УДК 004.77
О.О. Квачук
Національний авіаційний університет

ПОБУДОВА ВІРТУАЛЬНОЇ ПРИВАТНОЇ МЕРЕЖІ ЗА ТЕХНОЛОГІЄЮ MPLS

В статті представлений опис основних аспектів впровадження технології MPLS у мережах операторів для надання послуги «віртуальна приватна мережа» й похідних послуг; розглядаються питання, пов'язані з обґрунтуванням вибору технології MPLS; розглянуто принцип комутації, елементи архітектури, компоненти MPLS VPN; наведені варіанти топології мереж MPLS VPN; описані стандарти MPLS VPN; розглянуто питання безпеки, описано переваги MPLS VPN.

MPLS (MultiProtocol Label Switching) - це технологія швидкої комутації пакетів у багатопротокольних мережах, заснована на використанні міток. MPLS розробляється і позиціонується як засіб побудови високошвидкісних IP-магістралей, однак область її застосування не обмежується протоколом IP, а поширюється на трафік будь-якого мережевого протоколу, що маршрутизується.

Традиційно головними вимогами, що пред'являються до технології магістральної мережі, були висока пропускна здатність, мале значення затримки і хороша масштабованість. Проте сучасний стан ринку диктує нові правила гри. Тепер постачальнику послуг недостатньо просто надавати доступ до своєї IP-магістралі. Тепер потреби користувачів містять у собі і доступ до інтегрованих сервісів мережі, і організацію віртуальних приватних мереж (VPN), та ряд інших інтелектуальних послуг.

Для вирішення виникаючих завдань і розробляється архітектура MPLS, яка забезпечує побудову магістральних мереж, що мають практично необмежені можливості масштабування, підвищену швидкість обробки трафіка і гнучкість з точки зору організації додаткових сервісів. Крім того, технологія MPLS дозволяє інтегрувати мережі IP і ATM, за рахунок чого постачальники послуг зможуть не тільки зберегти кошти, інвестовані в устаткування асинхронної передачі, а й отримати додаткову вигоду зі спільного використання цих протоколів.

Огляд технології MPLS-VPN

Щоб економічно виділити технічні ресурси, необхідні для підтримки мереж IP VPN з різноманітними функціями, сервіс-провайдерам потрібні засоби, здатні розпізнавати різні типи додатків, щоб провайдер міг гарантувати певну якість послуг (QoS) і забезпечувати безпеку даних, причому робити це потрібно в мережах, які будуть менш складними, ніж оверлейні IP-тунелі й вузлові мережі з віртуальними каналами (VC-meshed networks). Оверлейні рішення VPN, надбудовані поверх IP, вимагають тунелювання або шифрування. Крім того, оскільки IP-трафік передається по віртуальних каналах, оверлейна мережа VPN не знає, який трафік по ній передається. Оверлейне рішення зосереджене на з'єднаннях і не дуже добре піддається масштабуванню. Більше того, воно конфліктує з бізнес-додтками IP, які не залежать від з'єднань і орієнтовані на протокол TCP/IP.

Мережа VPN повинна розпізнавати, до якого типу додатків відноситься трафік (голос, відеопотоки або електронна пошта). Вона повинна вміти швидко відокремлювати трафік одного додатка від іншого. Далі, мережа повинна бути VPN-обізнаною (VPN-aware), щоб сервіс-провайдер міг легко групувати користувачів і послуги, у мережах інтранет і экстранет. MPLS — це та технологія, яка надає комутуючим і маршрутизируючим мережам VPN-обізнаність. Вона дає можливість сервісам-провайдерам швидко й економічно створювати захищені мережі VPN будь-якого розміру — у єдиній інфраструктурі.

На відміну від оверлейних рішень, мережа MPLS може розділяти трафік і забезпечувати його захист без шифрування й тунелювання. Технологія MPLS підтримує безпеку в кожній окремій мережі, точно так само, як мережі Frame Relay і ATM підтримують її для кожного окремого з'єднання. Якщо традиційна мережа VPN надає базові послуги мережного транспорту, то мережа з технологією MPLS — це масштабовані послуги VPN, що допускають підтримку IP-додатків з доданою цінністю поверх базової транспортної мережі VPN. Цей сценарій відбиває перехід сервісів-провайдерів від транспортно-орієнтованої моделі бізнесу до моделі, орієнтованої на послуги.

MPLS-VPN — це справжня однорангова VPN, яка розділяє трафік на рівні 3 за допомогою роздільних IP VPN таблиць передачі. MPLS-VPN може відокремити трафік одного замовника від іншого, тому що кожній мережі VPN кожного замовника привласнюється унікальний ідентифікатор (VPN ID). Це створює такі ж умови безпеки, як у мережах ATM і Frame Relay, тому що користувач мережі VPN не може бачити трафік, що передається за межами цієї мережі.

Коротко перерахуємо основні характеристики мереж MPLS-VPN:

- Використання багатопротокольних розширень BGP для перетворення префіксів адреси IPv4 в унікальні VPN-IPv4 NLRI.
- З кожним маршрутом замовника зв'язана певна мітка MPLS. Її привласнює PE-маршрутизатор, що стоїть на початку маршруту. Ця мітка використовується для того, щоб направити пакет даних до потрібного кінцевого PE-маршрутизатора.
- У процесі передачі пакета даних по магістралі використовуються дві мітки. Верхня мітка направляє пакет до потрібного кінцевого PE-маршрутизатора. Друга мітка показує, куди цей PE-маршрутизатор повинен направити пакет.
- У каналах зв'язку між PE-маршрутизаторами й CE-маршрутизаторами використовуються стандартні схеми передачі (IP forwarding). PE зв'язує кожний CE з таблицею передачі (forwarding table), у якій зберігаються тільки ті маршрути, які доступні даному CE-маршрутизатору. [3]

Елементи архітектури

Мітки й способи маркування. Мітка — це короткий ідентифікатор фіксованої довжини, який визначає клас FEC. За значенням мітки пакета визначається його приналежність до певного класу на кожному з ділянок маршруту, що комутується.

Мітка повинна бути унікальною лише в межах з'єднання між кожною парою логічно сусідніх LSR. Тому те саме її значення може використовуватися LSR для зв'язку з різними сусідніми маршрутизаторами, якщо тільки є можливість визначити, від якого з них прийшов пакет з даною міткою. Інакше кажучи, у з'єднаннях «точка-точка» допускається застосовувати один набір міток на інтерфейс, а для середовищ із множинним доступом необхідний один набір міток на модуль або весь пристрій. У реальних умовах загроза вичерпання простору міток дуже малоймовірна.

Перед включенням до складу пакета мітка певним чином кодується. У випадку використання протоколу IP вона переміщується в спеціальний «тонкий» заголовок пакета, інкапсулючий IP. В інших ситуаціях мітка записується в заголовок протоколу канального рівня або кодується у вигляді певного значення VPI/VCI (у мережі ATM). Для пакетів протоколу IPv6 мітку можна розмістити в поле ідентифікатора потоку.

Стек міток. У рамках архітектури MPLS разом з пакетом дозволено передавати не одну мітку, а цілий їх стек. Операції додавання/вилучення мітки визначені як операції на стеці (push/pop). Результат комутації задає лише верхня мітка стека, нижні ж передаються прозоро до операції вилучення верхньої. Такий підхід дозволяє створювати ієрархію потоків у мережі MPLS і організовувати тунельні передачі. Стек складається з довільного числа елементів, кожний з яких має довжину 32 біта: 20 біт становлять власне мітку, 8 приділяються під лічильник часу життя пакета, один указує на нижню межу стека, а три не використовуються. Мітка може приймати будь-яке значення, крім декількох зарезервованих.

Шлях одного рівня, що комутується (LSP), складається з послідовного набору ділянок, комутація на яких відбувається за допомогою мітки даного рівня. З погляду трафіка нульового рівня, LSP першого рівня є прозорим тунелем. У будь-якому сегменті LSP можна виділити верхній і нижній LSR стосовно трафіка. Наприклад, для сегмента «LSR 4 — LSR 5» четвертий маршрутизатор буде верхнім, а п'ятий — нижнім.

Прив'язка й розподіл міток. Під прив'язкою розуміють відповідність між певним класом FEC і значенням мітки для даного сегмента LSP. Прив'язку завжди здійснює «нижній» маршрутизатор LSR, тому й інформація про неї поширюється тільки в напрямку від нижнього LSR до верхнього. Разом із цими відомостями можуть передаватися атрибути прив'язки.

Обмін інформацією про прив'язку міток і атрибути здійснюється між сусідніми LSR за допомогою протоколу розподілу міток. Архітектура MPLS не залежить від конкретного протоколу, тому в мережі можуть застосовуватися різні протоколи мережної сигналізації. Дуже перспективно в даному відношенні — використання RSVP для сполучення резервування ресурсів і організації LSP для різних потоків.

Існують два режими розподілу міток: незалежний і впорядкований. Перший передбачає можливість повідомлення верхнього вузла про прив'язку до того, як конкретний LSR одержить інформацію про прив'язку для даного класу від свого нижнього сусіда. Другий режим дозволяє висилати подібне повідомлення тільки після одержання таких відомостей від нижнього LSR, за винятком випадку, коли маршрутизатор LSR є вихідним для цього FEC.

Поширення інформації про прив'язку може бути ініційоване запитом від верхнього пристрою LSR (downstream on-demand) або здійснюватися спонтанно (unsolicited downstream). [2]

Принцип комутації

В основі MPLS лежить принцип обміну міток. Будь-який переданий пакет асоціюється з тим або іншим класом мережного рівня (Forwarding Equivalence Class, FEC), кожний з яких ідентифікується певною міткою. Значення мітки унікальне лише для ділянки шляху між сусідніми вузлами мережі MPLS, які називаються також маршрутизаторами, комутуючими по мітках (Label Switching Router, LSR). Мітка передається в складі будь-якого пакета, причому спосіб її прив'язки до пакета залежить від використовуваної технології канального рівня.

Маршрутизатор LSR одержує топологічну інформацію про мережу, беручи участь у роботі алгоритму маршрутизації — OSPF, BGP, IS-IS. Потім він починає взаємодіяти із сусідніми маршрутизаторами, розподіляючи мітки, які надалі будуть застосовуватися для комутації. Обмін мітками може проводитися за допомогою як спеціального протоколу розподілу міток (Label Distribution Protocol, LDP), так і модифікованих версій інших протоколів сигналізації в мережі (наприклад, незначно видозмінених протоколів маршрутизації, резервування ресурсів RSVP і ін.).

Розподіл міток між LSR приводить до встановлення усередині домена MPLS шляхів з комутацією по мітках (Label Switching Path, LSP). Кожний маршрутизатор LSR містить таблицю, яка ставить у відповідність парі «вхідний інтерфейс, вхідна мітка» трійку «префікс адреси одержувача, вихідний інтерфейс, вихідна мітка». Одержуючи пакет, LSR по номеру інтерфейсу, на який надійшов пакет, і за значенням прив'язаної до пакета мітки визначає для нього вихідний інтерфейс. (Значення префікса застосовується лише для побудови таблиці й у самому процесі комутації не використовується.) Старе значення мітки заміняється новим, що було в полі «вихідна мітка» таблиці, і пакет відправляється до наступного пристрою на шляху LSP.

Уся операція вимагає лише одноразової ідентифікації значень полів в одному рядку таблиці. Це займає набагато менше часу, ніж порівняння IP-адреси відправника з найбільш довгим адресним префіксом у таблиці маршрутизації, яке використовується при традиційній маршрутизації. [3]

Компоненти MPLS VPN

Мережа MPLS VPN ділиться на дві області: IP-мережі клієнтів і внутрішня (магістральна) мережа провайдера, яка служить для об'єднання клієнтських мереж(рис. 1). В загальному випадку у кожного клієнта може бути кілька територіально відособлених мереж IP, кожна з яких у свою чергу може включати декілька підмереж, зв'язаних маршрутизаторами. Такі територіально ізольовані мережні елементи корпоративної мережі прийнято називати сайтами. Сайти, які належать одному клієнту, обмінюються IP-пакетами через мережу провайдера MPLS і утворюють віртуальну приватну мережу цього клієнта. Обмін маршрутною інформацією в межах сайту здійснюється по одному з внутрішніх протоколів маршрутизації IGP.

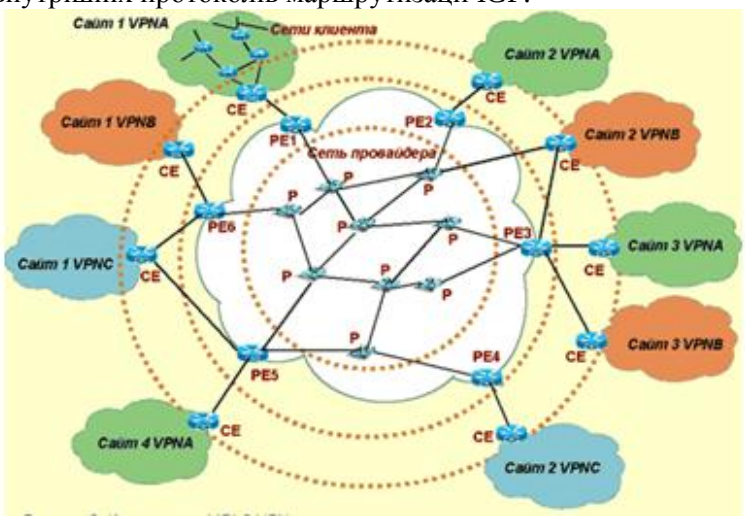

Рис.1 MPLS VPN

Структура MPLS VPN припускає наявність трьох основних компонентів мережі:

- Customer Edge Router, CE – прикордонний маршрутизатор клієнта (Edge LSR в термінології MPLS);
- Provider Router, P – внутрішній маршрутизатор магістральної мережі провайдера (LSR в термінології MPLS);
- Provider Edge Router, PE – прикордонний маршрутизатор мережі провайдера.[2]

Варіанти топології мереж MPLS VPN

Існують два варіанти топології, які використовуються в мережах MPLS VPN. Перший варіант - топологія однорангової мережі MPLS VPN. Другий варіант називається топологією Hub-and-Spoke.

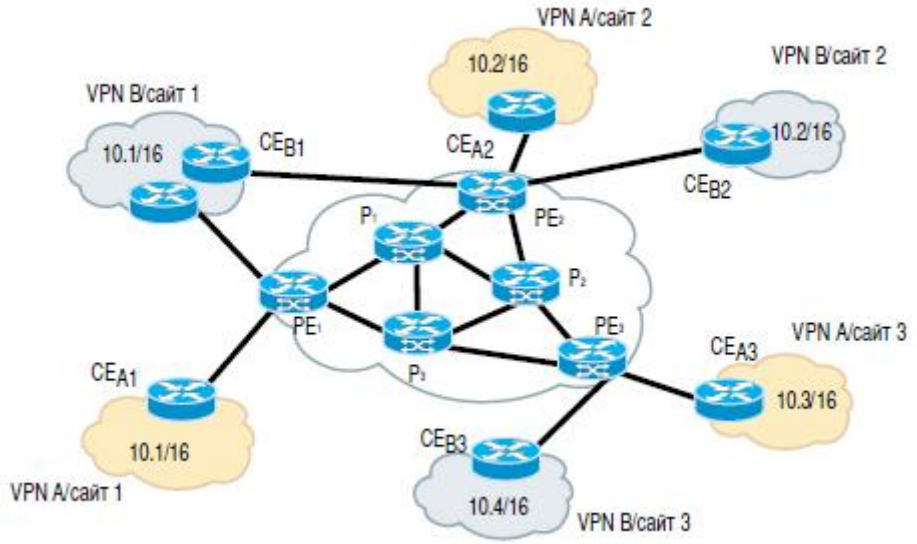

Рис.2 Топологія однорангової мережі MPLS VPN

Топологія однорангової мережі MPLS-VPN

Загальна топологія однорангових мереж MPLS-VPN складається з мереж замовників, що включають безліч сайтів і мереж VPN, CE-маршрутизаторів і PE-маршрутизаторів (прикордонних пристроїв LSR), і з мережі провайдера, у якій установлені PE-маршрутизатори (пристрої LSR).

Прикордонний пристрій LSR (PE-маршрутизатор) може підключатися до одного або декількох CE-маршрутизаторів, підтримувати одну або кілька мереж VPN і підключатися до одного або декількох сайтів у межах однієї VPN.

В одноранговій мережі MPLS-VPN магістраль має часткову або повну вузлову топологію (meshed topology). Якщо CEA1 прагне відправити дані для VPN A/Site 3, пакет надходить на пристрій PE1. PE1 додає до пакета необхідну мітку й передає його пристрою P3. P3 передає дані на пристрій PE3. PE3 видаляє мітку MPLS, переглядає IP-адресу й передає пакет пристрою CEA3. CEA3 відправляє пакет кінцевому адресатові, що перебуває в даному сайті.

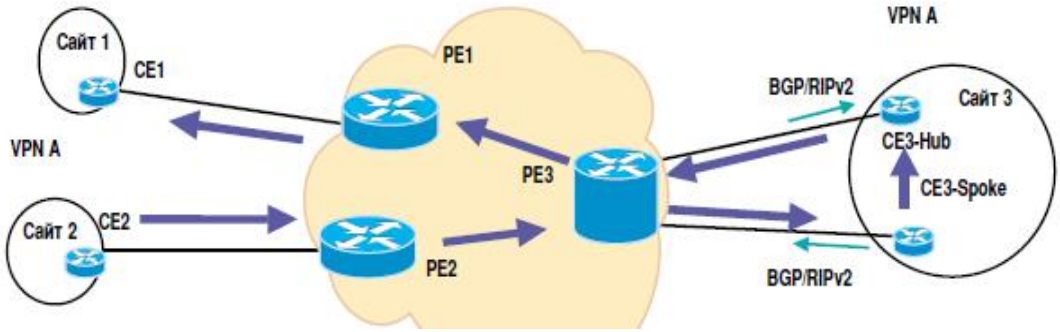

Рис.3 Топологія Hub-and-Spoke

Топологія Hub-and-Spoke

Хоча одна з головних переваг мережі MPLS-VPN є повна одноранговість, деякі замовники воліють відходити від неї й вибирають топологію Hub-and-Spoke. У цьому сценарії всі сайти (spokes) повинні відправляти свій трафік через концентратор (hub). Ця топологія є більш складною, тому що концентратор повинен знати всі інші сайти VPN і служити центральним транзитним пунктом для передачі трафіка між ними. У цьому сценарії весь трафік між сайтами повинен проходити через центральний маршрутизатор CE3-hub. Якщо, наприклад, сайт 2 хоче відправити інформацію сайту 1, то цей трафік пройде через мережу сервісу-провайдера, надійде на маршрутизатор CE3-hub, потім знову потрапить у мережу сервісу-провайдера й лише після цього потрапить на сайт 1. В одноранговій топології такий трафік проходить від CE2 до PE2, потім до PE1 і потім на сайт 1.

Дві перераховані топології — однорангова й Hub-and-Spoke — лежать в основі будь-яких мереж MPLS-VPN.[3]

Стандарти MPLS VPN

Хоча технологія MPLS VPN описана в рамках загальних стандартів на MPLS, в організації IETF існують спеціальні робочі групи, що займаються пророблення окремих питань MPLS VPN. Наприклад, робоча група PPVPN (Provider Provisioned Virtual Private Network) зайнята створенням "каркаса" VPN з поліпшеними механізмами безпеки, масштабованості й керованості.

Три основні типи VPN, над якими працює група PPVPN, — це MPLS BGP VPN, MPLS Virtual Routers і MPLS Layer 2 VPN. Група координує свою діяльність із іншої робочою групою — PWE3 (Pseudo Wire Emulation Edge to Edge), що створює стандарти для тунельних наскрізних з'єднань через мережі ATM і MPLS на першому й другому рівнях.

Віртуальні приватні мережі другого рівня (Layer 2 VPN) також визначені в проекті, що одержав назва Martini, - цей проект перебуває на розгляді робочої групи IETF PWE3. Ідея полягає в організації тунелів для трафіка Ethernet, Frame Relay, ATM і PPP через мережу MPLS. Група PWE3 працює й над іншими схожими пропозиціями, але з боку сервіс-провайдерів найбільший інтерес викликав проект Martini.

Безпека в мережах MPLS-VPN

Функціональність MPLS-VPN підтримує рівень безпеки, еквівалентний безпеці оверлейних віртуальних каналів у мережах Frame Relay і ATM. Безпека в мережах MPLS-VPN підтримується за допомогою комбінації протоколу BGP і системи дозволу IP-адрес.

BGP-протокол відповідає за поширення інформації про маршрути. Він визначає, хто й з ким може зв'язуватися за допомогою багатопротокольних розширень і атрибутів community. Членство в VPN залежить від логічних портів, які поєднуються в мережу VPN і яким BGP привласнює унікальний параметр Route Distinguisher (RD). Параметри RD невідомі кінцевим користувачам, і тому вони не можуть одержати доступ до цієї мережі через інший порт і перехопити чужий потік даних. До складу VPN входять тільки певні призначені порти. У мережі VPN з функціями MPLS протокол BGP поширює таблиці FIB (Forwarding Information Base) з інформацією про VPN тільки учасникам даної VPN, забезпечуючи в такий спосіб безпеку передачі даних за допомогою логічного поділу трафіка.

Саме провайдер, а не замовник привласнює порти певної VPN під час її формування. У мережі провайдера кожний пакет асоційований з RD, і тому спроби перехоплення пакета або потоку трафіка не можуть привести до прориву хакера в VPN. Користувачі можуть працювати в мережі інтранет або экстранет, тільки якщо вони пов'язані з потрібним фізичним або логічним портом і мають потрібний параметр RD. Ця схема надає мережам MPLS-VPN дуже високий рівень захищеності.

В опорній мережі інформація про маршрути передається за допомогою стандартного протоколу Interior Gateway Protocol (IGP), такого як OSPP або IS-IS. Прикордонні пристрої PE в мережі провайдера встановлюють між собою зв'язки-шляху, використовуючи LDP для призначення міток. Призначення міток для зовнішніх (користувацьких) маршрутів поширюється між PE-маршрутизаторами не через LDP, а через багатопротокольні розширення BGP. Атрибут Community BGP обмежує рамки інформації про доступність мереж і дозволяє підтримувати дуже великі мережі, не перевантажуючи їх інформацією про зміни маршрутної інформації. BGP не обновляє інформацію на всіх периферійних пристроях PE, що перебувають у мережі провайдера, а приводить у відповідність таблиці PIB тільки тих PE, які належать до конкретної VPN.

Якщо віртуальні канали створюються при оверлейній моделі, вихідний інтерфейс будь-якого індивідуального пакета даних є функцією тільки вхідного інтерфейсу. Це означає, що IP-

адреса пакета не визначає маршруту його передачі по магістральній мережі. Це дозволяє запобігти потраплянню несанкціонованого трафіка в мережу VPN і передачу несанкціонованого трафіка з неї.

У мережах MPLS-VPN пакет, що надходить у магістраль, у першу чергу асоціюється з конкретною мережею VPN на підставі того, по якому інтерфейсу пакет надійшов на PE-маршрутизатор. Потім IP-адреса пакета звіряється з таблицею передачі (forwarding table) даної VPN. Зазначені в таблиці маршрути відносяться тільки до VPN прийнятого пакета. Таким чином інтерфейс, що входить, визначає набір можливих вихідних інтерфейсів. Ця процедура також запобігає як влученню несанкціонованого трафіка в мережу VPN, так і передачу несанкціонованого трафіка з неї.[2]

Переваги організації віртуальної приватної мережі на базі MPLS

Основними перевагами організації ВПМ за технологією MPLS є:

- гнучкість при зміні смуги пропускання — до ВПМ можна підключитись на швидкостях від 56кбіт/с до 100Мбіт/с;
- керованість послуги — споживач може самостійно змінювати швидкість підключення (для DSL-з'єднань);
- швидка інсталяція послуги — дозволяє якнайшвидше підключити до ВПМ будь-який офіс споживача;
- широкий вибір технологій доступу — до ВПМ можна підключитися з використанням комутованих та постійних з'єднань;
- зв'язок "кожен-з-кожним" — обмін інформацією може здійснюватися безпосередньо між будь-якими підключеними до ВПМ офісами;
- резервування — для з'єднань ВПМ як на магістральному рівні, так і на рівні доступу можуть бути організовані альтернативні маршрути;
- мобільність — будь-яке підключення до ВПМ може бути перенесено в іншу географічну зону, при комутованому доступі таке перенесення здійснюється споживачем самостійно;
- диференційоване обслуговування — мережа може транспортувати трафік відповідно до пріоритетів, визначених споживачем;
- безпека — маршрутні таблиці будь-якої ВПМ ізольовані від таблиць інших ВПМ та Інтернет.

Література

1. Захватов М.А. Построение виртуальных частных сетей на базе технологии MPLS : - М. : Cisco Systems, 2009. - 52 с.
2. http://athena.vvsu.ru/docs/tcpip/mpls/
3. http://www.broadcasting.ru/wiki/