УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

КАТЕДРА ” ИНФОРМАЦИОННИ СИСТЕМИ И ТЕХНОЛОГИИ ”
МАГИСТЪРСКА ПРОГРАМА
” ИНФОРМАЦИОННИ ТЕХНОЛОГИИ ”

МАГИСТЪРСКА ТЕЗА

на тема:

ПРОЕКТИРАНЕ НА ЛОКАЛНА КОМПЮТЪРНА МРЕЖА

Дипломант:
Васил Стоянов
задочно обучение
Ф.№ 500-ИМЗ

Научен ръководител:.....
(проф. дн Иван Гарванов)

София
2018

РЕЗЮМЕ

Стоянов, В. Проектиране на локална компютърна мрежа. Научен ръководител проф. И. Гарванов. С. 2018. Катедра «Информационни системи и технологии», Магистърска програма «Информационни технологии» УНИБИТ. Брой на страници - 124.; Брой на цитирани и използвани източници - 39, Брой илюстрации - 35.

Целта на тази магистърска теза е проектиране на локална компютърна мрежа за голямо предприятие която да позволи изграждането на модерна информационна инфраструктура, осигуряваща всички необходими ресурси за нормалната работа на голям брой потребители. Проекта включва както хардуерно така и софтуерното осигуряване.

За изпълнението на така поставената цел произтичат следните задачи:

- Да се разгледат основите за изграждането на компютърните мрежи.
- Да се проучат компонентите за създаване на мрежа.
- Да се запознаем с видовете LAN Мрежи
- Да се разгледа същността на компютърната мрежа.
- Да се разгледат мрежовите протоколи за предаване и защита на данни, мрежовата топология, приложима физически и логически в конкретния случай.
- Да се избере преносна среда, която ще бъде най-удобна и подходяща.
- Да се намери подходящо мрежово пасивно оборудване.
- Да се намери подходящо мрежово активно оборудване.
- Да се намери подходящо сървърно активно оборудване.

Ключови думи: локална компютърна мрежа, оптични кабели, IP адресиране, активно мрежово оборудване;

Съдържание

УВОД

Телекомуникацията е една от най-бързо развиващите се предметни области през последните 25 години. Нарасналите потребности от достъп до изчислителните ресурси и нуждата от усъвършенстване на информационното обслужване доведоха до необходимостта от свързване на различни компютри и терминали помежду си и до създаването на т.нар. компютърни мрежи. Изградените комуникационни мрежи до деветдесетте години на миналото столетие претърпяха кардинални промени и развитие. Благодарение на това развитие се създаде възможност за високоскоростно предаване на големи обеми от данни на големи разстояния. Това предаване на данни може да се осъществи по различни преносни среди (безжична, кабелна) и чрез различни преносни методи (цифрови или аналогови). Милиони компютри са включени в тази и други глобални компютърни мрежи, обхващащи всички континенти на Земята и близкия космос. Създадена беше възможност за бърза информационна връзка между жителите на планетата. (1)

Едно от най великите достижения на миналия век е глобалната компютърна мрежа Интернет, който вече се е превърнал в дума от ежедневието в много държави и е неизменна част от живота на бизнес света. След включването на милионни хора в уеб пространството (World Wide Web), компютърните мрежи вече са неразделна част и във всяко домакинство. Закупуването и инсталирането във всеки дом на безжичен или кабелен рутер вече е не по-сложно от работата с домашните смарт (умни) устройства като телевизор, мобилен телефон, таблет и др. (фиг.1). Локалните мрежи се различават от глобалните мрежи по ограниченото разстояние между абонатите си и високата скорост на предаваната информация. Локалната мрежа е високоскоростна комуникационна връзка между устройства за обработване на данни, разположени в географски ограничен район. Локалните мрежи могат да свързват персонални компютри, терминали, мини компютри и големи компютри, принтери и други електронни устройства.

Свързването на компютри, така че да образуват локални мрежи, е обичайна практика дори и при малки инсталации и поради това често връзките на дълги разстояния се правят посредством линиите за пренос, предоставяни от телекомуникационните фирми. Бързото разширяване на конгломерата от мрежи по целият свят, обаче, направи свързването към световното село най-естественото нещо за всеки с достъп до компютър.

Мрежите създават условия за комуникация и разпределяне на технически и програми ресурси между разположени на различни места компютри и потребители, те са съвкупност от хардуерни и софтуерни компоненти. От тази гледна точка мрежа е всичко, позволяващо на два или повече компютъра да комуникират помежду си и/или с други устройства така, че всеки, който желае (и има съответното оборудване), да може да я из-ползва за обмен на информация, печат, обща работа и директна комуникация с различна цел. Локалните мрежи могат да бъдат с различен обхват, територия, топология или използвани технологии.

Основната тенденция в развитието на компютърните мрежи обаче е свързана по-скоро с възможността за съвместно и разпределено ползване на информация, за малки фирми обхвата на такава мрежа е обикновено един офис, етаж или сграда, а за големи организации необходимостта от съвместно ползване на информацията се разпростира между множество офиси в различни сгради, градове и държави.

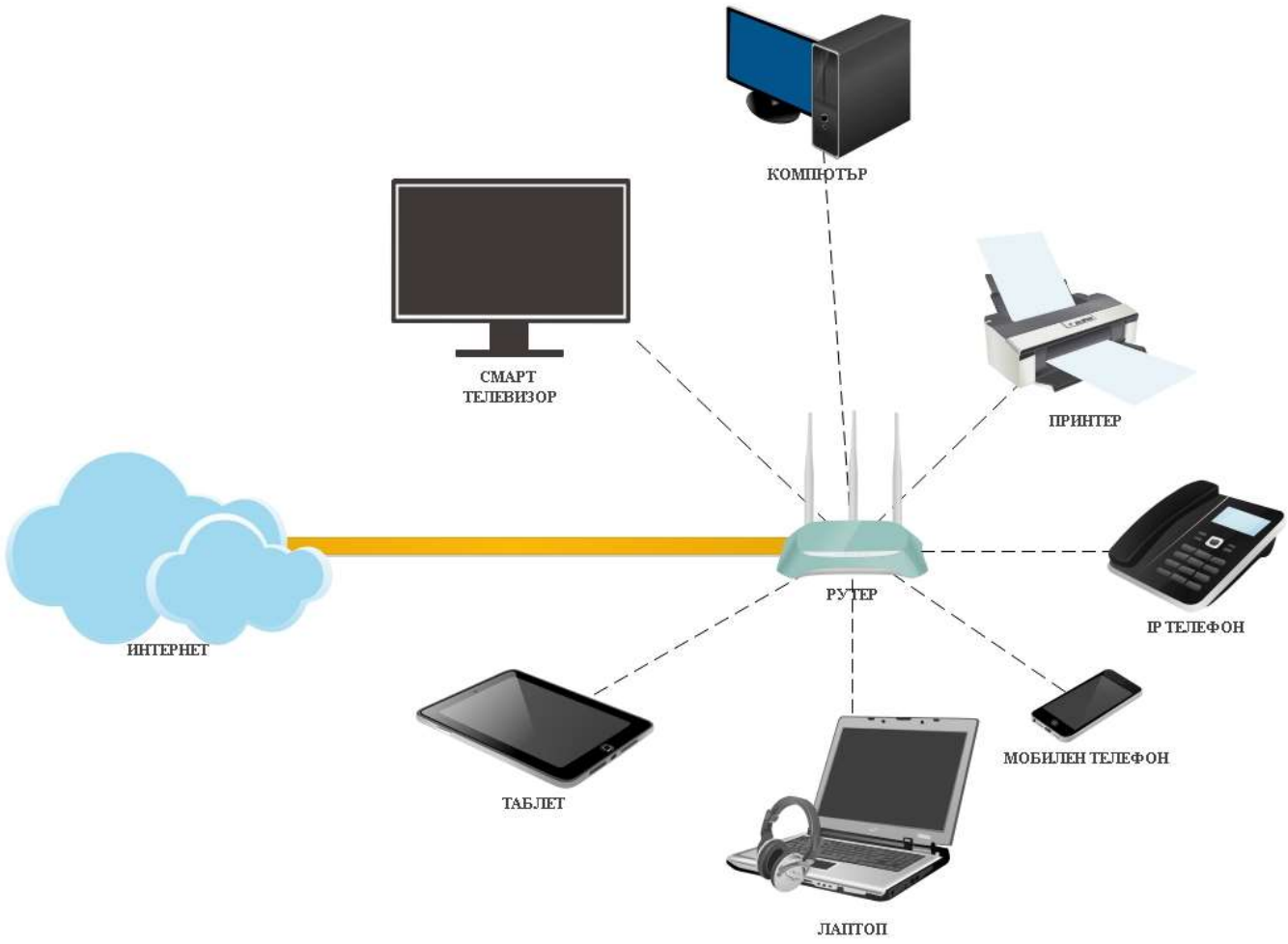
При проектирането и изграждането на компютърна мрежа е необходимо детайлно запознаване с мрежови топологии, хардуерното оборудване, кабелите, архитектурата на мрежата, сигурността и др. Едновременно с това мрежата трябва да съчетава в себе си надеждност, работоспособност, перспектива за разширение и да е лесна за управление и поддръжка. Изграждането на една локална мрежа от финансова гледна точка може да се окаже значителен разход за една компания, затова трябва да се

търси баланс между възможните за отделяне финансови средства и качеството, функционалността и сигурността на мрежата.

ГЛАВА ПЪРВА I. Същност на компютърните мрежи

1.1. Компютърна мрежа

Компютърна мрежа наричаме съвкупност от крайни устройства (компютри, таблети, смартфони, принтери, камери, и др.), специализирани мрежови устройства и средствата за тяхното свързване, изградена с цел обмен на информация, споделяне на ресурси и обща работа. (фиг.1)



фиг.1 – Домашна компютърна мрежа

Просто казано това са две или повече устройства, свързани с цел общо използване на информацията, ресурси или и двете. Връзката може да бъде чрез кабел или може да бъде безжична връзка, която използва радиовълни, лазерна или инфрачервена технология, или сателитно предаване. Споделената обща информация и ресурси могат да бъдат файлове с данни, приложни програми, принтери, модеми, скенери или други хардуерни устройства. 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 е обикновена, тя се оказа огромно достижение в сферата на комуникациите.

1.1.1. Кратка история на компютърните мрежи

През 60 години правителството на Съединените щати се заинтересува от разработването на компютърна мрежа, която би позволила на военните системи и на системите на главните образователни институции да комуникират едни с други. Тъй като това става в разгара на Студената война, те искат мрежата да притежава устойчивост, надеждност и достатъчен резерв, така че да може да оцелее при възможна ядрена война. Изследователите от Масачузетския технологичен институт, института RAND и Националната физична лаборатория във Великобритания изобретяват нова технология, наречена комутиране на пакети (packet switching), които при периодични пикови предавания работи по добре, отколкото традиционните технологии с комутиране на вериги. Тяхната работа полага основата на комуникационните технологии, използвани в днешният Интернет. Терминът комутиране на вериги и комутиране на пакети звучат близко, но имат различно значение. (1)

Обществената телефонна система, означавана понякога с POTS, представлява комуникационна мрежа с комутиране на вериги. Когато провеждате телефонен разговор в този тип мрежа, за цялото време на този

разговор се използва само една физическа пътека от вашият телефон до телефона, които сте избрали. Тази пътека или верига се поддържа изключително за ваше ползване до момента, до момента когато прекъснете връзката, поставяйки телефонната слушалка обратно на мястото и. При мрежа с комутиране на пакети не се изгражда специална пътека или верига. Комутирането на пакети понякога се означава като технология без установяване на конекции, поради липса на специално изградена пътека. Началото на първата компютърна мрежа с комутиране на пакети е поставено в края на 60 години под покровителството на Министерството на отбраната на САЩ. Тя е наречена ARPnet. Първият възел или точка на свързване, към ARPnet е инсталиран в Калифорнийският университет в Лос Анджелис през 1969 г. Само за три години мрежата се разпростира през целите Съединени щати, а две години след това достига до Европа.

С нарастването на мрежата тя бива разделена на две части. Военните наричат своята част от интернет мрежата Milnet, а ARPnet продължава да бъде използвана за описание на частта от мрежата, която свързва изследователските и университетските сайтове. През 80 години ARPnet е заменена от мрежата Defense Data Network и NSFNet. В последствие тази WAN мрежа се разраства в това, което днес наричаме Интернет.

Изграждането на компютърните мрежи не започва от такъв голям мащаб като проекта ARPnet, т.е. локалните мрежи се появяват преди WAN. С поевтиняването на компютрите и с увеличаването на тяхната мощност, търговските организации от всички мащаби започнаха да ги използват все по масово. Първите машини можеха да се използват само за ограничени видове обработка на данни, но с процъфтяването на разработката на софтуер новите програми позволиха на потребителите да правят повече от простото сортиране и събиране на данни. (1)

Използването на мейнфрейм компютри вършеше добра работа в много отношения, но те имаха няколко минуса в сравнение с по-малките

компютри. Недостатък беше тяхната висока цена, големите мейнфрейм системи струваха много повече от така наречените “персонални” компютри, проектирани така, че да бъдат поставени на бюрото и да функционират самостоятелно. Друг недостатък на мейнфрейм компютрите беше концепцията за единствена точка на отказ. При работата с мейнфрейм компютър, ако компютъра бъде изключен, той е изключен за всички. От друга страна, използването на отделни персонални компютри разрешава този проблем. Персоналните компютри представляват компютри, разработени като напълно функционални единици, които изпълняваха програми и извършваха работни задания напълно самостоятелно. Те осигуряваха известна отказоустойчивост – способността на системата да продължава да функционира и да осигурява цялост на данните при възникване на повреди. Ако компютърът на един служител прекъсне работа, той не влияе на възможността на останалите служители, които имат собствени персонални компютри да продължат работата. (1)

Тези фактори допринесоха за нарастване популярността на персоналните компютри като решение за малки, средни и големи търговски организации. Но след като всеки се сдоби с отделен компютър на бюрото си, компаниите се изправиха пред дилема как работниците да използват съвместно информацията. Решението беше изграждането компютърна мрежа и работата с нея.

1.1.2. Възможности и области на приложение на локалните компютърни мрежи

Локалните мрежи могат да свързват не само компютри, а и видео, телефонни и алармени системи, машини с цифрово-програмно управление и всевъзможни устройства, които изискват високоскоростен обмен на данни. Няколко локални мрежи могат да бъдат свързани чрез локални или отдалечени връзки, за да образуват по-големи обединени мрежи.

Основните области на приложение на локалните мрежи са автоматизация на :

- административна дейност;
- производство;
- финансовите и банковите системи;
- търговия;
- науката и образованието;
- съвместното използване на програми, принтери, модеми;
- изпращането на съобщения чрез електронна поща.

При внедряването на локалните мрежи се поставят две главни цели:

- да се осигури стандартен начин за комуникация между цифрово оборудване, изработено от различни производители;
- да се даде възможност за стандартна комуникация между различни мрежи чрез междумрежови адаптери

Мрежите предлагат много богата гама от възможности на потребителите и разработчиците на приложен софтуер. По важните от тях са:

- Улеснена работа. С локалните мрежи се работи лесно, като могат да се избират менюта с прозорци. Използването на мрежовите услуги е прозрачно за потребителите. Сложните параметри, както и възможностите на функциите се извеждат на екрана готови за избор. Функциите на мрежата могат да се изпълняват от менюто, от командния ред на дисковата операционна система или по време на изпълнението на приложната програма.
- Съвместимост с многопотребителски приложения.

Софтуерът на локалните мрежи е прозрачен и съвместим с операционната система и позволява изпълняването на различно многопотребителско

приложно програмно осигуряване, което е създадено за работа с мрежи и използва стандартното за операционна система заключване на файлове и записи.

- Висока ефективност. Локалната мрежа е високо скоростна. Тя използва буфери в паметта, с което увеличава скоростта на операциите с мрежовите ресурси. Оперативната памет може да се използва за симулиране на реално дисково устройство, за да се елиминират максимално входно/изходните операции. По този начин ефективността на мрежата се подобрява съществено, тъй като данните се извличат директно от паметта на компютъра, което е много по-бързо отколкото от диска.

- Компактност на програмите. Локалната мрежа е компактна. Потребителската част от софтуера на мрежата използва много малка част от паметта на компютъра и по този начин се осигурява необходимата оперативна памет за изпълнение на приложно програмно осигуряване. Компактността на програмите не се отразява върху производителността и ефективността на мрежата. Възможните системни параметри могат да бъдат настройвани в зависимост от особеностите на конкретното приложение. (1)

- Гъвкавост при поделяне на общите ресурси. Поделянето на ресурсите е многостранно и гъвкаво. Когато се работи с конфигурация с разпределено управление, без централна управляваща станция, всеки потребител в мрежата може да използва нейните ресурси съвместно и безконфликтно с всички останали потребители.

- Гарантирана цялостност и защита на данните. Мрежовите операционни системи прилагат стандарта на дисковите операционни системи за мрежа и архитектура за управление на файловете, които създават многопотребителска среда. Ресурсите могат да се ползват едновременно от няколко потребители, без да се застрашава целостта на данните. Мрежата осигурява необходимата сигурност и защита на потребителската информация.

- Осигуряване на достъп до ресурсите. Използването на общите ресурси може да бъде разрешено за определени потребители на мрежата с помощта на имена и пароли. Като използва правата си за достъп, потребителят може да ограничава ползването на своите ресурси за останалите потребители, като им разрешава да модифицират неговите ресурси или само да ги четат.

- Комуникационни функции. Мрежата осигурява изпращането и получаването на съобщения и воденето на диалог с останалите потребители на мрежата. По всяко време може да бъде изпратено съобщение до един или до всички компютри в мрежата. Воденето на диалог се извършва в реално време.

Съществуват и следните допълнителни възможности за увеличаване на списъка от услуги, които могат да се изберат за съвместна работа с локалната мрежа:

- Електронна поща. Електронната поща е средство, с помощта на което може да се осъществява, голямо по обем предаване на документи в мрежата между потребителите. Получената поща (файлове) се съхраняват в пощенска кутия, реализирана в сървъра на електронната поща, независимо от работната станция на клиента.

- Отдалечено първоначално зареждане. С помощта на отдалеченото първоначално зареждане компютър без диск може да направи първоначално зареждане на операционна система от всеки компютър в мрежата, който има дисково устройство. Софтуерът на локалните мрежи и всеки друг приложен програмен продукт може да се зареди отдалечено в компютър без диск от диска на друг компютър. Отдалеченото първоначално зареждане се предлага заедно с инсталационна програма за първоначално зареждане и ROM чип за първоначално зареждане, който се инсталира на мрежова интерфейсна платка.

- Асинхронна комуникационна връзка. Асинхронната комуникационна система дава възможност един или няколко модема или асинхронни комуникационни устройства, които са свързани с един компютър, да се използват колективно от други компютри в мрежата. Осигурява се и

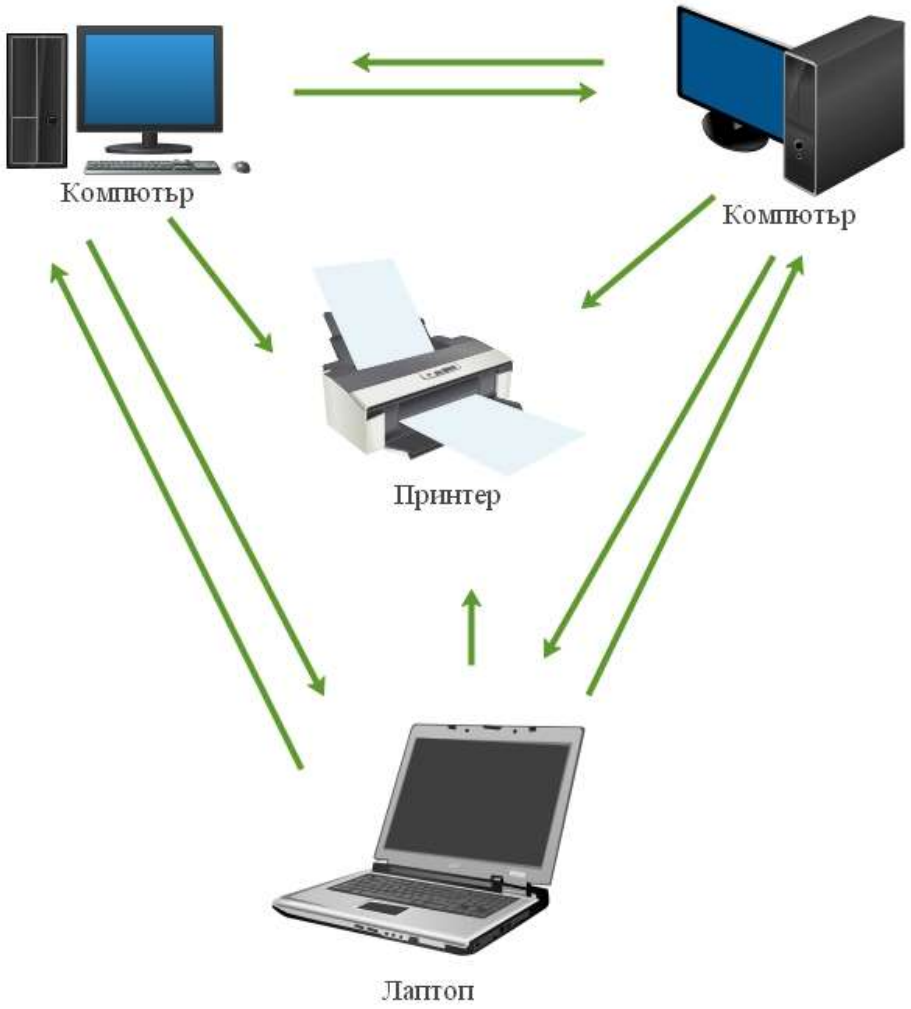
терминална емулационна функция, която позволява да се комуникира с друг компютър, който подържа портове RS – 232. (2)

- Свързване на две и повече мрежи. С помощта на специални хардуерни устройства и програмни продукти компютрите от една мрежа могат да комуникират и да поделят ресурси с компютрите от друга локална или глобална мрежа. (2)

1.1.3. Категоризация на мрежите според метода на администриране

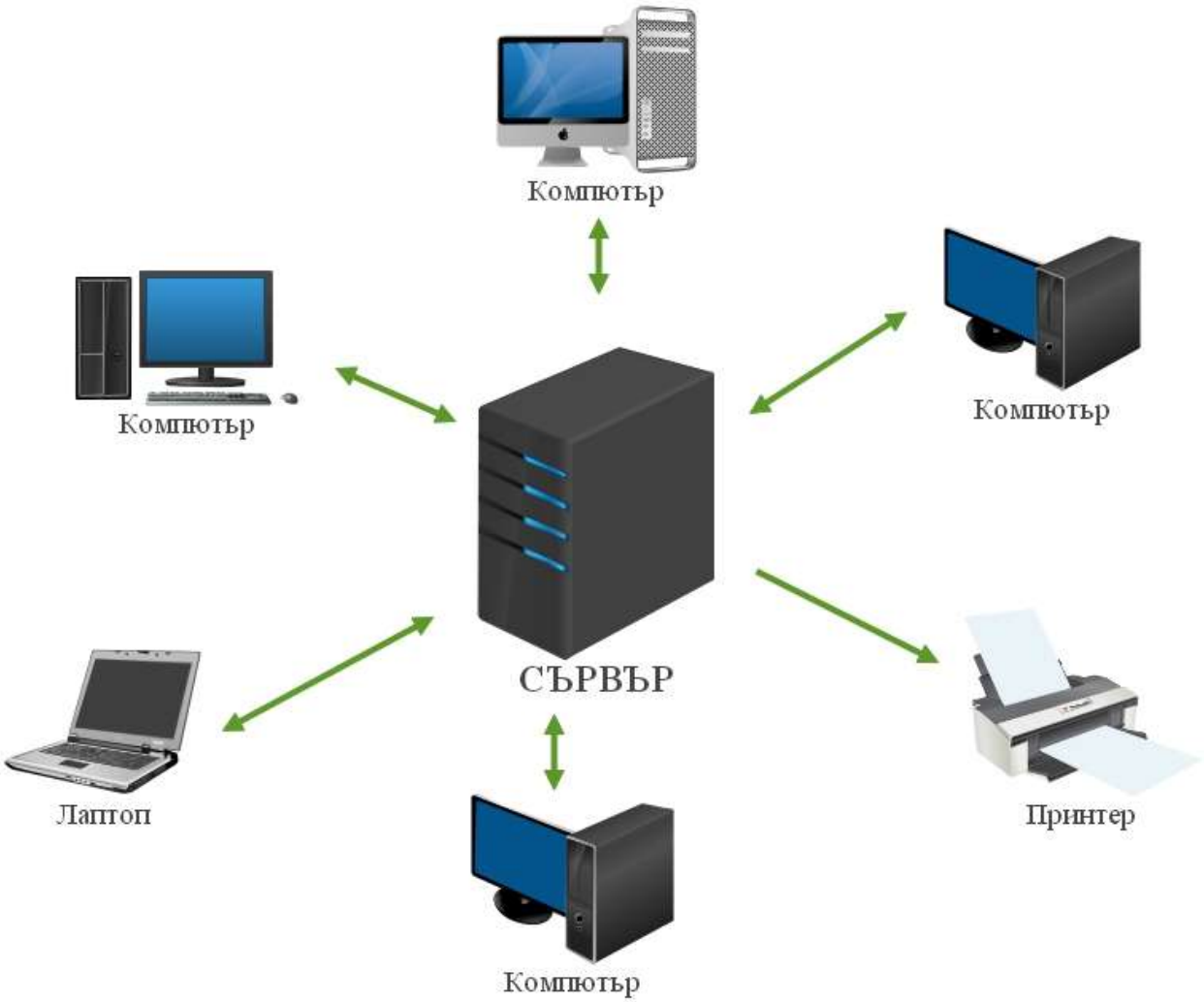
От гледна точка на администрирането, една мрежа може да бъде организирана по един от следните три начина:

- Локални мрежи с равноправен достъп - отличителната особеност на локалните мрежи с равноправен достъп (peer-to-peer) е, че те не изискват отделен сървър, на което се дължи относително ниската им цена (фиг.2). Според терминологията на информационните мрежи сървърът осигурява достъп до общите ресурси, например принтери, дискове или други устройства, а компютрите, които използват тези общи ресурси, се наричат клиенти. Големите локални мрежи обикновено изискват инсталирането на отделни високопроизводителни сървъри. Малките локални мрежи обаче често работят ефективно с общи ресурси – “сървъри”, които всъщност са част от компютъра на някои потребител от групата. (2)



Фиг.2 – Мрежа с равноправен достъп

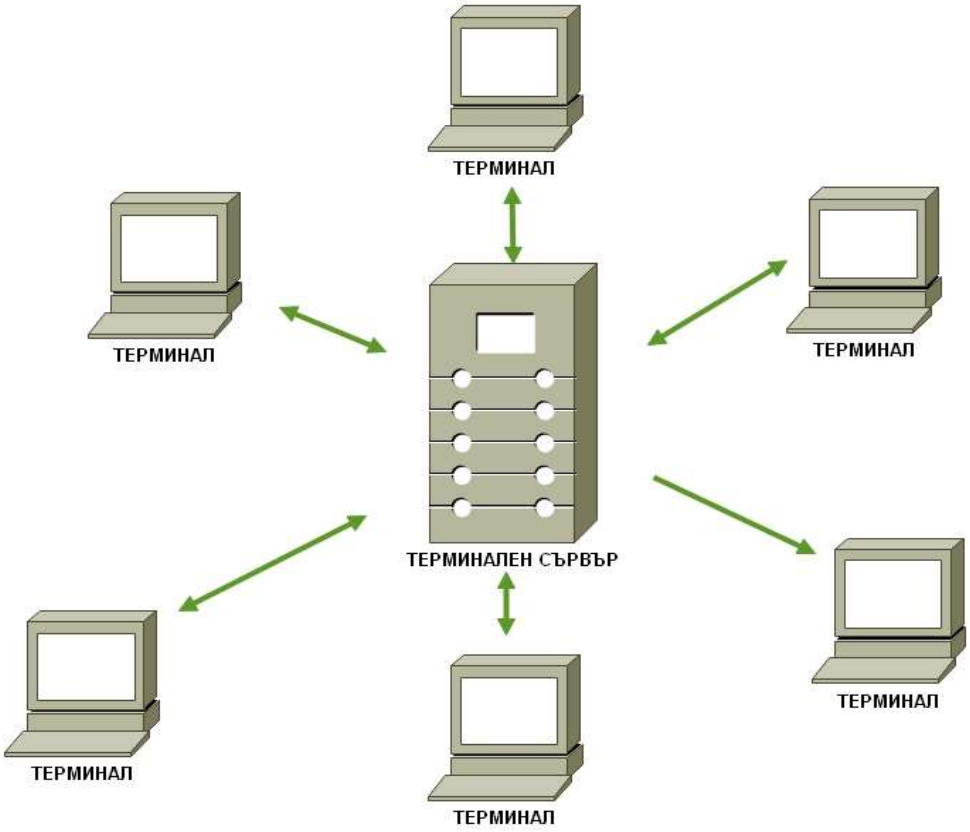
- Локална мрежова система “клиент - сървър”. Централно място при този тип локални мрежи заема сървъра (фиг.3). Тя предоставя управляван достъп до файловете и другите мрежови ресурси. Освен мрежова операционна система в системите “клиент - сървър” се използват и комуникационен софтуер, осъществяващ връзката между компютрите и свързаните с тях мрежови адаптери. Софтуер за пренасочване на входно-изходните операции, изпълнявани от приложенията или локалната операционна система към файловия сървър или към друг ресурс.



Фиг.3 – Мрежа клиент - сървър

- Локална мрежова система “хост - терминал”. Хост (host) е компютър извършващ приложна обработка на данни. Достъпът до него обикновено се осъществява чрез терминали или чрез персонални компютри, които емулират терминали (фиг.4). В системите “хост - терминал” обработването на данни става изцяло в централния компютър, а терминалите или компютрите на потребителите извършват само вход и изход на информация чрез клавиатура и екран. Обикновено локалните мрежи

използвани в такава система, не изискват специална мрежова операционна система. Те използват комуникационен софтуер за достъп до мрежовите ресурси, както и софтуер за терминална емулация, когато потребителите работят не с терминали, а с персонални компютри. Друг тип софтуер е необходим за прехвърляне на файлове между два централни компютъра или между централен компютър и работна станция. (2)



Фиг.4 – Мрежа хост-терминал

1.1.4. Категоризация на мрежите според предоставяните услуги

- Мрежи за достъп до Интернет

Тези мрежи обикновено се изграждат от организации, наречени Интернет доставчици (Internet Service Providers, ISP) и са създадени с цел да предоставят на потребителите достъп до ресурсите на световната мрежа - Интернет. Често в такива мрежи доставчикът на услуги не предоставя допълнителни свои ресурси на потребителите (например сървъри за файлове или мрежови игри), а само им позволява те да достъпват чужди такива сървъри, намиращи се някъде в Интернет. Понякога потребителите на един и същ доставчик на Интернет услуги не могат да споделят помежду си услуги, например да си обменят файлове, въпреки че физически са свързани към една и съща мрежа. (2)

- Мрежи за споделяне на ресурси

Такива обикновено са офисните компютърни мрежи, в които група хора споделят общи ресурси – файлове, принтери, документи, независимо дали тези ресурси се намират на сървър, на локалните компютри или на специализирано мрежово устройство. Възможно е да съществуват правила с различни нива на достъп, които да определят кой потребител с кой ресурс може да работи. Такива мрежи често имат и достъп до Интернет, но ресурсите в мрежата трябва да са достъпни само за служителите вътре в мрежата и се вземат допълнителни мерки за защитата им от външни потребители. Често Интернет достъпът в такива мрежи може да бъде ограничен до определени места или услуги.

- Корпоративни мрежи

Корпоративната мрежа свързва отделните офиси и устройства на една организация в една обща мрежа, така че всички служители да могат да обменят информация помежду си, независимо в кой офис и отдел се намират. В корпоративната мрежа на защитата от външен достъп до документите на компанията се отделя особено голямо внимание. При свързване с отдалечени офиси се използват технологии за глобални мрежи, а често информацията се предава през Интернет, но за да се защити от външните потребители

обикновено се използват различни механизми за сигурност, например виртуални частни мрежи (Virtual Private Networks, VPN). (2)

1.1.5. Видове компютърни мрежи според топологията

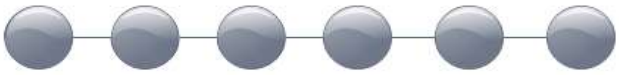
Топологията на мрежите може да бъде разглеждана в два аспекта – физически и логически. *Физическата топология* описва геометричното свързване на компонентите, т.е. начинът по който се разполага кабелът, който ги свързва. *Логическата топология* описва пътя, по който пътуват сигналите от една точка на мрежата до друга. Мрежата може да има една и съща физическа и логическа топология или те да бъдат различни. Така например в мрежа с топология линейна шина (физическа връзка с кабел, който минава последователно от един компютър към друг) данните пътуват в посока от един компютър към друг, което означава, че физическата и логическа топологии съвпадат. В друг вид мрежа компонентите могат да бъдат свързани помежду си посредством централен хъб (фиг.1). В този случай кабелните сегменти са свързани под формата на звезда и физическата топология ще е от тип звезда. Вътре в хъба връзките могат да са осъществени така, че сигналът да пътува в окръжност от един компонент към друг, което означава, че логическата топология е кръгова. В случая физическата и логическа топологии не съвпадат.

Като се абстрахираме от физическия и логически аспект на топологиите, мрежите могат да бъдат класифицирани според топологията, както следва:

- линейна шина;
- кръг;
- звезда;
- решетка;
- хибридна.

➢ Мрежи с линейна шина

Както показва самото име, линейната шина (понякога наричана просто шина) представлява мрежа, която е разположена в права линия. Реално линията не е задължително да бъде права, просто кабелът преминава от един компютър към следващия, след това към следващия и т. н. (фиг.5)



Фиг.5 – Мрежа с линейна шина

Тъй като има начало и край, мрежата с линейна шинна топология изисква терминиране на всеки край. Ако не бъдат терминирани и двата края на кабела, възниква отразен сигнал, който може да наруши или да прекъсне комуникациите по мрежата. Единият от краищата на линейната шина - но не и двата -трябва да бъде заземен. Към края на шината, на първия и последния компютър, свързани към линейния кабел, към „празната" страна на Т-конектора на мрежовата интерфейсна карта се свързва устройство, наречено терминатор.

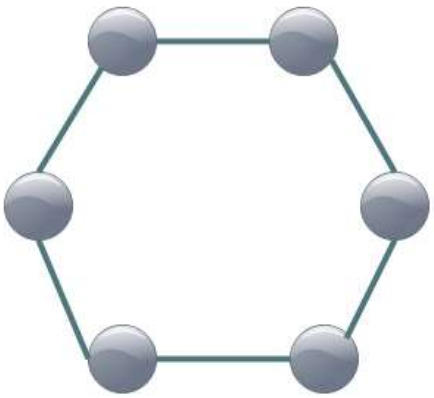
Шинните мрежи обикновено използват дебел или тънък коаксиален кабел и архитектура Ethernet 10Base2 или 10BaseS. По шинната мрежа, когато един компютър изпрати съобщение, това съобщение отива до всеки компютър в мрежата. Всяка мрежова интерфейсна карта (NIC) проверява хедъра на съобщението, за да определи дали то е адресирано за този компютър. Ако не е, съобщението бива игнорирано. Шинната топология е много проста и лесна за инсталиране. Тя е относително евтина и използва по-малко кабел в сравнение с други топологии. Шината е особено подходяща за малки, временни мрежи,

например такива в класни стаи, които може да бъдат използвани само няколко дни или седмици.

Шината е известна като пасивна топология, защото компютрите не регенерират сигнала и не го предават нататък, както правят това в кръга. Това прави мрежата уязвима към затихване, представляващо загуба на силата на сигнала с увеличаване на разстоянието. За решаване на този проблем могат да бъдат използвани повторители. Друг недостатък на шината е, че при прекъсване на кабела (или ако някой потребител реши да разкачи своя компютър от мрежата) линията се прекъсва. Това означава, че компютрите от двете стани на прекъсването не само не могат да комуникират, но също, че двата нови края не са терминирани и резултатният отразен сигнал може да срине цялата мрежа.

- **Кръгова топология**

Кръговата топология е евтина и лесна за реализация. При нея всеки компютър е свързан към два съседни такива, образувайки кръг (фиг.6). Кръговата топология бе реализирана за първи път под формата на шина, краищата на която бяха съединени. Нуждата от терминатори отпадна. За изграждане на мрежата, както и при шинната топология, би могъл да се използва коаксиален кабел.



Фиг.6 – Мрежа с кръгова топология

Кръговата топология има обаче един съществен недостатък - при прекъсване на кръга (при отказ на един от персоналните компютри или при прекъсване на кабела) се спира работата на цялата мрежа. Поради тази причина кръговите мрежи не намериха широка употреба. Мрежата Token Ring на IBM премахна този недостатък. В нея връзките от типа peer-to-peer (компютър с компютър) бяха заменени с връзки от тип звезда. Всеки компютър се свързва към централен хъб (концентратор), който реализира кръга вътрешно в себе си. По този начин бе избегната зависимостта на мрежата от отказа на една работна станция, като в същото време пътуването на сигналите по кръг се запази.

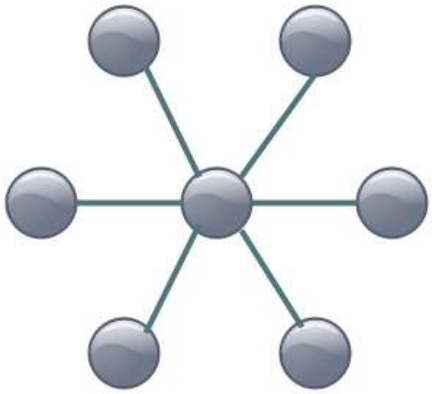
За реализация на архитектурата Token Ring, с която най-често бива асоциирана кръговата топология, се използва друг вид кабел, отбелязван като STP (STP – shielded twisted-pair) и отговарящ на спецификацията IEEE 802.5. Той представлява екранирана усукана двойка.

Под външната обвивка на кабела от тип усукана двойка се съдържат взаимно усукани по двойки изолирани медни проводници. Усукването ограничава в известна степен така наречените кръстосани шумове, предизвикани от външни електромагнитни смущения. Единият проводник неутрализира шума възникнал в другия. Колкото по-нагъсто са усукани проводниците, толкова по-добра е степента на защита срещу посочения вид смущения.

В кръговата мрежа сигналът пътува в една посока. Всеки компютър приема сигнала от своя предходен съсед, регенерира го и го препредава на следващия такъв.

- **Топология звезда**

Звездата (star) е една от най-популярните LAN топологии. Тя се реализира чрез свързване на всеки компютър към централен хъб. Хъбът може да бъде активен, пасивен или интелигентен. Пасивният хъб е просто точка на свързване. Той не изисква електрическо захранване. Активният хъб (най-разпространеният тип) реално представлява повторител с множеството портове; той усилва сигнала, преди да го предаде към другите компютри. Интелигентният хъб представлява активен хъб с диагностични възможности. Той има вграден процесорен чип. Топологията тип звезда свързва всички компютри към един централен хъб (фиг.7).



Фиг.7 – Топология звезда

Звездообразната топология най-общо се използва с кабел тип не екранирана усукана двойка (UTP) и Ethernet архитектура 100BaseT или 1000BaseT.

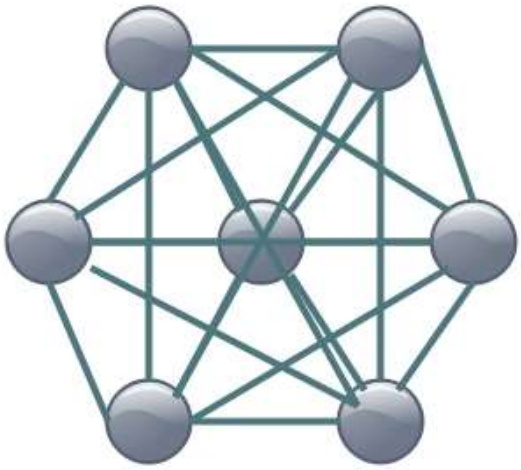
При типична мрежа от тип звезда сигналът се предава от мрежовата интерфейсна карта на изпращащия компютър към хъба, повишава се (т.е. усилва се) и се изпраща обратно през всички портове. При звездата, подобно на шината, всички компютри приемат съобщението, но само компютърът, чийто адрес отговаря на адреса на местоназначението в хедъра на съобщението, му обръща внимание.

Топологията тип звезда има две големи предимства пред шината и кръга. Първо, тя е много по-отказоустойчива (fault tolerant), т.е. ако един компютър бъде изключен или неговият кабел бъде прекъснат, само този компютър бива засегнат, а останалата част от мрежата може да продължи да комуникира нормално. Второ, тя предлага възможност за лесно преконфигуриране. Добавянето на още компютри към мрежата или премахването на компютри е много просто, защото се състои само във включване или изключване на техния кабел в хъба. Отстраняването на проблеми на физическия слой в мрежата от тип звезда също е лесно, особено при наличие на интелигентен хъб, който осигурява диагностична информация.

Независимо от предимствата на звездата, тя има и няколко недостатъка, свързани главно с нейната цена. Първо, тя използва повече кабел, отколкото линейната шина или кръга, защото трябва да има отделен кабел от хъба до всеки компютър. Друг източник на допълнително оскъпяване е самият хъб, който трябва да бъде закупен наред с кабела. Все пак малък плюс при мрежите от тип звезда е, че UTP кабелът е сравнително евтин и няма нужда от терминатори.

- **Топология тип решетка**

Всеки компютър е свързан към всеки от другите компютри (има директна връзка с останалите компютри от мрежата), надеждна и устойчива - ако се прекъсне една от връзките към даден компютър, сигналът се поема от друг път към него (фиг.8). Недостатък - голямо количество кабели, броят на връзките нараства експоненциално при добавяне на нов компютър, което е предпоставка за висока цена, среща се рядко.

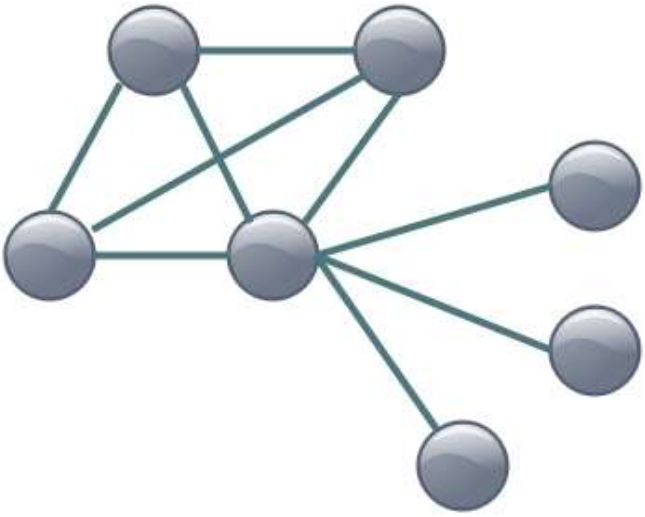


Фиг.8 – Топология тип решетка

- **Хибридна топология**

Думата хибрид се използва в два различни смисъла за означаване на мрежова топология. Думата се използва за означаване на топология, която комбинира елементи на две или повече стандартни топологии (например хибридна решетка, звезда или кръг).

Тъй като решетъчната топология бързо става сложна и неуправляема при нарастване, много мрежи се базират на полурешетъчна топология, при която има допълнителни връзки между някои от компютрите, но не между всички; този тип мрежа често се означава като хибридна решетка. Допълнителните връзки , трябва да бъдат създадени между компютрите, които имат най-голяма нужда от отказоустойчивост на връзката(фиг.9).



Фиг.9 – Хибридна мрежа

В хибридната решетка се осигуряват допълнителни връзки между някои компютри, но не между всички. Хибридната решетка осигурява много повече предимства от обикновената решетката при по-ниска цена и е по-лесна за инсталиране и управление. В хибридната решетка се осигурява допълнителни връзки между някои компютри, но не между всички. (2)

1.1.6. Видове компютърни мрежи според физическия обхват

В зависимост от разстоянието между отделните устройства компютърните мрежи се разделят на:

- **Персонални мрежи (Personal-Area Network - PAN)** включва компютърни устройства използвани от един човек или в рамките на един офис. Обхвата им не превишава 10 m. В PAN се включват настолен компютър, лаптоп, PDA, принтер, телефон, факс или мултимедийни устройства.
- **Локални мрежи (Local-Area Network – LAN)** включват компютри, мрежови адаптери, периферни устройства, среда за

предаване на данни и други мрежови устройства. Те имат следните характеристики:

- функционира в ограничена географска област
- притежава широка пропускателната способност
- предоставя постоянен достъп до ресурсите

- **Глобалните мрежи (Wide-Area Networks – WAN)** представляват комбинация от локални мрежи и допълнителни комуникационни връзки между тях. WAN съединяват потребители, разположени в обширни географски области.
- **Регионални (градски) мрежи (Metropolitan-Area Network – MAN)** се разглеждат като WAN в сравнително малка географска площ-град, област.
- **Мрежите от хранилища данни (Storage-Area Networks – SAN)** представляват специализирани високоскоростни мрежи, които свързват сървъри и хранилища на ресурси.
- **Виртуална частна мрежа (Virtual Private Network – VPN)** се нарича частна мрежа, получена в резултат на обединение на няколко териториално разделени LAN, с помощта на общодостъпни канали на глобални мрежи (например Internet).

1.1.7. Видове компютърни мрежи според използваната операционна система

Основните характеристики на мрежите според операционната система са следните:

- **Windows**

- базирани са на сървър (домейн);

- съществуват различни версии на операционната система с раз-лични характеристики и начини на управление (например при Windows NT 4.0 има главен компютър, наречен главен домейн контролер, в който се съхранява единствено копие за четене/запис на базата от данни за управление на акаутните за сигурност (SAM); в Windows 2000, 2003, 2008, 2012 домейните се наричат домейни от ниско ниво, базирани на Active Directory, а нейно копие се съхранява на всеки домейн контролер, т. е. мрежата съдържа множество домейн контролери и всеки от тях чете и записва в базата от данни на директорията);

- компютри с операционна система, произведена от Microsoft могат да бъдат клиенти и на Windows базирани сървъри;

- компютри с операционни системи Macintosh и Linux също могат да осъществяват достъп до ресурсите на Windows сървъри (ако е инсталиран подходящ софтуер).

- **NetWare**

- Novell NetWare;

- осигурява сигурност и поддържа файлов сървър и принт сървър;

- осигурява директорийни услуги (NetWare Directory Services) чрез йерархична база от данни (наречена *bindery* и подобна на Ac-tive Directory на Microsoft);

- клиентските операционни системи от фамилията Windows могат да осъществяват достъп до NetWare сървър (ако имат инсталиран подходящ клиентски софтуер; от Novell е разработена специална програма Client32 за инсталиране на 32-битова операционна система Windows).

- **UNIX**

- разработена от Bell Labs през 1969 г.;
- използвана е в повечето хостове на ARPAnet;
- има много разновидности;
- може да изпълнява графичен интерфейс.
- има структура с отворен код (написан на езика за програмиране C);

Отвореният код *(Open Source)* осигурява търговска марка за софтуерните разработчици; те предоставят (споделят) своя код с други разработчици и потребители, а те пък са свободни да променят (модифицират) и да дистрибутират самостоятелно кода. Софтуерът трябва да се разпространява безплатно. Повече информация виж на адрес: http://www.opensource.org

- **Linux**

- приема се, че е вариант на UNIX (т. е. UNIX-базирана операционна система);
- разработена е от Линус Торвалдс в началото на 90-те години на XX век;
- и мрежова (сървър), и клиентска (настолна) операционна система;
- множество различни версии (най-популярни сред тях са RedHat, Caldera, Corel);

- има отворен код (отворен стандарт);
- може да изпълнява графичен интерфейс.

➢ **Хибридна**

- повечето средни и големи мрежи се считат за хибридни;
- използва софтуер, разработен от различни производители;
- използва множество протоколи;
- може да комбинира концепциите на домейн и работна група;
- повечето производители предоставят инструменти за взаимодействие между различните видове софтуер (интероперативност); например: Client Services for NetWare (CSNW), Gateway Services for NetWare, File and print for NetWare, Services for Macintosh, Sys-tem Network Architecture (SNA) и др.

1.1.8. Видове компютърни мрежи според използваните мрежови протоколи

Една друга класификация на мрежите е според използваните от тях мрежови протоколи за комуникация. Мрежовите протоколи представляват набор от правила, които свързаните помежду си компютри спазват по време на комуникация. Трите най-популярни LAN протоколи са NetBEUI, IPX/SPX, TCP/IP.

Основните характеристики на мрежите според използваните мрежови протоколи са следните:

• **NetBEUI**

За споделяне на файлове и принтери (File and printer sharing) в операционните системи Windows, Microsoft предлага протокола NetBEUI (NetBIOS Extended User Interface). Това е прост, бърз протокол, позволяващ висока мрежова

производителност на използващите го системи. NetBEUI се използва само в локални мрежи, той не поддържа маршрутизиране. Единственото конфигуриране, което се изисква е задаване на уникално име на всеки компютър в локалната мрежа. За по-лесно търсене, компютрите се обединяват в работни групи. Евтина за изграждане, с малко ресурси, лесна инсталация и поддръжка.

- **IPX/SPX**

Фирмата Novell изгражда своите продукти на базата на Ethernet спецификацията IEEE 802.3 чрез протоколите IPX/SPX (Internet Package Exchange/Sequence Packet Exchange). Използването им е задължително до версия 4 на операционната система NetWare. Пълна поддръжка на TCP/IP за файлов и принт сървър се поддържат след NetWare 5.0. NetWare версия 4 поддържа TCP/IP за целите на вградения web сървър. (2)

Поради голямата популярност и надеждност на продуктите NetWare, Microsoft включва в операционните системи Windows, IPX/SPX съвместимия протокол NWLink. Всеки компютър с операционна система Windows може да бъде както клиент, така и сървър на NetWare мрежа, чрез използване на IPX/SPX или NWLink протоколите.

IPX/SPX мрежата изисква минимално конфигуриране (всяка мрежова интерфейсна карта има зададен MAC адрес) и предлага по-висока мрежова производителност в сравнение с TCP/IP мрежите. IPX/SPX протоколите се използват за връзка към NetWare сървъри. От съображения за сигурност много потребители използват IPX/SPX протоколите за споделяне на файлове и принтери в локални мрежи. Съответно интернет потребителите използват TCP/IP протокола и не могат да достигнат до локалните сървъри, използващи IPX/SPX. (2)

• **TCP/IP**

TCP/IP е протоколът, който използва глобалната мрежа Интернет. На практика всички хардуерни платформи и операционни системи поддържат TCP/IP. Той е най-бавен и труден за конфигуриране от популярните LAN протоколи, но това се компенсира с неговата сигурност, възможност за маршрутизиране и голямото количество клиентски и сървърни програмни продукти, които го поддържат. За споделяне на файлове и принтери в TCP/IP мрежите се използва протокола 'NetBIOS Over TCP/IP'.

- **Spanning-Tree** е мрежов протокол създаден с цел да предвижда съкращаване пътя, като се предотвратяват нежелани повторения (loop) в топологията на мрежата. Той е стандартизиран от IEEE IEEE 802.1D и се основава на алгоритъм, описан от Радия Перлман през 1985 г.

За Ethernet мрежа, за да функционира правилно, само един активен път може да съществува между две станции (компютъра).

При множество активни връзки между компютри се предизвикват повторения в мрежата. Ако повторението на пакети съществува в мрежовата топология, съществува и потенциал за дублиране на съобщения. Когато повторенията се случат някои суичове виждат един и същи компютър да се появява и от двете страни на суича. Това условие обърква алгоритъма за препращане и позволява дублираните фреймове да бъдат препращани.

За да се осигури съкращение на пътя, Spanning-Tree протокол определя дървовидна структура, която обхваща всички суичове в разширена мрежа. Spanning tree протокол кара някоя излишна или повтаряща се

информация в режим на готовност (блокирано) състояние. Ако един мрежов сегмент в Spanning-tree протокол стане недостъпен, или ако еквивалента на Spanning-Tree протокола за даден мрежов сегмент се промени, Spanning Tree алгоритъма се преконфигурира и променя дървовидната си структура и топология на мрежата възстановява връзката която е била в режим на готовност.

Spanning-Tree протоколът работи невидимо за крайни станции (компютри), които не знаят дали те са свързани с един LAN сегмент или са включени в LAN от множество сегменти.

Има различни разновидности и подобрения на STP, но базовата функционалност е същата: STP – IEEE 802.1D-1998 – базовата версия на протокола

- **2001 - RSTP (Rapid STP, IEEE 802.1w)** – При стандартния STP е необходима почти минута за да се включи нов порт или да се открие промяна в топология на мрежата и да се включи блокирана връзка. При RSTP са въведени някои подобрения, които позволяват това да стане много по-бързо.

- **2002 - MSTP (Multiple STP, IEEE 802.1s)** – Стандартния STP създава една топология за цялата мрежа. MSTP позволява да се създава отделна топология за отделните vlan-и в мрежата. Например даден порт може да е блокиран за една група от vlan-и, но разрешен за друга група.

• **Други**

- AppleTalk (набор от протоколи AppleTalk Address Resolution Protocol (AARP), разработени от Apple за организиране на мрежи с компютри Macintosh);

- Open System Interconnection (OSI) (комплект от протоколи, разработени от ISO през 80-те години с цел замяна на TCP/IP, но опитът е неуспешен).

1.2. Среда за предаване на данни.

Свързването между отделните устройства в една компютърна мрежа се осъществява чрез среда за предаване на данни. При кабелните мрежи тя се състои от набор проводници и кабелни съединители (конектори). При безкабелните мрежи средата за предаване на данни представлява земната атмосфера или безвъздушно пространство.

Кабелните съединения се използват най-често при изграждане на мрежи. Основно се използват медни проводници (коаксиален кабел и усукана двойка) и оптичен кабел.

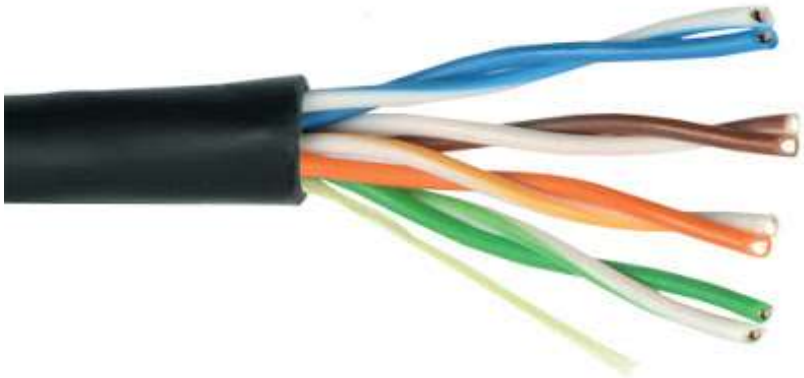
1.2.1. Усукана двойка (twisted pair)

Кабелите под външната обвивка са усукани по двойки и по този начин се предотвратяват паразитните кръстосани шумове, т.е. влиянието на един проводник върху сигнала предаван по друг. Колкото е по-голям броят на усукванията за един фут, толкова е по-добра степента на защита срещу кръстосани шумове. (3)

Видове усукана двойка:

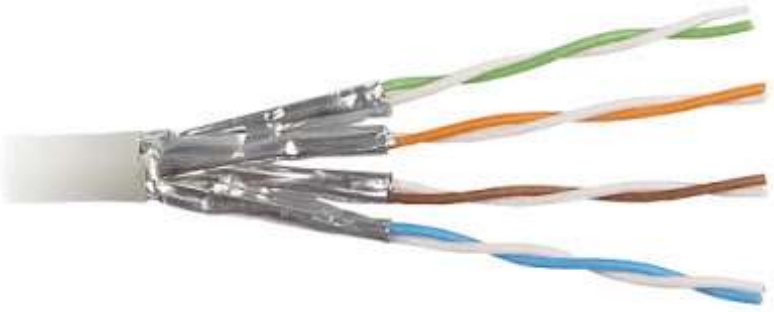
- **UTP** (unshielded twisted pair) – неекранирана усукана двойка. Този кабел се използва масово в съвременните компютърни мрежи, тъй като е евтин. UTP (фиг.10) е направен от една или повече двойки от медни проводници, като

всеки проводник в двойката е усукан около другия. UTP обикновено се състои от 4 двойки от усукани кабели с цветови кодове. Основен недостатък на UTP е, че диапазонът на предаване на данни с добро качество на сигнала е до 90-100 метра.



Фиг.10 - UTP кабел (4)

- **STP** (shielded twisted pair) – екранирана усукана двойка (фиг.11). Този кабел е подобен на UTP, с няколко цветово кодирани усукани двойки, но той включва и защитно фолио под пластмасовата изолация. Всяка двойка е екранирана. Защитното покритие предпазва проводниците от външни смущения и помага за защитата на данните. Това оскъпява STP кабела.

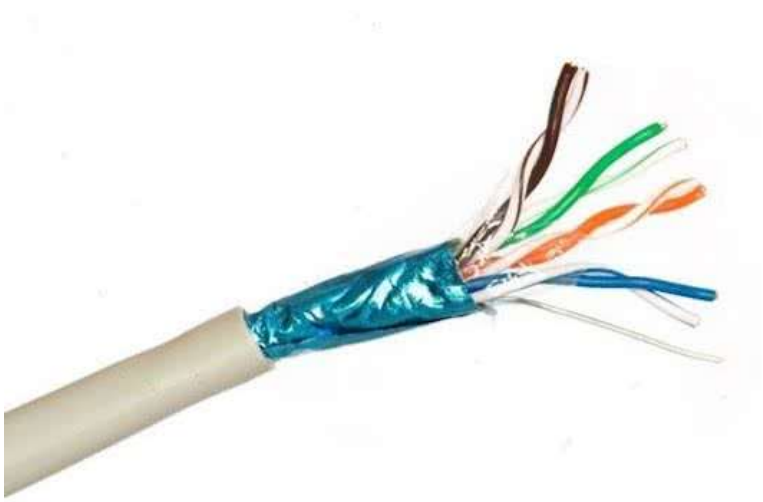


Фиг.11 - STP кабел (4)

- **FTP** (foiled twisted pair) – фолио-екранирана усукана двойка (фиг.12). Това е кабел с усукани двойки, който е по-евтин от STP. Екранът е един – общ за всичките двойки проводници. Неговата изолация е от по-

качествена пластмаса спрямо тази на UTP кабела. Този вид кабел е предназначен за външен монтаж.

Кабелите с усукана двойка се свързват към компютри и други устройства, използвайки конектор RJ-45 (Registered Jack –регистриран жак). Той има 8 кабелни връзки. Конекторът RJ-45 се монтира към кабел с усукани двойки проводници с помощта на специални клещи за кримпване.



Фиг.12 - FTP кабел (4)

1.2.2. Коаксиален кабел

Коаксиалният кабел в последно време най-често се използва за предаване на сигнал на кабелна телевизия. Сърцевината е изградена от меден проводник. Вида на проводника може да бъде многожичен или солиден. Сигналът се предава по медния проводник. Около медта се увива изолация, а над изолацията има друг меден проводник, като предназначението на горният проводник е да екранира сигнала от електромеханични смущения.

Видове коаксиален кабел

- Тънък коаксиален кабел – предава сигнал до 200 метра.

- Дебел коаксиален кабел – предава сигнал до 500 метра.

Фиг.12 - Коаксиален кабел (4)

1.2.3. Оптични кабели (fiber-optic)

Оптичните влакна представляват светлопропусклива стъклена сърцевина (core), облечена в светлоотразяваща обвивка (cladding). По сърцевината се разпространяват светлинни, вместо електрически сигнали.

Оптичните влакна безспорно са най-перспективната среда за предаване на информация. Най-бързите в съвременния свят мрежови технологии – 40 Gbit/s и 100 GBit/s Ethernet, както и други технологии за глобални мрежи работят само по оптични влакна и за тях няма разработени алтернативи за метални проводници. Към момента на написване на тази книга има експериментални изследвания в лабораторни условия, които доближават или дори надвишават 100 Tbit/s (терабита, 1 терабит = 1024 гигабита) по едно оптично влакно, но има още време, докато те се стандартизират и излязат на пазара.

Оптичните влакна имат и други предимства – докато предаването по метални кабели достига до 100 метра за усукана двойка (по стандарт – в практиката е възможно постигане и на по-големи разстояния) и до няколкостотин метра при коаксиален кабел, при оптичните влакна е типично достигането на няколко десетки километра, дори има
технологии за над 100 километра. Тъй като в оптичното влакно няма метал, то не се влияе от външни смущения.

Недостатъкът на оптичните влакна е, че те са доста крехки и по-лесно могат да бъдат пречупени, така че за тях трябва да се положат по-специални грижи за предпазване от механични въздействия. На пазара съществуват специално заздравени оптични кабели, предназначени за подземно или въздушно полагане, които гарантират, че оптичните влакна в кабела няма да се пречупят при определени условия.

Тези характеристики определят най-честата употреба на оптичните кабели – за магистрални трасета на големи разстояния, свързващи няколко локални мрежи, а
самите локални мрежи най-често се изпълняват с усукани двойки.

Оптическата система се състои от източник на светлина, предавателна среда и детектор. Оптичният кабел (fiber-optic) предава импулси от светлина, а не електрически импулси. Това позволява много по-високи скорости на трансфер на данните – оптичният кабел може да предава данни със скорост до 40 Gbps. Този кабел се използва за предаване на данни на дълги разстояния (Фиг.13).

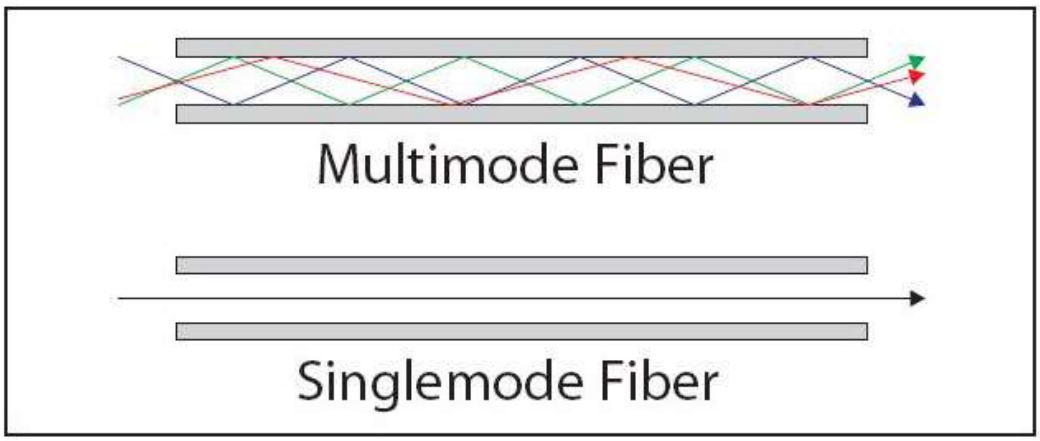
Фиг.13 - Оптичен кабел (3)

Режими на работа на оптичните кабели

В момента най-често се използват два типа оптични влакна – едномодови и многомодови (фиг.14) :

- Едномодовите (Single Mode) оптични влакна имат диаметър на стъклената сърцевина 8 или 9 микрометра. Външният диаметър на влакното и при двата вида обикновено е 125 микрометра. При едномодовите влакна светлината се излъчва от тясно фокусиран лазер, има една честота и се разпространява в права посока по дължината на влакното. Тези влакна постигат по-високи скорости на обмен и покриват по-големи разстояния, но светлинният източник е по-скъп, което повишава цената.

- Многомодовите (Multi-Mode) влакна имат диаметър на сърцевината 50 или 62,5 микрометра. При тях източникът на светлина е специален лазерен светодиод, който излъчва сноп лъчи с близки дължини на вълните. Те се разпространяват отразявайки се от обвивката, при което губят част от енергията си. Поради това скоростите и разстоянията са по-ниски, но устройствата за предаване са по-евтини. Ако например по едномодово влакно може да се предава с 10 Gbit/s на разстояние над 100 километра, то с многомодово влакно могат да се постигнат около 550 метра.



Фиг.14 – Режими на работа на оптичните кабели (4)

Многомодовите биват четири вида - OM1, OM2, OM3 и OM4

При тях имаме едновременно излъчване на няколко лъча (моди) от светлина. В сравнение със сингъл мод влакната, многомодовите са направени от по-голяма сърцевина – 62.5 и 50 микрона.

OM1 (optical mode 1) е първия тип мултимод и в днешно време се използва все по-рядко. Неговият размер е най-голям – 62.5 микрона, и също така използването му за 100Mb и 1Gb крие значителни препятствия и ограничения. Определено не се препоръчва за изграждане на нови инсталации, а само за доразвиване на вече изградени такива в миналото.

OM2 има размер на сърцевината от 50 микрона и е представен през далечната 1980 година с пренос на 1Gb, който за времето си се е считал за „поглед в бъдещето“. Към настоящия момент има нови и оптимизирани влакна, който правят избора на OM2 като нецелесъобразен за нови инсталации.

OM3 е най-широко разпространеното мултимод оптично влакно в днешно време, като то също има сърцевина от 50 микрона, която е оптимизирана. Влакното е проектирано да пренася скорости от 40Г на разстояние от 100 метра и обикновено се асоциира с морско-син цвят на кордите.

OM4 е последния тип мултимодно влакно, което се появи на пазара преди няколко години и наскоро беше официално стандартизирано. То има по-нисък insertion loss and спрямо всички останали мултимод влакна. То също има

оптимизирана сърцевина с размер от 50 микрона и позволява пренос на данни със скорост дори от 100Gb до 150 метра и се използват широко в съвременните дейта центрове. Все още обаче има немалка ценова разлика, спрямо OM3 влакната

1.2.4. Безпроводни (безжични) среди за предаване на данни

Безжичните технологии се използват като метод за предаване при локалните мрежи, разширените локални мрежи и мрежите с мобилни компютри. Стандартната безжична мрежа е като кабелната мрежа, само че във всеки компютър трябва да се инсталира мрежова карта с трансийвър, за да могат потребителите да комуникират с мрежата така, сякаш тя е свързана с кабел. (3)

Безжичните локални мрежи използват 4 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)

- **Инфрачервено предаване на данни** - всички инфрачервени безжични мрежи използват инфрачервено светлинно излъчване, което пренася данните между устройствата. Тези системи трябва да генерират много силни сигнали, защото слабите сигнали се влияят от други светлинни източници, като например светлина от прозорците. При този метод сигналите могат да се предават с голяма скорост, защото инфрачервената светлина има голяма широчина на честотната лента. При нормални обстоятелства една инфрачервена мрежа може да предава с 10 Mbps. (3)

- **Лазерната технология** прилича на инфрачервената по това, че изисква пряка видимост и всеки човек или предмет, блокирал този лъч, блокира предаването.

- **Теснолентово (едночестотно) радиоизлъчване -** този подход е подобен на излъчването от радиостанция-потребителят наглася предавателя и приемника на определена честота. Не се изисква пряка видимост, тъй като диапазонът на излъчване е 5000 кв.м., но тъй като сигналът е високочестотен, той не може да премине през бетонни или стоманени стени.

- **Мрежи с разпределен спектър -** радиомрежите с разпределен спектър излъчват сигнали в определен диапазон от честоти. Така се избягват проблемите, възникващи при мрежите с теснолентово радиоизлъчване.
Наличните честоти са разделени на канали. Адаптерите се настройват на даден канал за определено време, след което се превключват на друг канал. Компютрите от мрежата се синхронизират спрямо последователността на смяна на каналите. Така се изгражда защита против подслушване на потока от данни. За да се подсили тази защита получателят и изпращача могат да кодират предаването. Стандартната скорост от 250 Kbps прави този метод много по-бавен от останалите, но той може да предава на разстояние 2 мили на открито и 250 метра на закрито със скорост 4 Mbps. (3)

1.3. Активни мрежови устройства

Активните мрежови устройства са тези, които осъществяват основното предаване на информация (сигнали) в мрежата. Най-използваните от тях са:

- Конвертори на преносната среда
- Мрежови карти (NIC)
- Повторители
- Концентратори (хъбове,Hubs)

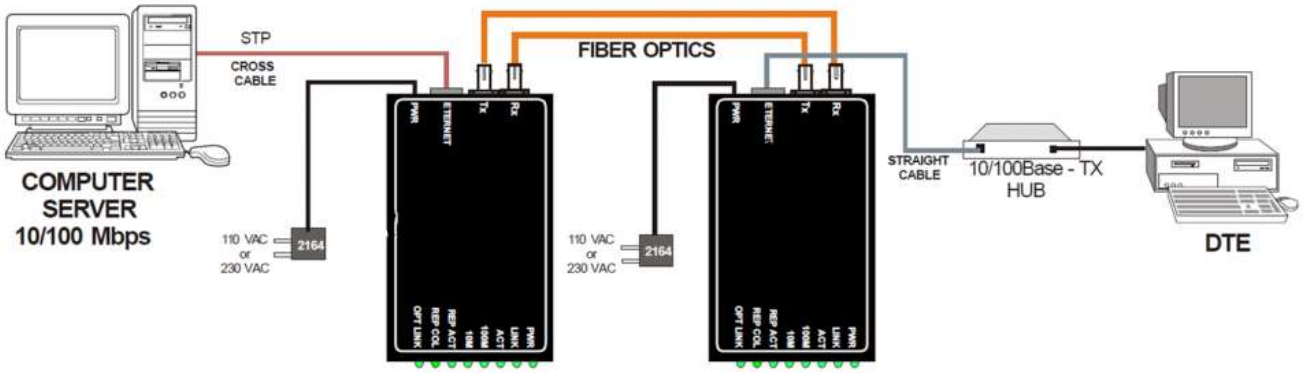
- Мостове (Bridges)
- Комутаторите (Switches)
- Маршрутизаторите (Routers)
- Шлюз (Gateway)

1.3.1. Конвертори на преносната среда

Наричат се още адаптери за преносна среда (media adapters), медия конвертор (media convertor) или транслатори на преносна среда (media translators) (фиг.15).

фиг.15 – Медия конвертор (4)

Извършват преобразуване на електрическите импулси на 10BaseT, 100BaseT и 1000BaseT или на Token Ring в светлинни импулси, предавани по оптичен кабел (фиг.16) .



фиг.16 – Приложение на медия конвертора за преобразуване на сигнала между две преносни среди (4)

1.3.2. Мрежови контролери (NIC)

За да може компютър да бъде свързан в мрежата, той трябва да има мрежов контролер (мрежова карта) – устройството, което осъществява физическата връзка на компютъра с мрежата.

Мрежовата карта служи за физически интерфейс между компютъра и мрежовия кабел при реализация на локални компютърни мрежи (LAN). Картите се инсталират в разширителните слотове на всеки компютър и сървър в мрежата.

- Мрежовия адаптер реализира функциите на каналното и физическото нива на модела OSI:
  - LLC - управление на логическите връзки.
  - MAC - управление на достъпа до физическата среда.

- Основни функции - преобразуване и подготовка на данните за изпращане от компютъра към мрежовия кабел.
  - Сериализиране на данните при предаване и десериализиране при приемане - преобразуване формата на данните от паралелен в сериен и обратно.

- Преобразуване на цифровите сигнали в електрически или оптически, така че да могат да се предават по мрежовите кабели.

- Изпращане на данните към друг компютър.
  - Установяване местоположението на адаптера. Всеки адаптер има индивидуален адрес, идентификатор, който го отличава от всички други произведени в света адаптери. За целта IEEE предоставя блокове от адреси на всеки производител.
  - Комуникация между картата и периферната шина на компютъра в процеса на предаване и приемане на данните.

- Управляване на потока от данни между компютъра и кабелната система.
  - Установяване параметрите на обмена между адаптера, реализиращи връзката. Преди да започне обмена на данни двете карти постигат споразумение за параметрите на обмена - Максимален размер на изпращаните групи от данни, скорост на предаване, временни съотношения и други.
  - Обмен на данни, след установяване параметрите на обмена.
- Архитектура - мрежовият адаптер е микропроцесорна система, която реализира програмно-апаратно средство за обмен на данни в локалните мрежи.

Мрежовите карти могат да бъдат отделни платки, които се поставят на слот в компютъра и могат да се сменят при нужда или да бъдат вградени в дънната платка на компютъра. Съществуват различни технологии за компютърни мрежи и всеки контролер е специализиран за конкретната

технология. На фиг.17 е показан мрежов контролер за жична мрежа, а на фиг.18 - за безжична мрежа.

Фиг.17 – Кабелна мрежова карта

Фиг.18 – Безжична мрежова карта

1.3.3. Повторители

Повторителят свързва два мрежови сегмента или служи за наставяне на кабел, той 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 усилва, а ефективната дистанция на кабела се увеличава.

Повторителите не филтрират преминаващите през тях данни. Те регенерират всички сигнали, включително броадкастните съобщения, шума и смущенията, предавайки ги нататък. (3)

1.3.4. Концентратори (хъбове,Hubs)

Hub, или както е прието в България, концентратор, представлява 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 включените 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 включени 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 (фиг.19).

Фиг.19 – Концентратор (HUB)(4)

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. Хъбове често имат портове с конектор RJ-45 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) комутатори (Switch) е в това, че концентраторите нямат възможност да буферират 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 буферира 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.

1.3.5. Мостове (Bridges)

Мостът (bridge) е устройство, предназначено за свързване на най-малко две LAN мрежи или на два мрежови сегмента на една и съща LAN, използващи един и същ протокол – например Ethernet и Token Ring (фиг.20).

Мостовете работят на второто ниво (каналния слой) на модела OSI. Основното им предназначение е да *препредават* или да *филтрират* пакетите в зависимост от MAC адресите на получателите им. Те прочитат от хедърите на пакетите MAC адресите на подателите и на получателите и ги обработват, без да засягат по-високите слоеве на OSI модела.

Фиг.20 – Свързване чрез мост (bridge)

Всеки мост изгражда автоматично *маршрутна таблица (routing table)* с MAC адресите на станциите (компютрите) от LAN мрежата, към която той е включен. Когато по мрежата бъде изпратен пакет (в Ethernet наричан фрейм), мостът прочита от него MAC адресите на подателя и на получателя и ги сравняна с адресите от таблицата. Ако адресът на получателя се намира в таблицата, т.е. ако пакетът е адресиран до някой от компютрите в същата LAN, мостът го *филтрира*, т.е не го пропуска през себе си. Пакетът остава в мрежата и достига до всички компютри в нея. Когато мостът свързва два сегмента на една и съща LAN, той изгражда таблица с MAC адресите на двата сегмента. Когато по мрежата бъде изпратен пакет, мостът прочита от него MAC адреса на получателя, сравнява го с адресите от таблицата и определя дали получателят и подателят се намират в един и същ сегмент. Ако те са в различни сегменти, мостът препраща пакетът в другия сегмент, където той се възприема от компютъра, за който е предназначен. (3)

Мостовете обработват пакетите много бързо, тъй като не ги преформатират. Те единствено прочитат адреса на получателя и вземат решение дали да филтрират или да препратят пакета. Обикновено мостовете притежават по няколко вида кабелни интерфейси, така че Ethernet LAN с

дебел коаксиален кабел (10Base5) може да бъде свързана чрез мост към Ethernet LAN с усукани двойки проводници.

Обикновено мостът представлява компютър с няколко мрежови карти, към всяка от които е свързан сегмент на локална мрежа. За да бъде ограничен потокът от данни между сегментите на мрежата, се използва правилото 80/20, в съответствие с което около 80% от трафика трябва да бъде локален (между компютрите на сегмента) и само 20% външен (между сегментите на LAN).

1.3.6. Комутатори (Switchs)

Основната функционалност на един комутатор (суич) 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 промеждутъчно 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.

Комутаторът е концентратор с възможност да комутира кадри в каналния слой. Използва се за намаляване на вероятността за конфликти в мрежите функциониращи по протокол IEEE 802.3 и за увеличаване на скоростта на предаване на данни. Комутаторите използват три вида комутации:

- Статична комутация;
- Динамична комутация;
- Комутация на сегменти.

При статичната комутация мрежовият администратор премества програмно потрбителите от един сегмент в друг. По този начин някои потребители се преместват от претоварен сегмент на мрежата в друг по-малко натоварен.

Динамичната комутация осигурява непрекъсната комутация между мрежовите устройства. Непрекъснато се създават динамични съединения между портовете на комутатора, като комутацията се извършва на базата на адресната информация в кадрите. По този начин в локалната мрежа се създават десетки съединения без да си влияят взаимно.

При комутацията на сегментите към всеки порт на комутаторът се свързва отделен сегмент на мрежата. Комутаторът не е в центъра на локалната мрежа, а в периферията и изпълнява следните задачи:

- Контролира достъпа до опорната мрежа;

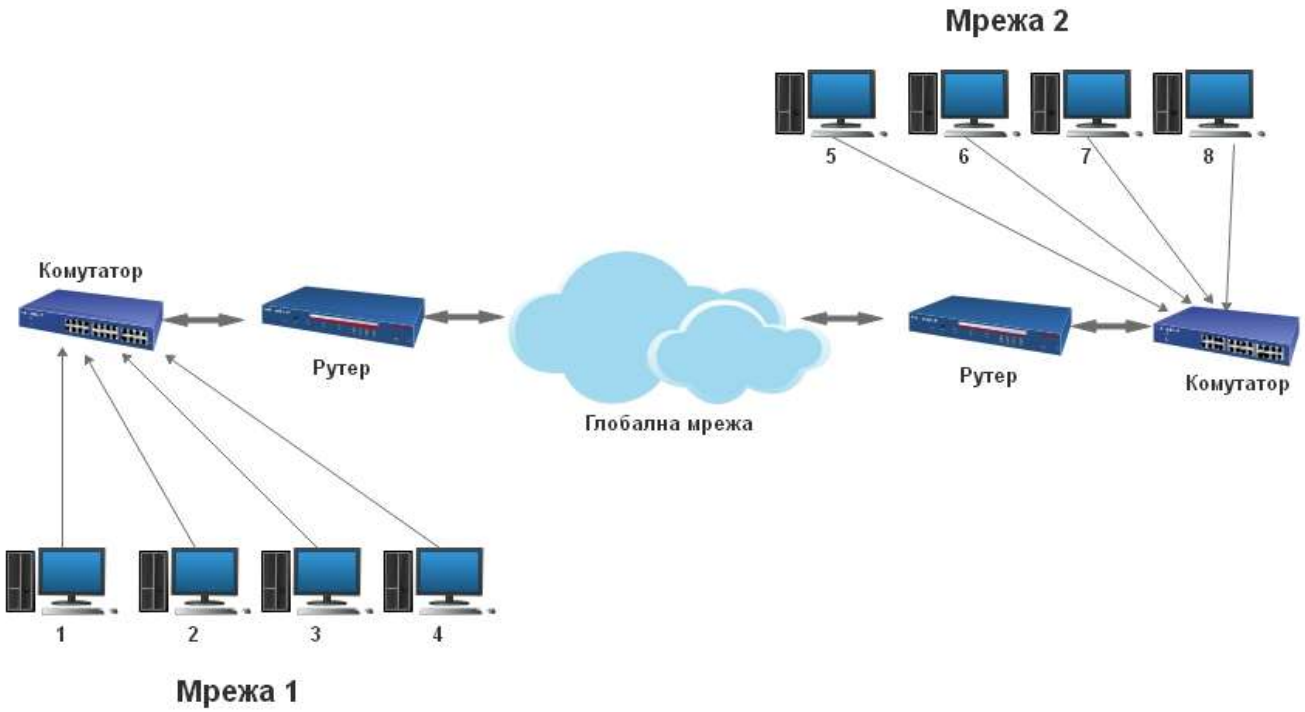
- Контролира обсега на разпространение на общодостъпните кадри – изпратени до всички;
- Контролира достъпа до глобалната мрежа или Internet.

Програмното управление на комутираните локални мрежи позволява създаване на виртуални локални мрежи (VLAN). За целта група възли и потрбители се отделят програмно и работят като отделна мрежа. Виртуалната локална мрежа се създава и реконфигурира лесно. Има възможност една работна станция да се включи към няколко такива мрежи. Използват се Ethernet комутатори, които поддържат до 64 виртуални мрежи към един порт.

1.3.7. Маршрутизатори (Routers)

Маршрутизаторът (на английски: router, рутер) е самостоятелно устройство, което служи за управление на разпределянето на трафика (пакетите) информация между различни мрежи или различни сегменти от дадена мрежа. Маршрутизаторът работи на слой 3 (мрежови) от седем слойния OSI модел. Тоест, маршрутизаторът работи с логически IP адреси, а не с MAC адреси, по което се различава от хъба или моста. Ако до някое устройство в мрежата връзката е през маршрутизатор, а не през суич или хъб, то ние не научаваме неговия MAC адрес.

За определяне на пътя за предаване на данните и насочване на пакетите маршрутизаторът използва таблица за маршрутизация, в която се съхраняват IP адресите на други маршрутизатори. Тази таблица маршрутизаторът си създава сам, като си набавя информация, а при някаква промяна сам я актуализира, „разпитвайки“ другите маршрутизатори кой докъде е свързан. Работата на маршрутизатора може да се разбере от следния пример фиг.21 :



Фиг.21 – Използване на маршрутизатори (рутери)

Мрежата 1 съдържа мрежови устройства 1, 2, 3 и 4. Мрежата 2 съдържа мрежови устройства 5, 6, 7 и 8. Двете мрежи са свързани чрез маршрутизатори (рутери) – данните, които трябва да се изпратят от мрежата 1 до мрежата 2, трябва да минат през маршрутизаторите. Когато мрежово устройство 1 иска да общува с мрежово устройство 2, маршрутизаторът не изпраща пакети към мрежа 2, като по този начин предпазва проникването на трафик към 2. Когато обаче, мрежовото устройство 1 поиска да общува с устройство 8, маршрутизаторът предава данните към мрежа 2, където те ще се получат от устройство 8. Маршрутизаторите обикновено са реализирани като самостоятелни устройства, със собствен процесор и собствена операционна система. В частност един компютър също може да бъде конфигуриран да работи и като маршрутизатор.

Кога се налага да използваме маршрутизатор?

• при свързване на една локална мрежа към Интернет (с реални IP адреси);

• при свързване на две или повече локални мрежи;

• за разделяне на една локална мрежа на две или повече подмрежи.

Използването на маршрутизатор като устройство за свързване ще доведе до намаляване на трафика между отделните мрежи и подобряване на сигурността в локалната мрежа. Все по-често се използват рутери с вграден хардуер за безжична мрежа. Има устройства, при които WAN порта е ADSL.

1.3.8. Шлюз (Gateway)

Шлюзовете са устройства за връзка между мрежи от различен тип. Тяхната работа е да преобразуват информацията, получена от дадена мрежа, във вид разпознаваем за мрежата получател.

Понятието gateway много често се смесва с входно/изходната точка при IP рутиране. В много случаи понятието gateway трябва да се употребява за реализация на входно/изходна точка на по-високо ниво за комуникация от рутер. Понякога такива устройства се използват за адресно преобразуване между отделни комуникационни мрежи. Използването на такива входно/изходни точки обикновено ограничава броя на конекциите между приложения, използващи ги за комуникация. Gateway е непрозрачен за IP комуникации. Ако определен хост изпрати дейтаграма през gateway, обикновено се реализира комуникация само до него, но не и прозрачно през него. Много често с това понятие се свързва и защитата, реализирана посредством „огнена стена” (firewall). Тя дава възможност за частично или пълно ограничаване на достъпа от една мрежа или група мрежи към друга такава. (5)

Шлюзът е устройство или софтуер инсталирано във възел посредник за съгласуване протоколни стекове. Софтуерът се инсталира в транспортния, сесийния или приложния слой на отворения модел за комуникации. За да могат две мрежи с различни протоколни стекове да си взимодействат е необходимо и двата стека да се инсталират в шлюза. Те преобразуват както протоколите така и системите за кодиране. Недостатък на шлзовете е, че те работят сравнително по-бавно от крайните възли и концентрацията на съгласуващия софтуер в един възел намалява производителността и сигурността на мрежата, тъй като при повреда или отказ на шлюза системата престава да работи. (3)

1.4.Мрежови модели и стандарти

Преди данните да бъдат предадени по мрежата като електрически импулси, те първо трябва да бъдат разделени на отделни парчета, които лесно могат да бъдат управлявани. Всеки файл – документ, видео, аудио или друг формат не може да бъде изпратен в един дълъг, непрекъснат поток. Това ще ограничи мрежата, и другите компютри няма да могат да предават. За да могат много компютри да използват мрежата едновременно, големите файлове трябва да бъдат разделени на по-малки секции, преди да бъдат изпратени по кабела или друга преносна среда. Малките секции, на които се разделят компютърните данни за предаване по мрежата, се наричат *пакети.* В зависимост от мрежовата архитектура и от точката в процеса на комуникация, до която е достигнало дадена секция, когато говорим за пакети, можем да използваме и термина *фреймове.*

Предимства от разделянето на данните на пакети

Предлагането на данните на малки пакети има няколко предимства:

• Компютрите в мрежата могат да използват обиколни пътища за

предаване на пакетите и един компютър, който предава големи количества данни, не може да монополизира пропускателната способност (честотната лента, капацитета) на мрежата.

• Ако мрежовата комуникация бъде прекъсната или даден пакет бъде из-губен, трябва да бъде предадена отново само тази малка част от данните, а не целият файл.

• В зависимост от топологията на мрежата и типа на свързването, всеки пакет може да премине по различен път, за да достигне до местоназначението. По този начин, ако един път започне да се препълва или стане прекалено бавен, следващите пакети могат да поемат по по-ефикасен маршрут.

1.4.1. Мрежови модели

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.

1.4.1.1 Моделът OSI

Един от основните модели, използвани в съвременния мрежов свят е съставен от международната стандартизационна организация ISO през 1984 година и се нарича „Препоръчителен модел за взаимодействие между отворени системи“ (Open System Interconnection reference model). Понятието „отворена система“ означава система изградена според препоръките и е отворена за

комуникация с други системи, също изградени според същите препоръки. Въпреки че повечето съвременни системи имат за цел да бъдат „отворени“, за да могат да си комуникират с останалите, практиката познава изграждането и на „затворени“ системи, изпълнявайки мрежова комуникация чрез нестандартна, скрита за света съвкупност от интерфейси, протоколи и правила за комуникация. Разбира се, целите на подобни системи са повишаване на степента на сигурност, запазване на авторски права или осигуряване на възможност за комуникация в такава мрежа само на системи, разработка на дадена фирма. Това противоречи на принципите на съвременния мрежов свят, чиято цел е да осигури възможност за еднаква комуникация навсякъде и със всякакви средства, но може да помогне на съответните компании за получаване на по-голяма печалба от разработените от тях системи. (5)

Моделът на ISO (често наричан OSI модел, стек OSI) е структура на седем нива. Техните наименования и местоположение са показани на фиг.22

Фиг.22 Модел OSI

Всеки слой на модела изпълнява конкретна задача. В предаващия компютър всеки слой получава данни от по-горния слой, добавя към тях своя информация (под формата на хедър) и предава данните надолу към следващия такъв.

На фиг.24 се визуализира процеса на комуникация.

Фиг.24 – Процес на комуникация

- **Приложен слой**

Слоят осигурява взаимодействието (интерфейса) между потребителското приложение и мрежата. Но това не е онази част на приложението, която създава самото изпращано съобщение, а частта, която изпълнява мрежови функции, изпълнявани в полза на приложението, като: трансфер на файлове, достъп до печат, обмен на съобщения и др. Изброените функции биват изпълнявани в съответствие с определени протоколи. Към протоколите на приложния слой се отнасят: FTP (File Transfer Protocol), Telnet (програма за терминална емулация), SMPT (Simple Mail Transfer Protocol), HTTP (Hypertext Transfer Protocol) и др. (5)

- **Представителен слой**

В предаващия компютър приложният протокол приема данните от потребителското приложение и ги изпраща надолу в представителния слой. Името на последния подсказва, че става дума за представяне (на данните). В представителния слой се извършва конвертиране на данните от една система на кодиране в друга с цел осъществяване на трансфера им между разнородни платформи или операционни системи, например конвертиране между кодовете ASCII (American Standard Code for Information Interchange) и EBCDIC (Extended Binary Coded Decimal Interchange Code). Представителният слой е в състояние да извършва и функции като криптиране и компресиране на данните. Представителният слой в приемащия компютър извършва обратните функции – декомпресиране, декриптиране и конвертиране на данните.

- **Сесиен слой**

Протоколите от този слой отговарят за изграждане и поддържане на сесия (комуникационен поток) между предаващия и приемащия компютър. Слоят установява и прекратява диалозите между комуникиращите приложения. Друга функция на сесийния слой е да управлява и контролира начина на

предаване – полудуплекс или пълен дуплекс. Пълният дуплекс осигурява двупосочна комуникация, при която двете страни биха могли да приемат/предават едновременно (подобно на телефонен разговор). Полудуплексът е също двупосочен, но в даден момент може да приема/предава само една от страните.

Сесийният слой би могъл да изпълнява още и функции, вързани със сигурността на данните, както и преобразуване на имена.

- **Транспортен слой**

Транспортният слой е важен елемент в мрежовите комуникации. Той управлява потока от пакети. В приемащия компютър той следи за тяхната валидност и ред на следване, като при необходимост пренарежда (сглобява) пакетите така, че да се възстанови целостта на съобщението. В предаващия компютър слоят структурира съобщението под формата на пакети и го изпраща в мрежата като поток от пакети. Друга важна функция на транспортния слой е преобразуването на имена, както и осигуряване на многозадачността на мрежовите приложения. Транспортният слой използва два типа транспортни протоколи – връзково-ориентиран и безвръзково-ориентиран.

При връзково-ориентираният протокол между предаващата и приемащата страни се създава функционална връзка за потвърждаване и отговор, посредством която приемната страна, след като получи данни ги проверява за наличие на грешка и изпраща на предаващата страна съобщение дали те са пристигнали успешно. Популярният от Интернет протокол TCP (Transmission Control Protocol) представлява връзково-ориентиран протокол.
Безвръзково-ориентираният протокол се различава от връзково-ориентираният по това, че описаната по-горе функционална връзка липсва. Приемната страна не извършва проверка на получаваните данни и не изпраща съобщение на предаващата страна дали те са пристигнали успешно. При този вид протокол няма никаква гаранция, че изпратените данни не са се загубили някъде по пътя.

Предимството му е в по-високата производителност (по-малко натоварване на мрежата и по-висока скорост на комуникация). Използва се за изпращане на кратки и прости съобщения, които не са критични по отношение на тяхната важност, например такива, които биват изпращани до всички компютри в една подмрежа едновременно. Протоколът UDP (User Datagram Protocol), който е член на комплекта TCP/IP, е безвръзково-ориентиран. Изпращаните с негова помощ съобщения се наричат дейтаграми (datagrams).

Преобразуването на имена представлява друга важна задача на транспортния слой. Транспортните протоколи TCP/IP (Transmission Control Protocol/Internet Protocol) и IPX/SPX (Internet Package Exchange/Sequenced Packet Exchange) използват логически имена на компютрите (хостовете), които биват преобразувани в логически мрежови адреси (IP-адреси), с чиято помощ се осъществява идентификацията на компютрите в мрежата. Преобразуването се извършва с помощта на мрежовата услуга DNS (Domain Name System).

Следваща важна задача на транспортния слой е осигуряването на многозадачността на мрежовите приложения. Последната позволява на потребителя да изпълнява в даден момент повече мрежови приложения едновременно, например да използва браузъра за достъп до някакъв Web сайт и в същото време да сваля e-mail писмата си от електронната поща. Сайтът и пощата пристигат на един и същ мрежов адрес – на IP-адреса на вашия компютър. За да се осъществи тяхното разделяне, протоколите от транспортния слой използват така наречените портове. Сайтът и пощата постъпват на портове с различни номера. За по-добро обяснение на ролята на портовете, тук може да бъде използвана следната аналогия. Ако приемем, че IP-адресът указва име на улица плюс номер на сградата, то портовете сочат номерата на апартаментите в сградата. Номерата на портовете са допълнение към мрежовия адрес. Всеки номер представлява 16-битово число (64536 различни порта), съдържащо се в едно от 12-те полета на 20 байтовия IP-хедър на транспортния слой. (3)

- **Мрежов слой**

Мрежовият слой отговаря за доставяне на пакетите до тяхното местоназначение. Той управлява маршрутизацията (routing). Под маршрутизация следва да разбираме изпращане на пакети от една мрежа (или подмрежа) към друга по най-ефикасния възможен път. С информацията от този слой работят два вида хардуерните устройства - маршрутизаторите (routers) и комутаторите от ниво 3 (switches of Layer 3).

Мрежовият слой изпълнява и функциите, свързани с приоритетността на данните. Данни, които изискват по-голяма пропускателна способност, каквото е например видеото, биват маршрутизирани с предимство пред останалите.

- **Канален слой**

Слоят се състои от два подслоя:

- подслой за контрол на достъпа до преносната среда (MAC – Media Access Control);
- подслой за контрол на логическите връзки (LLC – Logical Link Control).

Контролът на достъпа до преносната среда се извършва с помощта на MAC (Media Access Control) адреси. С тяхна помощ се осъществява физическото адресиране на компютрите в мрежата. MAC адресът представлява уникално шестнадесетично число, физически (хардуерно) постоянно записано в Ethernet или Token Ring мрежова интерфейсна карта (NIC – Network Interface Card).

MAC адресите в една Ethernet мрежа, наричани за краткост Ethernet адреси, биват записвани като 12 шестнадесетични цифри, подредени в 6 двойки, като всяка една от тях е отделена от останалите чрез двоеточие, като например 26:C4:2F:53:08:A4. Физически адресът представлява 6-байтово двоично число. Първите 3 байта съдържат кода на производителя (определя се

от IEEE), а последните 3 се задават от производителя и служат като идентификатор на конкретната карта. Всяка карта би трябвало да притежава свой уникален адрес, който да не се среща в останалите карти. На практика понякога някои от производителите на карти дублират MAC адресите, поради допускане на грешки или в резултат от повторно използване на 3-байтовите номера (поради тяхното изчерпване). Ако две карти с един и същ MAC адрес се окажат в една и съща мрежа, това би предизвикало проблеми.

В LLC подслоя се дефинира логическата топология на мрежата, която, както вече бе споменато (т.2.5), може да не съвпада с физическата. Той осигурява връзката на MAC подслоя със слоевете над и под него.

Хардуерните устройства, които действат с информацията от каналния слой, са мостовете (bridges) и комутаторите от ниво 2 ((switches of Layer 2), наричани още комутиращи хъбове.

- **Физически слой**

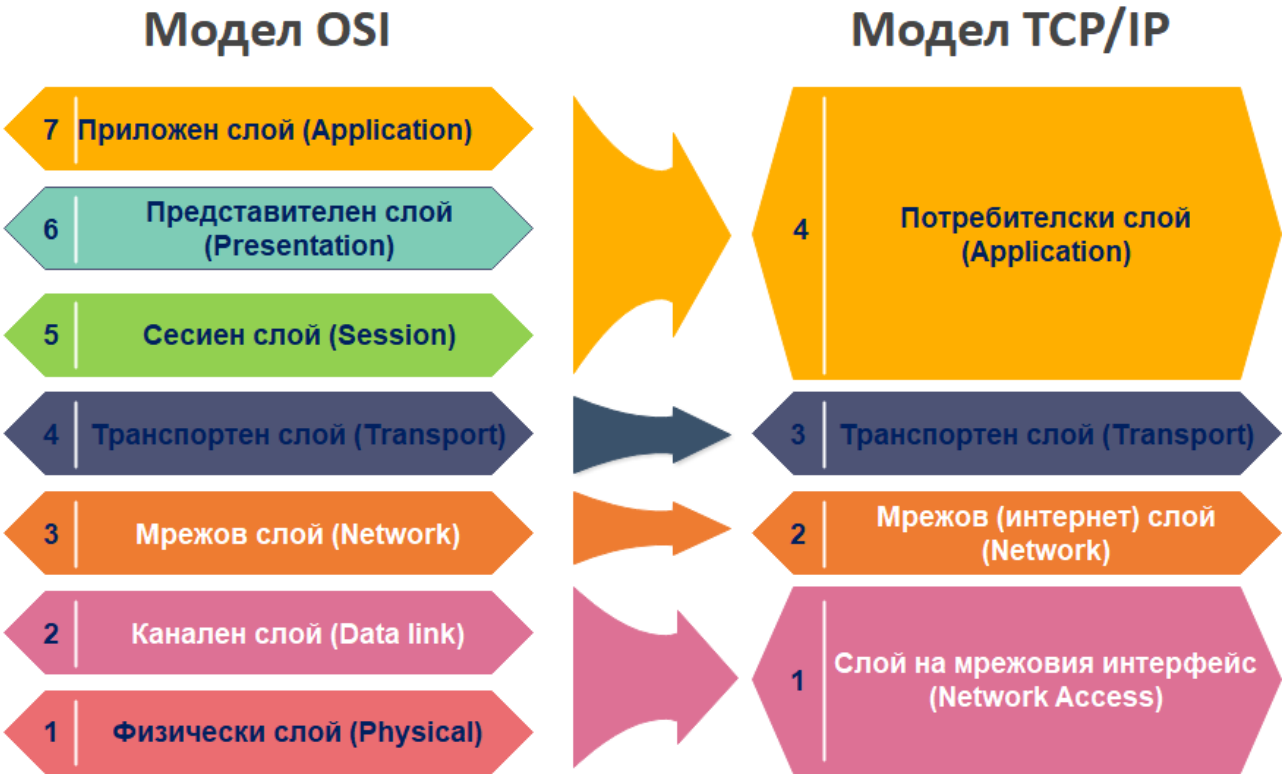
Тук данните, заедно с хедърите и трейлъра, получени от мрежовия слой, биват преобразувани в електрически или светлинни сигнали, който се предават в мрежата по кабел или безжично. Тук се взема под внимание физическата топология на мрежата.

Мрежовите карти, повторителите и хъбовете (пасивни, активни и интелигентни) са устройствата, който работят във физическия слой. Когато за комуникация се използват телефонни линии, мрежовата карта отсъства. На нейно място се използва модем. Когато два компютъра се намират близо един до друг, те могат да бъдат свързани съвсем просто (без мрежови карти или модеми) през сериийните си портове посредством сериен кабел. Такава връзка бива наричана нулев модем.

1.4.1.2. TCP/IP

TCP/IP (***T**ransmission **C**ontrol **P**rotocol/ **I**nternet **P**rotocol*) е концептуален модел на семейство от протоколи за комуникация между компютрите, който се използва в Internet и в почти всички други съвременни компютърни мрежи. Този модел се състои от много протоколи, но тъй като ключова роля имат протоколите TCP и IP, името се определя от тях. Моделът TCP/IP е създаден през 1980 г. заради необходимостта от единен начин за комуникация между компютрите, като по този начин предоставя възможност мрежите да бъдат свързвани помежду си. В модела TCP/IP информацията се пренася под формата на пакети. Често е наричан Интернет модел, а в ранните години на Интернет и DoD модел, тъй като разработването на мрежовия модел е финансирано от DARPA, агенция на Министерство на отбраната на САЩ.

Моделът TCP/IP се изгражда в съответствие с еталонния модел на слоевете. На фиг.1.1 е показано съответствието на еталонния модел с модела на TCP/IP.



Фиг.24 - съответствието на еталонния модел с модела на TCP/IP

Всеки един протоколен слой представлява съвкупност от мрежови функции:

- **Потребителски слой** – предоставя интерфейс за потребителските приложения, използващи TCP/IP за комуникация. Приложението представлява потребителски процес, който работи съвместно с друг процес на същия или на различен хост. Пример за такива приложения са TELNET, FTP, SMTP и др. Интерфейсът между отделните приложения и транспортния слой е дефиниран чрез комуникационни портове и сокети;

- **Транспортен слой** – реализира връзки от тип крайна точка – крайна точка, като множество приложения се обслужват едновременно. Транспортният слой отговаря за осъществяване на сигурен обмен на информация. Наличните два протокола за осигуряване на преноса са TCP и UDP (*User datagram protocol*). Протоколът UDP поддържа отделните мрежови услуги чрез несвързани с информационния поток комуникации. По този начин, приложенията използващи UDP като транспотен протокол, могат да реализират собствен контрол на потока от информация. Обикновено UDP се използва при приложения, които се нуждаят от бърз транспортен механизъм.

- **Мрежов слой** – този слой поддържа виртуално изображение на мрежата. Той представлява най-горният слой на физическата мрежова архитектура. IP (Internet protocol) е основният и най-важен протокол на този

слой. Той не е свързан с отделния информационен поток. Протоколът не поддържа механизми за осигуряване на надеждни комуникации, контрол на потока данни и възстановяване при грешки. Тези функции е необходимо да се реализират на по-високо ниво на комуникация. Част от информацията, обменяна между отделните компютри, е информация за маршрутизиране. Тази информация дава възможност отделните съобщения да бъдат правилно разпределени към тяхното предназначение. Тези функции за маршрутизиране се осигуряват от IP протокола. Други по-важни протоколи на мрежово ниво са ICMP, ARP и RARP.

- **Слой на мрежовия интерфейс** – той съответства на каналния слой в еталонния модел. Дава възможност за връзка към съответната мрежова апаратна част. Мрежовият интерфейс, в зависимост от изпълнението си, може да поддържа, или не, механизми за надеждно разпределение на информационния поток. Реализацията му може да бъде пакетно-ориентирана или поточно- ориентирана. На практика TCP/IP не дефинира определен протокол за това ниво, което дава възможност за по-голяма гъвкавост на изградената система. Примери за изпълнение на този слой са IEEE 802.2, ATM, FDDI и др. Най-високото ниво при модела TCP/IP са приложните протоколи. Те комуникират с приложения на друг мрежов хост и представляват видимите за потребителите интерфейси от съвкупността на TCP/IP протоколите.

Потребителските протоколи притежават някои общи характеристики: могат да бъдат създадени от отделни потребители, или могат да представляват стандартизирани приложения.

TCP/IP приложно ниво притежава приложни програми като:

- TELNET – осигуряващ интерактивен достъп до отдалечения хост;

• FTP (File Transfer Protocol) – осигуряващ висококоростен трансфер на файлове от дисково устройство към друго подобно;

• SMTP (Simple Mail Transfer Protocol) – използва се като мрежова пощенска система.

Най-долното ниво на TCP/IP модела съвпада с функциите, определени от физическото и каналното ниво на OSI. Мрежовия слой на OSI съвпада по функции и местоположение с мрежовия (интернет) слой, а транспортните нива са идентични, въпреки че според OSI транспортното ниво трябва да осигурява надеждност, а в TCP/IP има избор на протоколи дали да се осигурява надеждност или не.

Функциите на последните три нива на OSI са обединени в общото приложно ниво на TCP/IP, което означава, че самата мрежа не осигурява автоматично тези функции, а те са оставени за изпълнение на приложението, например ако е необходимо компресиране, криптиране на данни или проверка за потребителско име и парола, това се реализира не от мрежата, а от приложението.

TCP/IP моделът предшества OSI във времето, но той е важен, защото определя функционирането на най-голямата до момента компютърна мрежа – Интернет, която продължава да се развива с огромни темпове и практически достъпът до нея е навсякъде и функциите и се използват ежедневно от милиарди потребители по целия свят.

1.4.2 Мрежови стандарти

Моделите не са единствените стандарти и спецификации, по които се разработват мрежови компоненти. Множество организации за стандартизация публикуват спецификации за свързан с мрежите хардуер и софтуер. Разбира се, тези спецификации не са закон. Организациите по стандартизация не са правителствени институции и не могат да налагат задължително съответствие към дадени стандарти. Производителят е свободен да се отклонява от стандартите толкова, колкото желае, но не е в негов интерес да прави това.

Нестандартни продукти, които работят само с други продукти, произведени от същия производител, по принцип са непопулярни. В ранните дни на компютърните мрежи производителите безнаказано създаваха такива продукти, но днешната мрежова индустрия изисква съвместимост.

1.4.2.1 Спазване на стандартите

ISO дефинира стандартите като „документирани споразумения, съдържащи технически спецификации или други точни критерии, които трябва да бъдат използвани задължително като правила, указания или дефиниции на характеристики, за да гарантират, че дадени материали, продукти, процеси и услуги отговарят на целта, за която са предназначени".

Пазарът, както разбрахте, е една от причините производителите да спазват стандартите, но има и други предимства. Например стандартите осигуряват указания, които улесняват проектирането и производството на продукти, а от гледна точка на потребителя стандартизацията осигурява надеждност на продуктите и услугите.

1.4.2.1 Организации за стандартизация

ISO съществува от дълго време и е добре позната организация за стандартизация, но тя не е единствената организация, която осигурява стандартизирани спецификации за компютърни и мрежови компоненти. Някои от главните международни организации за стандартизация са следните, разгледани в следващите секции по азбучен ред:

- ISO
- IEC
- ITU
- IETF
- IEEE

ISO е световна федерация на националните организации по стандартизация с по един представител от всичките 100 различни страни. Тя е формирана през 1947 г. с цел разработване на международни стандарти в различни сфери. Един от стандартите на ISO, който много хора са виждали през годините, е ISO номерът на кутийката на фотографските филми, който показва скоростта на филма. Международните буквени кодове на страните са друг пример на работата на ISO. (5)

ISO работи в партньорство с други организации, като International Electrotechni-cal Commission (IEC), World Trade Commission (WTO) и International Telecommunications Union (ITU).

IEC съществува дълго преди ISO, още от 1906 г., но е по-специализирана. Докато ISO създава стандарти от всички видове, целта на IEC е създаването и установяването на стандарти в областта на електро и електронния инженеринг. IEC е изградена от 47 национални комитета и през 1967 г. влезе в споразумение за съвместна работа с ISO по разработката на стандарти и спецификации.

ITU е друга международна организация, усилията на която са съсредоточени върху спонсорирането на събития, публикуването на документи и установяването на стандарти за продукти и услуги, свързани с телекомуникациите.

Internet Engineering Task Force (IETF) е част от Internet Architecture Board (lAB), който от своя страна е техническа консултативна група, принадлежаща на Internet Society (ISOC). IETF е разделена на две работни групи, всяка от които решава различен проблем, свързан с изграждането на Интернет стандарти. Членството в нея е отворено; всяка заинтересована страна може да се присъедини към тази организация.

Основната задача на групите на IETF включва разработката и издаването на Интернет проекти (Internet Drafts), прерастващи в официални

документи (Request For Comments - IRFC), които от своя страна преминават през установен процес на одобрение, за да се превърнат в Интернет стандарти.

В качеството си на професионалисти по мрежи може да срещнете препратки към „RFC [номер]" за повече информация по характеристиките на определени мрежови услуги и протоколи. Тези услуги и протоколи включват такива елементи, като:

• Реализация на услугата Domain Name System (DNS)

• Разширения на TCP/IP

• Спецификации за софтуер от типа Network Address Translation (NAT)

Макар че много RFC документи произлизат от IETF, всяка заинтересована страна може да подава предложения за RFC. Не всички RFC документи описват стандарти, но ако даден документ е предназначен за стандарт, той преминава през три фази:

• Proposed Standard - предложен стандарт

• Draft Standard - пробен (проектен) стандарт

• Internet Standard - Интернет стандарт

Има дори RFC номер 2226 - „Инструкции за автори", който съдържа информация за начина на написване и форматиране на проект. След като бъде изпратен, групата Internet Engineering Steering Group (IESG), която е част от IETF, разглежда документа. След обсъждането, ако проектът бъде одобрен, той се редактира и публикува. Редакторът на RFC, назначен от Internet Society, поддържа и публикува главен списък на RFC документите. Той отговаря също за окончателното редактиране на документите. Следва преглед от техническите експерти или така наречената група „task force", по време на който RFC се класифицира в една от следните категории:

• Required Status (изискван статут) - Задължителен

• Recommended Status (препоръчителен статут) - Препоръчителен

• Elective Status (незадължителен статут) - Може да бъде реализиран, но реализацията не е задължителна

•Limited Use Status (статут на ограничено използване) - Не е предназначен за масова реализация .

• Not Recommended Status (непрепоръчван статут) - Не се препоръчва реализация

IEEE (наричан на английски „Ай-трипъл И" от членовете на индустрията) осигурява обмена на информация и разработва стандарти и спецификации за по-ниско ниво на мрежовите технологии (това на физическия и каналния слой).

От особен интерес за професионалистите по мрежи представляват спецификациите на проекта IEEE 802. Името е базирано на датата на заседанието на комитета. 80 означава годината (1980), а 2 означава месеца (февруари). Протоколите от физическия и каналния слой, за които комитетът установява стандартите 802, са следните:

• **802.1** - Въведение в стандартите: LAN и MAN мениджмънт, мостове, които действат в MAC подслоя и алгоритъмът STA (Spanning-Tree Algorithm), който предотвратява комуникационни проблеми, наречени, междумостово зациклят {bridge looping).

• **802.2** - Logical Link Control (LLC): Тези спецификации бяха предназначени за недопускане на затрупване на приемниците от изпращащите. Този стандарт се грижи за разделянето на каналния OSI слой на два подслоя, при което слоят LLC осигурява интерфейс между MAC подслоя и мрежовия слой.

• **802.3** - CSMA/CD: Тази спецификация установява правилата за работа на Ethernet мрежи, използващи метода на множествен достъп с разпознаване на носещата (честота) и откриване на колизии (CSMA/CD), и установяват стандарти за формата на Ethernet фреймовете (пакетите). Първоначално стандартът бе дефиниран като мрежа с линейно-шинна топология, използваща коаксиален кабел, но след това бе обновен за включване на 10BaseT мрежи (топология звезда).

• **802.4** - Token Bus: Задава стандарти за мрежи, реализиращи физическа и логическа шинна топология, която използва 75-омов CATV коаксиален или оптичен кабел и метод за достъп с предаване на маркер.

• **802.5** - Token Ring: Тази спецификация задава физическия стандарт и метод за достъп до преносната среда за мрежа с физическа топология звезда и логически кръг, която може да използва кабел с екранирана или неекранирана усукана двойка и метод на достъп с предаване на маркер. Този стандарт беше разработен на базата на технологията Token Ring на IBM.

• **802.6** - MAN: Задава стандарти за мрежи, които са по-големи от локалните мрежи и по-малки от глобалните мрежи.

• **802.7** - Broadband: Установява правилата за изграждане на мрежи с технологии за широколентово предаване, например CATV, използващи Frequency Division Multiplexing (FDM) за изпращане на различни сигнали на отделни честоти по един и същ кабел.

• **802.8** - Fiber Optics: Осигурява спецификации за мрежи, използващи оптични кабели - например Fiber Distributed Data Interface (FDDI).

• **802.9** - Integrated Voice and Data: Понякога наричан само „integrated services" (вградени услуги), този стандарт установява правилата за предаване на глас и данни по ISDN.

• **802.10** - LAN Security: Тези спецификации имат отношение към изграждането на виртуални частни мрежи (VPN) - начин за изграждане на сигурна връзка към частна мрежа по обществения Интернет.

• **802.11** - Wireless: Дава указания за реализиране на безжични (безкабел-ни) LAN технологии.

• **802.12 - 100 VG AnyLAN**: Този стандарт се отнася за метода на достъп с приоритет по заявка, разработен от Hewlett Packard с цел комбиниране на предимствата на Ethernet, Token Ring и ATM технологиите в едно високоскоростно решение за локални мрежи. (5)

1.5. IP АДРЕСИРАНЕ

Всеки хост в TCP/IP мрежа трябва да има уникален адрес. С тези уникални адреси, е възможно изпращането на информация от хост до хост. Всеки пакет съдържа информация за адреса в хедъра и IP адреса в хедъра се използва за маршрутизиране на пакета. Ако няколко човека на вашата улица имат един и същ адрес, това би било проблем за пощите например да сортират писмата. По аналогия IP адресите са уникални за всяка мрежа.

IP адресирането представлява конфигуриране на всеки TCP/IP хост с валиден IP адрес. За достъп до Интернет хоста трябва да има IP адрес, които не само идентифицира хоста (като адрес на къща) но също да идентифицира и мрежовия адрес (като номер/име на улицата). Администратора на мрежата трябва да поставя подходящи IP адреси, за да могат хостовете в мрежата да комуникират помежду си.

1.5.1 IP адреси

Всеки IP адреса идентифицира хоста в мрежата, точно както пощенския ви адрес идентифицира дома ви, така и IP идентифицира хоста. Може да дадем следния пример - вашия пощенски адрес се състои от 2 части. Част от него казва на пощальона на коя улица живеете, а друга част казва на кой номер от тази улица живеете. Всички адреси на вашата улица съдържат едно и също име за улица, но имат различен номер за всяка сграда. IP адресите са подобни, те могат да бъдат разделени на две части. Едната част представлява мрежата в която се намира хоста, а другата част представлява отделния хост в тази мрежа. Устройство, което притежава свой уникален IP адрес, е прието да се нарича *хост*. Адресирането в интернет се базира на IPv4 (версия 4) и новия IPv6 (версия 6).

При IPv4, понастоящем стандартен протокол за Интернет IP адресите представляват 32-битови двоични числа. TCP/IP разглежда адресите в двоичен формат, но хората предпочитат да виждат IP адресите в десетичен формат. Понеже протокола вижда двоичното, работата с IP адреси има повече смисъл когато гледате IP адреса в двоичен формат.

Състои се от четири десетични числа, разделени помежду си с точка. Числата биват наричани *октети*, защото всяко едно от тях бива представяно двоично с 8 бита. Това означава, че октетите могат да приемат стойности единствено от 0 до 255. Октетите понякога биват представяни в общ вид като w.x.y.z. Например IP адресът 11010100.10011000.00100010 .10001111 се представя в точково-десетичен формат като 212.152.34.143.

Октети:	W	X	Y	Z
IP адрес	212	152	34	143

Общият брой на IP адресите, които могат да бъдат представени с помощта на 32 бита е 2^{32} или 4 294 967 296.

Всеки IP адрес се състои от две части подобно на адреса на една сграда, който включва името на улицата и номера на сградата. Първата част на IP адреса идентифицира *мрежата*, а втората *хоста*. За компютрите (хостовете) от една и съща мрежа първата част е еднаква, но двете части заедно трябва да образуват уникална комбинация за всеки един от тях. Например в адреса 212.152.34.143 първите три октета - 212.152.34, идентифицират мрежата, а последният – 143, хоста. (5)

IPv6 е новият стандартен протокол за Интернет. При него адресите са 128-битови, което означава, че в обозримо бъдеще пространството от IP адреси ще бъде достатъчно дори и при щедро даване на *блокове от IP адреси*. Броят на различните адреси в IPv6 е равен на 18 445 618 199 572 250 625 (точно 2^{64}, или около $1{,}845*10^{19}$). Това огромно адресно пространство ще бъде рядко населено, което прави възможно отново да се кодира повече информация за маршрутизирането в самите адреси.

Адресът от версия 6 се записва с осем 4-цифрени (16-битови) шестнадесетични числа, разделени с двоеточия. Един низ от нули може да се прескочи, така че 1080::800:0:417A е същото, което и 1080:0:0:0:0:800:0:417A.

Глобалните уникални IPv6 адреси се състоят от две части: 64-битова маршрутизираща част, следвана от 64-битов идентификатор на хоста.

Блоковете от IP адреси представляват съвременен вариант на IPv4: мрежов номер, следван от наклонена надясно черта и броя на съответните битове в мрежовия номер (десетично число). Пример: 12AB::CD30:0:0:0:0/60 включва всички адреси, започващи с 12AB00000000CD3.

Освен по-голямото адресно пространство IPv6 има много други подобрения спрямо IPv4, като автоматично преномериране и повишена сигурност чрез задължително използване на стандарта IPsec. В България вече има доставчици на IPv6.

По обстойно ще разгледаме IPv4. В TCP/IP мрежите са възприети два начина за IP адресиране – класово адресиране (classful addressing) и безкласово адресиране (classless addressing). (5)

➢ Класово адресиране (classful addressing)

В хронологичен ред първо възниква класовото адресиране - адресиране посредством използване на класове. При него множеството от IP адреси се разбива на 4 различни вида подмножества. Видът на всяко едно от подмножествата определя неговия клас, а самите подмножествата биват наричани блокове (netblocks). Всеки блок спада към някой от четирите класа. За различните класове броят на блоковете е различен. Всички блокове от даден клас са с еднакъв размер (притежават еднакъв брой IP адреси). Блоковете биват предоставяни на отделните компании и организации за ползване в мрежите им. Размерът на блока определя големината на мрежата. Мрежите на по-големите предприятия получават по-големи блокове (повече IP адреси) в сравнение с тези на по-малките такива. Блоковете биват предоставяни от предназначената за целта организация IANA (Internet Assigned Numbers Authority).

В следващата таблица е показано разпределението по класове, блокове и IP адреси.

Адресен клас	Брой мрежи (брой блокове в класа)	Брой IP адреси в блока (брой IP адреси в мрежата)
A	126 *	16 777 216
B	16 384	65 535
C	2 097 152	254
D (мултикаст)	няма	няма
* Диапазонът от адреси 127.x.x.x е запазен за адреси за обратна връзка, който се използва за тестови и диагностични цели.		

Таблица 1

В клас А има 126 мрежи (блока), всяка една от които разполага с по 16 милиона IP адреса. Мрежите от клас А бяха разпределени между големите корпорации и университети, като: IBM, Hewlett Packard, Xerox, Масачузетския университет и др. Мрежите от клас В са повече на брой, но в замяна на това всяка една от тях разполага с по 65635 IP адреса. Microsoft Corporation получи мрежа от клас В. Мрежите от клас С са над 2 милиона, като всяка една от тях притежава по 254 адреса. Мрежи от клас D няма. Адресите се използват за мултикаст съобщения (съобщения, които се изпращат едновременно до повече получатели).

Поради използване на целия блок 127.x.x.x за обратна връзка, бяха загубени 24 милиона IP адреси. Отначало това не бе проблем на фона на 4-те милиарда адреси, оставащи за ползване. С течение на времето обаче всички адреси бяха заети и днес те вече не достигат.

Идентифицирането на отделните класове се определя от броя и стойностите на старшите битове на първия октет “w” в съответствие със следната таблица.

Адресен клас	Старши битове на първия октет “w”	Числени стойности в октета “w”	Брой битове за мрежовия идентификатор
A	0	0 – 127	7
B	10	128 – 191	14
C	110	192 – 223	21
D (мултикаст)	1110	224 - 239	28

Таблица 2

IP адресите от клас А се идентифицират от първия бит на октета “w”, чиято стойност е винаги 0. Адресите от клас В се определят от първите два бита на същия октет, които имат фиксирана стойност – 10. Например адресът 182.34.123.5 е от клас В, тъй като октетът “w” съдържа числото 182, попадащо

в диапазона 128 – 191. Числото 182, представено в двоична форма, има вида 10110110. Старшите два бита имат стойност 10, което съгласно таблицата означава, че адресът принадлежи на клас B.

По аналогичен начин, в съответствие с таблицата, се идентифицират адресите и на останалите два класа.

Интерес представлява последната колона на таблицата. Както вече споменахме, всеки IP адрес се състои от две части – идентификатор на мрежата и идентификатор на хоста в нея. За адресите от клас A, като идентификатор на мрежата служи първия октет “w”. Тъй като най-старшият бит в него определя класа, за идентификатора на мрежата остават 7 бита, с помощта на които могат да бъдат представени общо 128 числа - от 0 до 127. Тъй като идентификаторът 127 е резервиран за тестване с обратна връзка, а IP адресът 0.0.0.0 е запазен за представяне на всички IP адреси, общият брой на идентификаторите от клас A ще бъде 126 (виж колона 2 от първата таблица). Впрочем двата адреса 127.x.x.x и 0.0.0.0 касаят и останалите класове, което означана, че и техният общ брой на IP адресите ще бъде по-малък с 2.

В клас „B“ за идентификатор на мрежата се използват първите два октета (16 бита). Тъй като в тях двата старши бита на октет “w” служат за определяне на класа, за идентификация на мрежата остават общо 14 бита, с помощта на които могат да бъдат селектирани $2^{14} = 16384$ мрежи (виж първата таблица).

В клас C за идентификатор на мрежата се използват първите три октета (24 бита). Тъй като в тях трите старши бита на октет “w” служат да идентификация на класа, за определяне на мрежата остават общо 21 бита, с помощта на които могат да бъдат идентифицирани $2^{21} = 2097152$ мрежи (виж първата таблица).

В клас D за идентификатор на мрежата се използват четирите октета (32 бита). Тъй като в тях четирите старши бита на октет “w” служат да

идентификация на класа, за определяне на мрежата остават общо 28 бита, но както вече е известно адресите на клас D не се използват за селектиране на мрежи, а за мултикаст съобщения. (5)

- **Безкласово адресиране**

Класовото адресиране не е ефективен начин за адресация. Нека вземем за пример компания, която би желала да свърже с Интернет 1000 компютъра. Една мрежа от клас С няма да може да свърши работа, понеже максималният брой компютри в нея е 254. Следователно трябва да се използва мрежа от клас В с над 65000 адреса, а това означава, че над 64000 адреса биха били загубени. За преодоляване на подобен род проблеми бе възприето безкласовото адресиране.

Безкласово адресиране позволява разделяне не само по октети, но и по битове. За да работим с него трябва да си преговорим работата с бройни системи.

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 и 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 A
/16	Клас B
/24	Клас C

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.

Друго решение на изчерпващото се адресно пространство е въвеждането на т.нар. частни IP адреси. За да може да функционира интернет, е необходимо всеки хост, свързан към глобалната мрежа, да притежава уникален IP адрес. За мрежите, които обаче не са свързани към интернет може да се използват кои да е мрежови адреси, стига да не се повтарят вътре в самата мрежа.

Използването на кои да е IP адреси е опасно, понеже мрежата може евентуално да бъде свързана към интернет. Поради тази причина са резервирани три блока от IP адреси, които могат да бъдат използвани за адресиране на хостовете в частните мрежи. Пакети, които съдържат адрес принадлежащ на някои от тези три блока, няма да бъдат маршрутизирани от гръбначните маршрутизатори в интернет.

Частни IP адреси:

- **клас A** - 10.0.0.0/8 - от 10.0.0.0 до 10.255.255.255 (24 битов блок от адреси);
- **клас B** - 172.16.0.0/12- от 172.16.0.0 до 172.31.255.255 (20 битов блок от адреси);
- **клас C** - 192.168.0.0/16 – от 192.168.0.0 до 192.168.255.255 (16 битов блок от адреси);

Не е възможно мрежова точка (хост) с частен адрес да бъде свързана директно към Интернет. Такава връзка може да бъде реализирана единствено чрез gateway (например прокси сървър), който има валиден публичен адрес или чрез NAT устройство, което транслира частния адрес в публичен и обратно.

За опознаването на работата на мрежовия слой е необходимо познаването на основните функции на IP протокола. При него се използва дейтаграмен метод без установяване на връзка за обмен на данни. Това означава, че предаващата и приемащата страна не са установили логически канал и всяка дейтаграма се предава независимо. IP протоколът осигурява следните функции: адресиране, фрагментиране, таймаут на пакет, приоритет.

- **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 C мрежи, тогава 192.168.1.12 и 113 192.168.1.34 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.

➢ **Услугата DHCP** централизира и управлява разпределението на информация за конфигурирането на TCP/IP, като задава автоматично IP адреси и друга информация за параметрите на TCP/IP на компютри, които са настроени като DHCP клиенти. Използването на DHCP може да отстрани голяма част от проблемите, свързани с ръчното конфигуриране на TCP/IP. В това упражнение се разглеждат необходимите умения и се дава информация за инсталирането и конфигурирането на услугата DHCP. В него се разглеждат и DHCP договорите.

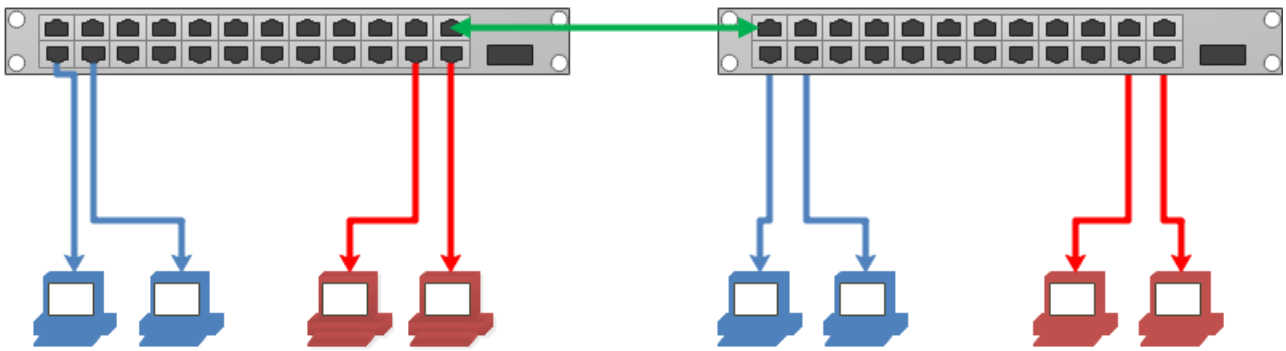
DHCP представлява TCP/IP стандарт за опростяване на управлението на IP конфигурацията. DHCP е разширение на протокола BOOTP (Bootstrap Protocol), който е базиран на UDP/IP (User Datagram Protocol/Internet Protocol). BOOTP позволява на хостовете да се самоконфигурират динамично по време на началното си зареждане. Всеки път, когато даден DHCP клиент се стартира, той иска адресна информация за IP от DHCP сървър. Тази информация включва следното:

- IP адрес,
- маска на подмрежата,
- адрес на подразбиращия се шлюз /default gateway/,
- адрес на DNS сървър,
- незадължителни параметри, като име на домейн, WINS сървър.

Когато някой DHCP сървър получи заявка за IP адрес, той избира адресна информация за IP от пул с адреси, дефиниран в неговата база данни, и предлага тази информация на DHCP клиента. Ако клиентът приеме офертата, DHCP сървърът разрешава на клиента да използва адресната информация за IP за определен период от време.

1.5.2 Виртуални локални мрежи (VLAN)

Дефиницията за Local Area Network гласи, че това е компютърна мрежа, която свързва крайните устройства в малко географско пространство – офис, сграда, фабрика, университет. Когато тази мрежа премине границата от 100 устройства, свързани в Ethernet среда, започват да се появяват проблемите. Ethernet използва broadcast съобщения, за да свърже едно устройство с друго (ARP request), и когато мрежата стане прекалено голяма, broadcast трафикът започва да доминира, като това води до забавяния по мрежата и неефективно използване на ресурсите на мрежовите устройства. За да се справи с този проблем на помощ идва концепцията за Virtual Local Area Network – VLAN. По същество – физическата локална мрежа се сегментира логически на отделни виртуални мрежи, като по този начин значително се намалява broadcast трафикът.



Фиг.25

Сегментацията се прави на мрежовите устройства, като всеки VLAN представлява един Broadcast Domain. Сините устройства (фиг.25) на графиката физически са свързани на два комутатора, но що се касае до самите устройства, за тях е все едно са свързани на един отделен, изолиран комутатор.

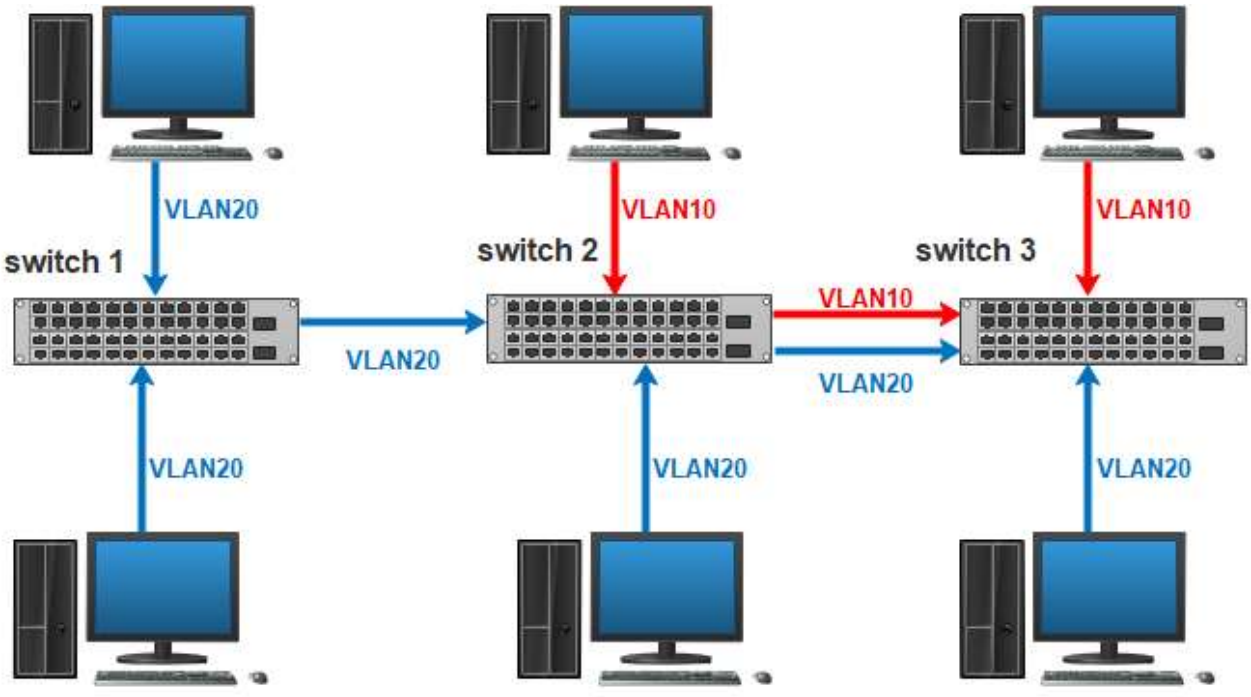
За да се осъществи връзка между сините и червените устройства е необходимо Layer 3 устройство – router или multi-layer switch.

Устройствата в един VLAN обикновено имат IP адреси от една мрежа, но е възможно да има устройства с IP адреси от различни мрежи. Това е така, защото VLAN е Ethernet (Layer 2) технология, и по същество тя има задача да дефинира границите на един Broadcast domain върху един или повече комутатори, т.е. да осигури Layer 2 свързаност между устройствата и не се интересува от работата на по-горните нива (Layer 3 IP и по-високи). (5)

Разграничаването на отделните виртуални мрежи е дефинирано в няколко стандарта, като най-използваният е IEEE 802.1Q или dot1q. Това е отворен стандарт и се поддържа от всички производители на мрежово оборудване (CISCO имат и собствен стандарт ISL, който обаче вече не се използва). Стандартът определя механизми за маркиране на отделните Ethernet фреймове на база принадлежност на различни виртуални мрежи. IEEE 802.1Q не използва отделна енкапсулация, ами вмъква VLAN етикета (tag) в едно от полетата на Ethernet фрейма. Мрежовите устройства поддържат номера на етикетите от 1 до 4096, което означава, че могат да разграничават 4096 отделни виртуални мрежи (VLANs). Виртуални мрежи с номера 1 и 1002-1005 са малко по-специални. VLAN1 се нарича Default VLAN или Native VLAN, докато VLAN1002 – 1005 са запазени за фреймове от други типове Layer 2 комуникация (Token ring, FDDI и др.) За нуждите на големите Carrier доставчици, IEEE дефинира и допълнителен стандарт 802.1ad, който позволява двойно маркиране (double tagging). Познат още като QinQ, този стандарт добавя още един етикет, което прави възможно маркирането с един 802.1ad tag

на фреймове с различни 802.1Q етикети, или на практика, устройствата, които поддържат QinQ, разграничават 4096x4096 различни етикета.

IEEE 802.1Q разграничава два типа портове на устройствата – trunk и access, като функционалността им е коренно различна: • Trunk (tagged) – фреймовете, които преминават през такъв порт в двете посоки запазват своя VLAN етикет (VLAN tag). Тези портове позволяват преминаването на фреймове от различни виртуални мрежи (VLANs) • Access (untagged) – входящите фреймове получават етикет (според конфигурацията), докато на изходящите фреймове им се премахва етикетът Крайните устройства (компютри, принтери и др.) обикновено не поддържат VLAN етикети. Затова, комутаторите махат етикетите, които отиват към крайното устройство. В обратна посока комутаторите маркират етикетите, според конфигурацията. Когато един VLAN се простира на повече от един комутатор, връзките между тях трябва да запазват етикетите - фиг.26 :



Фиг.26

Всички портове на комутаторите по подразбиране са в режим Access и първоначално принадлежат на един VLAN. Този VLAN се нарича Default VLAN или Native VLAN, и има VLAN ID 0001, или първи VLAN. Това е единственият VLAN, който преминава свободно и без етикет през всички портове на комутаторите, без тези, които са конфигурирани в режим Access в друг VLAN(!). Това означава, че VLAN1 минава през трънковете без tag и достига до другите комутатори в мрежата. В една мрежа, ако не сте конфигурирали всички портове на комутаторите и имате устройства, закачени към портове в 1ви VLAN, те ще могат спокойно да си комуникират помежду си. Или с други думи устройствата, закачени в първи VLAN на първия етаж ще виждат устройствата в първи VLAN на последния етаж от офиса, въпреки че трафикът преминава през десетки комутатора. Освен проблемите, свързани със стабилността на мрежата (голям broadcast трафик), това представлява и сериозен проблем от гледна точка на сигурността на мрежата – достатъчно е някой да се закачи към такъв порт (VLAN 1), за да види цялата информация, течаща в този VLAN. Ако портовете бяха конфигурирани да са членове на друг VLAN, същият този човек, ще трябва да отгатне номера на VLAN-а, докато VLAN 1 се знае от всички, понеже е Default VLAN на всички устройства. Затова, използването на VLAN 1 трябва да се избягва на всяка цена. Повечето производители на мрежово оборудване предоставят и начин за смяна на номера на дефолтния VLAN, което още повече затяга сигурността на мрежата. Добрите практики съветват да се конфигурира Default VLAN с номер, различен от 1, и всички неизползвани портове на комутаторите да се конфигурират да са от тип Access с VLAN номер, различен от тези, които реално ползвате в мрежата.

ГЛАВА ВТОРА II. Проектиране и изграждане на локална компютърна мрежа за нуждите на голяма организация.

2.1 Задание за изграждане на мрежата.

В ново изградена пет етажна сграда на организацията е необходимо изграждане на съвременна инфраструктура на информационната система която да осигури :

- модерна информационна инфраструктура, която да осигури всички необходими ресурси за нормалната работа на големия брой потребители;
- осигуряване на инфраструктура, лесна за управление от наличния малък брой системни администратори;
- осигуряване на защита на данните от случайна загуба, целенасочено унищожаване, външни атаки и други опасности;
- актуалност на закупените активи за минимум 7 годишен период;
- непрекъснатост на работата.

Необходимите компоненти на IT инфраструктурата могат да бъдат условно разделени на следните нива:

- структурна кабелна система (СКС)

- мрежово оборудване, включително защита на мрежата; сървърно оборудване за инфраструктурата за споделени услуги;
- сървърно оборудване за изграждане на инфраструктурата за виртуални потребителски компютри;
- система за архивиране и бекъпиране;

2.2 Проектиране на структурната кабелна система (СКС)

Проектът осигурява изграждане на СКС, съобразено с изискванията на международните стандарти ISI/IEC IS 11801, ANSI/TIA/EIA 568-A, EN 50173, при спазване на европейската директива 89/336/EEC и 2004/108/EC за електромагнитна съвместимост.

Пасивните компоненти, използвани за изграждане на СКС, са от производител, издаващ директно гаранция за параметрите на СКС, за срок не по-малък от 20 години.

Структурната кабелна система на сградата се изгражда с йерархична звездообразна архитектура и включва:

- централен (сграден) разпределител (включва и оборудване за етажно разпределение за близкостоящите помещения);
- магистрално окабеляване (гръбнак), осигуряващо скорост на обмен 10 Gbps: радиално от централния към етажните разпределители, изпълнено с медни двойноекранирани кабели 4x S/FTP Cat.7 и многомодови оптични кабели OM3 8 влакна (1x FO OM3 8f); допълнително, разпределителите на всеки етаж са свързани помежду си с 2x S/FTP cat.7 и 1x FO OM3 6f. Дължините на медните връзки от централния към етажните разпределители не надхвърлят 90м.
- етажни разпределители;
- хоризонтално окабеляване, изпълнено с медни екранирани кабели Cat.6A, осигуряващо скорост на обмен до 10 Gbps;
- телекомуникационни крайни точки - основно двойна комуникационна розетка с екранирани вложки RJ-45 Cat.6A и Cat.5 .
- частта за пренос на глас (телефония): за използване на съществуващото оборудване (хибридна/аналогова/IP АТЦ), централния репартитор реглетен тип е свързан с етажните разпределители с многочифтови екранирани телефонни кабели,

осигуряващи по два чифта на извод / работна точка, като в етажните разпределители многочифтовите кабели са терминирани на 50- или 25-портови телефонни панели. Хоризонталното окабеляване е изпълнено с медни екранирани кабели Cat.5, терминирани на 24-портови патч панели; осигурява преминаване към IP-телефония или, при необходимост, обмен на данни със скорост до 1 Gbps. Мрежата физически е отделена (в отделен разпределител). Отделена е и мрежата на охранителната система, която обхваща помещенията на охранителните органи, мониторинговия център (системата за видеонаблюдение) и работните точки на обслужващия банков офис.

2.2.1 Централни разпределители (сървърни помещения)

В 19" комуникационни шкафове се разполагат изводите на вертикалното окабеляване, опорни комутатори, маршрутизатори/защитни стени, сървъри и архивиращи устройства, интерфейсно оборудване за връзка с външни мрежи и доставчици на услуги.

Централния разпределител е разположени на третия етаж в сървърното помещение. Централните разпределители включват и оборудване за етажно разпределение за близкостоящите помещения.

Телефонните централи и централните репартитори на сградата се разполагат на същия етаж в отделно помещение в непосредствена близост до сървърното помещение.

Електрозахранването на централните разпределители, сървърните помещения (активно оборудване) и АТЦ, а така също разпределител на охранителна система с регистрираща апаратура и работни станции за видеонаблюдение, е резервирано с UPS-и средна мощност. Те са монтирани в сървърните шкафове, еднофазни, с твърда връзка към ел. табла и са окомплектовани с платки за мрежово управление и външни датчици за следене на температура и влажност в сървърните помещения. Климатизацията на

помещенията е с резервирано захранване. В сървърните помещения трябва да се поддържат температура в обхвата от 18°C до 24°C и относителна влажност от 30% до 55% и да се осигури минимална осветеност 500lx.

Централните разпределители са свързани помежду си с комбинирани връзки за скорости до 10 Gbps: оптичен многомодов кабел 50/125 OM3 с шест влакна, изведен на съединители SC в оптични панели, и два екранирани медни кабела S/FTP AWG23 Cat.7, изведени на портове RJ-45 Cat.6A в патч-панели. Шкафовете на двете АТЦ също са свързани помежду си с оптичен многомодов кабел 50/125 OM3 с 4 влакна и два екранирани медни кабела S/FTP AWG23 Cat.7.

2.2.2 Магистрално (вертикално) окабеляване.

Същите комбинирани връзки се използват за изграждане на вертикалното окабеляване (гръбнака), свързващо радиално централните разпределители с всеки от етажните разпределители в сградата (оптични многомодови кабели 50/125 OM3 с поне осем влакна (четири основни + две резервни + две за IP-телефония в перспектива), изведени на съединители SC в оптични панели, и по четири екранирани медни кабела S/FTP AWG23 Cat.7, изведени на портове RJ-45 Cat.6A в патч-панели). Вертикалните трасета са избрани в близост до централните разпределители, което осигурява дължини на медните връзки от вертикалното окабеляване, не надвишаващи максимално допустимите 90м.

Магистралното окабеляване на частта за пренос на глас (телефония) осигурява функционирането на две телефонни централи. За използване на съществуващото оборудване (хибридна/аналогова АТЦ), всеки централен репартитор реглетен тип е свързан с етажните разпределители с многочифтови екранирани телефонни кабели, осигуряващи по два чифта на извод / работна точка, като в етажните разпределители многочифтовите кабели са терминирани на 50- или 25-портови телефонни панели. Частичното или пълно преминаване

на IP-телефония се осигурява от част от ресурса на описаните по-горе комбинирани оптични/медни връзки и чрез предвиждане на свободни места за комутатори с PoE за захранване на IP-телефони, в етажните разпределители.

2.2.3 Етажни разпределители.

Съдържат пасивно и активно мрежово оборудване, осигуряващо свързаност между магистралното окабеляване (от опорните комутатори) и хоризонталното окабеляване (към работните точки). Разполагат се в определени за целта помещения, защитени от неоторизиран достъп, с осигурена подходяща осветеност, влажност до 60%, температура в диапазона от +10° до +30°. Оборудването се инсталира в 19" комуникационни шкафове. Комуникационните шкафове са специфицирани съобразно необходимото пасивно и активно оборудване, като при повече от 120 комуникационни извода шкафовете са с увеличен габарит, 800x600мм. При наличие на два разпределителя на етаж, между тях се изгражда комбинирана връзка 10 Gbps: оптичен многомодов кабел 50/125 OM3 с шест влакна, изведени на съединители SC в оптични панели, и два екранирани медни кабела S/FTP AWG23 Cat.7, изведени на портове RJ-45 Cat.6A в патч-панели, което осигурява възможност за стекиране на етажните комутатори.

В шкафовете на разпределителите на СКС се разполага също и оборудване на други слаботокови подсистеми – видеонаблюдение, информационна система, мрежа на биометрични датчици. Необходимото пространство е отчетено при оразмеряването на шкафовете, а в спецификацията за СКС са включени патч-панелите, необходими за терминиране на тези подсистеми. В спецификацията са добавени и три стенни шкафа – един към залата за видеоконференции, свързан към централния разпределител на с оптичен кабел 50/125 OM3 с шест влакна (четири изведени), и два шкафа за оборудване за видеонаблюдението.

Електрозахранването на етажните разпределители се резервира с локални UPS-и ниска мощност, от 800VA до 1600VA, с височина 2U - подходящи за монтаж в шкаф 19“, с предвидено допълнително свободно пространство 2U в тези от шкафовете, изискващи допълнителна мощност при добавяне на комутатори с PoE, поддържащи IP-телефони.

Тъй като СКС е изцяло екранирана, комуникационните шкафове на централните и етажните разпределители са свързани към сградната система заземление, със съпротивление не по-голямо от 4 Ω. В окомплектовката на комуникационните шкафове има предвидени заземителни шини и щипки, необходими за заземяване на всички патч-панели и корпуси на активното оборудване.

2.2.4 Хоризонтална кабелна система.

Свързва разпределителните шкафове с работните точки. Окабеляването за пренос на данни се изпълнява с екранирани медни кабели U/FTP, F/FTP или S/FTP, AWG23, категория 6A, изведени на екранирани портове RJ-45 Cat.6A в патч-панели и в розетките на работните точки. Свързващите и аранжиращи кабели са екранирани, Cat.6A. Окабеляването за пренос на глас се изпълнява с екранирани медни кабели F/UTP, AWG24, категория 5, изведени на екранирани розетки RJ-45 Cat.5 в кутиите на работните точки. Терминирането на хоризонталните кабели за пренос на глас в етажните разпределители се извършва на екранирани 24- или 16-портови патч.панели Cat.5, които се свързват чрез патч-кабели към 50-портовите телефонни панели на многочифтовите вертикални кабели или към комутатори с PoE в случай на внедряване на IP-телефония.

2.2.5 Крайни работни точки.

На всяко работно място се осигуряват излази от мрежите за данни и за глас в двойна комуникационна розетка с екранирани вложки RJ-45 Cat.6A и Cat.5, разположена в група заедно с 2 контакта тип „Шуко“ общо захранване и

2 контакта тип „Френски“-червени от резервирано захранване. Категорията на вложките RJ-45 съответства на категорията на кабелите, които терминират. Където това е възможно, контактните групи са стенни в конзоли за гипс-картон, разположени на 40 см от пода. В помещения с висока плътност на работните места се предвижда използване на парапетен кабелен канал (примерно, 120х55мм) за монтаж на модули 45х45мм. Парапетният кабелен канал осигурява изтеглянето на комуникационните и захранващите кабели, с разстояние помежду им по-голямо от 50мм, с възможност за фиксиране местата на контактните групи по дължината на канала в съответствие с реалната мебелировка на помещенията. В отделни помещения е предвидено използване на подови контактни кутии, с изтегляне на кабелите в гофрирани тръби в подова замазка.

В повечето работни помещения са осигурени в контактни групи по една двойна комбинирана розетка за всяко работно място, една двойна комбинирана розетка за свързване на мрежови принтери, факсове и пр. и една единична розетка, свързана към към кабелната подсистема за данни.

Предвидено е по една допълнителна и 3 резервни крайни точки за следните помещения: зала за видеоконферентна връзка, многофункционална зала, информационен център, регистратури, секретари, деловодство, компютърна обработка и статистика.

2.2.6 Инсталация на СКС

Кабелите на СКС се изтеглят и полагат, съблюдавайки изискванията и ограниченията на стандарта ISO/IEC 11801, които осигуряват запазване на техните характеристики:

- при изтегляне е недопустимо триене на кабелите в остри ръбове;

- максималната сила на теглене на кабел S/FTP и U/FTP да не надхвърля 100N (около 10кг) а на оптичен кабел 1000N (около 100кг);

- за кабели S/FTP минималният радиус на огъване е ≥ 8 пъти външния диаметър при теглене и ≥ 4 пъти външния диаметър при полагане, а за оптичните кабели минималният радиус на огъване е ≥ 20 пъти външния диаметър.

Кабелите се полагат по метални кабелни скари над окачен таван, между централните и етажните разпределители и по коридорите от етажните разпределители към крайните работни точки; в работните помещения кабелите влизат над окачен таван в гофрирани PVC тръби и се изтеглят в гофрирани тръби зад гипс-картон до конзолите на контактните групи.

При присъединяване на кабелите се спазват следните ограничения: Оптичните кабели трябва да са защитени от всякакви механични въздействия, способни да нарушат защитната им обвивка. За медните кабели S-FTP: минимално разстояние до силови кабели с мощност до 2kW е 50mm, а до луминесцентни лампи – 150 mm; при присъединяване максималната дължина на разплитате на усуканата двойка е 13 mm, а максималното разстояние между краищата на отделни двойки е 40 mm.

2.2.7 Безопасност, хигиена на труда и пожарна безопасност

До работа със системата се допускат лица, запознати с устройството и принципа на работа.

Монтажните работи да се извършват при изключено напрежение.

Всички монтажни работи да се извършват с изправни инструменти.

При монтиране на съоръжения на височина да се спазват изискванията и правилата за безопасност със стълби.

Всички модули заложени в настоящия проект са безопасни за обекта.

2.3 Мрежово оборудване и изграждане на комуникациите

2.3.1 Активно мрежово оборудване.

- **Опорни комутатори** :

Стек от 10Gbps L3 комутатори (фиг.27)**:**

2x Dell Networking N4064F, 48x 10GbE SFP+, 2x 40GbE QSFP+ Ports, lx Modular bay, 2x AC PSU, 10 to PSU Airflow - 210-ABVW1

2x Dell Networking N4064, 48x 10GBASE-T, 2x 40GbE QSFP+ Ports, lx Modular Bay, 2x AC PSU, 10 to PSU Airflow - 210- ABVU

Осигуряват следния брой портове в стека:

96x 10/1 Gbps Ethernet SFP+ изпълнени с два комутатора Dell Networking N4064F

96x 10000/1000/100 Mbps Ethernet RJ-45 изпълнени с два комутатора Dell Networking N4064

Необходимите портове за реализиране на решението са:

24 x 10Gbps връзки за свързване на етажните стекове - 6 етажа (-1, 1 2, 3, 4, 5) x 4 10Gbps връзки

28 x 10Gbps връзки за свързване на сървърите (3 за виртуализация и 4 за VDI, всеки с по 4 10Gbps връзки)

6 x 10Gbps връзки за свързване на дисковия масив 4 x 10Gbps връзки за свързване на „Дисково пространство за системата за бекъпиране и архивиране“

4 x 10Gbps връзки към системата за защита на мрежата NextGeneration Firewall (защитна стена)

2 x 10Gbps връзки към management комутатор

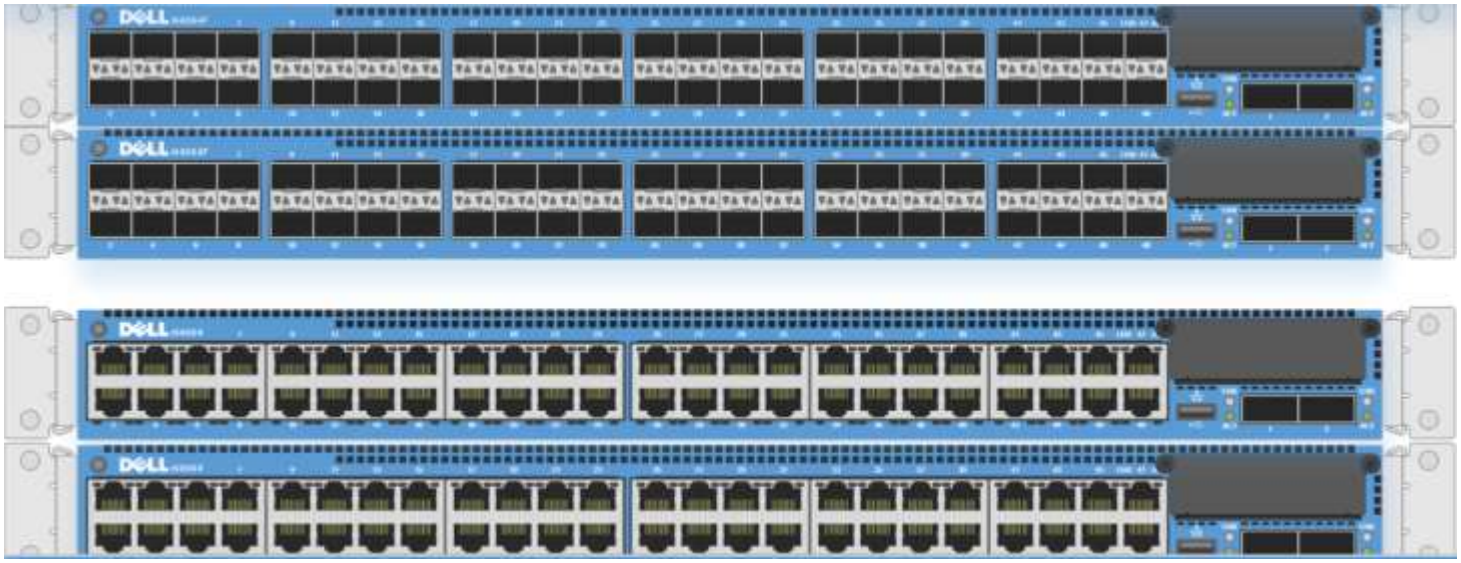
За защита от прекъсване на работата е осигурено резервирано захранване: осигурени са 2 x AC захранвания стандартни + 2 x Power Cord, PDU (Rack) - 450-ACSU

Спирането на компонентите от стека или шасито, няма да води до загуба на връзка с нито един компонент на останалото оборудване (сървъри, дискови масиви, етажни комутатори и др.) или загуба на управлението на стека/шасито - автоматично превключване между връзките в LAG (Link aggregation group) групата и поемане на управлението на стека от работещ комутатор, ако отпадналия комутатор е бил управляващ.

Функционални изисквания към стека:

От стека ще бъдат изградени минимум следните връзки:

- 4x10 Gbps към всеки един от 7те сървъра
- 4x10 Gbps към дисковия масив + 2 резервни
- 4x10 Gbps LAG (Link aggregation group) към всеки от етажните стекове
- 4x10 Gbps към системата за защита на мрежата
- 4x10 Gbps към дисковото устройство за бекъпиране и архивиране
- Други (2x10 Gbps към management комутатор)



Фиг.27 – Стек от 4 комутатора 2xDell Networking N4034F & 2x Dell Networking N4064

- **Етажни комутатори**

Етажни комутатори 21бр. Dell Networking N1548 (фиг.28)

Брой портове: 48 x 1000/100/10 Mbps Ethernet RJ-45 2x10 Gbps Ethernet за връзка с опорните комутатори и 2x10 Gbps Ethernet конфигурирани като 2 стек порта - 40 Gbps Full Duplex (2 x lOGbps x Full Duplex)

Фиг.28 – Етажни комутатори 2xDell N1548

Защита от прекъсване на работата:

За всеки комутатор: 1x RPS720 External Redundant Power Supply (Non-POE) Up To 4 Switches - 450-ADHV и 2x Power Cord, PDU (Rack) - 450-

ACSU. Спирането на компонент от стека или шасито, не води до загуба на връзка с на стека с опорните комутатори или загуба на управлението на стека/шасито. Тъй като резервираното захранване е за всеки комутатор по отделно, а не за стек, всеки комутатор се доставя със собствено резервирано захранване.

Функционални изисквания:

От стека ще бъдат изградени следните връзки:

- 4x10 Gbps към опорните комутатори
- 2 x. 10 Gbps x Full Duplex между компонентите на стека
- 1 Gbps към крайните устройства
- 1 Gbps към WiFi Access Points

- **Защитна стена - Next-Generation Firewall**

Реализирана е с 2x Dell SonicWall NSA4600 (фиг.29) - две устройства в High Availability двойка.

Налични ethernet портове:

2x10 Gbps SFP+ порта за връзка с опорните комутатори

4 x SFP 1 Gbps за връзка с Internet провайдери (с поддръжка на SMF трансивъри) или други нужди според архитектурата на Възложителя

12 x 1000/100/10 Mbps Ethernet RJ-45

1 x Ethernet Management port свързан към management комутатора

Производителност :

- класически firewall - 6 Gbps

- application firewall - 2 Gbps
- deep packet inspection - 800 Mbps
- encrypted packet inspection - 500 Mbps (включва и лицензa за Deep Packet Inspection – SSL

Функционалност:

Поддръжка на целия брой необходими VLAN за мрежата на организацията. Поддръжка на voice протоколи - VoIP Granular QoS control, VoIP Bandwidth management, DPI for VoIP traffic, H.323 gatekeeper and SIP proxy Load balancing или разпределение на трафика между два провайдера в зависимост от режима на работа.

Лиценз - TotalSecure-Comprehensive Gateway Security Suite (DPI included) с 3 годишна поддръжка за:

- антивирусни проверки на трафика
- противодействие на шпионски софтуер
- intrusion prevention
- управление на приложенията
- контрол и филтриране на съдържанието
- класически firewall
- deep-packet inspection - вкл. на криптирани пакети

Фиг.29 - Next-Generation Firewall реализиран с с 2x Dell SonicWall NSA4600

- **Безжична мрежа - Wi-Fi Access System - 31 броя**

31 (30 + един резервен) Dell SonicPoint N2 with PoE Injector (фиг.30)

Резервирано централизирано управление инсталирано върху Dell SonicWall NSA4600 appliance с лиценз за 64 устройства

Сигурност:

Security: WEP, WPA, WPA2

Ciphers:TKIP, AES, 64/128/152-bit WEP

Wireless Authentication: Open (no password), PSK, SSL VPN Enforcement

Wireless IDP (Intrusion Detection and Prevention) MAC Filtering Wireless Guest Services Lightweight Hotspot Messaging.

Функционалност:

Всички настройки и политики могат да се задават централизирано през централизираната система за управление.

Потребител свързан към Wi-Fi остава свързан при преминаването от едно AP към друго.

Устройства поддържат режим на до 8 Virtual Access Points (VAP). Това позволява всяко едно от устройствата да бъде конфигурирано да излъчва 6 SSID, всеки със своите права на достъп:

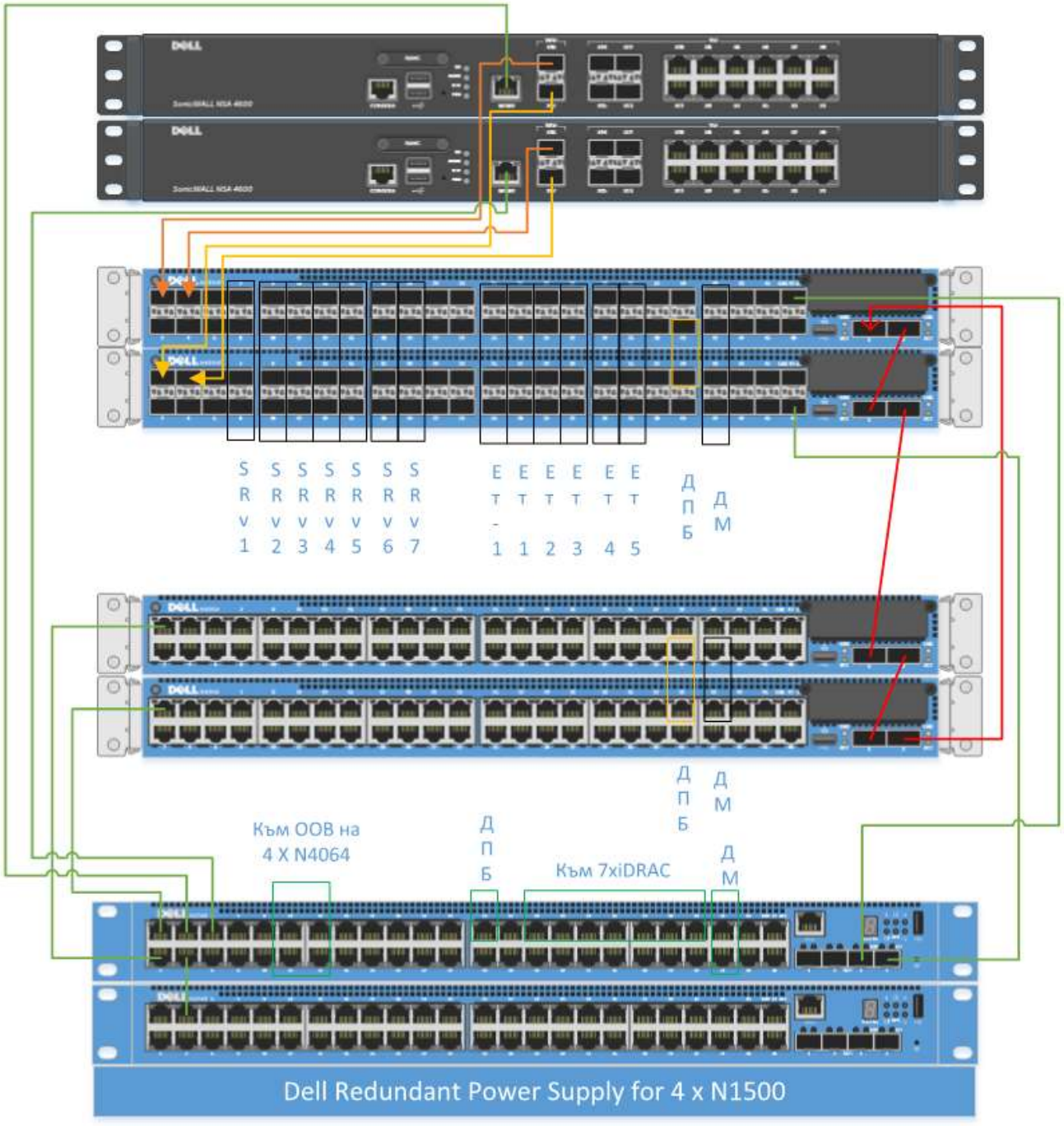
- Системни администратори
- Ръководство
- Вътрешни потребители
- Регистрирани потребители
- Гости
- Резервно

Фиг.30 - Dell SonicPoint

2.3.2 Изграждане на комуникациите

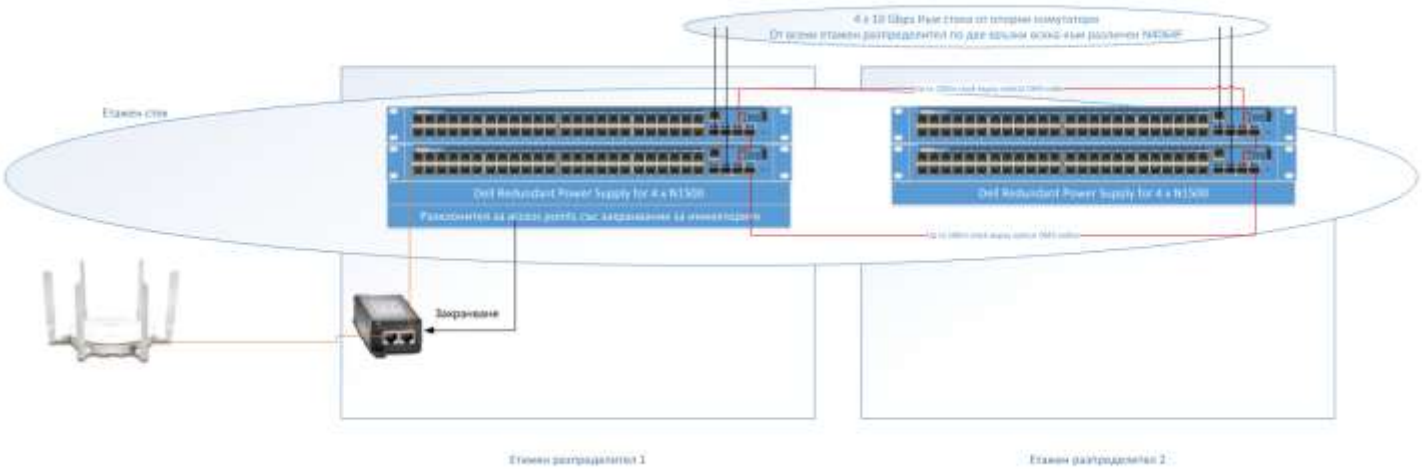
На базата на така изградената СКС и избраното активно мрежово оборудване са изградени следните комуникации :

А. Всички връзки в централната точка между сървъри, дисков масив, комутатори, защитни стени са на 10 Gbps. Тези връзки са реализирани по начин, че спирането на комутатор или проблем в кабел не трябва да води до прекъсване на връзката на цитираните по-горе устройства. Тези комутатори са обединени във високоскоростен стек. Всички портове за управление на цитираните по-горе устройства са свързани към отделен management комутатор с характеристиките на етажните комутатори(фиг.31). Всички комутатори са Layer 3 с дублирани захранвания



Фиг.31 Опорни комутатори и мениджмънт комутатор

B. На всеки етаж (без етаж -1) са разположени по два етажни разпределителя свързани към централната точка и по между си по оптични трасета с multimode кабели OM3(фиг.32). На всеки един етаж по наличните хоризонтални оптични трасета е изграден широк стек на база 2 x 10 Gbps (40 Gbps FullDuplex). Връзките на етажния стек към централната точка стават през LAG изграден от 2 x 10 Gbps оптични трасета от всеки един етажен разпределител (80 Gbps Full Duplex на етаж). Всички връзки са активни и балансирани. Използването на Spanning Tree или други active/passive протоколи не се допуска, освен за защита от грешки. Срив в една част от мрежата или единично трасе не трябва да води до прекъсване в друга нейна част;



Фиг.32 – стек етажни разпределители

C. От централната точка по положените оптични кабели се осигурена 2 x 2 x 10 Gbps Ethernet връзка до всеки един от етажните стекове от комутатори. Две от линиите водят към едното помещение на етажа, а другите две към другото помещение. Връзката работи в режим на разпределение на натоварването и взаимна защита на четирите линии от прекъсване;

D. Етажните стекове обединяват комутаторите от различните помещения на етажа, като осигурят при прекъсване на кабел от централната точка до определено помещение, комутаторите в това помещение да запазят връзката с централната точка през хоризонталните стек връзки. Ако се конфигурира повече от един стек на етаж, то за всички трябва да се спазва условието да са свързани с централната точка през две помещения, всяко с 2 x 10 Gbps (общо 4 x 10 Gbps). Връзката в стека трябва да е 80 Gbps full-duplex.

E. Етажните комутатори са еднакви, 48 порта 1 Gbps усукана двойка и 4 порта 10 Gbps SFP+. Разпределението на етажните комутатори е:

Помещение	Шкаф	Портове Cat.6A	Комутатори
Етаж 5	R52	46	1
Етаж 5	R51	52	2
Етаж 4	R42	91	2
Етаж 4	R41	117	3
Етаж 3	R32	25	1
Етаж 3	R31	38	1
Етаж 2	R22	68	2
Етаж 2	R21	63	2
Етаж 1	R1	103	3
Етаж -1	R0	31	1
Етаж -1	R16	156	3
		Общо:	21

F. В мрежата са дефинирани VLAN-и за различните функционални звена. Маршрутизацията ще се осъществява на централно ниво съгласно най-добрите практики съгласувани на етапа на изпълнение. По време на инсталирането на инфраструктурата се конфигурира цялото оборудване по начин осигуряващ различните функционални звена, потребители и трафик (за управление и наблюдение, между устройствата на инфраструктурата, на вътрешните потребители, на регистрираните потребители, на гостите и други дефинирани на етапа на изпълнение и др.) да работят в собствен VLAN. Layer 3 комутацията между отделните VLAN става в централната точка. Собствени VLAN са предвидени и за споделените устройства – принтери, WiFi access point, публични монитори и др. Всички VLAN портове, към които е свързано крайно устройство работи в Isolated mode;

G. В отговор на инициативата свободен достъп до WiFi, в публичните места на сградата е осигурен 802.11 безжичен достъп с централизирана точка на управление, позволяваща налагане на политики за достъп от едно място и филтриране на трафика при необходимост. Тези WiFi точки осигуряват достъп само до Интернет. При необходимост на устройство в WiFi мрежата за достъп до вътрешните ресурси на ще става само през VPN.

H. Цялата мрежа предоставя защитен достъп до Интернет през дублирана двойка от Next-generation firewall (NGFW). Защитната стена осигурява защитен достъп до другите сгради на организацията и до два Internet провайдера. При нормална работа на системата публичния Internet трафик се насочва към единия провайдер, а останалият към другия. При проблем с някоя от връзките трафикът изцяло се пренасочва по работещата връзка. Въпреки тази схема защитната стена разполага с възможност за пълен load-balancing между двете връзки. Производителността на защитната стена е достатъчна за пълна инспекция на всички пакети, включително deep packet inspection.

Производителността на защитната стена трябва да е достатъчна за да обслужва без забавяне на целия Internet трафик генериран от служителите в сградата, зоната за свободен достъп и връзките с другите сгради. Връзката ѝ към опорната мрежа става по резервирани 10 Gbps връзки.

2.4 Избор на сървърно оборудване за виртуалната инфраструктура за споделени услуги.

2.4.1 Сървъри за виртуализация на инфраструктурата за споделени услуги

Изградена е система от 3x Dell PowerEdge R730 model XD Generation 13, сървъра (фиг.33) всеки със следните характеристики:

Процесори: 2x Intel Xeon E5-2640 v4 2.4GHz,25M Cache,8.0GT/S QPI, Turbo, HT, 10C/20T (90W) Max Mem 2133MHz - 338-BJDL

Оперативна памет: 8x 16GB RDIMM, 2133 MT/s, Dual Rank, x4 Data Width - 370-ABUG

Постоянна памет: Dual 16 GB Flash in hardware mirror, съобразени с поддържаните от VMWare hypervisor носители:

- Redundant SD Cards Enabled - 385-BBCF, 2 x 16GB SD Card For IDSDM - 385-BBII
- Chassis with up to 12 + 4 Internal, 3.5” Hard Drives and 2, 2.5" Flex Bay Hard Drives - 350-BBEX
- Quad 600GB SAS (2 front, 2 rear flex-bay), 12 Gbps, 15 krpm (SAS), hot-swap, in hardware RAID 10 - конфигурирани за VM swap пространство:
- 2x 600GB 15KRPM SAS 12Gbps 2.5in Hot-plug Hard Drive,3.5in HYB CARR - 400- AJRV
- 2x front 6 TB NLSAS, hot-swap в хардуерен RAID 1 - конфигуриран като non-shared дисково пространство.

- 2x 600GB 15KRPM SAS 12Gbps 2.5in Flex Bay Hard Drive - 400-AJRI 2 x 6TB 7.2K RPM SATA6 6Gbps 512e 3.5in Hot-plug Hard Drive, 13G - 400-AGMM

RAID контролер:

Dell PERC (PowerEdge RAID Controller) H730P - SSD/SAS/SATA 12 Gbps, 2 GB protected cache с кабели за всички гнезда за дискове Възможност за конфигуриране в Pass-through access до дисковете.

Захранване:

Двойно, сменяемо без спиране, съобразено с конфигурацията на системата: Dual, Hot-plug, Redundant Power Supply (1+1), 750W, Titanium, 200-240VAC - 450- AD WT, 2x C13 to C14, PDU Style, 10 AMP, 6.5 Feet (2m), Power Cord - 450-AADY

Монтаж: За 19” рак, с подвижни релси и средства за подвеждане на кабелите - cable management arm.

Инфраструктурата за споделени услуги е реализирана като виртуалната инфраструктура, реализирана по схема „гарантиран клъстер от физически сървъри“ - дори при отпадане на един сървър системата да продължи да бъде в клъстер. Ключовите виртуални машини трябва са така конфигурирани, че да продължават работа дори при спиране на два сървъра.

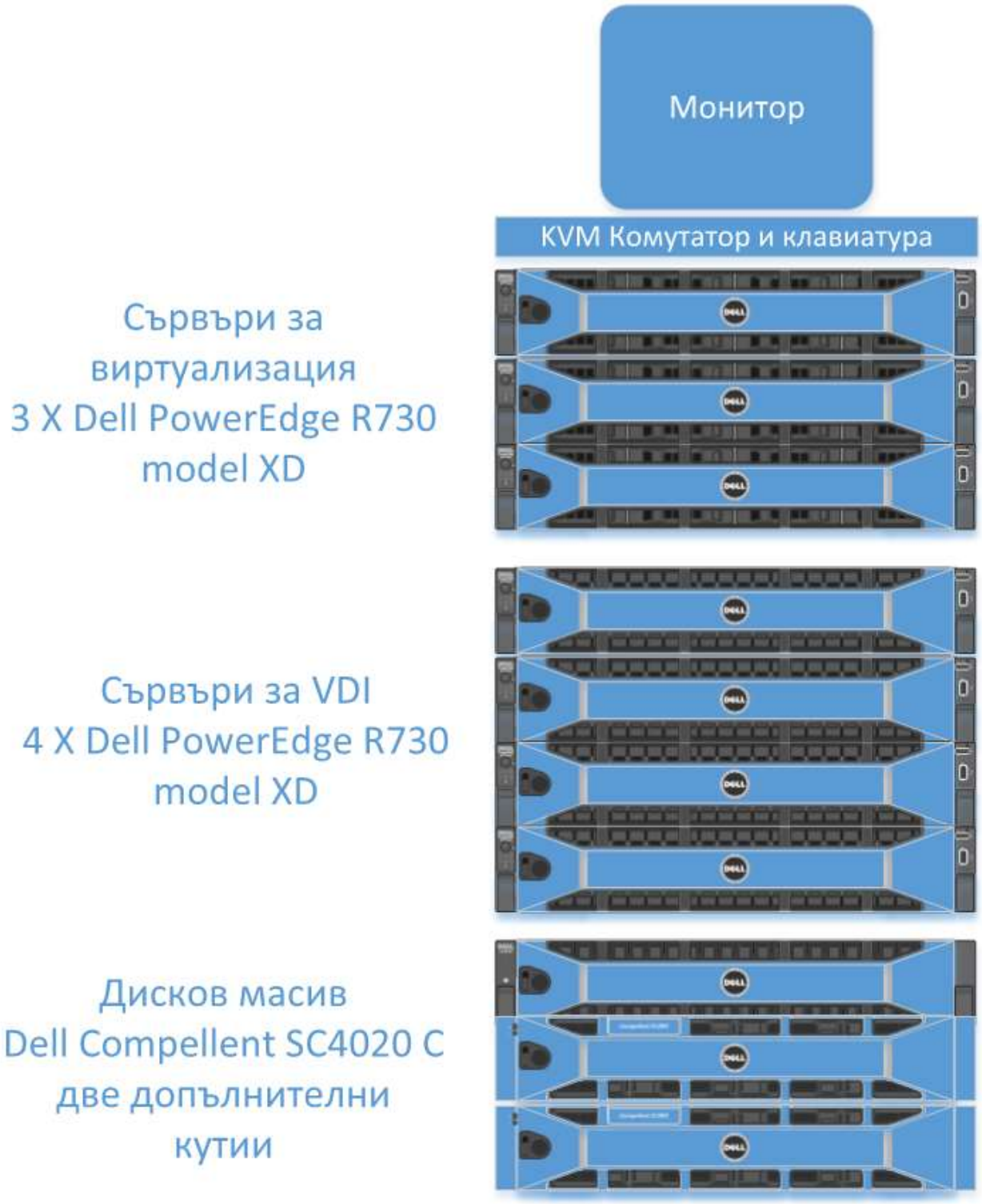
Отделните физически сървъри са машини само с хардуерно резервирано флаш пространство за зареждане на hypervisor. Техните ресурси трябва да бъдат така изчислени, че при спиране на един от тях да се гарантира, че предоставяните от тях услуги ще продължат работа без съществена промяна в производителността, а при спиране на два сървъра, отново няма да има спиране на услуги. Виртуалните машини трябва да бъдат така конфигуриране, че при сместването им на един сървър най-важните да получат приоритетно ресурси. Системата за виртуализация трябва да осигурява автоматично

стартиране на виртуалните машини при срив без човешка намеса. Местенето на една виртуална машина от сървър на сървър не трябва да води до спиране на работещите на не я приложения.

Минималната конфигурация трябва да бъде 128 GB ECC RAM с възможност за разширение, двупроцесорна машина с производителност над 800 SPECint_rate2006, 4 x 10 Gbps за SAN и LAN, 2 x 1 Gbps за управление на виртуализацията, резервирани захранвания. Сървърите трябва да разполагат с 1 Gbps Ethernet порт за управление, който да позволява отдалечена работа на администратора без разлика с действителното му присъствие при сървърите. Поради оповестената промяна в лицензионния модел на Microsoft процесорите трябва да са с минимален брой ядра. За да могат да се запускат неограничен брой машини, включително за защита на другата сграда на СРС, всеки един сървър трябва да има лиценз за Windows Server 2012 Datacenter.

Системата за виртуализация, заедно с придружаващите я продукти, трябва да осигурява непрекъсната работа на всички необходими виртуални машини в инфраструктурата на сградата. Тя трябва да разполага:

- с централизирана точка за управление с възможност за отдалечен достъп до нея през web browser – поне Internet Explorer и Google Chrome.
- Софтуер за наблюдение на работата на виртуалните машини и откриване на потенциални проблеми. Визуална информация за най-натоварените машини.
- Софтуер за репликиране на данните управлявани от виртуализираните машини



Фиг.33 – Сървъри за виртуализация, за VDI и дисков масив

2.4.2 Дисков масив

Всички данни, образи на операционните системи, служебна информация на виртуалните машини и други трябва да са на общ дисков масив. Дисковия масив трябва да разполага с пълна резервираност: два дискови контролера, две захранвания, два 10 Gbps порта на контролер, резервиран път до дисковете. Контролерите трябва да разполагат с поне 16 GB RAM и защита на кеша от спиране на тока. Дисковия масив трябва да разполага с поне 6 SSD диска 400 GB и 18 диска по 1 TB. След hot-spare и форматиране 1.8 TB SSD и 16.5 TB HDD. За повишаване на бързодействието всички операции по запис трябва да минават през SSD дискове независимо къде са разположени данните, като това не трябва да ангажира допълнително пространство от 6те SSD диска. Върху една и съща група от дискове трябва да могат да бъдат конфигурирани LUNs в RAID 5, RAID 6 и RAID 10 едновременно. Дисковия масив трябва да позволява конфигуриране като един LUN. Дисковият масив трябва да осигурява проактивно местене на данните в зависимост от използването им върху бързи или върху евтини дискове, като освобождава системните администратори от необходимост за постоянни корекции в конфигурацията.

Избран е общ SAN дисков масив Dell Compellent SC4020 с пълно резервиране и поддръжка на Flash/SSD, SAS и NL-SAS/SATA дискове, с операционна система Compellent Storage Center

Dell Compellent Модел: SC4020 - 10Gb iSCSI-210- ACRR

Контролери : два, работещи active/active

Разширяемост до 192 диска с доставените контролери

Свързаност : Два активни SFP+ конектора на контролер 10 Gbps Ethernet, свързани към опорните комутатори осигуряващи load balancing и high availability. Два допълнителни конектора 10GBase-T за връзка към опорните комутатори. Резервирана връзка към мрежата за управление.

Постоянна памет:

Данни тип 1: 10 TB raw еднотипни Flash дискове - 6 x Dell 1.92TB, SAS, 6Gb, 2.5 SSD Flash = 10.6 TB raw, 6 x Dell 1.92TB, SAS, 6Gb, 2.5 SSD, RI - 400-AGNS

Данни тип 2: 20 TB raw еднотипни 10000 rpm SAS дискове - 18 x Dell 1.2TB, SAS, 6Gb, 2.5", 10K, HD = 20.5 raw, 18 x Dell 1.2TB, SAS, 6Gb, 2.5", 10K, HDD - 400-ADON

Данни тип 3: 24 x 6 TB (вкл. един за hot-spare) - инсталирани в разширителни кутии SC200 Всички типове дискове са конфигурирани в RAID 10 и RAID 5 (RAID 6 за 6 TB)

Дисковия масив ще конфигуриран по начин осигуряващ всички операции по запис да минават през Flash дисковете. За осигуряване на максимална скорост всички запис операции ще бъдат конфигурирани да се извършват в RAID 10 върху SSD/Flash дисковете, като след това за спестяване на място в ненатоварен период ще се прехвърлят към предвиденото им място.

2.4.3 Сървъри за изграждане на инфраструктурата за виртуални потребителски компютри VDI

Изградена е система от четири броя Dell PowerEdge R730 model XD Generation 13 (фиг.33) със следните параметри:

Процесори:

2x Intel Xeon E5-2660 v4 2.0GHz,35M Cache,9.60GT/S QPI,Turbo,HT, 14C/28T (105W) Max Mem 2400MHz - 338- BJCW

Оперативна памет

192GB - 12 x 16GB RDIMM, 2133 MT/s, Dual Rank, x4 Data

Постоянна памет

Dual 16 GB Flash in hardware mirror, съобразени с поддържаните от VMWare hypervisor носители : Redundant SD Cards Enabled - 385-BBCF, 2x 16GB SD Card For IDSDM - 385-BBII

Dual 800GB PCIe, flash, hot-swap, конфигурирани като cache на част от дисковото пространство за VDI - 10x 2 TB SAS/NLSAS в pass-through, hot-swap -конфигурирани като дисково пространство на софтуера за Software Defined Storage : 800GB Dell PowerEdge NVMe Performance Express Flash 2.5in Hot Plug - 400-ALTY, 8x 2TB 7.2K RPM SATA 6Gbps 512e 2.5in Hot-plug Hard Drive - 400-AHMB, 2x 2TB 7.2K RPM SATA 6Gbps 512e 2.5in Hot-plug Flex Bay Drive - 400-AJDS

RAID контролер: PERC H730 Integrated RAID Controller, 1GB Cache - 405- AAEG

Захранване : Dual, Hot-plug, Redundant Power Supply (1 + 1), 750W, Titanium, 200-240VAC - 450- ADWT - 2x C13 to C14, PDU Style, 10 AMP, 6.5 Feet (2m), Power Cord - 450-AADY

Разпръснатостта на големия брой потребители и малкият състав от системни администратори налагат използването на съвременни технологии за работа и управление, които в максимална степен да улеснят поддръжката на системата. Във връзка с това трябва да се изгради система от виртуални десктоп машини (**VDI - Virtual Desktop Infrastructure**), отчитайки следните фактори:

- Крайните устройства, така наречените тънки клиенти, имат от гледна точка на потребителя и на администратора, по същество две състояния, напълно работещи или напълно неработещи. Т.е. устройство, на което не може да се визуализира информация, а друго устройство на негово място работи, може да се счита за подлежащо на сервиз и е проблем на сервизната

организация. Преминаването от едно устройство към друго е с обикновена подмяна и корекции в настройките на мрежата.

- Проблеми с операционната система, инсталирането на допълнителни продукти, дори при пълна загуба на инсталацията, може да стане от предварително подготвен template записан във виртуалната инфраструктура, като остане само донастройката за конкретния потребител
- Всички потребителски машини могат да бъдат включени към система за защита на данните, като им се прави редовен бекъп на определен интервал.
- Виртуалните машини за определени потребители могат да бъдат конфигурирани за достъп отвсякъде.
- Тънките клиенти нямат самостоятелна употреба и не представляват интерес за кражба или downgrade. Имат изключително ниска консумация и дълъг живот (обикновено равен на физическия живот на устройството), тъй като за подобряване работата се надстройва само сървърната част. Работейки без механични елементи, дефектируемостта е много малка. Не заемат съществено място. Не шумят.
- Основните проблеми на система VDI-тънки клиенти са потребителското усещане за ограниченост – нямат достъп до популярните entertainment канали, не могат да инсталират приложения. Някои специфични устройства като скенери, RS-232 устройства и други имат проблеми при интеграцията им системата.
- Друг проблем е системата за лицензиране – за обикновения потребител Windows Desktop операционните системи нямат постоянен лиценз, а само такъв на годишна база с цена приблизително равна ½ от цената на постоянен лиценз. Друг вариант е закупуването на Windows Server Datacenter поне за два от сървърите за VDI и използването на правото за стартиране на неограничен брой виртуални машини – по една за всеки потребител. Тук съществено би помогнал hypervisor с дедубликация на паметта, тъй като почти всички машини ще бъдат еднакви.

- Използване на Microsoft Remote Desktop Services, отново върху MS Windows Datacenter. С този подход може да се премине и към published applications – т.е. за крайните потребители да са достъпни само приложенията, които използват, без да се създава цяла Windows среда, която би изисквала и за най-малкият потребител администрация и защита, като за всеки друг.

- Отчитайки натоварването, което генерират отделните потребители, най-вероятната плътност на машините би била около 80 едновременно работещи на отделен сървър, т.е. за броя служители в организацията са достатъчни 4 сървъра. Това предполага двупроцесорен сървър с поне 1000 SPECint_rate2006, 256 GB RAM, 4 x 10 Gbsp + 2 x 1 Gbps Ethernet. За да се избегне „задръстване“ особено по време на сутрешното зареждане, образите на операционните системи и основните приложения трябва да бъдат разположени на software defined storage (SDS) върху самите сървъри базиран на SSD. Така достъпът до тях ще е със скоростта на локален диск и ще се избегне споделяне на връзките към дисковия масив от много потребители. Данните на потребителите трябва да са разположени на дисковия масив от предходната точка, защото скоростта за достъп до тях не е критична и е съпоставима с данни разположени върху файлов сървър с мрежа 10 Gbps. За целта към него трябва да се добави обем според изчисленията за необходимите потребителски данни. Ако с нарастване на потребителите или на натоварването (примерно с подвключване на потребители от друга сграда на отганизацията) четерите сървъра не са достатъчни, към тях трябва да се добави още един, два и повече според нуждите. Затова трябва да се търси лицензионен модел, който не отчита броя на сървъри и процесори, а само потребители.

- С цел намаляване на началната инвестиция, като тънки клиенти могат да се използват вече наличните PC-та с инсталиране на софтуер за достъп до VDI. Изградената VDI инфраструктура може да бъде разширявана за да включи и други потребители от другата сграда, като се намалят необходимите инвестиции там за подмяна на PC оборудването

- Системата за изграждане и управление на виртуалните машини трябва да е идентична с използваната за сървърна виртуализация и да позволява както статично дефинирани виртуални машини така и динамични изграждани виртуални машини на база стандартни образи на операционната система за временни потребители. Системата трябва да позволява на потребители с редуцирано използване на ресурси да имат достъп само до определени приложения, без достъп до цяла операционна система.

2.5 Система за защита на данните

Системата за защита на данните включва дисков обем достатъчен да поеме цялото пространство на общия дисков масив поне два пъти. За дългосрочно архивиране на данните се използват магнитни ленти. Така се осигурява възможност за бързо възстановяване на данни от дисковия масив и дългосрочно пазене върху магнитни ленти. Тази архитектура отчита и факта, че за момента още не е известен вирус атакуващ магнитните ленти.

Системата осигурява бекъп на всички виртуални машини – сървърни и десктоп. Системата позволява възстановяване на отделен файл или цяла виртуална машина

Пълен бекъп трябва да се прави всяка събота и неделя, а инкрементален всяка нощ. За някои особено отговорни машини пълен бекъп може да се прави и всяка нощ.

Хардуера за защита на данните е разположен в място различно от централната точка, в друга част на сградата, в помещение с два комутатора. Така се гарантира, че локално събитие в сградата няма да засегне и този хардуер.

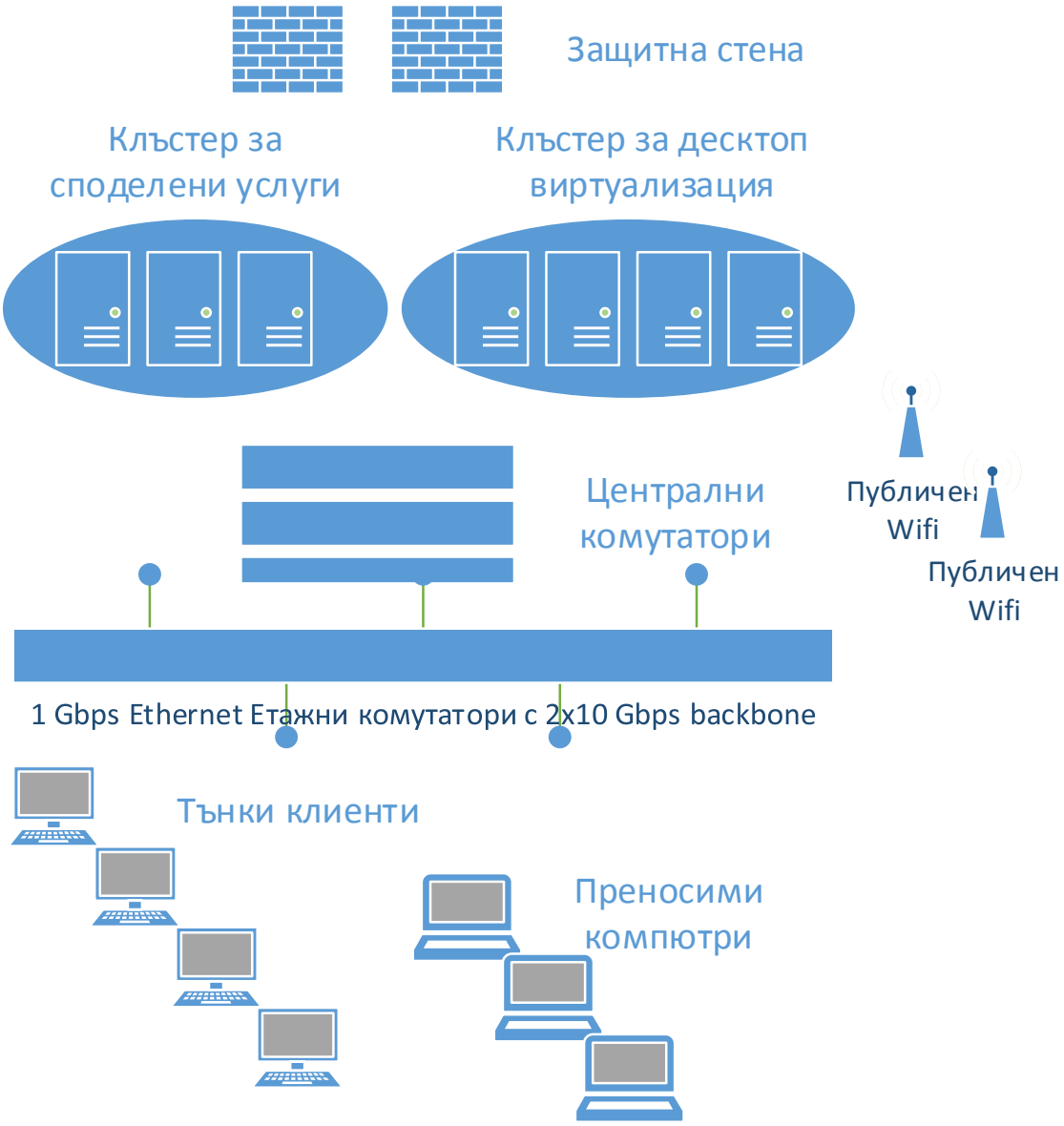
2.6 Избор на адресен план.

В мрежата са дефинирани 20 VLAN-а за различните функционални звена. Маршрутизацията ще се осъществява на централно ниво. Layer 3 комутацията между отделните VLAN става в централната точка. Собствени VLAN са предвидени и за споделените устройства – принтери, WiFi access point, публични монитори и др.

				Start	End
VLAN 1	10.2.0.1	Default VLAN	22/252	10.2.0.1	10.2.3.255
VLAN 6	10.2.6.1	VPN	24	10.2.6.1	10.2.6.255
VLAN 7		Internet 1	24	93.152.*.*	
VLAN 10	10.2.10.1	Servers	24	10.2.10.1	10.2.10.255
VLAN 11	10.2.11.1	Printers	24	10.2.11.1	10.2.11.255
VLAN 20	10.2.16.1	Infrastructure VLAN	20/240	10.2.20.1	10.2.23.255
VLAN 32	10.2.32.1	Administrators VLAN	24	10.2.32.1	10.2.32.255
VLAN 33	10.2.33.1	Administrators WiFi	24	10.2.33.1	10.2.33.255
VLAN 34	10.2.34.1	Managers	24	10.2.34.1	10.2.34.255
VLAN 35	10.2.35.1	Managers WiFi	24	10.2.35.1	10.2.35.255
VLAN 36	10.2.36.1	SonicPoints	24	10.2.36.1	10.2.36.255
VLAN 37	10.2.37.1	Public WiFi	24	10.2.37.1	10.2.37.255
VLAN 50	10.2.50.1	Thin Clients VLAN	21/248	10.2.50.3	10.2.55.254
		VDI Virtal Machines		10.2.48.2	10.2.49.255
VLAN 56	10.2.56.1	Internal WiFi	23	10.2.59.1	10.2.60.254
VLAN 57	10.2.57.1	Non Thin Clients	24	10.2.57.1	10.2.57.254
VLAN 64	10.2.64.1	Accounting	24	10.2.64.1	10.2.64.255
VLAN 66	10.2.66.1	Human Resources	24	10.2.66.1	10.2.66.255
VLAN 6x	10.2.xx.1	Други intranet машини			
VLAN 112		Voice(IP tel)	24/255	10.2.112.1	10.2.112.255
VLAN 120		Monitors(Infomation)	24/255	10.2.120.1	10.2.120.255

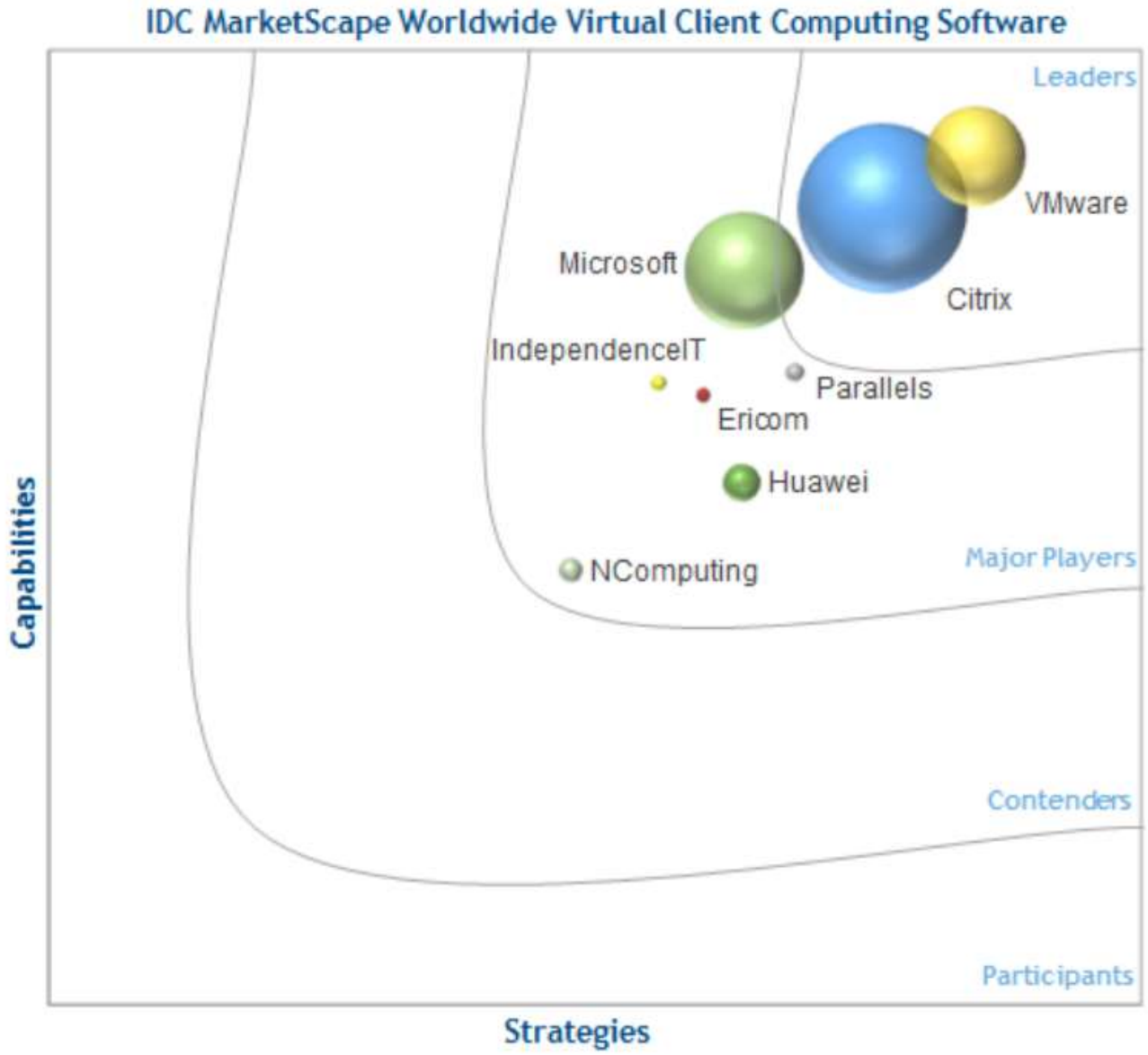
2.7 Краен резултат.

Постигнатия краен резултат от изградената локална компютърна мрежа и виртуална инфраструктура се визуализира на фиг.34:



Фиг.34

С цел използване на най-доброто от наличните архитектури, виртуализацията се базира на продуктите на VMWare, а всички операционни системи са базирани на Microsoft Windows. Така се комбинира най-доброто за всяка една от нуждите на организацията, а операционната среда за потребителите се запазва същата, както и в досегашната им работа. При избора на продуктите са използвани изследванията на водещите лаборатории в света, които лесно могат да бъдат обобщени в резултатите на IDC:



Source: IDC, 2016

Фиг.35

Графиката на фиг.35 показва, както пазарния дял (размера на кръга) така и възможностите на съответното решение (горният десен ъгъл е за най-големите възможности). Citrix е изключен заради липсата на достатъчно специалисти в България с достатъчно опит да реализират подобен проект. Отчитан е и положителния и отрицателен опит на Министерство на вътрешните работи и Центъра за превенция и противодействие на корупцията и организираната престъпност с различните видове десктоп виртуализация.

ЗАКЛЮЧЕНИЕ

Компютърните комуникации са една от най-бързо развиващите се технологии. За да отговорят на нуждите на комуникациите локалните компютърни мрежи също се развиват с бързи темпове. Те се използват както в малки фирми, големи организации и предприятия, така и в нашия дом. При проектирането и изграждането на компютърната мрежа трябва да определим за какви нужди ще се използва мрежата, колко да е голяма, колко надеждна, защитена, бърза и не на последно място възможността и за разрастване.

В разработената магистърска теза е извършено следното:

- разгледани са основите за изграждането на компютърните мрежи.
- запознахме се с видовете LAN Мрежи
- разгледахме същността на компютърната мрежа.
- Запознахме се с мрежовите протоколи за предаване и защита на данни, мрежовата топология
- Проучихме компонентите за създаване на мрежа.
- избрахме подходящо мрежово пасивно и активно оборудване за изграждане на комуникациите
- избрахме подходящо сървърно активно оборудване за изграждане на виртуалната инфраструктура

Задачите, които бяха поставени са постигнати, с което считам, че целта на магистърската теза е успешно представена и защитена. Към настоящия момент локалната компютърна мрежа по която е разработена магистърската теза е напълно изградена и функционираща. Може да се използва като основа за изграждане и на други компютърни мрежи.

Използвани източници

1. - КОМПЮТЪРНИ МРЕЖИ И КОМУНИКАЦИИ Автор: Александър Петров Милев

- https://sou7-smolian.weebly.com/uploads/1/6/1/6/16168774/mreji.pdf

- Компютърни мрежи-пълно ръководство по теория, изграждане и съвместна работа между мрежите Автор: Дебра Литълджон Шиндър Издател: СофтПрес

- Нортън П., Пълно ръководство за работа с мрежи, Инфодар 1999 г.

- Цонев И., Компютърни мрежи и комуникации, Шумен, 2008

- https://aleksandralyzhina.wordpress.com/2012/11/28/локална-мрежа/

- Шиндър Дебора, Компютърни мрежи, София, Изд. „СофтПрес”20

- http://drugi.dokumentite.com/download/kompiutyrni-mreji/11069

- http://www.referati.org/kompiutyrni-mreji/15412/ref/p9

- http://znanieto.net/diplomni/details/8054/20/

2. -https://www.kaminata.net/forum/kompyutarni-mrezhi-i-komunikatsii-t103995.html

- http://zdrasti.info/informatika-teoriya-tekstoobrabotka-i-tablici-s-libreoffice.html?page=7

- https://bg.wikipedia.org/wiki/ Мрежови_топологии

- https://tobleroncho.wordpress.com/2015/04/23/мрежа/

- https://aleksandralyzhina.wordpress.com/2012/11/28/локална-мрежа/

- http://pght-zelinskij.com/docs/IInform/

- https://www.scribd.com/

3. - http://e-learning.mgu.bg/files/activities/file/book-139-2-265.pdf

- http://vschool.info/cn/wp-content/uploads/2012/10/Optical-fiber-tagged1.jpg

- http://pgds.org/books/km/03.htm#_Toc216445934

- https://sou7-smolian.weebly.com/uploads/1/6/1/6/16168774/mreji.pdf

- http://ktt.ptgrz.org/CompNet.pdf

4. - http://ayokonfig.blogspot.bg/2016/11/pengertian-kabel-utp-stp-coaxial-dan.html

- https://www.bol.com/nl/p/linkbasic-ftp-kabel-cat6-shielded-kabel-305m/9200000057910554/

- http://jowang.over-blog.com/2016/03/multimode-fiber-optic-patch-cable-overview.html

- http://www.fiber-optic-tutorial.com/how-to-connect-fiber-media-converter-to-network.html

- https://www.emag.bg/mrezhova-karta-wireless-tp-link-ac-1900mbps-dual-band-pci-e-archer-t9e/pd/DGYB6MBBM/

- https://ardes.bg/product/tp-link-tg-3468-tg-3468-45562

- http://www.bcot1.com/networking.html

5. - http://info.fmi.shu-bg.net/skin/pfiles/administration_book.pdf

- Нортън П., Пълно ръководство за работа с мрежи, Инфодар 1999г.

- http://slides.bg

- http://dhstudio.bg/wireless_bluetooth.html

- http://www.iseca.org/downloads/2004_2005-1/papers/30661_30628_30708_LAN_ISP.pdf

- http://vmrejata.info/tcpip/314-ipadressing.html

- http://vschool.info/cn/km-p/cidr/

- http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml

- https://bg.wikipedia.org/wiki/IP_%D0%B0%D0%B4%D1%80%D0

- https://softuni.bg/downloads/svn/networks/July-2016/04.Networking-Fundamentals-VLAN/