3. Организация на комуникацията. Адресиране. Протоколи

3.1. OSI стандарт

Съвременните мрежови архитектури следват принципите на модела OSI (Open Systems Interconnection). Създаден е от Международната организация по стандартизация ISO за връзка между отворени системи (системи, чиито ресурси могат да се използват от други такива в мрежата).

Този модел причислява различните процеси на комуникационната сесия към различни функционални нива. Нивата са организирани спрямо естествената поредица от събития, възникващи по време на комуникацията. Именно това разграничаване позволява категоризацията на различните междинни устройства от компютърната подмрежа. По този начин по-лесно може да бъде обяснена и разбрана тяхната роля и функционалност.

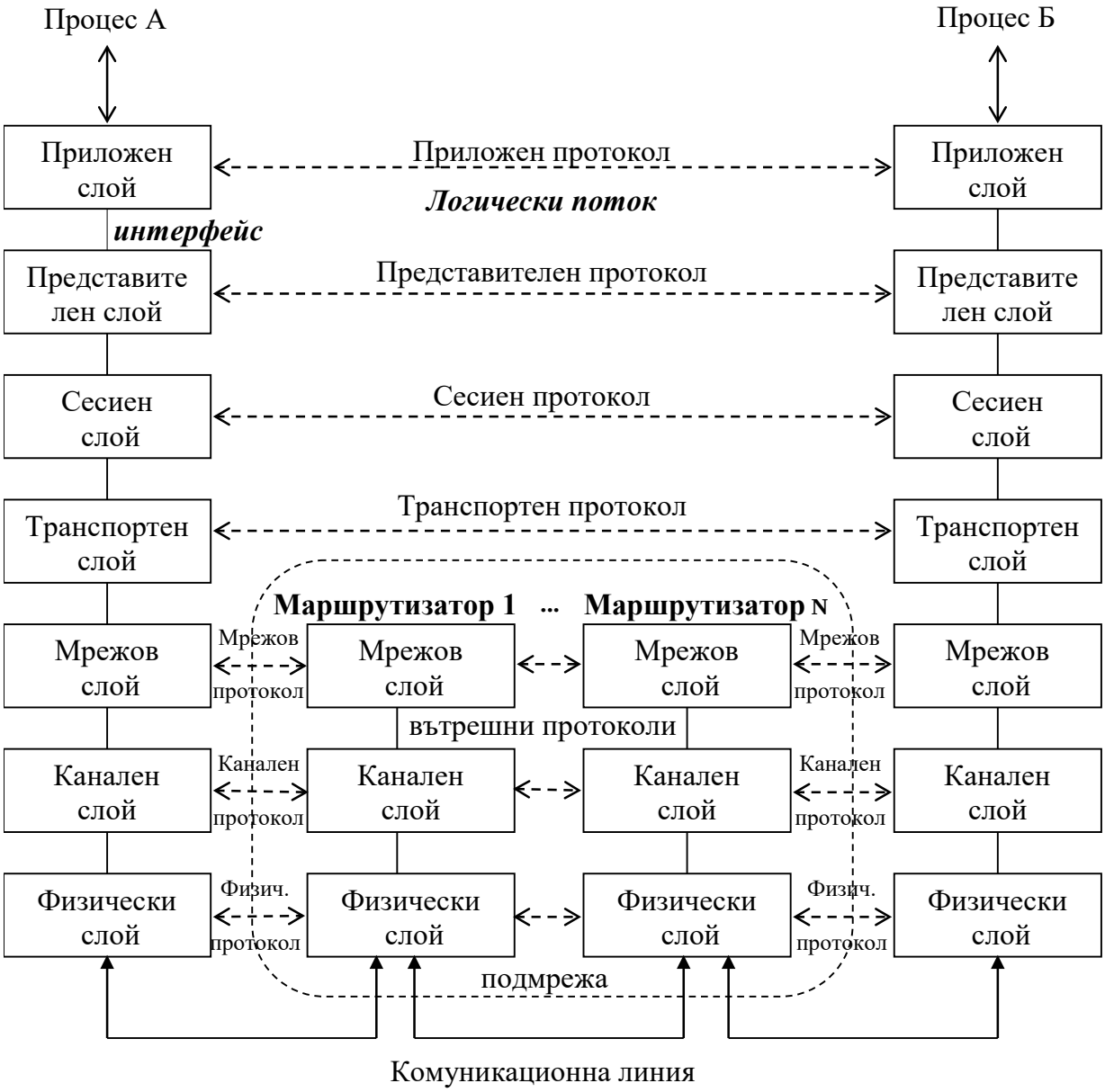
Когато се разглежда структурата и значението на OSI модела, е необходимо да се обърне внимание на следното:

- архитектура - нивата и тяхната функционалност;
- основни понятия – услуга, интерфейс и протокол;
- елементи за стандартизация – спецификация на протокола, дефиниция на услугата и адресация.

Относителният OSI модел е съставен от седем нива с различна функционалност (фигура 1). Всяко едно от тях се състои от обекти, изпълнява определена логическа функция и предлага специфични услуги за по-горния слой. Съвкупността от правила за взаимодействие между обекти от едноименни слоеве се нарича протокол, а правилата за взаимодействие на обектите от съседни слоеве на една и съща система се нарича интерфейс.

Във всеки слой има три елемента на стандартизация, споменати по-горе. Първият от тях е спецификация на протокола, което означава да е ясна структурата на неговата единица за данни, семантиката на всичките ѝ полета, начина на предаването ѝ и т.н. Дефиницията на услугите определя услугите, предоставени за по-горния слой. Самият модел не посочва как да бъдат реализирани. Адресацията се състои в идентифициране на точките за достъп (SAP-Service Access Point) до предлаганите услуги от конкретния слой.

Когато се говори за комуникация между два обекта от едно и също ниво, трябва да се прави разлика между логически и действителен поток на данните. Действителният поток преминава вертикално по нивата, докато за логически се счита непряката комуникация между два обекта от един и същи слой.



фигура 1 *Комуникационен сценарий на модела OSI*

Повечето съвременни мрежови модели се различават по степента, в която са наследили OSI модела. Често нивата се свиват до по-малко на брой, което означава и преразпределяне на функционалността. Въпреки това, всеки един от тези модели може да се съпостави с OSI и да се посочат

слоевете, до които той се разполага. Самата комуникация може да използва само част от нивата. Като пример може да се даде функционирането на единичен LAN сегмент, където обменът се извършва до второ ниво.

Физически слой (physical layer)

Физическото ниво е най-долният слой на стандарта. Той е непосредствено свързан с комуникационната линия (физическата среда, която се използва за предаване на сигналите). Основната му функция е предаване на неструктуриран поток от битове по нея. На това ниво няма механизъм за определяне на значението на предаваните битове, което означава, че не може да се определи тяхната валидност.

Устройствата, които осигуряват съгласуваност между два сегмента на това ниво, са: повторител (repeater) и концентратор (hub).

Повторителите са хардуерни устройства, чиито основни функции са свързани с възстановяване и усилване на сигнала, удължаване на покривното разстояние и съгласуване между сегментите във физическия слой.

Концентраторите са хардуерни устройства, осигуряващи възможност за лесно включване на допълнителни възли в локалната компютърна мрежа.

Канален слой (data-link layer)

Този слой използва услугите на физическия слой, разширява техните възможности и ги предоставя на мрежовия слой. Отговорен е за надеждното предаване на данните. Това означава осигуряване на надежден канал между два мрежови възли с отсъствието на каквито и да е грешки. Протоколната единица за данни се нарича кадър (frame) и съдържа достатъчно служебна информация за проверка на нейната правилност. Каналният слой е отговорен за откриването и коригирането на грешките на ниво кадър, както и превръщането на потоците от битове в кадри. Форматът на кадрите се определя от избрания протокол на канално ниво. Функциите на каналния слой обикновено се реализират смесено - апаратно и програмно. Колкото повече функции са реализирани софтуерно, толкова по-ниска е производителността.

Протоколите от този слой се разделят на две основни категории: асинхронни и синхронни. Трябва да се отбележи, че има разлика в понятието

„синхронизация“ за физическото и каналното ниво. На физическо ниво, то се свързва с определянето на границите на битовете на базата на общ синхронизационен сигнал. На канално ниво, смисълът е в разделянето на контролните от потребителските данни. Синхронните протоколи използват за граници уникална поредица от битове. Те могат да бъдат символно или битовоориентирани. При символноориентираните протоколи, потребителските данни се състоят от последователност от символи, ограничени от уникални контролни символи (SYN и EOT). Този тип протоколи са символнозависими, защото се базират на определен набор от символи (например ASCII или EBSDIC). При битовоориентираните протоколи няма специфичен набор от символи, както при символноориентираните. Последователността от битове се предава под формата на кадър, съдържащ потребителски, контролни и адресни данни, контролна сума, флаг за начало и за край.

Пример за синхронен символноориентиран протокол е Binary Synchronous Control (BSC; познат като BISYNC), създаден от IBM през 1960 г. за полудуплексна комуникация. Битовоориентиран протокол е High-level Data Link Control (HDLC), който се определя от стандартите ISO 3309, ISO 4335 и ISO 7809 и поддържа полудуплекс и пълен дуплекс.

Устройствата, които осигуряват съгласуваност между два сегмента на това ниво, са: мост (bridge) и комутатор (switch).

Основното предназначение на един мост е препредаване и филтриране на кадрите, използвайки указаните в тях MAC адреси на възлите получатели. Използва се най-често за сегментиране на големи и претоварени локални мрежи на по-малки мрежи.

Комутаторът е концентратор с възможност за комутация на кадри в каналния слой. Използва се за намаляване на вероятността от конфликти в IEEE 802.3 мрежи с интензивен трафик.

Физическият и каналният слой са необходими за всеки тип комуникация.

Мрежов слой (network layer)

Мрежовият слой управлява функционирането на подмрежата. Понятието „подмрежа“ означава съвкупност от комуникационни линии и междинни мрежови възли (комутатори/маршрутизатори), осигуряващи

предаването на информация между крайните възли. Крайните възли не се включват в подмрежата. Мрежовото ниво е отговорно за установяването на маршрут, който да се използва при комуникацията. То няма вграден механизъм за откриване и съответно коригиране на грешки при предаване. Разчита на надеждните услуги на каналния слой. Използва се за обмен на данни между системи, намиращи се в различни локални сегменти, отделени чрез маршрутизатори.

Основни функции на това ниво са:

- адресация;
- маршрутизация;
- комутация;
- управление на натоварването.

Адресацията е необходима за еднозначна идентификация на адресираните обекти на мрежовия слой. Обикновено се използва йерархичен принцип на адресация, при който пълният адрес се състои от няколко степени, като първата от тях специфицира адреса на мрежата, втората – адресът на крайния възел (хоста), третата – идентификаторът на виканата програма (порта). За пример може да се посочи стандартът IPv4, при който адресът е 4-байтов. Йерархията е по-проста, включваща две степени: адрес на мрежата и адрес на хоста.

Маршрутизацията е най-важната функция на мрежовия слой. Свързана е с избиране на оптимален маршрут за преминаване на пакетите през подмрежата на базата на предварително зададен критерий. Протоколната единица за данни се нарича пакет. Пакетите са с фиксирана големина в рамките на една мрежа, но при извършване на преход между две мрежи е възможно пакетът да се раздели на части (фрагментира), след което да се възстанови (дефрагментира). Например преходът LAN-WAN-LAN.

Комутацията е нужна поради факта, че липсва във всеки един момент пряко съединение между всеки два възела на подмрежата. Намира приложение и на канално ниво.

Управление на натоварването е свързано с избягването на задръствания в подмрежата, при което рязко се влошават нейните характеристики.

Маршрутизаторът (router) е устройството, което свързва хетерогенни мрежи на мрежово ниво. Той представлява отделен, многопротоколен мрежови възел със собствен адрес. Използва се и за свързване на локална към глобална мрежа (например Internet).

Транспортният слой освобождава по-горния сесиен слой от грижата за надеждното и ефективно транспортиране на данните между крайните системи.

Сесиен слой (session layer)

Петото ниво на OSI модела се нарича сесийно и се използва относително рядко като самостоятелно. Повечето протоколи свързват функциите му с тези на транспортно ниво. Основната му функция е да управлява комуникационния поток, наречен сесия. Към тези функции спадат:

- управление на диалога-двупосочен едновременен диалог (full duplex - FD), двупосочен алтернативен диалог (half duplex - HD), еднопосочен диалог (simplex);
- установяване, възстановяване и прекратяване на сесия;
- работа с пароли;
- осигуряване на статистика за работата на мрежата.

На това ниво се управляват т.нар. синхронизационни точки, които при грешка в предаването позволяват сесията да бъде възстановена от последната достигната точка.

Пример за протокол от този слой е Network Basic Input Output System (NetBIOS) на Microsoft. Той създава сесия между две машини, работещи под Windows операционна система, използвайки просто задаване на имена.

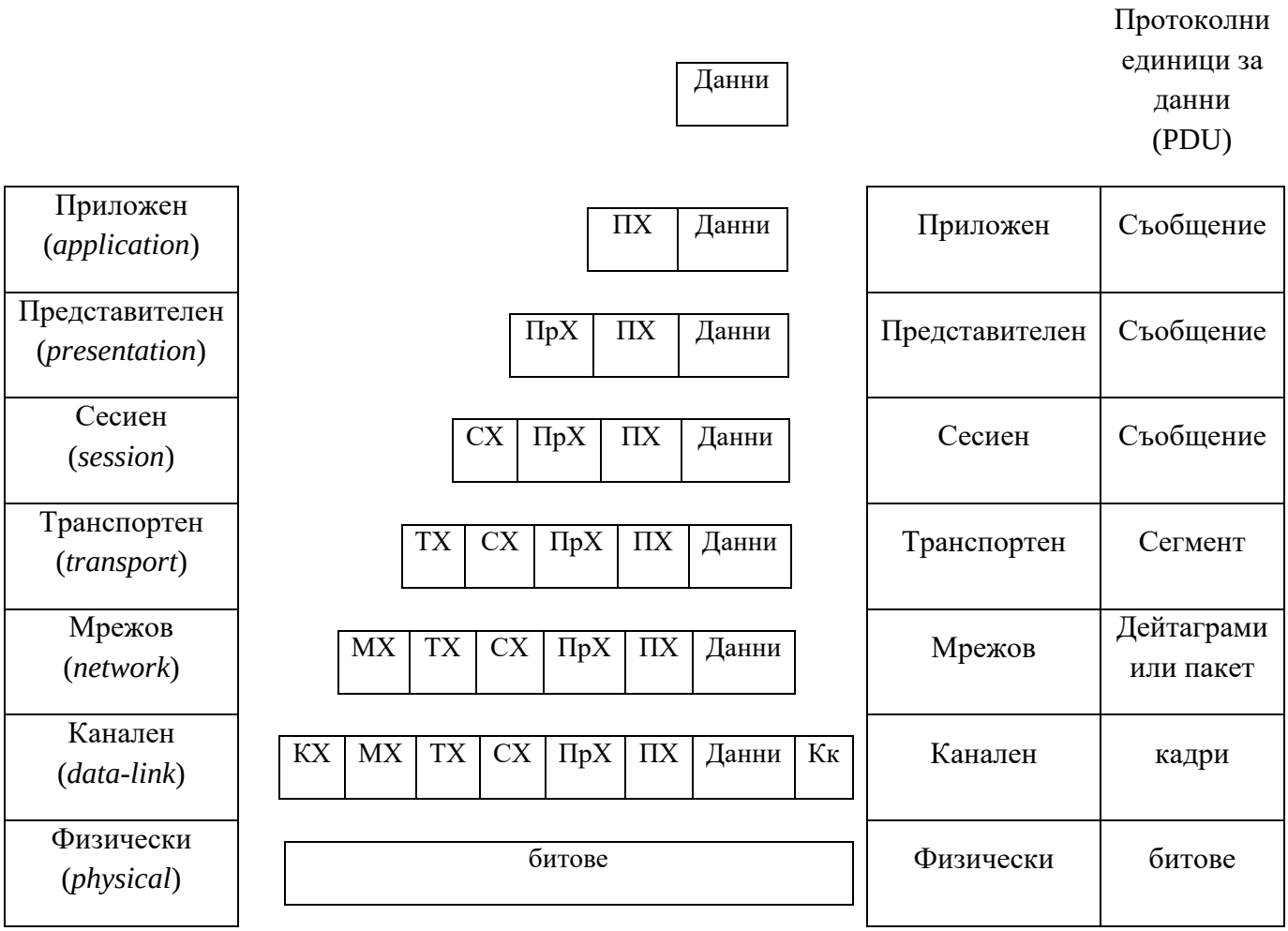
Представителен слой (presentation layer)

Представителното ниво е отговорно за управление кодирането на данните, свързано е със синтаксиса и семантиката на предаваните данни. Този слой е предназначен за преодоляване на различията във форматите, кодовете и структурите на данните. Осигурява кодиращи и декодиращи услуги.

Приложен слой (application layer)

Най-високото, седмо ниво, на OSI модела е приложният слой. Той осигурява услуги на приложните процеси и приложни протоколи, които ги реализират. Например достъп до HTTP, FTP, електронна поща, файлови и принтерни услуги.

Протоколни единици за данни



фигура 2 *Протоколни единици за данни*

На фигура 2 може да се види структурата на протоколната единица за данни и специалните и названия спрямо нивата на OSI модела.

3.2. Множествен достъп с разпознаване на носещата и откриване на колизии (CSMA/CD)

Стандартът IEEE 802.3 използва протокол с името CSMA/CD (Carrier Sense Multiple Access With Collision Detection). Този протокол допуска, че

всички възли в мрежата са равноправни, като им позволява да предават по общата комуникационна среда (шина), състезавайки се помежду си. Методът се основава на възможността всеки възел да разпознава кога шината е заета или свободна. Времето за разпространение на сигнала не трябва да превишава 512 бита (time slot – 51,2 μs).

След получаване на заявка за предаване от протоколите на горните слоеве протоколът CSMA/CD формира кадър, който се предава в двете посоки по шината. В същото време друг възел може също да изпрати кадър в шината. Възниква конфликт (колизия) между двата кадъра, вследствие на което се получава деформация на сигнала. За избягването му се грижат мрежовите адаптери. При възникване на колизия участниците продължават да предават следващи 32 бита от данните, за да засилят сблъсъка (jam сигнал). Това гарантира разпознаването на конфликта от другите станции. При откриване на ранна колизия (по време на преамбюла) станцията продължава да предава преамбюла, следван от 32 бита данни. Всеки възел, участвал в конфликта, включва backoff алгоритъм за изчакване на различен интервал от време, преди да изпрати отново кадъра си. След 16 неуспешни опита контролерът на мрежовата платка предава към компютъра сигнал за грешка. Общият брой на устройствата, които се съревновават за честотната лента, се нарича колизионен домейн (фигура 3). Диаграма за предаване на кадър по метода на съревнование до общата среда за комуникация е представена на фигура 4.

фигура 3 *Колизионен домейн*

Процедурата по предаване в свободна среда и тази по време на колизия може да се опише по следния начин:

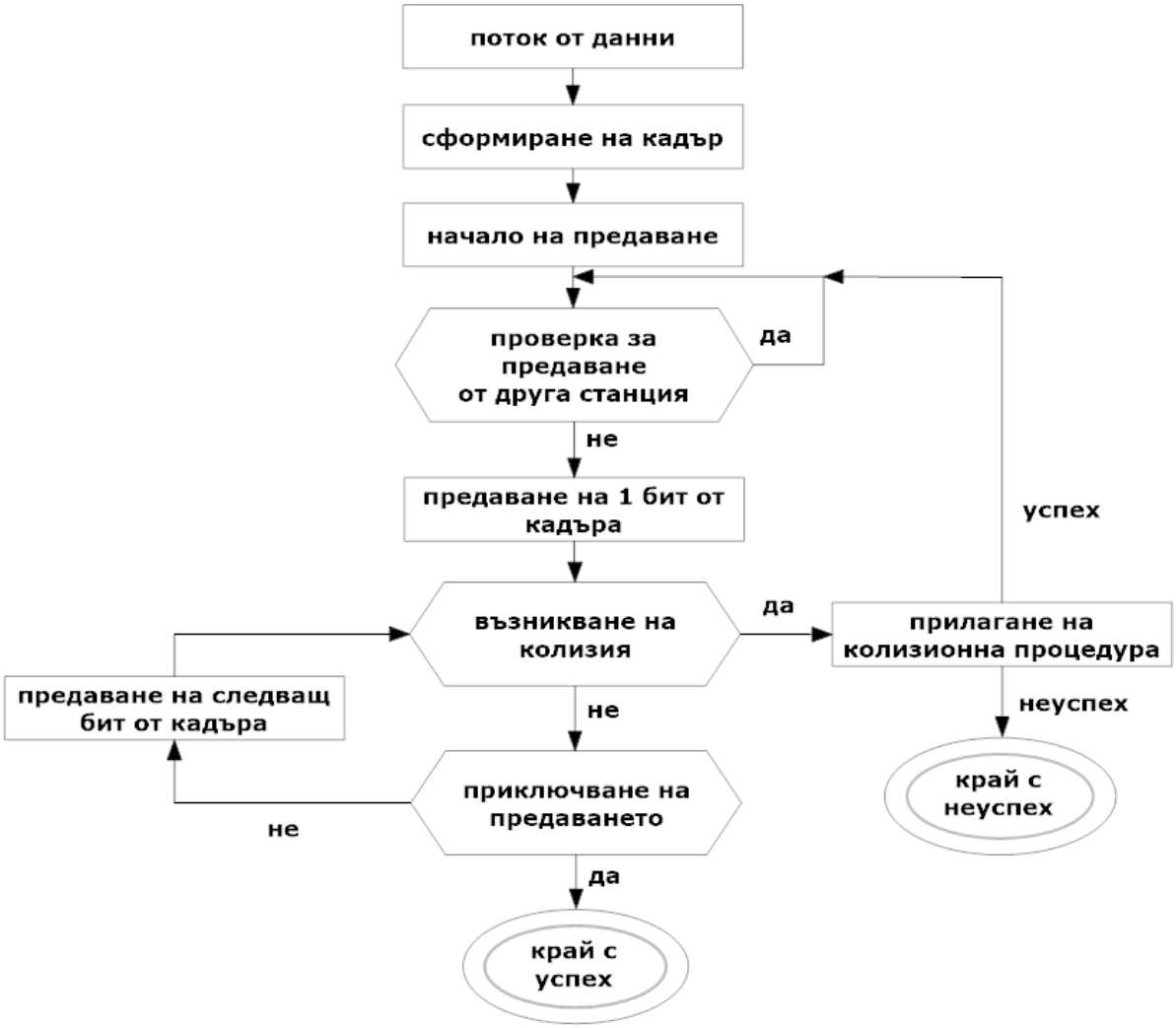
- *Главна процедура*

1. Кадърът е готов за предаване;

2. Свободна ли е средата? Ако не, изчаква се до нейното освобождаване;
3. Предаване;
4. Има ли колизия? Ако да, преминаване към *колизионната процедура*;
5. Успешно предаване;

- *Колизионна процедура*

1. Продължаване на опита за предаването;
2. Достигнат ли е максималният брой опити? Ако да, неуспех на предаването;
3. Случайно генериран период на изчакване;
4. Преминаване към точка 1.



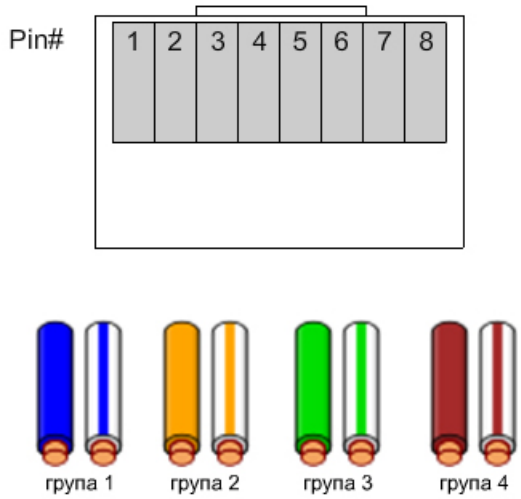
фигура 4 *Алгоритъм за обработка на колизии*

При увеличаване на възлите в мрежата конфликтите се увеличават и средната скорост намалява.

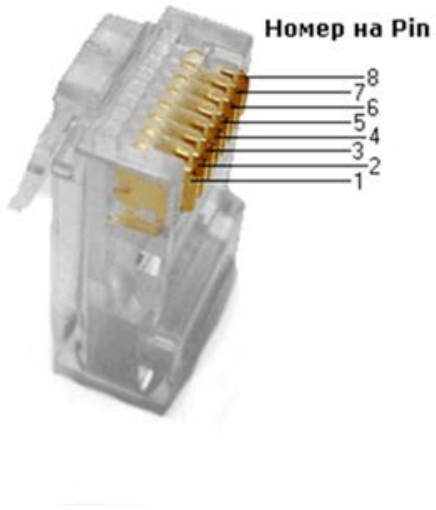
Локалните мрежи по стандарта IEEE 802.3 могат да бъдат комутирани. В този случай комуникационната среда престава да бъде обща. Използват се устройства – комутатори (устройства с високоскоростна комутационна матрица), които заместват концентраторите.

Използване на конектори тип RJ-45

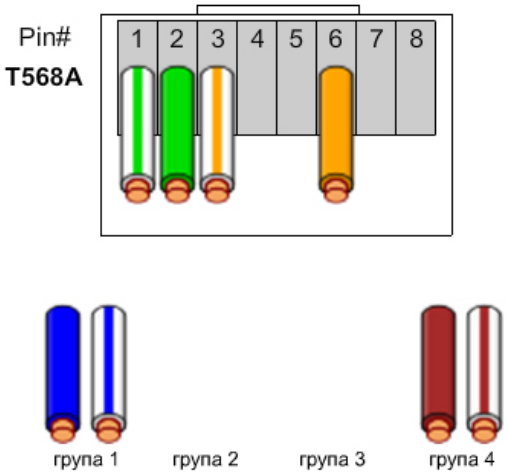
RJ-45 (Registered Jack, фигура 5б) е физически конектор, употребяван масово при съвременните локални мрежи за установяване на свързаност между устройства, на които физическите интерфейси позволяват използването на кабел с усукани двойки проводници. За целта стандартът TIA/EIA-568-B.1-2001 дефинира цветовите групи (фигура 5а), подредбата на цветовете T568A и T568B (фигура 5в,г,д,ж) и две основни схеми за реализиране на такъв тип свързаност – прав и кръстосан кабел.

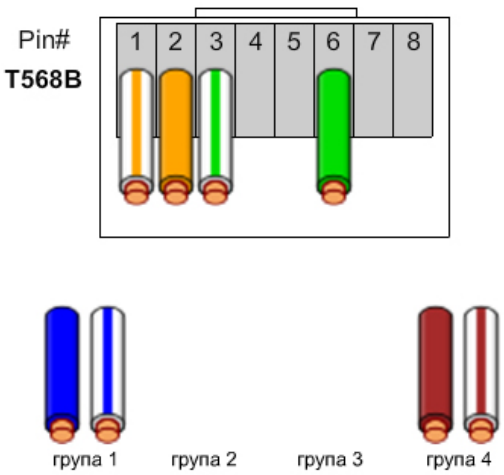


а) цветови групи

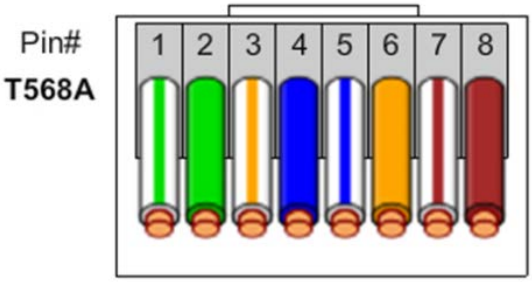


б) RJ-45 конектор

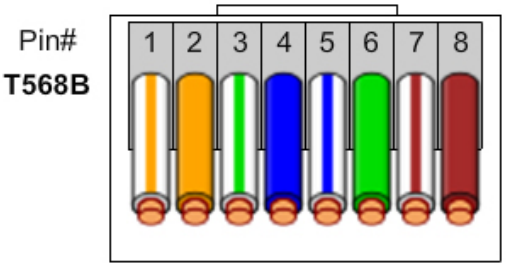




в) използване на две усукани двойки



г) използване на две усукани двойки



д) използване на четири усукани двойки

ж) използване на четири усукани двойки

фигура 5

Ако в двата края на кабела се приложи една и съща цветова схема (T568A или T568B), то получената реализация се нарича прав кабел (straight-through cable). При използване на различни схеми (T568A и T568B) кабелът се нарича кръстосан (crossover cable).

Тези схеми на свързаност са продиктувани от факта, че предаващите двойки пинове на порта от едната страна трябва да бъдат свързани с приемащите такива от другата страна. Всеки порт, поддържащ този начин на свързване, може да бъде означен като MDI (medium dependent interface) или MDI-X (medium dependent interface crossover) **Error! Reference source not found.**. Стандартно MDI се използва за крайните устройства (мрежови адаптери), докато MDI-X за портовете на междинните устройства (комутатори, концентратори). Правият кабел свързва MDI с MDI-X интерфейси, докато кръстосаният кабел е предназначен за еднотипни такива. Пример за използване на прав кабел може да бъде връзката между мрежов адаптер на компютър (MDI) и порт на комутатор (MDI-X). Ако поне едно от двете устройства поддържа функцията Auto-MDI/MDI-X, то може автоматично да открива необходимия вид кабелна връзка и да се преконфигурира по подходящ начин. Така се премахва необходимостта от кръстосан кабел. Съвременните междинни устройства притежават тази функция. В таблица 1 са показани MDI конфигурациите на пиновете на спецификациите 10Base-T, 100Base-TX и 1000Base-T. От нея се вижда, че 1000BASE-T използва и четирите двойки проводници за предаване в двете посоки (BiDirectional).

Pin	Сигнал	10Base-T	100Base-TX	1000Base-T
1	Предаване (+)/Двупосочен	TX+	TX+	BI_DA+
2	Предаване (-)/Двупосочен	TX-	TX-	BI_DA-
3	Приемане (+)/Двупосочен	RX+	RX+	BI_DB+
4	Липсва/Двупосочен	Липсва	Липсва	BI_DC+
5	Липсва/Двупосочен	Липсва	Липсва	BI_DC-
6	Приемане (-)/Двупосочен	RX-	RX-	BI_DB-
7	Липсва/Двупосочен	Липсва	Липсва	BI_DD+
8	Липсва/Двупосочен	Липсва	Липсва	BI_DD-

таблица 1 *MDI конфигурациите на пиновете*

Проверка на работоспособността на UTP кабел

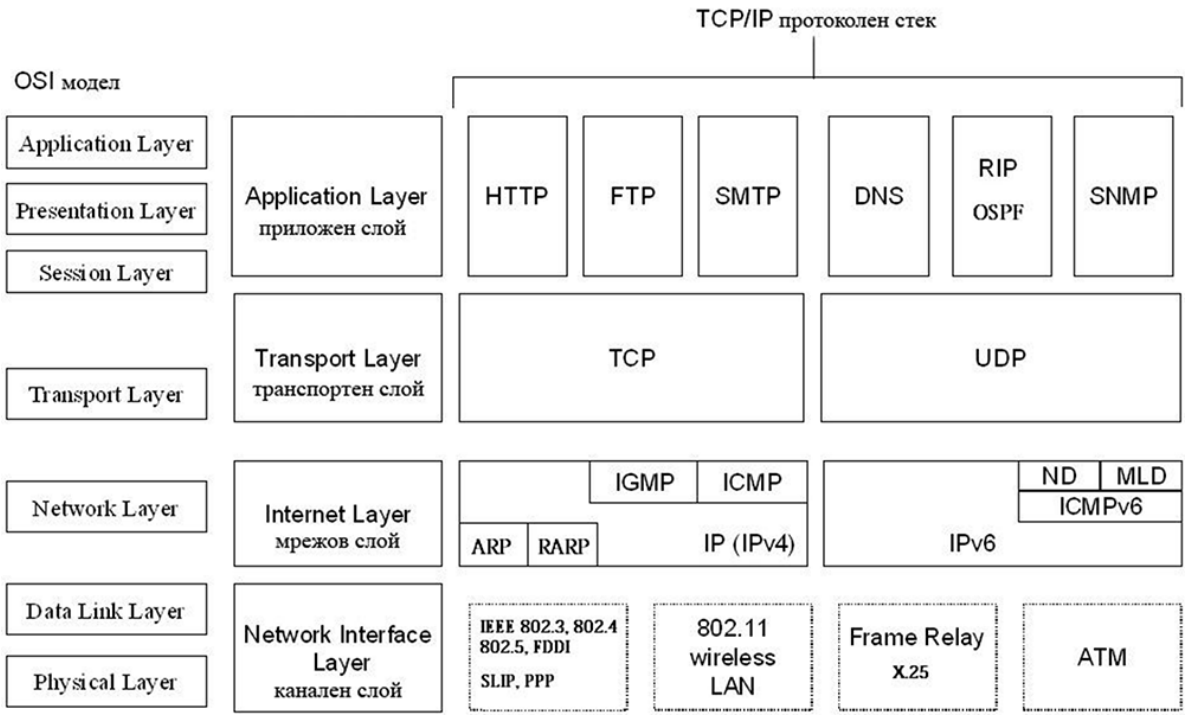
За правилното функциониране на UTP кабел е необходимо:

1. да не е прекъснат;
2. да е реализирана правилна подредба на проводниците спрямо пиновете на конекторите (в зависимост от стандарта);
3. да има добър контакт между отделните проводници и металните пластинки на пиновете на конектора.

При извършването на първоначална проверка на реализиран вече кабел е необходимо да се направи внимателен оглед за проблеми по т.2 и т.3 от изброените по-горе изисквания и ако има възможност, да се направи това и за т.1. Може да бъде тестван чрез обикновен омметър или кабелни тестери.

3.3.TCP/IP протоколен стек

TCP/IP (Transmission Control Protocol/Internet Protocol) е основният протоколен стек, необходим за функционирането на глобалната мрежа Интернет (фигура 6). 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 6.



фигура 6 *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**.

Разположение на устройствата спрямо OSI модела

В зависимост от нивото за съгласуване се различават следните видове устройства: повторители, концентратори, модеми, мостове, комутатори, маршрутизатори, мост-маршрутизатори. Позицията, която заемат в общата

схема, спрямо OSI модела **Error! Reference source not found.**, е показана на фигура 7.

фигура 7 *Разположение на устройствата спрямо OSI модела*

Видове домейни

Колизионен домейн – физически сегмент, където могат да възникнат колизии.

Броадкаст домейн – логически сегмент, определящ границите на броадкаст и мултикаст предаването.

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 8). 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 8). 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 8). 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 8 *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 2.

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 2 *Диапазон на десетичните стойности на първия байт*

Стандартните мрежови маски за клас могат да се видят в таблица 3.

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 3 *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 4.

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

таблица 4 *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

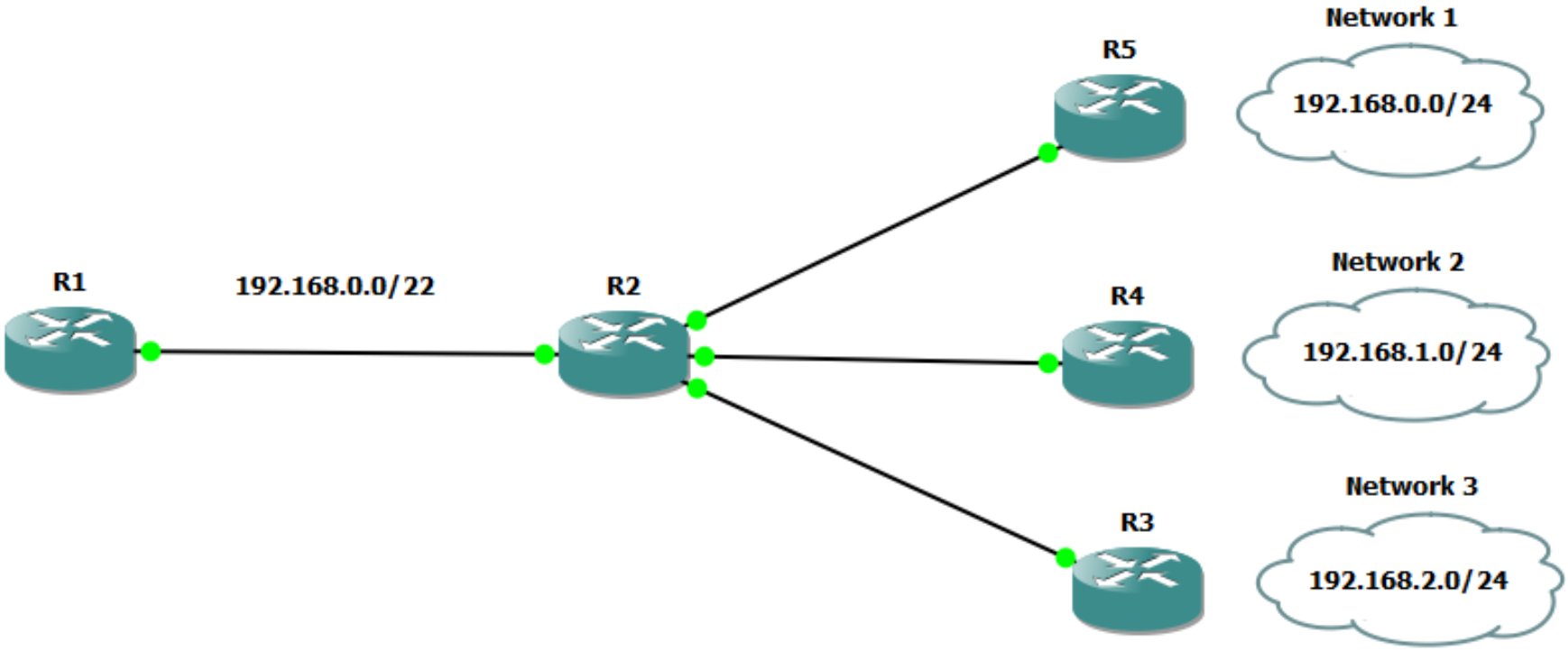
локални мрежи, за да не се заемат публични интернет адреси. Те функционират само в рамките на локалната мрежа, където са назначени. При работа с Интернет частните IP адреси се преобразуват в публични IP адреси. Обикновено тази функция се изпълнява от маршрутизатора (рутера) на LAN мрежата. Той се явява 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.

Определени са и Link-local адреси за случаи, при които хостът не може да получи TCP/IP конфигурационни параметри от DHCP сървър или не са му назначени статично. Хостът си определя адрес в обхвата 169.254.0.0 - 169.254.255.255. Подходът позволява отделни хостове с такива настройки да попаднат в една мрежа и да комуникират помежду си.

Означенията от вида 10.0.0.0/8 са от използваната алтернатива за безкласово адресиране, базирано на безкласовата междудомейнова маршрутизация CIDR (classless inter-domain routing - RFC 1517, RFC 1518, RFC 1519, RFC 1520, RFC 1812), позволяващо по-ефективно разпределение на IP адреси. Числото 8 след наклонената черта означава, че $8^{-те}$ най-леви бита се използват за идентификация на мрежата (префикс), а останалите за разпознаване на хоста. Обикновенно префиксите варират между /13 и /27 и се отъждествяват с брой мрежи от клас C.



фигура 9 *Supernetting и aggregation*

Например CIDR адресен блок с префикс:

- /27 се равнява на $\frac{1}{8}$ мрежи от клас C (32 хост адреса);
- /26 се равнява на $\frac{1}{4}$ мрежи от клас C (64 хост адреса);
- /25 се равнява на $\frac{1}{2}$ мрежи от клас C (128 хост адреса);
- /24 се равнява на 1 мрежа от клас C (256 хост адреса);
- /15 се равнява на 512 мрежи от клас C (131 072 хост адреса).

CIDR позволява подходите supernetting (използване на съседни блокове от адресното пространство за симулиране на по-голямо адресно пространство) и route aggregation (едно вписване в маршрутната таблицата на рутер, представляващо множество мрежи). Целта е намаляване на размера на този тип таблици.

На фигура 9 са представени три последователни мрежи от клас C с префикс /24. В двоичен вид те изглеждат по следния начин:

IP	**еднакви битове**	**разлика**
192.168.0.0	11000000.10101000.000000	**00.00000000**
192.168.1.0	11000000.10101000.000000	**01.00000000**
192.168.2.0	11000000.10101000.000000	**10.00000000**

Вертикалната черта показва докъде достигат от ляво надясно еднаквите битове. Тяхната бройка формира новия префикс на супермрежата. Адресът на самата мрежа се получава, като същите битове се допълват с нули до получаване на правилен такъв:

супермрежа	**нов префикс**	**еднакви битове**	**допълване**
192.168.0.0	**22**	11000000.10101000.000000	**00.00000000**

Третата стратегия, която според възникването си в исторически план се подрежда на второ място след класовата и се наследява при безкласовата адресация, за определяне на префикса, се нарича Variable-Length Subnet Masking (VLSM, RFC 950). При нея се използват подмаски (броят на единиците е различен от този на стандартните маски) за дефиниране на

подмрежи. Съществуват и някои ограничения, които отпадат при CIDR. Задачи от този тип са разгледани в следващата тема.

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.

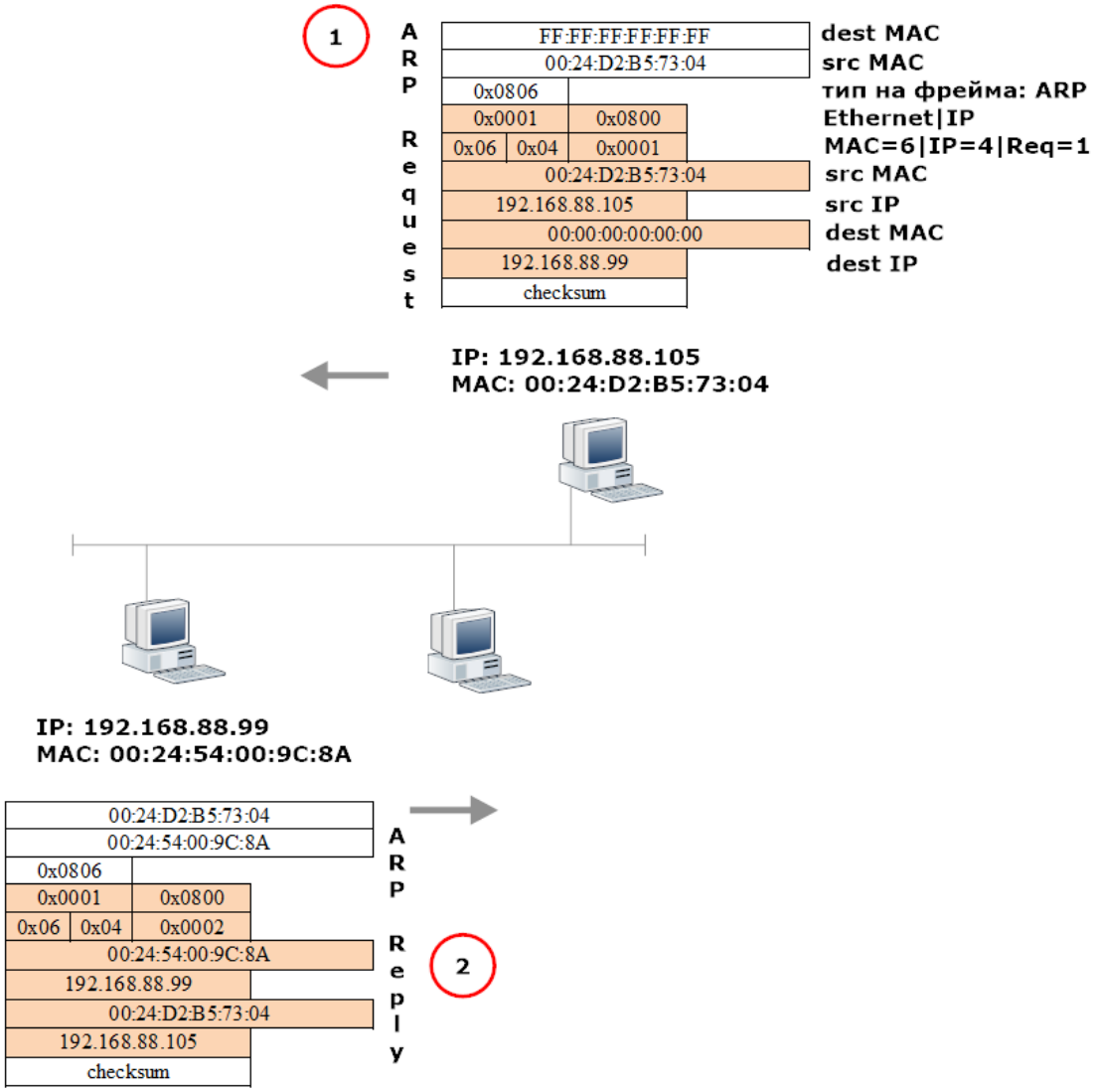
ARP (Address Resolution Protocol)

ARP е протокол за преобразуване на адреси. Превръща логическите адреси (например 32-битови IP адреси) от мрежовия слой във физически адреси от канален слой (например MAC адреси) [RFC 826]. За целта всеки хост поддържа ARP кеш таблица, където съхранява съответствията между IP и MAC адрес, научени динамично по време на комуникацията с други хостове или въведени статично от администратора на системата. ARP използва броадкасти до хостовете в локалния сегмент за определяне на дадено съответствие, което добавя като запис в ARP таблицата на хоста за бъдещо използване. Валидността на записите може да се контролира чрез няколко механизма:

- таймаут – при добавяне на запис в таблицата се определя време на валидност, след което той се премахва;
- периодични уникаст запитвания – изпращат се периодични уникаст запитвания към регистрираните хостове. Ако отдалеченият хост не отговори, записът се премахва от кеша;
- уведомяване от протокол – ако протокол от по-горен слой установи проблеми при доставката, той уведомява активния ARP процес в хоста, който от своя страна премахва записа за отдалечения хост от таблицата му.

На фигура 86 е представена ARP заявка (Operation=0x0001) и ARP отговор (Operation=0x0002). Компютър с IP адрес 192.168.88.105 изпраща в локалния сегмент ARP броадкаст (destMAC=FF:FF:FF:FF:FF:FF) за установяване на непознат MAC адрес, съответстващ на локален IP адрес 192.168.88.99. Търсеният хост отговаря на запитването чрез ARP отговор, като предоставя физическия си адрес на хоста изпращач. Втората възможност е, ако изпращащият хост е установил, че получателят не се намира в същия сегмент. Тогава неговият ARP броадкаст ще бъде

предназначен за установяване на физическия адрес на локалния шлюз (ако не го знае все още), който да препрати пакета до хоста местоназначение.

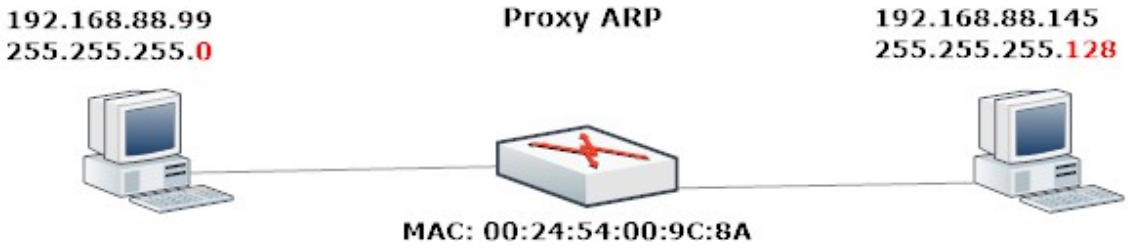


фигура 10 *ARP заявка и отговор*

В някои случаи е възможно използването на Proxy ARP, което позволява на друго устройство (например маршрутизатор) да отговаря на ARP запитвания от името на отдалечен хост, намиращ се в друга подмрежа. Това осигурява възможност за прозрачна комуникация между отдалечени хостове.

Например, ако даден хост изпращач е конфигуриран неправилно и се обърка при изпращането на ARP запитване към хост извън локалния сегмент, то маршрутизаторът, конфигуриран като Proxy ARP, ще отговори

със собствения си физически адрес. Това позволява пакетът да бъде препратен след това към правилния хост местоназначение.



фигура 11 *Proxy ARP*

Подобен пример е представен на фигура 91, където хост 192.168.88.99 от мрежа 192.168.88.0 иска да комуникира с хост 192.168.88.145 от мрежа 192.168.88.128. Мрежовата маска на първия хост (255.255.255.0) е сгрешена. Това го обърква при пресмятането на принадлежността на адрес 192.168.88.145. За него този адрес е част от локалния сегмент и затова изпраща локален ARP броадкаст за установяване на физическия му адрес. Това запитване не стига да хоста местоназначение и той не отговаря. Маршрутизаторът, конфигуриран като Proxy ARP, приема това запитване и отговаря от името на целевия хост, като изпраща собствения си хардуерен адрес. Изпратеният към него пакет бива препратен към хоста местоназначение.

RARP (Reverse Address Resolution Protocol)

RARP е протокол за динамично преобразуване на физическите адреси на хостове в логически адреси от мрежово ниво (например IP адреси). Той извършва противоположно действие на ARP протокола.

Протоколът е предназначен за назначаване на логически адреси на бездискови станции. За целта се използват RARP сървъри, където в статични таблици се съхраняват съответствията между хардуерни и логически адреси. За поддържането им се грижат мрежови администратори. Подобно на ARP, и този протокол използва броадкасти. Това означава, че във всеки локален сегмент трябва да има поне по един RARP сървър, който да отговаря на такъв тип запитвания. Недостатъците на RARP са свързани с необходимостта от:

- такъв тип сървъри за всеки един сегмент, поради невъзможността маршрутизаторите да препращат RARP броадкасти;

- администратор за създаване и поддържане на статичните асоцииращи таблици.

RARP не е единственият протокол за преобразуване на хардуерни в логически адреси. Представители на този тип асоцииране са още BOOTP и DHCP, предназначени да заменят RARP. Всеки един от тези протоколи се стреми да отстрани проблемите, съществуващи при предшественика му. В момента актуалният протокол е DHCP.

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 10), 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 12 *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:

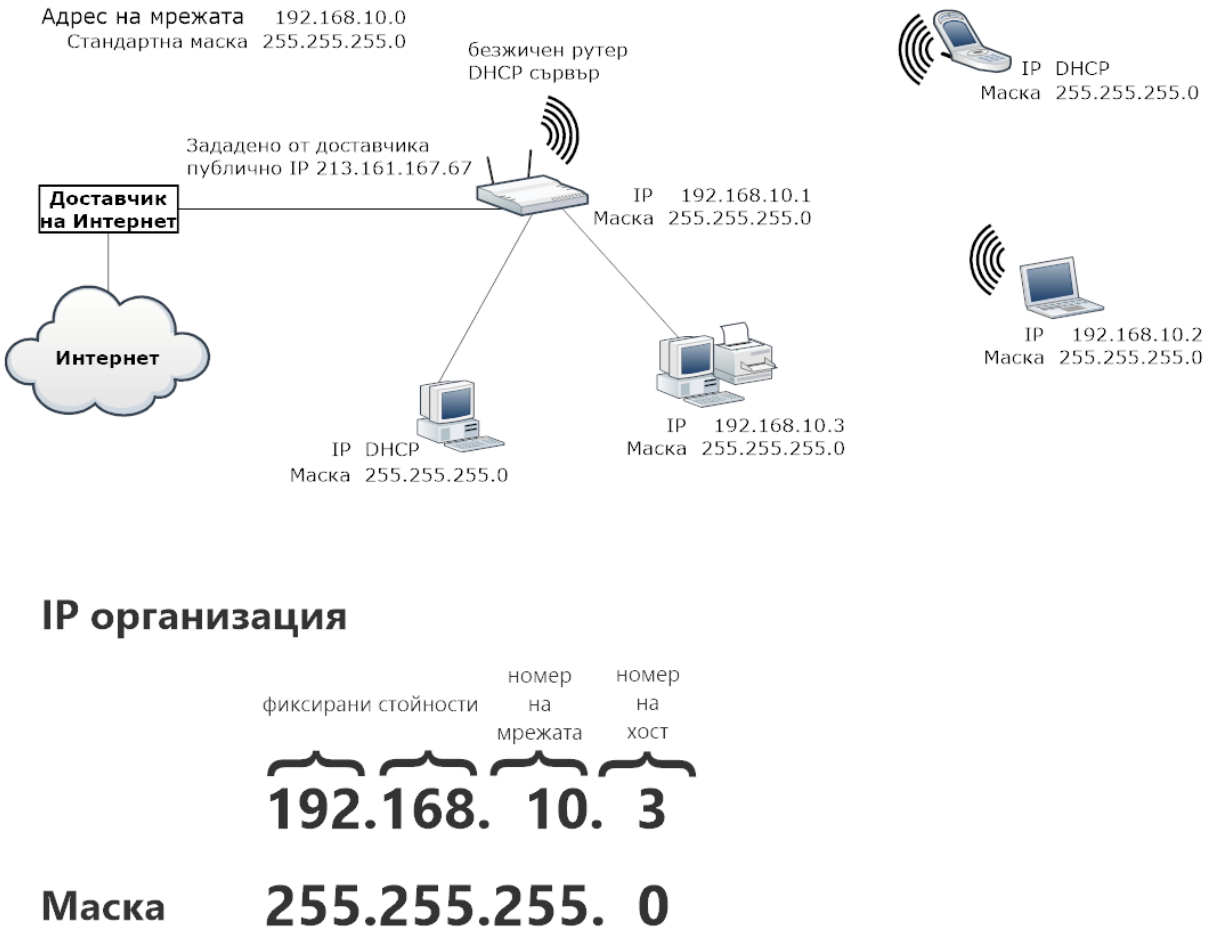
- SMTP (Simple Mail Transfer Protocol) – протоколът осигурява предаването на електронно съобщение между пощенските

(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.

3.4.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.



фигура 13 *Конфигуриране на мрежата с IP адреси*

В нея бяха включени безжичен рутер, суич, няколко компютъра и безжични клиентски устройства. Получените знания от тази тема могат да помогнат за преминаване към следващата стъпка – конфигуриране на мрежата с IP адреси. Примерна конфигурация е представена на фигура 11.

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.

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.

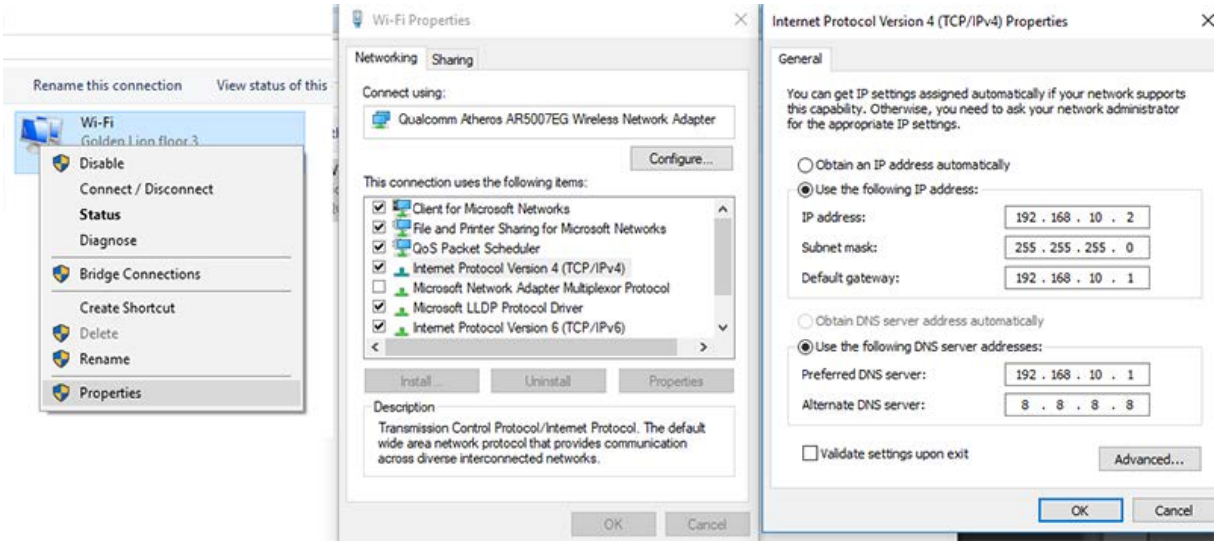
3. Десният бутон на мишката върху избрания интерфейс ще отвори контекстно меню, откъдето се избира последната опция *Properties*. Изборът и предизвиква отваряне на допълнителен прозорец, в който се избира протоколът TCP/IP (версия 4).

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 12 са показани настройки, отговарящи на настройките на

лаптопа от фигура 11. 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 14 *IP настройки на мрежов интерфейс*

Маршрутизаторът също притежава възможност за настройка на този вид параметри. 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.

3.5.Инструменти за тестване на TCP/IP конфигурацията

ping

Инсталирането на нов компютър или промени в конфигурацията на мрежовите настройки на дадена система, трябва да тества в последствие. Най-простият TCP/IP тест е да използвате инструмента *ping*, за да проверите връзката на компютъра с мрежата. *Ping* е инструмент за работа от командния ред и се използва по следния начин

ping host

Където *host* е хост компютърът, до който се прави опит за достигане. Вариантите са:

- ping-ване на IP адрес;
- за домейни, използващи WINS, може да се ping-не NetBios името на компютъра.

- за домейни, използващи DNS, може да се ping-не DNS името на хоста.

ipconfig

Може да използвате инструмента *ipconfig*, за подновяване или освобождаване на настройки:

- За освобождаване на текущите настройки се използва командата *ipconfig /release*.
- Подновяването на DHCP наема е чрез *ipconfig /renew*;
- Проверка на обновените настройки може да се извърши чрез командата *ipconfig /all*.

Кешът за DNS преобразуването поддържа история на DNS справките, които са били извършвани, когато даден потребител е осъществявал достъп до мрежови ресурси чрез използване на TCP/IP. Този кеш съдържа прави справки (fotward lookups), осигуряващи преобразуване на хост имена в IP адреси, както обратни справки (reverse lookups), осигуряващи преобразуване на IP адреси в имена на хостове. След като даден DNS запис се съхрани в кеша за преобразуване за конкретен DNS хост, локалният компютър вече няма нужда да запитва външни услуги за DNS информация относно този хост. Това позволява на компютъра да обработва заявки за DNS преобразуване локално, което пък води до по-бърз отговор.

Колко време записите се съхраняват в кеша зависи от TTL (Time to Live) стойността, назначена на записа от оригиналния сървър. За да разгледате текущия кеш:

ipconfig /displaydns.

Тези стойности се дават като брой секунди, за които даден запис може да остане в кеша, преди да стане невалиден. Локалният компютър непрекъснато намалява всички стойности с всяка изминала секунда. Когато TTL стойността достигне нула, записът става невалиден и се премахва от кеша.

За изчистване на кеша:

ipconfig /flushdns

За подновяване на записите:

ipconfig /registerdns

traceroute/tracert

Командата **tracert** (това е името на командата **traceroute** при работа с операционна система *Windows*) проверява наличност на връзка и нейното качество:

tracert host

Резултатът включва няколко колонки:

- В първата колона се изброяват рутерите (скокове, hops), които включва мрежовата връзка, преди да достигне до сървъра/домейна, който се проверява.
- Следващите три колони показват времето, необходимо за отговор от дадения рутер.
- Последната колона показва имената/адресите на рутерите или сървърите, през които преминава връзката.