4. Споделяне на ресурси в локална мрежа

4.1.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.

Пример за такава организация е Active Directory на Microsoft. Active Directory предоставя, както логически, така и физически структури за мрежови компоненти. Логическите структури са:

- Домейн (Domains) - група от компютри, които споделят обща директорийна база за данни;
- Организационни единици (Organizational units) - подгрупа в домейна, която често прави огледален образ на бизнеса на организацията или функционалната структура;
- Дървета от домейни (Domain trees) - един или повече домейни, които споделят непрекъснато пространство от имена;
- Гори от домейни (Domain forests) - едно или повече дървета от домейни, споделящи обща директорийна информация.
- Физическите структури са
- Мрежи (Subnets) - мрежова група със специфичен диапазон от IP адреси и мрежова маска;
- Сайтове (Sites) - една или повече подмрежи; използват се за конфигуриране на достъпа до директории и тяхното репликиране.

Логическите структури помагат за организиране на директорийни обекти, както и за управление на мрежови акаунти и споделени ресурси.

Домейнът представлява просто група от компютри, споделящи обща директорийна (справочна) база данни (directory database). Имената на АД домейните трябва да са уникални. Всеки домейн има собствени политики за сигурност и отношения на доверие (trust relationships) с други домейни. Домейните също така могат да се разпростират на повече от едно физическо местоположение, което ще рече, че даден домейн би могъл да се състои от множество сайтове, а тези сайтове биха могли да имат множество

подмрежи. В директорийната база данни на един домейн се намират обекти, дефиниращи акаунти за потребители, групи и компютри, както и споделени ресурси, като например принтери и папки.

Когато един или повече домейни споделят едни и същи директорийни (сиравочни) данни, те се наричат гора (forest).

Когато домейните имат структура от непрекъснати имена, за тях се казва, че са в същото домейново дърво (domain tree).

Ако домейните в една гора имат прекъснати DNS имена, тогава те формират отделни домейнови дървета в тази гора. Една домейнова гора може да има едно или няколко домейнови дървета.

Организационните единици са подгрупи в домейните, които подгрупи често създават огледален образ на функционалната или бизнес структура на дадена организация. Може да се мисли за организационните единици и като за логически контейнери, в които може да се поставят акаунти, споделени ресурси и други организационни единици. Организационните единици са много полезни при организирането на обектите спрямо бизнес и ли функционалната структура на организацията и още:

- Организационните единици позволяват назначаването на групова политика на малък набор от ресурси в даден домейн, без да се прилагат тази политика към целия домейн.
- Организационните единици създават по-малки и по-лесни за управление изгледи на директорийни обекти в даден домейн. Това помага за по-ефективното управление на ресурсите.
- Организационните единици позволяват делегирането на власт и лесно контролиране на административния достъп до ресурсите на домейна. Това помага за управление на обхвата на администраторските привилегии в домейна. Може да се даде на потребител А административна власт за една организационна единица, но не и за други и т.н.

Сайтът е група от компютри в една или повече IP подмрежи. Сайтовете се използват за създаване на съпоставяния за физическата структура на вашата мрежа. Съпоставянията на сайтове са независими от логическите домейнови структури, поради което не е необходимо непременно да съществува връзка между физическата структура на мрежата и нейната логическа домейнова структура.

Подмрежата може да се разглежда като група от мрежови адреси. За разлика от сайтовете, които могат да имат множество диапазони от IP адреси, подмрежите имат специфичен диапазон от IP адреси и мрежова маска във формат мрежа/маскирани битове (например 192.168.19.0/24).

Компютрите се причисляват към сайтове на база тяхното местоположение в подмрежата или набор от подмрежи. Ако компютрите в подмрежите могат да комуникират ефективно един с друг по мрежата, за тях се казва, че са добре свързани (well connected). В идеалния случай сайтовете се състоят от подмрежи и компютри, които са добре свързани. Ако подмрежите и компютрите не са добре свързани, може да се наложи създаването на множество сайтове. Доброто свързване дава на сайтовете няколко преимущества:

- Когато клиентите влизат в домейн, процесът на автентикация най-напред търси домейн контролери, намиращи се в същия сайт като клиента. Това означава, че ако е възможно, най-напред се използват локални домейн контролери, което пък локализира мрежовия трафик и може да ускори процеса на автентикация.
- Директорийната информация се репликира по-често вътре в сайтовете, отколкото между тях. Това намалява натоварването на мрежата, причинено от репликирането, като същевременно гарантира, че локалните домейн контролери получават бързо актуална информация. Можете също така да се укаже как да се репликира директорийната информация, като се използват сайтови връзки (site links).

Групови политики

Груповата политика може да се разглежда като набор от правила, които помагат при управлението на потребители и компютри. Груповите политики може да се прилагат към множество домейни, към индивидуални домейни, към подгрупи в даден домейн или към индивидуални системи. Политиките, които се прилагат върху индивидуални системи, се наричат локални групови политики(local group policies) и се съхраняват само на локалната система. Други групови политики са свързани като обекти в директорийната услуга Active Directory.

Group policy настройките се съхраняват в обекти за групови политики (Group — GPOs). GPO е като контейнер, предназначен за прилаганите от вас политики и техните настройки. GPO обекти могат да се прилагат към един сайт, домейн или организационна единица. При наследяването една политика, приложена върху родителски контейнер, се наследява от дъщерен

контейнер. По същество това означава, че дадена настройка на политика, приложена към родителски обект, се предава надолу към дъщерния обект. Например, ако прилагате настройка на политика в домейн, тази настройка се наследява от организационните единици в домейна. В този случай GPO обектът за домейна е родителският обект, а GPO обектите за организационните единици са дъщерните обекти.

Редът на наследяването е следният:

Сайт->Домейн-> Организационна единица

Това означава, че настройките на груповите политики за даден сайт се предават надолу към домейните в сайта, а настройките за даден домейн се предават надолу към организационните единици в този домейн. Допуска се и разрешаване на предефиниране на наследяването.

Последователност за прилагане на групови политики:

1. Локални ГП;
2. Групови политики на сайтове;
3. Групови политики на домейни;
4. Групови политики на ОЕ;
5. Дъщерни групови политики на ОЕ;

Груповите политики се разделят на две големи категории:

- Такива, които се прилагат на компютри – прилагат се при стартиране на системата.
- Такива, които се прилагат за потребители – прилагат се при логване на потребител в системата.

4.2.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.

За улесняване на администрирането се поддържат обикновено два типа акаунти – потребителски и групов. Потребителските акаунти (user accounts) се използват, за да се разреши на индивидуални потребители да влизат в мрежата и да осъществяват достъп до мрежовите ресурси. Груповите акаунти (group accounts) се използват за управление на ресурси за множество потребители. Позволенията и привилегиите, които са назначени на потребителските и груповите акаунти, определят кои действия могат да бъдат изпълнявани от съответните потребители, както и до кои компютърни системи и ресурси те могат да осъществяват достъп.

Потребителските акаунти са предназначени за отделни хора. Груповите акаунти са предназначени да улесняване администрирането на множество потребители.

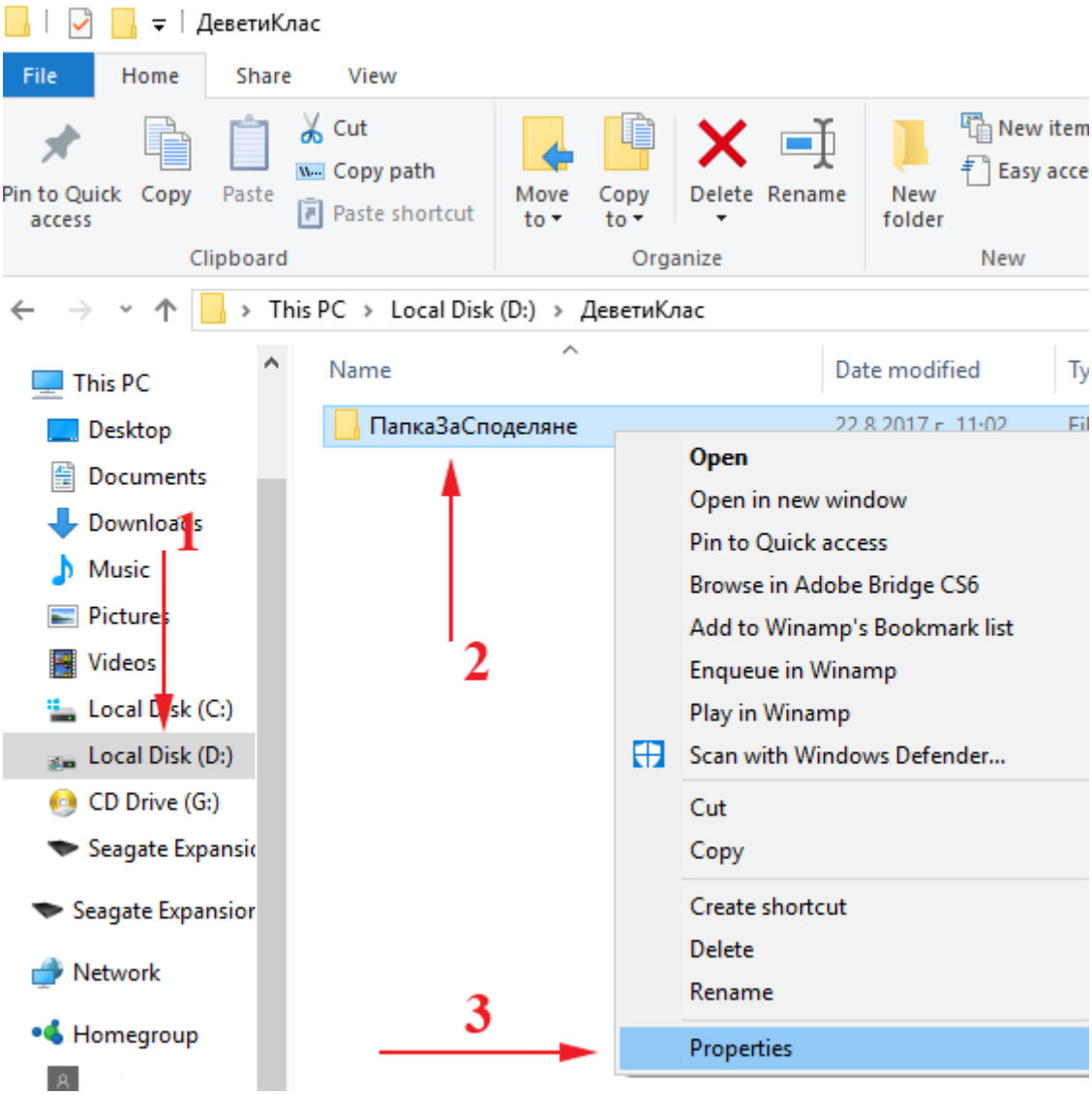
- Домейнови потребителски акаунти - Потребителските акаунти, дефинирани в Active Directory, се наричат домейнови потребителски акаунти (domain user accounts). С помощта на Single Sign-On, домейновите потребителски акаунти могат да осъществяват достъп до ресурси из целия домейн.
- Локални потребителски акаунти - Потребителските акаунти, дефинирани на локален компютър, се наричат локални потребителски акаунти (user accounts). Тези акаунти имат достъп само до локалния компютър, така че преди да могат да осъществят достъп до мрежови ресурси, те трябва да се автентицират.

В този случай обикновено автентикацията се реализирана като процес от две части. Този процес се състои от интерактивно влизане и мрежова

автентикация. Когато даден потребител влиза в компютър, интерактивният logon процес автентицира влизането на потребителя, което потвърждава идентичността на потребителя пред локалния компютър и дава достъп до директорийната услуга Active Directory. От тук нататък, когато потребителят се опитва да осъществява достъп до мрежови ресурси, за определяне на това, дали той има позволение да го направи, се използва мрежова автентикация.

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*.



фигура 1 *Стъпки 1-2*

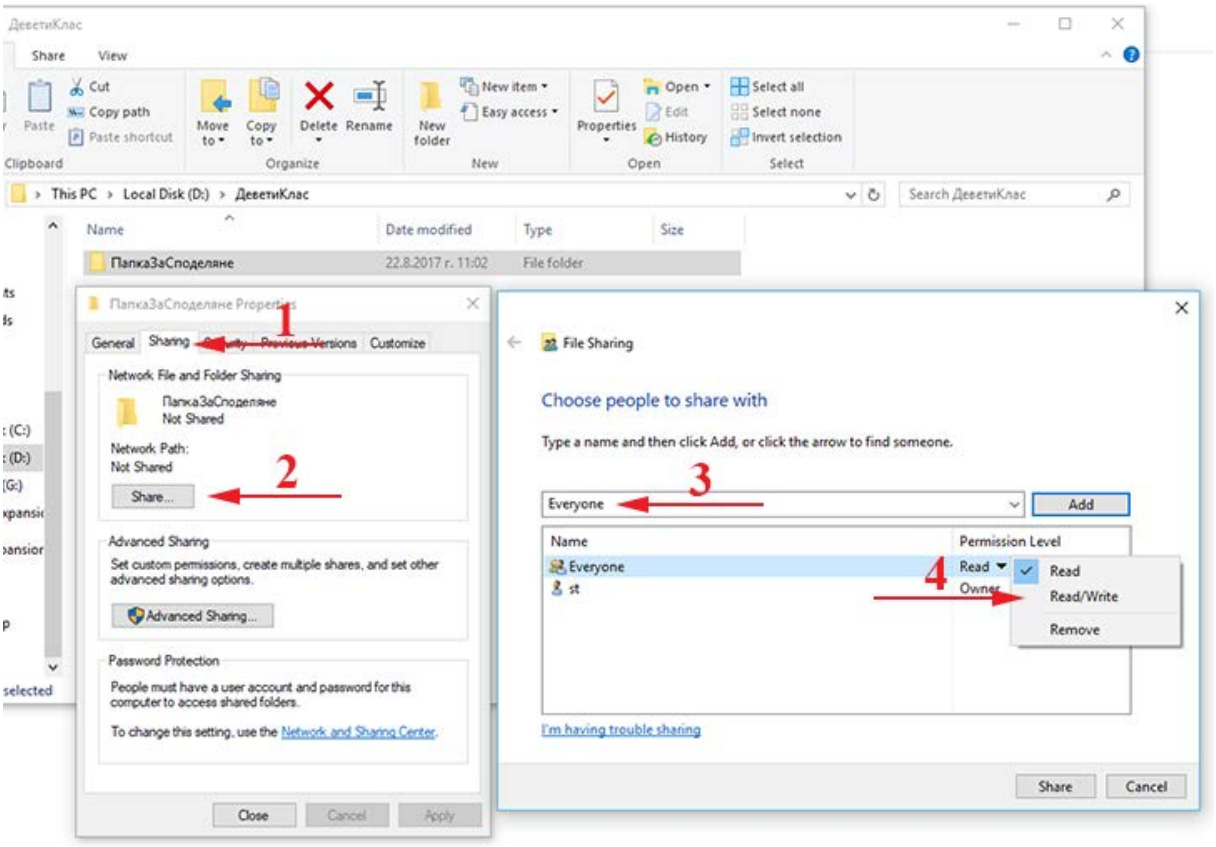
Отдаване на папката чрез таба Sharing става по следния начин:

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).

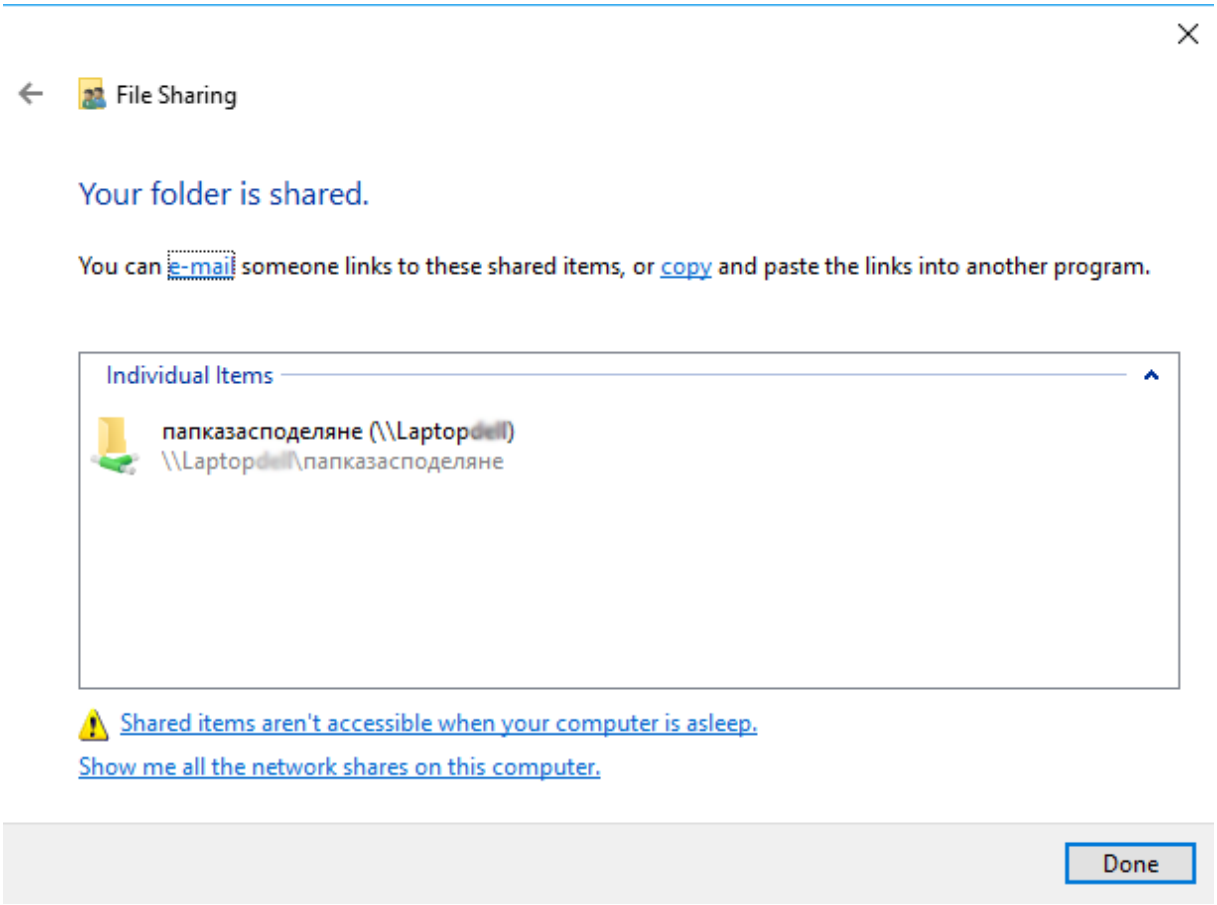
3. Избира се табът *Sharing* (фигура 2) и се натиска бутона *Share*, с което се предизвиква отварянето на нов прозорец, където трябва да се посочи групата или отделен потребител, с който се споделя ресурса. За целта се използва падащото меню, отляво на бутона *Add*. Търси се групата *Everyone*. Ако липсва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



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.

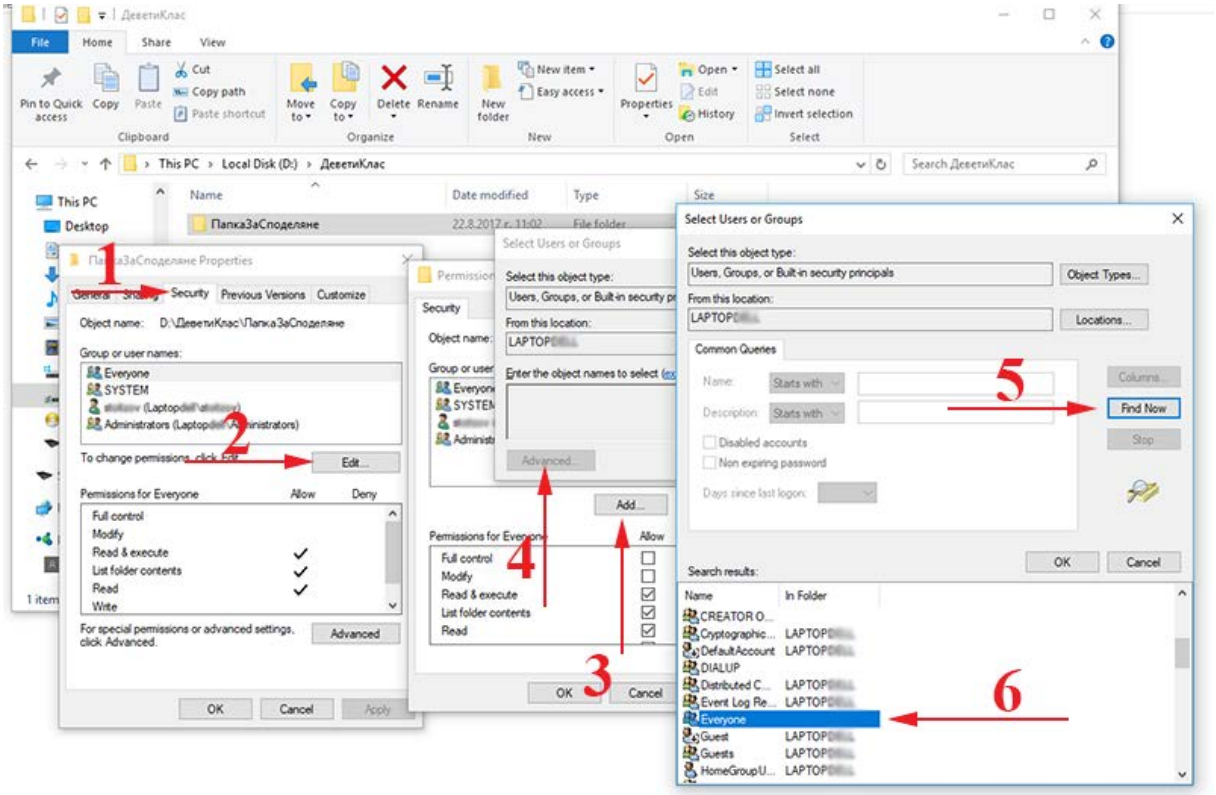


фигура 3 *Стъпка 5*

6. Потвърждението се извършва с бутона *OK*.

Последователността от стъпки за разрешаване на достъпа до споделената папка чрез таба *Security* е показан на фигура 6.

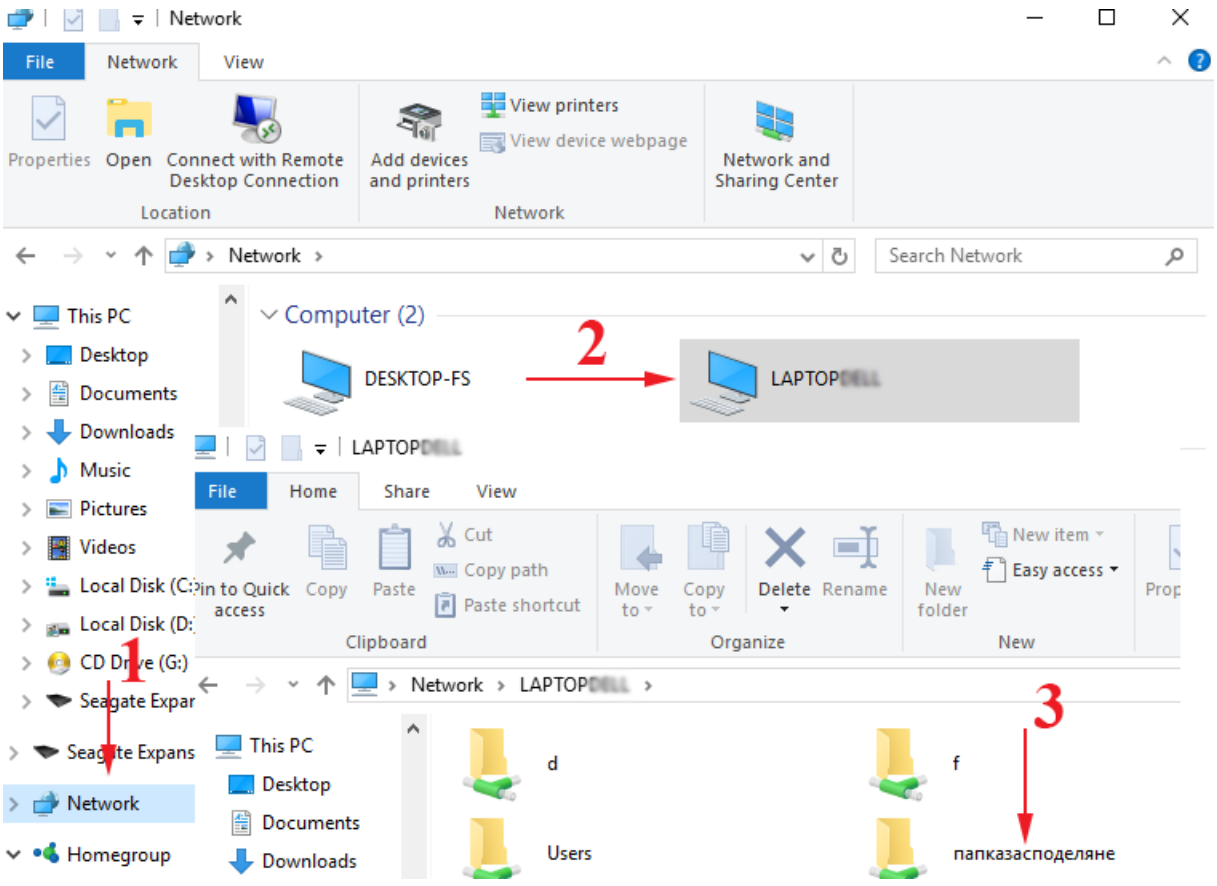
1. Избира се табът *Security* и се проверява дали в предложения списък съществува потребителят или групата, за които е споделена папката. Обикновено при използване на бутона *Share* се извършват и необходимите промени, свързани с разрешението за достъп в секцията *Security*. При липсата на целевия потребител 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 7).
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.



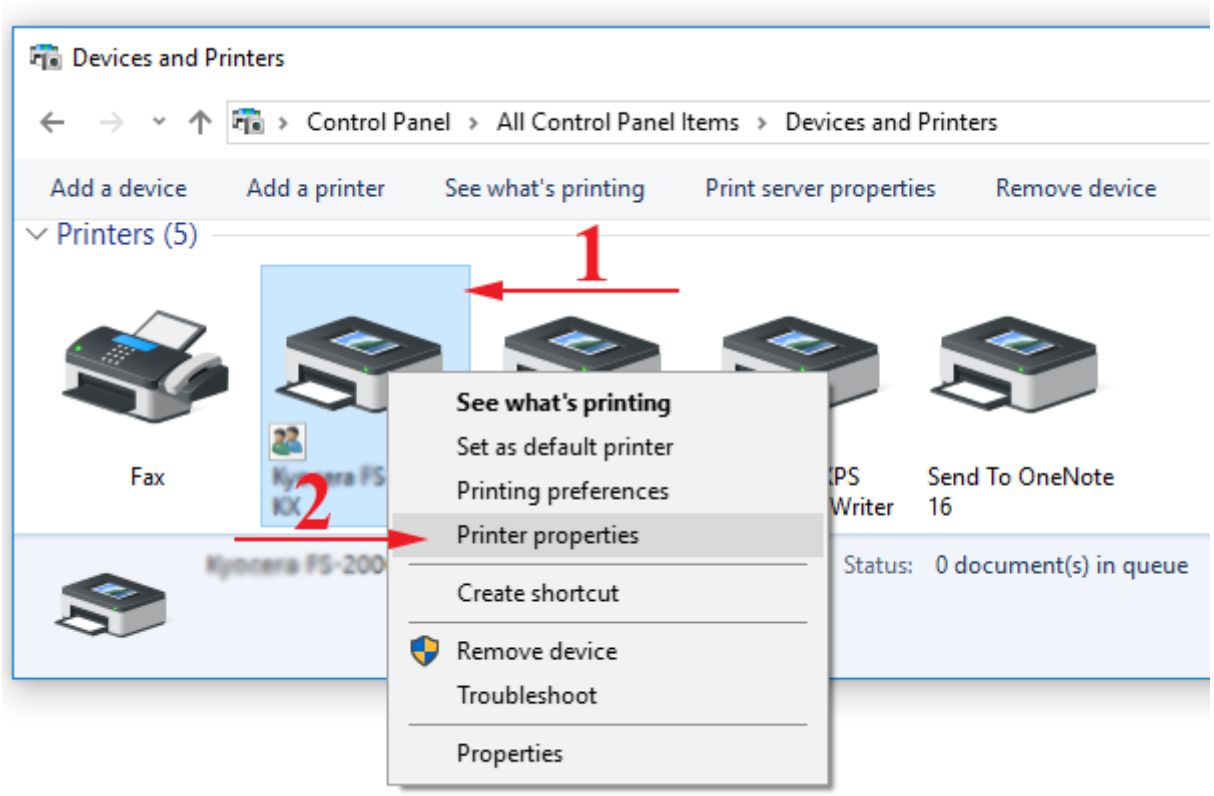
фигура 5 *Стъпка 2*

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:

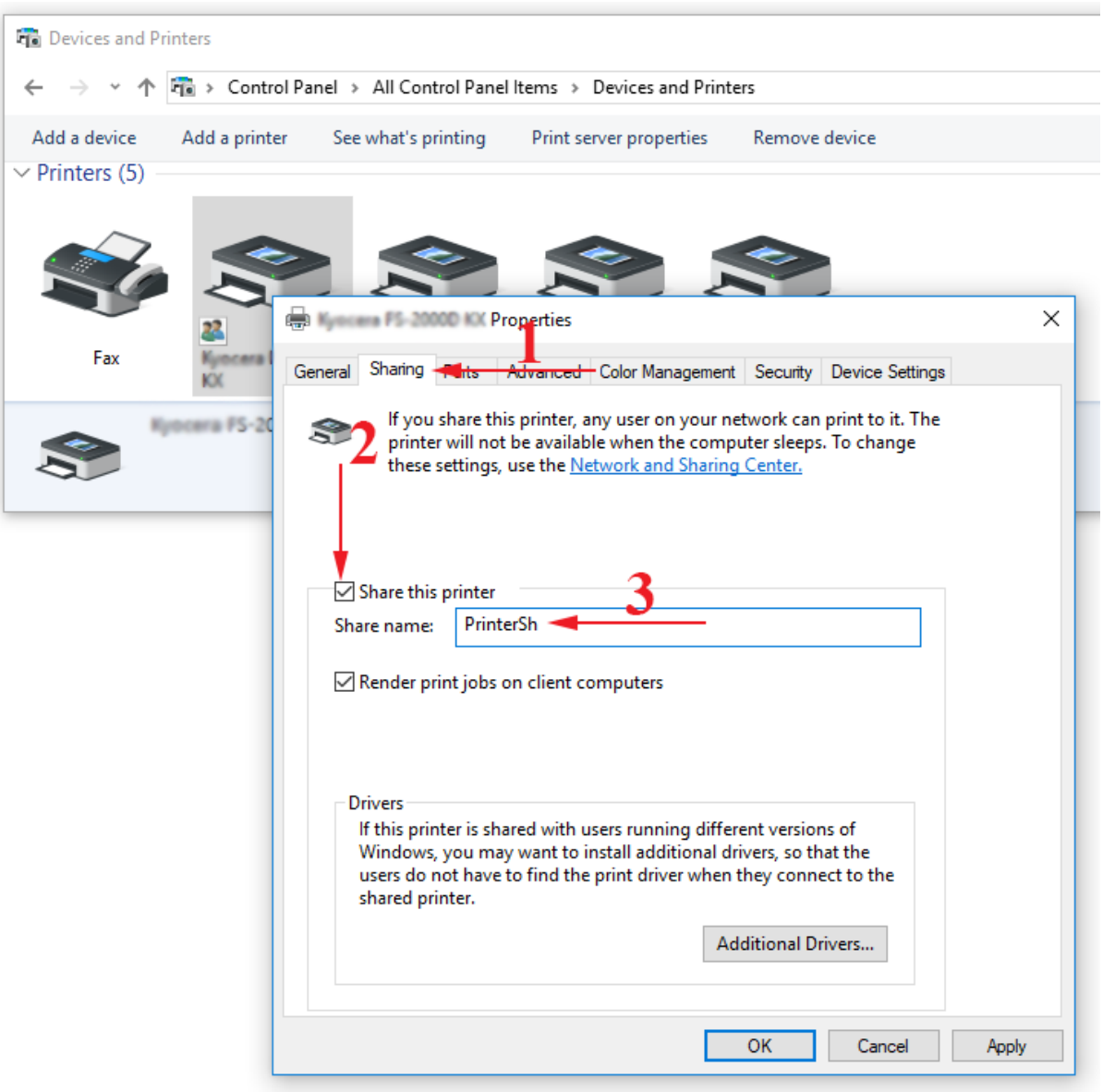
1. Прави се достъп до принтерите чрез последователността *Control Panel/Devices and Printers*. С десен бутон върху желания принтер се избира опцията *Printer properties* (фигура 8).



фигура 6 *Избор на принтер за споделяне*

2. Избира се табът *Sharing* (фигура 8). 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  .



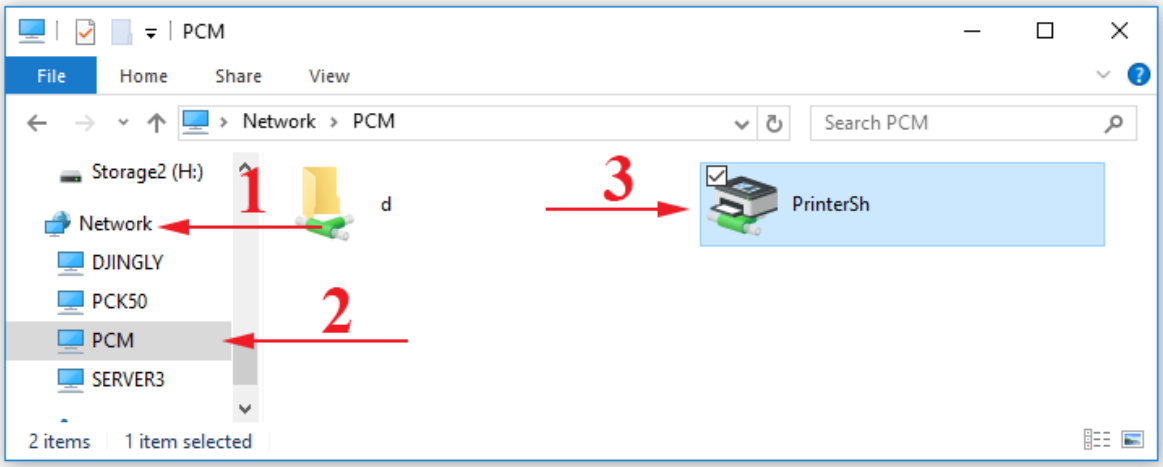
фигура 7 *Споделяне на принтер*

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 10). 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.