МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т Y.1310

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(03/2004)

СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА (IP) И СЕТИ СЛЕДУЮЩИХ ПОКОЛЕНИЙ

Аспекты межсетевого протокола (IP) – Транспортирование

Транспортирование IP над ATM в сетях общего пользования

Рекомендация МСЭ-Т Y.1310

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА (IP) И СЕТИ СЛЕДУЮЩИХ ПОКОЛЕНИЙ

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	
Общие положения	Y.100–Y.199
Службы, приложения и промежуточные программные средства	Y.200–Y.299
Сетевые аспекты	Y.300–Y.399
Интерфейсы и протоколы	Y.400–Y.499
Нумерация, адресация и присваивание имен	Y.500–Y.599
Эксплуатация, управление и техническое обслуживание	Y.600–Y.699
Безопасность	Y.700–Y.799
Рабочие характеристики	Y.800–Y.899
АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА (IP)	
Общие положения	Y.1000–Y.1099
Услуги и приложения	Y.1100–Y.1199
Архитектура, доступ, сетевые возможности и управление ресурсом	Y.1200–Y.1299
Транспортирование	**Y.1300–Y.1399**
Взаимодействие	Y.1400–Y.1499
Качество обслуживания и сетевые показатели качества	Y.1500–Y.1599
Сигнализация	Y.1600–Y.1699
Эксплуатация, управление и техническое обслуживание	Y.1700–Y.1799
Начисление платы	Y.1800–Y.1899
СЕТИ СЛЕДУЮЩИХ ПОКОЛЕНИЙ (NGN)	
Структура и функциональные модели архитектуры	Y.2000–Y.2099
Качество обслуживания и рабочие характеристики	Y.2100–Y.2199
Аспекты служб: Возможности служб и архитектура служб	Y.2200–Y.2249
Аспекты служб: Взаимодействие служб и сетей в NGN	Y.2250–Y.2299
Нумерация, присваивание имен и адресация	Y.2300–Y.2399
Управление сетью	Y.2400–Y.2499
Архитектура и протоколы сетевого управления	Y.2500–Y.2599
Безопасность	Y.2700–Y.2799
Обобщенная мобильность	Y.2800–Y.2899

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-T Y.1310

Транспортирование IP над ATM в сетях общего пользования

Резюме

С быстрым ростом сетей и приложений на основе IP как в частных сетях, так и в сетях общего пользования необходимо рассмотреть средства для транспортирования услуг IP над ATM в среде сети общего пользования.

Для среды частной сети ATM Форум определил многократный протокол над ATM (Multi-Protocol Over ATM, MPOA) [ATM_MPOA]. Целевая группа по разработке Интернет (IETF) определила классический протокол IP над ATM (Classical IP Over ATM, C-IPOA) [CIP_ATM], протокол определения следующего транзитного участка (Next Hop Resolution Protocol, NHRP) [NHRP] и многопротокольную коммутацию на основе меток (Multi-Protocol Label Switching, MPLS) [MPLS_ARCH]. Для обеспечения того, чтобы сети общего пользования взаимодействовали между собой, поддерживая набор услуг, определенных в этой Рекомендации, и для обеспечения взаимодействия сетей общего пользования и частных сетей необходимо рекомендовать в качестве предпочтительного подхода транспортирование IP над ATM в сетях общего пользования.

Подход, принятый в этой Рекомендации, – это задание общих требований, ключевых услуг IP и определение того, какой подход IP над ATM является предпочтительным для каждой службы. Предпочтительным является использование одного и того же подхода для всех рассматриваемых услуг. Этот подход рекомендуется для всех идентифицированных услуг, использующих транспортирование IP над ATM в сетях общего пользования.

Источник

Рекомендация МСЭ-T Y.1310 утверждена 15 марта 2004 года 13-й Исследовательской комиссией МСЭ-T (2001–2004 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-T A.8.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

Всемирная ассамблея по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяет темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соответствие положениям данной Рекомендации является добровольным делом. Однако в Рекомендации могут содержаться определенные обязательные положения (для обеспечения, например, возможности взаимодействия или применимости), и тогда соответствие данной Рекомендации достигается в том случае, если выполняются все эти обязательные положения. Для выражения требований используются слова "shall" ("должен", "обязан") или некоторые другие обязывающие термины, такие как "must" ("должен"), а также их отрицательные эквиваленты. Использование таких слов не предполагает, что соответствие данной Рекомендации требуется от каждой стороны.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на то, что практическое применение или реализация этой Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для реализации этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т Y.1310

Транспортирование IP над ATM в сетях общего пользования

1 Область применения

Эта Рекомендация посвящена транспортированию услуг IP над ATM. Услуги IP в этой Рекомендации определены как услуги, предоставляемые на уровне IP. Услуги IP в этой Рекомендации не включают услуги на прикладном уровне (например, предоставление банковских услуг в сети).

В данной Рекомендации определен подход к IP над ATM для сетей общего пользования, применяющих технологию ATM, включая сети поставщиков услуг и транспортные сети, но не исключая, там, где это возможно, применение этого же подхода в сетях доступа, частных сетях и оконечных системах. Рассматриваемые подходы включают в себя классические IPOA, MPOA и MPLS. Эти подходы кратко описаны в Добавлении I.

2 Ссылки

Указанные ниже Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других источников, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации.

2.1 Нормативные ссылки

2.1.1 МСЭ-Т

[I.321] ITU-T Recommendation I.321 (1991), *B-ISDN protocol reference model and its application*.

[I.326] ITU-T Recommendation I.326 (2003), *Functional architecture of transport networks based on ATM.*

[I.356] ITU-T Recommendation I.356 (2000), *B-ISDN ATM layer cell transfer performance*.

[I.361] ITU-T Recommendation I.361 (1999), *B-ISDN ATM layer specification*.

[I.364] ITU-T Recommendation I.364 (1999), *Support of the broadband connectionless data bearer service by the B-ISDN*.

[I.371] ITU-T Recommendation I.371 (2004), *Traffic control and congestion control in B-ISDN*.

[I.432] ITU-T Recommendations I.432.1 (1999), I.432.2 (1999), I.432.3 (1999) and I.432.4 (1999), *B-ISDN user-network interface – Physical layer specification*.

[Q.2931] ITU-T Recommendation Q.2931 (1995), *Digital Subscriber Signalling System No. 2 – User-Network Interface (UNI) layer 3 specification for basic call/connection control*.

[Q.2941] ITU-T Recommendation Q.2941.2 (1999), *Digital Subscriber Signalling System No. 2 – Generic identifier transport extensions*.

[Y.1311.1] ITU-T Recommendation Y.1311.1 (2001), *Network-based IP-VPN over MPLS architecture*.

2.1.2 ISOC/IETF

[ATM_MULTI] IETF RFC 2684 (1999), Multiprotocol Encapsulation over ATM Adaptation Layer 5.

[ATM_VCID] IETF RFC 3038 (2001), VCID Notification over ATM Link for LDP.

[CIP_ATM] IETF RFC 2225 (1998), *Classical IP and ARP over ATM.*

[CONTROL_SER] IETF RFC 2211 (1997), *Specification of the Controlled-Load Network Element Service*.

[CR_LDP] IETF RFC 3212 (2002), *Constraint-Based LSP Setup using LDP*.

[DIFF_AF] IETF RFC 2597 (1999), *Assured Forwarding PHB Group*.

[DIFF_ARCH] IETF RFC 2475 (1998), *An Architecture for Differentiated Services*.

[DIFF_HEADER] IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.

[DIFF_EF] IETF RFC 2598 (1999), *An Expedited Forwarding PHB*.

[GUAR_SER] IETF RFC 2212 (1997), *Specification of Guaranteed Quality of Service*.

[IP_V4] IETF RFC 791 (1981), *Internet Protocol*.

[IP_V6] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification*.

[LDP] IETF RFC 3036 (2001), *LDP Specification*.

[MPLS_ARCH] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture*.

[MPLS_ATM] IETF RFC 3035 (2001), *MPLS using LDP and ATM VC Switching*.

[MPLS_DIFF] IETF RFC 3270 (2002), *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*.

[MPLS_ENCAPS] IETF RFC 3032 (2001), *MPLS Label Stack Encoding*.

[NHRP] IETF RFC 2332 (1998), *NBMA Next Hop Resolution Protocol (NHRP)*.

[RSVP_AGG] IETF RFC 3175 (2001), *Aggregation of RSVP for IPv4 and IPv6 Reservations*.

[RSVP_FUN] IETF RFC 2205 (1997), *Resource Reservation Protocol (RSVP) – Version 1 Functional Specification*.

[RSVP_REFR] IETF RFC 2961 (2001), *RSVP Refresh Overhead Reduction Extensions*.

[RSVP_TE] IETF RFC 3209 (2001), *RSVP-TE: Extensions to RSVP for LSP Tunnels*.

[TCP] IETF RFC 793 (1981), *Transmission Control Protocol*.

[UDP] IETF RFC 768 (1980), *User Datagram Protocol*.

2.1.3 Форум ATM

[ATM_MPOA] ATM Forum AF-MPOA-0087.000 (1997), *Multi-Protocol Over ATM Specification v1.0*.

2.2 Информативные ссылки

2.2.1 ISOC/IETF

[BGP_VPN] IETF RFC 2547 (1999), *BGP/MPLS VPNs*.

3 Термины и определения

В этом разделе в алфавитном порядке перечисляются акронимы ключевых терминов, используемых в данной Рекомендации, и даются ссылки на источники их определений. Обращайтесь к разделу 4 по поводу акронимов и к разделу 2 по поводу ссылок:

CR-LDP [CR_LDP]

DS [DIFF_ARCH]

DSCP [DIFF_ARCH]

FEC [MPLS_ARCH]

LIB [MPLS_ARCH]

LSR [MPLS_ARCH]

MPLS [MPLS_ARCH]

PHB [DIFF_ARCH]

RSVP [RSVP_FUN]

RSVP-TE [RSVP_TE]

VPN [BGP_VPN]

4 Сокращения и акронимы

В данной Рекомендации используются следующие сокращения:

AAL Уровень адаптации ATM

ABR Доступная скорость передачи

ABT Перенос блока ATM

AESA Адрес конечной системы ATM

ARP Протокол определения адреса

ATC Возможность переноса ATM

ATM Асинхронный режим передачи

ATMARP Протокол определения адреса ATM

BGP Протокол пограничного шлюза

BUS Широковещательный и неизвестный сервер

CE Окончание клиента

CE Оборудование клиента

C-IPOA Классический протокол IP над ATM

CLP Приоритет потери ячейки

CLS Услуга с управляемой нагрузкой

CoF Функция координации

CR-LDP Протокол LDP с маршрутизацией на основе ограничения

DBR Определенная скорость передачи

DS Дифференцированные услуги

DSCP Кодовая точка дифференцированных услуг

ER Точная синхронизация

ES Конечная система

FEC Класс эквивалентности по пересылке

FIB Информационная база пересылки

GFR	Гарантированная скорость кадров
GS	Гарантированная услуга
ILMI	Встроенный интерфейс местного административного управления
IP	Межсетевой протокол
IPOA	IP над ATM
IPSF	Функции услуги IP
IP-SSCS	Услуга конвергенции, специфическая для услуги IP
IS	Интегрированная услуга
ISP	Поставщик услуг IP
LANE	Эмуляция локальной сети
LDP	Протокол распространения меток
LEC	Клиент LANE
LECS	Сервер конфигурации LANE
LER	Граничный маршрутизатор на основе меток
LES	Сервер LANE
LIB	Информационная база меток
LIS	Логическая подсеть Интернет
LLC	Управление логическим звеном
LSP	Коммутируемый тракт на основе меток
LSR	Маршрутизатор с коммутацией на основе меток
MAC	Управление доступом к среде передачи
MBS	Максимальный размер пачки
MCR	Минимальная скорость ячеек
MPC	Клиент MPOA
MPLS	Многопротокольный коммутатор на основе меток
MPOA	Многопротокольная передача над ATM
MPS	Сервер MPOA
NAT	Преобразование сетевого адреса
NHC	Клиент NHRP
NHRP	Протокол определения следующего транзитного участка
NHS	Сервер NHRP
NNI	Интерфейс "сеть–сеть"
OSPF	Начальный выбор кратчайшего тракта
PCI	Информация управления протоколом
PCR	Пиковая скорость ячеек
PDR	Пиковая скорость данных
PE	Окончание поставщика
PHB	Режим для каждого транзитного участка
PIM	Многопунктовая передача, не зависящая от протокола
PPP	Протокол "точка-точка"
PSC	Составление расписания на каждый транзитный участок
QoS	Качество обслуживания
RSVP	Протокол резервирования ресурсов
RSVP-TE	Протокол резервирования ресурсов – Расчет трафика
SBR	Статистическая скорость передачи
SLA	Соглашение об уровне обслуживания

SNAP Точка присоединения подсети

SSCS Услуга управления, специфическая для службы

TCP Протокол управления передачей

TMN Сеть административного управления сетями электросвязи

UDP Протокол передачи данных пользователя

UNI Сетевой интерфейс пользователя

VPN Виртуальная частная сеть

VPN-ID Идентификатор VPN

xDSL Цифровой абонентский шлейф x-типа

5 Общие требования

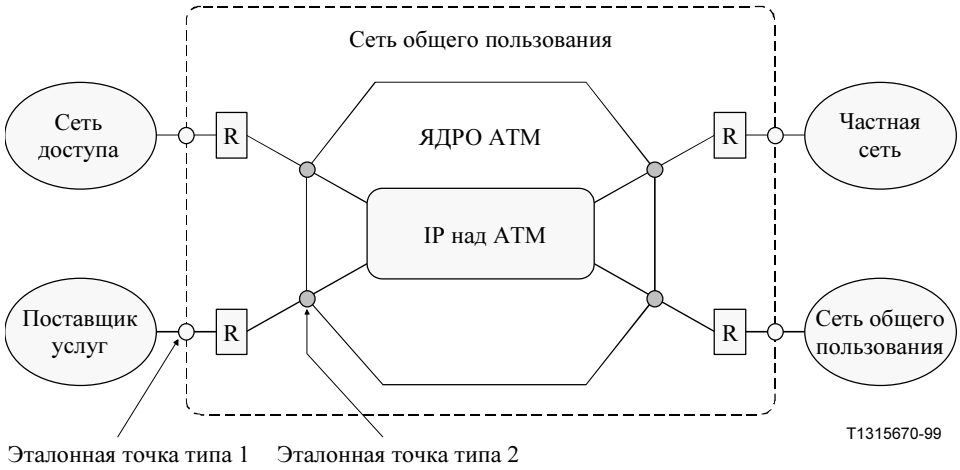
Данная Рекомендация определяет ряд общих требований к подходам к передаче IP над ATM. Такие требования применимы ко всем определяемым услугам IP. Обязательными общими требованиями являются следующие:

- Рекомендуемый подход должен быть независимым от поддерживаемой версии IP.
- Рекомендуемый подход должен иметь достаточную расширяемость для поддержки больших сетей. Вопросы, которые следует принимать во внимание относительно расширяемости, включают в себя:
  - использование значений идентификаторов виртуального канала (VCI) и виртуального тракта (VPI);
  - сложность вычисления маршрута на уровне 2 и уровне 3;
  - сложность механизма определения адреса;
  - нагрузку от передачи управляющих сообщений (например, частота установления и прекращения соединений ATM, частота сообщений сигнализации, относящихся к IP);
  - сложность механизма классификации пакетов, необходимого для поддержки QoS. Чем меньше число градаций в QoS (например, от назначения на поток IP до назначения на объединение потоков IP, на услугу, как в услуге Diffserv), тем проще механизм классификации пакетов.
- Рекомендованный подход должен включать в себя возможность эффективных и расширяемых решений для поддержки многопунктовой передачи IP над сетями ATM.
- Рекомендованный подход должен иметь достаточную устойчивость для поддержки больших сетей. Принимаемые во внимание вопросы должны включать в себя:
  - возможность поддержки систем восстановления.

6 Структурная архитектура

Структурная архитектура для поддержки услуг уровня IP над ATM определяется как включающая сетевую архитектуру и архитектуру протокола для поддержки требуемых услуг IP.

6.1 Сетевая архитектура



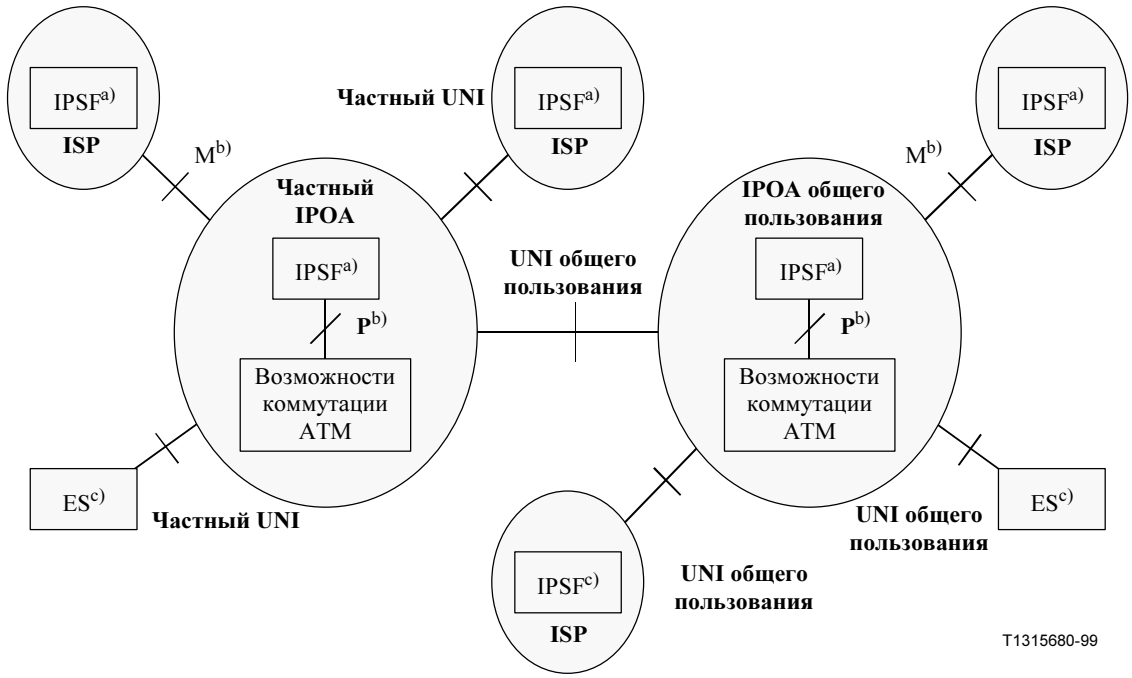
ПРИМЕЧАНИЕ 1. – Поставщики услуг Интернет также могут обеспечивать ядро ATM.

ПРИМЕЧАНИЕ 2. – Эталонные точки типов 1 и 2 могут быть стандартизованными эталонными точками, такими как интерфейс S, T сети ISDN или нестандартизованный интерфейс.

Рисунок 6-1/Y.1310 – Эталонная сетевая архитектура для IP над ATM

Эталонная сетевая структура для IP над ATM показана на рисунке 6-1. Эта конфигурация иллюстрирует возможные сценарии для поддержки услуг IP над ATM, определенные в этой Рекомендации. Пунктирный прямоугольник указывает сеть общего пользования, которую мы рассматриваем. Отметим, что сеть общего пользования в этой Рекомендации ограничена сетью, которая имеет ядро ATM. Блоки внутри пунктирного прямоугольника описывают общее устройство внутри сети общего пользования. Оно включает в себя ядро ATM, возможности IP над ATM и граничные маршрутизаторы. Ряд различных видов сетей описан вне пунктирного прямоугольника, при этом каждый определяет сценарий, в котором сеть общего пользования обеспечивает определенную услугу IP к определенному типу сети. С точки зрения сети общего пользования эти сети рассматриваются как абонентские сети.

На этом рисунке описываются два типа отдельных эталонных точек. Эталонная точка типа 1 является границей между сетью общего пользования и абонентскими сетями, а эталонная точка типа 2 является интерфейсом к IP над сетью ATM внутри сети общего пользования. Построение эталонной точки типа 1 может зависеть от средств абонентских сетей и определения услуг IP. В граничных маршрутизаторах могут потребоваться функции взаимодействия и/или функции адаптации. Данная Рекомендация главным образом рассматривает эталонную точку типа 2 и подход, принятый внутри сети общего пользования.



[a)] IPSF: Функции услуг IP.

[b)] P или M: на основе Рекомендации МСЭ-Т I.364.

[c)] ES: Конечная система имеет полный стек протокола IPOA.

Рисунок 6-2/Y.1310 – Эталонная конфигурация для услуг IP над ATM

На рисунке 6-2 показана эталонная конфигурация для услуг IP над сетями ATM общего пользования и частными сетями ATM. В частных сетях и сетях общего пользования IPOA обеспечение услуг IP реализуется с помощью возможностей коммутации ATM и Функций услуг IP (IPSF). В этом случае интерфейсы между возможностями коммутации ATM и IPSF должны быть определены в эталонных точках P или M [I.364]. Функции услуг IP (IPSF) являются теми функциями, которые необходимы для обеспечения передачи IP над ATM. Типичным примером функции IPSF является услуга определения адреса. В качестве конечной системы функция IPSF по существу является маршрутизатором с интерфейсом ATM.

Функция IPSF может быть реализована в том же оборудовании, в котором реализованы возможности коммутации ATM. В этом случае нет необходимости определять интерфейс в эталонной точке P. Функция IPSF возможности коммутации ATM могут быть также реализованы в отдельном оборудовании. В этом случае интерфейсы должны быть определены в эталонных точках M или P в зависимости от того, расположена ли функция IPSF вне или внутри базовой сети ATM.

Поставщики ISP и конечные системы (ES), находящиеся вне сетей ATM, могут быть подсоединены к частным сетям ATM или к сетям ATM общего пользования. Каждая система ES имеет полный стек протокола IPOA и подсоединяется с помощью частного интерфейса UNI для частной IPOA или с помощью интерфейса общего пользования UNI для IPOA общего пользования.

6.1.1 Взаимодействие сети и услуги

В сценарии сетевого взаимодействия информация управления протоколом IP (PCI) и данные полезной нагрузки прозрачно передаются через сеть ATM к другой сети на основе IP посредством функции взаимодействия (IWF) между двумя сетями. В типовом варианте IWF просто вкладывает пакет IP с использованием функции адаптации и прозрачно передает его к отдаленной функции IWF. Для текущего взаимодействия IP и ATM сетевое взаимодействие является типичным случаем, с ATM, обеспечивающей магистральную или базовую сеть для транспортировки протокола Интернет. В этом сценарии сеть ATM может рассматриваться как нижележащий транспорт для протокола уровня 3 (и выше).

Для случая взаимодействия услуг функция IWF завершает протокол IP и преобразует информацию PCI в информацию PCI сети ATM для функций переноса, управления и административного управления. Поскольку в общем случае не все функции могут быть поддержаны в одной или другой из сетей, сценарий взаимодействия услуг может быть способен только обеспечить "наиболее подходящее" преобразование между двумя различными технологиями. Однако это не должно приводить к каким-либо потерям данных пользователя, так как преобразование PCI в функции IWF взаимодействия услуг не затрагивает данные.

Рисунки 6-1 и 6-2 иллюстрируют сетевое взаимодействие, связанное с IP над ATM.

6.2 Архитектура протокола

6.2.1 Общее описание эталонной модели протокола IPOA

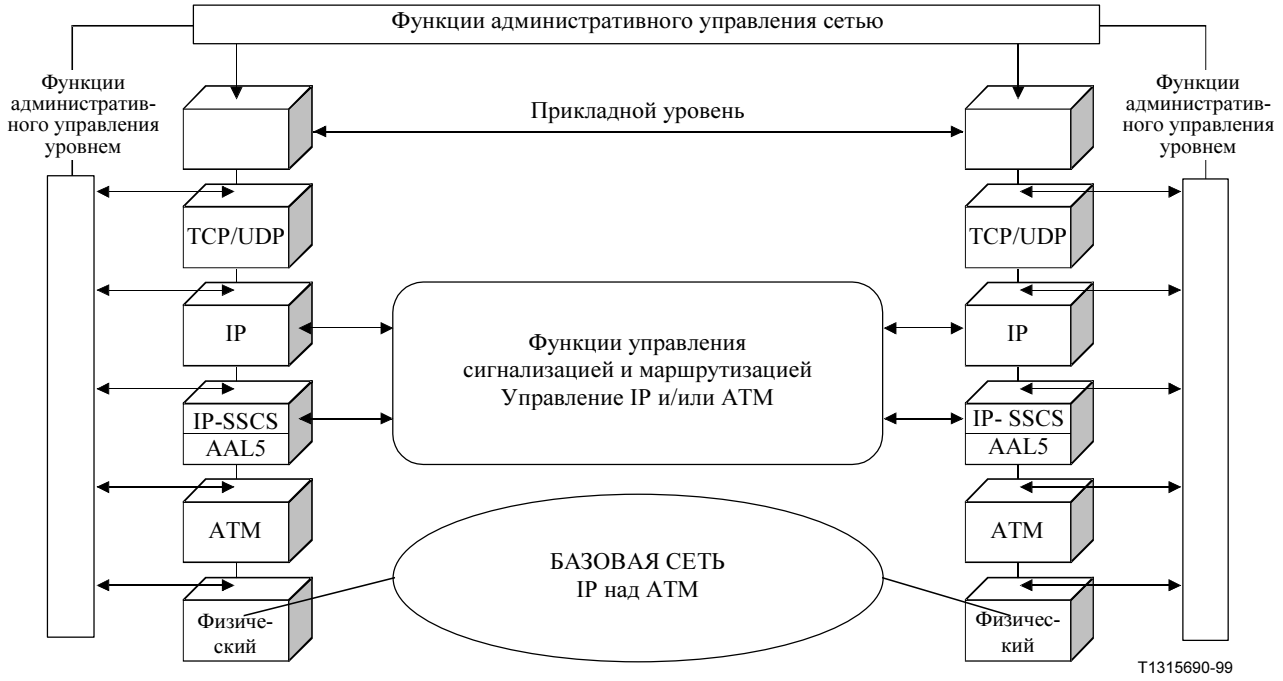


Рисунок 6-3/Y.1310 – Эталонная модель протокола для IP над ATM

На рисунке 6-3 показана обобщенная эталонная модель протокола для транспортирования IP над ATM в сетях общего пользования. Можно отметить, что концепции административного управления уровнем, административного управления сетью и управления сигнализацией и маршрутизацией эталонной модели нижележащего протокола расширены для включения функциональных блоков уровня 3 и выше. Следует отметить, что блоки, показанные на рисунке 6-3, соответствуют логическим представлениям функций и поэтому не означают или не ограничивают какую-либо конкретную реализацию сети.

Интерфейсы между функциональными блоками могут быть либо внутренней не стандартизированной связью между подуровнями, либо внешними стандартизированными протоколами. Каждый уровень в общей модели имеет свой, взаимодействующий с ним функциональный блок административного управления уровнем. Блоки административного управления уровнем отвечают за обеспечение административного управления и обработку информации управления протоколом (PCI) только для этого уровня. Обмен информацией между уровнями может происходить только через функцию сетевого административного управления. Это осуществляется через функцию координации (CoF) из сетевого административного управления.

Наличие всех функциональных блоков во всех сетевых приложениях IPOA не требуется. Таким образом, блоки можно рассматривать как основные "компоновочные блоки", которые позволяют реализовать любое заданное сетевое приложение IPOA. Однако для обеспечения устойчивого взаимодействия должны поддерживаться основные взаимосвязи и упорядочение между различными блоками.

6.2.2 Функциональное описание эталонной модели протокола IPOA

В этом подразделе описываются только функциональные блоки, относящиеся к IPOA, так как подробному описанию функций физического уровня, уровня ATM и уровня управления ATM посвящены другие Рекомендации [I.321], [I.326], [I.361], [I.432] и [Q.2931]. Блок прикладного уровня выходит за рамки этой Рекомендации.

6.2.2.1 Функции IP-SSCS/AAL5

IP-SSCS/AAL5 объединяет функции переноса, требуемые для отображения пакета IP в уровень AAL5. Функциональный блок IP-SSCS/AAL5 обеспечивает функции вложения и многопротокольного мультиплексирования, определяемые протоколом Управления уровнем звена/Точки присоединения подсети (LLC/SNAP), базирующимся на документе IEEE, как принято IETF в [ATM_MULTI].

6.2.2.2 Функции уровня IP

Функции уровня IP обеспечивают пересылку IP (доставка дейтаграмм IP) от источника к адресату через соединяющую систему. Пересылка IP является процессом получения пакета и применения процесса принятия решения с использованием очень малого заголовка о том, как обрабатывать пакет. Пакет может быть доставлен местному адресату или переслан во внешнюю область. Для трафика, который пересылается во внешнюю область, процесс пересылки IP определяет также, через какой интерфейс должен быть отправлен пакет, и, если необходимо, либо удаляет одно вложение уровня носителя информации и заменяет его другим, либо изменяет определенные поля во вложении уровня носителя информации.

Архитектура протокола IPOA должна быть независимой от версии IP. В настоящее время имеются две версии: IPv4 (версия 4 IP) и IPv6 (версия 6 IP). Функции уровня IP – это те функции, которые определены группой IETF в [IP_V4] и [IP_V6] для IPv4 и IPv6, соответственно.

Функция уровня IP не обеспечивает средств надежной связи. Здесь нет ни подтверждения "от конца до конца", ни подтверждения по транзитным участам.

Отметим, что функции уровня IP не следует менять для использования функций IP-SSCS/AAL5 над ATM.

6.2.2.3 Функции административного управления уровнем IP

Функция административного управления уровнем IP имеет две основные функции: адресацию и фрагментацию. Функции уровня IP используют адреса, переносимые в заголовке IP, для передачи дейтаграмм IP к их адресатам IP. Выбор тракта для передачи осуществляется путем использования блока функций сигнализации и маршрутизации. Функции уровня IP используют поля в заголовке IP для фрагментации и повторной сборки дейтаграмм IP, когда это необходимо для передачи.

Протокол IPv4 использует четыре основных ключевых механизма при обеспечении своих услуг: тип услуги, продолжительность существования, варианты выбора и контрольная сумма заголовка. Протокол IPv6 является новой версией протокола Интернет, разработанной в качестве преемника для IPv4. В основном изменения в IPv6 по сравнению с IPv4 имеют место в следующих категориях: расширенные возможности адресации, упрощение формата заголовка, улучшенная поддержка расширений и вариантов выбора, возможность присвоения меток потокам и возможности удостоверения подлинности и обеспечения секретности. Функция административного управления уровнем IP не обеспечивает коррекцию ошибок для данных, а только осуществляет проверку контрольной суммы. Отсутствует повторная передача. Нет управления потоком.

6.2.2.4 Функции транспортного уровня

Транспортный уровень включает в себя, соответственно, функции TCP типа, ориентированного на установление соединения, и функции UDP типа без установления соединения. Эти функции зависят от типа прикладной программы.

Функции TCP обеспечивают услугу надежного соединения между парами процессов. Функции TCP представляют собой те функци, которые определены группой IETF в [TCP]. Функции TCP включают в себя следующие возможности: перенос основных данных, обеспечение надежности, управление потоком, мультиплексирование, соединения, а также приоритет и безопасность.

Функции UDP обеспечивают перенос дейтаграмм. Функции UDP являются теми функциями, которые определены группой IETF в [UDP]. Протокол UDP является протоколом, ориентированным на транзакции, а доставка и защита путем повторной передачи не гарантируются.

Отметим, что функции транспортного уровня не следует изменять для использования функций уровня IP над ATM.

6.2.2.5 Функции прикладного уровня

Прикладной уровень и связанные с ним функциональные блоки административного управления уровнем включают такие приложения, характерные для пользователя или сети, как HTTP, FTP, TELNET и др. Описание функций прикладного уровня выходит за рамки этой Рекомендации.

Отметим, что в архитектуре протокола TCP/IP обычно принято, что функция прикладного уровня включает в себя функции сеансового уровня и уровня представления.

6.2.2.6 Функции сетевого административного управления

Функции сетевого административного управления зависят от конкретного сетевого приложения для IPOA. В общем случае они включают в себя функции TMN (сети административного управления сетями электросвязи), связанные с административным управлением при отказах, рабочими характеристиками, конфигурацией, безопасностью и т. д.

6.2.2.7 Функции управления сигнализацией и маршрутизацией

Эта функция включает в себя функциональные блоки сигнализации и маршрутизации в управлении IP и/или ATM. Управление и сигнализация IP охватывают различные аспекты управления IP, включая маршрутизацию. Управление ATM включает в себя сигнализацию и маршрутизацию ATM.

7 Услуги IP

В эту Рекомендацию включен спектр услуг IP в качестве средств для определения предпочтительного подхода к IP над ATM в сетях общего пользования. Первоначально рассматривается отображение QoS IP в услуги ATM и VPN. Дополнительные услуги оставлены для дальнейшего изучения.

7.1 Отображение QoS IP в ATM

7.1.1 Введение

Группой IETF созданы документы на два главных подхода для поддержки дифференциации QoS на уровне IP: парадигма (образец) Intserv, предназначенная для поддержки дифференциации QoS в каждом потоке IP, и парадигма Diffserv, предназначенная для поддержки дифференциации "необработанного" QoS для группировок потоков IP.

7.1.1.1 Парадигма IP Intserv

Парадигма Intserv базируется на явных запросах QoS по каждому потоку IP, переносимых с помощью протокола RSVP, и на управлении вдоль тракта потока допуском потока в маршрутизаторах, поддерживающих протокол RSVP. В парадигме Intserv определены две услуги: Гарантированная услуга – GS [GUAR_SER] и Услуга с управляемой нагрузкой – CLS [CONTROL_SER]. В GS для потока осуществляется управление максимальной задержкой в очереди. Для вычисления максимальной задержки, которая может иметь место для дейтаграммы, должна быть определена задержка тракта и добавлена к максимальной задержке очереди [GUAR_SER]. Услуга CLS не обеспечивает твердых гарантий задержки, но услуга, предоставляемая потоку, должна давать эффект, соизмеримый с тем, что поток испытывал бы в сети с малой нагрузкой, даже когда это не так [CONTROL_SER]. На практике для услуги CLS требуется пропускная способность, доступная в течение длительного времени.

Для обеих услуг требуется, чтобы характеристики потока были заданы с помощью спецификации маркерного блока [RSVP_FUN] и чтобы излишний трафик обрабатывался как наилучшая попытка.

7.1.1.2 Парадигма Diffserv IP

Модель Diffserv IETF основывается на концепции "Режимы для каждого транзитного участка" (PHB) [DIFF_HEADER] и [DIFF_ARCH]. PHB Diffserv определяются набором режимов пересылки, которых придерживается каждый местный маршрутизатор вдоль тракта. Группа IETF определила два главных режима PHB таким образом:

- Ускоренная пересылка (EF) PHB [DIFF_EF]:

  EF-PHB характеризуется конфигурируемой величиной пропускной способности, на которую не влияет другой трафик, использующий звено. EF-PHB может использоваться для организации услуги "от конца до конца", для которой требуются малые потери, малая задержка и малое изменение задержки при прохождении через области Diffserv.

- Группа PHB гарантированной пересылки (AF) [DIFF_AF]:

  Группа AF-PHB характеризуется четырьмя классами AF, и каждому классу AF выделяется определенное количество таких ресурсов пересылки, как объем накопительного устройства (буфера) и величина пропускной способности в узле Diffserv. Внутри каждого класса AF пакеты IP маркируются с помощью одного из трех возможных уменьшающихся значений приоритета отбрасывания. В случае перегрузки уменьшающийся приоритет отбрасывания пакета определяет относительную важность пакета внутри класса AF. Однако стандартизованные взаимосвязи между относительными характеристиками четырех классов AF отсутствуют. Группу AF-PHB можно использовать для обеспечения того, чтобы гарантировать с высокой степенью вероятности скорость информации, на которую "подписался" абонент.

7.1.2 Сетевая модель для поддержки услуг IP с обеспечением QoS

В этом подразделе описывается сетевая модель для поддержки услуг IP с обеспечением QoS в сетях IPOA. В структуре IETF качество QoS "от конца до конца" обеспечивается путем связывания областей Intserv на границе сети с областями Diffserv в ядре сети. Предлагаемая здесь сетевая модель, однако, рассматривает дополнительные возможности. Более того, в этом случае всегда предполагается, что уровень звена должен быть ATM.

7.1.2.1 Описание модели

Возможные сетевые модели для поддержки услуг IP с обеспечением качества QoS показаны на рисунках 7-1, 7-2 и 7-3. В каждом случае затененная область указывает используемую активную функцию.

Случай 1 – Intserv над сетями ATM

В этой модели связь между двумя областями сетей Intserv поддерживается через базовые сети IPOA. Устройства IPOA в базовых сетях могут обеспечивать возможности как Intserv, так и Diffserv. Однако для поддержки интегрированных услуг "от конца до конца" будут активированы только функциональные возможности Intserv устройств IPOA. Оба соглашения об уровне обслуживания (SLA 1 и SLA 2) требуют, чтобы выполнялись требования для услуги Intserv.

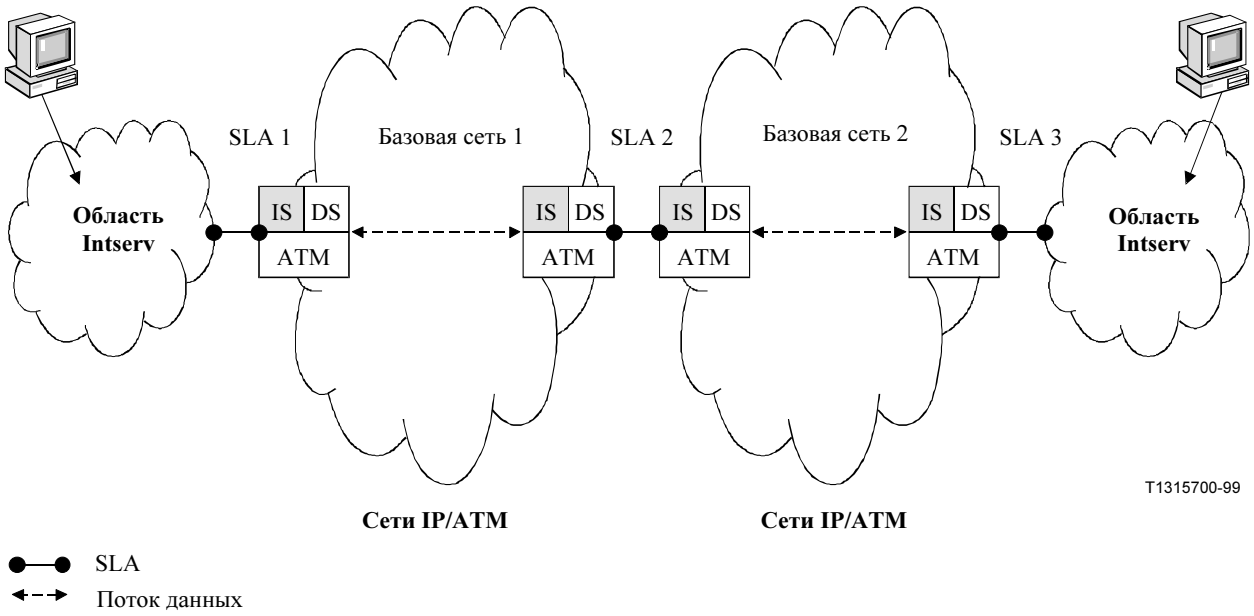


Рисунок 7-1/Y.1310 – Сетевая модель для поддержки Intserv над ATM

Случай 2 – Diffserv над сетями ATM

В этой модели связь между двумя областями сетей Diffserv поддерживается над базовыми сетями IPOA. Устройства IPOA в базовых сетях могут обеспечивать возможности как Intserv, так и Diffserv. Однако для поддержки дифференцированных услуг "от конца до конца" будут активированы только функциональные возможности Diffserv устройств IPOA. Оба соглашения об уровне обслуживания (SLA 1 и SLA 2) требуют, чтобы выполнялись требования для услуги Diffserv.

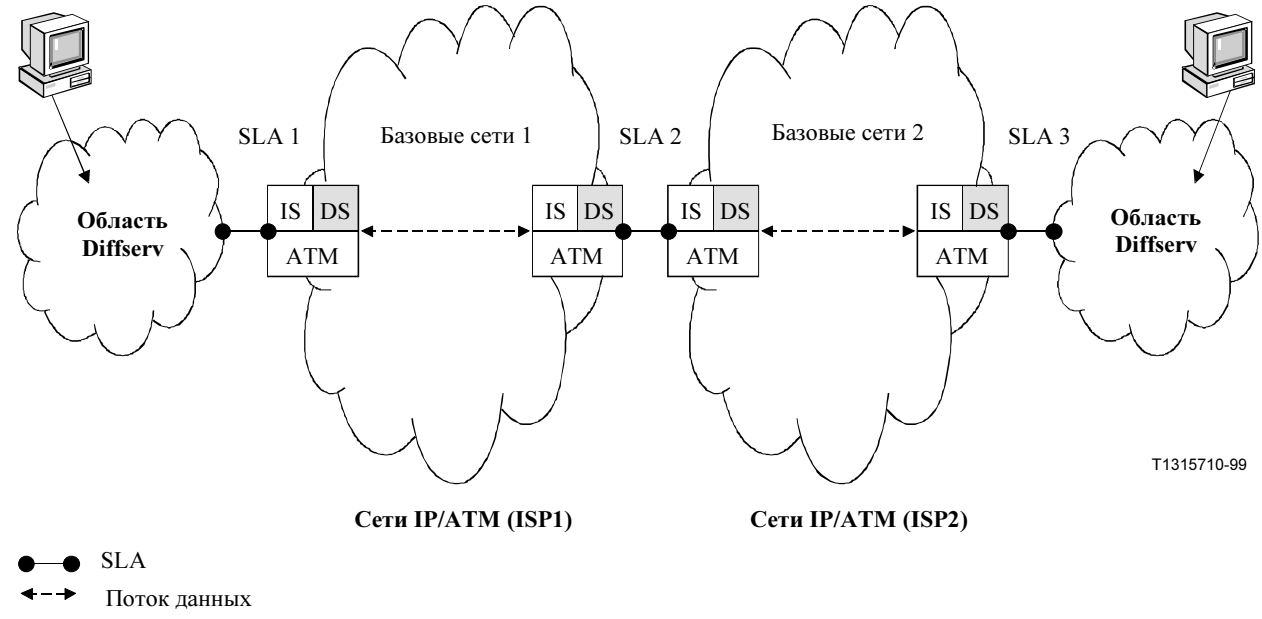


Рисунок 7-2/Y.1310 – Сетевая модель для поддержки Diffserv над ATM

Случай 3 – Intserv через области Diffserv над сетями ATM

В этой модели связь между двумя областями сетей Intserv поддерживается над базовыми сетями IPOA. В базовых сетях IPOA некоторые области могут обеспечивать только Diffserv, а другие могут обеспечивать возможности как Intserv, так и Diffserv. В этом случае Intserv может быть прозрачно транспортирована только над областями Diffserv. В этом случае имеются два типа соглашения по уровню обслуживания.

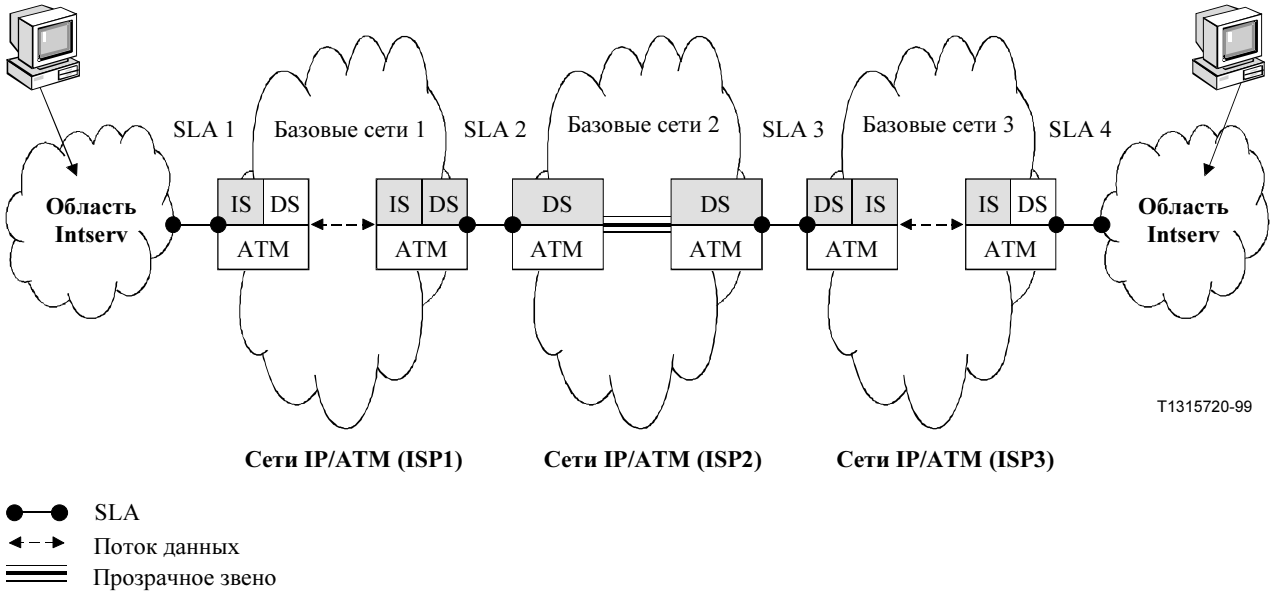


Рисунок 7-3/Y.1310 – Сетевая модель для поддержки Intserv через области Diffserv над ATM

7.1.3 Перечень функций отображения услуг

Функции отображения услуг не зависят от архитектуры окружающей сети, а зависят только от способа, которым поддерживается QoS в IP и ATM на обеих сторонах интерфейса, где требуется отображение. В соответствии с этим на рисунке 7-4 показан необходимый набор возможных отображений услуг IP в услуги ATM рассматриваемой структурной архитектуры (относится к разделу 6).

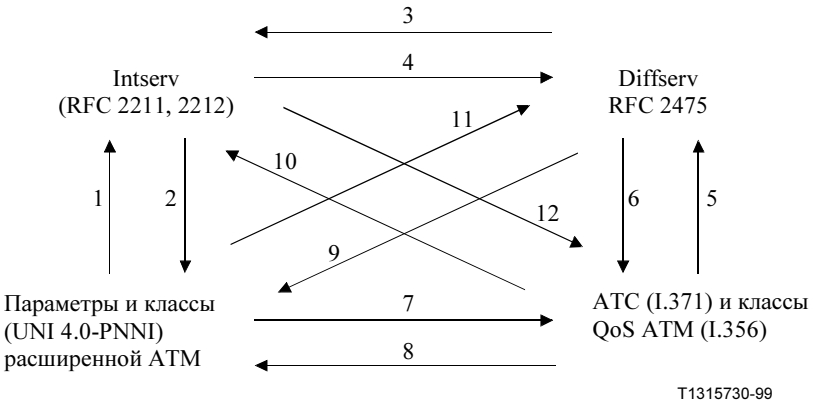


Рисунок 7-4/Y.1310 – Перечень функций отображения услуг

Из всех этих отображений в этой Рекомендации используются только отображения 6 и 12. Отметим, что в этом случае на выходе этой части ATM нет необходимости в функции отображения типа 5 или 10, поскольку в сети IP назначения поддержка QoS полностью основывается на информации уровня IP, которая прозрачно переносится частью ATM. Отображения 5 и 10 могут потребоваться в случае

естественного трафика ATM, который должен пересекать чистую сеть IP или достигать ее, и это оставлено для дальнейшего изучения.

Отображения 3 и 4 имеют отношение только к области IP и являются объектом деятельности внутри группы IETF, тогда как все отображения, начинающиеся/заканчивающиеся расширенными параметрами ATM и классами QoS (поддерживаемыми в частных сетях ATM), являются частью работы Форума ATM.

7.1.4 Отображение интегрированных услуг IP в услуги ATM

Вопрос об отображении Intserv в ATM возникает всякий раз, когда поток IP, запрашивающий гарантированные услуги (GS) [GUAR_SER] или услуги с управляемой нагрузкой (CLS) [CONTROL_SER], должен быть поддержан с помощью соединения ATM, связывающего два маршрутизатора с возможностями Intserv, и он является независимым от конкретного подхода к поддержке IP над ATM.

Предусмотрены два различных вида отображения: отображение "один в один" и отображение "многие в один".

7.1.4.1 Отображение "один в один"

Отображение "один в один" имеет место, когда одиночное соединение ATM полностью поддерживает только одиночный поток IP. А именно, процесс отображения представляет собой выбор услуги ATM (то есть ATC и связанного с ним класса QoS), которая может удовлетворять обязательства по QoS услуги IP (GS или CLS), и в этом плане возможны несколько отображений. В более общем смысле, однако, процесс отображения можно дополнительно рассматривать как способ получения доступа к дополнительной информации уровня ATM, относящейся к характеристикам переносимого потока, так что сеть ATM входящего потока может использовать эту информацию для эффективного переноса соединения (например, мультиплексировать его с другими). В этом смысле можно определить сравнительную эффективность всех возможных отображений, и некоторые отображения оказываются лучше других.

7.1.4.2 Отображение "многие в один"

Отображение "многие в один" имеет место, когда одиночное соединение ATM может переносить более одного потока. В этом случае процесс отображения представляет собой выбор услуги ATM, которая может удовлетворять обязательства по QoS для набора потоков IP. Поскольку потоки IP обычно начинаются и заканчиваются асинхронно, то это преобразование можно рассматривать как процесс группирования, в котором на основе характеристик уровней IP потоков (например, маркерный блок и запрашиваемое QoS) принимается решение о возможности переноса потока вместе с другими потоками в уже существующем соединении ATM (все еще удовлетворяя ограничения QoS потока IP) или о необходимости повторного согласования параметров соединения.

Правила принятия такого решения выходят за рамки этой Рекомендации.

7.1.4.3 Отображение гарантированной услуги (GS) в ATM

Для выполнения этих отображений ATM не требует каких-либо расширений. Однако выбранная схема отображения должна удовлетворять следующим требованиям:

- Выбранная возможность ATC должна быть возможностью, способной выполнять требования по задержке.
- Выбранная возможность ATC должна быть возможностью, способной резервировать для потока некоторую часть пропускной способности.

В Добавлении II содержатся предложения руководящих указаний для осуществления отображений.

7.1.4.4 Отображение услуги с управляемой нагрузкой (CLS) в ATM

Для выполнения этих отображений ATM не требует каких-либо расширений. В Добавлении II содержатся предложения руководящих указаний для осуществления отображений. Однако выбранная схема отображения должна удовлетворять следующему требованию:

- Выбранная возможность ATC должна быть способна резервировать для потока некоторую величину пропускной способности.

7.1.4.5 Влияние на административное управление трафиком ATM

Для дальнейшего изучения.

7.1.4.6 Влияние на сигнализацию ATM

Для дальнейшего изучения.

7.1.4.7 Влияние на маршрутизацию ATM

Для дальнейшего изучения.

7.1.5 Отображение дифференцированных услуг IP в услуги ATM

В модели дифференцированных услуг (Diffserv) IP используется концепция "Режим для каждого транзитного участка" (PHB) [DIFF_HEADER] и [DIFF_ARCH] для обеспечения услуг IP на основе QoS.

PHB можно использовать в качестве важного фактора для определения услуги IP в области Diffserv. Однако PHB сам по себе не связан с услугами QoS IP "от конца до конца". Таким образом, отображение между Diffserv и ATM должно основываться на услугах IP и на услугах ATM. Более точно услуги IP могут быть определены посредством объединения реализаций PHB с характеристиками трафика на границах областей Diffserv, а услуги ATM могут быть определены посредством объединения возможностей переноса ATM [I.371] с классами QoS [I.356].

7.1.5.1 Отображение услуги

Для предоставления услуг клиентам поставщики Diffserv должны объединять реализации PHB с регуляторами трафика и с правилами предоставления услуг. Концепция PHB не обращается к ATM. Таким образом, отображение режимов PHB в Возможность переноса ATM не представляется подходящей. Поэтому вместо этого можно рассматривать отображение конкретной дифференцированной услуги в услугу ATM. Отображение услуги из Diffserv в ATM четко обеспечивается путем согласования между двумя сетевыми поставщиками, основанного на определении рассматриваемых услуг IP.

Поэтому отображение услуги зависит от политики поставщиков услуги и может меняться среди различных поставщиков услуг. Некоторые примеры возможного отображения услуги приведены в Добавлении II.

К отображению услуги применяется следующее требование:

- Не требуется связывание минимальной скорости ячеек на каждое соединение с поддержкой некоторых PHB Diffserv над ATM.

Также имеется потребность в рассмотрении качественной и относительной услуги. Решения оставлены для дальнейшего изучения.

7.1.5.2 Влияние на административное управление трафиком ATM

Для дальнейшего изучения.

7.1.5.3 Влияние на сигнализацию ATM

Для дальнейшего изучения.

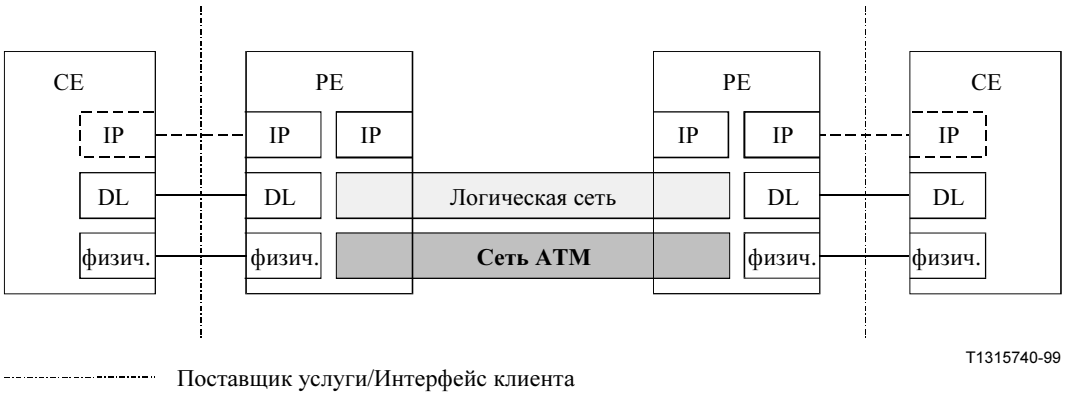
7.1.5.4 Влияние на маршрутизацию ATM

Для дальнейшего изучения.

7.2 Виртуальные частные сети IP (IP-VPN)

7.2.1 Сфера применения IP-VPN

Сеть IP-VPN в этой Рекомендации определяется как эмуляция средств частной территориальной сети на основе IP, предоставляемая через расширяемую несущую транспортную сеть ATM. На рисунке 7-5 показана структура сети IP-VPN в этой Рекомендации. Пример метода демонстрации поддержки IP-VPN в сети общего пользования MPLS/ATM приведен в Добавлении IV.



CE Оборудование клиента
PE Маршрутизатор окончания поставщика

Рисунок 7-5/Y.1310 – Сетевая модель для IP-VPN

Сайт (объект) клиента подсоединяется к сети поставщика услуги через оборудование клиента (CE). Это может быть одиночный главный компьютер, коммутатор или маршрутизатор IP. С другой стороны, сеть поставщика услуг соединяет сайт клиента с маршрутизатором окончания поставщика (PE). Когда оборудование CE является маршрутизатором, мы можем задавать конфигурацию таким образом, чтобы этот маршрутизатор являлся равноправным объектом по маршрутизации для присоединенного маршрутизатора PE, но не равноправным объектом по маршрутизации для оборудования CE на другом сайте. Маршрутизаторы на разных сайтах не осуществляют прямой обмен маршрутной информацией между собой. Эта структура позволяет просто осуществлять поддержку очень больших сетей VPN, в то время как маршрутная стратегия для каждого отдельного сайта значительно упрощается. Считается, что эта способность должна быть важна для поставщиков услуг расширенного переноса, которые обеспечивают внешнее предоставление услуги IP-VPN.

7.2.2 Определение услуги IP-VPN

Услуга IP-VPN дает возможность сайтам клиентов формировать группы, доступ IP к которым и из которых ограничен. Эта группа называется IP-VPN. Конкретный сайт может быть членом одной или более IP-VPN. Сайты членов конкретной IP-VPN могут осуществлять связь между собой, используя протокол IP. Конкретные сайты могут иметь дополнительные возможности, которые позволяют им получать доступ к сайтам вне группы и/или быть доступными для сайтов, находящихся вне группы.

7.2.3 Требования к услуге IP-VPN

7.2.3.1 Требования к плоскости пользователя

7.2.3.1.1 Поддержка непрозрачного транспортирования пакетов

Непрозрачное транспортирование пакетов позволяет клиентам IP-VPN использовать независимый адрес IP внутри своей сети. Сеть поставщика услуг требует наличия возможности направлять пакеты IP в зависимости от членства в VPN, даже если они используют перекрывающиеся пространства адресов. Могут потребоваться функции для идентификации сети VPN [например, использование идентификатора VPN (VPN-ID)] и/или функция для дифференциации пересылки пакетов для каждой VPN.

7.2.3.1.2 Поддержка безопасности данных

Безопасность данных обеспечивает клиентам IP-VPN определенный уровень защищенной связи между сайтами членов IP-VPN. Сеть поставщика услуг требует обеспечения исключения необходимости отслеживания данных, ошибочного направления или ошибочного вставления несвязанных пакетов. Могут потребоваться функции фильтрации, функции шифрования и функции для проверки полномочий.

7.2.3.1.3 Поддержка QoS

Качество QoS позволяет клиентам IP-VPN подписываться на определенный уровень гарантий качества связи между сайтами членов IP-VPN. Сеть поставщика услуг требует наличия возможностей

поддержки произвольных категорий услуг QoS, как это она делает для обеспечения общих услуг IP. Эти возможности подробно описываются в подразделе 7.1.

7.2.3.2 Требования к плоскости управления

7.2.3.2.1 Поддержка ресурсов логической сети сигнализации

Поставщик услуг должен обладать возможностью сигнализировать о своих сетевых ресурсах с целью поддержки транспортирования пакетов IP для клиентов IP-VPN.

7.2.3.2.2 Поддержка транспортирования идентификаторов VPN (VPN-ID)

Для дальнейшего изучения.

7.2.3.2.3 Поддержка маршрутизации для каждой VPN

Для дальнейшего изучения.

7.2.3.3 Требования к плоскости административного управления

7.2.3.3.1 Совместимый идентификатор VPN (VPN-ID)

Если сеть IP-VPN обеспечивается несколькими поставщиками услуг, то сети каждого поставщика может потребоваться правильное различение трафика IP-VPN. В этом случае для уменьшения обработки граничными маршрутизаторами необходимо общепринятое определение идентификатора VPN (VPN-ID).

7.2.3.3.2 Поддержка административного управления членством в IP-VPN

Поставщику услуг следует иметь возможность управлять информацией о членстве в VPN, например, о том, к какой сети принадлежит определенный сайт клиента. Этой возможности должна быть присуща достаточная степень совместимости, чтобы она могла использоваться разными поставщиками услуг при обеспечении IP-VPN несколькими поставщиками услуг.

7.2.3.3.3 Поддержка конфигурации ресурсов логической сети

Сеть поставщика услуг должна обладать возможностью конфигурирования своих сетевых ресурсов с целью поддержки транспортирования пакетов IP для клиентов IP-VPN. Этой возможности должна быть присуща достаточная степень совместимости для использования различными поставщиками услуг с целью поддержки IP-VPN, расположенных в нескольких сетях.

8 Предпочтительное сетевое решение

8.1 Рекомендуемый подход

С учетом общих требований, описанных в разделе 5, а также услуг, описанных в разделе 7, рекомендуется, чтобы в качестве единственного предпочтительного подхода для сетей общего пользования была принята коммутация MPLS [MPLS_ARCH]. Коммутация MPLS поддерживает все идентифицированные услуги. Признано, что MPLS не обеспечивает значительных преимуществ по сравнению с должным образом разработанной классической IP над ATM (как описано в I.1.2) для поддержки услуги Intserv. Однако коммутация MPLS, предоставляя не меньшие возможности для поддержки Intserv, чем классическая IPOA, в то же время обеспечивает поддержку всех других услуг.

Дополнительные мотивации для выбора MPLS в качестве единственного предпочтительного подхода включают в себя:

8.1.1 Малые сети в сравнении с большими сетями

Хорошо известно, что MPOA очень хорошо подходит для малых сетей, но имеет ограничения, когда применяется к большим сетям. Эта Рекомендация предназначена для поставщиков услуг и поэтому ориентирована на большие сети. MPLS была разработана для выполнения требований к большим сетям в части гибкости, расширяемости и управляемости.

8.1.2 ATM в сравнении с сетью переноса, не являющейся ATM

В то время как центральным вопросом этой Рекомендации является транспортирование IP над ATM, полезно понимать, что в больших сетях может использоваться несколько различных технологий переноса, включая ATM. При более широких масштабах полезно выбирать технологию, которая является оптимальной для транспортирования IP над ATM, но в то же самое время является оптимальной для транспортирования IP над другими технологиями уровня звена. MPLS является, вероятно, единственной возможной стратегией, которая охватывает эту широкую сферу.

8.1.3 Статическое управление в сравнении с динамическим

С точки зрения маршрутизации архитектура MPLS дает возможность иметь задаваемую маршрутизацию и динамическую маршрутизацию и в то же время позволяет выбирать между ними. Выбор подхода является задачей сетевого оператора.

8.1.4 Управление ATM в сравнении с управлением, не являющимся ATM, в IPOA

Предпочтительно иметь общее управление, которое является независимым от уровня звена. Однако управление ATM может, тем не менее, еще использоваться на тех же самых коммутаторах.

8.1.5 Расчет трафика услуг IP

ATM обладает наиболее полным известным к настоящему времени набором функциональных возможностей для расчета трафика. Однако наложенные модели IP над ATM могут неэффективно использовать все возможности ATM и иметь тенденцию к ограничению расширяемости из-за хорошо известной проблемы "n в квадрате", когда обеспечивается полное занятие постоянных виртуальных соединений (PVC). MPLS заимствует некоторые из возможностей технологии ATM в части QoS, маршрутизации, административного управления ресурсами и других свойств, добавляя понятие явной маршрутизации для содействия отображению запроса трафика в сетевые топологии. Таким образом, использование MPLS предоставляет новые и более многочисленные свойства административного управления трафиком, чем прежде.

8.1.6 Построение с использованием существующих инвестиций

При наличии существующих инвестиций в ATM и другие технологии имеется явная необходимость в переносе трафика IP над ATM и другими протоколами уровня звена, и поэтому необходима унифицированная коммутационная технология. В сегодняшних транспортных сетях, где аппаратные средства ATM используются в режиме предоставления их для переноса трафика IP, коммутация MPLS видится как логическое развитие C-IPOA в ближайшем будущем, поскольку явную маршрутизацию можно строить на основе существующих обеспечиваемых PVC, а архитектура является достаточно гибкой для приспособления к потенциальному развитию сетей.

8.1.7 Поддержка услуг VPN

Главным преимуществом протокола MPLS является его способность обеспечивать услуги, ориентированные на установление соединения, над маршрутизацией без установления соединения или над явной маршрутизацией, что делает MPLS идеальным протоколом для динамического образования туннелей. Не существует уникального способа построения сетей VPN на основе MPLS, что делает более трудным сравнение с другими технологиями IPOA.

8.1.8 Аспекты QoS

Имеется явное усиление свойств (синергия) между дифференцированными услугами IP и MPLS, поскольку обе технологии развиваются в ответ на требования поставщиков, присущие их разработкам. Метка с ее расширенной семантикой может нести информацию, относящуюся к Diffserv, а тракты LSP "от конца до конца" могут гарантировать устойчивость механизмов QoS внутри конкретной области MPLS благодаря соответствующим механизмам резервирования ресурсов.

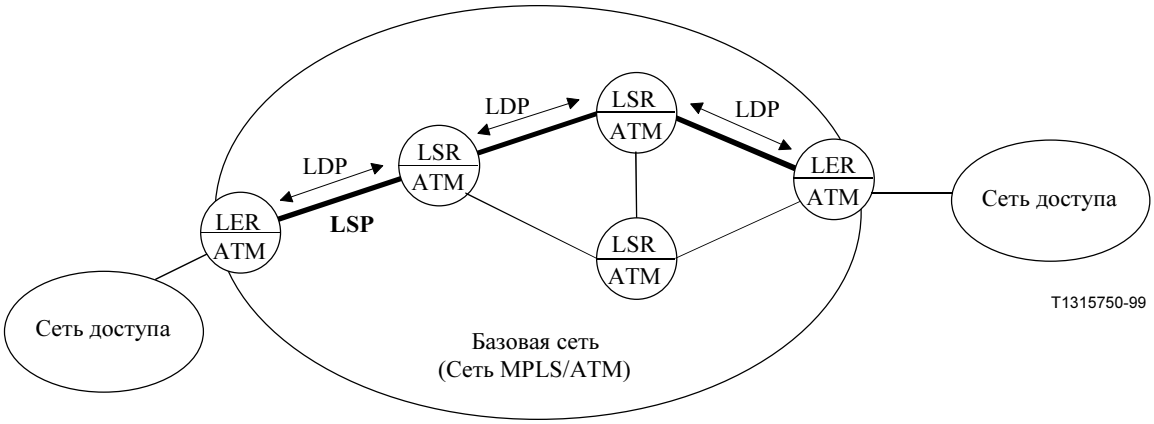
8.2 Структура для MPLS над ATM в сетях общего пользования

8.2.1 Архитектурная модель

На рисунке 8-1 показана общая сетевая модель базовой сети MPLS/ATM. Сеть общего пользования реализуется как MPLS с сетями ATM, которые составлены из граничных маршрутизаторов на основе меток (LER) и маршрутизаторов с коммутацией на основе меток (LSR). Маршрутизатор LER располагается на границе сети MPLS в качестве поддерживающего MPLS маршрутизатора

входа/выхода. Граница сети MPLS может совпадать или не совпадать с границей базовой сети ATM. Маршрутизатор LER выполняет полный объем функций уровня 3 и связывание меток, основанное на LIB (Информационная база меток), формируемой действующим протоколом LDP. Маршрутизатор LER соединен с внутренними маршрутизаторами LSR. Маршрутизатор LSR выполняет обмен меток, основанный на LIB. Тракт LSP (коммутируемый тракт на основе меток) между маршрутизаторами LER или между LER и LSR устанавливается с использованием протокола LDP, [LDP] и [MPLS_ENCAPS].

На основе этой простой модели для клиентов IP могут быть эффективно и гибко обеспечены такие различные услуги IP, как IP QoS (Intserv и Diffserv) и IP-VPN через различные сети доступа (такие, как чистая ATM, ретрансляция кадров, xDSL, чистая IP и т. д., включая область, не поддерживающую коммутацию MPLS).



LDP Протокол распространения меток
LER Граничный маршрутизатор на основе меток
LSP Коммутируемый тракт на основе меток
LSR Маршрутизатор с коммутацией по меткам

Рисунок 8-1/Y.1310 – Сетевая модель базовой сети MPLS/ATM

8.2.2 Протокол управления для MPLS над ATM

- *Режим объявления о метках*

  В коммутации MPLS над сетями ATM в качестве метки используются идентификаторы VCI и VPI ATM. Объявление в сети о метке может быть выполнено двумя следующими способами:

  – с помощью явного протокола распространения меток, такого как LDP;

  – путем дополнительного вложения в другие сообщения управления, например, RSVP, BGP и т. д.

  В сети можно использовать как явное распространение меток, так и дополнительное вложение. Однако в этой Рекомендации для распространения меток по принципу "один транзитный участок за другим" рекомендуется протокол LDP.

- *Режим распространения меток*

  Если используется LDP, то метки могут быть распространены в сети среди маршрутизаторов LSR следующими двумя путями:

  – в режиме входящего потока без запроса;

  – в режиме запроса входящего потока.

  В этой Рекомендации в качества режима объявления о метках в MPLS над сетями ATM рекомендуется использовать режим запроса входящего потока по следующим причинам:

  – В режиме запроса входящего потока значения VPI/VCI используются, если только они были запрошены.

  – Режим запроса входящего потока больше похож на обычную сигнализацию, такую как сигнализация ATM, и поэтому он может взаимодействовать с существующими сетями общего пользования.

- *Режим управления коммутируемым трактом на основе меток (LSP)*

  Управление метками для LSP осуществляется следующими двумя способами:

  – Упорядоченное управление LSP, когда маршрутизатор LSR только связывает метку с конкретным классом FEC, если он является выходным маршрутизатором LSR для этого FEC, или если он уже принял связывание метки с этим классом FEC от своего следующего транзитного участка для этого класса FEC.

  – Режим независимого управления LSP, когда каждый маршрутизатор LSR, отметив опознание конкретного класса FEC, принимает независимое решение о связывании метки с этим классом FEC и о распространении этого связывания своим равноправным объектам по распространению меток.

  В этой Рекомендации рекомендуется режим упорядоченного управления по следующим причинам:

  – Поскольку каждый маршрутизатор LSR независимо назначает метки эквивалентным классам по пересылке IP, то в режиме независимого управления может оказаться, что различные маршрутизаторы LSR могут принимать несовместимые решения. Для режима упорядоченного управления это не имеет места.

  – По сравнению с режимом независимого управления в режиме упорядоченного управления такие ресурсы, как идентификаторы VCI/VPI, могут быть использованы более эффективно.

Для удовлетворения требований поставщика услуг к расчету трафика возможны два подхода к сигнализации:

1) MPLS/LDP с помощью CR-LDP [CR_LDP].

2) MPLS/LDP с помощью расширений RSVP-TE [RSVP_TE, RSVP_REFR, RSVP_AGG].

Поставщики услуг могут выбрать для использования подход, основываясь на своих собственных конкретных требованиях, на потребностях в услуге и опыте развертывания.

Критерии для этого выбора могут включать в себя функциональные возможности, вопросы совместимости и уровень сложности эксплуатации и административного управления.

Отметим, что пока еще отсутствуют установочные протоколы для полной поддержки обеспечения качества обслуживания "от конца до конца".

Добавление I

Подходы для IP над ATM

I.1 Классический протокол IP над ATM

Классические протоколы IP и ARP над ATM (C-IPOA) определяются в [CIP_ATM]. На рисунке I.1 представлено функциональное описание классического протокола IP над ATM.

C-IPOA определяет механизм для сетей ATM для переноса многих типов протоколов, включая IP, над транспортом ATM с использованием адаптации AAL5. В этом подходе может быть выбран один из двух типов вложения, когда устанавливается виртуальный канал VC ATM [постоянное виртуальное соединение (PVC) или коммутируемое виртуальное соединение (SVC)]. Они представляют собой вложение управления уровня звена/точки присоединения подсети (Вложение LLC/SNAP) согласно документу IEEE 802.2 или мультиплексирование на основе канала VC. Вложение LLC/SNAP является форматом пакета по умолчанию для дейтаграмм IP. В мультиплексировании LLC/SNAP различия в протоколах вносятся с использованием идентификатора (ID) протокола LLC/SNAP в каждом сообщении уровня 3, в этом случае – IP. Для уменьшения заголовка вложения можно использовать механизм мультиплексирования на основе канала VC. Протокол, подлежащий использованию в канале VC, определяется во время установления канала VC и сохраняется в течение времени соединения VC. Этот механизм, однако, не предоставляет возможности многопротокольного вложения, доступной с помощью вложения LLC/SNAP.

Самого по себе многопротокольного вложения, несмотря на его необходимость, не достаточно для обеспечения маршрутизации и пересылки дейтаграмм IP над транспортами ATM. Требуется преобразование адресов IP в естественные адреса ATM. В [CIP_ATM] определена классическая

модель IP над ATM. На рисунке I.1 показаны функциональные блоки для построения плоскостей сигнализации, административного управления и пользователя, а также потоки сообщений между главным компьютером IP и сервером ATMARP. Сеть ATM разделяется на дискретные административные и функциональные области, называемые Логическими подсетями IP (LIS). Каждая подсеть LIS функционирует независимо от других подсетей LIS. Все члены (главные компьютеры и маршрутизаторы) внутри подсети LIS имеют одни и те же префиксы адреса сети/подсети IP и маски адресов. В этой модели развертывание ATM используется как прямое замещение территориальных сетей, поддерживающих IP. Таким образом, тип протокола определения адреса (ARP) в сервере, называемый ATMARP, нужен для преобразования целевых адресов IP в целевые адреса ATM внутри одной подсети LIS. Адреса ATM могут быть либо адресами E.164, либо адресами конечной системы ATM (AESA). Функции ATMARP остаются внутри одной подсети LIS.

В классической модели главные компьютеры осуществляют связь между собой непосредственно через ATM внутри той же самой подсети LIS, используя услугу ATMARP для преобразования целевого адреса. Связь вне местной подсети LIS предоставляется через маршрутизатор IP. Использование протокола определения следующего транзитного участка (NHRP) для осуществления связи между подсетями LIS является расширением классической модели (см. рисунки I.1 и I.1.1). ATMARP является протоколом "клиент–сервер" типа "запрос–ответ". Клиенты ATMARP (главные компьютеры ATM) должны быть конфигурированы или должны узнать через встроенный интерфейс местного административного управления (ILMI) адрес ATM сервера ATMARP перед тем, как станет возможной операция "запрос–ответ". Перед операцией "запрос–ответ" ATMARP клиенту ATMARP необходимо установить SVC или использовать предварительно конфигурированный PVC, чтобы зарегистрироваться у сервера ATMARP (шаг 1 на рисунке I.1). Во время операции ATMARP клиент посылает сообщение ATMARP-запрос к серверу через это соединение виртуального канала (VCC). Адреса источников IP и ATM включаются в сообщение запроса вместе с целевым адресом IP. Ожидается, что сервер ответит соответствующим целевым адресом ATM в сообщении ATMARP-Ответ, если адрес IP может быть определен. В противном случае будет возвращено сообщение ATMARP-NAK (шаги со 2 по 6 на рисунке I.1). После определении целевого адреса ATM связь между двумя главными компьютерами может начинаться путем установления соединения VCC ATM и выполнения переноса данных (шаги 7 и 8 на рисунке I.1). Каждый клиент ATMARP поддерживает таблицу, содержащую записи всех определенных адресов. Клиент должен обновлять эту таблицу с помощью своего сервера в течение периода старения, используя процедуры регистрации. Классической моделью также обеспечивается инверсный процесс определения адреса (в ATMARP), и он используется для определения целевого адреса IP для заданного целевого адреса ATM члена подсети LIS.

I.1.1 Протокол определения следующего транзитного участка (NHRP)

Протокол NHRP, заданный в [NHRP], расширяет классическую модель путем обеспечения связи между многими подсетями LIS. В протоколе NHRP станция источника (главный компьютер или маршрутизатор), известная как Клиент следующего транзитного участка (NHC), намеревающаяся осуществлять связь со станцией назначения, известной как клиент NHC назначения (главный компьютер или маршрутизатор), использует протокол запроса и ответа NHRP для получения адреса ATM станции назначения. Запрос NHRP проходит через ряд серверов NHRP (NHS), следуя по тракту, определенному используемым протоколом маршрутизации, пока он не достигнет сервера NHS, обслуживающего станцию назначения, после чего ответ NHRP возвращается к станции источника. Затем устанавливается "сокращенный тракт" между станциями источника и назначения через прямой виртуальный канал ATM. Если станция назначения находится внутри сети ATM, обслуживаемой с помощью сервера NHS, то доступ к ней будет происходить непосредственно через этот сокращенный тракт. Если она находится вне сети или в случае любого другого ограничительного алгоритма, к ней через сервер NHS будет подсоединен выходной маршрутизатор, "ближайший" к станции назначения. Если главный компьютер станции назначения не обслуживается какими-либо серверами NHS, то обратно будет послан отрицательный ответ NHRP, а маршрутизация к станции назначения будет осуществляться в соответствии с нормальным протоколом маршрутизации.

I.1.2 Использование местного сокращенного тракта ATM

Протокол NHRP оказывается особенно полезным, когда должны быть поддержаны требующие качества QoS потоки IP (например, потоки GS или CLS Intserv), поскольку это устраняет транзит IP на каждой границе подсети LIS. Однако это требует введения в сеть выделенных серверов и добавляет сложность другого протокола вопроса – ответа. Более того, задержка установления сокращенного соединения, поддерживающего поток, может быть значительной.

Другим путем, позволяющим избегать многократных транзитов IP без каких-либо дополнений классической модели, является создание местных сокращенных трактов ATM на каждой границе подсети LIS [51]. Это требует, чтобы граничные маршрутизаторы LIS были гибридными устройствами IP/ATM, то есть не только маршрутизаторами с интерфейсами ATM, но и интегрированными коммутаторами IP/ATM, способными к совместному использованию некоторой информации между двумя уровнями.

Более точно основными функциями, которые должны выполнять эти устройства, являются:

- составление и ведение карты взаимосвязей между потоками IP и соединениями ATM, поддерживающими их как для входящего, так и для исходящего направлений;
- создание местного сокращенного тракта ATM на основе этой карты взаимосвязей.

Затраты усилий на составление такой карты взаимосвязей, однако, являются оправданными для длительно существующих, требующих качества QoS потоков IP. Наиболее простым примером являются потоки через сигнализацию RSVP услуг GS или CLS Intserv, требующих некоторого качества QoS.

Отметим, что если гибридное устройство отвечает за установку соединений ATM в ответ на прием сообщений сигнализации RSVP, то составление карты взаимосвязей для исходящей стороны является простым и не требует использования какого-либо конкретного стандартного механизма: все, что необходимо, – это внутренняя связь между компонентами IP и ATM устройства. Для входящей стороны, напротив, гибридное устройство нуждается в использовании некоторой информации, которую можно переносить в сообщениях сигнализации ATM. В частности, новая Рекомендация МСЭ-Т Q.2941.2 [Q.2941] определяет возможность сигнализации DSS2 переносить среди прочего идентификаторы, связанные с Интернет (то есть идентификатор сеанса IPv4 или IPv6, который определяет поток IP). Эта информация, конечно, доступна, если в аналогичном гибридном устройстве исходящего потока приняты меры для заполнения вышеупомянутых полей в сообщениях сигнализации ATM.

В приведенной ниже таблице перечислены условия и способы использования гибридным устройством карты взаимосвязей и создания местного сокращенного тракта ATM в зависимости от типа взаимосвязи между потоками IP и соединениями ATM (один поток IP на каждое соединение ATM или множество потоков IP на единственное соединение ATM).

В случае 1 получаются максимальные преимущества: поток IP поддерживается через несколько подсетей LIS с помощью создания цепи соединений ATM, но благодаря возможности пересылки "на лету" достигаемое качество QoS идентично качеству, которое было бы получено в прямом соединении ATM.

В случае 3 (случай объединения VC) преимущество состоит только в исключении обработки уровня IP, но пересылка "на лету" не является достижимой. В двух других случаях обработка IP все еще нужна, и на этом транзитном участке не достигается улучшение характеристик.

	Входящая взаимосвязь	**Исходящая взаимосвязь**	**Потребность в обработке IP**	**Разрешение пересылки "на лету"**
1	Один в один	Один в один	Нет	Да
2	Многие в один	Один в один	Да	Нет
3	Один в один	Многие в один	Нет	Нет
4	Многие в один	Многие в один	Да	Нет

В таком сценарии каждое гибридное устройство отвечает за тип взаимосвязи для исходящей стороны согласно заданной политике. Например, оно может решить всегда устанавливать отдельное соединение ATM для каждого потока GS IP и таким образом иметь взаимосвязь "один в один", и всегда объединять потоки CLS в одном соединении ATM, чтобы сэкономить идентификаторы VCI. Конечно, крайне желательным является скоординированный выбор политик гибридных устройств одной административной области.

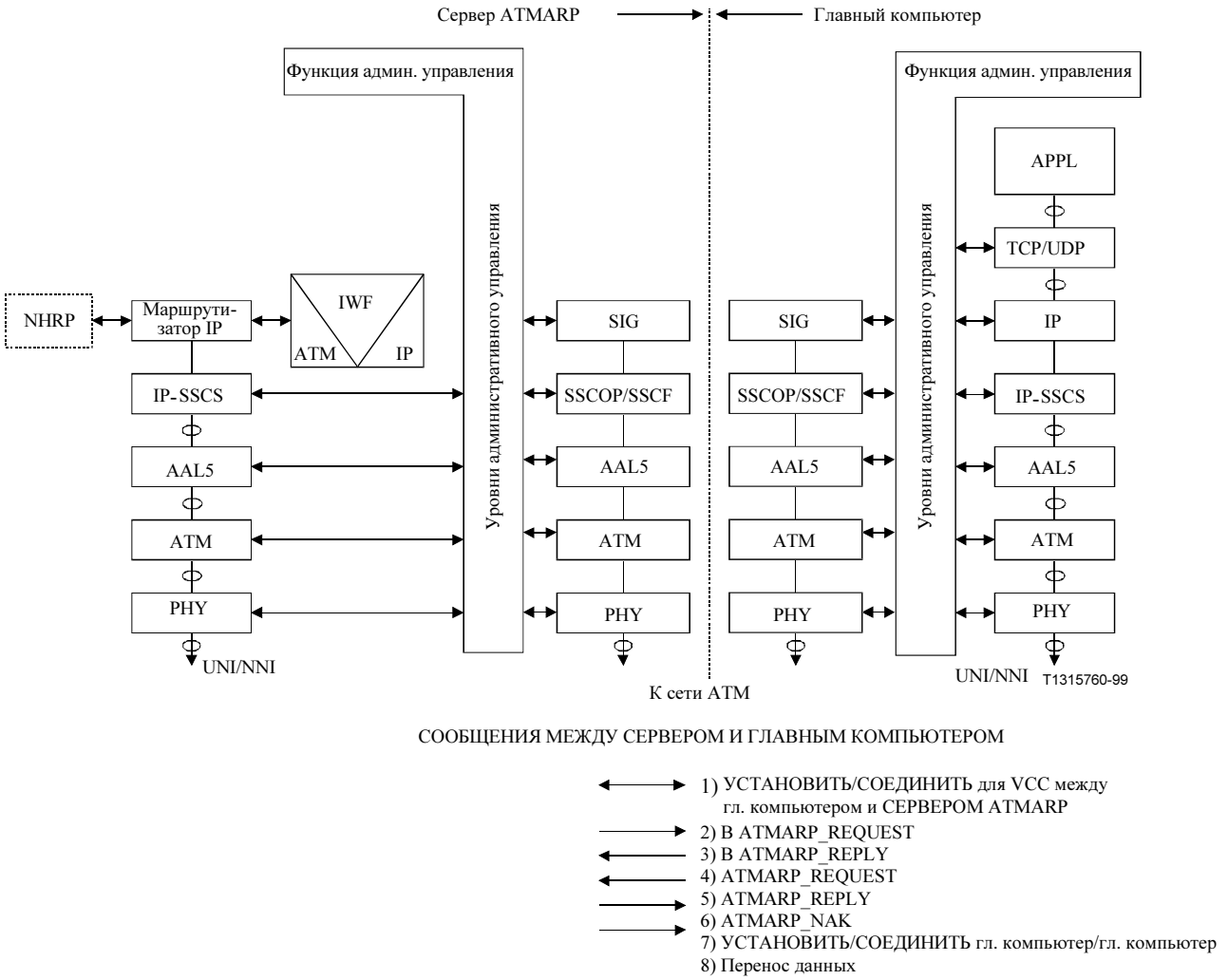


Рисунок I.1/Y.1310 – Функциональное описание классических IP и ARP над ATM

I.2 Многократный протокол над ATM (MPOA)

В [ATM_MPOA] задана общая конфигурация мостового соединения и маршрутизации для транспортирования многократных протоколов (например, пакетов IP) над прямыми соединениями ATM VCC. Технология объединяет Эмуляцию локальной сети (LANE) с технологией Протокола определения следующего транзитного участка (NHRP) для создания парадигмы (образца) сокращенного тракта ATM. На рисунке I.2 приведены функциональные блоки MPOA, показывающие взаимосвязи между плоскостями управления, административного управления и передачи данных. Компонентами MPOA на этом рисунке являются: NHS, NHC, MPC, MPS и LANE. Их функции объясняются ниже.

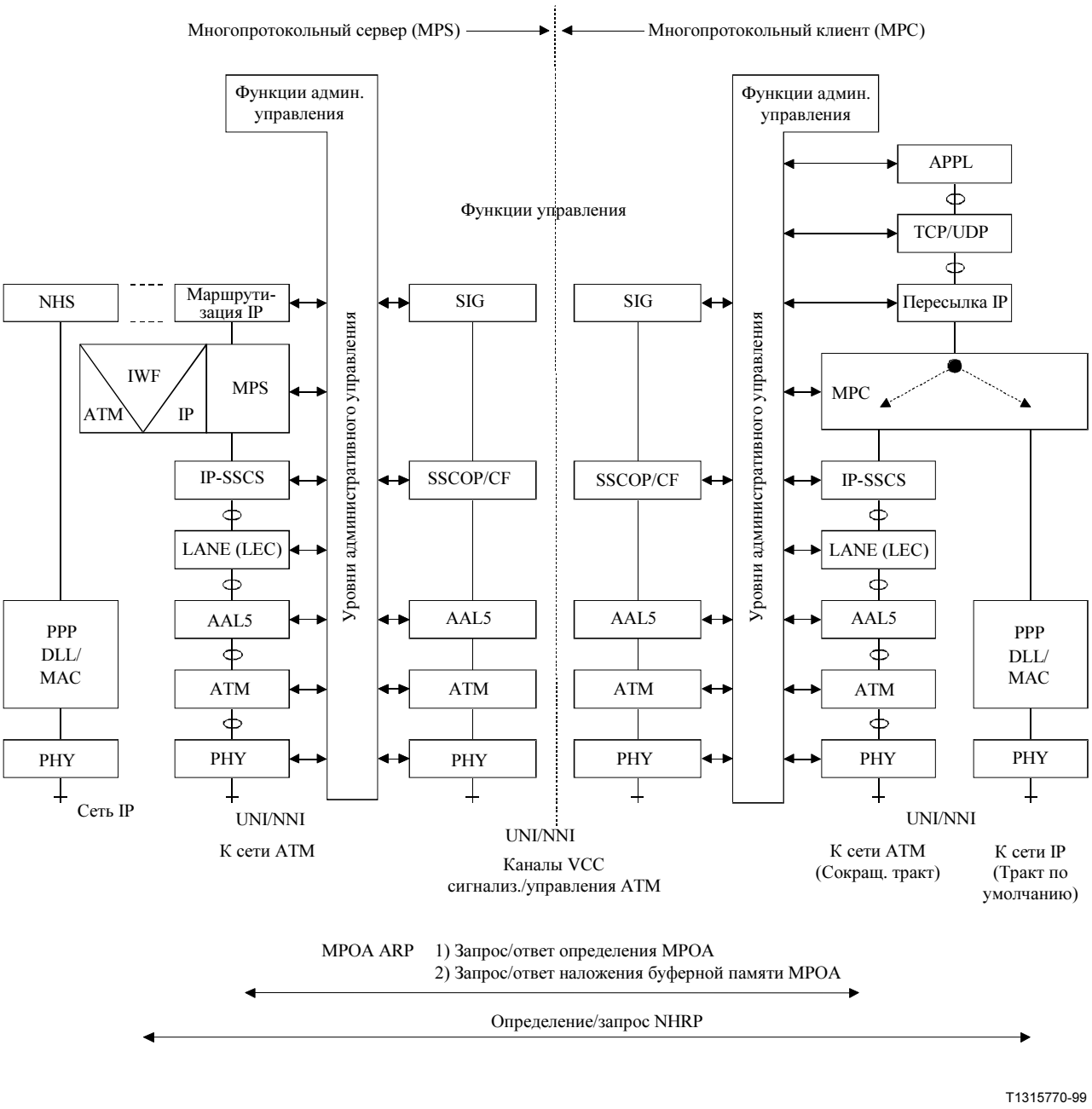


Рисунок I.2/Y.1310 – Функциональное описание MPOA

LANE образует составную часть протокола MPOA. LANE разделяет большую сеть ATM на много областей, каждая из которых может эмулироваться как сегмент LAN. LANE задает набор протоколов для пользователей сети LAN для осуществления связи между ними внутри конфигурации ATM. Эти пользователи LANE могут быть конечными системами, присоединенными к ATM, или пользователями, присоединенными к сети LAN. Услуги IP поддерживаются внутри этой среды LAN. Протокол LANE действует между уровнем AAL5 ATM и сетевым уровнем и уровнем LLC. LANE имеет четыре главных компонента LANE: Клиент LANE (LEC), Сервер LANE (LES), Широковещательный и неизвестный сервер (BUS) и Сервер конфигурации LANE (LECS). Клиент LEC (например, станция LAN) получает информацию о конфигурации от сервера LECS и регистрируется с его помощью. Сервер LES преобразует адреса MAC клиентов LANE в их соответствующие адреса ATM. Функции протокола определения адреса (LE_ARP) подобны тем, которые используются протоколом IP ARP. В установившемся режиме для соединения этих клиентов с целью переноса данных используются прямые каналы данных VC ATM. Сервер BUS распределяет данные клиентов перед тем, как завершается определение адреса и устанавливаются тракты данных, или когда клиент

не знает, какой прямой канал данных VC использовать. Пакеты IP переносятся путем вложения LLC/SNAP или посредством мультиплексирования канала VC, как описано ранее.

Другим составным компонентом MPOA является протокол NHRP, который описывается в I.1. Модель классической IP над ATM имеет ограничение, заключающееся в возможности обслуживания единственной подсети LIS. Протокол NHRP расширяет эту возможность, разрешая "сокращенные тракты" через многие подсети LIS внутри сети ATM.

I.3 Многопротокольная коммутация на основе меток (MPLS)

Многопротокольная коммутация на основе меток MPLS была разработана для достижения быстрой и эффективной пересылки данных для маршрутизаторов Интернет [MPLS_ARCH]. Хотя она архитектурно ориентирована на применение многих протоколов, до сих пор коммутация MPLS главным образом используется для протокола IP. В конфигурации IP без установления соединений маршрутизаторы IP обычно выполняют пересылку данных IP каждой дейтаграммы вдоль прокладываемого тракта к пункту назначения, основываясь на решении о маршрутизации по каждому транзитному участку. Это принятие решения о следующем транзитном участке включает в себя проверку заголовка пакета IP маршрутизатором с целью назначения пакету класса эквивалентности по пересылке (FEC) и отображение класса FEC на следующий транзитный участок для определения тем самым направления тракта маршрутизации. Этот процесс можно сделать более простым и более эффективным с помощью процесса MPLS. При коммутации MPLS назначение пакету IP класса FEC выполняется один раз с помощью входного маршрутизатора с коммутацией на основе меток (LSR), а класс FEC представляется и кодируется в виде метки постоянной длины. Метка присоединяется к заголовку IP пакета. Заголовок больше не используется последующими маршрутизаторами для пересылки пакета. Маршрутизаторы LSR вдоль коммутируемого тракта на основе меток (LSP) используют метку для индексирования таблицы, которая указывает следующий транзитный участок и новую метку. Старые метки заменяются новыми метками по мере того, как пакет проходит маршрутизаторы LSR вдоль тракта LSP в направлении пункта назначения. Метки имеют местное значение, и их кодирование задается в [MPLS_ENCAPS]. Метки определяют режим всей пересылки пакета. Эта пересылка осуществляется в режиме "транзитный участок за транзитным участком" и включает в себя выбор для пакета следующего транзитного участка и операцию, которую необходимо выполнить над меткой, например, удаление или замещение. При нормальных ситуациях тракт LSP соответствует тому же самому тракту, какой был бы определен таким обычным протоколом маршрутизации IP, как OSPF. Коммутация MPLS может выполняться над любым транспортом уровня звена, таким как ATM, ретрансляция кадров или протокол "точка-точка" (PPP). На рисунке I.3 показана структура протокола коммутации MPLS, функционирующего над ATM. Главными элементами протокола MPLS, показанными на этом рисунке, являются LDP, LIB и FIB. Протокол LDP описывается в следующем параграфе. Информационная база меток (LIB) и Информационная база пересылки (FIB) являются информационными базами данных, которые содержат информацию привязки меток и информацию пересылки в метках [MPLS_ARCH], [MPLS_ENCAPS] и [LDP].

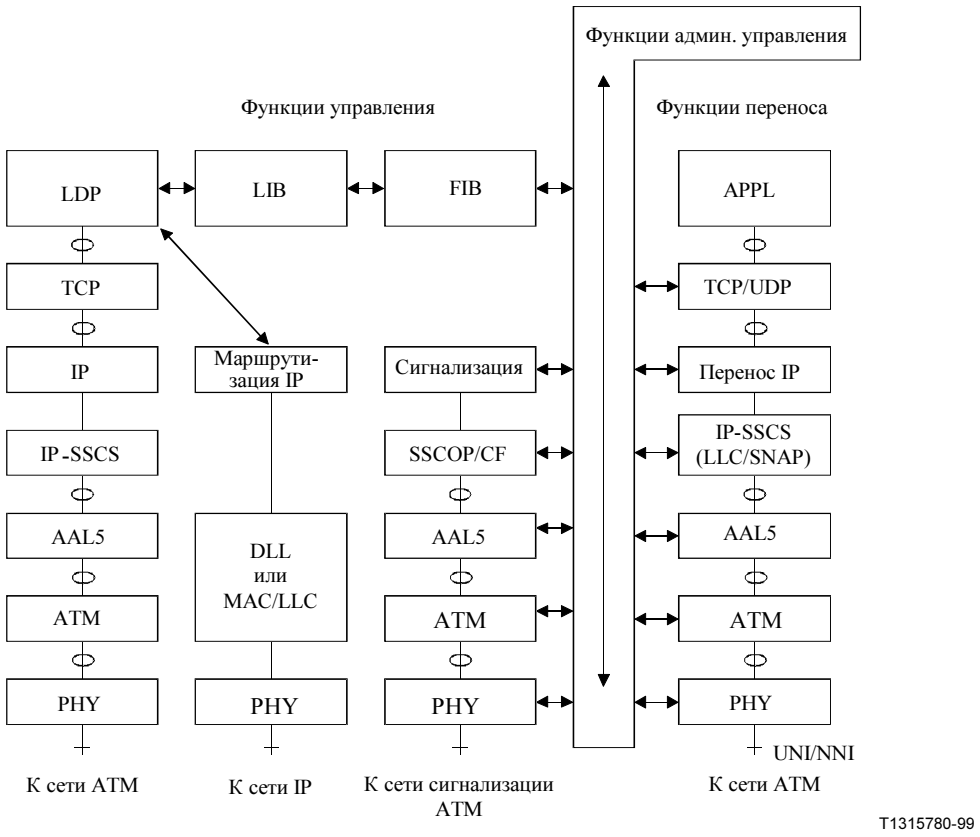


Рисунок I.3/Y.1310 – Функциональное описание MPLS

ПРИМЕЧАНИЕ. – Использование сигнализации ATM требуется только для взаимодействия MPLS с B-ISDN.

Для обеспечения содержательного определения и общего распознавания меток MPLS внутри области MPLS требуется протокол сигнализации MPLS. Он может быть реализован на основе использования Протокола распространения меток (LDP) [LDP], который представляет собой стандартизованный механизм сигнализации MPLS для назначения и распространения меток. Как показано на рисунке I.3, коммутация MPLS может использовать протокол LDP для построения информационной базы LIB, получающей информацию от используемого протокола маршрутизации, а также устанавливать соединения LSP между соответствующими входными и выходными конечными точками LSR. Протокол LDP главным образом работает на надежных соединениях TCP (за исключением установленного ниже процесса развертывания, в котором используется UDP). Протокол LDP имеет четыре рабочие фазы:

- Развертывание: Объявление и поддержка присутствия маршрутизаторов LSR в сети.
- Сеанс: Установление и поддержка сеансов между равноправными объектами LDP.
- Объявление: Назначение и распространение меток.
- Уведомление: Для сообщения об ошибках.

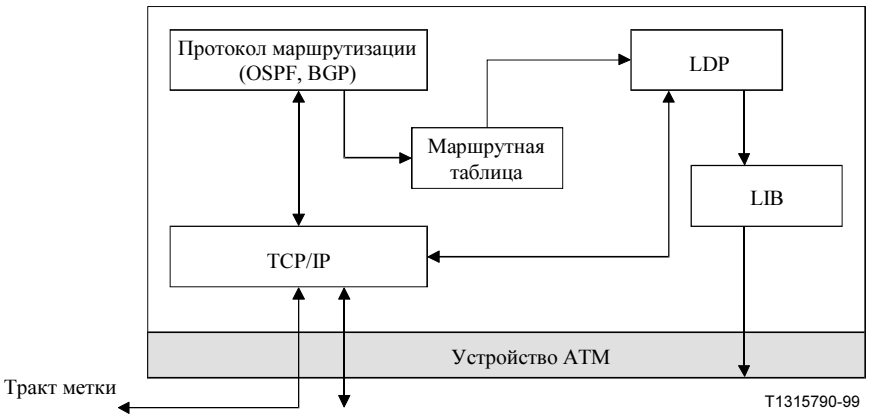
Когда производится распространение меток, могут быть выбраны определенные механизмы или режимы. Например, механизм распространения меток "по запросу входящего потока", где метки распространяются с помощью маршрутизатора LSR входящего потока в ответ на явный запрос от его маршрутизатора LSR исходящего потока. Другие механизмы распределения подробно приведены в [LDP]. Отличная от протокола LDP предварительная конфигурация или такие существующие протоколы IP, как RSVP и BGP, могут быть расширены для поддержки распространения меток [MPLS_ARCH].

Маршрутизация на основе ограничения (CR) является механизмом, который используется для предоставления возможности расчета трафика (TE) и характеристик показателей качества QoS внутри сети. Эти требования можно выполнить путем расширения "нормального" протокола LDP [LDP] или протокола резервирования ресурсов (RSVP) [RSVP_FUN] для поддержки коммутируемых трактов на основе меток, установленных на основе ограничений (CR_LSP). Оба расширенных протокола CR-LDP [CR_LDP] и RSVP-TE [RSVP_TE] обеспечивают следующие возможности CR:

- *Явная маршрутизация (ER):* Явный маршрут может быть определен как перечень узлов и установлен с помощью сигнализации. Он может не проходить по обычным трактам LSP, которые основаны на маршрутизации IP. Поддерживаются как ограниченные, так и свободные маршруты ER.
- *Описание характеристик трафика:* Характеристики трафика тракта CR-LSP могут быть определены с использованием параметров трафика [CR_LDP, RSVP_TE].
- *Предварительное занятие тракта:* Во время установления тракта сигнализация обеспечивает этот новый тракт возможностью предварительно занимать существующие тракты CR-LSP, если такая необходимость будет возникать. Может ли новый тракт предварительно занять существующий тракт, зависит от приоритета установки нового тракта и от приоритета удержания существующего тракта. Эта способность позволяет сетевому оператору удовлетворять сетевой политике и инженерным требованиям в пределах имеющихся ресурсов.
- *Закрепление маршрута:* Этот вариант выбора позволяет сделать постоянным сегмент свободного маршрута ER.
- *Классы ресурсов:* Сетевые ресурсы могут быть разделены сетевым оператором по "классам ресурсов".

Коммутаторы ATM могут быть использованы в качестве узлов коммутации на основе меток. Когда коммутатор ATM используется в качестве узла коммутации на основе меток или маршрутизатора (называемого ATM-LSR), метка, на основании которой принимаются решения по пересылке, переносится в поле VCI/VPI заголовка ячейки ATM. Для поддержки коммутации на основе меток маршрутизатор ATM-LSR должен поддерживать такой протокол управления и сигнализации для коммутации на основе меток, как LDP, и участвовать в таком протоколе маршрутизации сетевого уровня, как OSPF. Маршрутизация и адресация, характерные для ATM, не нужны. Между равноправными маршрутизаторами ATM-LSR должно быть установлено выделенное виртуальное соединение ATM (выделенный идентификатор VPI/VCI) для передачи сигналов управления LDP. Как и в обычных маршрутизаторах LSR, для распространения меток могут использоваться другие методы, такие как OSPF, RSVP, PIM. Маршрутизатор ATM-LSR может выполнять коммутацию на основе меток, содержащихся в полях VPI, VCI или VPI/VCI, в зависимости от того, используется ли объединение VC или VP для группирования потока. Равноправные маршрутизаторы ATM-LSR можно соединять непосредственно через звено ATM или дистанционно через "облако" ATM виртуальным соединением ATM. В последнем случае сигнализация ATM должна будет переносить информацию связывания.

На рисунке I.4 показана структура протокола для архитектуры MPLS на основе ATM. Архитектура MPLS/ATM состоит из двух частей, одна часть является модулем маршрутизации MPLS, а другая часть – модулем пересылки ATM. Модуль маршрутизации MPLS включает в себя функциональный блок протокола маршрутизации IP, поддерживающий OSPF и BGP, стек протоколов TCP/IP, LDP и результат его выполнения, LIB, используемый для распространения и назначения меток. Модуль пересылки ATM является устройством ATM.



LDP Протокол распространения меток
LIB Информационная база меток

Рисунок I.4/Y.1310 – Пример реализации MPLS

Добавление II

Руководящие указания по отображению услуг в соединения ATM

II.1 Отображение услуг Intserv в соединения ATM

II.1.1 Отображение гарантированной услуги (GS) в ATM

II.1.1.1 Сетевая модель для GS

Сетевая модель, предусмотренная в [GUAR_SER], показана на рисунке II.1.

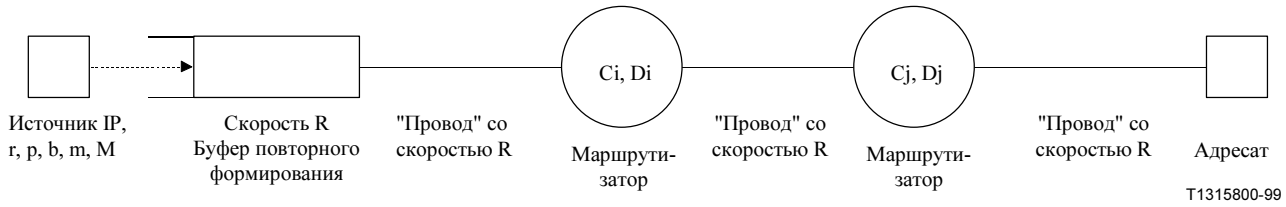


Рисунок II.1/Y.1310 – Сетевая модель для GS

Источник услуги GS, запросившей поток IP, выдает трафик согласно своей спецификации маркерного блока (r, p, b, m, M). После переходной фазы, в течение которой трафик может переноситься по принципу наилучшего усилия, ресурсы распределяются таким образом, что сеть может быть смоделирована как последовательность "проводов" со скоростью R. Как раз перед первым проводом весь трафик, мгновенно превышающий скорость R (даже если он соответствует спецификации маркерного блока), накапливается в буфере и повторно формируется на скорости R. Принимая это входное повторное формирование на выделенной скорости R, сетевая модель рассматривает ситуацию наихудшего случая в части изменения задержки. Провода связаны устройствами (маршрутизаторами), которые вводят "искажение" относительно идеальной модели движения потока (единственный провод со скоростью R). Искажение, вносимое каждым маршрутизатором, учитывается в соответствии с двумя членами, называемыми соответственно C (зависит от скорости) и D (не зависит от скорости). Сообщения RSVP переносят к получателю сумму всех значений Ci и Di так, что им может быть вычислена верхняя граница для переменной части задержки. Если скорость в проводах равна R, то эта верхняя граница составляет:

$$\frac{b-M}{R}\cdot\frac{p-R}{p-r}+\frac{M+C_{tot}}{R}+D_{tot} \quad \text{для } r \le R < p^{1}\ , \tag{II-1}$$

$$\frac{M+C_{tot}}{R}+D_{tot} \quad \text{для } r \le p \le R\,. \tag{II-2}$$

Таким образом, получатель запрашивает резервирование пропускной способности в проводах величины R (передавая исходящий поток в сообщении RSVP RESV), чтобы обеспечить целевое значение в приведенном выше уравнении II-1 или II-2. Отметим, что задержка в буфере повторного формирования (см. рисунок II.1) учитывается в первом члене уравнения II-1, но если R > p (как в уравнении II-2), трафик никогда не будет задерживаться в буфере повторного формирования.

II.1.1.2 Выбор услуги ATM

Проблема отображения возникает, когда провода должны быть заменены соединениями ATM. Строго говоря, если модель из проводов должна была бы соблюдаться, то не было бы возможности выбора, поскольку соединения ATM всегда вносят изменение задержки ячейки (CDV), которое отражает изменение задержки для пакетов, между тем как в проводах этого нет. На практике выбор следует ограничить теми возможностями ATC, которые можно связать с классом QoS, гарантирующим ограниченное изменение CDV (то есть Класс 1 QoS [I.356] или Класс 5 QoS [I.356]). Это изменение CDV можно затем учесть в члене D уравнения (II-1) или (II-2).

Скорости DBR [I.371] и SBR1 [I.371] возможности ATC могут быть связаны с Классом 1 QoS [I.356]. Скорости SBR2 [I.371] и SBR3 [I.371] возможности ATC могут быть связаны с Классом 5 QoS [I.356]. Таким образом, какой же критерий может быть использован для выбора услуги ATM? Первоначально, перед отправкой к уровню ATM, можно рассмотреть, является ли поток IP реально повторно сформированным на уровне IP на скорости R, как предполагается моделью. Если это так, то наиболее естественным выбором является принятие соединения ATM DBR класса 1 QoS со скоростью PCR = (эквивалент ATM от R)[2]. При выборе соединения SBR со скоростью SCR = (эквивалент ATM от R) будет бесполезно затребовано больше ресурсов, чем скорость DBR, за исключением случая PCR = SCR = (эквивалент ATM от R) и величины MBS = 0, что опять означает случай перехода к скорости DBR.

Наоборот, если начальная точка соединения ATM не осведомлена относительно любого повторного формирования пакета уровня IP, то наилучшим отображением было бы соединение SBR с SCR = (эквивалент ATM от R), PCR = (эквивалент ATM от p), MBS = [эквивалент ATM от $bp/(p - r)$]. Скорость DBR потребовала бы больше ресурсов для согласования соответствующих пачек трафика до скорости p, и поэтому потребуется скорость PCR = (эквивалент ATM от p) или минимальная скорость ячеек MCR = (эквивалент ATM от p).

Из трех версий SBR наилучшим образом согласующейся с моделью услуги GS является скорость SBR3, которая позволяет осуществлять маркирование несоответствующего трафика. Это позволяет возложить на уровень ATM всю сложность обработки излишнего трафика методом наилучшего усилия, как требует [GUAR_SER]. Связанным с этим классом QoS является класс 5 качества QoS [I.356].

---

[1] Эта формула остается той же, даже если повторное формирование возникает не на входе, а в одном или в большем числе пройденных маршрутизаторов.

[2] См. II.1.1.3.

Таблица II.1/Y.1310 – Предпочтительное отображение GS в ATM

	Уровень ATM информирован о повторном формировании пакета уровня IP на скорости *R* непосредственно перед начальной точкой соединения	Уровень ATM не информирован о повторном формировании пакета уровня IP на скорости *R* непосредственно перед начальной точкой соединения
Предпочтительные ATC и класс QoS	Класс 1 DBR	Класс 4 SBR3
Отображение между дескриптором трафика ATM и параметрами маркерного блока	PCR = (Эквивалент ATM от *R*)	Примечание 1 Примечание 2 PCR = (Эквивалент ATM от *p*) SCR = (Эквивалент ATM от *R*) MBS = (Эквивалент ATM от $bp/(p-r)$)
ПРИМЕЧАНИЕ 1. – Отображение параметра в скорость SBR всегда действительно, когда $R \leq p$. Однако в услуге GS параметр *R* может быть установлен большим, чем *p* [см. уравнение II-2)]. Поскольку PCR нельзя установить меньше *R*, то это будет приводить к скорости PCR = SCR = $R > p$, и не будет причины иметь MBS > 0. Таким образом, в случае $R > p$ предпочтительным отображением является DBR с классом 1 QoS, с PCR = (Эквивалент ATM от *R*). ПРИМЕЧАНИЕ 2. – Когда используется скорость SBR, то имеется существенная неэффективность в схеме отображения из-за того, что сетевая модель услуги GS рассматривает "провода" со скоростью *R*, в то время как соединения SBR гораздо "лучше", чем провода со скоростью *R*, в том смысле, что они могут поглощать мгновенные пачки трафика вплоть до скорости *p*, не полагаясь на накопление трафика, превышающего *R*. Эта неэффективность отражается в чрезмерном распределении для *R* из-за первого члена уравнения (II-1), который предполагается моделью GS, но в реальной сети может не существовать или быть значительно меньше.		

II.1.1.3 Эквиваленты ATM параметров маркерного блока

При преобразовании параметров маркерного блока в дескрипторы трафика ATM следует помнить, что первые параметры выражаются в байтах или байтах/с, в то время как последние параметры даются в ячейках или в ячейках/с. Более того, должны быть учтены заголовки ATM и AAL.

Верхняя граница для количества ячеек, необходимых для переноса пакета IP из *B* байтов, составляет:

$$C(B) = (H + B + T + 47)/48, \qquad \text{(II-3)}$$

где *H* и *T* являются длинами заголовка и хвостовика элемента PDU уровня AAL, а "47" считается последней ячейкой, которая может быть заполнена только частично.

Эквиваленты ATM для членов, появляющихся в таблице II.1, перечислены в таблице II.2. Сделано предположение, что спецификация маркерного блока есть (*r*, *b*, *p*, *m*, *M*).

Таблица II.2/Y.1310 – Эквиваленты ATM для отображения GS в ATM

Отображение в класс 1 DBR	Отображение в класс 4 SBR3
$PCR = \left\lfloor \frac{R}{m} \right\rfloor C(m)$	$PCR = \left\lfloor \frac{p}{m} \right\rfloor C(m)$ $SCR = \left\lfloor \frac{R}{m} \right\rfloor C(m)$ Примечание $MBS = \left\lfloor \frac{bp}{m(p-r)} \right\rfloor C(m)$
ПРИМЕЧАНИЕ. – Сколько времени источник, соответствующий спецификации маркерного сегмента, может посылать "байты" на пиковой скорости *p*[байты/с]? В течение $T = b/(p - r)$ секунд. Сколько байтов может он послать на пиковой скорости *p* перед тем, как станет "несоответствующим"? $bp/(p - r)$. Сколько пакетов максимум? $bp/[m(p - r)]$. Поэтому соединению SBR ATM, переносящему этот трафик, следует передавать это количество пакетов "прозрачно" (то есть на их пиковой скорости) и поэтому ему следует иметь указанную величину MBS (в ячейках).	

Эти эквиваленты представляют собой худший случай, то есть являются вычисленными в предположении, что все пакеты имеют минимальную объявленную длину, учитывая тем самым максимально возможное влияние заголовка. Более реалистическую оценку можно сделать, заменяя *m* в вышеуказанных формулах значением в диапазоне [*m, M*], но это требует подробного знания порождающего прикладного распределения размеров пакетов.

II.1.1.4 Учет CDVT

После выполнения сегментации пакетов ячейки, относящиеся к пакету, одновременно готовы для отправки и могут быть посланы на линейной скорости, если не было произведено повторное формирование уровня ячеек. Когда предполагается отсутствие функции формирования уровня ячеек для поглощения пачек за счет сегментации пакетов, необходимо учесть этот пачечный режим добавлением соответствующего значения к CDVT в параметре PCR соединения DBR или SBR. Это значение можно рассчитать так:

$$\left(C(M)-1\right)\left(\frac{1}{PCR}-\frac{1}{LCR}\right). \qquad \text{(II-4)}$$

II.1.2 Отображение услуги с управляемой нагрузкой (CLS) в ATM

Сетевая модель для услуги CLS, рассматриваемая в [CONTROL_SER], также состоит из источника, трафик которого описывается спецификацией маркерного блока (*r, p, b, m, M*), и последовательности маршрутизаторов, связанных "проводами" (см. рисунок II.1); но поскольку здесь нет явной гарантии на задержки, то нет и каких-либо конкретных формул, как уравнение (II-1) или (II-2). Когда провода должны быть заменены соединениями ATM, выбор больше не ограничен возможностями ATC, которые могут иметь ограниченные изменения CDV. Поскольку требование услуги CLS просто состоит в том, чтобы иметь "долговременную"[3] доступную пропускную способность и малые потери, то подходящими услугами ATM могут быть:

- DBR с классом 2;
- ABT с классом 2;
- ABR с классом 3;
- SBR1 с классом 2;
- SBR2 с классом 3;
- SBR3 с классом 3;

---

[3] "Долговременная" означает на временной шкале величину, которая значительно больше, чем b/r, где b и r являются частями параметра маркерного блока источника.

- GFR1;
- GFR2.

Отображение с помощью DBR с классом 2 потребовало бы установки скорости PCR где-то между ними (эквивалент ATM от r и p)[4], то есть нахождения эквивалентной пропускной способности для единственного потока, но, помимо существования конкретного вопроса по реализации, также существует риск, что это будет неэффективным. Более того, класс 2 не позволяет уровню ATM принимать меры для обработки трафика по принципу наилучшего усилия, превышающего спецификацию маркерного блока, как требуется в [CONTROL_SER].

Отображение с помощью ABT/dt с классом 2, даже если и потенциально привлекательное, имеет недостатком наличие повторного согласования заголовка на уровне пачки, вероятно, непереносимое. Для более долгосрочных повторных согласований имеет место тот же самый недостаток, что указан для DBR.

Отображение с помощью ABR с классом 3 может быть выполнено путем установки MCR = (эквивалент ATM от r), но оно имеет недостатком то, что весь трафик, мгновенно превышающий r, обрабатывается как наилучшее усилие. Установка скорости MCR где-то между ними (эквивалент ATM от r и p) имеет тот же самый недостаток, что указан для DBR, без какой-либо гарантии того, что уровень ATM может точно различать трафик, соответствующий и не соответствующий спецификации маркерного блока.

Отображение с помощью SBR1 с классом 2 или SBR2 с классом 3 позволяет уровню ATM знать максимальное количество информации, нужное для выполнения эффективного статистического мультиплексирования, но что касается обработки несоответствующей части трафика, оно не удовлетворяет ожиданию обработки по принципу наилучшего усилия.

Все три оставшихся отображения удовлетворяют как цели отражения на уровне ATM характеристик трафика настолько близко, насколько возможно, как задано спецификацией маркерного блока, так и цели обеспечения принципа наилучшего усилия точно для части трафика, превышающего ее. Подробные эквиваленты ATM приведены в таблице II.3.

Таблица II.3/Y.1310 – Эквиваленты ATM для отображения CLS в ATM

Отображение в SBR3	Отображение в GFR1 или GFR2
$PCR = \left\lfloor \frac{p}{m} \right\rfloor C(m)$	$PCR = \left\lfloor \frac{p}{m} \right\rfloor C(m)$
$SCR = \left\lfloor \frac{r}{m} \right\rfloor C(m)$	$MCR = \left\lfloor \frac{r}{m} \right\rfloor C(m)$
$MBS = \left\lfloor \frac{bp}{m(p-r)} \right\rfloor C(m)$	$MFS = C(m)$
	$MBS = \max\left(\left\lfloor \frac{bp}{m(p-r)} \right\rfloor C(m), MFS \right)$

Использованы те же самые соображения относительно необходимости замены m значением между [m, M] и относительно значения добавки к CDVT, которые приведены в конце II.1.1.4.

II.2 Отображение услуг Diffserv над ATM

В этом подразделе для информации описываются некоторые возможные примеры отображения дифференцированных услуг в услуги ATM. Группа IETF только что описала прикладные услуги, которые могут быть поддержаны с помощью каждого PHB или группы PHB [DIFF_AF] и [DIFF_EF].

---

[4] См. также II.1.1.3.

- *Услуга эмуляции арендованной линии*

  Она также называется "услугой с наивысшим качеством". Эта услуга может быть реализована с использованием EF-PHB. Этот вид услуги обычно требует строгих гарантий малых потерь и задержки. Эта услуга также характеризуется своей пиковой скоростью. Соответственно, эта услуга может быть просто отображена в ATC DBR, используя класс 1 QoS, чтобы удовлетворить такие требования по потерям и задержкам. Пиковая скорость может быть непосредственно отображена в параметр PCR из ATC DBR.

- *Услуга с гарантией количественных показателей*

  Она также называется "услугой гарантированной скорости". Эта услуга может быть реализована с использованием одного из четырех классов AF-PHB. Эта услуга характеризуется минимальной скоростью передачи, гарантируемой на статистической основе. Эта услуга предлагает более широкие гарантии, чем услуга эмуляции арендованной линии, но все еще рассматривается как количественная услуга. В частности, она обещает доставлять трафик с высокой степенью надежности и ограниченной задержкой вплоть до согласованной скорости. Соответственно, представляется совершенно подходящим отображать эту услугу в ATC ABR с использованием класса 3 QoS. В этом случае скорость MCR может быть установлена равной минимальной скорости услуги.

II.3 Intserv в MPLS над ATM

Параметры трафика Intserv, включающие *p, r, b* и *R*, определены в таких объектах RSVP, как *Tspec* и *Rspec*. Если для поддержки Intserv в MPLS над сетями ATM вместо RSVP используется CR-LDP, то в этом случае должны быть рассмотрены следующие требования:

– Когда поток RSVP/Intserv, включающий гарантированную услугу и услугу с управляемой нагрузкой, вводится во входной маршрутизатор LSR в сетях MPLS, то такие параметры *Tspec* RSVP, как *p, r* и *b,* должны быть отображены в параметры трафика в сообщении запроса метки CR-LDP.

– Для поддержки гарантированной услуги такие параметры *Rspec* RSVP, как *R* и *S*, должны быть отображены в транспортных параметрах в сообщении отображения метки CR-LDP.

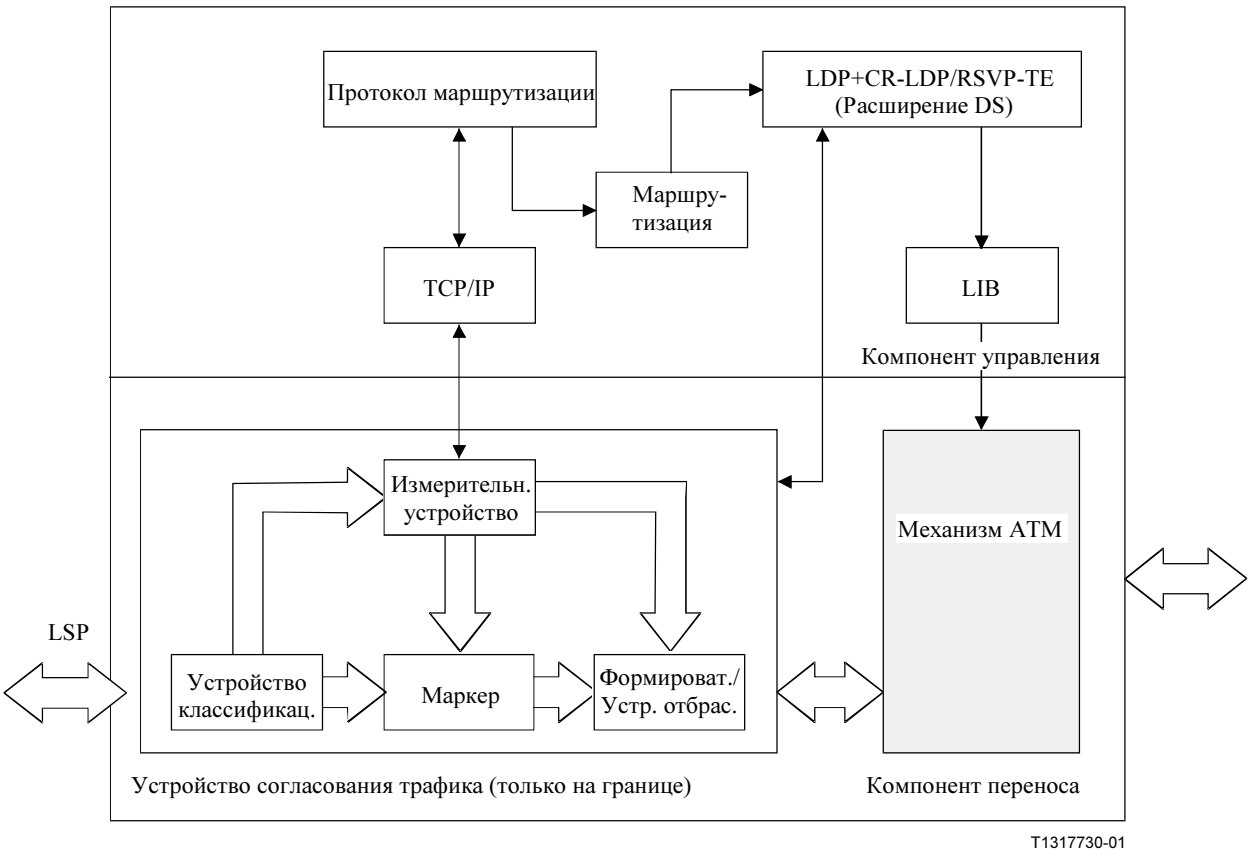
Отображение параметров трафика из Intserv в CR-LDP зависит от алгоритма согласования трафика во входном маршрутизаторе LSR.

II.4 Diffserv в MPLS над ATM

В этом подразделе описывается подход для поддержки Diffserv в сети ATM MPLS. Маршрутизатор ATM-LSR с возможностью Diffserv должен иметь логическую структуру, показанную на рисунке II.2. Следует отметить, что транзитному маршрутизатору ATM-LSR обычно не требуется элемент согласования трафика, но граничный маршрутизатор ATM-LSR должен иметь этот элемент для выполнения функций классификации пакетов, маркирования, измерения и формирования/ отбрасывания, требуемых архитектурой Diffserv [DIFF_ARCH].

В качестве системы сигнализации может использоваться CR-LDP или RSVP-TE.

Подробные сведения об устройстве согласования трафика см. в ссылке [DIFF_ARCH].



LIB Информационная база меток

Рисунок II.2/Y.1310 – Логическая архитектура маршрутизатора ATM-LSR с возможностью Diffserv

II.4.1 Процедуры установки LSP

Основная процедура установки ATM MPLS Diffserv LSP включает в себя следующие действия:

- На границе области ATM MPLS Diffserv маршрутизаторы ATM LER обрабатывают запросы услуг и выполняют процедуру классификации услуг. Затем маршрутизаторы LER определяют режим PHB (режим на каждом транзитном участке), который будет использоваться услугой. Затем маршрутизатор ATM LER отображает режим PHB в пары <PSC, CLP> (составление расписания на каждый транзитный участок, приоритет потери ячейки). Взаимосвязи при отображении заданы в таблице II.4.
- Согласно требованиям Diffserv, используется система сигнализации MPLS (например, мы можем использовать протокол CR-LDP с поддержкой Diffserv [MPLS_DIFF] в качестве системы сигнализации) для выполнения процесса предоставления услуги [DIFF_ARCH] и установки тракта LSP, поддерживающего QoS, для услуги. В этой точке таблицы пересылки в маршрутизаторах LSR вдоль тракта LSP будут иметь новую колонку для входящих расписаний PSC.

II.4.2 Процедура пересылки метки

Основная операция по пересылке метки схемы ATM MPLS Diffserv включает в себя следующие действия:

- На входе области ATM MPLS Diffserv маршрутизаторы LER определяют класс FEC и класс PHB пакета путем проверки адреса IP и значения DSCP (кодовой точки дифференцированной услуги), переносимых пакетом IP.
- Затем входной маршрутизатор ATM-LSR выполняет согласование трафика, определяет исходящий протокол CLP для пакета. Если был установлен L-LSP ATM, то может быть переписано только поле CLP.

- После этого входной маршрутизатор ATM-LSR определяет исходящий идентификатор VCI и номер интерфейса, выполняет исходящее PSC для пакета, вкладывает пакет IP в пакет ATM и посылает его в исходящий интерфейс.
- В области MPLS Diffserv транзитный маршрутизатор LSR проверяет поле идентификатора VCI и поле CLP в заголовке пакета ATM. Используя таблицу пересылки, он определяет расписание PSC, требуемое пакетом.
- Используя таблицу отображения, приведенную в таблице II.4, транзитный маршрутизатор LSR определяет режим PHB, требуемый пакетом. Обычно транзитный маршрутизатор LSR не выполняет действий по согласованию трафика, он только реализует режим PHB для пакета и использует таблицу пересылки для пересылки пакета к маршрутизатору входящего потока LSR. Если транзитному маршрутизатору LSR не нужно выполнять действия по согласованию трафика, то он использует результаты процедур согласования трафика для изменения исходящего приоритета CLP для пакета ATM.
- На выходе области ATM MPLS Diffserv выходной маршрутизатор LSR ATM проверяет поле идентификатора VCI и поле CLP в заголовке пакета ATM. Используя таблицу пересылки, он определяет расписание PSC, требуемое пакетом. Используя таблицу отображения, приведенную в таблице II.4, транзитный маршрутизатор LSR определяет затем режим PHB, требуемый пакетом. После этого он выполняет процедуры согласования трафика и использует результаты, объединенные с входящим режимом PHB, для определения исходящего PHB и исходящего значения точки DSCP для пакета.
- Затем выход ATM преобразует пакет ATM обратно в пакет IP, который переносит адрес IP и поле DSCP. (Это поле должно быть заменено на точку DSCP, полученную в результате вышеуказанного действия.)

Таблица II.4/Y.1310 – Отображение между парами Diffserv PHB и ATM <PSC, CLP>

Diffserv PHBs	PSC	ATM CLP
DF	DF	0
CSn	CSn (Примечание 1)	0
AFi1 (Примечание 2)	AFCi	0
AFi2	AFCi	1
AFi3	AFCi	1
EF	EF	0
ПРИМЕЧАНИЕ 1. – "n" ($1 \leq n \leq 8$) относится к номеру приоритета IP. ПРИМЕЧАНИЕ 2. – "i" ($1 \leq i \leq 4$) относится к классу AF PHB, например, когда i = 1, AFi1 представляет AF11, который относится к классу 1 AF PHB и имеет приоритет отбрасывания 1.		

II.4.3 Отображения между <PSC, CLP> и PHB

Были определены следующие режимы PHB:

II.4.3.1 DF (PHB по умолчанию): Этот режим PHB используется для пакетов наилучшего усилия или пакетов с неизвестными значениями DSCP.

II.4.3.2 CS (PHB селектора класса): Этот режим PHB используется для обратной совместимости с существующей 8-уровневой системой приоритета IP.

II.4.3.3 EF (PHB ускоренной пересылки): Этот режим PHB используется для услуг, которые требуют гарантии малой частоты потерь пакетов, малой задержки, малых фазовых дрожаний и пропускной способности. Пакет с этим режимом PHB получает наивысший приоритет обслуживания и наилучшее обслуживание в области.

II.4.3.4 AF (PHB гарантированной пересылки): Этот режим PHB используется для классификации пакетов с различными приоритетами отбрасывания в том же самом соединении. Группа IETF определила четыре класса AF, а внутри каждого класса имеются три режима PHB с различными приоритетами отбрасывания. Таким образом, всего имеются 12 AF PHB. Примером

использования этого режима PHB является случай, когда трафик превышает определенную скорость передачи; лишнему пакету назначается PHB с более высоким приоритетом отбрасывания. Другое важное требование этого режима PHB заключается в том, что пакеты, принадлежащие единственному соединению и тому же самому классу PHB, не могут быть переупорядочены.

В таблице II.4 показано отображение между парами PHB и <PSC, CLP>. Эти отображения должны быть совместимыми на каждом маршрутизаторе LSR в области ATM Diffserv, и эти отображения должны быть конфигурируемыми.

II.4.4 Соображения по реализации

Маршрутизаторам ATM MPLS LSR следует поддерживать режимы PHB и правила согласования трафика услуг IP. Однако подробная обработка пакетов и правила согласования трафика на маршрутизаторах ATM MPLS LSR являются вопросами реализации.

Добавление III

Возможные сценарии эволюции к коммутации MPLS для IP над ATM в сетях общего пользования

III.1 Введение

Какие маршруты из существующей сетевой инфраструктуры являются потенциальными маршрутами к MPLS? Они будут функцией фактического состояния, а также услуг, которые должны быть предоставлены конкретной транспортной сетью.

В этой Рекомендации мы предполагаем, что MPLS будет развертываться в существующих магистральных сетях ATM. Для целей исследования решений для эволюции к MPLS транспортные сети будут классифицированы по принципу, являются ли они новыми или уже существующими и обеспечивают ли они полный объем услуг (данные, голос, видео, арендованные линии) в сравнении с чистыми IP-сетями. Это не является универсальной классификацией; скорее, это удобный способ установления категории поставщиков услуг, основанный на фактическом состоянии их сети и ее ожидаемого предложения услуги.

В этом Добавлении рассматриваются несколько типов существующих инфраструктур и развернутых стратегий для введения MPLS в эти типы сетей. Затем в нем исследуются различные технологии для работы MPLS над оборудованием ATM, не поддерживающим MPLS, и даются рекомендации по использованию этих технологий.

III.2 Предлагаемые сценарии

Представляются и обсуждаются следующие различные сценарии:

III.2.1 Уже существующая транспортная сеть с полным объемом услуг

Мы предполагаем, что уже существующая транспортная сеть содержит наследуемую сеть передачи голосовой информации и транспортирует трафик передачи данных либо в сети с временным разделением каналов (ВРК), либо в отдельной сети. Мы также предполагаем, что такая транспортная сеть находится в процессе объединения своей сети передачи данных и сети передачи голосовой информации над одной и той же инфраструктурой.

Существующая транспортная сеть, вероятно, имеет наследованную инфраструктуру ATM, которая используется для трафика передачи данных (IP или ретрансляция кадров) и может быть использована для трафика голоса и видео или любых других естественных услуг ATM. В этом случае ATM используется в качестве коммутационной технологии многих услуг.

Существующий перенос IP в транспортных сетях с наибольшей вероятностью должен базироваться на одном из трех вариантов:

– использование соединения "точка-точка" PVC ATM с вложением согласно RFC 2684 [ATM_MULTI];
– использование классического протокола IP над ATM;
– использование MPOA.

В любом случае необходимо ввести MPLS в сеть, которая в настоящее время использует только соединения PVC, SPVC, SVC, протоколы PVP и SPVP и не использует каналы VC с управлением MPLS. Каналы VC MPLS могут быть обозначены как "Каналы VC с метками (LVC)", чтобы отличать их от SVC с идентификатором PNNI или подобным управлением.

III.2.2 Уже существующая сеть передачи голосовой услуги

Мы предполагаем, что транспортная сеть содержит только сеть для передачи голосовой информации, традиционные системы сигнализации и временного разделения каналов SS7/TDM без какого-либо существенного вложения в ATM, и существует план переносить в будущем как голос, так и данные, используя инфраструктуру MPLS на основе ячеек. Что является наилучшим путем развития?

В сети передачи голосовых сигналов в первой фазе, вероятно, будет сохранено управление сигнализацией SS7 и перенос голосового трафика из сети TDM в пакетную сеть. При предположении вероятности выбора MPLS на основе ячеек трафик данных, а также голосовой трафик будут транспортироваться в этой сети, основанной на MPLS. Для поставщика услуги имеется выбор – либо сохранить обе сети разделенными, либо работать в направлении их постепенной интеграции.

III.2.3 Новая транспортная сеть, ориентированная на IP

Вопрос заключается в том, имеет ли смысл осуществлять какое-либо развертывание ATM. Если для транспортной сети выбирается развертывание MPLS на основе ячеек, то тогда здесь имеет место небольшое продвижение в направлении управления ATM в сети. Главным моментом было бы повторное использование только коммутационных возможностей ATM.

III.2.4 Новая транспортная сеть с полным объемом услуг

Новая транспортная сеть с полным объемом услуг будет предлагать услуги голоса, видео и арендованных линий наряду с услугами, ориентированными на IP. Из-за изменяющихся типов трафика мы предполагаем, что для интеграции своих предложений услуг в составе одной сети транспортной сетью может быть выбрано развертывание инфраструктуры ATM.

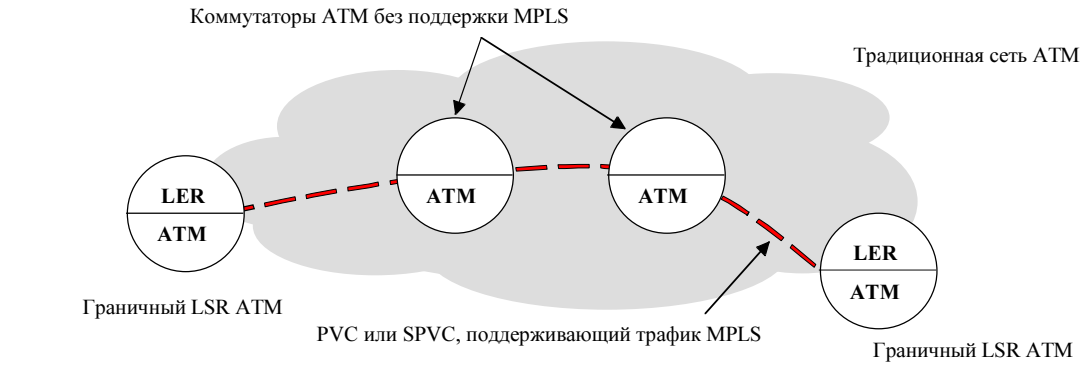
Маршрутизаторы могут быть развернуты на границах сети для поддержки услуг IP, но коммутируемой базовой сетью будет ATM. Коммутация MPLS на основе ячеек будет развернута в базовой сети. Могут потребоваться скрытые операции с ATM, чтобы интегрировать услуги, основанные на MPLS и ATM. Для расчета трафика потребуется коммутация MPLS с явной маршрутизацией; для обработки трафика, не переносимого внутри явно проложенных трактов LSP, потребовалась бы коммутация MPLS по каждому транзитному участку.

III.3 Гибридная сеть ATM

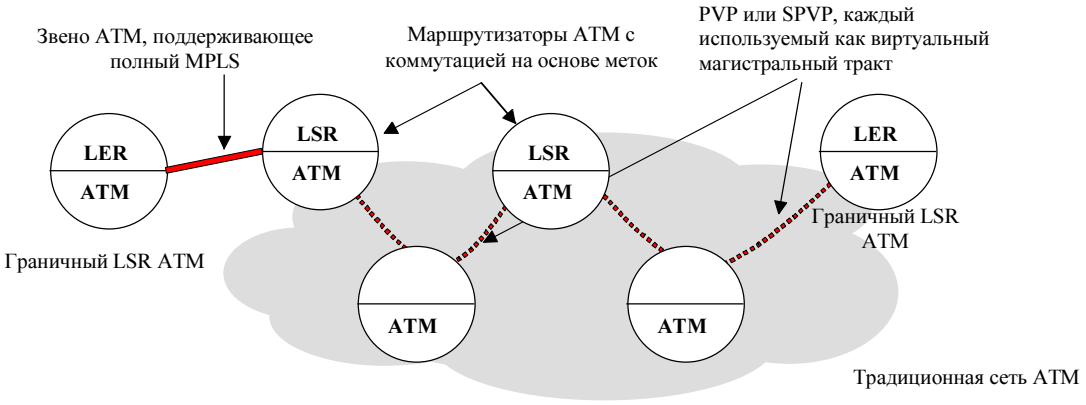
В этом подразделе обсуждаются три возможных способа интеграции в сети ATM оборудования MPLS с оборудованием, не использующим MPLS. В этом подразделе предполагается поддержка коммутации ATM в текущей сети. Поддержка MPOA и C-IPOA в этом подразделе не рассматривается; однако обсуждаемые здесь методы могут применяться.

III.3.1 Технологии для гибридных сетей ATM

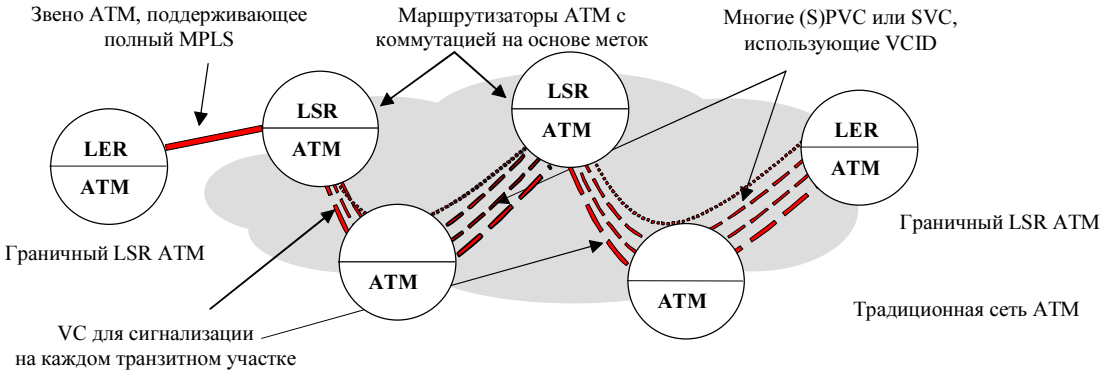
Во время введения ATM MPLS в существующую сеть ATM иногда будет необходимо соединять маршрутизаторы LSR над традиционным оборудованием ATM, формируя "гибридную" сеть. В гибридных сетях некоторые коммутаторы и/или маршрутизаторы обладают возможностью MPLS, а некоторые – нет. В этом подразделе обсуждаются возможные пути реализации гибридных сетей ATM: MPLS над PVC, виртуальные магистральные тракты и уведомление идентификатора виртуального соединения для протокола LDP (VCID). Эти методы иллюстрируются на рисунке III.1.



a) MPLS над каналами PVC



b) Виртуальные магистральные тракты



c) Уведомление идентификатора виртуального соединения

T1317740-01

Рисунок III.1/Y.1310 – Технологии для гибридных сетей

III.3.1.1 MPLS над каналами PVC

Коммутация MPLS над PVC показана на рисунке III.1 a). Она может быть использована только для соединения маршрутизаторов LSR на основе пакетов. Она не может быть использована для соединения между собой маршрутизаторов ATM с коммутацией на основе меток (ATM-LSR). Коммутация MPLS над PVC соединяет пакетные маршрутизаторы с коммутацией на основе меток (LSR) с помощью постоянных соединений виртуальных цепей (PVC) в традиционной сети ATM. Могут быть также использованы программные постоянные соединения виртуальных цепей (SPVC). (Любое упоминание о "PVC" по отношению к MPLS над PVC в этом приложении в равной степени применимо к SPVC.) Маршрутизаторы посылают один другому пакеты MPLS с метками, вложенными явно наряду с пакетом IP. Это называется "задание метки на пакет", поскольку метка MPLS применяется к целому пакету в противоположность применения к индивидуальным ячейкам. Когда задание метки на пакет используется над каналами PVC, пакеты со многими различными метками посылаются в одном и том же PVC. Это отличается от MPLS ATM, где каждая отличная метка представляется другим каналом VC, известным как "VC метки" (LVC). Задание метки на пакет над PVC виртуально идентично

случаю, где маршрутизаторы с коммутацией на основе меток MPLS (LSR) соединяются посредством таких звеньев, как "пакеты над SONET", "пакеты над СЦИ" или любые другие звенья "точка-точка". Отметим, что MPLS над PVC не использует MPLS ATM на коммутаторах ATM, поддерживающих PVC. Это означает, что поставщики услуг должны продолжать обеспечивать PVC и управлять ими в масштабах, равных подходу традиционного протокола IP над ATM.

В MPLS над PVC используется общее вложение, которое описано в спецификации кодировок стека меток MPLS [MPLS_ENCAPS]. Возможные вложения уровня звена для PVC включают в себя нулевое вложение и вложение LLC/SNAP. Если PVC переносят только пакеты MPLS, то тогда рекомендуется нулевое вложение. В противном случае следует использовать LLC/SNAP с заголовком SNAP, содержащим "мнимые типы", заданные для MPLS над носителями информации сетей LAN [MPLS_ENCAPS].

III.3.1.2 Виртуальные магистральные тракты

Другим методом реализации гибридных сетей ATM является использование виртуальных магистральных трактов. Виртуальные магистральные тракты основаны на соединениях виртуальных трактов (VP). ATM MPLS обычно выполняет присвоение меток пакетам IP путем размещения их в различных каналах VC в том же самом магистральном тракте ATM. Каждый отличный канал VC в магистральном тракте представляет другое значение метки. Маршрутизаторы ATM LSR обрабатывают виртуальные магистральные тракты почти идентично физической соединительной линии: каждый отличный канал VC внутри тракта VP представляет другое значение метки. Разница заключается в том, что виртуальный магистральный тракт не является физической соединительной линией, связывающей два смежных маршрутизатора LSR. Виртуальный магистральный тракт является постоянным соединением виртуального тракта (PVP) или программным постоянным соединением виртуального тракта (SPVP), которое соединяет маршрутизаторы ATM-LSR способом традиционных коммутаторов ATM. Виртуальные магистральные тракты могут также соединять граничные маршрутизаторы LSR ATM с маршрутизаторами ATM-LSR или соединять граничные маршрутизаторы LSR ATM друг с другом. Использование виртуальных магистральных трактов иллюстрируется на рисунке III.1 b). Использование MPLS ATM с виртуальными магистральными трактами и метками на основе идентификаторов VCI описывается в документе "MPLS, использующий LDP и коммутацию VC ATM" [MPLS_ATM] и в большинстве случаев идентично использованию коммутации MPLS над физическими соединительными линиями с метками на основе идентификаторов VPI/VCI. Канал VC должен быть назначен для переноса трафика управления протокола LDP, и это соединение VC должно использовать вложение LLC/SNAP.

III.3.1.3 Уведомление идентификатора виртуального соединения для LDP (VCID)

Идентификатор VCID позволяет использовать в MPLS ATM [ATM_VCID] PVC, SPVC и соединения коммутируемых виртуальных цепей (SVC). (Здесь "SVC" конкретно относится к динамически устанавливаемому каналу VC в традиционной сети ATM. Каналы VC, используемые непосредственно коммутацией MPLS ATM, упоминаются здесь как "каналы VC с метками", или "LVC".) В противоположность этому, MPLS над PVC использует MPLS на основе пакетов, а не MPLS ATM, а виртуальные магистральные тракты используют соединения PVP или SPVP, а не PVC, SPVC или SVC. Идентификатор VCID поддерживает использование соединений PVC, SPVC и SVC в подобных сетевых конфигурациях к виртуальным магистральным трактам, как показано на рисунке III.1 c). Когда используется идентификатор VCID, ряд PVC, SPVC или SVC используются для переноса пакетов с метками между устройствами MPLS ATM, с одним каналом VC на каждую метку. Поскольку здесь имеется отдельный канал VC для каждой метки, то пересылку пакета MPLS ATM можно использовать в устройствах MPLS ATM, использующих идентификатор VCID.

Для переноса маршрутизации IP и LDP на каждом "транзитном участке" между маршрутизаторами LSR должен быть предварительно установлен канал VC по умолчанию. Этот канал VC является дополнением к каналам VC, используемым идентификатором VCID для соответствия меткам.

III.3.2 Сети, использующие MPLS над PVC

III.3.2.1 Использование технологии MPLS над PVC

Самой простой сетевой структурой, использующей MPLS над PVC, является полный элемент сети, показанный на рисунке III.2 a). Работа протоколов маршрутизации IP в сети MPLS этой структуры вызывает те же самые проблемы расширяемости, как для традиционных сетей IP над ATM подобной структуры. Одно из решений для этого состоит в использовании частичного элемента сети между маршрутизаторами, но это привело бы к использованию неэффективных маршрутов с множеством транзитных участков. Другим альтернативным решением является добавление дополнительных граничных маршрутизаторов LSR ATM, как показано на рисунке III.2 b), или, возможно, резервной пары их. Дополнительные граничные маршрутизаторы LSR ATM уменьшают размер элементов сети. Отметим, что требования к характеристикам дополнительных маршрутизаторов LSR будут достаточно высокими, поскольку они должны переносить большую часть сетевого трафика. Не существует прямого способа использования маршрутизаторов ATM-LSR в сети при использовании MPLS над PVC.

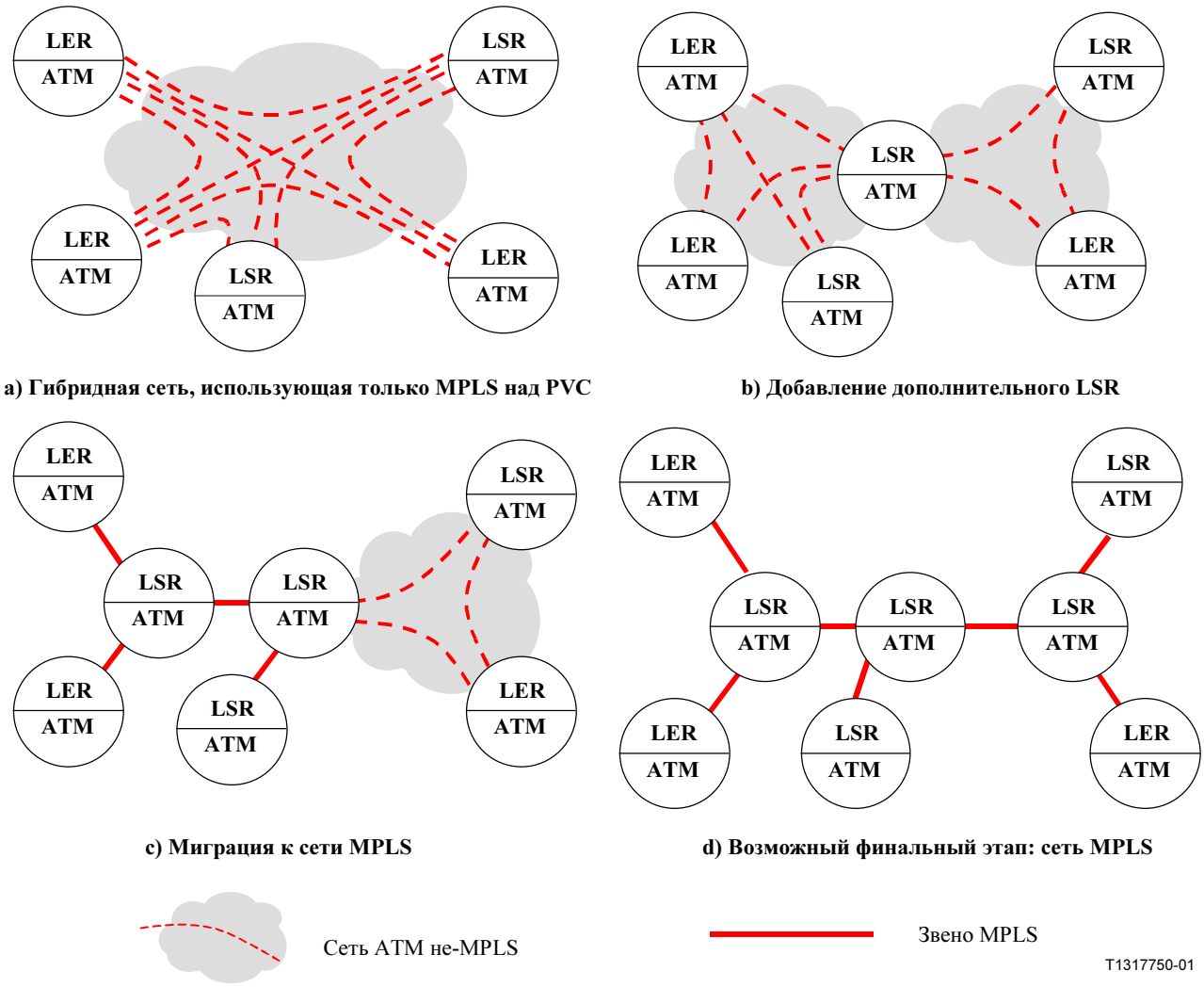


Рисунок III.2/Y.1310 – Сети MPLS ATM, использующие MPLS над PVC

В некоторых сетях связи могут предпочесть построение инфраструктуры для своего трафика MPLS, отдельной от своей традиционной сети ATM. В этой сети MPLS может использоваться MPLS ATM. В качестве альтернативного варианта в ней может использоваться MPLS на основе пакетов с маршрутизаторами LSR на основе пакетов и с такими звеньями, как протокол PPP над SDH. Так, в сети MPLS на основе пакетов может использоваться MPLS над соединениями PVC в качестве переходной стадии, позволяющей использовать традиционную сеть ATM для переноса трафика MPLS на ранних стадиях введения сети MPLS на основе пакетов. По мере роста этой сети звенья MPLS над PVC могут быть заменены физическими звеньями. Эта возможная будущая миграция показана на рисунках III.2 c) и d).

III.3.2.2 Оборудование для MPLS над PVC

Базовой сетью сети MPLS над PVC является традиционная сеть ATM, для которой нужно только поддерживать соединения PVC или SPVC. В сущности, можно использовать любую сеть ATM. Граничным маршрутизаторам LSR ATM следует поддерживать следующее:

- одну или более карт сетевых интерфейсов ATM;
- вложение MPLS на основе пакетов над соединениями PVC или SPVC;
- формирование трафика под параметры PVC или SPVC.

III.3.3 Сети, использующие виртуальные магистральные тракты

- *Использование виртуальных магистральных трактов*

  Простой способ использования виртуальных магистральных трактов заключается в подсоединении с их помощью граничных маршрутизаторов LSR ATM вообще без использования в сети любых маршрутизаторов ATM-LSR, как показано на рисунке III.3 a). Это означает, что все пакеты MPLS переносятся в виртуальных магистральных трактах и фактически в сети не возникает коммутации на основе меток. Часть ATM сети состоит полностью из традиционных коммутаторов ATM. В более общем случае некоторые коммутаторы в сети ATM поддерживают стек протоколов MPLS, а некоторые – нет. Виртуальные магистральные тракты можно использовать для соединения маршрутизаторов ATM-LSR с маршрутизаторами ATM-LSR или для соединения граничных маршрутизаторов LSR ATM с маршрутизаторами ATM-LSR, а также для соединения граничных маршрутизаторов LSR ATM между собой. Это показано на рисунке III.3 b).

- *Миграция к полной MPLS*

  На рисунках III.3 a), b) и c) показан возможный процесс миграции для введения MPLS в традиционную сеть ATM:

  Граничные маршрутизаторы LSR ATM добавляются вокруг границы традиционной сети ATM; в качестве альтернативы к существующим маршрутизаторам может быть добавлена функция MPLS. Это обеспечивает создание сетей VPN MPLS, а также предпосылок для следующих шагов.

  На следующем шаге в некоторые коммутаторы ATM добавляют функцию MPLS или в сеть добавляют дополнительные маршрутизаторы ATM-LSR. Это сокращает требуемое количество виртуальных магистральных трактов и позволяет начать устранение некоторых проблем расширяемости гибридных сетей.

  Добавляют больше маршрутизаторов ATM-LSR, которые далее уменьшают количество виртуальных магистральных трактов, и начинают вводить местные звенья ATM MPLS, как показано на рисунке III.3 c). Этот шаг, естественно, ведет к конечному шагу.

  В конечном счете все коммутаторы ATM становятся маршрутизаторами ATM-LSR, а виртуальные магистральные тракты вообще не используются. В полной сети функционирует MPLS ATM, и она не имеет никаких недостатков гибридных сетей. Это показано на рисунке III.3 d).

- *Другие варианты*

  Маршрутизаторы LSR и традиционные коммутаторы ATM могут комбинироваться многими различными способами. На рисунке III.4 показаны некоторые другие структуры гибридных сетей, которые могут возникать. Возможно множество других структур гибридных сетей. Сеть MPLS ATM должна включать в себя граничные маршрутизаторы LSR, но может использовать любое близкое сочетание из нуля или более маршрутизаторов ATM-LSR и из нуля и более традиционных коммутаторов ATM с виртуальными магистральными трактами.

- *Требования по поддержке виртуальных магистральных трактов*

  Виртуальные магистральные тракты реализуются с использованием постоянных виртуальных трактов (PVP) или программных постоянных виртуальных трактов (SPVP).

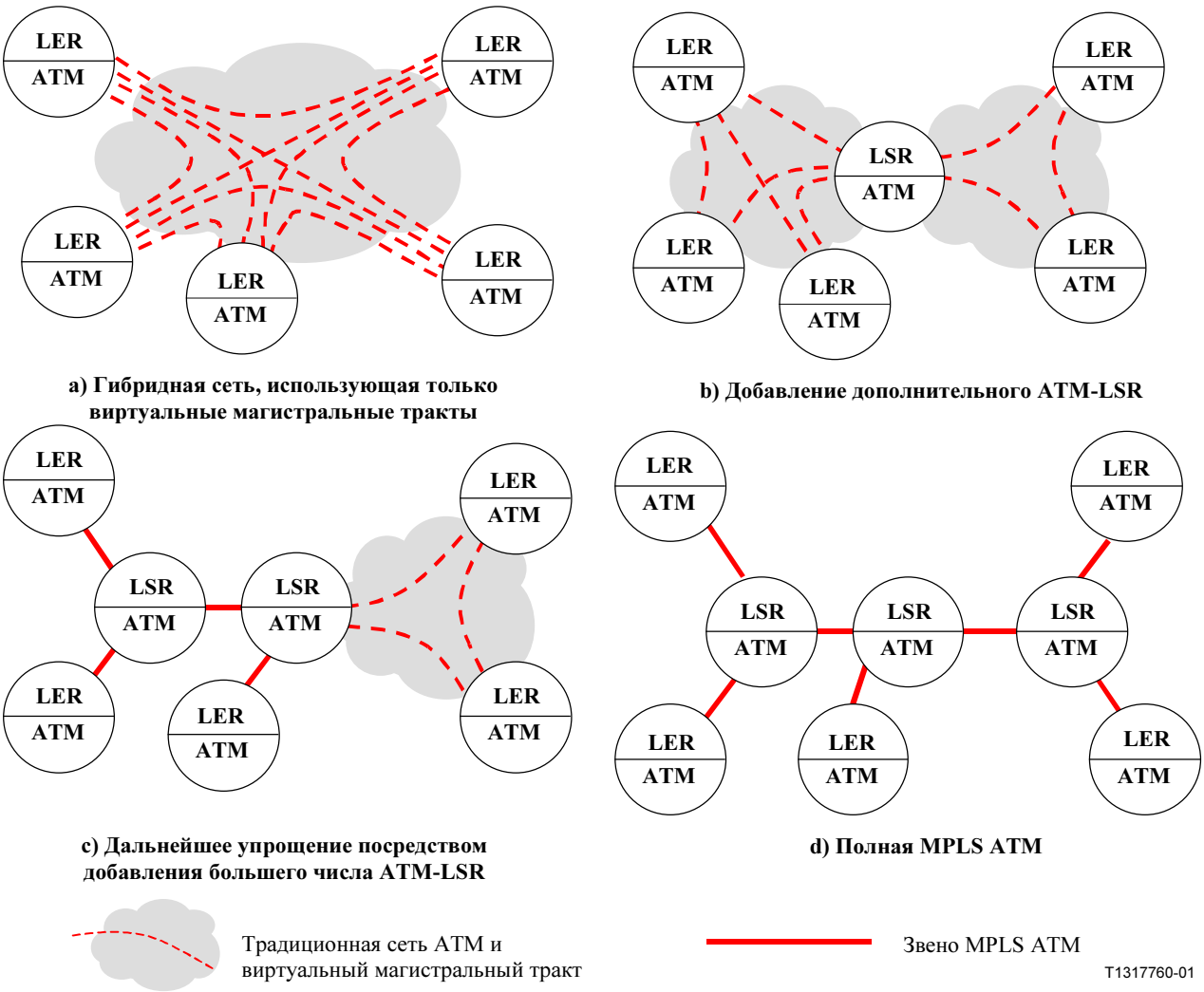


Рисунок III.3/Y.1310 – Сети ATM MPLS, использующие виртуальные магистральные тракты

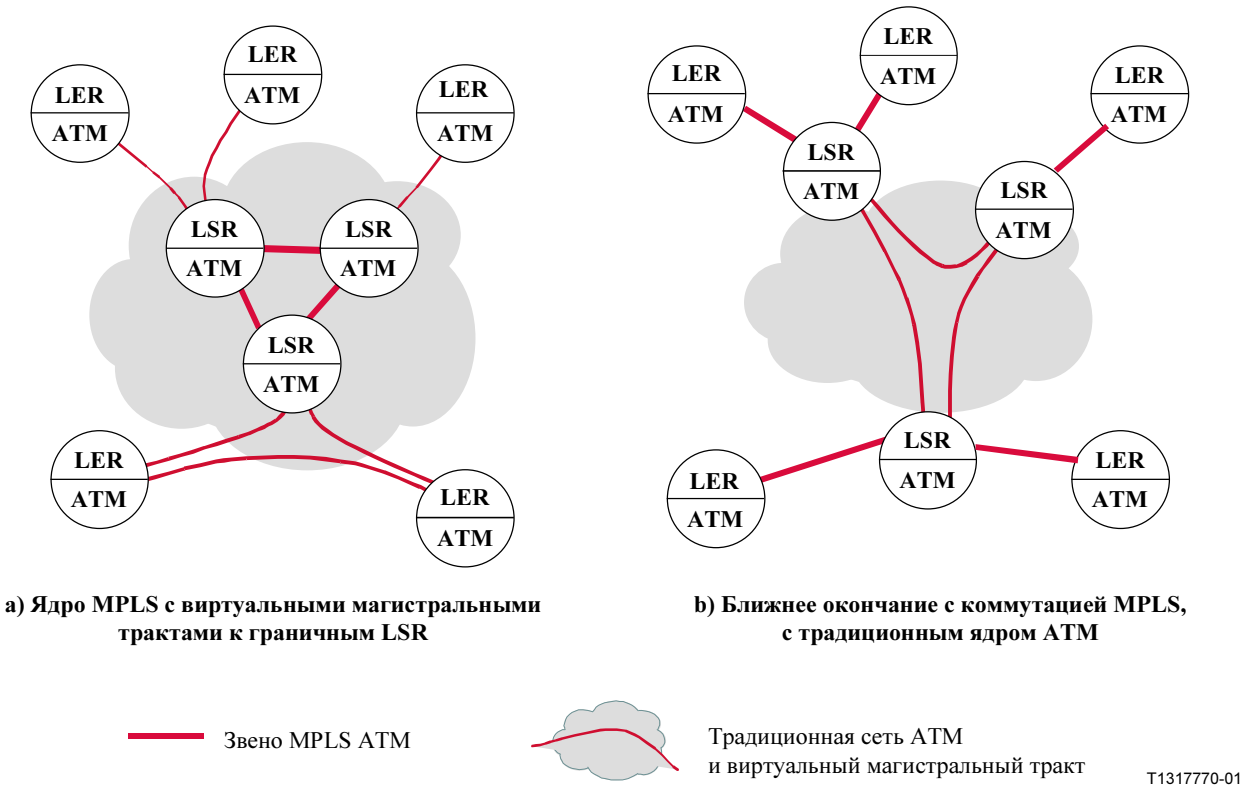


Рисунок III.4/Y.1310 – Другие примеры гибридных сетей, использующих виртуальные магистральные тракты в маршрутизаторах ATM-LSR

III.3.3.1 Поддержка виртуальных магистральных трактов в традиционных коммутаторах ATM

Коммутаторы в традиционных сетях ATM должны поддерживать соединения PVP или SPVP с помощью типов административного управления трафиком Форума ATM или МСЭ-Т, которые совпадают с типами, используемыми в граничных маршрутизаторах LSR. Для поддержки MPLS коммутаторы не требуются.

III.3.3.2 Поддержка виртуальных магистральных трактов в граничных маршрутизаторах LSR

Для поддержки виртуальных магистральных трактов граничные маршрутизаторы LSR ATM должны выполнять следующие требования:

- Они должны поддерживать одну или более карт сетевых интерфейсов ATM.
- Если конкретный виртуальный магистральный тракт использует идентификатор VPI *x* в граничном маршрутизаторе LSR, то тогда канал VC сигнализации LDP для виртуального магистрального тракта должен быть внутри *x*. Он может иметь идентификатор VPI = *x*, VCI = 32 вместо нормального идентификатора по умолчанию VPI = 0, VCI = 32 для сигнализации LDP [MPLS_ATM]. Однако другие значения VCI могут быть установлены на основании взаимных двусторонних соглашений.

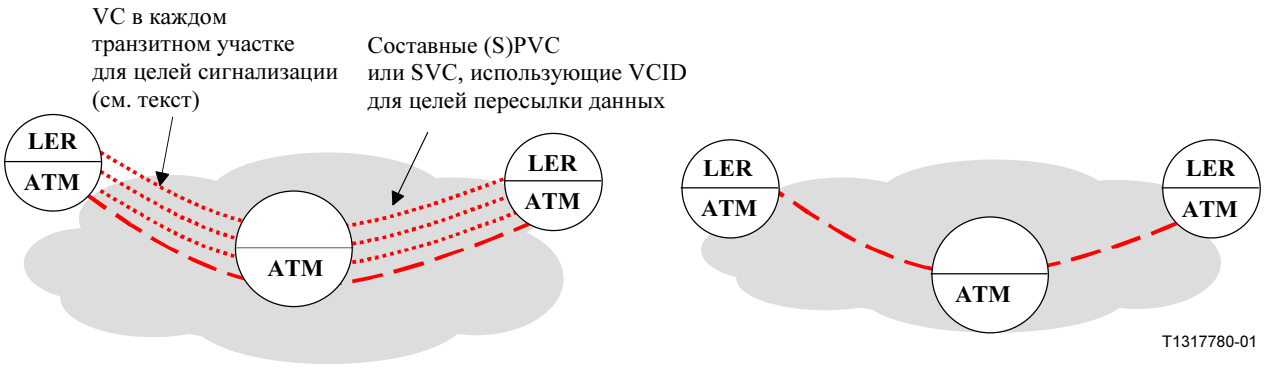
Для того, чтобы поддерживать виртуальные магистральные тракты, маршрутизаторы ATM-LSR должны выполнять те же самые требования, что и граничные маршрутизаторы LSR ATM:

- Если конкретный виртуальный магистральный тракт использует идентификатор VPI *x* в маршрутизаторе ATM-LSR, то тогда канал VC сигнализации LDP для виртуального магистрального тракта должен быть внутри *x*. Он может иметь идентификатор VPI = *x,* VCI = 32 вместо нормального идентификатора по умолчанию VPI = 0, VCI = 32. Однако другие значения VCI могут быть установлены на основании взаимных двусторонних соглашений.

III.3.4 Сети, использующие идентификатор VCID

III.3.4.1 Концепция "Логическое звено"

Идентификатор VCID использует многие PVC, SPVC или SVC для соединения каждой пары устройств MPLS ATM через традиционную сеть [ATM_VCID]. Несмотря на различия между идентификатором VCID и виртуальными магистральными трактами, идентификатор VCID можно использовать в подобных сетевых конфигурациях для виртуальных магистральных трактов. Это было проиллюстрировано рисунком III.1. На рисунке III.5 приводится концепция, которая позволяет непосредственно сравнивать идентификатор VCID с виртуальными магистральными трактами.



a) Соединения для VCID

b) Упрощенное представление как "логического звена" VCID

Рисунок III.5/Y.1310 – Представление соединений VCID в качестве "логических звеньев"

Когда два устройства MPLS ATM (маршрутизаторы ATM LSR или граничные маршрутизаторы LSR ATM) соединяются с помощью идентификатора VCID, требуются многие PVC, SPVC или SVC: одно для сигнализации и многие – для меток MPLS. Однако группа PVC, SPVC или SVC, используемая идентификатором VCID между двумя устройствами MPLS ATM, действует вместо одного звена ATM в сети MPLS ATM. Следовательно, полезно рассматривать эту группу PVC, SPVC или SVC как одно "логическое звено".

На рисунке III.3 показано, как могут быть использованы виртуальные магистральные тракты при введении MPLS в традиционную сеть ATM. "Логические звенья" VCID могут использоваться точно таким же способом, как показано на рисунке III.6. Варианты сетевых структур, показанные на рисунке III.4, также в равной степени применяются с идентификатором VCID.

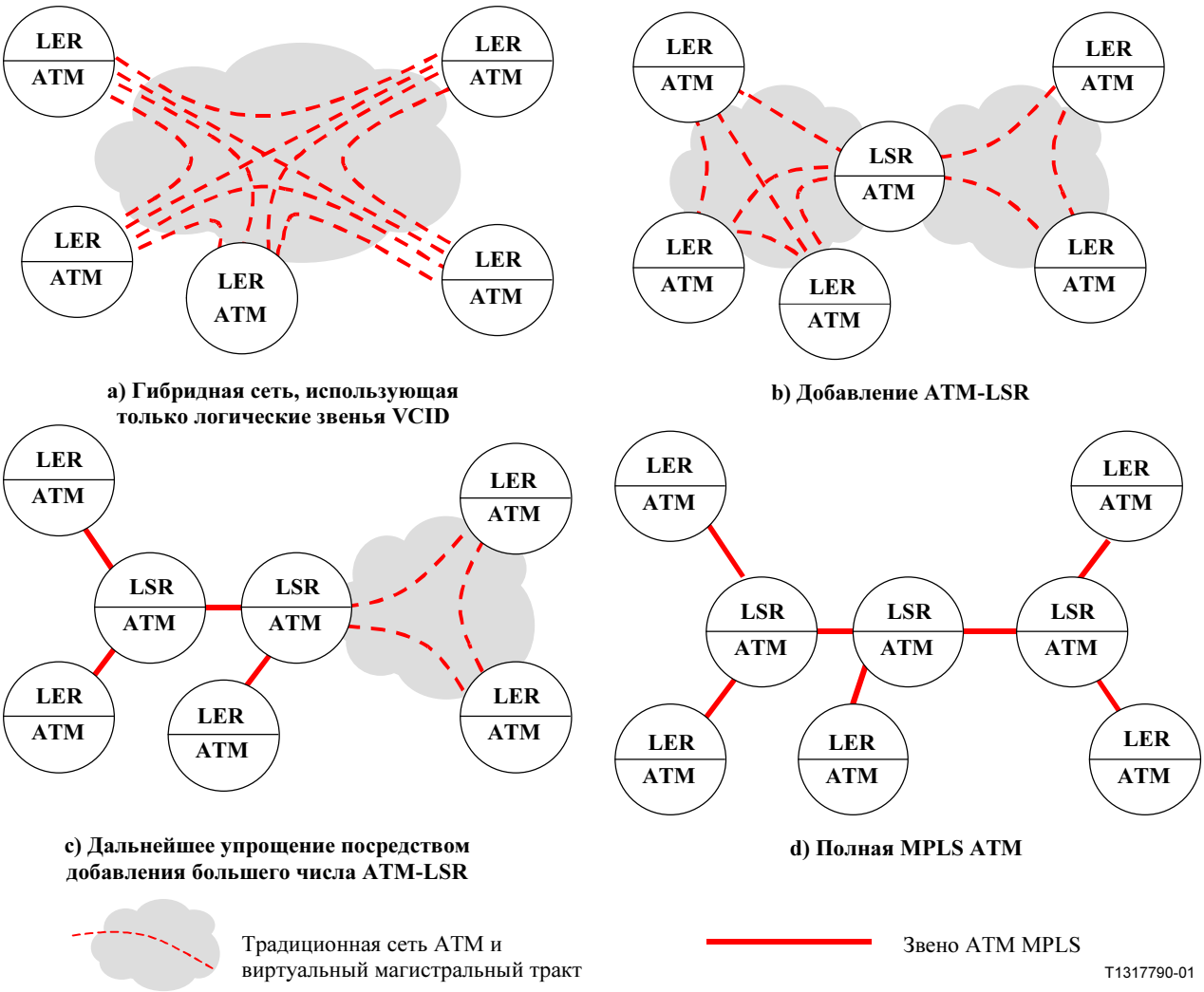


Рисунок III.6/Y.1310 – Сети MPLS ATM, использующие "логические звенья" VCID

III.3.4.2 Поддержка идентификатора VCID в традиционных коммутаторах ATM

Коммутаторы в традиционных сетях ATM должны поддерживать соединения PVC, SPVC или SVC с помощью типов административного управления трафиком Форума ATM или МСЭ-Т, которые совпадают с типами, используемыми в граничных маршрутизаторах LSR. Они не требуются для поддержки сигнализации VCID или каких-либо функций MPLS.

III.3.4.3 Поддержка VCID в граничных маршрутизаторах LSR ATM

Граничные маршрутизаторы LSR ATM должны выполнять следующие требования:

- Они должны поддерживать одну или более карт сетевых интерфейсов ATM.
- Они должны поддерживать VCID в дополнение к протоколам MPLS ATM.

Добавление IV

Примеры методов поддержки IP-VPN в сети общего пользования MPLS/ATM

IV.1 Введение

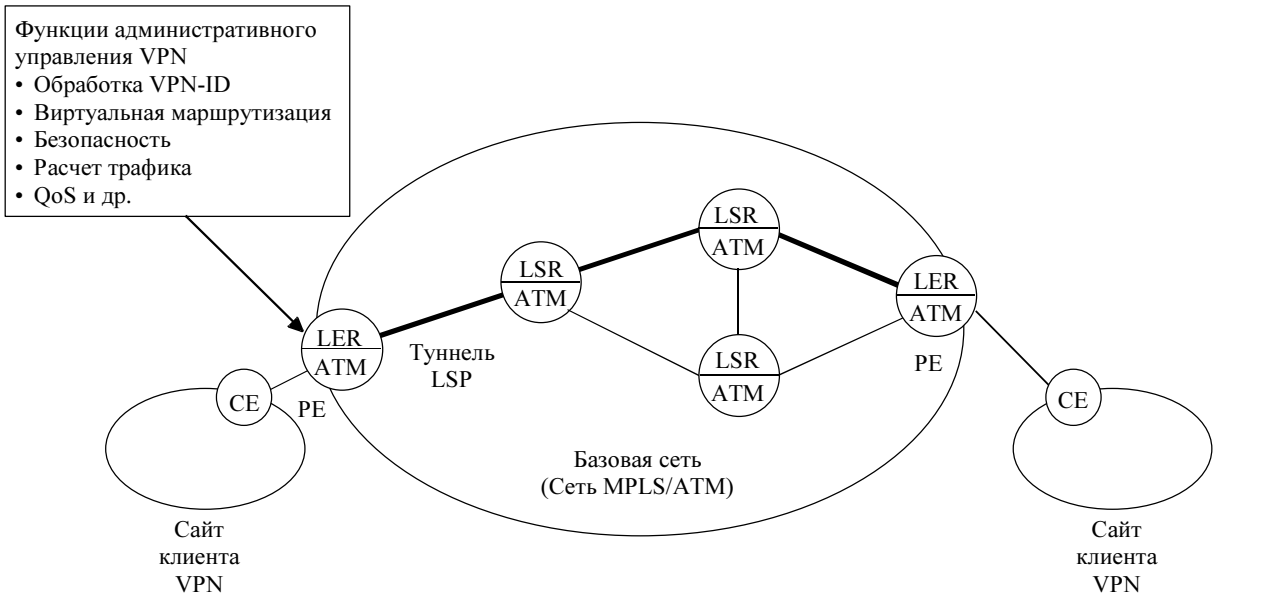
В этом Добавлении описываются примеры методов использования MPLS для обеспечения услуг виртуальной частной сети IP в сети общего пользования. Коммутация MPLS обеспечивает гибкую и расширяемую основу для построения услуг IP-VPN. В подразделе 7.2 определяется услуга IP-VPN и приводятся некоторые требования к услуге.

В [Y.1311.1] также приведены требования и описание архитектурного подхода к IP-VPN на основе MPLS.

Существует понимание того, что поставщики услуг будут реализовать проектные решения по поддержке сетей IP-VPN на основе своих внутренних сетей и требований клиентов. В этом Добавлении описываются примеры методов, и они не ограничивают возможности развертывания сетей VPN внутри транспортной сети.

Хотя концепция IP-VPN реализована на языке поддержки корпоративных клиентов транспортными сетями, те же самые методы могут быть использованы поставщиками услуг для поддержки других поставщиков услуг (например, транспортной сети – другой транспортной сетью).

На рисунке IV.1 показан общий сценарий для сетей IP-VPN:



CE Окончание клиента
LER Граничный маршрутизатор на основе меток
LSR Маршрутизатор с коммутацией на основе меток
PE Окончание поставщика

Рисунок IV.1/Y.1310 – Общий сценарий для сетей IP-VPN, использующих MPLS

Маршрутизатор CE является маршрутизатором окончания клиента, который сопрягает сайт клиента с сетью поставщика услуги. Маршрутизатор PE является маршрутизатором окончания поставщика услуги, который сопрягается с оборудованием CE клиента.

Сайт является набором (под)сетей, которые являются частью сети клиента, и подсоединяется к сети VPN через одно или более звеньев PE/CE. Сеть VPN является набором сайтов, совместно использующих общую информацию маршрутизации. Сайт может быть частью различных сетей VPN.

Рисунок IV.2 иллюстрирует случай, когда поставщик услуги поддерживает многие сети VPN. Как показано на рисунке, один сайт может принадлежать многим сетям VPN. Сайт, принадлежащий многим сетям VPN, согласно стратегии, может или не может обеспечивать транзит между двумя сетями VPN (порядок реализации выходит за рамки этой Рекомендации). Если сайт принадлежит многим сетям VPN, то он должен иметь адресное пространство, которое является уникальным среди сетей VPN.

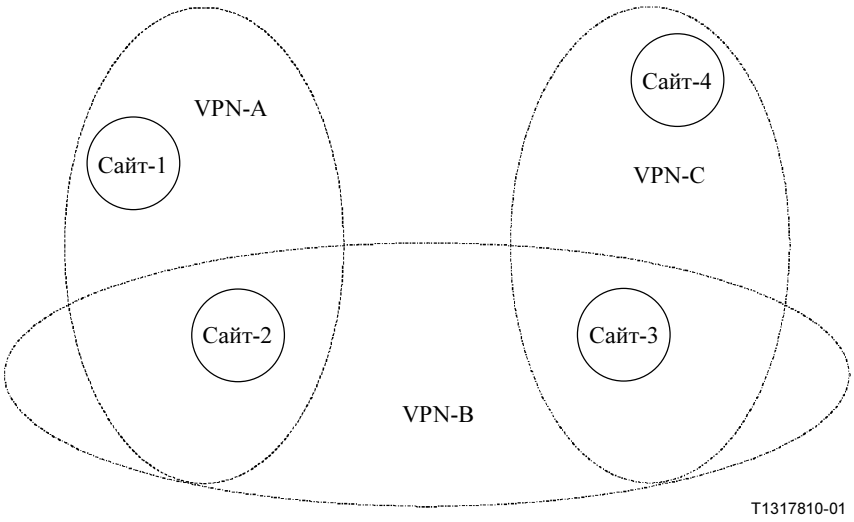


Рисунок IV.2/Y.1310 – Иллюстрация поддержки многих сетей VPN

IV.2 Сценарий 1

В этом подразделе описывается пример метода использования коммутации MPLS для обеспечения услуг IP-VPN в сети общего пользования. Коммутация MPLS и ее протокол LDP обеспечивают очень гибкую и мощную основу для построения услуг IP-VPN. В качестве нормальной операции LDP основная установка тракта LSP выполняется по методу, базирующемуся на топологии. Это основная установка тракта LSP, использующая основную метку. В этом случае для маршрутизации внутри сети VPN используются два уровня создания туннелей тракта LSP (помещение меток в стек).

IV.2.1 Простая сетевая конфигурация

IV.2.1.1 Архитектурный обзор

Рисунок IV.3 иллюстрирует пример конфигурации, составленной из маршрутизаторов LER и LSR для услуг IP-VPN в базовой сети MPLS/ATM.

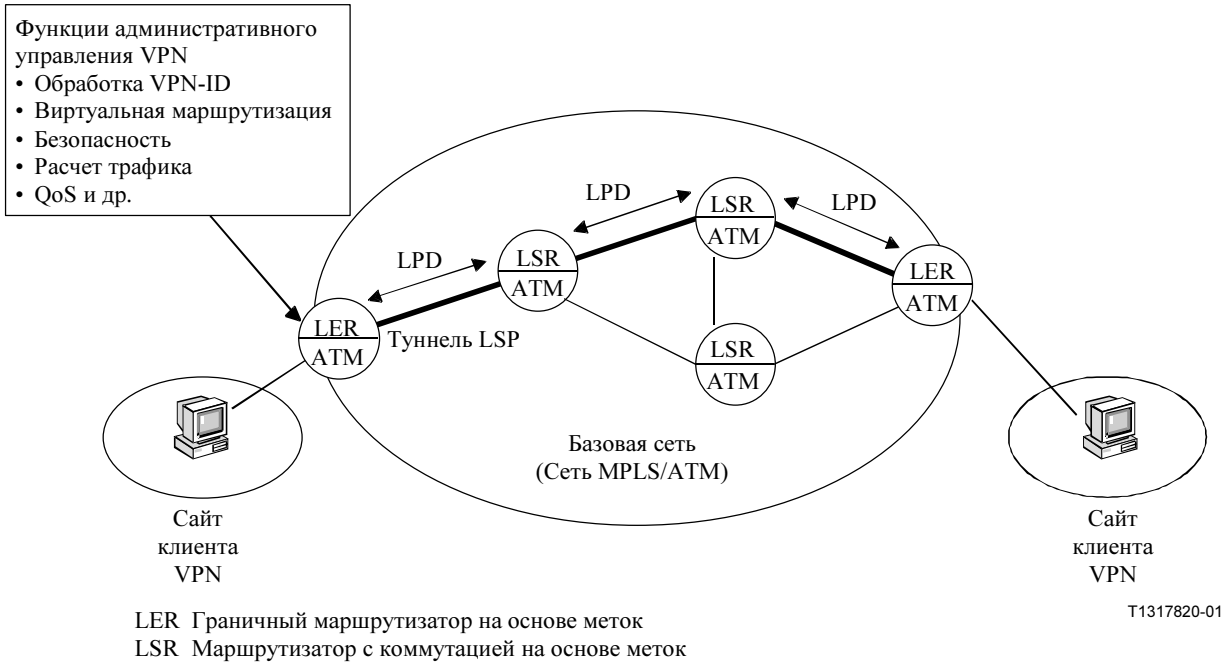


Рисунок IV.3/Y.1310 – Сетевая модель для поддержки IP-VPN в сети общего пользования MPLS/ATM

IV.2.2 Сетевые компоненты

IV.2.2.1 LER (Граничный маршрутизатор на основе меток)

Маршрутизатор LER является пограничным маршрутизатором MPLS, который расположен на границе сети поставщика MPLS/ATM. Эти маршрутизаторы служат в качестве входных и выходных точек туннеля LSP для трафика IP клиентов VPN. Если маршрутизатор LER совместно используется многими клиентами, то ему нужно выполнять виртуальную маршрутизацию, а это означает, что маршрутизатор LER поддерживает отдельные таблицы пересылки для каждой сети VPN, которую он обслуживает, поскольку их пространства адресов IP могут не отличаться.

IV.2.2.2 LSR (Маршрутизатор с коммутацией на основе меток)

Базовая сеть MPLS/ATM является нижележащей сетью поставщика, которая совместно используется услугами сети IP-VPN клиента.

IV.2.2.3 Операции для установления областей IP-VPN

Сетевой поставщик, желающий предложить услугу IP-VPN, сначала должен конфигурировать область MPLS. Область MPLS означает здесь область IP-VPN. Область IP-VPN состоит из маршрутизаторов LER и LSR. В качестве нормальной операции протокола LDP основная установка тракта LSP выполняется по базирующемуся на топологии методу, который определяется как основа, или уровень 1, установки LSP, использующей основную метку. Для маршрутизации внутри VPN используются два уровня организации туннелей LSP (помещение меток в стек).

IV.2.2.4 Обнаружение членства в VPN

Каждый маршрутизатор LER обнаруживает все другие маршрутизаторы LER в области VPN, которая обслуживает одну и ту же сеть IP-VPN. Процесс инициации сеанса LDP используется в качестве метода обнаружения маршрутизаторами LER их равноправных объектов, поскольку конечной задачей схемы является установление второго уровня туннелей MPLS. Каждый маршрутизатор LER посылает приветственное сообщение LDP по каждому тракту LSP основной сети, который выходит из этого маршрутизатора LER. Приветственные сообщения вкладываются с основной меткой MPLS

так, что они переносятся всеми путями к маршрутизатору LER назначения. Приветственное сообщение LDP является формой опроса для определения, находится ли маршрутизатор LER для той же самой сети VPN (равноправный объект) в маршрутизаторе LER назначения. Когда с помощью приветствия регистрируется соседство, то надлежащий маршрутизатор LER продолжает инициировать сеанс LDP со своим равноправным объектом. Один из двух маршрутизаторов LER инициирует соединение TCP с другим маршрутизатором. После установления соединения TCP и осуществления обмена необходимыми начальными сообщениями существует сеанс LDP между равными маршрутизаторами LER. Немедленно после установления сеанса LDP каждый из двух маршрутизаторов LER предлагает другому метку для туннеля LSP к себе. Если туннель LSP является вложенным туннелем, то его метка вводится в стек меток пакетов перед меткой LSP основной сети.

IV.2.2.5 Членство в VPN и распространение информации о достижимости

Маршрутизатор LER узнает префиксы адресов IP сайтов клиентов, с которыми он соединен напрямую, посредством обмена информацией маршрутизации. Маршрутизатору LER нужно найти свои равноправные маршрутизаторы LER. Он должен обнаружить, какие другие маршрутизаторы LER в области VPN обслуживают его сеть VPN. Маршрутизатор LER предлагает установить прямой сеанс LDP с каждым другим маршрутизатором LER в области VPN. Но только маршрутизаторы LER, обслуживающие ту же самую сеть VPN, обнаруживают друг друга и начинают установление сеансов LDP между собой. Сеансы LDP успешно устанавливаются только между маршрутизаторами LER, которые поддерживают одну и ту же сеть VPN.

IV.2.2.6 Достижимость внутри VPN

Первый трафик, который проходит по вложенным туннелям, представляет собой обмен информацией маршрутизации между маршрутизаторами LER. Предполагается, что когда маршрутизатор LER конфигурируется в первый раз для сети IP-VPN, то часть информации конфигурации является протоколом маршрутизации, который следует использовать "внутри сети VPN". Также выдаются какие-либо полномочия по безопасности, которые необходимы для работы в качестве соседнего маршрутизатора других маршрутизаторов LER. После любой фазы открытия схемы маршрутизации "внутри сети VPN" каждый маршрутизатор LER объявляет специфические префиксы адреса клиента сети VPN, достижимого через него.

IV.2.2.7 Пересылка пакетов IP

В результате обмена информацией маршрутизации между маршрутизаторами LER каждый маршрутизатор LER создает таблицу пересылки, которая связывает специфические префиксы адресов клиента сети VPN (FEC: Классы эквивалентности по пересылке) со следующим транзитным участком. Когда прибывают пакеты IP, для которых следующим транзитным участком является маршрутизатор LER, процесс пересылки вставляет сначала метку для равноправного маршрутизатора LER (метка вложенного туннеля). Затем в пакет вставляется базовая метка для первого транзитного участка тракта LSP основной сети, который ведет к маршрутизатору LER. Пакет с двумя метками затем пересылается следующему маршрутизатору LSR в тракте LSP основной сети. Когда пакет прибывает в маршрутизатор назначения LER, самая крайняя метка может быть изменена несколько раз, но вложенная метка не изменяется. Поскольку производится выдвижение меток из стека, то для направления пакета надлежащему маршрутизатору LER используется вложенная метка. В маршрутизаторе LER пространство вложенных меток, используемое каждой сетью VPN, должно быть непересекающимся по отношению ко всем другим сетям VPN, поддерживаемым тем же самым маршрутизатором LER.

IV.3 Сценарий 2

В этом подразделе описывается пример метода использования коммутации MPLS и Протокола многопротокольного пограничного шлюза для обеспечения услуг IP VPN в сети общего пользования, как определено в [BGP_VPN]. В этом подразделе содержится обзор. Подробности можно найти в [BGP_VPN].

IV.3.1 Архитектурный обзор

На рисунке IV.1 показан пример конфигурации, составленной из маршрутизаторов LER и LSR для услуг IP-VPN в базовой сети MPLS/ATM.

На рисунке IV.4 показана сетевая модель, использующая [BGP_VPN].

IV.3.2 Сетевые компоненты

В этом подразделе вводятся сетевые компоненты для поддержки сети IP-VPN и используемая терминология.

IV.3.2.1 Маршрутизатор окончания поставщика (PE)

Маршрутизатор PE является граничным маршрутизатором поставщика услуги, который сопрягается с маршрутизаторами окончаний клиентов (CE). Для целей этой Рекомендации данный маршрутизатор является граничным маршрутизатором LSR (то есть в интерфейсе между клиентом и поставщиком не используется коммутация MPLS).

IV.3.2.2 Маршрутизатор окончания клиента (CE)

Маршрутизатор CE является граничным маршрутизатором окончания клиента, сопрягающимся с маршрутизаторами окончания поставщика услуг (PE). Для целей этого сценария маршрутизатор CE не реализует коммутацию MPLS и является маршрутизатором IP. Оборудование CE не должно поддерживать какие-либо протоколы маршрутизации или сигнализацию, специфические для сети VPN.

IV.3.2.3 Маршрутизатор поставщика (P)

Маршрутизаторы P являются базовыми маршрутизаторами с коммутацией на основе меток.

IV.3.2.4 Сайт

Сайт – это набор (под)сетей, которые являются частью сети клиента и соединяются с сетью VPN через одно или более звеньев PE/CE. Сайт может быть частью различных сетей VPN.

IV.3.2.5 Различитель маршрута

Поставщик назначает каждой сети VPN уникальный идентификатор, называемый различителем маршрута (RD), который является различным для каждой сети Intranet или Exranet внутри сети поставщика. Таблицы пересылки в маршрутизаторах PE содержат называемые адресами VPN-IP уникальные адреса, образованные путем объединения различителя RD с адресами IP клиентов. Адреса VPN-IP являются уникальными для каждой конечной точки в сети поставщика услуги, а записи данных хранятся в таблицах пересылки для каждого узла в сети VPN (то есть каждого маршрутизатора PE в сети VPN).

IV.3.2.6 Модель соединения

На приведенном ниже рисунке IV.4 изображена модель соединения для сети VPN MPLS/BGP.

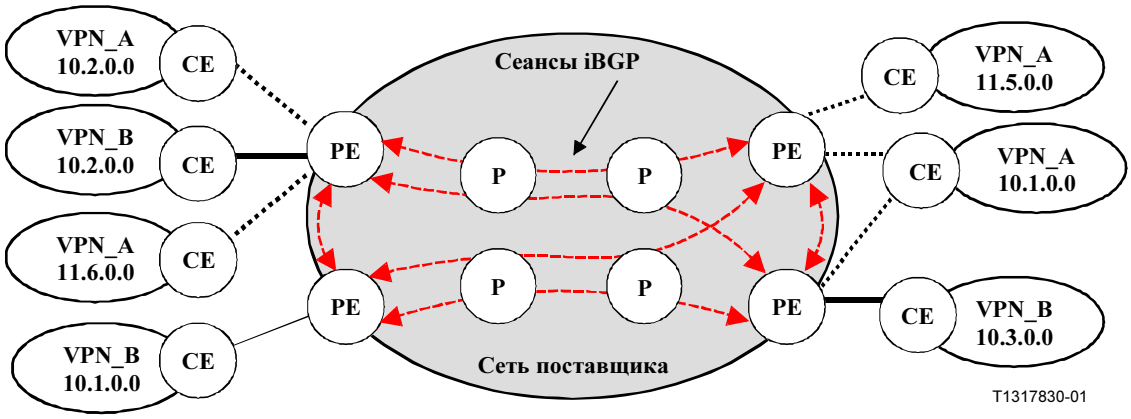


Рисунок IV.4/Y.1310 – Модель соединения для сетей IP/VPN, использующих MPLS/BGP

Маршрутизаторы P находятся в базовой сети MPLS. Маршрутизаторы PE используют коммутацию MPLS для осуществления связи с базовой сетью MPLS и маршрутизацию IP для осуществления связи с маршрутизатором CE. Маршрутизаторы P и PE используют протокол маршрутизации IP (внутренний протокол шлюза) для установления маршрутов IP через базовую часть MPLS и LDP для распространения меток между маршрутизаторами.

Маршрутизаторы PE используют многопротокольный протокол BGP-4 для осуществления связи между собой с целью обмена метками и реализации политики для каждой сети VPN. Маршрутизаторы PE являются полносвязными согласно протоколу BGP (пока не используется отражатель маршрута). Более точно, поскольку PE находятся в той же самой автономной системе, они используют внутренний протокол BGP (iBGP).

Маршрутизаторы P не функционируют по протоколу BGP и не обладают каким-либо знанием о сети VPN. Они используют нормальные протоколы и процедуры MPLS.

Маршрутизаторы PE могут обмениваться маршрутами IP с маршрутизаторами CE через протокол маршрутизации IP. Также могут использоваться статические маршруты. Между маршрутизаторами CE и PE используются нормальные процедуры маршрутизации. Маршрутизатор CE не должен реализовать коммутацию MPLS или обладать каким-либо конкретным знанием о сети VPN.

Маршрутизаторы PE распределяют маршруты клиентов к другим маршрутизаторам PE через iBGP. Адрес VPN-IP (образованный из различителя маршрута и адреса IPv4) используется в протоколе BGP для распределения маршрутов. Таким образом, различные сети VPN могут использовать перекрывающееся адресное пространство IPv4 без дублирования адресов VPN-IP.

Маршрутизаторы PE отображают маршруты, ставшие известными из протокола BGP, в свои таблицы маршрутизации для пересылки пакетов, принятых от маршрутизаторов CE, в надлежащий тракт LSP.

Используются два уровня меток. Внутренняя метка используется для определения надлежащей сети VPN к маршрутизатору PE. Внешняя метка используется маршрутизаторами LSR в сети MPLS, чтобы направлять пакеты к надлежащему окончанию PE.

IV.3.2.7 Операции для установления областей IP-VPN

Сетевой поставщик, желающий предложить услугу IP-VPN, должен разработать и обеспечить сеть, соответствующую требованиям к связности.

Каждое окончание PE должно быть конфигурировано для сетей VPN, которые оно должно поддерживать, и для сетей VPN, к которым принадлежит каждое присоединенное окончание CE. Равноправные отношения по протоколу iBGP должны быть конфигурированы между маршрутизаторами PE в сети MPLS или в отражателе маршрута. Могут быть использованы нормальные возможности расширяемости iBGP.

Для осуществления связи с окончанием CE должна быть установлена нормальная конфигурация протокола маршрутизации.

Для организации связи с базовой сетью MPLS должна быть установлена нормальная конфигурация MPLS (LDP, IGP и т. д.).

Маршрутизаторы P не следует конфигурировать для поддержки сети VPN (за пределами нормальной поддержки MPLS).

IV.3.2.8 Членство в VPN и распространение информации о достижимости

Окончанию PE становятся известны префиксы адресов IP сайтов клиентов, к которым оно непосредственно подсоединено, в результате обмена информацией о маршрутизации через протокол маршрутизации IP или через конфигурацию (статические маршруты).

Окончание PE обменивается префиксами адресов VPN-IP со своими равноправными объектами BGP, чтобы узнать маршруты к сайтам назначения сети VPN. Окончание PE также обменивается метками через протокол BGP со своими равноправными маршрутизаторами PE, чтобы определять тракт LSP, используемый для обеспечения связности между маршрутизаторами PE. Эти метки используются как метки второго уровня, и маршрутизаторы P их не обнаруживают.

Маршрутизаторы PE ведут отдельные таблицы маршрутизации и пересылки для каждой сети VPN, которую они поддерживают. Каждый маршрутизатор CE, присоединенный к маршрутизатору PE, использует соответствующую таблицу маршрутизации, основанную на интерфейсе, к которому он присоединен.

IV.3.2.9 Пересылка пакетов IP

В результате обмена информацией маршрутизации между окончаниями PE каждое окончание PE составляет таблицу пересылки на каждую сеть VPN, которая связывает специфические для клиентов VPN префиксы адресов с маршрутизаторами PE следующего транзитного участка.

Когда от маршрутизатора CE прибывают пакеты IP, маршрутизатор PE проверяет таблицу пересылки для сети VPN, определяемой этим интерфейсом. Если совпадение найдено, то маршрутизатор продолжает следующим образом:

- Если следующим транзитным участком является маршрутизатор PE, то процесс пересылки сначала выдвигает метку для равноправного маршрутизатора PE (вложенная метка туннеля), определенного с помощью маршрутной таблицы.
- Затем маршрутизатор PE продвигает основную метку в пакет для первого транзитного участка тракта LSP основной сети, который ведет к маршрутизатору PE назначения. Пакет с двумя метками затем пересылается к следующему маршрутизатору LSR в тракте LSP основной сети.
- Маршрутизаторы P (маршрутизаторы LSR) используют метки верхнего уровня и свои маршрутные таблицы для направления пакета к PE назначения.

- Когда пакет прибывает к маршрутизатору PE назначения, крайняя метка может быть изменена несколько раз, но вложенная метка не изменяется.
- Когда маршрутизатор PE получает пакет, он использует встроенную метку для определения сети VPN. В маршрутизаторе PE пространство вложенной метки, используемое каждой сетью VPN, должно быть не пересекающимся со всеми другими сетями VPN, поддерживаемыми этим же маршрутизатором PE. Маршрутизатор PE проверяет маршрутную таблицу, связанную с этой сетью VPN, чтобы определить, через какой интерфейс передавать пакет.

Если в маршрутной таблице VPN совпадение не найдено, то маршрутизатор PE для возможности выбора маршрута проверяет маршрутную таблицу Интернет (если эта возможность предоставляется поставщиком). Если маршрут не найден, то пакет отбрасывается.

Таблицы пересылки VPN-IP содержат метки, которые соответствуют адресам VPN-IP. Эти метки направляют трафик к каждому сайту в сети VPN. Поскольку метки используются вместо адресов IP, то клиенты могут иметь свои частные схемы адресации внутри корпоративной сети Интернет без необходимости Преобразования сетевого адреса (NAT) для пропуска трафика через сеть поставщика. Трафик разделяется между сетями VPN посредством использования логически различных таблиц пересылки для каждой сети VPN. На основе входящего интерфейса коммутатор выбирает конкретную таблицу пересылки, в которой благодаря использованию протокола BGP содержатся только действительные пункты назначения в сети VPN. Чтобы создать сети Extranet, поставщик явно конфигурирует достижимость между сетями VPN. (Могут потребоваться конфигурации NAT.)

IV.3.2.10 Безопасность

Внутри сети поставщика различители маршрутов с помощью маршрутизатора PE связаны с каждым пакетом, поэтому пользователь не может "обманным путем" направить поток или пакет в сеть VPN другого клиента. Отметим, что различители маршрутов не переносятся в пакетах данных пользователей. Пользователи могут участвовать в Intranet или Extranet, только если они находятся на надлежащем физическом порте и имеют надлежащие различители маршрутов, конфигурированные в маршрутизаторе PE. Эта установка делает практически невозможным вхождение в сеть и обеспечивает те же самые уровни безопасности, к которым пользователи привыкли в услугах ретрансляции кадров, арендованных линий или ATM.

ЛИТЕРАТУРА

Это Добавление содержит явные ссылки, которые введены в документы RFC, перечисленные в 2.1.2. Введенные ссылки, которые уже включены в качестве основных ссылок, не повторяются в этом Добавлении.

[1] POSTEL (J.): DoD Standard – Internet Protocol, *RFC 760, USC/Information Sciences Institute*, January 1980.

[2] POSTEL (J.): DoD Standard – Transmission Control Protocol, *RFC 761, USC/Information Sciences Institute*, January 1980.

[3] POSTEL (J.): Internet Control Message Protocol – DARPA Internet Program Protocol Specification, *RFC 792, USC/Information Sciences Institute*, September 1981.

[4] POSTEL (J.): Service Mappings, *RFC 795, USC/Information Sciences Institute*, September 1981.

[5] POSTEL (J.): Address Mappings, *RFC 796, USC/Information Sciences Institute*, September 1981.

[6] BRADEN (R.): Requirements for Internet Hosts – Communication Layers, *STD 3, RFC 1122*, October 1989.

[7] RIVEST (R.): The MD5 Message-Digest Algorithm, *RFC 1321*, April 1992.

[8] ALMQUIST (P.): Type of Service in the Internet Protocol Suite, *RFC 1349*, July 1992.

[9] BRADLEY (T.), BROWN (C.), MALIS (A.): Multiprotocol Interconnect over Frame Relay, *RFC 1490*, July 1993.

[10] MOY (J.): OSPF Version 2, *RFC 1583, Proteon Inc*, March 1994.

[11] SIMPSON (W.): The Point-to-Point Protocol (PPP), *STD 51, RFC 1661*, July 1994.

[12] REYNOLDS (J.), POSTEL (J.): Assigned Numbers, *RFC 1700*, October 1994.

[13] REKHTER (Y.), LI (T.): A Border Gateway Protocol 4 (BGP-4), *RFC 1771*, March 1995.

[14] BAKER (F.), Editor: Requirements for IP Version 4 Routers, *RFC 1812*, June 1995.

[15] SCHULZRINNE (H.), CASNER (S.), FREDERICK (R.), JACOBSON (V.): RTP: A Transport Protocol for Real-Time Applications, *RFC 1889*, January 1996.

[16] McCANN (J.), MOGUL (J.), DEERING (S.): Path MTU Discovery for IP version 6, *RFC 1981*, August 1996.

[17] BRADNER (S.): Key words for use in RFCs to Indicate Requirement Levels, *BCP 14, RFC 2119*, March 1997.

[18] BRADEN (R.) et al.: Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification, *RFC 2205*, September 1997.

[19] WROCLAWSKI (J.): The use of RSVP with IETF Integrated Services, *RFC 2210*, September 1997.

[20] WROCLAWSKI (J.): Specification of the Controlled-Load Network Element Service, *RFC 2211*, September 1997.

[21] SHENKER (S.), WROCLAWSKI (J.): General Characterization Parameters for Integrated Service Network Elements, *RFC 2215*, September 1997.

[22] SHENKER (S.), WROCLAWSKI (J.): Network Element Service Specification Template, *RFC 2216*, September 1997.

[23] HINDEN (R.), DEERING (S.): IP Version 6 Addressing Architecture, *RFC 2373*, July 1998.

[24] HEFFERNAN (A.): Protection of BGP Sessions via the TCP MD5 Signature Option, *RFC 2385*, August 1998.

[25] KENT (S.), ATKINSON (R.): Security Architecture for the Internet Protocol, *RFC 2401*, November 1998.

[26] KENT (S.), ATKINSON (R.): IP Authentication Header, *RFC 2402*, November 1998.

[27] KENT (S.), ATKINSON (R.): IP Encapsulating Security Protocol (ESP), *RFC 2406*, November 1998.

[28] NARTEN (T.), ALVESTRAND (H.): Guidelines for Writing an IANA Considerations Section in RFCs, *RFC 2434*, October 1998.

[29] DEERING (S.), HINDEN (R.): Internet Protocol, Version 6 (IPv6) Specification, *RFC 2460*, December 1998.

[30] CONTA (A.), DEERING (S.): Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, *RFC 2463*, December 1998.

[31] AWDUCHE (D.) et al.: Requirements for Traffic Engineering Over MPLS, *RFC 2702*, September 1999.

[32] POSTEL (J.): Internet Name Server, *USC/Information Sciences Institute, IEN 116*, August 1979.

[33] SOLLINS (K.): The TFTP Protocol, *Massachusetts Institute of Technology, IEN 133*, January 1980.

[34] CERF (V.): The Catenet Model for Internetworking, *Information Processing Techniques Office, Defense Advanced Research Projects Agency, IEN 48*, July 1978.

[35] BBN Technical Report 1822, *Specification for the Interconnection of a Host and an IMP*, Bolt, Beranek, and Newman, Revised May 1978.

[36] SHOCH (J.): Inter-Network Naming, Addressing, and Routing, *COMPCON, IEEE Computer Society*, Fall 1978.

[37] SHOCH (J.): Packet Fragmentation in Inter-Network Protocols, *Computer Networks, Vol. 3*, *No. 1*, February 1979.

[38] STRAZISAR (V.): How to Build a Gateway, *IEN 109, Bolt, Beranek and Newman*, August 1979.

[39] CERF (V.), KAHN (R.): A Protocol for Packet Network Intercommunication, *IEEE Transactions on Communications*, Vol. COM-22, No. 5, pp. 637-648, May 1974.

[40] DALAL (Y.), SUNSHINE (C.): Connection Management in Transport Protocols, *Computer Networks*, Vol. 2, No. 6, pp. 454-473, December 1978.

[41] DEMERS (A.), KESHAV (S.), SHENKER (S.): Analysis and Simulation of a Fair Queueing Algorithm, in *Internetworking: Research and Experience*, Vol. 1, No. 1, pp. 3-26.

[42] ZHANG (L.): Virtual Clock: A New Traffic Control Algorithm for Packet Switching Networks, in *Proc. ACM SIGCOMM '90*, pp. 19-29.

[43] VERMA (D.), ZHANG (H.), FERRARI (D.): Guaranteeing Delay Jitter Bounds in Packet Switching Networks, in *Proc. Tricomm '91*.

[44] GEORGIADIS (L.), GUERIN (R.), PERIS (V.), SIVARAJAN (K.N.): Efficient Network QoS Provisioning Based on per Node Traffic Shaping, *IBM Research Report No. RC-20064*.

[45] GOYAL (P.), LAM (S.S.), VIN (H.M.): Determining End-to-End Delay Bounds in Heterogeneous Networks, *Proc. 5th Intl. Workshop on Network and Operating System Support for Digital Audio and Video*, April 1995.

[46] FLOYD (S.), JACOBSON (V.): Link-sharing and Resource Management Models for Packet Networks, *IEEE/ACM Transactions on Networking*, Vol. 3, No. 4, pp. 365-386, August 1995.

[47] SHREEDHAR (M.), VARGHESE (G.): Efficient Fair Queueing using Deficit Round Robin, *Proc. ACM SIGCOMM 95*, 1995.

[48] BENNETT (J.), ZHANG (Hui): Hierarchical Packet Fair. Queueing Algorithms, *Proc. ACM SIGCOMM 96*, August 1996.

[49] STILIADIS (D.), VARMA (A.): Rate-Proportional Servers: A Design Methodology for Fair Queueing Algorithms, *IEEE/ACM Trans. on Networking*, April 1998.

[50] CONTA (A.), DOOLAN (P.), MALIS (A.): Use of Label Switching on Frame Relay Networks, *RFC 3034*, January 2001.

[51] NIKOLAOU (N.), RIGOLIO (G.), CASACA (A.), CIULLI (N.), STASSINOPOULOS (G.): Integration of IP and ATM for QoS and Multimedia Support, *4th International Distributed Conference (ICD 1999)*, 22-23 September 1999, Madrid, Spain.

[52] IETF RFC 2208 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Applicability Statement – Some Guidelines on Deployment*.

[53] IETF RFC 3260 (2002), *New Terminology and Clarifications for Diffserv*.

[54] IETF RFC 3496 (2003), *Protocol Extension for Support of Asynchronous Transfer Mode (ATM) Service Class-aware Multiprotocol Label Switching (MPLS) Traffic Engineering*.

[55] IETF RFC 2382 (1998), *A Framework for Integrated Services and RSVP over ATM.*

[56] IETF RFC 3215 (2002), *LDP State Machine*.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия B	Средства выражения: определения, символы, классификация
Серия C	Общая статистика электросвязи
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	TMN и техническое обслуживание сетей: международные системы передачи, телефонные, телеграфные, факсимильные и арендованные каналы
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных и взаимосвязь открытых систем
Серия Y	**Глобальная информационная инфраструктура, аспекты межсетевого протокола (IP) и сети следующих поколений**
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Женева, 2005 г.