УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ
КАТЕДРА "КОМУНИКАЦИИ И СИГУРНОСТ"
СПЕЦИАЛНОСТ ИНФОРМАЦИОННО БРОКЕРСТВО

ДИПЛОМНА РАБОТА

на тема:

Проектиране на мрежа за нуждите на малка и средна компания

Дипломант:
Тодор Генчев
№ 204-ИЗ, задочно об.

Научен Ръководител: . . . . .
(гл. ас. д-р Добри Бояджиев)

София

2016

Резюме.

Генчев,Тодор. Проектиране на мрежа за нуждите на малка и средна компания. Научен ръководител гл. ас. д-р Добри Бояджиев. София 2016. Катедра „Информационни системи и технологии“, факултет по „Информационни науки“, УНИБИТ. Страници 76. Брой източници 15, фигури и таблици – 34.

Целта на настоящата дипломна работа е да покаже процесът на проектиране и изграждане на симулационен модел на мрежа на компания от средния бизнес.

За осъществяването на този проект сме си поставили следните задачи.

- Да се посочат основите за изграждането на компютърните мрежи
- Да се проучат компонентите за създаване на мрежа.
- Да се запознаем с видовете LAN Мрежи
- Да се извърши практическа симулация и да се покаже как функционира мрежата в една средно голяма фирма.

Ключови думи: VLAN, IP адрес, мрежа, маршрутизатор, протокол, route.

Съдържание

Увод

В съвременния свят всички сме постоянно свързани с други хора, благодарение на мрежите. Използваме телефонните мрежи, за да говорим с познати и бизнес кореспонденти, гледаме телевизия благодарение на телевизионната мрежа, общуваме с приятели и партньори в социалните мрежи и използваме световната компютърна мрежа Интернет за всякакви разнообразни задачи. Компютърната мрежа представлява съвкупност от две или повече компютърни системи, свързани заедно за обмен на информация или за изпълнение на някакваобща работа. Различните видове компютърни мрежи имат различни цели, размери и принципи на изграждане. Освен глобалната мрежа Интернет, към която ежедневно свързваме своите компютри, телефони, таблети и други устройства, за да черпим информация, да общуваме с останалите, да работим и да се забавляваме, компютърни мрежи има и на други места, за които вероятно не се замисляме. Например отделните важни възли на автомобила ни се управляват от специализирани компютри, които също са свързани в компютърна мрежа, за да си обменят информация. Банкоматите и POS-устройствата, от които теглим банкноти или плащаме сметки също работят благодарение на компютърната мрежа, която ги свързва с устройствата на банката. Една от основните характеристики на една компютърна мрежа е нейната скорост на предаване на данни. Скоростта е важна, защото различните приложения имат различни изисквания за скорост. Например, скоростта необходима за гледане на един телевизионен канал със стандартна разрешаваща способност е приблизително равна на скоростта, необходима за провеждане на десет телефонни разговора едновременно. Всяка една добре развиваща се компания, използваща компютри се нуждае от добре функционираща компютърна мрежа.

Съвременните мрежи могат да включват много компоненти. Някои от най-основните компоненти са компютри, маршрутизатори (routers) и комутатора (switches). Използването на мрежа дава възможност за споделяне на ресурси. Когато бъдат свързани в мрежа, потребителите могат да споделят файлове, папки, принтери, музика, филми.

Cisco Systems, Inc., е световен лидер в областта на мрежи за Интернет. Днес, мрежите са съществена част от бизнеса, образованието, държавни, и вътрешните комуникации. Cisco хардуер, софтуерът и подръжка, се предлага за създаване на Интернет и мрежови решения. В допълнение, Cisco е пионер в използването на Интернет в собствения си бизнес практика и предлага консултантски услуги, базирани на своя опит, за да помогне на други организации по целия свят. Всички по-големи и сериозни компании разчитат на техните модели устройства за да изградят своята мрежа надеждно и качествено

Целта на настоящата дипломна работа е да покаже процесът на проектиране и изграждане на симулационен модел на мрежа на компания от средния бизнес.

За осъществяването на този проект сме си поставили следните задачи.

- Да се посочат основите за изграждането на компютърните мрежи
- Да се проучат компонентите за създаване на мрежа.
- Да се запознаем с видовете LAN Мрежи
- Да се извърши практическа симулация и да се покаже как функционира мрежата в една средно голяма фирма.

Глава I. Мрежови концепции, модели и стандарти

1.1 Въведение

Компютърната мрежа (за по-накратко – мрежа) е съвкупност от хардуерни компоненти и компютри, свързани помежду си чрез преносна среда, която позволява обмен на информация помежду им. Устройствата участващи в мрежата, за да обменят данни трябва да бъдат свързани помежду си чрез технология на свързване. Най-разпространените връзки са кабелната (коаксиален, усукана двойка или оптичен кабел) и безжичната (радиовълнова, сателитно предаване, лазерна или инфрачервена технология). Възможна е връзка чрез допълнително устройство – рутер (маршрутизатор).

За да се разбере как работи една комютърна мрежа е необходимо да се представи от какво е създадена. Години след като се появяват компютрите, една малка част от тях са били свързани в мрежа. Те са работили като малки информационни острови, без връзка помежду си. Данните между компютрите са се прехвърляли чрез копиране им на флопи диск, пренасяне на този диск до другия компютър и копиране на данните на целевата машина. Този процес понякога се е наричал иронично *sneakernet (*мрежа не гуменките). Една от основните характеристики на една компютърна мрежа е нейната скорост на предаване на данни. Скоростта е важна, защото различните приложения имат различни изисквания за скорост. Например, скоростта необходима за гледане на един телевизионен канал със стандартна разрешаваща способност е приблизително равна на скоростта, необходима за провеждане на десет телефонни разговора едновременно. Скоростите на предаване на информация в компютърните мрежи се измерват с няколко мерни единици. Първите две са единици за количество информация, а следващите за скорост:

- *Бит (bit)* е основна единица информация в компютрите, представляваща най-малката информация, която може да се съхранява или предава. Един бит може да има стойност 0 или 1.

- *Байт (byte)* е съвкупност от осем бита. Това е единица информация, която може да представи една буква в писмо или документ.

- *Бит в секунда (bps)* – мярка за скорост на предаване на информация, при

която за една секунда се предава един бит, т.е. за предаване на една буква са необходими осем секунди.

- *Байт в секунда (Bps)* - мярка за скорост на предаване на информация, при която за една секунда се предава един байт, което в повечето случаи означава една буква.

Тези мерни единици определят доста ниски скорости, в сравнение с типичните за съвременния мрежов свят, затова обикновено се използват техни производни:

- *Килобит в секунда (kbps)* – един килобит е равен на 1024 бита, т.е. при един килобит в секунда обикновено за една секунда се предават около 1024 / 8 или 128 букви.

- *Килобайт в секунда (kBps)* – 1024 байта или букви в секунда.

- *Мегабит в секунда (Mbps)* – 1024 килобита в секунда или 1048576 бита в секунда е основната мярка за скоростна свързаност към Интернет в съвременния свят.

- *Мегабайт в секунда (MBps)* – 1024 килобайта в секунда или малко над един милион букви в секунда.

- *Гигабит в секунда (Gbps)* – 1024 мегабита в секунда или 1073741824 (над един милиард) бита в секунда.

1.2 Мрежови Категоризации

Категоризация според ролите на отделните компютри

- Равноправни мрежи (peer-to peer)

При равноправните мрежи всеки компютър може да дава услуги на останалите в мрежата, както и да използва услугите, предоставяни от другите компютри. Равноправните мрежи са евтини за изграждане и са предназначени за малък брой компютри (според Microsoft – до 10). При тях обикновено на всеки компютър е инсталирана потребителска операционна система, например Windows 7 или Ubuntu Linux и на него може да работи потребител и да изпълнява програми. Всеки потребител сам решава какви ресурси на своя компютър (дисково пространство, принтери) ще позволи за използване от останалите компютри в мрежата и какви права ще даде на другите потребители. Администрацията на този вид мрежи е разпределена – имената на потребителите, техните пароли и права се назначават отделно на всеки компютър и един потребител може да има различни пароли и права на различните компютри. Равноправните мрежи са подходящи за домашна обстановка, където всеки може да сподели снимки, видео и други документи с останалите и всеки да печата на принтера, свързан към единия компютър.

- Сървърно базирани мрежи

При сървърно базираните мрежи има един или повече специализирани компютри, наречени сървъри с инсталирана мрежова операционна система, която поддържа функциите на мрежата. Ако сървърът не работи, обикновено няма услуги, които да са достъпни през мрежата за компютрите на потребителите или мрежата не работи. Затова често сървърите се намират в специализирано помещение, без достъп на неоторизирани лица. Обикновено на сървърите не работят потребители, а те са отделени специално за да поддържат функционирането на мрежата, което оскъпява този вид мрежи, в сравнение с предишните. Понякога мрежовите операционни системи за сървъри могат да струват доста – от порядъка на хиляди лева. При сървърно базираните мрежи администрацията е централизирана – всички настройки, имена на потребители, пароли, права и други параметри се създават и променят еднократно само на сървъра и важат за цялата мрежа, което повишава и сигурността на тези решения. Сървърно базираните мрежи са типични за средни и големи офиси и учреждения, учебни заведения, университети и други организации с повече компютри и с нужда от по-голяма сигурност и стабилност на мрежата.

Категоризация 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.

- 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).

1.3 Портове и номерация

Мрежовият порт е софтуерна абстракция служеща за определяне на различните крайни точки на комуникационните канали в рамките на един хост. Мрежовият адрес, заедно с порта, идентифицира крайната точка на един комуникационен канал в рамките на една мрежа и се нарича транспортен адрес (по OSI модела). Сборът от мрежовите адреси и портове (по един за хост) на два комуникиращи помежду си хоста, идентифицира еднозначно комуникационния канал помежду им и се нарича мрежов цокъл (или сокет). Два хоста могат да имат повече от един комуникационен канал помежду си-в този случай, комуникационните канали се различават с поне по един от портовете си.

Мрежовият порт, в най-общи линии, може да се разглежда като софтуерна аналогия на хардуерния порт. В тази аналогия, портът може да се разглежда като място на контакт между комуникиращи си процеси.

Отделният порт на един хост се идентифицира с число наречено номер на порт. Това число присъства в заглавието на съобщения на протоколи от транспортния слой. Такива протоколи са TCP, UDP, DCCP, SCTP. Протоколът ISO-TP използва подобен идентификатор – транспортен префикс.

„Компютрите могат да използват до 65535 порта. Портовете с номера от 1 до 1023, се наричат добре известни портове (well-known ports) за това, защото са стандартизирани. Портовете с номера от 1024 до 49151 се достъпни да бъдат регистрирани от производителите на софтуер, за да бъдат изпозлвани като идентификатори между крайните точки на мрежата за техните приложения. Те трябва да бъдат регистрирани от Internet Assigned Numbers Authority (IANA). Номерата от 49152 дп 65535 се наричат динамични портове и се изпозлват на случаен принцип.“

1.4. Мрежови Топологии

Топологията на мрежата представлява начина, по който са свързани компютрите в нея. Разглеждайки видовете топологии и техните

характеристики, трябва да се има предвид, че една мрежа има два вида топологии. Първата е физическата топология, която определя как физически са свързани компютрите с преносната среда. Втората е логическа топология, която определя как се чувстват компютрите спрямо останалите в мрежата. В някои мрежи физическата и логическата топология съвпадат, в други се различават. За по-лесно описание долните примери разглеждат физическа топология.

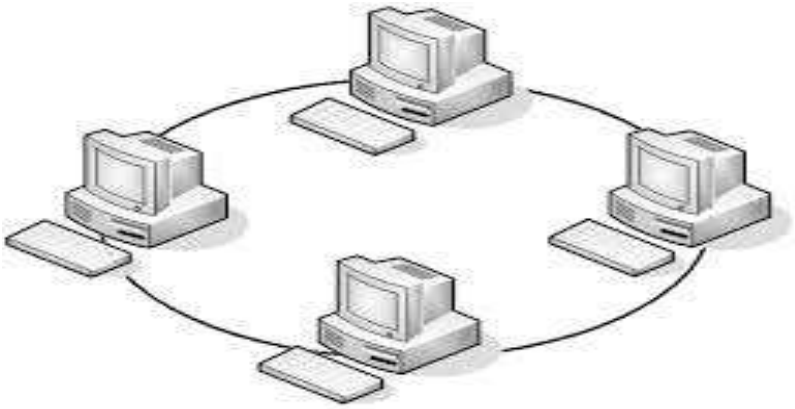
- Топология шина (bus) - при нея всички компютри споделят обща преносна среда. Когато един предава, неговият сигнал се приема от всички останали, свързани към шината. Затова само един може да предава в даден момент от време. При прекъсване на шината, цялата мрежа не работи. Тази топология е типична за старите Ethernet мрежи с коаксиален кабел, за кабелните телевизионни мрежи и за някои съвременни оптични мрежи, изградени без отказоустойчивост.

Пример за шинна топология е показан на фигура 1.

Фигура 1 - Шинна Топология

- Топология кръг (ring) – При нея кабелът от първия компютър се включва към втория, от втория в третия и така до последния, чиито кабел се включва обратно в първия. Когато един предава, неговият сигнал се приема само от следващия по кръга. Тази топология се отличава със отказоустойчивост, тъй като при прекъсване на кръга, все още има възможен път, по който да се предават данни между всички устройства. Такава топология имат мрежите от тип Token Ring, FDDI и съвременните оптични мрежи, изградени с отказоустойчивост.

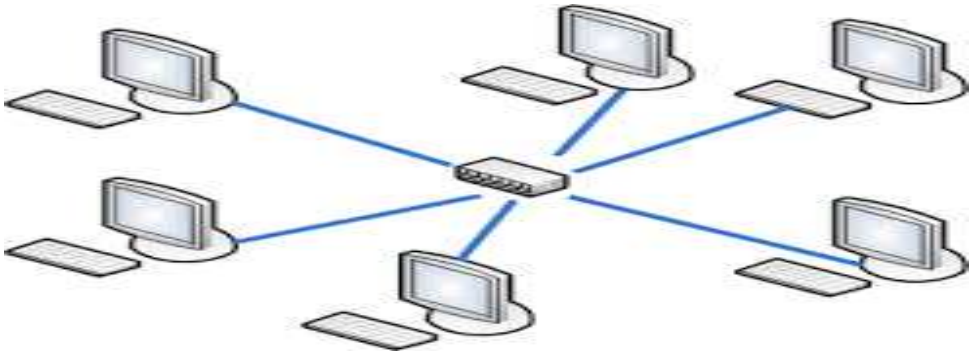
Пример на кръгова топология е показан на фиг.2



Фигура 2 - Кръгова топология

- Топология звезда (star) - при нея има централен възел, към който са свързани всички компютърни системи, всяка чрез собствена среда. Така всеки компютър може да предава самостоятелно, без да се съобразява с останалите. Прекъсването на дадена среда влияе само на конкретния възел и не пречи на останалите. Такава мрежа е уязвима при отказ на централното устройство- тогава цялата мрежа спира. Тази топология е типична за съвременните малки локални мрежи и за корпоративни мрежи, при които всеки от отдалечените офиси е свързан само към централата.

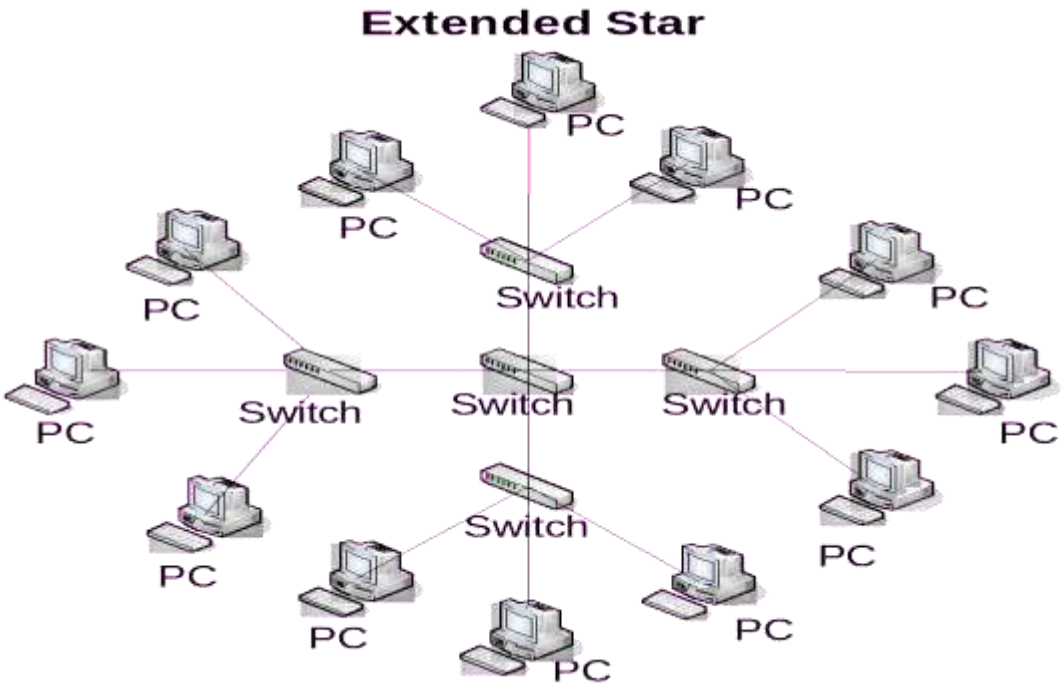
Пример за звездообразна топология е показан на фиг.3



Фигура 3 - Звездообразна топология

- Топология разширена звезда (extended star) - при нея някои от краищат на основната зведа стават центрове на свои звездообразни топологии. Структурата е типична за големите локални мрежи, например в многоетажна сграда една звезда свързва отделните етажи, където се поставя ново устройство (комутатор), разпределящо връзките до отделните стаи на етажа.

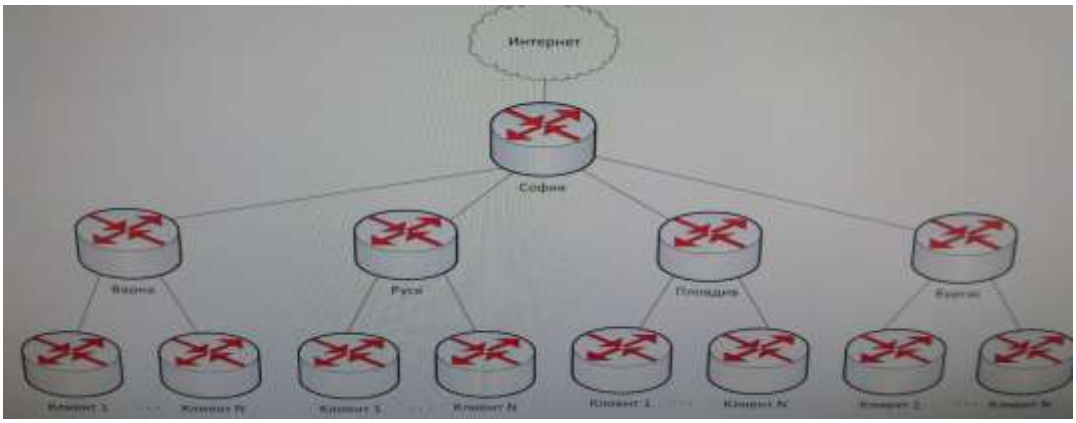
Пример за топология разширена звезда е показан на фигура 4



Фигура 4 - Разширена звезда топология

- Йерархична топология (tree) - йерархичната или дървовидна топология има главен възел, към който се свързват неговите подчинени възли. Всеки от подчинените възли може да бъде главен за нови възли на по-долно ниво. Структурата е типична за мрежа на доставчик на Интернет услуги, при който от главния град, където е връзката м у к ъм И нтернет и ма о тделни в ръзки заостаналите градове, където ще има клиенти, а от съответния град се изграждат нови връзки към клиентите. Топологията се характеризира с липса на отказоустойчивост – когато един възел или връзка отпадне, всички възли под нея губят достъп до мрежата.

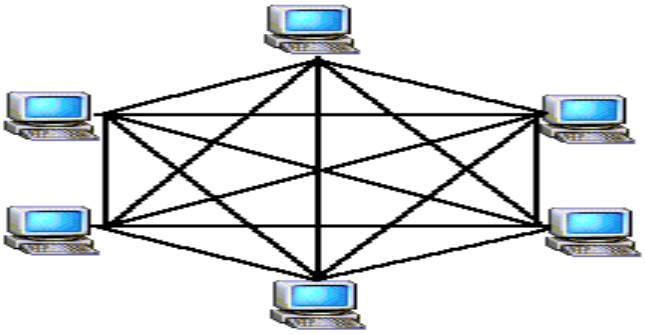
Пример за йерархична топология е показан на фирура 5



Фигура 5 - Йерархична топология

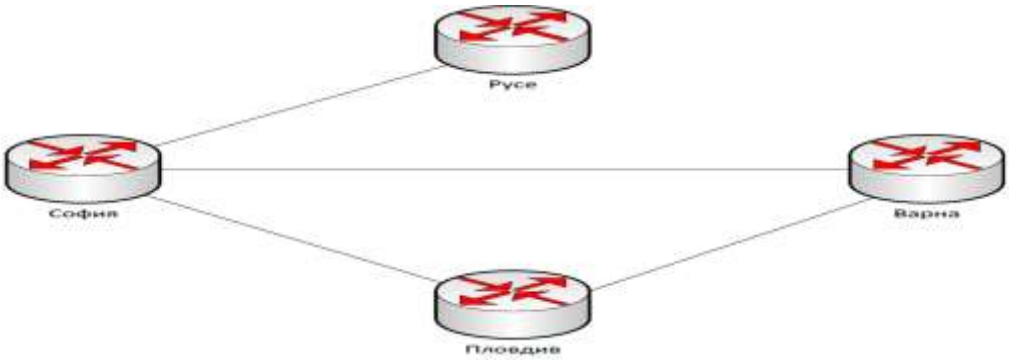
- Напълно свързана топология (mesh) - при нея всеки възел има независима връзка със всеки друг. Предимството на топологията е голямата степен на отказоустойчивост, защото има голям брой резервни трасета, по които може да се предава информация, при отпадане на основното трасе. Недостатък на топологията е големият брой необходими връзки, което води до значително повишаване на цената, особено при голям брой възли. Структурата е типична за компания с клонове в различни градове, която иска да има отлична отказоустойчивост.

Пример за напълно свързана топология е показан на фигура 6



Фигура 6 - Напълно свързана топология

- Непълно свързана топология- тя няма точно определена структура, но целта е да се използва предимството на отказоустойчивостта на напълно свързаната топология, но да се намали цената. Затова важните възли се дублират с резервни трасета, за да бъдат отказоустойчиви, а по-маловажните за работата на компанията се оставят с по-малък брой връзки, за да се намали цената. Всяка неправилна топология може да се превърне в напълно свързана, при добавяне на необходимите връзки. Пример за такава топология може да видим на фиг.7



Фигура 7 - Непълно свързана топология

1.5 Мрежови модели

Мрежовите модели описват начините, по който се извършва комуникацията в компютърните мрежи. На тяхна база се създават мрежовите

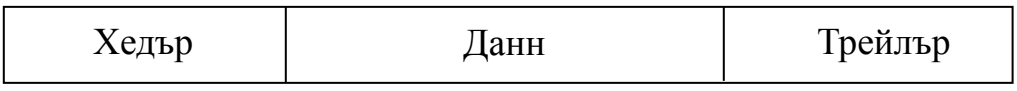
стандарти и спецификации, въз основа на които се произвеждат всички мрежови продукти.

1.5.1. Комуникация с пакети

В компютърните мрежи се използва технология, използваща *комутиране на пакети* (*packet switching*). За да могат компютрите в една мрежа да ползват мрежата едновременно, необходимо е големите файлове да бъдат разбивани и изпращани в мрежата под формата на по-малки информационни единици, наричани *пакети*, като времето за предаването им се разпределя между компютрите. В противен случай един компютър би монополизирал пропускателната способност на цялата мрежа, докато трае неговата комуникация.

По време на комутацията на пакетите на един файл всеки един от тях би могъл да пътува по различен път в мрежата и да достигне до крайната точка на комуникация за време, различно от това на останалите пакети на същия файл. След като всички пакети достигнат крайния пункт, те биват подреждани (сглобявани) в първоначалния им ред така, че да образуват отново файла. Информация за тяхната подредба се съдържа в хедърите (заглавната част) (фиг.8) на пакетите. Ако мрежовата комуникация бъде прекъсната или пък поради някакви други причини бъдат изгубени един или няколко пакета, повторно се предава само загубената информация, но не и целия файл.

За разлика от телефонните мрежи, където докато трае комуникацията се ползва винаги една единствена връзка, при комуникацията с пакети, ако даден път се окаже претоварен, следващите пакети биват изпращани автоматично по друг по-ефикасен маршрут.



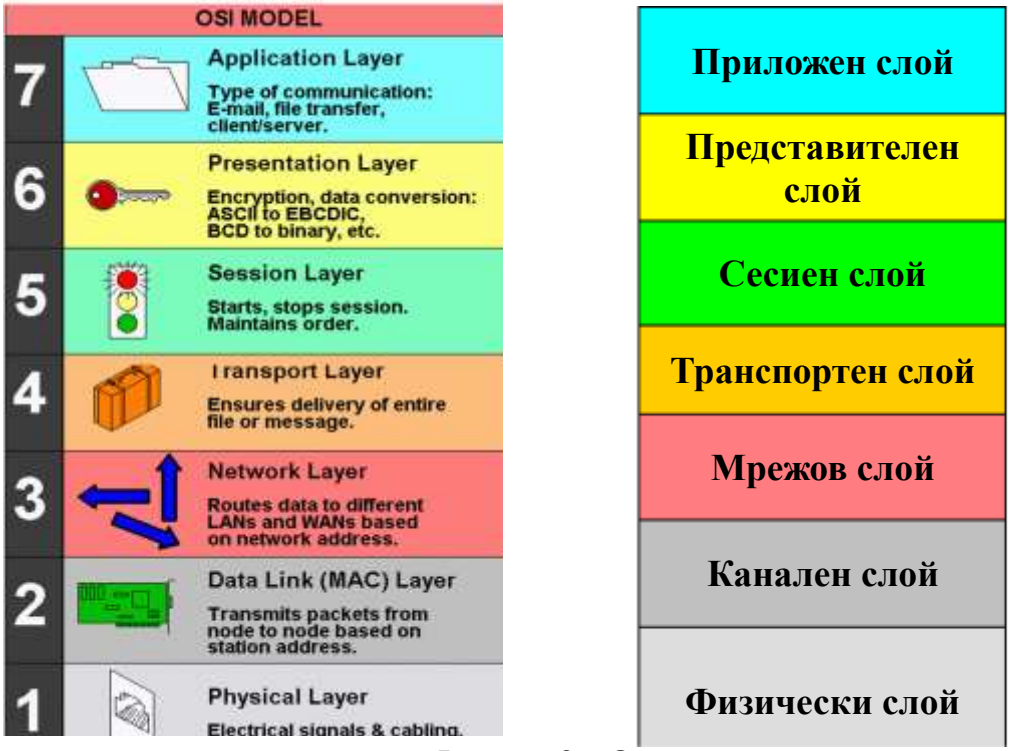
Фигура 8 - Подредба Пакети

Хедърът се разполага преди данните. Той се състои от полета, чийто брой и размер зависят от мрежовата архитектура и протоколите. Като правило в хедърните полета се съдържат: адреса на местоназначението, адреса на източника, както и друга информация, зависеща от протокола. Ethernet пакетите биват наричани фреймове (frames, кадри). Един фрейм може да бъде с размер между 64 и 1518 байта. При Token Ring пакетът (фреймът) е с размери 4202 байта.

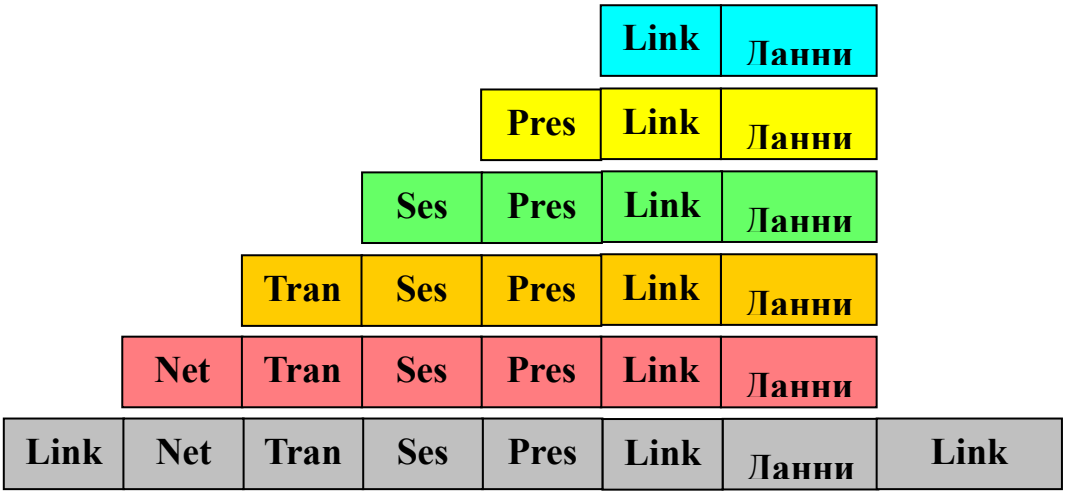
Пакетите включват и завършваща информация, наричана трейлър (trailer). Обикновено той съдържа информация, позволяваща да бъде извършена проверка дали в получените по мрежата данни не се е появила някаква грешка вследствие на електромагнитни смущения. Проверката се нарича *циклична проверка с излишък* (*cyclical redundancy check – CRC*). Данните на всеки пакет, преди да напуснат компютъра-източник, биват обработвани чрез образуване на сума по модул 2 (от битовете на данните). Тази сума се записва в трейлъра. Когато пакетът пристигне в местоназначението си, отново се образува сума от същите битове, след което тя се сравнява със сумата от трейлъра. Ако сумите се окажат различни, това означава, че данните са били променени по време на изпращането им и че пакетът следва да бъде повторно изпратен.

1.5.2. Мрежов модел OSI

Моделът OSI (Open System Interconnection) е разработен през 80-те години от ISO (International Standard Organization). Той има за цел да послужи като стандарт за изграждане и описание на мрежови модели. Но той не е първият мрежов модел. През 70-те години, като част от ARPAnet, бе разработен моделът TCP/IP, който впоследствие намери широко приложение и днес се наложи като основен в Интернет.



Фигура 9 - OSI модели



Фигура 10 - Функции на OSI слоеве

Моделът OSI е изграден от седем слоя (фиг.9), всеки един от които представлява една стъпка в многослойния процес на мрежовата комуникация. Наричат го понякога OSI-стек. Но това не е данновия стек, познат от програмирането като структура от данни. OSI е *протоколен стек*.

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 (фиг.10). В приемащия компютър процедурата е обратна – информацията се придвижва отдолу нагоре, като всеки един от слоевете премахва част от нея. На фиг.10 липсва изображение за физическия слой, тъй като той не добавя хедър. Неговата функция е да създаде сигнали и да ги пренесе по мрежата.

Функциите на отделните слоеве са следните:

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.

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.

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*.

Мрежовите карти, хъбовете, мостовете, комутаторите и маршрутизаторите, са разгледани в т.4.

1.5.3 Мрежови Протоколи

Протоколът представлява споразумение за това как трябва нещо да бъде направено. Съществуват много типове протоколи:

- **Бизнес протоколи**, които дефинират как трябва да се управлява бизнесът, и социални протоколи, които дефинират какъв тип поведение е приемливо. Протоколите за работа в мрежа дефинират правилата за комуникация между устройствата.

- **Мрежовият протокол** се отнася за протоколите намиращи се на ниво 3 от OSI модела. Тези протоколи осигуряват доставка на данни намиращи се извън локалната мрежа на изпращача.

- За компютрите е възможно да работят с повече от един протокол едновременно и това се нарича **Стек протокол.** Той е набор от протоколи на различни нива и е достатъчен за организация на взаимодействието на системите. За да могат обаче два компютъра да контактуват един с друг, и двете устройства трябва да споделят поне един протокол за работа в мрежа. В това отношение, протоколите приличат на езиците. Ако двете устройства не говорят общ език те не могат да си комуникират.

Как работят протоколите?

При изпращащия компютър протоколът прави следното:

• Разделя данните на малки части, наречени пакети;

• Добавя адресна информация към всеки пакет;

• Подготвя данните за реално предаване през мрежовия кабел.

При получаващия компютър протоколът извършва същите серии от стъпки в обратен

ред:

• Получава пакетите данни от кабела в мрежовата адаптерна карта;

• Отделя от пакетите служебната информация;

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

• Подава сглобените данни в използваем вид към съответното приложение.

Съществуват:

• немаршрутизируеми протоколи – за предаване на данни в една локална мрежа;

• маршрутизируеми протоколи – използват се за предаване на данните от една локална

мрежа към друга по един от няколко възможни пътя (маршрута).

Протоколите се разделят на следните три групи:

• Приложни – осигуряват обмена на данни и взаимодействието приложение-

приложение (SMTP, FTP, Telnet, HTTP и др.);

• Транспортни – отговарят за надеждността при придвижване на данните в мрежата

(TCP, NetBEUI);

• Мрежови – осигуряват така наречените свързващи услуги. Управляват адресиращата

и маршрутизираща информация, осъществяват проверките за грешки и заявките за повторно предаване (IP).

Ще разгледаме някой от основните мрежови протоколи:

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) е основен протокол в глобалната мрежа Интернет. TCP/IP е сложен протокол, който се състои от други протоколи. Първият и най-важен от тях е IP (Internet Protocol). IP протоколът използва технология за обмен на информация, наречена комутация на пакети. При комутация на пакетите, данните от едно съобщение, изпратено от един компютър към друг се разделят на пакети. Всеки пакет съдържа част от съобщението и служебна информация, като адрес на компютъра-получател, адрес

на компютъра, който изпраща съобщението. Отделните пакети се изпращат в мрежата. В зависимост от натоварването на мрежата, пътят на пакетите, може да бъде различен. При предвижването си пакетите се насочват от маршрутизатори. Когато всички пакети пристигнат в компютъра-получател, служебната информация се отстранява и се получава оригиналното съобщение. Използват се две версии на IP протокола – IPv4 и IPv6. IPv4 използва 32 битови интернет адреси, а IPv6 – 128 битови. Съответно структурата на пакетите е различна. Виж: Структура на IP пакет (IPv4), Структура на IP пакет (IPv6) IPv4 адресът се изписва като последователност от четири десетични числа, разделенис точка. Първото число е най-старшия октет (байт), следващите са младшите байтове.

RIP (Routing Information Protocol) е дистанционен векторен маршрутизиращ протокол. Подходящ е за малки вътрешни мрежи. Използва бродкастни съобщения. Представлява IGP протокол. Протокола има няколко предимства лесно се имплементира и управлява. Създава малко допълнителен служебен трафик м/у маршрутизаторите. Не е много стабилен при по големи и нарастване на мрежата. RIP може да се използва на крайни хостове или шлюзове. Работи в/у UDP и IP използвайки UDP порт 520, той функционира като протокол от мрежовия слой. RIP използва разстоянието като основната характеристика за определяне на най-добър маршрут колкото по-късо е разстоянието, толкова по-добър е маршрутът. Когато до местоназначението има множество маршрутизатори, маршрутизаторът, изпълняващ RIP, избира маршрута, който има най-късо разстояние за най-добър маршрут и го инсталира в маршрутизиращата таблица, след това използва тази информация за препращане на дейтаграмите.Независимо от това, че е един от най-популярните протоколи, използвани днес, RIP има следните недостатъци:

- Използва броадкастни съобщения. Изпраща цялата маршрутизиращата таблица, дори когато не настъпват промени

- Бавна конвергенция (уеднаквяване), дължаща се на периодичните таймери
- Има ограничение на максималното разстояние до 15 скока
- Предразположен е към зацикляне на маршрути.
- Той е класов маршрутизиращ протокол и следователно не поддържа VLSM маски

Съществуват две версии на RIP: RIPv1 и RIPv2.

Предназначен да се справи с някои от ограниченията на RIPv1, RIPv2 включва някои разширени възможности като поддръжка на автентификация и способност за разделяне на подмрежи. Някои организации преминаха на RIPv2 при използването на защитни стени. Но те използват RIPv2 защото им е необходима поддръжката на VLSM маски. Други маршрутизиращи протоколи, каквито са маршрутизиращите протоколи, отчитащи състоянието на връзките, бяха разработени, за да премахнат ограниченията на RIPv1 и предлагат много по-добри критерии за избор на маршрут, намалена консумация на пропускателна способност и по-бърза конвергенция от тези на RIPv2. Стойността на полето версия разбира се има стойност 2.

EIGRP (Enhanced Interior Gateway Routing Protocol) той е разработен от и е собственост на Cisco Systems. Той е базиран на IGRP, като са въведени много подобрения. Конфигурирането му е подобно на IGRP, но с много link-state характеристики, който са добавени за да позволят на EIGRP да обслужва по-големи корпоративни мрежи. Тези характеристики включват:

Бърза конвергенция (времето, което отнема за да се обработят промените в мрежата и да се влезе отново в оперативен режим);

Свободна от Loops (цикли) топология;

VLSM (variable length subnet masks) и обобщение на маршрутите;

Multicast

Намиране на маршрути едновременно за няколко рутирани протоколи (routed protocols).

1.6 Класификация на мрежите

Мрежите биват класифицирани според следните техни основни характеристики:

- физически обхват;
- метод на администриране;
- мрежова операционна система;
- мрежови протоколи;
- топология;
- архитектура.

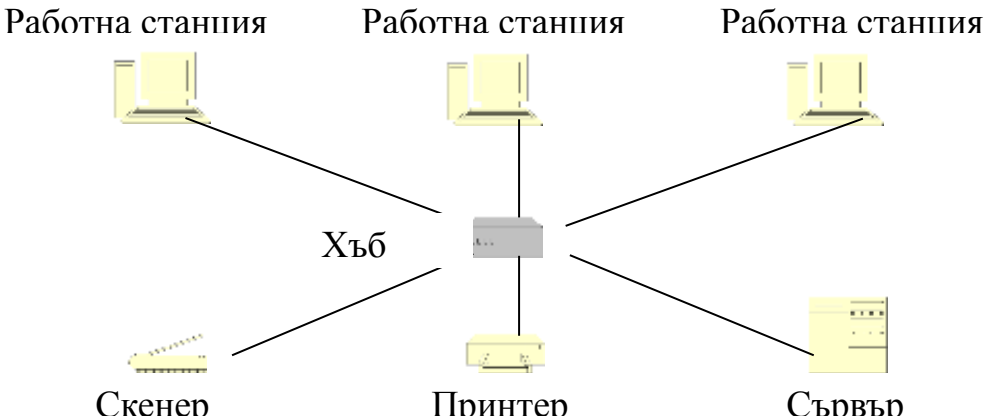
Ние ще разгледаме само някой от горепосочените класификации.

1.6.1 Класификация според физическия обхват

Под физически обхват следва да се разбира размера на географската област, в която е разположена мрежата, и на второ място броя на компютрите в нея. Според физическия си обхват мрежите биват:

- локални мрежи (LAN – Local Area Network);
- градски мрежи (MAN - Metropolitan Area Network);
- глобални мрежи (WAN – Wide Area Network).

LAN-мрежата обхваща ограничена географска област, като например: стая, етаж или сграда. Броят на компютрите в различните LAN би могъл да се различава съществено, като се започне от един два компютъра у дома или в офиса и се достигне до десетки дори стотици компютри, разположени в една сграда или в множество такива, намиращи се в близост една до друга. На фиг.11 е показана една примерна LAN, включваща три работни станции, скенер, принтер и сървър.

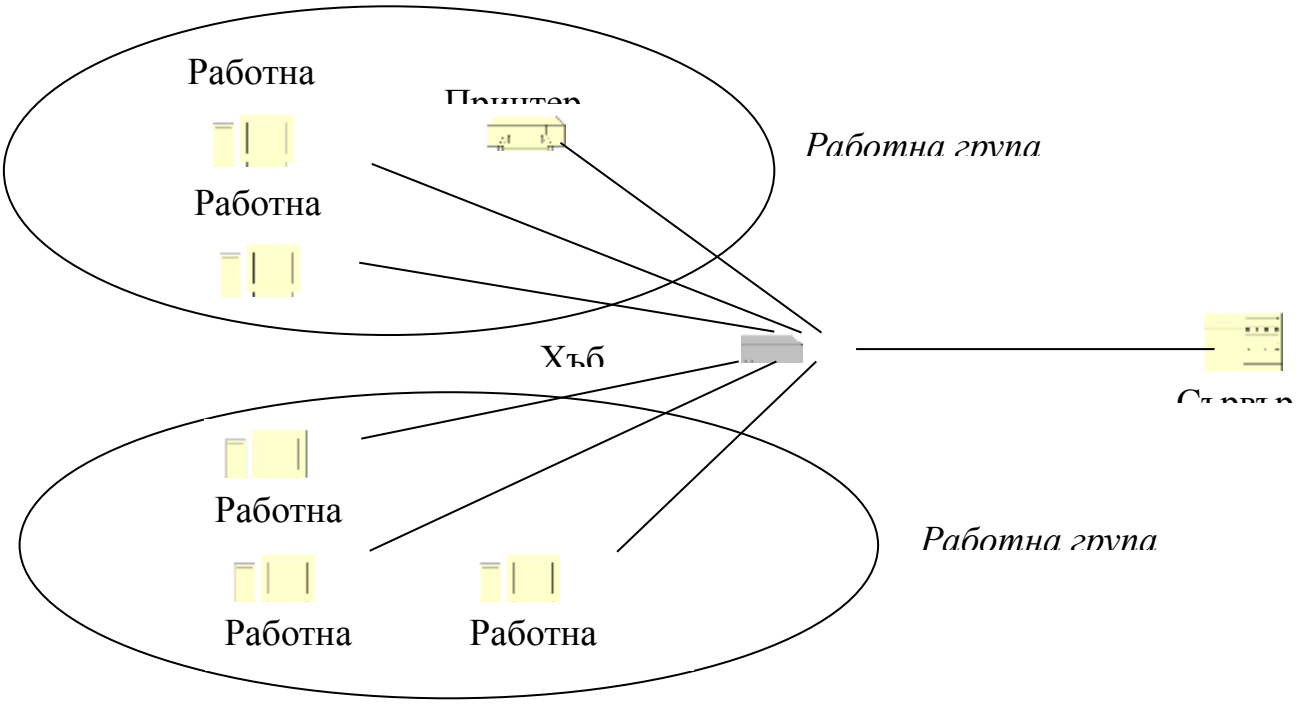


Фигура 11 - Пример за LAN мрежа

Терминът *работна станция* (workstation) означава, че компютърът работи под управление на своя собствена операционна система. Терминът се употребява още и за означаване на високопроизводителен компютър, използван най-често за извършване на сложна графична работа (графична работна станция). Работните станции изпълняват ролята на *клиенти*, т. е. на компютри, които използват споделяни в мрежата ресурси, осигурявани най-често от компютър, наричан *сървър*. Сървър е компютър, който споделя своите ресурси с останалите участници в мрежата, а хъбът ги свързва физически в мрежа.

За по-лесното им управление големите LAN биват разбивани на свързани помежду си *работни групи* (фиг.13). Под работна група следва да се разбира група от персонални компютри (потребители), които споделят общи ресурси като например: файлове, приложения, принтери и/или др. Например компютрите в

различните отдели (личен състав, счетоводство, продажби и др.) на едно предприятие могат да бъдат обособявани в отделни работни групи и последните свързани помежду си, образувайки една обща LAN.



Фигура 12 - Работна група

Когато в LAN-мрежа се използват протоколите и технологиите на Интернет, мрежата може да бъде определяна още и като *интранет*.

MAN-мрежите биват изграждани от две или повече LAN, разположени в границите на един град (в област с радиус не по-голяма от 50 до 80 км). По обхват те заемат междинно положение между LAN и WAN и често пъти вместо MAN биват квалифицирани като LAN или WAN. Затова определението MAN се среща рядко.

WAN обхваща широки географски области (повече градове, държави и дори континенти) и е изградена от свързани помежду си локални мрежи. Най-добрият пример за WAN е глобалната мрежа Интернет. Тя представлява множество

от различни по вид и топология компютърни мрежи, които са свързани помежду си и могат да комуникират с помощта на специално разработени интерфейсни протоколи (стандарти), които ги обединяват в една обща неразличима цялост.

Но WAN може да бъде и частна мрежа, обхващаща локалните мрежи на офисите на една фирма, чиито филиали са разположени в различни градове или страни. Такива WAN мрежи биват наричани още *интернет*. За разлика от глобалната Интернет, терминът се записва с малка начална буква. Когато в една частна WAN-мрежа се използват технологиите на Интернет, мрежата бива определяна като *екстранет*.

WAN-мрежите се подразделят на *разпределени* и *централизирани*. Разпределените, каквато е Интернет, нямат централна точка на управление, докато централизираните притежават централен сървър (например в главния офис на фирмата), към който са свързани всички останали компютри.

WAN-мрежите са *маршрутизирани* мрежи. Това означава, че пакетите, обменяни между LAN-мрежите, преминават през шлюзове (gateways). Шлюзът представлява специализиран компютър, наричан *маршрутизатор* (router), който изпълнява маршрутизиращите функции.

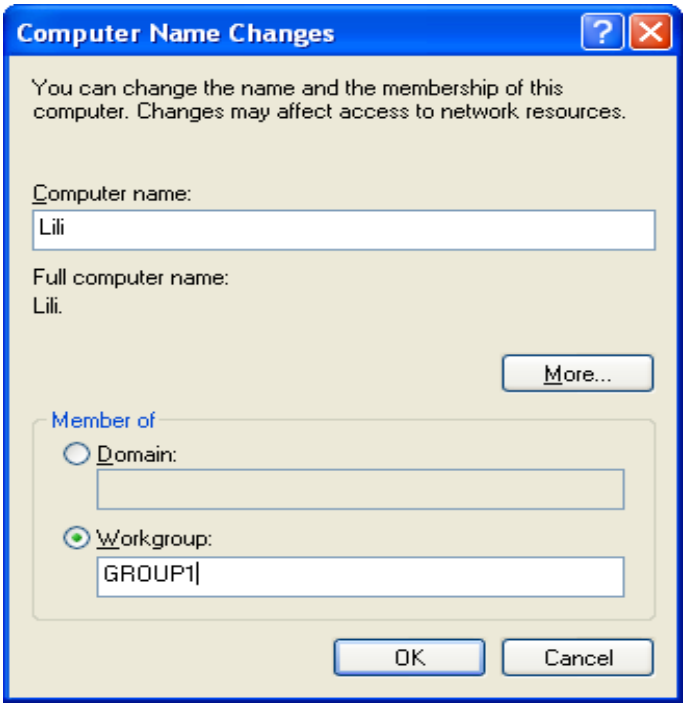
WAN-мрежите могат да използват частни или обществени среди за комуникация. WAN-връзките (връзките между LAN-мрежите) биха могли да бъдат постоянни (по кабел) или временни, които се изграждат по време на комуникацията. Временните връзки са по-често срещани. WAN-връзките са по правило по-бавни от LAN-връзките.

1.6.2. Класификация според метода на администриране

Една мрежа може да бъде организирана по два начина:

- като равноправна (peer to peer) работна група, в която всеки компютър може да изпълнява ролята на клиент или на сървър, при което всеки един от потребителите самостоятелно администрира ресурсите на своя компютър;
- като сървърно-базирана мрежа, администрирането на която е съсредоточено в един централен компютър, наричан сървър.

Равноправните мрежи са подходящи за малки мрежи, включващи не повече от 10 компютъра. Всички компютри в една такава мрежа образуват една обща работна група (workgroup). Това изисква всеки един от компютрите да бъде конфигуриран за работа в работна група. В Windows това се извършва чрез съответна настройка на компютъра за работа в мрежа, като името на работната група трябва да бъде едно и също за всеки един от компютрите. На фиг.13 е показан прозорецът, с чиято помощ в Windows XP се извършва задаване на имената на работната група и на конкретния компютър, участващ в мрежата.



Фигура 13 - Избор на работна група

Прозорецът се извежда с помощта на командата **Start/System/Control Panel/Computer Name** и щракване в последния изведен прозорец на бутона **[Change]**.

Администрирането в равноправните мрежи е децентрализирано. Всеки потребител отговаря за администрирането на своя компютър. Той създава потребителски акаунт и парола за онези потребители от мрежата, които ще ползват негови ресурси, като в акаунта указва кои от ресурсите (файлове и/или папки) могат да бъдат споделяни. В Windows XP за целта се използва помощната програма Network Setup Wizard, повиквана посредством командата **Start/Settings/Control Panel/Network Setup Wizard**.

Равноправната мрежа няма централна база данни, в която да се съхраняват всички използвани в мрежата потребителски акаунти и пароли. Последните следва да бъдат създавани и съхранявани на всяка отделна машина, което е неудобно (трябва да се помнят много пароли) и понижава сигурността в мрежата. Друг недостатък на равноправната мрежа е, че всеки един от потребителите трябва да бъде обучен да може да администрира ресурсите на своя компютър. Недостатъците на равноправните мрежи се избягват в сървърно-базираните мрежи.

В сървърно-базираните мрежи, наричани още мрежи клиент/сървър, администрирането на мрежата е *централизирано*, като същото е съсредоточено в сървъра. Потребителските акаунти се създават и съхраняват в сървъра. За да влезе в мрежата, всеки потребител трябва да притежава валиден потребителски акаунт и парола, създадени на сървъра. Отпада необходимостта от създаване на множество акаунти на различни машини и нуждата от запомняне на много пароли. Цялото администриране на мрежата е съсредоточено в едно лице, наричано *мрежов администратор*. Упражняването на контрол върху цялата мрежа от едно обучено

лице, вместо всеки един от крайните потребители да администрира собствения си компютър, повишава значително сигурността в мрежата и улеснява потребителите.

Сървърът, освен това, представлява компютър, който предоставя ресурси (данни, приложения и свързаните към него периферни устройства като принтер, скенер и др.) за ползване от другите компютри (клиентите), което улеснява ползването на споделяни ресурси.

В сървърно-базираните мрежи достъпът до ресурсите бива контролиран посредством *автентикация* (*authentication*) и *разрешения* (*permissions*). За всеки споделян ресурс мрежовият администратор задава разрешения (права на достъп) за всеки отделен потребител или за цяла работна група. Чрез разрешенията се указват нивата на достъп до ресурсите, например дали даден файл може само да бъде прочитан или в него могат да бъдат извършвани и промени (редакция или изтриване).

1.6.3. Класификация според мрежовата операционна система

Съвърите като правило са снабдени с мрежова операционна система (МОС). Последната е предназначена за управление на мрежата. Според типа на МОС мрежите биват:

- Windows-мрежа;
- NetWare-мрежа;
- UNIX-мрежа.

Някои от мрежите включват повече на брой сървъри, притежаващи различни МОС. Такива мрежи биват наричани *хибридни*.

Модерните МОС като правило използват *директорийна услуга* (*directory service*). Тя служи за съхраняване и осъществяване на достъп до информация, касаеща мрежовите ресурси, акаунти и услуги. Директорийната услуга се състои от два компонента – *директория* и *услуга*.

Понятието *директория* е познато от файловите системи. Там тя представлява място за съхранение на файлове, групирани под едно общо име – името на директорията. Когато се говори за МОС, понятието директория придобива друг смисъл. В МОС директорията представлява специална *обектно-ориентирана база данни*, която организира информацията в логическа структура. В нея, под формата на обекти, се съдържа необходимата информация за обслужване на мрежата. Такива обекти са например потребителските акаунти. Посредством атрибутите си всеки един от обектите съхранява (под формата на стойности): собствените имена на потребителя, потребителското му име, паролата на акаунта и евентуално някаква друга информация. Част от атрибутите на обектите биват задължителни, а други опционални.

Windows-мрежи

Сървърно-базираните Windows-мрежи се състоят от домейни. *Домейн* е група от компютри, представляващи част от мрежа, която споделя обща *директорийна база данни*. Домейнът бива администриран с общи правила и процедури и притежава свое уникално име.

Директорийната услуга *Active Directory* (въведена с Windows 2000) е стандартна за Windows-мрежите. Тя поддържа стандарта LDAP и използва, макар и не напълно, конвенциите на X.500 за именуване. Active Directory съхранява информация относно обектите в мрежата, която бива предоставяна за ползване на потребителите и администраторите. Логическата структура на Active Directory се състои от домейни, подредени йерархично в дървета (domain trees) и гори (forests).

Друга йерархична разпределена база данни, използвана в Windows-мрежите, е DNS (Domain Name System). Тя представлява дърво, съставено от поддървета. Както Active Directory и тя от своя страна представлява домейн, но различен от Active Directory.

NetWare-мрежи

Друга популярна мрежова операционна система е Novel NetWare. С нейна помощ биват изграждани NetWare-мрежи. Започвайки от версия 4, нейната директорийна услуга се нарича NetWare Directory Services (NDS). В по-старите версии базата данни се наричаше Bindery. Както Active Directory NDS поддържа стандарта LDAP и макар и не напълно, използва конвенциите на X.500 за именуване. NDS представлява йерархична база данни, подобна на Active Directory. Освен с NetWare, NDS би могла да работи и на множество други платформи, като например: Microsoft Windows, Sun Solaris, SCO UNIX и др., а версията Net eDirectory представлява междуплатформено решение

UNIX-мрежи

UNIX-мрежите използват мрежовата операционна система UNIX, използвана за първи път в ARPAnet. Днес широко разпространение получи Linux, представляваща вариант на UNIX. Linux може да работи както като сървър, така и като настолна операционна система. Както UNIX, така и Linux представляват продукти с отворен код, което позволи на много компании по света да разработят и предложат на пазара свои версии.

1.7 Какво е VLAN

Виртуална локална мрежа (на английски: Virtual Local Area Network, VLAN) представлява метод за разделяне на една физическа компютърна мрежа на различни виртуални мрежи с цел логическа организация, контрол и защита.

Потребителите в един VLAN могат да комуникират само помежду си, но не и с потребители от другите виртуални мрежи. Предимството е, че едни и същи комутатори могат да предоставят множество VLAN-и и по-този начин се спестяват разходи за оборудване. Като пример може да се разгледа мрежа на фирма с три отдела, разположени на три етажа – Инженерен (Engineering), Маркетинг (Marketing) и Счетоводен (Accounting). Във фирмата има една физическа LAN мрежа, която се използва от всички отдели, но всеки отдел е обособен в собствен VLAN. Различните портове на комутаторите са конфигурирани да предоставят достъп до различните VLAN-и. Служителите на Маркетинг отдела на първи и втори етаж могат да се достигнат един друг и имат достъп до техния сървър, но не могат да достъпят сървърите и служителите на другите два отдела. Ако не се използват VLAN-и, ще е необходимо да се изградят три отделни физически мрежи – по една за всеки отдел, което би оскъпило решението поне три пъти.

Глава II. Мрежов Хардуер

Мрежовият хардуер включва редица устройства, които действат на различни нива в многослойния OSI модел (фиг.9).

2.1. Мрежови интерфейсни карти

Мрежовата карта (NIC – Network Interface Card), наричана още мрежов адаптер е устройство от физическия слой . Драйверите за нея осъществяват връзката между картата и операционната система. Те работят в каналния слой на OSI модела. Когато връзката на компютъра с мрежата се осъществява дистанционно, посредством телефонна линия, вместо мрежова карта се използва модем.

Мрежовата карта преобразува формата на сигнала от паралелна в последователна (серийна). Единиците и нулите се преобразуват в: електрически импулси, светлинни импулси, радиовълни или инфрачервени лъчи. Важна съставна част на мрежовите карти е приемопредавателят, наричан *трансивър (tranceiver)*. Както показва названието му той извършва предаване и приемане на сигналите. В Ethernet картите от типа 10Base5 (thicknet) трансивърът е външен. Картата притежава конектор от тип AUI, посредством който, чрез кабел, тя се свързва към външния трансивър, който пък от своя страна бива съединяван с дебелия коаксиален кабел.

В съвременните компютри Ethernet картите са интегрирани в дънната платка (motherboard). Най-често те са два броя. Осигуряват три скорости на предаване – 10, 100 и 1000 Mbps, отговарящи съответно на 10BaseT, 100BaseT и 1000BaseT. Връзката с мрежата се осъществява посредством конектори от типа RJ-45 и кабел UTP (неекранирана усукана двойка).

Когато картата представлява отделна платка, тя се поставя в някой от свободните разширителни слотове на дънната платка. Необходимо е данновата

шина на картата да съответства на данновата шина на слота. Например една PCI мрежова карта следва да се постави задължително в PCI слот.

След поставяне на мрежовата карта в слот тя трябва да бъде конфигурирана. За нея следва да бъдат установени едно прекъсване IRQ, входно/изходен адрес и адрес от паметта, ако картата изисква такъв. Конфигурирането се извършва чрез dip-превключватели или джъмпери, намиращи се върху картата, или чрез програма за софтуерно конфигуриране, доставяна заедно с картата. PnP (Plug and Play) мрежовите карти биват автоматично откривани и конфигурирани от операционната система (при условие, че и BIOS-ът поддържа PnP).

2.2. Мрежова преносна среда

Мрежовата преносна среда служи за пренасяне на сигналите от едно мрежово устройство до друго. Тя може да бъде *жична* (кабелна) и/или *безжична* (радиовълни, лазерни лъчи, инфрачервени лъчи, микровълни). Кабелите, както е известно (т.2.6), биват медни и оптични. Към медните спадат коаксиалните кабели (тънък и дебел) и кабелите от тип усукана двойка (UTP и STP).

Безжичните технологии, въпреки че отстъпват на жичните по бързодействие, стават все по-популярни. Те са особено подходящи за потребители, които се намират в движение, или за такива, които желаят да комуникират с мрежата от дистанция. Безжичните технологии намират приложение в безжичните LAN и WAN мрежи. Фирмата Cisco Systems заедно с Motorola, Texas Instruments, Samsung и др. разработват висикоскоростни, сигурни и широко достъпни безжични технологии.

2.3. Устройства за изграждане на локални мрежи

Освен компютри, кабели и конектори в състава на локалните мрежи участват и специални устройства. Към тях спадат: конверторите на преносната среда, повторителите, хъбовете, мостовете, комутаторите и маршрутизаторите.

Конвертори на преносната среда

Наричат ги още адаптери за *преносна среда (media adapters)* или *транслатори на преносна среда (media translators)*. Извършват преобразуване на електрическите импулси на 10BaseT, 100BaseT и 1000BaseT или на Token Ring в светлинни импулси, предавани по оптичен кабел.

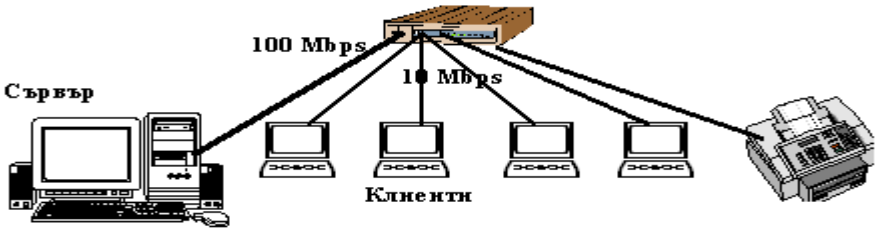
Повторители

Повторителят (repeater) се използва за *регенерация на сигнала*, когато затихването му надхвърля допустимите норми. Те усилват сигнала без да могат да премахват (филтрират) смущенията, насложени върху него. Степента на затихване се обуславя от характеристиките на кабела и се определя чрез максималната дължина на кабелния сегмент. Например максималната дължина на тънкия коаксиален кабел, използван за Ethernet от тип 10Base2, е 185 метра. При необходимост от по-дълъг сегмент се вземат две парчета кабел, като между тях се включва повторител.

Хъбове

Хъбовете (hubs), наричани още *концентратори*, биват пасивни, активни и интелигентни. Всички те работят във физическия слой на OSI модела (фиг.9). Използват се за свързване на елементите на LAN в топология звезда. Съдържат повече на брой равноправни портове, към които се свързват кабелите на отделните

елементи (фиг.14). Хъбовете биха могли да се съединяват един с друг с цел създаване на по-сложни топологии.



Фигура 14 - Свързване към Хъб

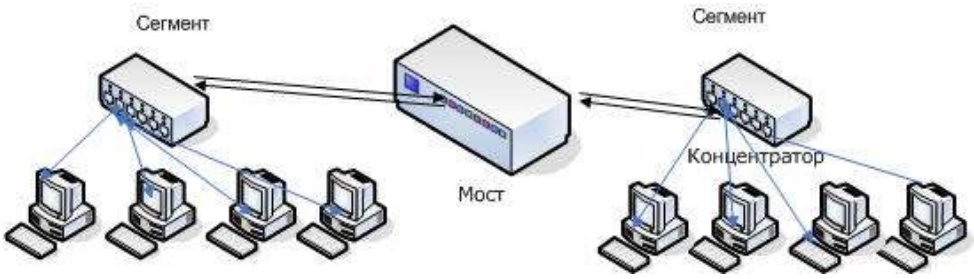
Пасивният хъб не съдържа електроника, поради което не изисква електрическо захранване. Сигналът, идващ от даден порт, се препраща на всички портове без регенериране.

Активният хъб съдържа електроника, която регенерира идващия от даден порт сигнал, преди той да бъде изпратен на останалите портове. Поради това си качество активните хъбове биват наричани понякога многопортови повторители (multiport repeaters). Активните хъбове изискват електрическо захранване.

Интелигентният хъб представлява специален вид активен хъб, позволяващ на оператора да контролира трафика през хъба, да конфигурира портовете и да извършва диагностика на същите. Поради това ги наричат още *управляеми хъбове* (*manageable hubs*).

Мостове

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.17).



Фигура 15 - Свързване чрез Bridge

Мостовете работят на второто ниво (каналния слой) на модела OSI (фиг.9). 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.

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.

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).

Маршрутизатори

Маршрутизаторите (routers) работят на ниво мрежов слой на OSI модела. Те служат за свързване на мрежи с различни топологии и архитектури. Когато биват свързвани две мрежи с несъвместим протокол, маршрутизаторът изпълнява ролята на *шлюз (gateway)*. В LAN те свързват подмрежи, а във WAN независими една от друга мрежи, каквито например срещаме в Интернет. Подобно на мостовете маршрутизаторите филтрират или препредават пакетите, но вместо физически хардуерни MAC адреси те използват логически мрежови адреси (IP или IPX адреси).

Маршрутизаторите са по-интелигентни устройства от мостовете. Те са в състояние да определят най-добрия маршрут до дадено местоназначение измежду множество възможни пътища. За целта те поддържат маршрутни таблици (forwarding tables), съдържащи мрежовите адреси и на други маршрутизатори.

Един маршрутизатор трябва да притежава поне два мрежови интерфейса, посредством които да могат да се свързват две мрежи. Като правило те притежават един WAN порт за връзка с Интернет посредством ISDN адаптер, ADSL адаптер или модем и поне един порт за връзка с LAN (фиг.21).

Фигура 16 - Маршрутизатор

Когато един маршрутизатор получи пакети, предназначени за отдалечена WAN мрежа, той ги изпраща на маршрутизатора, който обслужва тази мрежа. Маршрутизаторите на WAN мрежите могат да комуникират само с други маршрутизатори. Те не могат да комуникират директно с отдалечени компютри.

Маршрутизаторите от среден клас могат да изпълняват и функциите на хъбове и суичове. Като правило в тях е интегриран Ethernet суич или хъб (с 4 до 8 порта), което позволява на потребителите лесно да изграждат LAN мрежа, която би могла да споделя файлове и принтерски услуги и да има достъп до Интернет. Маршрутизаторите от нисък клас са снабдени само с единичен LAN порт (вместо с интегриран хъб или суич), предназначен за връзка с външен хъб или суич.

Маршрутизаторите от висок клас притежават около 50 порта с най-различно предназначение, между които и USB-порт и възможност за безжична връзка. Те интегрират в себе си и NAT-устройства (NAT boxes). NAT (Network Address Translator) е Интернет стандарт, който позволява използване в LAN на две множества от IP-адреси – вътрешно и външно. Вътрешното е предназначено единствено за трафика вътре в LAN, докато външното е за външния трафик. NAT извършва преобразуване на вътрешните адреси във външни и обратно. Възможността да се ползват вътрешни адреси позволява на корпорациите да увеличават броя на отредените им IP-адреси. Вътрешните адреси не се виждат извън LAN, поради което не е възможно възникване на конфликти с вътрешни адреси на други корпорации. NAT-устройствата извършват преобразуване на адресите по хардуерен път.

Маршрутизаторите от висок клас включват в себе си още DHCP (Dynamic Host Configuration Protocol) сървър, DNS (Domain Name Service) proxy-сървър и хардуерна защитна стена (firewall) за защита на LAN от злонамерени външни атаки през Интернет.

Комутатори

Основното предназначение на комутаторите (суичовете, switches) е да избират пътя, по който данните да бъдат изпращани до тяхното предназначение (фиг.17).

Съществуват различни типове комутатори. Те биват категоризирани според OSI слоя, на който те работят.

Комутатори от ниво 2. Действат подобно на хъбовете. Различават се по това, че хъбът изпраща пакетите до всички портове, докато при комутаторите всеки пакет бива *комутиран*, като се изпраща само на онзи порт, респективно компютър, за който е предназначен. Поради тази причина комутаторите от този тип биват наричани още *комутиращи хъбове (switching hubs)* или *портови комутатори (port switches)*.

Комутаторите от ниво 2 премахват ненужния трафик в мрежата, като същевременно увеличават сигурността на комуникацията. Тъй като съобщенията не се изпращат до всички портове, това намалява вероятността от прихващането им.

Друг вид комутатори от този тип са *сегментните комутатори (segment switch)*. Те позволяват към портовете да се свързват цели мрежови сегменти, съдържащи повече компютри. LAN мрежи, които използват комутатори за свързване на мрежови сегменти, биват наричани *комутирани LAN*.

Фигура 17 - Свързване чрез комутатор

Комутатори от ниво 3. Те работят в мрежовия слой на OSI модела, като могат да изпълняват едновременно функциите на маршрутизатори и на комутатори от ниво 2. Те представляват комбинация от маршрутизатор и комутатор, поради което биват наричани още *комутиращ маршрутизатор (switched router)*.

Комутатори от ниво 4. Това са комутатори от ниво 3, които допълнително оперират с информация от транспортния слой на OSI модела. По-конкретно те използват номерата на портовете, съдържащи се в TCP и UDP хедърите.

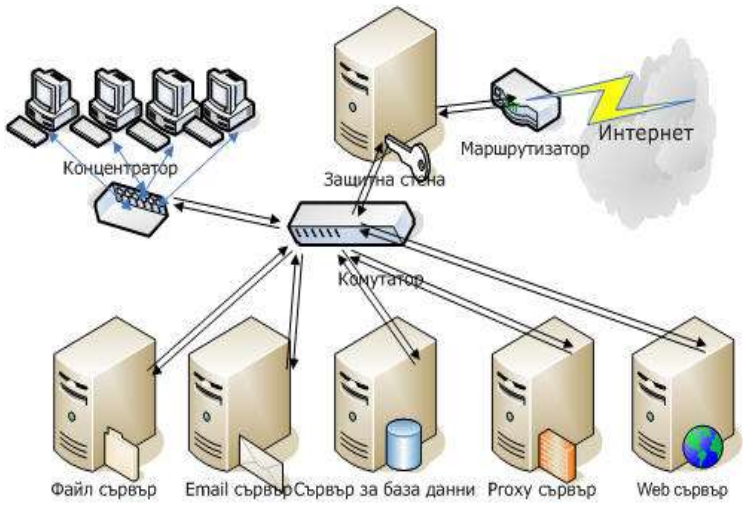
Накратко за различията между хъбовете, комутаторите и маршрутизаторите

На фиг.18 е показана конфигурация на мрежа с участието на гореизброените устройства. Връзката с Интернет е осъществена посредством маршрутизатор. В центъра на мрежата се намира комутатор (суич), който избира пътя, по който данните биват изпращани до тяхното предназначение.

Комутаторите се различават от хъбовете (концентраторите) по това, че всеки пакет бива *комутиран*, като се изпраща само на онзи порт, респективно компютър или мрежов сегмент, за който е предназначен. При хъбът (на фиг.21 означен като концентратор) всеки един пакет бива изпращан до всички негови портове, т.е. до всички компютри едновременно. Пакетът се възприема само от

онази мрежова карта, респективно компютър, за която е бил предназначен. Недостатък на хъбовете в сравнение с комутаторите от ниво 2 е, че пропускателната им способност зависи от броя на компютрите, извършващи едновременно комуникация, тъй като честотната лента на хъба се разпределя между повече потребители. При суичовете пропускателната способност остава винаги една и съща, независимо от броя на комуникиращите компютри, свързани към него. Честотната лента на комутатора се ползва цялостно само от един потребител – само от онзи, за когото пакетът е предназначен. По отношение на пропускателната способност суичовете са по-добри устройства от хъбовете.

Най-често хъбовете се използват за изграждане на мрежови сегменти, а суичовете, като по-ефективни от хъбовете, за интегриране на повече такива сегменти в една обща LAN мрежа.



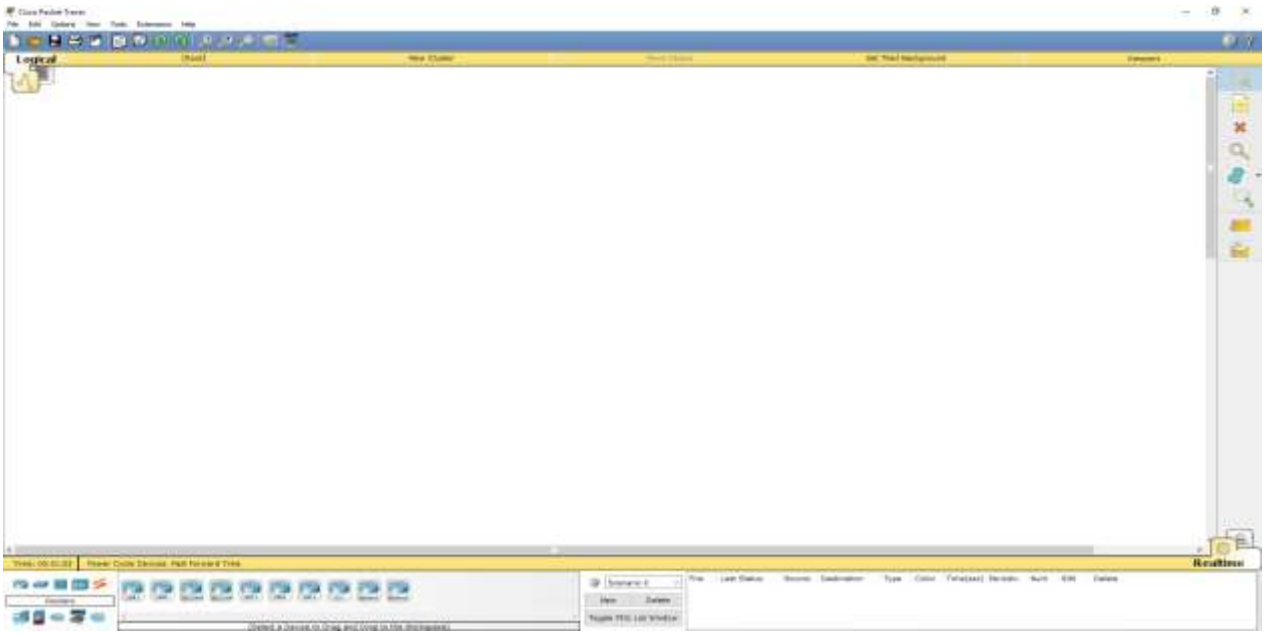
фигура 18 - Конфигурация чрез различни мрежови устройства

Маршрутизаторите (рутерите) са коренно различни устройства от хъбовете и комутаторите. Те определят най-късия маршрут, по който пакетите биват изпращани от една мрежа до друга. Докато хъбовете и комутаторите работят с MAC-адреси на канално ниво, маршрутизаторите използват логически адреси (IP и IPX адреси) на ниво мрежов слой.

ГЛАВА III. Проектиране на мрежа за нуждите на компания от средния бизнес

3.1. Мрежов симулатор Packet Tracer

За целите на настоящата дипломна работа, ще използваме софтуер за създаване на мрежови среди. Програмата се нарича Packet Tracer. Тя се използва за визуална мрежова симулация и е проектирана от Cisco Systems, позволявайки на потребителите да създават мрежови топологии и имитират съвременните компютърни мрежи. Софтуерът дава възможност на потребителите да симулират конфигурацията на Cisco маршрутизатори и комутатори с помощта на симулиран интерфейс и команден ред. Програмата е насочена основно към Сертифицирани студенти Cisco Network Associate академия като образователно средство за подпомагането им да научат основни понятия CCNA. Началният прозорец на програмата е показан на фиг.19.



Фигура 19 - Packet Tracer начален прозорец

3.2 Въведение в Cisco IOS.

Cisco IOS (Internetwork Operating System) е софтуера, използван от повечето Cisco Systems рутери и текущите мрежови комутатори Cisco. (По-ранни

комутатори работеха на CatOS.) IOS е пакет от всички мрежови функции, интегрирани в една многозадачна операционна система. Въпреки че кодовата база IOS включва кооперативна многозадачност на ядрото, повечето IOS функции са били пренесени към други ядра като QNX и Linux за използване в Cisco продукти или симулатори като VIRL.

Не всички Cisco продукти работят с IOS. Изключения са продукти като ASA (Adaptive Security Appliance),които комбинират в себе си защитна стена, система против проникване, Антивирусна система и VPN (Virtual Private Network), тези устройства работят под Linux. Някой от най високия клас рутери на Cisco използват IOS XR.

Cisco IOS има три командни режими, всеки с достъп до различни командни комплекти:

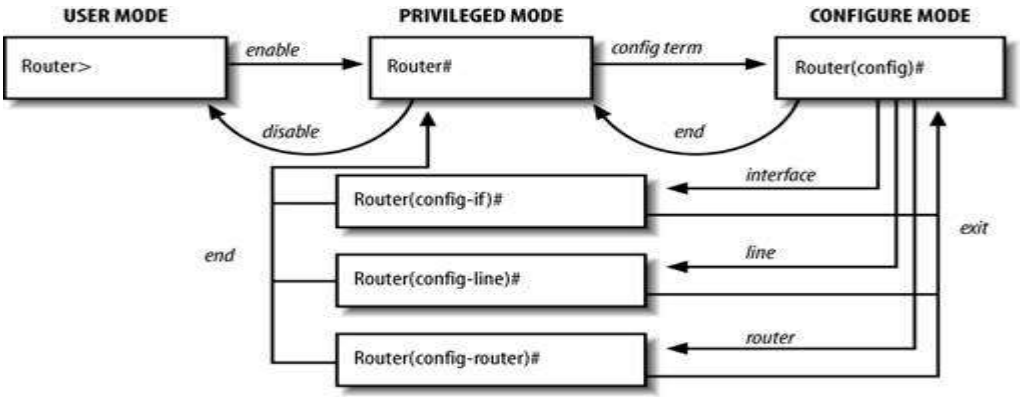
User mode (Потребителски режим) - е първия режим, в който потребител има достъп след като влезете в рутера. Режимът на потребителя могат да бъдат идентифицирани чрез > ред след името на рутера. Този режим позволява на потребителя да изпълнява само основните команди, като например тези, които показват състоянието на системата. Устройството не може да бъде конфигурирано или рестартирано от този режим.

Privileged mode (Привилегировани режим) - Този режим позволява на потребителите да гледат конфигурацията на системата, да рестартират системата, и да влизат в режим на конфигурация. Той също така позволява всички команди, които са налични в потребителски режим. Привилегировани режим могат да бъдат идентифицирани чрез # ред след името на рутера. Потребителския режим позволява използването на командата IOS, която показва, че потребителят иска да влиза привилегирован режим. Привилегирования режим позволява на потребителя

да направи всичко на рутера, така че трябва да се използва с повишено внимание. За да излезете от привилегирован режим, потребителят изпълнява команда disable.

Configuration mode (режим конфигурация) позволява на потребителите да променят конфигурацията на работеща система. За да влезе в режим на конфигурация, въведете командата configure terminal от Privileged mode (Привилегировани режим). Режим конфигуриране има различни submodes(под режими) , като се започне с global configuration mode (глобален режим конфигурация), която може да се идентифицира с **(config) #** ред след името на рутера. Зависи от промяната, която е направена от подрежима на configuration mode, думите в скобите се променят. Например, когато въведете конфигурация submode интерфейс, най-бързо се забелязва промяната в (config-if) # и името на рутера. За да излезете от режима на конфигурация, потребителят може да въведе командата end или комбинацията от клавиши Ctrl-Z.

Може да видите как се идентифицират режимите на операции на фигура 21.



Фигура 20 - Режими на операции

Имайте предвид, че в тези режими, въвеждане на контекстно-зависима команда **?** във всеки момент показва наличните команди на това ниво. Въпросителната команда **?** може да се използва в средата на команден ред, за да

покаже възможни варианти за завършване. Примерът по долу показва използването на **?** за да може да се покажат възможноите опции за текущия режим.

Router>?

Exec commands:

access-enable Create a temporary Access-List entry

access-profile Apply user-profile to interface

clear Reset functions

Може да видите и някои от командите които се използват в потребителски режим, чрез които се следи статуса на устройството на таблица 1.

Cisco IOS Command	Description
show interface	Показва текущия статус и конфигурация на целия интерфейс в системата.
show processes CPU	Показва натоварване на процесора и протичащите процеси, работещи в системата
show buffers	Показва как системата буфери са разпределени понастоящем и функциониращи за препращане на пакети
show memory	Показва колко памет се разпределя към различните функции на системата и колко е използваната памет.
show diag	Показва подробна информация за хардуера в системата
show ip route	Показва текущата активна маршрутизирана IP таблица
show arp	Показва текущия активен IP адрес към MAC адрес в ARP таблицата

Таблица 1 - Основни Cisco команди

3.3 Изграждане на Мрежа

Мрежата, която ще изградим през Packet Tracer, ще се състои от 2 офиса. Офис Бургас и Офис Унибит, те ще бъдат свързани към един и същ интернет доставчик. Всеки от бранчовете ще има следните мрежови устройства.

- Три комутатора свръзани помежду си с активен STP(Spanning tree protocol).
- Два рутера, които ще свързват офиса с Data Center-а презназначен за него, посредством статично рутиране.
- Един Безжичен рутер, за да могат лаптоп потребителите да не бъдат зависими от кабелния интернет.
- В центъра за данни (Data Center) ще има два сървъра единия от които ще бъде DNS сървър а другият ще бъде FTP сървър, от където потребителите ще могат да теглят и споделят данни с другите потребители.
- За да изградим интернет доставчика, ще са ни нужни един рутер, два DSL модема, които да пускат интернет на рутерите пред Data Center Бургас и Унибит и един DNS сървър.

3.4 Конфигурация на устройствата в Офис Бургас.

За повече информация може да видите ***Приложение 1***. Конфигурация Офис Бургас:

Ще започнем настройването на устройствата в Бургас първо с конфигурация на маршрутизатора, започваме с въвеждането на следните командите.

```
Router>en
Router#configure terminal
Router(config)#hostname
RTRBGSRTRBGS(config)#wr
Building configuration...
[OK]
```

Чрез командата **hostname** ние избираме какво да бъде името на рутера.

Ако не искаме да изгубим настройките които са направени до момента е нужно да въведем командата **wr** .

Маршрутизаторът трябва да поддържа ISL или 802.1Q канали на FastEthernet или GigabitEthernet интерфейс, за да извършва маршрутизация между различни VLANs. Интерфейса на рутера е разделен на логически връзки, наречени subinterfaces, по един за всеки VLAN. От FastEthernet или GigabitEthernet интерфейс на рутера, можете да настрои интерфейса за извършване на канали с командата капсулиране:

```
RTRBGS(config)#int fa0/0.10 – Създаване на подинтерфейс с ID:10
RTRBGS(config-subif)#encapsulation dot1q 10
RTRBGS(config-subif)#ip address 192.168.10.1 255.255.255.240
```

Сега създадохме и конфигурирахме под интерфейс 10. В по - горната конфигурация зададохме капсулирането да е зададено като IEEE 802.1Q за Inter-VLAN маршрутизация на VLAN 10.

Задавайки маска 255.255.255.240 ние позволяваме да се ползват само 14 хоста в този VLAN.

Използвайки горепосочените команди, ние ще създадем още 2 подмрежи в рутера RTRBGS. Детайли за виртуалните мрежи може да видите в таблица 1.

VLAN Име	VLAN ID	Network	Subnet Mask	Default Gateway	IP DHCP Scope
Admin	10	192.168.10.0	255.255.255.240	192.168.10.1	192.168.10.1-14
Sales	30	192.168.20.0	255.255.255.128	192.168.20.1	192.168.20.1-126
Management	40	192.168.20.128	255.255.255.128	192.168.20.129	192.168.20.129-254

Таблица 2 - VLAN детайли офис Бургас

След като сме готови със създаването на VLAN-овете, трябва отново да влезем в режим на конфигурация, да изберем интерфейса, който конфигурирахме до сега Fast Ethernet 0/0 и да напишем командата **no shutdown** за да активираме избраният от нас интерфейс.

```
RTRBGS(config)#int fa0/0
RTRBGS(config-if)#no shutdown

RTRBGS(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.40, changed state to up
```

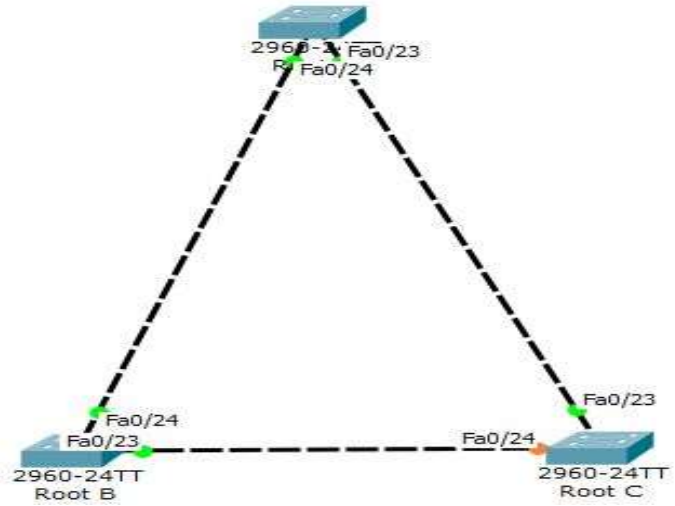
След като вече сме създали виртуалните мрежи и сме активирали порта да работи, сега трябва да стартираме *Протокол за динамично конфигуриране на хостове(DHCP)*. Чрез този протокол, ние ще зададем автоматично раздаване на диапазон от IP адреси за всеки VLAN. Така ще си спестим време, като не задаваме статични IP адреси за всяка мрежа.

```
RTRBGS(config)#ip dhcp pool 10 – създаване на DHCP pool за влан 10
RTRBGS(dhcp-config)#network 192.168.10.0 255.255.255.240 – посочване на мрежата исубнет маската за ВЛАН-а
RTRBGS(dhcp-config)#default-router 192.168.10.1 – задаване на default gateway
RTRBGS(dhcp-config)#dns-server 10.20.20.2 – задаване на DNS сървър
```

Горепосочените команди ще бъдат повторени за останалите два VLAN-а (30,40) като ще се заменят всички IP адреси с тези от таблица 1, единствено IP адреса на DNS сървъра, ще си остане същия. След като сме създали вече готовите DHCP басейни, за всеки VLAN е добре да изключим раздаването на IP адреса на Default-router за да не се получават конфликти в мрежата. Това става с командата **dhcp excluded-address** ,която се въвежда в режим конфигурация.

```
RTRBGS(config)#ip dhcp excluded-address 192.168.10.1
RTRBGS(config)#ip dhcp excluded-address 192.168.20.1
RTRBGS(config)#ip dhcp excluded-address 192.168.20.129
```

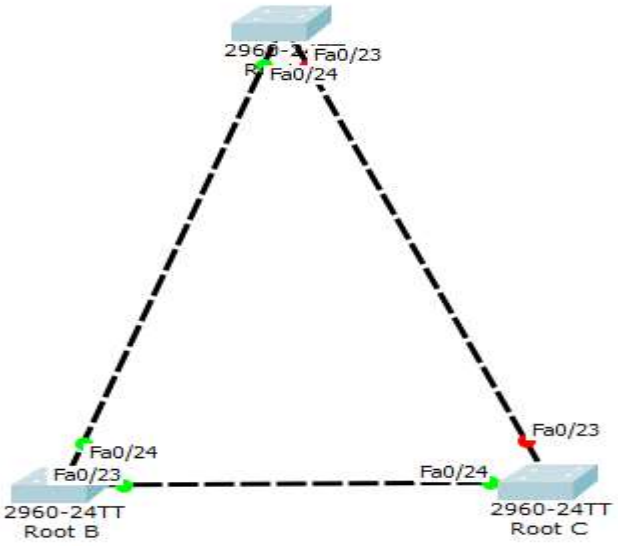
За момента приключваме с конфигурацията на интерфейс fa0/0 на рутер RTRBGS и преминаваме към конфигурацията, поставянето и свързването на суичовете. Ще поставим три суича, които ще бъдат вързани последователно, триъгълна топология. Фиг.21



Фигура 21 - Свързване на суичове офис Бургас

Както се вижда на фиг.22 интерфейс 0/24 на суич RootC свети в оранжево. Това е защото всички Layer 2 суичове имат включен *STP(spanning tree protocol)*, който предотвратява образуването на нежелание повторения в мрежата.

Ако направим тест и деактивираме интерфейс 0/23 на суич RootC, ще видим че порт 0/24, ще стане автоматично активен, защото STP протокола ще го отблокира фиг.22



Фигура 22 - Тест STP Протокол

Portfast е една от опциите на STP протокола, чрез която позволява устройството, което е закачено на дадения порт да се свърже в мрежата незабавно, заобикаляйки предоговарянето с режими listening и learning и отива директно на режим forwarding. Portfast е най добре да се използва само когато вързваме компютър към суич, но не и когато вързваме суич към суич, защото е възможно така да създадем повторения в мрежата.

Със следната команда, ние ще зададем на обсег от портове 0/1 до 0/20, към които очакваме да вържем компютри или други устройства различни от

комутатори, за да може да избегнем излишното изчакване вързвайки ги към локалната мрежа.

```
RootA(config)#int range fa0/1-20
RootA(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast will be configured in 20 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode
```

След като сме свързали трите суича, сега трябва да създадем трите VLAN-а във всеки един от тях, със следните команди:

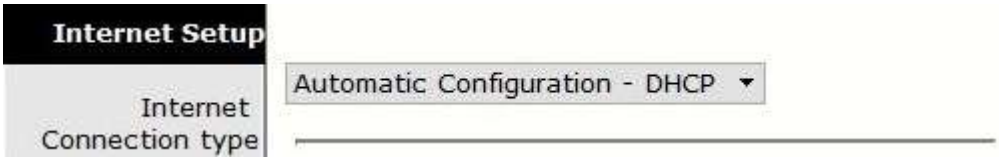
```
RootA(config)#vlan 10
RootA(config-vlan)#name Admin
RootA(config-vlan)#exit
RootA(config)#vlan 30
RootA(config-vlan)#name Sales
RootA(config-vlan)#exit
RootA(config)#vlan 40
RootA(config-vlan)#name Management
```

Преди да вържем главния комутатор към рутера, трябва да настроим портовете между тях в Trunk mode за да бъде възможно пропускането на VLAN информация през рутера към главния суич RootA, и от RootA до останалите суичове, както и между тях.

Това може да се случи с командата показана отдолу. Чрез **interface range fa0/23-24** ние избираме да конфигурираме заедно обсег от портове. А чрез командата **switchport mode trunk** задаваме режима на интерфейса.

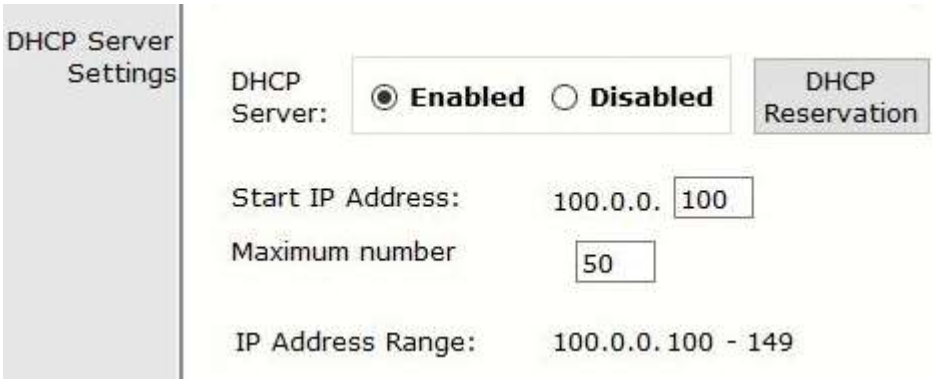
```
RootA(config)#interface range fa0/23-24
RootA(config-if-range)#switchport mode trunk
```

Преди да свържем главния суич към маршрутизатора, нека да конфигурираме и един безжичен рутер за лаптопите в офиса. Фигура 23. В полето до Internet connection type, избираме опцията Automatic configuration – DHCP, това означава, че безжичния рутер, ще взима IP адрес автоматично, в зависимост от зададения влан, интерфейса към който е свързан.



Фигура 23 - Избор тип свръзване на Безжичен рутер

Във Фигура. 24, ще видим опциите, които предлага DHCP сървъра, на безжичния рутер. Там е показано обсега от IP адреси, които ще бъдат раздадени на свързаните устройства, както и максималния им брой.



Фигура 24 - DHCP настройки

След всяка конфигурация направена на безжичното устройство, трябва да натискаме върху бутона Save Settings Фиг.25

Фигура 25 - Save бутон

Когато приключим с настройките в менюто **Setup** продължаваме с конфигуриране на името на безжичната мрежа както и със защитата му с парола.

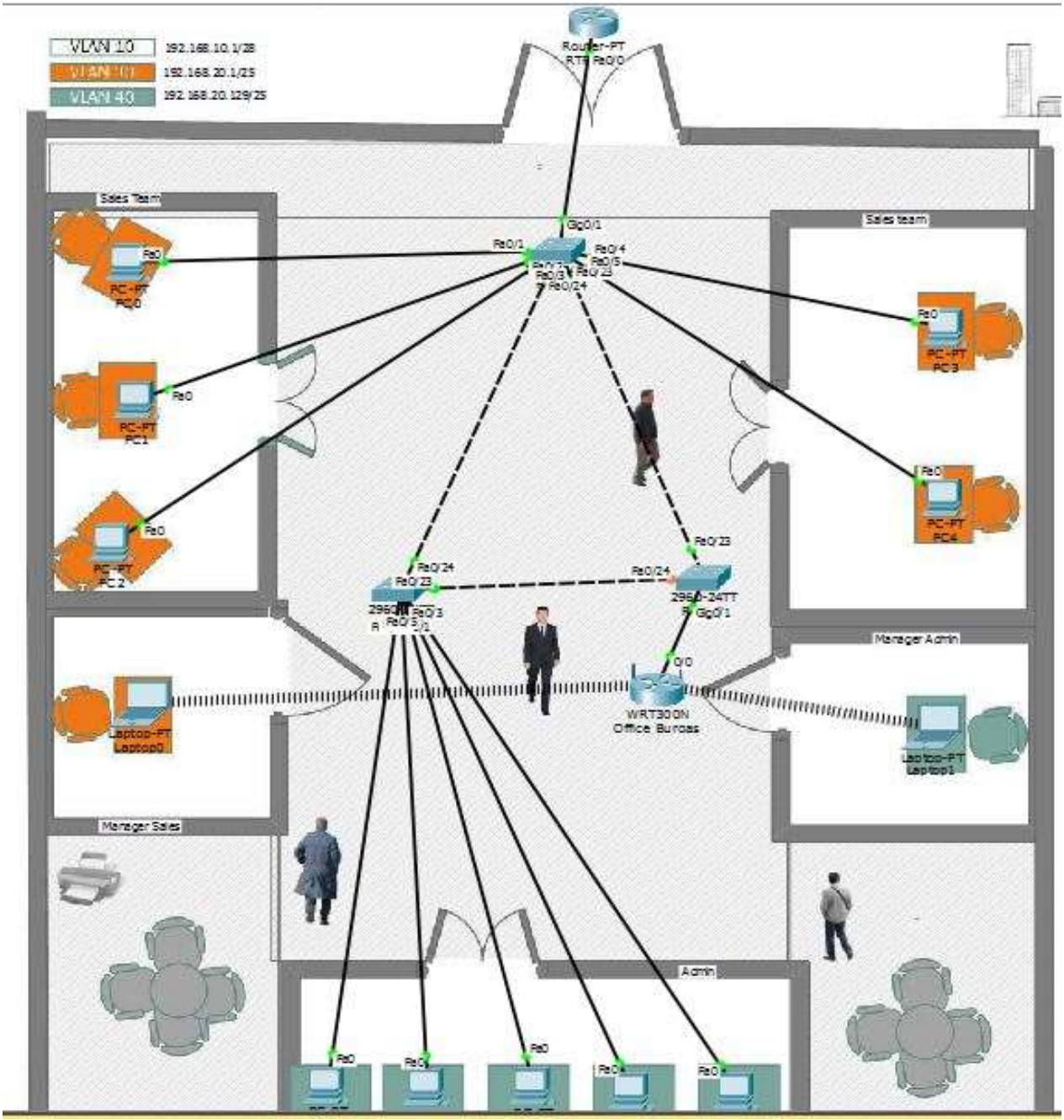
Отиваме в менюто Wireless Където в полето Network Name (SSID) трябва да изберем как ще се казва нашата мрежа, за офиса ни в Бургас избрахме името **BurgasBranch**. Останалите опции ги оставяме същите както са зададени по подразбиране фиг.26.

Фигура 26 - Задаване име на безжична мрежа

За да зададем парола с която да защитим нашия рутер, на фигура 27, избираме от опциите в менюто Security Mode: WPA2 Personal, като най сигурен режим за защита и в полето **Passphrase** пишем желата от нас парола, а в случая аз съм задал burgas@123

Фигура 27 - Задаване паролана безжичен рутер

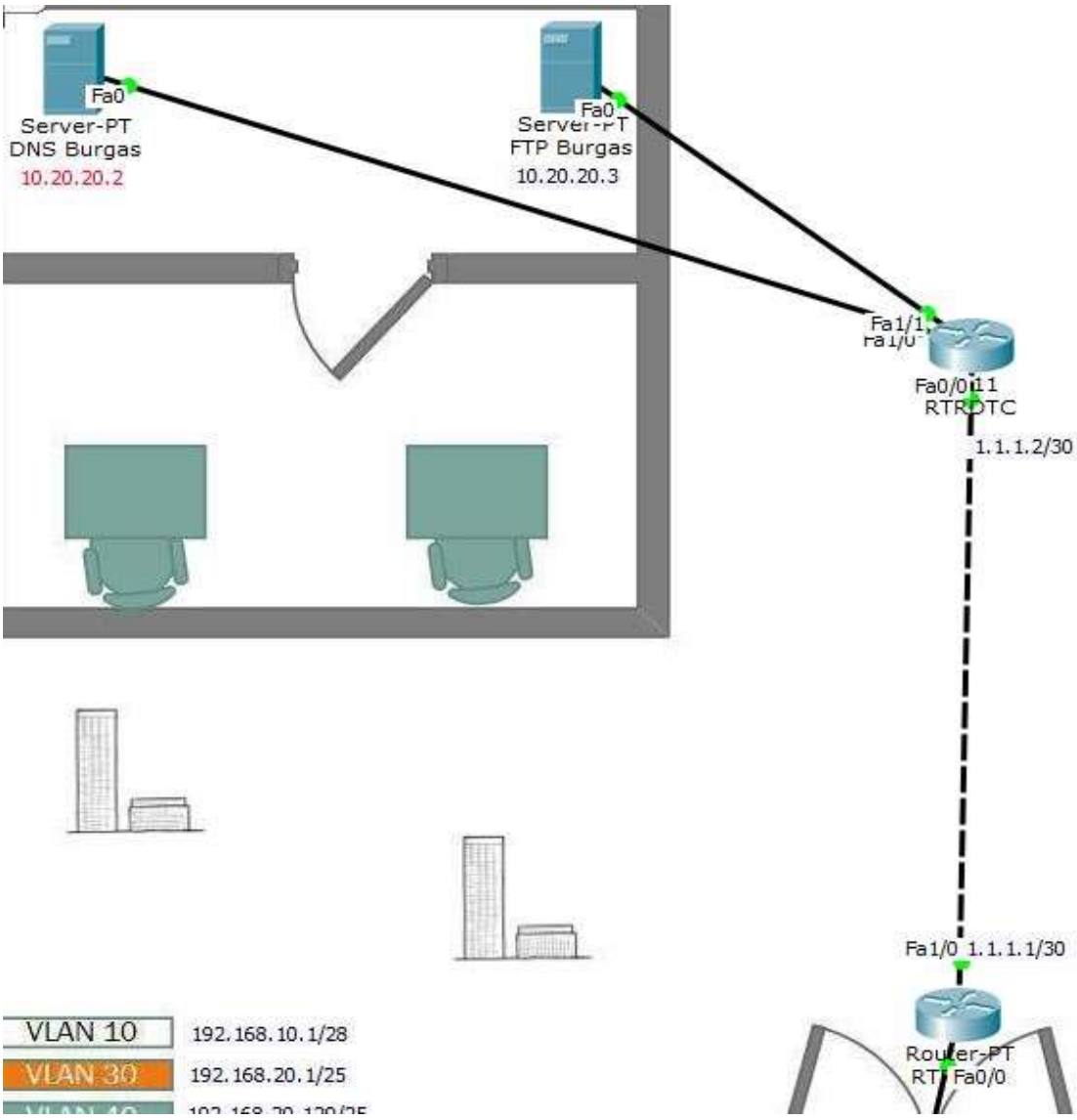
Като сме готови с конфигурацията на всички суичове и безжични устройства и свързването им с всеки компютър, вече може да продължим към свързването на главния комутатор (RootA) с рутера (RTRBGS) в офиса. На Фигура 28, може да видите как би трябвало да изглежда офиса ни в Бургас.



Фигура 28 - Готова инфраструктура офис Бургас

След като сме готови с изграждането инфраструктурата в офиса, следва да свържем маршрутизатора в офиса с маршрутизатора Дейта център Бургас. Следващата стъпка е да се конфигурира статично рутиране между тях и по този начин компютрите в офиса ще имат връзка с DNS и FTP сървъри.

На фигура 29 се представя свързването между двата маршрутизатора RTRBGS и RTRDTC, заедно със зададените IP адреси на всеки интерфейс.



Фигура 29 - Свързване Офис Бургас – Дейта Център

Първоначално зададохме IP адрес на RTRBGS интерфейс Fa1/0 – 1.1.1.1 с маска 255.255.255.252. Тази маска позволява в мрежата да има само 2 устройства. След това свързваме с кръстосан кабел към интерфейс Fa0/0 на рутер RTRDTC и задаваме IP адрес 1.1.1.2 със същата маска. Този процес се изпълнява с долупосочените команди.

```
RTRBGS(config)#interface FastEthernet1/0
RTRBGS(config-if)#ip address 1.1.1.1 255.255.255.252
RTRBGS(config-if)#no shutdown
```

```
RTRDTC(config)#interface FastEthernet0/0
RTRDTC(config-if)#ip address 1.1.1.2 255.255.255.252
RTRDTC(config-if)#no shutdown
```

Добавяме към RTRDTC модул с 16 порта, които ще ползваме за да свържем сървърите ни.

С командния ред по долу, ще създадем VLAN, и ще конфигурираме част от портовете в него. Към тях ще свържем DNS и FTP сървърите и ще активираме STP portfast.

```
RTRDTC(config)#int vlan 18
RTRDTC(config-if)#ip address 10.20.20.1 255.255.255.0
RTRDTC(config)#int range fa1/0-15
RTRDTC(config-if-range)#switchport access vlan 18
% Access VLAN does not exist. Creating vlan 18
RTRDTC(config-if-range)#spanning-tree portfast
RTRDTC(config-if-range)#no shutdown
```

Процеса на конфигурация между офиса и Дейта Центъра завършва със статично рутиране между RTRBGS и RTRDTC. Чрез по – долу описаните записи ние задаваме на маршрутизатора в Бургас, Default route, или всички мрежи, които не са зададени в IP таблицата да бъдат пренасочени към RTRDTC и това минава през интерфейса на Fa0/0 (1.1.1.2) на маршрутизатора RTRDTC. За да имаме обратна връзка, трябва да направим същото само, че от RTRDTC до RTRBGS, но със специфични мрежи.

```
RTRBGS(config)#ip route 0.0.0.0  0.0.0.0 1.1.1.2
RTRDTC(config)#ip route 192.168.10.0 255.255.255.240
1.1.1.1
RTRDTC(config)#ip route 192.168.20.0 255.255.255.128
1.1.1.1
RTRDTC(config)#ip route 192.168.20.129 255.255.255.128
1.1.1.1
RTRDTC(config)#ip route 192.168.20.128 255.255.255.128
1.1.1.1
```

Когато завършим процеса на статично рутиране може да направим тест с един произволно избран комютър и да проверим дали има връзка до DNS и FTP сървъра и от къде минава тя.

```
PC>tracert 10.20.20.2

Tracing route to 10.20.20.2 over a maximum of 30 hops:

1 1 ms 0 ms 9 ms 192.168.20.1
2 0 ms 0 ms 0 ms 1.1.1.2
3 0 ms 0 ms 0 ms 10.20.20.2

Trace complete.
```

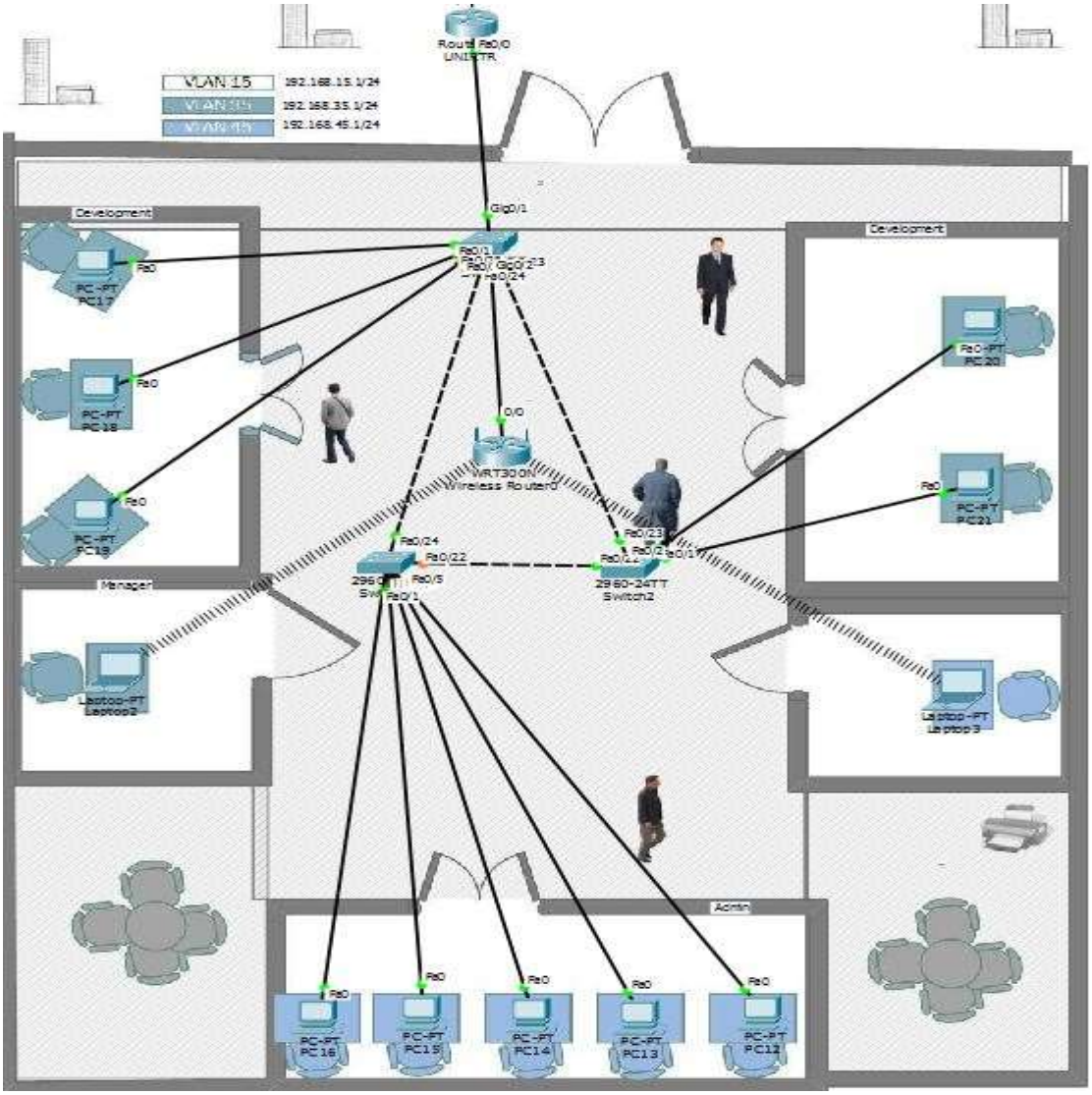
3.5 Конфигурация на устройства в Офис Унибит.

Инфраструктурата на офис Унибит е почти индентична с тази на офис Бургас. В таблица 3 са описани VLAN-ите, които са зададени в маршрутизатора и

комутаторите както и обесега от IP адреси, които може да бъде използван във всеки VLAN.

VLAN Име	VLAN ID	Network	Subnet Mask	Default Gateway	IP DHCP Scope
Admin	15	192.168.15.0	255.255.255.0	192.168.15.1	192.168.15.2-254
Development	35	192.168.35.0	255.255.255.0	192.168.35.1	192.168.35.2-254
Management	45	192.168.45.0	255.255.255.0	192.168.45.1	192.168.45.2-254

Таблица 3 - VLAN детайли офис УниБит



Фигура 30 - Инфраструктура офис Унибит

Най съществената разлика между двата клона е свързаността между офис маршрутизатора и маршрутизатора в Дейта Центъра. Те са свързани посредством RIP протокол версия 2.

Чрез командите по долу, ние посочваме на рутера(UNIRTR) и на (UNIDTC) подмрежите, към които е свързани. И отново задаваме Default Route на UNIRTR, за да може всичко непознати дестинации да бъдат пренасочени към маршрутизатор UNIDTC.

```
UNIRTR(config)#router rip
UNIRTR(config-router)#version 2
UNIRTR(config-router)#network 2.0.0.0
UNIRTR(config-router)#network 192.168.15.0
UNIRTR(config-router)#network 192.168.35.0
UNIRTR(config-router)#network 192.168.45.0
UNIRTR(config)#ip route 0.0.0.0 0.0.0.0 FastEthernet1/0

UNIDTC(config)#router rip
UNIDTC(config)#version 2
UNIDTC(config)#network 2.0.0.0
UNIDTC(config)#network 10.0.0.0
```

След като сме конфигурирали маршрутизаторите, може да направим тест чрез командата **ping** през произволен компютър от офис мрежата. Командата Ping работи на принципа на ехото, като изпраща съобщение чрез ICMP протокола до отдалечен компютър. Съобщението съдържа „искане“ за отговор от хоста. В този процес се измерва времето от предаване на съобщението до времето на получаването му от първоначалния компютър (двупосочния път) и се записва

всяка загуба на пакети. Резултатите от теста се отпечатват на екрана под формата на статистически съобщения.

```
PC>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 10.10.10.10: bytes=32 time=1ms TTL=126
Reply from 10.10.10.10: bytes=32 time=0ms TTL=126
Reply from 10.10.10.10: bytes=32 time=0ms TTL=126
Reply from 10.10.10.10: bytes=32 time=0ms TTL=126

Ping statistics for 10.10.10.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Когато сме готови с конфигуриране на устройствата в двата клона, следва да използваме трети протокол, който ще ни помогне да направим свързаността между офиса ни Бургас и офиса на Унибит. Протокола, който избрах да ползваме е EIGRP (Enhanced Interior Gateway Routing Protocol).

След като сме избрали протокол, чрез който офисите ни ще комуникират сега трябва да направим връзка между рутерите в Дейта Центровете ни RTRDTC и UNIDTC, това ще стане чрез кроснат кабел, между интерфейс fa6/0 на UNIDTC и интерфейс fa0/1 на RTRDTC. Маршрутизаторите ще бъдат в мрежа 5.5.5.0 с маска 255.255.255.0 като fa1/0 ще бъде с адрес 5.5.5.1, а fa6/0 ще ползва 5.5.5.2. Нека сега да конфигурираме EIGRP протокола между двете устройства с командата описана по – долу или в ***Приложение 2***. Конфигурация на Свързаност между Офис Бургас и Офис Унибит

```
RTRDTC(config)#router eigrp 1
RTRDTC(config-router)#network 5.5.5.0 0.0.0.255


UNIRTR(config)#router eigrp 1
UNIRTR(config-router)# network 5.5.5.0 0.0.0.255
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 5.5.5.1 (FastEthernet0/0) is up: new
adjacency
```

Сега след като конфирурирахме протоколите, двата рутера се „разпознаха“ и могат да обменят рутинг информация. За да успеем обаче да накараме офис Бургас, който е вързан със статично рутиране към своя дейта център да вижда офис Унибит, който е свързан чрез RIP Version 2 протокол към своя Дейта център ние трябва да използваме командата **redistribute**. Тя успява да покаже на своите EIGRP „съседи“ какви други протоколи са използвани в другите мрежи свързани към рутера и даде достъп до тях.

```
RTRDTC(config)#router eigrp 1
RTRDTC(config-router)#redistribute static – с тази команда казваме на рутера да
преразпредели статичните рутове към ЕИГРП процеса.
RTRDTC(config-router)#redistribute connected – преразпределя всички директно
свързани мрежи

UNIRTR(config)#router eigrp 1
UNIRTR(config-router)#redistribute rip metric 1500 0 255 1 1500
```

Метриките от преразпределянето на RIP Протокола означават:

Трафик: 1500

Забавяне: 0

Надеждност: 255

Натоварване: 1

Максимален размер на пакет: 1500

След като сме приключили с тази конфигурация може да направим тест дали имаме връзка от произволно избран компютър в офис Бургас до DNS сървъра, който се намира в Дейта Центъра на офис Унибит.

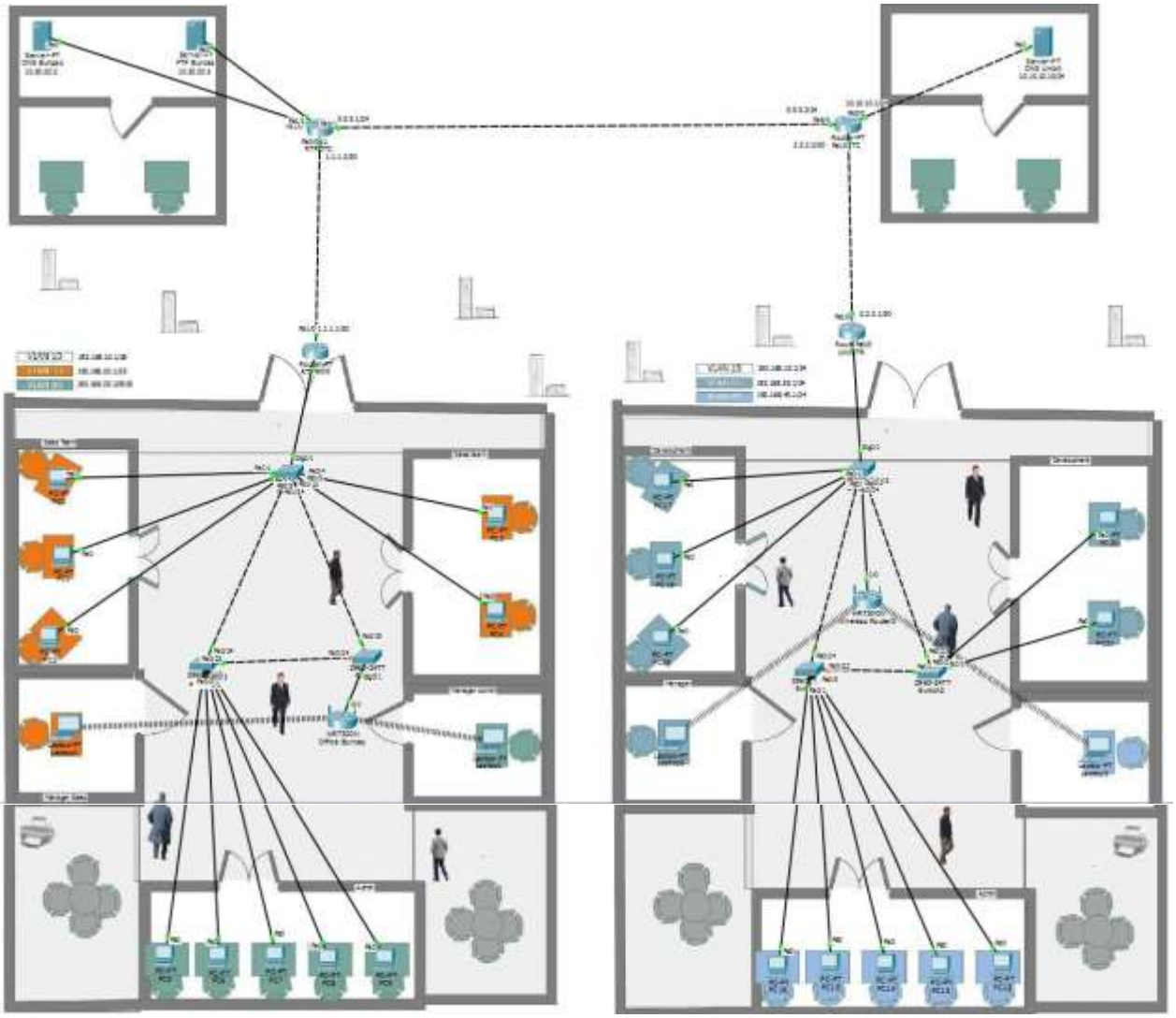
```
PC>tracert 10.10.10.10

Tracing route to 10.10.10.10 over a maximum of 30 hops:

1 0 ms 0 ms 0 ms 192.168.20.1
2 0 ms 9 ms 0 ms 1.1.1.2
3 0 ms 0 ms 0 ms 5.5.5.2
4 0 ms 0 ms 0 ms 10.10.10.10

Trace complete.
```

В резултата от командата **tracert** виждаме всички места от където минава рутирането за да може да стигне до адрес 10.10.10.10 . На фигура 31, може да видим готовия проект за изграждане и свързване на 2 офиса.



Фигура 31 - Свързаност между Офис Бургас и Офис Унибит

Заключение

В настоящата дипломна работа представихме накратко основите на компютърните мрежи, хардуера, който ни е нужен за да бъде изградена качествено една мрежа както и конфигурирането му. Избрахме да работим с мрежови устройства от фирмата Cisco, защото те са едни от най добрите на пазара за мрежово оборудване.Запознахме се с приложението Cisco Packet Tracer, което е много полезно при тестване симулиране и анализиране на мрежи и грешки при изграждането им. Показахме в Глава 3 как чрез команден ред, може да се настроят Cisco мрежови устройства, и накрая чрез команден ред успяхме да тестваме дали нашата мрежа е изградена успешно. В Процес на писането на дипломната работа се сблъскахме с различни видове рутиране, статично, чрез RIP Version 2 и EIGRP Протоколи. Изграждайки връзката между двата офиса с техните дейта центрове показахме в глава 3.5 как базирана на различни видове рутиране, успяхме да осъществим свързаността между тях, без това да бъде пречка. Чрез Packet Tracer може да симулираме мрежа на малка и средна компания както и на голямо предприятие и след това да използваме тази симулация за да реализираме проекта си. Единственият недостатък на софтуера, е че е тясно свързан само със Cisco мрежови устройства. Използването на различни протоколи в нашата симулация ни показва, че може да осъвместяваме устройства от всеки клас. Основните цели, които си бяхме поставили бяха изпълнени, като изградихме мрежа в два офиса, разделихме я на VLAN-и, свързахме по два рутера с различен вид рутиране и накрая успяхме чрез трети протокол, да свържем двата офиса успешно за да могат да имат връзка по между си компютрите и мрежовите устройства.

Дипломната работа в този вид, с леки допълнения може да се използва за осъществяването на реален проект.

Използвана литература

1. Макмилън, Трой. Cisco: Компютърни мрежи - основи. Портове и Номерация Трой Макмилън; Прев. от англ. Георги Далаков. -Ново изд.- София: ИК АлексСофт,2016.35с.
2. Генков, Делян. Основи на компютърните мрежи. Въведение в мрежите

Делян Генков: Първо изд. - Габрово: Юни, 2014. 8с.

3. Шиндър, Дебра, Литълджон.Компютърни мрежи – пълно ръководство по теория, за изграждане и съвместна работа между мрежите. Категоризиране на мрежите. – София: ИК Софтпрес, 2003. 59с.
4. CCNP Routing and Switching SWITCH 300-115 - David Hucaby, CCIE No. 4594. Configuring DHCP. Chapter 12. Ciscopress, 2015. 289c.
5. RIP, 20 Feb 2016. https://bg.wikipedia.org/wiki/RIP
6. Маршрутизиращи протоколи, EIGRP, 20 Септ. 2014. https://bg.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B8%D1%80%D0%B0%D1%89%D0%B8_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D0%B8
7. Cisco IOS, 27 June, 2014, https://en.wikipedia.org/wiki/Cisco_IOS
8. http://www.ciscopress.com/
9. http://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8606-redist.html#rip
10. http://www.cisco.com/
11. https://en.wikipedia.org/wiki/Cisco_Systems
12. https://en.wikipedia.org/wiki/Category:Cisco_protocols
13. https://en.wikipedia.org/wiki/IP_address
14. https://en.wikiversity.org/wiki/Network_Classifications
15. http://www.networkel.com/2015/11/what-is-eigrp-and-how-it-works.html

Списък на фигурите и таблиците

Приложение 1. *Конфигурация Офис Бургас:*

```
Router>en
Router#configure terminal
Router(config)#hostname RTRBGS
RTRBGS(config)#wr


RTRBGS(config)#int fa0/0.10
RTRBGS(config-subif)#encapsulation dot1q 10
RTRBGS(config-subif)#ip address 192.168.10.1 255.255.255.240

RTRBGS(config)#int fa0/0
RTRBGS(config-if)#no shutdown

RTRBGS(config)#ip dhcp pool 10
RTRBGS(dhcp-config)#network 192.168.10.0 255.255.255.240
RTRBGS(dhcp-config)#default-router 192.168.10.1
RTRBGS(dhcp-config)#dns-server 10.20.20.2

RTRBGS(config)#ip dhcp excluded-address 192.168.10.1
RTRBGS(config)#ip dhcp excluded-address 192.168.20.1
RTRBGS(config)#ip dhcp excluded-address 192.168.20.129

RootA(config)#int range fa0/1-20
RootA(config-if-range)#spanning-tree portfast

RootA(config)#vlan 10
```

```
RootA(config-vlan)#name Admin
RootA(config-vlan)#exit
RootA(config)#vlan 30
RootA(config-vlan)#name Sales
RootA(config-vlan)#exit
RootA(config)#vlan 40
RootA(config-vlan)#name Management

RootA(config)#interface range fa0/23-24
RootA(config-if-range)#switchport mode trunk

RTRBGS(config)#interface FastEthernet1/0
RTRBGS(config-if)#ip address 1.1.1.1 255.255.255.252
RTRBGS(config-if)#no shutdown

RTRDTC(config)#interface FastEthernet0/0
RTRDTC(config-if)#ip address 1.1.1.2 255.255.255.252
RTRDTC(config-if)#no shutdown

RTRDTC(config)#int vlan 18
RTRDTC(config-if)#ip address 10.20.20.1 255.255.255.0
RTRDTC(config)#int range fa1/0-15
RTRDTC(config-if-range)#switchport access vlan 18
% Access VLAN does not exist. Creating vlan 18
RTRDTC(config-if-range)#spanning-tree portfast
RTRDTC(config-if-range)#no shutdown

RTRBGS(config)#ip route 0.0.0.0  0.0.0.0 1.1.1.2
```

RTRDTC(config)#ip route 192.168.10.0 255.255.255.240 1.1.1.1

RTRDTC(config)#ip route 192.168.20.0 255.255.255.128 1.1.1.1

RTRDTC(config)#ip route 192.168.20.129 255.255.255.128 1.1.1.1

RTRDTC(config)#ip route 192.168.20.128 255.255.255.128 1.1.1.1

Приложение 2. *Конфигурация на Свързаност между Офис Бургас и Офис Унибит*

RTRDTC(config)#router eigrp 1

RTRDTC(config-router)#network 5.5.5.0 0.0.0.255

UNIRTR(config)#router eigrp 1

UNIRTR(config-router)# network 5.5.5.0 0.0.0.255

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 5.5.5.1 (FastEthernet0/0) is up: new adjacency

RTRDTC(config)#router eigrp 1

RTRDTC(config-router)#redistribute static

RTRDTC(config-router)#redistribute connected

UNIRTR(config)#router eigrp 1

UNIRTR(config-router)#redistribute rip metric 1500 0 255 1 1500