Глава 7.

СТРУКТУРА И ОРГАНИЗАЦИЯ НА МРЕЖИТЕ

Организацията на мрежите, тяхната структура и предлаганите услуги са въпроси, които са пряко свързани с конкретна компютърна мрежа. Те са еднакво значими, и определящи, както за мрежите от тип WAN и LAN, така и за отделния компютър, който е свързан по някакъв начин към Интернет пространството. В общия случай избора на мрежата като цяло се разглежда в контекста на възможностите на програмното осигуряване, чрез което се управляват всички процеси в рамките на една мрежова свързаност. То не значи единствено свързаност в Интернет, а засяга и всички други въпроси, които имат отношение към услугите, предлагани изобщо в състава на една мрежа.

Структура на мрежите, администриране и управление на услугите предлагани от тях са въпроси, пряко свързани с програмните средства. Единствено чрез програмното осигуряване се дефинират правилата и се регламентират услугите, предлагани в условията на осъществената информационна свързаност. Избраната структура непосредствено определя и набора от използвани програми за управление на мрежите. Така например при управление на услугите за отделния потребител в Интернет се използва един набор от програми и програмни средства, а при свързаност на една локална или глобална мрежа – други. Администрирането, настройката и контрола на осъществената мрежова свързаност за отделния компютър предвижда един набор от програмни средства, а за връзката между отделни мрежи друга. Едни са правилата и средствата за работа в рамките на една локална мрежа и други по-задълбочени, по-сложни и разнообразни са те в състава на свързаност между отделни

мрежи. За определяне на необходимите програмни средства и изясняване на структурата е нужно да се изходи и от основните компоненти, които са включени и изграждат състава на мрежите. Това са краен потребител на мрежовите услуги (компютри и устройства), физическо разстояние между свързаните помежду си компютри, начин на свързване на компютрите и устройствата и архитектура на изградената мрежа.

В контекста на това може да се направи извода, че избраната структура и осъществените в нея апаратни връзки между отделни компютри и устройства в условията на мрежова свързаност са пряко свързани с набора от необходими програмни средства. В общия случай за управление на процесите в условията на една мрежова свързаност се използват, както специализирани програми, така и широко разпространените понастоящем операционни системи за стационарни и мобилни устройства. В тях има заложени функции за изграждане и управление на мрежови структури, в това число отделна свързаност на един потребител, изграждане на затворени домашни мрежи, публични мрежи и затворени офис мрежи. Налице са и специфични средства за управление на мрежи, които са свързани посредством кабели, чрез ефирни безжични мрежи и за мрежи от смесени характер.

Изясняването на структурата на компютърните мрежите е пряко свързано с методите и технологията за адресиране на отделните устройства клиенти на мрежовата свързаност. Чрез тях се определя как се образуват адресите, кои мрежи какви адреси използват, кои са особеностите за отделните групи адреси и т.н. Еднозначното адресиране в мрежите е философия, която позволява да са налице огромно количество устройства. Тези устройства са в състояние свободно да обменят информация помежду си в мрежовата свързаност.

В структурно отношение компютърните мрежи са построени, така, че всеки един компютър или мрежово устройство еднозначно се идентифицира в конкретната мрежа със собствен уникален адрес. Този адрес се нарича IP и това е абревиатура от наименованието на един от протоколите, използвани в Ethernet мрежите. Пълното наименование на протокола е Transmission Control Protocol/ Internet Protocol, или TCP/IP. Към настоящият момент приложение в адресирането на устройствата в състава на компютърните мрежи имат два основни стандарта за IP протокола – това са IPv4 и IPv6. Наричат се IP-версия 4 и IP версия 6. Първият стандарт използва 32 битово двоично число за адресиране на устройствата, а вторият 128 бита. За сега все още масово се използва версията за адресиране IPv4. Вторият стандарт сега навлиза в практиката и се поддържа от всички съвременни потребителски и мрежови операционни системи. Основно предимство на IPv6 е многократно по-големият брой на предоставените IP-адреси, а от там и задоволяване на непрекъснато нарастващата необходимост от тях за компютри, устройства и мрежи в Интернет. Към момента съществуват и двете версии на протоколите. Счита се, че в следващите няколко години те ще продължават да съществуват и да се използват заедно, като първият постепенно ще бъде изместен от IPv6. В протоколите за комуникация има строго дефинирано и еднозначно определено адресно пространство за включените единични компютри и устройства или отделни компютърни мрежи. Контролирането и раздаването на IP-адресите е поверено на световна организация и Интернет доставчици, чиято основна задача е да не допуснат дублиране на представените за свързаност адреси.

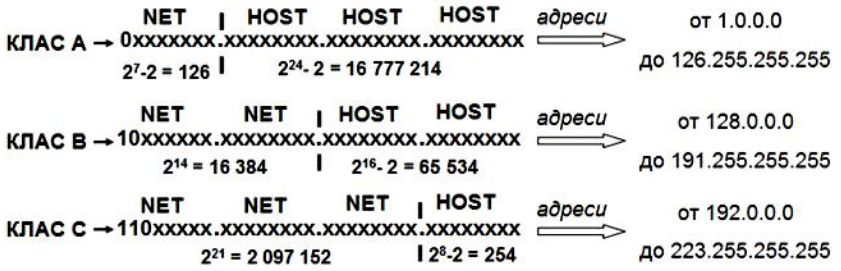
За IPv4 протокола, записът на адресите се състои от четири групи двоични цифри, всяка от които има по осем бита (един байт), или това са общо 32 бита. Теоретично с този протокол могат да се адресират повече от 4 милиарда устройства (2^{32}). На практика, обаче това е доста по-малко, тъй като има ограничения в използването на някои адреси от цялото възможно адресно пространство. Точно това ограничение намалява възможния брой на адресите и то вече осезаемо налага да се премине към новият IPv6 стандарт. Това е така, тъй като броят на устройствата в света, които са абонати на някоя мрежа много бързо нараства и съвсем скоро ще бъде невъзможно със стандарта IPv4 да се отговори на нарастващите нужди.

Структурата на IPv4 адреса е построена така, че определен брой групи от ляво на дясно (старшите байтове) се използват за адресиране на мрежи (NET) в адресното пространство, а останалите в дясно за адресиране на устройства и компютри (HOST). За полесно използване на адресите на потребителско ниво, всяка една от групите двоични цифри се представя с нейната еквивалентна десетична стойност, т.е. това е число, което може да бъде в интервала от 0 до 255. Този начин на записване вече беше засегнат във втора глава на това пособие и той се нарича десетично-точкова нотация. В лявата част на примера, посочен по-долу е записан един адрес от Интернет пространството, който е представен чрез двоично 32-разрядно число. В дясно е неговото изразяване чрез десетично-точкова нотация.

пример: **01010111 11111110 10110110 00010011 –– 87.254.182.19**

Основни класове мрежи са отделно обособените в рамките на протокола адреси. Те определят принадлежността на компютъра или устройството към някаква специфична област. Използването на класове мрежи предоставя по-добри възможности за структуриране на потребителите в рамките на цялото адресно пространство.

В зависимост от групите старши байтове отляво надясно на записа, които са определени и заделени за адресиране на мрежите (NET), в протокола IPv4 се предоставят три основни класа мрежи. Това са мрежите клас A, клас B и клас C и основно те се използват за адресиране на реални устройства. Структурата на адреса определя и обособява още два класа мрежи D и E. Те не се използват за адресиране на реални устройства, включени в състава на мрежите. Тези класове имат специално предназначение. Например адресите от клас D се използват за специално адресиране, а тези от клас E са заделени за експериментални цели. И двата класа не касаят потребителите и няма да бъдат разгледани в пособието. Те по-скоро имат значение за системните администратори, които се занимават в подробности с адресиране и управление на мрежите. Разпределението на адресното пространство при IPv4 протокола в първите три класа – A, B и C е показано схематично на Фиг. 22.



Фиг. 22. *Разпределение на адресното пространство за IPv4.*

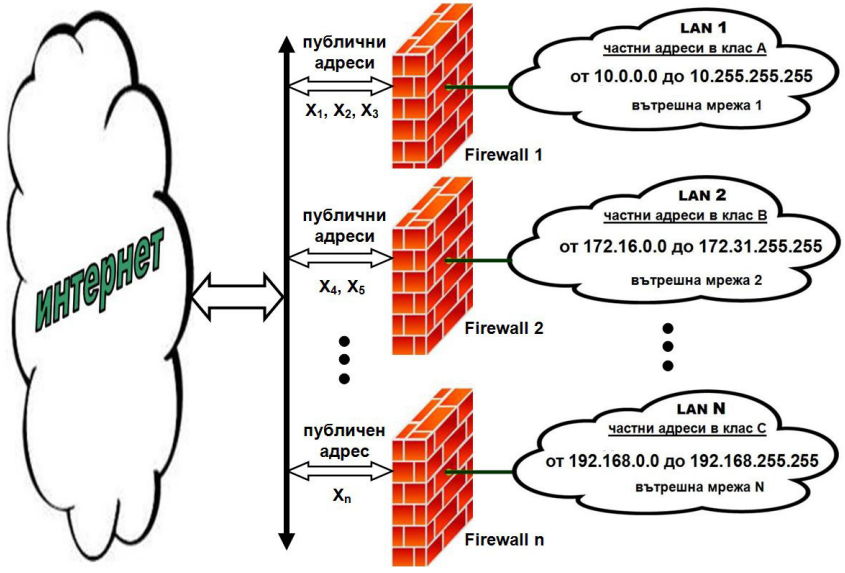
Мрежите от клас A са с адреси, които използват само първия байт за адресиране на мрежа – на схемата е показан с NET. Стойностите на числата тук са от 0 до 126. Това е така, тъй като първият бит на байта за адресиране в клас A винаги е 0. Останалите 3 байта от адреса предоставят 24 бита за адресиране на компютрите и устройствата (HOST) в мрежата от този клас. От това следва, че броят на мрежите в клас A е сравнително малък и фиксира само 126 различни мрежи. За сметка на това пък устройствата във всяка една от адресираните мрежи в този клас е 2^{24}, или това са 16 777 216 различни мрежови устройства. Две от тях са резервирани и не се използват за адресиране на реални устройства. Както се вижда и от схемата, адресите за този клас са от 1.0.0.0 до 126.255.255.255 представени в десетично-точкова нотация. Общият брой на адресираните в клас A устройства е равен на произведението от броя на мрежите NET по броя на устройствата HOST във всяка една от мрежите. Това са точно 2 113 924 216 устройства, т.е. повече от половината устройства, които протокола IPv4 позволява са в клас A. В практиката мрежите от този клас най-често се използва за адресиране на много големи по мащаб мрежи. Това са мрежи от национален характер, големи търговски мрежи, Интернет доставчици и други подобни.

Мрежите от клас B се използват за средно големи национални и регионални организации. При него първите два байта служат за адресиране на мрежата. Особеното тук е, че старшите два бита от първия байт винаги са в стойност 10 и не се променят. От тук следва, че общият брой на мрежите в този клас са 2^{14}, или това са 16 384 различни мрежи. Устройствата в клас B са 2^{16}, което е 65 536, но и тук първият и последният адрес не се използват, което значи, че възможният брой на адресираните устройства е 65 534. Допустимите адреси за този клас са от 128.0.0.0 до 191.255.255.255. Както и в предния клас, общият брой на адресираните устройства е равен на произведението на броя на мрежите 16 384 по устройствата 65 534 във всяка мрежа или това са 1 073 709 056 различни мрежови устройства.

Клас C са мрежи, които се използват от малки организации, при които устройствата са не повече от 254. При този клас адреси, броят на мрежите (NET) е най-голям и за тях се заделят първите три байта от адреса. Особеното тук е, че първите три бита не се използват и винаги са със стойност 110. Следователно общият брой на адресираните различни мрежи в клас C е 2^{11}, или това са 2 097 152 мрежи. Устройствата (HOST) се адресират с един байт или това са 2^8 , което е точно 256. Тук също адресите 0 и 255 не се използват, което означава, че за реално адресиране на устройства остават 254 адреса. Допустимите за използване адреси, както е показано и на фигурата са от 192.0.0.0 до 223.255.255.255. Ако броят на устройствата в една организация е по-голям от 254, то тогава трябва да се използват повече от една мрежа в този клас.

Основни класове адреси са части от цялото адресно пространство във всеки отделен клас мрежа. Те използват отделно обособени адресни области за отделните класове A, B или C. Това са адреси, които представят различни по характер мрежи в общото адресно пространство. Показани са схематично на Фиг. 23, като всеки един от разгледаните преди класове мрежи тук е разделен на два подкласа с отделно обособени в тях адреси. Първият подклас

определя публичните (външни/реални) адреси в Интернет пространството, а вторият частните (вътрешни/нереални) адреси.



Фиг. 23. *Публични и частни адреси в Интернет.*

Вътрешните (частните) адреси понякога наричани и нереални са част от цялостната мрежа, но адресите в тях са затворени и не се разпространяват в Интернет пространството. Те принадлежат на съответния клас мрежи A, B или C, но са затворени и недопустими за Интернет пространството. Тези адреси се присвояват само за нуждите на вътрешна локална мрежа. Недопускането на частните адреси до външното Интернет пространство се контролира от специално програмно осигуряване наричано Firewall (защитна стена). Освен него се използват и други програмни средства за филтриране на вътрешните адреси. Посредством отделените вътрешни адреси в трите класа могат свободно да се планират и изграждат частни локални мрежи. Такъв пример е показан схематично на Фиг. 23. Там са изобразени три вътрешни мрежи, за всяка от които се използват

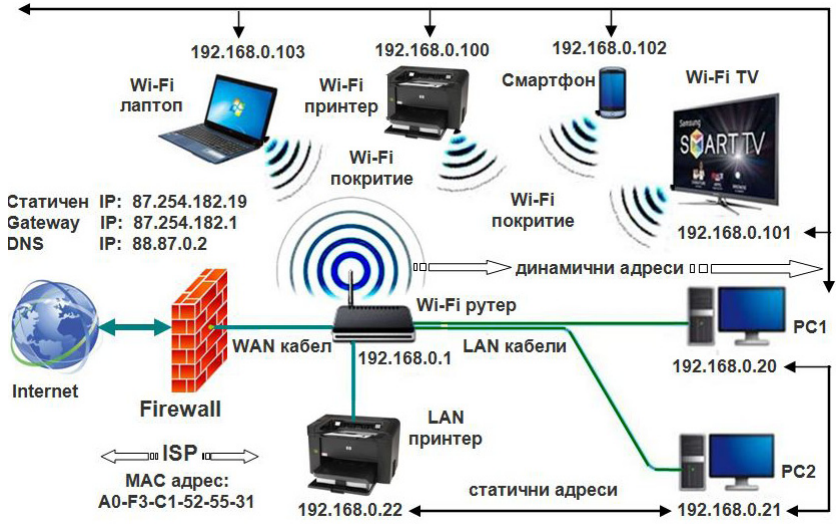
вътрешни адреси. За мрежа LAN 1 частните адреси са от клас A, за мрежа LAN 2 от клас B и за мрежа LAN N от клас C. Както се вижда и от схемата отделеното адресно пространство за тези адреси е както следва:

– за клас A от адрес 10.0.0.0 до адрес 10.255.255.255;
– за клас B от адрес 172.16.0.0 до адрес 172.31.255.255;
– за клас C от адрес 192.168.0.0 до адрес 192.168.255.255;

Външните (публичните) адреси, често наричани и реални, са уникални за цялото световно Интернет пространство на компютърните мрежи. Тези адреси не могат да се дублират, независимо от това къде по света и от какъв потребител или организация се използват те. Раздаването на тези адреси се контролира от организация, управляваща световната система за адреси и домейни ICANN (Internet Corporation for Assigned Names and Numbers). Тази организация поддържа таблица на реалните адреси в Интернет и предоставя такива за използване от потребителите по света. Връзката на вътрешните мрежи с Интернет пространството може да е с един или повече публични адреси. В примера от Фиг. 23 вътрешната мрежа LAN 1 използва три публични адреса – X_1, X_2 и X_3, мрежата LAN 2 е с два публични адреса – X_4 и X_5 и третата мрежа LAN N е с един публичен адрес X_n.

Поддържането на реални адреси се заплаща под формата на абонамент и се включва в месечната такса, която Интернет доставчиците вземат. В практиката публичните адреси обикновено се закупуват на блокове от големи национални и регионални доставчици, които се раздават произволно на по-малки организации, училища, университети, отделни фирми или пък потребители. Нуждаещата се организация, примерно доставчика на Интернет услуги Телнет, подава заявка за блок от IP адреси (netblock) до някоя оторизирана регистрираща организация. Блокът IP съдържа множество адреси, които организацията доставчик разпределя по свое усмотрение на потребителите свързвани към нея. Ако организацията изчерпи адресите от заделеното адресно пространство, то тя подава заявка за друг блок от IP адреси и така до задоволяване на нуждите.

В примера, показан на фиг. 24 е изградена мрежа на малък офис. Тя е свързана към Интернет пространството от доставчика (ISP) посредством специално програмно осигуряване, включващо и Firewall (защитна стена). Публичния адрес, чрез който тази мрежа се свързва в Интернет е само един и е предоставен от доставчика на Интернет, в случая фирма Телнет. Той е от клас A и е 87.254.182.19. Какъв точно е адреса, който е предоставил доставчика за Интернет пространството и е настроил към устройствата в мрежата може лесно да се провери чрез сайта http://www.whatismyip.com. Използването на този сайт е много полезно и



Фиг. 24. *Структурна схема на малка офис мрежа.*

особено в случаите, когато връзката се осъществява посредством рутер, както е в примера, показан на фигурата. В този случай адреса може да бъде открит или посредством статуса на мрежата съобщаван от софтуера на рутера или посредством посочения по-горе сайт. Съществуват и други начини за проверка на IP-адреса, настроен за връзката към Интернет пространството.

Освен разгледаните до тук адресни пространства и тяхното приложение, в практиката са налице и други адреси, които не се използват за адресиране на мрежи и устройства. Това са резервирани адреси и те се използват само за специални цели. Такива адреси са например онези, които съдържат само нули или единици. Резервиран е и адреса 127.0.0.1, който не може да се назначава на мрежи и устройства. С него например може да се тества дали самата мрежова LAN карта работи правилно на локалния компютър. За тази цел, от команден ред трябва да се изпълни командата *ping 127.0.0.1*. Тази команда тества инсталираният протокол TCP/IP на съответния компютър.

В зависимост от това дали назначаваните IP-адреси се променят или не в процеса на работа, те биват два вида – статични и динамични. При това какъв точно адрес ще се използва зависи от направените настройки на мрежите, както от страна на потребителя за вътрешните мрежи, така и от доставчика на Интернет услугата за външните. На Фиг. 24 са показани устройства, които са разделени на две части – едните ползват статични адреси, а другите динамични.

Статичните адреси са уникални за цялото вътрешно и външно Internet пространство. Те са винаги с една и съща стойност и значение и не могат да се дублират с други в рамките на мрежата. Както публичните, така и частните адреси могат да бъдат статични. Дали публичния адрес е статичен се определя от доставчика на услугата и от изричното желание на клиента. Предимствата на статичните адреси са, че те не се променят. Някои услуги ползвани в Интернет мрежите изискват да бъде настроен статичен адрес и това трябва да се има предвид от потребителите. В примера от Фиг. 24, зададеният от ISP публичен адрес (87.254.182.19) е статичен. Адресите във вътрешната мрежа от същия пример се определят от потребителя. Това става от програмното осигуряване на операционната система. Чрез него за една част от устройствата са зададени статични IP адреси. Това е мрежовият принтер с адрес 192.168.0.22 и двата десктоп компютри, които са съответно с адреси 20 и 21 в същата мрежа.

Динамични са адресите, които се присвояват в рамките на една локална или външна мрежа. Тези адреси също могат да се определят от доставчика или от администратора на частната мрежа. Характерното за тези адреси е, че те не са постоянни и могат да се променят в рамките на адресираните устройства (HOST). Това не се отнася за адресната част на мрежата (NET), там адресите са постоянни и не се променят. За определяне и назначаване на динамичните адреси се използва специално програмно осигуряване, наричано DHCP сървър (Dynamic Host Configuration Protocol). Посредством него се дефинира област от адреси, които се избират и се назначават динамично на устройствата. В примера от Фиг. 24 една част от устройствата са дефинирани с динамични адреси и те се определят от DHCP на рутера.

Разгледаните до тук адреси имат много съществено значение при изграждане на мрежите. Публичните адреси винаги се предоставят от ISP (доставчика) на услугата и не могат да се променят от потребителя. Частните адреси са задължение на клиента и той се грижи за тяхното разпределение, настройване и контрол. Динамичните и статичните адреси в конкретна мрежа се определят при администриране на мрежата. Изобщо всички настройки в една мрежа, регионална или локална са пряко свързани с нейното предназначение и те се осъществяват при нейното конфигуриране.

Конфигуриране на мрежите, са дейности извършвани от специалисти или потребители на мрежови услуги. Те са втората задължителна стъпка след хардуерното изграждане на мрежовата структура. Достъпни и изпълнявани са с помощта на специализирани или широко разпространени програмни средства, например ОС.

Специализираните програмни средства са мрежовите операционни системи и всички онези програми, които засягат управлението и администрацията на мрежите. Те се използват основно от специалисти и администратори на мрежите. Работата с тях е доста сложна и те рядко касаят широкия потребител.

Популярните операционни системи, в състава на които има заложени модули за управление и мрежови функции са операционните системи на Майкрософт – Windows за персонални компютри и Windows Phone за мобилни устройства. С множество мрежови възможности са също операционните системи MAC OS за персонални компютри на Apple MAC и iOS за мобилните устройства на тази фирма. Вградени функции за управление на мрежови възможности и конфигуриране има и в други устройства със заложени в тях мрежови функции. Това например са широко популярните смартфони с операционна система на Google – Android, устройства с операционна система Simbian, Linux базирани операционни системи за Nokia и други. Налице са и специализирани програмни модули, които под формата на драйвери се предлагат в състава на устройства с мрежови функции. Това е програмното осигуряване на рутерите за малки домашни и офис мрежи, драйверите за мрежовите принтери, телевизори със заложени в тях мрежови функции и други.

С голямо приложение при конфигуриране и обслужване на мрежите са и програми представяни като модули в операционните системи, чрез които може да се прави достъп до Интернет адреси. Тези програми се наричат браузери. Браузерът, предлаган към Windows е Internet Explorer, а в операционните системи на Apple той се нарича Safari. Браузери за управление на услуги в мрежите са също отделно обособените програми като Opera, Mozilla, Firefox и др.

За изясняване на отделни дейности по конфигуриране на мрежите ще се използва конкретен пример. Той е изразен схематично на Фиг. 24 и там са показани различни устройства, свързани в компютърна мрежа. Тя е с малък брой на устройствата в нея и представя нуждите и особеностите на домашна или малка офис мрежа.

В основата на мрежата (Фиг. 24) е безжичен рутер (Wi-Fi рутер), чрез който се осъществява връзката към Интернет. Информационния трафик в тази връзка се осигурява от доставчик на мрежови услуги (ISP). Безжичният рутер е свързан апаратно с доставчика посредством стандартен UTP (WAN кабел). От едната страна кабелът е включен към порт от устройството за достъп до Интернет. То

е собственост на доставчика на услугата (най-често суич) и се управлява от него. От другата страна на кабелната връзка е включен порта на рутера, означен с WAN. Рутерите имат такъв порт и чрез него се реализира физическата връзка с мрежата на доставчика. За връзката към Интернет в този пример ISP е предоставил статичен публичен адрес 87.254.182.19. Контрола на достъпа се осъществява от програмното осигуряване на доставчика посредством уникалния MAC адрес на рутера – в примера той е A0-73-C1-52-55-31.

Устройствата в показаната локална мрежа се свързват към рутера, като са реализирани двата способа за достъп – безжичен и кабелен. За кабелната връзка са използвани LAN портовете на рутера, които за този тип малки офис рутери те са обикновено четири. Към тях, чрез стандартни LAN кабели (UTP) са свързани двата стационарни (десктоп) компютъра PC1 и PC2 и мрежовият принтер (LAN принтер). Другите устройства, абонати на тази локална мрежа използват безжична връзка. Те са разположени в зоната на Wi-Fi покритието, осигурявано от безжичния Wi-Fi рутер. Устройствата в примера, които ползват безжичната връзка са мобилен компютър (Wi-Fi лаптоп), безжичен принтер (Wi-Fi принтер), смартфон и телевизионен приемник с вградени функции за работа в Интернет (Wi-Fi TV)

Използването на безжични рутери, както е показано в примера на Фиг. 24 е много популярно. Тези устройства са сравнително евтини (от 30 до към 100 лева, има и по-скъпи), осигуряват добри скорости на обмен 150, 300 и повече Mbps, и лесно се конфигурират. Имат вградено програмно осигуряване с доста функции за обслужване, защита и контрол. От друга страна те покриват и голям диапазон от функции за работа в условията на локална мрежа с Интернет доставка. Наличието в тях на безжични функции предоставя много голяма гъвкавост при свързване на широко разпространените вече смартфони, таблети, безжични мобилни компютри, телевизори и други.

Първата стъпка в конфигурирането на показаната малка офис или домашна локална мрежа е свързана с настройване на параметри-

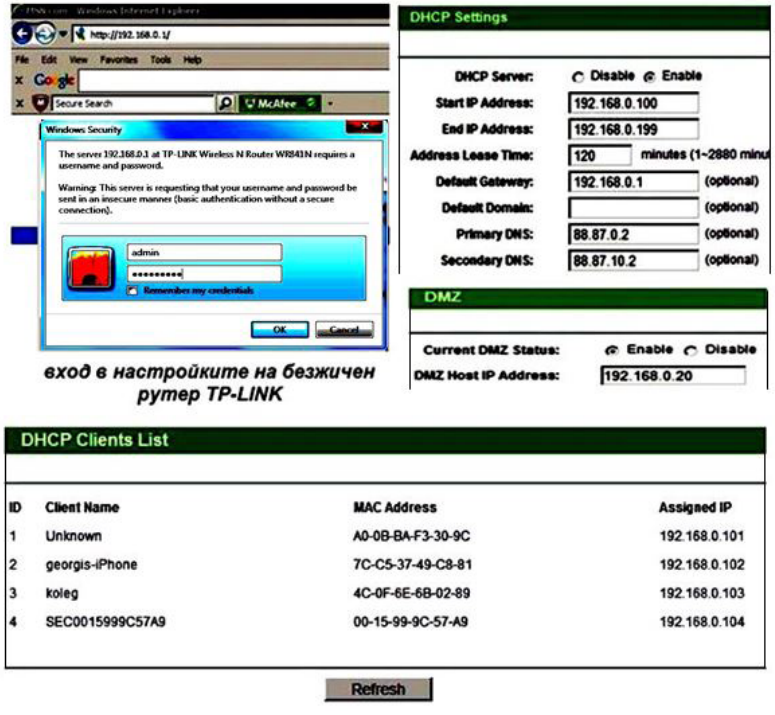
те на рутера за връзка. В практиката това обикновено се извършва от доставчика, който в повечето от случаите има и дистанционен достъп до устройството за връзка при клиента. Програмното осигуряване на рутера, което се използва за конфигуриране и настройка е защитено с потребителско име и парола за достъп. Входът към него най-често се осъществява чрез IP адрес 192.168.0.1, записан в адресната лента на стартиран браузер. При някои модели рутери това може да бъде и адрес 192.168.1.1, който също се въвежда чрез браузер.

След избора на адреса за достъп ще се отвори диалогов прозорец и чрез него ще бъдат поискани потребителско име и парола за достъп. На Фиг. 25 са показани примерни диалогови прозорци, които са специфични за вграденото програмно осигуряване на широко разпространените рутери от модел TP-LINK. За други модели рутери или за друго програмно осигуряване диалоговите прозорци са различни от показаните тук, но елементите в тях и предлаганите настройки са подобни на тези от моделите на TP-LINK.

Чрез диалоговия прозорец, горе вляво на фигурата се въвеждат потребителското име и паролата за достъп. Те трябва да се знаят от лицата, които предвиждат достъп до рутера. При загуба на тези параметри програмното осигуряване на устройството трябва да се „нулира“ и всички настройки да се направят отново. При нулирано програмно осигуряване се назначават служебни параметри за потребителско име и парола, които са обявени в описанието на рутера.

След въвеждане на валидно потребителско име и парола, ще се появи меню-системата на софтуера за управление на рутера. Това е система от менюта, всяко едно от които има достъп до определени функции за конфигуриране. Например чрез менюто *DHCP Settings* показано горе вдясно на фиг. 25, се настройват правилата за генериране на динамичните адреси за устройствата в мрежата. В примера е зададен диапазон на изменение на генерираните адреси от 192.168.0.100 до 192.168.0.199. На същата фигура, долу е изведена справката, предлагана от меню *DHCP Clients List*. Тя показва кои устройства в момента са активни в мрежата, кои са им MAC

адресите на мрежовите карти и какви IP адреси е получило всяко устройство.

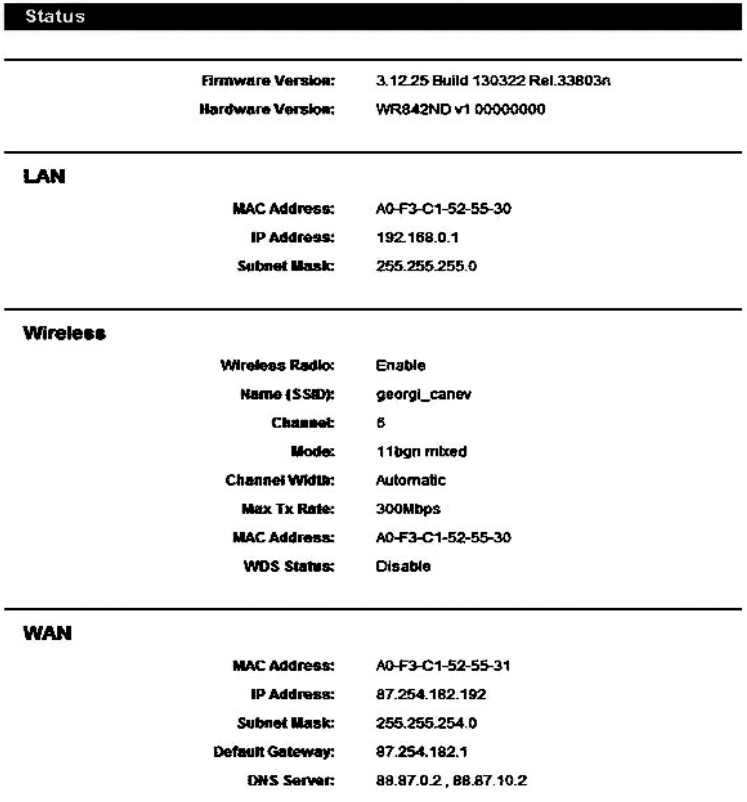


Фиг. 25. *Конфигуриране на мрежа чрез безжичен рутер.*

Менюто *DMZ*, показано на същата фигура намира доста често приложение в практиката. То се активира посредством секцията *Forwarding* от меню системата на рутера. Чрез него може да се определи зона за свободен достъп от Интернет мрежите до определен компютър от вътрешната мрежа. Нарича се „Демитализирана зона“, управлява се от показаното меню и позволява да се въведе статичен адрес на компютър от вътрешната мрежа. Компютърът, чиито адрес се запише в тази зона (в примера това е 192.168.0.20) и се включи опцията „*Enable*“ ще бъде достъпен за всички външни услуги – например услугата отдалечен достъп (RDC – Remote

Desktop Connection) от външни за мрежата компютри (ще бъде разгледана по-нататък).

Поставянето на компютър от вътрешна мрежа в демитализираната (DMZ) зона носи рискове за сигурността на информацията върху него. В този случай се заобикаля защитната стена (Firewall), изградена от софтуера на рутера и достъпът до компютъра остава неконтролиран. В практиката това понякога е наложително, защото има услуги, които го налагат. Много често, вместо демитализираната зона (DMZ), достъпна от меню „Forwarding“, се конфигурира така наречения виртуален сървър. Това може да се извърши, чрез меню „Virtual Server“ (не е показано в примера на схемата). В този



Фиг. 26. *Списък на най-съществените настройки на рутер.*

случай, вместо пълен достъп, се разрешава само конкретната информационна услуга за външни на мрежата компютри.

От информацията, която може да бъде осигурена чрез софтуера на рутера, най-голямо значение и приложение в практиката на потребителите има таблицата, показана на фиг. 26. В нея се съдържат всички параметри, свързани със статуса на конфигурираната вътрешна мрежа. За рутерите на TP-LINK, които са със стандартното си програмно осигуряване, таблицата може да бъде изведена в диалогов прозорец, чрез меню „*Status*“. Тя има видът показан на фигурата и е препоръчително всеки потребител да си я има като разпечатка и да я запази. От нея, по всяко време може да се видят текущо направените настройки и всички важни параметри на вътрешната локална мрежа. Ако справката не е по силите на потребителя на мрежата, то той може да поиска това да го направи доставчика на услугата.

Чрез справката се виждат всички характерни адреси, чрез които вътрешната мрежа се свързва с доставчика на Интернет. Там е MAC адреса на мрежовата карта на рутера, чрез който се осъществява контролът от доставчика, IP адреса предоставен за тази мрежа (87.254.182.192), адреса на шлюза (Gateway) за достъп до Интернет (87.254.182.1), осигурен от ISP и адреса на сървъра за преобразуване на Интернет имена (DNS), в примера 88.87.0.2.

Справките от другите секции на това меню са за локалната мрежа (LAN), като в примера това са частни адреси в мрежови сегмент с начален адрес 192.168.0.1. Безжичната мрежа (Wireless) е с идентификатор на „Точката за достъп“ (SIID) „georgi_canev“. Скоростта за достъп на безжичните устройства в тази мрежа е до 300 Mbps.

При изграждане на вътрешни мрежи чрез дискутирания по-горе пример са възможни редица особености. Често те са свързани с конкретни настройки, решаването на които в повече от случаи е от компетенциите на специалисти. Понякога при работата с мрежите може да се случи и пропадане на връзката с доставчика – „забиване на рутера“. Трябва да се знае, че не винаги това се дължи на

технически причини, а просто временно състояние, произтекло от връзката на мрежовите устройства. В такива случаи, преди да се потърси техническа помощ, е добре да се рестартира рутера. Най-лесният начин за рестартирането е да се изключи за няколко секунди захранването на рутера и да се включи отново. Ако връзката се възстанови, то това вероятно е било временно състояние, а не техническа причина. В случаите, когато забиванията са чести, то тогава трябва да се потърси техническа помощ от ISP.

Независимо от това каква услуга ще се използва, то винаги е налице компонент от нея, който е пряко свързан с адрес на компютър или общност от компютри. Адресите вече бяха разгледани и стана ясно, че представени в цифров вид те много трудно се запомнят и прекалено сложно се работи с тях. Ако все пак някъде се използва цифровото представяне, то това ще касае основно специалистите, които инсталират и поддържат мрежата и мрежовите услуги. На потребителско ниво компютри, устройства или обособени групи от компютри също се идентифицират с уникалните си адреси, но за по-лесно използване и боравене се използват не числовите им изрази, а техен еквивалент под формата на логически адреси.

Логически адреси в Интернет са онези записи, които представляват еквивалент на цифровите IP адреси. Те се образуват на базата на строго определени правила. Логически адрес има всеки компютър или множество от компютри обединени по общи функционални или информационни критерии. Логически адрес има също всяка информационна структура, в това число отделно обособен сайт или конкретна Интернет страница. Няма как да се направи достъп до Интернет сайт, ако той няма уникален адрес и не е поместен на свързан към Интернет компютър. В общия случай всичко, до което може да се направи достъп в Интернет притежава свой уникален IP идентификатор и свързан с него логически адрес.

Прието е уникалните логически адреси, които обединяват компютри и информационни структури в отделно обособени единици да се наричат домейни. Понятието домейн (domain) означава общ-

ност или област и чрез него се идентифицират свързани по някакъв признак структури, обединени под общото име на конкретния домейн. Домейните са въведени с цел по-лесно и по-разбираемо да се работи с IP адресите на информационните структури в Интернет. Преобразуването на числовите IP адреси в логически (домейни) и обратно се осъществява посредством специално програмно осигуряван. То се нарича DNS (Domain Name Server) и се разполага върху компютри на доставчиците на Интернет услуги (ISP). Върху сървъри се разполага и информацията за IP адресите и тяхното съответствие с назначените им логически имена.

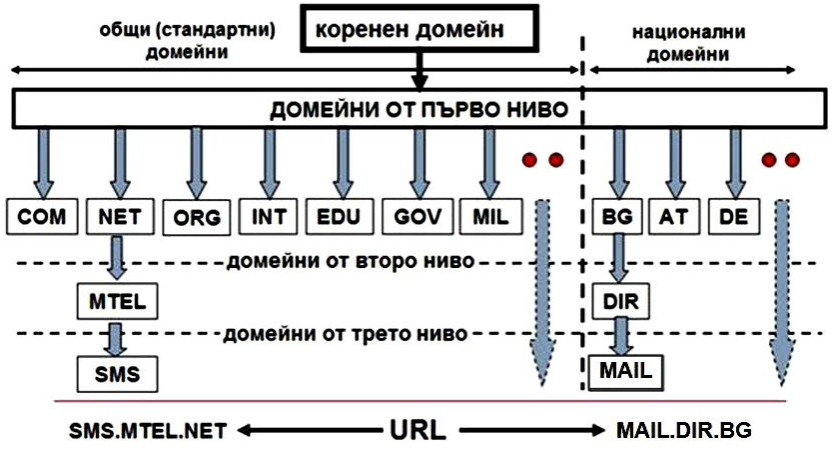
Цялостната система за имена на домейни DNS (Domain Name Sistem) на практика представлява дървовидна структура от свързани помежду си логически адреси. Структурата е уникална за цялото Интернет пространство и се контролира от корпорация с нестопанска цел ICANN (Internet Corporation for Assigned Names and Numbers). Корпорация е базирана основно в САЩ, но има клонове и в други страни по света. Основна задача на ICANN е да стандартизира логическите имена на домейните и да не допусне те да се повтарят. На базата на възприетата структура за имената на домейните всеки логически адрес в Интернет има следният вид:

отдел.организация.висш домейн

Прието е представеният по този начин уникален адрес в Глобалното пространството да се нарича URL (Uniform Recurs Locate). Той се състои от коренен домейн, домейни от първо ниво (висши домейни) и поддомейни от по-ниско ниво – второ, трето и т.н. Името на коренния домейн в структурата е условно и се означава с точка. Всички други имена на домейни, включени в логическия адрес се отделят едно от друго също с точка. Примерна структура за изграждане системата за имена на домейните е показана на фиг. 27.

Домейните от първо ниво (*висшите домейни)* са от особено значение в структурата на Интернет адресите. Те се наричат още TLD (Top Level Domain) или „глобални“ и са строго стандартизи-

рани. Тези домейни са ограничени по количество и имат фиксирани имена. Имената им се записват в най-дясната част от структурата на URL адреса и се определят от корпорацията ICANN и структурите по света управлявани от нея.



Фиг. 27. *Организация на домейните в Интернет мрежата.*

Използването на един или друг домейн от първо ниво е свързано с определена процедура, която много прилича на абонаментна услуга, за която се заплаща такса. Клиентите на домейните от първо ниво заявяват това пред организации наричани регистратори, които от своя страна определят името и срока за валидност на домейна. Правата за ползване на домейните от първо ниво са свързани със заплащане на определена такса. Абонаментите най-често се вземат за една година, след изтичането на която следва да се заплати нова такса и абонамента да се поднови. Някои регистриращи организации предлагат и по-дълг срок за регистриране, например три или повече години, като при по-дългия срок таксата е по-малка. Домейните от първо ниво се разглеждат в два основни класа – общи и национални.

Общите домейни gTLD (generic Top-Level Domains) от първо ниво най-често са от три букви, но вече има и с повече. Като изключение може да се счита и домейна от първо ниво на Европейския съюз, който пък е само с две букви (EU). Идеята за създаването на домейните от първо ниво е възникнала още в средата на осемдесетте години. Първоначално са били създадени само седем, като впоследствие техният брой е нараствал, за да се стигне към днешно време до няколко десетки. Общите домейни са избирани и създавани така, че да представят отделни направления и дейности, например търговия, образование и т.н. Най-често използваните от тях са:

– COM – Името на този домейн произлиза от думата Commercial (Търговски) и това може би е най-често използвания в Интернет пространството домейн. Създаден е още през 1985 год. и до момента регистрираните в него адреси са десетки милиони. Домейна обединява компютри с търговска цел, но в последно време в него се регистрират и всякакъв вид други организации, в това число и лични Интернет страници. Таксата за регистриране в този домейн е относително по-висока в сравнение с другите общи домейни.
– NET – Домейнът е създаден с идеята да обедини организации и компютри, чиито дейности са насочени основно в областта на информационните технологии. Името му е заимствано от Network (Мрежа) и към момента той се ползва масово, тъй като е подходящ за всякакви приложения. Почти всички структури и организации, които работят в глобалната мрежа, включително Интернет доставчици (ISP), телекомунакационни компании, кабелни оператори и други предпочитат да използват този домейн. Предвид на голямата си популярност и отсъствието на ограничения при регистрирането, домейна NET е смятан за следващия по значимост след COM.

– ORG – Името на домейна се образува от първите три букви на думата Organization (Организация). Той попада в състава на първите седем домейна и обединява общности от компютри и мрежи с неправителствена цел. Първоначалният замисъл при създаването на домейна е бил той да се използва само от организации, които не покриват изискванията за регистрация в другите домейни от първо ниво. С течение на годините това правило не спазвано и сега всеки клиент може да регистрира свой адрес в ORG домейна. В него е регистрирана и световната Интернет енциклопедия – Wikipedia (Уикипедия).
– INT – Домейнът е създаден с цел да позволи регистрация за организации, които представляват международни структури. В него могат да се регистрират и общности, които са създадени по силата на междуправителствени договорености. Името на домейна се образува от първите три букви на думата International (Интернационални). Той е освободен от такса, но за регистрирането в него се определят редица условия, на които клиента трябва да отговаря. INT не е много популярен и рядко се среща, макар да е от първите седем домейна.
– EDU – В този домейн се регистрират основно образователни институции от САЩ. Името му е образувано от първите три букви на думата Educational (Образователен) и това е също един от първите създадени домейни в средата на осемдесетте години. В него са регистрирани редица престижни университети в света, като Харвардския университет в САЩ (harvard.edu), Масачузетския технологичен институт (mit.edu) и други. Понастоящем не може да се счита, че има специфични ограничения, които да са спънка за регистриране в този домейн и на други институции по света.
– GOV – Домейна влиза в списъка на първите седем регистрирани и е ориентиран основно към правителствени институции от САЩ. Така например официалната страници на Белия дом (whitehouse.gov) е точно в домейна GOV. За регистрирането в този домейн трябва да са налице редици предявявани изисквания. Името GOV е образувано от първите три букви на думата Government (Правителство). Няма данни този домейн да се предоставя и за други потребители и абонати, които са извън правителствените структури на САЩ.
– MIL – Домейна принадлежи на военни структури от САЩ и не се предоставя на други организации. Името му произлиза от думата Military (Военен). Официалните сайтове на въоръжените сили на САЩ като Американската армия (army.mil), Морската пехота (marines.mil), Военновъздушните сили на щатите (af.mil) и други са регистрирани в този домейн. Той е също от първите седем домейна.

Освен посочените по-горе общи домейни са налице и редица други. Така например първоначално основната генерация на общите домейни е била разширена през 2001 година с още седем, сред които са INFO и BIZ. Домейна INFO (от Information) се оказва доста сполучлив и освободен от всякакъв вид ограничения. Това позволява за кратко време в него да се появят милиони сайтове. В този домейн може да се регистрират всякакъв вид организации и структури, включително и лични страници. По същият начин стои и въпросът с домейна BIZ. Неговото име е заимствано от думата Business, но той не е толкова разпространен както разгледаните до тук домейни.

В последните няколко години ICANN обяви и поредици от домейни на първо ниво, някои от които вече са и на кирилица. Така стои и въпроса с домейна на Европейския съюз, който за разлика от другите домейни е с две букви – EU. Този домейн е регистриран след одобрение от ICANN през 2005 година. Предназначен е за структури и организации на Европейския съюз и в началото е налагал определени условия, на които трябва да отговарят клиентите за него.

Така например, веднага след регистрирането му се е изисквало от желаещите да доказват документално правото за собственост върху избраното име в този домейн, като например търговска марка, име на фирма, обект с географско разположение в Европейския съюз и други подобни. Малко по-късно ограниченията са премахнати и са сведени единствено до посочването на валиден адрес в страна от Европейския съюз. Това на практика го прави почти напълно свободен домейн и в него вече има регистрирани повече от милион сайта. Към настоящия момент домейнът EU се предоставя и контролира от организацията с нестопанска цел EURID (European Registry of Internet Domain Names). Официалният сайт на организацията (www.eurid.eu/) предоставя информация относно условията за регистриране на имена на домейни на всички официални езици в Европейския съюз. Там се предоставя и сведение за оторизираните регистратори в този домейн за различните страни от ЕС и извън него.

Към настоящия момент одобрените от ICANN домейни от първо ниво наброяват няколко десетки, като тенденцията е те непрекъснато да нарастват. Мнението на редица анализатори е, че непрекъснатото нарастване на домейните от първо ниво води до усложняване на цялостната система за домейните. Счита се, че колкото повече нараства списъкът с общите домейни от първо ниво, толкова повече се увеличават и рисковете при използването на именната система.

Националните домейни от първо ниво са втората група на висшите домейни. Те са създадени с основната си цел да представят отделните държави по света в Интернет пространството. Наричат се още ccTLD (country-code Top-Level Domains) домейни и се състоят само от две букви. Например за домейна от първо ниво, определен за България се използва името .bg, за Австрия .at, за Германия .de, за Русия .ru и т.н. Регистрирането в тези домейни се извършва от регистратори, които са организации оторизирани от ICANN. Те определят правилата, цените и условията за избор на име и поддържането му тези домейни. За България, оторизираният регистратор на имена в домейна от първо ниво .bg е фирмата „Ре-

гистър.БГ“. На нейният официален сайт (www.register.bg/) може да се намери подробна информация относно условията и правилата за регистриране на домейни в тази област. Цената за регистриране в домейна .bg е по-висока от другите, но той е предпочитан от български институции, фирми и организации и е считан за престижен и представителен.

Домейните от второ ниво са всички, които са разположени непосредствено под висшите домейни в дървовидната структура. Те се определят от конкретните нужди на съответния клиент и името се избира от него. Името трябва да е уникално и да не се повтаря в Интернет пространството на URL адресите. Освен това има и изисквания към възможните символи, които могат да се включват в името. Поддръжката на домейните се осъществява от съответните регистратори и е свързано с определена такса – нещо като годишен абонамент. Като пример за URL адрес, регистриран в националния домейн от първо ниво на България може да се посочи този на Медицински университет – Плевен. Името на домейна е избрано mupleven и то е от второ ниво в домейна .bg, т.е. mu-pleven.bg. Това е логическият URL адрес, а физическият IP адрес е 194.141.67.7.

Какъв физически IP адрес отговаря на конкретен логически адрес може да се провери, като от команден ред се въведе команда *ping* – например *ping mu-pleven.bg***.** За прехода към команден ред от главното меню се въвежда команда *cmd* след което бутон *Enter*.

За обратната операция, чрез която може да се установи на какъв физически IP адрес отговаря зададен логически адрес има различни способи. Един от тях е да се ползват услугите на различни сайтове, които предлагат тази възможност. Такъв сайт например има на Интернет адрес http://www.dazzlepod.com/ip/. След въвеждането на този адрес в произволен браузер, ще се отвори страница, в която може да се въведе физическия IP и да се получи желаната информация. Информацията, предоставена от сайта е доста изчерпателна и полезна.

Домейните от трето и по-ниско ниво се разполагат непосредствено под висшите домейни. Техните имена се определят произ-

волно от собственика им и сочат сайт, който е разположен в основния сайт и е достъпен чрез него. По този начин в един домейн могат да се разполагат множество поддомейни, които на практика представляват различни сайтове. Адресирането им се осъществява чрез изписване на техните имена, разделени помежду си с точка. В примера от фиг. 27 е показан домейн от трето ниво MAIL, който е разположен в домейна DIR и е достъпен чрез него. Той, от своя страна е регистриран в домейна от първо ниво *.bg*.

Информационното съдържание на домейна може да бъде разположено на всеки компютър, който има реален IP адрес в Интернет пространството. Прието е този компютър на който се намира домейна да се нарича Host, а поддържането на информацията за него – хостване. Компютърът (сървъра) където се намира сайта може да бъде собствен на организацията, която е регистрирала домейна. Той може да бъде и друга собственост, като за услугата хостване обикновено се заплаща определена такса. Често таксата за хостване на сайтове представлява услуга в Интернет мрежите, която се включва и в таксата за поддържането на домейна от първо ниво. Има и услуги в Интернет, които предлагат безплатно хостване на сайтове. Там е достатъчно да се спазват някои правила, които се налагат от предоставящия тази услуга. В този случай, обаче са налице редица ограничения, като обем на сайта, време за хостване, нежелани реклами и други.