Нов български университет

Технология за многопротоколно етикетно комутиране (MPLS)

Доц. Д-р Емил Стоилов

Департамент по Информатика на НБУ

София, юни 2012

Съдържание

1. Основни изисквания към услугите, предлагани от съвременните мрежи

С бързото развитие на информационните технологии и Интернет, значително се увеличи вида и количеството генериран трафик от различни мрежови услуги. Заедно с предаването на файлова FTP (File Transfer Protocol), Електронната поща (E-mail), WWW и други традиционни услуги като Електронно правителство (E-government), Онлайн банкиране (Online Banking), Системите за управление на фирмени ресурси (Enterprise Resourse Planning – ERP systems) и Системите за управление на връзките с клиенти (Customer Relationship Management – CRM systems), се появиха и други онлайн услуги, включително предаване на видео, IP телефония и онлайн обучение. Тези услуги предполагат присъствието на IP мрежа като преносна среда. Те поставят от своя страна и високи изисквания към тази мрежа.

От съществено значение за един добър мрежови проект е наличието в него на услуги с висока производителност, с високо качество, с високо ниво на сигурност, с висока надеждност, както и тези услуги да могат да бъдат управлявани и оптимизирани [1].

1.1 Висока производителност на услугите (High Performance of Services)

За да се постигне това е необходимо при проектирането на ядрото на мрежата да се разглеждат равнопоставено услугите, които тя предлага, и необходимата производителност за реализирането на тези услуги. Това означава, че когато проектираме съвременна мрежа, тя трябва да предлага голям брой нови услуги като Виртуални частни мрежи (Virtual Private Networks – VPN), IP телефонни услуги, IP видео услуги и т.н. За да се покрият нуждите на тези услуги обаче, IP-ядрото на мрежата трябва да работи с максималната възможна скорост. За щастие с въвеждането в търговска употреба на 10 Gbps мрежовите процесори и ASIC технологии, ядрото на една IP мрежа, изградено с използване на новата генерация маршрутизатори и комутатори, има вече такава висока скорост. Голяма част от него е реализирана хардуерно, и това се прави не само за постигане на скорост, но и поради изискванията за по-голяма сигурност и защита на потребителите.

1.2 Високо качество на услугите (High Quality of Services)

По отношение на качеството, различните услуги имат различни изисквания към някои ключови параметри, като например честотна лента (bandwidth), забавяне (delay), трептене (jitter) и брой загубени пакети. Например IP телефонията и видео конферентните връзки са чувствителни към забавяне (<150ms) и трептене (<10ms). Услугите за предаване на данни не са чувствителни на закъснения, но те са с повишени изисквания към надеждността на преносната среда.

Традиционната IP мрежа просто извършва различни услуги без да гарантира тяхното качество. За да се гарантира качеството за някоя важна услуга, като например видео трафик, се изгражда временна мрежа (hoc network). Висококачествената интелигентна IP мрежа поставя високи изисквания към ядрото. Не става въпрос за прост контрол на достъпа, тук имаме нужда от динамично разпределение на ресурсите (процесора, паметта, буферите и допълнителния хардуер в мрежовите възли).

Ядрото на IP мрежата трябва да осигури честотна лента за всеки вид услуга. Например да осигури 384K честотна лента от край до край за видео услуга, 25K честотна лента от край до край за пренос на глас и 8M честотна лента за пренос на данни. Ресурсите за ключови услуги трябва да бъдат гарантирани в случай на недостатъчна честотна лента или възникване на мрежова аномалия.

Освен това мрежата е подложена на постоянни промени. Непрекъснато се изменя трафикът и се добавят нови услуги. Това налага ядрото на мрежата да може да бъде настройвано динамично. Проектирането на такова ядро се постига с интегриране на различни технологии. Например технологиите MPLS и VPN е желателно да бъдат комбинирани.

1.3 Висока сигурност на услугите (High security of services)

Сигурността на ядрото определя сигурността на услугите, особено тази на трафика. Тук различните услуги трябва да бъдат безопасно разделени. Всяка една услуга трябва да се разпространява в своя собствена логическа мрежа, така че да се избегне влиянието помежду им. Комбинирането на MPLS, VPN, VLAN и други технологии може да увеличи физическата независимост, като всеки тип услуга получи за използване част от мрежовите ресурси, такива като адреси, тунели, маршрутни таблици. Граничният възел на ядрото би трябвало автоматично да идентифицира услугата и да я насочи в различна VPN.

Едновременно с безопасното разделяне, може да се използва и технология за защита в самия тунел, така че за всякакъв незаконен трафик или атаки от типа DoS да се отказва достъп до защитен подтунелен ресурс. За някои ключови услуги ядрото може да гарантира сигурност подобна на гарантираната от ATM PVC.

Въпреки това е невъзможно да се гарантира сигурността на всякаква технология в мрежата. Вместо това трябва да се стараем стратегията за сигурност да бъде винаги в съответствие със състоянието на различните елементи, спазвайки временна и пространствена йерархия, т.е. необходима ни е динамична система за защита на ядрото. Тази система се изгражда от граничните възли заедно с управляващата система, и трябва да ни предпазва от вируси и от нежелан достъп. При това управляващата система динамично обновява таблиците за защита от вируси и неавторизиран достъп, а защитата в реално време се извършва от граничните на ядрото възли.

1.4 Висока надеждност на услугите (High reliability of services)

Надеждността на мрежовата услуга зависи от надеждността на IP ядрото. С увеличението на основните мрежови услуги на ядрото се увеличава и важността на мрежовата надеждност.

Висококачественото ядро е надеждно от край до край. Неговата надеждност се осигурява на три нива: обслужване, мрежа и устройства.

На ниво обслужване трябва да се гарантира, че обслужването няма да бъде прекъсвано по време на целия цикъл. Цикълът включва всички процеси на поддръжка на мрежата, нейното обновяване, разширяване и оптимизация.

На ниво мрежа ядрото трябва да бъде в състояние да възстанови прекъснатите връзки за по-малко от 50 ms. Използваните технологии като Resilent Packet Ring (RPR), Ethernet Automatic Protection Switching (EAPS), Link Aggregation позволяват да се постигне това. С използването на функцията IP/MPLS fast rerouting също може да се постигне възстановяването на мрежови маршрути и тунели за 50 ms.

На ниво устройства, за изграждането на ядрото трябва да бъдат използвани устройства от най-надеждния клас. В тях ключовите елементи като основния процесор, интерфейсните модули, захранването и вентилаторите са дублирани. В същото време някои функции, като обновяване например, са реализирани софтуерно, за да не се прекъсне услугата в определен момент, когато се актуализира софтуер или се добавят нови функции. Цялата система на IP ядрото трябва да има надеждност 99.999% и в него да се използват непрекъсваеми превключващи технологии.

1.5 Услуги за управление и оптимизация (Management and optimization services)

Управлението винаги е било най-слабата част на една IP мрежа. Това е проблем, който едно висококачествено ядро трябва да реши. Услугите за управление включват управлението на VPN, управлението на QoS и управление на сигурността. Управлението на VPN разделя физическата мрежа на логически мрежи и може да предостави мрежови ресурси на всяка една логическа мрежа поотделно. Управлението на QoS работи заедно с VPN за да гарантира необходимата надеждност на услугата от край до край. Управлението на сигурността основно включва управлението на достъпа на потребителите. То може лесно да бъде експлоатирано и оптимизирано, тъй като ресурсите могат лесно да бъдат настройвани и коригирани.

Ядрото трябва да позволява преминаването на IPv4 и IPv6 трафик едновременно. Бързото развитие на потребителските услуги даде тласък на развитието на IPv6 технологията и ядрата от следващите поколения ще се базират само върху IPv6. Въпреки това преходът от IPv4 към IPv6 ще продължи няколко години, следователно засега трябва да се позволява преминаването както на IPv6, така и на IPv4 трафик. Поради тази причина ние предявяваме изисквания към устройствата да поддържат и двата вида трафик, както и различни други технологии на предаване.

Решенията за преминаване от IPV4 към IPv6 се базират на три основни компонента: маршрутизиране и комутиране в мрежата, логиката на работа на мрежата и платформата за управление на услугите. Разработената стратегия покрива изцяло петте изисквания за високо качество на ядрото и предлага удобен преход към ядро с IPv6.

Краткото описание тук на основните изисквания към услугите предлагани от съвременните мрежи не е самоцелно. Идеологията на една нова технология по-лесно се възприема, ако в процеса на нейното представяне виждаме отчетливо какво ново тя ни дава, а също така и изпълнява ли всички изисквания предявявани към мрежата. Защото понякога новите технологии подобряват някои параметри, но за сметка на това драстично влошават други.

2. Защо да използваме MPLS технология?

Архитектурата на многопротоколното етикетно комутиране (Multiprotocol Label Switching – MPLS), така както е представена в [2], съчетава ползите от два различни подхода -

хардуерното комутиране на пакети в ATM и комутирането на пакети в мрежовия слой използвано при IP. Тази архитектура отделя контролната информация необходима за препредаване на пакетите в мрежата от данните. При традиционното IP маршрутизиране, когато пакетът се изпраща от един маршрутизатор към друг, всеки маршрутизатор независимо избира следващия скок за даден пакет, като анализира заглавната част на пакета наречена хедър (header) и използва някакъв маршрутизиращ алгоритъм. Хедърите обикновено съдържат много повече информация, отколкото е необходимо да се избере следващия скок. Можем да разглеждаме избора на следващ скок като съставен от две отделни функции. Първата функция разделя цялото множество от възможни пакети на еквивалентни за препредаване класове (Forward Equivalence Classes – FEC). Задачата на втората функция е да определи за всеки клас следващия маршрутизатор (скок). От тази гледна точка всички пакети, които принадлежат на един FEC са неразличими, т.е. те ще бъдат препредавани по един и същи път.

Ето защо при технологията MPLS задачата за определяне на FEC се решава само веднъж, на входа на MPLS мрежата. Решението зависи както от дестинациите на пакетите, така и от местоположението на входящия етикетно комутиращ маршрутизатор. Маршрутизаторите, които се намират на границата на ядрото на MPLS мрежата наричаме гранични етикетно комутиращи маршрутизатори (Label Edge Router – LER). Маршрутизаторите които се намират вътре в ядрото и не са на границата му, се наричат етикетно комутиращи маршрутизатори (Label Switching Router – LSR). Следователно това решение се взима от входящия LER и естествено е въз основа на анализ на информацията в мрежовия хедър на пакета. Класът, към който даден пакет се присъединява, се кодира като фиксирана стойност наречена етикет (label). В мрежата MPLS, когато пакетът се препредава от един маршрутизатор към друг, етикетът се изпраща заедно с него, т.е. пакетите са етикетирани преди да се изпратят.

При този възприет подход на препредаване на пакетите в MPLS, пакетът еднократно се присъединява към даден клас, като в следващите маршрутизатори не се извършва никакъв анализ на мрежови хедъри. Препредаването по-нататък се определя от етикетите. Това има значителни предимства пред традиционния начин на маршрутизиране.

Следователно FEC може да се разглежда като група от IP дестинации, към които предаването на пакетите се извършва по един и същи начин и за които е определен един общ идентификатор с фиксирана дължина, т.е. етикет. Пътят, съответстващ на всеки FEC, между входните и изходните LER се нарича етикетно комутируем път (Label Switched Path – LSP). Етикетът се прикачва към пакета или чрез маркиране (tagging) на съществуващо поле на хедъра на пакета или чрез добавяне на ново поле. Етикетът е основен елемент за определяне на пътя през всички маршрутизатори и комутатори в един MPLS домейн. Той се използва в тях като индекс в таблица за определяне на следващ скок и нов етикет. Старият етикет се заменя с нов такъв и пакетът се изпраща на следващия маршрутизатор. По дефиниция LSP е еднопосочен, т.е. необходими са два LSP за да се поддържа двупосочен трафик.

Преди да започнем с описанието на елементите, да представим накратко какви предимства би ни дал такъв подход. Основно те са следните [2], [3]:

- MPLS дава възможност за транспорт на пакети по произволни пътища в големи мрежи, с много възли, като осигурява специфична услуга за комутиране на вериги.

- За мрежи в които не се използва IP, например такива като ATM или Frame Relay, тази технология ни позволява да използваме добре познатите механизми за управление като маршрутизация (routing), избор на път (path selection), резервиране (reservation) и други, вместо технологично специфични управляващи протоколи (например PNNI). По този начин MPLS ни дава една обща архитектура за управление на потока, при използване на различен маршрутизиращ или комутиращ хардуер, както с установяване, така и без установяване на връзки.

- В тази технология се използва механизъм за групиране на пакети чрез използване на етикети, като по този начин се осъществява изолиране на една група пакети от друга. Така LSP може да бъде така настроен, че да се осигури обща тунелираща услуга, като например:
  - свързване на сегменти на една частна виртуална мрежа (Private Virtual Network – VPN) чрез публична мрежа,
  - свързване на две мрежи в които не се използва IP (без да прибягваме до услугите на L2TP),
  - използване на общи правила за препращане на пакети с един и същи етикет, т.е организиране на класове от услуги

- LSP могат да бъдат съединявани, като се образуват изключително дълги вериги. LSP могат да свързват една входна точка с много изходни точки, което ни дава възможност за групово предаване (multicasting). LSP могат също да свързват много входни точки с една изходна точка, т.е. получаваме възможност за агрегиране на трафик.

- Етикетите вече са дефинирани за повечето технологии от канално ниво (Ethernet, PPP, ATM, Frame Relay). В резултат на това MPLS услугите се предлагат за множество хетерогенни мрежи.

- Първоначалната мотивация за създаването на MPLS е необходимостта от бързо комутиране, като заменим търсенето на маршрут към дестинация с различен по дължина адрес с точно съвпадение на предварително определен брой битове. С появата на бързи маршрутизиращи алгоритми полезността на MPLS в това отношение е до известна степен ограничена. Въпреки това, използването на етикети за идентификация на група от пакети вместо съвпадението на различни части от хедърите може да бъде полезно в различни случаи, които изискват бързо индексиране в таблица от правила. Например пакети, за които изискваме определена проверка за сигурност, могат да бъдат обозначени с общ етикет. Или при балансиране на трафика при уеб сървъри, пакетите от една сесия могат да бъдат отбелязани с един етикет, така че да бъдат пренасочвани към един и същ сървър. Това следва да се разглежда като „нестандартно” използване на MPLS етикети.

- Понеже интерпретацията на пакетите е независима от управляващите протоколи, нови протоколи могат лесно да бъдат адаптирани. При смяната на комутиращия хардуер обикновено се решава само въпроса за свързване на етикета с поведението на комутиране.

Така описани ползите звучат в голяма степен абстрактно. Ще се убедим в тях едва след като разгледаме по-подробно елементите на системата.

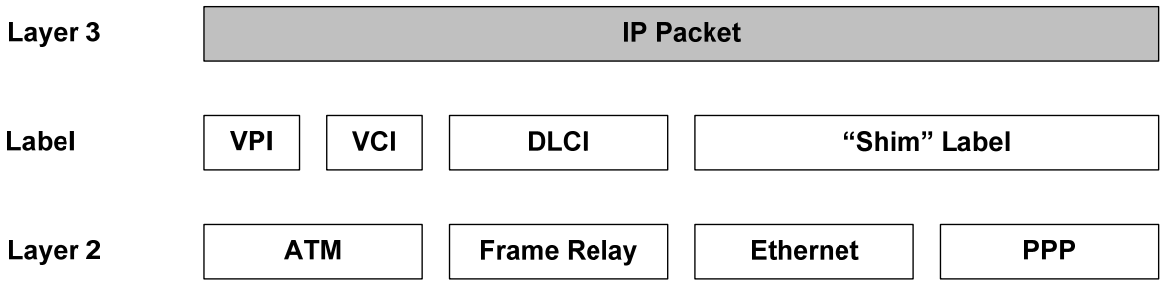
3. Етикети

3.1 Дефиниция на етикет

Етикетът е идентификатор с фиксирана дължина на група от множество свързани пакети. Пакетите, които имат общи атрибути, т.е. принадлежат на един FEC, получават един и същи етикет. Например всички пакети, насочвани към общ изходящ маршрутизатор в мрежата на Интернет доставчик, получават един и същ етикет..

3.2 Формат на етикета

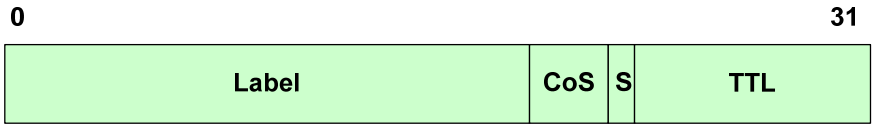
MPLS поддържа три различни вида етикети (Фиг.1). В ATM мрежата тя използва полетата Virtual Channel Identifier (VCI) и Virtual Path Identifier (VPI) на всяка клетка. При Frame Relay мрежата за етикет се използва полето Data Link Connection Identifier (DLCI) във всеки кадър. При останалите мрежи MPLS въвежда ново поле като хедър, който е вклинен между слоеве 2 и 3 и се нарича шайба или просто се употребява английското наименование shim header. В този хедър (Фиг.2) за етикета са отделени 20 бита, 3 бита са експериментални (QoS/DiffServ), 8 бита са за TTL (използват се за предотвратяване на зацикляне) и има един S бит, който дава възможност за стекиране на етикети. Този S бит има стойност 1 когато етикетът е на дъното на стека и 0 в останалите случаи.



Фиг.1 Видове етикети

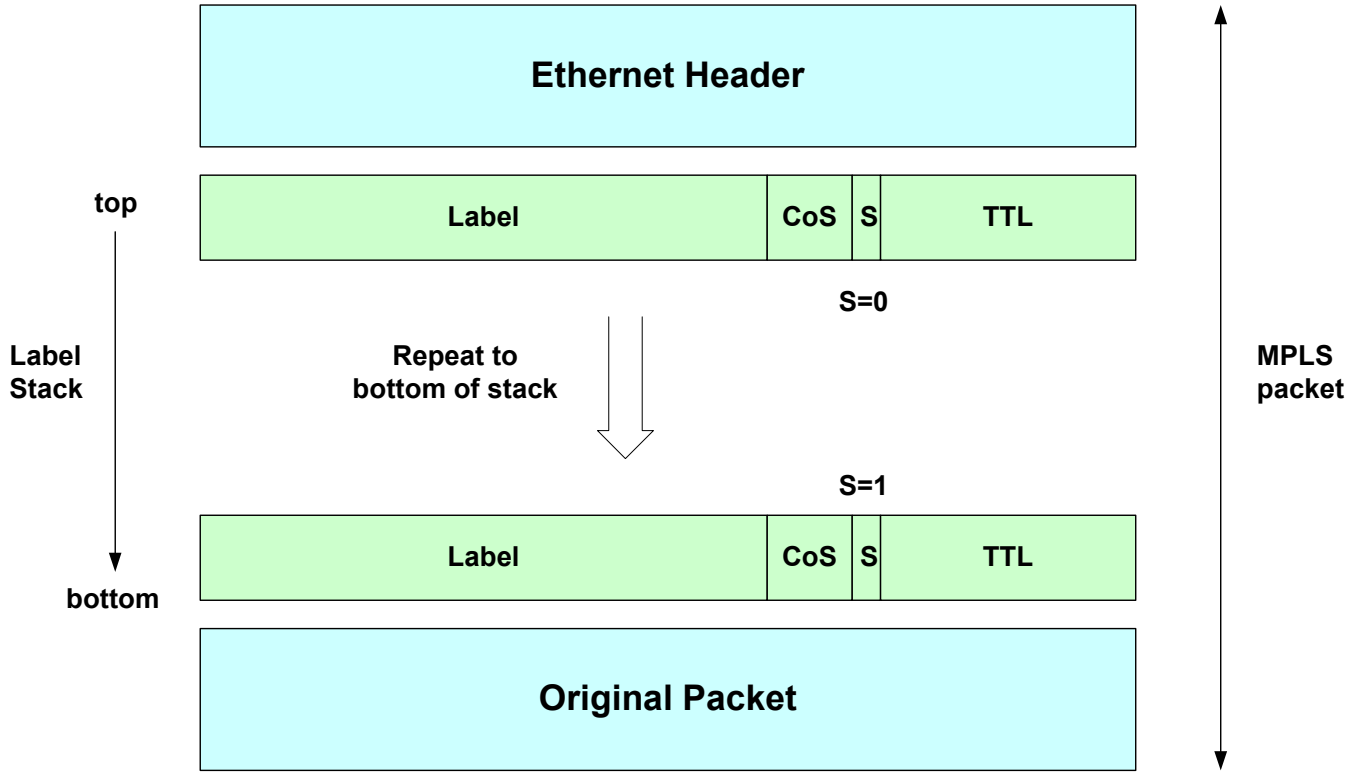
Shim хедърът се състои по принцип от четири октета, макар че няколко етикета могат да бъдат прикачени към даден пакет използвайки концепцията за стекиране на етикети. Стекирането на етикети дава възможност за създаване на тунели. Например един Интернет доставчик може да изгради тунел между двойка негови LER. В този тунел той може да мултиплексира трафик на различни виртуални частни мрежи (Virtual Private Networks – VPN). Тук се използва етикетен стек на две нива – външният етикет идентифицира целия трафик между двата маршрутизатора, докато вътрешният - трафика на конкретна VPN.

Форматът на shim хедъра е представен на Фиг.2.



Фиг. 2 Формат на shim хедъра

На Фиг.3 е показана структурата на пакет с използване на етикетен стек.



Фиг. 3 Етикетен стек

Първо се обработва етикета в MPLS пакета, който е на върха на стека, т.е. този, който е добавен последен. Когато пакетът преминава през тунел само последния етикет (на върха на стека) се променя, останалите етикети остават непроменени. Благодарение на това етикетно стекиране, LSR маршрутизаторите в ядрото не трябва да разпознават етикетите привързани към всички възможни пътища (LSP), които преминават през тях. Вместо това трябва да знаят само етикетите на агрегираните тунели между граничните маршрутизатори. Това в значителна степен увеличава производителността и мащабираемостта на мрежата.

Да обобщим информацията за етикетите:

- Етикетът е цяло положителна число, което идентифицира един FEC, т.е. един поток.

- Стойността на етикета не може да бъде уникална за цялата мрежа, т.е. глобална. Има две съображения, които водят да този извод: 1) Процесът на определяне на такъв глобален етикет е много сложен и 2) Етикетите стават твърде дълги.

- Етикетите са уникални само между два възела

- Стойността на етикетите е в диапазона от 0 до 1048575. Етикетите с номера от 0 до 15 за резервирани от IETF. В CISCO се използват етикети в диапазона [16, 100000], в Juniper Networks динамично използват етикетите в диапазона [100001, 1048575].

- Етикетите могат да бъдат определяни ръчно (по-лошо от статична маршрутизация), или да се използва метод за разпространение и съгласуване на етикетите (label distribution)

4. Етикетно комутиращ маршрутизатор LSR

Както вече споменахме, едно от ключовите предимства на архитектурата MPLS е, че процесът на маршрутизация е разделен на две, т.е. можем да го разглеждаме в две плоскости.

В едната плоскост, наречена плоскост на данните (data plane) или плоскост за препредаване (forwarding plane), се извършва самото физическо прехвърляне на пакета. Тази плоскост е организирана хардуерно, Информацията за препращане на MPLS пакетите и управлението на хардуера се намира в база данни за препращане, наречена Label Forwarding Information Base – LFIB. В нея се използват етикетите с фиксирана дължина. Всъщност тази база данни е разделена на две: Label Information Database (LIB), която се намира в управляващата плоскост и Label Forwarding Table, която се намира в плоскостта на данните. По-подробно описание на таблиците ще дадем след малко.

Хардуерът на плоскостта на данните се управлява от страна на втората плоскост наречена управляваща (control plane), В нея се намират маршрутизиращите протоколи от мрежово ниво и един или повече механизми за разпространение и съгласуване на етикетите. Такова разделение на функциите позволява приложенията да бъдат разработени и внедрени по мащабируем и гъвкав начин.

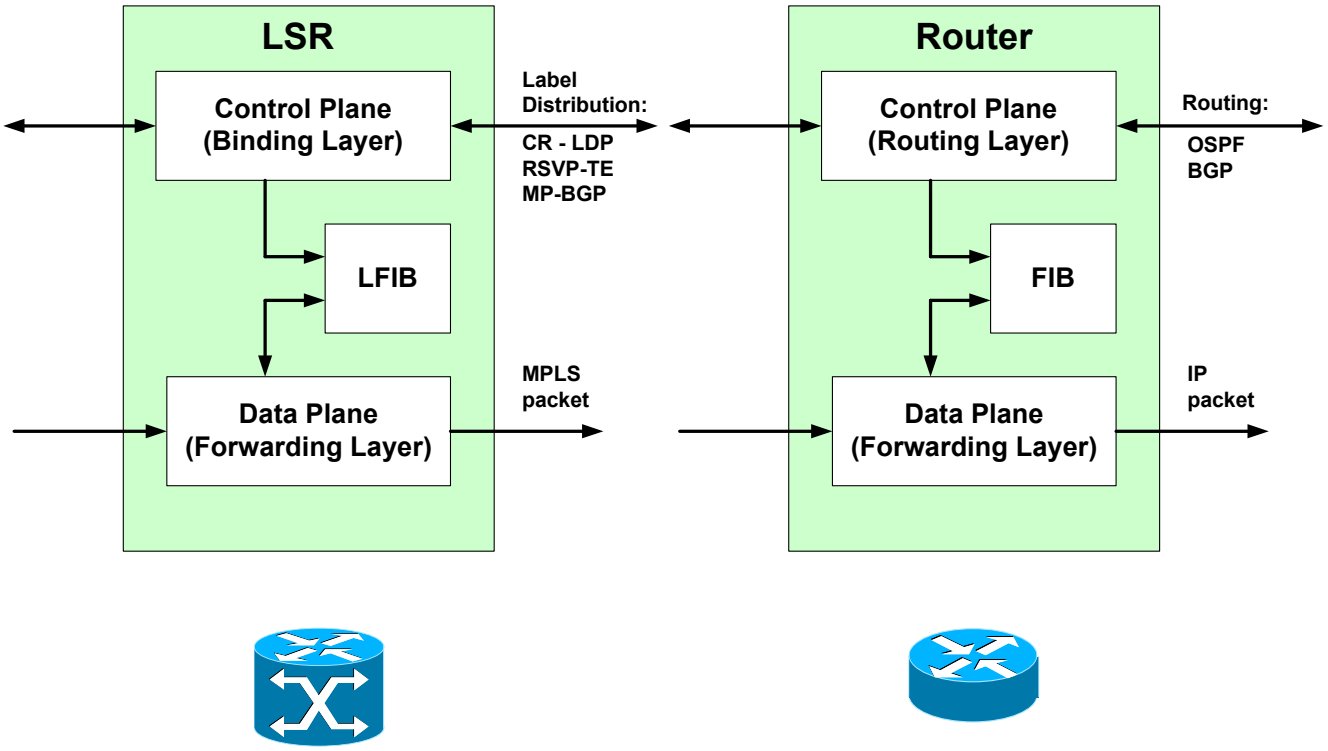
Същата организация имаме и при съвременните модерни маршрутизатори, където не се използват етикети. Там базата от данни FIB също е разделена на две. Частта, която се намира в управляващата плоскост се нарича маршрутна таблица или IP Routing Table (Routing Information Base - RIB), а частта в плоскостта на данните се нарича IP Forwarding Table (Forwarding Information Base - FIB).

Сравнение между двете концепции е направено на Фиг. 4.

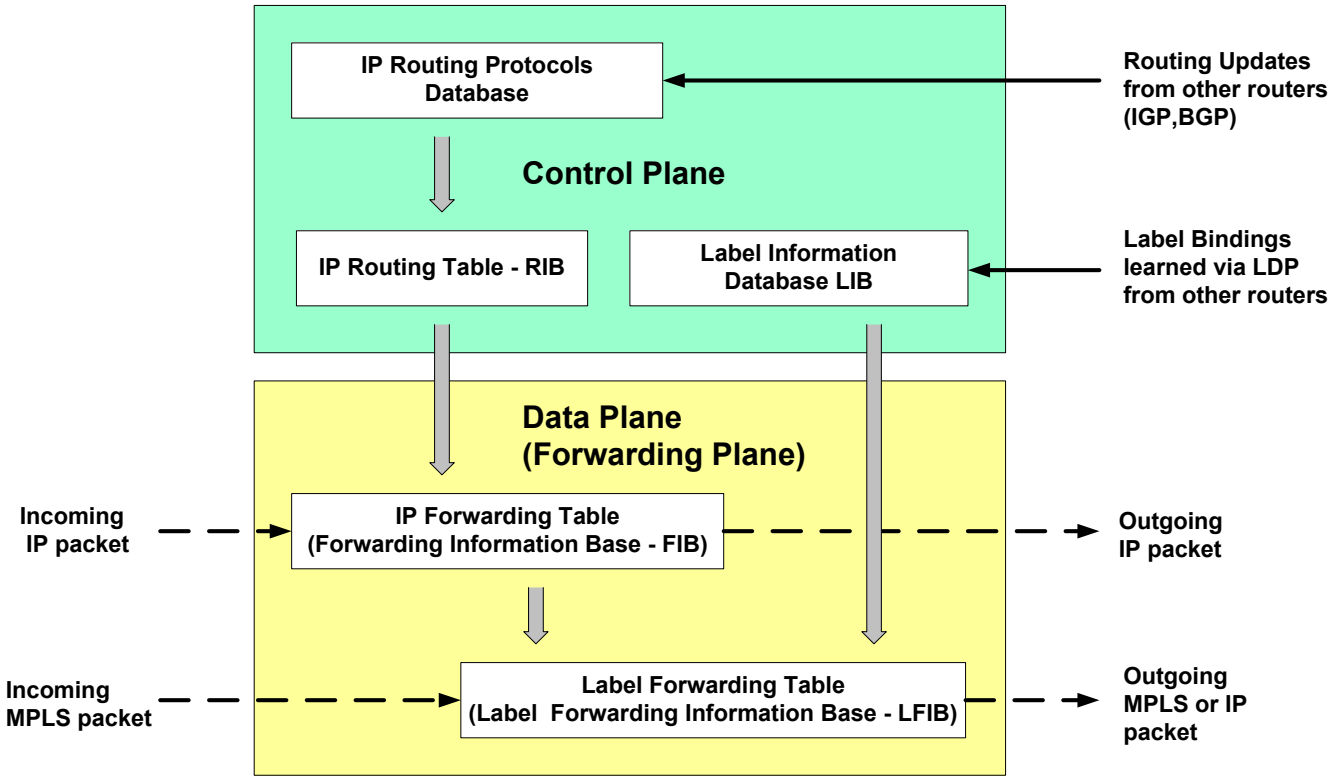
При обикновената IP маршрутизация, маршрутизиращите протоколи (например OSPF, BGP) обменят известна информация помежду си. По същия начин е необходимо при LSR да съществуват протоколи за обмен на информация за етикетите. На Фиг. 4 са показани три такива протокола: Constraint-Based Routing Label Distribution Protocol (CR-LDP) [4], [5], [6], Resourse Reservation Protocol – Traffic Engineering (RSVP-TE) [7], [8] и Multiprotocol BGP Extentions (MP-BGP) [9].

В съвременните маршрутизатори двете схеми на маршрутизиране са обединени, което позволява да се маршрутизират както IP пакети, така и MPLS пакети (Фиг. 5).

На Фиг.6 са показани основните принципи на функционирането на MPLS. За обмен на информация за етикетите и пътищата между два LSR или LER и LSR тук е използван протокола Label Distribution Protocol (LDP), тъй като носи по-общо наименование. Два LSR с установена вече между тях сесия се наричат LDP възли и обменът на информация между тях е двупосочен. Напоследък се препоръчва използването на RSVP-TE вместо LDP.

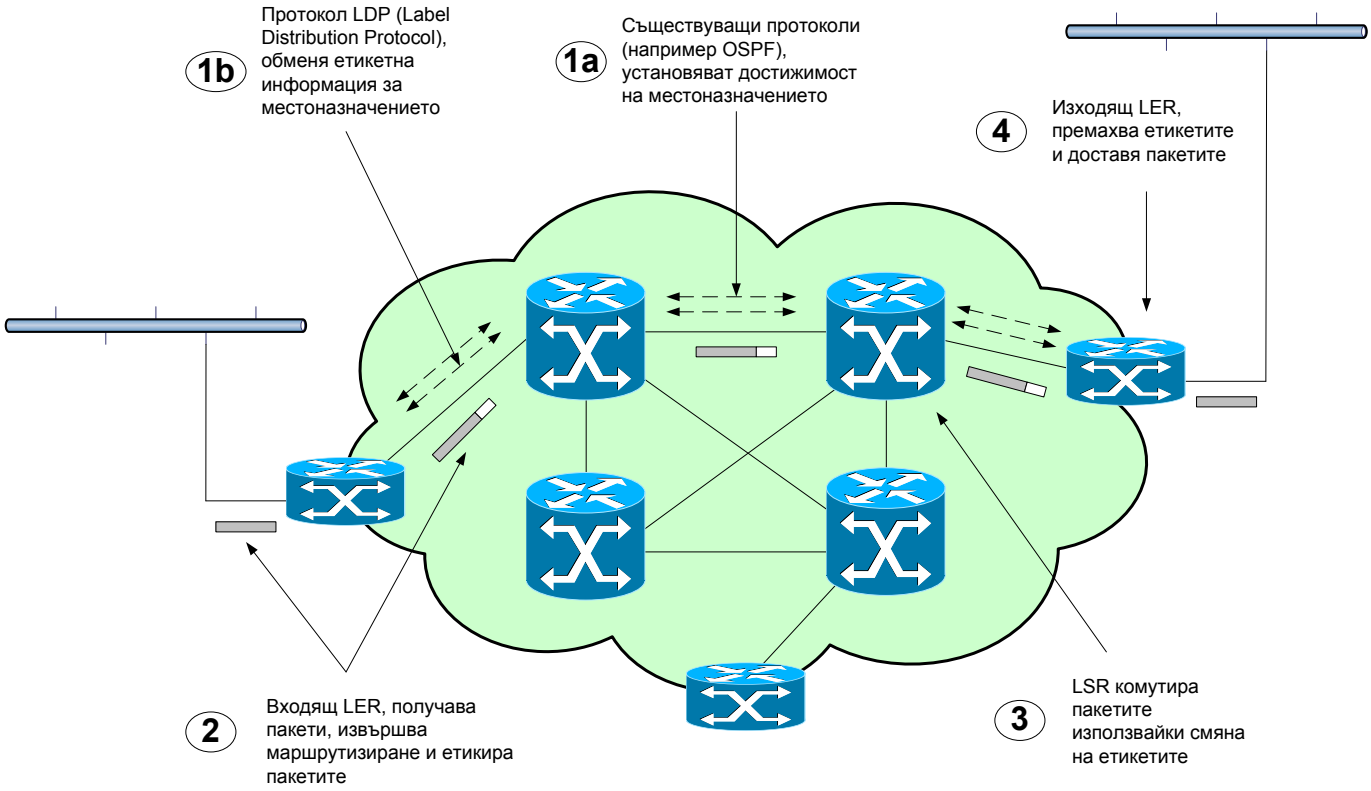


Фиг. 4 Сравнение на архитектурата на LSR и IP маршрутизатор



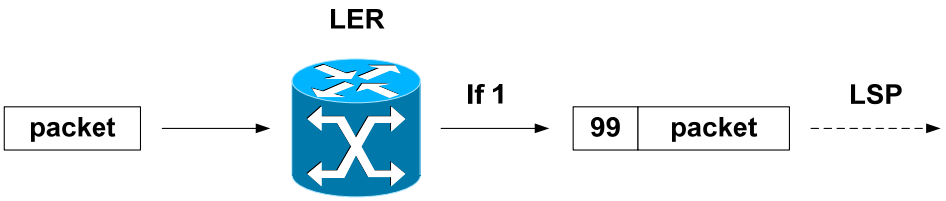
Фиг. 5 Вътрешна архитектура на IP/MPLS маршрутизатор

Остана да опишем малко по-подробно как изглеждат таблиците LFIB на LER и LSR.



Фиг. 6 Принципи на функциониране на MPLS

При проектирането на една IP/MPLS мрежа, за всеки LER трябва да бъдат създадена базата от данни с информация за етикетите Label Information Base (LIB). Въз основа на нея LER ще класифицира входящия IP трафик и ще го свърже с определен клас на еквивалентност FEC изграждайки FLIB. В общия случай това е процес, който се извършва автоматично от MPLS и намеса от страна на администратора е необходима само тогава, когато изрично трябва да се укаже какъв точно етикет да бъде присвоен. На Фиг.7 е показан пример на LFIB на LER.



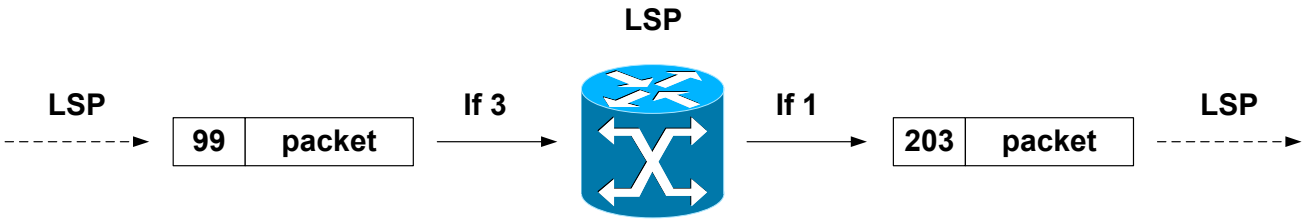
Recipient/ IP	Port number	FEC	Outgoing label	Next Node	Output interface	Operation
172.18.3.1	80	F1	99	172.19.4.1	if 1	push
172.18.3.1	443	F2	17	172.20.4.1	if 2	push
172.18.3.1	25	IP		172.21.4.1	if 3	Do nothing (Native IP)

Фиг. 7 LFIB на LER (Label Pushing)

Функциите, които извършва един входящ LER са следните:

- приема пакета, анализира го и го присъединява към определен клас FEC.
- Намира съответствие между FEC и LSP, с което дефинира етикета.
- Вмъква етикета в пакета (извършва операция push).
- Препраща пакета по LSP през изходящия интерфейс.

От LER пакетите се насочват към някой LSR, който пък от своя страна трябва да разпознае в тях наличието на етикети. LSR проверява своята LFIB за инструкции и променя етикетите (swap), така както е инструктиран. На Фиг.8 е показан пример на FLIB на LSR. Този процес също е автоматизиран и не е необходима ръчна намеса.



Iput interface	Incoming label	Operation	Outgoing label	Output interface	FEC
if 3	99	swap	203	if 1	FEC1
if 3	333	swap	978	if 2	FEC2

Фиг.8 LFIB на LSR (Label Swaping)

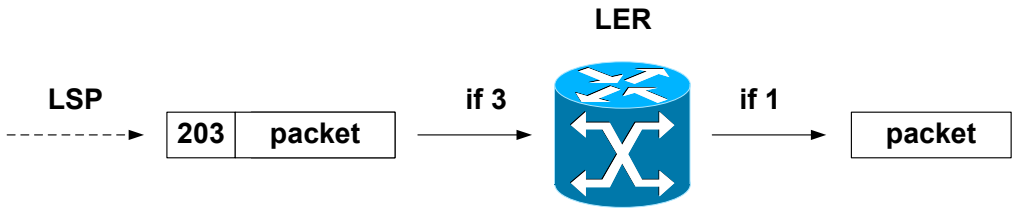
LSR извършва следните функции:

- Проверява LFIB таблицата и променя етикета (извършва операция swap).
- Презаписва MPLS хедъра
- Изпраща пакета по-нататък по неговия LSP.

Изходящият LER трябва извършва следното:

- Премахва етикетите (извършва операция pop)
- Препраща пакета по-нататък като обикновен пакет в съответствие с използваните протоколи за маршрутизация

На Фиг.9 е показан пример на таблица, която изходящият LER използва.



Input Interface	Incoming Label	Operation	Outgoing Label	Output interface	IP Address
if 3	203	pop		IP Lookup	

Фиг. 9 Част от LFIB на изходящ LER (Label Popping)

Видяхме, че MPLS маршрутизаторите извършват върху етикетите такива операции като вмъкване на етикет (push), промяна на етикет (swap) и отстраняване на етикет (pop). Някои етикети изискват специални операции от LSR, затова и между другото те са резервирани от IETF. Описанието на тези специални етикети и действията, които те предизвикват може да намерите например в [10].

За да функционира системата етикетите трябва да бъдат определени и записани (програмирани) в FLIB. За това се грижат протоколите за разпространение и съгласуване на етикетите. Всъщност те създават и пътищата LSP през MPLS мрежата. За да извършат тази дейност, те разчитат на някакъв вътрешен протокол (например OSPF, IS-IS) да намери най-късия път и този път да служи за техен LSP.

Преди да преминем към избора на протокол за разпространение и съгласуване на етикетите (споменахме вече, че съществуват няколко), трябва да се подчертае, че този избор понякога зависи от приложенията. Затова е уместно да изброим за кои приложения е подходяща технологията MPLS.

5. Примери на приложения, които са улеснени от MPLS технологията

Много приложения се изграждат по-лесно, ако използваме MPLS технология. Между тях са следните:

- **QoS** – Използваният механизъм на MPLS позволява в IP мрежи да се изградят пътища с гарантирана пропускателна способност. Досега това беше възможно само в мрежи с превключване на вериги, като Frame Relay и ATM.

- **Управление на трафика (Traffic Engineering)** – Управлението на трафика включва възможността за избор на път, по който трафикът да преминава през мрежата. Този път зависи от изискванията които имаме и от моментното натоварване на мрежата. Прилагането на методи за управление на трафика в мрежата води до по-ефективното използване на наличните ресурси. За управление на трафика обикновено се прилага маршрутизация с ограничения (Constraint-Based Routing). Тази маршрутизация позволява използването на такива методи като включване и изключване на пътища в зависимост от трафика и от нуждите (demand driven),

резервиране на ресурси (resourse reservation) и други, едновременно с конвенционалното, зависещо от топологията неявно маршрутизиране (implicit routing или topology-driven hop-by-hop), използвано в разпространените вътрешни маршрутизиращи протоколи.

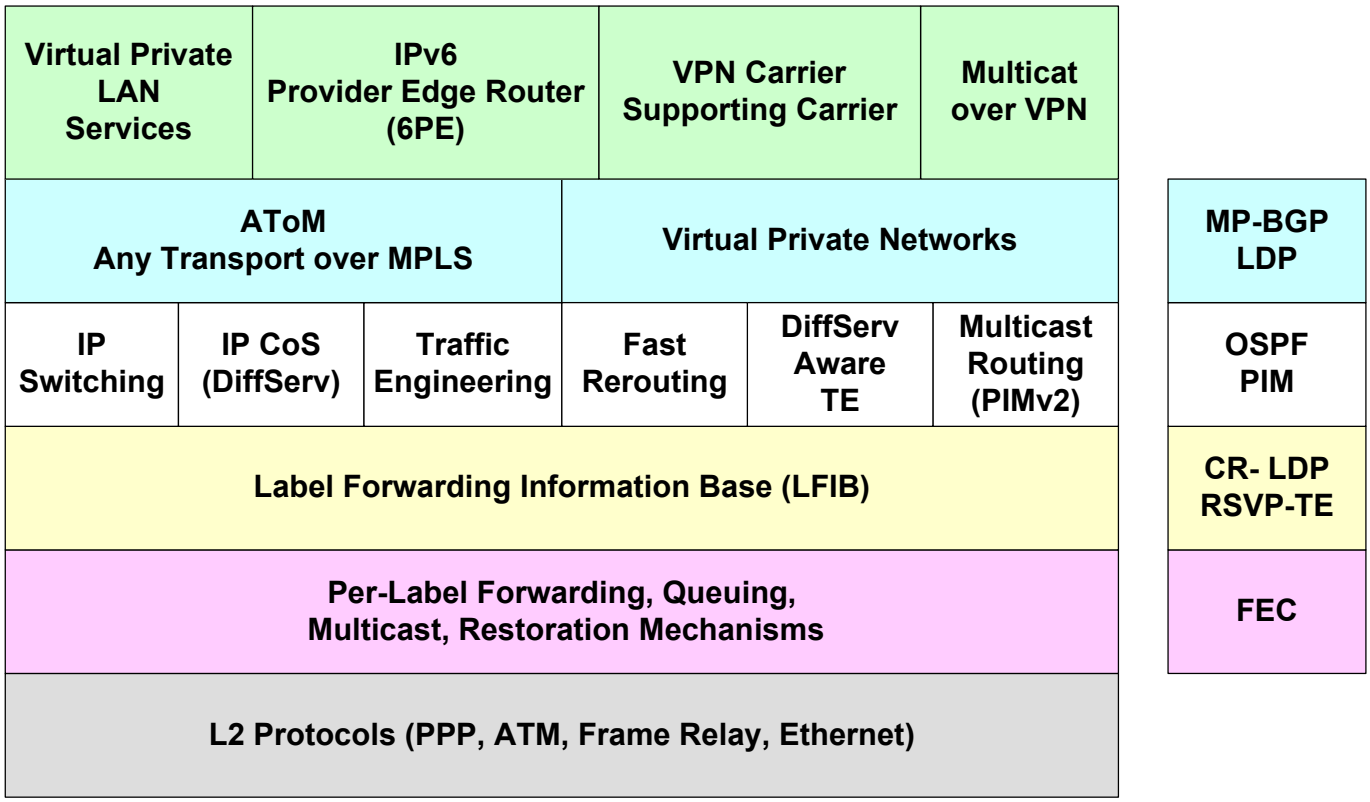
- **VPN** – Когато доставчикът на услуги използва IP/MPLS като ядро на мрежата, той може да изгради множество виртуални частни мрежи във втори и трети слой (Layer 3 VPN и Layer 2 VPN). MPLS се използва за разделяне на трафика на различните клиенти в ядрото.

- **Поддръжка на множество протоколи (Multiprotocol Support)** – Едно от най-значимите предимства на технологията MPLS е, че тя е независима от технологиите използвани в слой 2 и слой 3. Това позволява интегрирането на различни протоколи и не спира развитието на съществуващите вече мрежи и услуги, като Frame Relay, ATM, PPP, HDLC и Ethernet.

- **Групова маршрутизация (Multicast Routing)** – Протоколът PIM (Protocol Independent Multicast) се използва за създаване на FEC таблици. Освен това втората му версия се използва вече и за обмен на привързани към FEC етикети.

- **Обобщен MPLS (Generalized MPLS – GMPLS)** – Целта на GMPLS е да се интегрира управлението на маршрутизацията с това на оптичните канали, което да улесни управление на трафика в мрежите. Оптичните канали не проверяват трафика преминаващ през тях, за разлика например от маршрутизаторите. При GMPLS се осигурява капацитет за автоматично изпълнение на ресурсни резервации, например осигуряване на честотна лента.

Терминът управление на трафика включва извършването на конкретни действия с цел гарантиране, че необходимият трафик ще остане в рамките на наличния капацитет на мрежовите ресурси. Тези действия включват маршрутизиране, оразмеряване на различните процедури и оценка на необходимостите. Сега маршрутизацията в IP мрежите се базира на намиране на най-късите пътища, където „дължината” на връзката зависи от административно определено тегло. Ако матрицата на трафика (дефиниращa очаквания трафик между всички крайни точки на мрежата) е известна, тогава чрез подходящо определение на тези тегла може да се гарантира, че потоците от данни се разпределят оптимално. Например може да се гарантира, че наличният капацитет на отделни връзки се използва в максимална степен. MPLS предлага допълнителни възможности за маршрутизиране на трафика по връзки с достатъчен капацитет. LSP напълно определя пътя за определени класове агрегиран трафик (определен например с адресите на източника и местоназначението). Това става или в реално време или с помощта на управляващи процедури използващи оценки на матрицата на трафика. Изборът на маршрут се извършва или от край до край в граничния LER (Explicit Constraint-based Routing), или на принципа скок след скок (Hop-by-Hop Routing) във всеки маршрутизатор по пътя.



Фиг. 10 Архитектура за MPLS разширени услуги

На Фиг.10 е изобразена архитектурата на MPLS за разширени услуги, включваща такива компоненти като Управление на трафика (Traffic Engineering), Диференцирани услуги (Differentiated Services - DiffServ), Виртуални частни мрежи (VPN), Услуги на виртуални както и основните протоколи, които контролират и обслужват тези функции, като LDP, BGP, RSVP и тъй нататък. По-нататък ще разгледаме по-подробно някои от тези услуги.

6. Избор на протокол за разпространение и съгласуване на етикетите

Първоначално работната група на IETF по MPLS предвиждаше създаването на само един протокол за разпространение и съгласуване на етикетите – Label Distribution Protocol (LDP). В голямата си част LDP се основаваше на технологията за комутиране на етикети Tag Switching, която пък беше създадена за нуждите на маршрутизацията използваща принципа скок след скок. Нуждата от протокол определящ предварително целият път LSP стана критична, когато се разбра, че основното приложение на MPLS е управлението на трафика. Две различни предложения бяха разработени. Едното предложение “Constraint–based LSP Setup using LDP” добави цяло множество от разширения на LDP за да може предварително да се определя целия път LSP. Другото предложение “Extensions to RSVP for LSP Tunnels” представи разширение на протокола RSVP с което да се извършва разпространение на етикетите. Двете съревноваващи се предложения предизвикаха горещи дебати в работната група, като не се постигна консенсус за избор на някое от тях. В резултат се взе решението и двете предложения да бъдат стандартизирани. Тези две предложения са известни като CR-LDP (Constraint Routing Label Distribution Protocol) и RSVP-TE (Resource Reservation Protocol with Traffic Engineering Extensions). И двата протокола поддържат също определянето на LSP на принципа скок след скок. По-долу

първо ще представим LDP, а след това ще сравним приликите и различията между CR-LDP и RSVP-TE.

6.1 Протокол LDP

LDP е първият протокол за разпространение и съгласуване на етикети стандартизиран от MPLS работната група. Протоколът е предназначен за маршрутизация на принципа скок след скок. Два маршрутизатора LSR, които използват LDP протокола за да обменят информация за съответствието етикет/FEC наричаме LDP равноправни възли (LDP peers).

6.1.1 LDP съобщения

LDP равноправните възли обменят помежду си четири категории съобщения:

- Съобщения за обявяване и поддържане на информация за присъствието на LSR в мрежата (Discovery messages)
- Съобщения за създаване, поддържане и прекратяване на сесии между LDP равноправни възли (Session messages)
- Съобщения за създаване, промяна или изтриване на информация за връзка етикет/FEC (Advertisment messages)
- Уведомителни съобщения за разпространение на съвещателна информация и информация за грешки (Notification messages).

Съобщенията за обявяване позволяват маршрутизаторите LSR да покажат присъствието се в мрежата като изпращат периодично бродкастно съобщение „Здравей” (“Hello”). Това съобщение се предава като UDP пакет до порт 646 на всички маршрутизатори намиращи се в дадена подмрежа. След като веднъж сесията между равноправните LDP възли се установи, всички следващи съобщения се обменят по TCP.

6.1.2 Свързване на FEC с LSP

Решението си кога да поиска връзка етикет/FEC от съседен маршрутизатор или да обяви такава връзка на друг маршрутизатор, един LSR взима в голяма степен самостоятелно. Обикновено той иска връзка етикет/FEC от съседен маршрутизатор когато има нужда от нея. Обратно, обявява такава връзка към съседен LSR, когато иска този съседен маршрутизатор да използва този етикет.

LDP сортира пакетите в различни класове FEC, т.е. класифицира ги. С тези класове са свързани пътища LSP. Класифицирането дава много по-големи възможности и гъвкавост, отколкото само проверката на хедърите. Два примера:

Всички пакети към дадено местоположение, например с IP = 192.168.11.12 определят един клас FEC.

Всички UDP пакети с поле ToS = 0x42 от подмрежа 192.168.20.0/24 определят друг клас FEC.

Дефинирането на класовете FEC се извършва от „някой друг". Този някой може да бъде BGP маршрутна таблица, VPN, пакетен филтър и т.н. Това означава, че значението на FEC (неговата семантика) се определя от приложението.

Много е важно точно да се определи кои пакети по кои LSP пътища да бъдат изпратени [11]. Това се постига със спецификацията на FEC за всеки LSP. Всеки FEC се състои от един или повече елемента. Всеки FEC елемент определя множество от пакети, които могат да преминат по съответния LSP. Засега в LDP са дефинирани два FEC елемента:

- Address Prefix – Този елемент представлява мрежовата част на IP адреса, с дължина от 0 до пълния IP адрес включително.

- Host Address – Този елемент е пълният IP адрес на един хост.

Ние казваме, че конкретен IP адрес съвпада с конкретен Address Prefix тогава и само тогава, когато IP адресът започва с този Address Prefix. Също така казваме, че конкретен IP пакет съвпада с конкретен път LSP тогава и само тогава, когато този LSP има FEC елемент Address Prefix, който съвпада с IP адреса на местоназначението на пакета. Когато разглеждаме даден пакет и определен LSP, ние приемаме всеки Address Prefix елемент на FEC, който съвпада с пакета като "съвпадащ" ("matching prefix") .

В процедурата за насочване (привързване) на даден пакет към определен LSP се използват следните правила:

- Ако имаме само един път LSP, на когото FEC елемента Host Address е еднакъв с IP адреса на местоназначението на пакета, тогава пакетът се привързва към този път.

- Ако имаме много пътища LSP, които имат FEC елементи Host Address еднакви с IP адреса на местоназначението, пакетът се привързва към някой (само един) от тези пътища.

- Ако пакетът съвпада с FEC елемента Address Prefix само на един LSP, то той се привързва към този LSP.

- Ако пакетът съвпада с елементите Address Prefix на много LSP, то той се привързва към този LSP, чийто Address Prefix е най-дълъг.

- Ако пакетът трябва да премине през конкретен изходящ маршрутизатор (по информация получена например от протокола BGP), и LSP има FEC елемент Address Prefix който съвпада с адреса на този маршрутизатор, то пакетът се привързва към този LSP.

6.1.3 LDP идентификатори

Тъй като всеки интерфейс на LSR може да използва цялото пространство от етикети, много е важно при обмена на всяко съобщение с други равноправни възли LSR да идентифицира пространството от етикети което използва. Затова се използва

идентификаторът на етикети. LDP идентификаторът е дълъг 6 октета. Първите 4 октета идентифицират самия LSR и в тях трябва да има глобално уникална стойност, например 32-битовия идентификатор на маршрутизатора. Последните 2 октета определят специфичното пространство от етикети, които използва дадения LSR.

6.1.4 Откриване на равноправни възли в LDP

LDP позволява един LSR автоматично да открие равноправните възли с които е свързан. Затова са разработени два механизма. Единият е за откриване на съседни LSR, които са директно свързани, а другият е за откриване на LSR, които са отдалечено свързани. Основният механизъм за откриване се състои в това, че LSR изпраща по всички интерфейси съобщения Hello. Съобщенията се изпращат като UDP пакети към портовете за откриване на LSR маршрутизаторите като се използва групово адресиране за дадената подмрежа (all-routers-on-this-subnet). Hello съобщенията съдържат LDP идентификатор.

За откриване на LDP съседи, които са отдалечено свързани, LSR изпраща периодично друг вид пакети Hello, наречени Targeted Hello. Тези пакети се изпращат към LDP порт за откриване на определен IP адрес. LSR който получава пакета решава дали да отговори с Hello съобщение или не. Обмяната на Hello съобщения установява съседство. Механизмът за откриване на равноправни възли в LDP е описан подробно в [11].

6.1.5 Управление на LDP сесиите

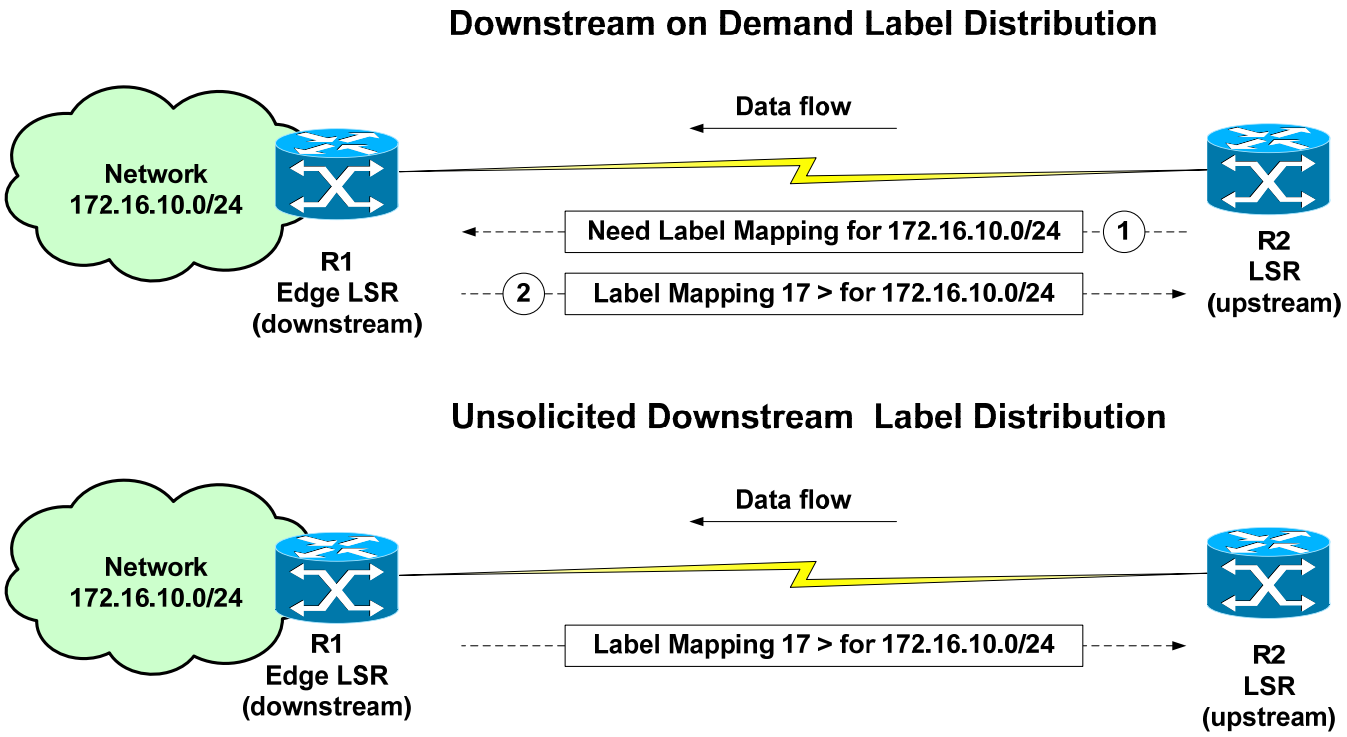
Обмяната на Hello съобщения между два LSR установява канал между тях и определя специфичното пространството от етикети, което тези LSR ще използват помежду си. След установяване на сесията започва процесът на инициализация. Той включва договаряне на версията на протокола, методът за разпространение на етикетите, стойности на таймери, VPI/VCI обхвата за управляван етикетно ATM и DLCI обхватите за управляем етикетно Frame Relay.

LSR одобрява инициализационни съобщения само от LSR с които вече са разменени съобщения Hello. LSR маршрутизаторите поддържат сесията като изпращат съобщения Hello и Keepalive периодично помежду си. Таймерите се рестартират, когато се получат такива съобщения. LSR смята че връзката е прекъсната ако съответният таймер изтече преди да е получено ново съобщение.

6.1.6 Разпространение на етикетите и управление

LDP поддържа два метода за разпространение на етикетите. В единия случай се използва заявка (downstream on demand), а в другия случай се разпространяват непоискани етикети (downstream unsolicited). И двата метода могат да се използват по едно и също време в една и съща мрежа. Въпреки това, в установена вече LDP сесия, трябва да се използва само един от тях.

На Фигура 11 са демонстрирани двата метода на разпространение. При метода по заявка R2 изисква (заявява) етикет за определен FEC (в случая за местоназначение 172.16.10.0/24). R1 определя етикет 17 и го свързва към 172.16.10.0/24, след което изпраща тази връзка на R2. При метода на разпространение на непоискани етикети R1 не чака заявка за определяне на етикет. Той просто определя етикета и го изпраща на R2.



Фиг. 11 Методи на разпространение на етикетите в LDP

LSP маршрутите могат да бъдат създавани независимо от всички LSR по пътя, или последователно, започвайки от изхода към входа на MPLS мрежата. Един LSR поддържа и двата метода на разпространение, като се конфигурира по кой от тях да работи.

При използване на независимия подход, всеки LSR автоматична привързва етикети към FEC и обявява тези връзки на своите съседи по всяко време когато пожелае. Обърнете внимание, че в този случай етикет към предходния LSR (upstream label) може да бъде обявен преди да бъде получен етикет от следващия LSR (downstream label). Този метод е подходящ когато привързването се основава на информация получена от маршрутизиращите протоколи и възлите могат да започнат етикиране преди да е изграден целия път.

При метода за последователно създаване на маршрут един LSR може да обяви етикетно съответствие само за FEC, за който вече има етикетно съответствие към следващия възел или за FEC за който дадения LSR е изход. Ако това не е изпълнено, LSR трябва да изчака докато получи етикетно съответствие от следващия възел и едва тогава да обяви етикет нагоре по веригата за дадения FEC. Този подход се използва за да се гарантира, че определен клас трафик следва пътя с определен набор от свойства на QoS.

6.2 Протокол CR-LDP

CR-LDP е протокол за разпространение на етикети специално разработен за поддръжка на управлението на трафика. В голямата се част той се основава на LDP спецификациите, като са направени специални разширения за предварително определяне на целия

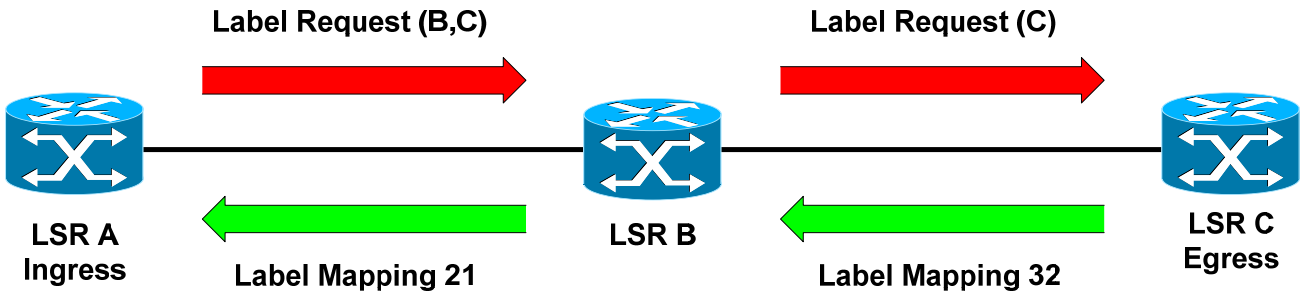
маршрут (явна маршрутизация - explicit routing) и ресурсни резервации. Новите функции, въведени в CR-LDP включват:

- Явна маршрутизация (Explicit routing)
- Резервиране на ресурси и класове (Resource reservation and classes)
- Запазване на път и приоритети (Path preemption and priorities)
- Реагиране при повреди (Handling failures)
- Идентификатор на път LSP ID

6.2.1 Явна маршрутизация

Под явна маршрутизация разбираме предварително избиране на целия маршрут от входа до изхода, т.е. LSP да следва предварително определен път, например списък от IP адреси. В CR-LDP предварително избрания път наричаме също явен маршрут (explicit route) или маршрут с ограничения (constraint-based route) и просто го означаваме с CR-LSP. CR-LDP поддържа два режима на определяне на явен маршрут - стриктен (strict) и хлабав (loose). Явният маршрут е представен в съобщението за заявка на етикет като списък от възли или групи от възли. Всеки CR-LSP се идентифицира с LSP ID, който е глобален идентификатор в MPLS мрежата. LSP ID е съставен от две части: от идентификатора на входящия LSR и локално определения (но единствен) от този маршрутизатор идентификатор за даден CR-LSP. LSP ID се използва когато трябва да бъдат променени параметрите на съществуващ LSP. При стриктния режим всеки скок на явния маршрут се идентифицира еднозначно с IP адрес. При хлабавия режим може да имаме няколко т.н. абстрактни възли. В CR-LDP са дефинирани следните типове абстрактни възли: IPv4 prefix, IPv6 prefix, номер на автономна система (AS) и LSP ID. Когато имаме абстрактен възел, явният маршрут между множеството възли, които сме означили като един абстрактен възел, се определя локално. Например явният път с хлабав режим може да бъде зададен със списък на номера на автономни системи, през които той трябва да мине. Точният път вътре във всяка автономна система не е определен и той зависи от маршрутната информация и политиката на дадената автономната система. Това добавя ново ниво на абстракция и позволява LSP пътищата да бъдат специфицирани по такъв начин, че ефектът от промяна на връзките вътре в една автономна система да се отрази само на тази автономна система.

Разпространението на етикетите за установяване на LSP е показано на Фиг.12. Входящият възел, LSR A инициира установяването на път LSP от LSR A до LSR C. LSR A определя, че LSP трябва да мине през LSR B, затова той изпраща заявка за етикет към LSR B с явен маршрут (B, C). LSR B получава съобщението и го препредава към LSR C, като преди това модифицира явния маршрут. LSR C вижда, че той е изходящ за този път. В отговор на заявката, той изпраща на LSR B етикет със стойност 32 за този път. LSR B използва LSP ID от съобщението-отговор за да направи еднозначно съответствие за пътя и изпраща отговор на LSR A с етикет 21. При това в таблицата FLIB на LSR B за дадения път се записва входящ етикет 21 и изходящ етикет 32.



Фиг.12 Определяне на LSP с CR-LDP

6.2.2 Резервиране на ресурси и класове

CR-LDP позволява да бъдат резервирани ресурси за явните маршрути. Характеристиките на пътя могат да бъдат описани с такива параметри като пикова скорост на предаване (Peack Data Rate – PDR), договорената скорост на предаване (Committed Data Rate – CDR), размера на пиковата експлозия (Peack Burst Size – PBS), размера на договорената експлозия (Committed Burst Size), тегло и изисквания на отделните услуги. Пиковите и договорените скорости описват ограниченията на честотната лента на пътя, а изискванията на отделните услуги специфицират скоростите, които са необходими за тези услуги. Теглото определя как допълнителната честотна лента се разпределя между потребители с различна пропускателна способност. Съществува и възможност да се укаже, че изискванията за ресурси могат да бъдат договаряни, например LSR може да поиска по-малка стойност на определен параметър, ако наличните ресурси не са достатъчни. Мрежовите ресурси могат също да бъдат разделени на отделни ресурсни класове, така че доставчиците на Интернет да специфицират ресурси от кой клас изисква техният явният маршрут.

6.2.3 Запазване на път и приоритети

Ако един LSP ще изисква определен ресурс, но наличните ресурси не са достатъчни, то този LSR може предварително да резервира съществуващи LSP пътища. За тази цел към всеки LSP са свързани два параметъра: установяване на приоритет (setup priority) и запазване на приоритет (holding priority). Тези два параметъра ни дават предимство при добавяне на нов LSP и при задържане на съществуващ LSP. Един нов LSP може за замести съществуващ LSP, ако setup priority параметъра има по-висока стойност от параметъра holding priority на съществуващия път. Двата параметъра приемат стойности от 0 до 7, където с 0 се означава най-важния път (пътят с най-голям приоритет).

6.2.4 Оптимизиране на път

При хлабав явен маршрут точният път в рамките на един абстрактен възел не е уточнен. Това означава, че когато моделът на трафика се промени, тази част от пътя може да се промени и да се адаптира. CR-LDP може отново да оптимизира пътя, като използва LSP ID за избягване на двойното резервиране по време на оптимизацията. В някои случаи маршрутните промени могат да не са желателни. При CR-LDP има опция за захапване на маршрут (route pinning option) . Когато използваме тази опция, LSP не може да бъде променят след като е създаден веднъж.

6.3 Протокол RSVP-TE

Както знаем, RSVP първоначално бе замислен като протокол за резервиране на ресурси в IP мрежи. Протоколът RSVP-TE разширява оригиналния RSVP с възможности за разпространение на етикети и поддръжка на явна маршрутизация. Новите функции добавени към RSVP включват:

- Разпространение на етикети (Label distribution)
- Явна маршрутизация (Explicit routing)
- Резервиране на честотна лента за даден път LSP (Bandwidth reservation for LSPs)
- Пренасочване на LSP при възникнали повреди (Rerouting of LSPs after failures)
- Проследяване на действителния маршрут на LSP (Tracking of the actual route of an LSP)
- Концепция за използване на абстрактни възли (The concept of nodal abstraction)

За разширение на възможностите за резервиране са включени пет нови обекта, представени на Фиг.12.

Име на обект	Използвано в съобщение
LABEL_REQUEST	PATH
LABEL	RESV
EXPLICIT_ROUTE	PATH
RECORD_ROUTE	PATH, RESV
SESSION_ATTRIBUTE	PATH

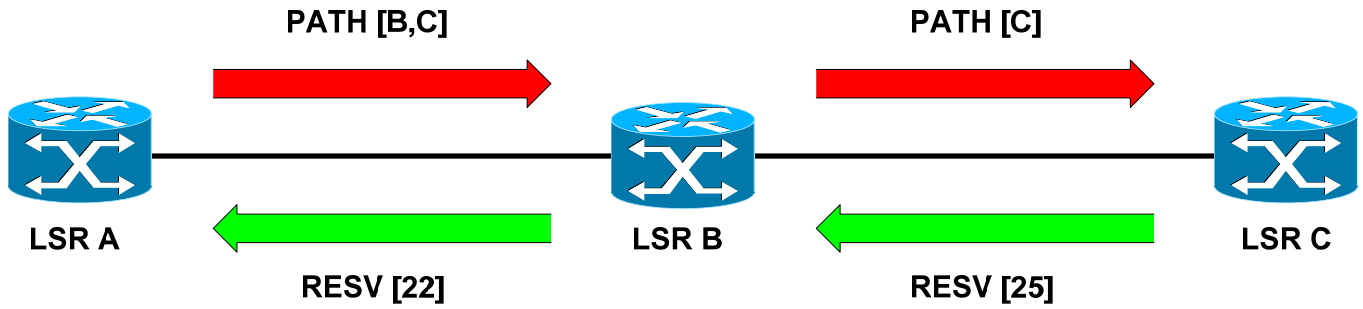
Фиг.13 Нови обекти в RSVP-TE

6.3.1 LSP тунел

Въпреки че оригиналния RSVP протокол беше проектиран да установява резервни пътища в IP мрежи, има една важна разлика между резервния път установен с оригиналния RSVP протокол и пътя LSP. В оригиналния RSVP резервираният път винаги е свързан с определена дестинация и протокол от транспортния слой, а междинните възли препращат пакетите въз основа на IP хедъра. При установяване на LSP от протокола RSVP-TE, входящият възел определя кои пакети се изпращат по този LSP и пакетите не се проверяват от междинните възли по пътя. За да се отрази тази разлика, в спецификациите на RSVP-TE пътят LSP се определя като LSP тунел (LSP Tunnel).

Фиг.14 показва установяването на явен маршрут с RSVP-TE. За да създаде LSP тунел, входящият възел LSR A първо създава съобщение PATH с тип на сесията LSP_TUNNEL. Съобщението PATH включва обект LABEL_REQUEST с което показва, че се изисква

привързване на етикет по този път, а също така дава информация за протокола от мрежовия слой, с който пакетите да се пренасят по този път. За да се създаде явния маршрут, LSR A трябва да опише маршрута в обект EXPLICIT_ROUTE и да го добави към съобщението PATH. LSR A може също така да добави в съобщението обект RECORD_ROUTE, с което иска действителния маршрут да се записва по пътя и тази информация да се върне на изпращащия възел. Обектът RECORD_ROUTE може също така да се използва за изискване на уведомление от мрежата за промени на действителния маршрут или за откриване на цикли в маршрута. Допълнителната информация като запазване на път, приоритети, местна защита и диагностика може да се включи като се добави обект SESSION_ATTRIBUTE в съобщението PATH.



Фиг.14 Установяване на LSP тунел

След като съобщението PATH е вече създадено, LSR A го изпраща към следващия възел, който е определен от обекта EXPLICIT_ROUTE. Ако няма EXPLICIT_ROUTE обект, следващия скок се определя от скок след скок маршрутизацията, т.е. определен е неявно. Междинният възел LSR B променя обекта EXPLICIT_ROUTE и препраща съобщението към изходящия възел LSR C.

LSR C определя нов етикет, включва го в обекта LABEL, и добавя този обект в съобщението RESV. След това LSR C изпраща съобщението RESV назад към подателя следвайки пътя преминат от съобщението PATH, но в обратен ред. Когато междинният възел LSR B получи съобщението RESV, той извлича етикета от обекта LABEL и го използва като изходящ етикет за дадения LSP. Той също определя нов етикет, поставя го в съответния LABEL обект на RESV съобщението и изпраща това съобщение нагоре по пътя към предишния възел. LSR B добавя тази нова двойка етикети към своята таблица FLIB. Когато съобщението RESV достигне до входящия възел LSR A, пътят LSP е вече установен.

6.3.2 Типове резервиране

За всяка RSVP сесия, входящият възел трябва да избере типа на резервиране (reservation style). В оригиналния RSVP протокол се използват три типа резервиране: фиксиран филтър (Fixed Filter – FF), филтър с маска (Wildcard Filter – WF) и изрично споделен филтър (Shared Explicit – SE). Протоколът RSVP-TE позволява само използването на фиксирания и изрично споделения филтър.

Типът резервиране с фиксиран филтър създава отделно резервиране на трафик за всеки източник и това резервиране не се използва от останалите източници. При RSVP-TE този

филтър резервира отделен път LSP от всяка входяща до всяка изходяща точка. Очаква се повечето пътища да бъдат създадени с помощта на този филтър.

Използването на изрично споделения филтър позволява на получателя да обяви точно изпращачите, които да бъдат включени в резервацията. За всички изброени изпращачи има само една резервация на връзка. Това по същество изгражда дърво от много входящи точки до една изходяща точка.

Понеже всеки изпращач е изрично посочен в RESV съобщението, различни етикети се определят за всеки един от тях, като по този начин се създават отделни пътища LSP. Използването на типа SE е много подходящо за избор на резервни пътища LSP, които се използват само ако съответните им активни LSP пътища пропаднат. Така при нормална работа на мрежата тези резервни пътища разделят честотната лента заедно със съответните им активни пътища.

6.3.3 Пренасочване (Rerouting) на LSP тунел

В много случаи може да пожелаем да пренасочим съществуващ LSP. Например когато искаме да оптимизираме използването на ресурсите в мрежата или да се възстановим връзката след повреди в нея. RSVP-TE използва техника наречена “направи преди прекъсване” (make before break) за да сведе до минимум преустановяването на трафика при едно такова пренасочване.

За да се пренасочи съществуващ LSP тунел, първо изграждаме заместващия тунел, след това пускаме трафика по него и накрая старият тунел се премахва. По време на преходния период старият и новият тунел могат да съществуват едновременно и да се конкурират помежду си за общите ресурси на мрежовите сегменти. Това може да доведе до състезателни състояния, където новият LSP тунел не може да бъде изграден, понеже старият LSP тунел не е освободил ресурсите. Той пък от своя страна не може да освободи ресурсите, преди новия LSP тунел да бъде изграден.

За да се разреши този проблем е необходимо да се уверим, че ресурсната резервация не е преброена два пъти, по един път за стария и новия тунел. Това се постига в RSVP-TE като използваме изрично споделен филтър (SE). Основната идея тук е, че старият и новият тунел разделят ресурси по връзки, които за тях са общи. За да направим тази схема работеща, използваме обекта LSP_TUNNEL и стесняваме обхвата на RSVP сесията само до въпросния тунел. Като уникален идентификатор на LSP тунела използваме комбинацията от IP адреса на изходната точка на тунела, идентификатора на тунела ID и IP адреса на входната точка на тунела. По време на операцията за пренасочване на тунела, входната точка трябва да се обяви на RSVP сесията като две различни входни точки. За новия LSP тунел използваме нов идентификатор LSP ID в обектите SENDER_TEMPLATE и FILTER_SPEC. Входящият възел на LSP тунела започва пренасочването на тунела, като изпраща ново съобщение PATH, в което имаме оригиналния обект SESSION, но нови обекти SENDER_TEMPLATE и EXPLICIT_ROUTE, както и нов LSP ID. Това ново съобщение PATH се третира като изграждане на нов LSP тунел. Въпреки това, във връзките които са общи за стария и новия тунел, филтърът SE гарантира, че старият и новият тунел използват една и съща резервация. След като входящият LSR получи съобщението RESV за новия път LSP, той може да прехвърли трафика по новия тунел и да премахне стария.

6.4 Сравнение на CR-LDP и RSVP-TE

И двата протокола, CR-LDP и RSVP-TE, са добри технически решения за управление на трафика по LSP. Ранните версии и на двата протокола имаха някои функционални пропуски, но те бяха открити и отстранени в следващите модификации, така че нивото на функционалност на двата протокола в момента е подобно. Някои основни разлики в структурите на протоколите и използваните транспортни механизми сочат, че предимствата, които ни дават тези протоколи никога няма да съвпаднат напълно. Тези различия, както и скоростта и обхвата на внедряване, ще бъдат основните фактори, които влияят на доставчиците при избора на протокол. Изборът между RSVP-Te и CR-LDP трябва да се ръководи от функциите, които изпълнява целевата система. Какъв модел за определяне на LSP ще бъде използван? Колко стабилни са пътищата LSP – дали това са постоянни магистрали за предаване на данни (trunks) или това са връзки за краткосрочни разговори? Колко голяма е мрежата и колко сложна е тя? Дали това е самостоятелна мрежа и дали нейните компоненти трябва да взаимодействат с различен хардуер и други мрежи? Накрая трябва да вземем под внимание надеждността на хардуерните решения . Какво ниво на отказоустойчивост е необходимо? Колко важна е високата степен на наличност?

Обикновено в различни статии дават сравнение на различните параметри на протоколите. Такъв подход е в голяма степен непродуктивен. Много по-стойностно е, ако ни се дадат някакви указания в кои случаи кой протокол да избираме. Такива указания има в следните две публикации:

- Applicability Statement for Extensions to RSVP for LSP-Tunnels [12]
- Applicability Statement for CR-LDP [13]

7. MPLS услуги

В този раздел би трябвало да се опишат различните допълнителни услуги, които предлага MPLS (виж Фиг.10). Няма да направим това, тъй като съществуват десетки публикации разглеждащи подробно различните възможности на разширените услуги, техните предимства и недостатъци, в кои случаи да бъдат използвани и т.н. При това тези публикации са от най различен тип - от точно специфицирани и пълни с конкретна информация технически доклади, до статии от международни симпозиуми, които внасят само шум в системата.

Наред с функционалността предлагана от MPLS, позволяваща оптималното използване на наличното оборудване, оптимизиране на обслужването и надеждност, имаме и две нови услуги които могат да бъдат предлагани на клиентите или да се използват за вътрешна употреба. Тъй като при описанието на конкретната система се сблъскваме с тези услуги, тук накратко ще подадем малко предварителна информация.за тях Това са частните виртуални мрежи от втори и трети слой (VPN Layer 3 и VPN Layer 2).

7.1. MPLS Layer3 VPN.

Както вече беше изяснено, в MPLS маршрутизирането се извършва като се използват етикети. Възможно е да се изградят MPLS тунели, по които да преминават пакети от различни маршрути с припокриващи се IP адреси, тъй като IP адресите не участват в

процеса на MPLS маршрутизацията. Ако в един физически маршрутизатор има създадени виртуални маршрутизатори и трябва да свържете тези виртуални маршрутизатори с виртуалните маршрутизатори в друг физически маршрутизатор, това може да се направи, като свържете физическите маршрутизатори с MPLS тунел със създадени етикети по него. Сред това се използва система от втори (стекирани) етикети за пренасяне на трафика между виртуалните маршрутизатори. Това е идеята, върху която е изградено функционирането на MPLS VPN Layer 3.

Проблемът е в използването на LDP между виртуалните маршрутизатори, тъй като механизмът за автоматична откриване на възли няма да работи вътре в тунела. Ако не можете да използвате LDP протокол, как етикетите ще се разпространяват между виртуалните маршрутизатори? Този проблем е решен с използването на протокола BGP, който се конфигурира отделно и ръчно за обмяна на етикети [14].

Така се получава Layer 3 VPN мрежа, където LDP се използва за отваряне на тунела, а BGP се използва за разпространение на етикетите вътре в тунела. Това е сложно и трудно за конфигуриране, особено в големи мрежи с много клиенти и портове.

Основният недостатък на Layer 3 VPN, освен че трудно се конфигурира и поддържа, е това че тунелът е на трето ниво, т.е. той участва във вътрешното адресно пространство на клиентите. Те не могат да използват техни вътрешни (IGP) маршрутизиращи протоколи, но дори и ако това го направят (използвайки преразпределение - redistribution), то ако имат алтернативен доставчик и изграден резервен маршрут по друг начин, системата ще работи бавно, ще се губят метрики и други параметри и в края на краищата резервният механизъм няма да работи ефективно.

7.2 MPLS Layer 2 VPN - AToM (Any Transport Over MPLS).

Това е механизъм за прехвърляне на кадри от слой 2 от точка до точка по MPLS. Тунелът се изгражда предварително и кадрите се предават по него. За да се избегне конфигурирането на BGP, има допълнителен сигнален механизъм (използващ частично LDP) с контролна дума от два етикета – етикет на тунел и етикет на подтунел. Тъй като изходящия интерфейс не може да се идентифицира с IP адрес (намираме се във втория слой), в контролната дума има уникален идентификатор, който се използва за тази цел. AToM не е направен от интерфейс до интерфейс, а от разделител в слой 2 (подадрес) към подобен разделител. Например в Ethernet, той е направен от VLAN към VLAN, в ATM от VPI към VPI, във Frame Relay от DLCI към DLCI. Вероятно за да не се дублира информацията разделителните данни не се предават (не се вземат под внимание), но отново се записват (регенерират) от другия край на тунела. Така например може да има тунел започващ от VLAN 44 и предаващ данни във VLAN 31 – на изхода VLAN ID се регенерира и пресъздава.

8. Проектиране на примерна IP/MPLS мрежа

В този раздел са представени резултатите от една разработка за проектиране на примерна мрежа използваща MPLS технология. Тук ще бъдат представени само основните елементи от които е изградена мрежата и нейната топология. Останалите важни елементи на проекта, като използваните адресни пространства, конфигурационните файлове на устройствата и резултатите от извършените симулации можете да намерите в [15].

Най-общо поставената задача е да се проектира IP/MPLS компютърна мрежа със следните параметри:

- Обхват на преносната среда – територията на Република България
- Скорост на предаване – до 1 Gbps

Целта е да се постигне:

1. Възможност за динамично преконфигуриране на маршрути. Да се демонстрира това, като в симулационния модел отпадне главния път.
2. Възможност за оптимизиране на трафика (TE). В симулационния модел да се организират тунели от София до Варна. Да се покаже тяхното функциониране при нормални условия и поведението им при възникване на проблем, като се симулира отпадане на маршрут.
3. Възможност за предоставяне на услуги характерни за следващото поколение мрежи (Next Generation Networks – NGN). Изградените Layer 2 VPN и Layer 3 VPN от София до Варна да бъдат в отделни VRF (VPN Routing and Forwarding, това е технология която позволява много версии на маршрутната таблица да съществуват съвместно в рамките на един и същи маршрутизатор по едно и също време).

При проектирането на мрежата са извършени следните дейности:

1. Определени са възлите на мрежата: главни, второстепенни и техните имена.
2. Определени са скоростите и пропускателните способности на връзките между градовете. Използвани са оптични кабели, като между главните възли имаме 2.4 Gbps, а към и между вторичните възли – 1 Gbps.
3. Избрани са мрежовите устройства в мрежата
4. Представена е графически топологията на мрежата
5. Разпределени са адресите на адресното пространство
6. Определени и описани са връзките между възлите
7. Направен е избор на вътрешен протокол IGP
8. Конфигурирана е MPLS мрежата
9. Конфигуриран е протоколът MP-BGP (Multi-Protocol BGP)
10. Конфигурирани са VPN-ите
11. Конфигурирани са TE тунелите.

По-долу ще се спрем само на някои от изброените дейности. За всички останали подробна информация може да бъде намерена в [15].

8.1 Определяне на възлите

Първо трябва да бъдат избрани точките в които ще се монтира оборудването, така че услугите които то предоставя да достигнат навсякъде на територията на България. Едно от изискванията е да се гарантира скорост на предаване 1 Gbps до всяка точка. Затова са използвани оптични наети линии с капацитет STM16 и скорост на предаване 2.4 Gbps между възлите в опорната мрежа. За такива възли са избрани градове с по-висока консумация и по-развита инфраструктура. Това са София, Варна, Пловдив, Велико Търново, Стара Загора, Бургас, Плевен и Русе. В първите три града, поради голямата консумация, са изградени по два възела, съответно със скорост 10 Gbps и 1 Gbps. За да се покрие страната са изградени второстепенни възли в градовете Видин, Враца, Благоевград, Пазарджик, Хасково, Ловеч, Шумен, Ямбол и Добрич.

Имената на възлите се определят със следния шаблон:

<име> - <тип> - <номер>

където:

- <име> е три буквена абревиатура на града, в който дадения възел се намира,
- <тип> е типа на възела, като също така характеризира и функциите на маршрутизатора в IP/MPLS мрежата. Със CR (Core Router) означаваме основен маршрутизатор в ядрото на мрежата, а с ER (Edge Router) означаваме граничен маршрутизатор.
- <номер> е поредния номер на маршрутизатора за дадения град.

Във Фиг.15 са изброени възлите които се използват, техните имена, местоположението и функциите, които маршрутизаторите трябва да изпълняват в IP/MPLS мрежата. Тези функции са означени като:

- edge – маршрутизатор който осъществява връзка между Layer 3 мрежата на потребителя и MPLS опорната мрежа, наречен граничен маршрутизатор на доставчика (Provider Edge, PE node)
- core – опорен маршрутизатор с MPLS комутиращи функции (P node)
- route reflector – BGP маршрутизатор с маршрутни рефлекторни функции [16].

На Фиг.16 са представени опорните маршрутизатори, граничните маршрутизатори, както и нивото на достъп, на което трябва да бъде направено агрегирането на услугите.

Име на маршрутизатор	Местоположение	Функция
Sof-CR-1	**София център 1**	**core, edge, route reflector**
Sof-CR-2	**София център 2**	**core, edge**
Var-CR-1	**Варна център 1**	**core, edge, route reflector**
Var-CR-2	**Варна център 2**	**core, edge**
Plo-CR-1	**Провдив център 1**	**core, edge**
Plo-CR-2	**Провдив център 2**	**core, edge**
Bur-CR-1	**Бургас център 1**	**core, edge**
StZ-CR-1	**Стара Загора център 1**	**core, edge**
Vta-CR-1	**В. Търново център 1**	**core, edge**
Ple-CR-1	**Превен център 1**	**core, edge**
Rus-CR-1	**Русе център 1**	**core, edge**
Bla-ER-1	**Благоевград център 1**	**edge**
Paz-ER-1	**Пазарджик център 1**	**edge**
Vid-ER-1	**Видин център 1**	**edge**
Vra-ER-1	**Враца център 1**	**edge**
Lov-ER-1	**Ловеч център 1**	**edge**
Has-ER-1	**Хасково център 1**	**edge**
Gab-ER-1	**Габрово център 1**	**edge**
Sli-ER-1	**Сливен център 1**	**edge**
Yam-ER-1	**Ямбол център 1**	**edge**
Shu-ER-1	**Шумен цунтър 1**	**edge**
Dob-ER-1	**Добрич център 1**	**edge**

Фиг.15 Дефинирани възли, тяхното местоположение и функциите които изпълняват

8.2 Описание на необходимите мрежови устройства

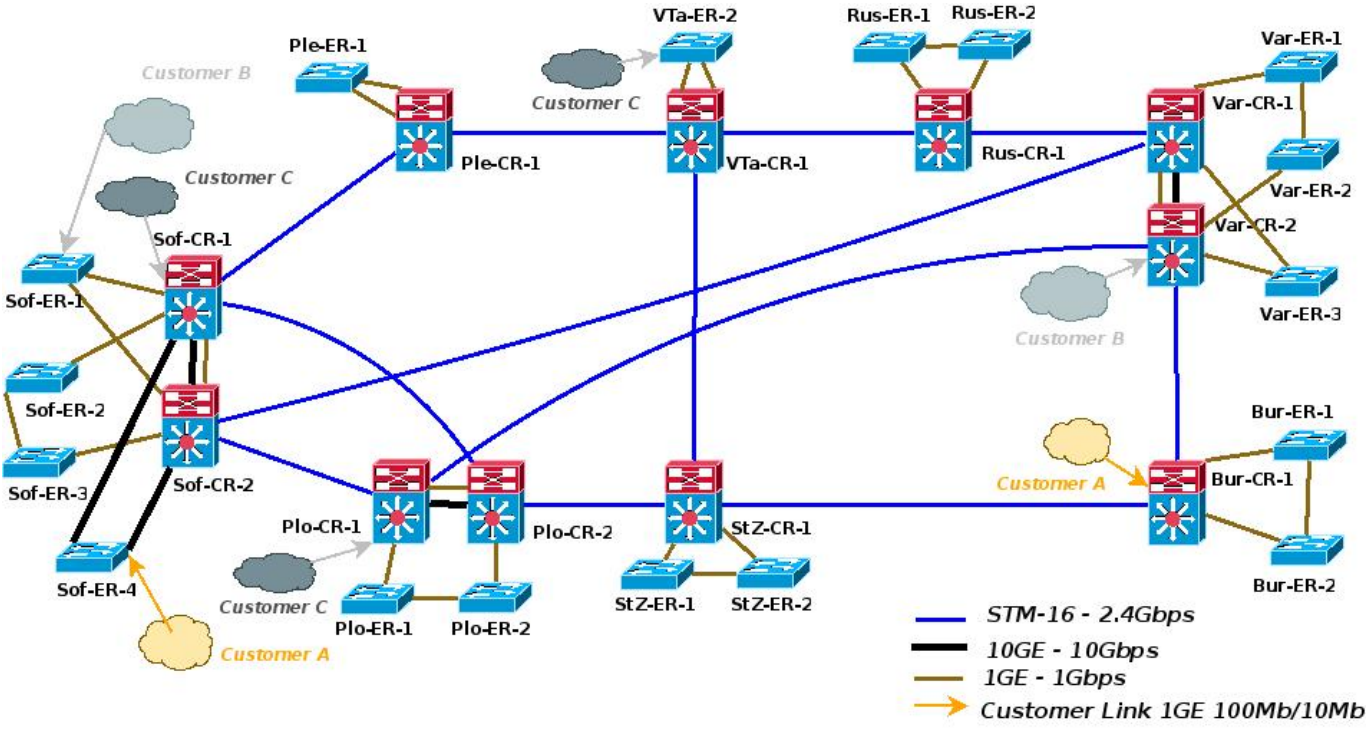
8.2.1 Опорни маршрутизатори (Backbone Routers)

За опорни маршрутизатори са избрани Cisco 7609-S (Фиг.17). За градовете, където търсенето е голямо, като София, Пловдив и Варна, ние използваме по два маршрутизатора. Разположените в Плевен, Велико Търново, Русе и Варна обслужват северната част на страната, докато тези в София, Пловдив, Стара Загора и Бургас обслужват южния клон на MPLS мрежата. Хардуерната конфигурация на Cisco 7609-S е показана на Фиг.17.

8.2.2 Гранични маршрутизатори (Edge Routers)

Като гранични маршрутизатори се използват Catalyst 3750 Series-Metro. Те могат да изпълняват две функции. Работят като шлюз между ядрото (опорната мрежа) и граничните зони. Освен това те могат да бъдат използвани за предоставяне на Layer 2

услуги и агрегиране на трафика на клиентите. В проекта конкретно се използват за достъп до мрежата MPLS и предоставяне на услуги. Поставени са в градовете, където търсенето не е особено високо - Видин, Враца, Ловеч, Благоевград, Пазарджик, Хасково, Габрово, Шумен, Добрич, Сливен и Ямбол. В градове с висока консумация те могат да бъдат използвани и за агрегиране.



Фиг.16 Достъп до опорната мрежа

8.2.3 Софтуерна конфигурация на Cisco 7609-S

В маршрутизаторите Cisco 7609-S е използвано програмно осигуряване 7609RSP720 със следните характеристики и изисквания:

- платформа – 7600-RSP720/MSFC4
- версия – 12.2.33-SRB2 (ED – Early Deployment)
- софтуерно функционално множество – Advanced IP Services SSH
- име на файла – c7600rsp72043-advipservicesk9-mz.122-33.SRB2.bin
- минимална изисквана памет – 1024 MB
- минимална flash памет – 128 MB
- дата на издаване – 12-OCT-2007

Име на модула	Описание	Брой
CISCO7906-S	Cisco 7609-S Chassis	1
6000W-DC	6000W DC Power Supply for 7609/7609-S/7613	2
S764AIK9-12233SRB	Cisco 7600-RSP720 IOS ADVANCED IP SERVICES SSH	1
WS-X6704-10GE	Cat6500 4-port 10 GE Module (req. XENPAKs)	1
WS-F6700-DFC3CXL	Catalyst 6500 Dist Fwd Card- 3CXL, for WS-X67xx	2
OSM-2OC48/1DPT-SS	Cisco 7600 Series 2-Port OC-48c OC-48c/1-port OC-48c DPT OSM	1/2
7600-ES20-GE3C	7600 ES20 Line Card, 20xGE SFP with DFC 3C	1

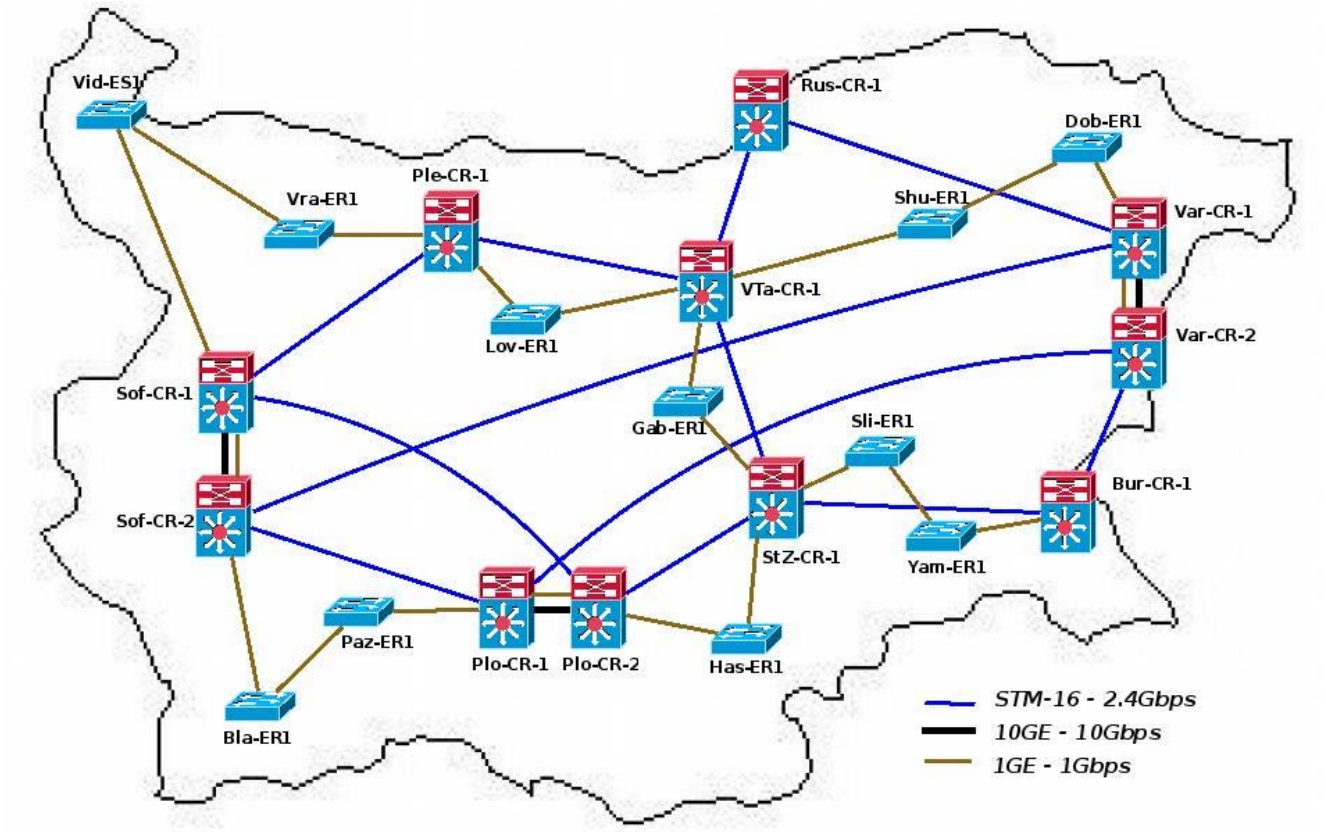
Фиг.17 Хардуерна конфигурация на Cisco 7609-S

Име на модула	Описание	Брой
ME-C3750-24TE-MA	ME C3750 24 10/100+2SFP+2SFP ES Prt (AC-pwrd): Std ME SW Img	1
PWR-ME3750-AC	Metro Catalyst 3750 AC power supply (spare)	1
GLC-LH-SM	GE SFP, LC connector LX/LH transceiver	1

Фиг.18 Хардуерна конфигурация на Catalyst 3750-Metro

8.3 Топология на мрежата

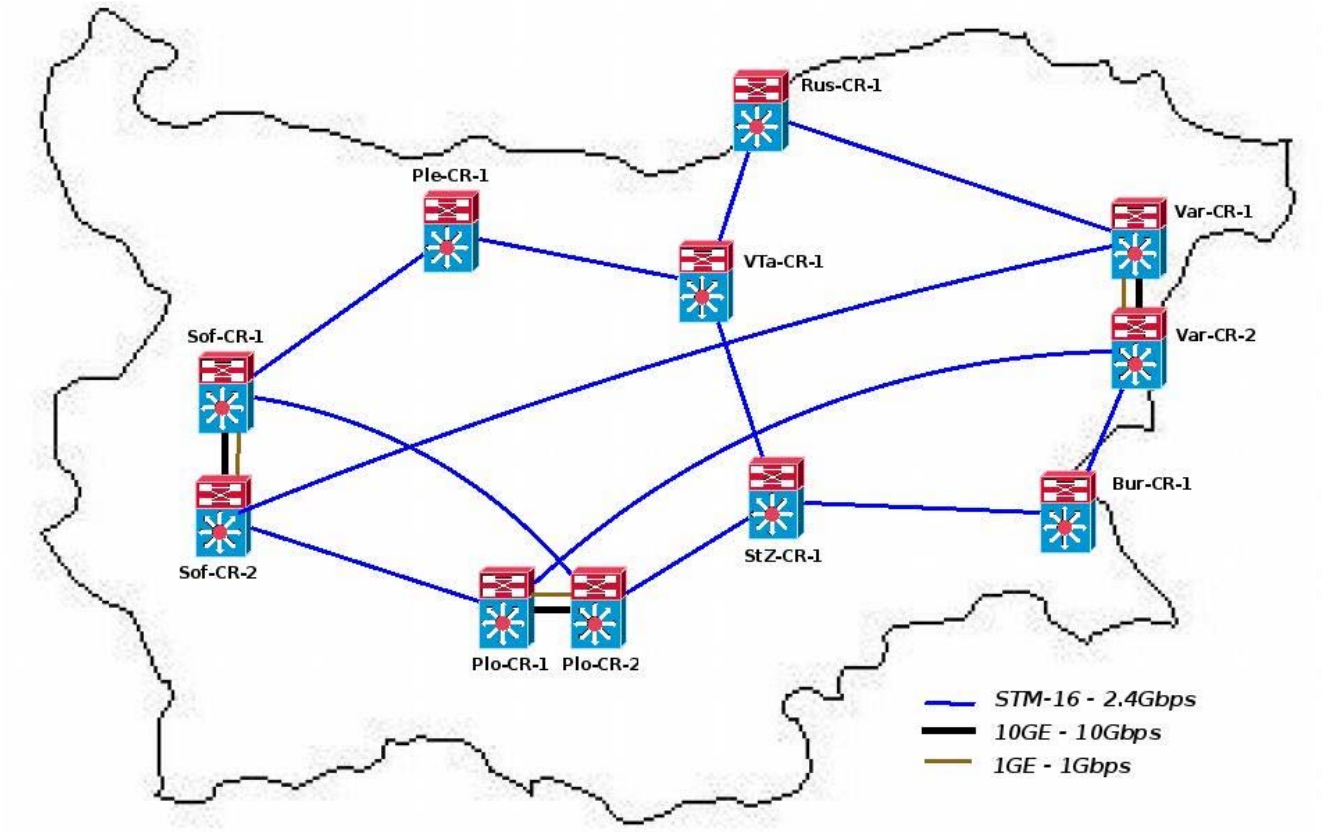
На Фиг.19 е представена топологията на проектираната IP/MPLS мрежа. Както вече казахме, за изграждане на опорната мрежа използваме Cisco 7609-S, а за останалата част Cisco Catalyst 3750-Metro. Показани са главните и второстепенни възли, както и връзките между тях. Главните възли са свързани с оптичен кабел по стандарта STM16, а към и между второстепенните възли се предава с 1 Gbps. В София, Варна и Пловдив имаме по два маршрутизатора с възможности 10Gbps и 1Gbps. Пълното описание на интерфейсите, на връзките между възлите и използваните IP адреси можете да намерите в [15].



Фиг. 19 Топология на мрежата

На Фиг. 20 е представена топологията на опорната мрежа.

Следващата стъпка е да изберем вътрешен маршрутизиращ протокол (Interior Gateway Protocol - IGP), който да ни осигури такива функции като достижимост на следващия възел от BGP, маршрутизиране на административния трафик, статистика на трафика и т.н. След сравняване на два IGP протокола (OSPF и ISIS) и следвайки различните препоръки в документацията на производителя на мрежовото оборудване, е избран протокола ISIS. Този протокол е по-лесно мащабируем, дава възможност за по-лесно увеличение на броя на възлите, има способност бързо да преизчислява маршрути в мрежата след възникване на проблеми и е много по-стабилен от OSPF. Тази мрежа трябва да има възможност за бъдещо разширение и оптимизиране на трафика с използване на системата MPLS-TE, а това също изисква използването на такъв протокол като ISIS.



Фиг.20 Топология на опорната мрежа

8.4 Конфигуриране на MPLS

Върху всички маршрутизатори трябва да бъде стартиран CEF и протокол за разпространение на етикетите. Cisco Express Forwarding (CEF) е основата с която работят всички MPLS услуги в маршрутизаторите на Cisco. Това е един патентован от Cisco механизъм за комутиране, който улеснява и ускорява препредаването на пакетите с което значително увеличава производителността. За да се стартира CEF е достатъчна само една команда за глобално конфигуриране – ip cef.

За разпространение на етикетите се използва протокол LDP. Необходима е глобална конфигурация и тя е стандартна за всички маршрутизатори:

```
mpls label protocol ldp                  (разрешаваме използването на LDP)
mpls ldp router-id Loopback0 force       (указваме на LDP да използва Loopback0 като
                                          идентификатор на маршрутизатор)
```

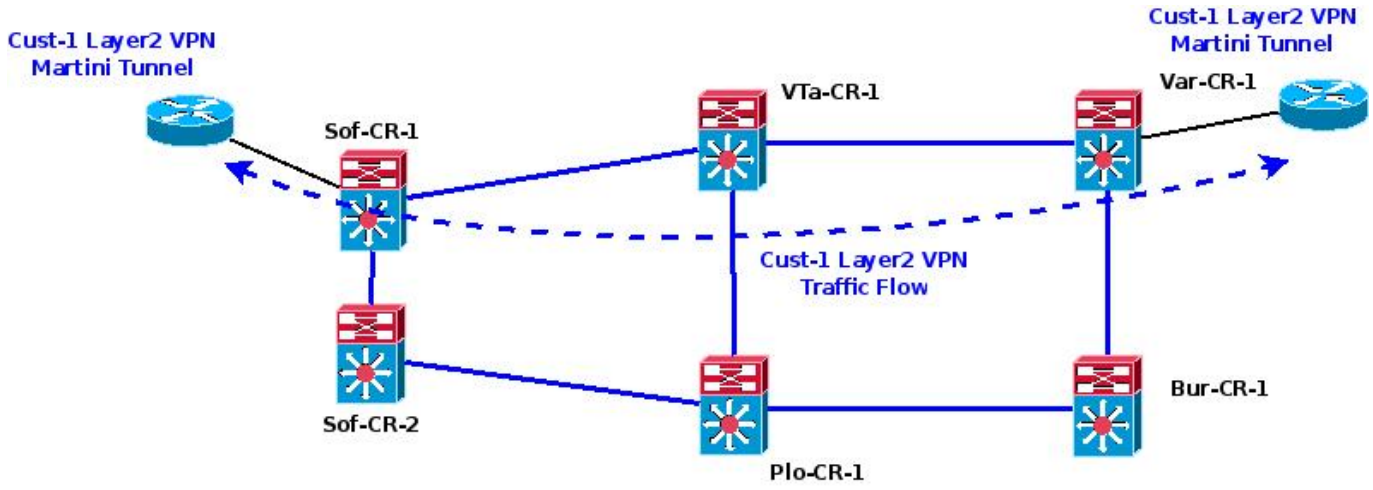
А това е използвания шаблон за конфигуриране на MPLS:

```
interface Loopback0
ip address <loopback-address> 255.255.255.255
ip cef
mpls label protocol ldp
mpls ldp neighbor <neighbor1-loopback> password 7 <ldp-pwd>
```

mpls ldp neighbor <neighbor2-loopback> targeted ldp
mpls ldp neighbor <neighbor2-loopback> password 7 <ldp-pwd>
mpls ldp neighbor <neighbor2-loopback> targeted ldp
mpls ldp holdtime 15
mpls ldp router-id loopback 0 force
interface <core-interface>
mtu 1600
mpls ip

8.5 Реализиране на Layer 2 VPN

В проекта е реализирано прехвърляне на VLAN трафик между София и Варна. Това прехвърляне е напълно прозрачно за потребителите свързани към VLAN 100 на маршрутизатор Sof-CR-1 и VLAN 100 на маршрутизатор Var-CR-1. На Фиг. 21 е показана логическата топология на конфигурирания тунел на Мартини (наричаме го също Ethernet Over MPLS – EoMPLS или Ethernet Layer 2 VPN).



Фиг. 21 Тунел на Мартини (Layer 2 VPN)

Конфигурането на Sof-CR-1 и Var-CR-1 за изграждането на този тунел е представено по-долу:

София

```
hostname Sof-CR-1
interface GigabitEthernet3/0.100
description cust1-L2circuit
encapsulation dot1Q 100
no snmp trap link-status
no cdp enable
xconnect 10.0.52.1 100 encapsulation mpls
```

Варна

```
hostname Var-CR-1
interface FastEthernet3/0.100
encapsulation dot1Q 100
no snmp trap link-status
no cdp enable
xconnect 10.0.2.1 100 encapsulation mpls
```

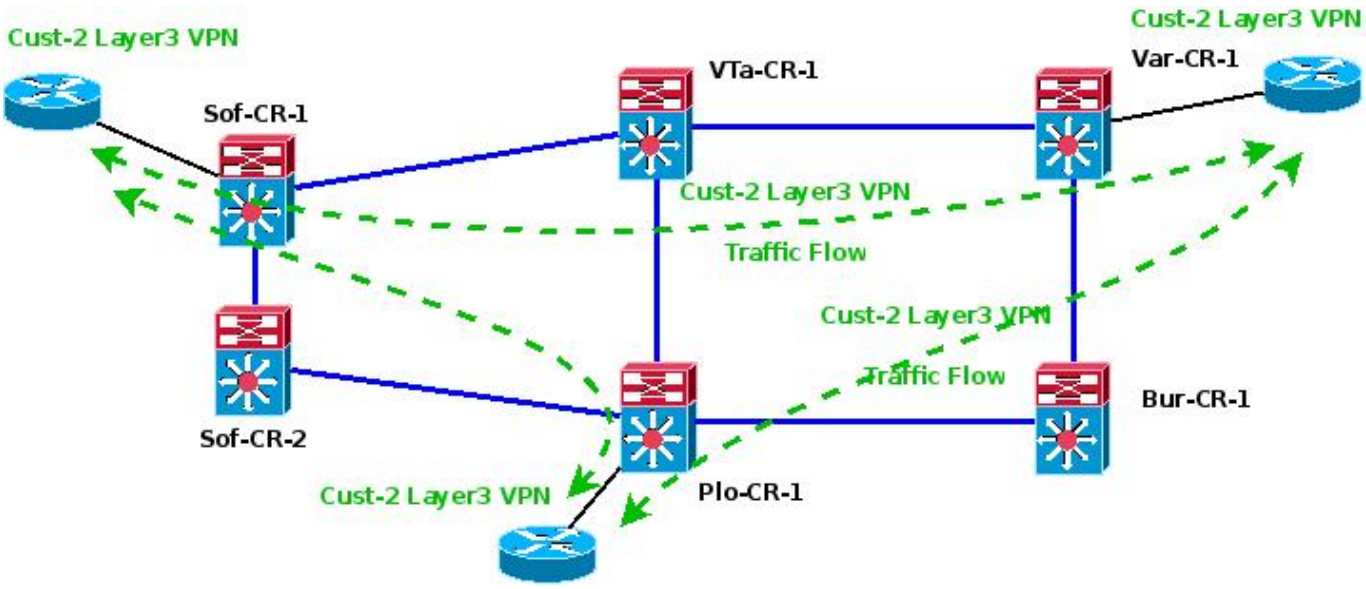
8.6 Реализиране на Layer 3 VPN

Разделянето на клиентите се постига като се използват виртуални маршрутни таблици. Те също се наричат виртуални таблици за маршрутизиране и препращане (Virtual Routing and Forwarding - VRF). По същество това е управлението на различни независими маршрути към потребителите, свързани с доставчика на мрежови услуги. Функцията на VRF е подобна на глобалната маршрутизираща таблица, с изключение на това, че тя включва всички пътища до дадена VPN. VRF е отделна CEF таблица, подобна на глобалната, и дефинира изискванията за свързаност и протоколи за всеки клиент. Интерфейсите, които са част от VRF трябва да имат възможност за CEF комутация [14].

За конфигуриране на VRF се използва глобалната команда ip vrf <name>.

LER (PE) маршрутизаторите трябва да позволяват препокриване на адресното пространство на клиентските мрежи. Те трябва да научават за тези мрежи от потребителите и да ги разпространяват в опорната мрежа. Това се постига с разделител, наречен маршрутен разграничител (route distinguisher - RD) за всяка VRF таблица. Имаме два формата на разделителя: базиран на номера на автономната система (<AS number>:<VPN ID>) и базиран на IP адрес (<IP address>:<VPN ID>).

В този проект е изградена Layer 3 VPN между три точки. Това са София, Варна и Пловдив. Клиентите са свързани към Sof-CR-1 по интерфейса GigabitEthernet3/0.2001 на VLAN ID 2001 и към Var-CR-1 по интерфейса FastEthernet3/0.2002 на VLAN ID 2002. На фиг.22 е показана логическата схема на реализираната Layer 3 VPN. Пълните конфигурационни програми може да намерите в [15].



Фиг. 22 Логическа схема на реализираната Layer 3 VPN.

8.7 Конфигуриране на TE тунели

За да конфигурираме TE тунели трябва последователно да извършим следните стъпки:

При глобалното конфигуриране на маршрутизатора трябва да укажем, че ще използваме TE тунели. Това става с въвеждане на командата

mpls traffic-eng tunnels.

При конфигурирането на интерфейсите, за всеки интерфейс през който ще преминава TE трафик трябва да въведем

mpls traffic-eng tunnels;
ip rsvp bandwidth <value of capacity in kbps>.

Стойността на <value of the capacity> показва каква част от капацитета на интерфейса ще бъде запазена. Ако тази стойност не е указана, по подразбиране е 75%.

За всеки от участващите тунели трябва да се зададе следната конфигурация:

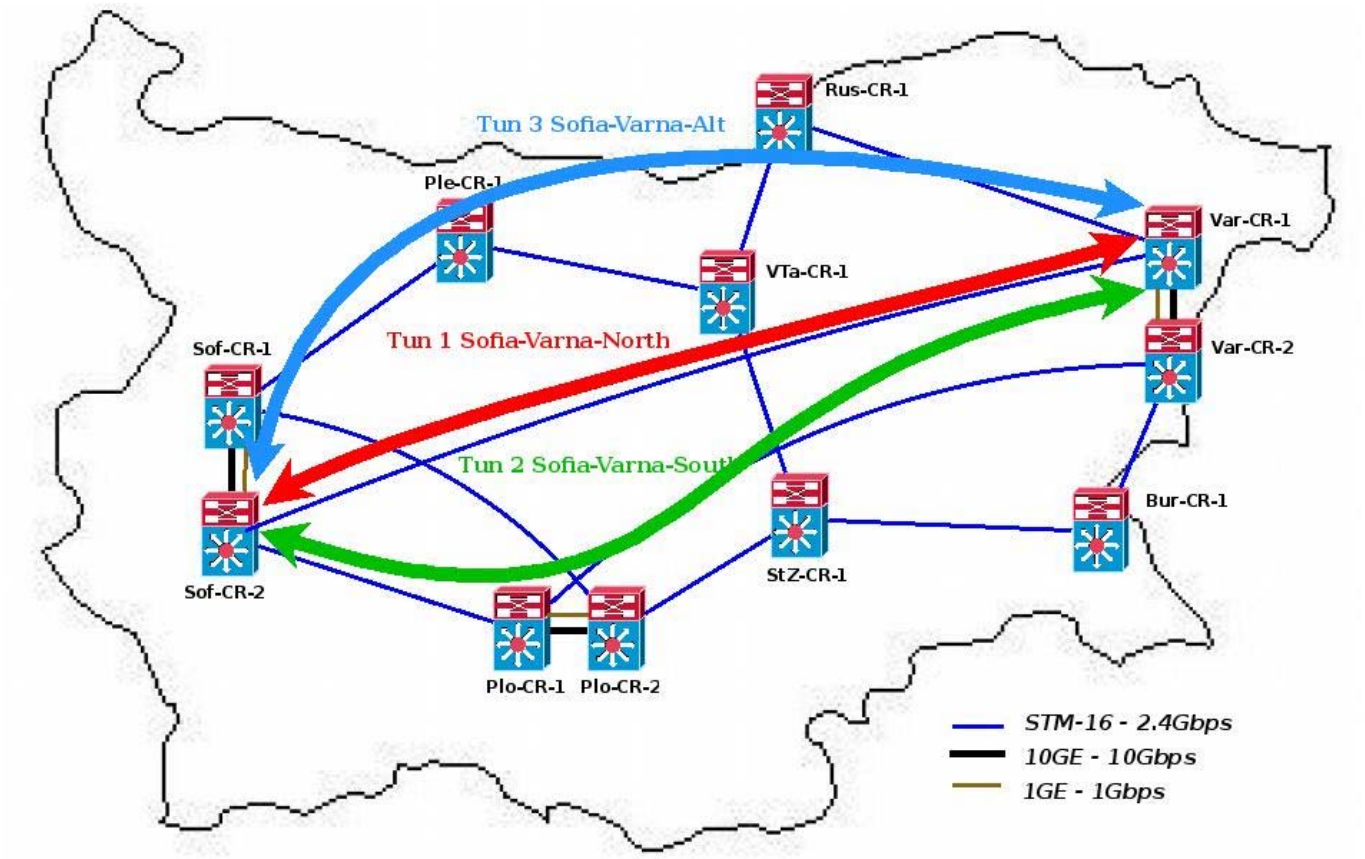
interface tunnel <number of tunnel>	Създава тунелен интерфейс
ip unnumbered Loopback <number of the loopback interface on the router>	Определя IP адрес на тунела
tunnel mode mpls traffic-eng	Определя типа на тунела
tunnel destination <address of the loopback address of the router at the other end of the tunnel>	Определя IP адреса на маршрутизатора на другия край на тунела
tunnel mpls traffic-eng path-option <x> <yyyy>	Определя пътя на TE тунела, където <x> е приоритетът на маршрута. Колкото е по-малко числото, толкова е по-голям приоритета. <yyyy> може да бъде: - dynamic – динамично се определя маршрута на тунела и - explicit name <path name> - пътят е фиксиран със списък от възли, посочени в <path name>.

Фиксирането на пътя със списък от възли изглежда по следния начин:

ip explicit-path name <path name>
next-address <IP address of the next node>
next-address <IP address the second node>
next-address <IP address to third node>
.....
next-address <IP address the final router>

Всеки тунел може да има повече от един път и изборът кой път ще бъде използван за излъчване на бродкастен трафик се извършва въз основа на приоритетите на пътищата. За да се осигури безпроблемно предаване на данни се добавя динамичен избор на път, но с по-нисък приоритет.

На фиг.23 и фиг.24 са показани логическите схеми на конфигурираните тунели.



Фиг. 23 Логическа топология на тунелите от София и Варна

На Фиг. 23 се са показани три тунела конфигурирани за предаване на данни от София (Sof-CR-2) до Варна (Var-CR-1). Те са:

- Тунел 1 – Предаване на данни по директна линия между Sof-CR-2 и Var-CR-1;
- Тунел 2 – Предаване на данни между Sof-CR-2 и Var-CR-1, преминаващ през Plo-CR-1 и Var-CR-2;
- Тунел 3 – Предаване на данни между Sof-CR-2 и Var-CR-1, преминаващ през Sof-CR-1, Ple-CR-1 and Vta-CR-1.

Тези тунели са конфигуриране с един и същи приоритет и по тях едновременно се предават данни. Така че трафикът е разделен на три в съотношение 3:1:1 съгласно принципа на разпределение на натоварването. За да се гарантира динамично преконфигуриране на тунелните пътища се използва динамичен път с по-малък приоритет. Тунелите трябва да бъдат конфигурирани в двете посоки.

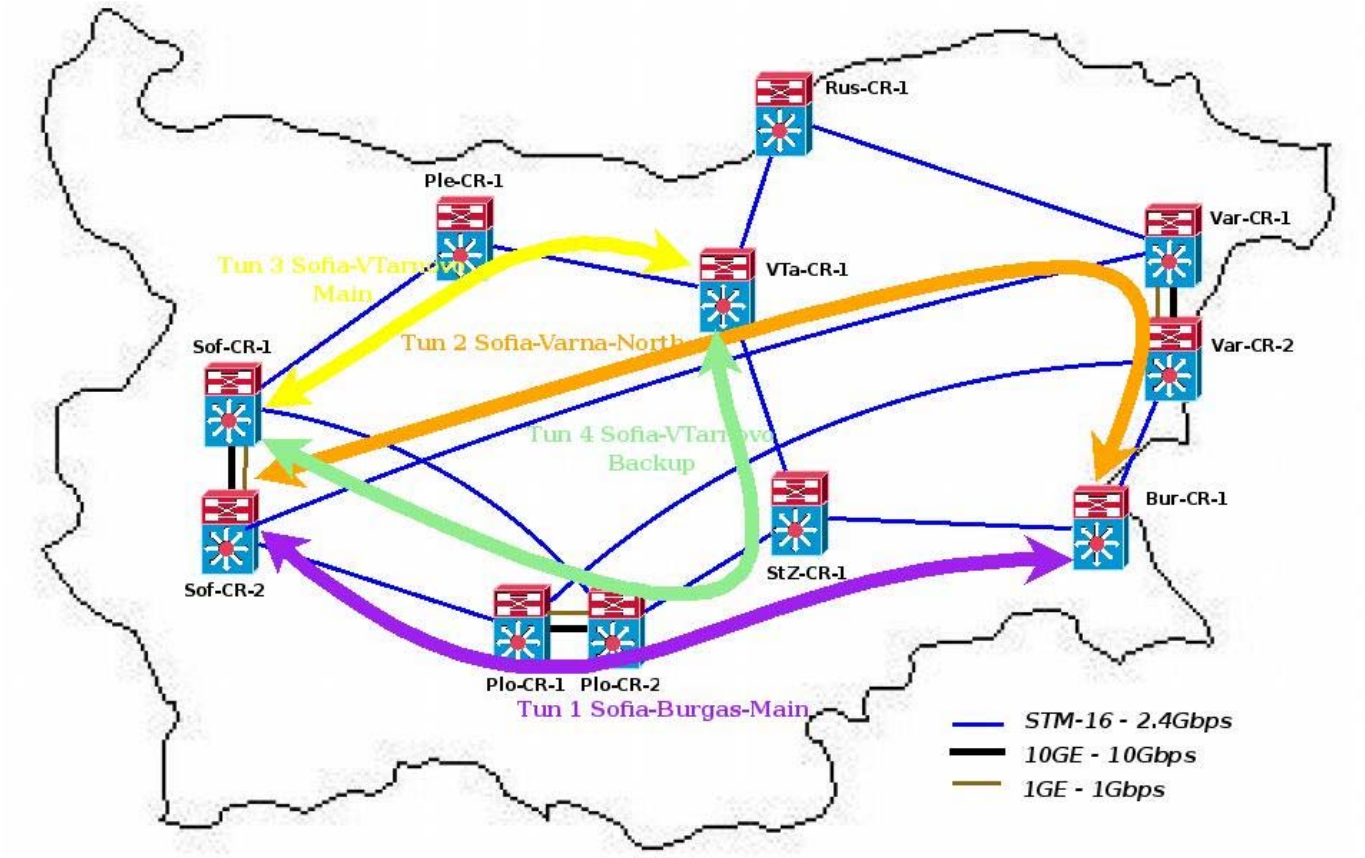
На Фиг. 24 са показани четири тунела за предаване на данни от (Sof-CR-2) до Бургас (Bur-CR-1) и от София (Sof-CR-1) до Велико Търново (Vta-CR-1). Тези тунели са:

- Тунел 1 (София – Бургас) – Предаване на данни между Sof-CR-2 и Bur-CR-1, преминава през Plo-CR-1, Plo-CR-2 и StZ-CR-1, основен тунел;

- Тунел 2 (София - Бургас) – Предаване на данни между Sof-CR-2 и Bur-CR-1, преминава през Var-CR-1 и Var-CR-2, резервен тунел;

- Тунел 3 (София - Велико Търново) – Предаване на данни между Sof-CR-1 и VTa-CR-1, преминава през Ple-CR-1, основен тунел;

- Тунел 4 (София – Велико Търново) – Предаване на данни между Sof-CR-1 и VTa-CR-1, преминава през Plov-CR-1, Plov-CR-2 и StZ-CR-2, резервен тунел.



Фиг. 24 Логическа топология на тунелите от София до Бургас и Велико Търново

Резервните тунели са конфигурирани с по-нисък приоритет, без разпределяне на натоварването (load sharing). Трафикът ще преминава само през основните маршрути. При отпадане на маршрут трафикът ще бъде пренасочен по резервния маршрут. Тук също имаме конфигуриран динамичен маршрут с по-нисък приоритет.

8.8 Заключение

За тестването на мрежи с MPLS технология има вече разработени симулационни модели и интегрирани пакети с помощта на които се доказва работоспособността на мрежите и дали те изпълняват заложените критерии. В проекта беше използван един такъв интегриран пакет – графичният мрежов симулатор GNS3. Подробните резултати от симулацията са представени в [15]. Те напълно потвърждават годността на възприетите технически решения.

Целта на представянето на част от проекта тук е не да запознае специалистите с методите на конфигуриране на MPLS мрежи, нито с техническите възможности на съвременните мрежови устройства. По-скоро идеята е да видим какъв тип проблеми можем да решим ефективно с използването на технологията на многопротоколното етикетно комутиране.

9. Литература

[1] Jim Guichard, François Le Faucheur, Jean-Philippe Vasseur, Networking Technology: Definitive MPLS Network Designs, Cisco Press, 2005

[2] Multiprotocol Label Switching Architecture (RFC 3031); www.ietf/rfc/rfc3031.txt

[3] Arup Acharya, Multi-Protocol Label Switching (MPLS), www.research.ibm/mplsws/publications/mpls1.pdf

[4] MPLS Label Distribution Protocol (LDP) – Cisco Systems. http://www.cisco.com/en/US/docs/ios/12_4t/12_4t2/ftldp41.html ,

[5] LDP Specifications, http://www.ietf.org/rfc/rfc3036.txt

[6] Constraint-Based LSP Setup using LDP, http://www.ietf.org/rfc/rfc3212.txt

[7] RSVP-TE: Extentions to RSVP for LSP Tunnels, http://www.ietf.org/rfc/rfc3209.txt

[8] Inter-Domain MPLS and GMPLS Traffic Engineering – RSVP-TE Extentions http://www.ietf.org/rfc/rfc5151.txt

[9] Multiprotocol Extensions for BGP-4, http://www.ietf.org/rfc/rfc2858.txt

[10] MPLS Fundamentals: Forwarding Labeled Packets, http://www.ciscopress.com/articles/article.asp?p=680824&seqNum=2

[11] LDP Specifications, http://www.ietf.org/rfc/rfc3036.txt

[12] Applicability Statement for Extensions to RSVP for LSP-Tunnels, http://www.ietf.org/rfc/rfc3210.txt

[13] Applicability Statement for CR-LDP, http://www.ietf.org/rfc/rfc3213.txt

[14] Luc De Ghein, MPLS Fundamentals, Cisco Press, 2006

[15] Mariyan Dimitrov, Planning, Implementing and Optimizing an NGN-ready Network Infrastructure, Bachelor Thesis, New Bulgarian University, 2012

[16] BGP Case Studies – Cisco Systems, http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800c95bb.shtml