О.Л. НЕДАШКІВСЬКИЙ

Технології та протоколи Інфокомунікаційних мереж (частина друга)

Київ 2018

ВСТУП

Курс "Технології та протоколи інфокомунікаційних мереж" є однією з фундаментальних теоретичних та практичних дисциплін базової підготовки фахівців-зв'язківців і відноситься до дисциплін загально-професійної підготовки за вибором вищого навчального закладу за напрямом 0924 "Телекомунікації". Дисципліна забезпечує професійне спрямування процесу навчання студентів. Складається з двох частин і вивчається протягом двох семестрів.

В навчальній дисципліні розглядаються Технології та протоколи інфокомунікаційних мереж мереж на базі стеку протоколів TCP/IP та технології IP/MPLS. Для стеку протоколів TCP/IP розглядаються протоколи канального, мережного та транспортного рівнів. Особлива увага приділяється алгоритму функціонування протоколу TCP. Для технології IP/MPLS визначаються особливості побудови архітектури мережі та створення віртуальних приватних мереж. Для обох технологій розглядаються архітектура, алгоритми та механізми забезпечення необхідної якості надання послуг.

Мета дисципліни « Технології та протоколи інфокомунікаційних мереж »: навчання студентів основним закономірностям, пов'язаних з принципами функціонування цифрових мереж, їх протоколів та алгоритмів; опанування основними термінами, категоріями, базовими знаннями із су¬часної організації цифрових мереж, використання і оцінювання у своїй практичній діяльності математичних моделей забезпечення якості послуг та планів передавання відповідного типу трафіку за різними політиками; здатність застосовувати правила, методи, принципи, закони у конкретних ситуаціях, своєчасно адаптуватися до зростаючого потоку інформації, впроваджувати новітні науково-технічні досягнення в інфокомунікаційних технологіях в галузь телекомунікацій.

Тому предметом дисципліни є: загальна характеристика цифрових мереж, архітектура мережі на базі стеку протоколів TCP/IP та технології IP/MPLS, протоколи і алгоритми функціонування цифрових мереж за даними технологіями; визначення методів забезпечення необхідної якості обслуговування (QoS) в мережах на базі відповідних технологій; математичний опис характеристик продуктивності протоколів TCP/IP та IP/MPLS, в тому числі з урахуванням політик QoS; алгоритми вирівнювання трафіку, механізми розподілу ресурсів та запо-бігання перевантаження мережі..

Процес створення ІС багато в чому ще не формалізовано. Вміння правильно створити систему чи окрему задачу, виявити і коректно сформулювати критерії і обмеження приходять з досвідом. Існуючі стандарти, керівні документи і методичні матеріали визначають організаційні питання і регламентують склад і зміст проектної документації, але не містять рекомендацій і вказівок, які розкривають суть процесу створення ІС. Це зумовило певні складнощі в ході підготовки навчального матеріалу, який складено з урахуванням окремих питань дисципліни, висвітлених у вітчизняній і зарубіжній літературі, а також досвіду щодо наукових основ створення ІС, практичних розробок ІС різного призначення.

У перших лекціях ви розглянете загальні поняття про архітектуру стеку протоколів TCP/IP, протоколи канального, мережного, транспортного та прикладного

рівнівм, алгоритми функціонування протоколів TCP та UDP, принципи побудови архітектури MPLS, структуру мережного елементу середовища MPLS, принципи комутації в середовищі MPLS, організацію віртуальних приватних мереж в середовищі MPLS. І закінчимо розглядом: архітектура QoS в мережах IP, архітектуру диференційних послуг, класифікацію пакетів, маркування пакетів та управління інтенсивністю трафіку, політикою розподілу ресурсів, політикою попередження перевантаження і політикою відкидання пакетів, якістю обслуговування в мережах MPLS, перерозподілои потоків в мережах MPLS, класами обслуговування IntServ, протоколом RSVP, механізмом обслуговування DiffServ, підтримкою механізмів QoS в віртуальних приватних мережах MPLS.

ЗМІСТ

ПЛАН НАВЧАННЯ

Кількість лекцій: 12.
Кількість практичних занять: 5
Кількість семінарський занять: 5
Модулів: 2
Підсумковий контроль: дифзалік.

ЧАСТИНА 1
МОДУЛЬ 1
ТЕМА 1
АРХІТЕКТУРА ТА ПРИНЦИПИ ФУНКЦІОНУВАННЯ СТЕКУ ПРОТОКОЛІВ TCP/IP

ЛЕКЦІЯ 1
ЗАНЯТТЯ 1
ЗАГАЛЬНІ ПОНЯТТЯ ПРО АРХІТЕКТУРУ СТЕКУ ПРОТОКОЛІВ TCP/IP. ПРОТОКОЛИ КАНАЛЬНОГО, МЕРЕЖНОГО, ТРАНСПОРТНОГО ТА ПРИКЛАДНОГО РІВНІВ

§1. Мета та задачі курсу

§2. Загальні поняття про архітектуру стеку протоколів TCP/IP

§3. Протоколи канального, мережного, транспортного та прикладного рівнів

§4. Основи та структура міжмережної взаємодії

§5. Протоколи ARP та RARP

Завдання на СРС

1. Вивчення стеку протоколів TCP/IP

2. Поглиблене вивчення протоколів канального рівня

ЛЕКЦІЯ 2
ЗАНЯТТЯ 2
ПРОТОКОЛИ ТРАНСПОРТНОГО РІВНЯ

§1. Алгоритм функціонування протоколу UDP. Формат UDP-повідомлення

§2. Інкапсуляція і розділ за рівнями

§3. Алгоритм функціонування протоколу TCP

§4. Забезпечення надійності доставки пакетів

Завдання на СРС

1. Поглиблене вивчення протоколів транспортного рівня

ЛЕКЦІЯ 3
ЗАНЯТТЯ 3
ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ ПРОТОКОЛУ TCP

§1. Механізм ковзаючого вікна

§2. Вікна змінного розміру та управління потоком

§3. Формат TCP-сегменту

§4. Алгоритм Карна і корегування тайм-слоту

Завдання на СРС

1. Вивчення протоколів прикладного рівня

ПРАКТИЧНЕ ЗАНЯТТЯ 1
ЗАНЯТТЯ 4
ОЦІНКА ПРОДУКТИВНОСТІ ФУНКЦІОНУВАННЯ ТРАНСПОРТНИХ ПРОТОКОЛІВ

§1. Формування логічного каналу

§2. Визначення характеристик продуктивності елементу мережі

Завдання на СРС:

1. Провести розрахунок для заданих начальних умов

ЧАСТИНА 2
ТЕМА 2
АРХІТЕКТУРА ТА ПРИНЦИПИ ФУНКЦІОНУВАННЯ ТЕХНОЛОГІЇ IP/MPLS

В этой теме мы изучим новый принцип передачи пакетов; проведем сравнительный анализ обычных технологий и многопротокольной коммутации по метке (Multiprotocol Label Switching — MPLS), которая в настоящее время используется в сетях операторов связи и провайдеров служб.

Технология MPLS является движущей силой развития IP-сетей, включая глобальную сеть Internet. MPLS предоставляет в распоряжение Internet новый принцип передачи пакетов, который влияет на перераспределение потоков данных и на реализацию виртуальных частных сетей (Virtual Private Network — VPN).

В этой теме также выясним, что такое MPLS-коммутация строчки зрения усовершенствованного метода передачи пакетов по сети с использованием информации, содержащейся в метке, которая назначается IP-пакету; проведем сравнительный анализ MPLS, IP и ATM.

MPLS представляет собой технологию, на основе которой в работают IP-сети, включая сеть Internet. Среда MPLS использует новый принцип передачи пакетов для сети Internet, влияющий на перераспределение потоков и на реализацию частных виртуальных сетей (Virtual Private Network — VPN).

Технология MPLS является усовершенствованным методом передачи пакетов по сети с использованием информации, содержащейся в метках, включенных в IP-пакет, ATM-ячейку или фрейм второго уровня.

Коммутация по метке позволяет маршрутизаторам и коммутаторам ATM с функциями MPLS принимать решение об отправке пакетов путем анализа содержимого простой метки, вместо использования сложного алгоритма поиска маршрутов, основанного на IP-адресе получателя.

Технология MPLS позволяет операторам связи и провайдерам служб предложить пользователям такие службы, как VPN-сети 3-го уровня и перераспределение потоков данных в магистральной сети с использованием обшей инфраструктуры без необходимости шифрования или использования приложений конечного пользователя.

Применение технологии MPLS оказывает влияние как на механизм отправки IP-пакетов, так и на выбор маршрута и привело к фундаментальному изменению структуры сети Internet.

ЛЕКЦІЯ 4
ЗАНЯТТЯ 5
ПРИНЦИПИ ПОБУДОВИ АРХІТЕКТУРИ MPLS

§1. Принципи функціонування середовища MPLS

В данном параграфе мы рассмотрим принцип работы среды MPLS. Изучим работу сетей, использующих коммутацию MPLS, и обсудим преимущества технологии MPLS по сравнению с обычной пересылкой пакетов на третьем уровне.

Для пересылки пакетов в сетях MPLS используются метки. Входной узел MPLS причисляет пакет к определенному классу эквивалентности при пересылке (Forwarding Equivalence Class — FEC) лишь один раз — в момент поступления пакета в сеть.

Класс FEC, к которому причисляется пакет, кодируется коротким значением фиксированной длины, называемом меткой (label). Метки присваиваются пакетам до отправки. На последующих транзитных узлах анализ заголовка сетевого уровня не производится. Метка используется как индекс позиции в таблице, которая указывает адрес следующей транзитной точки перехода и новую метку. Существующая метка заменяется новой, и пакет отправляется к следующему устройству.

В сетях MPLS передача пакетов управляется метками. Такой механизм предоставляет ряд описанных ниже преимуществ по сравнению с обычной пересылкой данных за счет функций сетевого уровня.

• В MPLS-сетях пересылка пакетов выполняется коммутаторами, которые выполняют поиск меток и их замену, но не могут анализировать заголовки сетевого уровня. Коммутаторы ATM выполняют аналогичную функцию путем коммутации ячеек, основанной на значениях идентификаторов VPI/VCI, находящихся в ATM-заголовке. Если значения VPI/VCI заменены значениями меток, то ATM-коммутаторы могут отправить эти ячейки, основываясь на значениях меток. ATM-коммутаторы необходимо контролировать с помощью основанных на технологий IP управляющих элементов среды MPLS, таких как контроллер коммутации по меткам (Label Switch Controller — LSC). Такой подход является основой интеграции технологий IP и ATM с использованием средств технологии MPLS.

• Пакет причисляется к определенному классу FEC при поступлении в сеть. Входной маршрутизатор может использовать любую информацию, которую он имеет о пакете, например входной порт или интерфейс, даже если необходимая информация не может быть получена из заголовка сетевого уровня. Пакет, который поступает в сеть через маршрутизатор, может получить иную метку, чем такой же пакет, поступающий в сеть через другой маршрутизатор. В результате такого подхода принимаемое решение об отправке зависит от входного маршрутизатора. При обычной пересылке данных это сделать невозможно, поскольку идентификационные данные маршрутизатора, являющегося входным для пакета, не передаются вместе с самим пакетом. Например, пакеты, прибывающие на различные интерфейсы, подсоединенные к CPE-маршрутизаторам пользователя, могут быть причислены к различным классам FEC. При этом назначаемые метки представляют соответствующие значения FEC. На основе этого построены виртуальные частные сети MPLS (MPLS Virtual Private Networks).

• В сетях с перераспределением потоков данных пакеты могут быть

принудительно отправлены по заданному маршруту, например по недогруженному маршруту. Необходимый маршрут явным образом выбирается до поступления пакета в сеть, а не с помощью обычного алгоритма динамической маршрутизации при перемещении пакета по сети. При использовании технологии MPLS метка может быть использована для представления маршрута, поэтому нет необходимости в передаче явных идентификационных данных маршрута вместе с пакетом. Эта функция лежит в основе перераспределения потоков MPLS.

• "Класс обслуживания" пакета может быть определен входным узлом MPLS. После этого входной узел MPLS может применять к пакетам разные пороги отбрасывания или методы установки очередности. Устройства последующих транзитных переходов могут расширить стратегию службы, используя разные правила поведения на транзитных переходах (Per-Hop Behavior — PHB). MPLS позволяет (но не требует) включать в содержимое метки приоритет или класс обслуживания. В этом случае метка представляет собой комбинацию записи FEC и приоритета в очереди или класса обслуживания. Данная функция образует основу качества обслуживания MPLS (Quality of Service — QoS).

§2. Структура мережного елементу середовища MPLS

В данном параграфе мы ознакомимся со структурой узлов MPLS, в качестве которых могут выступать маршрутизаторы, обладающие функциями MPLS, и коммутаторы ATM.

Узлы MPLS включают в себя плоскость управления и плоскость пересылки, детальное рассмотрение которых посвящены следующие параграфы.

Узлы MPLS имеют две структурных плоскости: плоскость пересылки и плоскость управления. В дополнение к коммутации пакетов, снабженных метками, узлы MPLS могут осуществлять маршрутизацию 3-го уровня или коммутацию 2-го уровня. На рис. 3.1 показана базовая структура узла MPLS.

Рисунок 3.3 - Информационная база пересылки по меткам (LFIB)

Плоскость пересылки пакетов технологии MPLS отвечает за перенаправление пакетов в соответствии со значениями, содержащимися в присоединенных метках. Плоскость пересылки пакетов использует информационную базу пересылки по меткам (Label Forwarding Information Base — LFIB), поддерживаемую узлом MPLS, для дальнейшей передачи помеченных пакетов. Алгоритм с коммутацией по метке, реализуемый этой плоскостью, использует информацию, содержащуюся в базе LFIB, а также информацию, которая содержится в значении метки. Каждый узел MPLS поддерживает две таблицы, относящиеся к пересылке информации MPLS: информационную базу меток (Label Information Base — LIB) и базу LFIB. База LIB содержит все метки, назначенные локальным MPLS-узлом, и таблицы преобразований этих меток в метки, полученные от соседних узлов в сети MPLS. База LFIB использует метки, содержащиеся в базе LIB, для пересылки пакетов.

Плоскость управления технологии MPLS отвечает за формирование и поддержку базы LFIB. Все узлы среды MPLS должны использовать протокол маршрутизации IP для обмена соответствующей информацией маршрутизации с другими узлами MPLS сети. Узлы среды ATM с функциями MPLS используют внешний контроллер коммутации по меткам (Label Switch Controller — LSC), например маршрутизатор серии 7200 или 7500, или встроенный модуль обработки маршрутов (Route Processor Module — RPM) для того, чтобы участвовать в процессе IP-маршрутизации.

Елементи MPLS

Глубокое знание элементов среды MPLS позволяет понять взаимодействие коммутации MPLS с протоколами и устройствами 2-го и 3-го уровней. Ниже обсуждаются следующие элементы MPLS:

• маршрутизатор, осуществляющий коммутацию по меткам (Label-Switched Router — LSR);

• маршрут, на котором выполняется коммутация по метке (Label-Switched Path - LSP);

• протокол распространения меток (Label Distribution Protocol — LDP).

Маршрутизатор, що виконує комутацію за мітками (LSR)

LSR (Label-Switched Router) представляет собой устройство, выполняющее функции управления и отправки при использовании MPLS-коммутации. LSR-устройство пересылает пакет, основываясь на значении метки, инкапсулированном в пакете. Маршрутизатор LSR может также пересылать обычные пакеты третьего уровня.

В качестве LSR-устройств могут выступать маршрутизаторы, выполняющие MPLS-коммутацию, или ATM-коммутаторы, обладающие функциями MPLS и использующие метки для отправки данных. Пакетные LSR-устройства легко могут быть созданы путем загрузки образа IOS с набором функций MPLS на обычный маршрутизатор. LSR-устройства MPLS в сети ATM могут быть созданы с помощью коммутатора ATM с интегрированным программным обеспечением MPLS или путем добавления функций MPLS с использованием внешнего контроллера LSC. Фундаментальной основой коммутации по меткам является то, что LSR-устройства согласуют свои действия в .отношении меток, используемых для передачи данных. Такое согласование осуществ-^ляется путем использования протокола

распространения меток или расширений протоколов PIM, BGP, RSVP или CR-LDP.

Граничные LSR-устройства находятся в точках присутствия провайдеров (Point Of Presence — POP) на границах сети MPLS и назначают пакетам метки (или стеки меток). Привязка меток или внедрение их в начало пакета также называются "вставкой" (push) меток. Граничные устройства LSR также вставляют или удаляют метки в точке выхода пакетов из MPLS-домена, что называется "вытеснением" (pop) метки. Граничные LSR-устройства могут также выполнять обычные функции пересылки пакетов по протоколу IP.

Действия, которые могут выполняться LSR-устройствами над помеченными пакетами, перечислены в табл. 3.2.

Таблица 3.2.

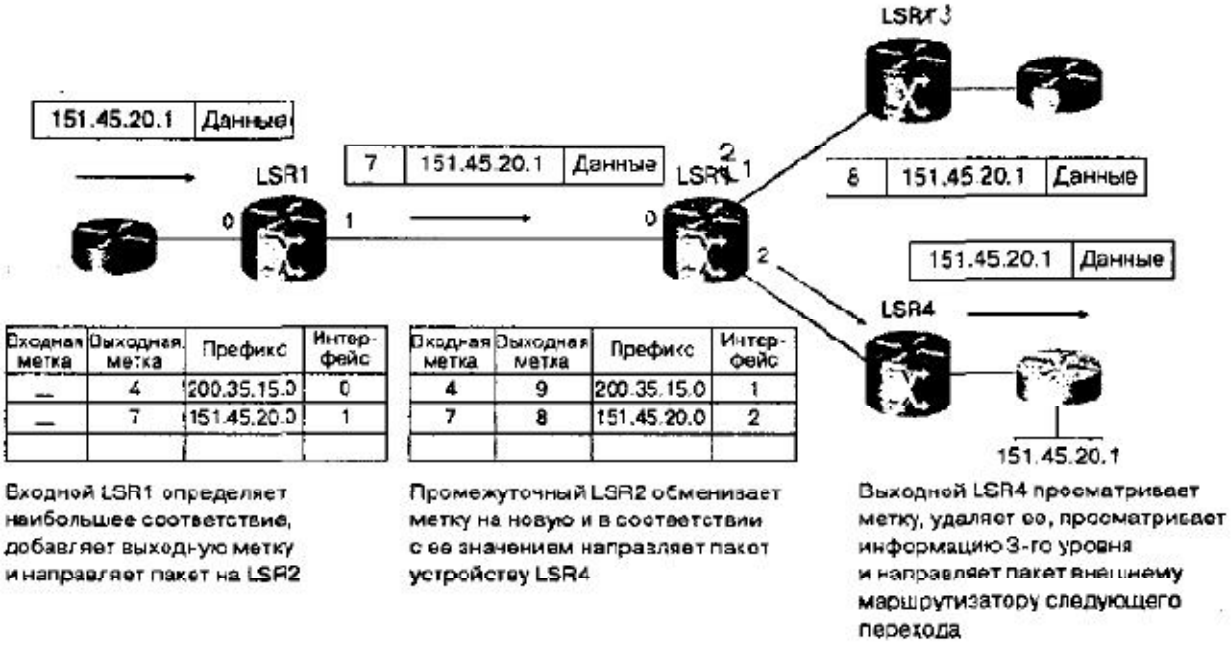
Действия над метками

Действие	Описание
Агрегирование	Удаляет верхнюю метку стека и выполняет поиск информации 3-го уровня
Вытеснение	Удаляет верхнюю метку стека и передает полезную нагрузку пакета в виде IP-пакета с меткой или без нее
Вставка	Заменяет верхнюю метку стека набором меток
Замена	Заменяет верхнюю метку стека другим значением
Удаление тега	Удаляет верхнюю метку и направляет IP-пакет по указанному адресу следующего IP-перехода

Принцип роботи пакетних LSR-пристроїв

Для передачи пакетов третьего уровня по сети, работающей на основе маршрутизаторов, пакетная технология MPLS использует принцип передачи пакетов по меткам.

Основные функции пакетной среды MPLS по поддержке одноадресатной маршрутизации с одноуровневым стеком меток показаны на рис. 3.4. Устройство LSR1 выполняет функции граничного маршрутизатора LSR. Оно присваивает пакету первоначальную метку после применения алгоритма наибольшего соответствия к заголовку IP и назначения пакету класса FEC. В случае использования технологии VPN на выбор класса FEC могут также влиять такие параметры, как номер входного интерфейса или заранее заданное правило перераспределения потоков. Назначение пакету класса FEC происходит лишь один раз — при поступлении пакета в сеть.



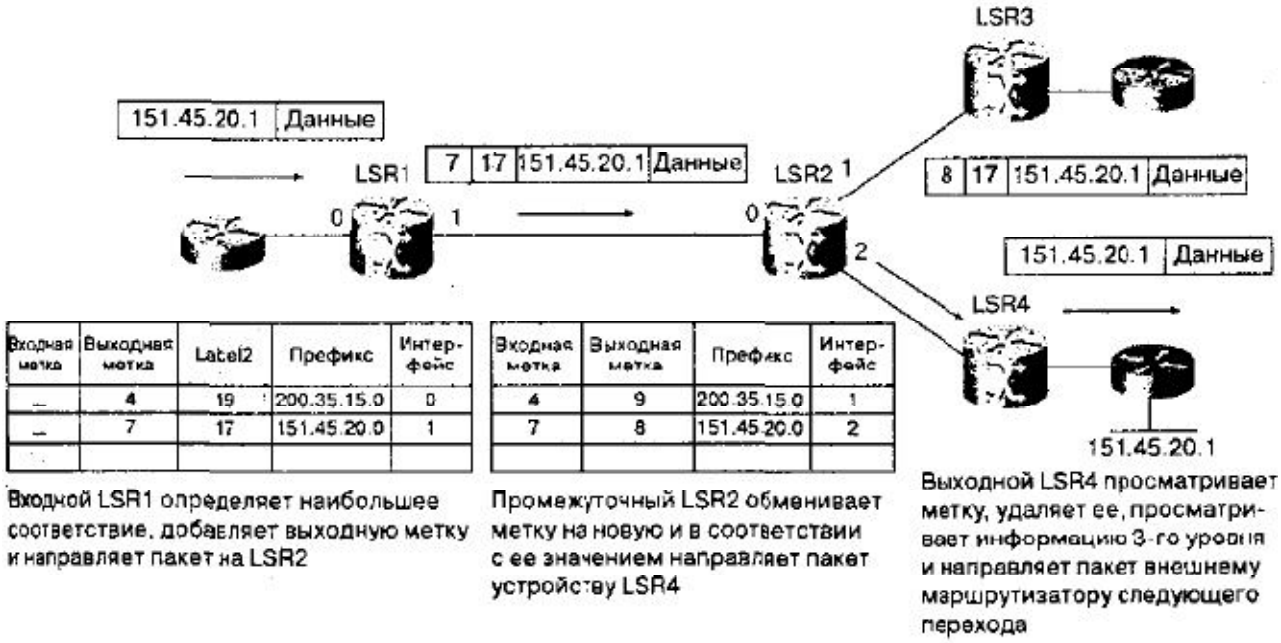
Входная метка	Выходная метка	Префикс	Интерфейс
—	4	200.35.15.0	0
—	7	151.45.20.0	1

Входная метка	Выходная метка	Префикс	Интерфейс
4	9	200.35.15.0	1
7	8	151.45.20.0	2

Рисунок 3.4 - Функции LSR-устройств для одноуровневого стека меток

Каждому классу FEC соответствует определенная метка. После того как пакету присвоена метка, последующие LSR-устройства направляют его далее, используя только эту метку. LSR-устройство обычно заменяет метку на входящем пакете новым значением в тот момент, когда передает этот пакет дальше. На выходе из сети устройство LSR4 просматривает метку, удаляет ее, выполняет анализ информации 3-го уровня и направляет пакет на внешний маршрутизатор следующего транзитного перехода.

На рис. 3.5 показаны операции LSR-устройсгв с пакетами при наличии в стеке нескольких уровней меток. Устройство LSR1 выполняет функции граничного маршрутизатора LSR. Оно назначает пакету первоначальный набор меток после применения обычного алгоритма наибольшего соответствия к IP-заголовку и определяет для пакета класс FEC Промежуточное устройство LSR2 удаляет верхнюю метку стека "7" и заменяет ее меткой со значением "8". На выходе из сети устройство LSR4 просматривает метки, удаляет метку, анализирует информацию третьего уровня и направляет пакет на внешний маршрутизатор следующего транзитного перехода.



Входная метка	Выходная метка	Label2	Префикс	Интерфейс
–	4	19	200.35.15.0	0
–	7	17	151.45.20.0	1

Входная метка	Выходная метка	Префикс	Интерфейс
4	9	200.35.15.0	1
7	8	151.45.20.0	2

Рисунок 3.5 - Операции LSR-устройств над пакетами в aiynae многоуровневого стека меток

<u>Видалення мітки на передостіннім переході</u>

Операции LSR-устройств над пакетами, которые описаны в предыдущем разделе, имеют определенные недостатки, связанные с тем, что на выходном устройстве LSR4 осуществляется двойной поиск. Маршрутизатору LSR4 требуется просмотреть стек меток и сравнить значение метки со значениями базы LFIB только для того, чтобы выяснить, что метку следует удалить. После этого ему необходимо просмотреть информацию 3-го уровня в своей глобальной таблице маршрутизации или в таблице маршрутизации, связанной с конкретной VPN-сетью, для того, чтобы правильно направить пакет на внешний маршрутизатор следующего перехода. Двойной анализ информации на устройстве LSR4 снижает производительность и приводит к сложностям в аппаратной реализации MPLS в специализированных интегральных микросхемах ASIC, используемых в наиболее современных многоуровневых коммутаторах.

Для удаления метки на предпоследнем транзитном переходе граничное устройство LSR4 (рис. 3.6) запрашивает операцию по вытеснению метки у следующего на маршруте соседнего устройства LSR2 с использованием протокола LDP или TDP и специальной неявной нулевой метки (implicit-null label). Эта метка имеет значение 3 для протокола LDP и J для TDP.

Маршрутизатор LSR2 удаляет метку перед тем как отправить пакет, содержащий только IP-информацию, на устройство LSR4. После этого устройство LSR4 выполняет анализ информации 3-го уровня, основываясь на адресе получателя, содержащемся в пакете, и направляет пакет соответственно в локальную подсеть или на внешний маршрутизатор следующего перехода.

Внимание!

Удаление метки на предпоследнем переходе необходимо только для непосредственно подсоединенных подсетей или агрегированных маршрутов, поскольку номер выходного интерфейса 2-го уровня может быть получен из записи метки в базе LFIB.

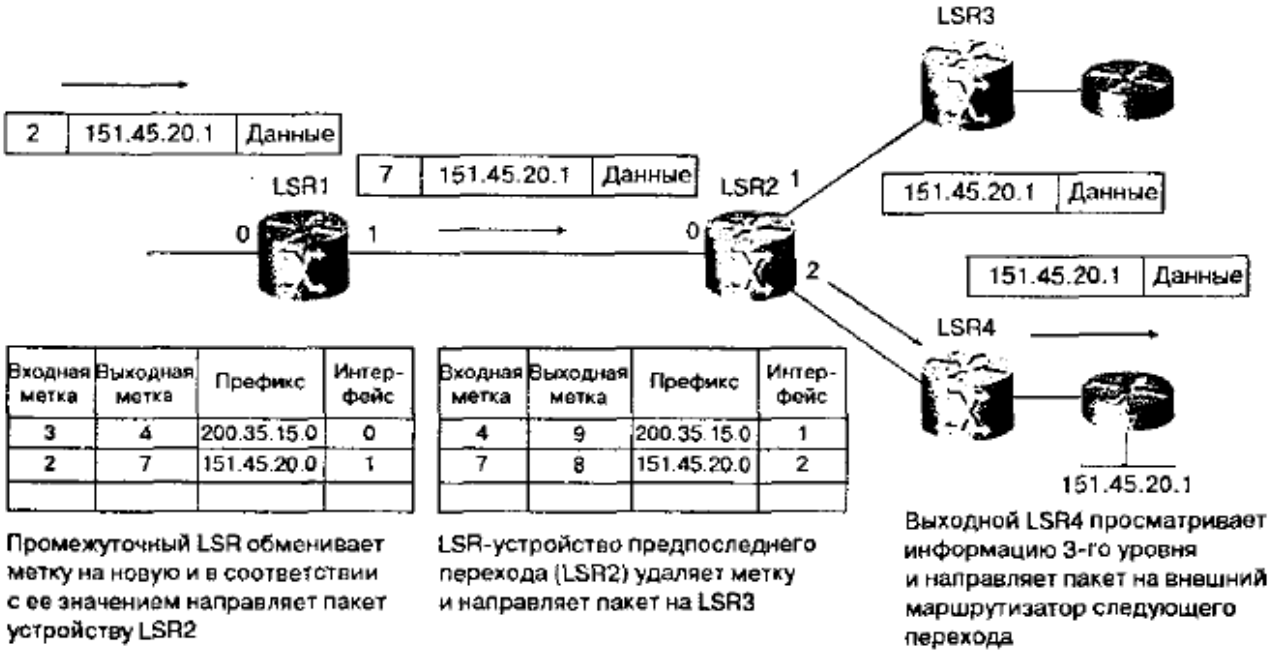


Рисунок 3.6 - Вытеснение метки на предпоследнем переходе

§3. Площина передавання пакетів

В данном параграфе мы опишем элементы, образующие сеть MPLS. Подробно рассматрим MPLS-маршрутизаторы с коммутацией по метке (Label-Switched Router — LSR), механизмы создания маршрута с коммутацией по метке (Label-Switched Path — LSP) и работу протокола распространения меток (Label Distribution Protocol — LDP).

Плоскость пересылки пакетов технологии MPLS отвечает за перенаправление пакетов в соответствии со значениями, содержащимися в присоединенных метках. Плоскость пересылки пакетов использует информационную базу пересылки по меткам (Label Forwarding Information Base — LFIB), поддерживаемую узлом MPLS, для дальнейшей передачи помеченных пакетов. Алгоритм с коммутацией по метке, реализуемый этой плоскостью, использует информацию, содержащуюся в базе LFIB, а также информацию, которая содержится в значении метки. Каждый узел MPLS поддерживает две таблицы, относящиеся к пересылке информации MPLS: информационную базу меток (Label Information Base — LIB) и базу LFIB. База LIB содержит все метки, назначенные локальным MPLS-узлом, и таблицы преобразований этих меток в метки, полученные от соседних узлов в сети MPLS. База LFIB использует метки, содержащиеся в базе LIB, для пересылки пакетов.

Рисунок 3.3 - Информационная база пересылки по меткам (LFIB)

Мітка в мережі MPLS

Метка представляет собой 32-битовый идентификатор фиксированной длины, используемый для идентификации класса FEC и обычно имеющий локальное значение. Метка, назначаемая пакету, указывает класс FEC, к которому причислен пакет.

В ATM-сетях метка размещается в полях VCI или VPI заголовка ATM. Однако, если фрейм относится к типу Frame Relay, метка размещается в поле DLCI заголовка Frame Relay.

Технологии 2-го уровня, такие как Ethernet, Token Ring, FDDI и каналы "точка-точка", не могут использовать адресные поля второго уровня для переноса меток. Эти технологии переносят метки во вспомогательных промежуточных заголовках. Промежуточный заголовок для метки вставляется между заголовками канального и сетевого уровня, как показано на рис. 3.2. Использование промежуточного заголовка позволяет поддерживать средства MPLS в большинстве технологий второго уровня.

Для поддержки вспомогательных заголовков требуется, чтобы отправляющий маршрутизатор мог сообщить принимающему о том, что фрейм содержит промежуточный заголовок. В различных технологиях это осуществляется разными способами. В сетях Ethernet для указания на присутствие промежуточного заголовка используются значения поля типа 0x8847 и 0x8848. Значение 0x8847 указывает на то, что фрейм переносит одноадресатный MPLS-пакет, а значение 0x8848 используется для уведомления о том, что фрейм переносит MPLS-пакет многоадресатной рассылки. В сетях Token Ring и FDDI информация помещается в поле "тип пакета" заголовка SNAP.

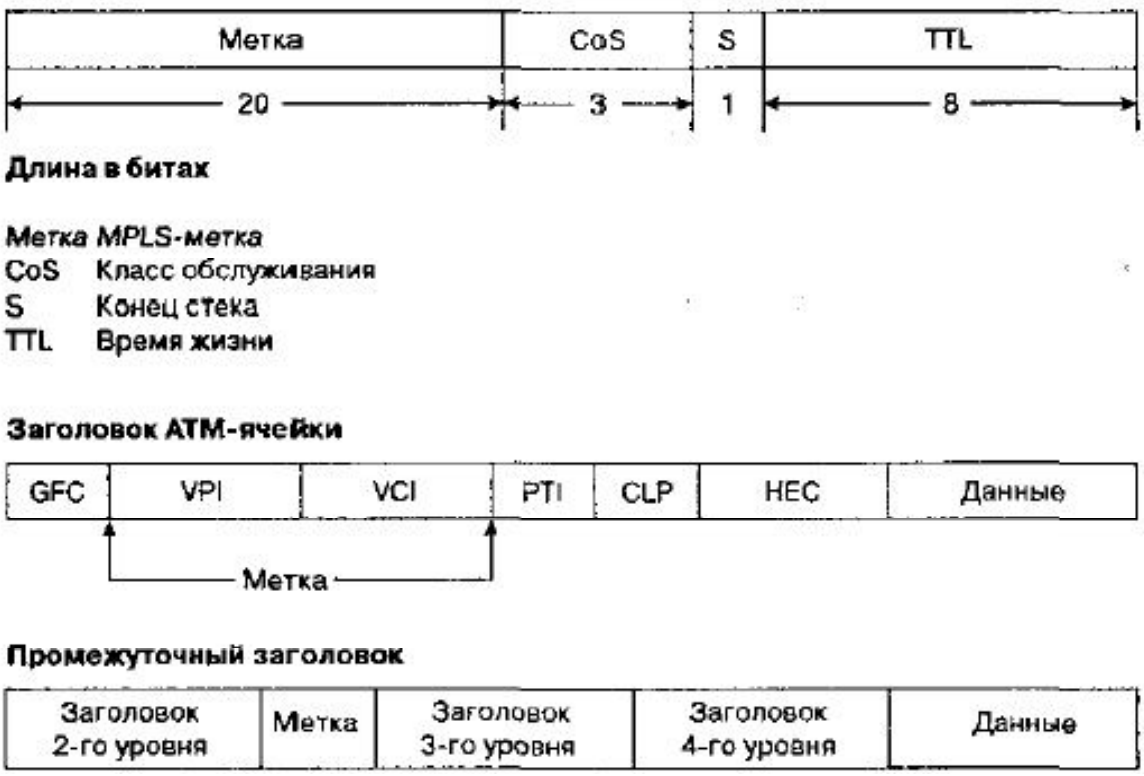


Рисунок 3.2 - Форматы меток MPLS

Протокол в рассматриваемой среде PPP использует модифицированный протокол управления сетью (Network Control Program — NCP), известный как управляющий протокол MPLS (MPLS Control Protocol — MPLSCPj, и помечает все пакеты, содержащие промежуточный заголовок, значением 0x8281 в поле протокола PPP. Протокол Frame Relay для указания фреймов, имеющих вспомогательные заголовки, использует идентификатор (ID) протокола сетевого уровня (Network Layer Protocol ID — NLPID) полей SNAP и SNAP-заголовок, в котором в поле типа стоит значение 0x8847. PVC-каналы стандарта Форума ATM используют для этой цели SNAP-заголовок со значениями в поле типа 0x8847 и 0x8848. В табл. 3.1 перечислены зарезервированные значения меток.

Метка MPLS содержит приведенные ниже поля:

• 20-битовое поле метки (Label field). В этом поле находится текущее значение MPLS-метки.

• 3-битовое поле класса обслуживания (CoS field). Это поле задает алгоритмы назначения очередности и отбрасывания, применяемые к пакету при его передаче по сети.

• 1-битовое поле стека (Stack field). Поддерживает иерархический стек меток;

• 8-битовое поле времени существования (time-to-live field —field). Выполняет функцию обычного поля TTL протокола IP.

Внимание!

MPLS-узлы сетей ATM пересылают метки в полях VCI или VPI/VCI заголовка ATM. Поля CoS, стека и TTL не поддерживаются. Однако функции качества обслуживания и обнаружения кольцевых маршрутов доступны и могут быть реализованы с использованием механизмов ATM.

Таблица 3.1.

Зарезервированные значения меток

Значение метки	Описание
0	Явно заданная нулевая метка протокола IPv4. Это значение метки допускается только в конце стека меток. Оно указывает на то, что метка должна быть удалена, а дальнейшая пересылка пакета должна осуществляться на основе заголовка протокола IPv4
1	Метка предупреждения маршрутизатора. Аналогична параметру "предупреждение маршрутизатора" (router alert) в IP-пакетах. Такая метка может использоваться в любой позиции стека, кроме последних записей
2	Явно заданная нулевая метка протокола IPv6. Это значение метки указывает на то, что она должна быть удалена, а дальнейшая пересылка пакета должна осуществляться на основе заголовка протокола IPv6
3	Неявно заданная нулевая метка. Такую метку узел MPLS может назначать и распространять, но для реальной инкапсуляции она никогда не применяется. Такая нулевая метка используется на предпоследнем транзитном переходе перед ее удалением
4-15	Эти значения зарезервированы для будущего использования

Стек міток

Стековый бит позволяет реализовать хранение меток MPLS в стеке; при этом IP-пакету может быть назначено более одной метки. Для указания конца стека соответствующий бит устанавливается в 1. Всем остальным битам стека задается значение 0. При использовании MPLS для коммутации пакетов начало стека находится сразу после заголовка канального уровня, а конец — непосредственно перед заголовком сетевого уровня. Пересылка пакетов осуществляется с использованием значения метки в начале стека. При одиночной рассылке пакетов IP-маршрутизация не использует размещение меток в стеке, однако VPN-сети MPLS и перераспределение потоков используют такой подход.

Поле часу існування пакету (TTL)

Папе TTL аналогично полю времени существования пакета (time-to-live), используемому в заголовке IP. Узел MPLS просто обрабатывает поле TTL в верхней позиции стека меток. TTL-поле протокола IP содержит значение TTL в версии IPv4 или параметр ограничения количества транзитных переходов (Hop Limit field) в версии IPv6 — в зависимости от того, какое из них применимо в конкретной ситуации.

Внимание!

Более подробно поля меток MPLS описаны в спецификации RFC 3032, а также в пособии "Коды стека меток MPLS" Е. Розена ("MPLS Label Stack Encoding", E. Rosen,

январь 2001).

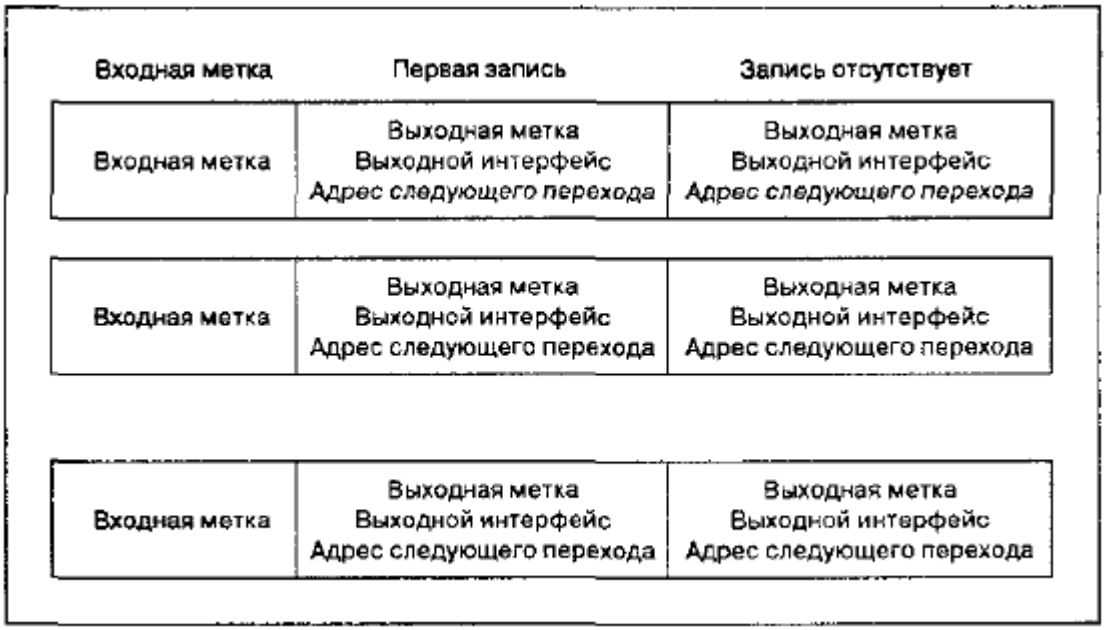
Внимание!

Технология Ethernet поддерживает максимальный размер блока передачи (Maximum Transmission Unit— MTU) равный 1518 байт. Устройства корпорации Cisco поддерживают двухуровневый стек меток, состоящий из 64 бит или 8 октетов за счет увеличения размера параметра MTU технологии Ethernet до 1526 байт. Однако в этом случае коммутаторы второго уровня также должны быть сконфигурированы для передачи "гигантских" (giant) фреймов. Другим вариантом является использование механизма поиска маршрута MTU (Path MTU Discovery), описанного в спецификации RFC 1191.

Інформаційна база міток при пересиланні

Информационная база пересылки меток (Label Forwarding Information Base — LFIB), поддерживаемая узлом MPLS, состоит из последовательных записей. Как показано на рис. 3.3, каждая запись состоит из входной метки и одной или более вложенных записей. В базе LFIB создаются индексы по значениям, содержащимся во входной метке.

Каждая вложенная запись состоит из выходной метки, номера выходного интерфейса и адреса следующего транзитного перехода. Запись внутри другой записи может иметь такие же или иные выходные метки. При многоадресатной пересылке требуются вложенные записи с несколькими выходными метками, поскольку поступающий на интерфейс пакет должен быть разослан на несколько выходных интерфейсов. Кроме выходной метки, выходного интерфейса и данных о следующей транзитной точке перехода, запись в таблице отправки может содержать информацию, связанную с такими используемыми пакетом ресурсами, как выходная очередь, в которую он должен быть помещен.



Структура информационной базы пересылки по меткам (LFIB)

Рисунок 3.3 - Информационная база пересылки по меткам (LFIB)

Узел MPLS может поддерживать одну таблицу пересылки пакетов, таблицу пересылки для каждого из своих интерфейсов или комбинацию таких таблиц. Если

используется несколько таблиц, пакеты пересылаются на основе значения входной метки и на основе входного интерфейса, на который поступает пакет.

Алгоритм пересилання за міткою

Коммутаторы меток используют алгоритм пересылки пакетов, основанный на обмене меток. Узлы MPLS, которые поддерживают одну базу LFIB, изшгекают значения меток из соответствующих полей входных пакетов и используют это значение в качестве индекса для таблицы LFIB, После того как обнаружено соответствие входной метки, узел MPLS заменяет метку в пакете выходной меткой из вложенной записи и отправляет пакет на указанный выходной интерфейс к следующему транзитному переходу. Если шюженная запись задает выходную очередь, то узел MPLS размещает пакет в указанной очереди.

Если узел MPLS поддерживает несколько баз LFIB для каждого из интерфейсов, то для выбора базы LFIB, с помощью которой будет перенаправляться пакет, используется физический интерфейс, на который он прибыл.

В обычных алгоритмах пересылки используется несколько механизмов для одноадре-сатной рассыпки пакетов, многоадресатной рассылки и для одноадресатной рассылки пакетов с установленным набором битов типа обслуживания ToS. Однако технология MPLS использует лишь один алгоритм пересылки данных, основанный на обмене меток.

Узел MPLS может получить всю информацию, которая требуется для отправки пакета, а также определить необходимость резервирования ресурсов, необходимых пакету с однократным доступом к памяти (т.е. таблице). Такие возможности высокоскоростного просмотра меток и пересылки превращают коммутацию по меткам в высокопроизводительную технологию коммутации потоков. Технология MPLS также может быть использована для передачи данных других протоколов третьего уровня (кроме IPv4): IPv6, IPX или AppleTalk. Такая возможность делает MPLS привлекательным средством при переводе сети с протокола IPv4 на IPv6.

§4. Площина управління

Данный параграф посвящен вопросам обнаружения, временного сохранения и предотвращения петель при использовании коммутации MPLS. Рассмотрим возможность возникновения петель маршрутизации в MPLS-сети и опишем различные методы временного сохранения, обнаружения и предотвращения петель в технологии MPLS.

Плоскость управления технологии MPLS отвечает за формирование и поддержку базы LFIB. Все узлы среды MPLS должны использовать протокол маршрутизации IP для обмена соответствующей информацией маршрутизации с другими узлами MPLS сети. Узлы среды ATM с функциями MPLS используют внешний контроллер коммутации по меткам (Label Switch Controller — LSC), например маршрутизатор серии 7200 или 7500, или встроенный модуль обработки маршрутов (Route Processor Module — RPM) для того, чтобы участвовать в процессе 1P-маршрутизации.

При этом могут использоваться протоколы маршрутизации по состоянию каналов, такие как OSPF и IS-IS, поскольку они предоставляют узлу MPLS топологию всей сети, В обычных маршрутизаторах таблица IP-маршрутизации используется для создания кэша быстрой коммутации (Fast Switching cache) или информационной базы пересылки (Forwarding Information Base — FIB), используемой для механизма

экспресс-коммутации корпорации Cisco (Cisco Express Forwarding — CEF). Однако в случае использовании технологии MPLS таблица маршрутизации протокола IP предоставляет информацию о сети получателя и префиксы подсетей, используемые для привязки меток.

Информация о привязке меток может распространяться с помощью протокола распространения меток (Label Distribution Protocol — LDP) или фирменного протокола Cisco — протокола распространения тегов (Tag Distribution Protocol — TDP), а также путем передачи информации о привязке меток в модифицированных высокоуровневых протоколах маршрутизации.

Протоколы маршрутизации по состоянию каналов, например OSPF, распространяют лавинным образом информацию о маршрутизации на маршрутизаторы, которые не обязательно являются смежными, в то время как информация о привязке меток распространяется только среди смежных маршрутизаторов. Такой механизм делает протоколы маршрутизации на основе данных о состоянии каналов неприемлемыми для распространения информации о привязке меток. Однако для достижения цели могут быть использованы расширения протоколов маршрутизации, такие как PIM и BGP. Они позволяют согласовать распространение информации о привязке меток с распространением данных маршрутизации и избежать ситуации, когда узел MPLS принял информацию о метках, не имея соответствующей маршрутной информации. Такой подход также упрощает работу системы, поскольку нет необходимости использовать отдельный протокол, например LDP, для распространения информации о привязке меток.

Метки, которыми обмениваются смежные узлы MPLS, используются для построения базы LFIB. Технология MPLS использует метод пересылки, основанный на замене меток, который может быть объединен с различными управляющими модулями. Каждый такой модуль отвечает за назначение и распространение набора меток и другой управляющей информации. Протоколы внутреннего шлюза (IGP — Interior Gateway Protocol) используются для определения достижимости узла, для привязки и преобразования адресов между классами FEC и адресами следующего транзитного перехода. Управляющие модули MPLS включают в себя:

- модуль маршрутизации для одноадресатной рассылки;
- модуль маршрутизации для многоадресатной рассылки;
- модуль перераспределения потоков;
- модуль виртуальных частных сетей (Virtual Private Network — VPN);
- модуль качества обслуживания (Quality of service — QoS).

Модуль маршрутизації при одноадресатній розсильці

Модуль маршрутизации при одноадресатной рассылке заполняет таблицу FEC, используя такие протоколы внутреннего шлюза (IGP), как OSPF, IS-IS и т.д. Таблица маршрутизации IP используется для обмена информацией о привязке меток со смежными узлами MPLS для подсетей, содержащихся в таблице маршрутизации IP. Обмен информацией о связывании меток осуществляется с помощью протокола LDP или фирменного T DP-протокол а Cisco.

Модуль маршрутизації при багатоадресатній розсильці

Модуль маршрутизации при многоадресатной рассылке создает таблицу FEC с помощью многоадресатных протоколов, таких как многоадресатная рассылка, не

зависящая от протокола (Protocol-Independent Multicast — PIM). В данном случае таблица маршрутизации используется для обмена информацией о привязке меток со смежными узлами MPLS для подсетей, содержащихся в таблице маршрутизации многоадресатной рассылки. Обмен информацией о метках осуществляется с помощью протокола PIM версии 2 с MPLS-расширениями.

Модуль перерозподілу потоків

Модуль перераспределения потоков позволяет указать в сети явно заданные маршруты коммутации по метке с целью перераспределения потоков. Этот модуль использует идентификаторы туннелей MPLS и расширения протоколов маршрутизации IS-IS или OSPF для построения таблиц FEC. Обмен информацией о привязке меток осуществляется с помощью протокола резервирования ресурсов (Resource Reservation Protocol — RSVP) или маршрутизации на основе протокола CR-LDP (Constraint-based Routing LDP), который представляет собой набор расширений LDP, позволяющих выполнять в сетях MPLS маршрутизацию, основанную на ограничениях.

Модуль віртуальної приватної мережі (VPN)

Модуль VPN использует таблицы маршрутизации каждой VPN-сети для построения таблиц FEC, которые создаются с помощью протоколов маршрутизации, используемых между маршрутизаторами CPE и граничными MPLS-узлами провайдера служб. Обмен информацией о привязке меток к таблицам маршрутизации VPN-сетейосуществляется с помощью расширенного мультипротокольного механизма BGP в сети провайдера службы.

Модуль якості обслуговування

Модуль QoS (Quality of Service) создает таблицу классов FEC с использованием обычного протокола внутреннего шлюза (ЮР), такого как OSPF, IS-IS или аналогичного. Таблица IP-маршрутизации используется для обмена информацией о привязке меток к смежным узлам MPLS для подсетей содержащихся внутри таблицы маршрутизации IP. Обмен информацией о метках осуществляется с использованием расширений протокола LDP или с помощью фирменного протокола корпорации Cisco — TDP.

Завдання на СРС

1. Порівняння технології MPLS з технологіями IP та ATM

Сравним MPLS с традиционным совмещением технологий IP и ATM.

При интеграции с коммутаторами ATM коммутация по метке приобретает преимущества аппаратного обеспечения коммутаторов, оптимизированных для использования фиксированной длины ячеек ATM и их коммутации с большой скоростью. В сетях с несколькими службами коммутация по метке позволяет коммутаторам BPX/MGX обеспечивать службы ATM, Frame Relay и Internet IP на одной платформе с высокой степенью расширяемости. Поддержка всех служб на одной платформе обеспечивает уменьшение операционных расходов и упрощает работу с провайдерами нескольких служб.

В магистралях сетей с коммутаторами ATM благодаря коммутации по метке маршрутизаторы Cisco BPX 8600, MGX 8800, коммутирующий маршрутизатор Cisco 8540 с несколькими службами и другие коммутаторы ATM Cisco обеспечивают

высокоуправляемую работу сети с большей расширяемостью, чем при простом наложении технологии IP на сеть ATM. Коммутация по метке позволяет избежать проблем, связанных с расширением сети и использованием большого количества одноранговых маршрутизаторов, и обеспечивает поддержку иерархической структуры внутри сети 1SP.

Інтеграція

При использовании в среде ATM коммутация MPLS интегрирует функции IP и ATM вместо простого наложения средств IP на сеть ATM. Такой подход делает инфраструктуру ATM "видимой" для IP-маршрутизации и устраняет необходимость в приближенном отображении функций IP и ATM. Коммутация MPLS не требует адресации ATM и таких методов маршрутизации, как PNNI, хотя они и могут быть при необходимости использованы параллельно.

Підвищення надійності

В распределенных сетях, которые основаны на инфраструктуре ATM, коммутация MPLS представляет собой простое решение для интеграции маршрутизируемых протоколов с сетью ATM. При традиционном наложении технологии IP на среду ATM необходимо создание полносвязной топологии PVC-каналов между соседними маршрутизаторами в среде ATM. Однако при этом возникает ряд проблем, обусловленных методом, с помощью которого каналы PVC между маршрутизаторами накладываются на сеть ATM. Такой подход делает структуру сети ATM невидимой для маршрутизаторов. Выход из строя одного канала ATM может вызвать разрыв нескольких каналов между маршрутизаторами, что создает серьезные проблемы ввиду большого количества обновлений маршрутизации и необходимости их последующей обработки.

Не требуя тонкой настройки весовых коэффициентов маршрутизации, все PVC-каналы "видны" процессам маршрутизации IP как маршруты единичных переходов с одной и той же оценкой доверительности. Такая ситуация может привести к неэффективной маршрутизации в сети ATM.

Безпосередня реалізація класів обслуговування

При использовании совместно с аппаратным обеспечением ATM коммутация MPLS позволяет установить очередность и буферизацию ATM для обеспечения различных классов службы. Такой подход позволяет осуществлять прямую поддержку очередности IP и значения CoS на коммутаторах ATM без сложной трансляции их в классы обслуживания форума ATM.

Ефективне використання багатоадресної пересилки і технологія RSVP

В противоположность технологии MPLS наложение протоколов IP на среду ATM имеет серьезные недостатки, особенно в вопросе поддержки усовершенствованных служб IP, таких как многоадресатная рассылка IP и использование протокола резервирования ресурсов (Resource Reservation Protocol — RSVP). Поддержка обеих служб требует больших затрат времени и усилий в органах, управляющих стандартами и реализацией; в результате чего взаимное отображение функций IP и ATM часто является приближенным.

Масштабованість служб VPN та керованість

Технология MPLS может сделать службы частных виртуальных сетей IP высокорасширяемыми и легкими в управлении. Службы VPN представляют собой важную службу для обеспечения промышленных сетей частными IP-сетями внутри их инфраструктуры. Когда провайдер ISP предлагает VPN-службу, носитель поддерживает множество индивидуальных сетей VPN на единой инфраструктуре. При использовании магистрали MPLS информация VPN может обрабатываться только в точках входа в сеть и выхода из нее; при этом метки MPLS позволяют передавать пакеты по совместно используемой магистрали в нужную выходную точку. В дополнение к MPLS многопротокольный протокол граничного шлюза (Multiprotocol Border Gateway Protocol — MBGP) используется для обработки информации, связанной с сетями VPN. Комбинация служб MPLS и многопротокольного BGP делает службы VPN, основанные на MPLS, более легкими в управлении; при этом возможны сквозные операции по управлению узлами VPN и принадлежностью отдельных узлов к среде VPN. Такой подход также делает службы VPN, основанные на средствах MPLS, расширяемыми; при этом одна сеть способна поддерживать тысячи сетей VPN.

Зменшення навантаження на басову систему мережі

Службы VPN демонстрируют, как технология MPLS поддерживает иерархию сведений о маршрутизации. Кроме того, они позволяют изолировать таблицы маршрутизации сети Internet от базовых систем сети провайдера службы. Технология MPLS позволяет осуществлять доступ к таблицам маршрутизации сети Internet только на входном и выходном устройствах сети провайдера службы. При использовании средств MPLS транзитные потоки данных, входящие на границе автономной системы провайдера, получают метки, связанные с выходными точками. В результате такой маркировки внутренним транзитным маршрутизаторам и коммутаторам требуется обрабатывать только соединения между граничными маршрутизаторами провайдера, избавляя корневые устройства от обработки значительного объема данных маршрутизации, имеющего место в сети Internet. Такое отделение внутренних маршрутов от маршрутов сети Internet также обеспечивает большую защиту от ошибок, безопасность и улучшает устойчивость работы сети.

Можливість перерозподілу потоків

Технология MPLS позволяет перераспределять потоки, что необходимо для эффективного использования сетевых ресурсов. Перераспределение потоков позволяет перемещать нагрузку с чрезмерно используемых частей сети в недостаточно используемые в соответствии с пунктом назначения потоков данных, типом потоков, нагрузкой, временем суток и т.д.

Висновки

В настоящей главе рассмотрены основы маршрутизации на 3-м уровне и коммутация по метке, а также выполнено подробное сравнение коммутации MPLS и маршрутизации 3-го уровня.

Мультиплексирование с разделением времени объединяет потоки данных путем назначения каждому потоку отдельного временного интервала. TDM регулярно передает фиксированную последовательность канальных интервалов по отдельному

каналу передачи. Frame Relay, X.25 и SMDS представляют собой технологии, использующие коммутацию пакетов, а в среде ATM осуществляется коммутация ячеек.

Функция маршрутизации включает две компоненты: пересылку и управление. При пересылке используется информация, содержащаяся в таблице пересылки и в заголовке 3-го уровня, а управляющая компонента отвечает за построение и поддержку таблицы пересылки данных.

Устройства, осуществляющие коммутацию по метке, назначают пакетам или ячейкам короткую метку фиксированной длины. Коммутирующие механизмы просматривают таблицу отправки для нахождения соответствующего данной метке пункта назначения. В метке обобщается наиболее важная информация об отправке пакета или ячейки. Такая информация содержит адрес получателя, очередность, принадлежность к частной виртуальной сети, требования к качеству обслуживания и маршрут перераспределения потоков для данного пакета или ячейки.

Провайдеры служб ищут способы повышения конкурентоспособности на рынке, предлагая потребителям расширенный спектр услуг, таких как частные виртуальные сети и IP-сети с перераспределением потоков, что легко достигается путем реализации технологии MPLS.

ЛЕКЦІЯ 5
ЗАНЯТТЯ 6
ПРИНЦИПИ КОМУТАЦІЇ В СЕРЕДОВИЩІ MPLS

В данном разделе мы болем подробно рассматрим механизмы создания маршрута с коммутацией по метке (Label-Switched Path — LSP) и работу протокола распространения меток (Label Distribution Protocol — LDP).

§1. Маршрут з комутацією за мітками

Маршрут LSP (Label-Switched Path) представляет собой соединение между двумя устройствами LSR, в которых для отправки пакетов используется коммутация по меткам. Такой маршрут является характерным для среды MPLS способом перемещения потоков данных по сети.

Маршруты LSP создаются с использованием протокола LDP или фирменного Cisco-протокол а TDP, применявшегося до появления соответствующего стандарта, протокола резервирования ресурсов с расширениями для перераспределения потоков (Resource Reservation Protocol with Traffic Engineering extensions — RSVP-TE), маршрутизируемого протокола LDP, основанного на ограничениях (Constraint-based Routed LDP — CR-LDP), или с помощью расширений протоколов маршрутизации, таких как многопротокольный механизм BGP (Multiprotocol BGP).

Внимание!

Для установки маршрута в сети MPLS могут быть использованы протоколы RSVP-TE или CR-LDP. Протокол RSVP-TE работает на базе дейтаграмм UDP, а CR-LDP — на базе пакетов протокола TCP. Хотя в отношении расширяемости, надежности и влияния на работу сети между RSVP-TE и CR-LDP нет особых различий, протокол RSVP-TE все же имеет определенные преимущества перед CR-LDP — он лучше приспособлен к взаимодействию с IP-сетями, поскольку поддерживает интегрированную сигнализацию на всем протяжении маршрута, качество обслуживания и обеспечивает взаимодействие оборудования различных производителей.

Маршрут LSP можно рассматривать как путь через набор LSR-устройств, по которому проходят к получателю пакеты, принадлежащие к одному классу FEC.

Коммутация MPLS позволяет установить иерархию меток, известную как стек меток. Вследствие этого возможно использование различных LSP-маршрутов для различных уровней меток при отправке пакета к пункту назначения. Такие маршруты создаются только для передачи пакета в одном направлении. Данное утверждение также означает, что на обратном пути может быть использован другой маршрут.

На рис. 3.8 устройства LSR1 и LSR6 представляют собой граничные LSR-маршрутизаторы, а LSR2, LSR3, LSR4 и LSR5 являются базовыми маршрутизаторамиLSR. Для отправки пакетов маршрутизаторы LSR1 и LSR6 осуществляют паритетный обмен информацией на уровне граничных шлюзов, а маршрутизаторы LSR2, LSR3, LSR4 и LSR5 — на уровне внутренних шлюзов. На упомянутом выше рисунке показаны два маршрута LSP: сквозной LSP-маршрут 1-го уровня от устройства LSR1 к LSR6 и LSP-маршрут 2-го уровня между устройствами LSR4 и LSR5.

Для создания маршрута LSP LSR-устройства используют протоколы

маршрутизации и маршруты, которые получены посредством них. Они могут также использовать другие протоколы, такие как RSVP, но это не является обязательным.

Створення маршрутів LSP

Маршруты LSP могут быть установлены одним из таких способов:

- путем использования механизма независимого контроля;
- путем использования механизма упорядоченного контроля.

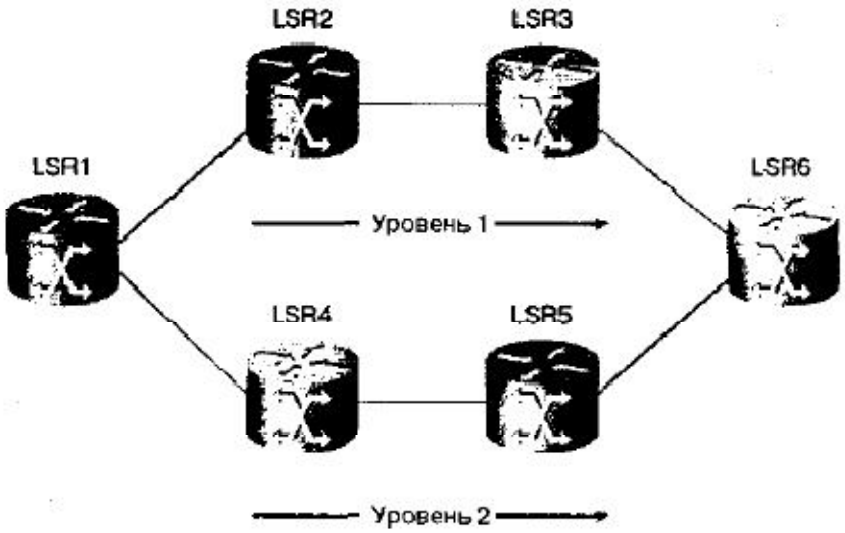


Рисунок 3.8 - Уровни маршрута с коммутацией по меткам

Независимый и упорядоченный контроль для установления LSP-маршрутов могут сосуществовать в одной и той же сети; при этом не возникают структурные проблемы или проблемы взаимодействия. Независимый метод обеспечивает более быструю сходимость и установку маршрутов LSP, поскольку LSR-устройства могут устанавливать и анонсировать привязку меток в любой момент, не затрачивая время на распространение сообщений от одной границы сети до другой. Установка маршрута LSP происходит сразу же после завершения конвергенции протоколов маршрутизации. При использовании метода упорядоченного контроля перед установкой маршрута LSP происходит распространение информации о привязке меток. Однако такой метод контроля предоставляет большие возможности предотвращения в сети кольцевых маршрутов.

Встановлення LSP-маршрутів методом незалежного контролю

При установке маршрутов LSP методом независимого контроля каждое LSR-устроиство распределяет свои префиксы получателей между классами FEC. Каждому классу FEC назначается метка, и все соседи LSR-устройства оповещаются о привязке меток. Все соседние LSR-устройства создают базы LFIB, используя преобразование классов FEC в адреса следующих транзитных переходов. Для преобразования класса FEC в адрес следующей точки перехода LSR-устройства обычно используют протоко-ы маршрутизации, основанные на одноадресатной рассылке, такие как OSPF или ISIS, и информацию, ими.

Как было показано на рис. 3.3, база LFIB содержит данные следующих полей: входной метки, выходной метки, адреса следующего транзитного перехода и выходного интерфейса. LSR-устроЙство создает локальную запись привязки конкретного FEC-класса, произвольным образом выбирая метку из пула (т.е. набора)

свободных в данный момент (вакантных) меток в информационной базе меток (Label Information Base — LIB), и обновляет свою базу LFIB. Поле входной (incoming) метки в базе LFIB устанавливается равным значению метки, выбранной из пула. Адрес следующего перехода устанавливается равным адресу следующего транзитного устройства 3-го уровня, связанного с данным классом FEC, а поле выходного интерфейса (outgoing interface) устанавливается равным номеру выходного интерфейса, используемого для следующего транзитного перехода.

После создания локальной таблицы LSR-устройство сообщает информацию о локальном соответствии меток соседним LSR-устройствам, используя протокол LDP или расширения модифицированного протокола маршрутизации. Распространяемая информация о привязке меток состоит из набора кортежей (группы взаимосвязанных элементов данных или записей), состоящих из префикса адреса (address prefix) и метки (label), где префикс адреса указывает класс FEC (в случае простой маршрутизации с одноадресатной рассылкой), а параметр label задает значение метки, которое LSR-устройство использует для построения локальной таблицы связей меток с конкретным классом FEC.

Когда LSR-устройство получает информацию о метке от своего соседа, оно проверяет наличие локальной записи о привязке метки в своей базе LFIB. Если локальная запись имеется, то значение выходной метки (outgoing label) для этой позиции обновляется и заменяется только что полученным значением. С этого момента LSR-устройство имеет полностью заполненную позицию в базе LF1B и готово к отправке пакетов. Если LSR-устройство получает информацию о метках от соседнего устройства, но не имеет в своей базе LFIB локальной записи для данного класса FEC, то у него есть возможность сохранить эту информацию (она может пригодиться позже) или отбросить ее. Если информация отбрасывается, то протокол LDP запрашивает у соседнего устройства сведения о метке. Информация о привязке меток распространяется только между смежными LSR-устройствами. Любое LSR-устройство совместно использует информацию о метках только с соседним LSR-устройством, которое совместно использует единую подсеть по крайней мере с одним интерфейсом локального LSR-устройства.

Как уже говорилось выше, протоколы маршрутизации, которые используют информацию о состояниях каналов, такие как OSPF или IS-IS, непригодны для распространения информации о метках, поскольку анонсируют протокольную информацию группе маршрутизаторов, участвующих в обмене маршрутными записями, а последние не обязательно являются соседними устройствами. Дистанционно-векторные протоколы, такие как IGRP, протокол RIP первой и второй версий, хотя и распространяют информацию о метках между смежными маршрутизаторами, требуют значительной модификации для распространения данных о привязке меток.

Однако в случае перераспределения потоков MPLS должна быть распространена информация, которая основана на ограничениях для нахождения подходящих маршрутов через есть. Туннели, используемые для перераспределения потоков, должны маршрутизироваться с учетом объема нагрузки. Информация об ограничениях должна распространяться по сети MPLS последовательным и согласованным образом. Механизм лавинной рассылки, используемый протоколами маршрутизации OSPF и IS-IS, используется при создании интегрированной базы данных ограничений и

пересылки.

Протокол BGP может быть модифицирован так, что для передачи информации о метках используется отдельный атрибут. Это связано с тем, что протокол BGP может распространять информацию об адресных префиксах {т.е. FEC) и переносить логически связанное с ним преобразование меток в качестве расширенного атрибута. Коммутация MPLS использует расширенный многопротокольный механизм BGP (Extended Multiprotocol BGP) для облегчения процесса распространения информации о привязке меток, особенно при реализации VPN-сетей MPLS.

Как показано на рис. 3.9, префикс адреса 172.16.0.0/16 непосредственно связан с устройством LSR6. Устройства LSR3 и LSR5 используют маршрутизатор LSR6 в качестве узла следующего транзитного перехода для класса FEC 172.16.0.0/I6.

Устройство LSR1 определяет, соответствует ли адрес следующего перехода для класса FEC маршрутизатору LSR2, который связан с классом 172.16.0.0/16 посредством протокола одноадресатной рассылки, такого, например, как OSPF. После этого устройство LSR1 произвольно выбирает метку из своего пула меток, используя свою базу LIB. Предположим, что значение соответствующей метки равно 50. Устройство LSRI использует метку в качестве индекса своей базы LFIB для нахождения соответствующей позиции, которая будет обновляться. После того как обнаружено соответствие, значение входной метки (incoming label) в этой позиции устанавливается равным 50. В качестве следующего перехода (next hop) устанавливается устройство LSR2, а в качестве выходного интерфейса (outgoing interface) выбирается интерфейс S0. На этом этапе значение выхадной метки (outgoing label) не устанавливается.

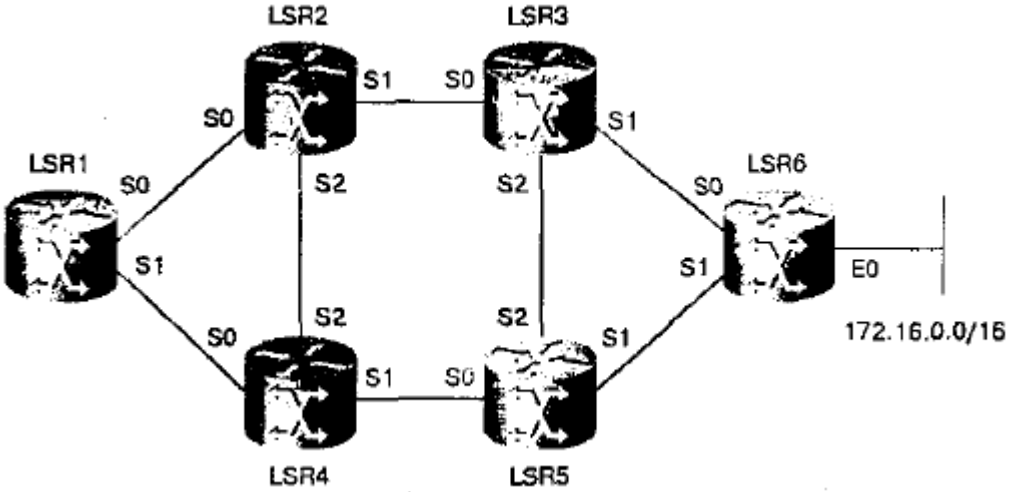


Рисунок 3.9 - Установка маршрута LSP посредством механизма независимого контроля

Устройство LSR1 посылает информацию о локальной привязке меток устройствам LSR2 и LSR4. В этот момент ни маршрутизатор LSR2, ни маршрутизатор LSR4 не используют устройство LSR1 в качестве узла следующего перехода для достижения сети 172.16.0.0/16, поэтому они не могут обновить свои выходные метки в базах LFIB для класса FEC 172.16.0.0/16. Однако, когда маршрутизатор LSR2 посылает информацию о своих локальных метках устройству LSRI, ему известно, что информация поступила от его соседнего узла следующего транзитного перехода дня

сети 172.16.0.0/16, поэтому использует ее в качестве информации удаленного устройства для этой записи. Предположим, что значение метки, произвольно выбранное устройством LSR3, равно 25. Устройство LSR1 использует метку, предоставленную устройством LSR2, для обновления выходной метки (outgoing label) в записи своей базы LFIB, которая связана с классом FEC 172.16.0.0/16. Если устройство LSR1 выполняет функцию входного граничного устрой-ства для такого маршрута LSP, то оно не задает значения входной метки.

Маршрутизатор LSR2 определяет, что устройство LSR3 является следующим переходом для класса FEC, связанного с записью 172.16.0.0/16. После этого оно произвольно выбирает метку из своего пула, используя собственную базу LIB. Предположим, что значение этой метки равно 25. Устройство LSR2 использует метку в качестве индекса своей базы LFIB для поиска совпадающей позиции, которая будет обновлена. После того как соответствие найдено, входная метка (incoming label) в записи устанавливается равной 25. В качестве следующего транзитного перехода (next hop) устанавливается адрес устройства LSR3, а в качестве выходного интерфейса (outgoing interface) выбирается порт SL На этом этапе значение выходной метки (outgoing label) не устанавливается.

После этого устройство LSR2 посылает свою информацию о локальной привязке меток устройствам LSR1, LSR3 и LSR4. В этот момент ни одно из них не использует маршрутизатор LSR2 в качестве следующего транзитного перехода для достижения 172.16.0.0/16, поэтому они не могут обновить выходные метки в записях баз LFIB для сети 172.16.0.0/16.

Однако, когда устройство LSR3 посыпает свою локальную информацию о метках устройствам LSR2, LSR5 и LSR6, то маршрутизатору LSR2 известно, что эта информация поступила от узла следующего транзитного перехода для сети 172.16.0.0/16, и он использует ее в качестве привязки меток удаленного маршрутизатора для класса 172.16.0.0/16. Предположим, что значение метки, произвольно выбранное устройством LSR3, равно 45. Устройство LSR2 использует метку, предоставленную маршрутизатором LSR3, для обновления значения выходной метки (outgoing label) в соответствующей записи своей базы LFIB, связанной с классом FEC 172.16.0.0/16. Аналогичным образом устройство LSR4 определяет, что маршрутизатор LSR5 является следующим транзитным переходом для класса FEC, связанного с сетью 172.16.0.0/16. Теперь устройство LSR4 произвольным образом выбирает метку из своего пула, используя базу LIB. Предположим, что значение этой метки равно 65. После этого устройство LSR4 использует эту метку как индекс в свое базе LFIB для нахождения совпадающей позиции, которая будет изменена. После того как найдено соответствие, поле входной метки (incoming label) данной позиции устанавливается равным 65. В качестве следующего транзитного перехода (next hop) устанавливается маршрутизатор LSR5, а в качестве выходного интерфейса (outgoing interface) используется порт S1. Затем устройство LSR4 посылает информацию о локальной таблице меток устройствам LSRI, LSR2 и LSR5. В этот момент ни одно из устройств LSRI, LSR2, LSR5 не использует маршрутизатор LSR2 в качестве следующего транзитного перехода к сети 172.16.0.0/16 и, следовательно, не может обновить выходную метку в записи базы LFIB для сети 172.16.0.0/16.

Однако, когда маршрутизатор LSR5 посылает локальную информацию устройствам LSR4, LSR3 и LSR6, устройству LSR4 известно, что информация

поступила от маршрутизатора следующего транзитного перехода для сети 172.16.0.0/16 и использует эту информацию в качестве таблицы меток удаленного устройства для класса 172,16.0.0/16. Предположим, что такое произвольно выбранное устройством LSR5 значение метки равно 95. После этого устройство LSR4 использует метку, предоставленную устройством LSR5, для обновления своей выходной метки (outgoing label) в записи базы LFIB, связанной с классом FEC 172J6.0.0/16. Когда маршрутизатор LSR6 посылает свою информацию о локальных метках устройствам LSR3 и LSR5, этим устройствам известно, что она поступила от узла следующего транзитного перехода для сети 172.16.0.0/16, и они оба используют ее в качестве таблицы меток удаленного устройства для класса FEC 172.16.0.0/16. Предположим, что это произвольно выбранное устройством LSR5 значение метки равно 33. В таком случае оба устройства, LSR3 и LSR5, используют метку, предоставленную устройством LSR6, для обновления *выходной метки* (outgoing label) в записях своих баз LFIB, связанной с классом FEC 172.16.0.0/16. Устройство LSR6 не содержит выходной метки в базе LFIB для класса 172.16.0.0/16, поскольку оно непосредственно подсоединено к сети 172,16.0.0/16, Для этой сети устройство LSR6 представляет собой граничное LSR-устройство, поэтому оно удаляет метку из пакета перед отправкой его в сеть 172.16.0.0/16.

На этой стадии, как показано в табл. 3.3, у всех LSR-устройств записи баз LFIB для класса FEC 172.16.0.0/16 заполнены, и они готовы к пересылке пакетов. Когда устройство LSRI получает пакет со значением метки, равным 50, оно использует ее в качестве индекса своей информационной базы LFIB для поиска записи необходимой для пересылки пакетов. После того как соответствующая позиция найдена, устройство обменивает значение метки на значение выходной метки, равное 25, и отправляет пакет через интерфейс S0 на устройство LSR2, которое осуществляет аналогичный поиск по своей базе, обменивает значение метки на значение 45 и направляет пакет устройству LSR3 через интерфейс S1. Устройство LSR3 выполняет поиск в базе LFIB, меняет значение метки на 33 и направляет пакет устройству LSR6 через интерфейс S1. В конечном итоге устройство LSR6 удаляет метку из пакета и направляет его к пункту назначения через интерфейс E0. В случае удаления метки на предпоследнем переходе, т.е. на устройстве LSR3, маршрутизатор LSR6 может выполнить поиск либо в базе LFIB, либо *в* таблице маршрутизации 3-го уровня.

Таблица 3.3

	Записи базы LFIB после распространения меток			
Устройство	Входная метка	Выходная метка	Следующий транзитный переход	Выходной интерфейс
LSR1	50	25	LSR2	SO
LSR2	25	45	LSR3	S1
LSR3	45	33	LSR6	S1
LSR4	65	95	LSR5	S1
LSR5	95	33	LSR6	S1
LSR6	33	—	LSR6	E0

<u>Встановлення маршруту LSP за допомогою механізму впорядкованого контролю</u>

При использовании для установки маршрута LSP метода упорядоченного контроля входное или выходное граничное LSR-устройство инициирует установку маршрута LSR Назначение меток происходит упорядоченным образом от конечной (выходной) до начальной (входной) точек LSP-маршрута. Установка пути LSP может быть начата с любого конца — со входа или с выхода. Устройство, инициирующее создание маршрута LSP, выбирает классы FEC, и все остальные LSR-устройства на данном LSP-маршруте используют те же самые записи FEC. Такой метод контроля при установке маршрута LSP требует, чтобы информация о привязке меток была распространена по всем LSR-устройствам до определения маршрута LSP. Описываемый подход приводит к тому, что время конвергенции при этом в несколько раз больше, чем при независимом контроле. Однако при использовании метода упорядоченного контроля вероятность возникновения петель на маршруте LSP меньше чем при независимом контроле.

Пример установки LSP-маршрута упорядоченным методом приведен на рис. ЗЛО. В этом примере устройство LSR7 является выходным LSR-маршрутизатором, которое инициирует установку LSP-маршрута. Устройству LSR7 известна своя роль, поскольку оно имеет непосредственное соединение с сетью 192.168.0.0/16. Предположим, что маршрутизатор LSR7 назначает классу FEC 192.168.0.0/16 метку со значением 66. После этого он извещает о своей локальной метке соседнее устройство LSR6. Получив такое оповещение, маршрутизатор LSR6 назначает данному классу FEC новую метку со значением 33 и сообщает о привязке метки к сети своим соседям: устройствам LSR3 и LSR5. Упорядоченная установка маршрута LSP продолжается таким способом на протяжении всего маршрута LSP ко входному или иному устройству LSR1.

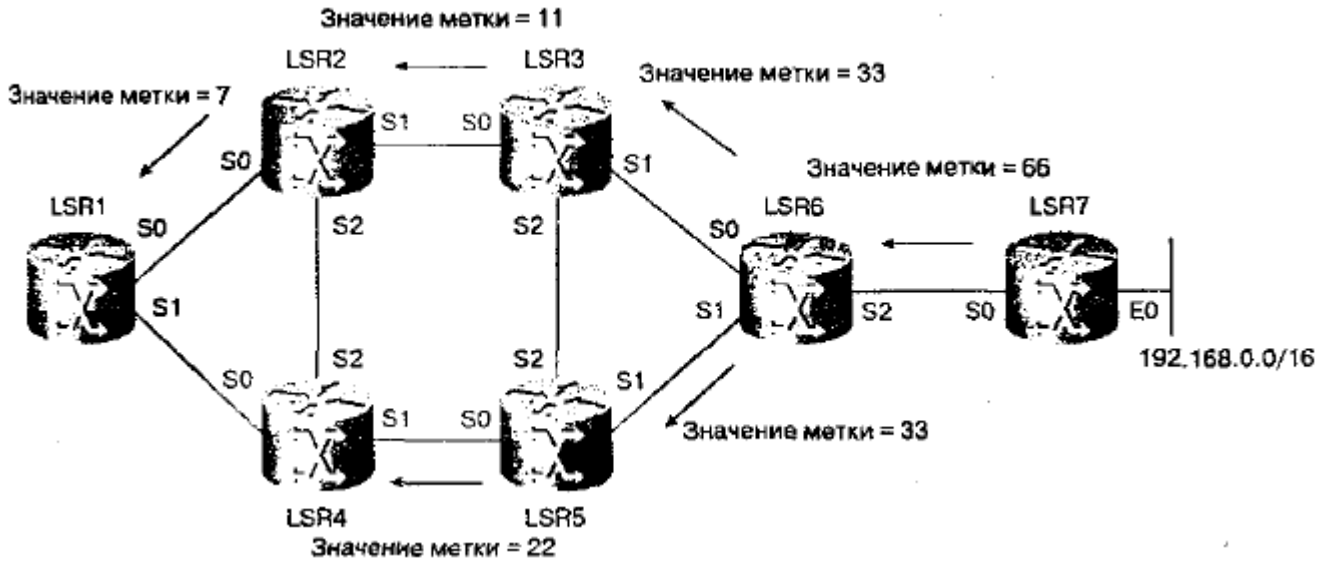


Рисунок 3.10 - Упорядоченный контроль при установке маршрута LSP

Внимание!

Программное обеспечение Cisco IOS использует режим независимого контроля (independent control) при установке LSP-маршрутов для сетей MPLS и упорядоченный контроль (ordered control) — для MPLS-сетей ATM.

§2. Протокол розповсюдження міток LDP

Протокол распространения меток (Label Distribution Protocol — LDP) используется вместе со стандартными протоколами маршрутизации сетевого уровня для распределения информации о метках между LSR-устройстьами в сетях с коммутацией по меткам. Протокол LDP позволяет LSR-устройствам распространять метки между LDP-устройствами того же уровня через порт 646 протокола TCP, в то время как протокол распространения тегов TDP использует порт 711. Использование TCP в качестве протокола транспортного уровня обеспечивает гарантированную доставку информации протокола LDP с помощью надежных механизмов упраадения потоком и обработки возможных заторов.

Внимание!

Протокол распределения тегов (Cisco's Tag Distribution Protocol — TDP) корпорации Cisco и основанный на стандартах MPLS-протокол LDP (Label Distribution Protocol) выполняют идентичные функции, но используют несовместимые между собой форматы сообщений и различные процедуры. В настоящее время корпорация Cisco работает над преобразованием TDP в протокол, полностью совместимый с LDP. В настоящем разделе основное внимание уделяется протоколу LDP.

Когда LSR-устройство назначает метку классу FEC, требуется известить об этом соответствующие устройства того же уровня. Для этой цели используется протокол LDP. Набор меток от входного LSR-устройства до выходного LSR-устройства в домене MPLS определяет маршрут LSP. Метки представляют собой способ преобразования маршрутной информации в коммутируемые маршруты канального уровня. Протокол LDP помогает устанавливать LSP-маршруты, используя набор процедур для распространения меток среди LSR-устройсте одного ранга.

Протокол LDP предоставляет LSR-устройствам механизм взаимного обнаружения и установки связи. При этом он использует четыре класса сообщений, приводимых ниже.

• Сообщения DISCOVERY (обнаружения) пересылаются по протоколу UDP и используют сообщения многоадресатной рассылки HELLO (приветствия) для получения информации о других LSR-устройствах, с которыми узел LDP имеет непосредственное соединение. После этого устанавливается TCP-соединение и, возможно, сеанс LDP с устройствами того же уровня. Сеансы LDP имеют двусторонний характер. LSR-устройства на любом конце соединения могут передать или запросить информацию о привязке меток к классам у устройства на другом конце соединения.

• Сообщения ADJACENCY (смежности) передаются по протоколу TCP и инициируют сеанс с помощью сообщения INITIALIZATION (инициализация) в начале согласования сеанса LDP. Передаваемая информация включает в себя режим выделения меток, значения таймера тестовых сообщений (keepalive) и диапазон значений меток, используемых при обмене информацией между двумя LSR-устройствами. Тестовые сообщения протокола LDP (сообщения KEEPALIVE) рассылаются периодически. Прекращение сеанса LDP между паритетными устройствами LSR происходит в том случае, если в течение заданного времени таймера не получены сообщения KEEPALIVE.

• Сообщения LABEL ADVERTISEMENT (анонс метки) обеспечивают распространение информации о привязке меток путем рассылки сообщений LABEL

MAPPING (преобразование метки), извещающих о связи между классами FEC и метками. Сообщения LABEL WITHDRAWAL (удаление метки) используются для процесса, обратного установлению соответствия. Сообщения LABEL RELEASE (освобождение метки) используются LSR-устройствами, которые получили информацию о преобразовании меток и желают удалить метку, поскольку она больше не требуется,

• Сообщения NOTIFICATION (уведомление) переносят справочную информацию и информацию об ошибках паритетным LSR-устройствам, участвующим в сеансе LDP.

Протокол LDP работает в рамках протокола TCP для обеспечения надежной передачи всех сообщений, кроме LDP-сообщений DISCOVERY, которые передаются по протоколу UDP. Сообщения LDP задаются как набор объектов "тип, длина, значение" (type-length-value — TLV). Распространение и назначение меток по протоколу LDP может быть осуществлено несколькими способами, которые обсуждаются ниже.

Режим протоколу LDP: «нисходящее» розповсюдження міток за вимогою

Структура MPLS позволяет LSR-устройству явным образом запросить у устройства следующего транзитного перехода класс FEC для пакета и информацию о привязке меток для объекта FEC. Такой режим известен как нисходящее распространение меток по требованию. Для запроса информации о преобразовании меток от последующего устройства интерфейс использует сообщение LABEL REQUEST (запрос на предоставление метки). Для отмены запроса LABEL REQUEST после его окончания или ранее используется сообщение LABEL REQUEST ABORT (прерывание запроса на предоставление метки).

Режим розповсюдження міток без запиту

Структура MPLS также позволяет LSR-устройствам распространять информацию о метках среди других LSR-устройств, которые ее явным образом не запрашивали. Такой режим называется нисходящим распространением меток без запроса. Оба способа распространения меток могут применяться одновременно. Два соседних LSR-устройства, обменивающиеся информацией о привязке меток к классам, должны согласовать между собой используемый метод. Он согласовывается этими устройствами в процессе соответствующего сеанса LDP с помощью сообщений INITIALIZE (инициализация).

Внимание!

Операционная система Cisco IOS использует режим распределения меток без запроса для пакетных MPLS-сетей и режим нисходящего распределения по требованию для MPLS-сетей ATM.

Несуворий режим збереження міток протоколу LDP

Если LSR-устройство использует такой режим сохранения меток (Liberal Mode), то оно поддерживает информацию о привязке меток и классов FEC, полученную от LSR-устройств, которые не являются для данного класса FEC устройствами следующего транзитного перехода.

LSR-устройство может получить информацию о метках для класса FEC от LSR-устройства того же уровня и в том случае, когда оно не является устройством следующего перехода для данного класса FEC. После этого устройство может принять

решение о том, следует ли сохранять такую информацию. Если принято решение сохранять ее, то метка может немедленно использоваться, если устройство, от которого получена информация станет следующим транзитным переходом для рассматриваемого класса FEC. Если принято решение отбросить полученную информацию, то в случае, когда LSR-устройство позднее станет адресом следующего перехода, информация о привязке меток будет вновь получена с помощью протокола LDP.

Суворий режим збереження міток протоколу LDP

Если LSR-устройство работает в строгом режиме (Conservative Mode) сохранения меток, то оно отбрасывает информацию о привязке метки к классу FEC, полученную от устройств LSR, не являющихся для данного класса FEC адресом следующего транзитного перехода. Такое LSR-устройство поддерживает только информацию о связи меток с классом FEC, которая требуется для отправки пакетов. Данный режим экономно использует метки и широко используется на коммутаторах ATM, используемых в качестве LSR-устройств.

Внимание!

Нестрогий режим сохранения меток способствует быстрой адаптации к изменениям маршрутизации, а в строгом режиме LSR-устройству требуется поддерживать меньшее количество меток. Операционная система Cisco IOS использует первый режим для пакетных MPLS-сетей и второй — для сетей ATM. Использование протокола LDP возможно в программном обеспечении Cisco IOS начиная с версии 12.2T.

Внимание!

Сочетание нестрогого режима сохранения меток с независимым механизмом контроля установки маршрута LSP обеспечивает быструю конвергенцию протоколов TDP или LDP в случае выхода канала из строя. Однако перед повторной установкой LSP-маршрута необходимо, чтобы была завершена конвергенция маршрутизации протокола внутреннего шлюза (IGP). Такая ситуация может привести к временной потере пакетов в связи с неспособностью LSR-устройств отправлять пакеты с метками.

§3. Умови виникнення петель маршрутизації в середовищі MPLS

Маршруты LSP создаются с использованием протоколов LDP, TDP или расширений протоколов маршрутизации, таких как BGP, PIM или RSVP. Протокол ШР использует информацию, собранную протоколами маршрутизации 3-го уровня, и такой принцип работы делает возможным образование петель в том случае, если протокол 3-го уровня сам не смог предотвратить их появление. Несмотря на стремление протоколов маршрутизации создавать свободные от петель маршруты, почти у всех протоколов возможно возникновение петель во время переходных процессов при нестабильном состоянии сети.

В дистанционно-векторных протоколах маршрутизации, таких как RIP, узлам сети не требуется полная топологическая информация о сети. В таких сетях может возникнуть ситуация бесконечного числа переходов, когда метрика маршрута, имеющего петлю, постепенно увеличивается и сообщается всем узлам до тех пор, пока не достигнет максимально возможного значения.

В протоколах, которые учитывают состояние канала связи, такие как OSPF, каждый узел поддерживает полную топологическую базу данных своей области

маршрутизации в сети. В таких сетях существует возможность возникновения петель маршрутизации в тех случаях, когда после изменения топологии сети не успела произойти синхронизация изменений базы данных, особенно в период сразу после выхода канала из строя.

Вплив петель маршрутизації на функціонування MPLS

Если предотвратить появление петель не удалось, то они воздействуют на процесс передачи данных на уровне коммутации MPLS как описано ниже.

• Зацикливание управляющих пакетов LSP. Пакеты, используемые для установки маршрута LSP, направляются в "бесконечную" петлю маршрутизации, и сквозной маршрут вообще не устанавливается. Такое состояние продолжается до тех пор, пока петля не будет тем или иным образом ликвидирована.

• Зацикливание пакетов данных MPLS. При перенаправлении пакетов данных по установленному маршруту LSP, имеющему петлю, они коммутируются по меткам на этом маршруте до тех пор, пока петля не будет ликвидирована.

§4. Контроль петель маршрутизації в середовищі MPLS

Имеется три основных способа контролировать процесс образования петель в сетях MPLS:

• временное сохранение петель
• обнаружение петель
• предотвращение образования петель.

Тимчасове збереження петель

При использовании этого метода контроля возникновение петель в маршрутах LSP признается допустимым. Однако при этом принимаются специальные меры, для того, чтобы пакеты, перемещающиеся по маршрутам с петлями, не влияли на передачу пакетов по маршрутам без петель. Обеспечить это могут узлы MPLS, которые способны уменьшать "время существования" (time-to-live — TTL) маршрутов LSP. Сегменты се-тн, не обладающие функциями TTL, такие как каналы ATM, используют в качестве механизма контроля петель выделение буферного пространства ATM-коммутатора для отдельных виртуальных каналов (VC).

Тимчасове збереження петель в сегментах з функцією TTL

При отправке IP-пакетов используется TTL-поле пакета, значение которого уменьшается на каждом IP-переходе. Если это значение становится равным 0, то делается заключение, что пакет движется по замкнутому маршруту, после чего он отбрасывается. Такой подход экономит ресурсы маршрутизатора и позволяет ему сосредоточиться непосредственно на отправке пакетов по маршрутам без петель и на обновлении таблиц маршрутизации. После окончания конвергенции, когда таблицы маршрутизации стабилизировались, петля обычно исчезает, кроме тех случаев, когда имеются ошибки в конфигурациях одного или нескольких маршрутизаторов.

Коммутация MPLS использует для контроля петель аналогичный подход. Пакеты, которые помечены между заголовками канального и сетевого уровней с помощью механизмов MPLS содержат промежуточный заголовок, в котором находится поле TTL, которое используется точно так же, как и IP-поле TTL. Заголовок может быть использован для того, чтобы пакеты, которые попали в петли, образовавшиеся в момент неустойчивого состояния сети, были отброшены. На рис.

ЗЛ1 показан маршрут LSP, содержащий петлю. Однако, как показано на рис. 3.12, механизм TTL уменьшает значение соответствующего параметра до 0, и петля разрывается.

Тимчасове збереження петель в сегментах, що не підртимують функції TTL

В каналах сетей ATM поле TTL недоступно. Такие каналы в структуре MPLS называют "сегментами без TTL". В качестве LSR-устройств в таких сетях используются коммутаторы ATM, обладающие функциями маршрутизации 3-го уровня. Буферное пространство, используемое отдельным виртуальным каналом может быть ограничено путем соответствующего конфигурирования. Такой метод выделения буферного пространства применяется для контроля процесса образования петель, поскольку пакеты, попавшие в петлю, могут использовать только ограниченное буферное пространство и не могут перегружать LSR-устройство сети ATM. Коммутатор по-прежнему может отправлять пакеты с обновлениями маршрутизации, и это позволяет осуществить конвергенцию и ликвидировать петли, образовавшиеся во время неустойчивого состояния сети. Петли, образовавшиеся по другим причинам, также могут быть ликвидированы, поскольку LSR-устройства ATM могут отправлять пакеты со служебной информацией и пакеты, передаваемые по маршрутам без петель. Ограничение буферного пространства затрагивает только пакеты, проходящие по маршрутам с петлями.

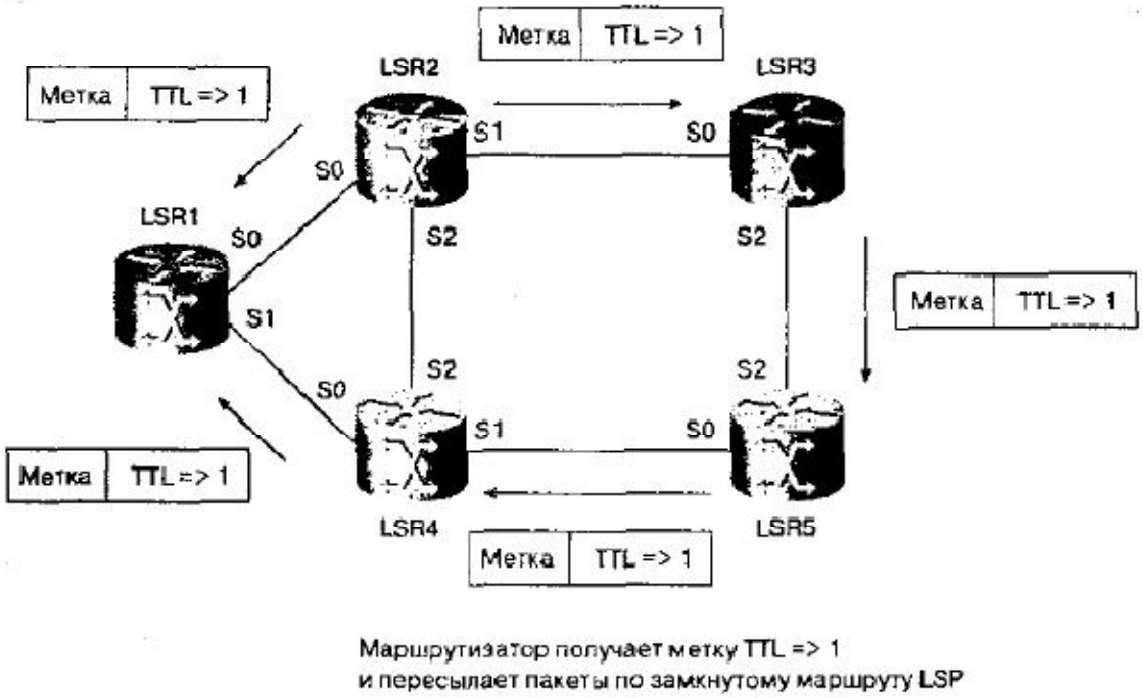


Рисунок 3.11 - Маршрут LSP с петлей

Виявлення петель

Данный метод контроля петель допускает их возникновение на LSP-маршруте, но позволяет быстро их обнаружить и ликвидировать. Протокол LDP и протокол TDP корпорации Cisco осуществляют обнаружение петель. При обнаружении петель используются те же механизмы контроля, что и при временном сохранении петель; уменьшение времени существования TTL и ограничение буферного пространства для

отдельных LSP-маршрутов в коммутаторах ATM.

В технологии теговой коммутации Cisco (Cisco Tag Switching), кроме временного сохранения меток, используется также подсчет транзитных переходов (hop count). Метод подсчета переходов реализуется точно так же, как метод TTL. Однако информация о количестве переходов передается в запросах и ответах протоколов LDP и TDP. Механизм подсчета транзитных переходов показан на рис. 3.13.

При передаче информации о привязке меток по требованию из точки, в которой изменилась топология сети, рассылаются запросы на выходные узлы сети MPLS. Предположим, что начальное значение переменной, содержащей количество переходов, равно 7. Это значение уменьшается на единицу на каждом проходе через любое из LSR-устройств, образующих петлю и в конечном итоге становится равным 0. В этот момент связывание меток становится невозможным и маршрут LSP удаляется. После того как произошла конвергенция и стабилизация информации о маршрутизации, посылается новый запрос о привязке меток, на основе которого создается новый маршрут LSR

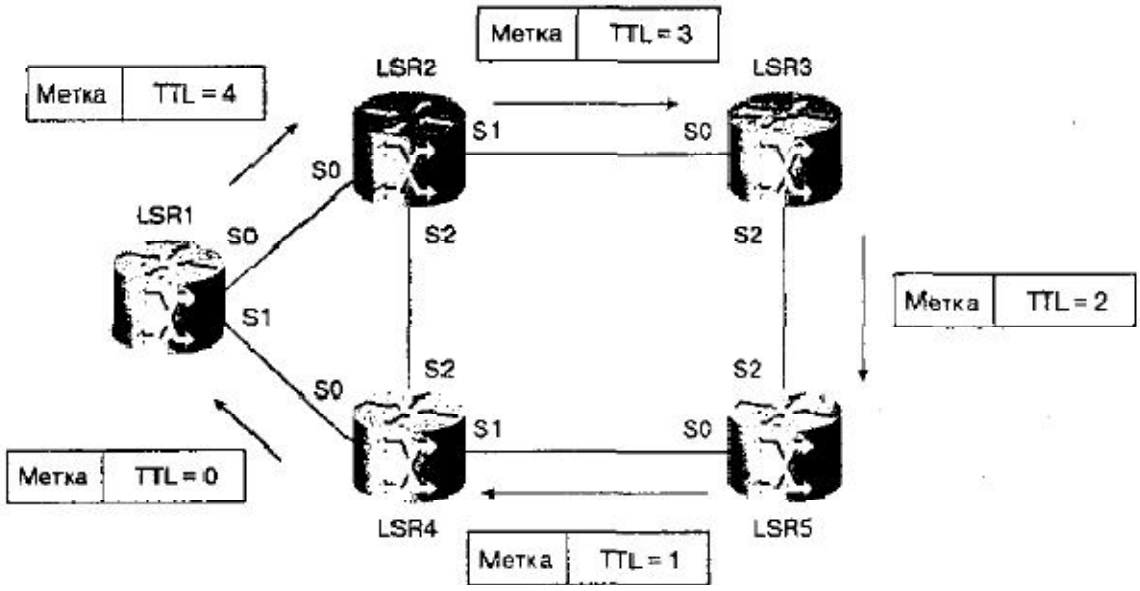


Рисунок 3.12 - Обнаружение петли в маршруте LSP с использованием механизма TTL

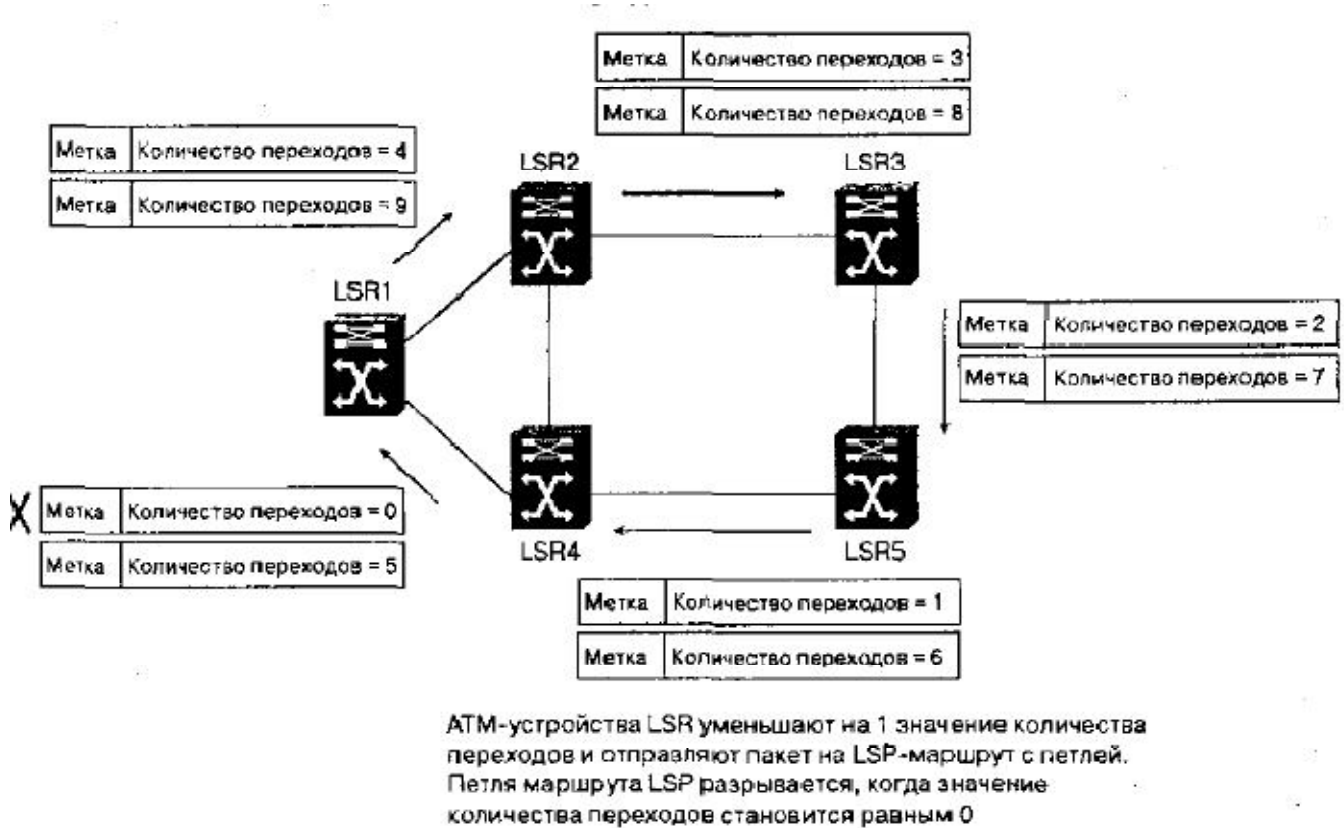


Рисунок 3.13 - Подсчет транзитных переходов для обнаружения петель

Запобігання утворенню петель

Предотвращение образования петель позволяет избежать образования кольцевых маршрутов до того, как по ним будут направлены пакеты. При использовании этого метода LSP-маршруты подразделяются на две категории:

- слияние маршрутов LSP без учета состояния;
- слияние маршрутов LSP с учетом состояния.

Об'єднання LSP-маршрутів без врахування стану

Для каждого состояния выходного канала существует отдельное состояние входного соединения. К такому типу принадлежат маршруты LSP, созданные с помощью протоколов CR-LDP или RSVP. Каждый запрос метки содержит адреса узлов LSR, добавляемые LSR-устройствами при отправке ими сообщений. Если в получаемом сообщении устройство LSR находит собственный адрес, то такая ситуация квалифицируется как наличие петли, и построение маршрута LSP прекращается.

Об'єднання маршрутів LSP з врахуванням стану

Для каждого состояния выходного канала существует несколько входных состояний. К данному типу принадлежат маршруты LSP, созданные с помощью протокола LDP. Для таких маршрутов LSP используются два метода предотвращения петель:

- диффузия вектора маршрута;
- метод "окрашенной нити".

Алгоритм дифузії вектору маршруту

Алгоритм PD (Path Vector Diffusion — диффузии вектора маршрута)

предотвращает возникновение петель путем использования списка LSR-адрссов, называемого вектором маршрута (path vector). Вектор маршрута представляет собой список LSR-устройств, через которые прошло сообщение LABEL REQUEST или LABEL MAPPING. Сообщение LABEL REQUEST, посланное устройством LSR соседнему устройству, содержит вектор маршрута с адресом только запрашивающего LSR-устройства. Перед отправкой запроса о метке для данного класса FEC устройству следующего перехода принимающее LSR-устройство добавляет к вектору маршрута свой адрес. Если вследствие наличия петли сообщение REQUEST или MAPPING постоянно перемещается по ней, то LSR-устройство обнаруживает в сообщении REQUEST или MAPPING собственный адрес и таким образом выявляет наличие петли. В таком случае создание соответствующего маршрута с петлей прекращается.

Внимание!

При использовании другого типа PD-элгоритма вектор маршрута не хранится на узле LSR. В данном случае при каждом преобразовании метки на входе пакета в сеть LSR-устройства создают запрос с вектором маршрута, который содержит только адрес создавшего его устройства. Такой запрос посылается лежащему далее по маршруту узлу, который подтверждает получение каждого запроса.

Более подробное описание различных вариантов алгоритма PD приведено в книге "Loop-Free Routing Using Diffusion Computations" IEEE/ACM Trans. Net Vol. 1, No. 1., J. Garcia-Lune-Aceves ("Беспетельная маршрутизация с вычислением диффузии", Дж. Гарсия-Льюн-Акивес).

Алгоритм "забарвленої нитки"

Предотвращение петель, называемое "алгоритмом окрашенной нити", требует упорядоченного контроля при установке маршрута LSP. Метод окрашенной нити можно сравнить с протягиванием окрашенной нити от начальной до конечной точки маршрута LSP. Любое промежуточное LSR-устройство обнаруживает наличие петли, если нить пересекается сама с собой, и не допускает построения кольцевого маршрута. В такой ситуации LSR-устройства ожидают окончания конвергенции таблиц маршрутизации и стабилизации топологии сети перед новой попыткой "протянуть нить" or точки входа в сеть до точки выхода. Метод окрашенной нити эффективно работает в LSR-устройствах сетей ATM.

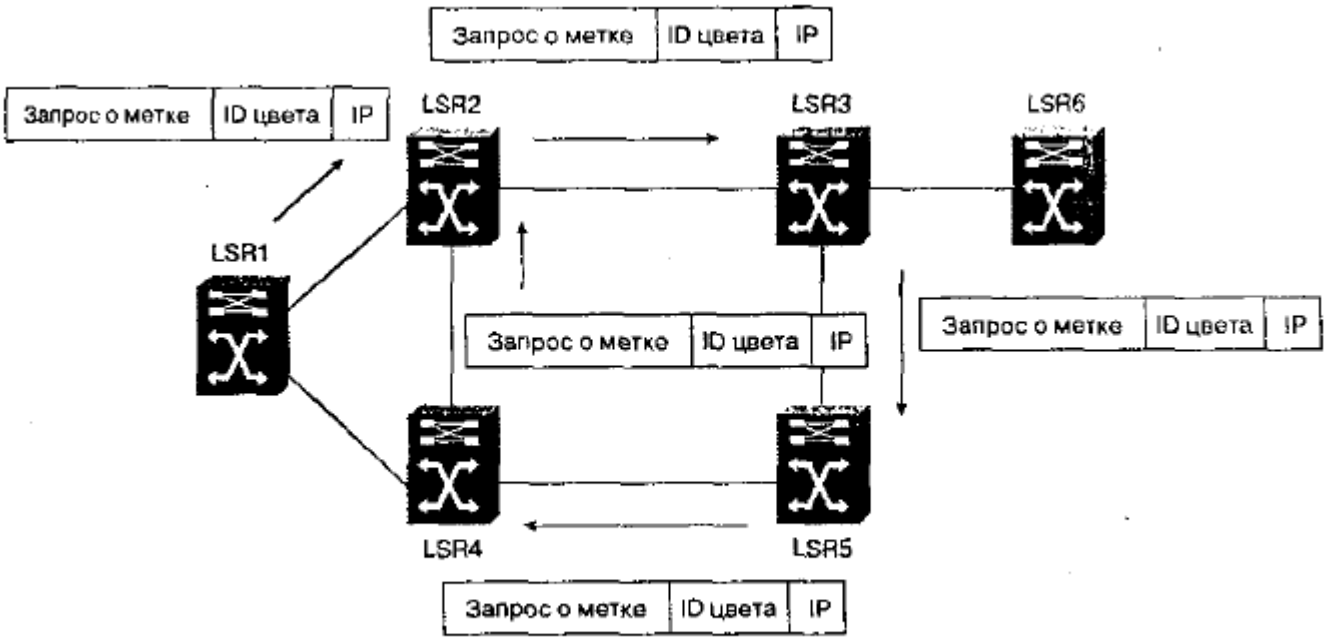


Рис. 3.14. Использование метода "окрашенной нити" для предотвращения петель

Рисунок 3.14 - Использование метода "окрашенной нити " для предотвращения петель

"Подовження" нитки

Рассмотрим сеть, показанную на рис. 3.14. Предположим, что устройство LSR1 пытается создать маршрут LSP, используя выделение меток с запросом предыдущего устройства. Маршрутизатор LSRJ удлиняет нить путем отправки сообщения LABEL REQUEST. Эта нить имеет "цвет", представляющий собой IP-адрес устройства LSR1 вместе с уникальным идентификатором. По мере построения маршрута LSP сообщение LABEL REQUEST проходит по узлам LSR2, LSR3, LSR4 и LSR5: при этом каждый узел сохраняет цвет входящей нити и передает этот же цвет в запросе выходной метки. В конечном итоге запрос метки от маршрутизатора LSR4 поступает на устройство LSR2. Поскольку запрос метки содержит тот же самый цвет, который был сохранен в LSR2 при получении запроса LABEL REQUEST от LSR1, устройство LSR2 констатирует наличие петли. В этот момент LSR2 прекращает отправлять сообщения LABEL REQUEST и отвечать на запросы о метке. Благодаря этому разрывается маршрут LSP и предотвращается возникновение петли.

"Змотування" нитки

После окончания конвергенции таблиц маршрутизации и стабилизации маршрутов петля разрывается. Это может произойти, например, если устройство LSR3 обнаруживает, что устройством следующего перехода для данного маршрута LSP является не LSR5, а LSR6. В таком случае узел LSR3 отзывает запрос метки, сделанный устройству LSR5, и запрашивает метку от маршрутизатора LSR6. Поскольку узел LSR6 представляет собой выходную точку данного MPLS-домена (устройством следующего перехода для данного класса FEC не является LSR-устройство), оно возвращает информацию о метках устройству LSR3, которое, в свою очередь, возвращает ее устройству LSR2 и т.д. Благодаря этому создается маршрут

LSP, не содержащий петель.

Завдання на СРС

1. Приклади комутації в фрагменті мережі з кільцевою та повнозв'язною структурою

Створення маршрутів LSP

Маршруты LSP могут быть установлены одним из таких способов:

• путем использования механизма независимого контроля;

• путем использования механизма упорядоченного контроля.

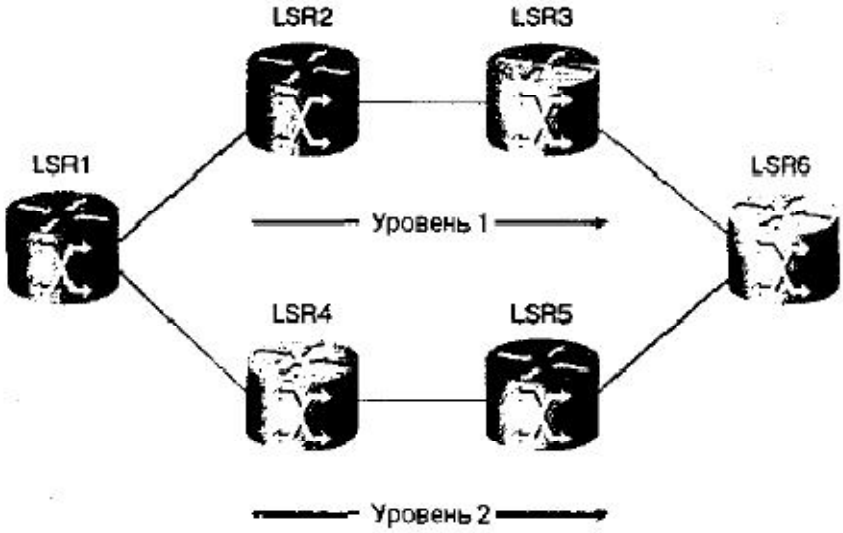


Рисунок 3.8 - Уровни маршрута с коммутацией по меткам

Независимый и упорядоченный контроль для установления LSP-маршрутов могут сосуществовать в одной и той же сети; при этом не возникают структурные проблемы или проблемы взаимодействия. Независимый метод обеспечивает более быструю сходимость и установку маршрутов LSP, поскольку LSR-устройства могут устанавливать и анонсировать привязку меток в любой момент, не затрачивая время на распространение сообщений от одной границы сети до другой. Установка маршрута LSP происходит сразу же после завершения конвергенции протоколов маршрутизации. При использовании метода упорядоченного контроля перед установкой маршрута LSP происходит распространение информации о привязке меток. Однако такой метод контроля предоставляет большие возможности предотвращения в сети кольцевых маршрутов.

Встановлення LSP-маршрутів методом незалежного контролю

При установке маршрутов LSP методом независимого контроля каждое LSR-устроиство распределяет свои префиксы получателей между классами FEC. Каждому классу FEC назначается метка, и все соседи LSR-устройства оповещаются о привязке меток. Все соседние LSR-устройства создают базы LFIB, используя преобразование классов FEC в адреса следующих транзитных переходов. Для преобразования класса FEC в адрес следующей точки перехода LSR-устройства обычно используют протоко-ы маршрутизации, основанные на одноадресатной рассылке, такие как OSPF или ISIS, и информацию, ими.

Как было показано на рис. 3.3, база LFIB содержит данные следующих полей:

входной метки, выходной метки, адреса следующего транзитного перехода и выходного интерфейса. LSR-устроЙство создает локальную запись привязки конкретного FEC-класса, произвольным образом выбирая метку из пула (т.е. набора) свободных в данный момент (вакантных) меток в информационной базе меток (Label Information Base — LIB), и обновляет свою базу LFIB. Поле входной (incoming) метки в базе LFIB устанавливается равным значению метки, выбранной из пула. Адрес следующего перехода устанавливается равным адресу следующего транзитного устройства 3-го уровня, связанного с данным классом FEC, а поле выходного интерфейса (outgoing interface) устанавливается равным номеру выходного интерфейса, используемого для следующего транзитного перехода.

После создания локальной таблицы LSR-устройство сообщает информацию о локальном соответствии меток соседним LSR-устройствам, используя протокол LDP или расширения модифицированного протокола маршрутизации. Распространяемая информация о привязке меток состоит из набора кортежей (группы взаимосвязанных элементов данных или записей), состоящих из префикса адреса (address prefix) и метки (label), где префикс адреса указывает класс FEC (в случае простой маршрутизации с одноадресатной рассылкой), а параметр label задает значение метки, которое LSR-устройство использует для построения локальной таблицы связей меток с конкретным классом FEC.

Когда LSR-устройство получает информацию о метке от своего соседа, оно проверяет наличие локальной записи о привязке метки в своей базе LFIB. Если локальная запись имеется, то значение выходной метки (outgoing label) для этой позиции обновляется и заменяется только что полученным значением. С этого момента LSR-устройство имеет полностью заполненную позицию в базе LF1B и готово к отправке пакетов. Если LSR-устройство получает информацию о метках от соседнего устройства, но не имеет в своей базе LFIB локальной записи для данного класса FEC, то у него есть возможность сохранить эту информацию (она может пригодиться позже) или отбросить ее. Если информация отбрасывается, то протокол LDP запрашивает у соседнего устройства сведения о метке. Информация о привязке меток распространяется только между смежными LSR-устройствами. Любое LSR-устройство совместно использует информацию о метках только с соседним LSR-устройством, которое совместно использует единую подсеть по крайней мере с одним интерфейсом локального LSR-устройства.

Как уже говорилось выше, протоколы маршрутизации, которые используют информацию о состояниях каналов, такие как OSPF или IS-IS, непригодны для распространения информации о метках, поскольку анонсируют протокольную информацию группе маршрутизаторов, участвующих в обмене маршрутными записями, а последние не обязательно являются соседними устройствами. Дистанционно-векторные протоколы, такие как IGRP, протокол RIP первой и второй версий, хотя и распространяют информацию о метках между смежными маршрутизаторами, требуют значительной модификации для распространения данных о привязке меток.

Однако в случае перераспределения потоков MPLS должна быть распространена информация, которая основана на ограничениях для нахождения подходящих маршрутов через есть. Туннели, используемые для перераспределения потоков, должны маршрутизироваться с учетом объема нагрузки. Информация об ограничениях

должна распространяться по сети MPLS последовательным и согласованным образом. Механизм лавинной рассылки, используемый протоколами маршрутизации OSPF и IS-IS, используется при создании интегрированной базы данных ограничений и пересылки.

Протокол BGP может быть модифицирован так, что для передачи информации о метках используется отдельный атрибут. Это связано с тем, что протокол BGP может распространять информацию об адресных префиксах {т.е. FEC) и переносить логически связанное с ним преобразование меток в качестве расширенного атрибута. Коммутация MPLS использует расширенный многопротокольный механизм BGP (Extended Multiprotocol BGP) для облегчения процесса распространения информации о привязке меток, особенно при реализации VPN-сетей MPLS.

Как показано на рис. 3.9, префикс адреса 172.16.0.0/16 непосредственно связан с устройством LSR6. Устройства LSR3 и LSR5 используют маршрутизатор LSR6 в качестве узла следующего транзитного перехода для класса FEC 172.16.0.0/I6.

Устройство LSR1 определяет, соответствует ли адрес следующего перехода для класса FEC маршрутизатору LSR2, который связан с классом 172.16.0.0/16 посредством протокола одноадресатной рассылки, такого, например, как OSPF. После этого устройство LSR1 произвольно выбирает метку из своего пула меток, используя свою базу LIB. Предположим, что значение соответствующей метки равно 50. Устройство LSRI использует метку в качестве индекса своей базы LFIB для нахождения соответствующей позиции, которая будет обновляться. После того как обнаружено соответствие, значение входной метки (incoming label) в этой позиции устанавливается равным 50. В качестве следующего перехода (next hop) устанавливается устройство LSR2, а в качестве выходного интерфейса (outgoing interface) выбирается интерфейс S0. На этом этапе значение выхадной метки (outgoing label) не устанавливается.

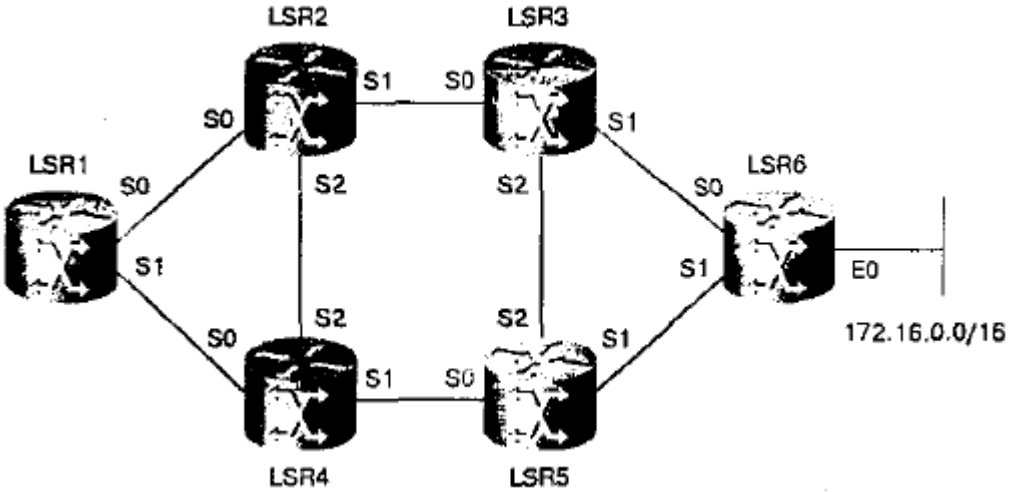


Рисунок 3.9 - Установка маршрута LSP посредством механизма независимого контроля

Устройство LSR1 посылает информацию о локальной привязке меток устройствам LSR2 и LSR4. В этот момент ни маршрутизатор LSR2, ни маршрутизатор LSR4 не используют устройство LSR1 в качестве узла следующего перехода для достижения сети 172.16.0.0/16, поэтому они не могут обновить свои выходные метки в

базах LFIB для класса FEC 172.16.0.0/16. Однако, когда маршрутизатор LSR2 посылает информацию о своих локальных метках устройству LSRI, ему известно, что информация поступила от его соседнего узла следующего транзитного перехода дня сети 172.16.0.0/16, поэтому использует ее в качестве информации удаленного устройства для этой записи. Предположим, что значение метки, произвольно выбранное устройством LSR3, равно 25. Устройство LSR1 использует метку, предоставленную устройством LSR2, для обновления выходной метки (outgoing label) в записи своей базы LFIB, которая связана с классом FEC 172.16.0.0/16. Если устройство LSR1 выполняет функцию входного граничного устрой-ва для такого маршрута LSP, то оно не задает значения входной метки.

Маршрутизатор LSR2 определяет, что устройство LSR3 является следующим переходом для класса FEC, связанного с записью 172.16.0.0/16. После этого оно произвольно выбирает метку из своего пула, используя собственную базу LIB. Предположим, что значение этой метки равно 25. Устройство LSR2 использует метку в качестве индекса своей базы LFIB для поиска совпадающей позиции, которая будет обновлена. После того как соответствие найдено, входная метка (incoming label) в записи устанавливается равной 25. В качестве следующего транзитного перехода (next hop) устанавливается адрес устройства LSR3, а в качестве выходного интерфейса (outgoing interface) выбирается порт SL На этом этапе значение выходной метки (outgoing label) не устанавливается.

После этого устройство LSR2 посылает свою информацию о локальной привязке меток устройствам LSR1, LSR3 и LSR4. В этот момент ни одно из них не использует маршрутизатор LSR2 в качестве следующего транзитного перехода для достижения 172.16.0.0/16, поэтому они не могут обновить выходные метки в записях баз LFIB для сети 172.16.0.0/16.

Однако, когда устройство LSR3 посыпает свою локальную информацию о метках устройствам LSR2, LSR5 и LSR6, то маршрутизатору LSR2 известно, что эта информация поступила от узла следующего транзитного перехода для сети 172.16.0.0/16, и он использует ее в качестве привязки меток удаленного маршрутизатора для класса 172.16.0.0/16. Предположим, что значение метки, произвольно выбранное устройством LSR3, равно 45. Устройство LSR2 использует метку, предоставленную маршрутизатором LSR3, для обновления значения выходной метки (outgoing label) в соответствующей записи своей базы LFIB, связанной с классом FEC 172.16.0.0/16. Аналогичным образом устройство LSR4 определяет, что маршрутизатор LSR5 является следующим транзитным переходом для класса FEC, связанного с сетью 172.16.0.0/16. Теперь устройство LSR4 произвольным образом выбирает метку из своего пула, используя базу LIB. Предположим, что значение этой метки равно 65. После этого устройство LSR4 использует эту метку как индекс в свое базе LFIB для нахождения совпадающей позиции, которая будет изменена. После того как найдено соответствие, поле входной метки (incoming label) данной позиции устанавливается равным 65. В качестве следующего транзитного перехода (next hop) устанавливается маршрутизатор LSR5, а в качестве выходного интерфейса (outgoing interface) используется порт S1. Затем устройство LSR4 посылает информацию о локальной таблице меток устройствам LSRI, LSR2 и LSR5. В этот момент ни одно из устройств LSRI, LSR2, LSR5 не использует маршрутизатор LSR2 в качестве следующего транзитного перехода к сети 172.16.0.0/16 и, следовательно, не может

обновить выходную метку в записи базы LFIB для сети 172.16.0.0/16.

Однако, когда маршрутизатор LSR5 посылает локальную информацию устройствам LSR4, LSR3 и LSR6, устройству LSR4 известно, что информация поступила от маршрутизатора следующего транзитного перехода для сети 172.16.0.0/16 и использует эту информацию в качестве таблицы меток удаленного устройства для класса 172,16.0.0/16. Предположим, что такое произвольно выбранное устройством LSR5 значение метки равно 95. После этого устройство LSR4 использует метку, предоставленную устройством LSR5, для обновления своей выходной метки (outgoing label) в записи базы LFIB, связанной с классом FEC 172J6.0.0/16. Когда маршрутизатор LSR6 посылает свою информацию о локальных метках устройствам LSR3 и LSR5, этим устройствам известно, что она поступила от узла следующего транзитного перехода для сети 172.16.0.0/16, и они оба используют ее в качестве таблицы меток удаленного устройства для класса FEC 172.16.0.0/16. Предположим, что это произвольно выбранное устройством LSR5 значение метки равно 33. В таком случае оба устройства, LSR3 и LSR5, используют метку, предоставленную устройством LSR6, для обновления *выходной метки* (outgoing label) в записях своих баз LFIB, связанной с классом FEC 172.16.0.0/16. Устройство LSR6 не содержит выходной метки в базе LFIB для класса 172.16.0.0/16, поскольку оно непосредственно подсоединено к сети 172,16.0.0/16, Для этой сети устройство LSR6 представляет собой граничное LSR-устройство, поэтому оно удаляет метку из пакета перед отправкой его в сеть 172.16.0.0/16.

На этой стадии, как показано в табл. 3.3, у всех LSR-устройств записи баз LFIB для класса FEC 172.16.0.0/16 заполнены, и они готовы к пересылке пакетов. Когда устройство LSRI получает пакет со значением метки, равным 50, оно использует ее в качестве индекса своей информационной базы LFIB для поиска записи необходимой для пересылки пакетов. После того как соответствующая позиция найдена, устройство обменивает значение метки на значение выходной метки, равное 25, и отправляет пакет через интерфейс S0 на устройство LSR2, которое осуществляет аналогичный поиск по своей базе, обменивает значение метки на значение 45 и направляет пакет устройству LSR3 через интерфейс S1. Устройство LSR3 выполняет поиск в базе LFIB, меняет значение метки на 33 и направляет пакет устройству LSR6 через интерфейс S1. В конечном итоге устройство LSR6 удаляет метку из пакета и направляет его к пункту назначения через интерфейс E0. В случае удаления метки на предпоследнем переходе, т.е. на устройстве LSR3, маршрутизатор LSR6 может выполнить поиск либо в базе LFIB, либо *в* таблице маршрутизации 3-го уровня.

Таблица 3.3

Устройство	Записи базы LFIB после распространения меток			
	Входная метка	Выходная метка	Следующий транзитный переход	Выходной интерфейс
LSR1	50	25	LSR2	SO
LSR2	25	45	LSR3	S1
LSR3	45	33	LSR6	S1
LSR4	65	95	LSR5	S1
LSR5	95	33	LSR6	S1
LSR6	33	—	LSR6	E0

Встановлення маршруту LSP за допомогою механизму впорядкованого контролю

При использовании для установки маршрута LSP метода упорядоченного контроля входное или выходное граничное LSR-устройство инициирует установку маршрута LSR Назначение меток происходит упорядоченным образом от конечной (выходной) до начальной (входной) точек LSP-маршрута. Установка пути LSP может быть начата с любого конца — со входа или с выхода. Устройство, инициирующее создание маршрута LSP, выбирает классы FEC, и все остальные LSR-устройства на данном LSP-маршруте используют те же самые записи FEC. Такой метод контроля при установке маршрута LSP требует, чтобы информация о привязке меток была распространена по всем LSR-устройствам до определения маршрута LSP. Описываемый подход приводит к тому, что время конвергенции при этом в несколько раз больше, чем при независимом контроле. Однако при использовании метода упорядоченного контроля вероятность возникновения петель на маршруте LSP меньше чем при независимом контроле.

Пример установки LSP-маршрута упорядоченным методом приведен на рис. ЗЛО. В этом примере устройство LSR7 является выходным LSR-маршрутизатором, которое инициирует установку LSP-маршрута. Устройству LSR7 известна своя роль, поскольку оно имеет непосредственное соединение с сетью 192.168.0.0/16. Предположим, что маршрутизатор LSR7 назначает классу FEC 192.168.0.0/16 метку со значением 66. После этого он извещает о своей локальной метке соседнее устройство LSR6. Получив такое оповещение, маршрутизатор LSR6 назначает данному классу FEC новую метку со значением 33 и сообщает о привязке метки к сети своим соседям: устройствам LSR3 и LSR5. Упорядоченная установка маршрута LSP продолжается таким способом на протяжении всего маршрута LSP ко входному или иному устройству LSR1.

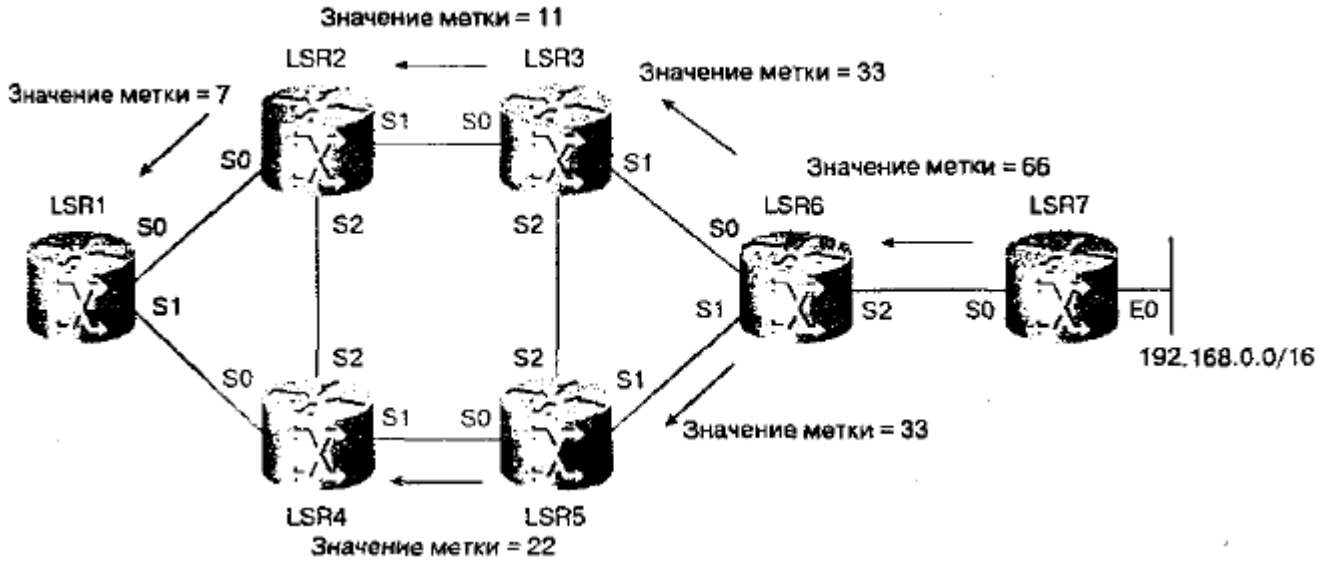


Рисунок 3.10 - Упорядоченный контроль при установке маршрута LSP

Внимание!

Программное обеспечение Cisco IOS использует режим независимого контроля (independent control) при установке LSP-маршрутов для сетей MPLS и упорядоченный контроль (ordered control) — для MPLS-сетей ATM.

Висновки

В сетях MPLS для отправки пакетов используются метки. Входной узел MPLS назначает пакету класс FEC единожды — при поступлении пакета в сеть. Назначаемый пакету FEC кодируется как короткое значение фиксированной длины, называемое меткой. Метки присваиваются пакетам до их отправки. При последующих переходах анализ заголовка сетевого уровня не производится. Метка используется как индекс позиции в таблице, которая указывает адрес следующего транзитного перехода и новую метку. Прежняя метка заменяется новой, и пакет отправляется к следующему транзитному переходу.

Узлы MPLS имеют две структурных плоскости — плоскость отправки и плоскость управления. Узлы MPLS, кроме коммутации помеченных пакетов, могут выполнять маршрутизацию 3-го уровня и коммутацию 2-го уровня. Плоскость отправки MPLS отвечает за отправку пакетов на основе значений, содержащихся в назначенных метках. Плоскость управления использует информационную базу LFIB, поддерживаемую узлом MPLS, для отправки помеченных пакетов. Плоскость управления также отвечает за создание и поддержку базы LFIB.

При использовании MPLS-коммутации LSR представляют собой устройства, которые реализуют функции управления и отправки. LSR-устройства отправляют пакеты на основе значения метки, инкапсулированной в пакете. LSR-устройства могут также отправлять обычные пакеты 3-го уровня. В качестве LSR-устройств применяются маршрутизаторы, обладающие функциями MPLS, или ATM-коммутаторы, использующие метки для передачи пакетов по сети.

Маршрут LSP представляет собой сконфигурированное соединение между двумя LSR-устройствами, в котором для пересылки пакетов используется коммутация по

меткам. LSP-маршрут представляет собой путь передачи потоков данных через сеть MPLS. Маршруты LSP создаются с помощью протоколов LDP, TDP, RSVP-TE, CR-LDP или расширений протоколов маршрутизации.

Установка LSP-маршрутов может быть осуществлена двумя способами: методом независимого контроля и методом упорядоченного контроля. Оба способа могут применяться в сети одновременно, и при этом не возникает структурных проблем или проблем совместимости устройств. Метод независимого контроля ускоряет сходимость и установку LSP-маршрутов, поскольку LSR-устройства при преобразовании меток и распространении информации о них не затрачивают время на распространение сообщений в границах сети. Установка LSP-маршрутов происходит сразу после окончания конвергенции протоколов маршрутизации. При применении метода упорядоченного контроля перед установкой LSP-маршрута в сети распространяется информация о привязке меток. Однако второй метод контроля обеспечивает большие возможности предотвращения кольцевых маршрутов.

В сети с коммутацией по меткам для распространения информации о привязке меток среди LSR-устройств используется протокол LDP вместе со стандартными протоколами маршрутизации сетевого уровня. Протокол LDP позволяет LSR-устройствам распространять метки между LDP-устройствами одного и того же ранга с помощью протокола TCP. Использование TCP в качестве протокола транспортного уровня обеспечивает гарантированную доставку информации протокола LDP с помощью надежных механизмов упраапения потоками и обработки заторов.

Структура среды MPLS позволяет LSR-устройствам явным образом запрашивать у устройства следующего перехода информацию о привязке меток для класса FEC. Такая операция известна как нисходящее распространение меток по требованию. Структура MPLS также позволяет распространять информацию о связывании среди LSR-устройств, которые не запрашивали ее явным образом. В таком случае говорят о нисходящем распространении меток без запроса. Оба способа распространения меток могут использоваться в сети одновременно.

Существует три способа контроля процесса образования маршрутных петель в сетях MPLS; временное сохранение петель, обнаружение петель и предотвращение петель. При использовании механизма временного сохранения петель пакеты, движущиеся по маршруту с петлей, не могут повлиять на передачу пакетов, не попавших на маршрут с петлей. Такой механизм может быть использован узлами MPLS, которые уменьшают время существования (TTL) маршрута LSP. Сегменты, в которых не используется TTL, такие как каналы ATM, выделяют буферное пространство для каждого VC-канала на ATM-коммутаторах для контроля образования петель. Кроме временного сохранения петель, в качестве дополнительного средства для обнаружения петель может быть использован подход, известный как подсчет количества переходов. Сущность его такова, как из метода с использованием параметра времени существования. Однако при этом информация о количестве переходов передается в запросах и ответах протоколов LDP или TDP. Использование метода предотвращения петель позволяет не допустить образования маршрутов с петлей до того, как по ним будут отправлены пакеты с данными.

ЛЕКЦІЯ 6
ЗАНЯТТЯ 7
ОРГАНІЗАЦІЯ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ В СЕРЕДОВИЩІ MPLS

В этом разделеглаве будет осуществлено рассмотрение следующих вопросов.

Обзор VPN-сетей: Виртуальные частные сети представляют собой замкнутый группы пользователей, использующих общую сетевую инфраструктуру. В этом разделе описываются и сравниваются службы TDM, X.2S, Frame Relay, SMDS и ATM. В Нем также рассмотрены виртуальные частные IP-сети.

VPN-сети с установлением соединения: VPN-сети с установлением соединения могут быть построены на базе инфраструктуры 2-го или 3-го уровня. В этом разделе обсуждаются VPN-сети 3-го уровня, созданные с использованием каналов с установлением соединения типа "точка-точка1', таких как виртуальные соединения Frame Relay и ATM. В нем также рассматриваются ориентированные на соединение VPN-сети 3-го уровня, использующие общую инкапсуля- цию маршрута (Generic Route Encapsulation — GRE) и открытых стандартов обеспечения безопасности (IP Security — IP Sec).

VPN-сети без установления соединения: Сетям VPN без установления соединения для установки связи между двумя конечными точками не требуются заранее определенные логические или виртуальные каналы. В этом разделе рассматриваются такие VPN-сети без установки соединения; как IP и MPLS.

Сравнение VPN-технологий: В этом разделе сравниваются различные технологии VPN и даются рекомендации по выбору VPN-технологии, исходя из типа приложения, требований безопасности, расширяемости, стоимости и других факторов.

Преимущества VPN-сетей MPLS: В этом разделе обсуждаются преимущества VPN-сетей MPLS с точки зрения провайдера служб. Рассматриваются такие вопросы, как расширяемость, безопасность, адресация, перераспределение потоков и качество обслуживания.

Огляд VPN-мереж

Провайдеры предлагают службы виртуальных частных сетей (Virtual Private Network — VPN) промышленным пользователям с момента начала эксплуатации сетей на базе TDM и сетей X.25 с коммутацией пакетов. Позднее сети Frame Relay и сети на основе технологии ATM с несколькими классами обслуживания в значительной степени заменили X.25 и выделенные линии. Провайдеры служб устанаапивают либо фиксированную стоимость служб VPN, либо оплату, зависящую от интенсивности пользования службой.

Термин "виртуальная частная сеть" (VPN) используется операторами связи и провайдерами служб для обозначения совокупности виртуальных каналов закрытых групп пользователей с момента разработки и начала применения служб X.25, Frame Relay, SMDS и ATM. Позднее этот термин стал использоваться при управлении промышленными сетями (Enterprise Network Management) для обозначения закрытых групп пользователей в IP-сетях.

Пользователи давно осознали преимущества заключения субдоговора на телекоммуникационные услуги с внешними провайдерами (outsourcing) и объединения служб данных, голоса и видео. Поэтому для них желательно использование службы управляемого протокола IP (Managed IP) с соглашениями об уровне обслуживания

(Service-Level Agreement — SLA) на всем маршруте передачи данных (end-to-end) и с гарантированным качеством обслуживания (QoS).

VPN-сети на базе протокола IP быстро становятся основой доставки объединенных голоса и видео и обычных цифровых данных. Многие провайдеры служб предлагают приложения с дополнительным» услугами (value-added) в дополнение к своим транспортным VPN-сетям.

Появляющиеся новые службы, такие как электронная торговля, размещение приложений и мультимедийные службы, позволяют провайдерам получить дополнительный доход и повысить конкурентоспособность. Основой обеспечения консолидированных служб являются две уникальные и дополняющие друг друга структуры сетей VPN, которые основаны на технологиях набора открытых стандартов обеспечения безопасности (IP Security — IPSec) и многопротокольной коммутации по меткам (Multiprotocol Label Switching — MPLS). В настоящей главе рассматриваются доступные в настоящее время топологии и структуры сред VPN.

Использование VPN-функций в протоколе IP позволяет установить в сетях на основе программного обеспечения Cisco IOS магистральные службы расширяемых VPN-сетей 3-го уровня с использованием протокола IP версии 4 (IPv4). VPN-сети протокола IP являются базой, используемой компаниями для размещения и администрирования дополнительных служб, включая приложения, размещение и хранение данных, электронную торговлю и телефонные службы для коммерческих потребителей.

В сетях уровня предприятия внутренние сети на базе протокола IP радикально изменили стиль коммерческих компаний, В настоящее время компании перемещают коммерческие приложения в локальные сети с последующим распространением их на распределенную сеть (WAN).

Компании также объединяют потребности пользователей, поставщиков и партнеров путем использования внешних сетей (под такой сетью понимается внутренняя сеть, которая обслуживает предприятия). Используя такие сети, компании могут уменьшить производственные расходы за счет автоматизации учета поставок, обмена электронными данными (Electronic Data Interchange — EDI) и других форм электронной торговли. Для того чтобы воспользоваться этими коммерческими возможностями, провайдерам служб требуется технология VPN-сетей протокола IP, которая предоставляет предприятиям службы частных сетей по совместно используемым инфраструктурам.

Поскольку большинство междугородных операторов связи (IntereXchange carriers — IXCs), государственных местных операторов связи (Incumbent Local Exchange Carriers — ILECs) и частных местных операторов связи (Competitive Local Exchange Carriers — CLECs) уже имеют инфраструктуру ATM или Frame Relay, технология MPLS часто оказывается оптимальным решением для построения устойчивых, надежных и легко расширяемых VPN-сетей.

VPN-мережі з втановленням з'єднань

VPN-сети с установлением соединения могут быть созданы на базе инфраструктуры 2-го или 3-го уровня. Примерами таких VPN-сетей 2-го уровня могут служить каналы с установлением соединения типа "точка-точка", такие как виртуальные соединения Frame Relay или ATM.

Примером VPN-сетей с установлением соединения 3-го уровня могут служить

структуры VPN, созданные с использованием полносвязной или частично-связной топологии туннелей на базе протокола IPSec (с шифрованием для обеспечения конфиденциальности) или с использованием технологии общей инкапсуляцией маршрутизации (Generic Routing Encapsulation — GRE).

VPN-сети доступа к службе используют механизм установления соединения с коммутацией каналов, обеспечивающие временное безопасное соединение удаленного доступа между индивидуальным пользователем (таким как мобильный пользователь или телеработник) и внутренней или внешней корпоративной сетью (intranet и extranet) через совместно используемую сеть провайдера службы с той же стратегией передачи данных, как и в частной сети. Такие сети используют удаленный доступ к точке присутствия (Point of Presence — PoP) провайдера ISP с последующей передачей данных по открытой сети Internet с конечным доступом к внутренней корпоративной сети.

Главной проблемой в VPN-сетях с установлением соединения является сложность расширения сети. В частности, эффективность VPN-сетей с установлением соединения без полносвязной топологии далека от оптимальной. Кроме того, в случае VPN-сетеЙ 3-го уровня при передаче по сети Internet невозможно твердо гарантировать качество обслуживания (Quality of Service — QoS) при передаче данных по такой структуре. С точки зрения менеджеров телекоммуникаций (telecom management) сложность создания виртуальных каналов ATM или Frame Relay сравнима со сложностью создания выделенных линий.

Использование VPN-сетей на базе виртуальных каналов требует от провайдера службы создания отдельных виртуальных каналов и управления ими или создания логических маршрутов и управления ими для каждой пары узлов, входящих в группу пользователей и осуществляющих обмен данными. Такое требование эквивалентно построению полносвязной топологии виртуальных каналов, включающей всех пользователей.

§1. Мережі VPN другого рівня з встановленням з'єднання

VPN-сети 2-го уровня с установлением соединения являются основой VPN-модели передачи информации одного уровня в среде другого. В этой модели провайдер службы предоставляет виртуальные каналы, а обмен маршрутной информацией происходит непосредственно между маршрутизаторами пользователя (т.е. CPE).

Мержі на основі технології TDM

Большинство провайдеров служб предлагают пользователям службы сетей с выделенными линиями. Они включают в себя цифровое мультиплексирование, при использовании которого из битового потока практически одновременно выделяются данные двух или более каналов, и их биты передаются поочередно. В Северной Америке провайдеры служб и операторы связи предлагают пользователям линии DS1 и DS3, а в Европе и в Тихоокеанском регионе, как правило, используются линии E1 и E3.

Как показано на рис. 4.1, пользователи А и Б совместно используют физическую инфраструктуру оператора связи, но логически отделены друг от друга механизмом преобразования адресов портов и электронными перекрестными соединениями, которые обеспечиваются оператором связи. Перекрестные соединения обычно

обеспечиваются системами DACS (Digital Automatic and CrossConnect System — система цифрового доступа и коммутации). Однако для достижения указанной цели также широко используются физические соединения.

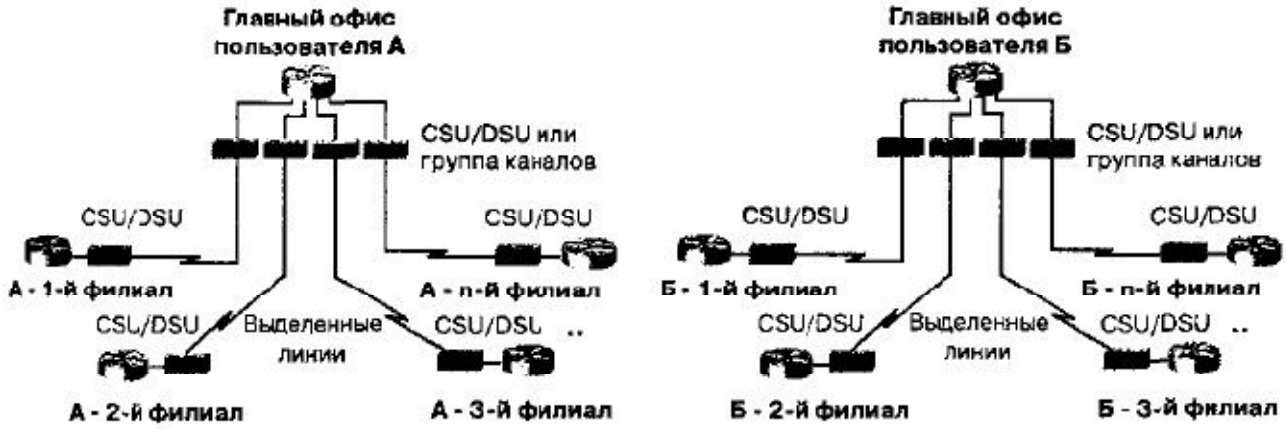


Рисунок 4.1 - Логическая схема использования выделенных линий в VPN-сетях

На рис. 4,2 показаны физические соединения между пользователями А и Б, а также сеть провайдера службы в целом.

Сеть TDM предстаатяет собой простейший пример виртуальной частной сети, предоставляющей пользователям фиксированную полосу пропускания высокого качества. Большинство операторов связи предоставляют пользователям полосу пропускания, кратную 64 Кбит/с (полоса пропускания одного канала DS0). Более подробная информация о TDM приведена в разделе "Коммутация каналов и TDM" главы 2, "Технологии распределенных сетей и коммутация MPLS".

VPN-мережі на основі технології передачі фреймів

VPN-сети на основе фреймов, такие как Frame Relay и X.25, используют логические маршруты, определяемые коммутируемыми и постоянными виртуальными каналами. Как показано на рис. 4.3, при этом несколько закрытых групп пользователей, совместно используют коммутируемую инфраструктуру провайдера службы. Пользователям предоставляется доступ только к тем виртуальным каналам, которые предназначены исключительно для частного использования. Такие каналы PVC или SVC могут предоставляться с фиксированной согласованной скоростью передачи (CIR) или на скорости порта (равной ширине полосы пропускания абонентского канала — local loop).

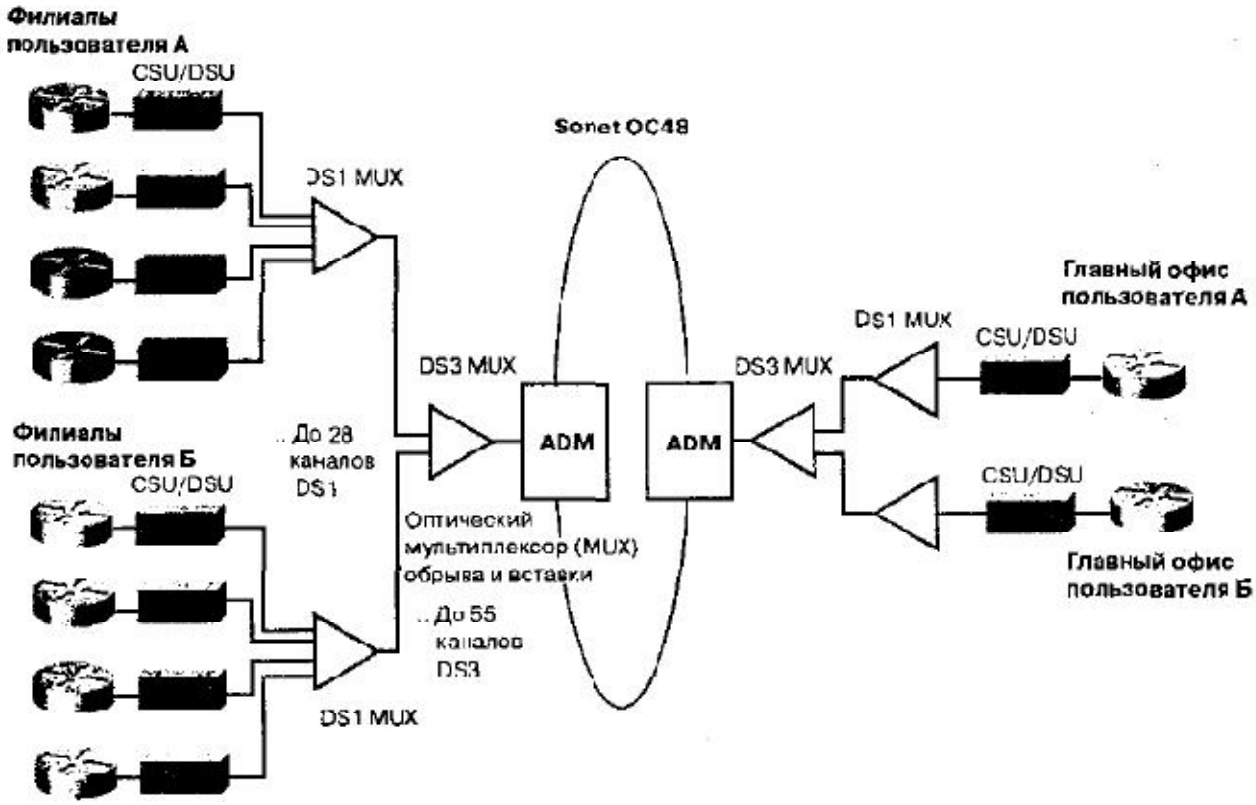


Рисунок 4.2 - Сеть VPN с выделенными линиями

На рис. 4.4 показана физическая картина сети Frame Relay. Оба пользователя А и Б подсоединены к точкам присутствия (Points of Presence — POPs) провайдера абонентских каналов TDM. Протокол Frame Relay функционирует между локальным CPE-устройством FRAD (например, маршрутизатор: Frame Relay Access Device — маршрутизатор, мультиплексор или другое устройство доступа к сети Frame Relay) и коммутатором Frame Relay.

Функция межсетевого обмена протокола Frame Relay преобразует фреймы Frame Relay в ячейки ATM для передачи по магистрали ATM.

Более подробное описание технологии Frame Relay приведено в разделе "Коммутация пакетов и ячеек" главы 2, 'Технологии распределенных сетей и коммутация MPLS".

Внимание!

В технологии X.25 на 2-м уровне используются фреймы X.25, а на 3-м уровне— пакеты X.25, в отличие от технологии Frame Relay, в которой используются только фреймы 2-го уровня. Провайдеры службы X.25 обычно предоставляют по желанию заказчика коммутируемые виртуальные каналы SVC или постоянные каналы PVC, которые описываются идентификаторами логического канала (Logical Channel Identifier— LCI). Идентификатор LCI включает в себя 4-битовый номер логической группы (Logical Group Number— LGN) и 8-битовый номер логического канала (Logical Channel Number — LCN). X.25 в качестве протокола создания фреймов на 2-м уровне использует сбалансированную процедуру доступа к каналу (Link Access Procedure Balanced — LAP B).

Дополнительная информация о протоколе X.25 приведена в "Рекомендации по протоколу X.25" (1996 г.) сектора стандартов Международного союза телекоммуникаций.

Этот документ можно получить по адресу www.itu.int/itudoc/itu-t/rec/x/xl-199/sx25.html.

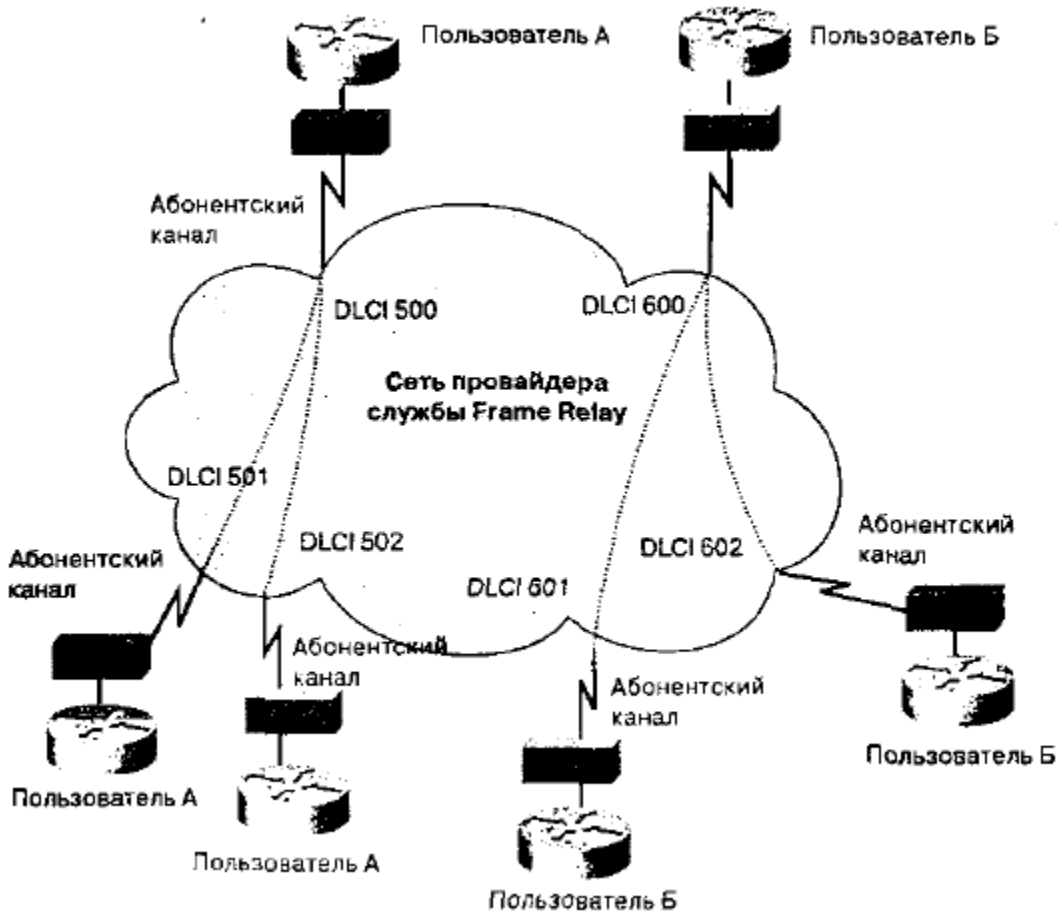


Рисунок 4.3 - Логическая структура VPN-сети Frame Relay

VPN-мережі основі на технології передачі комірок

VPN-сети на основе передачи ячеек, такие как ATM и SMDS, используют логические маршруты, определяемые коммутируемыми (SVC) и постоянными (PVC) вирту-ачьными каналами. При этом, как показано на рис. 4.5, несколько закрытых групп пользователей или потребителей совместно используют коммутируемую инфраструктуру провайдера службы. Пользователям предоставляются виртуальные каналы, зарезервированные исключительно для частного использования. Такие каналы PVC или SVC могут предоставляться со следующими классами обслуживания: CBR, VBR-RT, VBR-NRT, ABR и UBR. В сетях ATM также могут предоставляться перепрограммируемые каналы PVC (soft PVC), представляющие собой гибрид каналов SVC и PVC.

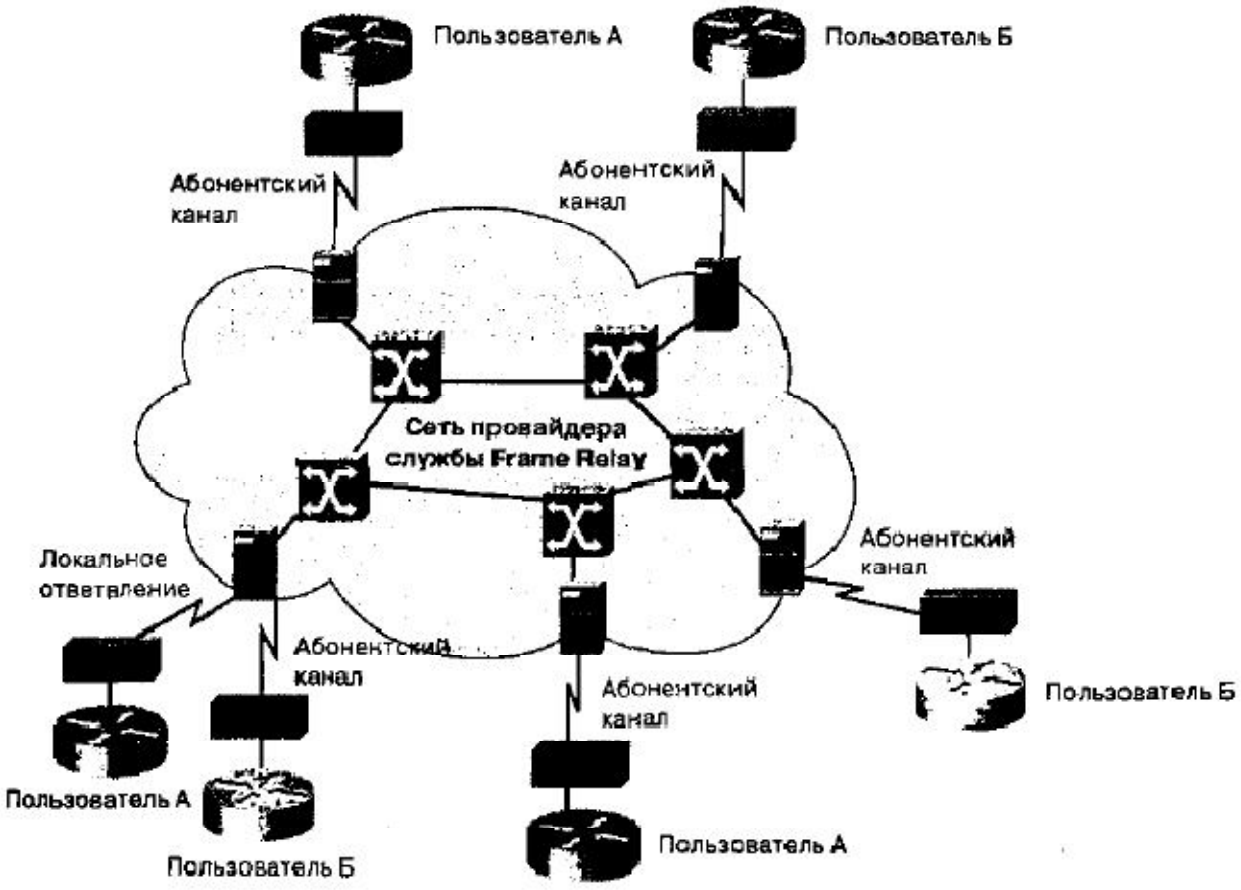


Рисунок 4.4 - Физическая структура сети VPN в среде Frame Relay

На рис. 4.6 показана физическая структура сети ATM. Пользователи А и Б подсоединены к точкам присутствия (Points of Presence — POPs) сети ATM с помощью абонентских каналов TDM или SONET/SDH на полной пропускной способности. ATM-маршрутизаторы оборудования пользователя (CPE) используют виртуальные каналы ATM в качестве транспортного механизма 2-го уровня для передачи данных протокола IP или любого другого протокола 3-го уровня.

§2. Мережі VPN третього рівня з встановленням з'єднання

VPN-сети 3-го уровня, в которых используется процедура установления соединения, яштяются основой туннельной модели VPN. При использовании технологий GRE или IP Security (IPSec) создается туннельная модель соединений "точка-точка" через внутреннюю сеть IP или через открытую сеть Internet, в то время как виртуальные частные сети удаленного доступа (Virtual Private Dialup Network — VPDN) представляют собой гибридную комбинацию удаленного доступа и безопасного туннельного соединения через среду Internet к точке концентрации трафика предприятия, такой как корпоративный шлюз.

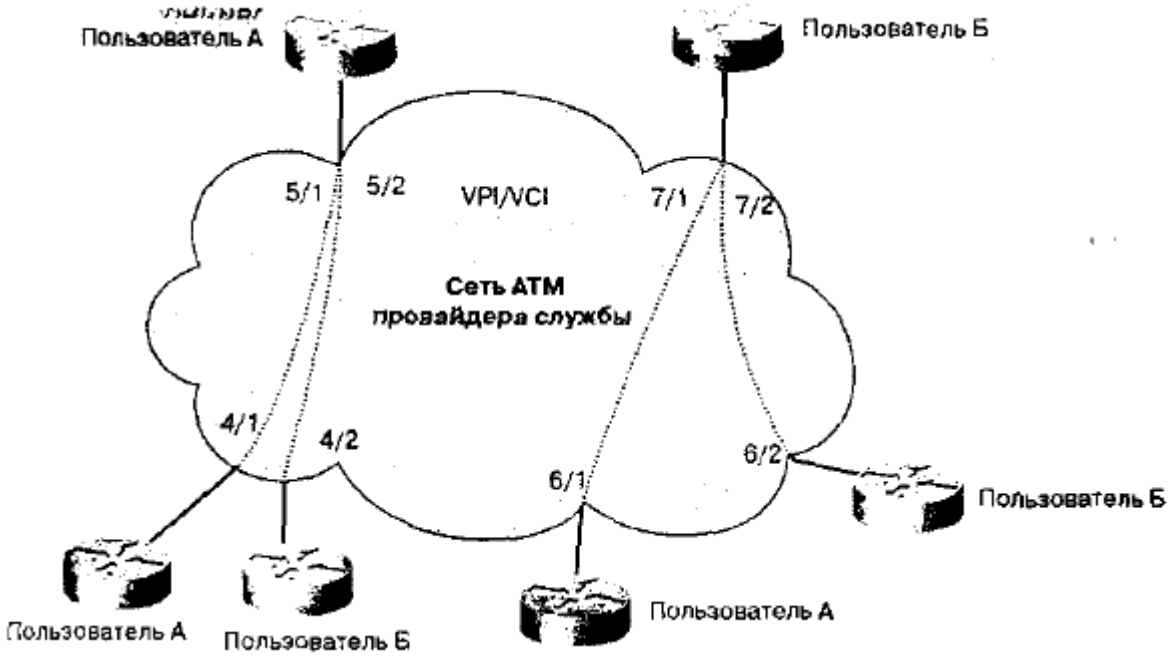


Рисунок 4.5 - Логическая структура VPN-сетей ATM

Тунельні VPN-мережі протоколу GRE

Туннельные VPN-сети протокола общей инкапсуляции маршрутизации (Generic Route Encapsulation — GRE) могут быть использованы для создания IP-соединений типа "точка-точка". Комбинация таких GRE-туннелей может быть использована для построения VPN-сети. Однако присущая GRE-туннелям недостаточная внутренняя безопасность, вытекающая из отсутствия механизмов шифрования, делает GRE-туннели недостаточно защищенными от несанкционированного доступа.

Как показано на рис. 4.7, использование GRE-туннелей целесообразно для построения VPN-сетей в частной магистральной IP-сети провайдера службы. Они также полезны для передачи по туннельным соединениям потоков данных 3-го уровня, отличных от IP, в частной IP-сети.

VPN-мережі протоколі IPSec з тунельними з'єднаннями

IPSec представляет собой технологию с высокой степенью безопасности, использующую шифрование и механизм создания туннельных соединений, которые защищают содержимое пакетов при прохождении по IP-сети. Протокол IPSec, как правило, используется при передаче данных через открытые недостаточно безопасные IP-сети, такие как Internet. Комбинация туннелей IPSec типа "точка-точка" позволяет создавать VPN-сети в открытых IP-сетях, Большая часть структуры IPSec реализуется на CPE-оборудовании пользователя, а провайдеры служб, как правило, предоставляют VPN-службы управляемого протокола IPSec (Managed IPSec). Топология сети, использующей технологию IPSec, приведена на рис. 4.7. Для мобильных пользователей и телеработников, которым требуется безопасный удаленный доступ, IPSec в настоящее время является единственной практической возможностью получения такого доступа через VPN-сеть.

Внимание!

VPDN-сети, использующие протоколы L2F И L2TP, также предоставляют определенную степень безопасности при удаленном доступе, хотя и не столь высокую,

как технология IPSec. Высокая эффективность защиты протокола IPSec обеспечивается глубоким шифрованием содержимого с помощью различных разновидностей стандарта шифрования данных (Data Encryption Standard— DES), таких как 168-битовый стандарт 3DES и аутентификация по заголовкам.

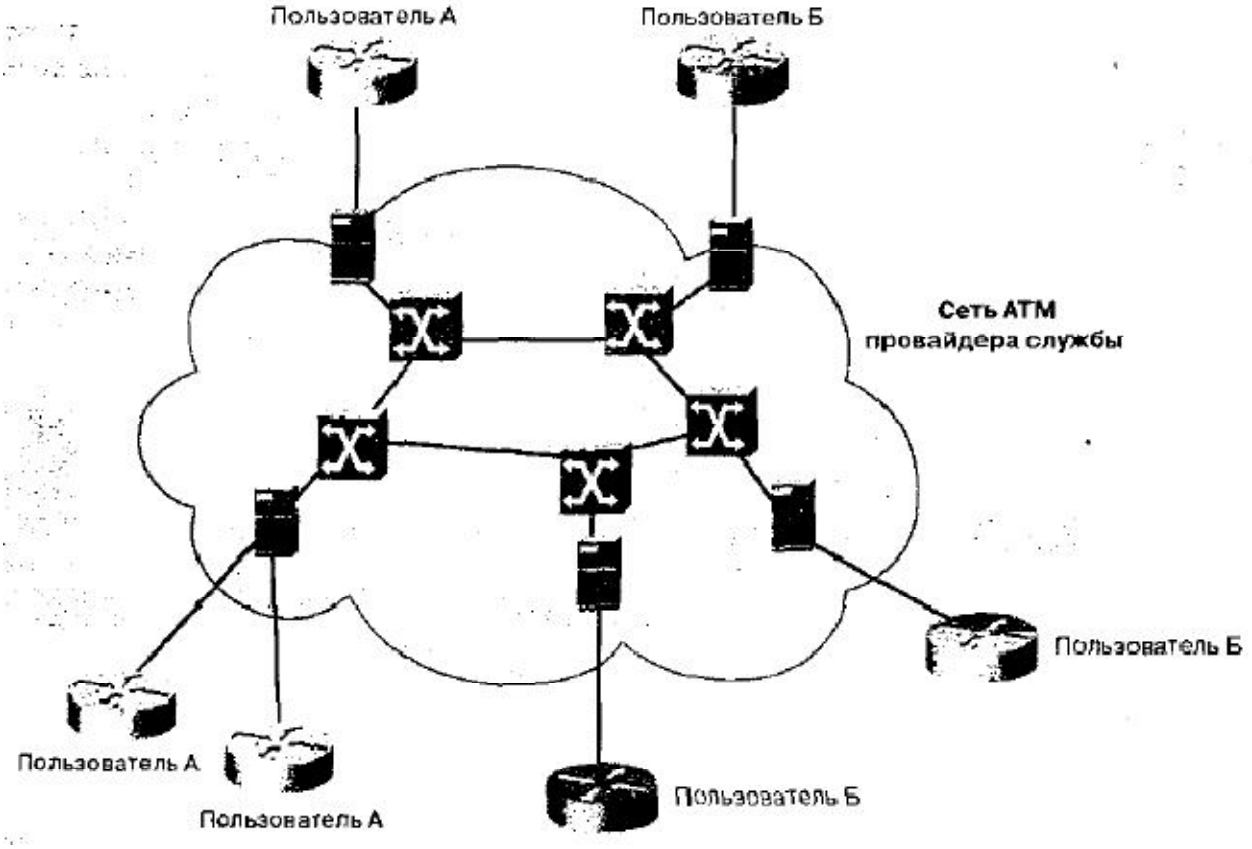


Рисунок 4.6 - Физическая структура VPN-сети ATM

Віртуальні приватні мережі віддаленого доступу

Телеработники и мобильные пользователи получают удаленный доступ к своим корпоративным сетям через службы открытой коммутируемой телефонной сети (Public Switched Telephone Network — PSTN) или через службы ISDN. Как показано на рис. 4.8, службы виртуальной частной сети удаленного доступа (Virtual Private Dialup Network — VPDN) реализуются главным образом по частной IP-магистрали провайдера. Для реализации служб VPDN по IP-сети используются такие протоколы, как протокол пересылки 2-го уровня (Layer 2 Forwarding — L2F) и протокол туннельного соединения 2-го уровня (Layer 2 Tunneling Protocol — L2TP),

Удаленные пользователи инициируют соединение удаленного доступа с сетевым сервером доступа (Network Access Server — NAS), используя протокол PPP, Сервер NAS выполняет аутентификацию вызова и напрааляет ячейки с помощью протоколов L2F или L2TP к корпоративному шлюзу пользователя. Шлюз принимает вызов, направленный серверу NAS, выполняет дополнительную аутентификацию и авторизацию, после чего завершает сеанс PPP пользователя. Функции аутентификации, авторизации и учета (Authentication, Authorization and Accounting — AAA) также могут быть выполнены сервером AAA, таким как TACACS+. Все параметры сеанса PPP согласовываются между пользователем удаленного доступа и корпоративным шлюзом. На VPN-сети удаленного доступа, такие как VPDN, имеют

определенные ограничения: они не поддаются расширению и не обеспечивают связь "всех-со-всеми".

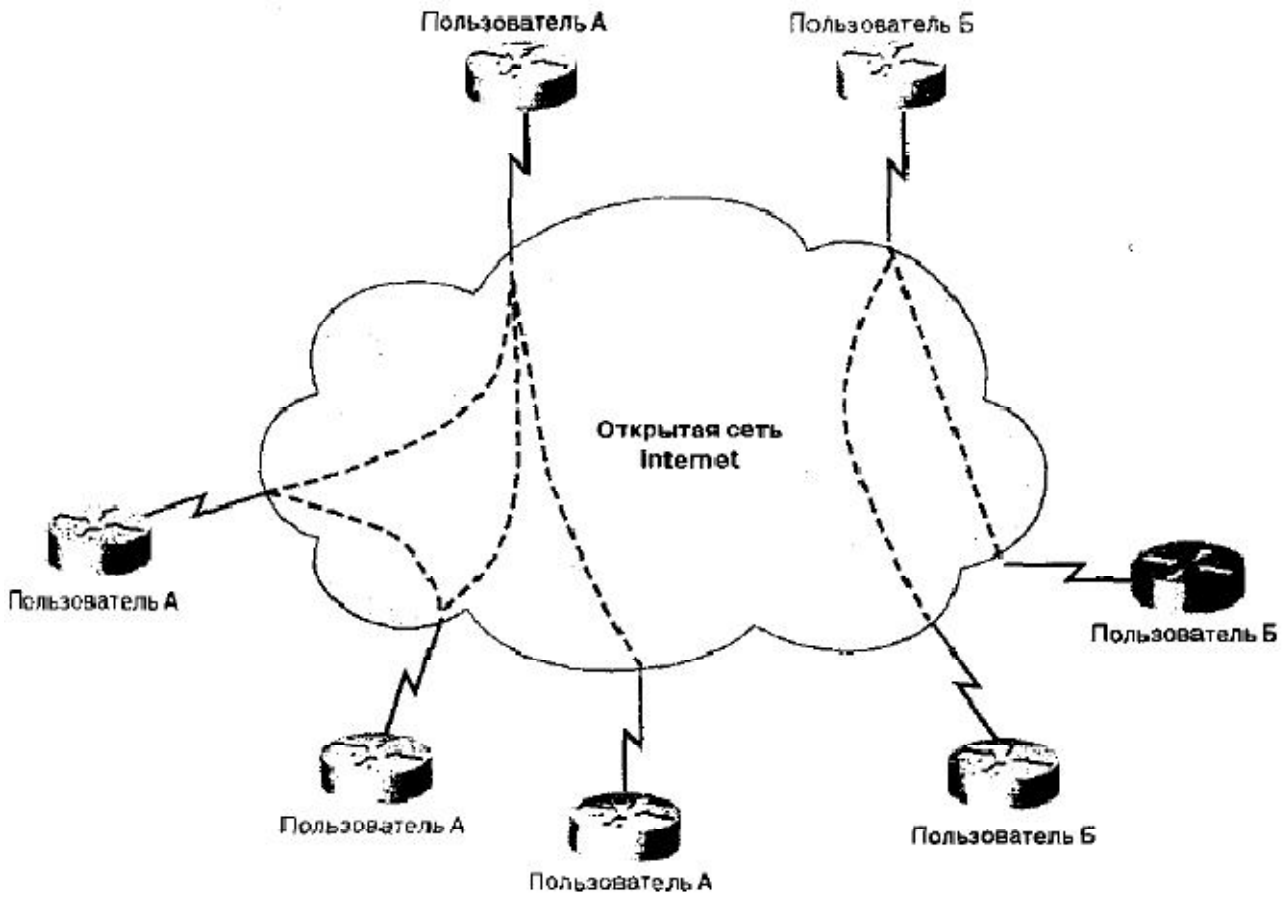


Рисунок 4.7 - Туннельные VPN-cennt протоколов GRE and IPSec

Протокол туннельного соединения типа "точка-точка" (Point-to-Point Tunneling Protocol — PPTP), наряду с протоколом шифрования "точка-точка" корпорации Microsoft (Microsoft Point-to-Point Encryption — MPPE), позволяет VPN-сетям на основе оборудования корпорации Cisco использовать PPTP в качестве протокола туннельного соединения. PPTP предсташшет собой сетевой протокол безопасной передачи данных от удаленного клиента к серверу частного предприятия путем создания VPN—сети в IP-сети. Протокол PPTP использует туннели по желанию пользователя (также называемые туннелями, инициированными пользователем, client-initiated tunneling), что позволяет клиентам сконфигурировать и установить зашифрованные туннели к туннельным серверам без промежуточного участия сервера NAS в согласовании параметров и установке туннеля.

Протокол PPTP использует MPPE в качестве метода шифрования при передаче данных по каналу удаленного доступа или по туннелю VPN-сети. MPPE функционирует как вспомогательная функция протокола сжатия типа "точка-точка" корпорации Microsoft (Microsoft Point-to-Point Compression — MPPC). MPPE использует шифровальные ключи длиной 40 или 128 бит. Все ключи создаются на основе передаваемого открытым текстом пароля пользователя. Алгоритм MPPE представляет собой механизм шифрования потока, поэтому зашифрованные и расшифрованные фреймы имеют ту же длину, что и первоначальные фреймы. Cisco-

реализация MPPE полиостью совместима и взаимозаменяема с реализацией корпорации Microsoft и использует все доступные опции последней, включая режим шифрования без предыстории.

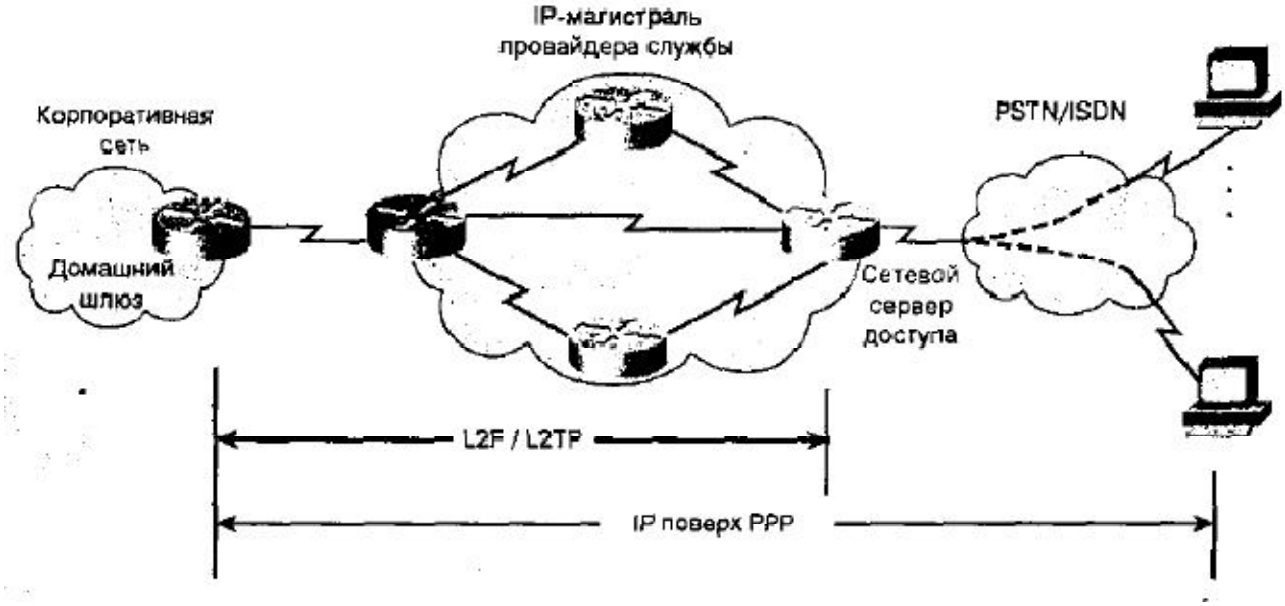


Рисунок 4.8 - Виртуальная частная сеть удаленного доступа (VPDN)

§3 Мережі VPN на основі комутації MPLS

VPN-мережі з встановленням з'єднання

VPN-сети без установления соединения при установке связи между конечными точками не требуют наличия заранее заданного логического или виртуального канала между ними.

Меренжі 3-го рівня без встановлення з'єднання

Сети 3-го уровня без установления соединения составляют базу одноранговой модели. В такой модели обмен о маршрутной информацией происходит между маршрутизаторами CPE и маршрутизаторами провайдера.

Звичайні VPN-мережі протокола IP

Многие провайдеры предоставляют пользователям управляемые службы IP (managed IP services), что дает пользователям возможность подсоединить свои IP-маршрутизаторы CPE к частным IP-магистралям провайдера. Большинство провайдеров службы IP организуют свои IP-сети в инфраструктуре 2-го уровня, такой как сеть ATM или Frame Relay. Типичный пример VPN-сети IP приведен на рис. 4.9.

Обычно провайдеры для различных пользователей конфигурируют на своих магистральных маршрутизаторах несколько протоколов маршрутизации или несколько процессов маршрутизации. Как правило, устройство маршрутизации Cisco (Cisco Routing engine) поддерживает на отдельных маршрутизаторах несколько протоколов маршрутизации для подсоединения сетей, использующих различные протоколы. В протоколы маршрутизации еще при создании закладывался принцип независимого функционирования от других аналогичных протоколов. Каждый протокол собирает и анализирует необходимую ему информацию и реагирует на

изменения топологии индивидуальным образом. Например, протокол RIP использует в качестве метрики количество транзитных переходов, а протокол E1GRP — вектор метрической информации, состоящий из пяти элементов.

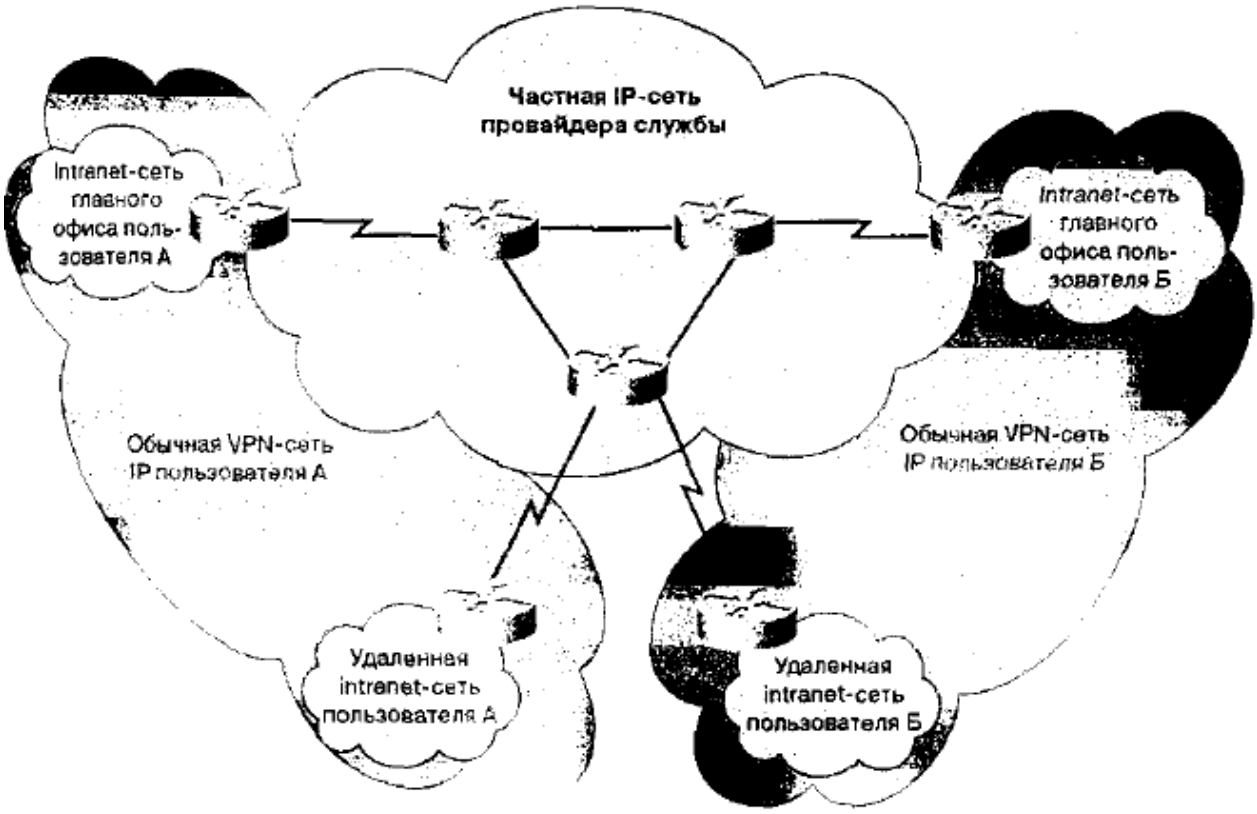


Рисунок 4.9 - Типовая VPN-сеть протокола IP на основе маршрутизаторов

Еще более важно то, что маршрутизаторы Cisco, как правило, могут одновременно обрабатывать до 30 процессов динамической IP-маршрутизации. При комбинировании различных процессов маршрутизации на одном маршрутизаторе могут использоваться следующие протоколы (приведены также имеющиеся ограничения):

- до 30 процессов IGRP-маршрутизации;
- до 30 процессов OSPF-маршрутизации;
- один процесс IS-IS;
- один процесс маршрутизации RIP;
- один процесс маршрутизации BGP;
- до 30 процессов маршрутизации EGP.

Пользователи получают доступ к VPN-сетям IP посредством комбинации списков доступа, протоколов маршрутизации и процессов. Самыми сложными проблемами, стоящими перед провайдерами управляемых IP-служб, являются расширяемость и сложность реализации. Большое количество доступных протоколов и процессов маршрутизации, поддерживаемых платформами маршрутизаторов, иногда вынуждает провайдеров размещать в точке присутствия отдельные маршрутизаторы для каждой пользовательской VPN-сети,

VPN-мережі на базі комутації MPLS

VPN-сети MPLS не устанавливают соединений. Механизмы MPLS разделяют

потоки данных на категории и обеспечивает конфиденциальность без использования туннельных протоколов 2-го уровня и шифрования. Такой подход значительно упрощает процесс инициализации сети.

Использование технологии MPLS позволяет решить проблемы расширяемости, возникающие при создании сетей Frame Relay и ATM за счет того, что провайдеры могут инициировать несколько сетей VPN для части пользователей, не инициируя все виртуальные каналы всех закрытых групп пользователей, число которых иногда составляет несколько десятков или даже сотен. Пример VPN-сети технологии MPLS приведен на рис. 4Л0. Пользователи А и Б совместно используют инфраструктуру провайдера, сохраняя способность формировать свои собственные замкнутые пользовательские группы с наивысшим возможным для них уровнем безопасности. Они также могут использовать собственные протоколы маршрутизации.

Модель MPLS требует, чтобы CPE-маршрутизаторы осуществляли непосредственный обмен маршрутной информацией только с граничными маршрутизаторами провайдера, вместо обмена такой информацией со всеми CPE-маршрутизаторами, принадлежащими к данной структуре VPN. Принадлежность устройств VPN-сети к замкнутой пользовательской группе фиксируется с помощью метки. Метки содержат информацию о следующем транзитном переходе, атрибуты службы и идентификатор VPN-сети, который обеспечивает конфиденциальность обмена информацией внутри структуры VPN.

На входе в сеть провайдера пакеты, поступающие от маршрутизатора CPE, обрабатываются, и им присваиваются метки в соответствии с физическим интерфейсом, на котором они были получены. Назначение меток основано на информации, содержащейся в таблицах маршрутизации и пересылки (VPN Routing and Forwarding — VRF). Необходимые таблицы составляются заранее, и входящие пакеты исследуются только на входном LSR-устройстве. Базовые устройства или LSR-устройства провайдера (Provider — P) лишь отправляют эти пакеты, основываясь на значениях меток.

Применение технологии MPLS дает возможность маршрутизируемым магистралям провайдера поддерживать VPN-сети и обеспечивает прозрачность механизмов 3-го уровня даже через инфраструктуры 2-го уровня. Такой подход позволяет создавать закрытые пользовательские группы и связанные с ними службы. Проектирование и конфигурирование VPN-сетеи MPLS подробно описано в главе 5 книги В.Олвейн, «Структура и реализация современной технологии MPLS»: Пер. с англ. — М.: Издательский дом "Вильямс", 2004. — 480 с.

Завдання на СРС

1. Переваги VPN мереж на базі технології MPLS

В процессе внедрения VPN-сетей для удовлетворения индивидуальных требований различных пользователей провайдеры должны рассмотреть вопрос о совместном использовании как технологии MPLS, так и IPSec. Обе технологии имеют определенные достоинства и дополняют друг друга, расширяя возможности средств для создания безопасного сквозного соединения VPN в инфраструктуре провайдера и через каналы открытой сети Internet.

В табл. 4.1 приведено сравнение различных технологий VPN и даются рекомендации по выбору подходящего решения на основе используемых приложений,

требований безопасности, расширяемости, финансовых возможностей и иных факторов.

Таблица 4.1.

Сравнение различных решений для VPN-сетей

Комментарий		Виртуальные каналы 2-го уровня	Туннели на 3-м уровн	VPN-сети MPLS
Уровень сложности при установке и управлении	Для быстрого создания новых служб, повышения уровня безопасности, качества обслуживания и поддержки соглашений об уровне обслуживания необходимо иметь усовершенствованные системы мониторинга и анализа проходящих потоков данных	Низкий	Средний	Высокий
Уровень безопасности	Должны предлагаться различные уровни безопасности,включая использование туннелей, шифрование, разделение потоков (traffic separation), аутентификация и управление доступом	Высокий	Высокий	Высокий
Расширяемость структуры	Должна позволять расширение служб VPN малых и средних предприятий до сетей крупных промышленных пользователей	Средняя	Средняя	Высокая
Качество обслуживания	Должна быть возможность назначать приоритеты критически важным или чувствительным к задержке приложениям и возможность управления в случае возникновения заторов путем изменения ширины полосы пропускания	Высокое	Для реализации QoS необходимо использовать другие технологии	Высокое
Стоимость установки	Прямые и косвенные расхо ды на установку VPN	Высокие	Средние	Низкие

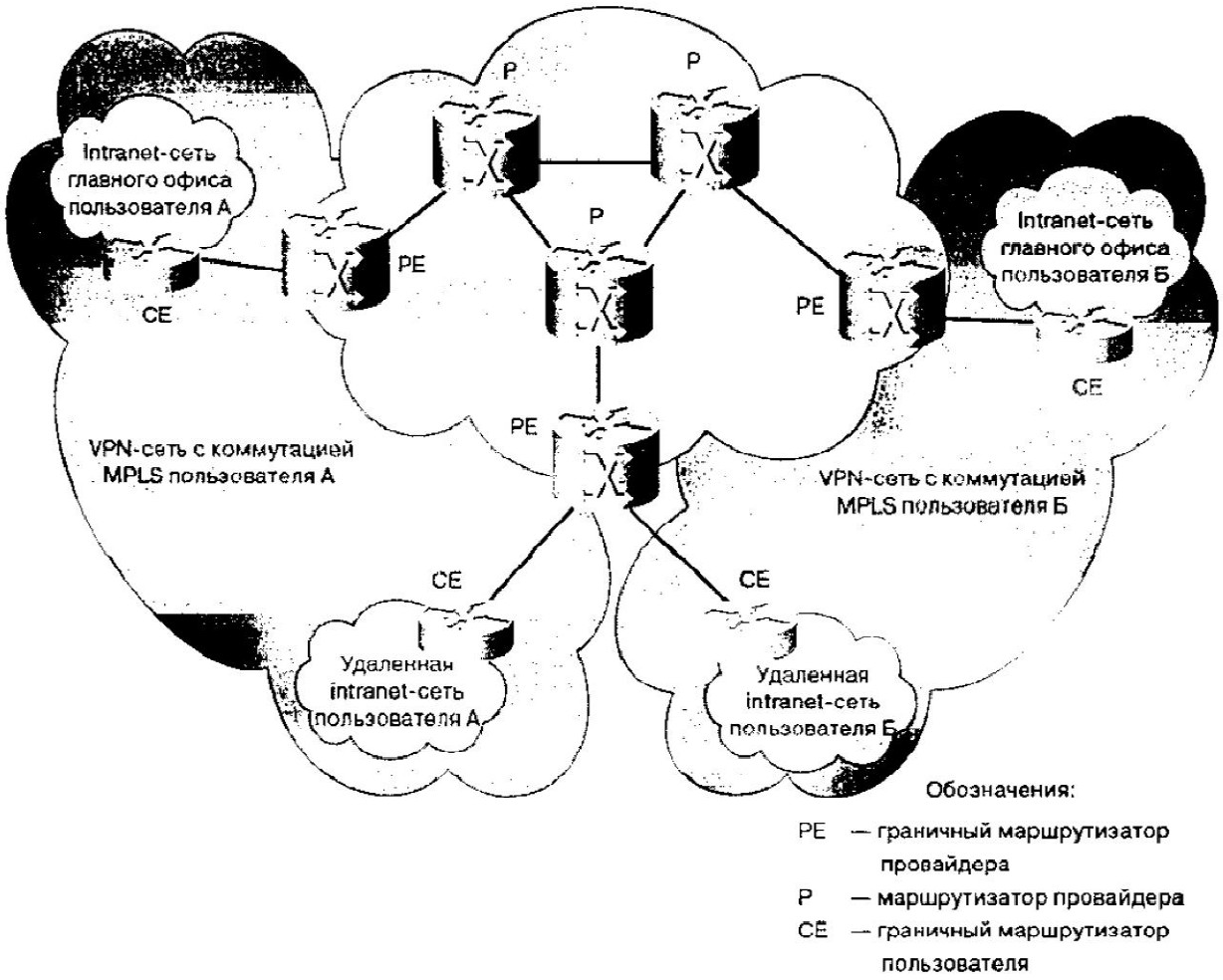


Рисунок 4.10 - Виртуальная частная сеть MPLS

Преимущества VPN-сетей MPLS рассмотрим в таких аспектах:
- расширяемость; безопасность;
- простота создания сетей VPN;
- гибкость адресации;
- соответствие стандартам;
- гибкость структуры;
- сквозные службы задания приоритетов;-
- консолидация (объединение разных типов данных);
- перераспределение потоков;
- централизованное обслуживание;
- поддержка интегрированных классов обслуживания;
- модернизация и модификация сети;
- централизованное управление и инициализация путем использования Cisco-протокола управления службой (Cisco Service Management — CSM).

Розширюваність

Коммутация MPLS была разработана, в частности, для эффективного решения проблем, связанных с расширением сетей. Ее использование позволяет создавать в одной и той же сети десятки тысяч VPN-структур. Структуры VPN на базе технологи

MPLS используют паритетную модель и структуру 3-го уровня без установления соединения для создания VPN-сетей с большой степенью расширяемости. Паритетная модель требует, чтобы узел пользователя имел одноранговую связь только с одним граничным маршрутизатором провайдера (Provider Edge router — PE-router), а не со всеми маршрутизаторами CPE или граничными маршрутизаторами пользователя (Customer Edge router — CE-router), которые принадлежат к VPN-сети. Структура без установления соединений позволяет создавать VPN-сети на 3-м уровне, устраняя необходимость в туннелях или виртуальных каналах (VC).

Безпека

VPN-сети технологии MPLS обеспечивают такой же уровень безопасности, как и VPN-структуры с установлением (Frame Relay или ATM). Пакеты одной VPN-сети не могут случайным образом попасть в другую сеть VPN. Безопасность обеспечивается на границе инфраструктуры провайдера, где пакеты, полученные от пользователя, отправляются в нужную VPN-сеть. В магистрали данные отдельных VPN-сетей перемещаются отдельно. Спуфинг (попытка получить доступ к PE-маршрутизатору (имитация соединения, например, за счет подстановки адреса злоумышленника в пакеты)) практически невозможен, поскольку IP-пакеты пользователей должны быть получены на конкретном интерфейсе или подынтерфейсе, где они однозначно идентифицируются по VPN-меткам.

Простота побудови мережі VPN

При создании VPN-сетей не требуется специальных таблиц преобразований для соединений "точка-точка" или дополнительных топологий. Для создания закрытых групп пользователей к внутренним и внешним сетям (т.е. intranet и extranet) могут быть добавлены новые узлы. При таком управлении VPN-сетями узел может находиться в нескольких VPN-сетях, что предоставляет максимальную гибкость при построении инфраструктуры. Функции MPLS выполняются в сети провайдера, а в конфигурировании оборудования пользователя либо вообще нет необходимости, либо требуется лишь незначительное. Среда MPLS прозрачна для маршрутизаторов CPE, а CPE-устройствам пользователя установка службы MPLS не требуется.

Гнучка адресація

Для того чтобы сделать службу VPN более доступной, пользователи провайдера могут создать собственную схему адресации, независимую от схем адресации других пользователей этого провайдера. Многие пользователи используют собственные адресные пространства, в соответствии со спецификацией RFC 1918 (Так называемые адреса частных сетей) и не имеют желания затрачивать время и средства на преобразование открытых IP-адресов для создания соединений внутренней сети. VPN-сети MPLS дают возможность использовать текущее адресное пространство без трансляции сетевых адресов (Network Address Translation — NAT) и адреса — как частные внутренние, так и открытые внешние. Использование службы трансляции NAT становится необходимым только в том случае, когда двум VPN-сетям с пересекающимися адресными пространствами требуется установить связь. Эта служба дает возможность использовать собственные незарегистрированные частные адреса и свободно осуществлять связь через открытую IP-сеть.

Відповідність стандартам

Коммутация MPLS может быть использована всеми разработчиками для обеспечения взаимодействия между сетями, содержащими оборудование различных производителей.

Гнучкість мережевої архітектури

Программное обеспечение Cisco IOS в сочетании с маршрутизаторами и коммутаторами Cisco позволяет провайдерам легко устанавливать межсетевые соединения с другими провайдерами для обеспечения глобального распространения технологии IP на нужные сети.

Наскрізні служби призначення пріоритетів

Механизмы качества обслуживания обеспечивают пользователям необходимое качество коммуникаций на всем протяжении маршрута, а провайдерам позволяют гарантировать выполнение условий соглашений об уровне обслуживания (SLA). Технология MPLS обеспечивает расширяемость QoS и его распространение на многочисленные технологии сквозных соединений.

Об'єднання різноманітних типів інформації (даних)

Объединение в одном потоке (консолидация) обычных цифровых данных, голоса и видео позволяет провайдерам уменьшить капитальные расходы и затраты на поддержание работы сети.

Перерозподіл потоків

Маршрутизация с перераспределением потоков и резервированием ресурсов (Traffic Engineering Routing with Resource Reservation — RRR), наряду с использованием расширений протокола RSVP позволяет провайдерам в максимальной степени использовать сетевые ресурсы и добиться оптимальной работы сети. Маршрутизация RRR позволяет оператору применять явно заданные маршруты и принудительно направлять по ним потоки данных, что заменяет традиционные методы IP-маршрутизации и предоставляет пользователю механизмы защиты и быстрого восстановления работы сети в случае отказа устройств. При этом достигается оптимизация работы недостаточно загруженных каналов и более эффективная маршрутизация.

Централізоване обслуговування

Построение VPN-сетей на 3-м уровне позволяет целевым образом предоставлять требуемые службы группам пользователей данной VPN. VPN-сеть должна не только предоставить провайдерам механизм частного подключения пользователей к intranet-службам, но и обеспечить способ гибкого предоставления дополнительных служб отдельным пользователям. При этом вопросы расширяемости приобретают исключительную важность, поскольку пользователи хотят использовать службы частным образом в своих внутренних и внешних сетях (intranet и extranet). Поскольку среды MPLS рассматриваются как частные внутренние сети, новые IP-службы могут быть использованы для следующих целей:

- для многоадресатной рассылки;
- для обеспечения качества обслуживания;
- для поддержки телефонной связи между сетями VPN;

• для централизованных служб внутри сред VPN;
• для соединения "всех-со-всеми".

Інтегрована підтримка класів обслуговування

Уровень качества обслуживания представляет собой важное требование многих потребителей VPN-сетей технологии IP. Функции QoS позволяют выполнить два фундаментальных требования к сети VPN:

• предсказуемое поведение сети и реализация заданной стратегии;
• поддержка различных уровней обслуживания в VPN-сетях MPLS.

Перед тем как потоки данных будут объединены в соответствии со стратегией, задаваемой клиентами, и направлены в пункты назначения по магистрали провайдера, на границе сети производится их классификация и назначение им меток. В магистрали или на границе сети потоки данных могут дифференцироваться по различным классам на основе вероятности отбрасывания пакетов или величины задержки в каналах.

Модернізація та модифікація мережі

Размещение службы VPN требует ясного плана модификации сети. VPN-сети MPLS уникальны, поскольку их можно построить на базе нескольких сетевых структур, включая IP, ATM, Frame Relay и гибридные сети. Модернизация сети для конечного пользователя упрощается, поскольку на граничном маршрутизаторе пользователя не требуется поддержки служб MPLS, а во внутренней сети пользователя не требуется никаких модификаций.

Централізоване управління та ініціалізація шляхом використання Cisco-протоколу управління службой

Cisco Service Management (CSM) значительно упрощает и ускоряет создание службы, инициализацию, функционирование и учет расходов VPN-службы в сетях без сложного конфигурирования отдельных виртуальных каналов (VC).

Висновки

Термин "виртуальная частная сеть" (Virtual Private Network — VPN) используется для обозначения группы пользователей внутри некоторой сети. Сети VPN на базе протокола IP быстро становится основой объединения голосовых и видеослужб и служб обычных цифровых данных. Технологии IPSec и MPLS представляют собой доминирующую тенденцию обеспечения консолидированных служб.

VPN-сети с установлением соединения могут быть созданы на базе инфрастуктур 2-го и 3-го уровней. Примером таких сетей на 2-м уровне могут служить VPN-сети Frame Relay и ATM. Примерами VPN-сетей с установлением соединения 3-го уровня могут служить среды которые используют туннельный протокол 2-го уровня IPSec (L2TP), протокол пересылки 2-го уровня (Layer 2 Forwarding — L2F) и общую инкапсуляцию при маршрутизации (Generic Routing Encapsulation — GRE). Другим примером VPN-сетей с установлением соединения являются виртуальные сети удаленного доступа VPDN (Access VPDN).

VPN-сети без установления соединения не требуют предварительной установки логического или виртуального канала для создания канала связи между двумя оконечными точками. Такие сети 3-го уровня образуют основу одноранговой модели.

При использовании данной модели обмен информацией происходит между маршрутизаторами CPE и маршрутизаторами провайдера службы. Примерами VPN-сетей без установления соединений могут служить обычные VPN-сети протокола IP и VPN-сети MPLS.

При создании VPN-сетей в качестве наилучших утвердились две технологии: MPLS и IPSec. Выбор провайдером одной из них должен основываться на требованиях пользователей и обслуживаемых сегментах, на дополнительных службах, которые могут быть предложены пользователям, и на приоритетах собственной сети.

МК1
(ПРАКТИЧНЕ ЗАНЯТТЯ 2)
ЗАНЯТТЯ 8
ВИКОНАННЯ КВАЛІФІКАЦІЙНИХ ЗАВДАНЬ ЗГІДНО ФОНДУ КВАЛІФІКАЦІЙНИХ ЗАВДАНЬ ЗА "МОДУЛЬ 1"

ЧАСТИНА 3
МОДУЛЬ 2
ТЕМА 3
АРХІТЕКТУРА QOS В МЕРЕЖАХ НА БАЗІ СТЕКУ ПРОТОКОЛІВ TCP/IP

ЛЕКЦІЯ 7
ЗАНЯТТЯ 9
АРХІТЕКТУРА QOS В МЕРЕЖАХ IP

§1. Архітектура диференційних послуг

§2. Класифікація пакетів

§3. Маркування пакетів на основі IP- пріоритету, DSCP та створення QoS-групи

§4. Управління інтенсивністю трафіку. Політики обмеження інтенсивності трафіку. Політики вирівнювання інтенсивності трафіку

Завдання на СРС

1. Розглянути класифікацію трафіка, запропонованого Cisco

ЛЕКЦІЯ 8
ЗАНЯТТЯ 10
ПОЛІТИКА РОЗПОДІЛУ РЕСУРСІВ

§1. Максимінна схема рівномірного розподілу ресурсів

§2. Алгоритм зваженого рівномірного обслуговування черг

§3. Алгоритм розподіленого зваженого рівномірного обслуговування черг

§4. Модифікований алгоритм зваженого кругового обслуговування черг

§5. Модифікований алгоритм зваженого кругового обслуговування черг з дефіцитом

Завдання на СРС

1. Розглянути інші алгоритми розподілу ресурсів

ЛЕКЦІЯ 9
ЗАНЯТТЯ 11
ПОЛІТИКА ПОПЕРЕДЖЕННЯ ПЕРЕВАНТАЖЕННЯ І ПОЛІТИКА ВІД¬КИДАННЯ ПАКЕТІВ

§1. Алгоритм довільного раннього виявлення перевантаження мережі

§2. Алгоритм зваженого довільного раннього виявлення перевантаження мережі

§3. Механізм явного повідомлення про перевантаження мережі

§4. Механізм вибіркового відкидання пакетів

Завдання на СРС

1. Розглянути інші політики відкидання пакетів

ПРАКТИЧНЕ ЗАНЯТТЯ 3
ЗАНЯТТЯ 12
ОЦІНКА ПРОДУКТИВНОСТІ ФУНКЦІОНУВАННЯ ТРАНСПОРТНИХ ПРОТОКОЛІВ З УРАХУВАННЯМ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ QOS

§1. Формування логічного каналу

§2. Формування моделі для заданого алгоритму обробки черги та відкидання пакетів

§3. Визначення характеристик продуктивності

Завдання на СРС:

1. Провести розрахунок для заданих начальних умов

ЧАСТИНА 4
ТЕМА 4
АРХІТЕКТУРА QOS В МЕРЕЖАХ НА БАЗІ ТЕХНОЛОГІЇ IP/MPLS

ЛЕКЦІЯ 10
ЗАНЯТТЯ 13
АРХІТЕКТУРА QOS В МЕРЕЖАХ IP/MPLS

§1. Перерозподіл потоків в мережах MPLS.

§2. Класи обслуговування IntServ. Протокол RSVP в мережах IP/MPLS. IP-пріоритет

§3. Механізм обслуговування DiffServ

§4. MPLS-реалізація функцій DiffServ

Завдання на СРС

1. Поглиблене вивчення протоколу RSVP для мереж IP/MPLS

ЛЕКЦІЯ 11
ЗАНЯТТЯ 14
ПІДТРИМКА МЕХАНІЗМІВ QOS В ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖАХ MPLS

§1. Модель з використанням ізольованого каналу для засобів забезпечення якості обслуговування в віртуальних приватних мережах MPLS

§2. Розподілена модель QoS в віртуальних приватних мережах MPLS

§3. Пріоритезація пакетів. Експериментальне поле MPLS

Завдання на СРС

1. Поглиблене вивчення структури кадру MPLS

ЛЕКЦІЯ 12
ЗАНЯТТЯ 15
УПРАВЛІННЯ ТРАФІКОМ В МЕРЕЖАХ IP/MPLS

§1. Маршрутизація на основі резервування ресурсів

§2. Створення та встановлення TE-тунелю

§3. Атрибути тунелю

§4. Атрибути ресурсів каналу

Завдання на СРС

1. Вивчення реалізації механізмів управління трафіком

МК2
(ПРАКТИЧНЕ ЗАНЯТТЯ 4)
ЗАНЯТТЯ 16
ВИКОНАННЯ КВАЛІФІКАЦІЙНИХ ЗАВДАНЬ ЗГІДНО ФОНДУ КВАЛІФІКАЦІЙНИХ ЗАВДАНЬ ЗА "МОДУЛЬ 2"

СПИСОК ЛІТЕРАТУРИ

Основні джерела

1. Вегешна, Шринивас. Качество обслуживания в сетях IP. : Пер. с англ. — М. : Издательский дом "Вильямс", 2003. — 368 с.
2. Дуглас 3. Камер. Сети TCP/IP. Принципы, протоколы и структура. Том 1. Четвертое Издание.- М. : Издательский дом "Вильямс", 2003. — 851 с.
3. Снейдер Й. Эффективное программирование TCP/IP. Библиотека программиста. — СПб.: Питер, 2002. — 320 с.
4. Вевек Олвейн. Структура и реализация современной технологии MPLS. : Пер. с англ. — М. : Издательский дом "Вильямс", 2004. — 480 с.
5. Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и ее инженернаые приложения - М.: Наука, 1991. - 384 с.
6. Гнеденко Б.В., Беляев Ю.К., Соловьев А.Д. Математические методы в теории надежности. - М.: Наука, 1965. - 526 с.
7. Стеклов В. К., Беркман Л. Н. Проектування телекомунікаційних мереж.: Підручник - К.: Техніка, 2002. - 792 с.
8. Барковський В.В., Беркман Л.Н., Кривуца В.Г. Математичне моделювання телекомунікаційних систем. Навчальний посібник. ДУІКТ.-к.:-2007, 467с.

Додаткова друковані джерела

9. Барлоу Р., Прошан Ф. Математическая теория надежности. - М.: Советское радио, 1969. - 487 с.
10. Баскер Р., Саати Т. Конечные графы и сети. - М.: Наука, 1974. - 368 с. RFC768 J. Postel, User Datagram Protocol, August 1980 RFC793 J. Postel, Transmission Control Protocol, September 1981 RFC791 J. Postel, Internet Protocol, September 1981.

Інтернет джерела

11. RFC2210 J. Wroclawski, The Use of RSVP with IETF Integrated Services, September 1997.
12. RFC2212 S. Shenker et al., Specification of Guaranteed Quality of Service, September 1997.
13. RFC2330 V. Paxson et al., Framework for IP Performance Metrics, May 1998.