Network Working Group
Request for Comments: 3945
Category: Standards Track

E. Mannie, Ed.
October 2004

GMPLS - обобщённая архитектура многопротокольной коммутации по меткам

Generalized Multi-Protocol Label Switching (GMPLS) Architecture

Статус документа

Авторские права

Аннотация

Сети передачи данных ближайшего будущего будут состоять из таких элементов, как маршрутизаторы, системы DWDM, ADM[1], PXC, OXC и т. п., которые будут использовать обобщённую коммутацию по меткам (GMPLS[2]) для динамического предоставления ресурсов и обеспечения живучести сети с использованием технологий защиты и восстановления.

В этом документе описана архитектура GMPLS. Технология GMPLS является расширением MPLS для использования временного мультиплексирования (например, SONET/SDH, PDH, G.709), разделения по длинам волн (лямбда) и пространственной коммутации (например, входной порт или волокно в выходной порт или волокно). GMPLS фокусируется на уровне управления системами, где разные технологии могут использовать физически отличающиеся методы передачи данных и пересылки. Целью является разработка механизмов сигнализации и маршрутизации для уровня управления.

Оглавление

[1]Add-Drop Multiplexor - мультиплексор с возможностью отвода.
[2]Generalized Multi-Protocol Label Switching.

1. Введение

Описанная здесь архитектура включает основные блоки, требуемые для построения согласованного уровня управления многочисленными системами (уровнями) коммутации. Архитектура не ограничивает способов взаимодействия различных уровней коммутации. Могут применяться разные модели (например, наложение - overlay, добавление - augment или интеграция - integrate). Более того, каждая пара смежных уровней может взаимодействовать разными способами, что приводит к возникновению множества возможных комбинаций и предоставляет свободу выбора производителям и операторам.

Архитектура явно разделяет уровни (плоскости) управления и пересылки. Кроме того, уровень управления явно делится на две части - сигнальная включает протоколы сигнализации, а маршрутная - протоколы маршрутизации.

Этот документ является обобщением архитектуры многопротокольной коммутации по меткам (MPLS) [RFC3031] и в некоторых случаях может незначительно отличаться от своего предшественника, поскольку в настоящем документе рассматриваются не только технологии с коммутацией кадров. Целью настоящего документа не является повторное описание концепций, используемых в архитектуре MPLS. Цель состоит в описании концепций, специфичных для обобщённой коммутации по меткам (GMPLS).

Однако часть рассматриваемых здесь концепций не является частью описанной к настоящему времени архитектуры MPLS, но применима как к GMPLS, так и к MPLS (например, связывание каналов, безадресные соединения, иерархия LSP). Поскольку эти концепции вводятся вместе с GMPLS и очень важны для работы сетей GMPLS, ниже будет приведено их подробное рассмотрение.

Документ начинается с введения в GMPLS. Далее представлены специфичные для GMPLS элементы, которые комбинируются для построения сетей GMPLS. Подробные описания отдельных элементов приводятся в соответствующих документах.

1.1. Используемые сокращения

AS Autonomous System - автономная система.

BGP Border Gateway Protocol - протокол граничного шлюза (протокол внешней маршрутизации).

CR-LDP Constraint-based Routing LDP - LDP с вменённой маршрутизацией.

CSPF Constraint-based Shortest Path First - вменённая маршрутизация по кратчайшему пути.

DWDM Dense Wavelength Division Multiplexing - мультиплексирование с разделением по длине волны и высокой плотностью.

FA Forwarding Adjacency - смежность по пересылке.

GMPLS Generalized Multi-Protocol Label Switching - обобщённая многопротокольная коммутация по меткам.

IGP Interior Gateway Protocol - протокол внутренней маршрутизации.

LDP Label Distribution Protocol - протокол распространения меток.

LMP Link Management Protocol - протокол управления метками.

LSA Link State Advertisement - анонс состояния канала.

LSR Label Switching Router - маршрутизатор с коммутацией по меткам.

LSP Label Switched Path - путь с коммутацией по меткам.

MIB Management Information Base - база данных управления.

MPLS Multi-Protocol Label Switching - многопротокольная коммутация по меткам.

NMS Network Management System - система управления сетью.

OXC Optical Cross-Connect - оптический кросс-коннектор.

PXC Photonic Cross-Connect - фотонный кросс-коннектор.

RSVP ReSource reserVation Protocol - протокол резервирования ресурсов.

SDH Synchronous Digital Hierarchy - синхронная цифровая иерархия.

SONET Synchronous Optical Networks - синхронные оптические сети.

STM(-N) Synchronous Transport Module (-N) - модуль синхронного транспорта уровня N.

STS(-N) Synchronous Transport Signal-Level N (SONET) - сигнал синхронного транспорта уровня N.

TDM Time Division Multiplexing - мультиплексирование с разделением по времени.

TE Traffic Engineering - построение трафика.

1.2. Множество типов иерархий коммутации и пересылки

Обобщённая коммутация по меткам (GMPLS) отличается от традиционной технологии MPLS тем, что она поддерживает множество типов коммутации, добавляя TDM, длину волны (лямбда) и оптические порты (волокна). Поддержка дополнительных типов коммутации требует от GMPLS расширения некоторых базовых функций традиционной архитектуры MPLS, а в некоторых случаях - добавления новых функций. Таким изменениям и дополнениям были подвергнуты базовые свойства LSP - регистрация меток и обмен ими, однонаправленная природа LSP, распространение ошибок, информация, служащая для синхронизации входных и выходных LSR.

Архитектура MPLS [RFC3031] была разработана для поддержки пересылки данных на основе меток. В этой архитектуре предполагалось, что маршрутизаторы LSR имеют уровень пересылки, способный (a) распознавать границу каждого пакета или ячейки и (b) обеспечивать возможность обработки заголовков пакетов (для LSR, распознающих границы пакетов) или ячеек (для LSR, распознающих границы ячеек).

Исходная архитектура MPLS была расширена путём включения LSR, уровни пересылки которых не распознают границ ни пакетов, ни ячеек и, следовательно, не могут пересылать данные на основе информации из заголовков пакетов или ячеек. К таким LSR относятся, в частности, устройства, где решение о коммутации принимается на основе временных интервалов, длин волн или физических портов. Новое множество LSR (точнее, интерфейсов этих LSR) можно разделить на несколько классов:

1. Интерфейсы с коммутацией пакетов (PSC[1]):

   Интерфейсы, способные распознавать границы пакетов и пересылать данные на основе содержимого заголовков каждого пакета. Примерами таких интерфейсов могут служить интерфейсы маршрутизаторов, пересылающих пакеты на основе заголовков IP, и интерфейсы маршрутизаторов, коммутирующие пакеты на основе данных shim-заголовков MPLS.

2. Интерфейсы с коммутацией на уровне 2 (L2SC[2]):

   Интерфейсы, которые распознают границы кадров/ячеек и могут коммутировать данные на основе содержимого заголовков этих кадров/ячеек. Примерами могут служить интерфейсы мостов Ethernet, которые коммутируют пакеты на основе заголовков MAC, и интерфейсы ATM-LSR, пересылающие данные на основе ATM VPI/VCI.

3. Интерфейсы с коммутацией TDM:

   Интерфейсы, которые коммутируют данные на основе временного интервала в циклически повторяющейся структуре. Примерами могут служить интерфейсы кросс-коннекторов SONET/SDH (XC), терминальных мультиплексоров (TM[3]), мультиплексоров ADM. Другим примером могут быть интерфейсы, поддерживающие G.709 (digital wrapper) и интерфейсы PDH.

4. Интерфейсы с коммутацией длин волн (LSC[4]):

   Интерфейсы, коммутирующие данные на основе длины волны, на которой эти данные были получены. Примерами таких интерфейсов являются интерфейсы кросс-коннекторов PXC или OXC, способные работать на уровне отдельных длин волн. Другим примером могут служить интерфейсы PXC, которые работают на уровне групп длин волн (полосы) и оптические интерфейсы G.709.

[1]Packet Switch Capable.
[2]Layer-2 Switch Capable.
[3]Terminal Multiplexer.
[4]Lambda Switch Capable.

5. Интерфейсы с коммутацией оптических волокон (FSC[1]):

   Интерфейсы, которые коммутируют данные на базе их пространственного (физического) расположения. Примером могут служить интерфейсы PXC или OXC, способные работать на уровне одного или группы волокон.

Соединение может быть организовано только между парой однотипных интерфейсов (с возможным участием промежуточных интерфейсов того же типа). В зависимости от используемой на каждом из интерфейсов технологии именование устройств может различаться (например, устройство SDH, оптический путь и т. п.). В контексте GMPLS все такие устройства (каналы) именуются путями с коммутацией по меткам (LSP).

Концепция вложенных LSP (LSP внутри LSP), уже введённая в традиционной технологии MPLS, позволяет создавать иерархию пересылки (т. е., LSP). Иерархия LSP может существовать на одном интерфейсе или между разными интерфейсами.

Например, иерархия может быть организована, если интерфейс может мультиплексировать несколько LSP с одной технологией (скажем, несколько SONET/SDH LSP низкого уровня - VT2/VC-12 в один SONET/SDH LSP - STS-3c/VC-4[2]).

Вложенность может использоваться и между разными типами интерфейсов. На верхнем уровне иерархии располагаются интерфейсы FSC, далее следуют LSC, TDM, L2SC и, наконец, PSC. Таким образом, LSP, начинающийся и заканчивающийся на интерфейсе PSC, может быть вложенным (вместе с другими LSP) в LSP, который начинается и заканчивается на интерфейсах L2SC. Этот LSP, в свою очередь, может быть вложен (вместе с другими LSP) в LSP, что начинается и заканчивается на интерфейсах TDM. Этот путь также может быть вложен (вместе с другими LSP) в LSP, начинающийся и заканчивающийся на интерфейсах LSC. И, наконец, этот путь может быть вместе с другими LSP вложенным в LSP, который начинается и заканчивается на интерфейсе FSC.

1.3. Расширение уровня управления MPLS

Организация LSP, проходящих только через интерфейсы PSC или L2SC, определена для уровней управления MPLS и/или MPLS-TE. GMPLS расширяет эти уровни управления для поддержки каждого из пяти классов интерфейсов (т. е., уровней), определённых в предыдущем параграфе.

Отметим, что уровень управления GMPLS поддерживает модели с перекрытием (overlay), добавлением (augmented) и одноранговые (integrated). На ближайшее будущее технология GMPLS представляется весьма подходящей для независимого управления каждым уровнем. Это элегантное решение будет способствовать развёртыванию других моделей.

Уровень управления GMPLS включает несколько базовых элементов, описанных ниже. Эти элементы базируются на общепринятых протоколах сигнализации и маршрутизации, которые были расширены или изменены для поддержки GMPLS. Для адресации применяется IPv4 и/или IPv6. Для поддержки работы GMPLS требуется только один специализированный протокол, который обеспечивает сигнализацию при управлении каналами [LMP].

GMPLS в действительности базируется на расширении TE для MPLS или MPLS-TE [RFC2702]. Это обусловлено тем, что большинство технологий, которые могут использоваться ниже уровня PSC, требует некоторого построения трафика. Размещение LSP на таких уровнях в общем случае требует принимать во внимание некоторые ограничения (такие, как кадрирование, полоса пропускания, поддержка защиты и т. п.) и обходить унаследованный алгоритм поиска кратчайшего пути SPF[3]. Отметим, однако, что эти требования не обязательны и в некоторых случаях можно применять маршрутизацию SPF.

Чтобы способствовать вменённой[4] SPF-маршрутизации LSP, узлам, создающим LSP, требуется больше информации о каналах в сети, нежели предоставляют стандартные протоколы внутридоменной маршрутизации. Эти атрибуты TE распространяются с использованием транспортных механизмов, доступных IGP (например, лавинной рассылки) и принимаются во внимание алгоритмом маршрутизации LSP. Оптимизация маршрутов LSP может также потребовать некоторых экспериментов по использованию эвристических методов, которые предоставляют входные данные для расчёта пути и процесса организации LSP.

По определению TE-канал представляется в анонсах состояния канала IS-IS/OSPF Link State, а также в базе данных о состоянии каналов некоторых физических ресурсов и их свойств между парой узлов GMPLS. Каналы TE используются уровнем управления GMPLS (маршрутизация и сигнализация) для организации LSP.

Требуются расширения для традиционных протоколов и алгоритмов маршрутизации, обеспечивающие однотипное представление и передачу информации TE, а также поддержку явных (например, задаваемых отправителем) маршрутов, которые нужны для сигнализации. Кроме того, сигнализация должна иметь возможность передачи параметров (таких, как полоса пропускания, тип сигнала, необходимость защиты/восстановления, положение в конкретном мультиплексе и т. п.) требуемого канала (LSP). Большинство таких расширений уже определено для построения трафика PSC и L2SC в MPLS. GMPLS главным образом определяет дополнительные расширения для построения трафика TDM, LSC и FSC. Лишь небольшое число элементов зависит от используемой технологии.

Таким образом, GMPLS расширяет два сигнальных протокола, определённых для сигнализации MPLS-TE - RSVP-TE [RFC3209] и CR-LDP [RFC3212]. Однако GMPLS не задаёт, какой из этих двух протоколов должен использоваться. Производители и операторы могут сами оценить эти варианты с учётом своих интересов.

Поскольку сигнализация GMPLS основана на RSVP-TE и CR-LDP, она диктует выделение и распространение меток по запросу вниз (downstream-on-demand) с инициированным на входе упорядоченным контролем. Обычно используется либеральное удержание меток, но в некоторых случаях может применяться консервативный режим удержания.

Более того, здесь нет ограничений на стратегию выделения меток - оно может управляться запросами/сигнализацией (обычно для устройств с коммутацией каналов), трафиком/данными и даже топологией. Нет ограничений и на выбор

[1] Fiber-Switch Capable.
[2] В иерархии мультиплексирования SONET/SDH определено несколько вложенных уровней сигнализации.
[3] Shortest-Path First.
[4] В оригинале «constrained-based». *Прим. перев.*

маршрута - обычно применяется явная маршрутизация (строгая или нестрогая), но может использоваться и поэтапный выбор маршрута.

GMPLS также расширяет для TE два традиционных протокола внутридоменной маршрутизации на основе состояния каналов - OSPF-TE [OSPF-TE] и IS-IS-TE [ISIS-TE]. Однако при использовании явной (заданной отправителем) маршрутизации применяемые этими протоколами алгоритмы больше не требуется стандартизовать. Расширение для междоменной маршрутизации (например, BGP) требует дополнительного исследования.

Использование технологий типа DWDM предполагает наличие очень большого числа соединений между парой смежных узлов (сотни или тысячи длин при использовании множества волокон). Такое количество соединений изначально не рассматривалось для уровня управления IP или MPLS, хотя это может быть сделано. Требуются некоторые незначительные изменения этих уровней управления, если мы хотим улучшить их использование в контексте GMPLS.

Например, в традиционной маршрутизации IP предполагается организация смежности (в плане маршрутизации) по каждому каналу, соединяющему два соседних узла. Наличие столь большого числа отношений смежности существенно осложняет масштабирование. Каждый узел должен поддерживать определённые отношения с каждым из своих смежных узлов и маршрутная информация должна рассылаться через сеть в лавинном режиме.

Для решения этой проблемы было введено понятие связывания каналов (link bundling). Тем не менее, настройка конфигурации и управление такими каналами (даже если они безадресные) требуют значительных усилий. Протокол управления каналом (LMP) позволяет решить эту проблему.

LMP работает между смежными узлами уровня данных и служит для управления каналами TE. В частности, LMP обеспечивает механизмы поддержки связности каналов управления (IP Control Channel Maintenance), проверки физической связности каналов передачи данных (Link Verification), сопоставления данных о свойствах каналов (Link Property Correlation) и контроля отказов (Fault Localization и Fault Notification). Уникальной особенностью LMP является возможность локализации отказов в прозрачных и «тёмных» (opaque) сетях (т. е., независимо от схемы кодирования и полосы каналов передачи данных).

Протокол LMP определён в контексте GMPLS, но его спецификация не зависит от сигнальной спецификации GMPLS, поскольку этот протокол работает локально между парами соседей по уровню данных.

Следовательно, LMP можно использовать в другом контексте, независимо от сигнальных протоколов GMPLS.

Протоколы маршрутизации и сигнализации MPLS требуют наличия по крайней мере одного двухстороннего канала управления для обмена данными даже в тех случаях, когда два смежных узла соединены односторонними каналами. Может использоваться несколько каналов управления. Для организации, управления и поддержки таких каналов может служить протокол LMP.

GMPLS не задаёт способов реализации каналов управления, однако требует поддержки протокола IP для доставки сигнальной и маршрутной информации через эти каналы. Каналы управления могут размещаться в основной полосе или использовать отдельные соединения. Для передачи IP может применяться несколько решений. Отметим также, что один из типов сообщений LMP (Test) передаётся в основной полосе уровня данных и может доставляться с использованием отличных от IP протоколов - этот тип сообщений нужен для проверки связности на уровне данных.

1.4. Ключевые расширения GMPLS для MPLS-TE

Ниже рассмотрены некоторые важные расширения, добавленные GMPLS в MPLS-TE. Некоторые из них обеспечивают ключевые преимущества GMPLS при управлении уровнями TDM, LSC и FSC.

- В MPLS-TE каналы, через которые проходит LSP, могут включать комбинации соединений с гетерогенным представлением меток (например, каналы между маршрутизаторами, между маршрутизатором и ATM-LSR, между ATM-LSR). GMPLS может работать с такими путями, а также поддерживает соединения, где метки кодируются во временной интервал, длину волны или положение в пространстве.
- В MPLS-TE путь LSP, передающий трафик IP, начинается и заканчивается на маршрутизаторе. GMPLS дополнительно требует, чтобы LSP начинался и заканчивался на интерфейсах похожих типов.
- Типы данных, которые могут передаваться в GMPLS с помощью LSP, расширены и позволяют включать данные SONET/SDH, G.709, 1Gb или 10Gb Ethernet и т. п.
- Использование смежности по пересылке (FA) обеспечивает механизм повышения эффективности расхода полосы в тех случаях, когда та может выделяться только дискретными порциями. Обеспечивается также механизм агрегирования состояния пересылки, позволяющий снизить число требуемых меток.
- GMPLS позволяет восходящим узлам предлагать метки для снижения задержки при организации LSP. Эти предложения могут быть отменены (изменены) нисходящим узлом, но в некоторых случаях такая отмена потребует больших издержек, нежели организация LSP.
- GMPLS расширяет возможности ограничения диапазона меток, которые могут быть выбраны нисходящим узлом. В GMPLS восходящий узел может ограничивать метки для LSP на уровне отдельных интервалов или пути LSP в целом. Такая возможность полезна в фотонных сетях, где преобразование длин волн может быть недоступно.
- Хотя традиционные LSP на базе TE (и даже LDP) являются односторонними, GMPLS поддерживает организацию двухсторонних LSP.
- GMPLS поддерживает завершение LSP на конкретном выходном порту, т. е. выбор порта на приёмной стороне.
- GMPLS с RSVP-TE поддерживает специфические механизмы RSVP для быстрого уведомления об отказах.

Отметим также некоторые ключевые различия между MPLS-TE и GMPLS:

- На интерфейсах TDM, LSC и FSC полоса для LSP может выделяться только дискретными блоками.
- Предполагается многократное снижение числа меток на каналах TDM, LSC или FSC по сравнению с PSC и L2SC, поскольку в первом случае метки являются «физическими», а во втором - логическими.

2. Модель адресации и маршрутизации

GMPLS базируется на моделях адресации и маршрутизации протокола IP. Это предполагает, что для идентификации интерфейсов используются адреса IPv4 и/или IPv6, а также применяются традиционные (распределенные) протоколы маршрутизации IP. В действительности раскрытие топологии и состояния ресурсов на всех каналах в домене маршрутизации осуществляется с использованием этих протоколов маршрутизации.

Поскольку уровни управления и данных в GMPLS разделены, соседи по уровню управления (например, определённые с помощью IGP) могут не быть соседями на уровне данных. Следовательно, нужны механизмы типа LMP для организации TE-каналов с соседними узлами.

IP-адреса используются не только для идентификации интерфейсов на хостах и маршрутизаторах IP, но и для идентификации любых интерфейсов PSC и других уровней. Протоколы маршрутизации IP применяются для нахождения маршрутов передачи дейтаграмм IP с использованием алгоритма SPF, а также при поиске маршрутов для устройств (каналов), не использующих коммутацию пакетов, с помощью алгоритма CSPF.

Однако для повышения уровня масштабируемости этих моделей и удовлетворения специфических требований построения трафика уровней, отличных от PSC, требуются некоторые дополнительные механизмы. Такие механизмы будут рассмотрены в дальнейшем.

Использование существующих протоколов маршрутизации IP позволяет для уровней, отличных от PSC, применять все преимущества, достигнутые за многие годы развития маршрутизации IP (в частности, для внутридоменной маршрутизации по состоянию каналов и междоменной маршрутизации на основе правил).

В модели с перекрытием каждый отдельный уровень, отличный от PSC, может быть виден, как набор автономных систем (AS), соединённых между собой произвольным способом. Подобно традиционной маршрутизации IP, каждая AS управляется одним административным органом. Например, AS может быть сеть SONET/SDH данного оператора. Набор соединённых между собой AS может быть виден как «сеть сетей» SONET/SDH.

Обмен маршрутной информацией между AS может осуществляться с помощью протокола междоменной маршрутизации типа BGP-4. В таких случаях обычно имеется множество проверенных схем маршрутизации на основе правил, которые BGP обеспечивает в контексте, отличном от PSC. Исключения для BGP-TE в контексте уровней, отличных от PSC, требуют дальнейшего изучения.

Каждая AS может быть поделена на разные домены маршрутизации и в каждом из таких доменов может использоваться свой протокол внутридоменной маршрутизации. В свою очередь, каждый домен может быть поделён на области.

Маршрутный домен состоит из поддерживающих GMPLS узлов (т. е., сетевых устройств с поддержкой функций GMPLS). Эти узлы могут быть краевыми (т. е., хосты, входные или выходные LSR) или внутренними LSR. Примером хоста, не являющегося PSC, может служить терминальный мультиплексор (TM) SONET/SDH. Другим примером является интерфейсная плата SONET/SDH в маршрутизаторе IP или коммутаторе ATM.

Отметим, что построение трафика внутри домена требует использования протоколов динамической маршрутизации по состоянию каналов типа OSPF или IS-IS.

GMPLS определяет расширения для таких протоколов. Эти расширения нужны для распространения специфических характеристик (статических и динамических) TDM, LSC и FSC, относящихся к узлам и каналам. В настоящее время делается фокусировка на построение трафика внутри областей, однако исследуются и вопросы построения трафика между областями.

2.1. Адресация уровней PSC и не-PSC

Факт использования адресов IPv4 и/или IPv6 не означает, что эти адреса должны выделяться из публичного адресного пространства IPv4 и/или /or IPv6, используемого для Internet. Если не требуется обмен с другими операторами, могут применяться приватные адреса IP, в противном случае нужны публичные адреса IP. Естественно, при использовании одноранговой модели два уровня могут разделять одно адресное пространство. И, наконец, каналы TE могут быть безадресными (unnumbered), т. е., не иметь адресов IP совсем (в случаях нехватки адресов IP или слишком высоких издержек на поддержку адресации).

Отметим, что использование публичных адресов IPv4 и/или IPv6 для уровней, отличных от PSC, может давать преимущества, если предполагается применение одноранговой модели с уровнем IP.

Если рассмотреть повышение уровня масштабируемости, предлагаемое в следующем параграфе, каждого из адресных пространств IPv4 (32 бита) и IPv6 (128 битов) более, чем достаточно для размещения любого уровня, отличного от =PSC. Резонно предположить, что число устройств, не относящихся к PSC (например, узлы SONET/SDH), будет гораздо меньше числа существующих сегодня хостов и маршрутизаторов IP.

2.2. Повышение уровня масштабируемости GMPLS

Уровни TDM, LSC и FSC вводят новые ограничения на модели адресации и маршрутизации IP, поскольку на этих уровнях пара узлов может соединяться через несколько сотен параллельных физических каналов (например, длин волн). Новое поколение систем DWDM будет поддерживать несколько сот длин волн в одном волокне.

Связывание адреса IP с каждым концом каждого физического канала, представление каждого канала, как отдельной смежности по маршрутизации, а также анонсирование и поддержка состояния каждого физического канала становятся непрактичными. По этой причине GMPLS расширяет модели адресации и маршрутизации MPLS.

Для повышения уровня масштабируемости адресации и маршрутизации могут использоваться два дополнительных механизма - безадресные каналы и связывание каналов. Эти механизмы могут использоваться одновременно. Для применения этих механизмов требуется расширение протоколов сигнализации (RSVP-TE и CR-LDP) и маршрутизации (OSPF-TE и IS-IS-TE).

2.3. Расширения TE для протоколов маршрутизации IP

Традиционно канал TE анонсируется, как дополнение в «обычному» каналу OSPF или IS-IS, т. е., смежность «поднимает» канал. Когда канал поднимается, анонсируются обычные IGP-свойства (прежде всего, метрика SPF) этого канала и свойства TE.

GMPLS вносит три дополнительных требования:

- во-первых, каналы, не относящиеся к PSC, могут, тем не менее иметь свойства TE, однако OSPF-смежность не может быть напрямую «поднята» на таких каналах;
- во-вторых, LSP могут анонсироваться протоколам маршрутизации, как TE-каналы «точка-точка» (т. е., как FA-смежность[1]); таким образом, анонсируемый TE-канал не обязательно связывает двух прямых соседей OSPF;
- в-третьих, множество каналов может анонсироваться, как один канал TE (например, с целью повышения уровня масштабируемости), в результате чего утрачивается взаимно-однозначное соответствие между обычной смежностью и каналами TE.

Таким образом, представление канала TE становится более обобщённым - TE-канал представляет собой логическое соединение, которое имеет свойства TE. Некоторые из этих свойств могут быть настроены на анонсирующем LSR, другие могут быть получены от иных LSR с помощью некого протокола, а третьи - выведены из свойств компонент канала TE.

Важное TE-свойство канала TE связано с учётом пропускной способности этого канала. GMPLS будет определять различные правила учёта для разных уровней, отличных от PSC. Однако базовыми атрибутами полосы пропускания определяемыми в маршрутных расширениях TE и GMPLS, являются такие параметры, как нерезервированная полоса (unreserved bandwidth), максимальная резервируемая полоса (maximum reservable bandwidth) и максимальная полоса LSP.

В динамической среде предполагается частое изменение учётных параметров полосы. Могут быть разработаны гибкая политика переключения обновлений о состоянии каналов на основе пороговых значений полосы и механизм подавления (флуктуаций) каналов.

К связанным с каналом свойствам TE следует относить также характеристики связанные с защитой от захвата и восстановлением. Например, совместно используемая защита может элегантно комбинироваться со связыванием каналов. Защита и восстановление являются базовыми механизмами, которые применимы и для MPLS. Предполагается, что эти механизмы будут разработаны сначала для MPLS, а потом обобщены на GMPLS.

Наличие канала TE между парой LSR не предполагает существования отношений смежности IGP между этими LSR. Канал TE должен также иметь те или иные средства, с помощью которых анонсирующий LSR может узнать о жизнеспособности канала (например, сообщения LMP Hello). Когда LSR знает, что TE-канал активен и может определить TE-свойства канала TE, этот LSR может анонсировать этот канал своим GMPLS-соседям по OSPF или IS-IS, используя объекты TE (TLV). Будем называть интерфейсы, через которые организуются расширенные с помощью GMPLS отношения смежности OSPF или IS-IS, «каналами управления».

3. Безадресные каналы

Безадресными каналами (интерфейсами) называют каналы (интерфейсы), не имеющие адресов IP. Безадресные каналы могут включаться в сигнализацию MPLS TE, а (TE) информация о таких каналах может передаваться в расширения IGP TE (IS-IS-TE и OSPF-TE).

A. Возможность задания безадресных каналов в сигнализации MPLS TE требует расширения RSVP-TE [RFC3477] и CR-LDP [RFC3480]. Сигнализация MPLS-TE не обеспечивает поддержку безадресных каналов, поскольку она не может показать безадресный канал в своих объектах/TLV Explicit Route и Record Route (такого TLV нет для CR-LDP). GMPLS определяет простые расширения для индикации безадресных каналов в эти два объекта /TLV с использованием нового субобъекта/суб-TLV (Unnumbered Interface ID).

   Поскольку безадресные каналы не идентифицируются адресом IP, для целей MPLS TE каждый конец канала должен получить некий другой идентификатор (локальный для LSR, к которому относится канал). LSR на безадресных каналах обмениваются между собой идентификаторами, которые каждый присвоил каналу. Обмен идентификаторами может быть выполнен с помощью конфигурационных параметров, протокола типа LMP ([LMP]), RSVP-TE/CR-LDP (особенно для описанного ниже случая, где канал образует смежность по пересылке) или расширение IS-IS/OSPF ([ISIS-TE-GMPLS], [OSPF-TE-GMPLS]).

   Рассмотрим (безадресный) канал между LSR A и B. LSR A выбирает идентификатор для канала и так же поступает LSR B. С точки зрения A идентификатор, который A выделил для канала, является «локальным идентификатором канала» (или просто локальным идентификатором), а идентификатор, присвоенный этому каналу маршрутизатором B, будет «удаленным идентификатором канала» (удаленным идентификатором). С точки зрения B локальный и удалённый идентификаторы поменяются местами.

   Новый субобъект/суб-TLV Unnumbered Interface ID для объекта/TLV ER содержит значение Router ID маршрутизатора LSR на восходящей стороне безадресного канала и локальный по отношению к восходящему LSR идентификатор канала.

   Новый субобъект Unnumbered Interface ID для объекта RR содержит локальный идентификатор с точки зрения добавившего объект RR маршрутизатора LSR.

[1] Отношения смежности по пересылке рассматриваются в разделе 8. Смежность по пересылке (FA).

B. Возможность передавать (TE) информацию о безадресных каналах в расширения IGP TE требует новых суб-TLV для расширенного IS Reachability TLV, определённого в IS-IS-TE, и TE LSA («тёмный» LSA), определённого в OSPF-TE. Определены два суб-TLV - Link Local Identifier и Link Remote Identifier .

3.1. Безадресная смежность по пересылке

Если LSR, на котором начинается LSP, анонсирует этот LSP как безадресную FA в IS-IS/OSPF или LSR использует эту FA, как безадресную компоненту связки каналов, LSR должен выделить для этой FA идентификатор интерфейса. Если LSP является двухсторонним, другой конец пути делает то же самое и выделяет идентификатор интерфейса для обратной FA.

Сигнализация расширяется для передачи Interface ID смежности FA в новом объекте/TLV LSP Tunnel Interface ID. Этот объект/TLV содержит значение Router ID (маршрутизатора LSR, генерирующего объект) и Interface ID. В сообщении Path/REQUEST это поле называется Forward Interface ID, а в сообщении Resv/MAPPING - Reverse Interface ID.

4. Связывание каналов

Концепция связывания каналов весьма важна для некоторых сетей, использующих уровень управления GMPLS, как определено в документе [BUNDLE]. Типичным примером являются оптические многосвязные (optical meshed) сети, где смежные оптические кросс-коннекторы (LSR) соединяются между собой несколькими сотнями «параллельных» длин волн. Рассмотрим для такой сети применение протоколов маршрутизации по состоянию каналов (типа OSPF или IS-IS) с подходящими расширениями для обнаружения ресурсов и динамического расчёта маршрутов. Каждая длина волны в такой ситуации должна анонсироваться отдельно, если не используется связывание каналов.

Когда пара LSR соединена между собой множеством каналов, можно анонсировать несколько (или все) этих каналов, как единый канал в OSPF и/или IS-IS. Этот процесс называется связыванием каналов или просто связыванием. Получаемый в результате логический канал называется связкой каналов (композитным каналом), а входящие в состав связки физические каналы называются компонентами связки (они идентифицируются индексами интерфейсов).

Получаемой в результате комбинации из трёх идентификаторов - идентификатор канала (связки), идентификатор компоненты, метка - достаточно для однозначной идентификации соответствующих ресурсов, используемых LSP.

Целью связывания каналов является повышение уровня масштабируемости за счёт снижения объёма информации, обрабатываемой OSPF и/или IS-IS. Это снижение обеспечивается за счёт агрегирования/абстрагирования данных. Как и в других приложениях агрегирования/абстрагирования в результате некоторая часть информации теряется. Для ограничения размера потерь требуется ограничить типы данных, которые можно агрегировать/абстрагировать.

4.1. Ограничения на связывание

При связывании каналов возникают некоторые ограничения, которые перечислены здесь. Все компоненты связки должны начинаться и заканчиваться на одной паре маршрутизаторов LSR; все компоненты должны иметь некий набор общих характеристик или свойств, определённых в [OSPF-TE] и [ISIS-TE], а именно:

- тип канала (например, «точка-точка» или множественный доступ);

- метрика TE (административная стоимость);

- набор классов ресурсов на каждом конце канала (например, цвета).

Отметим, что FA может также быть компонентой связки. Фактически, связка может состоять из смеси физических каналов «точка-точка» и смежностей FA, но все они должны иметь общий набор свойств.

4.2. Вопросы маршрутизации для связок

Связка каналов представляет собой просто другой тип канала TE, как определено в документе [GMPLS-ROUTING]. Жизнеспособность связки определяется жизнеспособностью каждой из её компонент. Связка сохраняется, пока работает хотя бы одна из её компонент. Жизнеспособность компоненты может быть определена несколькими способами - сообщения Hello узлов IS-IS или OSPF через компоненту, RSVP Hello (hop local), LMP Hello (link local), а также индикация уровней 1 или 2.

Отметим, что (согласно спецификации RSVP-TE [RFC3209]) механизм RSVP Hello предназначен для использования в тех случаях, когда недоступны уведомления об отказах на канальном уровне, а безадресные каналы не используются или в случаях, когда механизмов канального уровня недостаточно для своевременного обнаружения отказавшего узла.

После того, как рабочее состояние связки определено, она может быть анонсирована, как канал TE с лавинной рассылкой информации TE. Если приветствия IS-IS/OSPF передаются через каналы-компоненты, то лавинная рассылки IS-IS/OSPF может быть ограничена одной из компонент канала.

Отметим, что анонсирование связки TE между парой LSR не подразумевает наличия IGP-смежности между этими LSR по данному каналу. Фактически, в некоторых случаях канал TE между парой LSR может анонсироваться даже при полном отсутствии смежности IGP между LSR (например, когда канал TE представляет собой FA).

Формирование связки включает агрегирование идентичных параметров TE каждой компоненты для создания агрегатных параметров TE. Канал TE, как определено в [GMPLS-ROUTING], имеет множество параметров и для каждого из параметров должны быть определены адекватные правила агрегирования.

Некоторые параметры (например, нерезервированная полоса и максимальная резервируемая полоса) могут получаться путём простого суммирования характеристик компонент. Информация о полосе пропускания является важной частью анонсирования связки и абстрагирование должен быть определено чётко.

Узел GMPLS со связками каналов должен контролировать доступ на уровне отдельных каналов связки.

4.3. Вопросы сигнализации

Обычно для явного маршрута LSP (например, с объектом/TLV явного маршрута) будет выбираться связка каналов, а не отдельные компоненты. Это происходит потому, что лавинная рассылка осуществляется для связки, но не для отдельных компонент.

Выбор компоненты для использования всегда выполняется восходящим узлом. Если LSP является двухсторонним, восходящий узел выбирает канал-компоненту для каждого направления.

Для индикации сделанного выбора нисходящему узлу используется три механизма.

4.3.1. Неявная индикация

Этот механизм требует для каждого канала-компоненты выделенного сигнального канала (например, каналом-компонентой является канал Sonet/SDH с сигнализацией DCC в основной полосе). Восходящий узел говорит получателю, какую из компонент связки использовать, путём передачи сообщения через канал управления выбранной компоненты. Отметим, что сигнальный канал может размещаться в основной полосе компоненты или быть отдельным каналом. В последнем случае связь между сигнальным каналом и соответствующей компонентой связки должна быть явно задана в конфигурации.

4.3.2. Явная индикация через идентификатор интерфейса с адресом

Этот механизм требует для компоненты связки наличия уникального удалённого адреса IP. Восходящий узел показывает выбор компоненты путём включения нового объекта IF_ID RSVP_HOP или IF_ID TLV, содержащего адрес IPv4 или IPv6 в сообщении Path/Label Request (см. [RFC3473] и [RFC3472], соответственно). Для двухсторонних LSP восходящий узел указывает компоненту связки в каждом из направлений.

Этот механизм не требует наличия канала управления для каждой компоненты. Фактически, он не требует наличия канала управления даже у всей связки в целом.

4.3.3. Явная индикация через идентификатор безадресного интерфейса

В этом варианте каждая безадресная компонента связки получает уникальный идентификатор интерфейса (32 бита). Восходящий узел показывает выбор компоненты путём включения нового объекта IF_ID RSVP_HOP или IF_ID TLV в сообщение Path/Label Request (см. [RFC3473] и [RFC3472], соответственно).

Этот объект/TLV передаёт идентификатор интерфейса выбранной компоненты в нисходящем направлении для одностороннего LSP и, в дополнение, - идентификатор интерфейса выбранной компоненты двухстороннего LSP в восходящем направлении.

Два LSR на каждом конце связки обмениваются идентификаторами интерфейсов. Обмен может осуществляться путём задания конфигурационных параметров, с помощью протокола типа LMP (предпочтительно), с помощью RSVP-TE/CR-LDP (особенно для тех случаев, когда канал-компонента представляет собой FA), а также с помощью расширений IS-IS или OSPF.

Этот механизм не требует наличия канала управления для каждой компоненты. Фактически, он не требует наличия канала управления даже у всей связки в целом.

4.4. Безадресные связки каналов

Связка каналов, как таковая, может иметь адрес или быть безадресной, независимо от наличия адресов у компонент связки. Наличие адреса у связки оказывает влияние на анонсирование канала в IS-IS/OSPF и формат LSP ERO, которые будут проходить через связку. Идентификаторы интерфейсов для всех исходящих безадресных каналов (каналов-компонент, FA или связок) данного LSR должны быть уникальными в контексте данного LSR.

4.5. Формирование связок каналов

Основным правилом для связывания компонент является их размещение в связке таким образом, чтобы они как-то коррелировали между собой. Если корреляция компонент возможна на основе множества их свойств, связывание можно применять последовательно на основе этих свойств. Например, каналы можно сначала сгруппировать по первому свойству. В каждой из полученных групп можно провести группировку на основе второго свойства и т. д. Основным принципом связывания является то, что свойства полученной в результате связки должны описываться достаточно кратко. Связывание каналов может выполняться автоматически или путём настройки конфигурации. При автоматическом связывании правила могут применяться последовательно.

Например, первым свойством для связывания компонент может быть корреляция по ISC[1] [GMPLS-ROUTING], вторым - представление (Encoding) [GMPLS-ROUTING], третьим, установленный администратором «вес» (Administrative Weight - стоимость), четвёртым - класс ресурса (Resource Class) и заключительным - метрика типа SRLG[2]. При маршрутизации дополнительного пути для защиты общий принцип заключается в том, что дополнительный путь не маршрутизируется через какие-либо каналы, относящиеся к той же группе SRLG, в которую входит какая-либо из компонент. Таким образом, правило заключается в том, чтобы группировать каналы с одинаковым набором SRLG.

Этот тип последовательного деления на группы и подгруппы может приводить к организации многочисленных связок между парой смежных узлов. На практике, однако, свойства каналов между парой смежных узлов обычно не отличаются значительной неоднородностью. Следовательно, на практике число связок обычно не велико.

[1]Interface Switching Capability - коммутационные возможности интерфейса.
[2]Shared Risk Link Group - группа каналов с общим риском.

5. Связь с UNI

Интерфейс между краевым узлом GMPLS и маршрутизатором GMPLS LSR со стороны сети можно называть интерфейсом UNI[1], тогда как интерфейс между двумя узлами LSR со стороны сети - NNI[2].

GMPLS не задаёт интерфейсов UNI и NNI по отдельности. Краевые узлы подключаются к LSR на сетевой стороне и такие же LSR, в свою очередь, соединяются между собой. Естественно, поведение краевых узлов не совпадает в точности с поведением LSR на стороне сети. Отметим также, что на краевом узле может работать протокол маршрутизации, однако предполагается, что в большинстве случаев этого не будет (см. также параграф 5.2 и параграфы, посвящённые сигнализации при явно заданных маршрутах).

Концептуально делать различие между UNI и NNI имеет смысл, если оба интерфейса используют совершенно разные протоколы или работают по одинаковым протоколам, но с некоторыми различиями. В первом случае разные протоколы обычно определяют последовательно с тем или иным успехом.

Модель GMPLS ставит задачей построение непротиворечивой модели для сегодняшнего дня, рассматривая одновременно оба интерфейса UNI и NNI [GMPLS-OVERLAY]. По этой причине поначалу некоторые специфические вопросы UNI игнорируются. GMPLS будет развиваться для поддержки частностей на уровне UNI другими комитетами по стандартизации (см. дальше).

5.1. Связь с OIF UNI

Этот параграф включён лишь для упоминания о работе OIF, связанной с GMPLS. Текущая спецификация OIF UNI [OIF-UNI] определяет интерфейс между клиентским оборудованием SONET/SDH и сетью SONET/SDH, каждый из которых находится под своим административным управлением. Этот интерфейс предназначен для модели с перекрытием. OIF UNI определяет для UNI дополнительные механизмы, действующие на базе GMPLS.

Например, процедура обнаружения сервиса в OIF является предшественником процедур обнаружения сервиса в UNI. Обнаружение сервиса позволяет клиенту определить статические параметры соединения с сетью, включая сигнальный протокол UNI, тип конкатенации, уровень прозрачности, а также «тип разнообразия» (узел, канал, SRLG), поддерживаемого сетью.

Поскольку существующий интерфейс OIF UNI не включает фотонные сети, G.709 Digital Wrapper и т. п. с точки зрения архитектуры GMPLS относятся к UNI.

5.2. Достижимость через UNI

В этом параграфе рассматривается вопрос выбора краевым узлом явного маршрута. Выбор первого LSR краевым узлом, подключённым к множеству LSR, является частью этой задачи.

Краевой узел (хост или LSR) может более или менее глубоко быть вовлечён в маршрутизацию GMPLS. На UNI могут поддерживаться 4 разных модели маршрутизации — на основе конфигурационных параметров, на основе частичного партнёрства, на основе безучастного прослушивания[3] и на основе полного партнёрства.

- *Маршрутизация на основе конфигурационных параметров*. Эта модель требует ручной или автоматической настройки конфигурации краевого узла с указанием списка соседних LSR, отсортированного по предпочтительности. Для автоматической настройки конфигурации может использоваться, например, протокол DHCP. Обмена маршрутной информацией на уровне UNI не происходит, за возможным исключением передачи упорядоченного списка LSR. Указанный список является единственной маршрутной информацией, используемой краевым узлом. Краевой узел по умолчанию отправляет запрос на LSP предпочтительному маршрутизатору LSR. Этот LSR может возвращать сообщения ICMP redirect для перенаправления некоторых запросов LSP на другой LSR, соединённый с краевым узлом. GMPLS не препятствует использованию этой модели.

- *Частичное партнёрство.* Через UNI осуществляется ограниченный обмен маршрутной информацией (главным образом, о доступности) с использованием неких расширений на сигнальном уровне. Информация о доступности, передаваемая на уровне UNI, может использоваться для инициирования принятия краевым узлом конкретного решения о маршрутизации через сеть. GMPLS в настоящее время не имеет возможности поддерживать эту модель.

- *Безучастное прослушивание*. Краевой узел может прослушивать протоколы маршрутизации и принимать решения на основе полученной информации. Краевой узел получает полные маршрутные данные, включая расширения для построения трафика. LSR следует прозрачно пересылать все маршрутные PDU краевому узлу. Краевой узел в этом случае может рассчитать полностью явный маршрут, принимая во внимание маршрутные данные по всему пути. GMPLS не препятствует использованию этой модели.

- *Полное партнёрство.* В дополнение к прослушиванию маршрутной информации краевой узел принимает участие в её распространении, организуя отношения смежности с соседями и анонсируя LSA. Это полезно только в тех ситуациях, когда обеспечиваются преимущества для краевого узла за счёт анонсирования своей информации по построению трафика. GMPLS не препятствует использованию этой модели.

6. Управление каналом

В контексте GMPLS пара узлов (например, фотонных коммутаторов) может быть соединена десятками волокон, каждое из которых может передавать сотни длин волн при использовании DWDM. Волокна и длины волн из этого множества могут объединяться для маршрутизации в связки каналов. Более того, для организации обмена данными между узлами с целью маршрутизации, сигнализации и управления каналами требуется организация между парой узлов каналов управления.

[1] User to Network Interface - интерфейс между пользователем и сетью.
[2] Network to Network Interface - интерфейс между сетями.
[3] Silent listening.

Управление каналом представляет собой набор процедур, организуемых между смежными узлами, которые обеспечивают локальный сервис типа управления каналом управления, проверки связности каналов, сопоставления свойств каналов и контроля отказов. Протокол LMP[1] [LMP] был определён специально для выполнения этих операций. Разработка LMP была начата в контексте GMPLS, но его основные свойства можно применять и в ином контексте.

В GMPLS для каналов управления между двумя смежными узлами больше не требуется использовать ту же физическую среду, которая служит для организации между этими узлами каналов передачи данных. Более того, каналы управления, что используются для обмена информацией уровня управления GMPLS, существуют независимо от каналов, для управления которыми они служат. Следовательно, протокол LMP разрабатывался для управления каналами данных независимо от свойств этих каналов.

Процедуры управления каналом управления и сопоставления свойств каналов являются обязательными в LMP. Процедуры проверки связности каналов и контроля отказов являются необязательными.

6.1. Канал управления и управление им

Управление каналом управления LMP используется для организации и поддержки управляющих каналов между узлами. Каналы управления существуют независимо от каналов TE и могут использоваться для обмена данными уровня управления MPLS (сигнализация, маршрутизация, управление каналами).

LMP-смежность формируется между узлами, поддерживающими общий набор возможностей LMP. В каждой смежности одновременно может быть активно множество каналов управления. Канал управления может быть явно задан в конфигурации или выбран автоматически, однако LMP в настоящее время предполагает, что каналы управления конфигурируются явно, а возможности управляющих каналов могут согласовываться динамически.

Для целей LMP точная реализация канала управления остаётся неспецифицированной. Канал(ы) управления между парой смежных узлов могут не использовать ту же физическую среду, которая служит для организации каналов передачи данных между этими узлами. Например, канал управления может использовать отдельную длину волны или волокно при соединении Ethernet или туннель IP через отдельную сеть управления.

В следствие то, что канал(ы) управления между парой узлов может быть физически отделен от связанных с ним каналов передачи данных, состояние канала управления может не коррелировать с состояниями каналов данных и наоборот. По этой причине в LMP были разработаны новые механизмы управления каналами в части обеспечения связности и изоляции отказов.

LMP не задаёт механизм доставки сигналов в канале управления, однако предполагается, что сообщения доставляются по каналу управления на базе протокола IP. Более того, в результате использования IP для доставки сообщений протокол канального уровня не рассматривается в LMP. Для каждого направления управляющего канала выделяется 32-битовый (отличный от 0) целочисленный идентификатор CCId[2].

Каждый канал управления индивидуально согласует свои параметры и поддерживает связность с помощью протокола Hello. Последнее требуется в тех случаях, когда недоступны механизмы нижележащих уровней для детектирования отказов на каналах.

Протокол Hello в LMP предназначен для использования в качестве облегчённого механизма поддержки информации о жизнестойкости каналов, который будет быстро реагировать на отказы в управляющем канале, чтобы сообщения IGP Hello не терялись и связанные с этим отношения смежности в плане состояния каналов не удалялись бессмысленно.

Протокол Hello включает две фазы - согласование и сохранение (keep-alive). Первая фаза позволяет согласовать некоторые базовые параметры Hello (например, частоту передачи приветствий). Вторая фаза включает облегченный и быстрый двухсторонний обмен сообщениями Hello.

Если группа каналов управления, соединяющая пару узлов, поддерживает общий набор возможностей LMP, сообщения канала управления LMP (за исключением сообщений Configuration и Hello) могут передаваться через любой из активных каналов управления без координации между локальным и удаленным узлами.

Для LMP важно, чтобы по крайней мере один канал управления был всегда доступен. В случае отказа на канале управления может использоваться другой активный канал управления без какой-либо координации.

6.2. Корреляция свойств канала

Обмен информацией для сопоставления свойств каналов определён, как часть LMP. Этот обмен используется для агрегирования множества каналов передачи данных (например, каналов-компонент) в канал-связку, сопоставления и изменения параметров канала TE. Обмен корреляционными данными может осуществляться в любой момент, пока канал активен и не запущен процесс Verification (см. следующий параграф).

В дополнение к управлению компонентами связки это позволяет менять предельные значения полосы канала, идентификаторы портов и идентификаторы компонент в связке. Этот механизм поддерживается путём обмена сообщениями о состоянии канала.

6.3. Проверка связности

Проверка связности каналов является необязательной процедурой, которая может быть использована для контроля физических соединений в каналах передачи данных, а также для обмена идентификаторами каналов, используемыми в сигнализации GMPLS.

Эту процедуру следует выполнять при организации канала передачи данных и периодически повторять для всех невыделенных (свободных) каналов передачи данных.

Процедура проверки включает передачу сообщений Test в основной полосе канала передачи данных. Это требуется по той причине, что невыделенные каналы передачи данных должны быть «тёмными». Однако существует множество уровней «темноты» (например, проверка избыточных байтов, прерывание передачи данных и т. п.) и, следовательно

[1]Link Management Protocol - протокол управления каналом.
[2]Control Channel Identifier - идентификатор канала управления.

задаётся множество механизмов транспортировки сообщений Test. Отметим, что сообщение Test является единственным сообщением LMP, передаваемым по каналам данных, и дальнейший обмен сообщениями Hello в процессе проверки связности осуществляется по каналу управления. Каналы передачи данных тестируются в направлении передачи, как односторонние. В результате этого соседние узлы LMP могут одновременно обмениваться сообщениями Test для обоих направлений.

Для инициирования процедуры проверки канала узел должен сначала уведомить смежный узел о том, что он будет передавать сообщение Test через конкретный канал передачи данных или компоненту конкретной связки. Узел также должен указать число проверяемых каналов данных, интервал передачи тестовых сообщений, схему кодирования, транспортный механизм и скорость передачи данных для сообщений Test, а также, для случая, когда каналы передачи соответствуют волокнам, длину волны, на которой будут передаваться сообщения Test. Кроме того, передаются локальные и удалённые идентификаторы связки каналов для идентификации компонент связки.

6.4. Контроль отказов

Контроль отказов важен с точки зрения эксплуатационных требований. Обычно такой контроль включает детектирование отказов, их локализацию и передачу уведомлений. Когда отказ произошёл и был обнаружен (детектирование), оператору нужно точно знать место отказа (локализация), а узлу-отправителю может потребоваться уведомление для принятия тех или иных мер (передача уведомления).

Отметим, что локализация отказов может также использоваться для поддержки некоторых (локальных) механизмов защиты/восстановления.

В новых технологиях типа фотонной коммутации в настоящее время не определена локализация отказов и механизмы, с помощью которых информация об отказе должна быть передана «по отдельному каналу» (через уровень управления).

LMP обеспечивает процедуру локализации отказов, которая может быть использована для быстрого обнаружения вышедших из строя каналов путём передачи информации об этом восходящему (по отношению к точке отказа) узлу с помощью процедуры уведомления.

Нисходящий сосед LMP, который детектирует отказ канала, будет передавать сообщение LMP своему восходящему соседу, уведомляя того об отказе канала. Когда восходящий узел получает уведомление об отказе, он может связать этот отказ с соответствующим входным портом для проверки наличия отказа между двумя узлами. После локализации отказа может использоваться сигнальный протокол для инициирования процедур защиты/восстановления.

6.5. LMP для оптических линейных систем DWDM

В полностью оптических средах LMP фокусируется на обмене данными между партнёрами (например,OXC-OXC). OLS[1] известен очень большой объем информации о канале между парой оптических кросс-коннекторов OXC. Предоставление этой информации уровню управления может повысить уровень эффективности использования сети за счёт снижения выполняемой вручную настройки, а также значительно улучшить детектирование и устранение отказов.

LMP-WDM [LMP-WDM] определяет расширения LMP для использования между OXC и OLS. Эти расширения предназначены для выполнения требований к оптическим канальным интерфейсам, описанным в [OLI-REQ].

Детектирование отказов особенно важно для случаев, когда в сети применяются только фотонные коммутаторы (PXC). После организации соединения PXC имеет весьма ограниченные возможности контроля состояния этого соединения. Хотя устройства PXC полностью оптические, обычно на длинных линиях используются системы OLS с электрическим завершением и оптической регенерацией сигналов. Это обеспечивает возможность мониторинга состояния каналов между PXC. В таких случаях в OLS можно использовать расширения LMP-WDM с передачей информации в PXC.

В дополнение к известной OLS информации о канале, которая передаётся через LMP-WDM, некоторая информация от OXC может также передаваться в OLS с помощью LMP-WDM. Эта информация полезна для работы с сигналами тревоги и мониторинга каналов (например, мониторинг трассы). Работа с сигналами тревоги важна, поскольку административное состояние соединения, известное OXC (например, информация, полученная из объекта Admin Status сигнализации GMPLS [RFC3471]), может использоваться для устранения фиктивных сигналов тревоги. Например, OXC может знать, что соединение работает (up), отключено (down), тестируется или будет удалено (deletion-in-progress). OXC может использовать эту информацию для подавления сигналов тревоги от OLS, когда соединение находится в состоянии down, тестируется или удаляется.

Важно отметить, что OXC может быть партнёром одной или нескольких систем OLS, а OLS может быть партнёром одного или нескольких кросс-коннекторов OXC. Хотя существует много схожего в сессиях OXC-OXC LMP и OXC-OLS LMP (особенно в части управления каналом управления и проверки связности), имеются также некоторые различия. Эти различия обусловлены в первую очередь природой каналов OXC-OLS и целями организации сессий OXC-OLS LMP. Каналы OXC-OXC могут использоваться в качестве основы для сигнализации GMPLS и маршрутизации на оптическом уровне. Обмен информацией через сеансы LMP-WDM служит для дополнения сведений о каналах между OXC.

Для того, чтобы информация, передаваемая через сессии OXC-OLS LMP, могла использоваться в сессиях OXC-OXC, эта информация должна координироваться OXC. Однако сеансы OXC-OXC и OXC-OLS в LMP работают независимо и должны управляться раздельно. Критически важным требованием для сессий OXC-OLS LMP является способность OLS сделать канал данных прозрачным, когда не используется процедура проверки канала. Это обусловлено тем, что один и тот же канал данных может проверяться между OXC-OLS и между OXC-OXC. Процедура проверки в LMP используется для координации процедуры Test (и, следовательно, прозрачности/непрозрачности каналов данных). Для поддержки независимости сессий в LMP должна обеспечиваться возможность их активизации в произвольном порядке. В частности, это должно быть возможно для сессий OXC-OXC LMP, которые работают без сессии OXC-OLS LMP и наоборот.

[1]Optical Line System (оптическая линейная система) или терминальный мультиплексор WDM.

7. Обобщённая сигнализация

Сигнализация GMPLS расширяет некоторые базовые функции сигнализации RSVP-TE и CR-LDP, а в некоторых случаях добавляет функциональность. Эти изменения и дополнения влияют на базовые свойства LSP - запрос меток и обмен информацией о метках, однонаправленная природа LSP, распространение информации об ошибках, данные, распространяемые для синхронизации входа и выхода.

Спецификация ядра сигнальных функций GMPLS состоит из трёх частей:

1. описание сигнальных функций [RFC3471];
2. расширения RSVP-TE [RFC3473];
3. расширения CR-LDP [RFC3472].

В дополнение к этому имеется два документа, связанных с конкретными технологиями:

1. расширения GMPLS для управления SONET/SDH [RFC3946];
2. расширения GMPLS для управления G.709 [GMPLS-G709].

Для GMPLS применимы профили MPLS, выраженные в терминах свойств MPLS [RFC3031]:

- нисходящее выделение и распространение меток по запросам;
- инициированное входной стороной согласованное управление;
- либеральный (обычно) или консервативный (иногда) режим удержания меток;
- стратегия выделения меток, управляемая запросами, трафиком/данными или топологией;
- явная (обычно) или поэтапная маршрутизация.

Сигнализация GMPLS определяет новые «строительные блоки» в дополнение к MPLS-TE:

1. новый формат запроса меток;
2. метки для интерфейсов TDM, LSC и FSC, которые обычно называют обобщёнными метками;
3. поддержка коммутации диапазонов длин волн;
4. предложение меток восходящим узлом в целях оптимизации (например, задержки);
5. ограничение меток восходящим узлом в поддержку некоторых оптических требований;
6. организация двухсторонних LSP с разрешением конфликтов;
7. расширения для быстрого уведомления об отказах;
8. защита информации фокусируется в настоящее время на защите каналов с дополнительной индикацией первичного и вторичного LSP;
9. явная маршрутизация с явным управлением метками для тонкого управления;
10. специфические требования к трафику для каждой технологии;
11. обслуживание административного статуса LSP;
12. отделение управляющих каналов.

Эти блоки более детально описаны ниже. Полную их спецификацию можно найти в соответствующих документах.

Отметим, что технология GMPLS является весьма общей и имеет множество опций. Только блоки 1, 2 и 10 являются обязательными и только в конкретном формате, который требуется. Блоки 6 и 9 обычно следует реализовать. Блоки 3, 4, 5, 7, 8, 11 и 12 являются опциональными.

Типичная коммутируемая сеть SONET/SDH будет включать блоки 1, 2 (метки SONET/SDH), 6, 9, 10 и 11. Блоки 7 и 8 являются опциональными, поскольку защита может быть обеспечена с помощью служебных байтов SONET/SDH.

Типичная сеть с коммутацией по длинам волн будет реализовать блоки 1, 2 (базовый формат), 4, 5, 6, 7, 8, 9 и 11. Блок 3 требуется только для частного случая коммутации диапазонов длин волн.

Типичная сеть с коммутацией волокон будет реализовать блоки 1, 2 (базовый формат), 6, 7, 8, 9 и 11.

В типичной сети MPLS-IP перечисленные блоки не будут реализованы, поскольку отсутствие блока 1 будет указывать традиционную сеть MPLS-IP. Отметим, однако, что блоки 1 и 8 могут использоваться для сигнализации MPLS-IP. В этом случае сеть MPLS-IP может получить дополнительную защиту каналов (не поддерживается в CR-LDP, частично поддерживается в RSVP-TE). Блок 2 является обычной меткой MPLS и нового формата не требуется.

GMPLS не задаёт профилей для реализаций RSVP-TE и CR-LDP с целью поддержки GMPLS за исключением того, что напрямую связано с процедурами GMPLS. Выбор необязательных процедур и элементов RSVP-TE и CR-LDP остаётся за разработчиком. Некоторые опциональные элементы MPLS-TE могут быть полезны для уровней TDM, LSC и FSC (например, приоритеты организации и удержания, наследуемые из MPLS-TE).

7.1. Как запрашивать LSP (обзор)

TDM, LSC или FSC LSP организуются путём передачи сообщения PATH/Label Request в нисходящем направлении к адресату. Это сообщение содержит обобщенный запрос метки (Generalized Label Request) с типом LSP (т. е.,

определяется уровнем) и типом данных. В сообщение обычно добавляется объект ERO[1], но он может быть добавлен и/или заполнен первым или используемым по умолчанию LSR.

Требуемая полоса кодируется в объекте RSVP-TE SENDER_TSPEC или CR-LDP Traffic Parameters TLV. В этих параметрах трафика указываются специфические параметры используемой технологии (такие, как тип сигнала, конкатенация и/или прозрачность для SONET/SDH LSP). Для некоторых технологий может просто задаваться требуемая полоса (значение с плавающей точкой).

Локальная защита для канала может быть запрошена с помощью объекта/TLV Protection Information. Сквозная защита LSP рассматривается ниже в параграфе 11. Защита и восстановление LSP.

Если LSP является двухсторонним, в сообщениях Path/Label Request указывается также метка Upstream. Эта метка будет использоваться в восходящем направлении.

Кроме того, в сообщение могут включаться метки Suggested, Label Set и Waveband. Прочие операции определены в MPLS-TE.

Нисходящий узел будет передавать обратно сообщение Resv/Label Mapping, включающее объект/TLV Generalized Label, который может содержать несколько меток Generalized Label. Например, при запросе SONET/SDH с конкатенацией может возвращаться несколько меток.

В случае виртуальной конкатенации SONET/SDH возвращается список меток, каждая из которых идентифицирует сигнал с конкатенацией. Это ограничивает пределы конкатенации одним каналом (компонентой).

В случае непрерывной конкатенации SONET/SDH любого типа возвращается единственная метка. Эта метка является нижним сигналом из непрерывной конкатенации сигналов (порядок определён в [RFC3946]).

В случае «мультипликации[1]» SONET/SDH возвращается явно упорядоченный список всех сигналов, входящих в LSP.

7.2. Обобщенный запрос метки

Generalized Label Request представляет собой новый объект/TLV, который добавляется в сообщение RSVP-TE Path взамен обычного Label Request или в сообщение CR-LDP Request в дополнение к имеющимся TLV. В сообщение может включаться только одна метка, поэтому можно запрашивать по одному LSP на сигнальное сообщение.

Generalized Label Request обеспечивает три основных характеристики (параметра) требуемые для поддержки запрашиваемого LSP - Encoding Type (тип представления), Switching Type (тип коммутации, которая должна применяться) и тип данных LSP, называемый G-PID[2].

LSP Encoding Type показывает тип представления, который будет использоваться для данных, связанных с LSP, т. е., тип технологии (например, SDH, SONET, Ethernet, ANSI PDH и т. п.). Это значение показывает природу LSP, а не природу каналов, через которые проходит LSP. Тип представления указывается поэтапно на каждом узле.

Канал может поддерживать множество форматов представления (поддержка означает способность канала передавать и коммутировать сигналы в этих форматах). Значение Switching Type показывает тип коммутации, которую следует использовать на конкретном канале для данного LSP. Эта информация нужна для каналов, анонсирующих более одного поддерживаемого типа коммутации.

Узлы должны проверять, что тип, указанный значением Switching Type, реально поддерживается на соответствующем входном интерфейсе и при отсутствии такой поддержки должно генерироваться уведомление с индикацией Routing problem/Switching Type (проблемы при маршрутизации - тип коммутации).

Тип данных LSP (G-PID) идентифицирует данные, передаваемые через LSP, т. е., показывает идентификатор клиентского уровня для этого LSP. Для некоторых технологий это значение также показывает отображение, используемое клиентским уровнем (например, отображение байтов синхронизации E1). Значение должно интерпретироваться в соответствии с типом представления LSP и используется узлами на конечных точках (в некоторых случаях на предпоследнем узле) LSP для определения, какому клиентскому уровню адресован запрос.

Прочие параметры, относящиеся к конкретной технологии, не передаются в сообщениях Generalized Label Request, и включаются в связанные с технологией параметры трафика, рассматриваемые ниже. В настоящее время определены два набора параметров трафика - один для SONET/SDH, а второй для G.709.

Отметим, что в будущем предполагается определение специфических параметров трафика для фотонной (полностью оптической) коммутации.

7.3. Параметры трафика SONET/SDH

Параметры GMPLS для трафика SONET/SDH [RFC3946] используют развитые возможности технологий SONET [ANSI-T1.105] и SDH [ITUT-G.707].

Первый параметр задаёт тип элементарного сигнала SONET/SDH для включения в запрашиваемый LSP (например, VC-11, VT6, VC-4, STS-3c и т. п.). К элементарному сигналу могут быть применены некоторые преобразования для создания окончательного сигнала, который реально запрашивается для LSP.

К таким преобразованиям относится непрерывная конкатенация (слияние), виртуальная конкатенация, прозрачность и мультипликация. Каждое из этих преобразований является необязательным. Применяются преобразования строго в приведённом здесь порядке:

- во-первых, может опционально применяться непрерывная конкатенация для Elementary Signal;
- во-вторых, может опционально применяться виртуальная конкатенация непосредственно к элементарному сигналу или к результату непрерывной конкатенации;

[1]Explicit Route Object - объект явно заданного маршрута.
[1]Совместная маршрутизация устройств без конкатенации, но с включением всех устройств в один LSP.
[2]Generalized PID - обобщенный PID.

- в-третьих, может опционально применяться прозрачность, когда запрашивается сигнал, а не контейнер; определены несколько пакетов прозрачности;
- в-четвёртых, может опционально применяться мультипликация непосредственно для элементарного сигнала, результата непрерывной или виртуальной конкатенации, а также комбинации сигнала с той или иной прозрачностью.

Для RSVP-TE параметры трафика SONET/SDH передаются в новом SENDER_TSPEC и FLOWSPEC, которые имеют одинаковый формат. Значение Adspec не связывается с SENDER_TSPEC - оно просто опускается или используется принятое по умолчанию значение. Содержимое объекта FLOWSPEC, полученного в сообщении Resv, должно быть идентично содержимому SENDER_TSPEC в соответствующем сообщении Path. Иными словами, получателю обычно не разрешается менять значения параметров трафика. Однако возможен некоторый уровень согласования параметров, как описано в [RFC3946].

Для CR-LDP параметры трафика SONET/SDH просто передаются в новом TLV.

Отметим, что общее рассмотрение SONET/SDH и GMPLS приведено в работе [SONET-SDH-GMPLS-FRM].

7.4. Параметры трафика G.709

Говоря простым языком, сети на основе стандарта [ITUT-G.709] делятся на два основных уровня - оптический (длины волн) и цифровой. Эти два уровня делятся на подуровни и коммутация происходит на двух конкретных подуровнях - оптический уровень OCh (оптический канал) и электрический уровень ODU (блок данных оптического канала). Для обозначения ODU с разной полосой используется нотация ODUk.

Параметры трафика G.709 в GMPLS [GMPLS-G709] используют широкое возможности сетей ITU-T G.709.

Первый параметр задаёт тип элементарного сигнала G.709 для включения в запрашиваемый LSP (например, ODU1, OCh 40 Гбит/с и т. п.). К элементарному сигналу могут быть применены некоторые преобразования для создания окончательного сигнала, который реально запрашивается для LSP.

К таким преобразованиям относится виртуальная конкатенация и мультипликация. Каждое из этих преобразований является необязательным. Применяются преобразования строго в приведённом здесь порядке:

- во-первых, может опционально применяться виртуальная конкатенация для элементарного сигнала;
- во-вторых, может опционально применяться мультипликация непосредственно для элементарного сигнала или для результата виртуальной конкатенации.

Дополнительные параметры трафика мультиплексирования ODUk позволяют указать отображение ODUk (ODUj на ODUk) для запросов LSP с использованием мультиплексов ODUk. G.709 поддерживает мультиплексирование типа ODUj в ODUk (k > j) и ODU1 с ODU2 в ODU3.

Для RSVP-TE параметры трафика G.709 передаются в новом SENDER_TSPEC и FLOWSPEC, которые имеют одинаковый формат. Значение Adspec не связывается с SENDER_TSPEC - оно просто опускается или используется принятое по умолчанию значение. Содержимое объекта FLOWSPEC, полученного в сообщении Resv, должно быть идентично содержимому SENDER_TSPEC в соответствующем сообщении Path. Иными словами, получателю обычно не разрешается менять значения параметров трафика.

Для CR-LDP параметры трафика G.709 просто передаются в новом TLV.

7.5. Представление полосы

Для некоторых технологий, которые (пока) не имеют специфических параметров трафика, просто требуется представление полосы пропускания, передаваемое в базовом формате. Значение полосы передаётся в виде 32-битового числа с плавающей запятой в формате IEEE (единицей измерения является байт/с). Способ передачи значения зависит от протокола. Для LSP, не использующих пакеты, рекомендуется определять набор дискретных значений для идентификации полосы пропускания LSP.

Следует отметить, что описанное представление полосы не применяется в сетях SONET/SDH и G.709, для которых параметры трафика полностью определяют запрашиваемый сигнал SONET/SDH или G.709.

Полоса задаётся в поле Peak Data Rate (пиковая скорость передачи данных) объектов Int-Serv для RSVP-TE в объектах SENDER_TSPEC и FLOWSPEC, а также в полях Peak Data Rate и Committed Data Rate (контрактная скорость передачи данных) CR-LDP Traffic Parameters TLV.

7.6. Обобщённые метки

Обобщённые метки расширяют возможности традиционных меток MPLS, позволяя представлять не только метки, передаваемые в основной полосе с пакетами данных, но и (виртуальные) метки, идентифицирующие временные интервалы, длины волн, положение в пространственном мультиплексе.

Например, обобщённая метка может идентифицировать (a) одно волокно в группе, (b) одну длину волны в волокне, (c) одну длину волны в диапазоне (или волокне), (d) набор временных интервалов для длины волны (или волокна). Такая метка может также служить обычной меткой MPLS, а также меткой Frame Relay или ATM (VCI/VPI). Обобщённая метка может представлять собой просто целое число (например, метка длины волны) или иметь более сложный формат (как метки SONET/SDH или G.709).

SDH и SONET определяют свою структуру мультиплексирования. Эта структура будет использоваться в качестве дерева имён для создания уникальных меток. Такие метки будут уникально идентифицировать точную позицию (временные интервалы) сигнала в мультиплексной структуре. Поскольку структура мультиплексов SONET может рассматриваться, как подмножество структуры SDH, для обеих технологий используется один формат меток. Аналогичные концепции применяются и при построении меток для уровней ODU в G.709.

Поскольку узлы, передающие и принимающие обобщённые метки, знают типы используемых каналов, в обобщённых метках не содержится идентификатора их типа. Предполагается, что узел может определить из контекста, какой тип метки он ждёт.

Обобщённые метки имеют единственный уровень, т. е. не создают иерархической структуры. Если требуются метки нескольких уровней (LSP в LSP), каждый LSP должен организовываться раздельно.

7.7. Переключение диапазона длин волн

Коммутация оптических диапазонов является частным случаем коммутации длин волн. Оптический диапазон представляет собой «непрерывное» множество длин волн, которые совместно могут быть скоммутированы в другой диапазон. Для оптимизации процесса такое поведение может быть желательным для фотонных кросс-коннекторов. Это позволяет снизить дисторсию для отдельных длин волн и может обеспечить более тонкое разделение отдельных длин волн. Для поддержки этого специального случая определена метка Waveband.

Коммутация диапазонов естественным образом вводит другой уровень иерархии меток и по этой причине метки Waveband трактуются так же, как прочие метки верхних уровней. Как и при рассмотрении протоколов MPLS здесь имеется некоторая разница между метками диапазонов и метками длин волн. Исключение состоит в том, что семантически метка Waveband быть разделена на отдельные метки Wavelength, тогда как метка Wavelength может быть разделена лишь на метки, мультиплексируемые статистически или с разделением по времени.

В контексте коммутации диапазонов обобщённые метки служат для индикации диапазона длин волн и включают три поля - идентификатор длины волны (waveband ID), начальная метка (Start Label) и конечная метка (End Label). Начальная и конечная метки являются идентификаторами каналов, показывающие, с точки зрения отправителя, наименьшее и наибольшее значение длины волны диапазона.

7.8. Предложение меток восходящим узлом

GMPLS позволяет опционально предлагать метки восходящему узлу. Это предложение может быть изменено нисходящим узлом, но в некоторых случаях это будет приводить к издержкам, связанным с затратой времени на организацию LSP. Предложенная метка полезна при организации LSP через некоторые типы оптического оборудования, где возможна значительная (по сравнению с электрическим оборудованием) задержка при настройке машины коммутации (switching fabric). Например, при настройке конфигурации может потребоваться перемещение и юстировка микрозеркал, занимающая достаточно продолжительное время. Если конфигурация меток и, следовательно, машины коммутации настраивается в обратном (нормальном) направлении, сообщение Resv/MAPPING может задерживаться на десятки миллисекунд на каждом интервале при организации пригодного для использования пути пересылки. Это может оказаться важным для целей восстановления, где может потребоваться быстрая организация дополнительных LSP при возникновении отказов в сети.

7.9. Ограничение меток восходящим узлом

Восходящий узел может (опционально) ограничивать выбор меток от нисходящего узла неким набором приемлемых меток. Реализация таких ограничений обеспечивается включением списков и/или диапазонов включённых (подходящих) или исключённый (неприемлемых) меток в Label Set. Если ограничений не задано, могут использоваться все метки из диапазона допустимых значений. Существует по крайней мере 4 ситуации, когда ограничение меток полезно в «оптическом» домене.

Случай 1: оконечное оборудование способно принимать и передавать сигналы лишь в малом наборе длин волн/диапазонов.

Случай 2: имеется последовательность интерфейсов, не способных преобразовывать длины волн и требующих сквозного применения одной длины волны для всей цепочки или даже для пути в целом.

Случай 3: желательно ограничить число преобразований длины волны для снижения искажений оптических сигналов.

Случай 4: две стороны канала поддерживают разные наборы длин волн.

Получатель Label Set должен ограничить свой выбор меток в соответствии с Label Set. Присутствие Label Set возможно на множестве интервалов. В этом случае каждый узел генерирует свой исходящий набор Label Set, который может базироваться на входящем наборе Label Set и аппаратных возможностях данного узла. Предполагается, что такая ситуация будет обычной для узлов с неспособными к преобразованию интерфейсами.

7.10. Двухсторонние LSP

GMPLS позволяет организовывать двухсторонние симметричные LSP (не асимметричные LSP). Симметричный двухсторонний LSP имеет одинаковые требования по построению трафика (включая «общую судьбу», требования к защите и восстановлению, LSR и ресурсам) для каждого направления.

Далее в этом параграфе термин «инициатор» будет относиться к узлу, который начал процесс организации LSP, а термин «завершение» будет обозначать целевой (оконечный) узел LSP. Для двухсторонних LSP возможен только один инициатор и одно завершение.

Обычно для организации двухстороннего LSP при использовании RSVP-TE [RFC3209] или CR-LDP [RFC3212] требуется независимая организация пары односторонних путей. Эта модель имеет несколько недостатков.

1. Задержка при организации двухстороннего LSP равна периоду кругового обхода для сигнализации плюс задержка сигнализации при транзите «инициатор-завершение». Это не только увеличивает задержку при организации LSP, но и увеличивает задержку обнаружения неудачи при организации LSP на удвоенное время транзита «инициатор-завершение». Такие задержки весьма существенны для LSP, организуемых в целях восстановления.
2. Объем передаваемой служебной информации удваивается по сравнению с односторонним LSP. Это обусловлено тем, что должны генерироваться раздельные управляющие сообщения (например, Path и Resv) для обоих сегментов двухстороннего LSP.

3. Поскольку ресурсы организуются в раздельных сегментах, выбор маршрута усложняется. Потенциально также возникает дополнительная конкуренция при выделении ресурсов, которая может снижать вероятность успешной организации двухстороннего соединения.

4. Более сложно обеспечить понятный интерфейс для оборудования SONET/SDH, которое может полагаться на двухсторонние поэтапные пути в целях защитной коммутации. Отметим, что существующее оборудование SONET/SDH передаёт управляющую информацию по тому же каналу, где передаются данные.

5. Двухсторонние оптические LSP (или световые пути) представляются естественной потребностью для многих сервис-провайдеров оптических сетей.

С двухсторонними LSP восходящий и нисходящий пути передачи данных (т. е. от инициатора к завершению и от завершения к инициатору) организуются с использованием одного набора сигнальных сообщений. Это снижает задержку при организации до одного периода кругового обхода «инициатор-завершение» плюс время на обработку, а также ограничивает объем служебной информации до объёма, требуемого для организации одностороннего LSP.

Для двухсторонних LSP должны выделяться две метки. Организация двухстороннего LSP инициируется наличием метки Upstream Label в соответствующем сигнальном сообщении.

7.11. Разрешение конфликтов для двухсторонних LSP

При запросах организации пары двухсторонних LSP в противоположных направлениях могут возникать конфликты между метками. Такие конфликты возникают в случаях, когда обе стороны выделяют одни и те же ресурсы (порты) практически одновременно. Сигнализация GMPLS определяет процедуру разрешения таких конфликтов путём предоставления преимущества узлу с большим значением идентификатора (node ID). Для снижения вероятности возникновения конфликтов предложен ряд механизмов.

7.12. Быстрое уведомление об отказах

GMPLS определяет несколько сигнальных расширений, обеспечивающих возможность ускоренного уведомления об отказах и других событиях узлов, ответственных за восстановление при отказах LSP и обработку ошибок.

1. *Приемлемый набор меток Label Set для уведомления об ошибке Label Error*.

   Существуют ситуации в традиционной MPLS и GMPLS, которые приводят к выдаче сообщений об ошибке с индикацией недопустимого значения метки (Unacceptable label value). При возникновении таких ошибок узлу полезно генерировать сообщение об ошибке для индикации неприемлемой метки. Для таких случаев в GMPLS введена возможность передачи такого типа информации с помощью Acceptable Label Set. Набор Acceptable Label Set передаётся в подходящих сообщениях об ошибках соответствующего протокола. Формат Acceptable Label Set идентичен формату Label Set.

2. *Ускоренное уведомление*.

   Расширения RSVP-TE обеспечивают возможность ускоренного уведомления определённых узлов об отказах и других ошибках. Для CR-LDP подобных механизмов в настоящее время не определено. Первое расширение идентифицирует условия, при которых передаются уведомления о событиях. Второе расширение обеспечивает ускоренные уведомления о событиях с помощью сообщений Notify. Эти расширения могут использоваться механизмами быстрого восстановления. Уведомления могут запрашиваться как для восходящего, так и для нисходящего направления.

   Сообщение Notify обеспечивает обобщенный механизм уведомления, который отличается от определённых в настоящее время сообщений об ошибках тем, что уведомления могут быть «нацелены» на узел, отличный от непосредственного соседа в восходящем или нисходящем направлении. Сообщение Notify не является заменой существующим сообщениям об ошибках. Сообщение Notify может передаваться (a) обычным способом, когда не являющиеся целью узлы просто пересылают сообщение Notify целевому узлу, подобно обработке ResvConf в [RFC2205], или (b) инкапсулироваться в новый заголовок IP, где в качестве получателя указан целевой адрес IP.

3. *Быстрое устранение промежуточных состояний*.

4. Специфическая оптимизация RSVP в некоторых случаях позволяет быстрее устранять промежуточные состояния. Это расширение полезно при работе со специфическими механизмами RSVP.

7.13. Защита канала

Защитная информация передаётся в новом опциональном Protection Information Object/TLV. В настоящее время этот объект указывает желаемый тип защиты для каждого канала LSP. Если запрошен конкретный тип (например, 1+1 или 1:N), запрос соединения обрабатывается только при доступности желаемого типа защиты. Отметим, что GMPLS анонсирует возможности защиты каналов в протоколах маршрутизации. Алгоритмы расчёта пути могут учитывать эту информацию при вычислении путей для организации LSP.

Защитная информация показывает также, является данный LSP основным или вторичным (вторичный LSP является резервным для основного). Ресурсы вторичного LSP обычно не используются, пока на первичном LSP не возникает отказов, но они могут использоваться другими LSP, пока на основном LSP не возникает отказа, приводящего к переходу на вторичный LSP. При возникновении такого отказа обслуживание всех LSP, использующих ресурсы вторичного LSP, должно быть прервано.

В настоящее время определены флаги для шести типов защиты, которые могут применяться по отдельности или в комбинации — enhanced (улучшенный), dedicated 1+1 (выделенный 1+1), dedicated 1:1 (выделенный 1:1), shared (разделяемый), unprotected (без защиты), extra traffic (избыточный трафик). Точные определения каждого из этих типов приведены в параграфе 7.1 документа [RFC3471].

7.14. Явная маршрутизация и явное управление метками

За счёт использования явного маршрута пути, взятые для LSP, могут контролироваться более или менее точно. Обычно узел на головной стороне (head-end) LSP находит явный маршрут и строит ERO[1]/ER[2], содержащий этот маршрут. Возможно, что краевой узел не строит никакого явного маршрута и просто передаёт сигнальный запрос используемому по умолчанию соседнему LSR (так будет поступать хост IP/MPLS). Например, явный маршрут может быть добавлен в сигнальное сообщение первым коммутирующим узлом от имени краевого узла. Отметим также, что явный маршрут меняется промежуточными LSR в процессе прохождения к адресату.

Явный маршрут исходно определён в MPLS-TE, как список абстрактных узлов (т. е., групп узлов), через которые проходит явный путь. Каждый абстрактный узел может представляет собой адресный префикс IPv4/IPv6 или номер AS. Это позволяет генератору явного маршрута не иметь полной информации о деталях пути. В простейшем случае абстрактный узел может представлять собой точный адрес IP (32 бита), идентифицирующий конкретный узел (его называют простым абстрактным узлом).

MPLS-TE поддерживает строгие (strict) и нестрогие (loose0 абстрактные узлы. Путь между строим узлом и его предшественником должен включать только сетевые узлы строгого узла и предшествующего ему абстрактного узла. Путь между нестрогим узлом и его предшественником может включать не только сетевые узлы нестрогого узла или предшествующего ему абстрактного узла, но и прочие узлы сети.

Эта трактовка явного маршрута была расширена путём включения номеров интерфейсов в качестве абстрактных узлов для поддержки безадресных интерфейсов, а также дополнительно расширена в GMPLS со включением меток в качестве абстрактных узлов. Включение меток в явный маршрут достаточно важно, поскольку это обеспечивает возможность тонкого контроля за размещением LSP. Очевидно, что это будет наиболее широко применяться для каналов TDM, LSC и FSC.

В частности, явный контроль меток в явном маршруте позволяет завершать LSP на конкретном выходном порту выходного узла. Действительно, субобъект/TLV должен следовать за субобъектом/TLV, содержащим адрес IP или идентификатор интерфейса (для безадресного интерфейса), связанный с каналом, который будет использоваться.

Это может быть полезно в случаях, когда желательно объединить два LSP (т. е., при соединении «хвоста» одного LSP с «головой» второго LSP).

При использовании вместе с алгоритмом оптимизации можно обеспечить детализированный явный маршрут, включая метку (временной интервал) для использования на канале, чтобы минимизировать фрагментацию мультиплекса SONET/SDH на соответствующем интерфейсе.

7.15. Запись маршрута

Для повышения уровня надёжности и управляемости организуемых LSP в RSVP-TE была введена концепция записи маршрута со следующими функциями:

- Во-первых, механизм детектирования петель для обнаружения маршрутных петель L3 или петель, в явном маршруте (этот механизм используется только вместе с объектами явной маршрутизации).
- Во-вторых, механизм записи маршрута, который собирает подробную актуальную поэтапную информацию о пути в процессе организации LSP. Этот механизм обеспечивает полезную информацию для исходного и целевого узла. Любое промежуточное изменение маршрута в случае нестрогого задания явного маршрута может быть отражено в записи пути.
- В-третьих, записанный маршрут может использоваться в качестве входной информации для явного маршрута. Это полезно в тех случаях, когда исходный узел получает записанный маршрут от целевого узла и применяет его в качестве явного маршрута.

В архитектуре GMPLS только вторая и третья функции применимы главным образом для уровней TDM, LSC и FSC.

7.16. Модификация и перемаршрутизация LSP

Модификация и перемаршрутизация LSP уже доступны в MPLS-TE и GMPLS не добавляет в них ничего нового. В рамках концепции make-before-break[3] старый путь используется, пока создаётся новый путь, что позволяет предотвратить удвоенный расход ресурсов. Затем узел, меняющий маршрутизацию, может переключиться на новый путь и закрыть старый. Эта возможность поддерживается в RSVP-TE (с использованием разделяемый явных фильтров) и CR-LDP (с использованием флага индикации действия).

Модификация LSP состоит в изменении некоторых параметров LSP и обычно не меняет маршрута. Для её поддержки используются те же механизмы, которые служат для перемаршрутизации. Однако семантика модификации LSP будет различаться для разных технологий. Например, для понимания воздействия динамического изменения некоторых характеристик устройств SONET/SDH (полоса пропускания, тип защиты, прозрачность, конкатенация) требуются дополнительные исследования.

7.17. Обслуживание административного статуса LSP

GMPLS обеспечивает дополнительную возможность индикации административного статуса LSP с использованием нового объекта/TLV Admin Status. Информация об административном статусе может использоваться двумя способами.

В первом случае объект/TLV Admin Status передаётся в сообщении Path/Label Request или Resv/Label Mapping для индикации административного статуса LSP. В этом варианте информация об административном статусе показывает состояние LSP, которое может принимать значения up (активен) или down (не активен), указывать режим тестирования (testing) или процесс удаления.

[1]Explicit Route Object - объект явного маршрута.
[2]Explicit Route TLV - TLV явного маршрута.
[3]Создать новый путь до разрыва имеющегося пути.

На основе административного статуса узел может принимать локальные решения типа предотвращения генерации сигналов тревоги для неактивного или тестируемого LSP, а также сигналов тревоги, связанных с соединениями, приоритет которых не превышает Non service affecting.

Возможно, что некоторые узлы на пути LSP не будут поддерживать Admin Status. В таких случаях объект будет проходить через узел в неизменном виде и обработка может продолжаться.

В некоторых условиях (в частности, для оптических сетей) полезно устанавливать для LSP статус being deleted (будет удалён) до его перевода в неактивное состояние, чтобы предотвратить генерацию бесполезных сигналов тревоги. Входной LSR перед удалением LSP помещает подходящий объект/TLV Admin Status в сообщение Path/Label Request (с установкой для флага индикации действия значения modify). Транзитные LSR обрабатывают объект/TLV Admin Status и пересылают его. Выходной LSR отвечает сообщением Resv/Label Mapping (с установкой для флага индикации действия значения modify) с объектом Admin Status. При получении такого сообщения и объекта входной узел передаёт сообщение PathTear/Release в нисходящем направлении для удаления LSP и обычной обработки RSVP-TE/CR-LDP.

Во втором случае объект/TLV Admin Status передаётся в сообщении Notification/Label Mapping (с установкой для флага индикации действия значения modify) для запроса у входного узла смены административного статуса LSP. Это позволяет промежуточным и выходным узлам инициировать смену административного статуса пути. В частности, это позволяет промежуточным и выходным LSR запрашивать освобождение LSP по инициативе входного узла.

7.18. Отделение канала управления

В GMPLS канал управления отделен от канала данных. В действительности канал управления может быть полностью изолирован от основной полосы по различным причинам (например, канал данных не может передавать управляющую информацию). Эта проблема возникла ещё в MPLS в контексте связывания каналов.

В традиционной технологии MPLS существует неявная однозначная связь между каналом управления и каналом данных. При наличии такой связи не требуется дополнительной или специальной информации для связывания конкретной транзакции организации LSP с конкретным каналом данных.

С другой стороны необходимо передавать дополнительную информацию в сигнализации для идентификации канала данных, которым будут управлять. GMPLS поддерживает явную идентификацию канала данных с помощью информации, идентифицирующей интерфейс. GMPLS позволяет использовать множество схем идентификации интерфейсов, включая адреса Ipv4/IPv6, номера безадресных интерфейсов, а также безадресные связки интерфейсов.

Выбор интерфейса данных для использования всегда осуществляется отправителем сообщения Path/Label Request и указывается путём включения идентификатора интерфейса канала данных в сообщение с помощью нового субтипа объекта/TLV RSVP_HOP.

Для двухсторонних LSP отправитель выбирает интерфейс данных в каждом направлении. Во всех случаях, кроме связок, восходящий интерфейс определяется нисходящим интерфейсом. Для связок отправитель сообщения Path/Label Request явно указывает интерфейс-компоненту, используемую в каждом направлении. Новый объект/TLV используется в сообщении Resv/Label Mapping для индикации использования нисходящим узлом указанного интерфейса (интерфейсов).

Новый объект/TLV может содержать список вложенных TLV, каждый из которых может адресом IPv4/IPv6, индексом интерфейса, идентификатором нисходящего или восходящего интерфейса-компоненты. В трёх последних случаях вложенный TLV содержит IP-адрес и идентификатор интерфейса (адрес IP будет использоваться для идентификации Interface ID, в качестве которого может служить, например, идентификатор маршрутизатора для экземпляра).

В некоторых случаях полезно идентифицировать конкретный интерфейс, с которым связана ошибка. Для этого определены объекты RSVP IF_ID и ERROR_SPEC.

8. Смежность по пересылке (FA)

Для повышения уровня масштабируемости MPLS TE (и, таким образом, GMPLS) может оказаться полезным агрегирование множества TE LSP в один TE LSP. Промежуточные узлы в этом случае будут видеть только агрегат LSP. Им не потребуется поддерживать состояния пересылки для каждого агрегированного (внутреннего) LSP, снизится число передаваемых сигнальных сообщений и агрегат LSP может быть защищён как единое целое взамен (или в дополнение) защиты внутренних LSP. Это может существенно повысить уровень масштабируемости сигнализации.

Агрегирование осуществляется с помощью (a) LSR, создающего TE LSP, (b) LSR, формирующего смежность по пересылке за пределами данного LSP (анонсирование данного LSP, как канала TE в IS-IS/OSPF), (c) дозволения другим LSR использовать смежность по пересылке в своих расчётах путей и (d) вложения LSP, начинающихся на других LSR в данный LSP (например, за счёт создания стека меток в случае IP).

ISIS/OSPF в лавинном режиме рассылает информацию FA так же, как прочую информацию о состояниях каналов. В результате такой рассылки LSR имеет в своей базе данных о состоянии каналов TE не только обычную информацию о каналах, но и данные об FA.

LSR при расчёте путей использует не только обычную информацию о каналах, но и данные FA. После расчёта пути LSR использует RSVP-TE/CR-LDP для организации связывания меток на пути. FA требует лишь простого расширения для протоколов сигнализации и маршрутизации.

8.1. Смежность по маршрутизации и пересылке

Отношения смежности по пересылке могут быть представлены, как каналы с адресами или безадресные каналы. FA может также быть связкой LSP между парой узлов.

FA анонсируются, как каналы GMPLS TE типа определённых в [HIERARCHY]. Каналы GMPLS TE анонсируются в OSPF и IS-IS в соответствии с определениями [OSPF-TE-GMPLS] и [ISIS-TE-GMPLS]. Эти документы задают также расширения [OSPF-TE] и [ISIS-TE], определяющие каналы TE.

При динамическом создании FA атрибуты TE наследуются от FA-LSP, индуцировавшего создание FA. В документе [HIERARCHY] описано, как каждый из TE-параметров FA наследуется от FA-LSP. Отметим, что полоса пропускания FA должна быть не меньше полосы FA-LSP, вызвавшего создание, но может быть больше, если для полосы FA-LSP доступны только дискретные значения. В общем случае для динамически создаваемой смежности по пересылке может потребоваться основанный на правилах механизм связывания атрибутов со смежностью по пересылке.

Анонс FA может содержать информацию о пути, взятую из FA-LSP, связанного с FA. Другие LSR могут использовать эту информацию для расчёта путей. Информация передаётся в новых OSPF и IS-IS TLV, которые называют Path TLV.

Возможно изменение со временем лежащей в основе информации о пути за счёт обновления конфигурации или динамической смены маршрута, что приводит к изменению данного TLV.

Если отношения смежности по пересылке связываются (путём связки каналов) и получаемая в результате связка передаёт Path TLV, лежащий в основе путь для всех FA-LSP, формирующих каналы-компоненты, должен быть один и тот же.

Предполагается, что смежность по пересылке не будет использоваться для организации партнерских отношений IS-IS/OSPF между маршрутизаторами по разные стороны смежности.

Иерархия LSP может существовать как в партнерской, так и в оверлейной модели. В партнерской модели иерархия LSP реализуется через FA, а LSP создаётся и используется, как канал TE тем же экземпляром уровня управления. Создание иерархии LSP с перекрытиями не включает концепцию FA. В оверлейной модели LSP, созданный (и поддерживаемый) одним экземпляром уровня управления GMPLS, используется, как канал TE другим экземпляром уровня управления GMPLS. Более того, предполагается, что узлы, использующие канал TE, являются смежными по маршрутизации и сигнализации.

8.2. Аспекты сигнализации

В целях обработки явного маршрута в сообщении Path/Request пути LSP, который будет туннелироваться через смежность по пересылке, LSR в «голове» FA-LSP видит LSR в «хвосте» FA-LSP, как смежный (один интервал IP).

8.3. Каскадирование смежности по пересылке

В интегрированной модели несколько уровней контролируется с использованием общих протоколов сигнализации и маршрутизации. Сеть в этом случае может иметь каналы с разными возможностями мультиплексирования/демультиплексирования. Например, узел может быть способен мультиплексировать и демультиплексировать отдельные пакеты на данном канале и мультиплексировать/демультиплексировать каналы внутри SONET на других каналах.

Определены новые суб-TLV для OSPF и IS-IS, позволяющие анонсировать возможности мультиплексирования для каждого интерфейса - PSC, L2SC, TDM, LSC или FSC. Эти суб-TLV называют дескрипторами возможностей коммутации интерфейса[1] и они служат дополнением к суб-TLV, определённых в [OSPF-TE-GMPLS] и [ISIS-TE-GMPLS]. Информация, передаваемая в этих суб-TLV, используется для создания областей (region) LSP и определения границ областей.

При расчёте пути для LSP могут приниматься во внимание границы областей. Например, расчёт может ограничивать пути, принимаемые для LSP, могут ограничиваться набором каналов, которые поддерживают мультиплексирование/демультиплексирование PSC. Когда требуется, чтобы LSP пересекал границу области, на лежащем в основе уровне (т. е., на уровне L2SC) может организовываться FA. Это может вызвать каскадирование FA между уровнями в показанном здесь порядке - L2SC, далее TDM, затем LSC и, наконец, FSC.

9. Смежность по маршрутизации и сигнализации

По определению два узла являются смежными по маршрутизации (IS-IS/OSPF), если они являются соседями в IS-IS/OSPF.

По определению два узла являются смежными по сигнализации (RSVP-TE/CR-LDP), если они являются соседями в RSVP-TE/CR-LDP. Узлы A и B являются соседями RSVP-TE, если они напрямую обмениваются сообщениями RSVP-TE (Path/Resv) (например, как описано в параграфах 7.1.1 и 7.1.2 документа [HIERARCHY]). Отношения соседства включают обмен сообщениями RSVP-TE Hello.

По определению смежность по пересылке (FA) представляет собой канал TE между двумя узлами GMPLS, путь которого проходит через один или множество узлов (G)MPLS в том же экземпляре уровня управления (G)MPLS. Если между парой узлов есть один или множество каналов, не являющихся TE-каналами, предполагается (но не требуется), что эти узлы являются смежными по маршрутизации. Если между парой узлов нет каналов TE, не являющихся FA , предполагается (но не требуется), что эти два узла не являются смежными по маршрутизации. Разумеется, что если каналы TE между двумя узлами используются для организации LSP, два узла должны быть смежными по сигнализации.

Если нужно организовать отношения смежности по маршрутизации и/или сигнализации между двумя узлами, между ними должен быть путь IP. Этот путь может быть, например, каналом TE с поддержкой на интерфейсах коммутации PSC, чем-нибудь, похожим на канал IP (например, туннель GRE или двухсторонний LSP с поддержкой на интерфейсах коммутации PSC).

Канал TE может оказаться непригодным для прямой организации смежности по маршрутизации и/или сигнализации. Это обусловлено тем, что в GMPLS смежность по маршрутизации и сигнализации требует обмена данными на уровне кадров/пакетов и канал TE (например, канал между OXC) может быть неспособен обмениваться данными на уровне пакетов. В этом случае смежность по маршрутизации и сигнализации организуется с помощью одного или множества каналов управления (см. [LMP]).

Между парой узлов может быть канала TE даже при отсутствии между этими узлами смежности по маршрутизации. Естественно, на каждом узле должен работать протокол OSPF/IS-IS с расширениями GMPLS для того, чтобы можно

[1] Interface Switching Capability Descriptor sub-TLV.

было анонсировать канал TE. Точнее говоря, на узле должно работать расширение GMPLS для каналов TE с поддержкой коммутации на интерфейсах (см. [GMPLS-ROUTING]), отличной от PSC. Более того, на этом узле должны работать расширения GMPLS или MPLS для каналов TE с поддержкой на интерфейсах коммутации PSC.

Следует использовать механизмы отделения канала управления[1] [RFC3471] даже в тех случаях, когда путь путь IP между двумя узлами является каналом TE. Т. е., сигнализации RSVP-TE/CR-LDP следует использовать объект Interface_ID (IF_ID) для указания конкретного канала TE при организации LSP.

Путь IP может включать множество интервалов IP. В этом случае следует использовать механизмы, описанные в параграфах 7.1.1 b 7.1.2 of [HIERARCHY] (в дополнение к Control Channel Separation).

10. Обработка отказов на уровне управления

На уровне управления могут возникать отказы двух основных типов. Первый называют отказом канала управления и он относится к случаям, когда между соседними узлами теряется возможность обмена данными управления. Если канал управления встроен в канал данных, процедура восстановления канала данных должна решать и задачу восстановления канала управления. Если канал управления независим от канала данных, для решения задачи восстановления канала управления требуются дополнительные процедуры.

Второй тип, называемый отказом узлов, относится к тем случаям, когда узел теряет данные управления (например, после перезапуска), но не теряет возможности обмена данными.

В транспортных сетях такие типы отказов на уровне управления не должны оказывать влияния на обслуживание существующих соединений. По этой причине требуется механизм детектирования коммуникационных отказов на уровне управления и процедура восстановления, гарантирующая целостность соединения на обеих сторонах канала управления.

При восстановлении после отказа канала управления протоколы маршрутизации обычно способны восстановить работу, однако нижележащий сигнальный протокол должен показать, что узлы поддерживают информацию о состоянии после отказа. Сигнальный протокол должен также гарантировать, что любые изменения состояния, произошедшие во время отказа, были синхронизированы между узлами.

При отказе узла уровень управления перезапускается и теряет большую часть информации о состоянии. В этом случае восходящий и нисходящий узлы должны синхронизировать свои данные о состоянии с перезапущенным узлом. Для выполнения такой синхронизации перезапускаемый узел должен сохранить некоторую информацию типа отображения входящих меток на исходящие.

Эти вопросы решаются на уровне конкретных протоколов, как описано в [RFC3473], [RFC3472], [OSPF-TE-GMPLS] и [ISIS-TE-GMPLS]. Отметим, что это применимо только для случаев, когда имеются механизмы детектирования отказов на каналах данных независимо от отказов на каналах управления.

Устойчивость к отказам LDP[2] [RFC3479] задаёт процедуры восстановления при отказах канала управления. В [RFC3473] указано, как осуществляется восстановление при отказах каналов управления и узлов.

11. Защита и восстановление LSP

В этом разделе рассматриваются вопросы защиты и восстановления (P&R[3]) для GMPLS LSP. Это обусловлено требованиями [RFC3386] и некоторыми принципами, намеченными в [RFC3469]. По мере определения механизмов GMPLS P&R защита и восстановление будут улучшаться. Ниже приведён перечень вопросов, рассматриваемых в данном разделе.

- Информация этого раздела применима только к ситуациям, когда подверженные влиянию отказов LSP относятся у уровню данных (транспорту). В разделе 10 рассмотрены вопросы обработки отказов уровня управления на каналах управления и узлах. Данный раздел фокусируется на P&R для уровней TDM, LSC и FSC. Существуют специфические требования P&R для этих уровней, которые отсутствуют на уровне PSC.
- В данном разделе рассматриваются вопросы P&R внутри области в отличие от P&R между областями и между доменами. Отметим, что P&R можно ограничить даже уровнем оборудования заказчика, уровнем набора однотипного оборудования или уровнем одной области маршрутизации.
- В этом разделе рассматривается P&R внутри одного уровня (горизонтальная иерархия, определённая в [RFC3386]) в отличие от P&R между уровнями (вертикальная иерархия).
- Механизмы P&R в общем случае предназначены для обработки одиночных отказов, которые делают необходимым многообразие SRLG. Восстановление при множественных отказах требует дополнительного исследования.
- Поддерживаются как кольцевая, так и многосвязная (mesh) топология.

В дальнейшем предполагается, что:

- устройства TDM, LSC и FSC обычно выделяют ресурсы для восстановления способом, отличным от «выделения по возможности[4]»; ресурсы для восстановления уже используются (выделены) или зарезервированы логически (независимо от того, используются ли они для прерываемого трафика, эти ресурсы не могут быть доступны для обычного трафика);
- совместно используемые механизмы P&R позволяют операторам повысить коэффициент загрузки их сети;
- передача прерываемого избыточного трафика с использованием предназначенных для восстановления ресурсов удобна для операторов =.

[1]Control Channel Separation.
[2]LDP Fault tolerance.
[3]Protection and Restoration.
[4]Non-best effort way.

11.1. Обеспечение защиты через домены и уровни

Для описания архитектуры P&R требуется рассмотреть два варианта иерархии [RFC3386]:

- *Горизонтальная иерархия*, содержащая множество доменов P&R, представляющая важность в основанной на LSP схеме защиты. Зона действия P&R может быть расширена через канал (или интервал), административный домен или подсеть, LSP в целом.

  Административный домен может состоять из одного домена P&R или представлять собой объединение множества более мелких доменов P&R. Оператор может конфигурировать домены P&R на основе требований заказчиков с учётом сетевой топологии и требований по построению трафика.

- *Вертикальная иерархия*, включающая множество уровней P&R с различной гранулярностью (поток пакетов, трейлер STS, световой путь, волокно и т. п.).

  При отсутствии адекватной координации P&R отказ может распространяться на следующий уровень иерархии P&R. Это может порождать «коллизии» и одновременные действия по восстановлению могут вызывать конфликты, снижать уровень использования ресурсов и вызывать нестабильности [MANCHESTER]. Поэтому нужна согласованная стратегия защиты для координации действий по восстановлению в разных доменах и уровнях. Возможность использования GMPLS на разных уровнях может упростить такую координацию.

  Существует два типа стратегии расширения защиты - «снизу вверх» и «сверху вниз». Первый вариант предполагает, что схемы восстановления «нижнего уровня» является более рациональной. Следовательно, она может подавить и задержать P&R вышележащего уровня. В варианте расширения сверху вниз предпринимается попытка выполнить P&R на верхних уровнях до вовлечения в работу P&R нижележащих уровней. P&R верхнего уровня выбирается для сервиса и обеспечивает возможность перемаршрутизации на уровне CoS или LSP.

Сервисные соглашения (Service Provider или SLA) между сетевыми операторами и их клиентами нужны для определения необходимости временных рамок P&R для каждого уровня и каждого домена.

11.2. Отображение сервиса на ресурсы P&R

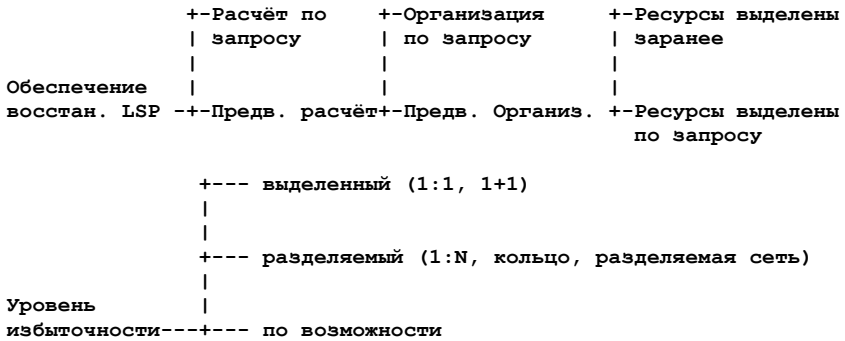
Выбор схемы P&R является компромиссом между уровнем полезной загрузки сети (стоимость) и временем прерывания обслуживания. С учётом этого предполагается что сервис-провайдеры будут поддерживать широкий спектр типов услуг и уровней сервиса.

Можно классифицировать LSP в небольшой набор уровней сервиса. Вместе с другими параметрами уровень сервиса определяет параметры надёжности LSP. Уровень сервиса, связанный с данным LSP, отображается на одну или множество схем P&R в процессе организации LSP. Преимущество такого отображения заключается в том, что LSP может использовать разные схемы P&R[1] в разных сегментах сети (например, некоторые каналы могут использовать span-защиту, а другие сегменты LSP - кольцевую). Очевидно, что такие детали определяются сервис-провайдером.

Дополнением к использованию разных уровней сервиса является задание для приложения набора конкретных механизмов P&R, которые будут использоваться при организации LSP. Это обеспечивает дополнительную гибкость за счёт использования различных механизмов с учётом требований приложений.

Критерием дифференцирования между уровнями сервиса является время прерывания обслуживания при отказах в сети, которое определяется продолжительностью периода между возникновением отказа и восстановлением связности. Выбор уровня сервиса (или схемы P&R) следует производить на основе требований по обслуживанию для различных приложений.

11.3. Классификация характеристик механизма P&R



На рисунке показана классификация возможных типов восстановления LSP и уровней избыточности, которые возможны для них.

11.4. Этапы P&R

Восстановление при отказе или повреждении в сети осуществляется в несколько этапов, как рассмотрено в работе [RFC3469], включая обнаружение отказа, его локализацию, уведомление, восстановление (т. е. собственно P&R) и возобновление трафика (т. е. возврат трафика к исходному состоянию работающего LSP или создание нового пути).

- *Детектирование отказа* представляет зависит от технологии и реализации. В общем случае отказы обнаруживаются с помощью механизмов нижележащих уровней (например, SONET/SDH, LOL[2]). Когда узел детектирует отказ, объекту GMPLS может передаваться сигнал тревоги, который будет инициировать соответствующие действия или передаваться на нижележащий уровень (например, SONET/SDH AIS).

[1] В оригинале ошибочно указано P&E. *Прим. перев.*
[2] Loss-of-Light - потеря оптического сигнала.

- *Локализация отказа* может выполняться с помощью GMPLS (например, путём использования локализации отказов LMP - см. параграф 6.4).
- *Уведомления об отказах* могут обеспечиваться средствами GMPLS (например, с помощью уведомлений GMPLS RSVP-TE/CR-LDP - см. параграф 7.12).
- В этом разделе рассматриваются различные механизмы, доступные для восстановления и возобновления трафика после детектирования и локализации отказа, а также уведомления о нем.

11.5. Стратегия восстановления

Методы P&R можно разделить на защиту (Protection) и восстановление (Restoration). Для целей защиты ресурсы, используемые в защиту конечных точек, организуются до возникновения отказа и связность при возникновении отказа обеспечивается простым переключением, выполняемым на защищённых конечных точках. При восстановлении же, напротив, используется сигнализация для выделения ресурсов по восстанавливаемому пути.

- Целью защиты является максимально быстрая реакция и защита может основываться на использовании избыточных полей управления для координации конечных точек. Защита для сетей SONET/SDH описана в документах [ITUT-G.841] и [ANSI-T1.105]. Механизмы защиты можно классифицировать по уровню избыточности и возможности их совместного использования.
- Механизмы восстановления могут опираться на протоколы сигнализации для координации переключений в процессе восстановления, а также могут включать простое восстановление с сигнализацией по факту возобновления сервиса или упреждающую сигнализацию (до возобновления обслуживания).

P&R можно применять локально или в режиме сквозной работы. В локальном варианте P&R фокусируется на возникающих вблизи отказах с целью снижения задержки при восстановлении сервиса. В сквозном режиме восстановлением управляют исходный и завершающий узлы LSP.

С использованием описанных стратегий можно определить несколько механизмов восстановления, описанных ниже.

11.6. Механизмы восстановления - схемы защиты

Отметим, что выбор схемы защиты обычно зависит от технологии, но не исключаются и иные подходы.

- *1+1 Link Protection*. Два заранее подготовленных ресурса используются параллельно. Например, данные передаются одновременно по двум параллельным каналам и на приёмной стороне используется селектор для выбора лучшего источника (см. также [GMPLS-FUNCT]).
- *1:N Link Protection*. Рабочие и защитные ресурсы (N рабочих, 1 резервный) подготавливаются заранее. При отказе рабочего ресурса данные переключаются на защитный ресурс с использованием механизма координации (например, в служебных байтах). В более общем случае N рабочих и M защитных ресурсов позволяют организовать защиту M:N (см. также [GMPLS-FUNCT]).
- *Enhanced Protection*. Могут применяться различные механизмы (типа защитных колец) для повышения уровня защиты при отказе более одного канала для обеспечения возможности обхода отказавшего узла или интервала (span) узлов с использованием заранее подготовленной топологии защитных ресурсов (на момент подготовки этого документа ссылок на завершённые работы не было).
- *1+1 LSP Protection*. Одновременная передача данных по рабочему и защитному LSP с выбором на оконечной стороне (см. также [GMPLS-FUNCT]).

11.7. Механизмы восстановления - схемы восстановления

Благодаря использованию в GMPLS распределенного уровня управления, восстановление можно выполнить за десятки миллисекунд. Значительно сложнее восстановить обслуживание при использовании только NMS - в таких случаях восстановление занимает секунды.

- *Сквозное восстановление LSP с возобновлением*. Сквозной путь восстановления организуется после отказа Путь восстановления может динамически рассчитываться после отказа или подготавливаться заранее (зачастую, при организации LSP). Важно подчеркнуть, что до отказа по пути восстановления не используется какой-либо специальной сигнализации и полоса для восстановления не резервируется. Следовательно, в таких случаях нет гарантии, что данный путь восстановления будет доступен в момент возникновения отказа. В результате при восстановлении может возникать задержка, связанная с поиском доступного пути.
- *Сквозное восстановление LSP с предварительной сигнализацией для резервирования полосы, но без предварительного выделения меток*. Путь восстановления рассчитывается до отказа и для этого пути передаются сигнальные сообщения с целью резервирования полосы, но метки заранее не выбираются (см. также [GMPLS-FUNCT]).

  Ресурсы, резервируемые на каждом канале пути восстановления, могут относиться к разным рабочим LSP, которые предположительно не могут отказать одновременно. Для определения уровня влияния отказов на разделяемых независимых каналах может применяться локальная политика узла. При обнаружении отказа по пути восстановления инициируется сигнализация LSP для выполнения требуемых переключений.
- *Сквозное восстановление LSP с предварительной сигнализацией для резервирования полосы и предварительным выделением меток*. Путь восстановления рассчитывается до отказа, для этого пути передаются сигнальные сообщения с целью резервирования полосы и заранее выбираются метки (см. также [GMPLS-FUNCT]).

  Ресурсы, резервируемые на каждом канале пути восстановления, могут относиться к разным рабочим LSP, которые предположительно не могут отказать одновременно. В сетях на основе технологий TDM, LSC и FSC

после обнаружения отказа используется сигнализация LSP для организации требуемых переключений на промежуточных коммутаторах пути восстановления с использованием заранее выделенных меток.

- *Локальное восстановление LSP*. Описанные выше модели могут использоваться локально (не в сквозном режиме) с целью снижения времени восстановления (на момент подготовки этого документа ссылок на завершённые работы не было).

11.8. Критерии выбора схемы

В этом параграфе рассматриваются критерии, которые могут быть использованы при выборе механизмов P&R.

- *Отказоустойчивость*. В общем случае снижение уровня предварительного планирования пути восстановления будет повышать отказоустойчивость схемы восстановления при условии доступности требуемых ресурсов. Схемы восстановления с заранее подготовленными путями не смогут обеспечить восстановления при отказах, затрагивающих одновременно рабочий и восстановительный путь. Поэтому пути следует выбирать как можно более развязанные между собой (т. е., не связанные на уровне узлов и SRLG), чтобы один отказ не мог воздействовать на оба пути. Риск одновременного отказа на обоих путях можно снизить путём пересчёта пути восстановления при возникновении на нем отказа.

  Предварительный выбор меток снижает уровень гибкости для многих сценариев отказа по сравнению с восстановлением без предварительного выбора метки. Если возникает отказ, воздействующий на два LSP, разделяющие метку на общем узле путей восстановления, восстановление возможно только для одного из этих LSP, если не будет изменено выделение метки.

  Отказоустойчивость схемы восстановления зависит также от размера резервируемой для восстановления полосы. По мере роста совместного использования полосы восстановления (снижение резерва) схема восстановления становится менее устойчивой к отказам. Схемы восстановления с предварительной сигнализацией для резервирования полосы (с предварительным выбором метки или без такового) могут обеспечивать резерв полосы для восстановления при любом заданном множестве отказов (отказ одного SRLG, отказ произвольной пары SRLG и т. п.). Очевидно, что для более крупных отказов выделяется большая полоса для восстановления. Таким образом, уровень защиты сети определяется политикой выделения полосы для восстановления.

- *Время восстановления*. В общем случае повышение уровня предварительного планирования восстановительного пути ускоряет работу схемы P&R. Схемы защиты обычно работают быстрее схем восстановления. Восстановление при зарезервированной с помощью сигнализации полосе (значительно) быстрее, чем восстановление с возобновлением пути. Локальное восстановление обычно быстрее сквозного.

  Требования к времени восстановления для защитной коммутации SONET/SDH (не включая время обнаружения отказа) в [ITUT-G.841] задают значение 50 мсек, с учётом ограничений на расстояния, число вовлечённых соединений и число узлов в кольце при использовании улучшенной кольцевой схемы защиты.

- Временные параметры механизмов восстановления для других технологий определены в [RFC3386].

- *Совместное использование ресурсов*. Защита каналов по схеме 1+1 и 1:N, а также защита LSP требует наличия выделенных путей восстановления с ограниченной возможность использования этих путей для других целей - схема 1+1 совместного использования каналов, 1:N разрешает некоторое использование защитных ресурсов для передачи другого (прерываемого) трафика. Гибкость решения ограничивается топологией (например, использованием традиционной технологии защитного кольца). Уровень дозволенного совместного использования защитных ресурсов напрямую влияет на размер восстановительного пула. В схемах восстановления с возобновлением может быть определён восстановительный пула, из которого выбираются все маршруты, доступные после аварии. Таким образом, степень совместного использования определяется размером доступной восстановительной ёмкости. При восстановлении с предварительным резервированием полосы с помощью сигнализации объем восстановительных ресурсов определяется локальной политикой резервирования полосы. Во всех схемах восстановления прерываемые ресурсы могут использовать резервную ёмкость, когда она не требуется.

12. Управление сетью

Сервис-провайдеры (Service Provider или SP) широко используют системы сетевого управления для настройки конфигурации, мониторинга и обслуживания различных устройств в своих сетях. Важно подчеркнуть, что оборудование SP может быть распределено географически по разным сайтам и это повышает уровень важности вопросов распределенного управления. Сервис-провайдерам следует использовать систему NMS, стандартные протоколы управления типа SNMP (см. [RFC3410], [RFC3411] и [RFC3416]) и соответствующие модули MIB в качестве стандартных интерфейсов для настройки, мониторинга и обслуживания устройств, расположенных на разных площадках. Провайдеры могут также использовать командный интерфейс управления (Command line interface или CLI), предоставляемый производителями оборудования. Однако такое решение нельзя отнести к стандартным и рекомендуемым по причине отсутствия стандартов для языка и интерфейса CLI, что приводит к наличию N[1] разных CLI в сети с оборудованием N различных производителей. В контексте GMPLS наличие стандартных интерфейсов (например, SNMP) для устройств SP очень важно в силу особенностей самой технологии GMPLS. Поскольку GMPLS включает множество разных технологий, используемых на уровнях управления и данных, очень важна гибкость интерфейсов управления, чтобы обеспечить администраторам возможность простого, эффективного и стандартного управления GMPLS.

12.1. Системы сетевого управления (NMS)

Системе NMS следует поддерживать информацию о каждом устройстве в системе. Отметим, что система NMS на практике может включать несколько распределенных приложений (например, средства сбора сигналов тревоги, консоли управления, приложения для опроса и т. п.), которые совместно образуют систему управления сетью

[1]На практике даже у одного производителя зачастую используются совершенно разные CLI в различных устройствах, что дополнительно усугубляет проблему. *Прим. перев.*

оператора. За счёт этого система управления позволяет принимать решения по предоставлению услуг и управлению на основе полной информации о сети SP. Информация по настройке и предоставлению услуг (например, запросы новых услуг) может вводиться в NMS и в последствии распространяться по протоколу SNMP на удалённые устройства. Это делает задачу управления сетью SP более компактной и менее трудоёмкой по сравнению с управлением на уровне отдельных устройств (например, с помощью CLI).

Защита и контроль доступа может обеспечиваться на основе моделей USM[1] SNMPv3 [RFC3414] и VACM[2] [RFC3415]. Эти модели могут очень эффективно применяться в сети SP, поскольку сервис-провайдер получает доступ и контроль для всех устройств своего домена. Требуется разработка стандартизованных MIB, которые позволят обеспечить повсеместное использование модели для управления, настройки и мониторинга устройств внутри сети и даже через границы сетей SP.

12.2. База данных управления (MIB)

В контексте GMPLS очень важно наличие стандартизованных интерфейсов для устройств. Поскольку GMPLS включает на уровне управления множество технологий, важно обеспечить достаточную гибкость модулей SNMP MIB, которая позволит администраторам полностью контролировать уровень управления. Для реализации этого следует использовать модули MIB, которые могут кооперироваться (например, скоординированное создание строк в агентах), или обобщённые модули MIB, которые агрегируют некоторые из нужных действий и передают детальную информацию в устройства. Важно отметить, что при некоторых обстоятельствах может потребоваться дублирование некоторого незначительного подмножества объектов в новых модулях MIB для обеспечения удобства управления. Управление некоторыми частями GMPLS может также обеспечиваться на основе имеющихся интерфейсов MIB (например, SONET MIB) или интерфейсов, которые будут определены. Модули MIB могут оказаться уже определёнными в IETF или ITU. Для имеющихся модулей MIB могут потребоваться расширения с учётом желаемой для GMPLS функциональности. В таких случаях рабочим группам следует подготовить новые версии MIB с требуемыми расширениями.

12.3. Инструментальные средства

Как и в традиционных сетях для отладки и мониторинга GMPLS нужны инструменты типа traceroute [RFC1393] и ping [RFC2151] прежде всего для топологии уровня управления GMPLS, которая будет подражать топологии уровня данных. Более того, такие средства обеспечивают информацию о доступности сетей. Протоколы управления GMPLS должны будут показывать часть информации для обеспечения корректной работы таких инструментов и обеспечения информации для GMPLS. Эти инструменты должны работать из командной строки (CLI). Следует также обеспечить возможность удалённой работы с инструментами через интерфейс SNMP [RFC2925].

12.4. Корреляция отказов на разных уровнях

По природе GMPLS и в силу использования множества уровней контроля и передачи данных и управляющей информации GMPLS нужно, чтобы информация об отказе на одном уровне передавалась на смежные (выше- и нижележащий) уровни для уведомления последних об авариях. Однако с учётом природы этих уровней возможна (и весьма вероятна) передача сотен и даже тысяч уведомлений между уровнями. Такое поведение нежелательно по ряду причин. Во-первых, эти уведомления будут перегружать устройства работой. Во-вторых, если устройства запрограммированы на генерацию сообщений SNMP Notification [RFC3417] может приводить к лавинам уведомлений о приёме уведомлений. Более того, система NMS, которая должна обрабатывать такие уведомления, будет вынуждена работать со множеством дубликатов информации. По этой причине, если 1000 интерфейсов на уровне B собирается в один интерфейс нижележащего уровня A и на интерфейсе A возникнет авария, каждому интерфейсу уровня B не следует передавать уведомления. Взамен следует передать одно уведомление от интерфейса уровня A. Система NMS, принявшая такое уведомление, должна быть способна найти корреляцию между фактом отказа интерфейса и индуцированными авариями на интерфейсах уровня B, а также предпринять соответствующие действия.

Поддерживающим GMPLS устройствам следует обеспечивать механизм агрегирования, резюмирования, включения и отключения межуровневых уведомлений с учётом приведённых выше соображений. В контексте модулей SNMP MIB все модули, используемые GMPLS, должны обеспечивать возможность разрешения/запрета для всех объектов уведомлений. Более того, эти MIB должны также обеспечивать объекты или функциональность для резюмирования (как сказано выше). Системы NMS и стандартные инструменты обработки уведомлений или их отслеживания на множестве уровней в любом данном устройстве должны быть способны обрабатывать значительный объем информации, которая потенциальном может генерироваться сетевыми устройствами GMPLS.

13. Вопросы безопасности

GMPLS определяет архитектуру уровня управления для множества технологий и типов сетевых элементов. В общем случае с момента, когда LSP, организованные с помощью GMPLS, смогут передавать большие объёмы информации и потреблять значительные сетевые ресурсы, требуются механизмы защиты для обеспечения безопасности лежащей в основе сети от атак на уровень управления и/или несанкционированного использования транспортных ресурсов. Уровню управления GMPLS следует включать механизмы, предотвращающие или минимизирующие риск вставки или подмены трафика управления со стороны атакующих. Эти риски зависят от уровня доверия между узлами, которые обмениваются управляющими сообщениями GMPLS, а также от реализации и физических характеристик каналов управления. Например, канал управления в основной полосе оптического волокна использующий служебные байты SONET/SDH в общем случае менее уязвим, нежели канал управления в основной полосе сети IP.

Механизмы защиты могут обеспечивать аутентификацию и конфиденциальность. Аутентификация может обеспечивать проверку источника, целостность сообщений и предотвращение повторного использования, а конфиденциальность гарантирует недоступность для посторонних содержимого сообщений. В ситуациях, когда реализация GMPLS требует в основном аутентификации, могут использоваться соответствующие механизмы протоколов-компонент GMPLS (см. [RFC2747], [RFC3036], [RFC2385] и [LMP]). В дополнение к этому может применяться стек протоколов IPsec (см. [RFC2402], [RFC2406] и [RFC2409]) для обеспечения аутентификации и/или конфиденциальности в каналах

[1]User-based Security Model - модель защиты с управлением на уровне отдельных пользователей.
[2]View-based Access Control Model - управление доступом на уровне представления.

управления GMPLS. IPsec обеспечивает преимущества комбинированной защиты для всех протокольных компонент GMPLS, а также для управления.

Связанным вопросом является проверка полномочности запросов на выделение ресурсов в поддерживающих GMPLS узлах. Проверка полномочий позволяет определить, является ли запрашивающая ресурсы сторона идентифицированной и имеет ли она право доступа к ресурсам. Это определение обычно выполняется на основе локальной политики [RFC2753] (например, путём задания предельной полосы, доступной некому «пользователю» в условиях конкурентного доступа к ресурсам. Такая политика может стать достаточно сложной, по мере роста в ней учитывается числа пользователей, типов ресурсов и более изощрённой проверки полномочий. После идентификации запроса элементы управления проверяются на предмет соответствия локальной политике проверки полномочий. Эти элементы управления должны обеспечивать возможность выбора на основе идентификации запрашивающей стороны криптографической и/или топологической верификации. Например, решение может зависеть от интерфейса (внутридоменный или внешний), через который принят запрос. Использование соответствующей локальной политики проверки полномочий может помочь в ограничении влияния прорех в защите на удалённых узлах сети.

В заключение следует отметить, что технология GMPLS сама по себе не создаёт новых проблем безопасности для существующих протоколов сигнализации MPLS-TE (RSVP-TE, CR-LDP), маршрутизации (OSPF-TE, IS-IS-TE) и сетевого управления (SNMP).

14. Благодарности

Этот документ является результатом работы множества людей и включает информацию из многочисленных более ранних документов, посвящённых той же теме.

Большое спасибо Ben Mack-Crane (Tellabs) за обсуждение вопросов, связанных с SONET/SDH. Благодарим также Pedro Falcao, Alexandre Geyssens, Michael Moelants, Xavier Neerdaels и Philippe Noel из Ebone за поддержку по вопросам, связанным с SONET/SDH и оптическими технологиями. В заключение хотим поблагодарить Krishna Mitra (Consultant), Curtis Villamizar (Avici), Ron Bonica (WorldCom), Bert Wijnen (Lucent) за их работу по подготовке раздела 12.

15. Литература

15.1. Нормативные документы

[RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, December 2001.

[RFC3212] Jamoussi, B., Andersson, L., Callon, R., Dantu, R., Wu, L., Doolan, P., Worster, T., Feldman, N., Fredette, A., Girish, M., Gray, E., Heinanen, J., Kilty, T., and A. Malis, "Constraint-Based LSP Setup using LDP", RFC 3212, January 2002.

[RFC3471] Berger, L., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description", RFC 3471, January 2003.

[RFC3472] Ashwood-Smith, P. and L. Berger, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Constraint-based Routed Label Distribution Protocol (CR-LDP) Extensions", RFC 3472, January 2003.

[RFC3473] Berger, L., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, January 2003.

15.2. Дополнительная литература

[ANSI-T1.105] "Synchronous Optical Network (SONET): Basic Description Including Multiplex Structure, Rates, And Formats," ANSI T1.105, 2000.

[BUNDLE] Kompella, K., Rekhter, Y., and L. Berger, "Link Bundling in MPLS Traffic Engineering", Work in Progress[1].

[GMPLS-FUNCT] Lang, J.P., Ed. and B. Rajagopalan, Ed., "Generalized MPLS Recovery Functional Specification", Work in Progress[2].

[GMPLS-G709] Papadimitriou, D., Ed., "GMPLS Signaling Extensions for G.709 Optical Transport Networks Control", Work in Progress[3].

[GMPLS-OVERLAY] Swallow, G., Drake, J., Ishimatsu, H., and Y. Rekhter, "GMPLS UNI: RSVP Support for the Overlay Model", Work in Progress[4].

[GMPLS-ROUTING] Kompella, K., Ed. and Y. Rekhter, Ed., "Routing Extensions in Support of Generalized Multi-Protocol Label Switching", Work in Progress[5].

[RFC3946] Mannie, E., Ed. and Papadimitriou D., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Extensions for Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH) Control", RFC 3946, October 2004.

[HIERARCHY] Kompella, K. and Y. Rekhter, "LSP Hierarchy with Generalized MPLS TE", Work in Progress[6].

[ISIS-TE] Smit, H. and T. Li, "Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)", RFC 3784, June 2004.

[1]Работа опубликована в RFC 4201. *Прим. перев.*
[2]Работа опубликована в RFC 4426. *Прим. перев.*
[3]Работа опубликована в RFC 4328. *Прим. перев.*
[4]Работа опубликована в RFC 4208. *Прим. перев.*
[5]Работа опубликована в RFC 4202. *Прим. перев.*
[6]Работа опубликована в RFC 4206. *Прим. перев.*

[ISIS-TE-GMPLS] Kompella, K., Ed. and Y. Rekhter, Ed., "IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching", Work in Progress[2].

[ITUT-G.707] ITU-T, "Network Node Interface for the Synchronous Digital Hierarchy", Recommendation G.707, October 2000.

[ITUT-G.709] ITU-T, "Interface for the Optical Transport Network (OTN)," Recommendation G.709 version 1.0 (and Amendment 1), February 2001 (and October 2001).

[ITUT-G.841] ITU-T, "Types and Characteristics of SDH Network Protection Architectures," Recommendation G.841, October 1998.

[LMP] Lang, J., Ed., "Link Management Protocol (LMP)", Work in Progress[3].

[LMP-WDM] Fredette, A., Ed. and J. Lang Ed., "Link Management Protocol (LMP) for Dense Wavelength Division Multiplexing (DWDM) Optical Line Systems", Work in Progress[4].

[MANCHESTER] J. Manchester, P. Bonenfant and C. Newton, "The Evolution of Transport Network Survivability," IEEE Communications Magazine, August 1999.

[OIF-UNI] The Optical Internetworking Forum, "User Network Interface (UNI) 1.0 Signaling Specification - Implementation Agreement OIF-UNI-01.0," October 2001.

[OLI-REQ] Fredette, A., Ed., "Optical Link Interface Requirements," Work in Progress.

[OSPF-TE-GMPLS] Kompella, K., Ed. and Y. Rekhter, Ed., "OSPF Extensions in Support of Generalized Multi-Protocol Label Switching", Work in Progress[5].

[OSPF-TE] Katz, D., Kompella, K., and D. Yeung, "Traffic Engineering (TE) Extensions to OSPF Version 2", RFC 3630, September 2003.

[RFC1393] Malkin, G., "Traceroute Using an IP Option", RFC 1393, January 1993.

[RFC2151] Kessler, G. and S. Shepard, "A Primer On Internet and TCP/IP Tools and Utilities", RFC 2151, June 1997.

[RFC2205] Braden, R., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.

[RFC2385] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, August 1998.

[RFC2402] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC2702] Awduche, D., Malcolm, J., Agogbua, J., O'Dell, M., and J. McManus, "Requirements for Traffic Engineering Over MPLS", RFC 2702, September 1999.

[RFC2747] Baker, F., Lindell, B., and M. Talwar, "RSVP Cryptographic Authentication", RFC 2747, January 2000.

[RFC2753] Yavatkar, R., Pendarakis, D., and R. Guerin, "A Framework for Policy-based Admission Control", RFC 2753, January 2000.

[RFC2925] White, K., "Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations", RFC 2925, September 2000.

[RFC3036] Andersson, L., Doolan, P., Feldman, N., Fredette, A., and B. Thomas, "LDP Specification", RFC 3036, January 2001.

[RFC3386] Lai, W. and D. McDysan, "Network Hierarchy and Multilayer Survivability", RFC 3386, November 2002.

[RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, December 2002.

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

[RFC3414] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, December 2002.

[RFC3415] Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3415, December 2002.

[RFC3416] Presuhn, R., "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3416, December 2002.

[RFC3417] Presuhn, R., "Transport Mappings for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3417, December 2002.

[2]Работа опубликована в RFC 4205. *Прим. перев.*
[3]Работа опубликована в RFC 4204. *Прим. перев.*
[4]Работа опубликована в RFC 4209. *Прим. перев.*
[5]Работа опубликована в RFC 4203. *Прим. перев.*

[RFC3469] Sharma, V. and F. Hellstrand, "Framework for Multi-Protocol Label Switching (MPLS)-based Recovery", RFC 3469, February 2003.

[RFC3477] Kompella, K. and Y. Rekhter, "Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)", RFC 3477, January 2003.

[RFC3479] Farrel, A., "Fault Tolerance for the Label Distribution Protocol (LDP)", RFC 3479, February 2003.

[RFC3480] Kompella, K., Rekhter, Y., and A. Kullberg, "Signalling Unnumbered Links in CR-LDP (Constraint-Routing Label Distribution Protocol)", RFC 3480, February 2003.

[SONET-SDH-GMPLS-FRM] Bernstein, G., Mannie, E., and V. Sharma, "Framework for GMPLS-based Control of SDH/SONET Networks", Work in Progress[1].

16. Разработчики документа

Peter Ashwood-Smith
Nortel
P.O. Box 3511 Station C,
Ottawa, ON K1Y 4H7, Canada
EMail: petera@nortelnetworks.com

Eric Mannie
Consult
Phone: +32 2 648-5023
Mobile: +32 (0)495-221775
EMail: eric_mannie@hotmail.com

Daniel O. Awduche
Consult
EMail: awduche@awduche.com

Thomas D. Nadeau
Cisco
250 Apollo Drive
Chelmsford, MA 01824, USA
EMail: tnadeau@cisco.com

Ayan Banerjee
Calient
5853 Rue Ferrari
San Jose, CA 95138, USA
EMail: abanerjee@calient.net

Lyndon Ong
Ciena
10480 Ridgeview Ct
Cupertino, CA 95014, USA
EMail: lyong@ciena.com

Debashis Basak
Accelight
70 Abele Road, Bldg.1200
Bridgeville, PA 15017, USA
EMail: dbasak@accelight.com

Dimitri Papadimitriou
Alcatel
Francis Wellesplein, 1
B-2018 Antwerpen, Belgium
EMail: dimitri.papadimitriou@alcatel.be

Lou Berger
Movaz
7926 Jones Branch Drive
MCLean VA, 22102, USA
EMail: lberger@movaz.com

Dimitrios Pendarakis
Tellium
2 Crescent Place, P.O. Box 901
Oceanport, NJ 07757-0901, USA
EMail: dpendarakis@tellium.com

Greg Bernstein
Grotto
EMail: gregb@grotto-networking.com

Bala Rajagopalan
Tellium
2 Crescent Place, P.O. Box 901
Oceanport, NJ 07757-0901, USA
EMail: braja@tellium.com

Sudheer Dharanikota
Consult
EMail: sudheer@ieee.org

Yakov Rekhter
Juniper
1194 N. Mathilda Ave.
Sunnyvale, CA 94089, USA
EMail: yakov@juniper.net

John Drake
Calient
5853 Rue Ferrari
San Jose, CA 95138, USA
EMail: jdrake@calient.net

Debanjan Saha
Tellium
2 Crescent Place
Oceanport, NJ 07757-0901, USA
EMail: dsaha@tellium.com

Yanhe Fan
Axiowave
200 Nickerson Road
Marlborough, MA 01752, USA
EMail: yfan@axiowave.com

Hal Sandick
Shepard M.S.
2401 Dakota Street
Durham, NC 27705, USA
EMail: sandick@nc.rr.com

Don Fedyk
Nortel
600 Technology Park Drive
Billerica, MA 01821, USA
EMail: dwfedyk@nortelnetworks.com

Vishal Sharma
Metanoia
1600 Villa Street, Unit 352
Mountain View, CA 94041, USA
EMail: v.sharma@ieee.org

Gert Grammel
Alcatel
Lorenzstrasse, 10
70435 Stuttgart, Germany
EMail: gert.grammel@alcatel.de

George Swallow
Cisco
250 Apollo Drive
Chelmsford, MA 01824, USA

[1]Работа опубликована в RFC 4205. *Прим. перев.*

EMail: swallow@cisco.com

Dan Guo
Turin
1415 N. McDowell Blvd,
Petaluma, CA 95454, USA
EMail: dguo@turinnetworks.com

Z. Bo Tang
Tellium
2 Crescent Place, P.O. Box 901
Oceanport, NJ 07757-0901, USA
EMail: btang@tellium.com

Kireeti Kompella
Juniper
1194 N. Mathilda Ave.
Sunnyvale, CA 94089, USA
EMail: kireeti@juniper.net

Jennifer Yates
AT&T
180 Park Avenue
Florham Park, NJ 07932, USA
EMail: jyates@research.att.com

Alan Kullberg
NetPlane
888 Washington
St.Dedham, MA 02026, USA
EMail: akullber@netplane.com

George R. Young
Edgeflow
329 March Road
Ottawa, Ontario, K2K 2E1, Canada
EMail: george.young@edgeflow.com

Jonathan P. Lang
Rincon Networks
EMail: jplang@ieee.org

John Yu
Hammerhead Systems
640 Clyde Court
Mountain View, CA 94043, USA
EMail: john@hammerheadsystems.com

Fong Liaw
Solas Research
Solas Research, LLC
EMail: fongliaw@yahoo.com

Alex Zinin
Alcatel
1420 North McDowell Ave
Petaluma, CA 94954, USA
EMail: alex.zinin@alcatel.com

17. Адреса авторов

Eric Mannie (консультант)
Avenue de la Folle Chanson, 2
B-1050 Brussels, Belgium
Phone: +32 2 648-5023
Mobile: +32 (0)495-221775
EMail: eric_mannie@hotmail.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.