслирани връзки;
- прокси сървъри;
- маршрутизирани връзки.

Транслирани връзки

В ценово отношение това е един от най-ефективните варианти. В него се използва така наречената мрежова адресна транслация (NAT - Network Address Translation , Native Address Translation или IP Masquerading). Тя позволява на всички компютри от LAN да осъществяват достъп до външния свят само през един компютър, използващ една телефонна линия или безжична връзка и един ISP акаунт. Компютърът се намира на границата между LAN и WAN и притежава два интерфейса за връзка с двата вида мрежи. Той притежава регистриран публичен IP адрес за комуникация с WAN и частен IP адрес, използван само вътрешно в LAN. Компютърът бива наричан NAT сървър или още хост за адресна транслация. Най- често хардуерно той представлява маршрутизатор (рутер) в съчетание със защитна стена (firewall).

Защитната стена е софтуер, който съхранява сведения за трафика в една мрежа и следи за коректността на комуникацията. С помощта на пакетни филтри защитните стени разпознават легитимните пакети, участващи в комуникацията, като отхвърлят ония от тях, които не отговарят на условията за легитимност.

Адресната транслация се състои в това, че асоциира частния IP адрес на компютъра от LAN, изпращащ данни навън, с номер на порт от NAT сървъра. Тази информация се запомня в NAT сървъра, в таблица на преобразуваните адреси, добавя се към IP хедъра на изпращаните пакети и заедно с IP адреса на сървъра се изпраща навън във WAN. Когато WAN върне даден отговор на LAN, например някакъв Web сайт, NAT сървърът се консултира с таблицата на преобразуваните адреси, намира съответствието между пакетите и компютъра от LAN, изпратил заявката, и му препраща сайта.

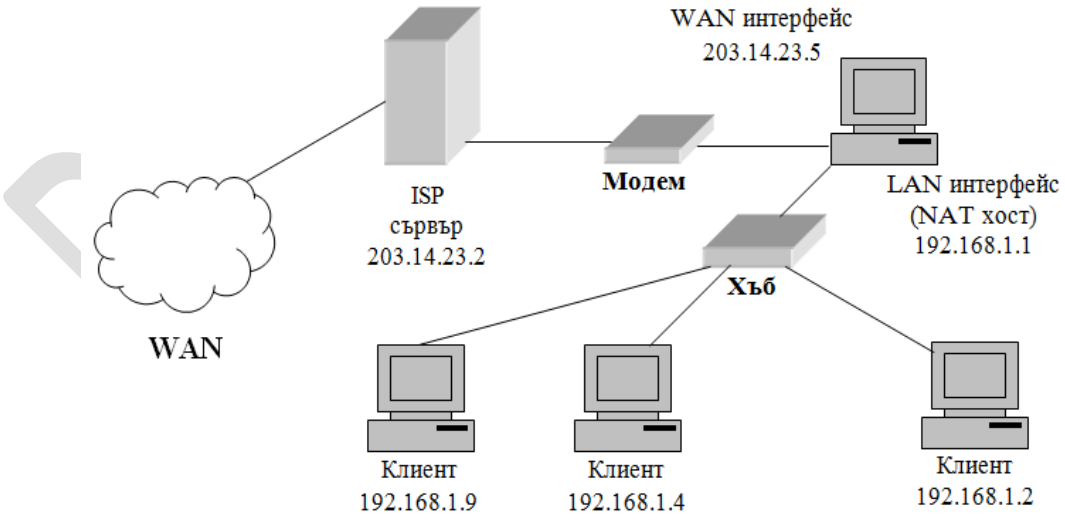
Днес NAT се използва съвместно с IP маскирането (IP masquerading), което представлява вид техника за скриване на адресно пространство. Използва се най-често за скриване на частните IP адреси на LAN зад един или няколко IP адреса от друго външно адресно пространство, най-често публично, каквото е това на Интернет. За целта

спецификацията RFC 1918 дефинира три адресни обхвата за използване от LAN. Те са приведени по-долу в таблицата, като са представени в три еквивалентни форми:

Табл.5.1

Диапазон на частните IP адреси	Обобщен начин на запис на диапазона	CIDR запис
10.0.0.0 – 10.255.255.255	10.x.x.x	10/8
172.16.0.0 – 172.31.255.255	172.16.x.x	172.16/12
192.168.0.0 – 192.168.255.255	192.168.x.x	192.168/16

Горепосочените адресни пространства се предназначени само за локални мрежи и не са достъпни отникъде, освен от локалната мрежа. Поради това те са естествено защитени от директни външни атаки. В съответствие с RFC 1918 на NAT сървърът се присвоява първият частен IP адрес от използваното за LAN адресно пространство (фиг.42). Първичната функция на NAT сървъра е да осигурява достъп до WAN, като препредава заявките от LAN във WAN, използвайки пред хостовете във WAN някой от своите публични IP адреси (маскира частните IP адреси, masquerading). По този начин се осигурява еднопосочен достъп на LAN до Интернет. NAT сървърът може да се свързва директно с други хостове, притежаващи рутируеми (регистрирани публични) IP адреси. Хостовете извън локалната мрежа не могат да се свързват с NAT сървъра посредством неговия частен IP адрес.



Фиг.5.5

По време на своята работа NAT използва маскиране на частните адреси, като по този начин определя дали заявката е предназначена за локалната мрежа или за WAN. В

първия случай съобщението остава за локално ползване. Във вторият случай, рутерът, след като преобразува по съответен начин частния адрес, осигурява транзитен трафик на съобщението към WAN.

На фиг.5.5 процесът на транслацията протича по следния начин:

1. Клиентският компютър с частен IP адрес 192.168.1.9 изпраща посредством своя браузър HTTP заявка до URL ресурса с IP адрес www.google.com.

2. NAT хостът асоциира заявката от 192.168.1.9 с номер на порт в таблицата на преобразуваните адреси. В нея се записва IP адреса на източника на заявката и IP адреса на нейното местоназначение, както и номерата на портовете на източника и на получателя (в случая двата номера ще са 80, тъй като се извършва HTTP комуникация).

3. NAT хостът променя хедъра така, че източника на заявката не е 192.168.1.9, а публичния адрес 203.14.23.5, назначен от Интернет доставчика.

4. NAT хостът изпраща заявката за www.google.com до ISP сървъра. DNS услугата преобразува името на домейна в IP адреса на сървъра, на който се съхранява началната страница на www.google.com.

5. Заявката са приема и изпълнява от www.google.com. Страницата се изпраща на публичния IP адрес 203.14.23.5 на NAT хоста.

6. NAT хостът извършва обратна транслация на IP адреса в съответствие с таблицата на преобразуваните адреси и определя, че трябва да изпрати страницана на порт 80 на клиента с адрес 192.168.1.9.

Много от съвременните NAT устройства позволяват на мрежовия администратор да конфигурира таблицата на преобразуваните адреси така, че тя да бъде постоянна, т.е. на частните IP адреси да съответстват точно определени външни IP адреси, табл.5.2 :

Табл.5.2

Вътрешен (частен) IP адрес	Външен (публичен) IP адрес
192.168.1.1	193.65.76.1
192.168.1.2	193.65.76.2
. . . . .	. . . . .
192.168.2.1	193.76.77.1

Такъв вид преобразуване на адресите бива наричано статично (static NAT). То позволява на трафик, възникнал във външната мрежа, да прониква във вътрешната.

Съществува и динамично преобразуване (dynamic NAT), при което определен брой външни IP адреси на маршрутизатора са конфигурирани така, че да влизат в употреба за обслужване на вътрешни адреси само при нужда. В този случай само една част от вътрешните адреси са свързани твърдо с външни такива. Останалата част от вътрешните адреси биват свързвани с външните такива динамично.

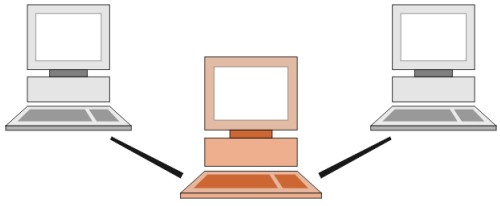
NAT преобразуването стана популярно в средата на 1990-те години, като средство за преодоляване на недостига на IPv4 адреси. То получи разпространение особено в страни, в които по исторически причини бяха алокирани малък брой адресни блокове. Днес NAT е стандарт, който стана задължителен за рутерите, предназначени за връзка на домашни мрежи или на малки офис-мрежи с Интернет.

NAT технологията бива наричана понякога споделяне на връзка или IP маскиране.

Друг по-интелигентен, но по-труден за конфигуриране, начин за осъществяване на връзка между LAN и WAN е използването на **прокси** сървър.

Прокси сървъри

Прокси сървърът (proxy server) представлява сървър, който обслужва клиентите си чрез препращане на заявките им към други сървъри. Той изпълнява ролята на посредник (фиг.5.6), отделяйки LAN мрежата от външната мрежа, като би могъл да осигурява и защити чрез филтриране на входящите и изходящите пакети. Клиентите се обръщат към прокси сървъра със заявки за получаване на файл, Web страница или някакъв друг ресурс от друг сървър. След като получи заявка прокси сървърът проверява настройките си за филтриране, зададени от администратора. Ако заявката удовлетворява изискванията на филтъра, сървърът преминава към нейното обслужване. Той осъществява връзка със сървъра, указан от клиента, и заявява услугата, посочена също от клиента. Прокси сървърът би могъл да променя клиентската заявка и/или получения от сървъра отговор.



фиг.5.6

Прокси сървърът е в състояние да обслужва клиентите без да се обръща към указаните от тях сървъри. За целта той кешира (съхранява в себе си) отговорите на

отдалечените сървъри и при повторно обръщане (на същия или на друг клиент) към съхранен в кеша ресурс, той го предоставя директно, от кеша си, без да се обръща към отдалечения сървър. Това повишава значително Web производителността.

Прокси сървър, който препредава заявките на клиентите и отговорите без да ги променя, биват наричан тунелиращ прокси (tunneling proxy) или още по-просто - шлюз (gateway). Както при NAT, клиентите от LAN, осъществяващи достъп до Интернет посредством прокси сървър, остават невидими за външния свят. Цялата външна комуникация се извършва от прокси сървъра. Нещо повече, прокси сървърите биха могли да комбинират NAT и прокси технологиите.

Прокси сървърът, като програма, може да бъде инсталиран в потребителски (локален) компютър или да бъде конфигуриран като отделна компютърна система.

Според функциите, които изпълняват, прокси сървърите биват най-различни. Някои от тях са следните:

- Кеширащ прокси сървър. Както вече споменахме, кеширащото прокси съхранява в своя кеш копия на често заявяваните ресурси. Процесът се нарича кеширане. То драстично увеличава производителността, разтоварва Интернет мрежата и значително намалява разходите на организациите за ползване на Интернет.
- Web прокси сървър. Това е прокси, което служи единствено за обслужване на Web трафик. Web прокси сървърите са същевременно и кеширащи сървъри. Повечето web прокси програми предоставят средства за забрана на достъпа до URL ресурси, указвани предварително в „черен списък". Някои web проксита извършват преформатиране на web страниците, пригаждайки ги за изобразяване върху такива устройства като мобилни телефони и PDA.
- Анонимни прокси сървъри. Най-често това са web проксита, които дават възможност за анонимно сърфиране в Интернет.
- Вражески прокси сървъри (hostile proxy). Това са проксита, инсталирани и ползвани с недоброжелателна с цел. Те подслушват данновия поток между набелязана клиентска машина и Интернет мрежата. Всички изпращани форми и приемани страници биват прихващани и анализирани. При

откриване в мрежата на такова прокси, необходимо е да бъдат променени веднага паролите за ползване на онлайн услуги.

В сравнение с NAT технологията, прокси сървърите осигуряват повишена производителност и повече защита. Софтуерът за тях обаче е по-скъп и се инсталира и конфигурира по-трудно, защото Интернет приложенията на всички клиентски машини, като например Web браузърите, трябва да бъдат индивидуално конфигурирани за ползване на прокси. При използване на NAT е достатъчно да настроите клиентската машина да ползва Интернет протокола TCP/IP и да укажете, че IP адресът на същата ще бъде назначен автоматично посредством DHCP сървър. Всичко останало се извършва автоматично от DHCP.

За различните операционни системи се предлагат множество приложения за прокси сървъри, подробна информация за които читателят може да намери в Интернет, например на адреса: http://en.wikipedia.org/wiki/Proxy_server.

Маршрутизирани връзки

При маршрутизираните връзки всеки един от компютрите в LAN има директен достъп до Интернет или до корпоративна WAN. За разлика от NAT и прокси технологиите тук липсва посредник. Вместо това всеки компютър от LAN, който се свързва с външния свят, притежава свой собствен регистриран публичен IP адрес и е свързан към маршрутизатор (рутер).

NAT технологията, използваща транслиране на адреси, е по-икономична, понеже изисква използване на само един IP адрес. Но тя не винаги е подходяща. Например протоколи, които в IP хедъра не съхраняват адресна информация, не биха могли да работят с NAT. В други случаи, например когато пакетите се автентикират и криптират с помощта на IP Security (IPSec), адресната транслация е направо невъзможна.

Маршрутизираната връзка изисква специализирано маршрутизиращо устройство, каквото е маршрутизаторът, или използване на компютър, чиято операционна система да позволява той да изпълнява ролята на маршрутизатор.

Компютрите от LAN, които ще комуникират с WAN, трябва да бъдат конфигурирани, както следва:

- да притежават IP адрес, който да е валиден за мрежата, в която той ще комуникира;
- да има установена подмрежова маска (т.3.4, подточка „Автоматично разпределяне на адреси”), определяща каква част от IP адреса идентифицира мрежата и каква част компютъра.

Ако компютрите от LAN ще се свързват с Интернет, те трябва да бъдат допълнително конфигурирани и с адрес на DNS сървър, получен от Интернет доставчика, както и с IP адреса на маршрутизатора, който ще изпълнява ролята на подразбиращ се шлюз.

Маршрутизирането е съществено важен аспект на TCP/IP, който е отговорен за междумрежовите комуникации и комуникациите в Интернет. Маршрутизирането означава препращане на пакети от една мрежа в друга. Както е известно IP протоколът използва логически адреси и маршрутизиране на пакетите. Когато се изпраща пакет, протоколът взема IP адреса на източника и този на местоназначението и с помощта на подмрежовата маска определя дали компютърът получател се намира в същата подмрежа или в друга. В случай, че той се намира в същата подмрежа, пакетът му се доставя директно. Ако компютърът е в друга мрежа, пакетът се изпраща на подразбиращия се шлюз (default gateway) и той го насочва по местоназначение.

Маршрутизаторът трябва да има две мрежови връзки – едната към LAN и другата към външната мрежа. За да бъде настроен за връзка с Интернет, необходимо е TCP/IP протоколът му да бъде конфигуриран с: IP адрес, подмрежова маска и адрес на DNS сървър, осигурени от доставчика на Интернет. След това е нужно да бъде конфигуриран статичен подразбиращ се маршрут за използване на Интернет интерфейса.

Въпросите с маршрутизирането са разгледани в раздел 6.

Моля, отговорете на контролните въпроси:

1. *Какви са осбеностите при FrameRelay технологията ?*
2. *Кой метод на комутация на пакети или вериги е по-добър и защо?*
3. *Коя е най-перспективната глобална технология?*
4. *Какво е предназначението на прокси сървър?:*
5. *Каква е разликата между NAT и PAT?.*

Раздел 6

Рутиране на данни. Рутиращи протоколи

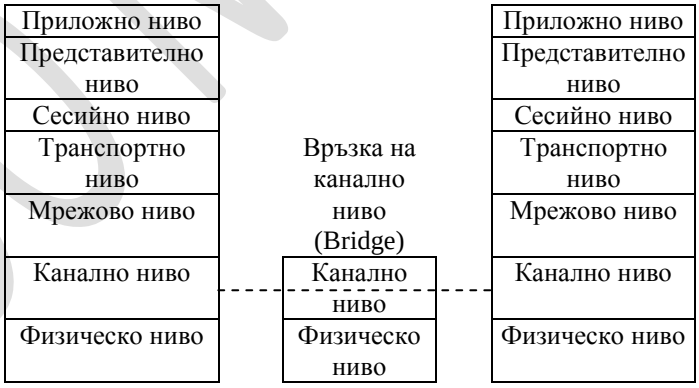
Ключови думи и съкращения

Рутиране - статични, динамично	**RIP**
Рутиращ протокол	**OSPF**
Метрика	**BGP**
Автономна система	**Административна дистанция**

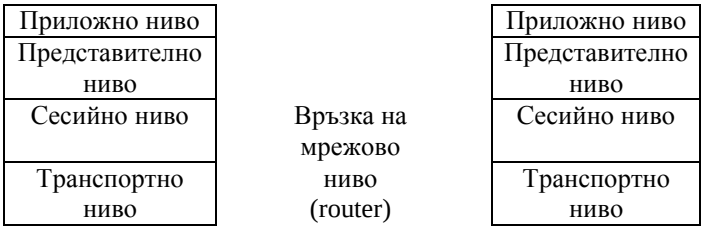
Една от основните функции на IP е способността да формира връзки между различни физически мрежи. Това е възможно поради гъвкавостта на IP да използва почти всякакви физически мрежи на по ниско йерархично ниво, както и на алгоритъма за маршрутизиране на ниво IP. Система, реализираща процеса на маршрутизация се нарича рутер, макар че се използва и термина IP шлюз (gateway).

6.1 Основи на рутирането (маршрутизирането)

Процесът на придвижване на пакети информация от един IP-адрес към друг се нарича маршрутизиране (routing). В рамките на този раздел е необходимо да бъде направено следното уточнение с цел да не се смесват понятията. В литературата процесът на маршрутизация много често се дефинира, като процес на връзка между физически мрежи от различен вид. От гледна точка на еталонния модел за отворени комуникационни системи това твърдение е неправилно.



а) Обмен на информационни пакети на канално ниво



б) Обмен на информационни пакети на ниво мрежови (IP) сегменти

Фиг. 6.1 Обмен на информационни пакети в съответствие с еталонния модел OSI/ISO

Не е задължително отделните IP- адресни сегменти да съответстват на физически мрежи. Маршрутизацията е процес, реализиран на по високо йерархично ниво в еталонния модел (фиг. 6.1).

Устройството мост (bridge) реализира трансфер на информационни пакети (кадри) използвайки съответствие с таблицата си за налични хардуерни адреси (фиг. 6.1 а). На тази база съответният кадър се пренасочва или респ. се отхвърля. Тези устройства по принцип се използват за реализация на връзки в локални мрежи.

Устройството маршрутизатор (рутер) реализира връзка на мрежово ниво. Той има възможности за определяне на оптимален път и осигурява преразпределение на мрежовия трафик. Тези устройства могат да свързват както локални, така и отдалечени компютърни мрежи.

Функция "маршрутизиране" е част от мрежовия (интернет) слой, макар че главната функция на един рутиращ протокол е да обменя информация за рутирането с други рутери. Една от основните задачи на маршрутизатора е определяне на най-добрия път. За тази цел маршрутизаторите използват различни мерни единици (метрика).

Мерните единици представляват оценки или стойности на даден параметър на мрежовата връзка. Най-често използваните от маршрутните протоколи мерни единици са:

- ✓ брой преходи (Hop count) - една от най разпространените мерни единици. С помощта на нея се проверява броя на рутерите през които е преминал даден пакет информация от мрежата източник към мрежата получател;
- ✓ закъснение (Delay) - с помощта на тази единица се измерва времето необходимо за придвижване на информационен пакет от информационната мрежа източник до съответната мрежа - получател. Факторите, от които зависи това време могат да бъдат разнообразни. В тях се включват пропускателната способност на комуникационните канали, броя заявки за обслужване на всеки един от съответните

маршрутизатори, разстояния между отделните мрежи, временни натоварвания или задръствания и др.;

- ✓ пропускателна способност - тази мерна единица указва възможностите на отделните комуникационни канали. По-високата пропускателна способност е винаги за предпочитане пред по ниската;
- ✓ надеждност - посредством оценката, отразена в тази мерна единица се правят заключения на надеждността на мрежовите връзки. Някой връзки излизат от строя по често, отколкото други. Предпочита се винаги по високата надеждност. Един от параметрите на надеждността е времето за възстановяване на пропадналата връзка;
- ✓ оценка състоянието на връзката – параметър, указващ относителни качества, като напр. важност, скорост и др.;
- ✓ цена на комуникацията - не винаги доставянето на информацията е единствената цел при нейното осъществяване. Много често е необходимо да се прави съотношението цена/към качество на комуникацията.

При различните протоколи за маршрутизация се използват различни параметри и измервателни единици. Някои от тях позволяват да се прави комбинация от отделните мерни единици и на тази основа да се реализират нива на значимост на отделните връзки. По този начин намирането на оптималния път се превръща в решаването на задача за целево оптимиране.

Налични са два основни начина за конфигурация на процеса маршрутизация. Първият се нарича статично маршрутизиране. Той изисква ръчна настройка на всички налични пътища в рамките на компютърната мрежа. Статичната маршрутизация работи най-добре в компютърни мрежи, със строго установена топология, без чести промени. При промени е необходимо ръчно преконфигуриране. В противен случай маршрутизацията няма да бъде коректна. В известна степен една такава конфигурация създава неудобството, свързано с повече разходи при поддръжката. Ако един от маршрутизаторите излезе от строя поради повреда, е необходима ръчна намеса за пренастройване на информационните пътища. Такива реализации изискват по-висока квалификация на системните и мрежовите администратори.

Другият начин на конфигуриране е посредством динамично маршрутизиране. В основата си динамичното маршрутизиране използва протоколи за автоматично

построяване на маршрутни таблици, описващи мрежата. При възникване на промяна в мрежата динамичният рутиращ протокол обявява тази промяна на всички маршрутизатори. В следващ момент следва преизчисляване на оптималните пътища за трансфер на информацията. Най разпространени протоколи за динамично рутиране това са:

- дистанционно-векторни протоколи;
- протоколи със следене състоянието на връзката.

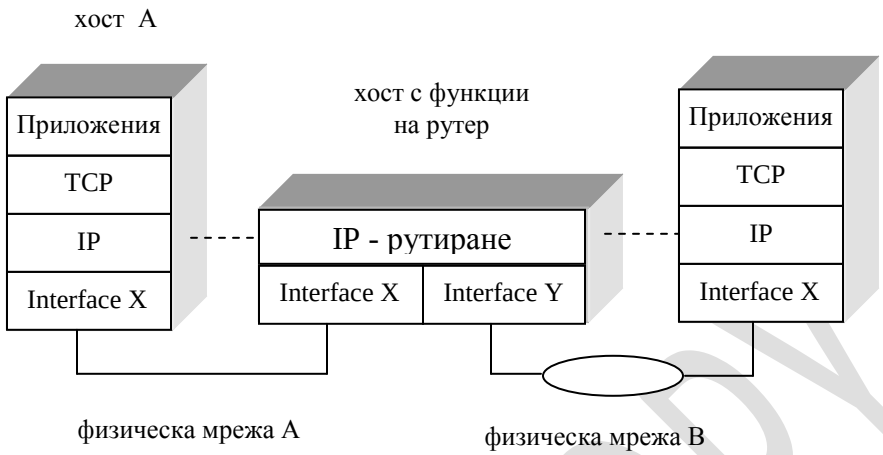
По-разпространени са дистанционно-векторните протоколи поради лесното им конфигуриране. В много случаи тези протоколи създават проблеми в мрежата, понеже са базирани на комуникация от множествен тип (broadcast) и създават условия за увеличаване на мрежовия трафик. В тази връзка е необходимо да се отбележи и сравнително голямото време за изчакване, необходимо на мрежата да се приспособи към направените в нея промени. Удобни са за неголеми компютърни мрежи.

Протоколите със следене състоянието на връзката дават възможност за обновяване на маршрутната информация във всички възли на мрежата. Фактът, че в рамките на тези протоколи се използва преди всичко комуникация от тип unicast или multicast създава възможности за редуциране на цялостния мрежови трафик. Неудобството при тях е необходимостта от по висока квалификация на обслужващия персонал по време на планирането и конфигурацията, и завишените апаратни и програмни изисквания към използваната техника.

Рутиране на ниво IP

Основната функция на рутирането се съдържа във всички реализации на IP:

- входящата IP датаграма, в която е посочен краен адрес, различен от адреса(адресите) на компютъра, се третира като нормална изходяща датаграма;
- тази изходяща IP датаграма се подлага на алгоритъма за IP рутиране в локалния хост, който избира следващата стъпка за датаграмата (в частност следващия компютър на който датаграмата да се изпрати). Следващият компютър може да бъде разположен в произволна физическа мрежа, към която е свързан междинния компютър. Ако тази мрежа е различна от мрежата, от която е получена датаграмата, то като краен резултат се явява факта, че междинният компютър е препредал IP датаграмата от една физическа мрежа към друга (фиг. 6.2).



Фиг. 6.2 Схема на IP-рутиране

Нормалната таблица за рутиране съдържа информация за мрежите, свързани към компютъра и IP адресите на техните рутери, плюс мрежите, свързани към тях. Тя може да се разшири с информация за по-далечни IP мрежи, както и път по подразбиране (default), но тя си остава таблица с ограничена информация, т.е. тя съдържа само част от всички възможни IP мрежи. По тази причина такива рутери се наричат рутери, съдържащи частична информация за рутиране.

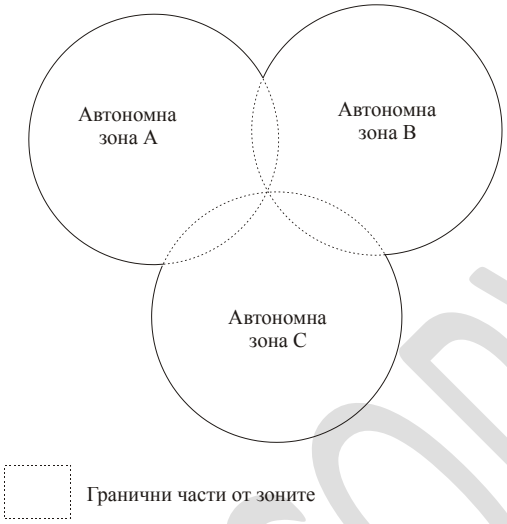
Основните причини за наличието на множество протоколи биха могли да се резюмират по следния начин:

- в терминологията на ***Internet*** е обособена концепцията за група мрежи, наречени "автономна система" (AS), които се администрират като цяло;
- появата на AS с различни размери предизвика търсене на адекватни решения за рутирането. За малки и средни AS популярни станаха група дистанционно-векторни протоколи за рутиране (напр. RIP). Протоколите със следене на състоянието на връзката (Link State - протоколите), като OSPF, са значително по-подходящи за такива мрежи;
- за обмен на информация за рутиране между AS бяха разработени специални протоколи (BGP - border gateway protocols)

Автономни системи

Автономната система представлява набор от мрежи и шлюзове между тях със своя собствена информация и механизми за маршрутизиране. Автономна система (АС)

(фиг.6.3) се дефинира като логическа част от по-голяма IP мрежа, която се администрира от самостоятелно звено.



Фиг. 6.3 Рутиращи автономни зони

АС обикновено обхваща мрежата в една организация и се обозначава като такава, за да може да комуникира чрез публичната IP мрежа с АС принадлежащи на други организации. Автономната система е мрежа, управлявана от единична група за мрежово управление. За идентификация на автономната система е възможно да се направи заявка в InterNIC за номер. Информацията за рутиране, предоставяна за останалите мрежи е само най-необходимата, за да има възможност да се достигне съответната автономна система.

Съвременният модел на рутирането е изграден на принципа на комуникиращи равноправни автономни системи. Те обменят информация по между си. Всяка автономна зона обработва информацията, получена от останалите. За разлика от йерархичния модел, тази концепция позволява независимост от една обща част за определяне на оптимални условия за рутиране. Всяка една от зоните извършва това определяне за себе си. Фиг. 6.3 онагледява тази концепция.

Протоколите за динамично рутиране биха могли да се разделят на две групи:

- вътрешни портални протоколи (IGP) – примери за такива са OSPF и RIP;
- външни gateway протоколи (EGP) – пример за такъв е Border Gateway Protocol Version 4 (BGP-4)

Порталните протоколи са външни или вътрешни в зависимост от това дали се използват в рамките на една автономна система или за свързване между автономни системи.

Вътрешните портални протоколи дават възможност на рутерите да обменят информация в рамките на една автономна система. В рамките на АС, вътрешните портални протоколи определят оптималните маршрути между локално управляваните мрежи.

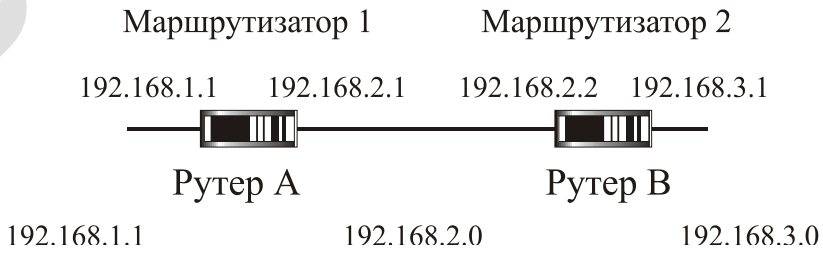
6.2 Алгоритми използвани при IP рутиране

Алгоритмите за IP рутиране могат да бъдат статични и динамични. Динамичните алгоритми дават възможност на рутерите да обменят информация за пътищата и връзките, на чиято база се пресмятат най-добрите пътища за препращане на съобщенията. Възможно е, използването на статичното рутиране в допълнение към динамичното.

6.2.1 Статично IP рутиране

Статичното IP рутиране изисква пътищата да бъдат конфигурирани ръчно за всеки рутер, което е една от главните причини системните администратори да избягват този метод, ако имат възможност.

При статичното IP-рутиране всички маршрути се задават от мрежовия администратор. Този тип маршрутизиране се използва основно при малки мрежи, тъй като всяка промяна в мрежата налага ръчно модифициране на статичните маршрутни таблици. При статичното IP-рутиране е необходимо да бъдат указани пътищата до всеки маршрутизатор за всеки маршрутизатор в мрежата. Ако в даден момент за даден мрежови IP-сегмент не бъде зададен маршрут, то към този сегмент не е възможно да се изпращат пакети. На фиг. 6.4 е показана схема на фрагмент от IP-мрежа, изискваща статични пътища към всеки маршрутизатор. Статичните маршрутни таблици определят как да бъдат пренасяни отделните IP пакети от мрежата източник към мрежата получател.



Фиг. 6.4 Схема на статични маршрути

Статичното рутиране има недостатъка, че достъпността на мрежата не зависи от съществуването и състоянието на самата мрежа. Ако някое направление е отпаднало, а указателите за него остават в таблицата за рутиране. По тази причина трафикът ще продължи да се изпраща в това направление без да се търсят и видят алтернативните пътища, ако има такива. Налични са решения за преодоляване на този недостатък, включително стандартизирания RFC 2338 VRRP (Virtual Router Redundancy Protocol) и продуктовата му реализация посредством параметъра nexthop awareness (“знание за следващия етап”).

За опростяване на работата на системните администратори, ръчното конфигуриране обикновено се избягва, особено за големи мрежи. Все пак, има обстоятелства, при които е примамливо да се използва статично рутиране. Например:

- за дефиниране на път по подразбиране или на път, за който не е съобщено в мрежата;
- за допълване или заместване на външни портални протоколи когато:
    - тарифите за линиите между АС са такива, че е желателно да се избегне рутирането на протоколна информация;
    - трябва да се прилагат твърде сложни техники за рутиране;
    - желателно е да се избягнат сривове, причинени от дефектни външни шлюзове в други АС.

Правилната настройка на статичните рутери, въпреки някой от посочените недостатъци гарантира по-висока пропускателна способност на отделните IP сегменти. За тяхното обслужване е необходима и по-висока квалификация на отделните мрежови администратори.

6.2.2 Дистанционно векторно рутиране (Distance Vector Routing)

Принципът на дистанционното векторно рутиране е много прост. Всеки рутер в една мрежа поддържа разстоянието от себе си до всяко известно направление в таблица на векторите. Таблиците на векторите се състоят от набор направления (вектори) и оценки (разстояния) за тяхното достигане и дефинират най-ниските стойности на разстоянията за достигане на целевия адрес при предаване.

Разстоянията в таблиците се пресмятат от информацията, получена от съседните рутери. Всеки рутер съобщава своята таблица на векторите на цялата мрежа. Последователността от операциите за това е следната:

- всеки рутер е конфигуриран посредством идентификатор и оценка за всяка от мрежовите си връзки. Оценката обикновено се конфигурира като 1, което означава единична стъпка (1 hop), но може да отразява и друга мярка за връзката, като напр. трафика, скоростта, и др.;
- всеки рутер се инициализира с таблица на векторно рутиране, в която оценката за себе си е 0, 1 за директно свързаните към рутера мрежи и безкрайност за всички останали мрежи;
- всеки рутер периодично (обикновено на всеки 30 сек) съобщава своята векторна таблица на всеки от своите съседи. Той може да съобщи таблицата и когато се появи заявка за първата връзка, или когато таблицата се промени;
- всеки рутер съхранява последните таблици, получени от всеки съсед и ги използва за пресмятане на собствената си векторна таблица;
- общата оценка за всяко направление се пресмята като се прибавя оценката, получена от таблиците на съседните рутери, към оценката на връзката до съответния рутер;
- векторната таблица (таблица на рутиране) за всеки рутер се създава като за всяко направление се взема най-ниската възможна оценка.

Алгоритъмът на векторните таблици създава стабилна таблица за рутиране след известен период, зависещ от броя на рутерите в мрежата. Този период се нарича “време за обвързване” (convergence time) и представлява времето, необходимо на информацията за рутиране да се разпространи из цялата мрежа. В голяма мрежа това време може да стане твърде дълго, за да бъде използваем този метод.

Таблиците се пресмятат отново, ако се получи съобщение за промяна от някой съседен рутер, или се промени състоянието на връзката към някой от съседите. В случай, че някоя от връзките в мрежата отпадне, то векторните таблици, получени посредством тази връзка, се изчистват и съответната локална таблица се пресмята отново.

Главното предимство на векторните таблици е, че лесно се използват. Налични са недостатъци, по-важните от които биха могли да бъдат обобщени по следния начин:

- нестабилност, причинена от стари маршрути, които се поддържат между мрежите преди поредното обновяване на съответните локални рутерски таблици;
- дълго време на обвързване (преизчисляване оценката на отделните маршрути) на рутерите при големи мрежи;
- ограничение в размера на мрежата, налагащо се поради ограничаване максималния брой преходи (hops);
- фактът, че векторните таблици винаги се съобщават, дори тяхното съдържание да не е променено.

6.2.3 Рутиране със следене състоянието на връзката (Link State Routing)

Нарастването на размерите на мрежите през последните години наложи замяната на рутирането чрез векторни таблици с други методи, които решават проблемите, описани по-горе. Това са методи, свързани с разработката на нови протоколи, основани на алгоритми "Състояние на връзките" (Link state) или "Първо най-краткия маршрут" (Shortest path first (SPF)). Най-добрият пример е OSPF.

Принципът на рутиране по състоянието на връзките е прост, макар че приложението му не е лесно:

- рутерите отговарят за свързването със съседите и познаването на техните характеристики;
- рутерите създават пакети с информация за състоянието на мрежовите връзки и техните метрики;
- пакетите се изпращат до всички рутери в дадена мрежа;
- всички рутери имат еднакъв списък на връзките в мрежата и могат да създадат еднаква карта на топологията на мрежата;
- картите се използват за пресмятане на най-добрите маршрути за всички направления;
- рутерите се свързват със съседите чрез изпращане на "Hello" пакети към мрежовите си интерфейси. Тези пакети се изпращат до съседите посредством връзки от тип крайна точка-крайна точка (point-to-point) и до мрежите без пълен множествен адрес (non-broadcasting networks). В LAN, пакетите "Hello" се изпращат до предварително

определена група или на множествен (multicast) IP адрес, за да бъдат получени от всички рутери. Съседите, които получават “Hello” от рутер, трябва да отговорят с “Hello” пакети, съдържащи тяхната идентичност;

- щом всички съседи са обменили пакети по този начин, може да се обмени информация за състоянието на връзките;
- информацията за състоянието на връзките се изпраща под формата на пакети за състоянието на връзката (Link state packets - LSP), позната също като обява на състоянието на връзката (Link state advertisement). LSP формират база данни от която всеки рутер може да се пресметне топологията на мрежата. LSP се изпращат само при следните обстоятелства:
  - ✓ когато рутерът открие нов съсед;
  - ✓ когато връзката до съсед отпадне;
  - ✓ когато се промени състоянието на дадена връзка;
  - ✓ на всеки 30 минути се изпращат опресняващи пакети.

Щом даден рутер генерира LSP, важно е той да бъде приет успешно от всички рутери в мрежата. Ако това не се случи, някои рутери ще пресметнат топологията на мрежата на базата на погрешна информация за състоянието на мрежата.

Разпращането на LSP става нормално на базата на рутиращите таблици на всеки рутер. В този случай може да се зададе въпроса: Кое е първичното - кокошката или яйцето. Рутиращите таблици зависят от LSP при своето създаване, а LSP зависят от таблиците при своето разпространение. Една проста схема, наречена flooding, преодолява този проблем и осигурява успешното разпространение на всички LSP в мрежата.

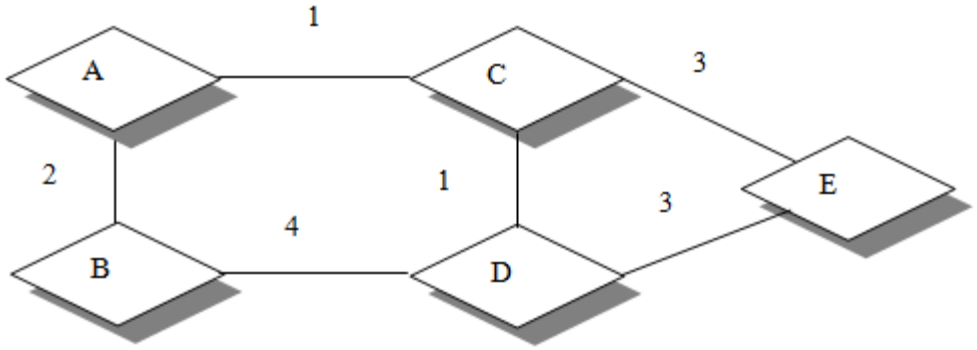
Flooding изисква рутерът, който получи LSP, да го препрати на всички свои съседи, освен на този, от който го е получил. Всички LSP трябва да бъдат точно разпознати, за да се осигури правилно препращане. Те са подредени и съдържат време на своето създаване, за да не се разпространяват дубликати. Когато един рутер получи LSP, той сверява в своята база данни дали е получил LSP с този номер от изпращащия рутер. Ако номерът е същият или по-малък от последния получен, LSP се пренебрегва. В противен случай се добавя към базата данни.

Процесът flooding осигурява на всички рутери в мрежата една и съща информация за състоянието на връзките. Всички рутери тогава могат да пресметнат дървото на най-

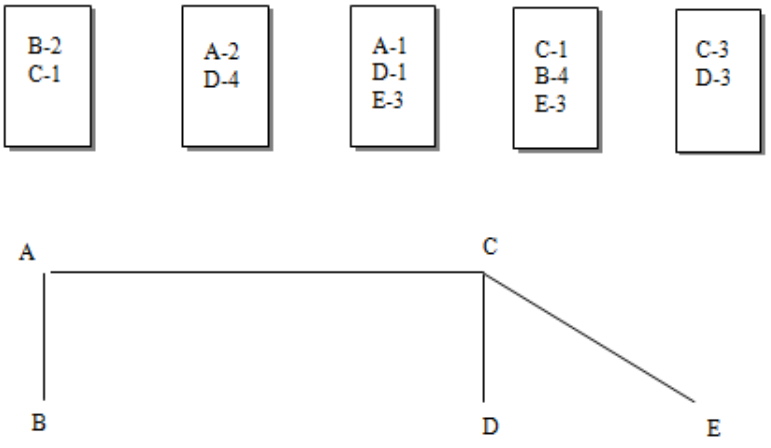
късите за топологията на мрежата маршрути и да избират най-добрите за препращане на трафика.

Алгоритъмът за най-късия път (Short path first, SPF), е алгоритъм, при който в рамките на една автономна система всеки рутер има една и съща база данни за състоянието на връзките, което води до еднакво графично представяне чрез пресмятане на дървото на най-късите пътища с начало самия рутер.

Дървото се нарича “дърво на най-късите маршрути” и дава пълните маршрути до произволен компютър или мрежа. Фиг. 6.5 и фиг. 6.6 показват пример за формиране на дърво от рутер A.



Фиг. 6.5 Примерна конфигурация



фиг. 6.6 Пример за обозначаване на SPF

Всеки рутер A, B, C, D и E има една и съща база данни за състоянието на връзките, както е показано. Рутер A генерира свое собствено дърво на най-късите маршрути, като го пресмята, започвайки от себе си като root (начален).

6.3 Вътрешни портални протоколи (Interior Gateway Protocols - IGP)

Налични са много стандартизирани и специфични вътрешни портални (gateway) протоколи. Вътрешните портални протоколи (IGP) са интегрирани стандартно в повечето операционни системи и рутери. В този раздел ще бъдат накратко разгледани само следните IGP:

- Routing Information Protocol (RIP);
- Routing Information Protocol Version 2(RIP-2);
- Open Shortest Path First (OSPF);

6.3.1 Протокол RIP (Routing Information Protocol)

Протоколът RIP е стандартизиран от IAB протокол. Статусът му е избираем, което означава, че той е един от няколкото налични вътрешни портални протоколи и може да се използва или не в дадена система. Ако в дадена система е имплементиран, то неговото използване трябва да става в съответствие с RFC 1058.

RIP се основава на два протокола за рутиране - Xerox PUP и XNS. RFC за протокола е издаден след появата на няколко негови варианта. По тази причина не са включени всички подобрения на главния протокол за векторно рутиране (напр. poison reverse или triggered updates).

RIP е протокол за дистанционно векторно рутиране, подходящ за малки мрежи. Налични са две версии на RIP. Версия 1 (RIP-1) е широко използван протокол с няколко съществени ограничения. Версия 2 (RIP-2) е подобреният вариант с който се преодоляват ограниченията на RIP-1, оставайки съвместим с него.

RIP определя два типа пакети: заявка и отговор (request, response)

Пакет-заявка (request) се изпраща от рутерите, за да поискат от съседите част от тяхната векторна таблица (ако пакетът съдържа destinations, целеви компютри или мрежи) или цялата таблица (ако пакетът не съдържа такива).

Пакет-отговор (response) се изпраща от рутер за разпространяване на собствената векторна таблица при следните обстоятелства:

- на всеки 30 секунди;
- в отговор на пакет заявка;
- при промяна на векторната таблица (ако се поддържа принудителното обновяване на таблиците).

Като мерна единица за метрика се използва броят преходи. Този подход е разумен, но не осигурява предпочитание за маршрути, използващи бързи мрежови връзки (напр. при някой локални мрежи) пред бавните глобални съединения.

Активните и пасивните системи прослушват всички пакети отговори и съответно обновяват своите векторни таблици.

RIP не се занимава с предаването на подмрежови маски заедно с векторните таблици. Рутер, получаващ RIP пакет отговор, трябва вече да има информацията за мрежовите подмаски, за да може да интерпретира правилно идентификатора на мрежата и частта от IP адреса, идентифицираща конкретния компютър.

Въпреки че RIP е лесно приложим, в неговата реализация са налични няколко съществени проблема. Простотата на протокола не води до решаване проблемите на мрежовите администратори. Някои от основните проблеми на RIP са следните:

- мрежовите подмаски не се обявяват. Съобщенията за обявяване не съдържат поле мрежова подмаска. Без наличността на такова поле се приема, че всички мрежи използват мрежова маска по подразбиране. Ако даден мрежови интерфейс на рутер използва друга мрежова маска за съответната подмрежа, се приема, че всички пътища получени от това направление, използват същата подмаска;
- няма механизъм за разпознаване - примерно наличност на идентификация, посредством пароли. Това дава възможност за включване на рутер, използващ RIP в мрежата, което от своя страна би могло да е предпоставка за потенциално повреждане на маршрутните таблици;
- използват се пълни множествени обяви (broadcast). Това е доста неефективен метод за разпространяване на маршрутна информация. В такъв случай би било далеч по-добре да се използват методи от тип unicast или multicast.

6.3.2 Протокол за рутиране RIP - Версия 2 (RIP-2)

Протоколът RIP-2 е вече-стандартен протокол. Неговият статус е изборен. Той е описан в RFC 1723. Използва се за отстраняване на част от недостатъците на предходната версия.

RIP-2 разширява RIP-1. Той не е толкова мощен като появилия се напоследък вътрешен портален протокол OSPF, но за сметка на това притежава предимствата на лесно прилагане и по-малки заглавни части (overheads). Идеята на RIP-2 е директно да замести RIP, използван в малки и средни мрежи и да може да работи с променливи големини на мрежи (виж описанието на подмрежи в предходните раздели) или надмрежи (виж описанието на безкласово рутиране между домейни - CIDR). Съществено и особено важно предимство на тази разработка е, че може да работи съвместно с RIP-1. Всъщност главната причина за разработването на RIP-2 е използването на CIDR, което не може да се използва с RIP-1.

Протоколът RIP-2 поддържа множествени обръщения (multicasting) вместо пълни множествени обръщения (broadcasting). Това намаля натоварването за хостове, които не прослушват за RIP-2 съобщения. Тази опция може да се конфигурира за всеки интерфейс, за да се осигури оптимално използване на възможностите на RIP-2 в случаи, в които рутерът свързва смесени RIP-1/RIP-2 подмрежи към мрежи използващи само RIP-2. Използването на опознаване (authentication) в смесени среди също може да се конфигурира така, че да отговаря на локалните изисквания.

RIP-2 е реализиран в повечето от последните версии на демона gated при операционните системи UNIX или техните деривати и често е наричан gated Version 3. Поддържа се и от повечето версии на TCP/IP при системите на Microsoft.

6.3.3 Протокол за рутиране RIPng for IPv6

Протоколът RIPng позволява на рутерите да обменят информация за пресмятане на маршрутите през IPv6 мрежа и е документиран в RFC 2080.

Протоколът RIPng е дистанционен векторен протокол, подобен на RIP-2 при реализация на компютърни мрежи от тип IPv4. RIPng е базиран на UDP и изпраща и получава датаграми на порт 521. Необходимо е да се отбележи че, RIPng трябва да се използва само в рутери. Реализацията на IPv6 дава нови механизми за откриване на рутер.

Всеки рутер, който използва RIPng, се смята че има интерфейс към една или повече мрежи, иначе това не е реален рутер.

RIPng, подобно на RIP-2, има следните ограничения, които са специфични за дистанционното векторното рутиране:

- ограничен брой мрежи, при което най-дългият маршрут е с метрика 15;
- RIPng зависи от броенето до безкрайност. Преодоляването на зацикляне би изисквало много повече време;
- фиксирана метрика. Това не е подходящо в ситуации, в които рутерите се избират на базата на приложения работещи в реално време.

6.3.4 Протокол за рутиране Open Shortest Path First (OSPF)

Протоколът OSPF е маршрутен портален протокол, работещ на принципа следене състоянието на връзката. Подходящ е за използване в рамките на една автономна система. Той е създаден за отстраняване на недостатъците при порталния протокол RIP. В сравнение с RIP, при OSPF са предвидени повече възможности за разширяване. По този начин протоколът позволява приложение на динамично рутиране в сравнително големи мрежи.

Протоколът OSPF V2 е вътрешен портален протокол, дефиниран в RFC 2328. Обзор на използването на OSPF V2 е даден в RFC 1246. Този протокол е стандартизиран от IAB, статусът му е по избор. RFC 1812 дефинира единствено OSPF V2 в списъка на задължителните протоколи за динамично рутиране.

Алгоритъмът за намиране на най-краткия път до мрежа, имплементиран в OSPF, е базиран на алгоритъма на Dijkstra. Този алгоритъм намира най-краткия път от единичен възел до всички възли в рамките на компютърната мрежа.

OSPF е важен, защото има ред характеристики, които липсват в другите вътрешни портални протоколи. Тези допълнителни характеристики правят избора на OSPF предпочитан при изграждането на нови и сравнително големи мрежи. OSPF може да се характеризира по следния начин:

- поддържа на рутиране “тип услуга” (TOS type of service routing);
- позволява разпределяне на натоварването;

- дава възможност за разделянето на дадено място (site) на подмножества с използването на зони;
- изисква опознаване (както и при RIP-2) при обмен на информация между рутерите;
- поддържа на специфични маршрути до дадени адреси и специфични маршрути за дадена мрежа;
- намалява мъртвото време за поддръжка на таблицата чрез използване на рутер по предназначение;
- позволява дефинирането на виртуални връзки за поддръжка на несвързани зони;
- позволява използването на мрежови подмаски с променлива дължина (както и при RIP-2);
- импортира RIP и EGP маршрути в своята таблица.

6.4 Външни портални протоколи за рутиране

Външните протоколи за рутиране или външните gateway протоколи (EGP) се използват за обмен на информация за рутиране между рутери в различни автономни системи.

Най-често се използват два външни портални протокола:

- Exterior Gateway Protocol;
- Border Gateway Protocol.

6.4.1 Външен портален протокол EGP (Exterior Gateway Protocol)

EGP е исторически протокол и е описан в RFC 904. Интересно е, че статусът му все още е "препоръчителен".

Протоколът EGP се използва за обмен на информация за рутиране между външни шлюзове (gateways), които не принадлежат към една автономна система. Най общо казано, EGP приема единствен гръбнак и следователно само един единствен път между две АС. Практическото използване на EGP днес е ограничено само за потребители, които искат да изградят частен Internet. На практика EGP бързо се заменя с BGP.

EGP се основава на периодично изпращане на съобщения "Hello"/"I Hear You" за да се следи достъпността на съседите и за заявки за нова информация. EGP ограничава

външните шлюзове, като им позволява да обявяват само онези целеви точки, които са достъпни за цялата автономна система в която е шлюза. По този начин външен шлюз използващ EGP пропуска информация до своите EGP съседи, но не излъчва информация за достъпността на своите съседи (шлюзовете са съседи, ако си обменят информация за рутирането) извън автономната система. Информацията за рутиране, идваща от АС, трябва да се събере от EGP шлюз, обикновено чрез вътрешен портален протокол.

Поради ограниченото му използване, в рамките на това изложение няма да се навлиза в повече подробности.

6.4.2 Външен портален протокол BGP-4 (Border Gateway Protocol)

Протоколът е стандартизиран, статусът му е "по избор". Описан е в RFC 1771. Протоколът BGP е външен портален протокол използван за обмен на информация за достъпността на мрежата между различни АС.

BGP-4 е въведен в Интернет там, където е наличен обмен на информация между автономни системи. Базиран на Classless Inter-Domain Routing (CIDR) (безкласово рутиране между домейни), BGP от беше развит за да поддържа натрупване и намаляване на информацията за рутиране.

Всъщност CIDR е стратегия, разработена за решаване на следните проблеми:

- пълноценно използване на адресното пространство при компютърните мрежи от клас B;
- нарастване на таблиците за рутиране.

CIDR елиминира концепцията за адресните класове и дава метод за обобщаване на n различни маршрута в един маршрут. Това съществено намалява количеството информация за рутиране, което BGP рутерите трябва да съхраняват и обменят.

BGP дефинира два типа връзки между АС:

- физическа връзка - АС е подключена към дадена физическа мрежа с друга АС и тази физическа мрежа е свързана поне към един граничен рутер за всяка от АС. Тъй като тези два рутера споделят една и съща физическа мрежа, те могат да си препращат пакети един на друг без да изискват рутиращи протоколи вътре в АС или между АС;
- BGP връзка - BGP връзка означава, че има BGP сесия между двойка BGP говорители, по един във всяка АС. Сесията се използва за съобщаване на

маршрутите през физически свързаните гранични рутери, които могат да се използват за специфични мрежи. BGP изисква съответните говорителите винаги да бъдат в същата мрежа, в която са физически свързаните гранични рутери, така че BGP сесията също не зависи от никакви протоколи за рутиране вътре в АС или между АС. Не е необходимо BGP говорителите да бъдат гранични, и обратно.

Трябва да се отбележи, че терминът BGP връзка може да се използва и за сесия между два BGP говорителя в една и съща АС.

Тип трафик

BGP класифицира трафика в дадена АС като един от следните два типа:

- локален - локален е трафикът, който произлиза от или пристига в тази АС. IP адреса на подателя или на получателя, трябва да бъде в дадената АС;
- транзитен - трафикът, който не е локален.

Една от целите на BGP е да минимизира транзитния трафик.

Тип АС

АС се категоризират в следните три типа:

- ограничена (stub) - тази АС има само една връзка към други АС. Тя носи само локален трафик;
- много насочена (Multihorned) - има връзки до повече от една АС, но отказва да пренася транзитен трафик;
- транзитната (transit) - АС има връзки до повече от една АС и пренася и локален, и транзитен трафик. АС може да налага ограничения за това кой трафик ще бъде пренасян.

Идентификатор на АС - Представлява 16 битово число, уникално идентифициращо АС. Това е същото число, използвано от EGP.

АС път - Списък от номерата на всички АС, през които преминава даден маршрут при обмен на информация за рутиране. Вместо да обменя проста метрика, BGP съобщава целите пътища на своите съседи.

Политиката на рутиране предствлява набор правила, ограничаващи рутирането съгласно желанията на администриращия АС. Политиката на рутиране не е дефинирана в BGP протокола, а се избира от владеещия АС и се предоставя на BGP под формата на

конфигурационни данни. Политиката на рутиране може да се избира от владеещия АС по произволен начин.

Избор на път

Всеки BGP трябва да оцени различни пътища до дадена целева точка от граничния рутер(и) за дадена АС връзка, да избере най-добрия, който отговаря на политиките на рутиране, и след това да съобщи този маршрут на всички свои BGP съседи по тази АС връзка.

BGP е векторен протокол, но за разлика от традиционните векторни протоколи като RIP, при които има единна метрика, BGP определя предпочитан ред прилагайки функция създаваща карта на всеки път със оценка за пътя и избира пътя с най-висока оценка. Използваната функция се генерира при прилагането на BGP и съответства на конфигурационната информация. Все пак, BGP не поддържа метрика от тип "оценка" за отделните пътища, което понякога се мисли за недостатък, но не съществува механизъм, по който от мястото на приложение на BGP да се събере информация и формира оценки за огромното множество налични мрежи.

Тъй като има множество проходими пътища до дадена целева точка, BGP поддържа всичките, но излъчва само този с най-висока оценка (preference value). Този подход дава възможност за бърза промяна към алтернативни пътища, ако основният отпадне.

Политика на рутиране - RFC 1772 съдържа набор препоръки за политиките при всички приложения на BGP.

За повече информация по въпроса за IP протоколи за рутиране може да се намери в следните RFC с номера: RFC 904, RFC 1058, RFC 1245, RFC 1246, RFC 1721, RFC 1722, RFC 1723, RFC 1724, RFC 1771, RFC 1812, RFC 1850, RFC 2080, RFC 2328

Моля, отговорете на контролните въпроси:

1. *Каква е целта на рутирането?*
2. *Каква информация има в една рутираща таблица?*
3. *За какво служи метриката?*
4. *Кой рутиращ протокол се с най-масово използване?*
5. *Каква е целта на автономната система?*

Раздел 7

Безжични мрежи

Ключови думи и съкращения

WiFi	**CDMA, TDMA, ,FDMA**
AP	**ZigBee**
802.11a/b/g/n	**GPS**
Bluetooth	**GPRS**
Ad-hoc	**UMTS**

7.1. История на безжичните мрежи

Безжичните мрежи стават все по-популярни. Те предлагат редица предимства пред традиционните жични технологии, като например: намаляване на разходите за изграждане (отпадат кабелите, конекторите и голяма част от познатите устройства, използвани в локалните мрежи), улесняване на инсталацията на мрежата, увеличено удобство за потребителите и прочее. Присъединяването на нови потребители се свежда до инсталиране на безжична карта (ако няма вградена такава) и включване на машината. Безжичните мрежи са полезно средство за предоставяне на мрежов достъп до места, където липсва традиционна мрежова инфраструктура. Като очевиден пример за популярността на безжичната технология могат да послужат съвременните преносими компютри, в които има интегриран безжичен интерфейс - 802.11b и/или 802.11g.

Безжичните LAN мрежи са базирани на радиовълнова технология, използваща разпределен спектър (spread spectrum). Технологията е била създадена в Англия по време на Втората световна война. За да се преборят с използваното от германците заглушаване на радиосъобщенията, военните специалисти прибягват до радиовръзки с разпределен спектър. При тях едно съобщение се изпраща едновременно по повече канали, които трудно могат да бъдат заглушени едновременно. След 1945 г. някои от цивилните предприятия започват да проявяват интерес към тази технология, осъзнавайки други нейни предимства, полезни за потребителите.

Като предшественик на съвременните безжични LAN мрежи се счита мрежата ALOHAnet, създадена през 1971 г. от Хавайския университет. Мрежата включва седем компютъра, разположени на различни острови, които могат да общуват двупосочно с централен комутатор, намиращ се на остров Оаху. Проучванията на университета

прокарват пътя към създаване на първото поколение оборудване за безжични мрежи, работещо в честотния диапазон 901-928 MHz. Ниската скорост на трансфер и възникналото във връзка с това задръстване на честотната лента ограничава използването на мрежата, предимно за военни цели. По-късно, през 1997 г., IEEE (Institute of Electrical and Electronics Engineers) създава спецификацията 802.11, дефинираща интерфейсите за връзка между безжичен клиент и базова излъчваща станция, както и между два безжични клиента. Съгласно 802.11 носещата честота е 2.4 GHz, максималната скорост на трансфер 2 Mbps, а схемите на модулация са DSSS (Direct Sequence Spread Spectrum) и FHSS (Frequency Hopping Spread Spectrum). Изброените характеристики бяха обявени като основни за безжичните мрежи, предназначени за свободно ползване. Не след дълго се появиха и други спецификации за безжични мрежи, които, заедно с 802.11, образуваха фамилия от спецификации, означавана като 802.11.

Друга организация, освен IEEE, която се занимава с разработване на политики и предписания в развитието на безжичните мрежи е WFA (Wi-Fi Alliance). Разработките на WFA биват утвърждавани като стандарти от IEEE.

7.2 Стандарти за безжични мрежи

IEEE присвои на безжичните технологии за LAN/MAN общия номер 802. Въз основа на него бяха създадени работни групи за разработка на спецификации. Една от тях е спомената по-горе група 802.11, която създаде фамилията от спецификации 802.11. Други работни групи и съответно спецификации са например 802.15 (за мрежата Bluetooth), 802.16 (за поддръжката на широколентовите безжични системи, предназначени за MAN мрежи) и др.

Фамилията 802.11 се състои от група спецификации, всяка една от които е означена със собствена буква след номера 802.11, като например 802.11a.

802.11a. Разполага с 8 канала. Вместо дефинираните в 802.11 схеми за модулация DSSS или FHSS, използващи разпределени спектри, тук се прилага схемата OFDM (Orthogonal Frequency Division Multiplexing). Технологията не получи широко разпространение поради относително високите цени на оборудването и ограничения обхват на действие. По-добра е от популярната 802.11b по отношение трансфера на аудио и видео,

но й отстъпва по обхвата на действие. Не е съвместима с 802.11b. Продуктите, отговарящи на този стандарт, биват отбелязвани с Wi-Fi сертификат (Wi-Fi CERTIFIED).

В таблица 7.1 са дадени най-важните спецификации за безжични LAN:

Табл.7.1

Тип	Максимална скорост	Реална скорост	Брой на каналите	Максимално покритие	Носеща честота
802.11a (Wi-Fi)	54 Mbps	~30 Mbps	8	50 m	5 GHz
802.11b (Wi-Fi)	11 Mbps	~6 Mbps	14	500 m	2.4 GHz
802.11g (Wi-Fi)	54 Mbps	~30 Mbps	14	50 m	2.4 GHz

802.11a. Разполага с 8 канала. Вместо дефинираните в 802.11 схеми за модулация DSSS или FHSS, използващи разпределени спектри, тук се прилага схемата OFDM (Orthogonal Frequency Division Multiplexing). Технологията не получи широко разпространение поради относително високите цени на оборудването и ограничения обхват на действие. По-добра е от популярната 802.11b по отношение трансфера на аудио и видео, но й отстъпва по обхвата на действие. Не е съвместима с 802.11b. Продуктите, отговарящи на този стандарт, биват отбелязвани с Wi-Fi сертификат (Wi-Fi CERTIFIED).

802.11b. Това е най-популярната безжична технология, утвърдена и обявена през 1999 г. като по-нататъшно развитие на стандарта 802.11. Бива означавана още като 802.11 High Rate или като Wi-Fi. Осигурява функционалност, отговаряща на Ethernet. Използва модулация DSSS. При честота 2.4 MHz осигурява максимална скорост 11 Mbps, която при намалена пропускна възможност (fallbacks) спада на 5.5 Mbps, 2 Mbps или 1 Mbps. Обхватът на действие достига до 500 метра. Разполага с 14 канала, от които 3 незастъпващи се. Продуктите, отговарящи на този стандарт, биват отбелязвани с Wi-Fi сертификат (Wi-Fi CERTIFIED).

802.11g. Този стандарт е разработен с цел постигане на по-високи скорости, достигащи 54 Mbps в честотната лента 2.4 GHz . При скорости над 20 Mbps се използва схемата OFDM, а при такива под 20 Mbps схемата DSSS. Разполага с 14 канала, от които 3 незастъпващи се. 802.11g предлага допълнителна сигурност чрез въвеждане на Wi-Fi Protected Access (WPA). Продуктите, отговарящи на този стандарт, биват отбелязвани с Wi-Fi сертификат (Wi-Fi CERTIFIED). 802.11g-устройствата са функционално съвместими

с 802.11b, което позволява 802.11b-устройствата да бъдат заместени директно с 802.11g-устройства. Към настоящия момент устройствата от тип 802.11g получиха широко разпространение, съизмеримо с това на тези от тип 802.11b. Днес преносимите компютри като правило притежават вградена карта за безжична връзка, отговаряща едновременно на стандартите 802.11b и 802.11g.

802.11n. Прокламиран е като стандарт, който се очаква да бъде утвърден от IEEE през септември 2008 г. През октомври 2007 г. WEA (Wi-Fi Alliance) публикува документа 802.11n draft 2.0, който на практика послужи като стандарт за производството на първите 802.11n- устройства. 802.11n разполага с два канала, всеки един от които работи с честота 20 MHz, осигурявайки скорост на трансфер 88.5 Mbps. Съвместно двата канала работят с честота 40MHz, постигайки скорост 146.83 Mbps, което е 5 пъти повече в сравнение със скоростта на 802.11g (около 30 Mbps). Стандартът 802.11n е съвместим с по-старите спецификации 802.11b и 802.11g.

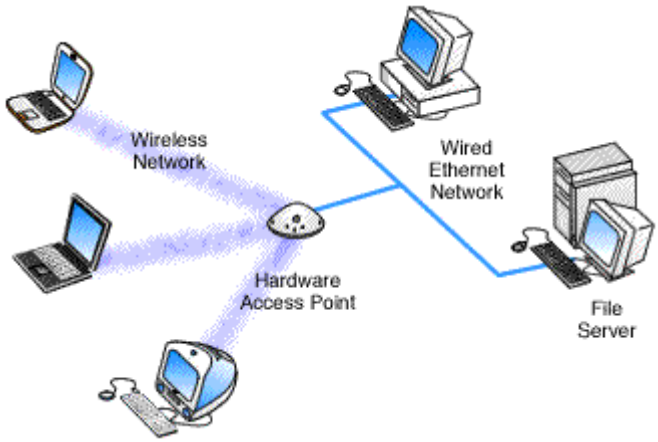
Понастоящем решението за използване на устройства, отговарящи на стандарта 802.11g, изглежда като най-удачно, тъй като върху него е поставен основният акцент от страна на производителите на безжични устройства. Използването на 802.11a е подходящо решение само в случаите, когато мрежата е разположена на място, където се ползват други безжични инфраструктури, използващи 2,4-гигахерцова носеща честота на сигнала.

Безжичните мрежи биват два вида:

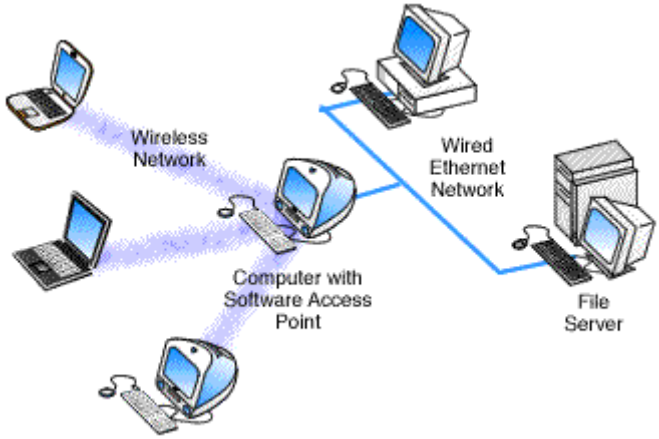
- Мрежи ad-hoc (peer-to-peer). Терминът ad-hoc означава “специален”, а peer-to-peer “равен с равен”. Става дума за специални мрежи, в които компютрите са свързани помежду си като равен с равен.
- Мрежи с използване на точки за достъп (AP – Access Point) до жични LAN.

Ad-hoc мрежите се състоят от компютри, снабдени с интерфейсни карти за безжична комуникация. Картите за безжичен достъп изпълняват същата роля както традиционните мрежови карти за Ethetrnet или Token Ring. Те също притежават свои уникални MAC-адреси, посредством които биват идентифицирани в мрежата. Всеки един от компютрите в ad-hoc мрежата би могъл да комуникира директно с всички останали компютри от същата мрежа (фиг.7.1).

фиг.7.1



фиг.7.2

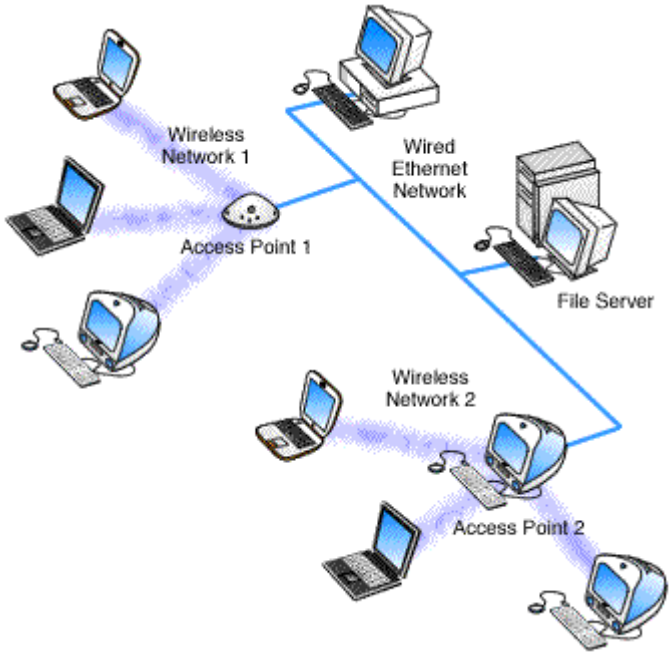


фиг.7.3

За да могат компютрите на една безжичната мрежа да получат достъп до ресурсите на жична LAN, необходима е поне една точка на достъп (AP), през която да се осъществява връзката с LAN. Тази точка може да бъде специализирано хардуерно устройство (HAP -

Hardware Access Point) (фиг.7.2) или компютър, снабден със нужния за целта софтуер (SAP – Software Access Point) (фиг.7.3).

За връзка с жична LAN биха могли да се използват повече на брой точки за достъп, което всъщност представлява свързване на повече безжични мрежи с една жична LAN (фиг.7.4). Посредством повече на брой точки за достъп може да бъде осигурена безжична връзка в отделни помещения (офиси, класни стаи, лаборатории и т.п.) с една базова жична LAN. В други случаи една безжична мрежа би могла да се свърже с повече жични LAN чрез използване на точки на достъп, свързани към всяка една от тези LAN.

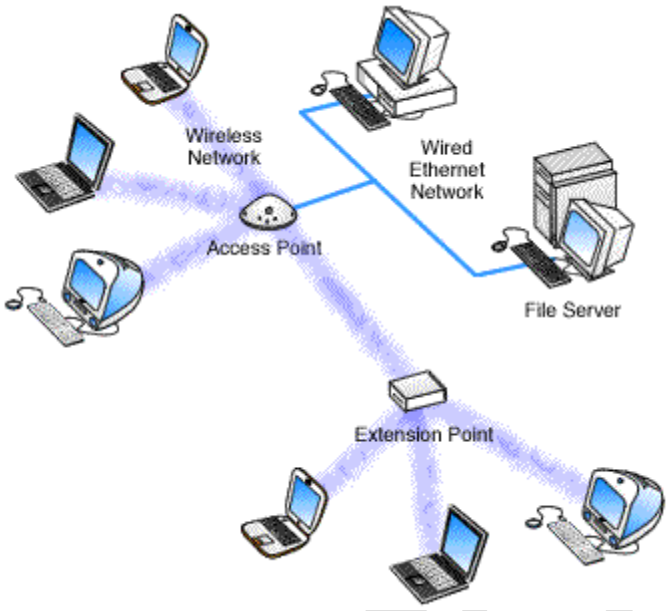


фиг.7.4

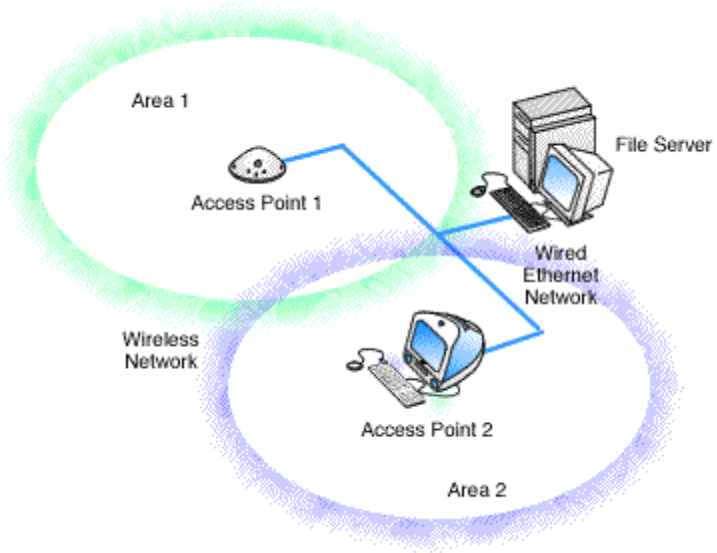
Максималният брой компютри, които могат да бъдат свързани към една точка за достъп, зависи от техническите характеристики на точката. За някои точки този брой е 10, а за други 100.

Обхватът на действие на безжичната комуникация може да бъде увеличаван чрез използване на разширителни точки (Extension Points) (фиг.7.5).

Безжичните мрежи биха могли да изпълняват функция роуминг. Радиовълните на всяка точка за достъп покриват определена област, наричана обхват на действие. Когато биват използвани едновременно повече точки на достъп, възможно е областите им да се припокриват (фиг.7.6).



фиг.7.5

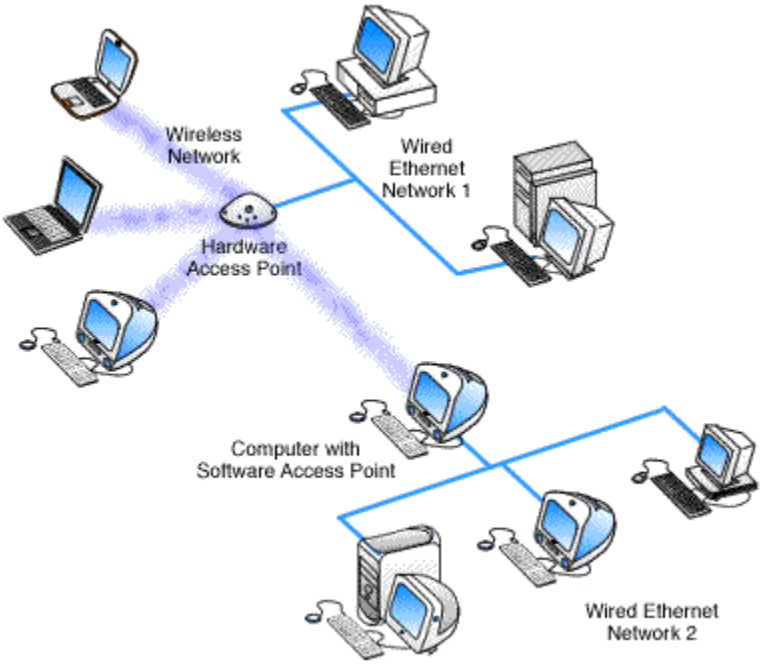


фиг.7.6

Роуминг функцията следи интензивносттана сигналите в припокриващите се области и осъществява връзка с онази точка на достъп, чийто сигнал е по-интензивен. Роумингът протича напълно прозрачно за потребителя. Функцията е особено полезна, когато компютърът е мобилен, например при движение на потребител, снабден с преносим компютър.

Поради липса на стандарт за роуминга, не всички точки на достъп, предлагани на пазара, могат да бъдат конфигурирани да извършват роуминг.

Две жични LAN могат да бъдат свързани помежду си безжично посредством използване на две точки за достъп (фиг.7.7) при условие, че двете точки са в състояние да комуникират помежду си (не всички точки за достъп са в състояние да осъществяват безжична връзка помежду си). Използване на такава връзка се налага, когато липсва физическа възможност за прокарване на кабел, който да свърже двете LAN, например, когато те се намират в две близко разположени сгради, разделени от една или повече улици. Всяка една от точките за достъп трябва да е в състояние да изпълнява за своята жична LAN ролята на безжичен мост (wireless bridge) за връзка с други LAN.

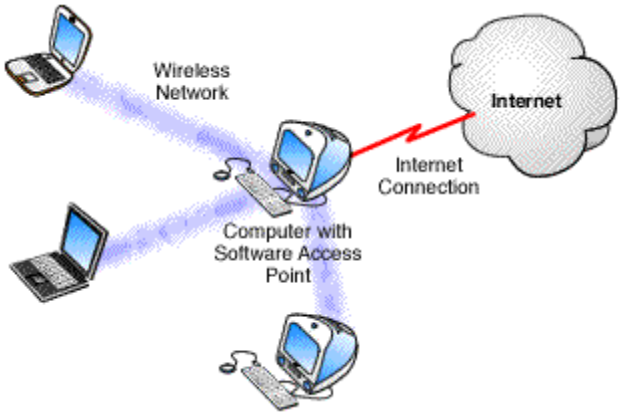


фиг.7.7

На фиг.7.7 една от точките за достъп (в случая двете точки представляват безжични мостове) изпълнява водеща роля - ролята на master, а другата е подчинена на първата, изпълнявайки ролята на slave. Връзката между тях е от типа poin-to-point. Ако взаимосвързаните точки за достъп са повече от две, възниква структурата poin-to multi point. В нея всички точки за достъп са безжични мостове, които комуникират всеки с всеки.

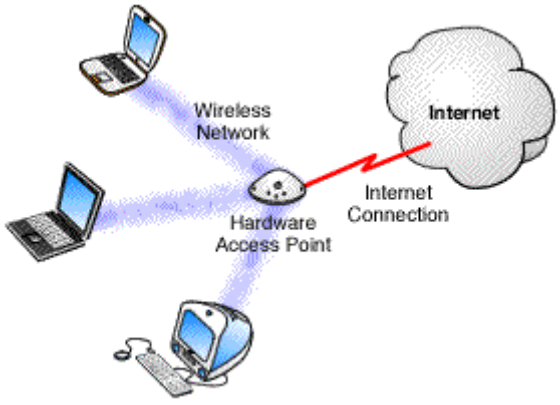
Когато само една от точките е безжичен мост, тя изпълнява ролята на master, а другите точки са slave. Такъв вид структура се нарича master plus APs (Access Points). В случая slave- точките не са в състояние да комуникират директно помежду си.

Съществуват и структури от типа AP to AP, при които всяка точка за достъп може да комуникира с всички останали. Тази структура е най-гъвкава, но цената на такива точки за достъп е висока (няколко стотин долара).



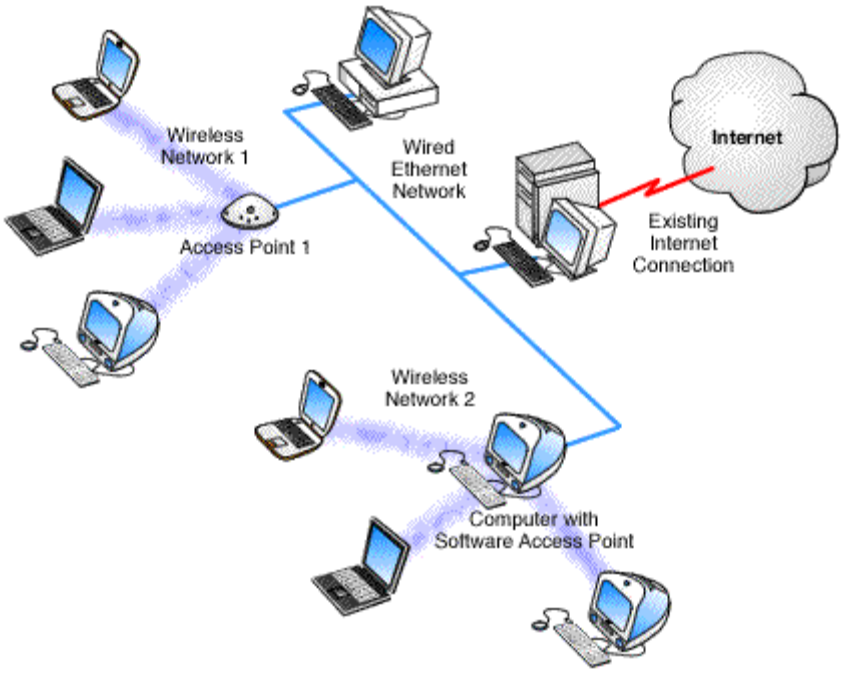
фиг.7.8

Безжичните мрежи биха могли да се свързват и към Интернет. За целта е достатъчно компютърът, към който е свързана точката за достъп, да има връзка с Интернет (фиг.7.8). На пазара се предлагат хардеурни точки за достъп, които могат да осъществяват директна връзка с Интернет (фиг.7.9).



фиг.7.9

Една безжична LAN би могла да осъществява връзка с Интернет посредством жична връзка със софтуерна точка на достъп (фиг.7.10, Wireless Network 2), принадлежаща на безжична мрежа. Друга безжична мрежа може да получи също достъп до Интернет, ако бъде свързана със същата жична LAN по традиционния начин чрез използване например на хардуерна точка за достъп (фиг.7.10, Wireless Network 1).



фиг.7.10

На фиг.7.10 софтуерната точка за достъп изпълнява едновременно три функции – връзка с Интернет, връзка с жична LAN и връзка с втора безжична мрежа. Това не изключва възможността жичната LAN да бъде свързана по традиционния начин с друга безжична мрежа. Последната също ще получи достъп до Интернет, тъй като жичната LAN е вече свързана с Интернет.

Като изхожда от нарастващата популярност на Wi-Fi технологията и на VoIP (Voice over IP), Wi-Fi Alliance разработи новата сертификационна програма Wi-Fi CERTIFIED Voice- Personal за Wi-Fi устройства за безжично предаване на глас у дома или в малки предприятия. Налице са вече първите устройства, получили такава сертификация.

Стандарти за безжични MAN мрежи

Към тях се отнасят стандартите IEEE 802.16 и IEEE 802.16a, означавани с общото име WiMAX. Те използват кодиращата схема OFDM (Orthogonal Frequency Division Multiplexing) и защитите DES3 и AES. Технологията 802.16 използва носеща честота в диапазона от 10 до 66 GHz, а 802.16a в диапазона 2 до 11 GHz.

В Европа е разработен и се ползва още един стандарт - HiperLAN/2, който представлява усъвършенстван вариант на предшественика си HiperLAN/1. Осигурява възможност за работа с ATM-клетки и IP-пакети, както и предаване на глас за клетъчни

телефони. Използваната носеща честота е 5 GHz, а скоростта на трансфер 54 Mbps. Кодиращата схема е OFDM (Orthogonal Frequency Division Multiplexing). Предвидени са средства за защита на информацията, включително възможност за лична автентикация.

Стандартът Bluetooth

Технологията Bluetooth се използва за безжични мрежи, в които биха могли да участват не само компютри, но и други устройства от типа на мобилни телефони, апарати от домашния интериор и др. Bluetooth се подържа от консорциум със свободно безплатно членство, основан през 1998 г, в който членуват над 2000 компании, между които IBM, Intel, Nokia, Erricson, Toshiba, 3COM, Lucent, Microsoft. Първата официална версия 1.1 на стандарта бе публикувана на 1 декември 2000 г.

Bluetooth работи в честотния диапазон 2400 – 2483.5 MHz, осигурявайки скорост на предаване, достигаща максимум до 2 Mbps. За устройствата, работещи в синхронен режим, типичната скорост е 723,2 Kbps, а за тези, които използват асинхронен режим тя е 433,9

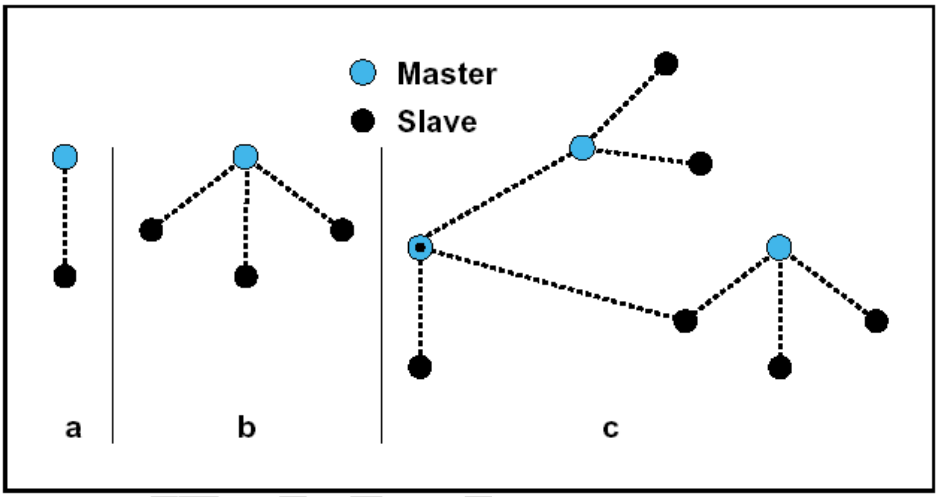
Kbps. Обхватът на действие е около 10 метра. Схемата на модулация е FHSS. Като средства за защита могат да бъдат използвани протоколите: PPTP, SSL или VPN. Bluetooth не подържа TCP/IP.

Bluetooth-устройството представлява приемо/предавател, изпълнен като отделен модул или интегриран в някакво друго устройство. За управление на същия се използва драйверна програма. Според спецификацията приемо/предавателят трябва да работи в честотния диапазон 2400 – 2483.5 MHz, който е свободен за използване в повечето държави и не изисква лицензиране. Съществуват обаче държави като Франция и Испания, в които част от този диапазон се използва за други цели, поради което там диапазонът е стеснен до 2445-2475 MHz (Испания), 2446,5-2483,5 (Франция).

Bluetooth притежава свойство, отличващо го от останалите технологи - Bluetooth устройствата влизат в контакт едно с друго автоматично, веднага след като попаднат в обсега на приемо/предавателя. За установяването на връзката, за автентификацията и др. се грижи програмното осигуряване.

Според терминологията на Bluetooth, устройството, което изпълнява водещата роля в комуникацията с други устройства, се нарича master, а подчиненото устройство, с което master-ът комуникира се нарича **slave**. Максималният брой на активните **slave**-устройства

може да бъде 7 (multislave-операция, фиг.7.11b). В обсега на master-а би могло да има и неактивни slave-устройства. Те установяват връзка с master-а (синхронизират се с него), но не обменят данни, докато не се създадат условия за осъществяване на пренос на данни. Броят на неактивните **slave**-устройства би могъл да бъде неограничен. Такъв тип връзка между устройства бива наричан piconet (фиг.7.11a). В рамките на една ***piconet*** връзка може да съществува само едно master-устройство. Когато едно slave-устройство ев състояние да променя статуса си в master и обратно, възниква друг тип структура, нарича scatternet (фиг.7.11c). **Scatternet** мрежата може динамично да променя структурата си в зависимост от текущите нужди на комуникацията.



фиг.7.11

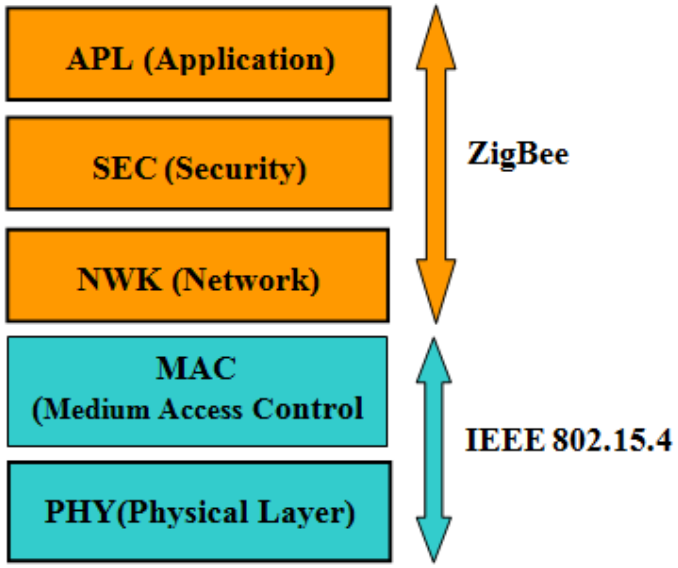
За да се избегне дублиране на устройствата, както и на появата на други нежелателни явления, всяко едно от устройствата, освен че притежава уникално име, взаимодейства с другите устройства, като използва втори канал за връзка (**hopping channel**), работещ с периодична промяна на честотата, определяна посредством параметър, наричан ***hopping***, който бива различен за различните устройства.

Bluetooth постепенно набира инерция. Големи производители на дънни платки като MSI и EpoX предлагат продукти с вграден интерфейс Bluetooth. Много модели GSM апарати, PDA и преносими компютри също притежават Bluetooth. Рано е още да се говори, че Bluetooth се е наложил окончателно. Както често се случва, появяват се нови по-прогресивни технологии, които изместват старите. Такава е например обещаващата технология ***ZigBee***.

Стандартът ZigBee

През 2002 г. се заговори за пореден стандарт за цифрова радиовръзка, наричан ZigBee. Днес зад него стои консорциумът ZigBee Alliance, включващ около 230 компании, между които гиганти като Samsung, Philips, Mitsubishi u Motorola. Първите произведени ZigBee- устройства се появиха през 2005 г. Названието ZigBee произлиза от зигзогобразния (zigzag) танц на пчелите (Bee-пчела), посредством който те предават помежду си информация относно местонахождението (посока и разстояние) на източниците на храна.

По същество ZigBee е комплект от протоколи (фиг.7.12), допълващи международния стандарт IEEE 802.15.4. Спецификацията IEEE 802.15.4 дефинира на какви честоти и кога трябва да се излъчва сигналът, а зад ZigBee се крият протоколите, осигуряващи логическата комуникация, която гарантира съвместимостта на устройствата, произвеждани от различни фирми.



фиг.7.12

Съвсем логично възниква въпросът - за какво ни е нужен още един вид безжична мрежа? Не може ли Bluetooth и Wi-Fi, макар и различаващи се, да задоволят всички безжични нужди? Оказва се, че не. Идеята за IEEE 802.15.4 се заражда в началото на 90-те години, когато конструкторските отдели с интерес проучват токущо публикуваните спецификации на Bluetooth и Wi-Fi и откриват, че тези стандарти са твърде енергоемки, за да бъдат използвани за маломощни устройства. Недоволството от това се оказало

достатъчно, за да стимулира създаването на нов стандарт, номериран по-късно като 802.15.4. През лятото на 2003 г. по инициатива на Philips е образувано сдружението ZigBee Alliance със задачата да осигури съвместимост между различните Bluetooth и Wi-Fi устройства, както и да ограничи в по- тесни рамки обхвата на стандарта IEEE 802.15.4. На 13 юни 2004 г. бе публикувана първата спецификация ZigBee 2004, а през септември 2006 г. спецификацията ZigBee 2006. В края на 2007 г. бе публикуван окончатилният документ ZigBee PRO.

Основният коз на ZigBee е икономичността по отношение на консумацията на електрическа енергия. Енергията на една стандартна батерийка тип AA е достатъчна за радиоизлъчване в продължение на повече от една година. Определението гласи, че IEEE 802.15.4. е стандарт за нискоскоростни частни мрежи – Low Rate Wireless Personal Area Network (LR-WPAN). Той има на разположение 27 радиоканала в три честотни диапазона - 16 канала в общоприетия в цял свят 2,4 GHz диапазон, един допълнителен диапазон на 915MHz в САЩ (10 канала) и още един на 868 MHz в Европа (един канал). Скоростта на предаване на данните зависи от броя на свободните канали и варира между 20 и 256 Kbps. Разпределението на каналите става по принципа на контрола на носещата (CSMA; Carrier Sense, Multiple Access) – устройството "слуша" ефира и започва предаване, само когато той се освободи.

Протоколите на ZigBee са разработени с цел максимално пестене на енергия. Те позволяват на устройството да прекарва преобладаващата част от време в пасивен режим без да излъчва радиовълни. От време на време, за части от секундата, то включва приемника си, за да провери дали някой не се обръща към него. Продължителността на "зимния сън" между две такива включвания може да бъде минути даже и часове. Но това не означава, че стандартът е подходящ само за "бавни" връзки. Той позволява създаване на устройства, чувствителни към закъсненията на данните, като например безжични клавиатури, джойстикове и др.

Конструкторите твърдят, че от алгоритмична гледна точка схемата на ZigBee е десетки пъти по проста от Bluetooth, а цената на хардуера не би трябвало да превишава няколко долара.

Когато в една радиомрежа има повече ZigBee устройства, те могат да работят както в топология звезда (един маршрутизатор управлява всички потоци от данни), така и

като еднорангова мрежа без координатор. При това ZigBee мрежите могат да се "саморемонтират", ако някой от участниците излезе от строя. Адресацията позволява в една мрежа да се свържат до 65000 устройства – възможност, която наистина може да е полезна за големите корпорации.

Техническите данни на ZigBee са следните:

Честотни диапазони: за Европа 868.3 MHz и 2.46 GHz
за САЩ 915.0 MHz и 2.46 GHz
Излъчвана мощност: при 915 MHz/2,46 GHz: средно 0.5 mW до 10 mW
при 868 MHz: максимално 25 mW (13.9 dBm)

- Обхват на действие: до 100 метра
- Скорост на трансфер: 20 Kbps при 868/915 MHz и 250 Kbps при 2.4GHz
- Метод на комуникация: CSMA (Carrier Sense, Multiple Access)

В таблица 7.2, в която са показани сравнителните характеристики на стандартите ZigBee, Bluetooth и Wi-Fi.

Табл.7.2

	ZigBee 802.15.4	**Bluetooth 802.15.1**	**WiFi 802.11b**
Основно предназначение	Контрол и наблюдение	Замества кабелите	Интернет, данни, видео и аудио
Продължителност на работа с батерия [дни]	100-1000 и повече	1-7	0,1 – 5
Брой устройства в една мрежа	255 – 65000 и повече	7	30
Скорост на данните [Kbps]	20 – 250	72	11000 и повече
Далечина на връзката [метри]	1 -75 и повече	1 – 10 и повече	100 и повече
Други особености	Висока надеждност, ниска консумация, ниска цена	Ниска цена и удобство	Скорост и гъвкавост

Интерес представлява фактът, че при ZigBee данните могат да се предават щафетно от устройство на устройство. Заедно със способностите за самонастройка това чувствително опростява разгръщането на мрежи върху голяма площ.

В ZigBee мрежите се използват три типа устройства:

- ZigBee End Device (ZED). Опростено крайно устройство, което реализира само част от протоколите на ZigBee, поради което бива наричано още RFD (Reduced Function Device). То осъществява връзка с маршрутизатор (рутер), където бива регистрирано. Рутерът заедно с повече крайни устройства, образува безжична мрежа тип звезда.

- ZigBee Router (ZR). Това е маршрутизатор, който изпълнява всички протоколи на ZigBee. Нарича се още FFD (Full Function Device). В състояние е да се регистрира в друг по-висшестоящ рутер от същия тип. Повече такива рутери образуват йерархична дървообразна структура.
- ZigBee Coordinator (ZC). Това е специален рутер, наричан координатор. Към функциите си на рутер той изпълнява допълнително и функциите на координатор на мрежата. В една ZigBee мрежа може да присъства само един единствен координатор. От него започва изграждането на мрежата. Той задава основните параметри на мрежата и я управлява. Способен е да помни информация за структурата на мрежата и, когато е необходимо, да изпълнява ролята на мост към други мрежи.

Устройствата, отговарящи на стандартите ZigBee 2006 и ZigBee 2007, са напълно съвместими. Устройствата от стандарта ZigBee PRO се различават от тях. Устройства от типа ZigBee 2006 и ZigBee 2007 биха могли да участват в мрежа от тип ZigBee PRO, но обратното не е възможно.

Адресирането на устройствата може да се извършва по два начина – директно и индиректно.

При директното адресиране всеки рутер и крайно устройство взаимно се осведомяват за своето присъствие. Един рутер може да обслужва повече крайни устройства, така както например един компютър в Интернет би могъл да обслужва повече TCP-връзки на различни свои портове. Всеки рутер предоставя възможност за връзка с 255 крайни устройства. Част от адресите (от 241 до 254) са резервирани за специални задачи, а адресът 255 е предназначен за броудкастни предавания (за едновременно комуникация с всички крайни устройства). Адресът 0 служи за целите на управлението на мрежата.

При индиректното адресиране координаторът „раздава" така наречените кратки адреси с дължина 16 бита (MAC-адреси). Когато даден рутер се включва за първи път в мрежата, той се обажда на координатора на същата и получава от него кратък адрес. Координаторът съхранява всички кратки адреси в своя таблица. Щом даден рутер реши да се свърже с друг такъв, той заявява това на координаторът, а той от своя страна препредава заявката на възела приемник. Този начин на свързване се нарича binding. Промените в мрежата се отразяват автоматично в binding-таблицата, съхранявана в паметта на

координатора. По този начин управлението на мрежата става гъвкаво, а включването/изключването на устройства в/от мрежата се опростява значително.

Тъй като в една ZigBee мрежа по принцип може да си използва само един координатор, отпадането на същия, например поради повреда, води до разпадане на цялата мрежа. Това представлява недостатък на ZigBee. Все пак рутерите позволяват така да бъдат конфигурирани, че да могат да поемат в известна степен задачите на координатора.

Сферата на приложение на ZigBee е много широка. Например ZigBee може да се вгражда в домашните уреди за отчитане на тока, водата и топлинната енергия. Със ZigBee няма да се налага инкасаторът да влиза в дома ви. Друга подходяща област са разнообразните системи за сигнализация и охрана – датчиците няма да се свързват с кабели, а просто ще се залепват със скоч за стената и веднъж годишно ще трябва да им се подменя батерийката. Най-общо ZigBee мрежите могат да намират приложение в следните области:

- в индустрията, в устройствата предназначени за контрол и управление на технологични процеси;
- в медицинската техника за предаване на данни за пациентите;
- в битовата електроника, компютърната периферия и устройствата за сигнализация.

Вече се появи и първият мобилен телефон с подддръжка на ZigBee – корейският производител на Pantech-Curitel го рекламира като "телефонът, способен да управлява вашата битова техника". Когато се появи и въпросната битова техника, ZigBee мрежите ще бъдат реалност.

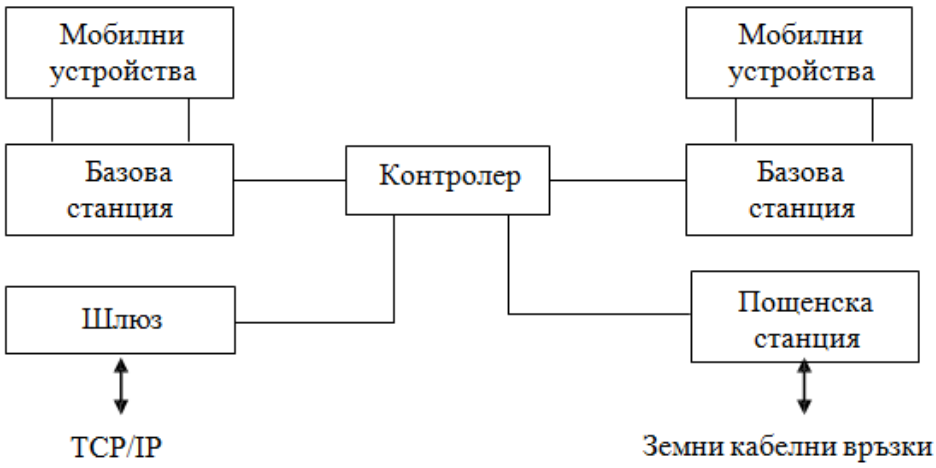
С цел тази мрежа да не бъде лесно уязвиматя поддържа 128-битово AES криптиране на данните.

Клетъчни мрежи

Преносът на компресирани цифрови данни по безжичен път посредством клетъчни технологии прави през последните години бум в областта на телекомуникациите. Постоянно увеличаващият се брой на потребителите и нарастващите изисквания за по-високо качество и разнообразие на този вид услуги тласкат развитието напред, като непрекъснато поставят все по-нови и все по-сериозни предизвикателства пред операторите на мобилни услуги и пред производителите на телекомуникационна апаратура.

За разлика от радиопредавателните мрежи, при които една единствена базова станция обслужва сравнително голям географски район, клетъчните мрежи се състоят от малък брой тясно интегрирани, компютърно управляеми клетки, всяка една от които покрива малък район с радиус от 500 м до няколко километра, например район обхващащ няколко големи жилищни блока. Областите от земната повърхност биват разделяни на клетки, оприличавани по форма със шестоъгълници. Общата структура на мрежата наподобява пчелна пита.

Клетъчната мрежа е изградена от повече компоненти (фиг.7.13).



фиг.7.13

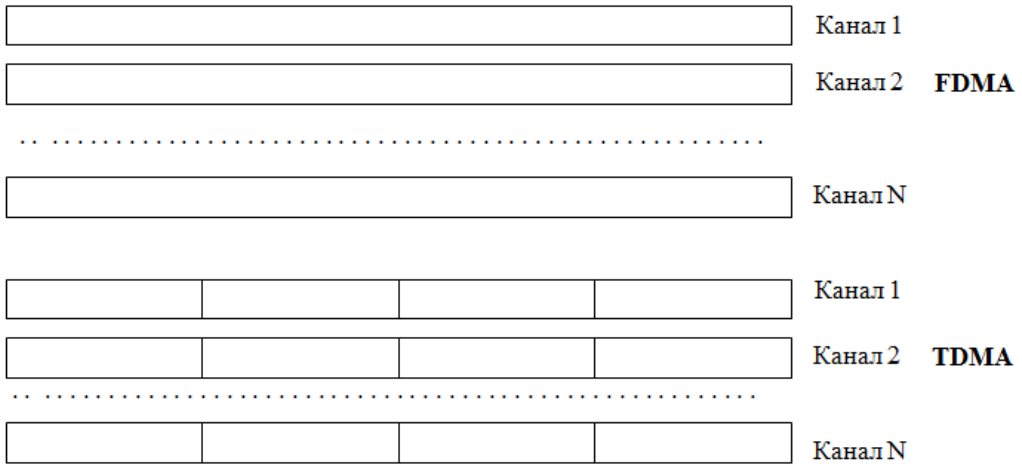
Базовата станция (cell tower) представлява приемо/предавател, чрез който абонатите (мобилните устройства) се включват към мрежата. Една такава станция обслужва една клетка. Няколко базови станции се свързват към контролер (MSC – Mobile Switching Center), който ги управлява. Той се грижи за прехвърляне на абоната от една клетка към друга, когато последният се движи. Контролерът следи непрекъснато за състоянието на трафика и управлява действието на своите клетки.

Контролерите от своя страна са свързани към устройства, наричани шлюзове (Gateways), осъществяващи връзка на клетъчната мрежа с Internet посредством TCP/IP протокол и към конвенционалните пощенски станции.

Към мобилните устройства (mobile embedded devices), които използват клетъчни технологии за комуникация, могат за бъдат отнесени: мобилните телефони, пейджърите, PDA, персоналните органайзери и др. Клетъчните технологии намират приложение и в изграждането на безжични LAN мрежи.

Идеята за радиосистема, базирана на клетъчна технология, възниква за първи път през 70- те години в лабораториите на Bell (САЩ), но не намира практическа реализация. Първата реална система за безжична комуникация бива създадена в Чикаго (САЩ) през 1980 г. от AT&T. Известна е под названието AMPS (Advanced Mobile Phone Service). Отначало тя е работила на честота 800 MHz, но по-късно преминава на 1900 MHz, на честотата на която днес работят повечето безжични оператори в САЩ. Тя бе аналогова система, предназначена единствено за предаване на глас. AMPS не бе в състояние да пренася цифрови данни. Тя беше изместена от по-прогресивните безжични технологии TDMA (Time Division Multiple Access) и CDMA (Code Division Multiple Access).

AMPS бе от тип FDMA (Frequency Division Multiple Access). Тук честотната лента бива разбивана на повече по-тесни ленти (канали), ползвани поотделно едновременно от повече потребители. При TDMA всеки един от тези канали бива разбиван на повече времеви слотове така, че повече потребители да могат да ползват едновременно един и същ канал (фиг.7.14). За отделните канали действието на TDMA е подобно на работата на компютърните системи с разделение на времето (time-sharing).



фиг.7.14

Първите клетъчни радиосистеми за мобилни телефони, наричани системи от първо поколение, са били аналогови. Те се създават в началото на 80-те години в САЩ, Канада, Япония, скандинавските страни, Великобритания, Франция и Германия. Отначало всяка една от тези страни развива собствена технология и създава свой стандарт за клетъчна радиосистема, в повечето случаи несъвместим с тези на другите страни. Така например в САЩ започват да оперират системите AMPS, ARTS и NAMPS, във Великобритания –

TACS и NTACS, в Канада – AURORA, в скандинавските страни – NMT, в Германия – NETWORK C-450, във Франция – RADIOCOM и в Япония – NTT и NAMTS. Много скоро тази тенденция довежда до възникване на съществен проблем – поради голямото разнообразие апаратурата, предназначена за изграждане на клетъчни мрежи, пазарът за същата се оказва силно стеснен. За преодоляване на проблема Конференцията на европейските пощи и телекомуникации (CEPT – Conference Europeene des Postes et Telecommunucation) създава през 1982 г. организацията Groupe Special Mobile (GSM), на която възлага да разработи общоевропейски модел за клетъчна радиосистема. Широко разпространеното днес съкращение GSM се появява по-късно и означава Global System for Mobile communications. През 1989 г. отговорността за изготвяне на спецификациите на GSM-системата бива прехвърлена от CEPT на Европейския институт за телекомуникационни стандарти (ETSI – European Telecommunucation Standart Institute). Целта на спецификациите бе да бъде стандартизиран всеки един от компонентите на системата и като цяло да се гарантира нейната работоспособност. Първата GSM-мрежа в Европа започва работа през 1991 г. По- късно различни версии на GSM бяха реализирани в Азия и Северна Америка.

Цифровите клетъчните системи спадат към второто поколение безжични телефонни системи. За разлика от аналоговите системи, които предлагат ограничен набор услуги и предават данните със скромните 1200 bps, системите от второ поколение позволяват:

- роуминг на абонатите в международен мащаб (възможност на потребителите да използват мобилните си телефони извън своята страна или пък да комуникират с потребители от други страни);
- предаване на реч с високо качество;
- предаване на: факс, данни и къси съобщения (SMS);
- защитеност срещу неразрешен достъп;
- възможност за засекретяване на информацията;
- идентификация на абонатите и определяне на местоположението им;
- намалени размери на мобилния апарат;
- намалена излъчвана мощност.

Към настоящия момент в света съществуват две основни клетъчни технологии от второто поколение – TDMA (Time Division Multiple Access) и CDMA (Code Division Multiple Access).

В САЩ появата на системите от второ поколение започва с пускането в действие на две системи. Първата от тях използва технологията TDMA и е базирана на стандарта IS-54/136. Втората използва CDMA-технологията. Разработката на CDMA започва в края на 80-те години от фирмата QUALCOMM и завършва през 1993 г. с публикуване на стандарта IS-95. Първата система, използваща CDMA, бива създадена през септември 1995 г. от фирмата Hutchison Telecom Of Hong Kong.

TDMA-технология за комуникация

TDMA (Time Division Multiple Access – многократен достъп с времеделение) е технология, която позволява даден брой абонати да имат достъп до една и съща радиочестота (фиг.7.14). Преносът на данни се осъществява в клетъчен канал за връзка, като всеки един от абонатите заема цялата честотна лента, но само за кратък интервал от време, наричан времеви слот. Общият пренос протича чрез разпределението му във времеви слотове.

TDMA е първата цифрова телефонна технология в САЩ. На нейна база първо е бил създаден стандартът IS-54 (Interim Standart - 54), който по-късно прераства в IS-136. Последният е бил приет през 1992 г. от TIA (Телекомуникационна индустриална асоциация). През 1993 г. бива пусната в действие първата TDMA-мрежа. TDMA се използва в широко използваните американски системи PDC (Personal Digital Cellular) и D-AMPS (Digital- Amerikan Mobile Phone Sevice).

CDMA-технология за комуникация

CDMA (Code Division Multiple Access – многократен достъп с кодово деление) е технология, при която се използва разпределен спектър (spread spectrum) и уплътняване/разделяне на каналите по код. Тя представлява технология на третото поколение (3G – Third Generation) клетъчни мрежи. Тя осигурява по-висока скорост на трансфер на данни от TDMA, която достига до 115 Kbps. Вместо честотната лента да бъде разбивана на по-тесни такива, CDMA позволява на повече потребители да

ползват колективно една и съща честота. Тайната на CDMA се крие в пакетите. Сигналите, излъчвани от отделните абонати, се разбиват и обособяват в пакети, като всеки пакет бива снабдяван със свой уникален кодиран номер. В приемната страна, на базата на номерата на пакетите, се извършва разпознаване и реконструиране на сигналите. Процесът наподобява използването на TCP/IP-пакетите в Internet, но е по-сложен.

Технологията се характеризира с висок капацитет и малък обхват на клетката. На базата на CDMA Телекомуникационната индустриална асоциация (TIA) на САЩ приема през 1993 г. стандарта IS-95. CDMA работи на честоти 800 MHz и 1.9 GHz. Днес съществуват многобройни варианти на CDMA. По-известните от тях са:

- CDMAOne. Това е първата тяснолентова технология, която все още продължава да бъде основна за клетъчните телефони в САЩ. Скоростта на предаване е 14.4 Kbit/s във вариант с един канал и 115 Kbit/s при осем канала.
- CDMA2000. Това е второто поколение на CDMA, при което е увеличена скоростта на предаване.
- WCDMA (Wideband CDMA). Технологията е стандарт на ITU (International Telecommunrcation Union), известен под името „IMT-2000 direct spread". Осъществява широкочестотен пренос на данни, който позволява постигане на висока скорост на предаване. WCDMA е технология, подходяща за аудио и видео комуникация. Тя е технология, използвана в днешните UMTS-мрежи от трето поколение.
- HSDPA (High Speed Downlink Packet Access). Това е технология, базирана върху принципите на WCDMA, която осигурява висока скорост на предаване - скорост на низходящия поток, достигаща до 8-10 Mbps, която в системите от тип MIMO (Multiple-Input and Multiple-Output) достига до 20 Mbps. HSDPA се използва като надстройка в съвременните UMTS системи.

GSM системи

GSM е цифрова безжична телефонна технология за пренос на компресирани данни, базирана на принципите на TDMA. Преносът се извършва по така наречените GSM-канали. Всеки GSM-канал предава на всеки 4.6 милисекунди по 8 малки пакета от по 114 бита. Абонатите от канала използват една и съща честота. Те се редуват да предават по един

кадър (пакет) през 4.6 милисекунди. За една секунда общата производителност на GSM-канала е 22.8 Kbps. Стандартно данните на потребителите се предават със скорост 9.6 Kbps, като останалите 13.2 Kbps се използват за осигуряване на стабилност на връзката. В резултат от усъвършенстване на технологията днес данните на потребителите се предават със скорост 14.4 Kbps, като за осигуряване на стабилност остават 8.4 Kbps.

Различните GSM-мрежи работят на различни честоти - 450, 900, 1800 или 1900 MHz. (По принцип радиовълните оперират в диапазона от 3 kHz до 300 GHz и имат дължина между 3 см и 300 метра. Радиотелевизионните и сателитни предавания използват радиочестотите както следва: 1 MHz за AM-радио, 100 MHz за FM-радио и 1.5 GHz за сателитните GPS (Global Positioning Satellite) системи).

Стандартът PCN/DCS представлява версия на GSM за работа в обхвата 1800 MHz и е известен още като GSM 1800. Първата GSM 1800 мрежа бе изградена във Великобритания. В Северна Америка се използва GSM-стандарт в обхвата 1900 MHz, известен под името PCS1900. Американските и европейските GSM-стандарти, както и съответстващите им клетъчни GSM-телефони, са несъвместими. Американските работят на честоти 800 MHz и 1900 MHz и не могат да бъдат използвани в Европа, а европейските работят на 900 MHz и 1800 MHz и са неизползваеми в Америка.

GSM-стандартът е отворен за промени и усъвършенстване. Без особени затруднения бяха реализирани усъвършенстванията GPRS (General Packet Radio Services) и EDGE, които представляват стъпки към системите от трето поколение. Някои от системите за сателитни телефони като: IRIDIUM, ICO и AceS използват стандарт близък до GSM, което дава възможност за съвместно им използване с GPRS.

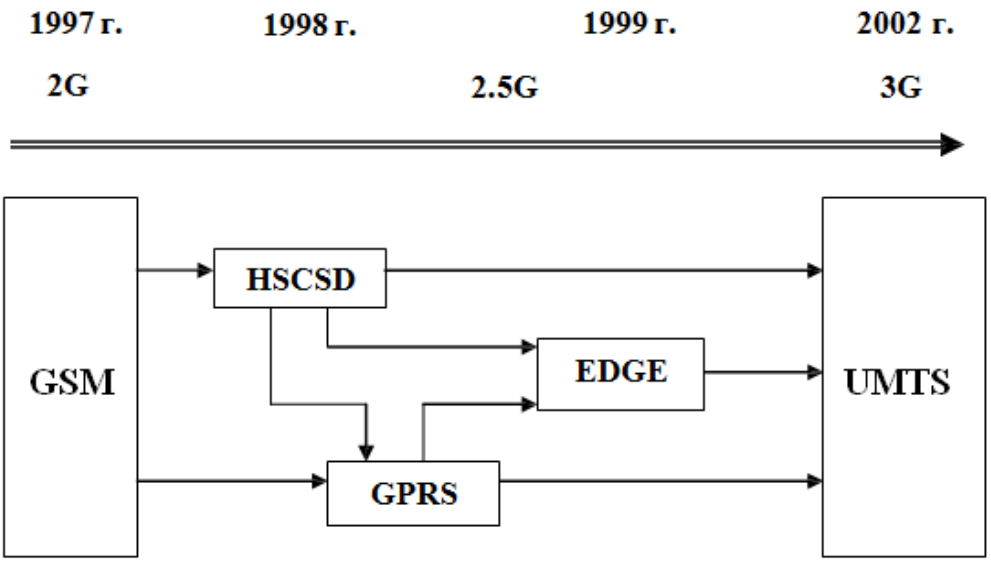
GSM-технологията стъпва в България през 1994 г., когато фирмата “Мобилтел” получава лиценз за изграждане и опериране на телекомуникационна мрежа по стандарта GSM. През 2000 г. бе даден лиценз за втори GSM-оператор на фирмата “Globul”. След приватизацията на БТК се появи трети GSM-оператор - Vivatel. Наличието на три GSM-оператора създаде условия за конкуренция между тях която несъмнено води до поевтиняване на комуникационните услуги и до тяхното разнообразяване и качествено подобряване.

Развитие на GSM-технологията в посока към третото поколение системи

С течение на времето се появиха някои нови технологии, които промениха безжичния свят. Към тях могат да бъдат отнесени:

- PCS (Personal Communications Service). Тя представлява комбинация от TDMA, CDMA и GSM. Работи на 1900 MHz.
- GPRS (General Packed Radio Service. Представлява надстройка над GSM.
- i-mode. Това е японска безжична телефонна мрежа, осигуряваща достъп до cHTML(compact HTML)-Web-сайтове и позволяваща възпроизвеждане на анимационни GIF-файлове и на други мултимедийни съдържания. Въведена е от NTT DoCoMo през 1999 г.
- UMTS (Universal Mobile Telecommunication System). Стандартът за тази технология, известен като IMT-2000, бе създаден от международните организации ITU (International Telecommunication Union) и IMT-2000 (International Mobile Telecommunications - 2000). UMTS гарантира производителност до 2 Mbps.

На фиг.7.15 е показано развитието на GSM по години. Означенията 2G, 2.5G и 3G означават съответно системи от второ, междинно и трето поколение (G - Generation). Технологията на третото поколение безжични клетъчни системи е UMTS (Universal Mobile Telecommunication System).



фиг.7.15

При технологията HSCSD (High Speed Circuit Switched Data) няколко GSM-канала биват обединявани механично в един общ канал с по-голяма пропускателна способност. За сега е възможно обединяване до три канала от по 14.4 Kbps, което при три канала прави общо 43.2Kbps. Технологията не можа да получи разпространение поради появата на GPRS.

GPRS (General Packet Radio Service) е най-значимото подобрение на GSM. Услугата се предлага и в България. GPRS е протокол, специално оптимизиран за пренос на данни. Подобен е на IP-протокола, при който данните се разбиват на пакети. Скоростта на предаване е в диапазона между стандартната за GSM скорост 9.6 Kbps и 115.5 Kbps. Характерна за GPRS е функцията "always-on", при която абонатите са постоянно свързани към мрежата. Това улеснява трансфера на пакетите и отпада нуждата от постоянно подсигуряване на връзката. Абонатите заплащат за пренос на количество информация, а не за престой в мрежата.

При GPRS 8 потребители поделят помежду си временни интервали. Когато дадени интервали се окажат свободни, те биват автоматично заемани от някой от останалите 8 потребителя. Един потребител би могъл да заеме всичките 8 интервала, ако в даден момент те са свободни. При това максималната скорост може да достигне до 8 x 14.4 = 115.5 Kbps. Два от интервалите са предназначени само за предаване, а 4 други само за приемане на данни.

GPRS-технологията позволява да се провежда едновременно телефонен разговор и да се пренасят данни, например да се получава електронна поща по телефона. Основното предимство на GPRS е възможността за осигуряване на достъп през мобилния апарат до компютърни приложения, с който сме свикнали да работим на персоналния компютър – чат, браузване, изпращане и приемане на данни, писане и изпращане на поща, трансфер на аудио- и видеоинформация и др. Това са приложения, които постепенно ще напуснат бюрото и чрез мобилните апарати ще станат достъпни навсякъде. GPRS предлага и няколко иновационни услуги. Например служителите на фирма биха могли да ползват локалната мрежа на фирмата, когато са извън фирмата. Друга такава услуга е наблюдението за дома от разстояние. Ако, докато сме на почивка, някой изключи алармата на дома, можем да бъдем веднага известени чрез мобилния си апарат, като съществува възможност и за получаване на образ от дома.

EDGE (Enhanced Data GSM Environment) е технология, която позволява постигане на скорости от 384 Kbps. Това е GPRS-технология, в която се ползва нов метод за модулация. Стандартът е базиран върху GSM и използва мултиплексиращата TDMA технология.

UMTS системи

UMTS (Universal Mobile Telecommunication System) са системи от трето поколение (3G). Стандартът UMTS е известен още като IMT-2000. Той бе създаден от международните организации ITU (International Telecommunication Union) и IMT-2000 (International Mobile Telecommunications - 2000). UMTS притежава производителност, достигаща до 2 Mbps. Тя използва технологията TMDA. Освен глас и кратки съобщения UMTS е предназначена да предава аудио и видео информация навсякъде по света по фиксирани, безжични и сателитни системи.

Високата скорост от 2 Mbps не може да бъде постигана навсякъде. Смущаващите отражения от стените на жилищата, налагат повторно изпращане на данновите пакети, което сваля драстично производителността. Това е наложило областта на приемане да бъде разделена на 5-те клетки, показани в таблица 7.3:

Табл.7.3

2		384 Kbps		144 Kbps
Домашна клетка	Pico-клетка	Micro-клетка	Macro-клетка	Глобална клетка
Жилище	Около жилището	Град	Градска област	

У дома и в pico-клетките (около жилищата) се гарантира скорост от 2 Mbps, тъй като там приложението на UMTS е стационарно. Micro- и macro-клетките са предназначени за градовете и околностите им. Тук се гарантират 384 Kbps, тъй като се счита, че потребителите са подвижни. Глобалната клетка обслужва бързо придвижващите се потребители, като в определени области те се обслужват и от сателити. Гарантираната скорост е 144 Kbps. Посочените по-горе стойности са минимални. При добро стечение на обстоятелствата скоростите могат да се окажат по-високи.

Вътрешно UMTS използва две мрежи:

- Мрежа-ядро. Данновите пакети се предават жично по оптични кабели. През възлови точки тази мрежа прави връзка с други типове мрежи, като например телефонната мрежа ISDN.
- UTRAN (UMTS Terrestrial Radio Access Network). Това е безжичната радиомрежа, която осигурява обмена на данни с мобилните UMTS-апарати.

UMTS означава: бърз достъп до Internet, мултимедия, видеоконференции и даже телевизия върху мобилните апарати. Новите услуги поставят все по-високи изисквания към скоростта на пренос. Най-високи са изискванията на видеото. Например видеостандартът MPEG изисква следните скорости на трансфер, отразени в таблица.7.4 :

Табл.7.4

Видостандарт	MPEG-1	MPEG-2 (DVD)	MPEG-2 (DV)	MPEG-4
Скорост	1 - 2 Mbps	1.5 - 2.5 Mbps	до 25 Mbps	768 Kbps

Максималните скорости на пренос, осигурявани от различните клетъчни технологии, са систематизирани в таблица 7.5.

Табл.7.5

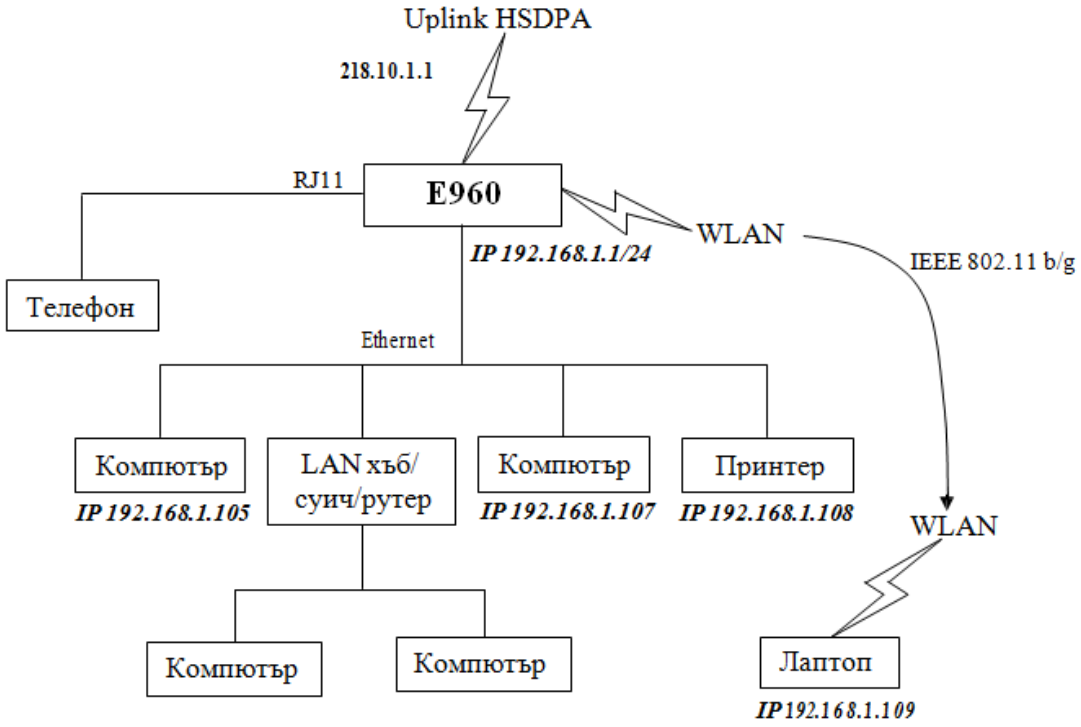
Технология	GSM	HSCSD	GPRS	EDGE	UMTS
Скорост	9.6 Kbps	14.4 Kbps	115.5 Kbps	384 Kbps	2 Mbps

Сравнението на данните от двете таблици показва, че скоростта, предлагана от GSM, е съвсем недостатъчна за трансфер на видео и за сърфиране в Internet. Двете 2.5G-технологии - GPRS и EDGE, значително подобриха нещата. Очевидно е, че бъдещето принадлежи на третото поколение системи, базирани на UMTS.

Накрая следва да се спомене и за още едно сравнително ново направление, наричано телематика (telematics). Нейн предмет са безжичните информационни системи, които изпращат/приемат съобщения и управляващи данни към/от мобилни устройства, инсталирани в автомобили. Телематиката използва сателитната GPS-технология за определяне на географските ширина и дължина с понататъшно конвертиране на същите в пътни карти, изобразявани на LED-конзоли, монтирани на таблата на автомобилите. Допълнително телематиката осигурява на превозните средства връзка с отдалечени центрове, които от своя страна осъществяват достъп до Internet, до фирмени бази от данни и гласова комуникация.

За изграждане на безжични локални мрежи (WLAN – Wireless LAN) операторите на мобилни телекомуникационни услуги предлагат техническо средство, представляващо безжичен терминал. Така например Мобилтел оферира абонатна услуга за безжична връзка с Интернет, предоставяйки на абонатите си устройството M-TEL HOMEBOX. Производител на същото е тайванската компания Huawei Technologies Co., Ltd, а моделът на самото устройство е HUAWEI E960. То работи като безжичен терминал и USB модем, подържайки технологиите HSDPA/WCDMA 2100 и GSM/GPRS/EDGE 1900/1800/900/850. Притежава 4 порта (куплунг тип RJ-45) за връзка с компютри или друга мрежова техника посредством Ethernet кабели, както и един USB порт и един порт за телефонен кабел (куплунг тип RJ-11). Когато устройството бъде свързано към компютър посредством своя USB порт, то изпълнява функцията на USB модем.

На фиг.7.16 е показана структурата на една примерна LAN, изградена посредством безжичния WLAN интерфейс и 4-те Ethernet интерфейса на безжичния терминал E960. Терминалът подържа хъбове (концентратори), суичове (комутатори) и рутери (маршрутизатори). За да бъде увеличен броя на компютрите в LAN следва да се използва допълнителен хъб или суич.



фиг.7.16

7.3 Защита на данните в безжичните мрежи

Паралелно с нарастване на популярността на безжичните комуникации и бързото им навлизане в дейността на хората, засили се и интересът на кракерите за осъществяване на пробиви в тях. Рисковете нарастнаха значително. Нещо повече, в Интернет се появиха безплатни програми за Windows и Linux, предназначени за кракване на безжични мрежи.

Появи се и друга опасност - жичните мрежи биват краквани по безжичен път. Това става посредством преносим компютър, включен чрез кабел към жична LAN, например от нищо неподозиращ служител на фирма, включил персоналния си компютър към мрежата на фирмата си. Тъй като вече, като правило, всеки преносим компютър е снабден с вградена карта за безжична връзка (интерфейс 802.11b/802.11g), един кракер, намиращ се някъде в близост, например отвън на паркинга на фирмата, може да влезе през безжичния интерфейс в преносимия компютър и от там в жичната LAN.

Непозволен достъп до мрежа на дадена компания може да се получи и случайно. Включвате своя преносим компютър и без да искате се свързвате с точка за достъп от безжичната мрежа на съседната компания, чийто обхват на действие припокрива действието на вашата безжична мрежа. През точката бихте могли да влезете в локалната мрежа на чуждата компания и да получите достъп до секретна информация или от там да се свържете по Интернет непозволено с някаква друга компания.

Злонамерени атаки кракерите могат да извършват посредством своя лаптоп. С помощта на специален софтуер те превръщат безжичната карта на лаптопа в легитимна точка за достъп, с помощта на която влизат в локалната мрежа на компанията вместо да използват легитимна точка за достъп, принадлежаща на мрежата. Такива лаптопи биват наричани „софт-точки” (soft APs). Атаката се извършва на MAC ниво (ниво 2 на фиг.37), поради което средствата за защита, използвани на ниво 3 (автентикация и VPN), не могат да послужат като бариера. MAC измама (кражба на идентификация) се осъществява, когато кракерът подслуша трафика и от него извлече MAC идентификатора (MAC адреса) на някой от компютрите в мрежата и присвоените му права на достъп. В безжичните мрежи е реализиран механизъм за MAC филтрация на адресите, който ограничава участието в мрежата, допускайки само устройства, които са били предварително регистрирани посредством своите MAC адреси. Съществуват обаче програми (например програмата SMAC), които подслушвайки трафика, разузнават мрежата и могат да регистрират в нея

допълнителен MAC адрес, посредством който след това може да се влезе нелегитимно в мрежата.

Съществува и друг начин да бъде „прескочена оградата". Става чрез използване на „посредник". Кракерът, превърнал компютъра си в „софт-точка" (soft APs), подмамва някой от легитимните участници в мрежата да се свърже с него. Веднъж осъществил това, кракерът прави връзка с реална точка за достъп (AP) от мрежата посредством другата безжична карта на компютъра си, създавайки нелегитимен трафик през хакнатия компютър. Атаки чрез използване на „посредник" се осъществяват с програми като LANjack и AirJack.

Друг вид атака е така наречената „отказ на услуга" (DoS - Denial of Service attack). Атакуващият непрекъсната бомбардира дадена точка за достъп до мрежата с лъжливи заявки, съобщения за неизправности или други команди. Това задръства мрежата и легитимните участници в мрежата не могат да получат достъп до нея. Мрежата отказва услуги.

За да се противодейства на атаките, необходимо е да се предприемат съответни защитни мерки, въпреки че 100%-ова защита е по принцип невъзможна. Стратегия за защита трябва да включва следните мерки:

- всички безжични LAN устройства трябва да бъдат осигурени със защитни средства;
- всички потребители на безжичната мрежа следва да бъдат обучени как се защитава мрежата;
- безжичната мрежа трябва да бъде непрекъснато наблюдавана за нарушения.

Всички технологии за безжични комуникации от групата IEEE 802.11 използват един или друг вариант на кодиране на данните с цел тяхната защита. Мрежите, отговарящи на стандартите 802.11a, 802.11b и 802.11g, използват методите WEP (Wired Equivalent Privacy) и WPA (Wi-Fi Protected Access) за криптиране на информацията. Криптирането на данни се извършва с помощта на алгоритма RC4, но биват използвани и по-прости начини за криптиране. Когато се закупува безжично устройство, необходимо е да се обръща сериозно внимание на начина на защита на данните. Някои производители на безжични устройства, за да поевтинят изделията си, използват по-прости алгоритми за кодиране. Така

или иначе, проблемът за защита на данните при безжичните комуникации остава открит. Все още е сравнително лесно да бъде уловен сигналът от ефира и да бъде декодиран за един или няколко дни.

WEP криптиране

WEP (Wired Equivalency Privacy) бе първият стандарт за криптиране в безжични мрежи. За съжаление той не можа да издържи изпитанията на времето. Появиха се програми като aircrack-ng, weplab, WEPCrack или airsnort, които позволяват бързо да бъдат откривани ключовете, с които е било извършено криптирането. Дължината на ключовете е 128 или 256 бита. Всички устройства в мрежата ползат един и същ WEP ключ. Достатъчно е да бъде разгадан ключът на едно от устройствата, за да рухне защитата на цялата мрежа.

Във WEP се използва алгоритмът за криптиране RC4, който се оказа, че притежава недостатъци. В един документ, наречен „Weaknesses in the Key Scheduling Algorithm of RC4" с автори Scott Fluhrer, Itsik Mantin и Adi Shamir, бяха описани теоретично с подробности слабостите в генерирането и реализирането на WEP. По-късно студентът Adam Stubblefield от Университета Райе проведе първата WEP атака. Макар че той не разпространи публично своите инструменти, вече се предлагат подобни такива за Linux, даващи възможност на атакуващите да пробият WEP, превръщайки го в ненадежден протокол за сигурност. Все пак подобре е с WEP отколкото съвсем без криптиране. WEP кодирането отстъпва по сигурност на WPA-PSK.

Всички безжични устройства (рутери, точки за достъп и безжични интерфейсни карти) притежават вградена WEP функция. Като правило производителите на тези устройства я изключват по подразбиране, поради което мрежите остават незащитени. Включването на функцията изисква известни умения, което в много от случаите затруднява или пък не се удава на по-малко опитните потребители. Освен това различните производители залагат в устройствата си различни криптиращи ключове (HEX, ASCII и др.), което затруднява използването на WEP.

WPA криптиране

WPA (Wi-Fi Protected Access) представлява първоначална версия на стандарта 802.11i за защита на безжичните мрежи посредством криптиране на информацията. Същият

бе разработен от Wi-Fi Alliance с цел да замени несъвършения WEP. В WPA като основен е заложен алгоритъмът за криптиране TKIP (Temporal Key Integrity Protocol), но WPA допълнително подържа и алгоритъма AES (Advanced Encription Standard), който е предпочетен като основен в следващата версия на стандарта WPA2. Ключът на криптиране е 256 битов.

При WPA криптиращите ключове са динамични. В съответствие с TKIP по автоматичен път те биват периодично променяни (rekeying) и автентикирани между устройствата, включени в мрежата. Периодът на промяната е по подразбиране 0, но може да бъде задаван в мрежата от потребителите.

WPA предлага механизъм за автентикация на участниците в мрежата. Съществуват два начина, според версиите на WPA - WPA Enterprise за безжични мрежи на компании и WAP Personal за частни безжични мрежи. Във WPA Enterprise се използва EAP (Extensive Authentication Protocol) автентикацията, използвана в стандартите IEEE 802.1x. Във WAP Personal се използва споделян ключ (PSK - Pre-shered Shared Key) за създаване на защита на базата на фраза, съставена от 8 до 63 символа (максимум 256 бита). Една неудачно съставена фраза може да бъде разгадана за няколко минути с помощта на програмата aircrack-ng. Добър PSK ключ е например фраза, състояща се от 64 шестнайсетични цифри. WPA в съчетание с PSK се бележи като WPA-PSK.

WPA2 криптиране

WPA2 е последната, най-нова версия на стандарта 802.11i. Основното подобрение на WPA2 спрямо WPA бе в залагането на AES (Advanced Encription Standard) алгоритъма за криптиране като основен. Подобно на WPA, WPA2 подържа автентикация на базата на методите EAP и PSK. WPA2 в съчетание с PSK се бележи като WPA2-PSK.

SSID имена

Освен криптиране на информацията и използване на автентикация, в безжичните LAN (WLAN – Wireless LAN) се използва и контрол на достъпа на безжичните устройства до точките за достъп (APs). Във всяка една от работните станции на безжичната мрежа се указва идентификационното име (SSID - Service Set ID) на точката, с която станцията ще извършва комуникация. Това име изпълнява ролята на парола, когато устройството реши да

се свърже с точката за достъп. Всички устройства и точки за достъп в една WLAN трябва да използват едно и също SSID име. То се явява идентификатор на мрежата. Припокриващите се по обхват на действие WLAN трябва да използват различни SSID.

Освен защитата чрез SSID, във всяка точка за достъп се съхранява списък с MAC адресите на устройствата, упълномощени да се свързват с нея. С помощта на списъка точката контролира достъпа до нея. MAC адресите и SSID се съдържат в хедерите на пакетите. Те на са криптирани, поради което могат да бъдат лесно прочитани. Поради това SSID не може да представлява сигурна защита на WLAN.

Моля, отговорете на контролните въпроси:

1. *Кога е разликат между ZigBee и Bluetooth ?*

2. *Какви са особеностите, ако е необходимо да се реализира безжична мрежа за по-големи разстояния?*

3. *Кое указаните не е технология? :*

а) UTP; б) CDMA; в) FDMA; г) TDMA.

4. *Каква е разликата между AP и безжичен рутер?*

5. *Кой вид криптиране използван при безжичните мрежи е най-добър?.*

Раздел 8

Виртуални частни мрежи. Виртуални локални мрежи

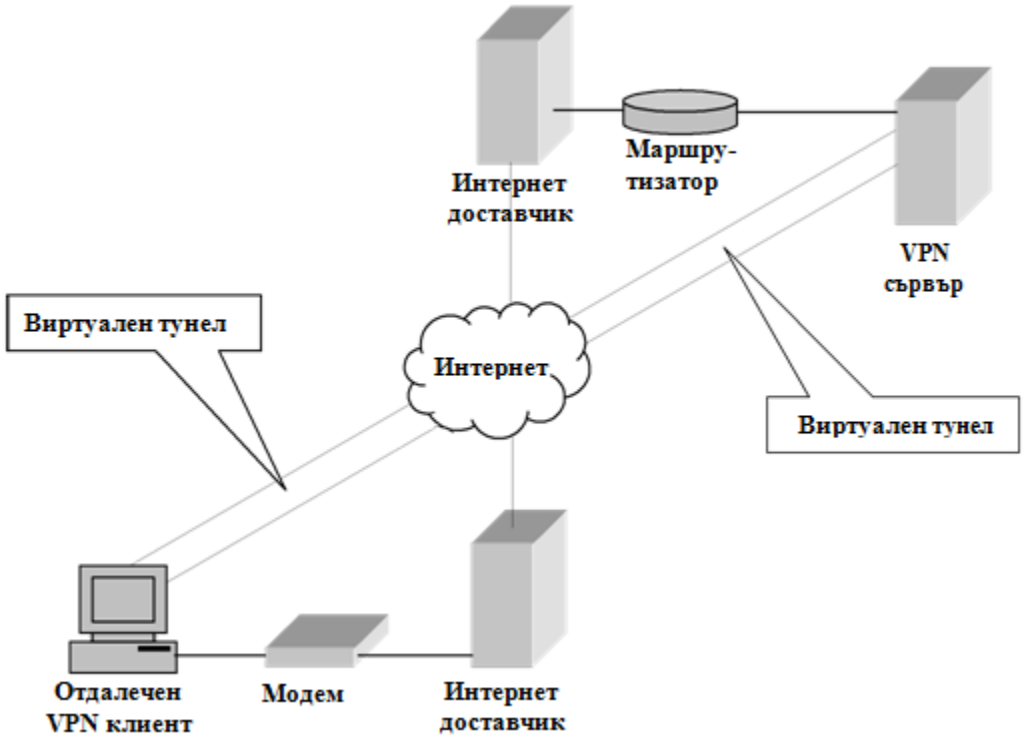
Ключови думи и съкращения

VPN **VLAN** **хеш**	**тунел** **VoIP** **IP телефон**

8.1 История на виртуалните частни мрежи

Връзката чрез виртуална частна мрежа (virtual private networking-VPN) придоби голяма популярност през последните години..

Вместо директна комуникационна връзка между компютрите, при VPN се създава тунел през обществена мрежа, обикновено Интернет, през която комуникиращите компютри се свързват помежду си (фиг.8.1).



Фиг.8.1

Данните се изпращат по обществената мрежа по начин, който емулира връзка от тип „от точка до точка”. VPN създава през обществената мрежа тунел, който е независим

от местоположението на комуникиращите компютри. Тунелът е **логическа връзка** от точка до точка, която поддържа автентикация и криптиране на данните.

Терминът „виртуална частна мрежа" се състои от три думи. Думата „мрежа" означава компютри, които комуникират помежду си, „виртуална" показва, че мрежата не използва директна връзка (кабелна или безжична), а „частна", че изпращаните данни са конфиденциални, понеже при VPN те са криптирани по време на тяхното преминаване през мрежата.

8.1.1 Тунелиране и капулиране

Тунелирането представлява процес на капсулация и декапсулация на данните Тунелирането скрива оригиналния пакет във вътрешността на нов пакет. Процесът се нарича **капсулиране на данните**. За извършване на маршрутизация през тунела, адресът на крайната точка на тунела се указва в хедъра на новия (външния) пакет, наричан **хедър на капсулацията**. Тук следва да се отбележи, че адресът на крайното местоназначение се съдържа в хедъра на оригиналния пакет.

Когато пакетът стигне до края на тунела, хедъра на капсулацията се премахва и оригиналният пакет се доставя до крайното му местоназначение..

Самият процес на тунелиране се изпълнява от специално разработени за целта протоколи. Според това на какво ниво от OSI модела работи протоколът, съществува тунелиране на ниво 2 и тунелеране на ниво 3.

При тунелирането на ниво 2, протоколът работи в каналния слой. Такъв е например протоколът **PPTP** (Point-to Point Tunneling Protocol) на Microsoft, който, както показва неговото название, осигурява виртуална връзка от една точка до друга. Друг такъв е протоколът **L2F** (Layer 2 Forwarding), разработен от Cisco Systems. За разлика от PPTP той може да подържа повече от една връзка.

Протоколът **L2TP** (Layer 2 Tunneling Protocol) комбинира елементи на PPTP и L2F. L2TP е в състояние да капсулира IP, IPX и други видове пакети при предаването им по IP мрежа.

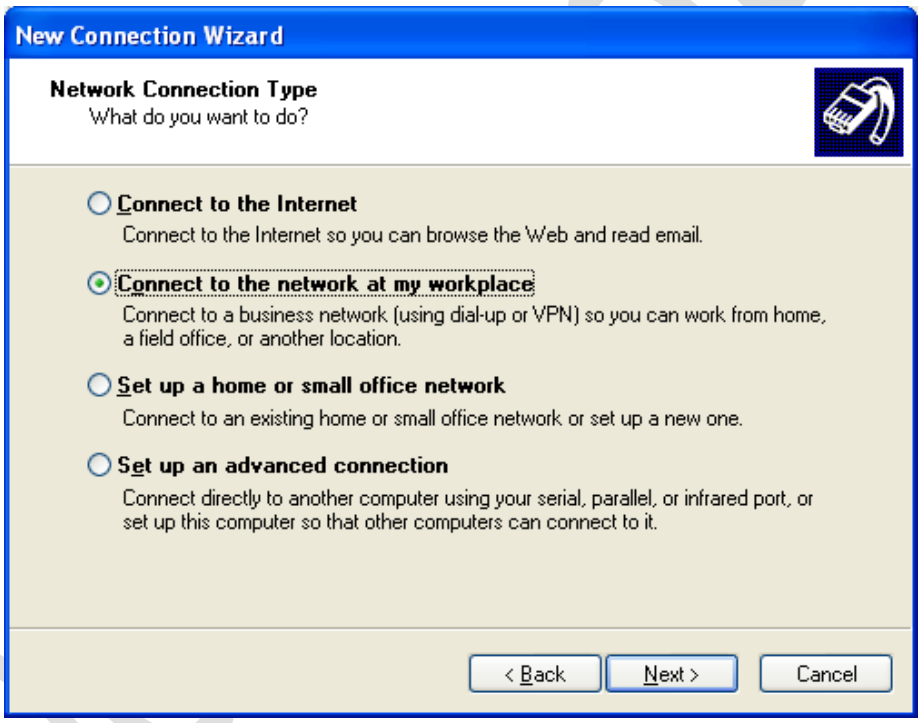
Тунелирането на ниво 3, работи в мрежовия слой, поради което е в състояние да осигурява IP-базирани виртуални връзки. Тук IP пакетите биват капсулирани в протоколни обвивки, които използват IPSecurity (IPSec), Internet Key Exchange (IKE) и методи за

автентикация и криптиране като: Message Digest 5 (MD5), Data Encryption Standard (DES) и Secure Hash Algorithm (SHA).

Протоколът IPSec може да капсулира единствено IP пакети. Той би могъл да се използва и съвместно с L2TP. В този случай L2TP изгражда тунела, а IPSec криптира, при което IPSec работи в транспортен режим.

Съвременните операционни системи притежават вградена подръжка на VPN. Те позволяват лесно създаване на връзка към VPN по начин, подобен на този, по който се изгражда една dialup връзка.

Като се започне от Windows 95 всички следващи версии на Windows могат да функционират като VPN клиенти (фиг.8.2).



Фиг.8.2

Linux подържа използването на IPSec и на PPTP. В допълнение Linux може да изпълнява протокола PPP (Point-to-Point Protocol) през Secure Shell (SSH), който използва RSA технология с публичен ключ за автентикация и управление на сигурността на връзката.

8.1.2 Изграждане на VPN мрежи

VPN могат да бъдат изграждани по няколко начина, в зависимост от конкретните нужди.

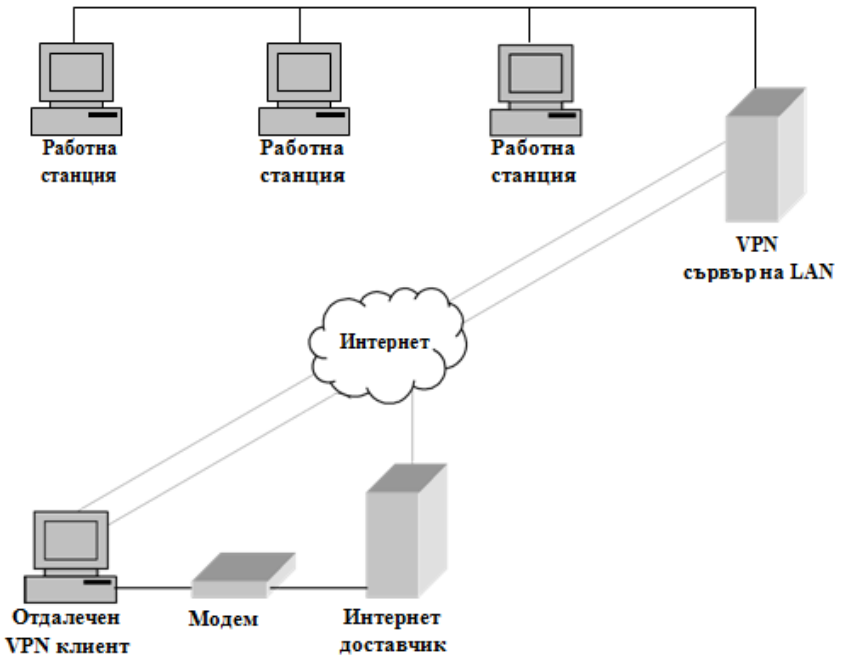
VPN биват използвани най-често за следните цели:

- За осигуряване на отдалечен достъп до мобилни служители или до такива, които работят вкъщи.
- За създаване на екстранет мрежа (частна мрежа, използваща отдалечени връзки, най- често Интернет), до която имат достъп служители, клиенти и партньори на дадена бизнес организация.
- За осъществяване на контакт между два офиса, разположени отдалечено един от друг, без да се изгражда за целта специална директна връзка.

VPN може да бъде конфигурирана да работи по dialup връзка (фиг.8.3) или да бъде конфигурирана като връзка от типа маршрутизатор-маршрутизатор (фиг.8.4), при която за маршрутизаторите са заделени специални Интернет връзки, т.н. ***T1 линии.***

VPN за отдалечен достъп до отделни потребители

На фиг. 8.3 е показан един примерен вариант на реализация. VPN клиентът трябва да може да подържа протоколите, използани от VPN сървъра.



Фиг.8.3

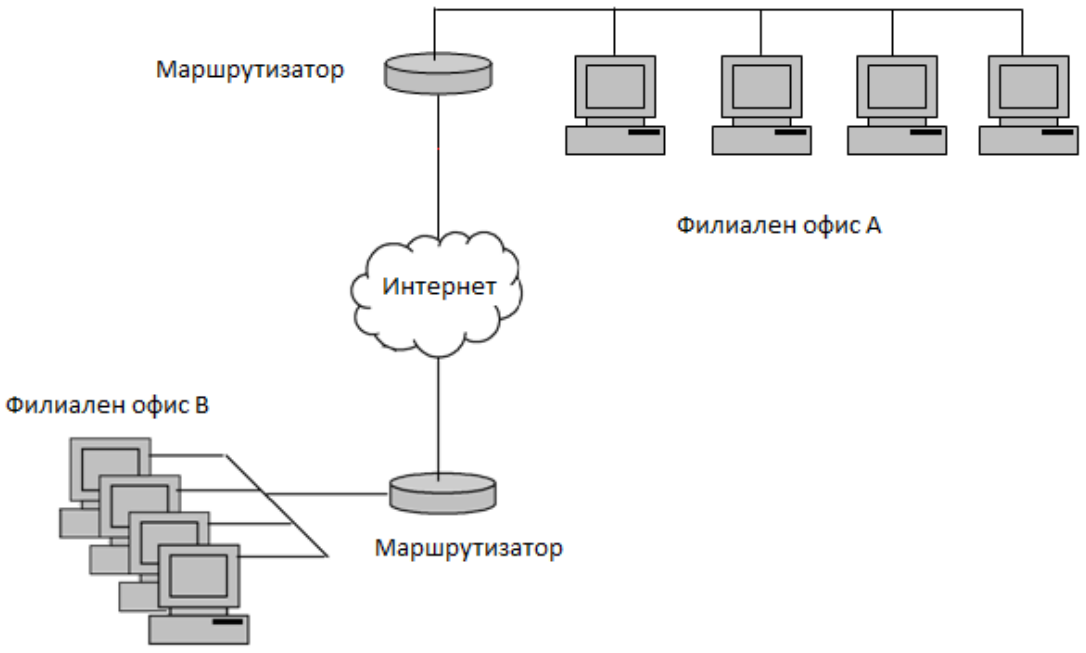
Мрежата работи по следния начин:

- За да изгради Интернет връзка, мобилният или домашният клиент набира по телефона локалния доставчик на Интернет и се свързва с него посредством потребителски акаунт. Ако клиентът използва наета връзка, например ADSL адаптер, тази стъпка отпада.
- След създаване на връзката с Интернет, клиентът извиква VPN сървъра на LAN, като използва неговия IP адрес. VPN сървърът е конфигуриран така, че да приема VPN заявки. В резултат от тази стъпка се изгражда тунелът.
- Клиентът се автентикира в частната LAN и получава достъп до нея.

Когато клиентът използва наета (постоянна) връзка с Интернет, той би могъл да конфигурира домашния си компютър като VPN сървър и след това да се свърже към него от офиса на фирмата за достъп до файлове, съхранявани върху домашния му компютър.

Изграждане на VPN връзки между офиси на фирма

На фиг. 8.4 е показана схема на VPN от тип маршрутизатор-маршрутизатор. Тя е изградена с помощта на маршрутизирани връзки към Интернет.



Фиг.8.4

Връзката на всеки офис към Интернет може да бъде набирана при необходимост (***dial on demand***) или да бъде постоянна.

При връзка с набиране маршрутизаторът използва dialup връзка с Интернет. Другият маршрутизатор, този който бива повикван, трябва да има постоянна връзка с Интернет и да е конфигуриран за приемане на връзки от типа набиране при необходимост. В повикващия маршрутизатор се конфигурират две връзки с набиране при необходимост – едната за набиране на Интернет доставчик (ISP) и другата за свързване към VPN.

Ако двата маршрутизатора имат постоянни връзки към Интернет, ако е необходимо, VPN връзката може да бъде установена и оставена постоянно открита.

VPN връзката от типа маршрутизатор-маршрутизатор може да бъде конфигурирана като еднопосочна или двупосочна. В първия случай единият маршрутизатор трябва да действа като клиент и да инициира връзката, а другият да функционира като VNP сървър. Във втория случай, при двупосочна връзка, двата маршрутизатора трябва да имат постоянна връзка с Интернет, да са настроени да работят като LAN и WAN маршрутизатори и всеки един от тях да е в състояние да инициира VPN връзка.

8.1.3 Предимства и недостатъци на VPN

Предимствата на VPN са следните:

- Спестяват разходите за междуградски разговори, когато отдалечените потребители се намират извън областта за набиране на локални номера.
- Изискват по-малко телефонни линии за осигуряване на отдалечен достъп до множество потребители едновременно.
- Изискват по-малко хардуерно оборудване.
- VPN мрежите, базирани на ISP (доставчици на Интернет), редуцират цените за администриране и обучение.

Към недостатъците на VPN мога да бъдат отнесени следните обстоятелства:

- Ако един от доставчиците на Интернет изключи ISP сървъра си за техническа профилактика, VPN връзка не може да се осъществи. При директна dialup връзка към LAN това не би могло да се случи.

- Производителността на VPN е по-ниска, тъй като допълнително се изпълняват протоколите, реализиращи VPN. При директна dialup връзка към LAN, протоколи за VPN не се изпълняват.

8.2 Виртуални локални мрежи

Мрежовата производителност е съществен фактор, който определя качеството на една компютърна мрежа. Една от технологиите, която допринася за подобряване на мрежовата производителност е разбиването на един голям броадкастен домейн в по-малък. Това е възможно чрез изпозлването на виртуална локална мрежа (Virtual Local Area Network, VLAN). По малките броадкастни домейни ограничават броя на устройствата, които участват в броадкастната комуникация и това дава възможност те да бъдат отделени в различни функционални групи, например като услуги за бази данни в счетоводен отдел и едновременно с това високоскоростен трансфер на данни за инженерен отдел..

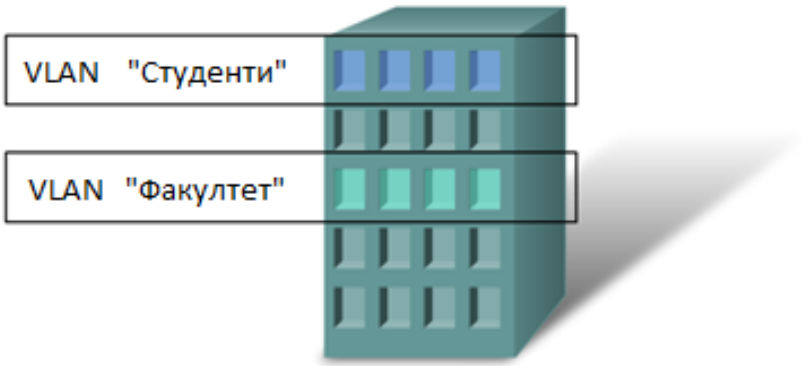
Виртуална локална мрежа (Virtual Local Area Network, VLAN) рредставлява метод за разделяне на една физическа компютърна мрежа на различни виртуални мрежови сегменти с цел логическа организация, контрол и защита. Потребителите в един VLAN могат да комуникират само помежду си, но не и с потребители от другите виртуални мрежи. Предимството е, че едни и същи комутатори могат да предоставят множество VLAN-и и по-този начин се спестяват разходи за оборудване.

Като пример може да се разгледа мрежа на фирма с три отдела, разположени на три етажа – Инженерен (Engineering), Маркетинг (Marketing) и Счетоводен (Accounting). Във фирмата има една физическа LAN мрежа, която се използва от всички отдели, но всеки отдел е обособен в собствен VLAN. Различните портове на комутаторите са конфигурирани да предоставят достъп до различните VLAN-и. Служителите на Маркетинг отдела на първи и втори етаж могат да се достигнат един друг и имат достъп до техния сървър, но не могат да достъпят сървърите и служителите на другите два отдела. Ако не се използват VLAN-и, ще е необходимо да се изградят три отделни физически мрежи – по една за всеки отдел, което би оскъпило решението поне три пъти

Виртулалните локални мрежи (VLAN) позволяват на мрежовия администратор да създава логичеки групи от мрежови устройства, които функционират така че все едно са в тяхна собствена независима мрежа, въпреки че те самите са в една обща инфраструктура с

други устройства и други виртуални локални мрежи. Използвайки VLAN мрежата може да бъде логически сегментирана на база отдели, финкциии или екипи, работещи по различни проекти. Например може да бъде дефинирана студентска VLAN, преподавателска VLAN и администраторска такава. Разделението на отделни VLAN може да бъде реализирано дори и на географски принцип.

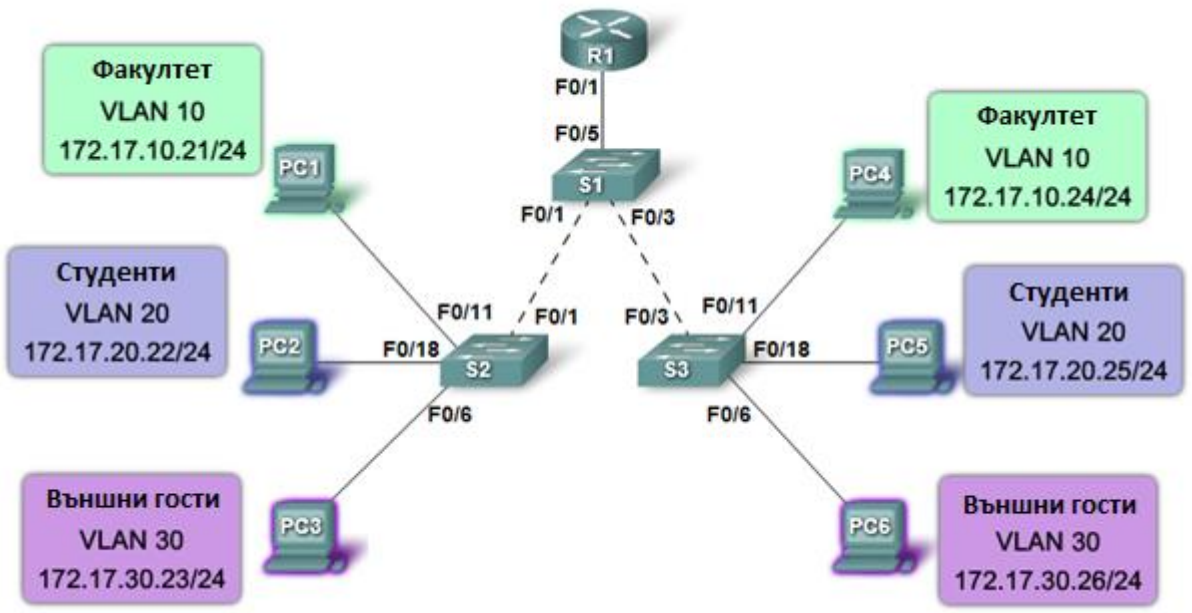
На фиг.8.5 са показани две виртуални локални мрежи за студенти и за един факултет. Тези VLAN позволяват на мрежовия администратор да прложи различни политики за достъп и сигурност за отделните групи потребители – студенти и преподаватели. Например на предподавателите може да бъде позволен достъпа до сървър с цел разработване на електронни материали за обучение, докато за студентите достъпа ще бъде ограничен само с цел ползване на разработените електронни материали.



Фиг.8.5

8.2.1 Същност на VLAN

Една VLAN представлява логически разделена IP подмрежова структура. Това рзделение позволява множество IP мрежи и подмрежи да съществуват в една и съща мрежова инфраструктура. Фигура 8.6 показва мрежа с три компютъра. За да могат компютрите да комуникират в една VLAN всеки от тях трябва да има IP адрес и маска, които са съществени за дадената VLAN. От друга страна комутатора (switch) трябва да бъде конфигуриран за работа с VLAN и всеки един от неговите портове трябва да бъде обвързан с определена VLAN. В този случай порта се дефинира като порт за достъп до определена VLAN (access port).



Фиг.8.6

Предимства на VLAN

Производителността и гъвкавостта на една мрежа по отношение на ресурсите, които тя предоставя на своите потребители. Основните предимства на VLAN са следните:

- ✓ Сигурност – Групите, които обработват „ключови" за сигурността данни са отделени останалите потребители на мрежата. По този начин се намалява вероятността за пробив в сигурността на конфиденциална информация. Компютрите на Факултета са в VLAN 10 и са напълно отделени от трафика на студентите и външните потребители.
- ✓ Ниска цена – Намаляването на разходите се получава в резултат от по малката необходимост от скъпо струващи подобрения (upgrade) на мрежата и по-доброто ефективно използване на честотната лента.
- ✓ По-висока производителност – Разбиването на една мрежа на Ниво 2 от модела OSI на по-малки логически работни групи (broadcast domains) намалява излишния трафик в мрежата подобрява производителността..
- ✓ Смекчаване на „броадкастната буря" – разделянето на мрежа в VLAN намалява броя на устройствата, които могат да участват в т.н. „броадкастна буря".

- ✓ Подобрена ефективност на IT отдела – VLAN прави процеса на управление на мрежата по лесен, защото потребителите с еднотипни изисквания и ресурси споделят една и съща виртуална мрежа. Когато се подсигури един нов комутатор и всички политики и процедури са предварително конфигурирани за опредлена VLAN, те автоматично биха могли да се приложат и активират.

По-лесно управление на приложенията – VLAN обединяват потребителите и мрежовите устройства в едно общо цяло не само по отношение на опредлено приложение, като това се реализира независимо от географското им разположение.

8.2.2 Типове VLAN

Един от най-използваните видове виртуални локални мрежи са порт базираните VLAN (port-based VLAN). При този вид виртуална локална мрежа порта на даден комутатор (switch) се обвързва с прнадлежност към дадена VLAN. В сферата ма мрежите съществуват множество термини, свързани с виртуална мрежа. Някои от тези термини дефинират вид на VLAN в зависимост от мрежовия трафик, който те пренасят, докато при други се нбляга на функциите, които конкретната VLAN изпълнява. Основни видове VLAN са следните:

VLAN за данни (data VLAN)

Този вид виртуална локална мрежа се конфигурира да пренася само трафика, който е генериран от потребителите. Дадена VLAN би могла да пренася гласов трафик или трафик, използван за конфигуриране на комутатора или други мрежови компоненти, но този трафик не е част от потребителския трафик. Добрите практики показват необходимостта от отделянето на гласовия и управляващия трафик от този на полезните данни.

VLAN по подразбиране (Default VLAN)

При първоначалното стартиране на един комутатор всички негови портове сса обвързани с т.нар. виртуална локална мрежа по подразбиране. Този факт определя участието на всички тези портове в един общ голям броадкаст домейн. Това позволява на всяко устройство, включено н който и да е порт да реализира комуникация с другите устройства по останалите портове. Обикновено виртуалната локална мрежа по

подразбиране е в номер 1 (VLAN 1). От гледна точка на игурност добра практика е смяната на подразбиращата се VLAN.

Обща (местна) VLAN (Native VLAN)

Общата виртуална локална мрежа се дефинира за т.нар „трънк" (trunk) порт (стандарт 802.1Q). Този порт пренася трафика за всички виртуални локални мрежи, чиито трафик е маркиран със специален „маркер" (tagged). Обикновено в мрежта съществува и немаркиран (untagged) трафик. Това е трафик, който не е обвързан с конкретна VLAN. Немаркираният трафик се пренася именно от тази „native" VLAN. На фиг.4444 native VLAN се явява VLAN 99. Такъв немаркиран трафик се генерира от компютър, който е свързан на порт, конфигуриран с „native" VLAN. Този тип "native" VLAN са включени в стандарта IEEE 802.1Q с цел да се осигури съвместимост с немаркран трафик в по-стари локални мрежи. Добра практика е да се предефинира „native" VLAN, която по подразбиране е VLAN 1.

VLAN за управление (Management VLAN)

Виртуалната локална мрежа за управление се използва за управление на комутатора. Добра практика е тя да се предефинира, тъй като по подразбиране е VLAN 1. На тази VLAN се присвоява IP адрес и маска, и по този начин се предоставя възможност за отдалечено конфигуриране. Комутаторът може да бъде управляван чрез HTTP, Telnet, SSH или SNMP.

Гласова VLAN (Voice VLAN)

Лесно е да се предположи защо е необходимо да се отдели VLAN специално за пренасяне на гласов трафик. С навлизането на мрежите в разлчини области се осигури възможност и за вкарването на глас в общия трафик (Глас върху IP, Voice over IP, VoIP). От друга страна за да се осигури качествено обслужване на този трафик, тъй като при приемане на спешни повиквания и внезапно пропадане на качеството на връзката, потребителя няма да може да разбере за какво говори обаждащия се. Трафикът за глас VoIP трафик изисква:

- ✓ Определена честотна лента за осигуряване на високо качество на гласа
- ✓ Приоритизация на този вид трафик по отношение на останалия, с цел по бързо обслужване от мрежовите устройства

- ✓ Способност да бъде рутиран дори и през натоварени участъци в мрежата
- ✓ Закъснение на не повече от 150 ms при разпротраняването му в мрежата

С цел да се осигурят тези изисквания цялата мрежа трябва да бъде проектирана да поддържа трафика за глас VoIP. В добавка е необходимода бъде използван IP телефон.

Режими на портовете на VLAN комутатора

Когато се конфигурира една VLAN е необхдимо да се дефинира и присвои номер-идентификатор (ID), който представлява номера на виртуалната локална мрежа. Именно с този идентификатор трябва да бъде обвързан даден порт на комутатора. Това обвързване определя прехвърлянето на кадър определената виртуална локална мрежа, примерно VLAN 4. Обвързването на даден порт като чрен на дадена VLAN може да се извърши по следните режими:

- ✓ ***Статичен (Static VLAN)*** – в този случай конфигурирането се извърша ръчно.
- ✓ ***Динамично (Dynamic VLAN)*** – използването на този подход изисква наличието на специален сървър за членство на определ компютър към конкретна VLAN (VLAN Membership Policy Server, VMPS). С използването на такъв сървър, динамичното обвързване на даден порт към определена VLAN се основана на физическия адрес на компютъра, свързан към този порт.
- ✓ ***Гласова VLAN (Voice VLAN)*** – в този случай в процеса на конфигуриране, изрично се споменава членството на порта на комутатора към гласовата VLAN. Необходимо е също така да се икажат и параметрите за подобряване качеството на обслужване (Quality of service, QoS) за този тип трафик.

Моля, отговорете на контролните въпроси:

1. *Какви протоколи за изграждане на виртуални частни мрежи познавате?*
2. *Какво представлява понятието "хеш" функция?*
3. *Какви видове криптиране се използват във виртуални частни мрежи?*
4. *С какво устройство може да се реализира виртуална локална мрежа?:*
5. *Каква е разликата между виртуални частни мрежи и виртуални локални мрежи?*

Раздел 9

Сигурност в мрежите

Ключови думи и съкращения

DoS	**UPS**
IP спуфинг	**SYN атака**
RAID	**Троянски кон**
Ping of death	**Контрол на достъп**

9.1 Защита на компютърните мрежи

Важен въпрос, касаещ мрежите, е защитата на данните от загуба и/или от злоупотреба. Той бива разглеждан в два аспекта – мрежова сигурност и предпазване от случайни сривове.

Под мрежова сигурност следва да се разбират мерките за защита от преднамерен или случаен достъп до информацията, съхранявана в мрежата. Пълна (100%-ова) гаранция за мрежова сигурност никога не може да има. Напълно сигурна е оная мрежа, до която никой няма достъп, а такава мрежа не е нужна никому.

Мрежовата сигурност е горещ проблем в света на информационните технологии. Бизнесът става все по-зависим от компютърните мрежи и информацията, съхранявана в тях. Но заедно с това той става все по-уязвим от пробиви в мрежовата сигурност. Често ставаме свидетели на съобщения в медиите за проникване в мрежите на правителствени и бизнес организации, както и за поражения, нанасяни от компютърни вируси.

Външните и вътрешни нарушители на мрежовата сигурност не са единствената заплаха за мрежите. Възможни са и случайни сривове, предизвикани от хардуерни повреди, природни бедствия или технически грешки в експлоатацията. Всички те водят до загуба на файлове, съдържащи в редица случаи ценна информация.

9.1.1 Видове заплахи

Когато започва изграждане на компютърна мрежа, винаги се поставя и въпроса за нейната сигурност. Анализира се степента на конфиденциалност на данните и се определят нуждите от защита. На тази база се съставя план за мерките, които трябва да се предприемат за осигуряване на нужната мрежова сигурност.

Заплахите за сигурността биват вътрешни и външни.

Вътрешни заплахи

Вътрешните пробиви на сигурността се осъществяват от служители на организацията, експлоатираща мрежата. Мотивите за това могат да бъдат:

- Корпоративен шпионаж, свързан с кражба на търговски, технически или други тайни. Осъществява се в полза на конкурентни компании от подкупни служители. Този вид шпионаж спада към най-интелигентните, тъй като се извършва от хора с висок професионален опит. Мерките за сигурност, предназначени за осуетяване на корпоративен шпионаж, се осъществяват на най-високо управленско ниво с помощта на специалисти, посветени в защитата от шпионаж на корпоративните мрежи.
- Саботаж. Понякога кариеристично настроени служители, за да покажат, че се справят в работата по-добре от техните колеги, прибягват до саботаж на дейността на последните. Формите на саботаж могат да бъдат най-различни, като се започне от претърсване на чужда електронната поща и на файлове за добиване на някаква уличаваща информация и се стигне до съзнателно унищожаване на важни данни. Особено опасни са служители, недоволни от политиката (понижение, уволнение и прочие), провеждана спрямо тях от страна на организацията, в която те работят. Те са в състояние да повредят съзнателно даден хардуер, да изтрият информация от твърдите дискове или да разпространят вируси в мрежата.
- Случайни пробиви. Причиняват се несъзнателно от служители на организацията, поради техническа некомпетентност или липса на подготовка. В старанието си да „поправят" възникнал дребен проблем, те биха могли да затрият ценна информация. Чрез въвеждане на позволения за работа само с определени файлове, тази опасност може да бъде сведена до някакъв минимум, но не може да бъде избегната напълно.

Външни заплахи

Към външните заплахи могат да бъдат отнесени:

- неоторизирано използване на пароли и ключове;
- DoS атаки;

- IP спуфинг;
- компютърни вируси и червеи;
- троянски коне.

Неоторизирано използване на пароли

Паролите и ключовете са ефективно средство, само когато те се пазят в тайна. Ако някой узнае вашите потребителско име и парола, той получава достъп до компютъра и мрежата и би могъл да свали от там конфиденциална информация.

В много случаи придобиването на парола представлява първа стъпка от хакването на една система. Хакер означава лице, което се вмъква в компютърните системи с намерение да открадне или унищожи данни. Първоначално терминът хакер означаваше добър програмист, но днес той придоби отрицателен смисъл. Когато един хакер получи неоторизиран достъп чрез име и парола на потребителски акаунт, казваме, че той е кракнал системата, а той самият бива наричан кракер (разбивач). Сигурността на паролите е важна част от изграждането на добра мрежова сигурност.

Хакерите придобиват паролите по много начини. Това може да стане чрез наблюдение, отгатване (когато за пароли се използват рождени дати, имена на съпруги или деца и т.п.), чрез измама (хакерите се представят за мрежови техници или администратори, на които наивния потребител поверява паролата си) или чрез налучкване (чрез програми, които автоматично генерират и изпробват различни пароли). По-грамотните хакери са в състояние, посредством така наричаните „снифър пакети", да прихващат от мрежата пакетите с данни, сдържащи паролите. За борба с тази техника на прихващане на пароли се използва криптиране на последните.

Атаки от типа DoS

Атаките от типа DoS (Denial of Service – отказ от услуга) биват наричани още нюк (nuke) атаки. Те не предизвикват срив на атакуваната машина, а нарушават нейното нормално функциониране. Най-често използвани форми на DoS атаки са:

- наводнението на протокола Ping/Internet Control Message Protocol (ICMP);
- смърф атаката;
- Ping на смъртта;
- SYN атаки.

Ping/ICMP наводнение.

ICMP е протокол за съобщения и проверки за грешки, използван в Интернет за предаване на информация. Командата ping е използвана за проверка дали даден компютър в мрежата се обажда. За целта тя използва ICMP пакети. Командата изпраща съобщение, наричано ***ICMP Echo Request*** и чака да получи отговор, наричан ***ICMP Echo Replay***. ICMP наводнението се състои в „наводнение" на протокола ICMP с пакети, предизвикващо „задавяне" на системата, към която е било извършено обръщане чрез командата ping. На IP адреса се изпращат непрекъснато пакети, в резултат на което той започва да забавя своята работа, след което се изключва поради таймаута на командата ping.

Смърф атаката е вид ICMP наводнение, което влияе на целия мрежов сегмент. Изпраща се съобщение до бродкастен адрес, което достига до всички компютри в мрежата, заставяйки ги да отговорят. Това натоварва мрежата и всички комуникации се забавят, в резултат на което всички потребители в един момент зцагубват връзката с мрежата.

Ping на смъртта е атака, която използва ограниченията, налагани от максималната единица за предаване (MTU - maximum transmission unit) на информация в мрежата. MTU се определя от пропускната способност на преносната среда и от архитектурата на мрежата. Ако бъде изпратен пакет, който надхвърля MTU, той бива разделян на по-малки парчета и след това сглобяван отново след като достигне до крайното си местоназначиние. IP пакетът, в който е капсулирана заявката за ICMP exo, е ограничен до 65535 октета (един октет съдържа 8 бита). Ако бъде изпратен пакет с размер, надхвърлящ максималния брой октети, компютърът-получател няма да бъде в състояние да сглоби разбития на части пакет и ще срине своята работа.

SYN атаката използва синхронизиращата последователност на TCP, за да осъществи прекъсване на комуникациите. За изграждане на сесия TCP използва процес на тристранно ръкостискане. Клиентът предава сегмент със заявка SYN за синхронизация, представляваща число. Сървърът изпраща на клиента отговор (потвърждението ACK), който включва числото, изпратено от клиента, увеличено с единица, заедно с друго SYN число, генерирано от сървъра. Клиентът добавя единица към числото на сървъра и го връща обратно на сървъра под формата на ACK. Ако процедурата протече нормално, двата компютъра установяват комуникационна връзка помежду си.

Атаката се състои в изпращане на голям брой SYN заявки, посредством подправен (спуфнат) IP адрес (виж следващия абзац). Приемащият компютър поставя заявките в опашка и започва да ги обслужва. Чрез непрекъснато запълване на опашката със заявки и поддържането й в това състояние, се пречи на компютъра да обслужва други заявки. По този начин потребителите не могат да получат връзка към сървъра.

IP спуфингът представлява подправяне на IP адрес. Изпращат се отвън съобщения, на които пакетите, по-конкретно техните хедъри, са така променени, че да изглеждат сякаш идват от компютър, принадлежащ на мрежата. С придобития по този начин достъп до мрежата може да започне атака за кражба или унищожаване на данни.

Компютърните вируси са програми, които могат да нанасят най-различни поражения – от смущаване на визуализацията до изтриване на файлове на операционната система. Те притежават способността да се репликират и да се разпространяват от един компютър на друг, без знанието на потребителите.

Червеят (worm) е вирус, който притежава способността да се саморепликира и да унищожава файлове в компютрите. Червеите се разпространяват най-често като атъчменти към електронната поща или като документи, съдържащи макроси. Те могат да попаднат в мрежата и с HTMLстраници, сдържащи червеи под формата на скриптове.

Троянските коне са зловредни програми, които биват представяни пред потребителите като програми, предназначени за извършване на някаква определена полезна дейност. Стартирането на една такава програма довежда до неочаквани вредни последствия. В много от случаите това са Web-сайтове, които изискват от потребителите въвеждане на личните им данни, които след това биват ползвани за пъклени цели.

9.1.2 Мерки за сигурност

Сигурност на паролите

Важна част от плана за сигурност на мрежата е осигуряване на по-неразгадаеми пароли. На потребителите на мрежата трябва да бъдат препоръчани следните правила за създаване на пароли.

- Паролите не трябва да бъдат думи или числа, имащи някаква връзка с потребителя, като например рождена дата, име на член от семейството, име на куче и т.п.
- Паролите не трябва да бъдат думи от речника, тъй като при отгатване на пароли с помощта на програми, последните използват думите от речника.
- Парола, която съдържа главни букви на случайно подбрани позиции е трудно разгадаема.
- Паролата трябва да бъде такава, че да може да се помни от потребителя, а не да се записва на хартия, откъдето друго лице би могло да я прочете.
- Колкото дължината на паролата е по-голяма, толкова по-трудно се разгадава, но и по-трудно се помни.
- Паролата трябва периодически да се променя, но не много често, за да може да се помни.

Повечето мрежови операционни системи позволяват на администраторите да задават минималната дължина на паролите, да проследяват тяхната история (съхранява се списък с предишните пароли, като не се допуска тяхното повторно използване) и да задават срокове на валидност на паролите (заставят потребителите да променат паролите си през зададен интервал от време).

Установяването на самоличността на потребителите е важен фактор за сигурността. В последно време се обръща внимание на технологии, които гарантират висока степен на сигурност при идентифициране на потребителите. Към тях могат да бъдат отнесени смарт картите и технологиите, проверяващи биометричните данни на потребителите, като разпознаване на пръстови отпечатъци, сканиране на ретината и разпознаване на ириса на окото, както и верификация на гласа.

Контрол на достъпа

Модерните операционни системи позволяват на множество потребителите да осъществяват достъп до компютрите и мрежата чрез създаване на отделни потребителски акаунти, състоящи се от потребителско име и парола. Акаунтите биват обвързвани с определени права на достъп до ресурсите на мрежата. Например на потребителя може да бъде разрешено да чете и записва само във ресурси, за които има разрешения.

Модерните операционни системи позволяват на администраторите да управляват достъпа до ресурсите гранулирано. Например на един акаунт може да бъде разрешено да разглежда съдържанието на даден файл, но не и да го променя. В същото време на друг акаунт може да бъде разрешено да разглежда, променя и изтрива файла. Позволенията могат да бъдат локални (да касаят ресурсите на само даден компютър от мрежата) или мрежови. Например след логване на потребителя в даден компютър, на него може да му бъде разрешено да има пълен контрол върху файл, намиращ се върху същата машина, но в същото време да бъде забранен достъпът до същия файл, ако той се извършва от друга машина в мрежата.

Във всяка организация, ползваща мрежа, трябва да има изградена политика, в която да бъде указано кой какви права на достъп притежава. Принципът трябва да бъде следния – всеки получава толкова права на достъп, колкото са му необходими, за да може пълноценно да изпълнява служебните си задължения.

С цел облекчаване на администраторите, мрежовите операционни системи позволяват задаване и на групови права на достъп. След като това бъде направено, за всеки член от групата се създава потребителски акаунт, който автоматично получава правата, присвоени на групата. Това е по-лесно отколкото за всеки отделен потребител да се задават едни и същи права на достъп.

Ако енеобходимо даден потребител да бъде лишен от достъп до даден ресурс, не е достъчно да се премахне от неговия акаунт позволението за работа с ресурса. Освен това той не трябва да бъде член на група, която има делегирани права за работа със същия ресурс.

Криптиране на файлове

Криптирането конвертира инфомацията във форма, неразбираема от другите. Извършва се по специални алгоритми с използване на криптографски ключ. Криптирането на файлове криптира информацията, съхранявана на дисковете на компютрите. В този си вид файловете могат да бъдат разглеждани само от потребители, разполагащи с ключа на криптиране.

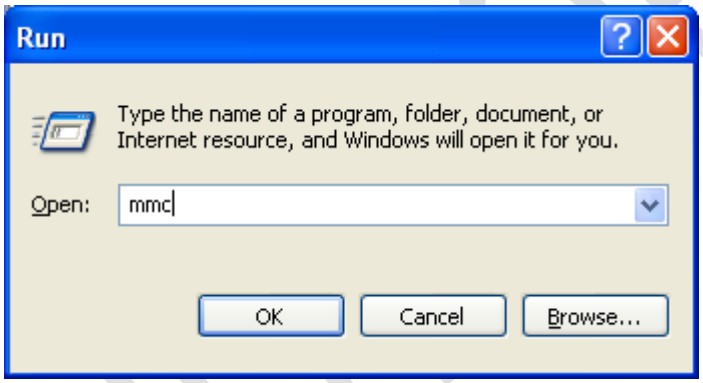
Конфиденциалните данни трябва да бъдат криптирани и защитени с позволения/забрани за достъп.

Някои операционни системи разполагат със собствени средства за криптиране, докато други изискват използване на външни програми за криптипане.

Протоколът IP Security

Криптипрането на файловете защитава данните, съхранявани върху диска, но не предлага сигурност по време на тяхното пътуване по мрежата. Протоколът IP Security (IPSec) решава този проблем на ниво пакет. Той извършва криптирането в мрежовия слой на модела OSI. Cisco Systems използва IPSec в своите маршрутизатори, а Windows включва IPSec в своя TCP/IP стек.

В Windows XP включването на IPSec в действие се осъществява с помощта на програмата ***mmc.exe***, стартирвана от прозореца на командата Start/Run (фиг.9.1).



Фиг.9.1

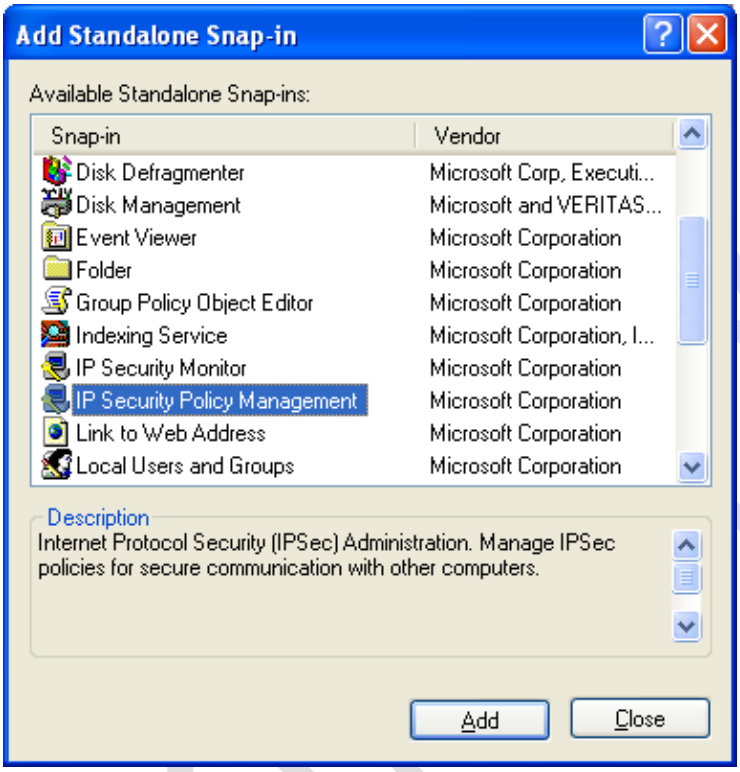
В резултат се отваря прозорец с име „Add/Remove Snap-in", от чието меню File се избира командата Add/Remove Snap-in. В прозореца се щраква бутона [Add], което води до отваряне на прозореца от фиг.9.2. В него се избира елементът IP Security Policy Management и по- нататък се следват инструкциите, извеждани върху екрана.

IPSec използва два протокола, които могат да работят поотделно или заедно:

- ***Authentikation Header*** (AH). Позволява проверка на самоличността на изпращания IPSec.
- ***Encapsulation Security payload*** (ESP). Гарантира конфиденциалността на самите данни.

IPSec може да работи в два режима – транспортен и тунелен. При транспортния криптирането се осъществява по целия път от компютъра източник до компютъра местоназначение. При тунелния режим криптирането се извършва от изходната точка на едната мрежа до входната точка на другата. Освен чрез криптиране, при тунелирането,

както е известно пакетите биват допълнително защитавани и чрез тяхното капсулиране в нови пакети.



Фиг.9.2

Secure Sockets Layer

Secure Sockets Layer (SSL) е друго средство за управление на мрежовата сигурност. SSL използва криптиране с публичен и частен ключ, но има недостатъка, че работи в приложния слой на OSI модела, което налага приложенията да подържат SSL.

SSL бе разработен от Netscape за управление сигурността на техния Web браузър.

Сигурност на електронната поща

Електронната поща прилича на открита пощенска картичка. Тя може да бъде прочетена от всеки по време на нейното пътуване. Съобщенията на електронната поща пътуват през десетки възли (сървъри) и могат лесно да бъдат прехващани. Ако писмото не е криптирано или подписано с цифров подпис, то може лесно да бъде прочетено, копирано или променено.

За осигуряване на електронната поща има разработени много софтуерни продукти, които осигуряват следното:

- не допускат съобщението да бъде прочетено от неоторизирано лице;
- не допускат съобщението да бъде променяно от момента на изпращането му до момента на прочитането му от приемащата страна;
- гарантират, че лицето, което изпраща пощата, е същото, а не някой друг, представящ се за него.

Популярни програми за защита на електронната поща са: Pretty Good Privacy (PGP), Kerberos, Baltimore Mail Secure, MailMarshal на Softec и др. Повечето от тях използват криптиране с ключове и цифрови подписи с цел автентикация на самоличността.

9.1.3 Криптиране на информацията

Криптирането на информацията е предмет на науката криптография, която представлява учение за тайнопис. Криптирането използва код, наричан ключ, с чиято помощ се извършва криптиране (шифриране) и декриптиране (дешифриране) на информацията. За осъществяване на криптирането е необходим и алгоритъм, по който то да бъде извършвано.

Формулата е следната:

Данни + Ключ + Алгоритъм = Криптирани данни

Колкото по-дълъг е ключът за криптиране, толкова по-трудно е разбиването на кода му. Стандартните ключове са с дължина 40 и 56 бита, но има и такива с дължина 128 бита.

За повечето страни криптирането на информацията е предмет на законова уредба. Експортът и импортът на технологиите за криптиране биват контролирани. Например САЩ разрешават свободен експорт на софтуер за криптиране с 40 битови ключове, но забраняват експорта на технологии, използващи 128 битови ключове. В Русия се контролира експорта и импорта и не се допуска използване на неоторизирано криптиране.

Съществуват различни концепции за криптиране, включително такива, използващи повече от един ключ. По-долу са разгледани накратко криптирането със секретен ключ и криптирането с публичен/частен ключ.

Криптиране със секретен ключ

Криптирането със секретен ключ бива наричано още симетрично криптиране, тъй като криптирането и декриптирането се извършват с един и същ ключ. Например нека приемем, че потребителите X и Y желаят да обменят поверителни съобщения, като за

целта използват следната схема на криптиране – всяка буква от азбуката бива конвертирана по схемата A=10, B= 11, C=12 и т.н., след което всяко едно от получените числа се умножава по 4. По този начин лицето X ще кодира съобщението си, като замества навсякъде буквата A с 40, B с 44, C с 48 и т.н. Лицето Y, за да декриптира съобщението, трябва да приложи същия алгоритъм, но в обратен ред – първо да раздели всяко число от съобщението на 4, след което да конвертира получените числа в букви по обратната схема 10=A, 11=B, 12=C и т.н.

Криптирането със секретен ключ изисква решаване на следните три проблема:

- генериране на секретни ключове;
- обмен на ключовете между комуникиращите страни, без те да попаднат в чужди ръце;
- как да се процедира с ключовете, когато комуникиращите страни са повече от две.

Както при паролите и при криптирането е благоразумно секретният ключ да бъде променян през определени интервали от време. Това означава, че трябва да разполагаме със средство за генериране на секретни ключове и с начин за изпращането им до страната, която ще извършва декриптирането. Ако изпратим ключа по електронната поща, съобщението, съдържащо ключа, лесно може да бъде прихванато. Ако криптираме съобщението, получателят няма да може да го декриптира, понеже не разполага с ключа.

За решаване на първите два проблема, свързани с генерирането и с обмена на секретни ключове има разработени специални механизми. Един от тях е например алгоритъмът на Дифи-Хелман. Той позволява на двете страни да създават тайна, известна само на тях, независимо, че комуникират по мрежа без сигурност.

Третият проблем е по-сложен. Когато лицето A комуникира с лицата B и C, то трябва да използва два различни секретни ключа – един за B и един за C. Иначе, при използване на един общ ключ, лицето B ще може да прочита съобщенията за C и обратно. Следователно лицето A трябва да помни два ключа. Когато A трябва да комуникира с по-голям брой лица, генерирането и помненето на повече секретни ключове се превръща в труден и дори неуправляем процес. За преодоляване на този проблем се използва втория вид криптиране с използване на публичен/частен ключ.

Криптиране с публичен/частен ключ

Криптирането с публичен/частен ключ бива наричано още асиметрично криптиране. Тук се използват два ключа – публичен и частен. На всеки публичен ключ отговаря един частен ключ. Публичният ключ е широко достъпен, докато частният се знае само от едно лице. Всяка една от комуникиращите страни притежава двойка ключове - публичен и частен. Те биват използвани по следния начин:

- Лицата А и В решават да комуникират помежду си. За целта те обменят своите публични ключове. Няма значение, че тези ключове могат да попаднат в чужди ръце, тъй като по принцип криптираните съобщения не могат да бъдат декриптирани посредством публични ключове.

- Нека приемем, че лицето А желае да изпрати съобщение на В. Лицето А криптира съобщението с помощта на публичния ключ на лицето В, получен преди това от В.

- Лицето В декриптира полученото съобщение с помощта на своя частен ключ. Това е възможно, тъй като то е било криптирано от лицето А с публичния ключ на лицето В. Публичният ключ на всяко лице съответства на частния ключ на същото лице.

Трябва да се отбележи, че ако лицето А криптира съобщението със своя частен ключ, съобщението може да бъде декриптирано от всеки, който разполага с публичния ключ на А.

В съответствие с описаната по-горе процедура, съобщението, получено от лицето В, ще бъде успешно декриптирано, но лицето В няма да бъде сигурно кой е автора на съобщението, при условие, че публичният ключ на В е бил раздаден на повече лица. Следователно необходима е още и автентикация. Това би могло да стане, ако лицето А криптира съобщението с частния си ключ, а лицето В го декриптира с публичния ключ на лицето А (лицето В разполага с публичния ключ на А).

Друг по-съвършен начин за криптиране и автентикация е използването на цифрови подписи.

9.1.4 Цифрови подписи и сертификати

Цифровите подписи се състоят от криптирана подписваща информация, добавена към изпращания документ. Самите данни в изпращаното съобщение не се криптират. Цифровият подпис гарантира, че изпращачът е автентичен и че данните в документа не са

били променяни, т.е. верифицира се идентичността на изпращача и се проверява автентичността на самия документ.

Верификацията на автентичността на съобщението се извършва с помощта на хеш алгоритъм. Това става по следния начин:

- Изпращачът хешира съобщението с ключ, който е известен на получателя на същото. Хешът изработва числов резултат, например 0111010100000001, наричан дайджест на съобщението. Хеширащите алгоритми изработват дайджести с дължина не по- малка от 128 бита, поради което възникването на един и същ резултат от различни съобщения е практически невъзможно.
- Дайджестът се изпраща на получателя.
- Получателят хешира съобщението със същия ключ и ако съобщението не е било променяно, трябва да се получи същия дайджест 0111010100000001, което ще означава, че документът е автентичен.

Популярни алгоритми за хеширане са: ***Secure Hash Algorithm*** (SHA) и ***Message Digest 5*** (MD5).

Цифрови сертификати

Цифровите сертификати гарантират автентичността на съобщенията, които пътуват по несигурни публични мрежи, каквато е например Интернет. Те представляват съобщения, които съдържат цифровия подпис на трета доверена страна, наричана сертификационна власт (***certificate authority***).

Потребител, който притежава публичен и частен ключ, изпраща до сертифициращата власт заявка за получаване на сертификат. Институцията издава цифров сертификат, който удостоверява, че публичният ключ действително принадлежи на този потребител.

Третата страна представлява оторизирана от държавата институция, която гарантира, че даден публичен ключ принадлежи на конкретно лице. Цифровите сертификати могат да бъдат оприличени на електронни смарт карти за идентификация на личност, каквито са например личните карти, шофьорските книжки и т.п.

Сертификатите са валидни за зададен период от време. Сертификационната власт има право да ги отнема (анулира).

Широко възприет формат на сертификатите е X.509. Той представлява международен стандарт, дефиниран от ITU-T (International Telecommunication Union – Telecommunication [Standartization Sector]).

В България сертификацията е регламентирана със Закона за електронния документ и електронния подпис. Оторизирана сертифициращата организация е ИНФОНОТАРИ ЕАД (www.infonotary.com), дружество създадено през 2004 г. То е част от холдинга Датамакс систем холдинг АД, включващ следните три фирми:

- ePay.bg (www.epay.bg) за електронни плащания;
- Easypay АД (www.easypay.bg) за пощенски парични преводи и платежни услуги Easypay;
- Датамакс АД (www.datamax.bg) за производство на банков софтуер.

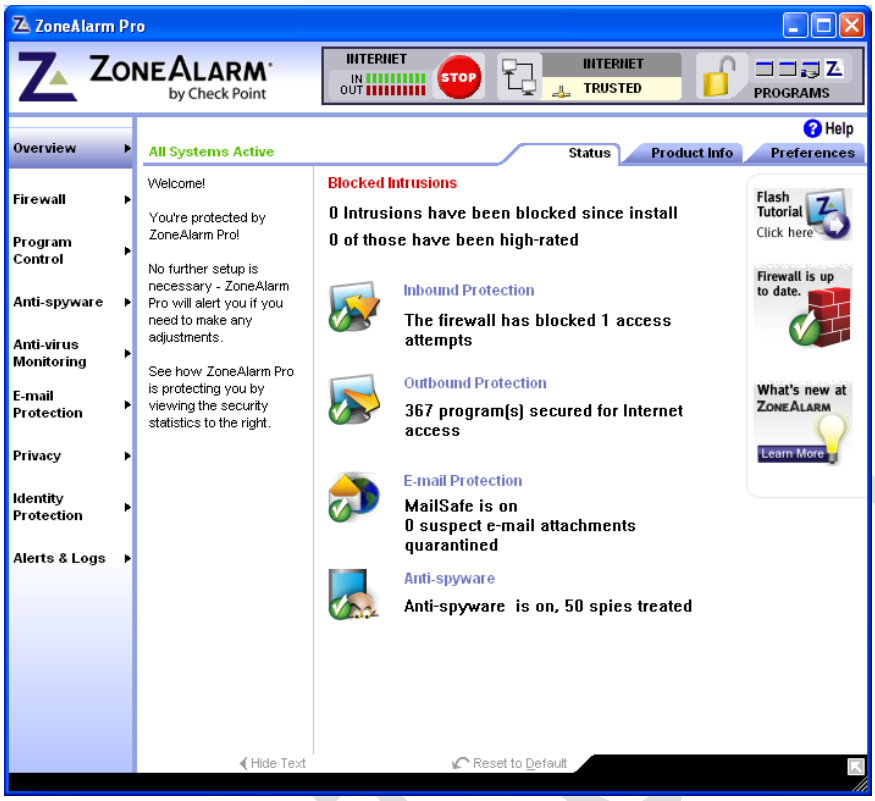
9.1.5 Защитни стени

Защитните стени (firewalls) биват използвани за създаване на бариера между LAN и външния свят.

Те са в състояние да изпълняват три вида филтриране:

- Филтриране на пакети. Извършва се на базата на информацията, съдържаща се в IP, TCP/UDP и ICMP хедърите на пакетите. Защитната стена блокира или разрешава преминаването през нея на указани IP адреси или номера на портове.
- Филтриране на вериги. Ако даден пакет не е част от създадена вече (текуща) връзка, той не се пропуска през защитната стена.
- Филтриране на приложения. Забранява изпълнението на приложения, постъпващи по мрежата, като например Java аплети или друг вид скриптове. Филтрира, като използва информацията за приложенията, съдържаща се в IP пакетите.

Хардуерните защитни стени представляват специализирани компютри, използващи нестандартни операционни системи. Те функционират единствено като защитни стени, поради което притежават по-високо бързодействие от софтуерните защитни стени, изпълнявани на компютри със стандартни операционни системи. Софтуерни защитни стени са например Windows Firewall, ZoneAlarm (фиг.9.3) и др.



Фиг.9.3

ZoneAlarm разделя трафика на три зони – Интернет зона, доверителна зона и блокирана зона. Интернет зоната прави компютъра анонимен и го защитава срещу хакерски атаки, а също така забранява споделянето с външния свят на ресурси, принадлежащи на компютъра. Защитата във втората зона - доверителната зона, допуска комуникация и споделяне на ресурси единствено с доверени (***trusted***) компютри, чийто адреси са били въведени предварителнo в списък (чрез панела Zones на фиг.9.3). Блокираната зона забранява комуникацията с източници, които са отразени като недоверителни (***untrusted***) в същия списък.

Когато в компютъра е инсталиран ZoneAlarm, защитната стена на Windows Firewall трябва да бъде изключена.

Маршрутизаторите и комутаторите от трето ниво биха могли да изпълняват ролята на хардуерни защитни стени. За целта те трябва да бъдат конфигурирани със списъци за контрол на достъпа (***ACL – Access Conrol Lists***), които да забраняват или разрешават на определени машинида извършват комуникация само в една определена посока. Маршрутизаторите, снабдени с ACL списъци, стават „първа линия в отбраната” на мрежите. На втора линия могат да застанат софтуерните защитни стени.

Прокситата изпълняват ролята на посредници между локалните мрежи и външния свят. Тази тяхна позиция им позволява да изпълняват ролята на защитни стени, ако са снабдени с необходимия софтуер.

9.2 Защита и възстановяване от сривове

Както е известно, нарушителите на мрежовата сигурност не са единствената заплаха за мрежите. Възможни са и случайни сривове, предизвикани от хардуерни повреди, природни бедствия или технически грешки в експлоатацията. Всички те водят до загуба на файлове, съдържащи ценна информация. Затова мерките за защита и възстановяване от сривове са важна част на всяка мрежа.

Защитата от тях включва следните мерки:

- аварийно захранване;
- архивиране на данните;
- отказоустойчивост на дисковете;
- отказаустойчивост на ниво сървъри.

9.2.1 Аварийно захранване

Внезапното прекъсване на електрическото захранване на компютрите (поради повреди в електрическата мрежа) може да доведе до загуба на ценни данни. Възможни са също и колебания в подаваното по мрежата електрическо напрежение, които да доведат до същите резултати.

За предпазване от пренапрежения се използват предпазители от пренапрежение, които представляват евтини защитни устройства. Те обаче не предпазват от понижаване или изключване на напрежението. Най-добрият начин срещу отпадане и колебания в напрежението е да се използват специални нескъпи устройства, осигуряващи непрекъсваемо постоянно електрозахранване. Това са така наречените ***UPS*** (Uninterrupted Power Suplay).

UPS представляват батерии, които след отпадане на електрическото захранване, са в състояние да осигурят еквивалентно захранване за определено ограничено време (от 5 до 20 минути). Целта на UPS е не да осигури захранване за продължаване на работата с компютрите, а да даде възможност на персонала да затвори отворените файлове и програми и да изключи компютрите по нормален начин.

UPS стоят включени постоянно в мрежата, а компютрите са включени в UPS. Захранват се от UPS. В един UPS могат да бъдат включвани повече компютри. В нормален режим батерията се зарежда непрекъснато от мрежата. Когато отпадне електрическото захранване, UPS продължава да захранва, като същевременно уведомява за това потребителите, най- често чрез звуков сигнал. В това положение може да бъде използван софтуер, който да изпрати съобщение до административните акаунти в мрежата и да стартира автоматично изключване на свързания към UPS компютър , когато UPS премине в режим на батерия.

Следваща стъпка в защитата от отпадане на захранването е използването на генератори на напрежение. Те позволяват нормална работа с компютрите през цялото време на липса на електрическо захранване от електрическата мрежа. Това са устройства, които генерират напрежение с помощта на двигател, захранван с някакъв вид гориво. Генераторите са скъпо струващи устройства, поради което те биват използвани само в системи, които изпълняват животоспасяващи функции (болнично оборудване в операционните зали) или такива, които не допускат отпадане, например военни инсталации.

9.2.2 Архивиране на данните

При отказ на твърд диск, пожар, наводнение или щети, нанесени от вирус(и), данните могат да бъдат безвъзвратно загубени или да станат нечетими. Ако данните са били архивирани преди това, те лесно могат да бъдат възстановени.

Архивирането се извършва по специален план, изготвен след като се отговори на следните въпроси:

- Какво да се архивира?
- Кога да се извършва архивирането на данните?
- Как да бъде извършвано архивирането?

Изясняването на първия въпрос е важно, защото това определя по-нататъшните ни действия. Идеалният случай е да архивираме всичко, но това никой не прави, тъй като е свързано със загуба на време и изисква значителен капацитет на архивния носител. Например операционната система и файловете на приложенията винаги могат да бъдат повторно инсталирани от дистрибутивните дискове, поради което тяхното архивиране е излишно. На архивиране подлежат важни документи и данни, чието пресъздаване не би

било възможно при една евентуална загуба. Към тях могат да бъдат отнесени документите, които създаваме творчески с помощта на различните приложения, като например: графика, литературни творби, финансова информация и т.н. Желателно е информацията, която ще подлежи на архивиране, да не е разпръсната по твърдите дискове, а да е групирана на едно или две места, за да може бързо да бъде локализирвана.

Друг важен въпрос е колко често да архивираме. Отговорът зависи от това колко данни може да си позволим да загубим – данните, натрупани за един работен ден или например за една седмица. Отговорът на този въпрос определя графика на архивиране.

Съществуват три вида архивиране:

- ***Пълно архивиране***. Данните, които следва да бъдат архивирани, биват винаги цялостно архивирани, независимо от това кога последно са били архивирани и дали от тогава те са били променяни. Пълното архивиране се извършва най просто, но отнема време и отнема повече пространство върху архивния носител.
- ***Диференциално архивиране.*** Архивират се само онези файлове, които са били променяни след пълното им архивиране. В сравнение с пълното архивиране се пести време. Прави се комбинирано с пълното архивиране, например всеки работен ден се извършва диференциално архивиране и един път седмично или месечно пълно такова.
- ***Инкрементално архивиране.*** Архивират се всички файлове, които са били промененни след последното им архивиране, независимо дали то е било пълно или диференцирано. Това е най-бързото архивиране, което обаче изисква повече време при възстановяване на данните.

За да бъдат възстановени данните след проведено диференциално архивиране, необходими са две стъпки – първо да се възстановят данните от последното пълно архивиране и след това промените в тях на базата на последното диференциално архивиране. Диференциалното архивиране се предпочита тогава, когато данните, подлежащи на архивиране, имат голям обем и биха отнемали много време всеки път при тяхното пълно архивиране.

За да бъдат възстановени данните след проведено инкрементално архивиране, необходимо е отначало да бъдат възстановени данните след последното пълно архивиране

и след това промените в тях, настъпвали последователно след всяко тяхно инкрементално архивиране. В този случай архивните копия са повече на брой, например по едно копие за всеки работен ден.

Повечето операционни системи включват помощна програма за архивиране. Например Windows включва програмата Windows Backup, NetWare програмата Sbackup, а UNIX вградената програма ***tar*.**

Съществуват и множество архивиращи програми, предлагани като независими приложения, отделни от операционните системи. По време на архивирането те извършват компресия на данните, което пести място върху носителите на архивни копия. По време на дезархивирането те извършват декомпресия на архивираните данни.

В компресиран вид изпълнимите програми са защитени от вируси, тъй като последните обикновено атакуват некомпресирани програми. От това обаче не следва, че една архивирана програма не съдържа вируси. Ако програмата е била заразена преди компресирането й, вирусът ще остане скрит в нейното архивно копие и при разархивирането й ще стане отново активен. Архивиращите програми по принцип не могат да дезинфектират заразени програми. Затова програмите, които подлежат на архивиране, трябва да бъдат винаги чисти от вируси.

Компресирането на информация съществува като научно направление от 1952 г. То е възникнало и се е развило във връзка с дистанционното предаване на данни по телефонни и други вид канали за комуникация. По-късно научните резултати от тази област намират приложение в компютърната техника, спътниковите системи и др. Днес се предлагат различни конкуриращи се методи за компресия на информацията, което обяснява голямото разнообразие от архивиращи програми, като например: ARJ, ARC, ZIP, RAR, PKLITE, CAB, LHA, LHZ, TAR, ACE,UUE, BZ2, ISO, GZ и др. Онези от тях, които са предназначени да работят под Windows носят представката Win, като например: WinZIP, WinRAR и др.

Много често в практиката биват използвани така наречените саморазархивиращи се архиви. Те биват отбелязвани със съкращението SFX (SelF eXtracing). SFX-архивите съдържат в себе си изпълним програмен модул, който извършва разархивирането. Това не пречи SFX-архивите да бъдат разархивирани по класическия начин чрез съответна архивираща програма като например WinZIP, WinRAR или др.

9.2.3 Отказоустойчивост на дисковете

Един от начините за защита на данните от повреда на твърдите дискове е да се осигури възможност за тяхното самовъзстановяване. Способността на системите да се самовъзстановяват е прието да се нарича отказоустойчивост.

При твърдите дискове отказоустойчивостта се осъществява посредством използване на пакет от взаимно подсигуряващи се дискове. С помощта на относително нескъпи дискове се изгражда структура, известна като ***RAID*** (Redundant Array of Independent Disks).

Най-често използвани варианти на изграждане на RAID са следните:

- ***RAID level 1.*** Дублиране на диск или създаване на копие на диск. Ако единият от дисковете се повреди, другият поема функциите. Това може да става автоматично или като се укаже на операционната система къде се намира втория диск.
- ***RAID level 1***. Дуплескиране на диск. Различава се от дублирането само по това, че всеки един от дисковете се управлява от отделен контролер. Повредата на един от дисковете и/или на контролера му не нарушава функциите на системата.
- ***RAID level 3.*** Лентов запис (страйпинг) с дисково устройство за четност. Изисква минимум три физически устройства – два еднакви диска, на които данните се записват на еднакви ленти и един диск, в който се записва информация за контрол по четност. Ако се повреди даден диск, данните биват регенерирани с помощта на информацията по четност.
- ***RAID level 5.*** Лентов запис (страйпинг) с лента за четност. Както при RAID level 3, използват се три диска. Разликата се състои в това, че информацията за контрол по четност се разполага по друг начин.

Съществуват и структури RAID level 2 и RAID level 4, но те са по-малко използвани. Със така са възможни и комбинации от изграждане на RAID структури. Например RAID10, което означава че първо се извършва RAID1 а след това RAID 0

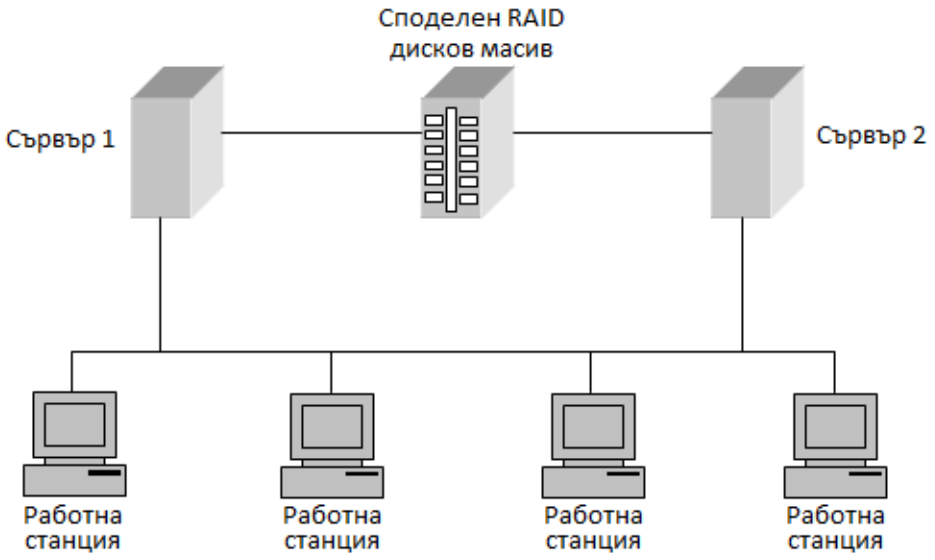
RAID може да бъде реализиран хардуерно или софтуерно. Хардуерният вариант е по- бързодействащ и по-надежден, но и по-скъп. Някои сървърни операционни системи като например Windows NT, Windows 2000 и по-високи версии подържат софтуерен RAID.

В основата на отказоустойчивостта стои излишъкът (редундантността). Използването на UPS, архивирането на данните, използването на множество от

допълнителни дискове представлява създаване на излишък с цел осигуряване на отказоустойчивост.

Друг метод, използващ редунтдантност, е ***клъстерирането***. При него се извършва групиране на сървъри в клъстери. Ако един от сървърите излезе от строя, работата се поема от друг сървър, участващ в клъстъра (фиг.9.4).

Клъстирането се подържа от такива множество операционни системи. Microsoft предлага софтуер за клъстиране на сървъри, работещи с различни операционни системи. Накрая следва да се отбележи, че освен отказоустойчивост клъстирането осигурява и балансирано натоварване на сървърите.



Фиг.9.4

Моля, отговорете на контролните въпроси:

1. *Какви са основните изисквания за повишаване на сигурността в мрежите ?*
2. *Какво представлява понятието UPS?*
3. *Какво представлява асиметричното криптиране?*
4. *Ккакви способи за защита познавате?:*
5. *Кой тип съхранение на данни е по-добър и защо?.*