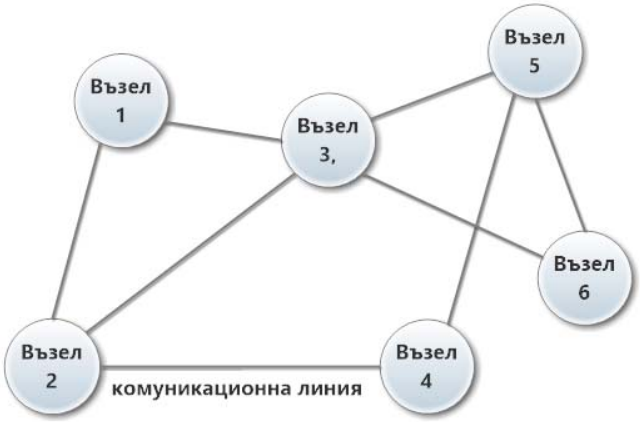
1. Локални и глобални компютърни мрежи. Услуги

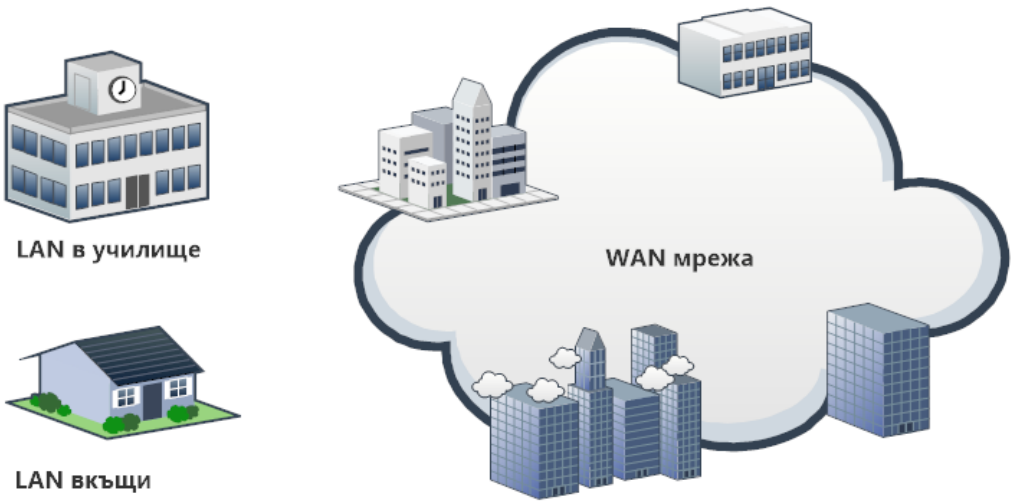
1.1.Компютърни мрежи

Мрежата е технология, позволяваща на независими устройства с възможност за комуникация да се свързват помежду си или да използват общи ресурси. Когато тези устройства са компютри, мрежата се нарича компютърна. Ако трябва да се направи съвсем прост примерен модел на мрежа, той би изглеждал като този от фигура 1, където кръговете се наричат **възли**, а свързващите линии – **комуникационни линии** (наричани още **преносни** или **съобщителни среди**).



фигура 1 *Прост примерен модел на мрежа*

В съвременното ежедневие е немислимо използването на компютъра като самостоятелна единица. Компютърната мрежа намира приложение навсякъде: в бизнеса, в обучението, в домакинството. В зависимост от обхванатата физическа област (фигура 2), могат ясно да се разграничат два основни типа мрежи: локална (LAN, Local Area Network) и глобална (WAN, Wide Area Network). **Локалната компютърна мрежа** обикновено се разполага на територията на стая, сграда или между няколко помещения, разположени на близко разстояние. **Глобалната компютърна мрежа** покрива голяма географска област. Тя осъществява свързаност между точки (LAN мрежи или отделни устройства), която LAN технологията не може да реализира. WAN използва телефонни линии, специални опорни мрежи или сателитна технология за свързване на компютри в различни градове, държави и континенти. Пример за такъв тип мрежа е Интернет.



фигура 2 *Локална (LAN) и глобална (WAN) мрежа*

1.2.Предимства и недостатъци на компютърните мрежи

Използването на дадена технология в повечето случаи е свързано с извличането на ползите от нея. Подобен е случая с компютърните мрежи, които предоставят предимства, като:

- Осигуряване на общи ресурси с цел, споделяне или намаляване на разходите за скъп хардуер. Такъв тип ресурси могат да бъдат процесорно време, дискова памет, файлове и входно-изходни устройства;
- Повишаване на ефективността на сравнително непроизводителни компютри. Например използване на процесорно време на друг компютър, повече дискова памет от сървър;
- Възможност за използване на общи бази от данни и системи за съхранение;
- Колективна работа при разработването на проекти в група;
- Възможност за електронна комуникация и обучение;
- Възможност за свързване към други LAN/WAN.

Една компютърна мрежа, в която работят съвместно различни устройства и потребители, притежава и недостатъци. Като такива могат да бъдат посочени:

- Уязвимост на мрежовата инфраструктура – всички устройства, изграждащи мрежата могат да бъдат обект на атака от нежелани потребители;

- Социални проблеми, свързани с разпространяването на нецензурирана информация и лъжи;
- Претоварване на мрежата, което може да бъде с локален характер (в някаква част от нея) или глобален характер (по всичките ѝ части), намаляващо нейната ефективност или причиняващо нейната неработоспособност;
- Технически проблеми с участващите устройства, което може да предизвика прекъсване на свързаността между отделните компютри.

1.3. Мрежови топологии

Локалните и глобалните компютърни мрежи поддържат различни видове физически топологии. **Физическата топология** (physical topology) указва физическото разположение на участващите устройства (възли) и използваната система от кабели (комуникационни линии). Обикновено този тип топология се нарича още **мрежова топология**. Съществува и друг вид топология, наречена **логическата топология** (logical topology), която се определя от начина на предаване на сигналите между устройствата, независимо от тяхното физическо разположение. При реализирането на една компютърна мрежа са налични и двата вида топологии.

Според функциите, които изпълняват възлите в една мрежа могат да бъдат междинни и крайни мрежови възли. **Междинните възли** осигуряват правилното функциониране на мрежата. Към **крайните възли** могат да бъдат причислени работните станции и сървърите. Под работна станция се разбира произволен компютър или терминал, чрез който се осъществява достъп до желан ресурс в мрежата. В този случай работната станция се явява **клиент**. **Сървърът** е този, който предлага желаните ресурси в мрежата под формата на така наречените **мрежови услуги**. Той представлява приложен процес (програма), реализиращ дадена услуга. Трябва да се отбележи, че е възможно един компютър да обслужва няколко сървъра едновременно, стига да не се натоварва прекалено компютърната система. Като примери за често използвани сървъри могат да се посочат следните видове:

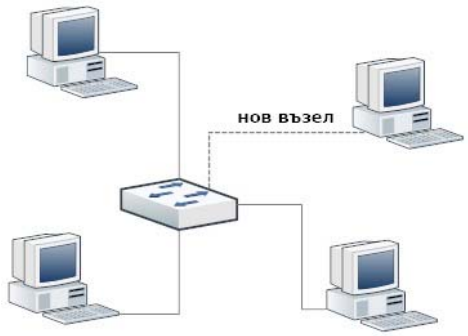
- **Файлов сървър** – програма, позволяваща достъп до файловата система на компютъра за съхранение и извличане на файлове и програми;

- **Сървър за печат** – програма, осигуряваща достъп до принтера на компютъра, на който е стартирана;
- **Сървър за електронна поща –** програма, управляваща електронните пощенски кутии на потребителите;
- **WEB сървър –** програма, предоставяща информация на клиент под формата на HTML документ.

1.3.1. Популярни мрежови топологии в LAN

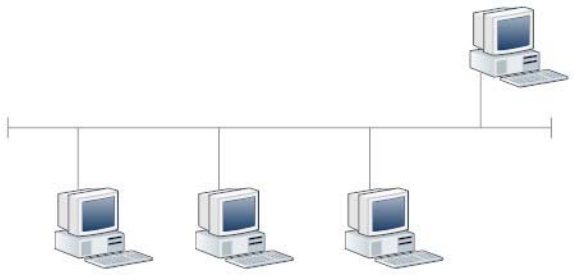
Като най-популярни физически топологии в LAN могат да се посочат следните:

- Топология тип „звезда“ (star)– крайните мрежови възли (работни станции, сървъри) са свързани към централен възел във вид на звезда (фигура 3). Позволява лесно добавяне на нов възел. Повреда в централния възел предизвиква разпад на мрежата. В момента това е актуалната мрежова топология за изграждане на локална компютърна мрежа.



фигура 3 *Тип звезда*

- Топология тип „пасивна шина“ (passive bus) – един кабел (наречен още шина) за данни, към която са свързани отделните мрежови възли (фигура 4). Сравнително евтина и позволява лесно добавяне на нов възел. Повреда на един възел не указва влияние върху другите. Като недостатъци могат да се посочат: ограничено покритие; слаба диагностика на мрежата; прекъсване на шината води до разпадане на мрежата.

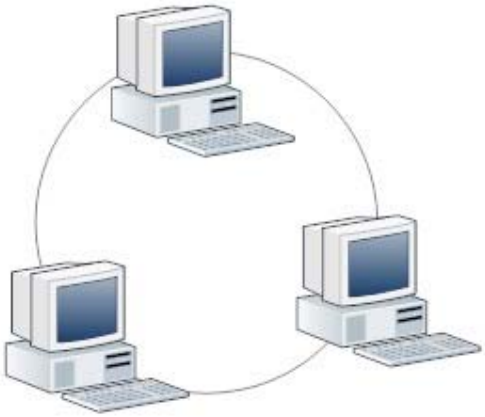


фигура 4 *Тип шина*

- Топология тип „активна шина“ (active bus) – изходът на всеки възел е свързан към входа на следващия. За предаване на сигнала в две различни посоки са необходими две активни шини. Всеки възел действа, като регенератор и усилвател (фигура 5).

фигура 5 *Тип активна шина*

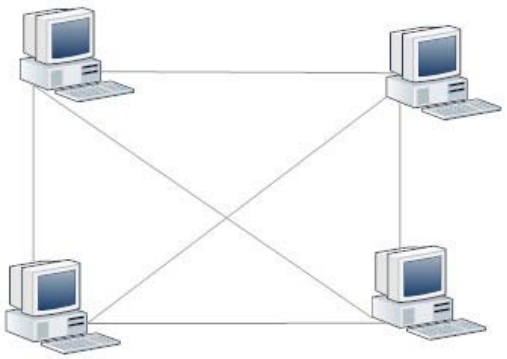
- Топология тип „кръг“ (ring)– възлите в мрежата са свързани в кръг (фигура 6). Подобно на активната шина всеки възел въздейства върху сигнала, което дава възможност за покриване на по-големи разстояния. Сравнително лесна за инсталиране. Изисква повече кабел от шината и по-малко от топологията тип „звезда“. Един от недостатъците е трудното добавяне на нов възел.



фигура 6 *Тип кръг*

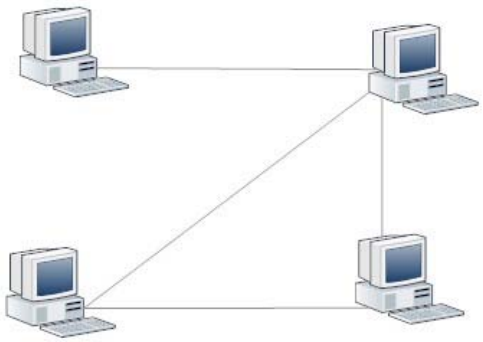
- Топология тип „решетка“ (mesh) – всеки компютър е свързан с всеки друг (фигура 7), което води до висока отказоустойчивост

(fault tolerant). **Отказоустойчивостта** гарантира функционирането на мрежата дори при проблем с някой от компютрите или свързващите ги кабели. Като недостатъци могат да се посочат висока цена за построяването ѝ и сложната реализация.



фигура 7 *Тип решетка*

- Топология тип „хибридна решетка“ – базира се на полурешетъчна топология, където допълнителни връзки има само между някои от компютрите (тези, които се нуждаят най-много от отказоустойчивост на връзката)(фигура 8).

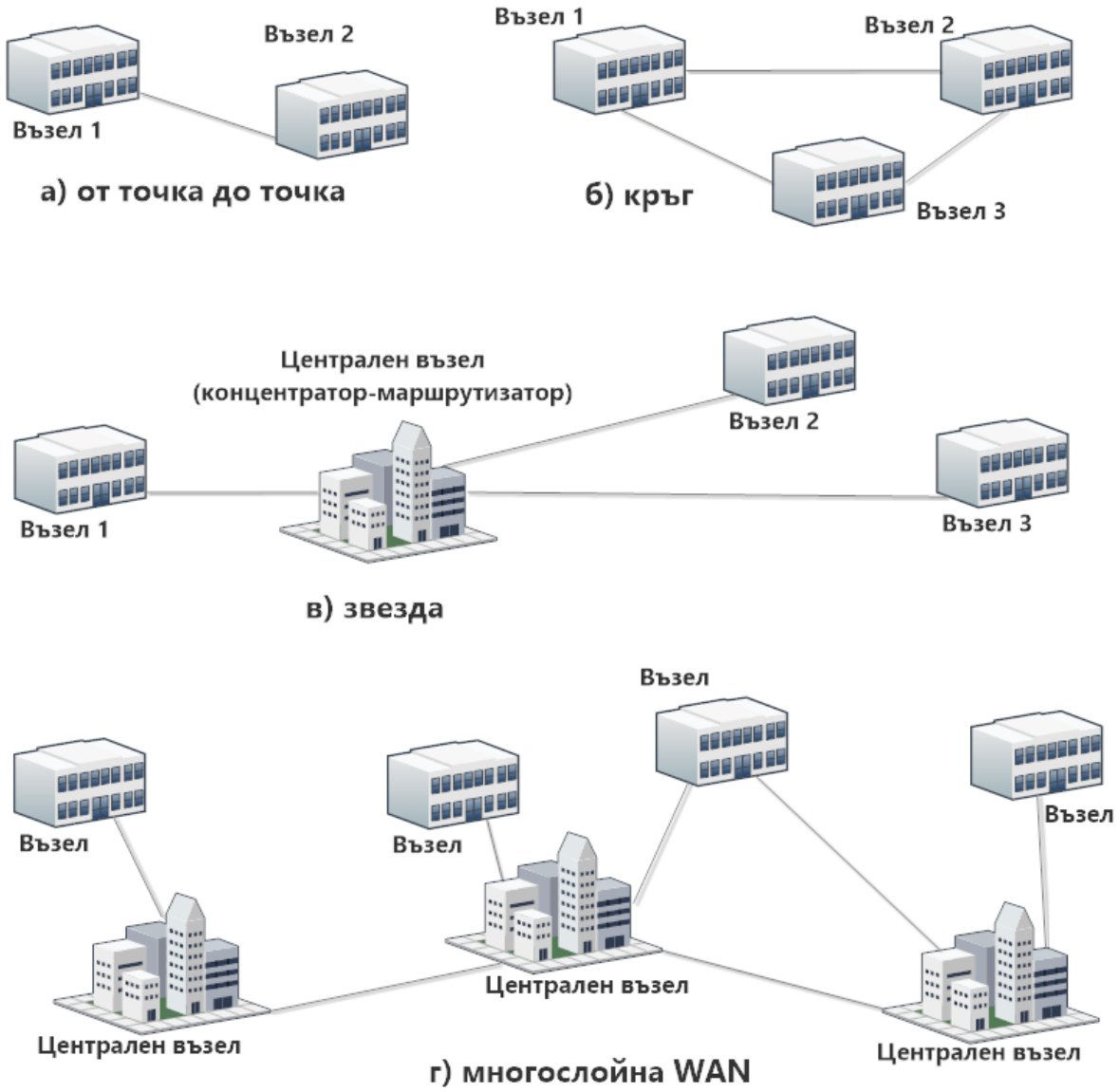


фигура 8 *Хибридна решетка*

1.3.2. Мрежови топологии в WAN

Мрежовите топологии в WAN са подобни на тези от LAN, но се отличават с по-сложна реализация, дължаща се на: големите разстояния, които трябва да покриват; свързването на местоположения, а не на локални възли; по-големия брой потребители, които трябва да се обслужат; по-интензивния трафик, който трябва да поддържат. Най-често реализираните мрежови топологии са:

- **от точка до точка** (peer to peer) – два възела са свързани помежду си със самостоятелна връзка. На фигура 9а се вижда такава свързаност (възел 1, възел 3) и (възел 2, възел 3). Тези свързващи линии се наемат от телекомуникационен оператор.
- **кръг** (ring) – всеки два възела са свързани помежду си с връзка (фигура 9б). По този начин всеки възел може да изпраща до останалите дори и при проблем с една от връзките.
- **звезда** (star) – единият от възлите действа като централна точка за връзка с останалите (фигура 9в). Така всеки възел получава свързаност към останалите през централната точка.
- **многослойна WAN** (tiered WAN) – това е начин за свързване на няколко звезди на различни нива (фигура 9г), което позволява по-лесна разширяемост и администриране на мрежовия трафик, намаляване на зависимостта на мрежата от мрежовия хардуер.



фигура 9 *WAN топологии*

1.4. Структура, организация и правила за работа в глобалната мрежа Интернет

Интернет е глобална мрежа, свързваща хиляди големи и малки мрежи, локализирани по целия свят. Инфраструктурата ѝ е йерархична. Изградена е от мрежи на различни нива, с различна степен на сложност и важност. Използва хибридна решетъчна топология, подобна на хибридната решетка при локалните мрежи и многослойната WAN при глобалните мрежи.

Основна част от приложенията в Интернет използват схема на работа, наречена клиент/сървър, при която сървърът отговаря на заявки за услуги от страна на клиента. Потребителят получава достъп до сървъра чрез клиентска програма, например Web браузър. Типични приложения в

Интернет, които използват схемата са Web, електронната поща (e-mail), прехвърлянето на файлове (FTP) и много други.

За комуникация помежду си приложенията използват пакет от съвместно работещи протоколи с общо наименование TCP/IP протоколен стек. Под **протокол** се разбира съвкупност от правила, по които приложенията си обменят данни, наречени **пакети**. Протоколите казват на мрежата как да изпълнява своите функции и да предлага своите услуги. За дадена услуга може да отговаря един или няколко протокола. Всяка съвременна операционна система поддържа TCP/IP протоколния стек, за осигуряване на достъп до Интернет.

Съществуват и други правила. От една страна организациите, предлагащи интернет услуги определят конкретни правила за достъп до тях. От друга страна потребителите са задължени да спазват определени етични норми при използването на предлаганите услуги и Интернет. Като такива могат да бъдат посочени:

- избягване на незаконен достъп до информационни ресурси на чужди системи;
- забрана за разпространяването на нежелана информация т.нар. спам;
- забрана за разпространяването на информация, която е защитена от различните законодателства;
- забрана за използването на лични данни на чужди лица;
- и много други.

Спазването на подобни правила, засягащи съдържанието и използването на Интернет, се нарича нетикет и произлиза от думите „интернет“ и „етикет“.

1.5.Основни услуги

Популярността на Интернет се дължи на услугите, които предлага. Трансферът на данни между потребители и организации, търсенето и намиране на информация за спорт, икономика, музика и много други неща са реалност, която е възможна на базата на тези услуги. Най-често използваните Интернет услуги са:

- **Web (World Wide Web, WWW)** – това е най-масово използваната мултимедийна услуга в Интернет. Информацията

се представя под формата на хипертекстови документи, съхранени и предоставяни от Web сървъри, с възможност за разглеждане от Web браузъри (например: Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome и др.). Протоколът, който обслужва тази услуга се нарича HTTP.

- **Трансфер на файлове (File transfer)** – услуга, даваща възможност за прехвърляне на файлове между приложения. Протоколът, който я поддържа се нарича протокол за трансфер на файлове (File Transfer Protocol, FTP). Съществуват специални програми за обмен на файлове, наречени FTP програми (например CuteFTP, FileZilla®). Съвременните браузъри също поддържат тази възможност.
- **Отдалечен достъп (Telnet)** - това е една от първите исторически възникнали услуги в Интернет. Позволява достъп до отдалечен компютър с цел, стартиране на приложения или достъп до данни на неговия харддиск. За целта се използват специални програми, например Telnet, Putty и др.
- **Електронна поща (e-mail)** – широко използвана в момента услуга, осигуряваща изпращането и получаването на електронни съобщения. Потребителите на тази услуга трябва да имат валидни електронни e-mail адреси. Адресът се получава след регистрация на избран от потребителя сървър за електронна поща, където автоматично му се създава пощенска кутия (mailbox). Достъпът до нея се осъществява чрез потребителско име и парола. Протоколите, които обслужват електронната поща са с означенията SMTP (Simple Mail Transfer Protokol), POP3 (Post Office Protocol, версия 3), IMAP4 (Internet Message Access Protocol, версия 4).
- **Световна разпределена дискусионна система (Usenet)** - новинарска услуга, осигуряваща среда за дискусии и обмен на информация между хора с общи интереси, разделени по групи (newsgroups). Тя предлага бюлетин бордове, чат-стаи (chat rooms) и мрежови новини (Network News).
- **Интернет телефония (VoIP)** - технология, позволяваща пренос на гласови съобщения и мултимедийна информация чрез IP пакети в Интернет среда. Услугата предлага евтин вариант за разговори на далечно разстояние. Крайните устройства могат да

бъдат два компютъра, два IP телефона или компютър и телефон. Качеството на VoIP зависи главно от скоростта на връзката и разстоянието между участващите устройства.

- **Чат разговори (Internet Relay Chat, IRC)** – услугата дава възможност на потребителите от цял свят да общуват помежду си в реално време. Потребителят се включва към канал (chanel) на избран IRC сървър, като се идентифицира с уникално име (nick), след което може да изпраща съобщения до всички присъстващи или само до избран участник.
- **Интернет на нещата (Internet of Things. IoT)** – следващата голяма революция в комуникационната сфера, която е базирана на технологии, протоколи и устройства, които могат сами да комуникират помежду си и да реагират адекватно на създалите се промени в околната среда.

Речник
Local Area Network (LAN) – лан мрежа – локална мрежа
Wide Area Network (WAN)– уан мрежа - глобална мрежа
physical topology – физикъл тополоджи - физическа топология
logical topology – логикъл тополоджи – логическа топология
star – стар – звезда
passive bus – пасив бъс – пасивна шина
active bus – актив бъс – активна шина
ring – ринг – кръг
mesh – меш – решетка
peer to peer – пиър то пиър – от точка до точка

Въпроси и задачи

1. Как изглежда опростен модел на мрежа?
2. Посочете разликите между LAN и WAN.
3. Избройте някои от предимствата на компютърните мрежи.
4. Посочете разликата между физическа и логическа топология.
5. Каква е разликата между междинен и краен възел в една мрежа?
6. Каква е разликата между сървър и работна станция?
7. Какви сървъри познавате?
8. Какво е протокол?
9. Посочете някои от предлаганите услуги в Интернет?

2. Основни комуникационни устройства и съобщителни среди

2.1. Основни комуникационни устройства

В предходната тема беше разгледана общата структура на една компютърна мрежа, където беше споменато, че едни от основните ѝ компоненти са нейните възли, които могат да бъдат крайни или междинни. Всеки възел представлява хардуерно устройство, което използва **мрежова платка** за свързване с преносната среда на мрежата. Например за компютърните системи се използва т.нар. **мрежова интерфейсна карта (NIC)**, която може да осигури жична или безжична свързаност към мрежовата среда.

фигура 1 *Жична мрежова карта*

фигура 2 *Безжични мрежови карти*

Съществуват различни подходи за включване към мрежата. Това се дължи на разнообразието от използвани мрежови технологии. За управление на мрежата и преодоляване на различията между отделните мрежи са проектирани и разработени специализирани междинни

устройства. Те притежават различна функционалност и наименования, които ги отличават спрямо ролята, която изпълняват.

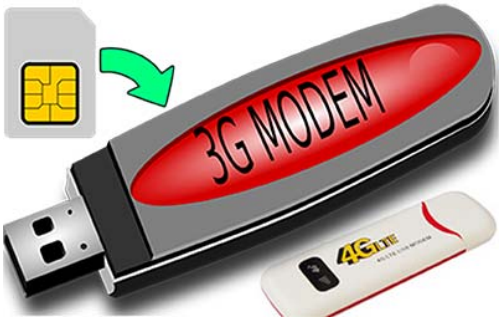
Модем (модулатор/демодулатор)

Модемът е специализирано комуникационно устройство за предаване на цифрови (компютърни) данни по аналогови (телефонни или телевизионни) трасета. Използват се за отдалечен достъп на единични потребители до локална или глобална мрежа. Достъпът до локална мрежа изисква наличието на специализиран сървър, наречен RAS-сървър (Remote Access Server) (фигура 3).

фигура 3 *Отдалечен достъп в локална мрежа*

Модемите могат да бъдат произведени като самостоятелни устройства (външни модеми) или да бъдат вградени в други устройства (вътрешни модеми). В момента масово са разпространени кабелните модеми, които се използват от операторите за кабелна телевизия за доставяне на интернет по телевизионни трасета (фигура 4). Друг пример за технология, използваща модем е DSL технологията. Една от нейните разновидности се нарича ADSL. Технологията осигурява WAN свързаност на базата на съществуващи медни проводници от телефонни трасета. По линията могат да бъдат предавани едновременно глас и данни. Мобилните оператори също предлагат безжични модеми (фигура 5), с които може да се осигури достъп до мобилната им мрежа за използване на предлагания от тях интернет.

фигура 4 *Кабелен модем*



фигура 5 *3G и 4G модем*

Комутатор (switch)

Комутаторът е междинно устройство, което осигурява допълнителни входни точки за включване на възли към локалната мрежа и управлява достъпа им до нея. Входните точки се наричат портове, а комутаторът – многопортов комутатор. Техният брой е различен и зависи от ценовата стойност на устройството. Често срещани са 5, 8, 16, 24, 32 портови комутатори. Английското му наименование е суич (switch). Използва се като централен възел в съвременните локални мрежи. Позволява възможност за свързване с друг комутатор, за получаване на топология „разширена звезда“. Запазва скоростта на мрежата за всеки един от портовете си. Възстановява и усилва предавания сигнал, което позволява удължаване на покривното разстояние.

фигура 6 *5-портов комутатор (суич)*

Маршрутизатор (router)

Маршрутизаторът е междинно устройство, което притежава по-голяма функционалност от комутатора. Използва се за свързване на поне две мрежи и преодоляване на различията между тях, като ги управлява на по-високо ниво, в сравнение със суича. Може да се използва и за разделяне на една голяма мрежа на няколко по-малки. Маршрутизаторът избира пътя, по-който трябва да преминат данните до достигане на крайната цел. Това се налага в случаите, когато има възможност за избор между няколко налични маршрута за достигане на целта. Английското му наименование е рутер (router). Използва се като входна/изходна точка за достъп до интернет и го разпределя между устройствата в локалната мрежа. Комутаторът не може да изпълнява тази функция.

Точка за достъп (access point, AP)

Точката за достъп е междинно устройство, което помага на безжични устройства да се свържат към една мрежа и да използват нейните услуги. Схема на такава свързаност е показана на фигура 10

2.2.Съобщителни среди

Предаването на данни по мрежата става възможно, благодарение на използваната среда за пренос. Когато средата е кабелна, мрежата се нарича **кабелна мрежа**. Използването на безжична среда класифицира мрежата като **безжична мрежа**.

Кабелна среда

Кабелната среда включва: коаксиален кабел, кабел с усукани двойки проводници и кабел с оптични влакна.

- *коаксиални кабели* – вътрешен проводник, обвит с изолационен материал, медна оплетка и външна обвивка (фигура 7). Оплетката играе роля на предпазен екран. Ако съществува първи изолационен слой от фолио и втори от метална оплетка, то кабелът е двойно екраниран. Неговите два основни варианта са тънък (thinnet) и дебел (thicknet). Дебелата изолация и доброто екраниране гарантират по-добра защита от електромагнитни смущения, в сравнение с усуканата двойка проводници. Тънкият кабел може да пренася качествен сигнал на разстояние до 185 метра, а дебелият до 500 метра. В ранните реализации на сегашната локална компютърна мрежа, коаксиалният кабел беше най-популярният тип. Сега се използва усукана двойка проводници.

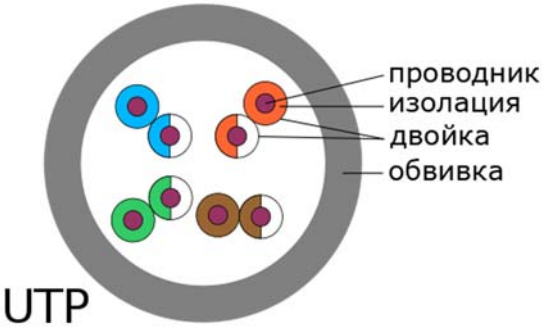
Съществуват различни типове и категории коаксиални кабели, предлагащи се от различните производители. Много от тях се използват от мрежи със специално предназначение. Например разновидност на такъв тип кабел се използва от кабелните телевизионни оператори. Към тях може да бъде включен кабелен модем за свързване на абонат към Интернет.

фигура 7 *Структура на коаксиален кабел*

- *кабели с усукана двойка проводници* – състоят се от четири двойки медни проводници. Двата проводника на всяка двойка са изолирани и взаимно усукани за намаляване на външните шумове (фигура 8). Предназначени са за малки разстояния. Съществуват различни категории, поддържащи различни скорости. Самата категория се идентифицира със символите Cat X и означава номера на успешно преминалия тест за производителност. В момента едни от най – разпространените категории са Cat 5e и Cat 6. Максималната дължина за сигнала без повторител е 100 м.

Този вид кабел може да бъде екраниран или неекраниран. Екранираният кабел усукана двойка се означава с наименованието STP (shielded twisted pair), а неекранираният като UTP (unshielded twisted pair). UTP вариантът се използва за окабеляване на места, където има по-малко електромагнитни смущения. Той е по-евтин, гъвкав и лесен за работа. STP кабелът е по-скъп и не е толкова гъвкав, както FTP кабелът. Използва се за външен монтаж и в среди с по-висока степен на електросмущения.

Съвременните локални компютърни мрежи използват кабел усукана двойка проводници като преносна среда.



фигура 8 *Структура на UTP кабел*

- *влакнестооптични кабели* – съставени са от отделни влакна, направени от стъкло или пластмаса. Оптичното влакно се състои от **ядро** (core) и **външен слой** (cladding) с различен показател на пречупване на светлината (фигура 9). Това важно свойство на оптиката не позволява преплитането на информация между отделните влакна в един кабел и му позволява той да се извива и усуква.

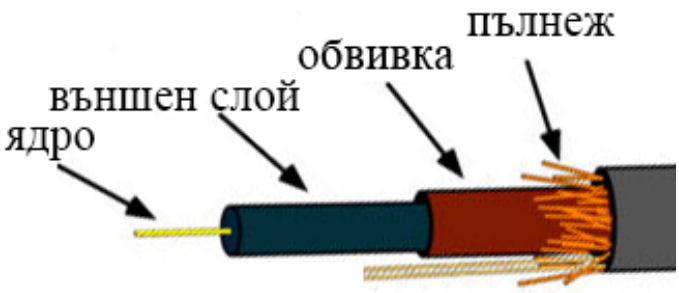
Този вид кабели е най-добрата среда за пренос, защото е по-сигурен от коаксиалния кабел и усуканата двойка проводници. По-устойчив е на затихване на сигнала, което позволява поддържането на по-голямо разстояние за предаване. Неподатлив е на външни електрически смущения. Поддържа по-високи скорости. В сравнение с останалите типове кабел оптичният е доста по-скъп и труден за работа.

Съществуват два режима на предаване:

- Единичен режим (Single mode) – при този режим светлината пътува по оста на кабела;

- Множествен режим (Multimode) – при този режим светлината навлиза в ядрото под различен ъгъл, което я кара непрекъснато да се отразява и отскача от стените на външния слой.

По-бързият от двата режима е единичният режим. Използва се при WAN мрежите и може да покрие разстояние до 80-200 км. Множественият режим е предназначен за LAN мрежите и покрива разстояние до 300-500 метра.



фигура 9 *Структура на оптичен кабел с едно влакно*

Влакната, използвани в телекомуникацията, са най–често с диаметър 125 μm. Ядрото на едномодовите влакна е с диаметър 9 μm, докато при многомодовите е с диаметър 50 μm или 62,5 μm. Описват се с двойка числа, показващи диаметъра на влакното и на неговата обвивка (например 62,5/125 микрона).

Безжична среда

Безжичната среда позволява протичането на комуникацията да се извършва без наличието на кабел. В момента е доста актуална като среда за пренос на данни, въпреки че предаването по нея е по-бавно в сравнение с кабелните връзки. За този тип комуникация могат да се използват: лазер, инфрачервени лъчи, радио честоти. Като пример за мрежи, използващи такъв тип среда могат да се посочат Wi-Fi мрежите или тези на мобилните оператори.

2.3.Проектиране на малка домашна или офис мрежа

Изграждането на такъв тип мрежа се реализира предимно с физически ресурси от нисък ценови клас. Обикновено това са рутер, суич, няколко компютъра и безжични клиентски устройства, жична и безжична среда за комуникация.

1. Рутерът е необходим за свързване на локалната ни мрежа към мрежата на доставчика на Интернет. Маршрутизаторът ще разпределя интернета към всички компютри и клиентски устройства от нашата мрежа.

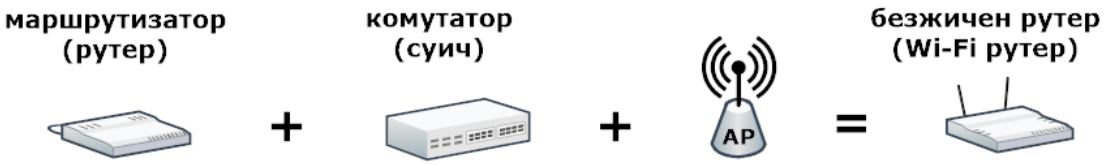
2. Суичът е междинното устройство в локалната ни мрежа, което ще играе ролята на централен възел и ще осигурява свързване на жичните устройства към нея. Трябва да бъде избран с необходимия брой физически портове Топологията ще бъде звезда, а използваният кабел – UTP.

3. За предоставянето и на безжичен начин за достъп до нашата LAN ще е необходима и безжична точка за достъп (AP). Тя ще се свързва към суича с кабелна връзка.

На фигура 10 е показана схема на описаната по-горе организация на една локална мрежа. Ако се премахне безжичната точка за достъп, проектираната локална мрежа ще се превърне в жична мрежа. Съществува вариант за изключване на суича от схемата, тогава мрежата ще остане безжична.

фигура 10 *Примерна схема на малка локална мрежа*

Понякога производителят обединява няколко междинни устройства в едно с цел, намаляване на техния брой и поевтиняване на реализацията на мрежата. На фигура 11 е представен такъв подход, където маршрутизатор, комутатор и безжична точка за достъп са комбинирани в едно устройство – безжичен рутер.



фигура 11 *Примерна схема на малка локална мрежа*

Речник
Modem – модем – модем
Switch – суич – комутатор
Router – рутер – маршрутизатор
Access point – аксес поинт – точка за достъп
Thinnet – тиннет – тънък
Thicknet – тикнет – дебел
Single mode – сингъл мод – единичен режим
Multimode – мултимод – множествен режим

Знаете ли, че …

Сегашният стандарт за кабелна локална мрежа се нарича Ethernet, а за безжична локална свързаност Wi-Fi.

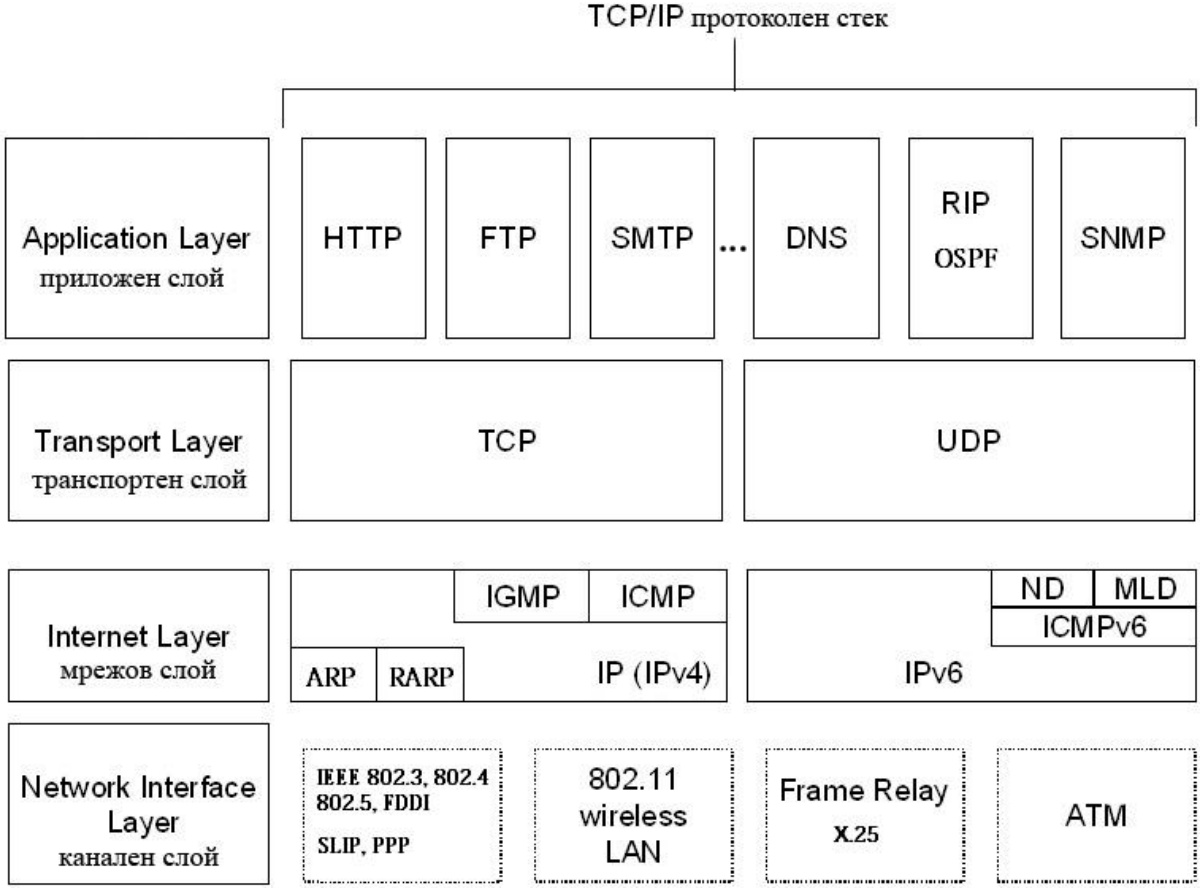
Въпроси и задачи

1. Определете типа на мрежовата карта, с която разполага Вашият компютър.
2. Посочете разликите между маршрутизатор и комутатор.
3. Какво устройство ще използвате в кабелна локална мрежа, ако желаете безжични системи да имат достъп до нея?
4. Кой кабел осигурява най-добра среда за пренос?
5. Какъв кабел използват съвременните локални мрежи за преносна среда? Коя е масово разпространената категория?
6. Посочете правилната последователност при подредбата на: суич, принтер, рутер, безжична точка за достъп, доставчик на Интернет, лаптоп.
7. Определете вида на кабела, който е използвал вашият доставчик на Интернет, за да Ви осигури достъп до глобалната мрежа.
8. Опитайте се да определите какви устройства участват в изграждането на домашната Ви връзка към Интернет и ги назовете с наименованията им, спрямо функциите, които изпълняват.

3. Свързване и конфигуриране на малка локална мрежа

3.1. TCP/IP протоколен стек

TCP/IP (Transmission Control Protocol/Internet Protocol) е основният протоколен стек, необходим за функционирането на глобалната мрежа Интернет (фигура 1). В момента се поддържа стандартно от всички модерни операционни системи. Наименованието на стека се базира на двата основни протокола в него, TCP и IP. Състои се от 4 слоя, които са подредени в йерархична последователност и съдържат набор от съвместно работещи протоколи. Подредбата и наименованията на отделните слоеве, както и малка част от включените протоколи са показани на фигура 1.



фигура 1 *TCP/IP протоколен стек*

Всяко комуникационно устройство, което използва Интернет трябва да има инсталиран този протоколен стек. Устройствата, отговарящи на това условие се наричат **хостове**. Предаваните данни обикновено се разделят на малки парчета, наричани **пакети**. Това се прави с цел да се управляват по-лесно и да не се натоварва мрежата. В противен случай тя ще бъде заета само от едно предаване и няма да може да се използва от другите хостове, които

искат също да предават. Например изпращането на голям файл по мрежата изисква разбиването му на пакети. Когато пакетите пристигнат при получателя, те се сглобяват в правилната последователност и се получава цялостният файл.

Инфраструктурата на Интернет позволява всеки пакет да бъде изпращан по различен път до крайния получател. Това се налага в случаите, когато някои път бъде натоварен и забавя предаването или вече не функционира. Пътят, по който преминава пакетът се нарича **маршрут**, а неговият избор – **маршрутизиране**.

Мрежови протоколи

Протоколът IP (Internet Protocol)

IP е основен протокол в TCP/IP стека. Отговаря за маршрутизирането на пакета от мрежата на подателя през междинните машрутизатори до мрежата на получателя. За реализирането на тази функция се използват **IP адреси**, идентифициращи еднозначно хостовете и мрежите, към които принадлежат. Например всеки компютър притежава уникален IP адрес.

Възможно е едно устройство да има повече от един IP адрес. Такъв е случаят с маршрутизаторите, които притежават поне два интерфейса, осигуряващи свързване към различни мрежи. Всеки от интерфейсите е необходимо да притежава собствен уникален IP адрес.

Съществуват два стандарта за представяне на IP адресите, в зависимост от версията на IP протокола, който се използва. Действащият стандарт в момента се означава като IPv4. При него IP адресът е 4 байтов (1 байт са 8 бита) и се записват с 4 десетични числа в интервала от 0 до 255, разделени с точки (фигура 2). Пример за такъв адрес е **192.168.1.15**.

Всеки IP адрес логически се разделя на две части: **адрес на мрежата** (Net ID) и **адрес на хоста** (Host ID). По този начин в една и съща мрежа могат да бъдат адресирани множество компютри. В дадения по-горе пример за IP адрес 192.168.1.15, адресът на мрежата е 192.168.1, а адресът на хоста е 15 (фигура 2). Правилното изписване на адреса на мрежата изисква липсващите позиции за хост да се запълват с нули т.е. 192.168.1**.0**. Например IP адресът **192.168.1.16** е следващия адрес в същата мрежа (192.168.1**.0**) с адрес на хоста 16.

Мрежовата маска е тази, която показва за един IP адрес до къде стига адресът за мрежата и кой е адресът на хоста в нея (фигура 2). Мрежовата маска не съществува самостоятелно. Както IP адреса, тя също е 4 байтова и е прикрепена към него. Стандартните мрежови маски използват две стойности, които в десетичен вид са 0 и 255. Позициите на числата 255 показват адреса на мрежата (Net ID), а позициите на 0 – адресът на хоста (Host ID). Например за анализираните IP адреси **192.168.1.15** и **192.168.1.16** стандартната мрежова маска е **255.255.255.0**.

фигура 2 *Структура и деление на IP адрес*

Класове IP адреси

Съществуват 5 класа IP адреси (по IPv4). Класифицират се по стойността на първия байт. Наименованието на отделните класове и диапазона от стойности за първия байт от адреса в десетичен вид са показани в таблица 1.

Клас	Десетична стойност на първия байт
клас A	от 1 до 126 включително
клас B	от 128 до 191 включително
клас C	от 192 до 223 включително
клас D	от 224 до 239 включително
клас E	от 240 до 254 включително

таблица 1 *Диапазон на десетичните стойности на първия байт*

Стандартните мрежови маски за клас могат да се видят в таблица 2.

Клас	Мрежова маска
клас A	255.0.0.0
клас B	255.255.0.0
клас C	255.255.255.0
клас D	липсва
клас E	липсва

таблица 2 *Стандартни мрежови маски*

Адресите от клас D и клас E се използват за служебни цели и не притежават мрежови маски. За назначаване на хостове са предназначени само първите три класа, за които има определена и мрежова маска.

Статистическата информация за броя на мрежите и адресите са представени в таблица 3.

Клас	Брой мрежи	Брой адреси
клас A	127	16777216
клас B	16384	65536
клас C	2097152	256

таблица 3 *Статистическа информация за поддържани мрежи и адреси*

Област на действие на IP адресите

Областта на действие на IP адресите ги разделя на публични и частни. **Публичните адреси** са валидни за цялата IP мрежа. Те представят хостовете в Интернет. **Частните IP адреси** са предназначени за конфигуриране на локални мрежи, за да не се заемат публични интернет адреси. Те функционират само в рамките на локалната мрежа, където са назначени. При работа с Интернет частните IP адреси се преобразуват в публични IP адреси. Обикновено тази функция се изпълнява от маршрутизатора (рутера) на LAN мрежата. Той се явява и **шлюз** (**gateway**) на мрежата към Интернет или друга LAN мрежа. Шлюзът управлява преминаването на пакетите от една мрежа в друга.

За всеки от трите класа са дефинирани области от частни IP адреси:

- **клас A** – адресите започват с 10. Примери за частни адреси от клас A са: 10.0.0.12, 10.10.1.100;

- **клас B** – адресите започват със стойности от интервала [172.16;172.31]. Примери за частни адреси от клас B са: 172.16.0.12, 172.17.1.12, 172.31.0.100;
- **клас C** – адресите започват със 192.168. Примери за частни адреси от клас C са: 192.168.0.12, 192.168.17.12, 192.168.100.1. Този тип адреси се срещат най-често при конфигурирането на малки локални и офис мрежи, защото осигуряват възможност за адресиране до 254 устройства, което е напълно достатъчно.

Протоколът ICMP (Internet Control Message Protocol)

Протоколът ICMP се счита за неделима част от IP, защото използва неговите услуги. Чрез него крайните хостове и маршрутизатори обменят служебна информация и съобщения за грешки.

Транспортни протоколи

Транспортните протоколи използват адреси, наречени портове и сокети. Портовете са 16-битови числа в интервала [0; 65535].

Портът и IP-адресът съвместно образуват сокет (89.68.180.5:21). Двойка сокети (от двете страни на комуникацията) еднозначно идентифицира едно TCP-съединение. Един сокет може да участва в няколко съединения едновременно.

Протоколът TCP (Transmission Control Protocol)

TCP е връзково-ориентиран протокол, който използва предварително създадени от него сигурни логически връзки за изпращане на данни между две комуникиращи устройства. Например при предаване на съобщение между компютър А и компютър Б чрез TCP се преминава през следните стъпки:

1. Изгражда се логическа връзка между двата компютъра, наречена **сесия**. Това означава, че те са се уговорили за необходимите параметри, които трябва да се спазват при предаването на данните.

2. При успешно изградена сесия се предават данните под формата на пакети. Процесът на предаване се грижи да не се допускат грешки, както и да не се разбърква последователността на

пристигане на отделните пакети. Това гарантира сигурността на връзката.

3. Разпадане на логическата връзка след приключване на предаването.

TCP може да поддържа едновременно множество логически връзки, базирани на сокети. Благодарение на тази възможност, потребителите на Интернет могат по-едно и също време да отварят няколко интернет страници, да слушат онлайн музика, да свалят файлове и да изпълняват много други дейности.

Протоколът UDP (User Datagram Protocol)

UDP е безвръзков протокол. Не изгражда логическа връзка. Не контролира реда на пакетите с данни. Не следи какво е изпратил. Затова предаването му е ненадеждно (може да има загуба на пакети). Това означава, че UDP изпраща пакетите без предварителна уговорка с приемащата страна. Тя разбира за това при получаване на пакет.

UDP е подходящ за малки съобщения, които могат да се предадат с един пакет. Този протокол е по-бърз от TCP.

Приложни протоколи

Протоколът HTTP (Hypertext Transfer Protocol)

HTTP е протокол за трансфер на хипертекст. Терминът hyper означава, че документът съдържа връзки, които могат да се избират. Неговото развитие осигурява поддържането на сложни типове данни, които лежат в основата на съвременния Web.

HTTP работи в приложния слой на TCP/IP стека и използва TCP за гарантирана доставка. Поддържа схемата клиент/сървър. Клиентът може да бъде браузър, паяк или друг потребителски инструмент, който използва URL (Uniform Resource Locator) адреси за изпращане на заявка до HTTP сървър, осигуряващ желаната услуга.

Системата URL предлага единен начин за наименуване на ресурси. Всеки документ (файл) може да се намери чрез неговия универсален индентификатор (фигура 3), който е съставен от три части:

1. Тип на протокола за достъп. При услугата WWW за тип на протокол за достъп се указва http. Допустими са mailto (за електронна поща), ftp (за прехвърляне на файлове) и др. Първата част завършва с двоеточие (:);
2. Име на компютър, съгласно приетото адресиране в Интернет (обяснено по-долу). Това име се предхожда от две наклонени черти (//);
3. Пълното име (path) на файла, съгласно определените стандарти на използваната операционната система и типа на протокола за достъп. Започва с наклонена черта (/). Може да липсва. Тогава се има предвид име по подразбиране. Например при протокола http много често това е index.html (зависи от настройките на съответния сървър).

В Интернет е прието цифровите (IP) адреси на хостове да се заменят с имена, които улесняват потребителя при тяхното запомняне и използване за достъп до сървър. Имената са подредени в йерархична дървовидна структура (на нива) под формата на **области от имена** (Domain Name), наречени **домейни**.

Управлението на домейните в Интернет се изпълнява от система, наречена DNS (*Domain Name System*), а сървърите, които предлагат такава услуга DNS сървъри. Основното и предназначение е да асоциира IP адреси с буквеноцифрови имена, което позволява хостовете да бъдат групирани по географски принцип или по тяхната принадлежност към някаква организация.

Имената се състоят от отделни части, разделени с точка. Най-високо в йерархията са приети трибуквени означения за области от определен тип или двубуквени за обозначаване на държави. Те се наричат *top-level* домейни. Такива съкращения са например:

- .edu - образователни институции;
- .gov - правителствени организации;
- .mil - военни организации;
- .com - големи корпорации или бизнес организации;
- .net - доставчици на Интернет услуги;
- .org - други видове организации;
- .au – Австралия;

- .bg – България.

Организации и отделни хора могат да запазват имена на домейни от второ ниво, като например *google.com*, *abv.bg*. Втората част от името (отдясно на ляво) се използва за идентифициране на организация, а всяка следваща част може да бъде име на по-малко подразделение, име на компютър или устройство. Например *kmk.fmi-plovdiv.org* означава компютър, предлагащ услугата WWW в подразделение *kmk* на организацията *fmi-plovdiv*.

фигура 3 *Структура на URL адрес*

Протоколът FTP (File Transfer Protocol)

Протоколът FTP е създаден за трансфер (качване, сваляне) на файлове. Използва услугите на TCP като транспортен протокол през стандартен порт 21.

Протоколът DHCP (Dynamic Host Configuration Protocol)

Протоколът DHCP осигурява динамичното конфигуриране на хостове в мрежата, без намеса на системен администратор. DHCP е базиран на клиент/сървър архитектура. Клиентите (хостовете) изпращат заявка, а DHCP сървърът отговаря с конфигурационни параметри - IP адрес, време за използване на този адрес, адрес на шлюз по подразбиране (default gateway), DNS сървъри и др.

Автоматичното раздаване на IP адреси е най-често използваният вариант, когато клиентско устройство се свързва към рутер на локална мрежа за достъп до Интернет. В този случай на рутера е стартиран DHCP сървър.

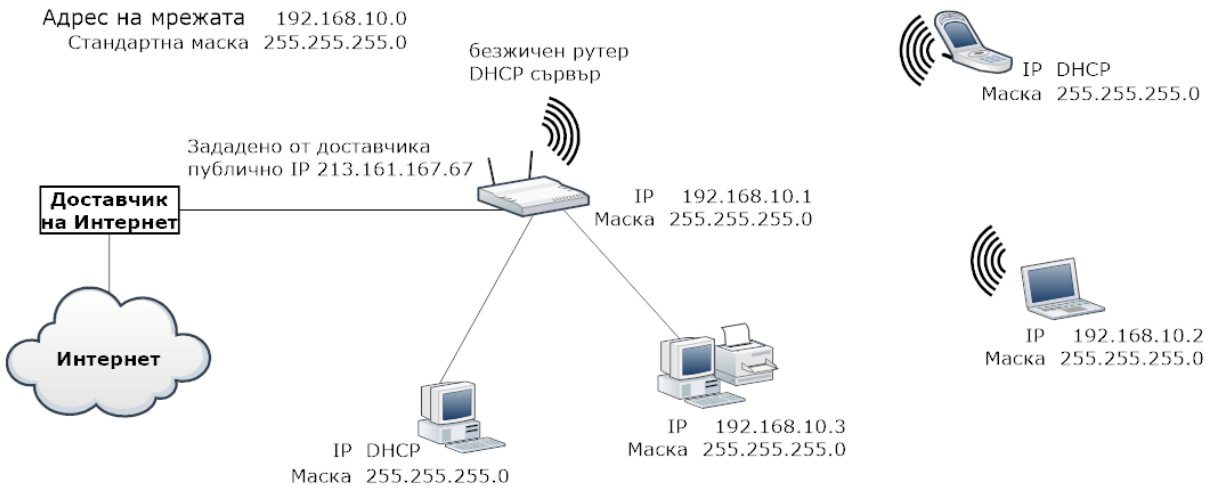
Протоколи за електронна поща

Електронната поща използва следните протоколи:

- SMTP (Simple Mail Transfer Protocol) – протоколът осигурява предаването на електронно съобщение между пощенските (SMTP) сървъри на подателя и получателя, чрез двупосочно TCP съединение през порт 25. SMTP сървърът обикновено се използва за изпращане на e-mail.
- POP3 (Post Office Protocol, версия 3) и IMAP4 (Internet Message Access Protocol, версия 4) – протоколите се използват за четене и обработка на получени e-mail съобщения, след пристигането им на пощенския сървър на клиента. Използва се един от двата протокола.

3.2. Конфигуриране на малка домашна мрежа

В предишната тема беше проектирана схема на малка локална мрежа, която може да бъде използвана при изграждането на домашна мрежа. В нея бяха включени безжичен рутер, суич, няколко компютъра и безжични клиентски устройства. Получените знания от този урок могат да помогнат за преминаване към следващата стъпка – конфигуриране на мрежата с IP адреси. Примерна конфигурация е представена на фигура 4. За адрес на мрежата е избран частен адрес 192.168.10.0 от клас C със стандартна мрежова маска 255.255.255.0. Такъв адрес позволява адресирането до 254 хоста, което е предостатъчно за малка локална мрежа.



фигура 4 *Конфигуриране на мрежата с IP адреси*

Клиентските устройства могат да получат IP адреси като последната цифра от адреса на мрежата (в случая 0) се замени със стойност от интервала [2;254], например 192.168.10.3. Адресът, завършващ на 1 (192.168.10.1) обикновено се назначава на шлюза (gateway), който в случая е маршрутизаторът на мрежата. На рутерът е активиран и DHCP сървър, който раздава динамични IP адреси. Част от устройствата са получили точно такива адреси. Останалите адреси се назначени статично.

Определянето на типа на получаване и начина на назначаване на IP адрес на компютър с Windows операционна система може да стане по следния начин:

1. От *Control Panel* се избира опцията *Network and Sharing Center*, която дава възможност за промяна на настройките на избран от нас мрежов интерфейс чрез опцията *Change adapter settings*;

2. След избор на опцията *Change adapter settings*, операционната система ни дава възможност за избор на мрежов интерфейс, за който да

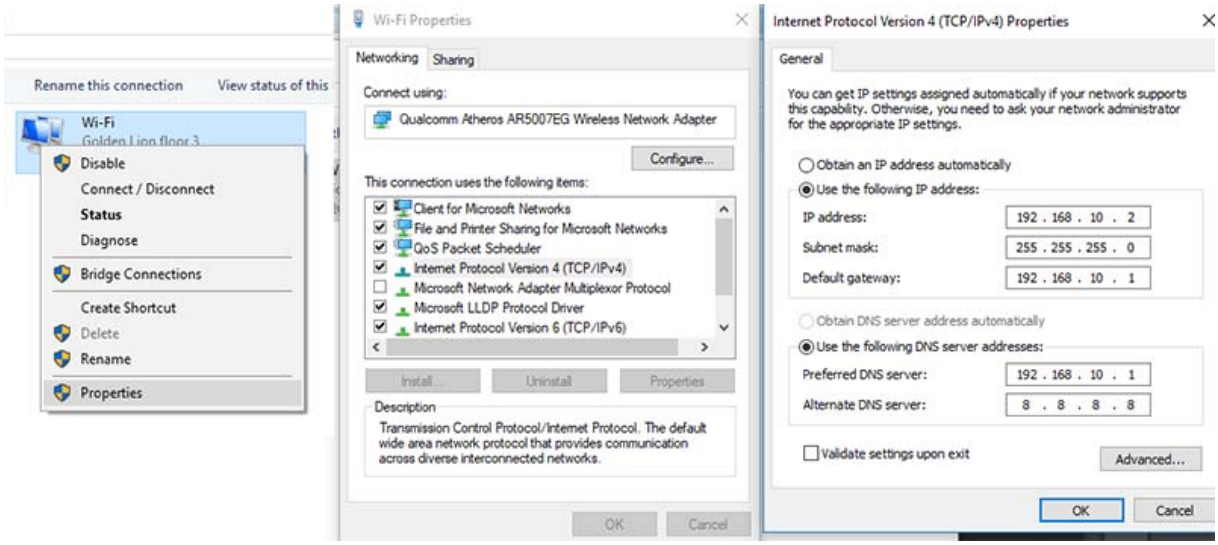
направим промените. Броя на интерфейсите зависи от наличните мрежови карти и портове, с които разполага компютърната система.

3. Десният бутон на мишката върху избрания интерфейс ще отвори контекстно меню, откъдето се избира последната опция *Properties*. Изборът и предизвиква отваряне на допълнителен прозорец, в който се избира протоколът TCP/IP (версия 4).

4. След избора на протокола се натиска бутона *Properties*. Той отваря нов прозорец, където са търсените от нас настройки.

5. Предлагат се два варианта за избор:

   - *Obtain an IP address automatically* – тази възможност позволява на компютъра да получи автоматични настройки от DHCP сървър. Изборът на DNS сървър е на *Obtain DNS server address automatically*.
   - *Use the following IP address* – тази опция дава възможност да се направят ръчни настройки на предложените параметри. На фигура 5 са показани настройки, отговарящи на настройките на лаптопа от фигура 4. В ролята на първи DNS сървър е посочен рутерът на локалната мрежа, а за втори IP адреса 8.8.8.8, който е един от DNS сървърите на Google.



фигура 5 *IP настройки на мрежов интерфейс*

Маршрутизаторът също притежава възможност да бъде настроен по-подобен начин. Понеже е междинно устройство с поне два мрежови интерфейса, той получава публичен IP адрес 213.161.167.67 за интерфейса (WAN интерфейса), свързан към доставчика.

Речник

Socket – сокет – комбинацията ***IP_адрес***:*порт*

Въпроси и задачи

1. Какво е хост?
2. Какво е маршрутизиране?
3. Кой протокол от TCP/IP протоколния стек отговаря за маршрутизирането на пакетите в мрежата?
4. За какво служи мрежовата маска?
5. Каква е разликата между адрес на мрежата и адрес на хост от нея?
6. Кои класове IP адреси се използват с мрежова маска?
7. Каква адресация се използва на ниво транспортен слой?
8. Какво означава връзково-ориентиран протокол?
9. За какво служи DNS системата?
10. Каква е ролята на DHCP сървърът в една мрежа?
11. Анализирайте структурата на URL адреса: http://kmk.fmi-plovdiv.org/kmk-lectures/info.html
12. Ако е зададен IP адрес на мрежа 192.168.0.0, определете:
    - Коя е стандартната мрежова маска, която му съответства;
    - Какъв адрес ще зададете на шлюза на мрежата;
    - Какъв е диапазонът от IP адреси, които могат да бъдат назначавани на хостовете в мрежата.

4. LAN мрежи, IP адреси и мрежови маски - упражнение

Задача 1. Посочете грешния IP адрес:

- 192.165.0.1;
- 192.168.100.101;
- 87.126.74.156;
- 88.256.75.25.

Задача 2. Определете класовата принадлежност на следните IP адреси:

- 192.168.101.100;
- 206.13.01.48;
- 10.10.10.100;
- 23.96.52.53.

Посочете стандартната мрежова маска и адреса на мрежата за всеки един от тях.

Задача 3. Научете IP адреса на компютъра си, като използвате командата **ipconfig /all** от командния прозорец *Command Prompt*. Открийте използваната мрежова карта от върнатите в списъка и определете: IP адреса (*IPv4 Address*), използваната мрежова маска (*Subnet Mask*), адресът на шлюза (*Default Gateway*), адресите на DNS сървърите (*DNS Servers*) и адресът на DHCP сървъра (*DHCP Server*). Сравнете Вашият IP адрес с този на съседния компютър.

Упътване: Командата **ipconfig** (за актуалните версии на Windows) с параметър **/all** връща списък от поддържани мрежови интерфейси за конкретната система. Обикновено в даден момент се използва един от тях, който се отличава с търсените в задачите параметри.

Задача 4. Използвайте командата **ping w.x.y.z** от прозореца *Command Prompt*, като заместите последователността **w.x.y.z** с научения:

- IP адрес на съседен компютър;
- IP адрес на шлюз.

При успешно свързване командата връща резултат от няколко реда (обикновено четири за Windows варианта), в които е указано времето до пристигане на отговора от отсрещната страна.

Упътване: Командата **ping** се използва за проверка за наличието на свързаност с друг хост чрез задаване на името (например **ping google.bg**) или IP адреса му (например **ping 216.58.206.163**). Разполага с допълнителни

параметри, които могат да се разгледат след задаване само на командата **ping**. Чрез нея може да се научи IP адреса на хост, ако се знае името му. Например **ping abv.bg** ще върне IP адреса на хоста **abv.bg**.

Задача 5. Използвайте Google търсачката с фраза „what is my ip“ и открийте кой е Вашият публичен IP адрес. Сравнете го с научения IP адрес чрез командата **ipconfig**. Коментирайте получените резултати.

Упътване: По принцип сравняваните IP адреси трябва да се различават, като се вземе под внимание частния характер на локалните IP адреси.

Задача 6. Направете справка в сайт на доставчик на хостинг услуги за възможността да регистрирате, измислен от Вас домейн и каква е цената за извършване на тази услуга.

5. Споделяне на ресурси в локална мрежа

5.1. Споделени ресурси

Основното предимство на LAN мрежите е възможността за достъп и съвместно използване на ресурси, предлагани от други участници в нея. Реализирането на тази основна функционалност е свързано с наличието на необходимите хардуерни устройства и специализиран софтуер.

Към хардуерните решения могат да бъдат причислени клиенти, сървъри, допълнителни устройства (принтери, плотери, дискови устройства) и др. Някои от допълнителните устройства са свързани към компютърни системи за отдаване, а други, които разполагат с мрежови интерфейсни карти могат да бъдат включени директно към LAN.

Софтуерните решения обхващат използваната операционна система (ОС) и специфичните управляващи програми (драйвери) за допълнителните устройства.

Съвкупността от всички тези средства се означават с термина **мрежови ресурси**.

Компютърната операционна система е основния софтуер, който осигурява възможностите за комуникация между устройствата и отдаването на ресурси за общо ползване. Обикновено една такава система се нарича мрежова операционна система (*network operating system*, NOS). Всички съвременни операционни системи поддържат такива мрежови възможности.

Разрешаването на отдалечен достъп до определен ресурс (устройство или данни) преминава през етап, наречен създаване на споделен ресурс (creating a share), а отдадените по този начин ресурси се наричат **споделени ресурси**. Достъпът до тези ресурси може да се реализира по един от двата начина:

- чрез мрежи с равноправен достъп от тип *peer to peer*;
- чрез мрежи от тип клиент/сървър.

Типът на мрежата зависи от начина на администрирането ѝ (как и от кого се управляват мрежовите ресурси).

Мрежи с равноправен достъп

Тези мрежи използват равноправна работна група (*peer to peer*), в която всеки компютър функционира и като клиент, и като сървър. Всеки потребител администрира самостоятелно ресурсите на своята система. Липсва специално обособен компютър за сървър, което означава че няма йерархична организация и зависимост.

Предимствата на такъв тип мрежи са свързани с:

- Евтина реализация и инсталиране. Не са необходими скъпи и сложни сървърни системи, както и специално обучен персонал за администрирането им. Тези мрежи представляват съвкупност от потребителски работни станции, които разполагат с мрежова операционна система, позволяваща равноправно споделяне на ресурси. Съвременните ОС поддържат тази възможност.
- По-голяма стабилност в сравнение с клиент/сървър мрежите. Теоретично сървърът може да спре да функционира, което означава прекратяване на достъпа до споделените от него ресурси. При мрежите с равноправен достъп отказът на една работна станция не води до срив в цялата мрежа.

Недостатъците на *peer to peer* мрежите са в областта на сигурността, администрирането и производителността.

От гледна точка на сигурността и администрирането могат да се посочат следните недостатъци:

- Наличие на множество пароли за достъп до ресурсите на отделните компютри, което принуждава потребителите да пазят копия с тези пароли. Това може да се окаже проблем за сигурността.
- Различията в техническите познания на потребителите могат да доведат до нарушаване на сигурността на мрежата. Обикновено сигурността на цялата мрежа зависи от познанията на най-неграмотните потребители.
- Затрудняване при търсенето на файлове, поради липса на централно място за разположение на споделените ресурси. Това неудобство води до проблеми с поддържането на резервни (backup) копия на данните и софтуера, защото всеки потребител е отговорен за своя компютър и няма гаранция, че ще изпълни тази операция или в кой момент ще го направи.

Производителността на този тип мрежи също може да създаде проблеми:

- Работната станция е предназначена за работа с един потребител. Нейната скорост може да бъде забавена при използване на споделените ѝ ресурси от отдалечен потребител.
- Необходимо е работната станция да бъде включена през цялото време, за да има достъп до споделените ѝ ресурси, дори когато нейният потребител го няма. Това може да създаде проблеми и със сигурността.
- Такъв тип мрежи са трудни за разширяване (мащабиране), защото стават по-неуправляеми като цяло. Те са добър вариант за малки организации с ниска степен на споделяне на ресурси и ограничени финансови възможности.

Мрежи от тип клиент/сървър

При този тип мрежи се поддържа централизирано администриране на компютър, работещ със специален сървърен софтуер и мрежова ОС (NOS). Сървърът идентифицира потребителя по име и парола и определя достъпът му до споделените ресурси. Тези ресурси се разполагат на отделни компютри (сървъри), които нямат основен потребител. Те се явяват многопотребителски машини, които управляват своите споделени ресурси между потребителите.

Предимствата на такъв тип мрежи, в сравнение с мрежите с равноправен достъп са:

- Сигурността се управлява централно. Всички потребителски акаунти и пароли се администрират и проверяват централизирано, преди на даден потребител да се разреши достъп до желания от него ресурс. Това премахва необходимостта от използване на множество пароли.
- Лесно поддържане на резервни копия на данните и софтуера, понеже се намират на определен сървър.
- На потребителите не се налага да търсят къде в мрежата се намират необходимите им ресурси.
- Сървърите са оптимизирани за изпълнение на мрежовите услуги. Разполагат с мощни процесори, с повече памет, по-големи и бързи дискове.
- Лесни за разширяване (мащабируеми). Разположението на ресурсите, тяхното управление и сигурността са централизирани,

което означава че функционирането на такава мрежа не се влияе от размерите ѝ.

Недостатъците на такъв тип мрежи са свързани с:

- Високата цена на хардуера и софтуера за сървърните системи.
- Необходимост от допълнителен обучен персонал за администрирането им.
- Възможност за отказ на сървъра. В този случай се използват различни подходи за намаляване на подобни рискове, което повишава цената на мрежата като цяло.

В някои случаи могат да бъдат използвани и двата подхода за реализиране на мрежа от комбиниран тип.

5.2.Споделяне на мрежови ресурси

Процесът на споделяне в мрежата зависи от мрежовата ОС. Тя трябва да осигурява средства за контрол на достъпа до споделените ресурси. Съществуват два начина за постигане на това:

- сигурност на ниво споделен ресурс (*share-level security*)
- сигурност на ниво потребител (*user-level security*)

Сигурност на ниво споделен ресурс

При този случай споделянето на определен ресурс, например папка, изисква установяването и на парола. За да може някой да направи достъп до споделената папка, той трябва да въведе вярна парола при поискване. Това е голям проблем при наличието на много потребители и много споделени ресурси.

Сигурност на ниво потребител

Този подход позволява по-лесно управление на сигурността в средни и големи мрежи. Всеки потребител притежава потребителско име (акаунт), защитено с парола. Всеки споделен ресурс се конфигурира така, че достъпът до него да е възможен от потребител, притежаващ потребителски акаунт. Паролата е една и осигурява достъп до множество мрежови ресурси. Може да се извърши и проследяване (Одит, audit) кой осъществява достъп до определен ресурс.

Споделяне на папка с помощта на File Explorer в Windows 10

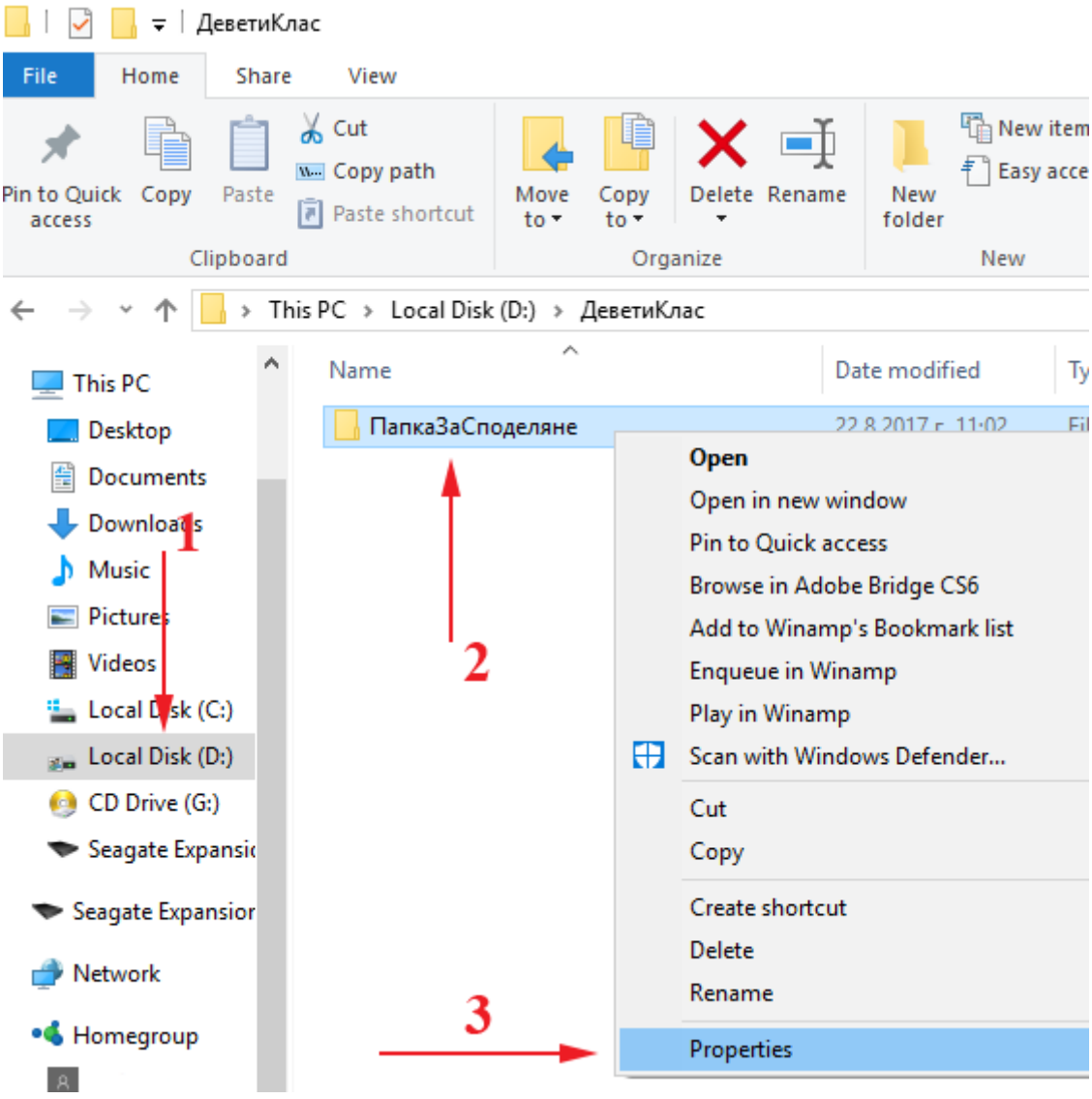
При споделянето на папка в Windows 10 е необходимо да се направят две неща, след като се избере опцията *Properties* от контекстното ѝ меню:

отдаване на папката чрез таба *Sharing* и разрешаване на достъпа до нея чрез таба *Security*.

Отдаване на папката чрез таба Sharing става по следния начин:

1. Стартира се File Explorer и се намира желаната папка за споделяне, например *ПапкаЗаСподеляне* (фигура 1).

2. С десен бутон на мишката върху папката се извиква контекстното ѝ меню и се избира опцията *Properties*(фигура 1).

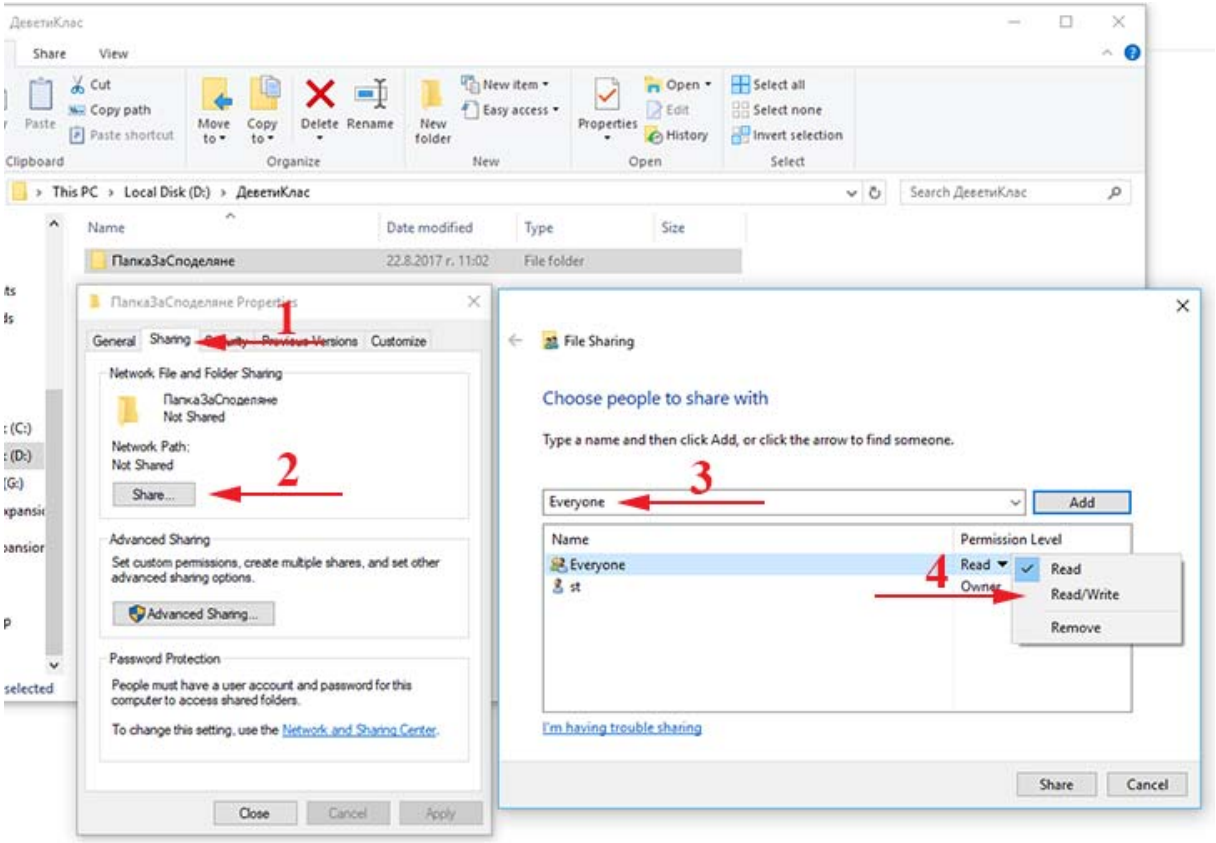


фигура 1 *Стъпки 1-2*

3. Избира се табът *Sharing* (фигура 2) и се натиска бутона *Share*, с което се предизвиква отварянето на нов прозорец, където трябва да се посочи групата или отделен потребител, с който се споделя ресурса. За целта се използва падащото меню, отляво на бутона *Add*. Търси се

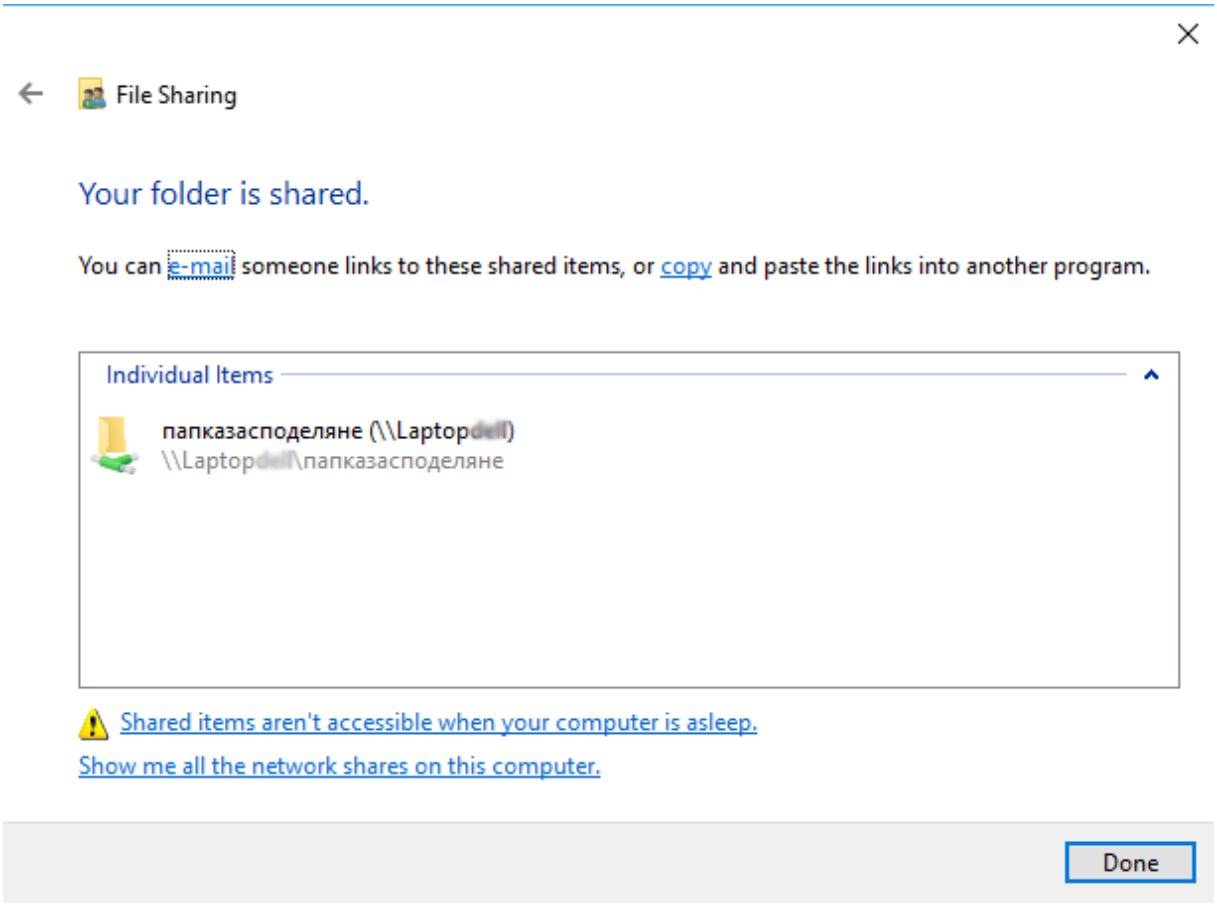
групата *Everyone*. Ако липсва се изписва. Натиска се бутона *Add*. Избраната група трябва да се появи в списъка отдолу.

4. От *Permission Level* се избира нивото на отдаване на ресурса. По подразбиране е *Read* – само за четене, а *Read/Write* добавя и позволение за модифициране и изриване.



фигура 2 *Стъпки 3-4*

5. Потвърждава се с бутона *Share*, след което се появява нов прозорец (фигура 3), указващ начина на изписване на пътя за достъп до папката от компютър в локалната мрежа.

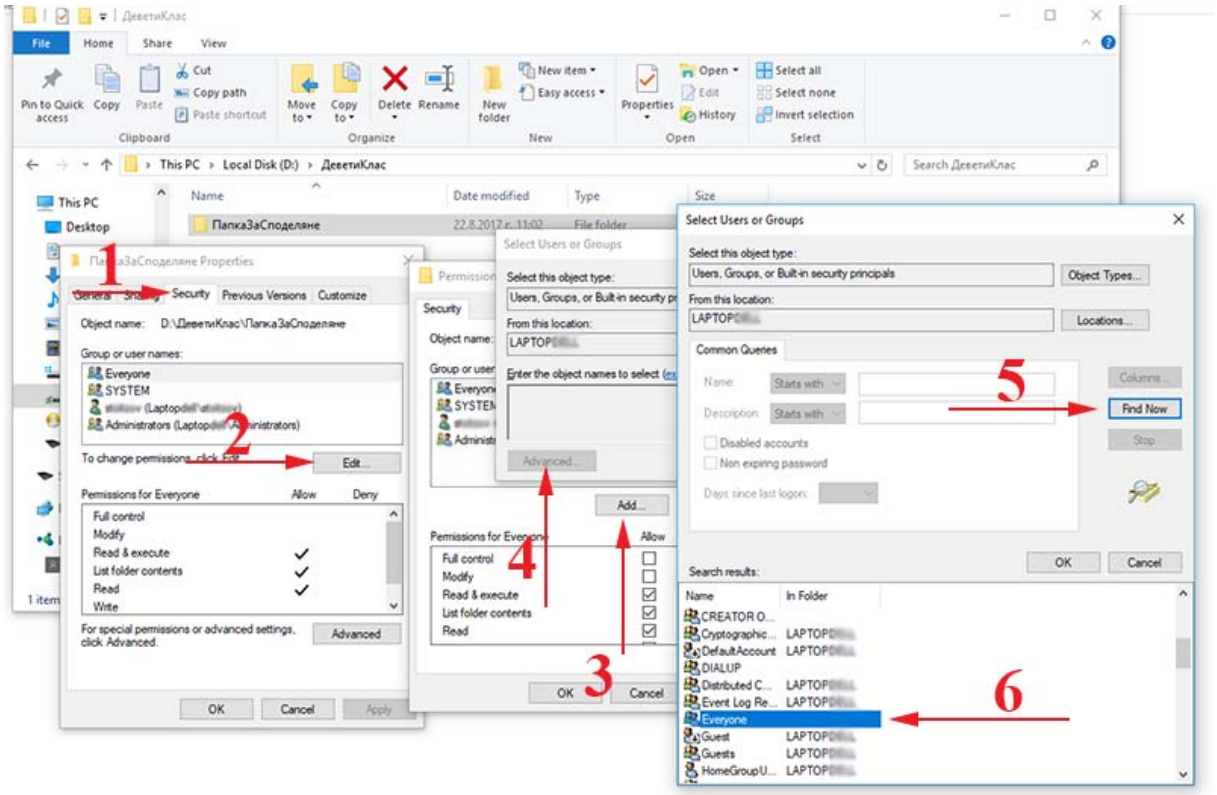


фигура 3 *Стъпка 5*

6. Потвърждението се извършва с бутона *OK*.

Последователността от стъпки за разрешаване на достъпа до споделената папка чрез таба *Security* е показан на фигура 4.

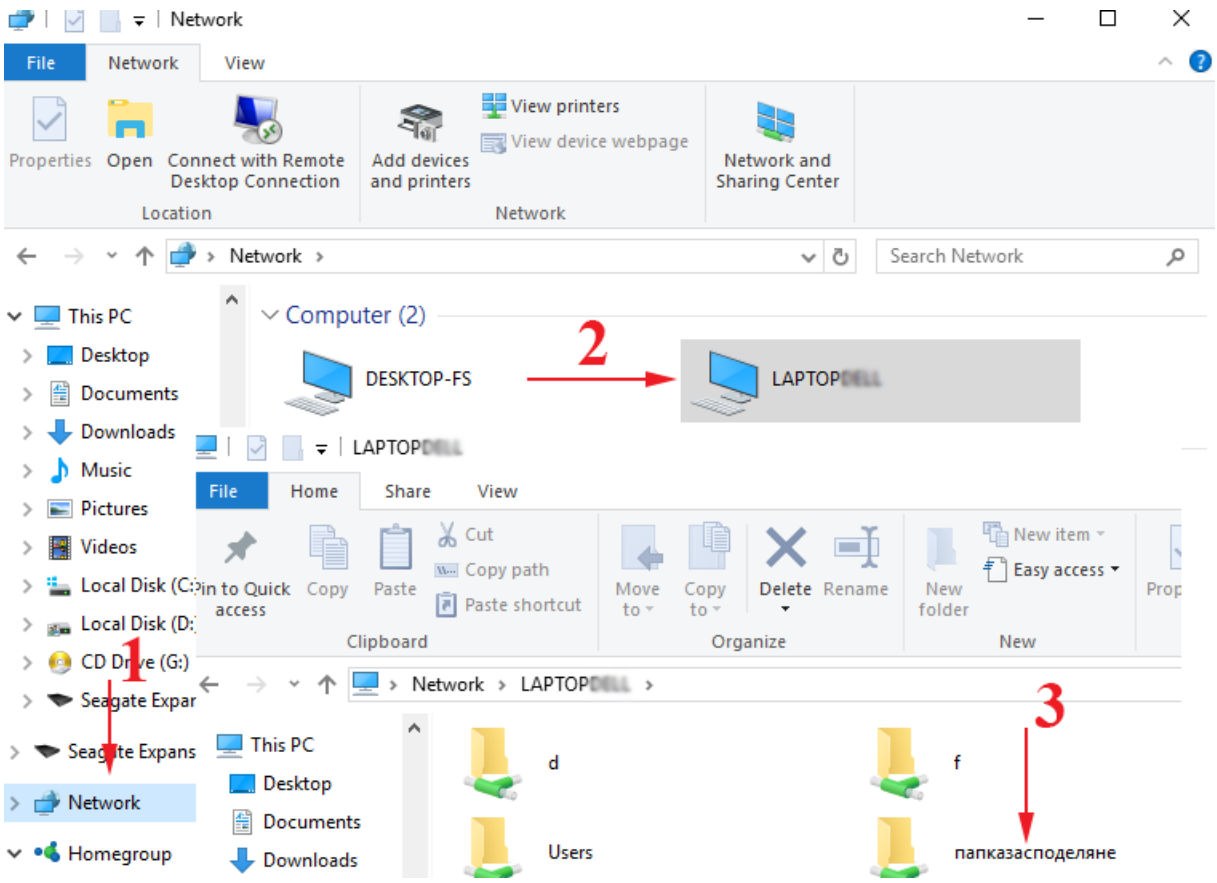
1. Избира се табът *Security* и се проверява дали в предложения списък съществува потребителят или групата, за които е споделена папката. Обикновено при използване на бутона *Share* се извършват и необходимите промени, свързани с разрешението за достъп в секцията *Security*. При липсата на целевия потребител или група в списъка е неоходимо да бъдат добавени чрез бутона *Add*.
2. От серията прозорци с наименование *Select Users or Groups* се избира бутонът *Advanced*, след което *Find Now* за откриване на желания потребител или група и добавянето им към списъка с разрешения.



фигура 4 *Разрешаване на достъпа до споделената папка чрез таба Security*

Достъп до споделената папка през LAN

1. Достъпът до споделения ресурс в локалната мрежа може да се получи, като се стартира *File Explorer* и се избере местоположението *Network*.
2. Избира се желаният компютър от намерените в локалната мрежа, след което се достъпва и желаната папка, в случая *папказасподеляне* (фигура 5).
3. Достъпът до папката може да се осъществи и с изписване на мрежовия път до нея *\\laptopxxxx\папказасподеляне* в позицията за адрес на *File Explorer*.
4. След отваряне на споделената папка, нейното съдържание може да бъде копирано по стандартния начин в друга папка на вашия компютър или модифицирано, ако е разрешено.



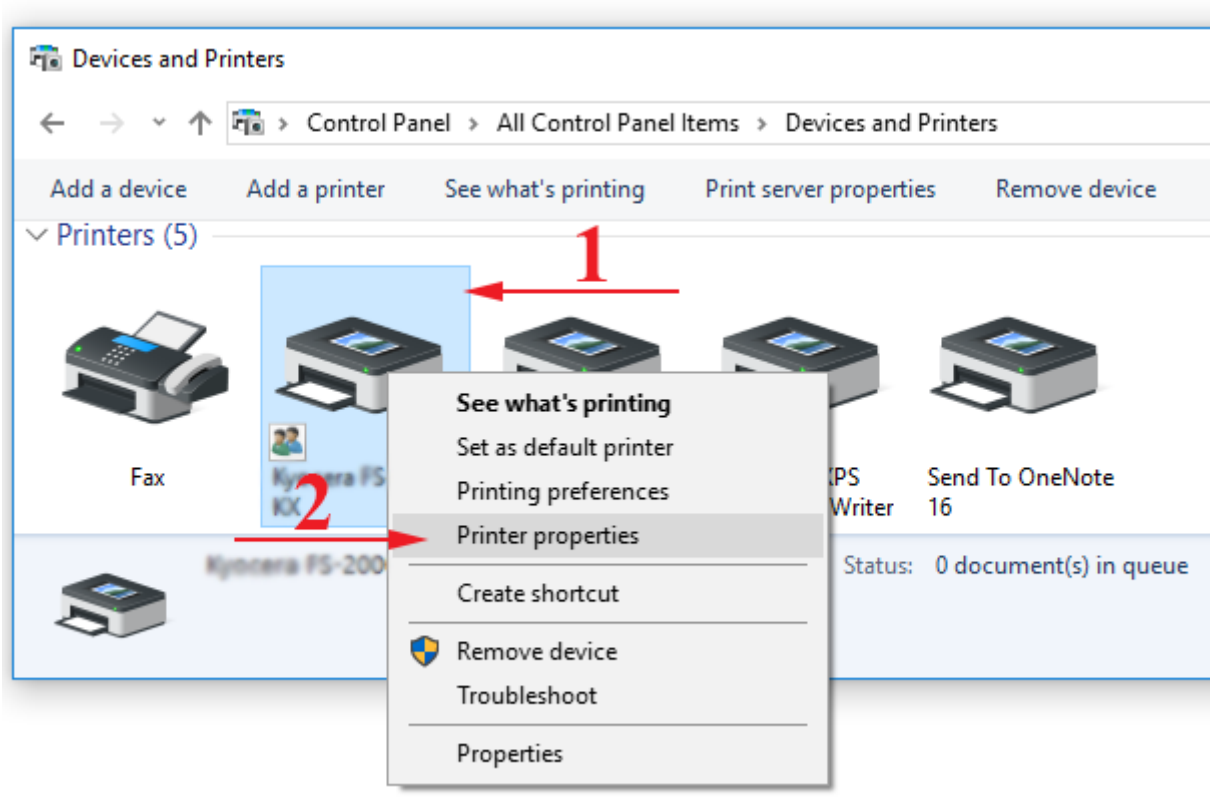
фигура 5 *Стъпка 2*

Използване на мрежов принтер

За да може да се използва един принтер в локалната мрежа, той трябва да бъде инсталиран на определен компютър и споделен, или да притежава мрежов интерфейс за директно свързване към LAN. Това ще позволи на останалите компютри в локалната мрежа да го използват при необходимост.

Процесът на отдаване преминава през следните стъпки:

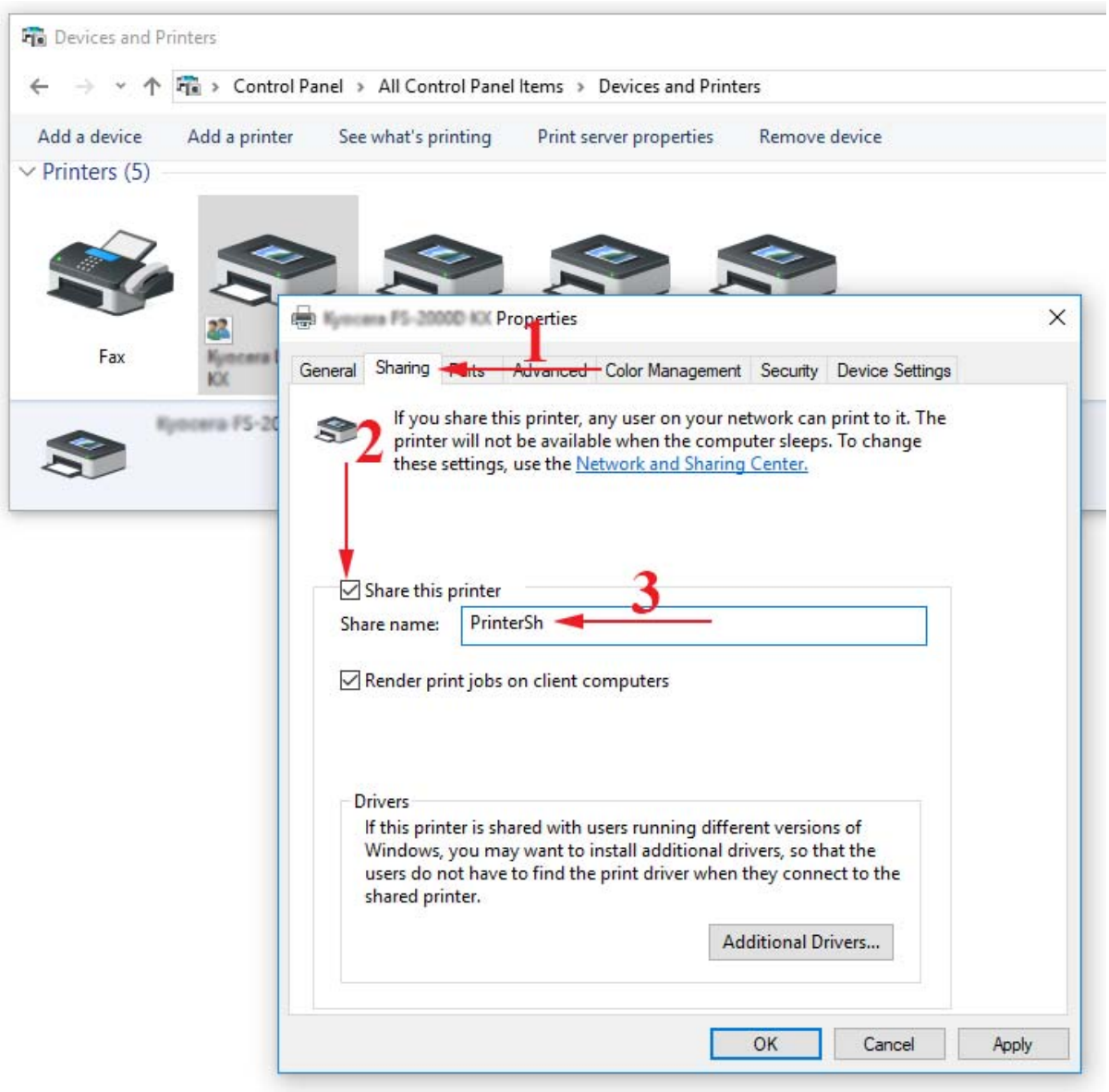
1. Прави се достъп до принтерите чрез последователността *Control Panel/Devices and Printers*. С десен бутон върху желания принтер се избира опцията *Printer properties* (фигура 6).



фигура 6 *Избор на принтер за споделяне*

2. Избира се табът *Sharing* (фигура 6). Поставя се отметка на *Share this printer* и се въвежда името, с което принтерът ще се открива (например *PrinterSh*) в локалната мрежа. Потвърждава се с бутона *OK*.

3. Споделеният принтер се маркира с иконата  .



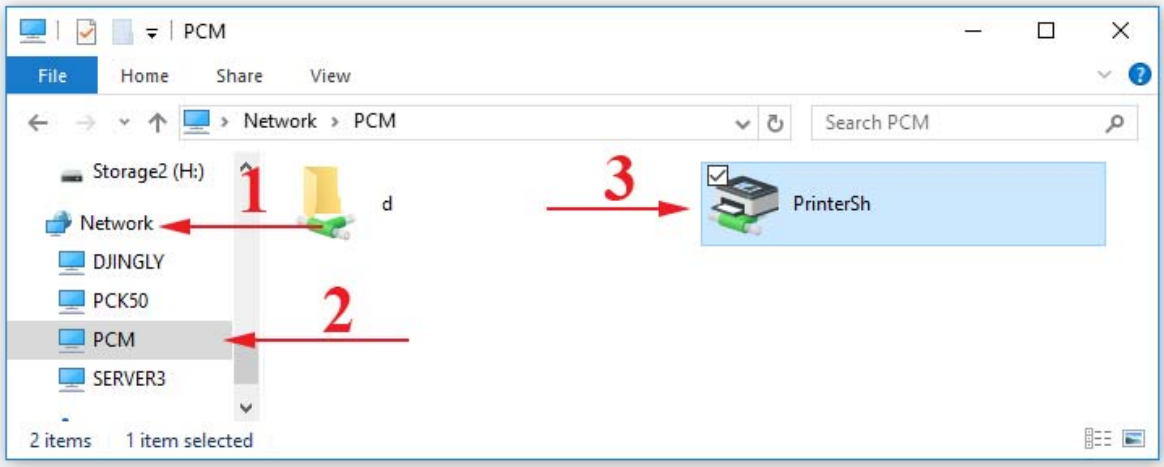
фигура 7 *Споделяне на принтер*

Използване на споделен принтер в LAN

Потребителят, желаещ да използва споделен принтер, първо трябва да е сигурен, че разполага с мрежов вариант на драйвера за този принтер, който се изисква да бъде инсталиран и на неговия компютър. Версията на драйвера трябва да отговаря на инсталираната операционната система на компютъра на потребителя. Възможен е и вариант принтерът вече да е инсталиран. Ако липсва, това може да се направи със следните стъпки:

1. Стартира се *File Explorer* и се избира местоположението *Network*.
2. Избира се компютърът със споделен принтер, след което с левия бутон на мишката се чуква два пъти бързо върху иконата на принтера (фигура 8). Изчаква се докато се инсталира драйвера, след което

принтера трябва да се появи с секцията *Devices and Printers* на *Control Panel*.



фигура 8 *Инсталиране на принтер*

3. Инсталираният вече принтер може да се използва по стандартния начин от всяко приложение, което позволява печат. Едно от необходимите условия за нормално изпълнение на печата е, че отдалеченият компютър със споделения принтер трябва да е включен.

Необходими допълнителни настройки

За правилното функциониране на отдадените устройства, освен описаните по-горе стъпки е необходимо да се маркират и следните допълнителни опции от секцията *Control Panel/Network and Internet/Network and Sharing Center/Change advanced sharing settings*:

1. *Turn on network discovery* – позволява откриването на съществуващи компютри в локалната мрежа.
2. *Turn on file and printer sharing* – разрешава процеса на отдаване на ресурси.
3. *Turn on password protected sharing* – тази опция изисква потребителско име и парола за достъп до ресурса. Опцията *Turn off password protected sharing* премахва необходимостта от парола.

Речник

network operating system (NOS) - - мрежова операционна система

backup – бекъп – резервно копие

Въпроси и задачи

1. Избройте някои мрежови ресурси в LAN.
2. Кои ресурси наричаме споделени?

3. Колко типа LAN мрежи познавате според начина на администрирането им?
4. Посочете някои предимства на мрежите от тип клиент/сървър.
5. Какви нива на сигурност могат да се постигнат при споделяне на ресурси
6. Създайте папка *Тест* на някой от твърдите дискове на вашия компютър. Споделете папката с групата *Everyone* и задайте пълни права за достъп до нея. Направете достъп от друг компютър в мрежата.

6. Защита на информацията в мрежова среда

6.1. Рискове, свързани с работата в мрежова среда

Компютърните мрежи са бъдещето за обмен на информация. Те непрекъснато се развиват и усъвършенстват. Този факт налага необходимостта от сигурна защита на данните от загуба или злоупотреба. Възникват два основни приоритета:

- Защита от отказ и възстановяване;
- Мрежова сигурност.

Защита от отказ и възстановяване

Хардуерните повреди могат да бъдат сериозна причина за загуба на информация, затова е необходимо вземането на определени мерки за защита и възстановяване на данните от сривове. Могат да се предприемат някои препоръчителни действия в тази насока:

- Използване на аварийно захранване за избягване на проблеми с електрозахранването. Често срещан вариант е включването на UPS устройства, които притежават батерии, съхраняващи определено количество заряд, осигуряващо време за работа на системата след прекъсване на основното захранване.
- Архивиране на данните с помощта на програма за архивиране, в случай на повреда на твърд диск или вирусен проблем. Необходимо е осигуряване на допълнително устройства, където да се съхраняват архивираните данни.

Мрежова сигурност

Мрежовата сигурност е основен проблем при използване на мрежова среда. Съществуват немалко случай, свързани с проникване в мрежи на правителствени и бизнес организации, както и сериозни атаки от компютърни вируси в широк мащаб. Терминът **сигурност** се обвързва с необходимите действия, които трябва да се предприемат за защита на един компютър и съдържащата се в него информация. Заплахите могат да бъдат външни и вътрешни.

Външни заплахи

Външните заплахи могат да възникнат, когато локалната мрежа е свързана към друга мрежа, например Интернет. Използват се различни методи на проникване:

1. Неоторизирано използване на чужди потребителски имена и пароли

Всяко лице, което се нуждае от достъп до ресурсите на определена система или мрежа е необходимо да се превърне в неин **потребител** чрез придобиването на акаунт - комбинация от потребителско име (*username*) и парола (*password*), които му осигуряват определени права за достъп до файлове, програми и хардуер. **Паролата** е последователност от букви, цифри и символи и се използва за удостоверяване на правилния потребител. Процесът на получаване на права за достъп до ресурсите на системата или мрежата се нарича **оторизация**. Ако някой използва чужд акаунт без да е упълномощен за това се казва, че е налице неоторизирано използване и е налична предпоставка за нарушаване на сигурността.

2. Атаки от тип отказ на услуга (*Denial of Service, DoS*)

Тези атаки целят прекъсване на установена връзка или възпрепятстване на създаването на такава към мрежата. Те не предизвикват срив в системата, а наводняват мрежата с непотребни пакети или симулират мрежов проблем, който прекъсва комуникацията.

3. IP спуфинг

При този подход се променя IP адреса на подателя в изпращаните пакетите, така че да изглежда, че са генерирани от сигурен източник. Получателят не знае това и насочва отговорите на приетите заявки към хоста, съответстващ на заложения IP адрес.

DoS атаките често използват този подход за претоварване на мрежата и устройствата с подправени пакети.

4. Компютърни вируси и червеи

Компютърните вируси са самовъзпроизвеждащи се програми, които могат да се разпространяват от една система на друга чрез прикрепяне на кода им към различни файлове, без съгласието или знанието на потребителя. Някои от тях са безобидни и досадни (например извеждат съобщения на екрана). Други са злонамерени и се стремят към унищожаване на файлове (програми, данни).

Червеят е самовъзпроизвеждащ се вирус, който използва мрежата, за да разпраща свои копия до крайните устройства. За разлика от вируса, компютърният червей не се нуждае от прикачване към вече съществуваща програма. Разпространява се като прикрепен файлов към електронната поща, като изпълними файлове, като HTML страници, съдържащи скриптове, или като документи с макроси.

5. Троянски коне

Това са злонамерени програми, представящи себе си като полезен софтуер с цел, събиране на важна информация и изпращане на атакуващия или отваряне на вратичка в сигурността на атакуваната система. Например лъжлив екран за логване в системата, кражба на поверителни данни (пароли, информация за банкови сметки и кредитни карти), контрол над системата и др.

Вътрешни заплахи

Вътрешните заплахи са тези, които могат да се извършат директно върху избрана система или през локалната мрежа. Мотивите за подобни пробиви в сигурността могат да бъдат свързани с корпоративен шпионаж, недоволни служители или случайни (непланирани) попадения.

Мерки за сигурност

Външните и вътрешните заплахи могат да бъдат избегнати при прилагане на определени мерки за сигурност, като:

1. Използване на операционни системи с висока степен на сигурност.

Съвременните операционни системи удовлетворяват това изискване. Например разновидностите на Windows или Linux очакват въвеждането на валидно потребителско име и парола, за да позволят зареждане и работа със системата. Съхранението на паролите е във вид, неудобен за осъществяване на лесен достъп до тях.

2. Автентикация и идентификация

Автентикацията е процес на удостоверяване на правилния потребител. В качеството на синоним на термина автентификация понякога се използва термина "проверка на идентичност". Идентификацията позволява на

субекта да назове себе си. За целта се използват различни идентификатори, като парола, личен идентификационен номер, криптографски ключ и др.

Например правилността на паролата за определено потребителско име гарантира, че потребителят е автентичен.

Друг често използван идентификатор за удостоверяване на самоличността на регистриран вече потребител на даден уебсайт, като част от процеса на влизане, е използването на „бисквитки“ (cookies). Те могат да спестят повторно въвеждане на потребителско име и парола при всеки следващ достъп до този сайт. Представляват текстови данни, които се съхраняват на клиентската система, обвързват се с конкретен браузър и сайт, и съдържат информация, която браузъра изпраща към сървъра при всяка негова заявка. Бисквитките имат различен период на валидност, от временни файлове, съществуващи до момента на напускане на уебсайта или деактивирате на използвания уеб браузър, до запазени за указан срок.

3. Криптиране на данните

Криптирането на данните е технология, базирана на науката криптография. Криптирането използва код или ключ за разбъркване (шифриране) и след това за подреждане (дешифриране) на данните, с цел представянето им в първоначалната им форма. Данните се криптират с помощта на алгоритъм или шифър.

4. Използване на защитна стена (Firewalls) и прокси сървър

Защитната стена филтрира входящите и изходящите пакети и определя дали да разреши преминаването на даден пакет. Тя се настройва от администратора на мрежата и обикновено се разполага на шлюза (*gateway*) на мрежата.

Прокси сървърът функционира като посредник между системите от вътрешната мрежа и тези от външната. Например една от функциите на такъв сървър е свързана с кеширане (съхраняване) на Web страници за подобряване на качеството на Web услугата.

5. Използване на антивирусен софтуер

В днешно време е задължително използването на антивирусни програми за защита на системата от вируси. Антивирусният софтуер

открива вирусни инфекции, сигнализира за тях и се опитва да предотврати евентуални техни поражения.

6. Ограничаване на физическия достъп

Тази стъпка е свързана с определяне на степента на директен физически достъп на лица до ресурсите на мрежата. При висока степен на сигурност сървърите и устройствата за връзка трябва да се поставят в зони без достъп на физически лица, освен упълномощените за това. Работните станции, които се намират в незащитени райони трябва да ограничават по софтуерен начин достъпа до важните данни в мрежата.

Основни нормативни документи

Съвременното общество и свързаните с него обществено-икономически реалности са пряко обвързани с компютърните технологии и тяхното динамично развитие. Този факт поражда значими юридически проблеми, свързани с правната регламентация на софтуера, базите данни и защитата им като интелектуални продукти. Филипините са първата страна в света, включила през 1972 г в авторското си право компютърните програми. През 1980 г. в САЩ също се приема закон за Авторското право върху компютърните програми. Подобни стъпки се правят във Франция и Германия. През 1991 г. Съветът на Европейските общности издава Европейската директива за правна защита на компютърните програми.

Българският Закон за авторското право и сродните му права (ЗАПСП) също разглежда компютърните програми и базите данни като обекти на авторско право и съдържа текстове, свързани със закрилата им от използване, копиране и разпространение.

Минималното ниво на технически и организационни мерки при обработване на лични данни и допустимия вид защита са определени от Комисията за защита на личните данни в Наредба № 1 от 30.01.2013 г. Тя разглежда защитата на автоматизираните информационни системи и/или мрежи като система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни.

Условията и реда за предоставяне на удостоверителни услуги чрез електронни документи и електронен подпис са описани в Закона за електронния документ и електронния подпис.

Основни принципи, гарантиращи сигурността на информацията

Представените мерки за сигурност имат за цел да запазят основните принципи, свързани с гарантиране на сигурността на информацията:

- предотвратяване на неупълномощен достъп до данните и ресурсите на системата и мрежата.
- запазване на конфиденциалността (поверителността) и целостта на информацията, което означава, че тя може да бъде използвана и променяна само от упълномощени потребители.
- осигуряване на непрекъснат достъп за упълномощените потребители.
- използване на стандартизирани решения за защита, базирани на международни стандарти и протоколи за сигурност.

Основни начини и средства за защита на мрежата от неоторизиран достъп

Осъществяването на мерките за сигурност може да бъде постигнато по различни начини и с различни средства. Те могат да бъдат реализирани софтуерно или хардуерно, а понякога и като комбинация от двата подхода.

1. Поддържане на потребители с различни нива на достъп

Поддържането на множество потребители от една операционна или уеб система е възможност, която позволява използването на потребителски акаунти за осъществяване на достъп до системата или мрежата. Процесът на оторизация задава правомощията на всеки потребител, което води до ограничаване на действията му до позволените за него, с което определя неговото **ниво на достъп**. Например Windows 10 предлага възможност за създаването и използването на два типа акаунти, осигуряващи различни нива на достъп:

- Администраторски (*Administrator)*, позволяващ пълен контрол над компютъра и достъп до всички програми, настройки, файлове и др. Могат да се създават или премахват други потребителски акаунти, да се извършват настройки на операционната система, да се инсталират/деинсталират софтуерни и хардуерни компоненти.
- Стандартен (*Standard*), който ограничава потребителя до използване на софтуер и възможността да прави промени, които не указват

въздействие върху другите потребители или сигурността на системата.

2. Използване на сигурни пароли

Важна част от всеки план за сигурност е използването на колкото е възможно по сложна парола. Когато се налага потребител да избира парола сигурните системи налагат някои изисквания (политики), като:

- Паролите не трябва да бъдат думи или числа, които лесно да бъдат отгатнати поради тяхната връзка с потребителя (например име, фамилия, рождена дата и др.).
- Паролата трябва да бъде лесна за запомняне от потребителя, за да не се записва някъде.
- Повечето системи, поддържащи пароли, правят разлика между главна и малка буква. Използването на комбинация от тях създава по-сигурна парола (например AlExooTr).
- По-голямата дължина на паролата и включването на специални символи я прави по-сигурна (например AlEx!2#ooTr).
- В среда с висока сигурност потребителите е необходимо да се задължават да сменят паролата на определен период от време, като новата не трябва да прилича на старата.

3. Криптиране на файлове

Криптирането на файлове е операция, която шифрира съдържанието на файловете и ги запазва във вид, който не може да бъде прочетен от друг, освен от създателя им. За правилното им разчитане е необходим ключ, който притежава само собственика им. Например Windows 10 предлага такава възможност от контекстното меню на избран файл чрез последователността от стъпки *Properties/Advanced/Encrypt contents to secure data*.

4. Използване на криптиращи протоколи

Криптиращите протоколи са необходими за защита на данните при пренос по мрежата. Съществуват различни реализации на такива протоколи. Например TLS (*Transport Layer Security*) и неговият предшественик SSL (Secure Sockets Layer) са криптиращи протоколи, осигуряващи сигурност на комуникацията по Интернет. Уебсайтовете, които използват криптирана връзка със SSL или TLS имат URL с префикс "https:", вместо "http:".

5. Използване на електронен (цифров) подпис

Електронният подпис замества стандартния подпис при подписване на електронни документи. Той е електронен, криптиран печат за потвърждаване, че изпращаната цифрова информация идва от подписващия и не е изменена. Цифровият подпис не криптира данните, а помага да се гарантира:

- Автентичност – потвърждава, че подписващият е този, за когото се представя.
- Цялост - гарантира, че съдържанието не е променено или манипулирано след цифровото подписване на документа.
- Невъзможност за отричане от страна на подписалия – доказва произходът на едно подписано електронно съдържание.

6. Сигурност на електронната поща

Електронната поща може да бъде достъпна за потребителите чрез уеб приложение или пощенски клиентски софтуер, инсталиран на използваната система (например Windows Mail). Препоръчително е при изпращане или получаване на съобщение да се осигури връзка чрез криптиращи протоколи. Почти всички уеб варианти за електронна поща в момента поддържат такъв тип връзка. Може да се разпознае по URL префикса "https:". Пощенският клиентски софтуер също дава възможност за използване на криптиране, което се задава при настройка на опциите на пощенския акаунт, стига да бъде поддържано от доставчика на услугата. Допълнително и в двата варианта може да се използва електронен подпис за доказване на автентичността на съобщението.

При използване на електронна поща е препоръчително спазването на следните съвети:

- Да не се отварят електронни съобщения ако подателят липсва, не е разпознат или полето за подател съдържа данни на получателя;
- Да се игнорират съобщения, съдържащи само хипервръзки.

7. Поддържане на актуални версии на софтуерните продукти

Актуалните версии на използвания софтуер разрешават проблема с открити бъгове, които могат да се окажат предпоставка за нарушаване на

сигурността на системата. Препоръчително е да се извършва актуализация на инсталираните програми. Обновяването на антивирусния софтуер и ъпдейтите на операционната система трябва да се извършват периодично, а там където е възможно и автоматично.

8. Контролиране на достъпа до мрежата чрез защитни стени

За контролиране на достъпа до мрежата могат да се използват защитни стени, които да са подчинени на планирани правила за защита спрямо потока от данни, който трябва да бъде разрешен. Възможно е внедряването им и в локалната мрежа за създаване на безопасност при съвместна работа на различни отдели, офиси и групи от една и съща организация. Те могат да бъдат реализирани софтуерно или да комбинират хардуерни и софтуерни решения. Софтуерните защитни стени могат да бъдат инсталирани на всеки персонален компютър, за да го защитават, докато хардуерните са предназначени за защита на мрежата. Обикновено, когато една програма се опита да осъществи достъп до Интернет за първи път, софтуерните защитни стени питат дали да и разрешат достъп. Защитната стена не може да защити от вирусна атака.

Задаване права на достъп до ресурси в локална мрежа в среда Windows 10

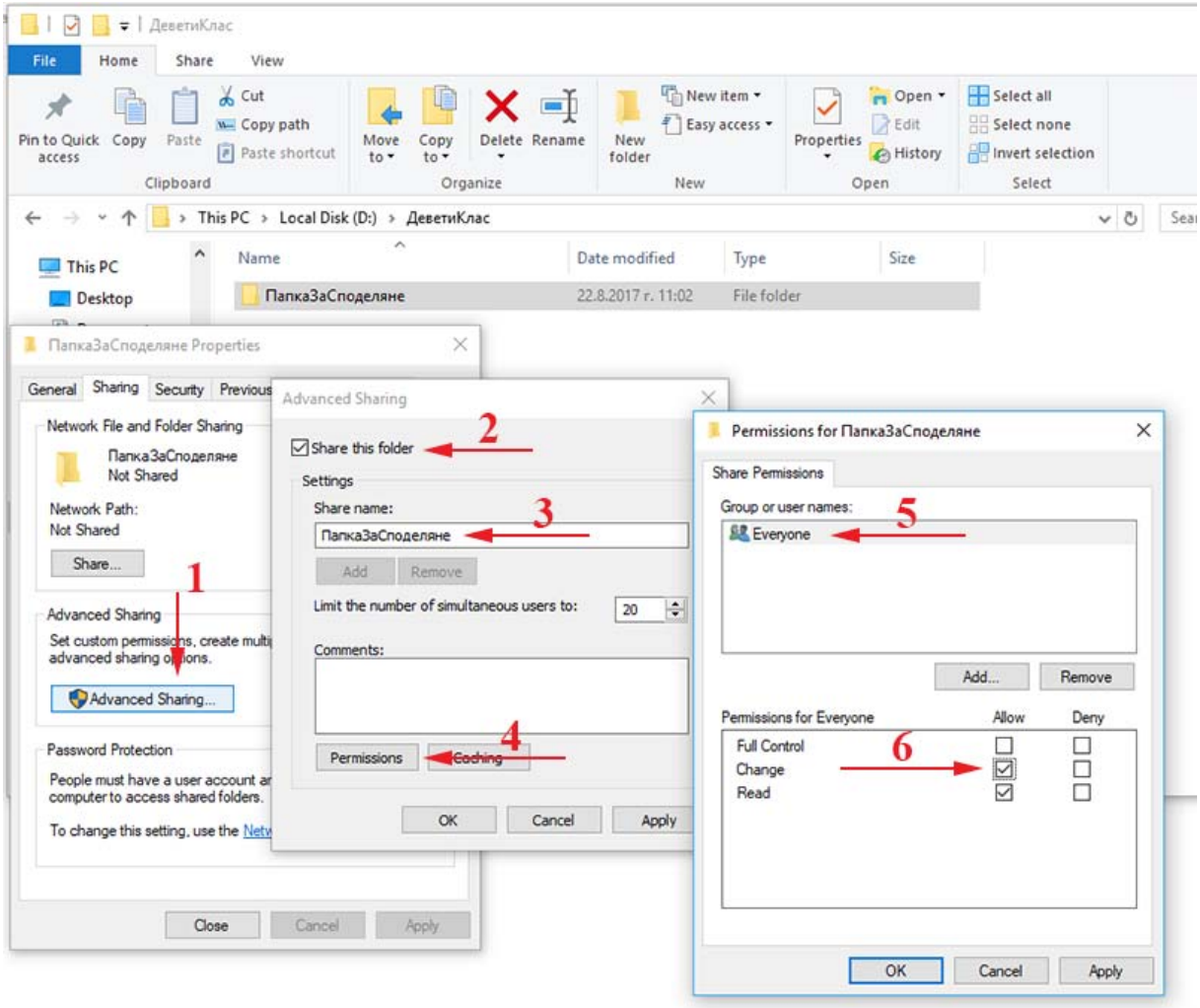
В предишния урок беше представена последователност от стъпки за споделяне на папка и принтер в средата на операционната система Windows 10. В стъпка 4 беше коментирана възможността за избор на ниво на позволение между предложените опции *Read* (само за четене, по подразбиране) и *Read/Write* (с добавяне на позволение за модифициране и изриване).

Съществува вариант за отдаване на ресурса (папката) с използването на бутона *Advanced Sharing* (фигура 1). Този бутон отваря нов прозорец, в който трябва да се сложи отметка на опцията *Share this folder* и да се посочи име, с което се отдава ресурсът (например *ПапкаЗаСподеляне*). С бутона *Permissions* се задава групата или отделен потребител, с който се споделя ресурса. В този пример това е подразбиращата се група *Everyone*, за която е поставена и отметка за модифициране на документа (*Change*) в колонката *Allow*. Възможните опции за избор са:

- *Read* – позволява да се виждат имената на отделните папки, файловете и техните атрибути, да се стартират програми, да се копират файлове.

- *Change* – включва всички привилегии от *Read* като допълва позволения за: създаване на папки, добавяне на файлове към папки, модифициране на съдържанието във файловете, изтриване на файлове или папки.

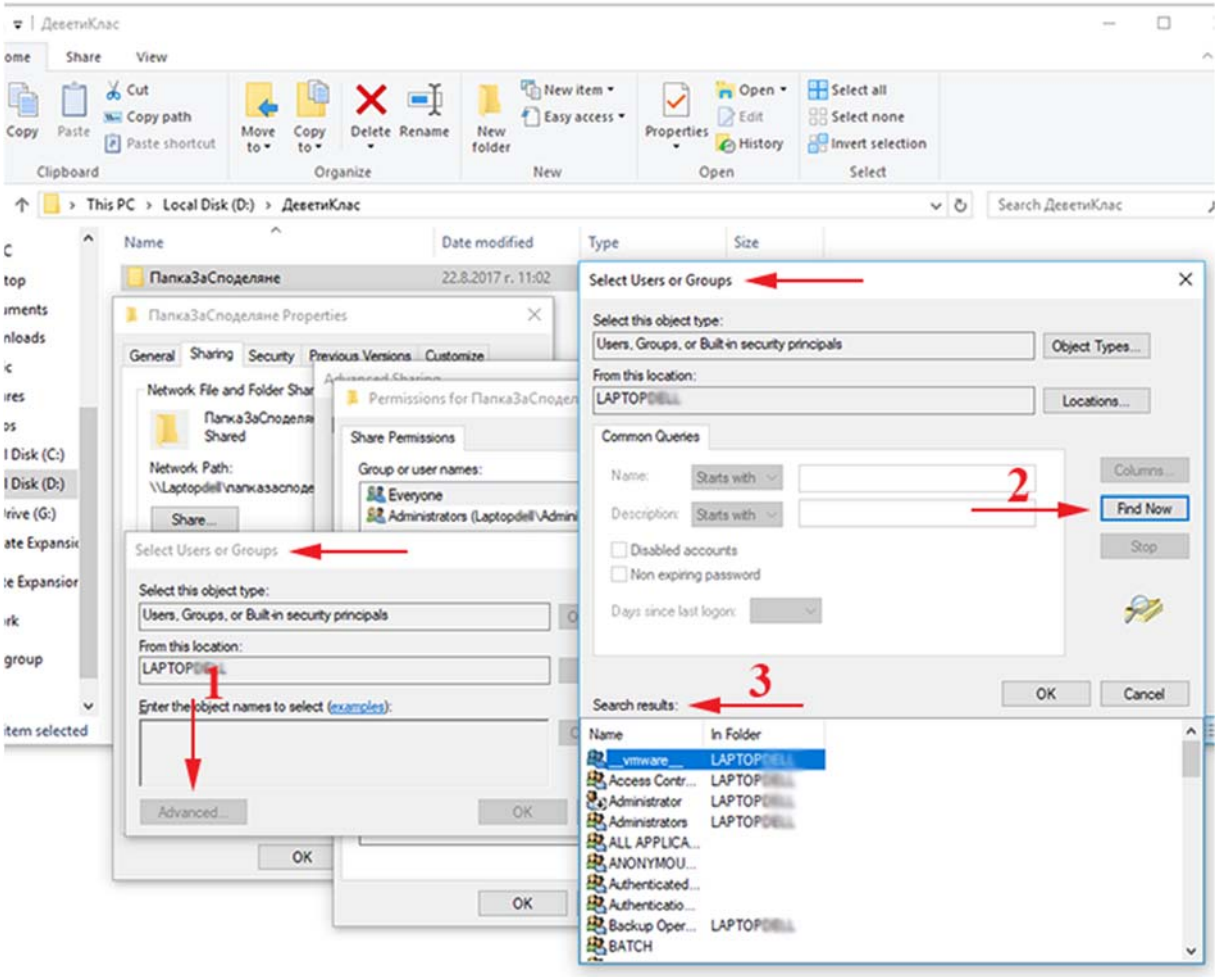
- *Full Control* – включва всички привилегии от *Change* като добавя възможности за промяна на позволения за файлове и вземане на собствеността върху тях.



фигура 1 *Използване на* ***Advanced Sharing***

Друг потребител или група може да се добави от бутона *Add*. От серията прозорци с наименование *Select Users or Groups* (фигура 2) се избира

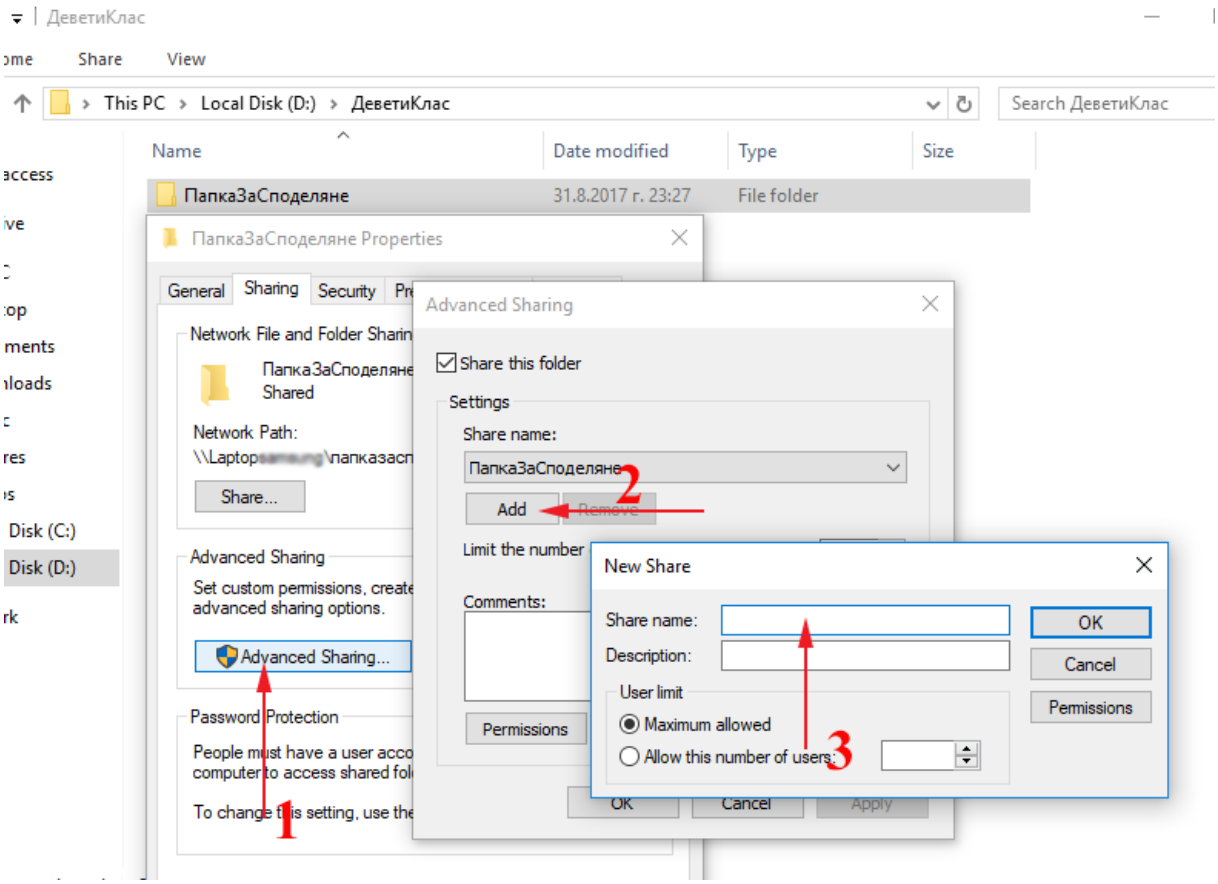
бутонът *Advanced*, след което *Find Now*. В получените резултати са предложени всички възможни варианти за избор.



фигура 2 *Добавяне на друг потребител или група*

Използването на опцията *Advanced Sharing* не извършва модификации в секцията *Security*, свързани с целевата група или потребител, затова е необходимо те да се направят допълнително и да са съобразени с предварително зададените права.

Windows 10 позволява и възможност за отдаване на даден ресурс под различни имена с различни позволения за достъп за различните потребители и групи. За извършване на това действие е необходимо да се използва бутона *Add* от прозореца *Advanced Sharing*, показан на фигура 3.



фигура 3 *Отдаване на ресурс под различно име*

Някои действия и съвети, свързани с управлението на споделените ресурси и задаването на позволения за тях, могат да бъдат представени по следния начин:

- Определят се потребителите, групите и техните позволения за необходимите им ресурси.
- Възможността за обединяване на потребители в групи улеснява процеса по задаване на позволения върху споделените ресурси.
- Позволенията трябва да се задават пестеливо.
- Ресурсите се организират така, че папки имащи еднакви изисквания за сигурност, да бъдат разположени в обща папка, след което само тя да бъде споделена.
- Назначените имена на споделените ресурси трябва да осигуряват лесното им разпознаване и намиране от потребителите, както и да се поддържат от всички операционни системи.

Въпроси и задачи

1. Какви рискове съществуват при работа с мрежова среда?
2. Кои са основните приоритети, свързани с опазване на данните при работа в мрежова среда?
3. Избройте някои външни заплахи за сигурността в мрежова среда?
4. Какви мерки за сигурност могат да се предприемат за предотвратяване на вътрешна заплаха срещу индивидуална система?
5. Какво означава криптиране на данните?
6. Каква е ролята на защитните стени?
7. Посочете начини и средства за защита на мрежата от неоторизиран достъп?
8. За какво служи електронният подпис?

7. Споделяне на файлове и папки в локална мрежа - упражнение

За изпълнението на това упражнение е необходимо да разполагате с администраторски права за акаунта Ви или да присъства преподавател, който знае администраторската парола.

Задача 1. Създайте папка *SharedFolder* на избрано от Вас устройство. Открийте съществуващи ***.pdf** файлове и копирайте няколко от тях в новосъздадената папка. Изпълнете следните действия:

- Прегледайте таба *Sharing* и *Security* от опцията *Properties* на контекстното меню на създадената папка. Коментирайте съществуващите позволения (Permissions).
- Използвайте бутона *Share* от таба *Sharing* и споделете папката с групата *Everyone* с позволение за четене и запис. Прегледайте отново нейните два таба *Sharing* и *Security* и коментирайте измененията.

Задача 2. Научете името на компютъра си (или IP адреса му) и се опитайте да достъпите новосъздадената папка със съдействието на съученика си от съседния за Вас компютър. За целта стартирайте File Explorer и използвайте един от посочените начините за достъп до нея:

- изберете местоположението Network, след което потърсете името на Вашия компютър, където би трябвало да се намира споделената от Вас папка и направете достъп до него;
- задайте в полето за адрес мрежовия път до споделената от Вас папка по следния начин:
    - **\\Име-на-компютър\име-на-споделена-папка**
    - **\\IP-адрес-на-компютър\име-на-споделена-папка**

Опитайте се да преименувате файл от нея. Копирайте папката с нейното съдържание на компютъра, откъдето е направен достъпът. Коментирайте резултатите от извършените действия.

Задача 3. Създайте документ на Word и го запишете в папката *SharedFolder*. Направете достъп до него от съседния компютър. Опитайте да

го отворите, модифицирате и запишете. Коментирайте резултатите от извършените действия.

Задача 4. Създайте подпапка на папката *SharedFolder* с избрано от Вас име. Копирайте в нея създадения документ на Word. Изпълнете следните действия:

- Направете достъп до него от съседния компютър. Опитайте да го отворите, модифицирате и запишете. Коментирайте резултатите от извършените действия.
- Използвайте бутона *Share* от таба *Sharing* и променете позволението за достъп до подпапката за групата *Everyone* само за четене. Направете отново достъп до документа в тази подпапка от съседния компютър. Опитайте да го отворите, модифицирате и запишете. Коментирайте резултатите от извършените действия.