Безжични компютърни мрежи- Wireless, Bluetooth

Автор: Полина Любчева
Благодарности на: http://www.dhstudio.eu

СЪДЪРЖАНИЕ

Увод

Интернет вече се е превърнал в дума от ежедневието в много държави и е неизменна част от живота на бизнес света. След включването на милионни хора в уеб пространството (World Wide Web), компютърните мрежи достигнаха статуса на телевизорите и микровълновите печки. Закупуването и инсталирането на безжичен концентратор (hub) е не по-сложно от работата с горните устройства. Интернет предлага необичайно високо отражение на медиите, като уеб дневниците често "загребват" истории от източниците на традиционните медии, а средите с виртуалнаа реалност, като пример онлайн игрите, и други подобни се развиха в "Интернет култура".
Разбира се компютърните мрежи отдавна са на сцената. Свързването на компютри, така че да образуват локални мрежи, е обичайна практика дори и при малки инсталации и поради това често връзките на дълги разстояния се правят посредством линиите за пренос, предоставяни от телекомуникационните фирми. Бързото разширяване на конгломерата от мрежи по целият свят, обаче, направи свързването към световното село най-естественото нещо за всеки с достъп до компютър. Създаването на хост с широколентов Интернет достъп, предлагащ бърза електронна поща и уеб достъп , става все по-лесно и достъпно.
Когато става дума за компютърни мрежи, чето става дума за Unix. Разбира се, Unix не е единствената операционна система с възможности за създаване на мрежа, нито пък ще остане лидер завинаги, но той е вбизнеса с мрежите от доста време и със сигурност ще остане още дълго. Това което прави Unix особено интересен за частните потребители е, че се работи здраво , за да се предложат безплатни Unix-подобни операционни системи като NetBSD, FreeBSD и Linux.
Linux е безплатно пазпостраяван клонинг на Unix за лична употреба, който в момента работи на различни машини с процесори от семейството на Intel, но също така на архитектури PowerPC, като Apple Macintosh. Той може да работи и върху машини като Sun SPARC и Ultra-SPARC, Compaq Alpha, MIPS и дори и върху редица конзоли за видео игри, като например Sony PlayStation 2, Nintendo Gamecube и Microsoft Xbox. Освен това, Linux вече е пренесен и върху някои сравнително редки платформи, като Fujitsu AP-1000 и IBM System3/90. Към момента в лабораториите на разработчиците се работи върху преминавания и към други интересни архитектури, а търсенето на начини за преминаването Linux света на вградените (embedded) контролери също изглежда обещаващо. Linux е разработен от огромен екип от доброволци в Интернет. Проектът е започнат през 1990 г. От финландският студент Линус Торвалдс като курсива работа за операционна система. От тогава насетне, Linux лавинообразно се разразна до напълно функционален клонинг на Unix,

който е способен да изпълнява най-различни приложения-програми за симулации и моделиране, текстови редактори, системи за разпознаване на говор, World Wide Web браузъри и купища друг софтоер, в това число и множество игри. Поддържа се голямо разнообразие на хардуер, а Linux съдържа пълна реализация на TCP/IP мрежова функционалност , включително PPP, защитни стени, както и много други възможности и протоколи, които не могат да бъдат открити при никоя друга операционна система. Linux е мощен, бърз и безплатен, а популярността му извън Интернет расте главомолно.
Самата операционна система е защитена от GNU General Public License – същият лиценз, използван от софтуера, разработен от Free Software Foundation. Този лиценз дава възможност на всеки да разпространява и променя софтуера (безплатно или с цел печалба), стига всички промени и дистрибуции също да се разпространяват свободно. Терминът “свободен софтуер” се отнася до свободата на приложение, а не свободата от разходи.

ГЛАВА 1. Компютърни мрежи. Топология. Сигурност.

1.1.История

Идеята за мрежите вероятно е стара, колкото самите комуникации. Нека назад във времето, когато хората са живели в Каменната ера и когато вероятно са се използвали тъпани за предаването на съобщения между хората. Да си представим, че пещерият човек А иска да извика пещерният човек Б да поиграят на хвърляне на камъни един по друг, но те живеят прекалено далече, за да може Б да чуе тъпана на А. Какви са възможностите пред А? Той би могъл 1) да отиде до пещерата на Б, 2) да си вземе по-голям тъпан, или 3) да помоли С, който живее между двамата, да предаде съобщението. Последната възможност се нарича създаване на мрежа.

Разбира се много неща са се променили от примитивните занимания и устройства на нашите предци. В днешно време, компютрите разговарят помежду си чрез огромни съоражения от кабели, оптични влакна, микровълни и други подобни, за да може да може да се осъществи връзката.

Желанието за комуникация с други хора е движеща сила за всички същества, а разработените интелигентни средства за комуникация ни отличават от другите биологически видове. От момента, когато стана възможно свързването на два компютъра и провеждането на разговор между тях, концепцията за развитие на Интернет стана неизбейжна.
В ранните дни на използването на компютрите, те представляваха огромни машини, които изпълняваха цели стаи и струваха ститици хиляди долара. Макар, че те са имали много по-малка мощност на обработка и памет от днешните ръчни компютри, те бяха последен вик на технологиите през 50-те и 60-те години. В свят, в който хората бяха бавни и предразположени към грешки, извършвайки ръчно всички изчисления, възможностите на компютъра бяха поразителни.

В средата на 20-ти век компютрите все още бяха редки, екзотични и мистериозни машини, собственост само на големи компании, държавни и образувателни институции. В по-голямата си част компютрите бяха самостоятелни системи, изолирани една от друга. Никой не е могъл дори да предположи, че персоналните компютри могат да се размножат толкова или че компютърните мрежи ще станат главна насока на развитие.

Мрежата се дефинира като колекция от хостове, които имат възмозност да общуват помежду си, често разчитайки на услугите на редица поставени хостове (dedicated hosts), които препредават данните между участниците в комуникацията. Хостовете най-често са компютри, но това не е задължително. Терминалните и интелигентните принтери

също могат да се считат за хостове. Колекцията от хостове се нарича още сайт (site).

Комуникацията е невъзможна без някакъв вид взаимен език или код. В компютърните мрежи, тези езици имат общо название протоколи. Тук обаче, не става дума за писмени протоколи, а по-скоро за строго официален код за поведение. Протоколите изпозвани в компютърните мрежи не са нищо повече от строги правила за размяна на съобщения между два или повече хоста.

Към средата на 2 век електронните коминикации съществуват вече повече от едно столетие и са реализирани както в Европа така и в Съединените щати. Тези ранни мрежи приемат множество форми и по тях се изпращат само кодирани сигнали. По-късно те получават възможността за предавне на глас по кабела.

- телеграфни кабели

В началото на 19 век французите разработват първата оптическа телеграфна мрежа, която изпраща информация с поразителната скорост от 20 знака за секунда, а Самюъл Морз демонстрира електрически телеграф, които слага началото на разработката на мрежовите комуникации в Съединените щати.

- телефонната мрежа

В края на 19 век започва изграждането на огромна телефонна мрежа. Но тогавашните технологични лидери не са били по-предвидливи от техните наследници от ранната компютърна ера. Едно вътрешно разпореждане в Western Union от 1876 г. твърди, че: “Този “телефон” има прекалено много недостатъци, за да може да бъде възприет като средство за комуникации. Устройството няма никаква стойност за нас”. Независимо от това становище, към 1880 г. в Съединените щати има повече от 50 000 телефонни линии, а към 1960 г. телефонните линии обхващат градските области и телефонната мрежа се превръща в световна комуникационна мрежа.

Телефонната система използва технологии с комутиране на електрически вериги, при която се изгражда верига или виртуална пътека при всяко свързване на един телефон с друг по мрежата. Тази технология е подходяща за предаване на глас, защото звуците се пренасят по кабела с относително постоянна скорост.

През 60 години правителството на Съединените щати се заинтересува от разработването на компютърна мрежа, която би позволила на военние системи и на системите на главните образувателни институции да комуникират едни с други. Тъй като това става в разгара на Студената война, те искат мрежата да притежава устойчевост, надежност и достатъчен резерв, така че да може да оцелее пи възможна ядрена война. Изследователте от Масачузетскят технологичен институт, нститута RAND

и Националната физична лаборатория във Великобртания изобретяват нова технология, наречена комутиране на пакети (packet switching), които при перидични пикови предавания работи по добре, отколкото традиционните технологии с комутиране на вериги. Тяхната работа полага основата на комуникационните тхнологии, изолвани в днешният Интернет.
Терминът комутиране на верихи и комутиране на пакети звучат близко, но имат различно значение.

Обществената телефонна система, означявана понякога с POTS, представлява комуникационна мрежа с комутиране на вериги. Когато провеждате телефонен разговор в този тип мрежа, за цялото време на този разговор се използва само една физическа пътека от вашият телефон до телефона, които сте избрали. Тази пътека или верига се поддържа изкчително за ваше ползване до момента, до момента когато прекъснете връзката, поставяйки телефонната слушалка обратно на мястото и.
При мрежа с комутиране на пакети не се изгражда специална пътека или верига. Комутирането на пъкети понякога се означява като технология без установяване на конекции, поради липса на специално изградена пътека.
Началото на първата компютърна мрежа с комутиране на пакети е поставено в края на 60 годинипод покровителството на Министерството на отбраната на САЩ. Тя е наречена ARPnet. Първият възел или точка на свързване, към ARPnet е инсталран в Калифорнийският университет в Лос Анджелес през 1969 г. Само за три години мрежата се разпростира през целите Съединени щати, а две години след това достига до Европа.
С нарастването на мрежата тя бива разделена на две части. Воените наричат своята част от интернет мрежата Milnet, а ARPnet продължява да бъде използвана за описание на частта от мрежата, която свързва изследователсските и университетските сайтове. През 80 години ARPnet е заменена от мрежата Defense Data Network и NSFNet. В последствие тази WAN мрежа се разраства в това, което днес наричаме Интернет.

Изграждането на компютърните мрежи не започва от такъв голям мащаб като проекта ARPnet, т.е. локалните мрежи се появяват преди WAN. С поевтиняването на компютрите и с увеличяването на тяхната мощност, търговските организации от всички мащаби започнаха да ги използват все по масово. Първите машини можеха да се използват само за ограничени видове обработка на данни, но с процъфтяването на разработката на софтуер новите програми позволиха на потребителите да правят повече от простото сортиране и събиране на данни.

Използването на мейнфрейм компютри вършеше добра работа в много отношения, но те имаханяколко минуса в сравнение с по-малките компютри. Недостатък беше тяхната висока цена, големите мейнфрейм системи струваха много повече от така наречените “персонални” компютри, проектирани така, че да бъдат поставени на бюрото и да функционират самостоятелно.

Друг недостатък на мейнфрейм комтрите беше концепцията за единствена точка на отказ. При работата с мейнфрейм комютър, ако компютъра бъде изключен, той е изключен за всички. От друга страна, използването на отделни персонални компютри разрешава този проблем. Персоналните компютри представляват компютри, разработени като напълно функционални единици, които изпълняваха програми и извършваха работни задания напълно самостоятелно. Те осигуряваха известна отказоустойчивост – способността на системата да продължява да функционира и да осигурява цялост на данните при възникване на провреди. Ако компютърът на един служител прекъсне работа, той не влияе на възможността на останалите служители, които имат собствени персонални компютри да продължят работата.

Тези фактори допринесоха за нарастване популярността на персоналните компютри като решение за малки, средни и големи търговски организации. Но след като всеки се сдоби с отделем компютър на бюрото си, компаниите се изправиха пред дилема как работниците да използват съвместно информацията. Решението беше изграждането и работата в мрежа.

По-рано споменахме телеграфните и телефонните мрежии, разбирасе, всички сме чували за телевизионните мрежи. Можем да наречем мрежа дори пътищата и железопътните линии, които пресичат страната. Като имамеме всичко това в предвид какво всъщност представлява една компютърна мрежа? Просто казано това са две или повече устройства, сързани с цел общо използване на информацията, ресурси или и двете. Връзката може да бъде чрез кабел или може да бъде безжична връзка, която използва радиовълни, лазерна или инфрачервена технология, или сателитно предаване. Споделената обща информация и ресурси могат да бъдат файлове с данни, приложни програми, принтери, модеми, скенери или други хардуерни устройства.

Тази фигура показва значимите събития в историятана мрежите от персонални компютри:

Фиг. 1.1

1.2. Категоризация на мрежите

Специалистите по технологии разделят мрежите на категории на базата на характеристиките, необходими за администрирането или отстраняването на неизправности на конкретната мрежа. Можете да квалифицирате типовете мрежи в зависимост от физическите свойства или характеристиките на софтуера, който се изпълнява на тях. Например категоризацията може да бъде базирана на следните характеристики:

- физически обхват
- метод на администратиране
- мрежова операционна система
- мрежови протоколи
- топология
- архитектура

1.3. Категоризация на мрежите според физически обхват

Един от методите за категоризация на мрежите е базиран на

физическият обхват, който включва географската област, която се обхеваща от мрежата, ив по-малка степен размера на мрежата. Използвайки този метод можем да квалифицираме дадена мрежа в една от следните три категории:

- Локална мрежа (LAN)
- Градска мрежа (MAN)
- Глобална мрежа (WAN)

Тези категоризации са свързани донякъде с размера на мрежата, представляващ броя на компютрите и потребителите (обикновенно LAN са по-малки от MAN, които от своя страна са по-малки от WAN). Те са свързани също до известна степен с финансовите ресурси (изобщо WAN е много по-скъпа за инсталиране и поддръжка от LAN), но най-важният определящ фактор е географската област, която мрежата покрива.

1.3.1. Характеристики на LAN мрежата

Речникът American Heritage Dictionary дефинира думата local като “свързан с или характерен за конкретно място, а не за по-голяма област”. Подобно на това терминът LAN описва мрежа, която обхваща ограничена област, компютрите принадлежащи към мрежата във физическа близост един до друг. Но LAN мрежите могат да варират драстично по броя на компютрите и потребителите. Например една локална мрежа може да се състои от два компютъра, разположени на разтояние няколко метра в офиса или в къщи, или да включва стотици компютри, обхващайки няколко етажа от небостъргач, или в някой случаи дори множество сгради, разположени близо една до друга. LAN мрежата е ограничена до конкретна географска област.

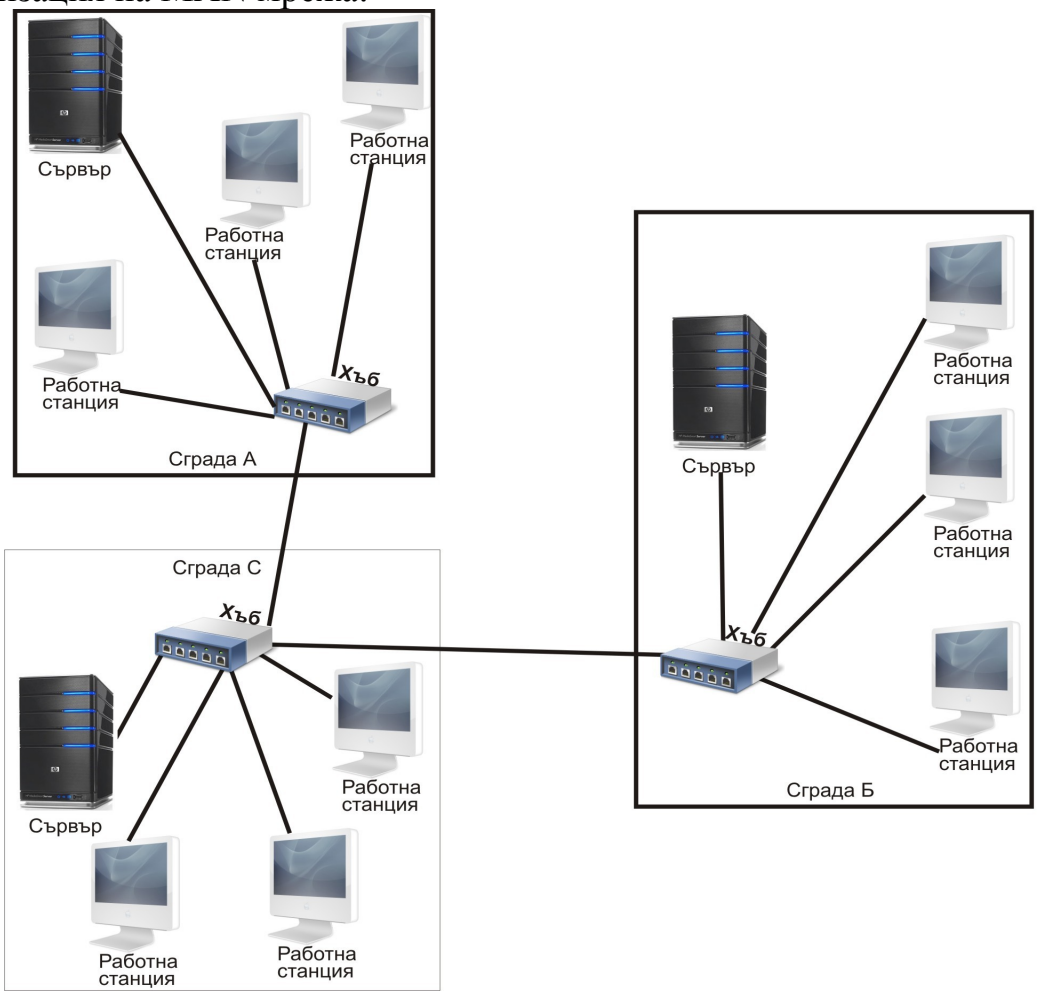
Визуализация на проста локална мрежа:

Фиг. 1.2

1.3.2. Характеристики на MAN мрежата

Както подсказва самото име, градската мрежа се състои от две или повече LAN мрежи, свързани в границите на пространство, което заема приблизително един голям град. Типичната MAN е високопроизводителна обществена мрежа. Терминът MAN се използва по-рядко за дефиниране на мрежи, отколкото термините LAN и WAN, защото градските мрежи се реализират много по-рядко. Повечето мрежи са в рамките на сграда или комплекс от сгради (например университетски комплекс) и поради това попадат в категорията на LAN, или пък обхващат по-големи разстояния с възли, разположени в различни градове, щати й дори държави, като по този начин могат да бъдат квалифицирани като WAN мрежи. Максималното разстояние, дефиниращо една MAN мрежа, е приблизително 80 км. MAN мрежата покрива по-обширна област от LAN, но е географски по-ограничена от WAN.

Визуализация на MAN мрежа:



Фиг. 1.3

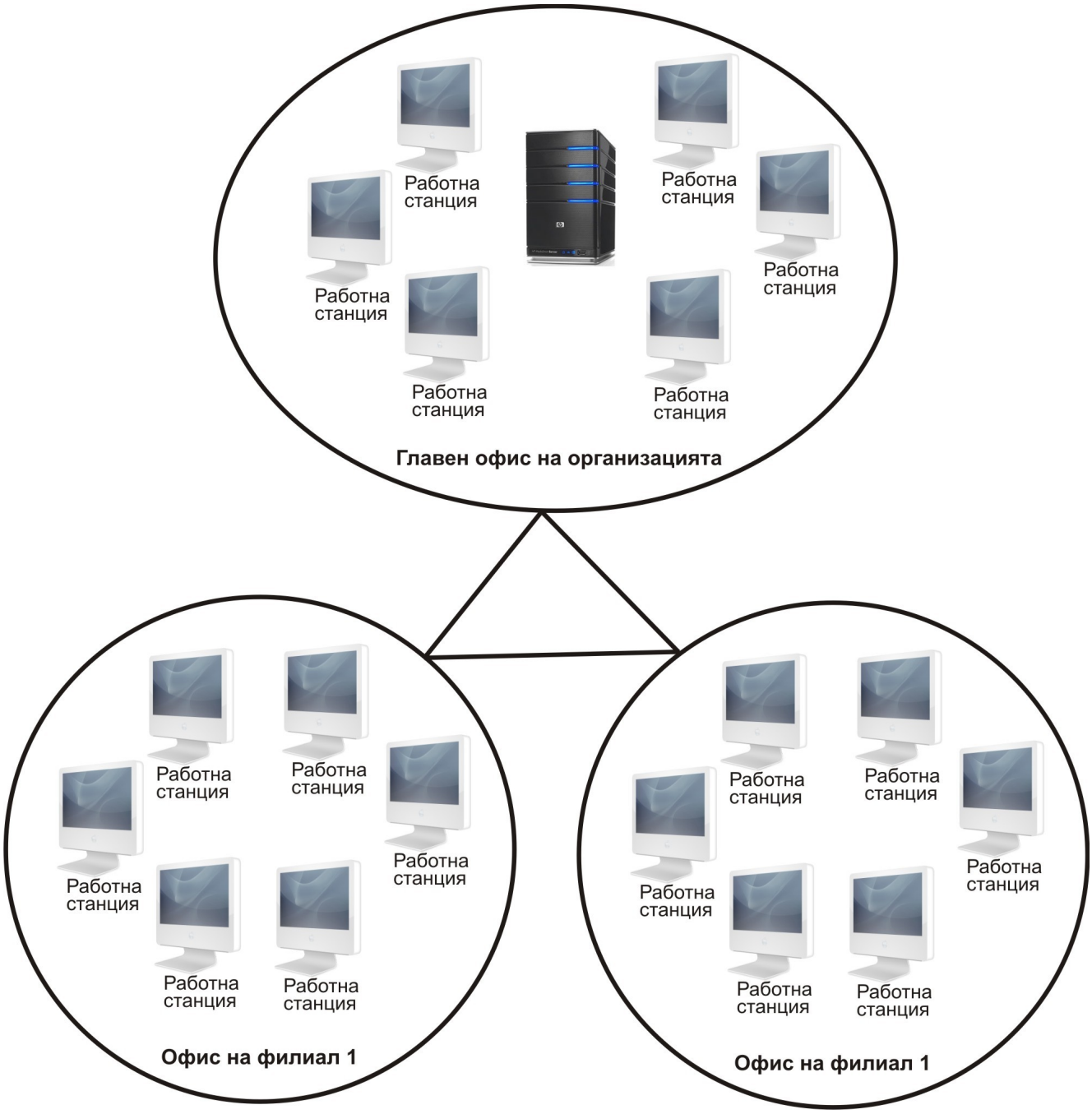
1.3.3 Характеристики на WAN мрежата

WAN представлява мрежа, която обхваща голяма географска област. Най-добрият и най-популярният пример за WAN е Интернет. Но WAN може да бъде и частна мрежа. Например организация с офиси в много страни може да има корпоративна WAN мрежа, свързваща отделните местоположения посредством телефонни линии, сателити или други технологии. Глобалната мрежа най-общо се състои от множество взаимосвързани локални мрежи. Резултатът от свързването на мрежите една с друга се означава като интермрежа, или интернет. Когато видите думата интернет, започваща с малка буква, това означава произволна мрежа от мрежи. Когато първата буква е главна, думата означава глобалната обществена мрежа от мрежи, която наричаме Интернет. Свързаните термини, произхождащи от термина интернет, са интранет и екстранет. Мрежата, наречена интранет, представлява частна мрежа в рамките на дадена организация, която използва едни и същи протоколи (например TCP, HTTP и FTP) и технологии, използвани по Интранет. Мрежата, наречена екст-ранет, също използва Интернет технологии, но достъпът до нея се осъществява по отдалечени връзки към клиенти, служители, разпространители и партньори ш дадена бизнес организация. Макар че WAN мрежите могат да използват и частни връзки за свързване на отделните мрежи, често те използват обществените среди за пренос, например обществената телефонна система. Следователно скоростта на предаване често е по-малка от тази на LAN мрежите; типичната скорост по аналогови телефонни линии със съвременен бърз модем е 50 kbps или по-малко. Дори високоскоростните WAN връзки, като например T1, връзките с кабелен модем и DSL линиите, притежават скорости в обхвата от 1 до 6 Mbps. От друга страна най-бавните й Ethernet LAN връзки имат скорост 10 Mbps.

Друга характеристика на WAN е, че връзката към тях може да не се установява с помощта на постоянно свързване по кабел, както при кабелните LAN мрежи. Вместо това WAN връзките често, но не винаги, се установяват „при необходимост". Много WAN връзки всъщност са специално изградени и са постоянно включени, но въпреки това временните връзки са много по-често срещани, отколкото при LAN.
В обобщение, WAN мрежите могат да използват частни или обществени преносни среди и могат да се състоят от постоянно изградени връзки или dial-up конекции (установявани при необходимост). WAN връзките обикновено са по-бавни в сравнение с LAN връзките. WAN мрежите се разделят на разпределени или централизирани. Разпределените WAN, например Интернет, нямат централна точка. От друга страна, централизираните WAN са базирани на централен сървър или

централизирано място (например главния офис на организация), към което се свързват всички други компютри.

Визуализация на централизирана WAN мрежа:



Фиг. 1.4

WAN мрежите са маршрутизирани мрежи, което означава, че за да могат съобщенията да преминават от една LAN мрежа в друга, пакетите трябва да преминават през шлюз (gateway). Шлюзът представлява маршрутизатор

(router) -компютър, конфигуриран за изпълнение на маршрутизиращи функции.

1.4. Категоризация на мрежите по метод на администриране

Можете да категоризирате мрежите на базата на метода на тяхното администриране, т.е. как и от кого се управляват ресурсите. Мрелсата може да бъде организирана както следва:

• Като равноправна (peer to peer) работна група, в която всеки компютър функционира и като клиент, и като сървър, и всеки потребител администрира ресурсите на своя компютър.

• Като клиент/сървър или сървърно базирана мрежа, в която администрирането е централизирано на компютър, работещ със специален сървърен софтуер и мрежова операционна система (NOS). Този компютър автентицира информацията за името на потребителя и паролата, за да позволи на оторизираните потребители да влизат в мрежата и да осъществяват достъп до ресурсите.

Табл. 1.1.

Предимства на равноправната мрежа	**Предимства на мрежата клиент/сървър**
По-евтина за реализация.	Предоставят по-добра сигурност.
Не изисква NOS сървърен софтуер.	По-лесни за администриране, когато мрежата е по-голяма, защото администрирането е централно.
Не изисква специално назначен мрежов администратор.	Всички данни могат да бъдат архивирани в едно централно място.
Недостатъци на равноправната мрежа	**Недостатъци на мрежата клиент/сървър**
Не можа да бъде мащабирана добре за разрастване до големи мрежи; администриране на мрежата.	Изисква скъп NOS софтуер, например Windows 2000 Server или пък NT.
Всеки потребител трябва да бъде обучаван да изпълнява задачи по администриране на мрежата.	Изисква скъп, но мощен хардуер за сървърна машина.
По-несигурна е.	Изисква професионален администратор.
Всички машини, обменящи ресурси, влияят отрицателни на производителността.	Има само една точка на достъп, ако има един единствен сървър, данните на потребителите могат да станат недостъпни ако сървърът спре да работи.

1.5. Категоризиране на мрежите по топология

В някои случаи мрежите биват категоризирани на базата на физическата или логическата топология на мрежата. Физическата топология означава формата на мрежата - начинът, по който се разполага кабелът. Логическата топология означава пътя, по който пътуват сигналите от една точка на мрежата до друга.

Физическата и логическата топология може да бъде една и съща; в мрежа, физически оформена като линейна шина (т.е. в права линия), данните пътуват в права линия от един компютър към следващия. Мрежата може да има също различна физическа и логическа топология. Кабелните сегменти могат да свързват всички компютри към централен хъб във формата на звезда, но вътре в хъба връзките да бъдат свързвани така, че сигналът да пътува в окръжност от , един порт към следващия, създавайки логически кръг.

Ето най-популярните LAN топологии за мрежи:

• Линейна шина

• Кръг

• Звезда

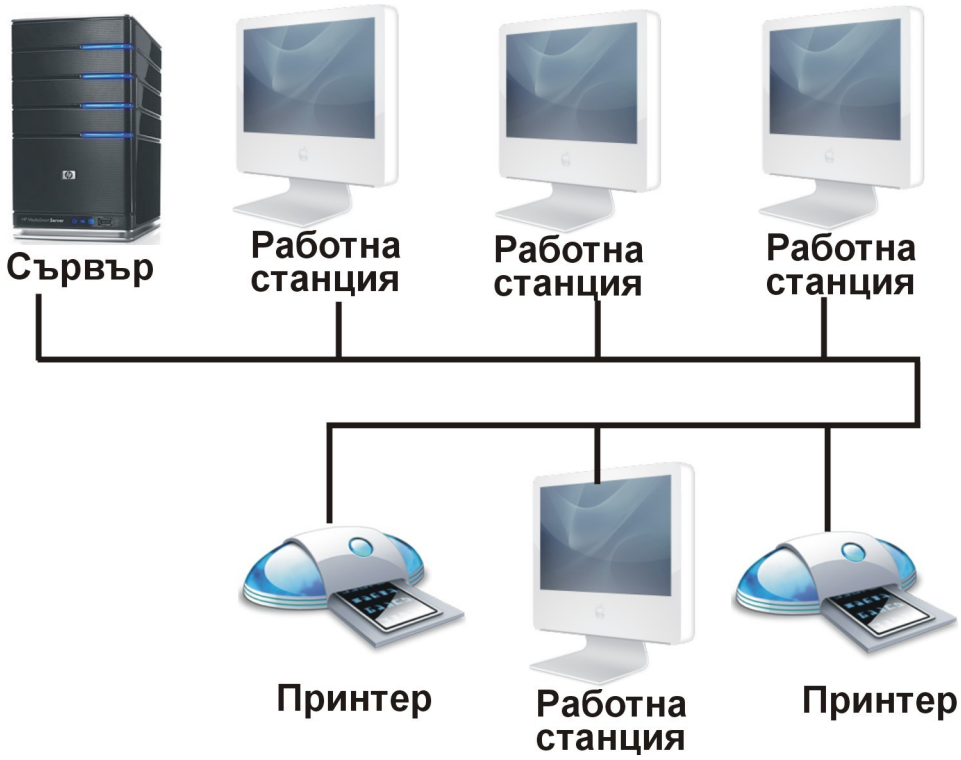
• Решетка

• Хибридна

1.5.1.Мрежи с линейна шина

Както показва самото име, линейната шина (понякога наричана просто шина) представлява мрежа, която е разположена в права линия. Реално линията не е задължително да бъде права, просто кабелът преминава от един компютър към следващия, след това към следващия и т. н.

Визуализация на линейна шина:



Фиг. 1.5

Тъй като има начало и край, мрежата с линейна шинна топология изисква терминиране на всеки край. Ако не бъдат терминирани и двата края на кабела, възниква отразен сигнал, който може да наруши или да прекъсне комуникацитите по мрежата. Единият от краищата на линейната шина - но не и двата -трябва да бъде заземен.

Към края на шината, на първия и последния компютър, свързани към линейния кабел, към „празната" страна на Т-конектора на мрежовата интерфейсна карта се свързва устройство, наречено терминатор. Шинните мрежи обикновено използват дебел или тънък коаксиален кабел и архитектура Ethernet 10Base2 или 10BaseS.

По шинната мрежа, когато един компютър изпрати съобщение, това съобщение отива до всеки компютър в мрежата. Всяка мрежова интерфейсна карта (NIC) проверява хедъра на съобщението, за да определи дали то е адресирано за този компютър. Ако не е, съобщението бива игнорирано.

Шинната топология е много проста и лесна за инсталиране. Тя е относително евтина и използва по-малко кабел в сравнение с други топологии. Шината е особено подходяща за малки, временни мрежи, например такива в класни стаи, които може да бъдат използвани само няколко дни или седмици.

Шината е известна като пасивна топология, защото компютрите не регенерират сигнала и не го предават нататък, както правят това в кръга. Това прави мрежата уязвима към затихване, представляващо загуба на силата на сигнала с увеличаване на разстоянието. За решаване на този проблем могат да бъдат използвани повторители.

Друг недостатък на шината е, че при прекъсване на кабела (или ако някой потребител реши да разкачи своя компютър от мрежата) линията се прекъсва. Това означава, че компютрите от двете стани на прекъсването не само не могат да комуникират, но също, че двата нови края не са терминирани и резултатният отразен сигнал може да срине цялата мрежа

1.5.2. Кръгови мрежи

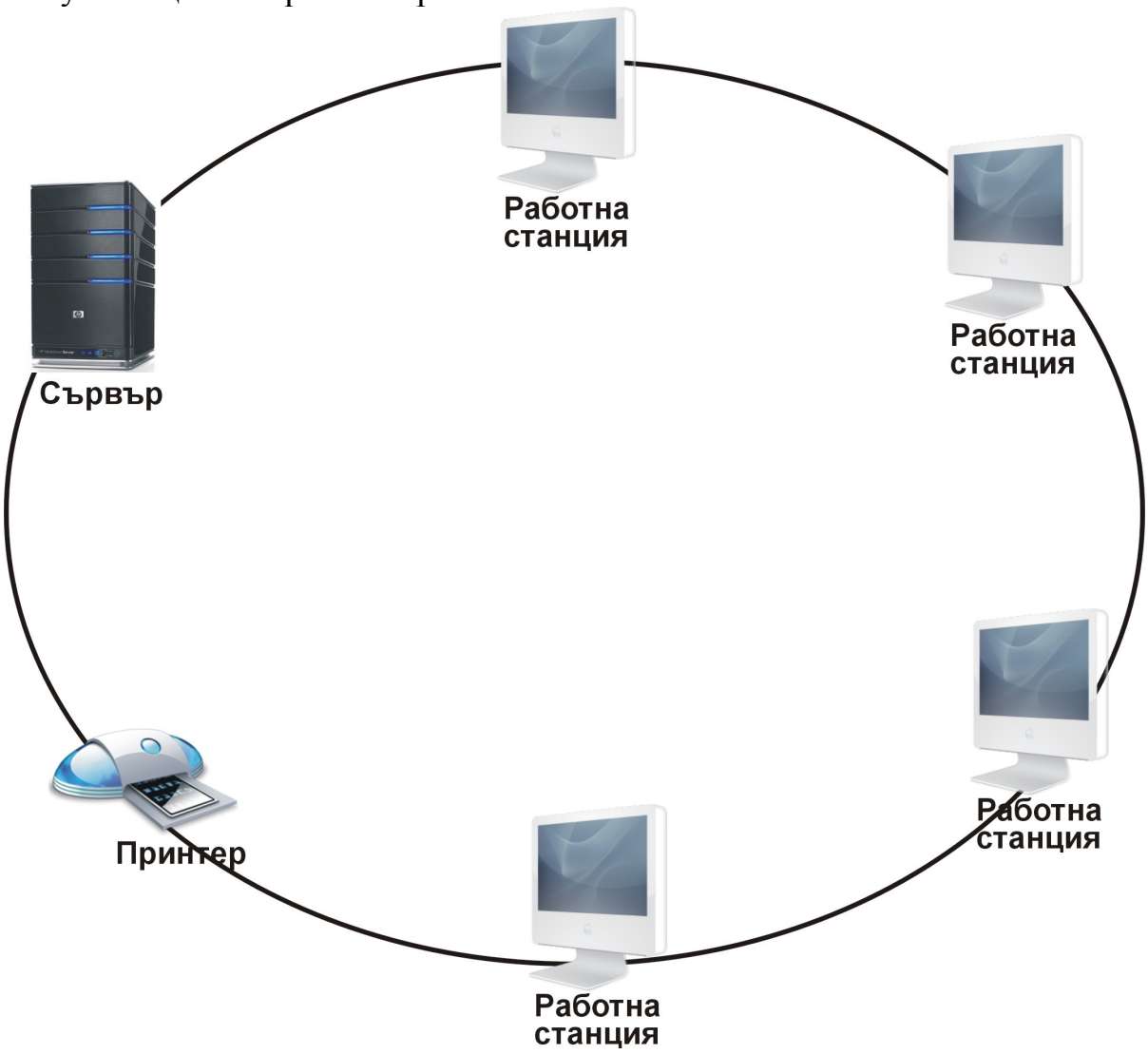
Ако свържете последния компютър в шината обратно към първия, получавате кръгова топология. В кръга всеки компютър се свързва към два други компютъра, а сигналът може да обикаля непрекъснато в кръга. Тъй като кръгът няма крайна точка, не е необходимо (или възможно) терминиране.

За изграждане на мрежа с физически кръг най-общо се използва коаксиален кабел, както при шината. Мрежата Token Ring, която представлява логически кръг, използва STP кабел (тип IBM) и отговаря на спецификациите IEEE 802.5.

По кръгова мрежа сигналът пътува в една посока. Всеки компютър приема сигнала от своя възходящ съсед (upstream neighbor*)* и го изпраща на своя низходящ съсед (downstream neighbor). Кръгът се счита за активна топология, защото всеки компютър регенерира сигнала, преди да го предаде към следващия.

Кръговата топология най-често се асоциира с архитектурата Token Ring. В тази реализация кръгът най-общо е логически - като окръжността се свързва вътре в Token Ring хъб, който се нарича модул за достъп до мнолсество станции (multistation access unit - MSAU). В кръгова мрежа компютрите се свързват към кръг, като последният компютър се свързва обратно към първия.

Визуализация на кръгова мрежа:



Фиг. 1.6

Кръгът е сравнително лесен за отстраняване на неизправности и подобно на шината е прост за инсталиране. Физическият кръг изисква повече кабел от шинта и по-малко от топологията тип звезда.

Кръгът страда от някои от същите недостатъци като шината. Ако се запази непрекъснат, кръгът е надеждна топология. Но ако някъде по мрежата възникне прекъсване или изключване от кабела, това води до прекъсване на всички мрежови комуникации.

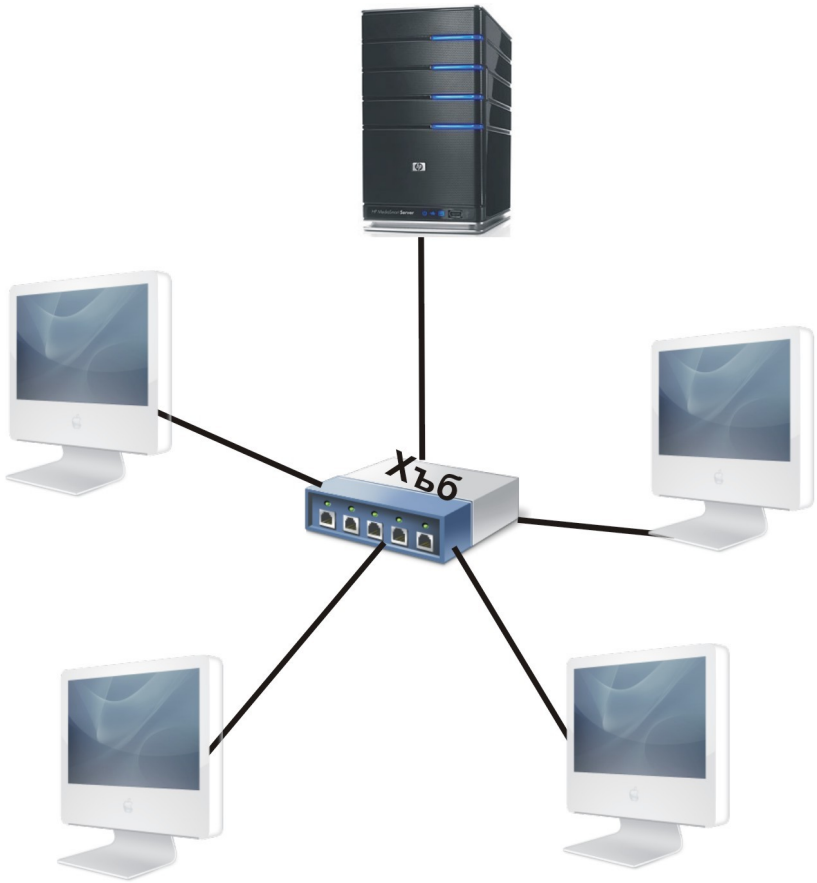
Друг недостатък на кръга е трудното добавяне на допълнителни компютри към мрежата. Тъй като кабелът описва затворен кръг, е необходимо кръгът да бъде прекъснат в някоя точка, за да бъдат вмъкнати

новите компютри. Това означава, че докато трае добавянето, мрежата не функционира.

1.5.3. Мрежаиот тип звезда

Звездата (star) е една от най-популярните LAN топологии. Тя се реализира чрез свързване на всеки компютър към централен хъб. Хъбът може да бъде активен, пасивен или интелигентен. Пасивният хъб е просто точка на свързване. Той не изисква електрическо захранване. Активният хъб (най-разпространеният тип) реално представлява повторител с множеството портове; той усилва сигнала, преди да го предаде към другите компютри. Интелигентният хъб представлява активен хъб с диагностични възможности. Той има вграден процесорен чип. Топологията тип звезда свързва всички компютри към един централен хъб.

Визуализация на топология тип звезда мрежа:



Фиг. 1.7

Звездообразната топология най-общо се използва с кабел тип неекранирана усукана двойка (UTP) и Ethernet архитектура 10BaseT или 100BaseT.

При типична мрежа от тип звезда сигналът се предава от мрежовата интерфейсна карта на изпращащия компютър към хъба, повишава се (т.е. усилва се) и се изпраща обратно през всички портове. При звездата, подобно на шината, всички компютри приемат съобщението, но само компютърът, чийто адрес отговаря на адреса на местоназначението в хедъра на съобщението, му обръща внимание.

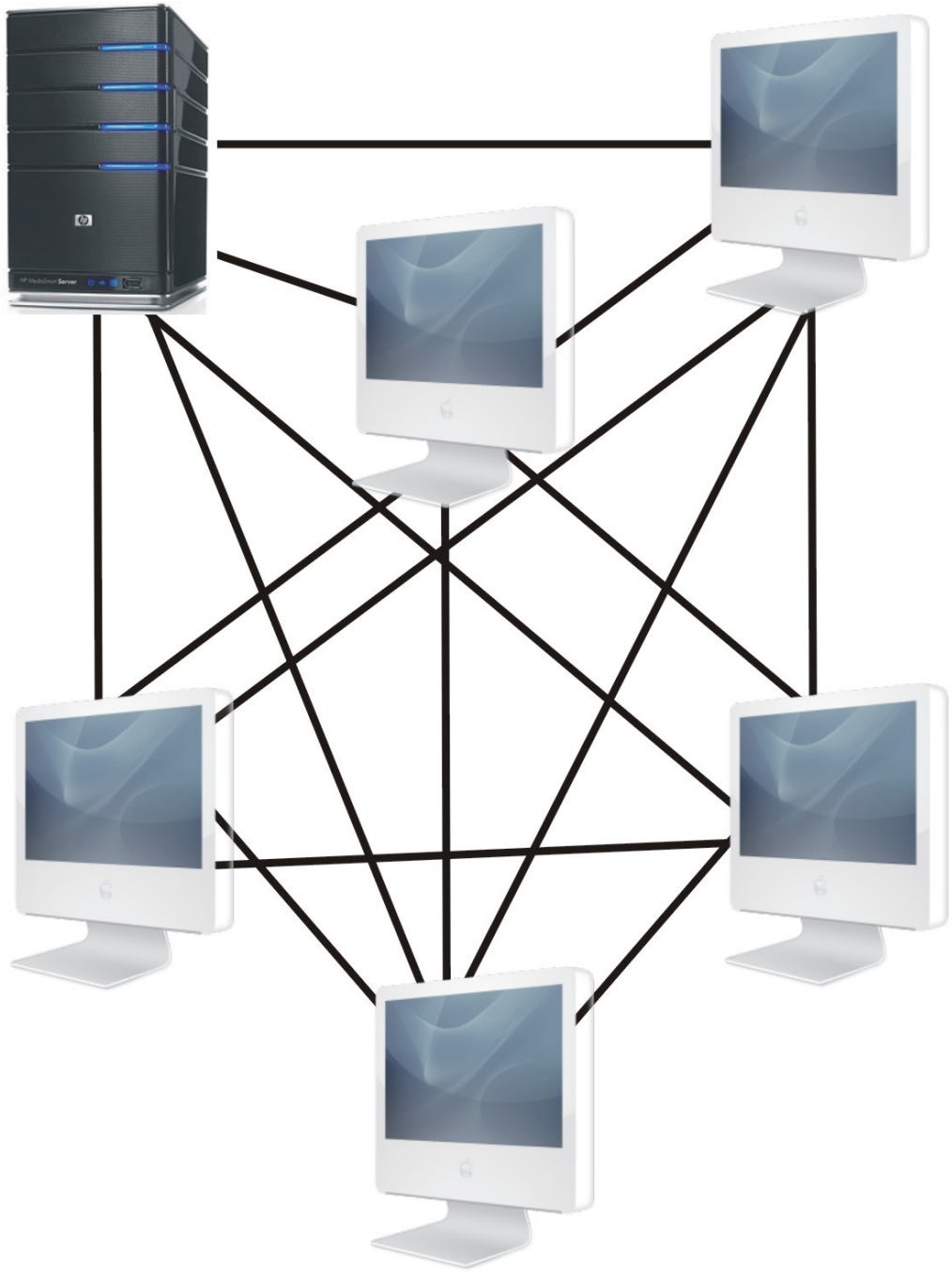
Топологията тип звезда има две големи предимства пред шината и кръга. Първо, тя е много по-отказоустойчива (fault tolerant), т.е. ако един компютър бъде изключен или неговият кабел бъде прекъснат, само този компютър бива засегнат, а останалата част от мрежата може да продължи да комуникира нормално. Второ, тя предлага възможност за лесно преконфигуриране. Добавянето на още компютри към мрежата или премахването на компютри е много просто, защото се състои само във включване или изключване на техния кабел в хъба. Отстраняването на проблеми на физическия слой в мрежата от тип звезда също е лес-но, особено при наличие на интелигентен хъб, който осигурява диагностична информация.

Независимо от предимствата на звездата, тя има и няколко недостатъка, свързани главно с нейната цена. Първо, тя използва повече кабел, отколкото линейната шина или кръга, защото трябва да има отделен кабел от хъба до всеки компютър. Друг източник на допълнително оскъпяване е самият хъб, който трябва да бъде закупен наред с кабела. Все пак малък плюс при мрежите от тип звезда е, че UTP кабелът е сравнително евтин и няма нужда от терминатори.

1.5.4. Решетъчни мрежи

Решетката (mesh) представлява топология, която не може да видите толкова често, колкото трите топологии, разгледани дотук. В решетъчната мрежа всеки компютър има директна връзка към всеки друг компютър в мрежата, както е показано на следващата фигура.
В решетъчната мрежа всеки компютър е свързан към всеки друг компютър.

Визуализация на решетъчна мрежа:



Фиг. 1.8

Тези допълнителни конекции правят решетката най-отказоустойчива от всички останали топологии. Ако пропадне един от пътищата от изпращащия компютър към компютъра-местоназначение, сигналът може да поеме по друг път.

За нещастие, това предимство става за сметка на високата цена и огромното количество кабел, необходим за реализиране на решетка и сложността на мрежата, ако в нея влизат повече от няколко компютъра. Броят на конекциите нараства експоненциално при добавяне на всеки нов компютър. Не е случайно, че „mesh" (решетка) звучи подобно на „mess" (бъркотия) - точно това получавате при нарастването на решетъчната мрежа.

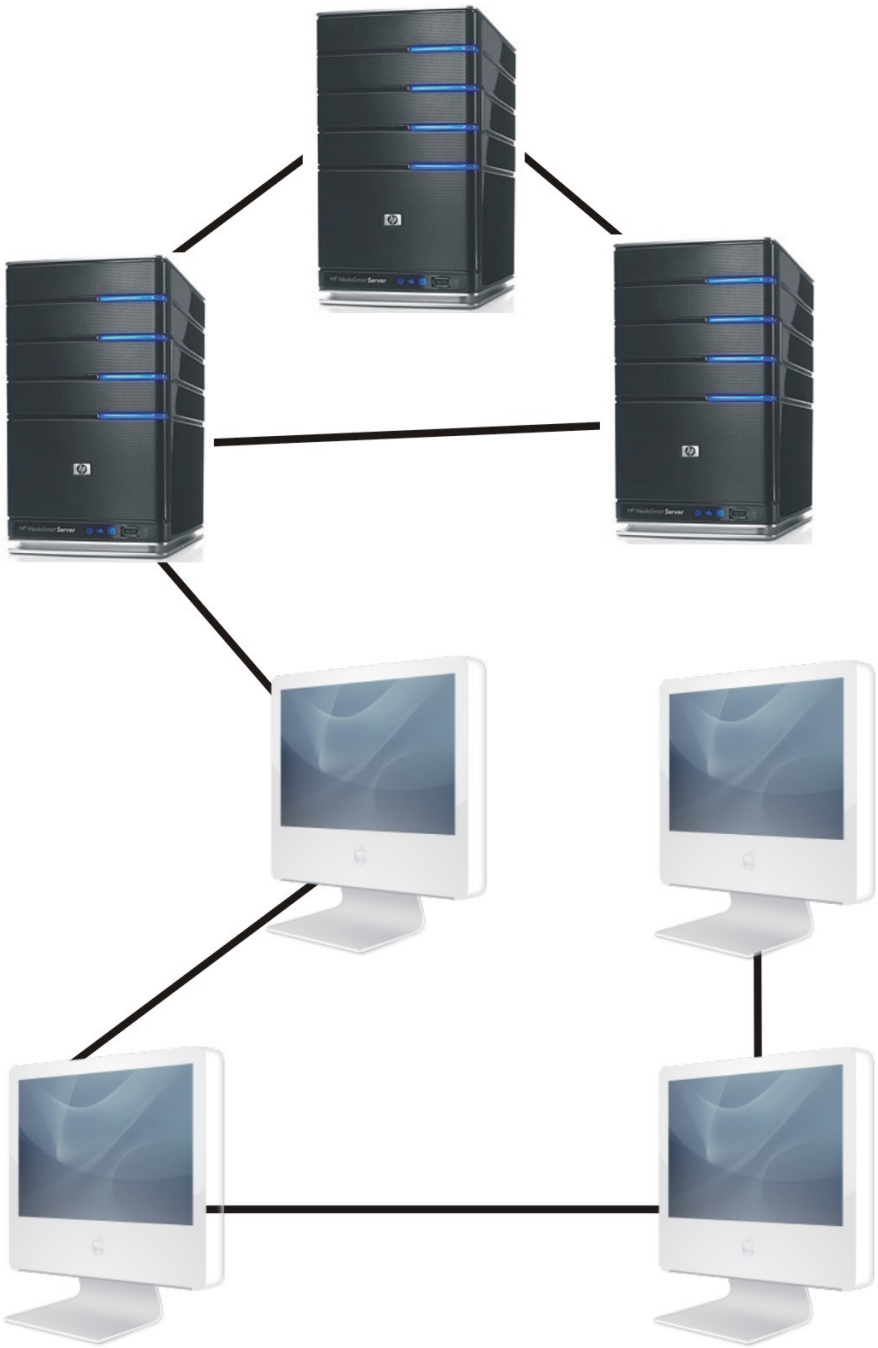
1.5.5. Хибридни топологии

Думата хибрид се използва в два различни смисъла за означаване на мрежова топология. Думата се използва за означаване на топология, която комбинира елементи на две или повече стандартни топологии (например хибридна решетка, звезда или кръг).

Тъй като решетъчната топология бързо става сложна и неуправляема при нарастване, много мрежи се базират на полурешетъчна топология, при която има допълнителни връзки между някои от компютрите, но не между всички; този тип мрежа често се означава като хибридна решетка. Допълнителните връзки , трябва да бъдат създадени между компютрите, които имат най-голяма нужда от отказоустойчивост на връзката.

В хибридната решетка се осигуряват допълнителни връзки между някои компютри, но не между всички. Хибридната решетка осигурява много повече предимства от обикновената решетката при по-ниска цена и е по-лесна за инсталиране и управление. В хибридната решетка се осигурява допълнителни връзки между някои компютри, но не между всички.

Визуализация на решетъчна мрежа:



Фиг. 1.9

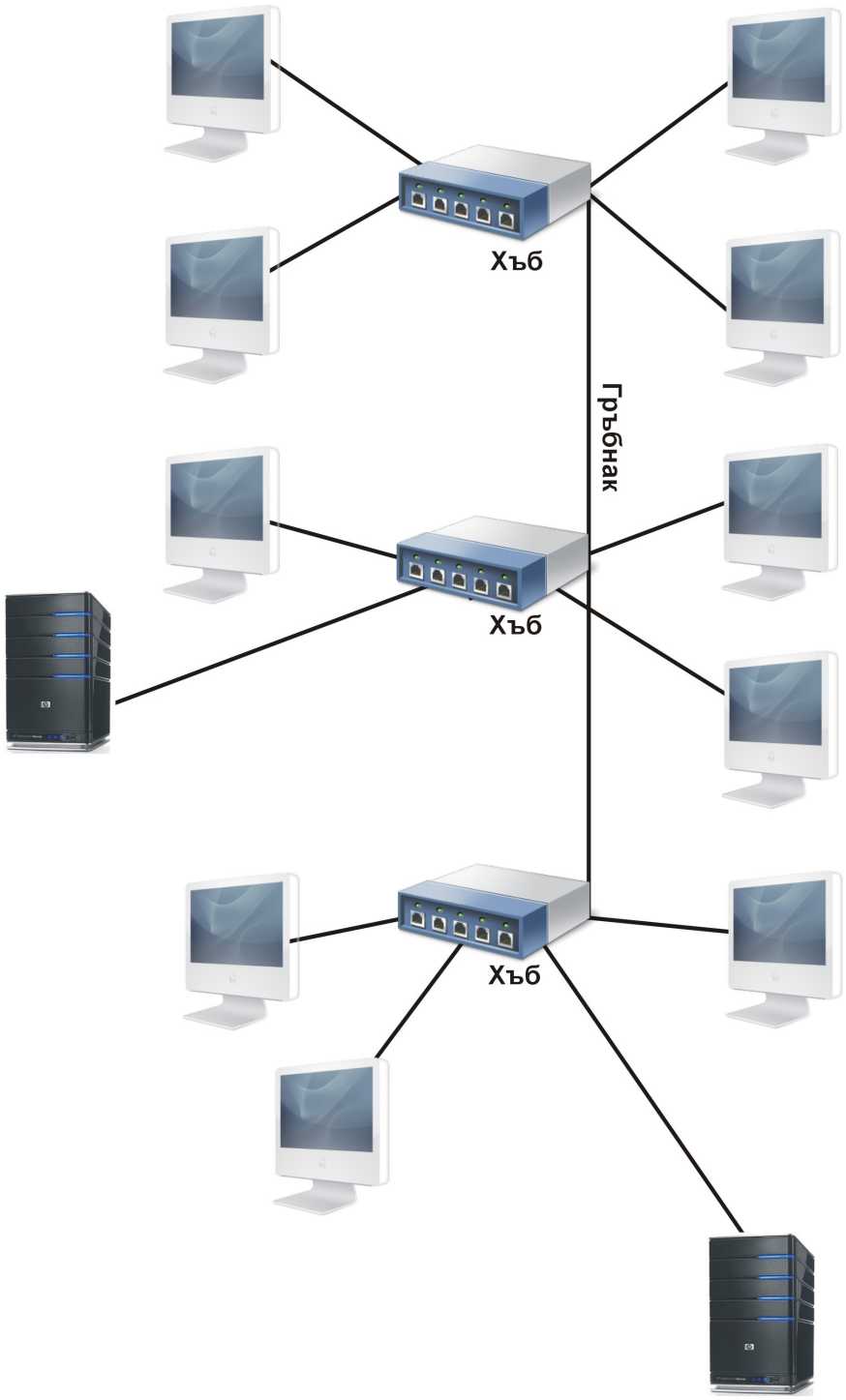
1.5.6. Комбинирани топологии

Терминът хибриден се използва и за означаване на мрежи, които използват множество топологии. Много мрежи комбинират една или няколко топологии. Например може да имате няколко хъба, към всеки от които има компютри, свързани в топология от тип звезда, а след това хъбовете да бъдат свързани в линейна шина. За тази цел много хъбове имат

BNC конектор за тънък коаксиален кабел заедно с няколко RJ45 порта за UTP връзки.

В този тип свързване коаксиалният кабел, свързващ хъбовете, се нарича гръбнак (backbone). Гръбнакът е част от мрежата, свързваща всички по-малки части, наричани още (сегменти). Няколко сегмента могат да бъдат свързани към един гръбнак за създаване на по-голяма мрежа.

Визуализация на комбинирани топологии:



Фиг. 1.10

1.6. Мрежови модели

Повечето хора зависят от визуалното стимулиране. Разбираме нещо по-добре, когато можем да го видим с очите си. Но абстрактните концепции, които нямат конкретна форма, могат да бъдат представени в модел, който да ни създаде визуална представа за дадена структура, процес или релационна връзка.

Моделите са навсякъде около нас. Генетиците използват двойна спирала за представяне на структурата на молекулата на ДНК. Физиците представят релационните връзки на протони и електрони на ниво атом. Атомите са много малки, за да могат да бъдат видени, но учените използват модели за подпомагане на изучаването на явления, които не могат да бъдат наблюдавани директно.

1.6.1. Целта на моделите

Ако потърсим думата модел в речника, ще открием много нейни значения, например „схематично описание на система, теория или явление, което представя нейни познати или предполагаеми свойства и може да бъде използвано за допълнително изучаване на нейните характеристики". Тази дефиниция обхваща една от целите на мрежовите модели: да ни помогнат да опишем, разберем и изучим процеса на мрежова комуникация. Моделът също „служи като пример, който може да бъде следван или сравняван". 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

1.6.2 Моделът OSI

“Моделът на моделите" в света на мрежите е моделът Open System Intercomiec (OSI). На практика всяка книга за компютърни мрежи разглежда този модел, който е разработен от Международната организация за стандартизация (ISO).

На някои места може да срщнем моделът OSI означен като Open System Interconnect, вместо Interconnection. Но по-късно се наложи използването на Web сайта на ISO.

Модельт QSI е изграден от седем слоя, всеки от които представлява една стъпка в процеса на мрежовите комуникации.Седемте слоя на OSI модела са показани на таблицата по-долу :
Табл. 1.2.

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

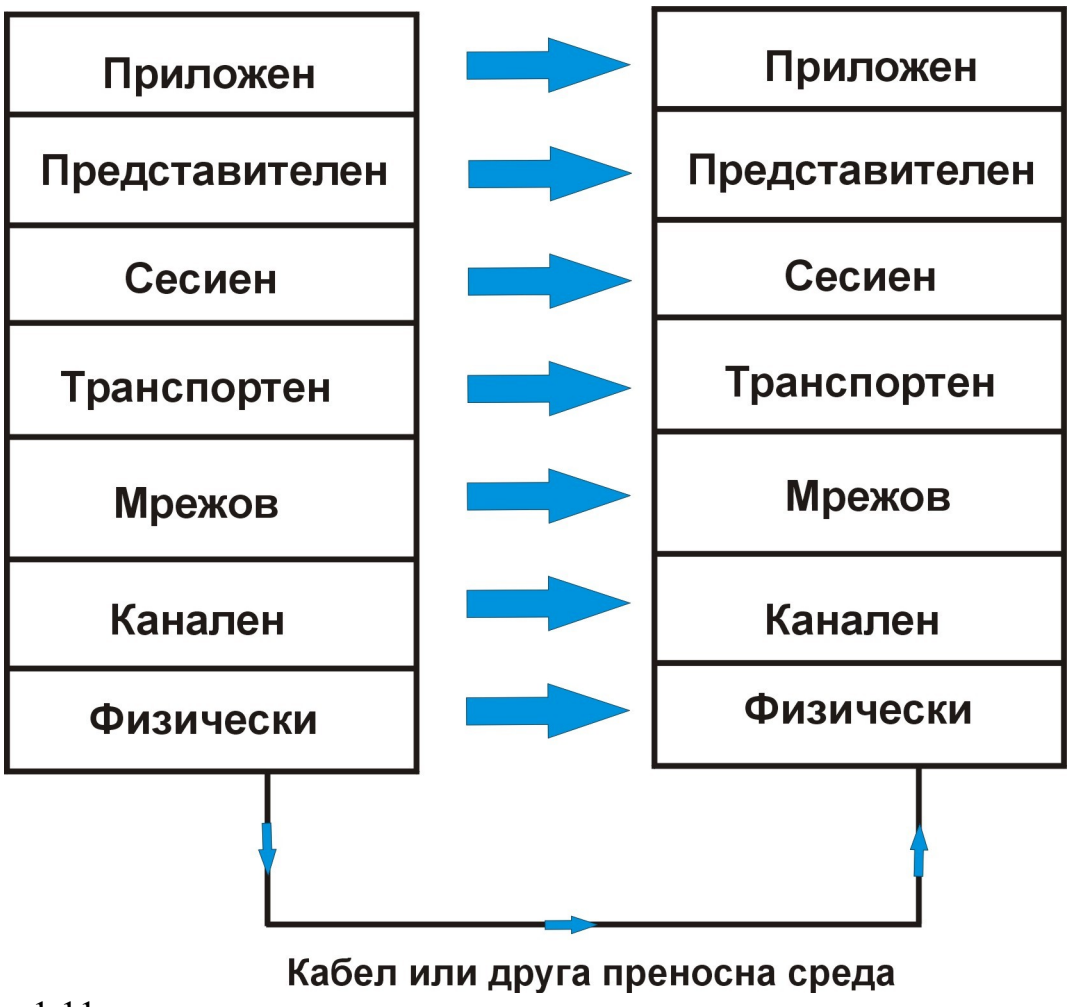
Протоколите, които изграждат комплекта от протоколи (protocol suit), работят на различни слоеве. Всеки слой на OSI модела изпълнява конкретна задача в процеса на мрежовата комуникация и след това предава данните нагоре или надолу към следващия слой (в зависимост от това дали слоят функционира в предаващия 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.

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 изпращащия компютър, и т.н. Всъщност всеки слой комуникира със слоя, който носи същото име от другата страна.

Визуализация на процеса на комуникация:



Фиг. 1.11

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 прилолсението на приемника под формата на информация.
като физическият слой се означава като Слой 1.

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.

Протоколите, 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. Модерните версии на Web браузъри, като Microsoft Internet Explorer и Navigator/Communicator на Netscape, също 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)V 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 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. Това са само няколко от протоколите на приложния слой.

Не трябва да бъркаме самите приложни програми с протоколите със същото име, на които са базирани програмите. Например съществуват разнообразни приложни програми, наречени FTP клиенти (например FTP Voyager, FTP Explorer, Fetch за Macintosh и GREED за Linux), предоставяни от различни производители. 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.

Протоколът от приложния слой приема данните от потребителското приложение и ги предава надолу в стека към представителния слой. Както подсказва ,името, 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 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 предетавлява устройство или софтуер, което служи като точка на свързване между две различни мрежи. Популярните шлюзове са следните:

• Gateway Services for Netware (GSNW) - Този софтуер е включен в операционните системи Windows NT и Windows 2000 Server, за да даде възможност на клиентите на сървъра да осъществяват достъп до файлове на Novell Netware сървър. 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 - Това е тип софтуер, транслиращ съобщения от разнородни несъвместими e-mail системи в общоприет Интернет формат, какъвто е SMTP. Това ви позволява да изпращате електронни съобщения от компютър 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.

Следващият слой по пътя надолу в стека в OSI модела е сесийният 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 (check pointing) 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. Пълният дуплекс представлява двупосочнакомуникация, при която и двете страни могат да изпращат и приемат едновременно дуплексът също е двупосочен, но в даден момент сигналите могат да протичат само в една посока.
Сесията в пълен дуплекс работи до известна степен подобно на разговор по обикновен аналогов телефон. И двете страни могат да говорят едновременно, и докато говорите, можете да чувате гласа на другия човек. Полудуплексът прилича повече на разговор по двуканална радиостанция. Когато включите микрофона, за да предавате, няма да можете да чувате нищо, казано от другото лице,с което говорите. Предаването може да преминава във всяка от двете посоки, но не и в двете едновременно. Еднопосочната комуникация, в която сигналът може да върви само по един път и никога не може да се обърне в другата посока, се означава като симплекс. УКВ радиопредаванията и телевизионните предавания представляват симплек-сни предавания. Но въвеждането на технологии като „интерактивната телевизия" изисква двупосочни комуникации, затова много кабелни компании модифицират своите инфраструктури, за да направят възможно двупосочното предаване на сигнали.

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.

Какво друго прави този работлив слой? 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.

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 връзково-ориентиран протокол за изпращане на съобщението.

Съществуват два типа протоколи, използвани от транспортния слой връзково-орйентиран (въстановяване на връзка) и безвръзково-ориентиран (без установяване на връзка). Други важни концепции на транспортния слой са преобразуването на имена и портовете и сокетите. Връзково-ориентирани транспортни протоколи TCP е връзково-ориентиран протокол, който работи в транспортния слой като част от протоколния стек TCP/IP. Връзково-ориентираните услуги изграждат връзка преди изпращането на данните и използват потвърждения за удостоверяване, че данните са пристигнали успешно до своето местоназначение.

Безвръзково-ориентираните протоколи работят подобно на обикновената пощенска услуга. Когато поставите марка на писмото и го изпратите по пощата, вие вярвате, че то ще стигне до местоназначението си, до което е адресирано, но не разполагате с механизъм, който да ви гарантира, че това е станало.

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.

Какво е предимството на безвръзково-ориентираните протоколи, при положение че те са по-малко надеждни? Предимството е тяхната скорост; простотата и малкото натоварване, които водят до по-висока производителност.

Друга задача на транспортния слой е преобразуването на имената на компютрите (хостовете) в логически мрежови адреси. 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.

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.

Мрежовият слой е отговорен за доставяне на пакетите до техните местоназначения. Този слой управлява маршрутизирането (routing). Можете да сравните отговорностите на протоколите от мрежовия слой с тези на навигатор, който чертае курс от едно местоположение до друго, като избира най-ефикасния възможен път. Повечето протоколи за маршрутизация работят в мрежовия слой. Този слой също така управлява приоритетите на типовете данни, което осигурява някакво ниво на гаранция за достатъчно мрежови ресурси за приложения, изискващи висока пропускателна способност - например за видео на живо.

Layer 2 бе дефиниран като канален слой (data link layer) в оригиналните спецификации на OSI; но този слой беше разделен допълнително на два подслоя:

- Контрол за достъп до преносната среда (Media Access Control - MAC)

- Контрол на логическите връзки (Logical Link Control - LLC)

MAC под слоят 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 в Ethernet мрежа (понякога наричан с още едно име - Ethernet адрес) най-общо се записва като 12 шестнадесетични цифри, подредени по двойки, като всяка двойка е отделена с двоеточие.

Тези 12 цифри в шестнадесетична бройна система представят 48-битови 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 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. Представете си логическия адрес като адрес на улица, който може да бъде променен с декрет на градския съвет. MAC адресът наподобява координата на географска ширина или дължина, която винаги остава постоянна.

На теория никога не трябва да има две карти с едни и същи MAC адреси. Но на практика производителите допускат грешки, като създават карти с дублиращи се адреси. Освен това някои производители започнаха да рециклират своите номера. Дублираните MAC адреси предизвикват проблеми, ако две карти с един и същ адрес се намират в една и съща мрежа, подобно на наличието на две къщи на една и съща улица с един и същ номер. Пощенската служба не знае къде да достави пощата.
Ако две мрежови интерфейсни карти в мрежата имат един и същ адрес, вие трябва да замените една от картите или да промените адреса на една от тях. Някои производители предоставят софтуер, който прави възможно това с помощта на препрограмиране на чипа на мрежовата карта.
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.

В LLC подслоя се дефинира логическата топология на мрежата. 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.
Накрая стигаме до Слой 1 - физическия 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. 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 отдалеченият 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. Когато избирате, трябва да се съобразите със следното:

• Архитектура на мрежата - Картата трябва да бъде предназначена за работа с архитектурата, която използвате във вашата 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. Вашата карта трябва да има правилен тип конектор, за да може да бъде свързана към преносната среда на вашата мрежа. (Ако имате 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 вашия компютър. Трябва да имате съответния тип шина и интерфейс от тип PCI, ISA или PC card, за да може картата да работи в компютъра. Също така е възможно, а често и желателно, да си купите комбинирана карта, която има конектори за два или дори три типа Ethernet кабели. Това е особено удобно, ако очаквате ъпгрейд на вашата ethernet мрежа например към UTP.

• 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 поддържате съответствие между скоростта на картата и останалите мрежови компоненти. Ethernet картите с конектори за UTP се разпространяват във версии със скорости 10 Mbps, 100 Mbps и 10/100 Mbps. Макар и по-скъп, вариантът 10/100 Mbps има очевидни предимства. Обърнете внимание, че ако вашият хъб поддържа 100 Mbps, с него можете да използвате карти на 100 Mbps или на 10/100 Mbps, но картата с 10 Mbps няма да работи.

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, 10BaseT или 100BaseT.

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.

Хъбовете, или така наречените концентраторщ служат като точка на централна точка на свързване. Повечето хъбове реално представляват мно-жествени 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, 10BaseT 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 многопортов 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 сигнлът.

1.6.3. Моделът DoD

Макар че OSI моделът е най-популярен, той не е единственият, нито първият модел за изграждане на мрежи. Факт е, че моделът на Министерството на отбраната на САЩ (Department of Defense - DoD) - понякога означаван като TCP/IP модел - беше разработен около десет години по-рано от OSI модела, през 70-те години на миналия век. Моделът на DoD беше разработен в сътрудничество със самия TCP/IP - част от проекта ARPAnet. Той е по-прост модел, състоящ се само от четири слоя, които могат да бъдат приблизително асоциирани със седемте слоя на OSI модела.

Функцията на всеки слой е следната:

• Слой приложение/процес (application/process layer) - Най-горният слой на модела DoD, който обхваща функциите на трите най-горни слоя на OSI модела: приложен, представителен и сесиен. В текстовете, отнасящи се за TCP/IP, може да прочетете, че криптирането на данните и контролът на диалога се осъществяват в приложния слой. Ако запомните, че това не означава приложния слой на OSI модела, ще избегнете объркването.

• Слой хост до хост (транспортен слой) (host to host (transport) layer) - В някои източници слоят хост до хост се означава като транспортен слой, дори в четирислойни диаграми на DoD, и съответства на транспортния слой от OSI модела. Тук функционират TCP, UDP и DNS.

• Слой интермрежа (internetworking layer) - Този слой съответства много близко на мрежовия слой на OSL Той се занимава с маршрутизация, базирана на логически адреси. Протоколът Address Resolution Protocol (ARP) транслира логическите адреси в MAC адреси. Тази транслация е необходима, защото по-долните слоеве могат да обработват само MAC адресите.

• Слой мрежов интерфейс (network interface layer) - Слоят мрежов интерфейс съответства на двата слоя - канален и физически - от референтния модел OSL В този слой работят стандартните Ethernet и Token Ring протоколи от каналния слой и физическия слой.

Една от целите на ISO при разработката на OSI модела беше по-конкретно да дефинира мрежовите функции, определени от DoD модела при създаване на TCP/IP. Но TCP/IP протоколите бяха проектирани по DoD модела, а не по OSI модела.

1.6.4. Мрежови стандарти и спецификации

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.

1.6.5. Защо трябва да се спазват стандарти?

ISO дефинира стандартите като „документирани споразумения, съдържащи технически спецификации или други точни критерии, които трябва 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, както разбрахте, 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.

1.6.6. 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, разгледани в следващите секции по азбучен ред:

- ISO
- IEC
- ITU
- IETF
- IEEE

ISO е световна федерация на националните организации по стандартизация с по един представител от всичките 100 различни страни. Тя е формирана през 1947 г. с цел разработване на международни стандарти в различни сфери. Един от стандартите на ISO, който много хора са виждали през годините, е ISO номерът на кутийката на фотографските филми, който показва скоростта на филма. Международните буквени кодове на страните са друг пример на работата на ISO.

ISO работи в партньорство с други организации, като International Electrotechni-cal Commission (IEC), World Trade Commission (WTO) и International Telecommunications Union (ITU).

IEC съществува дълго преди ISO, още от 1906 г., но е по-специализирана. Докато ISO създава стандарти от всички видове, целта на IEC е създаването и установяването на стандарти в областта на електро и електронния инженеринг. IEC е изградена от 47 национални комитета и през 1967 г. влезе в споразумение за съвместна работа с ISO по разработката на стандарти и спецификации.

ITU е друга международна организация, усилията на която са съсредоточени върху спонсорирането на събития, публикуването на документи и установяването на стандарти за продукти и услуги, свързани с телекомуникациите.

Internet Engineering Task Force (IETF) е част от Internet Architecture Board (lAB), който от своя страна е техническа консултативна група, принадлежаща на Internet Society (ISOC). IETF е разделена на две работни групи, всяка от които решава различен проблем, свързан с изграждането на Интернет стандарти. Членството в нея е отворено; всяка заинтересована страна може да се присъедини към тази организация.

Основната задача на групите на IETF включва разработката и издаването на Интернет проекти (Internet Drafts), прерастващи в официални документи (Request For Comments - IRFC), които от своя страна преминават през установен процес на одобрение, за да се превърнат в Интернет стандарти.

В качеството си на професионалисти по мрежи може да срещнете препратки към „RFC [номер]" за повече информация по характеристиките на определени мрежови услуги и протоколи. Тези услуги и протоколи включват такива елементи, като:

• Реализация на услугата Domain Name System (DNS)

• Разширения на TCP/IP

• Спецификации за софтуер от типа Network Address Translation (NAT)

Макар че много RFC документи произлизат от IETF, всяка заинтересована страна може да подава предложения за RFC. Не всички RFC документи описват стандарти, но ако даден документ е предназначен за стандарт, той преминава през три фази:

• Proposed Standard - предложен стандарт

• Draft Standard - пробен (проектен) стандарт

• Internet Standard - Интернет стандарт

Има дори RFC номер 2226 - „Инструкции за автори", който съдържа информация за начина на написване и форматиране на проект. След като бъде изпратен, групата Internet Engineering Steering Group (IESG), която е част от IETF, разглежда документа. След обсъждането, ако проектът бъде одобрен, той се редактира и публикува. Редакторът на RFC, назначен от Internet Society, поддържа и публикува главен списък на RFC документите. Той отговаря също за окончателното редактиране на документите. Следва преглед от техническите експерти или така наречената група „task force", по време на който RFC се класифицира в една от следните категории:

• Required Status (изискван статут) - Задължителен

• Recommended Status (препоръчителен статут) - Препоръчителен

• Elective Status (незадължителен статут) - Може да бъде реализиран, но реализацията не е задължителна

•Limited Use Status (статут на ограничено използване) - Не е предназначен за масова реализация .

• Not Recommended Status (непрепоръчван статут) - Не се препоръчва реализация

IEEE (наричан на английски „Ай-трипъл И" от членовете на индустрията) осигурява обмена на информация и разработва стандарти и спецификации за по-ниско ниво на мрежовите технологии (това на физическия и каналния слой).

От особен интерес за професионалистите по мрежи представляват спецификациите на проекта IEEE 802. Името е базирано на датата на заседанието на комитета. 80 означава годината (1980), а 2 означава месеца (февруари). Протоколите от физическия и каналния слой, за които комитетът установява стандартите 802, са следните:

• 802.1 - Въведение в стандартите: LAN и MAN мениджмънт, мостове, които действат в MAC подслоя и алгоритъмът STA (Spanning-Tree Algorithm), който предотвратява комуникационни проблеми, наречени, междумостово зациклят {bridge looping).

• 802.2 - Logical Link Control (LLC): Тези спецификации бяха предназначени за недопускане на затрупване на приемниците от изпращащите. Този стандарт се грижи за разделянето на каналния OSI слой на два подслоя, при което слоят LLC осигурява интерфейс между MAC подслоя и мрежовия слой.

• 802.3 - CSMA/CD: Тази спецификация установява правилата за работа на Ethernet мрежи, използващи метода на множествен достъп с разпознаване на носещата (честота) и откриване на колизии (CSMA/CD), и установяват стандарти за формата на Ethernet фреймовете (пакетите). Първоначално стандартът бе дефиниран като мрежа с линейно-шинна топология, използваща коаксиален кабел, но след това бе обновен за включване на 10BaseT мрежи (топология звезда).

•802.4 - Token Bus: Задава стандарти за мрежи, реализиращи физическа и логическа шинна топология, която използва 75-омов CATV коаксиален или оптичен кабел и метод за достъп с предаване на маркер.

•802.5 - Token Ring: Тази спецификация задава физическия стандарт и метод за достъп до преносната среда за мрежа с физическа топология звезда и логически кръг, която може да използва кабел с екранирана или неекранирана усукана двойка и метод на достъп с предаване на маркер. Този стандарт беше разработен на базата на технологията Token Ring на IBM.

•802.6 - MAN: Задава стандарти за мрежи, които са по-големи от локалните мрежи и по-малки от глобалните мрежи.

•802.7 - Broadband: Установява правилата за изграждане на мрежи с технологии за широколентово предаване, например CATV, използващи Frequency Division Multiplexing (FDM) за изпращане на различни сигнали на отделни честоти по един и същ кабел.

• 802.8 - Fiber Optics: Осигурява спецификации за мрежи, използващи оптични кабели - например Fiber Distributed Data Interface (FDDI).

• 802.9 - Integrated Voice and Data: Понякога наричан само „integrated services" (вградени услуги), този стандарт установява правилата за предаване на глас и данни по ISDN.

• 802.10 - LAN Security: Тези спецификации имат отношение към изграждането на виртуални частни мрежи (VPN) - начин за изграждане на сигурна връзка към частна мрежа по обществения Интернет.

• 802.11 - Wireless: Дава указания за реализиране на безжични (безкабел-ни) LAN технологии.

• 802.12 - 100 VG AnyLAN: Този стандарт се отнася за метода на достъп с приоритет по заявка, разработен от Hewlett Packard с цел комбиниране на предимствата на Ethernet, Token Ring и ATM технологиите в едно високоскоростно решение за локални мрежи.

1.7. TCP/IP

Съвременните мрежови приложения изискват доста сложен подход за пренос на данни от една машина на друга. Ако управлявате Linux машина с много потребители, всеки от които може да поиска да се свърже по едно и също време с отдаличен хост от мрежата, трябва да намерите начин потребителите да си споделят връзката към мрежата, без да си пречат един на друг. Подходът използван от повечето съвременни мрежови протоколи, се нарича комутиране на пакети (packet swishing). Пакетът представлява малък къс данни, които се предаава от една машина на друга по мрежата. Комутирането настъпва, когато дейтаграмата (datagram) се пренася по брънките в мрежата. Мрежите с комутиране на пакети споделят обща мрежова връзка с много потребители, като последователно изпращат пакети от един потребител към друг през въпросната връзка. Решението използвано от Unix, а в последствие и от много не-Unix системи, се нарича TCP/IP.

Корените на TCP/IP могат дабъдат проследени до изследователски проект, финансиран от Advanced Research Project Agency(DARPA) на американското министерство на отбраната през 1969 г. ARPANET е била експериментална мрежа, която е влязла в употреба през 1975 г. , след като е доказала своята ефективност. През 1983 г., новият комплект от протоколи TCP/IP е бил приет като стандарт и всички хостове от мрежата е трябвало задължително да го използват.

1.8. Ethernet

Най-често срещаният LAN хардуер се нарича Ethernet. В неговата най-проста форма той се състои от един кабел, към който се свързват хостове посредствовом конектори, тапи или приемно-предавтелни устройства. Простите Ethernet мрежи са отнсосително евтини за инсталиране, което, в комбинация със скоростта на пренос от 10, 100, 1000, а сега дори 10 000мегабита в секунда (Mbps), е причина за голямата им популярност.

Ethernet мрежите са най-различни: “дебели”, “тънки” и с усукана двойка. По-старите видове Ethernet, които използват тънък и дебел Ethernet

кабел, вече се намират рядко и се различават по диаметъра на използваният коаксиален кабел и начина, по които се свързват хостовете по него. “Тънкият” Ethernet използва Т-образен “BNC” конектор, които прекъсва кабела на определени места и се завинтва в накрайник от задната старна на компютъра. При “дебелият” Ethernet трябва да се пробие малка дупка в кабела, където да се закачи към приемно-предавателно устройство посредством “вампирска тапа. След това към приемно-предавателното устройство могат да се закачат един или повече хостове. Тънките и дебелите Ethernet кабели могат да бъдат опъвани съответно до 200 и 500 метра и понякога се наричат 10-base2 и 10-base5. “base” идва от “baseband modulation” и казано на прост език означява, че данните се подават директно към кабела без никакъв модем. Цифрите в началото указват мегабайтите в секунда, а числото в края показва максималната дължина на кабела в стотици метри. Усуканата двойка използва кабел, съставен от две двойки медни проводници, и обикновенно изисква използването на допълнителен хардуер, наречен активен концентратор, или хъб (hub). Усуканата двойка се нарича още 10-base T, като T означява означява усукана двойка. Стомегабитовата версия е известна като 100-baseT, а 1000 Mbps се нарича 1000-baseT или гигабайтова.

За да добавим хост към инсталацията с тънък Ethernet кабел, работата на мрежата трябва да бъде прекъсната поне за няколко минути, тъй като кабелът трябва да бъде срязън и да се добави конектор. Макар и добавянето на хост към системата с дебел Ethernet кабел да е малко сложно, то обикновенно не води до спиране на мрежата. Ethernet с усукана двойка е още по- прост. Той използва устройство, наречено концентратор или комутатор (още суич) което служи като точка на свързване. Добавянето и премахването на хостове към/от концентратор или суич става без абсолютно никакво прекъсване на работата на потребителите. Мрежите с дебел или тънък Ethernet вече се срещат по-рядко, тъй като бяха изместени почти изцяло от усуканата двойка. Това решение се превърна в нещо като стандарт благодарение на ниските цени на мрежовите карти и кабелите.

Безжичните локални мрежи също са много популярни. Те са базирани на спецификацията 802.11a/b/g и предоставят Ethernet чрез радио вълни. Предлагайки подомна функционалност на кабелите му еквиваленти, безжичният Ethernet беше подложен на атаки по редица въпроси за сигурността, по специално около криптирането. Ethernet работи като шинна система, в която хостовете могат да изпращат пакети с максимална големина от 1 500 на други хостове от същият Ethernet. Хостовете се адресират посредством 6-байтови адреси, записани твърдо във фърмуера на интерфейсната карта за Ethernet мрежа. Тези адреси обикновенно се записват като поредица от двуцифрени шеснадесетични числа, разделени с двоеточие.

Когато една станция изпрати кадър, той се изпраща до всички станции, но само станцията получател приема кадъра и го обработва. Ако две станции се опитат да изпратят в един и същи момент, настъпва колизия. Колизиите в Ethernet се установяват много бързо от електрониката на интерфейсните карти и се разширяват като две станции прекратяват изпращането, изчакват произволен интервал от време и опитват отново да изпратят.

Човек не иска работата му в мрежата да е ограничена до една Ethernet или една връзка за данни от тип точка до точка. В идеялният случай, човек иска да си комуникира с даден хост, независимо от типа мрежа, която физически е свързан. При големи инсталации обикновенно има редица отделни мрежи, които трябва да бъдат свързани по някакъв начин. Примерно една катедра по математика може да работи с две Ethernet мрежи: една с бързи машини за преподавателите и асистентите и друга с бавни машини за студентите.

Тази връзка се осъществява от посветен хост, наречен шлюз (gateway), който обработва входящите и изходящите пакети, като ги копира между двете Ethernet мрежи и оптичния FDDI кабел. Ако например, някой от математическата катедра иска да достигне до quark от локалната мрежа на катедрат по информатика от машина с Linux, мрежовият софтуер няма да изпрати пакети директно към quark, тъй като той не е от същата Ethernet мрежа. Поради това той трябва да разчита на шлюза, който служи за ретранслатор. След това шлюзът (наречен sophus) препраща тези пакети към еквивалентния шлюз niels от факултета по информатика, използвайки опорната мрежа, а niels ги доставя до търсената машина.

Тази схема на насочване на данните към отдалечен хост се нарича маршрутизиране, а в този контекст, пакетите често се наричат дейтаграми. За да се улеснят нещата, обмяната на дейтаграми се управлява от един протокол, който не зависи от използвания хардуер: IP, или Internet Protocol (Интернет протокол). Основната полза от IP е, че той кара различните физически мрежи да изглеждат като една еднородна мрежа. Оттам идва и терминът „интермрежа", а резултатът се нарича интернет (от internetwork). Има разлика между „една интернет мрежа" и „Мрежата Интернет". Второто е официалното име на една определена глобална интернет мрежа. IP, разбира се, също изисква схема за адресиране, която да не зависи от хардуера. Това се постига като на всеки хост се присвои уникален 32-битов номер, наречен „IP адрес". IP адресът обикновено се изписва като четири десетични числа, по едно за всяка 8-битова част, разделени с точки. Този формат се нарича още точково десетично представяне, а понякога и четворно точково представяне. Все по-често се използва и името IPv4 (от Internet Protocol, версия 4), тъй като новият стандарт IPv6 предлага много по-гъвкаво адресиране, както и други по-съвременни възможности. Както

забелязвате, вече имаме три различни вида адреси: първо е името на хоста, например quark, след това идва IP адресът, и накрая - хардуерният адрес, например 6-байтовия Ethernet адрес.

1.9. Сигурност

Добрата сигурност е добро системно администриране. Сигурността е фундаментална част от работата на един надежден мрежов сървър. Несъмнено нашият сървър ще бъде атакуван и подлаган на риск от различни хора в мрежата. Нашата задача е да намалим броя на успешните атаки, да ограничим количеството на причинените повреди и бързо да възстановим системата от атаката. Освен сигурността на мрежата изисква се и физическа сигурност за защита на хардуера на сървара и недопускане на неоторизиран достъп до системната конзола.

1.9.1. Заплахите

Свързването нс сървара към мрежата му дава достъп – и го прави уязвим – за всеки в мрежата. Колкото по-голяма е мрежата, толкова по-голяма е заплахата. Когато свържем нашата система към мрежата, трябва да преciним заплахата за сигурността, която създава режовата връзка. За да направим тази преценка, трябва да вземем в предвид потенциалните вреди върху нашата организация от една успешна атака срещу сигурността. Въздействието на една атака срещу сигурността зависи от това каква система и каква инфирмация са подложени на риск. Загубата на ключов сървър вляе на много потребители, докато загубата на настолен клиент може да повлияе само на един потребител. Макар че нашите усилия трябва да са насочени към защитата на нещета, които са важни, всяка система изисква някакво ниво на защита. Пробивът в една малка незначителна система може да завърши с излагане на риск на цялата система.

Съществуват три основни заплахи за информацията, съхранявана в мрежата:

1) Заплахи за сигурността на данните- Това е неоторизирано разкриване на секретни данни, което може да бъде причинено от задаването на неправилни позволения за файлове, неправилно задаване на root привелегии на някого или допускане на кражба на данни директно по линията.
2) Заплахи за целостта на данните – Тук се включва неоторизирано модифициране на данни, което може да бъде причинено от използването на неправилни позволения за файлове или от някой,

неправилно получил привелегии на root. Това е често срещана заплаха за Web сървари, при която нарушителите променят данните по очебиен начин и поставят институции в неудобно положение. Но една по-коварна заплаха е възможността за неуловими модификации на данните, които имат за цел да подкопаят репутацията на организацията. След като дадена система е пострадала от неоторизиран достъп, всички файлове на системата стават предмет на съмнение.

3) Заплахи за сигурността на данните – Тези атаки нарушават легитимният достъп на данните. Ако файловете са защитени неправилно или нарушител получи root достъп, файловете могат да бъдат изтрити. Вандали могат също да проведат атака Denial of Service, за да претоварят сървара, блокирайки достъпа до нашите данни , когато са ни необходими.

Заплахите от мрежата, които водят до тези проблеми с данни, са следните:

1) Неоторизиран достъп – Това е всеки случай когато някой, които не трябва да има достъп до нашата система, получи възможност да осъществи достъп до нея без позволение.
2) Отказ на услуга – Всяка атака, чието предназначение е не някой да придобие достъп до нашата система, а да бъдем възпрепятствани да използваме системата.

Всички системи, работещи в мрежата, са предразположени на тези атаки. За щастие Linux осигурява широк набор от инструменти, за да ни помогне да намалим заплахите.

Повечето атаки идват от неквалифицирани хора, които изпълняват масово разпространявани атакуващи скриптове. Скриптовете са толкова прости за използване, че хората, които сега ги използват, са “играещи си дечица”. Хората, изпълняващи тези скриптове, не се интерисуват от спионаж, но нямат нищо против да направят някой поразии! Linux също не е защитен от атаки срещу сигурността. За нещастие Linux е една от най-популярните цели на атаки. Определено отвореният сорс код не е защита от атака. Хората, които изпълняват атакуващи скриптове, не са мотивирани от това да подобрят системата- те просто търсят лесни мишени.

За да защитите една система трябва да познавате нейните уязвими страни. Повечето нарушители влизат в системата през известни пролуки в системният софтуер. Най-важното нещо което трябва да се направи, за да се подобри сигурността на системата, е да затеорите пролуките, като се инсталираме обновяванията на сигурността веднага

след тяхното появяване. Уязвимите страни не са ограничени само до ядрото на Linux. Всъщност повечето от уязвимите страни, които се използват от нарушителите, възникват в мрежовият софтуер, които се изпълнява от нашата Linux система. За да обновим софтуера, трябва да знаем какво трябва да бъде обновено и къде да го намерим. Съветниците по сигурността обикновенно описват проблема и ни указват вярното решение, често те посочват правилната поправка за софтуера. Можем да намил бремето на постоянното следене за обновяване на софтуера, като премахнем целият софтуер, от които не се нуждаем.

Съществуват два прости начина за блокиране на достъпа до излишните демони:

1) Забранете демоните от конфикурацията на inetd или xinetd. Повечето мрежови услуги се стартират с помща на inetd или xinetd, които стартират само услуги изброени в техните конфигурационни файлове. Забраняването на конкретна мрежова услуга в конфигурционнияфайл не допуска използването и от външни лица, но не блокира използването и от останалите клиенти по изходящите конекции. Оттук ако ftp е забранено в inetd.conf потребиелят пак може да осъществява ftp до отдличени сайтове, но никой от отдаличения сайт не може да използва ftp, за да влезе в настолната система на птребителя. За да забраним дадена услуга във файла inetd.conf трябва да поставим знак диез в началото на нейният запис. За да забраним на xinetd да стартира дадена услуга трябва да зададем периметъра disable = yes в конфигурацията на xinetd на тази услуа.
2) Премахнете скриптовете , които стартират ненужни демони при начално зареждне – Някой демони за мрежови услуги например sendmail и named, се стартират п време на началното зареждане. Трябва да използваме tksysv или chkconfig, за да премахнем нежеланите демони от началното зареждане. Мрежовите демони не са единственият непотребен софтуер, а клиентите не са единствените мишени. Непотребният софтуер на един сървър може също да отвори дупка за нарушиели.
3)

Съществуват два начина за ограничаване на софтуера, инсталиран на един сървър. Първо когато правим първоначяна инсталация на Linux, не трябва да инсталираме това , което не ни е необходимо. По време на първоначалната инсталация трябва да изберем софтуерните пакети , които е инсталрат , и демоните , които е зареждат. Трябва да избираме внимателно според плана на системта която инсталираме.
Другият начин за ограничаване на софтуера е да го примахнем когато го

инсталираме. Например за да премахнем IMAP от системата с rpm, можем да ъведем rpm –e imap-2000c-15.

Освен с инсталиране на най-новият софтуер и премахване на непотребния софтуер, трябва да осигурим досстъп до софтуера и услугите, изълнявани от нашата система, само натези системи, на които реално искаме да служим като сървър. Linux прави това просто като осигурява механизми за контрол на достъпа. Системите, които използват inetd, могат да контролират достъпа чрез софтуера tcpd. Системите, които изолзват xinetd, могат да използват възможностите за контрол на достпа включително в xinetd. А всички системи с ядро Linux 2.4 могат да използват iptables за ограничаване на достъпа.

Софтуера tcpd осигурява обвивката на TCP и се изпълнява от inetd. Той е неделима част от повечето Linux дистрибуции, които използват inetd. Използванто на tcpd на Linux система е по-лесно от това на много други системи, защото записите в файла inetd.conf вече сочат към програмата tcpd. Програмата tcpd изпълнява две основни функции: запис в дневника за заявки за Интернет услуги и осигурява механизъм за контрол на достъпа до тези услуги. Записване в дневника на заявките за конкретни мрежови услуги е полезна функция за наблюдение, особено ако следим за възможни нарушители. Tcpd използва източника authpriv на syslogd, за да записва в дневник своите съобщения. Ако записа на дневник беше всичко, което прави tcpd щеше да бъде просто един полезен пакет. Но истинската мощ на този полезен инструмент е неговата способност да контролира достъпа до мрежовите услуги.

Два файла дефинират конфигурацията за контрол на достъпа до tcpd:

1) Файлът hosts.allow съдържа списък на хостове, на които е разрешен достъп до услугите на системата.
2) Файлът hosts.deny съдържа списка на хостове, на които услугата е отказана.

Ако тези хостове не бъдат намерени, tcpd разрешава достъп на всеки хост и просто записва в дневника заявката за достъп. Когато файловета са налични, tcpd първо чете файла hosts.allow и след това чете файла hosts.deny. програмата спира веднага след като открие съвпаение на хоста и въпросната услуга. Следователно, достъпът даден от hosts.allow, не може да бъде отменен от hosts.deny. по тази причина често hosts.allow, срещано в практиката е да се започне първо с вмъкване на запис в hosts.deny, което отказва всякакъв достъп на всички системи, и след това да се продължава с поставяне на записи в файла hosts.allow, които позволяват достъп само на тези системи, които реално трябва да получат услуги. Форматът на записите и в двата

файла е един и същ:

услуги : клиенти [: shell-команда]

услуги е разделен със запетаи списък на мрежови услги или ключовата дума ALL. ALL означава всички мрежови услуги. В противен случай всяка мрежова услуга се идентифицира с името на нейният процес, което е името, следващо следващо непсредствено след пътя до tcpd във файла inetd.conf . например името на процес в следният запис във файла inetd.conf е imapd:

imap stream tcp nowait root /usr/sbin/tcpd imapd

клиенти представлява разделен със запис списк на имена хостове, имена на домейни, мрежови номера и ключовата дума LOCAL. Като алтернатива, може да се зададе ключовата дума ALL. ALL съответсва на всички имена на хостове и адреси; LOCAL съотвества на всички имена на хостове, които не включват част от името на домейн. Име на хост съответства на отделен хост. Ако дефинираме самостоятелен IP адрес, той съответства на конкретен хост, а ако го дефинираме с адресна маска, то съответства на обхват от адреси. Едно име на домейн започва с точка (.) и съответства на всеки хост в тзи домейн. Един мрежов номер завршва с точка и съответства на всеки IP адрес в дресното пространство на мрежата.

shell-команда е незадължителна шел-команда, която tcpd изпълнява при срещане на съответствие. При съответствие с tcpd записа в дневника достъпа, дава или отказва достъп до услугата и след това подава командата на шела за изпълнение. Командата на шела ни позволява да дефинираме доплнителна обработка, която се стартира при съвпадение в списъка за контрол на достъп. Тази възможност се използва във файла hosts.deny за събиране на още информация за нарушителя или за осигуряване на незабавно уведомление на сиситемният администратор за потенциална атака срщу сигурността. За да контролираме достъпа до услугите, които се стартират от стартови скриптове и които не четат конфигурационния файл на tcpd, трябва да използваме защитна стена на IP в Linux.

Мислим, си че знаем какво е зашитна стена, докато не се задълбочим в детайлите. В общият смисъл защитната стена (firewall) е сиситема, която защиава локалната мрежа от голямата лоша глоблна мрежа. Тя е страж, през които трябва да преминава целият мрежов трафик, преди да влезе или излезе през локалната мрежа. В нейото най-просто изплнение защитната е филтриращ маршрутизатор, които оставя нежеланият трафик. А в нейната най-сложна имплементация, тя е цяла мрежа с множество маршрутизатори и множество сървъри.

Linux осигурява инструменти за филтриране на трафика, необходими за създаване на проста защита стена. Комбинирането на възможностите на Linux с възможностите за филтриране на iptables създава филтриращ

маршрутизатор. Наред с това, и което е по-често срещано, софтуера iptables може да бъде изолзван за филтриране на трафик, който пристига на мрежовият интерфейс на един Linux сървър преди този трафик да бъде подаден към мржовите приложения, изпълнявани на този сървър. Това дава на Linux възможността да изгради защитна стена в самият сървър, което осигурява контрол на достъпа за всички възможнимрежови услуги.

Ядрото на Linux категоризира трафика а защитната стена в ри групи и прилага разлини правила за филтриране към всяка категория трафик:

1) Входящ за защитната стена – входящият трафик се проверява според входите правила на защитната стена, преди да бъде приет.
2) Изходящ за защитната стена – изходящият трафик се проверява според правилата на защитната стена, преди да бъде изпраен.
3) Трафик за препращане – трафикът препращан през Linux системата, се проверяа според правилата за препращае на защитнта стена.

Тадиционните пароли в Unix не са по-дълги от осем знака и се предават по мрежата като прав текст. Освен това тези пароли се съхранват във файла / etc/password, които може да бъде прочетен от всеки. Всички тези неща представляват проблеми за сигурността. Ограничаването на паролите до осем знака ограничава възможностите избор на потребителя и улеснява организирането на атака за декрептиране по метода на грубата сила. MD5 паролите могат да бъдат дълги до 256 знака. Затова е препоръчителн тя да се инсталира. Независимо колко е дълга паролат потебителят може да избере лоша такава. Лошата парола е парола, която лесно може да бъде разгадана.

“Да и не” при избор на парола:

- Изплзвайте смесица от числа, специални знакове и комбинация от главни и малки букви.
- Използвайте най-малко осем знака.
- Използвайте привидно случайна селекция от букви и числа, която е лесна за запмняне, например първата буква от всяка дума е ред от книга, песен или стихотворение.
- Не използвайте името на човек или животно.
- Не използвайте дума на англййски или друг чужд език, нито съкращение.
- Не използвайте никаква информация, асоциирана с акаунта.
- Не използвайте лесни клавищни комбинации.
- Не изпозайте парола съставена само от цифри.

- Не използвайте примерна парола, която сте взели от книга за компютърна сигурност, независимо колко е добра.

Linux не допуска потебителите да избират лоши пароли, като прилага много от правилата, които описахме по-горе, за да отхвърли лошите пароли. Паролите се избират с командата passwd. Макар, че Linux прави всичко, което зависи от него, за да гарантира, че ще използваме добра парола, тя става неизползваема ако някой я открадне. Тъй като паролите се изпращат по мрежата като прав текст, те могат много лесно да бъдат откраднати.

Дори когато се използва добро криптиране за паролите, съхранявани във файла passwd, ако паролите са избрани лошо, те са уязвими за речникова атака. Най-обрият начин да избегнем този проблем е да съхраним криптираните пароли във файл, който не може да бъде четен от всеки.

Файлът със скрити пароли може да бъде прочетен само root. Той няма позволения за “групата” или “останалите”. Предназначен е да не допусне обикновенни потребители да четат криптираните пароли и да ги подлага на речникова атака. Освен, че подобрява сигурността на паролите, файлът за скрити пароли осиурява на системният администратор някой възможности за управление на паролите. Освен, че съхранява паролите shadow файлът подържа време на живот за всяка парола и уведомява потребителя да я промени, когато тя приближи края на своят живот. Ако паролата не бъде променена, потребителя бива блокиран и не може да ползва своя акаунт.

Глава 2. Безжични мрежи

2.1 Същност и история на безжични мрежи.

Безжичните мрежи са обещаваща и все по-популярна технология, предлагаща голям набор от предимства пред традиционната жична технология. Тези предимства се простират от увеличено удобство за клиентите и намаляване на разходите за изграждане, до улесняване на инсталацията на мрежата. Едно внедряване на безжична мрежа може да спести значително количество средства, тъй като няма нужда от допълнителни кабели, куплунзи или мрежови комутатори. Добавянето на нови потребители се свежда до инсталирането на безжична карта и включването на машината. Безжичните мрежи се използват, също така, за предоставяне на мрежов достъп на места, където няма традиционна мрежова инфраструктура.
Вероятно най-голямото влияние на безжичните мрежи може да бъде усетено в доброто им възприемане от потребителите. Най-очевидният пример за популярността на тази технология може да бъде видян при новите преносими компютри, повечето от които вече се доставят с интегриран 802.11b или g интерфейс.

Безжичните LAN мрежи са базирани на радиовълнова технология, разпределения спектър, първоначално разработена за военна комуникация от армията на САЩ по време на Втората световна война. Военните техници са се спрели на разпределения спектър, тъй като той е по-устойчив на заглушаване. Други предимства по онова време дали възможност за увеличаване на скоростта на предаване на радио данни. След 1945 г., цивилните предприятия започнали да разширяват тази технология, осъзнавайки потенциалните ползи за потребителите. Технологията разпределен спектър еволюирала до предшественика на съвременните безжични LAN мрежи през 1971 г., благодарение на един проект на Хавайския университет, наречен AlohNet. Този проект дал възможност на седем компютъра на различни острови да общуват двупосочно с централен комутатор на остров Оаху.
Проучванията на университета покрай AlohNet прокара пътя към първото поколение от съвременно оборудване за безжични мрежи, което работеше в честотния диапазон 901-928 MHz. Тази фаза от развитието се радваше на ограничена употреба от потребителите, поради задръстване на честотната

лента и относително ниската скорост, поради което употребата беше ограничена предимно за военни цели.
От този момент насам, за свободно използване беше определена честотата 2.4 GHz, така че безжичната технология започна своя растеж в този диапазон и беше създадена спецификацията 802.11. Тази спецификация прераснала в широко разпространения стандарт 802.11b, като същевременно продължава да се развива към все по -бързи и по-сигурни реализации на технологията.

2.2 Стандарти на безжични мрежи

Стандартите за изграждането на безжични мрежи за компютри са създадени от Institute of Electrical and Electronics Engineers (IEEE). На технологията LAN/MAN е даден главен номер 802, който от своя страна е разделен на работни групи. Към някои от най-активните безжични работни групи съвпадат 802.15, предвидена за мрежи в личното пространство (Bluetooth), 802.16, която дефинира поддръжката на широколентови безжични системи, и накрая 802.11, разработваща технологията за безжични LAN мрежи. Дефиницията 802.11, от своя страна, е разделена на по-специфични дефиниции, които са с буквени означения. Ето списък на най-важните дефиниции за безжични LAN мрежи:

802.11a
Тази дефиниция предоставя безжичен достъп в честотната от 5 GHz.Тя предлага скорости от максимум 54 MBps, но не е много разпространена, вероятно поради относително високите цени на оборудването и късият обхват.

802.11b
Това все още е стандартът, който се има предвид от повечето хора, когато стане дума за безжични мрежи. Той позволява скорости от 11 MBps в честотната лента 2.4 GHz, а обхватът му може да достигне до повече от 500 метра.

802.11g
Този стандарт е разработен за предоставянето на по-високи скорости за данни 54 MBps в честотната лента 2.4 GHz и предлага допълнителна сигурност чрез въвеждането на WiFi Protected Access, или WPA. 802.11g устройствата в момента се внедряват на мястото на 802.11b устройствата и вече почти са достигнали широко разпространение.

802.lli

Макар и още във фаза на разработка, този стандарт има за цел да разреши много от проблемите със сигурността, които морят 802.11b, и да предостави по-надеждна система за удостоверяване и криптиране. По време на списването на настоящата книга, тази спецификация не е завършена.

802.lln
802.lln е прокламиран като висококоростният отговор на сегашните ограничени в скоростта безжични мрежи. С операционна скорост от 100 Mbps, той горе-долу ще удвои съществуващите скорости за безжичен пренос, като същевременно ще предлага съвместимост с по-старите спецификации b и g. По време на списването на настоящата книга, тази спецификация не е завършена. Някои производители, обаче, вече предложиха предварителни продукти, които са базирани на ранните чернови на спецификацията.

Стандартът IEEE 802.11 работи в съответствие с двете долни нива на модела OSI - физическо и канално ниво. Всяко едно мрежово приложение, протокол или операционна система могат да работят при това положение в една безжична мрежа не по-лошо, отколкото това става в обикновена Ethernet мрежа. Основната архитектура, особености, протоколи и служби са определени в стандарта 802.11, а спецификацията 802.11b засяга физическото ниво, променяйки скоростта на обмен и достъп към по-висока.

Табл. 2.1.

НИВО	ОЗНАЧЕНИЕ	
1	Физическо	
2	Канално	local link control
		media access control
3	Мрежово	
4	Транспортно	
5	Сесийно	
6	Представително	
7	Приложно	

На физическо ниво са отделени общо три метода за предаване на данни, единият от които е в инфрачервеният диапазон, а другите два са радиочастотни, работещи в интервала между 2.4 GHz и 2.483 GHz. Двата широколентови канала могат да използват различни методи за организиране на предаването - метод на пряка последователност (DSSS-

Direct Sequence Spread Spectrum), или метода на честотните подскоци (FHSS - Frequency Hopping Spread Spectrum).

Стандартът 802.11 фиксира два вида безжично мрежово оборудване - ***клиент***, ролята на който обикновено се поема от компютър с инсталирана безжична мрежова интерфейсна платка (Network Interface Card, NIC), и ***точка за достъп*** (Access point, AP), която служи за връзка между безжична и кабелна мрежа.

Фиг.1.1.

Клиентът, както споменах по-горе, е окомплектован с мрежова карта 802.11, която може да бъде с интерфейс ISA, PCI или PC Card, както и във вид на вградено решение. Точката за достъп обикновено е оборудвана с приемо-предавател, интерфейс към кабелна мрежа (802.3) и специализирано програмно осигуряване. Стандартът IEEE 802.11 определя два режима на работа на безжичната мрежа - режим точка-точка (***Ad-hoc***) и режим клиент/сървър, наричан още режим на инфраструктурата (***infrastructure mode***). По този начин са озаглавени режимите във повечето програмни пакети, управляващи Access Point, процедурите по настройването на които няма как да избегнете. Първият режим, точка-точка, наричан още IBSS - ***независим набор от служби*****,** както личи и от заглавието, сполучливо трансформирано от неразбираемото "Ad-hoc", представлява елементарна като структура мрежа, в която отделните станции се свързват една със друга пряко, без да е необходима точка за достъп. Разбира се, при това положение съществуват някои ограничения от

типа на максималния брой устройства, които могат да изграждат такава мрежа, което зависи от типа на безжичното мрежово оборудване и от спецификациите на 802.11. Режимът клиент/сървър предполага използването на поне една точка за достъп, представляваща специализирано устройства, която да е включена към кабелна Ethernet мрежа, и определен, често ограничен брой крайни безжични работни станции. Този тип конфигурация се нарича ***основен набор от служби*** (BSS - Basic Service Set), като при наличието на два или повече BSS се формира ***разширен набор от служби*** (ESS - Extended Service Set). Очевидно е предимството на режима клиент/сървър, когато безжичната мрежова станция може да получи достъп до локално мрежово устройство или специфична функция, свързано към стационарната мрежа (например, към мрежов принтер, скенер или Интернет).

Както споменах по-горе, основната промяна, внесена от 802.11b в основния стандарт, е поддръжката на две нови скорости на предаване на данни - 5.5 и 11 Mbps. За постигането на тези скорости се използва методът на пряка последователност (DSSS), което означава, че системите 802.11, използващи DSSS, ще са съвместими с DSSS системите 802.11, но няма да се "виждат" със системите, използващи FHSS 802.11. Другото полезно нещо при 802.11b е методът на динамична промяна на скоростта на трансфер в зависимост от силата на сигнала, шумовете в ефира или отдалечеността на станцията. Това, обяснено на неусложнен и разбираем език означава, че устройствата IEEE 802.11b могат да установят връзка помежду си при 11 Mbps, после, при възникване на смущения, или при отслабване на сигнала, те автоматично ще намалят скоростта на предаване. След определен период от време, след като се появи възможност устройствата пак да работят на по-висока скорост, скоростта пак ще бъде автоматично увеличена до максимално възможната. Просто и логично...

Повечето модели интерфейсни карти са предназначени за включване към шината PC Card/PCMCIA. За да могат те да бъдат монтирани в компютрите, които нямат такъв слот, производителите предлагат преходници към PCI от PCMCIA.

Фиг. 2.2.

За радост на всички, на които нямат свободно място на PCI слотовете на desktop системите им, много от производителите произвеждат и външни устройства с интерфейс USB.

В резюме основните характеристики на адаптерите IEEE 802.11b изглеждат така:

- интерфейс: PC Card, USB, PCI
- скорост на предаване на данни: до 11 Mbps
- работа в half-duplex режим
- възможност за работа в режим точка-точка и клиент/сървър с точка за достъп
- работна честота: 2.4 GHz
- далечина на връзката: 100..500 м в зависимост от външните условия и от скоростта

Логичното изискване към все по-големите обеми на трансферирана информация изисква нови промени в стандартите за безжични комуникации. Още през януари 1997 Федералната комисия на САЩ по съобщенията (FCC) даде разрешение да се използва за безлицензни радиочастотни мрежи 5 GHz-вия диапазон, в който са обособени два участъка (5.15 - 5.35 GHz и 5.725 - 5.825 GHz) с обща честотна лента от 300 MHz. Макар че и двете спецификации IEEE 802.11 са приети по едно и също време през есента на 1999 година, широкото разпространение на IEEE 802.11b устройства, предлагани още преди това от няколко големи производителя, им осигури предимство пред "конкурентите" от 802.11a.

Адаптерите, отговарящи на спецификациите IEEE 802.11a, на външен вид по нищо не се отличават от старите 802.11b, но имат три много основни "вътрешни" разлики:

- интерфейс: Card Bus, USB 2.0
- скорост на предаване на данни: до 54 Mbps

- работна честота: 5 GHz

Диапазонът от честоти, отделен за IEEE 802.11a, съвпада с европейския стандарт HIPERLAN (High Performance Local Area Network), благодарение на което произвежданото за HIPERLAN оборудване може да се използва на всички континенти.

Макар и да са спецификации на един и същ формат, отличаващи се само по една буква в наименованието си, устройствата , отговарящи на стандарта 802.11b не могат да бъдат модернизирани до по-бързия 802.11a. По този начин, ако в момента имате изградена 802.11b мрежа, единственият начин, по който можете да я накарате да заработи на 54 Mbps, е да подмените оборудването с ново. Единственото изключение са последните модели точки за достъп (Access Points), които позволяват монтирането в тях на PCMCI карти, отговарящи на стандарта 802.11b, и на 802.11a.

Когато IEEE създаде стандарта 802.11b, те осъзнаваха, че отворената същност на безжичните мрежи изисква някакъв механизъм за опазване на целостта и сигурността на данните и поради това създадоха Wired Equivalent Privacy (WEP). Стандартът обещаваше да предостави криптиране на ниво 128-бита и потребителите трябваше да могат да се наслаждават на същите нива на сигурност, както при традиционните кабелни мрежи.

Надеждите за такъв вид сигурност, обаче, много бързо бяха попарени. В един документ, наречен „Weaknesses in the Key Scheduling Algorithm of RC4" от Скот Флюрер (Scott Fluhrer), Итсик Мантии (Itsik Mantin) и Ади Шамир (Adi Shamir), бяха описани много подробно слабостите в генерирането и реализирането на WEP. Въпреки че по време на създаването на този документ тази разработка беше теоретична атака, един студент от Университета Райе, Адам Стъбълфийлд (Adam Stubblefield), я превърна в реалност и проведе първата WEP атака. Макар че той не разпространи публично своите инструменти, вече се предлагат много подобни такива за Linux, даващи възможност на атакуващите да пробият WEP, превръщайки го в ненадежден протокол за сигурност.
Все пак трябва да се отбележи, че провеждането на една WEP атака изисква значително количество време. Успехът на атаката зависи на количеството криптирани данни, които атакуващият е уловил. Инструментите от типа на AirSnort изискват приблизително 5 до 10 милиона криптирани пакети. За пробиването на една безжична LAN мрежа, постоянно натоварена с максималното количество трафик, може да са необходими до 10 часа. Тъй като повечето мрежи не работят на пълен

капацитет толкова време, може да се очаква, че атаката ще отнеме доста повече време, от порядъка на няколко дни при по-малките мрежи.
За истинска защита от злонамерено поведение и подслушване, обаче, трябва да се използва VPN технология и безжичните мрежи не трябва никога да се свързват директно към вътрешни, доверени мрежи.

Различните производители използват леко различаващи се архитектури за предоставянето на 802.11b функционалност. Има два големи производители на чипове, Hermes и Prism, а във всеки от тези чипове производителите на хардуер правят различни промени за подобряване на сигурността или ско-ростта. Например оборудването на USRobotics, базирано на чиповете на Prism, вече предлага 802.11b на 22 MBps, но то не може да работи на тази скорост съвместно с 22 MBps 802.11b хардуер на ВЬ11ж. Тези устройства, обаче, са съвместими на скорост 11 MBps.

801.11g u 802.11b B Linux

Поради новите чипове и разликите между производителите, поддръжката на 802.11g в Linux е донякъде трудна. Поддръжката на 802.11g устройства под Linux все още е в зародиш и не е стабилна и надеждна като тази за 802.11b. Нормалната поддръжка на g устройства под Linux, обаче, не е далеч. Благодарение на работата на групите от типа на Prism54.org, която разработва g драйвери, и обявлението на Intel, че ще предостави драйвери за своите чипове Centrino, пълната поддръжка е на разстояние по-малко от година.

Както беше споменато по-горе, съществуват два основни вида 802.11b чипове, Hermes и Prism. Макар в началото картите на Hermes да бяха доминиращи, благодарение на популярността на картите WaveLAN (Orinoco) на Lucent, значителна част от производителите на карти днес използват чипа prism2 на Prism. Някои много популярни Prism карти са например тези на D-Link, Linksys и USR. С всяка от тези карти ще получите приблизително едно и също бързодействие, а и те са взаимозаменяеми, когато работят по стандарта 802.11b. Това означава, че няма проблем да се свърже безжична карта на Lucent с точка за достъп на D-Link, и обратното. Следва кратък списък с основните производители на карти и техните чипове. Ако вашата карта не е в този списък, проверете в ръководството й за експлоатация или на уеб сайта на производителя.

- Карти с чипове на Hermes
  - Lucent Orinoco Silver и Gold Cards
  - Gateway Solo
  - Buffalo Technologies
- Карти с чипове Prism 2:

Addtron
Belkin
Linksys
D-Link
ZoomMax

2.3 Защита на данните

Всички технологии за безжични комуникации използват един или друг вариант на кодиране на данните с цел тяхна защита. Мрежите, отговарящи на стандарта IEEE 802.11, използват функции за криптиране WEP за кодиране на информацията, като, в зависимост от класа на устройството криптирането може да бъде 64- или 128- битово. При Bluetooth има три режима на защита, като най-защитеният Security mode 3 (link level enforced security) оперира с сеансови ключове (Bond), които се генерират в процеса на свързване на две устройства, и се използват в процеса на свързване, идентификация и предаване на данни между две устройства. При всички положения, проблемът със защитата на данните при безжичните комуникационни устройства е открит - все още е сравнително лесно да бъде уловен сигнала от ефира и той да бъде декодиран.Както споменах, 802.11b осигурява контрол на данните на MAC ниво и механизми на криптиране, известни като Wired Equivalent Privacy (WEP), които могат да бъдат включени или изключени.Когато WEP е включен, той защитава само пакета с данни, но не и заглавието му, така че всички свързани в мрежата устройства могат да "преглеждат" преминаващите данни. За контрол на достъпа във всяка точка на достъп се разполага ESSID (или WLAN Service Area ID), без информация за който станцията не може да се включи към точката за достъп. Освен това, при нея може да се съхранява списък от "разрешени" MAC адреси на упълномощените устройства, по този начин разрешавайки към мрежата да се включват само тези устройства, които се намират в списъка. Криптирането на данни се извършва с помощта на алгоритма RC4 с 40-битов ключ, но има и по-прости начини на криптиране. Решавайки, кое точно устройство да си закупите, обърнете внимание и на този параметър - някои производители на безжични комуникационни устройства, с цел поевтиняване на изделията си, използват по-прости алгоритми за кодиране.

2.4 Други безжични технологии: Bluetooth

Bluetooth. Тази безсмислена като превод дума (буквалния й превод е "син зъб") все по-често се среща в материалите, посветени на компютрите. Най-вероятно вие знаете, че става дума за технология, чрез която се изграждат безжични мрежи, в които могат да участват не само компютри,

но и други устройства - например мобилни телефони или дори апарати от домашния ни интериор - печки, хладилници...

Технологии за безжично свързване са били разработвани и преди Bluetooth, но по една или друга причина нито една от тях не е получила широко разпространение. От друга страна, има причини, който не позволяват на Bluetooth да увеличи своя дял при текущо използваните интерфейси. Ето някои от тях:

- висока (засега) производствена цена на необходимата за функционирането на интерфейса елементна база
- липса на добра поддръжка на ниво операционна система (може да бъде решено с написване на драйвери)
- липса на интерес от страна на производителите да предлагат устройства с Bluetooth интерфейс
- нерешени проблеми със запазването на неприкосновеността на обменяните между устройствата данни (лесно се прихващат и декодират от разстояние)
- ниска скорост на предаване на данни
- малък обхват на устройствата

Фиг. 2.3.

От друга страна, има предимства, които може би ще помогнат на тази технология да си изгради добро бъдеще (на Bluetooth в сегашния му вид или на негов наследник, изчистен от недостатъците на предшественика):

- добре обмислена структура

- неотклонно намаляваща цена на хардуерния модул (едночипово решение)
- поддръжка от страна на консорциум, основан през 1998 г, със свободно безплатно членство, в който членуват над 2000 компании, между които IBM, Intel, Nokia, Erricson, Toshiba, 3COM, Lucent, Microsoft.

Конструктивно, най-грубо погледнато, Bluetooth-устройството представлява хардуерен модул (обособен или интегриран, изпълняващ функциите на радиопредавател/приемник под управлението на драйвер. Приемо-предавателят според спецификациите трябва да работи в честотния диапазон от 2400 - 2483,5 MHz, който е свободен за използване в повечето държави и не изисква лицензиране. Съществуват държави като Франция и Япония, в които част от този диапазон се използва и за други цели, там диапазонът за тези устройства е стеснен до 2445-2475 MHz (Испания), 2446,5-2483,5 (Франция).

Ericsson Bluetooth модул

Фиг. 2.4.

Разстояние, на което могат да се отдалечат две устройства е около 20-30 метра (типичното разстояние обикновено не надвишава 10 метра), но се работи по удължаването му. В замяна на това, няколко Bluetooth устройства могат да се свържат в мрежа и през стена (стени) или на няколко етажа в една сграда, без да има необходимост от пряка видимост или външна антена, по същия начин, по който могат да се свързват IEEE 802.11 устройствата. Широчината на канала е 723,2 Kb/sec. за устройства, работещи в асинхронен режим, и 433,9 Kb/sec. за работещите в синхронен режим. Когато по канала е се предават данни, могат да бъдат предавани 3 аудиоканала, като всеки едни от тях поддържа 64 Kb/sec. синхронен пренос. Допуска се съставен сигнал от данни и аудио.Bluetooth има и

друга, отличваща го от останалите технологии особеност: различните Bluetooth устройства влизат в контакт едно с друго автоматично, веднага след като попаднат в обсега на приемо-предавателя, а за установяването на връзката, аутентификацията и др. се грижи програмното осигуряване.

Запознаването със спецификациите на Bluetooth стандарта, версия 1.1, официално излязла на 1 декември 2000 г. (първите спецификации на стандарта са от октомври 1998 г.), отнема доста време да се запознаеш с нея, като се има предвид, че само публичния документ е съставен от 1084 страници. Но ето някои данни ...

Едно от големите предимства на Bluetooth е, че устройството, поддържащо стандарта, влизайки в обхват може да установи връзка не с едно, а с множество други, поддържащи тази технология, като не е задължително те да си взаимодействат активно.

Устройство, обменящо активно информация с други устройства, според терминологията на Bluetooth се нарича ***master*****,** а устройствата, с които то комуникира активно се наричат ***slave*****,** като максималния брой slave устройства може да бъде 7. Освен това може да съществуват още неограничен брой неактивни slave устройства, които са установили връзка с него, макар, че са синхронизирани с master, не обменят данни с последния, очаквайки освобождаване на свободно място, за да осъществят преноса на данни. Такъв тип връзка между устройствата се нарича ***piconet.*** В рамките на една piconet връзка може да има само едно master устройство, но когато е необходимо, свързаното с него slave може да смени статуса си на master, образувайки своя pinocet структура. Този тип сложна съставна структура носи наименованието ***scatternet*****,** в която всяко едно устройство може да бъде едновременно и master и slave, в зависимост от конкртената ситуация и мястото му в структурата.

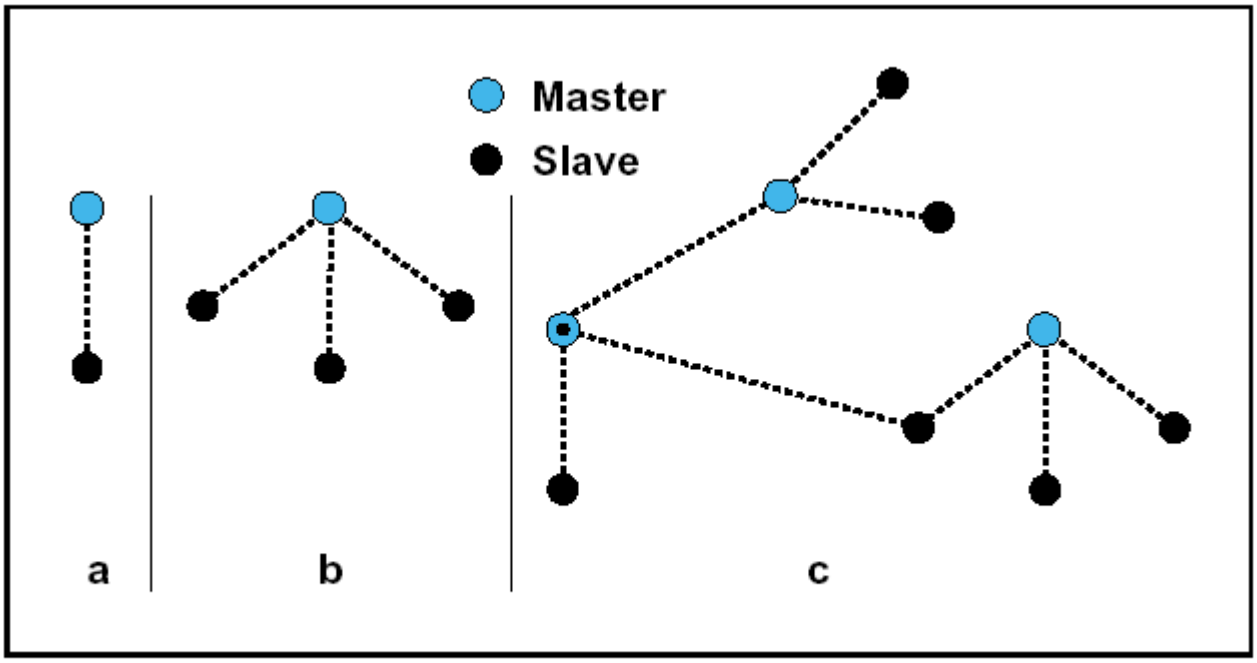


Figure 1.2: Piconets with a single slave operation (a), a multi-slave operation (b) and a scatternet operation (c).

Фиг. 2.5.

По този начин една scatternet мрежа от Bluetooth устройства е един, образно казано, динамично променящ се организъм, преобразуващ структурата си според текущите нужди (в зависимост от това, към кои точки от мрежата се комутират новите устройства). Разбира се, за да се избегне дублирането на устройствата и други нежелани отклонения, всяко устройство, освен уникалното си име, взаимодейства с другите, използвайки различен канал за връзка, на различна честота и с различен от другите параметър hopping, характеризиращ hopping channel (хопинг-канал). Хопинг (hopping)-това е периодична промяна на честотата, определяна от параметъра hopping sequence. Ето какво представлява най-просто казано процеса установяване на връзка на ново устройство, попаднало в обхвата на друго (други) Bluetooth устройства. Първоначално всяко Bluetooth устройство, попадайки в някакво пространствено положение, извършва претърсване на каналите за свързване, търсейки други устройства. Този режим носи името Device Discovery, и, в зависимост от това, в кой от описаните режими се намират евентуално откритите устройства, се установява или не връзка. Тези устройства може да се намират в няколко режима:

- discovery mode-устройствата, работещи при този режим се намират в готовност да приемат установяващите връзка процедури.

- limited diskoverable mode-при този режим устройствата приемат връзката само при спазване на някои условия (например ограничено време).
- non-discoverable mode-този режим се използва, когато устройствата не трябва да приемат нови запитвания.

Фиг. 2.6.

Освен всичко това, устройствата, намиращи се в някои от първите два режима могат да пребивават и в connectable или non-connectable mode. Ако устройството е в първия mode, устройствата разменят служебна информация, настройвайки специфични параметри на връзката помежду им.От друга страна при положение, че устройството е във втория mode, то може да бъде открито от участници в сеанса, но не позволява установяване на някои параметри на връзката и респективно, приемането и предаването на данни.

На следващия етап се извършва прочитането на имената на всички достъпни Bluetooth устройства. Според спецификациите, освен, че разполага с уникален мрежов адрес, всяко устройство на ниво потребител оперира със собствено име. Името на устройството може да бъде с дължина до 248 байта, като не задължително то да бъде уникално в рамките на една мрежа от Bluetooth устройства.

Bluetooth устройствата имат много ценно свойство, определено от спецификациите, което му позволява автоматично, при установена връзка с друго устройство, автоматично да се включи към списъка с предоставените от последното (или последните) услуги. За това се "грижи" протоколът Service Discovery Protocol (SDP).

Последното нещо, върху което бих искал да се спра, е болният въпрос със защитата на данните. Технологията за защитата им е вградена в самия протокол, като съществуват три режима за защита:

1. Security mode 1 (non secure) - устройството няма право да активира защитни механизми.
2. Security mode 2 (service level enforced security) - устройството не активира защитни механизми, докато не бъде свързано с друго, след което механизмът за защита се активира в съответствия с типа и изискванията на използваните служби.
3. Security mode 3 (link level enforced security) - защитният механизъм се активира още по време на установаване на връзката, като ако някое от устройствата не отговаря на изискванията, то няма да може да се свърже.

Security mode 2 и 3 могат да се използват съвместно, което още увеличава нивото на защита, като основата за най-високата степен на защита в Security mode 3 е сеансовият ключ, или Bond. Сеансовият ключ се генерира в процеса на свързване на двете устройства, и се използва за идентифициране и криптиране на данните. Макар че системата за защита на стандарта Bluetooth използва множество известни и специфични методи за защита, очебийно е това, че съществува възможност за прихващане на трафика и разшифроването на данните впоследствие - нещо, което е един сериозен недостатък на безжичните комуникации и кето трябва да се има предвид.

Въпреки ниските скорости на трансфер, интерфейсът Bluetooth си има и своите положителни страни. От една страна, това е лесният начин за връзка между отделните устройства, не изискващ сложни настройки и някакви специални познания от страна на потребителя. От друга - при невъзможност да се изгради мрежа между два компютъра (или някакви други две устройства с интерфейс Bluetooth) по друг начин, този интерфейс позволява безжичен пренос на данни между тях, и то на разстояние минимум 10 метра.

Не трябва да изпускаме от поглед и другите възможни сфери на приложение на устройтвата с този интерфейс. Това са, например, вече съществуващите безжични гарнитури с Bluetooth интерфейс за мобилмите телефони, снимка на която има в началото на статията. Някои производители се опитват да проправят път на пазара, предлагайки първите мишки и клавиатури с такъв интерфейс, а съм срещала данни за прототипи на ново поколение битови уреди, използващи интерфейса за връзка с централния команден център на едно ново "умно" жилище от близкото бъдеще.

Дали ще се наложи този интерфейс? В света на компютърните технологии това може само да се предполага. Факт е, че големите производители на дънни платки като MSI и EpoX имат продукти с вграден

интерфейс Bluetooth, множество модели GSM апарати, PDA и преносими компютри - също, говори за нарастващия интерес от страна на производителите, които понякога също участват в прогреса. Рано е още да се говори за реакция на потребителите, които често консумират това, което производителите им го предлагат, дори и без да го искат целенасочено. Така или иначе, малко по малко Bluetooth набира инерция, и, както често се получава в света на компютърните технологии, при излизането на следващата, по-бърза и защитена версия, най-вероятно ще стане това, което всички биха искали, и ще си осигури добро бъдеще. Ако, разбира се, другите безжични технологии не го изпреварят.....

ЗАКЛЮЧЕНИЕ

Безжичните мрежи са лесни и рентабилни за изграждане. Повишавайки мобилността и гъвкавостта на мрежовите потребители те са привлекателна алтернатива на кабелните мрежи. Безжичните локални мрежи намаляват разходите свързани с инсталацията и поддръжка на мрежата и повишава производителността на персонала. Съществува голямо разнообразие от топологии и конфигурации, от връзка между две устройства до сложен дизайн поддържащ много на брой потребители.
Мрежовите потребители в една фирма обикновено са свързани към локална мрежа за да имат достъп например до интернет, електронната си поща, онлайн услуги или обща информация. Чрез безжичните решения потребителите могат да имат достъп до тези мрежови услуги без да е необходимо да търсят място за включване в кабелната мрежа. В същото време компаниите могат да изграждат нови или да разширяват съществуващите мрежи без да се налага да инсталират или да преместват

кабели. Безжичните локални мрежи много предимства в сравнение с траидиционните кабелни мрежи
Безжичната локална мрежа е информационна комуникационна система, която приема и предава данни по въздуха като използва радио технологии. Безжичните локални мрежи се използват както в компаниите така и в домашна обстановка. Те могат да бъдат разширение към съществуващата мрежа или в по- малките фирми като алтернативен заместник на кабелните мрежи. Те осигуряват всички предимства и характеристики на традиционните технологии за локални мрежи като Ethernet или TokenRing без ограниченията от инсталиране на нови кабели. По този начин безжичните локални мрежи позволяват на компютърните потребители да имат връзка с мрежата навсякъде в рамките на сградата.

ЛИТЕРАТУРА

1. Хънт, К. Linux Мрежови съвъри. С., Софтпрес,2003;
2. Комър,Б. TCP/IP Мрежи и администратиране. С., ИнфоДАР, 1999;
3. http://www.dhstudio.eu
4. http://linux-bg.org/
5. Комър,Б. TCP/IP Мрежи и администратиране. С., ИнфоДАР, 1999;