Эффективный механизм передачи данных в опорных IP-сетях

с использованием технологии MPLS

В настоящее время технология MPLS, разработанная концерном Cisco в 2001 г. для магистральных и локальных сетей Ethernet, начинает широко использоваться также и в различного рода беспроводных сетях, включая беспроводные децентрализованные самоорганизующиеся сети (Mobile Ad Hoc Network, MANET).
Целью настоящей публикации является знакомство разработчиков беспроводных систем с этой популярной технологией. Рассмотрены сравнительные характеристики стандартных IP- и MPLS-сетей, полученные экспериментально для различных вариантов конфигурации и режимов работы. Показано, что в сетях MPLS задержка передачи данных, время обработки и загрузка ЦПУ меньше по сравнению с традиционными IP-сетями. Отмечено, что применение технологии MPLS способствует повышению уровня безопасности при построении сетей VPN. Сделан акцент на то, что данные самой метки не подвергаются шифрованию в процессе передачи с использованием технологии MPLS.
В статью добавлены комментарии переводчика, поясняющие некоторые специальные термины, приведенные в оригинале.

Валид Ильтаф (Walid Iltaf)
Walid.Iltaf@fh-kaernten.ac.at

Перевод:
Виктор Алексеев, к. ф.-м. н.

Введение

Переход к технологиям нового поколения 4G/5G обуславливает все возрастающие требования современных пользователей Интернета, связанные с увеличением полосы пропускания (ШПД), безопасностью, стабильностью связи, расширением спектра предоставляемых услуг, качеством обслуживания (Quality Of Service, QoS) и виртуальными персональными сетями (Virtual Private Network, VPN). Ведущие провайдеры NSP (Network Service Provider) стремятся организовать свой сервис так, чтобы на базе одной опорной сети можно было бы предоставлять комплекс различных услуг, таких, например, как ШПД, IP-телефония, интерактивные игры, потоковое видео (IPTV), электронная торговля, вебинары, видеоконференции, электронная медицина и др.

Одним из эффективных средств, которые могут быть использованы с этой целью, является технология MPLS (Multiprotocol Label Switching — мультипротокольная коммутация по меткам). Эта масштабируемая технология первоначально была разработана фирмой Cisco для передачи данных от одного узла сети к другому с помощью меток, без использования традиционных методов адресации. Сегодня мы можем наблюдать, как MPLS проникает в наиболее популярные направления новых поколений сетевых технологий (Next Generation Networks, NGN), такие, например, как оптические сети, высокоскоростные магистральные IP-сети, беспроводные сети 3G/4G.

Современные MPLS-сети могут работать с IP-пакетами, ячейками ATM, фреймами SONET/SDH, а также могут быть использованы и для передачи стандартных кадров Ethernet. Целесообразно отметить, что MPLS не заменяет IP-маршрутизацию, а работает поверх нее [1].

С точки зрения модели OSI (рис. 1), технология MPLS включает в себя комбинацию методов передачи данных на сетевом (Network layer — L3) и канальном (Data Link layer — L2) уровнях. Контроль трафика реализуется с помощью передачи части функций уровня L2 уровню L3. Поэтому в описании технологии MPLS говорят о комбинированном подуровне, объединяющем преимущества L2 и L3, который часто называют уровнем L2.5 [2].

Технология MPLS позволяет достаточно легко создавать виртуальные каналы между узлами сети и инкапсулировать различные протоколы передачи данных.

В сетях MPLS пакетам данных присваиваются так называемые «метки» (Label). Они используются в качестве своеобразного адреса узла, которому предназначен конкретный пакет данных. При этом содержание самого пакета не имеет значения, и данные передаются в соответствии с меткой.

Основное преимущество меток заключается в том, что они коммутируются быстрее, чем маршрутизируются пакеты в стандартных IP-сетях. Под термином «стандартные IP-сети» в данной статье подразумеваются сети, в которых для идентификации устройства, подключенного к локальной сети или Интернету, используется уникальный идентификатор — IP-адрес (Internet Protocol Address). В стандартном варианте Internet IETF (далее Интернет) конечный пользователь определяется по IP-адресу пункта назначения (Destination Internet Protocol address). Каждое устройство в IP-сетях имеет возможность выбирать самостоятельно направление доставки пакета в соответствии с IP-адресом пункта назначения и таблицей маршрутизации.

Технология MPLS дает возможность создания сквозного виртуального канала с любым протоколом передачи данных, независимого от среды передачи. Применяя разные метки, можно создавать несколько разных виртуальных сетей на базе одних и тех же узлов. Кроме того, сети MPLS можно масштабировать.

Следует отметить, что прототипы современных меток MPLS использовались и в более ранних технологиях, таких, например, как FR (Frame Relay) и ATM (Asynchronous Transfer Mode). В технологии FR используются метки с изменяемым размером, а в ATM метки имеют фиксированный объем. Однако сама метка трансформируется в процессе передачи [3]. Аналогичный механизм задействован в MPLS, где метка меняется после каждого транзитного шлюза.

На рис. 2 показан классический формат метки MPLS, определенный регламентом RFC [4].

Четыре поля метки занимают общий объем 32 бита. Первое поле («Метка», Label Value), размером 20 бит, определяет путь коммутации по меткам. Второе поле (Experimental, Exp), занимающее 3 бита, первоначально было зарезервировано для развития технологии. Также это поле можно использовать для указания класса трафика, необходимого для обеспечения уровня QoS. Третье поле (Set field, S), размером 1 бит, определяет иерархию стека меток MPLS. В заголовке последней метки бит S = 1, а во всех остальных бит S = 0. Последнее поле (Time to Live, TTL), занимающее 8 бит, используется для определения количества действующих транзитных маршрутизаторов. Информация этого поля позволяет выбраковывать из пакета закольцованные или поврежденные посылки.

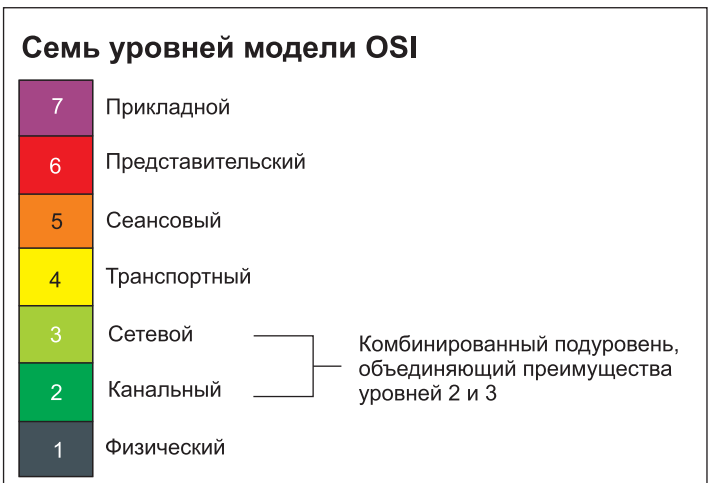
В общем случае MPLS поддерживает форматы кадров технологий PPP, Ethernet, Frame Relay и ATM. В этих кадрах можно размещать пакеты сетевого уровня. Самым распространенным на сетевом уровне является протокол IP. В этом случае метка MPLS встраивается в заголовок IP. Основные характеристики и параметры технологии MPLS описаны в Internet Engineering Task Force (IETF): RFC–2547, 2917, 3031, 3032, 3035, 3270 [5, 6]. Подробное описание структуры метки и методов ее организации можно найти, например, в публикации [7]. Пример простейшей сети MPLS показан на рис. 3 [6].

Базовым устройством сети MPLS является маршрутизатор коммутации меток (Label Switch Router, LSR), который в общем случае определяется, как устройство любого типа, способное создавать, менять и удалять метки MPLS в IP-пакетах [8, 9]. Маршрутизатор LSR также может выступать в роли IP-роутера, коммутатора Frame Relay, а также коммутатора ATM.

В сетях MPLS различают несколько типов маршрутизаторов коммутации меток.

Входной (граничный) маршрутизатор, как следует из названия, — это первое устройство в домене MPLS, предназначенное для связи с другими сетями. В документациях различных производителей граничный маршрутизатор часто обозначают как LER (Label Edge Router) или PER (Provider Edge Router). Именно этот тип роутера генерирует и ставит метку сразу после того, как IP-пакет попадает в сеть MPLS. Кроме того, используется также термин CER (Customer Edge Router). Под этим названием выступает граничный маршрутизатор пользователя, который подключен в сеть провайдера. Термин PER определяет граничный маршрутизатор провайдера, к которому подключаются устройства CE. Чтобы принять пакет, LER, кроме работы с метками MPLS, должен также поддерживать работу с другими протоколами — такими, например, как обычная маршрутизация по IP-адресу.

Выходной (граничный) Egress LSR — это последний маршрутизатор в домене MPLS. Это устройство снимает метку и отправляет «чистый» IP-пакет во внешнюю сеть. Промежуточный (внутренний) Intermediate LSR работает с протоколами MPLS, меняет метки для различных устройств в домене MPLS и коммутирует пакеты по метке. Под LSP (Label Switched Path) понимают совокупность всех роутеров, через которые передается пакет в сетях MPLS.



Уровень	Функции
7. Прикладной	Доступ к сетевым службам, перенос файлов, обмен почтовыми сообщениями и управление сетью.
6. Представительский	Преобразование данных из внутреннего формата компьютера в формат передачи, шифрование данных.
5. Сеансовый	Установка, поддержание и разрыв соединений, распознавание имени пользователя и пароля.
4. Транспортный	Обеспечение целостности доставляемых данных, контроль очередности прохождения компонент сообщения.
3. Сетевой	Определение маршрута, логическая адресация, вставка заголовка в пакет информации, доставка сообщений.
2. Канальный	Физическая адресация, определение правил использования физического уровня узлами сети
1. Физический	Получение пакетов данных от канального уровня и преобразование их в оптические или электрические сигналы, соответствующие «0» и «1» бинарного потока.

Рис. 1. Модель OSI для технологии MPLS

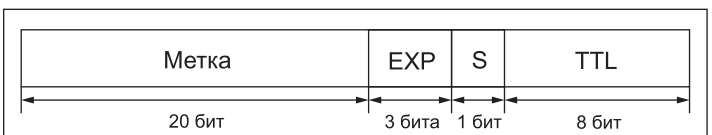


Рис. 2. Классический формат метки MPLS, определенный регламентом RFC

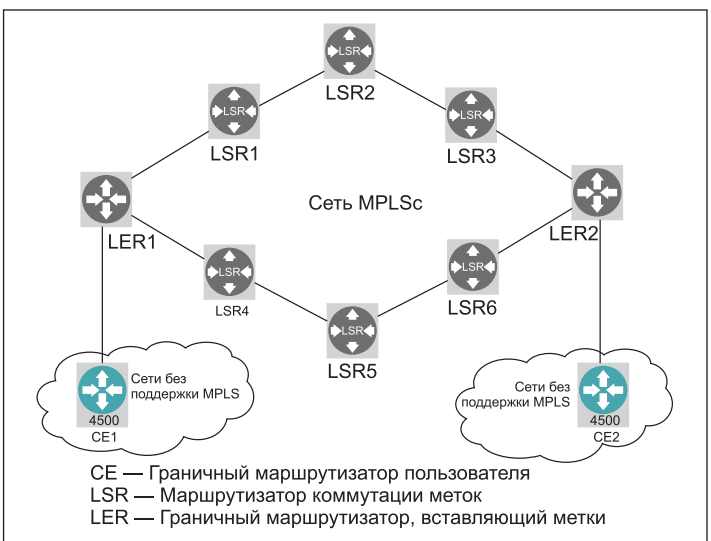


Рис. 3. Пример простой сети MPLS

Сеть Customer's Network (C Network, клиентская сеть) полностью контролируется только пользователем. Протокол MPLS не поддерживается этой сетью.

Термин Provider's Network (P Network), или Backbone Network, определяет опорную (магистральную) сеть интернет-провайдера. В таких сетях может поддерживаться технология MPLS.

Принципы работы технологии MPLS

В зависимости от этапа трансляции данных маршрутизаторы в системе MPLS могут реализовывать различные функции коммутации и управления пакетами.

Как было отмечено выше, MPLS работает только в P Network, в то время как C Network работает как обычная IP-сеть. Технология MPLS начинает действовать с того момента, как IP-пакет попадает в клиентские сети.

Граничные маршрутизаторы выполняют функции назначения и удаления меток. Так, например, на рис. 3 входной граничный маршрутизатор LER1 вставляет метку в пакет, поступивший из внешней сети, между заголовком IP и заголовком уровня 2. Кроме того, LER1 устанавливает класс эквивалентности пересылки пакета (Forwarding Equivalency Class, FEC), определяющий пакеты, пересылаемые одинаково. Маршрут, проходящий через один или более LSR, по которому следуют пакеты одного и того же класса FEC, называется скоммутированным по меткам маршрутом LSP. Этот путь определяется полным набором меток во внутренних маршрутизаторах (LSR1–LSR6), через которые передается пакет в домене MPLS. В технологии MPLS также используется понятие LSP-tunnel, под которым подразумевается последовательность маршрутизаторов, в которой первый маршрутизатор является входным, а последний — выходным пунктом некоего виртуального туннеля.

Внутренние маршрутизаторы LSR пересылают пакет с меткой от одного узла к другому. При этом метка заменяется в зависимости от задачи.

Информация о маршруте пакета передается на все подключенные PER с использованием любого протокола, поддерживаемого системой протокола. Такой процесс часто называют термином PER–CER при описании сетей MPLS VPN. Информация о клиенте сохраняется в исполнительной копии программы в виде виртуальной маршрутизации вместо стандартной таблицы маршрутов. Данная процедура обозначается как Virtual Routing & Forwarding (VRF).

Каждому клиенту присваиваются свои собственные уникальные метки-ярлыки. При этом разграничители маршрутов (Route Distinguishers, RD) позволяют выделить нужный сайт клиента среди всех остальных, доступных данному PER. Обмен информацией с целевым устройством реализуется с помощью протоколов IGP (Interior Gateway Protocols), в качестве которых могут быть использованы OSPF, RIP, EIGRP и др.

В большинстве случаев замена меток осуществляется с помощью LDP (Label Distribution Protocol). Однако необходимо иметь в виду, что в случае использования MPLS/BGP VPN применяется многофункциональный протокол BGP (MP–BGP).

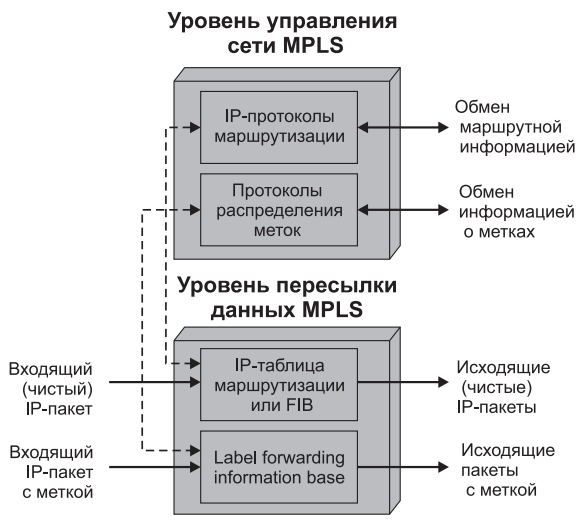


Рис. 4. Уровни управления и пересылки данных технологии MPLS

Для дополнительной протокольной сигнализации и трафик-инжиниринга в сетях MPLS, как правило, применяется протокол резервирования сетевых ресурсов (Resource ReSerVation Protocol, RSVP).

Следует упомянуть режим работы маршрутизаторов MPLS, связанный с созданием таблицы пересылки (Label Information Base, LIB), которая содержит входную метку и дополнительные вложенные записи. Вложенная запись может нести информацию о назначенной выходной метке, номере выходного интерфейса и адресе следующего внутреннего маршрутизатора LSR.

Выходной граничный маршрутизатор LER2 (рис. 3) снимает метку и направляет пакет во внешнюю сеть [10].

Функции контроля, управления и пересылки данных технологии MPLS схематически показаны на рис. 4.

Архитектура MPLS имеет двухуровневую структуру — уровень управления (Control Plane) и уровень пересылки данных (Data Plane). В процессе пересылки пакета по сети MPLS от одного узла к другому метки могут меняться. При этом роутеры на каждом этапе обмениваются соответствующей информацией и выполняют определенные функции.

Сеть MPLS может конфигурироваться с помощью специальных программных средств.

Сразу после появления IP-пакета в сети MPLS ему присваивается метка, которая вставляется между заголовком канального уровня и заголовком IP.

Если сеть имеет несколько транзитных узлов, то при попадании данных в сеть MPLS первый граничный маршрутизатор присваивает IP-пакету свою метку. Затем этот пакет направляется к заданному узлу, и каждый следующий маршрутизатор меняет одну метку на метку другого узла. После выхода из сети MPLS метка снимается и дальше транслируется непосредственно IP-пакет, в том неискаженном виде, каким он был на входе в эту сеть. При этом IP-пакеты могут направляться как в сети пользователя, так и в другие магистральные сети с поддержкой MPLS.

Как видно из рассмотрения рис. 4, последовательность выполнения конкретной операции для определенного маршрутизатора определяется отрабатываемыми на данный момент времени управляющими командами.

Методы доставки пакетов

IP-адресация

Устройство в магистральной IP-сети имеет огромное количество адресных записей, которые сохраняются в IP-таблице маршрутизации. Поиск нужного адреса в таблице представляет собой достаточно сложную комплексную операцию. Роутер должен выполнять поиск IP-адреса по всей таблице для каждого поступающего на него IP-пакета.

Современные маршрутизаторы содержат целый ряд аппаратных и программных средств оптимизации выбора маршрутов. В то же время процедура поиска нужного адреса может отнимать дополнительные ресурсы ЦП, особенно при перестройке таблицы маршрутизации в аварийных ситуациях, при обновлениях маршрутной информации и др.

Метод доставки пакетов в MPLS принципиально отличается от стандартного метода IP, основанного на адресах пунктов назначения. Вместо этого используется метка, внедряемая в заголовок пакета.

Маршрутизатор MPLS проверяет входящую метку и меняет ее на соответствующую исходящую, просматривая таблицу LFIB (Label Forwarding Information Base). Размер таблицы LFIB много меньше по сравнению с IP-таблицей маршрутизации IP-сети.

Поскольку в сети MPLS заранее определяется алгоритм работы с метками, каждое устройство действует в соответствии с общими правилами и не может по своему усмотрению трактовать приоритет и назначение метки.

Технология MPLS в VPN

VPN строятся на базе специальных технологий и протоколов, которые позволяют подключать к частной сети сервисные сети через стандартный Интернет. VPN дают возможность подключения клиентов через

маршрутизатор с использованием частных, а не публичных адресов, как это реализуется в варианте IP-сети.

В варианте клиентского VPN личные данные с частными адресами упаковываются в пакеты с публичными адресами и пересылаются через Интернет. В случае провайдерского VPN клиенту предоставляется несколько точек подключения с каналами связи между ними.

В технологии MPLS VPN используется так называемый виртуальный маршрутизатор (Virtual Routing and Forwarding instance, VRF), который дает возможность организовать на одном физическом маршрутизаторе множество виртуальных. Основные параметры отдельных виртуальных маршрутизаторов, такие, например, как таблицы маршрутизации (FIB), список интерфейсов и другие, являются строго индивидуальными. Следует подчеркнуть, что каждый VRF жестко привязан к конкретному физическому маршрутизатору и не может быть задействован другими маршрутизаторами. Однако, несмотря на то, что между отдельными VRF возможно установление связи, они обособлены также и от самого физического маршрутизатора. Таким образом, реализуется возможность создания множества виртуальных сетей, которые друг с другом не пересекаются.

В технологии MPLS VPN вводятся дополнительные понятия (согласно терминологии Cisco): граничный маршрутизатор клиента (CER), который подключен в сеть провайдера, и граничный маршрутизатор провайдера (PER), к которому подключаются устройства CE. Частный клиентский трафик вводится на одном конце PER и выводится на другом его конце в узле назначения. В технологии MPLS VPN коммутация в пределах магистральной сети осуществляется по одной метке MPLS, а принадлежность к конкретному VPN определяется по другой, дополнительной метке. PER назначает и снимает сервисные метки. В принятой терминологии роутеры PE играют роль Ingress LSR и Egress LSR.

Транзитный маршрутизатор, который не является точкой подключения и просто коммутируется по транспортной метке, обозначается как P (Provider router). На нем нет интерфейсов, привязанных к VPN.

Маршрутная информация для конкретного клиента не сохраняется в общей таблице IP-маршрутизации. Вместо этого в память PER записываются данные маршрутизации для каждого VPN, определяющие его путь и конечный пункт назначения.

В настоящее время существуют две различные технологии — L2VPN и L3VPN, в названиях которых подчеркивается тот факт, что передача пакетов в данной технологии реализуется либо через второй (L2), либо через третий (L3) уровни модели OSI.

Технология MPLS L3VPN

Технология MPLS L3VPN позволяет передавать пакеты с использованием только одного протокола IP через сетевой уровень (Network L3).

В случае MPLS L3VPN частные сети подключаются к сервису с использованием магистральной сети MPLS. Этот тип VPN обладает лучшей производительностью, большей масштабируемостью и гибкостью. Частный трафик вводится в LSP-туннель через первый граничный маршрутизатор и выводится из него через последний граничный. В технологии MPLS L3VPN на уровне L3 реализуются: логическая адресация, определение маршрута, вставка заголовка IP в пакет. Одним из основных преимуществ данной технологии является то, что на магистральной сети трафик групп пользователей изолируется, и при этом гарантируется, что данные каждой из групп не будут смешиваться.

Информация о маршрутизации клиента не сохраняется в глобальной адресной таблице. Вместо этого используется виртуальный маршрутизатор VRF.

Следует отметить, что для данной технологии в настоящее время не существует стандартной, общепринятой процедуры обеспечения безопасности. Кроме того, существенным ограничением технологии L3 VPN является то, что она не может работать с другими протоколами, реализуемыми через канальный уровень: например, нельзя использовать интерфейс E1.

Технология MPLS L2VPN и функция AToM

Технология MPLS L2VPN позволяет работать с протоколами второго канального уровня (Data Link L2), на котором определяются правила использования физического уровня узлами сети. С протоколами канального уровня работают некоторые базовые станции мобильной связи и большинство современных дата-центров. Технология стандартизована документами IETF. Она также поддерживает работу с IP-пакетами, поэтому представляется более гибкой и универсальной по сравнению с MPLS L2VPN.

Важнейшей особенностью технологии MPLS L2VPN является функция AToM (Any Transport over MPLS), которая дает возможность инкапсулировать трафик любого канального уровня в MPLS-пакеты [11].

Функция AToM поддерживает следующие протоколы:

- ATM Adaptation Layer Type-5 (AAL5) over MPLS;
- ATM Cell Relay over MPLS;
- Ethernet over MPLS;
- Frame Relay over MPLS;
- PPP over MPLS;
- High-Level Data Link Control (HDLC) over MPLS.

Технология L2VPN позволяет реализовать сети двух типов конфигурации. В сетях типа P2P (Point-to-Point) используется принцип псевдопровода (PseudoWire, PW), позволяющий использовать сеть провайдера как один виртуальный туннель (провод), соединяющий два PER, по которому информация передается без изменений. В литературе сервис MPLS L2VPN P2P также называют Virtual Private Wire Service.

В варианте сети P2M (Point-to-Multipoint), который может быть реализован только для Ethernet, сеть MPLS работает как обычный Ethernet-коммутатор. В этом методе отдельные части сети заказчиков фактически представляют собой одну ЛВС, по которой пересылаются фреймы Ethernet. Такие сети часто называют Virtual Private LAN Service (VPLS).

Спецификации и приложения MPLS

Оптимизация управления трафиком MPLS

В англоязычной литературе оптимизация управления трафиком определяется очень емким термином Traffic Engineering (TE). В общем случае под термином TE MPLS подразумевают управление трафиком на базе создания оптимальной модели маршрутизации, обеспечивающей заданное качество обслуживания QoS при минимальных затратах сетевых ресурсов и их сбалансированной загрузке. Такой подход позволяет получить лучшие условия трафика, поскольку учитывает не только кратчайший маршрут, но также дополнительные параметры — такие, например, как полоса пропускания, качество обслуживания и др. [3]. Механизмы, заложенные в структуре TE MPLS, позволяют обеспечить разное качество обслуживания (QoS) для трафиков разных типов. Благодаря отмеченным свойствам TE MPLS в последнее время начинает активно применяться в различных сервисах ИТ и беспроводных технологий.

Спецификация Generalized MPLS (GMPLS)

Модернизированная, расширенная версия MPLS, получившая название Generalized MPLS (GMPLS), стандартизована в документации IETF RFC 3495. Спецификация GMPLS поддерживает работу с оптическими сетями с пространственной и временной коммутацией на канальном уровне L2. В технологии GMPLS поддерживаются SONET/SDH, PDH и TDM [11]. Эта спецификация предназначена для использования в системах оптического управления, а также в системах коммутации пакетов физического пути поверх оптического. Благодаря использованию MPLS непосредственно поверх уровня DWDM появилась возможность отказаться от ATM и SDH. Технология GMPLS позволяет заметно улучшить качество эксплуатации, администрирования и обслуживания сетей MPLS.

Транспортный профиль MPLS-TP

Транспортный профиль MPLS (MPLS-TP) представляет собой стандарт, разработанный IETF специально для использования технологии MPLS в транспортных сетях [12]. Эта спецификация позволяет интегрировать различные транспортные сети в единую инфраструктуру, позволяющую сократить расходы обслуживания и повысить эффективность управления.

В настоящее время спецификация MPLS-TP используется для управления распределением ресурсов, а также для диагностики и устранения сбоев на маршрутах LSP в сетях с псевдопроводом. В таких приложениях используются две важные дополнительные опции: метка общего связанного канала (Generic Associated Channel Label, GAL) и специальный заголовок общего связанного канала (Generic Associated Channel Header, G-Ach).

Опция GAL вводит специальную метку для общего связанного канала управления. Специальное поле заголовка G-Ach идентифицирует тип полезной нагрузки, содержащейся в маршрутах коммутации с меткой MPLS (LSP). G-Ach имеет тот же формат, что и заголовок канала управления, связанный с псевдопроводной связью.

Подробная информация о стандарте MPLS-TP приведена в документе RFC 5654. Дополнительную информацию о GAL и G-Ach можно найти в RFC 5586.

Технология MPLS в беспроводных сетях и сетях MANET

Сети нового поколения 4G представляют собой полноценные IP-системы, в которых голосовая связь и широкополосный доступ выступают в роли приложений. Поэтому оптимизация контроля трафика, модернизация систем IP-адресации и VPN являются крайне актуальными задачами, стоящими перед разработчиками систем 4G/5G.

В беспроводных сетях использование технологии MPLS связано, прежде всего, с разработкой новых систем, связывающих базовые станции с функциональными элементами LTE, которые в англоязычной литературе обозначают термином Mobile Backhaul. Системы Mobile Backhaul в сетях 4G играют одну из главных ролей при предоставлении всех необходимых сервисов, а также в обеспечении синхронизации и качества обслуживания QoS, гарантированного соглашением об уровне сервисных услуг (Service-Level Agreement, SLA).

С этой точки зрения технология MPLS позволяет объединять различные виды транспортного трафика в беспроводных сетях. Кроме того, MPLS дает возможность выбора нескольких вариантов подключения сетей поставщиков услуг, обеспечивая наилучший уровень сервиса для каждого конкретного пользователя.

В настоящее время технология MPLS широко используется не только в магистральных и локальных сетях Ethernet, беспроводных сетях, но также находит все большее применение в MANET, состоящих из мобильных устройств, которые могут независимо передвигаться в любых направлениях. В таких сетях, из-за частого самопроизвольного разрыва связи и необходимости ее быстрого восстановления, одной из основных проблем является сохранение маршрутизации и идентификации узлов назначения. С этой точки зрения технология адресации с использованием меток является очень перспективной для MANET. Более подробно эти вопросы рассмотрены в документе RFC 7367.

Проблемы безопасности в сетях MPLS

Концепция безопасности MPLS

Принципы конфиденциальности в сетях MPLS базируются на запрете приема маршрутной информации и пакетов с метками от непроверенных источников. В сетях IP для этой цели могут быть использованы стандартные средства, например IPSec. В MPLS-сетях, в которых работа с метками осуществляется на канальном уровне, применяется протокол туннельного соединения второго уровня (Layer 2 Tunnelling Protocol, L2TP), поддерживающий процедуры аутентификации. Также на этом уровне используется протокол туннельного соединения (Point to Point Tunneling Protocol, PPTP), обеспечивающий, помимо прочего, функции шифрования.

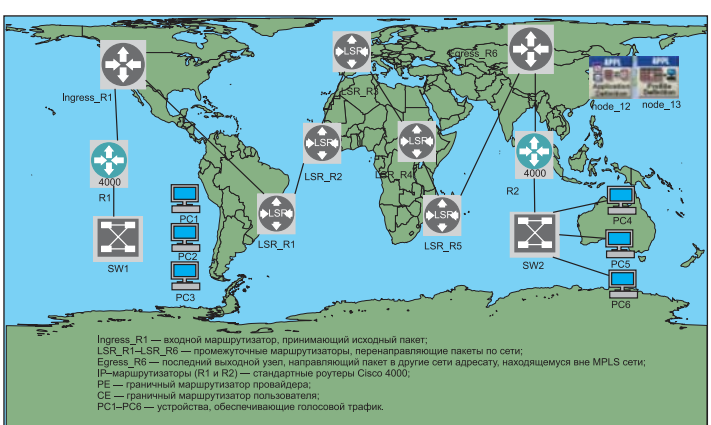


Рис. 5. Структурная схема экспериментальных исследований сравнительных характеристик стандартных IP- и MPLS-сетей

Для большинства приложений MPLS работа с метками реализуется через протокол распределения меток (Label Distribution Protocol, LDP) [13]. Так, как в технологии MPLS не требуется читать заголовки транспортируемых пакетов, LDP-сообщения не подвергаются шифрованию и не нуждаются в аутентификации. Этот момент можно рассматривать как недостаток — с точки зрения уязвимости сети к хакерским атакам.

Уязвимость протокола LDP

В протоколе LDP не предусмотрены специальные механизмы, обеспечивающие защиту от несанкционированного распределения меток.

В принципе, преднамеренные внешние воздействия могут привести к игнорированию адресов определенных узлов и грубому искажению маршрута. Кроме того, возможно несанкционированное создание «вредоносного» LSP, которым можно манипулировать с использованием внешних сетей.

Угрозу, с точки зрения хакерских атак, при работе с LDP представляют два типа передачи данных: по протоколам UDP и TCP. При использовании UDP работа сети может быть нарушена с помощью сообщений типа «Hello», с адресацией ко всем узлам типа «To all LSR» во всех группах многоадресной рассылки данной подсети. Предотвратить такие атаки можно с помощью запрета подобных сообщений, полного запрета приема сообщений от непроверенных источников или введения дополнительной защитной информации.

Протокол TCP при передаче сообщений LDP уязвим на уровне имитированных сегментов TCP в LDPK-сеансах. Для борьбы с подобными методами используется сигнатура TCP Message Digest 5 (MD5). Более подробно эти проблемы описаны в документе RFC 2385.

Уязвимость меток к атакам полного перебора

Существенную опасность для сетей MPLS представляют так называемые атаки полного перебора (Brute Force Attack, BFA). В этом случае внешний сервер методом перебора всех возможных значений адресов пытается установить связь с меткой. После получения ответа от взломанной метки сервер получает возможность управлять ею и перераспределять маршруты по своему усмотрению. Кроме того, искаженная информация может быть занесена в информационную базу меток (Label Information Base, LIB), что равнозначно разрушению всей сети.

В качестве защиты от подобного рода атак для особо критичных узлов сети используются специальные системы шифрования. Однако это значительно увеличивает расход ресурсов сети.

Экспериментальные исследования сети с поддержкой технологии MPLS

Структурная схема эксперимента

Авторами данной статьи были проведены экспериментальные исследования сравнительных характеристик сетей IP и MPLS для различных вариантов конфигурации и режимов работы. На рис. 5 показана структурная схема экспериментальных исследований.

Сеть тестировалась посредством передачи голосового трафика между конечными устройствами сети, показанной на рис. 5.

На схеме роль входного маршрутизатора, принимающего исходный пакет и помещающего в него метку MPLS, выполняет роутер Ingress_R1. Промежуточные маршрутизаторы LSR_R1–LSR_R6 перенаправляют пакеты по сети. Последний выходной узел Egress_R6 направляет исходный пакет к адресату, находящемуся вне MPLS-сети.

В качестве IP-маршрутизаторов (R1 и R2) использовались стандартные роутеры Cisco 4000. Роутеры R1 и R2, по существу, являются граничными маршрутизаторами пользователя (CE) и обеспечивают прямое подключение к маршрутизатору провайдера (PE — Ingress_R1), с которого и начинает функционировать сеть MPLS. Голосовой трафик обеспечивался устройствами PC1–PC6.

Для сравнения сквозной задержки в обеих сетях (End-To-End Delay, E2ED) маршруты MPLS были заменены на стандартные IP-маршрутизаторы Cisco 4000.

Для моделирования сетей было задействовано программное обеспечение OPNET, с помощью графической среды которого тестировались и анализировались экспериментальные параметры прохождения голосового трафика через сеть.

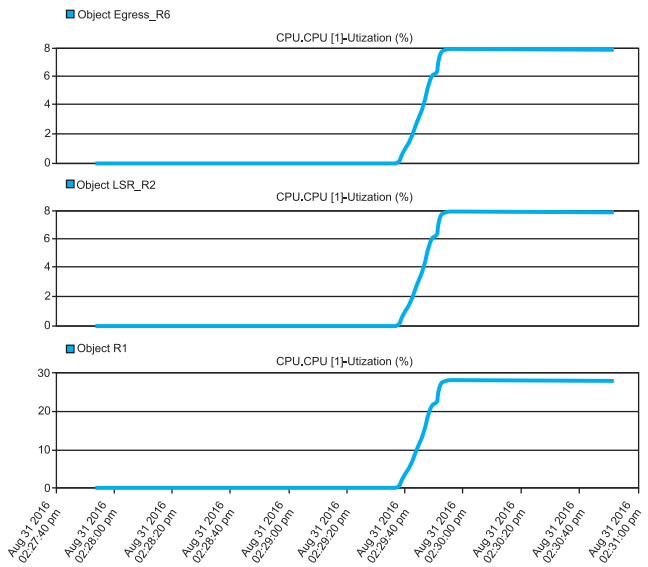


Рис. 6. Результаты измерений эффективности использования ЦПУ различными устройствами сети

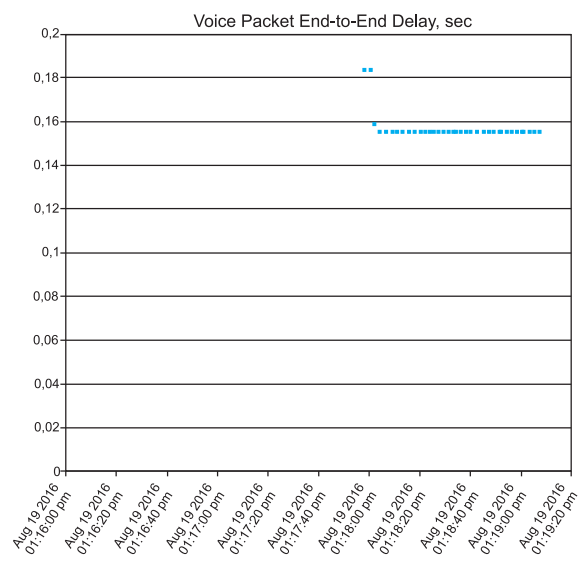


Рис. 7. Результаты измерений сквозной транзитной задержки голосового пакета в сетях с IP-адресацией

Результаты экспериментальных исследований

На рис. 6 приведены результаты определения эффективности использования ЦПУ различными устройствами сети, показанными на рис. 5.

Полученные результаты позволяют говорить о том, что в сети MPLS, показанной на рис. 5, при использовании голосового трафика и программного обеспечения OPNET маршрутизаторы MPLS использовали примерно 8% загрузки ЦПУ. В то же время в стандартной IP-сети с аналогичной конфигурацией, в которой LSR были заменены на роутеры Cisco, IP-маршрутизатор R1 отбирал примерно 30% загрузки. В принципе, такая разница загрузки ЦПУ может быть объяснена разницей методов пересылки пакетов в IP и MPLS. Вполне вероятно, что в другой схеме построения эксперимента и для других видов трафика результаты могут быть другие. Следует отметить, что загрузка ЦПУ в значительной мере зависит от количества устройств в сети и используемого программного обеспечения. Поэтому в реальных магистральных сетях загрузка ЦПУ будет выше из-за большего количества использованных устройств, а соответственно, и большего количества записей в таблицах IP-адресов и LFIB.

На рис. 7 приведены результаты измерений транзитной задержки голосового пакета (E2ED) в стандартной IP-сети. Результаты испытаний показали, что сквозная транзитная задержка в IP-сети составляет почти 156 мс. Для некоторых приложений, таких, например, как Voice over IP (VoIP), такие времена задержки считаются недопустимо большими. Как показано на рис. 8, за счет использования более эффективного механизма пересылки пакетов в технологии MPLS сквозная транзитная задержка уменьшается до 140 мс.

То же самое относится не только к голосовой сети, но и к другим видам трафика, поддерживаемым сетью.

Меньшая задержка приводит к повышению пропускной способности, а также к потерям и закольцовываниям пакетов, что улучшает общую производительность магистральной сети.

Одним из важных параметров, характеризующих работу сети, является вычислительная задержка (PD), определяемая как время обработки пакета маршрутизатором. На рис. 9 показаны результаты определения вычислительной задержки маршрутизаторов в сетях IP и MPLS.

Приведенные на нижней части рисунка данные для роутера R1 в стандартной IP-сети дают значение вычислительной задержки,

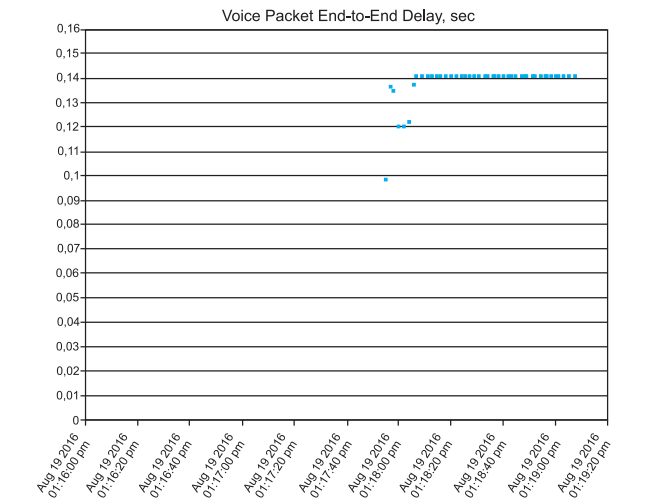


Рис. 8. Результаты измерений сквозной транзитной задержки голосового пакета в MPLS-сетях

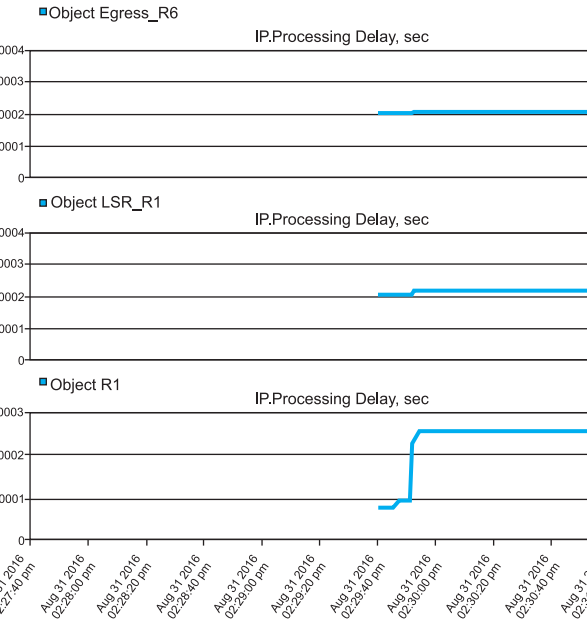


Рис. 9. Результаты определения вычислительной задержки маршрутизаторов в сетях IP и MPLS

равное примерно 250 мкс. В то же время в сети MPLS вычислительная задержка для маршрутизаторов Egress_R6 и LSR_R1 на порядок меньше (около 20 мкс) за счет упрощенного механизма адресации с помощью меток.

Заключение

Стратегия переадресации, используемая в традиционных сетях с IP-адресацией, очень громоздка и требует значительных затрат вычислительных ресурсов. Использование технологии MPLS позволяет значительно уменьшить загрузку ЦПУ и сократить вычислительную задержку маршрутизаторов.

Простая схема адресации, совместимость с другими технологиями и поддержка протокола IPv6 объясняют, почему технология MPLS становится все более привлекательной для использования в различных магистральных сетях. Благодаря ряду эффективных функций эта технология с успехом внедряется в таких приложениях, как MPLS/BGP VPN, VPLS и других мобильных сетях с обратной связью. Также технология MPLS нашла применение в транспортных сетях и MANET.

Из недостатков технологии MPLS следует отметить несовершенство методов безопасности, связанное с отсутствием соответствующих стандартов. Возрастающая агрессивность хакерских атак на интеллектуальные сети вызывает необходимость разработки более надежных методов защиты. Поэтому вопросы совершенствования и стандартизации способов защиты сетей MPLS от хакерских атак представляются крайне актуальными. С этой точки зрения важно всесторонне исследовать возможные варианты уязвимости механизмов перераспределения меток. Кроме того, необходимо обратить внимание на проблему зацикливания пакетов в сетях MPLS. Также требуется дальнейшее совершенствование методики применения протокола IPv6 в сетях MPLS.

В документе RFC 3945 подробно описан модернизированный вариант технологии — GMPLS, который дает возможность использования технологии меток в приложениях TDM. Это направление является перспективным и требует детального изучения.

Особый интерес представляет внедрение MPLS в беспроводные технологии LTE, WiMAX и другие, использующие протоколы IP. ■

Оригинал статьи опубликован в International Journal Of Computers & Technology (ноябрь 2016, Vol. 15, № 13), www.cirworld.com.

Литература

1. Francesco Palmieri. VPN scalability over High Performance Backbones Evaluating MPLS VPN Against Traditional Approaches. Eighth IEEE International Symposium on Computers and Communication (ISCC'03). 2003.
2. Rohit Mishra, Hifzan Ahmad. Comparative Analysis of Conventional IP Network and MPLS Network over VoIP Application // International Journal of Computer Sciences and Information Technologies. 2014. Vol. 5(3).
3. Luc De Ghein. MPLS Fundamentals. Cisco Press, USA, 2006.
4. Rissal Efendi. A Simulation Analysis of Latency and Packet Loss on Virtual Private Network through Multi Virtual Routing and Forwarding // International Journal of Computer Applications. 2012. Vol. 60. № 19.
5. What is MPLS? http://mplsinfo.org/
6. Muhmmad Ahsan Chishti, Ajaz Hussain Mir. Performance Analysis of Traffic Engineering (TE) in IPv6 with IPv4 over Multi Protocol Label Switching (MPLS). // International Journal of Computing and Network Technology. January, 2015.
7. MPLS label format. www.cisco.com/c/dam/en_us/about/ac123/ac147/images/ipj/ipj_4-3/figure3.gif.
8. E. Rosen, A. Viswanathan, R. Callon. Multiprotocol Label Switching Architecture. // RFC 3031. January, 2001.
9. Edmira Xhaferra. A Review Paper: Analysis of OSPF & RIPv2 over MPLS VPN with OPNET Simulation // ImperialJournal of Interdisciplinary Research (IJIR). 2016. Vol. 2.
10. Vivek Alwayn. Advanced MPLS design and Implementation. Cisco Systems. Cisco press, USA, 2001.
11. Tran Cong Hung, Le Quoc Cuong, Tran Tahi Thuy Mui. A Study on Any Transport over MPLS (AToM). ICACT 2010.
12. Understanding MPLS-TP and Its Benefits. www.cisco.com/en/US/technologies/tk436/tk428/white_paper_c11-562013.pdf.
13. Thorsten Fischer. MPLS Security Overview // Information Risk Management. London. December, 2007.