Local area network (LAN) е комуникационна система, която свързва два или повече компютъра върху териториално ограничен район (например: къща, офис или квартал) в обща среда- Интернет. Основната идея при внедряването й е осигуряване и повишаване на връзката между хората, и предоставяне на достъп до общи данни или мрежови ресурси. Елементите на една локална мрежа най-често са компютри, терминали, принтери, факс-машини, аудио и видео системи, използват се също сървъри и хост-компютри.Тя е в основата на:

- metropolitan area networks (MANs) – свързва компютрите в един град;
- wide area networks (WANs) – обединява потребителите по света;

Те се различават по обхвата и скоростта на преноса на данни.

LAN мрежите могат да се категоризат по различни признаци:

1. В зависимост от метода на администриране:
   - ✓ **мрежа с равноправен достъп (Peer-to-Peer)** – всеки компютър функционира и като клиент, и като сървър. Потребителят администрира ресурсите на своята машина. Този тип мрежи се използва, когато броят компютри е сравнително малък и няма нужда от централизирано съхраняване на файлове и мрежови приложения.


   - ✓ **мрежа тип клиент-сървър**- при тази архитектура персоналните компютри, свързани в мрежата, се обозначават като клиенти или сървъри. Последният представлява компютър, който се занимава с обслужването на работните станции в мрежата. Той осигурява заявките на клиентите за достъп до Интернет и ресурсите**.** Предимствата на мрежата клиент – сървър са:
     - по - добра сигурност- изисква се потребителят да се автентицира с username & password, за да получи право на достъп до мрежата и ресурсите.

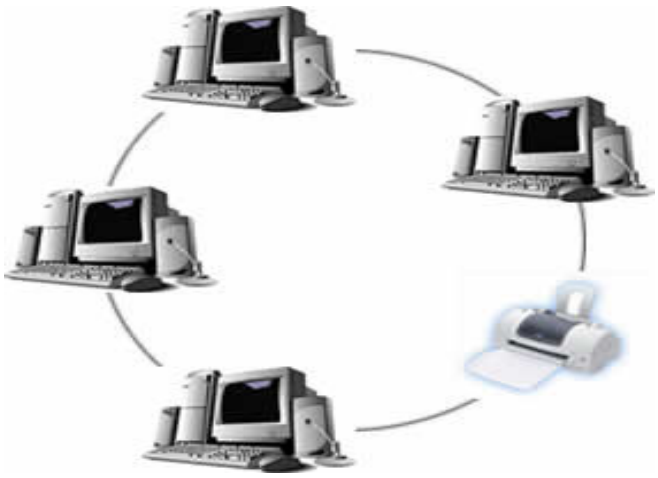
- има централизирано администриране, която я прави по-удобна за по – големи мрежи.


✓ **смесени мрежи** - комбинация от мрежа с равноправен достъп и клиент-сървър. Този подход е предпочитан при изграждането на мрежи за организации.

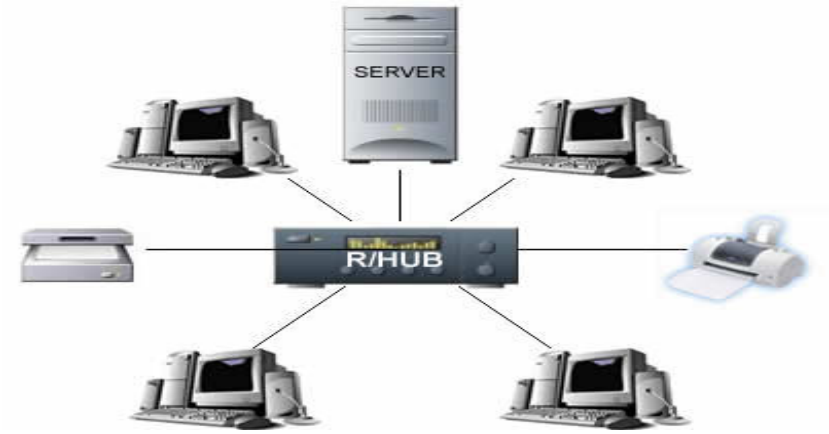
2. Според топологията си биват:

✓ **линейна (последователна)** - всички възли от мрежата се свързват към един кабел, наричан "опорна магистрала". Когато един компютър изпрати съобщение, то отива до всеки възел от мрежата. Всяка мрежова интерфейсна карта проверява неговия хедър, за да определи дали то е адресирано до тази работна станция, в противен случай се игнорира. Сигналът не се регенерира на всяка стъпка, което понякога води до неговото затихване. Ако кабелът се повреди някъде по средата на опорната магистрала, мрежата престава да работи. Изисква се терминиране във всеки край. Шинната топология е много проста и лесна за инсталиране.

- ✓ **кръгова -** при тази топология отделните устройства са свързани в мрежа, в която връзките условно казано имат формата на кръг. По този начин, всеки един възел от мрежата има по две връзки към всеки съседен. По кръговата мрежа сигналът пътува в една посока и се регенерира постоянно. Кръгът е сравнително лесен за отстраняване на неизправности и е прост за инсталиране. Ако се запази непрекъснат, той е надежна топология. При прекъсване или изключване на кабела, се губи мрежовата комуникация. Друг недостатък е трудното добавяне на допълнителни компютри към мрежата.



- ✓ **звездна** - тази топология е най-разпространената в момента и може да се използва и при двата вида мрежи- с равноправен достъп и тип клиент-сървър. Тя се реализира чрез свързването на всички компютри към централен hub. При нея сигналът се предава от мрежова интерфейсна карта на изпращащия компютър към концентратора, който го усилва и изпраща обратно към всички портове. PC-тата поемат съобщението, но само този, за който е адресирано му обръща внимание. Ако връзката между едно от устройствата и R/HUB-а (hub-маршрутизатора) бъде нарушена, това няма да попречи на цялостната работа на мрежата (стига това да не е мрежа тип клиент-сървър и това да е връзката към сървъра). Разбира се, при дефект в концентратора цялата мрежа спира да работи. Съвременните 100 Mbps /1 Gbps мрежи се изграждат по тази топология.




- ✓ **решетъчни мрежи** - в решетъчната мрежа всеки компютър има директна връзка към всяка друга машина като ако пропадне някоя от връзките сигналът може да се поеме от друга.
- ✓ **хибридни мрежи** – работи с множество протоколи, OS-ми или компютърни платформи. Тя комбинира в себе си елементи на две или повече стандартни топологии.

3. В зависимост от архитектурата съществуват два основни вида- **Ethernet или Token Ring**. Тези два метода се различават по управлението на достъп до локалната мрежа и по топологията.

- ✓ **Ethernet (IEEE, стандарт 802.3)** - е най-предпочитаният тип локални мрежи за свързване на различни платформи персонални компютри. Той използва метод на достъп с откриване на носещата информация и разпознаване на конфликтите - CSMA/CD,който е описан в Ethernet и Fast Ethernet стандартите (IEEE 802.3). При него устройствата започват предаване на данни само след откриване на свободен в дадения момент канал за връзка. Ако те двете започнат едновременно да препращат информация, настъпва колизия и спират предаването за различен (случайно избран) интервал от време. При него всички устройства, свързани в мрежата, проверяват дали в момента се изпращат сведения (т.е. откриват носеща честота) преди да започне пренасянето им. Методът е такъв, че няма гарантиран период, за който съобщението ще получи достъп до линията и работните станции трябва да изчакат, докато тя не се освободи. С този тип мрежи се постига максимална скорост на обмен на данните (до 10 Mbps). В днешно време се предлагат два типа технологии, които са реализирани на базата на Ethernet на 100 Mbps: Fast Ethernet 100 Base-T и 100 Any VG-Lan.Съществува и Gigabit Ethernet, който има възможност за работа при скорост, надхвърляща 1 Gbps.

- ✓ **Token Ring-** при него сигнал, наречен "маркер", се предава в кръг и никой компютър не може да предава докато не го получи. Това означава, че за разлика от Ethernet тук не съществува колизия на данни. Той се разполага като топология тип звезда и PC-тата в него са свързани към централен hub, наречен MSAU. Скоростта на този вид LAN е сравнително нисък - от 4 до 16 Mbps и броят на свързаните компютри е ограничен до 256.

Най-важните елементи на локалната мрежа са клиент- персонален компютър, сървър и периферни устройства (принтер, скенер, факс и др.). Клиентът представлява компютър или друго мрежово устройство, отправящо заявки за достъп до мрежови ресурси и услуги. Сървъра обикновенно е мощна машина с бърз процесор и голямо количество памет. Той предлага на потребителите разнообразни Интернет услуги и им осигурява достъп до своите ресурси (данни, софтуер или свързаните към него периферни устройства, като например принтери). Към мрежата могат да се изградят специализирани сървъри, които изпълняват различни функции:

- ✓ **Файлов сървър** – предоставя централизирано съхранение на файлове с данни и осигурява управляем достъп на клиентите до тях.
- ✓ **Принт сървър –** представлява машина, която управлява един или няколко принтера, към които потребителите могат да изпращат по мрежата документи за отпечатване.
- ✓ **Приложен сървър –** това е компютър, на който са инсталирани мрежови приложения. Клиентите могат да изпълняват приложението (например текстообработваща програма) по мрежата, макар то да не е инсталирано на техните локални машини.
- ✓ **Logon сървър –** съхранява база данни за сигурността (security database), която съдържа информация за потребителските акаунти.
- ✓ **Web сървър –** използва се за комуникация в Интернет и работи на базата на http заявки.
- ✓ **Mail сървър –** осигуряват пощенски кутии за събиране на електронна поща, изпратена към потребителите на мрежата.
- ✓ **Терминален сървър –** осигурява многосесийна среда и изпълнява приложните програми, които се използват на клиентските машини.
- ✓ **Клъстерен сървър –** изпълнява софтуер, който позволява множество сървъри да бъдат свързани в клъстери (clusters), представляващи групи от независими компютърни системи.Те

работят заедно като една система, за да осигурят непрекъснат достъп на клиентите до важни приложения и ресурси.

- ✓ **Прокси сървър –** действа като посредник между потребителите с работни станции и Интернет като предоставя услуги с административен контрол и кеширане на web страници.
- ✓ **Факс сървър –** контролира изпращането и получаването на факсове по мрежата.
- ✓ **DNCP сървър –** назначава IP адреси и TCP/IP конфигурационна информация на потребителските компютри.
- ✓ **DNS сървър –** асоциира йерархично структурирани имена на хостове с IP адреси.

Всики възли на мрежата са свързани в обща физическа среда, чийто компоненти са:

- **мрежови интерфейсни карти** – те трябва да бъдат съвместими с архитектурата както на преносната среда, така и с тази на компютъра. Отговарят за управлението на входния и изходния поток от данни между компютрите и мрежата.
- **мрежова преносна среда** – служи за пренасяне на сигналите от едно мрежово устройство към друго, най-често се използва кабел, но съществуват и форми на безжични връзки (например радиовълни, лазерни и инфрачервени лъчи, сателитни връзки и микровълни ). Важно изискване е кабелната система да отговаря на различните характеристики на проектираната мрежова инфраструктура – топология, скорост на предаването и др. Съществуват следните видове компоненти за предаване на данни:

  - ❖ **усукана двойка медни проводници** – съществуват два вида:

    - ✓ *неекраниран кабел с усукана двойка проводници* (Unishilded Twisred Pair-UTP)- използва се една двойка проводници за изпращане на сигнала и друга за приемане. Недостатък при този вид кабел е това, че е твърде податлив на смущения и разстоянията, до което може да бъде използван без концентратор е сто метра.
    - ✓ *екраниран кабел с усукана двойка проводници* (Shieilded Twisred Pair-STP)- състои се от медна оплетка или фолио, обвити около изолираните медни двойки вътре в най-външната опаковка. В сравнение с неекранирания кабел се постига по-висока скорост на предаване на данните и се покриват по-големи разстояния.

- **коаксиален кабел**- сърцевината му е изградена от мед, обвита в изолатор, около който има друг проводник от метално фолио или оплетка. Различаваме два типа - тънък и дебел. Положителните страни на този кабел са, че той е сравнително надежден, има възможност за пренасяне на графични изображения и човешки говор, предава сигнала на големи разстояния. Също така притежава добра шумоустойчивост, висока скорост на пренос на данни и лесно се инсталира. Недостатък при него, е че лесно се повреждa и високата му цена.
- **оптичен кабел** – вместо мед се използват тънки нишки стъкло или пластмаса, по които сигналът се предава под формата на светлинни импулси. Не може да се огъва на повече от 30 градуса и е неподатлив на външни електромагнитни смущения. Развива голямата скорост на предаване на данни (над 1000 Mbit/s) и покрива големи разстояния без нужда от концентратор. Различаваме два вида – едномодов (single mode) многомодов (multi mode).
- **cross-over cable/кросиран или кръстосан кабел /-** този вид кабел се използва при връзването на два компютъра. В кросирания кабел предаващата и приемащата двойка проводници сменят местата си на свързване в конектора (кръстосват се). По този начин предаващата част на единия модул се свързва с приемащата на другия и обратно.
- **устройства за свързване на мрежата:**
  - ✓ *прости конектори* - осигуряват само точка на свързване и не усилват и модифицират сигнала (BNC и RJ конектори, свързващи панели, пасивни хъбове, конектори за оптични влакна).
  - ✓ *сложни конектори* – увеличават сигнала преди да го предадат нататък като го конвертират от един тип преносна среда за друг (конвертори на преносна среда, повторители (repeater), интелегентни хъбове).
- **устройствата за разделяне на сегменти и подмрежи са:**
  - ✓ *мостове ( bridges )* – свързва два мрежови сегмента и извършва филтриране на трафика като се базира на MAC (media access control) адресите в пакетите. Използва таблици, в които пази адресите на получаващите и изпращащите информация компютри, като препраща само бродкастнатите съобщения.
  - ✓ *рутерът (router)*- устройство, което свързва мрежите и избира най-добрия път до дадена дестинация, по който трябва да се изпратят данните. Те проучват фрейма и

определят IP адреса на търсеното устройство. Поддържат таблици, които съдържат мрежови адреси на други машрутизатори и мярка за качество на връзките. Рутерите споделят информацията, съдържаща се в тези таблици и са в състояние да задават нов път и премахнат неустойчивите или непригодните връзки.

- ✓ *мост- маршрутизатори ( bridge-router )* – действат като мост или маршрутизатор в зависимост от използвания мрежов транспортен протокол.
- ✓ *суич ( switch )* – избира път, по който да се изпратят данните и постига добра скорост на пренос.
  a. cut – through switching – препредаването на пакета до местоназначението му започва преди да е пристигнал изцяло. Този метод е по – бърз, но по – несигурен, защото може да се допусне преминаването на "лоши пакети ".
  b. store – and – forward switching – изпраща пакета, чак като го получи напълно и провери неговия интегритет. Той е по – надежден, но по – бавен.

Суичовете се характеризират на базата на OSI слоя, върху който работят:

a. Layer 2 (Datalink) комутиране - изпраща съобщението само на порта, за който то е предназначено. По този начин се намалява общото количество ненужен мрежов трафик, което от своя страна редуцира натоварването.
b. Layer 3 (Network) комутиране -те са специален тип маршрутизатори, които изпълняват и функциите на Layer 2 комутатор.
c. Layer 4 (Transport) комутиране - суичовете от този тип могат да ползват и информация от по- горни слоеве. Важно приложение при тях е осигуряването на ACL (access control list - списък за контрол на достъпа) филтриране за целите на сигурността. Те са способни да управляват разпределението на честотната лента за реализиране на качество на услугата (quality of service – QoS) и балансиране на натоварването.

Кварталният доставчик предоставя Интернет на клиента чрез някакъв вид свързаност, която както споменахме може да се осъществи с помоща на кабелни, сателитни или други безжични съоръжения. Връзката от главния сървър (например: free.evro.net.) до подсървърите се осъществява по лицензирани кабели, които могат да са оптични като по- надеждни. Така се осигурява качествена 100 MB връзка. Понатък преноса на данни преминава през маршрутизитащо устройство наречено рутер, който е

пряко свързан с главния компютър на доставчика. До крайния потребител свързването се продължава пак с оторизирани преносители /кабели/, които кварталния доставик предлага. За по- голяма сигурност те трябва да са например FTP кабели. Важна особеност е, че на определено разстояние (например на всеки 100 метра) между мрежовите компоненти трябва да се включва усилвател на сигнала, за да не се загуби.Това зависи от модела на комутатора, който се използва. Такива устройства са switch-а и hub-а. Превключвателят е по- добрия вариант, защото за разлика от концентратора, не препраща заявките до всички портове, а само до тези, които са ги заявили. От усилвателите тръгва кабел, който се свързва с клиента и по-конкретно към мрежовата карта, намираща се в дънната платка на компютъра чрез букса. В нея стандартно се подреждат осем жички :

- бяло-червена ;
- червена ;
- бяло-зелена ;
- зелена ;
- синя ;
- бяло-синя ;
- бяло-кафява ;
- кафява ;

Трафика на данни се извършва само по четири от тях (първа, втора, трета и шеста), а другите остават свободни . В някои страни функционират и другите, но за момента в България се използват за подмяна на работещите.

Ако се свързват повече компютри се правят кръстосани кабели **(cross-over cable)** от по два- първият е със стандартна букса, а при втория местата на активните и пасивните жички се разменят.

По този начин се изгражда физическата среда на мрежата.

За да се осъществи връзка между всички тези компоненти е необходимо инсталирането на сигурен софтуер. Той включва следните елементи:

- **мрежовите протоколи**- набор от правила, по които мрежата работи. За да се осъществява комуникация между отделните компютри трябва да се използва един и същ протокол. Трите стандартни стека, поддържани от множество популярни операционни системи, са NetBEUI (NetBIOS Extended Interface), IPX/SPX (Internet Packet Exchange/Sequenced Packet Exchange), TCP/IP (Transmission Control Protocol/Internet Protocol)
- ✓ **NetBEUI** е най- простият от трите протоколни стека. Това го прави най- високо производителен по отношение на същинската скорост,

но също така ограничава неговата функционалност. Той не включва средства за логическо адресиране в мреживия слой и не може да се маршрутизира от една мрежа към друга. Въпреки това той работи много добре за комуникацията в единичен LAN и е лесен за инсталиране. Може да се използва съвместно с друг транспортен протокол като TCP/IP като по този начин могат да се комбинират високата му производителност в локалната мрежа и способност за комуникация извън нея с помощта на TCP/IP.

- ✓ **IPX** работи заедно със SPX, за да осигури маршрутизируеми мрежови комуникации. Понякога стека се използва за вътрешни LAN комуникации за повишаване на сигурността. "Външните" компютри, осъществяващи достъп до мрежата от Internet, които работят само с TCP/IP, не могат да достигнат локалните системите, употребяващи само IPX/SPX. IPX работи в мрежовия слой, който доставя пакета до неговото местопредназначение. SPX е протокол от транспортния слой, който гарантира целостта и качеството на преноса на данни и проверява дали същите са получени.
- ✓ **TCP/IP** е комплект от протоколи, работещи в много от слоевете на OSI модела.

**IP** е протокол от мрежовия слой. Той осигурява надеждно доставяне на пакети без установяване на конекция, тоест не гарантира успешното достигане на местоназначението на данните. Основните функции на протокола са логическото адресиране в мрежовия слой на хостовете и доставянето на информация под формата на дейтаграми между тях. Всеки компютър, свързан към мрежа, принтер, маршрутизатор и други мрежови устройства, притежават уникален IP адрес. В зависимост от свойте интерфейси едно устройство може да има няколко IP адреса. Всеки от тях се състои от две части, които служат за идентификация както на мрежата, така и на конкретното устройство. Едната част представлява средата, а другата – хоста. Идентификаторът на мрежата е един, но всеки компютър вътре в нея има различно IP. Когато се извършва предаване на данни идентификационния протокол трябва да определи дали PC-то – местоназначение се намира в същата подмрежа като изпращащия, ако и двата са в една и съща среда съобщението се бродкаства, иначе то се изпраща към адреса на подразбиращият се шлюз ( default gateway ), който всъщност е интерфейс на маршрутизатора.

**TCP** е протокол от транспортния слой. Той изгражда връзка между постовете на отделните портове, за да осигури надеждно предаване на данни между процесите. TCP поддържа тази връзка през целият разговор и я прекратява, когато приключи работа. Протоколът позволява започването на сесии с множество хостове едновременно. Има два главни типа портове - сървърни и клиентски, като всяка услуга или приложение има отделен порт. Клиентските се прилагат динамично по време на работа. TCP

контролира входния поток от данни, като не позволява претоварване на конкретен хост. Той гарантира доставката на пакети, като налага контрол на следване за всеки бит на изпращащата страна и иска потвърждение за получаването му. Всичко това прави TCP много сигурен, но бавен протокол.

**UDP** не създава сесии, тъй като е протокол без установяване на конекции. Той не контролира реда на следване на изпращаните данни и не потвърждава приетите такива. UDP приема, че някой друг протокол от по–горен слой ще контролира дали изпратената информация е достигнала местоназначението си.

**Протоколи от приложния слой :**

*HTTP (Hypertext Transfer Protocol)* – използва се за обмяна на хипертекстови файлове, които могат да включват връзки към други файлове. Той осъществява връзката между браузера на клиента и web сървъра.

*SMTP (Simple Mail Transfer Protocol)* – осигурява обмена на електронна поща (e-mail) между клиента и сървъра.

*NNTP (Network News Transfer Protocol)* – протокол за предаване на новини, използва се от повечето news сървъри и програми за четене на новини.

*FTP (File Transfer Protocol)* – позволява на отдалечен или локален клиент и сървър ефективно да извършват трансфер на файлове или данни.

*Telnet* – дава възможност на потребител, изпълняващ клиентска терминална сесия, да осъществява достъп до отдалечен хост (или Telnet сървър). Не позволява прехвърляне на файлове от една машина на друга, но потребителя може да стартира програми и да преглежда файлове от сървъра.

Към стека се включват и следните общи помощни програми :

**Packet Internet groper** (ping) – използва се за определяне на IP свързването на две системи;

**Address Resolution Protocol** (ARP) и **Reverse ARP** (RARP) - разглежда и модифицира ARP кеша, който съдържа съпоставяния на IP и MAC адреси;

**Netstat** (Windows и UNIX/Linux) и **tpcon** (NetWare) –показва статистики относно мрежовите връзки и протоколи ;

**Nbstat** – извежда информация за връзки и статистики на NetBIOS;

Помощни програми за конфигуриране на IP : **ipconfig**, **winipcfg**, **config** и **ifconfig** – предоставят информация относно TCP/IP конфигурацията (например IP адрес, подмрежова маска, default gateway,MAC адрес и др.) ;

Помощни програми за проследяване на маршрута : **traceroute**, **tracert** и **iptrace** – проследяват маршрута на даден пакет до местоназначението си и идентифицират маршрутизаторите, през които той преминава.

Комуникацията между компонентите на мрежата се извършва през логически точки на свързване - портове. Те се използват от транспортните протоколи TCP и UDP, за да идентифицират специфичното приложение , което изпраща и получава съобщението. Широкоизползваните Интернет приложения имат предварително назначени портове.

- Мрежови операционни системи:

Мрежовата операционна система (network operating system - NOS) позволява на устройствата, изграждащи мрежата, да комуникират помежду си и да споделят ресурси. Не всеки ресурс трябва да бъде споделян с всички потребители. Ето защо една NOS трябва да осигури средства за контролиране на достъпа до файлове, папки, принтери и др. Има два начина за постигане на това:
*Сигурност на ниво споделен ресурс (share-level security)* – използва се в равноправните мрежи, където машините обикновенно работят под Windows95/98 и при споделяне на някой ресурс се задава парола за него. Когато мрежата има много потребители и споделени данни този метод е не ефикасен.
*Сигурност на ниво потребител (user-level security)* – по-лесна за управление от първия метод в средна или голяма мрежа. Всеки клиент има потребителски акаунт(user account), който е защитен с парола. Споделеният ресурс се конфигурира така, че достъпа до него е разрешен само за оторизирани потребители. Когато един клиент се опита да осъществи достъп до него, се проверява списъка за контрол на достъпа, асоцииран с ресурса. Този списък съдържа акаунтите, които имат право да ползват ресурса.
Разглеждат се следните видове акаунти:
*Потребителски* – създават се от мрежовия администратор чрез специален акаунт, който се получава при инсталирането на NOS. Състоят се от потребителско име, парола, условия и ограничения на клиента, информация за сигурност и др. Създаването на потребителски акаунти зависи от използваната мрежова операционна система, но всички притежават административни инструменти, които могат да се използват за добавяне на нов потребител към базата данни за сигурност.
*Групови* - потребителски акаунти се групират за по-лесно управление на NOS.
*Компютърни* - някои мрежови OS изискват всеки компютър , който се логва в мрежата да има акаунт.
Мрежовите операционни системи се занимават с управлението на споделените ресурси (файлове,папки, принтери, приложения, връзки). Начините за администриране зависи от конкретните

OS-ми (например Windows, Linux, UNIX), върху които работи главния компютър на локалната мрежа.

След изграждането на физическото и софтуерното ниво клиентът вече може да има пряк достъп до сървъра, включително Интернет. Преди това администраторът или DNCP сървъра (ако е изграден такъв) задава на потребителя следните постоянни параметри:

- IP address- представлява 32 битово число, задаван на host-овете, използващи TCP/IP протокола.Той се определя от доставчика и се настройва на всеки компютър в мрежовата карта;
- subnet mask - 32 битово число, асоциирано с IP address; всеки бит в подмрежовата маска индицира как да се интерпретира съответния бит в IP address;
- IP address на gateway(доставчика на интернет);

Те се задават, за да може да се идентифицира клиента пред сървъра и като обезпечителна мярка срещу злоупотреби на и към другите потребители.
След конфигуриране, инсталиране и свързване на всички мрежови компоненти, една типична LAN структура работи по следния начин:
На постоянно работещ компютър със статичен IP адрес се стартира програма сървър. Той очаква TCP връзки на предварително определен порт.При стартиране на програмата-клиент се изпълнява следната последователност:

- адресация - определя се IP адреса на сървъра и порта за връзка;
- свързване - клиентът инициира TCP връзка към сървъра;
- обмен - обменят се данните, съобразно спецификата на работата;
- край - TCP връзката се затваря;

При изграждането на локалната мрежа, кварталният доставчик трябва да осигури надеждна защита на данните в нея. Нека разгледаме някои от основните заплахи и методите за справяне с тях :
1. Нарушаване на сигурността - като най-често срещаните опасности са:

- ✓ **компютърни вируси и червеи:**
  - компютърният вирус е програма, която може да се разпространява от един компютър на друг, като копира нейния код в други файлове на системата без съгласието и знанието на потребителя. Най-известните са Melissa, CIH (Чернобил), Michelangelo и ILoveYou.
  - червеят (worm) е форма на злонамерен вирус, който се самореплекира и унищожава файлове на компютъра. Най-често се разпространяват под формата на изпълними файлове,

документи, съдържащи макроси, HTML страници със скриптове и spam-ове.

- ✓ **атаки** – умислено причинени вреди върху всички слоеве. Най – често са свързани с крадене на акаунти и пароли, подслушване на трафик и присвояване на самоличност т.е. представяне за друг при статичните адреси и т.н. Могат да се извършат като някой се закачи за кабела при серийната връзка или се подслушва преносната среда. Най – известните атаки на datalink слоя са: ARP poisoning, Sniffing; на network слоя са: IPID( idle scan ); на transport слоя са: TCP kill, TCP nice, Blind TCP spoofing, SYN flood и DNS spoof на application слоя.
- ✓ **злоупотреба с информацията или съзнателно повреждане на данни и програми-** често срещано компютърно престъпление, което се извършва от вътрешни или външни лица, които имат достъп до системата ;
- ✓ **заден вход**- с този термин се означават недокументираните възможности за използване на програмните системи, които позволяват достъп до информационните ресурси по заобиколен начин.
- ✓ **логически бомби**- модификации на компютърни програми, предизвикващи специфични действия при определени обстоятелства.
- ✓ **троянски кон-** разновидност на компютърен вирус. Представлява набор от програми, които имитират безобидна функция, а в същото време променя данни, унищожава файлове и директории, извършва неправомерни и непочтени действия.
- ✓ **атаки от типа Denial of Service (DoS) ( нюк атаки)-** те не предизвикват срив на компютъра , а са проектирани така, че да прекъснат или попречат на установяване на връзка към мрежата. Работят като наводняват мрежата с непотребни пакети или като симулират мрежов проблем, който кара компютъра да прекрати установената връзка. Някои най-често използвани форми на DoS атаки са :
    - *наводнението на протокола Ping/ICMP(Internet Control Message Protocol)* – състои се в изпращане на голям брой ICMP пакети, които натоварват сървъра.
    - *смърф атаката* – вид ICMP наводнение, което влияе на целия доставчик на услуга или мрежов адаптер. ICMP съобщение се изпраща до бродкастнатия адрес, което принуждава всички компютри от тази мрежа да отговорят.
    - *Ping на смъртта* – хакера изпраща пакет, надхвърлящ броя на октетите, които са разрешени в полета на ехо заявката. Когато

компютъра по местоназначение се опита да сглоби този пакет, той се срива.

- *SYN атаките* – атакуващия чрез SYN- пакет стартира голям брой заявки за установяване на сесия (обикновенно с помощта на "подправен" (спуфнат) IP адрес). Приемащият компютър поставя тези заявки в опашка, където изчакват за завършване на процеса. Чрез попълване на опашката и подържането й постоянно запълнена, атакуващият не допуска установяване на други заявки за връзка.

✓ **мрежови анализатори** – това са специални програми, които четат целия трафик, дешифрират сигналите, слухтят по мрежата с цел да използват получената информация.

✓ **претоварен трафик** – пренатоварването на мрежата води до застрашаване на сигурността поради големия поток от информация и включването на потребители от различни места.

✓ **погрешни команди** –получават се при неумело или неграмотно използване на клавиатурата, което води до известна загуба на данни или грешки в системата. Ето защо, при разработване на системата трябва да се търсят пътища за блокиране на тази опасност.

✓ **хардуерни ( технически ) повреди.**

✓ **пожар и природни бедствия**- за да се избегне в подобни случаи загубата на информация, трябва да се прехвърля предварително върху други носители(дискети, cd-ита).

2. Методи и средства за защита на информацията - най- важен е контролът на достъпа до нея, предотвратяващ възможността за злонамерени действия на други лица или нейното унищожаване. Защитата на данните в една локална мрежа се извършва основно по редица направления:

- **сигурност на електронната поща**- тъй като едно електронно съобщение минава през твърде много сървъри и компютри, където се пази негово копие, то е лесно за прихващане. Затова е добре да се криптира или подпише с цифров подпис, за да се осигури защитата му.
- **одитинг на сигурността и откриване на нарушения**- процес на проследяване на действията на потребителите и системата. Събитията на сигурността се записват също във файл - дневник. Одитингът е пасивна форма за откриване на нарушения, тоест администраторът първо трябва да се усъмни в полученото съобщение и едва тогава да определи точния характер на проблема. При активното откриване се използва софтуер, който непрекъснато сканира мрежата за признаци на нарушения, а някои програми дори предупреждават администратора и изключват връзката на подозрителната секция.

- **криптиране на файлове-** способ за криптиране на данни, съхранявани на диска на компютъра, които могат да бъдат разглеждани чрез използване на правилен ключ.

  ***Протокол IP security*** *(IPsec)*- осигурява сигурност при преноса на криптирани данни.

  ***Secure Sockets Layer*** *(SSL)*- използва се от повечето интернет сървъри и web сайтове за осигуряване на защита на данните. Предлага кодиране на информацията, автентичност на сървъра, цялостност на съобщенията и възможност за автентикация на клиента в TCP/IP връзка, както е и съвместим е със защитни стени (firewalls) и тунелни връзки.

  ***SSH*** *( Secure Shell )* замества telnet и е много по – сигурен. Осигурява се криптиран канал за свързване между компютри в мрежата, като позволява да се извършват процеси включително и прехвърляне на файлове.Предлага силна host-to-host и user аутентикация, както и сигурно криптирана комуникация през Интернет.SSHv2 е много по – сигурна и ефикасна версия от SSH, която съдържа SFTP. Той изпълнява фуккциите на FTP протокола, но е SSHv2 криптиран.
- защитата срещу загуби на данни и възстановяването им- включва **аварийно захранване**, **архивиране на данните**, **отказоустойчивост** (възможността на дадена система да се възстановява след срив) при дисковете, **отказоустойчивост** на ниво сървъри (клъстериране).
- **защита от атаки** - при локалните мрежи е препоръчителна употребата на managed switch, а не на hub. Комутаторът изпраща получените пакети само до порта, на който е свързан техния получател, знае правилния MAC и IP адреси, а при концентратора се препраща до всички. Реална защита се осигурява и чрез криптиране на трафика (VPN, SSL, PGP) и протоколите.Съществува широк набор от инструменти за разпознаване и предотвратяване на атаките. Някои от тях са: arp, ping –r, traceroute, egress филтриране, syncookies, смяна на операционната система и на TCP/IP имплементацията, така че да не са лесно предвидими ISN номерата.
- **защитни стени и проксита**:

  Защитните стени (firewalls) и прокситата могат да бъдат използвани за създаване на бариера между локалната мрежа и връзката към външния свят. Тази област може да бъде инсталирана в нейна собствена подмрежа и понякога се означава като демитализирана зона (DMZ) или прикрита подмрежа (screened subnet).

  Защитната стена може да бъде базирана на хардуер или софтуер. Осигурява средства за филтриране на входящите и

изходящите пакети и определя дали да разрешава преминаването им до адреса на местоназначение. Тя обикновенно се намира на шлюза (gateway) на мрежата, който представлява точката, в която мрежата се свързва с друга. Firewalls извършват три основни типа филтрирания:

- на пакети- на базата на информацията във IP, TCP/UDP, ICMP хедърите като при този процес могат да се блокират конкретни IP адреси или номера на портове;
- на вериги- базирано на текущата връзка- ако даден пакет не е част от установена връзка той няма да бъде пропуснат през защитната стена;
- на приложения- в зависимост от протоколите използвани за конкретни IP приложения;

Хардуерно базираните защитни стени понякога се наричат "черни кутии". Те представляват специализирани компютри, които изпълняват собствени нестандартни операционни системи. Функционират само като защитна стена, поради което са по-стабилни и по- бързи.

Прокси сървърите работят като посредници в мрежата, изпълняващи сходни със защитните стени функции. Компютрите във вътрешната мрежа комуникират с проксито, което след това препредава тяхната заявка към главния сървър. Те осигуряват следните услуги:

- реверсно прокси – позволява даден прокси сървър да пренасочва външни http заявки само към една специално предназначена за това машина. Това дава сигурност на достъпа до вътрешен web- сървър без излагането му пред външната мрежа.
- реверсно хостване – позволява на прокси сървъра да пренасочва http заявки към повече от един web- сървъри, като ги асоциира към един логически адрес.

Прокситата осигуряват също кеширане на web- страници за подобряване производителността на връзката.

Кварталният доставчик предлага на своите потребители основните усуги :

**World Wide Web**

Информационната система **World Wide Web (www)** е една от най-популярните услуги, достъпни чрез Internet.Тя е базирана на хипертекст (hypertext) технология и работи върху HTTP протокола от TCP/IP стека . Една дума в хипертекст документ може да служи като указател (hyperlink)

към друг документ, в който се намира информация свързана с думата-указател. В съвременните Web документи свободно се комбинират хипервръзки, аудио и видео фрагменти, графични икони и изображения, което ги превръща в хипермедийни. **WWW** се състои от множество информационни сървъри (Web servers), които са постоянно достъпни по мрежата и непрекъснато се променят. Наблюдаваните промени са насочени към съдържанието на информацията, начина на нейното представяне и структуриране. За осъществяване на достъп до **WWW** е необходима връзка с мрежата и браузер, който интерпретира и визуализира информацията. Документите са хипермедийни и съдържат текст с команди за структуриране. По този начин **WWW** клиентът извършва форматиране с цел получаване на най-добрите възможни визуални резултати върху екрана на компютъра.

**E-MAIL** (Електронна поща)

Това е една от най- старите услуги в Интернет и все още една от най-извесните. Използва се за изпращане на текстови съобщения от един потребител към друг. С развитието си вече може да се изпращат не само текстови съобщения, но и HTML страници, както и файлове с програми и изображения. Базира се на протоколите IMAP, POP3 и SMTP. SMTP се използва за изпращане на съобщенията, а POP3 за тяхното изтегляне от пощенския сървър.

**FTP** (Трансфер на данни)

Тази услуга се използва за прехвърляне на файлове между сървъра и потребители или обратно. Тук могат да се задават нива на достъп на отделните потребители, които се идентифицират с потребителско име и парола. Услугата се базира на протокола **FTP**. Той се основава на даване на команди на сървъра от клиента и тяхното изпълнение. Командите могат да бъдат за получаване или изпращане на файл, разглеждане на директории и др. Командите се изпълняват от ftp сървъра и информацията се подава към потребителя. Порта по подразбиране на протокола е 21.

**TELNET** (Отдалечено администриране)

Отдалечена сесия (отдалечен терминал) е услуга, при която потребител може да се свърже с друг компютър от мрежата и да стартира процес в него. От този момент до края на връзката, всеки натиснат клавиш се изпраща на отдалечената машина и се интерпретира от нея. Обслужването се извършва от локалната машина, но Telnet програмата прави невидим вашия компютър. Първоначално връзката се осъществява чрез разпознаване на потребителя с user name и парола. Telnet приложенията за

микрокомпютри обикновено са придружени с терминални емулатори за определен тип терминали, подходящи за работа в среда UNIX или VMS.

**USENET**

Това е самостоятелна система, превърнала се в среда за дискусии и обмен на информация между хора с общи интереси, разделени по групи- "newsgroups". Обменът на новини по Интернет се обслужва от услугата NEWS, която се реализира чрез NNTP протокол.

**IRC**

IRC е относително нова услуга в Интернет. Базира се на протокол, който дава възможност на множество потребители да осъществяват директна връзка помежду си във форум (channels) или по единично (Peer-to-peer). При работа в общ канал всеки участник в конференцията се свързва първо към определен сървър, където се идентифицира и при наличие на други участници може да вземе участие в тяхната дискусия. Работата по единично свързва две машини, имащи достъп до Интернет мрежата по техните IP адреси. В този случай дискусия няма, но може да се проведе разговор между двамата участника.

По принцип обменът на информация може да се извършва с текст, звук или видео.

**DNS** (Domain Name System)

Това е услугата, която прави съпоставка между IP и URL адреси. Компютрите в мрежата обработват много по - бързо и лесно IP адреса, и затова ползват него. Но за потребителят е напълно невъзможно да запомни толкова много несвързани числа и затова се е наложило въвеждането на URL адресите, които са разбираеми за хората. DNS е услугата, която преобразува име на host в IP адрес и обратно. Name домайните са TLD – top level domain (това са разширенията .com, net, org, edu, mil, arpa, info, biz, aero,name, museum...) и ccTLD: country-code top-level domains, и CLD – second level domain (всичко преди .com, .org, .bg ). Те образуват граф, по който се извършва търсенето. На пример ако трябва да превърнем host адресът fmi.uni-sofia.bg към IP адрес: заявката се изпраща до DNS сървъра и се приема от stub resolver-a. После той я препраща към recursing resolving cache**,** който, ако знае отговора го дава, ако не започва да търси. Тръгва от **root servers,** проследява **delegation chain,** стига до **записа**, който клиентът му е поискал, и **cache-**ва информацията за следващо ползване. Така се преобразува host адрес към IP адрес. От IP към host преобразуването се извършва по същия начин.

DNS може да се използва и при изпращането на поща – MX (mail exchange). Тази услуга може да се използва за запитване на това кой сървър приема заявки за даден домейн.
За да се регистрира домейн трябва да се извърши следното:

- В базата данни за домейните се записва, името на собственика, съответните лица за контакт, срок на годност, и фирмата, извършила регистрацията;
- В базата данни на DNS сървърите, отговарящи за областите "com", "net" и "org", се записват тези, които отговарят за този домейн;

Тъй като тези бази данни се обновяват веднъж на 24 часа, домейнът става валиден най - рано на следващия ден след регистрацията.

**VPN** (Virtual Private Network)

VPN технологията използва Интернет като канал, през който може да установи сигурна връзка между отдалечен клиент и частна локална мрежа. Тя свързва два компютъра като гарантира сигурен тунел през обществена мрежа (най – често Интернет). Той позволява да се създаде логическа мрежа, която е независима от местоположението и възможността за установяване на директна физическа връзка. Данните, които минават през тунела са криптирани. Тунелът поддържа и аутентикация. При тунелирането оригиналният пакет се скрива във външния. В неговия хедър се задава адресът на крайната точка на тунела. Адресът на местоназначението се намира в хедъра на вътрешния пакет. Тунелите могат да са в различни слоеве на OSI модела. При изграждането им във втория слой се използват протолите Point – to – Point Tunneling Protocol (PPTP) и Layer 2 Forwarding (L2F). Последният не зависи от IP и може да бъде използван за тунелиране по ATM и Frame Relay. За разлика от PPTP, L2F може да поддържа повече от една връзка. Тунели могат да бъдат създавани и в мрежовия слой . По този начин се осигуряват IP базирани виртуални връзки. Те работят, чрез изпращане на IP пакети - капсулирани във вътрешността на определени протоколни обвивки. Използват се IPsec и други меотди за аутентикация и криптиране. Тунел може да се изгради и чрез L2TP.
**IPsec** може да капсулира само IP пакети, докато **L2PT** работи с пакети на Internet Packet Exchange(IPX) и други протоколи. За сметка на това някои шлвюзове не поддържат VPN мрежи базирани на L2TP.

**ISDN** (Integrated Services Digital Network)

Цифровата мрежа с интеграция на услугите ISDN интегрира всички видове телекомуникационни услуги - телефония (говор), факс, обмяна на данни и видеоизображения, като осъществява цифрова свързаност през цялата

мрежа между потребителите. ISDN осигурява една връзка за всички услуги и само един интерфейс за връзка с далекосъобщителната среда.

Кварталният Интернет доставчик трябва да извършва поддръжка и администриране на локалната мрежа за улеснение на своите клиенти и защита от неправомерни действия.
Поддръжката включва някои от следните услуги:

- Отстраняване на хардуерни проблеми по сървъри, активни мрежови устройства и работни станции;
- Отстраняване на софтуерни проблеми;
- Инсталиране, upgrade и подмяна на мрежови компоненти;
- Настройки и мениджмънт на мрежата;
- Мониторинг на мрежата;
- и др.

Администрирането се свързва със създаване на правила за ефективната работа на мрежата.Те трябва да са написани съобразно общоприетите Accetable Use Policy (AUP) закони.Нека разгледаме някои примерни условия за работа на една локална мрежа:

- Включването на потребител се извършва от представители на кварталния Интернет доставчик до 10 дни след заявката.
- При приемането на нов абонат към мрежата, същият се задължава да подпише договор за услугите, които ще ползва и да спазва правилата в него.При нарушаване на контракта той бива безпрецедентно изключван от мрежата.
- На потребителите на мрежата се забраняват:
    - Действия нарушаващи или заплашващи да нарушат нормалната работа на останалите потребителите на локалната мрежа и/или глобалната световна мрежа - Интернет.
    - Оптити за неауторизирани прониквания независимо от крайната цел.
    - Предоставяне или прехвърляне на услуги на доставчика на други потребители или трети лица, освен в случаите когато има друго предварително споразумение за това.
    - Смяна на настройките на операционната система за работа в локалната мрежа и интернет - IP Address, gateway (шлюз), и др., освен в случаите, когато това се изисква от мрежовия администратор.

- Предоставянето на услуги с комерсиална цел използващи ресурсите мрежата, освен в случаите когато предварително е договорено друго.
- Действия нарушаващи или заплашващи да нарушат действащ закон.
- При всяко едно от горепосочените нарушения, кварталният Интернет доставчик има правото да наложи глоба и/или да преустанови връзката на нарушителя (групата нарушители).

- На абонатите на мрежата се препоръчва:

  - Редовно да проверяват компютрите си за вируси, като постоянно актуализират (update-ват) антивирусния си софтуер. За целта трябва да имат инсталирана антивирусна програма.
  - Редовно да update-ват операционната си система.
  - Да не отварят писма с неясен произход, да не се свалят изпълними файлове освен от напълно сигурни източници, да не се приемат изпратени по ICQ или IRC файлове дори при най-малко съмнение относно тяхното съдържание.

- При напускане на нов абонат, същият трябва да уведоми Интернет доставчика за да се преустанови връзката му към мрежата.
- И други

## Основни компоненти на сигурен квартален Интернет доставчик

**Тип мрежа:** Ethernet ; клиент/сървър ; звездна топология
**Мрежов софтуер :** използват се протоколите от TCP/IP стека за осъществяване на връзката; сървърна операционна система – Linux ;
**Мрежов хардуер:** сървъри – файлов, принт, приложен, logon, web, mail, прокси; router, switch, FTP окабеляване между работните станции;
**Защита:** Firewall, Proxy – за контролиране достъпа на клиентите до Интернет;
PGP за криптиране на преноса на данни; протоколи – SSHv2 вместо FTP, SMTP – за изходящата поща, POP3 криптиран със SSL за входящата поща;
**Услуги :** WWW, E-Mail, FTP, VPN , IRC ;