

Понятието компютърна мрежа

На най-елементарно ниво мрежата се състои от два компютъра, свързани помежду си, за да могат да обменят данни. Всички мрежи, независимо от тяхната сложност, използват тази елементарна система. Въпреки че идеята да се свържат два компютъра не изглежда необикновена, тя се оказва огромно достижение в сферата на комуникациите.

Компютърните мрежи са възникнали поради нуждата от бърз обмен на данни. Персоналните компютри са чудесни бизнес инструменти за обработка на данни и създаване на електронни таблици, графики и други видове информация, но не позволяват бърз обмен на данните. Когато няма мрежа, документът трябва да се отпечата, за да могат другите да го редактират или използват. В най-добрия случай файловете се копират на дискети и се дават на останалите колеги, които ги прехвърлят на своите компютри. Ако те, от своя страна, направят промени в даден документ, вече няма начини да се обединят двата променени документа. Този начин на действие се нарича работа в самостоятелна среда (stand-alone environment).

Локалната мрежа (LAN) се състои от няколко компютъра и периферни устройства, свързани помежду си и заемащи ограничено пространство - примерно фирмен отдел или сграда. Чрез компютърните мрежи хората могат да поделят ресурси, например файлове и принтери, и да използват интерактивни приложения, като e-mail програми и програми за разписания.

Компютърните мрежи предоставят много предимства, някои от които са:

Намаляване на разходите чрез поделянето на данни и периферии.

Стандартизиране на приложенията.

Навременна обработка на данните.

По-ефективни комуникации и разписания.

И още много други.

В днешни дни мрежите се разраснаха и от **локални (LAN)** се превърнаха в **глобални мрежи (WAN)**, разпростиращи се из целия свят.

Кратък преглед на компютърните мрежи

По принцип всички мрежи имат общи компоненти, функции и възможности, които включват:

Сървъри - компютри, осигуряващи поделени ресурси за мрежовите потребители.

Клиенти - компютри, които ползват поделените мрежови ресурси, осигурявани от сървъра.

Физическа среда (media) - начинът на свързване на компютрите.

Поделени данни - файлове, предоставяни от сървъра по мрежата.

Поделени принтери и други периферни устройства - други ресурси, предоставяни от сървъра.

Ресурси — файлове, принтери и други обекти, използвани от потребителите на мрежата

Дори и при тези сходства, мрежите могат да се разделят на две главни категории:



Равноправни (peer-to-peer)



Базирани на сървър (server-based)

Разликата между равноправната мрежа и тази със сървър е важна, защото всяка от тях предлага различни възможности. Типът на изгражданата мрежа зависи от много фактори:

Големината на фирмата.

Необходимата степен на сигурност.

Видът на бизнеса.

Нивото на административната поддръжка.

Количеството на мрежовия трафик.

Нуждите на мрежовите потребители.

Бюджета на мрежата.

И други.

Равноправни мрежи

При равноправната (peer-to-peer) мрежа няма посветени сървъри (dedicated servers) или йерархия между компютрите. Всички компютри са равнопоставени и затова мрежата се нарича равноправна. Обикновено всеки компютър работи и като сървър (server), и като клиент (client), като няма конкретен администратор, който да отговаря за цялата мрежа. Потребителите сами определят какви данни да поделят в мрежата.

Размер

Равноправните мрежи се наричат още работни групи (workgroups). Терминът работна група визира малка група от хора. Обикновено при равноправната мрежа компютрите не са повече от десет.

Цена

Равноправната мрежа е сравнително проста. Тъй като всеки компютър работи и като клиент, и като сървър, няма нужда от мощен централен сървър или от компонентите, необходими за работата на мрежа с висок капацитет. Равноправните мрежи могат да бъдат по-евтини от мрежите със сървър.

Операционни системи за равноправна мрежа

При равноправната мрежа не е необходимо мрежовият софтуер да има същата производителност и ниво на защита, както при мрежа с сървър.

Мрежи със сървър

В среда с повече от десет потребителя равноправната мрежа (с компютри, изпълняващи функциите и на сървър, и на клиент) вече би била неподходяща. Поради тази причина повечето мрежи имат посветени сървъри (dedicated servers). Посветеният сървър е компютър, работещ само като сървър, без да се използва като клиент или работна станция. Сървърите са "посветени", защото са оптимизирани за бързо обслужване на заявките от мрежовите клиенти и осигуряване на модел за сигурност върху файловете и директориите. Мрежите със сървър се превърнаха в стандартен модел и ще бъдат използвани в примерите по-нататък в книгата.

С нарастването на размера и трафика на мрежите се появи нуждата от повече от един сървър. Разпределянето на задачите между няколко сървъра позволява мрежата да работи възможно най-ефективно.

Специализирани сървъри

Задачите, които сървърите трябва да изпълняват, са разнообразни и сложни. Сървърите за големите мрежи трябва да бъдат специализирани, за да задоволяват нарастващите нужди на потребителите. Например в мрежа под Windows NT Server и следващите мрежови операционни системи има следните видове сървъри:

Файлови и принтерни сървъри (File and print servers). Файловите и принтерни сървъри управляват достъпа на потребителите до файловете и

принтерите. Например, ако сте стартирали приложение за текстообработка, то работи на вашия компютър. Документите на текстообработващата програма, които се съхраняват на файловия и принтерен сървър, се зареждат в паметта на вашия компютър, за да ги редактирате локално. С други думи, файловете и принтерните сървъри служат за съхраняване на файлове и данни.

Сървъри за приложения (Application servers). Сървърите за приложения правят данните и сървърната част (server side) на приложенията от тип клиент/сървър, достъпни за клиентите. Например съхраняват огромни количества данни, които са структурирани с цел по-лесното им извличане. Този вариант се различава от случая с файловете и принтерни сървъри. При тях данните или файловете се свалят (download) на клиентския компютър, направил заявката. При сървъра за приложения базата от данни се намира на сървъра, а на клиентския компютър се свалят само резултатите от направената заявка. Клиентското приложение, което е стартирано локално, получава достъп до данните на сървъра за приложения. Вместо цялата база данни от сървъра да се сваля на локалния компютър, на него се зареждат само резултатите от заявката. Можете например да претърсвате базата от данни за служителите, търсейки всички, които са родени през ноември.

Пощенски сървъри. Пощенските сървъри управляват електронните съобщения между потребителите на мрежата.

Факс сървъри. Факс сървърите управляват трафика на факсове към и от мрежата, като поделят една или повече факс-модемни карти.

Комуникационни сървъри. Комуникационните сървъри управляват потока от данни и e-mail съобщения между мрежата, на която принадлежат, и останалите мрежи, големи (mainframe) машини или отдалечени потребители, използващи

модеми и телефонни линии за връзка със сървъра.

Сървъри за директорийни услуги. Сървърите за директорийни услуги позволяват на потребителите да локализират, съхраняват и защитават информацията в мрежата. Windows NT Server обединява компютрите в логически групи, наречени домейни, които позволяват на всеки потребител в мрежата да получи достъп до всички нейни ресурси.

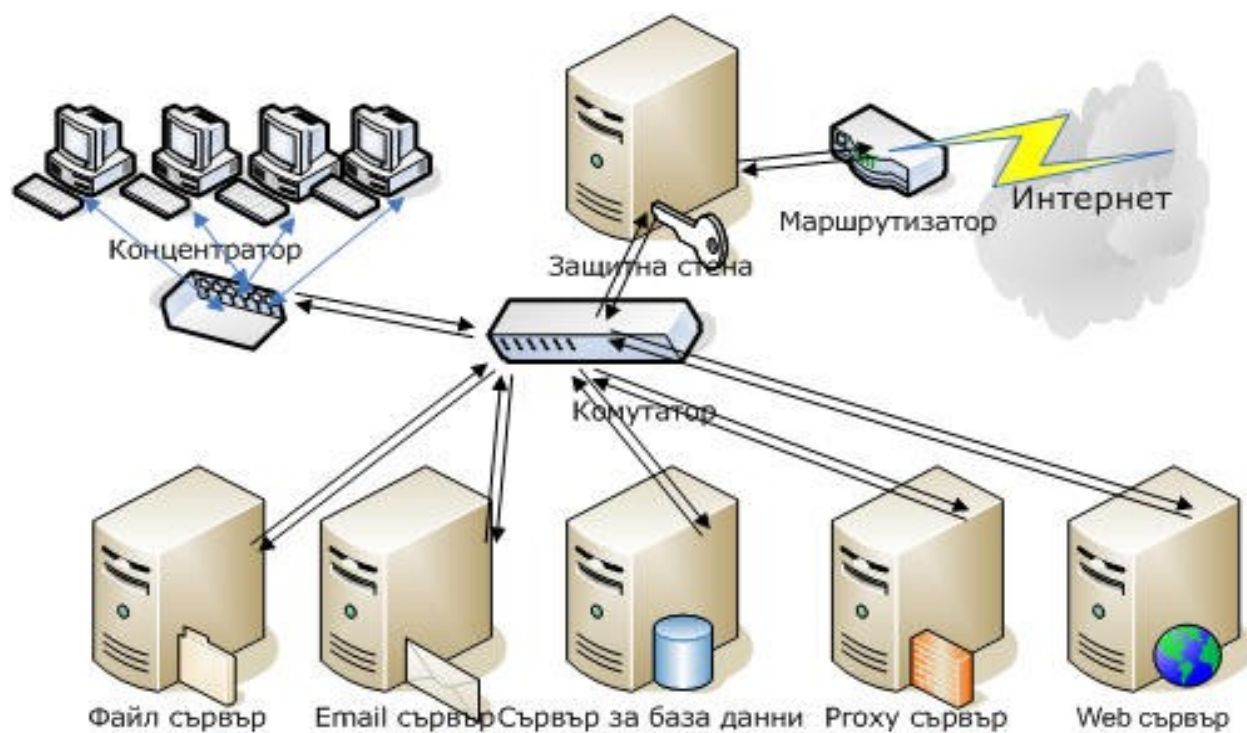
С разширяването на мрежата става все по-важно да се планират различните сървъри. Проектантът на мрежата трябва да предвиди **възможното ѝ разрастване**, така че работата с мрежата да не бъде прекъсната, ако се наложи промяна на ролята на даден специализиран сървър.

Комбинираните мрежи

В модерните мрежи често се комбинират най-добрите възможности на равноправните мрежи и на мрежите със сървъри.

При комбинираната мрежа две операционни системи работят съвместно, за да осигурят функционирането на цялата мрежа.

Операционните системи за сървър, каквито са Microsoft Windows NT Server, Novell® NetWare® или Linux(Unix) се грижат за поделянето на основните приложения и данни.



Специализирани сървъри

Клиентските компютри могат да работят под произволна операционна система. Те могат както да достъпват ресурсите на сървъра, така и да поделят своя твърд диск и да правят достъпни своите персонални данни, когато това се налага.



Комбинираните мрежи имат посветени сървъри и компютри

Такъв тип мрежа се среща често, но изисква по-сериозно предварително планиране и подготовка, за да се осигури добра защита.

Мрежови устройства

Физическа среда (media)

Основни видове кабели

Огромна част от съвременните мрежи са свързани с някакъв вид кабел, който служи за среда за предаване на сигналите между компютрите. Има различни кабели за различни цели и за различни по размер мрежи - от малка до голяма.

Окабеляването може да бъде доста сложно. Фирмата Belden, водещият производител на кабели, разполага с каталог с повече от 2200 типа кабели. За щастие само три основни групи от кабели се използват в повечето мрежи:

Коаксиални (coaxial)

С усукана двойка проводници (twisted-pair)

Неекраниран (unshielded) кабел с усукана двойка проводници.

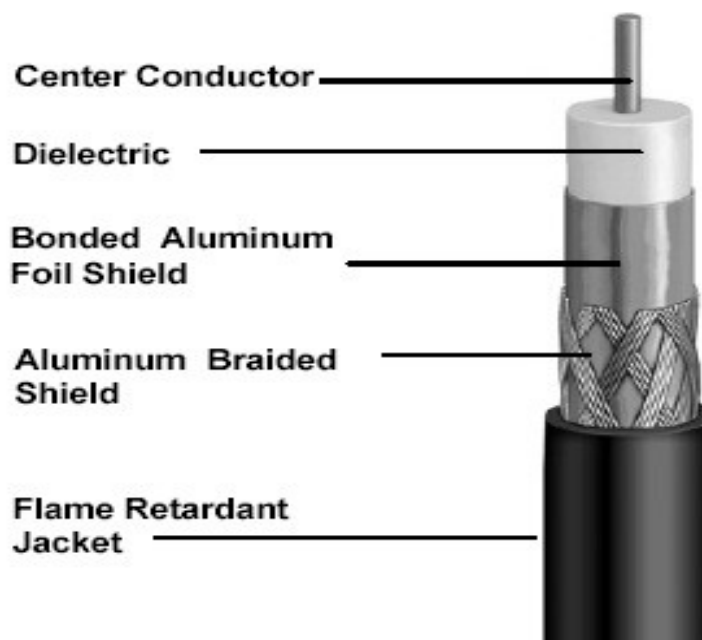
Екраниран (shielded) кабел с усукана двойка проводници.

С оптични нишки (fiber-optic).

Коаксиален кабел

Някога коаксиалният кабел бе един от най-широко използваните мрежови кабели. За това имаше редица причини. Той е относително евтин, лек, гъвкав и с него лесно се работи. Популярността му се дължи и на това, че инсталирането му е сигурен и лесен процес.

В най-простия си вариант коаксиалният кабел се състои от медно ядро, обвито с изолационен материал, върху който има оплетка от мед и алуминий и накрая външна обвивка. Ако има първи изолационен слой от фолио и втори слой от оплетена метална обвивка, наричаме го двойно екраниран. За работни среди със силни смущения има кабели с четворна защита, която се състои от два слоя пластмасова изолация и два слоя метална оплетка.



Коаксиален кабел

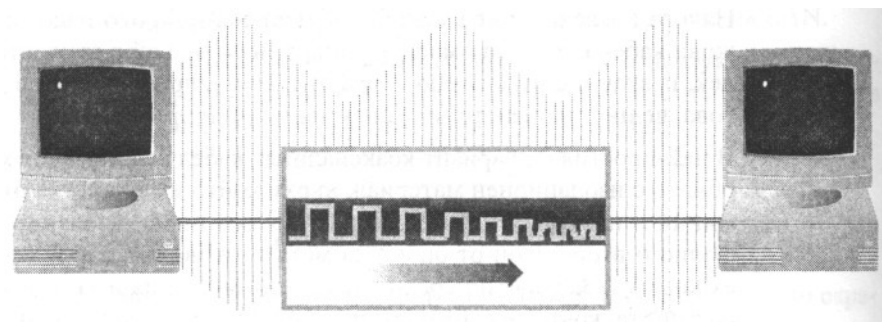
Екранирането се осигурява от металната оплетка (мрежа, изплетена от метални нишки), която обвива проводника. Тя предпазва предаваните данни от нахлуване на случайни (странични) електронни сигнали, които се наричат шум и могат да повредят информацията.

Сърцевината на коаксиалния кабел пренася електронните сигнали, които представляват данните. Тази сърцевина може да бъде както плътна (един проводник), така и изплетена (от много жици). Ако сърцевината е плътна, тя обикновено е медна.

Сърцевината е заобиколена от диелектричен изолационен слой, отделящ я от металната оплетка, която служи за заземяване и предпазва проводника от електрически шумове и преплитане на сигнали от съседни проводници. Преплитане (crosstalk) е смесване на сигнала с този от съседен проводник.

Проводящата сърцевина и металната оплетка трябва винаги да са разделени. Ако се докосват, ще дават накъсо, и шумовете и блуждаещите сигнали от оплетката ще се предадат по проводника, което ще доведе до унищожаване на данните. Целият кабел е заграден от външна изолация, обикновено каучукова, тефлонова или пластмасова.

Коаксиалният кабел е по-устойчив на смущения и заглъхване от кабела с усукана двойка проводници. Заглъхването е загуба на силата на сигнала, възникваща при предаване на сигнали по меден кабел на големи разстояния.



Загльхването води до влошаване качеството на сигнала

Защитната обвивка може да абсорбира блуждаещите електронни сигнали, така че те да не повлияят на данните, изпращани по вътрешния меден кабел. Поради тази причина коаксиалният кабел е добър вариант за надеждно изпращане на данни с висока скорост на дълги разстояния и с не толкова сложно оборудване.

Видове коаксиални кабели

Има два основни вида коаксиални кабели:

Тънък (thinnet)

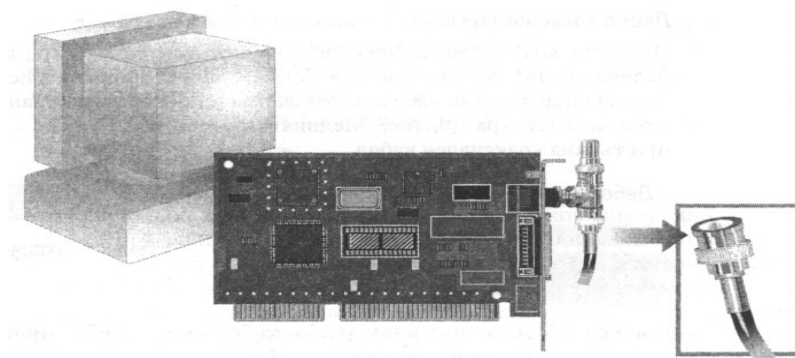
Дебел (thicknet)

Кой вид ще изберете зависи от нуждите на конкретната мрежа.

Тънък коаксиален кабел

Тънкият коаксиален кабел (thinnet) е гъвкав кабел с дебелина около 0.25 инча. Поради това че е гъвкав и с него лесно се работи, той може да се използва за инсталация на почти всеки вид мрежа. Тънкият коаксиален кабел се свързва

директно към мрежовите адаптерни карти на компютрите.



Свързване на тънък коаксиален кабел към компютъра

Тънкият коаксиален кабел може да предава сигналите на разстояние до 185 метра (около 607 фута; 1 фут = 30.48 см), без да се получи заглъхване.

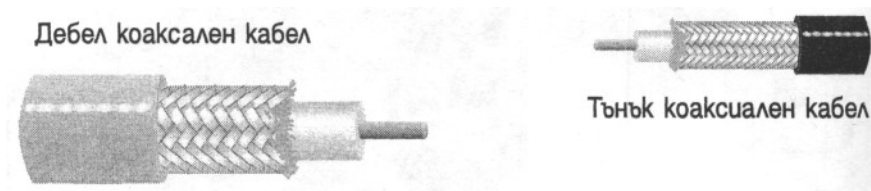
Производителите на кабели са приели определени правила за различните видове кабели. Тънкият коаксиален кабел е включен в групата RG-58 и има импеданс от 50 ома. Импедансът е електрическото съпротивление, което се оказва на променливия ток в проводника и се измерва в оме. Основните различия в групата RG-58 са в централния меден проводник. Той може да бъде или жица с преплетени нишки, или плътен меден проводник.



RG-58 коаксиални кабели с преплетена жица и с плътен проводник

Дебелият коаксиален кабел (thicknet) е относително твърд кабел с дебелина

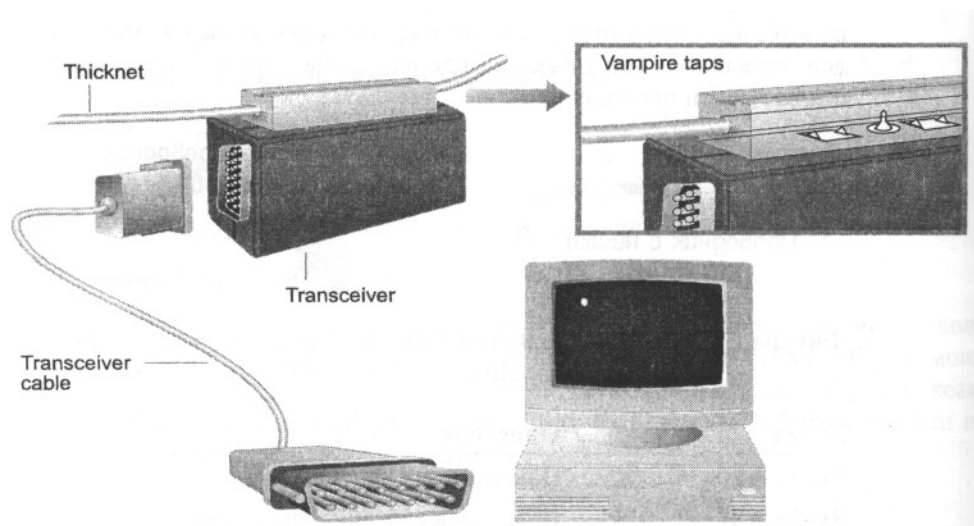
около 0.5 инча. Той понякога се нарича Standard Ethernet, защото беше първият тип кабел, използван за широкоразпространената мрежова архитектура Ethernet. Медният проводник е по-дебел, отколкото при тънкия коаксиален кабел.



Дебелият коаксиален кабел има по-дебел проводник от тънкия коаксиален кабел

Колкото по дебел е проводникът, толкова по-далече кабелът може да пренася сигнали. Това означава, че дебелият коаксиален кабел може да пренася сигналите на по-големи разстояния от тънкия кабел - на около 500 метра (около 1640 фута). Поради тази причина дебелият коаксиален кабел се използва като гръбнак (backbone) за свързване на няколко по-малки мрежи, окабелени с тънък коаксиален кабел.

Едно устройство, наречено **трансийвър (transceiver - приемо-предавател)**, свързва тънкия коаксиален кабел към дебелия коаксиален кабел.



Трансийвър за дебел коаксиален кабел с вампирска тапа, пронизваща сърцевината (проводника)

Трансийвърът е проектиран за дебел Ethernet кабел, включващ конектор, известен като "вампирска букса" (vampire tap) или "пронизваща букса" (piercing tap), чрез който се извършва действителната физическа връзка с проводника на дебелия коаксиален кабел. Този конектор пробоща изолационния слой и осъществява директна връзка с проводника. Връзката между трансийвъра и мрежовата адаптерна карта се осъществява с помощта на специален трансийвърен кабел, който се свързва към AUI5-конектора на мрежовата карта. AUI конекторът за дебелия коаксиален кабел е известен още като Digital Intel Xerox® (DIX конектор), на имената на трите компании, които са го създали, или като DB-15 конектор.

Тънък коаксиален или дебел коаксиален кабел

В общи линии, колкото по-дебел е кабелът, толкова по-трудно се работи с него. Тънкият кабел е гъвкав, лесен за инсталиране и относително евтин. Дебелият кабел не е лесен за огъване и затова инсталирането му е по-трудно.

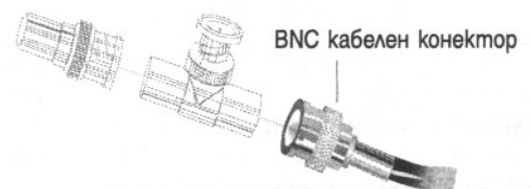
Трябва да имате предвид това съображение, когато инсталацията изисква прокарване на кабела през тесни места - например тръби. Дебелият коаксиален кабел е по-скъп от тънкия, но може да пренася сигнала на по-голямо разстояние.

Хардуер за свързване на коаксиални кабели

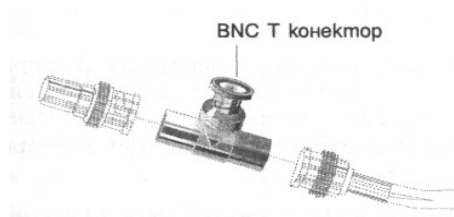
И тънкия, и дебелият коаксиални кабели използват компонент за свързване, известен като **BNC (British Naval Connector)** конектор, който осъществява връзката между кабела и компютрите. Семейството BNC конектори има няколко важни компонента:

BNC кабелен конектор

BNC кабелният конектор е или запоен, или закрепен с помощта на кримпер-клещи към края на кабела.

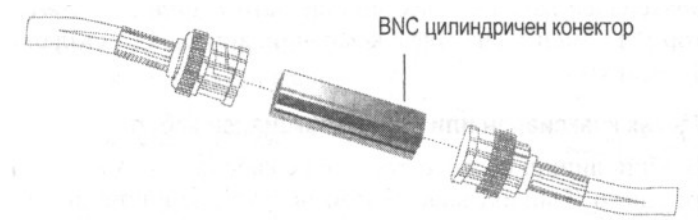


BNC кабелен конектор



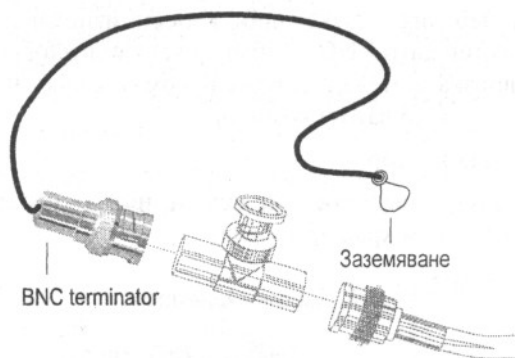
BNC T конектор

Този конектор свързва мрежовата интерфейсна карта към мрежовия кабел.



BNC цилиндричен конектор

Използва се за свързване на два тънки коаксиални кабела, за да се получи по-голяма дължина.



BNC терминатор

BNC терминаторът затваря всеки край на шинния кабел, за да абсорбира блуждаещите сигнали. Без BNC терминатор шинната мрежа няма да функционира.

Коаксиални кабели и противопожарни изисквания

Типът на използвания от вас коаксиален кабел зависи от неговото

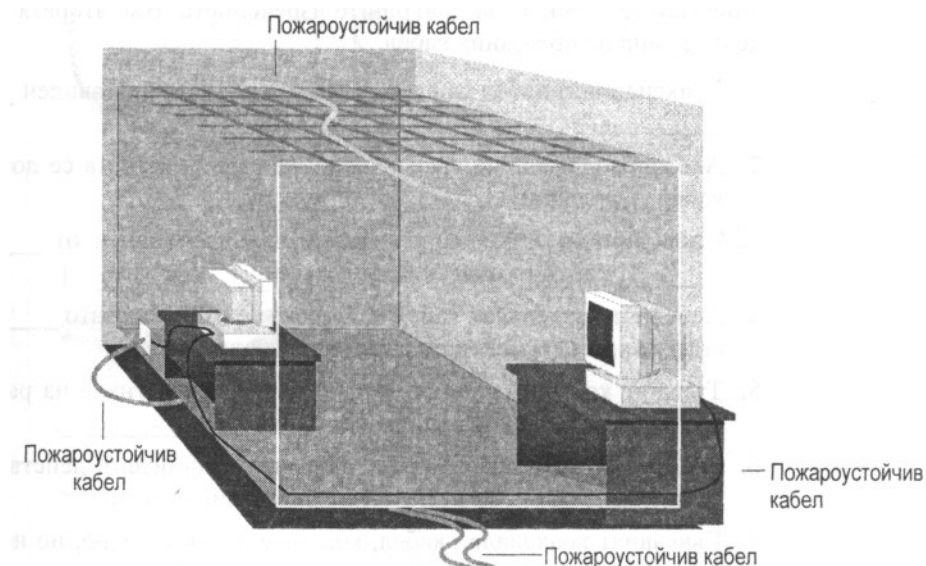
местоположение в офиса ви. Има два типа коаксиални кабели, в зависимост от изолационния материал:

Поливинилхлоридни (PVC)

Пожароустойчиви (plenum)

Поливинилхлоридът е вид пластмаса, използвана за направата на изолацията и на кабелната обвивка за повечето видове коаксиални кабели. Поливинилхлоридните коаксиални кабели са гъвкави и могат лесно да се прокарват през отворените пространства в офиса. Неприятното е, че когато се запалят, изпускат отровен дим.

Пожароустойчивите кабели използват тясното пространство между фалшивия таван (окачен таван) и долната част на пода на горното помещение (истинския таван) в някои сгради. Това разстояние се нарича пленум (plenum). То се използва за циркулиране на топлия и студен въздух в сградата. Противопожарните правила изискват през тази зона да се прокарва специално окабеляване, защото всякакъв дим или газ, минаващ оттук, може да бъде вдишан от всички хора в сградата.



Противопожарните правила изискват пожароустойчиви кабели, които използват тясното пространство между фалшивият и истинския таван

Пожароустойчивите кабели (plenum) са коаксиални кабели, съдържащи специални материали в своята изолационна обвивка. Тези материали са устойчиви на огън и при запалване произвеждат минимално количество дим, което намалява опасността от натравяне. Пожароустойчивите кабели могат да се използват в пространствата над тавана, както и да се прокарват във вертикална посока (например в стените, зад ламперия и пр.), без необходимост от тръби. Но те са по-скъпи и по-малко гъвкави от кабелите с PVC изолация.

Забележка: Трябва да се консултирате със специалистите по противопожарната и електрическата безопасност относно правилата за прокарване на мрежови кабели в сградата на вашия офис.

Избор на коаксиален кабел

При изборът на коаксиален кабел трябва да се съобразите с някои условия.

Използвайте коаксиален кабел, ако ви трябва:

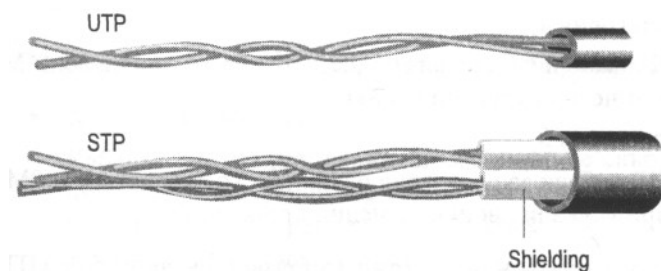
Физическа среда, по която ще се предават глас, видео и данни.

Да предавате данни на дълги разстояния, за които по-евтиното окабеляване няма да свърши работа.

Позната технология, предлагаща разумно ниво на защита на данните.

Кабел с усукана двойка проводници

В най-елементарния си вариант кабелът с усукана двойка проводници (twisted-pair) се състои от два изолирани и взаимно усукани медни проводника. Има два вида кабели с усукана двойка проводници: неекранирани (unshielded twisted-pair - UTP) и екранирани (shielded twisted-pair - STP).



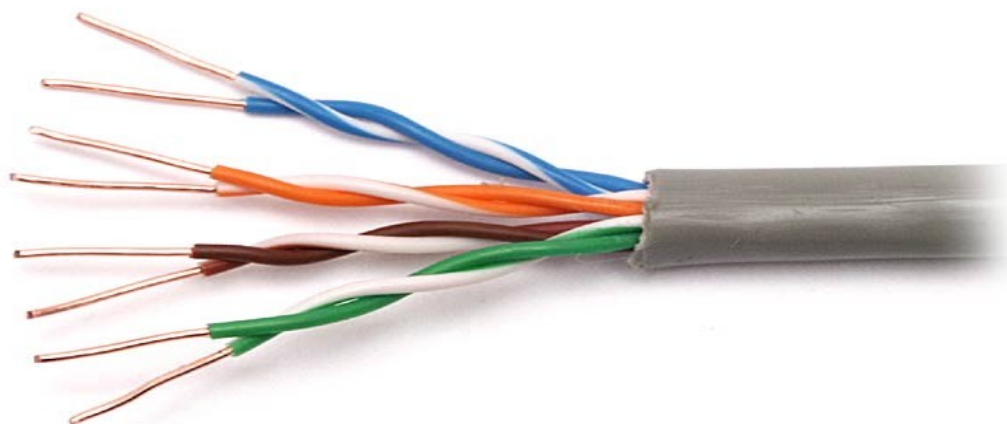
Неекраниран кабел и екраниран кабел с усукана двойка проводници

Често няколко двойки от усукани проводници са групирани заедно и са поставени в обща защитна обвивка, оформяйки кабели. Броят на двойките проводници е различен. Усукването на проводниците намалява (но не елиминира) външните шумове, причинени от различни източници, като двигатели, релета, трансформатори и др.

Неекраниран кабел с усукана двойка проводници (UTP)

UTP, използващ спецификацията 10BaseT, е най-популярният вид кабел с усукана двойка проводници и бързо се превръща в най-широко разпространения тип окабеляване за LAN. Максималната дължина на един сегмент е 100 метра или около 328 фута.

UTP се състои от два изолирани медни проводника. Има спецификации, които определят колко двойки са разрешени за дължина на кабела от един фут. В Северна Америка голяма част от телефонните системи използват UTP кабел, затова той е предварително инсталиран в много офис сгради.



UTP кабел (неекранирана усукана двойка)

UTP е дефиниран от стандарта за окабеляване на търговски сгради (568 Commercial Building Wiring Standard) на Electronic Industries Association и на Telecommunications Industries Association (EIA/TIA). Този стандарт разделя UTP кабелите на пет категории:

- Категория 1. Традиционните UTP телефонни кабели, които могат да

пренасят глас, но не и данни. До 1983 г. повечето телефонни кабели бяха от Категория 1.

- Категория 2. UTP кабели за предаване на данни със скорост до 4Mbps (мегабита в секунда). Състоят се от четири усукани двойки.

- Категория 3. UTP кабели за предаване на данни със скорост до 10Mbps. Има четири усукани двойки с по три усуквания на всеки фут.

- Категория 4. UTP кабели за предаване на данни със скорост до 16Mbps. Състои се от четири усукани двойки.

- Категория 5. UTP кабели за предаване на данни със скорост до 100Mbps. Има четири усукани двойки от медни проводници.

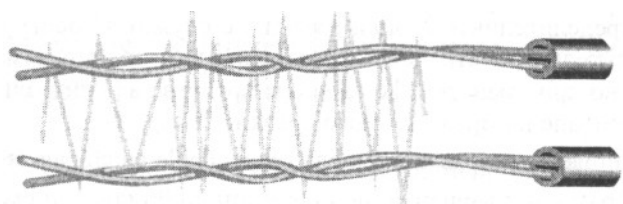
- Категория 5e (Enhanced). UTP кабели за предаване на данни със скорост до 1000Mbps. Има четири усукани двойки от медни проводници.

- Категория 6. UTP кабели за предаване на данни със скорост до 1000Mbps. Има четири усукани двойки от медни проводници.

Повечето телефонни системи използват някакъв вид UTP. Всъщност една от причините UTP да е толкова разпространен е, че доста сгради предварително са окабелени с него, а и често е инсталиран допълнителен UTP кабел за бъдещи нужди. Ако този предварително инсталиран кабел е от достатъчно добра категория, за да покрие изискванията за предаване на данни, той може да се използва за изграждане на компютърна мрежа. Трябва обаче да се внимава, защото стандартните телефонни кабели може и да не разполагат с точното усукване и

други електрически характеристики, необходими за чисто и сигурно предаване на компютърни данни.

Един от потенциалните проблеми за всички видове кабели е преплитането на сигналите. Ако си спомняте, преплитане (crosstalk) се получава, когато сигналът от една линия се смесва с този от друга линия. UTP кабелът по принцип е податлив на преплитане. За да се избегне този недостатък, се използва екранирането (shielding).

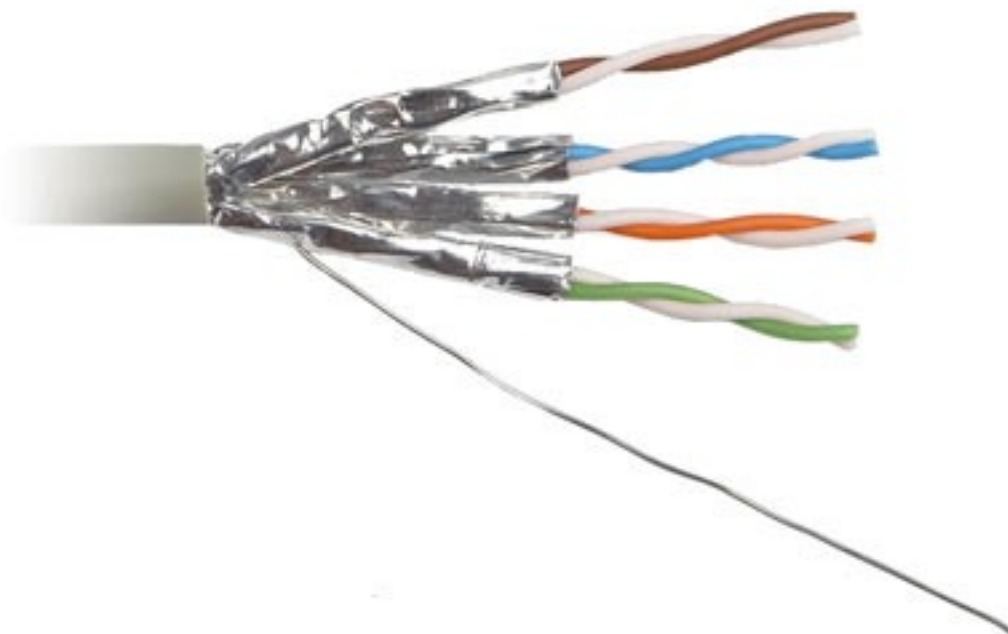


Преплитането се получава при смесване на сигналите от две линии

Екраниран кабел с усукана двойка проводници (STP)

STP използва за обвивка медна оплетка, поради което е по-висококачествен и надежден от UTP. При STP се използва и пластмасова обвивка между и около двойките проводници. В резултат на това STP кабелът осигурява чудесна защита на предаваните данни от външни смущения.

Тъй като STP е по-малко податлив на електрически смущения, той поддържа по-висока скорост на предаване на данните на по-дълги разстояния, отколкото UTP.



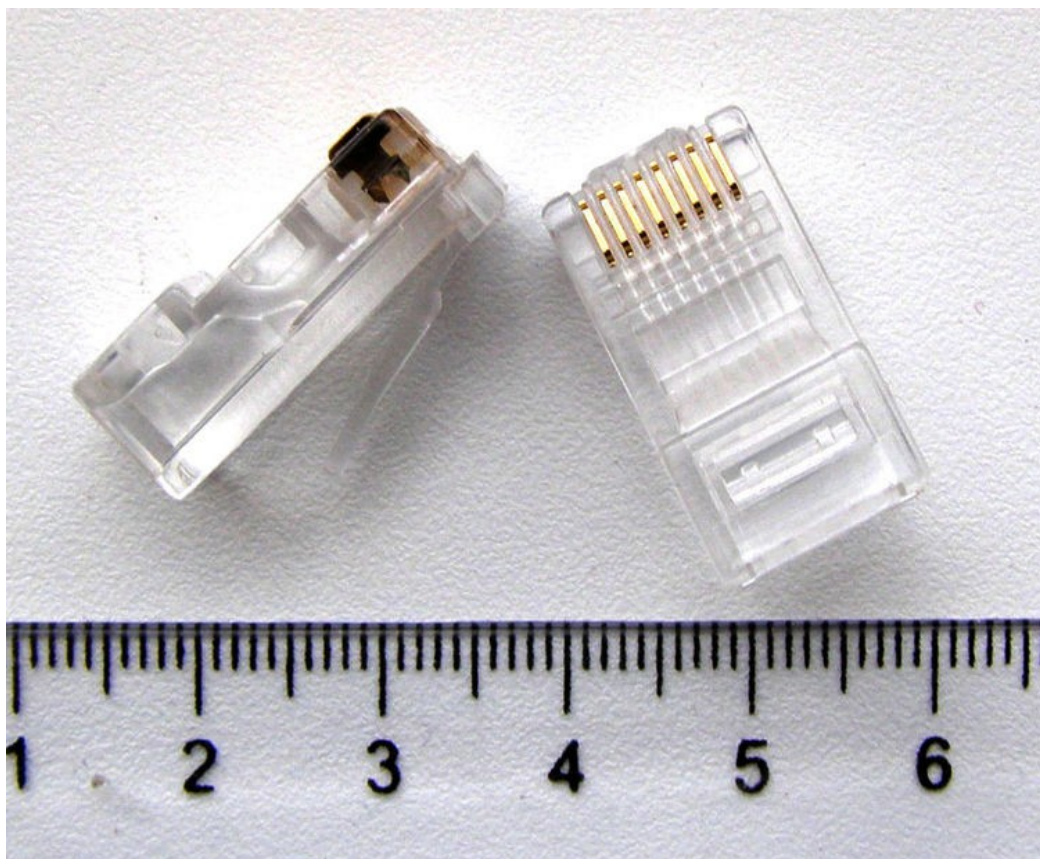
STPкабел

Компоненти на кабелите с усукана двойка проводници

Хардуер за свързване

Кабелът с усуканата двойка проводници се свързва към компютъра чрез телефонен **конектор RJ-45**, който наподобява телефонния конектор RJ-11. Въпреки че на пръв поглед изглеждат еднакви, между тях има съществени разлики.

RJ-45 е малко по-голям и не влиза в буксата за RJ-11. Той има осем кабелни връзки, докато при RJ-11 те са само четири.



RJ-45 конектор



RJ-45 бункс

Има няколко компонента, които помагат за изграждането на големи UTP

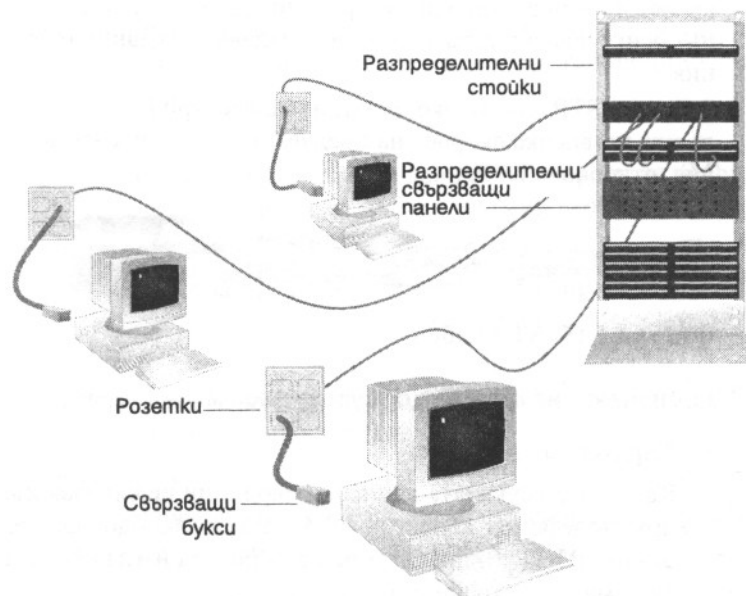
инсталации и улесняват работата с тях:

Разпределителни стойки с рафтове (distribution racks and rack shelves)
Разпределителните стойки с рафтове служат за осигуряване на допълнително пространство за кабелите там, където няма достатъчно подово пространство. Те са добро средство за централизиране и организиране на мрежа с много връзки. **Разширяеми свързващи панели (expandable patch panels).** Има различни варианти, поддържащи до 96 порта и скорост на предаване от 100Mbps.

Свързващи букси (fack couplers)

Тези единични или двойни RJ-45 букси се пъхат в разширяемите свързващи панели и в розетките, и поддържат скорости до 100 Mbps.

Розетки (wall plates) Поддържат две или повече свързващи букси



Различни компоненти за кабелите от тип усукана двойка

Избор на кабел с усукана двойка проводници

Използвайте кабел с усукана двойка проводници, ако:

Вашата LAN е с ограничен бюджет.

Желаете относително лесна инсталация, при която компютърните връзки са прости.

Не използвайте кабел с усукана двойка, ако:

Ви трябва абсолютно сигурен трансфер на данни на голямо разстояние и с висока скорост.

Кабел с оптични нишки

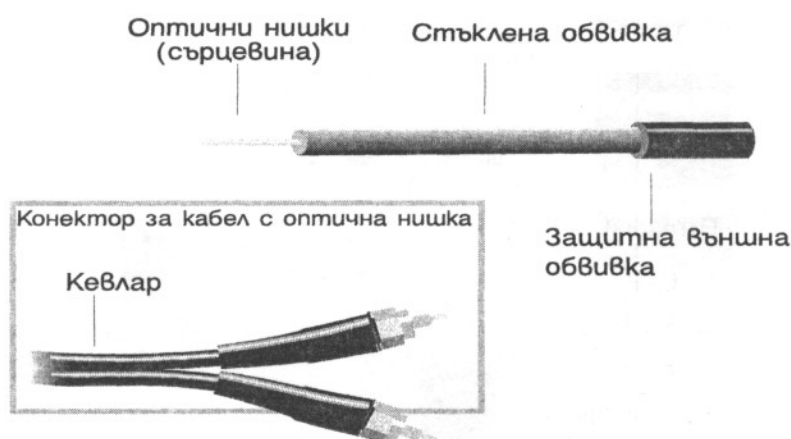
При кабела с оптични нишки (fiber-optic cable) цифровите сигнали се пренасят от оптичните нишки под формата на модулирани светлинни импулси. Това е относително безопасен начин за изпращане на данни, защото по оптичния кабел не пътуват електрически импулси. Това означава, че кабелите с оптични нишки не могат да бъдат "подслушвани", за да се откраднат данни, което е възможно при всички видове медни кабели, пренасящи електронни сигнали.

Кабелите с оптични нишки се характеризират с високоскоростно, висококапацитетно предаване на данните, тъй като няма заглъхване и сигналът е много чист.

Състав на кабела с оптични нишки

Оптичните нишки (optic fibers) представляват изключително тънко цилиндрично стъкло, наречено сърцевина (core), облицовано в концентричен стъклен слой, известен като обвивка (cladding). Понякога нишките се правят от пластмаса, която е по-лесна за инсталиране, но не може да пренася светлинните импулси на толкова дълго разстояние, колкото стъклото.

Всяка стъклена нишка пренася сигнала само в една посока, така че кабелът се състои от две нишки в отделни обвивки. Едната нишка предава, а другата приема. Подсилващ слой пластмаса обгражда всяка от стъклените нишки, като необходимата якост се осигурява от кевларни нишки (kevlar fibers). (Вижте фигура 2.18). Кевларните нишки в оптичния конектор са поставени между двата кабела, които са обвити с пластмаса.



Кабел с оптични нишки

Предаването по кабелите с оптични нишки сигнали не се влияят от електрически смущения и са много бързи (понастоящем скоростта е 100 Mbps, но може да достига нива, по-високи от 1 Gbps). Сигналите могат да се пренасят на много километри под формата на светлинни импулси.

Съображения за кабелите с оптични нишки

Използвайте кабел с оптични нишки, ако:

Трябва да предавате данни с голяма скорост на дълги разстояния по много добре защитена физическа среда.

Не използвайте кабел с оптични нишки, ако:

Сте с ограничен бюджет (Забележка: Цените на оптичните кабели са съизмерими с тези на най-висококачествените медни кабели.)

Нямате необходимия опит, за да инсталирате и свържете устройствата към него. (*Забележка: Работата с оптични кабели става все по-лесна. Техниките за полиране и терминиране изискват все по-малко части и по-малък технически опит.)

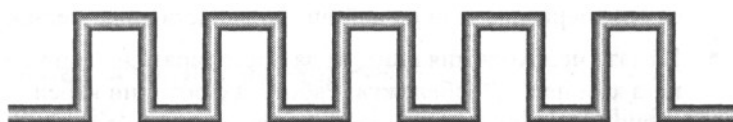
Предаване на сигнала

За предаването на кодиран сигнал по кабел се използват две техники едноканално (baseband) и многоканално (broadband) предаване.

Едноканално предаване

Едноканалните (baseband) системи предават цифрови сигнали по единствен канал (на една честота). Сигналите се предават под формата на

дискретни електрически или светлинни импулси. Капацитетът на целия комуникационен канал се използва за предаване на един-единствен сигнал с данни. Цифровият сигнал използва цялата пропускателна способност на кабела, която образува само един канал. "Пропускателна способност" на кабела, или така наречената "ширина на честотната лента" (bandwidth), е разликата между най-високата и най-ниската честоти, на които се предават сигнали по този кабел.



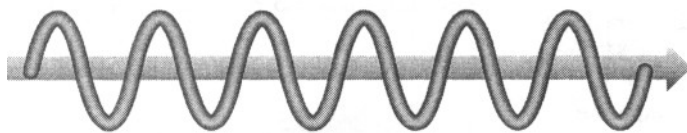
Едноканално предаване, показващо цифрова вълна

Пътувайки по мрежовия кабел, сигналът постепенно губи силата си и може да се изкриви. Ако кабелът е дълъг, в края му се получава твърде слаб или изкривен сигнал, който може да бъде разпознат погрешно или изобщо да не бъде разпознат.

За предпазна мярка едноканалните системи използват повторители (repeaters), които получават сигнала и го препредават с първоначалната му сила, като по този начин позволяват да се увеличи дължината на кабела.

Многоканално (широколентово) предаване

Широколентовите (broadband) системи за многоканално предаване използват аналогови сигнали и диапазон от честоти. При аналоговото предаване сигналите са непрекъснати (недискретни). Те пътуват по физическата съобщителна среда под формата на електромагнитни или оптични вълни. При широколентовото предаване сигналът пътува само в едната посока.



Широкополосно предаване, показващо еднопосочна аналогова вълна

Ако ширината на честотната лента на кабела е достатъчна, той ще може да се използва едновременно от няколко аналогови предавателни системи, например кабелна телевизия и компютърна мрежа.

Всяка предавателна система заема определена част от общата широчина на лентата. Всички устройства на съответната предавателна система, например всички компютри в мрежата, трябва да бъдат настроени да използват честоти, които са в рамките на определения диапазон.

Докато системите за едноканално предаване използват повторители, широкополосните системи използват усилватели за възстановяване на аналоговите сигнали до тяхната първоначална величина.

Тъй като сигналът при широкополосното предаване пътува само в едната посока, трябва да има два пътя за данните, за да могат сигналите да достигат до всички устройства. За тази цел се използват два подхода:

Mid-split broadband - ширината на честотната лента се разделя на два канала, всеки от които използва различна честота или диапазон от честоти. Единият от каналите се използва за предаване на сигналите, а другият - за приемането им.

Dual-cable broadband - към всяко устройство се свързват два кабела.

Единият се използва за предаване, а другият - за приемане.

Безжична среда

Безжичните среди все повече се налагат като удачни варианти за мрежа. С напредъка на технологиите, производителите ще могат да предлагат на пазара все повече продукти на атрактивни цени, което ще доведе до нарастване на търсенето и на продажбите. А с нарастването на търсенето, безжичните мрежови среди ще стават все по-разнообразни и все по-добри.

Терминът **"безжични" (wireless)** заблуждава, защото предполага пълното отсъствие на кабели. В повечето случаи това не е така. Почти всички безжични мрежи всъщност се състоят от безжични компоненти, комуникиращи с обикновена кабелна мрежа, като по този начин образуват смесена мрежа, наречена хибрид (hybrid).

Възможности, предлагани от безжичните мрежи

Идеята за безжични мрежи е привлекателна поради следните причини:

Осигурява временна връзка към съществуваща кабелна мрежа.

Спомага да се осигури резервна на съществуваща мрежа.

Осигурява някакво ниво на преносимост.

Прескача ограниченията, наложени от медните и дори от оптичните кабели.

Използване на безжичните мрежи

Трудностите при прокарването на кабели водят до все по-нарастващото използване на безжичните мрежи. Те са полезни при следните случаи:

Натоварени зони, като фойета или рецепции.

Хора, които постоянно са в движение, като например лекарите и медицинските сестри в болниците.

Изолирани зони и сгради.

Отдели, в които интериорът често се променя.

Някои специални места, като например исторически сгради, където окабеляването е трудна задача.

Видове безжични мрежи

Безжичните мрежи могат да се разделят на три категории на базата на използваната технология:

Локални мрежи

Разширени локални мрежи

С използване на мобилни компютри

Основната разлика между тези категории се крие в съоръженията за предаване. Безжичните LAN мрежи и разширените LAN мрежи използват предаватели и приемници, собственост на фирмата, която изгражда мрежата. Мобилните компютърни потребители използват обществени услуги, като тези на AT&T, MCI, Sprint и местните телефонни компании, за да предават и получават сигнали.

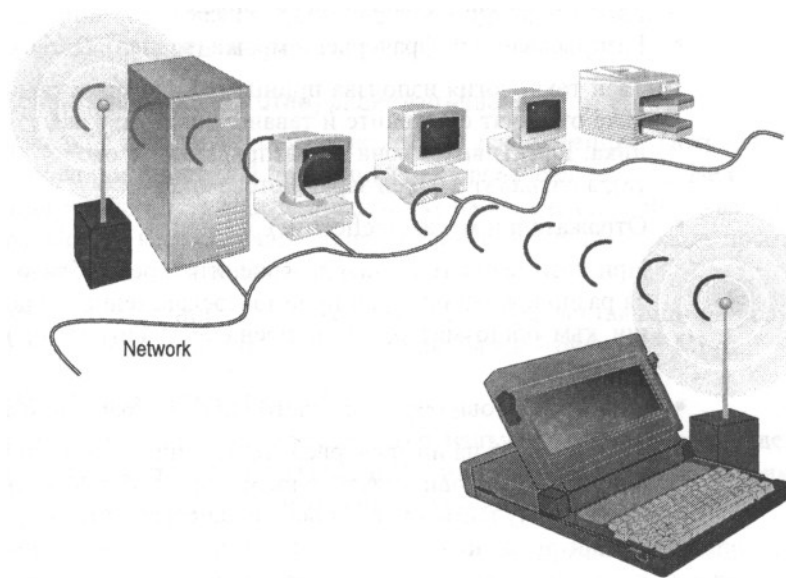
Локални мрежи

Стандартните безжични локални мрежи изглеждат и работят точно както и тези с кабели, с изключение на физическата среда. Във всеки компютър се инсталира безжична мрежова адаптерна карта с приемо-предавателно устройство, наречено трансийвър (transceiver), а потребителите комуникират с мрежата по същия начин, както ако бяха свързани с кабел.

Точки на достъп

Трансийвърите, понякога наричани още и точки на достъп (access points), излъчват и получават сигнали от заобикалящите ги компютри, като ги препредават по безжична или кабелна среда.

Безжичните локални мрежи използват за връзка с кабелната мрежа малки трансийвъри, монтирани в стените. Трансийвърите установяват радио-контакт с портативните мрежови устройства. Това не е изцяло



Безжичен портативен компютър, свързан чрез точка на достъп към кабелна мрежа

Техники на предаване

Безжичните локални мрежи използват четири техники за предаване на данни:

1. Инфрачервена (infrared)

2. Лазерна (laser)

3. Теснолентово (narrow-band) или едночестотно (single-frequency) радиоизлъчване

4. Радиоизлъчване с разпределен спектър (spread-spectrum radio)

Инфрачервени мрежи

Всички инфрачервени безжични мрежи използват инфрачервено светлинно

излъчване, което пренася данните между устройствата. Тези системи трябва да генерират много силни сигнали, защото слабите сигнали са податливи на влияния от други светлинни източници, например светлина от прозорците.

При този метод сигналите могат да се предават с висока скорост, тъй като инфрачервената светлина има голяма широчина на честотната лента. При нормални обстоятелства една инфрачервена мрежа може да предава със скорост от 10Mbps.

Има четири вида инфрачервени мрежи:

- С пряка видимост (line-of-sight)

Както се вижда от наименованието, този метод работи само когато приемникът и предавателят имат пряка ("видима") светлинна връзка помежду си, т.е. могат да се "виждат" един друг.

- Разпръскващи инфрачервени мрежи (scatter infrared)

Тази технология използва принципа на разпръскването, като сигналите отскачат от стените и тавана, докато накрая стигнат до приемника. Ефективната зона на разпръскване е около 30 метра (100 фута), а сигналят е бавен заради отскачането.

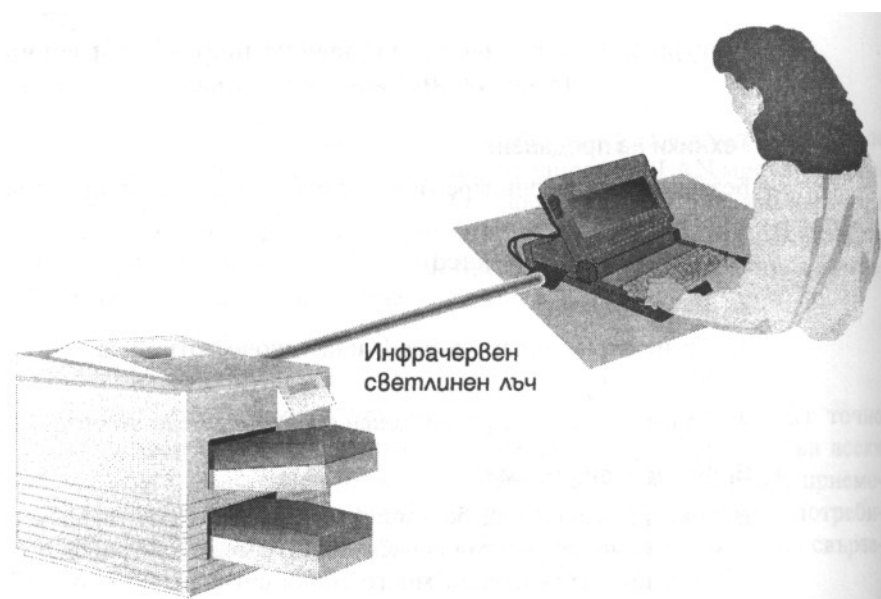
- Отражателни мрежи (reflective)

При този вариант на инфрачервените мрежи близо до компютрите са разположени оптични приемо-предавателни устройства, излъчващи към общо

място, което пренасочва сигналите към съответния компютър.

- Широколентови оптични телеточки (broadband optical telepoint)

Този вариант на инфрачервените безжични локални мрежи осигурява широколентови услуги с възможност за предаване на висококачествена мултимедия със същото качество, предлагано от кабелните мрежи.



Безжичен портативен компютър, използващ инфрачервени светлинни лъчи за връзка с принтера

Скоростта и удобството, предлагани от инфрачервените мрежи, представляват голям интерес, но предаванията на разстояния, по-големи от 30 метра (100 фута), са доста затруднени. Освен това инфрачервените мрежи са обект на смущения, причинявани от силна околна светлина, каквато е характерна за повечето офиси.

Лазерни мрежи

Лазерната технология прилича на инфрачервената по това, че изисква пряка видимост, и всяко нещо (човек или предмет), което прекъсне този лъч, блокира предаването.

Теснолентово (едночестотно) радиоизлъчване

Този подход е подобен на излъчването от радиостанция. Потребителят настройва предавателя и приемника на определена честота. Не се изисква пряка видимост, защото диапазонът на излъчване е 5000 квадратни метра. Но тъй като сигналят е високочестотен, той не може да премине през стоманени или бетонни стени.

Клиентите се абонират за такъв тип мрежа към доставчици на услуги, като Motorola. Този метод е относително бавен - около 4.8 Mbps.

Мрежи с разпределен спектър

Радиомрежите с разпределен спектър излъчват сигнали в определен диапазон от честоти. По този начин се избягват проблемите, възникващи при мрежите с теснолентово радиоизлъчване.

Наличните честоти са разделени на канали. Адаптерите за разпределен спектър се настройват на даден канал за предварително-определен период от време, след което превключват на друг канал. Компютрите от мрежата се синхронизират спрямо последователността на смяна на каналите. Така се осигурява една своеобразна "вградена" защита, при която трябва да е известен алгоритъмът на смяна на каналите, за да може да бъде подслушван потокът от данни.

С цел да се подсили допълнително защитата и да се предотврати възможността за неправомерно послушване на излъчвания сигнал, изпращачът и получателят могат да шифроват (кодират) предаването.

Стандартната скорост от 250 Kbps (килобита в секунда) прави този метод много по-бавен от останалите. Обаче при някои мрежи с радиоизлъчване с разпределен спектър може да се реализира скорост от 4 Mbps за разстояние от две мили на открито и повече от 250 метра (800 фута) на закрито.

Този вид мрежи предлагат изцяло безжична среда. Например два или повече компютри с карти Xircom CreditCard Netwave Adapters и операционни системи Microsoft Windows 95 или Microsoft Windows NT, могат да работят като равнопоставена мрежа без свързващи кабели. Но ако разполагате с изградена мрежа под Windows NT Server, можете да присъедините към нея горепосочената безжична мрежа, като добавите Netwave Access Point (точка на достъп) към един от компютрите на мрежата под Windows NT Server.

Предаване тип point-to-point (точка-до-точка)

Този метод за предаване на данни не се вписва напълно в настоящата дефиницията на компютърните мрежи. Тук се използва технологията point-to-point за предаване на данни от един компютър до друг, което се различава от комуникацията, извършвана между няколко компютъра и периферни устройства. При point-to-point технологията са необходими допълнителни компоненти, например трансивъри, които могат да се поставят на самостоятелни компютри или на компютри, които вече са в мрежа, за да се образува безжична мрежа за трансфер на данни.

Технологията point-to-point осигурява безжичен сериен трансфер на данни,

който:

Използва point-to-point радиовръзка за бърз и безпогрешен трансфер на данни.

Прониква през стени, тавани и подове.

Поддържа скорости от 1.2 до 38.4 Kbps на разстояния до 60 метра (200 фута) на закрито, или до една трета от милята при пряка видимост.

Тези системи извършват трансфер на данни между компютри, както и между компютри и други устройства, като принтери или четци на бар-кодове.

Разширени локални мрежи

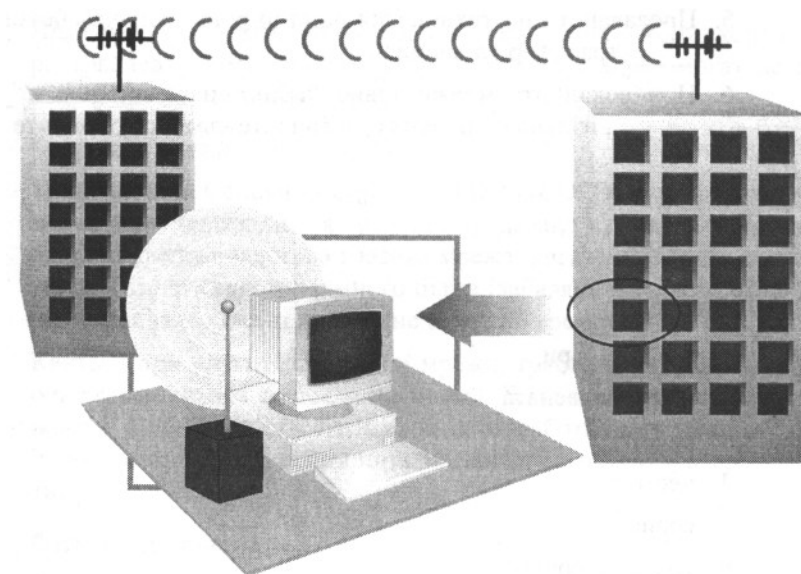
При разширената локална мрежа се използват други по вид безжични компоненти, изпълняващи същите функции, като техните аналози в кабелните мрежи. Например безжичните LAN мостове могат да свързват мрежи на разстояния до три мили.

Многоточкова безжична връзка

Един компонент, наречен безжичен мост, предоставя лесен начин на реализиране на връзка между две сгради, без да се използва кабел. Както обикновеният мост осигурява път за хората между два бряга, така и безжичният мост осигурява път за данните между две сгради. AIRLAN/ Bridge Plus например използва радиотехнология с разпределен спектър за изграждане на безжичен гръбнак (wireless backbone) за свързване на мрежи, намиращи се на разстояния

извън пределите на съответната LAN. В зависимост от условията, това разстояние може да е до три мили.

Цената на такава връзка може и да е приемлива, защото се елиминират разходите за наети телефонни линии.



Безжичен мост, свързващ две LAN

Безжичен мост с голям обхват

Ако безжичният мост не осигурява връзка на достатъчно голямо разстояние, може да се замени с безжичен мост с голям обхват (long-range wireless bridge). Той също използва радиотехнологията с разпределен спектър, осигурявайки мостова връзка за Ethernet и Token Ring мрежи на разстояния до 25 мили.

Както и при обикновените безжични мостове, високата цената на мостовете с голям обхват може да е оправдана, защото се премахва необходимостта от T1 линия или микровълнови връзки. Линията T1 е стандартна цифрова линия и

осигурява скорости на предаване от 1.544 Mbps. Тя може да пренася както глас, така и данни, (б.ред. В Европа стандартната цифрова линия е E1 - 2048Mbps).

Мрежи с мобилни компютри

Безжичните мобилни мрежи използват телефонни линии и обществени телефонни услуги за получаване и изпращане на сигнали с помощта на:

Пакетни радио комуникации (packet-radio communication)

Клетъчни мрежи (cellular networks)

Сателитни станции (satellite stations)

Потребителите, които често пътуват, могат да използват тази технология с помощта на портативни компютри или PDA (Personal Digital Assistants - персонални цифрови помощници), за да обменят e-mail съобщения, файлове или друга информация.

Тази форма на комуникация е доста удобна, но е бавна. Скоростите на предаване варират между 8 Kbps и 19.2 Kbps. Те дори са още по-бавни, когато е включена корекция на грешките.

Работата с мобилни компютри включва безжични адаптери и клетъчна телефонна технология за свързване на портативните компютри с кабелните мрежи. Портативните компютри комуникират с околните им радио-кули с помощта на малки антени. Сателитите в близка орбита хващат слабите сигнали от мобилните мрежови устройства.

Пакетни радиокомуникации

При тази система предаваните сигнали се разделят на пакети, подобни на стандартните мрежови пакети. Тези пакети съдържат следното:

Адресът на източника

Адресът на местоназначението

Информация за корекция на грешките

Пакетите се предават до сателити в около земна орбита, които ги разпространяват. Само устройствата с коректния адрес могат да получат излъчените от сателита пакети.

Клетъчни мрежи

Технологията Cellular Digital Packet Data (CDPD) е същата, като тази за клетъчните телефони. Тя предлага предаване на компютърни данни по съществуваща аналогова гласова мрежа, когато гласовата система не е заета. Тази технология е много бърза (забавянето е части от секундата) и е доста надеждна за предаване в реално време.

Както и при другите безжични мрежи, трябва по някакъв начин да се осъществи връзка с кабелната мрежа. Една компания от Онтарио, Канада - Nortel out of Mississauga - разработва устройството Ethernet interface unit (EIU), с помощта на което се реализира връзка от този тип.

Сателитни станции

Добър вариант за осъществяване на връзка между сгради, намиращи се на близки разстояния, са микровълновите системи. В момента микровълновата технология е най-широко разпространеният метод за предаване на дълги разстояния в САЩ. Той е чудесен за комуникация между две точки с пряка видимост, като:

Сателит със земята

Между две сгради

През големи, равни пространства, като водни басейни или пустини.

Микровълновата система се състои от:

Два радио трансивъра - един за генериране (предавател) и един за получаване (приемник) на излъчването.

Две насочени една към друга антени, които реализират комуникацията. Често тези антени се поставят на високи места, като кули, за да се разшири покриваната област и да се предотврати възможността нещо да застане на пътя на сигналите и да ги блокира.

Сложни конектори

Простите устройства за свързване на мрежата просто съединяват кабелите; сложните вършат много повече неща. Например те могат да усилят сигнала,

преди да го предадат нататък, и дори да го конвертират от един тип преносна среда за друг.

Конвертори на преносната среда

Повторители

Активни/интелигентни хъбове

Конвертори на преносната среда



Конверторите на преносната среда се наричат също адаптери за преносна среда (media adapters) или транслатори на преносна среда (media translators). Те се използват, за да конвертират един сегментен тип в друг; например те могат да конвертират 10Base2 в 10BaseT, 100BaseT Ethernet в оптично влакно или Token Ring в оптично влакно.

Повторители

Повторителят свързва два мрежови сегмента или служи за наставяне на кабел. Само че за разлика от цилиндричния конектор, повторителят не прехвърля просто сигнала от единия кабел към другия - той го регенерира. Поради тази причина, ако сигналът е отслабнал поради ефекта на затихването, той се усилюва, а ефективната дистанция на кабела се увеличава.



Повторителите не филтрират преминаващите през тях данни. Те регенерират всички сигнали, включително бродкастните съобщения, шума и смущенията, предавайки ги нататък. На снимката е показан повторител за коаксиален кабел.

Концентратори (Активни и интелигентни hub-ове)

Hub, или както е прието в България, концентратор, представлява от себе си многопортов (от 4 до 16 и повече) повторител (repeater) на мрежа с автоматична сегментация, предназначен най-вече за свързване на отделни работни места, оборудвани с мрежови карти, в една мрежа, като отделните работни места могат

да работят под управлението на различни операционни системи и да бъдат от различен тип (работещи на различна скорост, например). Всички портове на концентратора по правило имат един и същ приоритет, така че при получаването на сигнал на единия от портовете концентратора го препредава към всички свои активни портове.



При положение, че логиката на концентратора открие някаква неизправност във някой от подвключените към портовете мрежови сегменти, концентраторът автоматично се изключва, като след като при някой от следващите цикли установи, че повредата е отстранена, отново започва да функционира нормално.

Концентраторите са автономни устройства, които могат да бъдат свързвани едно с друго с цел увеличаване на физическия брой подвключени устройства и разширяване топологията на една (хетерогенна) мрежа. Hub-овете отговарят на стандарта IEEE 802.3, работейки в съответствие с ниво 1 (физическо) на модела OSI (Open System Interconnect), което ще рече че те не се влияят от типа на протоколите от по-високо ниво. Процесът, при който концентраторът изключва някой от портовете при откриване на неизправност се нарича сегментация.

Мрежите, в които се използват най-често концентратори, са на базата на

кабели с усукана двойка (UTP) - 10Base-T или 100Base-TX/T4. Има концентратори за мрежи 10Base-2 с коаксиален кабел и 10Base-F с оптичен кабел, както и други. Десет-мегабитовите хъбове често имат портове с конектор RJ-45, така и за коаксиален кабел (BNC) или AUI, което позволява сегментите с коаксиален или оптичен кабел да се използват като главна магистрала (Backbone) между концентраторите.

Основната (и съществена) разлика между концентраторите (Hub) и значително по-разпространените напоследък комутатори (Switch) е в това, че концентраторите нямат възможност да буферизират пропусканите през тях пакети с данни, а комутаторите - могат. Това на практика довежда до по-високи скорости на обмен на данни в мрежи, изградени с комутатори, отколкото с концентратори.

"Неумението" на концентратора да буферизира пакетите води и до невъзможността му да синхронизира работещи на различни скорости портове, макар че не е изключено да има разработени чипове, които да се справят успешно с този проблем. Липсата на синхронизация по скорост довежда до там, че ако към концентратора има комутирани работни станции, работещи при скорост 10 и 100 мегабита/секунда, всички портове на концентратора ще работят на 10 MBit.

Активните хъбове се наричат също многопортови повторители (multiport repeaters), защото разполагат с множество портове (подобно на пасивните хъбове) и регенерират сигнала, идващ от даден порт, преди да го предадат по друг порт (подобно на повторител). Активните хъбове изискват електрическо захранване.

Интелигентният хъб е специален тип активен хъб. Той не само регенерира сигнала, но също така разполага с процесор, позволявайки ви да извършвате диагностика и да разберете дали има проблем с даден порт. Хъбовете работят във физическия слой на референтния OSI модел.

Мостове

Един традиционен мост (наричан също прост прозрачен мост) свързва два мрежови сегмента и извършва филтриране на трафика, като се базира на MAC (media access control) адресите в пакетите. Когато се използва правилно, това ви позволява да намалите претоварването.

Един добър пример за използване на мост (bridge) е безжичният Ethernet мост, който превръща сигналите от жично Ethernet устройство за нуждите на безжични компютърни мрежи. Bridge-ът и USB адаптерите понякога са наричани wireless media adapters. Те позволяват на устройства за Wi-Fi да използват Ethernet или USB физически устройства.

За разлика от повторителите, някои мостове могат да свързват мрежови сегменти, използвайки различни методи за достъп до преносната среда, стига да използват един и същ мрежов протокол (например TCP/IP). Те се наричат транслационни мостове (translation bridges) или капсулиращи мостове (encapsulation bridges).

В една мрежа може да има повече от един мост. Това осигурява отказоустойчивост, но е свързано с риск да се получи междумостово зацикляне (bridging loop), което възниква при наличие на няколко различни пътя между две точки.

В последно време мостовите се използват все по рядко като вместо това се използват комутатори (switches).

Маршрутизатори (routers)

Маршрутизаторите свързват отделни мрежи една с друга. Това може да се случи в една локална мрежа (в който случай отделните мрежи се наричат подмрежи) или между независими една от друга мрежи, както е например при глобалния Интернет.



Подобно на моста, маршрутизаторът филтрира трафик. За разлика от моста обаче, маршрутизаторът прави това, използвайки логически мрежови адреси (IP или IPX адреси) вместо физическите хардуерни адреси. Маршрутизаторите са по-интелигентни от мостовете; те вземат сложни решения, избирайки най-добрия маршрут до дадена дестинация измежду множество възможни пътища.

ЗАБЕЛЕЖКА: Специализираните маршрутизиращи устройства всъщност са компютри със специално предназначение; те съдържат микропроцесори и изпълняват своя собствена операционна система. PC-тата също могат да бъдат конфигурирани да действат като маршрутизатори, ако операционната система поддържа IP или IPX препращане.

Маршрутизаторите поддържат маршрутни таблици, съдържащи мрежовите адреси на други маршрутизатори. Един маршрутизатор трябва да притежава поне два мрежови интерфейса, защото той служи като шлюз (gateway) между мрежи.

Адресът на интерфейса на маршрутизатора, който обслужва конкретна подмрежа, се нарича подразбиращ се шлюз (default gateway) за тази подмрежа.

Маршрутизаторите могат да се използват за свързване на множество мрежи в една по-голяма, както и да разделят една голяма мрежа на няколко по-малки.

Когато в дадена мрежа съществуват множество пътища, мостът избира един от тях и винаги използва него, за да достигне до специфична дестинация. Маршрутизаторите взимат под внимание всички налични пътища за всеки изпратен пакет и взимат решение за всеки отделен пакет. По този начин, ако даден маршрут е много натоварен в дадено време, маршрутизаторът избира друг по-ефективен маршрут.

Комутатори (switches)

Основната функционалност на един суич (комутатор) е измамно проста: да избере път, по който да изпрати данните до тяхното местоназначение.

Комутаторите позволяват всяка една работна станция да предава данните през комуникационната среда без да се конкурира с другите. Основната разлика между концентратора (hub) и комутатора (switch) идва от възможността на последния да буферира пакетите с данни.

Ethernet суичовете се превръщат в популярно решение за свързване, при това поради добра причина. Те увеличават производителността (скоростта) и са сравнително евтини.

Суичовете използват една от двете схеми за комутиране:

Комутация без буфериране на пакетите (cut-through switching) - Суичът започва да препредава пакета до неговото местоназначение, преди пакетът да е пристигнал изцяло. Този метод е по-бърз, но може да доведе до преминаването на лоши пакети.

Комутация с промeждутъчно съхранение (store-and-forward switching) - Суичът не изпраща пакета, докато не го получи напълно и не провери неговия интегритет. Това е по-бавно, но по-надеждно.

Почти всички комутатори, за разлика от концентраторите, имат изведена върху горния капак или лицевата страна на кутията светодиодни индикации за режима на работата на портовете.

Мрежови интерфейсни карти

Най-основният хардуер, необходим за свързване на един компютър в мрежа, е мрежовата интерфейсна карта, наричана също мрежов адаптер или просто мрежова карта. Мрежовите карти съществуват под няколко форми, които са дискутирани в секцията избиране на мрежова карта.

Мрежовата карта обикновено е устройство от физическия слой, а драйверите за нея (софтуерът, осъществяващ връзката между картата и операционната система на компютъра) работят в каналния слой на OSI модела.

Ролята на мрежовите карти в мрежовите комуникации

За комуникиране по мрежа винаги се изисква някакъв вид мрежов интерфейс. Мрежовата интерфейсна карта е основният хардуерен компонент в

мрежовите комуникации. Тя преобразува паралелния сигнал, произведен от компютъра, в серийна (последователна) форма, която се изпраща по мрежовия кабел. Единиците и нулите на двоичната комуникация се преобразуват в електрически импулси, светлинни импулси, радиовълни или каквато и да е друга схема за предаване на сигнали, използвана от преносната среда.

Важна част от мрежовия интерфейс е така нареченият трансивър (или приемопредавател). При някои мрежови карти, като например тези за 10Base2 и 10BaseT мрежи, трансивърът е вграден в самите тях. Други, например предназначени за 10Base5 мрежи, са снабдени с интерфейс за свързване на (мрежови) устройства (attachment unit interface - AUI), представляващ конектор, към който кабелът се свързва към външен трансивър. Трансивърът (приемопредавателят) служи именно за приемане и предаване на сигнали.

Освен че подготвя данните за изпращане към преносната среда, мрежовата карта отговаря и за управлението на потока от данни между компютрите и преносната среда, както и за приемане на входящите данни. На снимката е показана една типична PCI мрежова карта, предназначена за 100BaseT мрежа.

Избиране на мрежова карта

Когато избирате мрежова карта за даден компютър, трябва да вземете предвид следните неща:

Мрежова архитектура

Мрежовата карта трябва да може да работи със съществуващата технология за предаване. Въпреки това е възможно да се използва филтър на преносната среда

{media filter}), който ви позволява например да използвате Token Ring карта в Ethernet мрежа.

Тип на преносната среда

Ethernet мрежите могат да използват дебел коаксиален кабел (10Base5), тънък коаксиален кабел (10Base2) или кабел с усукана двойка (10BaseT). Конекторът на картата трябва да съвпада с буксата на кабела. Съществуват и мрежови карти за безжични или оптични мрежи.

Скорост на предаване на данните

Ако имате 100Mbps хъбове, една 10Mbps мрежова карта няма да работи с тях. Можете обаче да поставите двускоростни компоненти (било то мрежови карти или хъбове), които работят със скорост или 10Mbps или 100Mbps.

Тип на свободен разширителен слот

Имате ли свободен ISA или PCI слот? Дали компютърът е лаптоп и трябва да използва PCMCIA (т.е. PC Card) интерфейс? Нуждаете ли се от специална карта, която се свързва към сериен или SCSI порт? .

Типове разширителни шини

Шината за данни представлява канал за предаване, разположен на дънната платка на компютъра. Сигналите се приемат от или предават към всяко устройство, свързано към този канал. Съществуват няколко шинни архитектури, за които се произвеждат мрежови карти:

ISA (Industry Standard Architecture - стандартна за индустрията архитектура)

EISA(Extended ISA - разширена ISA)

PCI (Peripheral Component Interconnect - свързване на периферни компоненти)

MCA (Micro Channel Architecture)

PCMCIA (Personal Computer Memory Card International Association; нарича се още PC Card)

Съществуват и мрежови карти, които се свързват към SCSI шина. Има също USB (universal serial bus - универсална серийна шина) модели.

Също така трябва да отбележим, че дънните платки на някои компютри притежават вградени мрежови адаптери, т.е. компонентите на мрежовата карта се намират на самата дънна платка

Операционната система

Трябва да се уверите, че производителят на мрежовата карта осигурява драйвери за използваната от вас операционна система. Ако използвате някоя от операционните системи Windows, погледнете списъка Microsoft Hardware Compatibility List (HCL) на адрес www.microsoft.com, където са изброени тестваните с операционната система мрежови карти.

Мрежова архитектура

Проектиране на разположението на мрежата

Терминът топология, и по-специално мрежова топология, се отнася до физическото разположение на компютрите, кабелите и другите компоненти на мрежата. Топология е стандартният термин, използван от повечето мрежови специалисти, когато става въпрос за основния проект на мрежата. Освен топология (topology), подредбата на мрежата може да се нарича още:

Физическо разположение (Physical layout)

Дизайн (Design)

Диаграма (Diagram)

Карта (Map)

Топологията на мрежата влияе върху нейните възможности. Изборът на една топология пред друга може да повлияе върху:

Вида на оборудването

Възможностите на оборудването

Разрастването на мрежата

Управлението на мрежата

Осмислянето на различията в начините на използване на отделните топологии е един от ключовете към осъзнаването на възможностите, предлагани от различните видове мрежи.

Компютрите трябва да бъдат свързани помежду си, за да поделят своите ресурси или да изпълняват други комуникационни задачи. В повечето мрежи за свързване на компютрите се използват кабели.

Свързването на компютрите не е толкова лесна задача, колкото изглежда. Не е достатъчно двата края на един кабел да се пъкнат в два компютъра. Различните типове кабели, в комбинация с разнообразните мрежови карти, мрежови операционни системи и други компоненти, изискват различни видове мрежови настройки.

От вида на мрежовата топология зависят доста неща. Например изборът на дадена топология може да определи не само вида на кабелите, но и начините за тяхното прокарване през пода, тавана или стените на сградата.

Топологията определя и начина, по който компютрите комуникират помежду си. Различните топологии изискват различни комуникационни методи, които от своя страна имат голямо влияние върху мрежата.

Стандартни топологии

Всички мрежови конфигурации произлизат от трите основни топологии:

Шинна (bus)

Тип звезда (star)

Кръгова (ring)

Ако компютрите са свързани помежду си с един общ кабел (сегмент), топологията се нарича шинна (или просто топология "шина"). Ако компютрите са свързани към кабелни сегменти, които се разклоняват от обща точка, наречена хъб (hub), топологията е известна като звезда. А ако компютрите са свързани с кабел, оформящ кръг, топологията се нарича кръгова (или "кръг").

Макар тези три основни топологии да изглеждат сами по себе си прости, техните варианти в реалния свят на компютрите често обединяват възможностите на повече от една топология и могат да бъдат доста сложни.

Шинна топология

Шинната топология (bus) е известна още като линейна шина. Това е най-простият и най-често срещан метод на свързване на компютрите в мрежа. Състои се от единичен кабел, който се нарича магистрала (или още гръбнак или сегмент) и свързва всички компютри от мрежата в една единична линия.



Мрежа с шинна топология

Комуникацията по шината

При мрежа с шинна топология компютрите комуникират, като адресират данни до определен компютър и ги изпращат по кабела във вид на електронни сигнали. За да разберете как компютрите комуникират по шината, трябва да сте запознати със следните три концепции:

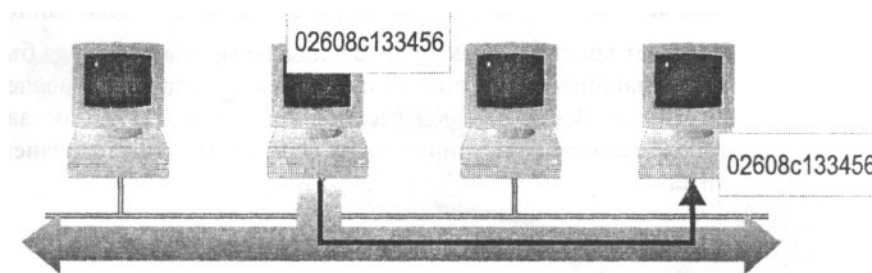
Изпращане (sending) на сигнала

Отскачане (bounce) на сигнала

Терминатор (terminator)

Изпращане на сигнала

Мрежовите данни се изпращат във вид на електронни сигнали до всички компютри в мрежата. Но информацията се приема само от този компютър, чиито адрес съвпада с адреса, кодиран в сигнала. В даден момент само един компютър може да изпраща съобщения.



Данните се изпращат до всички компютри, но само получаващият компютър ги приема

Тъй като при мрежа с шинна топология само един компютър може да изпраща данни в даден момент, производителността на мрежата се влияе от броя на свързаните към шината компютри. Колкото повече сате, толкова по-дълго ще чакат ред за изпращане на данни по шината и толкова по-бавна ще е мрежата.

Няма конкретни средства за измерване влиянието на броя на компютрите върху дадена мрежа. Падането на скоростта на мрежата не е непременно свързано само с броя на нейните компютри. Върху това влияят и други фактори, като:

Хардуерните възможности на компютрите в мрежата.

Броя на осъществяваните трансфери на данни.

Вида на приложенията, работещи в мрежата.

Вида на използвания кабел.

Разстоянията между компютрите.

Шинната топология е пасивна. Компютрите на шината могат само да прослушват за данни, изпратени по мрежата. Те не се грижат за пренасянето на тези данни. Повредата на даден компютър не пречи на останалата част от мрежата. При активна топология, компютрите регенерират сигналите и придвижват данните по мрежата.

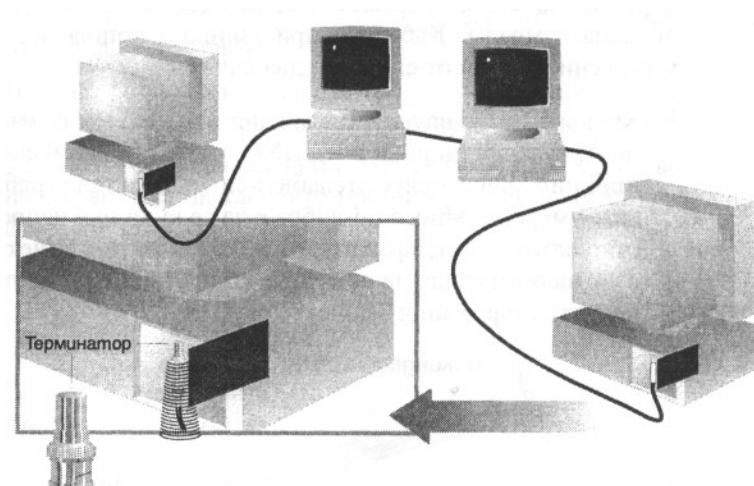
Отскачане на сигнала

Тъй като данните, или по-точно електронните сигнали, се изпращат по цялата мрежа, те пътуват от началото до края на кабела. Ако им се позволи да продължат своя път, сигналите ще започнат да отскачат (bounce) от края на кабела и да се връщат обратно, пречейки на компютрите да изпращат други сигнали. Затова сигналите трябва да бъдат спрени, след като са получили възможност да достигнат местоназначението си.

Терминатор

За да се предотврати отскачането на сигнала, той трябва да бъде спрян. За тази цел, на всеки край от кабела се поставя компонент, наречен терминатор (terminator). Той поглъща свободните сигнали и освобождава кабела, за да могат компютрите да изпращат още данни.

Всеки от краищата на кабелите в дадена мрежа трябва да бъде пъхнат в нещо, например в компютър или в конектор за увеличаване дължината на кабела. Всеки отворен кабелен край (който не е поставен в нищо) трябва да бъде терминиран, за да се предотврати отскачането на сигналите.

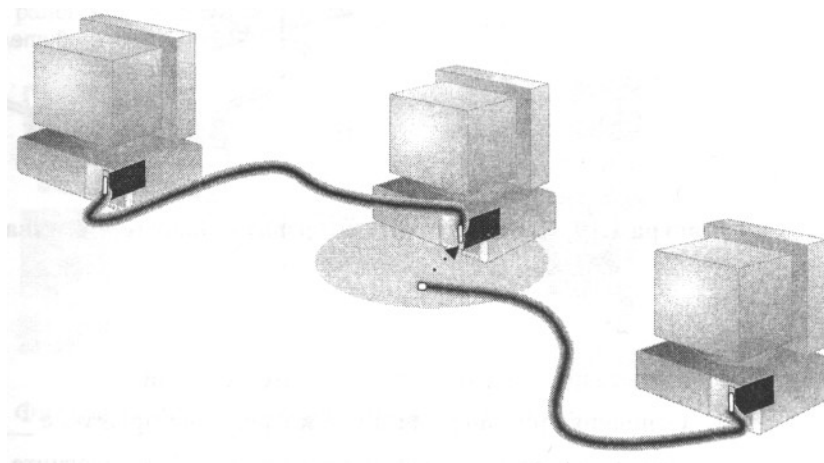


Терминаторите поглъщат (абсорбират) свободните сигнали

Разпадане на мрежовата комуникация

Прекъсване на кабел се получава, когато той бъде физически разрязан на две или когато единият му край се откачи. И в двата случая един или повече краища на кабела нямат терминатор, сигналът отскача и дейността на мрежата спира. В такъв случай се казва, че мрежата се е "разпаднала".

Компютрите в мрежата все още ще могат да функционират като самостоятелни единици, но докато сегментът е повреден, те няма да могат да комуникират помежду си.

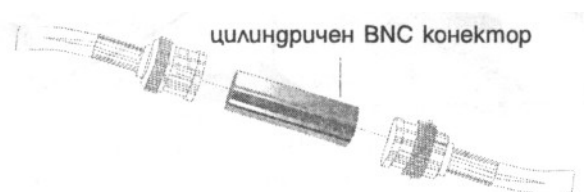


Ако прекъснатият кабел не се терминира, следва разпадане на мрежата

Разширение на LAN

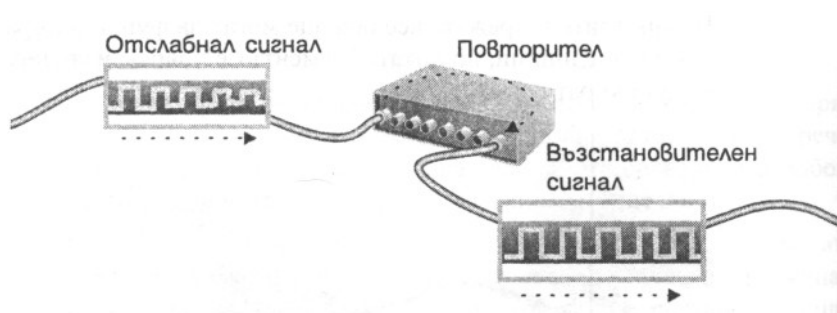
С разрастването на фирмата възниква необходимост от разширяване на локалната мрежа. Кабелите при шинната топология могат да бъдат удължени по един от следните два начина:

- За свързването на два кабела с цел удължаване се използва компонент, наречен цилиндричен BNC конектор (barrel connector). По принцип конекторите отслабват сигнала, затова трябва да се използват умерено. Много по-добре е да се купи цял непрекъснат кабел, отколкото да се свързват две по-малки части с конектор. Възможно е сигналът изобщо да не стигне до местоназначението си, ако се използват твърде много конектори.



Конекторите се използват за свързване на отделни сегменти

- Устройство, наречено повторител (repeater), също може да се използва за свързване на два кабела. Повторителят всъщност усилва сигналите, преди да ги изпрати нататък. Това е по-добър вариант от конектора, особено при дълги кабелни сегменти, защото повторителят позволява сигналът да се изпраща на по-голямо разстояние и все пак да бъде правилно приет.



Повторителите свързват кабелите и усилват сигнала

Топология тип звезда

При топологията тип звезда (star) компютрите се свързват чрез кабелни сегменти към централен компонент, наречен хъб (hub). Сигналите се предават от изпращащия компютър през хъба до всички останали компютри в мрежата. Тази топология води началото си от ранните дни на компютъризацията, когато компютрите се свързваха към голям централен компютър. Мрежата от тип звезда предлага централизирани ресурси и управление. Но тъй като всеки компютър е свързан към централна точка, тази топология изисква много кабели, когато се изгражда голяма мрежа. Друг недостатък е, че ако се повреди централната точка, цялата мрежа се разпада.

Ако даден компютър, или кабелът, който го свързва с хъба, се повредят, само този компютър няма да може да изпраща или получава данни. Останалата част от мрежата продължава да работи нормално.



Елементарна мрежа тип звезда

Кръгова топология

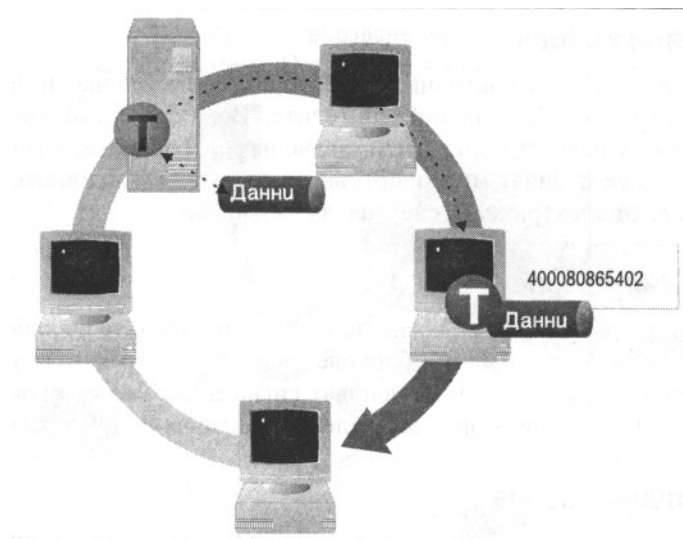
Кръговата топология (ring) свързва компютрите с един кабел, оформящ кръг - няма терминирани краища. Сигналят пътува по кръга в едната посока и преминава през всеки компютър. За разлика от пасивната шинна топология, тук всеки компютър работи като повторител, като усилва сигнала и го препраща към следващия компютър. Тъй като сигналят минава през всички компютри, повредата на един от тях може да повлияе върху цялата мрежа.



Елементарна кръгова мрежа, на която се вижда логическият кръг

Управляващ маркер

Един от методите за предаване на данни по кръга се нарича управляващ маркер (token passing⁴). Маркерът обхожда компютрите, докато стигне до този, който трябва да изпраща данни. Изпращащият компютър модифицира маркера, поставя електронен адрес на данните и ги изпраща нататък по кръга.



Компютърът прихваща управляващия маркер и го препраща по кръга

Данните преминават през всеки компютър, докато стигнат до този, чийто адрес съвпада с техния. Получаващият компютър връща съобщение към изпращащия, с което указва, че е получил данните. След потвърждението изпращащият компютър създава нов маркер и го предава по мрежата.

Създава се впечатление, че методът с управляващ маркер отнема много време, но всъщност маркерът пътува почти със скоростта на светлината и може да обиколи кръг с диаметър 200 метра около 10 000 пъти за една секунда.

Вариации на основните топологии

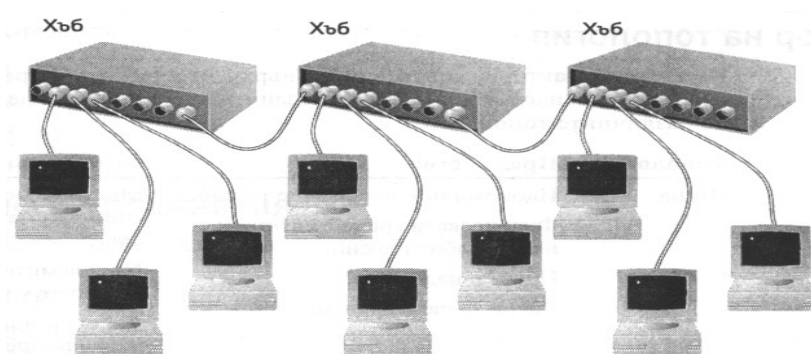
В днешно време много от действащите топологии са комбинации от трите основни: шината, звездата и кръгът.

Звезда/шина

Звезда/шина (star bus) е комбинация от топологиите звезда и шина. При нея

няколко мрежи с топология тип звезда се свързват помежду си с линейна шина, наричана магистрала (trunk).

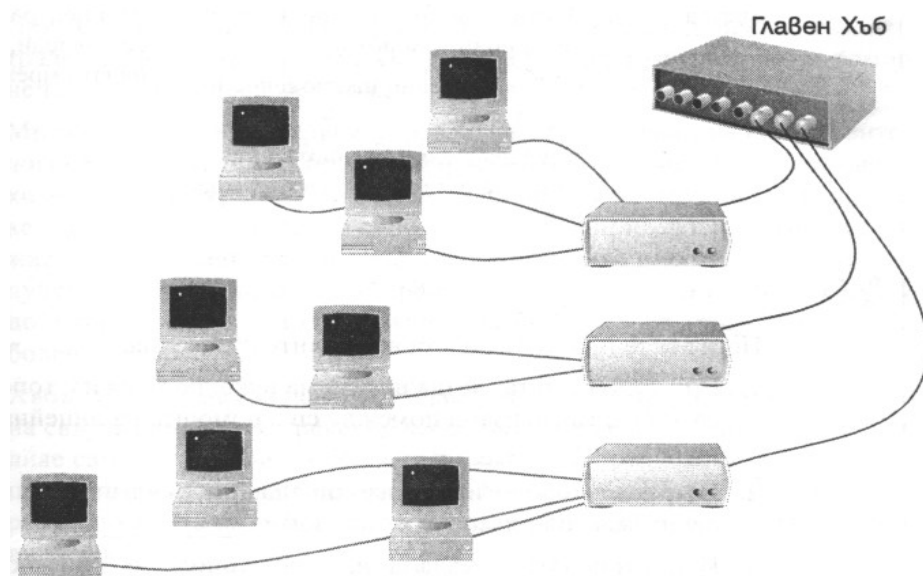
Повредата на един компютър не влияе на останалата част от мрежата, като другите компютри продължават да комуникират помежду си. При повреда на някой от хъбовете, всички компютри, свързани към него, загубват възможност за комуникиране. Ако въпросният хъб е свързан с други хъбове, тези връзки също ще бъдат разрушени.



Мрежа с комбинация от топологиите звезда и шина

Звезда/кръг

Звезда/кръг (star ring) е комбинацията от топологиите звезда и кръг и наподобява комбинацията звезда/шина. И двете смесени топологии имат за централна точка хъб, към който е свързана мрежа или с кръгова, или с шинна топология. Хъбовете при звезда/шина са свързани помежду си с линейна шина, докато хъбовете при звезда/кръг са свързани като звезда към един главен хъб.



Мрежа с комбинация от топологии звезда и кръг

Избор на топология

Има много фактори, които влияят върху избора на конкретна топология. В следващата таблица са показани предимствата и недостатъците на различните топологии.

Топология	Предимства	Недостатъци
Шина	<p>Икономично използване на кабел.</p> <p>Физическата среда е евтина и с нея се работи лесно.</p> <p>Проста, надеждна. Лесна за разширяване.</p>	<p>Мрежата може да се забави при натоварен трафик.</p> <p>Проблемите трудно се откриват.</p> <p>Кабелната повреда може да попречи на много потребители.</p>
Кръг	<p>Еднакъв достъп до мрежата за всички компютри.</p> <p>Еднаква производителност, независимо от броя на потребителите.</p>	<p>Повредата в един компютър може да повлияе на останалата част от мрежата.</p> <p>Проблемите трудно се откриват.</p> <p>Преконфигурирането на мрежата прекъсва нейната работа.</p>
Звезда	<p>Лесна за модифициране и добавяне на нови компютри.</p> <p>Централизирано наблюдение и управление.</p> <p>Повреда в един компютър не влияе на останалата част от мрежата.</p>	<p>Ако централната точка се повреди, разпада се цялата мрежа.</p>

Мрежови модели

Повечето хора зависят от визуалното стимулиране. Разбираме нещо по-добре, когато можем да го видим с очите си. Но абстрактните концепции, които нямат конкретна форма, могат да бъдат представени в модел, който да ни създаде визуална представа за дадена структура, процес или релационна връзка.

Моделите са навсякъде около нас. Генетиците използват двойна спирала за представяне на структурата на молекулата на ДНК. Физиците представят релационните връзки на протони и електрони на ниво атом. Атомите са много малки, за да могат да бъдат видени, но учените използват модели за подпомагане на изучаването на явления, които не могат да бъдат наблюдавани директно.

Целта на моделите

Ако потърсим думата модел в речника, ще открием много нейни значения, например „схематично описание на система, теория или явление, което представя нейни познати или предполагаеми свойства и може да бъде използвано за допълнително изучаване на нейните характеристики". Тази дефиниция обхваща една от целите на мрежовите модели: да ни помогнат да опишем, разберем и изучим процеса на мрежова комуникация.

Моделът също „служи като пример, който може да бъде следван или сравняван". Мрежовите модели са основата на стандартизацията; ако един и същ модел се използва от производителите на мрежови продукти, тези продукти могат да бъдат сравнени с едни с други. Моделите описват начина, по който се извършват комуникациите на данни. Ако даден производител, произвеждащ

продукти за изграждане на мрежи, съблюдава стандартите на всеки слой, мрежовите компоненти трябва да работят с тези, произведени от други производители

Моделът DoD

Макар че OSI моделът е най-популярен, той не е единственият, нито първият модел за изграждане на мрежи. Факт е, че моделът на Министерството на отбраната на САЩ (Department of Defense - DoD) - понякога означаван като TCP/IP модел - беше разработен около десет години по-рано от OSI модела, през 70-те години на миналия век.

Моделът на DoD беше разработен в сътрудничество със самия TCP/IP - част от проекта ARPAnet. Той е по-прост модел, състоящ се само от четири слоя, които могат да бъдат приблизително асоциирани със седемте слоя на OSI модела.

Функцията на всеки слой е следната:

- Слой приложение/процес (application/process layer) - Най-горният слой на модела DoD, който обхваща функциите на трите най-горни слоя на OSI модела: приложен, представителен и сесиен. В текстовете, отнасящи се за TCP/IP, може да прочетете, че криптирането на данните и контролът на диалога се осъществяват в приложния слой. Ако запомните, че това не означава приложния слой на OSI модела, ще избегнете объркването.

- Слой хост до хост (транспортен слой) (host to host (transport) layer) -

В някои източници слой хост до хост се означава като транспортен слой,

дори в четиристойни диаграми на DoD, и съответства на транспортния слой от OSI модела. Тук функционират TCP, UDP и DNS.

- Слой интермрежа (internetworking layer) - Този слой съответства много близко на мрежовия слой на OSI Той се занимава с маршрутизация, базирана на логически адреси. Протоколът Address Resolution Protocol (ARP) транслира логическите адреси в MAC адреси. Тази транслация е необходима, защото по-долните слоеве могат да обработват само MAC адресите.

- Слой мрежов интерфейс (network interface layer) - Слой мрежов интерфейс съответства на двата слоя - канален и физически - от референт-ния модел OSI В този слой работят стандартните Ethernet и Token Ring протоколи от каналния слой и физическия слой.

Една от целите на ISO при разработката на OSI модела беше по-конкретно да дефинира мрежовите функции, определени от DoD модела при създаване на TCP/IP. Но TCP/IP протоколите бяха проектирани по DoD модела, а не по OSI модела.

Моделът OSI

Най-ефикасният начин да се реализира мрежова комуникация е под формата на многослоен процес - процес разделен на отделни стъпки.

Всеки слой (т.е. мрежови компонент отговаря за конкретна задача)

С оглед да се осигури определено единство между производителите на мрежи Международната организация по стандартизация ISO (Open System

Interconnection) разработи Стандарти за взаимната връзка между отворени системи (OSI). Основната идея е че, комуникационните системи трябва да се проектират като съвкупност от модули така, че един модул да осигурява определени функции и да поддържа връзка с съседните модули. Всеки модул представлява слой (layer) в комуникационния модел, изграден върху предишните слоеве.

Различните компютри, свързани в мрежа, трябва да "познават" формата на информацията, която ще приемат - кога една дума ще започне, кога тя ще завърши и кога ще започне следващата дума. Може ли станцията да провери дали съобщението и е претърпяло известна деформация по време на предаването? Моделът OSI отговаря на тези и на много други въпроси със серия от стандарти, които ще позволят на потребителите да купуват в бъдеще мрежови продукти от различни производители с известна увереност, че те ще бъдат съвместими.

Application	Приложен
Presentation	Представителен
Session	Сесиен
Transport	Транспортен
Network	Мрежов
Data link	Канален
Physical	физически

Предназначение на нивата в OSI

1. Физическо ниво. Отговаря за приемането и предаването на бинарните данни. Това ниво определя електрическите, механическите и процедурните

характеристики на канала между крайните системи. Точно спецификациите на физическото ниво определят нивата на напреженията, скоростта на предаване на физическата информация, фиксира изискванията за средата за предаване на информация и т.н. В стандартите за физическия слой са включени също предписания за куплунгите и за интерфейсите със съобщителната среда на мрежата. В този слой моделът OSI е свързан с електрически характеристики и битове (единици и нули). В действителност на това ниво битовете нямат определено значение; логически смисъл им се влага в следващия слой на модела. В този слой се описват и кабелни спецификации, най популярните са

IEEE 802.3 – Ethernet, напр. 10BASE-2 и 10BASE-T

IEEE 802.5 – Token Ring 10BASE-2 и 10BASE-T

2. Канално ниво. Осигурява транспортирането на данните под физическото ниво, подсигурявайки физическата адресация, мрежовата топология, информирание за неизправности, администрирането на информационният поток. На каналното ниво необработените до тук битове, а с кадри от данни - пакети, които съдържат, както данни, така и управляваща информация.

В каналния слой към данните се добавят флагове, които показват началото и края на съобщенията. Стандартите за този слой осигуряват две важни проверки: дали данните са с верни флагове и дали има грешки в кадрите. Проверката за грешки може да се извършва чрез изпращане на допълнителна информация за кадъра с данни към приемната страна и чрез получаване на потвърждение в случай, че всичко е прието правилно. Каналният слой определя също механизмите за достъп до кабела и предаване на управляващ маркер.

В този слой са определени и спецификациите и мрежовите стандарти

(например LM IEEE 802.2 и IEEE 802.5, HDLC за последователни съединения, FDDI, X.25, Frame Relay).

3. Мрежово ниво. Отговаря за избор на маршрута между двете крайни устройства, дори те да се намират в различни географски райони, за разлика от физическото ниво, което следи само близко стоящите мрежови връзки. Третият слой от модела OSI специфицира механизъм за превключване на пакетите. В него е описано как се изграждат виртуални канали за обмен на данни (съобщителни линии между два компютър или терминала). В мрежовия слой на предавателната страна съобщенията, осигурени от транспортния слой, се разделят на пакети с данни с оглед двата най-нисши слоя да могат да ги предадат. В приемния край на линията мрежовият слой възстановява съобщението. За да се разберат операциите с пакетите с данни, необходимо е да се разгледа промишления стандарт X.25, който е обект на трите нисши слоя на модела OSI. Този слой най-общо организира маршрутизирането от един възел до друг. Той може да скрива долните слоеве от горните, като позволява използването на различен мрежов хардуер. В него са реализирани протоколи като например:

Internet Packet Exchange (IPX) на Novell за между мрежов обмен

IP Internet Protocol

X.25 (частично този протокол се реализира на слой 2)

CLNP мрежов протокол без организация на съединения.

4. Транспортно ниво. Най-високо в йерархията на нивата, отговарящи за транспорта на данни. Осигурява следенето за цялостност на изпращаните или

получаваните данни, контролира потока и последователността на пакетите с данни, осигурява механизмите за функционирането на виртуалните канали и системите за откриване и отстраняване на неизправности.

Транспортният слой на модела OSI специфицира много функции, както и няколко нива от процедурите за откриване и коригиране на грешки. На най-високото от тях транспортният слой може да открива и дори да коригира грешки, да идентифицира пакети, предадени в неправилна последователност, и да ги препоръчва в необходимия ред. Освен този слой мултиплексира каналите на няколко съобщения в една линия, като поставя заглавия на съобщенията, посочващи принадлежността им към съответните канали. Транспортният слой регулира информационния поток чрез управление на движението на съобщенията. В този слой е реализиран протоколът:

Sequenced Packet Exchange (SPX) на Novell

TCP за управление на предаването

NCP Netware Core Protocol

SPX

TP4

5. Сесийно ниво. На основата на множество мрежови протоколи установява, управлява и затваря сеансите за взаимодействие между приложенията, администрирайки заявките им. Сесийният слой дефинира функциите, свързани с управлението на мрежата. Той определя механизма за работа с пароли,

процедурите за включване в мрежата, както и методите за контрол и осигуряване на статистическа информация за мрежата.

Дотук разгледахме спецификации на модела OSI, свързани с битове и съобщения, но не и с разпознаването на отделните потребители на системата. Сесийният слой засяга управлението на мрежата. На това ниво дадена сесия може да се прекрати или да завърши в съответствие с определени правила. Диалогът с потребителя се осигурява от сесийния слой.

На сесийното ниво се проверява паролата, въведена от потребителя, и му се предоставя възможност да превключи режима за обмен от полудуплексен в дуплексен. Сесийният слой позволява да се определи: кой предава, колко често и колко дълго. Към функциите на този слой спадат управлението на обмена на данни и дори възстановяването на предаването след откриване на неизправност в системата. На това ниво се контролира използването на мрежата и се регистрира времето, отделено за всеки потребител.

6. Представително ниво. Осигурява "читаемост" на информацията, изпращана от представителното ниво на една система към същото ниво на друга система. За целта това ниво може да транслира изпращаната информация към някакъв общ формат, разбираем за другата система. Защитата на информацията в мрежата, обмена на файлове и форматирането на данните са функции на представителния слой. Представителният слой на модела OSI специфицира функции, осигуряващи защита на информацията в мрежата от неправомерен достъп, обмен на файлове и форматиране на данните. На това ниво данните могат да се формират по различни начини, включително чрез кодовете ASCII и EBCDIC.

В американския стандартен код за обмен на информация (ASCII) всеки

символ се представя чрез седем информационни и един бит за контрол. Този код има почти универсално приложение. Разширеният двоично-десетичен код за обмен на информация (EBCDIC) се използва в много от големите ЕИМ на IBM. Представителният слой трябва да предвижда възможност за обмен на данни и по двата стандарта.

За да се осъществи обмен на информация между два компютъра без изкривяване, те трябва да използват еднакви протоколи (правила за обработка на данните) по отношение на представителния слой на мрежата. На това ниво е възможно да се преобразуват протоколите на различни компютри с различни формати на информацията. Повечето функции на текстообработката, свързвани с форматирането на текстове (включително страницирането, определянето на броя на редовете на екрана и дори преместването на курсора), се осигуряват от представителния слой.

7. Приложно ниво. Осигурява изпълнението на потребителските задачи, служейки за интерфейс между крайният системен потребител и мрежовите услуги. На това ниво се синхронизират съвместно работещите приложения, идентифицират се устройствата, с които ще се установява връзка, оценява обемът на ресурсите, необходими за предполагаемата връзка. Мрежовите програми от приложения слой включват софтуер за електронна поща, за управление на бази от данни, за сървер за принтер. Приложният слой специфицира функции, свързани с обработката на съобщенията, с отдалеченото включване в мрежата и с осигуряването на статистическа информация, необходима за управлението на мрежата. На това ниво от модела на мрежата се намират програмите за управление на бази от данни, програмите за електронната поща, софтуера за файловете сървери и сърверите за принтер, както и програмите на операционната система.

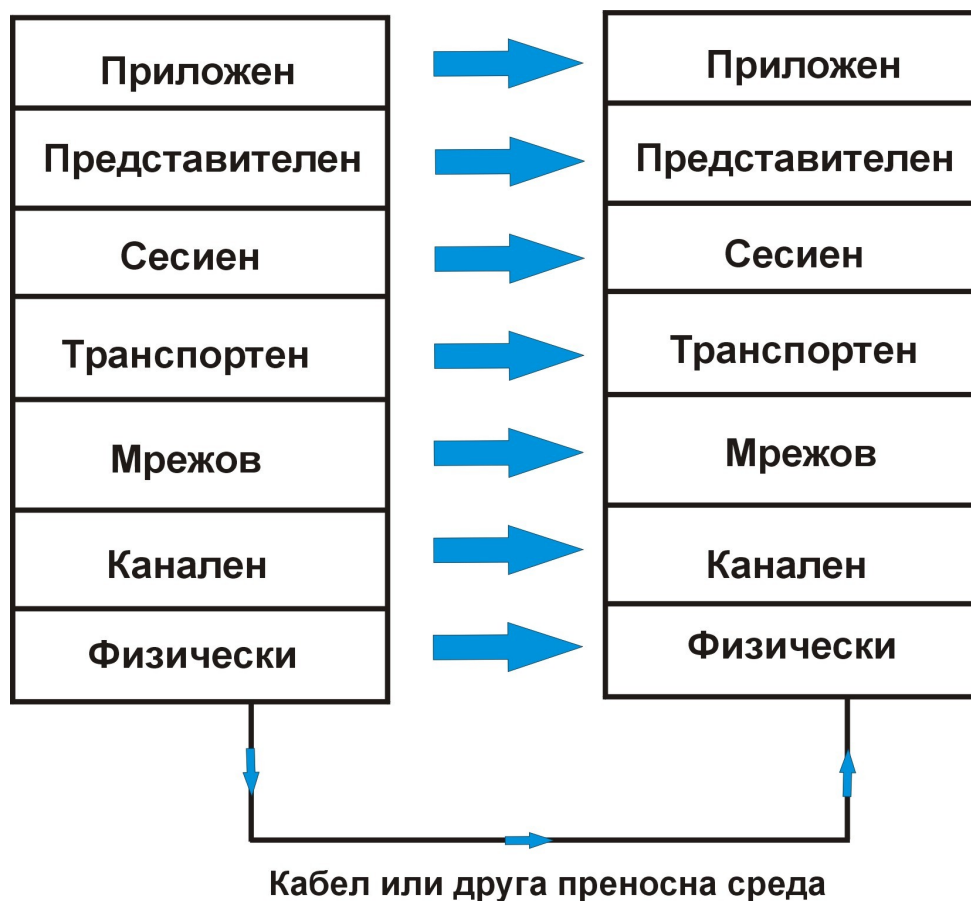
В по-голямата си част функциите, изпълнявани на това ниво, се определят от

потребителя. Тъй като програмите на потребителите въвеждат различни изисквания, трудно е да се правят обобщения за различните протоколи. За някои приложения (например за банковото дело) са разработени серия от стандарти за този слой.

Въпреки че, моделът OSI предлага добра основа за описване на комуникационните функции на ЛМ, малко от съществуващите сега мрежи са постигнали точно съответствие с него. Въпреки че се говори за мрежи, съответстващи на модела OSI, стандартите все още са непълни, а продуктите слабо разпространени. Докато някои организации очакват завършването на стандартите OSI, много други се насочват към TCP/IP, който предлага сходни по тип услуги, като по този начин задържат разпространението на OSI

Мрежова комуникация

Процесът на мрежова комуникация работи по следния начин: от изпращащата страна дадено приложение създава данни, които трябва да бъдат предадени по мрежата. След това той ги предава на приложния слой от мрежовия компонент на операционната система. Когато данните преминават през слоевете, те биват капсулирани или затваряни в рамките на по-голяма единица, тъй като . Когато данните достигнат приемащият компютър, процесът се извършва в обратния ред; информацията се предава нагоре през всеки слой и докато става това, капсулиращата информация постепенно бива премахвана, слой по слой, в ред, обратен на реда, в който е била добавяна. Каналният слой {data link layer} в приемния край чете и сменя хедъра, добавен от каналния слой на изпращащата страна. След това мрежовият слой на приемащата страна обработва информацията в хедъра, добавен от съответния слой на изпращащия компютър, и т.н. Всъщност всеки слой комуникира със слоя, който носи същото име от другата страна.



На илюстрацията се вижда как работи този процес на комуникация. Всеки слой комуникира директно със своя равноправен слой от другата страна.

Когато данните преминат целия си път през слоевете на приемащия компютър, цялата хедър информация бива премахната и данните се възстановяват в тяхната оригинална форма, т.е. както са създадени от приложната програма на изпращащия. В тази форма те се представят на приложението на приемника под формата на информация.

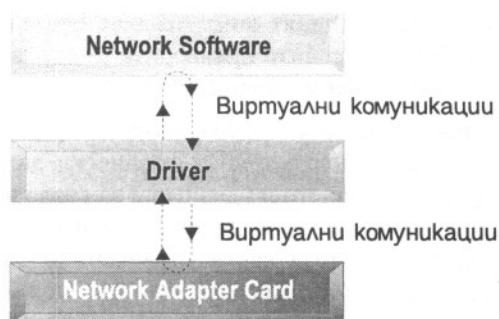
Мрежова среда

Мрежовите драйвери осигуряват комуникацията между мрежовата адаптерна карта и мрежовия пренасочвател (redirector), работещ на компютъра. Пренасочвателят е част от мрежовия софтуер, която приема входно изходните

заявки към отдалечени файлове, след което ги изпраща или пренасочва към друг компютър от мрежата. Мрежовият администратор инсталира драйвера посредством инсталационна програма, която най-често се нарича setup програма. По време на инсталирането драйверът се записва на твърдия диск на компютъра.

Драйверите и OSI моделът

Драйверите на мрежовите адаптерни карти се намират в подслоя за контрол на достъпа до физическата среда (MAC) на каналният слой на OSI модела. Подслоят за контролиране на достъпа до физическата среда е отговорен за предоставянето на поделен достъп на мрежовата адаптерна карта до физическия слой. С други думи, драйверите за мрежови адаптерни карти осигуряват директната комуникация между компютъра и картата. Кое, от своя страна, осигурява връзка между компютъра и останалата част от мрежата.



Комуникация между мрежовата адаптерна карта и мрежовия софтуер

Драйверите и мрежовият софтуер

По правило производителите на мрежови адаптерни карти предоставят драйвери за създателите на мрежов софтуер, за да могат тези драйвери да бъдат включени в мрежовата операционна система.

Списъкът за хардуерна съвместимост (hardware compatibility list -HCL) на производителите на операционни системи съдържа драйверите, които са били тествани и са включени в операционната система.

Например HCL на Microsoft Windows NT Server съдържа над 100 драйвера за мрежови адаптерни карти от различни производители, които са тествани от Microsoft и са включени в Windows NT Server. Това означава, че Windows NT Server, във вида, в който се доставя, може да работи с повече от 100 различни вида мрежови адаптерни карти.

Дори и ако драйверът за дадена карта не е включен в мрежовата операционна система, нормално е производителите на мрежови адаптерни карти да ви предложат драйвери за най-популярните мрежови операционни системи, на диск, който се продава с картата. Необходимо е, преди да купите карта, да се уверите, че тя има драйвер за съответната операционна система, под която ще я използвате.

Инсталиране

Всяка мрежова операционна система има свой собствен метод за инсталиране на драйвери, но инсталационните процедури на най-популярните операционни системи обикновено използват интерактивен графичен интерфейс, който ръководи потребителя по време на инсталационния процес.

Конфигуриране

Мрежовата адаптерна карта обикновено има конфигурируеми опции, които трябва да се настройат правилно, за да може тя да функционира нормално.

Повечето от новите мрежови адаптерни карти обаче се конфигурират софтуерно или използват технологията Plug and Play. При тях няма DIP превключватели или джъмperi. Конфигурирането им се извършва софтуерно по време на или след инсталирането на драйвера, или ако имаме Plug and Play съвместима система, самата операционна система ще се опита автоматично да конфигурира хардуерното устройство.

Обновяване

Ако производителят направи промени в драйвера, които подобряват производителността на компонента, той може да го изпрати по пощата до регистрираните потребители, да го публикува в Интернет, в бюлетин борд система, или да го разпространи чрез онлайн услуга, като Microsoft Network (MSN), CompuServe или друга. След това потребителят може да инсталира новия драйвер на своя компютър.

Процесът на обновяване на драйверите обикновено е подобен на инсталационния процес.

Премахване (removing)

Понякога се налага да се премахват драйвери. Това например се случва, когато по някаква причина първоначалните драйвери влизат в конфликт с новоинсталирани драйвери. В други ситуации, ако част от оборудването се премахне, ще е добра идея да се премахнат и драйверите за него, за да не възникнат конфликти с други драйвери, които ще бъдат инсталирани по-късно.

Процесът на премахване на драйвери е подобен на инсталирането и

обновяването им.

Подготовка на данните

Преди данните да могат да бъдат изпратени по мрежата, мрежовата адаптерна карта трябва да ги промени от вид, който се разпознава от компютъра, във вид, който може да се предава по мрежата.

Данните се движат в компютъра по така наречените шини (busses). В действителност шината има няколко писти, разположени една до друга (паралелно), поради което данните могат да пътуват на групи, вместо в единичен (сериен) поток, както е по мрежата.

По-старите шини, например тези на първоначалните IBM PC, бяха 8-битови и можеха да предават по 8 бита едновременно. IBM PC/AT използва 16-битова шина, т.е. може да предава данните по 16 бита едновременно. Много компютри използват 32-битови шини. Когато данните пътуват по компютърната шина, се казва, че те се предават паралелно. Можете да гледате на 16-битовата шина като на магистрала с 16 платна и с 16 автомобила, пътуващи един до друг (в паралел), като всеки носи по един бит от данни.

По мрежовия кабел данните трябва да пътуват в поток от единични битове. Когато те се движат по кабела, се казва, че има серийно предаване, защото битовете се предават последователно един след друг. С други думи, кабелът е еднолентова магистрала. Данните пътуват по тази магистрала винаги в една посока. Компютърът или изпраща, или получава данни.

Мрежовата адаптерна карта взема пътуващите паралелно данни от шината и

ги преструктурира така, че да могат да пътуват по широката 1 бит пътека на серийния кабел. Това се осъществява чрез преобразуването на цифровите сигнали в електрически или оптични, които могат да се предават по мрежовите кабели. Компонентът, който се грижи за това, се нарича трансийвър (transceiver - приемо-предавателно устройство - от transmitter/receiver).

Мрежови адреси

Освен да преобразува данните, мрежовата адаптерна карта трябва да обозначи тяхното местоположение, т.е. техния адрес, за да може останалата част от мрежата да ги различава от данните на другите мрежови адаптерни карти

Мрежовите адреси се определят от комитета на IEEE (Institute of Electrical and Electronics Engineers, Inc.). IEEE приписва блокове от адреси за всеки производител на мрежови адаптерни карти. Производителят вгражда тези адреси в чиповете на картата посредством процес, известен като "прогаряне" на адреса в картата. След извършването на тази процедура, всяка карта, а следователно и всеки компютър, имат уникален адрес в дадена мрежа.

Мрежовата адаптерна карта изпълнява и някои други функции по получаването на данните от компютъра и подготвянето им за изпращане по мрежовия кабел.

1. Компютърът и мрежовата адаптерна карта трябва да комуникират помежду си, за да прехвърлят данните от компютъра в картата. При карти, използващи директен достъп до паметта (direct memory access - DMA), компютърът заделя част от паметта си за мрежовата адаптерна карта.

2. Мрежовата адаптерна карта сигнализира на компютъра, изисквайки данни от него.

3. Компютърната шина прехвърля данните от паметта на компютъра към мрежовата адаптерна карта.

Често данните се движат с по-голяма скорост от тази, с която би могла да ги обработи мрежовата адаптерна карта, затова те се изпращат в нейния RAM буфер, където се съхраняват временно, както при предаване, така и при получаване.

Изпращане и контролиране на данните

Преди да изпрати данните по мрежата, изпращащата мрежова адаптерна карта, образно казано, води електронен диалог с приемащата карта, като двете постигат съгласие за следното:

Максималният размер на изпращаните групи от данни

Количеството изпратени данни, преди да се върне потвърждение

Времеви интервали между изпращането на отделните групи

Времето на изчакване преди изпращане на потвърждение

Какво количество данни може да побере всяка от картите, преди да се получи препълване

Скоростта на предаване на данните

Ако нова, по-бърза и по-усъвършенствана карта, трябва да комуникира с някоя по-стара и по-бавна, те трябва да намерят някаква обща скорост на трансфер, удобна и за двете. Някои по-нови мрежови карти имат възможност да се настройват към скоростта на по-бавната карта, с която комуникират.

Всяка карта сигнализира на другата, указвайки параметрите си и приемайки или настройвайки се към параметрите на другата карта. Когато се установят всички подробности по комуникацията, двете карти започват да изпращат и получават данни.

Мрежови пакети

Преди да изпрати данните по мрежата, изпращащият компютър ги разделя на малки пакети, които са по-лесни за предаване по кабела. Тези пакети са основната съставна единица в мрежовите комуникации. Благодарение на тях комуникациите се осъществяват навременно, без да се стига до блокиране или забавяне на мрежата.

Всички пакети се състоят от следните основни компоненти: адрес на подателя, данни, адрес на получателя, инструкции, и информация за корекция на грешки. Всеки пакет има три секции: заглавна част, данни и завършваща част. Заглавната част съдържа предупреждаващ сигнал, адресите на подателя и получателя и информация за синхронизация на предаването, а завършващата част се състои от компонент за корекция на грешки, наречен CRC (cyclical redundancy check).

Пакетите започват да се формират в приложния слой на OSI модела и преминават надолу през всички слоеве, като всеки слой добавя своя информация към пакета.

Структура на пакетите

Пакетите могат да съдържат няколко вида данни:

Информация - например съобщения или файлове.

Данни и команди за управление на компютъра, като например заявки за услуги.

Кодове за контрол на сесиите - например корекция на грешки, указваща необходимостта от повторно предаване.

Компоненти на пакетите

Всички пакети се състоят от следните компоненти:

Адрес на подателя (source address), идентифициращ изпращащия компютър.

Самите данни, които трябва да бъдат предадени

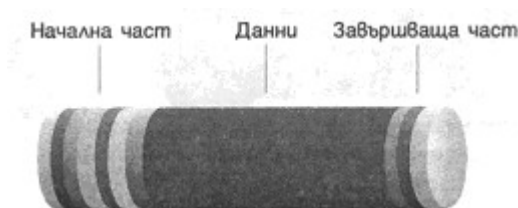
Адрес на получателя (destination address), идентифициращ приемащия компютър.

Инструкции, указващи на мрежовите компоненти как да "пуснат" данните по мрежата.

Информация, която указва на получаващия компютър как да свърже пакетите заедно, за да сглоби първоначалните данни.

Информация за проверка за грешки, гарантираща че данните са пристигнали "непокътнати".

Компонентите са групирани в три секции: *заглавна част (header)*, *данни (data)* и *завършваща част (trailer)*.



Компоненти на пакета

Протоколи

Функция за протоколите

Протоколите са правила и процедури за комуникиране. Например дипломатите на дадена държава спазват протокола при срещите си с дипломатите на други държави. По аналогичен начин в компютърната среда се прилагат правила за комуникиране. Когато няколко компютъра са свързани в мрежа, правилата и процедурите, регулиращи тяхното взаимодействие, се наричат протоколи.

Когато се разглеждат протоколите в мрежова среда, има три пункта, на които трябва да се обърне внимание:

1. Съществуват много протоколи. Въпреки че всеки от тях позволява елементарни комуникации, отделните протоколи имат различни цели и изпълняват различни задачи. Всеки протокол си има своите предимства и ограничения.

2. Някои протоколи работят в различни OSI слоеве. Слой, в който работи даден протокол, характеризира неговите функции. Например щом даден протокол работи във физическия слой, значи той се грижи за преминаването на пакетите с данни през мрежовата адаптерна карта към мрежовия кабел.

3. Няколко протокола могат да работят съвместно в общ протоколен комплект (protocol stack или suite), (б.ред. В терминологията на български често се използва и "протоколен стек")

Точно както мрежата обединява функциите на всеки слой на OSI модела, така и различните протоколи работят съвместно на различни нива в един общ комплект. Нивата в комплекта протоколи съответстват на слоевете на OSI модела. Взети заедно, протоколите характеризират функциите и възможностите на целия протоколен комплект.

Как работят протоколите

Всички технически операции по предаването на данни по мрежата трябва да се разделят на отделни систематизирани стъпки. Във всяка стъпка се извършва определено действие, което не може да бъде извършено в друга стъпка. Всяка стъпка има свои правила и процедури, т. е. протокол.

На всеки компютър в мрежата стъпките трябва да се прилагат последователно и по един и същи начин. При изпращащия компютър тези стъпки трябва да се

извършват от горе на долу, а при получаващата машина - обратното, от долу на горе.

Изпращащият компютър

При изпращащия компютър протоколът прави следното:

Разделя данните на малки части, наречени пакети, които може да управлява.

Добавя адресна информация към пакетите, за да може получаващият компютър в мрежата да знае, че данните са предназначени за него.

Подготвя данните за реалното им предаване през мрежовата адаптерна карта директно навън в мрежовия кабел.

Получаващият компютър

При получаващия компютър протоколът извършва същите серии от стъпки в обратен ред:

Получава пакетите данни от кабела.

Вкарва пакетите данни в компютъра през мрежовата адаптерна карта.

Отделя от пакетите с данни служебната информация, добавена от изпращащия компютър.

Копира данните от пакетите в буфер, за да ги сглоби в първоначалния им вид

Подава сглобените данни в използваем вид към съответното приложение.

И изпращащият, и получаващият компютър трябва да изпълняват всяка стъпка по един и същ начин, за да могат данните да се запазят във вида, в който са били изпратени.

Например, ако два протокола трябва да разделят данните на пакети и да добавят синхронизираща и контролна информация, но го правят по различен начин, то който и да е компютър, използващ един от тези протоколи, няма да може успешно да комуникира с компютър, използващ другия протокол.

Маршрутизируеми или немаршрутизируеми протоколи

До средата на 80-те години повечето мрежи бяха изолирани. Те обслужваха даден отдел или фирма, и рядко биваха свързвани към по-голяма комуникационна среда. Но с развитието на LAN технологията нараснаха и комуникационните нужди в бизнеса. Локалните мрежи станаха част от по-големи мрежи, в които самите LAN обменят информация помежду си.

Изпращането на данните от една локална мрежа към друга по един от няколкото възможни пътя се нарича маршрутизиране (routing). Протоколите, които поддържат многомаршрутни (multipath) комуникации от тип LAN-към-LAN, се наричат маршрутизируеми (routable) протоколи. И тъй като маршрутизируемите протоколи се използват за свързване на няколко локални мрежи и създаването на глобална мрежа (WAN), те се превърнаха в много важни компоненти.

Протоколите в слоеста архитектура

В мрежите се налага съвместната работа на няколко протокола, за да се гарантира, че данните са:

Подготвени

Прехвърлени

Получени

Обработени

Работата на различните протоколи трябва да бъде координирана, за да няма конфликти и незавършени операции. Това става чрез разпределянето на протоколите в отделни слоеве.

Протоколни комплекти

Протоколните комплекти са комбинации от протоколи. Всеки слой използва конкретен протокол за управление на дадена функция или подсистема от комуникационния процес. Всеки слой спазва свой собствен набор от правила.



OSI моделът, показващ слоевете с протоколи

Както и при OSI модела, най-долният слой в протоколния комплект определя как производителите да направят така, че тяхното оборудване да може да се свързва с оборудването на другите производители. По-горните слоеве определят правилата за провеждане на комуникационни сесии и взаимодействията с приложенията. Колкото по-високо в комплекта се намират, толкова по-комплексни стават задачите и асоциираните с тях протоколи.

Процесът на свързване

Процесът на свързване (binding) осигурява доста голяма гъвкавост при настройката на мрежата. Протоколите и мрежовите карти могат да се комбинират според конкретните нужди. Например два протоколни комплекта, като IPX/SPX и TCP/IP, могат да се свържат към една мрежова адаптерна карта. Ако в компютъра има повече от една мрежова карта, всеки протоколен комплект може да се свърже с всяка една от картите, или с всички тях.

Редът на свързване (binding order) определя последователността, в която

операционната система работи със съответния протокол. При наличието на много протоколи, свързани към една мрежова адаптерна карта, той определя реда, в който протоколите ще се използват, докато се установи успешна връзка (connection). Обикновено свързването (binding) се прави при инсталирането или инициализирането на протокола или операционната система. Например, ако TCP/IP е свързан като първи протокол, той ще се използва при първия опит за осъществяване на мрежова връзка. Ако такава не бъде осъществена, компютърът незабавно ще се опита да осъществи връзка, използвайки следващия протокол, указан в реда на свързване.

Свързването не се ограничава само до асоцииране на протоколния комплект с мрежовата адаптерна карта. Протоколните комплекти трябва да се свържат или асоциират с компонентите над и под тях, така че данните да могат да преминават плавно през комплекта по време на изпълнение. Например TCP/IP може да бъде свързан със сесийния слой NetBIOS, намиращ се над него, и с драйвера на мрежовата адаптерна карта, намиращ се под него. От своя страна, драйверът на мрежовата адаптерна карта е свързан със самата карта.

Стандартни комплекти

Компютърната индустрия е определила няколко комплекта като стандартни протоколни модели. Най-важните от тях включват:

Протоколния комплект ISO/OSI.

IBM Systems Network Architecture (SNA)

Digital DECnet™

Novell NetWare (б.ред. по-точно протоколното семейство IPX/SPX за Novell NetWare)

Apple AppleTalk®

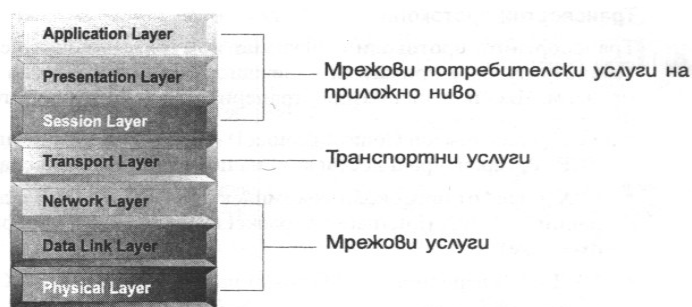
Протоколния комплект за Интернет - TCP/IP

На всяко ниво от тези комплекти има протоколи, изпълняващи специфична за това ниво задача. Обаче комуникационните задачи, които трябва да изпълнява мрежата, се възлагат на протоколи, работещи като един от следните три протоколни типа. Тези типове протоколи съответстват грубо на OSI модела:

Приложен

Транспортен

Мрежов



Комуникационни задачи в рамките на OSI модела

Приложни протоколи

Приложните протоколи работят в горния слой на OSI модела. Те осигуряват обмена на данни и взаимодействието приложение-приложение. Някои от популярните приложни протоколи са:

APPC (Advanced Program to Program Communication) - SNA протокол на IBM, използван най-вече в AS/400.

FTAM (file transfer access and management) - OSI протокол за достъп до файлове.

X.400 - CCITT протокол за международни e-mail предавания.

X.500 - CCITT протокол за файлови и директорийни услуги между различни системи.

SMTP (simple mail transfer protocol) - Интернет протокол за трансфер на e-mail съобщения.

FTP (File Transfer Protocol) - Интернет протокол за трансфер на файлове.

SNMP (simple network management protocol) - Интернет протокол за наблюдение на мрежите и на мрежовите компоненти.

Telnet - Интернет протокол за влизане в отдалечени хостове и обработка на данните локално.

Microsoft SMBs (server message blocks) и клиентски обвивки (shells) или пренасочватели (redirectors).

NCP (Novell NetWare Core Protocol) и клиентски обвивки или пренасочватели за Novell.

AppleTalk и Apple Share® - Протоколният мрежов комплект на Apple.

AFP (AppleTalk filing protocol) ~ Протокол на Apple за дистанционен достъп до файлове (т.е. достъп до отдалечени файлове).

DAP (data access protocol) - DECnet протокол за достъп до файлове.

Транспортни протоколи

Транспортните протоколи осигуряват комуникационните сесии между компютрите и се грижат за надеждното придвижване на данните по мрежата. Някои от най-разпространените транспортни протоколи са:

TCP (Transmission Control Protocol) - протоколът от комплекта TCP/IP, гарантиращ доставката на последователно предавани данни.

SPX - част от протоколния комплект на Novell за последователни данни IPX/SPX (internetwork packet exchange/sequential packet exchange).

NWLink - вариантът на Microsoft на протокола IPX/SPX.

NetBEUI (NetBIOS [network basic input/output system] extended user interface) - протокол за установяване на комуникационни сесии между компютри (NetBIOS) и осигуряване на съответните транспортни услуги за данни (NetBEUI).

ATP (AppleTalk transaction protocol), NBP (name binding protocol) -протоколите на Apple за комуникационни сесии и транспорт на данни.

Мрежови протоколи

Мрежовите протоколи осигуряват така наречените свързващи услуги (link services). Тези протоколи управляват адресиращата и маршрутизиращата информация, проверките за грешки и заявките за повторно предаване. Мрежовите протоколи дефинират и комуникационните правила за конкретна мрежова среда, като например Ethernet или Token Ring, Най-популярните мрежови протоколи са:

IP (Internet Protocol) - TCP/IP протокол за насочване и препредаване на пакетите.

IPX (internetwork packet exchange) - протокол на NetWare за насочване и препредаване на пакетите.

NWLink - вариантът на Microsoft на протокола IPX/SPX.

NetBEUI - транспортен протокол, осигуряващ услуги за транспортиране на данни за NetBIOS сесии и приложения.

DDP (datagram delivery protocol) ~ AppleTalk протокол за транспортиране на данни.

TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) е стандартен комплект

протоколи, обезпечаваш комуникациите в хетерогенна среда. Освен това TCP/IP предлага маршрутизиращ протокол за промишлени мрежи, и достъп до световната мрежа Интернет и нейните ресурси.

Той се превърна в стандартен протокол за осигуряване на взаимодействието между различни видове компютри, наричано интероперативност (interoperability). Тази интероперативност е едно от основните предимства на TCP/IP. Почти всички мрежи поддържат TCP/IP като протокол. TCP/IP поддържа още и маршрутизиране (routing) и често се използва за междумрежов (internetworking) протокол.

Поради своята популярност, той стана фактическият стандарт за междумрежова работа (internetworking).

Други протоколи, написани специално за комплекта TCP/IP, са:

SMTP (simple mail transfer protocol) - протокол за електронна поща

FTP (File Transfer Protocol) - протокол за обмен на файлове между компютри, работещи с TCP/IP

SNMP (simple network management protocol) - протокол за мрежово управление

TCP/IP има два основни недостатъка: размерът и скоростта. Той е относително обемен протоколен комплект, което може да доведе до проблеми при MS-DOS базирани клиенти. Но при операционните системи с графичен потребителски интерфейс (GUI), като Windows NT или Windows98, размерът не е проблем, а скоростта е почти същата, както при IPX.

NetBEUI

NetBEUI идва от "NetBIOS extended user interface". Първоначално NetBIOS и NetBEUI бяха много тясно свързани помежду си и се считаха за един протокол. Обаче някои мрежови производители отделиха протокола за сесийния слой - NetBIOS - за да може да се използва с маршрутизируеми транспортни протоколи. NetBIOS (network basic input/output system) е LAN интерфейс за сесийния слой на IBM, който действа като приложен интерфейс за мрежата. Той осигурява инструментариума, необходим на една програмата за установяване на сесия с друга програма по мрежата, и е доста популярен, защото се поддържа от много приложни програми.

NetBEUI е малък, бърз и ефикасен протокол за транспортния слой. Той се поддържа от всички мрежови продукти на Microsoft. NetBEUI беше създаден в средата на 80-те и се поддържаше от първия мрежов продукт на Microsoft - MS®-NET.

Предимствата на NetBEUI са неговият малък размер (което е важно за MS-DOS базираните компютри), скоростта на трансфера на данни и съвместимостта му с Microsoft-базираните мрежи.

Главният недостатък на NetBEUI е, че не поддържа маршрутизиране. Освен това е ограничен само до Microsoft-базирани мрежи.

X.25

X.25 е набор от протоколи, които са стандарт за пакетно-комутируеми мрежи, съставени от комутируеми услуги. Комутируемите услуги първоначално служеха

за установяване на връзка между отдалечени терминали и големи машини (main frame systems).

XNS

Xerox Network System (XNS) беше разработен от Xerox за техните Ethernet мрежи. Той беше широко използван през 80-те години, но постепенно беше изместен от TCP/IP. XNS е обемен и бавен протокол, но причинява повече бродкасти, водещи до по-голям мрежов трафик.

IPX/SPXnNWLink

IPX/SPX (internetwork packet exchange/sequenced packet exchange) е протоколен комплект, използван в мрежите на Novell. Както NetBEUI, той е относително малък и бърз протокол за LAN. Но за разлика от NetBEUI той поддържа маршрутизиране. IPX/SPX води началото си от

XNS.

Microsoft предлагат NWLink като своя версия на IPX/SPX. Той е транспортен протокол и поддържа маршрутизиране.

APPC

APPC (advanced program-to-program communication) е транспортният протокол на IBM, разработен като част от SNA (systems network architecture). Целта му е да позволи на приложните програми, работещи на различни компютри, да комуникират помежду си и директно да обменят данни.

AppleTalk

AppleTalk е протоколният комплект на Apple Computer, създаден с цел да се даде възможност на компютрите Apple Macintosh да поделят файлове и принтери в мрежова среда.

Комплектът от OSI протоколи

Комплектът от OSI протоколи е пълен протоколен комплект, в който всеки протокол съответства на точно определен слой от OSI модела. Комплектът от OSI протоколи включва маршрутизируеми и транспортни протоколи, протоколи от серията IEEE 802, протокол за сесийния слой, за представителния слой, както и няколко протокола за приложния слой, създадени с цел осигуряване на пълна мрежова функционалност, включително файлов достъп, печат, и емуляция на терминал.

DECnet

DECnet е протоколният комплект на Digital Equipment Corporation. Той представлява набор от хардуерни и софтуерни продукти, реализиращи архитектурата Digital Network Architecture (DNA). DECnet дефинира комуникационни мрежи по локални Ethernet мрежи, градски мрежи FDDI MAN (fiber distributed data interface metropolitan area networks) и по глобални WAN, използващи частни или обществени средства за трансфер на данни. DECnet може да използва и TCP/IP, и OSI протоколите, освен своите собствени. Той е маршрутизируем протокол.

DECnet е обновяван няколко пъти, като всяко обновяване се нарича фаза (Phase). Сегашната версия е DECnet Phase V, а използваните протоколи са специфични за Digital, но също така представляват и почти пълна реализация на комплекта от OSI протоколи.

Добавяне и премахване на протоколи

Протоколите се добавят и премахват по почти същия начин, както и драйверите. В зависимост от операционната система, по-съществените протоколи се инсталират автоматично по време на първоначалната ѝ инсталация. В мрежовата операционна система Windows NT Server, протоколът по подразбиране е TCP/IP.

За да добавите протокол като NWLink след първоначалната инсталация, трябва да използвате помощната програма, предлагана от съответната операционна система. Например при Windows NT Server програмата Setup предлага серия от графични прозорци, които помагат на администратора при:

Инсталиране на нов протокол.

Промяна на реда, по който са свързани инсталираните протоколи.

Премахване на протокол.

TCP/IP

TCP/IP е не само протоколен стек, състоящ се от протокол от мрежовия слой и протокол от транспортния слой, но и пълен комплект от протоколи, работещи в много слоеве на мрежовия модел.

Много от протоколите, включени в комплекта, функционират като инструменти за събиране на информация и отстраняване на проблеми.

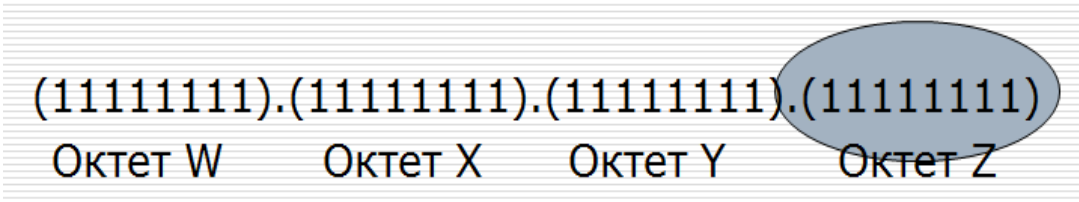
TCP/IP използва двукомпонентен логически адрес - IP адресът - за да идентифицира компютрите източници и компютрите местоназначения в мрежовите комуникации.

Протоколът от мрежовия слой: IP

Знаете, че мрежовият слой се занимава със задачите по маршрутизирането. TCP/IP протоколите позволяват това маршрутизиране, като използват IP адреси, за да идентифицират мрежовите устройства. Всеки компютър, свързан в мрежата принтер, маршрутизатор и други мрежови устройства, притежават уникален IP адрес. В действителност едно устройство може да има няколко IP адреса. IP адресите могат да бъдат частни, т.е. валидни само в локалната мрежа в която се използват или публични (“истински”), т.е. такива които са валидни и уникални в целият Интернет. ”Истинските” IP адреси се купуват от IANA (Internet Assigned Numbers Authority).

Какво представлява IP адресирането

Всеки IP адрес се състои от четири 8-битови части (т.н. октети).



(11111111).(11111111).(11111111).(11111111)
Октет W Октет X Октет Y Октет Z

Заедно те идентифицират мрежата, в която се намира устройството, и конкретното устройство в тази мрежа. Една част от IP адреса представлява мрежата, а втората част представлява хоста (т.е. конкретния компютър).

Когато изпратите съобщение по Интернет до различна LAN, маршрутизаторите не се интересуват от хост порцията на IP адреса; те се интересуват само от частта с мрежовия адрес. След като пакетът достигне вярната мрежа (подмрежа), хост адресът се използва за препращане до специфичен компютър.

IP адресите, подобно на останалата информация, обработвана от компютрите, са изградени от двоични цифри, или битове. Тъй като работата с дълги низове от единици и нули е трудна за повечето хора, ние обикновено обозначаваме IP адресите в точково-десетичен формат.

Дължината на един октет е осем бита; има осем цифри, всяка от които е единица или нула. Четирите октета понякога се обозначават като w.x.y.z.

Тъй като има по осем бита във всеки от четирите октета, всеки IP адрес е 32-битово двоично число. Това означава, че съществуват над четири милиарда възможни IP адреси (за да бъдем точни, 4 294 967 296, което е 2^{32}). Един IP адрес обикновено изглежда по следния начин:

192.168.1.12

Класове IP адреси

Знаем, че част от IP адреса идентифицира мрежата, а останалата част идентифицира отделното устройство (хоста), но коя част е и кое от двете представлява?

За нещастие, отговорът е, че зависи.

По традиция това зависеше от класа, към който принадлежеше мрежата .

В ранните дни на Интернет комуникациите изглеждаше логично да се назначават IP адреси на компании и организации на блокове.

Методът на разделяне на IP адреси на класове според размера на мрежата се нарича класово адресиране .

Адресен клас	Брой мрежи	Брой хостове за мрежа
A	126	16777216
B	16384	65535
C	2097152	254
D	-	-

С изобретяването на технологии като транслирането на мрежови адреси вече не важи изискването всеки компютър в локалната мрежа да притежава публичен IP адрес за да може да работи в Интернет.

Както можете да видите в наличност има само 126 адреси от Клас А. Тези адреси бяха изчерпани още преди години; те бяха назначени на много големи корпорации и образователни институции, включващи IBM, Hewlett Packard, Xerox, Масачузетския технологичен институт (Massachusetts Institute of Technology - MIT), Университетът на Колумбия, Digital Equipment Corporation, General Electric и Apple. Всяка мрежа има над 16 милиона хост адреса, които могат да бъдат назначавани на компютрите в тези мрежи.

Схемата за класове от IP адреси създава над 2 милиона Клас С мрежи, но в от тези мрежи не може да има повече от 254 хост адреса. Мрежовите адреси Клас С често пъти се назначават на Интернет доставчици, които разпределят дадения им диапазон на по-малки блокове за компании, разполагащи само до 20 хост машини в техните мрежи.

Клас В адресите попадат между адресите от Клас А и тези от Клас С. Microsoft Corporation е пример за компания с Клас В мрежа.

Клас D адресите не се използват за мрежи, а за мултикаст съобщения, представляващи средство за изпращане на едно съобщение до множество получатели едновременно. Клас D адрес се назначава на указана група от компютри, а мултикастните протоколи се занимават с дистрибуцията на пакетите.

Какво представлява класовото адресиране

Адресният клас се идентифицира от старшите битове, т.е. първите няколко бита в най-левия октет (понякога наричан октет „w"). Адресните класове могат да се идентифицират на базата на диапазона от адреси на първия октет.

Октет W	Октет X	Октет Y	Октет Z
192	168	1	14
Мрежов идентификатор			Хост идентификатор

<i>Идентифициране на адресните класове</i>			
Клас IP адреси	Старши битове	Диапазон от адреси на първия октет	Брой битове в мрежовия адрес
Клас А	0	0-127	7
Клас В	10	128-191	14
Клас С	110	192-223	21
Клас D	1110	224-239	28

Както можете да видите клас А адресите се идентифицират от първия бит (със стойност 0), Клас В адресите се определят от първите два бита -10, първите три бита на Клас С адресите са 110, а мултикаст адресите (Клас D) използват 1110 за първите четири бита.

Адресът 0.0.0.0 е запазен за представяне на всички IP адреси.

Може би вече сте си направили извода, че класовото адресиране не е най-ефективният начин на използване на ограничения брой IP адреси, налични в 32-битовата схема за адресиране. За да илюстрираме това, нека използваме примера за компания, притежаваща 2000 компютъра, които иска да свърже към Интернет.

Един Клас С адрес няма да свърши работа, защото това би ограничило мрежата до 254 хоста. Следващият по-горен клас са Клас В адресите, но ако компанията получи такъв адрес, той би заел диапазон от 65 000 адреса. Тъй като компанията се нуждае само от 2000 от тези адреси, над 63 000 IP адреси ще бъдат загубени. Безкласовото адресиране, се справя с този проблем.

Какво представлява безкласовото адресиране

Загубата на адреси, свързана с класовото адресиране, съдейства за бързото изчерпване на свободни IP адреси. Едно от предложените решения е реализацията на IPv6, който използва по-голямо адресно пространство (128 битово). Счита се, че преминаването към нова версия на IP не е просто и ще отнеме известно време (днес е реалност), докато това се случи. Междувременно съществува друго решение: безкласово адресиране, базирано на безкласовата междудомейнова маршрутизация (classless interdomain routing - CIDR).

Вместо да използва адресни класове, CIDR използва обозначение, прикрепено към всеки IP адрес, което указва броя битове, използвани за мрежовата част на адреса. CIDR мрежите понякога се наричат „slash x” (слаш екс) мрежи, защото IP адресът се разделя от суфикса посредством наклонена черта (слаш). При това положение един CIDR адрес изглежда по следния начин:

192.168.1.0/24.

Числото 24 след наклонената черта означава, че 24-те най-леви бита се използват за идентификация на мрежата, а останалите осем бита се използват за идентификация на хоста. С други думи, първите три октета посочват мрежата, докато последният посочва хост компютъра.

Ако адресирането беше класово това щеше да е Клас С мрежа.

CIDR адрес	Класов адрес
/8	Клас А
/16	Клас В
/24	Клас С

Таблицата показва как CIDR адресите съответстват на традиционните класови адреси.

CIDR позволява много по-ефективно разпределение на IP адреси.

CIDR мрежите могат да бъдат означавани като /20, /21, /28 и т.н.; това означава, че след наклонената черта може да следва какъвто и да е брой битове, които искате да използвате за мрежов идентификатор. Това позволява създаване на мрежи с размери, които попадат между традиционните мрежови класове.

Автоматично разпределяне на адреси

За да комуникира чрез използване на TCP/IP, един компютър или мрежово устройство трябва да притежава уникален IP адрес. Това е логически адрес и се обработва в мрежовия слой.

Частта от адреса, предназначена за мрежата, трябва да бъде същата като тази останалите компютри в дадената подмрежа. Например, ако използвате подразбиращата се подмрежова маска за Клас С мрежи, тогава 192.168.1.12 и

192.168.1.34 ще бъдат два компютъра в една и съща подмрежа, защото мрежовият идентификатор, представян от първите три октета, е един и същ. Точно обратното е при хост частта - тя не трябва да бъде същата за нито един друг компютър в дадената подмрежа. Например, не може да има два компютъра с хост адрес .6 в същата подмрежа.

Съществуват два начина за получаване на IP адрес:

Адресът може да се въведе ръчно в TCP/IP свойствата на операционната система. Това изисква мрежовият администратор да разбира TCP/IP адресирането и да знае как да избере валиден адрес за конкретната мрежа.

Адресът може да се назначи автоматично. По принцип това означава, че даден компютър в мрежата се конфигурира като DHCP сървър, за да задава IP адреси. В други случаи една възможност на операционната система, наречена Automatic Private IP Addressing (APIPA), позволява на компютъра да си самоназначи адрес, ако не успее да се свърже с DHCP сървър.

DHCP

DHCP е протокол, работещ на машина, конфигурирана като DHCP сървър, която назначава IP адреси на машини, конфигурирани като DHCP клиенти.

DHCP сървърът отдава под наем адрес на DHCP клиент.

Стъпките, изпълнявани, когато DHCP клиент получава наем за IP адрес от DHCP сървър, са следните:

1 Компютър, чиито TCP/IP свойства са установени за получаване на IP адрес чрез DHCP, се появява в мрежата. Този компютър бродкаства(т.е.изпраща до всички компютри) съобщение, наречено съобщение за откриване на DHCP. (Бродкастните съобщения се изпращат до всеки компютър чрез използване на специален бродкастен адрес 0.0.0.0 .)

2 Ако в мрежата има DHCP сървър, той приема бродкастното съобщение и отговаря със съобщение, наречено DHCP предложение. Съобщението предлага на клиента IP адрес от диапазона от адреси на сървъра, които са налични за разпределение. Предложеният адрес временно се резервира, докато сървърът не получи отговор от клиента. Съобщението с предложението също се изпраща като бродкаст, защото клиентът все още няма IP адрес, до който съобщението да бъде изпратено директно.

3 Клиентът може да получи множество предложения, ако в мрежата има множество DHCP сървъри. Когато пристигне първото предложение, клиентът отговаря със съобщение, наречено DHCP заявка (DHCP request). Това е приемане на първото получено предложение. То отново е бродкастно съобщение; по този начин всички DHCP сървъри го получават и онези, отправили предложенията си по-късно, ще знаят, че техните предложения не са приети. След това те могат да поставят предложените адреси, които са резервирали за клиента, обратно в своите пулове от свободни адреси.

4 Последната стъпка в тези преговори е DHCP потвърждението (DHCP acknowledgment) (наречено също ACK). DHCP сървърът, чието предложение е прието, получава съобщението за заявка от клиента. Сървърът потвърждава приемането и назначава IP адреса на този клиент за предварително дефиниран „наемен" период. Сървърът може да изпрати на клиента допълнителна информация за конфигуриране на TCP/IP, като например IP адресите на DNS и

WINS сървъри.

Когато тези стъпки приключат, клиентът може да използва назначения му IP адрес, за да комуникира с останалите компютри, работещи с протокола TCP/IP. Това става, докато не изтече предоставеният наем. Забележете, че наемният период може да се зададе от администратор на DHCP сървъра.

Преди изтичането на наема клиентът започва да преговаря, за да го поднови, така че да продължи да използва адреса. Обикновено DHCP сървърът отговаря положително на заявката. Ако обаче DHCP сървърът е изключен, или ако изпрати отговор за отрицателно потвърждение (Negative Acknowledgment - NACK), клиентът трябва да започне DHCP процеса от самото начало.

DHCP има множество предимства пред ръчното задаване на IP адреси:

Спестява време, защото администраторът не трябва да въвежда адрес в настройките на всеки компютър.

Гарантира по-голяма точност, защото администраторът не е необходимо да следи кои адреси вече са били назначени и кои все още са свободни.

Ако компютри в една мрежа трябва постоянно да имат един и същ IP адрес (това често е в сила за сървърите), те пак могат да използват DHCP. В този случай трябва да конфигурирате тези компютри да използват резервиран адрес (reserved address). DHCP сървърът винаги назначава същия адрес на даден клиент, притежаващ такава резервация. Резервацията се извършва на базата на MAC адреса на DHCP клиента (т.е. на база физическия му адрес).

Подмрежовата маска

Подмрежовата маска установява битовете, представляващи мрежовия идентификатор, в единици, а битовете, представляващи хост идентификатора, се установяват в нули. За частта за мрежовия идентификатор се казва, че е „маскирана“ от вдигнатите битове.

По подразбиране, за мрежов идентификатор Клас А мрежите използват битовете в първия октет, Клас В мрежите използват битовете в първите два октета, а Клас С мрежите използват първите три октета.

Протоколите от транспортния слой: TCP и UDP

TCP/IP комплектът включва не един, а два протокола от транспортния слой

Transmission Control Protocol (**TCP**) - Връзково-ориентиран протокол

User Datagram Protocol (**UDP**) - Безвръзков протокол

Кой от двата протокола се използва за изпращане на дадено съобщение? Зависи от нуждите за това предаване. TCP е подходящ, когато най-важна е надеждността, а UDP се използва, ако с най-висок приоритет е производителността (скоростта)

Портове и сокети

TCP/IP използва двукомпонентен логически адрес - IP адресът - за да

идентифицира компютрите източници и компютрите местоназначения в мрежовите комуникации. Какво става обаче, ако две мрежови приложения, работещи на един и същ компютър, изпращат заявки и получават отговори едновременно. Например какво става, ако дадено входящо съобщение е предназначено за вашата e-mail програма, докато друго е Web страница, която се връща към вашия Web браузър? Протоколът се нуждае от начин, по който да прави разлика между тях. Ето къде се намесват TCP и UDP портовете.

Ролята на номерата на портовете

Запомнете, че IP адресът на даден компютър местоназначение се състои от части: мрежов адрес, който функционира подобно на име на улица, и хост адрес, функциониращ подобно на номер на къща. За номерата на портове може да си мислите като специфична маршрутизираща информация вътре в даден адрес. Номерът на порт е допълнение към IP адреса, точно както името на адресата на пощенския плик е допълнение към адреса на улицата. По същия начин можете да си мислите за отделните приложения като за отделни обитатели.

Портът е логическа точка на свързване. Портовете се използват от транспортните протоколи (TCP или UDP) за да идентифицират специфичното приложение което изпраща или получава съобщението.

Широко използваните Интернет приложения имат предефинирани номера портове. Тази стандартизация улеснява комуникациите. Предварително назначените номера на портове се наричат добре познати портове. Съществуват 65 536 използваеми порта. Портове от 0 до 1024 (или т.н. „добре познатите портове“) са запазени за предефинирани услуги

Какво представляват сокетите

След като вече разбирате функцията на портовете, ще дискутираме концепцията за сокетите. Общата дефиниция за сокет е „крайната точка на една връзка, За да може да се осъществи комуникация, трябва да се създаде сокет.

Различните типове сокети използват различни методи за адресиране. Най-популярният метод използва IP адрес, комбиниран с номер на порт, за да идентифицира сокета.

Ping

Ping работи, като изпраща ICMP ехо заявка към компютъра местоназначение. Приемащият компютър след това изпраща обратно съобщение за ICMP ехо отговор.

Също така е възможно да използвате ping, за да разберете IP адреса на даден хост, когато знаете името. Ако въведете командата

ping www.dir.bg

ще видите IP адреса, от който е върнат отговорът.

ARP

ARP е средството, чрез което компютрите в мрежата съпоставят логически IP адреси с физически хардуерни (MAC) адреси. ARP изгражда и поддържа таблица, наречена ARP кеш, в която се съдържат тези съпоставяния. RARP се използва от

машина, която не знае собствения си IP адрес, за да получи информацията на база своя MAC адрес.

ARP също така е помощна програма, работеща от командния ред, която се разпространява с TCP/IP стека на Windows и UNIX/Linux; тя може да се използва за разглеждане и промяна на съпоставяния между IP и MAC адреси. С помощта на помощната програма ARP можете да покажете съдържанието на кеша и да добавяте или изтривате специфични записи.

С командата arp могат да се използват следните ключове:

arp -a - Показва кеша

arp -s - Добавя перманентно съпоставяне между IP и MAC адрес

arp -d - Изтрива запис

В отделните реализации на производителите са включени и други ключове.

Ipconfig, Winipcfg, Config и Ifconfig

Конфигурационните помощни програми могат да предоставят богата информация, включваща текущо използвания IP адрес, MAC адреса, подмрежовата маска и подразбиращия се шлюз; адреси на DNS и WINS сървъри; DHCP информация; разрешени услуги. Съществуват множество ключове, зависещи от производителя и специфичната помощна програма.

Информацията за TCP/IP конфигурацията може да се изведе чрез използват

следните помощни програми, които зависят от операционната система:

Ipconfig - Windows NT и Windows 2000 (от командния ред)

Winipcfg - Windows 95 и 98 (графичен интерфейс)

Ifconfig - UNIX и Linux (от командния ред)

Tracert, Iptrace и Traceroute

Често пъти е полезно да проследите маршрута, по който даден пакет поема пътя от компютъра източник до хоста местоназначение. TCP/IP стековете включват помощна програма за проследяване на маршрута, която ви позволява да идентифицирате маршрутизаторите, през които преминава съобщението. В зависимост от вашата операционна система можете да използвате една от следните:

Tracert - Windows

Iptrace - NetWare NLM

Traceroute - UNIX/Linux