МОДУЛ ЗА ДИСТАНЦИОННО ОБУЧЕНИЕ

по дисциплината „КОМПЮТЪРНИ МРЕЖИ”

Иван Цонев

Шумен
2013

ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ

ВКК – вторични кадри с дължина „К” бита
ДИКМ – диференциална импулсно-кодова модулация
ДМП – демултиплексор
ИКМ – импулсно-кодова модулация
ИОВ – информационна обратна връзка
КВ – комуникационен възел
КК – комутатор на каналите
КК – комуникационен канал
КМ – комуникационна мрежа
КОВ – комбинирана обратна връзка
КП – комутация на пакетите
КС – комуникационна система
КЧ – крайна част
МВ – междинни възли
МОС – мрежова операционна система
МП – мултиплексор
МРК – модифициран разширен канал
МС – мрежов слой
ОВ – обратна връзка
РК – разширен канал
РОВ – решаваща обратна връзка
СС – сесиен слой
ТК – телекомуникация
ТС – транспортен слой
ФС – физически слой
ЦК – цифров канал
AAL – ATM Adaptation Layer
AFP –Apple Talk Filing Protocol
AH – Authentication Header
AMI – Alternative Mark Inversion
AP – Access Point
API - Application Programming Interface
ARP – Address Resolution Protocol
ASN 1 – Abstract Syntax Notation
ASP – Apple Talk Session Protocol
ATM – Asynchronous Transfer Mode
ATP – Apple Talk Transaction Protocol
BDC – Backup Domain Controller
BSS – Basic Service Set
CBR – Constant Bit Rate
CHAP – Challenge Handshake Authentication
CIPE – Crypto IP Encapsulation Protocol
CIR – Committed Information Rate
CLP – Cell Loss Priority
CMIP – Common Management Information Protocol
CS – Convergence Sub layer
CSMA/CD – Carrier Sense Multiple Access / Colision detection
CXML – Commerce Extensible Mark up Language

DCE – Data Circuit Terminating Equipment
DDP – Datagram Delivery Protocol
DES – Data Encryption Standard
DHCP – Dynamic Host Configuration Protocol
DNS – Domain Name System
DSAP – Destination Service Access Point
DSDV – Digital Simultaneous Data and Voice
DSP – Data Stream Protocol
DTE – Data Terminal Equipment
DTP – Distributed Transaction Processing
DVR – Distance Vector Routing
EAP – Extensible Authentication Protocol
EP – Echo Protocol
ESP – Encapsulating Security Pay load
FCS – Frame Check Sequence
FDDI – Fibre Distributed Data Interface
FDM – Frequency Division Multiplexing
FR – Frame Relay
FTAM – File Transfer, Access and Manipulation
FTP – File Transfer Protocol
GFC – Generic Flow Control
GRE – Generic Routing Encapsulating
HDB – High Density Bipolar
HDSL – High Bit Rate Digital Subscriber Line
HEC – Header Error Check
HTML – Hyper Text Mark- up Language
IDN – Integrated Digital Network
IEC – International Electrotechnical
IEEE – Institute for Electrical and Electronics Engineering
IETF – Internet Engineering Task Force
ISO – International Standardization Organization
ITU – International Telecommunication Unit
IGRP – Interior Gate Way Routing Protocol
IKE – Internet Key Exchange
IMAP 4 – Interactive Mail Access Protocol Version 4
IP – Internet Protocol
IPX – Internet work Packet Exchange
IPSec – IP Security
IRC – Internet Relay Chat
ISDN – Integrated Service Digital Network
ISP – Internet Server Provider
ITU – International Communication Union
JTM – Job Transfer and Manipulation
LAC – L2TP – Enabled Access Concentrator
LAN – Local Area Networks
LAPB – Link Access Protocol – balanced
LCI – Logic Circuit Identifier
LCP – Link Control Protocol
LLC – Logic Link Control
L2F – Layer 2 Forwarding

L2TP – Layer 2 Tunnelling Protocol
MAC – Media Access Control
MAN – Metropolitan Area Networks
MAU – Multi station Access Unit
MMC – Microsoft Management Console
MMS – Manufacturing Message Specification
MNP – Micro com Networking Protocol
MOTIS – Message Text Interchange Standard
MPLS – Multi protocol Label Switching
MTU – Maximum Transport Unit
NAT – Network Address Translation
NBR – Name Banding Protocol
NCP – Network Core Protocol
NDS – Nowell Direktory Services
NLSP – Netware Link Service Protocol
NMC – Networking Management Centre
NNI – Network – Network Interface
NNTP – Network News Transport Protocol
NRZ- L – Non Return to Zero Level
NRZ1 – Non Return to Zero, Invert to Ones
NSAP – Network Service Access Point
OAM – Operation and Maintenance
OBI – Open Buying on the Internet
ODI – Open Data Link Interface
OMC – Operation and Maintenance Centre
OSI – Open System Interconnection
OSPF – Open Shortest Path First
PAC – PPTP Access Concentrator
PAP – Password Authentication Protocol
PAP – Printer Access Protocol
PCM – Pulse Code Modulation
PDC – Primary Domain Controller SAM
PDH – Plesiochronous Digital Hierarchy
PDU – Protocol Data Unit
PMD – Physical Media Dependent
PMI – Physical Media Independent
PNS – PPTP Network Server
POP 3 – Post Office Protocol – Version 3
PP – Post Script Protocol
PPP – Point to Point Protocol
PPTP – Point to Point Tunnelling Protocol
PSN – Packet Switched Node
PVC – Permanent Virtual Circuits
QAS – Quality of Service
RARP – Reverse ARP
RAS – Remote Access Server
RDA – Remote Database Access
RIP – Routing Information Protocol
RNR – Receive Not Ready
RR – Receive Ready

RTMP – Routing Table Maintenance Protocol
SAM – Security Accounts Management
SAP – Service Access Point
SAR – Segmentation and Reassembly
SDH – Sinchronous Digital Hierarchy
SFTP – Simple File Transfer Protocol
SLA – Service-level Agreement
SLIP – Serial Line Internet Protocol
SM – Statistical Multiplexing
SMBs – Server Message Blocks
SMT – Station Management
SNTP – Simple Mail Transfer Protocol
SPX – Sequence Packet Exchange
SSAP – Source Service Access Point
SSH – Secure Shell
STA – Spanning – Tree Algorithm
SVC – Switched Virtual Circuits
SVN – Secure Virtual Networking
TC – Transmission Convergence
TCP – Transmission Control Protocol
TDM – Time Division Multiplexing
TELNET – Terminal Hetworking
TFTP – Trivial FTP
TMN – Telecommunication Management Network
TTPT – Target Token Ring Time
UDP – User Datagram Protocol
UNC – Universal Naming Convention
UNI – User – Network Interface
VBR – Variable Bit Rate
VCI – Virtual Channel Identifier
VPI – Virtual Path Identifier
VPN – Virtual Private Networks
VT – Virtual Terminal
WAN – Wide Area Networks
WEP – Wired Equivalent Privacy
WECA – Wireless Ethernet Compatibility Alliance
WLAN – Wireless Local Area Network
WWW – World Wide Web
XML – Extensible Mark up Language
ZIP – Zone Information Protocol

ВЪВЕДЕНИЕ

Телекомуникацията е една от най-бързо развиващите се предметни области през последните 20 години. Изградените комуникационни мрежи до деветдесетте години на миналото столетие претърпяха кардинални промени и развитие. Благодарение на това развитие се създаде възможност за високоскоростно предаване на големи обеми от данни на големи разстояния.

Едно от най великите достижения на миналия век е глобалната компютърна мрежа Internet. Милиони компютри са включени в тази и други глобални компютърни мрежи, обхващащи всички континенти на Земята и близкия космос. Създадена беше възможност за бърза информационна връзка между жителите на планетата.

Учебната дисциплина "Компютърни мрежи" има за цел да се дадат на студентите от техническите висши учебни заведения базови знания по теоретичните основи за изграждането и функционирането на компютърните мрежи. В настоящия модул са разгледани особеностите на различни мрежови операционни системи и възможностите за управление на апаратните и информационните ресурси на мрежите. Направен е преглед на популярните стандарти за изграждане на локални и глобални компютърни мрежи и са посочени техните специфични характеристики. Специално внимание е отделено на безжичните технологии за създаване на комуникационни мрежи. Описана е и технологията за изграждане на виртуални частни мрежи в средата на глобалните комуникационни среди. Компютърните мрежи са класифицирани по множество характерни признаци. Нивото на представените знания в учебника е съобразено с подготовката на студентите на ниво трети курс, обучаващи се в образователна квалификационна степен бакалавър.

В първа глава е направена класификация на компютърните мрежи. Използвани са показатели като: методът за администрация на мрежите; типът на използваната мрежова операционна система; протоколният стек на комуникационния модел; топологията на мрежата; архитектурата на компютърната мрежа.

Във втора глава са обосновани мрежови концепции и модели. Представени са различни методи за комуникация и предаване на данни в компютърните мрежи. Анализирани са различни методи за достъп до общия комуникационен канал в локалните компютърни мрежи.

В трета глава са представени различни мрежови операционни системи. Дадени са общите принципи на мрежовото администриране, споделянето на мрежови ресурси и управление на достъпа до тях. Анализирано е управлението на споделените мрежови ресурси. Разгледани са характеристиките на различни мрежови операционни системи.

Глава четвърта е посветена на локалните компютърни мрежи (LAN). Направена е обосновка и класификация на тези мрежи и са представени различните топологии за изграждане. Разгледани са различните стандарти за изграждане на LAN и са описани в голяма степен физическите и каналните им слоеве: IEEE 802.3. (Ethernet), IEEE 802.4. (Token Bus), IEEE 802.5. (Token Ring), IEEE 812.3. (100 VG-AnyLAN). Специално внимание е отредено на безжичните радиомрежи, изградени по стандарт 802.11. Представени са информативно и протоколните стекове, касаещи изграждането на горните слоеве на LAN: NetWare (SPX/IPX) на фирма Novell и AppleTalk на фирма Apple. Разгледани са виртуалните частни компютърни мрежи като ефективно решение на фирмите и организациите за ефективно и конфиденциално управление. Обосновани са протоколите за изграждане на VPN мрежите. Проведено е изследване на локална компютърна мрежа на три нива. В графичен вид са представени резултатите от изследването и са направени изводи и препоръки, необходими за практиката.

В пета глава са разгледани глобалните компютърни мрежи (WAN). Направени са обосновка и описание на стандартите за изграждане на WAN. Представени са стандартите: X.25., Frame Relay, ATM, ISDN и B-ISDN. За всички стандарти са разгледани особеностите

на слоевете от отворения модел за комуникации. По-подробно са разгледани приложените в различните стандарти методи за избор на маршрута на протоколните единици през комуникационната среда. Проведено е изследване на структурата на глобалната компютърна мрежа на Шуменския университет "Епископ Константин Преславски". Изследвани са параметрите на мрежата и са направени изводи и препоръки за нейното бъдещо развитие.

Шеста глава е посветена на междумрежовите комуникации. Разгледани са междумрежовите съгласувания на долните и горните слоеве на отворения модел за комуникации. Представен е начинът на включване на устройства като повторители, концентратори, комутатори, модеми, мостове, маршрутизатори и шлюзове. Повече данни и описание са направени за модемите. Направена е обосновка на виртуалните частни мрежи, изградени в средата на Internet. Анализирана е структурата на тези мрежи и са представени основните протоколи за изграждането им.

Съдържанието на модула е изложено на базата на научни изследвания, публикации, и лекции, които авторът е провеждал със студенти по информатика, по математика и информатика, по комуникационни и информационни системи, по сигнално-охранителни системи и технологии и по радиолокационна техника и технологии от Факултета по математика и информатика и Факултета по технически науки на Шуменския университет „Епископ Константин Преславски".

Изложеният материал може с успех да се ползва от студентите на Факултета по технически науки и Факултета по математика и информатика на Шуменския университет „Епископ Константин Преславски", обучаващи се по специалностите: „Информатика", „Математика и информатика", „Комуникационни и информационни системи", „Радиолокационна техника и технологии", „Радиокомуникационна техника и технологии" и „Сигнално-охранителни системи и технологии". Съдържанието е подходящо и може да е полезно и за студентите от университетските специалности „Физика", „Астрономия", „Туризъм", „Журналистика", както и за всички, които проявяват интерес към компютърните мрежи и комуникации.

Книгата може да се използва и от други, желаещи да се запознаят с архитектурата и стандартите за изграждане на различните видове компютърни мрежи.

Изложеният материал не е достатъчен за цялостното и всеобхватно изучаване на компютърните мрежи. За по-задълбочено изучаване на процесите на компютърните комуникации и мрежи е необходимо придобиване на допълнителни знания, прочитане на допълнителна литература. Затвърждаване и задълбочаване на знанията и уменията за работа с компютърните мрежи може да се придобият след провеждане на предвидените упражнения по дисциплините "Предаване на данни и компютърни комуникации" , „Компютърни мрежи" и „Администриране на компютърни мрежи".

Изказвам моите най-сърдечни благодарности към научния редактор доц. д-р инж. Станимир Станев и рецензентите проф. дтн инж. Борислав Беджев и проф. дтн инж. Христо Лалев за внимателното прочитане на ръкописа и направените, важни забележки и препоръки.

Предложения и бележки по съдържанието се приемат по електронната поща на автора: tsonev@shu-bg.net.

Авторът

ГЛАВА 1. КЛАСИФИКАЦИЯ НА КОМПЮТЪРНИТЕ МРЕЖИ

Класификацията на компютърните мрежи може да се направи по различни параметри и критерии. Специалистите в тази област разглеждат основно физическите свойства на мрежите и използваното базово и приложно програмно осигуряване. Класификацията на компютърните мрежи може да се извърши на базата на следните характеристики [35]:

- Физически обхват на мрежата.
- Метод на администриране.
- Използвана мрежова операционна система.
- Използвани мрежови протоколи.
- Реализирана топология на мрежата.
- Архитектура на мрежата.

Всяка от изброените характеристики има своята степен на въздействие върху облика, параметрите и възможностите на компютърната мрежа. В зависимост от условията за реализация и предназначението на мрежата се предпочитат една, друга или в съчетание представените по-горе характеристики.

1.1. Класификация на компютърните мрежи в зависимост от обхвата на мрежата

В тази класификация се отчитат параметри като размера на територията, в която е разположена мрежата, броя на потребителите и количеството и разположението на компютрите. Доминираща характеристика за тези мрежи е размерът на географската област, в резултат на което са приети следните три вида:

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

Параметрите на локалните компютърни мрежи приемат стойности в доста широк диапазон. По отношение на броя на компютрите една локална мрежа може да има в състава си от два до стотици компютри. Тя може да е разположена в една стая, офис, на един етаж, в един или няколко корпуса. Големите по размер и брой компютри се управляват трудно и могат да се разделят на обособени работни групи. Потребителите в работните групи имат общи интереси в съответствие със структурата на ведомството, като мрежи на отдели: «Човешки ресурси», «Маркетинг», «Продажби», «Финанси», «Логистика» и др. Свързаните групи от локални мрежи образуват по-големи мрежи – като градските и глобалните.

Градските компютърни мрежи, както подсказва името, са разположени на територията на един по-голям град. Такава мрежа може да се състои от няколко локални мрежи – на областната управа, на общината, висшето училище, полицията, болницата и др. Градските мрежи се реализират много рядко, повечето от тях се категоризират като глобални мрежи. Прието е максималното разстояние, на което могат да са най-отдалечените компютри в тези мрежи, да е до 80 км.

Глобалните компютърни мрежи са разположени в големи географски области. Те могат да са разположени на територията на една държава, континент, на повече от един или всички континенти. Най-голямата глобална компютърна мрежа на земното кълбо е Интернет. Глобалната компютърна мрежа се състои от множество взаимносвързани локални мрежи. От свързването на много локални мрежи се получава интермрежа, която е прието да се нарича интернет. Когато думата интернет започва с малка буква, се визира множество свързани

локални мрежи. Ако започва с главна буква, се има предвид глобалната световна мрежа, която се нарича Интернет. От термина интернет произхождат нарицателните интранет и екстранет. Интранет е ведомствена компютърна мрежа, в която абонатите използват едни и същи протоколи и технологии. Екстранет мрежата използва интернет технологии за отдалечен достъп на абонатите до ресурсите на ведомствената мрежа.

Глобалните мрежи обикновено използват изградената обществена комуникационна среда. Някои елементи на комуникационата среда, където изискванията са високи, се изграждат целево за предаване на данни с висока скорост. За разлика от локалните мрежи не всички комуникационни линии в глобалните мрежи са постоянно свързани. Съществуват множество временни комуникационни линии, които се изграждат в зависимост от текущите нужди при обслужването на абонатите (dial-up). Използват се както обществената комуникационна среда, така и специално изградени линии.

От друга гледна точка глобалните мрежи могат да се разделят на два вида – разпределени и централизирани. Разпределени са тези мрежи, които нямат обособен център за управление. Такава е глобалната световна мрежа Интернет. Централизираните мрежи имат централен сървър и офис за управление, към който са включени всички компютри от мрежата.

Тези мрежи се наричат още маршрутизирани мрежи. За да могат съобщенията да преминават от една локална мрежа в друга, се използват устройства, наречени маршрутизатори (Ruters).

1.2. Класифициране на компютърните мрежи по метода на администриране

В зависимост от приложения метод за управление на апаратните и информационни ресурси компютърната мрежа може да се изпълни по три начина:

- Компютърна мрежа с равноправен достъп (peer to peer).
- Компютърна мрежа тип „клиент/сървър”.
- Комбиниран тип компютърна мрежа.

Компютърна мрежа с равноправен достъп е тази, в която всички компютри функционират като клиент и като сървър едновременно. Всеки потребител администрира ресурсите на своя компютър.

Фиг. 6.1. Компютърна мрежа с равноправен достъп

В компютърни мрежи с равноправен достъп – фиг.6.1, всички участници са равнопоставени и в един момент един компютър може да действа като сървър, а в друг – като

клиент. Достъпът до общите мрежови ресурси не се администрира от отделен сървър, както е при мрежите тип клиент/сървър. Този тип мрежи се използва, когато броят на компютрите е сравнително малък и няма нужда от централизирано съхраняване на файлове и мрежови приложения. Поддръжката на този тип мрежа е вградена във всички версии на мрежовите операционни системи на Microsoft: Windows 95, 98, 2000 и XP, включително и в Home edition. Към другите предимства на този тип мрежи може да се отнесат: ниската цена на изграждане; лесното администриране на всеки отделен компютър (възел); липсата на необходимост от мрежов системен администратор, който би трябвало да се грижи за конфигурирането и администрирането на мрежата.

Компютърна мрежа от типа клиент/ сървър се администрира централно от специален сървър, в който е инсталирана мрежова операционна система. В този тип мрежи достъпът на потребителите до мрежовите ресурси се разрешава с оторизация посредством потребителско име и парола за достъп.

В мрежите тип клиент/ сървър – фиг. 6.2 – предназначението на отделните машини е строго дефинирано. В момента на генериране на мрежата се определят един (или няколко) сървър(а), управляващ(и) достъпа до ресурси и услуги на свързаните към него работни станции. На сървъра могат централизирано да се съхраняват файлове и приложения, достъпни за използване от всеки компютър, което предполага, че ако сървърът е включен, всеки от компютрите клиенти може да получи достъп до файловете във всеки един момент. Нивото на сигурност в една машина от този тип може да бъде относително лесно повишено благодарение на централизираното управление, обикновено извършвано от мрежовия администратор, който освен това може да се грижи и за централизирано архивиране на данните, инсталирането на приложения, администрирането на потребителите и т.н. Мрежите от този тип, освен че са по-бързи от мрежите с равноправен достъп, позволяват включването на повече устройства (не само компютри, но и мрежови принтери и др.). Достъпът до мрежовите периферни устройства е по-бърз, отколкото при мрежите с равноправен достъп.

Фиг. 6.2. Компютърна мрежа тип клиент/сървър

От друга страна, оборудването за изграждане на този тип мрежи е в пъти по-скъпо в сравнение с мрежите с равноправен достъп. За изграждането и администрирането им е необходим мрежов администратор, който, освен всичко друго, трябва да се занимава и с въпросите на сигурността, особено ако мрежата е свързана към Интернет или към друга глобална компютърна мрежа.

Комбиниран тип мрежи – фиг.6.3, е комбинация от горните два типа – мрежа с равноправен достъп и мрежа клиент/сървър. Много често поради спецификата на задачите, които се изпълняват в рамките на една организация, този тип мрежи е за предпочитане. Една

обособена част от мрежовите устройства, създадени като работна група, образуват мрежа с равноправен достъп, в която ресурсите се споделят между тях, без да се ангажира сървърът. Същевременно същите компютри са свързани и към сървър, който е част от мрежа тип клиент/сървър. Така, от една страна, сървърът контролира първостепенните ресурси, необходими на цялата мрежа, а от друга, не отделя ресурси за управлението на устройства, необходими за работата само на компютрите от работната група, свързани в мрежа с равнопоставен достъп.

Фиг. 6.3. Комбиниран тип компютърна мрежа

В зависимост от предназначението на мрежата се избира един от двата типа локални компютърни мрежи. Факторите, които оказват влияние върху избора на типа на мрежата, са броят на компютрите и потребителите, изискванията за сигурност, квалификацията на персонала и наличният бюджет на фирмата или ведомството.

Предимствата на компютърните мрежи с равноправен достъп са следните: по-ниска себестойност; не се изисква специална мрежова операционна система за сървър; не е необходим администратор на мрежата. Недостатъците на мрежата са: администрирането на мрежи с голям брой работни места е трудно; операторите на работните места трябва да имат умения по администриране на ресурсите на компютрите; малки гаранции за сигурността на ресурсите; компютрите, които обменят ресурси, намаляват производителността на мрежата.

Предимствата на мрежи тип клиент/ сървър са следните:

- по-висока сигурност на ресурсите;
- по-лесно централно администриране;
- файловете за общо ползване се записват в постоянната памет на сървъра.

Недостатъците на този тип мрежи са следните:

- изисква се скъпа мрежова операционна система;
- необходимо е закупуване на сървър с добри параметри и на висока цена;
- изисква се назначаване на подготвен мрежов администратор;
- при повреда на сървъра мрежата престава да функционира.

Сървър се нарича компютър със значителни апаратни и информационни ресурси, които могат да се отдават на останалите компютри от мрежата. Към сървърите се свързват и периферни устройства (принтер, плотер, скенер и др.), които също се предоставят на останалите работни станции. Сървърите са инструмент за управление и не се използват за изпълнение на рутинните за мрежата производствени задачи.

Работната станция (клиентът) е компютър, който не отдава своите ресурси на останалите и ползва споделените ресурси на сървъра.

За да се осъществи достъп до ресурс в компютърната мрежа, е необходимо той да бъде споделен (shared) и да му се присвои споделено име (share name). Името се използва от компютрите в мрежата като идентификатор на споделения ресурс. Не е задължително името за идентификация да е същото, както на споделения ресурс. Ако във файловата система има папка с име Potrebiteli, която трябва да се сподели със студенти при провеждане на упражнения от група с номер едно, може да й се даде име studentgrup1. Studentgrup1 е името на папката, която потребителите ще виждат, когато разглеждат мрежата, и ще се използва това име, за да се установи връзка със споделения ресурс. Някои мрежови операционни системи позволяват споделените ресурси да се публикуват в директория (Active Directory в Windows 2000). Това дава възможност на потребителите да откриват споделените ресурси, без да се интересуват къде са инсталирани физически.

Всеки компютър, който споделя своите ресурси, може да се нарече сървър. Този термин се използва за именуване на компютри, които споделят своите файлове, приложения и периферни устройства. Сървърът е мощен компютър с много бърз процесорен блок и значителна по обем оперативна и постоянна памет. Тези компютри по правило не се използват за решаване на ежедневни задачи. Достъпът до сървъра е привилегия на мрежовия администратор, който го използва за управление, наблюдение и поддържане на мрежата. В големите компютърни мрежи сървърите се специализират по отделни ресурси като: файлов сървър; приложен сървър; принт сървър; Logon сървър; Web сървър; Mail сървър; Telnet сървър; терминален сървър; телефонен/факс сървър; клъстерен сървър; прокси сървър; BOOTP сървър; DNCP сървър; сървър за преобразуване на имена.

Файловият сървър се използва за записване и съхранение на файлове с данни. Потребителите на мрежата записват данните на твърдия диск на сървъра, а не на дисковете на своите работни станции. Файловете, записани на диска на сървъра, се намират лесно от потребителите, могат да се архивират и има по-големи гаранции за сигурност.

Принт сървърът е компютър, който управлява един или няколко принтера за колективно ползване. Към тези принтери потребителите в мрежата изпращат готовите документи за отпечатване.

Приложният сървър е компютър, на който са инсталирани мрежови приложения. Потребителите изпълняват приложенията, без да са инсталирани в локалните дискове на работните им станции.

Logon сървърът съхранява база от данни за сигурност, която съдържа информация за потребителските акаунти. Сървърът проверява акредитивите на потребителите в базата данни за сигурност и контролира достъпа до мрежата и нейните ресурси.

Web сървърът изпълнява специален Web софтуер в комбинация с операционната система. Съвременните операционни системи имат вграден Web сървър и сървърния софтуер FTP (File Transfer Protocol) и NNTP (Network News Transfer Protokol).

Mail сървърът служи за управление на електронната поща. На неговия твърд диск се създават пощенски кутии на потребителите, в които се получава електронната поща. Електронните писма могат с помощта на специализиран софтуер да се изтеглят от компютрите на потребителите.

Telnet сървър е компютър, с който може да се установи dial-up връзка с отдалечена работна станция. Работната станция получава оторизиран достъп до ресурсите на мрежата, които са под управление на сървъра. Обикновено връзката се реализира по съществуващата инфраструктура и телефонни линии.

Терминалният сървър е под управление на софтуер, който разрешава на клиентите да изпълняват своите приложения на сървъра. Така евтините работни станции с ограничени

локални ресурси използват възможностите на сървъра за изпълнение на задачи, изискващи големи ресурси.

Телефонен/ факс сървърите изпълняват функции на телефонен секретар, гласова поща, пренасочват разговори и приемат и изпращат факсове между свързаните абонати.

Клъстерният сървър работи под управление на софтуер, който обединява ресурсите на множество сървъри, работещи паралелно. Формира се компютърен клъстер със значителни апаратни и информационни ресурси. Потребителите имат достъп до ресурсите на клъстера и могат да изпълняват значими по обем задачи.

Прокси сървърът е посредник между работните станции и глобалната компютърна мрежа Интернет. Сървърът извършва административен контрол, гарантира сигурност и предоставя услуги на клиентите. Прокси сървърът кешира интернет съдържания и по този начин облекчава натоварването на мрежата с повтарящи се заявки от абонатите.

BOOTP сървърът чрез протокола за първоначално зареждане стартира операционната система и компютрите на потребителите получават IP конфигурационна информация по мрежата.

DNCP сървърът конфигурира клиентите на мрежата и замества администратора, като присвоява уникални IP адреси на потребителските компютри.

Сървърът за преобразуване на имена поддържа съответствие между имена и IP адреси. Асоциираните имена с IP адреси позволяват на протоколите от стека TCP/IP да откриват компютрите в мрежата.

Терминът **клиент** се използва за означаване на компютър на потребител, периферно устройство или приложна програма, които осъществяват достъп до сървъри и сървърни програми. Клиентските операционни системи се инсталират по правило в работните станции, които са свързани като равноправни компютри в мрежата.

Работна станция е компютър на потребител, работещ под управление на клиентска операционна система. Тя може да се използва за изпълнение на приложни програми, които използват мрежови ресурси.

Хост е компютър, на който е присвоен собствен IP адрес и е свързан в мрежа, работеща под управление на протоколния стек TCP/IP.

Възелът е компютър или друго мрежово устройство, което съхранява за известно време протоколни единици и изпълнява комутационни или маршрутизиращи функции. Обикновено възелът не притежава потребителски интерфейс, а предоставя диагностичен интерфейс на мрежовия администратор или потребителя.

Структурата и архитектурата на мрежите с равноправен достъп е подходяща за локални мрежи до 10 абоната. Реализацията на тези мрежи е със сравнително ниска себестойност и лесна за изпълнение. Съвременните операционни системи (Windows, Linux) имат вградени мрежови функции и поддържат мрежите с равноправен достъп. За да участва в такава мрежа, компютърът се конфигурира за присъединяване към работната група чрез настройка на свойствата за работа в мрежа (Networking properties). На компютрите от работната група, които споделят ресурсите си, е необходимо да се присвоят еднакви имена.

Администрирането на потребителите и ресурсите на мрежите с равноправен достъп е децентрализирано. Всеки компютър от групата може да отдава своите ресурси и да ползва споделените ресурси на останалите. Потребителите на отделните работни места са отговорни за администрирането на ресурсите на своя компютър и за архивирането на данните. Когато броят на компютрите в мрежата е голям, потребителите се затрудняват в достъпа до споделените ресурси поради големия обем от имена, които абонатите на мрежата трябва да помнят.

Сигурността в мрежите с равноправен достъп се решава от потребителя на отделните работни места. В операционната система Windows сигурността се реализира с пароли на ниво споделен ресурс, а не на ниво потребител. Използват се множество различни пароли за

отделните потребители или някои от ресурсите се предоставят на свободен достъп за всички. Това създава дискомфорт за потребителите и несигурност в сравнение с централизираното администриране.

Компютърните мрежи, базирани на сървъри, са с централизирано управление от администратор. В тези мрежи най-малко един от компютрите работи под управление на мрежова операционна система от версиите Windows NT, Windows 2000 Server или NetWare. Потребителските акаунти се създават на сървърите от мрежовия администратор и той упражнява контрол на цялата мрежа от едно работно място. Работните станции са освободени от сървърни услуги и производителността на тези мрежи е значително по-голяма в сравнение с мрежите с равноправен достъп. Администрирането на тези мрежи е улеснено в голяма степен, тъй като споделените ресурси дори и в големите мрежи се намират на сървъра, където се намират и архивират с лекота. Изискването за мрежов администратор оскъпява поддържането на мрежата, но за сметка на това тези мрежи са по-сигурни и потребителите могат да ползват по всяко време компетентни консултации. За да се регистрира в мрежата и да ползва мрежов ресурс, всеки потребител получава валиден потребителски акаунт и парола, които са създадени на сървъра. Не е необходимо да се помнят от потребителите множество от потребителски акаунти за множество от компютрите в групите и пароли за различни споделени ресурси.

1.3. Класифициране на компютърните мрежи в зависимост от използваната мрежова операционна система

Мрежовата операционна система обосновава съществени особености на компютърната мрежа. Най-често използваните операционни системи за инсталация на сървърите и управление на мрежата са:

- Windows NT и Windows 2000
- NetWare
- UNIX.

Компютърните мрежи под управление на Windows операционна система се дефинират като *домейни*. Главният компютър се нарича *главен домейн контролер*, който съхранява файловете за четене или запис и базата от данни за управление на акаунтите за сигурност. Windows 2000 домейните са базирани на *Active Directory*, копие на която се съхранява на всеки домейн контролер и съдържа информация за акаунтите за сигурност и мрежовите ресурси. Една мрежа от този тип може да има няколко домейн контролера, като всеки от тях записва в базата данни на директорията. Всички Windows и MS-DOS операционни системи могат да са клиентски базов софтуер на Windows NT и Windows 2000. Macintoch и Linux също осъществяват достъп до ресурси на Windows сървъри при допълнително инсталиране на подходящи програми.

Мрежовата операционна система NetWare на Novell гарантира сигурност на ресурсите, като файлов сървър и принт сървър. Работните станции под Windows имат достъп до NetWare сървъри при инсталиране на подходящ клиентски софтуер. Създадена е клиентска програма Client32, която се инсталира на 32-битова операционна система Windows.

UNIX мрежовата операционна система е разработена и предложена през 1969 г. от Bell Labs и апробирана в ARPAnet, която се счита за предшественик на Интернет. Това е мощна операционна система с отворен код и има много разновидности. Операционната система Linux е безплатен вариант на Unix, която се предлага в много версии като RedHad, Caldera и Corel.

Голяма част от съвременните компютърни мрежи могат да се определят като хибридни, тъй като работят под управление на софтуер, разработен от различни производители. Използват се множество от протоколи и комбинации на домейни и работни групи. Компютърна мрежа под управление на Windows NT домейн контролер може да има NetWare файлов сървър, до който клиентите да имат достъп, както и Unix сървър за услуги Web хостинг. Повечето създатели на операционни системи предлагат допълнителни модули за взаимодействие между различното базово програмно осигуряване. Пример за програмна интероперативност са:

- Client Services for NetWare and Gateway Services for NetWare (GSNW) – позволява на клиенти, използващи софтуер на Microsoft, да осъществяват достъп до NetWare сървъри. Достъпът до NetWare ресурси се реализира с посредничеството на шлюзове, които се инсталират на Windows сървърите.
- File and print services for NetWare – разрешава на клиентите на NetWare сървър да ползват ресурси на Windows сървър.
- Services for Macintosh – позволява на Macintosh компютри да осъществяват достъп до файлове и принтери в Windows мрежи.
- Systems Network Architecture (SNA) – позволява на PC мрежи връзка с IBM минифрейм компютри.
- SAMBA – това е съвкупност от програми, които позволяват на група компютри да реализират достъп до файлове и принтери на Unix сървъри.

1.4. Класифициране на компютърните мрежи по протоколни стекове

Компютърните мрежи могат да се класифицират и в зависимост от протоколните стекове, които се използват за мрежови комуникации. Мрежовите протоколи определят правилата, които се спазват при комуникации между компютрите в мрежата. Най-използваните в практиката протоколни стекове са NetBEUI, IPX/SPX и TCP/IP. Други използвани са протоколният стек Apple-Talk и комплектът протоколи на OSI модела.

Мрежите, използващи NetBEUI модела, се ползват за изграждане на малки локални мрежи, които използват операционни системи на Microsoft. Комуникацията в тези мрежи се основава на протоколите NetBIOS (Network Basic Input/Output System), които са разработени от IBM за малки работни групи. Локалните мрежи от този тип не могат да се свързват информационно помежду си. Маршрутизирането на съобщения между тях изисква инсталация на допълнителни протоколи.

Мрежите IPX/SPX (Internet Package Exchange /Sequenced Packed Exchange) използват пакет от протоколи, разработени от Novell. Протоколният стек IPX/SPX се асоциира с NetWare и Microsoft мрежите. Microsoft има своя реализация на протоколен стек под името NWLink, който се инсталира в клиентските компютри, за да имат връзка с NetWare сървър.

Протоколният стек TCP/IP е по-труден за конфигуриране и работи най-бавно в сравнение с останалите. Независимо от тези недостатъци той е намерил най-широко приложение. Причините за предпочитанието му са:

- TCP/IP използва различни методи за адресиране и е подходящ за маршрутизиране на съобщенията през големи мрежи.
- Голяма част от операционните системи поддържат TCP/IP.
- Съществуват широк кръг от програми и инструменти за наблюдение и управление на TCP/IP мрежите.
- TCP/IP е протоколният стек, който се използва за Интернет комуникации.

Протоколите AppleTalk са разработени от Apple за управление на мрежи с компютри Macintosh. AppleTal мрежите използват протокола AARP (Apple Talk Addres Resolution Protocol) за асоцииране с адресите на Ethernet и Token Ring. Към стека са включени и протоколите:

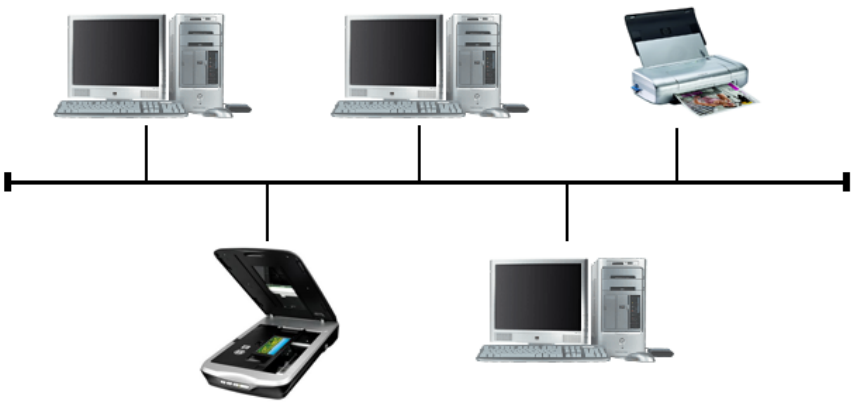
- LocalTalk – използва се за свързване на Macintosh компютри в малки работни групи до 32 устройства, със скорост на предаване на данни до 230,4 kbps.
- EtherTalk – за свързване на Macintosh работни групи към Ethernet мрежи.
- TokenTalk – за свързване на Macintosh работни групи към TokenRing мрежи.

Протоколният стек Open System Interconnection (OSI) е създаден, за да замени TCP/IP. Създателите на протоколния стек са го регистрирали в Международната организация по стандартизация (ISO) и са имали намерения да въведат строг ред в стандартите за създаване на мрежови продукти от световните производители. Въпреки усилията за въвеждане на OSI модела и досега TCP/IP моделът е основен за глобалната световна мрежа Интернет.

1.5. Класифициране на компютърните мрежи по топология

Използват се два вида топологии – физическа и логическа. Физическата топология е свързана с геометричното разположение на кабелите и компютрите, а логическата – с пътя на сигналите от една точка на мрежата до друга. И двете топологии могат да са от един и същ вид, но могат да се различават. Често се наблюдават локални мрежи, изградени по една физическа топология, а логическата е от друг тип. Най-често използваните топологии за локални мрежи са: линейна шина; кръг; звезда; решетка; хибридна.

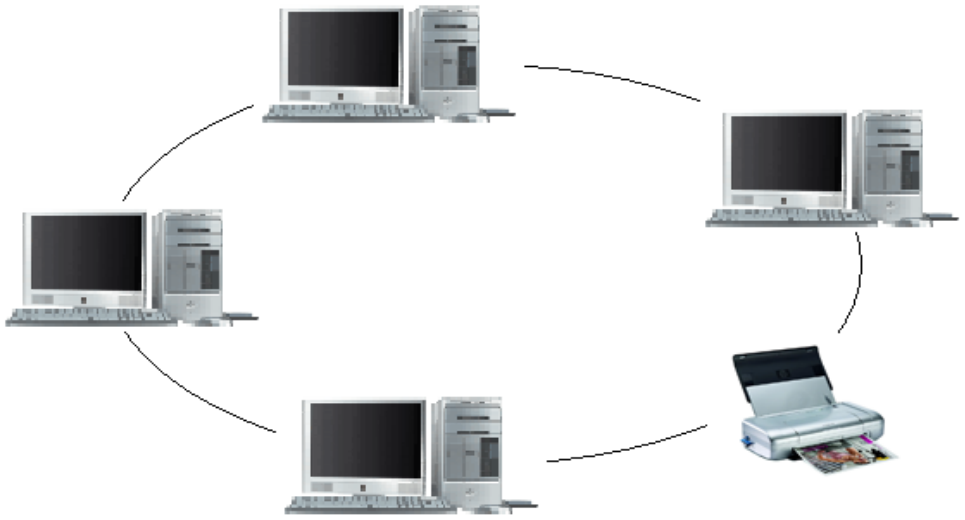
Компютрите в мрежи, изпълнени в **топология тип шина** (фиг. 6.4), са разположени в една линия. Свързващият кабел преминава последователно от един компютър към друг. Тези мрежи имат начало и край, към които се включват устройства, наречени терминатори. Терминаторите поглъщат правата вълна на сигналите и не позволяват получаване на отразена вълна. Всички компютри в тази топология приемат сигналите, които се разпространяват по шината. В паметта й се копират само сигналите, които в заглавната си част имат адрес, съвпадащ с адреса на компютъра.



Фиг. 6.4. Компютърна мрежа с топология тип „шина”

Шинната топология е с ниска цена и лесна за инсталиране. Подходяща е при изграждане на временни мрежи с малко на брой компютри. Комуникационният канал се изгражда от коаксиален кабел с вълново съпротивление 50 или 75 ома. Недостатък на този тип мрежи е пасивната роля на компютрите. Те не усилват сигналите по линията и на определени разстояния сигналът намалява своята амплитуда, с което се ограничава размерът на мрежата. Друг недостатък на мрежата е, че при прекъсване на кабела разделените компютри губят връзка и в участъците се появяват отразени вълни.

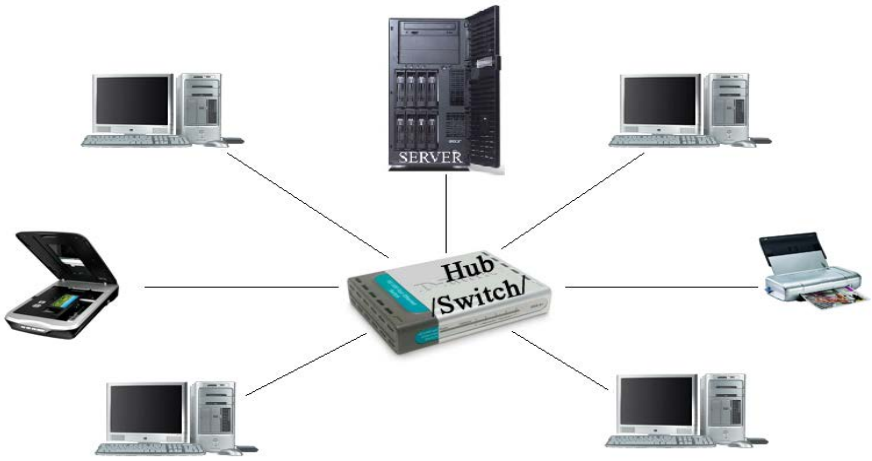
В кръговата топология (фиг. 6.5) всеки компютър се свързва към два други и сигналите обикалят непрекъснато в кръга. За изграждане на комуникационния канал в началото е използван коаксиален кабел, за който не е необходимо поставяне на терминатори, тъй като кръгът няма крайни точки. На по-късен етап е използван кабел STP, отговарящ на спецификациите на стандарта IEEE 802.5. Сигналите се разпространяват в една посока, всеки компютър ги приема от предходния съсед и ги изпраща на следващия. Кръговата топология е активна, тъй като компютрите регенерират сигналите, когато ги предават на следващия компютър. Тази топология е известна като Token Ring мрежа. Логическият кръг се реализира от специален за стандарта хъб, който се нарича модул за достъп до множество станции (multistation access unit – MSAU). Кръговата технология се инсталира лесно и неизправностите се откриват и отстраняват безпроблемно. Като недостатъци на топологията може да се посочат, че мрежата престава да функционира при прекъсването на комуникационния канал и за времето на добавяне на нови абонати.



Фиг. 6.5. Компютърна мрежа с топология тип „кръг”

Топологията тип „звезда” (фиг. 6.6) е една от най-широко разпространените. Изпълнението на тази топология става чрез централен хъб. Познати са три вида хъбове: пасивни, активни и интелигентни. Пасивният хъб не е под захранване и изпълнява ролята на многоточков съединител. Активният повторител има собствено електрическо захранване и работи като множествен повторител на сигналите. Сигналите се формират и усилват при предаването им от компютъра източник към получателя. Интелигентният хъб е активен, има собствен процесор и може да работи като комутатор. Тази топология се изгражда основно с кабели тип усукана двойка и Ethernet архитектура. Сигналите в мрежата се излъчват от предаващия компютър, хъбът ги усилва и разпространява през своите портове към всички

останали компютри. Само компютрите, които разпознаят своя адрес в хедъра на съобщението, го копират в своята памет. Топологията тип „звезда” има доста предимства пред останалите. Когато някой от компютрите излезе от строя или се прекъсне свързващ кабел, останалата част от мрежата работи устойчиво. Този тип локални мрежи лесно се реконфигурират. С лекота се премахват и добавят компютри, без да се преустановява функционирането на мрежата. Недостатък на топологията е по-високата цена заради повечето кабел за изграждането на комуникационната среда и зависимостта й от състоянието на централния хъб.



Фиг. 6.6. Компютърна мрежа тип „звезда”

Топология тип „решетка” се изпълнява по-рядко в сравнение с останалите. Комуникационната мрежа на тази топология е изградена така, че всеки компютър има директна връзка с останалите. Това я прави устойчива на неизправности, тъй като сигналите могат да достигнат до компютрите по различни маршрути. Това предимство на топологията тип „решетка” за съжаление води до увеличаване на броя на връзките между компютрите и цената на компютърната мрежа.

Хибридните топологии се срещат нерядко в практиката. Те са от смесен тип в зависимост от потребностите на ползвателите на мрежата. Шината в повечето случаи се изгражда като гръбнак на хибридната мрежа. От гледна точка на топологията най-често се комбинират шина със звезда и кръг.

1.6. Класифициране на компютърните мрежи по архитектура

Мрежовата архитектура е съвкупност от спецификации за мрежите, които определят физическата и логическата топология, типа на комуникационната мрежа, ограниченията в дължината на разстоянията между компютрите, метода за достъп до комуникационния канал, размера и структурата на пакетите и кадрите. Най-широко приложение в практиката са намерили архитектурите Ethernet и Token Ring. По-рядко се срещат архитектурите Apple Talk и ARCnet.

Ethernet мрежите се изграждат по физическа топология тип „шина” или „звезда” и използват метод за достъп до комуникационния канал, наречен множествен достъп до преносната среда с разпознаване на носещата честота и откриване на колизиите (CSMA/CD – Carrier Sense Multiple Access With Collision Detection). Компютрите прослушват канала и ако е

свободен, който пръв излъчи кадри, го заема, а останалите преминават в режим приемане. Когато два и повече компютъра излъчат кадри, възниква колизия и участниците в конфликта преминават в режим мълчание. Следващото обръщение към канала за всеки компютър е след интервал, чиято продължителност се формира по случаен закон. Поради възникващите конфликти реалната скорост за предаване на данни може да достигне до 30% от проектната. Стандартните мрежи за тази архитектура работят със скорост от 10 Mbps. В момента най-често използваната е Fast Ethernet, която работи със скорост на предаване на данните 100 Mbps. Използва се и Gigabit Ethernet архитектурата, която работи с по-голяма скорост от 1 Gbps. В зависимост от типа на използвания кабел съществуват различни типове Ethernet мрежи. Допуска се изграждане на комуникационната среда от коаксиални кабели, кабел тип усукана двойка и оптически влакна.

Компютърните мрежи Token Ring са създадени за избягване на проблемите с колизиите в Ethernet мрежите. Тези мрежи използват физическа и логическа топология тип „кръг". В кръга се движи служебен маркер и само компютърът, който го притежава, може да излъчва информационни кадри. По-често мрежите от този тип се изграждат по физическа топология звезда, а логическата остава кръг. Компютрите се свързват към централен хъб, наречен модул за достъп до множество станции (MSAU – Multistation Access Unit). Хъбът реализира логическия кръг чрез конекция на кабелите и портовете. Стандартните мрежи от този тип използват основно екранирани кабели с усукани двойки. През последните години се използва и оптическото влакно за повишаване ефективността на стандарта. Независимо от по-високата цена спрямо Ethernet мрежите Token Ring архитектурата е с висока надеждност и е намерила широко приложение в практиката.

Архитектурата Apple Talk се използва за изграждане на мрежи с компютри Macintosh. Тези мрежи могат да се разделят на зони, подобни на работните групи. Компютрите ползват само споделените ресурси в зоната, на която принадлежат. Комуникацията между зоните се реализира от специално инсталиран протокол. В тези мрежи за поддържане на динамично адресиране се използва протоколът LLAP (Local Talk Link Access Protokol) и понякога тези мрежи се наричат Local Talk.

Въпроси за самостоятелна работа

1. По какви показатели се класифицират компютърните мрежи?
2. Какви са характеристиките на работните станции?
3. Какви са характеристиките на сървърите?
4. Какви са особеностите на локалните операционни системи?
5. Какви са особеностите на мрежовите операционни системи?
6. Кои са най-често използваните операционни системи?
7. Кои са използваните протоколни стекове в съвременните КМ?
8. Дефинирайте понятието физическа топология.
9. Дефинирайте понятието логическа топология.
10. Какви архитектури са приложени в компютърните мрежи?

ГЛАВА 2. МРЕЖОВИ КОНЦЕПЦИИ И МОДЕЛИ

2.1. Мрежови концепции

Основната причина за свързване на компютрите в мрежа е създаване на възможност за комуникация между абонатите. Обменът на съобщения между свързани компютри е сложен процес. Принципите на комуникация са свързани с възможностите на компютрите да обработват информационни масиви от данни. В основата на компютърните комуникации стоят следните основни концепции [35]:

- Използване на двоичната бройна система.
- Създаване на модели на мрежи за графично представяне на процесите.
- Приемане на спецификации и стандарти за комуникации на мрежово оборудване.

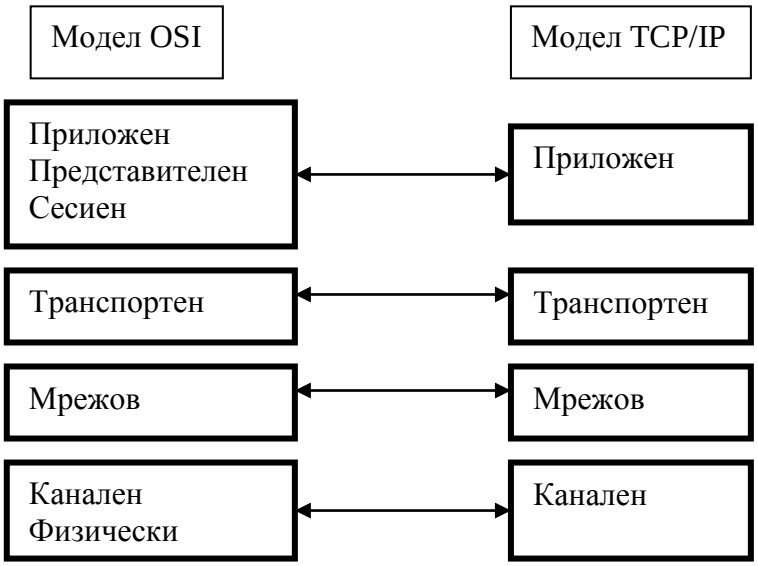
Съвременният компютър е електронно устройство, което работи в двоичен код под управлението на програми. С изпълнение на различни програми компютрите обработват текстови файлове, моделират сложни процеси, синтезират музика, реализират впечатляващи графични решения, използват се за телекомуникации, сигнализация и управление. Реализацията на тези сложни функции се постига с използване на двоичната бройна система, която е подходяща и за електронни комуникации. Съществуват и други бройни системи като десетична и шестнадесетична, които в практиката се използват за съкратено записване на сравнително големи числа. Преобразуването на числата от една бройна система в друга е сравнително лесно за изпълнение, но за големите числа се изискват множество изчисления. За компютъра, който работи с изпълнението на десетки милиони операции в секунда, не е проблем да работи в двоична бройна система и да представя резултатите в десетична и шестнадесетична бройна система. В компютрите се използва шестнадесетичният запис поради по-лесното преобразуване на числата от двоична в шестнадесетична бройна система, и обратно. Двоичната бройна система е най-простата и за съжаление чрез нея големите числа се представят с прекалено дълги записи. Съвременните компютри разполагат с големи обеми от оперативна и външна памет и работят с големите по размери двоични числа, без потребителите да се съобразяват с този факт.

Двоичната бройна система е подходяща и за преобразуването на съобщенията в двоични сигнални последователности. Цифровите системи за предаване на данни след 80-те години на миналия век постепенно изместиха аналоговите. Преди съобщенията да се предадат през комуникационните мрежи, се разделят на малки пакети, които могат лесно да се предават и подлежат на ефективно управление. Разделянето на съобщението на пакети се извършва от компютъра, източник на съобщението. Задачата на комуникационната мрежа е да пренесе пакетите от източника до получателите. Създадена е възможност множеството от пакети да премине по различни комуникационни канали на мрежата, за да достигне до компютъра получател на съобщението. По този начин се постига равномерно натоварване на комуникационните канали и се постига производителност на мрежата, близка до проектираната. Информацията за управление на пакета през мрежата се поставя в началото му; тя съдържа основно адресите на източника и получателя и номера на пакета от съобщението. Обикновено пакетите се кодират с циклични кодове с цел повишаване достоверността на съобщението. Компютърът получател има задача да подреди пакетите и да формира съобщението. Ако някой пакет липсва или е приет с грешка, получателят прави заявка до източника тези пакети да се пуснат отново в мрежата. Предимствата на този метод за предаване на съобщения се заключават в следното:

- Компютър, който предава големи по обем съобщения, не може да монополизира мрежата.

- Равномерно се натоварват каналите на мрежата и се постига висока производителност.
- Ако се прекъсне мрежовата комуникация, изгуби се пакет или се приемат пакети с грешка, отново се предават само тези части от съобщението.

Компютрите, включени в мрежа, изпълняват локални задания и поддържат сложни процеси, свързани с мрежовите комуникации. През 60-те години на миналия век започва процесът по моделиране и формализация на комуникационните процеси. На симпозиуми на Международната организация на електроинженерите (IEEE) се обсъждат варианти за модел и сценарии на компютърните комуникации. Възприема се многослойният модел, като се предлага различен брой на слоевете (от 4 до 10). Обменът на съобщения между компютрите в голяма степен е свързан и с типа на инсталираната в компютрите операционна система. Използването на различни компютри и операционни системи и многостранните интереси на потребителите допълнително усложняват стандартизирането на компютърните комуникации. Все пак под въздействието на големите производители на компютри и комуникационно оборудване се постига споразумение и се създават модели за комуникация. Общото за всички модели е, че процесите на комуникация са разделени на нива и за всяко ниво са дефинирани набор от услуги и протоколи. Освен IEEE, в утвърждаването на комуникационните модели голяма роля изиграва и Международната организация по стандартизация ISO. Обществата на потребителите на компютърни комуникации нарастват с голяма скорост и предявяват претенции за глобални комуникационни услуги. Те стават втората след производителите движеща сила в развитието на компютърните мрежи. В резултат на влиянието на производителите и потребителите се появяват и съответните комуникационни модели. Доминиращите модели, които възникват под въздействието на производителите и потребителите, са съответно отвореният модел за комуникации (OSI – Open System Interconnection) и моделът на Министерството на отбраната на САЩ (DoD – Department of Defense).



Фиг. 7.1. Съответствие между комуникационните модели OSI и TCP/IP

В модела OSI процесите в компютърните мрежи са разделени на седем слоя и моделът се възприема от големите световни производители. Слоевете на модела отдолу нагоре са следните: физически, канален, мрежов, транспортен, сесиен, представителен и приложен.

Международната организация ISO регистрира модела и става негов гарант с пакет от стандарти. Производителите на компютри, базово програмно осигуряване и комуникационно оборудване възприемат тези стандарти, с което започва развитието на компютърните мрежи и комуникации.

Моделът DoD е четирислоен и е по-известен като TCP/IP. Услугите в този модел се развиват под въздействието на потребителите и той става основа за изграждането на световната глобална мрежа Интернет. Слоевете в този модел са: канален, мрежов, транспортен и приложен. Съответствието на двата модела е показано на фиг. 7.1.

С разработката на OSI модела Международната организация по стандартизация ISO е имала намерение по-конкретно да се определят мрежовите функции на TCP/IP модела. Поради големия интерес на човечеството към глобалните комуникации и високото темпо, с което се развиват компютърните мрежи, TCP/IP протоколите се проектират по модела на Министерството на отбраната на САЩ DoD.

Производителите на мрежови операционни системи създават свои специфични мрежови модели. Такива са мрежовите модели на Windows NT и Windows 2000, в които са включени гранични слоеве като интерфейс между основните слоеве. Всички производители на мрежови операционни системи се съобразяват с OSI модела, който се възприема като световен стандарт.

2.2. Методи за комуникация и предаване на данни в компютърните мрежи

Предаването на съобщения в компютърните мрежи става посредством обмен на сигнали между възлите на мрежата. В зависимост от използваната среда на комуникационната мрежа се използват електрически сигнали, светлинни сигнали, инфрачервени вълни или радиовълни. Съобщенията се формират и съхраняват в компютрите в двоичен код, но за да се предават през мрежата, се превръщат в сигнали, които се модулират или кодират от възлите предаватели. В зависимост от характеристиките на сигналите може да се направи следната категоризация на компютърните мрежи:

- аналогови или цифрови;
- таснолентови или широколентови;
- синхронни или асинхронни;
- симплекс, полудуплекс, пълен дуплекс или мултиплексни.

Аналоговото и цифровото предаване на данни са различни методи за кодиране на съобщенията в компютърните мрежи. Може да се каже, че аналоговите методи за кодиране са началото на предаване на данни, а цифровите са съвременните методи за компютърни комуникации. Всеки от двата метода има свои предимства и недостатъци и е подходящ за реализация на мрежа при определени обстоятелства. Не е съвсем вярно твърдението, че цифровите методи ще заменят напълно аналоговите в бъдеще.

Аналоговият сигнал представлява електромагнитна вълна, чиято амплитуда и фаза се променят във времето. Параметрите на аналоговите сигнали, които се използват за предаване на данни, са амплитуда, честота и фаза. Предаването на данни е свързано с модулиране на параметрите на аналоговите сигнали. Предимствата на аналоговото предаване са:

- Аналоговите сигнали лесно се мултиплексират с цел увеличаване на пропускателната способност на комуникационните канали.
- Аналоговите сигнали могат да се разпространяват на големи разстояния, без да губят голяма част от мощността си.

Цифровите сигнали изменят своята амплитуда мигновено, без да заемат междинни стойности между две състояния. Тъй като компютрите са цифрови устройства, може да се каже, че цифровите системи за предаване на данни са по-подходящи от аналоговите. Това е основната причина повечето от компютърните мрежи да използват цифрово предаване на сигнали. Предимствата на това предаване в сравнение с аналоговото са:

- Себестойността на цифровото оборудване е сравнително по-ниска.
- Цифровите сигнали са устойчиви и по-малко уязвими от смущенията.

В днешно време се използва повече цифровото предаване на данни. То предлага по-висока сигурност, достоверност и надеждност на телекомуникационните системи. Цифровите комуникационни линии предават данните с ниска вероятност за грешка, която може да се пренебрегне.

Тяснолентовото и широколентовото предаване на сигнали е свързано с честотната лента на мрежовата преносна среда. Честотната лента на каналите определя максималната скорост за предаване на данните. Тя може да се раздели на множество канали, по които се предават различни потоци от данни.

Тяснолентовото предаване на сигнали е сравнително просто решение. По комуникационната линия се предава един сигнал, който заема цялата честотна лента на канала. Това предаване е типично за цифровите канали, независимо че се среща и в аналоговите системи. Разпространението на сигналите е в двете посоки на комуникационните линии, което позволява едновременно предаване и приемане на данни.

Широколентовото предаване позволява разделяне на лентата на пропускане на няколко канала. Каналите работят едновременно и всеки от тях може да пренася различни сигнали. Предаването за отделните канали е еднопосочно, но е възможно различните канали да предават сигнали в различни посоки.

Мултиплексирането е метод за едновременно предаване на данните на едно съобщение по повече от един канал. Предавателят разделя данните на съобщението на отделни потоци, а приемникът възстановява потоците в съобщение. Мултиплексирането може да се приложи както за аналоговите, така и за цифровите сигнали. То може да се реализира по следните методи:

- Честотно мултиплексиране (Frequency Division Multiplexing – FDM).
- Мултиплексиране чрез времеделение (Time Division Multiplexing – TDM).
- Мултиплексиране чрез разделяне дължината на вълната (Dense Wavelength Division Multiplexing – DWDM).

Аналоговите сигнали се предават по метода на честотното мултиплексиране. По една и съща комуникационна линия се предават множество сигнали, като за отделните подканали се използва различна честота. Двупосочните комуникационни канали изискват и на двата края на линията да се поставят устройства, наречени мултиплексор/демултиплексор.

Цифровите комуникационни канали използват мултиплексиране с времеделение. Сигналите се комбинират и се предават по линията в отделни времени сегменти с кратка продължителност. Последователно сегментите се предават по линията и приемащият демултиплексор ги формира в съобщение.

Каналите, използващи оптични влакна за преносна среда, използват мултиплексиране чрез разделяне дължината на вълната. Сигналите на различните съобщения се предават през оптическото влакно с различна дължина на вълната. Няма изискване скоростта на предаване за различните съобщения да е еднаква.

Синхронното и асинхронното предаване на данни е свързано с два вида синхронизация – тактова и циклова. Цикловата синхронизация е свързана с предаването на

цялото съобщение или фрагменти от него. Тактовата синхронизация касае побитовото предаване на данните между предавателя и приемника.

При синхронното предаване на данните се изисква в предавателя и приемника да се вгради специален генератор за координиране тактовете на предаване и приемане. Съществува и метод на синхронизация с използване на допълнителен канал за синхронизация. В практиката често се използва и синхронизация на приемника по приеманите сигнали. В този случай се налага генераторът на приемащото устройство да работи с малко по-голяма скорост от генератора на предавателя.

Асинхронното предаване на данни използва стартова група от битове в началото на съобщението или фрагмента. След като се приеме стартовата група, приемникът синхронизира своя вътрешен генератор с тактовия генератор на предавателя.

Симплексното, полудуплексното и пълнодуплексното предаване на данни е начинът, по който се предават данните по комуникационния канал. Различията между трите начина е основно в посоката на предаване на сигналите и броя на използваните канали.

Симплексното предаване на данни е еднопосочно. При него сигналите пътуват в посока от предавателя към приемника. От приемника към предавателя не се предават никакви сигнали, както в реализираната досега система за телевизионно предаване. Предстои внедряване на интерактивна телевизия, в която се изисква двупосочно предаване. Кабелните оператори допълниха мрежите си с двупосочни усилватели и по този начин преобразуваха комуникационната мрежа в двупосочна. По този начин допълниха дейността си и като доставчици на интернет услуги.

Полудуплексното предаване на данни е подобрен вариант на симплексното. Трафикът на данни при него е в посока предавател – приемник и обратно, като двупосочните сигнали се редуват последователно. Този начин изисква определено време за превключване на предавателя в режим приемане и на приемника в режим предаване. През това време не се предават сигнали по комуникационната линия.

Пълнодуплексното предаване осигурява двупосочен трафик на сигнали в едно и също време. Тази технология увеличава производителността на компютърната мрежа, защото едновременно могат да се изпращат и приемат данни по комуникационните канали.

2.3. Методи за достъп до комуникационния канал в локалните компютърни мрежи

Комуникационната среда на локалните компютърни мрежи разполага с един общ канал за предаване на сигнали, към който са включени всички компютри. Когато два и повече компютъра излъчат сигнали в канала, възниква конфликт (колизия) в мрежата и предаването на съобщения се прекратява. Всички компютри в мрежата прослушват канала и когато разпознаят своя адрес в съобщението, го записват в паметта си. Допуска се повече от един компютър да приема предадените съобщения в локалната мрежа. За да не се допускат конфликти в каналния слой на комуникационния модел, е предвиден специален подслой, който решава достъпа до комуникационния канал на всеки компютър. В зависимост от топологията и мрежовата архитектура се използват следните методи за достъп до преносната среда:

- Множествен достъп с разпознаване на носещата честота и откриване на колизии (Carrier sense multiple access/ Collision detection – CSMA/CD).
- Множествен достъп с откриване на носещата честота и избягване на колизии (Carrier sense multiple access/ Collision avoidance – CSMA/CA).
- Предаване на маркер.
- Приоритет по заявка.

CSMA/CD е най-използваният метод за достъп на компютрите до комуникационния канал в локалните мрежи. Намерил е приложение в една от широко разпространените архитектури – стандартът Ethernet. При този метод, преди някой компютър да се обърне към комуникационния канал за предаване на съобщение, първо подслушва линията, за да разбере дали в момента друг компютър не предава данни. Ако не се открият други сигнали, компютърът излъчва съобщението. В противен случай възниква конфликт (колизия) и участниците в конфликта преминават в режим мълчание. Следващото обръщение на компютър към канала за всички, които имат съобщение за останалите, е след интервал, чиято продължителност се формира по случаен закон. При този метод компютрите правят опит да заемат канала с излъчване на информационни кадри.

CSMA/CA е по-непопулярен метод в сравнение с предходния. Разликата между тях е, че при този метод компютрите правят опит за заемане на канала с излъчване на служебен кадър (request to send – RTS). Независимо че този метод изглежда по-организиран, той няма широко приложение. Това се дължи на отрицателното влияние на колизиите върху производителността на мрежата. Методът за достъп се прилага в компютърните мрежи, изградени по модела Apple Talk.

Предаването на маркер е метод, при който липсва състезателният елемент между компютрите. Използва се служебен маркер, който се предава между крайните възли на мрежата и само компютърът, който го притежава, може да излъчва съобщения за останалите. Времето за задържане на служебния маркер може да се ограничава, с което се въвежда справедливо използване на комуникационния канал от всички компютри. Този метод е приложен в стандарта Token Ring. В някои архитектури – като стандарта FDDI, се допуска използване на повече от един служебен маркер с цел увеличаване производителността на мрежата.

Приоритет по заявка е метод за управление на достъп до преносна среда, изградена с помощта на многопортови хъбове. Хъбовете сканират кръгово компютрите, включени във входовете им за надолу. Когато компютри от различни сегменти комуникират, регистрират заявка чрез своя хъб. Хъбовете от горните нива сканират портовете за нагоре на хъбовете от следващите нива. Приоритетът за обработка на заявките се задава в полето управление на кадрите. Този метод е реализиран в архитектурата 100VG AnyLAN на стандарта IEEE 802.12.

Въпроси за самостоятелна работа

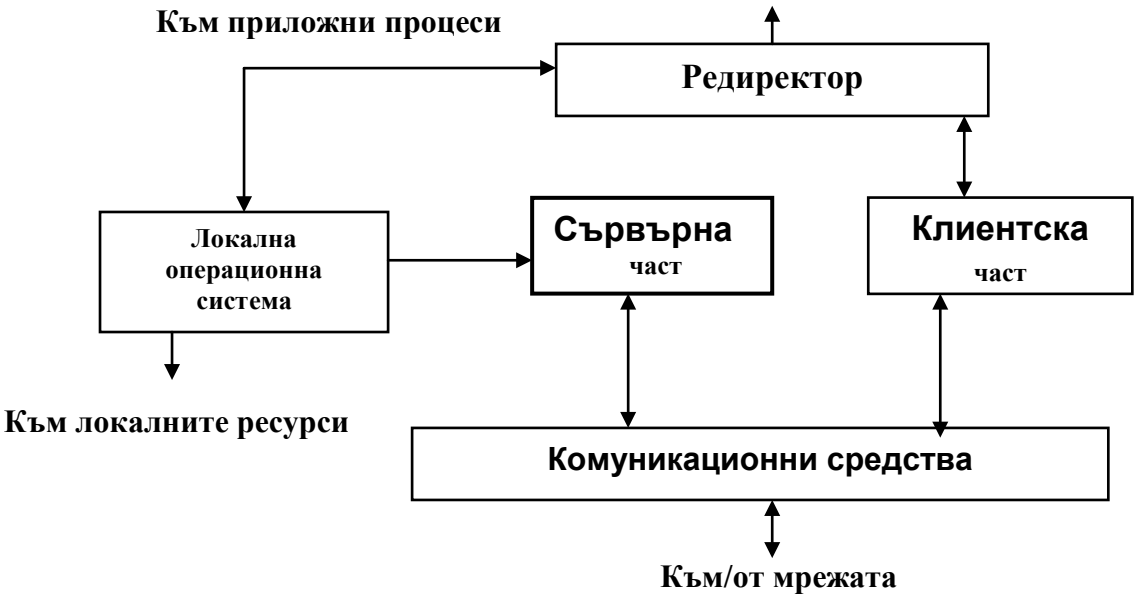
1. Защо в КМ се използва двоичната бройна система?
2. Какви методи за предаване на сигнали се използват в компютърните комуникации?
3. Кои методи за модулация на сигналите се използват в КМ?
4. Какви методи за мултиплексиране на сигналите се използват в КМ?
5. Защо комуникационните процеси в КМ са специфицирани и стандартизирани?
6. Кои са основните комуникационни модели, приложени в КМ?
7. Каква са различията между комуникационните среди на локалните и глобалните компютърни мрежи?
8. Какви проблеми възникват в КМ в комуникациите и предаването на сигналите?
9. Какви методи за достъп до преносната среда са приложени в локалните компютърни мрежи?
10. Какви методи за комутация са приложени в глобалните компютърни мрежи?

ГЛАВА 3. МРЕЖОВА ОПЕРАЦИОННА СИСТЕМА

3.1. Обосновка на мрежовата операционна система

Горните слоеве на комуникационния модел в локалните компютърни мрежи се реализират от мрежова операционна система (МОС), която се инсталира в крайните възли на мрежата. В широк смисъл под МОС се разбира съвкупността от операционните системи на отделните компютри, които взаимодействат помежду си по протоколи с цел обмен на съобщения и ползване на общи ресурси. Инсталираната МОС на компютрите (фиг.8.1) се състои от две основни части [5]:

- *Локална ОС* – средства за управление на локалните ресурси на компютъра /памет, процесор, процеси/.
- *Сървърна част* – предоставя собствените си ресурси за ползване от останалите компютри от мрежата.



Фиг. 8.1. Блокова схема на МОС

Във функциите на сървърната част от МОС са включени дейностите:

- Заключване на файлове и записи чрез използване на примитиви като семафори, монитори и др.
- Обслужване на заявките за отдалечен достъп към локалните файлови системи и бази от данни.
- Управление на опашките на заявки на отдалечени потребители към локалните входно-изходни (периферни) устройства.

Клиентска част на МОС – осигурява достъп и ползване на отдалечени ресурси. Редиректорът прехваща заявките от приложните процеси и ги пренасочва към компютъра клиент. Съвкупността от функциите, чрез които приложните процеси се обръщат към редиректора, се наричат приложен интерфейс – Application Programming Interface (API). Редиректорът на операционната система е прозрачен за локалните заявки и отдалечените ресурси. Той носи името на фирмата създател като:

- LAN Requester от IBM;

- NET x. COM (shel) при Novell;
- Redirector от Microsoft.

Комуникационните средства служат за обмен на съобщения в компютърната мрежа. Това са програмни модули, разпределени по комуникационните слоеве на протоколния стек, използван от операционната система. Те изпълняват следните функции:

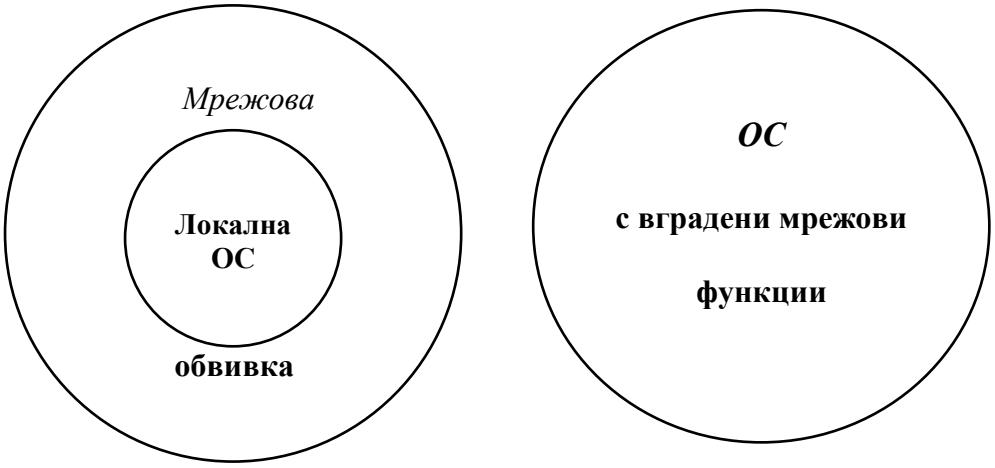
- адресиране на съобщенията;
- буфериране на съобщенията;
- избор на маршрут за предаване;
- осигуряване на достоверност и надеждност при предаване.

В зависимост от мястото и ролята на мрежовия възел той може да има различна по структура операционна система:

- само клиентска част;
- само сървърна част;
- клиентска и сървърна част.

Използват се два различни подхода (фиг. 8.2) при създаване на МОС.

При първия подход МОС е съвкупност от локална операционна система с вградени мрежови възможности и надстроена около нея мрежова обвивка, която изпълнява основните мрежови функции. По този модел са създадени операционните системи OS 12 и DOS 7.



Фиг. 8.2. Схема на видовете операционни системи

При втория подход МОС е с мрежови функции, вградени в основните й модули. Този подход е използван при създаването на операционни системи – Windows NT, Windows NT Server, NET Were, UNIX и др. В зависимост от метода на администриране и разпределението на функциите между компютрите в локалните компютърни мрежи МОС се делят на два вида:

- МОС с равноправен достъп (Per to per).
- МОС с отделни сървъри (dedicated servers).

Ако изпълнението на сървърните функции е възложено на един компютър, то той се нарича сървър. На него се инсталира операционна система, която изпълнява сървърни функции. МОС с отделни сървъри са NetWere и Windows NT. Прието е ресурсите на сървъра да не се натоварват с локални задачи, за да не се намалява неговата производителност и възможност за управление.

Операционните системи Windows NT Server и Windows NT Work station поддържат функции на клиент и сървър. При този вариант на МОС има възможност да се представят повече ресурси и съединения едновременно. Реализира се централно управление на мрежата и има добра система за защита на апаратните и информационните ресурси.

Сървърите са най-мощните компютри в мрежата. За администрирането на такава мрежа се грижи системен администратор, който осъществява централизирано управление на компютърната мрежа.

При МОС с равноправен достъп всички компютри са равноправни по отношение предоставянето и ползването на мрежови ресурси. Всеки компютър може да се конфигурира или само като клиент, или като сървър. Някои от компютрите в мрежата могат да бъдат клиенти за едни, а за други – сървъри. В такава мрежа във всички компютри се инсталира една и съща ОС като: LANtastic, Personal Were, Windows for Workgroup и версиите Windows 95/2000, XP. Тези мрежи са по-лесни за обслужване, но няма достатъчно сигурна гаранция за защита на ресурсите.

Операционната система е програмно осигуряване, което създава условия за работа на приложенията и предлагане услуги на компютрите. Мрежовата операционна система позволява компютрите да комуникират помежду си и да споделят апаратни и информационни ресурси. МОС е развитие на локалната операционна система и се инсталира по правило на мрежов сървър. В компютърните мрежи се използват следните видове МОС [35]:

- Microsoft Windows NT 4.0
- Microsoft Windows 2000
- Novell Net Ware
- UNIX
- Linux
- Banyan Vines
- OS/2 Warp Server
- Apple NOS
- LANtastic.

3.2. Общи принципи на мрежовото администриране

Всяка компютърна мрежа е съставена от работни станции и от един или повече от един сървъри. Сървърът е компютър с по-големи апаратни и информационни ресурси в сравнение с работните станции. Инсталирана на сървър, операционната система създава възможност за централизирано разположение и администриране ресурсите на компютърната мрежа. В зависимост от използваните приложения в мрежата, решаването на заданията може да се реализира на клиентските компютри или споделено с част от ресурса на сървърите [35].

Компютърните мрежи тип клиент/сървър се различават съществено от равноправните. Изградената на сървъри мрежа е среда, която е лесна за администриране на ресурсите, архивиране на данните и решаване на проблемите по безопасна експлоатация. Сървърът има възможност да споделя с работните станции информационни ресурси от файловата система, апаратни ресурси и да предлага комуникационни услуги. Приложенията клиент/сървър използват ефективно мощността на процесорите на компютъра и имат възможност да оптимизират изпълнението на задачи от типа изпълнение на заявки за достъп до бази от данни. Високата начална цена на приложенията клиент/сървър се счита за недостатък, но базите данни SQL Server и Oracle са скъпи за малките мрежи, в които заявките за базите от данни са малко на брой. Когато потребителите ползват бази от данни в Access, на техните локални компютри данните се съхраняват на файлов сървър, в резултат на което се

затруднява производителността на мрежата. Мрежата тип клиент/сървър може да се конфигурира по един от следните два начина:

- Данните се разполагат на един сървър за бази от данни.
- Данните се разпределят на множество сървъри за бази от данни.

На мястото за съхраняване на базите от данни се създават огромно количество записи. Съвременните ОС са проектирани специално за тази цел, като данните могат да се съхраняват на един диск или на множество дискове, инсталирани на повече от един сървър.

3.3. Споделяне на мрежови ресурси

Степента на споделяне на мрежовите ресурси зависи от типа на МОС и направените настройки на нейните модули. В практиката се използват различни подходи в предварителното договаряне на ресурсите. Съществуват МОС като тези от фамилията Windows, в които по подразбиране не се споделят никакви ресурси. Ако някои ресурси се предоставят на клиентите, те изрично се създават като споделени ресурси (creating a share). Има и МОС, като NetWare, в които всички ресурси са споделени с подразбиране.

За да се споделят ресурсите на компютър, използващ МОС Windows 9x, услугата File and Print Sharing трябва да е разрешена. Когато компютър използва МОС Windows NT и Windows 2000, е необходимо да се инсталира и стартира услугата Server. Възможно е не всички ресурси на сървърите да се разрешат за ползване от всички работни станции на мрежата. Някои от ресурсите може да се разрешат за едни работни станции, за други може да се забранят. Всяка МОС трябва да има средства за контрол на достъпа до файловата система, апаратните ресурси на компютъра и периферните устройства, включени към него. Съществуват два способа за предоставяне на достъп до ресурсите на сървърите:

- Предоставяне на права за достъп до споделени ресурси.
- Предоставяне на достъп до споделен ресурс на потребители.

Предоставяне на права за достъп до споделени ресурси (share-level security) се използва по правило в компютърните мрежи с равноправен достъп. При този тип достъп, когато се избере споделен ресурс по мрежата, се изисква и използване на парола за защита на ресурса. На потребителя се предлага да въведе вярната парола за достъп до съответния ресурс. Независимо от опростения достъп, когато броят на ресурсите е голям, на потребителите, които имат права за достъп, се налага да запомнят множество пароли.

Предоставяне на достъп до споделен ресурс на потребители (user-level security) е по-лесна процедура за управление на достъпа до ресурсите за средни и големи по мащаби компютърни мрежи. При този способ всеки потребител има потребителски акаунт, защитен с парола. Потребителите влизат в сървърите със своите акаунти. Достъпът до споделените ресурси се конфигурира с възможност за достъп на упълномощените потребители. Когато потребителят направи обръщение към споделен ресурс, се проверява има ли го в списъка за контрол на достъпа (Access control list). Списъкът за контрол на достъпа се състои от авторизирани акаунти, които имат разрешение за достъп до съответния ресурс. Само ако акаунтът на потребителя се съдържа в списъка, се разрешава достъп до съответния ресурс. При този способ на достъп потребителят е длъжен да помни само една парола, с която осъществява достъп до множество ресурси в компютърната мрежа.

3.4. Управление на достъпа до мрежовите ресурси на компютърната мрежа

Достъпът до мрежови ресурси на ниво потребител изисква създаване на потребителски акаунти. По-голяма част от МОС изискват подреждане на потребителските акаунти в групи за улеснение на администраторите при управление на мрежата. Някои от МОС изискват всеки компютър, който се логва в мрежата, да има и компютърен акаунт (машинен акаунт). Това изискване е допълнително ниво на защита и подобрява сигурността в компютърната мрежа. МОС контролират достъпа до мрежовите ресурси посредством три типа акаунти:

- потребителски акаунти
- групови акаунти
- компютърни акаунти.

Потребителските акаунти са свързани със сигурността на ниво потребител. Всеки потребител има създаден персонален акаунт за осъществяване на достъп до ресурси. Този тип акаунти се поддържа от операционни системи като Windows NT и Windows 2000 на локално ниво. Сигурността на ниво потребител се асоциира със сигурност на ниво мрежа (network-level security), която в Microsoft Windows мрежите се нарича сигурност на ниво домейн (domain-level security).

Всяка МОС има свои особености при защитата на мрежовите ресурси, но мрежовата сигурност се реализира посредством потребителски акаунти и списъци за контрол на достъпа, които изпълняват следните функции:

- При инсталиране на МОС се създава администраторски акаунт (supervisor root), посредством който мрежовият администратор може да създава потребителски акаунти.
- Когато потребителят се логва в мрежата, се въвежда име на потребителски акаунт и парола, след което се проверяват в базата данни с акаунт за сигурност. Тази база от данни е инсталирана на сървър за автентификация при логване. В Microsoft Windows мрежите този сървър се нарича домейн контролер.
- Ако акредитивите се окажат валидни, на потребителя се издава маркер за достъп (access token), идентифициращ потребителя и групите, към които той принадлежи.
- Всеки споделен ресурс има списък за контрол на достъпа, в който се съдържат отделните потребители и групи, оторизирани за осъществяване нивото на достъп до ресурса. Когато някой потребител се опита да реализира достъп до даден ресурс, маркерът за достъп се сравнява със списъка за контрол на достъпа.
- Ако потребителският или груповите акаунти се авторизират в списъка за контрол на достъпа, потребителят получава достъп до ресурса. Когато няма съвпадение, достъпът се отказва.

Структурата на потребителските акаунти се състои от следните записи:

- потребителско име;
- парола;
- условия и ограничения на потребителя;
- информация за сигурност относно потребителя;
- допълнителна информация.

Единна методика за създаване на потребителски акаунти за различните МОС не може да се създаде, но всички те имат в състава си помощни програми, наречени административни инструменти (administrative tools). С тези инструменти администраторите на компютърните

мрежи добавят нови потребители на базите от данни за сигурност. Независимо от различията между видовете МОС се прилагат следните общи принципи в създаването на потребителските акаунти:

- Потребителските имена са уникални.
- Могат да се използват главни и малки букви от азбуката.
- Необходимо е да се избягва използването на символи в потребителските имена като: **„ \ / : | + * ? < > . .**
- Операционната система може да ограничава броя на знаците в едно име.
- Необходимо е избягване на интервал в потребителските имена.

Груповите акаунти се използват в големите компютърни мрежи, които притежават големи информационни и апаратни ресурси. Обикновено потребителите се групират по признаци като работещи в един отдел; преподаватели от една катедра (специалност); студенти от една група и т.н. Групите могат да се използват за по-лесно изпращане на копия от съобщения до голям брой потребители.

Групите, които получават позволения за достъп, се наричат групи за сигурност (security group). Групите, създадени само за приложения като E-mail програми и нямат други права, се наричат групи за разпределение (distribution group).

Някои от операционните системи разделят групите на категории, базирани на област на действие (локални или глобални), други не. Повечето МОС създават една или повече подразбиращи се групи по време на инсталирането. Една от тези групи обхваща автоматично всички потребителски акаунти. В Windows NT, Windows 2000 и NetWare 3x тази група се нарича *всеки* (*everyone*), в UNIX групата се нарича *World.*

Всички потребители от една група притежават правата, дадени на групата. В повечето МОС потребителите могат да принадлежат на повече от една група. В тези случаи е възможно възникване на конфликти между различните групи. Конфликтите могат да се избягнат с внимателна настройка на модулите на операционната система.

Компютърните акаунти се използват в мрежите, в които има високи изисквания за сигурност и достъп до мрежовите ресурси. В Windows домейните е необходимо администраторът да създаде компютърен акаунт на всеки компютър, работещ под управлението на Windows NT и Windows 2000, преди да се съедини към домейна. МОС използва компютърния акаунт, за да валидира идентичността на компютъра и да провежда контрол по време на използване на компютърния акаунт.

3.5. Управление на споделени мрежови ресурси

В МОС от семейство Windows създадените мрежови ресурси се споделят по подразбиране от потребителите на групата *Everyone*. Когато това не е желаният статус, администраторът може да промени разрешенията за ползване на ресурса.

На споделените ресурси се задават имена (*share name*), които могат да са същите, каквито са били до момента, или да са нови. След споделяне на ресурсите е необходимо да се управлява достъпът до тях, който се състои от две основни дейности:

- Улесняване на достъпа до споделените ресурси за потребителите, които са оторизирани да осъществяват достъп до тях.
- Защита на споделените ресурси от неоторизиран достъп.

Двете задачи в известен смисъл са противоположни, но могат да се постигнат чрез използване на директорийните услуги (*directory services*). В компютърната мрежа може да се сподели всеки от апаратните и информационните ресурси, включително и периферните

устройства. Независимо от естеството на мрежовия ресурс, целта на споделянето е достъпност и контрол.

Споделените папки и файлове са най-често срещаните споделени ресурси в мрежата. Документите, предоставени за разглеждане и редактиране от множество потребители, е необходимо да се представят от едно единствено копие. Не се допуска потребител да създаде копие на документ на своя диск и да го предостави на останалите като мрежов ресурс. Правилният начин за съхранение на документите е записване и четене само от файловия сървър на мрежата. Причините за това изискване са следните:

- Администраторът може да гарантира, че всички документи се архивират съгласно приетия регламент.
- Ако някоя работна станция не е включена в мрежата или се повреди, няма проблем с ползването на документите от останалите.
- Документите, архивирани на един сървър, се откриват много лесно.

На всеки потребител може да се предостави собствена директория (*home directory*) на файловия сървър. Всичките данни, създадени от потребителя, се записват в собствена директория, разположена на диска в мрежовия сървър. Останалите потребители нямат достъп до тази директория. Домашните директории се архивират всеки път при планово архивиране на сървъра. Споделените папки могат да се идентифицират с една буква от азбуката, което улеснява достъпа до тях.

Споделянето на принтери и други периферни устройства е една възможност за постигане на по-висока ефективност на компютърната мрежа. Всеки потребител, на когото са дадени права, може да ползва услугите на принтера независимо дали е включен директно или към някой от компютрите на мрежата.

Приложните сървъри предоставят възможност на потребителите да ползват наличните приложни програми. По този начин приложенията са инсталирани само на сървъра и не заемат дисковото пространство на работните станции. Независимо че производителността на мрежата в този случай е по-ниска в сравнение с локалното разположение на приложенията, могат да се отбележат следните предимства:

- На работните станции се инсталират по-малки и евтини твърди дискове.
- Мрежовият администратор контролира конфигурирането на приложните програми.
- Всички потребители гарантирано ползват едни и същи приложения.
- Всяко приложение може да се обнови един път на сървъра.

Предлагането на комуникационни услуги е сериозно основание за свързването на компютрите в мрежа. По този начин всички абонати на мрежата ползват едно устройство за връзка с други мрежи или глобалната мрежа Интернет. Това се постига по следните способи:

- Използване на маршрутизатор, свързващ компютрите към Интернет, като всеки от тях разполага с IP адрес.
- Използване на софтуер за транслиране на мрежови адреси. В този случай компютрите се свързват към Интернет през хост, който ползва само един IP адрес.
- Използване на прокси сървър за адресно транслиране и гарантиране на сигурност на изходящите пакети.

3.6. Анализ на мрежовите операционни системи

Изборът на МОС за инсталиране е важно решение за всяка институция. Всяка операционна система има своите предимства и по-слаби страни. Когато се управляват големи компютърни мрежи, цената често се оказва важен аргумент за избора на МОС.

Мрежовите администратори знаят основните характеристики на съвременните операционни системи. Възможно е различните сървъри в мрежите да използват и различни видове МОС. По този начин може да се съчетаят предимствата на една и да се избягнат недостатъците на друга. Генерирането на хибридни компютърни мрежи изисква сериозни знания и умения от администраторите. Сложността на проблематиката произлиза и от факта, че различните производители на операционни системи използват едни и същи термини по различен повод. С термина root в UNIX се идентифицира акаунтът на администратора, в NetWare мрежите се използва за идентификация на обект, в Windows се отнася за домейн на върха на дърво от домейни. Трите най-използвани семейства МОС за изграждане на компютърни мрежи в практиката са [35]:

- Windows NT и Windows 2000 мрежи
- NetWare мрежи
- UNIX/Linux мрежи.

Windows сървърите се базират на концепцията за домейна. Домейнът е група от компютри и потребители, управлявани от един администратор. Независимо че са от една фамилия, Windows NT и Windows 2000 домейните взаимодействат помежду си по различен начин.

Microsoft използва термина „домейн", за да се опишат група от компютри, потребители и ресурси в областта на управление на един администратор. Използва се и терминът „домейн контролер", за да се опишат сървърите за автетификация, съдържащи копие от базата данни с акаунти за логване. Терминологията на Windows 2000 мрежите е известна на администраторите, които са работили с Windows NT 4.0.

Windows NT 4.0. има графичен интерфейс, подобен на Windows 95. Всеки NT домейн се нуждае от един главен контролер на домейн – PDC (*Primary Domain Controller*). Това е главният сървър, на който е изградена базата от данни за управление на акаунтите за сигурност. Този сървър е известен и като сървър SAM (*Security Accounts Management*). Всеки домейн се осигурява с един или повече резервни контролери на домейна – BDC (*Backup Domain Controller*). Всеки от резервните контролери на домейна е копие на базата данни за сигурност (SAM), който се използва само за четене.

Потребителите на мрежата могат да се логват и да се автентифицират от PDC контролера или от някой BDC контролер. Промяна в базата данни SAM могат да се правят само в главния контролер PDC, след което промените се нанасят в BDC контролерите. BDC контролерите служат за облекчаване на трафика при автентифициране на потребителите и за резерв, ако BDC контролерът откаже да работи. Когато PDC контролерът получи непоправим отказ, BDC контролерът може да се преинсталира като PDC контролер.

Инструментът за създаване и премахване на потребителски акаунти в Windows NT 4.0. е програмата *User Manager for Domains*. Тя позволява на администратора на компютърната мрежа следните възможности:

- Създаване на нови потребителски и групови акаунти.
- Преименуване, модифициране и изтриване на акаунти.
- Назначаване на пароли.
- Установяване на политика за акаунтите.
- Задаване на рестрикции спрямо правата на потребителите.

Мрежите, управлявани от Windows 2000, използват програмата *Active Directory* за съхраняване на информация, свързана със сигурността и достъпа до ресурсите. В директорията се създава йерархична база от данни. Домейните в Windows 2000 могат да се обединяват в дървета, а множествата от дървета се обединяват в гори. Този начин за управление на сигурността позволява мащабиране на мрежата до неограничен размер. В тази версия на Microsoft не се създават PDC и BDC контролери, а всички контролери на домейни имат копие в *Active Directory*. Администраторът може да прави промени в един домейн контролер, които се репликират в останалите домейн контролери.

За администрирането на акаунти в Windows 2000 се използва основата *Microsoft Management Console* (MMC). Този инструмент използва модули за специфични административни функции. Потребителите и групите се създават и управляват с модула *Active Directory Users and Computers*, който създава потребителите и ресурсите като контейнерен обект (организационна единица). С този инструмент администраторът има значително по-големи възможности в сравнение с Windows NT 4.0.

Изборът на мрежово устройство в Windows мрежова операционна система в сравнение с други МОС е улеснено и може да се извърши по два начина:

- чрез използване на Windows Explorer;
- чрез използване на команда **net use**.

За да се избере мрежово устройство с *Windows Explorer*, е необходимо да се достигне до папката на отдалеченото устройство. Отваря се менюто *Tools*, след което се избира *Map Network Drive*. Новите версии на Explorer позволяват изборът да стане чрез двукратно щракване с десния бутон на мишката върху името на папката, след което се избира командата *Map Network Drive* от контекстното меню. Избраното устройство се появява означено с буква в левия панел на Explorer заедно със CD устройствата и дяловете от твърдия диск. От този момент нататък може да се осъществява достъп до това устройство от Windows Explorer, My Computer или от Desktop, ако е изграден *Shortcut* към него.

Избор на устройство с команда **net use** става с използване пътя на конвенцията за универсалните имена – UNC (Universal Naming Convention). Идентификация на споделен ресурс се извършва чрез следния синтаксис:

\\име_на_компютър\име_на_споделен_ресурс

За да се избере мрежово устройство, към споделеното устройство е необходимо да се напише следният команден ред

net use буква_на_устройството:
\\име_на_компютър\име_на_споделен_ресурс

За да се сподели принтер, свързан към локален компютър, е необходимо да се избере папката Printers, достъпна от Control Panel, след което с десния бутон на мишката се избира името на принтера. Избира се програмата *Sharing* и се щраква върху *Shared as*, след което се въвежда името на споделения принтер.

Съществуват два начина да се сподели принтер, който е включен към друг компютър в мрежата:

- използване на съветника *Add Printer Wizard*;
- използване на командата **net use**.

Най-лесният начин да се използва отдалечен принтер в Windows компютърните мрежи е да го изберете с програмата *Add Printer Wizard*. За целта е необходимо да се щракне два

пъти върху иконата *Add Printer* в папката *Printers* и да се следват по-нататъшните инструкции. Когато съветникът приключи работата си по инсталацията, мрежовият принтер се появява в папката *Printers* на компютъра. От този момент приложенията на отдалечения компютър могат да се отпечатват като на локален принтер. Зададените за печат документи се подреждат обикновено на твърдия диск и изчакват реда си. Списъкът на чакащите документи се нарича *принт спул* (print spool).

Командата **net use** може да се използва за пренасочване на задания за печат от локален порт (LPT1) към мрежов принтер. Командата, която се въвежда за това действие, е следната:

net use LPT1: *\\име на компютър\име на споделен ресурс*

Името на компютъра е принт сървъра, към който е включен мрежовият принтер.

NetWare мрежите стартират своето развитие с МОС версия NetWare 3.x., която работи с протоколния стек IPX/SPX. NetWare 5.1. е МОС, която има възможност да работи с протоколния стек TCP/IP.

Мрежовата операционна система NetWare 3.x. използва база от данни *binderi*, която се създава на всеки сървър. Тази база от данни съхранява информация за акаунтите само на компютрите, на които е инсталирана. Когато в компютърната мрежа има повече от един сървър, потребителите трябва да имат акаунти за сървърите, до споделените ресурси на които искат да имат достъп. Това изискване затруднява в голяма степен администрирането на мрежата. Във версия NetWare 3.11. са въведени допълнителни зареждащи модули NLMs (NetWare loadable modules). Това са инструменти и драйвери, които се инсталират на сървъра, за да се подобри функционирането му.

Във версия NetWare 4. е въведена сложна директорийна услуга NDS (Nowell Direktory Services), която разрешава проблемите, свързани с изискването на база от данни за сигурност на всеки сървър. NDS е разпределена база от данни, която позволява на потребителите да се логват на един сървър с един потребителски акаунт и да реализират достъп до всички мрежови ресурси. Базата данни NDS е построена по йерархичен модел и е организирана като дърво. Тя има аналогичен модел с Active Directory на Microsoft. И двете бази от данни имат обща концепция за организационните единици и възможностите за откриване на обекти в дървовидна директорийна структура, без да се знае къде са разположени ресурсите в мрежата.

Администрирането на NetWare 3.x. изисква създаването на два акаунта: Guest и Supervisor. Потребителите с акаунта Guest имат ограничен достъп до мрежовите ресурси, а акаунтът Supervisor предоставя административни права. Мрежовите операционни системи NetWare версии 3. и 4. имат само един акаунт, наречен Admin. Акаунтите на МОС NetWare 4.x се създават с един от следните инструменти:

- NetWare Administrator за Windows клиент, на който се изпълнява NDS клиентски софтуер.
- NETADMIN – текстово базиран инструмент, който може да се стартира от DOS.

NetWare версия 5. има графична конзола, написана на Java, наречена **Console One**, която позволява отдалечено администриране. Тя е проектирана, за да се създадат административни инструменти. МОС NetWare версия 5. може да се администрира през стандартната клавиатура от командния ред или от базирана на менюта програма *Monitor*. В NetWare 5.1. е въведен NetWare Management Portal, който е Web-базиран инструмент, позволяващ управление на NetWare 5.1. сървъри от клиентски компютри през Web браузер.

Клиентските станции се управляват от локална операционна система, за която е създаден NetWare клиентски базов софтуер. Novell са създали клиентски софтуер за DOS и всички версии на Windows. От своя страна Microsoft имат създаден базов софтуер за

NetWare клиенти в Windows операционните системи. За Macintosh и Linux също има клиенти, които са създадени от независими производители на софтуер.

Избиране на ресурс от Windows сървър може да се направи чрез Windows Explorer. Процедурите са същите, както при използване софтуера на Microsoft. Възможно е да се избере устройство и от командния интерпретатор, като се използва командата **map** със следния синтаксис:

map име_на_устройството:=сървър\том:директория\поддиректория

Клиентският софтуер на Novell има опция за избор на устройство като главно (root) или като устройство за търсене(search drive).

За да се отпечата документ на мрежов принтер, може да се използва и командата **capture** за пренасочване на заданията за печат от локалния порт към порта на мрежовия принтер. Синтаксисът на командата **capture** е следният**:**

Capture L=< номер_на_порт>Q=<име_на_опашката> P=<име_на_принтера>

В операционната система NetWare в опашката на мрежовия принтер (printer queue) са съхранените документи, които чакат ред за отпечатване, подобно на принт спула в Windows компютърните мрежи.

UNIX (Linux) мрежовата операционна система е разработена през 1969 г. и оттогава е претърпяла много сериозно развитие. Сорс кодът на софтуера е написан на езика С и е отворен за модификация и допълнения. Бизнес организациите, академичните среди и дори отделни физически лица могат да разработват свои версии. Тази МОС се инсталира в работни станции от висок клас. UNIX може да работи под управление на команден интерпретатор и с графичен потребителски интерфейс.

Linux е UNIX базирана операционна система, предназначена да работи с Intel процесори и съвместими с тях персонални компютри – PC. МОС Linux е разработена през 1990 г. от Линус Торвалдс. Както UNIX, Linux е МОС с отворен код и съществуват множество различни варианти.

Административният акаунт в UNIX и Linux за поддържане на системата се нарича **root.** Използват се и акаунтите **bin** и **sys** за стартиране на програми. Сървърните услуги в UNIX се наричат *демони (deamons).*

Съществуват различни версии на МОС UNIX, като най-използваните в практиката са:

- Berkeley Software Design, Inc.(BSD UNIX)
- Santa Cruz Operation (SCO) UNIX
- Sun Solaris
- AIX (UNIX на IBM)
- HP-UX (UNIX на Hewlett Packard).

Отвореният сорс код на UNIX има своите положителни и отрицателни страни. От една страна, разработчиците имат свободата да подобряват и да правят специфични настройки на системата. От друга страна, липсата на стандартизация води до затруднения в администрирането и разработката на приложения за тези мрежи. Независимо че операционната система UNIX се свързва с високи цени и изискване за скъп хардуер, с разработката на Linux все повече потребители я инсталират на своите компютри (PC).

Операционната система Linux също е предназначена да работи с Intel съвместими персонални компютри. Тази МОС притежава качествата на UNIX и става все по-приложима за домашните компютри и мрежите на бизнеса. Съществува широк кръг от версии на операционната система, някои от които се разпространяват комерсиално, други безплатно. Най-широко използваните версии са:

- RedHat Linux

- OpenLinux
- Slackware
- Debian GNU/Linux
- SuSE Linux.

Списък на актуалните версии и дистрибуции на Linux може да се намери на Web сайта с адрес: WWW.linux.org.

Мрежовата информационна система NIS (Network Information System) може да се използва за администриране на UNIX сървъри. Тази система позволява достъп на потребителите до мрежовите ресурси само с едно логване.

За да се добави потребителски акаунт в UNIX и Linux от администраторите, е необходимо да се използва командата **adduser** със синтаксис:

име_на_потребител:/# adduser

Потребителските акаунти се управляват с редактиране на файла **/ets/passwd.** Повечето версии на UNIX и Linux предлагат скриптове, които задават въпроси и водят по схема администратора при създаване на потребители. В операционната система Windows се използват аналогични съветници.

UNIX поддържа групи за управление на потребителските акаунти по отношение на мрежовите ресурси. Групите се създават с командата **addgrup**, а управлението се извършва чрез модифициране на файла **/ets/groups**. Повечето версии предлагат и графични иструменти за администриране, което в значителна степен улеснява администраторите на компютърните мрежи.

Файловата система клиент/сървър – NFS (Network File System), е разработена от Sun Microsystems. Тя може да се инсталира и на Windows клиенти с помощта на софтуер като Solstice Network Client на компанията Sun. Windows клиентите имат достъп до UNIX сървъри без клиентски софтуер, ако сървърите изпълняват програмата **Samba**, която използва протокола SMB , работещ в приложния слой на комуникационния модел.

Изборът на устройства в UNIX мрежите става с командата **mount,** която има следния синтаксис:

mount име_на_сървър:/директория/поддиректория/локална_директория

Обозначението на локалната директория, която посочва мястото на отдалечения ресурс, се посочва от първата част на командата, която се нарича точка за монтиране на директория (directory mount point). Тази точка трябва да съществува, преди да се прикрепи споделен ресурс към нея.

Изборът на мрежов принтер в UNIX мрежите става с помощта на командата **lpr.** Принт сървърът изпълнява програмата **lpd** (line printer deamon), която има следния синтаксис:

Lpr –p име_на_принтер _име_на_файл

Когато командата се въведе без име на принтер, заданието се изпраща за отпечатване на подразбиращия се принтер.

По-голямата част от персоналните компютри работят под управлението на една или повече от разгледаните дотук МОС: Windows NT или Windows 2000; NetWare и UNIX/Linux. Освен тези, съществуват и други МОС, като: Banyan VINES, OS/2 Varp Server, Apple NOS и LANtastic. Тези операционни системи предлагат централизирано администриране на компютърните мрежи и имат своето специфично приложение.

Въпроси за самостоятелна работа

1. Какви са основните функции на ОС?
2. Какви са различията между локалната и мрежовата ОС?
3. Кои са основните принципи на мрежовото администриране?
4. Кои ресурси на компютърните възли са споделени?
5. Кой управлява достъпа до мрежовите ресурси?
6. Как се инсталира мрежовият принтер?
7. Как се предоставя файловата система на компютър за ползване от останалите?
8. Кои мрежови операционни системи са актуални в момента?
9. Кои са предимствата и недостатъците на КМ с равноправен достъп?
10. Кои са предимствата и недостатъците на КМ тип клиент/сървър?

ГЛАВА 4. СТАНДАРТИ ЗА ИЗГРАЖДАНЕ НА ЛОКАЛНИ КОМПЮТЪРНИ МРЕЖИ

4.1. Обосновка на стандартизацията на компютърните мрежи

Утвърдените в световната практика мрежови модели не са единствени. Производителите на компютри, комуникационно оборудване и мрежов софтуер имат относителна самостоятелност, но не е в техен интерес да произвеждат и да не могат да реализират своите високотехнологични изделия и софтуер. Създадените в областта международни организации публикуваха редица спецификации и стандарти за изграждане на компютърни мрежи. Макар някои документи да имат препоръчителен характер, много скоро потребителите и производителите започнаха да се съобразяват с изискванията за съвместимост между мрежовите устройства и програмните средства. Международната организация по стандартизация ISO регистрира стандартите за изграждане на компютърните мрежи като документи споразумения, съдържащи технически спецификации, критерии и правила. Световният пазар също изигра голяма роля в процеса на създаване на стандартите за изграждане на компютърните мрежи. Производителите бързо се убедиха, че ако се съобразяват със стандартите, ще реализират по-големи печалби. Организациите, които имат значение за стандартизацията на компютърните комуникаци, са: International Standardization Organization – ISO, International Electrotechnical – IEC, International Telecommunication Unit – ITU, Internet Engineering Task Force – IETF и IEEE [35].

ISO е федерация на националните ведомства по стандартизация. Формирана е през 1947 г. с цел разработване на международни стандарти в предметните области на човешката дейност. В областта на компютърните мрежи ISO работи в тясно сътрудничество с международните организации ITU, IEC, IETF и IEEE.

ITU е международна организация за изработване на документи и стандарти в областта на телекомуникациите.

IEC е създадена още през 1906 г. с предмет на дейност установяване на световни стандарти в областта на електро- и електронния инженеринг. През 1967 г. IEC сключва споразумение с ISO за съвместна работа по разработка на стандарти и споразумения.

IETF е организация, съставена от работни групи за решаване на проблеми, свързани с разработване на стандарти за Интернет. Членството в тази организация е отворено за заинтересованите човешки общности. Основна задача на работните групи на организацията е разработка на интернет проекти, превръщането им в официални документи. Тези документи се одобряват по установен ред и се превръщат в интернет стандарти. Публикуват се като характеристики на мрежови услуги и протоколи по наименованието RFC. (xxxx).

IEEE е международна организация на електроинженерите, структурирана по общества, като най-голямото общество е компютърното. На научни форуми на организацията са обсъдени и приети спецификации и стандарти за физическия и каналния слой на отворения комуникационен модел. Известни са като проект IEEE 802. XX с номера от 01 до 16, приети окончателно през 1980 г., месец февруари.

Подробна информация за характеристиките и мрежовите услуги на протоколите се съдържа в база данни, която е достъпна за потребители. Всеки протокол може да бъде изтеглен и разпечатан от Интернет с име „RFC номер на протокола”. В съдържанието на обяснителната записка са включени елементи като:

- реализация на услугата;
- разширения на протоколния стек TCP/IP;
- спецификация за софтуер от типа Network Address Translation (NAT).

Заинтересовани страни и организации, както и юридически лица могат да предлагат RFC спецификации. Не всички RFC документи се превръщат в стандарти. Когато някой документ се предлага за стандарт, той се обсъжда и утвърждава, като движението му преминава през 3 етапа:

- предложение на стандарта;
- експериментиране на стандарта;
- утвърждаване на Интернет стандарт.

В базата данни има документ с инициали RFC 2226 – Инструкция за автори- (fttp://ftp.isi.edu/in-notes/rfc2026.txt). В този документ е дадена методика за създаване на проект за стандарт. Предложените проекти се обсъждат и ако бъдат одобрени, се редактират и публикуват с един от следните статуси:

- задължителен статус
- препоръчителен статус
- незадължителен статус
- статус на ограничено използване (не е предназначен за масова реализация)
- не се препоръчва за реализация.

Стандартите за изграждане на компютърните мрежи условно могат да се разделят на две основни групи:

- Стандарти за изграждане на локални компютърни мрежи.
- Стандарти за изграждане на глобални компютърни мрежи.

4.2. Стандарти за изграждане на локални компютърни мрежи

4.2.1. Канален слой на локалните компютърни мрежи

Тъй като в локалните компютърни мрежи се ползва обща комуникационна среда, каналният слой е разделен на два подслоя:

- **Горен подслой** – за формиране на кадрите и управление на логическия канал – LLC (Logic Link Control)
- **Долен подслой** – за управление на достъпа до комуникационната среда – MAC (Media Access Control) .

Функциите на каналния слой в LAN се реализират от мрежовия адаптер. Той се инсталира в слота за разширение на крайния мрежов възел.

MAC подслоят управлява разпределението на комуникационната среда между мрежовите възли. При предаване MAC подслоят получава от LLC подслоя LLC блок данни, които се вграждат в поле <данни> на кадъра. Към кадъра се добавят: MAC адрес на подателя и MAC адрес на получателя. Следва кодиране на тези полета с шумоустойчив код и запис на контролното число в контролното поле. Кадърът се ограничава в началото и края с флагове и се предава на физическия слой, който го изпраща на получателя във вид на структуриран поток от данни. MAC подслоят на получателя разпознава MAC адреса и ако не се открият грешки при предаването, кадърът се предава към LLC подслоя на приемащия възел за по-нататъшна обработка.

LLC подслоят получава пакети от мрежовия слой, формира и номерира LLC блокове (кадри или фреймове), контролира и коригира грешки и допълнително определя последователността на кадрите. По заявка от мрежовия слой прекъсва връзката с

комуникационната среда. Функциите на LLC подслоя съгласно стандарт IEEE 802.2. се състоят от три типа услуги:

- **Тип 1 (LLC1)** – осигурява се предаване на данни между два мрежови възела без установяване на логическо съединение и без потвърждение (дейтаграмен режим без потвърждение). Коригирането на възникналите грешки се извършва в по-горните слоеве.
- **Тип 2 (LLC 2)** – за предаване на данни между два възела с установяване на логическо съединение (режим на виртуално съединение). Използва се методът "плъзгащ се прозорец" с размер на прозореца 8 или 128 кадъра.
- **Тип 3 (LLC3)** – за предаване на данни без установяване на логическо съединение, но с потвърждение.

Стандарт IEEE 802.2. групира тези типове услуги в 4 класа:

- клас 1 – услуга тип LLC1;
- клас 2 – услуги тип LLC1 и LLC2;
- клас 3 – услуги тип LLC1 и LLC3;
- клас 4 – услуги тип LLC1, LLC2 и LLC3.

Фиг. 9.1. Структура на LLC блок

Структурата на LLC блока е представена на фиг. 9.1. Полета <DSAP> (Destination Service Access Point) и <SSAP> (Source Service Access Point) идентифицират протокола на по-горния (мрежов) слой, като по този начин позволяват в една и съща мрежа да се използват различни протоколни стекове.

Полето <данни> съдържа част от данните на пакета на мрежовия слой.

Полето <управление> съдържа управляваща информация за правилно функциониране на LLC подслоя.

4.2.2. Международни стандарти за физически и канален слой на LAN

Международните стандарти за физическия и каналния слой на LAN са създадени от компютърното общество на Международната организация на електроинженерите IEEE (Institute of Electrical and Electronics Engineers) и имат означение, свързано с реализацията на проекта IEEE 802. Името на проекта е формирано от времето на заседание на Комитета по стандарти на организацията – 1980 година, месец февруари. В резултат на изпълнение на проекта се установяват следните стандарти 802.xx за физическия и каналния слой на локалните компютърни мрежи [34]:

- **IEEE 802.1.** Въвеждащ стандарт за локалните и градските мрежи. Дефинират се мостовете, действащи в MAC подслоя на алгоритъма STA (Spanning – Tree Algorithm). Този алгоритъм предотвратява комуникационни проблеми от рода зацикляне на процедури.

- **IEEE 802.2.** Стандарт, съгласно който в съответствие с комуникационния модел OSI каналният слой в локалните компютърни мрежи се разделя на два подслоя: долен – MAC (Media Access Control) подслой и горен LLC (Logical Link Control) подслой.
- **IEEE 802.3.** Този стандарт определя правилата за работа на Ethernet мрежите. Тези мрежи използват метода на множествен достъп с разпознаване на носещата честота и откриване на колизиите (CSMA/CD). В стандарта е дефинирана структурата на Ethernet кадрите (фреймовете). В началото стандартът е описвал локални компютърни мрежи с линейно-шинна топология, използващи коаксиални кабели за изграждане на комуникационната среда. По-късно стандартът е развит и допуска използване на кабел тип усукана двойка и изграждане на мрежа по топология тип звезда.
- **IEEE 802.4.** Този стандарт е известен под името Token Bus и описва мрежи, реализирани по логическа и физическа топология тип шина. Комуникационната среда се изгражда от коаксиален кабел с вълново съпротивление 75 ома или оптически влакна. Методът за достъп е реализиран чрез предаване между абонатите на мрежата на служебен маркер.
- **IEEE 802.5.** За идентификация на стандарта се използва името Token Ring. Описва се компютърна мрежа с физическа топология звезда и логическа топология кръг. Предвижда се възможност за използване на кабел с екранирана и неекранирана усукана двойка. Методът за достъп на компютрите до комуникационния канал се реализира с помощта на служебен маркер, който се предава последователно.
- **IEEE 802.6.** Стандартът описва големи локални компютърни мрежи. Наричат се още градски компютърни мрежи – MAN (Metropoliten Area Network).
- **IEEE 802.7.** Стандартът описва правилата за изграждане на компютърни мрежи по технология широколентово предаване. Използва се методът FDM (Frequency Division Multiplexing). По един и същ кабел едновременно се изпращат различни сигнали на различни честоти.
- **IEEE 802.8.** Този стандарт описва спецификации за изграждане на комуникационна среда от оптически влакна. За означаване се използва абревиатурата FDDI (Fiber Distributed Data Interface).
- **IEEE 802.9.** Установяват се правилата за предаване на глас и данни по стандарта за изграждане на глобалната компютърна мрежа ISDN.
- **IEEE 802.10. LAN Sequrity.** Този стандарт описва изграждането на виртуалните частни мрежи VPN (Virtual Privit Network). Тези мрежи осигуряват сигурни връзки на чстните локални мрежи през глобалната мрежа Internet.
- **IEEE 802.11.** Стандарт за реализиране на безжични компютърни мрежи по LAN технологии.
- **IEEE 802.12. 100 VG AnyLAN.** Този стандарт е разработен от Hewlett Packard и описва компютърни мрежи, при които методът за достъп до комуникационната среда е приоритет по заявка. Комбинирани са предимствата на компютърните мрежи Ethernet, Token Ring и ATM в едно високоскоростно предаване на данни.
- **IEEE 802.15.** Стандарт, който описва радиомрежата за близка комуникация Bluetooth.
- **IEEE 802.16. C**тандарт, който регламентира поддържането на широколентови безжични системи, предназначени за градски (MAN) компютърни мрежи.

4.3. Стандартът IEEE 802.3. Ethernet

Стандартът IEEE 802.3. е най-използваният в практиката и по същество се явява развитие на създадения стандарт Ethernet от фирмите INTEL, XEROX и DEC. Физическият слой на стандарта IEEE 802.3. описва локална мрежа с логическа топология тип ШИНА. Скоростта на предаване на данни е 10 Mb/s , а в последните версии са достигнати скорости от 100 Mb/s до 1 Gb/s. Използват се два метода на предаване на данни по комуникационния канал:

- директно цифрово предаване (baseband);
- модулирано аналогово предаване (broadband).

При директното цифрово предаване на данни се използва или цялата честотна лента на комуникационната линия, или само един канал за предаване на данни. Кодираният сигнал е цифров, модулиран с манчестерски или диференциален манчестерски код. Данните се предават едновременно в двете посоки на комуникационния канал. Покриват се малки разстояния поради затихването на сигнала и загубите в комуникационната линия.

При модулираното аналогово предаване на данни се осигурява повече от един канал. Честотната лента на кабела се разделя на отделни канали, по които се предават аналогови сигнали от различни възли на компютърната мрежа. Предаването на данни се извършва само в една посока на шината, след което следва превключване в обратна посока с друга честота. Този начин на предаване се нарича разделено модулирано предаване (mid-split-broadband). По стандарта IEEE 802.3. е възможен и друг вариант на предаване – с използване на два кабелни канала (dual-cable-broadband) – единият за предаване, другият за приемане. В този случай предаването и приемането се извършва на една работна честота.

Стандартът IEEE 802.3. има различни версии, които ползват общото обозначение **<V>, <метод>, <L>,** където:

- V е скоростта на предаване в Mb/s;
- Метод – Base за директно предаване и Broad за модулирано предаване;
- L е дължината на сегмента (кабела между 2 съединения на терминатори) в метри.

Когато са използвани обозначенията:

- $L = \{T, T_x, T_4\}$ (Twisted pair), това означава, че в LAN се използват кабели с усукана двойка проводници.
- $L = \{F, F_x\}$, това означава, че в LAN се използва влакнесто-оптичен кабел (Fibre optics).

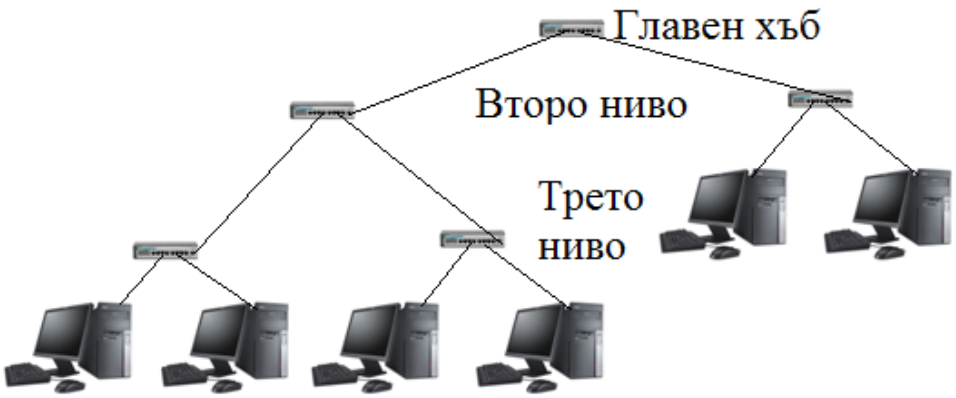
При стандартите 10 Base T и 10 Base F физическата топология на мрежата е ЗВЕЗДА , но логическата топология остава тип ШИНА.

Мрежовите възли се свързват към концентратор (HUB), който изпълнява роля на множествен повторител. Стандартът 10 Base T използва за връзка две неекранирани усукани двойки проводници – едната за предаване, другата за приемане. При стандарта 10 Base F се използва двойка оптични влакна (едното за предаване, другото за приемане).

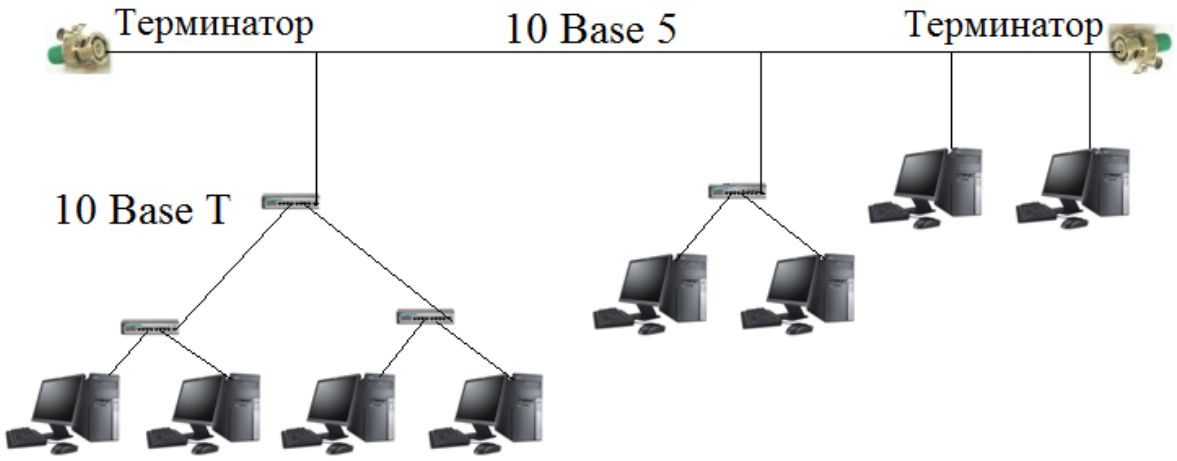
Концентраторите могат да се свързват йерархично най-много до три нива – фиг. 9.2. На първо ниво има само един главен концентратор и той работи като множествен повторител. Останалите концентратори имат по един UP порт за връзка с горния концентратор (HUB), и няколко DOWN порта за връзка с концентратори, сървъри или работни станции от по-ниско ниво.

При постъпване на кадър на един от DOWN портовете на концентратора той го пренасочва през своя UP порт към горния концентратор. Обратно, при постъпване на кадър

на UP порта (отгоре) той го предава надолу чрез своите DOWN портове. По този начин се съхранява логическата шина и генерираният кадър от някой възел достига до останалите възли, а в случаи, когато два възела генерират едновременно кадри, възниква конфликтна ситуация.



Фиг. 9.2. Схема на локална мрежа на три нива, изградена по стандарт 10 Base T



Фиг. 9.3. Приложение на мрежа 10 Base 5 като гръбнак за мрежа 10 Base T

Необходимо е да се спазва правилото, че между всеки два възела в мрежата може да има не повече от четири концентратора. Ако това условие не може да се изпълни, се поставя комутатор за разделяне сегментите на мрежата.

Пример за смесена версия на стандарт IEEE 802.3. е показана на фиг 9.2. В този случай се спазва правилото 5 – 4 – 3, което означава:

- Между две работни станции или два сървъра може да има само пет кабелни участъка (сегмента).
- Между две работни станции може да функционират само четири концентратора.
- Между две работни станции може да функционират само три сегмента с работни станции (сървъри).

През юни 1995 г. компютърното общество на IEEE одобри нова версия на стандарта 802.3.u. (Fast Ethernet) със скорост на предаване на данни 100 Mb/s. Това е допълнение към стандарта 802.3. През юни 1998 г. IEEE одобри стандарта 802.3.z. за изграждане на комуникационна среда с влакнесто-оптични кабели. През март 1999 г. IEEE одобрява стандарта 802.3.ab. за UTP кабели, категория 5. Тези стандарти са известни като Gigabit Ethernet за предаване на данни със скорост до 1 Gb/s.

В стандарта IEEE 802. 3. MAC подслоят се управлява от протокол CSMA/CD – (Carrier Sense Multiple Access With Collision Detection), т. е. множествен достъп с откриване на носещата честота и разпознаване на конфликтите. Протоколът допуска, че всички мрежови възли са равноправни. Всички предават по общата комуникационна среда, като се състезават помежду си. Възлите в компютърната мрежа сами разпознават дали шината е заета или свободна.

След заявка от по-горен слой протоколът CSMA/CD формира кадър, който се предава едновременно в двете посоки на шината. Възможно е в този момент и друг възел да установи, че шината е свободна, и той също да изпрати кадър, тъй като сигналът от първия възел се разпространява със закъснение. В този случай възниква конфликт между двата кадъра. Налага се мрежовите адаптери да "подслушват" канала, докато предават съобщения. След конфликт възелът, разпознал конфликта, предава по комуникационната среда заглушаващ сигнал. Всеки възел, участвал в конфликт, изчаква различен интервал от време, чиято продължителност се формира по случаен закон, преди отново да изпрати нов кадър. След шестнадесет неуспешни опита мрежовият адаптер изпраща към горните слоеве на комуникационния модел сигнал за инициализация на мрежата. Ако при разпространение на кадъра в шината няма конфликт, той се приема от получателя и каналът се освобождава. При скорост на предаване 10 Mb/s поради наличие на конфликти и необходимо време за изчакване на практика реалната скорост намалява до 3 Mb/s.

Всъпи-телна част	Начален ограни-чител (SFD)	MAC – адрес на В. по-лучател	MAC – адрес на възел-подател	Дължи-на	Данни LLC блок	PAD	Контрол но поле (FCS)
7	1	2 V 6	2 V 6	2	0 ÷1500	46/0	4 байта

Фиг. 9.4. Формат на кадър на MAC подслоя за протокол CSMA/CD

Встъпителната част на кадъра (фиг. 9.4) е от седем байта, всеки от които има стойност $(10101011)_2$ и заедно с <началния ограничител > $(10101011)_2$ се използват за синхронизация и определяне началото на кадъра. MAC адресът на възела подател се ползва от получателя, за да определи от кой възел идва съобщението. MAC адресът на получателя определя за кой възел е съобщението. Ако първият бит е 0_2, то кадърът е за един получател. Ако първият бит е 1_2, то кадърът е предназначен за група получатели (multicast адресиране). Ако всички битове са 1_2, кадърът е предназначен за всички възли в мрежата (broadcast адресиране). В полето <дължина > се посочва дължината на полето <данни>. То може да е от 0 до 1500 байта. Ако данните са с дължина, по-малка от 46 байта, се използва полето <PAD> за допълване на поле <данни> до 46 байта. Ограничението от минимална дължина на поле <данни> 46 байта се налага, за да има достатъчно време да се върне заглушаващият сигнал при конфликт. Полето <FSC> се използва за кодиране на данните (без първите две полета) с шумоустойчив код (CRC – 32), което дава възможност на възела получател да установи дали кадърът е приет с грешки или коректно.

Стандартът IEEE 802.3. позволява локалните компютърни мрежи да се комутират, в резултат на което комуникационната среда престава да е обща. При достигане на максималния капацитет на мрежата се използват комутатори, които обикновено се поставят на мястото на концентраторите.

Комутаторът е устройство с високоскоростна вътрешна комутационна матрица. Когато мрежов възел, свързан към комутатора, изпрати към него 802.3.-кадър, той проверява дали възелът, за който е предназначен, е свързан в мрежата на подателя. Всеки комутатор има от 4 ÷ 32 линейни платки, всяка от които има 1 ÷ 8 порта. Когато получателят е свързан към същата линейна платка, кадърът се копира (предава) директно към съответен порт, без да се използва вътрешната комутационна матрица. В противен случай кадърът се предава чрез матрицата към съответната линейна платка, а тя го предава към порта на получателя. Когато към порта на комутатор е свързан концентратор, отделните възли, включени към него, се състезават помежду си за достъп до порта, както при некомутираните 802.3. компютърни мрежи. В случай, когато на два и повече порта на една линейна платка постъпят едновременно различни кадри, се използват два начина за решаване на такива конфликти.

В **първия случай** не се разрешава едновременно предаване на кадри и всяка платка може да извършва само една комуникация.

Във втория случай всички портове на една линейна платка могат да предават кадри едновременно. За целта всеки порт се буферира с RAM памет и кадрите се натрупват в съответен буфер. По този начин производителността на комутираната мрежа се увеличава.

4.4. Изследване на локална компютърна мрежа IEEE 802.3. Ethernet

Като обект на изследване локална компютърна мрежа на три нива, изградена по стандарт IEEE 802.3. Ethernet, е представена на фиг. 9.5. На първото ниво на локалната мрежа е включен комутатор и свързан към него DHCP сървър. На второ ниво са включени три комутатора и свързани към всеки от тях компютри. Трето ниво се състои от шест комутатора и свързани към тях компютри. Комуникационният канал на локалната мрежа е изграден от кабел UTP – категория 5.

Управлението на потока от данни (flow control) между възлите в компютърните комуникации се извършва по два метода:

- старт-стопен метод;
- метод на управление “хлъзгащ се прозорец”.

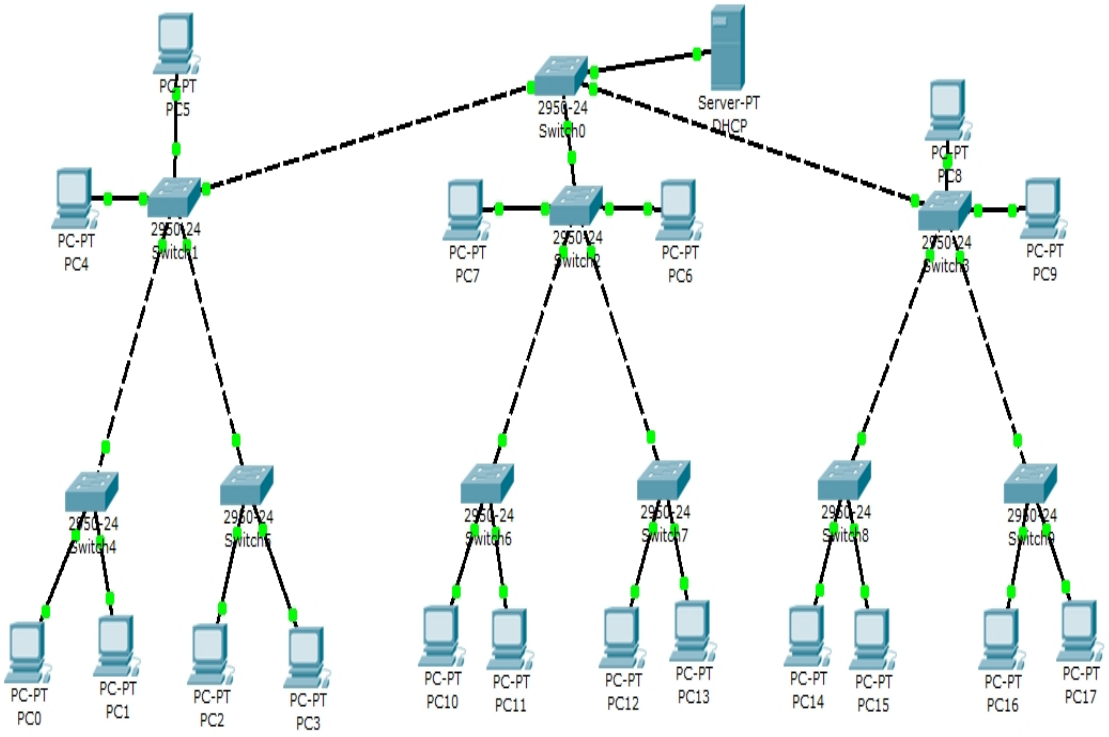
Старт-стопен метод за управление на потока от данни (Alternating Bit Protocol) се прилага при свързване на компютри с асинхронните модеми за предаване на данни. Източникът на съобщението изпраща в канала за предаване на данни само един кадър, след което се чака квитанция от получателя за правилно приемане и след получаването й се излъчва следващият кадър.

Използва се механизмът на ***таймаута***, при който, ако не се получи положителна квитанция в течение на зададен интервал от време, то кадърът се повтаря. Ако по обратния канал се “загуби” положителна квитанция, след таймаута се предава отново същият кадър. За да не се дублират тези кадри, се използва поредният номер на кадъра в служебната част на кадъра. Този номер за всеки кадър е уникален и се съхранява при повторно предаване. Предаването на квитанцията изисква допълнително време и това се счита за недостатък.

Метод на управление “хлъзгащ се прозорец” се използва от семейство LAP протоколи. В канала с един прозорец се предават N кадъра един след друг. N е размер на прозореца и зависи от сумарното закъснение на сигнала в права и обратна посока. Предавателят

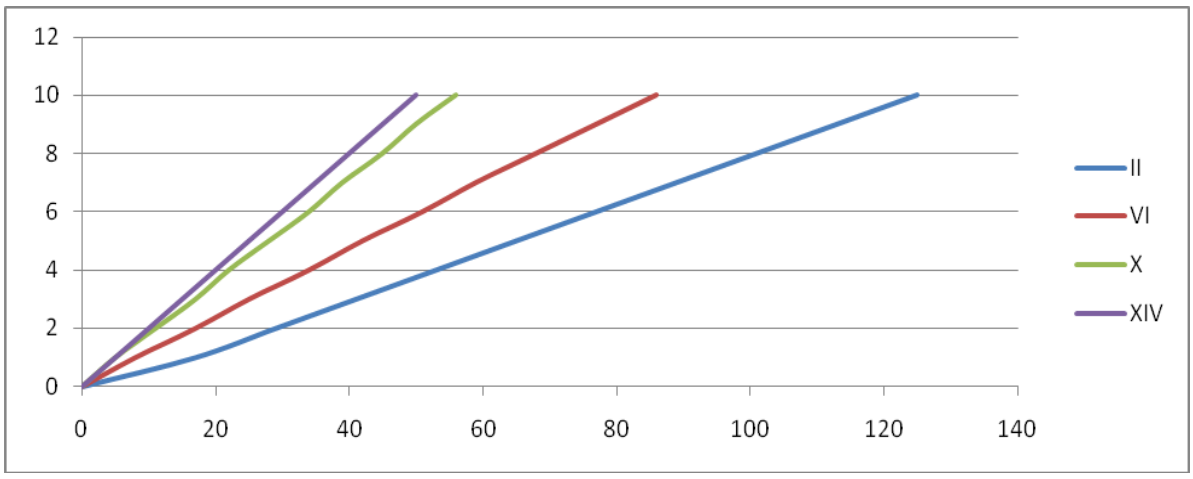
предава прозорец от N кадъра в канала до момента на получаване на първата квитанция на приемника. Квитанциите се издават или в съответствие с номера на кадъра, или за последния кадър от групата на приетите кадри.

Протоколите от семейство LAP използват две широчини на прозореца от протоколни единици: нормална, при която широчината на прозореца е N = 8 (кадъра), и разширен прозорец, при който N = 128 кадъра. За проведеното изследване е приет широкият прозорец за предаване на кадрите по стандарта IEEE 802.3. Ethernet. Връзките между комутаторите от трите нива на компютърната мрежа са изградени съгласно фиг. 9.5.



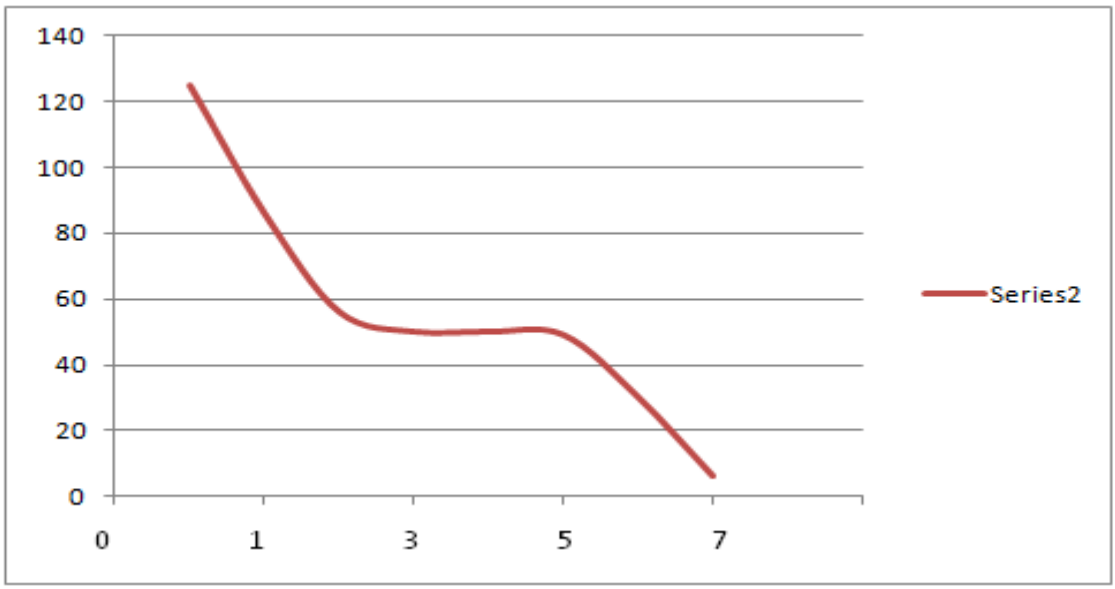
Фиг. 9.5. Схема на локална мрежа на три нива

Резултатите от изследването на трафика при едновременна комуникация на две, шест, десет и четиринадесет двойки компютри е показана на фиг. 9.6.



Фиг. 9.6. Ефективност на компютърната мрежа

Производителността на компютърната мрежа, измерена в брой пакети, предадени за една секунда в зависимост от броя на двойките комуникиращи компютри, е показана на фиг. 9.7.



Фиг. 9.7. Характеристика на трафика в мрежата за различен брой комуникации

Локалната мрежа на три нива е симулирана на програмния продукт Packet Tracer. Packet Tracer е програма за мрежова симулация, създадена от Cisco. Главната цел на фирмата е да се създаде инструмент за използване в учебния процес на Cisco академията. Програмният пакет позволява да се създаде мрежа с голям брой симулирани реални мрежови възли, така че да се тестват различни конфигурации и опции на компютърната мрежа. Съществува възможност да се емулират рутери, комутатори, крайни клиентски системи и връзки, за симулиране на различни конфигурации на мрежата. Операционните системи на рутерите и дори на част от компютрите също са симулирани. По този начин потребителите могат да се научат да конфигурират рутери и да оценят промените, които могат да направят по мрежата. Възможно е да симулират и опциите на оборудването за достъп до реалните компютърни мрежи.

В резултат на симулацията могат да се изследват следните параметри на компютърните мрежи:

- топология на мрежата;
- скорост за предаване на данните между абонатите;
- коефициент на грешка в комуникационния канал;
- производителност на локалната компютърна мрежа;
- максимален брой на едновременно обслужваните абонати при зададена производителност на мрежата.

Резултатите от проведените изследвания са представени графически на фиг. 9.6 и фиг. 9.7. Направено е изследване на производителността на компютърната мрежа в зависимост от броя на абонатите, които обменят съобщения едновременно. Приета е дължина на кадъра от 1500 байта и метод на обмен на данни „хлъзгащ се прозорец” с дължина от 128 кадъра. Броят на комуникиращите двойки компютри се изменя от два до седем. От фиг. 9.7 се вижда, че производителността на мрежата е стабилна при едновременна комуникация на две до пет

двойки компютри. При едновременна комуникация на повече от пет двойки производителността на компютърната мрежа намалява значително.

От направените изследвания могат да се направят следните изводи и препоръки за практиката по изграждане на локални компютърни мрежи на три нива:

- Максималната скорост за предаване на данни в LAN на три нива при зададения брой абонати достига 2,097mbps.
- Производителността на изследваната локална компютърна мрежа при 6 комуникиращи двойки компютри е 7680 кадъра за секунда.
- Локалните компютърни мрежи на три нива имат оптимална производителност при обслужване от 2 до 5 комуникиращи двойки.
- Препоръчва се изграждане на локални компютърни мрежи до три нива на управление.

4.5. Стандарт IEEE 802.4. (Token Bus)

Стандартът IEEE 802.4. (Token Bus) използва за изграждане на комуникационни линии коаксиални кабели. Сложен е за изпълнение и поддръжка и рядко се е прилагал в миналото.

Стандартът описва локална компютърна мрежа с физическа топология тип "шина". Линиите за предаване на данните са изградени от широколентов коаксиален кабел с вълново съпротивление R = 75 Ω. Използват се два режима на предаване на данни:

- немодулирано аналогово предаване (carrier band);
- модулирано аналогово предаване (broad band).

При немодулираното аналогово предаване по кабел се осигурява само един канал със скорост 5 Mb/s. Дължината на сегмента достига до 700 м при максимален брой на възлите 32.

При модулираното аналогово предаване се осигуряват няколко канала за предаване на данни, работещи със скорост до 10 Mb/s за всеки.

MAC-подслой на стандарта IEEE 802.4**.** използва протокола Token Bus. Достъпът на компютрите до комуникационния канал се реализира чрез управляващ маркер. Използва се специален кадър – щафета, който се предава от възел на възел.

Само възелът, който притежава маркера, има право да предава данни към останалите, като всеки възел знае адресите на съседите си. При инициализация на мрежата пръв има право да притежава маркера и да предава възелът с най-голям адрес.

Встъпи-телна част	Начален раздели-тел	Управ-ление	MAC – подател	MAC – получа-тел	Данни	Контрол -но поле FCS	Краен раздели-тел
1	1	1	2 или 6	2 или 6	0 ÷8182	4	1 байт

Фиг. 9.5. Формат на кадъра на протокола Token Bus

Всеки възел владее маркера за определено време, след което го предава на съседа с по-малък адрес. За това време се предават кадрите (фиг. 9.5) с данните към възела, за който са предназначени. Когато даден възел няма съобщение за останалите, маркерът се предава на

следващия възел. След като маркерът се изпрати към следващия възел, се получава потвърждение за получаването му. Ако след второто изпращане на маркера не се получи потвърждение, се изпраща специален кадър "кой е следващият". Ако и тогава не се получи потвърждение, в шината се изпраща запитване "търся заместник". Очаква се произволен възел да се обади и да приеме маркера.

По протокола Token Bus може да се използва и схема за приоритетно предаване на съобщения. Някои възли могат да се изключат и да не получават право на служебен маркер за предаване, а само да работят в режим приемане.

Недостатък на този протокол е, че локалната компютърна мрежа трудно се реконфигурира, защото трябва да се пренастройват и описват съседните възли.

4.6. Стандарт IEEE 802.5. (Token Ring)

Стандарт IEEE 802.5. (Token Ring) възниква през 1985 г. на базата на стандарта Token Ring на фирмата IBM. Стандартът описва локална компютърна мрежа с логическа топология тип "кръг". При нея сигналът обхожда в кръг последователно всички възли. Физическата топология може да е от друг тип, най-често "звезда".

Разстоянията, които се покриват от мрежата, са по-големи от тези при стандарти 802.3. и 802.4., тъй като сигналът, преминавайки през възлите, се формира и усилва по форма и амплитуда.

Използва се само режим "директно предаване". За комуникационните линии се използват следните кабели:

- неекранирани усукани двойки (UTP) със съединители RJ – 45;
- екранирана усукана двойка (STP) със съединители RJ – 45 или с MIC на IBM;
- коаксиален кабел;
- влакнесто-оптичен кабел.

Скоростта на предаване на данни за стандарта е 16 Mb/s или 4 Mb/s. По кабел UTP се постига скорост до 4 Mb/s.

Крайните възли се свързват към кръга чрез специални съединителни устройства MAU (Multistation Access Unit). Чрез съединителите MAU може да се изключва повреден или невключен към захранването краен възел, с което се запазва целостта на кръга на компютърната мрежа.

В една LAN по този стандарт може да има до 33 броя съединители тип MAU. Разстоянието между възела на мрежата и MAU съединителя трябва да е не по-малко от 2,5 m и максимално – до 100 m за кабел STP и 45 m за кабел UTP. Допуска се дължина на кабела между два съседни MAU съединителя до 150 m и до 750 m с използване на междинен усилвател (повторител).

В MAC подслоя на стандарта се използва протоколът Token Ring. Управлението на достъпа става с маркер. Маркерът се генерира при инициализиране на мрежата, след което той циркулира по кръга само в една посока. Право на излъчване на информационни кадри в комуникационната среда има само възелът, който владее маркера. Когато един възел иска да владее маркера с цел предаване в полето AC (фиг. 9.6), в маркера се променя един бит, с което маркерът се превръща в начало на кадър на този възел. В този момент във възела се пуска таймер, с който се определя времето, за което възелът може да задържи маркера.

Излъчените кадри преминават последователно през всички възли, но само възелът, който разпознае своя адрес, ги копира в паметта си. Когато последният информационен кадър достигне до възела подател, служебният маркер се освобождава и преминава към следващия възел. За правилното изпълнение на процедурите се грижи специална мониторна

станция. За тази цел един от крайните възли на мрежата премахва „забравени кадри” и възстановява изгубен служебен маркер.

Начален ограничител (SD)	Управление на достъпа (AC)	Управление на кадъра (FC)	MAC – адрес на получателя (DA)	MAC-адрес на подателя (SA)	Данни	Контролно поле (FCS)	Краен ограничител (ED)	Състояние на кадъра (FS)
1 B	1	1	2 v 6	2 v 6	пром. дължина	4	1	1 байт

Фиг. 9.6. Формат на кадъра на MAC подслоя за протокол Token Ring

Протоколът Token Ring има предварително зададено максимално време за закъснение на кадъра, поради което е удобен за работа в реално време.

В LAN с по-висока скорост (16 Mb/s) се използва методът на “предварително освобождаване на кадъра”. Възелът подател не чака последният кадър да “направи кръг”, а щом го предаде в мрежата, веднага предава служебния маркер към следващия възел.

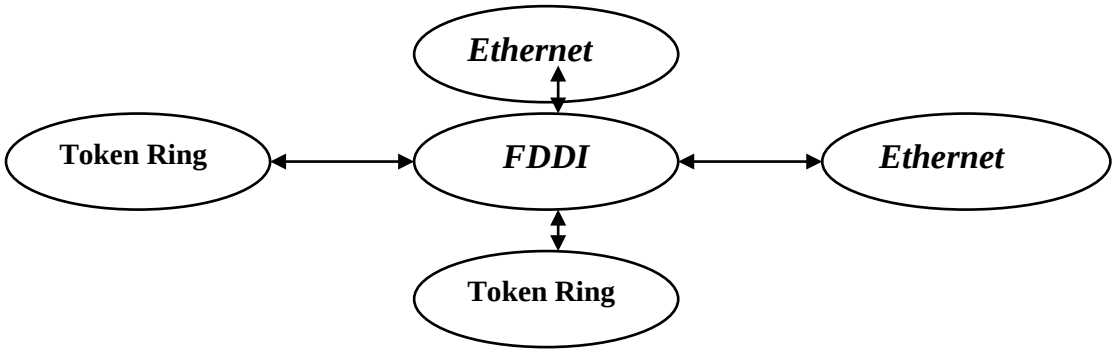
4.7. Стандарт IEEE 802.8. FDDI (Fibre Distributed Data Interface)

Този стандарт е създаден за скорост на предаване на данни 100 Mb/s и се прилага за локални мрежи, разположени на големи територии (Extended LAN). MAC-протоколът е базиран на протокола Token Ring. Стандартът FDDI се използва като високоскоростна опорна мрежа (гръбнак) за свързване на няколко LAN помежду им – фиг. 9.7.

Топологията на мрежата е “двоен кръг”, като единият кръг е основен (първичен), а другият – резервен (вторичен). Посоката на предаване на служебните маркери и данните на съобщенията в двата кръга е различна.

Мрежовите възли на компютърната мрежа са два типа:

- мрежови възли, свързани към двата кръга (DAS);
- мрежови възли, свързани към единия кръг (SAS).



Фиг. 9.7. Приложение на стандарта FDDI

При този стандарт SAS възлите се свързват към кръга чрез DAS концентратори. При нормален режим на работа данните преминават през всички мрежови възли и всички участъци на кабела на първия кръг, затова той се нарича транзитен. Вторичният кръг в този режим не се ползва.

Стандартът FDDI поддържа 1000 порта за достъп, или 500 DAS възела. Максималната обиколка на кръга е до 100 km. Могат да се използват освен влакнесто-оптични кабели, и медни усукани двойки проводници. При оптични комуникации разстоянието между два съседни междинни възела е до 2 km. Ако се използва едномодов кабел, съчетан с лазер, това разстояние достига до 60 km.

Ако се използва кабел UTP, разстоянието между междинните възли е до 100 m (този вариант на мрежата FDDI е с абревиатура TPDDI).

Двойният кръг на FDDI осигурява висока живучест на мрежата при прекъсване на едната линия, повреда на възел или концентратор, или възникване на грешки при предаване по линията. В тези случаи мрежата се реконфигурира чрез концентраторите и/или мрежовите адаптери на междинните възли. При множество откази мрежата може да се разпадне на няколко несвързани мрежи.

Физическият слой на FDDI се състои от два подслоя:

- Горен подслой, независим от комуникационната среда – подслой PHY(Physical).
- Долен подслой, зависим от средата – подслой PMD (Physical Media Dependent).

Подслой PMD изпълнява следните функции:

- Определя изискванията към мощността на сигналите.
- Определя параметрите на съединителите и маркировката им.
- Извършва NRZ-I линейно кодиране на сигналите в кабелите.

Подслоят PHY извършва кодиране и декодиране на данните, циркулиращи между MAC-слоя и подслоя PMD. В неговите спецификации се определят:

- Кодиране на информацията в съответствие със схемата 4B/5B.
- Правилата за тълкуване на сигналите.
- Поддържане стабилност на тактовата честота от 125 MHz .
- Правилата за преобразуване на данните от паралелен код в последователен.

4.8. Стандарт IEEE 802.10. – LAN Sequrity – виртуални частни мрежи (VPN)

4.8.1. Обосновка на виртуалната частна мрежа

Общото между локалните и глобалните компютърни мрежи е преносната среда за данните – кабелна или безжична връзка, чрез която директно се свързват комуникиращите компютри. При виртуалните частни мрежи – VPN (Virtual Private Networks), се изгражда тунел за предаване на съобщенията през комуникационната среда на глобалната компютърна мрежа Интернет. Комуникиращите компютри във VPN мрежата се свързват, както е показано на фиг. 9.8 [34].

Съобщенията между абонатите на мрежата се изпращат чрез глобалната мрежа по модела от тип „от точка до точка" чрез протокола Point-to-Point (PPP). Данните се капсулират и по този начин се създава логическа независима мрежа от местоположението на крайните точки, в които се поддържа автентификация. Предаваните съобщения по тунелите се

защитават с метода на криптиране. Криптирането на съобщенията е от голямо значение, в противен случай всеки може да ги прехване по време на пътуването през обществената интернет мрежа между предаващата и приемащата крайна точка на тунела.

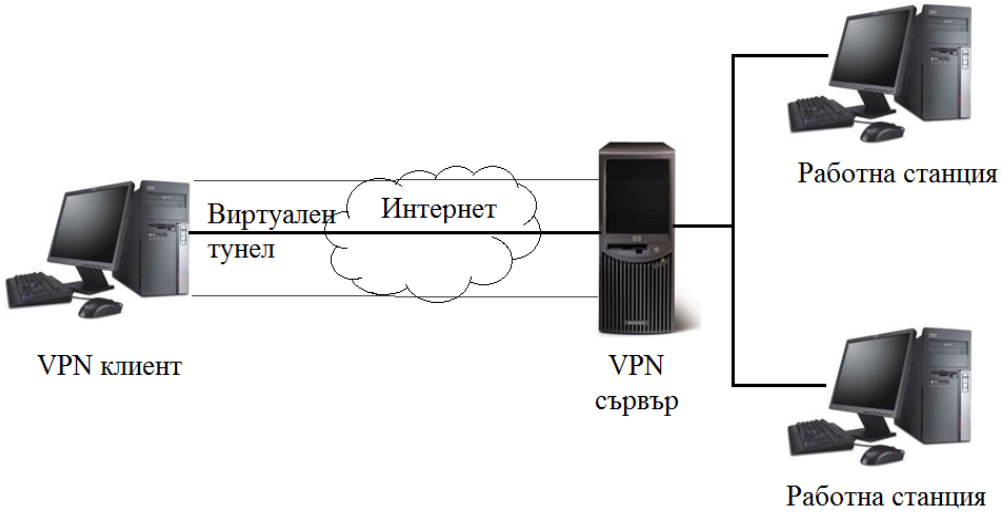
VPN технологията позволява да се създаде логическа мрежа, която е независима от местоположението на служителите или клиентите и създава условия за установяване на директна информационна връзка между тях. За разлика от използването на скъпи системи от наети линии, които могат да бъдат използвани само от една организация, VPN мрежата предоставя на организациите еднакви възможности на много по-ниска цена, което е голямо предимство.

Фиг. 9.8. Схема на VPN комуникация

VPN мрежата работи с криптиран трафик, преминаващ през несигурната интернет среда, и е значително евтина алтернатива спрямо използването на наети линии за изграждане на частна мрежа за дадена организация. VPN мрежите се използват за осигуряване на отдалечен достъп до мобилни служители, осигуряване на екстранет мрежа с достъп до нейни клиенти или за осигуряване на връзка между два офиса с различни местоположения. VPN мрежите използват надеждно защитени тунели в средата на Internet за връзка между две мрежи и обмен на данни между тях.

Виртуалните компютърни мрежи използват два вида канали за предаване на данните: комутируеми канали (dial-up) и наети канали от типа „маршрутизатор до маршрутизатор”. И за двата типа мрежи се изисква конфигуриране и настройка на мрежите от администратор.

Изграждането на тунел през глобална компютърна мрежа е свързано със създаване на логическа връзка между две крайни точки, в които се поддържа автентификация и криптиране на данните от едната до другата страна. Тунелирането е термин, използван за описание на капсулацията, маршрутизацията и декапсулацията на пакетите. Капсулирането представлява скриване на оригиналния пакет в нов пакет, който се използва за маршрутизирането през тунела, т.е. в хедъра на новия пакет се задава адресът на крайната точка от тунела, в хедъра на оригиналния пакет се намира адресът на възела получател, който остава криптиран до пристигането му в крайната точка на мрежата.



Фиг. 9.9. Връзка между отдалечен VPN клиент и VPN сървър

VPN мрежата позволява на локалните частни мрежи, намиращи се в различни географски региони, физическо свързване към мрежата на дадена организация посредством VPN сървър. Връзката между отдалечен VPN клиент и VPN сървър е показана на фиг. 9.9. Администраторът на VPN мрежата разрешава на някои от работните станции на локалните мрежи връзка с VPN сървъра. Само потребители, които имат достъп до виртуалната мрежа на организацията, могат да ползват защитените ресурси на конфигурираната частна виртуална мрежа. Тези потребители получават акредитивни писма за достъп, а останалите не виждат локалната мрежа и нямат достъп до общите ресурси.

4.8.2. Тунелиране на каналния и мрежовия слой на OSI модела

VPN мрежите използват тунелни протоколи, работещи в каналния слой. Тези протоколи осигуряват виртуална връзка от сървъра до клиента. Могат да се използват различни протоколи за изграждане на тунела на каналния слой на възлите от мрежата.

Протоколът Point-to-Point Tunneling Protocol (PPTP) работи на каналния слой на OSI модела. Освен него може да се използват и други тунелни протоколи на този слой като Layer 2 Forwarding (L2F), който осигурява тунелиране по глобалните компютърни мрежи за стандартите ATM и Frame Relay. За разлика от тунела, изграден от протокола PPTP, протоколът L2F поддържа повече от една връзка между крайните абонати. VPN мрежите, функциониращи в каналния слой на OSI модела, използват и двата протокола (PPTP и L2TP).

Протоколът PPTP е по-стар, използва се главно за отдалечен достъп, функционира в режим клиент/сървър. Клиентската част може да бъде отдалечен хост с инсталиран PPTP протокол или сървър за мрежов достъп с разрешение за функциониране на протокола PPTP от страна на доставчика на Интернет. Реализацията на сървърната част може да е рутер, специализиран VPN концентратор или приложен сървър. Протоколът PPTP капсулира PPP пакети в модифицирана версия на протокола GRE (Generic Routing Encapsulation), който ги транспортира през мрежата. Той представлява механизъм за капсулиране на произволен протокол от мрежовия слой към друг такъв протокол. Протоколът PPTP може да се използва за транспортиране на протоколни единици на протоколи като IP, IPX и NetBEUI. Той разчита на автентифициращите механизми на протоколите PPP – PAP (Password Authentication Protocol) и CHAP (Challenge Handshake Authentication Protocol), които не се считат за особено сигурни. Протоколът PAP изпраща паролите като чист текст – т.е. паролите остават незащитени по време на предаване на пакетите по обществената мрежа. Протоколът CHAP е по-сигурен от PAP, той изпраща един вид „покана" (challenge), на която другата страна трябва да отговори, за да се автентифицира. Microsoft създава разширена версия на протокола CHAP, наречена MS-CHAP. Протоколът L2TP се разглежда като заместник на PPTP и се счита за по-надежден. Протоколът L2TP също функционира в режим клиент/сървър и подобно на PPTP, L2TP тунелът може да бъде инициран от отдалечен компютър към LNS (L2TP network server) или от LAS (L2TP-enabled access концентратор) към LNS. L2TP дефинира свой собствен тунелиращ протокол в зависимост от транспортната среда, като не използва протокола GRE. L2TP може да се използва за функционирането на протоколи от мрежовия слой, различни от IP, но не всички версии го поддържат. L2TP може да използва протоколите PAP, CHAP и EAP за автентификация. Протоколът L2TP поддържа използването на IPSec, което може да се използва за сигурност на трафика по целия му маршрут от крайния потребител до корпоративната мрежа.

Тунели могат да се създават и в мрежовия слой на OSI модела, като по този начин се осигуряват IP базирани виртуални връзки. Те работят чрез изпращане на IP пакети, капсулирани във вътрешността на специфицирани от IETF (Internet Engineering Task Force) протоколни обвивки. Използват се IPSec (IPSecurity), IKE (Internet Key Exchange) методи за автентикация и криптиране, като DES (Data Encryption Standard) и Secure SHA (Hash Algorithm). IPSec може да бъде използван заедно с протокола L2TP, който изгражда тунела, а IPSec криптира данните. По този начин IPSec работи в транспортен режим. Той може също да бъде използван и в тунелен режим, при който осигурява тунела. Една важна особеност е тази, че IPSec може да капсулира само IP пакети. L2TP може да осигурява капсулиране на IPX (Internetwork Packet Exchange) пакети и на пакети на други протоколи по IP мрежа. Някои от шлюзовете не поддържат VPN мрежи, базирани на L2TP или PPTP, като в този случай за осигуряване на тунела се използва IPSec. Тези тунели обикновено работят от шлюз до шлюз.

VPN, изградени на мрежовия слой на OSI модела, обикновено са такива мрежи, използващи IP протокола като протокол от мрежовия слой. VPN от мрежовия слой използват комуникациите MPLS (Multiprotocol Label Switching) и IPSec.

MPLS обикновено се предлага като тип връзка site-to-site VPN услуга от ISPec. Доставчикът построява частна IP базирана мрежа и предлага връзка на множество клиенти между техните местоположения в мрежата. Технологията позволява на отделни клиенти да гледат на MPLS услугата като на частна IP мрежа, свързваща различните им местоположения. По този начин се предлагат на клиентите предимства като на частните мрежи от каналния слой, като при стандартите Frame Relay и ATM, но с възможност за лесно управление на мрежите от мрежовия слой. Тъй като MPLS функционира чрез частна IP базирана мрежа вместо Internet, доставчикът може да предостави обособени нива на услугите на своите клиенти: QoS (Quality of Service – качество на услугите) и SLA (Service-level Agreements – споразумения за нивата на услугите). MPLS е базирана на частна мрежа на определен

доставчик, достъпността на услугата е ограничена до обхвата, в който функционира доставчикът.

4.8.3. VPN мрежи за отдалечен достъп

Използването на VPN за осигуряване на отдалечен достъп до потребители е най-често използваният метод за изграждане. Реализацията може да бъде усложнена от фактори като: използване на различни операционни системи и протоколите, които са инсталирани от страната на клиентите.

VPN клиентът трябва да може да използва протоколи, поддържани от VPN сървъра – тунелни, мрежови и транспортни протоколи, както и протоколи за криптиране. След инсталиране и конфигуриране на компонентите на VPN мрежата се установява връзката между абонатите, както е показано на фиг. 9.10. Редът за изграждане и пускане в експлоатация на такава мрежа е както следва:

- Мобилният потребител набира локален ISP (Internet Server Provider) доставчик и влиза с потребителски акаунт и парола, за да изгради интернет връзка, ако клиентът използва наета или постоянна връзка.
- След установяване на интернет връзката клиентът извиква сървъра за отдалечен достъп, конфигуриран да приема VPN връзки, като използва IP адреса на отдалечения сървър и по този начин се изгражда тунелът.
- Потребителят трябва да се автентифицира в частната мрежа, за да му се разрешат определен достъп и права.

Фиг. 9.10. Схема на връзките във VPN

Виртуален частен екстранет се създава, като на част от LAN мрежата на организацията или на определено нейно звено се разрешава санкциониран достъп от отдалечени потребители по VPN връзка.

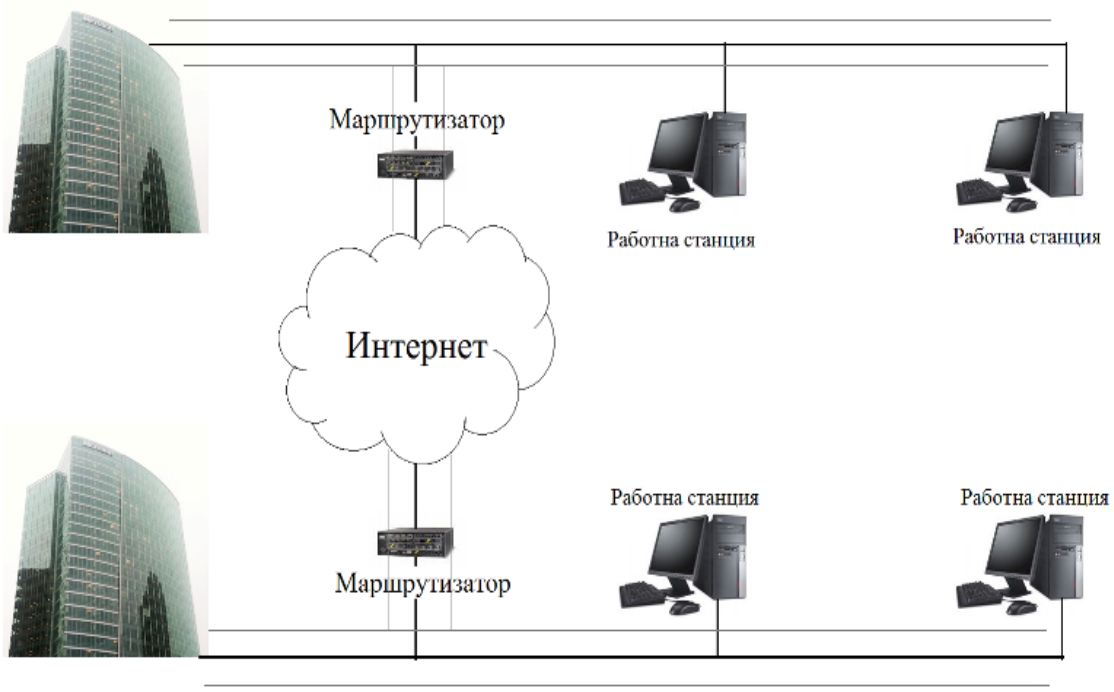
Един от основните проблеми е защитата на останалата част от вътрешната мрежа от външен достъп. Създава се отделна подмрежа за екстранет мрежата, а останалата част от LAN мрежата се скрива зад защитна стена, за да може да й се осигури необходимата защита. Потребителите на екстранет осъществяват достъп до данни през Web браузър, затова в подмрежата с връзка към VPN трябва да се инсталира Web сървър, също така там могат да бъдат разположени и файлови сървъри.

Съществуващите перспективни стандарти улесняват организациите в използването по екстранет на общи данни и приложения. Някои от тези стандарти са следните:

- Hypertext Markup Language (HTML) – позволява споделянето на документи през всеки Web браузър. На потребителите не е нужно да се инсталира конкретна програма за текстообработка или друга програма, за да отварят файловете.
- Extensible Markup Language (XML) и Commerce XML (CXML) – предлага между-платформена съвместимост.
- Open Buying on the Internet (OBI) – създава стандарти за транзакции на електронната търговия.

При създаването на връзки между различни офиси се използва виртуална частна мрежа за свързване на двата офиса във VPN конфигурация от тип маршрутизатор – маршрутизатор. VPN сървърът може да функционира като маршрутизатор с разрешено IP препращане, както е показано на фиг. 9.11.

LAN във всеки филиален офис има маршрутизирана връзка към Интернет. Тази връзка може да бъде реализирана по комутируема или постоянно изградена (арендована) линия.



Фиг. 9.11. VPN връзка между офиси на фирма

При използване на комутируема връзка маршрутизаторът, иницииращ връзката, използва dialup интернет комуникация. Маршрутизаторът, който се извиква, трябва да има постоянна интернет връзка и трябва да бъде конфигуриран за приемане на връзки от този вид (набиране при необходимост). На извикващия маршрутизатор се конфигурират две връзки с набиране при необходимост – едната за набиране на ISP и другата за свързване към VPN. Ако и двата маршрутизатора имат постоянни връзки към Интернет, VPN връзката може да бъде установена и оставена непрекъснато открита.

VPN връзки от типа маршрутизатор – маршрутизатор може да бъдат конфигурирани така, че единият маршрутизатор да действа като клиент и да инициира връзката, а другият да функционира като VPN сървър. По този начин се реализира еднопосочна връзка и представлява добър избор за постоянни връзки. При двупосочната връзка всеки от маршрутизаторите може да инициира връзката. В този случай и двата маршрутизатора трябва да имат постоянна връзка към Интернет и трябва да бъдат настроени като LAN и WAN маршрутизатори.

При връзката маршрутизатор – маршрутизатор маршрутните таблици и на двата маршрутизатора трябва да бъдат конфигурирани с необходимите маршрути, за да препращат пакети през връзката. Маршрутите могат да бъдат добавени ръчно или може да бъде използван протокол за динамична маршрутизация, ако интерфейсът за набиране има постоянна връзка. Може да бъде използван софтуер като vpnd (VPNdaemon) за свързване на две локални мрежи, използващи Linux или FreeBSD за защита на данните, преминаващи през съответната връзка и да се използва алгоритъмът за криптиране Blowfish.

4.8.4. Обосновка на VPN протоколите

Протоколите, осигуряващи функционирането на VPN мрежите, работят на различни нива от избрания комуникационен модел. Във VPN мрежите се използват три типа протоколи:

- Тунелни протоколи – понякога означавани като VPN протоколи, и се използват за изграждане на тунели в комуникационните мрежи.
- Протоколи за криптиране – означавани като протоколи за сигурност, използват се за криптиране на данните.
- Мрежови/транспортни протоколи – означавани още като LAN протоколи, използват се за комуникация на съобщенията във виртуалната частна мрежа.

Тунелните протоколи капсулират данните така, че хедърите на протоколните единици от оригиналния протокол се обвиват в тунелни капсулиращи хедъри. За да могат VPN клиентът и сървърът да комуникират, на техните компютри е необходимо да се инсталира еднакъв стек от мрежови транспортни протоколи. Тунелните протоколи се класифицират като стандартни и нестандартни.

Стандартните тунелни VPN протоколи са следните:

- Point-to-Point Protocol (PPP)
- Secure Shell (SSH) и Secure Shell 2 (SSH2)
- Протокол IP Sec
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Forwarding (L2F)
- Layer 2 Tunneling Protocol (L2TP).

Протоколът PPP е протокол за комуникация между два компютъра, използващи сериен интерфейс. Типичен е за персоналните компютърни връзки по телефонна линия към сървър. PPP връзката се осигурява на каналния слой на OSI модела. Протоколът PPP включва в себе

си автентификации с помощта на PAP (Password Authentication Protocol), автентификация на парола и CHAP (Challenge Handshake Authentication Protocol) – протокол за автентификация чрез използване на съгласуване от двете крайни точки.

Протоколът SSH представлява Unix базиран команден интерфейс и протокол за получаване на сигурен достъп на отдалечен компютър. Тази технология се използва широко от мрежовите администратори за WEB отдалечен контрол. SSH всъщност служи за няколко цели: slogin, ssh, и scp. SSH командите са криптирани и са подсигурени няколко пъти. Двете крайни точки на клиент – сървър връзката са автентични. Те използват цифров сертификат и паролите са защитени. SSH използва RSA криптиращ алгоритъм за двете връзки и автентификации. Другите криптиращи алгоритми, които могат да се използват, са DES, Blowfish и IDEA.

Първоначално SSH е предназначен за осигуряване на сигурна алтернатива на UNIX команди за отдалечен достъп като rsh, rlogin и rep. SSH използва надеждно криптиране и автентификация. SSH2 е развит в сигурен тунелен протокол, който може да се използва за създаване на VPN мрежа, работеща под операционни системи Linux или UNIX. Типът на VPN мрежата, изградена с помощта на SSH2, се нарича VPN на ниво верига. Клиентски софтуер на SSH е достъпен и за операционна система Windows.

Шлюзовете на ниво верига работят в сесийния слой на референтния OSI модел. Когато данните се предават до отдалечен компютър по шлюз на ниво верига, изглежда, че се предават от самия шлюз. Това позволява да се замаскира информация за защитени мрежи.

SSH може да бъде инсталиран на защитната стена, а тунелът да бъде изграден от SSH клиент с dail-up Интернет достъп до защитната стена. Тя може да бъде конфигурирана да препраща трафика до сървър по вътрешната мрежа. Това е лесно решение за VPN връзки, когато не се цели постигане на висока производителност. SSH изисква акаунт за логване, затова е най-подходящ в ситуации, когато се разрешава на доверени служители да се свържат към малка офис мрежа от домовете им.

Протокол IPSec може да бъде използван за криптиране на данни, които се предават през тунела, изграден от друг VPN протокол. Той може да бъде използван също за изграждане на тунел, когато действа в режим на тунелиране. Тогава IPSec може да бъде конфигуриран за защита на данните или между два IP адреса, или между две IP подмрежи. IPSec е разширение на IP протокола, което гарантира сигурност на IP и протоколите от по-висок ред.

IPSec може да използва един или и двата протокола: Authentication Header (AH) и Encapsulating Security Payload (ESP), за да осигури автентификация, цялостност и поверителност на комуникацията. Той може да защитава или целия IP дейтаграм – тунелна форма, или само протоколите от по-висок ред – транспортна форма. Използването на комбинация от криптографско базирани алгоритми и ключове прави информацията много сигурна. Алгоритъмът на Дафи – Хелман позволява сигурен обмен на споделен ключ без изпращане на самия ключ по мрежовата връзка.

Протоколът PPTP е на Microsoft с установен стандарт Той представлява разширение на протокола PPP, който се използва за изграждане на WAN връзка с отдалечен достъп. Принципът на работа на PPTP протокола е следният: PPTP капсулира PPP клетка, която може да бъде IP, IPX или NetBEUI пакет, във вътрешността на Generic Routing Encapsulation (GRE) хедър. Добавя IP хедър за осигуряване на IP адресите на източника и местоназначението. Адресът на източника е този на VPN клиента, а адресът на местоназначението е на VPN сървъра. Данните в оригиналната дейтаграма обикновено са криптирани, за да не могат да бъдат прочетени от неоторизирани лица. VPN мрежите на Microsoft използват протокола MPPE заедно с PPTP за осигуряване на сигурни комуникации.

PPTP-Linux е клиентски софтуер, който се изпълнява на компютри под управление на MOC Linux и UNIX и позволява да се установява връзка с PPTP сървъри. Софтуерът на PPTP сървъра (PoPToP) е достъпен за Linux, Sun Solaris, FreeBSD и други реализации на UNIX,

също така той поддържа и Windows клиенти, както и PPTP-Linux клиенти и се разпространява безплатно.

PPTP се състои от два компонента: контролна връзка между всяка двойка PPTP Access концентратори (PAC) и PPTP Network Server (PNS), и IP тунел, действащ между тази PAC – PNS двойка. Тунелът служи да транспортира капсулирани PPP пакети за потребителски сесии между PPTP двойката. Контролната връзка е стандартна TCP сесия, отговаряща за установяването, управлението и освобождаването на тунела. Това става с помощта на контролни съобщения, изпращани между PAC и PNS като контролни пакети в TCP дейтаграми. След като се създаде PPTP тунелът, данните на потребителя се изпращат от PAC и PNS във вид на IP дейтаграми, съдържащи PPP пакети.

MPPE се използва с PPTP базирани VPN връзки (или PPP dial-up връзки) и може да използва криптиращ алгоритъм с 40-, 56- или 128-битов ключ. 128-битовият ключ се използва за надеждно криптиране и може да бъде използван само в САЩ и Канада.

Протоколът L2F е разработен по технологията от Cisco през 1996 г. и включва в нея софтуер IOS – също разработен от Cisco. Като алтернатива на PPTP, L2F има възможност да използва протоколите на стандартите ATM и Frame Relay за тунелиране в глобални комуникационни мрежи. За да работи PPTP, е необходимо да е инсталиран и IP стекът. При L2F това изискване не е задължително. L2F технологията осигурява автентификация на крайните точки на тунела във VPN.

Протоколът L2TP е разработен от Microsoft и Cisco. Комбинират се възможностите на PPTP и L2F и се създадава L2TP, който капсулира данните за изпращане по IP както PPTP, като L2TP може да капсулира данни за изпращане по стандарти ATM, Frame Relay и X.25. По този начин той може да бъде използван за изграждане на тунел през Интернет или може да бъде използван по конкретна WAN среда без необходимост от протокола IP. Някои от предимствата на L2TP пред PPTP са следните:

- L2TP поддържа множество тунели между крайните точки. Това позволява създаването на отделни тунели, осигуряващи различни качества на услугите.
- L2TP поддържа компресиране на хедъри, с което се намалява обемът на допълнителната информация в протоколните единици.
- L2TP за разлика от PPTP има възможност за тунелна автентификация.
- L2TP работи на мрежи неизискващи протокола IP, изградени по ATM или Frame Relay стандарти.

L2TP комбинира най-доброто от решението на Microsoft Point-to-Point Tunneling Protocol (PPTP) и Layer 2 Forwarding (L2F) на Cisco Systems. Отдаленият потребител установява PPP връзка към мрежата на ISP. L2TP ползва два типа съобщения: контролни съобщения и съобщения за данни. Контролните съобщения се използват при установяването, поддържането и премахването на тунела, а съобщенията за данни капсулират PPP клетките, пренасяни по тунела. Контролните съобщения се изпращат по надежден контролен L2TP канал, за да се гарантира тяхното получаване. Контролните съобщения имат пореден номер, осигуряващ сигурното им транспортиране по контролния канал. Пореден номер се използва и при предаване на клетките от съобщенията, за да се подреждат в приемния пункт и да се установява евентулната загуба на пакети.

Нестандартни протоколи за изграждане на VPN мрежи са следните:

- протокол VTUN
- crypto IP Encapsulation протокол (CIPE).

Протоколът VTun позволява да се ограничат входната и изходната скорост на тунелите за избягване на претоварвания на сървъра при наличие на голям брой клиенти. Системата работи чрез уникалните драйвери tun и tap. Tun се използва за тунелиране на IP пакети, а tap при тунелиране на Ethernet мрежи.

Протоколът CIPE представлява драйвер за ядрото на Linux, който може да бъде използван за осигуряване на сигурен тунел между две IP подмрежи. Данните се криптират в мрежовия слой на референтния OSI модел. Това се нарича криптиране на ниско ниво. То има предимство пред криптирането на високо ниво, защото не трябва да бъдат правени никакви промени на приложния софтуер, когато две мрежи се свързват с помощта на VPN технология. Освен това CIPE е по-прост и по-ефикасен от IPSec .

4.8.5. Надеждност и сигурност на VPN мрежите

Надеждността на една система се определя от надеждността на най-слабия й елемент. Ето защо не е необходимо да се атакуват използваните криптографски алгоритми. Достатъчно е да се атакува един от компонентите на системата. Надеждността на VPN мрежата зависи от следните фактори:

- Условията и външната среда, в която работи компютърната мрежа.
- Режимът на работа на мрежата.
- Надеждност на елементите, от които тя е изградена.
- Вътрешната й надеждностна структура.
- Възстановимостта на съставните й части след отказ.

Сигурността на VPN се гарантира от три компонента:

- автентификация на клиентите
- оторизация на клиентите
- криптиране на данните.

Автентификацията на VPN клиента включва проверката за истинност на самоличността на компютъра и на потребителя, който инициира VPN връзката. Автентификацията може да бъде осъществена на нивото на потребителския компютър. Например когато една VPN връзка, базирана на Windows 2000, използва IPSec за L2TP VPN мрежа, сертификатите на компютрите се обменят като част от изграждането на IPSec асоциация за сигурност. Потребителят може да бъде автентифициран с помощта на един от няколкото метода за автентификация, като Extensible Authentication Protocol (EAP), Challenge Handshake Authentication Protocol (PAP) или Shiva PAP (SPAP).

Оторизация означава зададените ограничения, на базата на които на едни потребители се предоставя достъп до VPN мрежата, а на други се отказва.

Криптирането служи за защита на данните във VPN мрежи. Могат да бъдат използвани най-различни технологии за криптиране. Много VPN реализации позволяват да се избере методът на криптиране, който трябва да бъде приложен. Криптирането осигурява сигурност на данни, които пътуват по VPN мрежата. Без тази сигурност данните биха могли лесно да бъдат прехванати и анализирани, докато се предават по обществената комуникационна мрежа.

VPN мрежата може да бъде реализирана софтуерно или хардуерно. Всяка от тези реализации има свои предимства и недостатъци. Разликите между тях и възможността за изграждане на хибриди води до повишаване нивото на сигурност на мрежата.

Софтуерно базираните VPN мрежи включват използването на разгледаните по-горе тунелни протоколи. Тази категория може да бъде разделена допълнително на продукти на независими производители и VPN софтуер, поддържан от операционната система. Очевидното предимство на последните е тяхната ниска цена. Няма допълнително заплащане,

а VPN решенията, включени в модерните операционни системи като Windows 2000, са достатъчни за нуждите на много организации. VPN софтуерните продукти на независимите производители обикновено предлагат допълнителни възможности и разширяват използваемостта на VPN, като често осигуряват повече опции за сигурност и в някои случаи по-лесно реализиране. Някои софтуерно базирани VPN мрежи позволяват да се предават данни в тунела на базата на протокола или IP адреса. Този тип филтриране обикновено не е достъпен при хардуерно базираните продукти. Продуктите на независимите производители включват Safeguard VPN, Checkpoint SVN (Secure Virtual Networking) и NetMAX VPN Suite за операционна система Linux.

Хардуерно базираните VPN мрежи се произвеждат от компании като Shiva, 3Com и VPNet Technologies. Поддръжката на VPN е вградена в маршрутизаторите на Cisco, както и в маршрутизаторите на други компании. NTS Tunnel-Builder осигурява сигурни VPN комуникации за Windows, NetWare и Macintosh. Такива производители като Raptor Systems предлагат VPN мрежи, базирани на защитни стени, които са комбинирани със средства за сигурност. Хардуерните VPN мрежи могат най-общо да бъдат категоризирани в следните две групи:

- Базирани на маршрутизатори – VPN решения, представляващи маршрутизатори с възможности за криптиране. Те предлагат по-добра производителност на мрежата и като цяло са по-лесни за инсталиране и използване.
- Базирани на защитна стена. Решенията, базирани на защитна стена, осигуряват допълнителни мерки за сигурност като сигурна автентификация и детайлно логване. Базираната на VPN защитна стена има възможност да преобразува адреси. Производителността й може да бъде проблем, макар че в някои реализации хардуерните криптиращи процесори решават тази задача.

Необходимо е да се осигури контролиран достъп на отдалеченото мрежово решение до ресурсите и информацията на организацията, тъй като се разрешава на отдалечения клиент да се свързва към ресурсите на локалната мрежа. Решението трябва да позволява на отдалечените офиси да се свързват един с друг, да споделят ресурси и съобщения, да се осигурява цялостност и неделимост на данните при преминаването им през Интернет. VPN решението трябва да отговаря на следните изисквания:

- Автентификация на потребителя – проверка на идентичността на VPN клиента, ограничаване на VPN достъпа само на упълномощени потребители.
- Управление на адресите – назначаване на VPN клиенти на адрес в Интранет и осигуряване използваните в Интранет адреси, съхранени като частни.
- Криптиране на данните – данни трябва да се пренасят като криптирани през Интернет.
- Управление на ключовете – генериране и обновяване на декриптиращи ключове за криптираните данни.

Виртуалните частни мрежи могат да бъдат реализирани по няколко начина, най-използваните от които са:

- За осигуряване на отдалечен достъп до мобилни служители или служители, работещи от дома си.
- За осигуряване на екстранет мрежа, до която да имат достъп служители, клиенти или партньори.
- За осъществяване на контакт между два офиса с различни местоположения, без за целта да е необходима специална директна връзка.

Предимствата на VPN мрежите са свързани с намаляване на разходите за междуградски разговори, когато отдалечените потребители се намират извън областта за набиране на

локални номера. Тези мрежи изискват по-малко телефонни линии за осигуряване на отдалечен достъп до множество потребители едновременно. Също така изискват по-малко хардуерно оборудване, например банки от модеми. VPN мрежите, базирани на ISP, редуцират цените за администриране и обучение.

Като недостатък може да се приеме изискването за връзка към Internet в двата края на VPN мрежата. Това може да бъде проблем, ако единият или двата края имат ненадеждна връзка към Интернет. Друг недостатък на VPN мрежите се състои в проблемите, свързани с производителността. Те могат да бъдат от незначителни до съществени, в зависимост от типа на реализацията на VPN и от типа на използваните Internet връзки. Проблемите на производителността, свързани с VPN мрежите, могат да бъдат категоризирани по два начина: общи проблеми на производителността и проблеми, които са специфични за конкретни VPN реализации.

Една от алтернативите на VPN мрежата е dial-up комуникацията. В някои случаи dial-up сървърът може да постигне същата цел, както VPN мрежата, но при много други обстоятелства виртуалната частна мрежа има определени предимства пред услугата на dial-up сървъра за отдалечен достъп.

Проблемите, свързани с производителността на VPN мрежите, могат да бъдат категоризирани по два начина: общи проблеми на производителността и проблеми, които са специфични за конкретни VPN реализации. Повечето сериозни проблеми на производителността се дължат на глобалната мрежа Интернет. Често възникват прекъсвания на достъпността от регионален и от всеобщ характер. Тежкият трафик може да предизвика забавяния и блокирания на системите. Освен това отделни ISP доставчици могат да се сблъскат с изключвания на сървъри, които обслужват стотици или дори хиляди свои потребители. Технологията на VPN мрежите може също да доведе до различни количества допълнителни служебни данни, които намаляват производителността. VPN мрежи на ниво вериги не могат да постигнат скоростта на виртуалните мрежи на ниво мрежа. Когато се използва обществената мрежа за установяване на връзката, се загубва елементът на контрол, който се реализира при директна входяща dial-up връзка.

4.9. Стандарт IEEE 802.11.

4.9.1. Обосновка на стандарт IEEE 802.11.

Стандарт 802.11. е създаден от работна група за безжични локални мрежи на Комитета по стандарти на организацията IEEE, която започва работа през 1990 година. Задачата на тази работна група е била да разработи всеобщ стандарт за предаване на данни по радиоканал за безжични локални мрежи, които ще работят на честота 2.4 GHz със скорост на предаване на данни 1 и 2 Mbps. Работата по създаването на стандарта е завършена през 1997 година, когато е ратифицирана първата официална спецификация на стандарт 802.11. Стандартът 802.11. е първият стандарт за безжични мрежи (WLAN, Wireless Local Area Network), приет от независима международна стандартизираща организация. Организацията IEEE е разработила освен стандарта 802.11. и множество други спецификации и стандарти за мрежовите връзки между компютри по кабелни линии и оптически влакна.

Междувременно технологиите за предаване на данни се развиват с нарастващо темпо, така че първоначално заложените в стандарта скорости за предаване на данни от 1 и 2 Mbps не са достатъчни за обмен на големите по обем съобщения, които се обменят по съществуващите мрежи и много бързо стават безинтересни за потребителите. Това подтикна разработчиците на стандарта IEEE 802.11. към развитие и създаване на нови стандарти, които се явяват разширения на основния.

Това става през септември 1999 година, когато е ратифицирано разширението на стандарта, получило наименованието IEEE 802.11.b. (IEEE 802.11. High Rate). Основната разлика от предишния стандарт е повишената до 11 Mbps скорост на обмен на данни между безжичните устройства, което означава трансфер над 1.4 Mbps между устройствата, и се създават възможности за преминаване към изграждането на гъвкави безжични корпоративни мрежи.

Съвместимостта между продуктите, произведени от различни производители, се гарантира от независима организация, наречена Wireless Ethernet Compatibility Alliance (WECA, http://www.weca.net), създадена през 1999 година от лидерите в производството на мрежови устройства, между които са: Cisco, Lucent , 3Com , IBM , Intel, Apple, Compaq, Dell, Fujitsu, Siemens, Sony, AMD (над 80 компании).

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 служебни функции са определени в стандарта 802.11., а спецификацията 802.11.b. засяга физическото ниво на комуникационния модел.

На физическо ниво са предвидени общо три метода за предаване на данни, единият от които е в инфрачервения диапазон, а другите два са радиочестотни, 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 метод на честотните подскоци (FHSS – Frequency Hopping Spread Spectrum).

4.9.2. Режими на работа и методи за предаване на съобщения в стандарт 802.11.

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.

Клиентът 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 в повечето програмни пакети, управляващи Access Point процедурите по настройването на компютрите, които няма как да се избегнат.

Първият режим, точка – точка, наричан още IBSS – независим набор от обслужвания, както личи и от заглавието, сполучливо трансформирано от неразбираемото Ad-hoc, представлява елементарна като структура мрежа, в която отделните станции се свързват една с друга пряко, без да е необходима точка за достъп. Това налага 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 протокола 802.11.

Режимът клиент/сървър предполага използването на поне една точка за достъп, представляваща специализирано устройство, 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 обслужвания** (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, свързана към стационарната мрежа (например към мрежов принтер, скенер или Интернет).

Безжичната локална мрежа представлява гъвкава система за обмен на данни, която може да се разглежда като разширение или алтернатива на жичната локална мрежа.

Безжичните LAN мрежи са базирани на радиовълнова технология, използваща разпределен спектър (spread spectrum). Технологията е била създадена в Англия по време на Втората световна война. За да преодолеят използваното от германците заглушаване на радиосъобщенията, военните специалисти прибягват до радиовръзки с разпределен честотен спектър. С използване на тази технология всяко съобщение се изпраща едновременно по повече от един канал, които трудно могат да бъдат заглушени едновременно.

През 1997 г. международната организация IEEE създава спецификацията 802.11., дефинираща интерфейсите за връзка между безжичен клиент и базова излъчваща станция, както и между два безжични клиента.

Съгласно спецификацията 802.11. носещата честота е 2.4 GHz, максималната скорост на предаване на данни е 2 Mbps, а методите за модулация на сигналите са DSSS (Direct Sequence Spread Spectrum) – непрекъсната последователност в радиочестотния спектър и FHSS (Frequency Hopping Spread Spectrum) – честотно прескачане в радиочестотния спектър. Изброените характеристики в спецификацията са обявени като основни за безжичните мрежи, предназначени за свободно ползване.

Повечето безжични локални мрежи използват разгърнат (широк честотен) спектър за предаване на информацията. Тази технология е разработена първоначално за военни цели и се използва в комуникационните системи, където сигурността е от първостепенно значение. Сигналите на предавателите, които се предават по широка честотна лента, са по-силни и по-лесни за улавяне от приемника. Ако приемникът не е настроен на точната честота, сигналът се приема като фонов шум, тъй като енергийният спектър се определя само за ограничения на мощността за отклонения до ± 11 MHz от централната честота, при което мощността отслабва до –50 dB.

Обикновено се приема, че енергията на канала се простира не по-далеч от тези честотни граници. По-правилно е да се каже, че за дадено раздалечение между канали 1, 6 и 11 сигналът на всеки канал трябва да бъде достатъчно затихнал, за да се намали до минимум влиянието на предавателя за всеки друг канал. Вследствие на проблема „*заглушаване на слабия сигнал*” (near-far problem), при който приемането на слаб сигнал се „*потиска*” поради наличето на по-силен такъв, е възможно да се ограничи приемането на сигнали в области на „не-препокриващи” се канали. Този проблем се случва само когато заглушаваният приемник е разположен в рамките на метър или при работа с мощност над допустимите нива.

Технологията на предаване на сигнали в разгърнат честотен спектър има две разновидности: честотно прескачане (Frequency-Hopping Spread Spectrum – FHSS) и непрекъсната последователност (Direct-Sequence Spread Spectrum – DSSS).

При технологията **честотно прескачане** се използва носеща честота с тясна честотна лента, която мени честотата си по начин, известен както на предавателя, така и на приемника. При подходяща синхронизация се осъществява поддръжка на постоянен логически канал между приемника и предавателя. Приемниците, настроени на останалите честоти, възприемат работния сигнал като краткотраен импулсен шум. Известно е, че телефонните линии, които първоначално са използвани за предаване на глас, могат да предават и цифрови данни. По същия начин и радиовълните се разглеждат като среда, която се асоциира предимно с радиопредавания и могат да се използват за предаване на сигнали, носещи цифрови данни. Създаването на безжичните устройства е по-нататъшно развитието на предаване на глас и цифрови данни. Създава се възможност за по-голяма свобода и удобство при изграждането на комуникационните мрежи. Увеличаващият се брой на мобилни абонати, нежелаещи да използват фиксирани точки за включване към комуникационните мрежи, допълнително

стимулира развитието на радиочестотните технологии. Глобално погледнато, потребността на съвременния човек от модерни бързо действащи и високоскоростни комуникации нараства непрекъснато. Според изчисленията на аналитиците през следващите години в света ще има милиарди мобилни устройства, оборудвани с безжична връзка.

При технологията **с непрекъсната последователност** за всеки бит, който трябва да се предаде, се генерира битова последователност с излишък, наречена чипов код. По-дългият код увеличава вероятността да бъдат възстановени оригиналните данни. В случай на грешка в един или няколко бита по време на предаването вградените средства в приемника могат да възстановят информацията, без да се налага да се препредава отново. Останалите приемници възприемат този сигнал като слаб широкочестотен шум, който се пренебрегва от повечето тяснолентови честотни приемници.

Не след дълго се появяват и други спецификации за безжични мрежи, които, заедно с 802.11., образуват фамилия от спецификации, означавана като 802.11.

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

За стандартизиране на радиомрежите за предаване на данни в глобален мащаб IEEE присвои на безжичните технологии общия номер **802** за изграждане на локални мрежи (LAN) и градски мрежи (MAN). На базата на този общ номер са създадени работни групи за разработка на спецификации. Една от тях е групата 802.11., която създава фамилията от спецификации 802.11.

Други работни групи и съответно спецификации са 802.15. за създаване и развитие на мрежата Bluetooth и 802.16. за поддръжката на широколентовите безжични системи, предназначени за MAN мрежи.

Най-важните създадени спецификации за безжични локални компютърни мрежи са с характеристики, показани в таблица 9.1.

Таблица 9.1

Тип	Максимална скорост	Реална скор	Брой каналите	Вероятен вътрешен/въ обхват	Носеща честот
802.11a (Wi-Fi)	54 Mbit/s	~30 Mbps	8	35/120 m	5 GHz
802.11b (Wi-Fi)	11 Mbit/s	~6 Mbps	14	38/140 m	2.4 GHz
802.11g (Wi-Fi)	54 Mbit/s	~30 Mbps	14	38/140 m	2.4 GHz
802.11n (Wi-Fi)	300 Mbit/s	~130 Mbps	2	70/250 m	2.4 / 5 GHz

Стандартът 802.11.a. предвижда използване на 8 канала за предаване на данни. Вместо дефинираните в 802.11. схеми за модулация DSSS или FHSS, използващи разпределени честотни спектри, в 802.11.a. се прилага методът OFDM (Orthogonal Frequency Division Multiplexing). Тази технологията не е получила широко разпространение поради относително високите цени на оборудването и ограничения обхват на действие. По-добра е от популярната 802.11.b. по отношение трансфера на данни за аудио- и видеосъобщения, но й отстъпва по отношение на обхвата на действие. Като сериозен недостатък на този стандарт се изтъква и несъвместимостта на оборудването му със стандарт 802.11.b. Продуктите, отговарящи на този стандарт, са маркирани с Wi-Fi сертификат.

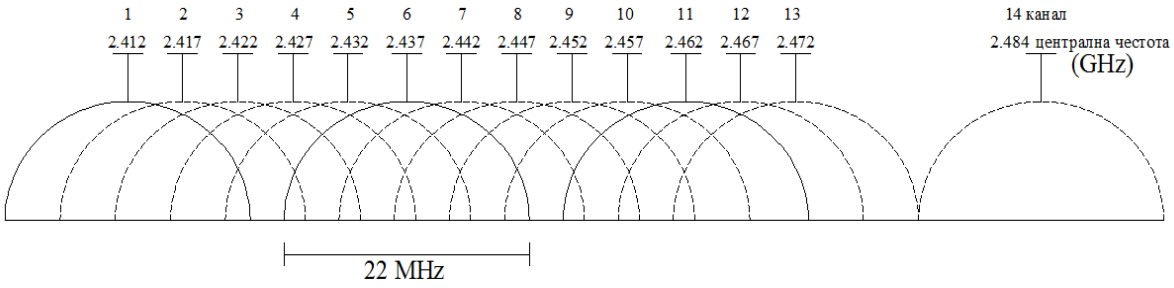
Стандарт 802.11.b. е най-популярната безжична технология, утвърдена и обявена през 1999 г. като по-нататъшно развитие на стандарта 802.11. Означава се още като 802.11. High Rate или като Wi-Fi и използва модулация DSSS. Технологията осигурява функционалност на

компютърната мрежа, съответваща на стандарта Ethernet. При честота 2.4 MHz осигурява максимална скорост за предаване на данни от 11 Mbps, която при намалена пропускателна възможност (fallbacks) спада на 5.5 Mbps, 2 Mbps или 1 Mbps. Обхватът на действие на комуникационната среда достига до 500 метра. Стандартът предвижда възможност за използване на 14 честотни канала, от които 3 са с незастъпващи се честотни ленти. Продуктите, отговарящи на този стандарт, са маркирани с Wi-Fi сертификат.

Стандарт 802.11.g. е разработен с цел постигане на по-високи скорости, достигащи до 54 Mbps в честотната лента на 2.4 GHz диапазон. При скорости над 20 Mbps се използва схемата OFDM, а при такива под 20 Mbps схемата DSSS. И този стандарт разполага с 14 канала, от които 3 са незастъпващи се (фиг. 9.12). Предвидена е допълнителна сигурност чрез въвеждане на системата Wi-Fi Protected Access (WPA). Продуктите, отговарящи на този стандарт, са отбелязвани с Wi-Fi сертификат. Устройствата на стандарта са функционално съвместими с тези на стандарт 802.11.b., което позволява 802.11.b. устройствата да бъдат заместваны директно с 802.11.g. устройства. Към настоящия момент устройствата от тип 802.11.g. имат широко разпространение, съизмеримо с това на тези от тип 802.11.b. Днес преносимите компютри като правило притежават вградена карта за безжична връзка, съвместима едновременно със стандартите 802.11.b. и 802.11.g.

Разделянето на честотните ленти на отделни канали е аналогично с това на радио и телевизионните предавателни канали. Например честотният диапазон от 2.400 до 2.4835 GHz е разделен на 13 канала с широчина от 22 MHz, всеки от които е разположен на 5 MHz от друг. Първият канал е центриран на 2,412 GHz , а тринадесетият на 2,472 GHz. Към тези канали Япония добавя 14-и канал, центриран на 12 MHz над канал 13.

Използването на каналите се урежда на държавно и регионално ниво в зависимост от приетите правила за разпределение на радиочестотния спектър. В Япония е позволено използването на всички 14 канала, докато в други държави – като Испания, първоначално се позволява използване само на 10. и 11. канал, във Франция са разрешени комуникации само на 10., 11., 12. и 13. канал. В днешно време повечето страни следват европейския модел и са почти толкова либерални, колкото Япония, недопускайки комуникации само по канал 14. В Северна Америка и някои страни от Централна и Южна Америка допълнително се забраняват 12. и 13. канал. Разпределението на каналите от 1 до 14 е показано на фиг. 9.12.

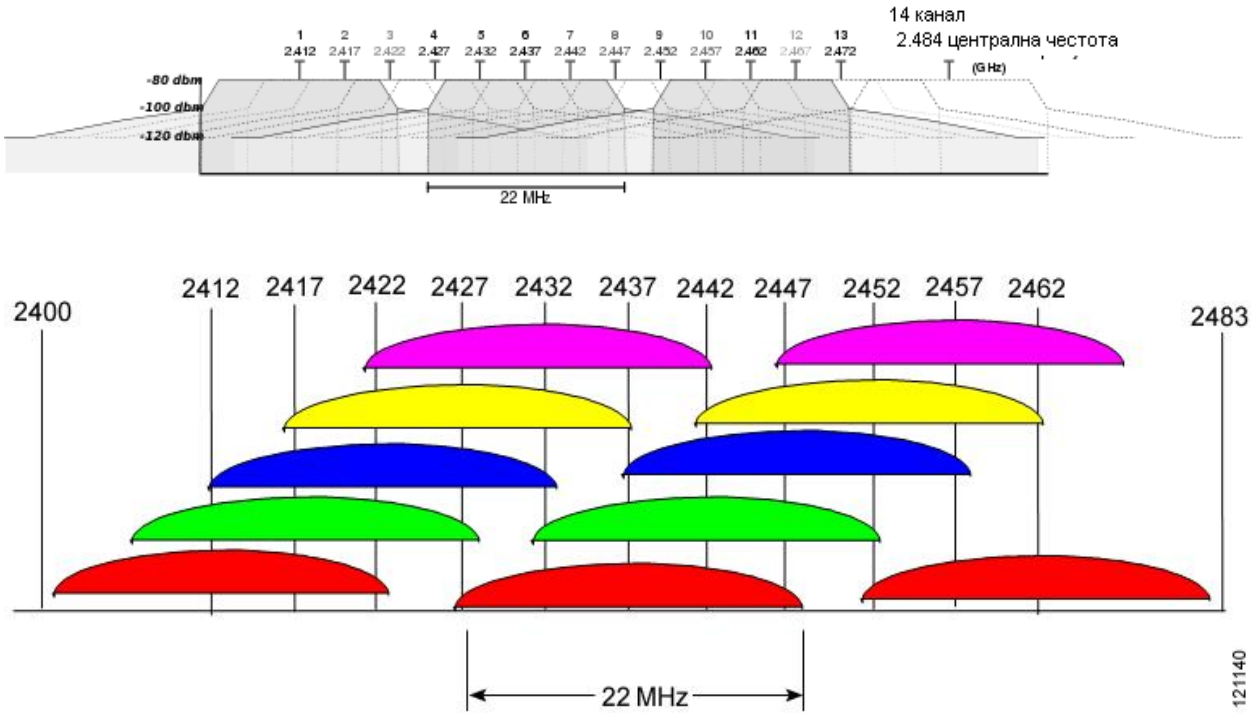


Фиг. 9.12. Графично представяне на каналите в 2.4GHz честотен диапазон

Освен определяне на централната честота на всеки канал в стандарта 802.11. също така се уточнява *спектрална картина (маска)* (фиг. 9.13), определяща разрешеното разпределение на енергията между всеки канал. Изисква се сигналът да затихне най-малко с 30 db от пиковата си енергия на отстояние ±11 MHz от централната честота на канала, което означава, че каналите са ефективни в честотна лента с широчина от 22 MHz. За да се осигури електронна съвместимост, станциите могат да използват само всеки четвърти или пети канал,

без да се препокриват. Обикновено в Северна и Южна Америка се използват 1., 6. и 11. канал, в Европа се препоръчва работа на мобилните мрежи на 1., 5., 9. и 13. канал.

Въпреки твърдението, че каналите 1., 6. и 11. са "непрепокриващи се", съществуват ограничения по отношение на разстоянието или мощността на разпространение на отделните сигнали. Правилото за ползване на канали 1-6-11 има своите предимства от гледна точка на електронната съвместимост. Ако предаватели са сближени спрямо каналите 1., 6. и 11. (например 1., 4., 7. и 10.), препокриването между каналите може да доведе до неприемливо влошаване на качеството на сигнала и пропускателната способност. Въпреки тези проблеми застъпващи се канали може да бъдат използвани при определени обстоятелства.



Фиг. 9.13. Спектър на сигналите за стандарт 802.11.g.

Стандартът 802.11.n. е утвърден от IEEE през септември 2008 г. През октомври 2007 г. WEA (Wi-Fi Alliance) публикува документа 802.11.n. draft 2.0, който на практика служи като стандарт за производството на първите 802.11.n. устройства. Стандартът разполага с два канала, всеки един от които работи с честотна лента от 20 MHz, осигурявайки скорост на предаване на данни от 88.5 Mb/s. Съвместно двата канала работят в честотна лента от 40 MHz, постигайки скорост 146.83 Mb/s. Постигнатата скорост е 5 пъти по-голяма в сравнение със скоростта на стандарт 802.11.g., която е около 30 Mbps. Стандартът 802.11.n. е съвместим с по-старите спецификации 802.11.b. и 802.11.g.

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

Приемопредавателите, наричани точки за достъп (access points), се използват за предаване и приемане на данни между безжичното устройство или устройства и кабелната мрежа, както е показано на схемите на фиг. 9.14 до фиг. 9.23.

Безжичните компютърни мрежи се изграждат по различни методи за достъп на крайните възли до мрежовите ресурси и комуникационните услуги към други мрежи. На практика се изграждат следните мрежи:

- Безжични компютърни мрежи ad-hoc (peer-to-peer).
- Безжични компютърни мрежи с използване на точки за достъп (AP – Access Point) до жични LAN.

Ad-hoc мрежите се състоят от компютри, снабдени с интерфейсни карти за безжична комуникация. Картите за безжичен достъп изпълняват същата роля, каквато изпълняват традиционните мрежови карти за Ethernet или Token Ring. Те също притежават свои уникални MAC адреси, посредством които компютрите са идентифицирани в мрежата.

Всеки компютър от компютърната мрежа ad-hoc може да заема комуникационния радиоканал, да комуникира директно с всички останали компютри от същата мрежа и да предава съобщения (фиг. 9.14).

Фиг. 9.14. Точка-точка (Ad-hoc) мрежа

За да могат компютрите на една безжична мрежа да получат достъп до ресурсите на жична локална мрежа, е необходимо да съществува поне една точка на достъп (AP), през която да се осъществява връзката между двата типа мрежи.

Тази точка може да бъде специализирано хардуерно устройство (HAP – Hardware Access Point), както е показано на фиг. 9.15, или компютър, на който е инсталиран необходимият за целта софтуер (SAP – Software Access Point), както е показано на фиг. 9.16. За реализация на връзка на безжична с жична LAN биха могли да се използват повече на брой точки за достъп, което всъщност представлява свързване на повече безжични мрежи с една жична LAN (фиг. 9.17).

Фиг. 9.15. Ad-HAP – Hardware Access Point

Фиг. 9.16. Софтуерна точка за достъп (SAP – Software Access Point)

Посредством повече на брой точки за достъп може да бъде осигурена безжична връзка в отделни постройки и помещения – офиси, класни стаи, лаборатории – с една базова жична LAN. Този начин на свързване на безжични и жични мрежи е подходящ за изграждане на училищни и университетски компютърни мрежи.

В други случаи една безжична компютърна мрежа би могла да се свърже с повече жични LAN чрез използване на точки на достъп, свързани към всяка една от тези LAN.

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

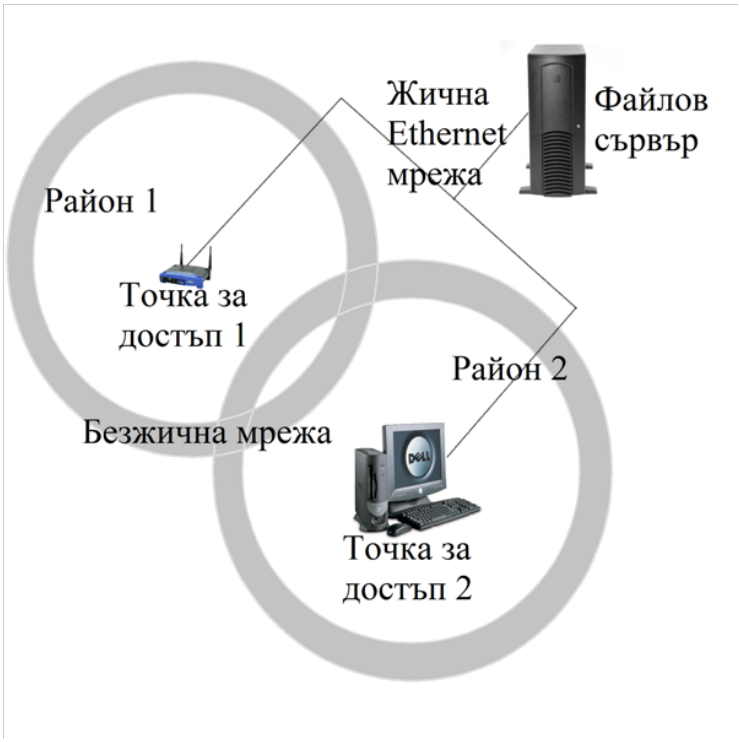
Фиг. 9.17. Мрежа с повече N-брой точки

Обхватът на действие на безжичната комуникация може да бъде увеличаван чрез използване на разширителни точки (Extension Points) – фиг. 9.18.

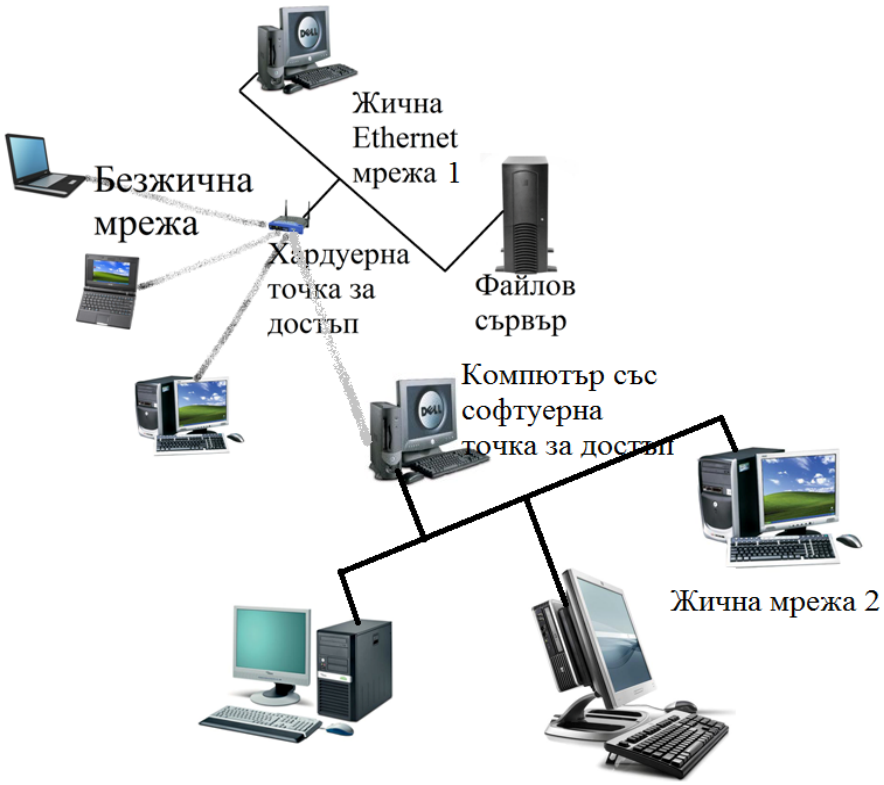
Безжичните мрежи биха могли да изпълняват функцията роуминг. Радиовълните на всяка точка за достъп покриват определена област, наричана обхват на действие. Когато биват използвани едновременно повече точки на достъп, възможно е областите им да се препокриват (фиг. 9.19). Роуминг функцията следи интензивността на сигналите в препокриващите се области и осъществява връзка с онази точка на достъп, чийто сигнал е по-интензивен. Роумингът протича напълно прозрачно за потребителя. Функцията е особено полезна, когато компютърът е мобилен, например при движение на потребител, снабден с

преносим компютър. Поради липса на стандарт за роуминга не всички точки на достъп, предлагани на пазара, могат да бъдат конфигурирани да извършват тази функция.

Фиг. 9.18. Разширителни точки (Extension Points)



Фиг. 9.19. Роуминг схема



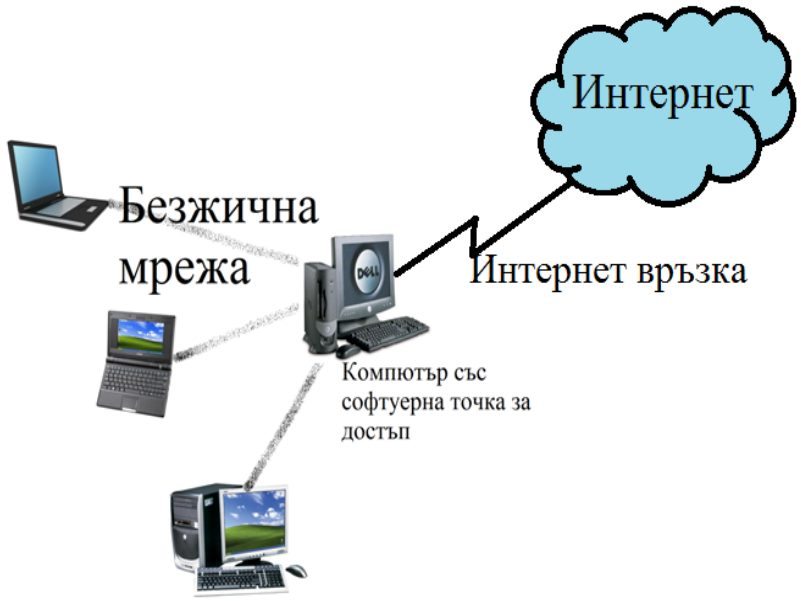
Фиг. 9.20. Две точки мостове (2p Bridges)

Две жични LAN могат да бъдат свързани помежду си безжично посредством използване на две точки за достъп (фиг. 9.20) при условие, че двете точки са в състояние да комуникират помежду си. Трябва да се знае, че не всички точки за достъп са в състояние да осъществяват безжична връзка помежду си. Използване на такава връзка се налага, когато липсва физическа възможност за прокарване на кабел, който да свърже двете LAN, например когато те се намират в две близко разположени сгради, разделени от една или повече улици. Всяка една от точките за достъп трябва да е в състояние да изпълнява за своята жична LAN ролята на безжичен мост (wireless bridge) за връзка с други LAN.

На фиг. 9.20 една от точките за достъп (в случая двете точки представляват безжични мостове) изпълнява водеща роля – ролята на *master*, а другата е подчинена на първата, изпълнявайки ролята на *slave*. Връзката между тях е от типа *poin-to-point*. Ако взаимносвързаните точки за достъп са повече от две, възниква структурата *poin-to multi point*. В нея всички точки за достъп са безжични мостове, които комуникират всеки с всеки.

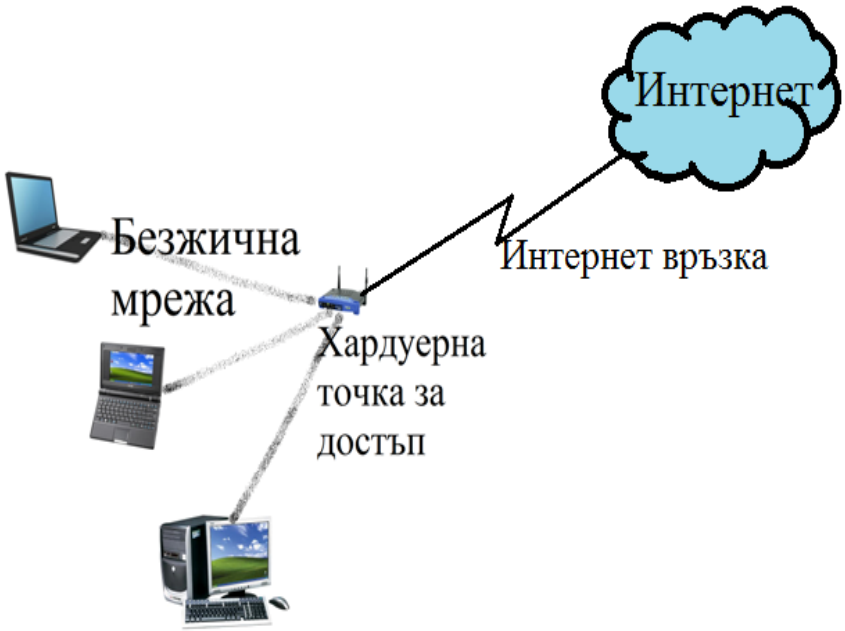
Когато само една от точките е безжичен мост, тя изпълнява ролята на **master**, а другите точки са *slave*. Такъв вид структура се нарича *главен плюс точки за достъп* – **master** *plus APs* (Access Points). В случая slave точките не са в състояние да комуникират директно помежду си.

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

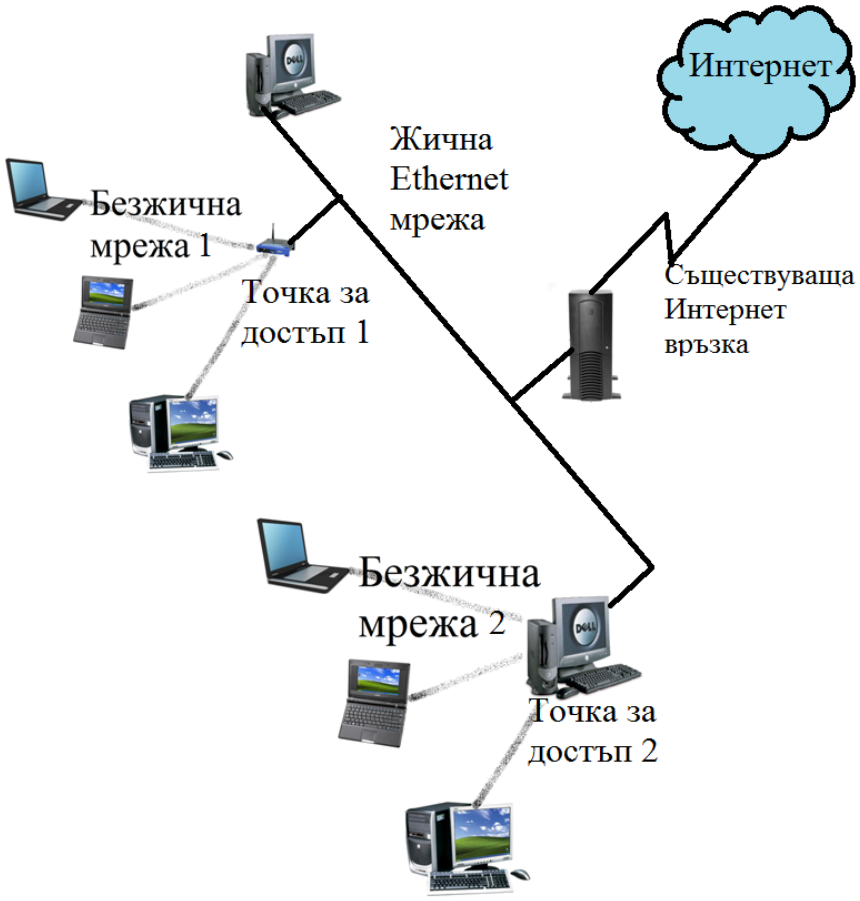


Фиг. 9.21. Мрежа със софтуерна точка за достъп, свързана към Интернет

Безжичните мрежи биха могли да се свързват и към Интернет. За целта е достатъчно компютърът, към който е свързана точката за достъп, да има връзка с Интернет (фиг. 9.21). На пазара се предлагат хардуерни точки за достъп, които могат да осъществяват директна връзка с Интернет (фиг. 9.22).



Фиг. 9.22. Хардуерна точка за достъп



Фиг. 9.23. Мрежа с хардуерна и софтуерна точка за достъп

Една безжична LAN би могла да осъществява връзка с Интернет посредством жична връзка със софтуерна точка на достъп, принадлежаща на безжична мрежа. Тази връзка е илюстрирана с безжична мрежа 2, показана на фиг. 9.23. Друга безжична мрежа (безжична мрежа 1) може да получи също достъп до Интернет, ако бъде свързана със същата жична LAN по традиционния начин чрез използване например на хардуерна точка за достъп – фиг. 9.23.

На фиг. 9.23 софтуерната точка за достъп изпълнява едновременно три функции – връзка с Интернет, връзка с жична LAN и връзка с втора безжична мрежа. Това не изключва възможността жичната LAN да бъде свързана по традиционния начин с друга безжична мрежа. Последната също ще получи достъп до Интернет, тъй като жичната LAN е вече свързана с Интернет.

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

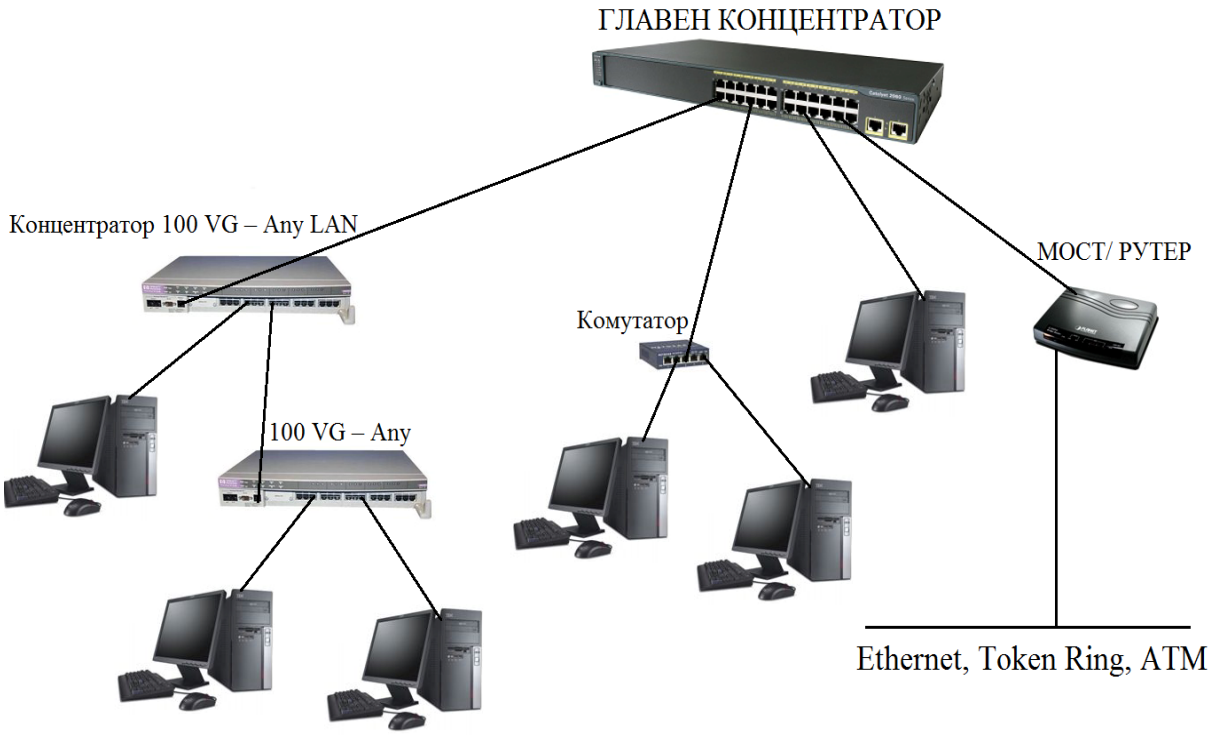
4.10. Стандарт IEEE 802.12. (100 VG – Any LAN)

Стандартът е създаден за предаване на данни със скорост до 100 Mb/s. Абревиатурата Any LAN означава, че стандартът поддържа предаване на съобщения във взаимодействие с останалите локални мрежи. Този стандарт поддържа кадри с формат Ethernet и кадри с формат Token Ring, които използват в 90 – 95% от LAN технологиите на практика. Технологията 100 VG – Any LAN се конкурира с Fast Ethernet, но фирмите производителки на мрежово оборудване поддържат и двата стандарта.

Протоколите на стандарта IEEE 802.12. напълно съответстват на OSI модела. Единствената разлика е във физическия слой на стандарта, който е разделен на два подслоя:

- долен подслой PMD, зависещ от физическата среда;
- горен подслой PMI, независещ от физическата среда.

В стандарта се използва физическа топология тип "дърво" – фиг. 9.24. Състои се от главен концентратор на първо ниво. Към него са включени концентратори от второ ниво или мрежови възли като компютри, мостове, рутери и комутатори. Допуска се каскадно свързване на концентратори до пет нива.



Фиг. 9.24. Структура на LAN 100 VG – Any LAN

Главният концентратор е интелигентен контролер, който управлява достъпа до средата, като сканира портовете си в кръг. Той приема кадър от възела, изпратил заявка, и го предава към порта, където е свързан възел получател.

Всеки концентратор 100 VG – Any LAN може да се конфигурира, за да поддържа кадри 802.3. (Ethernet) или кадри 802.5. – Token Ring. Спазва се изискването концентраторите в един сегмент да поддържат кадри само от един тип.

Всички концентратори освен главния имат един възходящ (up-link) порт и N низходящи (down-link) портове. Up-link портът се ползва за свързване с концентратор от по-високо ниво, а низходящите портове са за връзка с концентратори от по-долно ниво или крайни мрежови възли.

Възлите в мрежата се свързват чрез следните линии:

- четири двойки UTP категория 3 или 4;
- две двойки UTP категория 5;
- две двойки STP тип 1;
- две оптични влакна.

Когато за комуникационна среда се използват четири броя усукани двойки, данните се разпределят по четири канала, като MAC кадърът се разделя на 5-битови порции (квинтети). Всяка порция се подава последователно на съответен канал (отделен). Така се намалява скоростта на предаваните данни по линиите и се увеличава разстоянието между съседните възли.

Когато се ползват две усукани двойки или две оптични влакна, се извършва мултиплексиране и каналите от четири стават два.

Функциите на горния PMI подслой включват:

- скемблиране;
- линейно кодиране (5B/6B);
- добавяне към кадъра на встъпителна част;
- добавяне на начален и краен ограничител на кадъра;
- предаване на кадъра към долния PMD подслой.

Скемблирането на данните е случайно разбъркване на квинтетите с цел избягване на комбинации с повтарящи се 0_2 или 1_2. По този начин се намалява излъчването на електромагнитни вълни и взаимното влияние между проводниците.

Кодирането по схемата 5B/6B е преобразуване на квинтетите в 6-битови комбинации. Това е линейно кодиране с цел получаване на балансирани кодови комбинации с еднакво количество 1_2 и 0_2. По този начин по-добре се синхронизира приемникът и могат да се откриват грешки при приемане на данните.

Протоколът MAC на стандарта е усъвършенстван с цел поддържане на новите мултимедийни приложения. Този протокол е наречен “приоритетен достъп” (Demand Priority). Концентраторът става арбитър, който решава въпроса за достъпа до общата споделена комуникационна среда. Използват се две нива на приоритет: ниско и високо.

Функциите на MAC подслоя са:

- подготовка за заемане на комуникационната линия;
- формиране на кадър със съответен формат.

Предаването на кадъра по този протокол става със заявка. Заявката може да има нисък или висок приоритет. Високият приоритет е за трафик на мултимедийни приложения, които са чувствителни към закъснения.

Главният концентратор сканира кръгово портовете си и проверява за заявки (round – robin). На един възел се разрешава предаване само на един кадър за едно сканиране. Концентраторите от по-ниски нива също сканират кръгово свързаните към тях портове и възли. За един цикъл те имат право да предадат нагоре толкова кадри, колкото на брой крайни

възли са свързани. Заявките с нисък приоритет се обслужват само ако няма такива с висок приоритет.

В началото съществува процедура за подготовка на линията (Link Training), при която концентраторите автоматично разпознават включените устройства към портовете. Разменените служебни кадри съдържат следните данни:

- Вид на устройството (краен възел, концентратор, мост, рутер и др.).
- Режим на работа (нормален или мониторен).
- Адрес на възела.

Концентраторите си разменят серия от специални кадри за тестване на кабела и проверка на правилното свързване на съединителите.

4.11. Други стандарти за безжични мрежи

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

В Европа е разработен и се ползва още един стандарт – HiperLAN/2, който представлява усъвършенстван вариант на предшественика си HiperLAN/1. Осигурява възможност за работа с ATM клетки и IP пакети, както и предаване на глас посредством клетъчни телефони. Използваната носеща честота е 5 GHz, а скоростта на трансфер 54 Mbps. Кодиращата схема е OFDM (Orthogonal Frequency Division Multiplexing). Предвидени са средства за защита на информацията, включително възможност за лична автентикация.

Стандартът Bluetooth работи в честотния диапазон 2400 – 2483.5 MHz, осигурявайки скорост на предаване, достигаща максимум до 2 Mbps. За устройствата, работещи в синхронен режим, типичната скорост е 723,2 Kbps, а за тези, които използват асинхронен режим, тя е 433,9 Kbps. Обхватът на действие е около 10 метра. Схемата на модулация е FHSS. Като средства за защита могат да бъдат използвани протоколите PPTP, SSL или VPN. Bluetooth не поддържа протоколния стек TCP/IP.

Bluetooth притежава свойство, отличващо го от останалите технологии – Bluetooth устройствата влизат в контакт едно с друго автоматично, веднага след като попаднат в обсега на приемо/предавателя. За установяването на връзката между абонатите на мрежата, за автентификацията на потрбителите и др. се грижи приложно програмно осигуряване.

Стандартът ZigBee получава името си по подобие на зигзагообразния (zigzag) танц на пчелите (*Bee – пчела*), посредством който те предават помежду си информация относно местонахождението (посока и разстояние) на източниците на храна.

Основният коз на *ZigBee* е икономичността по отношение на консумацията на електрическа енергия. Енергията на една стандартна батерия тип AA е достатъчна за радиоизлъчване в продължение на повече от една година. Определението гласи, че IEEE 802.15.4. е стандарт за нискоскоростни частни мрежи – Low Rate Wireless Personal Area Network (LR-WPAN). Той има на разположение 27 радиоканала в три честотни диапазона – 16 канала в общоприетия в цял свят 2,4 GHz диапазон, един допълнителен диапазон на 915 MHz в САЩ (10 канала) и още един на 868 MHz в Европа (един канал). Скоростта на предаване на данните зависи от броя на свободните канали и варира между 20 и 256 Kbps. Разпределението на каналите става по принципа на контрола на носещата (CSMA; Carrier Sense, Multiple Access) – устройството "слуша" ефира и започва предаване само когато той се освободи.

Предимствата на безжичните мрежи могат да се обобщят, както следва:

- **Подвижност:** безжичните мрежи предлагат на потребителите достъп до информацията в реално време от всяка точка. Това води до производителност, която не може да бъде постигната при жичните мрежи.
- **Простота на инсталирането:** то става бързо и лесно, тъй като не се налага да се прекарват кабели през стени и тавани.
- **Гъвкавост на инсталация**: безжичната технология позволява да се осъществи достъп до мрежата от точки, до които не могат да бъдат прекарани кабели.
- **По-ниска стойност**: въпреки че стойността на необходимия хардуер за изграждането на една безжична мрежа е по-висока, разходите, свързани с инсталирането и поддръжката ѝ, се оказват значително по-ниски.
- **Универсалност**: безжичните мрежи могат да бъдат изградени по различни топологии – като се започне от връзките точка – точка, подходящи за малък брой потребители, и се стигне до инфраструктурните мрежи с хиляди потребители.

В таблица 9.2 са показани сравнителните характеристики на стандартите ZigBee, Bluetooth и Wi-Fi.

Таблица 9.2

Характеристики	**ZigBee 802.15.4**	**Bluetooth 802.15.1**	**WiFi 802.11b**
Основно предназначение	Контрол и наблюдение	Замества кабелите	Интернет, данни, видео и аудио
Продължителност на работа с батерия [дни]	100 – 1000 и повече	1 – 7	0,1 – 5
Брой устройства в една мрежа	255 – 65000 и повече	7	30
Скорост на данните [Kbps]	20 – 250	720	11000 и повече
Далечина на връзката [метри]	1 – 75 и повече	1 – 10 и повече	100 и повече
Други особености	Висока надеждност, консумация, ниска цена	Ниска цена и удобство	Скорост и гъвкавост

Инфрачервената технология за предаване на данни е друг начин за предаване на съобщения и се използва сравнително рядко в изграждането на безжичните компютърни мрежи. В тази технология за пренасянето на данни се използват много високи честоти. Това става с помощта на инфрачервени лъчи (Infrared – Ir). Инфрачервената технология е позната на широк кръг от потребители, тъй като тя се използва в дистанционните устройства за телевизори, видеокасетофони, аудиоуредби и т.н. Тя може да се използва и за изграждане на безжични мрежи, като сигналът се пренася с помощта на лъчи в инфрачервения спектър. За целта се използват много високи честоти, намиращи се в диапазона точно под видимия спектър на светлината.

Стандартите за Ir хардуера и софтуера се задават от организацията Infrared Data Association (IrDA). IrDA съвместимите устройства са проектирани така, че когато даден потребител прекрати инфрачервената връзка, тя се възстановява при повторното навлизане на устройство в Ir обхвата.

Ir мрежите изискват наличие на приемопредавател и в двете комуникиращи устройства. Възможно е да се изисква и специално програмно осигуряване за синхронизация на предавателите и приемниците. Някои операционни системи като Windows XP и 2000 притежават вградена Ir поддръжка. Скоростта на предаване варира от 4 Mbps до 16 Mbps. Инфрачервените вълни подобно на лазера са технология, която изисква пряка видимост между предавателя и приемника.

Недостатък при Ir технологията за изграждане на компютърни мрежи е уязвимостта от смущения, предизвикани от околната среда.

Думата **лазер** (laser) е съкращение от light amplification by stimulated emission of radiation (усилване на светлината чрез стимулирана емисия на лъчение, или още оптичен квантов генератор). Лазерът излъчва поле от кохерентна електромагнитна енергия, в което всички вълни са с еднаква честота и са подредени във фаза. Фазата е част от пълен цикъл, която е изминала и се измерва от конкретна опорна точка. Различните типове лазери произвеждат лъчи с различна дължина на вълната. Лазерните мрежи работят чрез използване на импулси лазерна светлина, с които се представя сигналът. Лазерът е технология, изискваща пряка видимост, т.е. между предаващите и приемащите устройства не трябва да има никакви препятствия. Необходимостта от гарантирана пряка видимост е недостатък на базираните на лазер безжични комуникации.

Въпроси за самостоятелна работа

1. Кога и от коя организация са създадени стандартите за изграждане на локалните компютърни мрежи?
2. Защо процесите на компютърните комуникации са стандартизирани?
3. Как се декомпозира каналният слой на възлите в локалните кампютърни мрежи?
4. Какви физически и логически топологии се използват за изграждане на локалните компютърни мрежи?
5. Какви видове комуникационни среди се използват за комуникационни канали?
6. Какви структури на кадрите се използват за различните стандарти?
7. Какви са архитектурите на съвременните компютърни мрежи?
8. Направете обосновка на необходимостта от изграждане на виртуални частни мрежи.
9. Какви са предимствата и недостатъците на безжичните компютърни мрежи?
10. Кои са предпочитаните съвременни стандарти за изграждане на локалните компютърни мрежи?

ГЛАВА 5. СТАНДАРТИ ЗА ИЗГРАЖДАНЕ НА ГЛОБАЛНИ КОМПЮТЪРНИ МРЕЖИ

Глобалната компютърна мрежа WAN (Wide Area Network) е компютърна мрежа, покриваща големи географски региони (държави, континенти).

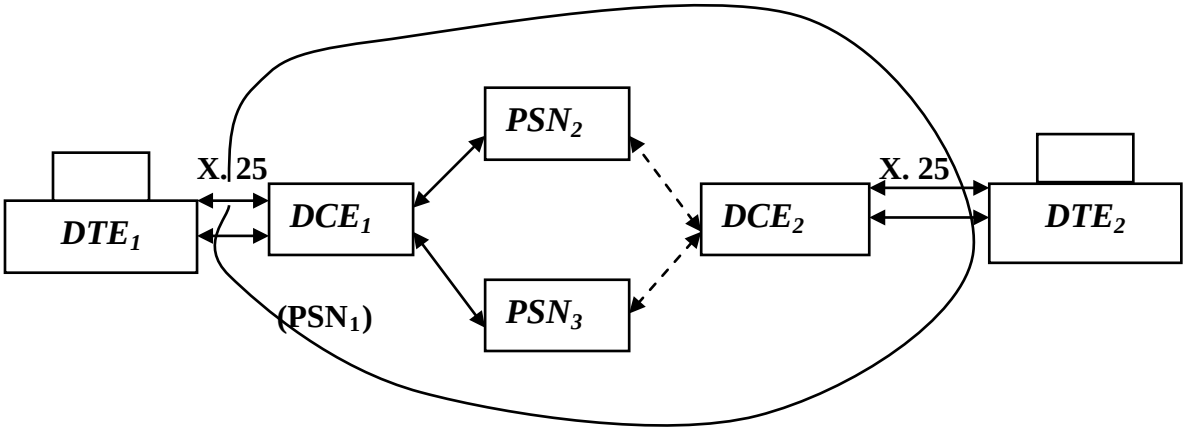
WAN се състои от множество комуникационни възли, свързани помежду си чрез комуникационни линии. Топологията на WAN е от произволен тип (смесена). Съобщенията от крайните възли податели се маршрутизират от комутационните възли, за да достигнат до крайните възли получатели. По правило междинните комутационни възли не се интересуват от вида и формата на информацията, която се предава през тях. Задачата им се свежда единствено до правилно предаване на съобщенията през мрежата до техните получатели. Стандартите, по които се проектират и изграждат глобалните компютърни мрежи, намерили широко приложение, са: X.25., Frame Relay, ATM и интегрираната мрежа ISDN [5].

В глобалните компютърни мрежи се използват различни методи на комутация на протоколните единици като:

- комутация на каналите (стандарт ISDN);
- комутация на пакетите (стандарт X.25.);
- бърза комутация на пакетите (стандарти Frame Relay – ATM);
- режим на виртуално съединение (всички стандарти).

5.1. Стандарт X.25.

Стандартът X.25. се прилага за изграждане на глобална компютърна мрежа с комутация на пакети. Скоростта на предаване на данни в тези мрежи достига до 2 Mbps. Стандартът определя интерфейса между крайния възел и глобалната подмрежа, показан на фиг. 10.1. Крайните възли се наричат DTE устройства (Data Terminal Equipment). За междинни мрежови възли се използват PSN устройства (Packet Switched Node). В стандарта се използва и DCE устройство (Data Circuit Equipment Equipment), което изпълнява ролята на крайно устройство в каналите за предаване на данни. Интерфейсът между DTE и DCE устройствата се определя от самия стандарт.

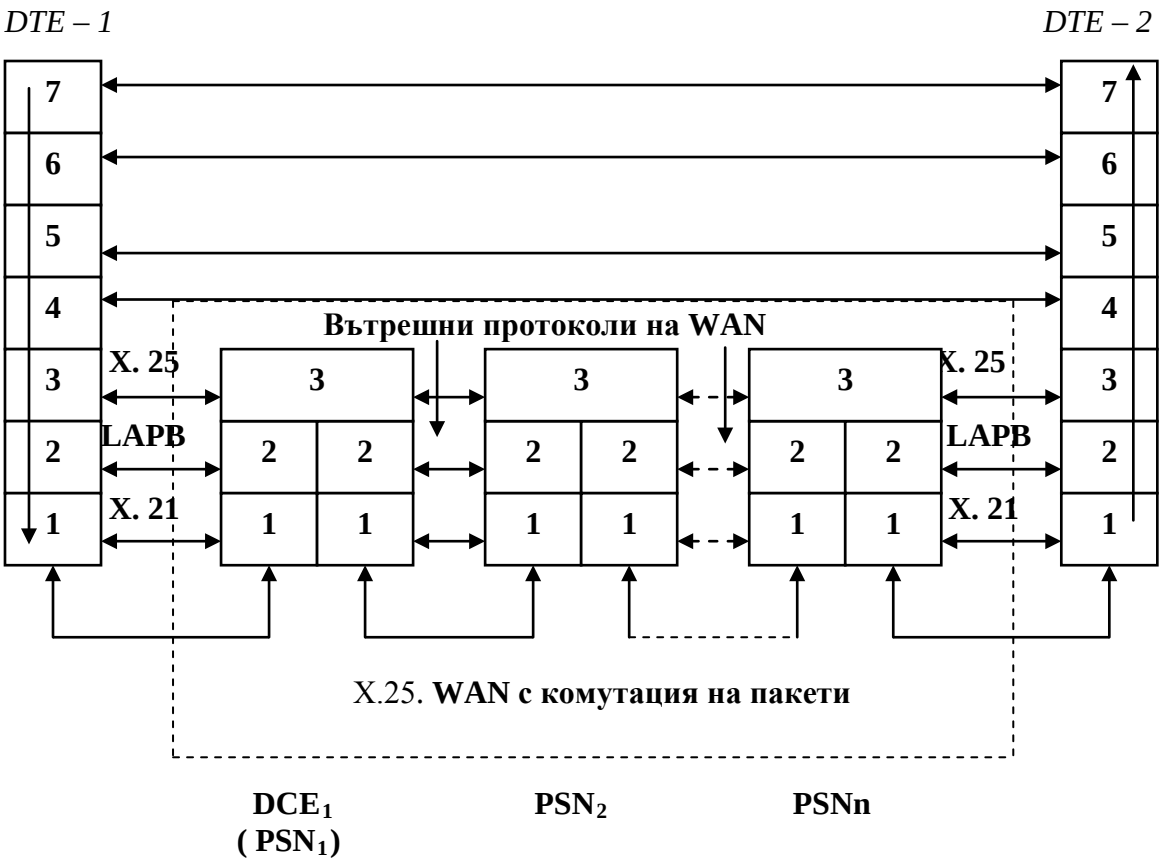


Фиг. 10.1. Схема на WAN с комутация на пакети, изградена по стандарт X.25.

X.25. е стандарт за достъп до WAN с комутация на пакети, като глобалната мрежа използва протоколния стек X.25., който съответства на долните три слоя на OSI модела (фиг. 10.1). Съответствието на стандарта с долните три слоя на отворения модел за комуникации е дадено в таблица 3.1.

Таблица 3.1

Протоколен стек X.25.	Слой от OSI модела
X.25.	Мрежов
LAPB	Канален
H.21,H.21bis	Физически



X.25. **WAN с комутация на пакети**

Фиг. 10.2. Приложение на протокол X.25. за достъп до WAN с комутация на пакети

Комуникационният сценарий на стандарт X.25. е представен на фиг. 10.2. Протоколните единици на стандарта за долните четири нива на комуникационния модел са дадени в таблица 3.2.

Таблица 3.2

Протоколна единица (PDU)	Слой от OSI модела
Транспортен блок	Транспортен
X.25. пакет	Мрежов
LAPB кадър	Канален
Поток от битове	Физически

Ф	А	У	Данни	К	Ф
1	1	1		2	1 байт

Фиг. 10.3. Структура на LAPB кадър в стандарта X.25.

Транспортният блок предава съобщението надолу към мрежовия слой на DTE подателя. Поставя му се заглавна част (ако е необходимо след пакетиране), за да функционира нормално мрежовият протокол X.25. Пакетът се предава в каналния слой, където се формират кадри, на които се съставят полетата Ф (флаг), А, У и К от протокола LAPB. Формира се LAPB кадър, показан на фиг. 10.3, който се предава на физическия слой на DTE устройството. Следва предаване на данните от физическия слой на DTE_1 към DCE_1, PSN_1, PSN_2….. PSNn и към DTE_2. Ако някъде кадърът се приеме с грешка или с променена структура, то съответният мрежов възел прави заявка до подателя за повторно предаване на кадъра. Повторението може да се извърши многократно до правилното приемане на пакетите. Мрежовият слой на приемния възел проверява дали пакетите се приемат с поредния номер на следване и след като ги подреди, ги препраща към транспортния слой на приемащото DTE_2 устройство.

Процесът на предаване на данни е бавен за съвременните изисквания за скорост и обем и затова се прилагат по-новите стандарти за изграждане на глобални мрежи като Frame Relay и ATM, при които се използват оптически линии за комуникация и каналите за предаване на данни са високоскоростни и с по-малка вероятност за грешка в предаването. В резултат на прилагането на съвременни технологии в комуникационното оборудване времето за закъснение на съобщенията е значително по-малко.

5.1.1. Физически слой на стандарт X.25.

Във физическия слой на стандарт X.25. се използват протоколите X.21. и X.21.bis. Тези протоколи описват електрическите, механическите, функционалните и процедурните характеристики на интерфейса DTE – DCE.

Протоколът X.21. използва цифров интерфейс, цифрова адресация и правила за достъп до наети цифрови линии. Протоколът X.21.bis. се ползва за работа със смесени аналогово-цифрови канали. Този протокол е съвместим с протокола RS – 232 C (V.24) и поддържа синхронно пълнодуплексно предаване по съединение тип “точка – точка” по четирипроводна линия при максимално разстояние между DTE и DCE устройствата не повече от 15 m.

5.1.2. Канален слой на стандарт X.25.

Между обектите на каналния слой данните се предават под формата на кадри. Използва се протоколът LAPB (Link Access Protocol – Balanced).

Протоколът LAPB се нарича балансиран, защото позволява на DTE и DCE да инициализират съединение към другата страна. Протоколът LAPB проверява всеки приет кадър за грешки с помощта на цикличен CRC код и реда на следване на кадрите. Кадрите се предават по метода на плъзгащия се прозорец с размер 8 кадъра в стандартен режим и 128 кадъра в разширен режим. Процедурите за контрол се дублират и в мрежовия слой, в резултат на което вероятността за грешки в каналите за предаване на данни се намалява от $1*10^{-3}$ до $1*10^{-6}$. Протоколът LAPB формира три вида кадри:

- информационни (I) кадри
- супервайзорни (S) кадри
- неномерирани (U) кадри.

Информационните кадри се използват за предаване на съобщенията между абонатите на компютърната мрежа.

Супервайзорните кадри са служебни. В тях липсва полето <данни> и изпълняват управляващи функции като:

- потвърждение за приети I-кадри;
- заявка за повторно предаване на I-кадри;
- временно задържане на предаване;
- доклад за състоянието на канала.

Неномерираните (U) кадри се използват за допълнително управляващи при:

- преминаване от стандартен към разширен режим на работа и обратно;
- генериране на съобщения за протоколни грешки.

5.1.3. Мрежов слой на стандарта X.25.

Функциите на мрежовия слой на стандарта се реализират от протокол с аналогично обозначение – X.25. Обектите на мрежовия слой си разменят данни във вид на пакети по установени виртуални (логически) съединения.

Стандартът определя два вида виртуални съединения:

- Постоянни PVC (Permanent Virtual Circuits) съединения.
- Комутируеми SVC (Switched Virtual Circuits) съединения.

PVC съединенията се използват по направления за непрекъснато предаване на данни. Съдиненията SVC се ползват за съединения с променлив трафик. Комутацията при SVC съединенията протича на три етапа:

- Установяване на логическо съединение между обектите, които си взаимодействат.
- Предаване на данни по пълнодуплексен комуникационен канал.
- Разпадане на съединението след завършване на предаването.

Използваните пакети в стандарта X.25. са два вида:

- Информационни пакети.
- Управляващи (служебни) пакети.

Информационните пакети съдържат части от съобщенията на крайните възли в полето <данни>. Управляващите пакети съдържат полета от данни за управление на комуникационните канали и мрежата.

Заглавната част на пакета е с три или четири байта. Тя се състои от отделни полета, които са различни за двата вида пакети. Полето <LCI> (Logic Circuit Identifier) е общо за двата вида пакети и съдържа дванадесетбитов номер на виртуалното съединение.

Максималният размер на полето <данни> е 4096 байта, като с подразбиране се приема предаване на данни с размер на прозореца от 128 пакета.

Мрежовият слой на стандарта X.25 извършва следните функции:

- Сегментация и десегментация – извършва се в крайния възел – подател и крайния възел – получател.
- Адресация на пакетите.
- Комутация на пакетите.
- Маршрутизация на пакетите.
- Мултиплексиране на пакетите.
- Управление на потока данни (Flow Control).
- Контрол на грешки в пакетите.

Адресацията на пакетите се прилага само при установяване на виртуални комутируеми съединения (SVC). Използват се X.121. адреси за идентификация на обекти от мрежовия слой. Тези адреси се указват само в служебните пакети. След установяване на логическа връзка и виртуално съединение в пакетите се указва само LCI номерът на виртуалното съединение, към което те принадлежат.

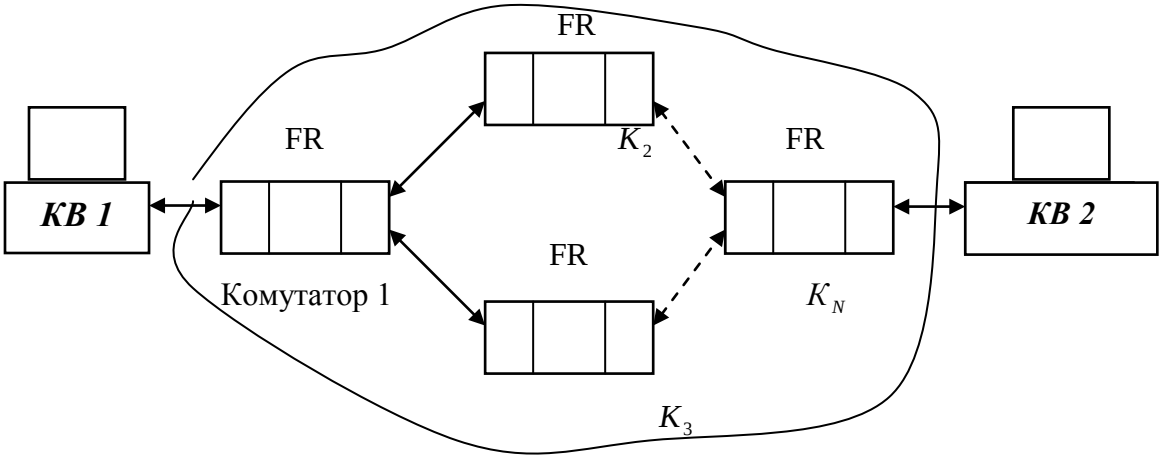
Мултиплексирането се реализира чрез DTE устройство, което може едновременно да установява 4095 виртуални съединения с други DTE устройства, по една линия, свързваща го с DCE устройство. Полето <LCI> от заглавната част служи за различаване на пакетите от различните виртуални съединения. Мултиплексирането е пълнодуплексно. Номерата на PVC съединенията започват с 1_{10}.

Използва се механизмът на плъзгащия се прозорец с размер 8 пакета в стандартен режим и 128 пакета в разширен режим. Всеки информационен пакет съдържа в заглавната си част собствения си номер P(S) от прозореца и номера P(R) на следващия пакет. Номерът P(R) се тълкува от отсрещната страна като групова квитанция за изпратените до този момент пакети от прозореца. Ако едната страна няма данни за предаване, тя потвърждава приетия пакет чрез управляващ пакет RR (Receive Ready), съдържащ номер P(R). Скоростта на предаването се регулира от приемащата страна, която изпраща управляващ пакет RNR (Receive Not Ready), с който се сигнализира, че пакетите са получени, но повече не могат да се приемат от приемащата страна.

Контролът на грешките се заключава във възстановяване на неполучени пакети. За всеки неполучен пакет се връща специален управляващ пакет REJ. Предаващата страна повторно предава неприетия пакет. В мрежовия слой на стандарт X. 25 липсва същинска CRC – проверка за грешки в получените пакети. Такава проверка се извършва за всеки получен кадър в каналния слой от протокола LAPB.

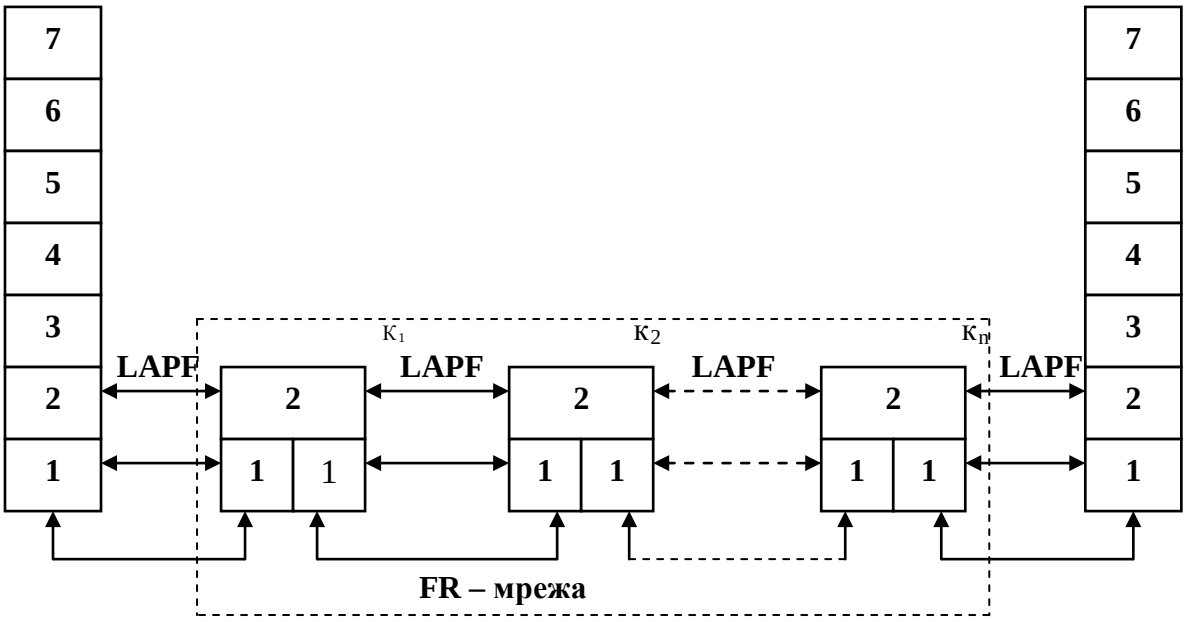
5.2. Стандарт FRAME RELAY

Словосъчетанието Frame Relay (FR) в превод на български език означава „комутация на кадри". Стандарт FR е от ново поколение за достъп до глобална мрежа с комутация на пакети. В началото той е част от стандарт ISDN, но по-късно намира приложение в частните компютърни мрежи. Блоковата схема на стандарта е представена на фиг. 10.4.



Фиг. 10.4. Схема на FR глобална мрежа

FR стандартът може да се разглежда като виртуална наета линия. Абонатите наемат през мрежата постоянно виртуално съединение между два и повече крайни възела. Между възлите информацията се предава във вид на Frame Relay кадри. При наемане на виртуалната линия се заплаща стойността на договорена средна скорост, като на моменти може да се предава и с по-голяма или по-малка скорост от договорената. Стандартът FR е подходящ за пулсиращ трафик, какъвто е трафикът на компютърните комуникации между крайните възли на мрежите. Комуникационният сценарий на стандарта е показан на фиг. 10.5.



Фиг.10.5. Модел на глобална комуникационна мрежа Frame Relay

Стандартът FR е по-добър от X.25. по отношение на скорост на предаване на данните. Проектиран е за работни скорости до 34 Mb/s за Европа и до 45 Mb/s в САЩ и Канада. Закъснението на кадрите в мрежата, изградена по стандарт FR, е в много пъти по-малко в сравнение със стандарта X.25.

Междинните възли в стандарта са еднакви и се наричат FR комутатори (фиг. 10.4). FR комутаторите са развити до второ ниво на отворения модел за комуникации (фиг. 10.5). Функциите на FR комутаторите са свързани основно с определяне на границите на кадрите и с откриване на грешки в тях. Кадрите, приети с грешки, се бракуват, а възстановяването на съобщението е функция на горните слоеве.

FR стандартът предава данните, като ги капсулира в кадри чрез протокола LAPF. Форматът на кадрите е показан на фиг. 10.6.

Флаг	***Заглавна част***	***ДАННИ***	**Контролно поле**	***Флаг***
1	2 ÷ 4	до 1600 байта	2	1

Фиг. 10.6. Формат на LAPF кадър за FR протокол

Флаговете ограничават кадрите с един байт, чиято стойност е 01111110. Заглавната част на кадъра съдържа следната информация:

- Адресна информация за маршрутизация.
- Информация за претоварване на мрежата.

- Информация за приложния процес, чиито данни се предават по мрежата.

Контролното поле от два байта съдържа контролните битове на CRC – кодът, използван за откриване на грешки при предаването.

Стандартът FR използва само постоянни виртуални съединения (PVC). Всяко PVC съединение е с фиксиран маршрут между два крайни възела. PVC съединенията се специфицират с 10-битов номер в заглавната част. Позволени са до 1024 съединения по една физическа линия за достъп до мрежата. От тях 1000 са за потребителите, а останалите 24 се използват за управлението на комуникационната мрежа. Когато заглавната част на кадъра се състои от четири байта, броят на съединенията, които могат да се реализират, е много повече.

Междинните възли в мрежата бракуват кадри само в два случая:

- Когато кадърът е приет с грешка.
- Когато кадърът не може да се съхрани поради препълване буфера на комутатора.

При заявка за PVC съединение през мрежа FR доставчикът и абонатът се договарят за три параметъра:

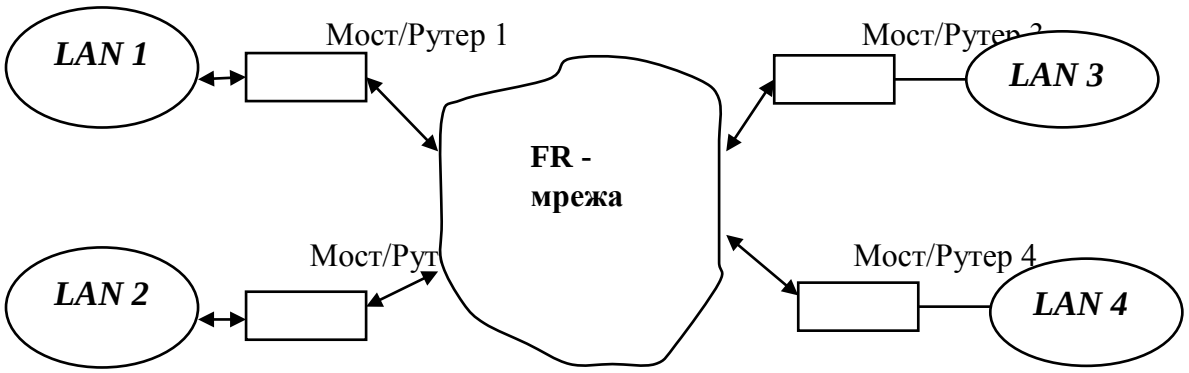
- T_c – продължителност на интервал от общото време за комуникация.
- B_c – брой на байтове, доставени за време T_c.
- B_e – брой на байтове, доставени след доставените B_c за време T_c .

Средната скорост за предаване на данни CIR (Committed Information Rate) се определя от израза $CIR = B_c/T_c$. С този израз се определя средната скорост, с която абонатът има намерение да предава съобщенията в комуникационната мрежа.

С отношението $(B_c + B_e)/T_c$ може да се определи максималната скорост на предаване на данни. Когато FR мрежата не е натоварена, скоростта на предаване расте, обратно, ако е натоварена – скоростта намалява. Този метод на регулиране на скоростта намалява вероятността за задръствания в мрежата.

Стандартът FR, както е показано на фиг. 10.7, се използва за:

- свързване на локални компютърни мрежи;
- за глобални мрежи, при които всички абонати не предават данни едновременно с максималната си скорост;
- като средство за достъп до ATM мрежи.

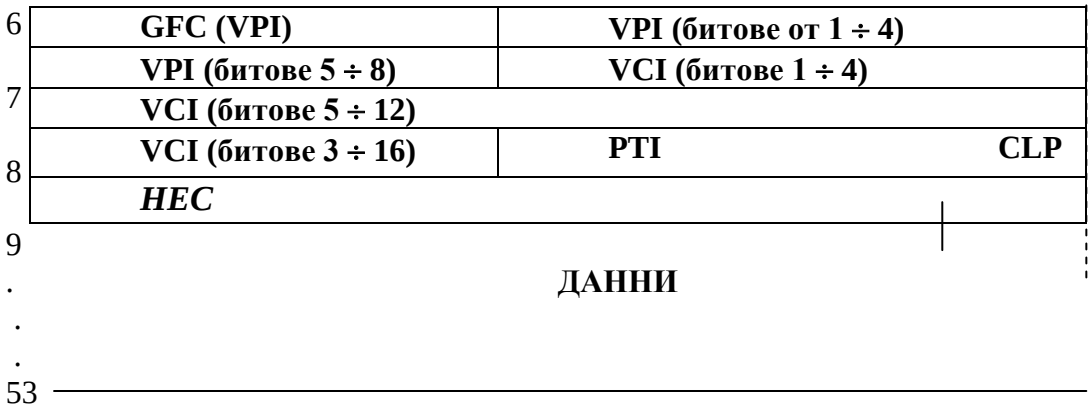


Фиг. 10.7. Приложение на FR мрежа за свързване на LAN

Стандартът FR е подобрение на стандарта X.25. При него са отчетени по-добрите параметри на оптически комуникационни линии. Недостатък на стандарта Frame Relay е, че е неподходящ за мрежи, при които се изисква гарантирано минимално закъснение на данните.

5.3. Стандарт ATM

Стандартът ATM (Asynchronous Transfer Mode) е създаден от телефонната индустрия. Известен е като стандарт Cell Relay (комутация на клетки). За предаване на данни се използват блокове с фиксирана дължина от 53 байта, наречени клетки.

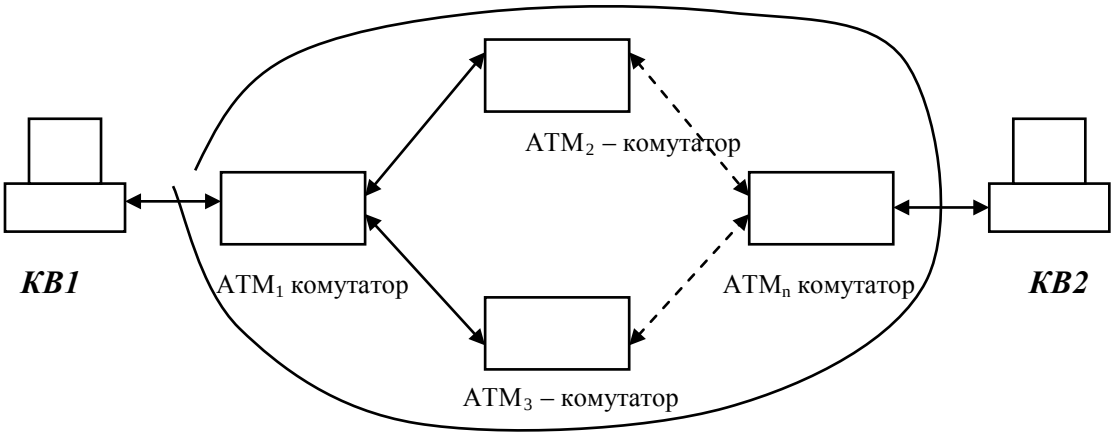


Фиг. 10.7. Структура на ATM клетка

Структурата на ATM клетката е показана на фиг. 10.7. Всяка клетка (фиг. 10.7) се състои от заглавна част, съставена от първите 5 байта, и данни от съобщението – следващите 48 байта. В стандарта ATM се използват два вида клетки:

- Клетки UNI – за интерфейса “потребител – мрежа”.
- Клетки NNI – за комуникация между междинните мрежови възли.

Разликата между тях е в първите четири бита на заглавната част. При UNI клетките това е поле <GFC> и се използва за контрол на потока от данни. При NNI клетките това поле е разширение на полето <VPI> и се използва за адресиране на клетките.

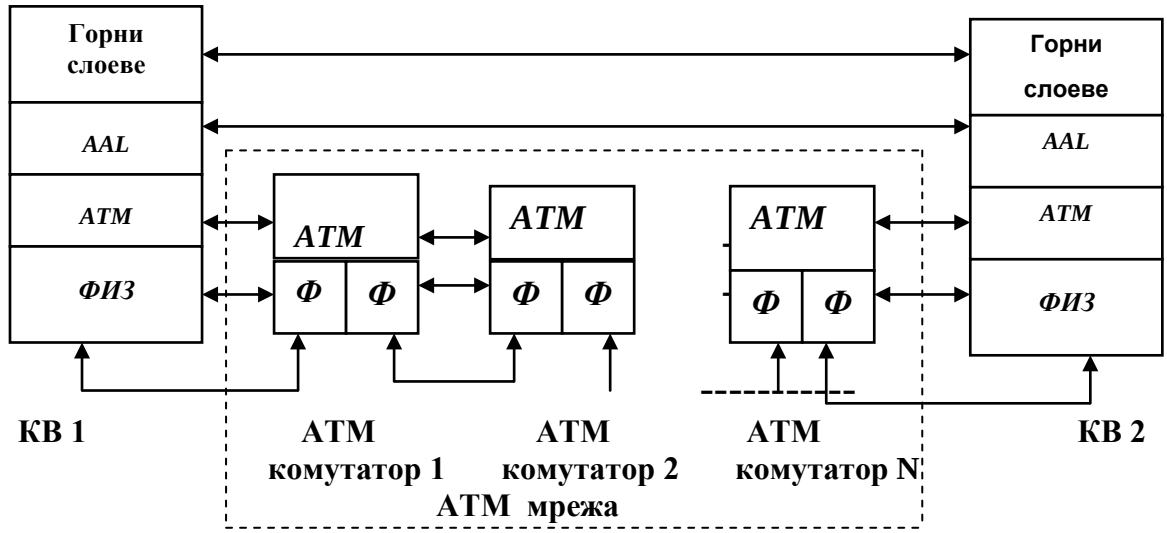


Фиг. 10.8. Схема на ATM мрежа

Стандартът ATM е сроден със стандартите X.25. и FR. Той използва комутация на клетките и мултиплексиране на няколко логически съединения по един физически интерфейс (фиг. 10.8). Използват се по-добрите характеристики на новите цифрови линии за предаване на данни, които осигуряват по-бърза комутация на клетките.

Стандартът ATM постига много по-големи скорости в сравнение с разгледаните до тук. Той използва минимални средства за контрол на грешките и за управление на потока от данни. По този начин е намален процентът на служебните битове в клетките.

Фиксираният размер на клетките допълнително опростява обработката им в комутаторите и позволява постигане на още по-високи скорости. Стандартът постига няколко порядъка по-високи скорости от Frame Relay.



Фиг. 10.9. Модел на ATM мрежа

Предимство на ATM стандарта е, че поддържа анизохронен и изохронен трафик на данните. Поддържа се трафик с постоянна скорост CBR (Constant Bit Rate) и променлива скорост VBR (Variable Bit Rate). Поддържат се трафици както в реално време, така и със закъснение.

Стандартът ATM е част от комуникационния модел B – ISDN, който е различен от OSI и TCP/IP, той заема долните три слоя на модела B – ISDN. Комуникационният модел на стандарта е показан на фиг. 10.9.

5.3.1. Физически слой на стандарт ATM

Физическият слой на ATM се разделя на два подслоя:

- Долен PMD (Physical Medium Dependent) – зависещ от физическата среда.
- Горен подслой TC (Transmission Convergence), който преобразува потока, съставен от ATM клетки, в поток от битове.

Функциите на PMD подслоя са:

- Осъществяване на физически достъп до мрежата с помощта на съединители и кабели.
- Кодиране в линията.
- Синхронизация по битове на приемника и предавателя.
- Други функции съгласно модела OSI.

Основните функции на TC подслоя са:

- Адаптация към рамката на използвания физически стандарт за пренасяне и възстановяване на рамката. Стандартите за пренасяне на ATM клетки са: SDN, PDN, FDDI и Fibre Chance.
- Определяне на границите на отделните клетки в рамката на пренасящия физически стандарт. Използва се механизмът за проверка на контролното CRC поле <HEC> и това, че клетките имат фиксирана дължина 53 байта.
- Генериране на контролно CRC <HEC> (Header Error Check) в заглавната част. Полето <данни> се защитава, ако е необходимо, в по-горния AAL слой.
- "Развързване" на ATM клетките по скорост. Към рамката на пренасящия физически стандарт се добавя "празна" клетка с цел съгласуване скоростта на крайния възел към скоростта, осигурена от пренасящия протокол.
- Обмен на OAM (Operation And Maintenance) клетки за управление, в които има информация за работата на TC подслоя.

5.3.2. ATM – слой на стандарта ATM

ATM слоят е независим от физическата среда. Основните му функции са следните:

- Мултиплексиране и демултиплексиране на ATM клетки, принадлежащи на различни логически (виртуални) съединения в един и същ поток ATM клетки, предавани към физическия слой.
- Комутация на ATM клетки в междинните възли на мрежата.
- Преобразуване на идентификатора на виртуалното съединение (VPI/VCI) при комутация на клетките в междинните възли.
- Добавяне и премахване на заглавна част към или от всяка ATM клетка.
- Осигуряване на допълнителен клас обслужване QOS (Quality Of Service), даващ възможност на потребителите да определят приоритет на своите клетки чрез установяване на специален бит <CLP> (Cell Loss Priority) в заглавната част.
- Създаване на механизъм за управление на потока от данни в интерфейса абонат – мрежа. Използва се полето <GFC> (Generic Flow Control) на заглавната част.

5.3.3. ATM комутация

Комутацята в ATM стандарта се извършва от междинните възли (ATM комутатори). Комутацията се състои в предаване на информация от дадено входящо виртуално или логическо съединение към определено изходящо ATM виртуално съдинение.

ATM виртуалните съединения имат две характеристики:

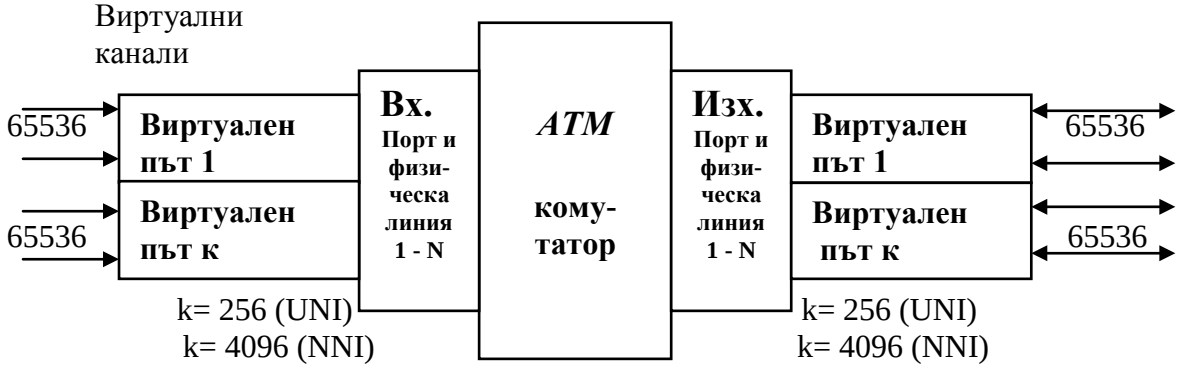
1. **Физическа**, специфицирана чрез номера на физическата линия (номера на порта на ATM комутатора), по която се предават ATM клетките.
2. **Логическа**, определена от два параметъра:
   - VPI (Virtual Path Identifier) – идентификационен номер на виртуалния път.
   - VCI (Virtual Channel Identifier) – идентификационен номер на виртуалния канал.

Виртуалният път е логическа група от виртуални канали, които се комутират и маршрутизират заедно през ATM мрежата. ATM стандартът допуска множество канали по

една и съща физическа линия. Максималният брой на линиите е различен за двата интерфейса:

- $k = 256 = 2^8$ за интерфейса потребител – мрежа – UNI (User – Network Interface);
- $k = 4096 = 2^{12}$ за интерфейса между мрежовите възли NNI (Network – Network Interface).

Номерът на виртуалния път (VPI) е указан в заглавната част на ATM клетката в полето <VPI>, което е с размер осем бита за UNI клетките и дванадесет бита за NNI клетките. Допълнително по всеки виртуален път стандартът ATM позволява да се дефинират до 65536 = 2^{16} виртуални канала.



Фиг. 10.10. Виртуални съединения през ATM комутатор

Номерът на виртуалния канал, към който принадлежи дадена ATM клетка, е указан в 16-битово поле <VCI> на заглавната част. Следователно всяко логическо съединение (виртуално ATM съединение) по дадена физическа линия логически се определя от значението на комбинацията VPI/VCI.

ATM комутаторите (фиг. 10.10) установяват съответствието между входящите физически и логически характеристики на ATM клетките с изходящите логически и физически характеристики, които ATM клетките трябва да приемат на изхода им след комутатора. Всеки ATM комутатор поддържа съответна комутационна таблица, която се актуализира при всяко ново ATM съединение. ATM комутацията може да се извърши едновременно по отношение на VPI и VCI или само на VPI.

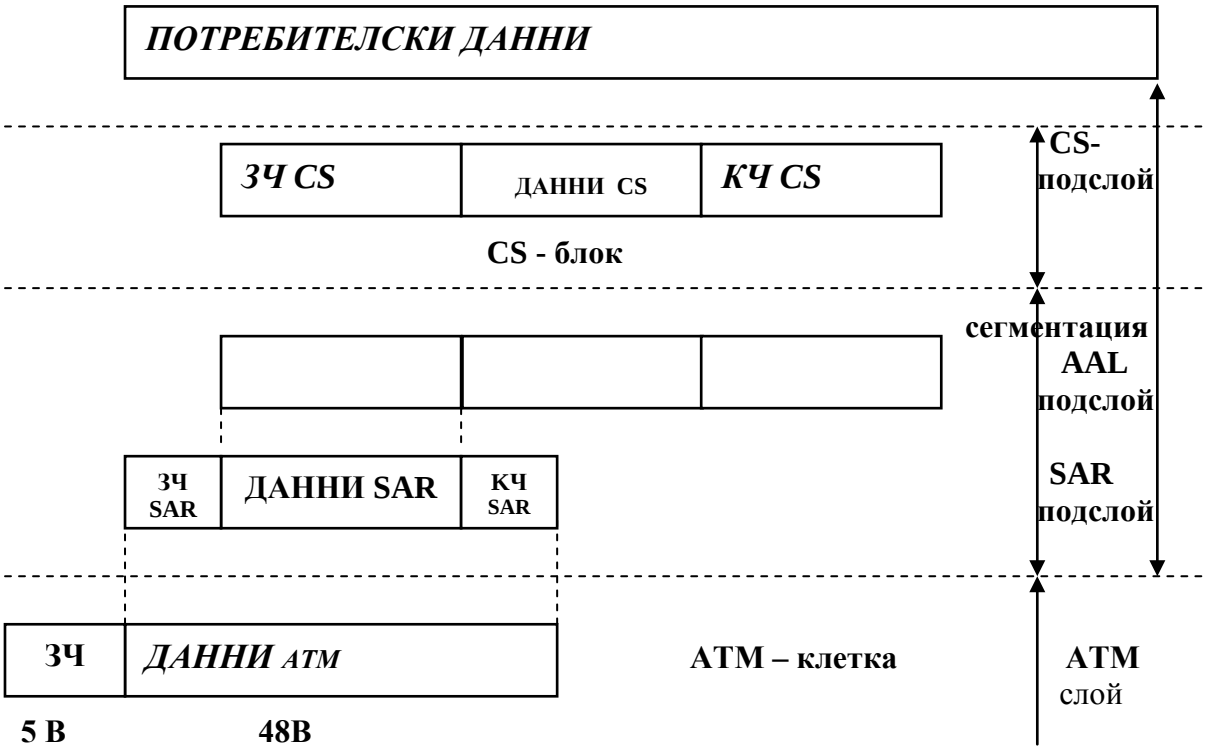
5.3.4. AAL слой на стандарт ATM

AAL слоят (ATM Adaptation Layer) е предназначен да подобри обслужването, предоставено от ATM слоя до изискванията на следващия по-горен слой.

AAL слоят се състои от два подслоя:

- Долен подслой SAR (Segmentation And Reassembly).
- Горен подслой CS (Convergence Sublayer) – за конвергенция.

Фрагментирането на съобщенията в ATM клетките е показано на фиг. 10.11.



Фиг. 10.11. Капсулация на потребителска информация в АТМ клетки

Основната задача на SAR подслоя е сегментация на информацията от горния CS подслой на отделни SAR блокове с размер, подходящ за вмъкване в полето <данни> на АТМ клетките. Този слой изпълнява и обратната задача при приемане – десегментация.

CS подслоят извършва конвергиране на потребителския информационен поток от CS блокове с формати, съответстващи на пет вида трафик.

Потребителският информационен поток от CS блокове може да бъде един от следните пет вида трафик:

- Трафик в реално време с постоянна скорост на предаване – протокол AAL 1.
- Трафик в реално време с променлива скорост на предаване на данни – протокол AAL 2.
- Трафик от пакети, предавани по предварително установено съединение – протокол AAL 3.
- Трафик от дейтаграми, предавани без установяване на съединение между абонатите – протокол AAL 4.
- IP пакети – протокол AAL 5.

5.4. Стандарт ISDN

В стандарта ISDN (Integrated Service Digital Network) е описана цифрова мрежа с интеграция на услугите. Осигурява се пренасяне в цифров вид на: компютърни данни, глас, видеоинформация, факсимилна и аудиоинформация [25].

Развитието и внедряването на концепцията за ISDN се разглежда като развитие и внедряване на нова информационна технология, интегрираща в себе си двата най-важни за комуникационната техника процеса – предаване на съобщенията и тяхната комутация. Стандартът ISDN е технологията, която решава проблемите, породени от интензивното развитие на комуникациите в информационното общество.

Появата и развитието на стандарта ISDN е обусловено от:

- Нарастването на обема на дискретната информация, предавана по различните комуникационни канали.
- Предимствата на цифровите методи за предаване, обработка и комутация.
- Достиженията в областта на цифровите многоканални системи.

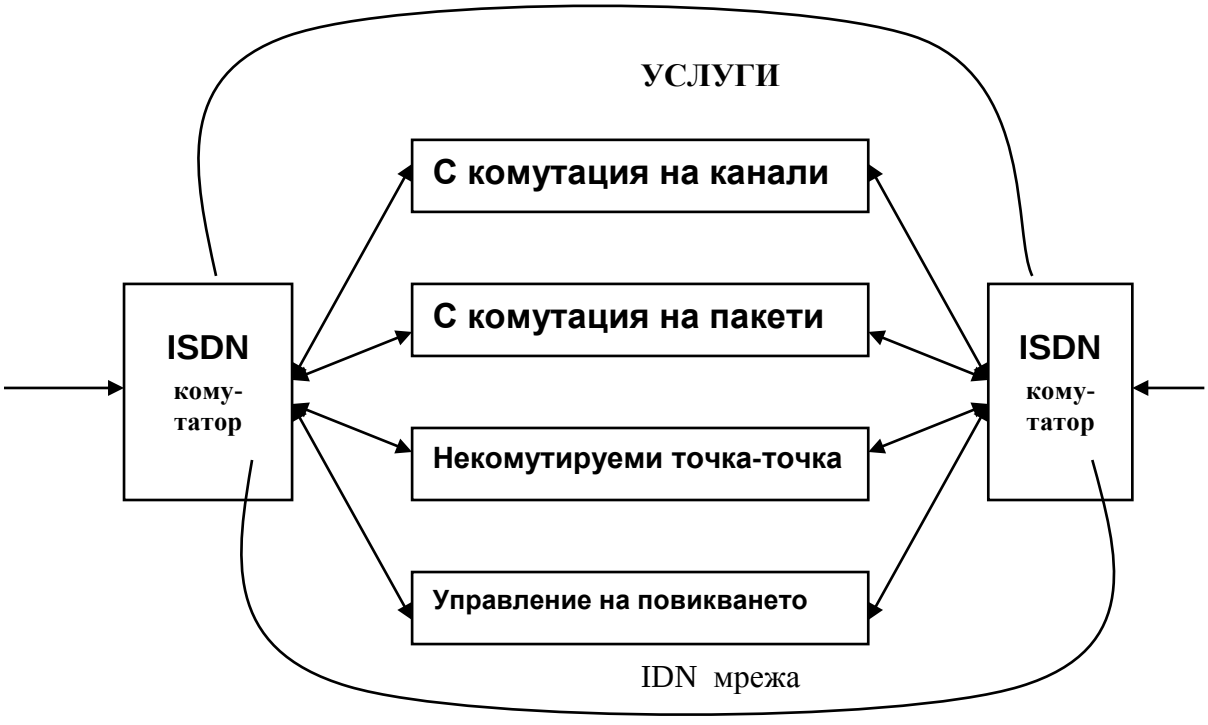
Техническата база на ISDN са многоканалните системи с временно уплътняване на каналите и цифровите схеми за комутация. Използвани са достиженията в областта на оптическите връзки и елементната база, позволяващи достигане на големи магистрални скорости за предаване на данни. Това позволява интегриране на всички видове връзки в широколентови комуникации.

Стандартът ISDN се развива на базата на цифровата телефонна мрежа IDN (Integrated Digital Network). Тази мрежа пренася глас в цифров вид и използва стандарта X.25. с комутация на пакети – фиг. 10.12.

Услугите на ISDN мрежата се делят основно на три вида:

1. **Преносни услуги**, които се използват за следното:
   - Пренасяне на глас, видео- и аудиоинформация по комутируеми канали със скорост 64 Kb/s (B-канали).
   - Предоставяне на цифрови комутируеми канали (H-канали) с по-високи скорости на предаване, кратни на 64 kbps.
   - Пренасяне на данни по виртуални съединения с X.25. комутация на пакети.
   - Пренасяне на данни във вид на дейтаграми без установяване на съединение.

Стандартите за реализиране на тези услуги покриват функциите и протоколите на долните три слоя на отворения модел за комуникации.



Фиг. 10.12. Конфигурация на ISDN мрежа

2. **Телеуслуги**. Тези услуги са за комуникация от абонат до абонат. Обхващат се всички слоеве на OSI модела и се заключават в следното:

- ISDN телефон – високо качество, добро отношение сигнал/ шум, използва се канал с лента 3100 Hz и 7000 Hz за предаване на стереозвук и провеждане на конферентни разговори.
- ISDN телетекст – това е протокол за предаване на буквено-цифрова информация – една страница формат А 4 се предава за по-малко от 1 s при скорост 64 Kbps.
- ISDN телефакс – страница с формат А 4 обикновен телефакс предава за повече от 20 s, а с ISDN телефакса – за 3 s .
- ISDN видеотекст – използва се за търсене на информация, обучение, игри, пазаруване, резервация на билети и други.
- Видеотелефон – за предаване на глас и движещо се изображение, използва се подходяща разделителна способност и компресия.
- Специални ISDN услуги – това са телеграми за пожар, бедствие, грабеж и телеметрия за дистанционно отчитане и управление на промишлени процеси.

3. **Допълнителни видове услуги**. Това са услуги, чрез които се подобрява качеството на обслужване на абонатите в комуникациите, като:

- Изчакване на зает абонат при повикване.
- Индикация на номера на викащия абонат.
- Регистрация на входящи повиквания.
- Прехвърляне на повиквания.
- Бързо избиране на абонат.
- Провеждане на конферентни разговори.
- Сигнализация за текущо таксуване при разговор.

5.5. СТАНДАРТ B – ISDN

Стандартът B – ISDN осигурява интерфейс за скорост на предаване на данни до 622 Mb/s с възможност за увеличаване на скоростта в бъдеще. Стандартът поддържа комутируеми и постоянни съединения от типа “точка – точка” и “точка – много точки”. Допълнително се осигуряват и услугите:

1. **Разговорни услуги** – в реално време „от край до край” по двупосочни и еднопосочни комуникационни канали:
   - Предаване на анимирани изображения, съпроводени със звук.
   - Предаване на звук.
   - Висикоскоростно предаване на цифрови данни.
   - Висикоскоростно предаване на документи.

2. **Съобщителни услуги** – извършват се в нереално време, чрез комутация на съобщения и пощенски кутии.

3. **Услуги за извличане на различна информация от мрежата** – видеотекст, телетекст, реклами, справки.

4. **Разпръскващи услуги** – от типа "точка – много точки" за разпространение на документи, периодичен печат, книги, видеоинформация, телевизионни програми.

Характерно за стандарта B – ISDN е, че използваните комуникационни линии са основно влакнесто-оптични. Връзките между междинните пунктове (комутатори) са изпълнени по стандарт с влакнесто-оптични линии.

Стандартът B – ISDN предлага три вида скорости за предаване:

- Пълнодуплексна скорост от 155,2 Mbps.
- Асиметрична услуга на скорост 155,2 Mbps от абоната към мрежата и 622, 08 Mb/s в обратна посока.
- Пълнодуплексна скорост от 622,08 Mb/s – ползва се от доставчици на видеоуслуги.

Под управление на ISDN се разбира процесът на привеждане и поддържане на компютърната мрежа в състояние, при което функционирането й е оптимално. Оптимизирането се извършва по избрания критерий с отчитане на съответните ограничения, чрез избор на управляващи въздействия от множество възможни.

Системата за управление на ISDN представлява съвкупност от програмнотехнически средства, предназначени за изграждане и контрол на съединения, за приемане, натрупване, предаване и обработка на информация.

Под структура на системата за управление на ISDN се разбира съвкупността от отделните й подсистеми и връзките между тях, разглеждани в процеса на взаимодействие с управлявания обект.

В стандарта ISDN могат да се отделят четири основни нива на управление [25]:

1. Поддържане в изправно (работно) състояние на отделните програмнотехнически средства, когато обекти за управление са средствата, изграждащи мрежата. Цел на управлението е осигуряването с различни методи (въвеждане на излишество, дублиране, резервиране, тестване и т.н.) на зададените параметри за надеждност на мрежата.

2. Управление на доставката на съобщенията на зададения адрес, когато обекти на управлението са комутационните системи на крайните възли, а **основната цел на управлението се явяват изборът на път в комутационната система, създаване на маршрут за предаване в съответствие с адреса и удовлетворяване на някои допълнителни изисквания (приоритет, времето за доставка, достоверност и т.н.).** На това ниво се извършва и управлението на комутацията. В междинните възли с програмно управление, използвани в ISDN, е възможна реализацията на адаптивни алгоритми, способни да реагират на изменящите се параметри на входящите и изходящите потоци, както и да извършват оценка на състоянието на комутационната система на възлите**.**

3. Управляване разпределението на комуникационните канали и регулиране (ограничаване) интензивността на потоците потребителска информация, когато обекти на управление се явяват крос-системите, а основна цел – разпределение и преразпределение на каналите между вторичните мрежи, създаване на сноп от прави канали и изработване на алгоритми за удовлетворяване изискванията за доставка на информация при изменения в мрежата или в интензивността на потоците. С други думи, на това ниво се осъществява управление на предаваната информация, заключаващо се в управление на интензивността на потоците и маршрутизацията им.

4. Комплексно управление на ISDN като технико-икономическа система, включващо задачите по административното управление, управление на

експерименталните изследвания и мрежовите измервания, които с отчитане сложността на ISDN като обект за управление са автоматизирани.

Тъй като мрежите ISDN са интегрални, то функциите, за които те са предназначени, са интегрирали в себе си много от функциите на хомогенните мрежи. Освен това, паралелно с развитието на интегралните мрежи възниква задачата за осигуряване на взаимодействието им с компютърните мрежи, поради което управлението на процесите за обмен на информация в ISDN е целесъобразно да се организира на базата на концепцията и стандартите, приети за съществуващите в момента мрежи. Общоприет модел за изграждане на комуникационни мрежи, както и на стандарта ISDN, е **OSI моделът.**

Методите и алгоритмите за комутация, маршрутизация и ограничаване на потоците в ISDN мрежата се реализират в протоколите на **каналния, мрежовия и транспортния** слой. От тази гледна точка задачата за управление на процесите на обмен на информация в ISDN се превръща в задача за избор на оптимални по отношение на някакъв избран критерий методи за маршрутизация и ограничаване на интензивността на потоците в мрежа със зададена топологична структура, при съответстващи ограничения. От друга страна, процесът на обмен на информация в стандарт ISDN е тясно свързан с използваните в мрежата методи на комутация. Това налага по-подробното разглеждане на съществуващите методи за комутация с цел разкриването на възможностите за използването им в мрежата ISDN.

Понастоящем в съществуващите компютърни мрежи се прилагат основно два метода за комутация:

- Комутация на каналите (КК).
- Комутация на съобщенията или пакетите (КС/КП).

Методът с КП се прилага в две разновидности:

1. Комутация на дейтаграмите, при която всеки пакет от дадено съобщение получава адреса на получателя и може да се придвижва по маршрут, често пъти различен от маршрутите на другите пакети от същото съобщение.

2. Комутация на виртуални канали (ВК)), при която всички пакети от едно съобщение преминават по един и същи маршрут, определян във фазата на установяване на виртуалния канал.

Достойнствата и недостатъците на методите КК и КС (КП) са изследвани многократно. По-широко приложение в КМ последните години е намерил методът с КП. Този метод има много предимства, но и много недостатъци, поради което в ISDN се използва и методът с КК. Изборът на метода за комутация в съществуващите КМ се определя, като се изходи от особеностите на предаваните съобщения. За съжаление, такъв подход за ISDN се оказва невъзможен поради разнообразието на информационните потоци в нея.

Стремежът за преодоляването на "чистите" методи за комутация е довел до появяването на голям брой методи за хибридна и адаптивна комутация, от които най-перспективни от гледна точка на използване на каналите и икономическа ефективност са **методите за адаптивна комутация**. При тези методи се извършва динамично разпределяне на пропускателната способност на каналите в зависимост от състоянието на мрежата в даден момент. Изследванията показват, че използването на хибридните и адаптивните принципи на комутация дава възможност за постигането на висока ефективност при функционирането на цифровите мрежи, като осигуряват в същото време необходимото качество на обслужването на потребителите. В цифровите мрежи, характеризиращи се с голямото си разнообразие на предаваната информация и специфичните изисквания към качеството на предаване, използването на методите за хибридна и адаптивна комутация се превръща в необходимост.

Управлението на процеса на обмен на информация в ISDN се характеризира със следните особености:

- Мрежата, по която се предава служебна информация за управление на обектите, притежава същите характеристики, каквито и цифровата мрежа, в която се извършва обмен на потребителска информация, така че в общия случай тези мрежи са еднакви.
- Елементите на системата за управление са териториално отдалечени един от друг. Следователно информацията за състоянието на обектите винаги ще закъснява и ще отразява минало състояние на процеса на обмен на съобщения. С други думи, решението за управление ще се приема на основата на данните за минало състояние на процеса.
- Пропускателната способност на мрежата ISDN, представляваща количеството информация (бит/с), предавано едновременно между всички крайни възли за единица време, при известни условия може да бъде по-малка от производителността на източниците.
- Непрекъснато изменение на работните условия на ISDN като случайни изменения в интензивността и направленията на входящите потоци случайни грешки в предаваната цифрова информация в каналите.
- Случайни изменения в топологичната структура вследствие повреди в крайните възли или каналите за предаване на данни.
- Еволюционни изменения в топологичната структура, т. е. добавянето на нови възли, канали и т.н.

Задачата за управлението на обмена на съобщения обикновено се свежда до задача за управление на потоците в мрежата. Задачата за управление на потоците се заключава в ограничаване на интензивността им с оглед предотвратяване на претоварването в мрежата (водещо до блокиране на работата й) и в разпределение на потоците (маршрутизация). В цифровите мрежи от различен тип (в това число и ISDN) се използват две групи методи за управление интензивността на потоците:

- централизирани
- децентрализирани.

При централизираните методи необходимата обобщена служебна информация за състоянието на мрежата се набира от централния управляващ възел от междинните възли, към които се изпращат съответни команди.

Децентрализираните методи се разделят на локални и глобални методи. Децентрализираните методи са получили по-голямо приложение. При тях ограничаването на потоците може да стане или като се ограничава натоварването на междинните възли, или като се ограничава производителността на самия информационен източник.

При локалните методи за управление решение за ограничаване на потоците от данни взема отделният възел. Глобалните методи се реализират в два варианта: изоритмично управление, при което общият брой пакети в мрежата се поддържа постоянен, и с непрекъснато управление, при което се ограничават потоците на всяка двойка взаимодействащи си възли.

Управлението на разпределението на потоците (маршрутизацията) се свежда до управление структурата на мрежата, което се реализира или чрез изменение капацитета на каналите, или чрез преразпределянето им. Използват се три групи методи:

- Методи за преразпределяне на маршрутите, заключаващи се в определяне на реда за избора на обходните маршрути (свързано е с изменения в така наречения план за разпределение на информацията) или в управление на конфигурацията на маршрута.

- Методи, свързани с управлението на броя на допустимите обходни маршрути.
- Методи за управление на режима на комутация на каналите на избрания маршрут.

Планът за разпределение на протоколните единици определя реда за избор на маршрут за движение на потоците от данни. Задава се най-често във вид на маршрутни таблици за всеки междинен възел. Съществува голямо разнообразие от методи за избор на маршрутите, използвани в цифровите мрежи от различен тип. В качеството на класификационни признаци най-често се използват:

- Насочеността на потоците информация.
- Начинът на отчитане на текущото състояние на мрежата.
- Начинът на разпределение на информацията по възможните маршрути.
- Централизация на управлението.
- Използваната информация за избора на маршрута.
- Начинът на получаване на тази информация.

В цифровите мрежи най-широко приложение са намерили адаптивните методи и методите за зонова маршрутизация.

Адаптивните методи за маршрутизация се характеризират с това, че нямат твърдо установени маршрутни таблици към междинните възли. На основата на качествен анализ на методите за адаптивна маршрутизация, използвани в действащите възли, са определени основните параметри на тези методи, определящи способността на процеса на обмен на информация да се адаптира към стохастичните изменения на условията в мрежите. Такива параметри са:

- **Част от служебната информация**, необходима за нормалната работа на алгоритмите за маршрутизация.
- **Глобалност**, под което се разбира свойството на тази информация да отразява състоянието на определен участък от мрежата или на цялата мрежа.
- **Актуалност** на информацията.

Именно тези характеристики на служебната информация, на базата на която функционират алгоритмите за маршрутизация в цифровите мрежи за информационен обмен, определят нейната адаптация към отказите на каналите и междинните възли, към претоварването и блокировката на комуникационната мрежа.

Анализът на методите за маршрутизация, многочислените изследвания, както и опитът от експлоатацията на съществуващите компютърни мрежи показват, че нито един от методите за маршрутизация не може да осигури желаната адаптация напълно. Ето защо специално за цифровите мрежи са създадени и изследвани комбинирани алгоритми за маршрутизация, осигуряващи компромисно решение на алтернативата глобалност – актуалност на служебната информация, при съответстващи ограничения на частта от съобщения, създаваща допълнителен трафик в стандарта ISDN.

В съответствие с такъв комбиниран подход е разработен конкретен алгоритъм за маршрутизация, наречен **алгоритъм за адаптивна маршрутизация с ограничен избор на изходящите канали.** Маршрутната таблица при този алгоритъм се изгражда на основата на съчетаването на принципите на фиксираните многомаршрутни и локалните адаптивни алгоритми за маршрутизация. Използването на принципите за построяване на многомаршрутни методи за маршрутизация осигурява до известна степен удовлетворително решение на едната страна на алтернативата – **глобалност.** Използването пък на принципите за построяване на локалните адаптивни алгоритми осигурява решението на втората страна на

алтернативата – **актуалността** на служебната информация, т. е. минимизирането на служебния трафик в ISDN.

Приемливи характеристики на служебната управляваща информация в големите мрежи, към които спадат и ISDN, могат да се получат и при използването на методите за **зонова маршрутизация**. Според тези методи цялата територия, обхващана от мрежата, се разбива на зони. Вътре във всяка зона, както и между зоните, се използват отделни адаптивни алгоритми за маршрутизация. Изборът на метода за маршрутизация вътре в зоната и между зоните ще се влияе както от топологичната структура на зоновата и междузоновата мрежа, така и от характеристиките на трафика им. Ако зоните имат централизирана топология, то целесъобразно е използването на централизирано управление. При разпределена структура на зоновите и междузоновите части от мрежите за предпочитане са методите за децентрализирано управление на разпределението на потоците от данни и съобщения в тях.

В общия случай **управлението на процесите на обмена на съобщения в стандарта ISDN може да бъде сведено до управление на маршрутизацията,** ако интензивността на входящите в мрежата потоци е сравнително ниска. При увеличаване на интензивността възниква опасност от претоварване на мрежата (макар че локални претоварвания могат да възникват и при ниска интензивност), налагащо ограничаване на потоците съобщения.

По такъв начин **главна задача на системата за управление обмена на информация в транспортната система на стандарта ISDN се явява осигуряването на необходимото качество на обслужване на всички класове потребители.** Постигането на желаното качество на обслужване, при отчитане на влияещите върху него фактори, може да бъде осъществено само ако експлоатация на мрежата се извършва в условията на динамично изменение на някои системни параметри в протоколите на транспортната система. **Необходимото условие за управление на качеството на обслужване е реализацията на комплекс от мрежови средства за измерване и оценка на показателите за качество и съответните средства за управление, явяващи се част от програмното осигуряване на цифровите системи за комутация на възлите.**

Като особеност на управлението на обмена на информация на транспортно ниво в **ISDN** може да се счита принципната възможност за избиране на технологията за предаване на информацията в момента на създаването на логическо съединение в зависимост от състоянието на мрежата. Тази особеност спомага за постигане на желаното качество на обслужване на потребителите.

В качеството на пример и като методологична база за системно мрежово управление може да се разгледа разработената неотдавна архитектура на TMN (Telecommunication Management Network). Характерното за тази архитектура е:

- Изгражда се като система с разпределена интелигентност в отделните си йерархични нива, т. е. представлява симбиоза между положителните страни на централизираната и децентрализираната система за управление.
- За системен хардуер архитектурата TMN ползва съвременни професионални микрокомпютри, устройства за визуализация и специализирани комуникационни процесори, функциониращи под управлението на мощни платформени и мрежови операционни системи.
- Приложният софтуер е реализиран преимуществено на езика **MLL, CHILL, PROTEL, СИ и Паскал.**
- Използване на достиженията на експертните системи за целите на апаратната и програмната диагностика на повредите и отказите.

В структурно отношение базираните на архитектурата на TMN автоматизирани системи за управление на стандарт ISDN (национални и ведомствени) се изграждат основно на две йерархични нива:

- Ниво на мрежов център за управление NMC (Network and Management Centre).
- Ниво на регионалните (доменните, клъстърните) центрове за управление OMC (Operation and Maintenance Centre).

С цел повишаване надеждността на системата за управление на мрежата се препоръчва изграждането на два вида NMC – основен и резервен.

Основните функции, изпълнявани от **OMC центъра,** са следните:

- Регистриране и обработка на алармени съобщения.
- Дистанционно управление на елементите на мрежата.
- Изпращане на агрегирани данни към **NMC центъра.**
- Поддържане на интерфейс към други **OMC**, към съществуващата регионална аналогова обществена телефонна мрежа и към мрежата за връзка с мобилни обекти.

Центърът NMC реализира системния и мрежовия контрол с изпълнението на следните функции:

- Контрол на отказите и повредите в мрежата.
- Конфигуриране и реконфигуриране на мрежата.
- Определяне на разходите за поддръжката и трафиците.
- Динамично адаптивно управление на маршрутизацията на информационните потоци.
- Контрол на работата на системата за сигнализация.
- Експлоатационен контрол.
- Контрол на достъпа до ресурсите на мрежата и др.

Подобен подход на реализиране на автоматизирана система за управление на стандарт **ISDN** използват фирмите **Siemens** и **Ericsson** на базата на цифрови автоматични централи съответно **EWSD** и **AXE (MD – 110).**

Българската телекомуникационна компания (БТК) също използва подобен подход при изграждането на системата за управление на националната мрежа ISDN.

В заключение трябва да се подчертае, че за разглежданите ISDN засега не съществува удовлетворително решение на задачата за управление на информационния обмен. Основна причина за подобно състояние на проблема е отсъствието на единна концепция за развитието на стандарта ISDN, както и липсата на подходящ модел на процеса на управление на обмена на съобщения в стандарт ISDN.

5.6. Изследване на глобалната компютърна мрежа на Шуменския университет

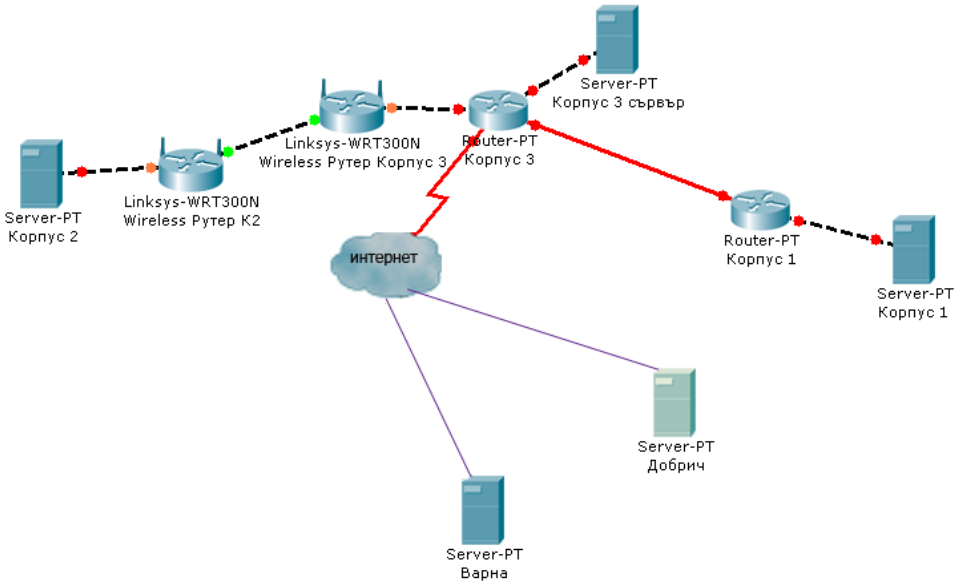
Регионалното разположение на Шуменския университет „Епископ Константин Преславски” предполага изграждане на мащабна компютърна мрежа. Глобалната компютърна мрежа на Шуменския университет е представена на фиг. 10.13. Тя е хибридна мрежа с физическа топология тип звезда. Позиционирана е в три сгради в гр. Шумен – Корпус 1 (К1), Корпус 2 (К2) и Корпус 3 (К3), в гр. Варна – Департамент за информация и повишаване квалификацията на учителите (ДИПКУ) и в Педагогическия колеж в гр. Добрич.

Интернет услугите на Университета се осъществяват от доставчик до Корпус 3 по оптичен кабел, посредством комуникационен канал със скорост от 100 Mbit/s. От Корпус 3 трафикът се разпределя между Корпус 1 и Корпус 2. Сградите в гр. Варна и гр. Добрич

ползват услугите на национален интернет доставчик с наета линия по оптичен кабел с гарантирана скорост от 10 Mbit/s.

Комуникацията на Корпус 1 с останалите корпуси се реализира с рутери, които работят със скорост от 1 Gbps. Скоростта за предаване на данни в мрежата на Университета е съобразена с възможния реален трафик от и към корпуса на ректората.

Поради факта, че сградите на Корпус 2 и Корпус 3 са на отстояние малко повече от 2 км и между тях има пряка видимост, връзката между тях е реализирана с радио линк. Използвани са параболични антени с решетъчен рефлектор. Антените са с тясна диаграма на насочено действие и работят надеждно в неблагоприятни атмосферни условия.



Фиг. 10.13. Структура на мрежата на Шуменския университет

Здравата монтажна конструкция на антените елиминира влиянието на силни ветрове, в резултат на което комуникационният канал между сградите функционира устойчиво и с голяма надеждност. Максималната скорост за предаване на данни между Корпус 2 и Корпус 3 достига до 100 Mbit/s.

Корпус 1 е разположен на приблизително 350 метра разстояние от Корпус 3 и между двата корпуса е изградена оптична комуникационна линия с 4 влакна.

Изследванията и анализът на глобалната компютърна мрежа на ШУ са извършени с помощта на специализираната програма IPERF.

Програмата е често използван инструмент за тестване параметрите на глобални компютърни мрежи. Кодът на програмата е отворен и е написан на алгоритмичния език C ++. Тази програма може да създава TCP и UDP потоци от данни за обмен на съобщения между абонати на компютърната мрежа. Администраторите на мрежата могат да контролират следните параметри:

- измерване пропускателната способност на мрежата;
- измерване на производителността на компютърната мрежа;
- измерване на честотната лента на комуникационните канали;
- установяване качеството на връзката между абонатите.

Програмният продукт е универсална среда за измерване параметрите на големи компютърни мрежи. Кодът на програмата е отворен и може да се допълва с модули по желание на изследователя. Работи под управление на операционните системи Linux, Unix и

Windows. Предлага се и приложение, написано на Java, което може да бъде асоциирано с програмата и да се предостави графична визуализация на резултатите, получени от проведеното изследване.

В симулацията на мрежовата връзка се разграничават два хоста, с които програмата работи. Единият от хостовете трябва да бъде настроен като клиент, а другият като сървър.

Качеството на връзка между хостовете може да бъде тествано както следва:

- Латентност (време за реакция или RTT) – измерва се с командата Ping.
- Jitter (латентност вариация) – измерва се с Iperf UDP тест.
- Загуба на пакети – измерва се с Iperf UDP тест.

Честотната лента на комуникационните канали се измерва чрез тестове за проверка на протокола TCP. Разликата между протокола TCP (протокол за контрол на предаването) и UDP (User Datagram Protocol) е, че TCP използват процедури, за да се провери достоверността на получените пакети в приемника, докато при UDP пакетите се изпращат и приемат без никакви проверки. За сметка на занижения контрол предимство на протокола UDP е по-голямата скорост на предаване на съобщения от протокола TCP.

Програмният пакет IPERF предоставя възможности на потребителя да зададе различни параметри, които могат да се използват за тестване, оптимизация или настройка на компютърната мрежа. Създадена е възможност за симулиране на функционални клиенти и сървъри. Има възможност за измерване на пропускателната способност на канала между абонати от двата края на мрежата по еднопосочни или двупосочни канали.

Фиг. 10.14. Схема за свързване на клиент и сървър през Интернет

Когато се провежда изследване за тестване на UDP капацитет, програмният пакет позволява на потребителя да уточни размера на дейтаграмата (пакета) и предоставя резултати за пропускателната способност на мрежата и загуба на пакети .

Примерна схема за провеждане на изследване параметрите на компютърна мрежа с помощта на програмен пакет IPERF е представена на фиг. 10.14. На фигурата е показана постановка, на която Linux машината се използва като Iperf клиент, а Windows машината като Iperf сървър. Възможно е да се свържат и две машини под управление на операционни системи Linux.

При тестване на компютърната мрежа с пакета Iperf тестове е необходимо да се дефинират следните аргументи:

- b – формат на данните;
- r – двупосочна честотна лента;
- d – едновременна двупосочна честотна лента;

- w – размер на TCP прозореца;
- p, t, I – порт, време и интервал;
- u, -b UDP – тестове, настройки на трафика на информация;
- m – визуализиране максималния размер на сегментите;
- M – настройка на максималния размер на сегментите;
- P – паралелни тестове;
- h – помощна информация.

Когато не се дефинират параметрите на мрежата и методът за комуникация, програмният пакет приема средата по подразбиране, като за целта параметрите са зададени таблично.

Анализ на трафика на съобщения между сградите на ШУ е проведен и представен графично. По-нататък е представен кодът на програмата за изследване на трафика на данните между К1 и останалите корпуси на Университета.

```
#> iperf –c fpi.shu-bg.net
------------------------------------------------------------------------------------------------------
Client connecting to fpi.shu-bg.net, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------------------------------------------------
[    )] local 194.141.47.2 port 51669 connected with 194.141.47.66 port 5001
[ ID] Interval              Transfer              Bandwith
[    )] 0,0-10,0 sec        622 MBytes            88,2 Mbits/sec

#> iperf –c fmi.shu-bg.net
------------------------------------------------------------------------------------------------------
Client connecting to fmi.shu-bg.net, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------------------------------------------------
[    )] local 194.141.47.2 port 36368 connected with 194.141.47.130 port 5001
[ ID] Interval              Transfer              Bandwith
[    )] 0,0-10,0 sec        105 MBytes            522  Mbits/sec

#> iperf –c 194.141.78.1
------------------------------------------------------------------------------------------------------
Client connecting to 194.141.78.1, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------------------------------------------------
[    )] local 194.141.47.2 port 36368 connected with 194.141.78.1 port 5001
[ ID] Interval              Transfer              Bandwith
[    )] 0,0-10,1 sec        5,88 MBytes           4,90  Mbits/sec
```

Обработените резултати от изследването на глобалната компютърна мрежа на ШУ с програмния пакет Iperf са представени графично на фиг. 10.15 до фиг. 10.20.

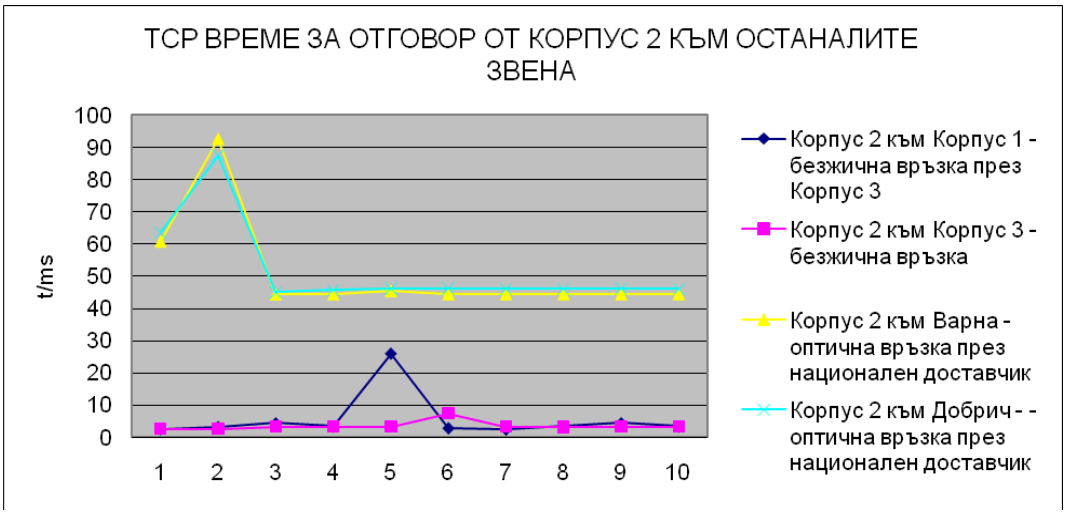
Проведени са симулации и на обмен на съобщения, както следва:

- Скорост за трансфер на данни между сградите на ШУ.
- Трансфер на данни между сградите на ШУ за интервал от 10 s.
- TCP време за отговор от Корпус 2 към другите звена.
- TCP време за отговор от Корпус 1 към другите звена.
- TCP време за отговор от Корпус 3 към другите звена.
- TCP време за отговор от Варна към другите звена.

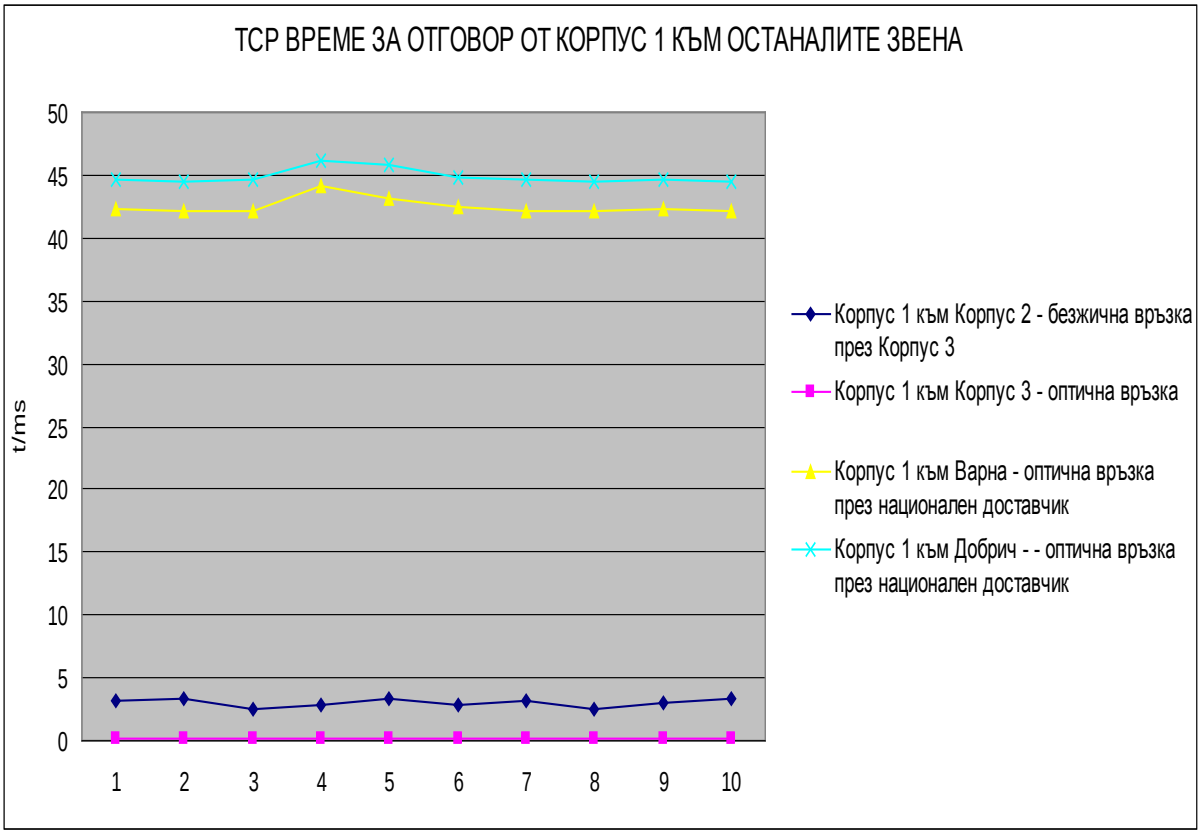
Фиг. 10.15. Скорост за трансфер на данни между сградите

Фиг. 10.16. Трансфер на данни между сградите

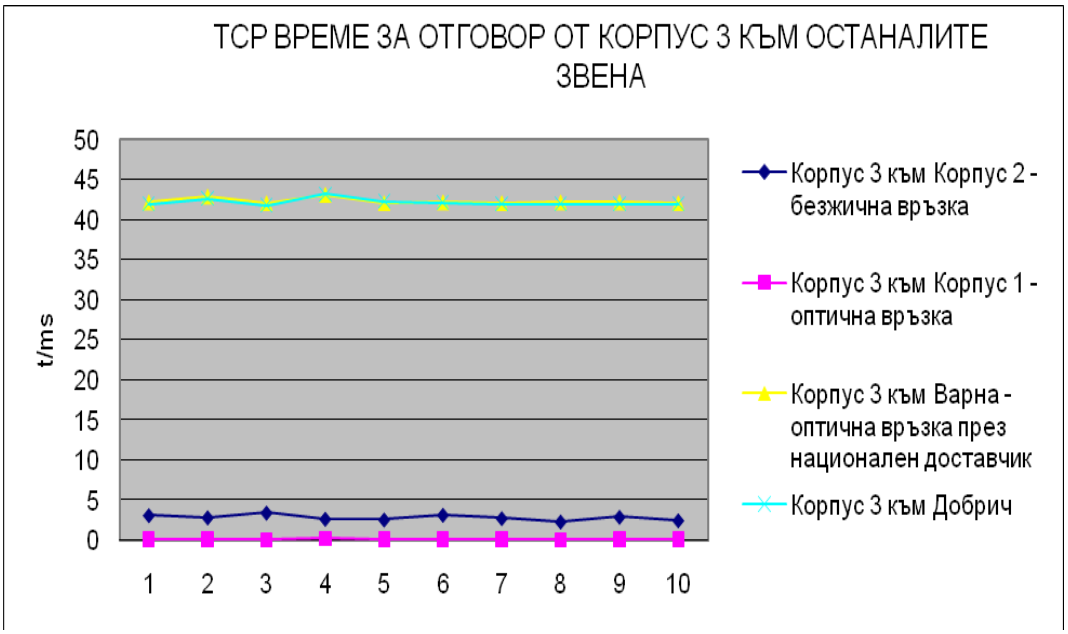
При изследване на протокола TCP е измерено времето за отговор между корпусите на ШУ. Приложен е тест за определяне минималното, средното и максималното време, необходимо за завършване на TCP трансакция. Използват се 10 итерации по 100 байта в една рамка.



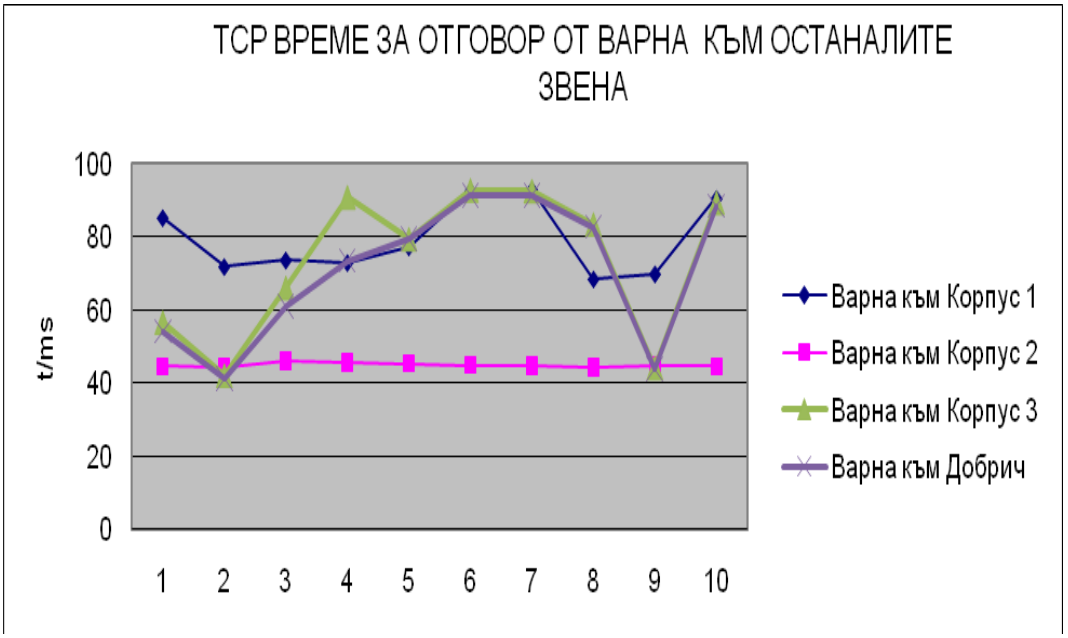
Фиг. 10.17. TCP време за отговор от Корпус 2 към другите звена



Фиг. 10.18. TCP време за отговор от Корпус 1 към другите звена



Фиг. 10.19. TCP време за отговор от Корпус 3 към другите звена



Фиг. 10.20. TCP време за отговор от Варна към другите звена

В резултат на проведените изследвания могат да се направят следните изводи:

1. Програмният пакет IPERF е подходящ за установяване параметрите на ведомствени комуникационни мрежи.

2. Трафикът между корпусите на Шуменския университет може да се реализира със скорости за предаване на данни както следва:

- Максимална скорост между К3 и К1 – 598 Mbitps.
- Максимална скорост между К3 и К2 – 90,8 Mbitps.
- Максимална скорост между К3 и Колеж Добрич – 8,44 Mbitps.
- Максимална скорост между К3 и ДИПКУ Варна – 8,89 Mbitps.

3. Максималното време за закъснение на данните (40 до 80 ms) се реализира при предаване на данни от Колежа в Добрич и ДИПКУ Варна до корпусите в гр. Шумен.

4. Времето за закъснение на данните на трафика между корпусите на ШУ в гр. Шумен не превишава 5 ms.

5. Комуникационната мрежа на корпусите в гр. Шумен позволява работа на локалните мрежи в реално време и електронно управление на Университета.

6. Параметрите на наетите линии, ползвани от Департамента в град Варна и Колежа в град Добрич, са съобразени с нуждите на звената, но за електронното управление на деканатите е необходимо привеждане на характеристиките им в съответствие с изискванията на приложния софтуер.

Въпроси за самостоятелна работа

1. Кои са съвременните стандарти за изграждане на глобални компютърни мрежи?
2. Кои методи за комутация са приложени в глобалните компютърни мрежи?
3. Какви методи и алгоритми за маршрутизация се използват в глобалните компютърни мрежи?
4. Кои са основните характеристики на стандарта X.25.?
5. Кои са основните характеристики на стандарта FR?
6. Кои са основните характеристики на стандарта ATM?
7. Направете обосновка на физическия слой на стандарт ATM.
8. Кои са основните характеристики на стандарта ISDN?
9. Направете обосновка на проложението на стандарт ISDN.
10. Направете обосновка на режим виртуално съединение в глобалните компютърни мрежи.

ГЛАВА 6. МЕЖДУМРЕЖОВИ КОМУНИКАЦИИ

При междумрежовите комуникации се налага съгласуване на хетерогенни мрежи, съставени от различни видове работни станции, и сървъри с различни операционни системи, на които са инсталирани различни стекове от мрежови протоколи и приложни програми. Съществуването на множество стандарти и протоколни стекове за изграждане на различни компютърни мрежи налага използване на технически и програмни средства за съгласуване на кодовете и формата на съобщенията. При тези мрежи е необходимо да се реализират два вида съгласувания:

- Съгласуване на нивото на долните слоеве на OSI модела – Internetworking.
- Съгласуване на горните слоеве на OSI модела – Interoperability.

6.1. Съгласуване на компютърните мрежи в долните слоеве на модела

Когато горните слоеве на мрежите използват еднакви протоколи, а долните – различни, между тях се поставят различни устройства за съгласуване обмена на протоколни единици на канално и мрежово ниво. Тези устройства функционират на физическо, канално и мрежово ниво. В съвременните компютърни мрежи се използват устройства като: повторители, концентратори, модеми, мостове, маршрутизатори, мостмаршрутизатори и комутатори.

Повторителят (repeater) е междинен усилвател, разположен между два локални сегмента на компютърната мрежа (фиг. 11.1). Той приема сигналите, възстановява ги по форма и ги усилва до стандартното ниво, с което се увеличава дължината на сегмента на локалната мрежа. Повторителят функционира на нивото на физическия слой на отворения модел за комуникация (OSI). Той е прозрачен за работните станции и сървърите на компютърната мрежа. Повторителите за стандарт IEEE 802.3. Ethernet се произвеждат с повече от един порт, които имат различни интерфейси за свързване с медни проводници и оптически световоди. Основната функция на повторителите е удължаване на кабелните сегменти, свързващи компютри и компютърни мрежи.

Фиг. 11.1. Схема на повторител

Концентраторите функционират само във физическия слой на OSI модела. Тези устройства позволяват лесно включване на допълнителни възли в локалните мрежи. Известни са два вида концентратори:

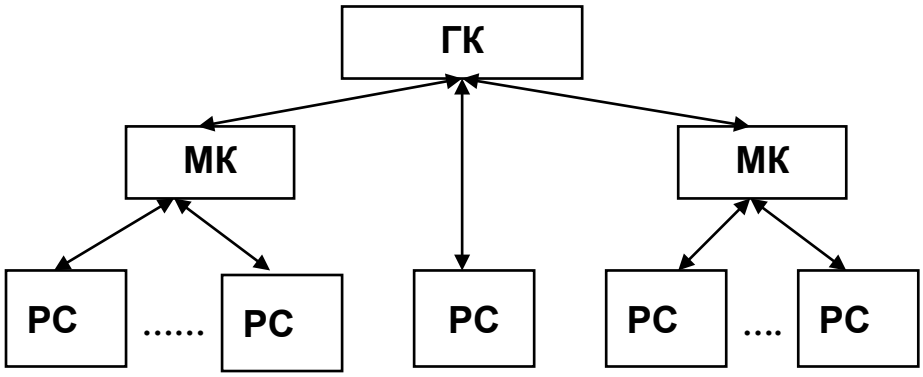
- пасивни концентратори;
- активни концентратори.

Пасивните концентратори разпределят сигналите и съгласуват включените мрежови възли. Активните концентратори освен разделителните функции усилват сигналите и компенсират затихването им по линиите за връзка.

В повечето случаи концентраторите работят като множество повторители. Постъпилите сигнали на някои от входовете се предават на всички изходни портове. Броят на портовете на концентраторите за надолу (down ports) може да бъде 4, 8, 16 и 24.

В локалните компютърни мрежи, изградени по стандартите IEEE 802.3.10 Base T и IEEE 802.12. (100VG – Any LAN), концентраторите се свързват йерархично до три нива за стандарта 10 Base T и до 5 нива за 100VG – Any LAN. Към всеки концентратор може да се включат работни станции, сървъри или други концентратори. Концентраторите се монтират в сградите по един на етаж и по един в стая, като към всеки концентратор се свързват компютрите от мястото, където е разположен.

Стандартът 10 Base T използва физическите топологии "звезда" или "дърво" (фиг. 11.2), като логическата топология е тип "шина". На първо ниво се включва главният концентратор (ГК). Той предава сигналите, постъпили на някой от входовете, към останалите портове. Междинните концентратори (МК) предават сигналите, идващи от долното ниво към горното, както и сигналите, идващи от горното ниво към долното.



Фиг. 11.2. Схема на LAN на две нива с главен и междинни концентратори

За стандарта IEEE 802.12. (100VG – Any LAN) концентраторите изпълняват и функции, типични за MAC подслоя на отворения модел, като осигуряване на приоритетен достъп до комуникационната среда, при заявка от краен възел.

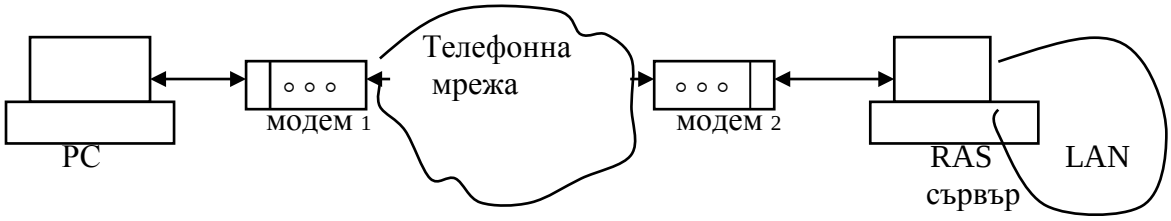
Стандартът 802.5. (Token Ring) изисква използване на концентратори тип MAU, които позволяват включване на нови възли в мрежата и изключване на повредени възли с цел възстановяване на кръга. Освен че концентраторите са център на локалните компютърни мрежи, чрез тях се разширяват и възможностите за реконфигурация на мрежата, като към тях се включват мостове, комутиращи и маршрутизиращи възли.

Комутаторът Super Stack II на фирма 3COM поддържа две скорости 10 Mb/s и 100 Mb/s. Скоростта, с която работи насрещният възел, се разпознава автоматично, когато този комутатор притежава възможности за междумрежова комуникация.

Модемът (Modem) е комуникационно устройство за предаване и приемане на цифрови данни през аналогови линии. В компютърните мрежи се използва за отдалечен достъп на потребители до локални и глобални компютърни мрежи.

Отдалеченият достъп до локалната компютърна мрежа се управлява от специален RAZ сървър (Remote Access Server), който позволява едновременно включване на 256 отдалечени

потребители към локална мрежа под управление на мрежовата операционна система Windows NT (фиг. 11.3).



Фиг. 11.3. Отдалечен достъп на PC до LAN чрез модем и телефонна линия

Потребителите получават отдалечен достъп до локалната компютърна мрежа чрез Internet, като се ползва протоколът PPTP (Point to Point Tunneling Protocol). Този протокол капсулира данните на протоколите IP и IPX и създава условия те да се пренесат през тунел по глобалната компютърна мрежа Internet.

На фиг. 11.4 е показан начинът на свързване на два отдалечени компютъра през телефонна мрежа с помощта на два модема.

Фиг. 11.4. Комуникация между компютри чрез модеми и телефонна линия

По-голямата част от модемите използват аналоговите телефонни линии за предаване на данни. В повечето развити държави са изградени и продължава изграждането на цифрови мрежи. Предстои замяна в голяма степен на модемите, работещи по аналогови технологии с цифрови модеми и контролери.

В компютърните мрежи се използват модеми с възможности за:

- Автоматично набиране на телефонни номера и/или отговаряне на повиквания.
- Свързване към модем посредством парола с последователно прекъсване на връзката, и обратно – позвъняване за "подслушване" на линията с цел адаптиране на скоростта на предаване.
- Активиране на пейджър при пристигане на факс или телефонно съобщение.
- Свързване с пощенски кутии за гласови съобщения с пароли на различни потребители.
- Отдалечен достъп чрез пароли за тестване и конфигуриране.

Съществуват цифрови DSDV модеми (Digital Simultaneous Data and Voice) за едновременно предаване на глас и данни. Чрез тях може да се говори по телефон и данните да се приемат и изобразяват на персонален компютър. Тези модеми използват две честотни ленти, едната за предаване на глас, а по другата лента се предават цифрови данни. Тази

технология позволява коментар на данните, предавани по широката честотна лента. Намерила е приложение в реализацията на устройства за хора с увреден слух, които могат да говорят по един канал, а по другия да четат текст от екрана на компютъра.

Модемите работят в два режима:

- Команден режим – модемът получава и изпълнява команди от крайно DTE устройство (компютър).
- Режим на предаване на данни – съобщенията се преобразуват и предават или приемат по или от комуникационната линия.

Модемите се превключват от режим предаване в приемане и обратно за 1 s. с команда от три последователни знака "+++". По-голямата част от модемите изпълняват набор от стандартни команди. Модемите се състоят от пет основни елемента [5]:

- DTE интерфейс
- микроконтролер
- модулатор
- демодулатор
- линеен интерфейс.

DTE интерфейсът е средство за свързване на модема с крайното DTE устройство, което може да бъде компютър, терминал, хост, мост или маршрутизатор. Външните модеми се свързват с персоналните компютри чрез един от серийните (COM) портове. Използваните стандарти за DTE – DCE интерфейси са: RS – 232 C/V.24; RS – 422 IV.36; RS – 485; RS – 530; H.21; V.35; G – 703 и др.

Най-разпространеният интерфейс за свързване на модем към персонален компютър е стандартът RS – 232 C/V.24. В този стандарт е предвидено битовете със стойност единица да се предават по линия, която свързва компютъра с модема, като отрицателни импулси, а нулите се предават с нулево ниво. Дължината на свързващия кабел между модема и компютъра е ограничена до 15 метра. Максималната скорост за предаване на данни по серийния канал на компютъра е 38 400 b/s.

Предаваните данни се разделят на малки блокове от 5 до 8 бита (обикновено 7 или 8). Към всеки блок се добавя един импулс с двойна широчина за означаване началото на блока. След всеки блок се добавят един или два бита за означаване края на блока. Към всеки блок се добавя и един контролен бит за контрол по нечетност или четност. Контролният бит допълва броя на единиците в блока съответно до нечетно или четно число. Тогава, когато сумата по модул 2 на информационните разряди не съвпада със стойността на контролния разряд, се приема, че предаването на блока е извършено с грешка. При откриване на грешка блокът се предава отново.

При свързване на модема към серийния порт на компютър е необходимо да се извърши конфигуриране на характеристиките на серийния порт и на модема. А за инструмент се използва съответна програма от операционната система на компютъра. Чрез нея се установява скоростта за предаване на данните, броят на информационните разряди и стоп битовете, видът на проверката за достоверност на данните, наличие или отсъствие на протокол за управление на потока от данни (flow control) и номерът на използвания COM порт.

Микроконтролерът служи за подготовка на данните. Той анализира входящия поток от данни, компресира го, променя кода в по-ефективен и извършва шумоустойчиво кодиране. В режим на приемане микроконтролерът изпълнява същите функции в обратен ред. Микроконтролерът има вградени апаратни методи за откриване и/или коригиране на грешки при предаването на данни. Данните, приети от компютъра, се обединяват в блокове до 20 000 байта в зависимост от качеството на канала. Към всеки блок се добавят чрез използване на сумиране или циклически кодове контролни данни за проверка на достоверността. В някои

модеми се използват и програмни методи за проверка на достоверността на данните, които забавят предаването. Най-разпространените стандарти за предаване на данни чрез модеми са MNP4, MNP10 и V-42.

Модулаторът и демодулаторът се изпълняват като един възел. Те преобразуват цифровите сигнали на микроконтролера в аналогови сигнали, подходящи за предаване по телефонна линия. Преобразуването се нарича дискретна модулация, при която се използват два сигнала: модулиращ цифров сигнал и модулиран аналогов сигнал. Цифровият сигнал въздейства върху амплитудата, фазата или честотата на аналоговия сигнал. В зависимост от параметъра на сигнала, върху който се въздейства, съществуват различни видове модулации:

- амплитудна модулация (ASK)
- честотна модулация (FSK)
- фазова модулация (PSK)
- диференциална фазова модулация (DPSK) с 2 или 4 фази.

Амплитудната модулация ASK (Amplitude Shift Keying) е свързана с включване и изключване по линията на носещия сигнал по въздействието на модулиращите цифрови сигнали. Съществува и разновидност, при която двоичните 0 и 1 се представят с различни нива. Индуктираните шумове в канала за предаване на данни се сумират с полезния сигнал, което довежда до грешно тълкуване смисъла на данните. По тази причина този вид модулация почти не се използва.

Честотната модулация FSK (Frequency Shift Keying) по принцип използва две честоти. По-високата честота се използва за предаване на двоичната единица, а по-ниската за предаване на двоичната нула. Този вид модулация заема сравнително широк честотен диапазон и се използва в модеми за предаване на данни с по-малки скорости.

Фазовата модулация PSK (Phase Shift Keying) е свързана с промяна на фазата на носещия сигнал под въздействието на модулиращия цифров сигнал. Когато се използват само две фази, разположени на 180^0, модулацията се нарича двоична фазова манипулация – BPSK (Binary Phase Shift Keying).

Диференциална фазова модулация – DPSK (Differential Phase Shift Keying) е тази, при която фазата на елементите на модулирания сигнал се отчита спрямо фазата на предходния сигнал. При този вид модулация не се изисква наличие на еталонен сигнал. Методът използва модулация на сигнали с използване на 2, 4 и 8 фази.

Потребителският интерфейс е средство за взаимодействие на потребителя с модема. Използва се за настройка и диагностика на модема и може да се реализира чрез:

- индикаторни светодиоди;
- високоговорител;
- светлинен дисплей;
- течнокристален дисплей.

Линейният интерфейс осигурява връзка на модема с комуникационната линия. Сигналите в изхода на модема се формират и усилват до нивото на телефонните сигнали. Класификацията на модемите се извършва по следните показатели:

- Вид на използваните линии.
- Режим на работа.
- Режим на предаване и приемане.
- Разположение на модема.
- Начин на свързване на модема.

В зависимост от използваните линии модемите се разделят на две групи:

- модеми за комутируеми линии;
- модеми за арендовани линии.

Широко приложение намират модемите, използващи арендовани линии за предаване на данни. Това са ADSL, XDSL и HDSL (High Bit-rate Digital Subscriber Line). Тези модеми пренасят данни със скорост до няколко десетки Mb/s в дуплексен режим на разстояние до няколко километра. Използваните линии за връзка са медни усукани двойки с дебелина на проводниците 0.5 mm.

В зависимост от режима на работа модемите се делят на:

- асинхронни модеми;
- синхронни модеми.

В зависимист от режима на предаване и приемане модемите се делят на:

- пълнодуплексни модеми;
- полудуплексни модеми;
- симплексни модеми.

Пълнодуплексните модеми (Full Duplex) могат да предават и приемат данни едновременно. Тези модеми имат широко приложение в практиката. Те използват две честотни ленти за предаване и приемане на данни. Когато единият комуникиращ модем използва горната честотна лента за предаване, а долната за приемане, другият модем приема по горната лента, а предава по долната. По този начин се постига едновременно предаване и приемане на данни, но за съжаление двете честотни ленти намаляват наполовина. Разновидност на двупосочните модеми са асиметричните модеми – ADSL. Те работят в статистически дуплексен режим. При тях също се използват две честотни ленти за предаване на данни, но с различна широчина. По-голямата честотна лента се предоставя на посоката, която се използва за предаване на повече данни. Високоскоростният канал се използва за предаване на данните, а нискоскоростният изпраща потвържденията. Тази схема се прилага при свързване на интернет потребителите. Заявките се изпращат по нискоскоростния канал, а информацията от Интернет се получава по високоскоростния канал.

Полудуплексните модеми (Half Duplex) не могат да предават и приемат данни едновременно. В процеса на работа последователно сменят режимите на предаване и приемане на данни. Те използват по-широки честотни ленти, но вследствие на смяната на режимите имат по-малка скорост на предаване и приемане спрямо пълнодуплексните модеми. Времето, необходимо на модемите за превключване от един режим на друг, допълнително влияе отрицателно върху средната скорост за предаване на данни.

Симплексните модеми се използват само за режим предаване или приемане. Те намират приложение в телеизмерителните системи, където предаването на данни в едната посока е значително повече спрямо другата.

В зависимост от разположението си спрямо компютъра модемите се делят на:

- външни модеми
- вътрешни модеми.

От своя страна вътрешните модеми се делят на:

- Модеми, поставени в разширителния слот на PC.
- PC – карт модеми за Laptop.

В зависимост от начина на свързване модемите се делят на:

- Модеми с директно свързване чрез съединител RJ – 11 към телефонна линия.

- Модеми с акустичен съединител (адаптер).

В модемите са приложени различни методи и технологии за повишаване скоростта на предаване на данни. Скоростта, с която модемите предават, се измерва в битове за секунда (b/s) и се нарича информационна скорост. Съществува и понятието **скорост на модулация,** която се измерва в бодове (baud). Двете скорости за предаване са различни и не бива да се слага знак за равенство между тях. Скоростта на модулация е скоростта на предаване на елементите на модулирания сигнал , а информационната скорост е скоростта за предаване на битовете на модулиращия сигнал. Двете скорости са равни само тогава, когато при предаване един бит от модулиращия сигнал отговаря на един бит от модулирания. По правило скоростта на модулация е по-малка от информационната скорост.

Съществува теоретичен максимум за скоростта на модулация на цифров сигнал, предназначен за предаване по аналогов канал със зададена честотна лента. Този максимум се нарича граница на Найкуист. При използване на амплитудна, честотна и фазова модулация максималната скорост за предаване на данни се определя от израза

$$V = 0{,}75.F_к ,$$

където с V е означена скоростта, а с $F_к$ е означена честотната лента на канала.

Когато се използва стандартен телефонен канал с честотна лента $F_к$ = 3100 Hz, теоретичната граница за скоростта на Найкуист ще бъде приблизително 2400. Вижда се, че тази скорост е твърде ниска за приложение на модемите в практиката. В приетите стандарти за модемите са предвидени различни техники и технологии за повишаване скоростните характеристики на модемите. Най-ефективните от тези технологии са:

- изследване на линията;
- групово кодиране;
- решетъчна модулация;
- формиране на сигнала;
- измамване на протоколите;
- потискане на ехото;
- компресия на данните в реално време;
- използване на няколко носещи честоти.

Изследване на линията е метод, при който комуникиращите модеми интелигентно определят параметрите за трансфер на данни между тях. За тази цел модемите обменят служебна информация и установяват максимално допустимата скорост за предаване на данни. Изследва се честотният диапазон и методът за кодиране с цел постигане на най-високата информационна скорост. При този метод модемите компенсират отклоненията в характеристиките на телефонните линии, като предотвратяват смущенията в канала чрез методи за линейни компенсации. Обменят се сигнали на различни честоти и се води статистика за измененията на силата и фазата на сигнала.

Групово кодиране се извършва по алгоритъм, по който всеки бод носи информация за няколко бита. За кодиране на два бита от съобщението в един бод модемът е необходимо да разполага с четири състояния на модулирания сигнал – 00, 01, 10 и 11. Чрез такава модулация информационната скорост на модема се увеличава двукратно. Използва се квадратурна модулация, при която фазата на манипулирания сигнал се променя през 90^0, съответно се използват четири фази на носещия сигнал – 0^0, 90^0, 180^0 и 270^0.

Решетъчната модулация е метод, при който се използват няколко различни фази, честоти или амплитуди на носещия сигнал. Комбинират се два или повече метода за

модулация с цел поместване на повече битове в един бод. Така се постига по-висока информационна скорост.

Формиране на сигнала е метод, подобряващ отношението сигнал/шум чрез изменение на сигналите при определени състояние на канала. Сигналните точки, които се появяват по-често, се предават с по-голяма сила. По този начин се подобрява отношението сигнал/шум, което води до увеличаване пропускателната способност на комуникационния канал.

Измамване на протоколите е метод, при който в предавателния възел се премахва част от служебната информация в протоколните единици. Приемащият възел възстановява премахнатите полета и по този начин се намалява обемът на данните за трансфер между двата модема и се увеличава скоростта за предаване на данни.

Потискане на ехото е свързано с намаляване влиянието на отразените сигнали в комуникационната линия. Предаващият модем изпраща към приемащия сигнал, който се отразява от края на линията. Приемащият модем измерва времето за закъснение и силата на отразения сигнал. При работа модемите компенсират тези сигнали, като създават обратни по амплитуда и фаза сигнали за компенсиране на отразените, които се разглеждат като смущения.

Компресия на данните в реално време се прави с цел намаляване обема на потока от данни и увеличаване на информацията в тях. Повтарящите се единици блокове от данни могат да се закодират с един блок от данни и друг блок с информация за схемата на повторение. Този метод е ефективен при предаване на графична информация. Повтарящите се елементи се предават информационно само еднократно. Използват се „речникови" схеми за компенсация, при които части от потока от данни се заместват с указатели към речник. Съществуват международни стандарти за компресия като: MNP5, MNP7 и V42bis, които се основават на „речникови" методи за компресия. Препоръчва се файловете, които се изпращат към модема за предаване, да се компресират още в паметта на компютъра. По този начин се постига по-висока скорост за предаване на данни през серийния порт на компютъра. За да се предотврати загуба на части от съобщението, е необходимо да се предвиди управление на потока от данни. Той се използва за съгласуване производителността на компютъра с възможностите на модема да приема и предава данните. Модемът съобщава на компютъра, когато се препълва буферът му за данни, в резултат на което временно се ограничава предаването от страна на компютъра. Протоколът за управление на данни се изпълнява апаратно или програмно. Формата на реализация се указва при конфигуриране на системата посредством програмата Modem Commands на менюто Settings.

Използване на няколко носещи честоти е сравнително нов метод за подобряване възможностите на модемите за предаване на данни. Повечето модеми следят качеството на комуникационната линия и променят скоростта за предаване на данни, с цел избягване на грешки. При този метод, когато качеството на линията се влоши, не се намалява скоростта за предаване на данни, а се преминава на друга работна честота. Статистически се установяват работните честоти, в които се появяват грешки и не се използват от модемите.

Стандартите за разработване на модемите са създадени основно от следните организации и фирми: Международният телекомуникационен съюз (ITU); фирма Microcom – стандарти MNP; американски стандарти – Bell.

Стандартите ITU основно са предназначени за предаване на данни по телефонни мрежи. По-важните от тях са: V.21.; V.22.; V.22.bis.; V.23.; V.32.; V.32.bis.; V.32.turbo.; V.34. (V.fast); V.FS.; V.42.; V.2.bis.; V.90. С нарастването на номера на версията се повишава скоростта за предаване на данните [6].

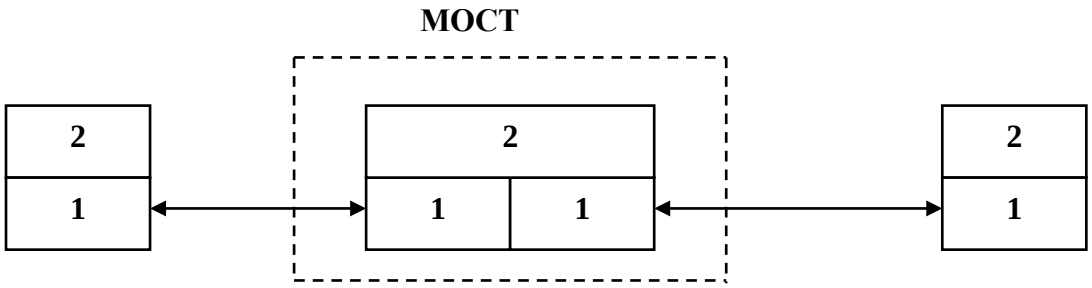
Стандартът MNP (Microcom Networking Protocol) изисква апаратна реализация. Приложена е технологията на компресия, както и методика за откриване и/или коригиране на грешките при предаване и приемане на данни. Стандартът е развит по класове – от 1. до 10.

без клас 8., който не съществува. Модемите от клас MNP – 1 до MNP – 4 откриват и коригират грешки. Всички модеми от стандарта са обратно съвместими. При установяване на връзка между два MNP модема се избира най-високият възможен клас.

При предаване на данни MNP-модемите използват метода на „хлъзгащия се прозорец" с размер от 5 кадъра, които се предават заедно. За проверка достоверността на данните се използва цикличен код. Когато се установи грешка, приемащият модем връща отрицателна квитанция и целият прозорец се предава отново (протокол Go Bback N).

Съвременните високоскоростни модеми имат вградени функции за изпращане и приемане на факсимилни съобщения. С помощта на факса се предават копия на документи на големи разстояния по електронен път. Страниците се сканират с фотодетектор и изображението се разделя на черно-бели точки (пиксели) с разделителна способност 720x360 dpi (dots per inch). Регистрират се 720 точки на един инч хоризонтално и 360 точки вертикално. Използват се и компютърно базирани факс системи, при които факсимилетата се изобразяват на монитор и се отпечатват на принтер. В локалните компютърни мрежи, свързани към Интернет, се използват факс сървъри, които премахват необходимостта от факс модеми и специална телефонна комуникационна линия.

Мостът (Bridge) е устройство за свързване на локални компютърни мрежи на нивото на каналния слой на отворения модел (OSI) – (фиг. 11.5) [5].

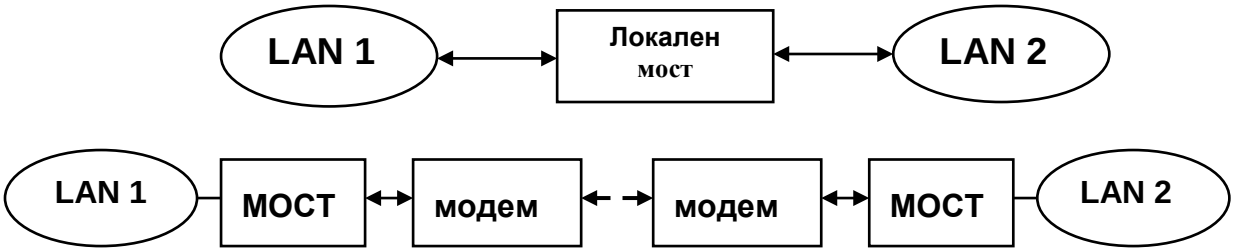


Фиг. 11.5. Схема за свързване на мост

Съществуват два вида мостове, които се използват за свързване на компютърни мрежи и имат различно приложение, показано на схемата на фиг. 11.6:

- Локални мостове за свързване на близко разположени локални мрежи.
- Мостове за свързване на локални мрежи на големи разстояния.

Персоналните компютри могат да изпълняват и функции на локален мост. За целта в разширителния слот се поставят повече от един мрежови адаптери, всеки от които е свързан към различна локална компютърна мрежа. Необходимо е и инсталиране на съответното програмно осигуряване за управление на процесите по адаптиране на различните мрежи.



Фиг. 11.6. Схеми за свързване на локални мрежи с мостове

Мостовете се използват за сегментиране на големи и претоварени локални мрежи. Генерираните кадри от едната мрежа и предназначени за другата се разпознават по MAC адреса на възела получател. Форматът на кадъра, преминал през моста към друг сегмент, не се променя. От гледна точка на каналния слой мостовете се разделят на два вида:

- MAC мостове, действащи на нивото на MAC подслоя.
- LLC мостове, действащи на нивото на LLC подслоя.

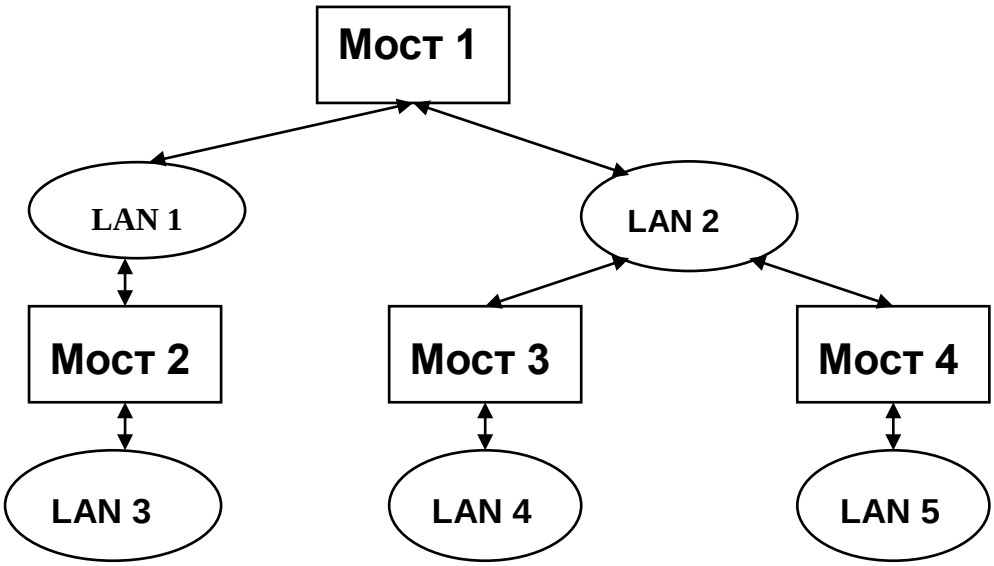
MAC мостовете се използват за свързване на еднотипни локални компютърни мрежи като 802.3. с 802.3., 802.5. – с 802.5. и т.н.

LLC мостовете се използват за свързване на локални компютърни мрежи с различен формат на кадъра като 802.3. с 802.5.

MAC мостовете се разделят на още два вида:

- Интервални мостове(Sponning Tree Bridges).
- Маршрутизиращи мостове от източника (Source Routing Bridges).

Интервалните мостове работят по стандарта IEEE 802.3. и използват алгоритъм "покриващо дърво". Наричат се "обучени", защото научават MAC адресите на свързаните към тях крайни възли чрез самообучение при преминаване на кадрите през мостовете. Проектирани са за неразклонени локални компютърни мрежи, за да изглеждат като една мрежа. Мрежите се конфигурират програмно в дървовидна топология от администраторите.



Фиг. 11.7. Схема на свързване на LAN 802.3.

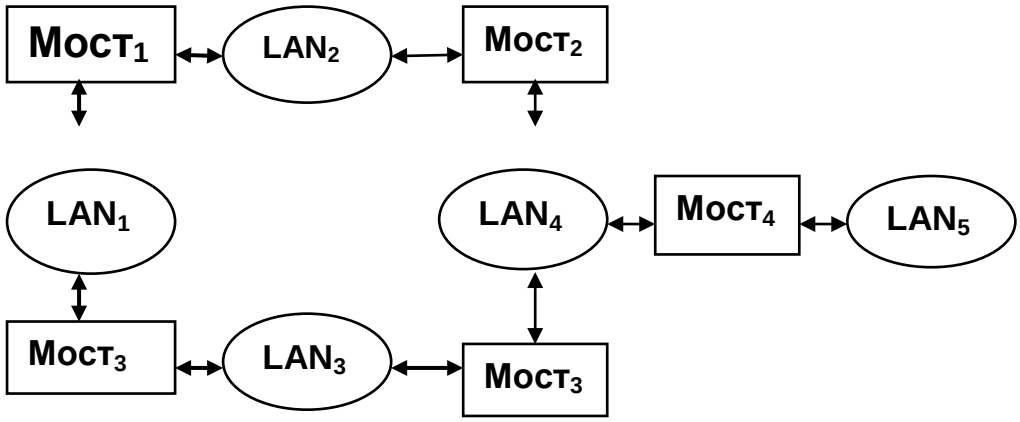
Работата на интервалните мостове се базира на таблица с MAC адреси, която те построяват чрез самообучение. Когато получи кадър на своя порт, мостът проверява дали указаният в него MAC адрес на възела получател се съдържа в таблицата му. Ако адресът го няма в таблицата, мостът изпраща кадъра до всички останали портове от своя сегмент. Ако адресът на възела получател се намира в таблицата, мостът насочва кадрите към съответния изходен порт. Този вид мостове не се интересуват от точния маршрут на преминаване на кадрите. Те се интересуват единствено от номера на порта си, към който трябва да се пренасочи съответният кадър.

Маршрутизиращите мостове работят по стандарта IEEE 802.5. и се използват за свързване на Token Ring мрежите. Мостовете пренасочват кадрите на базата на маршрутна информация, записана в тях от крайния възел подател. На всяка локална мрежа Token Ring се

присвоява отделен идентификационен номер. Крайният възел, който има съобщение за друг, изпраща общодостъпен кадър “до всички” и очаква в отговор да узнае маршрута до получателя. Всеки мост добавя към служебния кадър номера на локалната мрежа, от която го е получил, и го предава по-нататък.

Интервалните и маршрутизиращите мостове не са съвместими. В смесените конфигурации на локалните мрежи от стандарти 802.3. и 802.5. се използват LLC мостове за преобразуване на кадрите.

Мостовете обработват кадрите в реално време, тъй като не се налага преформатиране на полетата им. Прочита се MAC адресът на възела получател, след което кадърът се филтрира или препредава. Мостовете се предлагат от фирмите производители с повече от един кабелен интерфейс. Най-често се предлагат интерфейси за коаксиален кабел и интерфейс за усукана двойка.



Фиг. 11.8. Схема на свързване на LAN в смесена топология

Маршрутизаторите (Routers) са многопротоколни устройства за свързване на хетерогенни мрежи на нивото на мрежовия слой на OSI модела. При тези устройства доминират маршрутизиращите функции пред комутиращите. Освен че вземат решение за маршрута на пакетите, те откриват възникнали грешки в данните и съставят и актуализират таблица за мрежовата топология, която се използва за маршрутизиране.

Прието е маршрутизаторите да се наричат още рутери. Те не са прозрачни за работните станции и сървърите, както мостовете и повторителите. Рутерът се приема като самостоятелен мрежов възел със собствен мрежов адрес. Схемата на свързване на рутера е показана на фиг. 11.9.

Всеки порт на рутера има свой уникален адрес в зависимост от типа на мрежата, към която е свързан. Маршрутизаторът е сложно в сравнение с компютъра скъпоструващо програмно техническо устройство. Той може да се реализира и чрез инсталиране на подходящо програмно осигуряване в обикновен компютър.

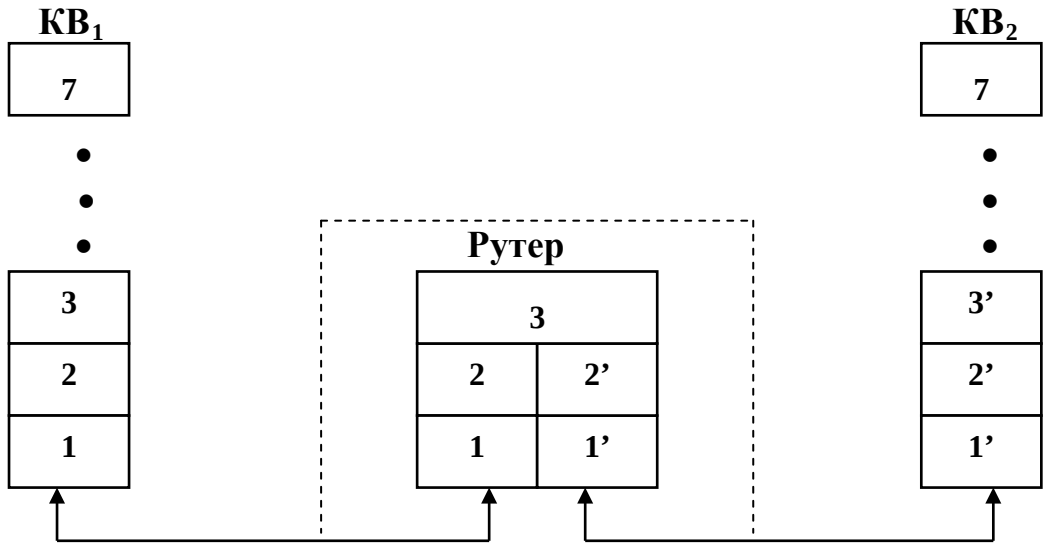
Преди да се изпрати пакет към възел получател, рутерът анализира условията на трафика и избира един от няколко алтернативни маршрута за предаване на базата на критерии за оптимизиране. Вследствие на използването на софтуерни решения рутерът има ниска скорост на маршрутизиране, в резултат на което се намалява производителността на компютърните мрежи. За повишаване на скоростта на обработка на пакетите обикновено в архитектурата на маршрутизаторите се използват RISC и секционните процесори.

Съществуват многопротоколни рутери, чрез които се обединяват локални компютърни мрежи, използващи различни протоколи от физическото и каналното ниво на комуникационния модел. Обединяването на локални мрежи с помощта на рутери създава

възможност за изграждане на защитни прегради на мрежите от генерирани пакети в други компютърни мрежи.

Мрежовите протоколи, които допускат маршрутизиране на пакети, са: IPX, IP, XNS и DDP. Маршрутизаторите се използват за свързване на локални компютърни мрежи към глобални мрежи и Интернет, както и за обединяване на няколко локални компютърни мрежи в глобална мрежа.

Мост–маршрутизаторът (Bruters) е устройство, което се използва като мост за някои пакети на нивото на каналния слой и като маршрутизатор за други пакети на нивото на мрежовия слой на комуникационния модел. В зависимост от начина на настройка той може да работи като рутер за някои протоколи (IP и IPX) и като мост за други протоколи (LAT).



Фиг. 11.9. Схема за свързване на рутер

Комутаторите (Switches) са концентратори с възможност да комутират кадри в каналния слой на комуникационния модел. Използват се за намаляване на вероятността за конфликти в компютърните мрежи от типа *клиент/сървър*, функциониращи по протокол IEEE 802.3. В изградените на повече от едно ниво локални компютърни мрежи, поради възникване на множество конфликти за заемане на комуникационния канал, скоростта на предаване на данни е значително по-ниска от предвидената за стандарта. С използването на комутаторите се създават условия за намаляване на конфликтите между компютрите и производителността на мрежите нараства. Комутаторите използват три вида комутации:

- статична комутация;
- динамична комутация;
- комутация на сегменти.

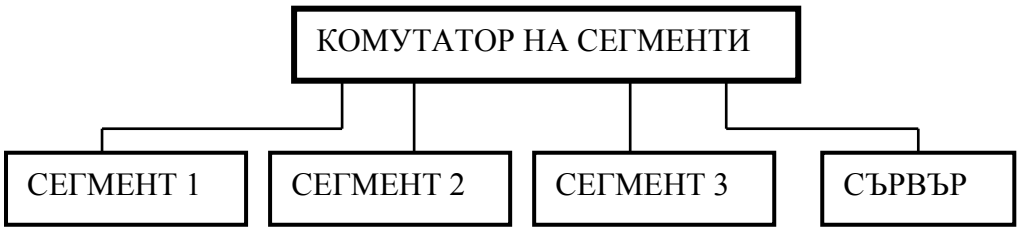
При статичната комутация администраторът премества програмно потребителите от един сегмент на компютърната мрежа в друг. По този начин някои потребители се преместват от претоварен сегмент на компютърната мрежа в друг, по-малко натоварен.

Динамичната комутация осигурява непрекъсната комутация между мрежовите устройства. При използване на този метод непрекъснато се създават динамични съединения между портовете на комутатора за предаване на данни със скорост 10 или 100 Mb/s. Самата комутация се извършва на базата на адресната информация в кадрите. По този начин в

локалната мрежа се създават десетки и стотици съединения, без да си влияят взаимно. Тази комутация се нарича още *комутация на портовете*.

Съществува и *комутация на сегментите*, при която към всеки порт на комутатора се свързва отделен сегмент на мрежата. По този начин голямата локална компютърна мрежа се разделя на по-малки части (сегменти). Комутаторът не е в центъра на локалната мрежа, а в периферията (фиг. 11.10) и изпълнява следните задачи:

- Контролира достъпа до опорната мрежа.
- Контролира обсега на разпространение на общодостъпните кадри – изпратени *до всички*.
- Контролира достъпа до глобалната мрежа или Internet.



Фиг. 11.10. Комутация на сегментите на компютърна мрежа

С помощта на комутатор може да се изгради висикоскоростна връзка до всеки сегмент и сървър на компютърната мрежа. Когато компютрите, свързани към сегменти 1, 2 и 3, обменят съобщения между абонати само в своя сегмент, комутаторът не участва в управлението на трафика. Ако компютри от един сегмент се обърнат към компютри от друг сегмент, комутаторът изгражда комуникационен канал между сегментите. Портовете на комутатора, към които се свързват сегментите, имат възможност да управляват до 4096 MAC-адреса на компютрите, свързани към съответните сегменти на мрежата.

Програмното управление на комутираните локални мрежи позволява създаване на виртуални локални мрежи (VLAN). За целта група възли и потрбители се отделят програмно и работят като отделна мрежа. Виртуалната локална мрежа се създава, реконфигурира и премахва лесно, без да се налага физическо преместване на компютри. Има възможност една работна станция да се включи към повече от една виртуална мрежа. Няколко виртуални частни мрежи могат да ползват общи мрежови ресурси като сървъри за комуникационни услуги, електронна поща и др. За конфигурирането на VLAN се използват Ethernet комутатори, които поддържат до 64 виртуални мрежи към един порт.

6.2. Съгласуване на компютърните мрежи в горните слоеве на комуникационния модел

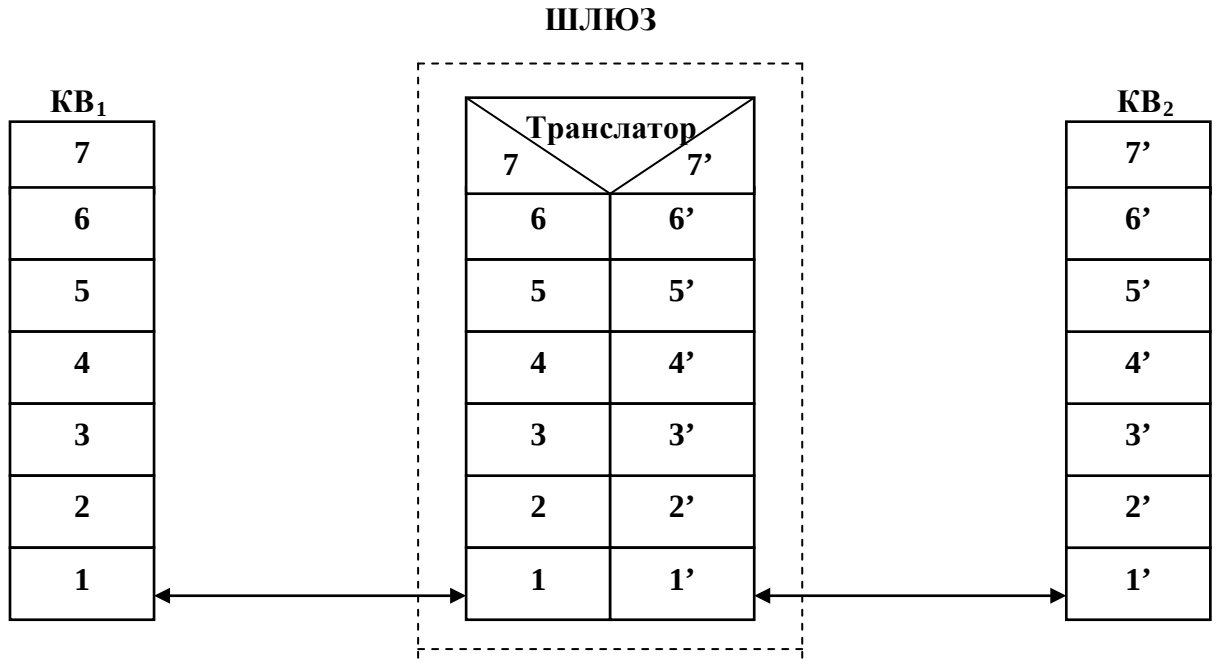
Съгласуване на компютърните мрежи в слоеве, по-високи от мрежовия на комуникационния модел, се реализира значително по-сложно от долните слоеве. Използват се програмни средства и процедури, реализирани като стандартни протоколи. Прилагат се основно два подхода за решаване на проблема:

- транслация на протоколи;
- мултиплексиране на протоколни стекове.

Транслацията на протоколи се извършва от специализирано устройство, наречено *шлюз* (gateway). Тези устройства се разполагат между две мрежи, които функционират под управлението на различни операционни системи и протоколни стекове.

И двата метода имат положителни и отрицателни страни. Най-доброто решение е да се инсталира във всички мрежи един-единствен протоколен стек. С такава цел е бил проектиран отвореният модел за комуникации OSI. За съжаление, на практика се оказа, че внедряването на този модел не се случва. Единствено правителството на САЩ е финансирало програма, с която всички държавни учреждения се задължават да поддържат отворения комуникационен модел. Останалият компютърен свят се съпротивлява на такава мярка и институциите от всички държави продължават да развиват и използват паралелно няколко мрежови протоколни стека.

Шлюзът (Gateway) е програмно осигуряване, инсталирано във възел, посредник за транслация на различни версии протоколни стекове. Той функционира основно от транспортния до приложния слой на комуникационния модел. Функционалният модел за съгласуване на различни протоколни стекове е показан на фиг. 11.11. Програмното осигуряване за съгласуване между компютри и мрежи се инсталира в транспортния, сесийния или приложния слой на отворения модел за комуникации. За да могат две мрежи с различни протоколни стекове да си взаимодействат, е необходимо и двата стека да се инсталират в шлюза. Те преобразуват както протоколите, така и системите за кодиране.



Фиг. 11.11. Функционален модел на шлюз в съответствие с OSI модела

Достъпът на работните станции до ресурсите на сървърите се осъществява през *компютър/шлюз*. Програмното осигуряване на шлюза позволява обмен на файлове и отпечатване на документи на мрежовия принтер. Информация за състоянието на шлюза може да се изведе на дисплея на *компютъра/шлюз*. Шлюзът има възможности да поддържа едновременно до 128 сесии от типа «работна станция – сървър» и до 98 сесии «работна станция – принтер».

Мултиплексиране на протоколни стекове е метод, при който някой от крайните възли разбира езика на други крайни възли или компютърни мрежи. За целта в крайните възли е необходимо да се инсталира нов протоколен стек. Неудобство на метода е, че когато

се налага съгласуване с повече от една версия на мрежови протоколни стекове, в компютъра е необходимо да се инсталират всичките протоколни стекове. В резултат на това операционната система на компютъра се допълва с допълнителен модул за насочване на получените съобщения към съответния протоколен стек.

Недостатък на шлюзовете е, че те работят сравнително по-бавно от крайните възли и концентрацията на съгласуващия софтуер в един възел намалява производителността и сигурността на мрежата, тъй като при повреда или отказ на шлюза системата престава да работи.

Въпроси за самостоятелна работа

1. Защо се налага съгласуване на компютърните мрежи на долните нива на комуникационните модели?
2. Защо се налага съгласуване на компютърните мрежи на горните нива на комуникационните модели?
3. Какви са функциите на повторителите в компютърните комуникации?
4. Какви са функциите не модемите в компютърните комуникации?
5. Какви видове и стандарти модеми познавате?
6. Какви са функциите на мостовете в компютърните мрежи?
7. Какви са функциите на маршрутизаторите в компютърните мрежи?
8. Какви са функциите на шлюзовете в компютърните мрежи?
9. Каква е ролята на комутаторите в локалните компютърни мрежи?
10. Променят ли се протоколните единици в глобалните компютърни мрежи при преминаване на съобщението от един стандарт към друг?

ЛИТЕРАТУРА

1. Асенов, Б., П. Крипов. Теория на контраразузнаването. София, Труд, 2000.
2. Антонов, П., С. Малчев. Криптография в компютърните комуникации. Варна, ТУ, 2000.
3. Антонов, П. Комплексен подход към надеждността, безопасността и сигурността на компютърните и комуникационните системи и мрежи. Компютърни науки и технологии, брой 1, 2004 г., ТУ – Варна, с. 4 – 11.
4. Бенкс, М. Как да защитим компютъра си. София, СофтПрес, 2001.
5. Ганчев, И. Компютърни мрежи и комуникации. Пловдив, ИМН, 1999.
6. Георгиев, Г., Р. Иванов, Й. Атанасов. Модеми и факс-модеми. София, 1996.
7. Домарев, В. Безопасность информационных технологий. Москва, Диасофт, 2002.
8. Дънам, К. Компютърните вируси. София, Алекс Софи, 2001.
9. Золотов, С. Протоколы Internet. Санкт-Петербург, BHV, 1998.
10. Зюко, А. Г., Д. Д. Кловский, М. В. Назаров, Л. М. Финк. Теория передачи сигналов. Москва, Радио и связь, 1986.
11. Кент, П. Да научим Netskape Communicator 4. София, ИнфоДар ООД, 1998.
12. Кловский, Д. Передача дискретных сообщений по радиоканалам. Радио и связь, Москва, 1982.
13. Кориган, П., А. Гай. Изграждане на локални мрежи с Net Ware v.2.2. и 3.x. на Novell. София, Техника, 1993.
14. Мардон, Т. Локални мрежи с равноправен достъп. София, Техника, 1995.
15. Максимална защита (хакерско ръководство...). София, ИнфоДар, 2003.
16. Максимална защита (хакерско ръководство за защита на вашия сайт и мрежа – Книга 1). София, ИнфоДар, 2002.
17. Максимална защита (хакерско ръководство за защита на вашия сайт и мрежа – Книга 2). София, ИнфоДар, 2002.
18. Мизин, И. А., В. А. Богатырев, А. П. Кулешов. Сети коммутации пакетов. Москва, Радио и связь, 1986.
19. Милев, П. Теория на информацията и предаване на данни. София, ВТС, 1993.
20. Огнянова, Н. Право и етика на информационното общество. София, Нова звезда, 2002.
21. Олифер, Н. А., В. Г. Олифер. Сетевые операционные системы. М., ЦИТ,WWW.citforum.ru.
22. Остерло, Х. TCP/IP. Пълно ръководство. София, СофтПрес, 2002.
23. Петров, Р. Защита на информацията в компютрите и мрежите. София, Корени, 2002.
24. Пенин, П., Л. Филиппов. Радиотехнические системы передачи информации. Москва, Радио и связь, 1984.
25. Попов, М., М. Калбанов. ISDN – нова мрежова и информационна технология. Велико Търново, Фабер, 2004.
26. Рош, У. Компютърна библия – ч. II. Компютър таймс ООД, 1995.
27. Соколов, А. Шпионские штучки. Новое и лучшее. Санкт-Петербург, Полигон, 2000.
28. Станев, Ст., Ст. Железов. Компютърна и мрежова сигурност. Шумен, 2005.
29. Стърлинг, Б. Удар срещу хакерите. София, УИ "Св. Климент Охридски", 2000.
30. Тарас, А. Наръчник по разузнаване и сигурност. София, 1999.
31. Тужаров, Хр. Компютърни мрежи. Велико Търново, ПИК, 2000.
32. Шиндър, Д. Компютърни мрежи. С., СофтПрес, 2003.
33. Шатт, С. Мир компьютерных сетей. К., BHV, 1996.
34. Шварцман, Б. О., Г. А. Емельянов. Теория передачи дискретной информации. М., Связь, 1979.

35. Microsoft Corporation. Компютърни мрежи – превод от англ. СофтПрес, Artech House Inc., 1994.
36. An introduction to PGP version 7.1.
37. Onvural, R. Asynchronous Transfer Mode Networks. Performance Issues, Artech House Inc., 1994.
38. Simmonds, A. Data Communications and Transmission Princciples. Macmillan Press LTD, 1997.
39. Stallings, W. Data and Computer Communications. 5 ed., Prentice–Hall, Inc., 1997.
40. Stallings, W. ISDN and Broadband ISDN with Frame Relay and ATM. 3 ed., Prentice–Hall, Inc., 1995
41. Tanenbaum, A. Computer Networks. 3 ed., Prentice-Hall,1996.
42. Tourlakov, S., L. Boyanov and others Internet-Working. Networks. Morgan Kaufmann Publishishers, Inc. 1996.
43. http://www.weca.net.
44. http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook
45. http://en.wikipedia.org/wiki/Iperf