И. Краљевски, З. Гацовски

ВОВЕД ВО КОМПЈУТЕРСКИ МРЕЖИ

Скопје, 2006

Краљевски Иван, Гацовски Зоран,
Вовед во компјутерски мрежи, 2006

Предговор

Кога се учи и усвојуваат нови теми или технологии, многу е важно да се имаат сите основи на дофат на рака. Оваа книга ги нуди градбените блокови за учење и разбирање на концептите и технологиите, користени при дизајн и имплементација на компјутерски мрежи.

Оваа книга е напишана со намера на лесен и прифатлив начин, без непотребно навлегување во детали, да го запознае читателот со светот на мрежните комуникации и да овозможи стекнување на практични сознанија од оваа област на компјутерската технологија.

Книгата нуди комплетно претставување на оваа област и примарно е создадена да биде учебник за студентите на техничките науки, пред се информатика и телекомуникации, но слободно може да ја користат сите кои сакаат да ги запознаат начините и технологијата на функционирањето на компјутерските мрежи, и да научат повеќе за концептите како работат компјутерските мрежи, како се пренесуваат податоците по Интернет и мрежите, имплементација на реални компјутерски мрежи, донесување одлуки при дизајн и инсталација на мрежите итн. За да се овозможи лесно и ефикасно примање на содржината, книгата е поделена по тематски поглавја со илустрации, фотографии и примери. Низ книгата се дадени објаснувања и аналогии на комплексни поими за мрежите, како и практични примери како се користат опишаните технологии во реалниот свет.

Првото поглавје, „Вовед во компјутерски мрежи“, дава опис на основните поими и концепти на компјутерските мрежи, како и историјата на развитокот на мрежите од првобитната замисла па до денешниот Интернет. Покрај тоа дадени се и примери на постоечки мрежни технологии, како што се Ethernet и безжичните мрежи.

Во второто поглавје „ОСИ референтен модел“, е опишан моделот за интерконекција на отворени системи – ОСИ, при што секој од седумте составни слоеви се детално опишани преку примери на карактеристичните протоколи и апликации.

Во третото поглавје „Мрежна инфраструктура“, опишани се начините за пристап кон медиумот, мрежните топологии и архитектура.

Во четвртото поглавје „Мрежни уреди“, даден е преглед на видовите на мрежни медиуми и конектори, а детално се опишани и поголем број на мрежни уреди, нивната функционалност како и нивната поврзаност со останатите уреди во компјутерската мрежа.

Петото поглавје, „LAN технологии“, дава опис на протоколите и изведбите на најпопуларните варијанти на локални мрежи како што се Ethernet, Token Ring и FDDI.

Во шестото поглавје „WAN технологии“, прикажани се најзначајните WAN концепти како што се поимите за виртуелни и комутирани кола. Покрај тоа даден е преглед на PPP протоколот, интегрираните сервиси на дигитална

мрежа - ISDN и дигиталната претплатничка линија – DSL и кабелска мрежа како најпопуларни имплементации на WAN мрежи.

Седмото поглавје „Безжични технологии“, дава преглед на безжичните технологии користени во изведба на безжична локална, метрополитен и приватна мрежа, и тука се опишани протоколите за WiFI, WiMAX и Bluetooth.

Во осмото поглавје „Мрежни протоколи“, се прикажани најпопуларните протоколи користени во имплементација на модерните компјутерски мрежи, TCP за транспортниот слој и IP за мрежниот слој на ОСИ референтниот модел.

Деветото поглавје „Мрежни сервиси и софтвер“, ги дава основните карактеристики и специфичности на мрежните сервиси и софтверот со кои треба да бидат запознаени дизајнерите со цел да направат правилен избор при имплементација на една мрежа. Даден е приказ на најчесто користените мрежни оперативни системи, како и нивните карактеристики во поглед на можностите кои ги нудат и системските побарувања.

Во десетото поглавје „Имплементација на мрежа под Windows“, се дадени практични насоки за конфигурација на компјутерска мрежа со користење на Windows оперативните системи, начини за адресирање и разрешување на логичките имиња.

1 Вовед

1.1 Поим за компјутерски мрежи

Мрежа преставува систем кој овозможува комуникација помеѓу два корисници или машини. Во светот на компјутерските мрежи, потребно е детално дефинирање на правилата за комуникација; компјутерите кои меѓусебно комуницираат мора да ги познаваат овие правила, како и луѓето кои зборуваат на ист јазик за да комуницираат без проблеми.

Ако компјутерите не се разбираат меѓусебно, не може да се оствари нивно поврзување и мрежните сервиси, како што се пристапот кон Интернет, делењето на датотеки и фолдери или печатењето, не се возможни.

Секој од последните 3 века бил доминиран од една технологија; во 18-тиот век тоа биле механички системи кои ја придружувале Индустриската револуција, во 19-тиот тоа била парната машина, додека во 20-тиот век клучната технологија станало прибирањето, процесирањето и дистрибуцијата на информации. Помеѓу другото се развил глобален телефонски систем, се појавиле радиото и телевизијата, раѓањето и експанзијата на компјутерската индустрија и користењето на комуникациските сателити.

Како резултат на брзиот технолошки развиток овие области брзо конвергираат една кон друга и се губат разликите помеѓу прибирање, пренесување, чување и процесирање на информациите.

Организациите со стотици оддалечени локации преку поширок географски области, очекуваат да бидат во можност да пристапуваат и ја испитуваат состојбата на било кое нивно оддалечено одделение на најлесен начин. Како што се зголемува способноста за прибирање, процесирање и дистрибуција на информациите, уште побрзо се зголемуваат барањата за пософистицирано процесирање на информациите.

Иако компјутерската индустрија е сè уште релативно млада во споредба со другите индустрии (автомобилската или авио-индустријата), компјутерите направија спектакуларен прогрес за релативно кратко време. Во текот на првите две декади од нивното постоење, компјутерските системи биле централизирани, и сместени обично во една голема просторија. Не толку ретко, оваа просторија имала и стаклени ѕидови преку кои посетителите можеле да фрлат поглед на големото електронско чудо кое се наоѓало внатре. Средно-големите компании или универзитети можеле да имаат еден или два компјутери, додека поголемите институции дури и повеќе.

Идејата дека во текот на дваесет години поседнакво моќни компјутери помали од поштенска марка масовно ќе се произведуваат и продаваат била чиста научна фантастика.

Мешањето на компјутерите и телекомуникациите имало големо влијание на начинот на кој се организирани компјутерските системи. Концептот на

„компјутерски центар“ како просторија со голем компјутер каде што корисниците би ги носеле своите програми за извршување станал комплетно застарен.

Стариот принцип на единствен компјутер кој ги опслужува потребите на целата организација се заменува со модел каде што голем број на одделени но поврзани компјутери ја извршуваат сета работа. Овие системи се наречени компјутерски мрежи.

Поимот „компјутерска мрежа“ означува множество на автономни компјутери поврзани со посредство на иста технологија. За два компјутери се вели дека се поврзани ако се во можност да разменуваат информации. Поврзувањето може да се оствари на многу начини, не само преку бакарни жици, туку и преку оптички влакна, микробранови и инфрацрвени бранови и комуникациски сателити. Постојат компјутерски мрежи со различни големини, форми и облици како што ќе биде прикажано понатаму.

Иако звучи чудно, но ниту Internet ниту WWW не се компјутерски мрежи, а тоа по читањето на книгата ќе стане јасно зошто. Накратко, одговорот би бил: Интернет не е единична мрежа - туку мрежа од мрежи, а WWW преставува дистрибуиран систем кој го користи Internet-от.

Постои значајна конфузија во литературата околу поимите за компјутерска мрежа и дистрибуиран систем. Клучната разлика се состои во тоа што, кај дистрибуираниот систем - множеството од самостојни компјутери се преставуваат на корисникот како еден кохерентен систем. Обично, тоа е единичен модел (парадигма) кој се презентира на корисниците, и обично софтверски слој над оперативниот систем наречен „middleware“ е одговорен за неговата имплементација. Познат пример за дистрибуиран систем би бил World Wide Web, каде што сè преставува документ (Web страница).

Во компјутерската мрежа, не постои таков кохерентен модел или софтвер. На корисниците им се презентира актуелната машина, без обид за преставување дека машините изгледаат и се однесуваат како една машина. Ако машините имаат различен хардвер и различни оперативни системи, тоа е потполно видливо за корисниците. Ако корисникот сака да извршува програма на оддалечена машина, треба да се најави на машината и да го изврши на неа.

Во суштина дистрибуираниот систем е софтвер изграден над мрежата. Софтверот овозможува висок степен на кохерентност и транспарентност. Така, разликата помеѓу мрежата и дистрибуираниот систем лежи во самиот софтвер (особено оперативниот систем), а не во хардверот.

1.2 Основи на умрежување

Мрежите се користат за поефикасна работа и комуникација. Мрежата може да поврзува компјутери, принтери, оптички уреди, скенери и друга опрема. Предноста на поврзувањето на компјутерите и опремата се состои во поефикасно пренесување на податоците.

Пред појавата на мрежите, корисниците за делење на информациите користеле магнетни дискови, а пред тоа и печатен материјал. Друга предност при користењето на мрежите е овозможеното делење на ресурсите; печатарите, тврдите дискови и апликациите може да се делат и со тоа да се намалат трошоците со што ќе се овозможи пристап на секој корисник во организацијата.

Компјутерската мрежа е изградена околу концептот на испраќач – извор (sender - Source), кој врши испраќање на податоци кон примател, односно одредишен компјутер (receiver – destination computer).

Компјутерите не се единствени машини кои можат да комуницираат на мрежата - и другите уреди имаат способност да бидат и извор и одредиште. Печатач, компјутер или било која друга машина која е способна за комуникација преку мрежата се нарекува *мрежен уред* или *јазол.*

Кога уредите учествуваат во комуникацијата на мрежата, треба да постои начин за пренесување на информациите помеѓу себе. Во повеќето мрежи, се користат кабли за поврзување на уредите. Можат да бидат поврзани со единствен кабел кој ги поврзува сите или пак каблите да го поврзуваат секој уред со централна локација. Каблите кои обично се користат се направени од бакарни жици слични на телефонските, но со значително повисок квалитет. Покрај бакарните кабли, се користат и други видови на медиуми како што се кабли направени од стакло или пластика, а од неодамна се користат радио бранови и микробранов пренос.

Поврзувањето на две или повеќе мрежи кои се способни да комуницираат меѓусебно се нарекува умрежување (*internetwork)*. Умрежувањето е способност различни мрежи да комуницираат со користење на специјален хардвер или софтвер.

1.3 Видови на мрежи

Компјутерските мрежи може да се поделат на три главни категории:

- Локална мрежа (Local Area Network - LAN) е мала мрежа составена од компјутери и уреди во склоп на една зграда или кат.
- Метрополитен мрежа (Metropolitan Area Network - MAN) е умрежување на повеќе LAN мрежи со брзи врски преку област на еден град.
- Глобална мрежа (Wide Area Network - WAN) поврзува локални мрежи со користење на јавна телефонска мрежа.

Локалните, метрополитен и WAN мрежите се меѓусебно различни. Покрај тоа што покриваат различни географски области, тие имаат и различни типови на инсталации и користат различни уреди како и различен начин на одржување.

Уредите во состав на една локална мрежа може да бидат релативно ефтини и лесни за одржување и обично доволно е еден корисник за одржување. Во помалите мрежи, доволно е еден корисник да преземе покрај своите работни

обврски и одговорност за одржување на мрежата, додека во средните и поголемите организации, постои потреба од администратори за обезбедување на техничка поддршка и одржување.

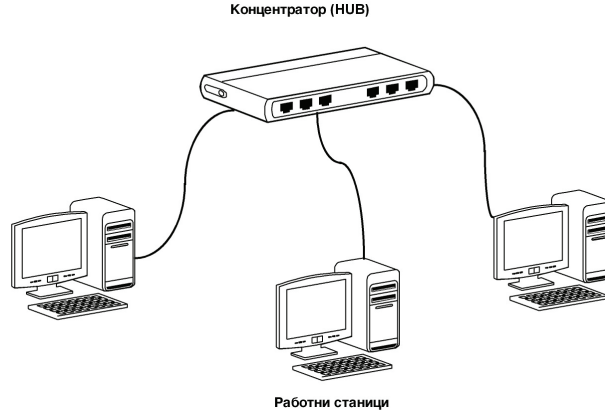
Во поголемите мрежи како што се MAN и WAN, постои пософистицирана мрежна опрема за одржување и во цената на инвестицијата на овие мрежи влегуваат и трошоците за долговремено одржување и администрација, а постои потреба и од барем еден професионален мрежен администратор.

Во денешно време, заради едноставниот пристап на Интернет, компаниите може да се поврзуваат со оддалечените локации без поголеми трошоци. Корисниците може да делат документи и да пристапуваат кон сервери од оддалечени локации, овозможувајќи им секаков вид на поврзување без високи трошоци за поставување и одржување на приватните WAN мрежи.

Многу од корисниците инсталираат и домашни компјутерски мрежи *„Home Area Networks - HAN“*, кои им овозможуваат поврзување на различни електронски уреди како што се компјутери и нивни периферии, телефони, видео игри, домашни безбедносни системи и интелигентна техника.

1.3.1 Локални мрежи (Local Area Networks)

Локалните мрежи *(Local Area Network - LAN)* играат важна улога во секојдневната работа на училиштата, претпријатијата и владините институции. Локалните мрежи им овозможуваат на корисниците заштеда на времето, помали трошоци преку користење на централизирана опрема и заштита на чувствителните податоци преку чување на сигурна локација. Дури, локалните мрежи се користат и за подобрување на соработката помеѓу вработените како и за обука преку користење на звук и видео.



Слика 1.1: Поврзување на компјутери во локална мрежа

Локалната мрежа се користи за поврзување на компјутери и други мрежни уреди така што уредите може да комуницираат еден со друг и да делат ресурси. Уредите на LAN мрежата се поврзани со кабли и во зависност од

ограничувањата за досегот, перформансите и управливоста, поимот за локална мрежа се однесува на канцеларија, кат или зграда.

На сликата е даден приказ каде што повеќе компјутери се поврзани со кабли кон еден централен уред наречен хаб (*hub)* или преклопник (*switch)*. Хабовите и преклопниците се уреди кои обично се наоѓаат на мрежата. Линиите од компјутерите кон хабот се каблите кои овозможуваат пренос на податоците од еден компјутер кон други. Во последно време сè повеќе се користат и безжични мрежи за поставување на локални мрежи.

Безжичните *(Wireless)* локални мрежи им овозможуваат на корисниците да се поврзуваат кон мрежните ресурси без инсталација на кабли или ожичување. Тука се користат безжични уреди наречени „пристапни точки“ (*Access Points)*, за примопредавање на податоците. Во зависност од големината на компанијата или објектот, може да постојат една или повеќе локални мрежи. Компанијата која е лоцирана во објект со повеќе катови и стотици вработени може да има локални мрежи на секој кат. Помеѓу секој кат, за поврзување на локалните мрежи може да се користат уреди како што се мостови (*bridge)* или рутери (*router)*. Во составот на еден LAN - компјутерите, печатарите и други мрежни уреди користат мрежни адаптери (*Network Interface Cards - NIC)* за поврзување кон мрежата и пренесување на податоците.

Локалните мрежи ги имаат следниве карактеристики:

- Се користат на помал простор (канцеларија или зграда).
- Комуникација со големи брзини од 10 Mbps па до 1 Gbps.
- Се овозможува пристап кон повеќе уреди.

Се користи специфична опрема како што се репетитори, концентратори, преклопници и мрежни адаптери.

При мерењето на брзината на пренесувањето на информациите преку компјутерските мрежи, обично се користат овие три кратенки: Gbps означува милијарда битови во секунда, Mbps означува милион битови во секунда, додека, Kbps е килобит во секунда и одговара на околу илјада пренесени битови во секунда.

1.3.2 Метрополитен мрежи (Metropolitan Area Networks)

Метрополитен мрежата (*Metropolitan Area Network - MAN)* се состои од локални мрежи кои се меѓусебно поврзани преку површината на еден град или метрополитен област. MAN стануваат сè попопуларни затоа што им овозможуваат на локалните управи да делат ресурси, комуницираат едни со други и да обезбедуваат приватен телефонски сервис на поголем простор. Иако MAN се релативно скапи за имплементација, тие овозможуваат алтернатива на побавните конекции кои се остваруваат преку WAN. MAN нудат поголема брзина заради користење на кабли и опрема со високи перформанси при нивната имплементација.

За разлика од LAN-овите, каде што постојат повеќе конекции кон уредите, MAN мрежите обично имаат само една конекција кој секоја локација (site). Причината се состои во високата цена на каблите и опремата.

Метрополитен мрежите ги имаат следниве карактеристики:

- Локациите се дисперзирани преку градската и приградските области.
- Со појавата на MAN мрежите, стана можно да се изведува поврзување со стотици Mbps, дури и со гигабитски брзини.
- Постои една точка на поврзување помеѓу секоја локална мрежа.
- Се користат уреди како што се рутери, телефонски и *ATM* преклопници и микробранови антени.

1.3.3 Глобални мрежи (Wide Area Networks)

Мрежата за поширок области (*Wide Area Network - WAN)* поврзува две или повеќе локални или метрополитен мрежи преку конекции кои обично се земаат под наем од локалниот телекомуникациски провајдер. Поврзувањето може да се изведе и со користење на кабли со оптички влакна или со безжични технологии.

WAN-овите обично работат преку телефонската инфраструктура затоа што е можно покривање на поголема географска област, можат да поврзуваат градови и држави. Поврзувањето на LAN-ови и MAN-ови на големи далечини бара софистицирана опрема и координација. Во повеќето случаи постои телефонска компанија која врши обезбедување на физичка конекција. Ако е потребно поврзување на локации на различни континенти може да се обезбеди и сателитска врска. Поголемиот дел од WAN мрежите комуницираат со брзини помеѓу 56Kbps и 1.5Mbps, иако се можни и повисоки брзини. WAN мрежите ги имаат следниве карактеристики:

- Може да покријат поголема географска област.
- Во споредба со LAN-ови комуницираат со помали брзини.
- Пристапот кон WAN е ограничен; LAN-овите обично имаат една WAN врска која се дели на сите уреди.
- Се користат уреди како што се рутери, модеми и WAN преклопници.

1.4 ИСТОРИЈА НА КОМПЈУТЕРСКИТЕ МРЕЖИ

Развојот на компјутерските мрежи е динамичен, но технологијата која е нивна основа не се сменила многу. Мрежите можат да бидат побрзи или поефикасни, или да имаат повеќе можности, но начинот како работат во основа останува ист. Администраторите на мрежите треба да имаат познавања од технологиите, што ќе им овозможи полесно справување со

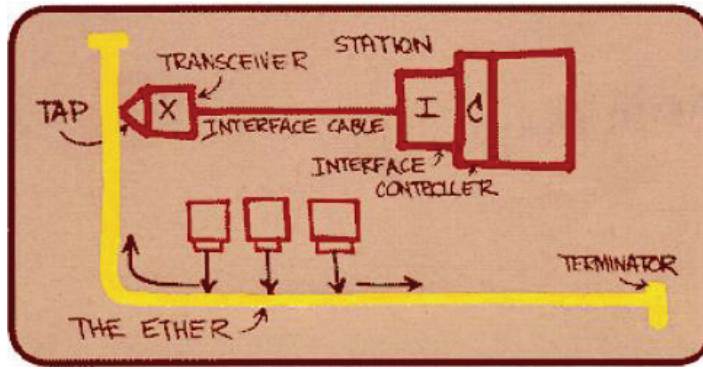
евентуални проблеми и разбирање на начинот како функционираат постоечките мрежи.

Првичните мрежи претставувале *mainframe* системи преку кои работеле преку посветени линии, во некои случаи и преку поголеми растојанија. Модерните компјутерски мрежи се појавиле со развојот на две мрежи: Semiautomatic Ground Environment (SAGE) била една од првите мрежи (1958) која била развиена со цел за поврзување на владините компјутери со радарски станици во Соединетите Држави и Канада. Во 60-тите години, истражувачите на MIT развиле систем наречен *Compatible Time-Sharing System (CTSS)* на еден IBM mainframe систем. Системот со временска поделба овозможува на повеќе корисници да извршуваат задачи истовремено на еден сервер. CTSS понатаму користел и модеми за поврзување на корисниците со лабораторијата преку обично повикување на одредени броеви, и овозможувал пристап од кампусот и од дома.

Една од првите комерцијализирани апликации која користела пристап од оддалечена локација за изведување на трансакции биле инсталирана за American Airlines во 1964. IBM-овиот SABRE систем за резервација поврзувал 2000 машини во 65 градови на IBM mainframe со користење на телефонски линии, и бил во можност да даде информација за било кој лет во рок од 3 секунди.

1.4.1 Мрежни комуникации

Mainframe системите користени во 60-тите и 70-тите биле засновани на „mainframe“ процесирање на сите информации. Терминалите поврзани со mainframe-от чекале на нивен ред, а информациите се процесирале и враќале кон секој терминален екран. Овие рани мрежи биле големи, скапи и комплицирани за користење. На mainframe мрежите додавањето на дополнителен терминал било сложена и скапа процедура. Но со развојот на мрежите се промовирал начин за делење на ресурсите и се овозможило повеќе корисници да се поврзат и комуницираат меѓусебно.



Слика 1.2: Цртежот од 1976 година, направен од Dr. Robert M. Metcalfe

Поголеми промени се случиле 70-тите години со создавањето на комуникациските протоколи. Првите мрежни протоколи биле *Token Ring*, *ARCNET* и *Ethernet*. Секој протокол користи различен метод за пристап до мрежата со компјутери, а најзначаен од трите бил Ethernet.

Роберт Меткалф (Robert Metcalf), како студент на Харвард прво го скицирал концептот за Ethernet на парче хартија како дел од неговата докторска теза, чија цел била испитување на преклопување на пакетите на *ARPAnet* и *ALOHAnet* мрежи. Денеска, Ethernet е најкористениот начин за пристап кон компјутерските мрежи.

1.5 Примери за компјутерски мрежи

Поимот компјутерски мрежи покрива повеќе различни видови на мрежи, поголеми и помали, познати и непознати. Имаат различна намена, големина и технологии. Во понатамошниот текст ќе биде даден краток преглед, за да се долови различноста која може да се најде во компјутерските мрежи.

Ќе започнеме со Интернет како најпозната мрежа, нејзината историја, еволуција и технологија. Потоа ќе биде претставен ATM кој се користи како јадро во поголемите телефонски мрежи, и е технички доста различен од Интернетот; потоа ќе биде опишан Ethernet, како доминантна технологија во локалните мрежи и на крајот ќе биде даден осврт на IEEE 802.11, стандардот за безжични локални мрежи.

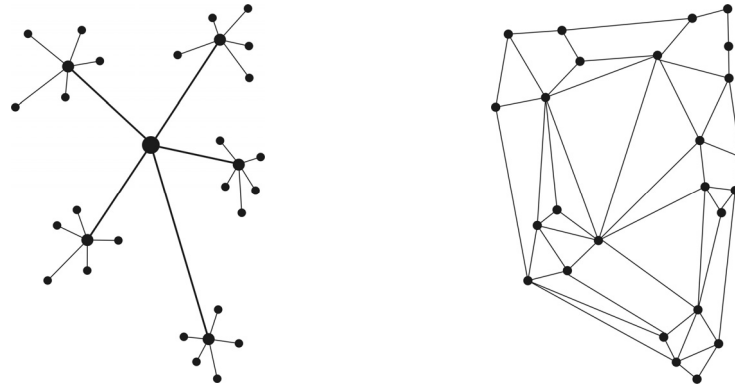
1.5.1 Интернет

Интернет е глобална мрежа. Пред сè, поимот интернет означува мрежа од мрежи, или интерконекција помеѓу повеќе компјутери. Постојат мали мрежи кои се поврзуваат меѓусебно и ја создаваат оваа структура. Интернет сè повеќе се именува како глобална мрежа на информации (голема интернационална - глобална база на податоци). Бројот на компјутерите на Интернет моментно се проценува на околу 150.000.000. Количеството на информациите кои се поставени на тие сервери е огромно и тешко може да се процени и реално прикаже колку навистина е нивниот обем. Уште од првите денови па до денес, Интернет прославил повеќе родендени, но тешко е да се каже кој е вистинскиот. Се мисли дека тоа е 1961, кога д-р Леонард Клајнрок на универзитетот MIT за прв пат објавил труд за техника на пакетско преспојување (*packet-swiching)*. Други пак наведуваат дека 1969 е година кога е роден Интернетот, затоа што тогаш Министерството за одбрана на САД ја избрало *Advanced Research Project Agency Network*, попозната како ARPANET, за истражување и развој на комуникациски и командни мрежи кои ќе го преживеат нуклеарниот напад. Во седумдесетите години се појавиле неколку значајни откритија кои го одбележале развојот на Интернетот како што ни е познат денеска, а потоа се случило и одвојување на ARPANET од воен експеримент во јавен истражувачки проект. Најверојатно најзначајниот момент се случил 1983, кога тогашната

мрежа поминала од NCP-а (*Network Control Protocol*) на TCP/IP (*Transmission Control Protocol/Internet Protocol*), со што се поминало на технологија која и ден денес се користи. Протоколите се стандарди кои овозможуваат комуникација помеѓу компјутерите со посредство на мрежата, а во 1983 година постоеле помалку од 1000 јазли споени на ARPANET со користење на примитивниот *Network Control Protocol*, кој наспроти многуте ограничувања бил употреблив во помалите мрежи, но не бил доволно флексибилен за поширока употреба. Како што експоненцијално се зголемувал ARPANET, се видело дека е потребен поширок пристап за комуникациските протоколи со цел задоволување на сè поголемите барања и создавање на посложени компјутерски мрежи. Винтон Церф и Роберт Кан започнале со работа на нов протокол многу поодамна од 1983 година, (т.е. 10 години порано се јавила идеја за тој протокол), а наредните години се развивале и усовршувале деталите на протоколот кој ќе ја измени историјата. Имплементацијата на TCP/IP во тоа време во тогашните оперативни системи траела 5 години, додека на ARPANET биле приклучени околу 400 јазли.

1.5.2 ARPANET

Приказната за ARPANET започнува во доцните 50-ти години; во екот на Студената војна, Министерството за одбрана (DoD) на САД сакало да командно-контролната мрежа опстане по нуклеарен напад. Во тоа време сите воени комуникации ја користеле јавната телефонска мрежа, што се сметала за ранлива на вакви напади. Причината за ова верување може да се воочи од сликата. Тука црните точки ги претставуваат централите, а на секоја од нив се приклучени илјадници телефони. Овие централи пак биле поврзани со централи на повисоко ниво и ја формирале националната хиерархија која овозможувала многу мала редундантност. Ранливоста на системот се состоела во фрагментација на системот во мали изолирани делови при уништувањето на неколку клучни централи.



Слика 1.3: Структура на телефонски систем и дистрибуиран преклопувачки систем.

Во 1960, Министерството за одбрана склучило договор со RAND корпорацијата да изнајде решение за проблемот. Еден од нивните вработени, Пол Баран (Paul Baran), претставил идеја за високо-дистрибуиран дизајн отпорен на грешки. Бидејќи патеките помеѓу било кои две централи станале многу подолги отколку што можеле да патуваат аналогните сигнали без појава на дисторзија, Баран предложил користење на технологија на преклопување на дигитални пакети во системот. По барањето да се направи прототип на овој систем, компанијата AT&T го одбила со објаснение дека таква мрежа не може да се изгради и идејата пропаднала.

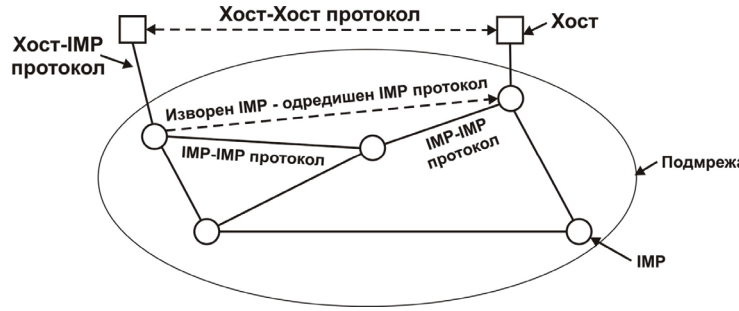
Агенцијата за напредни истражувачки проекти ARPA, Advanced Research Projects Agency се насочила кон истражување на мрежите. Еден од повиканите експерти, Весли Кларк (Wesley Clark), предложил формирање на пакетска мрежа каде што секој јазол би имал свој рутер, како што е прикажано на сликата. Сличен систем бил дизајниран и имплементиран под водство на Доналд Дејвис (Donald Davies) во Националната лабораторија за физика во Англија (National Physical Laboratory). NPL системот не бил национален систем, туку само демонстрирал како може да се изведе преклопувањето на пакети.

Подмрежата би се состоела од миникомпјутери наречени IMP (Interface Message Processors) поврзани со 56-kbps преносни линии. За повисока доверливост, секој IMP би требало да биде поврзан со најмалку два други IMP. Подмрежата претставува мрежа на датаграми, така што ако некои линии или IMP се уништени, пораките можат да бидат препратени преку алтернативни патеки.

Секој јазол на мрежата се состои од IMP и хост (host), поврзани во иста просторија со кратка врска. Хостот може да испраќа пораки до 8063 бита кон својот IMP, кој потоа ги разбива во пакети од најмногу 1008 бита и ги испраќа независно кон одредиштето. Секој пакет се прима во целост пред да биде препратен, така што оваа подмрежа претставувала прва зачувај-и-препрати пакетска мрежа (store-and-forward). ARPA објавила тендер за изградба на подмрежата, и во конкуренција на 12 компании ARPA го доделила тендерот на BBN, консултантска фирма од Кембриџ, Масачусетс во декември 1968, со задача да ја изгради мрежата и да го креира софтверот. BBN избрал да користи специјално модифицирани Honeywell DDP-316 миникомпјутери, со 12K 16-битни зборови меморија, како IMP. IMP уредите не користеле дискови, затоа што се сметало дека подвижните делови се недоверливи. Тие меѓусебно се поврзувале со 56-kbps линии изнајмени од телефонските компании. Софтверот бил поделен во два дела: подмрежа и хост. Подмрежниот софтвер се состоел од хост-IMP конекција, IMP-IMP протокол и изворен-до-одредишен IMP-протокол, создаден за подобрување на сигурноста.

Експерименталната мрежа била пуштена во употреба во декември 1969, со четири јазли UCLA, UCSB, SRI и Универзитетот во Јута. Овие четири биле избрани, затоа што сите имале поголеми договори со ARPA и сите имале различни и комплетно некомпатибилни компјутери. Целата мрежа брзо

нараснала со додавање на сè повеќе IMP уреди и наскоро се проширила по целата територија на Соединетите Држави.



Слика 1.4: Оригиналниот дизајн на ARPANET

Со цел да се помогне развојот на ARPANET, агенцијата ARPA вршела истражување за користењето на сателитските мрежи и мобилните пакетски радио мрежи. Притоа се покажало дека ARPANET протоколите не се погодни за работа преку повеќе мрежи, и ова согледување довело до истражувања на други протоколи, што пак довело до појава на TCP/IP протоколите во 1974. TCP/IP бил специјално изграден да управува со комуникацијата преку различни мрежи што станало сè позначајно со поврзување на сè повеќе мрежи на ARPANET.

За да се охрабри прифаќањето на овие нови протоколи, ARPA склучила неколку договори со BBN и Универзитетот на Калифорнија во Беркли, за да се интегрираат во Berkeley UNIX оперативниот систем. Истражувачите на Беркли развиле програмски интерфејс кон мрежата (sockets) и напишале повеќе апликации, алатки и управувачки програми за олеснување на умрежувањето. Повеќе универзитети ги прифатиле оперативниот систем 4.2BSD со TCP/IP, socket-ите и другите мрежни алатки, а со користењето на TCP/IP, поврзувањето на локалните мрежи со ARPANET станало едноставно, па повеќето го сториле тоа.

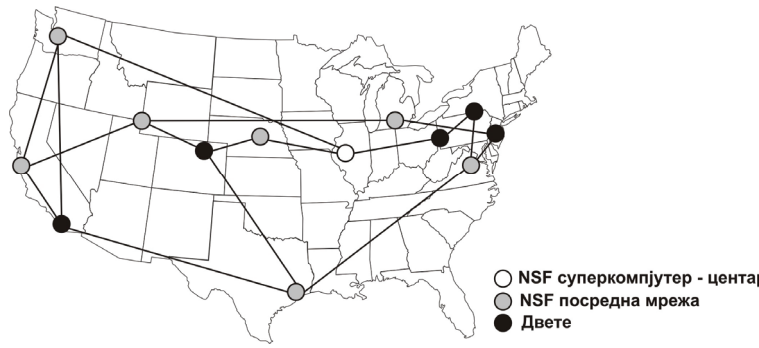
Во текот на 80-тите, дополнителни мрежи, особено LAN, биле поврзани кон ARPANET. Како што се зголемувал обемот, пронаоѓањето на хостовите станало многу сложено, така што бил претставен систем за имиња на домени DNS (Domain Name System) за организирање на машините во домени, кој ги пресликува нивните имиња во IP адреси. Оттогаш, DNS станала генерализирана и дистрибуирана база на податоци за чување на различни информации поврзани со именувањето.

1.5.3 NSFNET

Во доцните 70-ти, NSF (U.S. National Science Foundation) го увиделе огромното влијание на ARPANET врз истражувачката работа на универзитетите, овозможувајќи им на научниците да делат податоци и да

соработуваат на истражувачки проекти. Меѓутоа, за да се добие пристап на ARPANET, универзитетите требале да имаат склучено договор за истражувачки проекти со Министерството за одбрана, а повеќето немале.

Одговор на NSF било создавање на наследник на ARPANET кој би бил отворен кон сите универзитетски истражувачки групи. NSF решил да изгради „backbone“ мрежа и да ги поврзе шесте центри кои поседувале суперкомпјутери. Секој суперкомпјутер имал помал компјутер LSI-11 микрокомпјутер наречен „fuzzball“. Тие биле поврзани со 56-kbps изнајмени линии и формирале подмрежа со ист хардвер и технологија како и ARPANET. Додека софтверската технологија била различна: TCP/IP бил имплементиран уште од самиот почеток со што се формирала првата TCP/IP WAN мрежа. NSF исто така финансирал околу 20 регионални мрежи кои биле поврзани кон „backbone“, за да се овозможи на корисниците на илјадници универзитети, истражувачки лаборатории, библиотеки, музеи исл. да пристапат кон секој од суперкомпјутерите и да комуницираат еден со друг. Целата мрежа, вклучувајќи го „backbone“-от и регионалните мрежи била наречена NSFNET. И таа била поврзана со ARPANET преку линк помеѓу IMP и еден „fuzzball“ во серверската соба на Карнеги Мелон Универзитетот (Carnegie-Mellon).



Слика 1.5: NSFNET „backbone“ 1988

Заради големиот успех на NSFNET, NSF започнал со планирање на наследникот и склучиле договор со MERIT конзорциумот. Биле изнајмени оптички влакна со брзина од 448 kbps од страна на MCI за остварување на „backbone“-от верзија 2. Како рутери биле користени IBM PC-RT, а подоцна втората верзија била надградена на 1.5 Mbps.

Со помош на NSF, компаниите MERIT, MCI, и IBM формирале непрофитна организација - Напредни мрежи и сервиси - ANS (Advanced Networks and Services), како прв чекор кон комерцијализацијата. Во 1990, ANS ја презел NSFNET и ја надградил од 1.5-Mbps линкови на 45 Mbps за да се формира ANSNET. Оваа мрежа работела 5 години и потоа била продадена на America Online. Оттогаш разни компании почнале да нудат комерцијални IP услуги. За да се олесни транзицијата и да се осигури дека секоја регионална мрежа може да комуницира со сите други комерцијални мрежи, NSF склучил

договори со четири различни мрежни оператори за воспоставување на пристапни точки кон мрежата - т.н. NAP (Network Access Point). Тие оператори биле PacBell (San Francisco), Ameritech (Chicago), MFS (Washington, D.C.), и Sprint (New York City). Секој мрежен оператор кој сакал да овозможи „backbone“ услуга кон NSF-регионалните мрежи, морал да се приклучи кон сите NAP точки. Во текот на 90-тите, многу други држави и региони исто така изградиле национални истражувачки мрежи, како што се EuropaNET и EBONE во Европа, кои започнале со 2-Mbps линии и потоа се надградиле со 34-Mbps линии.

1.5.4 Користење на Интернет

Откако TCP/IP станал официјален протокол, бројот на мрежите, машините и корисниците поврзани на ARPANET започнал брзо да расте, а откако NSFNET и ARPANET биле меѓусебно поврзани, порастот станал експоненцијален. Повеќе регионални мрежи се поврзале и се поставиле врски и кон Канада, Европа и Пацифик. Во средината на 80-тите, множеството на мрежи почнало да се нарекува интернет, а подоцна и Интернет. Сврзното ткиво на Интернет е TCP/IP референтниот модел и стекот на протоколи TCP/IP, што овозможило користење на универзални сервиси.

Традиционално во периодот од 1970-те до 1990-те години, Интернетот и неговите претходници имале четири главни апликации:

Електронска пошта (E-mail). Можноста да се состави, испрати и прими електронска пошта постоела уште од деновите на ARPANET и е многу популарна, како примарен начин за интеракција со надворешниот свет

Новински групи (News). Новинските групи се специјализирани форуми каде што корисниците ги делат заедничките интереси со рамена на пораки. Постојат илјадници групи, технички и не-технички, вклучувајќи компјутерска техника, наука, рекреација, политика и други. Секоја група има сопствен назив, стил и прилагодување.

Далечински пристап (remote login). Користејќи ги telnet, rlogin, или ssh програмите, корисниците насекаде на Интернет може да се пријават на било која машина на која имаат сопствен кориснички налог (account).

Пренос на датотеки (file transfer). Со користење на FTP програми, корисниците може да копираат датотеки од еден компјутер кој е на Интернет, на друг. На тој начин станале достапни голем број на податочни бази, текстови и други информации.

Сè до раните 90-ти, Интернетот беше раширен кај академската заедница, владите и индустриските истражувачи. Една нова апликација наречена WWW (World Wide Web) предизвика појава на нови не-академски корисници на мрежата. Апликацијата била развиена од страна на CERN, и не сменила ништо во начинот на работењето, туку уште повеќе ја олеснила употребата на Интернетот.

Заедно со Mosaic прелистувачот, WWW овозможил поставување на повеќе страници на информации кои содржат текст, слики, звуци и видео, со вметнати врски кон други слични страници кон други сајтови. Со активирање на линкот, корисникот наеднаш се префрлувал кон страницата насочена со тој линк. Се појавиле многу различни видови на страници со различни информации во многу кратко време, како што се мапи, берзански информации, библиотечни каталози, снимени радио емисии како и комплетни книги, а многу корисници имаат и сопствени страници.

Поголемиот раст настанал во текот на 90-тите кога компаниите наречени Интернет сервис провајдери ISP (Internet Service Providers), почнале да нудат можност на индивидуални корисници во домашни услови да повикаат една од нивните машини и да се поврзат на Интернет, добивајќи пристап кон сервисите за електронска пошта, WWW и други. На тој начин, од корен се сменила природата на мрежата - од академска и воено-истражувачка, во јавен сервис сличен на телефонскиот систем.

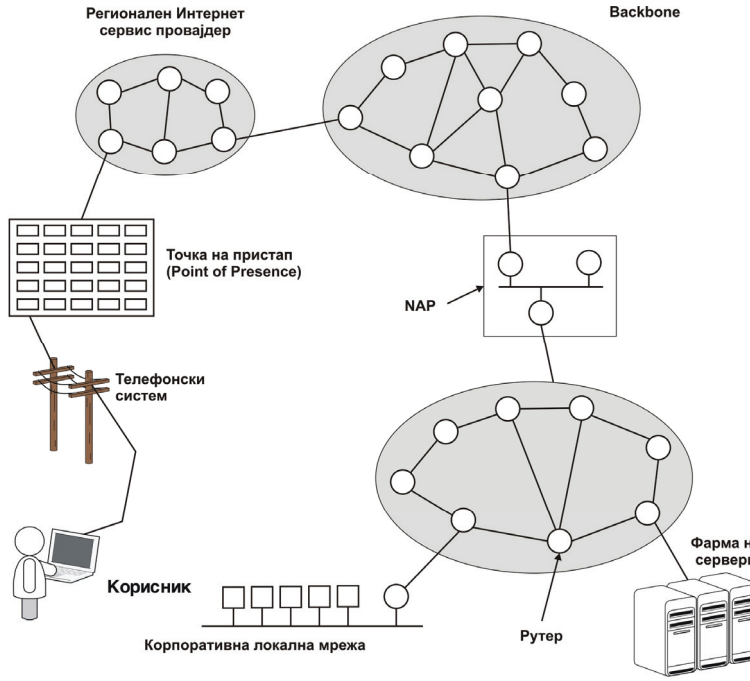
1.5.5 Архитектурата на Интернет

Клиентите во домашни услови го повикуваат нивниот ISP преку „dial-up“ телефонска линија како што е прикажано на сликата. Модемот претставува картичка за проширување, вградена во PC, која врши претворање на дигиталните сигнали создадени од компјутерот во аналогни, кои се соодветни за пренесување на телефонскиот систем. Овие сигнали се пренесуваат до точката на присуство на ISP - POP (Point of Presence), од каде се отстрануваат од телефонскиот систем и се вметнуваат во регионалната мрежа на сервис-провајдерот.

Од оваа точка па понатаму, системот е целосно дигитален и пакетски. Регионалната мрежа на ISP се состои од поврзани рутери во различни градови кои ги опслужува тој провајдер. Ако пакетот е наменет за хост директно поврзан со ISP, пакетот се испорачува директно, во другите случаи се предава на „backbone“ операторот.

На врвот се наоѓаат главните „backbone“ оператори, компании како што се AT&T и Sprint. Тие оперираат со големи интернационални „backbone“ мрежи со илјадници рутери поврзани со оптички влакна со големи пропусни опсези.

Поголемите компании и сервисите за хостирање на web страници кои управуваат со серверски фарми (машини кои опслужуваат повеќе илјадници страници во секунда) обично се поврзани директно на „backbone“-от. Ако пакетот доделен на „backbone“ е наменет за ISP или компанија опслужувана до страна на „backbone“, се испраќа на најблискиот рутер и се предава на него. За да се овозможи префрлување на пакетите помеѓу „backbone“-ите, сите поголеми се поврзуваат со NAP точките. Во суштина NAP претставува просторија исполнета со рутери, барем по еден за секој „backbone“. LAN мрежата во просторијата се поврзува со сите рутери, така што пакетите може да бидат пренасочени од било кој „backbone“ кон друг „backbone“.



Слика 1.6: Приказ на артхитектурата на Интернет

Дополнително за поврзување со NAP точките, поголемите „backbone“ имаат повеќекратни директни конекции помеѓу нивните рутери, техника позната како приватен пиринг (private peering). Еден од парадоксите на Интернет е и што сервис-провајдерите кои јавно се натпреваруваат еден со друг за корисници, обично имаат воспоставен меѓусебен пиринг.

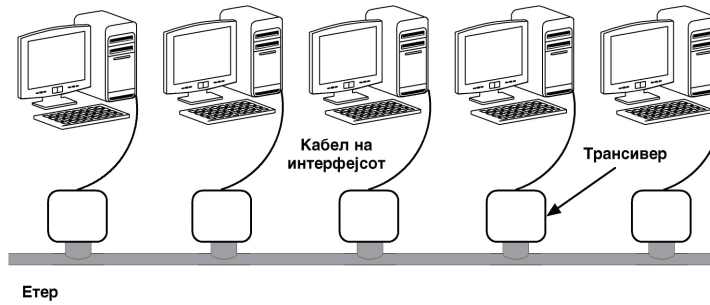
1.6 ETHERNET

Интернет и ATM беа дизајнирани за умрежување во широка област (WAN). Но, многу компании, универзитети и други организации имаат голем број компјутери што мораат да се поврзат. Потребата од вакво нешто довела до издигнување на локалната мрежа (LAN). Во овој дел ние ќе зборуваме за најпопуларниот LAN - Ethernet.

Студентот Bob Metcalfe кој дипломирал на М.И.Т и потоа ги продолжил докторските студии на Харвард, со неговиот колега David Boggs, ја дизајнирале и ја имплементирале првата локална мрежа. Тие системот го нарекле ETHERNET по етерот, преку кој се мислело дека се пренесува електромагнетската радијација.

Преносниот медиум тука не е воздухот, туку еден дебел коаксијален кабел (етер) долг до 2.5 км (со засилувачи на секои 500м). До 256 машини можеле да се поврзат со системот на примо-предаватели или трансивери поставени на каблите, а кабелот со кој се поврзале повеќе машини паралелно се викал „multidrop“ кабел. Системот вршел пренос со брзина од 2.94 Mbps. Кај Ethernet се направени големи подобрувања во однос на ALOHANET, и пред процесот на пренос, првин се ослушнува кабелот дали веќе некој јазол врши пренесување на податоци. Ако медиумот е зафатен, испраќачот останува да чека до неговото ослободување. На тој начин се избегуваат колизиите и се овозможува поголема ефикасност.

И покрај тоа што се врши ослушнување пред преносот, може да се појави проблем: што ќе се случи ако два или повеќе компјутери чекаат додека не заврши тековниот пренос и потоа сите почнат одеднаш. Решението е - секој компјутер да ослушнува при пренесувањето и ако се детектираат пречки на сигналот- да се блокира етерот за да ги алармира сите испраќачи. Потоа се повлекува од преносот и чека случајно време пред повторен обид.



Слика 1.7: Поврзување на работните станици на Ethernet преку кабли со трансивери

Ethernet-от на Xerox бил толку успешен, така што DEC, Intel и Xerox направиле нацрт-стандард во 1978 за 10Mbps Ethernet наречен DIX стандард. Со две мали измени DIX станал IEEE 802.3 во 1983. Ethernet продолжи да се развива, и сè уште се развива, со појавата на верзиите со брзина на пренесување - 100 Mbps, 1000Mbps и поголеми. Исто така усовршено е каблирањето, како и мрежната опрема - хабови и преклопници.

1.7 Безжични LAN мрежи: 802.11

Набрзо по појавувањето на преносните компјутери (notebook), повеќето корисници имале потреба од безжично поврзување кон Интернет или локалните мрежи. Како последица на тоа, различни развојни групи започнаа дефинирање на начините за постигнување на таа цел. Најпрактичен начин да се овозможи комуникацијата, е да се опремат и канцеларијата и компјутерите со радио примо-предаватели со краток досег. Ова доведе до тоа да безжичните LAN-ови бидат продавани и купувани од различни компании, а настана проблем што меѓусебно не беа компатибилни.

Заради тоа на IEEE комитетот, кој го создал жичниот LAN стандард, му била доделена задача за стандардизација на безжичниот LAN. Стандардот се појави под ознаката 802.11. Во вообичаениот говор името му е познато како WiFi. Предложениот стандард мора да работи на два начина:

1. Во присуство на базна станица
2. Во отсуство на базна станица

Во првиот случај сите комуникации мораа да одат низ базната станица наречена *точка на пристап (access point)* во 802.11 терминологијата. Во вториот случај компјутерите би комуницирале еден со друг директно. Овој начин во поново време е нарекуван и како „ad hoc networking“. Типичен пример се двајца или повеќе луѓе кои седат во просторија неопремена со безжичен LAN, чии компјутери комуницираат директно. Двата начина се илустрирани на сликите 1.8а. и 1.8б.

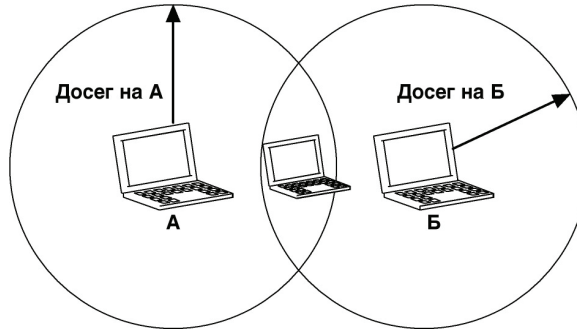
Слика 1.8: (a) Безжични мрежи со базна станица, (b) Ad hoc networking.

Некои од многуте предизвици кои што се појавиле биле: да се најде соодветна фреквенција што е слободна, по можност во светски рамки; да се реши проблемот кој се однесува на радио-сигналите кои имаат конечен досег; да се обезбеди приватноста на корисниците; да се земе во предвид мобилноста на компјутерите; и конечно, да се гради систем со доволен пропусен опсег, земајќи ја предвид и економичноста.

Процесот на стандардизација започна во средината на 90-тите. Ethernet веќе доминираше со LAN, па Комитетот одлучи да го направи 802.11 компатибилен со Ethernet над второто, податочно ниво (data link). Особено треба да биде возможно да се испрати IP пакет низ безжичниот LAN, на ист начин како што ожичениот компјутер испраќа IP пакет низ Ethernet. На почетокот компјутерот поврзан на Ethernet го проверува сигнал-етерот пред испраќањето на сигналот. Само ако медиумот е слободен, тогаш компјутерот започнува да испраќа сигнали. Овој механизам не функционира кај безжичниот LAN.

Примерот е илустриран на слика 1.9. Да претпоставиме дека компјутерот А испраќа сигнал кон компјутерот В, но радио-сигналот на испраќачот А е прекраток за да стигне до компјутерот С. Ако С сака да испрати сигнал кон

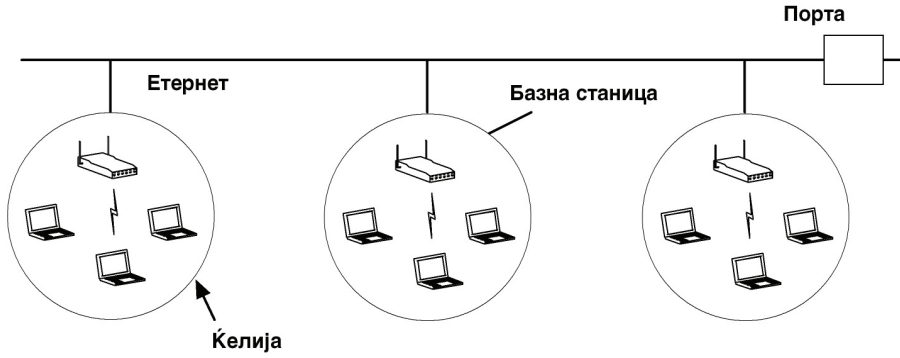
В може да провери дали фреквенцијата е слободна, но фактот дека не наоѓа ништо, значи дека испраќањето нема да биде успешно.



Слика 1.9: Опсегот на радио-сигналот може да не го покрива целиот систем

Вториот проблем што мора да се реши е дека радио сигналот може да биде рефлектиран од цврсти предмети, така да може да биде примен повеќе пати (по многу патишта). Оваа интерференција резултира со она што се нарекува „*multipath fading*“ (придушување на сигналот заради поминување по повеќе патишта до приемникот).

Третиот проблем е што, постоечкиот софтвер не бил подготвен за мобилноста. На пример, многу текст процесори имаат листа на печатачи, од која корисниците можат да изберат од кој печатач да го печатат својот документ. Кога компјутерот чијшто текст процесор се стартува, е сместен во нова околина, изградената листа на печатачи станува неважечка.



Слика 1.10: Повеќеќелиска 802.11 мрежа

Четвртиот проблем е ако преносниот компјутер е надвор од границите на базната станица што ја користи и се наоѓа во досегот на друга базна станица; потребно е да се најде начин за нивно меѓусебно комуницирање. Овој проблем се јавува и кај мобилните телефони, и потребно е да се најде решение за него. Мрежите се составени од мноштво на ќелии, секоја со сопствена базна станица, но базните станици се конектирани со Ethernet како

што е покажано на слика 1.10. Конекцијата помеѓу 802.11 системот и надворешниот свет е наречена *порта (portal).*

После завршувањето на својата задача, во 1997, Комитетот дојде со стандард каде што е опишано дека безжичниот LAN ќе работи и на 1 Mbps и на 2 Mbps. Во 1999 беа донесени два нови стандарди: 802.11a стандардот користи повисока фреквенција и работи на брзина од 54 Mbps; 802.11b стандардот користи иста фреквенција како и 802.11a, но користи поинаква техничка модулација и остварува брзина од 11Mbps. Се појавува уште една варијанта, 802.11g, која користи техничка модулација од 802.11a, но фреквенција како 802.11b.

2 OSI РЕФЕРЕНТЕН МОДЕЛ

Комуникацискиот систем се состои од многу компоненти, а се однесува на најмалку две "страни" што сакаат да комуницираат. Компјутерската мрежа се состои од два или повеќе јазли (компјутери), поврзани преку одреден комуникациски канал. Треба да се истакне дека поврзувањето во мрежа овозможува зголемена функционалност, делење на ресурси итн., и дека Интернет претставува всушност мрежа од многу поврзани мрежи. Мрежите вообичаено претставуваат сложени структури. Следејќи го принципот раздели па владеј, модерните мрежи се дизајнираат, конструираат и опишуваат како повеќе-слојна архитектура, т.е. дефинирани се мрежни стандарди и протоколи за поврзување на различните слоеви (нивои) од мрежата. Во основа, повеќе-слојните протоколи се развиени заради следните цели:

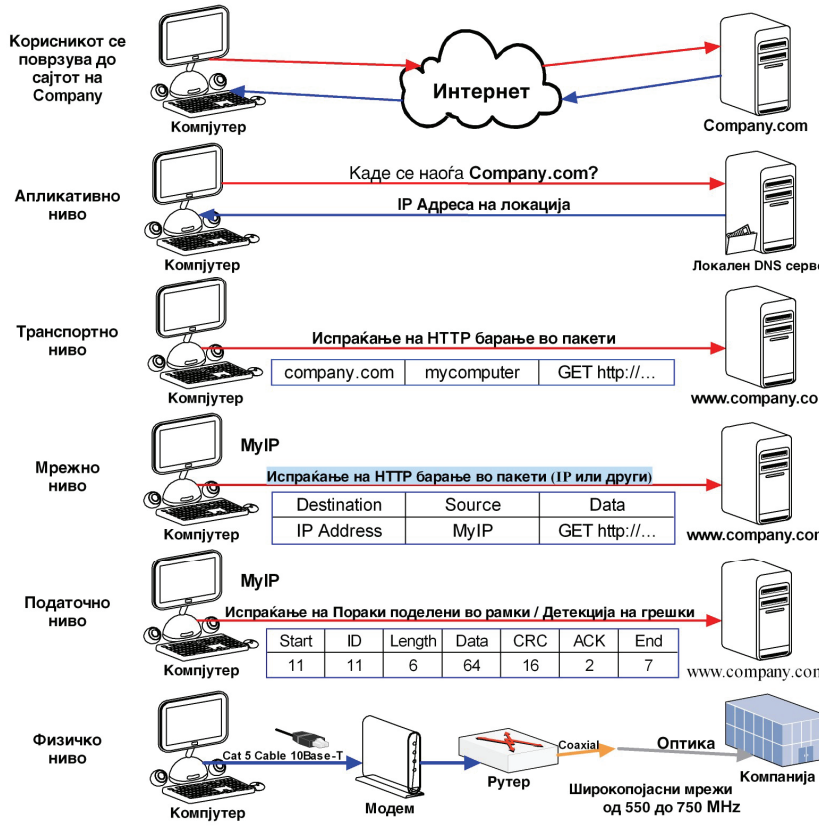
- Ја редуцираат сложеноста на мрежата, т.е. нејзиниот дизајн и имплементација.
- Овозможуваат „peer-to-peer" комуникација помеѓу соодветните слоеви во мрежата.
- Овозможуваат да се прават модификации на одредено ниво, кои не би ги засегнале останатите слоеви.

Кај повеќе-нивоовската архитектура, сложениот мрежен модел се дели на повеќе модули, кои припаѓаат на различни нивоа. Промените во дизајнот и конструкцијата на едно ниво, немаат значително влијание врз функционирањето на другите нивоа. На пр. промената на алгоритамот за корекција на грешка кај пониските нивои, не влијае на рутирачкиот алгоритам од повисоките нивои. Од друга страна, енкрипцискиот алгоритам на презентациското ниво кај испраќачот, е во тесна корелација со декрипцискиот алгоритам кај презентациското ниво на примачот. Компонентите од секое ниво кај испраќачот, комуницираат виртуелно со соодветното ниво кај примачот. Сепак, податоците реално се движат од највисокото ниво кај испраќачот кон пониските нивоа, па преку медиумот пристигнуваат кај примачот, и таму патуваат од најниското кон највисокото ниво (слика 2.1). Секое ниво кај испраќачот додава свое заглавје (header) кон податоците, а кај примачот заглавјата се анулираат и на крај остануваат чисти податоци.

Протоколите се подредени во нивои со цел да извршуваат точно одредени мрежни функции. Секое ниво користи услуги од нивото што е под него, а дава услуги на нивото над него. Во 1983г. ISO го дефинирал седум-нивоовскиот отворен систем за интер-конекција (ОСИ), со цел да воспостави стандард што ќе опише комплетното множество од протоколи, наменети за хетерогени мрежни околини.

Мрежната архитектура според ОСИ е поделена во седум нивои, почнувајќи од најдолното – физичко, па до најгорното – апликативно ниво:

1. Физичко ниво – го опфаќа медиумот за пренос и форматот на сигналите кои се пренесуваат во бинарен облик. Ова ниво се грижи за механичките и електричните компоненти на мрежата, т.е. води сметка да битовите испратени на едната страна, бидат примени на другата страна.
2. Податочно (data link) ниво – служи за пристап и контрола на медиумот за трансмисија. Ова ниво се справува со регулацијата на протокот, форматирање на пакетите во рамки (frames) и детекција и корекција на грешки.
3. Мрежно ниво – ги форматира индивидуалните податочни пакети. Одговорно е за рутирање на пакетите низ мрежата; се справува и со адресирањето и испораката на податоците. Рутерите и IP-протоколот припаѓаат на мрежното ниво.



Слика 2.1: Седум-нивоовски ОСИ модел – peer to peer комуникацијата помеѓу нивоата е виртуелна, додека вистинскиот тек на податоци е од горе-надолу, па од доле-нагоре.

4. Транспортно ниво – се грижи за точен редослед на достава на пакетите. Главна задача на ова ниво е интегритетот на податоците - преносот на податоци помеѓу јазлите да биде сигурен и навремен. Два главни транспортни протоколи се TCP и UDP.
5. Сесиско ниво – ја воспоставува конекцијата помеѓу програмите кај испраќачот и примачот. Ова ниво управува со дијалогот, а исто така го синхронизира и мрежното време.
6. Презентациско ниво – служи за конверзија и приказ на податоците во соодветен формат. Примарната функција на ова ниво се синтаксата и семантиката на податочната трансмисија. ASCII и EBCDIC-конверзиите и крипто-заштитата се имплементирани во ова ниво.
7. Апликациско ниво – опфаќа апликациско-специфични информации за податоците што се пренесуваат. Ова ниво претставува интерфејс кон корисникот и дел од него се програмите: Telnet, FTP, E-mail client, Web browser.

Кај типичните мрежи, највисоките нивои – апликациското и презентациското, обично се реализирани преку апликативни програми (web browser, e-mail client и сл.). Средните нивоа се често дел од оперативниот систем (драјвери, TCP/IP протокол), додека најниските нивои го претставуваат мрежниот хардвер (преклопници, кабли итн.).

Иако денес има тврдења дека ОСИ моделот не е доследно имплементиран кај ниедна мрежа, и се предлагаат нови, скратени модели (како на пр. 4-слојниот TCP/IP-модел), може да се смета дека ОСИ претставува костур за сите постоечки и идни мрежни концепти.

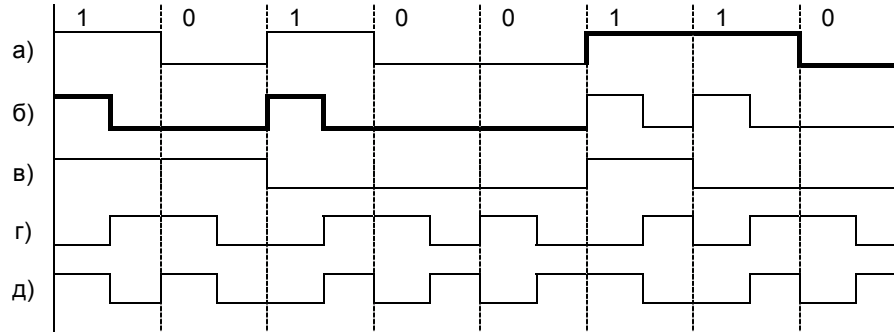
2.1 Физичко ниво

Физичкото ниво е задолжено за пренос на “чисти битови“ преку комуникацискиот канал. Неговиот дизајн треба да обезбеди да испратениот податок ’1’ биде примен како ’1’, а не како ’0’. Типични прашања овде се - со колку волти е прикажана ’1’, а со колку ’0’, колку микросекунди трае битот, дали трансмисијата се одвива истовремено во двете насоки, како се воспоставува иницијалната конекција, како конекцијата се прекинува кога ќе заврши преносот, колку пинови има мрежниот конектор и за што се користи секој од пиновите. Дизајнот на ова ниво се бави со механичките, електричните и процедуралните интерфејси, како и со физичкиот медиум за пренос (бакарни и оптички кабли, сателитски и безжичен пренос).

2.1.1 Кодирање на податоците

Дигиталните податоци ретко се пренесуваат во нивната оригинална форма. Кодирањето е процедура што ги претвора оригиналните сигнали во различна форма поради различни причини (подобро искористување на каналот, поголема ефикасност, помала рата на грешки, синхронизација, безбедност

итн.). Постојат повеќе методи за кодирање што се прават пред да започне трансмисијата. И модулацијата е форма на кодирање што се користи за кодирање на дигитални податоци што се пренесуваат преку аналогна линија. Кодирачките техники се користат и за детекција и корекција на грешки, за податочна компресија и за енкрипција (ќе бидат споменати и подолу).



Слика 2.2: Различни техники за дигитално кодирање: а) NZR-L кодирање, б) RZ кодирање, в) NZR-I кодирање, г) Манчестерово кодирање, д) Диференцијално Манчестерово кодирање.

Во својот чист формат, податочниот ток е низа од бинарни податоци што се пренесуваат како ниска волтажа (битот 0) и висока волтажа (битот 1); ако сигналот има ист поларитет велиме дека е униполарен – во спротивно негативниот сигнал може да претставува 0, а позитивниот 1. За шемата за кодирање велиме дека е поларна. 1 и 0 се наречени импулс и празнина соодветно. Кога бинарните податоци 0 и 1 се прикажани со различен напон, кодирањето е наречено NZR-L (non-return-to-zero level), Слика 2. а). Кај ова кодирање, битот 0 или 1 се пренесува со помош на сигнал. Но и повеќе битови се пренесуваат со еден сигнал. ISDN и ADSL користат т.н. 2B1Q (2 бинарно, едно квадрантно) кодирање за да пренесат 2 бита истовремено со различни напонски нивоа. Кај NZR-L напонското ниво е константно во бит-интервалите. Заради едноставност, ова кодирање се користи за внатрешниот податочен трансфер во компјутерскиот хардвер.

Return-to-zero (RZ) кодирањето прави премин (транзиција) од низок-кон-висок напон на почеток на сигналот 1, а потоа од висок-кон-низок на средина на битот – Слика 2. б). Сигналот 0 нема транзиција на почетокот. NZR-L кодирањето може да предизвика проблем во комуникациите ако се сменат жиците кај плетената парица. (Сите 1 и 0 ќе бидат инвертирани). Варијација на NZR-L користи транзиција на почеток од сигналот 1, а нема транзиција на почеток од 0. Со други зборови, ги споредува напоните на двата претходни сигнали, а не ја зема апсолутната вредност на сигналот, за да одреди дали се пренесува 0 или 1. Ако двата напони се различни, се пренесува 1, ако се исти – се пренесува 0. Ова кодирање е наречено NZR-Invert-on-ones, т.е. NZR-I. NZR-I нема проблем со промена на жиците и ја подобрува ратата на грешка кога комуникациските услови се влошени. NZR-

I е пример на диференцијално кодирање. Диференцијалното кодирање има слабост – ако се пропушти една транзиција на сигналот, сите 0 и 1 ќе бидат инвертирани.

И двете NZR- L и NZR-I одржуваат константен напон за време на сигналот. Тие се лесни за имплементација. 1 и 0 имаат подеднакви шанси да се појават во преносот, и има шанси 50:50 дека нема да се промени претходниот бит, па напонот се менува поретко, отколку во случај на поединечни битови. NZR кодирањето, на тој начин, ефикасно го користи пропусниот опсег (bandwidth). Ни NZR-L, ни NZR-I не овозможуваат синхронизација. Така, податочната низа 000010000 може погрешно да се интерпретира како 00001 или 10000, во зависност од бројачот.

Манчестер и диференцијалното Манчестер кодирање се воведени за да овозможат синхронизирачки можности. Кај Манчестер кодирањето, се користи транзиција на средина од секој бит-интервал и за податоците и за часовникот. Транзицијата ниско-во-високо прикажува 1, а високо-во-ниско 0 (Слика 2. г)). Кај диференцијалното Манчестер кодирање, 0 се прикажува со транзиција на почеток од интервалот, а 1 се прикажува со отсуство на транзиција на почеток на интервалот. Секогаш има транзиција на средина на интервалот, заради синхронизирачки цели (Слика 2. д)). Диференцијалното Манчестер кодирање има предност над останатите техники за кодирање – тоа е отпорно на шум.

Манчестер и диференцијалното Манчестер кодирање се двофазни кодови, кои се многу раширени во компјутерските мрежи. Ethernet и CSMA/CD користат Манчестер кодирање со медиуми коаксијален кабел и плетена парица (twisted pair). Диференцијалното Манчестер кодирање се користи и кај IEEE 802.5 Token Ring, пришто користи кабел - плетена парица (twisted pair).

Двофазното кодирање е лесно за имплементација. Тоа не содржи наизменични компоненти и е поотпорно на грешки во однос на NZR кодирањата. Сепак, бидејќи бара барем една транзиција по бит-интервал, а во пола случаи има и 2 транзиции, импулсите се со половина ширина од оригиналната. Затоа трошат двојно повеќе пропусен опсег (bandwidth) во однос на NZR кодирањата. Ова го ограничува двофазното кодирање да се применува само кај брзите мрежи, на пр. 100 Mbps FDDI.

2.1.2 Мултиплексирање

Мрежата може да се состои од милиони компјутери, и е невозможно сите да се поврзат со директна линија. Сепак, може да се реализира целосна поврзаност преку делење на физичките врски. Техниките за мултиплексирање овозможуваат повеќе комуникациски канали да се сместат во една физичка врска – слично со мулти-таскинг опциите кај компјутерите. Постојат повеќе различни техники за мултиплексирање. Во традиционалната телефонија со аналогна трансмисија, најпогодно е да се примени мултиплексирање со делење на фреквенцијата (FDM). За податочната

комуникација и компјутерските мрежи – најпогодно е мултиплексирањето со делење на времето (TDM). За дигиталните мобилни телефони сè поголема популарност има мултиплексирањето со делење на кодот (CDM).

Фреквентно мултиплексирање (FDM)

Идејата на FDM техниката потекнува од радио емитувањето. Воздухот се третира како голем комуникациски канал. Различните радио бранови се пренесуваат без интерференција, бидејќи како носачи користат бранови со различна фреквенција. Разликата во фреквенцијата на носачот е она што ги разликува сигналите кај приемникот. Аналогните FDM сигнали се пренесуваат преку физичка врска (кабел) на различна фреквенција, како на пример што се пренесува телевизискиот сигнал – и преку воздух, и преку коаксијален кабел.

Кај класичниот телефонски систем, дванаесет 4000 Hz гласовни канали се групирани заедно, модулирани и мултиплексирани во 60-108 KHz носач. Само 3000 Hz се користат за правиот сигнал (300-3300 Hz), додека крајните 500 Hz лево и десно служат за избегнување на интерференцијата. Кај приемникот постојат ниско- и високо-фреквентен филтер, кои ги одвојуваат корисните сигнали од носачот.

Временско мултиплексирање (TDM)

Дигиталните сигнали, како гласот, сликите и податоците, се пренесуваат преку мултиплексирање со делење на времето TDM, при што протокот на податоците се дели во мали временски слотови. TDM се имплементира со доделување на делови од секој канал во секој временски слот. Кај TDM повеќе комуникациски канали делат иста врска со голема податочна рата (т.н. проток=bandwidth), т.е. се доделува посебен bandwidth за секоја апликација (корисник). Мултиплексерот за TDM циклично ги скенира податоците што пристигнуваат од различни влезни порти. Се земаат делови од податоците (на пр. бајти или блокови), и се вметнуваат во рамки во една многу брза комуникациска линија. Така TDM системот ги прима влезните дигитални податоци. За пренос на податоците, потребна е канална банка која врши семплирање, квантизација и кодирање на податоците со помош на PCM (импулсно-кодна модулација), т.е. аналогните сигнали ги претвора во дигитални и претставува интерфејс помеѓу изворот на податоци и телефонската (кабелската) мрежа.

Потребна е синхронизација помеѓу уредите што испраќаат и уредите што примаат податоци. Најпознати системи што користат TDM се T1 и E1, кои се развиени во осумдесеттите години, во САД, од компанијата AT&T.

Code Division Multiple Access (CDMA)

Благодарение на нејзината ниска цена, и развојот на микрочипот со кој се намалиле димензиите на уредите, една стара техника за мултиплексирање

(развиена пред 50 години) – техника со поделба на кодот CDMA, зема повторно замав кај мобилната телефонија.

Важна особина на мобилните уреди е можноста за повеќе пристапи, т.е. поддршка на повеќе корисници истовремено. Кај мобилната телефонија ова значи дека повеќе корисници можат да делат заедничко множество од радио канали, па корисникот секогаш добива пристап до некој канал, и тоа не мора да е истиот канал. CDMA користи иновативен „multiple-access“ метод за да дефинира како радио спектарот се дели во канали и како каналите се алоцираат на секој корисник во системот.

CDMA ја користи теоријата на кодирање, т.е. сложени алгоритми за да ги распореди податоците во повеќе канали од целиот фреквентен спектар. Мобилните телефони почнуваат со стандардна рата од 9600 bps, а потоа се шират во трансмисиона рата од 1.23 Mbps. Ширењето значи дека се применуваат дигитални кодови на податоците кај корисниците на една базна станица. Податочните битови од еден телефон се пренесуваат заедно со другите сигнали од други корисници од таа станица. Кога сигналот ќе се прими, кодовите се бришат од оригиналниот сигнал со што се раздвојуваат корисниците и се враќа ратата од 9600 bps. Кодовите кои се заеднички за мобилниот телефон и базната станица се т.н. псевдо-случајни кодни секвенци. Сите корисници делат ист дел од радио спектарот.

Клучот за високиот капацитет на CDMA е едноставен – наместо да користи константна моќност во [dB] – трансмитерите ја примаат моќноста од корисниците, па секој корисник зафаќа ист спектар.

Браново мултиплексирање (WDM)

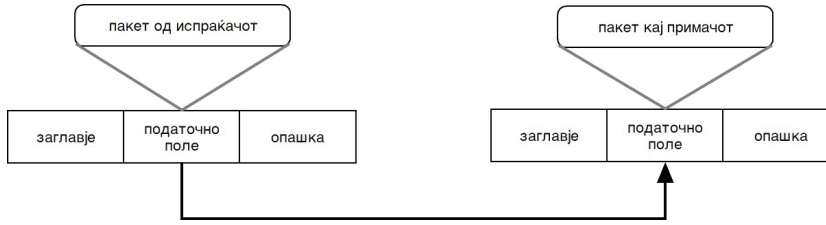
Брановото мултиплексирање се користи кај фибер-оптичките системи за многу брза трансмисија. Секој оптички канал може да пренесува податоци преку едно оптичко влакно со рата до 10 Gbps. За 128-канален WDM преклопник (switch), секое влакно ќе може да пренесе 1.28 терабити во секунда, што е еквивалент на 16 милиони телефонски линии.

WDM е слично со фреквентното мултиплексирање, и кај него различните бои светлина претставуваат носители за пренос на податоци преку влакното. WDM овозможува повеќе канали да делат исто влакно, со што се зголемува брзината без инсталирање на дополнителни влакна. WDM е исто важна како средство за поставување на податочни центри (data centers), како и за случаи на бекап при несреќи и сл. Главната предност на WDM е големиот капацитет на веќе постоечките фибер- оптички мрежи, и сè што треба да направи корисникот е да стави бранов мултиплексер на двата краја од линијата. WDM не бара рипитер до растојание од 10 км, а преклопниците се независни од протоколот за комуникација (ATM, FDDI или друг тип на рамка).

2.2 Податочно (Data Link) ниво

Главна задача на податочното ниво е да ги прифати "чистите битови" и да ги спроведе без никакви грешки (во преносот) кон мрежното ниво. Тоа ја извршува оваа задача на тој начин, што кај испраќачот - ја дели пораката во податочни рамки (data frames), големи во ранг на kB. Секоја рамка се состои од заглавје (header), поле со податоци, и опашка (trailer), како на слика 2.3. Испраќачот ги испраќа рамките секвенцијално, а од примачот бара потврда (acknowledgement frame) дека секоја рамка е примена. Бидејќи физичкото ниво испраќа и прифаќа само битови, без да се грижи за нивната структура и значење, податочното ниво е тоа што ги формира границите на рамките. Ова се прави со додавање на посебна секвенца од битови на почеток и крај од секоја рамка. Ако истата бит-секвенца случајно се најде и во телото на пораката, мора да се води сметка, таа да не биде интерпретирана како граничник на рамката.

Иако во ова поглавје ќе зборуваме за протоколите на податочното ниво, како на пример корекцијата на грешки и податочниот тек, истите функции се застапени и кај транспортното и другите нивои.



Слика 2.3: Врска помеѓу пакетите и рамките

Шумот на линијата за пренос може целосно да ја уништи рамката. Во овој случај, софтверот на податочното ниво треба да обезбеди повторна ретрансмисија на целата рамка. Сепак, повеќе-кратното испраќање на една рамка може да доведе до дуплирани рамки кај примачот. Дуплирана рамка се праќа само во случај рамката за потврда од примачот, да е изгубена. Податочното ниво се грижи за проблемите, како што се изгубени, оштетени и дуплирани рамки.

Друг проблем за кој треба да се грижи ова ниво (а и погорните исто така), е како брз испраќач да се усогласи со бавен примач на податоци. Се применуваат одредени механизми за регулација на сообраќајот, со цел на испраќачот да му се стави на знаење колкав е бафер-просторот на примачот во даден момент. Честопати, регулацијата на податочниот тек и контролата на грешки - се интегрирани во еден модул.

Ако линијата за пренос на податоци е двонасочна, тоа воведува нови компликации за кои е задолжено податочното ниво. Проблемот е што рамките за потврда од B кон A, ја зафаќаат линијата во момент кога A испраќа наредна податочна рамка кон B. Постои интелигентно решение за

овој проблем, т.н. piggybacking. Мрежите со емитирање (broadcasting), донесуваат нова задача за податочното ниво - како да се контролира пристапот до заедничкиот канал. Специјално подниво од податочното ниво, т.н. подниво за пристап на медиумот (meduim access sublayer) се занимава со овој проблем.

2.2.1 Асинхрона и синхрона комуникација

Во компјутерскиот систем, вклучително и влезно-излезните единици, поголемиот податочен трансфер се одвива паралелно. На пример, преносот помеѓу меморијата и процесорот, и од дискот кон меморијата се случуваат паралелно. Паралелниот пренос е побрз, бидејќи дозволува 8, 16, 32 и 64 бита со податоци да се пренесат одеднаш. Сепак, паралелниот пренос бара повеќе линии на поврзување помеѓу испраќачот и примачот, а цената на каблите кои поврзуваат оддалечени компоненти – е премногу висока. Значи паралелната трансмисија е погодна само за кратки растојанија.

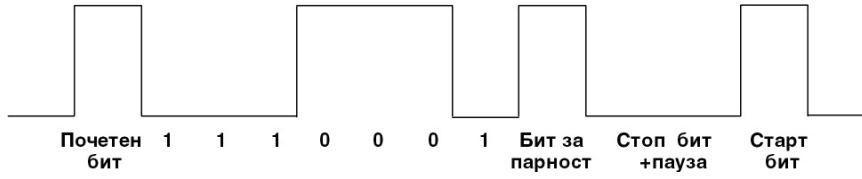
Спротивно од компјутерскиот систем, кај дигиталните комуникации и компјутерските мрежи, податоците скоро секогаш се пренесуваат сериски (т.е. преку еден комуникациски канал, наместо со паралелни линии). Многу повеќе уреди можат да се поврзат на сериска линија, отколку на паралелна магистрала. Исто така, сериската конекција може да се одвива преку различни медиуми (на пр. бакарни жици, па фибер-оптички, па пак бакарни), што е речиси невозможно кај паралелната комуникација. Кај сериската комуникација, сигналите се испраќаат преку комуникациското канал еден по еден. Кога се користи небинарна логика, преку серискиот канал во даден момент ќе може да се испрати повеќе од еден бит, (како со QAM модемите).

Асинхрониот сериски пренос, претставува наједноставна форма на комуникација и се среќава кај точка-точка комуникациските системи. Податочна единица за пренос претставува карактерот (знак), т.е. еден бајт. Системот за асинхрона трансмисија работи со временски мерки и ги решава синхронизационите проблеми со тоа што го дели карактерот во фиксен број на битови, а во единица време пренесува само еден карактер, т.е. бајт. За да се одржува комуникацијата синхрона, кон оригиналните податоци се додаваат екстра битови – еден почетен и два крајни (stop) бита, со што се креира мала рамка. Еден опционен бит за парност може да се додаде кон податоците, а пред крајниот бит, кој ќе служи за проверка на грешки. Овој бит за парност може да биде:

- За парна парност: го прави бројот на 1-ици во 8-те бита, да биде секогаш парен.
- За непарна парност: го прави бројот на единици да биде секогаш непарен.
- Ознака: секогаш 1.
- Празно место: секогаш 0.
- Без парност: овој бит претставува дел од податоците.

Кога се користи бит за парност, најмногу 7 бита со податоци можат да се пренесуваат во даден момент. Проверката на парност се врши само за податочните битови, а не за почетниот и крајните битови. Бидејќи два или три бита се користат да ја формираат рамката за секој карактер (од можните 7 бита), синхроната трансмисија не е многу ефикасна. Сепак, асинхроната комуникација бара помала хардверска поддршка и е поедноставна. Овој начин на работа се користи кај комуникацискиот софтвер на персоналните компјутери. Најчест формат кој се користи е N-8-1-1, т.е. без парност, 8 податочни битови, еден почетен и еден краен (stop) бит. Слика 2. прикажува како карактерот G се пренесува во систем за асинхрона комуникација. Забележете дека во таквиот систем, најмалку значајниот бит се пренесува прв. Синхроната трансмисија е поефикасна и посоодветна за брз сериски пренос, како во случајот со брзите дигитални мрежи. Кај синхроните системи, низата од битови, т.е. карактери се пренесува без почетен и краен бит за секој карактер. Временската синхронизација се постигнува на три различни начини кај различните нивоа:

- Сигналот за синхронизација и часовникот можат да се вметнат во податочниот сигнал преку механизмот за кодирање. Двофазното кодирање, како на пр. Манчестер кодирањето и диференцијалното Манчестер кодирање се погодни за ваквата синхрона комуникација.
- Посебен сигнал за часовник може да се додаде како интерфејс помеѓу терминалните и линиските уреди. Синхронизацијата не се постигнува помеѓу модемот-испраќач и модемот-примач, туку помеѓу компјутерот-испраќач и неговиот модем, и компјутерот-примач и неговиот модем. Овие сигнали за усогласување на часовникот не се користат кај асинхроната комуникација.



Слика 2.4: ASCII карактерот G (47_{16}), се пренесува преку E-7-1-1 формат за асинхрона трансмисија со еден почетен бит, еден бит за парност и седум податочни битови. Најмалку значајниот бит се пренесува прв. Нулите се прикажани со високо напонско ниво.

- На повисокото ниво, на секој блок со податоци (битови) може да се додаде преамбула и постамбула на почеток и крај од блокот, со што се формира рамка. Овие додатни битови содржат контролни и статусни информации и информации што се однесуваат на испраќачот и примачот. Податочниот блок може да биде бит-ориентиран или карактер-ориентиран. Точниот формат на рамката и преамбулата/постамбулата зависи од мрежното опкружување и применетиот протокол за комуникација. Вообичаено, овие почетни

и крајни контролни додатоци се 8-битни торки. На пример, Ethernet рамката користи преамбула долга 8 бајти.

За големи податочни блокови, синхроната трансмисија е многу поефикасна во однос на асинхроната. На пример, за Ethernet рамка што има максимална должина 1500 бајти, преамбулата за синхронизација изнесува само 8/1500.

2.2.2 Детекција и корекција на грешки

Електро-магнетните бранови што патуваат преку медиумот за трансмисија – се подложни на шум. Многу чест пример е кога напонската инсталација предизвикува оштетување и загуба на податоците. Шумот е присутен и кога има грмотевици и кога ќе се вклучи некој уред во домаќинството. И аналогните и дигиталните сигнали се подложни на шум кој може да предизвика оштетување на податоците. Кај компјутерските комуникации – промената на еден бит може да има огромни негативни ефекти. Така на пример, ASCII кодот на буквата 'а' е 1100001. Доколку кодот се промени во 1100011 за време на преносот – ќе се прими буквата 'с'. Овие грешки може да бидат и подрастични кога се пренесуваат финансиски трансакции – една нула повеќе значи 10 пати повеќе.

За среќа, грешките во еден бит се најчести и постојат ефикасни техники за нивна детекција и корекција. Сепак, можни се и грешки кај повеќе битови при преносот. Така на пример, секвенцата 1100001 може да се промени во 1000000. Ова се случува, ако линијата била изложена на шум подолго време.

За да не се проследат бит-грешките кон погорните ОСИ нивои, податочното ниво мора да ги детектира грешките во примените пораки. Уште подобро – веднаш кога ќе се детектира погрешен бит – тој се корегира. Едноставен механизам за детекција на грешки е да се испраќа секој бит два пати. Ако приемникот открие два различни соседни бита – ќе сигнализира грешка во погорните нивоа. Сепак оваа редундантна техника двојно ја редуцира ефикасноста на пренос, бидејќи постои префикс за секој пренесен бит.

Попрактичен метод е кога префиксот би бил помал. Постојат три редундантни техники кои ќе ги дискутираме во продолжение. Првата техника е базирана на парност и додава еден бит кон податочниот блок; битот за парност може да служи за парна или непарна парност. Втората техника се базира на пресметување на аритметичка сума, со примена на бинарна едно-комплементарна аритметика. Пресметаната сума за проверка се додава на крајот од пораката, па кај приемникот се пресметува сумата од податоците плус сумата за проверка. Ако збирот е составен само од 1-ци, пораката е пренесена без грешки; во спротивно има грешка при преносот. Третиот редундантен метод се базира на бинарно делење во полиноми по модул 2, за да се пресмета цикличната редундантна сума (CRC).

Детекцијата на грешки кај податочното ниво обично задоволува и ако се јави грешка, рамките се ре-трансмитуваат кон приемникот. Сепак, постојат и методи кои ги корегираат грешките кај приемникот, без потреба за ре-трансмисија. Еден таков код претставува Хаминговиот, во кој се дефинира

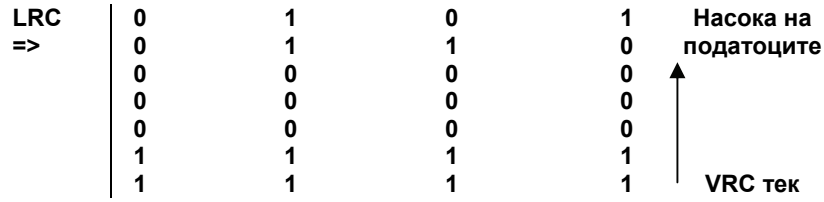
парна парност на податоците, така што во случај на еден погрешен бит, сумата за проверка кај приемникот – посочува кон погрешно пренесениот бит.

Парност

Редундантните системи базирани на парност, користат парна или непарна парност. Битот за парност се добива врз база на бројот на единици во податочниот блок. Бројот на единици, вклучувајќи го и битот за парност, кај парна парност – мора да биде парен. На пример, парната парност за ASCII карактерот 'c' е 1100001. Парноста со еден бит за детекција, не го открива парниот број на грешки (грешки во парен број битови не се детектираат). Ако за пренос на буквата 'a', добиениот знак е 11011001, грешката ќе биде детектирана, заради тоа што има непарен број единици. За да се реши проблемот со недетектирани грешки кога бројот на грешки е парен, се користи дво-димензионален механизам за парност. Кај него, парната парност за секој вертикален блок со податоци е наречена вертикална проверка на редунданса (VRC). Парноста во втората димензија е наречена логитудинална проверка на редунданса (LRC) и овозможува дупла проверка. За пренос на ASCII пораката 'abc' - соодветната проверка е прикажана на Слика 2.5.

Хамингов код

Техниката VRC/LRC прикажува како се користи парната парност за детекција на грешка во еден бит. Друга редундантна техника што се базира на парна парност и овозможува корекција на грешка е Хаминговото кодирање.



Слика 2.5: Парност со примена на LRC и VRC.

Во ова кодирање, бројот на редундантни битови потребни за да се корегира грешка кај порака што е долга m бити, се означува со p. Резултантниот код е долг m+p бита. Овој код може да се примени кај податочни блокови со произволна должина, но p расте драстично со бројот на податочни битови. Во општ случај $2^p \geq m+p+1$, така што за ASCII знак што се состои од m=7 бита, потребни се p=4 контролни бита, т.е. вкупно 11 бита. Контролните (редундантни) битови се стават на позиции 1, 2, 4, 8, ..., 2^n, каде n е цел број. Се почнува од позиција 1 (најлевата), па се пополнуваат сите позиции со податочни и битови за парност.

Како се одредува вредноста на редундантните битови? За r-битот на позиција 1, се гледаат соодветните податочни битови што се десно од r преку еден, т.е. се зема парната парност на податочните битови на позициите 3, 5, 7, 9, 11. За r-битот на позиција 2, се земаат парови податочни битови преку два, т.е. 3, 6, 7, 10, 11. Овој процес продолжува и за редундантните битови на позиција 4, 8, итн.

Корекцијата на грешка, на страната кај примачот се прави со пресметување на с битови, кои се r битовите од погоре, но се зема и битот на позиција r. Нека е примена низата 10011001001, со грешка во позиција 3. Битот с на позиција 1 ќе биде парната парност на позициите 1, 3, 5, 7, 9, 11 (за 1,0,1,0,0,1 тоа е 1). Битот с на позиција 2 ќе биде парната парност на позициите 2, 3, 6, 7, 10, 11 (за 0,0,0,0,0,1 тоа е 1). За позиција 4, тоа е парноста на 1, 1, 0, 0, што дава 0, и за позицијата 8 - тоа е парноста на 1, 0, 0, 1, што дава 0. Сега, ставајќи ги битовите с на позиции 8, 4, 2, 1 се добива вредност 0011, што асоцира на грешка во третиот бит.

Ова Хамингово кодирање работи добро доколку има грешка само во еден бит, а треба да се модифицира за да открива и корегира повеќе грешки, со тоа што бројот на редундантни битови ќе биде зголемен.

Аритметичка сума за проверка (checksum)

Кај аритметичката сума за проверка, испраќачот ги дели податоците во еднакви сегменти од по n бита. Се користи комплементарна аритметика за да се соберат сегментите и да се добие резултатот во n-битна форма. Оваа сума се комплементира и се прилепува кон податоците во полето Checksum. Двете полиња кои се комплементарни едно на друго, мора да дадат сума која се состои само од 1-ци. Примачот ги чува примените n-битни податочни единици и ги собира со checksum (која е на крај). Ако нема грешки - резултатот ќе биде само од 1-ци. Ако се појави грешка, податоците се отфрлаат. На пр. нека разгледаме 4 податочни единици 1000, 1101, 0101, 1110. Checksum за нив ќе се добие со последователно комплементарно собирање, кога резултатот се додава на следната единица: 1000+1101=0110, следено со 0110+0101=1011, следено со 1011+1110=1010. За безгрешна трансмисија, резултантниот checksum би бил 0101, што ако се собере со 1010, дава 1111. Ако има грешки - било кај податоците, било кај checksum, резултатот ќе содржи и некоја 0.

Циклична повторувачка сума (CRC)

Како и другите методи за детекција на грешка, и CRC се генерира кај испраќачот со помош на хардверски механизам кој содржи шифт-регистри и флип-флопови. Се применува делење по модул 2 на полиномот што ја претставува пораката M(x), со полиномијалниот генератор G(x) со степен n. Се добива n-битна рамка, т.е. сума за проверка на остатокот по модул 2, од ова делење. Пред делењето се додаваат n нули на крај од пораката M(X).

На пример, да го разгледаме $M(x) = X^7 + X^6 + X^5 + X^2 + X$, каде M(x) ја претставува пораката 1 1 1 0 0 1 1 0. За $G(x) = X^4 + X^3 + 1$, степенот е n=4, па делиме 1110011000000 со 11001. Остатокот што ќе се добие е 0110, кој кога ќе се додаде кон пораката дава 111001100110.

Хардверската имплементација на CRC за $G(x) = X^4 + X^3 + 1$ користи два флип-флопа за ексклузивно ИЛИ и два шифт регистри. На почеток содржината на шифт регистрите е нула. Како податоците пристигаат секвенцијално, резултатот од портите за ексклузивно ИЛИ се носи во шифт-регистрите бит по бит. По секој пренесен бит, шифт-регистерот шифтира еден бит налево. На крај, во шифт регистрите останува остатокот, кој се прикачува кон податоците и се пренесува непроменет.

Кај приемникот се наоѓаат истите уреди. Шифт регистрите се поставени на нула иницијално. Податоците прво пристигнуваат во флип-флопот, а после се пренесуваат во шифт регистрите. Разликата е во тоа што - откако ќе стигнат сите податоци, вклучително и CRC остатокот, шифт регистрите ќе содржат само нули. Во спротивно, се појавила грешка при преносот.

2.2.3 Рамки и контрола на проток

Асинхроната трансмисија се состои од движење на кратки секвенци на податоци со фиксна должина. За да се примат податоците коректно, потребна е синхронизација помеѓу испраќачот и примачот, и бидејќи должината на податоците е фиксна - доволно ќе биде да се примени часовник за синхронизација. Сепак, едноставниот механизам за синхронизација не работи добро со долги низи од податоци. Во пракса, се користат секвенци од битови наречени пакети со цел да се зголеми ефикасноста на пренос. Преносот на долгите пакети бара посложена синхронизација кај примачот и затоа се воведени рамките. Рамките помагаат да се означи почетокот и крајот на секој пакет, дозволувајќи произволно долги секвенци со податоци. Постојат два типа на трансмисија со вградена синхронизација и контрола на проток: бит-ориентирана и карактер-ориентирана. Овие два метода се разликуваат во начинот на кој ги врамуваат битовите. Бит-ориентираната трансмисија користи бит-секвенци за приказ на карактерите, додека карактер-ориентираната користи цели карактери.

Механизмот за бит-ориентирана трансмисија е прикажан на Слика 2.6. Специјалната низа 01111110 е т.н. flag и се користи да го означи почетокот и крајот на рамката. Рамката се состои уште и од адреса, контролно поле, CRC, и податоци. Должината на секое поле зависи од применетиот протокол. Популарен бит-ориентиран протокол е високо-нивоовската податочна контрола (HDLC).

Flag	Address	Control	Data	CRC	Flag

Слика 2.6: Примена на бит-ориентиран протокол за конструкција на рамка

Кај карактер-ориентираната трансмисија, се претпоставува дека пакетите се состојат од интегрални 8-бајтни броеви. Типичниот изглед на рамката е даден на Слика 2.7. Почетокот на рамката е означен со специјален синхронизирачки карактер SYN, следен со DLE (data link escape) карактер и карактер STX (start-of-text). Крајот на рамката е означен со DLE, следен со ETX (end-of-text) карактер. Два CRC бајта и бајтот SYN се додадени на крај за да се комплетира рамката.

Слика 2.7: Примена на карактер-ориентиран протокол за конструкција на рамка

Flag-от кај бит-ориентираниот протокол ги одредува почетокот и крајот на рамката. Сепак, податоците и другите полиња можат да ја содржат истата flag секвенца. Ако не се преземат специјални мерки за крајот на пораката, примачот можеби ќе прими погрешна секвенца која ќе ја третира како завршен flag. За да се избегне таквата грешка, испраќачот мора да обезбеди да нема бит-секвенца што е идентична со flag-от што ќе се појави во средина на пораката. Ако се забележи таква секвенца, таа може да се модифицира, со вметнување на бит 0 (т.н. stuffing). Обратно од stuffing, кај примачот се прави de-stuffing, со што се трга контролниот бит и се прима оригиналната порака.

Слично со bit stuffing, потребно е да се прави character stuffing кај истоимениот протокол за да се избегне конфузија за крајот на пораката. Карактер stuffing се состои од замена на секое појавување на секвенцата DLE во рамката, помеѓу вистинските DLE, со DLE DLE. Ова овозможува да не се појави секвенца DLE ETX никаде освен на крајот на текстот. Со механизмот на de-stuffing кај примачот се брише едното DLE во сите случаи каде се примени две соседни DLE.

Контрола на проток

Контролата на проток ги дефинира начинот на кои се испраќаат рамките и начинот на кој се следат, т.е. како се прави контролата за грешки. Контролата за грешки дефинира како станицата ги проверува рамките и што се прави ако се пронајде грешка. Општ метод за проверка на грешки е да примачот испрати порака до испраќачот дека се појавила грешка во претходната трансмисија. Пораката е всушност барање да се испрати повторно погрешната рамка. Овој тип на контрола на грешки е наречен барање за автоматско повторување (ARQ).

Во општ случај, контролата на проток треба да овозможи да рамките пристигнат на нивната дестинација, без грешка и во точен редослед. Треба да се земат предвид сите физички ограничувања на станиците за да се обезбеди соодветна контрола на проток. Некои од ограничувањата се капацитетот на баферот, процесирачката моќ, и грешки во линијата за

пренос. На пример, баферот кај примачот, честопати е со ограничен капацитет, и ако се наполни, а испраќачот продолжи да праќа рамки - некои од нив ќе се загубат. За да не дојде до ова, примачот мора да испрати порака XOFF до испраќачот за тој да престане со испраќање на рамки. Кога баферот ќе се испразни - се праќа порака XON, за да се продолжи трансмисијата. Овој метод е посебно погоден кај карактер-ориентираните протоколи.

Бит-ориентираните протоколи бараат подобра организација во однос на карактер-ориентираните, бидејќи кај нив податоците се испраќаат и примаат во поголеми квантуми, а не само бајти (карактери). Постојат два протоколи што овозможуваат контрола на проток кај синхроната трансмисија, и тоа се протоколот застани-и-чекај, и протоколот со лизгачки прозорец.

Протокол Застани-и-чекај

Кај протоколот застани-и-чекај, се смета дека баферскиот простор кај примачот е ограничен, така што испраќачот не продолжува со испраќање сè додека не се добие потврда дека претходната рамка е примена. Се испраќа рамка за потврда (acknowledge) од примачот која индицира успешна трансмисија. Испраќачот, значи, праќа податочна рамка и чека потврда од примачот дали е примена, и затоа протоколот се вика застани-и-чекај. Ако рамката за потврда индицира грешка во преносот - испраќачот ја праќа повторно претходната рамка, а не нова.

Примачот ги проверува примените рамки (со CRC, checksum и сл.) и ако нема грешки - податоците ги проследува кон погорните нивоа, а рамка за потврда се враќа кон испраќачот. Во случај на грешка, примачот во полето за грешка од рамката за потврда става 1, па рамката ќе биде ре-трансмитирана.

Иако овој протокол изгледа навидум добар, тој има и слабости. На пример, тој не му овозможува на испраќачот да дознае дали некоја рамка се изгубила на пат кон примачот (воопшто не стигнала). Ако примачот не ја примил, нема да врати ни рамка за потврда, па испраќачот нема како да дознае дали рамката е примена. Слично - ако рамката за потврда е изгубена или оштетена, испраќачот ќе помисли дека претходната трансмисија била неуспешна, иако била во ред. Понекогаш - и испраќачот и примачот мора да водат сметка за овој недостаток.

За среќа, решението на овие проблеми е во временскиот механизам (timer) кај испраќачот и способноста на примачот да утврди присуство на дуплирани рамки, во случај кога рамката за потврда е изгубена. Временскиот механизам му овозможува тајм-аут на испраќачот пред да ја ре-трансмитира рамката. Ако причина за тајм-аут била загуба на податочна рамка, тогаш примачот ја добива рамката одново и продолжува со нормална работа. Сепак, ако причината била загуба на рамката за потврда, испраќачот ќе ја испрати повторно истата рамка, т.е. ќе се појават дуплирани рамки. Бидејќи само една рамка е валидна, другата ќе се избрише, со проверка на секвентниот бит кој има вредност 0 или 1. (Затоа овој протокол се нарекува и алтернативен бит протокол). Ако две последователни рамки кај примачот

имаат ист секвентен број, тоа значи се изгубила рамката за потврда, па едната од рамките треба да се отфрли.

Протокол со лизгачки прозорец

Кај протоколот со лизгачки прозорец, кој претставува проширување на протоколот застани-и-чекај, секвенцата на пакети мора да се испраќа и прима симултано (истовремено). Идејата е да се држи зафатена линијата цело време во двете насоки. Сепак, постои лимитирачки фактор. Бројот на рамки што чекаат помеѓу испраќачот и примачот не смее да го надмине бројот што е дефиниран со секвентниот број. Така, ако секвентниот број се состои од 3 бита, можно е да се генерираат 0-7 рамки во исто време (7=111). За да се осигури дека рамките од првата група се различни од оние во втората група, испраќачот не може да испрати повеќе од 8 рамки во исто време.

За да се води евиденција на испратените и примените рамки - имплементирани се кружни прозорци, кои се отвораат или затвораат, како што се испраќаат или пристигнуваат рамките. Кај прозорецот на испраќачот - левата стрелка се движи во насока на стрелките на часовникот - по еден поделок за секоја испратена рамка. Десната стрелка се движи во истата насока, но по еден поделок за секоја примена рамка за потврда.

Прозорецот кај примачот работи на сличен начин: левата стрелка се придвижува за еден поделок кога ќе се прими податочна рамка, а десната - кога ќе се испрати рамка за потврда. Може да се забележи дека кога се користи лизгачки прозорец, рамките кои се пренесуваат не секогаш ги имаат броевите 0-7. Секвентниот број е всушност континуален број по модул 7. Исто така, за да се обезбеди безгрешна работа на протоколот, максималниот број на рамки што чекаат не смее да надмине половина од величината на прозорецот (на пр. 4 за прозорец со величина 8).

2.3 МРЕЖНО НИВО

Мрежното ниво се занимава со контрола на функционирањето на подмрежите. Негова клучна задача е одредување на патеката (рутата) по која се движат пакетите од изворот кон дестинацијата. Рутите можат да се базираат на статички табели, кои се вградени во мрежата и ретко се менуваат. Тие исто така, може да се одредуваат пред стартот на секоја конверзација, т.е. сесија. Конечно, рутирачките табели може да бидат многу динамички, и да се одредуваат за секој пакет посебно, на начин кој ќе зависи од оптоварувањето на мрежата. Ако многу пакети се присутни во една подмрежа во даден момент, тие ќе си сметаат еден на друг, формирајќи т.н. bottleneck (тесно грло). Контролата на ваквото натрупување е исто така во рацете на мрежното ниво.

Секој провајдер на мрежни услуги, сака да ги наплати истите, па користи софтвер за броење на пакети кои се пренесени од/до секој корисник,

формирајќи на тој начин информација за наплатата. Ако пакетот патува надвор од границите на земјата - се применуваат други цени во наплатата. Овој софтвер за наплата е исто така дел од мрежното ниво. Бидејќи пакетот поминува низ повеќе мрежи пред да стигне на својата дестинација, како проблем се јавуваат различните начини за адресирање во секоја од мрежите. Проблем е и користењето на различни протоколи за пренос. Некоја од мрежите може воопшто да не го прими пакетот ако е голем. Мрежното ниво се грижи за сите овие проблеми и овозможува поврзување на хетерогените мрежи.

Кај емитувачките (broadcasting) мрежи, рутирачкиот проблем скоро и да не постои, па затоа и мрежното ниво кај нив е многу тенко или е изоставено. Детали за мрежното ниво ќе бидат обработени во шестото поглавје од книгава, кое се однесува на мрежните протоколи.

2.3.1 Концепт на подмрежа (subnet)

Меѓу-мрежата (internetwork) се состои од повеќе помали мрежи, кои се во можност да прават преклопување, рутирање и проследување помеѓу себе. Овие помали мрежи се т.н. подмрежи. Секоја подмрежа може да функционира самостојно. Меѓу-конекцијата на подмрежите се прави со специјални прекинувачки уреди - на мрежно ниво тоа се рутери, а на податочно - мостови (bridge). Рутерот овозможува проследување и рутирање на пакети помеѓу различните подмрежи кои работат со различни протоколи. Сепак, мостот работи со подмрежи кои користат ист протокол. Мостот не ја модифицира содржината на применот пакет, тој само работи како адресен филтер што го зема пакетот од една подмрежа и го проследува на друга подмрежа, каде што се наоѓа дестинацијата. Рутерите и преклопниците (switches) можат да се конфигурираат така што да работат во конекциски и неконекциски режим. Постојат протоколи имплементирани кај овие уреди кои овозможуваат меѓу-мрежен сообраќај во подмрежите и нив ќе ги опишеме подоцна.

2.3.2 Прекинувачки/комутациони (switching) техники

Доколку се обезбеди посебно коло (dedicated circuit) за одредена комуникација - брзината би била Gigabit/sec. Но таква скапа конекција може да се оправда само со континуиран пренос на податоци помеѓу два компјутери. Мрежата се состои од стотици компјутери, а во случај на Интернет - од милиони. Невозможно е да се поврзат сите компјутери директно еден со друг. Линиите за поврзување (каблите) мора да се делат заеднички. За таа цел се користи мултиплексирањето. Кај мултиплексираната мрежа постојат два методи на прекинување (switching) - комутација на линии и комутација на пакети. Комутацијата на линии е слична со традиционалната телефонија, бидејќи се обезбедува посебна (dedicated) конекција помеѓу двете страни за време на “разговорот“. Постојат и други техники за комутација - комутација на ќелии (ATM), комутација на

рамки (frame relay) и комутација на пакети (packet switching). Комутацијата на линии обезбедува најдоверлива комуникација - константен сообраќај, со минимални процесирачки операции кај мрежните уреди.

Од друга страна, комутацијата на пакети и датаграми, која е технички и процесирачки најсложена, овозможува пофлексибилна, динамичка, робусна и делива трансмисија со променлива брзина на пренос. Помеѓу овие две спротивни техники за комутација, се наоѓаат релеј на рамки (frame relay), ATM и повеќекратната комутација на линии. Сите тие претставуваат релативно нови телекомуникациски техники.

Системите за податочна комуникација имаат неправилен сообраќај; каналот во некои моменти е празен, а другпат е многу зафатен (кога голем пакет се пренесува во краток временски интервал). Кога се јавува згуснат сообраќај - пожелно е комуникациските канали да се мултиплексираат, за да се зголеми искористеноста на каналот. Пожелна е брза ре-конфигурација на комутациониот систем, т.е. префрлување од еден канал на друг. Комутацијата на линии се покажала неефикасна за брза ре-конфигурација, бидејќи поставувањето на линии е во ранг на секунди, а не микросекунди.

Комутацијата на пакети е специјално дизајнирана да се справува со неправилен сообраќај, кој е често присутен кај компјутерските мрежи и дистрибуираните компјутерски системи. На рамките и пакетите што потекнуваат од еден компјутер им се додаваат заглавја, кои ги содржат адресите и рутирачките информации за изворишето и дестинацијата. Потоа пакетите се пуштаат преку физичкиот канал. Секој преклопник или рутер го проверува заглавјето на пакетот, а потоа одлучува каде ќе го проследи. Ако е во рамките на иста физичка мрежа - веднаш го проследува до одредишниот компјутер. Додека две мрежи што се поврзани со комутација на линии мора да работат со иста брзина, кај комутацијата на пакети - тие можат да работат и со различни брзини. Сепак, заради природата зачувај-проследи кај пакетската комутација е можно појавување на различно доцнење.

Системите со пакетска комутација можат да се опоравaт после грешка за пократко време и со помалку напор, отколку системите со комутација на линии. Исто така, пакетите може да патуваат по различни патишта, доколку некои од патиштата станат недостапни или премногу оптоварени. Заради ова – комутацијата на пакети е поробусна од комутацијата на линии; сепак пакетите може ќе стигнат кај одредиштето во различен редослед од оној по кој се испратени. Губењето на редоследот може да се јави како последица на повторното испраќање на некој пакет, или заради различните рути (со различни доцнења) по кои патуваат пакетите.

Бидејќи комутацијата на пакети функционира кај различни мрежи кои работат со различна брзина, за контрола на проток се воведуваат бафери. Кога се преполнува баферот – се појавува натрупување и преклопниците ќе бидат принудени да ги вратат пакетите што не можат да се пренесат или сочуваат. Кога се случува ова – натрупувањето уште повеќе доаѓа до израз. Детекцијата, превенцијата и избегнувањето на натрупувањето се важни поими од техниката на пакетска комутација. Развиена е и техника за

виртуелна комутација на линии со која пакетите се примаат во ист редослед, и со која се редуцираат шансите за натрупување. Кај ваквата виртуелна комутација на линии – изгледа дека пакетите патуваат од еден јазел до друг преку резервирана линија, но во реалноста не постои таква линија. Податоците и тука се доставуваат во форма на пакети, во точен редослед, но со променливо доцнење. Кога сообраќајот ќе се интензивира – изборот на патека сè уште претставува сериозен предизвик.

Првата мрежа со пакетска комутација – Arpanet (претходник на Интернет), е развиена од Воено-истражувачката Агенција на САД - DARPA, во 1969. Системот користел компјутери PDP-8 како пакетсаки преклопници, кои биле поврзани на резервирани 50 Kbps телефонски линии. Од тогаш се развиени и други слични проекти, т.е. јавни и приватни пакетски мрежи, како и системот X.25, брзини од 56/64 Kbps до 1.5/2 Mbps (T1/E1).

Комуникациските канали за пакетска комутација го делат нивниот проток помеѓу сите корисници што сакаат да им пристапат. Комуникацискиот канал се нарекува пакетско-комутиран, бидејќи секогаш кога корисникот испраќа пакет со податоци, пакетот патува по истиот канал, каде што патуваат и сите други податоци. Ваквиот канал комутира пакети, а не линии. Кога каналот се користи истовремено од голем број на корисници (т.е. кога е многу оптоварен), испраќањето податоци ќе одземе повеќе време отколку кога го користат мал број корисници (слабо оптоварен). Оваа особина претставува разлика помеѓу комутацијата на пакети и комутацијата на линии. Кај комутацијата на линии – целиот проток е секогаш достапен на еден корисник. Кај комутацијата на пакети – протокот се дели помеѓу сите корисници.

2.3.3 X.25 протокол

Стандардот X.25 за пакетска комутација е поедноставен 3-нивоовски еквивалент на ОСИ моделот. Овој протокол, базиран на физичкото, податочното и мрежното ниво, е стандардизиран од ITU-T и се дефинира како интерфејс помеѓу податочно-терминалната опрема (DTE) и податочно-линиската опрема (DCE). Се користи кај јавните мрежи кои се дел од пошироките мрежи (WAN), и го употребува стандардот на физичко ниво X.21. На податочно ниво го користи протоколот LAP-B, кој овозможува доверлив трансфер на податоци преку физичкиот линк.

Кај мрежното ниво на X.25, податоците се испраќаат во пакети преку виртуелни линии, кои можат да бидат перманентни или да се воспоставуваат динамички. Перманентната виртуелна линија е фиксна и се доделува од мрежата, без посебно барање. Контролата на протокот и контролата на грешки кај X.25 се исти како кај HDLC (високо-нивоовска податочна контрола, развиена од IBM во 1975).

2.3.4 Стратегии за рутирање

Цената за преносот на податоци помеѓу две станици зависи од неколку фактори, како што се доцнењето, бројот на меѓу-јазли, и растојанието помеѓу станиците. Кога се познати цените на врските (линковите), рутерот може да ја пресмета најповолната патека за секој пакет. Постојат неколку алгоритми кои ги прават овие пресметки. Две најпознати техники се „distance vector“ и „link state“ рутирањето. Кај методот distance vector - рутерите ја разменуваат информацијата за цената на патеките со непосредните соседи. Тие исто така ја делат заеднички целосната рутирачка табела, и за да се ажурираат постоечките табели се користат влезовите добиени од други рутери. Цената на една врска се зема да биде еден. Така - цената за испраќање на податоци од еден рутер до друг во пет скокови, ќе биде 5.

Практичен пример за овој тип на рутирање е Интернет, кој претставува меѓу-мрежа составена од подмрежи, поврзани со рутери и gateway. Рутерот на почеток креира иницијална рутирачка табела за подмрежите на кои е конектиран, и ги испраќа тие информации до соседните рутери. Слично, другите рутери ги испраќаат нивните информации до првиот рутер, и по оваа иницијална фаза, ажурираните мрежни табели се дистрибуираат до сите рутери.

Link state рутирањето опфаќа споделување на рутирачките информации помеѓу сите рутери во мрежата. Наместо испраќање на цела рутирачка табела, се испраќа само информацијата за соседите. Рутерите испраќаат периодични ажурирања до соседните рутери, кои пак ги испраќаат тие информации до нивните соседи итн. Овој процес на рутирање е т.н. поплава - flooding. Може да се забележи дека ваквото рутирање може да предизвика и непотребни дупликати. Сепак, загарантирано е дека рутерите ќе ја добијат најновата оригинална информација од оригиналниот рутер.

Споредувајќи ги двата методи, забележуваме дека цената се изразува преку бројот на скокови кај distance vector, додека кај link state врз база на тежински фактор што ги опфаќа состојбата со врските, количината сообраќај и безбедносното ниво. Исто така, размената на информации кај distance vector е почеста од онаа кај link state (секои 30 секунди во споредба со 30 минути). Distance vector се состои од броење на скоковите што ги прави пакетот и идентификација на рутерите од сите одредишни мрежи.

Алгоритмите за одредување најкраток пат се омилен предмет за истражување во компјутерското инженерство. Во примената на најкраток пат, повеќето рутери ги користат двата најпознати алгоритми - на Дијкстра и на Белман-Форд. И двата алгоритми користат графови кои се состојат од темиња и лакови, за да го пресметаат најкраткиот пат помеѓу два јазли. Може да се формира и дрво со најкратки патишта од даден рутер до сите одредишни рутери. Конечно, рутерите користат вакво дрво на најкратки патишта при конструкцијата на своите рутирачки табели.

2.3.5 Контрола на натрупувањето

Ги споменавме различните техники за рутирање и мултиплексирање. Главен предизвик за имплементација на овие стратегии е постигнување на максимален проток со контролирано доцнење. Сепак, протокот и доцнењето се директно зависни едно од друго. Ако се зголеми протокот, ќе се зголеми и доцнењето, бидејќи повеќе податоци ќе циркулираат низ ист канал. Кога мрежата е малку оптоварена, нема натрупување, бидејќи нема ни доцнење. Ако оптоварувањето расте, ќе расте и доцнењето - па ќе се појави и мало натрупување. Ако оптоварувањето продолжи да расте, се појавува големо натрупување, и мрежниот проток започнува да опаѓа, наместо да расте. Доколку протокот опаѓа со голема брзина - мрежата станува нестабилна. Задачата на механизмите за контрола на натрупување е избегнување на натрупувањето и превенција од колапс на мрежата. Избегнување на натрупувањето се прави уште пред да се појави истото. Постојат и механизми за опоравување (recovery) после натрупувањето и тие се користат во случај кога мрежата почнала да испушта (враќа) пакети, како резултат на натрупувањето.

2.4 Транспортно ниво

Основната функција на транспортното ниво е да ги прифати податоците од погорното - сесиско ниво, да ги подели во помали единици (пакети), и да ги проследи кон мрежното ниво, водејќи сметка да сите делови стигнат коректно на другата страна. Оваа постапка мора да се направи ефикасно и на тој начин што погорните нивоа ќе бидат независни од хардверската технологија на пониските нивоа.

Транспортното ниво обезбедува два типа на сервис: конекциски-ориентиран и неконекциски-ориентиран. Кај конекциски-ориентираниот, постојат 3 фази во комуникацијата: воспоставување на конекцијата, податочен трансфер и раскинување на конекцијата. Во нормални услови, транспортното ниво креира посебна мрежна конекција за секоја транспортна конекција побарана од сесиското ниво. Ако се бара голем проток - транспортното ниво може да формира повеќе мрежни конекции и ги разделува податоците соодветно. Од друга страна, ако креирањето или одржувањето на повеќе мрежни конекции е скапо, транспортното ниво мултиплексира повеќе транспортни конекции во една мрежна. Во сите случаи, овие операции се транспаренти за сесиското ниво.

Транспортното ниво исто така одредува каков тип на сервис ќе му се понуди на мрежниот корисник. Најпопуларен тип на транспортна конекција е без-грешниот point-to-point канал, кој ги доставува пораките во ист редослед како што се испратени. Можни се и други начини на транспорт, на пр. транспорт кој не гарантира редослед на доставените пакети, транспорт со емитирање на пораките до повеќе дестинации итн. Типот на транспорт ќе се одреди откако ќе се воспостави конекцијата.

Транспортното ниво е вистинско end-to-end ниво, од испраќачот кон дестинацијата. Со други зборови, софтверот кај испраќачот води конверзација со софтверот на примачот, со примена на заглавја на пораките и контролни пораки. Кај пониските нивои - протоколите се одвиваат помеѓу секоја машина и нејзините соседи во мрежата, а не помеѓу изворот и дестинацијата (кои може да се раздвоени и со неколку рутери). Нивоата над транспортното се исто така end-to-end, што не важи за физичкото, податочното и мрежното ниво.

Многу од јазлите се мулти-програмабилни, што значи постојат повеќе конекции кај секој јазел, од кои некои се појдовни, а некои - дојдовни. Треба да постои информација што ќе каже кои пораки припаѓаат на која конекција, а заглавјето (header) на транспортното ниво може да ја складира таа информација.

Во контекст на мултиплексирањето на повеќе пораки во еден канал, треба да се каже дека транспортното ниво е тоа што ги воспоставува и брише конекциите низ целата мрежа. Ова бара механизам за доделување имиња, со кој машините ќе можат да кажат со кого сакаат да водат конверзација. Исто така, мора да постои механизам кој ќе го регулира протокот на информации, така што побрзите јазли да не ги преплават побавните. Таквиот механизам се вика контрола на проток (flow control), и игра клучна улога кај транспортното ниво (но и кај другите нивои). Контролата на проток помеѓу јазлите се разликува од контролата на проток помеѓу рутерите, иако како што ќе видиме подоцна, истите принципи се применливи и во двата случаи.

Транспортното ниво ќе биде исто така обработено во детали, во шестото поглавје од книгава, кое се однесува на мрежните протоколи.

2.4.1 Транспортен сервис

Конекциски-ориентираниот транспортен сервис е сличен со конекциски-ориентираниот мрежен сервис на повеќе начини. Во двата случаи, конекцијата има 3 фази: воспоставување, трансфер на податоци, и ослободување. Адресирањето и контролата на проток се слични и кај двете нивоа. Понатаму, неконекцискиот транспортен сервис е исто сличен со неконекцискиот мрежен сервис.

Се поставува прашањето: ако транспортниот сервис е сличен со мрежниот, зошто постојат две нивоа, а не само едно? Транспортниот сервис се одвива на корисничките машини, а мрежниот - претежно кај рутерите, кои се дел од мрежата (барем кај глобалните мрежи). Што се случува кога мрежното ниво нуди неадекватен сервис? Што ако често се губат пакетите? Што ако паднат рутерите?

Се јавува проблем, ете што. Корисниците немаат контрола врз мрежното ниво, така што не можат да го решат проблемот ако земат друг рутер или ако вршат зголемена контрола во податочното ниво. Единствен начин е да се стави ново ниво над мрежното што ќе го унапреди нивото на услуги. Постоењето на транспортното ниво овозможува подоверлива работа на сите

подолни нивоа. Ги детектира изгубените пакети и користи стандардни процедури кои се независни од мрежните примитиви. Мрежниот сервис може да се разликува значително од една мрежа до друга (на пр., безжичниот LAN сервис во многу се разликува од жичениот WAN сервис). Со криење на мрежниот сервис зад транспортниот, промените во мрежното ниво нема да се одразат врз погорните нивоа.

Благодарејќи на транспортното ниво, апликациските програмери пишуваат програми со стандардни примитиви, кои можат да се извршуваат дистрибуирано, т.е. на оддалечени машини, без да се грижат за мрежните интерфејси и за доверливоста на преносот. Ако сите реални мрежи се фиксни и непроменливи, транспортното ниво можеби нема да биде потребно. Сепак, во реалниот свет тоа ги изолира погорните нивоа од технологијата, дизајнот и несовршеностите на мрежата.

Примитиви на транспортниот сервис

Транспортниот сервис е сличен со мрежниот, со тоа што има неколку важни разлики. Главна разлика е што мрежниот сервис е наменет да работи со реални мрежни модели. Реалните мрежи можат да губат пакети, така што мрежниот сервис е недоверлив. Конекциски-ориентираниот транспортен сервис е доверлив. Се разбира, реалните мрежи не се безгрешни, но тоа е и улогата на транспортното ниво - да обезбеди доверлив сервис на врвот од недоверливата мрежа.

Како пример, да разгледаме два процеси поврзани со проточни цевки во UNIX. Тие претпоставуваат дека конекцијата помеѓу нив е совршена. Тие не сакаат да знаат за потврдување (acknowledge), изгубени пакети, натрупување итн. Тие сакаат 100 проценти доверлива конекција. Процесот А ги става податоците на едниот крај од цевката, а процесот В ги прима на другиот. Затоа служи конекциски-ориентираниот транспортен сервис - криење на несовршеностите на мрежниот сервис така што процесите ќе добијат непрекинат безгрешен податочен тек.

Од друга страна, транспортното ниво може да обезбеди и недоверлив (datagram) сервис. Сепак, нема многу што да се каже за него, затоа претежно вниманието е насочено кон конекциски-ориентираниот транспортен сервис. Се разбира, постојат некои апликации, како на пример client-server процесирањето и streaming multimedia, кои користат не-конекциски транспорт, затоа не смее да се заборави во пракса.

Друга разлика помеѓу мрежниот и транспортниот сервис е нивната намена. Мрежниот сервис се користи само преку транспортните ентитети. Многу малку програмери го користат мрежниот сервис. За разлика од нив, многу програмери ги користат транспортните примитиви. Следствено, транспортниот сервис мора да биде погоден и лесен за употреба. За да разбереме како се користат примитивите, да разгледаме случај со еден сервер и неколку оддалечени клиенти. На почеток, серверот извршува примитива LISTEN, повикувајќи готова процедура, т.е. системски повик да

се блокира серверот сè додека не се добие повик од клиентот. Кога клиентот сака да зборува со серверот, извршува примитива CONNECT.

Примитива	Испратен пакет	Значење
LISTEN	none	чека некој процес да побара конекција
CONNECT	CONNECTION REQ.	активно се обидува да воспост. конекција
SEND	DATA	испраќа податоци
RECEIVE	none	блокира дури да стигнат податоци
DISCONNECT	DISCONNECTION REQ.	сака да ја ослободи конекцијата

Слика 2.8: Сервисни примитиви

Транспортното ниво на клиентот го прави овој повик и испраќа пакет до серверот. Во тој пакет (примитива) се наоѓа порака за транспортното ниво на серверот. Потоа следува SEND/ RECEIVE на податоците, и на крај конекцијата се раскинува.

2.4.2 Елементи на транспортниот протокол

Во податочното ниво, не е потребно во рутерот да се специфицира со кој рутер сака да зборува - секоја излезна линија специфицира точно одреден рутер. Кај транспортното ниво, се бара експлицитно адресирање на дестинацијата.

Процесот на воспоставување на конекција кај податочното ниво е едноставен: другата страна е секогаш присутна (доколку не е падната). Во секој случај - нема многу што да се направи. Кај транспортното ниво, иницијалното воспоставување на конекција е посложено.

Друга вознемирувачка разлика помеѓу податочното и транспортното ниво е потенцијалното постоење на диск простор во мрежата. Кога рутерот испраќа рамка, таа може да пристигне или да се загуби, но не може да кружи низ мрежата и да се смести некаде, па да се појави 30 секунди подоцна. Ако мрежата користи датаграми и адаптивно рутирање, постои незанемарлива веројатност дека пакетот ќе се смести некаде и ќе се достави подоцна. Последиците од способноста на мрежата да чува пакети можат да бидат многу големи и да бараат примена на специјални протоколи.

Последна разлика помеѓу податочното и транспортното ниво е бројот на бафери. Баферите и контролата на проток се битни и кај двете нивоа, но присуството на голем и променлив број на конекции кај транспортното ниво бара различен пристап во однос на податочното ниво. Некои од протоколите алоцираат фиксен број на бафери за секоја линија, така што кога ќе пристигне рамката - баферот е секогаш достапен. Кај транспортното ниво,

големиот број на конекции за кои се води сметка значи доделување на многу бафери за секоја од нив.

Адресирање

Кога апликацијата (т.е. корисникот) сакаат да воспостават конекција со оддалечен процес, мора да специфицираат со кого ќе се конектираат. (Неконекцискиот транспорт го има истиот проблем: до кого да се испрати пораката?). Методот што се користи е да се дефинира транспортна адреса на која процесите ќе очекуваат (наслушуваат) барања за конекции. Кај Internet, овие крајни точки се наречени порти. Кај ATM мрежите, тие се наречени AAL-SAP. Ќе користиме генерички поим за транспортната адреса - TSAP, (Transport Service Access Point). Аналогно - крајните точки кај мрежното ниво (т.е., адресите од мрежното ниво) ги нарекуваме NSAP. IP адресите се пример за NSAP.

Можно сценарио за транспортна конекција е следново:

1. Еден временски сервер работи на хост 2, давајќи си себе адреса TSAP 1522 и чекајќи повици. Давањето на сопствена TSAP-адреса не зависи од мрежниот модел туку само од локалниот оперативен систем. За чекањето повик се користи примитива LISTEN.
2. Апликацискиот процес на хост 1 сака да го дознае тековното време, така што испраќа барање CONNECT, специфицирајќи TSAP 1208 како своја адреса и TSAP 1522 како дестинација. Оваа акција резултира со транспортна конекција која се воспоставува помеѓу апликацискиот процес на хост 1 и серверот на хост 2.
3. Апликацискиот процес потоа испраќа барање за тековното време.
4. Временскиот сервер одговара праќајќи го тековното време.
5. Тогаш се ослободува транспортната конекција.

Постои специјален процес наречен именски сервер, понекогаш наречен и директориумски сервер. За да се најде TSAP-адреса што одговара на дадено име на сервис, на пр. 'време во денот', корисникот воспоставува конекција до именскиот сервер (кој слуша на добро-позната јавна TSAP-адреса). Корисникот прво праќа порака специфицирајќи го името на сервисот, а именскиот сервер ја враќа TSAP-адресата на сервисот. Потоа корисникот ја ослободува конекцијата со именскиот сервер и воспоставува конекција со потребниот сервис. Во овој модел, кога се креира нов сервис, тој мора да се регистрира кај именскиот сервер, кажувајќи го своето име на сервис (типично ASCII стринг) и својата TSAP-адреса. Именскиот сервер ја снима таа информација во својата база, така што кога ќе се постави прашање во иднина, тој ќе го знае одговорот.

Функцијата на именскиот сервер е слична со оператор во телефонска централа - овозможува пресликување на имиња во броеви. Како и во телефонскиот систем, неопходно е добро-позната TSAP-адреса да се користи

како именски сервер (кој е активен сервер при воспоставување на конекцијата).

Воспоставување на конекција

Воспоставувањето на конекција звучи едноставно, но во пракса е проблематично. На прв поглед, изгледа дека е доволно транспортниот ентитет да испрати CONNECTION REQUEST TPDU кон дестинацијата и да чека CONNECTION ACCEPTED одговор. Проблемот се јавува кога мрежата губи, зачувува, и дуплира пакети. Ова поведение предизвикува сериозни компликации.

Да замислиме натрупана мрежа во која потврдите за прием едвај се враќаат назад навреме, па секој пакет се ре-трансмитира два или три пати. Нека мрежата користи датаграми и секој пакет нека оди по различна рута (патека). Некои од пакетите можеби заглавиле во мрежното натрупување и нема да пристигнат навреме; затоа се складираат внатре во мрежата и ќе се проследат подоцна. Проблемот е што се јавуваат вакви задоцнети дупликати. Овој проблем може да се реши на повеќе начини, но ниеден не задоволува. Еден начин е да се отфрлаат транспортните адреси. Во овој пристап, секогаш кога се бара нова транспортна адреса, се генерира нова адреса. Кога конекцијата се ослободува, адресата се отфрла и не се користи никогаш повеќе.

Ако се осигуриме да пакетот не живее подолго од некое дадено време, проблемот станува решлив. Животниот век на пакетот може да се ограничи со примена на следните техники:

1. Ограничен дизајн на подмрежата.
2. Ставање бројач на скокови кај секој пакет.
3. Временска маркичка на секој пакет.

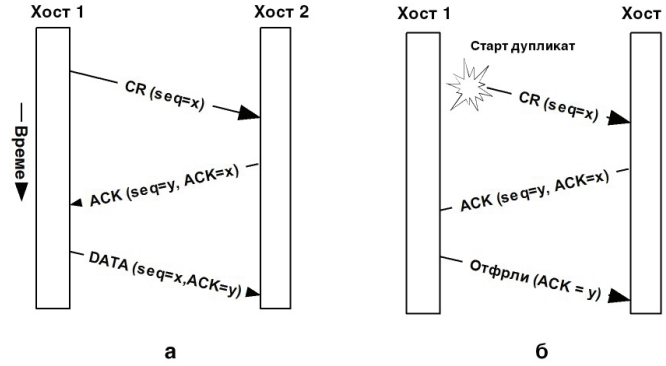
Првиот метод вклучува превенција од бесконечни циклуси, заедно со пресметаното време на доцнење преку најдолгиот познат пат. Вториот метод се состои од бројач на скокови иницијализиран на некоја соодветна вредност која се декрементира секогаш кога пакетот ќе се проследи. Мрежниот протокол едноставно ги отфрла пакетите чиј бројач на скокови станал нула. Третиот метод бара секој пакет да го носи со себе времето во кое е креиран, па рутерите ќе го отфрлат пакетот ако не го носи пре-дефинираното време. Овој метод бара часовниците кај рутерите да бидат синхронизирани, што е нетривијална задача, бидејќи синхронизацијата се постигнува надвор од мрежата, на пр. со GPS или радио-станица што го емитува точното време периодично.

За да го реши проблемот со загубата на меморијата (поплава од пакети) што доведува и до пад на машината, Tomlinson предложил во секој хост да се стави дневен часовник. Часовниците кај различни хостови не мора да се синхронизирани. Секој часовник има облик на бинарен бројач и се инкрементира во униформни интервали. Понатаму, бројот на битови во

бројачот мора да е поголем или еднаков од бројот на бити во секвентните броеви. Конечно и најважно, часовникот треба да работи дури и хостот да е паднат. Откако двата транспортни ентитети се договориле за почетниот секвентен број, за контрола на протокот може да се употреби било кој протокол со лизгачки прозорец.

За да креира доверлива конекција, Tomlinson (1975) воведува тро-насочно ракување. Овој протокол не бара двете страни да почнат испраќање со ист секвентен број, така што методот за синхронизација е различен од глобалниот часовник. Нормалната процедура е кога хост 1 иницира комуникација како на Слика 2.9 .а). Хост 1 бира секвентен број, x, и испраќа CONNECTION REQUEST TPDU со тој број кон хост 2. Хост 2 одговара со ACK TPDU потврдувајќи го x и воведувајќи свој почетен секвентен број, y. Конечно, хостот 1 го потврдува изборот на секвентниот број y, при првите испратени податоци TPDU.

Сега да го разгледаме три-насочното ракување во случај на задоцнет дуплиран TPDU.



Слика 2.9: Две сценарија за воспоставување конекција со тро-насочно ракување. CR значи CONNECTION REQUEST. (а) Нормална работа. (b) Стар дуплиран CONNECTION REQUEST се појвува од никаде.

На Слика 2.9 .б) првиот TPDU е задоцнет дуплиран CONNECTION REQUEST од некоја стара конекција.Овој TPDU пристигнува кај хост 2 без знаење на хост 1. Хост 2 реагира на овој TPDU испраќајќи му на хост 1 - ACK TPDU, барајќи верификација дека хост 1 навистина сака да воспостави конекција. Кога хостот 1 го одбил обидот на хост 2 да воспостави конекција, хостот 2 сфаќа дека тоа бил некој задоцнет дупликат и ја отфрла конекцијата. На овој начин, задоцнетиот дупликат не прави штета.

Ослободување на конекцијата

Ослободувањето на конекцијата е поедноставно од воспоставувањето. Сепак, и тука има одредени тешкотии. Постојат 2 начини за крај на конекцијата: симетрично и симетрично ослободување. Асиметричното работи како телефонскиот систем: кога едната страна ќе спушти слушалка,

конекцијата се прекинува. Симетричното ослободување ја третира конекцијата како две еднонасочни конекции и бара секоја да биде прекината посебно.

Асиметричното прекинување може да резултира со губење на податоци. Треба да се примени софистициран протокол за да не дојде до таква загуба. Најдобро е да се примени симетрично раскинување, при што секоја насока се ослободува независно од другата. Така, хостот ќе продолжи да прима податоци дури и кога испратил DISCONNECT TPDU.

Симетричното ослободување работи така што секој процес има фиксна количина на податоци што сака да ги испрати и знае кога е завршено испраќањето. Во некои ситуации, одредувањето на крајот на работата не е така очигледно, па не се знае точно кога да се раскине конекцијата. Раскинувањето е протокол во кој хост 1 вели: јас сум готов. Дали си и ти готов? Ако хост 2 одговори: И јас сум готов, тогаш конекцијата може безбедно да се прекине. За жал, тоа не е секогаш случај.

2.5 СЕСИСКО НИВО

Сесиското ниво од ОСИ има мало практично значење во современите компјутерски мрежи. Многу задачи што би требало да ги извршува ова ниво - се веќе вградени во апликациите, т.е. се преземени од апликативното ниво. Сепак, ова ниво е одговорно за управување со сесијата (комуникацијата помеѓу двете страни) и извршува задачи како што се проверка за логирање на корисник на оддалечен систем, и управување со дијалогот со цел да се овозможи делење на заеднички канал за пренос. Сесиското ниво може да овозможи да има пренос во двете насоки истовремено, но и само еднонасочно. Ако транспортот е еднонасочен - сесиското ниво се грижи за тоа - кој е на ред да пренесува. Овој сервис е т.н. token management. За некои протоколи - важно е двете страни да не извршуваат иста операција во исто време. За таа цел - сесиското ниво обезбедува жетони (tokens), и само онаа страна која во даден момент го поседува жетонот - ќе може да ја изврши саканата операција.

Друга активност на сесиското ниво е синхронизацијата. Да го разгледаме примерот за 2-часовен пренос на податоци помеѓу две машини, кои се договориле - доколку "пукне врската", да прават еден час пауза пред да почнат повторен пренос. Доколку врската навистина се прекине, целиот трансфер би требало да почне одново, а постои шанса повторно да се јави грешка во преносот. Затоа сесиското ниво вметнува контролни точки (checkpoints) во самите податоци, со цел податоците кои биле пренесени пред да настане прекинот - да не се испраќаат повторно. Така, по евентуалниот прекин на врската, ќе се повторат само податоците испратени после последниот checkpoint.

2.6 ПРЕЗЕНТАЦИСКО НИВО

Презентациското ниво извршува одредени функции кои често се повторуваат и за кои корисникот не може постојано да води сметка. За разлика од подолните нивои кои се грижат за доверлив пренос на битовите (податоците), презентациското ниво е одговорно за синтаксата и семантиката на информациите што се пренесуваат.

Типичен пример за презентациски сервис е кодирањето на податоци на стандарден, однапред договорен начин. Повеќето програми не разменуваат само случајна низа од битови. Тие разменуваат податоци, како на пр. имиња на луѓе, датуми, фактури итн. Овие податоци може да бидат од тип стринг, целобројни, со подвижна запирка и посложени податочни структури. Различните платформи користат различни кодови за приказ на текстуалните знаци (карактери), на пр. ASCII и Unicode се некои од нив. Со цел да се овозможи комуникација на различните платформи - податоците се пренесуваат кодирани на т.н. "стандарден мрежен начин". Презентациското ниво раководи со ваквото кодирање, т.е. кај испраќачот врши кодирање, а кај примачот декодирање на податоците.

2.6.1 Податочна компресија

Компресијата и кодирањето на податоци се важни, бидејќи со нив се штеди мемориски простор, како и време за трансмисија. Иако оригиналните податоци се веќе кодирани во дигитална форма за компјутерска обработка, уште поефикасно кодирање (со помалку бити) може да се добие со примена на компресирачки техники. На пример кодирањето run-length ги заменува повторувачките карактери во стрингот со еден таков карактер и бројот на појавувања. Сепак, компресираните податоци мора да се распакуваат пред да се употребат.

Постојат повеќе методи и алгоритми за компресија. Под UNIX се користи алатката compress, иако подобра е gzip. Други алатки се Winzip, pkzip, Winrar.

Перформансите на компресијата зависат од степенот (ратата) на компресија, т.е. односот на големината на податоците после и пред компресијата. Така на пример, ако некој алгоритам земе 1000B податоци и ги спакува во 500B, неговиот однос е 1:2. Поголемиот број компресирачки техники се однесуваат различно за различни типови податоци. Како и да е – стартувањето на алгоритмот за компресија врз веќе компримирани податоци – нема да придонесе за нивно натамошно намалување. Ратата на компресија е одлика на секој алгоритам.

Постојат два типа на податочна компресија. Компресиските техники што се користат кај zip датотеките и GIF сликите, се алгоритми без загуба. Ова значи дека кога ќе се компресираат податоците, а подоцна распакуваат – ќе се добијат истите оригинални податоци. Ова е многу важна карактеристика

кај zip апликациите. Сепак, кај сликите – загубата на мал дел нема да има голем ефект врз целата слика, па оваа особина не е клучна.

Кога неколку слични датотеки се компресираат, подобро е да се спојат (на пр. во еден фолдер), па да се компресираат заедно. На овој начин се постигнува подобар степен на компресија, заради начинот на кој работат алгоритмите.

Хофманово кодирање и JPEG

JPEG (Joint Photo Experts Group), создадена од ITU, ISO и други организации, дефинира стандард за компресија на слики. Овој стандард користи Хофманово кодирање за податочна компресија, користејќи ја особината дека не сите симболи во пораката се појавуваат со иста фреквенција. Во овој метод помалку бита се користат за кодирање на најчестите карактери, а со повеќе битови се кодираат поретките карактери. Значи ќе има променлив број битови за секој карактер.

Пред трансмисијата, се анализира стрингот од карактери и се одредува релативната фреквенција на секој карактер. Се формира Хофманово стебло што претставува бинарно дрво, при што на левите гранки се доделува вредност 0, а на десните – вредност 1. Бинарниот збор за секој карактер се добива одејќи од коренот кон секој лист, т.е. карактерите се сместени во лисјата.

JPEG претставува алгоритам со загуба и е погоден за кодирање слики. Се вели дека JPEG работи во секвентен мод со загуби. Главните чекори во овој алгоритам се формирање на блок, примена на дискретна косинусна трансформација (DCT), квантизација и кодирање. Во формирањето на блокот, сликата се трансформира во приказ со пиксели, што може, но не мора да предизвика намалување на резолуцијата. Пикселите се разгледуваат како групи од блокови, и се добива DCT за секој блок во вид на DCT коефициенти. Коефициентите го индицираат нивото на спектрална моќ за секоја просторна фреквенција.

Во фазата на квантизација, која внесува загуби, се користи квантизациона табела што ги трансформира DCT коефициентите. Табелата ги прави високо-фреквентните коефициенти да станат нула и тие се губат за време на кодирањето. Во последнта фаза, се применува run-length кодирање на секој блок со помош на zigzag облик на блоковите. Ова кодирање се применува само на нулите што се групирани заедно после квантизацијата. Овој процес ги компресира податоците, т.е. индивидуалните коефициенти се кодираат со помош на Хофманов код. Конечно се добива листа од броеви што ја репрезентираат сликата.

Run-length компресија

Ова е техника која користи обична логика за да го скрати последователното појавување на ист карактер. На пример, стрингот AAABBCCBBB ќе се

замени со 3A2B2C3B. За бинарни низи, заштедата ќе биде поголема, т.е. компресиониот однос - подобар. На пример, сликата може да се состои од 25 нули, па 1, па 55 нули и 1. За должините на карактерите - може да се користат бинарни вредности. На пример, низа од 15 нули може да се кодира со 1111, па така низата од 25 нули би се запишала како 1111 1010.

Методот run-length може да се користи за компресија на дигитални слики со споредба на пикселите кои се последователни и да ги кодира само промените на вредностите. Оваа техника е многу ефикасна за слики со хомогени региони и може да постигне однос на компресија 8:1. За слики со многу варијации, оваа компресија може да биде и со поголема величина од оригиналната слика.

LZW компресија

Лемпел и Зив дизајнирале метод за компресија што користи кодирачки сегменти. Сегментите од оригиналниот текст се чуваат во речник што се гради во процесот на компресија. Кога се пронајде сегмент од речникот за време на скенирањето на текстот, тој се заменува со индексот од речникот. Речникот е централна точка на алгоритамот. Сите префикси на зборовите од речникот, се исто така во речникот. За поефикасна имплементација на алгоритамот - се користи хеш техника. Алгоритамот LZ е усовршен од Велш (Welsh), и затоа е нарачен LZW. Ваквиот алгоритам е имплементиран во UNIX кај командата compress.

Кај LZW компресијата, речникот се иницијализира со сите стрингови со должина 1, т.е. буквите од азбуката. Кога читаме сегмент W од текстот и 'a' е следната буква, го запишуваме индексот W во излезен фајл и го додаваме Wa во речникот. Потоа го ресетираме W во 'a', и продолжуваме со следниот симбол. Ако Wa е веќе во речникот, продолжуваме со следниот симбол, со сегмент Wa, а не W. На почеток сегментот W се сетира да биде прв симбол од изворниот текст. Методот за декодирање е сличен, т.е. речникот се обновува во процесот на декомпресија. Се чита на пр. кодот 'c' од компресираниот фајл, во излезен фајл се запишува сегментот W (што има индекс 'c' во речникот) и се додава зборот Wa во речникот, каде што 'a' е првата буква од следниот сегмент. Програмата gzip користи една варијанта на LZW компресија.

Фрактална компресија

Фракталната компресија претставува ветувачка патентирана технологија за компресија на слики, која е посуериорна во поглед на JPEG. Таа претставува облик на векторска квантизација и е техника со загуби, која има бавна компресија и брза декомпресија. Техниката потекнува од математичарот вработен во IBM - Манделброт, уште од 1977 година. Тој тврдел дека традиционалната геометрија не е погодна за приказ на дрвјата и облаците, додека фракталната геометрија е иделна, заради конволуционите рабови и детализирањето на бесконечноста. За приближна апроксимација на

сцената се користи итеративен систем од функции (IFS). Сепак, чистата фрактална компресија не е многу ефикасна, па се користат парцијални IFS - PIFS. Со ова - трансформациите не ја пресликуваат целата слика во нејзините составни делови, туку пресликуваат поголеми во помали делови. Големите зони се наречени домен блокови, а малите - ранг блокови. Секој пиксел од оригиналната слика припаѓа барем во еден ранг блок. Множеството од ранг блокови се нарекува поделба на сликата.

Процесот на декомпресија почнува со чиста сива позадина. Потоа се применува множество трансформации и по 4 итерации - атракторот се стабилизира. Добиената слика не е реплика на оригиналот, туку е приближна со него.

Факс компресија

Со оригиналното Хофманово кодирање, може да се добие компресија на текстуален документ во однос 1:2. Подобра компресија може да се добие со скенирање на документот, со т.н. факс компресија, т.е. модифицирано Хофманово кодирање. Методот користи две табели за кодирање, т.н. составна и завршна табела за кодирање. Кодните зборови во овие табели овозможуваат комбинации од битови за црните и белите точки од скенираниот текст. Секоја линија се состои од црни и бели елементи, кои се кодираат, со што се намалува величината на сликата. На пр. некомпресирана скенирана страница има 2 милиони бити и се пренесува за 6 минути со 4800 bps. Со компресирачки однос 1:2, времето за трансмисија е скратено за пола.

MPEG и MPEG-2

Стандардите на Motion Picture Experts Group, (MPEG, MPEG-2) се користат за компресија на видео и аудио материјали. Сепак, MPEG е најефикасен за видео, бидејќи бара поголем пропусен опсег, а и видеото е поредундантно во однос на аудиото. Целта на MPEG-1 е да обезбеди видео со квалитет на видео рекордер, со примена на бит рата околу 1.2 Mbps. Компресијата е многу битна, бидејќи 1 час некопримирано видео, може да бара опсег 472 Mbps. Следната верзија на MPEG, MPEG-2, е оригинално дизајнирана да овозможи квалитет како ТВ-сигнал, т.е. 4-6 Mbps со што ќе ги покрие PAL, NTSC и HDTV.

MPEG аудио компресијата се прави со брза Фуриеова трансформација (FFT) на брановите форми. FFT го менува сигналот од временски домен во фреквентен домен. Просторната редундантност кај видеото се решава со JPEG кодирање на секоја рамка. Временската редундантност (помеѓу рамките) е незгодна, бидејќи може да бара да се води сметка за промената на сликите. Тоа се решава со блоковски промени кај последната рамка (предиктивна P рамка) или со промени кај следните рамки (бидирекциони B рамки). Кај MPEG-1 се користат и D рамки за брзо премотување на видеото, како и I рамки за неподвижни JPEG слики.

2.6.2 Енкрипција и декрипција

Мрежната безбедност не била клучна во раната фаза на компјутерските мрежи. Денес, кога милиони луѓе ги користат мрежите за банкарство, шопинг и други финансиски трансакции, мрежната безбедност е неопходна. Голем број од безбедносните проблеми се намерно предизвикани од хакери, а не се резултат на хардверска грешка.

Решението за безбедносните проблеми лежи во системите за енкрипција и декрипција. Енкрипцијата е процес со кој чистиот текст кај испраќачот се конвертира во шифриран текст со помош на клуч за енкрипција. Потоа се пренесува шифрираниот текст. Кај примачот се применува процес на декрипција за да се открие оригиналниот текст. За време на преносот - пораката може да биде пресретната и отворена од напаѓачи, но не и да биде прочитана, бидејќи е шифрирана и може да се дешифрира само со декрипцискиот клуч. Се претпоставува дека декрипцискиот клуч го знаат само испраќачот и примачот.

Традиционално, мрежната безбедност се смета како дел од презентациското ниво на ОСИ моделот. Сепак, многумина ја сместуваат и во апликативното ниво исто така. Според нас, и двата пристапи се точни. Кај моделот TCP/IP кој се состои од само четири нивоа, има смисла безбедноста да се смести кај апликативното ниво. Сепак, кај 7-слојниот ОСИ модел, презентациското ниво е она што се грижи за мрежната безбедност.

Повеќе за мрежната безбедност и за методите на енкрипција и декрипција ќе зборуваме во Поглавје 11 - Безбедност и одржување на компјутерските мрежи.

2.7 Апликациско ниво

Апликациското ниво претставува интерфејс кон корисникот, т.е. ги опфаќа апликативните програми преку кои корисникот ги користи мрежните сервиси. Според четири-слојниот TCP/IP-модел, апликативното ниво дури ги претставува заедно сесиското, презентациското и апликативното ниво од ОСИ. Во последните години се развиени многу апликации базирани на TCP/IP, а најпознати се: Telnet (далечинско логирање), FTP (File Transfer Protocol, пренос на датотеки), SMTP (Simple Mail Transfer Protocol, протокол за електронска пошта), SNMP (Simple Network Management Protocol, протокол за управување со мрежата), HTTP (Hypertext Transfer Protocol, протокол за размена на хипер-медиски информации преку Интернет, т.е. World Wide Web). Овие апликации овозможуваат да мрежата биде транспарентна кон корисникот, а му ги овозможуваат и сите споменати корисни функции (e-mail, file transfer итн.).

Основната идеја на мрежните апликации е постоењето на клиент-сервер архитектура, преку која апликативната програма (клиентот) бара услуги од друга програма (сервер), која го нуди бараниот сервис. Клиентската и

серверската програма вообичаено се лоцирани на два различни компјутери, кои се поврзани во мрежа.

Графичкиот кориснички интерфејс (GUI) овозможува интеракција помеѓу клиентската и серверската програма, односно му овозможува на корисникот да ги користи мрежните сервиси, без да има длабоко познавање на мрежните компоненти. Најпознат пример за графички интерфејс е Web browser-от, преку кој корисникот може да прави и трансфер на датотеки, со помош на хипер-линкови, без да е свесен за тоа. Во Unix - околина, графичкиот интерфејс кон корисникот е овозможен преку X-Windows, со кој е можно да се стартуваат повеќе мрежни апликации истовремено.

Апликативното ниво исто така содржи множество од протоколи, од кои најупотребуван е "виртуелниот мрежен терминал". Во светот постојат стотици некомпатибилни типови на терминали, со различен распоред на тастатурата. Со цел да се оствари разбирлива комуникација помеѓу нив, постои софтвер кој ги пресликува функциите на виртуелниот мрежен терминал, во функции на вистински терминал.

Мрежната безбедност и криптографијата, за кои се смета дека се дел од апликативното ниво, ќе бидат обработени во посебно поглавје од книгава. Во истото поглавје ќе биде обработен и протоколот за менаџмент со мрежата - SNMP.

Програмите за доделување имиња и за адресирање: DNS (Domain name system), DHCP (Dynamic Host Configuration Protocol) и WINS (Windows Internet Name Service), кои исто така претставуваат дел од апликативното ниво, ќе бидат обработени во седмото поглавје од книгава.

2.7.1 Електронска пошта

Електронската пошта, или e-mail, постои скоро 3 децении. Пред 1990, се користел само во академските кругови во САД. За време на 1990-те, станува достапен за јавноста и масовно почнува да се користи, така што бројот на e-mail пораки пратени дневно во многу го надминува бројот на класични (хартиени) писма. E-mail, како и другите видови комуникација, има свои конвенции и стилови. Во глобала, многу е неформален и лесен за користење. Луѓето кои се воздржуваат од пишување писма, не се срамат да испратат лежерно напишан e-mail.

E-mail системот има 2 главни дела: кориснички агенти и агенти за пренос на пораките. Корисничкиот агент претставува програма (т.н. читач на пораки) што овозможува разни опции - составување, примање, одговарање на пораки, и манипулација со Inbox-от. Некои mail програми имаат графичко мени и користат глушец, додека други прифаќаат команди само од тастатура. Некои имаат менија, но користат и команди од тастатура. Функционално, сите се исти.

Испраќање E-mail

За да се испрати e-mail порака, корисникот мора да ја напише пораката, да стави адреса на примачот, и некои други параметри. Пораката може да се напише во било кој текст едитор, или специјален едитор во рамки на mail програмата. Дестинационата адреса мора да е во формат кој ќе го разбере корисничкиот агент (програма). Во најголем број случаи адресата е од облик user@dns-address. DNS ќе биде објаснет во посебно поглавје. Адресата специфицира земја, регион, локација, лична адреса или име (Ken Smith). Можни се и други атрибути, така што можете да испратите e-mail до некого чија e-mail адреса не ја знаете, ако наведете доволно атрибути (на пр., компанија и звање). Иако постојат X.400 адреси кои не се интуитивни како DNS имињата, повеќето e-mail системи користат алиаси (или nicknames) што им овозможуваат на корисниците да го внесат само името на примачот и пораката ќе се испрати на саканата e-mail адреса. Значи, дури и со X.400 адреси, не е потребно да се внесува огромна адреса во неколку реда.

Повеќето e-mail системи поддржуваат mailing листи, така што корисникот може да испрати иста порака до повеќе луѓе истовремено. Ако mailing листата се одржува локално, корисничката програма испраќа поединечна порака до секој примач. Сепак, ако листата се одржува далечински, пораката ќе замине сама, а ќе се умножи на оддалечениот сервер.

На пример, ако некои љубители на птици имаат mailing листа наречена birders, инсталирана на meadowlark.arizona.edu, пораката испратена до birders@meadowlark.arizona.edu ќе биде проследена до Универзитетот Arizona, а потоа посебни пораки ќе се испратат до сите членови на mailing листата, било каде да се наоѓаат. Корисниците надвор од mailing листата не мора да знаат тоа е mailing листа. Тоа можеби е личната адреса на Prof. Birders.

Читање E-mail

Типично, кога е стартувана корисничката програма, таа го отвара Inbox-от со примените пораки. Исто така го означува бројот на непрочитани пораки во mailbox и дава по една линија опис (Subject) за секоја порака. Како пример за кориснички агент (програма), да разгледаме типично сценарио за mail. По стартувањето на корисничката програма, корисникот сака да види листа на примените пораки. Секоја линија се однесува на посебна порака. Сега ќе се осврнеме на форматот на e-mail пораките. Прво ќе го разгледаме основниот ASCII e-mail дефиниран со RFC 822. После тоа ќе ги разгледаме мултимедиските проширувања на RFC 822.

RFC 822 формат

Пораката се состои од т.н. плик (опишан со RFC 821), неколку полиња за заглавје, празна линија, па тело на пораката. Секое заглавје се состои од една линија ASCII текст што го содржи насловот на полето, колона и вредноста

на полето. RFC 822 е дизајниран пред 30 години и не ги разликува полињата на пликот од заглавјата. Иако е ревидиран во RFC 2822, комплетна преработка не била можна заради широката примена. Во нормални услови, корисничкиот агент (програма) ја пишува пораката и ја доставува до трансфер-агентот, кој ги користи заглавјата за да го формира пликот.

Типични полиња со заглавја се To, Cc, Bcc. Полето To: ја дава DNS адресата на главниот примач. Дозволено е да имаме повеќе примачи. Полето Cc: ја дава адресата на секундарните примачи. Во поглед на преносот, нема разлика помеѓу примарниот и секундарните примачи. Разликата е чисто психолошка – кој е примарен, а кој секундарен примач, но е неважно за mail системот. Терминот Cc: (Carbon copy) е застарен, но сеуте се користи. Полето Bcc: (Blind carbon copy) е слично со полето Cc:, освен што адресите наведени во него не се прикажуваат кај примарниот и секундарните примачи. Оваа особина им овозможува на луѓето да испраќаат копии до трети лица без примарниот и секундарните примачи да знаат за тоа.

MIME—Multipurpose Internet Mail Extensions

Во раните години на ARPANET, e-mail-от се состоел само од текстуални пораки напишани на англиски и претставени со ASCII. За таа намена, RFC 822 бил сосема доволен: тој ги дефинира заглавјата, но ја остава содржината целосно на корисникот. Денес, на глобалниот Internet, овој пристап не е адекватен.

Потребно е испраќање и примање на:

- Пораки во јазици со акценти (на пр., француски, германски).
- Пораки во не-латинични јазици (на пр., македонски).
- Пораки во јазици без азбука (на пр., кинески).
- Пораки кои не содржат текст - attachments (на пр., audio или слики).

Предложено е решението RFC 1341 и е дополнето во RFCs 2045–2049. Ова решение наречено MIME (повеќенаменски Internet Mail екстензии) денес се користи масовно. Во продолжение ќе го опишеме.

Основната идеја на MIME е проширена употреба на форматот RFC 822, но давање структура на телото од пораката и кодирачки правила за не-ASCII пораките. Бидејќи концепцијата на RFC 822 не е напуштена, MIME пораките можат да се испраќаат со постоечките mail програми и протоколи. Сè што треба да се избере е која програма за примање и испраќање пораки, ќе ја користиме.

MIME дефинира 5 нови заглавја: MIME Version, Content Description, Content ID, Content Encoding и Content Type. Првото заглавје и кажува на програмата што ја прима пораката дека добиената порака е MIME, и која верзија на MIME користи. Ако пораката не користи заглавје MIME-Version, се претпоставува дека е чист текст напишан на англиски и се пренесува како таков.

SMTP—Simple Mail Transfer Protocol

Системот за пренос на пораки ги проследува пораките од испраќачот кон примачот. Наједноставен начин е да се воспостави транспортна конекција од изворната до одредишната машина и потоа да се пренесе пораката. Ќе разгледаме случаи кога ова функционира без проблеми, и случаи кога не функционира.

Кај Internet, пораката се доставува кога машината на испраќачот ќе воспостави TCP конекција со порта 25 на одредишната машина. На оваа порта е активиран e-mail демон што го разбира SMTP (едноставен протокол за пренос на пораки). Овој демон ги прифаќа доаѓачките конекции и ги копира пораките во соодветните сандачиња. Ако пораката не може да се достави, се дава извештај за грешка во горниот дел од недоставената порака, и се враќа кон испраќачот.

SMTP е едноставен ASCII протокол. По воспоставувањето на TCP конекција до порта 25, испраќачот, кој работи како клиент, чека од примачот, т.е. сервер, да добие сигнал. Серверот испраќа линија текст кажувајќи го својот идентитет и потврдува дали е спремен да прими порака. Ако не е, клиентот ја ослободува конекцијата и се обидува подоцна.

Ако серверот е спремен да ја прифати пораката, клиентот означува од каде доаѓа пораката и кон кого е упатена. Ако постои наведениот примач на одредишната адреса, серверот му одобрува на клиентот да ја испрати пораката. Тогаш клиентот ја испраќа пораката и серверот ја доставува. Не се потребни проверки, бидејќи TCP обезбедува доверлив пренос. Ако има повеќе пораки – сите се испраќаат заедно. Кога ќе се разменат сите пораки во двете насоки, конекцијата се ослободува.

POP3 доставување на пораките

Сè до сега, претпоставувавме дека корисниците работат на машини што се способни за примање и праќање на e-mail. Како што видовме, e-mail-от се испраќа кога испраќачот ќе воспостави TCP конекција до примачот, а после ја испорачува пораката преку таа конекција. Овој модел работи со години, бидејќи ARPANET (а подоцна Internet) хостовите биле, всушност цело време on-line и прифаќале TCP конекции.

Сепак, голем број корисници пристапуваат на Internet со dial-up модем, па горното не важи. Проблемот е следниот: што ако Elinor сака да прати порака до Carolyn, а Carolyn не е моментално on-line? Elinor не може да воспостави TCP конекција до Carolyn и така не може да го стартува SMTP протоколот. Едно решение е да се има агент за трансфер на пораки на провајдерската машина што ги прифаќа пораките на корисниците и ги чува во нивни поштенски сандачиња на таа машина. Бидејќи агентот може да биде on-line цело време, e-mail-от може да се испрати 24 часа на ден.

За жал, ова креира друг проблем: како корисникот го прима e-mail-от од агентот за трансфер на пораки на провајдерот? Решението на овој проблем е

во креирање на посебен протокол, со кој агентот за трансфер на корисникот (клиентскиот PC) ќе го контактира агентот за трансфер на провајдерскиот сервер и ќе овозможи да се копира e-mail-от од серверот на корисничкиот компјутер. Овој протокол е POP3 (Post Office Protocol 3), кој е опишан во RFC 1939.

POP3 се стартува кога корисникот ќе ја отвори својата e-mail програма. Читачот на mail се обраќа кај провајдерот (или веќе сме на Интернет) и воспоставува TCP конекција со агентот за пренос на пораки на порта 110. Откако е воспоставена конекцијата, протоколот POP3 се состои од следните 3 чекори:

1. Авторизација.
2. Трансакции.
3. Ажурирање.

Авторизацијата проверува дали корисникот е логиран. Трансакцијата води сметка за означување на пораките кои подоцна би се избришале од mailbox. Ажурирањето води сметка за тоа кои пораки се избришани.

2.7.2 World Wide Web

World Wide Web претставува архитектура за пристап до поврзани документи кои се наоѓаат на милиони различни машини на Internet. За само 10 години, вебот стана не само начин за пристап до податоци, туку и поим што за милиони луѓе значи зборот "Internet". Неговата огромна популарност доаѓа од графичкиот интерфејс што е лесен за почетници, и огромната количина на информации што се наоѓаат на веб - од aardvarks до Zulus. Ако податокот што го барате го нема на веб, бидете сигурни дека и воопшто го нема.

Web (исто познат како WWW) е развиен во 1989 на CERN, Европски центар за нуклеарни истражувања. CERN има повеќе истражувачки тимови во различни земји. Web-от бил создаден од потребата да се разменуваат и да се споделуваат голем број на извештаи, графикони, фотографии и други документи. Иницијалниот предлог за web-поврзани документи, дошол од физичарот Tim Berners-Lee во март 1989. Првиот (текст-базиран) прототип веќе функционирал 18 месеци подоцна. Во декември 1991, имало јавна презентација на Конференцијата Hypertext '91 во San Antonio, Texas.

Оваа презентација и присутната публика го свртеле вниманието на сите истражувачи, што довело Marc Andreessen од Универзитетот во Илиноис да почне да го развива првиот графички пребарувач (browser), Mosaic. Тој бил готов во февруари 1993. Mosaic бил толку популарен што, Andreessen формирал своја компанија, Netscape Communications, чија цел била да развива клиенти, сервери, и друг Web-базиран софтвер. Кога Netscape бил готов во 1995, инвеститорите помислиле дека тоа е новиот Microsoft, и платиле 1.5 милијарда долари за неговите акции. Овој рекорд бил многу изненадувачки, со оглед што компанијата располагала само со еден производ, била многу задолжена, и предвидувала дека ќе нема профит во

следните неколку години. Во следните 3 години, Netscape Navigator и Microsoft Internet Explorer влегуваат во "browser" војна, секоја додавајќи повеќе можности (и повеќе bug-ови) во својот пребарувач. Во 1998, America Online го купи Netscape Communications за 4.2 милијарди долари, со што заврши краткиот живот на Netscape како независна компанија.

Во 1994, CERN и M.I.T. потпишаа договор со кој се формира World Wide Web Конзорциум (скратено W3C), организација што ќе биде задолжена за понатамошниот развој на Web, за стандардизирање на протоколите, и за компатибилност помеѓу сајтовите. Berners-Lee стана негов директор. Оттогаш, илјадници универзитети и компании му се придружиле на Конзорциумот. Иако денес има стоцици книги за Web, сепак, најдобрата информација што можете да ја добиете за Web-от, се разбира се наоѓа на Web. Официјалната страна на Конзорциумот е www.w3.org. Заинтересираните читатели на оваа страница ќе најдат линкови кон многубројните документи и активности на Конзорциумот.

Архитектура на WWW

Од гледиште на корисникот, Web се состои од огромна колекција на документи т.н. Web страни, кои се складирани на различни машини ширум светот. Секоја страница може да содржи линкови (врски) кон друга страница, сместена на било кое место. Корисникот го отвора линкот со кликање врз него, со што ќе ја отвори страницата кон која покажува линкот. Овој процес се повторува бесконечно. Идејата за линк од една страница кон друга, е наречена hypertext, и била воведена од професорот по електротехника на M.I.T. - Vannevar Bush, во 1945, долго пред да се измисли Internet.

Страниците се отвораат со т.н. пребарувач (browser), при што Internet Explorer и Netscape Navigator се два познати пребарувачи. Пребарувачот ја вчитува бараната страна, ја интерпретира нејзината содржина и соодветно форматирана ја прикажува на екранот. Во голем број случаи, веб страницата почнува со наслов, содржи информации и на крај завршува со e-mail адреса на оној што ја одржува (webmaster). Текстот што претставува врска кон друга веб страна, е наречен hyperlink, и е прикажан со друга боја или подвлечен. За да отвори линк, корисникот го носи поентерот на глушецот врз него, со што курсорот добива друг облик, па клика. Иако постојат не-графички пребарувачи, како Lynx, тие не се толку популарни како графичките, и се користат многу ретко. Развиени се и пребарувачи базирани на гласовни команди.

Клиентска страна

Да ја разгледаме клиентската страна во детали. Во суштина, пребарувачот е програм што ја прикажува веб страницата и ги прифаќа кликовите на глушецот и другите кориснички влезови. Кога ќе се одбере некоја ставка,

пребарувачот го следи hyperlink-от и вчитува нова страница. Затоа на hyperlink-от му треба начин за именување на Web страниците.

Страниците се именуваат со помош на URL (Uniform Resource Locators). Типичен URL е http://www.abcd.com/products.html. Важно е да се забележи дека URL содржи 3 дела: име на протоколот (http), DNS име на машината каде е сместена страницата (www.abcd.com), и име на фајлот што ја содржи страницата (products.html). Кога корисникот клика врз hyperlink, пребарувачот презема серија на чекори со цел да ја вчита саканата страница.

Да претпоставиме дека корисникот сурфа на Web и сака да ја посети страницата на ITU, која гласи http://www.itu.org/home/index.html. Да ги разгледаме чекорите кои се реализираат.

1. Пребарувачот го утврдува URL-то (т.е. гледа што е внесено или кликнато).
2. Пребарувачот го прашува DNS-серверот за IP адресата на www.itu.org.
3. DNS-серверот одговара со 156.106.192.32.
4. Пребарувачот прави TCP конекција до порта 80 на 156.106.192.32.
5. Пребарувачот испраќа барање за фајлот /home/index.html.
6. Серверот www.itu.org ја испраќа датотеката /home/index.html.
7. TCP конекцијата се ослободува.
8. Пребарувачот го прикажува текстот на документот /home/index.html.
9. Пребарувачот ги вчитува и ги прикажува сликите од овој фајл.

Повеќето пребарувачи прикажуваат до кој чекор стигнале во статусна линија – на дното од екранот. На овој начин, ако перформансите на мрежата се слаби, корисникот ќе види дали DNS не одговара, веб серверот не одговара, или настанало натрупување на мрежата.

За да прикаже една страна, пребарувачот мора да го разбере нејзиниот формат. За да можат сите пребарувачи да ги отвораат сите Web страници, страниците се пишуваат во стандарден јазик HTML, кој ги опишува веб содржините.

Иако пребарувачот во основа е HTML интерпретер, повеќето пребарувачи нудат разни копчиња и опции за да се олесни навигацијата по Web. Повеќето содржат копче за одење назад кон претходната страна, копче за одење напред кон следната страна (ако веќе сме биле кај неа), и копче за одење на почетната (home) страница. Повеќето пребарувачи имаат копче или мени Bookmark (Favourites), за да можат да ја отворат саканата страница многу брзо при следните посети. Страниците можат исто така да се испечатат или снимат на диск. Се нудат многу опции за изгледот на екранот, величината на фонтовите и различни кориснички подесувања.

Како додаток на обичниот текст и hypertext-от, Web страницата може да содржи икони, цртежи, мапи, и фотографии. Секоја од нив може да претставува линк кон друга страница. Кај фотографиите и мапите, може да

се направи линк кон друга страница, ако се кликне на одреден дел од сликата.

Не сите страници содржат HTML. Страницата може да содржи документ во PDF формат, икона во GIF формат, фотографија во JPEG формат, песна во MP3 формат, видео во MPEG формат, и стотици други типови на датотеки. Бидејќи стандардните HTML страници можат да содржат непостоечки линкови, пребарувачот понекогаш има проблем да ја интерпретира страницата.

Серверска страна

Многу работи се веќе направени на клиентската страна. Сега да ја разгледаме серверската страна. Како што спомнавме, кога корисникот ќе внесе URL или кликне на линк, пребарувачот го дели URL-то и го преведува делот помеѓу http:// и следната коса црта, како DNS-име на веб серверот што се бара. Добивајќи ја IP адресата на серверот, пребарувачот воспоставува TCP конекција со порта 80 на тој сервер. Потоа го праќа остатокот од URL-то, што претставува име на бараниот фајл (најчесто .html), сместен на серверот. Серверот го наоѓа фајлот и му го праќа на пребарувачот. Во кратки црти, чекорите што ги извршува серверот се следните:

1. Ја прифаќа TCP конекцијата од клиентот (browser-от).
2. Го презема името на бараниот фајл (најчесто .html).
3. Го вчитува HTML фајлот (од диск).
4. Го испраќа фајлот на клиентот.
5. Ја ослободува TCP конекцијата.

Модерните Web сервери имаат многу повеќе можности, но во суштина тоа се нивните главни задачи.

3 МРЕЖНА ИНФРАСТРУКТУРА

3.1 МЕТОДИ НА ПРИСТАП

Мрежите се организирани во стандардизирани форми или архитектури, и секоја претставува комплетен систем на компатибилен хардвер, протоколи, преносни медиуми и топологии. Топологијата е всушност мапата на мрежата, таа е план на кој начин мрежните кабли ги поврзуваат мрежните јазли (nodes) или уреди, и како тие функционираат едни во однос на други.

Еден од најзначајните фактори со кои се обликуваат мрежните топологии е изборот на методот за пристап (access method). Методот за пристап е множество на правила за делење на преносниот медиум. Во ова поглавје се опишани двете најважни категории на пристап кон медиумот: натпреварување (contention) и додавање на токени (token passing). Ќе бидат објаснети CSMA/CD и CSMA/CA, како два начини за пристап со натпреварување, како и Ethernet, token-ring, ARCNet, и FDDI мрежите, кои го користат или методот на натпревар, или методот со проследување на токени.

3.1.1 Начини на пристап кон преносниот медиум

Метод на пристап (access method) е множество на правила преку кои се определува како мрежните јазли го делат преносниот медиум. Правилата за делење помеѓу компјутерите се слични како и кај луѓето, и може да се сведат на два основни концепти:

1. Прв пристигнат, прв услужен;
2. Наизменично.

Преку овие концепти се дефинираат трите најважни видови на методи на пристап кон медиумот:

- Натпревар (Contention). Ова значи дека компјутерите се натпреваруваат за користење на преносниот медиум, и секој компјутер во мрежата може да врши емитирање во било кое време (прв пристигнат – прв услужен).
- Повикување (Polling). Еден уред е одговорен за повикување на другите уреди за да се види дали тие се подготвени за пренесување или примање на податоци.
- Проследување на токени (Token passing). Компјутерите пристапуваат кон медиумот кога ќе им дојде редот за користење.

Методите базирани врз начинот на натпревар, доведуваат до ситуација каде што два или повеќе мрежни јазли се обидуваат да вршат емитување (broadcast) истовремено и нивните сигнали се судруваат, односно се појавува колизија. Затоа се специфицираат процедури за избегнување на колизиите, т.е. што да се направи кога ќе се појави таква ситуација. Претставени се

CSMA/CD и CSMA/CA методи за пристап. На повеќето мрежи базирани врз методата - натпревар за пристап до медиумот, јазлите се во основа еднакви меѓусебно; ниту еден јазол нема поголем приоритет во однос на другите јазли, иако новата метода за пристап наречена demand priority, покрај тоа што ги разрешува натпреварувањето и колизиите, има во предвид и приоритети за пренос на одредени типови на податоци.

3.1.2 Натпревар (Contention)

Во контролата на пристап заснована на натпреварување, секој компјутер може да емитува во било кој момент. Ваквиот систем потфрлува во случај кога два компјутери ќе се обидат да емитуваат сообраќај истовремено, во тој случај се појавува судир, односно колизија (слика 3.1). Ако мрежата е премногу оптоварена, повеќето од обидите за пренос на податоци резултираат со колизии и се остварува намалена ефективна комуникација.

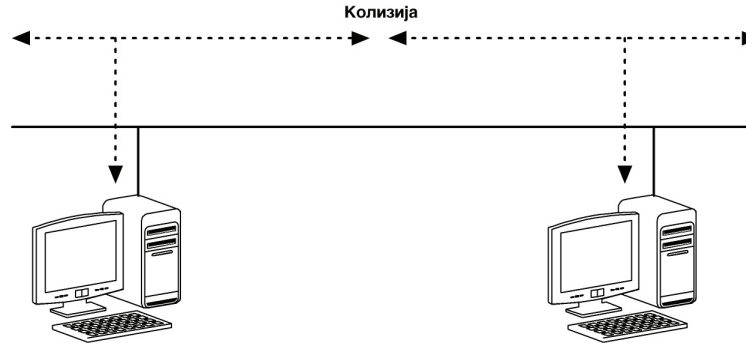
За намалување на колизиите се користат разни механизми, а еден од нив е „чувствување на носачот“ (carrier sensing), каде што секој компјутер ја ослушнува мрежата пред да се обиде да емитува податоци за пренос. Ако мрежата е зафатена, компјутерот се откажува од трансмисија сè додека не се ослободи мрежата; ова е едноставна „слушај пред да зборуваш“ стратегија која значително ги намалува колизиите.

Другиот механизам се нарекува „детекција на носачот“ (carrier detection). Со оваа стратегија, компјутерите продолжуваат да ја ослушнуваат мрежата и при трансмисијата. Ако еден компјутер детектира друг сигнал кој се меша со сигналот кој тој го испраќа, прекинува веднаш со преносот. Двата компјутери чекаат случајно време и се обидуваат повторно да пренесуваат. Освен ако мрежата е премногу оптоварена, двата наведени механизми можат да се справат со поголемо количество на трансмисии.

Детекцијата на носачот и чувствувањето на носачот, користени заедно формираат протокол што се користи во сите видови на Ethernet мрежи: Carrier Sense Multiple Access with Collision Detection (CSMA/CD). CSMA/CD ја ограничува големината на мрежата до 2500 метри. На поголеми растојанија, механизмот за препознавање и чувствување на преносот не може успешно да работи од причина што јазолот на едниот крај не може да го почувствува преносот од јазолот кој се наоѓа на другиот крај на мрежата.

Сличен протокол наречен Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) кој се користи во Apple LocalTalk мрежите, користи дополнителни техники за намалување на веројатноста на појава на колизии. Во CSMA/CA, секој компјутер објавува предупредување дека ќе започне со пренесување на податоци на мрежата, па другите компјутери чекаат на преносот. CSMA/CA помага за поуспешно намалување на колизиите, меѓутоа пораките за предупредување го зголемуваат мрежниот сообраќај, а задачата за константно ослушнување на медиумот дополнително ги оптоварува јазлите.

Методите за пристап со натпревар, иако се чини дека се неупотребливи заради ризикот од колизии, всушност се најкористените методи за контрола на пристап кон медиумот (особено CSMA/CD во облик на Ethernet) на локалните мрежи (LAN). Ниту еден од користените LAN стандарди не применува полна контрола на пристап преку натпревар, без додавање на некои механизми за намалување на појава на колизиите.



Слика 3.1: Појава на колизии на мрежа која користи метода на натпревар за контрола на пристап

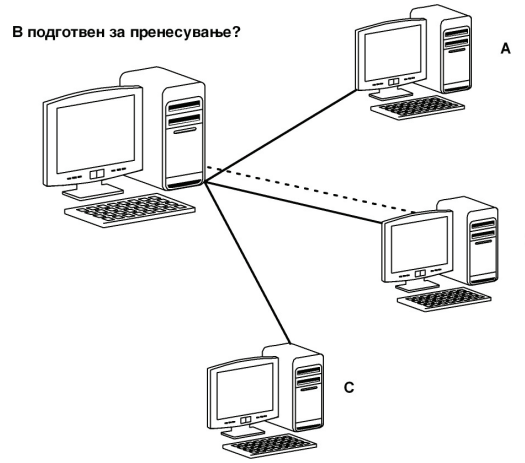
Натпреварување за пристап кон медиумот е едноставен протокол што може да се изведе со едноставен мрежен софтвер и хардвер. Сè додека нивото на оптовареност на достапниот преносен опсег (bandwidth) не премине преку 30%, методот работи добро и нуди добри перформанси за ниска цена. Бидејќи колизиите се појавуваат во непредвидени интервали, на ниеден компјутер не му е гарантирана можноста да врши пренесување во било кој момент. Ваквите мрежи се нарекуваат „веројатностни“, затоа што можноста за емитување на еден компјутер не може прецизно да се определи.

Честотата на појава на колизиите се зголемува со зголемувањето на бројот на компјутерите во мрежата. Кога многу компјутери ја користат истовремено мрежата, колизиите можат да бидат доминантен дел од мрежниот сообраќај и само мал дел од податочните рамки се пренесуваат без грешки. Бидејќи сите компјутери се еднакви на мрежата, не постои можност да се даде приоритет за пренесување на одреден компјутер, а со тоа и поголем пристап кон мрежата. Контролата на пристап кон медиумот со натпреварување е погодна за користење на мрежи кои имаат напливи (burst) во сообраќајот и имаат релативно мал број на компјутери.

3.1.3 Повикување (Polling)

Системите базирани на повикување бараат постоење на уред (наречен контролер или „master“ уред) за повикување на други уреди на мрежата, за да се види дали се подготвени за пренесување или за примање на податоци, како што е прикажано на сликата 3.2. Оваа метода не е широко користена кај мрежите, бидејќи прозивката може да предизвика значителен мрежен

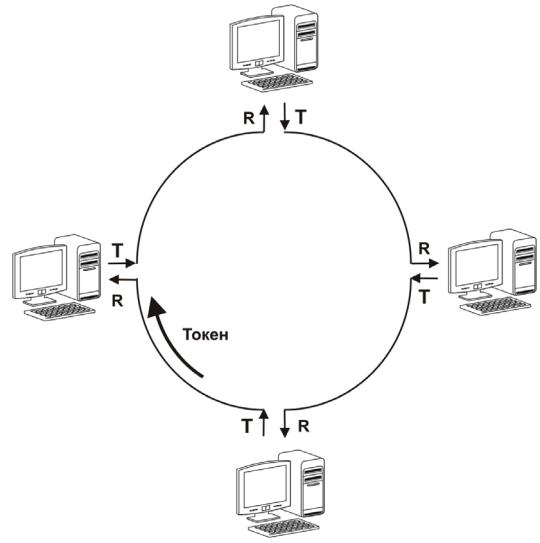
сообраќај. Наједноставен пример за прозивка е кога компјутерот го повикува својот печатар за примање на „print job“.



Слика 3.2: Повикување на уредите на мрежата

3.1.4 Проследување на токени (Token Passing)

Проследувањето на токени користи податочна рамка наречена токен (*token)*, која кружи околу мрежата. Компјутерот кој има потреба да емитува, треба да чека сè додека не прими токен со кој му се дозволува да пренесува на мрежата. По завршувањето на преносот, ја додава токен-рамката кон следната станица на мрежата. Сликата 3.3 прикажува како се имплементира методата за проследување на токенот низ „token-ring“ мрежа.



Слика 3.3: Проследување на token-и

Неколку мрежни стандарди користат начин на контрола на пристап преку проследување на токени:

- Token ring. Најпознатиот стандард опишан во IEEE 802.5 стандардот.
- IEEE standard 802.4; ретко применуван, дефинира мрежа со магистрала (bus) кој исто така користи токени за контрола на пристап.
- FDDI. Стандард за оптичка мрежа со брзина од 100Mbps која користи проследување на токени преку прстен на сличен начин како и 802.5 token ring.

Методите за проследување на жетони можат да користат приоритети за станиците и други начини за одбегнување на монополизација на мрежата од страна на една станица. Бидејќи секој компјутер има можност за емитирање, секој пат кога токенот патува по мрежата, на секоја станица и се гарантира можност за пренос во одреден временски интервал.

Проследувањето на токени е попогодно за користење од методата на натпреварување во следниве услови:

- Кога мрежата пренесува податоци за кои е критично времето. Бидејќи проследувањето на токени резултира во попредвидливо пренесување, ваквите мрежи се нарекуваат детерминистички.
- Кога мрежата трпи поголемо оптоварување. Перформансите на токен мрежите помалку опаѓаат во однос на мрежите кои користат натпревар за медиумот. Мрежите со проследување на токени не можат да станат „натрупани“ заради преголем број на колизии.
- Кога некои станици треба да имаат поголем приоритет од другите. Некои шеми поддржуваат доделување на приоритети за пренесување.

3.1.5 Споредба на контрола со натпревар и преку проследување на токени

Како начин за контрола на пристап, проследувањето на токени е многу посупериорно во однос на методата со натпреварување, иако Ethernet кој користи контрола на пристап со натпреварување е далеку подоминантен стандард за локалните компјутерски мрежи.

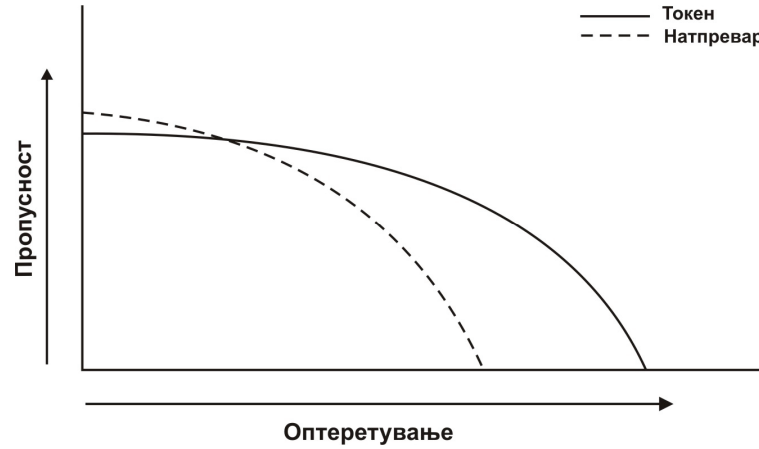
Проследувањето на токени бара повеќе сложени контролни механизми, и потребниот хардвер е значително поскап во однос на хардверот потребен за имплементација на поедноставните механизми за натпреварување за медиумот. Повисоката цена за поставување на мрежи со проследување на токени не се оправдани освен ако нема одредени специјални барања.

Бидејќи мрежите со токени се дизајнирани за поголема сигурност, се вградуваат и дополнителни можности за дијагностика и отстранување на

проблеми во мрежниот хардвер, со што дополнително се зголемува и цената на чинење.

Иако мрежите со токени имаат подобри перформанси од мрежите со натпреварување, при услови на поголемо оптоварување, овие вторите појавуваат подобри перформанси во услови на значително помало оптоварување.

Проследувањето на токенот по мрежата (и другите придружни операции) го користат достапниот преносен опсег. Како резултат на тоа, Ethernet со 10Mbps и мрежата со токени со 16Mbps се однесуваат слично при помал мрежен сообраќај, со таа разлика што Ethernet чини значително помалку.



Слика 3.4: Карактеристики на методите на контрола на пристап.

3.1.6 Барање за приоритет (Demand Priority)

Барање за приоритет е метода за пристап користена во новиот стандард 100Mbps 100VG-AnyLAN. Иако официјално е разгледуван како метода за пристап со натпреварување, барање на приоритет значајно се разликува од основниот CSMA/CD Ethernet. Во ова метода, мрежните јазли се поврзани со хабови (hubs), и овие хабови се поврзани со други. Така, натпреварувањето се појавува во уредите -хабови. (100VG-AnyLAN каблите можат да примаат и предаваат податоци во исто време). Барањето за приоритет обезбедува механизам за давање на приоритет на одредени типови на податоци; ако се појави колизија - податоците со поголем приоритет имаат можност за пренесување.

3.2 Топологии

Мрежната топологија дефинира начин на кој меѓусебно се поврзуваат компјутерите, печатарите и други уреди. Изборот на топологијата има големо влијание врз начинот на работата на мрежата.

Мрежната топологија може да биде физичка или логичка топологија. Физичката топологија е мапа или опис на поставувањето на мрежниот медиум кој ги поврзува уредите на мрежата. Физичките топологии кои се имплементирани денес вклучуваат магистрала (bus), прстен (ring), ѕвезда (star), мрежеста (mesh), како и хибрид од повеќе топологии во една мрежа. Логичката топологија го дефинира начинот на кој уредите комуницираат и пренесуваат податоци по мрежата, тоа може да биде во форма на магистрала или прстен.

3.2.1 Физички наспроти логички топологии

Во терминологијата користена во компјутерските мрежи, физичкото поставување на мрежните уреди на медиумот, претставува физичка топологија.

Начинот на кој податоците пристапуваат кон медиумот и се пренесуваат во форма на пакети преку мрежата, е логичката топологија на мрежата.

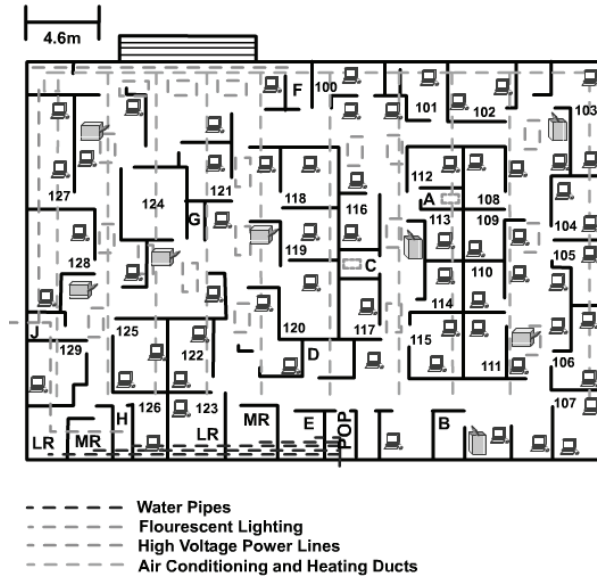
Логичката топологија може да биде иста со физичката, но во повеќето случаи тоа не е така; ако на пример земеме дека еден мрежен кабел се поврзува од централната единица за ожичување (ормар) кон секој уред во мрежата - тоа може да се означи и како физичка и како логичка топологија на ѕвезда. Но зависно дали уредот се поврзува во ормарот на хаб, или со MTU уред (Multistation Access Unit), логичката топологија може да биде магистрала или прстен, значи да нема логичка топологија на ѕвезда.

Изборот на логичката топологија може да влијае на физичкото поставување на каблите и обратно. Решението кое ќе се применува подоцна ќе биде тешко за измена, затоа треба да се согледаат ограничувањата на физичката и логичката топологија, пред донесување на конечното решение кој вид на мрежа да се поставува. На пример, физичката топологија на ѕвезда обично користи логичка топологија на магистрала, физичката топологија на прстен обично користи логичка топологија на прстен. И физичката и логичката топологија имаат влијание на начинот како ќе се поставуваат каблите, кои мрежни уреди ќе се користат и кои протоколи ќе се имплементираат за пренесување на податоците.

Најбитната карактеристика на која треба да се внимава при дизајнирање на мрежите е можноста за идно проширување на мрежата и пропусниот опсег. Ако се избере погрешна топологија на самиот почеток, ќе се појави потреба за целосно преинсталирање на мрежниот медиум и купување на нови мрежни уреди.

3.2.2 Видови на физички топологии

Физичките топологии се дефинираат според начинот на кој мрежниот медиум ги поврзува уредите. Дијаграмот на физичката топологија на мрежата, ја покажува патеката на медиумот за поврзување на секој уред на мрежата.

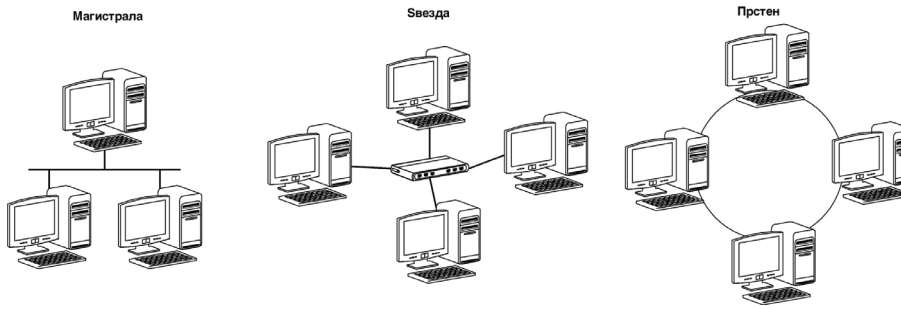


Слика 3.5: Физичка топологија на мрежа.

Трите најкористени физички мрежни топологии се магистрала (bus), прстен (ring), и ѕвезда (star). Видот на физичката топологија кој ќе биде избран за примена, ќе има влијание на начинот на комуникација на мрежните уреди. Покрај тоа треба внимателно да се земат во предвид и следниве фактори:

- Цена на чинење (Cost)
- Скалабилност (Scalability)
- Преносен капацитет (Bandwidth capacity)
- Едноставност на инсталацијата (Ease of installation)
- Едноставност на решавањето на проблеми (Ease of troubleshooting)

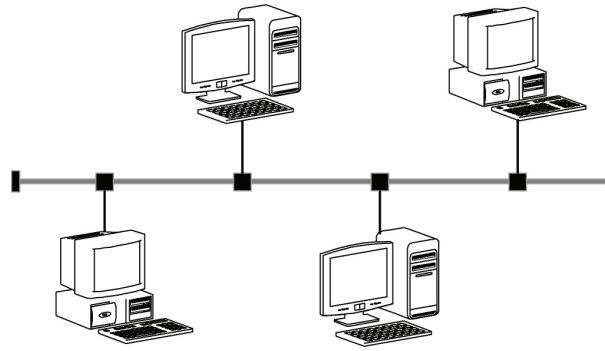
Поголемиот дел од постоечките компјутерски мрежи ги користат топологиите ѕвезда, проширена ѕвезда или хибридната топологија, со што се овозможува имплементација или на Ethernet или Token Ring стандардот.



Слика 3.6: Најкористени видови на топологии

Топологија на магистрала

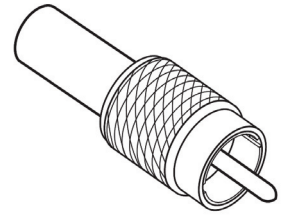
Мрежите кои имаат физичка топологија на магистрала обично користат коаксијален кабел кој ги поврзува мрежните јазли преку BNC конектор.



Слика 3.7: Топологија на магистрала

Како што може да се види од сликата, овој вид на конектор може да се користи за поврзување на два или повеќе компјутери во „daisy chain“ начин, или може да се додаде терминатор на едниот дел од кабелот. Стандардот на организацијата - Institute of Electrical and Electronics Engineers, IEEE 802.3 ги поставува ограничувањата во однос на должината на кабелскиот сегмент и бројот на уредите на Ethernet магистралата.

За таканаречена „Thinnet“ мрежа, означена како 10Base2 или Thin Ethernet, најголемата должина на сегмент е 185 метри и поврзува најмногу до 30 уреди. Може да се користат најмногу 4 засилувачи - рипитери (repeaters) за поврзување на најмногу 5 сегменти, од кои три можат да содржат уреди, што дава должина на кабелот од 925 метри и број на мрежни јазли 150.



Слика 3.8: BNC конектор

Друга опција која се користи е „Thicknet“, уште позната како Thick Ethernet или 10Base5. Thicknet каблите користат подебел коаксијален кабел од Thinnet, и се чест избор за backbone инсталации. Ограничувањето на кабелскиот сегмент е 500 метри, со најмногу 1000 јазли по сегмент. Thicknet дозволува и најмногу 4 засилувачи со вкупна должина од 2400 метри и 300 јазли. Многу е битно да се почитуваат стандардите на мрежните медиуми за да се обезбеди доверлив пренос на податочните пакети.

Предностите на топологијата на магистрала се:	Недостатоците на топологијата на магистрала се:
• Цената на инсталацијата на магистралата. • Лесно додавање на нови јазли. • Користи помалку кабел од другите физички топологии. • Оваа топологија најдобро работи за мали мрежи (2–10 уреди).	• Не се препорачува за нови инсталации, застарена. • Ако се прекине „backbone“- целата мрежа е вон функција. • Може да се вклучат само ограничен број на уреди. • При појава на проблем тешко се лоцира. • Делењето на ист кабел доведува до бавно време на пристап.

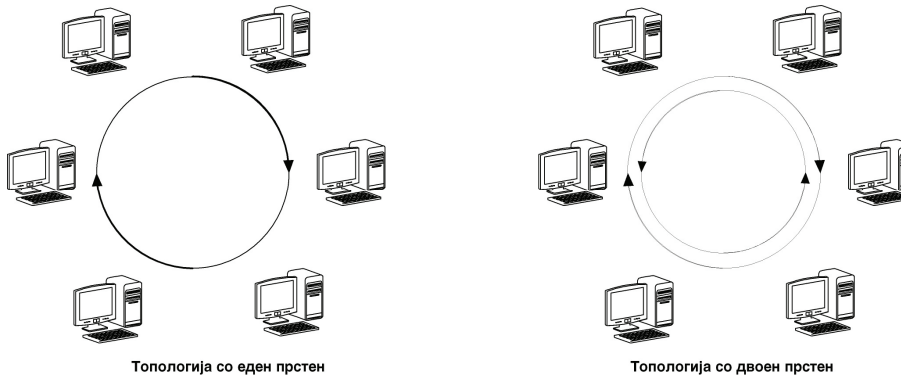
Топологија на прстен (Ring Topology)

Како што и самото име кажува, топологијата на прстен е топологија во која станиците се поврзани во облик на прстен или круг (физички прстен), каде што податоците кружат по прстенот од станица до станица (логички прстен). Не постои почеток или крај што треба да се затвори т.е. терминира. Со тоа се овозможува секој уред да има подеднаков третман за пристап кон медиумот. Постојат два вида на топологии на прстен:

- Единечен прстен;
- Двоен прстен.

При инсталацијата на првите мрежи што ја користеле топологијата на прстен, тие ја користеле првата варијанта на единичен прстен, како што е прикажано на сликата. Во мрежа со единичен прстен, еден кабел се дели помеѓу сите уреди и податоците се движат само во еден правец. Секој уред

чека на својот ред да пренесува податоци. Кога податоците ќе пристигнат на одредиштето, тогаш друг уред добива право да пренесува. Најпозната имплементација на топологијата на прстен е Token Ring мрежата. Со развојот на технологијата се развила и топологијата на двоен прстен, и таа овозможува два прстени да пренесуваат податоци во различни насоки. Не само што се овозможило повеќе пакети да патуваат по мрежата, туку и преносот се одвива по должината на медиумот со што се добива и редундантност на мрежата. Fiber Distributed Data Interface (FDDI) е технологија слична на Token Ring, но користи оптика за пренесување на податоците. FDDI мрежите користат два прстени заради редундантноста; при прекинот на еден прстен, оваа мрежа продолжува непречено да функционира.



Слика 3.9: Видови на топологии со прстен

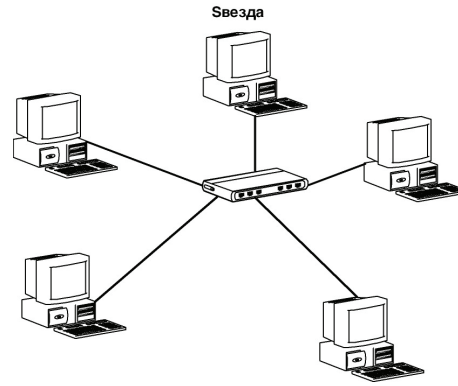
Предностите на топологијата со прстен се:	Недостатоците на топологијата со прстен се:
• Податочните пакети се движат со поголема брзина. • Не постојат колизии. • Полесно се лоцираат проблемите на мрежата. • Не се потребни терминатори.	• Мрежата со прстен бара повеќе кабел во однос на магистрала. • Прекин на кабелот може да предизвика испад на повеќе мрежи. • При додавање уред на прстенот, сите уреди се суспендираат од користење на мрежата • Не е вообичаена како магистралата, па не постои голем избор на опрема.

Топологија на ѕвезда (Star Topology)

Топологија на физичка ѕвезда се инсталира во облик на ѕвезда, и се состои од централна точка на поврзување, хаб каде што се поврзуваат сите кабелски сегменти (Слика 3.10). Секој уред во мрежата со ѕвезда е поврзан кон

централниот хаб со својот кабел. Иако поставувањето на оваа мрежа бара многу повеќе кабел од другите, топологијата на ѕвезда има повеќе предности над магистралата и прстенот.

Мрежите со ѕвезди и продолжени ѕвезди многу бргу станаа доминантна технологија кај повеќето мрежи. Една од предностите се состои во тоа што многу лесно можат да се прават измени и проширување на мрежата, без прекинување на другите корисници. Секогаш може да се додаде нов јазол или да се прошири мрежата без да се влијае врз нејзините перформанси.



Слика 3.10: Топологија на ѕвезда

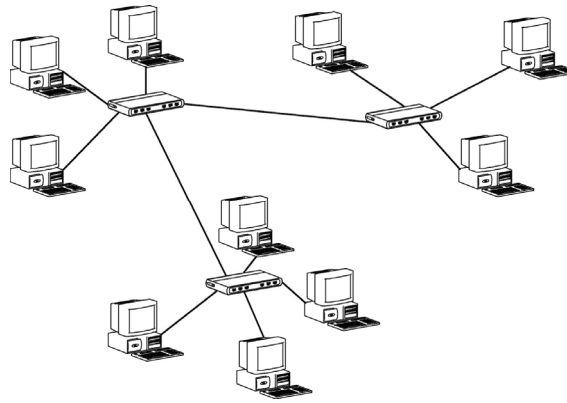
Предностите на топологијата на ѕвезда се:	Недостатоците на топологијата на ѕвезда се:
• Лесно се додаваат уреди при проширувањето на мрежата. • При испад на еден кабел нема испад на целата мрежа • Хабот овозможува централизирано управување. • Лесно се наоѓаат проблемите со уредите и каблите. • Ѕвездестата мрежа лесно се надградува на поголеми брзини. • Таа е најраспространета топологија и лесно се наоѓа опрема за неа.	• Ѕвездестата мрежа бара повеќе кабел од мрежите со магистрала и прстен. • Испадот на централниот хаб доведува до испад на целата мрежа. • Цената на инсталација и опремата се поголеми од повеќето мрежи со магистрала

Топологија на проширена ѕвезда (Extended Star Topology)

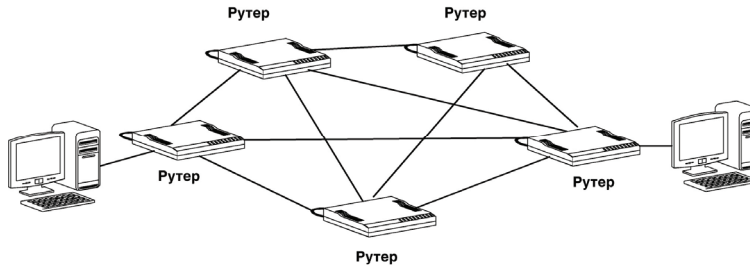
Ако мрежата со ѕвездеста топологија се прошири да вклучува и дополнителен хаб поврзан со главниот хаб (слика 3.11) се добива топологија наречена проширена ѕвезда.

Мрежеста топологија (Mesh Topology)

Физичката мрежеста топологија не е многу раширена во локалните мрежи, и обично се користи за WAN конекции при поврзување на локалните мрежи. Во оваа топологија, секој уред е поврзан се секој друг уред. Со ова се овозможува сите уреди да продолжат да комуницираат меѓусебно при испад на една конекција. На тој начин се добива безбедност во поврзувањето на мрежата, односно се добива толеранција на испади (fault tolerance).



Слика 3.11: Топологија на проширена ѕвезда



Слика 3.12: Мрежеста топологија

Предностите на мрежеста топологија се:	Недостатоците на мрежеста топологија се:
• Се добива толеранција на испад, ако дел од системот прекине со работа.	• Многу е скапа и тешко се поставува. • Тешко се управува со мрежата. • Тешко се откриваат и решаваат проблеми.

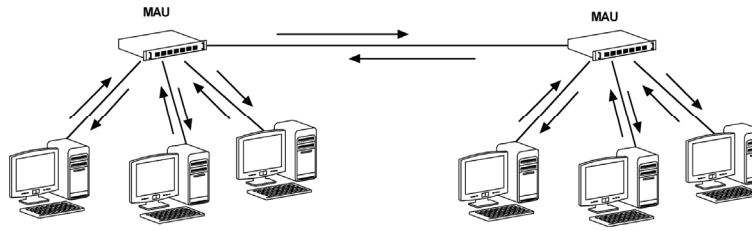
WAN (Wide Area Networks) ја користат мрежестата топологија за поврзување на локални мрежи, заради избегнување на системски испади.

Хибридни топологии (Hybrid Topologies)

Хибридната топологија комбинира две или повеќе различни физички топологии во една мрежа. Двата најпознати и најкористени хибриди на топологии се ѕвезда-магистрала и ѕвезда-прстен топологиите. Кога два хаба од различни топологии се поврзани така што уредите прикачени на нив можат меѓусебно да комуницираат (како на сликата 3.13) тоа се нарекува ѕвезда-магистрала мрежа.

Слика 3.13: Хибридна топологија

Кога две или повеќе топологии на ѕвезди се поврзани меѓусебно преку специјализиран хаб наречен MAU, се добива магистрала-прстен топологија.



Слика 3.14: Топологија прстен-магистрала

3.2.3 Видови на логички топологии

Логичките топологии ги опишуваат начините на кои уредите на локалните мрежи комуницираат и пренесуваат податоци, и постојат само две: магистрала и прстен.

Кога мрежата физички е поставена во магистрала, лесно може да се претпостави дека испраќањето на податоците се одвива по логичка магистрала, т.е. податоците се движат од уред до уред линеарно. Слично, физичката топологија на прстен лесно се интерпретира како логичка топологија на прстен. На сликата е дадена споредбата на патеките преку кои се пренесуваат податоците во мрежа со логичката магистрала и логички прстен.

Кога мрежата користи топологија на физичка ѕвезда, медиумот може да се пристапи и да се испратат податоците било како логичка магистрала или

како логички прстен, зависно од уредите за поврзување кои се користат во мрежата - како мрежните адаптери (NIC), хаб или MAU, и протоколите од второто ниво на OSI референтниот модел кои се имплементирани.

Логичка магистрала (Logical Bus)

Во модерните Ethernet мрежи, физичката поставеност на мрежата е во форма на топологија на ѕвезда. Во центарот на ѕвездата се наоѓа хаб преку кој всушност се дефинира логичката топологија. Ethernet хабот користи топологија на логичка магистрала за пренесување на податоците кон сите сегменти на својата ѕвезда.

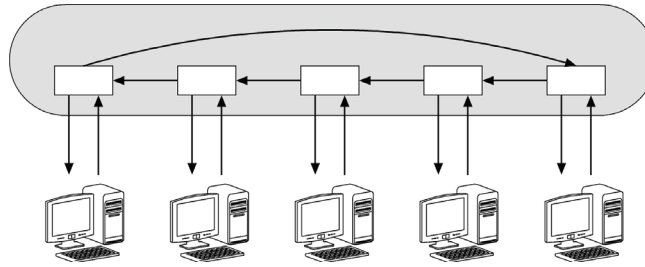
Предностите на логичка магистрала се:	Недостатоците на логичка магистрала се:
• Ако испадне еден јазол, не доведува до испад на целата мрежа. • Најраспространета логичка топологија. • Измени и проширување може да се прават без прекин и влијание врз другите корисници.	• Лесно се појавуваат колизии. • Само еден уред може да пристапува кон медиумот едновремено.

Логички прстен (Logical Ring)

Ако податоците на мрежата патуваат од еден уред до следниот и потоа пак се враќаат кон првиот уред, таквата логичка топологија одговара на прстен. Најпозната имплементација на логичкиот прстен е Token Ring мрежата, каде податоците се пренесуваат со користење на проследување на жетони. При проследувањето на токените, секој уред прима „празен“ токен кој поминува по прстенот. Ако токенот е празен, уредот може да го пополни со податоци и да го испрати по прстенот. FDDI е друга технологија кој исто така користи проследување на токени.

Уред за пристап на повеќе станици (Multistation Access Unit - MAU)

Централниот хаб во Token Ring мрежата е ожичен како физичка ѕвезда. Исто така е можно за мрежа со топологија на физичка ѕвезда, да пренесува податоци во логички прстен. Уредот наречен Multistation Access Unit (MAU) е централен уред од овој тип во Token Ring мрежата, и може да изгледа како обичен хаб, но како што може да се види од сликата 3.15, податоците во MAU се проследуваат од уред до уред со користење на логички прстен.

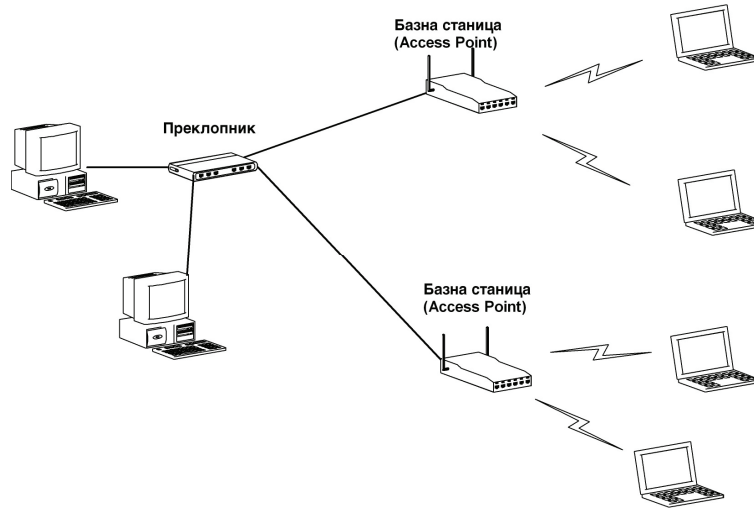


Слика 3.15: Логички прстен со користење на MAU

Предностите на логички прстен се:	Недостатоците на логички прстен се:
• Количеството на податоци кои можат да се пренесуваа во една порака е поголемо од логичка магистрала. • Не постојат колизии.	• Прекинат прстен значи прекин на сите трансмисии. • Уредот треба да чека за празен токен за да може врши пренос.

Безжични LAN топологии (Wireless LAN Topologies)

Безжичните мрежи не подлегнуваат на ограничувањата на традиционалните мрежи и нивните топологии. Бидејќи уредите што користат безжичен пренос емитуваат во сите правци, тие не се ограничени на традиционалните топологии како што се магистрала, ѕвезда или други. На сликата 1.10 (во Глава 1) се прикажани три јазли кои комуницираат на ad-hoc начин, со користење на безжични мрежни картички; ова уште се нарекува и peer-to-peer начин на комуникација.



Слика 3.16: Безжична LAN топологија

Безжичните LAN мрежи, WLAN, исто така може да бидат проширување на жичените LAN мрежи. Уредите комуницираат еден со друг и со ресурсите од жичената мрежа, со користење на „точка на пристап“ (access point - AP). Ова е наречено инфраструктурен начин. Пристапните точки може да бидат комбинирани за да се преклопуваат и обезбедуваат простирање на сигналот до било која точка. На сликата 3.16 е прикажан начинот како се проширува LAN мрежа во инфраструктурен начин со користење на две пристапни точки.

3.3 МРЕЖНИ АРХИТЕКТУРИ

Мрежна архитектура претставува спецификација за дизајнирање на физичкото поставување на поврзани уреди. Таа вклучува кој тип на кабел ќе се користи (или безжичен медиум), типот на мрежните интерфејси кои ќе се користат и механизмот преку кој ќе се врши пренос на податоците низ мрежата и уредите. Накратко, мрежната архитектура се однесува на целосниот дизајн и поставеноста на мрежата и начинот како компјутерите влијаат еден на друг.

Постојат три вида на мрежни архитектури кои се најпознати: еднаков-еднаков (peer-to-peer), клиент-сервер (client-server), и хибридна (hybrid). Видот на архитектурата соодветен на организацијата, зависи од неколку фактори, како што се географската локација, бројот на корисниците, потребни специјални апликации како и нивото на достапната техничка поддршка.

Во peer-to-peer мрежите, корисниците подеднакво ги делат нивните компјутерски ресурси, правејќи ги достапни на другите. Peer-to-peer мрежите се појавиле уште во 1984, кога Apple Computer го претставил својот Macintosh Plus, кој бил способен за умрежување со други Macintosh компјутери без користење на сервер. Microsoft исто така претставил оперативен систем кој имал способност за peer-to-peer умрежување во 1992 наречен Windows for Workgroups 3.11.

Најосновната peer-to-peer мрежа им овозможува на корисниците да делат меѓусебно ресурси, како што се папки со датотеки, печатари итн. Peer-to-peer умрежувањето му овозможува на корисникот пристап кон датотеки или печатари преку мрежа со што се намалуваат трошоците поврзани со користење на централизиран сервер или повеќе печатари.

Client-server мрежните архитектури ги централизираат ресурсите, податоците, и што е најважно апликациите на компјутери - сервери. Централизираната структура на клиент-сервер мрежите овозможува дополнителна предност во однос на сигурноста, затоа што е многу поедноставно да се обезбедат важните информации кога се наоѓаат на една локација. Покрај централизираните сервиси и безбедноста, клиент–сервер архитектурите даваат и подобрување на перформансите во однос на peer-to-peer мрежите. Кога многу корисници имаат потреба од пристап кон истиот компјутер или печатар, на peer-to-peer мрежата доаѓа до деградација на

перформансите. Клиент-сервер архитектурите го избегнуваат овој проблем преку комбинација на процесирачката моќ на работните станици со серверите, каде и двата компјутери симултано ги процесираат податоците. Оваа карактеристика ги подобрува перформансите и ефикасноста, особено за апликации како што се пребарувањето на бази на податоци.

Во големи организации каде што се имплементирани архитектури со клиент-сервер модел, може да биде тешко за мали кориснички групи ефикасно да работат. Хибридните мрежни архитектури дозволуваат и клиент-сервер и peer-to-peer мрежи да коегзистираат на истата мрежа. Помали групи на корисници може едноставно да ги делат своите ресурси без потреба за интервенција на мрежниот администратор.

3.3.1 Еднаков-еднаков мрежи (Peer-to-Peer Networks)

Peer-to-peer умрежувањето им овозможува на корисниците да ги делат ресурсите, датотеките и печатарите на децентрализиран начин; овие мрежи ги имаат следниве карактеристики:

- Тие дозволуваат на корисниците да делат ресурси на нивните работни станици.
- Соодветни се за групи од 10 корисници или помалку.
- Тие се децентрализирани, датотеките не се чуваат на централна локација.
- Овозможуваат лесна комуникација помеѓу компјутерите.

Peer-to-peer умрежувањето е обично интегриран дел од оперативниот систем на компјутерот. По конфигурацијата на софтверот на секоја станица, корисниците се одговорни за делењето на нивните податоци и управувањето на пристапот до нив.

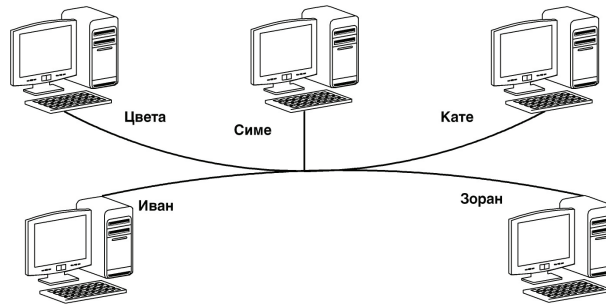
Кога корисниците учествуваат во истата „peer“ мрежа, припаѓаат во иста работна група (workgroup). На работната група и е доделено име, кое може да претставува корисници кои работат во одредена локација или кои работат на исти задачи, со што се олеснува паметењето на името и тоа е особено важно кога постојат повеќе работни групи на иста мрежа.

Избор на „Peer-to-Peer“ мрежи

Пред да се изврши изборот и имплементација на „peer-to-peer“ мрежа, потребно е да се направи евалуација на реалните потреби и важните фактори. Факторите може да бидат материјални потреби и можности како што се каблирањето и хардверските уреди, или пак корисничкото искуство за користење и управување со компјутерите и мрежата.

Основните критериуми до кои треба да се држиме при изборот на „peer-to-peer“ мрежа се:

- Помалку од 10 корисници кои ќе ги делат ресурсите.
- Не постои сервер.
- Не постои мрежен администратор.
- Мала и непостоечка потреба од безбедност.



Слика 3.17: Peer-to-peer мрежа

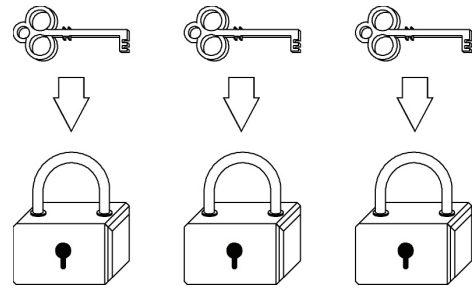
Предностите на „peer-to-peer“ мрежи се:	Недостатоците на „peer-to-peer“ мрежи се:
• Лесно се конфигурираат. • Не се бара дополнителен софтвер или хардвер. • Корисниците можат да управуваат со своите ресурси. • Не е потребен мрежен администратор. • Се намалуваат вкупните трошоците.	• Обезбедуваат ограничен број на конекции за делените ресурси. • Компјутерите со делените ресурси може да пројават деградација на перформансите. • Нема централизирано управување. • Нема централна локација за чување на датотеките. • Корисниците се одговорни за управување со ресурсите. • Мала или непостоечка безбедност.

Вкупните трошоци (total cost of ownership - TCO) е тешко да се пресметаат, и ги вклучуваат цената на опремата и софтверот, како и цената на чинење на управувањето со технологијата (времето потрошено за управувањето), како и скриени трошоци кои лесно се превидуваат.

Безбедност на „Peer-to-Peer“ мрежите

Peer-to-peer мрежите користат безбедност на ниво на делење („share-level security“). Ваквата безбедност им дава на корисниците-автори да доделуваат лозинки на локалните ресурси на своите компјутери. Со тоа се дозволува, корисник кој дели ресурс да имплементира безбедност преку поставување

или не на лозинка (password); во вториот случај секој преку мрежата може да пристапи на делените ресурси. Кај постарите оперативни системи, доделувањето на лозинката за заштита на одреден ресурс бараше таа да се додели на сите корисници кои имаат потреба да пристапуваат кон тој ресурс. Истата лозинка може да се додели на секој ресурс, но тоа не овозможува подобра заштита, туку може да се постави лозинка за секој оддел во организацијата како што е прикажано на сликата 3.18. Во peer-to-peer мрежите, доделување на единствена лозинка на секој ресурс ја максимизира заштитата, меѓутоа се отежнува управувањето со тие лозинки.



Слика 3.18: Поставување на одделни лозинки за секој ресурс во мрежата

Примена на Peer-to-Peer мрежите

Peer-to-peer мрежите се многу поедноставни за имплементација од другите мрежни архитектури, од таа причина тие се и поефективни во однос на цената. Примената ја наоѓаат во мали организации каде што корисниците имаат потреба за соработка и меѓусебна размена на податоци. За поставување на peer-to-peer мрежа покрај работните станици потребни се и:

- Мрежни интерфејс картички, или безжични картички за секој компјутер за поврзување на мрежата.
- Кабелски медиум за поврзување на компјутерите.
- Уред како што е хаб (hub) или преклопник (switch), преку чии портови се поврзуваат каблите до компјутерите.

(Или ако се поставува безжична мрежа - уред за точка на пристап Wireless Access Point (WAP), кој овозможува безжичните уреди да се поврзуваат преку пренесување на сигналите преку воздушниот простор).

3.3.2 Клиенти и сервери (Clients and Servers)

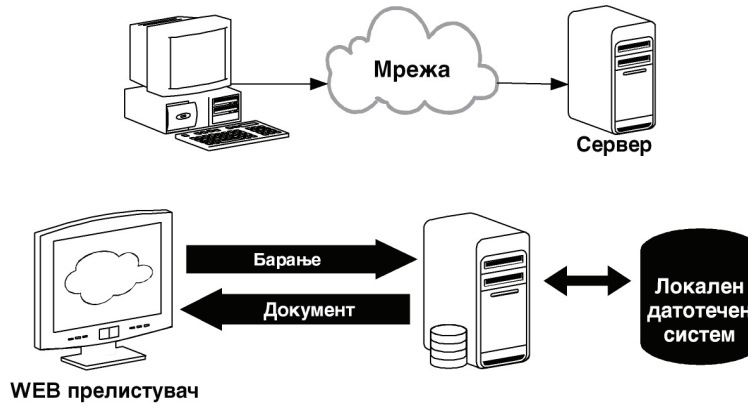
Клиент-сервер мрежната архитектура е централизиран модел за податочно складирање, безбедност, извршување на апликации и мрежна администрација; таа е најкористената мрежна архитектура која евалуирала со надраснувањето на „peer-to-peer„ мрежите за изнаоѓање на подобри

мрежни решенија. Клиент-сервер мрежите, исто така означени како серверски-базирани мрежи, ги имаат следниве карактеристики:

- Засновани се на скалабилен модел кој може да поддржи мали мрежи од 5 до 10 корисници, како и мрежи со илјадници корисници.
- Користат специјализирани компјутери – сервери кои обезбедуваат сервиси на клиентските станици.
- Даваат услуги како што се печатење, чување на датотеки и апликации.
- Овозможуваат повисоко ниво на безбедност, заснована врз дозволи на пристап (access permissions).
- Централно се управуваат од мрежниот администратор или тим на администратори.

Клинет-сервер моделот бара специјална хардверска и софтверска имплементација, при што го користи клиентскиот компјутер за дистрибуција на дел од работата помеѓу него и серверот. Еден начин е кога клиентот учествува со локално извршување на клиентска верзија на апликацијата. Тогаш серверот ја превзема задачата за зачувување на големиот дел од податоците и барањата за процесирање од повеќе клиенти.

Серверот најчесто е многу помоќен компјутер кој е способен да се справи со илјадници симултани барања. Како на пример, корисникот користи клиентска програма за E-mail која се извршува на компјутерот и бара нови електронски пораци од серверот. Серверот го процесира барањето и ако има нови e-mail пораци - ги праќа назад кон корисникот.



Слика 3.19: Пример за клиент-сервер модел

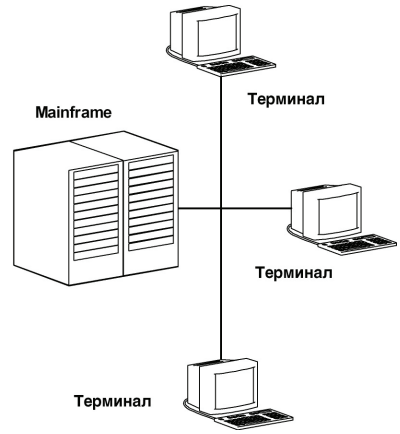
Видови на сервери (Common Server Types)

Со порастот и проширувањето на организацијата, се доведува до ситуација кога еден сервер не може да одговори на барањата. При појава на деградацијата на перформансите, обично се пристапува кон додавање на повеќе сервери со одредени улоги, каде секој од нив извршува различни апликации и одредени задачи. Постојат повеќе видови на сервери, во зависност од улогата што ја извршуваат:

- Сервери на датотеки (File servers). За разлика од делењето на датотеките во „peer“ мрежа, серверите на датотеки нудат услуга за користење на централна локација за чување на датотеките. Датотеките за обезбедени со тоа што за да се пристапи кон нив потребно е да се изврши автентификација на корисникот со помош на корисничко име и лозинка.
- Сервери на печатари (Print servers). Со растењето на мрежата, се зголемуваат и барањата на корисниците за печатење. Серверите на печатари помагаат при балансирањето на оптовареноста на печатењето, дозволувајќи им на корисниците да печатат симултано на серверот. Серверот ги чува сите задачи за печатење во редица за печатење (print queue) – привремен фолдер сè додека принтерот не стане достапен.
- Сервери за пораки (Messaging servers). Овие сервери одговараат на барањата за електронска пошта од клиентите или ги препратуваат пораките кон други соодветни сервери.
- Апликациски сервери (Application servers). Кога постои зголемено барање за користење на одредена апликација, со користење на апликациски сервер се подобруваат перформансите и безбедноста преку чување на апликацијата и податоците на истиот компјутер. Пример, многу WEB сајтови интегрираат два апликациски сервери, еден web сервер и еден сервер со базата на податоци.
- Сервери на WEB сајтови (Web servers). Уште познати и како HTTP сервери, WEB серверите даваат пристап до информации на корисниците до било кој компјутер кој има пристап на Интернет. Клиентскиот компјутер извршува апликација наречена прелистувач (browser) преку кој се побаруваат информациите од web серверот.
- Сервери за базите на податоци (Database servers): база на податоци е апликација која чува записи кои содржат информации. Големите бази на податоци се чуваат на сервери, така што клиентите можат да бараат од серверот да изврши процесирање, т.е. пребарување на базата или да генерира извештај.

Терминали и хостови (Terminals and Hosts)

Пред појавата на клиент-сервер моделот, постоеле терминали кои биле поврзани кон компјутер наречен хост. Хост компјутерот, уште наречен и „mainframe“, бил одговорен за целосната комуникација, складирањето и процесирањето. Мејнфрем компјутерот бил мозокот на сите терминали. Во овој модел терминалот (dummy terminal), ја извршувал апликацијата од мејнфрејмот, терминалите немале свој сопствен диск или друг начин на чување на податоци, туку само ги пренесувале командите од тастатурата кои се појавувале на терминалниот екран и ги испраќале кон мејнфрејмот. Целата работа за чување на податоците или извршување на апликациите се одвивало на компјутерот хост, односно мејнфрејмот.



Слика 3.20: Поврзување на mainframe со терминали

Како што се појавувала потреба од помоќни и поголеми системи, „terminal-host“ системот станал несоодветен, а истовремено развојот на технологијата дозволил користење на компјутери со можност за чување на податоци, извршување на апликации и процесирање на барања.

Избор на клиент-сервер мрежа

Основни критериуми за избор на клиент-сервер модел за мрежата се:

- Потребата од централно чување на датотеки.
- Безбедноста на чување на важни податоци.
- Корисниците имаат потреба од пристап кон исти апликации и податоци.
- Серверите ги одржува и управува мрежен администратор.
- Постојат повеќе од 10 корисници.

Предностите на клиент-сервер мрежи се:	Недостатоците на клиент-сервер мрежи се:
• Податоците се чуваат на централна локација и може лесно да се сочуваат (backed up). • Високо ниво на безбедност. • Можност за делење на можна хардверска опрема. • Хардверот и софтверот на серверите се оптимизирани за перформанса и сигурност. • Корисниците се ослободени од управувањето со ресурсите. • Управувањето со корисничките налози е централизирано.	• Планирањето, дизајнот и управувањето е комплицирано. • Управувањето со серверите бара соодветен кадар. • Серверскиот хардвер и софтвер се скапи.

Безбедност на клиент-сервер мрежите

Клиент-сервер мрежите имаат многу подобра сигурност во однос на „peer-to-peer“ мрежите. Иако самите работни станици се способни да обезбедат подобра локална сигурност, таа е неспоредлива со безбедноста што е достапна со користење на сервери. Прво, серверите ги централизираат ресурсите на мрежата така што единствен кориснички налог (user account) може подобро да се управува. Управувањето со корисничките налози и ресурсите кон кои корисниците имаат пристап, е одговорност на еден. Конечно, серверите нудат апликации за подобра за заштита како што се енкрипција и софистицирани системи за автентификација.

Примена на клиент-сервер модел

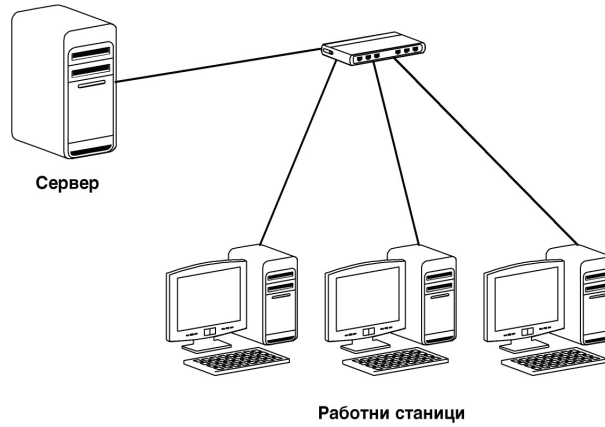
Имплементацијата на серверски-базирани мрежи не е едноставна како имплементацијата на „peer-to peer“ мрежите. Постојат многу начини за дизајнирање на серверски-базирани мрежи, а постојат и многу начини за конфигурација на хардверот и софтверот за серверите.

Изборот на вистинскиот приод зависи од големината на организацијата, потребите и цената на чинење, па серверски базираните мрежи може да се дизајнираат според следните три критериуми:

- Број на корисници
- Потреба од апликации
- Географска локација

Мрежи со еден сервер (Single-Server Networks)

Со надраснување на „peer-to-peer“ мрежата, обично се додава еден сервер и мрежата се трансформира во клиент-сервер мрежа. Мрежи со еден сервер обично се користат каде што има од 10 до 50 корисници, иако и помали организации може да користат повеќе од еден сервер. Дополнителен сервер се додава за апликации со специјална намена или за подобрување на доверливоста на мрежата; стратегијата со еден сервер е ризична заради можноста на губење на податоците при испад на серверот. Мрежи со еден сервер треба да се користат само ако се користат мал број на сервиси, пример за ваква мрежа е даден на сликата 3.21.



Слика 3.21: Локална мрежа со еден сервер

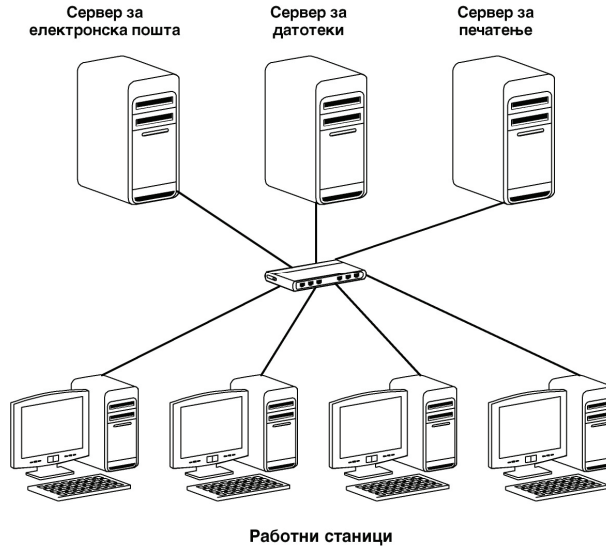
Мрежи со повеќе сервери (Multiserver Networks)

Бидејќи серверите можат да обезбедат различни функции, не е необично да се има повеќе сервери кои работат на иста мрежа и секој да дава различни услуги. Овој тип на мрежа се нарекува мрежа со повеќе сервери, и обично одговара на мрежа со 50 до 500 корисници. Раздвојувањето на сервисите преку повеќе сервери ги подобруваат перформансите и доверливоста на целата мрежа. Секој сервер може да биде оптимизиран за извршување на еден сервис - ако еден сервер падне другите сервери продолжуваат да работат нормално, дури и може да ја преземат улогата на паднатиот сервер.

Корпорациски мрежи (Enterprise Networks)

Како што се зголемува организацијата, така соодветно се зголемува и нејзината мрежа. Ваквите мрежи корисниците ги користат за да комуницираат подобро и да работат поефикасно, при што може да се соработува и со соработници кои се наоѓаат на локации надвор од компанијата ширум светот. Така се појавува потреба од мрежи кои се

способни за опслужување на илјадници корисници кои се наречени *enterprise networks*. Тие можат да бидат огромни - до илјадници корисници и можеби стотици сервери, секоја локација може да работи како мрежа со еден или повеќе сервери, а ќе биде поврзана со остатокот од корпоративната мрежа преку WAN конекции.



Слика 3.22: Локална мрежа со еден сервер со поделени улоги

Тука се појавува можност за развој на клиент-сервер апликации кои ги користат овие WAN линкови за поврзување на оддалечени сервери, со што се проширува клиент–сервер моделот преку повеќе локални мрежи и се вклучуваат повеќе сервери за исполнување на корисничките барања.

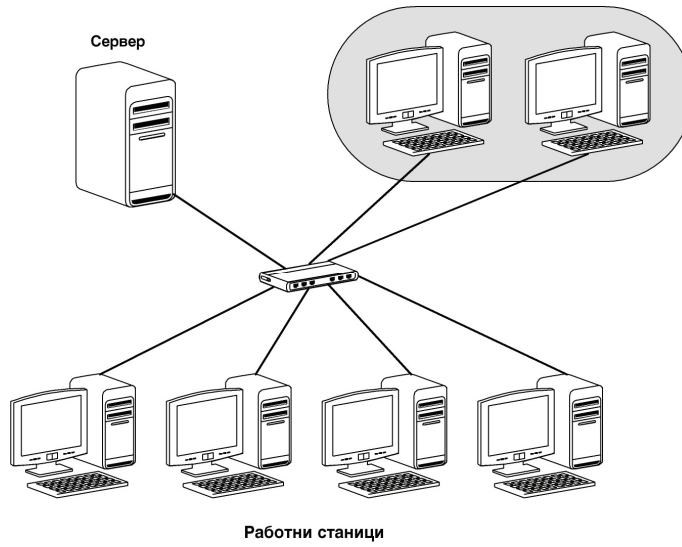
Хибридни мрежи (Hybrid Networks)

Хибридните мрежи ги инкорпорираат добрите карактеристики на работните групи од „peer-to-peer“ мрежите, со перформансите, безбедноста и доверливоста на серверско-базираните мрежи. Хибридните мрежи обезбедуваат централизирани сервиси на серверите, но исто така им дозволуваат на корисниците да делат и управуваат со своите ресурси во склоп на една работна група.

По логирањето на корисникот од една работна група на мрежата, корисникот нема потреба од други интеракции со серверот додека пристапува кон деленитe ресурси во својата група.

Во големите корпоративни мрежи, корисниците обично немаат можност да делат ресурси, заради поголема сигурност и заштита од илегални апликации и вируси, како и за поедноставување на поддршката на клиентските станици.

Предностите на хибридни мрежи се:	Недостатоците на хибридни мрежи се:
• Клиент-сервер апликациите се централно лоцирани и управувани. • Корисниците може да доделуваат локален пристап кон ресурсите на нивните компјутери. • Работните групи може да управуваат со ресурси без барање на помош од мрежниот администратор.	• Пристапот кон мрежата може да биде поголемо оптоварување за некои корисници. • Корисниците треба да паметат повеќе лозинки. • Датотеките може да бидат дуплицирани и промените да бидат препишувани помеѓу компјутерот со делен фолдер и серверот. • Датотеките снимани на работната станица не се зачувуваат (backed up).



Слика 3.23: Хибридна локална мрежа со еден сервер и работна група peer-to-peer корисници

4 МРЕЖНИ УРЕДИ

4.1 МРЕЖНИ МЕДИУМИ И КОНЕКТОРИ

Изборот на мрежен медиум е од суштинско значење за поставување и функционирање на мрежата, затоа што за разлика од другата компјутерска опрема која може и почесто да се менува, мрежниот медиум е долгорочна инвестиција која ќе се користи најмалку 10 до 15 години. Постојат повеќе видови на медиуми кои можат да се користат за пренос на сигналите, трансмисија на податоците и поврзување со другите мрежни уреди. Најкористените медиуми се изградени од бакар, стакло и воздух, и секој има сопствени карактеристики кои имаат влијание врз мрежните перформанси.

Поголемиот дел од постоечките мрежи користат некој облик на каблирање со бакар, и тоа од следниве видови: коаксијален кабел (coaxial), оклопена плетена парица (shielded twisted pair) и неоклопена плетена парица (unshielded twisted pair). За мрежи со поголеми брзини, повеќето организации се одлучуваат за користење на оптички влакна (fiber-optic), иако и бакарните кабли обезбедуваат високи брзини дури и во опсег на Gbps. Постојат мрежи кои воопшто и не користат кабли; безжичните мрежи го користат воздушниот простор за пренесување на податоци и се користат секаде каде што е невозможно физичко поставување на каблите. Тие исто така овозможуваат мобилно умрежување (mobile networking) и можност за лесно вршење на измени во физичката поставеност на крајните уреди.

Скоро иста важност како и при изборот на каблите, е и изборот на конекторите кои се поставуваат на каблите и се поврзуваат со уредите. Конекторите се користат за сите видови на медиуми вклучувајќи го и безжичниот. Видот на конекторот кој ќе се користи зависи од неколку фактори од кои најважни се видот на медиумот како и видот на мрежата.

Изборот на медиумот, како што е веќе напомнато, е најзначајна долготрајна инвестиција при креирањето на мрежата и треба многу внимателно земајќи ги во предвид сите фактори да се направи најсоодветна селекција. Изборот на медиумот ќе влијае и врз изборот на видот на мрежните адаптери (NIC) кои ќе се инсталираат на јазлите во мрежата, брзината на мрежата како и способноста на мрежата да во иднина одговори на потребите за надградба и проширување. Ако мрежниот медиум не може да ги поддржи брзините на пренос поголеми од тековните брзини на мрежните адаптери, на пример 100Mbps, тогаш во иднина мрежата не ќе може да одговори на потребите за пренос на податоци кои бараат поголем пропусен опсег (bandwidth-intensive). Иако оптичките влакна се сметаат за идеален мрежен медиум заради големиот потенцијал за пренос со голема брзина, тие имаат многу поголема цена за поставување и одржување. UTP кабелот со категорија 5 е способен да пренесува податоци со брзина од 1Gbps, и неговата цена е многукратно помала во однос на оптичките влакна.

Меѓутоа сè повеќе се појавува тренд за користење на оптички мрежни адаптери и оптиката се усвојува како мрежен медиум за да се овозможи поддршка на сè побрзите мрежни технологии кои ќе се појават во иднина.

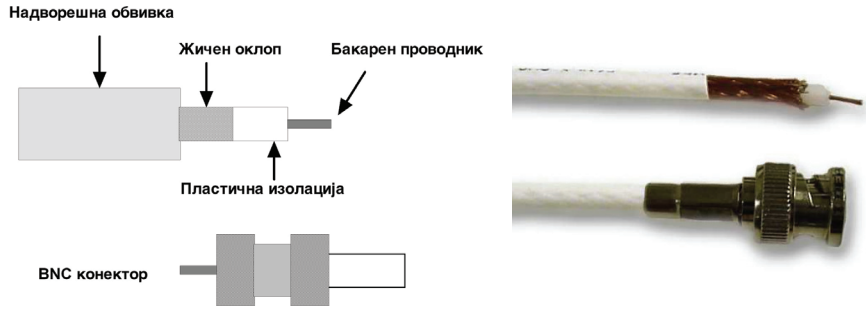
4.1.1 Бакарен медиум (Copper Media)

Бакарниот кабел е најстариот облик на мрежен медиум; се применувал во првите IBM мејнфрејм (mainframe) мрежи со користење на оклопени плетени парици. Постојат неколку типови на бакарен медиум кои овозможуваат различни брзини на пренос и опслужуваат различни видови на мрежи. Како што е веќе наведено, во бакарните медиуми спаѓаат: коаксијалниот кабел, оклопената и неоклопената плетена парица.

4.1.2 Коаксијален кабел (Coaxial Cable)

Коаксијалниот кабел е првиот вид на мрежен медиум, користен во Ethernet локални мрежи. Од ARCNET до Ethernet, многу различни видови на мрежи користеле некаков вид на коаксијален кабел, и сè уште постојат многу мрежи кои го користат.

Коаксијалниот кабел е направен од една централна бакарна жица која е прекриена со пластичен изолатор, наречен диелектрик, и оклопена заради заштита од интерференција со алуминиумска фолија или жица; надворешната обвивка е направена од пластика и тоа или од PVC или од plenum. Обвивката на пленум кабел е направена од тефлон и е отпорна на оган. Фолијата или жиците треба да бидат заземјени заради заштита од електромагнетна интерференција.



Слика 4.1: Коаксијален кабел

Видови на коаксијални кабли

Постојат повеќе видови на коаксијални кабли кои се користат како мрежни медиуми или за други намени, како што е пренос на кабелска телевизија. Секој тип на коаксијален кабел поседува одредени карактеристики кои

одговараат на потребите и начинот на пренос на податоците. Во табелата се прикажани најкористените видови на коаксијални кабли споредувајќи ги нивните отпорности (импеданси изразени во Оми), видот на мрежата каде што се употребуваат и некои основни својства. Многу видови на коаксијални кабли користат RG (radio grade) класификација со која се дефинира големината на централната бакарана жица и дијаметарот на надворешната обвивка.

Дебел и тенок коаксијален кабел (Thicknet and Thinnet)

Во умрежувањето каде што се користи коаксијален кабел, се користат два вида:

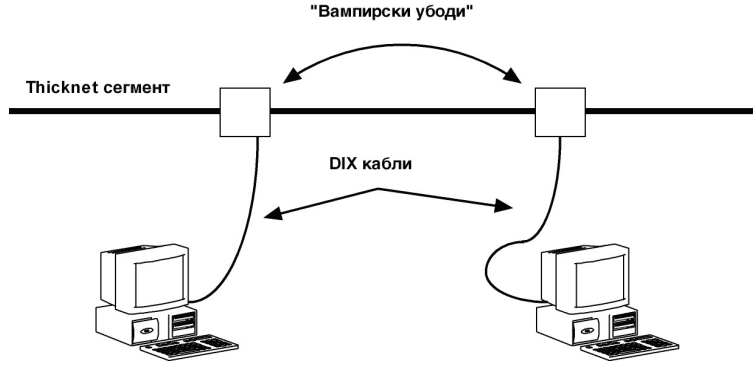
- Дебел коаксијален (Thicknet)
- Тенок коаксијален (Thinnet)

Дебелиот коаксијален кабел - Thicknet повеќе не се користи, но може да се најде во постарите инсталации и затоа е потребно да се познаваат и неговите карактеристики. „Thicknet“ е оригиналното каблирање кое е користено во Ethernet мрежите - кабелот се протегал низ ѕидовите и користел уред за поврзување – конектор наречен „вампирски убод“ (vampire tap) со кој се поврзувале уредите кон главниот кабел со користење на таканаречен drop cable.

Табела 4.1. Класификација и карактеристики на видови на коаксијални кабли

Класификација	Импеданса	Примена	Опис
RG-6	93 ohm	Кабелска телевизија	Сличен на RG-59, но со поголем дијаметар за поголем пропусен опсег за телевизиски пренос
RG-S	50 ohm	Дебел Ethernet (Thicknet)	Полно бакарно јадро со 1 мм во дијаметар, потребен е кабел (drop cable) за приклучување на адаптер на уред
RG-11	75 ohm	Кабелска телевизија	Обично има 4 слоја заштитни обвивки
RG-58/U	50 ohm	Тенок Ethernet (Thinnet)	Полно бакарно јадро со 0.5 мм дијаметар
RG-58 A/U	50 ohm	Тенок Ethernet (Thinnet)	Сличен на RG-58/U, но со плетено бакарно јадро
RG-5S C/U	50 ohm	Тенок Ethernet (Thinnet)	Сличен на RG A/U но се користи за воена намена
RG-59	75 ohm	ARCNET: кабелска TV	Дебело бакарно јадро со големо надворешно куќиште
RG-62	93 ohm	ARCNET; IBM mainframe-ови	Користен кај IBM 3270 системите за поврзување на терминали кон „mainframe“-ите

На сликата 4.2 е даден обичен „Thicknet“ кабел со вампирски убод и „drop“ кабел. „Thicknet“ уште се означува и со називот 10Base5, каде што 10 означува преносна брзина од 10Mbps на кабелот, а Base означува начин на пренос по основен опсег „baseband“. „Thicknet“ многу тешко се поставува и се работи со него, заради невообичаената цврстина на кабелот. Иако, сè уште постојат мрежи кои користат ваков медиум, не треба да се разгледува како избор на медиум за нови инсталации, постојат подобри и поефикасни алтернативи како што е на пример UTP кабел категорија 5. Тенкиот коаксијален кабел – „Thinnet“, уште познат и под ознаката 10Base2, е развиен по имплементацијата на „Thicknet“. „Thinnet“ има помал дијаметар и е многу полесен за експлоатација. Конекторите кои се користат за поврзување кај „Thinnet“, се познати како BNC конектори и можат да бидат цилиндрични (barrel) со кои се поврзува еден кабел со друг, или „T“ конектори со кои се поврзуваат уредите на еден кабел. Овие конектори треба да бидат цврсто поставени за да се обезбеди нивната конекција. Тие може да се користат за имплементација на топологија на магистрала каде што многу едноставно се додаваат нови јазли, но пронаоѓањето на проблемите е отежнато. Исто како и за дебелиот коаксијален кабел важи и за тенкиот - дека ако веќе нема постоечка инсталација, се препорачува да не се користи за поставување на нова мрежа.



Слика 4.2: Thicknet“ кабел со вампирски убод и „drop“ кабли

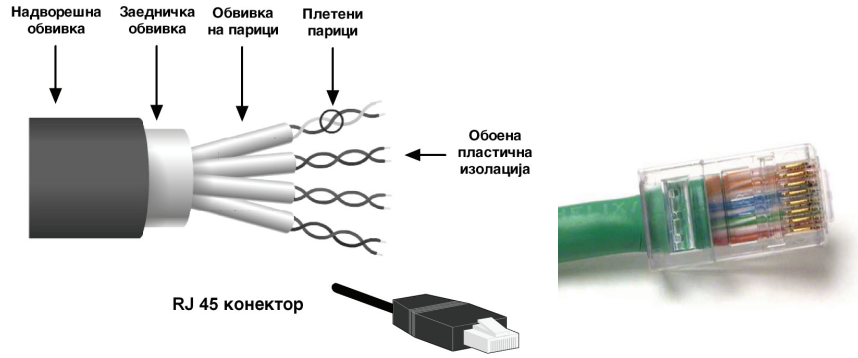
Предности при користење на „Thinnet“ коаксијален кабел се:	Недостатоците при користење на „Thinnet“ коаксијален кабел се:
• Лесен за инсталација. • Има помал дијаметар. • Неговиот оклоп ако е заземјен ја намалува електромагнетната интерференција (EMI) и радио фреквентна интерференција (RFI)	• ако се прекине кабелот, целата мрежа испаѓа. • кабелот треба да биде заземјен за одбегнување на интерференцијата. • поскап е во однос на неоклопена плетена парица UTP. • конекторите се поскапи во однос на другите • не поддржува пренос со поголема брзина.

Имплементација на коаксијален кабел

„Thinnet“ коаксијалните кабли многу ретко се инсталираат во нови мрежни инсталации, иако нудат едноставен начин за создавање на мрежа со мал број на корисници со користење на физичка топологија на магистрала. Постојат мрежни адаптери кои имаат приклучок за коаксијален кабел и приклучок за неоклопена плетена парица UTP, и кои овозможуваат замена на медиумот при проширувањето на мрежата и постепено исфрлање на коаксијалниот од употреба. А и поставувањето на BNC конекторот на кабелот е многу потешко од користењето на Category 5 UTP кабел и RJ-45 конектори.

4.1.3 Оклопена плетена парица (Shielded Twisted-Pair Cable)

Оклопена плетена парица - Shielded twisted pair (STP) е составена од пар на бакарни жици кои меѓусебно се преплетуваат. Париците се покриени со фолија или жичен оклоп, како и со надворешна PVC обвивка. Како и со коаксијалниот кабел, оклопувањето треба да биде заземјено заради превенција на фолијата или жичената заштита, да не станат магнет за електрицитет.



Слика 4.3: Изглед на оклопена плетена парица и RJ-45 конектор

Ознаките со бои за 150 ohm STP-A кабел, се црвена и зелена за парицата 1 и портокалова и црна за парицата 2.

Видови на оклопени плетени парици

Постојат 5 вида на STP кабли кои се користат во LAN мрежите, дефинирани од страна на IBM. Во табелата се дадени видовите на STP кабли, бројот на париците, дијаметарот на користениот бакар и нивна имплементација.

Иако се смета дека се помалку чувствителни на интерференција во однос на UTP, STP трпат појава на преслушување на краевите на кабелот, тоа се случува кога соседните жици интерферираат со сигнал кој се пренесува од други жици.

Предности при користење на STP кабли се:	Недостатоците при користење на STP кабли се:
• Оклопувањето ја намалува интерференцијата и преслушувањето • Може да се користи со RJ конектори наместо со IBM конекторите.	• Потребно е да се изврши заземјување. • поскапо е од користење на UTP кабел. • тешко се терминира.

Имплементации на STP

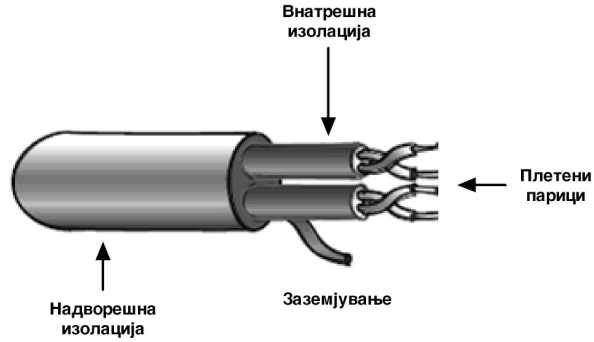
Иако STP се користи многу почесто, сè помалку се користи за примена во IBM Token Ring околината и постепено се врши негова замена во Category 5 UTP. Многу ретко се користи во Ethernet мрежите, заради цената и тешкотиите при изведување на терминацијата.

Табела 4.2. Видови на STP кабли

Вид	Број на парици	Дијаметарот на бакарот	Примена
Тип 1	2	22	Користен во IBM-овите Token Ring мрежи за главниот прстен или за поврзување на јазлите со MAU
Тип 2	4	22	Хибриден кабел за пренос на глас и податоци
Тип 6	2	26	Користен како адаптерски кабел за поврзување на јазлите со MAU во Token Ring мрежи, се користи за помали растојанија, може да се користи како „patch“ кабел
Тип 8	2	26	Користи плоснати жици и дизајниран е за спроведување под подови, за кратки растојанија
Тип 9	2	26	Се користи за поврзување помеѓу катови и згради, има полно или плетено јадро и „plenum“ обвивка

4.1.4 Неоклопена плетена парица (Unshielded Twisted Pair)

Неоклопена плетена парица - Unshielded twisted pair (UTP) е најчестата имплементација на бакарен медиум, се состои од плетени парови на обоени бакарни жици, но за разлика од STP - не содржи метална фолија или жичен оклоп како заштита од интерференции. Наместо тоа, паровите на жици имаат различен број на вплеткувања по единица мерка за произведување на придушување – укинување (cancellation). Придушувањето е многу важно во UTP каблирањето затоа што тоа е единствен начин за превенција на интерференцијата. На сликата е прикажан изгледот на UTP кабел:



Слика 4.4: Изглед на неоклопена плетена парица

Постојат повеќе вида на UTP кабли кои се идентификуваат според бројот на категоријата. Ознаката за категоријата се наоѓа на пластичната обвивка и на следнава слика се прикажани ознаките за категоријата на UTP кабел:

Слика 4.5: UTP кабли

UTP кабелот почесто се означува со кратенката „cat“ наместо категорија, Cat 5 означува кабел со ознака Category 5 UTP.

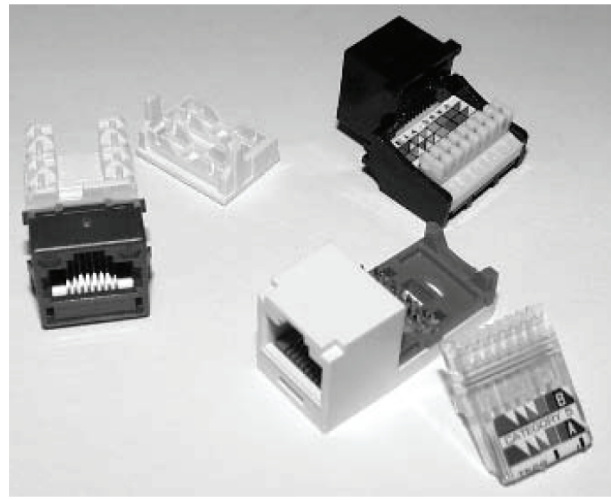
EIA/TIA Electronics Industries Alliance/ Telecommunications Industry Association.

Во јули 2002, EIA/TIA ја одобрила употребата на стандардот Category 6 наречен 568-B2.1. Овој стандард е дизајниран за поддршка на апликации кои користат брзини од повеќе од 1 Gbps. Претходно само видовите на UTP - Category 3, Category 4, Category 5e, и Category 5 биле специфицирани во EIA/TIA 568-A стандардот. Се смета дека Category 6 ќе стане нов стандард за инсталации на локални мрежи. Category 5e кабелот е најкористен вид на UTP во податочни мрежи; може да се користат и повеќе парици (во групи од 25) кои формираат таканаречен „Backbone UTP“ кабел.

Инсталација и терминација на UTP кабел

Кога се користи UTP кабел, потребно е да се разгледа кој вид на кабел и конектор ќе се користат. Цврстиот (Solid) UTP, кој се состои од цели непрекинати жици се користи за трајни инсталации, обично зазидани во канали. Овие трајни кабли се простираат (horizontal cross-connects), и се терминирани на едниот крај со панел за поврзување (patch panel) во ормар за ожичување, а на другиот крај обично со користење на RJ-45 приклучница (зидна). На сликата 4.6 се прикажани разни RJ-45 конектори од различни производители. Тие се разликуваат според стандардот (568-A или 568-B), иако некои вендори може да ги понудат и двете колор-шеми во еден приклучок.

UTP „stranded“ каблите се состојат од тенки жици (влакна) вплетени во секоја индивидуална жица. Овој вид на UTP е многу пофлексибилен од цврстиот (полниот) UTP. Се користи за „patch cords“ кабли со кои се приклучуваат уредите на RJ-45 зидните приклучници. Во ормарот за ожичување, „patch“ кабелот се користи за поврзување на панелот за поврзување со хабот или преклопникот. Овие печ корд кабли се терминирани со користење на RJ-45 конектори (слични на телефонски конектори R-11 само разликата е во големината).



Слика 4.6: RJ-45 конектори

Категории на UTP кабли

На следнава табела се прикажани категориите на UTP каблите, бројот на паричите, оценката за користење и начинот како се имплементирани:

Табела 4.3. Категории на UTP кабли и нивни карактеристики

Тип	Број на парици	Брзина на пренос	Примена
Категорија 1	2	Пренос на глас	Се користи во телефонска индустрија, не е погоден за пренос на податоци (иако може да се користи за кратки растојанија)
Категорија 2	2	4 Mbps	Може да се користи за податочни комуникации, но ретко се инсталира
Категорија 3	4	10 Mbps	Се користи за 10Base-T мрежи и за гласовна комуникација
Категорија 4	4	16Mbps	Во IBM Token Ring мрежи
Категорија 5	4	100 Mbps и поголеми	Во Ethernet 100BaseX мрежи
Категорија 5e	4	100 Mbps и поголеми	Во Ethernet и 100-1000 Base-X мрежи
Категорија 6	4	100 Mbps и поголеми	Во Ethernet и 1000Base-X мрежи

Имплементација на UTP

UTP каблирањето е поставено на повеќе од 80% од постоечките LAN мрежи. Каблирањето со оптички влакна се користи како „backbone“ кабел помеѓу мрежните сегменти, а UTP се инсталира како медиум за поврзување на десктоп компјутерите и другите уреди. Моментно, специјална категорија на кабли на Category 5 UTP, подобрена - Enhanced Cat 5 или Cat 5e, можат да поддржат брзини од 350Mbps, што е 35 пати поголема брзина отколку што се користела пред 5 години; стандардната спецификација за Category 5 UTP е 100Mbps. При планирањето на мрежата, потребно е да се земе во предвид дека поставената инсталација треба да трае минимум 10-15 години, односно неколку пати повеќе од другите мрежни компоненти.

Предности при користење на Category 5 UTP кабли се:	Недостатоците при користење на Category 5 UTP кабли се:
• евтина инсталација. • лесна терминација. • нашироко користен. • поддржува повеќе типа на мрежи.	• чувствителност на интерференции. • лесно може да се оштети при инсталацијата. • грешки заради ограничувањата во должината при инсталацијата.

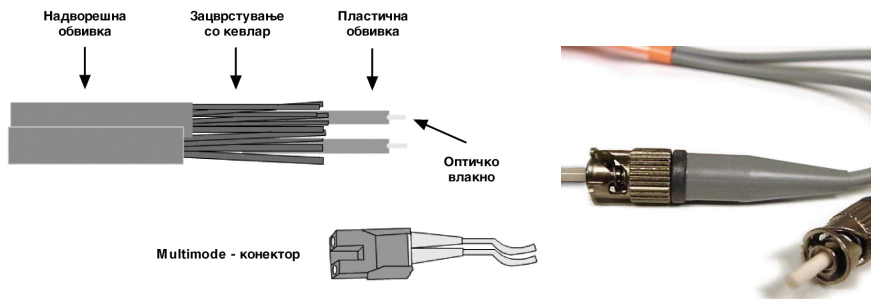
4.1.5 Оптички влакна (Fiber-Optic Media)

Оптичките влакна нудат повеќе предности во однос на бакарните медиуми и само неколку недостатоци. Иако повеќето постоечки мрежи користат оптички кабел за „backbone“ медиум, сè повеќе се користи оптиката и за поврзување на десктоп станиците со локалните мрежи. Оптичките влакна или кабли користат стакло за јадрото на кабелот, иако се користи и високо квалитетна пластика која не е прифатена според стандардот EIA/TIA 568-A. Користењето на оптичкиот медиум во мрежата овозможува избегнување на EMI и RFI, кои би ги оштетиле податочните сигнали. Оптиката е исто така отпорна на ефектите на молњи и пренапон кои можат да се појават по бакарниот медиум, што можат да предизвикаат оштетување или уништување на мрежните уреди. Оптиката како најбитна карактеристика овозможува поширок пропусен опсег (bandwidth) на поголеми растојанија, без користење на репетитор. За разлика од бакарниот медиум, оптиката ги пренесува сигналите преку светлина, изворот на светлината може да биде ласер или светечка диода (lightemitting diode LED). Иако ласерот се смета како подобар избор за оптичките мрежи, LED изворите се почести, поевтини, а нудат и поголем работен век и се посигурни во работата.

Оптички кабел

Оптичкиот кабел (Fiber-optic cable) се состои од централно јадро од силикон, стакло или пластика. Тоа е создадено за пренесување на одредени видови на светлински бранови преку големи растојанија со многу мала загуба на сигналот. Централното јадро на мултимоден светловод има дијаметар од 125 микрони (125μ), и има големи како отприлика 2 човечки влакна.

На сликата е прикажан пресекот на мултимоден оптички кабел. Околу централното јадро се наоѓа „cladding“, што е рефлексивен материјал кој помага за прекршување на светлината како што поминува низ кабелот. За пополнување и зацврстување на кабелот се користи кевлар кој е многу цврст и отпорен на оштетувања. Оптичките кабли може да се најдат како единични или парови до 36 влакна; за воспоставување на целосна двонасочна врска потребни се 2 влакна („full-duplex“).



Слика 4.7: Изглед на оптички кабел со ST конектор

Оптичките влакна се произведуваат во различни големини кои може да се идентификуваат преку големината на централното јадро. Најкористената големина изнесува 62.5/125 микрони, и тоа е типична големина за мултимоден оптички кабел (multimode). Едномодниот оптички кабел (Single-mode) се користи за поголеми растојанија и има јадро со големина од 8/125 микрони. Овој тип на оптика може да се користи на далечини до 3 километри, без користење на репетитор. Исто така може да се користи и во повеќе изведби на локални мрежи и апликации, вклучувајќи ги Ethernet, 10Base-F, FDDI, оптички Token Ring (Token Ring), и некои ATM архитектури.

Во следнава табела се дадени карактеристики на „single-mode“ и „multimode“ оптичките кабли:

Табела 4.4. видови на оптички кабли

Вид на кабел	Големина на јадро	Примена / карактеристики
Single-mode оптика	8/125 микрони	Каде што има потреба од голем пропусен опсег; поддржува една трансмисија едновремено
Multimode оптика	62.5/125 микрони	Најкористениот оптички кабел, дозволува повеќе трансмисии истовремено

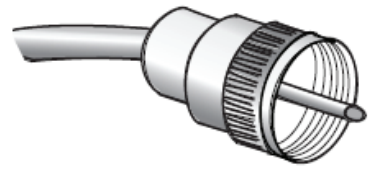
4.1.6 Оптички конектори (Fiber-Optic Connectors)

Оптичките кабли може да бидат инсталирани со различни типови на конектори:

- SMA (SMA 905/SMA 906)
- ST (straight tip)
- SC (subscriber connector)

SMA конектори

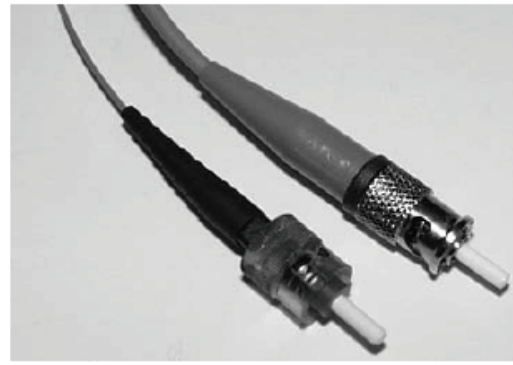
SMA е конектор за оптички кабли кој има навој, како што е прикажано на сликата, и постојат два различни типа. Типот 905 има „straight“ конектор, а типот 906 има конектор кој е помал на крајот; два конектори може да се спојат со користење на каплер. SMA конекторот има ограничена употреба во новите инсталации, заради тешкотиите за спарување на два конектори и креирање на двоен оптички интерфејс.



Слика 4.8: Изглед на SMA конектор

ST конектори

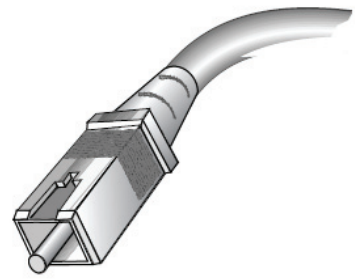
ST конекторите користат начин на поврзување кој е сличен на BNC конекторот. По вметнувањето на конекторот, се завртува на едната страна и се прицврстува. ST е едноставен и лесно се поставува и заради тоа е популарен, но исто така потешко се спарува за дуал-оптички инсталации. На следната слика се прикажани пар на ST конектори.



Слика 4.9: Изглед на ST конектори

SC конектори

Третиот и најкористен конектор е SC конекторот, кој за разлика од SMA или ST конекторите, многу полесно може да се распознае заради правоаголниот облик. SC конекторот е едноставен за инсталација и обично се спарува во „duplex“ кабли. Спарениот сет може да содржи механизам за заклучување кој оневозможува погрешна инсталација, (еден од конекторите има различен облик и при приклучувањето не може да дојде до вкрстување на каблите). На сликата е прикажан SC конектор прифатен од EIA/TIA 568-A стандардот како препорачан конектор за електрични инсталации, кој уште се нарекува 568-SC.



Слика 4.10: Изглед на SC конектор

Предности при користење на оптички кабли се:	Недостатоците при користење на оптички кабли се:
• Може да се инсталираат на поголеми раздалечини. • Нудат поголеми брзини на пренос. • Не се чувствителни на EMI или RFI. • Не може да се прислушуваат, имаат подобра сигурност.	• Најскап медиум за поставување и одржување. • Строги правила при поставувањето на каблите.

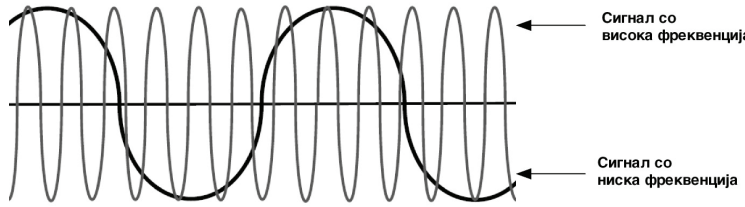
Оптичките кабли кои се користат надвор, треба да бидат специјално дизајнирани и да имаат соодветна заштита и потпора. Треба да се нагласи дека SC конекторите се најкористени во денешните оптички Ethernet мрежи. Терминацијата на оптичките кабли бара специјализирана обука иако целиот процес прилично се упростува со користење на нови техники и специјализирани алати и материјали.

4.1.7 Опции за безжично умрежување (Wireless Networking Options)

Безжичните комуникации покрај пренесувањето на радио и телевизија, се користат и за пренесување на податоци; на овој начин се решава проблемот на континуирана комуникација. Безжичните локални мрежи (Wireless Local Area Networks - WLAN) сè повеќе ги заменуваат традиционалните жичени конекции на секој јазол.

Со користење на високофреквентни сигнали, безжичната трансмисија може да покрие поголеми оддалеченост - тие го делат воздушниот простор на начин како што се шират радио и телевизиските сигнали. Секој сигнал користи различна фреквенција прикажана со херци (hertz), или циклуси во секунда време, и така се разликуваат еден од друг. На сликата е прикажано како сигналите на различни фреквенции создаваат комплетно различни

облици на сигнали и можат да бидат препознаени од уреди подесени на тие фреквенции.



Слика 4.11: Сигнали со висока и ниска фреквенција

Стандардите за безжичен пренос на податоци се опишани во IEEE 802.11, кој е усвоен во 1997. Постојат повеќе стандарди за 802.11, како што се 802.11a, 802.11b, и 802.11g. Денес, безжичните комуникации постојат во локални LAN, метрополитен MAN и WAN мрежи. Заради простирањето на сигнали кое се извршува преку атмосферскиот простор, ова е соодветен медиум каде што жичното каблирање од било која причина не е можно. Во зависниот од имплементацијата, изборот на безжичната технологија може да се разликува. Постојат три основни вида на безжични технологии:

- Радио бранови, кои се емитираат од 10KHz до 1GHz
- Микробранови, кои се емитираат од 1GHz до 500GHz
- Инфрацрвени, кои се емитираат од 500GHz до 1THz

Радио трансмисии (Radio Transmissions)

Радиобрановите се користат за пренесување и примање на податоци на сличен начин како и со користење на обичен радио уред: се подесува фреквенцијата на станицата од која се очекува пренос на податоци, истото важи и за спротивната страна - предавателот. Радио преносот кој се користи во умрежувањето користи повисоки фреквенции. Безжичните локални мрежи користат радио-бранови за примо-предавање на податоците и постојат повеќе видови на радио-трансмисии користени во мрежите:

- теснопојасни (Narrow-band)
- со голема моќност (High-powered)
- Frequency-hopping spread spectrum
- Direct-sequence-modulation spread spectrum

Теснопојасен радио-пренос (Narrow-Band Radio Transmissions)

Едно-фреквентен радио-пренос се користи во безжичните локални мрежи. Теснопојасниот пренос не е регулиран од страна на локалната комисија за

комуникации (Federal Communications Commission FCC) и работи на следниве фреквенции: 902–928MHz, 2.4GHz, и 5.72– 5.85GHz. Теснопојасните радио комуникации се ограничени на 70 метри. Овој вид на комуникации е екстремно чувствителен на интерференции и може да биде прифатен и ослушнуван од секој приемник подесен на таа фреквенција, со што се појавува безбедносен проблем при преносот на податоците.

Радио-пренос со голема моќност (High-Powered Radio Transmissions)

Друг еднофреквентен радио-пренос, користен во безжичните комуникации на локалните мрежи, е радио-преносот со голема моќност, кој има ограничување на оптичка видливост (line-of-sight). Ограничувањето на оптичка видливост е кога антените на приемникот и предавателот се насочени една наспроти друга. Овој начин на пренос е многу посигурен од теснопојасниот радио-пренос, но е поскап за имплементација. Обично овој вид на пренос треба да има официјална дозвола од страна на FCC. Обично ваков сервис користат поголемите телекомуникациските компании, а најголеми придобивки имаат мобилните корисници. Кога ќе се најдат вон опсегот на радио-сигналот, потребно е да се користат репетитори за зголемување на преносното растојание.

Радио-пренос со „раширен спектар“ (Spread-Spectrum Radio Transmissions)

За разлика од претходно споменатите еднофреквентни преноси, радио-преносот со проширен спектар користи повеќе фреквенции истовремено.

Овој вид на комуникација може да се подели во три категории, во зависност како ги користат фреквенциите. Првата категорија користи „прескокнување на фреквенции“ (frequency hopping - FH, FHSS). FHSS го префрла преносот на податоците помеѓу различни фреквенции во одредени временски моменти. Уредите кои користат ваква мрежат треба да бидат синхронизирани и треба да комуницираат меѓусебно за избор на следната фреквенција што ќе се користи. Брзината на ваквиот пренос е релативно бавна, помалку од 2Mbps.

Втората категорија се нарекува „модулација со директна секвенца“ (direct-sequence modulation –DS, DSSS). Се користат повеќе фреквенции за истовремено пренесување на податоците. Податоците се делат на сегменти наречени „чипови“ (chips). Способноста за пренос на повеќе фреквенции резултира со побрз пренос и се постигнуваат брзини од 2Mbps до 6Mbps. Уредите на мрежата која користи ваков тип на пренос, ги реасемблираат добиените делови во податочен сегмент.

Третата категорија на пренос со проширен спектар е мултиплексирање со ортогонални фреквенции (orthogonal frequency division multiplexing - OFDM). OFDM го дели преносниот канал во подканали кои се пренесуваат

симултано по различни фреквенции до приемникот. OFDM е избран како основа на стандардот 802.11g, и овозможува брзина на пренос до 54Mbps; 802.11b, кој не го користи OFDM има брзина на пренос од само 11Mbps. Во следнава табела се прикажани фреквентните опсези, преносните растојанија и брзините за безжичен пренос:

Табела 4.5. Видови на сигнали за безжичен пренос

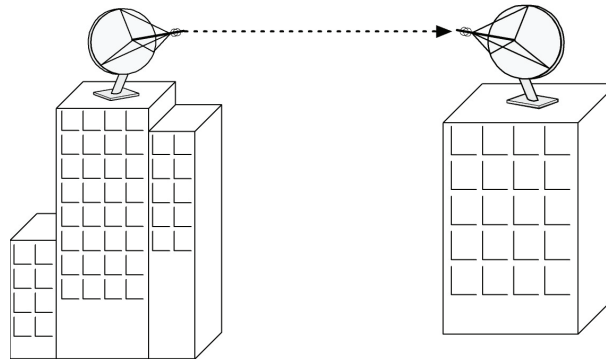
Вид на сигналот	Фреквентен опсег	Најголем досег	Ранг на брзини
Една фреквенција Теснопојасен опсег (Narrow-Band Single Frequency)	902-928 MHz 2.4 GHz 5.72-5.85 GHz	50-70 метри	1-10 Mbps
Една фреквенција со голема моќност (High-Powered Single Frequency)	902-928 MHz 2. 4 GHz 5.72-5.85 GHz	Оптичка видливост	1-10 Mbps
FHSS (Frequency-Hopping Spread Spectrum)	902-928 MHz 2. 4 GHz	Може да биде неколку километри зависно од ограничувањето на ќелијата	1-2 Mbps
DSSS (Direct-Sequence-spread spectrum)	902-928 MHz 2. 4 GHz	Може да биде неколку километри зависно од ограничувањето на ќелијата	2-6 Mbps
OFDM SS (Orthogonal frequency division multiplexing spread spectrum)	5.15-5.25 GHz 5.25-5.35 GHz 5.725-5.825 GHz	Неколку километри	до 54 Mbps

Микробранов пренос (Microwave Transmissions)

Микробрановите системи кои пренесуваат со одредена брзина на фреквенции помеѓу 1*GHz* и 1THz, потребно е да имаат дозвола од FCC. Постојат два вида на микробранови преноси, кои обично се користат во MAN и WAN мрежите: земјени и сателитски. (Постојат и локални мрежи кои користат микробранов пренос, но се многу ретки). Микробрановите системи може да покријат многу поголеми растојанија од радио-трансмисијата; радиото е ограничено на неколку километри, додека микробрановата трансмисија преку сателит постигнува глобални растојанија. Сите микробранови преноси се чувствителни на временски услови, како што се молњи.

Земјен микробранов пренос (Terrestrial Microwave)

Земјениот микробранов пренос се користи за пренос на податоци помеѓу две антени кои имаат меѓусебна оптичка видливост. Овие антени имаат облик на чинија, како што е прикажано на сликата. Преносот се врши на многу повисоки фреквенции од радио преносот 4–6GHz и 21–23GHz, и потребна е лиценца од FCC за емисија во овој фреквентен опсег. Земјена микробранова комуникација може да се одвива на растојанија од 1 до 80 км, ако постои оптичка видливост.



Слика 4.12: Терестријална микробранова комуникација со насочени антени

Сателитски микробранов пренос (Satellite Microwave)

Сателитскиот микробранов пренос користи сателити поставени во геостационарна орбита за пренесување на податоците до одредиштето. Користењето на сателитите дозволува преносот да покрие долги - скоро неограничени растојанија. Како што може и да се претпостави, цената на лансирање на сателит за проширување на мрежата е екстремно скапо, и повеќето имплементации на сателитска микробранова мрежа го наплаќаат преносот на податоци на одредена компанија врз база на временска единица (екстремно скапо).

Брзината преку која се комуницира со сателитот се движи помеѓу 1Mbps и 10Mbps, и се појавува и доцнење како резултат на големите растојанија преку кои поминува сигналот. Сателитите користат уреди наречени транспондери (transponders) за пренос кон станиците и иако областа кон која се пренесува е огромна, (дури и повеќе од 10000 км во ширина), сепак треба да се воспостави оптичка видливост со станиците на земјата.

Инфрацрвен пренос (Infrared Transmissions)

Иако инфрацрвените сигнали често се користат за далечинско управување со уреди, тие не се соодветни и практични за мрежна околина. Инфрацрвениот пренос може да се врши само еднонасочно и едновремено. Комуникацијата која се појавува во една насока може да се одвива со брзина до 16Mbps, но

ако се одвива во двете насоки - само до 1Mbps. Ограничувањето на растојанието за пренос изнесува 30 метри.

Табела 4.6. Споредбен приказ на мрежните медиуми

Вид на медиумот	Максимален сегмент	Пропусен опсег	Предности	Недостатоци
„Thicknet“„ коаксијален кабел	500 метри	10 Mbps	Помалку чувствителен на EMI од другите бакарни медиуми	Тежок за работа, скап
„Thinnet“ коаксијален кабел	185 метри	10 Mbps	Поевтин од „Thicknet“ или оптика, едноставен за инсталација	Ограничена брзина и примена, оштетувањето на кабелот доведува до прекин на мрежата
STP	100 метри	10 Mbps	Намалено преслушување, поотпорен на EMI од „Thinnet“ или UTP	Тежок за работа, поскап од UTP
Cat 3 UTP	100 метри	10 Mbps	Најевтин од сите медиуми	Ограничена брзина, примарно користен за гласовни апликации, слаб квалитет на сигналот
Cat 5 UTP	100 метри	100 Mbps	Малку поскап од Cat 3 UTP, но многу подобри перформанси, едноставен за инсталација, широко достапен и применуван	Чувствителен на интерференција, покрива само мали растојанија
Enhanced Cat 5 UTP	100 метри	1000 Mbps	Поголема брзина и отпорен на прислушување	Поскап од Cat 5; потежок за инсталација и бара уреди со иста брзина за поврзување
Single-mode оптика	3 километри	100 Mbps-100 Gbps	Поголема брзина во однос на бакарните медиуми, не може да се прислушува, нечувствителен на EMI	Скап, тежок за манипулација и терминација, поддржува само единичен пренос
Mulrimode оптика	2 километри	100 Mbps-9.92 Gbps	Поддржува повеќе преноси истовремено, не може да се прислушува, подобра безбедност, големи растојанија, нечувствителен на EMI	Скап, тежок за манипулација и терминација
Радио со една фреквенција (Single-frequency)	50-70 метри Оптичка видливост	1-10 Mbps	Не бара инсталација на медиум	Покрива само ограничено растојание
Spread-spectrum радио	До неколку километри	1-54 Mbps	Не бара инсталација на медиум	Може да биде скап
Земјени микробранов Пренос	1-70 километри	1-10 Mbps	Не бара инсталација на медиум, може да се користи за поврзување на оддалечени точки	Помалку скап од оптиката, чувствителен на атмосферски влијанија
Сателитски микробранов пренос	Глобално	1-10 Mbps	Не бара инсталација на медиум, се користи за глобално поврзување	Екстремо скап, чувствителен на атмосферски влијанија

Овој вид на пренос е истовремено многу чувствителен на интерференции од светлосни извори, како што се сонцето и флуоресцентното осветлување. Инфрацрвениот пренос користи фреквенции кои се нешто пониски од видливата светлина. FCC дозволува инфрацрвен пренос во опсег на терахерци, (1000 пати побрзо од GHz).

4.2 МРЕЖНИ УРЕДИ

Мрежните уреди имаат основна улога за поврзување и комуникација која се одвива на мрежата. Додека некои од уредите се специфични само за локалните мрежи, другите може да функционираат и кај LAN и кај WAN. Со развојот на технологијата, сè повеќе уреди обезбедуваат сервиси за повеќе нивоа на OSI референтниот модел. Во ова поглавје се прикажани видовите на уреди преку кои може да се изврши поврзување и проширување на мрежата.

4.2.1 Проширување на мрежата

При поставување на едноставна мрежа, таа може да содржи неколку компјутери и други ресурси како што се сервер за печатари и датотеки. Како што нараснуваат потребите, така се проширува и мрежата со додавање на дополнителни уреди како што се репетитори (repeaters) и мостови (bridges), кои се користат за поврзување на локалната мрежа со други ресурси. Безжичните уреди, како што се точки на пристап и безжични мостови (wireless bridges), овозможуваат мрежата да се проширува без поставување на жици. На крајот во мрежата може да се додаде и рутер (router) со кој се овозможува комуникација во состав на приватна WAN мрежа; тој исто служи и за поврзување кон Интернет.

4.2.2 Мрежни сегменти

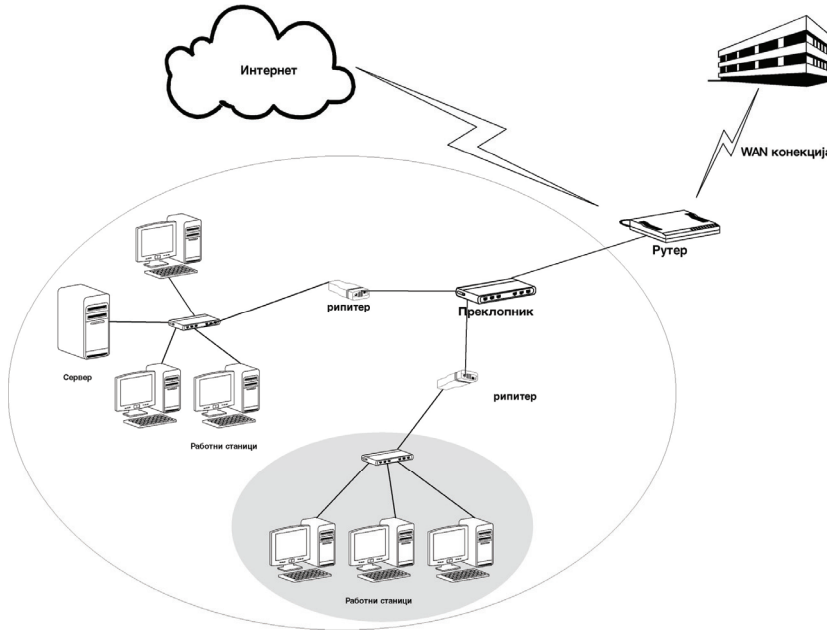
Поимот сегмент се користи во терминологијата за мрежи и за опишување на кабел користен за поврзување на два уреди, но поимот „мрежен сегмент“ се користи во поопшта конотација - кога се означува одредена област од локалната мрежа.

При додавање уреди на мрежата, со зголемување на растојанијата кои може да ги покрие мрежата, може да се дојде до нарушување на перформансите на мрежата. Еден од недостатоците од проширувањето на мрежата со поставување на повеќе уреди, се состои од тоа што со зголемувањето на бројот на уреди - се зголемува и мрежниот сообраќај. Овој проблем може да се надмине со одредени уреди кои вршат филтрирање на сообраќајот. Тие ги намалуваат натрупувањата со пропуштање на неопходните информации на мрежата.

Една поголема мрежа со повеќе уреди на неа, може да се подели на повеќе мрежни сегменти, со што се помага при контрола на натрупувањето на

сообраќајот и се подобруваат перформансите на мрежата. Секој уред може да комуницира со секој, но само кога има потреба за тоа.

Поголемиот дел од мрежниот сообраќај останува на локално на мрежниот сегмент. Големината на мрежниот сегмент се одредува во зависност од два фактори: домени на емисии (broadcast domains) и домени на колизии (collision domains).



Слика 4.13: Широка мрежа

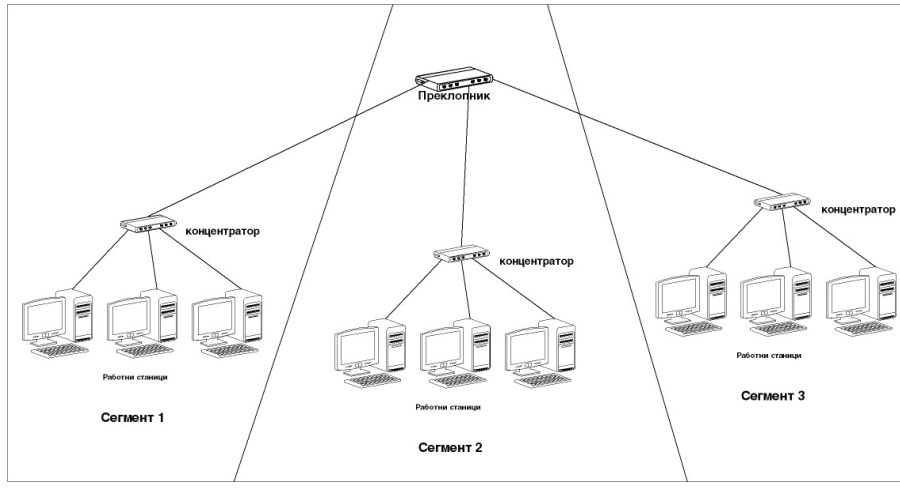
Емисија (broadcast) е сигнал кој се испраќа од еден уред и се прима и отчитува од сите други уреди поврзани на истата мрежа. Кај сите видови на мрежи, емисионите пораки (broadcast messages) може да се користат за наоѓање на имињата на компјутерите на мрежата или за испраќање на пораки на целата мрежа. Проблемот со емисиите е што можат непотребно да трошат од мрежниот преносен опсег и тоа станува сè поизразено како што се додаваат нови уреди на мрежата. Проблемот постои и кога уредите не ја користат мрежата, емисионите пораки се емитуваат во регуларни временски интервали.

Домен на емисии (broadcast domain) е дефиниран од границите во кои се одвива емисијата. На пример, ако емисионата порака е испратена по кабелот и застанува кога ќе достигне уред, пораката ја достигнала границата на доменот. Ако пак пораката се пропушти од страна на уредот (во овој случај хабот) тогаш емисиониот домен продолжува сè до уредот кој ќе ја блокира емисијата. Постојат уреди кои ја блокираат емисијата, но ги пропуштаат другите пораки.

Друга карактеристика која го дефинира мрежниот сегмент е доменот на колизии (collision domain). Колизиите се случуваат кога два уреди се обидуваат да вршат пренос истовремено, предизвикувајќи зголемување на нивото на електричниот сигнал. Кога ќе се случи колизија, сите уреди од истиот домен на колизии ја детектираат грешката и се повлекуваат од пренесувањето за одреден временски период. Во поранешните Ethernet мрежи, домените на емисии и колизии се однесувале на иста област на мрежата, сè до појавата на мостовите и (подоцна) преклопниците.

Поделба – сегментирање на локална мрежа

Одредени уреди како што се мостовите, преклопниците и рутерите можат да се искористат за поделба на LAN врз основа на домени на колизии. Секој порт на мостот или преклопникот е засебен домен на колизии. Овие уреди се дизајнирани да ги спречат колизиите да преминат кон другите поврзани сегменти. Другите уреди ги пропуштаат колизиите кон сите уреди поврзани со нив; репетиторите и концентраторите ги пропагираат колизиите и го прошируваат доменот на колизии. Потребно е внимателно користење на овие уреди за да не се надмине дозволениот број на јазли по мрежен сегмент. На следнава слика се прикажани повеќе сегменти на една локална мрежа LAN.



Слика 4.14: Сегментирање на мрежа

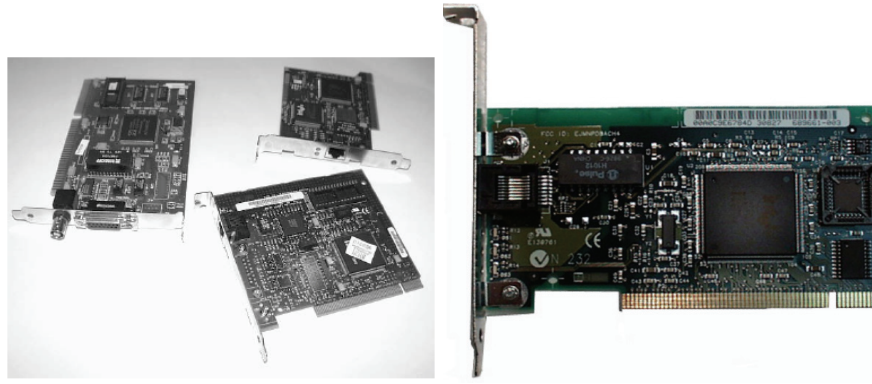
4.2.3 Мрежни адаптери (Network Interface Cards)

Мрежен адаптер или мрежна картичка (Network Interface Card – NIC), овозможува поврзување на уредите кон мрежата. Мрежните картички можат да обезбедат поврзување со секаков вид на мрежен медиум, вклучувајќи го и безжичниот пренос. За поврзување на мрежата, покрај серверите и работните станици, и мрежните принтери и другите уреди може да имаат мрежен

адаптер. Мрежната картичка користи софтвер – драјвер (driver), за комуникација со оперативниот систем на работната станица.

Секоја Ethernet и Token Ring мрежна картичка поседува физичка адреса која е хардверски кодирана во уредот од страна на производителот. Таа адреса се нарекува и Media Access Control (MAC), и претставува хексадекаден број преку кој се идентификува производителот на уредот. MAC адресата треба да биде единствена, така што пакетите може соодветно да се адресираат и да ги достигнат одредените уреди. Со замена на мрежната картичка, исто така се менува и MAC адресата.

Кога еден уред сака да комуницира со друг уред, тој ја користи табелата од ARP протоколот, каде што се содржани MAC адресите на другите уреди од мрежата. При промената на хардверот или со додавање на нов уред, потребно е краток временски период за обновување во табелата. Кај некои уреди пак, како што се рутерите, може да е потребно да се избрише ARP табелата која се чува во меморијата. На тој начин се чистат старите информации и се принудува уредот да ја креира ARP табелата одново. Некои видови на мрежни картички NIC дозволуваат измена на MAC адресата; оваа способност е ретка и може да се најде кај постарите модели на мрежни картички.



Слика 4.15: Различни изведби на мрежни картички

При изборот на мрежна картичка за работна станица, преносен компјутер или сервер, потребно е да се внимава на следниве фактори:

- Картичката треба да го поддржува типот на мрежата. На пример, за Ethernet мрежа треба да се користи соодветна Ethernet мрежна картичка.
- Картичката треба да има соодветен конектор за мрежниот медиум, на пример оптички SC конектор, коаксијален BNC или RJ-45 конектор.

- Картичката треба да ги поддржува типовите на слотови за проширување кои постојат на матичната плоча, како што е на пример PCI.

Преносниците (Laptop) кои немаат вградена мрежна картичка треба да имаат уред како што е PCMCIA картичка која има приклучок за одреден вид на мрежа, вклучувајќи ја и безжичната. Повеќето производители на матичните плочи им вградуваат мрежен адаптер за Ethernet мрежа 10/100, иако може да постои потреба за вградување и на дополнителен мрежен адаптер.

Извор и одредиште

Мрежната картичка обезбедува и други комуникациски системи и механизми кои овозможуваат уредот да комуницира на мрежата. Мрежната картичка работи на податочното и физичкото ниво од OSI референтниот модел и обезбедува повеќе функции - како извор за испраќање на податоци и како одредиште за примање на податоците. Како изворен уред, мрежната картичка:

- прима пакети од мрежното ниво
- додава своја MAC адреса на податочниот пакет
- додава MAC адреса на одредишниот уред на податочниот пакет
- ги претвора податоците во пакети соодветни на методот за пристап на мрежата (Ethernet, Token Ring, FDDI)
- ги претвора пакетите во електрични, светлосни или радио сигнали за испраќање преку мрежата
- обезбедува физичка конекција кон медиумот

Како одредишен уред, мрежната картичка:

- обезбедува физичка конекција на медиумот
- ги претвора електричните, светлосните или радио сигналите во податоци
- ја чита одредишната MAC адреса, за да види дали се совпаѓа со сопствената
- ако се совпаѓа, ги пренесува пакетите кон мрежното ниво

4.2.4 Репетитори (Repeaters)

Репетирори (Repeaters) се мрежни уреди кои овозможуваат поврзување на сегментите заради продолжување на максималното растојание на кабелскиот сегмент. Репетиторот функционира на физичкото ниво на OSI моделот и поврзува два сегменти на иста мрежа. Репетитор со повеќе портови, познат и како хаб - hub, поврзува повеќе сегменти заедно. Репетиторот може да изврши поврзување на сегменти на истата мрежа кои користат различни

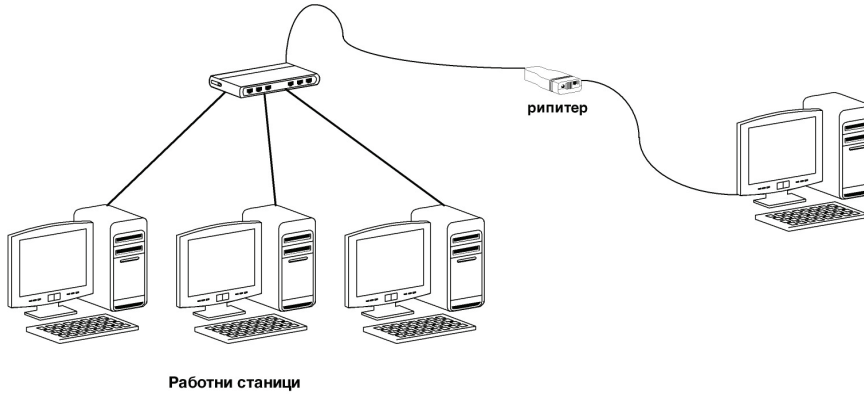
мрежни медиуми, како што се на пример Ethernet сегмент со коаксијален кабел и друг сегмент кој користи Cat 5.

Репетиторот има три основни функции:

- го прима и прочистува дојдовниот сигнал.
- го ресинхронизира сигналот заради избегнување на колизии.
- го емитува сигналот на поврзаниот сегмент.

На сликата 4.17 е прикажано како репетиторот може да го продолжи досегот на мрежата, надминувајќи го ограничувањето на растојанието на единичниот кабелски сегмент.

Слика 4.16: Изглед на различни изведби на репетитори (оптички и безжичен)



Слика 4.17: Продолжување на досегот на мрежен сегмент со репетитор

Користењето на репетиторот може да помогне при регенерирање на сигналите кои патуваат низ области со високо ниво на електромагнетна интерференција (EMI).

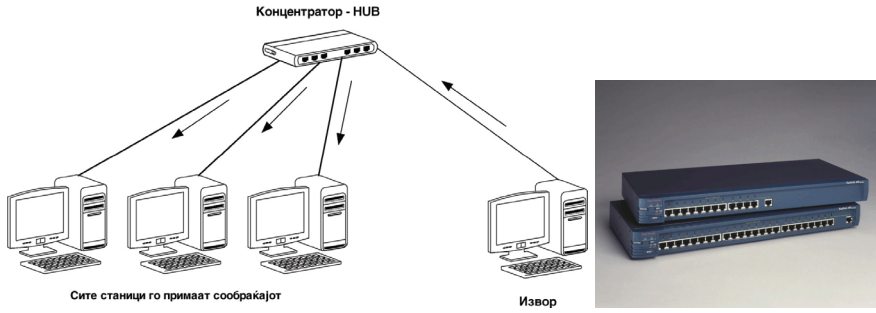
4.2.5 Хабови (Hub)

Концентраторот е централна точка на поврзување на кабелските сегменти во физичката топологија на ѕвезда. Тој овозможува поврзување на повеќе уреди

на мрежата и може да обезбеди различни дополнителни сервиси во зависност од сложеноста на концентраторот. Според потребите може да се избере некој од понудените варијанти како што се управувани концентратори (managed hubs), преклопувани (switched hubs), дури и интелигентни концентратори (“intelligent hubs”), каде секој нуди дополнителни сервиси, покрај основните што ги дава основниот концентратор.

Иако поимот концентратор се однесува на одреден мрежен уреди, тој всушност претставува репетитор со повеќе порти.

Како повеќе-портен репетитор, концентраторот работи на ист начин, со тоа што тој треба да го регенерира сигналот за сите поврзани сегменти. Концентраторите работат на физичкото ниво на OSI моделот. Тие ги пропуштаат сите податоци кои ги примаат, без разлика за кој уред и на кој сегмент се наменети, со што се придонесува кон натрупувањето на сообраќајот на мрежата. На следната слика е даден приказ на едноставен 4-портен концентратор поврзан со мрежните уреди во физичка топологија на ѕвезда:



Слика 4.18: Хаб поврзан во топологија на ѕвезда

Како што може да се претпостави, користење на поголем концентратор (како што е 24-портен) или поврзување на повеќе концентратори меѓусебно (stacking), може да има значително влијание на мрежните перформанси, затоа што сите уреди треба да ослушнуваат кон сите други уреди и да чекаат момент кога ќе снема активност на мрежата за да вршат пренос. При изборот на концентратор за Ethernet мрежа, треба да се обрне внимание на:

Видот на медиумот. Обично концентраторите имаат приклучоци за еден вид на мрежа, иако некои додаваат и друг порт ; на пример многу 10BaseT концентратори обезбедуваат еден BNC порт, а останатите се RJ-45 портови.

Бројот на потребни портови. Хабовите може да се најдат во конфигурации од 4 до 48-порти. Можно е заедничко поврзување на 24-портни концентратори за добивање на вкупно 96 порти.

Брзина. Концентраторите обично пренесуваат податоци со брзина од 10Mbps. Некои пософистицирани имаат една или повеќе порти да примо-

предаваат на 10Mbps или 100Mbps, или пак се способни да префрлување од една брзина на друга, во зависност од прикачениот уред.

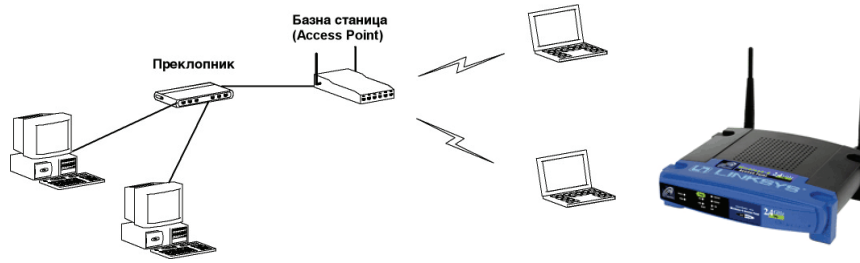
Управуван или не-управуван. Управуваните уреди му овозможуваат на мрежниот администратор да користи софтверска апликација и да врши увид во работењето на уредот од оддалечена работна станица.

Постоење на „uplink“ порта. Uplink портата е неопходна кога се поврзуваат два концентратори со користење на „patch“ кабел. Повеќето концентратори имаат мал преклопник поставен до „uplink“ портата за префрлување на „uplink“ или обичен начин на работа. Ако не постои таква порта, потребно е да се користи „crossover“ кабел за поврзување помеѓу концентраторите.

Концентраторите на Token Ring мрежите, наречени MAU, обезбедуваат иста централна конекција за уредите во форма на физичка топологија на ѕвезда. MAU работат на различен начин во однос на Ethernet концентраторите, со пренесување на податоците од уред до уред во облик на логички прстен.

4.2.6 Пристапни точки (Access Points)

Пристапни точки (Access points AP) се хардверски уред или софтвер, кој се однесува како безжичен концентратор. Кога се користи во комбинација со обична жичена LAN мрежа, AP им овозможува на корисниците поврзување на жичените мрежни сервиси. Кога AP се користи за поврзување кон жичена мрежа, се вели дека безжичната мрежа работи на инфраструктурен начин. На следнава слика е прикажан AP поврзан на мрежа, кој обезбедува сервиси на безжичните уреди.



Слика 4.19: Точка на пристап поврзана во инфраструктурен мод и изглед на AP

Во домашните мрежи - безжичните пристапни точки се користат за поврзување на DSL линија, кабелски модеми или дури 56K „dial-up“ конекција - на тој начин повеќе корисници може да пристапат на Интернет или други уреди со користење на еден уред.

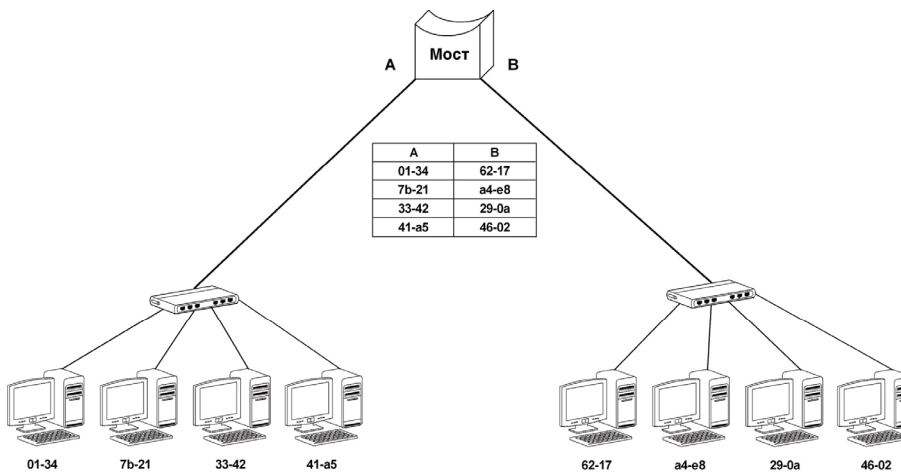
AP можат да се користат и независно без поврзување на жичена LAN мрежа. На овој начин, го прошируваат досегот на безжичната комуникација во еден WLAN; повеќе безжични уреди може да комуницираат секој со секој преку AP.

Пристапните точки, како и самиот безжичен пренос не се безбедни како уредите на жичената мрежа. Потенцијално секој што поседува безжична мрежна картичка може да пристапи на сервисите на точката за пристап. Затоа на уредите се овозможува избор на ниво на обезбедување кое може да се движи од 64-битна, до високо-ниво 256-битна енкрипција. Wireless Equivalent Privacy (WEP) е еден начин за енкрипција користен во 802.11 безжичните мрежи, а Wireless Protected Access (WPA) е наследникот на WEP и обезбедува 256-битна енкрипција.

4.2.7 Мостови (Bridges)

Мостовите, како и концентраторите поврзуваат LAN сегменти, но функционираат на податочното (Data Link) ниво на OSI моделот. Затоа што работат на второто ниво, мостовите може да ги користат MAC адресите за донесување на одлуки за примените податочни пакети - дали ќе ги пропуштат или не кон следниот мрежен сегмент. Мостовите обезбедуваат четири основни функции:

- Креираат табела за премостување, за следење на сите уреди на секој сегмент.
- Вршат филтрирање на пакетите кои не треба да се пропуштат на другите сегменти, во зависност од нивната MAC адреса.
- Ги пропуштаат пакетите чија одредишна MAC адреса е на различен мрежен сегмент од изворот.
- Вршат поделба на една мрежа во повеќе домени на колизии, намалувајќи ги колизиите на секој мрежен сегмент.

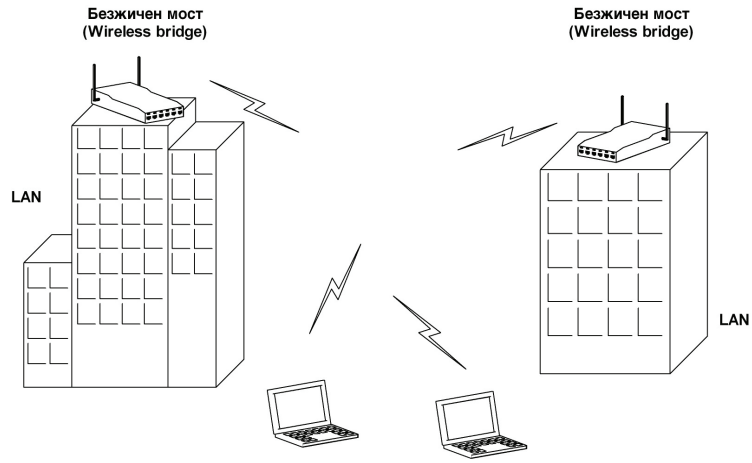


Слика 4.20: Функционирање на мостовите

Мостовите го користат протоколот Spanning Tree Protocol (STP) за донесување одлука дали да се пропушти пакетот низ мостот кон друг мрежен сегмент. STP служи за две намени: една е да се одреди главниот мост, наречен root, кој ќе ги донесува сите одлуки за премостување и ќе ги решава проблемите. Втората функција е да се одбегнат повратните врски (bridging loops). Сликата 4.20 покажува како мостовите примаат податоци, ги филтрираат во зависност од MAC адресата и ги пропуштаат ако има потреба за тоа.

4.2.8 Безжични мостови (Wireless Bridges)

Безжичните мостови се дизајнирани за поврзување на две или повеќе мрежи, обично во различни објекти. Безжичните мостови се поевтини за имплементација од поставување на оптички кабли, или изнајмување на линии од провајдер. Безжичните мостови може да обезбедат брзини на пренос од 10Mbps или дури 100Mbps, во зависност од моделот; истите мостови може да послужат за поврзување на безжичните клиенти на мрежата, исто како и базната станица – точка на пристап. На следната слика е прикажан безжичен мост кој поврзува два LAN сегменти и исто така обезбедува безжичен пристап на клиентите:



Слика 4.21: Безжични мостови кои поврзуваат два сегменти

4.2.9 Преклопници (Switch)

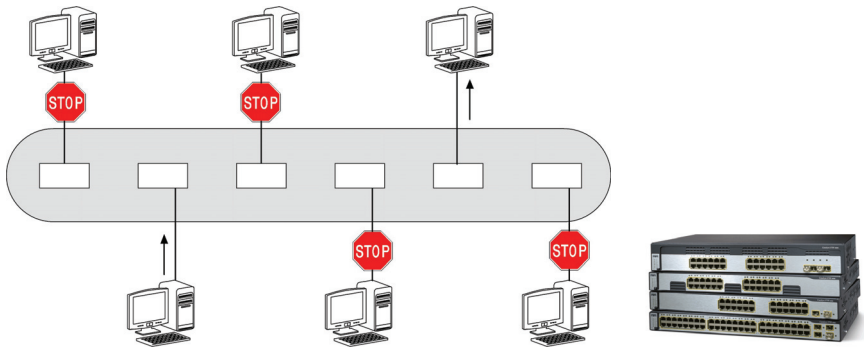
Преклопниците всушност претставуваат повеќепортни мостови кои функционираат на податочното ниво од OSI моделот. Постојат Ethernet, Token Ring, FDDI, ATM, и многу други видови на преклопници (вклучувајќи и оние кои работат на повисоките нивоа на OSI моделот). Секој порт на преклопникот врши пропуштање или не на пакетите кон мрежата.

Преклопникот води сметка за сите MAC адреси на прикачените јазли и на кој порт се поврзани, и со таа информација се врши филтрирањето исто како кај мостовите.

Преклопниците го намалуваат непотребниот мрежен сообраќај и го оневозможуваат влијанието на интензивен пренос на податоци на целата мрежа.

Исто и како кај мостовите, секоја порта на преклоникот е сопствен домен на колизии. Ако на еден порт е поврзан само еден уред, скоро и да не постојат шанси за појава на колизии.

На следнава слика е прикажано како преклопник кој поврзува сегменти од мрежата, го филтрира сообраќајот кој обично би бил пропуштен кон сите уреди од страна на концентратор:

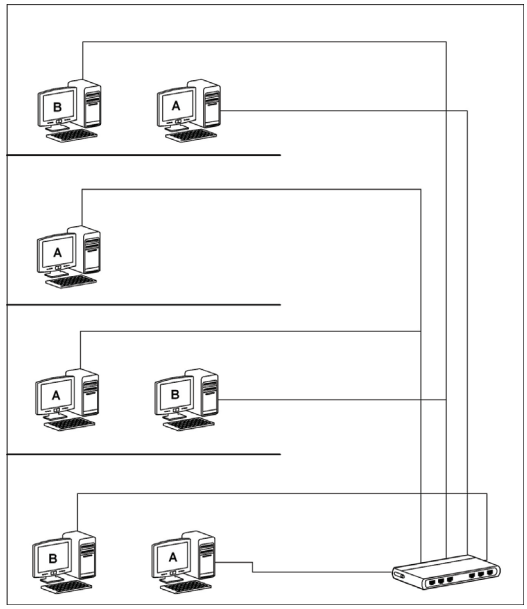


Слика 4.22: Филтрирање на сообраќајот помеѓу мрежни сегменти

4.2.10 Виртуелни локални мрежи (Virtual LAN)

Преклопниците покрај поддршката за оптичките мрежи и поголеми брзини, се развиле во правец на поддршка на сервисите на повисоките нивоа на OSI моделот. На апликациското ниво, многу преклопници имаат вграден web сервер за управување со неговите функции, што е од особено значење за далечинска администрација. Најзначајниот напредок во преклопниците е способноста за создавање на виртуелни локални мрежи Virtual LANs (VLAN).

VLAN се применуваат за креирање на емисиони домени на самиот уред. Преку VLAN, портовите може да се групираат во еден единствен емисионен домен (broadcast domain). Овој тип на VLAN може да се создаде на второто ниво преку користење на MAC адресите, или пак на третото ниво со користење на мрежните адреси (како што се IP адреси). VLAN имаат свој сопствен стандард (IEEE 802.1P и 802.1Q) кој ја специфицира употребата на рутерите за пренесување на пакетите помеѓу VLAN и другите мрежи. На слика 4.23 се прикажува како VLAN дозволуваат работата на уредите да



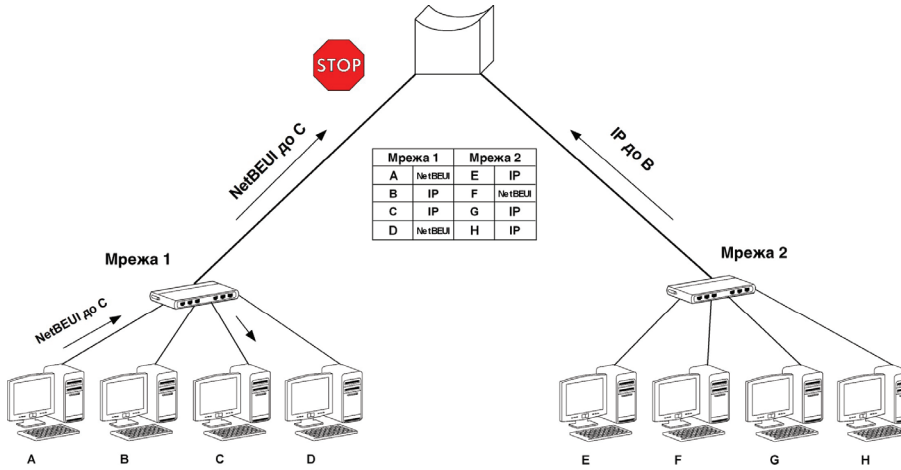
биде дел од ист мрежен сегмент, наспроти нивната физичка локација и поврзувањето.

Преклопниците може да поддржуваат една или повеќе MAC адреси по порта; на пример преклопник кој поддржува само една MAC адреса по порта не може директно да се поврзе со концентратори, затоа што постои потенцијална опасност за поврзување на повеќе уреди кои имаат свои MAC адреси.

Слика 4.23: Виртуелни локални мрежи

4.2.11 Мостови-рутери (Brouter)

Името brouter доаѓа од поимите bridge и router, уредот е хибрид кој може да работи и како мост и како рутер и може да се користи за поврзување на повеќе мрежи. Уредот може да работи на мрежи кои користат повеќе различни протоколи и дозволува мрежата да го надмине максималниот број на дозволени уреди.



Мрежа 1		Мрежа 2	
A	NetBEUI	E	IP
B	IP	F	NetBEUI
C	IP	G	IP
D	NetBEUI	H	IP

Слика 4.24: Начин на работа на brouter

„Brouters“, можат да бидат програмирани да работат на одреден начин; ако уредот е програмиран за пропуштање на пакети од тип на нерутабилни протоколи како што е NetBEUI - уредот користи MAC адреси од второ ниво за одлучување за пропуштањето на пакетот, и на овој начин работи како мост. Ако „brouter“-от е подесен за рутирање на пакетите кон соодветната мрежа со користење на рутиран протокол како што е IP, тогаш работи како рутер на мрежното ниво. На сликата 4.24 е прикажано како „brouter“ функционира истовремено како мост и како рутер.

4.2.12 Рутери (Router)

Рутерите се уреди кои работат на мрежното ниво на моделот и користат пософистициран софтвер и интелигенција во однос на другите мрежни уреди. Рутерите можат да поврзат повеќе различни мрежни сегменти кои можат да се наоѓаат во иста или оддалечена локација. Тие работат во LAN, MAN, и WAN околина. Рутерите му овозможуваат на корисникот пристап кон ресурсите во склоп или надвор од локалната мрежа, преку наоѓање на најдобрата патека до нив. Се користи мрежната адреса, т.е. IP адресата во TCP/IP протоколите за одредување на патеката по која ќе се достигне одредиштето.

Рутерите може да се користат за поврзување на различни видови на мрежи како што се Token Ring и Ethernet мрежите. Рутерот ја менува големината и форматот на пакетот за да се совпадне со видот на одредишната мрежа каде што е испратен пакетот. Рутерите уште може да поврзуваат мрежи кои користат еден од рутираните протоколи: Internet Protocol (IP), Internetwork Packet eXchange (IPX), DECnet, и AppleTalk. Не сите рутери може да се прилагодат на сите мрежи; на кои мрежи може да се поврзе рутерот е определено од типот на хардверот и софтверот кои ги користи.

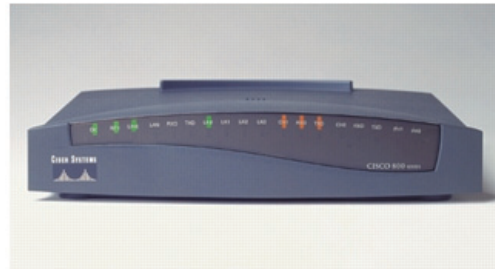
Изборот на најдобрата патека

Рутерот има две примарни функции: одредување на најдобрата патека кон дестинацијата и делење на информациите за патеките со другите рутери. Рутерот ја одредува информацијата на патеката врз основа на два вида на рутирање: статичко и динамичко рутирање. Било кој начин да се користи, рутерот ја определува патеката на пакетот преку табелата за рутирање (routing table), каде што се наоѓаат информациите за другите мрежи.

Табелата ги содржи податоците за мрежите, портата на рутерот која се користи за пристап кон одредена мрежа и „цената“ за да пакетот стигне на таа мрежа. „Цената“ уште се нарекува и метрика или мерка, и се базира на алгоритам одреден од рутирачкиот протокол кој се користи или се поставува рачно од страна на мрежниот администратор.

На слика 4.25 е прикажан шематски приказ на рутер и портовите кои се користат за поврзување на мрежата. Некои рутери имаат само два портови за

поврзување, додека другите имаат поголем број за повеќе конекции кон повеќе мрежи.

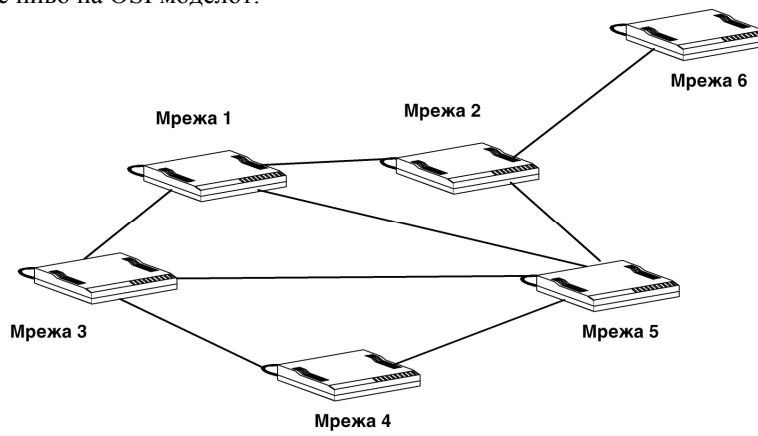


Слика 4.25: Изглед на рутер

На слика 4.26 се прикажани повеќе мрежи поврзани преку рутери. Иако постојат повеќе начини - патеки за да се стигне од мрежа 1 кон 6, рутерот ја селектира најдобрата патека врз основа на цената потребна да се стигне до неа.

Мрежни излези (Gateways)

Мрежните излези (Gateways) се уреди кои овозможуваат комуникација на различни мрежни системи. Тие обично се јазли на мрежата кои обезбедуваат сервиси за преведување, без кои не може да комуницираат две мрежи. Во зависност од видот на преведувањето кое го обезбедуваат, тие работат на секое ниво на OSI моделот.



Слика 4.26: Мрежа од мрежи

Gateway-те се користат за различни задачи на мрежата и можат да бидат категоризирани во три вида:

- Адресен излез (Address gateway) - ги поврзува мрежите кои користат ист протокол, но различни директориумски простори, како што се MHS (Message Handling Service).

- Протоколен излез (Protocol gateway) - ги поврзува мрежите кои користат различни протоколи, преку преведување на изворниот протокол на одредишната мрежа.
- Апликациски излез (Application gateway); пример, кога стандарден Интернет сервис за електронски пораки треба да испрати порака кон серверот за пораки, мрежниот излез се користи за преведување во формат разбирлив за серверот.

Поимот мрежен излез (gateway) се користи во општа смисла во умрежувањето и може да има различно значење. Ако поимот се користи за означување на уред на мрежата, тогаш значи дека се однесува на еден од овие сервиси се преведување. Обично и рутерот се нарекува мрежен излез, бидејќи извршува преведување на различните типови на мрежи на физичко, податочен–линк и на мрежно ниво.

Табела 4.7. Споредба на мрежните уреди со нивни предности и недостатоци

Уред	Предности	Недостатоци
Репетитор (Repeater)	Може да поврзува различни водови на медиуми, да ја зголеми должината на мрежата, не го зголемува мрежниот сообраќај	Го продолжува доменот на колизии, не може да поврзе различни мрежни архитектури, може да се користи само ограничен број во мрежата
Хуб (Hub)	Поврзува сегменти со различни медиуми	Го проширува доменот на колизии, не филтрира и врши пропуштање на сите пакети кон поврзаните сегменти
Пристапна точка (Access point)	За користење на помал број на уреди, не бара физичка конекција за пристап кон мрежата	Намалена сигурност, ограничен досег, влијание на пречки и интерференција
Мост (Bridge)	Го ограничува доменот на колизии, го проширува мрежниот досег, ги филтрира пакетите врз основа на нивната MAC адреса, поврзува различни видови на медиуми и мрежни архитектури	Емитуваните пакети (Broadcast) не може да се филтрираат, поскап и побавен заради процесирање на пакетите
Безжичен мост (Wireless bridge)	Дозволува безжична врска на повеќе жичени LAN сегменти, сервиси за безжични клиенти	Поскап од пристапна точка
Преклопник (Switch)	Го ограничува доменот на колизии, обезбедува преместување на повеќе сегменти од мрежата, може да биде конфигуриран за ограничување на домен на „broadcast“ преку виртуелни LAN-ови	Поскап од концентраторот и мостот, конфигурацијата е посложена
Brouter	Го ограничува доменот на колизии, обезбедува сервиси од рутери и мостови во еден уред	Поскап од мостот
Рутер (Router)	Го ограничува доменот на колизии; може да работи и во LAN или WAN околина, поврзува мрежи со користење на различни медиуми и архитектури, може да определи најдобра патека за достигнување на друга мрежа, филтрира „broadcast“ сообраќај	Скап, мора да се користи со рутабилни протоколи, конфигуриран од администратор, сложен за конфигурација, побавен од мостот заради процесирање на рутирачките табели
Мрежен излез (Gateway)	Поврзува различни системи на мрежи со користење на различни протоколи, адреси и апликации	Сложен за инсталација и конфигурација, дополнителното губење на време за процесирање го забавува сообраќајот

5 LAN ТЕХНОЛОГИИ

5.1 ВОВЕД ВО LAN ПРОТОКОЛИ

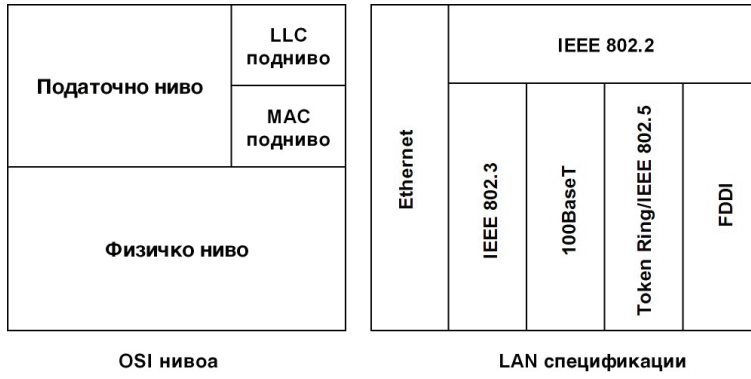
Во ова поглавје се прикажани различни методи за пристап на медиумот, начини на трансмисија, топологии и уреди кои се користат во локалните мрежи (LAN). Посебно внимание е посветено на методите и уредите користени во Ethernet/IEEE 802.3, Token Ring/IEEE 802.5, и Fiber Distributed Data Interface (FDDI).

5.2 ПОИМ ЗА ЛОКАЛНА МРЕЖА - LAN

Како што е претходно објаснето, локалната мрежа претставува податочна мрежа со големи брзини на пренос која покрива релативно мала географска област. Таа обично поврзува работни станици, персонални компјутери, печатари, сервери и други уреди. Локалните мрежи им овозможуваат на корисниците многу погодности, како што се пристап до делени ресурси – уреди и апликации, размена на датотеки и комуникација помеѓу корисниците преку електронска пошта и други апликации.

5.2.1 LAN протоколите и OSI референтниот модел

LAN протоколите работат на најниските две нивоа на OSI референтниот модел, физичкото и податочното ниво. На сликата се прикажани неколку популарни протоколи во LAN мрежите, пресликани во нивоата на OSI моделот.



Слика 5.1: LAN протоколи пресликани во OSI референтниот модел

5.2.2 Начини на пристап на медиумот кај локалните мрежи

Натпревар за пристап на медиумот помеѓу два или повеќе мрежни уреди, се појавува при обид за истовремено испраќање на податоци на мрежата. Бидејќи уредите не можат да пренесуваат на мрежата истовремено, потребно е да се користи некој метод за овозможување само на еден уред да пристапи кон мрежниот медиум во даден момент. Како што е веќе опишано во Глава 3, тоа може да се оствари на два начини: со механизмот „Carrier Sense Multiple Access Collision Detect“ (CSMA/CD) и проследување на токени.

Во мрежите кои користат CSMA/CD технологија, како што е Ethernet, мрежните уреди се натпреваруваат за мрежниот медиум. Кога уредот има податоци за испраќање, првин ослушнува дали мрежата се користи - ако не започнува со испраќањето на податоци. По завршувањето на преносот, ослушнува пак за да види дали се појавила колизија. При појава на колизија, секој уред чека случајно време пред да започне со повторно испраќање на податоците. Во најголем број на случаи, колизијата нема да се повтори пак помеѓу двата исти уреди. Заради натпреварот за мрежниот медиум, како што мрежата станува пооптоварена, се зголемува бројот на колизиите, и како што беше кажано во поглавјето 3, перформансите на мрежата опаѓаат со зголемување на бројот на мрежните уреди.

Во мрежите со проследување на токени (token-passing), како што се Token Ring и FDDI, се пренесува мрежна рамка наречена токен, по мрежата од уред до уред. Кога уредот има податоци за испраќање, потребно е да чека сè додека не го добие слободниот токен и тогаш да започне со преносот. По завршувањето на преносот, токенот се ослободува така што и другите уреди може да го користат мрежниот медиум. Главната предност на овој тип на мрежи е тоа што тие се детерминистички, и лесно се преместува максималното време на чекање за добивање на можност еден уред да врши пренесување. Мрежите со проследување на токени се користат во околини кои работат во реално време, како што се производни погони, каде што машините треба да комуницираат во одреден интервал.

Кај CSMA/CD мрежите, преклопниците ја сегментираат мрежата во повеќе домени на колизии, со што се намалува бројот на уредите по мрежен сегмент кои ќе се натпреваруваат за пристап на медиумот и се постигнува подобрување на перформансите на мрежата.

Треба да се истакне дека CSMA/CD мрежите работат во „half-duplex“ начин, што значи додека уредот што испраќа информација, истовремено не може и да прима, односно не може да ослушнува за друг сообраќај. Со појавата на преклопниците станало можно и „full-duplex“ функционирањето - уредот може и да испраќа и да ослушнува за сообраќај. Кога мрежниот уред е прикачен директно на пората на мрежниот преклопник, и двата уреди се способни да работат во „full-duplex“, со што се добива зголемување на перформансите. Ethernet сегментот со 100-Mbps е способен за пренос на податоци со брзина од 200 Mbps, но само 100 Mbps може да се користат во една насока.

Мрежите со проследување на токени, како што е Token Ring, исто може да имаат корист од мрежните преклопници; во поголемите мрежи, доцнењето помеѓу времето за испраќање може да биде значително поради патувањето на токенот низ мрежата.

5.2.3 Начини на пренесување по локални мрежи

Пренесувањето на податоци по LAN мрежите може да се категоризира во три категории: unicast, multicast, и broadcast. Во секој вид на пренос, пакетот се испраќа кон еден или повеќе јазли.

Во „unicast“ преносот, еден пакет се испраќа од изворот кон одредиштето на мрежата. Прво јазолот – извор го адресира пакетот со адресата на одредишниот јазол, го испраќа по мрежата и мрежата го донесува до одредиштето.

Во „multicast“ преносот, единичниот пакет се копира и се испраќа кон одредено множество на јазли на мрежата. Прво изворниот јазол го адресира пакетот со користење на „multicast“ адреса. Пакетот се испраќа на мрежата, која прави копии на пакетот и испраќа по една копија за секој јазол кој е дел од „multicast“ адресата.

При „broadcast“ пренос, единичниот пакет се копира и се испраќа на сите јазли на мрежата. Изворниот јазол го адресира пакетот до „broadcast“ адреса, пакетот се испраќа на мрежата која прави копии од него и ги испраќа до секој јазол на мрежата.

5.3 ETHERNET ТЕХНОЛОГИИ

Поимот Ethernet (Ethernet) се однесува на фамилија производи за локални мрежи опфатени со стандардот IEEE 802.3, кој го дефинира она што е познато како CSMA/CD протокол. Моментно се дефинирани три брзини за пренос преку оптички кабли и плетени парици:

- 10 Mbps - 10Base-T Ethernet
- 100 Mbps - Fast Ethernet
- 1000 Mbps - Gigabit Ethernet

10-Gigabit Ethernet е објавен како дополнение со ознака IEEE 802.3a кон IEEE 802.3-основниот стандард во 2002 година.

Ethernet е најкористената LAN технологија (се користи кај околу 85% од постоечките умрежени компјутери), затоа што овој протокол ги има следните карактеристики:

- Лесен е за имплементација, управување и одржување
- Евтина имплементација на мрежи
- Овозможува флексибилниот на топологијата при инсталација

- Гарантира успешна интерконеција и работа на компатибилни уреди, без разлика на вендорот.

5.3.1 Кратка историја на Ethernet

Оригиналниот Ethernet е развиен како експериментална мрежа со коаксијален кабел во 70-тите, од страна на Xerox корпорацијата, за работа со брзини од 3 Mbps и користење на CSMA/CD протоколот за локални мрежи со спорадичен и повремено интензивен сообраќај. Успехот на тој проект довел до заеднички развој на Ethernet со 10-Mbps со ознака верзија 1, од страна на конзорциум на компаниите: Digital Equipment Corporation, Intel Corporation, и Xerox Corporation. Оригиналниот IEEE 802.3 стандард е базиран и многу сличен на Ethernet верзијата 1.

Во 1985 е објавен званичниот стандард со ознака ANSI/IEEE Std. 802.3-1985. Оттогаш наваму, се појавиле бројни дополненија на стандардот (со развојот на новите технологии, и за поддршка на новите медиуми и повисоки брзини на пренос, како и нови опционални начини на пристап кон медиумот).

5.3.2 Елементи на Ethernet мрежата

Ethernet локалните мрежи се состојат од мрежни јазли и медиум за поврзување. Мрежните јазли спаѓаат во две категории:

- Податочна терминална опрема (Data terminal equipment DTE) – уреди кои се или извор или одредиште на податочни рамки. Обично DTE уредите се компјутери, работни станици, сервери за датотеки и печатачи, и обично се нарекуваат крајни станици (end stations).
- Податочна комуникациска опрема (Data communication equipment DCE) – посреднички мрежни уреди кои ги примо-предаваат рамките низ мрежата. DCE може да бидат самостојни уреди како што се репетиторите, мрежните преклопници и рутерите, или комуникациски интерфејси како што се мрежните адаптери и модеми.

Медиумите за поврзување ги вклучуваат двата вида на бакарни кабли UTP и STP, како и неколку вида на кабли со оптички влакна.

5.3.3 Ethernet мрежни топологии и структури

Локалните мрежи може да имаат повеќе тополошки конфигурации, но без разлика на нивната големина или сложеност, сите се комбинација од трите најосновни поврзувачки структури или градбени блокови на мрежата.

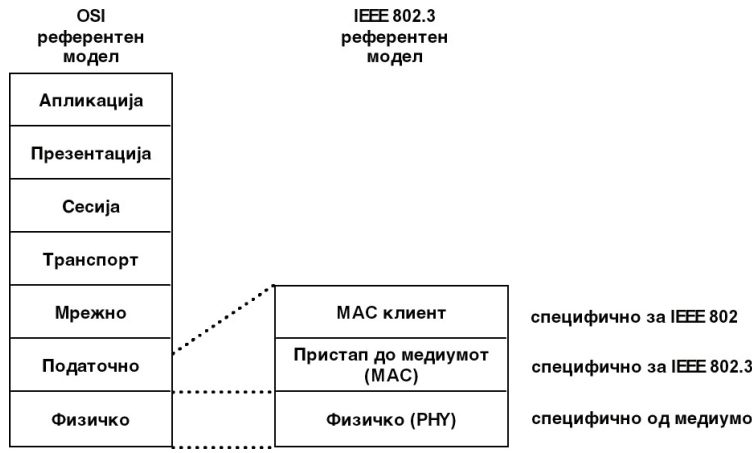
Наједноставната структура е конекција еден-еден (point-to-point). Во поврзувањето учествуваат два уреди и тоа може да биде DTE-DTE, DTE-DCE, или DCE-DCE. Кабелот во конекцијата еден на еден се нарекува мрежен линк, а максималната дозволена должина на кабелот зависи од видот и методот на пренос што се користи.

Оригиналните Ethernet мрежи се имплементирани во структура на коаксијална магистрала. Должините на сегментите се ограничени на 500 м и најмногу 100 јазли може да се поврзат на еден сегмент. Поединечните сегменти може да бидат поврзани со репетитори, доколку не постојат повеќе патеки помеѓу две станици, и бројот на DTE уреди е помал од 1024. Вкупната должина на патеката помеѓу најоддалечените станици, исто така, не смее да го надмине препорачаното ограничување.

Иако новите мрежи не се поврзуваат во топологијата магистрала, сè уште постојат постари мрежи кои користат магистрала. Во раните 90-ти, сè попопуларни стануваат топологиите на ѕвезда. Централниот уред е или повеќе-портен репетитор (концентратор), или мрежен преклопник. Сите конекции во мрежата со топологија на ѕвезда се од типот еден-еден, со користење на плетени парици или оптички влакна.

5.3.4 Поврзаност на IEEE 802.3 со ISO референтниот модел

На сликата 5.2 се прикажани слоевите на IEEE 802.3 и нивната поврзаност со OSI референтниот модел. Како и со сите IEEE 802 протоколи, ISO податочното ниво е поделно во два подслоеви, Media Access Control (MAC) поднивото и MAC-клиент поднивото. Физичкото ниво на IEEE 802.3 соодветствува на ISO физичкото ниво.



Слика 5.2: Логичката поврзаност на Ethernet моделот со OSI референтниот модел

MAC-клиент поднивото може да биде едно од наведените:

- Logical Link Control (LLC), ако уредот е DTE. Ова поднивото обезбедува интерфејс помеѓу Ethernet MAC и повисоките нивоа во протоколниот стек на крајната станица. LLC поднивото е дефинирано од страна на IEEE 802.2 стандардите.

- Ентитет-мост, ако уредот е DCE. Обезбедуваат LAN-LAN интерфејси помеѓу локални мрежи што користат ист протокол (на пример, Ethernet со Ethernet), а исто така помеѓу различни протоколи (Ethernet со Token Ring). Ентитетите-мостови се дефинирани со IEEE 802.1 стандардите.

Бидејќи спецификациите за LLC и ентитетите на мостовите се исти за сите IEEE 802 LAN протоколи, компатибилноста на мрежата станува главна одговорност на одреден мрежен протокол.

MAC нивото го контролира пристапот на јазлите кон мрежниот медиум и е специфично за индивидуален протокол. Сите IEEE 802.3 MAC спецификации треба да ги имаат истите основни логички барања, без разлика дали вклучуваат еден или повеќе опционални проширувања на протоколите. Основно барање за комуникација помеѓу два мрежни јазли е дека и двете MAC поднивоа треба да ја поддржуваат истата брзина на пренос.

Физичкото ниво на 802.3 е специфично според брзината на пренос, кодирањето на сигналите и видот на медиум што ги поврзува двата јазли на мрежата. На пример, гигабитскиот Ethernet е дефиниран да работи или преку плетена парица или преку оптички влакна, но секој вид на кабел или процедура за кодирање бара различна имплементација на физичкото ниво.

5.3.5 Ethernet MAC подниво

MAC поднивото има две глави одговорности:

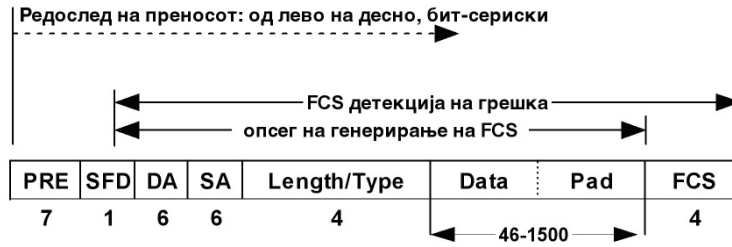
- Енкапсулација на податоците, вклучувајќи составување на рамката пред испраќање на мрежата, и парсирање и проверка од грешки по нејзиното примање.
- Контрола на пристапот кон медиумот, вклучувајќи и иницијација на испраќањето на рамката и опоравување од неуспешно пренесување.

5.3.6 Формат на Ethernet рамка

Стандардот IEEE 802.3 дефинира основен формат на Ethernet рамка, што е неопходна за сите MAC имплементации, плус неколку дополнителни формати кои се користат за проширување на основните можности на протоколот. Основниот формат на рамката содржи 7 полиња прикажани на сликата 5.3.

- Преамбула (Preamble PRE) - се состои од 7 бајти и претставува наизменична низа на единици и нули со кои се најавува доаѓањето на рамката и обезбедува начин за синхронизација за прифаќање на рамката од страна на физичкото ниво.
- Ограничувач на почетокот на рамката (Start-of-frame delimiter SOF) – се состои од 1 бајт, и SOF е наизменична низа на единици и нули која завршува со две единици, со што се означува дена наредниот бит е најлевиот до најлевиот бајт на одредишната адреса.

- Одредишна адреса (Destination address DA) – се состои од 6 бајти. Полето DA идентификува кои станица(и) треба ја примат рамката. Најлевиот бит до полето означува дали адресата е индивидуална (означена со 0), или групна адреса (означена со 1). Вториот бит означува дали DA е глобално адресирана (означено со 0) или локално (означено со 1). Останатите 46 бита имаат еднозначна вредност со која се идентификува една станица, дефинирана група на станици, или сите станици на мрежата.
- Изворна адреса (Source addresses SA) – се состои од 6 бајти. SA полето ја идентификува станицата што испраќа и секогаш е индивидуална адреса при што најлевиот бит во полето е секогаш нула.
- Должина / вид (Length/Type) - се состои од 2 бајти и ова поле го означува бројот на податочните бајти содржани во податочното поле на рамката, или видот на рамката ако е составена со користење на опционален формат. Ако вредноста на ова поле е помала или еднаква на 1500, бројот на LLC бајтите во податочното поле е еднаков на вредноста на полето. Ако вредноста во полето е поголема од 1536, рамката користи опционален формат, и вредноста на полето идентификува одреден тип на рамка која се примо-предава.
- Податоци (Data) – претставува низа од *n* бајти со било која вредност, каде што n е помало или еднакво на 1500. Ако должината на податочното поле е помало од 46, полето треба да се дополни до нули за да се доведе до 46.
- Секвенца за проверка на рамката (Frame check sequence FCS) – се состои од 4 бајти и содржи 32 битна (Cyclic Redundancy Check - CRC) вредност, која се креира од страна на MAC поднивото и повторно се пресметува при примањето од страна на MAC - за проверка за оштетени рамки. FCS се генерира од полињата DA, SA, Length/Type, и податочното поле.



Слика 5.3: IEEE 802.3 MAC формат на податочна рамка

5.3.7 Пренесување на рамката

Кога MAC подслојот на крајната станица ќе прими барање за испраќање на рамката придружено со информација за адресата и податоците од страна на

LLC подслојот, MAC ја започнува секвенцата на преносот со префрлувањето на LLC информацијата во рамковниот бафер на MAC подслојот.

1. Преамбулата и почетниот делимитер се вметнуваат во PRE и SOF полињата.
2. Одредишната и изворната адреса се вметнуваат во адресните полиња.
3. Се бројат бајтите од LLC податоците и се вметнуваат во полето за должина или видот на рамката.
4. LLC податоците се вметнуваат во податочното поле и ако бројот е помал од 46 се дополнува до оваа вредност.
5. Се пресметува вредноста на FCS преку полињата DA, SA, Length/Type, и се додава на крајот на податочното поле.

По составувањето на рамката, пренесувањето кон мрежата зависи дали MAC работи во „half-duplex“ или „full-duplex“ начин. Тековниот IEEE 802.3 стандард бара сите Ethernet MAC подслоеви да поддржуваат „half-duplex“ функционирање, а „Full-duplex“ е опционална можност.

5.3.8 „Half-Duplex“ пренос - CSMA/CD метод за пристап

CSMA/CD протоколот е развиен како начин со кој две или повеќе станици можат да делат заеднички медиум во средина каде што нема централно управување, токени за пристап или доделени временски слотови, за индикација кога на станицата ќе и биде дозволено да врши пренос. Секој Ethernet MAC подслој самостојно одредува кога може да испрати податочна рамка.

Правилата за пристап на CSMA/CD протоколот може да се сведат на:

- „Чувствување на носачот“ (Carrier sense) - секоја станица континуирано ослушнува за сообраќај на медиумот и дознава кога ќе се појави слободен период помеѓу преноси.
- „Повеќекратен пристап“ (Multiple access) – Станиците може да започнат со пренесувањето секогаш кога мрежата мирува односно нема сообраќај.
- Collision detect – ако две или повеќе станици на истата CSMA/CD мрежа, односно домен на колизии, започнат со пренос во приближно исто време, битските низи ќе интерферираат една со друга и податоците што се пренесуваат ќе станат нечитливи. Ако дојде до овој случај, секоја станица треба да биде способна да ја детектира колизијата пред завршување на испраќањето на рамката.

Секоја станица треба да го запре испраќањето штом ќе се детектира колизија и треба да почека одредено случајно време (одредено со „back-off“ алгоритам), пред повторниот обид за ретрансмисија на рамката.

Најлошиот случај се појавува кога две оддалечени станици на мрежата се обидуваат да испратат рамка и кога втората станица не започнува со

испраќање сè до моментот пред да пристигне рамката од првата станица. Колизијата ќе се детектира веднаш кај втората станица, но не и кај првата, и оштетениот сигнал ќе се испрати назад кон неа. Максималното време кое е потребно за детекција на колизијата (прозорец на колизијата, или временски слот) е еднакво на два пати од времето на пропагација на сигналот помеѓу две најоддалечени станици на мрежата.

Тоа значи дека и минималната должина на рамката и најголемиот дијаметар на колизии се директно поврзани со прозорецот на колизиите. Подолги минимални должини на рамки се поврзуваат со подолг временски слот и поголеми мрежни дијаметри; пократки минимални должина на рамки одговараат на пократки времиња и помали колизиони дијаметри.

Компромисот се состои во потребата да се намали влијанието на опоравувањето од колизии и потребата за поголеми мрежни дијаметри за поддршка на поголема мрежа; се избира најголемиот мрежен дијаметар (околу 2500 метри) и тогаш се поставува најмалата должина на рамките - доволно голема за обезбедување на детекција и во најлошиот случај на појава на колизии.

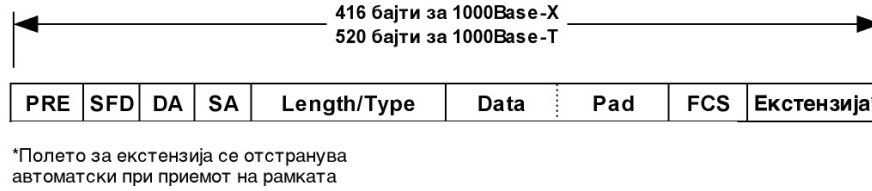
Компромисот работи многу добро за брзини 10 Mbps, но се појавува проблем за повисоки брзини на Ethernet мрежи. Брзиот Ethernet (Fast Ethernet) треба да поддржи компатибилност со поранешните Ethernet мрежи, вклучувајќи го постоечкиот IEEE 802.3 формат на рамки и процедури за детекција на грешки, како и апликациите и мрежниот софтвер кој се извршувал на 10-Mbps мрежи.

Иако брзината на пропагација на сигналот е во принцип иста за сите брзини на пренос, времето потребно за испраќање на рамката е обратно пропорционално со брзината на пренос.

Со брзина од 100 Mbps, рамка со најмала дефинирана должина може да се пренесе во една десетина од времето на прозорецот на колизијата, и ако се појави колизија во тоа време - нема да биде откриена од станиците кои емитираат. Од тоа произлегува дека најголемиот мрежен дијаметар специфициран за мрежа од 10-Mbps не може да се користи за 100-Mbps мрежи. Решението за брзиот Ethernet е да се намали максималниот мрежен дијаметар за фактор 10 (нешто повеќе од 200 метри).

Истиот проблем се појавува и при развојот на гигабитски Ethernet (Gigabit Ethernet), но намалувањето на мрежниот дијаметар за фактор 10 (20 метри) за работа при брзина 1000-Mbps, не е практично. Затоа се избира приближно ист дијаметар за домени на колизии, како и за 100-Mbps мрежи, и се зголемува најмалата големина на рамката преку дополнување со поле за проширување на рамките кои се помали од најмалата должина (полето за проширување се отстранува по примањето на рамката).

Сликата го прикажува форматот со полето за проширување за гигабитскиот Ethernet, а табелата го покажува ефектот на компромисот помеѓу брзината на пренесувањето и најмалата големина на рамката за 10-Mbps, 100-Mbps, и 1000-Mbps Ethernet.



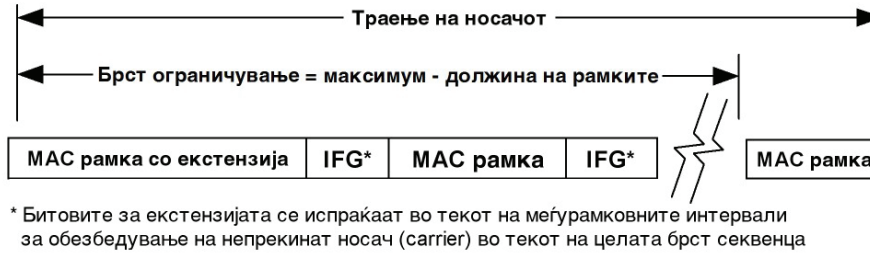
Слика 5.4: MAC рамка за Гигабтиски Ethernet

Друга измена на Ethernet CSMA/CD спецификацијата е додавање на „bursting“ на рамките за гигабитско работење. „Burst“ начинот дозволува MAC подслојот да испрати кратка секвенца (наречена „брст“ - burst) од рамки еднакви на приближно 5.4% од максималната должина на рамките, без водење сметка за контрола на медиумот. MAC подслојот кој испраќа рамки, пополнува меѓурамка со битови за проширување како што е прикажано на сликата, така што другите станици на мрежата можат да видат дека мрежата е зафатена и нема да се обидат да вршат пренос сè додека брстот не заврши.

Табела 5.1: Ограничувања на „Half-Duplex“ функционирањето

Параметар	10 Mbps	100 Mbps	1000 Mbps
Најмала големина на рамка	64 бајти	64 бајти	520 бајти [1] (со додадено поле за проширување)
Најголем дијаметар на колизија DTE до DTE	100 метри UTP	100 метри UTP	100 метри UTP
		412 метри оптика	316 метри оптика
Најголем дијаметар на колизии со репетитори	2500 метри	205 метри	200 метри
Број на репетитори на мрежата	5	2	1

[1] 520 бајти за однесуваат на 1000Base-T имплементации. Минималната големина на рамка со полето за проширување за 1000Base-X е намалена на 416 бајти, затоа што 1000Base-X кодира и пренесува 10 бита за секој бајт.



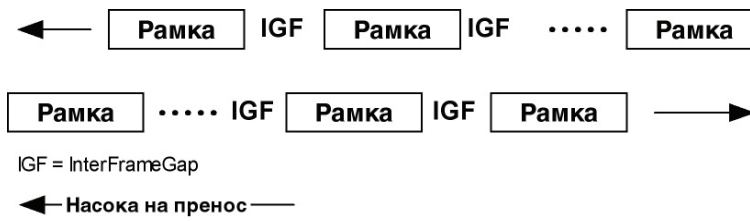
Слика 5.5: Burst секвенца кај гигабитска рамка

Ако должината на првата рамка е помала од најмалата дозволена должина, се додава полето за проширување за продолжување на рамката до вредноста означена во табелата. Последователните рамки во брст-секвенцата немаат полиња за проширување и брстот може да продолжи, сè додека не се достигне брст ограничувањето. Ако се достигне ограничувањето по започнување на преносот, дозволено е да продолжи трансмисијата сè додека не се испрати целата рамка.

Полињата за проширување на рамката не се дефинирани и брст начинот не е дозволен за брзини на пренос од 10 Mbps и 100 Mbps.

5.3.9 „Full-Duplex“ пренос за поголема ефикасност на мрежата

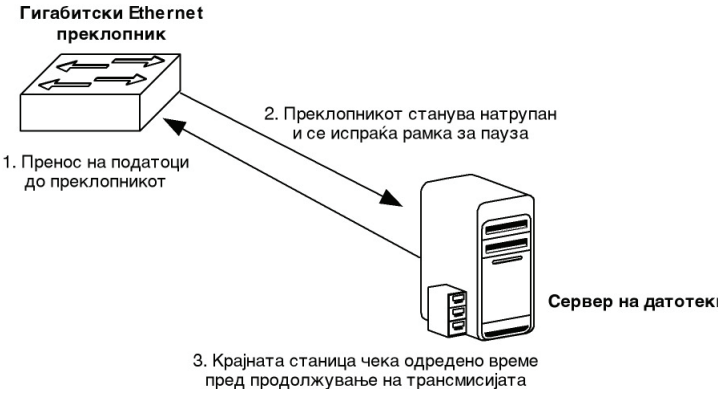
„Full-duplex“ методот е можност на MAC подслојот што дозволува симултано двонасочно пренесување преку врски точка-точка. „Full duplex“ трансмисијата е функционално поедноставна од „half-duplex“ начинот на пренесување зашто нема натпревар за медиумот, нема колизии ниту има потреба од битови за проширување на крајот од покусите рамки. Резултатот е не само зголемено време за трансмисии, туку и ефективно удвојување на преносниот опсег, бидејќи секој линк поддржува симултана двонасочна трансмисија со потполна брзина. Преносот може да започне штом рамките ќе бидат подготвени за испраќање. Единствено ограничување е што мора да постои минимален меѓурамковен простор (IGF) како што е прикажано на сликата и секоја рамка треба да подлегнува на стандардите за формат на Ethernet рамка.



Слика 5.6: „Full Duplex“ работата дозволува симултан двонасочен пренос на ист линк

5.3.10 Контрола на проток (Flow Control)

„Full-duplex“ начинот на работа, бара конкурентна имплементација на контрола на проток, која овозможува јазолот што прима (порта на мрежен преклопник) и станува натрупан, да му каже на јазолот што испраќа (како што е сервер на датотеки) да престане со испраќање на рамки за одреден краток временски период. Контролата се одвива на ниво MAC-MAC, преку користење на рамка за пауза, која автоматски се генерира од страна на MAC примачот. Ако натрупувањето се отстрани пред да измине бараниот период, може да се испрати и втора рамка за пауза со вредност на „time-to-wait“ еднаква на нула, за продолжување на трансмисијата. На сликата е даден приказ на операцијата за контрола на проток.



Слика 5.7: Приказ на секвенца на контрола на проток кај IEEE 802.3

„Full-duplex“ методот и контролата на проток се опции применети за сите Ethernet MAC подслоеви, за сите брзини на пренос. Двете опции се овозможени врз база на линк-линк, претпоставувајќи дека придружените физички нивоа се исто така способни за поддршка на „full-duplex“ работење.

Рамките за пауза се идентификувани како MAC контролни рамки преку доделување на резервирана вредност за полето должина/вид (length/type). Тие имаат и резервирана вредност за дестинацискатa адреса, преку која се обезбедува дека нема да поминат кон повисоките нивои на таа точка, или на другите порти на мрежниот преклопник.

5.3.11 Примање на рамката

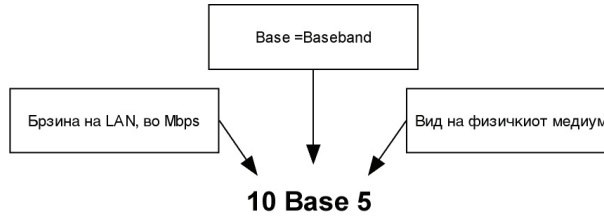
Примањето на рамката е во принцип исто и за двата режими на работа, освен што „full-duplex“ MAC подслојот треба да има одделени бафери (buffers) и патеки за податоци (data paths) за овозможување на симултано примопредавање на рамките.

Примањето на рамката е инверзна операција од испраќањето, дестинацискатa адреса по примањето се проверува и споредува со адресата на станицата (нејзината MAC адреса, групна адреса и „broadcast“ адресата),

за да се одреди дали рамката е наменета за оваа станица. Ако се совпадне некоја од адресите, се проверува должината на рамката, и применият FCS се споредува со FCS кој се пресметува при примањето на рамката. Ако должината на рамката е валидна и нема грешки при преносот, се одредува видот на рамката преку содржината на „должина/вид“ полето. Рамката конечно се парсира и проследува кон соодветното повисоко ниво.

5.3.12 Физички нивоа на Ethernet

Бидејќи Ethernet уредите ги имплементираат само двата најниски нивоа на OSI моделот, обично се имплементираат како мрежни адаптери, кои се идентификуваат преку ознака со која со опишуваат физичките атрибути: брзината на LAN-от, методот на сигнализација и видот на физичкиот медиум/кодирање на сигналот.



Слика 5.8: Ознака за физичкото ниво на Ethernet

На пример:

- 10Base-T = 10 Mbps, основен опсег (baseband), преку две плетени парици,
- 100Base-T2 = 100 Mbps, основен опсег (baseband), преку две плетени парици,
- 100Base-T4 = 100 Mbps, основен опсег, преку четири плетени парици,
- 1000Base-LX = 100 Mbps, основен опсег, долга бранова должина преку оптичко влакно.

Се поставува прашање зошто средната ознака секогаш е „основен опсег“ Base; поранешните верзии на протоколот исто така овозможувале пренос во широк опсег „broadband“ (на пример, 10Broad), но овие имплементации не се покажале квалитетни, и сите тековни верзии го користат преносот во основен опсег.

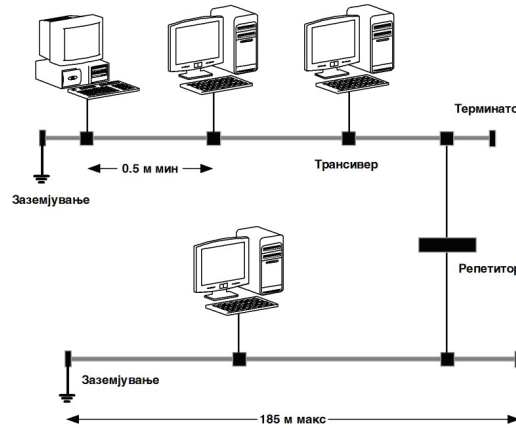
5.3.13 Имплементации на Ethernet и IEEE 802.3

Табела 5.2 Карактеритики на различни имплементации на Ethernet и IEEE 802.3

Карактеристики	Ethernet вредности	IEEE 802.3 вредности				
		10Base5	10Base2	10BaseT	10BaseFL	100BaseT
Брзина (Mbps)	10	10	10	10	10	100
Метода на сигнализација	Baseband	Baseband	Baseband	Baseband	Baseband	Baseband
Максимална должина на сегмент (m)	500	500	185	100	2000	100
Медиум	50-ohm коаксијален (дебел)	50-ohm коаксијален (дебел)	50-ohm коаксијален (тенок)	UTP кабел	оптика	UTP кабел
топологија	магистрала	Магистрала	Магистрала	Ѕвезда	Точка-точка	магистрала

10BASE2

10BASE2 топологијата на каблирање (Thinnet) користи примопредавател на мрежната картичка за преведување на сигналите, од и кон мрежата, со користење на BNC T-конектори кои директно се прикачени на адаптерот. Секој крај на кабелот треба да има терминатор на еден крај, а на другиот заземјен терминатор. Главната предност за користење на 10BASE2 е цената и во случаи кога нема потреба мрежниот сегмент да биде подолг од 185 метри, 10BASE2 е најевтината варијанта за поставување на локална мрежа.



Слика 5.9: 10BASE2 топологија на каблирање

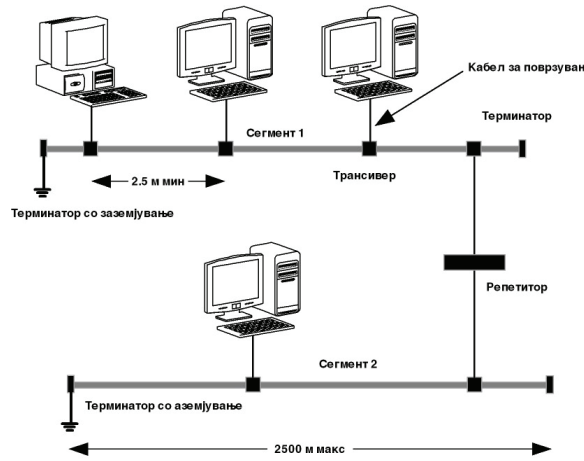
10BASE2 е исто така релативно лесна за поврзување. Секој од мрежните јазли се поврзува директно на мрежниот кабел со T-конектор.

За успешна инсталација, потребно е да се следат препораките:

- Најмалата дистанца помеѓу клиентите треба да биде 0.5 метри.
- Кратките кабли за поврзување (Pig tails, или уште познати како drop cables), не смеат да се користат за поврзување на BNC конекторот кон мрежниот адаптер; T-конекторот треба да е поврзан директно на мрежниот адаптер.
- Не смее да се надмине должината на мрежниот сегмент од 185 метри.
- Целата мрежа не смее да ја надмине должината од 925 метри.
- Максималниот број на јазли по сегмент е 30 (клиенти и репетитори).
- Треба да се користи 50 омски терминатор на секој крај од магистралата.
- Не може да има повеќе од 5 сегменти.

10BASE5

10BASE5 топологијата користи надворешен примопредавател прикачен на мрежната картичка. Надворешниот трансивер се прикачува на коаксијалниот кабел. Attachment Universal Interface (AUI) се поврзува од примопредавателот на DIX конектор кај мрежниот адаптер; како и во претходниот случај магистралата треба да се затвори со заземјени терминатори.



Слика 5.10: 10BASE5 топологија на каблирање

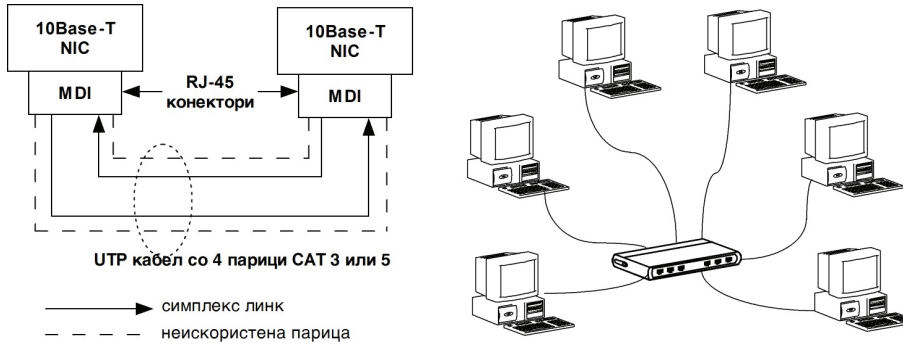
Главната предност на 10BASE5 е способноста да се надминат ограничувањата на кабелот кои се однесуваат на 10BASE2.

За правилно работење на мрежата, потребно е да се следат препораките:

- Најмалото растојание помеѓу примопредавателите е 2.5 метри.
- Најдолгиот мрежен сегмент не треба да надмине должина од 500 метри.
- Целата мрежа не смее да биде подолга од 2,500 метри.
- Едниот крај од терминираната мрежа треба да биде заземјен.
- Каблите за поврзување не можат да бидат подолги од 50 метри од примопредавателот до компјутерот.
- Најголемиот број на јазли по сегмент изнесува 100.

10-Mbps Ethernet - 10Base-T

10Base-T обезбедува Manchester кодирана 10-Mbps бит-сериска комуникација преку две неоклопени плетени парици. Иако стандардот е дизајниран за поддршка на пренос преку обичен телефонски кабел, обично се користат две или четири парици од кабелот Category 3 или 5, терминиран на секој мрежен адаптер со 8-пински RJ-45 конектор (MDI), како што е прикажано на сликата. Бидејќи секој активен пар е конфигуриран како симплекс линк (еднонасочна комуникација), физичките нивоа на 10Base-T можат да поддржат или „half-duplex“ или „full-duplex“ работење.



Слика 5.11: 10Base-T линк составен од 4 паричен UTP кабел каде што 2 парици не се користат и поврзувањето на мрежата со концентратор

Иако 10Base-T може да се смета како застарен, сè уште постојат мрежи кои користат 10Base-T Ethernet и заради можноста за „full-duplex“ режимот на работа. Исто така оваа спецификација е прва која користела проверка на интегритетот на линкот.

Веднаш по стартувањето се емитува импулс за нормален линк (normal link pulse NLP), за да му се покаже на мрежниот адаптер на другата страна дека тој адаптер сака да воспостави активно поврзување:

- Адаптерот на другата страна, ако е вклучен, одговара со својот NLP.
- Ако адаптерот NIC на другата страна не е вклучен, овој продолжува да испраќа NLP на секои 16 ms, сè додека не прими одговор.

Поврзувањето се активира само ако и двата мрежни адаптери се способни за размена на валидни NLP импулси.

10BASE-FL

10BASE-FL е спецификација за Ethernet преку оптички влакна. Името 10BASE-FL означува брзина од 10Mbps со користење на основен опсег.

Предностите на кабелот со оптички влакна се претходно објаснети (поглавје 3). Најбитната предност е во најголемата должината на кабелот од 1 километар, и отстранување на било каква појава на EMI, како и бројот на јазли кои можат да се постават на еден мрежен сегмент (далеку поголем од 10BASE-T, 10BASE2, и 10BASE5).

100 Mbps – Брз Ethernet

Зголемувањето на брзината на пренос за фактор 10 во однос на 10Base-T не е едноставна задача и развојот довел до појава на 3 различни стандарди на физичките слоеви за 100 Mbps преку UTP кабел: 100Base-TX и 100Base-T4 во 1995, и 100Base-T2 во 1997. Секој се дефинира со различни начини на кодирање и различни медиумско-зависни подслоеви.

Табела 5.3: Физички карактеристики на физичкото ниво на 100Base-T.

Верзија на Ethernet	Брзина на пренесување на симболи[1]	Кодирање	Каблирање	Full-Duplex работење
10Base-T	10 MBd	Manchester	2 парици од UTP Category -3 или подобар	Поддржана
100Base-TX	125 MBd	4B/5B	2 парици од UTP Category -5 или Тип1 STP	Поддржана
100Base-T4	33 MBd	8B/6T	4 парици од UTP Category -3 или подобар	Не е поддржана
100Base-T2	25 MBd	PAM5x5	2 парици од UTP Category -3 или подобар	Поддржана

[1] 1 baud = еден пренесен симбол во единица време и може да биде еквивалент еден или повеќе битови

100Base-X

100Base-X е дизајниран за поддршка на пренос преку две парици од Category 5 UTP бакарна жица, или две оптички влакна. Иако кодирањето, декодирањето и процедурите за синхронизација на интерниот часовник се исти за двата медиуми, начинот на пренесување на сигналот е различен - електрични импулси во бакарот и светлосни импулси во оптичкото влакно. Примопредавателите кои се вклучени во PMA функцијата во генеричкиот логички модел се редефинирани како посебни, физичко зависни подслоеви (physical media-dependent PMD).

100Base-X процедурата за кодирање се базира на поранешните стандарди за сигнализација, користени во FDDI со оптика и FDDI/CDDI со бакарни парици, развиени од ISO и ANSI.

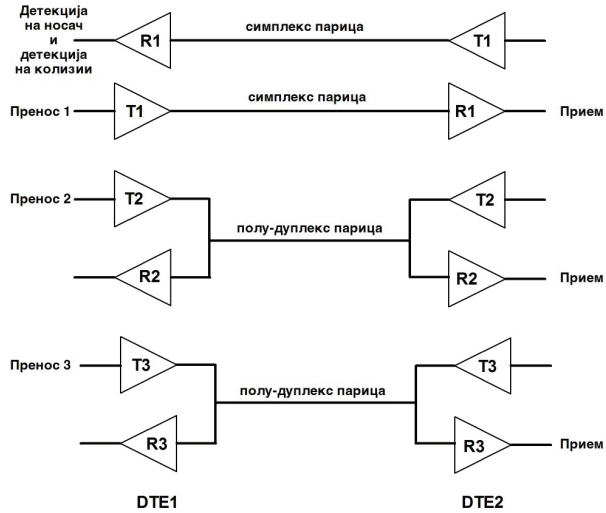
100Base-TX медиум-зависното подниво се имплемтира преку CDDI полупроводнички примопредаватели и RJ-45 конектори; оптичкото PMD се имплементира со FDDI оптички примопредаватели „duplex“ SC конектори.

Процедурата за кодирање 4B/5B е истата користена и од FDDI, само со мали измени за прилагодување кон контролата на рамките во Ethernet мрежи.

100Base-TX предава и прима преку истите парици и користи иста распределба на пиновите на MDI како и 10Base-T. 100Base-TX и 100Base-FX поддржуваат и „half-duplex“ и „full-duplex“ трансмисија.

100Base-T4

100Base-T4 е развиен да им овозможи на мрежите со 10BaseT да бидат надградени во 100-Mbps режим, без замена на четири-паричните кабли со ознака Category 3 UTP, со поновите кабли со Cat 5.



Слика 5.12: 100Base-T4 користење на париците при пренесување на рамките

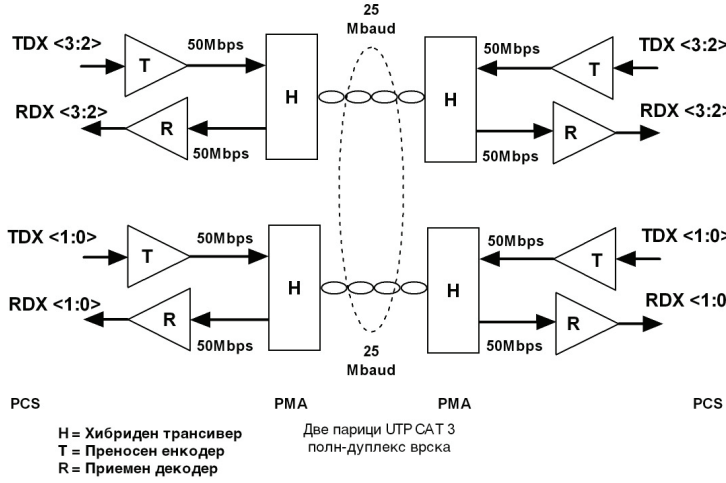
Двете од четирите парици се конфигурирани за „half-duplex“ работа и може да поддржат пренос во двете насоки, но само во една во даден момент. Другите две парици се конфигурирани како симплекс парици посветени за трансмисија само во една насока. Пренесувањето на рамките ги користи и двете „half-duplex“ парици, заедно со симплекс парот кој е соодветен за насоката, како што е прикажано на сликата. Симплекс парицата за спротивната насока обезбедува детекција на носачот и колизиите. На може да се оствари „full-duplex“ работа на мрежите со 100Base-T4.

100Base-T2

Спецификацијата на 100Base-T2 е развиена како подобра алтернатива од 100Base-T4 за надградба на мрежите со инсталација од категорија 3.

Дефинирани се две цели:

- Обезбедување на комуникација преку две парици од категорија 3 или подобар кабел,
- Поддршка и на „half-duplex“ и на „full-duplex“ режим на работа.



Слика 5.13: Топологија на 100Base-T2 линкот

100Base-T2 користи различна процедура за испраќање на сигналот во однос на поранешните Ethernet имплементации кои користат плетена парица. Наместо користење на два симплекс линка за формирање на еден „full-duplex“ линк, 100Base-T2 методата за пренос, во основен опсег со двоен дуплекс испраќа кодирани симболи симултано во двете насоки кај двете парици, како што е прикажано на сликата.

Името "TDX<3:2>" ги означува 2-та најзначајни бита во нибл (4-те бита), пред кодирањето и трансмисијата. "RDX<3:2>" ги означува истите два бита по примањето и декодирањето.

„Dual-duplex“ трансмисијата во основен опсег, бара и двата мрежни адаптери на краевите од линкот да работат во „master/slave“ начин. Кој адаптер ќе биде мастер, а кој ќе биде „slave“ е одредено при договарањето при воспоставувањето на линкот.

Кога линкот ќе стане оперативен, синхронизацијата ќе се остварува врз основа на интерниот часовник на мастер-мрежниот адаптер. Адаптерот „slave“ го користи добиениот такт за примопредавање. Секоја испратена рамка се енкапсулира и синхронизацијата се одржува со континуирана низа на симболи во меѓу -рамковните празнини.

Процесот на 100Base-T2 кодирање прво ги преместува нибл (4 бита) во рамката и ги мапира двата повисоки битови и двата пониски бита за секој нибл, во два импулса со пет можни нивоа (+2, +1, 0, -1, -2), односно импулсно-амплитудно модулацирани (Pulse Amplitude-Modulated - PAM5) симболи, кои истовремено се пренесуваат преку два пара на жици (PAM5x5).

Приемот на сигналот е инверзна операција од преносот на сигналот, и, бидејќи сигналот на секоја парица на MDI е сума на пренесениот сигнал и применият, секој приемник го одзема пренесениот симбол, за наоѓање на симболите во дојдовната податочна низа. Дојдовниот пар на симболи се декодира, подредува и воспоставува како податочен нибл за пренесување кон MAC.

1000 Mbps – Гигабитски Ethernet (Gigabit Ethernet)

Стандардите за гигабитски Ethernet се развиле во две примарни спецификации: 1000Base-T за UTP бакарен кабел и 1000Base-X за STP бакарен кабел, како и за единечно и мултимодно оптичко влакно.

1000Base-T

1000Base-T Ethernet обезбедува „full-duplex“ трансмисија преку 4-паричен UTP кабел од Категорија 5 или подобар. 1000Base-T се базира врз истражувањата и пристапот за дизајнирање кој довел до имплементација на физичкото ниво на брзиот Ethernet:

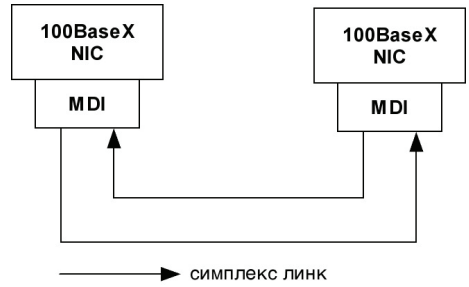
- Со 100Base-TX е докажано дека низата на бинарни симболи може успешно да се пренесува преку Category 5 UTP кабел - до 125 MBd.
- 100Base-T4 обезбедува разбирање на проблемите поврзани со испраќање на повеќе-нивоовски сигнали преку 4-жични парици.
- 100Base-T2 покажува дека PAM5 кодирањето, заедно со дигиталното процесирање на сигнали, може да се справи со симултаните двонасочни податочни стримови и со потенцијалните проблеми со преслушување, кои се резултат на надворешни сигнали од соседните парици.

Синхронизацијата на часовник и „master/slave loop timing“ процедурите се истите што се користат кај 100Base-T2. Кој мрежен адаптер ќе биде „master“

(обично адаптерот во повеќепортниот мрежен јазол), а кој ќе биде „slave“ се одредува при процесот на преговарање. 1000Base-T ги поддржува и „half-duplex“ и „full-duplex“ режимот на работа.

1000Base-X

Сите три 1000Base-X верзии поддржуваат „full-duplex“ бинарен пренос, со брзина од 1250 Mbps преку две оптички влакна, или две STP бакарни парици како што е прикажано на сликата. Преносното кодирање се базира врз ANSI Fibre Channel 8B/10B шемата, каде што секои 8 бита се мапираат во 10-битна кодна група за бит-сериски пренос. Како и постарите верзии на Ethernet, секоја податочна рамка се енкапсулира на физичко ниво пред испраќање, а синхронизацијата на линкот се одржува преку континуирана низа на „IDLE“ кодни групи – симболи, при појава на празнини. Сите физички нивоа на 1000Base-X поддржуваат и „half-duplex“ и „full-duplex“ режим на работа.



Слика 5.14: Линк конфигурација на 1000Base-X

Основната разлика помеѓу 1000Base-X верзиите се медиумот за поврзување и конекторите; во овој случај тоа се оптичките влакна и брановата должина на светлосниот сигнал.

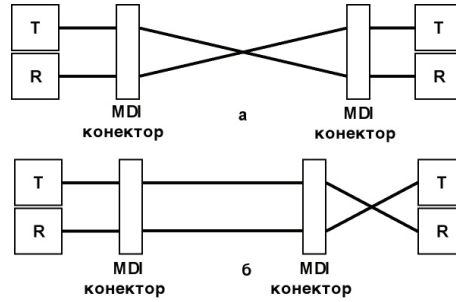
Табела 5.5: 1000Base-X поддршка на конфигурацијата на линкот

Конфигурацијата на линкот	1000Base-CX	1000Base-SX (850 nm бранова должина)	1000Base-LX (1300 nm бранова должина)
150 W STP бакар	Поддржан	Не е поддржан	Не е поддржан
125/62.5 mm multimode оптика	Не е поддржан	Поддржан	Поддржан
125/50 mm multimode оптика	Не е поддржан	Поддржан	Поддржан
125/10 mm single mode оптика	Не е поддржан	Не е поддржан	Поддржан
Дозволени конектори	IEC style 1 или Fibre Channel style 2	SFF MT-RJ или Duplex SC	SFF MT-RJ или Duplex SC

5.3.14 Мрежни кабли - Link Crossover

Компатибилноста на линковите бара секој предавател на секој крај од линкот да биде поврзан со својот примач. Бидејќи конекторите на каблите на двата краја на линкот се означени како исти, проводникот треба да се вкрсти во некоја точка, за да се обезбеди излезите секогаш да се поврзуваат со влезовите на адаптерот.

При развојот на 10Base-T, во IEEE 802.3 стандардот не е стриктно посочено дали вкрстувањето да се изведе на кабелот или интерно, како што прикажано на сликата.



Слика 5.15: Алтернативни начини за изведба на вкрстувањето на линкот

Стандардот IEEE 802.3 дефинира две правила и две препораки:

- Мора да постои непарен број на вкрстувања во сите проводнички линкови.
- Ако PMD уредот е опремен со интерно вкрстување, неговиот MDI мора јасно да биде означен со графички симбол X.
- Изведбата на интерното вкрстување е опционо.
- Кога DTE уред се поврзува со порт на репетитор или преклопник (DCE), се препорачува вкрстувањето да биде во склоп на DCE портот.

Резултатот е дека портовите во повеќето DCE уреди се опремени со PMD кои содржат интерно вкрстено коло, и дека DTE имаат PMD-ови без внатрешно вкрстување. Ова доведува до правило за инсталација:

- За DTE со DCE приклучување да се користи „исправен кабел“ (straight-through).
- Вкрстен кабел се користи за поврзување на DTE со DTE, или DCE со DCE.

Правилото не се однесува на сите верзии на Ethernet кои биле развиени од 10Base-T. Сега важат овие препораки:

- Сите оптички системи користат кабли кои имаат изведено вкрстување преку кабел.
- Сите 100Base системи со вкрстена парица користат исти правила и препораки како 10Base-T.

- 1000Base-T мрежните адаптери може да имплементираат селективна опција за вкрстување која се нагодува при процесот на автоконфигурација (autonegotiation). Ако нема селектибилна опција, се применува правилото за 10Base-T.

5.3.15 Повисоки брзини на пренос во CSMA/CD мрежи со мрежни преклопници

Со користење на преклопници наместо повеќепортни репетитори (hab), се постигнува подобар ефект во работењето на мрежата, затоа што преклопниците ги имаат следниве својства:

- MAC - базирани портови со В/И бафери за рамките кои ефективно го изолираат портот од сообраќајот кој истовремено се испраќа кон, или од другите портови;
- Повеќекратни внатрешни податочни патеки (data paths) кои овозможуваат испраќање на неколку рамки помеѓу различните портови во исто време.

Иако изгледаат како мали разлики, имаат значително влијание врз мрежата, затоа што секој порт обезбедува пристап кон мрежниот мост со голема брзина (всушност тоа е преклопникот), а доменот на колизии во мрежата се намалува со низа од мали домени, каде што бројот на јазлите е намален за два – портот на преклопникот и на него поврзаниот мрежен адаптер. Уште повеќе, бидејќи секој учесник е нов приватен домен на колизии, достапниот пропусен опсег не само што е ефективно зголемен, туку е постигнат без менување на брзината на линкот.

На пример, на 100-Mbps CSMA/CD мрежа постои работна група од 48 јазли со неколку поголеми сервери на датотеки и неколку мрежни печатари. Просечниот достапен мрежен пропусен опсег без да се земат во предвид меѓурамковните празнини или опоравувањето од колизиите, би изнесувал 100/50 = 2 Mbps (мрежните печатари не произведуваат сообраќај). Од друга страна, ако истата група е поврзана на мрежа со 10Base-T, каде што репетиторите се заменети со мрежни преклопници, достапниот опсег за секој корисник би бил 10 Mbps. Следува заклучок дека и конфигурацијата на мрежата е исто така значајна како и брзината на линковите.

5.4 TOKEN RING/IEEE 802.5

Token Ring мрежата оригинално е развиена од страна на IBM во 1970-те години. Сè уште е примарна LAN технологија користена од IBM. IEEE 802.5 спецификацијата е скоро идентична и потполно компатибилна со IBM-овата Token Ring мрежа. Во принцип IEEE 802.5 спецификацијата е направена според IBM Token Ring мрежата, и го следи нејзиниот развој. Поимот Token Ring се однесува и на двете спецификации: IBM-овата Token Ring мрежа и IEEE 802.5 мрежите.

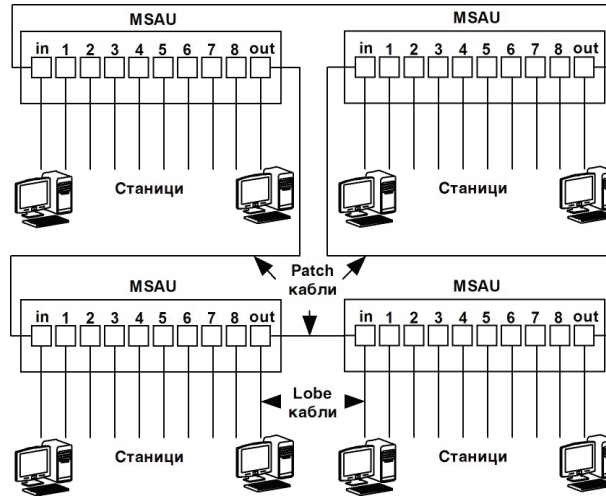
Табела 5.7: Споредба на карактеристиките на IBM Token Ring и IEEE 802.5

Карактеристика	IBM Token Ring network	IEEE 802.5 network
Брзина на пренос	4 или16 Mbps	4 или 16 Mbps
Јазли по сегмент	260 (STP), 72 (UTP)	250
Топологија	Ѕвезда	Не е одредено
Медиум	Плетена парица	Не е одредено
Сигнализација	Основен опсег	Основен опсег
Метод на пристап	Додавање на токени	Додавање на токени
Кодирање	Диференцијален Manchester	Диференцијален Manchester

Token Ring и IEEE 802.5 мрежите се во основа меѓусебно компатибилни, иако имаат некои ситни разлики. IBM-овиот Token Ring дефинира топологија на ѕвезда каде што сите јазли во мрежата се поврзуваат со т.н. уред за пристап кон повеќе јазли (Multistation Access Unit MSAU). Обратно, IEEE 802.5 не ја специфицира топологијата, иако виртуелно сите изведби на IEEE 802.5 се засновани на ѕвездеста топологија. Во табелата е даден преглед на спецификациите на IBM Token Ring и IEEE 802.5.

5.4.1 Физички врски

IBM Token Ring мрежните станици директно се поврзуваат на MSAU уредите, кои можат меѓусебно да се поврзуваат и да формираат еден голем прстен (слика 5.16). „Patch“ каблите ги поврзуваат соседните MSAU, додека со „lobe“ кабли се поврзуваат MSAU со станиците. Во MSAU уредите постојат релеи за премостување на станиците и нивно отстранување од мрежата.



Слика 5.16: Поврзување на MSAU за создавање на поголем прстен

5.4.2 Каблирање кај Token Ring

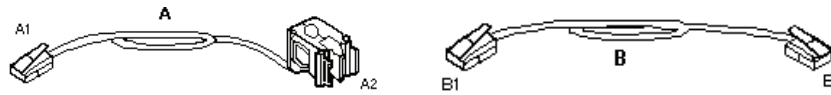
Традиционалните token-ring мрежи користат плетена парица, и стандардните видови на кабли за IBM Token Ring се:

- Тип 1 - жичена обвивка околу две плетени парици од полн бакар - се користи за поврзување на терминалите и дистрибуциските панели, или за поврзување на различни ормари за ожичување кои се наоѓаат во иста зграда. Максималното растојание за поставување на кабелот е 100 метри.
- Тип 2 користи вкупно 6 плетени парици, од кои две се STP (за умрежување) и четири се UTP (за телефонски системи). Овој кабел се користи за иста намена како и Тип 1, но овозможува и телефонските сигнали и податоците да бидат во една целина. Максималната должина изнесува 100 метри.
- Тип 3 се користи како алтернатива на тип 1 и тип 2 заради намалените трошоци. Тип 3 има неоклопена плетена парица со најмалку 2 вплетувања по инч. Тип 3 не може да се користи кај 16Mbps Token-Ring мрежите. Максималното растојание (според IBM) е 45 метри, иако некои вендори дефинираат и растојанија до 150 метри.

Каблирањето од Тип 3 (UTP) е најкористениот медиум за Token Ring мрежите, а со користење на овој тип може да се опслужат 72 компјутери. Token-Ring мрежата со користење на STP каблирање може да поддржи до 260 компјутери, како што е наведено во табелата. Минималното растојание помеѓу компјутерите или MSAU уредите е 2.5 метри.

„Patch“ кабелот служи за поврзување на MSAU уредите. Овие кабли обично се IBM Тип 6 кабли кои доаѓаат со стандардна должина. Тие можат да се користат за продолжување на каблите од тип 3, или за поврзување на компјутерите со MSAU; тие имаат IBM конектор на секој крај.

Token-Ring адаптер–каблите имаат IBM конектор на едниот крај и девет-пински конектор на другиот крај, а можат да користат и UTP кабли со RJ-45 конектори на секој крај. Адаптер каблите ги поврзуваат мрежните адаптери на клиентите и серверите со други мрежни компоненти кои користат IBM податочни конектори. Видот на конекторот кој е потребен за Token-Ring мрежата зависи од типот на кабелот кој се користи. Каблите од тип 3 користат RJ-11 или RJ-45 конектори (слика 5.17б). Тип 1 и 2 користат IBM Type A конектори (слика 5.17а).



Слика 5.17. а) RJ-11 со RJ-45, б) IBM Type A конектори

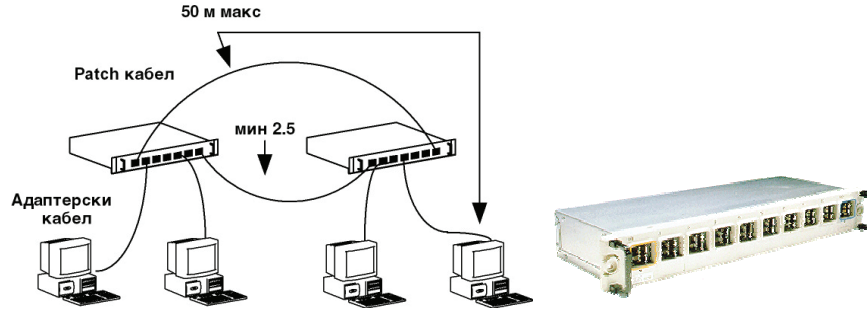
Token-Ring мрежите може да се најдат во неколку големини и дизајни. Малиот подвижен Token Ring систем (small movable) поддржува до 12

MSAU уреди и користи кабли од тип 6 за поврзување на клиентите и серверите кон IBM Model 8228 MSAU. Тип 6 е флексибилен - има ограничено растојание и е погоден за помали мрежи или „patch“ кабли.

Големиот неподвижен Token Ring (large nonmovable) поддржува до 260 клиенти и сервери на датотеки, со максимум до 33 MSAU уреди. Оваа мрежна конфигурација користи IBM тип 1 или тип 2 кабли. Системот кој е голем и неподвижен бара и дополнителна опрема за ожичување како што се „punch“ панели и дистрибуциски панели, рекови за опрема за MSAU, и ормари за ожичување.

MSAU уредот е централната компонента во IBM Token-Ring мрежите. Типот 8228 MSAU е оригиналниот концентратор развиен од IBM за нивните IBM Token-Ring мрежи. На сликата 5.18 се прикажани 8228 MSAU уреди. Секој 8228 има 10 конектори, осум кои се способни за поврзување на клиенти, а другите се одбележени со RI (ring in) и RO (ring out). RI и RO конекторите служат за поврзување на повеќе 8228-ци за формирање на поголема мрежа, при што последниот RO мора да се поврзе со RI на првиот MSAU во прстенот.

8228-ците се механички уреди кои се состојат од релеи и конектори. Нивната намена е да ги приклучуваат и исклучуваат клиентите во мрежата. Секој порт е контролиран од страна на релеј напојуван со електрична енергија која се испраќа кон MSAU од клиентот. Кога се поставува 8228, секој од овие релеи треба да биде иницијализиран со одредена алатка која се испорачува со уредот. Алатот се вметнува во секој порт и се држи сè додека не се појави светлосен индикатор дека портот правилно се иницијализирал.



Слика 5.18: Поврзување на MSAU уреди во Token Ring мрежа

5.4.3 Работа на Token Ring

Token Ring и IEEE 802.5 се два примери на мрежи кои користат додавање на токени (покрај FDDI). Мрежите со додавање на токени работат преку движење на мала рамка наречена токен по мрежата. Поседувањето на токенот гарантира право на пренесување, а ако јазолот прими токен, а нема информации за пренесување - едноставно го предава на следната станица. Секоја станица може го задржи токенот одреден временски период.

Ако станицата која го поседува токенот има информација за испраќање, го зема и менува 1 бит во токенот (со што го претвора во секвенца „start-of-frame“), ја додава информацијата за пренесување и ја испраќа до следната станица во прстенот. Додека податочната рамка кружи по прстенот, не постои токен, што значи дека другите станици треба да чекаат за пренесување. Оттука во Token ring мрежите не може да дојде до појава на колизии. Ако е поддржан механизмот за предвремено ослободување на токенот, кога ќе се заврши пренесувањето се генерира нов токен, пред да го ослободи предавателот.

Информацијата кружи по прстенот, сè додека не ја достигне саканата дестинација која потоа ја копира информацијата за понатамошно процесирање. Податочната рамка продолжува да кружи по прстенот, сè додека не се отстрани по пристигнувањето кај изворниот јазол, при што се проверува дали рамката пристигнала до дестинацијата и била прочитана.

За разлика од CSMA/CD мрежите (како што е Ethernet), мрежите со токени се детерминистички, што значи дека може да се пресмета максималното време кое ќе измине пред крајната станица да стане способна да пренесува. Оваа карактеристика, како и способноста за толеранција на испади, ги чинат Token Ring мрежите идеални за апликации кај кои доцнењето треба да биде предвидливо; со тоа е зголемена робустноста на мрежата.

5.4.4 Систем за приоритет (Priority System)

Token Ring мрежите користат софистициран систем за приоритет кој дозволува одредени станици со повисок приоритет да ја користат мрежата почесто. Token Ring рамките имаат две полиња кои управуваат со приоритетите: поле за приоритет и поле за резервација.

Само станиците со приоритет еднаков или поголем од вредноста на полето во токенот може го превземаат. По преземањето на токенот и измената на податочната рамка, само станиците со поголем приоритет од станицата која емитува може да го резервираат токенот за следно поминување околу мрежата. Кога се генерира следниот токен, тој го вклучува приоритетот на станицата која извршила резервација. Станиците кои го подигнуваат нивото на приоритет треба да ја вратат претходната состојба по завршување на преносот.

5.4.5 Механизми за управување со испади (Fault-Management Mechanisms)

Token Ring мрежите користат неколку механизми за детекција и надминување на испади на мрежата. На пример, една станица во мрежата се избира да биде активен набљудувач (active monitor). Оваа станица може да биде било која на прстенот и врши различни функции за синхронизација и одржување на прстенот.

Една од овие функции е отстранување на рамките кои континуирано кружат по прстенот. Кога станицата која врши пренос на рамки испадне од мрежата, токенот може да продолжи да циркулира по прстенот. Тоа може да ги спречи другите станици да пренесуваат нивни сопствени рамки и ефективно да доведе до застој во мрежата. Активниот набљудувач ги детектира таквите рамки и ги отстранува од прстенот, а потоа поставува нов токен.

Ѕвездестата топологија на IBM Token Ring мрежите, придонесува за доверливоста на мрежата. Бидејќи сите информации во Token Ring мрежите се гледаат од активните MSAU уреди, тие можат да бидат програмирани за проверка на проблеми и селективно да ги отстрануваат јазлите од прстенот, ако постои потреба за тоа. Алгоритамот наречен „beaconing“ детектира и се обидува да поправи одредени мрежни испади. Секојпат кога станицата детектира сериозен проблем со мрежата (како што е на пример прекин на кабелот) врши испраќање на „beacon“ рамка со која се дефинира доменот на испадот. Овој домен ги вклучува станицата која испраќа известување, најблискиот активен следен сосед (nearest active upstream neighbor NAUN), и сѐ што се наоѓа помеѓу нив.

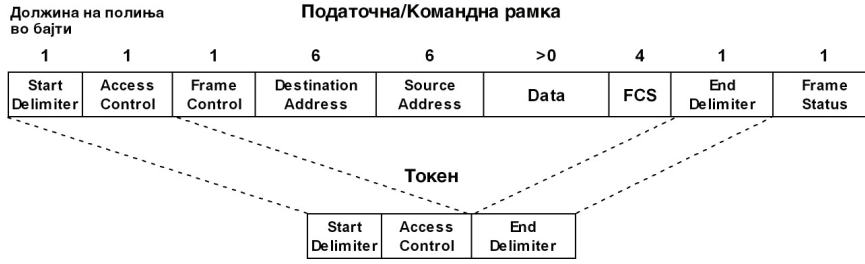
Процесот на „Beaconing“ иницира процедура наречена автоконфигурација, каде што јазлите во доменот на испадот автоматски изведуваат дијагностика и се обидуваат да ја реконфигурираат мрежата околу зоната на испадот. Физички - тоа се изведува во MSAU уредот преку електрична реконфигурација.

5.4.6 Формат на рамка (Frame Format)

Token Ring и IEEE 802.5 поддржуваат два вида на рамки: токени и податочни/контролни рамки.

Токени (Tokens) - токените се со должина 3 бајти и се состојат од стартен делимитер, бајт за контрола на пристап и завршен делимитер.

Податочни/контролни рамки (Data/command frames) - Data/command рамките можат да имаат различна должина, зависно од големината на информациското поле. Податочните (Data) рамки носат информации за протоколите од повисоките нивоа. Командните (Command) рамки содржат контролни информации и немаат податоци за повисоките нивоа.



Слика 5.19: IEEE 802.5 и Token Ring формат на рамките

5.4.7 Полиња на токен рамката (Token Frame Fields)

- Start Delimiter – служи да го најави доаѓањето на рамката (токен или контролна/податочна). Ова поле содржи сигнали со кои бајтот се разликува од остатокот на рамката, со прекршување на шемата на кодирање во остатокот од рамката.
- Access Control Byte – го содржи полето за приоритет (најзначајните 3 бита) и полето за резервација (најнезначајните 3 бита), како и token бит (за да се разликува од data/command рамката) и monitor бит (користен од активниот монитор за одредување дали рамката кружи низ прстенот бесконечно време).
- End Delimiter – го одбележува крајот на рамката (токенот или data/command). Ова поле исто така содржи битови за индикација на оштетена рамка и дали рамката е последна во логичката секвенца.

5.4.8 Полиња на податочно-командна рамка

Податочните/командни рамки ги имаат истите три полиња како и токен рамката (Start Delimiter, Access Control Byte и End Delimiter), со додаток на неколку други полиња:

- Frame Control Bytes – покажува дали рамката содржи податоци или контролни информации. Во контролните рамки овој бајт го одредува видот на контролната информација.
- Destination и Source Address - две 6-бајтни адресни полиња со кои се идентификува изворот и одредиштето.
- Data – должината на полето е ограничена со времето на задржување на токенот во прстенот, со кое се дефинира максималното време кое станицата може да го задржи токенот.
- Frame Check Sequence (FCS) – поле кое се пополнува од изворот со пресметани вредности, зависно од содржината на рамката. Одредиштето ја пресметува одново и одредува дали рамката е оштетена во преносот и по потреба ја отфрла.
- Frame Status – 1-бајтно поле со кое се завршува command/data рамката, и вклучува индикатор за препознаена адреса и копирана рамка.

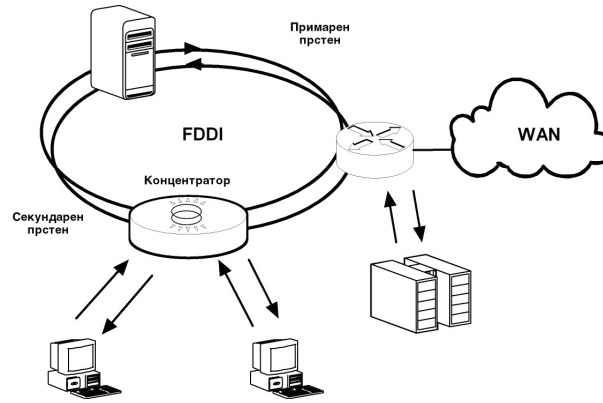
5.5 Оптички дистрибуиран податочен интерфејс (Fiber Distributed Data Interface)

Fiber Distributed Data Interface (FDDI) специфицира 100-Mbps token-passing, dual-ring LAN кој користи оптички кабел (fiber-optic). FDDI обично се користи како „high-speed backbone“ технологија, затоа што поддржува висок пропусен опсег и поголеми дистанци од бакарот (UTP, STP). Треба да се забележи дека релативно подоцна се појавила спецификацијата која поддржува 100-Mbps брзина преку бакарни жици, наречена бакарен

дистрибуиран податочен интерфејс (Copper Distributed Data Interface CDDI), и е имплементирана кај FDDI протоколите преку плетена парица.

Кога брзите работни станици започнале сè повеќе да го заземаат пропусниот опсег на постоечките локални мрежи базирани на Ethernet и Token Ring, се појавила потреба од нов вид на LAN-медиум за поддршка на тие работни станици и новите дистрибуирани апликации. Во исто време, доверливоста на мрежата станала подеднакво значајна кога администраторите ги мигрирале критичните апликации од големите компјутери кон компјутерските мрежи, па FDDI е развиен со цел да ги задоволи овие потреби.

FDDI користи dual-ring архитектура со сообраќај кој тече во спротивни насоки во секој прстен (counter-rotating). Двојните прстени се состојат од примарен и секундарен прстен. При нормална работа, примарниот ринг се користи за пренос на податоците, а секундарниот останува неискористен (idle). Намената на двојните прстени е да се обезбеди супериорна доверливост и робустност. На сликата се прикажани примарен и секундарен прстен со спротивни насоки на циркулација.



Слика 5.20: FDDI користи примарен и секундарен прстен со спротивни насоки на кружењето на сообраќајот

5.5.1 Преносен медиум во FDDI

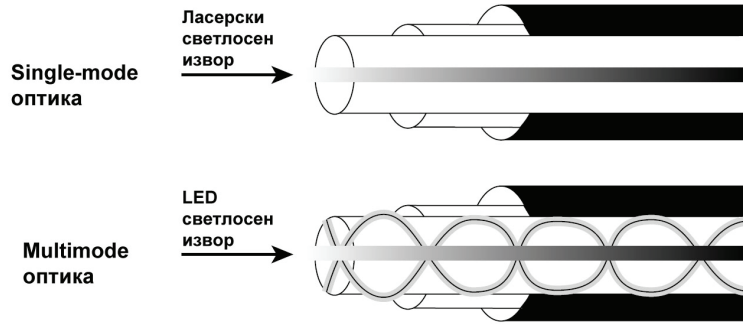
FDDI користи оптика како примарен преносен медиум, но може да користи и бакарно ожичување. FDDI преку бакар се нарекува Copper Distributed Data Interface (CDDI). Предноста на користењето на оптичките влакна во однос на бакарното ожичување се состои од:

- Безбедност (Security) – оптиката не емитира електрични сигнали.
- Сигурност (Reliability) – оптиката е имуна на радио и електромагнетна интерференција.
- Брзина (Speed) – оптиката овозможува поголема брзина на пренос од бакарното ожичување, иако сега и бакарот може да пренесува преку 100 Mbps.

- Поголеми растојанија за пренос - FDDI овозможува растојание од 2 km помеѓу станиците со користење на multimode оптика, и поголеми со користење на single mode оптички влакна.

FDDI дефинира два вида на оптички влакна: „single-mode“ и „multimode“. Поимот „mode“ означува светлосен зрак кој влегува во влакното под одреден агол. Multimode оптиката користи LED диоди како извор на светло, додека „single-mode“ користи ласер за таа намена. „Single-mode“ оптиката дозволува само еден мод на светлина да пропагира низ влакното, додека „multimode“ оптиката дозволува пропагација на повеќе светлосни модови. Бидејќи овие модови влегуваат во влакното под различни агли, ќе пристигнуваат на крајот на влакното во различни времиња. Ова карактеристика се нарекува модална дисперзија и таа го ограничува пропусниот опсег и оддалеченоста кои можат да се постигнат со користење на „multimode“ влакна. Заради тоа, овој тип на влакна се користи за поврзување во згради и поблиски географски локации.

„Single-mode“ влакното дозволува пропагација на еден светлосен мод и тука нема појава на модална дисперзија. Затоа, „single-mode“ оптиката е способна за постигнување на значително поголеми перформанси преку поголеми растојанија и обично се користи за поврзување помеѓу згради и поголеми географски растојанија.



Слика 5.21: Извори на светлина за „Single-Mode“ и „Multimode“ оптика

5.5.2 Спецификации на FDDI

FDDI ги специфицира физичкиот дел и делот за пристап кон медиумот од OSI референтниот модел. FDDI не е единична спецификација, туку е множество од четири засебни спецификации, секоја со одредена функција. Комбинирани овие спецификации обезбедуваат поврзување со голема брзина помеѓу протоколите од повисоките нивоа, како што се TCP/IP и IPX, и медиумот како што е каблирање со оптички влакна.

Четирите спецификации на FDDI се: контрола за пристап кон медиумот (Media Access Control MAC), протокол на физичкото ниво (Physical Layer Protocol PHY), физичко-зависен медиум (Physical-Medium Dependent PMD), и управување со станици (Station Management SMT).

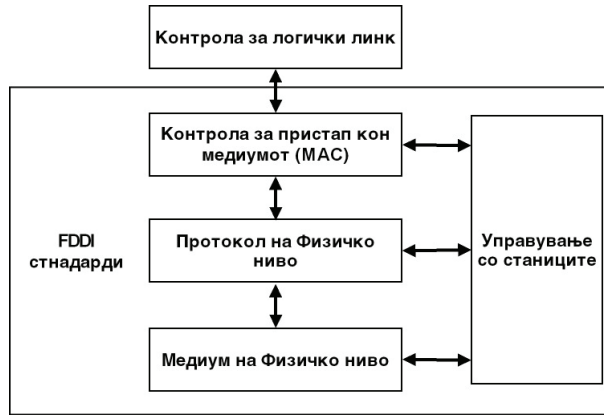
MAC спецификацијата дефинира како се пристапува кон медиумот, форматот на рамката, управување со токените, адресирањето, CRC, и механизмите за опоравување.

PHY спецификацијата ги дефинира процедурите за кодирање и декодирање, врамувањето и други функции.

PMD спецификацијата ги дефинира карактеристиките на преносниот медиум, оптичкиот линк, напонските нивоа, BER, оптичките компоненти и конекторите.

SMT спецификацијата ги дефинира FDDI конфигурацијата на станиците, на прстенот и контролата врз прстенот, вклучувајќи вметнување и исклучување на станиците, иницијализацијата, изолацијата на испадите, итн.

FDDI е сличен со IEEE 802.3 Ethernet и IEEE 802.5 Token Ring, во однос на поврзаноста со OSI моделот. Неговата примарна намена е да се обезбеди поврзување помеѓу протоколите од повисоките нивоа на OSI моделот и користениот медиум за поврзување на мрежните уреди. На сликата се илустрирани четирите FDDI спецификации и нивната поврзаност со секое IEEE-дефинирано подниво за контрола на логичкиот линк (Logical Link Control LLC). LLC подслојот е компонента на вториот слој - MAC.



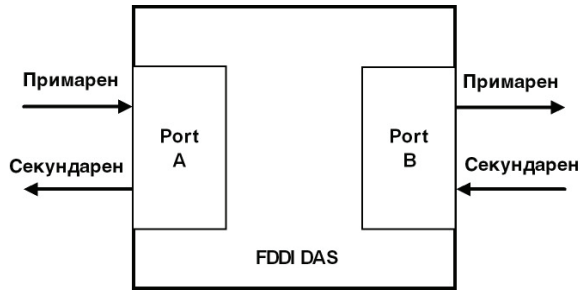
Слика 5.22: Поврзување на FDDI спецификациите во OSI моделот

5.5.3 FDDI станици – видови на поврзувања

Една од уникатните карактеристики на FDDI е дека постојат повеќе начини за поврзување на FDDI уредите. FDDI дефинира четири типа на уреди:

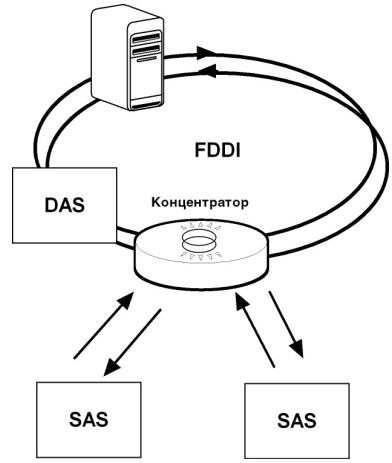
Станица со едно поврзување (single-attachment station SAS), станица со двојно поврзување (dual-attachment station -DAS), концентратор со едно поврзување (single-attached concentrator SAC), и концентратор со двојно поврзување (dual-attached concentrator DAC). Еден SAS се поврзува кон само еден прстен (примарниот) преку концентратор. Една од предностите од поврзување на уредите со SAS поврзување, е дека уредот нема да има

влијание на FDDI прстенот ако се откачи или исклучи. Секој FDDI DAS има две порти, означени како A и B, и преку нив се врши поврзувањето на уредот на двојниот прстен. Секоја порта обезбедува поврзување со примарниот и секундарниот прстен.



Слика 5.23: FDDI DAS порти прикачени на примерниот и на секундарниот прстен

FDDI концентраторот (наречен уште и концентратор со двојно поврзување DAC) е градбениот блок на една FDDI мрежа. Тој се закачува директно на два прстени и обезбедува да испадот или исклучувањето на станиците (SAS), не го доведе прстенот до испаѓање. Ова е особено значајно кога персонални компјутери или други уреди почесто се вклучуваат и исклучуваат од прстенот.



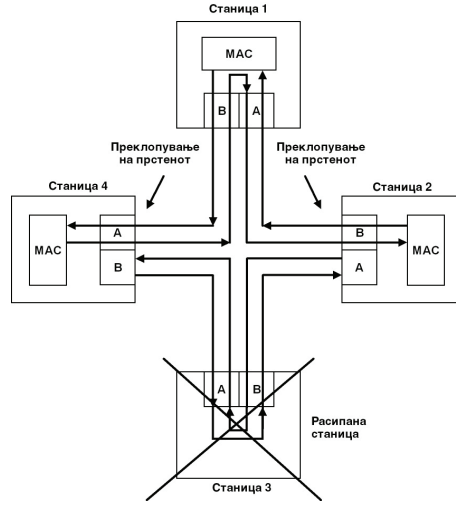
Слика 5.24: Концентраторот се поврзува и на примарниот и на секундарниот прстен

5.5.4 FDDI толеранција на испади

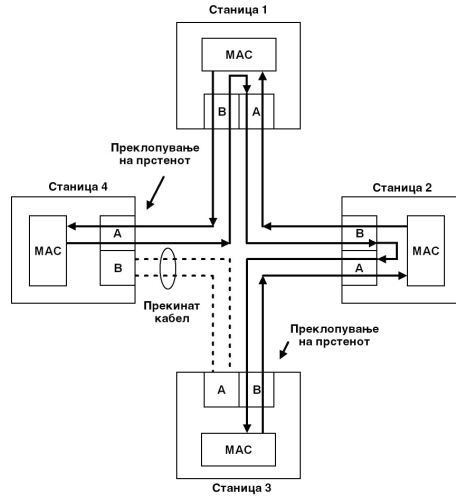
FDDI обезбедува повеќе можности за справување со испади како што се имплементација на двоен прстен, оптички преклопник-премостувач (optical bypass switch), и поддршка за „dual-homing“.

Двоен прстен (Dual Ring)

Примарната карактеристика за отпорност на испади е двојниот прстен. Ако станицата на прстенот испадне или се исклучи, или кабелот е оштетен, двојниот прстен автоматски се преклопува во единичен прстен. При преклопување на прстенот - топологија на двојниот прстен се претвора во топологија на единичен. Повеќе испади произведуваат повеќе независни прстени.



Слика 5.25: Прстенот се опоравува од испад на станица со преклопување



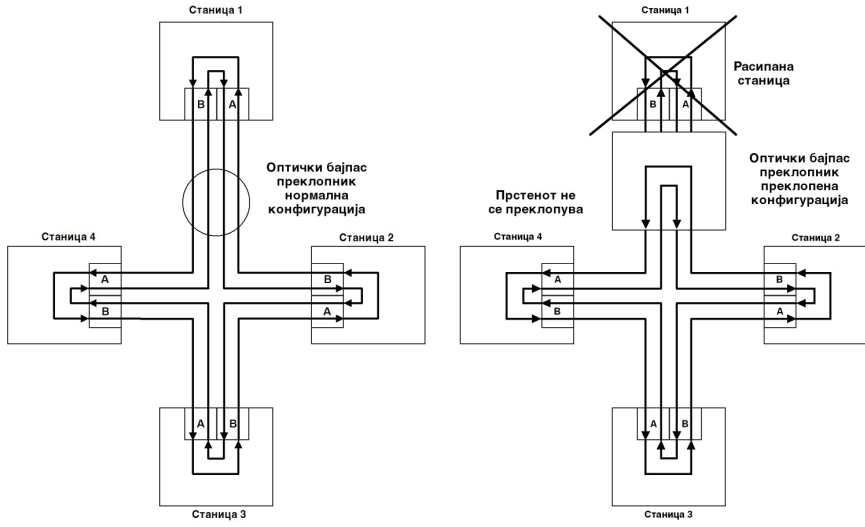
Слика 5.26: Прстенот исто така се преклопува ако има прекин на кабелот

Опоравување на прстенот по испад на станица

Кога една станица испаѓа, уредите на секоја страна на паднатиот (или исклучениот уред) вршат преклопување и формираат единичен прстен. Кога ќе се појави прекин на кабел, уредите на двата краја на кабелот се преклопуваат. Мрежата и во двата случаи продолжува да работи за останатите станици. Треба да се нагласи дека FDDI остварува толеранција на испади само за единичен испад; ако се појават два или повеќе испади, FDDI прстенот се сегментира во два или повеќе независни прстени кои не се во можност меѓусебно да комуницираат.

Оптички преклопник-премостувач (Optical Bypass Switch)

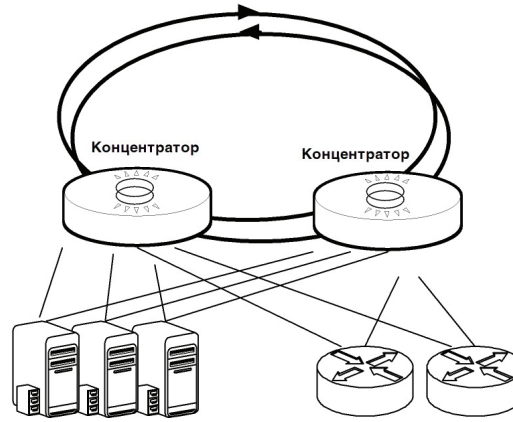
Оптичкиот преклопник - премостувач (optical bypass switch) обезбедува континуирана работа во двоен прстен во случај кога уред од прстенот ќе испадне. Се користи и за превенција од сегментација на прстенот и за елиминација на паднатите станици од прстенот. Оптичкиот преклопник-премостувач ја изведува оваа функција со користење на оптички огледала кои ја пропуштаат светлината од прстенот директно на DAS уредот при нормално работење. Ако се појави испад на DAS уредот, како што е неговото исклучување, оптичкиот преклопник ја премостува светлината низ себе со користење на огледала и на тој начин се задржува интегритетот на прстените. Придобивка од оваа способност се состои во тоа што прстенот нема да се преклопи во случај на испад на уредот.



Слика 5.27: Оптичкиот преклопник-премостувач користи внатрешни огледала за одржување на мрежата

Dual Homing

Критичните уреди, како што се рутери или mainframe хостови, можат да користат техника за толеранција на испади наречена „dual homing“ (за обезбедување на дополнителна редундантност и гаранција на нормална работа). Во „dual-homing“ ситуациите, критичниот уред е закачен на два концентратори. На сликата е прикажана „dual-home“ конфигурација на уреди, како што се сервери на датотеки и рутери.

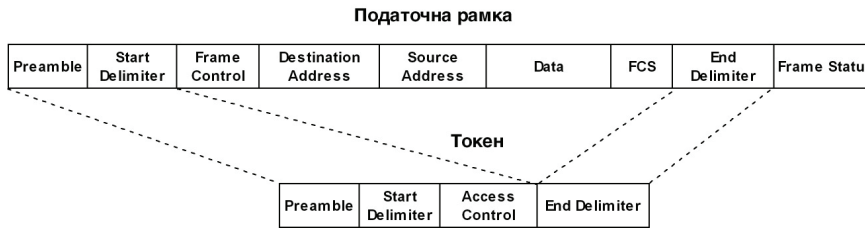


Слика 5.28: „Dual-Home“ конфигурација гарантира нормала работа

При dual-homing ситуации, критичниот уред е закачен на 2 концентратори. Еден пар од врските со концентраторот е деклариран како активен линк, а другиот како пасивен. Пасивниот линк останува во „backup“ мод, сè додека на примарниот линк (или концентраторот на кој е закачен) не му се случи испад. Потоа пасивниот линк автоматски се активира.

5.5.5 FDDI формат на рамки

Форматот на FDDI рамките е сличен со форматот на Token Ring рамката; FDDI рамките можат да бидат долги и до 4,500 бајти.



Слика 5.29: Рамката на FDDI е слична на Token Ring рамката

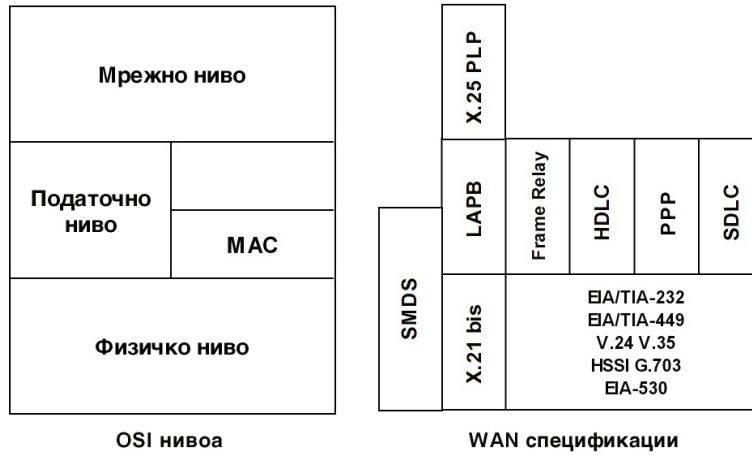
Полиња во FDDI рамката

- Preamble – единствена секвенца за подготовка на станицата за доаѓачка рамка.
- Start Delimiter
- Frame Control – големина на адресните полиња, синхрони или асинхрони податоци и други контролни информации.
- Destination Address – содржи unicast, multicast или broadcast адреса. Како и кај Ethernet и Token Ring адресите, FDDI одредишната адреса е долга 6 бајти.
- Source Address – ја идентификува единствената адреса на испраќачот долга 6 бајти.
- Data – содржи или контролни или податоци за протоколите од повисоките нивоа.
- Frame Check Sequence
- End Delimiter
- Frame Status – овозможува изворот да открие дали се појавила грешка при преносот и дали рамката е препознаена и копирана од страна на одредишната станица.

6 WAN ТЕХНОЛОГИИ

6.1 ВОВЕД ВО WAN ТЕХНОЛОГИИ

Мрежа која опфаќа поширока област од локалната мрежа - WAN (Wide Area Network) е податочно-комуникациска мрежа, која покрива релативно поголема географска област и користи преносни структури обезбедени од телекомуникациски компании (телефонска инфраструктура). WAN технологиите функционираат на пониските 3 слоја на OSI референтниот модел: физичкото ниво, податочен-линк нивото и мрежното ниво.



Слика 6.1: WAN технологиите работат на најниските слоеви од OSI моделот

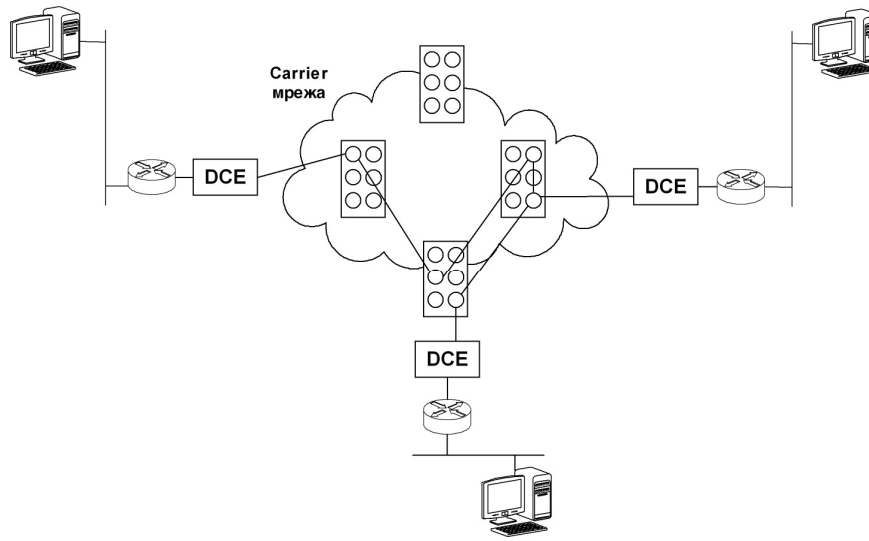
6.1.1 Врски точка-точка (Point-to-Point)

Врската точка-точка (point-to-point link) обезбедува единична воспоставена WAN комуникациска патека од корисничката мрежа, преку носечката (carrier) мрежа, (како што е телефонска компанија) - кон оддалечената мрежа. Врските точка-точка обично се изнајмуваат од провајдерот и се нарекуваат изнајмени линии. За воспоставување на една линија точка-точка, провајдерот доделува парици и хардвер само за таа линија. Изнајмените линии се наплаќаат според пропусниот опсег и оддалеченоста помеѓу двете точки на поврзување, тие обично се поскапи од делените сервиси како што е Frame Relay.

Слика 6.2: Типична врска точка-точка која функционира преку WAN поврзувајќи оддалечена мрежа

6.1.2 Преклопување на кола (Circuit Switching)

Преклопените кола (Switched circuits) овозможуваат податочните конекции да се иницираат по потреба и да се прекинуваат по завршувањето на комуникацијата. Принципот е ист како кај обичниот телефонски сервис за гласовна комуникација, - пример се интегрираните сервиси на дигитална мрежа Integrated Services Digital Network (ISDN). Врската со преклопени кола се иницира кога мрежниот уред (рутер) има податоци за пренос до оддалечената мрежа, со користење на бројот на мрежата. Во случај на ISDN кола, уредот едноставно го повикува телефонскиот број на оддалеченият ISDN приклучок. Кога ќе се поврзат и меѓусебно валидираат двете мрежи, може да започне преносот на податоците; по завршувањето повикот се прекинува.

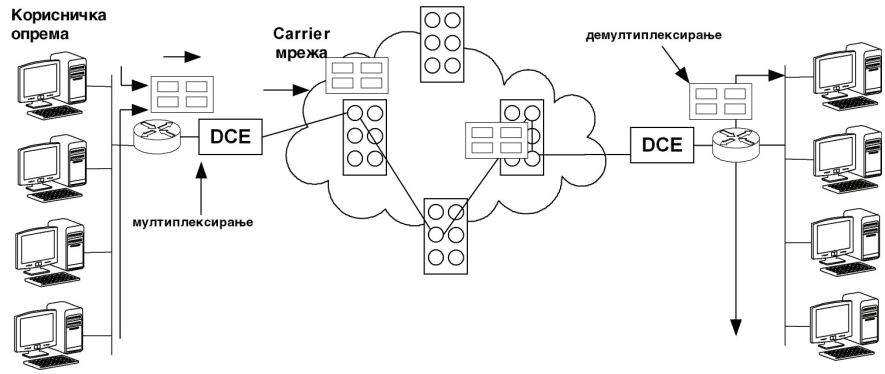


Слика 6.3: Воспоставување на врска преку WAN со преклопени кола - функционира како телефонски сервис

6.1.3 Преклопување на пакети (Packet Switching)

Преклопувањето на пакети (Packet switching) е WAN технологија каде што корисниците користат делени ресурси на провајдерот. Заради тоа провајдерот може поефикасно да ја користи својата инфраструктура, и цената на користење е многу поповолна за клиентите во споредба со врските точка-точка. При користење на пакетското преклопување, мрежите имаат врски кон мрежата на провајдерот и повеќе клиенти ја делат мрежата. Провајдерот потоа креира виртуелни врски помеѓу локациите на корисниците, преку кои пакетите со податоци се испорачуваат од еден до друг корисник, преку мрежата. Делот од мрежата на провајдерот кој е делен, обично се одбележува со облак.

Примери за мрежи со пакетско преклопување се Асинхрон начин на пренос (Asynchronous Transfer Mode ATM), Релеј на рамки (Frame Relay), Преклопувани мултимегабитски податочни сервиси (Switched Multimegabit Data Services SMDS), и X.25. Виртуелните конекции помеѓу клиентите обично се нарекуваат виртуелни кола.



Слика 6.4. Пакетско преклопување преку мрежата на провајдерот

6.1.4 Виртуелни кола во WAN мрежи

Виртуелно коло е логичко коло креирано во делена мрежа помеѓу два уреди. Постојат два вида на виртуелни кола: преклопени виртуелни кола (switched virtual circuits SVC) и постојани виртуелни кола (permanent virtual circuits PVC). SVC се виртуелни кола кои динамички се воспоставуваат по потреба, и се прекинуваат по завршувањето на преносот. Комуникацијата преку SVC колата се состои од три фази: воспоставување на колото, податочен трансфер и прекинување на колото. Фазата на воспоставување вклучува креирање на виртуелно коло помеѓу изворниот и одредишниот уред. Преносот на податоците вклучува пренесување на податоци помеѓу уредите на виртуелното коло; фазата на прекин на колото претставува раскинување на виртуелното коло помеѓу уредите на двата краја. SVC се користат во ситуации кога преносот на податоци помеѓу уредите е спорадичен, најмногу

заради тоа што SVC колата го зголемуваат потребниот пропусен опсег (заради фазите на воспоставување и прекинување на колото), но притоа се намалува цената за користење на постојаната виртуелна конекција.

PVC е постојано воспоставено виртуелно коло кое се состои од една фаза во работата: пренос на податоци. PVC се користат во ситуации каде што податочниот трансфер помеѓу уредите е постојан и константен. PVC колата го намалуваат пропусниот опсег потребен за воспоставување и прекинување на виртуелните кола, но се зголемува цената заради целовремена достапност на виртуелното коло.

6.1.5 Dial-up WAN сервиси (WAN Dial-up Services)

„Dial-up“ сервисите нудат ефикасен начин за поврзување преку WAN мрежи. Најкористените „dial-up“ имплементации се рутирање со бирање по потреба (dial-on-demand routing DDR) и „dial backup“ сервиси.

DDR е техника каде што рутерот динамички иницира повик преку преклопени кола, кога постојат податоци за пренос. При поставување на DDR, рутерот се конфигурира за иницирање на повик при постигнување на одредени критериуми, како што е одреден вид на сообраќај кој треба да се пренесе. По воспоставување на конекцијата, сообраќајот се пренесува по линијата. При конфигурацијата на рутерот, може да се специфицира бројач на неактивност (idle timer) со кој се определува моментот кога рутерот да ја прекине конекцијата, ако линијата е неактивна за одреден временски период.

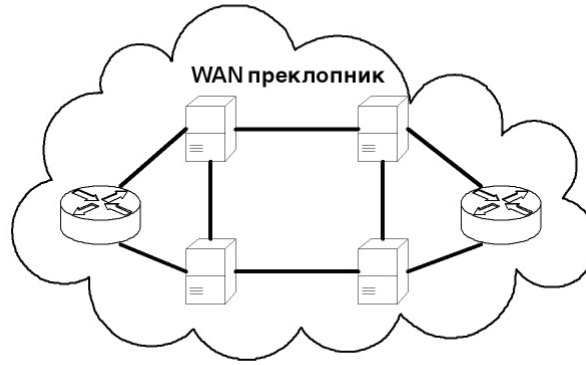
Dial backup е друг начин за конфигурација на DDR, каде што преклопеното коло се користи за обезбедување на резервен сервис за друг тип на кола, како што се точка-точка или пакетско преклопување. Рутерот е конфигуриран така што, кога се детектира испад на примарното коло, се воспоставува врска преку резервната линија и се одржува WAN конекцијата сè додека примарната линија не се воспостави повторно - тогаш се прекинува врската преку резервната линија.

6.1.6 WAN уреди

WAN мрежите користат повеќе видови на уреди кои се специфични за WAN околина, како што се WAN преклопници, сервери за пристап (access servers), модеми (modem), CSU/DSU, и ISDN терминални адаптери, како и рутери, ATM преклопници и мултиплексери.

6.1.7 WAN преклопник

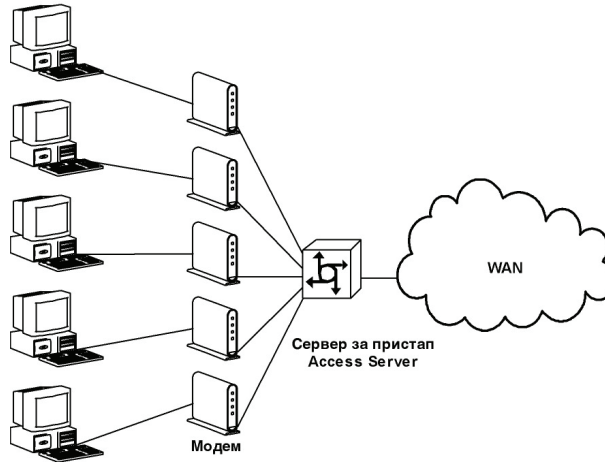
Преклопник (WAN switch) е повеќе-портен уред за умрежување кој се користи во мрежи-носачи (carrier) и врши преклопување на сообраќај како што е Frame Relay, X.25, и SMDS, а работи на податочен-линк слојот на OSI референтниот модел.



Слика 6.5: Два рутери на краевите на WAN мрежата може да се поврзат преку WAN преклопници

6.1.8 Сервер за пристап (Access Server)

Серверот за пристап се однесува како точка на концентрација за „dial-in“ и „dial-out“ врски.



Слика 6.6: Сервер за пристап концентрира „Dial-Out“ конекции во WAN

6.1.9 Modem

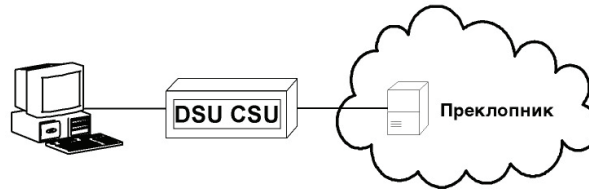
Модем (modem) е уред кој врши интерпретација на дигитални во аналогни сигнали и обратно, со што овозможува податоците да бидат пренесени преку телефонски линии за пренос на глас. На испраќачката страна, дигиталните сигнали се конвертираат во погоден облик за пренос преку аналогни

комуникациски линии, а на приемната страна тие аналогни сигнали повторно се претвораат во дигитални.

Слика 6.7: Модемска врска преку WAN

6.1.10 CSU/DSU

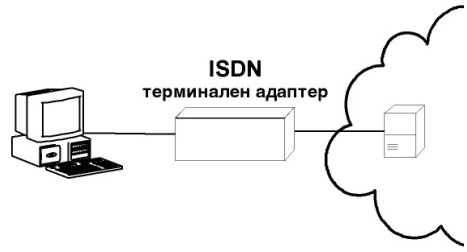
„Уред за каналски сервис/уред за дигитален сервис“ (channel service unit/digital service unit CSU/DSU) е дигитален интерфејс кој се користи за поврзување на рутерот со дигитална врска како што е T1. CSU/DSU исто така обезбедува синхронизација за сигналот помеѓу двата уреди.



Слика 6.8: Локацијата на CSU/DSU (помеѓу преклопникот и терминалот)

6.1.11 ISDN терминален адаптер

Терминален адаптер (ISDN terminal adapter) е уред кој врши поврзување на ISDN Basic Rate Interface (BRI)-конекциите со други интерфејси како што е EIA/TIA-232 на рутерот. Всушност терминалниот адаптер претставува ISDN модем, иако се нарекува терминален адаптер, зашто не врши конверзија од дигитален во аналоген сигнал и обратно.



Слика 6.9: Терминалниот адаптер ги поврзува ISDN со други интерфејси

6.2 ПРОТОКОЛ ТОЧКА-ТОЧКА (POINT-TO-POINT PROTOCOL)

Протоколот „точка-точка“ (Point-to-Point Protocol PPP) се појавил како протокол за енкапсулација на IP сообраќајот преку врските „точка-точка“. Point-to-Point Protocol (PPP) е наследник на Serial Line IP (SLIP) протоколот. PPP обезбедува конекции рутер-рутер и хост-мрежа преку синхрони и асинхрони конекции (кола).

PPP воспоставил и стандард за доделување и управување на IP адреси, асинхрона (start/stop) и бит-ориентирана синхрона енкапсулација, мултиплексирање на мрежните протоколи, конфигурација на линкови, тестирање на квалитетот на линковите, детекција на грешки, како и опции за договарање на можностите за пренос, како што се мрежните адреси и компресијата на податоците.

PPP ги поддржува овие функции со обезбедување на протокол за контрола на линкот (Link Control Protocol LCP), и фамилија на мрежни контролни протоколи (Network Control Protocols NCP) за договарање на опционалните конфигурациски параметри и услуги. PPP поддржува голем број на протоколи од мрежното ниво како што се Novell IPX и DECnet.

6.2.1 Компоненти на PPP

PPP обезбедува начин за пренесување на датаграми преку сериски врски „точка-точка“ и се состои од 3 основни компоненти:

- Начин за енкапсулација на датаграми преку сериски линкови. PPP го користи High-Level Data Link Control (HDLC) протоколот за енкапсулација на датаграмите, преку врски „точка-точка“.
- Link Control Protocol (LCP) - LCP се користи за воспоставување, конфигурација и проверка на врската на податочното ниво.
- Множество на NCP се користат за воспоставување и конфигурација на различни протоколи на мрежното ниво. PPP е дизајниран да овозможи симултано користење на повеќе мрежни протоколи.

6.2.2 Работа на PPP протоколот

PPP конекциите се воспоставуваат по фази. Јазолот кој иницира PPP врска првин испраќа LCP рамки за конфигурација и проверка на податочниот линк. Кога ќе се воспостави линкот, се договараат дополнителни опции кои се бараат од страна на LCP. Изворниот PPP јазол потоа испраќа NCP рамки за избор и конфигурација на протоколите од мрежното ниво.

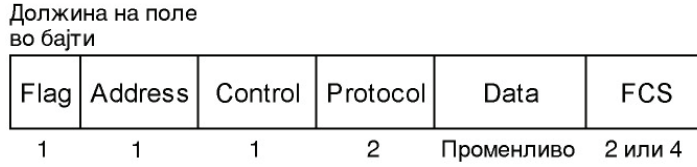
Кога секој од избраните протоколи се конфигурирани, пакетите од секој протокол од мрежното ниво можат да се испраќаат по линкот. Линкот останува конфигуриран за комуникација сè додека експлицитна LCP или NCP рамка не го затвори, или додека не се појави некој надворешен настан (на пример, неактивност на линкот или интервенција на корисникот).

Физичко ниво (Physical Layer Requirements)

PPP физичките конекции дозволуваат работа преку било кој DTE/DCE интерфејс. Примери за поддржани физички интерфејси вклучуваат EIA/TIA-232-C (поранешен RS-232-C), EIA/TIA-422, EIA/TIA-423, и ITU-T V.35. За да може PPP да функционира, потребно е да постои „duplex“ коло, било посветени или преклопувано, кое може да работи во асинхрон или синхрон бит-сериски начин, транспарентно за рамките од PPP податочното ниво.

PPP не поставува никакви ограничувања во однос на брзината на пренесувањето, освен оние поставени од одредени DTE/DCE интерфејси кои се користат.

PPP слој на линк (Link Layer)



Слика 6.10: PPP рамка се состои од 6 полиња

- Flag – почеток и крај на рамката, полето се состои од следната бинарна низа 01111110.
- Address – единичен бајт кој содржи стандардна broadcast адреса (11111111). PPP не доделува индивидуални адреси.
- Control - 1 бајт кој се состои од бинарната секвенца 00000011, која повикува пренос на податоци во несеквенционирана рамка.
- Protocol - два бајти кои го идентификуваат протоколот енкапсулиран во податочното поле во рамката.
- Data – нула или повеќе бајти кои содржат датаграм за протоколот даден во Protocol - полето. Крајот на податочното поле се наоѓа со End Flag секвенца и дозволува 2 бајти за FCS полето. Максималната должина на полето е 1,500 бајти.
- Frame Check Sequence (FCS) - обично 16 bit-а (2 бајти), одредени по претходен договор; PPP имплементациите може да користат 32-битен FSC за подобрена корекција на грешки.

LCP може да договори измени на стандардната структура на PPP рамка, но изменетите рамки видливо ќе се разликуваат од стандардните.

PPP протокол за контрола на линкот (Link-Control Protocol)

PPP LCP обезбедува начин за воспоставување, конфигурација, одржување и прекинување на врските „точка-точка“. LCP се извршува во 4 фази:

1. Воспоставување на линкот и конфигурацијата на договарањето (Link Establishment and Configuration Negotiation). Пред да може било кои датаграми (на пример IP) да бидат разменети, LCP мора прво да ја отвори конекцијата и да ги договори конфигурациските параметри. Ова фаза е комплетна кога ќе се испрати и прими рамка за потврда (acknowledgment frame).
2. Одредување на квалитетот на линкот (Link-Quality Determination). LCP дозволува опционална фаза за одредување на квалитетот на линкот по воспоставувањето на врската. Во оваа фаза, линкот се тестира за да се утврди дали квалитетот задоволува, и оваа фаза е опционална. LCP може да го одложи испраќањето на информациите од мрежните протоколи сè додека не заврши оваа фаза.
3. Преговарање за конфигурација на протоколите од мрежното ниво (Network Layer Protocol Configuration Negotiation). По завршувањето на фазата на одредување на квалитетот на линкот, протоколите од мрежното ниво можат да бидат засебно конфигурирани, и соодветен NCP може да се активира во секое време. Ако LCP го затвори линкот, ги известува мрежните протоколи за да можат навремено да превземаат соодветна акција.
4. Прекинување на линкот (Link Termination). LCP може да го прекине линкот во било кое време. Тоа обично се извршува по барање на корисникот, или од физички настан како што е губењето на carrier-от или истекување на idle-period бројачот.

Постојат три вида на рамки за секоја фаза од LCP: Link establishment frames – рамки за воспоставување и конфигурација на линкот, Link termination frames – рамки за прекинување на врската, Link maintenance frames – рамки за одржување на врската.

6.3 Дигитална претплатничка линија (Digital Subscriber Line - DSL)

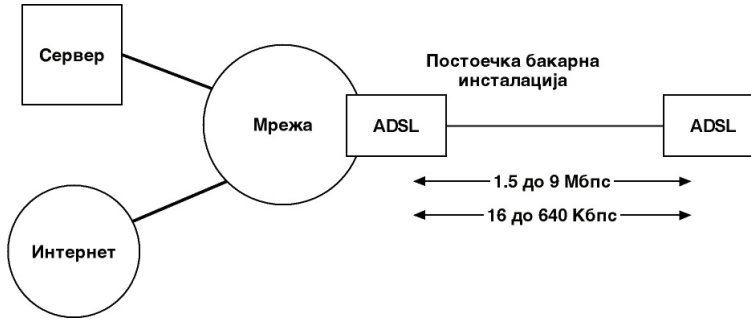
Дигиталната претплатничка линија - Digital Subscriber Line (DSL) е модерна технологија што ја користи постоечката телефонска мрежа со плетени парици за пренос на податоци со голем проток (bandwidth), како што се мултимедија и видео. Поимот xDSL покрива слични технологии на DSL како што се: ADSL, SDSL, HDSL, HDSL-2, G.SHDL, IDSL, и VDSL. xDSL е значајна технологија заради можноста за доставување на брз сообраќај до оддалечени локации користејќи ја постоечката телефонска структура. xDSL сервисите користат „point-to-point“ пристап на јавна мрежа преку бакарни плетени парици за воспоставување на конекција помеѓу сервис-провајдерот и корисникот.

6.3.1 Асиметрична дигитална претплатничка линија (Asymmetric Digital Subscriber Line - ADSL)

ADSL технологијата е асиметрична. Таа дозволува поголем downstream проток од сервис-провајдерот до корисникот, од upstream проток - од страна на корисникот до сервис-провајдерот. Асиметричноста комбинирана со постојан пристап, always-on access (без фаза на повик), ја прави ADSL технологијата идеална за Интернет/интранет пристап, video-on-demand, и пристап кон LAN од оддалечена локација. Корисниците на овие апликации обично превземаат повеќе податоци отколку што испраќаат.

ADSL пренесува повеќе од 6 Mbps до корисникот и 640 kbps повеќе во двете насоки. Овие брзини го зголемуваат постоечкиот капацитет на пристап за фактор 50 или повеќе, без потреба за ново каблирање. Со ADSL може буквално да се трансформира постоечката јавна мрежа ограничена само на говор, текст, и видео со низок квалитет - во мрежа способна за пренос на мултимедија, вклучувајќи и full motion video.

Со оглед што за поставување на новото „broadband“ каблирање ќе биде потребно повеќе време (да ги достигне сите потенцијални корисници), ADSL станува главна технологија подеднакво атрактивна и за корисниците, и за сервис провајдерите - телефонските компании.



Слика 6.11: ADSL врска

6.3.2 Можности и карактеристики на ADSL

ADSL колото поврзува ADSL модем на секој крај од телефонската линија, и креира три канали:

- брз downstream канал (high-speed downstream channel),
- дуплекс канал со средна брзина (medium-speed duplex channel),
- и основен телефонски канал (basic telephone service channel).

Основниот телефонски канал се издвојува од дигиталниот модем со филтер, со што се гарантира непрекинат основен телефонски сервис, дури и ако има прекин на ADSL. Каналот со висок проток има опсег на брзини од 1.5 до 6.1

Mbps, и дуплекс брзини од 16 до 640 kbps. Секој канал може да биде под-мултиплексиран за формирање на повеќе канали со помали брзини.

ADSL модемите обезбедуваат брзини соодветни на Американските T1- 1.544 Mbps и Европските E1 - 2.048 Mbps дигиталните хиерархии, и можат да бидат со различни брзини и можности. Минималната конфигурација обезбедува 1.5 или 2.0 Mbps downstream и 16 kbps duplex канал; другите обезбедуваат брзини од 6.1 Mbps и 64 kbps duplex. Можни се и downstream брзини од 8 Mbps и duplex брзини од 640 kbps. ADSL модемите ги поддржуваат Asynchronous Transfer Mode (ATM) со различни брзини, како и IP протоколите.

Downstream брзините зависат од голем број фактори, како што е должината на бакарната линија, дијаметарот на жицата, интерференцијата итн. Линиското слабеење се зголемува со должината на линијата и фреквенцијата, а се намалува со зголемување на дијаметарот на линијата. Во следнава табела се дадени можните комбинации на брзини на 3-те канали, како и промената на брзината во однос на растојанието и дијаметарот на жицата.

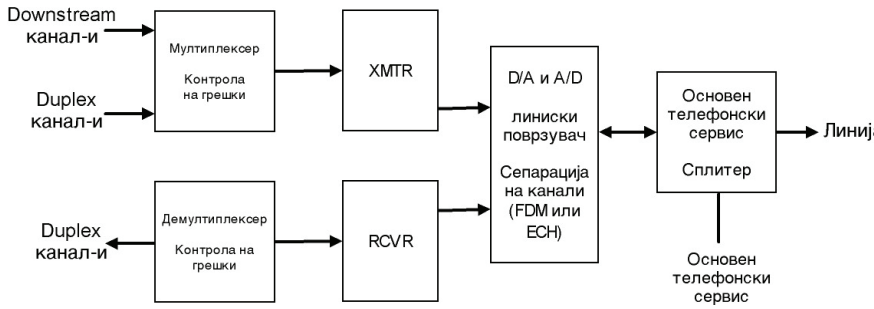
Downstream канали	
n x 1.536 Mbps	1.536 Mbps
	3.072 Mbps
	4.608 Mbps
	6.144 Mbps
n x 2.048 Mbps	2.048 Mbps
	4.096 Mbps
Duplex канали	
C канал	16 Kbps
	64 Kbps
Опционални канали	160 Kbps
	384 Kbps
	544 Kbps
	576 Kbps

Брзина на пренос (Mbps)	Оддалеченост (Km)	Дијаметар на жицата (mm)
1.5 или 2	5.5	0.5
1.5 или 2	4.6	0.4
6.1	3.7	0.5
6.1	2.7	0.4

Слика 6.12: Брзини на ADSL канали во зависност од растојанието и дијаметарот на жицата

6.3.3 ADSL технологија

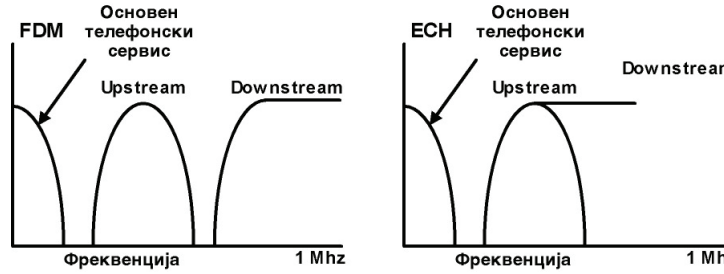
ADSL зависи од напредни технологии за дигитално процесирање на сигналот и алгоритами за пренос на информации преку плетени парици кај телефонските линии. Долгите телефонски линии можат да го ослабат сигналот на 1 MHz (надворешниот крај од фреквентниот спектар користен од ADSL) за дури 90 dB, присилувајќи ја аналогната секција на ADSL модемите да се преоптовари, за да постигнат големи динамички опсези, разделување на каналите, и одржување на ниско ниво на шум.



Слика 6.13: ADSL трансивер на мрежниот крај

За да креираат повеќе канали, ADSL модемите го делат достапниот опсег на телефонската линија на два начини: мултиплексирање со фреквентна поделба (frequency-division multiplexing FDM), и укинување на ехото (echo cancellation). FDM доделува еден опсег за upstream податоците и еден опсег за downstream податоците. Downstream патеката потоа се дели со мултиплексирање со временска поделба (time-division multiplexing), во еден или повеќе канали, со голема или мала брзина. Upstream патеката исто така се дели на соодветни канали со помала брзина.

Со echo cancellation се доделува upstream опсег кој преклопува дел од downstream, и тие се одделуваат со укинување на ехото, техника користена во V.32 и V.34 модемите. ADSL го одделува опсегот 4 kHz за основен телефонски сервис, на DC крајот од опсегот.



Слика 6.14: FDM – мултиплексирање и ECH - укинување на ехото

ADSL модемот ги организира збирните податочни протоци со мултиплексирање на downstream каналите, duplex каналите и каналите за одржување - во блокови, при што се додава и код за корекција на грешки на секој блок. Приемникот ги исправа грешките кои се појавуваат при преносот до нивото дозволено со кодот и големината на блокот. На барање на корисникот, може да се создадат и суперблокови со пуштање на податоци во подблоковите. Ова овозможува приемникот да ја исправи секоја комбинација од грешки во одредено растојание на битови. Со тоа се остварува ефикасен пренос на податочни и видео сигнали.

6.3.4 ADSL2 и ADSL2+

ADSL2 технологијата додава нови особини, ги подобрува перформансите и додава поддршка за нови апликации и сервиси. Меѓу другото, има подобрување во брзините и достигнување на перформансите, приспособување на брзината и stand-by модот.

Подобрување на брзината и досегот

ADSL2 е специјално дизајниран да ги подобри брзината и досегот на ADSL, т.е постигнување на подобри перформанси на подолги линии. ADSL2 го достигнува ова со подобрување на модулацијата, постигнување на поголема придобивка од кодирањето, подобрување на иницијалната состојба на машината и обезбедување на алгоритами за обработка на засилен сигнал. Како резултат, ADSL2 дава поголеми перформанси за сите стандардни уреди.

ADSL2 обезбедува подобра модулација со quadrature amplitude modulation (QAM), која обезбедува поголеми брзини на долги линии каде што односот сигнал-шум signal-tonoise ratio (SNR) е мал. ADSL2 системите го намалуваат framing overhead-от со одредување на рамка со програмиран број на битови. Затоа, за разлика од првата генерација на ADSL стандардите, каде битовите по рамка се фиксни и трошат 32 kbps, во ADSL2 стандардот битовите по рамка можат да бидат програмирани од 4 до 32 kbps. Во првата генерација на ADSL системите, на долги линии каде брзината е мала (пример 128 kbps), фиксните 32 kbps (или 25% од вкупната брзина) се наменети за информација. Во ADSL2 системите, брзините можат да бидат намалени на 4 kbps, кои обезбедуваат додатни 28 kbps за податоци. Почетната состојба на машината има бројни подобрувања кои обезбедуваат зголемени брзини на ADSL2 системите:

- Способност за намалување на моќноста на двата краја од линијата за да се намали ехото и севкупното ниво на преслушување.
- Одредување на локацијата на носечкиот тон од примателот, за да се спречи неважечкото насочување од слабата радио фреквенција од АМ радиото.
- Одредување на преносниците користени за почетните пораки од примачот, за да се спречи неважечкото насочување од слабата радио-фреквенција од АМ радиото.
- Прекин на тонот за време на иницијализацијата, за да се овозможи мешањето на радио фреквенцијата, radio frequency interference (RFI).

Очигледно се подобрени брзината и досегот на ADSL2 споредено со ADSL стандардот од првата генерација. На долгите телефонски линии, ADSL2 ќе обезбеди зголемување на брзината од 50 kbps, важно зголемување за оние корисници на кои им е најпотребно. Ова зголемување на брзината резултира во зголемување на досегот од 180 м.

Подобрувања на потрошувачката на енергијата

Првата генерација на трансивери работат во full-power начин денонoќно, дури и да не се во употреба. Со неколку милиони ADSL модеми, значајно количество на електрицитет може да биде заштедено ако модемите работат во standby/sleep начин - исто како компјутерите. ADSL2 стандардот има два начини на работа кои помагаат во намалување на вкупната потрошувачка на енергија. Тие начини се:

- L2 low-power начин - овој начин овозможува статистичка заштеда на енергијата кај ADSL трансивер-единицата (ATU-C), со брзо влегување и излегување од low-power модот последователно преку ADSL врската.
- L3 low-power начин - овој начин овозможува севкупна заштеда на енергијата кај двете единици ATU-C и ATU-R, односно remote ADSL transceiver unit со влегување во sleep начинот, кога врската не се користи во поголем период.

L2 начинот е еден од најважните иновации на ADSL2 стандардот. ADSL2 трансиверите можат да влезат и излезат од L2 low-power модот базиран на Internet сообраќајот преку ADSL врската. Кога се симнуваат големи фајлови, ADSL2 работи во full-power начинот (наречен L0 power mode) за да се постигне максимална брзина на симнување. Кога опаѓа Internet сообраќајот, на пр. кога корисникот чита долга текст страна, ADSL2 системите можат да преминат во L2 low-power начинот, во кој брзината е значајно намалена и вкупната потрошувачка на енергија е смалена. ADSL2 системите можат моментално да влезат од L2 во L0 и да ја зголемат брзината, ако корисникот започне симнување на фајл. L3 low-power начинот е sleep начин, каде не може да биде пренесен сообраќај преку ADSL врската кога корисникот не е online. Кога корисникот се враќа во online, потребни се приближно 3 секунди за да се врати во steady-state начинот.

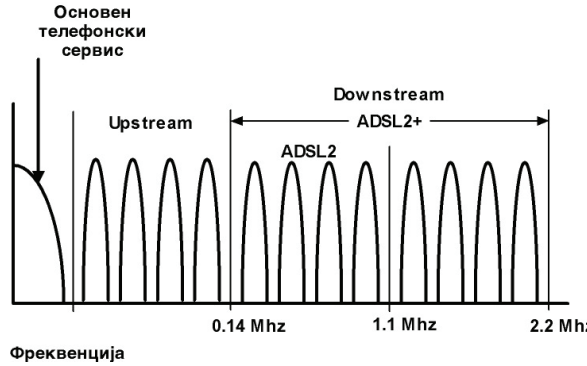
Приспособување на брзината

Телефонските жици се намотани со multi-pair врзувачи кои содржат 25 или повеќе плетени жичани парици. Како резултат, електричните сигнали од една парица може електромагнетно да влијаат врз соседната парица во врзувачот. Оваа појава е позната како преслушување “crosstalk” и може да пречи врз перформансите на брзината на ADSL. Како резултат, промените во crosstalk нивоата во врзувачот може да предизвикаат паѓање на врската на ADSL системите. Crosstalk е само една причина за паѓање на врските на ADSL линиите. Други причини се и AM радио пречките, температурните промени и водата во врзувачите.

Новата иновација наречена seamless rate adaptation (SRA), овозможува ADSL2 системот да ја промени брзината на врската за време на работењето, без некои прекинувања или грешни битови.

ADSL2+

ADSL2+ напредува за да се стандардизира како нов член во фамилијата ADSL2 стандарди. ADSL2+ препорачува дуплирање на downstream протокот. Додека првите два члена од ADSL2 фамилијата G.992.3 (G.dmt.bis) и G.992.4 (G.lite.bis) одредуваат downstream фреквенција до 1.1 MHz и 552 kHz за секого посебно, ADSL2+ одредуваат downstream фреквенција до 2.2 MHz. Резултатот е значајно зголемување на брзините на пократки телефонски линии. ADSL2+ исто така обезбедува алтернативен начин што го дуплира upstream протокот, кој исто така ќе обезбеди дуплирање на upstream брзината. ADSL2+ може исто така да се користи за да се намали crosstalk.



Слика 6.15: Удвојување на upstream протокот

ADSL2+ обезбедува способност да се користат тонови под 1.1 MHz и 2.2 MHz со прикривање на downstream фреквенцијата под 1.1 MHz. Ова може да биде особено корисно кога ADSL сервисите од централниот уред (CO) и оддалечениот терминал (RT) се присутни во истиот врзувач. ADSL2+ може да биде користен за да се исправи проблемот на користење на фреквенциите под 1.1 MHz од CO, и фреквенциите помеѓу 1.1 MHz и 2.2 MHz -од оддалечениот терминал до претпоставениот корисник.

6.3.5 Други DSL технологии

SDSL

Symmetric Digital Subscriber Line (SDSL) е верзија на HDSL со променливи брзини и е симетрична. Downstream и upstream опсезите се симетрични со ист проток. SDSL поддржува податоци на една линија и не овозможува аналогни повици. SDSL може да пренесе до 1.54 Mbps кон и од корисникот, или може да биде конфигуриран за помали брзини до 1.45 Mbps. Симетријата што ја нуди SDSL, комбинирана со перманентен пристап ја прави прифатлива WAN технологија за мали до средни бизниси и оддалечени локации. Таа може да биде евтина алтернатива за изнајмените

линии и Frame Relay сервисите. Бидејќи сообраќајот е симетричен - може ефективно да се имплементираат апликации за далечинско учење, трансфер на датотеки и хостирање на web страници.

HDSL

HDSL стандардот обезбедува T1 пренос преку две парици со брзини на пренос од 784 kbps на секоја парица. ETSI стандардите постојат за секој E1 систем преку две парици, (секоја парица носи 1168 kbps), и три E1 парици со по 784 kbps. HDSL се користи во инфраструктурата на мобилната телефонија. HDSL има недостатоци како што се немање на аналоген пренос, бидејќи го користи и телефонскиот опсег. Друго, ADSL постигнува подобри брзини од HDSL, затоа што асиметричноста на ADSL намерно го сузбива преслушувањето „crosstalk“ на една страна од линијата. Симетричните системи имаат преслушување на двете страни.

HDSL-2

HDSL-2 е стандард кој е алтернатива на HDSL. Тој нуди симетричен сервис на T1 брзини со користење на единична парица, а не две. Потребна е поагресивна модулација, пократки далечини и подобри телефонски линии. Најголемата предност на HDSL-2, е тоа што е дизајнирана да нема меѓусебно влијание со други сервиси, иако HDSL-2 има најголема брзина од само 1.5 Mbps.

G.SHDSL

G.SHDSL е заснован на HDSL-2 верзија со повеќе брзини и е симетричен. Multirate HDSL-2 е стандард познат како G.SHDSL, и нуди брзини од 2.3 Mbps.

ISDN дигитална претплатничка линија

ISDN digital subscriber line (IDSL) е вкрстување помеѓу ISDN и xDSL. Сличен со ISDN во тоа што користи единична парица за пренос на full-duplex брзина од 128 kbps. Исто како ISDN, IDSL користи 2B1Q код за обезбедување транспарентно работење преку ISDN "U" интерфејсот. За разлика од ISDN, ISDL не се поврзува преку говорен преклопник. Ограничувањето на ISDL е тоа што корисникот нема пристап кон ISDN сервисите.

VDSL

Very-High-Data-Rate Digital Subscriber Line (VDSL) пренесува податоци со голема брзина на кратки растојанија, преку телефонска парица со брзина во зависност од должината на линијата.

Максималната downstream брзина е помеѓу 51 и 55 Mbps, преку линии со должина до 300 m. Можни се и downstream брзини од 13 Mbps, до 1500 m оддалеченост.

Upstream брзините во првите изведби ќе бидат асиметрични исто како и ADSL, со брзини од 1.6 - 2.3 Mbps. Двата податочни канали се издвоени фреквентно од основните телефонски сервиси и ISDN, овозможувајќи имплементација на VDSL преку постоечките сервиси.

Моментно двата канали се фреквентно издвоени и како што растат потребите за поголеми брзини - може да се користи и техниката со укинување на ехото (echo cancellation).

6.4 Кабелски технологии

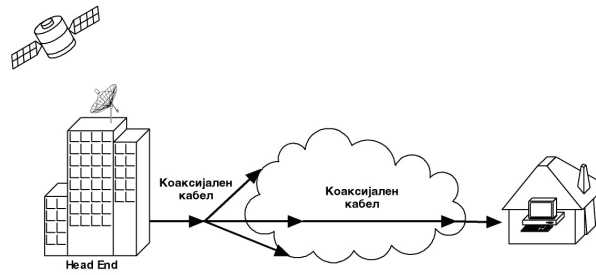
Кабелскиот телевизиски систем - CATV е еднонасочен медиум создаден за дистрибуција на емисии на аналогни видео сигнали кон максимален број на корисници по најниска цена. Од појавата на овој сервис пред 50 години, малку нешто се изменило, освен додавањето на повеќе канали.

Во текот на 90-те, со појавата на сателити со директно емитување (direct broadcast satellite DBS) и дигиталната претплатничка линија (Digital subscriber line (DSL), кабелските оператори добиле сериозна конкуренција во појавените нови технологии. Заради тие причини се пристапи кон дефинирање на стандарди на системи и производи, способни за обезбедување на податочни сервиси преку постоечките CATV системи.

Како резултат на тоа дефиниран е стандардот „Data Over Cable Service Interface Specification (DOCSIS) 1.0“ кој препорачува повеќе-вендорска интероперабилност преку строги тестирања на опремата, која ако е успешна - добива сертификат. Дефинирани се верзијата DOCSIS 1.1 за поддршка на Voice Over Internet Protocol (VoIP) со подобрена сигурност, како и DOCSIS 2.0 која обезбедува подобра искористеност на мрежата, отпорност на шумови и изедначување на брзината на upstream и downstream каналот.

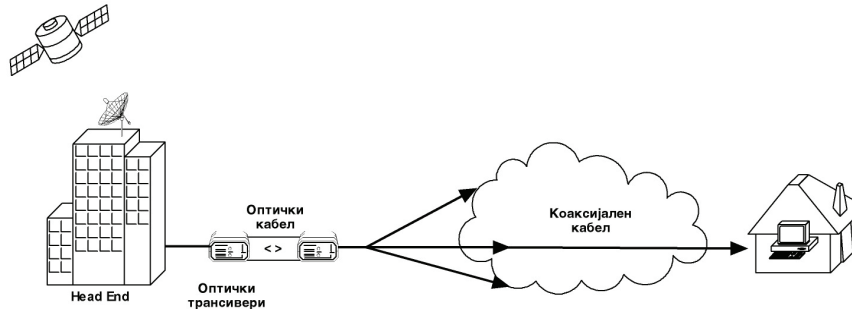
6.4.1 Еволуција од еднонасочен кон двонасочен хибриден оптичко-коаксијален систем (Hybrid Fiber Coax)

CATV мрежата се состои од „head-end“ локација каде што се примаат сите сигнали и без разлика на изворот фреквентно се мултиплексираат, засилуваат и пренесуваат downstream за дистрибуција. Оригиналните CATV мрежи се исклучиво еднонасочни, составени од засилувачи поставени во каскада, за компензација на слабеењето на сигналот во коаксијалниот кабел (во серија со главните транкови „trunks“ до корисничките домови).



Слика 6.16: Едноставна еднонасочна топологија со коаксијален кабел

Покрај тоа што е еднонасочна, низата од засилувачи резултира во систем подложен на шумови и испади, кој не е сигурен и е чувствителен на RF интерференција. Прво значајно подобрување на CATV системите е примената на fiber-optic технологија и појавата на HFC централа.



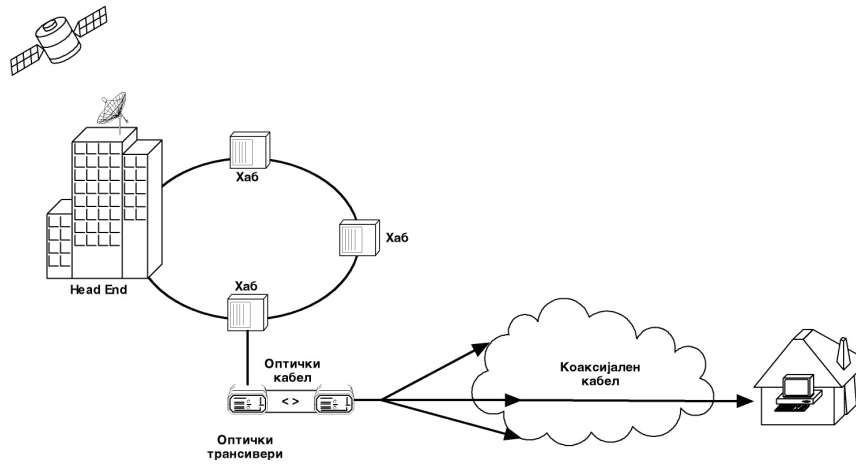
Слика 6.17: Едноставна HFC дистрибутивна мрежа

Делови од коаксијалниот кабел и засилувачите се заменуваат со оптички кабел со повеќе влакна кај „head end“ или hub-овите. Агрегатните видео сигнали го модулираат downstream ласерот, кој го пренесува сигналот до оптичкиот јазол, кој понатаму го претвора во електричен и така се пренесува кон корисниците.

Со примена на оптиката се намалува бројот на каскадните засилувачи и се подобруваат сигурноста, односот сигнал-шум како и пропусниот опсег. Со тоа се овозможува подготовка на системот за следниот чекор за двонасочно работење. Како дополнителна придобивка - HFC ги намалува и трошоците за работа и одржување и ја зголемува отпорност на појава на шум.

Двонасочно работење се постигнува со додавање на upstream засилувачи и теснопојасен upstream ласер во оптичкиот јазол, upstream оптика до „head end“, и компатибилен оптички рисивер за конверзија на секоја upstream информација во електричен сигнал. Со додавање на оптичка-прстен топологија, кабелската мрежа нуди поголема сигурност, проток и можност за пренос на повеќе информации и е подготвена за поддршка на двонасочна информација (после додавање на компонентите). Робустноста на мрежата,

скалабилноста и флексибилноста уште повеќе се подобруваат со додавање на посреднички hub.



Слика 6.18: Напредна HFC мрежа со топологија на прстен

6.4.2 Ограничувања и спецификации на HFC централата

HFC мрежата има потенцијал да понуди голем проток во downstream - од „head end“-от или hub-от до корисникот. Во зависност од обемот на надградбата на системот, достапниот фреквентен опсег може да биде од 54 до 860 MHz, при што downstream каналите се одредени од стандардите за емитување соодветно на државата. Broadcast видео каналите го ограничуваат upstream-от и повратната насока од корисникот во спектарот помеѓу 5 - 42 MHz. Овој дел од спектарот е особено чувствителен на RF сигнали.

DOCSIS системот мора да обезбеди повеќе од 99 % достапност при испраќање на 1500-бајтни пакети со брзина од најмалку 100 пакети во секунда, и за постигнување на овие стандарди потребно е да се придржуваат одредени спецификации за „upstream“ и за „downstream“ фреквентниот опсег.

Поголем предизвик за кабелскиот оператор е реализација на доволен искористив „upstream“ преносен опсег, за постигнување на бараната пропустност за податочни и други сервиси. Ограниченият „upstream“ пропусен опсег обично се дели со други сервиси како што се „impulse pay-per-view (IPPV)“, телеметрија и системи за обезбедување, кои црпат информации од оддалечени сензори, како и други сигнали кои интерферираат со ниско пропусниот опсег.

6.4.3 DOCSIS стандарди и сигнални протоколи и апликации

DOCSIS интерфејс спецификацијата овозможува развој и примена на „data-over-cable“ системи на мултивендорска и интероперабилна база за двонасочен транспарентен пренос на Internet Protocol (IP) сообраќај помеѓу „head end“ на кабелскиот систем и корисникот, преку целосно коаксијална или hybrid-fiber/coax (HFC) кабелска мрежа. Системот се состои од CMTS лоциран на „head end“, коаксијален или HFC медиум и кабелски модем (CM) кој се наоѓа кај корисникот, во конјункција со DOCSIS-дефинираните слоеви кои поддржуваат интер-операбилност и можност за додавање на нови идни сервиси.

Дефиниции на DOCSIS нивоа:

- IP мрежно ниво
- Ниво на податочен линк (Data link layer) составено од:
    - Logical Link Control (LLC) подниво, соодветно на Ethernet стандардите,
    - Link security подниво за приватност, авторизација и автентификација,
    - Media Access Control (MAC) подниво за операции кои поддржуваат „protocol data units (PDU)“ со варијабилна должина:
        - CMTS контрола на натпреварување и резервација на можност за пренесување
        - Низа на мини-слотови во „upstream“ каналот
        - Ефикасност на пропусноста преку пакети со варијабилна должина
        - Проширување за идна поддршка на Asynchronous Transfer Mode (ATM) или други видови на PDU
        - Поддршка на повеќе степени на услуги и опсег на брзини

- Физичкиот слој (PHY) се состои од:
    - Слој на конвергенција на „Downstream“ според стандардот MPEG-2 (Rec. H.222.0)
    - Physical Media Dependent (PMD) подслој за:
    - Downstream со 64 или 256 квадартурна амплитудна модулација (Quadrature Amplitude Modulation - QAM), поврзување на Reed-Solomon и Trellis FEC корекција на грешки
    - Upstream, кој ги вклучува:
        - Quadrature phase shift keying (QPSK) или 16 QAM модулација

- Поддршка за повеќе-симболни брзини
- Кабелски модеми кои се контролирани и програмабилни од страна на CMTS
- Фреквентна агилност
- Поддршка за рамка со фиксна и променливи PDU формати
- Time-division multiple access (TDMA)
- Програмибилни Reed-Solomon FEC и преамбули
- Способност за поддршка на идни технологии за физичкиот слој

Како додаток, спецификацијата уште дефинира начин како CM сам да открива соодветни фреквенции за „upstream“ и „downstream“, брзини на пренос, формат на модулација, корекција на грешки и нивоа на моќност. За да се одржат рамномерноста на сервисите, на индивидуалните CM не им се дозволува пренесување, освен во строго дефинирани и контролирани услови.

<table>
<tr><th>OSI</th><th colspan="3">DOCSIS податочен пренос преку кабел</th></tr>
<tr><td>Повисоки нивоа</td><td colspan="2">Апликации</td><td rowspan="3">DOCSIS контролни пораки</td></tr>
<tr><td>Транспорт</td><td colspan="2">TCP или UDP</td></tr>
<tr><td>Мрежно</td><td colspan="2">IP</td></tr>
<tr><td rowspan="2">Податочно</td><td colspan="3">IEEE 802.2</td></tr>
<tr><td colspan="3">DOCSIS MAC (MPEG рамки - downstream)</td></tr>
<tr><td rowspan="3">Физичко</td><td>Upstream
TDMA</td><td colspan="2">Downstream
TDM</td></tr>
<tr><td>Дигитална IF модулација
(QPSK или QAM-16)</td><td colspan="2">Дигитална RF модулација
(QAM-64 или QAM-256)</td></tr>
<tr><td colspan="3">HFC</td></tr>
</table>

Слика 6.19: DOCSIS и слоевите на OSI моделот

DOCSIS физичкото ниво дозволува значајна флексибилност за обезбедување на квалитетен пренос преку системи со променлив квалитет на пренос. Значајни се опционалните опсези на upstream каналот и изборот на модулацијата достапна и за upstream и за downstream сигналите.

Во зависност од пропусниот опсег и опциите за модулација, и во додаток на DOCSIS-специфицираните симболни брзини, вкупните и ефективните брзини за пренесување на податоци се дадени во следната табела. Разликата се состои во редундантноста генерирана од страна на неефикасноста на FEC кодот.

Табела 6.1

Номинални DOCSIS Downstream брзини со модулација во 6-MHz канал	64 QAM	256 QAM
Симболна брзина	5.057 MSs	5.360 MSs
Вкупна брзина	30.34 Mbps	42.9 Mbps
Ефективна брзина	27 Mbps	38 Mbps

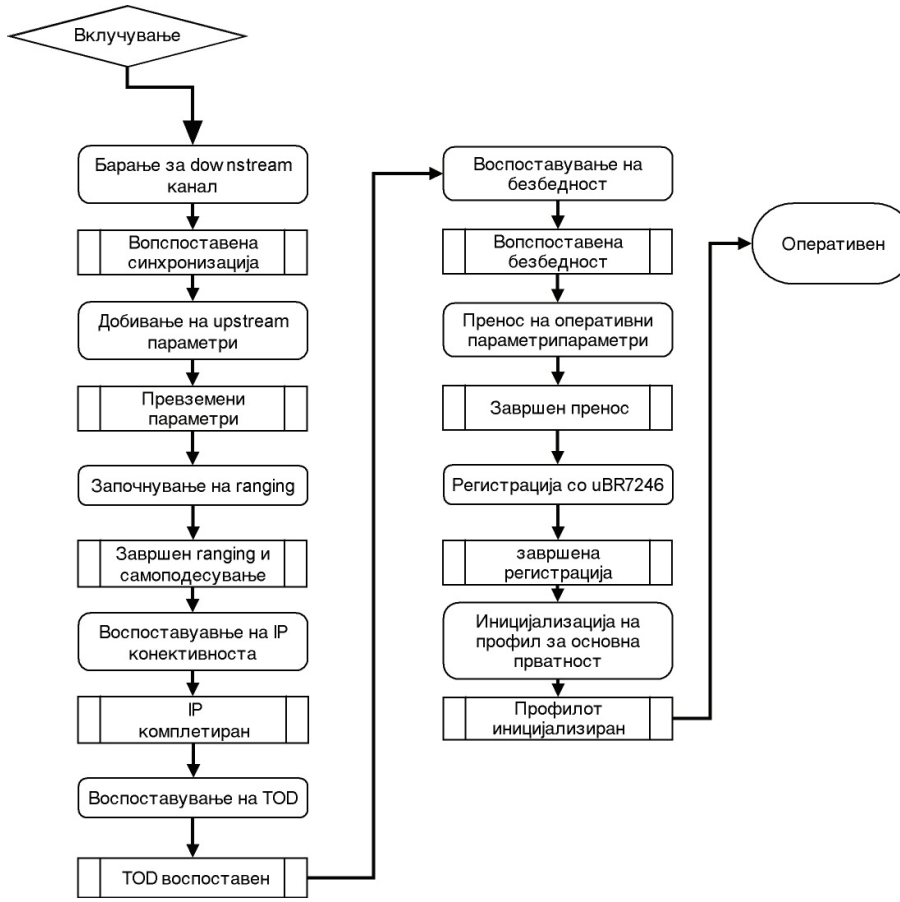
За системот да стане функционален, DOCSIS специфицира потреба од задолжителни сервери кои ќе бидат дел од системот на поврзување на CMTS и CM и кои ќе вклучуваат следниве:

- Dynamic Host Configuration Protocol (DHCP) сервер кој обезбедува потребни IP адреси и за CM и други PC уреди.
- Time of Day (TOD) сервер со намена за забележување на системските настани.
- Trivial File Transfer Protocol (TFTP) сервер, со намена за регистрирање и преземање на конфигурациските датотеки на CM за индивидуалните корисници. Тие треба да вклучуваат QoS параметри, имплементација на основна приватност, работна фреквенција, број на хост уредите итн..

За поголеми кабелски системи, препорачливо е да серверите бидат поддржани со посветена хардверска платформа за обезбедување на брз одзив на системот и скалабилност. DOCSIS спецификацијата диктира регистрациски процес на кабелскиот модем. Во околина со CMTS која е поддржана со потребните сервери, кога CM иницијално ќе се вклучи - напојувањето врши скенирање на „downstream“ спектрумот за компатибилен RF канал, кој пренесува податоци според карактеристиките на DOCSIS физичкото ниво. CMTS периодично емитува (broadcasts) таканаречени „upstream channel descriptors (UCD)“ преку DS каналот, од кој CM ја дознава доделената „upstream“ оперативна фреквенција. CM ги има воспоставено и двете US и DS фреквенцијата.

CMTS периодично емитува „upstream bandwidth allocation maps“ (во продолжеток - MAP) во делените временски слотови во DS насоката. CMTS доделува привремен идентификатор - service identifier (SID) (обично SID = 0) кон CM, и модемот започнува со грубо подесување на моќноста R1 (со зголемување од 3dB) и процес на временска синхронизација помеѓу себе и CMTS со користење на натпреварување и делени временски слотови.

CMTS периодично испраќа „keepalive“ пораки за верификација на линкот помеѓу себе и сите CM уреди во ист домен. Кога CM ќе ја прими првата, се префрла кон фино подесување на напојувањето (R2 со користење на 0.25 dB чекори).



Слика 6.20: Процесот на регистрација на кабелскиот модем

По R2 процесот, за CM се смета дека воспоставил врска помеѓу себе и CMTS, но ако линкот ќе биде исклучен ако се загубат 16 последователни „keepalive“ пораки. Во зависниот од достапноста на временски слот и со користење на привремениот SID, CM испраќа барање за проток (bandwidth) кон CMTS, кој враќа дозвола за испраќање на upstream податоци во достапниот временски слот.

CM последователно прави откривање на DHCP серверот со порака за барање на адреса (DHCP (req). CMTS препраќа порака за потврда (DHCP ack) од DHCP серверот со IP адресата, default gateway, адресите на TFTP и TOD серверот и името на TFTP конфигурацискатa датотека. CM ги иницијализира TOD и TFTP процесите. Од TFTP серверот, CM ја прима конфигурацискатa датотека со QoS, безбедносните параметри, доделувањето на фреквенциите, надградба на софтверот на кабелскиот модем како и други параметри. CM ја испраќа конфигурацискатa датотека кон CMTS и иницира барање за

регистрација. Ако конфигурацијата е валидна, CMTS доделува траен SID на CM и го регистрира со статус online. По регистрацијата - CM опционално иницира активација на 56-bit DES за енкрипција на врската помеѓу CMTS и самиот себе преку кабелскиот систем.

6.5 Дигитална мрежа на интегрирани сервиси (Integrated Services Digital Network - ISDN)

Дигиталната мрежа за интегрирани сервиси „Integrated Services Digital Network (ISDN) се однесува на множество на протоколи предложени од страна на телефонските компании за пренос на податоци, говор и други материјали преку телефонската мрежа. ISDN обезбедува сет на дигитални сервиси кои истовремено обезбедуваат говор, податоци, текст, графика, музика, видео и информации до крајните корисници преку постоечките телефонски системи.

Појавата на оваа технологија претставува резултат на напорот за стандардизација на претплатничките сервиси, корисничко-мрежните интерфејси, и мрежните и меѓумрежните можности.

ISDN е алтернатива на Frame Relay и T1 wide-area телефонските сервиси (WATS), и служи за поврзување на мали оддалечени локации кон корпорациските кампуси. Типични ISDN апликации и имплементации вклучуваат пренос на слика со голема брзина (како факсимил Group IV), трансфер на податоци со голема брзина, видео-конференции итн.

6.5.1 ISDN уреди

ISDN уредите се терминали, терминални адаптери (TA), уреди за мрежна терминација, за линиска терминација и терминација на централи. Уредите може да се категоризираат во следниве три основни групи:

- ISDN терминална опрема (terminal equipment),
- ISDN уреди за терминација (termination devices),
- ISDN референтни точки (reference points).

Постојат два вида на ISDN терминали: специјализирани ISDN терминали кои се означени како терминална опрема тип 1 (TE1), и не-ISDN терминали како што се DTE, означени како терминална опрема тип 2 (TE2).

TE1 се поврзуваат на ISDN мрежата преку 4-жичен дигитален линк со плетени парици. TE2 се поврзуваат на ISDN мрежата преку TA. ISDN TA може да биде и самостоен уред вграден во TE2. Ако TE2 е имплементиран како самостоен уред, се поврзува со TA преку стандарден интерфејс од физичкото ниво. Примери се EIA/TIA-232-C (порано познат како RS-232-C), V.24, и V.35.

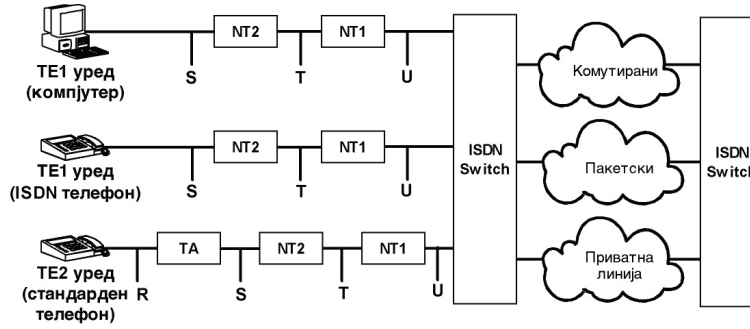
Покрај TE1 и TE2 уредите, ISDN специфицира вид на посреднички уреди наречени „network termination (NT)“ уреди. NT уредите ги поврзуваат 4-

жичените врски (претплатнички) во 2-жичени локални јамки. Постојат 3 поддржани вида на NT уреди:

- NT Type 1 (NT1) уред - тој се обезбедува од страна на провајдерот.
- NT Type 2 (NT2) уред - се поставува во дигиталните „private branch exchanges“ (PBX) централи. NT2 извршува функции на протоколите од второ и 3-то ниво како концентрациски сервиси.
- NT Type 1/2 (NT1/2) уред - ги комбинира функциите на NT1 и NT2 уредите. NT1/2 е компатибилен и со NT1 и со NT2 и потполно ги заменува.

ISDN специфицира и одреден број на референтни точки кои ги дефинираат логичките интерфејси помеѓу функционалните групи, како што се TA и NT1. ISDN ги дефинира следниве референтни точки:

- R референтна точка - ја дефинира точката помеѓу не-ISDN опремата и TA.
- S референтна точка - ја дефинира точката помеѓу корисничките терминали и NT2.
- T референтна точка - ја дефинира точката помеѓу NT1 и NT2 уредите.
- U референтна точка – ја дефинира точката помеѓу NT1 уредите и линиската терминална опрема во „carrier“ мрежата.



Слика 6.21: Пример за ISDN конфигурација со прикажани поврзувања помеѓу уредите и референтните точки

На сликата е илустриран пример за ISDN конфигурација со 3 уреди прикачени на ISDN преклопник во централана локација. Два од овие уреди се ISDN-компатибилни, и можат да бидат прикажани преку S референтна точка на NT2 уредите. Третиот уред (стандарден не-ISDN телефон) се поврзува преку R референтна точка на TA. Било кој од овие уреди може исто така да се закачи на NT1/2 уред, со кој се заменуваат и NT1 и NT2.

6.5.2 Сервиси на ISDN

Постојат два вида на сервиси асоцирани со ISDN:

1. Основен сервис – Basic Rate Interface - BRI.
2. Примарен сервис - Primary Rate Interface - PRI.

ISDN BRI сервис

ISDN основниот пристап (Basic Rate Interface -BRI) обезбедува 2 B канала и 1 D канал. BRI B-каналот работи на 64 kbps и пренесува податоци, додека BRI D-каналот работи на 16 kbps и се користи за пренесување на контролни и сигнални информации, иако може да поддржува и пренесување на кориснички податоци под одредени услови.

Сингнализациониот протокол кај D каналот ги опфаќа физичкото, податочното и мрежното ниво на OSI референтниот модел. BRI исто така обезбедува контрола на врамување со вкупна битска брзина од 192 kbps.

ISDN Primary Rate Interface (PRI)

ISDN примарниот пристап (Primary Rate Interface PRI) обезбедува 23 B канали и еден 64-kbps D канал за Северна Америка и Јапонија, со вкупен проток од 1.544 Mbps. Во Европа, Австралија и другите делови на светот ISDN дава 30 B канали и еден 64-kbps D канал, за вкупен битски проток од 2.048 Mbps.

6.5.3 Спецификации на ISDN

Во продолжение е даден опис на спецификациите на ISDN за слоевите 1, 2 и 3 од OSI референтниот модел.

Физички слој (Layer 1)

Физичкиот слој на ISDN (Layer 1) има различен формат на рамки во зависност дали се појдовни (од терминалот кон мрежата), или се дојдовни (од мрежата кон терминалот). Двата интерфејси за физичкото ниво се дадени на сликата. Рамките се долги 48 бита, од кои 36 содржат податоци. Битовите користени во ISDN рамката на физичкото ниво се:

- Framing Bit (F) – обезбедува синхронизација.
- Load Balancing Bit (L) – користен за подесување на средната вредност на битовите.
- Echo Bit (E) – ехо на претходниот D bit за разрешување кога неколку терминали на пасивната магистрала се натпреваруваат за канал.
- Activation Bit (A) – активира уреди.
- Spare Bit (S) - недоделен.

- B1 Channel Bits (B1) – резервиран за кориснички податоци.
- B2 Channel Bits (B2) - резервиран за кориснички податоци.
- D Channel (D) - резервиран за кориснички податоци.

Слика 6.22: Формат на рамките во физичкото ниво на ISDN во зависност од нивната насока на пренесување

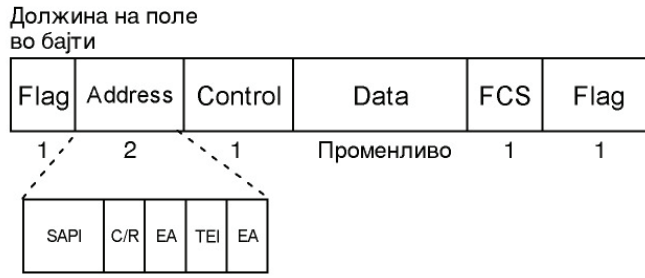
На едно коло може физички да се поврзат повеќе ISDN кориснички уреди. Во таква конфигурација можно е да дојде до појава на колизии во услови кога два уреди се обидуваат да пренесуваат истовремено. ISDN спецификацијата обезбедува начин за заземање на линкот. Кога NT прима D бит од TE, го враќа назад на следната позиција на E-битот. TE го очекува следниот E бит да биде ист како и последниот емитуван D бит. Терминалите не можат да емитуваат на D каналот, сè додека не детектираат одреден број на единици (ознака дека нема сигнал - "no signal"), соодветно со предефиниран приоритет. Ако TE детектира бит во ехо каналот (E) кој се разликува од D битот, траба итно да прекине со емитувањето. Ова едноставна техника обезбедува да само еден терминал емитува D порака едновремено. По успешното пренесување на D-порака, терминалот го намалува својот приоритет со барањето за детекција на поголема низа на континуирани единици, пред повторно да емитува.

Терминалите не го подигнуваат својот приоритет, сè додека сите другите уреди на истата линија ја искористат можноста за испраќање на D порака. Телефонските врски имаат поголем приоритет од сите други сервиси, а сигналната информација има поголем приоритет од не-сигнална информација.

Слој на податочен линк (Layer 2)

Слојот 2 од ISDN сигнализацискиот протокол е процедура за пристап кон линкот (Link Access Procedure, D channel LAPD). Овој слој се користи преку D каналот за правилно пренесување на контролната и сигнализацискатa информација. Форматот на LAPD рамката е даден на сликата и контролното поле има 3 различни формати зависно од видот на рамката:

- Information (I) рамка – носи информација за повисоките нивоа и некои контролни информации.
- Supervisory (S) рамка – обезбедува контролна информација. Оваа рамка може да бара и суспендира трансмисија, дава извештај за статусот и потврдува примање на I рамки. Supervisory рамките немаат информациско поле.
- Unnumbered (U) рамка – се користи за контролна намена и не е секвенционирана.



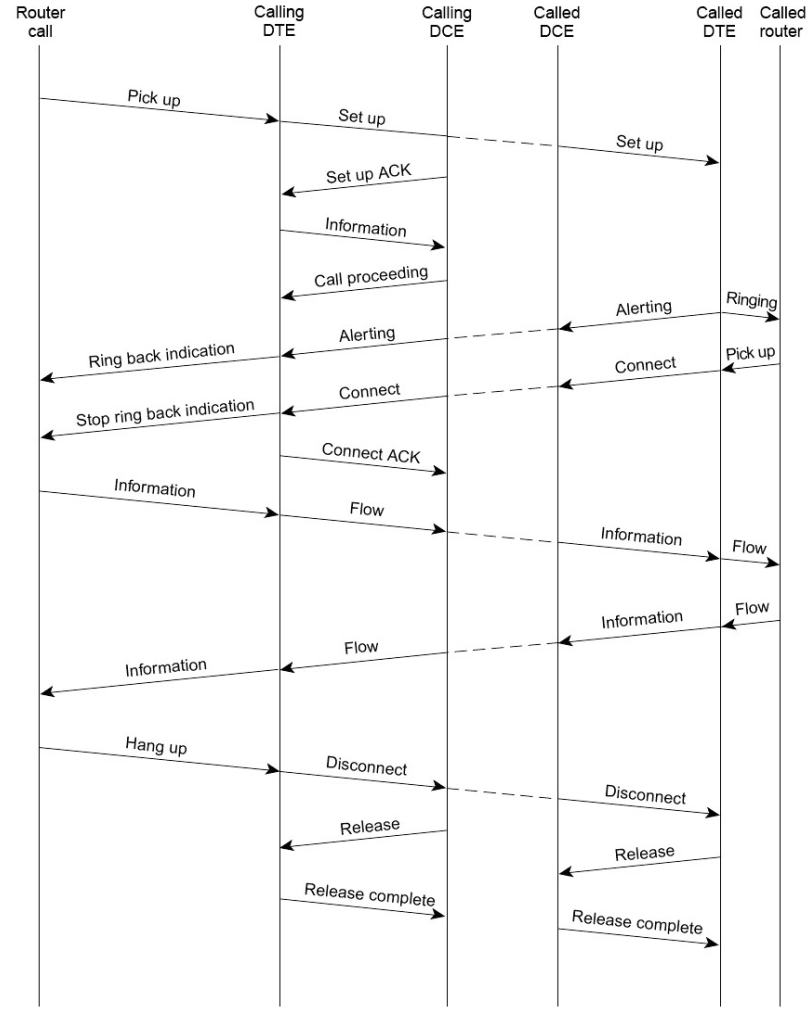
Слика 6.23: Формат на LAPD рамка

LAPD адресното поле може да биде со 1 или 2 бајти должина. Ако се постави бит на првиот бајт за проширена адреса, тогаш должината е 1 бајт, во другиот случај е 2 бајти. Првиот бајт од адресното поле содржи идентификатор за пристап до сервисна точка (service access point identifier SAPI), со кој се дефинира местото каде LAPD сервисите се пренесуваат на слојот 3 (Layer 3). Битот C/R bit покажува дали рамката содржи команда или одговор. Идентификаторот за терминална крајна точка (Terminal Endpoint Identifier TEI) идентификува еден или повеќе терминали; ако TEI ги има сите единици - тоа означува „broadcast“ емитување.

Мрежен слој (Layer 3)

ISDN операциите на мрежно ниво опфаќаат серија од фази кои се одредени со размена на специфични пораки. Генерално, ISDN повикот опфаќа воспоставување на врска, прекинување, информации и други разни пораки. Фазата на повик го дефинира начинот на кој се иницира, потврдува и завршува ISDN повикот. Специфичностите на фазите во ISDN повикот се дефинирани во ISDN мрежното ниво во OSI моделот.

Компонентите на фазата на повикот вклучуваат SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, и DISCONNECT.



Слика 6.24: ISDN повик преку комутирани кола поминува преку различни фази до дестинацијата

7 БЕЗЖИЧНИ ТЕХНОЛОГИИ

7.1 ВОВЕД

Покрај Ethernet, како најкористен мрежен стандард сè повеќе стануваат застапени безжичните локални мрежи (wireless LAN). Постојат 18 вида на различни безжични технологии со огромен број на подмножества од технологии и стандарди, од ATM базирани протоколи, до WLAN (Wireless Local Area Network). Фреквенциите на различните технологии можат да покријат растојанија во опсег од неколку стотина метри (wireless LAN), до 30 км (MMDS). Начинот на кој се пренесуваат радио брановите, количеството на податоци што се пренесуваат, отпорноста на интерференции од внатрешни и надворешни извори и ред други карактеристики, се разликуваат од технологија до технологија.

7.1.1 Пренос на радио бранови

Радио брановите лесно се создаваат и имаат способност да се пренесуваат на големи растојанија, па долго време се носечка технологија во телекомуникациите. Радио брановите се карактеризираат со простирање во сите насоки (omni-directional) и карактеристиките на пренесувањето се фреквентно зависни. На пониските фреквенции, радио брановите лесно ги надминуваат пречките, но нивната енергија опаѓа со оддалечување од изворот со степен $1/r^2$ во воздух. На повисоките фреквенции, радио брановите се простираат по прави линии и се одбиваат од пречките. Исто така, во овој случај и атмосферските прилики можат да влијаат врз нивното простирање и можат, на пример, да бидат апсорбирани од дождот. За било кој фреквентен опсег може да се појави влијание од пречки предизвикани од моторите и електричните уреди.

Заради способноста на радио брановите да се пренесуваат на големи растојанија, се појавува проблем на интерференции помеѓу корисниците. Заради оваа причина употребата на радио предавателите е лиценцирана од страна на државните институции, освен во еден случај, кој ќе биде опишан во продолжението на текстот. Во VLF, MF и LF фреквентните опсези, радио брановите се шират по контурата на земјата (ground waves).

Овие бранови можат да се детектираат дури на 1000 km на ниски фреквенции, и помалку ако се пренесуваат на повисоките. AM радио-преносот употребува MF фреквенција; радио брановите во овој опсег поминуваат лесно преку ѕидовите на зградите, но главен проблем е нивниот мал пропусен опсег (bandwidth).

Во HF и VHF фреквентните опсези, радио брановите имаат тенденција да бидат апсорбирани од земјата. Брановите кои ја достигаат јоносферата, (слојот од наелектризирани честички кои кружат околу земјата на височина

од 100 до 500 km), се рефлектираат и се враќаат назад на земјата. Под одредени атмосферски услови сигналите можат повеќекратно да се прекршуваат и затоа може да се пренесуваат на големи оддалеченост.

7.1.2 Микробранов пренос

Над фреквенциите од 100 MHz брановите се шират по скоро прави линии, и можно е нивно тесно насочување. Со концентрирање на целата енергија во мал зрак со посредство на параболична антена, се добива многу поголем однос на сигнал-шум, но и антените кај предавателот и примачот треба да бидат соодветно подесени и порамнети. Уште пред појавата на оптичките влакна како медиум, микробрановиот начин за пренос овозможувал функционирање на телефонскиот систем на големи растојанија.

Заради пренесувањето на брановите по права линија, ако засилувачките станици (репетиторите) се меѓусебно многу оддалечени, како пречка се појавува закривеноста на земјината топка. Затоа треба репетиторите да се употребуваат периодично, при што нивното растојание се зголемува со квадратен корен од висината на кулата на репетиторската станица; на пример, за кули со висина од 100m - репетиторите можат да бидат на поставени на растојание од 80km.

За разлика од радио брановите на ниски фреквенции, микробрановите не можат да поминуваат низ објектите. Некои бранови во линија на преносот можат да бидат одбиени од ниските атмосферските слоеви и да пристигнат задоцнети во однос на директните бранови. Задоцнетите бранови можат да пристигнат де-фазирани со директните бранови при што доаѓа до придушување и губење на сигналот. Овој ефект претставува сериозен проблем и е наречен multipath fading; тој е временско и фреквентно зависен. Како начин за справување, некои од операторите на овие микробранови системи поседуваат дополнителни 10% неупотребени канали од достапниот фреквентен опсег како резерва, за да се вклучат во моментот кога привремено ќе се придуши сигналот во тој фреквентен канал.

Потребата од поширок фреквентен опсег доведе до рутинска употреба и на фреквенциите до 10 GHz, но се појавува проблем за употреба на фреквенциите околу 4 GHz, имено тие се апсорбираат од водата. Овие бранови се долги само неколку сантиметри и можат да бидат апсорбирани од дождот, што доведува до проблеми во комуникацијата; при појава на дожд, системот треба привремено да се исклучи и комуникацијата да се пренасочи по заобиколен пат.

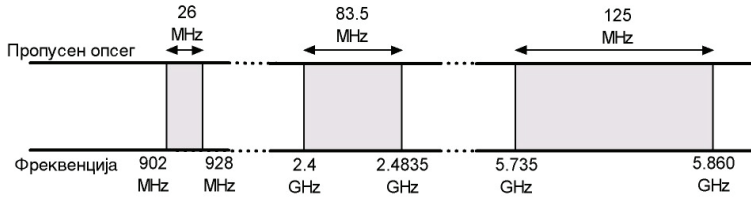
Микробрановата комуникација е во широка употреба за телефонска комуникација на големи растојанија, мобилна телефонија, пренос на телевизиски сигнал и за други намени. Овој начин на безжичен пренос нуди повеќе предности споредено со оптичките кабли: со поставување на микробранови кули на одредени растојанија и со нивно директно комуницирање може да се заобиколи телефонскиот систем. Поставувањето и употребата на микробранов систем е релативно поевтино во однос на

поставување на оптички кабел во урбаната средина, а уште поевтино од изнајмување на оптиката од страна на телекомуникациските компании.

7.1.3 Управување со поделбата на електромагнетниот спектар

За да се одбегне хаосот во начинот на употребата на радио-фреквентниот спектар, постојат национални и интернационални договори. Потребата од повисок пропусен опсег за пренос на податоци, повлекува и користење на поширок фреквентен опсег. Националните влади извршиле доделување на делови од радио спектарот за AM и FM радио, телевизијата и мобилната телефонија, како и за телефонските компании, војската, владата и др.

Еден начин за доделување на фреквенциите од опсегот би било, тие воопшто и да не се доделуваат. Секој вид пренос би бил регулиран според моќноста на емитувањето на станиците и нивниот досег, за да не си пречат еден на друг. Согласно ова, повеќето влади оставија не-управувани одредени фреквентни опсези наречени ISM (Индустриски, Научни и Медицински) за нелиценцирана употреба. За да се минимизира појавата на интерференција, за различните уреди кои емитуваат во овој опсег, FCC наложува тие да ја користат техниката за раширен спектар (spread spectrum).



Слика 7.1: Поделба на електромагнетниот спектар

Положбата на ISM опсезите варираат во различни земји. На пр. во Америка, уредите чија што моќност е под 1W (ват) може да употребуваат опсег на фреквенции прикажани на сликата, без потреба од лиценца од FCC. Фреквенцијата од 900MHz е најдобра, но е пренатрупана и не е секаде достапна. 2.4GHz е во употреба во повеќето земји, но постои појава на пречки предизвикани од микробрановите и радарските инсталациите. Bluetooth и некои од 802.11 безжични LAN мрежи ја употребуваат оваа фреквенција. Преносот на 5,7GHz е сè уште нов и недоволно развиен, така што опремата за користење на истата фреквенција е скапа, но со оглед дека 802.11 ја употребува таа - за кратко време ќе стане многу популарна.

7.1.4 Инфрацрвени и милиметарски бранови

Инфрацрвените и милиметарските бранови се наменети за комуникација на кратки растојанија. Тие се употребуваат за контрола на телевизорите, видео рекордерите VCR, аудио системите. Релативно се евтини, директни и лесни за произведување, но нивниот недостаток е што не ги пробиваат тврдите објекти.

Од друга страна, фактот дека инфрацрвените бранови не преминуваат преку ѕидовите има одредени предности. Имено, системот од инфрацрвени бранови од една соба не може да комуницира со ист таков систем во друга соба (т.е. не може со далечински управувач за телевизор да се управува друг телевизор кој е во друга соба). Со тоа безбедноста на овој систем од прислушување е подобра отколку кај радио системите. Користењето на комуникација во инфрацрвениот спектар не бара лиценца за разлика од радио брановите, но има ограничена употреба во околина на работниот простор за безжично поврзување на компјутери и периферии, но не пошироко во областа на комуникациите.

7.1.5 Светлосен пренос

Преносот на информации со посредство на светлосни сигнали се користел многу одамна. Во поново време се користат насочени кохерентни ласери за поврзување на LAN-овите од два различни објекти сместени на нивните покриви. Користењето на оптичко сигнализирање е строго еднонасочно и насочено, така што и приемната и предајната страна треба да имаат сопствен ласер и сопствен фотодетектор. Овој начин на пренос овозможува висок пропусен опсег за многу ниска цена, со едноставна инсталација при што не е потребна дозвола од страна на FCC.

Предноста на ласерот што се состои од тенок кохерентен зрак, воедно е и негов недостаток во контекст на овој начин на пренос. Насочувањето на ласерскиот зрак широк 1 mm, на далечина од 500 m, бара огромна прецизност, и затоа самиот зрак се дефокусира за да може да се порамни со фотодетекторот од примената страна.

Главниот недостаток се состои во тоа што ласерските зраци не можат да продрат низ дождот или магла, но нормално функционираат во услови на чиста атмосфера. Прекршувањето може да биде предизвикано и од струење на топол воздух, при што може да дојде до осцилации на зракот и прекин на комуникацијата.

7.1.6 Базна станица

Базната станица (наречена хаб - hub или ќелија - cell site) претставува централна локација која го прибира и го дистрибуира сообраќајот од и кон претплатниците во состав на една ќелија. Внатрешната опрема за базната станица се состои од каналски групи (channel groups) кои се поврзуваат кон постоечката мрежа. Нивната основна функција е да бидат радио модем за пренесување на мрежниот сообраќај.

Надворешната опрема на базната станица (Tx/Rx јазол) се наоѓа на носач поставен на покрив или кула и се состои од хардвер за транслација на фреквенции и предаватели и приемници (transmitters/receivers).

Tx/Rx јазолот дистрибуира и прибира сообраќај од и кон претплатниците во една ќелија или сектор. Опремата на Tx/Rx јазолот ги преведува излезите од

каналските групи во соодветна фреквенција за пренос. Повеќе каналски групи се користат во секој сектор за задоволување на барањата со што се обезбедува скалабилна архитектура.

7.1.7 Поделба на безжичните технологии

Групирањето на безжичните технологии може да се изведе и според одредени карактеристики како што се:

- Користен протокол - ATM или IP
- Вид на конекција - Point-to-Point (P2P) или multipoint (P2MP) врски
- Спектар (Spectrum) - Лиценциран или нелиценциран

Безжичниот пренос може да работи во една од двете можни конфигурации: со базна станица или без базна станица. И двата начина на конфигурирање се одредени со 802.11 LAN стандардот, со кој се обезбедува нивна правилна употреба.

7.2 IEEE 802.11 – Безжични локални мрежи

Иако Ethernet е доста популарен, добива своја конкуренција во облик на безжични локални мрежи (Wireless LAN). Безжичните LAN може да работат во една од двете конфигурации: со базна станица и без базна станица. Стандардите со ознака 802.11 LAN ги земаат во предвид и двете конфигурации.

7.2.1 802.11 Протоколен стек

Сите протоколи од фамилијата 802, вклучувајќи го и Ethernet имаат заедничка структура. На сликата е даден преглед на протоколите со ознака и нивната поставеност во однос на трите пониски слоеви на OSI референтниот модел.

Слика 7.2: Множеството на протоколи во IEEE 802.11

Физичкиот слој се совпаѓа со физичкиот слој на OSI, но слојот за податочниот линк (data link layer) во сите 802 протоколи е поделен на два или повеќе подслоја. Во 802.11 подслојот MAC (Medium Access Control) го специфициран начинот на кој се врши доделување на каналот. Над него е поставен подслојот за контрола на логичкиот линк LLC (Logical Link Control), чија задача е да ги прикрие разликите помеѓу варијантите на 802 протоколите и да ги направи такви да не можат да се разликуваат во рамките на мрежниот слој.

802.11 стандардот специфицира три техники на пренос кои се дозволени во мрежниот слој. Инфрацрвениот метод користи многу слична технологија како и далечинскиот управувач за телевизорот. Другите две варијанти користат радио бранови со краток досег, користејќи техники наречени FHSS и DSSS. И двете оперираат во фреквентно подрачје за чие користење не треба дозвола (2,4 GHz ISM), односно во нелиценциран опсег на фреквенции.

Наведените техники работат со брзини од 1 или 2 Mbps. За да се постигнат поголеми брзини на пренос, подоцна се појавиле две нови техники наречени OFDM и HR-DSSS. Тие функционираат со брзини на пренос од 54 Mbps и 11 Mbps соодветно. Во 2001 беше претставена втората верзија на OFDM, која користеше различно фреквентно подрачје од претходната. Сите овие техники се дефинираат за физичкиот слој на протоколите.

7.2.2 802.11 Физички слој

Секоја од петте достапни техники за пренос, овозможува да се испрати MAC рамка од еден јазол кон друг. Тие се разликуваат во технологијата која се користи и брзината што ја постигнуваат при процесот на пренесувањето на податоците.

Инфрацрвената опција користи дифузен пренос (неограничен со линија на видливост). Двете брзини што се овозможени се 1 Mbps и 2 Mbps. При преносот со 1 Mbps се користи шема за кодирање во која група од 4 бита се кодира со 16 бита, од кои 15 се нули, а само една единица, т.н. Грејов код (Gray code). Овој код има својство да исправи мала грешка во временската синхронизација што може да доведе до промена на еден бит во група од 16 бита. На 2 Mbps кодирањето зема два бита и дава 4-битен кодиран збор исто така со една единица, односно еден од зборовите 0001, 0010, 0100, 1000. Инфрацрвените зраци не можат да минуваат низ ѕидови, и со тоа одделени соби се меѓусебно изолирани. Ова решение не е многу популарно за имплементација на безжични мрежи, поради малата брзина на пренесување како и фактот што сончевата светлина има влијание врз нив.

FHSS (Frequency Hopping Spread Spectrum) користи 79 канали од кои секој е широк 1MHz и започнува од долниот крај на 2.4 GHz-ниот ISM интервал. Се користи генератор на случајни броеви за да се произведе секвенцата од фреквенции на кои се врши префрлувањето. Сè додека сите станици ја користат истата шема на генераторот на случајни броеви и се временски

синхронизирани - ќе прескокнуваат симултано на истите фреквенции. Времето поминато на една фреквенција е параметар кој може да се менува, но препорачливо е да биде под 400 msec. Случајноста на FHSS обезбедува начин за подеднакво доделување на одреден спектар во нерегулираниот ISM интервал. Исто така обезбедува и задоволително ниво на сигурност, бидејќи за да натрапник се приклучи во оваа безжична мрежа треба да ја познава секвенцата на фреквенции за префрлување и времетраењето на присуство во одреден фреквентен канал. При пренос на поголеми растојанија може да се појави проблем со слабеењето на сигналот, но FHSS нуди можности за справување со него. Покрај тоа оваа техника е доста отпорна и на радио интерференцијата, па е особено погодна за врски помеѓу оддалечени објекти. Главниот недостаток на оваа модулациска техника е малата брзина на преносот.

Третиот модулациски метод е наречен DSSS (Direct Sequence Spread Spectrum) кој исто така е ограничен на брзини од 1 или 2 Mbps. Секој бит се пренесува како 11 делови, користејќи ја т.н. Баркерова секвенца (Barker sequence). Таа користи фазна модулација на 1 Mbaud и пренесува 1 бит по бауд кога се работи со 1 Mbps, и 2 бита по бауд кога се работи со 2 Mbps.

Првиот стандард за безжични мрежи со голема брзина - 802.11a, користи OFDM (Orthogoal Frequency Division Multiplexing) за да овозможи брзини од 54 Mbps во поширокиот 5 GHz-ен ISM интервал. Како што кажува и самиот термин „Мултиплексирање на поделени фреквенции“ (Frequency division multiplexing), се користат 52 фреквенции, од кои - 48 за податоци и 4 за синхронизација, но не на начинот како ADSL. Бидејќи трансмисиите се одвиваат едновремено на повеќе фреквенции, оваа техника се смета за форма на широк спектар (spread spectrum). Делењето на сигналот во повеќе тесни интервали има неколку предности над користењето на еден широк интервал, вклучувајќи подобра отпорност кон интерференција и можност за користење на неконтинуирани интервали. Се користи сложен кодирачки систем базиран на фазно-поместувачка модулација (phase-shift modulation) за брзини од 18 Mbps па и повеќе. На 54 Mbps, 216 податочни битови се кодираат во 288-битни симболи. Дел од мотивацијата за креирање на OFDM е компатибилноста со европскиот HiperLAN/2 систем. Оваа техника има добра спектрална ефикасност во односот битови/херци (bits/Hz) и добра отпорност на слабеењето на сигналот.

HR-DSSS (High Rate Direct Sequence Spread Spectrum) е уште една техника со широк спектар која постигнува 11 Mbps. Наречена е 802.11b, но не е наследник на 802.11a. Всушност овој стандард беше одобрен прв и прв излезе на пазарот. Брзините на пренос на податоци кои се поддржани со 802.11b се 1, 2, 5.5, и 11 Mbps. Иако 802.11b има послаба пропусност од 802.11a, неговиот домет е околу 7 пати поголем што во многу случаи е значаен фактор за избор на оваа техника за модулација.

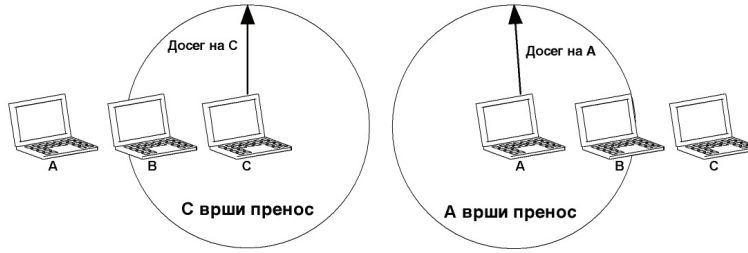
Подобрената верзија на 802.11b, 802.11g беше одобрена од страна на организацијата IEEE во ноември 2001. Таа го користи OFDM модулацискиот метод на 802.11a, но оперира во потесниот 2.4 GHz ISM интервал заедно со

802.11b. Теориски може да постигне брзина на пренос од 54 Mbps, но сè уште не е јасно дали оваа брзина може да се постигне практично.

7.2.3 802.11 MAC протокол

Овој протокол е доста различен од оној што се употребува за Ethernet поради поголемата комплексност на безжичната околина од онаа на жичниот систем. Во Ethernet мрежа, јазолот кој сака да испраќа податоци, ја ослушнува мрежата и чека на момент кога медиумот ќе стане слободен и почнува со трансмисија; ако нема појава на колизија односно не се добие шум во првите 64 бајти од преносот, тогаш преносот е валиден.

Овој принцип во безжичните комуникации не важи. Еден од проблемите на овој тип на комуницирање е проблемот на скриената станица. Бидејќи не сите станици меѓусебно се опфаќаат со својот радио домет, трансмисиите кои се одвиваат во еден дел од ќелијата - може да не се фаќаат во друг дел на ќелијата.



Слика 7.3: а) проблемот на скриената станица, б) проблем на откриената станица

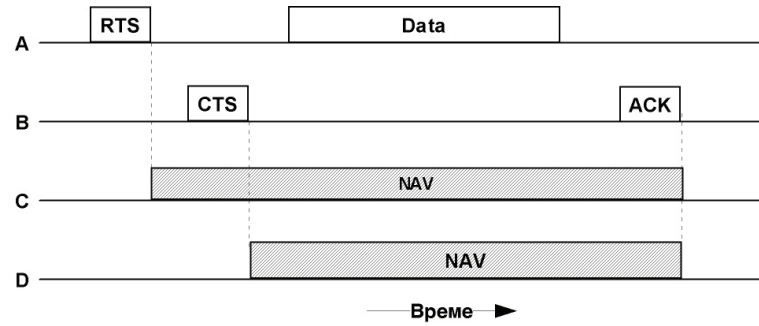
Во овој пример станицата C емитува кон станицата B. Ако станицата A се обиде да прати нешто - го ослушнува тој канал и нема да чуе ништо, па погрешно ќе заклучи дека B е слободен и дека може да емитува податоци кон него. Постои и обратниот проблем, кога B сака да емитува кон C и ослушнува на каналот, но погрешно заклучува дека нема да може да испрати податоци, иако A може да емитува кон D-станицата која не е прикажана на сликата. Освен тоа, повеќето радио уреди се такви што не можат истовремено да емитуваат и детектираат шум на една фреквенција.

За да се справи со овој проблем, 802.11 поддржува два вида на функционирање: првиот - DCF (Distributed Coordination Function) не користи било каков вид на централна контрола. Вториот наречен PCF(Point Coordination Function) ја користи базната станица за да ја контролира целата активност во својата ќелија.

Кога се употребува DCF, 802.11 користи протокол наречен CSMA/CA (CSMA with Collision Avoidance). Во овој протокол се врши прислушување и на физичките и на виртуелните канали. Два методи на работа се поддржани од CSMA/CA. Во првиот метод, кога станицата сака да емитува таа слуша на

каналот. Ако нема никаков пренос во тој момент едноставно започнува со емитувањето и притоа не го ослушнува на каналот, при што ја емитува целата своја рамка која може да биде уништена кај примачот поради интерференција.

Ако каналот е зафатен, испраќачот се повлекува сè додека не се ослободи. Ако се случи колизија, станиците кои се одговорни за овој настан чекаат временски интервал со случајно траење користејќи го бинарниот Ethernet експоненцијален алгоритам за отстапување и после тоа повторно се обидуваат. Другиот начин на CSMA/CA се базира на MACAW и користи ослушнување на виртуелните канали како што е прикажано на долната слика.



Слика 7.4: Ослушнување на виртуелниот канал со користење на CSMA/CA

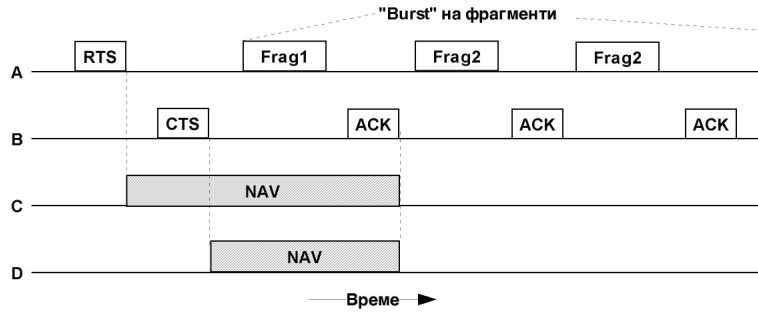
Во овој пример A сака да испрати податоци на B. C е станица во дофат на A (може да е и во дофат на B, но тоа не е битно). D е станица во дофат на B, но не е во дофат на A. Протоколот започнува кога A одлучува да испрати податоци на B. Тоа го прави со испраќање на RTS (Request to Send) рамка на B, за да добие дозвола да испрати рамка со податоци на B. Кога B ќе го добие ова барање, може да даде дозвола со тоа што ќе испрати CTS (Confirm to Send) рамка назад до A. По приемот на CTS рамката, A ја испраќа својата рамка и стартува ACK бројач. По правилниот прием на податочната рамка, B одговара со ACK (Acknowledge) рамка со што ја прекинува размената. Ако ACK бројачот на станицата A достигне некоја максимална вредност пред да стигне ACK рамката од B, целиот процес се повторува од почеток.

Размена од гледна точка на C и D: C е на дофат на A па може да ја добие RTS рамката испратена за B. Ако ја добие, сфаќа дека некој во скоро време ќе врши испраќање на податоци, па за доброто на сите се откажува од емитување било што сè додека на заврши размената. Од информациите во RTS рамката може да предвиди колку долго ќе трае размената вклучувајќи ја и крајната ACK рамка. Затоа поставува еден вид виртуелен канал “зафатено” на себе, кој е означен со NAV (Network Allocation Vector). Станицата D не ја детектира RTS рамката, но ја препознава CTS рамката од B, па исто како и C се поставува во виртуелен канал “зафатено”. Треба да се забележи дека NAV

сигналот не се емитува, тој е само внатрешен потсетник за да се паузира одредено време.

Безжичните мрежи се доста склони на грешки во преносот. Ако веројатноста еден бит да е погрешен е p, тогаш веројатноста да една рамка од n бита биде примена целосно исправна е $(1-p)^n$. Може да се каже дека ако една рамка е подолга, таа има многу мали шанси да се пренесе неоштетена, и најверојатно ќе треба да се повтори преносот.

За да се справи со шумот кој се јавува во каналите за пренос, 802.11 стандардот овозможува рамките да се фрагментираат на помали делови секој со свои податоци за корекција. Фрагментите индивидуално се нумерираат и проверуваат користејќи "запри и чекај" протокол (на пр. испраќачот не може да го испрати фрагментот к+1 сè додека на добие потврда за фрагментот број к). Откако каналот е ставен во употреба користејќи RTS и CTS, повеќе фрагменти може да се испратат по ред како што е прикажани на сликата.



Слика 7.5: „Брст" на фрагменти

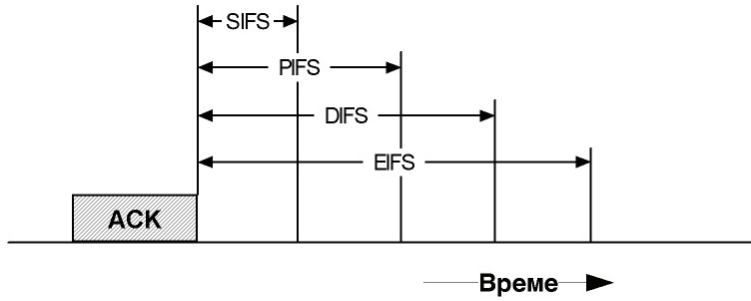
Фрагментацијата ја зголемува пропусноста, бидејќи во случај на неуспешен пренос се пренесува повторно само оштетениот фрагмент, а не целата рамка. Големината на фрагментот не е фиксно одредена со стандардот туку е променлива и може да се контролира преку базната станица.

Во 802.11 DCF модот, нема централна контрола и секоја станица се натпреварува за да добие простор за пренос преку каналот, исто како и за Ethernet. Во другиот мод PCF, базната станица ги контролира другите станици, така што ги прашува дали имаат податоци за испраќање. Со оглед на тоа што преносот комплетно се контролира од базната станица - никогаш нема да дојде до интерференција. Стандардот го опишува механизмот за распоредување, но не и фреквенцијата, редоследот и дали станиците треба да добиваат еднакво време за користење на каналот.

Основниот механизам е базната станица да емитува сигнална рамка периодично (секој 10 до 100 пати во секунда). Сигналната рамка содржи системски параметри како фреквенциите на кои се скока, синхронизација на станиците итн.

PCF и DCF можат да коегзистираат во рамките на една ќелија, бидејќи 802.11 стандардот го предвидува и овозможува тоа. Функционира со

внимателно дефинирање на меѓурамковниот временски интервал. Откако е испратена една рамка со податоци, потребно е одредено време на неактивност пред било која станица да испрати нешто. Четири различни интервали се дефинирани - секој со специфична намена. Овие интервали се прикажани на сликата 7.6.



Слика 7.6: Простор меѓу рамките во 802.11

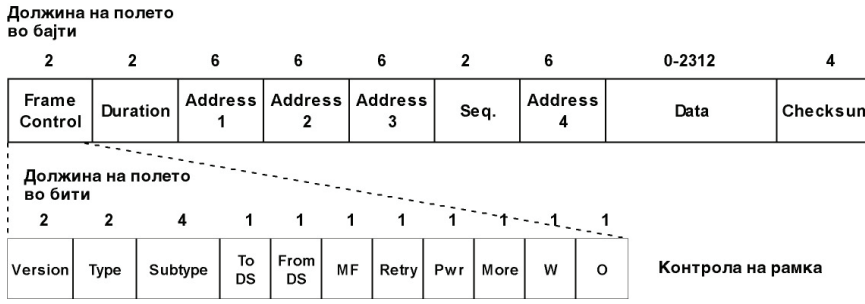
Најкраткиот интервал е SIFS (Shortest interframe spacing). Се користи да им овозможи на уредите кои водат дијалог, да им се даде шанса некој да започне прв. Ова вклучува дозвола примачот да испрати CTS како одговор на RTS, да испрати ACK за фрагмент или за цела податочна рамка, како и дозвола на испраќачот да испрати нова низа на фрагменти, без да испраќа повторно RTS.

Има точно една станица која треба да одговори после SIFS интервалот, ако не успее да ја искористи својата шанса и времето одредено со PIFS (PCF interframe spacing) помине, базната станица може да испрати сигнална рамка или повикувачка рамка.

Ако базната станица нема што да каже и времето одредено со DIFS (DCF Interframe spacing) помине, било која станица може да се обиде да го заземе каналот за да испрати нова податочна рамка. Последниот временски интервал EIFS (Extendet interframe spacing) се користи за да станицата која добила оштетена рамка го пријави тој проблем.

7.2.4 Структура на рамките на 802.11 стандардот

802.11 стандардот дефинира три различни класи на рамки: податочни, контролни и управувачки. Секоја од овие рамки има заглавје со најразлични полиња кои се користат во склоп на MAC подслојот. Форматот на податочната рамка е прикажан на следнава слика.



Слика 7.7: Податочна рамка кај 802.11

Најпрво е полето за контрола на рамката (Frame control) кое содржи 11 потполиња. Второто поле (Duration) е полето кое кажува колку рамката и потврдата за нејзиниот прием ќе го зафатат каналот. Следни се четирите полиња за адреси - сите во стандарден IEEE 802 формат. Другите две адресни полиња се за почетната и крајната база за комуникација помеѓу ќелиите.

Полето секвенца (Sequence) овозможува фрагментите да се нумерираат. Од 16 бита кои се на располагање, 12 ја идентификуваат рамката, а 4 бита го идентификуваат фрагментот. Полето Data ги содржи податоците кои треба да се пренесат заедно со вообичаената сума за проверка CheckSum.

Рамките за управување имаат слична структура со податочните рамки, освен што ги немаат двете адресни полиња за почетна и крајна базна станица.

Контролните рамки се уште пократки. Имаат едно или две адресни полиња, а немаат поле за податоци и поле за секвенца.

7.2.5 Сервиси

802.11 стандардот кажува дека секоја безжична мрежа, за која може да се каже дека е стандардизирана, мора да обезбеди девет сервиси. Овие сервиси се поделени во две категории: 5 дистрибутивни сервиси и 4 сервиси за станиците. Дистрибутивните сериски се користат за регулирање на припадноста кон одредена ќелија и интеракција со станиците кои се надвор од ќелијата. Спротивно на ова - сервисите наменети за станици се користат за активности во рамките на една ќелија.

Петте дистрибутивни сервиси се обезбедуваат од базната станица и се справуваат со мобилноста на станиците, како што тие влегуваат и ја напуштаат станицата, при што се приклучуваат на една, а исклучуваат од друга станица. Еве ги по ред:

1. Асоцијација – овој сервис се користи од мобилните станици за да се приклучат на базните станици.
2. Дисасоцијација – станицата или базната станица може да се дисасоцира, односно да ја прекине врската.

3. Реасоцијација – станицата може да ја промени својата базна станица користејќи го овој сервис.
4. Дистрибуција – овој сервис одредува како да се рутираат рамките испратени кон базната станица.
5. Интеграција – ако рамката треба да биде испратена преку не-802.11 мрежа, со друга адресна шема или формат на рамките, овој сервис се грижи за конвертирањето од 802.11-формат во формат што го бара одредишната мрежа.

Следните четири сервиси се користат откако ќе се изврши асоцијација:

1. Идентификација – бидејќи во безжичната комуникација може лесно да се испратат или примат податоци од неавторизиран корисник, станицата мора да се идентификува себеси за да може да испраќа и прима податоци.
2. Исклучување – кога претходно идентификувана станица сака да ја напушти мрежата - таа се деавторизира, после што не може да ја користи мрежата.
3. Приватност – за доверливите информации испратени преку безжична мрежа да бидат сигурни, тие мора да се енкриптираат. Овој сервис се грижи за енкрипцијата и декрипцијата.
4. Пренос на податоци – конечно ова е сервис што служи за пренесување на податоците.

Безжичните мрежи сè повеќе се користат во канцелариите, аеродромите, хотелите, ресторaните и многу други места, каде што безжичното комуницирање има предности над другите техники на поврзувања.

7.3 IEEE 802.16 - Широкопојасен безжичен пристап

Широкопојасниот безжичен пристап (Broadband wireless access - BWA) станува најдобар начин за да се задоволи брзо-растечката побарувачка на Интернет сервиси, интегрираните податочни, говорни и видео сервиси. BWA може да ги прошири постојните оптички мрежи и да обезбеди поголем капацитет од досегашните кабелски мрежи или дигиталните кориснички линии (DSL).

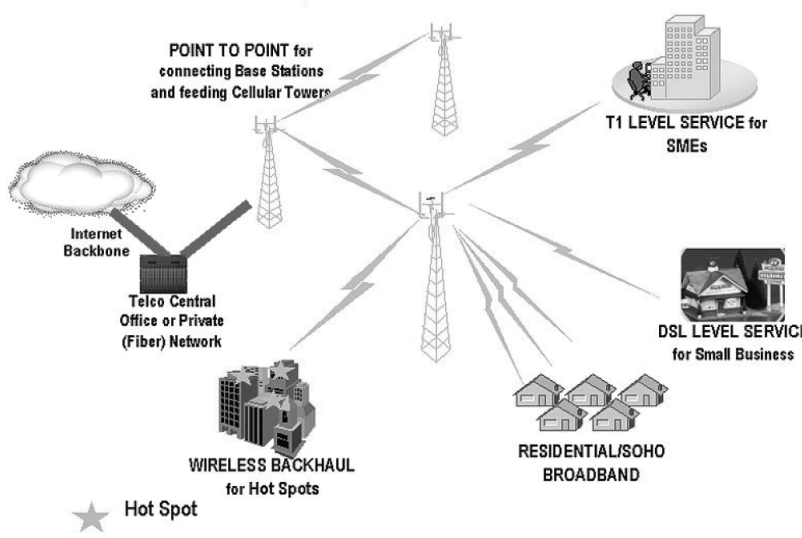
Асоцијацијата за стандардизација при IEEE го има објавено стандардот IEEE 802.16, кој специфицира безжичен MAN воздушен интерфејс за безжична MAN (WirelessMAN Air Interface for wireless metropolitan area networks). Стандардот популарно е наречен WiMax (Worldwide Integration for Microwave Access). IEEE 802.16 фокусира на ефикасно искористување на опсегот помеѓу 10 и 66 GHz, како и опсегот помеѓу 2 и 11 GHz (на точка до повеќе точки) и опционална Mesh (секој со секој) топологија. Второто фреквентно подрачје, 2 - 11 GHz, како и Mesh топологијата се покриени со стандардот IEEE 802.16a.

Табела 7.1. Преглед на карактеристиките на 802.16 стандардот

	802.16	802.16a	802.16e
Комплетиран	Декември 2001	Јануари 2003	во изработка
Спектар	10 -66 GHz	<11 GHz	<6 GHz
Состојба на каналот	LOS	NLOS	NLOS
Битски проток	32-134 Mbps на 28MHz канал	до 75 Mbps на 20MHz канал	до 15 Mbps на 5MHz канал
Модулација	QPSK, 16QAM, 64QAM	OFDM 256субносители QPSK, 16QAM, 64QAM	како и 802.16a
Мобилност	фиксна	фиксна	Мобилност на пешак – Регионален Роаминг
Ширина на канал	20, 25,28 MHz	Селективен опсег на канал помеѓу 1.25 и 20 MHz	исто како 802.16a со UL подканализација
Радиус на клетка	до 70 km	до 9 km max домет до 50 km, базирано висината на антената и енергијата на трансмисија	до 5km

Стандардот 802.16, освен физичкото ниво го дефинира и нивото за контрола на медиумот (medium access control - MAC), кое поддржува повеќе спецификации за физичкото ниво, т.е. за фреквентното подрачје што се користи. Стандардот за подрачјето 11 - 66 GHz поддржува нивоа на сообраќај со варијабилен проток на многу лиценцирани фреквентни подрачја (на пример 10.5, 25, 26, 31, 38 и 39 GHz) за двонасочна комуникација. Тој овозможува интероперабилност помеѓу уредите, со што може да се користи опрема од повеќе производители, а со тоа е загарантирана можноста за пониска цена на опремата. Подетален преглед на карактеристиките на стандардот се дадени во Табелата 7.1.

Системите, пак, базирани на IEEE стандардот 802.16 BWA нудат различни „broadband“ сервиси, кои овозможуваат илјадници корисници да делат капацитет за податочни, говорни и видео сервиси; исто така имаат скалабилни капацитети и протоци, и можат да се зголемуваат по барање на корисниците за поголем проток со додавање на канали или ќелии.



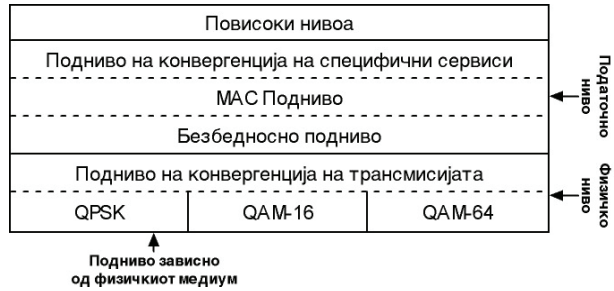
Слика 7.8. WiMAX секаде

BWA се емитува низ слободниот воздушен простор и е предмет на слабеење и дисторзија од различни причинители, како што се вегетацијата, зградите, врнежи, одрони и возила, кои се движат и менуваат непредвидено. IEEE стандардот 802.16 ги препознава овие пречки и постојат механизми за изработка на системи за PMP BWA со оптичка видливост (LOS). Трансмисиите со попречена оптичка видливост и оние кои немаат оптичка видливост (NLOS) се разгледани и стандардизирани во амандманот 802.16a. Механизмите на Wireless MAN MAC-нивото, овозможуваат различни QoS кои поддржуваат различни потреби на различните апликации. На пример, говорот и видеото бараат мало доцнење, но толерираат одредено ниво на грешка. Од друга страна, некои апликации не толерираат грешка, а доцнењето за нив не е критично. Стандардот ги опслужува говорните, видео и другите податочни трансмисии со користење на соодветни решенија во MAC нивото, кои се поефикасни од решенијата во нивоа над MAC нивото. Во првичното сценарио со безжичната MAN технологија, дефинирана во IEEE 802.16 стандардот, се обезбедува пристап на мрежата до зградите со надворешни антени кои комуницираат со централна базна станица - BS. Корисниците внатре во зградите се поврзани со конвенционални мрежи како што се Ethernet (IEEE 802.3) или безжичен LAN (IEEE 802.11).

7.3.1 Протоколен стек на 802.16

Протоколниот стек на 802.16 е илустриран на сликата 7.9. Општата структура е слична на другите 802 мрежи, но постојат повеќе подслоеви. Долниот подслој се справува со преносот. Користено е традиционално радио со тесен пропусен опсег со конвенционални модулациони шеми. Над

физичкиот слој се наоѓа еден конвергентен подслој наменет да ги прикрие различните технологии од слојот на податочната врска.



Слика 7.9: Протоколен стек на 802.16

Се работи на тоа да се додадат два нови протоколи од физичкиот слој. Стандардот 802.16a ќе поддржува OFDM во доменот 2-11G Hz. Стандардот 802.16b ќе функционира во доменот 5 GHz на ISM опсегот. Слојот на податочната врска се состои од три подслоеви. Долниот се справува со приватноста и сигурноста, што е многу поважно за јавни надворешни мрежи, отколку за приватни внатрешни мрежи. Управува со криптирањето, декриптирањето и клучевите.

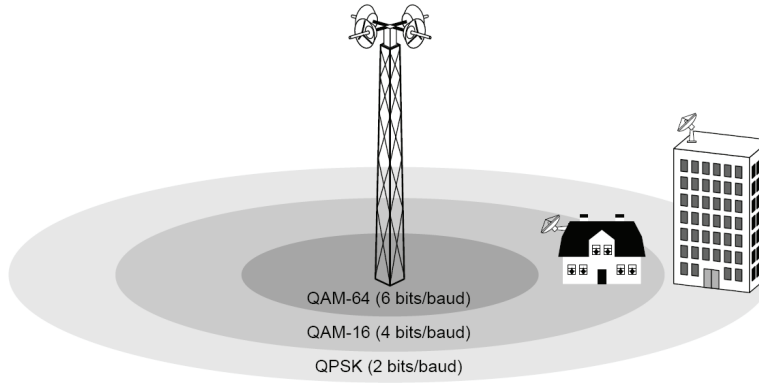
Над него се наоѓа заедничкиот дел на MAC подслојот. Тука се сместени главните протоколи. Во моделот е дефинирано базната станица да го контролира системот. Може да ги распоредува каналите на надолниот поток (т.е. база - корисник) и игра голема улога во управувањето со каналите на нагорниот поток (т.е. корисник - база). Една необична особина на MAC слојот е тоа што за разлика од тие на 802 мрежите, тој е целосно конекциски ориентиран, со цел да овозможи гаранција за квалитетен сервис за телефонија и мултимедијална комуникација.

Подслојот за конвергенцијата специфициран за сервиси, го зазема местото на подслојот за логичка врска во другите 802 протоколи. Неговата функција е да посредува со мрежниот слој. Проблемот е што 802.16 беше дизајнирана лесно да се интегрира со дијаграм протоколи (пр. PPP, IP и Ethernet) и ATM. Исто така, постои проблем: пакетските протоколи се без-конекциски, а ATM е конекциски ориентиран. Ова значи дека секоја ATM врска мора да се пресликува на врска со 802.16, тоа е задача на овој подслој.

7.3.2 Физичкиот слој на 802.16

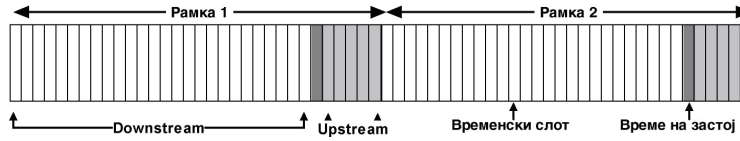
Големата безжична мрежа бара широко фреквентно подрачје и единствено место каде што може да се најде тоа е опсегот на фреквенции од 10-66GHz. Овие милиметарски бранови имаат интересна особина што ја немаат подолгите микробранови: тие патуваат по прави линии, на различен начин од простирањето на звукот, но слично со простирањето на светлината. Како последица на оваа карактеристика, базната станица може да има повеќе

антени, секоја насочена кон одделен сектор на околниот терен, како што е покажано на слика. Секој сектор има свои корисници и е независен од соседните сектори, нешто што не е важи за целуларно радио кое е насочено во сите правци.



Слика 7.10: Околина на трансмисија на 802.16

Бидејќи моќноста на сигналот во милиметраскиот опсег брзо опаѓа со оддалечување од базната станица, односот сигнал-шум исто така опаѓа со оддалечување од базната станица. Заради оваа причина - 802.16 употребува три шеми за модулација, зависно од оддалеченоста на корисничката станица од базната. За блиските корисници се користи QAM-64 со 6 bits/baud. За корисници на средна далечина се користи QAM-16 со 4 bits/baud. За оддалечени корисници се користи QPSK со 2bits/baud. На пример, за типична вредност од 25 MHz спектар, QAM-64 дава 150 Mbps, QAM-16 дава 100 Mbps и QPSK дава 50 Mbps. Со други зборови - што подалеку од корисникот - толку е помала брзината на пренос на податоци (слично како кај ADSL). Земајќи ја предвид целта за создавање на систем за широк пропусен опсег и земајќи ги предвид физичките ограничувања, дизајнерите на 802.16 работеа напорно да го искористат ефикасно достапниот фреквентен опсег. 802.16 нуди еден пофлексибилен начин за поделба на пропусниот опсег. Се користат две шеми, удвојување на фреквентната поделба -FDD (Frequency Division Duplexing) и удвојување на временската поделба - TDD (Time Division Duplexing). Последното е илустрирано на сликата. Прикажано е како базната станица периодично испраќа рамки, и секоја рамка содржи временски слотови. Првите неколку слотови се за надолна комуникација. Потоа доаѓа времето на застој (сталожување), за да станицата изврши промена на насоката на пренос, па потоа идат слотови за нагорна комуникација. Бројот на временските слотови доделени на секоја насока на пренос, може динамички да се измени за да се совпаѓа со пропусниот опсег во секоја насока на комуникацијата.



Слика 7.11: Рамки и временски слотови за „time division duplexing“

Надолната комуникација е пресликувана во временските слотови од базната станица. Базната станица има целосна контрола на оваа насока. Нагорната комуникација е покомплексна и зависи од квалитетот на сервисот што се бара. Треба да се спомне и користењето на Хаминговиот код, кој прави корекции на грешки нанапред во физичкиот слој. Скоро сите други мрежи се потпираат на проверка на сумата за да откријат грешки и да го повторат преносот при погрешно предавање на рамките. Но во широкопојасните безжични мрежи, се очекува појава на грешки и затоа нивната корекција е вградена во физичкиот слој, како додаток на механизмот за проверка на суми во повисоките слоеви. Вкупниот ефект на корекција на грешки е да се направи каналот да изгледа подоверлив одошто е.

Со стандардот IEEE 802.16, во делот што се однесува на физичкото ниво, е обработено фреквентното подрачје од 10 до 66 GHz, додека со амандманот 2, кој е означен како 802.16a е обработено фреквентното подрачје од 2 до 11 GHz.

- 10-66 GHz – во дизајнот на физичката спецификација за ова подрачје претпоставено е дека пропагацијата на сигналот е помеѓу системи со оптичка видливост (LOS) во лиценцирано фреквентно подрачје. Изберена е модулацијата со еден носител (single carrier modulation). Воздушниот интерфејс е означен како “WirelessMAN-SC”. Бидејќи архитектурата е точка до повеќе точки (PMP), базната станица испраќа TDM сигнал, кој е составен од сериски одредени временски слотови - за секоја од корисничките станици. Во обратната насока - од SS до BS, пристапот е со TDMA (Time Division Multiple Access). Овој стандард овозможува дуплекс со временска поделба TDD, во кој примањето (downstream) и праќањето (upstream) делат ист канал (но не симултано), и дуплекс со фреквентна поделба FDD, во кој примањето и праќањето се одвива на различни канали (понекогаш симултано). Овој „burst“ дизајн дозволува двете TDD и FDD на сличен начин да бидат управувани. Постои поддршка и за полу-дуплекс FDD кориснички станици.
- 2-11 GHz – овој опсег се однесува за лиценцирани и нелиценцирани фреквентни подрачја, а е специфициран со стандардот 802.16a. Стандардот е развиен следствено на потребата за системи каде не постои оптичка видливост (NLOS). Ова може да се случи поради некои пречки, како што се повисоките дрва (или можеби локацијата каде се инсталира антената се наоѓа премногу ниско). Инсталацијата на надворешна антена (out-door antenna) е поскапа од онаа која може

да се инсталира внатре (in-door), ако нема потреба од потребна оптичка видливост. Амандманот 802.16a ја отвора можноста за поголеми промени во спецификациите на физичкото ниво кои ќе се однесуваат на подрачјето од 2 - 11 гигахерци. Ова е постигнато со воведување на три нови спецификации за физичкото ниво:

- WirelessMAN-SC2: користи формат на модулација со еден носител.
- WirelessMAN-OFDM: користи мултиплексирање со ортогонална фреквентна поделба со трансформација на 256 точки. Овој интерфејс е наменет за нелиценцирани фреквентни подрачја.
- WirelessMAN-OFDMA: користи повеќекратен пристап со ортогонална фреквентна поделба со трансформација на 2048 точки. Во овој систем, повеќекратниот пристап е обезбеден со адресирање на подмножество на повеќе носители до индивидуални приемници.

Предностите на физичкото ниво во 802.16a, што овозможуваат робусни перформанси во широкопојасна околина со канали, се: флексибилната ширина на канали, адаптивните „burst“профили, напредна корекција на грешка со конкатенациско Reed-Solomon и конволуциско кодирање, опциони напредни антенски системи AAS (advanced antenna systems) со кои се зголемува дометот и капацитетот, динамичко селектирање на фреквенции DFS (dynamic frequency selection) кое помага за минимизирање на интерференцијата, просторно-временско кодирање STC (space-time coding) кое ги зголемува перформансите во околината со придушување.

7.3.3 IEEE 802.16 MAC протокол

IEEE 802.16 MAC протоколот е дизајниран за широкопојасен безжичен пристап, за пренесување од точка до повеќе точки. Стандардот ги задоволува потребите за многу високи битски протоци во двете насоки, за праќање (upstream) кон BS, како и за примање (downstream) од BS. Алгоритамите за пристап и доделување на фреквентен опсег мораат да сместат стотици терминали по канал, и тоа терминали кои можат да бидат поделени на повеќе крајни корисници.

Сервисите побарувани од овие крајни корисници се најразлични по нивната природа и вклучуваат мултиплексиран со временска поделба (TDM), говорен и податочен пренос, поврзување со Интернет протокол (IP), како и пакетски говор преку Интернет протокол (VoIP). За да ги поддржи овие најразлични сервиси - стандардот 802.16 MAC мора да ги поддржува и двата, постојаниот од една страна, како и краткиот и брз (bursty) сообраќај. Додатно, овие сервиси очекуваат да бидат поврзани со одреден квалитет на сервис (QoS) кој ќе го задржи потребниот тип на сообраќај.

Стандардот 802.12 MAC обезбедува многу типови на сервиси аналогно на класичниот асинхрон трансфер мод (ATM), како и на поновите категории,

како што е гарантираниот проток на рамки (GRF). 802.12 MAC протоколот ги поддржува и различни додатни побарувања, вклучувајќи ги асинхрониот начин на пренос (ATM) и пакетски-базираните протоколи. Конвергентните поднивоа се употребуваат за да ги означат спецификите за сообраќај на транспортниот слој од MAC-нивото, кое е доволно флексибилно за ефикасен пренос на било каков тип на сообраќај. Поради ваквите карактеристики (суспензија на товарот на заглавјето /header, пакување, фрагментација), конвергентните поднивоа и MAC нивото работат заедно за да пренесуваат сообраќај во форма што е многу поефикасна од оригиналните транспортни механизми.

Ефикасноста на транспортот исто така се помага и од интерфејсот помеѓу MAC нивото и физичкото ниво PHY. На пример, модулацијата и шемите за кодирање се специфицирани со „burst“ профил, кој може да биде нагоден за секој „burst“ до секоја корисничка станица SS. MAC може да го искористи ефикасно фреквентниот опсег на „burst“ профилот под погодни услови на линкот, но и да го направи понадежен за сметка на ефикасноста. На тој начин се искористува расположливоста на линкот до планираните 99.999 проценти.

Механизмот побарај-одобри (request-grant) е дизајниран да биде скалабилен, ефикасен и сам да се поправа (self-correcting). Системот за пристап на 802.16 не губи од својата ефикасност кога постојат повеќекратни конекции по терминал, повеќе нивоа на QoS по терминал и голем број на статистички мултиплексирани корисници. Самиот 802.16 MAC има предности поради широката различност на механизми за барање (request mechanisms), и балансирањето на стабилноста на неконекциски-ориентираниот (contentionless) пристап со ефикасноста на конекциски-ориентираниот (contention-oriented) пристап.

Слојот на податочната врска е поделен на три подслоја. Криптирањето овозможува заштита на податоците што се пренесуваат, при што само податоците во рамките се криптирани, но не и заглавјата. Тоа значи дека евентуалниот натрапник може да ги дознае јазлите кои комуницираат, но не и содржината на комуникацијата. MAC рамките заземаат интегрален број на временски слотови на физички слоеви. Секоја рамка е составена од подрамки, од кои првите две се пресликувањата на надолниот и нагорниот поток. Овие пресликувања кажуваат што има во кој временски слот и кој временски слот е слободен. Базната станица обично одлучува што да стави во која подрамка. Нагорниот канал е покомплициран, бидејќи постојат натпреварувачки и некоординирани корисници што имаат потреба за пристап, и неговата поделба е тесно поврзана за квалитетот на сервисот.

Дефинирани се четири класи на сервиси:

- сервис со константна рата на битови,
- сервис со променлива рата на битови во реално време,
- сервис со променлива рата на битови - не во реално време,
- сервис Најдобар Обид.

Сите сервиси на 802.16 се конекциско-ориентирани, и секоја конекција зазема една класа од наведените сервиси при воспоставување на врската. Овој дизајн во суштина се разликува од тој на 802.11 или Ethernet, кои немаат воспоставување на конекции во MAC подслојот.

Сервисот со константна рата на битови е направен за пренос на некомпресиран звук како на пример преку T1 канал. Овој сервис треба испрати предодредено множество на податоци во предодредени интервали на време. Се прилагодува со доделување на одредени временски слотови на секоја конекција од овој тип. Кога е доделен пропусен опсег, временските слотови автоматски стануваат достапни, без потреба да се побарува секој поединечно.

Сервисот со променлива рата на битови во реално време е прилагоден за пренесување на компресирана мултимедија и други апликации во реално време во кои пропусниот опсег што е потребен во одреден временски интервал може да варира. Се прилагодува со повикување на базната станица од корисникот во определени фиксни интервали за добивање на информација за потребниот пропусен опсег.

Сервисот со променлива рата на битови што не работи во реално време, се користи при големи преноси кои не се во реално време, како што е пренесување на големи датотеки. За овој сервис базната станица го повикува корисникот, но не во определени предефинирани интервали. Константната рата на битови може да постави бит на некој од своите рамки, барајќи повик за испраќање на дополнителни податоци.

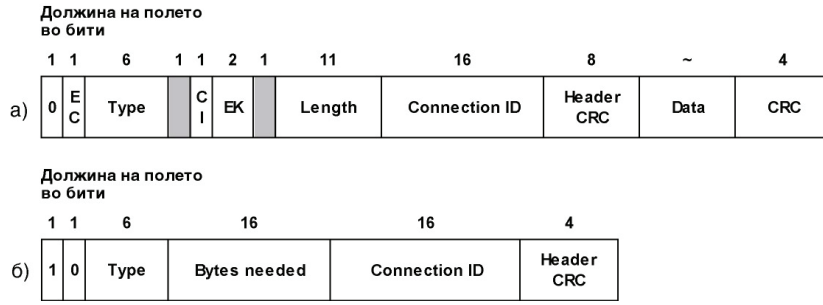
Ако станицата не одговари на повикувањето к-пати по ред, базната станица ја става во мултикаст групата и му го одзема неговиот личен повик. Наместо тоа - кога мултикаст група е повикана, било која од станиците во неа можат да одговарат, натпреварувајќи се на овој начин, а станиците кои помалку комуницираат не ја губат можноста за примање на повикувањата од базната станица.

Сервисот за најдобар обид се однесува за сите други случаи кои не се опфатени со претходните три. Не постои повикување на корисникот и тој мора да се натпреварува за доделување на пропусен опсег со другите корисници. Барањата за комуникација се испраќаат во временските слотови од нагорниот поток, означени како достапни за натпревар. Ако едно барање е успешно - неговиот успех ќе се запише во подолниот поток. За да се минимизираат судирите се користи алгоритам за отстапување од испраќањето како кај Ethernet.

Стандардот дефинира две форми на доделување на пропусниот опсег: за станица и за врска. Во првиот случај - корисничката станица ги прибира сите потреби на корисниците во зградата и прави колективно барање до сите нив. Кога му е доделен пропусен опсег, на секој корисник ми се дава дел од опсегот соодветно на неговите потреби. Во вториот случај базната станица директно управува со секоја конекција.

7.3.4 Структурата на рамките кај 802.16 стандардот

Сите MAC рамки започнуваат со генеричко заглавие, кое е следено со една опционална содржина (payload) и опционално CRC, како што е илустрирано на сликата. Дополнителни податоци не се потребни во контролните рамки, на пример кај тие што побаруваат каналски слотови. Проверката на сума е исто така опционална, заради постење на механизам за корекција на грешки имплементиран во физичкиот слој и фактот дека никогаш не се врши ретрансмисијата на рамките во реално време.



Слика 7.12: а) Генеричка рамка, б) рамка за барање на пропусен опсег

Рамките се составени од заглавја со следниве полиња:

- EC-битот кажува дека содржината е криптирана.
- Type го дефинира типот на рамката со што кажуваме дали има пакување или фрагментација.
- CI индицира присутност или отсутност на конечната сума.
- EK кажува кој клуч за криптирање е потребен, ако воопшто се употребува.
- Length ја дава целата должина на рамката, вклучувајќи го и заглавјето.
- Connection Identifier кажува на која конекција и припаѓа оваа рамка.
- Header CRC полето е сума на заглавјето, само користејќи го полиномот $x^8 + x^2 + x + 1$.

Форматот на другиот тип на заглавја, (за рамките со кои се побарува пропусен опсег) е прикажан на сликата, започнува со 1 бит наместо со 0 бит и е сличен на генеричкото заглавје, само што вториот и третиот бајт формираат 16-битен број кој кажува колкав пропусен опсег е потребен за пренос на специфицираниот број на битови. Рамката за барање на пропусен опсег не носи содржина, ни CRC за целата рамка.

7.4 BLUETOOTH

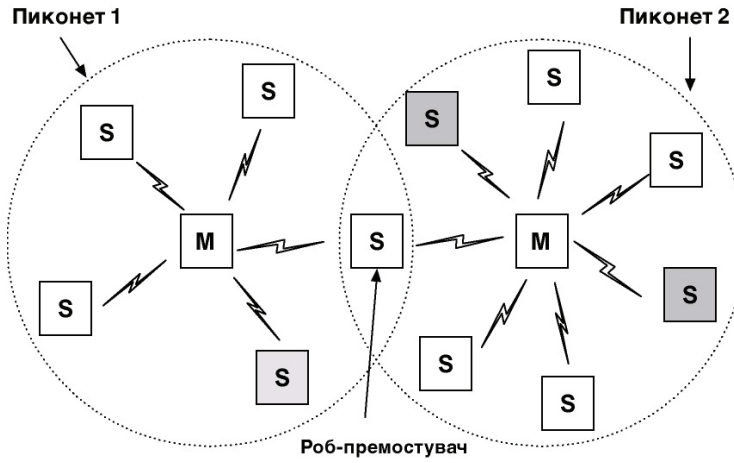
Во 1994 год. L.M. Ericsson Company се заинтересирала за можноста за поврзување на мобилните телефони со други апарати (како PDA), без употреба на кабли. Проектот бил наречен Bluetooth. Оригиналната идеја била само да се исфрлат каблите од употреба, но набрзо истражувањата се проширила и во областа на безжичните LAN мрежи. Со тоа стандардот станал покорисен, а истовремено довел до зголемување на конкуренцијата.

Набрзо потоа IEEE групата за стандарди ја прифатила документацијата за Bluetooth основата за безжичен стандард. Bluetooth спецификацијата се однесува на комплетниот систем, од физичкото ниво до апликативното ниво. IEEE 802.15 групата ги стандардизирала само физичкото и податочно ниво, додека остатокот од протоколот отпаѓа надвор од нивните ингеренции.

7.4.1 Bluetooth архитектура

Основата на Bluetooth системот е „piconet“, кој се состои од главен јазол и од 7 јазли робови (slave) на растојание од 10 метри. Во една соба може да бидат повеќе „piconet“ мрежи и дури тие да бидат поврзани заедно. Интерконекцијата меѓу повеќе „piconet“ мрежи се нарекува „scatternet“.

Во дополнение на седумте јазли “робови”, може да постојат до 255 паркирани јазли во мрежата. Овие паркирани јазли всушност претставуваат исклучени т.е. јазли префрлени да работат на пониско ниво на напојување со цел да ги зачувуваат батериите. Во паркирана состојба, уредите можат само да одговорат на сигналот за активација од главниот јазол (господарот). Постојат уште две состојби на работа hold и sniff, но тие не се многу важни во однос на функционирањето на безжичните врски.



Слика 7.13: Поврзување на два „piconet“-а за креирање на „scatternet“

Причината за принципот господар-роб настанал, бидејќи дизајнерите сакале обезбедат имплементација на целосните Bluetooth чипови за што пониска цена. Резултатот на таа одлука е што робовите го прават тоа што ќе им наложи мастерот. Piconet е централизиран TDM систем. Господарот го користи часовникот и одредува кој уред ќе ја добие комуникацијата во даден временски интервал. Директната комуникација slave-slave не е возможна, бидејќи имаме само комуникација помеѓу master и slave.

7.4.2 Примени на Bluetooth

Повеќето мрежни протоколи овозможуваат канали за комуникација и им оставаат на дизајнерите на апликации да одлучат за што ќе ги користат. Bluetooth V1.1 спецификацијата набројува 13 специфични апликации кои се поддржани и овозможува посебни протоколи за секој од нив.

Табела 7.2: Bluetooth профили

Име	Опис
Generic Access	Процедура за управување со линкот
Service Discovery	Протокол за откривање на достапните сервиси
Serial port	Замена за сериски порт
Generic Object Exchange	Дефинира клиент-сервер односи за преместување на објекти
LAN access	Протокол помеѓу мобилен компјутер и фиксиран LAN
Dial-up Networking	Овозможува повик од преносен компјутер преку мобилен телефон
FAX	Овозможува поврзување на мобилна FAX машина со мобилен телефон
Cordless teleph-ony	Поврзување на слушалката со својата базна станица
Intercom	Дигитален „токи-воки“
Headset	Овозможува „hands-free“ комуникација
Object Push	Начин за размена на едноставни објекти
File Transfer	Начин за пренос на датотеки
Synchronisation	Овозможува синхронизација на PDA со друг уред

Generic access - профилот всушност не е апликација и претставува основа за создавање на вистинските апликации. Нивната работа е да овозможи сигурни канали помеѓу master-от и slave-от.

Service discovery – профилот се употребува за детекција - кои сервиси ги нудат другите уреди.

Овие два профила се задолжителни додека останатите се опционални.

Serial port – сериската порта е профил кој овозможува комуникација за пренос на податоци, и е протокол кој е употребуван од другите профили. Сериската порта емулира сериска врска.

Generic exchange – дефинира клиент-сервер врска за пренос на податоци. Клиентот ја иницира операцијата, дозволено е "робот" да може да биде клиент или сервер.

LAN access, Dial-up networking и fax профилот се мрежни профили.

- LAN access – овозможува пристап на мрежа од Bluetooth уреди и е директна конкуренција со 802.11 стандардите.
- Dial-up networking – овозможува вградениот модем на преносниот компјутер да се конектира на мобилен телефон безжично.
- Fax – факс профилот е сличен со Dial-up networking и со него е дозволена конекција меѓу два факса со помош на мобилен телефон кој е поврзан безжично барем со едниот факс.

Cordless telephony, Intercom, Headset се профили за телефонија и се дизајнирани за безжично поврзување на овие апарати.

Opject push, File transfer, Synchronization се направени за размена на објекти меѓу два безжични уреди. Synchronization е за префрлање и преземање на податоци од PDA или преносен компјутер.

Бидејќи во развојот учествувале различни развојни тимови и секој дал решение за протокол од неговото поле на интерес, тоа резултирало со добивање на 13 протоколи иако можело да се постигне истото со само два протокола, еден за трансфер и еден за „streaming" комуникација во реално време.

7.4.3 Bluetooth протоколен стек

Стандардот за Bluetooth обединува повеќе протоколи во група на поврзани нивоа. Структурата на нивоата не одговара на ниту еден од познатите модели за комуникација како OSI, TCP/IP или 802 моделот. IEEE групацијата работи на модификација на Bluetooth за да одговара на 802 моделот.

Слика 7.14: Верзијата 802.15 на Bluetooth протоколната архитектура

Најнискиот слој е физичкото радио ниво, кое се грижи за радио трансмисијата и модулацијата. Најголемиот дел од залагањата се однесуваат на ова ниво со цел да се намали цената на чинење, а со тоа да се постигне поголем пазарен успех.

Второто ниво е „baseband“ и тоа се грижи како господарот го контролира часовникот и групирањето на временските делови во рамки.

Следното ниво има група на поврзани протоколи. Link manager кој се грижи за воспоставување на логички канали помеѓу уредите, а тука е вклучено искористувањето на напојувањето, проверката за автентикација и квалитетот на сервисот. „Logical link control adaptation protocol“ ги штити погорните нивоа од техничките детали од процесот на емитување. Следното повисоко ниво содржи повеќе различни протоколи кои се грижат за радио комуникација, телефонија, препознавање на сервиси и друго. На највисокото ниво се наоѓа т.н. Application/ Profiles. Во највисокото ниво се лоцирани апликациите и профилите. Тие ги користат протоколите од пониските слоеви.

Радио нивото на Bluetooth

Радио нивото ги префрла битовите од master-от до slave-от и е систем со мала моќност и може да пренесе сигнал до 10 метра. Оперира на фреквенција од 2.4GHz ISM бранова должина. Се состои од 79 канали секој од 1 MHz. Фреквенцијата на модулацијата е 1 bit/Hz, а тоа дава пропусна моќ од 1 Mbps, но најголемиот дел од овој дијапазон е искористен од „overhead“-от.

Бидејќи и IEEE 802.11 и Bluetooth работат на истата фреквенција од 2.4 GHz ISM - тие предизвикуваат меѓусебна интерференција. Бидејќи модулацијата на Bluetooth е поголема - тој го уништува сигналот од IEEE 802.11 стандардот. IEEE 802.11a стандардот работи со другите 5 GHz ISM бранова должина, но затоа пак има помал домет од IEEE 802.11b. Некои компании го решиле проблемот со целосна забрана на Bluetooth.

Baseband нивото на Bluetooth

Baseband нивото ги претовара битовите за пренос во рамки и дефинира некои важни формати. Master-от во секој piconet доделува по 625 μsec временски делови. Master-от ги емитува парните, а slave-от непарните. На тој начин master-от добива половина од сегментите, а робовите останатата половина. Рамките можат да бидат долги 1, 3 или 5 сегменти. Секоја рамка се емитува преку логички канал помеѓу господарот и робот. Има повеќе формати на рамки. Најважниот формат започнува со код за пристап кој го идентификува господарот, така што робовите распознаваат во радио дијапазонот од два господара, кој сигнал е наменет за нив.

Времето на префрлувањето на фреквенциите дозволува време од 250–260 μsec по скок - да се овозможи радиот колата да се стабилизираат. Можни се и побрзи сталожувања, но по повисока цена.

Кај рамка со еден слот, по сталожувањето - 366 од 625 бита остануваат. Од тие, 126 се за кодот за пристап и за заглавјето, оставајќи само 240 бита за податоци. Кога пет слота се поврзани заедно потребен е само еден период на сталожување и малку пократок период на сталожување, така што од 5 x 625 = 3125 бита во 5 слота, 2781 се достапни за „baseband“ слојот.

Така подолгите рамки се поефикасни од рамките кои запоседнуваат само еден слот. Секоја рамка се пренесува преку логички канал наречен линк, помеѓу „господарот“ и „робот“. Постојат два вида на линкови, првиот е ACL (Asynchronous Connection-Less) линк, кој се користи за пакетски податоци достапни во нерегуларни интервали.

Овие податоци пристигнуваат од L2CAP нивото на предајната страна и се испорачуваа на L2CAP нивото на приемната страна. ACL сообраќајот се испорачува на „best-efforts“ основа, и нема никаква гаранција за пренесувањето; рамките можат да бидат изгубени и потребно е да се изврши нивна ретрансмисија. „Робовите“ може да имаат само еден ACL линк кон нивниот господар.

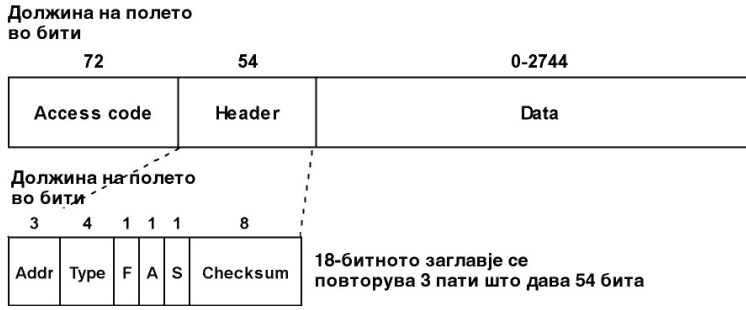
Другиот вид на линкови се нарекува SCO (Synchronous Connection Oriented) линк, за податоци во реално време како што се телефонските врски. На овој вид на канал му се доделува фиксиран слот во секоја насока. Заради временските ограничувања на SCO линковите, на рамките што се испраќаат преку нив никогаш не им се врши ретрансмисија. Наместо тоа се користат корекции на грешки однапред (forward error correction) за обезбедување на поголема доверливост. Еден „роб“ може да има до 3 SCO линкови со неговиот „господар“. И секој SCO линк може да пренесува еден 64,000 bps PCM аудио канал.

Bluetooth L2CAP ниво

L2CAP слојот има три главни функции. Прво врши прифаќање на пакетите до 64 KB до повисоките нивоа и ги дели во рамки за пренесување. На другиот крај рамките повторно се реасемблираат во пакети. Второ, управува

со мултиплексирањето и демултиплексирањето од повеќе извори на пакети. Кога пакетот треба да се реасемблира, L2CAP слојот одредува на кој од повисоките протоколи да му го предаде, на пример, „Rfcomm“ или „telephony“. Трето, L2CAP управува со барањата за квалитетот на сервисите, и кога се воспоставуваат линковите и при нормално функционирање. При воспоставувањето - се преговара за поставување на максималната дозволена големина на полето за содржина (payload), со цел - превенција на уред, способен за пренос на големи пакети, да ги загуши уредите со мали пакети. Ова е потребно затоа што не сите уреди може да се справат со максимална големина на пакетот од 64-KB.

Постојат повеќе формати на рамките, од која најважната е прикажана на сликата. Таа започнува со пристапен код (access code) со кој обично се идентификува господарот, така што робовите од досегот на радио брановите на два господари можат да одредат за кој е наменет сообраќајот. Потоа доаѓа 54-битно заглавје кое содржи полиња карактеристични за MAC подслојот. По него се наоѓа податочното поле од кои 2744 бита (за пренос преку 5 временски слота). За единичен временски слот, форматот е ист, освен што податочното поле содржи 240 бита.



Слика 7.15: Типична Bluetooth рамка

Рамките се составени од заглавјата со следниве полиња:

- Адресното поле (Addr) - идентификува за кој од осумте активни уреди е наменета рамката.
- „Type“ го идентификува видот на рамката f (ACL, SCO, poll, или null), видот на корекцијата на грешките користени во податочното поле и колку временски слота е долга рамката.
- „Flow“ битот се поставува од страна на робовите кога нивниот „buffer“ е полн и не се во состојба да примаат податоци, и ова претставува примитивна контрола на сообраќајот.
- „Acknowledgement“ битот служи за прикажување на ACK на рамката.

- „Sequence“ битот служи за нумерирање на рамките за детектирање на ретрансмисии. Бидејќи протоколот е застани и чекај (stop-and-wait), доволен е 1 бит.
- „Checksum“ е 8-битна вредност на сумата пресметана од заглавјето.

Целото 18-битно заглавје се повторува 3 пати за да се формира 54-битно заглавје и приемната страна ги испитува сите три верзии на заглавјето - ако секој бит три пати е ист се прифаќа, ако не се зема мнозинската вредност. Така 54 бита од преносниот капацитет се користат за пренесување на 10 бита од заглавјето. Причината за тоа е доверлив пренос на податоци во околина со шум; при користење на евтини уреди со мала моќност (2.5 mW) и мал процесирачки капацитет - потребна е поголема редунданса.

Се користат повеќе формати за податочното поле во ACL рамките. SCO се поедноставни, податочното поле секогаш изнесува 240 бита. Дефинирани се три варијанти, кои дозволуваат 80, 160, или 240 бита за податоците, а останатите се користат за корекција на грешки. Во најдоверливата верзија (80-битна содржина), содржината се повторува 3 пати исто како и заглавјето.

Бидејќи робовите може да ги користат само непарните временски слотови, добиваат 800 slots/sec, исто како и господарот. Со 80-битен товар, капацитетот на каналот кај робовите изнесува 64000 bps, исто како и кај господарот (64000 bps), доволно за единичен полн-дуплекс PCM аудио канал. Овие вредности означуваат дека полн-дуплекс гласовен канал со 64000 bps во двете насоки, со користење на најдоверливиот формат ја заситува „piconet“ мрежата, наспроти чист пропусен опсег од 1 Mbps. За најмалку доверливата варијанта (240 bits/slot без било каква редунданса на било кое ниво), можат да бидат поддржани три полн-дуплекс канали истовремено, затоа се дозволени максимум 3 SCO линкови по еден роб.

8 МРЕЖНИ ПРОТОКОЛИ

8.1 ВОВЕД

Протоколите претставуваат множество на правила и конвенции кои дефинираат на каков начин уредите во мрежата ги разменуваат информациите. Еден протокол не може да овозможи комплетна комуникациска независност, туку треба да соработува со другите протоколи, на различни нивоа на OSI моделот преку т.н. точки за пристап на сервисот (Service Access Points). На тој начин се овозможува целосна „од крај до крај“ (end–to–end) комуникација. Кога постои множество на протоколи кои работат заедно и соработуваат меѓусебно, тоа се нарекува низа на протоколи (protocol suite) или протоколен стек (stack).

8.1.1 Значењето на протоколите

Како што е спомнато претходно, стандардите дефинираат како уредите ќе комуницираат меѓусебно и на кој начин ќе пристапуваат кон мрежниот медиум. Производителите на мрежни уреди и апликации ги следат овие стандарди при Приоритет во развојот на протоколите била интеркомуникацијата помеѓу уредите и потребно е да се задоволи условот за функционирањето на мрежата и комуникацијата со другите мрежи.

На пример, еден од протоколите кој е достапен на сите Windows машини е NetBEUI. Тој е еден од најбрзите комуникациски протоколи кои се користат, но негова карактеристика е тоа што не е рутабилен. Односно, Net BEUI податочните пакети не може да се пренесат преку рутер за поврзување со надворешни мрежи и може да се користи само во внатрешноста на мрежата - интранет.

За разлика од NetBEUI протоколниот стек IPX/SPX, има многу предности и може да се рутира, но работи само во Novell NetWare мрежи. Може да се изврши поврзување и со други NetWare мрежи, но не може да се користи за пренос на податоци преку Интернет. За таа цел потребен е посебено хардверско решение или софтвер во облик на меѓу мрежен оперативен систем (Internetwork operating system - IOS) за да се пропуштат специфични протоколи помеѓу рутерите. Најкористените протоколни стекови кои се користат во WAN и LAN мрежите се:

- Transmission Control Protocol / Internet Protocol (TCP/IP)
- Internet Packet Exchange / Sequence Packet Exhange (IPX/SPX)
- AppleTalk

Секоја од овие протоколни низи имплементира множество на правила кои овозможуваат единствен метод за интеркомуникација помеѓу уредите. TCP/IP е највообичаен од сите мрежни протоколни низи и преставува

стандард за мрежното работење. Тој содржи протоколна низа која се користи за комуникација на Интернет.

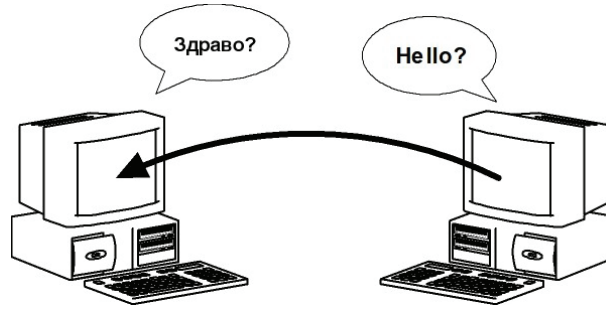
IPX/SPX е развиен од страна на Novell, користи свои методи за да ја обезбеди комуникацијата помеѓу уредите искористени од страна на NetWare оперативниот систем. Секој од индивидуалните протоколи во NetWare стекот може да овозможи слична функција како протоколите во TCP/IP стекот, но тие се во сопственост на Novell. AppleTalk содржи низа на протоколи за комуникација помеѓу уредите користејќи го MAC оперативниот систем.

Протоколите во секоја низа функционираат на различно ниво од OSI моделот, и тоа, од ниво два (податочно ниво), до ниво седум (апликациско ниво). Во ова поглавје е даден краток опис на карактеристиките на протоколнитот стек на TCP/IP со оглед на неговото значење и начинот како протоколите се поставени на различните нивоа во OSI моделот:

- Протоколи на податочно ниво
- Протоколи на мрежното ниво
- Протоколи на транспортно ниво
- Протоколи на апликациско ниво

8.1.2 Кратка историја на TCP/IP протоколот

Во воведното поглавје на книгата е дадена кратка историја на компјутерските мрежи, но заради подбро разбирање на концептите и барањата врз кои се развивал TCP/IP протоколот, потребно е малку подетално да се обајсни патот по кој се развивал. Појавата на TCP/IP била резултат на истражувачки проекти финансирани од страна на владата на САД, исклучиво за потребите на Министерството за Одбрана (Department of Defence – DoD). DoD поседувало опрема која била меѓусебно некомпатибилна и не постоела можност да се воспостави комуникација помеѓу тогашните IBM–овите и Burroughs mainframe компјутери. Овие проекти подоцна довеле до креирање на начини за надминување на овој проблем од кој на крајотпроизлегол TCP/IP протоколот. Основна причина било тоа што двата компјутери имале различни протоколи, како што е покажано на сликата 8.1.



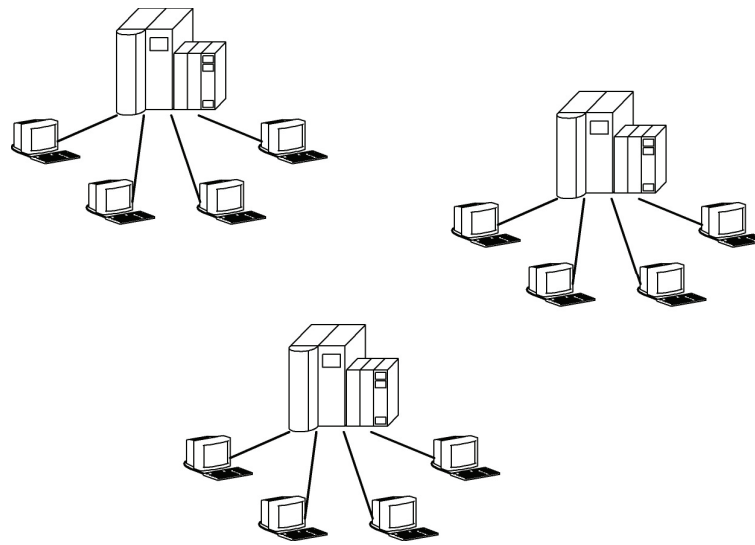
Слика. 8.1. Компатибилен хардвер некомпатибилни протоколи

TCP/IP настанал како единствен алтернативен јазик за комуникација, и со текот на времето, TCP/IP се развил во сет на протоколи кој е најкористен во имплементација на компјутерските мрежи.

Потекло на TCP/IP протоколи: од ARPANET до Интернетот

Оригиналната DoD мрежа не била наменета само за обично поврзување на различни воени локации, иако тоа била една од поважните цели на одбранбената компјутерска мрежа под име ARPANET. Името ARPANET произлегло од агенцијата за напредни истражувачки проекти (Advanced Research Projects Agency–ARPA), гранка на Министерството за Одбрана на САД што го финансирало проектот. ARPA вложувала и сè уште вложува голема сума на пари во универзитетските истражувања во сите области. На слика 6.2 и слика 6.3 е прикажана архитектурата на компјутерската мрежа пред и после ARPANET.

Новата мрежа по име ARPANET е дизајнирана и инсталирана од страна на компанијата Bolt, Beranek and Newman. Во прво време оваа мрежа ги поврзувала професорите и раководителите на проекти низ цел САД, подоцна ARPANET почнал да поврзува одделни приватни универзитети со одвоени воени компјутерски мрежи, и ова поврзување преставувало еден вид „мрежа на компјутерски мрежи“.



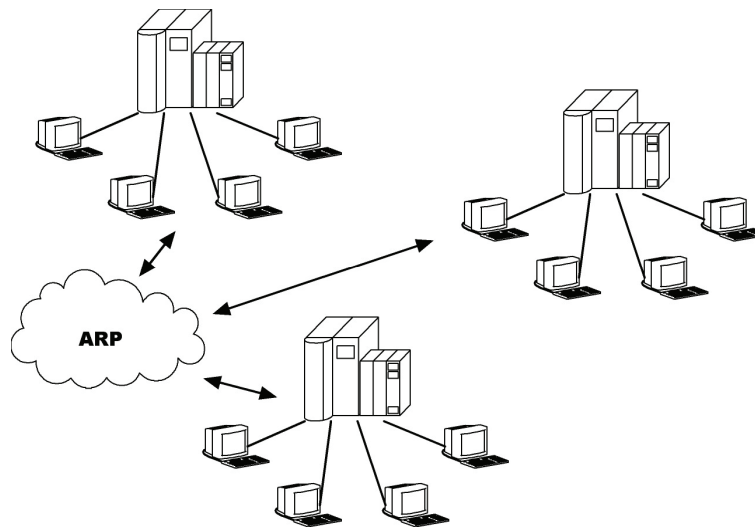
Слика 8.2: Поврзување на истражувачите пред појавата на ARPANET

ARPANET се засновал на протоколот под име NCP (Network Control Protocol); подоцна NCP се поделил на две компоненти: IP (Internet Protocol) и TCP (Transmission Control Protocol). Преоѓањето од NCP на TCP/IP

протоколот, технички гледано претставува единствена битна разлика помеѓу ARPANET и Интернет. На 01.01.1983 година, уредите на ARPANET за преклопување на пакетните податоци престанале да ги превземаат NCP пакетите и почнале да пропуштаат исклучиво TCP/IP пакети, па според тоа - се зема дека 01.01.1983 е официјален ден на раѓањето на Интернет.

ARPANET се трансформирал во Интернет во неколку еволуциски чекори. До првиот позначаен развоен чекор дошло најверојатно во 1984 година кога Винстон Керф и Роберт Кан предложиле употреба на протоколи од кои подоцна настанале TCP и IP. Во тек на повеќе од дваесет годишна историја, Интернет и неговите претходници поминале низ неколку значајни фази на раст и прилагодување. Во 1987 година Интернет имал неколку илјади корисници. До 1993 година овој број се зголемил на 20 милиони, а според некои анкети - во 2002 година на Земјата имало нешто помалку од 600 милиони корисници на Интернет.

За функционирање на Интернет неопходно е да се има само неколку апликативни програми. Најважни сервиси на Интернет преставуваат електронската пошта (e–mail), потоа WWW–World Wide Web, и на трето место се наоѓа протоколот за пренос на фајлови (File Transfer Protocol–FTP).



Слика 8.3. Поврзување на истражувачите после појавата на ARPANET

Оригиналната намена на Интернет протоколите е поддршка за меѓусебно поврзување на мрежи засновано на таканаречени mainframe компјутери, кои истовремено биле и единствена мрежа за време на седумдесеттите години во претходниот век. Во 1980-тите години имало голем напредок на UNIX–овите работни станици, микро-компјутерите и таканаречените миникомпјутери. Берклиевата верзија на UNIX е изградена со помош на

владини пари, па затоа владата им наложила да вградат TCP/IP протокол во него. Вградувањето на IP протоколот во Берклиевиот UNIX довело до раст на самиот UNIX, како и на целиот Интернет. Во осумдесеттите години IP протоколот е користен на голем број Ethernet мрежи кои биле засновани на UNIX, на кои останал во употреба сè до денешен ден.

Во средината на осумдесеттите години, фондацијата National Science Foundation креирала пет супер компјутерски центри и ги поврзала на Интернет, и тоа го искористила во две цели. Супер-компјутерите станале достапни за сите NFS корисници во земјата, а оваа мрежа послужила како главен „'рбет“ (backbone) на Интернетот. Дел на мрежата која припаѓала на фондацијата National Science позната како NSFnet долго време претставувала најголем дел на Интернет. Оваа мрежа ја наследила таканаречената „национална мрежа за истражување и едукација“ (National Research and Education Network–NREN). Низ многу години Интернетот преставувал забранета зона за комерцијалните корисници, затоа што за негово финансирање била задолжена Владата на САД. Сите овие забрани одамна престанале, па денес поголемиот дел од сообраќајот на Интернет го обавуваат комерцијалните, а не политичките линии. Во денешно време доминацијата на Интернетот е многу поголема од страна на комерцијалните и приватните корисници, поради тоа владините и образовните институции во САД користат многу побрз „Интернет 2“.

Сите дилеми околу користење на разни мрежни протоколи се надминати, и веќе не се или многу ретко се користат NetBEUI, IPX, X.25, HDLC, или DDCMP; од 1995 година па наваму, Интернетот се заснова исклучително на TCP/IP протоколот.

8.1.3 Цели при дизајнирањето на TCP/IP протоколите

Кога Министерството за Одбрана на САД почнало со изработувањето на овој сет мрежни протоколи, неговите создавачи си поставиле неколку цели. Намерата на дизајнерите била да TCP/IP ги има следните карактеристики:

- Способност за брзо опоравување во случај на испад на мрежата,
- Можност за приклучување на нова мрежа, без нарушување на постоечките сервиси,
- Отпорност на појавување на голем број грешки,
- Независност на типот на мрежата и производувачот на конкретните уреди од кои е составена мрежата,
- Многу мало дополнително оптоварување (overhead) на податочните пакети.

Способност за брзо опоравување по испад на мрежата

Мрежата во почетокот била замислена како одбранбена (defense) компјутерска мрежа, па поради тоа морала да функционира дури и во случаи

кога голем број од хардверските уреди ненајдено (без било какво предупредување) ќе откажат. Значи мрежата би требало беспрекорно да работи дури и ако поголем дел од нејзините делови бидат погодени со нуклеарен удар.

Можност за приклучување на нова мрежа, без нарушување на постоечките сервиси

Оваа цел е поврзана со претходната, и кажува дека треба да се овозможи приклучување на цела нова мрежа или уреди на интранетот, без било какво нарушување во работата на постоечките мрежни сервиси. Ова во денешно време звучи многу тривијално и очигледно, но голем број на старите мрежни протоколи биле чувствителни на промени. Пример: ако сите корисници би се задржале на употребата на старите PC мрежни протоколи, тогаш немало да помине многу време кога сите корисници би морале да го рестартираат Интернетот, секогаш кога некој нов корисник ќе се конектирал на Интернет.

Отпорност на појавување на голем број грешки

Оваа цел се состои во тоа што интранетот треба да биде толерантен на појавата на голем број непредвидливи грешки, за на крајниот корисник да му овозможи 100% доверлив сервис, без разлика на природата на овие грешки. Пример: Доколку се врши пренос на податоци од Вашингтон ДЦ до Пентагон во државата Орегон, и притоа торнадо ги уништи линковите кои водат преку Оклахома, сите податоци кои се изгубени за време на торнадото, ќе бидат автоматски повторно пренесени и пренасочени преку некоја друга линија.

Независност на хостот

Со оваа цел е замислено архитектурата на некоја нова мрежа да функционира без никаков проблем во сите постоечки типови на мрежи, т.е. да не биде посветена или поврзана со некој конкретен произведувач на компјутерски компоненти. Компаниите мораат да се прилагодат на околината опкружена со голем број различни произведувачи.

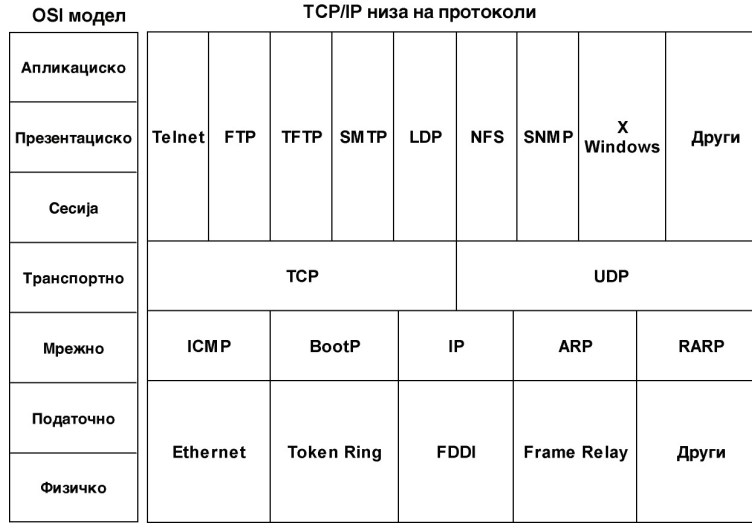
Многу мало дополнително оптоварување

Оваа последна цел се состои во тоа што мрежните протоколи треба да преставуваат што помало додатно оптоварување за мрежата. За подобро да се разбере ова - се споредува TCP/IP со некој друг протокол. Иако никој не знае кој протокол за дваесет години ќе преставува главен светски-признат мрежен протокол, ако некогаш некој протокол доживее таква општа прифатеност – тоа би бил сетот протоколи креиран од страна на меѓународната организација за стандардизација (International Organization for Standardization – ISO). ISO поседува извесни стандарди кој по начинот на

функционирање се многу слични на TCP/IP протоколот, од кои најпознати стандарди се со ознаката X.25 и TP4. Меѓутоа при пакувањето на податоци, секој протокол во овој пакет сместува еден додатен сет на бајтови, кои играат улога на електронски коверти (пликови). Голем број од пакетните податоци кои почнале да употребуваат IP протоколи имаат едноставно заглавје со фиксна големина од 25 бајтови. Максималната големина на ова заглавје, ако се вклучени сите можни опции, изнесува 60 бајтови. Овие дваесет бајтови секогаш се сместени на самиот почеток од податочниот пакет. Наспроти тоа, протоколот X.25 употребува десет различни начини на поставување на заглавје, што значи дека нивните димензии не се фиксни или предвидливи. Едноставен протокол подразбира брз пренос и преклопување на податочните пакети.

8.2 TCP/IP ПРОТОКОЛЕН СТЕК

Неговото име доаѓа од двата основни протоколи во стекот: TCP и IP. TCP е одговорен за доверлива конекција и комуникација преку користење на проверка на грешки, додека IP го опслужува TCP и преку него е имплементиран адресниот систем кој се користи при пренесувањето на пакетите во мрежните уреди. TCP/IP се применува во сите типови на мрежи LAN, MAN и WAN. TCP/IP е најшироко имплементиран протоколски пакет кој се користи на различни платформи, вклучувајќи ги UNIX, Windows и Macintosh. На сликата 8.4 се прикажани протоколите од TCP/IP протоколниот стек распоредени врз нивоата од OSI моделот.



Слика 8.4: Споредба на OSI моделот со TCP/IP моделот

Најлесен начин да се откријат протоколите на TCP/IP пакетот е да се види каде тие функционираат во OSI моделот. Секој протокол во овој стек

функционира на едно од четирите нивоа и тоа: податочното ниво, мрежното ниво (познат како Интернет ниво во TCP/IP моделот), транспортното ниво и апликациското ниво.

8.2.1 Протоколи на податочно ниво

Протоколите кои оперираат во податочното ниво го дефинираат методот за пристап до медиумите, архитектурата и интерфејсот со физичкото ниво на мрежата. Овие протоколи можат да се поделат во LAN протоколи и WAN протоколи. Овие протоколи се базирани на стандарди кои се усвоени од страна на IEEE познати како 802 стандарди. LAN протоколите вклучуваат Ethernet, Token Ring и FDDI, додека WAN протоколите вклучуваат: PPP, ISDN и Frame Relay.

8.2.2 Протоколи на мрежно ниво

Во TCP/IP пакетот, мрежното ниво е познато како Интернет ниво. Ова ниво е одговорно за логичкото адресирање на уредите на мрежата. Исто така мрежното ниво е одговорно за рутирање на податоците помеѓу изворот и дестинацијата. Четирите најважни TCP/IP протоколи кои функционираат во ова ниво се:

- Internet Protocol (IP)
- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)
- Internet Control Message Protocol (ICMP)

Internet Protocol (IP) е еден од најважните протоколи. Тој го дефинира адресниот систем со кој се идентификуваат сите уреди на Интернет. Негова главна цел е да овозможи логичко адресирање со користење на IP адреси. Овие адреси се идентификацискиот број кој се користи да ја води информацијата помеѓу мрежите со користење на TCP/IP и на Интернет. Овој број е единствен за секој уред на мрежата. Без него не е можно да се пристапи на www.

Address Resolution Protocol (ARP) - овој протокол овозможува сервис за споредување на познатата IP адреса на дестинацискиот уред со MAC адресата. ARP праќа MAC барање на целата дестинациска мрежа, барајќи ја MAC адресата на посакуваната IP дестинација. Уредот кој е идентификуван со IP адресата на пакетот одговара на барањето и ја праќа својата MAC адреса.

Reverse Address Resolution Protocol (RARP) - овој протокол овозможува спротивен сервис од ARP. Наместо да ја бара MAC адресата на уред чија IP адреса веќе ја знае, RARP дава IP адреса за уред што ја знае сопствената MAC адреса.

Овој сервис е потребен во мрежите кои користат работни станици со мал дисковен простор. Овие уреди не можат да ги чуваат своите IP адреси во меморијата, но имаат пристап до своите MAC адреси. Тие мораат да ја побараат IP адресата за да комуницираат. Уред познат како RARP сервер одговара на RARP барањето и овозможува IP адреси за работната станица или за уредите - за да можат да ја користат мрежата. Откако уредите ќе се исклучат, IP адресите се слободни и достапни на RARP серверот да ги даде на друг уред.

Internet Control Message Protocol (ICMP) е корисен протокол за мрежните администратори. Тој е имплементиран во сите TCP/IP мрежи и праќа пораки кои можат да помогнат при дијагностика на грешки и решавање на проблеми во кои можат да се појават на мрежата. ICMP пораките се вклучени во IP датаграмот. Најчестите пораки кои се праќаат кога ќе се појават грешки, во себе вклучуваат:

- Недостижна дестинација
- Истекување на времето
- Ехо
- Одговор на ехо
- Барање на информација
- Одговор на информација
- Барање на адресна маска

8.2.3 Протоколи на транспортно ниво

Протоколите кои се наоѓаат во транспортното ниво треба да овозможат доверлива комуникација од крај до крај (end–to–end) помеѓу уредите. Основната функција на овие протоколи е ефикасен пренос на податочните пакети до дестинацијата. Во TCP/IP протоколниот стек, следниве два протоколи од транспортното ниво овозможуваат крај-до-крај комуникациски сервиси:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

Разлика помеѓу нив се состои во тоа што TCP користи конекциски-ориентирани сервиси и гарантиран пренос, додека UDP користи безконекциски сервиси во преносот и не гарантира испорака на пакети до дестинацијата.

Transmission Control Protocol (TCP) – Конекциски ориентираниот сервис на TCP го осигурува преносот на пакетите. TCP користи checksum кој се додава на податочниот пакет така што дестинацискиот уред може да детерминира дали пакетот е примен без грешки. Со споредување на информацијата која се наоѓа во checksum и со податокот кој е примен, може да се одреди на дестинацијата дали пакетот е во ред. TCP/IP поседува и систем за проверка на грешки кој користи секвенцијално нумерирање, и го идентификува редоследот по кој пакетите биле пратени. Овој конекциски-ориентиран

систем, исто така креира додатен сообраќај на мрежата и може да има негативно влијание на перформансите на мрежата.

User Datagram Protocol (UDP) – користи безконекциски транспортен систем. Тој не користи систем за проверка на грешки или за секвенцијално нумерирање со цел да се гарантира преносот. UDP смета дека другите протоколи, како и нивоата во стекот, ќе овозможат проверка на грешките. Овој протокол се грижи само да го однесе податокот на транспортното ниво до дестинацискиот уред. Тој не се грижи што другите нивоа прават со податокот. UDP користи помал проток на сообраќај отколку TCP. Тоа го прави поефективен, но помалку доверлив како независен протокол. Но во комбинација со другите протоколи од низата - тој го овозможува потребниот сервис за комуникација.

8.2.4 Протоколи на апликациското ниво

Протоколите во апликациското ниво се сместени помеѓу сесиското ниво и апликациското ниво на OSI моделот. Тие овозможуваат мрежни сервиси, како што се e–mail и пренос на фајлови. TCP/IP пакетот вклучува многу протоколи кои се наоѓаат на апликациското ниво, и тие се:

- File Transfer Protocol (FTP)
- Trivial File Transfer Protocol (TFTP)
- Simple Mail Transfer Protocol (SMTP)
- Hypertext Transfer Protocol (HTTP)
- Domain Name System (DNS)
- Telnet
- Dynamic Host Configuration Protocol (DHCP)
- Symple Network Management Protocol (SNMP)

File Transfer Protocol (FTP) – не е само протокол; тој е и сервис и апликација. FTP е важен протокол кој овозможува фајловите да се копираат помеѓу уредите. Фајловите исто така можат и да се симнат (download). FTP бил еден од првите протоколи за пренос.

Trivial File Transfer Protocol (TFTP) – како и FTP, така и TFTP се користи за трансферирање на фајлови, и тоа специфично преку Интернет. Тој работи со UDP и овозможува сопствен систем за проверка на грешки и систем за потврда. TFTP бара потврда за секој пакет кој бил пратен пред следниот да биде пренесен.

Simple Mail Transfer Protocol (SMTP) – ја има одговорноста за трансферирањето на e–mail помеѓу компјутерите. Тој користи конекциски ориентирани сервиси на TCP за праќање и примање на пораките. Сите оперативни системи не го разбираат SMTP бидејќи тој е дизајниран специјално за UNIX.

Hypertext Transfer Protocol (HTTP) – се користи за пристап до Hypertext Markup Language (HTML) фајловите на Интернет. Тој им овозможува на клиентите и серверите да разменуваат податоци многу рапидно. HTTP нуди

само два типа на пораки кои можат да се разменат, и тоа барање од страна на клиентот и одговор од страна на серверот. Тој не овозможува никаква безбедност или меморија за трансакцијата која се одвива помеѓу клиентот и серверот. Тој може само да зема и да праќа фајлови и тоа е сè. HTTP има големо влијание на Интернет. Денес се познати нови верзии на HTTP, како што е Secure HTTP (SHTTP), кој овозможува безбедност која беше изоставена во оригиналната верзија на протоколот, со помош на енкрипција и безбедносни проверки.

Domain Name System (DNS) – е имплементиран со цел да ги управува и централизира домен-имињата на Интернет. Тој го овозможува сервисот со преведување на хост-името на единствениот домен, како на пример www.sybex.com, во IP адресата на серверот каде хостот е лоциран. Домен името е направено на три нивоа. Највисокото ниво на доменот е за да се идентификуваат последните карактери на доменот, на пример: .com, .org, .mk. Второто ниво во домен-името (како што е sybex.com) е точното име на организацијата. И третото ниво е www, што типично се однесува на хостот, кој обично е сервер.

Telnet – во исто време е и протокол и апликација. Неговото име доаѓа од начинот на кој повеќето Telnet сесии се одвиваат т.е. со користење на поврзување преку телефонски врски. Telnet протоколот се користи за да се овозможат далечински терминални сервиси. Тоа му овозможува на крајниот корисник кој користи компјутер како терминал, да врши интеракција со уредите кои нудат далечински пристап, т.е. да има комуникациска сесија со програма што се наоѓа на оддалечениот сервер. Крајниот корисник користи приказ и тастатура за да врши интеракција со далечинскиот сервер, исто како да се наоѓа на иста физичка локација со серверот. Telnet овозможува повеќе корисници од различни локации во исто време да пристапат на серверот со далечински пристап. Telnet софтверот е дизајниран да ги преведува командите на уредите со далечински пристап, за да оддалечениот серверот ги разбере. Telnet апликациите го имплементираат Telnet протоколот, за преведување на командите во општ формат.

Dynamic Host Configuration Protocol (DHCP) – динамички ги доделува IP адресите и другите конфигурациски информации, за уредите да ја препознаат мрежата. Како RARP, така и DHCP им доделува IP адреси на уредите кои немаат. Овој сервис, обично е овозможен од рутер или од посебен сервер. Тој исто така е многу важен. DHCP овозможува множество на IP адреси, кои се базирани на наведените мрежни адреси, кои се ставени во листа кај серверот. Во зависност од тоа како протоколот е имплементиран, тој може да трае специфично време, или само за време на користењето на мрежата од страна на уредот.

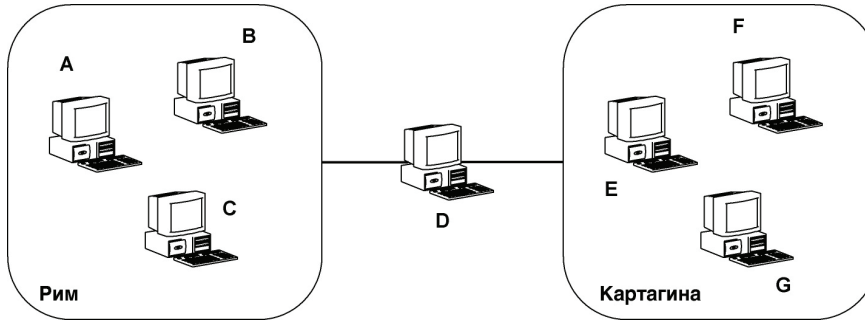
Symple Network Management Protocol (SNMP) – овозможува можност за конфигурирање, надгледување и управување на мрежните ресурси и уреди. Како и другите апликациски протоколи, потребен е софтвер за користење на SNMP, и сите уреди кои се во мрежата мора да го разбираат овој протокол.

8.3 ИНТЕРНЕТ ПРОТОКОЛ – IP

8.3.1 Концепти на интернет поврзување

Основната компонента на глобалната мрежа, а може да се каже и сврзниот елемент на Интернет е Интернет Протоколот или скратено наречен IP. Секој податок што се пренесува преку Интернет мора да биде енакпсулиран во IP пакет (IP packet), кој понатаму се рутира соодветно интернет адресата на одредишниот хост. Основната улога на IP е да им овозможи пренос на пораките - од едниот дел на мрежата до другиот.

Секој интранет е составен од најмалку две под-мрежи (subnets). Самиот поим под-мрежа е втемелен на фактот што LAN архитектури се базираат на мрежни сегменти кои користат „broadcast“ пренос на пакети во еден домен на колизии. Секој хост што се наоѓа на одреден Ethernet сегмент, може да го слушне целиот сообраќај кој се одвива на тој сегмент, исто како што секој уред на даден прстен во некоја Token Ring мрежа, може да ја анализира секоја порака која поминува низ мрежата. Ethernet и Token Ring работат на тој начин така што - без разлика што секој хост станица може да ги прими сите пораки, тие се игнорираат освен оние кои се наменети за него. На еден единствен Ethernet сегмент, или на еден прстен од Token Ring мрежата, не постои никакво рутирање, нема потреба за донесување никакви одлуки за пренасочување на сообраќајот, бидејќи сите можат да го преимат пренесуваниот сообраќај. Ако се претпостави дека постојат две посебни Ethernet, меѓусебно поврзани како на слика 8.5.



Слика 8.5. Мулти–сегментен интранет

На слика 8.5 се гледаат два Ethernet сегменти со име Рим и Картагина. Во сегментот Рим се сместени три компјутери, и на секој од тие три компјутери е вградена по една Ethernet картичка, која е означена со буквите A, B и C. Другите три компјутери се сместени во сегментот Катрагина, нејзините Ethernet картички се означени со буквите F, G и H. Еден од прикажаните PC компјутери (средишниот) има две Ethernet картички – една означена со буквата D, што е конектирана со Рим, и другата означена со буквата E - конектирана со сегментот Картагина.

8.3.2 Поим за под-мрежи и рутери

Архитектурата на интранетот во голем дел се заснова на интерфејси, при што компјутерите со Ethernet картичките A, B и C можат директно да комуницираат директно меѓу себе, но компјутерите A, B и C не можат да комуницираат со F, G и H, без помош на машината која ги содржи Ethernet картичките D и E. Според тоа, D/E машината ќе функционира како рутер, т.е. како компјутер кој овозможува комуникација помеѓу различни мрежни сегменти. За компјутерите A, B и C и D може да се каже дека се наоѓаат во еден домен на емитување, истото може да се каже за групата на компјутери E, F, G и H. Домен на емитување во интранет технологијата попрецизно се нарекува под−мрежа (subnet), односно множество на машини кои можат меѓусебно да комуницираат без потреба за рутирање.

Во примерот, F и H можат да комуницираат директно, без потреба од рутерот (во овој случај тоа е компјутерот E) да ја проследува пораката, (поради тоа што овие два компјутера се наоѓаат на иста подмрежа). Исто така, компјутерите A и C можат да комуницираат директно, без потреба од рутерот да им ја проследи пораката, бидејќи се наоѓаат во иста подмрежа. Меѓутоа доколку B побара да воспостави комуникација со G, тој би морал својата порака да ја прати до компјутерот D и тој да ја прати пораката до G, затоа што B и G не припаѓаат на иста под−мрежа.

8.3.3 IP адреси и Ethernet /MAC адреси

Нека се земат компјутерите од претходната слика како пример, при што секој компјутер е приклучен на мрежата преку својот Ethernet интерфејс кој што се карактеризира со два индентификатори, односно две адреси: IP-адреса и Ethernet или MAC адреса.

Ethernet /MAC адреси

Ethernet адреса на секоја Ethernet картичка претставува единствен 48−битен идентификационен код. Ethernet адресата претходно е одредена, т.е. хардверски кодирана на самата картичка. Ethernet адресите уште се нарекуваат и Media Access Control (MAC) адреси, и се изразуваат со помош на 12 хексадекадни цифри. Доделувањето на Ethernet адресата се врши централизирано, така што за одредени производувачи постојат одредени блокови на адреси.

IP адреси и квартален формат

За разлика од 48−битните MAC адреси, IP адресата се состои од вкупно 32 бита. IP адресите претставуваат броеви, кои на работната станица (или серверот) се подесени од страна на мрежниот администратор − броевите не се хардверски кодирани на матичната плоча, како што е тоа во случајот на

Ethernet адресите. Според тоа постојат вкупно 4 милијарди различни Интернет адреси.

IP адресите заради полесно паметење се прикажуваат во формат w.x.y.z, каде w, x, y и z претставуваат децимални броеви од 0 до 255. Ако се земе како пример адресата 199.34.57.53. секој од овие четири броеви се нарекува квартал (quad); и бидејќи овие квартали меѓусебно се поделени со точки (dots), овој формат се нарекува нотација на точкести квартали (dotted quad).

Секој од броевите во точкестот квартал одговара на еден 8–битен дел од Интернет адресата. Но бидејќи, бројот од 8 бита може да има вредност од 0 до 255, и секој квартал може да се претстави со број од опсегот од 0 до 255. На пример, при преведување на IP адресата 11001010000011111010101000000001 во dotted quad формат, најпрво потребно е овој број да се подели во група од по 8 бита:

```
11001010    00001111    10101010    00000001
```

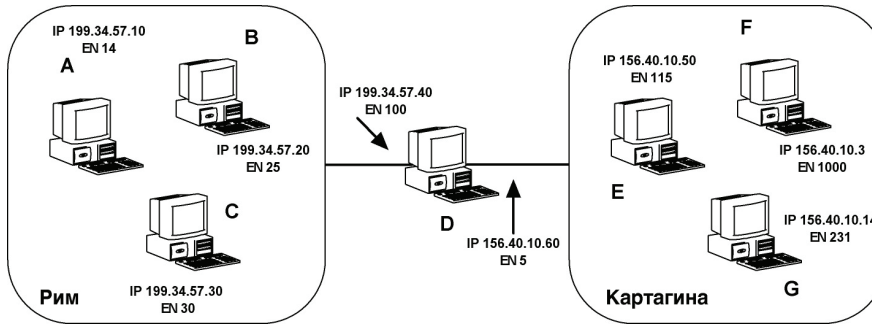
потоа, секој од овие 8–битни броеви треба да се конвертираат во нивниот децимален еквивалент. И се добива следниот резултат:

```
11001010    00001111    10101010    00000001
  202          15          170          1
```

што значи IP адресата прикажана претходно, запишана во нотација на точкести квартали гласи 202.15.170.1.

Кажано накратко: секој компјутер поседува барем една Ethernet картичка, со што секоја Ethernet картичка содржи претходно дефинирана MAC адреса. Мрежниот администратор на компјутерската мрежа, на секој компјутер инсталирал IP софтвер и во текот на тој процес на секој од компјутерите им доделил IP адреса.

Нека на интранетот од горниот пример, на компјутерите им се доделат произволни IP адреси и Ethernet адреси како што е прикажано на слика 8.6.



Слика. 8.6. Интранет составен од две подмрежи, со Ethernet и IP адреси.

8.3.4 IP рутери

Нека се земе во предвид средниот компјутер од сликата 8.6. Тој претставува дел на двата сегменти, на двете под-мрежи, преку се инсталација на две Ethernet картички. Компјутер кој содржи повеќе од една мрежна картичка се нарекува multihomed компјутер. Една од инсталираните Ethernet картички припаѓа на под–мрежата Рим, додека другата картичка е составен дел на под–мрежата Картагина.

Секоја Ethernet картичка мора да има посебна IP адреса, а компјутерот кој има две Ethernet картички има две IP адреси, D и E. Кога некоја порака се емитува во Рим, адаптерот D ќе слушне, но картичката E нема да слушне. Исто така кога некоја порака ќе се емитува во под–мрежата Картагина, адаптерот E ќе ја слушне оваа порака, додека D нема да ја слушне.

Единствен начин да пораката од A стигне до G е да пораката прво биде примена од страна на Ethernet адаптерот со адреса D, па потоа повторно да се прати преку Ethernet адаптерот со адреса E. Кога картичката E ќе ја ре-емитува оваа порака, картичката G ќе ја слушне, бидејќи се наоѓа на иста под–мрежа како и картичката E. За да може сето ова да функционира, машината на која се инсталирани картичките D и E треба да има инсталиран сервис кој ќе ја изврши оваа функција, т.е. да разменува податоци помеѓу D и E кога тоа е потребно. Оваа машина по дефиниција претставува IP рутер. Машина на која е инсталиран Windows Server 2003 може ефикасно да одигра улога на IP рутер, иако постојат голем број на хардверски изведени рутери (како што се опишани во поглавје 3).

Кај IP протоколот, станицата што испраќа (во примерот - станицата со Ethernet картичка A) ја анализира адресата на одредишната станица (во примерот е PC со Ethernet картичка G), и бидејќи не е на истиот мрежен сегмент (подмрежа) се испраќа на адреса на рутерот (default router) или мрежен премин (default gateway). Адресата на рутерот кај компјутерот A е претходно веќе подесена од страна на мрежниот администратор и во овој пример ќе биде D, и хостот A ги испраќа на D сите пораки кои имаат непознато одредиште. Кога D ќе прими една ваква порака, тој ќе забележи дека таа порака не му е наменета нему туку на компјутерот G, па оваа порака ја ре-емитува преку картичката E.

Пример за рутирање

Да направиме детална анализа за тоа како некоја порака пристигнува од A до G. Се знае дека секој компјутер може да има една или повеќе IP адреси, според тоа не постои релација помеѓу MAC адресата на некоја Ethernet картичка, и нејзината IP адреса; MAC адресата е хардверски втисната во Ethernet картичката од страна на некој производувач, додека IP адресата се доделува од страна на мрежниот администратор.

Доколку детално се разгледа примерот, ќе се види дека сите компјутери во подмрежата Рим имаат адреса од тип 199.34.57.z, каде z е некој број, додека

сите компјутери во Картагина имаат адреса од типот 156.40.10.z, каде z е исто така некој број од опсегот 0 до 255. Наспроти ова, Ethernet адресите не се подложни на некоја шема и групирањето исклучиво се врши според произведувачот на конкретните картички. Меѓусебната сличност на IP адресите во Рим и Картагина е од пресудна важност за да се разбере рутирањето.

Се разгледува пример во кој од компјутерот A се праќа порака до компјутерот G:

Прво: IP софтверот на A одлучува дали пораката едноставно да ја емитира или да ја рутира. Оваа одлука ја донесува врз основа на тоа дали G се наоѓа во истата под-мрежа (како A) или не. Хостот со Ethernet картичка A прашува дали G е составен дел на Рим, како и A.

Потоа компјутерот A заклучува дека G се наоѓа на различна под-мрежа, па прави паралелна анализа на својата адреса и неговата адреса. Компјутерот A знае дека неговата адреса е 199.34.57.10 и знае дека пораката мора да ја прати на адреса 156.40.10.50. Тука A го применува едноставното правило: ако одредиштето на адресата е 199.34.57.z, каде z може да биде било кој број од 0 до 255, тогаш тоа значи дека одредишниот компјутер се наоѓа во истата под-мрежа, па не мора да се изврши рутирање. Од друга страна, очигледно е дека адресата 156.40.10.50 не припаѓа на истата под-мрежа. Во случај G да се наоѓа на иста под-мрежа како и A, тогаш A само ќе викне и G ќе ја слушне пораката.

Трето: A не може директно своите IP пакети да ги праќа до G. Оттука A бара некој поалтернативен начин за праќање на пораките. Кога мрежниот администратор го подесил IP софтверот на компјутерот A, тој во него дефинирал адреса на рутер кој се подразбира. Рутер кој се подразбира е во основа адреса која вели „ако не знаете каде треба нешто да се прати, пратете ми го тоа на мене, а јас тоа ќе пробам да го пратам на правата адреса“. Рутер кој се подразбира за компјутерот A е компјутерот D, па според тоа A има задача пораката да ја прати на компјутерот D кој има адреса 199.34.57.40. Сега може да се прати пораката кон Ethernet картичката на D, освен што Ethernet картичката не разбира IP адреси, таа разбира само MAC адреси. TCP/IP и за ова има одговор: така наречениот протокол за преведување на адреси (Address Resolution Protocol – ARP). Компјутерот A на локален сегмент емитува порака која гласи „ ако има некоја машина со IP адреса 199.34.57.40 да ја прати својата MAC адреса“. Компјутерот D ќе ја слушне оваа порака и ќе ја прати својата MAC адреса, која во овој пример е 100. После ова A праќа една Ethernet рамка на D. Оваа рамка ги содржи следниве информации: постојната Ethernet адреса 14; одредишната Ethernet адреса 100; IP адреса на испраќачот 199.34.57.10; одредишната IP адреса 156.40.10.50.

Ethernet картичката D ја прима оваа рамка и ја проследува на IP софтверот што функционира на дадениот компјутер. Компјутерот согледува дека одредишната IP адреса не е негова IP адреса, и дека мора да изврши рутирање на пакетот. Со анализирање на под-мрежата, компјутерот

заклучува дека одредишниот компјутер лежи во под-мрежата на која се наоѓа Ethernet адаптерот E, па ја праќа ARP пораката, за да ја добие MAC адресата на компјутерот G; на ова барање G одговара со „мојата MAC адреса е 115“ по што картичката E праќа рамка со следнава информација: постојната Ethernet адреса 5; одредишната Ethernet адреса 115; IP адреса на испраќачот 199.34.57.10; одредишна IP адреса 156.40.10.50.

На овој начин компјутерот G конечно ќе го прими пакетот со податоци кој му е наменет. Со анализирање на Ethernet и IP адресите, G согледува дека оваа рамка ја примил од картичката E, но дека оригиналната порака пристигнала од друга машина чија IP адреса гласи 199.34.57.10.

Ова е само еден едноставен пример за IP рутирање, но може да послужи како основа на огромна мрежа како што е Интернетот.

8.4 Мрежни класи, CIDR блокови, рутабилни и нерутабилни адреси и подмрежување

Основната идеја за користењето на 32-битни IP адреси била поедноставување на управувањето со Интернет, или било која интранет мрежа. За да се стане дел од Интернет, потребно е да се има блок со IP адреси, како и име или група на имиња.

8.4.1 Класи на мрежи A, B и C

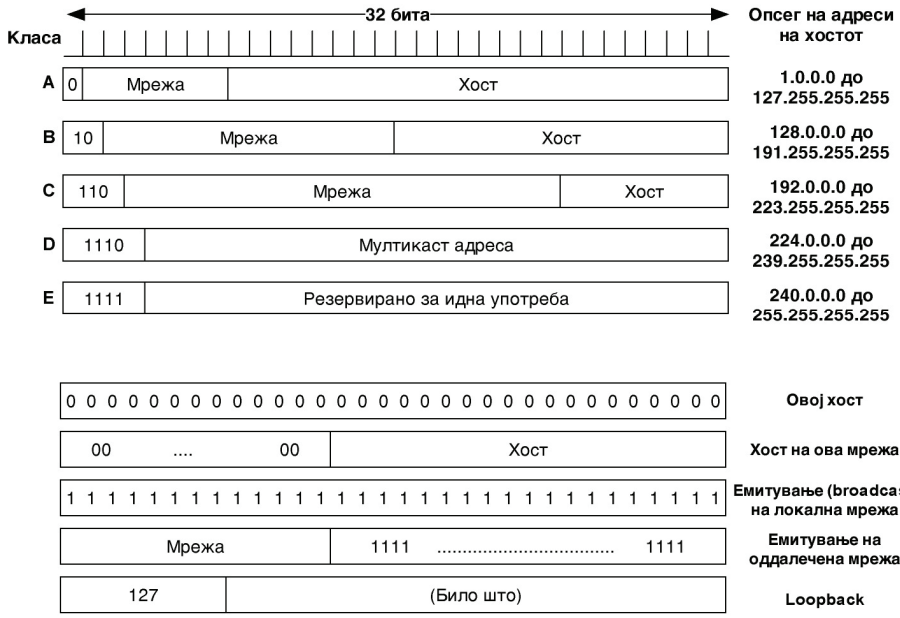
Локалниот Интернет провајдер доделува блок IP адреси врз основа на големината на одредена компанија. Овој блок адреси се вика мрежа (Network). (Под–мрежа не преставува ништо друго, туку дел од овој сет на доделени адреси). Големите компании добиваат мрежа од класата A (во оваа класа нема повеќе слободни мрежи, поради тоа што сите се доделени), компаниите со средна големина добиваат мрежи од класата B (и од нив има многу малку слободни), додека сите останати добиваат мрежи од класата C (нив сè уште ги има во изобилство). Иако има само три класи на компјутерски мрежи, постојат пет различни врсти на IP адреси, како што е прикажано на слика 8.7.

Во почетокот на Интернетот се мислело дека 4 милијарди адреси се сосема доволни за негов раст. Неговите дизајнери дефинирале три класи на мрежи на Интернет: голема, средна и мала мрежа. За разграничување помеѓу различните класи на мрежи, креаторите на Интернет употребиле 8-битни секции на 32-битните адреси: класа на мрежа A, B, C, D и E и резервирани адреси.

Мрежи од класа A

Кај големите мрежи првите 8 битови се одредени од страна на NIC картичката, додека преостанатите 24 бита можат да се подесат од страна на локалните мрежни администратори. Последните 8 битови од лево можат да

имаат вредност од 0 до 126, што значи дека има 127 мрежи од класата А. Овие адреси се доделуваат само на најголемите компании, како што е на пример IBM. На овој начин зафатени се само првите 8 битови и компаниите имаат на располагање вкупно 24 бита. Или со други зборови - мрежите од класа А можат да имаат најмногу 224 односно околу 16 милиони хостови. Меѓу најпознатите мрежи од класа А спаѓаат мрежите на следните компании: General Electric, BBN, IBN, Xerox, DEC, Apple, MIT, Ford, итн.



Слика 8.7: Класи на Интернет мрежи и резервирани адреси

Мрежи од класа B

Кај мрежите од средна големина, првите 16 бита се однапред одредени, така да за локална употреба остануваат уште 16 бита. Адресите од класа B во првиот квартал секогаш имаат вредност помеѓу 128 и 191, додека во другиот квартал може да имаат било кој број од 0 до 255. Според тоа постојат вкупно 16.384 можни мрежи од класата B, при што секоја од нив може да има до 65.536 хостови. Меѓу најпознатите компании кои имаат мрежи од класата B се Microsoft и Exxon (Apple и IBM поседуваат мрежи од класата A, додека на Microsoft му припаднала само B класа).

Мрежи од класа C

Кај малите мрежи дури 24 бита се однапред дефинирани, така да само 8 бита остануваат за локалната администрација (тоа значи дека мрежите од класа C

може да имаат помалку од 254 хоста); од друга страна NIC картичката има на располагање 24 бита и може многу лесно да дистрибуира мрежни адреси од класата C. Адресите од класа C започнуваат со броевите од 192 до 223, во својот прв квартал. Вториот и третиот квартал може да имаат било која вредност од 0 до 255; тоа значи потенцијално можат да се поседуваат 2.097.152 компјутерски мрежи од класата C. Последната мрежа од класа C кога еднаш ќе биде доделена ќе има адреса 223.255.255.z, и сопственикот на мрежата може да го контролира кварталот со вредност z.

Резервирани адреси

Поединечни адреси се резервираат за таканаречена мултикаст употреба, како и за експериментални цели. Тие не можат да бидат доделени на ниедна мрежа. На пример, адресата 224.0.0.0 е оставена на страна за мултикаст, односно за мрежни преноси на цели групи од компјутери.

8.4.2 Рутабилни и нерутабилни адреси

Нерутабилни адреси дефинирани во RFC 1918

Наглиот раст на Интернет хосотвите доведе адресна криза, при што веќе одредено време се прават напори за замена на тековниот IPv4 со IPv6. Со користење на 128-битната шема на адресирање се овозможува постоење на повеќе IP адреси отколку што има електрони во универзумот, но во меѓувреме се користат алтернативни начини за проширување на бројот на достапните адреси. Под ознаката RFC 1918, креаторите на Интернет дефинирале три типа на нерутабилни IP адреси и тоа:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Идејата за ваков опсег на нерутабилни адреси, е во тоа да извесен број на адреси е одделен на страна со цел поедини корисници да градат пробни интранети без потреба да ги изнајмуваат неопходните адреси од IANA организацијата. Со употребата на ваков тип на адреси, секој може да креира мрежа заснована на IP протоколот. Дури и мрежите формирани од ваков тип на адреси да се приклучат на Интернет, тие не би претставувале никаков проблем, бидејќи рутерите на Интернет претходно се програмирани, ваквиот тип на адреси да ги игнорираат. Исто така, ниедна порака која потекнува од овие адреси нема да биде рутирана на јавниот Интернет; од ова следи дека е сосема логично овие адреси да се нарекуваат опсег на нерутабилни (nonroutable) адреси.

Тоа значи дека можат истовремено да постојат милиони мрежи, со опсег на адреса од (на пример) 192.168.1.0 – 192.168.1.255, бидејќи овие мрежи не можат да комуницираат со јавниот Интернет, и со тоа не можат да бидат

причинители на било какви проблеми на Интернет. Освен тоа, компаниите кои се одлучиле да користат нерутабилни адреси, имаат уште една додатна предност, а тоа е безбедноста (не може да се воспостави надворешна врска со овој тип на адреса). Од оваа причина повеќето компании употребуваат барем две множества на IP адреси: адреси кои се употребуваат во внатрешноста (интерни) во компанијата (во нејзиниот интранет), и адреси кои се дефинитиви т.е. Интернет адреси добиени од ISP или некој друг огранок на организацијата IANA.

Рутирање на нерутабилните адреси: преведување на мрежните адреси

Корисниците кои на своите компјутери им доделиле нерутабилни адреси можат да рутираат пораки интерно во мрежата на својата компанија, но потполно им е оневозможен јавен пристап на рутабилниот Интернет. Постои специјален протокол имплементиран во рутерите кој изведува преведување на мрежните адреси (Network Address Translation – NAT), и со кој се овозможува комуникација со Интернетот, без разлика што при тоа се користи приватна IP адреса од интранетот на компанијата, која не е доделена од страна на IANA.

На пример, некоја компанија набавила од IANA или од одреден Интернет провајдер опсег на адреси од класата C и тоа вкупно 256 адреси. Без разлика на тоа што компанијата има над илјада компјутери, таа добила вкупно 256 адреси и тоа не претставува проблем, бидејќи NAT рутерот може без проблем да воспостави нивна комуникација со Интернетот. NAT рутерот на машините со нерутабилни адреси им дозволува да иницираат комуникација со компјутерите кои се наоѓаат на рутабилниот јавен Интернет, но истовремено на машините кои се на Интернет не им дозволува да започнат комуникација во обратна насока.

Пример, ако компјутерот со IP адреса 192.168.1.17, кој се наоѓа зад некој NAT рутер посака да ја посети страницата www.microsoft.com, тоа може да го направи без никаков проблем, но ако некој компјутер од јавниот Интернет сака да воспостави конекција со компјутерот со IP адреса 192.168.1.17, нема да може да успее; неговото барање ќе биде одбиено, бидејќи неговиот локален рутер нема да ја воспостави комуникацијата со некоја нерутабилна адреса.

8.4.3 Ограничувања на IP адресите

Има некои специјални правила во врска со IP адресите. Постои цела група на броеви кои под никакви услови не можат да бидат доделени на ниедна машина. Тоа се адресите на рутите кои се подразбираат (default route), адресите на повратна спрега (loopback), мрежниот број (network number), адреса на емитување (broadcast address) и адресата на рутерите кои се подразбираат (default router).

Адреса на рути кои се подразбираат (default route)

Адресата 0.0.0.0 претставува друг начин да се каже „целокупен Интернет“. Меѓутоа, бидејќи адресата 0.x.y.z спаѓа во класата A, сите типови на адреси со изглед 0.x.y.z мора да се остават на страна (вакви адреси има вкупно 16 милиони).

Адреси на повратна спрега (loopback)

Адресата 127.0.0.1 е резервирана за повратна спрега. Доколку на адресата 127.0.0.1 се прати некоја порака, тогаш таа порака автоматски се враќа, освен ако во IP софтверот нешто не е во ред. Пораките кои се пратени на адресата за повратна спрега воопшто не излегуваат на мрежата, туку остануваат во внатрешноста на IP софтверот на конкретниот компјутер. Од тоа произлегува дека не постои ниедна мрежа со адреса 127.x.x.x, што претставува голема загуба од неискористени 16 милиони IP адреси.

Мрежен број (network number)

Многу е важно да се познава дефинитивниот метод за означување на опсегот на адресите. На пример, за да рутерот пренесе одредена порака на под–мрежата со опсег од 100.100.100.0 до 100.100.100.255, најнапред треба да изврши рутирање на пораката кон рутерот со адреса 99.98.97.103. Мора на некој начин да се означи променливиот опсег на адресите 100.100.100.0 – 100.100.100.255. За таа цел, мора да се употреби почеток и крај на опсегот со цртичка помеѓу нив, но тоа е неефикасно и заморно. Наместо тоа, адресата која завршува со бинарна нула, резервирана е за така наречениот мрежен број (network number), што е TCP/IP-термин за опсег на адресите на под–мрежите. Во примерот за мрежата 100.100.100.z, за означување на опсег на адреси од 100.100.100.0 до 100.100.100.255, се користи скратената ознака 100.100.100.0.

Битно е да се знае дека адресата 100.100.100.0 некогаш не може да се употреби - кај TCP/IP протоколот, оваа адреса не може да се додели на ниеден компјутер. Според тоа, кога на рутерот ќе му се каже да пренесе одредена порака на под–мрежата со опсег од 100.100.100.0 до 100.100.100.255, најнапред извршувајќи рутирање на пораката кон рутерот со адреса 99.98.97.103 - во командната линија мора да се напише нешто како ова: route add 100.100.100.0 99.98.97.103 (т.е. мора да се додадат дополнителни информации).

IP адреса за емитување (broadcast address)

Постои уште една резервирана адреса – адреса за TCP/IP емитување, која се употребува за емитување на пораки кон секоја машина на под–мрежата. Оваа адреса се состои исклучително од бинарни единици.

На пример, на некоја едноставна под–мрежа од класата C, адресата на емитување ќе гласи w.x.y.255. Според тоа, доколку мрежата од класа C, 199.34.57.0 се користи како засебна под–мрежа, тогаш адресата на емитување на оваа мрежа би гласела 199.34.57.255.

Адресата на рутерот кој се подразбира (default router)

На секоја мрежа мора да има инсталирано барем еден рутер, т.е. кога некоја под–мрежа не би имала рутер, таа не би можела да комуницира со другите мрежи, и за таква мрежа не може да се каже дека претставува интранет.

По конвенција, првата адреса зад мрежниот број претставува адреса на подразбирливиот мрежен премин (односно рутер). На пример, на некоја едноставна мрежа од класата C, адресата на подразбирливиот рутер треба да гласи како w.x.y.1. Треба да се наспомене дека тука нема некое строго правило како што има кај мрежниот број или кај адресата на емитување, туку се работи за конвенција.

На пример, некоја компанија станала сопственик на една мрежа од класата C, 222.210.34.0. На оваа мрежа компанијата може да приклучат 253 компјутери, а не може да ја употреби адресата 222.210.34.0, бидејќи таа служи за означување на целата мрежа. Адресата 222.210.34.255 се употребува како адреса на емитување, а адресата 222.210.34.1 компанијата или нејзиниот Интернет провајдер ја користи како адреса на подразбирливиот рутер, кој служи за поврзување на мрежата со останатиот Интернет.

8.4.4 Подмрежни (subnet) маски

На компанија што има мал интранет составен од само еден сегмент, не постои потреба од никакво рутирање. Меѓутоа кај повеќето компјутерски мрежи тоа не е случај. Рутирањето претставува одличен начин за изолирање на поедини делови на мрежата, а тоа е од суштинско значење кога LAN мрежата се конектира на WAN мрежа. Друга причина за рутирање е тоа што компанијата има премногу IP адреси и тие не би можеле да се вметнат во само еден сегмент.

Пример - да ја разгледаме состојбата кај компанијата IBM која има мрежа од класата A, која теоретски може да поддржи до 16 милиони хостови. Управувањето на таков тип на мрежа не може да се замисли без користење на рутери. Од таа причина, IP софтверот на компјутерите од компанијата, мора да ги насочи податоците со помош на рутер, иако некои податоци воопшто не излегуваат надвор од компанијата.

Под–мрежите му овозможуваат на хостот (на секое PC до IP адреса) да одреди дали својата порака може едноставно да ја дофрли на другиот хост, или мора тоа да го изврши преку рутер. IP софтверот на хостот може да овозможи да разликува - дали некој друг хост се наоѓа на истата под–мрежа

или не. Тоа го прави со помош на така наречените под–мрежни маски (subnet mask).

Ако се земе примерот со двете под–мрежи Рим и Картагина, се гледа дека сите IP адреси во Рим имаат форма како 199.34.57.z, каде z може да биде било кој број од 1 до 255. Врз основа на ова, може да се каже дека сите членови на под–мрежата Рим кои се дефинирани како хостови, имаат идентични први три квартали во IP адресата. Поедини мрежи може да бараат членство во истата под–мрежа, но ќе ги имаат идентични само првите два квартала во IP адресата. Ова е пример за компанија која одлучила да во цела мрежа од типот B, има една единствена под–мрежа. Кога некој компјутер сака да дознае дали IP адресата што ја поседува се наоѓа на истата под–мрежа со локацијата со која сака да воспостави комуникација, тој користи под–мрежна маска. Значи под–мрежната маска одговара дали битовите се поклопуваат, за да бидат компјутерите што сакаат да комуницираат во иста под–мрежа. IP тоа го прави со помош на маска, т.е. со помош на комбинации од единици и нули како на пример:

```
11111111    11111111    11111111    00000000
```

На овој начин, сите хостови ќе ја употребуваат оваа маска. Хостот со IP адреса 199.34.57.10 (тоа е станицата A на слика 8.5), сака да потврди дали се наоѓа на иста под–мрежа како и хостот со IP адреса 199.34.57.20 (тоа е станицата B на слика 6.5). Адресата 199.34.57.10 изразена во бинарен систем гласи:

```
11000111   00100010   00111001   00001010
```

Од друга страна, IP адресата на станицата B изразена во бинарен систем гласи:

```
11000111   00100010   00111001   00010100
```

Според тоа, IP софтверот во компјутерот A врши подредување на својата IP адреса и IP адресата на станицата B. Тоа изгледа вака:

```
11000111   00100010   00111001   00001010    адреса A
11000111   00100010   00111001   00010100    адреса B
```

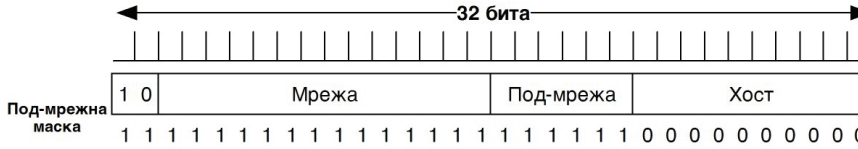
Се гледа дека вредностите на левите 27 битови потполно се поклопуваат, како и последниот краен десен бит. Но тоа не значи дека овие две адреси се наоѓаат на иста под–мрежа, бидејќи за да било кои две адреси се наоѓаат на иста под–мрежа, мора одредени битови да се поклопуваат, а тоа се оние кои

се наоѓаат во под–мрежната маска означени со единица. За да биде поочигледно - се споредува и под–мрежната маска со адресите А и В:

```
11111111   11111111   11111111   00000000  подмрежна маска
11000111   00100010   00111001   00001010    адреса А
11000111   00100010   00111001   00010100    адреса В
```

Ако се погледнат позициите на единците во секоја колона, се гледа дека овие адреси потполно се поклопуваат. Од друга страна, на позициите во под–мрежната маска каде што има нули, адресите А и В негде се поклопуваат, а негде не, тоа е ирелевантно.

Под–мрежната маска може да се разгледува и на друг начин: IANA на некоја компанија и доделува одреден опсег на IP адреси, таа компанија ги распоредува адресите како и одговара нејзе. Од вкупно 32 бита, од кои се состои секоја IP адресата на компанијата, некои битови се под контрола на компанијата, додека останатите се под контрола на IANA. Во општ случај, битовите кои се наоѓаат на левата страна ги контролира IANA, додека битовите кои ги контролираат компаниите се наоѓаат на десна страна. Така на пример, кај мрежата со класа А, IANA ги контролира првите 8 битови (крајните од лево), кај мрежата од класата В - под нејзина контрола се првите 16 бита, додека кај мрежите од класата С - цели 24 бита се под контрола на IANA.



Слика 8.8: Подмрежна маска и деловите за мрежата, подмрежата и хостот

Прашањето е - како да се знае која вредност да се искористи за под–мрежна маска. Ако компанијата поседува адресна класа С, каде што станиците се наоѓаат во само една под–мрежа, тогаш под–мрежната маска ќе биде 11111111 11111111 11111111 00000000, која во “dotted–quad” форматот може да се напише како 255.255.255.0.

Треба да се нагласи дека по дефиниција, штом некоја компанија поседува мрежа од класа С, значи дека IANA ги заклучила првите три квартали т.е. 24 бита од сите IP адреси што ги поседува компанијата; препуштени се само последните 8 бита за манипулација од страна на компанијата. Тоа значи дека првите 24 бита од IP адресите мора да се поклопуваат, додека со преостанатите 8 бита може да се прави што се сака. Под–мрежната маска мора да гласи 11111111 11111111 11111111 00000000 или 255.255.255.0.

Ако се сака оваа мрежа да се подели на две под–мрежи, тогаш може да се дефинираат броевите од 1 до 127 односно од 00000001 до 01111111 да ја претставуваат под–мрежата 1, а преостанатите броеви од 128 до 255 т.е.

100000000 до 11111111 да ја претставуваат под–мрежата 2. Во тој случај сите вредности од било која под–мрежа ќе се разликуваат во последните 7 битови, наместо како што беше кажано претходно во последните 8 битови. Според тоа под–мрежната маска мора да гласи:

```
11111111  11111111  11111111  10000000
```

односно 255.255.255.128.

Вистинската под–мрежа се состои од опсег на адреси w.x.y.0 до w.x.y.127, каде w.x.y. ги означуваат кварталите кои автоматски се доделени од NIC картичката. Другата под–мрежа се состои од адреси од опсегот од w.x.y.128 до w.x.y.255.

Потребно е исто така да се одреди мрежниот број, адресата на рутерот кој се подразбира и адресата на емитување. Мрежниот број, како што е кажано претходно, е првиот број во секој опсег на адреси, според тоа мрежниот број на првата под–мрежа гласи w.x.y.0, додека мрежниот број на втората под–мрежа гласи w.x.y.128. Втората по ред адреса од опсегот претставува адреса на рутерот кој се подразбира, па за двете под–мрежи - адресите на рутерите кои се подразбираат се w.x.y.1 и w.x.y.129. Од друга страна, адресите на емитување за двете под–мрежи се w.x.y.127 и w.x.y.255, респективно.

8.4.5 Подмрежување на мрежа од класа C

На пример, ако некоја компанија поседува мрежа од класа C и сака таа мрежа да ја подели на помали под–мрежи, тогаш одредувањето на под–мрежните маски кои ќе одговараат, мрежните броеви, адресите на емитување и адресите на рутерите кои се подразбираат може да биде многу комплицирана задача. Во Табелата 6.1. е прикажано на кој начин може некоја мрежа од класата C да се подели на една, две, четири и осум помали под–мрежи, како и одредувањето на под–мрежните маски кои ќе одговараат, мрежните броеви, адресите на емитување и адресите на рутерите. За попрегледно претставување на кварталите, воведени се ознаките w.x.y.

На пример некоја компанија сака мрежата од класа C 200.211.192.z, да ја подели на две под–мрежи. Како што се гледа од приложената табела - компанијата за секоја од двете под–мрежи ја користи под–мрежната маска и тоа 255.255.255.128. Првата под–мрежа би го имала мрежниот број 200.211.192.0, адресата на рутерот би била 200.211.192.1, додека адресата на емитување е 200.211.192.127. На тој начин на компанијата би и останале на располагање уште 125 различни адреси, од опсегот 200.211.192.2. до 200.211.192.126, што може да ги додели на своите мрежни компјутери. Што се однесува на другата под–мрежа, нејзиниот мрежен број би бил 200.211.192.128. адресата на рутерот кој се подразбира би била 200.211.192.129, додека адресата на емитување би била 200.211.192.255.

Табела 8.1: Делење на мрежа од класа C на повеќе под–мрежи.

Број на саканите под–мрежи	Под–мрежна маска	Мрежен број	Адреса на рутерот	Адреса на емитување	Преостанатите расположливи IP адреси
1	255.255.255.0	w.x.y.0	w.x.y.1	w.x.y.255	253
2	255.255.255.128	w.x.y.0	w.x.y.1	w.x.y.127	125
	255.255.255.	w.x.y.128	w.x.y.129	w.x.y.255	125
4	255.255.255.192	w.x.y.0	w.x.y.1	w.x.y.63	61
	255.255.255.	w.x.y.64	w.x.y.65	w.x.y.127	61
	255.255.255.	w.x.y.128	w.x.y.129	w.x.y.191	61
	255.255.255.	w.x.y.192	w.x.y.193	w.x.y.255	61
8	255.255.255.224	w.x.y.0	w.x.y.1	w.x.y.31	29
	255.255.255.	w.x.y.32	w.x.y.33	w.x.y.63	29
	255.255.255.	w.x.y.64	w.x.y.65	w.x.y.95	29
	255.255.255.	w.x.y.96	w.x.y.97	w.x.y.127	29
	255.255.255.	w.x.y.128	w.x.y.129	w.x.y.159	29
	255.255.255.	w.x.y.160	w.x.y.161	w.x.y.191	29
	255.255.255.	w.x.y.192	w.x.y.193	w.x.y.223	29
	255.255.255.	w.x.y.224	w.x.y.255	w.x.y.255	29

На пример некоја компанија сака мрежата од класа C 200.211.192.z, да ја подели на две под–мрежи. Како што се гледа од приложената табела - компанијата за секоја од двете под–мрежи ја користи под–мрежната маска и тоа 255.255.255.128. Првата под–мрежа би го имала мрежниот број 200.211.192.0, адресата на рутерот би била 200.211.192.1, додека адресата на емитување е 200.211.192.127. На тој начин на компанијата би и останале на располагање уште 125 различни адреси, од опсегот 200.211.192.2. до 200.211.192.126, што може да ги додели на своите мрежни компјутери. Што се однесува на другата под–мрежа, нејзиниот мрежен број би бил 200.211.192.128. адресата на рутерот кој се подразбира би била 200.211.192.129, додека адресата на емитување би била 200.211.192.255.

Ако сакаме, со овој процес на подмрежување може да продолжиме и понатаму, т.е. да се креираат 16 под–мрежи, од кои на секоја од нив да бидат сместени 13 хостови (треба да се знае дека за секоја под–мрежа се губат по три адреси - за мрежен број, за адреса на рутерот и за адресата на емитување). Исто така, со овој процес на подмрежување може да се креираат дури 32 под–мрежи, и на секоја под–мрежа би биле сместени по 5 хоста, но треба да се наспомене дека тоа е голем и непотребна загуба на IP адресите што се расположливи.

8.4.6 Classless Inter–Domain Routing (CIDR)

IANA доделува адресни класи A, B и C. Меѓутоа постојат голем број на помали компании на кои им е потребен Интернет домен што им одговара, т.е. не е економично на такви компании да им се додели мрежа од класата C, бидејќи C мрежата содржи 256 расположливи адреси, додека повеќето од таквите компании поседуваат само десетина компјутери што би сакале да имаат пристап на Интернет. Постојат исто така и големи компании што сакаат да имаат таен пристап на Интернет, а поради безбедност не сакаат сите компјутери да имаат пристап на Интернет, туку само на интерната компјутерска мрежа што не е прикачена на Интернет. Меѓутоа одреден степен на присуство на Интернет, денес е апсолутно неопходно, како на пример за потребите на e–mail серверот, FTP серверот, web серверот и слично – така да потребно е да се има отприлика неколку десетини IP адреси. Во вакви случаи, доделувањето на цела мрежа од типот C со вкупно 256 адреси претставува недопустливо трошење на адреси.

Исто така има примери кога на некоја компанија и се потребни неколку стотина адреси, што е повеќе од 256, но не и многу повеќе од тој број. Овој тип на фирми се премногу големи за да поседуваат мрежа од класата C, но истовремено и многу мали за да поседуваат мрежа од класата B, која пак содржи 65.536 расположливи адреси. Од таа причина IANA започнала со доделување на IP адреси, кои се потполно ослободени од рестрикциите што ги имаат веќе застарените распределби на мрежите од класи A, B и C. Оваа нова метода на доделување на адреси, е позната под името „бескласно меѓу–доменско рутирање“, односно Classless Inter–Domain Routing, или скратено CIDR, кое се изговара како „сајдер“. CIDR мрежите се означуваат како „slash x“ (коса цртичка x) мрежи, каде x претставува број на битови во опсегот на IP адресата што ја контролира IANA.

Доколку некоја компанија поседува мрежа од класата A, тогаш IANA ги контролира горните 8 бита, додека компанијата ги контролира останатите т.е. долните 24 бита. Ако од некоја причина, компанијата одлучи од својата A мрежа да формира една единствена огромна под–мрежа, како тогаш би гласела подмрежната маска? Бидејќи целата мрежа од класа A преставува единствена под–мрежа, за да се одреди дали почетната и одредишната адреса припаѓаат на иста под–мрежа, компанијата ќе мора да ги спореди само првите квартали на овие IP адреси. На пример, ако некоја компанија има мрежа 4.0.0.0, тогаш адресите 4.55.22.81 и 4.99.63.88, се наоѓаат на истата под–мрежа.

Според тоа, подмрежната маска на компанијата би била 11111111 00000000 00000000 00000000 или 255.0.0.0. Ако се прочита подмрежната маска од лево, таа се состои од осум бинарни единици, после кои следат само бинарни нули. Меѓутоа според CIDR терминологијата, компанијата впрочем не поседува мрежа од класата A, туку slash 8 мрежа. Таа се означува како „4.0.0.0/8“, наместо како „4.0.0.0 со подмрежна маска 255.0.0.0“.

Кај мрежите од класа B, IANA ги контролира горните 16 бита, додека компаниите (корисниците на адреси) ги контролираат преостанатите 16 битови. Ако компанијата одлучи од мрежата со класа B да направи само една единствена под–мрежа, тогаш ќе ја користи подмрежната маска 11111111 11111111 00000000 00000000, или 255.255.0.0. Ако се чита од лево на десно, ќе се види дека подмрежната маска се состои од 16 бинарни единици, а преостанатите се бинарни нули. Според CIDR терминологијата - мрежата од класа B се означува како slash 16 мрежа. Така на пример, ако компанијата поседува мрежа од класата B, со подмрежна маска 255.255.0.0, тогаш таа во „slash" форматот би била означена како 164.109.0.0/16.

Што се однесува за мрежата од класа C, тука IANA ги контролира горните 24 бита, додека компаниите (корисниците) ги контролираат останатите 8 бита. Доколку мрежата од класа C се третира како една единствена под–мрежа, нејзината подмрежна маска би била 11111111 11111111 11111111 00000000. Ако се чита од лево на десно ќе се види дека подмрежната маска се состои од 24 бинарни единици, а преостанатите се бинарни нули. Според CIDR терминологијата мрежата од класа C се означува како slash 24 мрежа. Така на пример, ако компанијата поседува мрежа од класата C и тоа 206.246.253.0, со подмрежна маска 255.255.255.0, тогаш таа во „slash" форматот би била означена како „206.246.253.0/24". Разбирањето на /24 номенклатурата е многу важна бидејќи таа често се сретнува во праксата кај поедини типови на рутери. Така на пример, ASCEND рутерот никогаш не бара да се внесе подмрежна маска, исклучиво прифаќа коса црта.

Флексибилноста на CIDR методот се гледа во тоа што IANA сега може да дефинира не само A, B и C типови на мрежи, меѓутоа и голем број на други мрежи чија подмрежна маска се наоѓа помеѓу A, B и C мрежата. На пример, ако некоја компанија сака да креира мрежа со 50 компјутери, во минатото IANA морала да и додели мрежа со класа C, со вкупно 256 адреси. Денеска IANA може да и понуди на компанијата мрежа со подмрежна маска 11111111 11111111 11111111 11000000 (255.255.255.192), оставајќи на тој начин само 6 бита со кои компанијата може да прави што сака. Бројот 2^6 изнесува 64, така да компанијата добила вкупно 64 адреси, што може да ги преуредува и доделува како сака. Овој тип на мрежа би се означила како slash 26 (/26) мрежа.

Од изнесената табела се гледаат сите можни типови на мрежи. Некои од нив едноставно не се достапни како на пример мрежата slash 0, додека други немаат никаква смисла, како на пример мрежата slash 31, (која содржи само две можни адреси што веднаш би се потрошиле за мрежниот број и адресата на емитување, па после тоа доделување ќе се остане без ниедна адреса за практична употреба). Најмалата мрежа која ARIN (тоа е американски огранок на организацијата IANA), може да ја додели, е мрежата slash 20 која има вкупно 4.094 IP адреси.

Во денешно време кога се креира компјутерска мрежа, не може да се изостави т.е. заобиколи CIDR методот. Поради тоа Интернет провајдерите обично доделуваат slash 26 мрежи.

8.4.7 Детекција на гршки во IP

Секој IP пакет содржи 1 бит на податоци, со име - контролна сума на заглавјето (checksum header) со кој се проверува дали на патот од испраќачот до примачот дошло до оштетување на информацијата во заглавјето (header) на пакетот.

Многу протоколи за комуникација употребуваат вакви контролни суми, кои функционираат на следниот начин: на пратената порака со помош на контролната сума се проверува дали податоците во пораката се оштетени во текот на транспортот, од одредени шумови на линијата. Доколку се потврди дека податоците не претрпеле никакво оштетување - се праќа порака на испраќачот во која пишува „сè е во ред – примено“. Ако контролната сума покаже дека податоците пристигнале оштетени, тогаш се праќа порака на испраќачот во која пишува „податоците се оштетени – пратете ги повторно“, по што испраќачот го праќа повторно истиот пакет со податоци на примачот. Овие пораки кои меѓусебно ги разбираат и примачот и испраќачот се викаат ACK и NAK пораки – односно позитивни и негативни потврди (acknowledgments) за приемот на податоците. За протоколите кај кои се применува овој пристап на „проверка и потврда“ (check – and – acknowledge), се вика дека даваат доверлив (reliable) сервис.

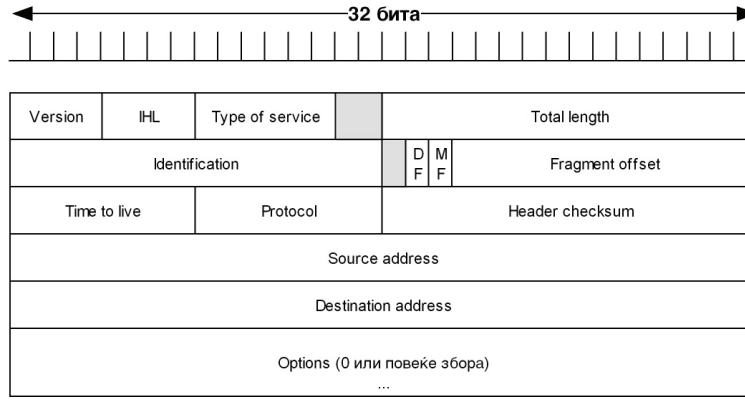
Меѓутоа IP протоколот не дава доверлив сервис. Кога IP примачот ќе добие некој оштетен пакет на податоци, тој едноставно ќе го одбие тој пакет и за тоа нема да го извести испраќачот. Тоа е поради тоа што TCP е протоколот кој обезбедува доверливост. Од друга страна, IP контролната сума на заглавјето служи само за проверка дали заглавјето на пакетот е валидно; доколку не е - оштетениот датаграм ќе биде одбиен.

Заклучно со ова се кажани сите задачи што се во надлежност на IP протоколот. IP не е наменет да овозможи гарантиран пренос на податоци од крај до крај на комуникациската линија. IP протоколот постои за една единствена причина: рутирањето. Бидејќи IP протоколот не е одговорен, при преносот на податоците да го обезбеди нивниот потполн интегритет, создаден е TCP протоколот кој е негов придружник и е задолжен за тоа.

8.4.8 Заглавје на IP протоколот

Соодветно место за изучување на мрежното ниво на Интернет е форматот на IP датаграмите. IP датаграмот се состои од header и текстуален дел. Хедерот има 20-бајтен фиксен дел и работен дел со променлива должина. Форматот на хедерот е даден на сл. 8.9. Тој се пренесува по big-endian редослед: од лево надесно, при што најзначајниот бит од полето Version оди прв. (SPARC

е big endian; Pentium е little-endian.) Кај little endian машините, потребна е софтверска конверзија кај испраќачот и кај примачот.



Слика 8.9: Заглавје на IPv4 (Интернет Протокол).

Полето Version ја содржи верзијата на протоколот на кој припаѓа датаграмот. Со вклучување на верзијата во секој датаграм, станува можно преводот на IP адреси да трае со години, при што некои машини користат стара, а други - нова верзија. Во моментов се прави превод од IPv4 во IPv6, и тоа трае повеќе години, и нема изгледи дека ќе заврши набрзо.

Бидејќи должината на хедерот не е константна, полето IHL служи да каже колку е долг хедерот во 32-битни зборови. Минималната вредност е 5, и таа се користи кога не постојат додатни опции. Максималната вредност на ова 4-битно поле е 15, што го лимитира хедерот на 60 бајти, и полето Options на 40 бајти. За некои опции, како што е снимање на патеката на пакетот, 40 бајти е многу малку, т.е. некорисно.

Полето Type of service е едно од неколкуте полиња што го сменило своето значење со тек на годините. Тоа се користело и сеуште се користи за правење разлика помеѓу различните класи на сервис. Можни се различни комбинации за доверливоста и брзината. За пренос на глас, брзата достава е многу важна. За пренос на датотеки, без-грешната трансмисија е поважна отколку брзата трансмисија.

Оригинално, 6-битното поле содржи (од лево надесно), три-битно Precedence поле и три флага, D, T, и R. Полето Precedence го дава приоритетот, од 0 (нормален) до 7 (мрежен контролен пакет). Трите флага му овозможуваат на хостот да специфицира што му е најважно од {Доцнење, Проток, Доверливост}. Теоретски, овие полиња им овозможуваат на рутерите да направат избор помеѓу, на пр., сателитска врска со голем проток и големо доцнење, или изнајмена линија со мал проток и мало доцнење. Во пракса, рутерите честопати го игнорираат полето Type of service.

Евентуално, IETF го менува малку полето за да овозможи различни класи на сервиси. Шест бита се користат да индицираат на кој сервис му припаѓа

пакетот. Класите на сервис имаат редоследни приоритети, три веројатност за отфрлање, и историски класи.

Полето Total length опфаќа сè што е во датаграмот - и хедерот и податоците. Максималната должина е 65,535 бајти. Денес, горната граница се толерира, но во идните гигабитни мрежи, можеби ќе бидат потребни поголеми датаграми.

Полето Identification е потребно за да му овозможи на дестинациониот хост да одреди на кој датаграм припаѓа ново-пристигнатиот фрагмент. Сите фрагменти на датаграмот содржат иста вредност Identification.

Потоа доаѓа еден неискористен бит и две 1-bit полиња. DF значи Don't Fragment. На рутерите им се наредува да не го фрагментираат датаграмот, бидејќи дестинацијата не може да ги склопи парчињата заедно. На пр., кога компјутерот се подига, ROM-от може да побара од меморијата да испрати слика како еден датаграм. Со означување на датаграмот со DF bit, испраќачот знае дека тој ќе пристигне како една целина, дури и ако датаграмот ги избегнува малите пакетни мрежи и избере понеоп. Сите машини треба да користат фрагменти од 576 бајти или помалку.

MF значи More Fragments. Сите фрагменти освен последниот ги имаат овие битови. Потребно е да се знае кога пристигнале сите фрагменти на датаграмот.

Fragment offset кажува каде во тековниот датаграм припаѓа фрагментот. Сите фрагменти освен последниот во датаграмот мора да се мултипли од 8 бајти, што е елементарна фрагментна единица. Бидејќи се обезбедени 13 бита, има максимум 8192 фрагменти по датаграм, давајќи максимална должина на датаграмот од 65,536 бајти, еден повеќе од Total length полето.

Полето Time to live е бројач што се користи да го ограничи животниот век на пакетот. Се претпоставува дека времето се мери во секунди, дозволувајќи максимален животен век 255 sec. Тоа се намалува во секој скок за еден, а се намалува за повеќе ако пакетот долго чека во ред кај рутерот. Во пракса, се бројат само скоковите. Кога дојде до нула, пакетот се враќа и предупредувачки пакет се праќа назад кон изворишето. Оваа особина ги заштитува датаграмите од лутање наоколу, што може да се случи ако рутирачките табели се оштетат.

Кога мрежното ниво ќе го состави целиот датаграм, треба да знае што ќе прави со него. Полето Protocol кажува на кој транспортен протокол ќе се предаде датаграмот. TCP е една можност, но постои и UDP и други протоколи. Броењето на протоколи е глобално за целиот Internet. Протоколите и другите доделени броеви биле содржани во RFC 1700, но денес се содржат во база на податоци лоцирана на www.iana.org.

Header checksum го верификува хедерот. Таквата сума се користи за детекција на грешки генерирани во меморијата на рутерот. Алгоритамот додава до 16-битни зборови како што пакетите пристигнуваат, користејќи единечно комплементарна аритметика и правејќи комплемент на резултатот. За овој алгоритам, Header checksum треба да биде нула по пристигнувањето.

Овој алгоритам е поробусен отколку обичното собирање. Забележете дека Header checksum мора да се пресмета во секој скок, бидејќи барем едно поле секогаш се променува (Time to live полето), а можат да се применат трикови за да се забрзаат пресметките.

Source адресата и Destination адресата го индицираат бројот на мрежата и бројот на хостот. Internet адресите ќе бидат дискутирани подолу. Полето Options е дизајнирано да обезбеди различни верзии на протоколот, да вклучи информации кои не се во оригиналниот дизајн, да им забрани на хакерите да испробуваат нови идеи, и да не ги доделуваат хедерските битови за информации кои ретко се користат. Опциите се со променлива должина. Секоја почнува со 1-бајтен код што ја идентификува опцијата. Некои опции се следени со 1-бајтно опционо поле за должина, а потоа следат податоците. Полето Options се дели на полиња од по 4 бајти. Оригинално, се дефинираат пет опции, како во табела 8.2, но во последно време се додаваат и некои нови. Најновата листа на опции се одржува on-line на www.iana.org/assignments/ip-parameters.

Табела 8.2: Некои IP опции.

Опција	Опис
Security	Ја специфицира тајноста на датаграмот
Strict source routing	Ја определува патеката која треба да се следи
Loose source routing	Дава листа на рутери кои не треба да се одминат
Record route	Секој рутер придружува своја IP адреса
Timestamp	Секој рутер придружува своја IP адреса и временска маркица

Опцијата Security кажува колку тајна е информацијата. Теоретски, воениот рутер може да го користи ова поле да забрани рутирање низ некои земји кои се "опасни." Во пракса, рутерите го игнорираат, така што негова практична функција е да им помогне на шпионите да откријат каде се кријат тајните.

Опцијата Strict source routing ја дава целосната патека од изворишето до дестинацијата како секвенца од IP адреси. Потребно е датаграмот да ја следи точната патека. Најкорисно за администраторите е да испратат пакет за итна помош кога рутирачките табели се оштетени, или да прават мерење на времето.

Опцијата Loose source routing бара да пакетот да патува преку точно одредени рутери, по наведен редослед, но можно е да помине и преку други рутери на патеката. Нормално е, оваа опција која наведува само неколку рутери, да форсира одредена патека. На пр., ако се форсира пакетот од London до Sydney да оди на запад наместо на исток, оваа опција мора да ги наведе рутерите во New York, Los Angeles, и Honolulu. Оваа опција е корисна кога политичките или економските услови диктираат избегнување на одредени земји.

Опцијата Record route им кажува на рутерите да ја додадат својата IP адреса на опцијата Поле. Ова им овозможува на мрежните менаџери да ги следат грешките во рутирањето ("Зошто пакетите од Houston до Dallas отишле прво

во Токио?"). Кога била дизајнирана ARPANET, ниеден пакет не поминувал низ повеќе од 9 рутери, така што 40 бајти за оваа опција биле доволни. Како што спомнавме погоре, ова е многу мала вредност.

Конечно, опцијата Timestamp е слична со опцијата Record route, при што освен чувањето на 32-битната IP адреса, секој рутер снима и 32-битна временска маркица. Оваа опција, исто така претежно се користи за дебагирање на алгоритмите за рутирање.

8.5 TCP (TRANSMISSION CONTROL PROTOCOL)

IP протоколот е задолжен за рутирање, и не се грижи за тоа дали некоја порака стигнала до своето крајно одредиште. Ако постојат 7 IP скокови (hops) од една до друга точка на мрежата, тогаш секој од овие скокови преставува потполно независна активност – не постои никаква координација, никакво значење дали конкретниот скок претставува трет по ред во низата од седумте скокови, или петти. Ниеден IP скок не е свесен дека постојат други скокови. Од овде следи дека со IP протоколот не може да се овозможи доверлив сервис за пренос на податоци.

TCP (т.е. Transmission Control Protocol) дава доверлив „end–to–end" сервис, кој гарантира правилна испорака на пакетите. Освен тоа TCP дава уште неколку сервиси, меѓу кои најзначајни се оние под името sockets. Покрај изразената доверливост, TCP се одликува и со други вредности. Треба да се наспомене дека TCP има свој „роднина" т.е. протокол кој има слична улога како TCP, со таа разлика што тој не гарантира потполн (end–to–end) интегритет при преносот на податоци. Овој протокол е познат под името UDP (User Datagram Protocol).

Ова е сè што може да се каже за основната идеја на која се заснова TCP. Негова основна задача е да обезбеди правилен пренос на податоци од еден интранет хост на друг. Негови главни карактеристики се:

- Ракување (handshake)
- Секвенцирање на пакети (packet sequencing)
- Контрола на текот (flow control)
- Отстранување на грешки (error handling)

За разлика од IP протоколот, кој воопшто не води сметка – и едноставно ги турка податоците кон одредишниот компјутер без оглед дали компјутерот е спремен да ги прими или не, TCP секогаш проверува дали двете страни прописно се претставиле една на друга пред да почне трансферот на податоци. Од ова следи дека TCP протоколот е тој кој воспоставува конекција.

8.5.1 Секвенцирање на пакети (packet sequencing)

Бидејќи IP не користи т.н. виртуелно коло (virtual circuit), може да се случи различни пакети на одредиштето да пристигнат во различно време и тоа во неправилен редослед. Да замислиме еден едноставен интранет, на кој се врши пренос на четири сегменти од некои податоци, при што на мрежата постојат повеќе алтернативни патишта за пренос. Да претпоставиме дека првиот сегмент од некоја причина го употребил заобиколниот пат и поради тоа на одредиштето пристигнал со мало задоцнување. За разлика од него - вториот, третиот и четвртиот сегмент го употребиле пократкиот пат и на одредиштето стигнале пред да стигне првиот сегмент. Во тој случај, работата на TCP софтверот кај одредишниот компјутер е да ги подреди овие сегменти повторно по нивниот правилен редослед.

8.5.2 Контрола на текот (flow control)

Контролата на текот (flow control) на податоци, тесно е поврзана со секвенцирањето. На пример, се следат 50 сегменти на податоци; кај одредишниот компјутер пристигнуваат сите 50 сегменти и тоа по испревртен редослед. Приемниот компјутер мора сите овие сегменти најнапред да ги складира во работната меморија, а потоа по правилно сортирање да ги сними на хард дискот. Од овде произлегува една задача на TCP протоколот, а тоа е ускладување на ритам (pacing) при преносот на податоците – тој нема да ги прати кон одредиштето, сè додека примачот не биде спремен да ги прими.

8.5.3 Детекција/корекција на грешки

TCP протоколот е одговорен за детекција на грешките и нивно отстранување. По начинот на кој тој се справува со настанатите грешки, може да се каже дека TCP е многу ефикасен во оваа работа. Поедини протоколи вршат детална анализа за секој поединечен блок на податоци, при тоа генерализирајќи голем број на додатни (overhead) блокови. Наспроти тоа, TCP протоколот користи сосема друг метод. Тој на испраќачот му праќа порака со содржина „јас сум способен да примам одреден број на блокови во својот бафер, па не очекувајте од мене потврда за прием, сè додека не го примам максималниот можен број на блокови. Освен тоа, доколку потврдам дека некои од примените блокови се оштетени, јас за нив нема да пратам потврда за прием. Според тоа, ако во очекуваниот временски интервал од мене не примиш потврда за некој конкретен блок, слободно можеш да го пратиш повторно“.

8.5.4 Функционирање на TCP протоколот

Во ова поглавје ќе дадеме општ приказ на TCP протоколот. Подолу ќе го опишеме хедерот на овој протокол, поле по поле.

Главна особина на TCP, т.е. главна карактеристика на неговиот дизајн, е дека секој бајт од TCP конекцијата има сопствен 32-битен секвентен број. Кога почнал Internet, линиите помеѓу рутерите во главно биле 56-kbps изнајмени линии, така што и на најбрзиот хост му требало 1 недела да ги листа секвентните броеви. Кај модерните мрежи, секвентните броеви се во разумни граници, како што ќе видиме подоцна. Одделни 32-битни секвентни броеви се користат за потврда и за механизмот со прозорци, како што ќе опишеме подолу.

Испраќачките и примачките TCP ентитети разменуваат податоци во форма на сегменти. TCP сегментот се состои од фиксен 20-бајтен хедер (плус опционен дел) проследен со нула или повеќе податочни бајти. TCP софтверот одлучува колку големи треба да бидат сегментите. Тој може да акумулира податоци од неколку запишувања во еден сегмент или да ги подели податоците од еден запис во повеќе сегменти. Постојат две ограничувања за големината на сегментот. Прво, секој сегмент, вклучително TCP хедерот, мора да се смести во 65,515-бајтен IP простор. Второ, секоја мрежа има максимален трансфер MTU, и секој сегмент мора да се смести во MTU. Во пракса, MTU е обично 1500 бајти (Ethernet товар) и ја дефинира горната граница за големината на сегментот.

Основниот протокол што го користат TCP ентитетите, е протоколот со лизгачки прозорец. Кога испраќачот праќа сегмент, тој стартува тајмер. Кога сегментот пристига кај одредиштето, приемниот TCP ентитет враќа сегмент (со или без податоци) носејќи број за потврда еднаков со следниот секвентен број што очекува да го прими. Ако тајмерот кај испраќачот се исклучи пред да пристигне потврдата, испраќачот повторно го испраќа сегментот.

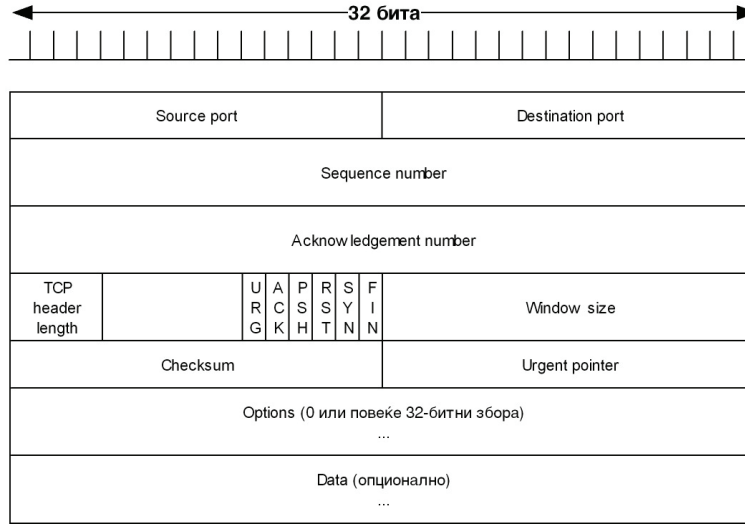
Иако овој протокол звучи едноставно, постојат голем број додатоци, што ќе бидат објаснети подолу. Сегментите можат да пристигнат без ред, така што бајтите 3072–4095 можат да пристигнат, но не можат да се потврдат, бидејќи бајтите 2048–-3071 сеуште не се активни. Сегментите можеби ќе доцнат при транспортот, така што испраќачот оди во тајмаут и ги испраќа повторно. Ретрансмисијата може да опфати различни бајтни интервали во однос на оригиналниот пренос, барајќи точна евиденција за тоа кои бајти се примени коректно. Сепак, бидејќи секој бајт од низата има свој сопствен offset, ова може да се постигне.

TCP мора да биде спремен да се справи со овие проблеми и да ги реши на ефикасен начин. Одреден напор треба да се вложи за оптимизација на перформансите на TCP низите, дури и во присуство на мрежни проблеми. Различни алгоритми кои се применети во различни TCP имплементации се дискутирани подолу.

8.5.5 Заглавје на TCP сегмент

Слика 8.10 го прикажува изгледот на TCP сегментот. Секој сегмент почнува со фиксно-форматиран, 20-бајтен хедер. Фиксниот хедер може да биде проследен со хедерски опции. После опциите доаѓаат 65,535 - 20 - 20 =

65,495 податочни бајти, при што првите 20 се однесуваат на IP хедерот, а вторите - на TCP хедерот. Сегменти без податоци се дозволени и се користат за потврдни и за контролни пораки.



Слика 8.10: Заглавје на TCP сегмент

Да го разгледаме TCP хедерот поле по поле. Полињата Source port и Destination port ги идентификуваат локалните крајни точки на конекцијата. Добро-познатите порти се дефинирани на www.iana.org, но секој хост може да алоцира други по желба. Портата плус IP адресата на хостот формираат 48-битна единствена крајна точка. Изворишната и дестинационата крајна точка заеднички ја идентификуваат конекцијата.

Полињата Sequence number и Acknowledgement number ги обавуваат нивните вообичаени функции. Забележете дека се очекуваат спецификациите за следните бајти, а не за претходно примените. И двете се долги по 32 бита, бидејќи секој бајт со податоци е означен како TCP низа.

Должината на TCP хедерот кажува колку 32-битни зборови се содржани во TCP хедерот. Оваа информација е потребна, бидејќи полето Options е со променлива должина, а исто така и хедерот. Технички, ова поле го означува почетокот на податоците во сегментот, измерени во 32-битни зборови, и тој број ја претставува должината на хедерот изразена во зборови, така што ефектот е ист.

Потоа доаѓа 6-битно поле што не се користи. Фактот што ова поле опстанало повеќе од 25 години е доказ колку добро е осмислен TCP. На другите протоколи им требало отклонување на грешките во оригиналниот дизајн.

Потоа доаѓаат шест 1-битни флага. URG е поставен на 1 ако се користи Urgent покажувачот. Urgent покажувачот го прикажува offset-от од тековниот секвентен број на кој се наоѓаат ургентните податоци. Овој покажувач е индикатор на прекинатите пораки. Како што спомнавме погоре,

овој покажувач претставува главно средство што му овозможува на испраќачот да му сигнализира на примачот (без примена на TCP) за причината на прекинот.

Битот ACK е поставен на 1 за да индицира дека бројот за потврда е валиден. Ако ACK е 0, сегментот не содржи потврда, така што полето Acknowledgement number се игнорира.

Битот PSH ги покажува PUSHed податоците. Примачот се замолува да ги достави податоците до апликацијата по пристигањето, а не да ги чува во бафер (што може да го направи за подобра ефикасност).

Битот RST се користи за ресетирање на конекцијата што станала конфузна заради пад на хост или некои други причини. Тој исто така се користи за отфрлање на погрешните сегменти и за детекција на неуспешен обид за отворање конекција. Во општ случај, ако добиете сегмент со вклучен бит RST, веќе имате проблем.

Битот SYN се користи за воспоставување на конекцијата. Барањето за конекција има SYN = 1 и ACK = 0 за да индицира дека piggyback полето за потврда не се користи. Одговорот на конекцијата содржи потврда, па така SYN = 1 и ACK = 1. Во суштина, SYN битот се користи да означи CONNECTION REQUEST и CONNECTION ACCEPTED, со бит ACK кој ги разликува овие две можности.

Битот FIN се користи за ослободување на конекцијата. Тој специфицира дека испраќачот нема повеќе податоци за пренос. Сепак, по затворање на конекцијата, процесот на примање податоци може да продолжи бесконечно. И SYN и FIN сегментите имаат секвентни броеви и гарантираат процесирање во точен редослед.

Контролата на проток кај TCP се прави со лизгачки прозорец со променлива величина. Полето Window size кажува колку бајти може да се испратат после бајтот за потврда. Полето Window size = 0 е дозволено и кажува дека бајтите и бројот Acknowledgement - 1 се примени, но дека примачот е оштетен и не може да прима повеќе податоци. Примачот може подоцна повторно да се активира пренесувајќи сегмент со ист Acknowledgement број и ненулто поле Window size.

Кај претходните протоколи, рамките за потврда пристигаа заедно со дозволата за испраќање на нови рамки. Ова е последица на прозорецот со фиксна големина кој се користи кај сите протоколи. Кај TCP, потврдата и дозволата за испраќање понатамошни податоци се целосно одвоени. Како резултат, примачот може да каже: “јас примив доволно бајти и не сакам повеќе во моментов“. Ова раздвојување (всушност, прозорец со променлива должина) дава дополнителна флексибилност. Тоа е опишано подолу.

Checksum се користи за дополнителна доверливост. Тоа го проверува хедерот, податоците и концептуалниот псевдо-хедер. Кога се прави проверката, полето Checksum е поставено на нула, а податочното поле се проширува со додатна нула ако неговата должина е непарен број. Алгоритамот за checksum едноставно додава 16-битни зборови во единичен

комплемент, а потоа прави комплемент и на сумата. Како последица на ова, кога примачот ќе ја пресмета вредноста на целиот сегмент, вклучувајќи го и Checksum полето, резултатот треба да биде 0.

Псевдо-хедерот содржи 32-битни IP адреси на изворишетето и дестинацијата, број на протоколот TCP (6), и број на бајти во TCP сегментот (вклучувајќи го хедерот). Вклучувањето на псевдо-хедерот во TCP checksum помага во детекцијата на недоставените пакети, но исто така ја нарушува протоколската хиерархија, бидејќи IP адресите во него припаѓаат на IP нивото, а не на TCP. UDP го користи истиот псевдо-хедер во неговата checksum.

Полето Options обезбедува дополнителни можности кои не се содржани во обичниот хедер. Најважна опција е онаа што му овозможува на секој хост да го специфицира максималниот TCP товар што е спремен да го прими. Користењето на големи сегменти е поефикасно, бидејќи 20-бајтниот хедер може да се амортизира со поголемиот податочен дел, но некои хостови не се способни да примаат големи сегменти. За време на поставување на конекцијата, секоја страна го кажува својот максимум и го дознава максимумот на другите. Ако хостот не ја користи оваа опција, тој зема предефиниран 536-бајтен товар. Сите хостови на Интернет прифаќаат TCP сегменти од 536 + 20 = 556 бајти. Максималната големина на сегмент во двете насоки не мора да биде иста.

За линии со голем опсег, големо доцнење, или двете, 64-KB прозорец е проблем. Кај T3 линија (44.736 Mbps), треба само 12 msec за испраќање на цел 64-KB прозорец. Ако доцнењето во двата правци е 50 msec (што е типична интер-континентална оптичка врска), испраќачот ќе биде празен 3/4 од времето чекајќи потврди. Кај сателитските врски, ситуацијата е и полоша. Поголемиот прозорец ќе му дозволи на испраќачот да испраќа многу податоци, но примената на 16-битно поле Window size, не дозволува нивно примање. Со RFC 1323, предложена е опција Window scale, која им овозможува на испраќачот и примачот да се договорат за ширината на прозорецот. Овој број им дозволува на двете страни да го шифтираат полето Window size до 14 бита на лево, овозможувајќи на тој начин прозорци со 2^{30} бајти. Повеќе TCP имплементации ја содржат оваа опција.

Друга опција предложена од RFC 1106 и широко имплементирана, е протоколот со селективно повторување без враќање назад. Ако примачот добие еден лош сегмент и многу добри после него, обичниот TCP протокол ќе оди тајмаут и ќе ги ретрансмитира непотврдените сегменти, вклучително и точно-примените (т.н. go back n протокол). RFC 1106 воведува NAK за да му овозможи на примачот да бара точно одредени сегменти. После ова, тој ги потврдува баферираните податоци, со што се редуцира количината на ретрансмитирани податоци.

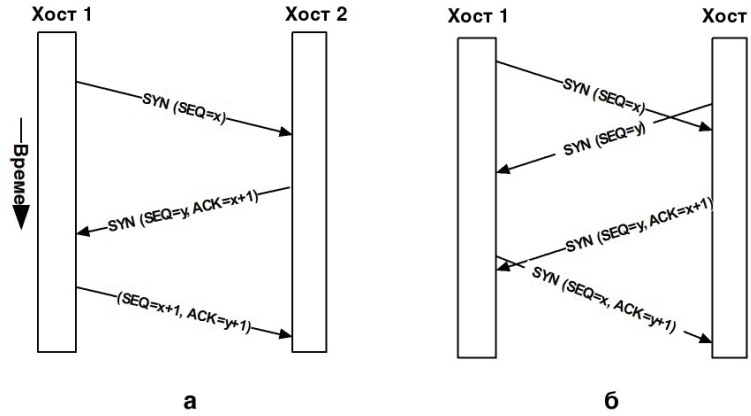
8.5.6 Воспоставување на конекција кај TCP

Конекциите се воспоставуваат кај TCP со помош на три-насочно ракување опишано погоре. За да се воспостави конекција, серверот пасивно чека извршувајќи ги примитивите LISTEN и ACCEPT, специфицирајќи или не одреден извор.

Другата страна, т.е. клиентот, извршува примитива CONNECT, специфицирајќи IP адреса и порта на која сака да се конектира, максимална големина на TCP сегментот, и некои додатни податоци (на пр., password). Примитивата CONNECT испраќа TCP сегмент со вклучен SYN bit, исклучен ACK bit и чека одговор.

Кога сегментот пристигнува кај одредиштето, TCP ентитетот проверува дали постои процес што прави LISTEN на портата наведена во полето Destination port. Ако не постои, испраќа одговор со RST bit како отфрлање на конекцијата.

Ако некој процес ја слуша портата, на тој процес му се доделува примачки TCP сегмент. Тој може да ја прифати или одбие конекцијата. Ако ја прифати, се враќа сегмент за потврда. Секвенцата од TCP сегменти испратена во нормален случај е дадена на слика 8-1(a). Забележете дека SYN сегментот троши 1 бајт од секвентниот простор така што може да се потврди недвосмислено.



Слика 8.11: (a) Ослободување на TCP конекцијата во нормален случај. (b) Колизија на повици.

Ако два хоста истовремено се обидат да воспостават конекција помеѓу два исти сокети, секвенцата на настани е илустрирана на слика 8.11(b). Резултатот на овие настани е што се воспоставува една, а не две конекции, бидејќи конекциите се идентификуваат според нивните крајни точки. Ако прво имаме конекција означена со (x, y), а вториот обид го прави истото - во табелата ќе има само еден запис (x, y).

Почетниот секвентен број на конекцијата не е 0 заради гореспоменатите причини. Се користи шема базирана на часовник, со импулс на секои 4 μsec.

За дополнителна сигурност, кога ќе падне хостот, тој може да не се подига извесно време (колку што е животниот век на пакетите) за да се осигура дека нема пакети кои кружат од претходните конекции.

8.5.7 Ослободување на конекцијата кај TCP

Иако TCP конекциите се full duplex, за да се разбере како се ослободува конекцијата - треба да се разгледува како пар simplex конекции. Секоја simplex конекција се ослободува независно. За да ја ослободи конекцијата, секоја страна испраќа TCP сегмент со FIN битови, што значи дека нема повеќе податоци за пренос. Кога ќе се потврди FIN, таа насока е затворена за нови податоци. Сепак, податоците можат да течат во другата насока. Кога двете насоки ќе се исклучат, конекцијата се ослободува. Вообичаено, четири TCP сегменти се потребни за ослободување на конекцијата, по еден FIN и еден ACK за секоја насока. Сепак, можно е првиот ACK и вториот FIN да се содржани во ист сегмент, намалувајќи го вкупниот број на три.

Како и во случајот со телефонски повик, кога и двете страни можат да кажат ’чао’ истовремено и да спуштат слушалка, двата краја на TCP конекцијата може да пратат FIN сегменти истовремено. Тие се потврдуваат на идентичен начин, и конекцијата се прекинува. Не постои суштинска разлика помеѓу двата хоста кога ја ослободуваат врската заедно или еден по еден.

За да се избегне проблемот на две армии, се користат тајмери. Ако нема одговор на FIN во максимум 2 животни века на пакетот, испраќачот на FIN ја ослободува конекцијата. Другата страна ќе забележи дека никој не слуша повеќе и ќе оди во тајмаут. Иако ова решение не е совршено, фактот дека не постои совршено решение, го прави применливо. Во пракса, ретко се јавуваат проблеми.

8.5.8 Управување со TCP конекцијата

Чекорите потребни за воспоставување и ослободување на конекциите можат да се прикажат со конечен автомат со 11 состојби дадени на слика 8.12. Во секоја состојба, дозволени се одредени настани. Кога ќе се случи дозволен настан, се превземаат одредени акции. Ако се случи друг настан, се јавува грешка.

Секоја конекција започнува со состојба CLOSED. Таа ја напушта состојбата, кога е пасивно отворена (LISTEN), или активно отворена (CONNECT). Ако другата страна го прави спротивното, се воспоставува конекција и состојбата станува ESTABLISHED. Ослободувањето на конекцијата може да го направи било која страна. Кога ќе се комплетира, состојбата се враќа во CLOSED.

Конечниот автомат е прикажан на слика 8.13. Вообичаен случај е клиентот активно да се конектира на пасивен сервер, што е прикажано со дебели линии - полна кај клиентот, испрекината кај серверот. Тенките линии претставуваат неочекувани настани. Секоја линија на слика 8.13 е означена со пар настан/акција. Настанот може да биде системски повик од корисникот

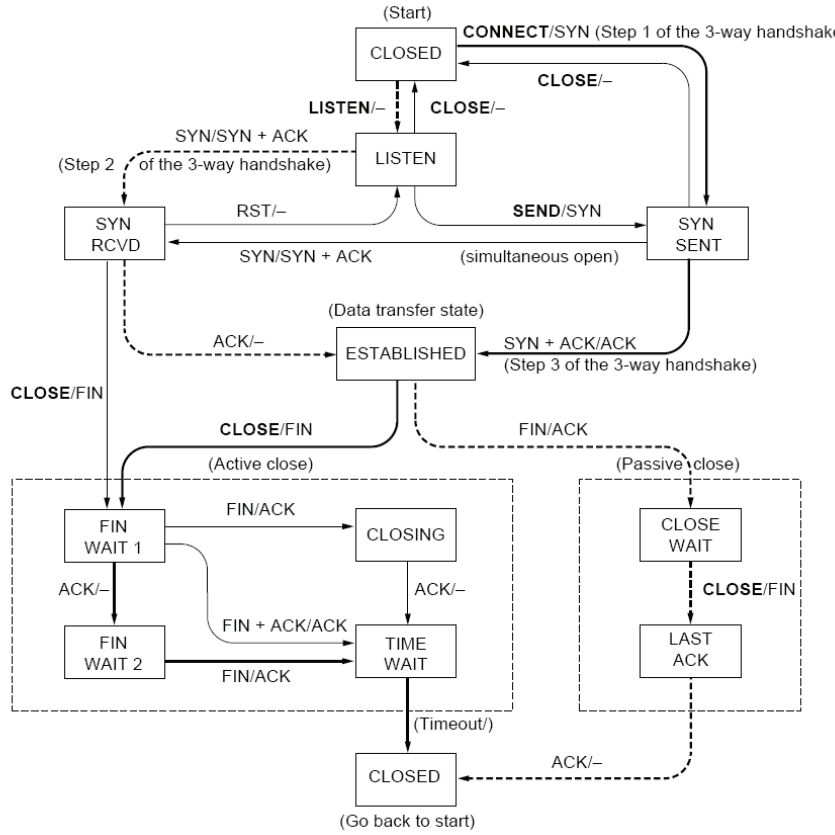
(CONNECT, LISTEN, SEND, или CLOSE), пристигање на сегмент (SYN, FIN, ACK, или RST), или тајмаут кој е дупло од животниот век на пакетот. Акцијата значи испраќање на контролен сегмент (SYN, FIN, или RST) или ништо, означено со -. Коментарите се дадени во наводници.

Состојба	Опис
CLOSED	Нема активна конекција или на чекање
LISTEN	Серверот чека на барања за конекции
SYN RCVD	Барањето за конекција пристигнало, се чека за ACK
SYN SENT	Барањето за конекција само што е испратено се чека на SYN+ACK
ESTABLISHED	Може да се примаат и предаваат податоци
FIN WAIT 1	Клиентот само што испратил барање за ослободување на врската
FIN WAIT 2	Серверот се сложил со барањето за раскинување на врската
TIMED WAIT	Чекање пакетите да им истече рокот
CLOSING	Клиентот и серверот се обидуваат за затворање
CLOSE WAIT	Другата страна иницира ослободување на врската
LAST ACK	Чекање на сите пакети да им истече рокот

Слика 8.12: Состојби кои се користат кај TCP конекцијата.

Дијаграмот може да се разбере со следење на патеката од клиентот (дебелата полна линија), а потоа следење на патеката на серверот (дебелата испрекината линија). Кога апликацискиот програм на клиентската машина направи барање CONNECT, локалниот TCP ентитет креира конекциски запис, го означува истиот со состојба SYN SENT, и испраќа SYN сегмент. Забележете дека е можно да се отворат повеќе конекции (или биле отворени во исто време) заради различните апликации, така што состојбата се однесува на дадена конекција и се снима во конекцискиот запис. Кога SYN+ACK пристигнува, TCP го испраќа последниот ACK од три-насочното ракување и преминува во состојба ESTABLISHED. Податоците сега можат да се испраќаат и примаат.

Кога апликацијата завршува, се извршува командата CLOSE, што предизвикува локалниот TCP ентитет да испрати FIN сегмент и да чека соодветен ACK (испрекинатото поле е маркирано како активно затворено). Кога пристига ACK, се прави премин во состојба FIN WAIT 2 е едната насока на конекцијата се затвора. Кога ќе се затвори и другата страна, пристигнува FIN, што потоа се потврдува. Сега и двете насоки се затворени, но TCP чека одредено време (колку што е животниот век на пакетот) да гарантира дека сите пакети од конекцијата се 'мртви', за случај потврдата да била изгубена. Кога ќе се исклучи тајмерот, TCP го брише конекцискиот запис.



Слика 8.13: Конечен автомат за менаџмент со TCP конекцијата. Дебелата полна линија е нормалната патека за клиентот. Дебелата испрекината линија е нормалната патека за серверот. Тенките линии претставуваат неочекувани настани. Секој премин е означен од настанот што го предизвикал и од резултантната акција, одделени со коса црта.

Сега да ја разгледаме конекцијата од аспект на серверот. Серверот прави LISTEN и чека да види кој ќе се вклучи. Кога ќе дојде SYN, тоа се потврдува и серверот оди во SYN RCVD состојба. Кога серверскиот SYN ќе биде потврден, три-насочното ракување е потврдено и серверот оди во состојба ESTABLISHED. Сега може да почне податочниот трансфер.

Кога клиентот е готов, тој прави CLOSE, што предизвикува праќање на FIN кон серверот. Серверот е тогаш сигнализиран. Кога тој ќе направи CLOSE, се испраќа FIN кон клиентот. Кога се појавува потврдата од клиентот, серверот ја ослободува конекцијата и го брише конекцискиот запис.

8.5.9 Сокети, порти и Winsock интерфејс

Сè што треба да се направи со Интернет или со интранетот на некоја компанија, се сведува на меѓусебна комуникација на некои две програми. На

пример, кога се сака да се посети некоја веб страница, клиентот има програма (свој веб пребарувач, односно клиентска програма) што воспоставува комуникација со веб серверот (кој содржи серверска програма). Употребата на „протоколот за трансфер на фајлови“ (File Transfer Protocol – FTP) бара на една машина да се извршува програмот под името FTP сервер, а на друг компјутер да се извршува некој FTP клиент. За да функционира Интернет поштата, неопходно е клиентската програма за електронска пошта непрекинато да комуницира со серверската програма за електронска пошта – ова се само неколку од многубројните примери.

Според TCP терминологијата, бројот на телефонот се вика сокет (приклучок). Сокетот се состои од три компоненти: IP адреса на примачот, бројни ознаки на портот (port number), т.е. програмот на примачот, и информации за тоа дали се работи за TCP порт или UDP порт (секоја програма поседува сопствен сет на порти). На секоја апликација или сервис која треба да прими или прати TCP информација, и се доделува по еден 16-битен број кој се нарекува порта на тој програм. Најпопуларните Интернет апликации ги добиле специјалните броеви на порти, кои уште се нарекуваат добро познати порти (well – known ports). Некои од овие добро познати порти се прикажани во Табелата 8.3.

Специфичните програми можат да ги употребуваат своите посебни порти, како што е тоа случај за серверот на глобалните каталози на активни директориуми кој користи број на порта 3268.

Како функционираат портите и сокетите

На пример, клиентот својот HTTP клиентски програм (кој се нарекува Интернет веб пребарувач, како што е Internet Explorer) го насочил кон некој HTTP сервер (кој се вика веб сервер како што е Internet Information Server). Клиентот сака да ја посети веб страницата www.acme.com, при што веб серверот на доменот acme.com се наоѓа на адресата 123.124.55.67, а IP адресата на клиентот е 200.200.200.10.

Клиентскиот пребарувач сака да воспостави контакт со машината која се наоѓа на адресата 123.124.55.67. Меѓутоа само познавањето на IP адресата на целниот компјутер не е доволно, мора да се познава и адресата на портата на тој програм со кој сакаме да воспоставиме комуникација, бидејќи целниот компјутер може истовремено да биде и mail сервер. Клиентскиот веб пребарувач добро знае по усвоената конвенција дека веб серверот се наоѓа на порта 80. Од таа причина клиентскиот пребарувач „праќа повик“ – т.е. воспоставува една TCP/IP сесија – со портата 80 на адресата 123.124.55.67, која може да се напише и како 123.124.55.67:80, користејќи две точки помеѓу IP адресата и бројот на портата. Оваа комбинација на IP адресата и бројот на портата се нарекува адресен сокет.

За да компјутерот на кој е инсталиран веб сервер може да комуницира со клиентскиот компјутер, веб сервер-компјутерот мора да биде спремен за

комуницирање – некој на веб серверот мора да го слушне повикот на клиентот. Тоа се нарекува пасивна отвореност спрема TCP.

Значи клиентскиот веб пребарувач разговара со веб серверот преку веб серверската порта 80. Но, како веб серверот му одговара на клиентот– која порта на клиентот серверот ја користи, т.е. која порта на клиентот го слуша одговорот на серверот?

Табела 8.3: Интернет протоколи и броеви на порти

Интернет протокол	Број на порта
FTP	TCP 20/21
Telnet	TCP 23
Simple Mail Transport Protocol (SMTP)	TCP 25
DNS	UDP и TCP 53
Trivial FTP (TFTP)	UDP 69
Hypertext Transfer Protocol (Web)	TCP 80
Kerberos logons	UDP и TCP 88
Post Office Protocol v3 (POP3)	TCP 110
Simple Network Time Protocol (SNTP)	UDP 123
NetBIOS	UDP и TCP 137, UDP 138, TCP 139
IMAP4	TCP 143
SNMP	UDP 161/162
LDAP	TCP 389
Secure HTTP (SSL)	TCP и UDP 443
SQL Server	UDP/TCP 1433

На прв поглед портата 80 изгледа како логичен одговор – но оваа порта не може да се употреби за оваа цел. Еве зошто: компјутерот на кој е поставен веб серверскиот програм, покренува Internet Explorer за да посети друга страна. Веб страницата не може да ја употреби портата 80 на компјутерот на кој што има веб сервер бидејќи таа порта е веќе зафатена. Веб серверот преговара со веб пребарувачот за заедно да изберат некоја порта која компјутерот со веб пребарувачот не ја користи. Нивната комуникација изгледа вака:

1. Од веб пребарувач кон веб серверот: „Ало има ли некој на портата 80, на адресата 123.124.55.67?“
2. Од веб серверот кон веб пребарувачот:„Секако, на кој начин ќе разговараме?“
3. Од веб пребарувачот кон веб серверот: „Што мислите за портата 40000?“

4. Од веб серверот кон веб пребарувачот: „Може, ајде да воспоставиме врска преку портата 40000“.

На тој начин сите прашања од веб пребарувачот кон веб серверот ќе бидат пратени преку сокетот 123.124.55.67:80, додека одговорите од веб серверот ќе бидат пратени преку 200.200.200.10:40000.

Поентата е во следново: комуникацијата со серверот подразбира употреба на некоја добро позната порта како што е порта 80 за HTTP серверот. Наспроти тоа, за повратна комуникација со клиентот не се користи некоја конкретно однапред дефинирана порта, т.е. серверот и клиентот едноставно се договараат која порта ќе ја употребат на клиентскиот компјутер.

9 МРЕЖНИ СЕРВИСИ И СОФТВЕР

Првите персонални компјутери биле дизајнирани како самостојни десктоп системи. Самиот оперативен систем дозволувал еден корисник едновремено да пристапува кон документите и системските ресурси, и за да изврши одредени задачи требало да има физички пристап кон системот.

Како што PC компјутерските мрежи добивале на популарност, софтверските компании развиле специјализирани мрежни оперативни системи (network operating systems - NOS) за овозможување на мрежни сервиси на десктоп работните станици. Мрежните оперативни системи биле создадени да овозможат начин за обезбедување на датотеките, овозможување на кориснички привилегии и делење на ресурси помеѓу повеќе корисници. Наглиот раст на Интернетот, ги поттикнал производителите да развиваат оперативни системи базирани на технологии поврзани со Интернетот, како што е концептот на World Wide Web (WWW).

Умрежувањето станало од централно значење и за десктоп компјутерите. Се изгубила разликата помеѓу новите десктоп оперативни системи, дополнети со мрежни сервиси и нивните мрежни пандани. Моментно најпопуларните оперативни системи како што се Microsoft Windows 2000, XP и Linux може да се најдат како кај мрежните сервери со високи перформанси, така и кај десктоп компјутерите на крајните корисници.

9.1 ПРЕГЛЕД НА PC ОПЕРАТИВНИ СИСТЕМИ

Персоналните десктоп компјутери стекнале поголема популарност во текот на 80-те години. Тогашните машини се користеле за најразлични намени како што се процесирање на текст, домашно сметководство и за играње. Исто така се појавиле и како дел од работните места, но нивната продуктивност и ефикасност била намалена заради неможноста за делење на информации со другите компјутери во состав на истата или различна организација.

Оперативните системи за овие рани десктоп компјутери биле дизајнирани за работа на еден корисник на единичен самостоен систем. Претпоставката која се земала во предвид при развојот на овие оперативни системи била дека само еден корисник ќе има потреба да пристапува кон хардверските и софтверските ресурси во било кое време. Концептите за сигурност и безбедност на компјутерите и корисничките привилегии не биле имплементирани, затоа што само еден корисник би работел едновремено и тој морал физички да биде присутен на системот. Со развојот на десктоп компјутерите, компаниите започнале да инсталираат локални компјутерски мрежи (LAN) за да овозможат поврзување на десктоп персоналните компјутери, заради делење на податоци и периферни уреди, како што се на пример печатарите, со цел намалување на трошоците за опремата како и зголемување на продуктивноста.

Преку инсталацијата на мрежни интерфејси во самите компјутери и со поставување на жичена кабелска инфраструктура со бакарни плетени парици, се создавале локалните компјутерски мрежи (LAN-ови). Со процесот на умрежувањето на компјутерите, проблемот за ефикасна комуникација бил решен, но притоа се појавиле нови проблеми поврзани со безбедноста и повеќе-корисничкиот начин на работа.

Првите LAN мрежи составени од персонални компјутери имале потреба од решавање на овие проблеми - пред сè, безбедност на документите, повеќе-кориснички пристап кон ресурсите и одредени кориснички привилегии, како и комуникација со „mainframe“ компјутерите, кои заземале централно место во тогашните корпоративни сметачки центри.

Еден пристап за решавање на овие проблеми бил развојот на оперативни системи кои се специјализирани за работа во мрежни околини, наречени „мрежни оперативни системи“ (Network Operating Systems - NOS). Употребата на таквиот софтвер побарувала поголема процесирачка моќ од постоечките десктоп работни станици. Ова било причината за појава на нова категорија на моќни компјутери под поимот сервери. Овие компјутери биле специјализирани за работа и извршување под мрежни оперативни системи и станале централна точка на локалните мрежи засновани врз моделот клиент-сервер. Кај овој модел, во мрежата околина со поставени сервери, клиентските машини се поврзуваат и пристапуваат кон ресурсите на серверот. На овие клиентски машини можат да бидат инсталирани десктоп оперативни системи, додека серверите користат мрежни оперативни системи.

Како што мрежните сервери станувале сè помоќни и покомплексни, тие полека ја превземале улогата на mainframe-ите и миникомпјутерите. Компаниите како Sun Microsystems и Hewlett Packard (HP) извршиле модификација на UNIX оперативниот систем за да може да се извршува и да се користи на постоечките серверски конфигурации.

Во минатото, за извршување на критични апликации и складирање на податоци се користеле исклучиво само скапи „mainframe“ компјутерски системи. Денеска сите организации се потпираат на микрокомпјутерите за складирање на критичните податоци и обезбедување на клучни апликации и сервиси. Умрежувањето на компјутерите не се однесува само на работните места, туку сè повеќе домашни корисници се поврзуваат на Internet и користат некој од начините за далечински пристап кон корпоративните мрежи. Пребарувањето на Интернет, сервисот за електронска пошта (e-mail), и другите Интернет апликации се во фокусот на домашните корисници. За овозможување на овие Интернет технологии, компаниите како Microsoft ги преправија нивните десктоп оперативи системи кои сега вклучуваат многу од карактеристиките и сервисите претходно резервирани за мрежните оперативни системи.

9.1.1 Десктоп оперативни системи

Во последните 20-тина години, десктоп оперативните системи еволуирале и во нивниот состав вклучуваат софистицирани графички кориснички интерфејси и мрежни компоненти. Набројани се некои од најкористените видови на десктоп оперативни системи:

- Microsoft Disk Operating System (MS-DOS) е застарен систем кој сè уште се користи за поддршка на застарени апликации. Сите верзии на Windows до појавата на Windows 95 во суштина се кориснички посредници за DOS.
- Microsoft Windows ги вклучува верзиите Windows 95, 98, ME, NT, 2000, и XP.
- Apple Macintosh OS (Mac OS) вклучува OS 8, OS 9, и OS X (OS 10), Tiger 10.4.
- Linux покрива дистрибуции од различни компании и групи како што се Red Hat, Caldera, Santa Cruz Operation (SCO), SuSE, Slackware, Debian, и други.
- UNIX го вклучува HP-UX, Sun Solaris, Berkeley System Distribution (BSD), IBM AIX и други.

Денеска производителите на оперативните системи, како и корисниците го гледаат Интернет како централно место за користење на компјутерите.

Умрежувањето и Интернетот станаа интегрален дел од користењето на компјутерите, а тоа предизвика - можностите и достапните сервиси на десктоп оперативните системи - да конвергираат кон оние на мрежните оперативни системи.

Microsoft Windows и Mac OS имаат корени уште од почетокот на развитокот на десктоп оперативните системи; нивните последните верзии во нивното јадро имаат имплементирано мрежни компоненти и сервиси. Windows XP е изграден на Microsoft NOS технологија (NT и 2000), додека Mac OS е изграден околу UNIX. UNIX се смета дека е прв мрежен оперативен систем кој се појавил. Исто како и за UNIX, IT индустријата секогаш го сметала Linux прво како мрежен оперативен систем, а потоа како и како десктоп оперативен систем.

WINDOWS 1.0 и MS-DOS

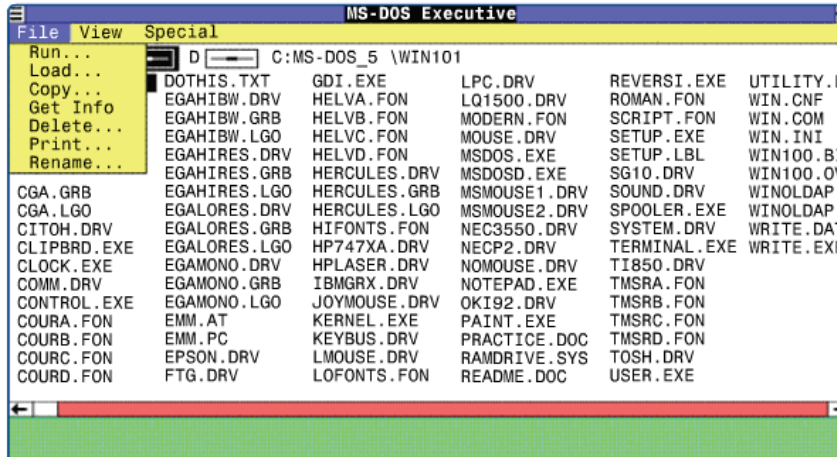
Microsoft го објавил својот прв Windows производ Windows 1.0, во 1985; пример за тоа како изгледал корисничкиот интерфејс на првата верзија на овој оперативен систем е дадена на сликата 10.1. Втората верзија со ознака Windows 2.0 е претставена во 1987 година. Најраните верзии на Windows функционирале како графички посредници кои се извршувале на основниот оперативен систем наречен Disk Operating System (DOS). Windows претставувал само обвивка (shell) преку која корисникот управувал со DOS

софтверот. DOS-верзијата на Microsoft (MS-DOS) е изградена врз оперативен систем наречен 86-DOS или Quick and Dirty Operating System (QDOS).

MS-DOS започнал како едноставен оперативен систем со текстуален командно-линиски посредник (CLI). Создаден да работи на 16-битен Intel 8088 процесор, MS-DOS е 16-битен оперативен систем способен да обработува само 16-бита едновремено.

MS-DOS и 16-битно процесирање се застарени за примена во Интернет и графичко ориентирани околини; 32-битните оперативни системи се стандард како и низа од 64-битни оперативни системи прилагодени за користење на 64-bit процесорски системи.

Од друга страна пак, многу компании сè уште го користат MS-DOS за извршување на застарени кориснички апликации. Поимот “Legacy application" е назив на застарен софтвер кој сè уште работи заради оправдување на почетната инвестиција за неговиот развој и имплементација.



Слика 9.1: Windows 1.0 GUI

MS-DOS

Постојат неколку причини со кои се оправдува користење на MS-DOS оперативниот систем:

- MS-DOS е едноставен оперативен систем, со мали мемориски и процесорски побарувања. Притоа DOS може да се извршува и на застарен хардвер.
- MS-DOS е евтин како со цената за софтверот, така и за хардверот.
- MS-DOS е стабилен и сигурен, затоа што не е мултитаскинг, не постои опасност од конфликти заради делењето на адресниот простор.

- MS-DOS е едноставен за учење, иако не е интуитивен лесен за користење.

Постојат многу апликации за MS-DOS, затоа што тој оперативен систем имал статус на стандард долг временски период. Некои компании продолжуваат да го користат затоа што нивниот сопствен и прилагоден софтвер не може правилно да работи на новите варијанти на оперативните системи.

Од друга страна, не постои можност да се извршуваат софистицирани графички програми напишани за модерни 32-битни Windows оперативни системи. А и датотечниот систем кај MS-DOS наречен FAT е несигурен и непогоден за повеќекорисничка работа. Мрежното работење на MS-DOS клиентите е проблематично, а во одредени случаи клиентите не се во можност да се приклучат на мрежните ресурси кои користат претставување со долги имиња.

На крај, најочигледна мана на MS-DOS е неговиот командно-линиски интерфејс. Тој придонесе да верзиите Windows 1.0 and 2.0 бидат првите чекори кон создавање на графичка корисничка околина (GUI) за работа.

Microsoft Windows 3.1

Во 1992, Microsoft објавил надградба на верзијата 3.0 наречена Windows 3.1. Потоа доаѓа верзијата Windows 3.11, па целата фамилијата е попозната како Windows 3.x. Работењето на MS-DOS со Windows 3.x ги надминува недостатоците на користењето на MS-DOS оперативниот систем. Обвивката кај Windows 3.x (shell) овозможува графички кориснички интерфејс и поддржува мултитаскинг за истовремено извршување на повеќе програми. Меѓутоа, верзијата Windows 3.x имала и значајни недостатоци, како што се недостаток на безбедност на датотеките и мрежна поддршка.

Кооперативен и контролиран мултитаскинг (Cooperative and Preemptive Multitasking)

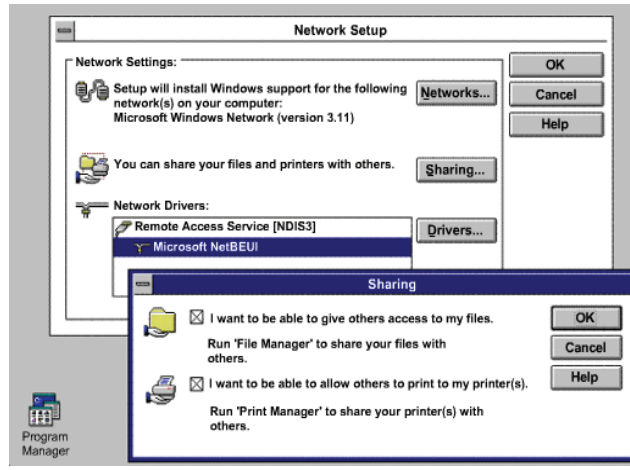
Кооперативен мултитаскинг е околина каде што програмите ја делат меморијата и меѓусебно разменуваат информации. Во таква околина процесите го делат процесорот преку временска поделба. Постои опасност - ако апликацијата е лошо напишана, може да зафати ресурси како што е процесорот и да доведе до закочување на системот; дури и ако еден програм „падне“ може да го прекине извршувањето на другите процеси кои се извршуваат во тој момент.

Поефикасна форма на мултитаскинг се користи во верзиите Windows 9x и е наречена контролирана (preemptive multitasking), која се користи и во поновите верзии. Оперативниот систем го контролира доделувањето на процесорското време, и 32-битните програми се извршуваат во нивен сопствен адресен простор. Со користењето на контролиран мултитаскинг, ниедна програма не може да го преземе системот, и отказот или

прекинувањето на извршувањето нема никакво влијание врз работата на другите процеси.

Умрежување со Windows 3.x

MS-DOS и Windows 3.1 бараат инсталација на дополнителен софтвер за овозможување на работа како мрежен клиент. Верзијата наречена Windows for Workgroups 3.1 (1992) бил првиот Microsoft оперативен систем кој имал вградено и мрежна поддршка и компоненти. Microsoft го издал Windows for Workgroups 3.11 во 1993 година и тој бил дизајниран да им овозможи на корисниците да делат датотеки и ресурси со други персонални компјутери во состав на нивната работна група (workgroup), во „peer-to-peer“ мрежа.



Слика 9.2: Windows for Workgroups 3.11

Windows 3.x се смета за застарен и заедно со MS-DOS можат да бидат искористени за поврзување со модерните Windows NT или Windows 2000 мрежи, но во овие случаи ќе имаат ограничени сервиси.

Windows 9x

Microsoft Windows 95 е дизајниран за лесно умрежување, како и Windows 98; множеството на овие оперативни системи се означуваат како Windows 9x:

- Windows 95a – оригиналното издание на првиот Microsoft 32-bit десктоп оперативен систем.
- Windows 95b – со ознака OSR2 со вградена поддршка за FAT32, достапен само на производителите како Original Equipment Manufacturers (OEM) инсталација.
- Windows 98 – надградба на Windows 95 со Active Desktop технологија, Advanced Configuration and Power Interface (ACPI),

поддршка за Universal Serial Bus (USB) и TV-tuner картички, и подобрување на инсталацијата и одржувањето.

- Windows 98 Second Edition (SE) – со вграден Internet Explorer 5.0 web прелистувач, посилна енкрипција за dial-up умрежување и поддршка за делење на Интернет конекцијата - Internet Connection Sharing (ICS).
- Windows Millennium Edition (Windows ME) – е оперативен систем наменет за домашни корисници, изграден врз кодот на Windows 9x, а ги има следниве карактеристики:
  - Подобрена поддршка за мултимедија, видео и дигитални фотографии;
  - Механизам за опоравување преку враќање на системот во претходна состојба во случај отказ (system restore);
  - Поедноставно подесување на peer-to-peer мрежи;
  - Побрзо подигање и исклучување (кога се користи нов хардвер кој користи FastBoot технологијата, т.н. plug & play).

Умрежување со Windows 9x

Windows 9x оперативните системи имаат специјализиран софтвер за мрежни клиенти кој овозможува учество и работа во локални мрежи со поставени сервери. Клиентите ги користат предностите на услугите, кои се нудат од системите кои имаат некои од мрежните оперативни системи како што се Windows NT или Novell Netware. Овие сервиси вклучуваат автентификација, делење на фајлови, принтери, директориумски сервиси, mail и web сервиси.

Windows 9x има клиентски софтвер за повеќе типови на мрежи и претставува избор на многу компании за „peer-to-peer“ мрежи, како и за клиенти на Microsoft NT, NetWare, и UNIX сервери.

32-битно процесирање и превентивен мултитаскинг

Windows 9x поддржува 32-битни апликации и користи 16-битен код за овозможување на компатибилност со постарите програми кои се извршуваат под DOS и Windows 3.x. Користи Virtual File Allocation Table (VFAT) за поддршка на долгите имиња, а Windows 95b и 98 можат да користат FAT32 за ефикасно искористување на дискот. Некои предности:

- Помалку скапи од Windows NT, Windows 2000 итн.
- Работи со низа DOS, 16-bit, и 32-bit Windows апликации.
- Интерфејсот е добро познат за повеќето PC корисници.
- Клиентскиот софтвер може да се поврзе со повеќето видови на мрежни ОС како Windows, NetWare, UNIX, и Linux.

Windows NT и Windows 2000

Во 90-тите години, Microsoft започнал со развој на модерен оперативен систем кој ќе ги задоволи барањата за мрежно работење. Резултатот од развојот е оперативниот систем Windows NT, каде што NT е ознака за New Technology. Microsoft прво ја издал верзијата на NT како 3.0 во 1993. Верзијата Windows NT 4.0 е издадена во 1996 година. Windows NT се извршува на потполно нов начин и не се потпира на стариот DOS код, врз кој се градени другите верзии на Windows.

Windows NT е прв мрежен оперативен систем и има подобрена заштита на фајлови, стабилност, умрежување и 32-битна поддршка, како и нов датотечен систем наречен NTFS. Заради супериорните карактеристики на NT, Microsoft планирал да ги обедини десктоп оперативните системи (Windows 9x) со мрежните (NT) во нова фамилија на производи наречени Windows NT 5.0. NT 5.0 проектот е преименуван во Windows 2000 оперативен систем за напредни корисници („power users“), работни станици и „high-end“ серверски системи.

Windows XP

Windows XP е издаден 2001 и претставува прв оперативен систем изграден врз основа NT, кој е директно насочен кон домашните како и корпоративните корисници:

- Windows XP Home Edition
- Windows XP Professional

Иако Windows XP и XP Professional имаат многу заеднички компоненти со нивните NT/2000 претходници, тие се сметаат за десктоп оперативни системи. Тие нудат многу клучни карактеристики на мрежните оперативни системи, како што се на пример софистицирана заштита и делење на ресурси, поддршка за повеќе кориснички налози, оддалечена администрација и многубројни мрежни компоненти и сервиси.

И Windows XP Home Edition и XP Professional поддржуваат повеќе кориснички налози, но само Windows XP Professional поддржува оддалечен пристап (remote access).

UNIX и Linux на десктоп

UNIX е име за група на оперативни системи кои потекнуваат од 1969 во Bell Labs. UNIX бил создаден за поддршка на повеќе корисници и мултитаскинг. UNIX е прв оперативен систем кој вклучувал поддршка за IP протоколите. Историјата на развојот на UNIX, која опфаќа период од 30 години, е многу сложена од причина што многу компании и организации учествувале во неговиот развој. Во текот на 70-тите, UNIX еволуирал преку работата на програмерите од Bell Labs и неколку универзитети, особени Универзитетот на Калифорнија во Беркли. При првата комерцијална појава во почетокот на

80-тите, првенствено бил наменет за користење во мрежни сервери, но не и на десктоп компјутери. Денеска постојат повеќе различни верзии на UNIX:

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

Наспроти популарноста на Microsoft Windows - оперативниот систем на корпоративните LAN мрежи, поголемиот дел од Интернет работи под UNIX системи. Иако UNIX обично асоцира на скап хардвер и се смета како „user-unfriendly“, создавањето на Linux значително ја изменило таа слика.

Linux

Во 1991, финскиот студент - Linus Torvalds развивал оперативен систем наменет за извршување под процесорот 386 кој е сличен на UNIX, но користи код кој е отворен и комплетно бесплатен. Кон крајот на 90-тите Linux стана алтернатива на UNIX кај серверите, и на Windows кај десктоп оперативните системи.

Како и со UNIX, постојат поголем број на верзии на Linux. Некои можат слободно да се преземат од WWW, а другите се дистрибуираат комерцијално:

- RedHat Linux (FEDORA), од RedHat Software
- OpenLinux, од Caldera
- Corel Linux
- Slackware
- Debian GNU/Linux
- SuSE Linux
- Mandrake
- Knoppix

Linux е еден од најмоќните и најстабилни оперативни системи и заради тоа се користи како платформа за „power users“ и „enterprise“ сервери. Поретко се користи како корпоративен десктоп систем; иако има комфорен графички интерфејс, повеќето корисници им е полесно да го користат Mac OS или Windows. Бројот на апликациите е ограничен во споредба со Windows, но некои вендори обезбедуваат софтвер за емулација на Windows програми (како што се WABI и WINE) на Linux.

Умрежување со Linux

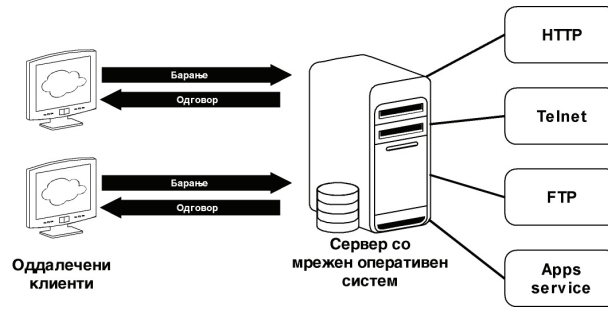
Последните дистрибуции имаат вградено мрежни компоненти за поврзување со LAN, воспоставување на dial-up врска кон Интернет или други оддалечени мрежи. Всушност TCP/IP е интегриран во Linux kernel-от наместо да биде имплементиран како посебен подсистем. Некои од предностите на Linux како десктоп ОС и како мрежен клиент:

- Вистински 32-bit ОС.
- Превентивен мултитаскинг и виртуелна меморија.
- Кодот е отворен и достапен за измена и надградба.

Треба да се забележи дека иако UNIX најчесто се применува како серверски оперативен систем, UNIX машините може да работат и како мрежни клиенти. Во повеќето случаи, конфигурацијата и командите за UNIX се исти како и во Linux системите.

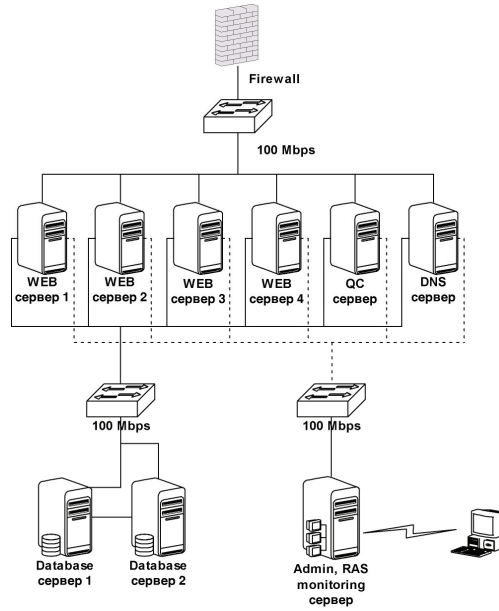
9.1.2 Клиент-сервер модел кај мрежните оперативни системи

Повеќето мрежни апликации како што се Интернет (World Wide Web - WWW) и e-mail, се изградени околу клиент-сервер моделот. Специјализирана програма наречена сервер, обезбедува мрежни сервиси на другите програми наречени клиенти (сервер-програмите кај корисниците на UNIX се нарекуваат демони “daemons”).



Слика 9.3: Клиент-сервер модел кај МОС

Сервер програмите при работата очекуваат барања од клиентите, и ако е добиено легитимно барање, серверот одговара со враќање на бараните информации. На пример, кога е стартуван web сервер, тој чека на клиентски барања. Пример за клиентски програм е web пребарувач. Web пребарувачот испраќа барања кон серверот. Серверот одговара со испраќање на одговор и пребарувачот ги прикажува HyperText Transfer Protocol (HTTP) податоците во неговиот прозорец.



Слика 9.4: Корпоративна мрежа

Теориски, секој компјутер може да се однесува како сервер сè додека е поврзан на мрежата и конфигуриран со соодветен софтвер. Практично - повеќето организации ги поставуваат своите клучни мрежни сервиси на „high-end“ компјутери –сервери кои работат на мрежни оперативни системи, оптимизирани за сервисирање на оддалечени клиенти. Типичен сервер со МОС може да биде конфигуриран да понуди огромен број на сервиси на клиентите, дури повеќето сервери можат да комуницираат со различни клиентски платформи преку универзални правила или протоколи.

Интернетот е изграден околу фамилијата протоколи Transmission Control Protocol/Internet Protocol (TCP/IP). Заради важноста на Интернетот, повеќето сервери и клиенти го користат TCP/IP за размена на податоци.

Еден сервер со имплементиран мрежен оперативен систем може да работи подобро ако опслужува помалку клиенти, па повеќето организации користат повеќе сервери за да задржат прифатливи перформанси на серверите. Типичен дизајн е да се поделат сервисите на сервери така што еден би бил одговорен за e-mail, друг за делење на фајлови итн. High-end серверите со мрежни оперативни системи се конфигурирани да ја користат Интернет фамилијата на протоколите и да обезбедуваат еден или повеќе TCP/IP сервиси. Серверите исто така се користат за автентификација на корисниците и обезбедување на пристап на делените ресурси.

9.2 БАРАЊА ЗА ПОСТАВУВАЊЕ НА ОПЕРАТИВНИ СИСТЕМИ

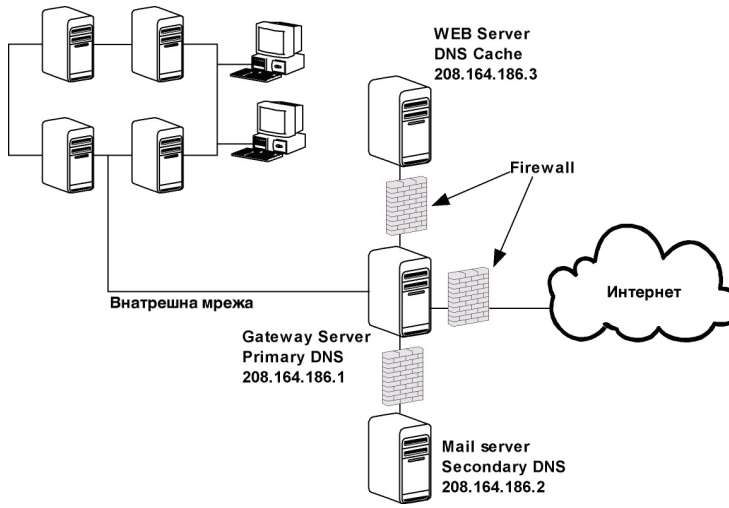
9.2.1 Работни станици (Workstations)

Корисниците бараат специфичен хардвер и софтвер кој ќе биде инсталиран на системот. На пример, барањата за „low-end“ систем потребен за процесирање на текст не мора да биде систем со брз процесор или голема меморија или хард диск. Меѓутоа барањата на корисник на „high-end“ систем, кој работи задачи со поголема комплексност, како обработка на видео или слики, можат да бидат многу поголеми. Тој систем ќе има потреба од брз процесор и поголема меморија и хард диск.

Други хардверски барања кои може да се најдат на станиците се на пр. звучни картички, звучници, преносни медиуми со голем капацитет, zip драјвови, CD-R или CD-RW, DVD-ROM, DVD-RW итн.

9.2.2 Сервери (Servers)

Хардверските побарувања на серверите можат многу да се разликуваат од работните станици. Серверите немаат потреба од кориснички-ориентирани периферии како што се големи монитори, звучници или микрофони. Од друга страна, серверите содржат хард дискови отпорни на грешки и испади (Small Computer System Interface - SCSI) дискови, наместо Extended IDE (EIDE) дискови, инсталирани на работните станици (SATA).



Слика 9.5: Разни типови на сервери

Големината на мрежата која треба да се опслужува од серверот ја диктира и големината на потребните процесори-CPU и меморијата. На пример, ако корисникот постави сервер на голема мрежа за опслужување на голем број

на барања, потребен е систем со брз CPU и голем RAM, за разлика од сервер кој би се користел во SOHO мрежа со неколку корисници.

Друг аспект во одредувањето на барањата е - кој тип на услуги ќе ги опслужува серверот. Дали ќе биде web или File Transfer Protocol (FTP) сервер, NNTP, сервер на податочни бази или друго.

На пример, ако серверот управува со веб сајт кој ќе биде често посетуван - потребен е помоќен сервер, или дури повеќе сервери за обезбедување на квалитетно ниво на услугите.

9.3 Видови на мрежни сервиси

Еден сервер може да обезбеди различни мрежни сервиси. Некои од сервисите не се видливи за корисникот меѓутоа вршат индиректно влијание на начинот како работи серверот. Другите пак влијаат врз начинот како корисниците ги извршуваат нивните задачи преку мрежата. Сервисите може да се групираат во неколку категории:

- Датотечни сервиси
- Сервиси за печатење
- Апликациски сервиси, вклучувајќи ги податочните бази и WEB серверите
- Сервиси за испраќање на пораки во форма на електронска пошта

Постојат и други сервиси кои се достапни со инсталација на серверскиот софтвер:

- Сервис за автоматско адресирање - Dynamic Host Configuration Protocol (DHCP).
  Овој сервис динамички доделува IP адреси кон работните станици кои побаруваат комуникација со IP мрежата. Користењето на DHCP во главно ја елиминира потребата од рачно поставување на адресите и ја избегнува појавата на двојни IP адреси кои се резултат на човечка грешка. Сервисот DHCP може да се најде како дел од софтверот вграден и во DSL рутерите и кабелските модеми.
- Сервис за пренос на датотеки - File Transfer Protocol (FTP).
  Иако користењето на „web“ прелистувач за преземање на датотеки од Интернет предизвикало намалување на користењето на FTP сервисот, тој сè уште се користи како начин за испраќање и преземање на датотеки од сервер со користење на TCP/IP протоколите. FTP серверот ја обезбедува оваа услуга без кој FTP клиентите би биле бескорисни.
- Сервис за системот на доменски имиња - Domain Name System (DNS).
  Сервисот за DNS е база на податоци која врши пресликување на IP адресите од WEB серверот или друг мрежен уред кон логички имиња кои се користат на World Wide Web. При обидот за

поврзување кон одреден web сајт, се испраќа барање за разрешување на името кон DNS сервер, кој како одговор ја враќа IP адресата преку која се врши поврзување на WEB сајтот.

- Сервиси за виртуелна приватна мрежа (Virtual Private Network VPN). VPN претставува комбинација на хардвер и софтвер кој им овозможува на корисниците и мрежните администратори да пристапуваат кон внатрешната мрежа во организацијата со посредство на било каква конекција на Интернет. За разлика од решенијата за далечински пристап кои користат модеми и телефонски линии, VPN врши намалување на трошоците со елиминација на локалните и меѓународните повици. Некои организации не користат VPN затоа што податоците, иако во криптирана форма, треба да поминуваат преку небезбедната мрежа - Интернетот. Во многу мрежи сè уште постојат сервери за далечински пристап, за корисници кои се поврзуваат преку „dial-up“ конекција.

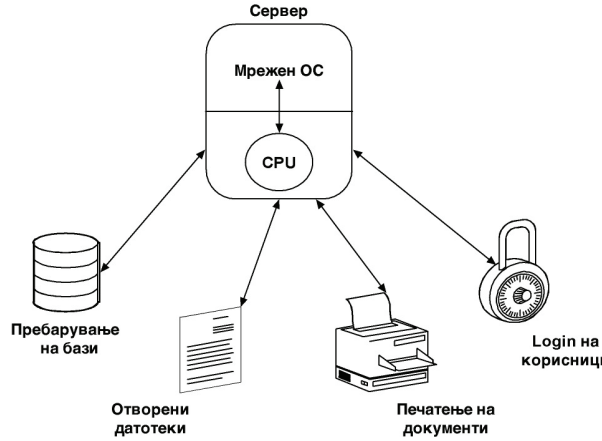
9.4 Избор на серверски мрежен оперативен систем (МОС)

Овој вид на системски софтвер е специјално дизајниран за користење на мрежни сервери и обезбедување на повеќе сервиси, како и висок степен на перформанси. Обично кога се споменува поимот сервер, тоа се однесува на софтверот кој се извршува на компјутерот која се нарекува *сервер*, а не само компјутерот. Овој софтвер е мрежниот оперативен систем. Постојат повеќе различни видови на оперативни системи, и иако технологијата на кои се базираат може да е различна, основните сервиси кои ги нудат во основа се исти.

Иако различни пакети на мрежни оперативни системи обезбедуваат слични сервиси, можеби нема да обезбедат исто ниво на перформанси, флексибилност, безбедност или скалабилнот. Многу е важно да се обрне внимание на задоволување на потребите на организацијата со истовремено задоволување на барања за мрежни ресурси.

9.4.1 Мултитаскинг (Multitasking)

Серверите треба брзо да одговараат на големиот број барања од корисниците, а софтверот треба да биде способен да ги процесира барањата и да извршува други задачи истовремено. Способноста за извршување на повеќе задачи истовремено се нарекува мултитаскинг (multitasking). За подобро изведување на мултитаскинг се користи процесот наречен преемптивен мултитаскинг (preemptive multitasking).

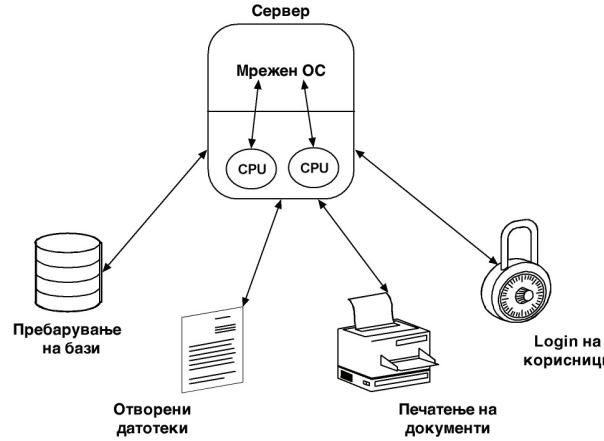


Слика 9.6: Преемптивен мултитаскинг

9.4.2 Мултипроцесирање (Multiprocessing)

Дури и ако серверскиот софтвер може да изведува мултитаскинг, може да стигне до точка кога барањата за серверот се преголеми. Кога процесорската единица (CPU) е преоптоварена со многу барања, перформансите брзо ќе деградираат, а процесорот нема да биде во состојба да држи чекор со сите информации кои доаѓаат од различни внатрешни уреди (како што се мрежниот интерфејс, или контролерите на хард дисковите). Ако не постои можност за надградба со побрз процесор, потребно е да се знае дали мрежниот оперативен систем поддржува мултипроцесирање (multiprocessing). Мултипроцесирањето ги подобрува перформансите преку додавање на повеќе процесори на истиот серверски компјутер. Кога еден сервер има повеќе од еден процесор, оперативниот систем врши подеднакво распределување на задачите на секој процесор.

Поголемите организации скоро секогаш имаат потреба за сервер со мултипроцесирање. Иако тоа не е случај со помалите организации, како што се малите претпријатија (small businesses) и училишта, нивните потреби се менуваат како што апликациите стануваат се поробусни. Секако, пред да се направи одлука за користење на мултипроцесорски систем, потребно е да се осигури дека користените апликации може да ја искористат предноста на мултипроцесирањето.



Слика 9.7: Мултипроцесирање

Конечно - мрежните оперативни системи треба да бидат и стабилни; стабилноста се дефинира - како серверот се однесува под големо оптоварување и појава на софтверски грешки. Во стабилен систем, ако апликацијата која се извршува ненајдено се прекине, серверскиот софтвер ќе продолжи нормално. Погрешната апликација ќе биде терминирана и рестартирана без исклучување на серверот.

9.4.3 Серверски хардвер

Како еден од одлучувачките фактори при избор на оперативниот систем (не само видот, туку и верзијата на серверската фамилија) е одредување на типот на компјутерот кој ќе је има улогата на сервер и кој најоптимално ќе ги задоволи потребите. Серверот треба да се бира според следниве критериуми:

- Доверливост (Reliability). Серверот е способен за овозможување на континуирана работа во случај на критичен испад или зголемено оптоварување.
- Скалабилност (Scalability). Како што се зголемуваат потребите, серверот може да биде надградуван и обновуван според нараснатите потреби.
- Толеранција на испади (Fault tolerance). Серверот со користење на различни хардверски и софтверски решенија ја минимизира веројатноста од губење на податоци при појава на грешки и испади на системот. Соодветно на тоа, серверот кој е подоверлив, поскалабилен или потолерантен на испади, ќе има поголема цена за неговото поставување, иако цената е многу помала од цената за опоравување и реставрација на изгубените податоци. При изборот на хардверот, потребно е да се земе во предвид и решението за изведување на backup процедури, и за заштита на напојувањето.

Зависно од потребите, може да се додадат и други опции како што е мултипроцесирањето, или систем на редундантни дискови (Redundant Array of Inexpensive Disks (RAID). Со додавањето на овие опции се зголемува толерантноста на испади на серверот, како и заштитата на податоците и избегнувањето на неактивноста на системот (downtime).

- Backup на податоците и оправување од испади. Една од најбитните процеси во организациите е чувањето на податоците и оправување од испади. Не може да се толерира комплетно губење на податоци од било која причина како што се хардверските испади или елементарни непогоди. Без соодветна стратегија за изведување на backup процедури, не е можно оправување и реставрација на изгубените податоци. Постојат повеќе стратегии кои може да се искористат за заштита на податоците, како што се на пример, користењето на екстерен хард диск, или користењето на магнетна лента која е многу попопуларно решение. Уредите со магнетните ленти (tape backup drive) користат софтвер или хардвер за backup-ирање на податоците од серверот, или било кој друг компјутер од мрежата. Лентите се релативно издржливи и поевтини така што може да се транспортираат надвор од локацијата на мрежата за чување. Во дополнение на магнетните ленти, популарни и поприфатливи стануваат и уредите за мрежни мемориски складови - networked attached storage (NAS); иако не се замена за уредите со ленти, играат важна улога во backup решенија каде што NAS се достапни во случаи кога главниот сервер или серверите се паднати.
- RAID - Серверите обично имаат два или повеќе дискови за чување на податоците. RAID конфигурација вклучува хардвер и софтвер за заштита на податоците во случај кога еден од дисковите престане со работа. Постојат повеќе различни RAID нивоа, со RAID ниво 5 како најкористена имплементација во односот цена-перформанси. RAID ниво 5 ги подобрува перформансите односно брзината на снимањето на податоците на хард дисковите со истовремено запишување на повеќе дискови.
- Напонска заштита (Power protection). Заштитата на напојувањето на серверите и другите уреди е многу битна, особено при зголемена потреба од електрично напојување. Најкористената опрема за заштита на напојувањето користена на серверите се системите за непрекинато напојување (Uninterruptible Power Supply - UPS). UPS е резервен систем кој го обезбедува серверот со напојување или го напојува од батерија при недостаток на електрична енергија. Кога батеријата ќе се истроши до одредено ниво, софтверот за управувањето со напојувањето ќе иницира исклучување на серверот со што се заштитува од ненајдено и ризично нагло исклучување. Како додаток на UPS, серверите може да бидат опремени и со редундантно напојување. Во сценарио на околина со комплетна

толеранција на испади, серверите би имале едно напојување поврзано со UPS, а другото редундантно напојување би било поврзано со вториот UPS, кој би бил поврзан на друг приклучок на електричната мрежа, со што практично само комплетно губење на напојувањето во објектот, би предизвикало префрлување на напојување од батериите.

9.5 Видови на Мрежни оперативни системи

Ограничувањата на поранешните десктоп оперативни системи и зголемената побарувачка на мрежни персонални компјутери, доведе до развој на сè помоќен мрежен софтвер. Спротивно на десктоп оперативните системи, мрежните обезбедуваат вградени мрежни компоненти и сервиси, повеќе-корисничка работа, заштита на фајлови и делење на ресурси.

Мрежните оперативни системи мора да имаат робустен kernel за превенција на испади и време на неработење (downtime). Бидејќи со овие системи управуваат специјализирани администратори, обично нема потреба од графичка околина за работа. Историски гледано мрежните ОС нудат помалку „пријателски“ кориснички интерфејс, споредено со нивните десктоп пандани. Меѓутоа и Windows 2000/3 и Linux имаат GUI, дури и web-базирани контроли. Мрежните ОС побаруваат софистициран датотечен систем кој дозволува ефикасно складирање и максимална безбедност. Наместо FAT, обично се користат NTFS, UFS (UNIX file system), или некој друг еднакво робустен датотечен систем.

Novell NetWare е првиот МОС кој ги задоволувал овие барања и уживал голема распространетост во LAN-овите назад во 1980. Од тоа време, Novell ја изгубил таа позиција на најкористен мрежен оперативен систем во корист на Microsoft и Linux.

Примери за типови и верзии на мрежни оперативни системи:

- Microsoft Windows – мрежни ОС понудени од Windows се: NT 3.51, NT 4.0, 2000, XP, и 2003. NT 3.51 и NT 4.0 се застарени (прекината е корисничката поддршка од производителот) како резултат на подобрите Windows 2000, XP, и 2003.
- Novell NetWare – Novell оперативните системи се: NetWare 3.12, IntraNetWare 4.11, NetWare 5.0 и 5.1.
- Linux – Linux ОС се: Red Hat Fedora, Caldera, SuSE, Debian, Slackware, Mandrake
- UNIX –HP-UX, Sun Solaris, BSD, SCO, и AIX.

Како што е претходно веќе спомнато, повеќето од мрежните оперативни системи обезбедуваат во основа слични функции и сервиси. Затоа е важно да се познаваат карактеристиките на различните типови и нивните верзии. Еден вид на серверски софтвер може да биде едноставен за инсталација, друг пак да биде постабилен и подоверлив. Изборот на серверот исто така бара познавање на потребите на организацијата каде треба да биде поставен. Во

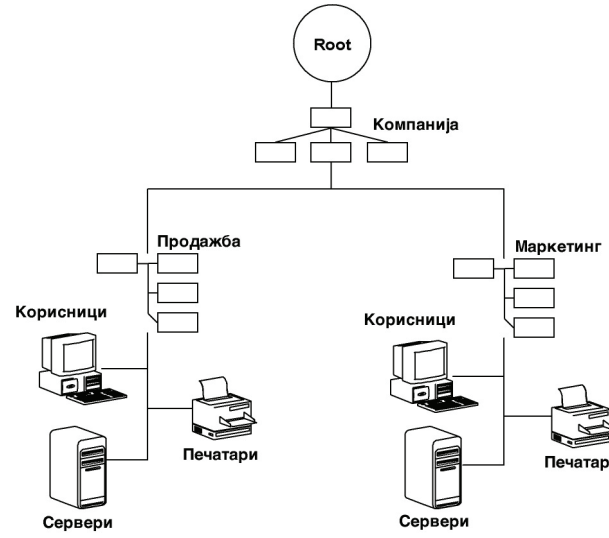
продолжение ќе биде даден краток преглед на најпопуларните и најкористените мрежни оперативни системи.

9.5.1 Windows 2003 Server

Microsoft Windows 2003 Server е најнова серверска технологија на Microsoft. Како и повеќето софтверски надградби, Windows 2003 Server има многу подобрувања и надградби во однос на неговиот претходник Windows 2000, од кого ги презел најдобрите карактеристики, при тоа зголемувајќи ја доверливоста, и подобрувајќи ја хардверската поддршка. Windows 2003 се нуди во неколку верзии: Small Business Edition, Standard, Enterprise, Datacenter, Web, Storage Server. Карактеристиките на овие верзии се дадени во табелата (само 32-битни процесори):

Табела 9.1. Карактеристики на верзии на Windows MOC

	Small Business Edition	Standard Edition	Enterprise Edition	Datacenter Edition	Web Edition	Storage Server
Max CPU	2	4	8	32	2	Зависи
Max Memory	4 GB	8 GB	32 GB	32 GB	2 GB	4 GB
Clustering	×	×	✓	✓	×	✓
Load Balancing	×	×	✓	✓	×	✓



Слика 9.8: Примена на Active Directory

Секоја од верзиите е создадена да задоволи одредени барања и потреби на поголеми и помали организации. Како и кај Windows 2000, директориумскиот сервис наречен Active Directory во Windows 2003, им овозможува на администраторите преглед и управување на сите мрежни ресурси. Со користењето на Active Directory значително се поедноставува управувањето со корисниците и ресурсите за одреден оддел или локација. За поголеми организации, Active Directory може да се реплицира помеѓу повеќе доменски контролери, за поширок преглед на сите ресурси достапни во организацијата, без разлика на нивната физичка локација.

Избор на Windows 2003

Со Windows 2003, администрацијата на серверите стана уште подоверлива и поедноставна. Иако се смета дека компонентата на директориумските сервиси Active Directory стана уште посложена, таа обезбедува платформа за интеграција и на други производи.

Предности при користење на Windows 2003 Server:	Недостатоците при користење на Windows 2003 Server:
• едноставно управување преку голем број на алатки. • помалку рестартирања при реконфигурација на серверот • подобрена поддршка на хардверот преку можноста за Plug and Play. • подобрена стабилност и достапност (uptime). • поддршка за проширување од еден сервер со еден процесор кон поголеми сервери.	• сопственоста на технологијата ја намалува флексибилноста • високи трошоци за лиценцирање на компаниите • не е стабилен и брз како верзиите на Unix. • високи барања за CPU, диск и меморија.

Табела 9.2: Минимум системски барања за инсталација на Windows 2003 Standard Server

	Минимална	Препорачана
CPU	133 MHz	550 MHz
Меморија	128 MB	256 MB
Простор на дискот	2 GB	4 GB

9.5.2 Unix

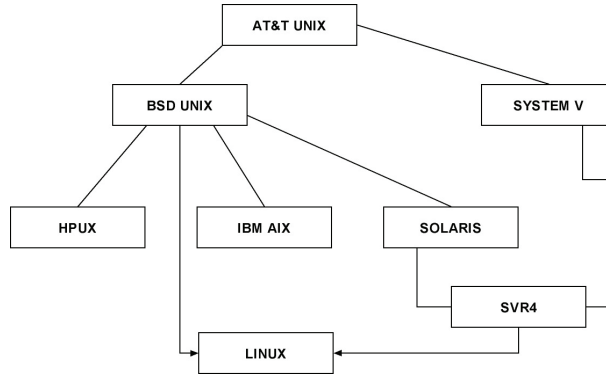
Оперативен систем кој поддржува повеќе-корисничко опкружување, мултитаскинг и во повеќето случаи и мултипроцесирање. Unix е создаден од страна на AT&T во 1969, и денеска постојат неколку варијанти на овој оперативен систем. Unix е оперативен систем исто како и Windows или Mac

OS, но се карактеризира со доверливост, брзина и моќност. Веќе долго време се користи за апликации во инженерство и научни истражувања, а од скоро и за напредни Интернет апликации, каде што е примарна платформа на која работат најголемиот дел од WEB сајтовите на Интернет.

BSD Unix

Верзијата на Unix развиена од страна на Универзитетот на Калифорнија, Беркли (University of California, Berkeley). BSD Unix е достапен за користење без надокнада од Berkeley Software Distribution (BSD) корисничката група. Оперативниот систем е развиван од страна на студентите со користење на оригиналниот софтвер на AT&T. Извршено е репрограмирање на целиот оперативен систем, од кој понатаму се развиле и дополнителни варијанти на Unix, базиран на BSD. Листата на различните варијанти на Unix ги вклучува и верзиите развиени од најголемите софтверски компании во светот: Solaris на Sun Microsystems, HP-UX на Hewlett- Packard, AIX на IBM, и од скоро OS X серверот на Apple.

Како што е спомнато, постојат повеќе варијации на UNIX, од кои некои се дизајнирани за извршување на специјални процесори, додека други се извршуваат на повеќе типови на процесори. Треба внимателно да се специфицираат потребите при изборот на одредена варијанта на UNIX; иако се достапни повеќе бесплатни верзии, комерцијалните сепак имаат подобра доверливост и корисничка поддршка. AT&T сè уште ја развива својата верзија на Unix означена како System V. Последната верзија - System V Release 4 (SVR4), заеднички е развивана помеѓу AT&T и Sun Microsystems.



Слика 9.9: Варијанти на UNIX оперативни системи

Избор на UNIX

При изборот на серверски софтвер, Unix би требало да биде опција во случај кога има мрежен администратор кој има искуство со Unix.

Предности при користење на UNIX:	Недостатоците при користење на UNIX:
• стабилен оперативен систем • може да работи и како работна станица и како сервер • брзина • вклучува голем број на вградени алатки и апликации	• комплексноста и користење на архаични команди. • може да биде многу скап (иако BSD Unix е бесплатен). • вклучува огромен број на вградени алатки, апликации и команди

9.5.3 Linux

Linux е верзија на Unix оригинално развиена од Linus Torvalds на Универзитетот во Хелсинки. Од самиот почеток, софтверот е достапен бесплатно за другите Unix програмери од целиот свет, следејќи го концептот на отворен софтвер (open source). Идејата е едноставна, кодот е достапен без надоместок за секој кој во замена треба да ги објави измените без ограничувања.

Предности при користење на LINUX:	Недостатоците при користење на LINUX:
• едноставна и брз инсталација споредена со Windows XP • се карактеризира со брзина и доверливост. • се извршува на PC, PowerPC, SPARC станици. • неговото користење е бесплатно или со минимални трошоци. • постои голем број на апликации. • затоа што изворниот код е достапен, грешките и пропустите се исправаат многу побрзо во однос на било кој друг оперативен систем.	• постојат стотици команди и апликации кои треба да се совладаат. • иако Linux е полесен за администрирање, сепак е потребен искусен Unix администратор. • мал број на компании обезбедуваат корисничка поддршка

Изворниот код на Linux може да се преземе од Интернет и единствена тешкотија е потребата од неговото компајлирање. Иако задачата не е неизводлива, процедурата е далеку од едноставна како инсталацијата на другите комерцијални оперативни системи. За среќа, повеќе компании го поедноставиле процесот и уште го дополниле со апликативен софтвер, (некои од тие компании се Caldera Systems, Mandrake, и Red Hat Software). Тие дистрибуираат верзии на Linux оперативниот систем кои се карактеризираат со едноставна инсталација, а од скоро и со „plug-and-play“ инсталација на хардверот, и имаат повеќе опции за избор на работа во графичко окружување слично на Windows, (како што се XFree86 и GNOME). Linux е популарен најмногу заради следниве карактеристики:

- се извршува на машини со Intel 486 или побрзи процесори.
- редовно се надополнува со нови и бесплатни апликации.
- неговото користење е бесплатно.

Linux сè уште не се смета за замена на критични апликации кои работат под Unix.

Табела 9.4: Минималните системски барање на повеќе верзии на Linux

	Минимална	Препорачана
CPU	Intel 486	Intel Pentium 100
Меморија	32 MB	128 MB
Простор на дискот	250 MB	1 GB

9.5.4 Novell NetWare

Во средина на 80-те, софтверската компанија за мрежен софтвер наречена Novell, Inc. со *NetWare* мрежниот оперативен систем, стана доминантна на пазарот на серверските базирани системи. И во доцните 80-ти, NetWare верзија 3.11 беше доминантен серверски софтвер за делење на датотеки и печатење. Во раните 90, Novell го загуби приматот од страна на Windows NT Server. Иако Novell беше добро позициониран на пазарот, NetWare производите биле дизајнирани за мали мрежи кои барале само еден сервер. Како што нараснувале мрежите, не постоел лесен начин преселување на корисничките информации и лозинки од еден на друг NetWare 3 сервери.

Novell Directory Services (NDS)

Novell го претставил NetWare 4.11 во 1995, и оваа верзија имала подобрувања со цел поедноставно управување и имплементација на NetWare во ентерпрајз мрежите. Значајно подобрување е поддршката за TCP/IP протоколите. (Поранешните верзии го поддржувале само Novell –овиот сопствен протокол, IPX. Иако IPX се користел на локалните мрежи, за пристап кон Интернет потребен е IP).

Novell исто така го претставил новиот директориумски сервис, наречен *Novell Directory Services (NDS)*. Следната NetWare 5 верзија имала вградена поддршка за TCP/IP и за повеќето популарни Internet апликации. Во последната верзија 6.5, NetWare вклучил целосна поддршка за TCP/IP, подобрени перформанси и фамилија на апликации за Internet и бизнис намена. Дополнително, Novell Directory Services, како и Active Directory на Microsoft, ги поддржуваат отворените стандарди за директориумски сервиси како што се Lightweight Directory Access Protocol (LDAP), со кој се овозможува интегрирање во мешана околина со NetWare, Windows, или Unix. Исто како и кај Active Directory во Windows 2000 и 2003, NDS ја организира мрежата во структура наречена директориумско стебло. Под NDS, стеблото се проширува со додавање на нови објекти. Секој објект

преставува корисник или уред на мрежата, како што се сервери, работни станици, печатачи или други мрежни уреди.

Предности при користење на NetWare:	Недостатоците при користење на NetWare:
• стабилен мрежен оперативен систем. • отворени стандарди за директориумски сервиси NDS • поддршка за управување со NetWare, NT, и Unix сервери • обезбедува Java-базиран управувачки софтвер наречен ConsoleOne базиран на NDS.	• како и кај Unix, администрацијата на NetWare 6 бара познавање на одредени команди. • NDS може да биде сложен за имплементација на големи мрежи во однос на не-директориумски системи. • NetWare 6 е чест како Windows 2000/2003 или Unix.

На мрежните администратори NDS им овозможува управување и надгледување на повеќе NetWare, NT, и Unix сервери како и други уреди од една локација. Нема потреба од користење на повеќе апликации за надгледување на перформансите или за управување со серверите. За да го задржи присуството на денешните мрежи, Novell го нуди NDS како одделен производ кој може да се извршува и на други оперативни системи.

Табела 9.5: Минималните системски барања за NetWare 6

	Минимална	Препорачана
CPU	Pentium II	Pentium III или подобар
Меморија	128 MB	512 MB
Простор на дискот	2 GB	10 GB

9.5.5 Mac OS X сервер (Panther)

Mac OS X серверот претставува варијанта на Unix со графички кориснички интерфејс на Mac. Mac OS X серверот издаден во март 1999 беше базиран на две верзии на Unix: BSD Unix и Mach, варијанта на BSD Unix развиена како дел од Mach проектот на Carnegie Mellon универзитетот. Apple исто така изработил добар дел од софтверот на јадрото на Mac OS X, кој е исто така достапен без надоместок. Идејата е програмерите да го развиваат и подобруваат серверскиот софтвер, на сличен начин како што се развивани и BSD Unix и Linux. За разлика од било која друга верзија на Unix, OS X серверот може да извршува било која верзија на Unix софтвер кој се извршува на Mach кернелот и FreeBSD.

Во Mac OS X сервер се вклучени неколку стандардни апликации како што се:

- стандардни DNS, FTP, DHCP, и други стандардни серверски апликации
- Apache Web сервер и Tomcat Java Applet Server

- Mail Server со WebMail интерфејс
- Network File Sharing (NFS) за делење на фолдери и датотеки на други компјутери
- технологија на отворени директориумски сервиси (Open Directory) за едноставна интеграција со Windows Active Directory и други директориумски базирани сервиси, како што се наоѓаат во Novell и Unix.

Во дополнение, Mac OS X серверот ги има и следниве можности:

- управувачка алатка, наречена Server Admin, за сите серверски апликации
- клиентска поддршка за сите верзии на Windows
- QuickTime сервер за стриминг за „on-demand“ видео за Web
- командно-линиски пристап кон сите конфигурациски опции

Најкарактеристична можност на Mac OS X серверот, е дека претставува робустен и скалабилен мрежен оперативен систем, кој е тесно поврзан и интегриран со Apple хардверските платформи, има поддршка на симетрично мултипроцесирање и „преемптивен мултитаскинг“ со користење на G4 процесорската технологија.

Предности при користење на Mac OS X:	Недостатоците при користење на Mac OS X:
• подобрена сигурност со користење на едноставни апликации. • базиран на доверлив BSD Unix и Mach софтвер. • вклучува многу стандардни Интернет апликации како што е Apache Web сервер. • поддржува централизирано управување на Macintosh компјутери. • Неговата Open Directory архитектура може да се искористи за интеграција на корисниците и фолдерите со Unix, Novell, и Windows 2000 Active Directory.	• не е докажан како другите мрежни оперативни системи. • не ги поддржува постоечките серверски апликации за Macintosh. • перформансите му се ограничени на користење на хардвер произведен од Apple.

Табела 9.6 Минималните системски барања Mac OS X сервер

	Минимална	Препорачана
CPU	G3	G5
Меморија	256 MB	512 MB
Простор на дискот	4 GB	20 GB

10 ИМПЛЕМЕНТАЦИЈА НА МРЕЖА ПОД WINDOWS

10.1 ПОВТОРУВАЊЕ НА АДРЕСИТЕ

Во TCP/IP, на секој уред му е потребна логичка адреса, наречена IP адреса, која го идентификува. IP адресата е 32-битен бинарен број. Ако уредот треба да се поврзе на Интернет, адресата мора да биде единствена помеѓу сите други уреди поврзани на Интернет. Дека IP адресата е единствена, се проверува преку Internet Information Center (InterNIC). За мрежите, InterNIC означува блокови од адреси.

Класа	Први битови	Мрежи	Хостови
A	0	126	16,777,214
B	10	16,384	65,534
C	110	2,097,152	254

Слика 10.1: Класи на мрежи

Рутерите ги користат идентификационите битови за да одредат кој дел од IP адресата е мрежната адреса, а кој адресата на корисникот. На пример, ако првиот бит во IP-адресата е 0, рутерот ќе креира подмрежна маска со облик 255.0.0.0. Користејќи логичка И операција помеѓу IP-адресите и подмрежните маски, се маскираат последните четири делови, оставајќи ја само мрежната адреса.

Забелешка: Некои експерти ги земаат IP-адресите како цифри, битови или бајти. Секој дел од IP адресата разделен со точка може да содржи една, две или три цифри. Бајтот може да биде претставен како еден хексадекаден симбол или осум дигитални битови. Многу текстови содржат грешки во опишувањето на IP-адресите и нивните класи.

Организациите не се заклучени во поглед на бројот на мрежи и корисници, овозможени од мрежната класа што ја користат. Мрежниот инженер може да креира мрежна подмаска за да го зголеми бројот на единствени мрежни адреси или може да користи proxy сервер. Со користењето на прокси-сервер, на секој корисник во мрежата нема да му треба единствена IP-адреса. Само прокси-серверот е обезбеден со единствена Интернет IP-адреса. Корисничките барања до Интернет се прифаќаат и обработуваат од прокси серверот. Бидејќи само IP-адресата на прокси-серверот е видлива на Интернет, внатрешните мрежни и кориснички адреси може да бидат единствени само внатре во мрежата.

10.1.1 TCP/IP инфраструктура

За секоја мрежа, било да е составена од два компјутери со една Интернет конекција, или пак глобално распространета мрежа, мора да се решат два основни проблема. Прво, на секој компјутер мора да му се обезбеди единствена IP-адреса, и мора на некој начин да се конфигурира, т.е. тој мора

да ја знае адресата на својот рутер, како гласи неговиот домен, каде се наоѓа најблискиот DNS-сервер и слично. Второ, корисникот треба да може на мрежата да ги најде одговорите на некои прашања, на пример, како да испрати e-mail на колегата од соседниот град или каде може да најде книга која што ќе ја купи преку Интернет.

Мрежите под Microsoft оперативните системи кои работат со TCP/IP протокол бараат примена на три технологии, со што би се постигнала успешна IP-конфигурација и управување со имињата: Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS) и Windows Internet Name System (WINS). Од оваа позната тројка, само WINS во извесна мерка претставува архаизам, односно технологија која според теоријата може и да се изостави, меѓутоа во пракса тоа може да се направи само доколку мрежата се состои од Windows 2000 или друг понов оперативен систем, како и сите мрежни апликации кои се во употреба после Win NT 4, (а не за него или некој постар оперативен систем). Сè на сè, правилната конфигурација на DNS претставува основа на секоја добро функционална мрежа.

10.2 DHCP – Автоматска конфигурација на TCP/IP

Под претпоставка дека сте се сретнале со конфигурирање IP адреси на некој компјутер со инсталиран Windows Сервер 2003, секако дека не треба истото тоа да се прави и за 3000 компјутери во некоја мрежа одејќи од еден до друг и рачно конфигурирајќи ги сите со различна IP адреса. Или за секој нов корисник во мрежата да се оди во неговата канцеларија за да му се додели IP адреса, притоа внимавајќи да не биде веќе постоечка. DHCP може во огромна мерка да ја поедностави оваа работа, па затоа да видиме како се инсталира и конфигурира DHCP.

Пред само неколку години ако некој сакаше да конфигурира компјутери во мрежа мораше рачно да ги запишува сите компјутери со нивните IP адреси на лист хартија и да оди од компјутер до компјутер за на секого да му додели по една IP адреса. Тоа секако е најтешкиот начин. Подоцна е воведен еден нов помошен TCP/IP протокол наречен “bootstrap protocol” или скратено “BOOTP”. За да може да го употреби овој протокол, секој администратор мора прво да собере листа на сите MAC адреси на компјутерите во мрежата. После тоа, тој мора за секоја MAC адреса да додели по една IP адреса. Така составената листа се чува на некој локален сервер, па кога некоја BOOTP работна станица го започнува својот работен ден, таа преку мрежата ќе побара да и се додели соодветна IP адреса. BOOTP серверот ќе ја препознае MAC адресата на компјутерот што бара IP адреса, ќе види која адреса му одговара во листата и ќе му ја даде соодветната IP адреса. Така BOOTP дури и денеска во некои случаи се користи за конфигурирање на TCP/IP протокол и за доделување IP адреса на некој оддалечен компјутер, без да се пристапува физички до него.

Ова решава и еден друг проблем во однос на конфигурација на компјутерите во мрежа. Да претпоставиме дека еден компјутер е конфигуриран, а еден допрва треба да се инсталира. Без BOOTP, кога ќе се ископира инсталацијата на компјутерот од веќе конфигурираниот компјутер при стартување на новиот, тој ќе ја земе истата IP адреса од постоечкиот компјутер. Така се доаѓа до проблем, ниту еден од двата компјутери нема да може да пристапи на мрежата. Доколку има инсталирано BOOTP, новиот компјутер ќе добие иста наредба како и веќе конфигурираниот: "земи ја IP адресата од BOOTP листата што одговара на твојата MAC адреса". Под претпоставка дека во листата постои новиот компјутер - тој ќе си ја земе соодветната IP адреса и нормално ќе се вклучи во мрежата.

Способноста на BOOTP секако е добра, но не е она што го бара современиот свет, а тоа е да биде динамичка. Денеска компјутерите не се стартуваат од некој локален сервер туку секој компјутер се стартува посебно од свој BOOT наречен BIOS. Покрај тоа, нема потреба сите MAC-адреси да се внесуваат во листа, а веќе постои команда за добивање на MAC-адреса на одреден компјутер IPCONFIG/ ALL. Исто така, треба да се овозможат и привремени IP адреси, на пример за некој гостин во постоечката мрежа што се конектирал со Лаптоп. Затоа на некого му текнало да воведе BOOTP протокол, но со нешто изменети карактеристики, а тоа е DHCP.

DHCP претставува големо подобрување во однос на BOOTP алатката. Тој работи така што му се доделува само опсег на IP-адреси и самиот почнува да ги доделува по системот "кој стигне прв до мене, прво ќе му дадам IP-адреса", на сите компјутери што ќе го побараат тоа од него. Од друга страна, доколку треба DHCP да личи како BOOTP, со помош на DHCP може однапред да се доделат одредени IP адреси на конкретни MAC адреси, и тоа се вика DHCP резервација. Понатаму ќе опишеме како и кога треба да се прави DHCP резервација, а кога треба да се доделуваат променливи IP адреси. Не секој компјутер треба да има статичка IP адреса, и обратно, не смее да се случи DHCP, DNS или WINS-серверот да имаат динамичка IP адреса.

10.2.1 Инсталирање и конфигурација на DHCP сервер

DHCP серверите се компјутери кои доделуваат IP адреси на сите компјутери кои бараат пристап до LAN мрежата. DHCP ќе функционира само под услов работната станица да има TCP/IP конфигуриран за употреба на DHCP, односно доколку TCP/IP софтверот во себе содржи DHCP клиентски програм. Во денешно време скоро секој компјутер ги има овие предуслови.

Инсталирање DHCP сервер

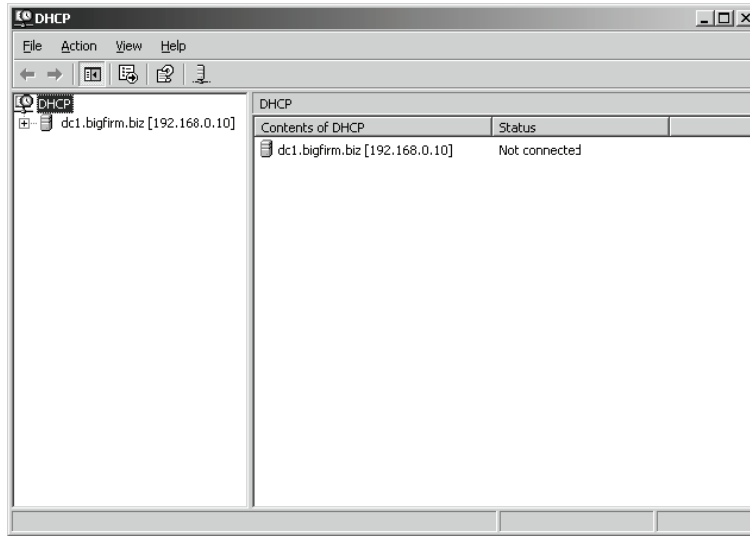
За конфигурирање на DHCP сервер, потребно е да се има на располагање една статичка IP адреса за потребите на DHCP, и да се знае опсегот на IP адреси кои се дадени на располагање.

За да од некој сервер се креира DHCP сервер, потребниот софтвер ќе се инсталира на идентичен начин како што би се инсталирал и било кој друг мрежен сервис, преку палетата Add/Remove Windows Components Control од Panel. Да го објасниме процесот чекор по чекор:

1. Во Control Panel, се отвора аплетот Add or Remove Programs (Start/Control Panel/Add or Remove Programs);
2. Се кликнува на Add/Remove Windows Components, а потоа малку се чека додека не започне извршувањето на Windows Components Wizard;
3. Се притиска на Networking Services, а потоа на Details;
4. Се внесува знакот за потврда покрај опцијата Dynamic Host Configuration Protocol (DHCP);
5. Се притиска на OK, со што се враќа на Windows Components;
6. Се притиска на Next, за да започне инсталирањето на овој сервис. Ова конфигурирање на компоненти ќе потрае неколку минути. При рака треба да се има инсталационото CD за Win 2003 Server;
7. Се притиска на копчето Finish, со што ќе се затвори волшебникот;
8. Се притиска на Close, со што ќе се затвори аплетот Add/Remove Windows Components.

Најдоброто е тоа што после ова не мора да се рестартира компјутерот.

Управувањето со DHCP се врши преку посебен snap-in прозорец кој може да се пронајде во Administrative Tools/DHCP. Со негово стартување се појавува почетна страница со лев и десен панел. Во овој конкретен прозорец е прикажан инсталираниот сервер со знак плус покрај него. Кога ќе се кликне на овој знак плус на екранот ќе се покаже изгледот како на слика 10.2.

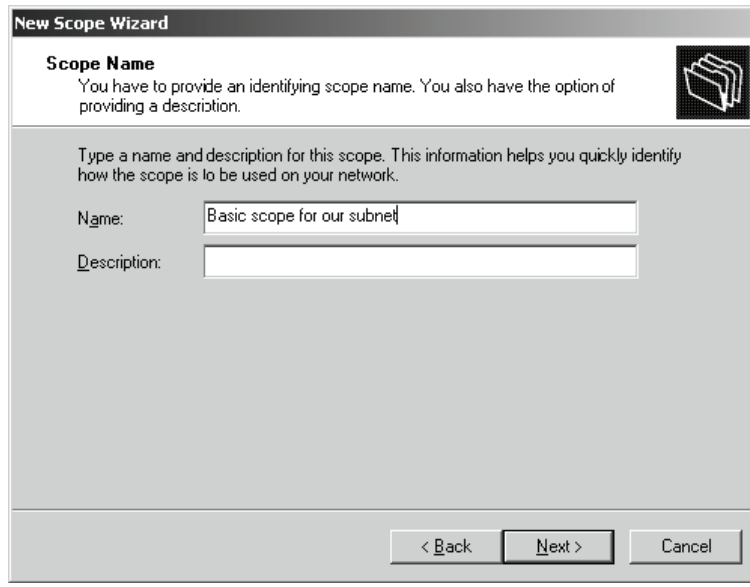


Слика 10.2: Иницијален изглед на инсталиран DHCP сервер

Може да се забележи дека во овој прозорец, листата на сервери е прикажана на левата страна, што значи дека може да се додаваат произволно многу сервери со едноставна команда Action/Add Server.

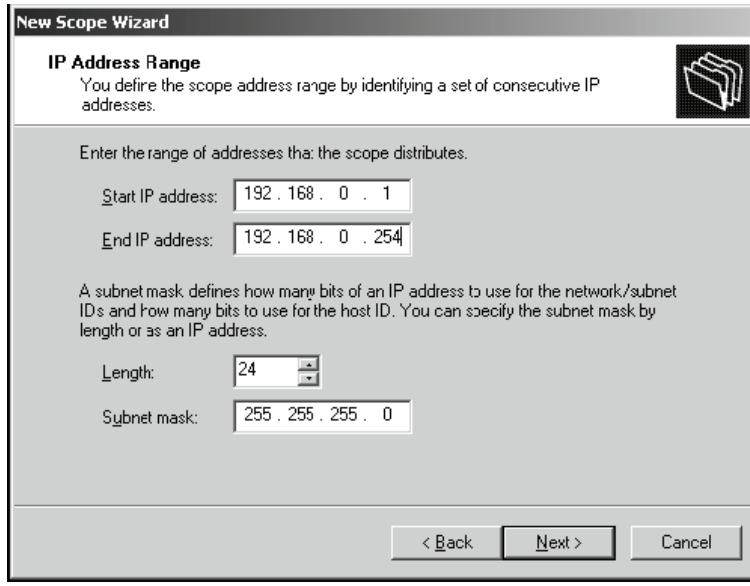
10.2.2 Креирање на подрачје (опсег) на IP адреси

За да може DHCP да врши доделување на адреси, тој мора да биде запознаен со опсегот на адреси што му е на располагање. За креирање на опсег, се притиска на десно копче на иконата за сервер и се одбира командата New Scope, со што ќе започне извршувањето на волшебникот New Scope Wizard. На почетната страница на волшебникот се притиска на Next, па ќе се појави прозорот што е прикажан на слика 10.3.



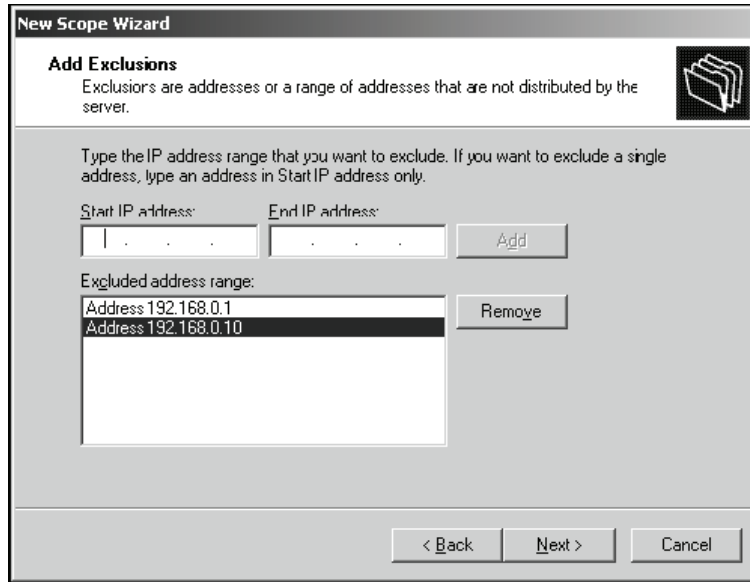
Слика 10.3: Внесување име и опис на подрачјето

На оваа страница треба да се внесат податоци кои се неопходни за идентификација на опсегот, односно неговото име и коментар. Откако ќе се внесат бараните податоци, повторно се притиска Next и се појавува прозорецот од слика 10.4.



Слика 10.4: Внесување IP адреси на опсегот

Опсегот на адреси не е ништо друго освен едно множество на адреси од кој што DHCP може да извлекува IP адреси. Во примерот на сликата 10.4 е креирано едно подрачје со опсег од 192.168.0.1 до 192.168.0.254, т.е. DHCP е употребен како помош при креирање и управување со интранет мрежа од класа C, која што во потполност ќе се состои од нерутабилни адреси.



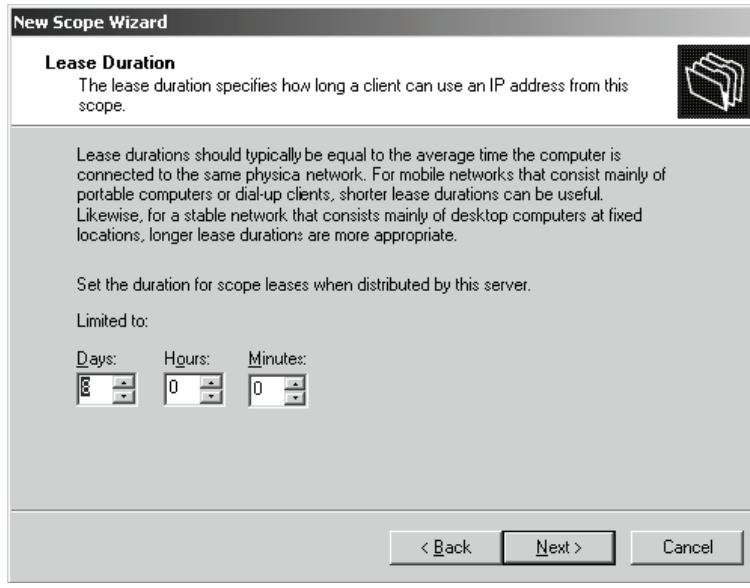
Слика 10.5: Кои адреси да се избегнуваат при доделувањето

Така DHCP е овластен да врши доделување на сите мрежни интранет адреси, но тоа очигледно нема смисла затоа што мора да се остави барем една статичка IP адреса за самиот DHCP. Исто така мора да му се објасни на DHCP таа IP адреса да не ја доделува на никој друг. Се притиска два пати на Next со што на екранот ќе излезе нов прозорец од волшебникот прикажан на слика 10.5, со што на серверот ќе му се наложи кои адреси да ги избегнува при доделувањето.

Како што се гледа, наведени се неколку адреси: адресата .1 претставува default gateway, односно NAT рутер, додека адресата .10 е доделена на самиот DHCP сервер.

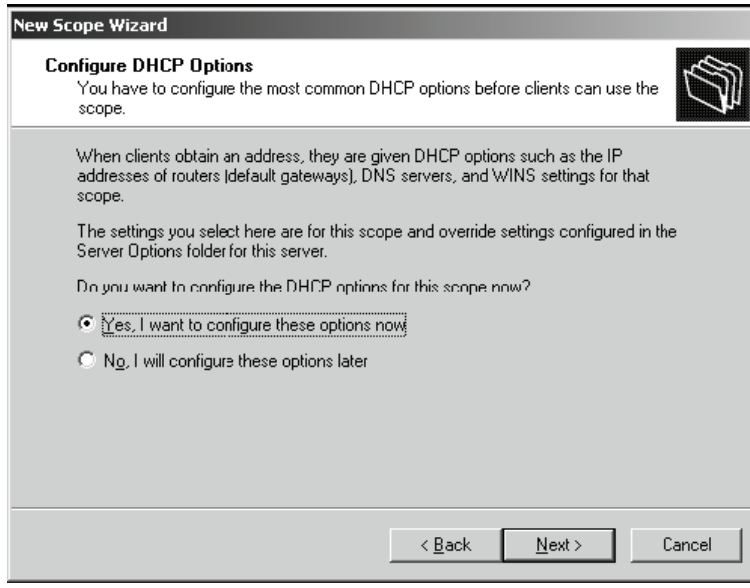
10.2.3 Одредување на периодот на изнајмување

DHCP серверот не ги доделува IP адресите на компјутерите за трајна употреба. Наместо тоа, клиентските компјутери добиваат IP адреса само на одредено време, кое се вика период на изнајмување (lease); после истекот на ова време клиентот мора од DHCP серверот да ја изнајми истата или нова IP адреса, во спротивност клиентот мора да престане со употреба на IP протоколот во целина. Ова време на изнајмување може да се определи рачно, меѓутоа препорака е да тоа биде не повеќе од неколку дена (осум дена би било сосема доволно). Ако се работи за безжична мрежа, овој рок се скратува најчесто на еден ден. За да се конфигурира ова времено изнајмување, се оди пак на волшебникот и се притиска Next, со што ќе се определи времето.



Слика 10.6: Времетраење на доделувањето

10.2.4 Подесување на опции на клиентските компјутери



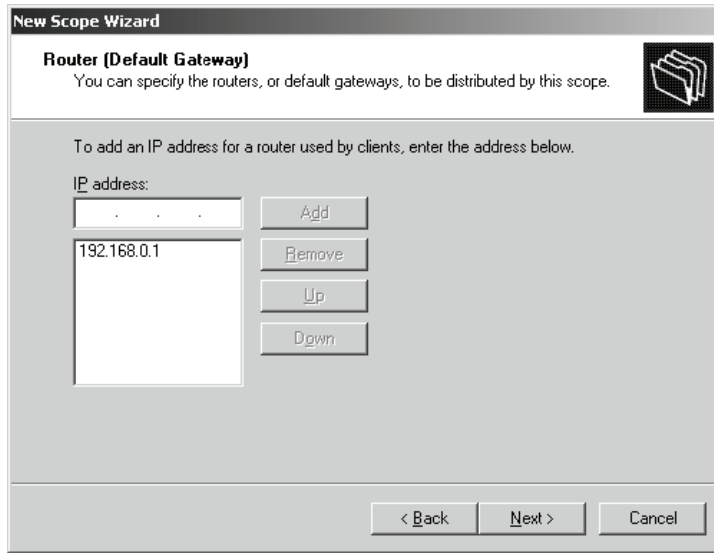
Слика 10.7: Конфигурирање на DHCP опциите

За конфигурирање на IP адресите на клиентските компјутери не мора да се оди од компјутер на компјутер и рачно да се подесуваат опциите за TCP/IP. DHCP серверот ни го овозможува ова директно од серверот. Имено, DHCP може на клиентските компјутери да им ги испорача вредностите што се подразбираат за целата палета на TCP/IP-конфигурацијата:

- одредениот мрежен излез (default gateway)
- името на доменот
- DNS серверот
- WINS серверот

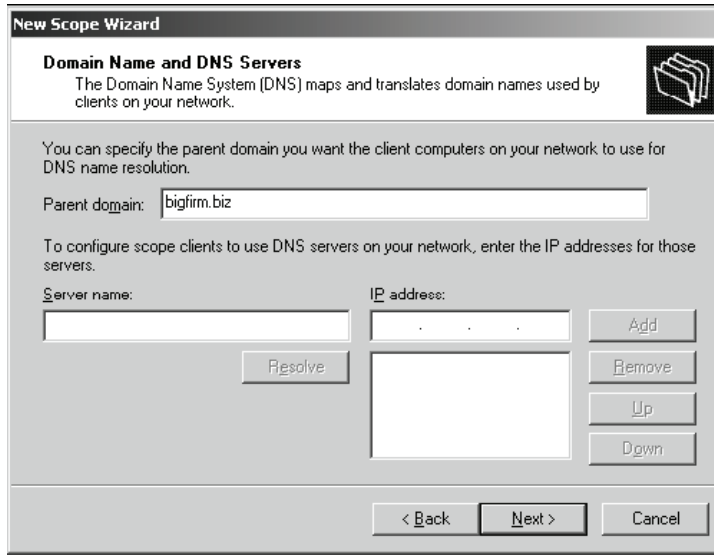
Ова се вредности кои клиентот ќе ги подразбира; инаку секоја од овие вредности може да се промени од самиот клиентски компјутер. Најбитните карактеристики кои треба да се конфигурираат се: IP адресата, подмрежната маска, default gateway, и адресата на локалниот DNS сервер.

По самата своја природа, DHCP серверот секогаш ќе ги изнајми првите две, третата адреса на DNS сервер ја пишувате сами. Иако може да се внесат произволен број мрежни излези (default gateway), никогаш не може да се користи повеќе од еден, па така препорачано е да се внесе само еден. Ова е покажано и на сликата 10.8.



Слика 10.8: Внесување IP адреса на рутерот

На оваа страница од волшебникот може да му се наложи на DHCP серверот да - кога и да му додели на некој клиентски компјутер IP адреса од ова подрачје, името на DNS доменот на тој клиент да го подеси на некоја вредност, пример win2ktest.com, како и да му соопшти на тој клиент на која адреса може да пронајде DNS сервер. Исто така DNS серверите може да се дефинираат и на друг начин: "Овој конкретен DNS сервер додели го на сите подрачја".

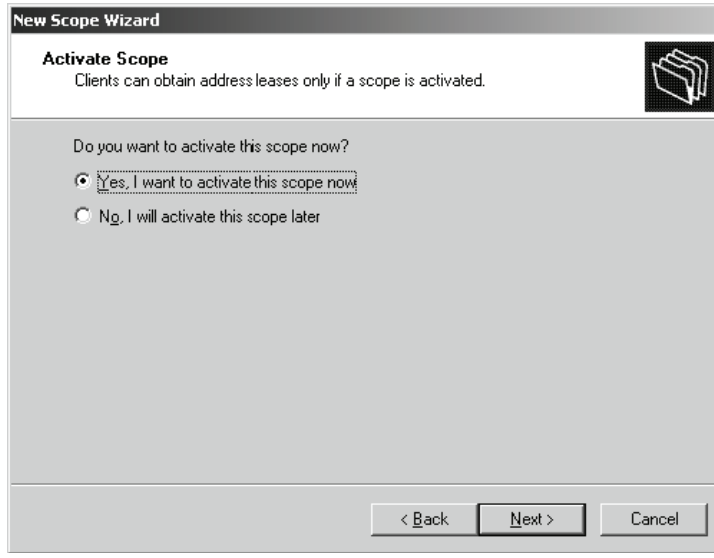


Слика 10.9: Внесување на DNS име

Од друга страна на сите компјутери се дефинира DNS суфикс bigfirm.biz. На тој начин, DNS името на секој компјутер ќе завршува со bigfirm.biz. Како што ќе се види понатаму, кога се зборува за DNS, тоа значи дека овој компјутер својата сопствена регистрација ќе ја изврши со помош на DNS серверот од доменот bigfirm.biz. Се клика на Next со што се појавува нова страница од волшебникот, слика 10.9.

Активација на подрачјето

Се клика на тастерот Next и со тоа се активира опсегот што е дефиниран претходно. Тоа е крај на основните опции за подрачјето што се дефинира, па сега може да се затвори овој волшебник.

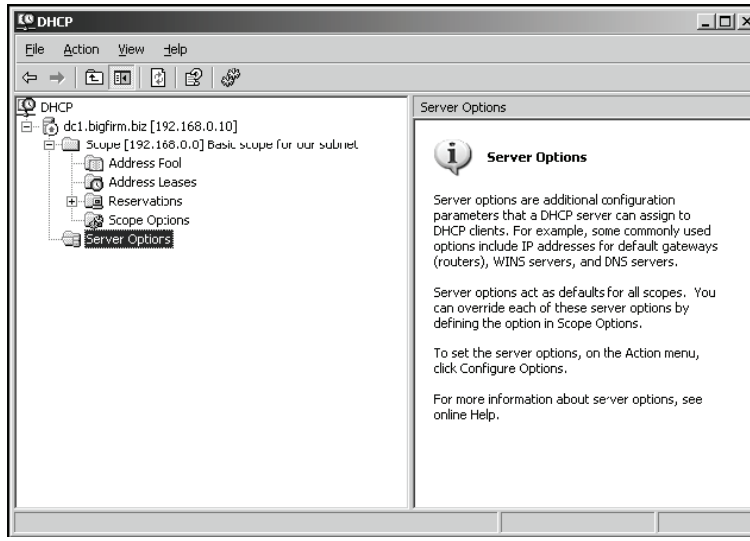


Слика 10.10: Активирање на подрачјето

На самото излегување од него, волшебникот ќе праша дали овој сервер е спремен за доделување на IP адреси. Се притиска на Yes, а потоа на Next, со што волшебникот ќе се затвори, а новото подрачје ќе биде ставено во функција. Сега DHCP прозорецот би изгледал како на слика 10.11.

Ако малку се проанализира оваа слика, ќе се види дека прикажаната хиерархија јасно прикажува неколку работи во врска со функционирањето на DHCP. Овој прозорец овозможува од една локација да имате контрола над било колку DHCP сервери, иако во овој конкретен пример е прикажан само еден DHCP сервер 192.168.0.10. Секој сервер може да има неколку подмрежи што ги опслужува, со по еден опсег на IP адреси за секоја подмрежа. Како што видовме, овие опсези се нарекуваат подрачја, и иако во овој пример има едно подрачје - факт е дека може да постојат неограничен број на подрачја. Во секое подрачје може да се воочат неколку важни информации: опсегот на адреси, листа на адреси кои овој сервер веќе ги

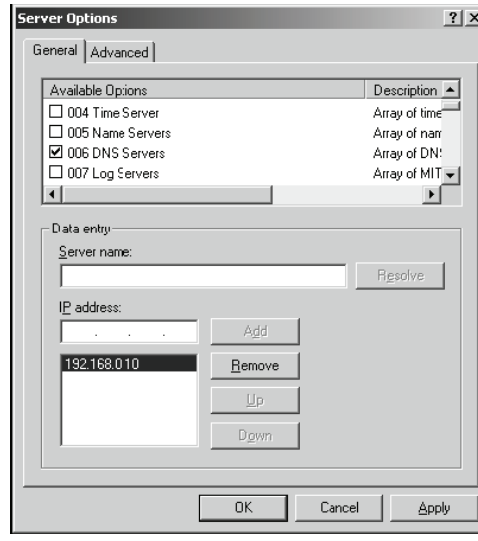
доделил, адреси кои се однапред резервирани за одредени компјутери, како и специјални TCP/IP подесувања што DHCP серверот треба да им ги испорача на своите клиенти.



Слика 10.11: Изглед на DHCP прозорецот

10.2.5 Подесување на опции за сите подрачја

Во долните делови на прикажаната слика може да се види директориумот со името Server Options. Значењето на овие серверски опции доаѓа до израз кога на еден сервер се дефинирани повеќе од едно подрачје.



Слика 10.12: Конфигурирање на опции на серверот

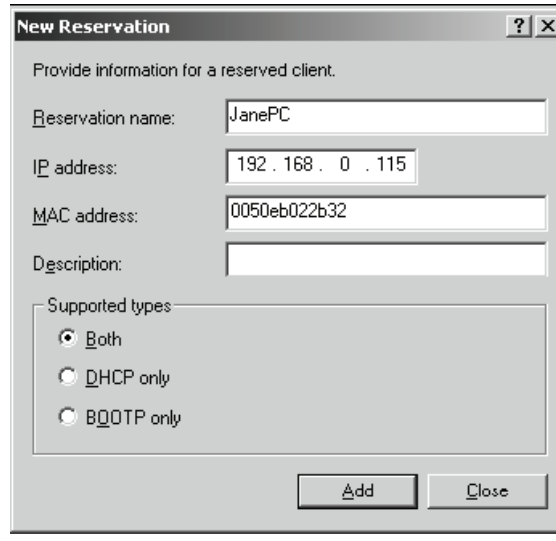
Така на пример, доколку постојат три различни подрачја, а два DNS сервери, со еден потег може да се конфигурираат опциите за сите подрачја на даден сервер. Доволно е да се кликне на десното копче на глушецот врз директориумот Server Options, и од помошното мени да се избере Configure Options, со што ќе се отвори прозорецот кој е прикажан на слика 10.12.

Овде се клика на DNS сервер, со што се овозможува внесување адреси на DNS сервери, слично како што се прави истото и со помош на волшебникот. Другите опции во овој дел подобро е да не се подесуваат, од едноставна причина што DHCP нема да знае како да ги искористи.

10.2.6 DHCP резервација

Некогаш има ситуации кога мора едноставно да се нареди: ”Овој компјутер ќе ја добие точно оваа IP адреса”. За среќа тоа со DHCP е многу едноставно. Во DHCP прозорецот може да се воочи директориум со име Reservations. Се клика врз него со десното копче и се одбира командата New Reservation. Ќе се отвори прозорец сличен на оној прикажан на слика 10.13.

Има и уште една многу подобрена опција кај Windows Сервер 2003, а тоа е следнава. Кога ќе се креира резервација за некој компјутер, тогаш тој се појавува во листата на резервации. Со десен клик врз него, се добива помошна команда Configure Options, којашто ако се кликне, ќе може да се дефинираат конкретни параметри за тој компјутер, како што се DNS сервер, име на домен, WINS сервер и слично. Ова е навистина многу значајна опција.



Слика 10.13: Внесување на резервирана адреса

DHCP на клиентската страна

Откако инсталацијата на DHCP протоколот е завршена на серверската страна, ќе може да се испроба како тој се користи на клиентската страна. Тоа е многу едноставно. Кога на некој компјутер му е доделена IP адреса, за да се види која IP адреса му е доделена - треба да се појде до тој компјутер и да се внесе во командната линија команда ipconfig /all. Оваа команда може да се искористи и за друга намена. На пример, може да се присили DHCP клиентот да ја напушти изнајмената IP адреса и да побара од DHCP серверот друга, нова IP адреса. Тоа се прави најпрво со командата `ipconfig /release`, а потоа со `ipconfig /renew`. Во поновите Windows оперативни системи постои и една команда за двете работи:

```
Netsh int ip reset filename
```

меѓутоа ова е многу посложена команда која за да може да се користи, треба многу добро да се проучи.

10.2.7 Како функционира DHCP?

Сега ќе видиме во кратки црти како функционира во суштина DHCP сервисот. Секој компјутер кој има изнајмено IP адреса, податоците за изнајмувањето ги чува во некој скриен фајл. Поради ова, доколку на пример имате компјутер кој има IP адреса со траење од 4 дена, тој после истекот на тоа траење нема слепо да оди и да бара нова IP адреса. Наместо тоа, тој уште пред да заврши тој рок ќе оди до DHCP серверот што му ја доделил таа адреса, и ако тој е сè уште активен ќе побара од него продолжување на рокот за истата IP адреса. Тоа е наједноставната опција за продолжување на неговата IP адреса. Доколку тој DHCP сервер не е активен, тогаш компјутерот треба да бара друг DHCP сервер што ќе му додели нова IP адреса. Основните чекори на преземање на IP адреса се следниве:

- Со порака DHCPDISCOVER се емитува барање за доделување на IP адреса кое е упатено до сите блиски DHCP сервери,
- Серверите одговараат со порака DHCPOFFER, која ги содржи IP адресата и нејзиното време на траење,
- Клиентот ја одбира најатрактивната понуда и праќа повратна порака DHCPREQUEST, со што ја потврдува избраната IP адреса,
- Серверот што ја понудил оваа IP адреса ја завршува процедурата со порака DHCPACK, што претставува потврда за позитивно решеното барање.

Оваа комуникација, бидејќи се остварува пред компјутерот да има IP адреса, се одвива преку посебен протокол наречен UDP протокол (составен дел од TCP/IP протоколот).

10.3 ПРЕВЕДУВАЊЕ НА ИМИЊА

Една од заедничките особини на NetBIOS (IBM) и Winsock (Microsoft) се состои во тоа што апликациите сакаат да поддржат употреба на едноставни имиња на компјутерите. Точно е дека секоја машина или компјутер на Интернет, исто како и на сите Сервер 2003 мрежи, поседуваат единствени IP адреси, но никој не сака да ги користи овие адреси за идентификација на серверот. Кога ќе се отвори директориумот MB Network Places, во него компјутерите би требало да бидат прикажани по името, како на пример \\Personel, а не по IP адресата 220.10.99.32. Исто така, компанијата Amazon, рекламира продажба на книги преку www.amazon.com, а не преку својата IP адреса 208.216.182.15. Значи потребен ни е некој сервер со база на податоци, кој може името www.amazon.com да го преведе во IP адреса 208.216.182.15, и името \\Personel во 220.10.99.32. Оваа постапка за конвертирање на имињата на компјутерите во нивни IP адреси се вика преведување на имиња (name resolution). Со овие проблеми беа соочени и Winsock и NetBIOS, но тие дојдоа до две различни решенија. За преведување на имињата NetBIOS употребува Windows Internet Name Service (WINS), а од друга страна Winsock објавува преведување на имиња со помош на Domain Name System (DNS) серверот.

Ова ќе го поедноставиме со користење на еден пример. Замислете ја оваа аналогија. Телефоните и поштата претставуваат уреди за комуникација. Доколку сакате да повикате некој свој пријател по телефон можете да го најдете под бројот 02\3222055, а доколку сакате да го добиете по пошта тогаш неговото име ќе биде ул."Партизанска" бр.505. И двете имиња совршено го отсликуваат вашиот пријател, меѓутоа тоа се две различни имиња, бидејќи комуникациските системи наложуваат употреба на различни типови на имиња. На сличен начин и server01.bigfirm.biz и \\server01 претставуваат валидни, но различни имиња за еден ист сервер.

Како и да е, со појавата на Windows Server 2003 многу од стручњаците на оваа тематика претпоставуваа дека комплетно ќе биде исфрлен од употреба WINS и ќе дојде крајот на неговото постоење. Меѓутоа не само што не се случи тоа, туку и нема најава дека ќе се случи и во многу наредни оперативни системи, па така ќе мора да се совлада и овој начин на преведување на имиња, заедно со DNS начинот на преведување. Едноставно морате да ги имате и двата, ако сакате непречена работа на сите компјутери во вашата мрежа.

10.3.1 Преведување на имињата пред појавата на WINS

Клиентите кои немаат дефинирано WINS сервер, при обидот да преведат некое NetBIOS име во IP адреса, користат неколку различни методи.

Доколку ги имаат на располагање овие клиенти, ќе ги употребат следниве алатки:

- HOSTS фајлот, ако го имаат,

- Емитување на порака, broadcasts,
- LMHOSTS фајлот, ако го имаат,
- DNS сервер, ако е присутен на мрежата.

HOSTS фајловите се едноставни ASCII фајлови. Секоја линија се состои од IP адреса, барем едно празно место и името што одговара на таа IP адреса. LMHOSTS функционира на сличен начин како и HOSTS. LMHOSTS фајлот се состои од парови на IP адреси и нивни NetBIOS имиња, со максимална должина од 15 карактери.

```
100.100.210.12 ducky
211.39.82.15 jabberwock
```

Овие фајлови се од голема помош дури и во најновите оперативни системи, бидејќи некогаш се единствениот начин за решавање на проблемите со имињата во мрежата.

10.3.2 WINS: Сервис за имиња за Windows

Видовме дека пред појавата на WINS, светот на компјутерските мрежи бил прилично негостољубиво место, каде многу прашања во врска со преведувањата на имиња останале неодговорени.

За да може WINS да работи, тој мора да биде инсталиран под NT4 или некој понов оперативен систем. На постари оперативни системи од NT4, тој нема да работи.

Во основа, кога прв пат ќе се стартува некој клиентски компјутер со WINS, тој веднаш ќе отиде до WINS серверот и уредно ќе му се претстави, односно ќе изврши регистрација на своето име. Клиентите ја знаат IP адресата на WINS серверот, било им била внесена рачно со инсталирањето на TCP/IP софтверот, или пак клиентот ја добил IP адресата на WINS од DHCP серверот, при изнајмувањето на IP адреса.

Клиентот всушност добива две IP адреси, една на примарниот, една на секундарниот WINS сервер. Тој се обидува да добие внимание од примарниот WINS сервер, а ако тој во одреден период не може да одговори на барањето на клиентот, клиентот ќе се обиде да се регистрира кај секундарниот WINS сервер. Дали сме се конектирале на примарниот или на секундарниот WINS сервер, може да се види со командата ipconfig /all со што се добива адресата на WINS серверот.

Во текот на процесот на регистрација на своето име, клиентот ќе може да провери дали името што му го дава на серверот, е единствено во дадената мрежа. Ако WINS серверот забележи дека името што го дава клиентот веќе постои во мрежата, тој ќе му се обрати на клиентот и ќе му каже дека тоа име е веќе зафатено. Кога клиентот ќе се исклучи од мрежата, тогаш WINS серверот ќе го ослободи неговото име и тоа име ќе биде достапно за друг клиент што ќе се вклучи во мрежата.

Слично како и кај DHCP, и кај WINS серверот имињата имаат таканаречен период на важење, кој се нарекува интервал на обновување (renewal interval).

Под општо-прифатени предлози овој период трае 6 дена, и најверојатно никогаш нема да има потреба да се менува ова време. Најкраткиот интервал за некое име што WINS серверот може да го прифати е 40 минути.

Многу слично на DHCP, и клиентите на WINS се обидуваат пред истекот на своето време да ги продолжат своите имиња кај серверот. Тие поднесуваат барања за продолжување на нивното време на живот кај серверот, многу пред да им се заканува истекување на регистрацијата за нивното име, отприлика една осмина од вкупното време.

10.3.3 Инсталирање на WINS

Инсталирањето на WINS е многу слично со инсталирањето на другите мрежни сервиси. При инсталирањето на WINS сервери на една мрежа, имајте на ум дека не мора воопшто да се поставува по еден WINS сервер на секоја подмрежа. Тоа е многу голема предност на WINS серверот. Секако, добра идеја е да се обезбеди уште еден WINS сервер кој ќе служи како секундарен, чисто поради остварувањето на потребен степен на толеранција од грешки.

Под нормални услови, клиентот ќе може многу лесно да го пронајде серверот, но во еден мал број на случаи може да се случи WINS серверот да биде зафатен, па да не може навреме да му одговори на својот клиент, по што клиентот ќе отстапи од него. Ова ќе се случи доколку се преоптовари WINS серверот. Тоа пак најверојатно ќе се случи доколку WINS се инсталира на истиот сервер каде е инсталиран и контролерот на домени. Како што се очекува, WINS серверот има најмногу работа наутро кога сите ги вклучуваат своите компјутери, со што автоматски започнува процесот на регистрација, а исто така и контролерот на домени најмногу е зафатен наутро кога сите се логираат на мрежата. Овој факт сам по себе би требало да претставува доволно предупредување.

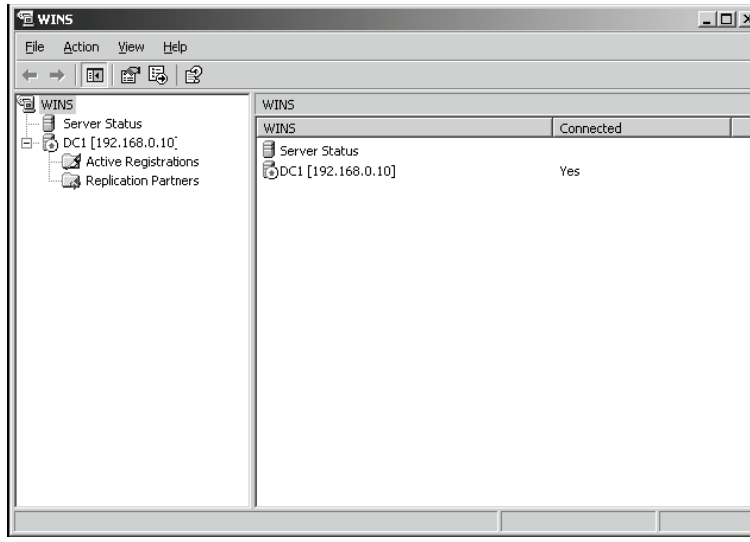
Токму овде доаѓа до израз инсталирањето на секундарен WINS сервер, кој најпожелно е да се инсталира на истата машина каде што има инсталирано резервен контролер на домени, ако постои таков.

За инсталирање на WINS серверот, потребно е да се постапи по следнава процедура:

- Се отвора Control Panel (Start/Control Panel/Add or Remove Programs),
- Се кликнува на Add/Remove Windows Components, па потоа се чека да се појави прозорецот Windows Components Wizard,
- Се кликнува на Networking Services, а потоа на копчето Details,
- Се внесува знак за потврда кај Windows Internet Name Service,
- Се кликнува OK, за да се вратиме на Windows Components,

- Се кликнува Next, со што ќе започне инсталација на одбраниот сервис. Ова ќе потрае неколку минути и на екранот ќе се појави страница со наслов Completing the Windows Components Wizard,
- Се кликнува Finish, со што завршува волшебникот,
- Се кликнува Close, за да се затвори прозорот за дијалог Add or Remove Windows Components.

После ова не е потребно никакво рестартирање на компјутерот. Под Start/Administrative Tools, се добива нова опција која служи за контрола на WINS. Се отвора овој прозорец и се притиска на знакот плус покрај новокреираниот сервер, со што се добива нешто слично на слика 10.14.



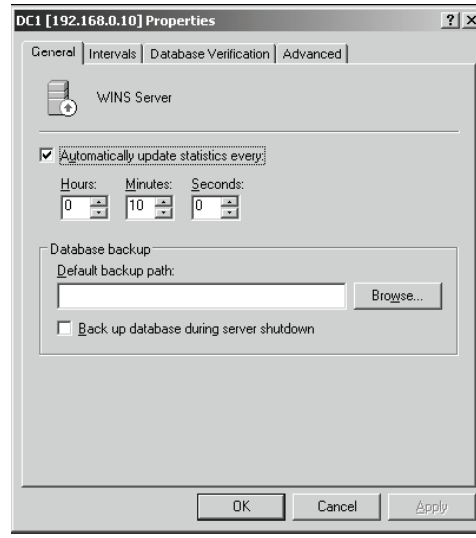
Слика 10.14: Почетен изглед на WINS подрачјето

Овде нема никаква потреба за авторизација на WINS серверот. Прва работа што треба да се направи на WINS серверот, е да се информира за оние компјутери на подмрежата кои не се WINS клиенти, туку користат NetBIOS преку TCP/IP. Вакви машини нема да има многу, но сепак ќе постојат, на пример може да има компјутери кои се тука пред 1995 година. WINS серверот не мора да биде информиран за компјутерите што имаат статичка IP адреса. Тие самите ќе се регистрираат кај него.

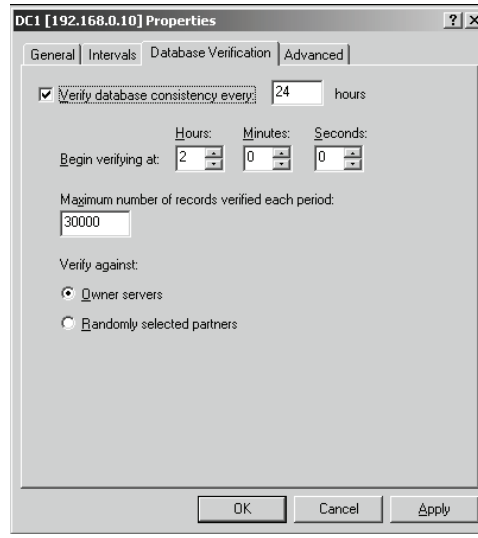
10.3.4 Конфигурирање на WINS серверот

Во левиот панел од WINS прозорецот, се клика на иконата сервер, па од помошното мени се одбира Properties. На мониторот ќе се појави страница со својства како на слика 10.15. Ако во полето default backup path се внесе име на некој директориум, WINS редовно ќе креира резервни копии на своите податоци, што е одлична опција за опоравување од катастрофи или нешто

слично. Сега се кликнува на табот за да се добие прозорецот како на слика 10.16.



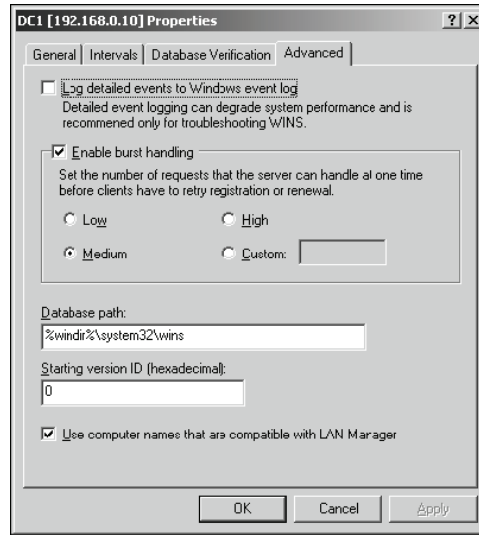
Слика 10.15: Особини на WINS серверот



Слика 10.16: Верификација на базата на податоци

Овде има навистина големо подобрување во однос на NT4. WINS отсекогаш се соочувал со проблеми на својата база на податоци дистрибуирана низ мрежата. Кај овие записи постојано доаѓа до оштетување. Ова оштетување брзо се шири така што за кратко време ќе мора од почеток да се креираат WINS податоците. Оваа опција е воведена за да може WINS серверот периодично да ги проверува своите записи и да ги споредува со другите

записи од другите сервери од мрежата. Вклучувањето на оваа опција е многу добра идеја. Препорачливо е таа да биде наместена на 24 часа, како и проверката да се врши на сопственичкиот сервер, а не на некој случајно избран сервер. Ова значи дека ќе се проверува со серверот на кој е генериран дадениот запис. Ако се притисне Advanced табот, ќе се покаже прозорец како на слика 10.17.



Слика 10.17: Напредни опции на WINS серверот

Веднаш ќе се забележи опцијата за бележење (log) на податоците. Оваа опција може да се остави вклучена, меѓутоа WINS така ќе бележи многу непотребни настани, и после некое време ќе стане многу бавен. Затоа препорачливо е оваа опција да се исклучи, освен ако навистина има потреба да се следи сè што се случува со работата на WINS серверот.

10.4 DNS – DOMAIN NAME SERVICE

Дали некогаш сте се запрашале што се случува кога ќе влезете или ќе притиснете на web адреса во вашиот пребарувач? Како вашиот компјутер се конектира на сајтот што го барате? Делот што ракува со оваа процедура, е Интернет Domain Name Service (DNS) сервисот.

Слично како што секој телефон има свој идентификационен број, секој web сајт или "домен" на Интернет има своја единствена IP адреса. IP адресите се 32-битни броеви претставени по четири бајти одделени со точки. Секој бајт презентира број од 0 до 255, затоа најголемата IP адреса е 255.255.255.255.

На луѓето им е тешко да запаметат 12 цифрен број, затоа web сајтовите се идентифицираат со имиња како www.sitename.com наместо неговата IP адреса. DNS е податочна база на имиња и нивните соодветни IP адреси.

На почетокот, секој компјутер на Интернет имал листа на сите домен имиња и нивните соодветни IP адреси. Но таа брзо станала преголема. Сега базата со податоци за имињата и нивните преводи во IP адреси се одвиваат од компјутери назначени како DNS сервери.

Секој DNS сервер има податоци само за домените што тој ги сервисира. Кога компјутерот прави барање до неговиот DNS, можно е тој DNS сервер да нема податоци за да се одговори на барањето. Специјални "root name" сервери имаат листа на DNS сервери со највисоки домен-и како .org, .com, .edu и слично. На пример, највисокиот DNS за .com, ги листа сите имиња на DNS серверите за домени кој завршуваат на ".com".

Ако DNS серверот нема податоци да одговори на барањето, прави барање до root-name серверот. Тој му враќа адреса од серверот каде таа информација може да се најде. Секое domain име на Интернет потребно е да биде во листата на најмалку два DNS сервери. Ова е за случај ако еден DNS сервер падне, барањето за тоа име да биде одговорено.

DNS исто така преведува IP адреси во домен-имиња. Ова им овозможува на серверите да го логираат пристапот, а администраторите да изведуваат одредени административни задачи и безбедносни мерки.

Информациите препратени преку Интернет се делат на помали пакети со TCP протоколот. TCP ги прикачува IP адресите на бараниот домен на секој пакет, така што тој може да биде рутиран до доменот. TCP исто така ги прикачува и IP адресите на барачкиот компјутер на пакетите, така што може да се прати повратен одговор.

Кога ќе влезете или притиснете на web адреса во вашиот пребарувач, DNS ги преведува web адресите на сајтот во IP адреси.

IP адресите се 32-битен цел број. Ако некој сака да прати порака неопходно е да ја вклучи и адресата на дестинацијата, но на луѓето им е поедноставно да им дадат на машините други имиња, што полесно се памтат (имиња на хостови). За оваа причина се користи DNS (Domain name system). Овие логички имиња исто така дозволуваат независност од познавањето на физичката локација на хостот. Хостот може да се премести во друга мрежа, додека корисниците продолжуваат да го користат истото логичко име.

DNS е дистрибуирана база на податоци, користена од TCP/IP апликациите за поврзување на имињата на хостовите со IP адреси, и овозможува рутирање на информациите од електронската пошта. Секоја Интернет страна (универзитет, кампус, компанија, или оддел во компанија) си одржува своја база на податоци и има свој сервер што другите системи можат да го пребаруваат преку Интернет. DNS го обезбедува протоколот кој овозможува клиентите и серверите да комуницираат помеѓу себе.

Системот го користи DNS преку преведувач на адреси. Преведувачот го зема името на хостот и ја враќа IP адресата, или ја зема IP адресата и го враќа името на хостот. Како што можеме да заклучиме - преведувачот ја враќа IP адресата пред да побара од TCP да отвори конекција или да прати податок користејќи UDP.

Време е да заборавиме на теоријата; ќе покажеме како практично се инсталира еден едноставен DNS сервер со што ќе се испробаат неговите способности во преведување имиња. Овој сервер постепено ќе го надградувате до крајот на ова поглавје. Може да се каже дека во девет од десет случаи, основна причина на проблемот лежи во DNS-от. Без правилно подесен DNS, вашите компјутери нема да можат да се пронајдат еден со друг за проверување на автентичноста, (а познато е дека, доколку две машини на растојание сакаат да воспостават меѓусебна комуникација, тие мора да извршат проверка на автентичноста, зошто во спротивно ништо нема да се случи). Заради сето ова, овој пример ќе го објасниме полека, чекор по чекор. Во овој прв чекор, потребно е да се инсталира и да се подигне DNS серверот.

10.4.1 Запознавање со доменот bigfirm.biz

Ќе биде креиран еден DNS домен, а подоцна и активен директориум, за една измислена компанија, под името bigfirm.biz. Кога сѐ ќе заврши, ќе постојат две работи. Прво, ќе постои DNS домен под името bigfirm.biz, а вашиот компјутер ќе игра улога на авторитативен DNS сервер за тој домен. Второ, ќе треба и еден активен директориум под името bigfirm.biz. За вкупниот број на потребни компјутери да се сведи на минимум, на вашиот компјутер воедно ќе му доделите и улога контролер на доменот за компанијата Bigfirm.

Сепак, во овој момент треба да се креира наједноставен можен DNS сервер, кој само ќе знае како да излезе на Интернет и да одговори на поставените прашања (queries). Сега ќе објасниме како се инсталира DNS–сервер под Windows Server 2003. Што ќе ви биде потребно? Во секој случај, за работа со Server 2003 не ви е потребна некоја голема и силна машина. Потребно е, само да го обезбедите следново:

- На вашиот компјутер да биде инсталиран Windows Server 2003,
- Тој да е конектиран на Интернет, и
- Во времето на изведување на сите овие вежби, да се зачува иста IP адреса.

Во повеќето случаи, “вистинските” DNS сервери во реалниот свет, оние на кој доверливо се одвиваат секојдневните работи, ќе поседуваат било статички IP адреси или некои непроменливи IP адреси, добиени по пат на DHCP -резервации. На крајот на оваа вежба, од вас ќе се бара на оваа машина да доделите некоја конкретна IP адреса, но засега тоа воопшто не е важно. Сепак, дозволете ми да ви истакнам дека:

1. секоја машина, на која имате намера да и доделите улога на DNS сервер во вашата мрежа, мора да има постојана IP адреса, и
2. доколку сакате овој DNS сервер да биде способен за пронаоѓање адреси на јавниот Интернет, тој мора да има IP адреса која ќе може да се конектира на Интернет.

Забележете дека е сосема нормално адресата на оваа машина да претставува некоја од адресите на нерутабилниот опсег на адреси - можете да и доделите било кој тип адреса, на пример 192.168.x.x, 10.x.x.x, или 172.x.x.x.

Сè додека можете со успех да „ping-ате“ IP адреси на глобалниот Интернет, вашата машина ќе претставува совршено добар DNS сервер за потребите на овој едноставен пример.

Сепак, без оглед кој метод ќе го примените, од големо значење е да ја препознаете IP адресата на овој компјутер: за тоа да го дознаете, отворете ја командната линија и испишете ipconfig, па потоа притиснете Enter. Запишете ја оваа адреса и чувајте ја на сигурно место. Во продолжение ќе му додадете на DNS серверот неколку посакувани, но не и задолжителни карактеристики.

Секој контролер на домени за некој активен директориум мора да има DNS суфикс, чие име ќе се поклопува со активниот директориум. Ќе креирате домен под името bigfirm.biz. За овој DNS сервер, кој подоцна ќе ја одигра улогата на DNS сервер за доменот bigfirm.biz, веќе сега се доделува DNS суфикс bigfirm.biz. Во оваа почетна фаза, тоа воопшто не е од суштинско значење, но нема причина тоа веднаш да не се направи; освен тоа, доколку DNS серверот нема одреден суфикс, во неговиот log file на настани (event log), ќе бидат забележани некои вознемерувачки пораки.

Конечно, ќе предложиме име на овој компјутер. Оваа машина ќе извршува голема работа за потребата на bigfirm.biz доменот, па поради тоа предлагаме да и дадете назив bigdog.

10.4.2 Промена на имињата на компјутерите и суфиксите на DNS серверот

Промената на името на компјутерот и неговиот DNS назив се извршува преку картичката Computer Name, или попрецизно:

1. Се кликнува на Start, потоа се клика со десното копче врз My Computer, па од помошното мени се избера Properties.
2. Се кликнува на картичката Computer Name.
3. Се кликнува на копчето Change, со што се отвора дијалог за името Computer Name Changes.
4. Во полето Computer Name, се внесува bigdog.
5. Се кликнува на копчето More.
6. Ќе се отвори дијалог-прозорец со DNS Suffix and NetBIOS Computer Name, па во полето под името Primary DNS Suffix of this Computer, се внесува bigfirm.biz.
7. Се кликнува OK, за да се вратите во дијалог-прозорецот Computer Name Changes.
8. Се кликнува OK, со што се затвора дијалог-прозорецот Computer Name Changes.

9. После тоа, на екранот ќе се појави дијалог кој ќе ве предупреди дека морате да го рестартирате компјутерот, за извршените измени да влезат во сила. Се клика на ОК, со што се затвора и овој дијалог.
10. Се кликнува ОК, со што се затвора страницата System Properties.
11. Се кликнува на тастерот Sec, со што би го рестартирале компјутерот.

После рестартирање на компјутерот, се задава команда ipconfig /all. Треба под Host Name да биде испишано bigdog, а под Primary DNS Suffix да биде прикажано bigfirm.biz.

Проверка на IP адресите и конективноста

Додека на екранот сè уште се прикажани излезни податоци на командата ipconfig, се гледа доделената IP адреса. После тоа, се проверува дали вашиот компјутер може да „ping-ува“ компјутери од реалниот свет. Го отворате командниот prompt, па испишувате, да кажеме, ping 164.109.1.3, со што би „ping-увале“ DNS сервер на еден голем Интернет провајдер, а можете да се обидете и со еден ping од страна на AOL-овиот DNS сервер, на адреса 152.163.159.232.

10.4.3 Инсталирање на DNS серверски софтвер

Сега сте сосема спремни да го подигнете DNS серверот. Постапката за инсталирање на DNS сервер е потполно слична со инсталирање на било каков друг мрежен сервис, како што е, да речеме, DHCP или WINS. Проверете дали ви е при рака инсталационото CD за Server 2003, односно дали имате пристап до фолдерот I386, во кој претходно сте извршиле инсталирање на самиот оперативен систем; на системот ќе му биде неопходен пристапот на CD-то, за да го “симне” софтверот за DNS серверот. После тоа, се постапува по следнава процедура:

1. Се отвора Control Panel (Start/Control Panel/Add or Remove Programs),
2. Се клика на Add/Remove Windows Components, па се чека да се појави прозорецот Windows Components Wizard,
3. Се клика на Networking Services, а потоа на копчето Details,
4. Се означува знакот за потврда кај Domain Name System (DNS),
5. Се клика на ОК, со што ќе се вратиме на Windows Components.
6. Се клика на Next, за да започне инсталирањето на сервисот.

За време отприлика неколку минути, системот на екранот ќе прикаже порака “Configuring Components” и можеби ќе бара во CD-ROM уредот да се внеси инсталационото CD за Server 2003.

Нешто покасно, на екранот ќе биде прикажана завршната страница на постапките, под следниот наслов- Completing the Windows Components

Wizard. Доколку во меѓувреме, важечката IP адреса на компјутерот се добие од DHCP серверот, извршувањето на постапките ќе се запостави, и тој ќе предложи дека е добро за вашиот сервер да набавите статичка IP адреса, иако не присилува да се направи тоа. После тоа на екранот ќе биде прикажана страница со TCP/IP својства. Во реалност, за некој произволен DNS сервер, секогаш се употребува статичка IP адреса, или DHCP резервација. Меѓутоа, поради тоа што овде се занимавате само со DNS серверот, може слободно да се употреби било која IP адреса, која ќе ви ја додели DHCP серверот, т.е. вашиот ISP по случаен избор (или вградениот DHCP сервер внатре во DSL/кабелскиот рутер, ако е тој начинот на кој сте конектирани на Интернет). Едноставно, се кликнува три пати на OK и се завршува постапката.

7. Се клика на Finish, со што се затвора прозорецот.
8. Се клика на копчето Close, со што се затвора прозорецот Add/Remove Windows Components.

Насочување на DNS-серверот самиот на себе

Бидејќи поставувањето на едноставни DNS-барања ќе ги прави вашиот DNS сервер, а секако треба серверскиот компјутер да работи на преведување на DNS имиња, тој се упатува кон самиот себеси (всушност DNS-серверскиот софтвер кој е инсталиран на него). Тоа можете да се направи преку GUI интерфејсот - во внатрешноста на Network Connections, се притиска десното копче на Local Area Connection, или како што гласи вашето име за конкретната NIC картичка, од помошното мени се избира Properties, се клика на картичката General, потоа се притиска на Internet Protocol (TCP/IP), па на копчето Properties и на крај се селектира радио копчето Use the following DNS address, т.е. во прикажаното поле се внесува IP адресата на вашиот DNS сервер. Значи, со оглед на работата, претпоставуваме дека сте обезбедиле еден тест-компјутер, на кој успешно сте го инсталирале DNS серверскиот софтвер. Потоа, претпоставуваме дека неговата IP адреса гласи: 192.168.0.12. Сега ќе мора да отворите страница со TCP/IP својства (Properties) на тој компјутер, па така во полето Preferred DNS Server ја внесувате неговата IP адреса- 192.168.0.12.

Алтернативно, преферираниот DNS сервер може да се дефинира и преку командната линија:

```
netsh int ip set dns name static ipaddress primary
```

каде наместо ipaddress треба да се напише вистинската адреса на вашиот сервер, а наместо parameter name да се внесе првиот збор од името на инсталираната NIC картичка. Според тоа, ако на вашиот компјутер му е доделена IP адреса 192.168.0.12, а инсталираната мрежна картица има име Local Area Connection, тогаш вашиот преферирaн DNS може да се дефинира со командата:

```
netsh int ip set dns local static 192.168.0.12 primary
```

Од друга страна, доколку инсталираната NIC картичка има име Wireless Network Connection, тогаш зборот “local” ќе го замените со “wireless”, па командата ќе изгледа вака:

```
netsh int ip set dns wireless static 192.168.0.12 primary
```

Зошто баш “wireless” и “local”? Затоа што, доколку компјутерот поседува повеќе од една NIC картичка, тогаш командата netsh мора точно да знае на која мрежна картичка се однесува. Секоја NIC картичка има свое име, како “Local Area Connection”, “Local Area Connection 2”, “Wireless Network Connection” или слично. Затоа, за нивно разликување, може да се употреби целосно име, или само толку почетни букви колку што е неопходно да се избегне секоја можност на забуна. На пример, ако поседувате две мрежни конекции, од кои една носи име “Local Area Connection”, а другата “Wireless Network Connection”, тогаш ќе биде доволно да се внесе само “l” или “w”, за на netsh командата недвосмислено да и се соопшти - на која NIC картичка ќе се однесува. Доколку се користи целосно име, што во себе содржи празнини, тогаш мора да се стави под наводници, на пример “Local Area Connection”.

Еве уште еден пример. Ако на вашиот компјутер е инсталирана една NIC картичка со име Local Area Connection, и друга NIC картичка со име Local Area Connection 2, тогаш во командата netsh ќе мора да се употреби полно име со наводници, тоа е:

```
netsh int ip set dns "Local Area Connection 2" static
192.168.0.12 primary
```

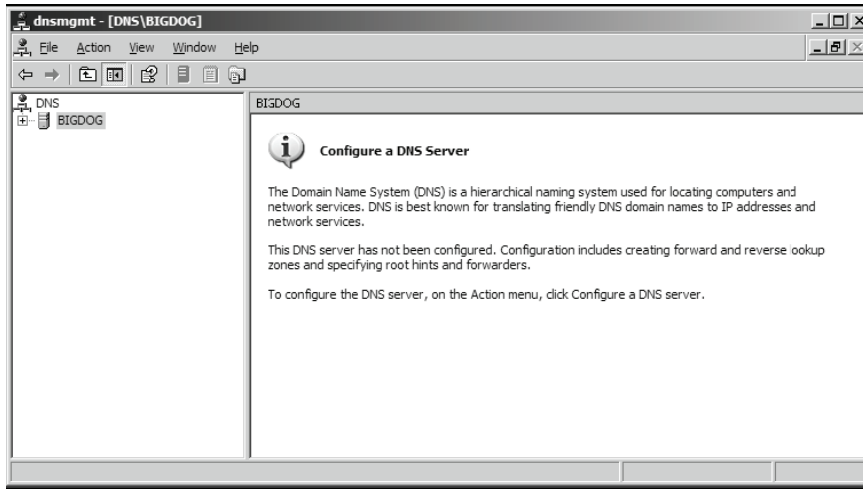
Совет: Општото правило гласи - заради преводот на името, DNS серверите обично треба да се насочат сами кон себе; тоа наједноставно се постигнува со внесување на IP адресата на тој сервер во полето Preffered DNS Сервер. Ако пак, конфигурацијата на овој сервер се врши преку DHCP резервации, тогаш и адресата на неговиот преферирaн DNS сервер може, исто така, да се дефинира преку DHCP резервации.

Заради повторна проверка на извршената постапка со помош на командниот промпт, уште еднаш се задава командата ipconfig /all. За таа прилика, во параметарот “IP Address” и “DNS Servers”, би требало да биде прикажана идентична IP адреса. Доколку тоа не е случај, се враќате на почеток и повторно ги дефинирате адресата на преферираниот DNS сервер, било преку GUI интерфејс, или со помош на командата netsh, на претходно опишаниот начин.

10.4.4 Стартување на DNS прозорци

Како и кај DHCP и кај WINS, после инсталирањето на DNS серверскиот софтвер, не е потребно да се прави рестарт на компјутерот. Се кликнува на Start/Administrative Tools/DNS, за да се отвори DNS снап-прозорецот. Во

неговиот лев панел ќе видите икона што го претставува вашиот сервер; се клика на неа, па ќе видиме страница која е прикажана на сликата 10.18.



Слика 10.18: Почетна страница на DNS прозорецот

Почетна страница на DNS snap-от

Во десниот панел ќе се прикаже навидум корисна порака, која ви нуди автоматско конфигурирање на вашиот DNS сервер. Послушајте го нашиот совет:

Внимание: Никогаш немојте да ја употребувате опцијата Configure a DNS Server, за конфигурација на вашиот DNS сервер.

Всушност, доколку кликнете со десниот тастер на глушецот врз иконата на серверот, па со помошното мени ја изберете опцијата Configure a DNS Server, ќе покренете извршување на еден волшебник, кој е многу склон кон присвојување на многу погрешни претпоставки, во однос на начинот на кој сакате да го подесите својот сервер. Овој волшебник е многу ефикасен во тоа, од DNS серверот, "по грешка" да направи нешто што се вика "приватен root". (Се знае дека овој проблем поретко се јавува под Сервер 2003, отколку кај Сервер 2000, но ние и понатаму гласаме против оваа опција). Иако поправката на овој приватен root и не е толку комплицирана, сепак изгледот може да биде прилично застрашувачки, кога за прв пат ќе се сретнете со него. Сега ќе покажеме како еден сервер се конфигурира без никакви потешкотии, (и без помошта на волшебникот Configure a DNS Server Wizard).

Пред да се напушти овој прозорец, дозволете ни да ви обрнеме внимание на едно место, кај кое морате да стекнете навика почесто да навраќате: log фајлови Event Viewer. Се клика на знакот за плус покрај иконата на серверот, па ќе се отвори директориум под име Event Viewer; во него, покрај останатото, се наоѓа и еден директориум под името DNS Events. Се клика на

него, па во десниот панел ќе се видат записи кои можат да ви пружат многу значајни информации во врска со функционирањето на вашиот DNS Server. Доколку практично сте ги завршиле сите чекори кои досега ги изложивме, тогаш во овој лог фајл ќе бидат забележани само две случувања. Првиот од нив е еден настан со подолг опис, под ознаката Event ID 708, кој во основа го кажува следното: "Хмм, изгледа дека овој DNS сервер во себе не содржи никакви DNS информации", така да, веројатно сакате тој при преведувањето на имињата потребните податоци да ги земе од некоја друга локација- т.е. да биде исклучиво со кеширање на DNS сервер. Ова е само информативна порака, поради која воопшто не би требало да се вознемирувате. Друг забележан настан носи ознака Event ID 2 и едноставно ве известува за стартувањето на DNS сервисот. Значи, имате само две информативни пораки; дали тоа значи дека прегледот на Event Viewer претставуваше залудно потрошено време? Напротив. Многу е корисно, од време на време да ја анализирате содржината на овој лог фајл, дури и ако поединечните пораки на кои ќе наидете во него, се по малку шифрирани.

10.4.5 Обид за преведување на имињата

Сега, кога пред себе имате активен DNS сервер, како и еден компјутер кој на него се потпира, (т.е. истиот тој серверски компјутер), да ја испробаме наједноставната работа на светот - простото преведување на име. Ќе се обидеме да го преведеме името www.minasi.com. Значи, го стартувате командниот промпт (доколку не е отворен), па во него се внесува команда nslookup и се притиска Enter. Веројатно ќе се покаже нешто како ова:

```
C:\>nslookup
DNS request timed out.
timeout was 2 seconds.
*** Can't find server name for address 206.246.253.12: Timed
out
Default Server: UnKnown
Address: 206.246.253.12
>
```

Вашата IP адреса ќе биде различна, но ако тоа го занемарите, содржината на вашиот екран веројатно ќе биде идентична со прикажаното. Алтернативно, можеби ќе видите нешто помалку застрашувачки излезни податоци како:

```
C:\>nslookup
Default Server: ip68-106-120.hr.hr.cox.net
Address: 68.106.183.120
>
```

Единствена разлика е во начинот на кој се подесени некои други DNS сервери. Доколку на екранот упорно се прикажува порака за грешка од типот "*** Can't find server name for …" тогаш едноставно игнорирајте ја. Нешто подоцна ќе научите како засекогаш да ја отстраните. Всушност, командата nslookup е донекаде нестрплива, така да, ако DNS серверот не одговори во

рок од две секунди, веднаш ќе се пожали со "истек на временскиот рок" (тајмаут) порака. Затоа, тајмаутот се прави малку пофлексибилен. Се внесува:

```
Set timeout=10
```

Ќе се согласите дека 10 секунди звучи како многу разумен рок. После тоа внесете:

```
www.minasi.com
```

па притиснете Enter. Би требало да го видите следното:

```
Default Server: UnKnown
Address: 206.246.253.12
Non-authoritative answer:
Name: cablenic.minasi.com
Address: 68.15.149.117
Aliases: www.minasi.com
>
```

Повторуваме, конкретните излезни податоци кои ќе бидат прикажани на вашиот монитор може донекаде да се разликуваат, затоа што вашиот DNS сервер поседува различна IP адреса, а можеби и додека ја испробувате постапката ќе ја смените адресата на Web Серверот. Но сето тоа е небитно. Најважно е следното: вашиот DNS сервер преведе некое име од Интернет.

Исто така постои нешто што се нарекува проследувач (forwarder). Многу луѓе сметаат дека мора да ги конфигурираат проследувачите на DNS серверот, за DNS серверите воопшто да можат да вршат превод на адреси на Интернет. Тоа воопшто не е точно; сè што му е потребно на DNS серверот, е конекција на Интернет и листа на 13 ICANN root сервери. Повторуваме, IP адресата на овој сервер воопшто не мора да биде рутабилна, под услов на мрежата да постои соодветен NAT/PAT рутер. Пробајте ја сами оваа постапка- инсталирајте Internet Connection Sharing, па поставете еден компјутер на вашата интерна мрежа, мрежа на која и е доделена IP адреса 192.168.0.x. Направете од тој компјутер DNS сервер, па испробајте на него тоа што пред малку го направивме, сè би требало да работи без никакви потешкотии, под услов вашата конекција со ISP да остане недопрена (доколку Web серверот minasi не е достапен, пробајте со преведување на некое друго име, на пример www.ibm.com).

Според тоа, после инсталирањето и подигањето на вашиот DNS сервер, веднаш треба да ја испробате неговата основна функција -насочете го тој DNS сервер кон самиот себе, подигнете го помошниот програм nslookup, и пробајте да преведете некое име од Интернет.

10.4.6 Отстранување грешки на едноставен DNS сервер

Ако не функционира, се проверуваат следните работи:

- Двапати проверувате дали DNS сервисот навистина се извршува. Додека се извршува DNS сервис, отворате DNS снап, се клика на десниот тастер врз иконата која го претставува вашиот DNS сервер, од помошното мени се одбира опција All Tasks, и потоа се анализираат понудените опции. Би требало да ги видите опциите Stop, Pause и Restart, но никако опцијата Start, затоа што тоа укажува дека DNS сервисот не е подигнат, (одбирате опција Start за да се подигне). Ако тоа не се случи, или започне па прекине, се отвора директориум под име Event Viewer - можеби во него постои порака за грешка поради настанатиот проблем.

- Се проверува дали DNS серверот е насочен сам спрема себе; давате команда ipconfig /all и се уверувате во идентичноста на IP адресата на компјутерот и адресата на DNS серверот.
- Се проверува дали серверот може да се рутира од Интернет. „Ping“-ате на неколку IP адреси. Доколку не постои можност за ping на овие IP адреси, тогаш проблемот не е во DNS, туку во рутерот.
- Се проверува дали вашите мрежни администратори не инсталирале некој параноичен firewall, кој ги блокираа сите DNS пребарувања. Се внесува nslookup, па Enter, и потоа се внесува сервер 164.109.1.3, за вашиот компјутер да го насочите кон DNS серверот на еден голем ISP. Сега би требало без проблем да можете да преведувате. Доколку тоа не е случај, тогаш - или поседувате оштетена копија на помошната програма nslookup, или вашата способност за комуникација со јавниот Интернет е грубо спречена од firewall-от.
- Уште еднаш ја анализирате содржината на Event Viewer. Во него често ќе наоѓате корисни информации.

Со малку среќа, во овој момент ќе поседувате успешно инсталиран DNS сервер, кој во извесна мерка сте го испробале. Затоа е време да се вратиме на некои концепти и теории.

10.4.7 Зона против доменот (и уште малку за делегирање)

Значи до сега образложивме дека на DNS серверите се чува база на податоци за DNS доменот, и тоа прецизно зборувајќи - не за домените, туку за зоните (zones). Што е тоа зона?

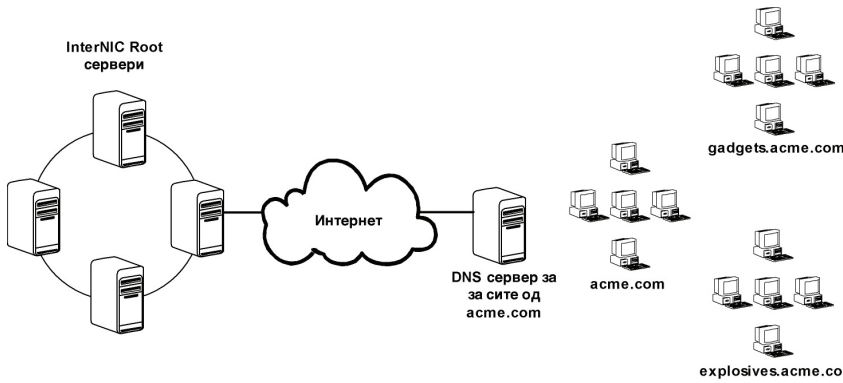
Тоа е специфичен DNS термин, кој во основа значи “опсег на Интернет адреса”, за која DNS серверот е конкретно заинтересиран. За да можете да сфатите како тоа функционира, ќе разгледаме еден пример за компанијата Acme Industries (acme.com), фирма која е добро позната на сите обожаватели на Warner Bros цртаните филмови. Воедно, со уште еден пример ќе го објасниме процесот на делегирање.

Кога компанијата Acme воспоставила конекција со Интернет, нејзиниот примерен DNS сервер бил поставен во главното седиште на оваа корпорација во Чикаго, а на сите компјутери на мрежата се доделени DNS имиња. Потоа, на мрежата се поставени машини со имиња како jills-pc.acme.com, bigserver.com, www.acme.com <http://www.acme.com> и така натаму.

Меѓутоа, како што времето поминувало, Acme сè повеќе почнало да чувствува напади од конкуренцијата, од страна на својот долгогодишен омразен ривал, компанијата Apex Limited (apex.com). Затоа своето познато одделение Gadgets, во чии производствени хали настанале изумите како Acme instant rupe, Acme санки на ракетен погон, и Acme кондурчиња, го преместиле на територијата на Мексико, надевајќи се на намалени трошоци на производство. Во меѓувреме, компанијата Acme ја купила една белгиска фабрика за производство на муниција и одлучила да затвори уште една домашна фабрика, од одделот за Explosives, за на пазарот да пласира исклучиво експлозив од Белгија.

Напомена: Треба да имате на ум дека овде се зборува за DNS домен, а не домен за активниот директориум. Односно, доколку вие го поседувате АД доменот под името acme.com, би било добро на сите компјутери на тој домен да им се додели DNS суфикс acme.com; на тој начин, ако името на вашиот компјутер е mypc, тогаш неговиот комплетен DNS назив ќе гласи mypc.acme.com.

Мрежни стручњаци на компанијата Acme имаат на располагање две основни опции за конфигурирање на свој DNS, кои се илустрирани на сликите 10.19 и 10.20.

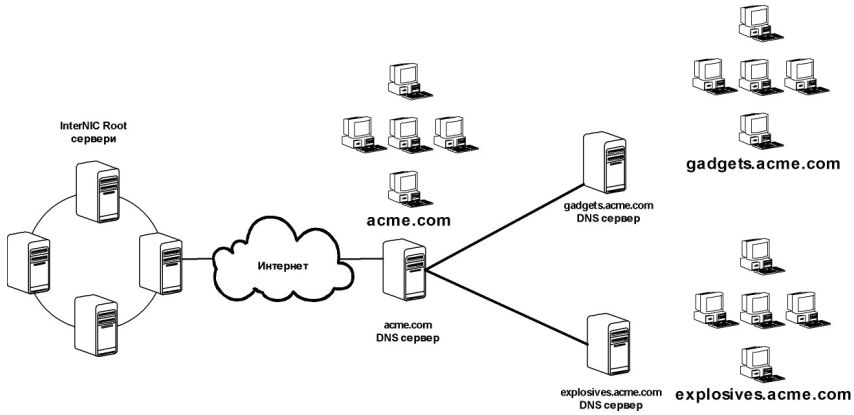


Слика 10.19: Мрежна структура на компанијата Acme

Во конфигурацијата прикажана на сликата 10.19, Acme ја има задржано постоечката состојба на работите: постои само еден сервер, кој е примарен авторитет за сите Acme машини. Ова е совршено правилно решение, но тоа нема да им се допадне на сите, како што веројатно и самите претпоставивте.

Да се разбереме, ова воопшто не е погрешно решение; тоа е само едно од можните решенија, што на некои луѓе нема да им се допаднат. Имено, на

овој начин, вработените во Белгија би морале да се потпираат на мрежните оператори во Чикаго, за да бидат нивните машини правилно распоредени во DNS базата на податоци; притоа би можело да се случи, секогаш кога Белгијанците ќе имаат потреба да сместат во базата на податоци нови машини и IP адреси, во Белгија е утро, а во Чикаго полноќ, така што Белгијанците ќе бидат принудени да чекаат. А, бидејќи се тие експлозивни момчиња, нивното барање за сопствен DNS сервер нема да може да помине без соодветна реакција на елегантно дотераните менаџери од Чикаго. Одделението во Мексико би можело да се соочи со слични проблеми како Белгијанците. Тоа, на крајот, неизбежно би довело до креирање на конфигурацијата која е прикажана на сликата 10.20.



Слика 10.20: Поинаку формирани домени на компанијата Acme

На сликата 10.20, одделението Explosives поседува сопствен DNS сервер, а истото важи и за мексиканското одделение Gadgets. Чикашкиот DNS сервер acme.com, поседува многу мала база на податоци - во основа, таа ги содржи само имињата на неколку компјутери сместени во Чикаго, како и неколку записи кои велат: „Иако сум јас, навистина, DNS сервер за доменот acme.com, немојте да ме прашувате ништо во врска со компјутерите кои имаат име како нешто-точка-Explosives.acme.com или нешто-точка-Gadgets.acme.com; таквите прашања поставувајте им ги на други машини“. Се сеќавате дека, според DNS терминологијата, во овој случај би рекле дека acme.com серверот ја делегирал задачата за преведување на имињата за доменот Gadgets.acme.com на некој DNS сервер во Мексико, односно дека задачата за преведување на името во доменот Explosives.acme.com ја делегирал на некој друг DNS сервер, кој е сместен во Белгија.

Според тоа, acme.com сè уште претставува еден домен, но неговите DNS одговорности - т.е. „неговите должности во областа на DNS именскиот простор“ - сега се поделени на повеќе сервери. Значи, како да ги наречеме овие под-сетови на доменот, на кои исклучиво авторитет имаат новите DNS сервери на компанијата Acme? Правилниот термин би бил DNS зона, или едноставно зона. На сликата 10.19, Acme својот DNS го има конфигурирано

во облик на само една зона. Од друга страна, на сликата 10.20, Acme поседува три зони: својата top-level зона acme.com, потоа зоната Explosives.acme.com и зоната Gadgets.acme.com.

Какво значење има тоа за активниот директориум? Па, ако вашата мрежа користи AD домени - што е многу веројатно - тогаш секој домен ќе бара своја DNS зона. Според тоа, од точката на гледиште на DNS-от, во светот во кој не би постоел AD, компанијата Acme своите домени acme.com, Explosives.acme.com и Gadgets.acme. com би можела да ги конфигурира во облик на една голема зона, но и во облик на две или три зони. Меѓутоа, Acme не би можела да ја одржи ваквата флексибилност доколку би креирала домени на активниот директориум под името acme.com, Explosives.acme.com и Gadgets.acme.com; во тој случај, активниот директориум би барал три одвоени зони.

10.4.8 Lookup зони за нормално и инверзно пребарување

Во целото досегашно излагање кажувавме дека основната задача на DNS-от се сведува на конвертирање на имињата на хостовите, како што е kiwi.fruit.com во соодветни IP адреси, како што е на пример 205.22.42.19. Но, DNS-от може да ја извршува и обратната задача; DNS серверот може да биде запрашан: „Кое име на хост и е придружено на IP адресата 205.22.42.19?“

Процесот на конвертирање на имињата на хостови во соодветна IP адреса се нарекува преведување нанапред на имињата (forward name resolution). Обратниот процес, т.е. конвертирањето на IP адресата во соодветно име на хостот, се нарекува инверзно преведување на имињата (reverse name resolution).

Сите информации за дадениот домен, како што е на пример fruit.com, на DNS-от се чуваат во таканаречени зонски датотеки (zone files). Според тоа, на доменот fruit.com постои една зонска датотека, која DNS-от може да ја употреби за пронаоѓање на IP адресата на компјутерот под име kiwi.fruit.com. Но, каде ќе го најде DNS-от името на хостот кој и одговара на IP адресата 205.22.42.19?

Да се потсетиме дека организациите, кои се задолжени за управување со Интернетот, IP адресите им ги доделуваат на корисниците во блокови. На секоја Интернет мрежа постои една DNS зона наречена зона за инверзно пребарување (inverse lookup zone). Значи, ако претпоставиме дека доменот fruit.com е поставен на некоја мрежа од класата C, со мрежен број 205.22.42.0, на некого ќе му биде доделена задачата да се грижи за зоната за инверзно пребарување, на мрежата 205.22.42.0. Додуша, името на оваа зона за инверзно пребарување е донекаде чудно. За да се конструира ова име, се земаат оние квартали (делови од IP адреса) кои се добиени од овластената Интернет организација - се отфрлаат ги оние квартали над кои имате целосна контрола - па се запишуваат по обратен редослед, додавајќи на крајот .in-addr.arpa. На пример, одговорниот за мрежата 205.22.42.0, ќе мора

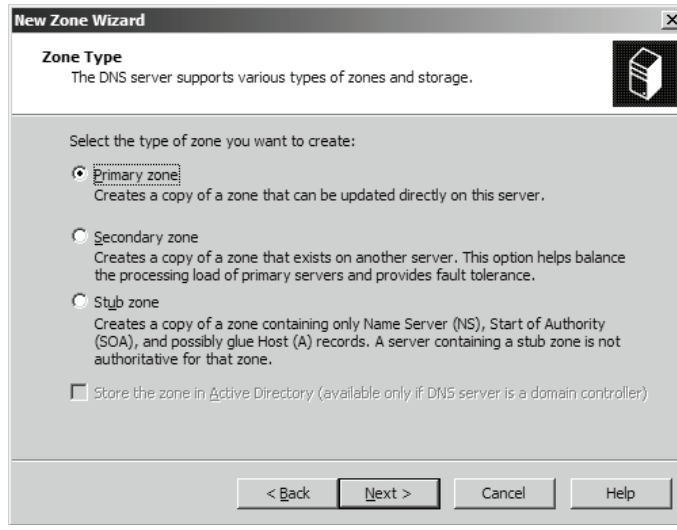
да креира зона за инверзно пребарување, под името 42.22.205.in-addr-arpa. Еве уште неколку примери:

- На мрежата од Б класа, 164.109.0.0/16, треба да се отфрлат двата последни квартали, чија вредност е нула, па останатите два квартали да се запишат по обратен редослед, за да се добие зона за инверзно пребарување, под името 109.164.in-addr.arpa. Забележете дека тука постојат само два квартали, бидејќи се работи за мрежа од класата B, чиј сопственик има целосна контрола над последните два квартали.
- За мрежата од класата A, 4.0.0.0/8, името на зоната за инверзно пребарување би гласело 4.in-addr.arpa. Значи, во случајот на мрежата од класа A, употребен е првиот квартал, така што името на соодветната зона за пребарување се состои од само еден број.
- За мрежата од класата C, 200.120.50.0/24, треба да се отфрли само последниот квартал и останатите квартали да се испишат по обратен редослед, со што името на зоната за инверзно пребарување станува 50.120.200.in-addr.arpa.

10.4.9 Креирање на зона bigfirm.biz

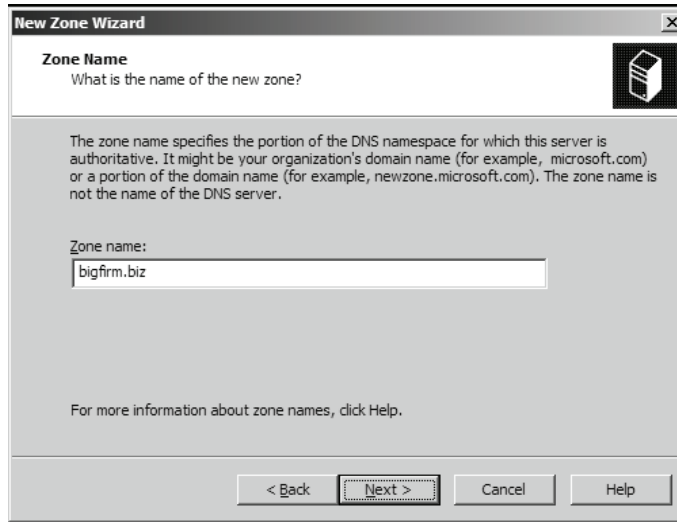
Да видиме што е потребно за конфигурирање на нов DNS домен, т.е. да почнеме со усвојување на стручниот речник, кој го користат повеќето DNS експерти за конфигурирање на DNS зона. Ќе направиме зона за bigfirm.biz. Со оглед на тоа што тоа ќе биде зона во која на DNS серверот ќе му го соопштите името на некој компјутер, како на пример mypc.bigfirm.biz, а тој ќе ви одговори со соопштување на IP адресата на тој компјутер, тоа ќе биде зона за нормално пребарување (forward lookup zone). Еве ја процедурата за креирање на bigfirm.biz зоната:

1. Се отвора DNS snap-in, ако не е веќе отворен: се кликнува на Start/Administrative Tools/DNS.
2. Се клика на знакот за плус покрај икончето кое го претставува вашиот сервер - икончето со името bigdog - за да го отворите овој серверски објект. (Ако покрај ова иконче е веќе прикажан знакот минус „-“, тогаш можете да го прескокнете овој чекор).
3. Под икончето bigdog ќе забележите три директориуми: Forward lookup zone, Reverse lookup zone и Event Viewer. Кликате со десниот тастер од глувчето на директориумот Forward lookup zone, па од помошното мени се одбира опцијата New Zone, со што ќе започне извршувањето на волшебникот под име New Zone Wizard. Кликате на Next, после што на екранот ќе ја видите страницата која е прикажана на сликата 10.21.



Слика 10.21: Опции за конфигурирање на нова зона

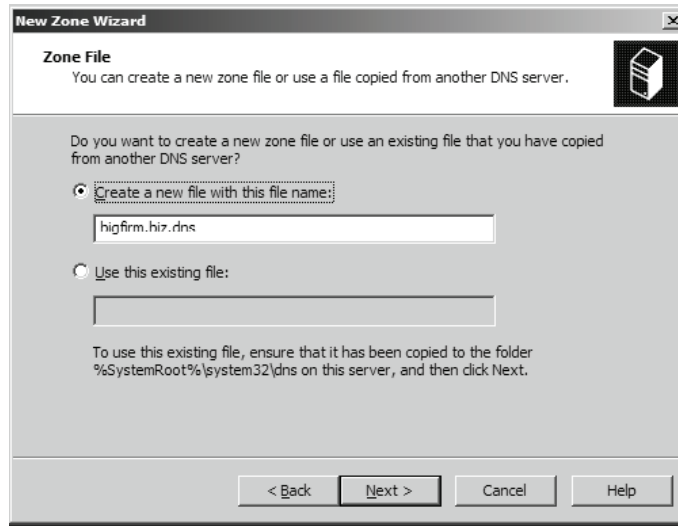
4. Забележете дека на располагање имате три опции за нова зона - Primary, Secondary и Stub. Бидејќи ќе креирате примарна зона, одберете ја опцијата Primary - всушност, таа е веројатно веќе селектирана, (по default) - па потоа кликате на Next, за да ви се појави страницата од сликата 10.22.



Слика 10.22: Определување на името на зоната

5. Како што се препорачува на самата страница, се внесува посакуваното име на зоната, кое во овој случај гласи bigfirm.biz. Се

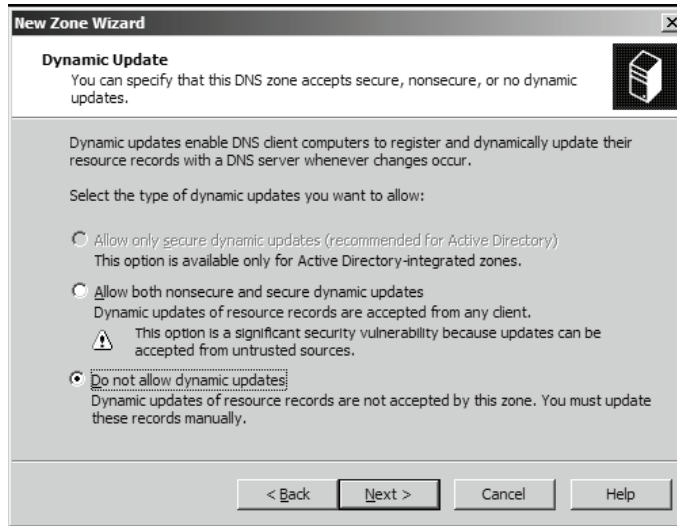
кликнува на Next, за да се отвори страницата која е прикажана на сликата 10.23.



Слика 10.23: Кое е името на зонската датотека?

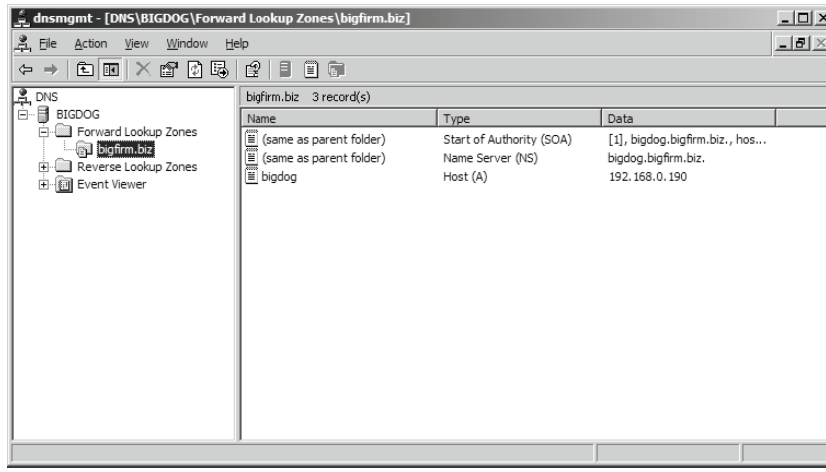
6. На најголем број од различните верзии на DNS сервери - а DNS серверот базиран на оперативниот систем Сервер 2003, по default, не е никаков исклучок - сите зонски информации се чуваат во обична текстуална ASCII датотека. (По default, затоа што, како што ќе видите подоцна, DNS информациите можат да бидат складирани и во базата на податоци на активниот директориум). Доколку не е наредено поинаку, DNS серверот автоматски ќе креира датотека со име име-на-зоната.DNS, која ќе биде сместена во директориумот Windows\System32\DNS. Всушност, ова е многу добро, бидејќи, на тој начин, поправката на DNS-от од катастрофа е многу лесно. Ако, случајно, дојде до ненадејно откажување на серверот bigdog, за кратко време би можело да се креира замена за него, под услов да поседувате резервна копија од датотеката bigfirm.biz.DNS. Едноставно, улогата на сервер му се доделува на некој компјутер со оперативен систем 2000 или 2003, па потоа се презема датотеката bigfirm.biz.DNS од стариот сервер и се копира во директориумот Windows\ System32\ DNS, на новиот DNS сервер. Се стартува извршувањето на истиот овој волшебник кој беше претходно употребен, но на оваа негова страница се одбира опцијата Use the Existing File, со што се насочува волшебникот кон датотеката под име bigfirm.biz.DNS.
7. Заради продолжување на креирањето на зоната bigfirm.biz, се кликнува на тастерот Next, за да се види на екранот страницата која е прикажана на сликата 10.24.

8. Деталите за динамичкиот DNS се надвор од овој материјал, но накратко, тој на компјутерите им овозможува автоматски да ги регистрираат сопствените информации во DNS серверот, слично како на WINS сервер. DNS-от оваа можност ја доби дури пред неколку години, така што во волшебникот таа, по default, е исклучена. Меѓутоа, со оглед на тоа што оваа опција ќе ни биде многу корисна, селектирајте ја опцијата Allow Both Nonsecure and Secure Dinamyc Updates - игнорирајте ја предупредувачката порака со застрашувачка содржина - па потоа кликнете на Next и Finish, со што креирањето на зоната ќе биде приведено кон крајот.



Слика 10.24: Подесување на динамичкото ажурирање

9. Се отвора директориумот Forward lookup zone, па во него ќе видите нов директориум, со име bigfirm.biz; се кликнува врз него во левиот панел, па на екранот ќе видите нешто слично како на сликата 10.25.

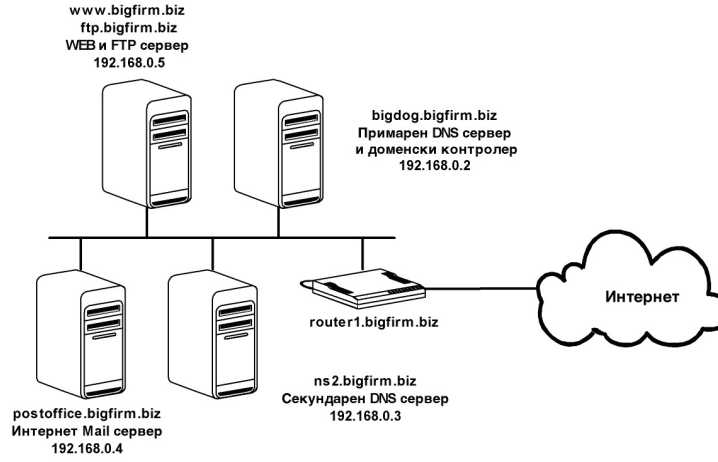


Слика 10.25: Зоната bigfirm.biz, прва верзија

Забележувате дека во десниот панел се прикажани три ставки. Овие ставки се нарекуваат DNS записи (records) - тоа се навистина записи, затоа што се работи за база на податоци - а ќе забележите дека сите ставки се од различен „вид“: тука има еден SOA запис, потоа запис од видот NS, додека третата ставка се нарекува A запис. За што, всушност, се работи тука?

Општ приказ на зоната bigfirm.biz

Сега ќе бидат претставени различните видови на DNS записи, давајќи ви, таму каде што е можно тоа, нивни практични примери во овој фиктивен bigfirm.biz домен. Затоа, замислете дека компанијата Bigfirm поседува сет од серверски компјутери, кои се прикажани на сликата 10.26.



Слика 10.26: bigfirm.biz сервери

Со оглед на тоа што сега ќе започнеме малку посериозно да се однесуваме кон структурата на овој пример, ќе мораме прецизно да ги дефинираме IP адресите. Доменот bigfirm.biz ќе го изградиме под претпоставката дека тој се наоѓа на една нерутабилна мрежа од класата C, со адреса 192.168.0.1.

Постојат само неколку машини, кои се доволно важни за да биде креиран посебен запис во DNS-от за секоја од нив:

- Како што веќе споменавме, би било пожелно да му се даде име на рутерот, кој се наоѓа на адресата 192.168.0.1.
- Mail-серверот за bigfirm.biz претставува машина под име postoffice.bigfirm.biz, на адресата 192.168.0.4.
- Web серверот за bigfirm.biz претставува машина под име www.bigfirm.biz, на адресата 192.168.0.5.
- Истата таа машина, на адресата 192.168.0.5, воедно претставува и FTP сервер, за кој би сакале да одговара на името ftp.bigfirm.biz.
- Машината која има име bigdog.bigfirm.biz, која веќе ја креиравте, истовремено ќе игра улога и на контролер на доменот (доколку инсталирате AD) и примарен DNS сервер. Ве молиме да и ја доделите статичката IP адреса 192.168.0.2.
- Постои уште еден DNS сервер, под името ns2.bigfirm.biz кој воедно игра улога и на датотечен сервер, а се наоѓа на адресата 192.168.0.3.

Записите што постојат во базата на секој DNS сервер се следните:

- A записи - основните записи на секој DNS кои служат за преведување, т.е. име на компјутер и придружена IP адреса;
- SOA записи - Start of authority, кажуваат кој е примарен DNS за даден домен, e-mail адреса на администраторот и дозволен период на кеширање податоци;
- NS записи - name server, ги дефинираат сите именски сервери за конкретниот домен;
- CNAME записи - алијаси, служат за хостови со повеќе имиња;
- MX записи - содржат име и IP адреса на mail server-от;
- SRV записи - кажуваат кои сервери вршат одреден сервис, на пр. TCP;
- PTR записи - pointers, служат за инверзно преведување - име од дадена IP адреса (обратно од A записите).

Некои важни забелешки во врска со овој пример

Како што веќе нагласивме, на сите овие машини им се доделени адреси од нерутабилниот опсег 192.168.0.0. (Сетете се на она што, во претходните поглавја, го научивте за нерутабилните адреси и преведувањето на мрежните адреси/адресите на портовите). Со тоа се имплицираат неколку работи:

Доколку, при практичното испробување на овој пример, користите неколку сопствени компјутери, тогаш тие не ќе имаат можност за пристап на јавниот Интернет, освен во случај да поседувате рутер од типот NAT/PAT. Едноставно, на секоја машина (односно, на машините) им се доделува една од IP адресите од овој пример, за подмрежна маска се одбира 255.255.255.0, а како адреса на подразбираниот мрежен премин се зема 192.168.0.1. Промената на IP адресата на серверот Bigdog, може да се направи од командна линија со следната наредба:

```
netsh int ip set address local static 192.168.0.2
255.255.255.0 192.168.0.1
```

Од претходните поглавја знаете дека Windows 2000 и сите понови оперативни системи можат да играат улога на NAT рутери, како и дека постои една упростена верзија на NAT рутерот, под име ICS, која може да се конфигурира со помош на само два-три клика на тастерот од глувчето. ICS по default, е дизајниран така што ги користи адресите од опсегот 192.168.0.1-192.168.0.254, што е една од причините заради која во овој пример го употребивме токму овој опсег на IP адреси. Таму каде што на сликата 9.26 е прикажан хардверски рутер, може, значи, слободно да се употреби некој компјутер со Windows 2000 или понов компјутер, во улога на ICS рутер. Во тој случај, неговата IP адреса воопшто не мора да се подесува на 192.168.0.1, бидејќи, со вклучувањето на ICS сервисот, IP адресата на Ethernet картицата на интранет страната на рутерот ќе биде автоматски наместена на 192.168.0.1. Алтернативно, како NAT/PAT рутер може да се употреби некој веќе постоечки рутер на корпорацијата, или специјализираниот рутер на DSL/кабелскиот модем.

Исто така, присетете се дека компјутерите со нерутабилни адреси, кои на Интернет пристапуваат преку некој NAT/PAT рутер како што е ICS, поседуваат способност да иницираат комуникација со јавниот Интернет и компјутерите од јавниот Интернет да можат да одговорат на прашањата поставени од страна на компјутерите со нерутабилни адреси. Тоа практично значи дека овие сервери можат да ги опслужуваат само компјутерите од својата локална 192.168.0.x мрежа. Значи, компјутерите од јавниот Интернет нема да можат да им пристапат, да речеме, на вашите Web или DNS сервери, освен доколку својот NAT/PAT сте го конфигурирале така што, портовите од јасно видливиот рутер се мапирани на конкретните портови на серверските компјутери од мрежата 192.168.0.x. Или доколку поседувате дополнителни, рутабилни IP адреси, кои преку NAT/PAT рутерот можете да им ги доделите на конкретни компјутери од мрежата 192.168.0.x.

11 Литература

[1] Andrew S. Tanenbaum, Computer Networks, Fourth Edition, Prentice Hall, 2003.

[2] Stallings, W.: Data and Computer Communications, 6th ed., Upper Saddle River, NJ: Prentice Hall, 2000.

[3] Kurose, J.F., and Ross, K.W.: Computer Networking: A Top-Down Approach Featuring The Internet, Boston: Addison-Wesley, 2001.

[4] Internetworking Technologies Handbook, Fourth Edition, by Cisco Systems, Inc., Cisco Press, 2003.

[5] Patrick Ciccarelli, Christina Faulkner,Networking Foundations, Sybex, 2004.

[6] Mark Minasi, Mastering Windows Server 2003, Sybex, 2003.

[7] MCSE Training Guide: Networking Essentials, Second Edition, New Riders Publishing, 1998.

[8] Radia Pearlman, Interconnections, Second Edition, Bridges, Routers, Switches and Internetworking Protocols, Addison Wesley.

[9] Youlu Zheng, Shakil Akhtar, Networks for Computer Scientists and Engineers, Oxford University Press, 2002.

[10] Michael J. Martin, Understanding the Network A Practical Guide to Internetworking, New Riders Publishing, 2000.

[11] Gilbert Held, Data Communications Networking Devices: Operation, Utilization and Lan and Wan Internetworking, 4th Edition, 1998.