УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

КАТЕДРА „ИНФОРМАЦИОННИ СИСТЕМИ И ТЕХНОЛОГИИ“
МАГИСТЪРСКА ПРОГРАМА
„ИНФОРМАЦИОННИ ТЕХНОЛОГИИ“

МАГИСТЪРСКА ТЕЗА

на тема:

МЕХАНИЗМИ ЗА РАЗПРЕДЕЛЯНЕ НА ТРАФИКА МЕЖДУ ДВА ИНТЕРНЕТ ДОСТАВЧИКА

Дипломант:
Кирил Митов
дистанционно обучение
Ф.№0095-имд

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

София

2015

УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

ДЕКЛАРАЦИЯ

От Кирил Пенчев Митов

Декларирам, че представената дипломна работа/магистърска теза е подготвена и изпълнена самостоятелно от мен.

При откриване на плагиатство поемам съответната отговорност по смисъла на чл.31 (1-3) от Наредбата.

Дата:…… **Подпис:**……..

(дипломант)

УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

ДЕКЛАРАЦИЯ

От Кирил Пенчев Митов

С настоящата отстъпвам □ / не отстъпвам □ безвъзмездно право на УНИБИТ да публикува представената моя авторска разработка (курсова работа, дипломна работа, магистърска теза) като общодостъпен ресурс за безплатен публичен достъп чрез информационните системи на УНИБИТ.

Дата:..... **Подпис**.....

(дипломант)

Съгласен съм авторската разработка (курсова работа, дипломна работа, магистърска теза) да бъде публикувана като общодостъпен ресурс за безплатен публичен достъп чрез информационните системи на УНИБИТ.

Дата:..... **Научен ръководител:**гл.ас.д-р Добри Бояджиев

……

(подпис)

Кирил Митов, Механизми за разпределяне на трафика между два интернет доставчика. Научен ръководител гл.ас.д-р Добри Бояджиев. 2015. Катедра „Информационни системи и технологии“. Магистърска програма „Информационни технологии“.УНИБИТ. 85 с. Брой източници - 18. Брой на приложения – 4. Брой фигури – 40. Брой таблици – 5.

Цел на магистърската теза е да се опишат и анализират някои механизми за разпределяне на мрежовия трафик и отказ от услуга между два интернет доставчика.

От така поставената цел произтичат следните **задачи:**

- Да се разгледат основите на мрежовата комуникация и нейните принципи;
- Да се анализират методите и средствата, посредством които мрежовият трафик може да бъде разделян, да се дефинира ясно проблема и да се предложат възможни решения;
- Да се изгради работна установка, чрез която да се покаже практическо конфигуриране на хардуерни и софтуерни решения за разпределяне на интернет трафика и отказ от услуга;
- Да се проектира и конфигурира компютърна мрежа, чрез софтуер за мрежова симулация GNS3 и да се демонстрира вариант на разпределяне на интернет трафика и отказ от услуга.

За решаване на поставените задачи са използвани следните **методи:**

- теоретични методи – изучаване и анализ на научно-техническа литература и нормативни документи; класификация, аналогия, системен анализ, обобщение, сравнение, моделиране, обектно-ориентиран анализ;

емпирични методи – наблюдение, диагностиране, експеримент, анализ на резултатите от експеримента.

В първа глава са разгледани някои от основните понятия за осъществяване на мрежова комуникация. Изяснена е сложността на предаването и получаването на информация посредством компютърни мрежи.

Показани са теоретичните модели, описващи принципния начин на комуникация и строежа на компютърните мрежи. Обяснени са основните мрежови протоколи и принципите при установяване на комуникационна сесия.

Втората глава разглежда методи, алгоритми, протоколи и средства за разпределяне на интернет трафика между няколко доставчика.

В трета глава са показани няколко практически решения на проблема. Обяснено е конфигуриране на маршрутизатор Микротик, защитна стена pfsence и хардуерно устройство, предназначено за разпределяне на трафика между два WAN порта – ZyXELL. Чрез използването на софтуер за симулиране на мрежови трафик GNS3 е конфигуриран протокол Сиско GLBP (Gateway Loadbalancing Protocol) и е направена демонстрация на работата му по разпределяне на трафика между два интернет доставчика, и при отказ от услуга на един от тях.

Ключови думи: Интернет, компютърни мрежи, разпределяне на трафика, мрежови протоколи, маршрутизиране

СЪДЪРЖАНИЕ

УВОД

В съвременния свят човек все повече свиква с ползването на безграничното море от информация наречено интернет. Ежедневно почти всеки човек ползва интернет пространството за информация, онлайн покупки, сделки, комуникация, забавление и др. Представете си колко неприятно би било за човек, свикнал с постоянния си достъп до интернет, същият да бъде много бавен или спрян, поради технически проблем или натовареност на мрежата. Докато частният потребител може да си позволи такава неприятност, то за бизнеса това може да бъде нещо фатално, водещо до големи загуби на средства, а дори и до фалит. Нито един голям и уважаващ себе си бизнес ръководител, ползващ интернет пространството за увеличаване печалбите на фирмата, не би си позволил неговата услуга да остане недостъпна или служителите му да имат ограничен /намален/ достъп до световната мрежа.

За осигуряване на безотказност се прибягва до използването на два и повече интернет доставчика. В случай че единият откаже, интернет трафикът преминава през другия. При наличие на две и повече връзки към интернет пространството идва въпросът за ефективното им използване, така че мрежовият трафик да бъде разпределен между тях и капацитетът им да бъде оползотворен.

Разпределянето на мрежовия трафик не става автоматично. Потока на информацията в компютърните мрежи следва сложни правила, които определят правилното им трансфериране. Тези правила се базират на система от стандарти за обмяната на информация между процеси или компютри, които са свързани в една компютърна мрежа, и то по начин, гарантиращ успешната връзка между две и повече крайни устройства. Комуникацията в тази мрежа се базира на множество протоколи с различни функции и се осъществява посредством обмяната на съобщения (пакети). Описаните в протокола правила дефинират каква информация се предоставя в пакетите и в какъв формат, за да се приеме от комуникационните партньори.

Цел на магистърската теза е да се опишат и анализират някои механизми за разпределяне на мрежовия трафик и отказ от услуга между два интернет доставчика.

От така поставената цел произтичат следните **задачи:**

- Да се разгледат основите на мрежовата комуникация и нейните принципи;
- Да се анализират методите и средствата, посредством които мрежовият трафик може да бъде разделян, да се дефинира ясно проблема и да се предложат възможни решения;
- Да се изгради работна установка, чрез която да се покаже практическо конфигуриране на хардуерни и софтуерни решения за разпределяне на интернет трафика и отказ от услуга;
- Да се проектира и конфигурира компютърна мрежа, чрез софтуер за мрежова симулация GNS3 и да се демонстрира вариант на разпределяне на интернет трафика и отказ от услуга.

За решаване на поставените задачи са използвани следните **методи:**

- теоретични методи – изучаване и анализ на научно-техническа литература и нормативни документи; класификация, аналогия, системен анализ, обобщение, сравнение, моделиране, обектно-ориентиран анализ;
- емпирични методи – наблюдение, диагностиране, експеримент, анализ на резултатите от експеримента.

ГЛАВА I. КОНЦЕПЦИЯ НА МРЕЖОВИЯ ТРАФИК НА ДАННИ

1.1. Представяне на информацията в компютрите

Информацията в компютрите се представя и обработва в двоичен код. Компютрите работят в двоична бройна система, при която цифрите са две – нула и единица. Всички команди и данни се записват като комбинации от единици и нули. Двоичното представяне е удобно и за комуникацията между компютрите.

Компютрите са електронни машини и те работят с електрически импулси. Компютрите използват цифрови сигнали. Наличието на сигнал се кодира като 1, а липсата на сигнал – като 0.

1.2. Използване на пакети[1]

При комуникацията между компютрите се обменят данни, които в много от случаите могат да бъдат големи по обем. Изпращането на един текстов файл например, като непрекъснат поток ще доведе до излишно натоварване на мрежата. През това време останалите компютри трябва да изчакат файловия трансфер да приключи. За да не се получава това, големите файлове трябва да бъдат разделени на по-малки части, преди да бъдат изпратени по мрежата.

Малките парчета, на които се разделят компютърните данни за предаване по мрежата се наричат пакети.

Разделянето на данните на пакети има следните предимства:

- По време на придвижването си по мрежата отделните пакети могат да преминат по различен маршрут. По този начин, ако един път се препълни или забави, останалата част от пакетите могат да минат и по друг маршрут.

[1] Йорданова,Н Електронен курс „Компютърни мрежи“ <http://193.192.57.240/po/courses/problemni/komputarni%20mrezi/pdf/10.pdf>

- Ако мрежовата връзка се прекъсне по време на изпращането на даден файл или някой от пакетите се загуби, то ще трябва да се изпратят само липсващите пакети, а не целият файл.

Ако при изпращането на файлове, данните се разделят на отделни парчета, то при получаването им от съответния компютър, до който са адресирани, те трябва да бъдат подредени и сглобени, така че да се получи файл, който е абсолютно еднакъв с изпратения. За да се случи това, към отделните парчета с данни се прибавя служебна информация.

Към началото на пакета, преди оригиналните данни, се добавя информация под формата на хедъри. Хедърите съдържат адресна информация, с помощта на която всеки пакет достига до местоназначението си. Те съдържат и информация за последователността на пакетите, така че всеки пакет да може да бъде подреден правилно, преди да се сглоби целия файл.

Към края на пакета, след оригиналните данни, се добавя завършваща информация или трейлър (trailer information). Често тя включва информация за проверка на грешки (CRC-Critical Redundancy Check). Проверката за грешки включва изчисления, които се извършват с пакета преди той да бъде изпратен по мрежата. След получаването се извършват отново същите изчисления. Ако резултатите от двете изчисления съвпаднат, тогава няма грешка при пренасянето на данните. В противен случай има грешка и се налага съответния пакет да бъде изпратен отново.

Големината на един пакет може да бъде различна. В TCP/IP мрежите пакетите могат да съдържат до 1500 байта данни, като при това общата дължина на пакета е 1518 байта. В Интернет може да има устройства, които работят с по-малки дължини на пакета. Например, в протокола PPPoE максималната дължина на пакета е 1492 байта. Затова е въведена единица MTU (Maximum Transmission Unit). Това е максималната дължина на данните, които могат да се пренесат през комуникационно съединение или устройство без разделяне.

1.3. Мрежови модели[2]

Процесът на мрежовата комуникация е сложен. Информацията, която искаме да предадем по мрежата до друг компютър, преди да постъпи в преносната среда се преобразува до поредица от електрически импулси, светлинни импулси или радиосигнал. При достигане на компютъра получател се извършва обратното преобразование. Този процес се извършва на няколко етапа. Разработчиците на хардуер и софтуер са стигнали до извода, че най-ефикасният начин за мрежова комуникация е многослойния модел. Отделните етапи от комуникацията се обозначават като слоеве. Всеки слой извършва конкретна задача. Така сложният процес на комуникация се свежда до поредица от елементарни действия. Например, при изпращане на данните по мрежата елементарните действия се свеждат до: взаимодействие с потребителската програма, компресиране на данните, изграждане на пакети, проверка за правилно адресиране и т.н. Многослойният модел е по-добрият вариант и при диагностицирането и отстраняването на мрежови проблеми.

Взаимодействието между отделните слоеве на многослойния модел се осигурява от протоколите, като за всеки слой има различен протокол.

1.3.1. Моделът OSI

Мрежовият модел OSI (Open System Interconnect) е абстрактен модел, който описва начина на комуникация в компютърните мрежи. Разработен е от Международната организация по стандартизация (ISO). OSI моделът позволява на различни системи да комуникират безпроблемно помежду си. Той е стандарт, който производителите на мрежово оборудване използват при проектиране на хардуер, операционни системи и протоколи.

Моделът се използва, само когато се пакетират данни за предаване на данни по мрежата, и не се използва, когато се осъществява локален достъп до данните на собствената компютърна система.

---

[2] Йорданова,Н Електронен курс „Компютърни мрежи“ <http://193.192.57.240/po/courses/problemni/komputarni%20mrezi/pdf/11.pdf>

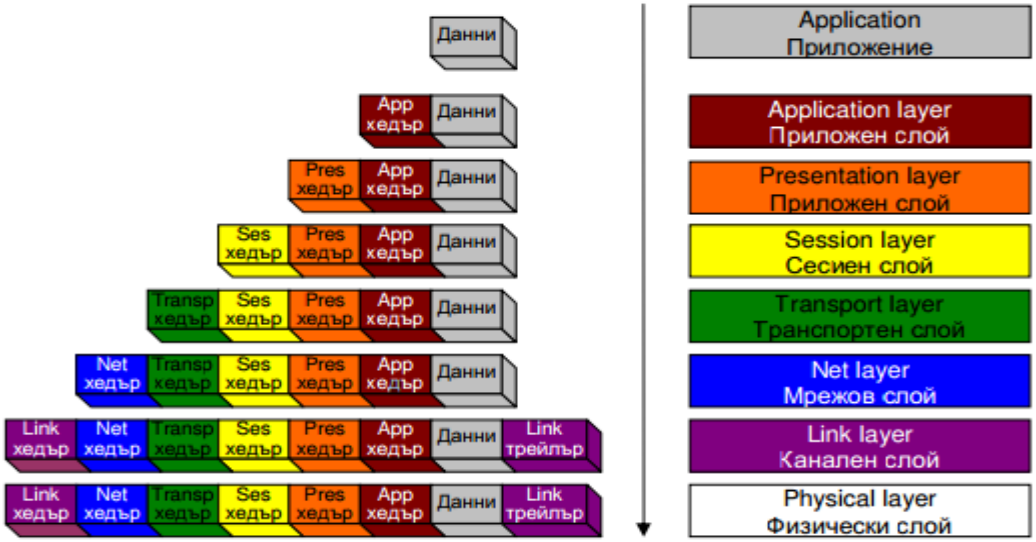
Структура на OSI модела

Той включва 7 слоя, всеки от които е една стъпка в процеса на комуникация (вж. таблица 1).

Application	Приложен слой	слой 7
Presentation	Представителен слой	слой 6
Session	Сесиен слой	слой 5
Transport	Транспортен слой	слой 4
Network	Мрежови слой	слой 3
DataLink	Канален слой	слой 2
Physical	Физически слой	слой 1

Таблица 1. Моделът OSI

Всеки слой има точно определени функции – предоставя интерфейс и услуги към горния си слой, като също така получава услуги от слоя под него. Преди да се изпратят данните по мрежата те преминават последователно през отделните слоеве, като всеки слой добавя своя собствена информация към оригиналната информация (вж. фигура 1). Информацията по мрежата се предава във вид на пакети. При достигане на получаващия компютър, пакетите преминават през отделните слоеве по възходящ ред като всеки слой отстранява допълнителната информация добавена от едноименния слой при изпращането й. По този начин след преминаване през всички слоеве информацията трябва да бъде сглобена, така че да се получи оригиналното съобщение.



Фигура 1. Път на данните в OSI модела

Приложен слой

Слой 7 или Приложен слой е най-горният слой в модела. Той служи като посредник между софтуерните приложения и мрежовите услуги. В този слой работят протоколите HTTP, FTP, Telnet, SMTP, POP3, IMAP4, SNMP. Задачата на слоя е да управлява общия мрежов достъп, контрола на потоците от данни и поправката на грешки.

Представителен слой

Слой 6 или Представителен слой определя използвания формат за обмен на данните. Тук получените от приложния слой данни се представят във вид на пакети („универсален" формат за пренос). При получателя става обратно преобразуване на данните от „универсален" във формат, използван от приложния слой на получаващия компютър. Този слой отговаря за преобразуването на данните:

- компресиране – намаляване на техния размер;
- криптиране – кодиране с цел защита от неоторизиран достъп;
- транслация на протоколи – с цел пренасяне между различни хардуерни платформи и операционни системи.

Тук работи софтуерът за споделяне на файлове и принтери – редиректор (redirector). Той определя дали заявка за вход/изход до файл се обработва от локалния компютър или от мрежово устройство чрез пренасочване на заявките.

Сесиен слой

Слой 5 или Сесиен слой отговаря за изграждане на канал за връзка – сесия – между два компютъра в мрежата. Подобно на телефонен разговор, в сесията програмите „разговарят" помежду си. Сесиите могат да бъдат в режим на пълен дуплекс (full duplex) или полу-дуплекс (half duplex). И двата режима позволяват двупосочна комуникация. В режим на пълен дуплекс двете страни могат да изпращат и получават данни едновременно, а при полу-дуплекс – последователно.

Протоколите от сесийния слой включват:

- Network Basic Input/Output System (NetBIOS) интерфейс – позволява компютрите от мрежата да осъществяват двупосочна връзка, обработка на големи съобщения, откриване на грешки и тяхното коригиране;
- Berkeley UNIX sockets (Sockets) интерфейс – базов приложен интерфейс (API) за използване на TCP/IP. Част от операционните системи UNIX/Linux, позволяват изграждането на TCP и UDP връзки.
- Windows Sockets (Winsock) – версията на Socket за Microsoft Windows. Освен базовите функции включва разширение, позволяващо по-строг контрол на връзките.

Транспортен слой

Слой 4 или Транспортен слой отговаря за транспортирането на пакетите с данни без грешки, в точна последователност и без загуби. Той може да оптимизира трафика чрез обединяване на непълни съседни пакети. При получаващия компютър транспортният слой разопакова пакетите и ги подрежда в първоначалния им вид, след което изпраща потвърждение за получаването им. Този слой осигурява контрол на потока и обработката на грешки при преноса на пакетите.

Транспортните протоколи TCP, UDP от TCP/IP и услугата за преобразуване на имена – Domain Name System (DNS) работят в този слой.

Мрежови слой

Слой 3 или Мрежов слой отговаря за адресирането на съобщенията и за определянето на маршрут, по който да преминат данните от компютъра – източник до компютъра – получател. Слоят следи и за проблеми при трафика. Също така управлява приоритета на данните – Quality of Service (QoS) – гарантиране на мрежов ресурс (пропускателна способност) за интерактивни приложения като аудио и видео разговори.

Протоколът IP от TCP/IP работи в този слой. Тук работят маршрутизаторите.

Канален слой

Слой 2 или Канален слой изпраща кадрите с данни от мрежовия слой към физическия слой. Той включва два подслоя:

- Контрол за достъп до преносната среда – Media Access Control;
- Контрол на логическите връзки – Logical Link Control (LLC);

MAC подслоят разпределя достъпа на компютрите до физическата преносна среда. Той дефинира MAC адресите.

В LLC подслоя се дефинира логическата топология. Тя може да не съвпада с физическата.

В каналния слой работят устройствата маршрутизатор и комутатор.

Данните пътуват по мрежата във вид на фреймове (frames). Всеки фрейм (кадър) се състои от няколко елемента:

- Идентификатор на получателя (Destination ID) – адресът на компютъра, към който се изпращат данните;
- Идентификатор на подателя (Sender ID) – адресът на компютъра, изпращащ данните;
- Контролна информация – определя типа на фрейма, маршрута и сегментирането;
- Пакет данни – същинската информация, предавана по мрежата;
- Циклична проверка на контролната сума (Cyclical Redundancy Checks – CRC) – информация за проверка и корекция на грешките.

След изпращането на всеки фрейм обратно се изпраща потвърждение за пристигането му. Фреймовете, за които не се получи потвърждение или са повредени, се изпращат повторно.

Физически слой

Слой 1 или Физически слой предава потока от битове (единици и нули) от мрежовата карта към преносната среда. Битовете са кодирани като електрически или светлинни импулси (при безжичните системи са електромагнитни вълни). Този слой определя типа на връзката между

мрежовата карта и кабела, както и техниката на предаване на информацията по мрежата. Устройствата, които работят на това ниво са мрежови карти, повторители, хъбове, медиа конвертори.

1.3.2. Моделът DoD TCP/IP

Моделът е създаден от Министерството на отбраната на САЩ – Department of Defense (DoD) – през 70-те години на миналия век (около 10 години преди OSI модела). Този модел е разработен съвместно с TCP/IP – част от проекта ARPAnet. Протоколите на TCP/IP са проектирани в този модел. Затова и този модел е известен с наименованието TCP/IP модел.

Състои се от четири слоя(вж. таблица 2):

Слой 4. Приложен (application layer) – най-горният слой от модела. Обхваща функциите на трите най-горни слоя на OSI модела;

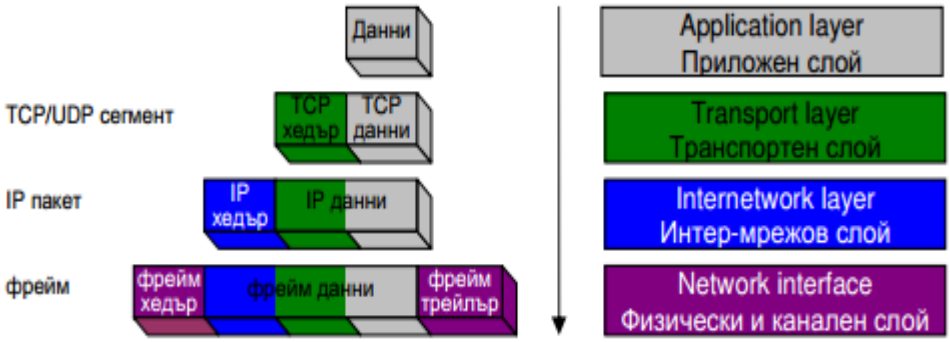
Слой 3. Транспортен (хост до хост) (host to host (transport) layer) – съответства на транспортния слой на OSI модела. Тук работят TCP, UDP, DNS;

Слой 2. Слой интер-мрежа (internetworking layer) – съответства на мрежовия слой на OSI. Занимава се с маршрутизацията основана на логическите IP адреси. Протоколът Address Resolution Protocol (ARP) преобразува логическите IP адреси в MAC адреси;

Слой 1. Мрежов интерфейс (network interface layer) – съответства на двата слоя – канален и физически на модела OSI. Тук работят Ethernet и Token Ring протоколите. В този слой се използват само MAC адреси.

DOD TPC/IP Model	OSI Model
Process/Application	Application
	Presentation
	Session
Host-to-host	Transport
Internet	Network
Network Access	Data link
	Physical

Таблица 2. Съответствие на слоевете на DOD TCP/IP и OSI моделите



Фигура 2. Път на данните в TCP/IP модела

На фиг.2 е представен пътят на данните в TCP/IP модела от гледна точка на компютъра, който изпраща информацията. При компютъра-получател информацията преминава в обратна посока през отделните слоеве, като всеки слой прочита и отстранява добавената информация от едноименния слой. При достигане на информацията в приложния слой трябва да се получи оригиналното съобщение.

1.4. Мрежови протоколи

Мрежовите протоколи са съвкупност от правила за комуникация между отделните устройства включени в компютърната мрежа. Чрез тях мрежови компоненти на различни производители могат успешно да обменят информация помежду си.

Мрежовите услуги предоставят възможност за управление на различни задачи – преобразуване на имена, автоматично назначаване на мрежови адреси на компютрите и др. Основната работа на протоколите е да подготвят първичните данни от изпращащия компютър за изпращане по мрежата, разделяйки ги на пакети и добавяйки адресна информация за всеки пакет и да ги подготвят за реално предаване през преносната система, а на приемащия компютър по обратен път да получат пакета, да отделят служебната информация, да обединят пакетите в първоначалния им вид и да подадат така получената първична информация на съответното приложение. По-долу са представени някои мрежови протоколи, създадени и използвани от различни фирми.

1.4.1. Протоколът NetBIOS

Протоколът NetBIOS (Network Basic Input/Output System) е създаден през 80-те години на миналия век от IBM. NetBIOS има два режима на комуникация – сесиен и дейтаграмен режим. В сесиен режим NetBIOS позволява да се осъществи връзка (сесия) с откриване на грешки и възстановяване. В дейтаграмен режим съобщенията се изпращат без установяване на връзка. Откриването на грешки и коригирането им е задача на приложението. NetBIOS осигурява услуга за именуване на хостовете. Адресацията става по име на компютър като компютрите са обединени в работни групи. Няколко години по-късно е създаден друг протокол на базата на NetBIOS, който работи в TCP/IP мрежи – NetBIOS Over TCP. Използва се за споделяне на файлове и принтери в TCP/IP мрежите.

1.4.2. Протоколът NetBEUI

Малки локални мрежи могат да се конфигурират чрез протокола NetBEUI (NetBIOS Extended User Interface). NetBEUI използва протоколите NetBIOS. Той се използва само в локални мрежи и не поддържа маршрутизиране. Единственото конфигуриране, което се изисква, е задаване на уникално име на всеки компютър в локалната мрежа. За по-лесно търсене, компютрите се обединяват в работни групи. Той е по-бърз от TCP/IP протокола.

1.4.3. Протоколът IPX/SPX

IPX/SPX (Internet Package Exchange/Sequenced Packet Exchange) е мрежовият протокол на фирмата Novell. Той е задължителен при NetWare мрежите. Може да работи и на мрежа на Microsoft. Фирмата е създала собствена реализация на IPX/SPX съвместими протоколи, която се нарича NWLink. Протоколът IPX/SPX изисква минимално конфигуриране (всяка мрежова интерфейсна карта има зададен MAC адрес) и предлага по-висока мрежова производителност в сравнение с TCP/IP мрежите. От съображения за сигурност много потребители използват IPX/SPX протоколите за споделяне на файлове и принтери в локални мрежи.

1.4.4. Протоколът Apple Talk

Apple Talk е съвкупност от протоколи на фирмата Apple за организиране на мрежи с компютри на Macintosh. Комплектът включва следните протоколи: LocalTalk – използва се при свързване на компютри на Macintosh в малки локални групи; EtherTalk – за свързване на Macintosh групи към Ethernet мрежи; TokenTalk – за свързване на Macintosh групи към Token Ring мрежи.

1.4.5. Протоколът TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) е семейство протоколи, което се използва в глобалната мрежа Интернет. На практика всички хардуерни платформи и операционни системи поддържат TCP/IP. Този модел се състои от много протоколи (Таблица 3), но тъй като ключова роля имат протоколите TCP и IP, името се определя от тях. Моделът TCP/IP е създаден през 1980 г. заради необходимостта от единен начин за комуникация между компютрите, като по този начин предоставя възможност мрежите да бъдат свързвани помежду си.

	OSI	**TCP/IP**	**протоколи**
7	Application	Application	HTTP, FTP
6	Presentation		ASCII, Unicode
5	Session		DNS, SSL
4	Transport	Transport	TCP, UDP, RTP, SCTP
3	Network	Network	IP, ICMP, IGMP
2	Data Link	Physical	Ethernet, Token ring
1	Physical		T1, E1

Таблица 3. Протоколи в TCP/IP

Канален слой

Каналният слой от TCP/IP модела е комбинация между каналния и физическия слой на OSI модела. Той описва по какъв начин пакетите с данни

(кадри) се предават по физическия слой, включвайки кодирането (т.е. специалните последователности от битове, които определят началото и края на кадъра). При Ethernet например, в полетата на хедъра на кадъра се съдържа информация относно това, за коя машина е предназначен този кадър.

Някои от протоколите на каналния слой са: MAC, ARP, NDP.

Media Access Control[3] (MAC) протоколът предоставя адресиране и механизми за контрол на достъпа до преносната среда, които позволяват няколко терминали или мрежови възли да комуникират в мрежа с множествен достъп, при която преносната среда е споделена (напр. Ethernet мрежа). MAC емулира логически комуникационен канал от типа "пълен дуплекс" в мрежа с много възли. Този канал може да свърже даден възел с един, няколко или всички останали възли от мрежата. Например, за еднозначното идентифициране на всеки от възлите в Ethernet мрежа се използват MAC адреси. MAC адресът е уникален идентификатор на мрежовия адаптер, зададен от производителя при производството му. Използва се при контрола на достъпа до общата преносна среда. MAC адресът се използва от комутаторите (суичовете) за определяне на пътя, по който да минават кадрите с информация, за да достигнат крайната точка.

Address Resolution Protocol[4] (ARP) е мрежови протокол за намиране на физическия адрес (MAC адрес) на дадено мрежово устройство по неговия адрес от мрежовия слой (IP адрес). Протоколът е дефиниран в RFC 826. ARP не е само за Internet Protocol (IP) и Ethernet, въпреки че се използва най-вече за тях поради преобладаващото най-широко разпространение на IPv4. Протоколът може да се използва за много други видове физически адреси и адреси на мрежови протоколи, например Token Ring, FDDI или IEEE 802.11, и IP over ATM.

Neighbor Discovery Protocol (NDP) предоставя функциите на ARP за IPv6.

---

[3] Уикипедия, Статия Media Access control < https://en.wikipedia.org/wiki/Media_access_control>

[4] Уикипедия, Статия Address Resolution Protocol <https://bg.wikipedia.org/wiki/Address_Resolution_Protocol>

Мрежови слой

Чрез мрежовия слой пакетът достига до желаното място. Основният протокол тук е IP.

IP (Internet Protocol) 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 придвижването си пакетите се насочват от маршрутизатори. Когато всички пакети пристигнат в компютъра-получател, служебната информация се отстранява и се получава оригиналното съобщение.

IP адресът е логически адрес, който се присвоява на всеки хост в мрежата. Един хост може да има няколко мрежови карти (няколко интерфейса). Всеки от тези интерфейси притежава собствен IP адрес. Хост, който има реален IP адрес, има достъп до всички услуги в Интернет, също така може да предлага услуги. Достъп до Интернет може да се извършва чрез посредник (програма proxy или NAT). Единствено посредникът има реален адрес, другите хостове имат частни IP адреси. В този случай потребителите могат да ползват, но не могат да предлагат интернет услуги. За разпределянето на адресите в глобалната мрежа Интернет отговаря американската организация IANA (Internet Assigned Numbers Authority). В рамките на една локална мрежа, IP адресите трябва да са уникални. Компютрите в локалните мрежи, непредставляващи част от Интернет, използват частни IP адреси.

Понастоящем се използват версиите IPv4 и IPv6. При IPv4 (ver.4) IP адресите са 32-битови цели числа. За удобство един такъв IP адрес се записва като 4 осем битови десетични числа разделени с точка. Основният недостатък на IPv4 е, че броят на адресите, които могат да се запишат с 32 бита е недостатъчен. За справяне с този проблем са създадени редица механизми

(например NAT), но те решават проблема само частично и временно. При IPv6 (ver.6) IP адресите са 128 битови числа. Тези IP адреси се представят като осем 16-битови цели числа, разделени с двоеточие. Допустимо е да се пропуснат нулите в старшите битове на всяко от числата. IPv6 може да се представи и по класическия начин, познат от IPv4.

Други протоколи, работещи на това ниво са: ICMP и IPsec.

ICMP (Internet Control Message Protocol) се използва от мрежовите устройства за изпращане на съобщения за грешка, показвайки недостъпност на Интернет услугата или че хостът в Интернет не може да бъде достигнат.

IPsec (Internet Protocol Security) е кодиращ протокол, гарантиращ автентичността и целокупността на обменената информация между две машини. IPsec е реализиран директно върху TCP/IP стека.

Транспортен слой

Транспортният слой отговаря за начина на транспортиране на информацията –обикновено тя трябва да бъде разделена на малки части, за да може да бъде пренесена по мрежата. Използваните протоколи от това ниво са: TCP, UDP, SCTP и др.

TCP (Transmission Control Protocol) е основния транспортен протокол, включен в пакета TCP/IP. Осигурява високо ниво на надеждност при предаване на данните. При него се гарантира, че всяко изпратено съобщение ще бъде получено. В TCP се следи за изгубени, повторно изпратени, не поредно получени и т.н. пакети. Затова и този протокол е по-бавен. Протоколът TCP е най-използваният от всички мрежови протоколи, доколкото той работи с логически IP адреси, като използва гъвкава схема за адресиране и позволява маршрутизиране на пакетите с информация. Почти всички операционни системи могат да го използват.

UDP (User Datagram Protocol) е другият транспортен протокол. Той е сравнително прост протокол – не се занимава с установяване на последователност на пакетите, с препредаването им при грешка. При него не се гарантира достигането на съобщението до получателя. В структурата на

пакетите, предавани чрез UDP се съдържа контролна сума. Чрез нея получателят на пакетите може да провери достоверността на информацията. Подходящ е за: кратки съобщения, които могат да се предадат в един пакет, за приложения работещи в реално време като VoIP (разговори по интернет), поточно аудио и видео.

SCTP[5] (Stream Control Transmission Protocol) предлага комбинация от качествата на предишните два протокола – ориентиран е към съобщенията като UDP и осигурява надеждност като TCP (RFC 4960). При липса на реализиран SCTP в операционната система е възможно тунелиране на SCTP посредством UDP, както и свързване на TCP API методите с SCTP методите.

Приложен слой

Приложният слой отговаря за предаването на данните, които са специфични за определен приложен софтуер. Работещи протоколи тук са: DNS, FTP, SSH, HTTP, SMTP, POP3, IMAP, TLS/SSL и др.

DNS (Domain Name System) [6]

DNS е набор от протоколи и услуги в TCP/IP мрежова среда, който позволява на потребителите на мрежата да използват йерархични приятелски имена, когато се обръщат към други хостове (компютри), вместо да е необходимо да помнят и да използват съответните IP адреси. DNS се използва в Интернет и много частни корпоративни мрежи. Главната функция на DNS е да съпоставя IP адреси към имена. Хостовете се обръщат един към друг с IP адреси, но хората оперират с имената им. При заявка от потребителя с приятелското име компютърът (заявител) изпраща това име на DNS сървъра, който връща заявката със съответстващия IP адрес, след което компютърът използва този IP адрес, за да се свърже с търсения хост.

DNS работи в приложния слой на OSI модела и използва UDP протокола за комуникация, а при непълна заявка използва TCP протокола.

---

[5] Уикипедия, Статия Stream Control Transmission Protocol <https://en.wikipedia.org/wiki/Stream_Control_Transmission_Protocol>

[6] Дудин,Ф. Уроци по комуникации <http://pchelp.cablebg.net/Tutorials/Communications/DNS.htm>

FTP (File Transfer Protoco)l[7]

File Transfer Protocol представлява мрежов протокол от тип клиент-сървър, предоставящ възможност за обмяна на файлове между машини, свързани в локална мрежа или в Интернет. Клиентът е специално разработена програма, чрез която се предоставя лесен начин за използване на възможностите за комуникация. Съществуват множество FTP-клиенти, както безплатни, така и платени. Протоколът предоставя възможността за изпълняване на операции на сървъра като показване на съдържанието на директории, смяна на директорията, създаване на директории и триене на файлове.

Свързването със сървъра може да бъде "нормално" или "анонимно". При нормалното свързване достъпът до сървъра се осигурява само при използването на потребителско име и парола на потребител с достатъчни права. Анонимно свързване се осъществява с потребителско име anonymous и каквато и да е парола и може да се използва за сървъри, които позволяват такъв достъп.

Модерните браузъри поддържат свързването с FTP-сървъри с цел изтегляне или показване на файлове в зависимост от вида на файла и възможностите на браузъра.

Протоколът работи в два режима – двоичен или текстов ASCII режим. Разработките на протокола включват различни варианти за криптирана комуникация и пренос на данните, наречени SFTP и FTPS.

SSH[8]

SSH (на английски: Secure SHell – Сигурна обвивка) е мрежов протокол, позволяващ криптирано предаване на данни. Разработен е от SSH Communications Security Ltd. Най-често се използва за изпълняване на команди на отдалечена машина, прехвърляне на файлове от една машина на друга и самото й менажиране. Предоставя високо ниво на автентификация и сигурност по време на комуникацията между машините през незащитена връзка.

[7] Postel,J Reynolds,J. Internet Standard <https://tools.ietf.org/html/rfc959>

[8] Уикипедия, Статия SSH <https://bg.wikipedia.org/wiki/SSH>

Проектиран е да замести подобни протоколи, като например TELNET, rsh и rexec на Бъркли, rlogin, rcp, rdist.

Всеки път, когато от компютър се изпращат данни към мрежата, SSH автоматично ги криптира. След получаването им от крайния потребител, SSH отново автоматично ги декриптира. Този процес се нарича прозрачно криптиране (на английски: transparent encryption). Така потребителите могат да работят нормално, без да подозират, че техните съобщения се криптират, така че да бъдат безопасно използвани в мрежата.

SSH използва клиент/сървър архитектура. На сървъра се инсталира SSH програма от системния администратор, която приема или отхвърля изпратените заявки от SSH клиент до самата нея. Всички заявки между клиента и сървъра са сигурно криптирани, за да не могат да бъдат модифицирани. SSH може да бъде използван от машини с различна операционна система, като Windows, Unix, Macintonsh и OS/2.

HTTP[9]

Протоколът за трансфер на хипертекст (англ.: 'hypertext transfer protocol', съкр. HTTP) е създаден като средство за публикуване на HTML страници. На практика протоколът довежда до формирането на Световната уеб мрежа. Разработването на протокола е дело на WWW Consortium и IETF (Internet Engineering Task Force) и завършва с публикуването на серия от документи, от които RFC 2616 (юни 1999) е със статут на стандарт и описва HTTP/1.1.

Понеже HTTP е протокол от високо ниво под понятията "клиент" и "сървър" не се разбират физическите хостове в мрежата. Клиентите са Web-браузърите или web-навигаторите, а сървърите са web-сървърите — т.е. самите приложения.

HTTP е безсесиен протокол — това означава, че резултатът на всяка следваща заявка не зависи от резултата на предишната и така всички клиенти получават равноправно еднакви ресурси. Тази функционалност би създала

[9] Уикипедия, Статия HTTP <https://bg.wikipedia.org/wiki/HTTP>

проблем например в един електронен магазин, където потребителите би трябвало да бъдат идентифицирани с различните си потребителски имена и покупки. Съществуват различни способи за приложението на сесии в HTTP. Най-надеждният от тях е употребата на бисквитки (cookies). При този способ сървърът залага бисквитките на клиентите със Set-Cookie в хедъра.

Във версиите 0.9 и 1.0 на HTTP, сървърът затваря връзката с клиента след всяка заявка. С версия 1.1. е въведен нов механизъм за поддържане на връзката наречен "keep alive", при който връзката може да бъде използвана многократно. Този тип постоянна връзка премахва забавянето, получено при установяването на TCP връзката след първата http заявка. Това свойство на протокола обикновено трябва изрично да бъде настроено на сървърния софтуер.

През май 2015 г. е приета следваща версия на протокола HTTP/2, който за разлика от предходните версии е бинарен. Някои от особеностите му са: мултиплексиране и поставяне на приоритети на заявките, съкращаване на заглавията, паралелно зареждане на няколко елемента, поддръжка на активни push уведомления от страната на сървъра (RFC 7540)[10].

SMTP[11]

SMTP (Simple Mail Transfer Protocol) е Интернет протокол, използван при обмена на електронни писма. Традиционно оперира с TCP порт 25. SMTP протокола се използва от повечето имейл системи, които изпращат поща. Писмата след това могат да се изтеглят с POP3 или IMAP от локален клиент или програма. Широко разпространение е получил в началото на 80-те години (1980). Преди това е бил използван Unix to Unix Copy Program протоколът, който изисква от изпращача пълен маршрут до получателя или постоянно съединение между компютрите на изпращача и получателя. SMTP протоколът е създаден да бъде еднакво полезен на който и да е компютър и потребител.

POP3 и IMAP

[10] Belshe,M. Proposed Standard <https://tools.ietf.org/html/rfc7540>

[11] Уикипедия, Статия SMTP <https://bg.wikipedia.org/wiki/SMTP>

POP3[12] (Post Office Protocol, текущата и най-използвана версия в момента е ver.3) е протокол за извличане на получена електронна поща от e-mail сървър върху клиентски компютър. Инициирането на връзката се извършва от клиентския компютър и инсталирания на него софтуер, най-често наричан "клиент за електронна поща" (или "e-mail клиент"), чрез който се четат получените съобщения. Протоколът позволява управление на съхраняваните съобщения, като те могат да се изтриват от сървъра след изтегляне, или да останат и да бъдат повторно изтегляни. Последното дава защита от повреда на клиентския компютър, както и възможност за четене на обща поща от няколко компютъра. С конфигурирането на клиента потребителят избира дали след получаването им писмата да остават на сървъра или да бъдат изтрити.

IMAP[13] (Internet Message Access Protocol, наричан в миналото Interactive Mail Access Protocol) е интернет протокол от приложния слой за достъп до електронна поща на отдалечен сървър от локален клиент. Той е по-нов от POP3 и през последните няколко години все повече се налага използването му. Той позволява двупосочен обмен на поща със сървъра, както и забрана на изходящата поща по SMTP от клиентските станции и използването на SMTP само за обмен между сървъри, с което се намалява възможността за изпращане на нежелана поща (спам).

И двата протокола се поддържат на практика от всички съвременни клиенти и сървъри за електронна поща, въпреки че в някои случаи са добавени към специфични за доставчика, обикновено частни, интерфейси. По принцип и двата протокола позволяват на един клиент за електронна поща да чете съобщенията, съхранени на сървъра за електронна поща.

Когато се използва POP3, клиентите обикновено се свързват със сървъра за много кратко, само колкото да заредят новите съобщения. С IMAP4 клиентите обикновено са свързани постоянно докато потребителският интерфейс е активен и те зареждат съдържанието на съобщенията само при

[12] Уикипедия, Статия Post Office Protocol <https://bg.wikipedia.org/wiki/Post_Office_Protocol>

[13] Уикипедия, Статия IMAP <https://bg.wikipedia.org/wiki/IMAP>

поискване. За потребители с много или големи съобщения, начинът на работа на IMAP4 носи много по-бързи времена на отговор.

POP3 протоколът предполага, че свързаният в момента клиент е единственият клиент, свързан с пощенската кутия. За разлика от него, протоколът IMAP4 позволява едновременен достъп от много клиенти и осигурява на клиентите механизми за откриване на промени, направени от други, едновременно свързани, клиенти.

Почти цялата електронна поща в Интернет се предава в MIME формат. MIME позволява на съобщенията да имат дървовидна структура, като листата са от един от многото единични типове съдържание, а възлите от по-висок ред са от един от структурните типове. Протоколът IMAP4 позволява на клиентите да изтеглят произволни отделни MIME части, а също така да изтеглят и само част от отделните MIME части или от цялото съобщение. Тези механизми позволяват на клиентите да изтеглят текстовата част на едно съобщение, без да се изтеглят приложените файлове или да извежда поточно съдържание по време на изтеглянето.

Чрез използване на флагове, дефинирани в протокола IMAP4 клиентите могат да следят състоянието на съобщенията, например прочетено ли е съобщението или не, дали му е отговорено и дали е изтрито. Тези флагове се записват на сървъра, така че много клиенти, които четат пощенската кутия по различно време, могат да отчитат промените в състоянието, направени от други клиенти.

IMAP4 клиентите могат да създават, преименуват и/или изтриват пощенски кутии на сървъра и да прехвърлят съобщения между различните пощенски кутии. Поддържането на много пощенски кутии дава възможност на сървърите да предлагат достъп до поделени или публични кутии.

IMAP4 осигурява механизъм за запитване към сървъра за търсене на съобщения, отговарящи на различни критерии. Този механизъм избягва необходимостта от зареждане на съобщенията на клиента при търсене.

Независимо дали използват POP3 или IMAP4 за получаване на съобщения, клиентите използват протокола SMTP за изпращане на съобщения. Клиентите за електронна поща често се наричат POP или IMAP клиенти, но и в двата случая се използва и SMTP.

IMAP често се използва в големи мрежи, каквито са университетските системи за електронна поща. Той позволява на потребителите да получават новите съобщения веднага на своите компютри, тъй като пощата се съхранява в мрежата. С POP3, потребителите трябва или да заредят електронната поща на своя компютър, или да я четат през уеб-интерфейс. И двата начина са по-бавни от IMAP, като новата поща трябва да се зарежда периодично или да се опреснява страницата в уеб-браузъра, за да се видят новите съобщения.

За разлика от много интернет протоколи, IMAP4 има вградени шифрирани механизми за достъп до акаунтите. Паролите, разбира се, могат да се предават по IMAP4 и нешифрирани. Тъй като механизмът за шифриране трябва да се договори между клиента и сървъра, при някои комбинации клиент-сървър се използват нешифрирани пароли (най-често Windows клиенти с не-Windows сървъри). IMAP4 обменът на данни може да се шифрира и с SSL.

TLS/SSL[14]

TLS (на английски: Transport Layer Security) и неговият предшественик SSL (на английски: Secure Sockets Layer) са криптографски протоколи, които осигуряват сигурност на комуникацията по Интернет. TLS и SSL са протоколи за криптиране, позиционирани над транспортния слой. Те използват асиметрична криптография за автентификация, симетрично шифриране за конфиденциалност и кодове за автентичност на съобщенията за запазване на целостта на съобщенията.

Няколко версии на протоколите се използват широко при уеб сърфиране, изпращане на електронна поща, изпращане на факс по Интернет, изпращане на мигновени съобщения и IP-телефония (VoIP).

[14] Уикипедия, Статия SSL <https://bg.wikipedia.org/wiki/SSL>

TLS позволява на клиент/сървърните приложения да комуникират в мрежата по начин, осигуряващ защита от подслушване и подправяне.

Когато клиентът и сървърът са се договорили за използване на TLS, те започват да установяват защитеното съединение. Това става с процедурата за потвърждаване на връзката. По време на този процес клиентът и сървърът се договарят за различните параметри, необходими за установяване на безопасното съединение.

1.5. Портове и сесии[15]

Протоколите TCP и UDP са посредници между приложенията и IP протокола. Съобщенията се изпращат на устройство, по зададен IP адрес. На съответното устройство (или компютър) работят много програми. Необходимо е да се укаже коя програма да бъде получател на съобщението. Това става чрез задаване на номер на порт.

Портът представлява число от 0 до 65 535. За да се осъществи комуникация, в устройството получател е стартирана програма, която „слуша" определен порт. Портовете с малки номера (от 0 до 1 023) са наречени добре познати портове (well-known ports), присвоени на конкретни приложения от организацията IANA. Например, портът за HTTP е 80, за FTP е 21 и т.н.

За определяне на крайната точка на TCP сесия се използва сесиен адрес. Той се състои от IP адреса и номера на порта. При изписване номера на порта се разделя от IP адреса със символ двоеточие. Примерно: 194.145.63.12:80 е сесиен адрес на WEB услугата на 'www.dir.bg'.

При установяване на TCP сесия от сървър се извършва пасивно отваряне (passive open). Така приложението-сървър указва на операционната система кой порт желае да приема връзки. Портът се намира в състояние на приемане (listening state).

---

[15] Йорданова,Н Електронен курс „Компютърни мрежи"
http://193.192.57.240/po/courses/problemni/komputarni%20mrezi/pdf/16.pdf

Програма в устройство-клиент изисква от операционната система да се свърже към сесиен адрес. Това е активно отваряне (active open), открива се сесията. Програмата клиент също трябва да притежава сесиен адрес. Операционната система служебно задава номер на порт, случайно число, по-голямо от 1024.

Състоянието на изградените сесии може да се наблюдава чрез TCP помощната програма netstat.

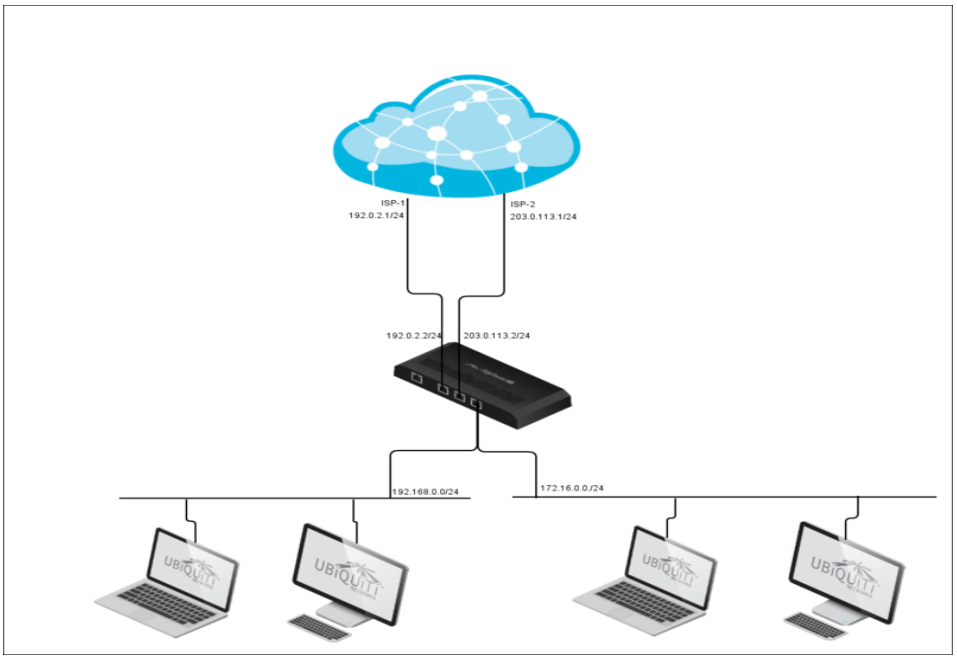
ГЛАВА II. АНАЛИЗ НА МЕТОДИ И СРЕДСТВА ЗА РАЗПРЕДЕЛЯНЕ НА ТРАФИКА

2.1. Статични методи за планиране

Статичното планиране за изпълнение на механизъм за балансиране на натоварването може да се приложи, когато е налична цялата информация, касаеща разделянето на трафика.

2.1.1. Мрежово разделяне на трафика

При наличие на данни за броя на крайните устройства, посредством които потребителите ползват интернет услуга, мрежовото адресно пространство, ползвано от тях, може да бъде разделено на две, като първата половина ползва шлюза на първия доставчик, а останалата на втория (вж. фигура 3). Политика на същият принцип може да бъде определена и посредством използването на адресни листи.



Фигура 3. Мрежово разделяне на трафика

Друг вариант на мрежово разпределение на трафика е посредством разделяне на интернет протокол адресите в глобалната мрежа на две. По този начин, без да имаме информация за броя на компютрите в локалната мрежа, можем да ползваме и двата доставчика. Маршрутизатора проверява пакета за адреса на получателя и спрямо него го изпраща към съответния шлюз.

Трети вариант е интернет трафикът в локалната мрежа да бъде разделен на жичен и безжичен такъв, като по този начин безжичният трафик преминава през единия доставчик а жичния през другия.

2.1.2. Разделяне на трафика по протокол и номер на порт

Портът е логическа точка на свързване. Портовете се използват от транспортните протоколи, TCP и UDP, за да идентифицират специфичното приложение, което изпраща или получава съобщението. Широко използваните Интернет приложения имат предефинирани номера на портове. Част от тях са показани в следващата таблица.

Порт	Протокол	Приложение
80	TCP	HTTP
21	TCP/UDP	FTP
23	TCP/UDP	Telnet
25	TCP/UDP	SMTP
110	TCP/UDP	POP3
119	TCP/UDP	NNTP
137	TCP/UDP	NetBIOS
161	TCP/UDP	SNP
194	TCP/UDP	IRC
389	TCP/UDP	LDAP
396	TCP/UDP	NetWare over IP
458	TCP/UDP	Apple Quick Time
500	TCP/UDP	ISAKMP

Таблица 4. Приложения и портове

В зависимост от ползваните услуги зад защитната стена/маршрутизатор, входящият и изходящият трафик може да бъде разделен по вида на протокола TCP/UDP и определен порт.

Трафикът може да бъде разделен по много критерии. Един прост пример за това е като определим HTTP и HTTPS трафика на портове 80 и 443 да преминава през единия шлюз, а останалият по другия. Така, когато

посещаваме интернет страници ще ползваме единият доставчик, а през другият ще сваляме файлове и вършим всички останали дейности в интернет.

2.1.3. Условно разделяне на трафика

Условното разделяне на трафика може да се определи на базата на цена/тежест на интерфейсите на доставчиците. Трафикът може да бъде разделен на базата на брой пакети. Например, ако искаме разделянето да стане в съотношение 1:2, то ще определим всеки трети пакет да бъде изпращан през втория доставчик. Недостатъкът на този метод е, че е необходимо трафикът да бъде следен и по отношение адресите на местоназначение и източник, за да не допуснем една сесия да преминава през различни портове.

2.2. Динамични методи за планиране

Динамичните методи за планиране на разпределяне на натоварването се използват когато няма налична информация по отношение на преминаващия интернет трафик. Тя постъпва и се анализира по време на работа на маршрутизатора, който съответно взима решения за определяне на ползвания шлюз.

2.2.1. Балансиращи сесии

Динамичното разпределяне на натоварване не се базира на предаването на пакет по пакет, а посредством така наречените балансиращи сесии.

Различните балансиращи сесии се различават по ИП адресите на източника и адресата, както и на протокола от по-високо ниво - TCP. В случай че е установена сесия и се появят нови пакети, различаващи се от тези в сесията само по номера на порта на източника и/или на адресата, те ще бъдат счетени като част от същата сесия. По такъв начин, дори пакетите да принадлежат на нова TCP сесия, те ще бъдат присъединени към вече установената балансираща сесия.

Веднъж открита, балансиращата сесия ще бъде маршрутизирана през един и същ балансиращ ресурс /шлюз/ докато не изтече. Единствено трафик,

който е разпознат като нова, отделна балансираща сесия /различен ИП адрес или протокол/ ще бъде маршрутизиран през различен балансиращ ресурс /шлюз/.

Поведението, което е описано по-горе е нужно, защото много уеб сървъри и други такива имат нива на сигурност, които, за да продължат, съответно вече отворената сесия, постоянно идентифицират ползвателя по неговия ИП адрес. WAN балансирането на трафика обикновено се използва във взаимодействие със защитната стена и NAT. Това предопределя, че разпределянето на трафика трябва да бъде съобразено по такъв начин, че за всяка балансираща сесия ще бъде ползван един WAN интерфейс и една и съща адресна транслация /NAT/. На потребителя няма да е никак приятно, ако по време на работа изведнъж бъде сменен неговият ИП адрес, поради смяна на номера на порта. Това може да доведе до загуба на идентификация към даден сървър.

Балансиращите сесии се управляват(създаване, изтриване и т.н.)чрез стартиране на таймер за всяка новосъздадена такава. Таймерът се нулира когато пакет от неговата сесия премине през разпределянето на трафика. Когато отделен таймер достигне определен краен лимит, то се счита, че сесията е изоставена и се прекратява.

2.2.2. Методи за планиране на разпределението на трафика

Има множество методи, които могат да бъдат приложени за разпределяне на мрежовото натоварване, такива биват разработвани и към момента. Всеки от тях използва специфична подредба или прехвърляне на мрежови пакети в различни буфери за предаване или получаване на данни. Методите биват използвани за компенсиране на различни мрежови проблеми, като намаляване на латентността за конкретни класове от мрежови пакети, а най вече като част от качеството на услугата (QoS).

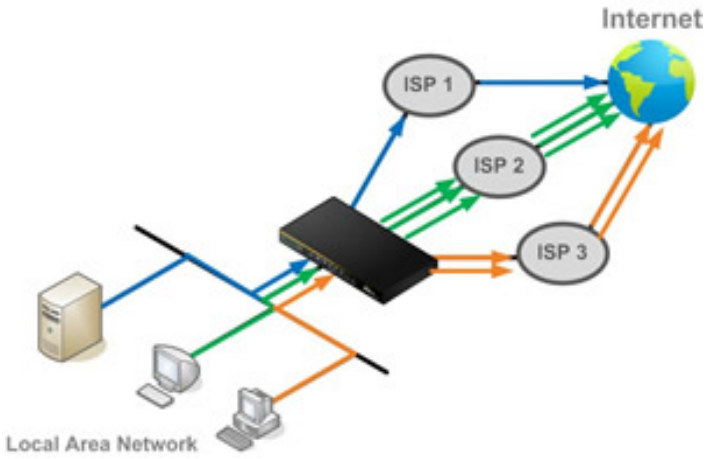
Някои основни методи са:

- RR Round-Robin – Това е стандартния метод за разпределяне на натоварването. Той работи като разпределя последователно и по равно

натоварването за определено време. Мрежовите устройства, които поддържат Round Robin планиране, имат отделни опашки от данни за всеки трафик, където той може да бъде идентифициран с адресите на своя източник и дестинация. Методът позволява на всеки активен трафик, който има пакети от данни в опашката, да трансферира пакети по споделен канал в периодичен, повтарящ се ред.

Механизмът на Round-robin планирането е равномерен, в случай че пакетите от данни са с еднаква големина. В противен случай, приоритет има потребителя с по-голям размер.

-WRR (weighted round robin)- Подобрена версия на round-robin с възможност за определяне на отношения при предаване на трафика през WAN портовете (вж. фигура 4). Например, ако знаем, че скоростта на връзката през даде WAN порт е два пъти по голяма, можем да определим трафика минаващ през него да бъде два пъти по голям от другите. Това става посредством определяне на тежест на порта.



Фигура 4. „Weighted Round Robin“ метод

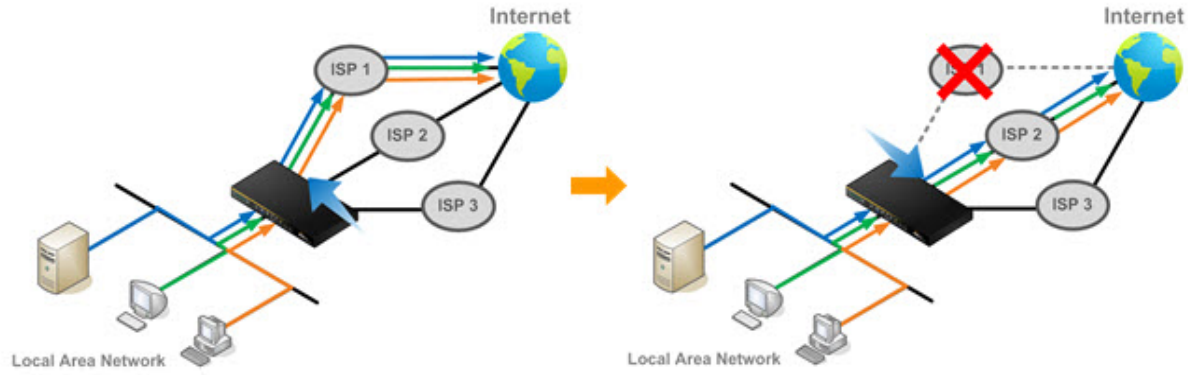
- Динамичен round-robin /Dynamic Round Robin, Dynamic Ratio/ - подобен на WRR, обаче тежестта се базира на постоянно следене на натоварването на линиите и съответно бъде променяно. Това е динамичен метод за разпределяне на мрежовите ресурси.

- Least connection: Агоритъмът разпределя натоварването на базата на броя на сесиите открити през даден канал. Работи най добре в среда с еднаква

скорост на WAN портовете. Методът е динамичен, като се основава на постоянно следена на откритите сесии и канала с най добро време за отговор.

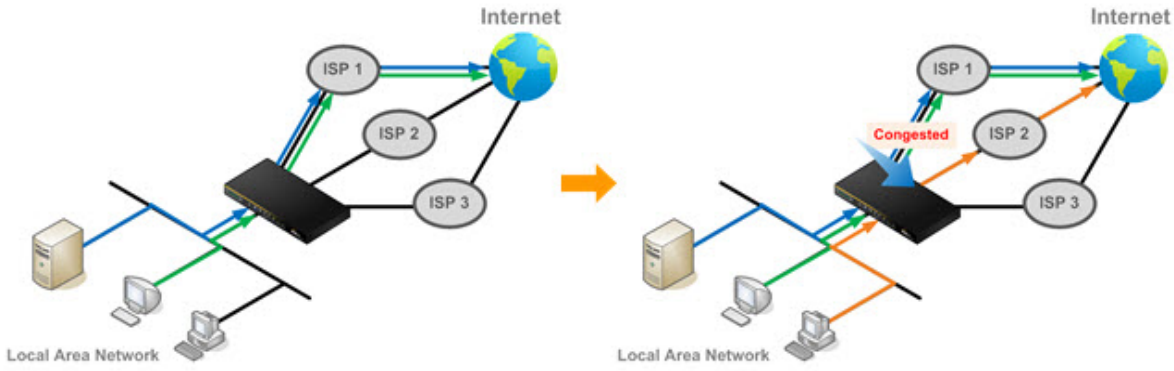
- Host Dependent: MAC адресът на дадено крайно устройство се използва, за да се определи WAN порта през който ще се свързва и трафикът ще минава единствено през него.

- Prority: Организира приоритетен ред на WAN портовете, през които се маршрутизира трафика (вж. фигура 5). Конфигурира се дадена приоритетна стойност на всеки порт, този с най голям ще поеме трафика, останалите, в съответния ред, ще поемат трафика, в случай на недостъпност на активния такъв.



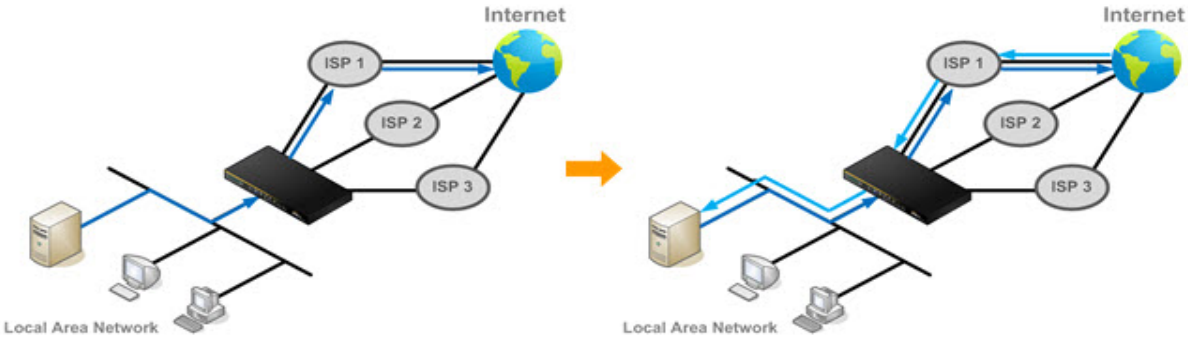
Фигура 5. Приоритетен метод

- Overflow: Трафикът се маршрутизира през WAN порта с най голям приоритет (вж. фигура 6). Динамично се следи натоварването му. В случай, че се претовари капацитетът му , с цел да се предотврати забавяне, новите сесии започват да се маршрутизират през следващия по проритет WAN порт.



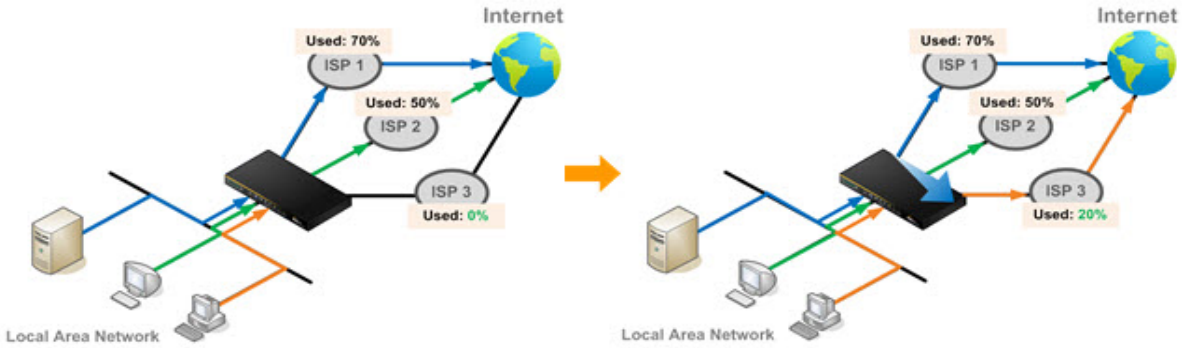
Фигура 6. Метод тип „Препълване“

- Presistance: Методът има за цел да реши проблема с прекъсването на сесии, ползващи HTTPS, електронно банкиране и други такива (вж. фигура 7). След определяне на типа специфичен трафик, той ще бъде маршрутизиран само през една връзка, докато сесията приключи.



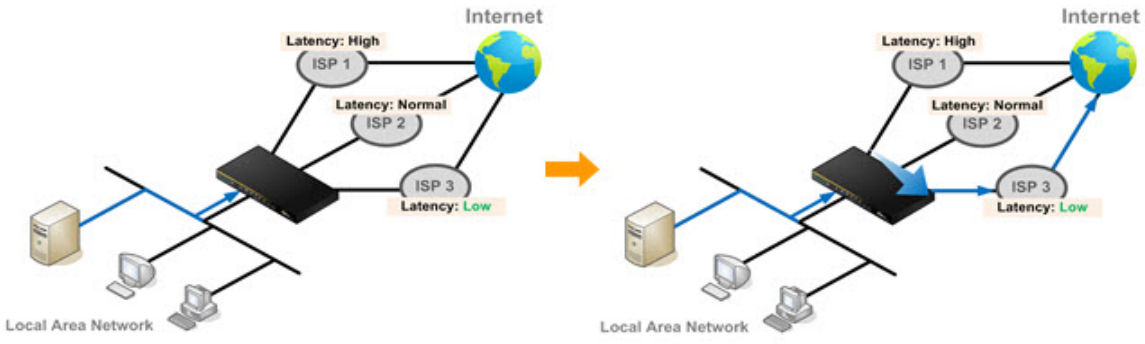
Фигура 7. „Presistance“ метод

- Least Used: Трафикът се пренасочва към WAN порта с най-малка натовареност (вж. фигура 8).



Фигура 8. Метод на най малкото натоварване

- Lowest Latency – Трафикът се маршрутизира през порта с най малко време за отговор (вж. фигура 9). Методът е подходящ за приложения, в които бързият отговор е от голямо значение, като например в онлайн игрите.

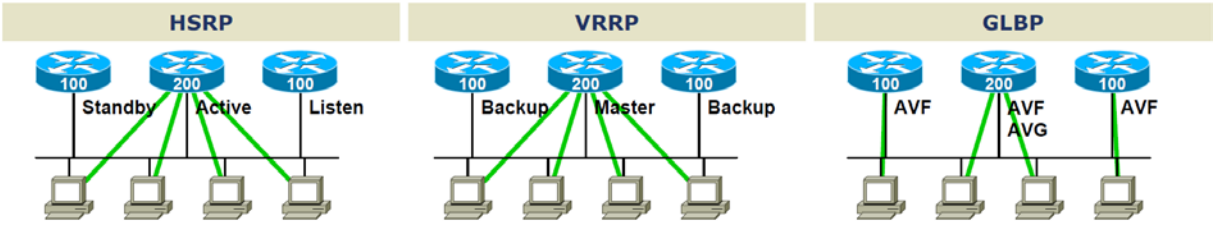


Фигура 9. Метод „Най малко време за реакция“

2.3. Маршрутизиращи протоколи за разпределяне на натоварването и отказ от услуга

Има много маршрутизиращи протоколи, които могат да осъществят връзка посредством няколко WAN порта, такива са RIP, OSPF, BGP, но тези протоколи обикновено избират своят маршрутизиращ път посредством метрика, вместо динамично, според съответното натоварване. Маршрутизатор с два WAN порта, свързани към различни доставчици, в повечето случаи ще маршрутизира трафика през порта, който осигурява най добра метрика. Това спомага, в случай че едната връзка се повреди, но при нормални обстоятелства допълнителната връзка е просто загуба на пропускателна способност.

Компанията Сиско има разработени протоколи, приложими към проблема отказ от услуга и разпределяне на трафика. Високата надеждност на достъпа (High availability) се постига чрез протоколи за дублиране на първия скок (First Hop Redundancy Protocol-FHRP), като например Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol(VRRP) и Gateway Load Balancing Protocol (GLBP).



Фигура 10. Основна схема на протоколите HSRP, VRRP и GLBP

GLBP протоколът изпълнява подобни функции като протоколите HSRP и VRRP. Последните два позволяват множество рутери да участват в една виртуална рутер-група, конфигурирана с виртуален ИП адрес. Един от участващите маршрутизатори се избира за активен и през него преминава трафика, изпратен през виртуалния ИП адрес за групата. Останалите рутери в групата са в положение изчакване, докато активният такъв не откаже. Видно е, че протоколите HSRP и VRRP не използват рационално наличните канали за трафик. Въпреки това, за разпределение на натоварването може да се конфигурират няколко виртуални групи рутери към всеки от физическите

такива, като се ползват различни шлюзове на крайните устройства, което е допълнително административни натоварване.

Предимството на GLBP протоколът е, че допълнително предоставя балансиране на трафика, използвайки само един виртуален IP адрес и няколко виртуални MAC адреси. Натоварването е споделено между всички рутери в GLBP групата, вместо да е поето от един рутер докато другите стоят неизползвани. Всяко крайно устройство се конфигурира с един и същ изходен виртуален IP адрес и всички рутери в групата участват в предаването на трафика. Участниците в протокола комуникират помежду си, чрез "Hello" съобщения, изпращани на всеки три секунди към мултикаст адрес 224.0.0.102, UDP порт 32222.

2.3.1. Описание на GLBP протокола[16]

2.3.1.1. Използване на активен виртуален шлюз

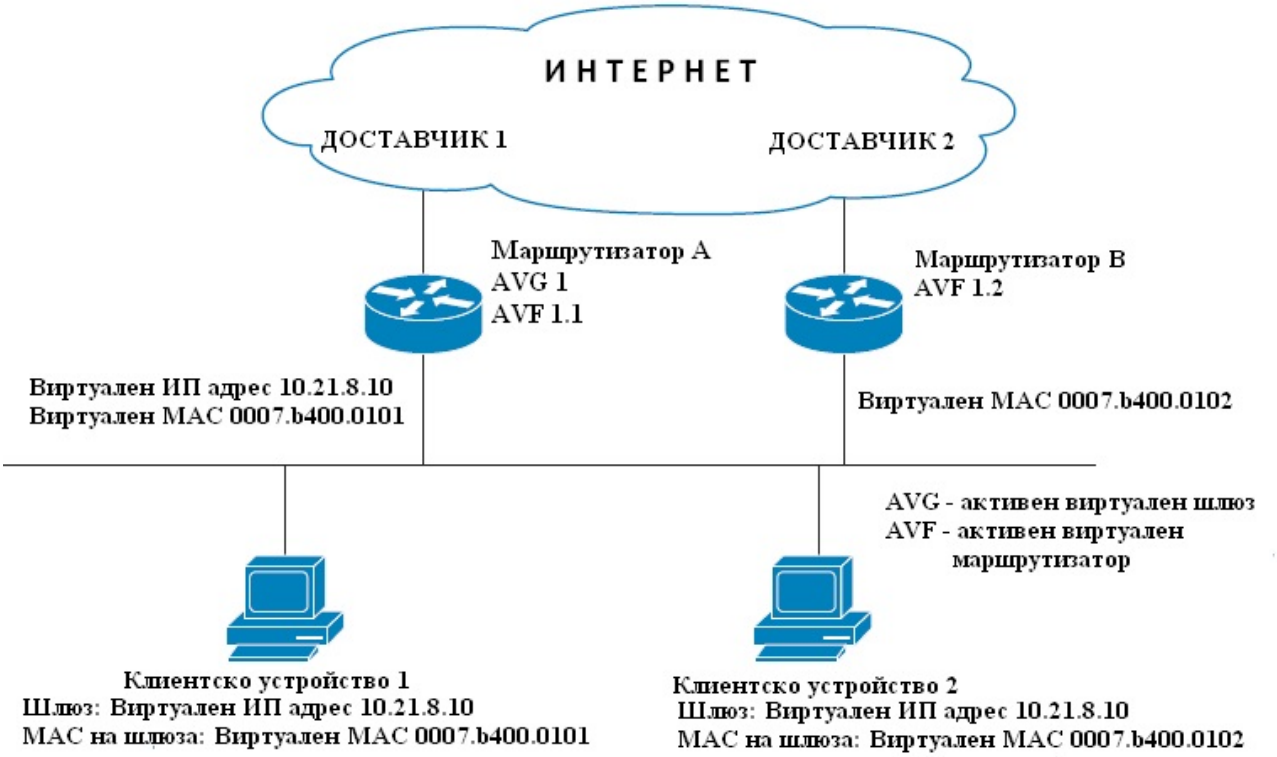
Участниците в GLBP групата избират един шлюз, който да бъде активния виртуален шлюз /active virual gateway(AVG)/ за тази група. Останалите членове на групата предоставят резервен такъв, в случай, че първия откаже. Функцията на активния виртуален шлюз е да определи виртуален MAC адрес на всеки участник от GLBP групата. Всеки шлюз има отговорността да маршрутизира пакетите, изпратени към виртуалния MAC адрес, определен от активния виртуален шлюз (AVG). Тези шлюзове са известни като активни виртуални маршрутизатори /active virtual forwarders (AVF)/, за техния MAC адрес.

AVG е също така отговорен за да отговаря на отправените запитвания на ARP /Address Resolution Protocol/, като връща съответните виртуални интернет протокол адреси /Virtual IP address/.

На фигура 11, маршрутизатор A е активният виртуален шлюз – AVG за GLBP групата и му е присвоен виртуален интернет протокол с адрес 10.21.8.10. Маршрутизатор A е също така и активен виртуален маршрутизатор

[16] Cisco Systems,Inc First Hop Redundancy Protocols Configuration Guide, Cisco IOS XE Release 3S, 2012

/AVF/ за виртуален MAC адрес 0007.b400.0101. Маршрутизатор B е член на същата GLBP група и е избран като активен виртуален маршрутизатор /AVF/ за виртуален MAC адрес 0007.b400.0102. Клиентско устройство 1 има шлюз с ИП адрес 10.21.8.10 и MAC адрес 0007.b400.0101. Клиентско устройство 2 споделя същия шлюз, но получава MAC адрес за кореспонденция - 0007.b400.0102, защото маршрутизатор B споделя натоварването на трафика с маршрутизатор A.



Фигура 11. Действие на GLBP протокола

Ако маршрутизатор A стане недостъпен, клиентско устройство 1 няма да изгуби интернет връзка, защото маршрутизатор B ще поеме отговорността за трансфериране на пакетите изпратени към виртуалния MAC адрес на маршрутизатор A, както и на пакетите изпратени към неговия виртуален MAC адрес. Маршрутизатор B ще поеме ролята на активен виртуален шлюз /AVG/ за цялата GLBP група. Въпреки повредата на маршрутизатор, комуникацията между участниците в GLBP групата продължава.

2.3.1.2. Присвояване на виртуален MAC адрес

В една GLBP група могат да бъдат ползвани до четири виртуални MAC адреси. Активният виртуален шлюз е отговорен за присвояването на виртуални MAC адреси на всеки участник в групата. За да стане това, участниците изпращат hello съобщения, за да установят активния виртуален шлюз /AVG/, след което изпращат заявка за присвояване на виртуален MAC адрес. На шлюзовете се присвояват последователни MAC адреси. Активният виртуален маршрутизатор, на който е присвоен виртуален MAC адрес от AVG се нарича първичен виртуален маршрутизатор. Останалите членове на групата научават своите виртуални MAC адреси посредством „Hello”-съобщения. Виртуалният маршрутизатор, на който е присвоен виртуален MAC адрес посредством hello съобщение, се нарича вторичен виртуален маршрутизатор.

2.3.1.3. Виртуална шлюзова резервираност

GLBP управлява виртуалната шлюзова резервираност по същият начин като HSRP. Един шлюз е избран като активен виртуален шлюз /AVG/, друг шлюз е избран за резервен виртуален шлюз, а останалите са поставени в режим на слушане.

Ако AVG се повреди, резервният виртуален шлюз ще поеме отговорност за трафика на виртуалния ИП адрес, след което ще бъде избран нов резервен виртуален шлюз от шлюзовете в режим на слушане.

2.3.1.4. Приоритет на шлюза

GLBP шлюзовият приоритет определя ролята, която всеки GLBP шлюз играе и какво се случва, ако AVG се повреди.

Приоритетно, може да бъде определен реда на маршрутизаторите, функциониращи като резервни виртуални шлюзове, при определяне на следващият AVG, ако той откаже. Конфигурирането на всеки от тези шлюзове може да стане посредством число от 1 до 255, чрез използване на команда glbp priority.

Във фиг.9, ако мрежовата връзка до маршрутизатор A, който е AVG, се повреди, веднага се извиква процес на избор, за установяване на резервен виртуален шлюз, който ще го замести. В посоченият пример, маршрутизатор B е единственият участник в групата и по тази причина ще стане AVG. Ако съществуваше друг маршрутизатор в групата, с по-голям приоритет, тогава той щеше да бъде излъчен като AVG. Ако двата имаха един и същ приоритет, то резервният виртуален шлюз с по-големия ИП адрес ще бъде избран за активен виртуален шлюз.

По подразбиране, GLBP подредбата на виртуални шлюзове е изключена. Резервният виртуален шлюз може да стане AVG, единствено ако настоящият се повреди, независимо от присвоените приоритети на виртуалните шлюзове. Посредством командата glbp preempt, можем да включим автоматична подредба на виртуалните шлюзове. Това позволява на резервен виртуален шлюз да стане активен, ако му е присвоен по-висок приоритет от настоящият.

2.3.1.5. Натоварване и следене на шлюза

GLBP използва система за планиране на натоварването, чрез която установява капацитета на всеки маршрутизатор в групата. След като се определи този капацитет, се определя и пропорцията от потребителски крайни устройства, които той да обслужва. При превишаване на капацитета, натоварването автоматично се прехвърля на друг маршрутизатор.

Капацитетът на всеки маршрутизатор се определя чрез следене на натоварването на интерфейсите му. Ако даден интерфейс се повреди, капацитетът на маршрутизатора се намалява с определена стойност.

По подразбиране, GLBP превантивната схема на виртуалният шлюз е включена и работи със закъснение от 30 секунди. Резервният виртуален шлюз ще стане активен такъв, ако капацитетът на текущия падне под определен праг за 30 секунди. Това може да се забрани с командата no glbp forwarder preempt или да бъде променено времето за изчакване с командата glbp forwarder preempt delay minimum.

2.3.1.6. Предимства на GLBP протокола

- Споделяне на натоварването – Протоколът може да бъде конфигуриран по такъв начин, че трафика от клиентите в локалната мрежа да бъде споделен между множество маршрутизатори поравно.
- Множество виртуални маршрутизатори – Протоколът поддържа до 1024 виртуални маршрутизатора /групи/ на всеки физически интерфейс на рутера и до четири виртуални шлюза на група.
- Взаимозаменяемост – В зависимост от ползваната схема, протоколът извършва подбор на виртуалните шлюзове. При включване в групата на виртуален шлюз с по висок капацитет от активния такъв, той автоматично става предпочетен и излъчен като активен.
- Автентичност – Може да бъде използвана проста текстова парола за автентичност между участниците в GLBP групата, за установяване на конфигурационни грешки. Всеки маршрутизатор с различна парола за автентикация, ще бъде игнориран от останалите членове.

2.3.1.7. Конфигуриране и проверка на GLBP протокола

Протоколът е създаден по такъв начин, че да бъде лесно конфигуриран. Всеки шлюз в групата трябва да бъде конфигуриран с един и същ номер на група и най малко един шлюз в групата трябва да бъде конфигуриран с виртуален ИП адрес, който ще бъде използван от цялата група. Останалите параметри могат да бъдат научени от участниците автоматично.

Ако използваме VLAN-ове на интерфейсите, номерата в GLBP групата трябва да са различни за всеки VLAN.

Командни стъпки за бързо конфигуриране на протокола:

1. enable – команда за даване на права в режим на изпълнение.
2. configure terminal – влизане в режим на глобални настройки.

3. interface *mun* - определяне на типа и номера интерфейса, който ще конфигурираме.
4. ip address *ip-address mask* – Определяме ИП-то на интерфейса.
5. Glbp *group* ip *ip-address* – Стартира GLBP протокола на конкретния интерфейс и идентифицира ИП адреса на виртуалния шлюз.
6. Exit – излизане от ниво конфигурация на интерфейс и връщане в ниво конфигуриране на глобални настройки.
7. Show glbp [*interface-type interface number*] [*group*] [*state*] [***brief***] – Командата не е задължителна. Показва състоянието и дава информация за GLBP групата. Опцията brief може да бъде ползвана за получаване на кратка информация за всеки виртуален шлюз.

2.4. Използване на софтуерни защитни стени/маршрутизатори за разпределяне на натоварването

Един от евтините варианти за решение на проблема за разпределяне на натоварването между два интернет доставчика е ползването на безплатни продукти, представляващи защитна стена/ рутер. Самият продукт дава информация за оптимизацията, тъй като осигурява средства за мониторинг на трафика. Така може да разберем и каква част от капацитета се използва по предназначение и колко се разхищава. Информацията включва количество трафик, брой сесии, хост и приложение източник на трафика. С тази информация, на защитните стени могат да се дефинират различните политики спрямо вида трафик. По посочените критерии трафикът може да се пренасочва и разпределя.

Примери за софтуерни мрежови защитни стени са PfSense, Endian, Untagle, Vyatta, Alpine, Astaro Heartbeat, HAProxy и др.

Цитираните продукти могат да бъдат ползвани в компютърна конфигурация с минимални хардуерни изисквания.

2.4.1. Софтуерна защитна стена Endian[17]

Endian е дистрибуция на Линукс, създадена за маршрутизиране, защитна стена, а също така и като интегрирана система за управление на заплахи. Това означава, че в едно самостоятелно решение и на един управляем панел, можете конфигурирате, в допълнение към защитната стена, защитни механизми като антивирус, антиспам, VPN, разпределяне на натоварването и др. Софтуера има удобен web интерфейс, който е достъпен през всички web браузери.

Endian поддържа и допълнителни функции като Stateful Inspection Firewall, Intrusion Detection and Prevention, VoIP support, Dos and DDos Protection, NAT, HA (High Availability), Load Balancing, VPN с опции IPsec, OpenVPN и PPTP, AntiVirus, AntiSpam, Dynamic DNS.

2.4.2. Софтуерна защитна стена Pfsense

Pfsense е Free-BSD базирана безплатна дистрибуция с отворен код за защитни стени и маршрутизатори. Проектът стартира през 2004г. на базата на m0n0wall. Използва се като софтуер за защитна стена, малък/домашен рутер, рутер за средни и големи мрежи, Wireless Access Point, а също и за устройства със специално предназначение – VPN, VoIP, DNS сървър, подслушване на мрежовия трафик и др. PfSense софтуера включва web интерфейс, през който лесно могат да бъдат правени настройки на всички компоненти и не са необходимо знания относно UNIX/Linux команди. Последната стабилна версия е 2.2. Тя може да бъде изтеглена от следния линк: https://www.pfsense.org/download/ и инсталирана на компютърна система с минимални изисквания (RAM-256 MB, PentiumII).

[17] Уикипедия, Статия Endian Firewall <https://en.wikipedia.org/wiki/Endian_Firewall>

2.5. Хардуерни решения за разпределяне на трафика между два интернет доставчици

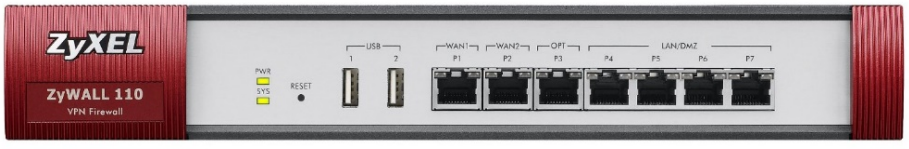
Когато се говори за разпределяне на мрежовото натоварване в повечето случаи се има предвид устройство, създадено за тази цел. Това устройство е вид сървърен компютър със специфична операционна система, настроена да управлява мрежовия трафик използвайки правила създадени от потребителя. Големите компании и фирми предоставящи хостинг услуги разчитат на устройствата за разпределяне на натоварването за постигнат най високо ниво на надеждност на услугата.

В допълнение, тези устройства предлагат разпределящи услуги към множество сървъри, спомагат за противодействие на атаките за отказ от услуга, осигуряват на потребителите непрекъсваема услуга и предотвратява недостатъчна пропускателна способност.

Това са маршрутизатори с два WAN порта, които лесно се конфигурират през web интерфейс и притежават множество вградени опции за статично и динамично балансиране на трафика, както и много други функции на защитна стена.

В таблицата са показани маршрутизатори, притежаващи два WAN порта и изпълняващи функция за разпределяне на натоварването между тях.

модел	**снимка**	**цена**
Предложения от фирма TP-LINK Technologies Co., Ltd		
TL-ER6020		224,69лв
TL-R4299G		325,80лв

TL-ER6120		350.00лв.
Фирма CISCO Systems Inc.		
RV042		317.00лв.
RV325		640.00лв.
RV320		400.00лв.
RV082		585.00лв.
Фирма Cisco-Linksys, LLC		
LRT224		387.00лв.
	Фирма ZyXEL Communications Corp.	
ZyWALL110		

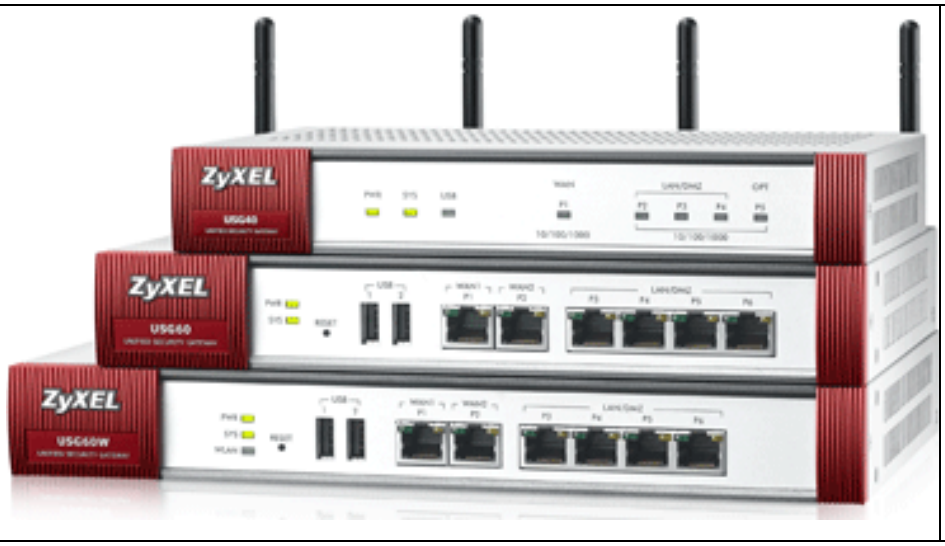
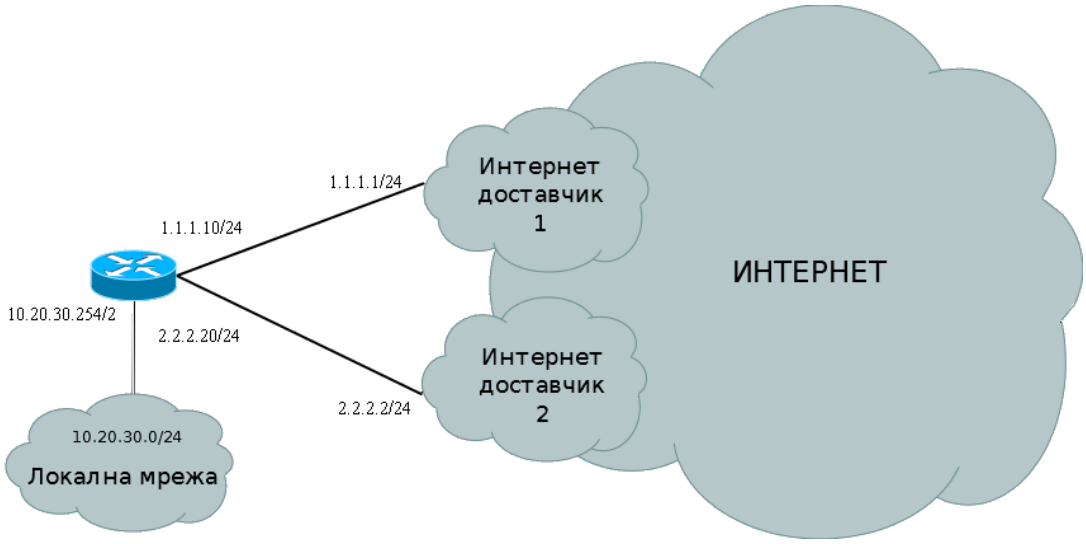
USG60 USG60W USG40 USG40W		650 euro 690 euro 430 euro 490 euro
Фирма PePLink Ltd		
Balance One		830.00лв
Balance 20		495.00лв

Таблица 5. Списък на маршрутизатори с два WAN порта

ГЛАВА III. РЕАЛИЗАЦИЯ И ПРАКТИЧЕСКИ РЕШЕНИЯ НА ПРОБЛЕМА ЗА РАЗПРЕДЕЛЯНЕ НА ТРАФИКА И ОТКАЗ ОТ УСЛУГА

3.1. Реализация с политика за маршрутизация с Микротик[18]



Фигура 12. Схема на интернет с два доставчика

3.1.1. Базова конфигурация

Конфигуриране на IP адресите на мрежовите интерфейси и NAT.

```
/ipaddress
add address=10.20.30.254/24 interface=ether5-LAN
add address=1.1.1.10/24 interface=ether2-ISP1
add address=2.2.2.20/24 interface=ether3-ISP2
/ipfirewall nat
add action=masquerade chain=srcnatout-interface=ether2-ISP1
add action=masquerade chain=srcnatout-interface=ether3-ISP2
        /ipdnsset allow-remote-requests=yes servers=1.1.1.1,2.2.2.2
```

3.1.2. Дефиниране на маршрутни таблици

Ще дефинираме следните маршрути:

```
/iproute
add gateway=1.1.1.1
add gateway=2.2.2.2
add gateway=1.1.1.1 routing-mark=ISP1
```

---

[18] Димитров, П. Разпределение на трафика, София, MUM България, 2014 <http://mum.mikrotik.com/presentations/BG14/pdimitrov.pdf>

add gateway=2.2.2.2 routing-mark=ISP2

3.1.3. Маршрути за директно свързани мрежи

При добавяне на IP адрес към интерфейс, се добавя автоматично динамичен маршрут само в маршрутната таблица main. Трафика за локалните мрежи, насочен към таблици ISP1 и ISP2, ще попадне на маршрутите по подразбиране в тези таблици. Ще осигурим маршрути за директно свързаните мрежи в маршрутните таблици, различни от main.

```
/iproute
add dst-address=10.20.30.0/24 gateway=ether5-LAN routing-mark=ISP1
add dst-address=1.1.1.0/24 gateway=ether2-ISP1 routing-mark=ISP1
add dst-address=2.2.2.0/24 gateway=ether3-ISP2 routing-mark=ISP1
add dst-address=10.20.30.0/24 gateway=ether5-LAN routing-mark=ISP2
add dst-address=1.1.1.0/24 gateway=ether2-ISP1 routing-mark=ISP2
add dst-address=2.2.2.0/24 gateway=ether3-ISP2 routing-mark=ISP2
```

3.1.4. Разпределяне на трафика чрез /ip route rule

/ip route rule съдържа правила за маршрутизация, указващи какво действие да се извърши с трафик, отговарящ на определени условия:

- Трафикът може да се разграничава по адрес на източника/местоназначението, маркировка за маршрутизация или входящ интерфейс;
- Трафика може да се унищожи (drop, unreachable) или обработи в определена маршрутна таблица (lookup, lookup only in table);

Да маршрутизираме първата половина от адресното пространство на локалната мрежа през ISP1, втората половина –през ISP2:

```
/iproute rule
add src-address=10.20.30.0/25 table=ISP1
add src-address=10.20.30.128/25 table=ISP2
```

3.1.5. Разпределяне на трафика по протокол

Правилата в /ip firewall mangle работят на принципа "ако-тогава". Условията в частта "ако" ще използваме за да разграничим трафика според желанието ни, действията в частта "тогава" -за да поставим съответната маркировка.

Маркировка за маршрутизация може да се постави само във вериги prerouting и output. Тя указва за местоназначението на маркирания пакет в коя маршрутната таблица да се търси маршрут.

Маркировката на връзки предоставя възможност за оптимизация на mangle, както и за работа с всички пакети, принадлежащи на определена връзка.

Ще използваме следния подход:

При установяването на нови връзки, ще маркираме връзките по различен начин, в зависимост от желанието ни през кой доставчик да бъдат маршрутизирани. Ще маркираме всички пакети, принадлежащи на връзки с определена маркировка, с маркировка за маршрутизация през съответния доставчик.

/ipfirewall mangle
add chain=preroutingprotocol=tcpdst-port=80 connection-mark=no-mark action=mark-connection new-connection-mark=ISP1
add chain=preroutingconnection-mark=ISP1 action=mark-routing new-routing-mark=ISP1 passthrough=no
add chain=preroutingprotocol=tcpdst-port=443 connection-mark=no-mark action=mark-connection new-connection-mark=ISP2
add chain=preroutingconnection-mark=ISP2 action=mark-routing new-routing-mark=ISP2 passthrough=no

По този начин трафикът ще бъде разделен по протоколи. Трафикът на протокол HTTP ще минава през единия доставчик, а трафикът на протокола HTTPS ще минава през другия.

3.1.6. Разпределяне на трафика на база адресни листи

/ipfirewall address-list
add address=10.20.30.1-10.20.30.100 list=isp1
add address=10.20.30.101-10.20.30.200 list=isp2
/ipfirewall mangle
add chain=preroutingsrc-address-list=isp1 connection-mark=no-mark action=mark-connection new-connection-mark=ISP1
add chain=preroutingconnection-mark=ISP1 action=mark-routing new-routing-mark=ISP1 passthrough=no
add chain=preroutingsrc-address-list=isp2 connection-mark=no-mark action=mark-connection new-connection-mark=ISP2
add chain=preroutingconnection-mark=ISP2 action=mark-routing new-routing-mark=ISP2 passthrough=no

3.1.7. Осигуряване на механизъм за безотказност

Ще осигурим за всяка от маршрутните таблици за двата доставчика маршрут по подразбиране с по-висока цена през другия доставчик.

/iproute
add gateway=2.2.2.2 distance=2 routing-mark=ISP1
add gateway=1.1.1.1 distance=2 routing-mark=ISP2
Ще използваме check-gateway=ping за да следим достъпността на шлюзовете
/iproute set check-gateway=ping [/iproute find dst-address=0.0.0.0/0]

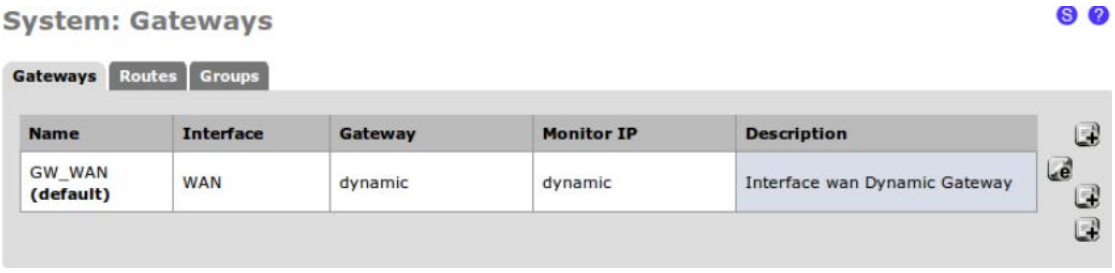
3.2. Пример за конфигуриране на защитна стена Pfsense за разпределяне на трафика между два WAN интерфейса[19]

3.2.1. Конфигуриране на WAN интерфейсите

За конкретния пример ще бъдат ползвани частни ИП адреси за конфигуриране на WAN интерфейсите, но при реална конфигурация, те трябва да бъдат заменени с публични, предоставени от доставчиците ви.

Последователни действия:

1. Чрез web интерфейса, отиваме на страница System | Router и избираме меню Gateways.
   - Обърнете внимание, че автоматично е създаден динамичен шлюз по подразбиране (вж. фигура 13).

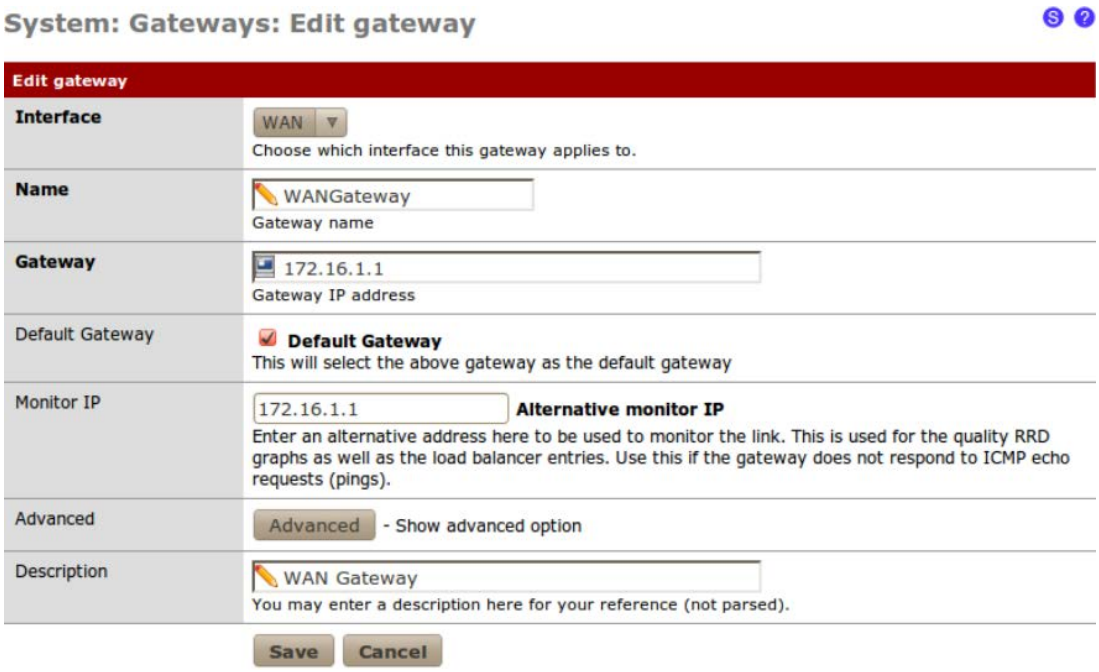


Фигура 13. Избор на шлюз

2. Избираме бутон плюс (+), за добавяне на нов шлюз (вж. фигура 13).

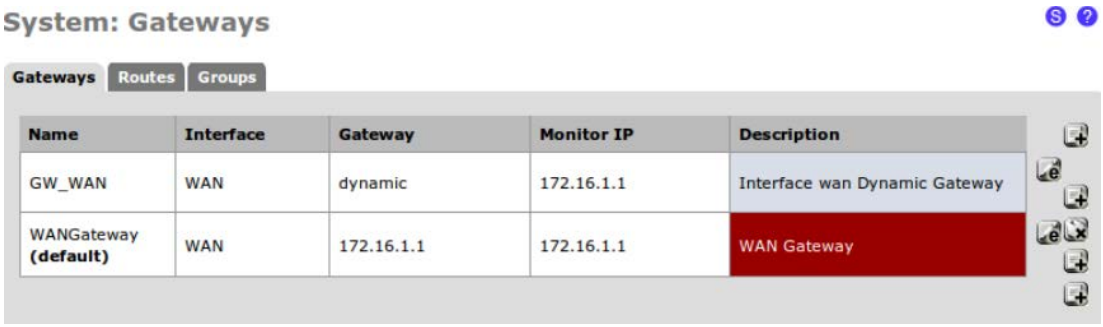
[19] Статия, „Балансировка нагрузки, приоритезация траффика (QoS), отказоустойчивость в pfSense 2.0“ <http://shop.nativepc.ru/content/94--pfsense-load-balance->

3. Избираме интерфейс (Interface), указваме неговото име (Name) и ИП адрес.
4. Правим отметка на флага шлюз по подразбиране (Default Gateway)(вж. фигура 14).
5. Добавяме описание в полето (Description), например WAN Gateway (вж. фигура 14).



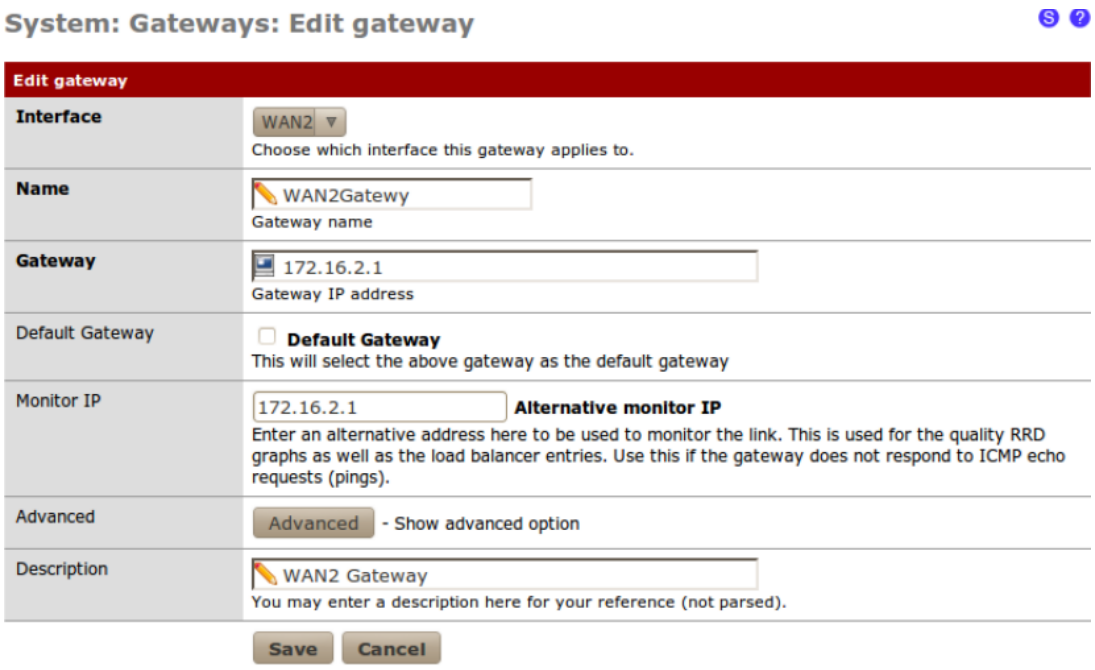
Фигура 14. Конфигуриране на Шлюз №1

6. Записваме (Save) измененията.



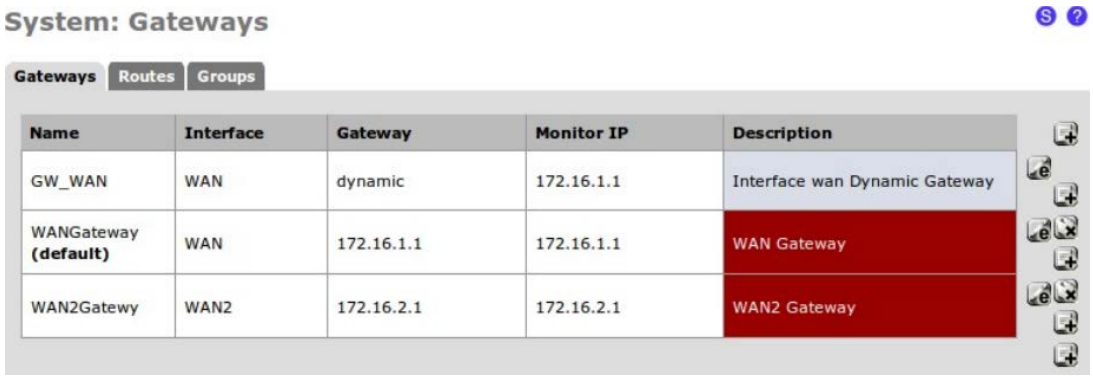
Фигура 15. Шлюзове след конфигуриране

7. Избираме бутон плюс (+) и добавяме нов шлюз.
8. Избираме интерфейс (Interface), указваме неговото име (Name) и ИП адрес (вж. фигура 16).
9. Правим отметка на флага шлюз по подразбиране (Default Gateway).
10. Добавяме описание в полето (Description), например WAN2 Gateway (вж. фигура 16).



Фигура 16. Конфигуриране на Шлюз 2

11. Запазваме (Save) промените.



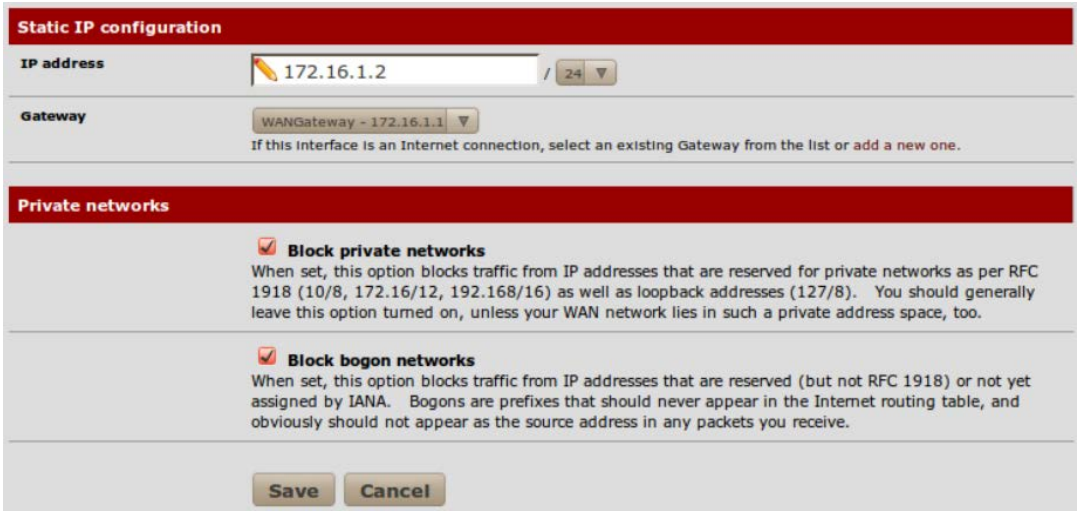
Фигура 17. Шлюзове, след конфиг. на двата интерфейса

12. Отиваме на страница Interface | WAN и изберете тип (Type) статичен (Static) (вж. фигура 18).

Фигура 18. Определяне на статичен път на интерфейс 1

13. Указваме ИП адрес (IP Address) и избираме новосъздадения шлюз (Gateway). Правим отметка на флагове Block private networks

(Блокиране на частни мрежи) и Block bogon networks (Блокиране на резервирани мрежи) (вж. фигура 19).

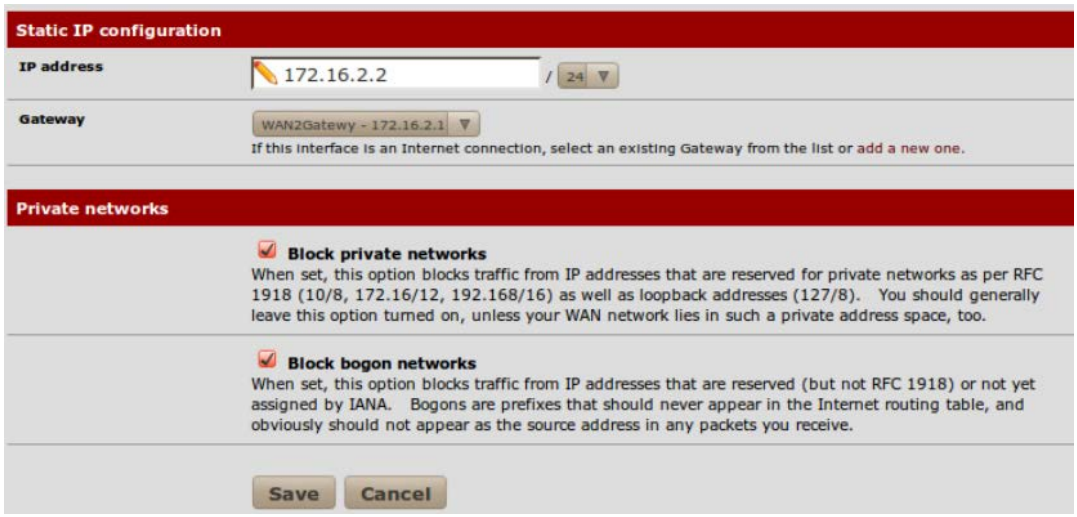


Фигура 19. Блокиране на частните мрежи на интерфейс 1

14. Запазваме (Save) промените.
15. Отиваме на страница Interface | WAN2 и избираме тип (Type) статичен (Static) (вж. фигура 20).

Фигура 20. Определяне на статичен път на интерфейс 2

16. Указваме ИП адрес и избираме новосъздадения шлюз (Gateway).
17. Правим отметка на флагове Block private networks (Блокиране на частни м-жи) и Block bogon networks (Блокиране на резерв. мрежи).



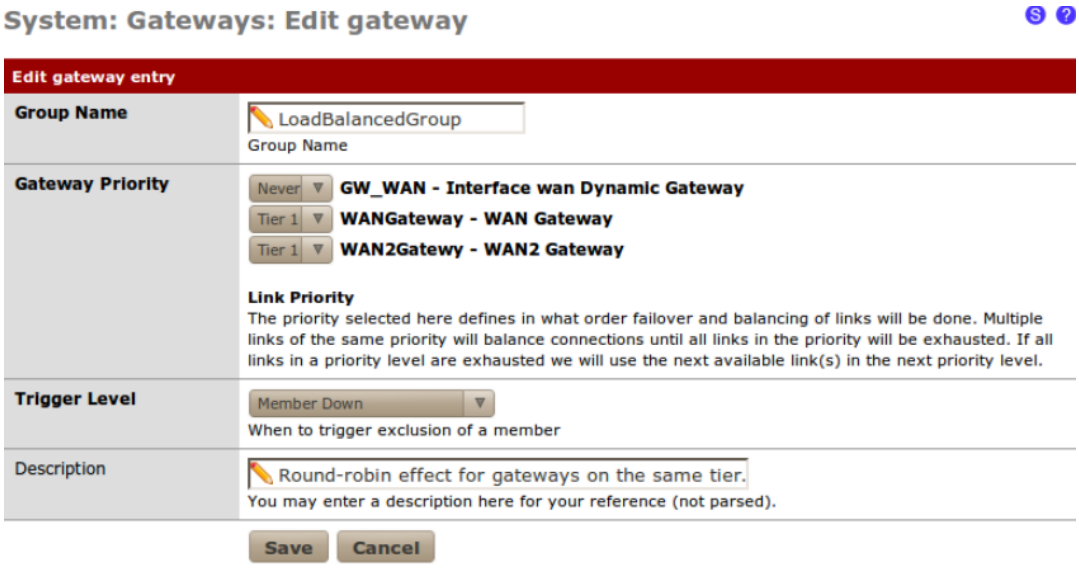
Фигура 21. Блокиране на частните мрежи на интерфейс 2

18. Запишете (Save) и приемете промените (Apply).

3.2.2. Настройки за разпределяне на трафика и отказоустойчивост в pfsense.

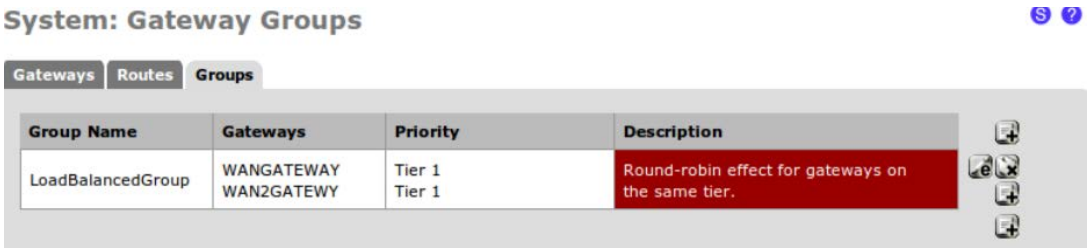
Поредност на действията:

1. Отиваме на страница System | Routing
2. Избираме меню Group.
3. Въвеждаме името на групата (Group Name) (вж. фигура 22).
4. Установяваме приоритетния шлюз (Gateway Priority), двата WAN порта поставяме в значение Tier 1 (вж. фигура 22).
5. Оставяме свойството на ниво на тригер (Trigger Level) в състояние Member Down (фигура 22) (Member Down: сработва, когато Monitor IP, установен за шлюза, престава да отвръща на ICMP заявките).
   - Packet Loss: сработва, когато пакетите, изпратени през даден шлюз се губят.
   - High Latency: сработва, когато пакетите изпратени през определен канал имат голямо забавяне.
   - Packet Loss or High Latency: сработва, когато пакетите, преминаващи през даден шлюз се губят или имат голямо забавяне.
6. Добавяме описание (Description).



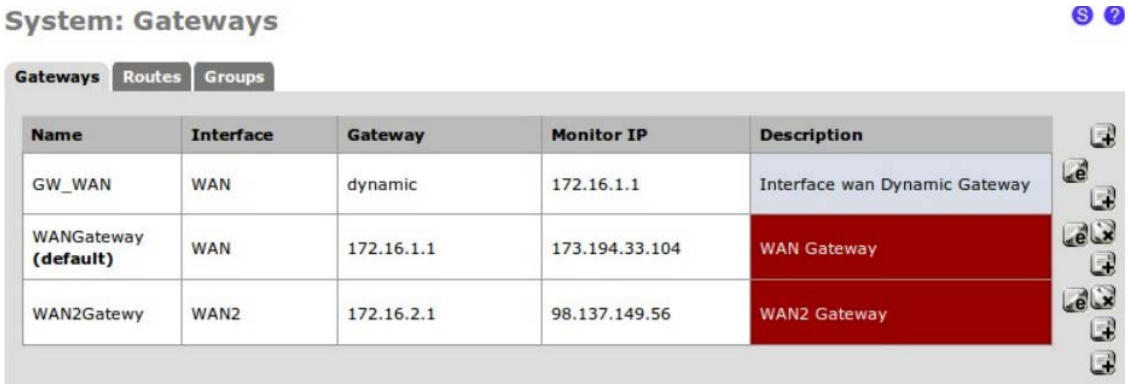
Фигура 22. Конфигуриране на балансиране на натоварването.

7. Записваме (Save) промените.
8. Приемаме (Apply) измененията.



Фигура 23. Балансираща група

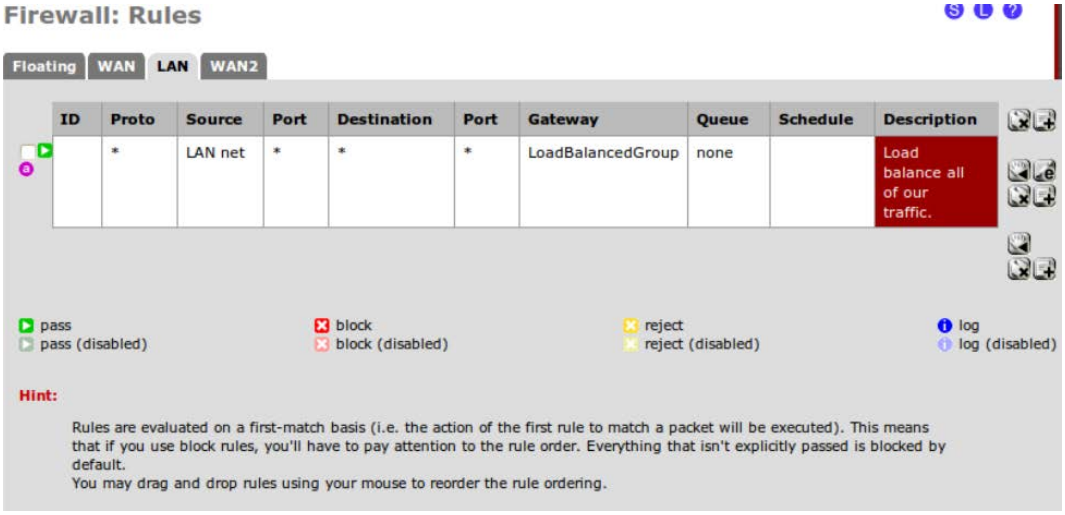
9. Отиваме на страница System|Routing.
10. Правим промяна на шлюз WAN.
11. Указваме външен ИП адрес, който ще се ползва за следене на трафика, в полето „Monitor IP“. В конкретния случай избираме ИП за http://www.google.com, но може да се избере и по близък такъв.
12. Записваме промените (вж. фигура 24).
13. Правим промени и в шлюз WAN2, като указваме външен ИП адрес в полето „Monitor IP“, в случая е въведено ИП на сайта http://www.yahoo.com/ (вж. фигура 24).
14. Записваме (Save) и приемаме (Apply) измененията.



Фигура 24. Изглед на конфигурираните шлюзове.

15. На страница Firewall|Rules натискаме знак плюс (+), за да добавим ново правило за защитната стена. Избираме действие “Pass”, след което отиваме на LAN интерфейса, където установяваме (Protocol) в „any“ (вж. Фигура 25).
16. Установяване на източника (Source) в „LAN subnet“.
17. Установяваме местоназначение (Destination) в „any“.

18. Добавяме описание в (Description).
19. В менюто разширени възможности (Advanced Features), под шлюза (Gateway), изберете бутон Advanced.
20. Задайте шлюза (Gateway) в значение „LoadBalancedGroup“ (вж. фигура 25).
21. Запишете (Save) и приемете (Apply) измененията.



Фигура 25. Определяне на правила за защитната стена

Конфигуриран по този начин, софтуерът Pfsense ще направлява трафика от локалната мрежа през създадената шлюзова група, в която са двата WAN порта. Тъй като последните са с еднакъв приоритет, те ще бъдат ползвани в цикличен стил. Когато ползваме разпределяне на натоварването, автоматично работи и услугата за отказоустойчивост.

3.3. Конфигуриране на разпределянето на трафика между два WAN порта на серията маршрутизатори ZyWALL на фирма ZyXEL[20]

Фигура 26. Маршрутизатор ZyWALL 110

[20]Статия, „Функция балансировки нагрузки (Load Balancing) между двумя WAN-портами на ZyWALL” <http://zyxel.ru/kb/1443>

При серията ZyWALL (вж. фигура 26), на фирмата ZyXEL, за балансиране на натоварването между двата WAN порта могат да бъдат определени два режима на работа:

- Active/Passive mode означава, че само един WAN порт се използва постоянно. Когато той откаже, трафикът автоматично се прехвърля на втория WAN порт.
- Active/Active mode означава, че двата WAN ще бъдат ползвани едновременно. При този режим на работа е възможно да бъдат определени различни алгоритми за разпределение на натоварването между двата порт. Всички алгоритми работят на база сесии.

Поддържат се три алгоритъма на балансиране:

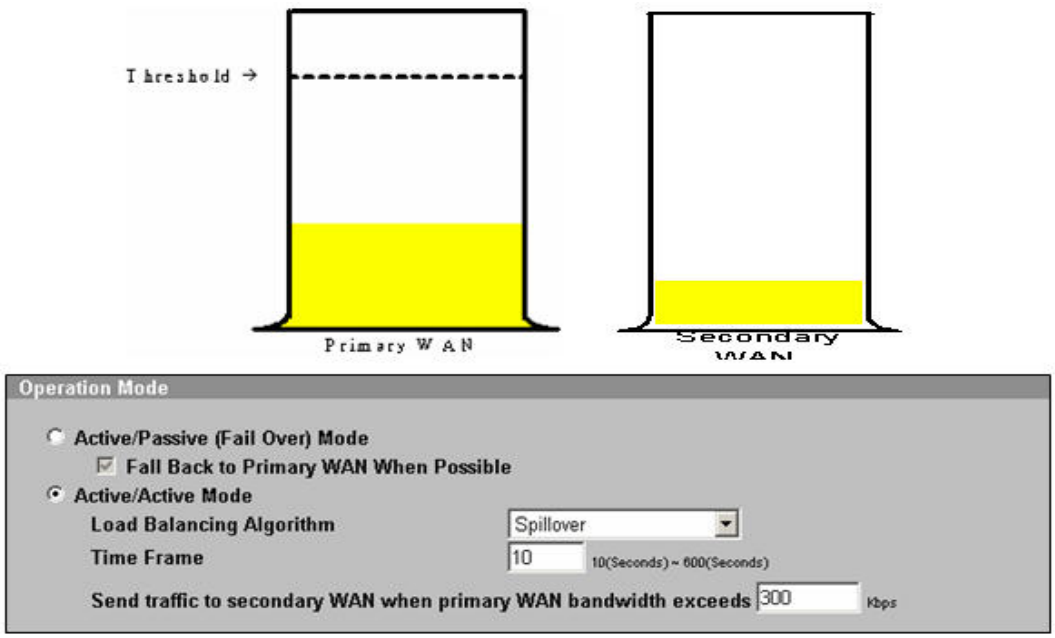
- Spillover
- Weighted Round Robin
- Least Load First

Посредством ползване на функцията за разпределяне на натоварването, двата WAN интерфейса могат да работят паралелно. Всеки път, когато възникне нова изходяща TCP сесия с LAN интерфейс или DMZ, устройството на ZyXEL избира един от двата WAN порта за трансфериране на пакетите. TCP сесията се открива и закрива само на един и същ WAN интерфейс.

По подробно описание на механизмите на изпълнение за разпределяне на натоварването:

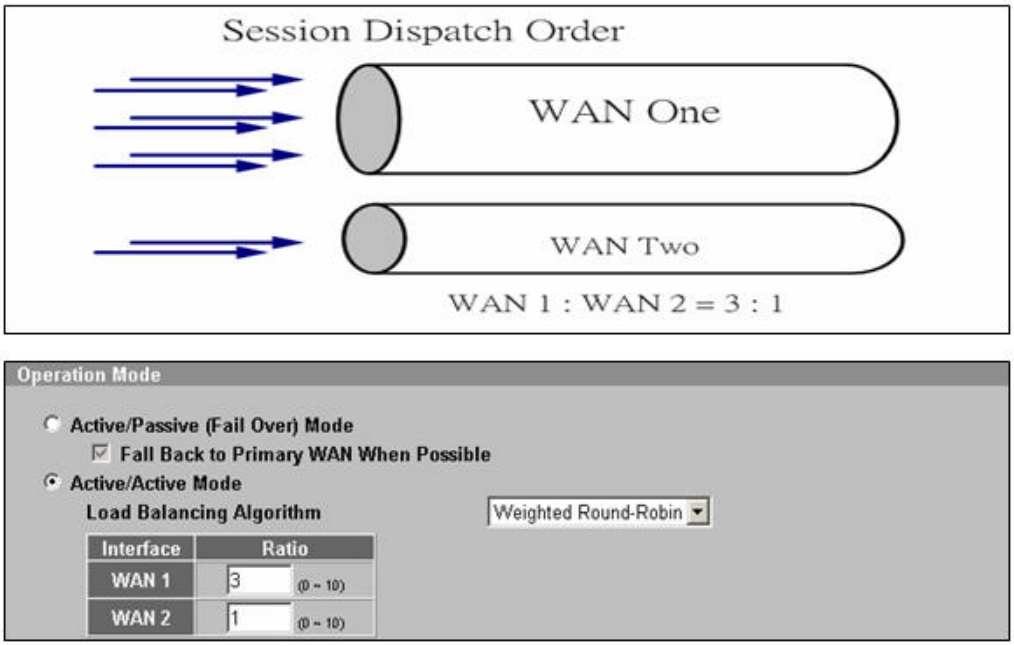
- Spillover (Алгоритъм за препълване) (вж. фигура 27)
  - Определя се пределно ниво за натоварване на основния WAN порт. При достигане на това натоварване за период (10~600 секунди) започва използването на втория WAN port за всички нови сесии. Когато натоварването на основния канал намалее, новите сесии се прехвърлят обратно на него.

Пример:



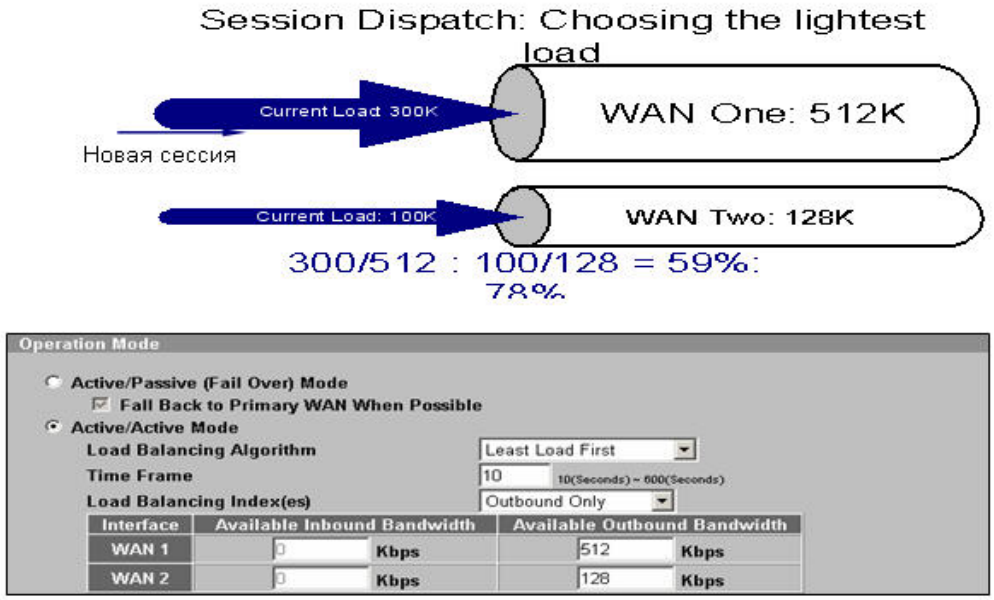
Фигура 27. Алгоритъм за препълване

- Weighted Round Robin (Циклично претеглен алгоритъм)
  - Определя се коефициент на натоварване на двата канала. Спрямо това се определя и съотношението на количеството сесии, които ще преминат през даден канал. Например, WAN1:WAN2=3:1. Това означава, че количеството открити сесии през портове WAN1 и WAN2 ще бъде кратно на 3:1. При този метод реалното натоварване на каналите не се взема предвид (вж. фигура 28).



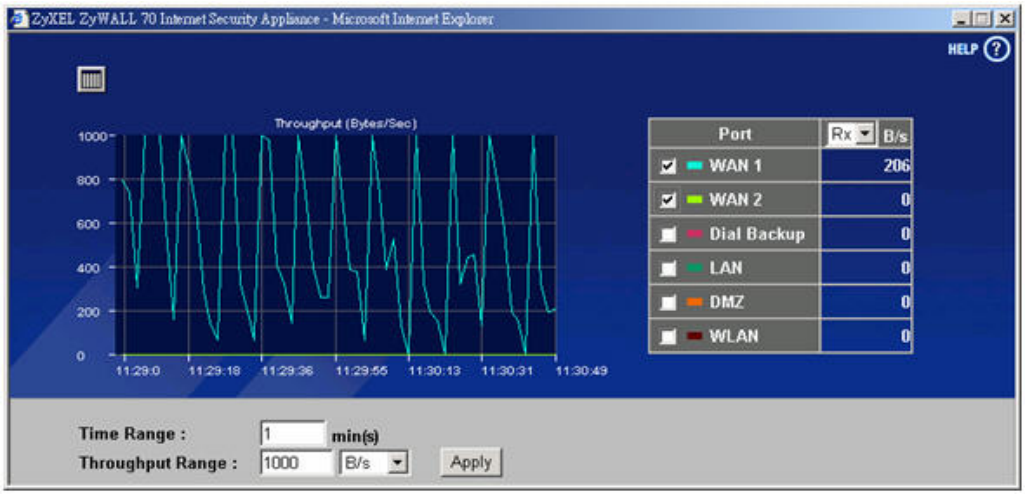
Фигура 28. Циклично претеглен алгоритъм

- Least Load First (Правило на ненатоварения порт)
  - Устройството определя натоварването на изходящия поток, входящия и изходящия такъв или входящия в определен момент от време, и по този начин използва различните канали в съответствие с пределната им пропускателна способност. Нова сесия се стартира през по малко натоварения канал (вж. фигура 29).



Фигура 29. Правило на ненатоварения порт

Чрез Web-интерфейса на устройството, в меню Home – Show Statistic може да се проследи в реално време натоварването на всеки канал. Потребителят може да избира интерфейс и направлението на потока от данни за всяка графика (вж. фигура 30).



Фигура 30. Изглед на статистика

3.4. Симулиране на разпределяне на трафика с програмен продукт GNS3

За демонстриране на практическо решение за изграждане на компютърна мрежа с опция разпределяне на трафика между два интернет доставчика и отказ от услуга, ще бъде използван програмен продукт GNS3.

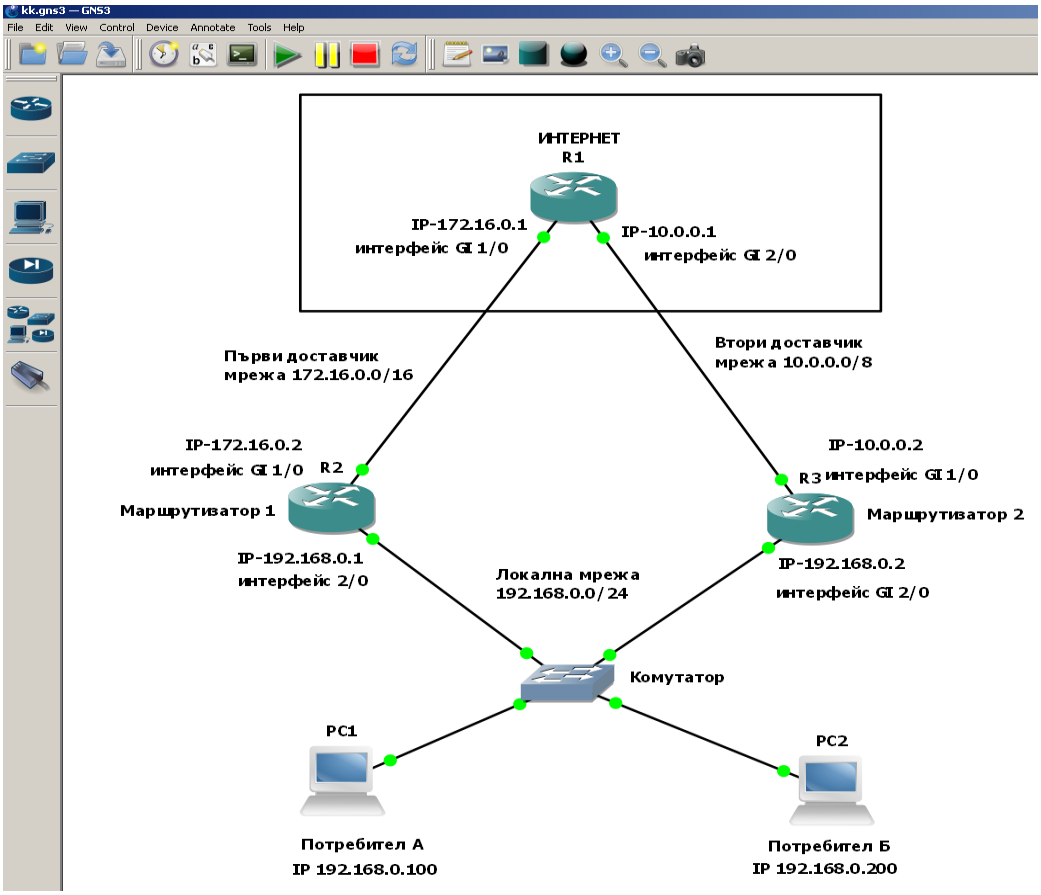
Проектираната мрежа ще се състои от Сиско маршрутизатори, серия C7200. Техните интерфейси ще бъдат конфигурирани, след което ще бъде пуснат поддържания от тях протокол за балансиране на натоварването GLBP.

Натоварването ще се симулира посредством изпращане на ICMP пакети с голям размер към интерфейса, свързан към един от интернет доставчиците.

Отказ от услуга ще бъде демонстриран, чрез прекъсване на връзката до интерфейса на маршрутизатора, свързан към един от интернет доставчиците.

За целите на симулацията ще ползваме частни интернет протокол мрежи.

3.4.1. Схема на компютърната мрежа.



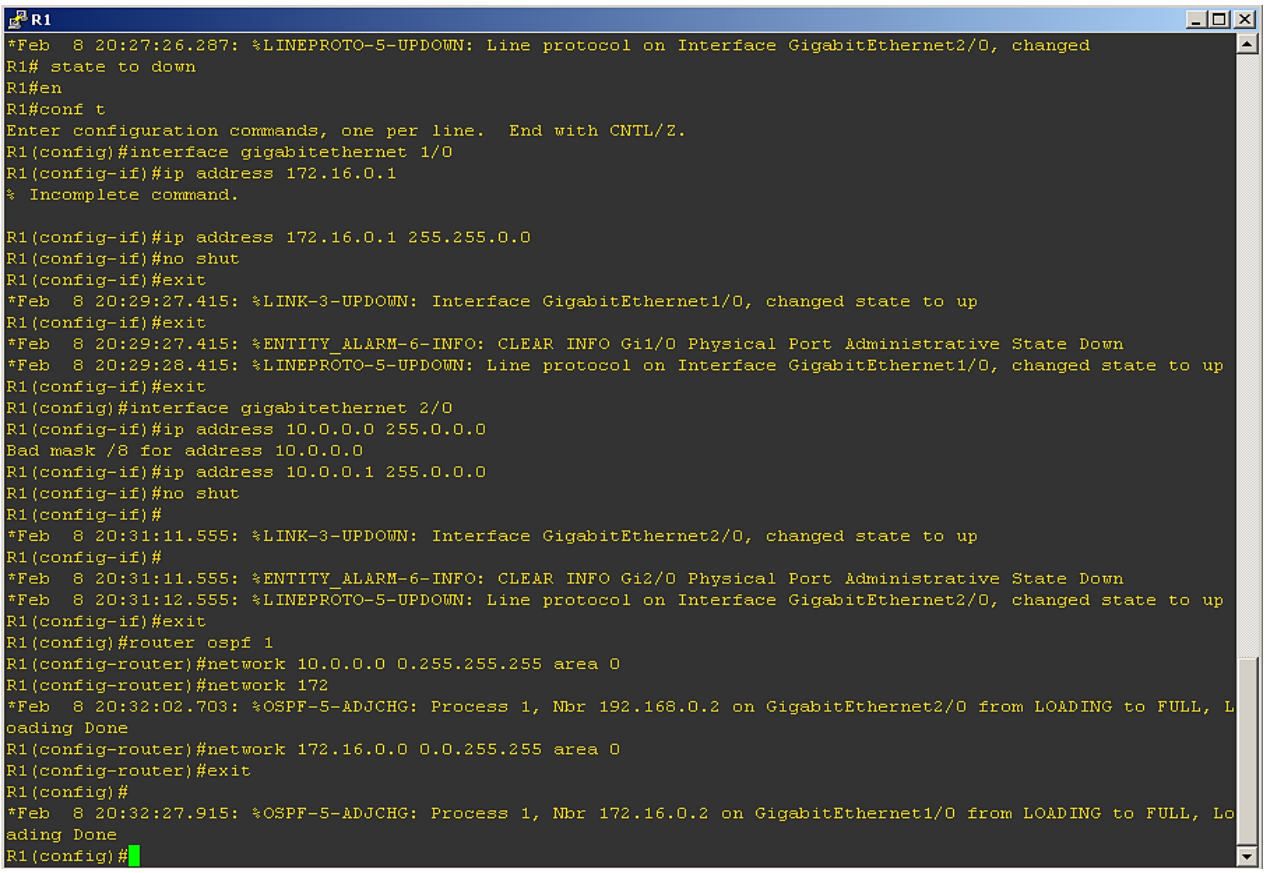
Фигура 31. Модел на компютърната мрежа

Ще предположим, че доставчик номер едно ни е дал статичен ИП адрес 172.16.0.2/16, а доставчик номер две ИП адрес 10.0.0.2/8. Нашата локална мрежа ще е конфигурирана в обхвата на ИП мрежовото пространство 192.168.0.0/24.

3.4.2. Конфигуриране на мрежовите устройства

3.4.2.1. Конфигуриране на маршрутизатор R1

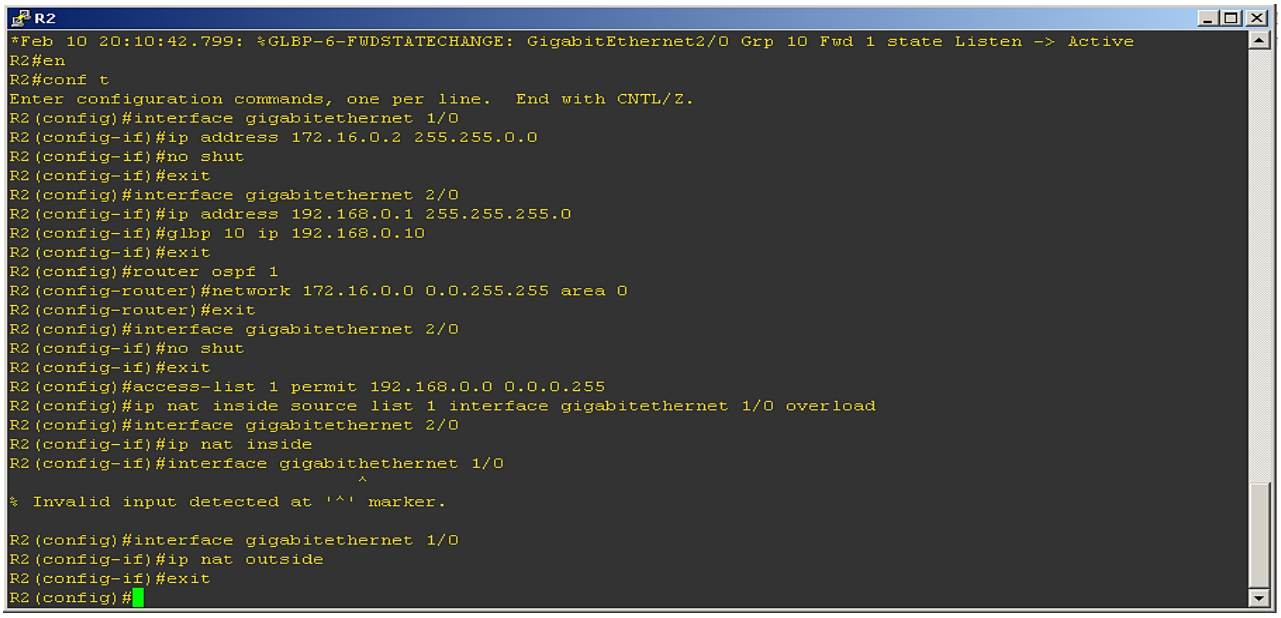
Конфигурираме интерфейсите, със съответните ИП, съгласно схемата и стартираме мрежови протокол OSPF, който ще маршрутизира пакетите между двете мрежи/двата интерфейса (вж. фигура 32).



Фигура 32. Конфигуриране на маршрутизатор R1

3.4.2.2. Конфигуриране на маршрутизатор R2

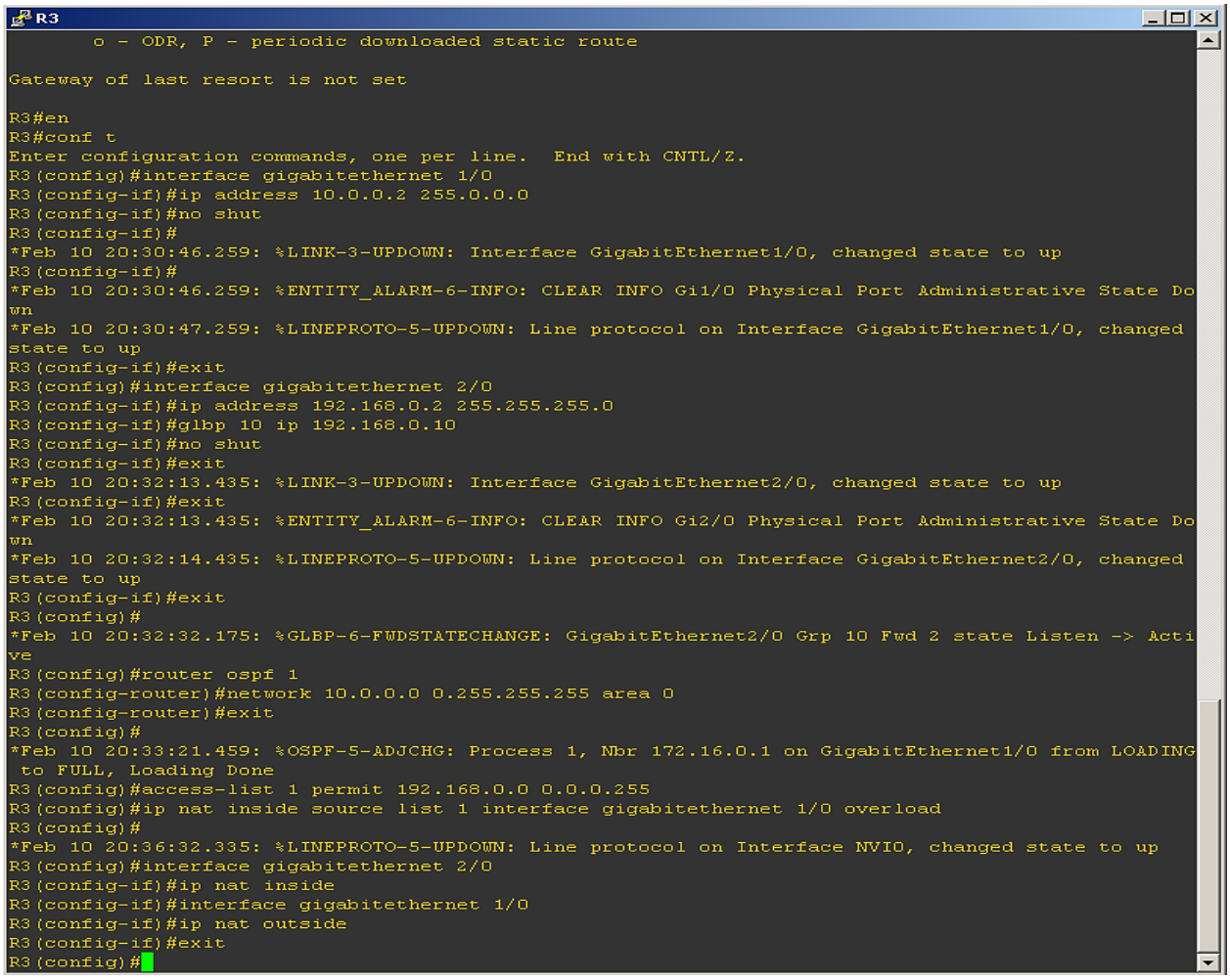
Конфигурираме интерфейсите със съответните ИП адреси. На интерфейса към мрежа 172.16.0.0/16 конфигурираме мрежови протокол OSPF. На интерфейс GI 2/0, свързан към вътрешната ни мрежа, пускаме протокол на Сиско за разпределяне на трафика – GLBP. Тъй като имаме предвид, че вътрешната ни мрежа ще ползва частни ИП адреси, на маршрутизатора ще бъде конфигуриран NAT (вж. фигура 33).



Фигура 33. Конфигуриране на маршрутизатор R2

3.4.2.3. Конфигуриране на маршрутизатор R3

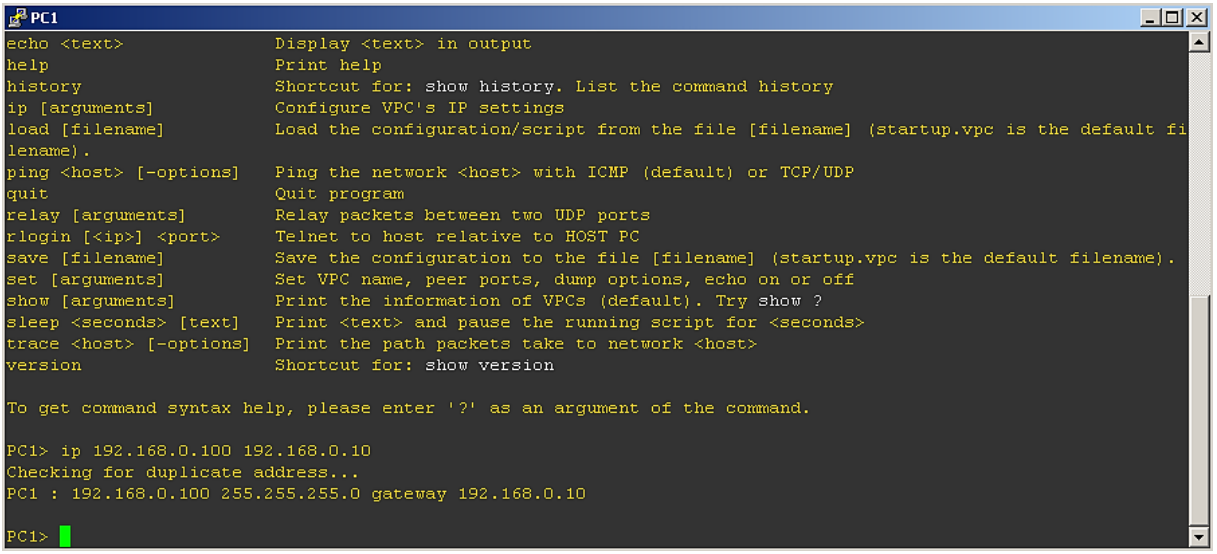
Маршрутизатор R3 ще бъде конфигуриран със съответните ИП адреси, съгласно схемата, в същата последователност както маршрутизатор R2.



Фигура 34. Конфигуриране на маршрутизатор R3

3.4.2.4. Конфигуриране на компютъра на Потребител А – PC1

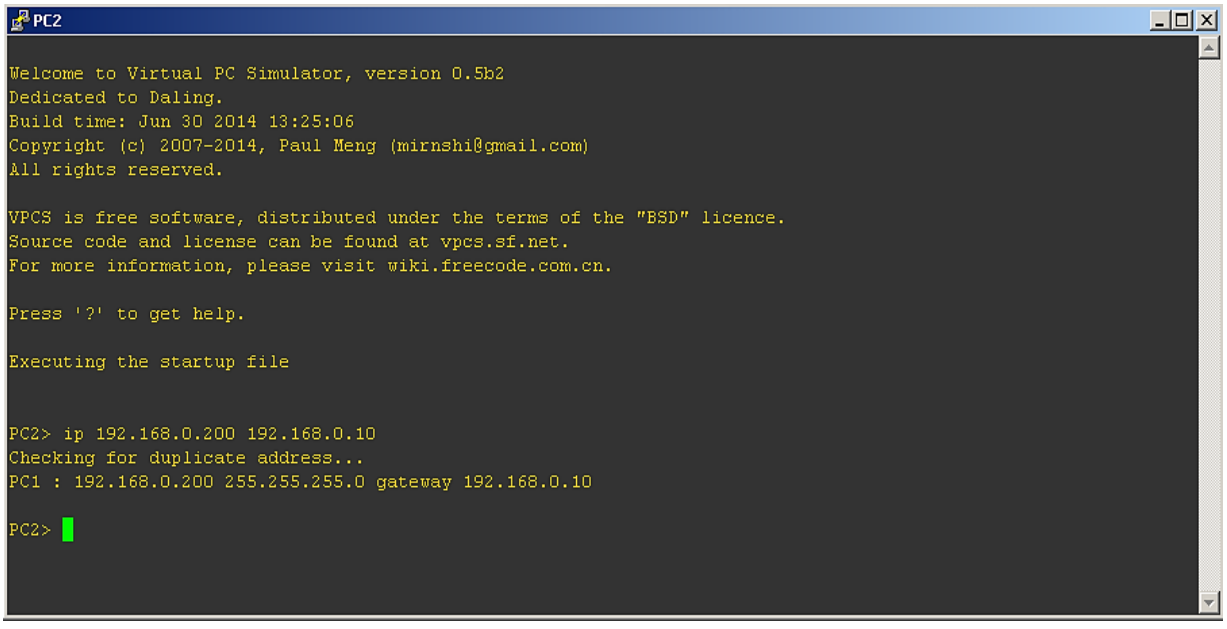
Компютърът на потребител А ще бъде конфигуриран с ИП адрес 192.168.0.100/24 и шлюз с ИП адрес 192.168.0.10 (вж. фигура 35).



Фигура 35. Конфигуриране на PC1

3.4.2.5. Конфигуриране на компютъра на Потребител Б – PC2

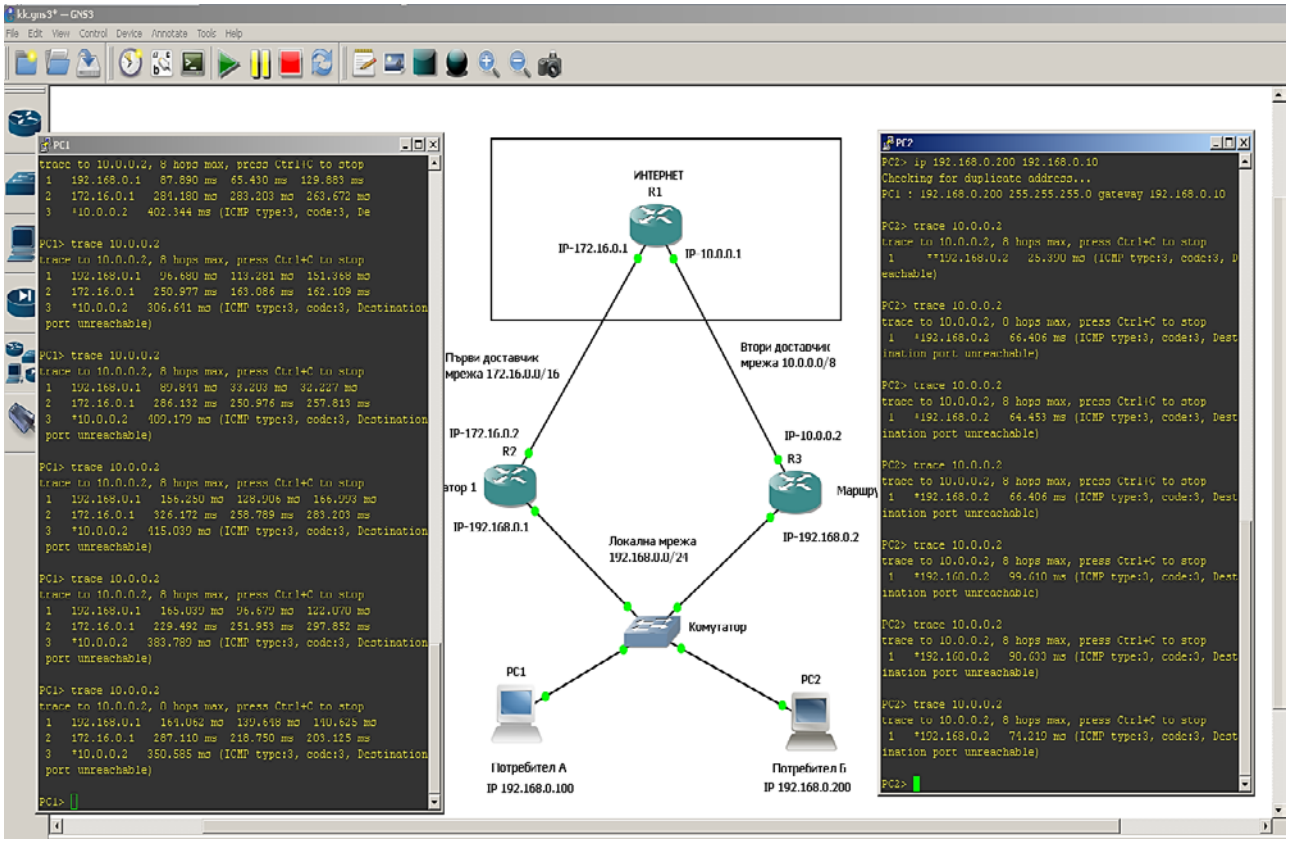
Компютърът на потребител А ще бъде конфигуриран с ИП адрес 192.168.0.200/24 и шлюз с ИП адрес 192.168.0.10 (вж. фигура 36).



Фигура 36. Конфигуриране на PC2

3.4.3. Проверка на свързаност и работа на протоколите.

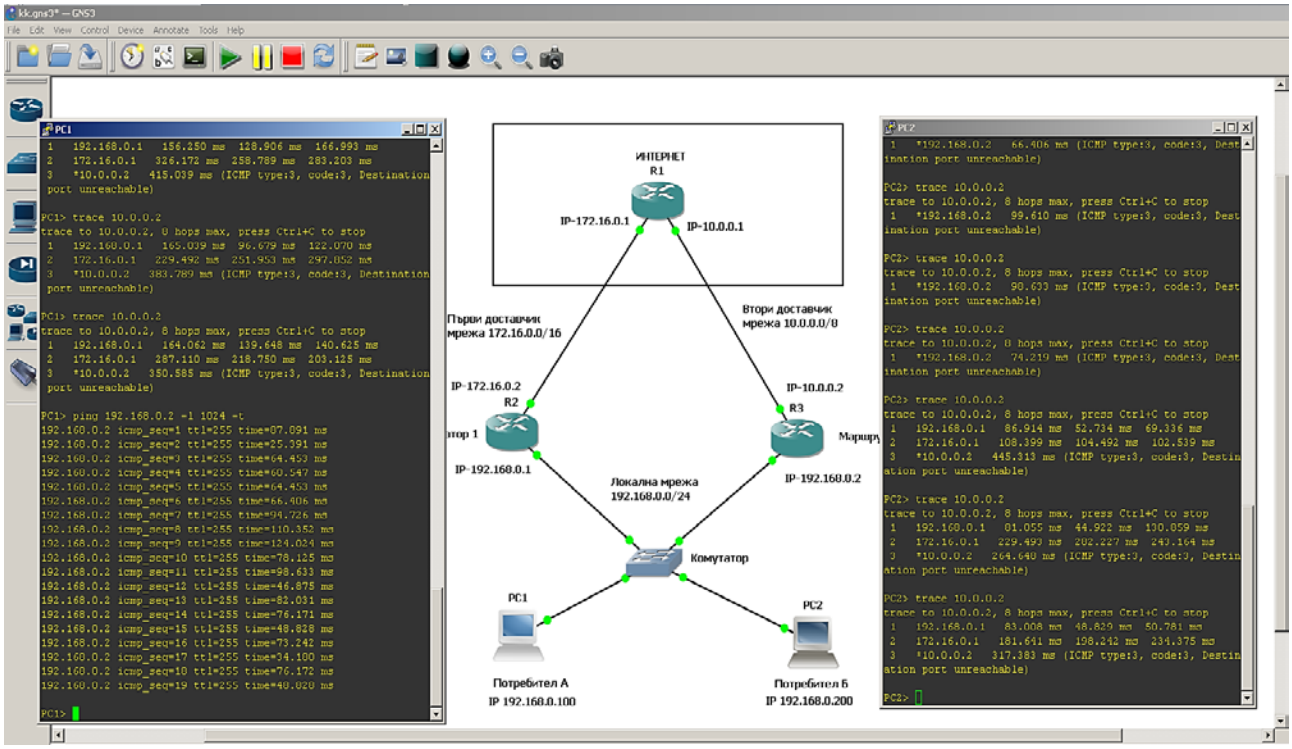
Както виждаме на фигура 37, трафикът на двамата потребители е разделен, като всеки от тях ползва различен шлюз/интернет доставчик, за достигане на една и съща цел – ИП адрес 10.0.0.2. Трафикът на Потребител А минава през порта на маршрутизатор R2 с ИП адрес 192.168.0.1, а трафикът на потребител Б през порта на маршрутизатор R3 с ИП адрес 192.168.0.2.



Фигура 37. Проверка на свързаност

3.4.4. Симулация на разпределяне на трафика, при натоварване на един от доставчиците.

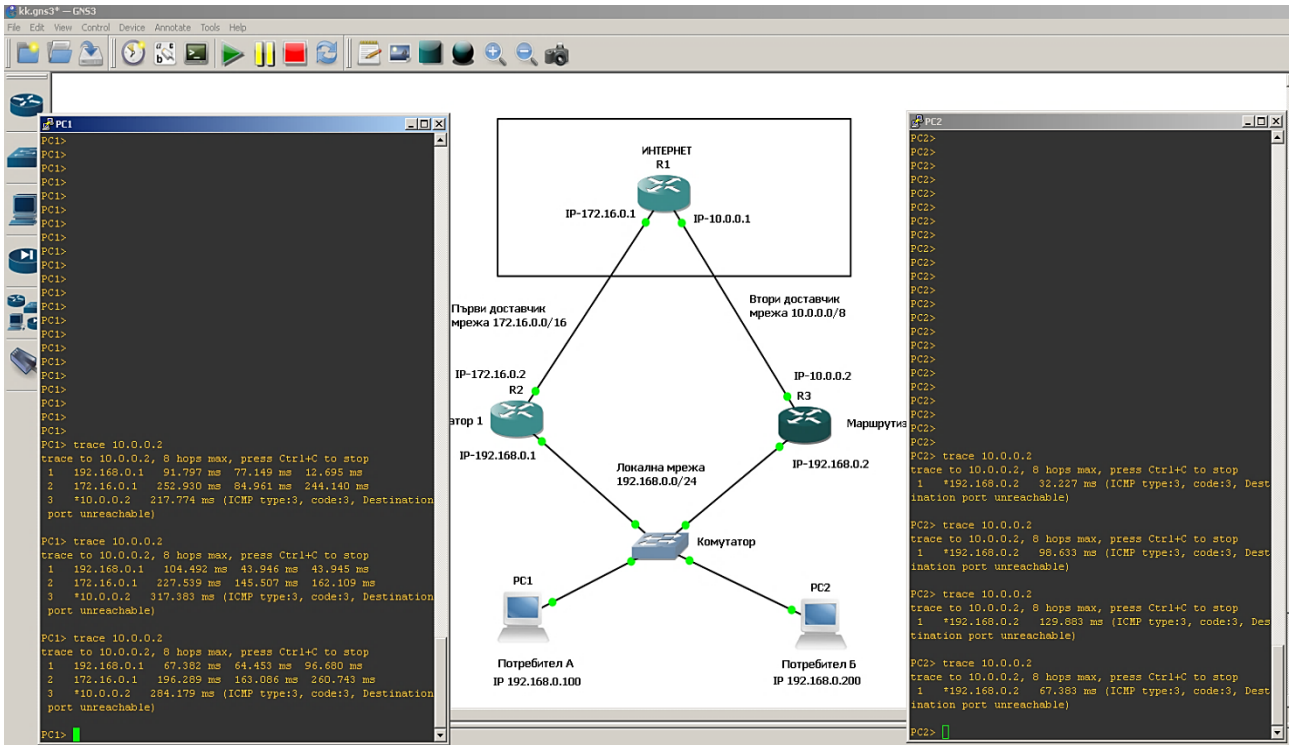
На фигура 38 е показано, че Потребител Б – PC2 достига ИП адрес 10.0.0.2 през маршрутизатор R3. След натоварване на вътрешния интерфейс на маршрутизатор R3, посредством команда ping и изпращане на ICMP пакети с големина 1024 байта, виждаме, че трафикът на Потребител Б-PC2 сменя шлюза и започва да комуникира през ненатоварения маршрутизатор R2.



Фигура 38. Разпределяне на трафика

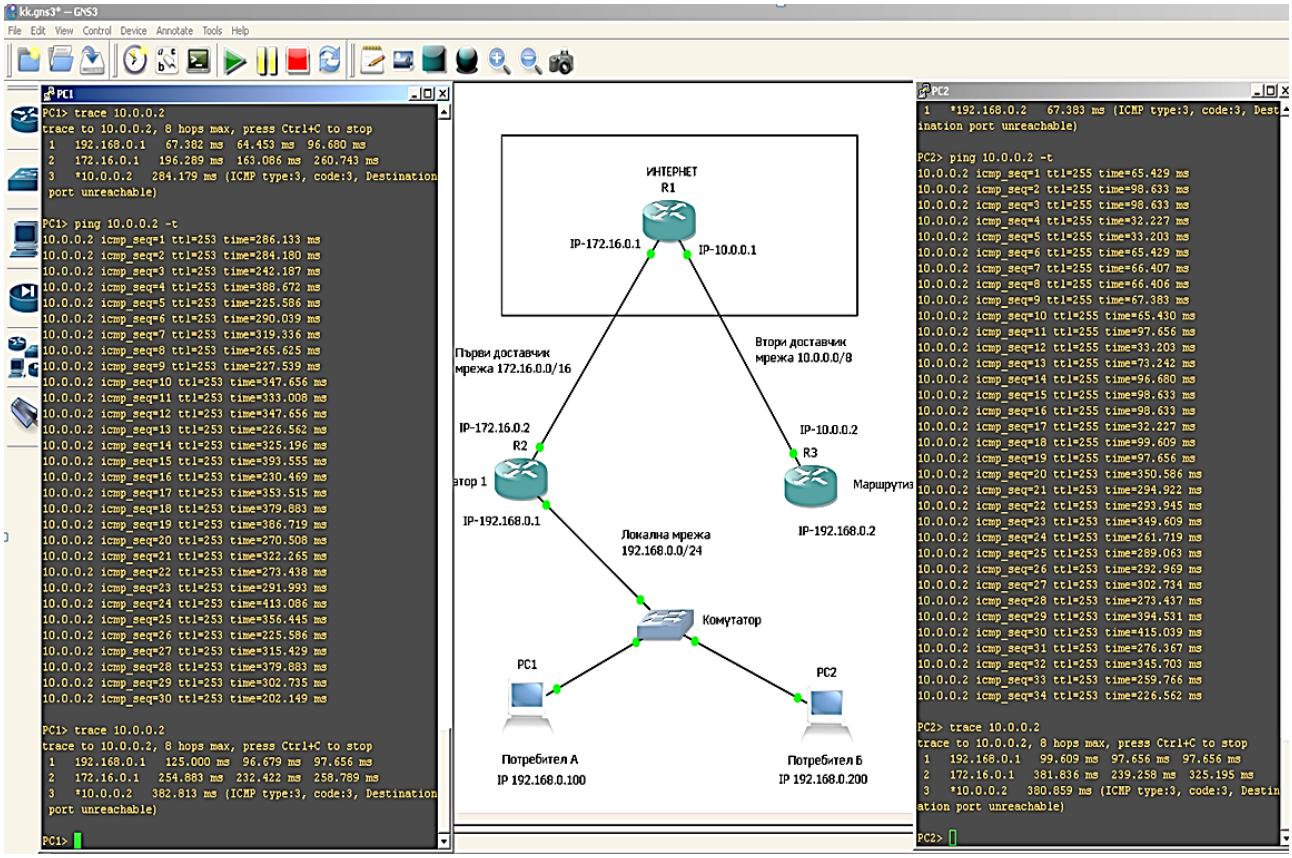
3.4.5. Симулация на отказ от услуга.

На фигура 39 е показано, че трафикът на потребителите е разделен между двата доставчика. Всеки един от тях ползва различен интернет доставчик. Потребител А ползва доставчика през маршрутизатор R2, а потребител Б доставчика през маршрутизатор R3.



Фигура 39. Симулация на отказ от услуга

След прекъсване на връзката между маршрутизатор R3 и комутатора, Потребител Б – PC2, веднага прехвърля своят трафик през маршрутизатор R2.



Фигура 40. Симулация на отказ от услуга.

ЗАКЛЮЧЕНИЕ

Поставените в увода на магистърската теза задаачи са решение както следва:

- В първа глава са разгледани някои от основните понятия за осъществяване на мрежова комуникация. Изяснена е сложността на предаването и получаването на информация посредством компютърни мрежи. Показани са теоретичните модели, описващи принципния начин на комуникация и строежа на компютърните мрежи. Обяснени са основните мрежови протоколи и принципите при установяване на комуникационна сесия.
- Във втора глава са разгледани и анализирани методи, протоколи и средства – софтуерни и хардуерни, приложими към проблема за рапределяне на трафика и отказ от услуга. Методите са разделени на две – статични и динамични и са обяснени принципите по които работят. Разгледани са различни мрежови протоколи. Подробно е описано конфигурирането и работата на протокол за разпределяне на трафика GLBP (Gateway Load Balancing Protocol) - решение на фирмата Сиско за балансиране на мрежовия трафика. Показани са софтуерни варианти тип защитни стени, посредством които може да бъде разпределян трафика на базата на различни политики. Разгледани са хардуерни устройства на различни фирми с два WAN порта, създадени за балансиране на трафика/натоварването.
- В трета глава е изградена работна установка и са реализирани няколко практически решения на проблема за разпределняне на мрежовия трафик и отказ от услуга. Подробно е обяснено конфигурирането на маршрутизатор Микротик, защитна стена pfsence и хардуерно устройство, предназначено за разпределяне на трафика между два WAN порта – ZyXELL. Чрез използването на софтуер за симулиране на мрежови трафик GNS3 е проектирана компютърна мрежаконфигуриран протокол Сиско GLBP (Gateway Loadbalancing Protocol) и е направена

демонстрация на работата му по разпределяне на трафика между два интернет доставчика и при отказ от услуга на един от тях.

От всичко казано по-горе считам, че целта на магистърската теза е постигната успешно.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. Kopparapu, C. „Load Balancing Servers, Firewalls, and Caches”, 2002, ISBN 0-471-41550-2;
2. Йорданова, Н. Електронен курс „Компютърни мрежи“, 2008 <http://193.192.57.240/po/courses/problemni/komputarni%20mrezi/start.html>
3. Уикипедия, Статия Media Access control <https://en.wikipedia.org/wiki/Media_access_control>
4. Уикипедия, Статия Address Resolution Protocol https://bg.wikipedia.org/wiki/Address_Resolution_Protocol
5. Уикипедия, Статия Stream Control Transmission Protocol <https://en.wikipedia.org/wiki/Stream_Control_Transmission_Protocol>
6. Дудин,Ф. Уроци по комуникации <http://pchelp.cablebg.net/Tutorials/Communications/DNS.htm>
7. Postel,J Reynolds,J. Internet Standard <https://tools.ietf.org/html/rfc959>
8. Уикипедия, Статия SSH <https://bg.wikipedia.org/wiki/SSH>
9. Уикипедия, Статия HTTP <https://bg.wikipedia.org/wiki/HTTP>
10. Belshe,M. Proposed Standard <https://tools.ietf.org/html/rfc7540>
11. Уикипедия, Статия SMTP <https://bg.wikipedia.org/wiki/SMTP>
12. Уикипедия, Статия Post Office Protocol <https://bg.wikipedia.org/wiki/Post_Office_Protocol>
13. Уикипедия, Статия IMAP <https://bg.wikipedia.org/wiki/IMAP>
14. Уикипедия, Статия SSL <https://bg.wikipedia.org/wiki/SSL>
15. Cisco Systems, Inc First Hop Redundancy Protocols Configuration Guide, Cisco IOS XE Release 3S, 2012 <http://www.cisco.com>
16. Димитров, П. Разпределение на трафика, София, MUM България, 2014 <http://mum.mikrotik.com/presentations/BG14/pdimitrov.pdf>
17. NativePC, Статия, „Балансировка нагрузки, приоритезация траффика (QoS), отказоустойчивость в pfSense 2.0“ <http://shop.nativepc.ru/content/94--pfsense-load-balance->

18. ZyXEL Communications Corp, Статия „Функция балансировки нагрузки (Load Balancing) между двумя WAN-портами на ZyWALL” http://zyxel.ru/kb/1443

СПИСЪК НА ФИГУРИТЕ В ТЕКСТА

СПИСЪК НА ТАБЛИЦИТЕ В ТЕКСТА

ПРИЛОЖЕНИЕ 1 – ЕКСПОРТ НА МАРШРУТИЗАТОР R1

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
boot-start-marker
boot-end-marker
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip tcp synwait-time 5
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface GigabitEthernet1/0
 ip address 172.16.0.1 255.255.0.0
 negotiation auto
interface GigabitEthernet2/0
 ip address 10.0.0.1 255.0.0.0
 negotiation auto
```

```
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 0
 network 172.16.0.0 0.0.255.255 area 0
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
end
```

ПРИЛОЖЕНИЕ 2 – ЕКСПОРТ НА МАРШРУТИЗАТОР R2

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R2
boot-start-marker
boot-end-marker
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip tcp synwait-time 5
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface GigabitEthernet1/0
 ip address 172.16.0.2 255.255.0.0
 ip nat outside
 ip virtual-reassembly
 negotiation auto
interface GigabitEthernet2/0
 ip address 192.168.0.1 255.255.255.0
```

```
 ip nat inside
 ip virtual-reassembly
 negotiation auto
 glbp 10 ip 192.168.0.10
router ospf 1
 log-adjacency-changes
 network 172.16.0.0 0.0.255.255 area 0
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1/0 172.16.0.1
no ip http server
no ip http secure-server
ip nat inside source list 1 interface GigabitEthernet1/0 overload
access-list 1 permit 192.168.0.0 0.0.0.255
no cdp log mismatch duplex
control-plane
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
end
```

ПРИЛОЖЕНИЕ 3 – ЕКСПОРТ НА МАРШРУТИЗАТОР R3

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
ip cef
no ip domain lookup
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
```

```
 duplex auto
 speed auto
!
interface GigabitEthernet1/0
 ip address 10.0.0.2 255.0.0.0
 ip nat outside
 ip virtual-reassembly
 negotiation auto
!
interface GigabitEthernet2/0
 ip address 192.168.0.2 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 negotiation auto
 glbp 10 ip 192.168.0.10
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 0
!
!
no ip http server
no ip http secure-server
!
ip nat inside source list 1 interface GigabitEthernet1/0 overload
!
access-list 1 permit 192.168.0.0 0.0.0.255
no cdp log mismatch duplex
!
control-plane
```

```
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

ПРИЛОЖЕНИЕ 4 – КОМПАКТ ДИСК

На компакт дискът е записан файл, съдържащ проектираната и показана в Глава 3 мрежова конструкция, посредством която е направена демонстрация на разпределяне на трафика и отказ от услуга, изготвена с помощта на програмата за мрежови симулации GNS3.