Министерство образования и науки Российской Федерации

**ГОУ ВПО «Тамбовский государственный технический университет»**

**Н.А. КОЛЬТЮКОВ, О.А. БЕЛОУСОВ**

# СЕТЕВЫЕ ТЕХНОЛОГИИ

*Рекомендовано Учебно-методическим объединением по образованию в области радиотехники, электроники, биомедицинской техники и автоматизации в качестве учебного пособия для студентов, обучающихся по направлениям 210200 – Проектирование и технология электронных средств и 210300 – Радиотехника*


Тамбов
Издательство ТГТУ
2009

УДК 004.7(075)
ББК з841я73
К625

Рецензенты:

Доктор технических наук, профессор ТГТУ
*П.С. Беляев*

Кандидат технических наук, доцент
начальник кафедры «Радиосвязь (авиационная)» ТВВАИУРЭ(ВИ),
*Ю.И. Лёвочкин*

**Кольтюков, Н.А.**
К625 Сетевые технологии : учебное пособие / Н.А. Кольтюков, О.А. Белоусов. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2009. – 100 с. – 100 экз. – ISBN 978-5-8265-0843-5.

Представлены основные сведения о маршрутизации, базовых протоколах маршрутизации и коммутации, а также перспективные интегрированные протоколы коммутации четвёртого уровня, стандарты IEEE 802.1Q и IEEE 802.1P. Рассмотрены приоритеты и классы обслуживания в сетях, протоколы реального времени RTP и RSVP, вопросы безопасности корпоративных сетей.

Предназначено для студентов, бакалавров и магистров, обучающихся по направлениям 210200 – Проектирование и технология РЭС и 210300 – Радиотехника.

УДК 004.7(075)
ББК з841я73

**ISBN 978-5-8265-0843-5**

Учебное издание

КОЛЬТЮКОВ Николай Александрович,
БЕЛОУСОВ Олег Андреевич

# СЕТЕВЫЕ ТЕХНОЛОГИИ

Учебное пособие

Редактор Т.М. Глинкина
Инженер по компьютерному макетированию Т.Ю. Зотова

Подписано в печать 22.09.2009
Формат 60 × 84/16. 5,81 усл. печ. л. Тираж 100 экз. Заказ № 376

Издательско-полиграфический центр
Тамбовского государственного технического университета
392000, Тамбов, Советская, 106, к. 14

# ВВЕДЕНИЕ

Сетевые технологии представляют собой одно из направлений развития систем обработки данных, которое возникло в связи с необходимостью объединения территориально рассредоточенных вычислительных средств в единую систему. Сетевые технологии обеспечивают пользователю широкий набор услуг и позволяют создавать целый ряд различных по назначению автоматизированных систем распределённой обработки информации.

Наиболее значимыми технологиями обработки передаваемых данных (пакетов) являются коммутация и маршрутизация. До недавнего времени эти два понятия имели абсолютно разные значения – как по технологии обработки пакетов, так и по уровням модели OSI, на которых работают оба эти метода управления данными в сети, – и не могло быть и речи, чтобы объединить эти понятия. Сегодня развитие сетевых технологий идёт быстрыми темпами. Всё возрастающий объём передаваемой информации, физический рост сетей и межсетевого трафика подстегивают производителей к выпуску всё более мощных и «умных» устройств, использующих новые (совсем новые или комбинации традиционных) методы передачи и сортировки данных, а также коммутации и маршрутизации, и методы их комбинирования для оптимизации межсетевого трафика и увеличения производительности.

# Глава 1. УРОВНИ МОДЕЛИ OSI

## 1.1. УРОВНИ МОДЕЛИ АРХИТЕКТУРЫ ОТКРЫТЫХ СИСТЕМ

В настоящее время общепринятой является семиуровневая модель архитектуры открытых систем (Open System Interconnection, OSI). В этой модели рассматриваются [1]:

1. Физический уровень (управление физическим каналом).
2. Канальный уровень (управление информационным каналом).
3. Сетевой уровень (управление сетью).
4. Транспортный уровень (управление передачей).
5. Сеансовый уровень (управление сеансом).
6. Представительный уровень (управление представлением).
7. Прикладной уровень (управление сервисом).

Какие же задачи решаются на различных уровнях протоколов открытых систем? Рассмотрим этот вопрос несколько подробнее.

**Прикладной уровень.** В модели OSI прикладная программа, которой нужно выполнить конкретную задачу (например, обновить базу данных на компьютере B), посылает конкретные данные в виде дейтаграммы на прикладной уровень. Одна из основных «обязанностей» этого уровня – определить, как следует обрабатывать запрос прикладной программы, иными словами – какой вид должен принять данный запрос. Если в запросе прикладной программы определён, например, дистанционный ввод заданий, то это потребует работы нескольких программ, которые будут собирать информацию, организовывать её, обрабатывать и посылать по соответствующему адресу. Ещё одна важная функция прикладного уровня – электронная почта.

**Виды сервиса прикладного уровня.** Прикладной уровень содержит несколько так называемых общих элементов прикладного сервиса (ACSE – Application Common Service Elements) и специальных элементов прикладного сервиса (SASE – Specific Application Service Elements). Сервисы ACSE предоставляются прикладным процессам во всех системах. Они включают, например, требование определённых параметров качества сервиса.

Допустим, необходимо установить связь через модем по глобальной сети между рабочей станцией локальной сети в Лос-Анджелесе и мэйнфреймом в Бостоне. Поскольку качество телефонной линии иногда оказывается неудовлетворительным, прикладной процесс, работающий в ЛВС, может запросить такое качество сервиса, которое предусматривает подтверждение приёма и распознавания информации.

Если провести аналогию с почтой, то указанное действие равносильно требованию, чтобы доставка вашей посылки подтверждалась квитанцией.

Специальные элементы прикладного сервиса (SASE) обеспечивают сервис для конкретных прикладных программ, таких как программы пересылки файлов и эмуляции терминалов. Если, например, прикладной программе необходимо переслать файлы, то обязательно будет использован протокол передачи, доступа и управления файлами (FTAM – File Transfer, Access and Management), являющийся одним из ключевых протоколов прикладного уровня.

Давайте на минутку заглянем в будущее, когда локальные сети и мэйнфреймы станут работать с OSI-совместимым программным обеспечением. Поскольку FTAM работает как виртуальный банк файлов и имеет собственную службу каталогов, то программы смогут получать доступ к базам данных, не имея информации о фактическом местонахождении файла. Поскольку FTAM поддерживает широкое разнообразие различных типов структур, включая последовательную, упорядоченную иерархическую и общую иерархическую, то информация из базы данных, расположенной на удалённом Unisys-компьютере, будет использоваться для обновления другой базы данных, работающей в локальной сети в другом городе. Данные из первой базы, в свою очередь, будут обновляться на основе информации, взятой из третьей базы данных, размещённой на IBM-мэйнфрейме.

Ещё одна важная составляющая SASE прикладного уровня – сервис виртуального терминала (VT – Virtual Terminal). VT – это сложный сервис, который освобождает компьютер от необходимости посылать соответствующие сигналы для обращения ко всем терминалам, подключённым ко второму компьютеру. Первый компьютер может использовать набор параметров виртуального терминала, а решение вопросов конкретизации конфигурации терминалов можно предоставить второму компьютеру.

На разных этапах разработки находятся ещё несколько SASE: обработка транзакций (trunks actions), электронный обмен данными (EDI – Electronic Data Interchange), передача и обработка заданий (JTM – Job Transfer and Manipulation). Разработка стандарта OSI на EDI, в частности, очень важна для пользователей ЛВС. Например, на рабочей станции ЛВС можно составить заказ на покупку и передать эту информацию по сети непосредственно изготовителю или продавцу, где данные будут автоматически внесены в счёт-фактуру. Можно проверять и автоматически корректировать инвентаризационные ведомости, можно заключать договора на поставку товаров – и всё это без бумаг и волокиты.

**Функции управления сетями на прикладном уровне.** По мере усложнения информационных сетей вопрос административного управления ими приобретает всё большее значение. Поскольку сейчас любые системы передачи информации позволяют обрабатывать и передавать также и речевые данные, а локальные сети всё теснее связываются с глобальными сетями и мэйнфреймами, то всё очевиднее необходимость в разработке эффективного метода организации этой информации и управления ею. Фирма IBM в качестве решения предложила свои системы NetView и NetView/PC, а Hewlett-Packard вышла на рынок с пакетом прикладных программ OpenView.

На сегодняшний день проблема заключается в том, что при наличии нескольких решений нет международного стандарта по управлению сетями. Для прикладного уровня модели OSI существует несколько спецификаций информационно-управляющих протоколов, которые претендуют на то, чтобы в будущем стать международными стандартами. Вопросы, касающиеся разработки международных стандартов по управлению сетями, будут рассмотрены позже.

**Уровень представления данных.** Уровень представления данных отвечает за физическое отображение (представление) информации. Так, в полях базы данных информация должна быть представлена в виде букв и цифр, а зачастую – и графических изображений. Обрабатывать же эти данные нужно, например, как числа с плавающей запятой.

Уровень представления данных обеспечивает возможность передачи данных с гарантией, что прикладные процессы, осуществляющие обмен информацией, смогут преодолеть любые синтаксические различия. Для того чтобы обмен имел место, эти два процесса должны использовать общее представление данных или язык.

Важность уровня представления данных заключается в том, что в основу его работы положена единая для всех уровней модели OSI система обозначений для описания абстрактного синтаксиса – ASN.1. Эта система служит для описания структуры файлов. На прикладном уровне система ASN.1 применяется и для выполнения всех операций пересылки файлов, и при работе с виртуальным терминалом. Использование этой системы позволяет также решить одну из важнейших проблем, возникающих при управлении крупными сетями, – проблему шифрования данных. Шифрование данных с помощью ASN.1 можно выполнять на уровне представления данных; разработка стандарта OSI для этого уровня окажет значительное влияние на обеспечение межмашинной связи.

**Сеансовый уровень.** Представьте себе опытного администратора, отвечающего за подготовку и согласование всех деталей предстоящей важной встречи двух высокопоставленных руководителей. Если он действует правильно, встреча проходит чётко и организованно. Аналогично и работа сеансового уровня обеспечивает проведение сеанса и в конечном итоге обмен информацией между двумя прикладными процессами.

Сеансовый уровень отвечает за такие серьезные вопросы, как режим передачи и установка точек синхронизации. Иными словами, на этом уровне определяется, какой будет передача между двумя прикладными процессами: полудуплексной (процессы будут передавать и принимать данные по очереди) или дуплексной (процессы будут передавать и принимать данные одновременно). В полудуплексном режиме сеансовый уровень выдаёт тому процессу, который первым начинает передачу, маркер данных. Когда второму процессу приходит время отвечать, маркер данных передаётся ему. Сеансовый уровень, таким образом, разрешает передачу только той стороне, которая обладает маркером данных.

Синхронизирующие точки представляют собой точки внутри «диалога», в которых сеансовый уровень проверяет наличие фактического обмена.

Ещё одна функция сеансового уровня модели OSI заключается в решении вопроса о восстановлении связи в случае её нарушения. Например, логично было бы ставить точки синхронизации между страницами текста и в случае нарушения связи начинать передачу с последней синхронизирующей точки. Таким образом, для восстановления сеанса не нужно будет начинать всё сначала и повторять передачу текста, который уже принят правильно.

Сеансовый уровень, кроме того, отвечает за детали, связанные с упорядоченным («плавным») завершением соединения в конце сеанса. Могут возникнуть и ситуации, когда требуется безусловное («резкое») завершение. Это необходимо в тех случаях, когда одна из сторон прекращает обмен и отказывается с этого момента принимать данные.

Сеансовый уровень обрабатывает не все запросы на соединения. Он может выдать примитив отказа от соединения, если определит, что соединение приведёт к перегрузке сети или что затребованный прикладной процесс отсутствует.

**Транспортный уровень.** Транспортный уровень имеет большое значение для пользователей компьютерных сетей, поскольку именно он определяет качество сервиса, которое необходимо обеспечить посредством сетевого уровня. Для того чтобы лучше понять функции транспортного уровня, представим его как аналогию набора специальных услуг, которые местное почтовое отделение предоставляет клиентам за дополнительную плату. Например, заплатив некоторую сумму, клиент может получить квитанцию о том, что письмо доставлено по указанному им адресу. Можно заказать срочную доставку, если клиент желает, чтобы его посылка пришла, к примеру, в Бостон на следующий день. Плату за эти дополнительные высококачественные услуги почтовое ведомство США взимает с клиентов деньгами, а для пользователя сети, работающего с OSI-совместимыми аппаратными и программными средствами, эта плата выражается в дополнительных битах, необходимых для предоставления информации о статусе возможных дополнительных услуг.

На транспортном уровне предусмотрено три типа сетевого сервиса. Сервис типа А предоставляет сетевые соединения с приемлемым для пользователей количеством необнаруживаемых ошибок и приемлемой частотой сообщений об обнаруженных ошибках. Сервис типа В отличается приемлемым количеством необнаруживаемых ошибок, но неприемлемой частотой сообщений об обнаруженных ошибках. Наконец, сервис типа С предоставляет сетевые соединения с количеством необнаруженных ошибок, не приемлемым для сеансового уровня.

Возникает вопрос: а для чего вообще нужны классы сервиса с неприемлемым количеством ошибок? Ответ состоит в том, что для установки многих сетевых соединений необходимы дополнительные протоколы, обеспечивающие обнаружение и устранение ошибок на достаточном для нормальной работы уровне, и на транспортном уровне такой сервис просто не нужен.

Транспортный уровень, тем не менее, предоставляет программистам возможность писать программы для прикладного уровня в самых различных сетях, не обращая внимания на то, надёжна ли передача по этим сетям или нет. Некоторые называют три верхних уровня модели OSI «пользователями транспортного уровня», а четыре нижних – «поставщиками транспортного уровня».

Существует пять классов сервиса транспортного протокола (табл. 1.1).

Класс 0, известный как телекс, представляет собой сервис с самым низким качеством. В этом классе сервиса предусматривается, что управление потоком данных осуществляет сетевой уровень (под транспортным уровнем). Транспортный уровень разрывает соединение, когда аналогичную операцию выполняет сетевой уровень. Сервис класса 1 был разработан CCITT для стандарта X.25 на сети с коммутацией

пакетов. Он обеспечивает передачу срочных данных, однако управление потоком все равно осуществляется на сетевом уровне.

Класс 2 – это модифицированный класс 0. Уровень сервиса этого класса базируется на предположении о том, что сеть обладает высокой надёжностью. Предлагаемое качество сервиса предусматривает возможность мультиплексирования множества транспортных соединений из одного сетевого соединения. Класс 2 обеспечивает необходимую сборку мультиплексированных пакетов данных, прибывающих неупорядоченными.

### 1.1. Пять классов сервиса транспортного протокола

| Класс | Наименование | Тип |
|---|---|---|
| 0 | Простой | A |
| 1 | Устранение основных ошибок | B |
| 2 | Мультиплексирование | A |
| 3 | Обнаружение ошибок и мультиплексирование | B |
| 4 | Обнаружение и устранение ошибок | C |

Класс 3 обеспечивает виды сервиса, предлагаемые уровнями 1 и 2, а в случае обнаружения ошибки предоставляет возможность ресинхронизации для переустановления соединения.

Класс 4 предполагает, что сетевому уровню присуща надёжность, поэтому он предлагает обнаружение и устранение ошибок.

**Сетевой уровень.** На сетевом уровне осуществляется сетевая маршрутизация. Этот уровень – ключ к пониманию того, как функционируют шлюзы к мэйнфреймам IBM и другим компьютерным системам. Протоколы верхних уровней модели OSI выдают запросы на передачу пакетов из одной компьютерной системы в другую, а задача сетевого уровня состоит в практической реализации механизма этой передачи.

Сетевой уровень является основой стандарта CCITT X.25 на глобальные сети. Позже мы изучим структуру пакета X.25, включая назначение и структуру полей управляющей информации.

На сетевом уровне реализован ряд ключевых видов сервиса для транспортного уровня, который в модели OSI расположен непосредственно над сетевым. Сетевой уровень уведомляет транспортный уровень об обнаружении неисправимых ошибок, помогая ему поддерживать качество сервиса и избегать перегрузки сети путём прекращения, если это необходимо, передачи пакетов.

Поскольку в процессе обмена информацией между двумя сетями физические соединения время от времени могут изменяться, сетевой уровень поддерживает виртуальные каналы и обеспечивает правильную сборку пакетов, прибывающих в неправильной последовательности. Работа этого уровня осуществляется с помощью таблиц маршрутизации, которые служат для определения пути продвижения того или иного пакета. Во многих случаях сообщение, состоящее из нескольких пакетов, идёт по нескольким путям. Сетевой уровень предоставляет соответствующую «отгрузочную» информацию, необходимую для этих пакетов (например, общее число пакетов в сообщении и порядковый номер каждого из них).

С передачей данных в сетях связана одна очень неприятная проблема: такие характеристики, как длина поля адреса, размер пакета и даже промежуток времени, в течение которого пакету разрешается перемещаться по сети и по истечении которого пакет считается потерянным и выдаётся запрос на пакет-дубликат, в каждой сети различны. По этой причине управляющая информация, включаемая в пакеты на сетевом уровне, должна быть достаточной для предотвращения возможных недоразумений и обеспечения успешной доставки и сборки пакетов.

Как уже упоминалось выше, транспортный и сетевой уровни в значительной степени дублируют друг друга, особенно в плане функций управления потоком данных и контроля ошибок. Главная причина подобного дублирования заключается в том, что существует два варианта связи – с установлением соединения (connection-orientied) и без установления соединения (connectionless). Эти варианты связи базируются на разных предположениях относительно надёжности сети.

Сеть с установлением соединения работает почти так же, как и обычная телефонная система. После установления соединения происходит поэтапный обмен информацией, причем в данном случае «собе-

седники» не обязаны завершать каждое заявление своим именем, именем вызываемого партнёра и его адресом, поскольку предполагается, что связь надёжна и противоположная сторона получает сообщение без искажений.

В надёжной сети с установлением соединения адрес пункта назначения необходим лишь при установлении соединения, а в самих пакетах он не нужен. В подобной сети сетевой уровень принимает на себя ответственность за контроль ошибок и управление потоком данных. Кроме того, в его функции входит сборка пакетов.

Сетевой сервис без установления соединения, наоборот, предполагает, что контроль ошибок и управление потоком данных осуществляются на транспортном уровне. Адрес пункта назначения необходимо указывать в каждом пакете, а соблюдение очерёдности пакетов не гарантируется. Основная идея такого сервиса состоит в том, что важнейшим показателем является скорость передачи и пользователи должны полагаться на собственные программы контроля ошибок и управления потоком данных, а не на встроенные стандартные средства модели OSI.

Как это всегда бывает, когда члены комитета обсуждают сложный вопрос, был найден компромисс, который не удовлетворил ни одну из сторон. Он состоит в том, что возможности и сервиса с соединением, и сервиса без соединения встроены в оба уровня: сетевой и транспортный. Конечный пользователь может выбрать соответствующие стандартные значения для управляющих полей этих уровней и использовать тот метод, который ему больше по душе. Недостаток этого компромисса состоит в излишней избыточности, предусмотренной в обоих уровнях, что означает значительное количество дополнительных информационных битов. При передаче информации в таком формате по линиям дальней связи это приводит к дополнительным накладным расходам, поскольку процесс передачи занимает больше времени.

**Канальный уровень.** Канальный уровень можно сравнить со складом и погрузочно-разгрузочным цехом крупного производственного предприятия. Обязанность канального уровня – брать пакеты, поступающие с сетевого уровня, и готовить их к передаче (отгрузке), укладывая в кадры (коробки) соответствующего размера. В процессе перемещения информации вверх по уровням модели OSI канальный уровень должен принимать информацию в виде потока битов, поступающих с физического уровня, и производить её обработку. Этот уровень обязан определять, где начинается и где заканчивается передаваемый блок, а также обнаруживать ошибки передачи. Если обнаружена ошибка, канальный уровень должен инициировать соответствующие действия по восстановлению потерянных, искажённых и даже дублированных данных.

Между компьютерными системами может одновременно существовать несколько независимо работающих каналов передачи данных. Канальный уровень обязан обеспечить отсутствие перекрытия этих каналов и предотвратить возможное искажение данных. Канальный уровень инициализирует канал с соответствующим уровнем на компьютере, с которым будет обмениваться данными. Он должен обеспечить синхронизацию обеих машин и использование в них одинаковых схем кодирования и декодирования.

Поскольку управление потоком и контроль ошибок также входят в функции канального уровня, то он отслеживает получаемые кадры и ведёт статистические записи. По завершении передачи информации пользователем канальный уровень проверяет, все ли данные приняты правильно, а затем закрывает канал.

**Контроль ошибок на канальном уровне.** Для выполнения этой функции на канальном уровне применяется метод автоматического запроса повторной передачи (ARQ – Automatic Repeat Request). В зависимости от типа протокола, который работает на канальном уровне, для контроля ошибок используется одна из трёх разновидностей этого метода. ARQ с остановкой и ожиданием – это метод, при котором компьютер передаёт кадр информации, а затем ожидает получение кода подтверждения приёма (ACK – acknowledgment), который показывает, что кадр принят правильно. Если выявлена ошибка, то принимающая станция передаст код неподтверждения приёма (NAK – negative acknowledgment) и передающая станция повторяет передачу.

При использовании метода непрерывного ARQ с возвратом на N станция принимает несколько кадров (в зависимости от используемого протокола), а затем отвечает выдачей ACK или NAK с указанием кадра, который содержит ошибку. Если станция передала один за другим семь кадров и в четвёртом кадре выявлена ошибка, то передающая станция ответит на NAK повторной передачей кадров с 4-го по 7-й.

Метод непрерывного ARQ с избирательным повторением представляет собой модификацию предыдущего варианта ARQ. Принимающая станция записывает все получаемые кадры по порядку в специальный буфер, а затем отвечает, что такой-то кадр (скажем, номер 4) содержит ошибку. Сохраняя все остальные кадры в буфере, принимающая станция передаёт NAK. Передающая станция повторно передаёт только кадр, содержавший ошибку (т.е. номер 4). Принимающая станция вновь собирает пакеты в нужном порядке (с 1-го по 7-й) и обрабатывает информацию.

**Основные протоколы канального уровня.** Канальный уровень содержит ряд протоколов, которые разработаны комитетом IEEE 802. Для того чтобы понять, как работает этот уровень – ключевой в модели OSI, – нужно иметь некоторое представление о деятельности упомянутого комитета. Протоколы IEEE канального уровня будут рассмотрены позже.

**Физический уровень.** Физический уровень модели OSI наименее противоречивый, поскольку включает международные стандарты на аппаратуру, уже вошедшие в обиход. По сути дела, единственная реальная проблема на этом уровне заключается в том, как ISO собирается учитывать вновь разрабатываемые стандарты на аппаратуру. Методы передачи данных становятся всё более скоростными, появляются новые интерфейсы с дополнительными функциями контроля ошибок. В связи с этим возникает вопрос: будут ли добавлены к модели OSI новые стандарты или же физический уровень останется без изменений? Суд ещё не вынес свой вердикт, поэтому предсказать реакцию ISO сейчас не представляется возможным.

Для физического уровня определён очень подробный список рекомендованных к употреблению соединителей. Здесь упомянуты, к примеру, 25-контактные разъёмы для интерфейсов RS-232C, 34-контактные разъёмы для широкополосных модемов спецификации V.35 CCITT и 15-контактные разъёмы для интерфейсов общедоступных сетей передачи данных, определённых в рекомендациях CCITT X.20, X.21, X.22 и т.д. Кроме того, регламентируются допустимые электрические характеристики, в частности
RS-232C, RS-449, RS-410 и V.35 CCITT.

Физический уровень может обеспечивать как асинхронную (последовательную) передачу, которая используется для многих персональных компьютеров и в некоторых недорогих ЛВС, так и синхронный режим, который применяется для некоторых мэйнфреймов и мини-компьютеров.

Поскольку подкомитеты ISO и IEEE последние несколько лет работают в тесном контакте, не удивительно, что во многих стандартах на ЛВС используются определения, предложенные на физическом уровне модели OSI. На базе физического уровня различные подкомитеты IEEE разрабатывают подробные описания реального физического оборудования, которое передаёт сетевую информацию в виде электрических сигналов: требования к применяемым кабельным системам, разъёмам и соединителям.

На физическом уровне модели OSI определяются такие важнейшие компоненты сети, как тип коаксиального кабеля для одноканальной передачи при скорости 10 Мбит/с. Сюда включено принятое в стандарте IEEE 802.3 определение более тонкого коаксиального кабеля cheapenet. К физическому уровню будет добавлено и включённое в стандарт IEEE 802.3 определение одноканальной передачи данных по кабелю на витых парах со скоростью 10 Мбит/с.

К средствам, определённым на физическом уровне, также относятся волоконно-оптические кабели и витые пары, применяемые в самых различных ЛВС. В некоторых сетях, например стандарта Token Ring Network фирмы IBM, используются неэкранированные витые пары, а в сетях других типов – экранированные. Упомянутым подкомитетом, кроме того, были разработаны спецификации различных типов коаксиальных кабелей для широкополосных ЛВС различных типов.

На физическом уровне модели OSI должна быть определена и схема кодирования, которой компьютер пользуется для представления двоичных значений с целью их передачи по каналу связи. В стандарте Ethernet, как и во многих других локальных сетях, используется манчестерское кодирование. В манчестерском кодировании отрицательное напряжение в течение первой половины такта передачи с переходом на положительное напряжение во втором полутакте означает единицу, а положительное напряжение с переходом на отрицательное – нуль. Таким образом, в каждом такте передачи имеется переход с отрицательного на положительное напряжение, или наоборот.

Итак, физический уровень отвечает за тип физической среды, тип передачи, метод кодирования и скорость передачи данных для различных типов локальных сетей. К его функциям, кроме того, относятся установление физического соединения между двумя коммуникационными устройствами, формирование сигнала и обеспечение синхронизации этих устройств. Тактовые генераторы обоих устройств должны работать синхронно, иначе передаваемая информация не будет расшифрована и прочитана.

В табл. 1.2 представлено описание четырёх нижних уровней модели OSI. Особо следует отметить избыточность, предусмотренную в модели OSI для связи с установлением соединения и связи без установления соединения.

**1.2. Четыре нижних уровня модели BOC/MOC**

| | | | |
|---|---|---|---|
| Транспортный уровень | Определение транспортного сервиса. Транспортный протокол с установлением соединения | | |
| Сетевой уровень | Сетевой сервис без установления соединения | | |
| Канальный уровень | Управление логическим каналом. Неквитируемый сервис без установления соединения. Сервис с установлением соединения. Квитируемый сервис без установления соединения | | |
| Физический уровень | CSMA/CD. Коаксиальный кабель для одноканальной передачи. Коаксиальный кабель для широкополосной передачи. Неэкранированная витая пара (10 Мбит/с) 10 Base-T (10 Мбит/с) | Маркерная шина. Коаксиальный кабель для широкополосной передачи | Маркерное кольцо. Экранированная витая пара. Волоконно-оптический кабель |

## 1.2. ТРАДИЦИОННАЯ КОММУТАЦИЯ

Что же такое коммутатор? Согласно определению IDC, «коммутатор – это устройство, конструктивно выполненное в виде концентратора и действующее как высокоскоростной многопортовый мост; встроенный механизм коммутации позволяет осуществлять сегментирование локальной сети и выделять полосу пропускания конечным станциям в сети» [2].

Другими словами, коммутаторы 2-го уровня являются по сути обычными очень быстрыми многопортовыми мостами на основе стандарта IEEE 802.1d.

Концепция работы коммутатора 2-го уровня очень проста. Рассмотрим в качестве примера функционирование узла A (рис. 1.1).

Любой кадр, отправленный узлом A и имеющий адрес получателя в узле на сегменте Бета (например, Q), приходит в порт 1 коммутатора 2-го уровня и выходит из порта 2, чтобы быть полученным узлом Q. Этот процесс называется ретрансляцией (forwarding). Говорят, что кадр ретранслирован, если он получен одним портом коммутатора 2-го уровня и передан через другой.

Кадр, переданный узлом A и имеющий адрес получателя, который соответствует узлу B, естественно, приходит и на узел B, и на коммутатор 2-го уровня. Тем не менее коммутатор 2-го уровня знает, что узлы A и B находятся в одном сегменте, поэтому кадр не ретранслируется. Данный процесс называется фильтрацией (filtering). Говорят, что кадр отфильтрован, если он получен одним портом коммутатора и не ретранслирован другим.

Обратите внимание, что мы используем термин «кадр», а не «пакет». Коммутатор – это устройство уровня 2, которое оперирует кадрами, а не пакетами как повторитель. Коммутатор работает с кадрами и

понимает адреса MAC. Повторитель работает только с пакетами, в которых содержатся кадры. Порт коммутатора, как и узла, является обычным сетевым интерфейсом со средствами MAC. Фактически коммутатор представляет собой узел, обладающий несколькими сетевыми интерфейсами.

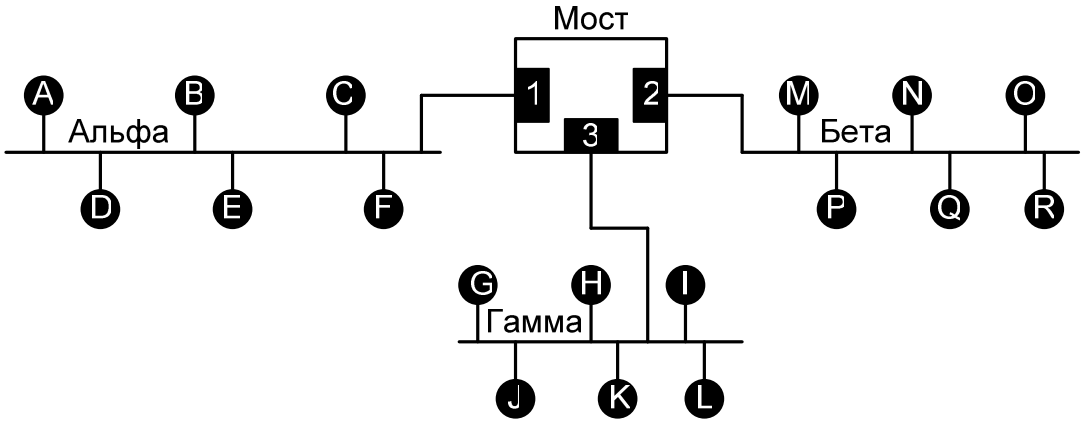


**Рис. 1.1. Схема сети с трёхпортовым мостом**

В литературе и технических описаниях коммутаторов и некоторых сетевых устройств часто говорят, что они работают (коммутируют или маршрутизируют трафик) на полной скорости канала (wire speed). Что это значит? Предположим, в ходе тестирования выяснилось, что устройство маршрутизирует 20 потоков Ethernet на полной скорости канала. Следовательно, оно маршрутизирует пакеты с такой же скоростью, с какой они поступали по 20 каналам Ethernet. При размере пакета 64 байт мы получаем скорость маршрутизации около 297 тыс. пакетов в секунду.

Важно подчеркнуть, что если маршрутизатор работает на скорости канала, то бессмысленно говорить о том, что он работает медленно.

В этом случае производительность маршрутизации определяется не скоростью работы устройства, а пропускной способностью каналов связи.

Для ретрансляции кадров из одного сегмента ЛВС в другой коммутатор может использовать следующие способы коммутации:

- Cut-Through (сквозная коммутация);
- Interim Cut-Through (модифицированная сквозная коммутация);
- Store-and-Forward (накопление и ретрансляция или промежуточная буферизация);
- гибридная коммутация.

Каждый из этих способов имеет свои преимущества и недостатки.

Технология коммутации 2-го уровня обеспечивает высокую производительность, позволяет строить достаточно сложные сети, являющиеся широковещательными доменами (областями).

## 1.3. КЛАССИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Главное различие между маршрутизатором и коммутатором 2-го уровня состоит не в производительности, а в способе принятия решения о ретрансляции. Маршрутизаторы используют для этой цели заголовок протокола, а не кадра. Как мы уже говорили ранее, разные сетевые технологии работают на различных уровнях модели OSI. Повторители являются устройствами уровня 1, мосты и коммутаторы – устройствами уровня 2, а маршрутизаторы – устройствами уровня 3.

Повторители работают с пакетами и не зависят от содержимого поля данных пакета, в котором заключён кадр. Мосты и коммутаторы работают с кадрами и не зависят от содержимого поля данных кадра, в котором обычно (но не всегда) заключена дейтаграмма. Маршрутизаторы работают с дейтаграммами, которые иногда называются пакетами данных, или сообщениями. Работа маршрутизаторов обычно не зависит от содержимого поля данных дейтаграммы, но тем не менее некоторые интеллектуальные маршрутизаторы должны разобраться в его содержимом, прежде чем принять весьма важное решение о ретрансляции или фильтрации.

При традиционной технологии каждый пакет обрабатывается маршрутизатором индивидуально, при этом устройство выполняет чётко определённую последовательность операций, к тому же такие операции, как просмотр таблицы маршрутов, формирование нового MAC-адреса, уменьшение поля TTL и т.д., являются обязательными. Некоторые маршрутизаторы обладают дополнительными функциями,

например фильтрацией. Выполнение основных и дополнительных операций отнимает много времени. В результате многие сетевые администраторы больших распределённых сетей со значительной нагрузкой довольно неохотно активизируют дополнительные функции обработки пакетов на маршрутизаторах. Традиционную схему обработки пакетов иллюстрирует рис. 1.2.

Каждый пакет обрабатывается независимо от других. Большое количество доступных функций обработки повышает общую функциональность изделия, но снижает его производительность.

И коммутаторы, и мосты, и маршрутизаторы соединены с сетью обычным сетевым интерфейсом. Тем не менее маршрутизатор работает не так, как коммутатор. Каждый узел, нуждающийся в передаче данных по маршрутизованной сети, должен участвовать в процессе, отправляя необходимые дейтаграммы непосредственно маршрутизатору. Коммутатор же получает все кадры сети вне зависимости от их назначения, а ретранслирует только кадры, предназначенные другим сегментам.

При отправке дейтаграммы узел помещает в поле отправителя собственный сетевой адрес, а в поле получателя – сетевой адрес получателя. Прежде чем передать дейтаграмму, узел должен установить, может ли он отправить её непосредственно получателю или же её нужно переслать маршрутизатору. Узел может отправить дейтаграмму непосредственно получателю без использования маршрутизатора, если его собственный номер сети совпадает с номером сети получателя. В случае Ethernet это означает, что оба узла находятся в одной широковещательной области. Узел просто заполняет MAC-адрес кадра сетевым адресом получателя. Если же номера сетей отправителя и получателя не совпадают, то передающий узел должен поместить дейтаграмму в кадр, адресованный маршрутизатору, после чего маршрутизатор возьмёт на себя заботу о доставке дейтаграммы получателю.

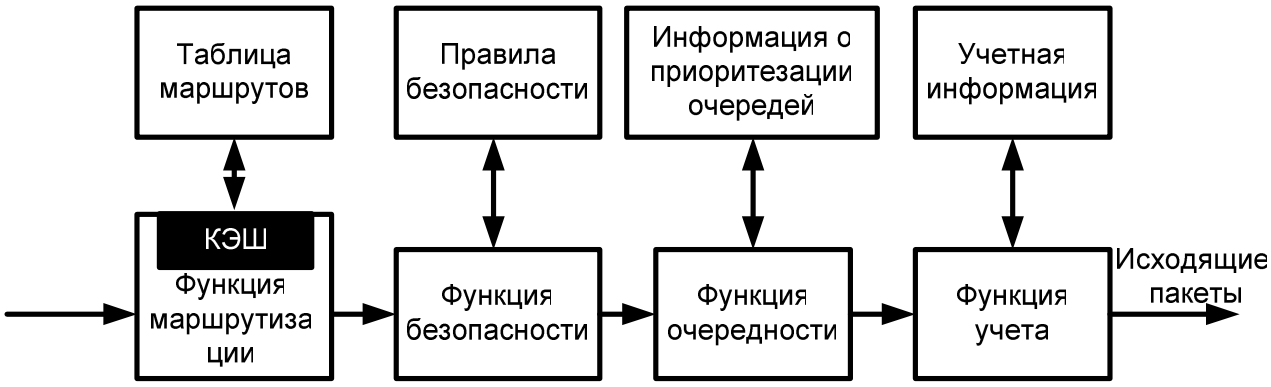


**Рис. 1.2. Традиционная схема обработки пакетов в маршрутизаторах**

Большое преимущество маршрутизаторов перед коммутаторами и мостами состоит в том, что маршрутизированная сеть хорошо масштабируется. Под масштабируемостью в данном случае понимается способность маршрутизованной сети быть достаточно большой и сложной и в то же время работать должным образом, обеспечивать нужную производительность и оставаться управляемой. Сеть с коммутаторами (мостами) в отличие от неё масштабируется плохо.

Маршрутизованные сети могут быть исключительно сложными, намного сложнее сетей с мостами. Колоссальной маршрутизованной сетью, которая соединяет миллионы компьютеров всего мира, является Internet. Такие сети хорошо масштабируются именно благодаря наличию маршрутизаторов. Сети с коммутаторами (или мостами) не масштабируются при достижении определённого размера по следующим причинам:

- широковещательные кадры занимают слишком большую часть полосы пропускания;
- сеть всегда должна оставаться остовным деревом.

Коммутаторы и мосты хорошо подходят для сегментирования отдельных областей коллизий. В сети с коммутаторами однопунктовые кадры распространяются только по тем сегментам, которые необходимы для доставки кадра от отправителя к получателю. А в сети с мостами широковещательный кадр, переданный одним узлом, должен быть получен всеми узлами. Когда размер сети с мостами возрастает, то всё большая часть общего сетевого трафика становится широковещательной, оставляя всё меньше места для кадров, несущих полезную информацию. Другими словами, чем больше широковещательных кадров, тем меньше показатель использования сети. Тем самым устанавливается практический предел размеру сети с мостами или переключателями.

Сеть с коммутаторами должна также оставаться остовным деревом. Это означает, что один коммутатор должен быть первичным, или корневым, мостом (root bridge). Если корневой мост выходит из

строя, то оставшиеся должны восстановить остовное дерево. В больших сетях с мостами это отнимает много времени и часто становится причиной катастрофы, поскольку сеть с мостами не может иметь активных избыточных связей. Трудно представить, что Internet зависит от единственного устройства!

Так как маршрутизаторы не пропускают широковещательных кадров и поддерживают множественные активные связи, то именно с их помощью можно решить указанные проблемы. Подобно тому, как мосты и переключатели используются для объединения нескольких областей коллизий, маршрутизаторы применяются для объединения широковещательных областей. На рис. 1.3 показано пять BD (broadcast domain – широковещательная область, ЛВС), соединённых тремя маршрутизаторами.

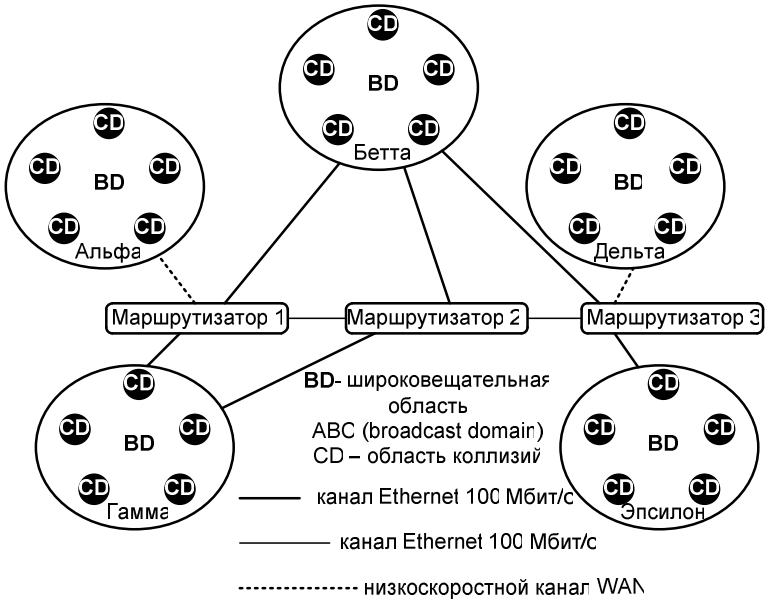


**Рис. 1.3. Маршрутизаторы и ЛВС**

Слово FAST обозначает связь Fast Ethernet, а слово SLOW – связь Ethernet. Связи, обозначенные словом WAN, работают ещё медленнее.

Любой узел маршрутизованной сети может взаимодействовать с любым другим, однако широковещательные кадры никогда не покидают той ЛВС, где они возникли, и не используют полосы пропускания других локальных сетей. В отличие от ЛВС с коммутаторами (мостами), маршрутизованные сети поддерживают множественные активные пути между сегментами. Маршрутизаторы осуществляют это, всегда пересылая дейтаграмму по наилучшему пути. Определение наилучшего пути дать очень сложно. Некоторые пути могут быть, например, быстрыми, а следовательно, предпочтительными. Тем не менее если один из таких быстрых путей перегружен, то маршрутизатор может выбрать для дейтаграммы альтернативный путь. Маршрутизаторы, запоминая топологию маршрутов, решают и проблему петель, от которой страдают сети с коммутаторами и мостами. Один из самых существенных недостатков классической маршрутизации – её чрезвычайно низкая производительность, что делает её малопригодной для современных высокоскоростных сетей.

## 1.4. ПРОТОКОЛЫ МАРШРУТИЗАЦИИ

В пересылаемых по сетям пакетах данных содержится большой объём информации; увы, она ничего не говорит о том, каким образом данный пакет должен найти свой путь в хитросплетении маршрутизаторов, коммутаторов и других устройств в корпоративной глобальной сети. Пакету каким-то образом следует указать путь к цели. Протоколы маршрутизации помогают пакетам найти не только верную, но и самую короткую дорогу к станции назначения. Это экономит и время, и деньги.

Планируя глобальную сеть, связывающую пользователей, серверы и мэйнфреймы, администратору приходится решать множество серьёзных проблем, одной из которых является проблема выбора протокола маршрутизации. В настоящее время существует несколько протоколов, обеспечивающих эффективную передачу данных. Администратору сети придётся выбрать тот протокол, который наилучшим образом соответствует потребностям его компании; главнейшим критерием выбора является размер сети.

Протоколы маршрутизации определяют топологию сети и сохраняют информацию о ней в таблице маршрутизации. Если маршрутизатор не применяет протокол маршрутизации, он хранит статические

маршруты или использует отдельный протокол на каждом интерфейсе. Обычно маршрутизаторы работают с одним протоколом маршрутизации [2].

Таблица маршрутизации, иногда называемая базой данных маршрутизации, – это набор маршрутов, используемых маршрутизатором в данный момент. Строки таблицы маршрутизации содержат по крайней мере следующую информацию:

- действительный адрес или множество действительных адресов в сети;
- информацию, вычисленную протоколом маршрутизации или необходимую ему;
- информацию, необходимую для того, чтобы переслать сообщение на один маршрутизатор ближе к получателю.

Информация о маршрутизации содержит метрику, т.е. меру времени или расстояния, и несколько отметок о времени. Информация о пересылке включает в себя данные о выходном интерфейсе и адрес следующей системы по пути. Обычно маршрутизаторы хранят данные о нескольких возможных следующих транзитных маршрутизаторах в одной строке таблицы.

Протоколы маршрутизации выполняют две важнейшие функции.

Во-первых, с их помощью определяется оптимальный путь передачи пакета по сети. Обычно избирается путь, обеспечивающий минимальное время доставки при максимальной надёжности. Как правило, это путь с минимальным числом транзитных узлов; передача данных в обход загруженных участков (с целью избежания заторов) – исключение из этого правила.

Протокол маршрутизации предполагает постоянный сбор информации о состоянии маршрутов и обновление таблиц маршрутизации при изменении топологии сети вследствие отказов или перегрузок. Таким образом, таблицы маршрутизации всегда содержат точную информацию о топологии сети.

Во-вторых, функцией протоколов маршрутизации является передача пакетов по сети. Получая очередной пакет, маршрутизатор считывает адрес назначения из заголовка пакета и определяет, в каком направлении (через какой узел) следует осуществить дальнейшую передачу пакета. Для принятия такого решения используется информация из таблицы маршрутизации.

Протокол маршрутизации может работать только тогда, когда формат пакетов соответствует одному из маршрутизируемых протоколов (routable protocol) – не путать с протоколами маршрутизации (routing protocols). Примеры маршрутизируемых протоколов – IP, IPX, Xerox Network System. Маршрутизируемые протоколы задают формат пакетов, в которые данные упаковываются для передачи по сети, а протоколы маршрутизации обеспечивают передачу этих пакетов, определяя путь их следования по адресам назначения, приведённым в полях заголовка.

Планируя сеть, следует использовать только один стандартный маршрутизируемый протокол. Некоторые маршрутизаторы могут работать с несколькими протоколами, однако применение разных протоколов в одной и той же сети снижает её производительность и усложняет работу администраторов сети.

Например, такие протоколы, как NetBEUI или LAT, являются немаршрутизируемыми и не способны обеспечивать функции сетевого уровня. Конечно, данные в формате NetBEUI или LAT можно пересылать по глобальной сети, но для этого надо либо инкапсулировать их с использованием маршрутизируемого протокола (например, IP), либо организовать мост между маршрутизаторами. В последнем случае дорогостоящие ресурсы маршрутизатора применяются для организации мостового соединения, что снижает общую производительность сети. По-видимому, наилучшим выходом из положения оказывается IP-инкапсулирование, однако время передачи данных возрастает – на сей раз из-за увеличения накладных расходов. Следовательно, лучше всего вообще отказаться от использования немаршрутизируемых протоколов.

Протоколы, используемые при создании таблицы маршрутизации, можно разделить на три категории:

- протоколы длины вектора расстояния;
- протоколы состояния канала;
- протоколы политики маршрутизации.

Классификация протоколов маршрутизации показана на рис. 1.4.

Протоколы длины вектора – простейший и наиболее распространённый тип протоколов маршрутизации. Большинство используемых сегодня протоколов этого типа ведёт свое начало от протокола Routing Information Protocol компании Xerox (иногда они даже так и называются). Протоколы данного

класса включают IP RIP, IPX RIP, протокол управления таблицей маршрутизации AppleTalk RTMP и Cisco Interior Gateway Routing Protocol.

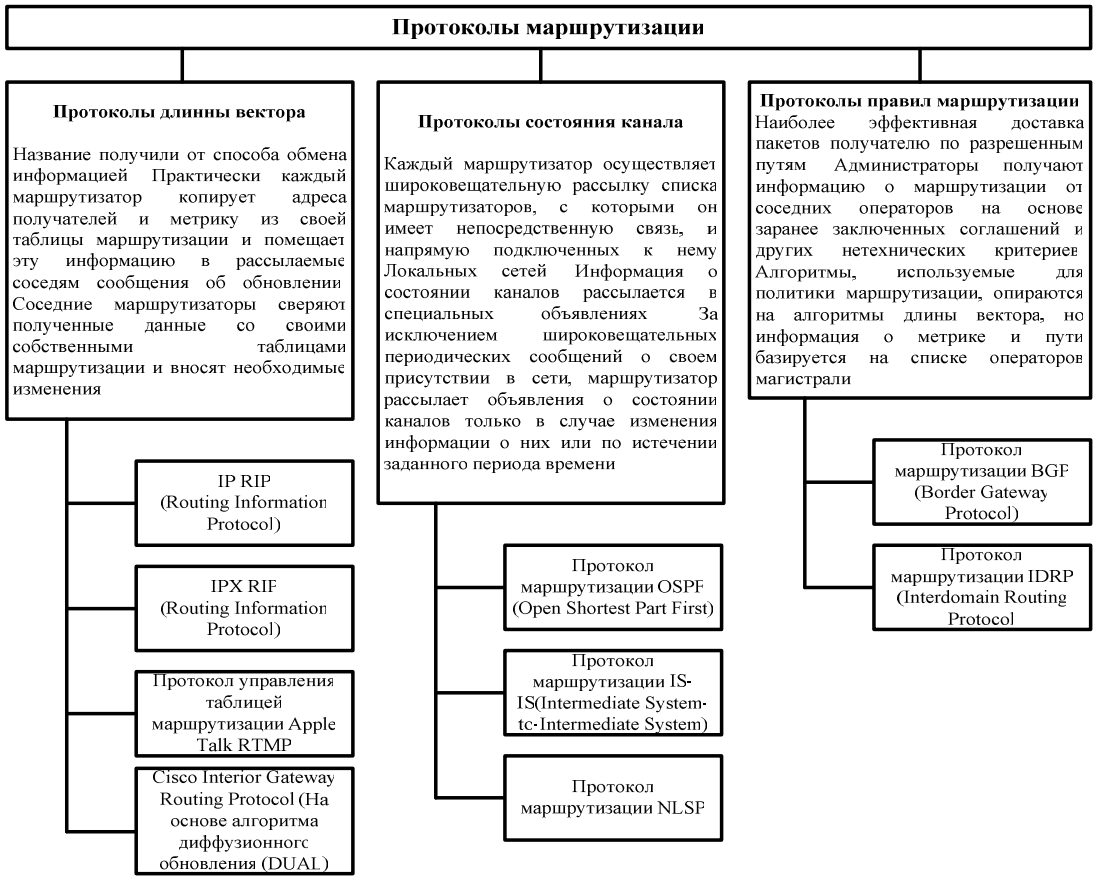


**Рис. 1.4. Классификация протоколов маршрутизации**

Своё название этот тип протоколов получил от способа обмена информацией. Периодически каждый маршрутизатор копирует адреса получателей и метрику из своей таблицы маршрутизации и помещает эту информацию в рассылаемые соседям сообщения об обновлении. Соседние маршрутизаторы сверяют полученные данные со своими собственными таблицами маршрутизации и вносят необходимые изменения.

Этот алгоритм прост и, как кажется на первый взгляд, надёжен. К сожалению, он работает наилучшим образом в небольших сетях при (желательно полном) отсутствии избыточности. Крупные сети не могут обойтись без периодического обмена сообщениями для описания сети, однако большинство из них избыточны. По этой причине в сложных сетях возникают проблемы при выходе линий связи из строя, так как несуществующие маршруты могут оставаться в таблице маршрутизации в течение длительного периода времени. Трафик, направленный по такому маршруту, не достигнет своего адресата. Эвристически данная проблема решаема, но ни одно из таких решений не является детерминистским.

Подобные проблемы могут быть решены усовершенствованным алгоритмом, который называется алгоритмом диффузионного обновления (DUAL). При этом маршрутизаторы используют алгоритм длины вектора для составления карты путей между ними и DUAL для широковещательного объявления об обслуживаемых ими локальных сетях. Информация об изменениях в топологии также рассылается по всей сети. Примером такого усовершенствованного протокола может служить Cisco Enhanced IGRP.

Вторую категорию протоколов обслуживания среды составляют протоколы состояния канала. Впервые предложенные в 1970 г. в статье Эдсгера Дейкстры, протоколы состояния канала сложнее, чем протоколы длины вектора. Взамен они предлагают детерминистское решение типичных для их предшественников проблем. Вместо рассылки соседям содержимого своих таблиц маршрутизации каждый маршрутизатор осуществляет широковещательную рассылку списка маршрутизаторов, с которыми он имеет непосредственную связь, и напрямую подключённых к нему локальных сетей. Эта информация о состоянии канала рассылается в специальных объявлениях. За исключением широковещания периодических сообщений о своём присутствии в сети, маршрутизатор рассылает объявления о состоянии каналов только в случае изменения информации о них или по истечении заданного периода времени.

Недостатком таких протоколов состояния каналов, как OSPF, IS-IS и NLSP, является их сложность и высокие требования к памяти. Они трудны в реализации и нуждаются в значительном объёме памяти для хранения объявлений о состоянии каналов. При всем своём превосходстве над ранними протоколами длины вектора их реальное преимущество перед DUAL далеко не очевидно.

К третьей категории протоколов по обслуживанию среды относятся протоколы правил маршрутизации. Если протоколы маршрутизации на базе алгоритмов длины вектора и состояния канала решают задачу наиболее эффективной доставки сообщения получателю, то задача маршрутизации – наиболее эффективная доставка сообщения получателю по разрешённым путям. Такие протоколы, как BGP (Border Gateway Protocol) или IDRP (Interdomain Routing Protocol), позволяют операторам Internet получать информацию о маршрутизации от соседних операторов на основе контрактов или других нетехнических критериев. Алгоритмы, используемые для политики маршрутизации, опираются на алгоритмы длины вектора, но информация о метрике и пути базируется на списке операторов магистрали.

Одно из следствий применения протоколов такого рода заключается в том, что пути сообщения и ответа на него через Internet, вообще говоря, различны. В корпоративных же сетях Intranet, не использующих политику маршрутизации, эти пути, как правило, совпадают.

Рассмотрим более подробно наиболее популярные протоколы маршрутизации: протокол маршрутной информации (Routing Information Protocol, RIP), протокол предпочтения кратчайшего пути (Open Shortest Path First, OSPF), «транзитная система – транзитная система» (Intermediate System-to-Intermediate System, IS-IS). У каждого из перечисленных протоколов свои достоинства, однако администратору сети придётся выбрать из них какой-нибудь один – тот, что более всего подходит для нужд его сети.

## 1.5. ПРОТОКОЛ МАРШРУТИЗАЦИИ RIP

Протокол RIP очень популярен среди тех, кто имеет отношение к Internet. Это протокол с использованием алгоритма длины вектора, где маршрут определяется исходя из расстояния (числа транзитных узлов) на пути следования данных до точки назначения. RIP известен довольно давно – впервые он появился в 1982 г. как часть набора протоколов TCP/IP в версии UNIX, предложенной Berkley Software Distribution. В настоящее время RIP служит основой для многих других протоколов маршрутизации, например для протокола маршрутизации AppleTalk. Другие компании (Novell и Banyan, кстати говоря, в их числе) также разработали протоколы на основе RIP. По существу, компании Microsoft удалось расширить возможности Windows NT для работы в глобальных сетях именно за счёт поддержки маршрутизации пакетов на основе RIP.

В маршрутизаторе, работающем с RIP, вся информация хранится в виде таблицы маршрутизации, содержащей следующие поля:

- пункт назначения (в нём перечислены все конечные, в смысле адреса, локальные сети);
- следующий транзитный узел (определяет, на какой порт должен быть переслан пакет для отправки на следующий маршрутизатор);
- расстояние (число транзитных узлов, необходимых для того, чтобы достичь пункта назначения).

Таблица маршрутизации RIP содержит информацию о наилучшем пути к месту назначения. После получения новых данных от другого узла старая информация стирается и на её место записывается новая.

Выбор оптимального маршрута в RIP обеспечивается рассылкой соответствующих сообщений при изменении топологии сети. Например, если маршрутизатор выявляет отказ в одном из каналов связи, он вносит изменения в свою таблицу маршрутизации, а затем рассылает копии новой таблицы всем своим соседям. Соседи соответственно вносят изменения в свои таблицы и рассылают их копии своим соседям и т.д. В результате через короткое время необходимая информация достигает всех маршрутизаторов.

В соответствии с протоколом RIP каждый маршрутизатор автоматически посылает (примерно раз в 30 секунд) своим соседям пакет типа «ответ» со своей таблицей маршрутизации. Для передачи больших таблиц маршрутизации требуется несколько пакетов. Помимо этого в протоколе RIP предусмотрено, чтобы каждый маршрутизатор следил за тем, сколько времени прошло с момента получения последнего ответа; если ответ от кого-нибудь из соседей не поступает в течение длительного времени (обычно 90 секунд), соответствующий путь удаляется из таблицы маршрутизации данного устройства, а все соседи извещаются об этом событии.

В протоколе RIP предусмотрен ряд мер, призванных повысить стабильность работы протокола. Среди них: лимит числа промежуточных узлов (hop-count limit), временный отказ от приёма информа-

ции (hold-down) и расщепление горизонта (split horizon). Лимит на число промежуточных узлов позволяет предотвратить зацикливание пакета при пересылке. Данный лимит в RIP равен 15, откуда следует, что этот протокол годится только для не слишком больших сетей. (Во второй версии протокола RIP это ограничение снято, и количество промежуточных узлов может достигать 255.)

Основным недостатком RIP является не слишком высокая функциональность: он не годится для больших сетей и не может эффективно определять альтернативные маршруты.

## 1.6. ПРОТОКОЛ МАРШРУТИЗАЦИИ OSPF

Для замены RIP Группа инженерной поддержки (IETF) разработала протокол OSPF; предполагается, что новый протокол обеспечит лучшую поддержку TCP/IP. Протокол OSPF, основанный на алгоритме предпочтения кратчайшего пути, был разработан Болтом, Беранеком и Ньюменом (Кембридж, шт. Массачусетс) для сети ARPANet в 1978 г. Благодаря своей функциональности OSPF быстро приобретает черты отраслевого стандарта. Данный протокол обеспечивает поддержку нужд крупных вычислительных сетей: обслуживание запросов на специальные услуги, работу с несколькими протоколами сетевого уровня, а также аутентификацию. OSPF способен осуществлять эффективную маршрутизацию пакетов с учётом изменений топологии сети, соответствующим образом меняя путь прохождения сетевого трафика. Кроме того, накладные расходы на пересылку данных об изменении топологии в OSPF меньше: рассылке подлежит не таблица маршрутизации в целом, а только информация об изменениях. OSPF иногда называют протоколом на основе распределённых баз данных, хотя правильнее его называть протоколом маршрутизации на основе данных о состоянии каналов связи (link state routing protocol). Термин «link state routing protocol» означает, что в OSPF поддерживается топологическая база данных, где хранится информация о состоянии каналов связи в автономной сети. Данная информация используется для вычисления кратчайшего пути передачи пакета.

В настоящее время многие компании выпускают маршрутизаторы, поддерживающие OSPF.

Протокол OSPF предусматривает, что новый маршрутизатор, начав работу в сети, рассылает «приветствия» всем своим соседям. Такие же сообщения периодически рассылают все маршрутизаторы, подтверждая тем самым свою работоспособность. В итоге новый маршрутизатор очень быстро «знакомится» со всеми своими соседями.

OSPF работает с запросами верхнего уровня [Type of Service (ToS) или Quality of Service (QoS)], содержащимися в заголовке пакетов IP. Вычисление кратчайшего пути в OSPF осуществляется на основе информации, содержащейся в ToS. Всего насчитывается восемь комбинаций битов ToS, описывающих все возможные сочетания уровней задержки, пропускной способности и надёжности связи. OSPF в состоянии подобрать путь таким образом, чтобы удовлетворить любую из этих восьми комбинаций. Например, если в ToS указано, что данный пакет должен быть передан с малой задержкой, высокой пропускной способностью и малой надёжностью, то OSPF-маршрутизатор подберёт путь передачи, как можно лучше отвечающий всем этим требованиям. OSPF – открытый стандарт, его описание приводится в документе RFC 1427.

## 1.7. КОММУТАЦИЯ ТРЕТЬЕГО УРОВНЯ

В настоящее время под термином «коммуникация» понимают иногда совершенно разные технологии и устройства, большинство которых появились на рынке совсем недавно. Возникновение этого термина вполне объяснимо. Для многих коммутация switching ассоциируется с высокой производительностью и относительно низкой ценой, т.е. с характеристиками, свойственными традиционным коммутаторам, работающим на уровне 2, канальном. На уровне 3, сетевом, работают традиционные маршрутизаторы, которые выполняют функции, необходимые для эффективной работы сколько-нибудь крупных сетей.

Однако сочетание слов «коммутация» (switching) и «уровень 3» (layer 3) является не совсем удачным. По-видимому, термин обязан своим появлением сотрудникам отделов маркетинга фирм-производителей, но никак не техническим специалистам. Поэтому относиться к нему надо как к термину, описывающему некое множество технологий и устройств, объединённых скорее общей целью, чем принципами работы.

Тогда, в конце 1980-х, сети строились таким образом, что рабочие станции пользователей и обслуживающие их серверы находились в одной подсети (сегменте). В этих условиях большая часть трафика передавалась внутри подсетей и лишь малая его часть – между подсетями. Так и возникло хорошо из-

вестное «правило 80/20», т.е. 80 % трафика локализовано внутри подсетей и только 20 % пересекает их границу. С этими 20 % спокойно справлялись маршрутизаторы, связывающие подсети между собой.

Со временем значение ЛВС для успешной деятельности предприятий росло, а следовательно, увеличивался и объём передаваемого по ним трафика. Возникла необходимость в повышении производительности сетей. Одним из способов достижения этого стала их микросегментация. Она позволяла уменьшить число пользователей на один сегмент и снизить объём широковещательного трафика, а значит, повысить производительность сети.

Первоначально для микросегментации использовались маршрутизаторы, которые, вообще говоря, не очень приспособлены для этой цели. Решения на их основе были достаточно дорогостоящими и отличались большой временной задержкой и невысокой пропускной способностью. Более подходящими устройствами для микросегментации сетей стали коммутаторы. Благодаря относительно низкой стоимости, высокой производительности и простоте в использовании они быстро завоевали популярность.

Таким образом, сети стали строить на базе коммутаторов и маршрутизаторов. Первые обеспечивали высокоскоростную пересылку трафика между сегментами, входящими в одну подсеть, а вторые передавали данные между подсетями, ограничивали распространение широковещательного трафика, решали задачи безопасности и т.д.

Однако централизация серверов, внедрение технологий интрасетей, широкое применение приложений мультимедиа и т.п. не только существенно повышают объём трафика в сетях, но и изменяют картину его распространения. С внедрением интрасетей о «правиле 80/20» можно забыть, так как картина распространения трафика становится абсолютно непредсказуемой: 80/20, 20/80, 50/50, ... Всё это предъявляет новые требования к средствам межсетевого взаимодействия, причём традиционные маршрутизаторы зачастую уже не отвечают этим требованиям. Необходимо существенно ускорить пересылку трафика между подсетями (на 3-м уровне) и снизить задержку при такой пересылке. Кроме того, при использовании центрального маршрутизатора значительно увеличивается нагрузка на сетевую магистраль, поскольку весь трафик между подсетями должен передаваться через маршрутизатор, а следовательно, проходить через магистраль. Отсюда вытекает ещё одно требование: сделать маршрутизацию распределённой, чтобы в процессе маршрутизации участвовали устройства (коммутаторы), находящиеся ближе к рабочим станциям.

Производители сетевого оборудования быстро среагировали на новые требования и разработали соответствующие технологии и продукты, очень часто объединяемые общим термином.

Уровень 3 – это сокращённое обозначение сетевого уровня в эталонной модели взаимодействия открытых систем (OSI). На этом уровне маршрутизаторы выполняют свои функции исходя из адресной информации, используемой в таких сетевых протоколах, как IP и IPX.

Коммутаторы действуют на 2-м уровне (канальном), передавая пакеты на базе физической адресации, применяемой в среде передачи данных сети. Вводя в свои изделия определённую информацию о 3-м уровне, изготовители коммутаторов создают коммутаторы уровня 3.

На первый взгляд всё выглядит так, будто каждый изготовитель подходит к этому техническому принципу по-разному. Но если обратиться к составным элементам любой конкретной конструкции, где реализуется этот принцип, выявятся три метода: маршрутизирующая коммутация, коммутация потоков и коммутирующая маршрутизация (табл. 1.2).

**1.2. Сопоставление архитектур третьего уровня**

| Архитектура | Описание | Достоинства | Недостатки | Наилучшее применение |
|---|---|---|---|---|
| Маршрутизирующая коммутация | Расчёт маршрута выполняется на 3-м уровне аппаратными или программными средствами в зависимости от вида реализации, а пакеты обрабатываются аппаратными средствами коммутации 2-го уровня. При пересылке информации о маршрутизации маршрутизаторы работают по стандартным протоколам маршрутизации | Хорошо знакомые функции; совместимость с имеющейся сетевой аппаратурой | Возможна потеря некоторых функций маршрутизации. Маршрутизация аппаратными средствами может затруднить модернизацию | Комплекс зданий кампуса и магистраль ISP |

| | | | | |
|---|---|---|---|---|
| Коммутация потоков | До обнаружения потока расчёт маршрута и обработка пакетов производятся на 3-м уровне. Далее поток пересылается на 2-м уровне через сеть. При пересылке информации в потоках коммутаторы потоков действуют по протоколам управления потоками | После обнаружения потоков линия данных освобождается от сложных операций маршрутизации | Архитектура – индивидуальные разработки различных фирм. Продолжает осуществляться маршрутизация непотокового трафика | Магистраль ISP и региональная вычислительная сеть |
| Коммутирующая маршрутизация | Тэговая коммутация. Расчёт маршрута и обработка пакетов производятся на 3-м уровне, но пакеты дополняются тэгами, которые содержат информацию о пересылке пакетов, поэтому для прохождения пакетов через сеть требуется меньший объём обработки данных на 3-м уровне | Масштабируемость применительно к большим сетям. Усиливается действие существующей аппаратуры маршрутизации (тэговая коммутация). Уменьшается объём операций маршрутизации в канале данных | Архитектура – индивидуальные разработки различных фирм. Совместимость под вопросом | Предприятие, магистраль ISP и региональная вычислительная сеть |

## 1.8. МАРШРУТИЗИРУЮЩАЯ КОММУТАЦИЯ

Маршрутизирующий коммутатор действует почти так же, как обычный маршрутизатор, в котором для выяснения маршрута каждого пакета используется информация, расположенная на 3-м уровне. Уменьшение стоимости и повышение производительности маршрутизирующего коммутатора достигаются благодаря сокращению числа выполняемых им функций и максимально возможному перемещению логических средств в интегральные схемы. В чисто маршрутизирующем коммутаторе обработка информации для выбора маршрута тесно объединена с процессом коммутации и пакеты во время обработки остаются в пределах коммутирующего механизма.

Маршрутизирующие коммутаторы покажутся администраторам сетей хорошо знакомыми устройствами, поскольку функционируют они практически так же, как и традиционные маршрутизаторы, и работают в соответствии с обычными протоколами маршрутизации. Однако необходимо иметь в виду весь комплекс их функций, поскольку некоторыми из них нередко жертвуют в пользу быстродействия и снижения цены. Чаще других исключаются функции, предусматривающие работу с протоколами, отличающимися от IP (такими как AppleTalk и IPX), и со сложными протоколами маршрутизации (подобными IP Multicast и OSPF), а также со средствами защиты (с применением шифрации и «брандмауэров»).

Системы с маршрутизирующей коммутацией анонсированы компаниями Lucent Tecnologies, Nortel Networks, Cisco, Extreme Networks и др. В каждом из изделий для снижения нагрузки маршрутизаторов существующих сетей применяется метод ответвления (drop-in) трафика. Такие коммутаторы в большинстве случаев совместимы с имеющимся оборудованием. Маршрутизирующие коммутаторы предназначены прежде всего для комплекса зданий, хотя изделие по крайней мере одного поставщика – GRF IP Switch фирмы Ascend – рассчитано на поставщиков услуг Интернета ISP (Internet Service Provider) и коммерческие службы связи.

Ряд фирм вводит также определённые новшества, облегчающие часть административных функций, связанных с управлением маршрутизаторами в выпускаемых ими маршрутизирующих коммутаторах. Так, например, SwitchNode фирмы Bay Networks может действовать в режиме автообучения IP Autolearn, в котором коммутатор «узнает» топологию сети, контролируя трафик по протоколу определения адресов Address Resolution Protocol (ARP). Этот протокол используется в сети для согласования адресов 3-го и 2-го уровней. Таким образом, SwitchNode можно прямо ставить в сеть без настройки его

конфигурации на протокол маршрутизации и изменения установок любых уже имеющихся маршрутизаторов.

## 1.9. КОММУТАЦИЯ ПОТОКОВ

Основной принцип коммутации потоков состоит в идентификации долговременных потоков данных между двумя IP-узлами. В ответ на обнаружение потока (программными средствами 3-го уровня) между концевыми точками устанавливается коммутируемое соединение, после чего поток передаётся аппаратными средствами 2-го уровня. В качестве примеров типов трафика, идентифицируемых как потоки, можно назвать пересылку файлов и передачу Web-графики. Трафик, не удовлетворяющий критериям потока, направляется обычным образом. Концепция коммутации потоков естественным образом сочетается с режимами ATM или ретрансляции кадров (frame relay), в которых потоки могут отображаться виртуальными цепями или маршрутами. Коммутация потоков рассчитана на поставщиков услуг Интернета и магистральные линии предприятий.

Решающую роль в этой области играют две организации: ATM Forum и Ipsilon. ATM Forum недавно утвердила стандарт коммутации потоков применительно к режиму ATM под названием Multiprotocol over ATM (MPOA), но этот стандарт разрабатывался очень долго. Ipsilon воспользовалась задержкой с выпуском MPOA и выдвинула собственный вариант коммутации потоков под названием IP-коммутации (IP switching). Она разработала серию IP-коммутаторов для коммутации потоков информации, соответствующих протоколу управления потоками Ipsilon Flow Management Protocol (IFMP). Ipsilon призывает поддержать свою платформу и убеждает другие фирмы предусматривать в своих устройствах коммутации и маршрутизации возможность работы по протоколу IFMP.

Технология Secure Fast Virtual Networking смело может быть отнесена к классу технологий коммутации потоков, ориентированных на соединение и установление виртуального канала (SVC). Входящий поток пакетов подвергается анализу на предмет выявления пар MAC-адресов. Для пар адресов формируется виртуальный путь. Далее, коммутатор анализирует пары MAC-адресов входящих пакетов и при наличии виртуального пути продвигает их по нему (сквозная коммутация на уровне 2). Таким образом, маршрутизации (вычислению виртуального пути) подвергается только первый пакет, а остальные пакеты коммутируются. Обработка пакетов по такой схеме показана на рис. 1.5.

Все широковещательные и групповые пакеты перехватываются и с использованием службы SmartSwitch ARP отправляются только адресатам, которым они необходимы.

Достоинства:

- малое время ожидания;
- высокая производительность;
- дешёвая сегментация сети;
- совместимость с маршрутизаторами;
- возможность автоматической конфигурации сети с использованием межкоммутаторных связей.

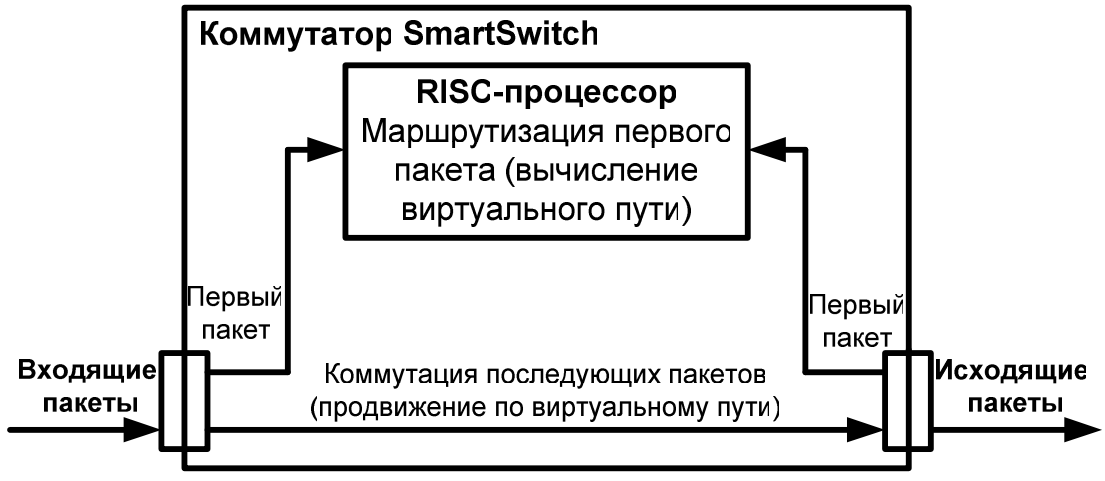


**Рис. 1.5. Обработка пакетов по технологии Secure Fast Virtual Networking фирмы Cabletron**

Недостатки:

- фирменное решение;
- необходимость изменения настроек на рабочих станциях сети (указание маршрутизатора по умолчанию);
- для достижения максимального эффекта требуется полный переход на архитектуру SecureFast Virtual Networking (см. выше).

Такую маршрутизацию ни в коем случае нельзя считать полноценной. Она предназначена для применения в ограниченных сетях и получила название «Виртуальная маршрутизация». Тем не менее коммутаторы серий Smart Switch 2000/6000/9000, использующие данную технологию, показывают очень хорошие результаты при обработке больших объёмов сетевого трафика.

## 1.10. КОММУТИРУЮЩАЯ МАРШРУТИЗАЦИЯ

Последний, и самый трудный для практического воплощения, метод связан с путями сокращения дополнительных (избыточных) операций при маршрутизации, в результате чего коммутаторы получают возможность выполнять функции передачи на 3-м уровне без сложных расчётов маршрутов.

Хорошим примером коммутирующей маршрутизации служит архитектура Tag Switching (тэговой коммутации), разработанная фирмой Cisco. Для реализации метода тэговой коммутации программное обеспечение маршрутизаторов фирмы Cisco модернизируется, и в зависимости от положения в сети они становятся либо концевыми тэговыми маршрутизаторами, либо тэговыми коммутаторами. Концевой тэговый маршрутизатор – это чистый маршрутизатор, который располагается на конце сети и дополняет поступающие в сеть пакеты адресной информацией в форме идентификаторов фиксированной длины, называемых тэгами. Тэговый коммутатор – это маршрутизатор или коммутатор, который расположен во внутренней сети и по тэгам определяет подходящий маршрут через сеть для каждого пакета. Благодаря наличию тэгов уменьшается сложность декодирования пакетов и преобразования таблиц при пересылке пакетов. Фирмой Cisco разработан также протокол распространения тэгов Tag Distribution Protocol (TDP), по которому осуществляется распределение тэговой информации тэговыми маршрутизаторами и коммутаторами. Cisco представила метод тэговой коммутации Рабочей группе инженеров Internet (Internet Engineering Task Force – IETF) для выработки стандарта.

Методы многопротокольной коммутации – Multiprotocol Switched Services (MSS) фирмы IBM и FastIP компании 3Com – основаны на маршрутизации по «протоколу выделения следующего скачка» (Next Hop Resolution Protocol – NHRP). Согласно этому протоколу клиент сети запрашивает маршрут у выделенного маршрутного сервера. Если маршрутный сервер может установить местоположение пункта назначения, то между концевыми точками устанавливается коммутируемое соединение. Благодаря этому маршрутизатор, в сущности, устраняется с пути передачи данных. Для реализации протокола NHRP на сетевом ПК MSS нуждается в дополнительных программных средствах, а FastIP требует, чтобы ПК был оснащён сетевым адаптером фирмы 3Com.

Разработка большинства методов коммутирующей маршрутизации проводилась для ликвидации «узких мест» сложных IP-сетей, подобных сетям, используемым поставщиками услуг в Интернете и коммерческими службами связи. Пытаясь реализовать коммутируемую маршрутизацию в масштабах всего предприятия, а не только для поставщиков услуг Интернета или региональной вычислительной сети (РВС), фирмы Lucent, IBM и 3Com согласились на совместное использование методов коммутации на 3-м уровне.

Заслуживает внимания и технология IP-коммутации компании Ipsilon Networks IP Switching. Схема Ipsilon относится к классу коммутации потоков и работает следующим образом. IP-коммутатор анализирует поступающие данные и, если посылка короткая (например, запрос к серверу), обрабатывает пакеты точно так же, как маршрутизатор. Отличие проявляется, когда коммутатор идентифицирует поток, т.е. длительную последовательность пакетов от конкретного отправителя конкретному получателю. В этом случае коммутатор посредством анализа заголовка пакета и сравнения этого заголовка с установленными пользователем правилами определяет, что такая последовательность является потоком. После этого он решает, что наилучший способ обработки пакета состоит в его коммутации. Какой трафик составляет поток, а какой нет, можно увидеть из табл. 1.3.

### 1.3. Различные виды трафика

| Потокоориентированный трафик | Короткоживущий трафик |
|---|---|
| Данные ftp | Запрос к DNS |
| Данные telnet | Данные SMTP |
| Данные HTTP | Network Timing (NTP) |
| Загрузка изображений из Web | POP |
| Мультимедиа аудио/видео | Запросы SNMP |

Специалисты утверждают, что продукты Ipsilon способны занять место традиционных маршрутизаторов от Cisco Systems и других поставщиков, так как Ipsilon закрывает не только маршрутизацию, но и IP. Если спросить, какой протокол наиболее важен для компании, то большинство респондентов наверняка ответят, что IP. Маршрутизация не исключается, но появление Интернета и Интранета ещё более углубляет наметившуюся тенденцию к унификации. Если 30 % трафика в сети представляют собой пакеты IP, то тогда коммутацию можно и нужно рассматривать в качестве одного из вариантов.

Наряду с поддержкой стандартных протоколов маршрутизации RIP, OSPF, BGR и CIP, Ipsilon разработала собственный протокол, получивший название «Протокол управления потоком» (Ipsilon Flow Management Protocol – IFMP). Благодаря этому протоколу несколько коммутаторов IP могут взаимодействовать друг с другом и с хостами. Продукты, поддерживающие IFMP, среди которых маршрутизаторы, коммутаторы и концентраторы нескольких поставщиков, могут идентифицировать потоки пакетов. Потоки отождествляются с высокоскоростными виртуальными соединениями ATM, а не маршрутизируются пакет за пакетом через сеть. IFMP получил также поддержку ещё нескольких поставщиков, таких как 3Com и IBM.

Ipsilon опубликовала также «Общий протокол управления коммутатором» (General Switch Management Protocol – GSMP) для управления оборудованием ATM. Оба протокола – IFMP и GSMP – имеют статус RFC. Кроме того, информацию о них можно получить на узле www.ipsilon.com.

Несмотря на все преимущества, решение Ipsilon также не избежало критики. В общих чертах она сводится к тому, что IP отдаётся предпочтение среди других протоколов. Хотя многие компании используют IP как в глобальных, так и в локальных сетях, во многих сетях по-прежнему преобладают другие протоколы, такие, например, как IPX компании Novell. В ответ на эту критику Ipsilon объявила, что намерена поддерживать IPX.

IP-коммутация обеспечивает также несколько уровней качества услуг (QoS). Поскольку IP-коммутаторы сами определяют характеристики потока для передачи трафика наиболее эффективным образом, они могут также принимать решение о требуемом QoS в зависимости от определения потока и гарантировать его с помощью RSVP или аппаратного обеспечения коммутатора. IP-коммутаторы способны также поддерживать многоадресную рассылку IP-пакетов с помощью процессов классификации потоков.

Стратегии миграции для компаний, заинтересованных в IP-коммутации, не представляют собой чего-либо сверхсложного. Если вы знаете, что такое IP-маршрутизация, то вам известно и то, что такое IP-коммутация. Приобретать новые знания или вкладывать средства в обучение не надо. Предлагается начать с пилотной программы, когда IP-коммутаторы работали бы бок о бок с имеющимися маршрутизаторами, а затем постепенно добавлять коммутаторы. Не требуется, чтобы потребитель пересмотрел архитектуру своей сети (а ведь эта задача отнюдь не тривиальная). Люди хотят, чтобы медленный трафик стал быстрее, и это можно сделать с помощью IP-коммутации.

## 1.11. КОММУТАЦИЯ ЧЕТВЁРТОГО УРОВНЯ

В последнее время производители сетевого оборудования много говорят о «коммутации 4-го уровня». Что же это такое – новейшая технология или маркетинговая «приманка»? Всего понемногу.

Давайте попробуем разобраться, в чем тут дело. Вспомним, что на уровне 4 модели OSI в качестве основы используются номера портов протоколов TCP и User Datagram Protocol (UDP) стека Internet Protocol. Протокол TCP относится к протоколам транспортного уровня, а UDP описывает, как сообщения доходят до приложения в компьютере адресата. На уровне 4 каждый пакет содержит информацию, кото-

рая может использоваться для того, чтобы идентифицировать то приложение, что генерировало пакет. Это возможно потому, что TCP- и UDP-заголовки включают «номера портов», которые идентифицируют, какие протоколы прикладного уровня включены в каждый пакет. При этом различные приложения более высоких уровней, используя сервис транспортного уровня, обращаются к различным номерам портов (рис. 1.6).

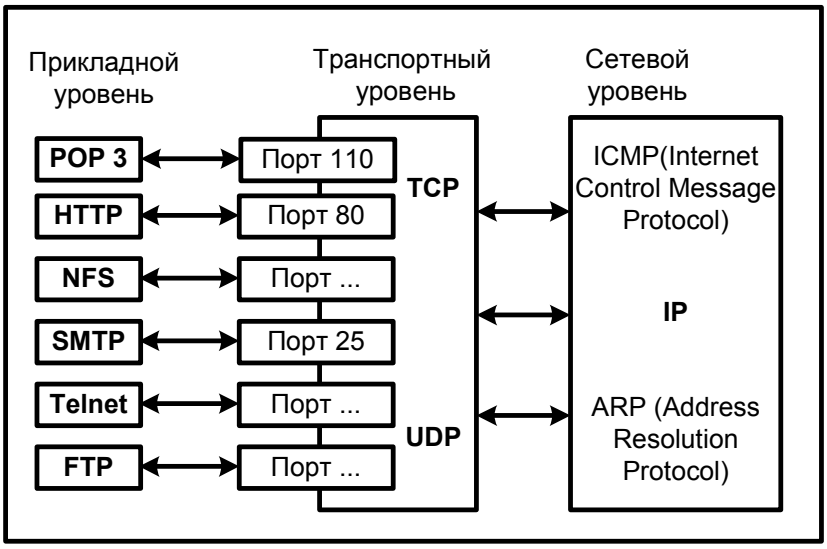


**Рис. 1.6. Взаимодействие между уровнями стека прокотолов TCP/IP**

Информация о номере порта заголовка уровня 4 в сочетании с информацией об источнике/приемнике заголовка уровня 3 может использоваться для обеспечения действительно детального управления. Индивидуальные потоки каждого приложения могут быть проконтролированы между клиентом и сервером, а если коммутирующий маршрутизатор является полнофункциональным, то все они могут быть обработаны на проводной скорости.

Читая заголовки на уровне 4, коммутатор 4-го уровня способен делать различия между приложениями, принимая решения о маршрутизации. Приложениям можно назначить различные приоритеты маршрутизации, гарантируя разное качество обслуживания (QoS), или они могут иметь фильтры защиты, тем самым обеспечивая управление уровнем приложения поверх сетевого. При этом необходимо помнить, что никакой информации о маршрутизации «в чистом виде» на уровне 4 не содержится. Таким образом, под коммутацией уровня 4 следует понимать использование параметров TCP-сессий протоколов HTTP, NFS, Telnet, FTP, SMTP, POP 3 и т.д. для принятия решений о политике коммутации (приоритезации). По мнению обозревателей, такая схема обеспечивает более оптимальный контроль и даёт возможность назначать приоритеты передачам в соответствии с типами приложений. Коммутаторы уровня 2 передают данные от порта к порту, учитывая лишь адрес назначения каждого пакета, как и коммутаторы уровня 3, выполняющие маршрутизацию на скорости, близкой к максимальной. Следовательно, коммутация уровня 4 является всего лишь расширением функциональности коммутаторов уровня 3.

Для представления функциональности различного рода устройств на рис. 1.7 даётся сравнение функциональности коммутаторов 2-го уровня, коммутаторов 3-го уровня и коммутирующего маршрутизатора (на примере Smart Switch Router производства компании Cabletron Systems – лидера в данном классе продуктов).

Коммутирующий маршрутизатор можно одновременно использовать как коммутатор, работающий по нескольким интерфейсам только на уровне 2 и представляющий на этом уровне поддержку стандартов 802.1d/p/Q, port based VLANs, Flow Switching, фильтрацию фреймов L2 и т.д.; как маршрутизатор, работающий на 3-м уровне по протоколам IP/IPX и поддерживающий port based VLANs, а также все сервисы этого уровня: DNS, L3 QoS, ACLs, Proxy ARP и т.д., и подключать функции 4-го уровня, такие как функции безопасности, качества сервиса, RMON2, выполняющиеся на высочайшей скорости.

По словам Джона Армстронга, аналитика компании Dataquest, маршрутизаторы давно выполняют такие же функции, используя фильтры. Коммутатор уровня 4 – это на самом деле коммутатор, работающий на уровне 3 модели OSI, но оснащённый дополнительными программными средствами, типичными для маршрутизаторов, – поясняет он. – В действительности коммутация на уровне 4 осуществляется не на транспортном уровне. Поэтому, раз они работают на уровне 3 и передают пакеты на сетевом, их уместнее называть устройствами уровня 3.

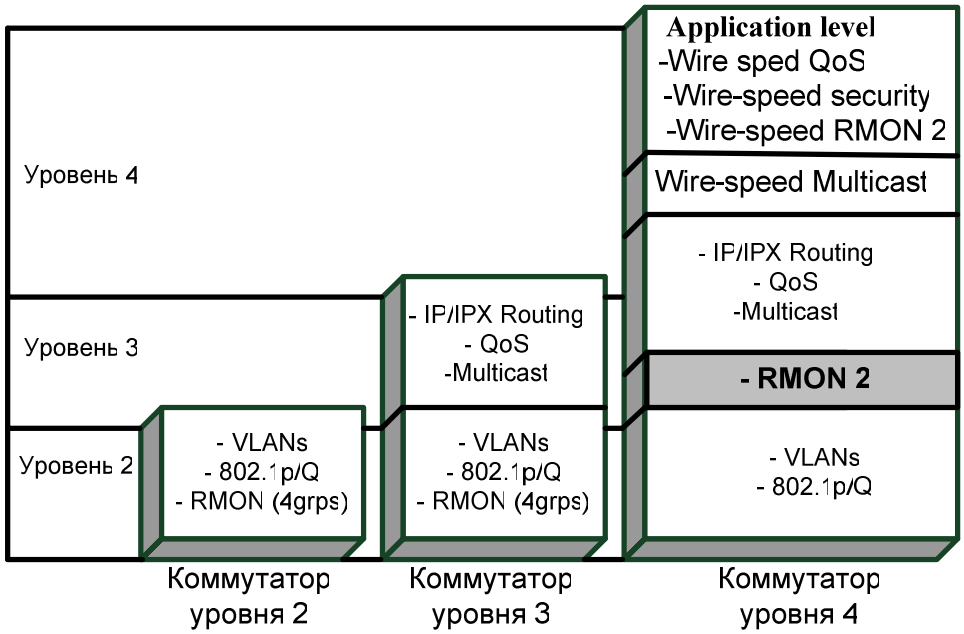


**Рис. 1.7. Сравнение функциональности коммутаторов 2-го уровня, коммутаторов 3-го уровня и коммутирующего маршрутизатора**

Если отвлечься от рекламных трюков, возможности работы уровня 4 могут понадобиться сетевым администраторам для управления трафиком на основе приоритетов. Предположим, сетевой администратор захочет упорядочить трафик клиентов своей сети, например электронную почту или доступ к базе данных электронных таблиц. Если в коммутаторах будут средства работы на уровне 4, он сможет это сделать.

## 1.12. СТАНДАРТЫ IEEE 802.1Q И IEEE 802.1P

Задача рабочих групп, трудящихся над стандартами P и Q, – дать сетевой отрасли единый метод передачи по сети информации о приоритете кадра и его принадлежности к виртуальным локально-вычислительным сетям (ВЛВС). Были разработаны две спецификации маркировки пакетов:

- первая, одноуровневая, определяет взаимодействие виртуальных сетей по магистрали Fast Ethernet;
- вторая, двухуровневая, касается маркировки пакетов в смешанных магистралях, включая Token Ring и FDDI.

Первая спецификация с самого начала нуждалась лишь в минимальной доработке, так как она, по сути, представляет собой технологию тэговой коммутации, продвигаемую на рынок усилиями Cisco. Задержки с принятием стандарта 802.1Q объясняются необходимостью детальной проработки куда более сложной «двухуровневой» спецификации.

Стандарт должен был удовлетворять следующим достаточно высоким требованиям:

- *масштабируемости* на уровне обмена пакетами между коммутаторами;
- *преемственности* на уровне существующих конечных приложений;
- *адаптации* на уровне существующих протоколов и таблиц маршрутизации;
- *экономичности* в плане утилизации высокоскоростных магистралей;
- *совместимости* с ATM, особенно с эмуляцией ЛВС;
- *управляемости* процесса маркировки пакетов.

В соответствии со стандартом 802.1Q к кадру Ethernet добавлены четыре байта. Эти 32 бита содержат информацию по принадлежности кадра Ethernet к ВЛВС и о его приоритете. Говоря точнее, тремя битами кодируется до восьми уровней приоритета, 12 бит позволяют различать трафик до 4096 ВЛВС, один бит зарезервирован для обозначения кадров сетей других типов (Token Ring, FDDI), передаваемых по магистрали Ethernet, и т.д.

Поле идентификатора уровня приоритета даёт возможность использовать восемь таких уровней, соответствующих системе приоритетов стандарта 802.1P.

В заголовке кадра Ethernet поля 802.1Q размещаются между адресом отправителя и полем с информацией о длине кадра полезной нагрузки 802.3 (кадр Ethernet) или о типе протокола более высокого уровня (кадр Ethernet II) (рис. 1.8).

В настоящее время практически все сетевые фирмы уже создали коммерческие версии продуктов, поддерживающие стандарты 802.1P и 802.1Q. Кроме того, многие производители коммутаторов Ethernet уже реализовали службы приоритезации собственной разработки (рис. 1.9).

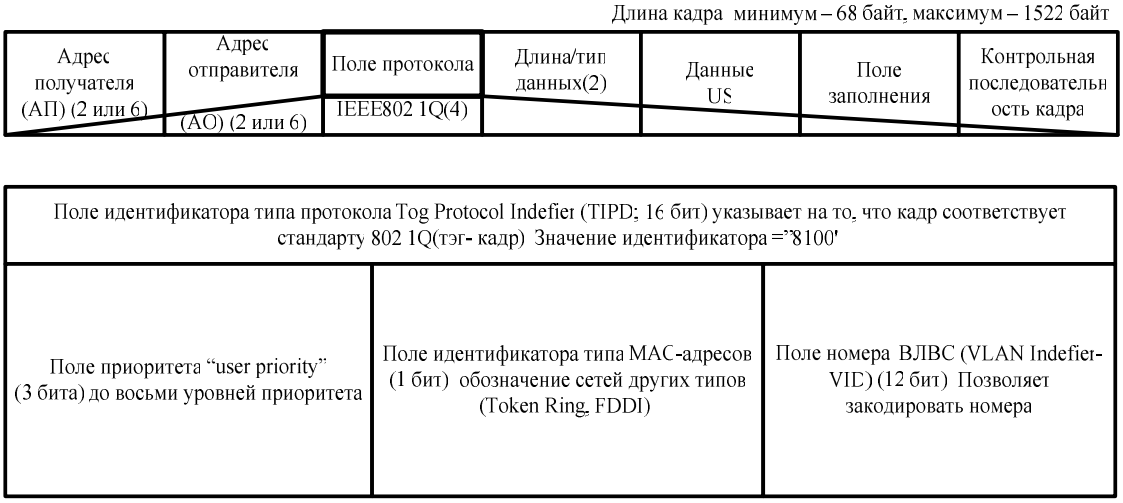


**Рис. 1.8. Формат поля протокола IEEE 802.1Q кадра Ethernet**


**Рис. 1.9. Формирование схемы управления приоритетами в сети**

Очевидно, что изменение структуры кадра Ethernet влечёт за собой возникновение серьёзных проблем – ведь он теряет совместимость со всеми традиционными устройствами Ethernet, ориентированными на старый формат кадра.

В самом деле, из-за того что данные 802.1Q размещаются перед полем с информацией о длине полезной нагрузки (или типе протокола), традиционный сетевой продукт не обнаружит эту информацию на привычном месте и вместо неё «прочитает» число x8100 – значение по умолчанию нового поля «Тэг протокольного идентификатора» (Tag Protocol Identifier) в кадрах 802.1Q.

Источником проблем является не только изменение в размещении полей заголовка кадра Ethernet, но и увеличение максимальной длины данного кадра. Многие сетевые устройства не способны обрабатывать кадры длиннее 1518 байт. Между специалистами возникли споры по поводу того, нужно ли максимальный размер кадра Ethernet удлинять на четыре байта или следует укоротить на четыре байта максимальный размер полезной нагрузки и таким образом компенсировать увеличение заголовка. Спецификация 802.1Q предусматривает оба подхода, поэтому производителям самим предстоит обеспечивать взаимную совместимость своих продуктов.

С технической точки зрения, осуществить взаимодействие старого оборудования с 802.1Q-совместимыми современными устройствами несложно, и большинство производителей сумеют реали-

зовать такую возможность в своих продуктах на уровне их портов. Для состыковки 802.1Q-совместимого устройства с прежним коммутатором или сетевой платой потребуется просто отключить поддержку стандарта 802.1Q на нужном порте, и весь трафик будет посылаться в сеть в обычном виде.

**Приоритеты и классы обслуживания.** Спецификация IEEE 802.1P, создаваемая в рамках процесса стандартизации 802.1Q, определяет метод передачи информации о приоритете сетевого трафика. Хотя в большинстве ЛВС редко случаются длительные перегрузки, отдельные всплески трафика представляют собой обычное явление и могут привести к задержкам передач пакетов. Это абсолютно неприемлемо для работы сетей, предназначенных для передачи голоса и видео. Стандарт 802.1P специфицирует алгоритм изменения порядка расположения пакетов в очередях, с помощью которого обеспечивается своевременная доставка трафика, чувствительного к временным задержкам.

Рабочая группа по стандартизации интегрированного обслуживания в сетях с разными канальными уровнями (ISSLL) определила ряд классов обслуживания в зависимости от того, какое время задержки допустимо для передачи пакета того или иного типа трафика. Представьте себе сеть с разными видами трафика: чувствительного к задержкам порядка 10 мс, не допускающего задержек более 100 мс и почти не чувствительного к задержкам. Для успешной работы такой сети каждый из этих типов трафика должен иметь свой уровень приоритета, обеспечивающий выполнение требований, предъявляемых к величине задержки. Используя концепцию протокола резервирования ресурсов (Resource Reservation Protocol – RSVP) и систему классов обслуживания, можно определить схему управления приоритетами. Протокол RSVP, который будет рассмотрен ниже, поддерживается большинством коммутирующих маршрутизаторов и, в частности, моделями SSR 8000/8600 производства Cabletron.

В дополнение к определению приоритетов стандарт 802.1P вводит важный протокол GARP (Generic Attributes Registration Protocol) с двумя специальными реализациями. Первая из них – протокол GMRP (GARP Multicast Registration Protocol), позволяющий рабочим станциям делать запрос на подключение к домену групповой рассылки сообщений. Поддерживаемую этим протоколом концепцию назвали подсоединением, инициируемым «листьями». Протокол GMRP обеспечивает передачу трафика только в те порты, из которых пришёл запрос на групповой трафик, и хорошо согласуется со стандартом 802.1Q.

Второй реализацией GARP является протокол GVRP (GARP VLAN Registration Protocol), похожий на GMRP. Однако, работая по нему, рабочая станция вместо запроса на подключение к домену групповой рассылки сообщений посылает запрос на доступ к определённой ВЛВС. Данный протокол связывает стандарты P и Q.

С принятием предварительных вариантов стандартов 802.1Q и 802.1P появились все возможности для широкого использования средств приоритезации трафика в сетях Ethernet. Задействуя продукты, поддерживающие механизмы приоритезации, сетевые администраторы смогут распоряжаться коммутирующей инфраструктурой своей сети таким образом, чтобы, например, высший уровень приоритета получил трафик офисного пакета Lotus Notes и электронной почты, а аудиопотоки RealAudio – низший уровень. Механизмы приоритезации трафика, основанные на спецификациях 802.1Q и 802.1P, бесспорно, стали ещё одним козырем технологии Ethernet.

Но хотя упомянутые спецификации и обеспечивают приоритезацию трафика для наиболее популярных топологий второго уровня, они не гарантируют того, что вся инфраструктура сети (от одной её конечной точки до другой) будет поддерживать обработку приоритетного трафика. В частности, спецификации 802.1Q и 802.1P бесполезны при управлении приоритетом IP-трафика (трафика третьего уровня), передаваемого через низкоскоростную распределённую сеть или каналы доступа в Интернет, т.е. через наиболее вероятные «узкие места» сетевой инфраструктуры.

Чтобы в полной мере управлять трафиком во всей сети, необходимо прежде всего реализовать эффективную приоритезацию IP-трафика. В связи с этим возникает ряд вопросов. Поддерживает ли локальная сеть механизмы такой приоритезации? А оборудование распределённой сети? Поддерживает ли эти механизмы ваш поставщик услуг Интернета? Что в связи с этим можно сказать об инфраструктуре на другом конце соединения? Если хотя бы одно устройство, находящееся между двумя системами, не поддерживает механизмы приоритезации, будет невозможно реализовать передачу приоритетного трафика от одного конечного узла сети до другого.

В отличие от технологии Ethernet, протокол IP уже довольно давно обладает средствами приоритезации сетевого трафика – впервые они были предложены в версии, опубликованной в 1981 г. Каждый IP-пакет имеет восьмибитовое поле «Тип сервиса» (Type of Service, ToS), состоящее из двух подполей (см. структуру заголовка пакета IP):

- трёхбитового – для установления уровня приоритета пакета;
- четырёхбитового – для указания класса (типа) обслуживания, предпочтительного для данного пакета (оставшийся восьмой бит не используется).

Три первых бита поля ToS позволяют устанавливать для IP-трафика те же восемь уровней приоритета (от 0 до 7), что и спецификации 802.1Q и 802.1P, а также большинство других технологий ЛВС. Поэтому можно взаимно однозначно отображать информацию о приоритетах кадров Ethernet и пакетов IP, а значит, реализовать сквозную обработку приоритетного трафика, передаваемого из одной сети Ethernet в другую через распределённую сеть IP или инфраструктуру поставщика услуг Интернета.

Четыре других используемых бита поля ToS позволяют администратору сети осуществлять индивидуальную маршрутизацию каждого пакета в соответствии с особенностями содержащихся в нём данных. Так, например, пакетам протокола NNTP (Network News Transfer Protocol), транспортирующим новости UseNet, можно установить класс обслуживания с низкой стоимостью («low cost»), а пакетам Telnet – класс обслуживания с низкой задержкой («low latency»).

Изначально стандарт RFC 791 (первоначальный вариант протокола IP) определял только три класса обслуживания, каждому из которых ставился в соответствие отдельный бит, устанавливаемый в «1» или «0» в зависимости от потребностей в том или ином типе обслуживания. С принятием стандарта RFC 1349 был добавлен ещё один класс, и теперь ранее разобщённые четыре бита стали рассматриваться как единое целое. Поэтому сегодня с их помощью можно задавать максимум 16 значений (от 0 до 15).

Сетевые администраторы, управляющие сложными сетями с множеством маршрутов, могут использовать биты для определения типа обслуживания в сочетании с такими протоколами маршрутизации, как OSPF, для создания специальных служб маршрутизации. Например, пакеты с «отметкой» low latency (низкая задержка) можно посылать не по спутниковому соединению, а по высокоскоростной оптической линии, тогда как «неприхотливый» трафик (класс обслуживания «low cost») направить через Интернет, а не через корпоративную распределённую сеть.

Комбинируя биты установки типа обслуживания с битами приоритета, можно очень точно задавать режимы обработки пакетов с конкретными типами данных, например: определить правила, в соответствии с которыми сетевые фильтры будут присваивать всем пакетам приложения Lotus Notes средний уровень приоритета и назначать класс обслуживания с низкой задержкой. При этом пользователи Notes получат льготное обслуживание по сравнению с пользователями других, менее важных приложений. Можно определить иной набор фильтров, который пометит весь трафик аудиоприложения RealAudio как низкоприоритетный и установит для него класс обслуживания с высокой пропускной способностью (high throughput).

Если вы располагаете собственным сквозным соединением между узлом-отправителем и узлом-получателем, то можете распоряжаться пакетами по своему усмотрению. Но в большинстве сетей поставщиков услуг Интернета пакеты с установленными уровнями приоритета и непомеченные пакеты будут обрабатываться одинаково. Поэтому с точки зрения приоритезации трафика и назначения ему разных классов обслуживания лучшим вариантом является использование частной территориально распределенной сети. При работе через Интернет можно назначить фильтры для поступающего из этой глобальной сети трафика, чтобы по крайней мере контролировать его продвижение по вашей собственной сети.

Однако далеко не всё зависит от сетевой инфраструктуры. В настоящее время имеются значительные проблемы, связанные с установкой битов приоритета и типа обслуживания в IP-пакетах. Эти биты могут быть установлены как самим приложением по мере формирования и отправки пакетов, так и сетевым устройством с помощью специальных фильтров. И в том и в другом случае поддержка этих функций всецело зависит от производителей приложений, операционных систем и сетевого оборудования.

Но удивительно, что лишь некоторые операционные системы используют в своих IP-стеках механизмы записи в пакет информации об уровне его приоритета и требуемом для него классе обслуживания. В прикладном программном интерфейсе WINSOCK.DLL, поставляемом вместе с Windows XP и Windows Server 2003, такие возможности вообще отсутствуют, так что попытки вызвать функцию «setsockopt (IP_TOS)» приводят к выдаче диагностического сообщения «invalid operation» («Недопустимая операция»). В других операционных системах, например в Irix, HP-UX и Solaris, реализована лишь частичная поддержка данных функций.

Среди всех операционных систем мощная поддержка функций ToS реализована только в Linux и Digital UNIX. Причём она имеется как непосредственно в самих системах, так и в наборах их стандартных приложений. Например, обе системы предоставляют клиенты и серверы Telnet, способные устанавливать бит low latency поля ToS – ни одна другая из протестированных нами операционных систем такими важными возможностями не обладает. Клиент и сервер FTP, работающие в среде Linux и Digital UNIX, способны устанавливать бит low latency в пакетах, передаваемых по каналу управления, а бит high throughput – в пакетах, передаваемых по информационному каналу. В итоге такая команда FTP, как

abort operation (прервать команду), будет передана на сервер по самому скоростному маршруту и соответственно за минимальное время (оперативно отменив при этом загрузку файла с сервера).

Почему же лишь немногие приложения поддерживают функции байта ToS? Да потому, что большая часть операционных систем, в среде которых они работают, не обеспечивает надлежащую поддержку этих функций. И до тех пор, пока Microsoft не модифицирует программный интерфейс WINSOCK.DLL системы Windows, поставщики приложений вроде Lotus Development, Netscape Communications и Oracle не смогут реализовать в своих приложениях механизмы управления приоритетами.

Тем не менее существуют способы, позволяющие обходить те проблемы, которые не спешат решать поставщики операционных систем и приложений. Самый верный из них – реализовать службы приоритезации трафика IP не в приложениях и операционных системах, а в устройствах сетевой инфраструктуры. Администраторы многих крупных и сильно загруженных сетей уже несколько лет осуществляют приоритезацию с помощью фильтров, устанавливаемых в маршрутизаторах отдельно для каждого приложения.

Так, например, можно вручную определить фильтр, обеспечивающий обслуживание с более высоким уровнем приоритета, скажем, трафика Notes, по сравнению с трафиком FTP. И хотя такой способ не отличается особым изяществом, его можно использовать, если не в масштабе сети всего предприятия, то по крайней мере в пределах отдельных её сегментов.

Существует немало средств для реализации в IP-сетях различных механизмов управления приоритетами, ориентированных на конкретные приложения. Эти механизмы можно связать со схемой приоритезации, определённой в спецификациях 802.1Q и 802.1P.

## 1.13. ПРОТОКОЛЫ RTP И RSVP

Современные приложения не могут допустить, чтобы их пакеты поступали с опозданием. Два протокола (RTP и PSVP) позволяют гарантировать своевременность доставки с обеспечением качества услуг.

Непрекращающийся рост Интернета и частных сетей предъявляет новые требования к пропускной способности. Клиент-серверные приложения далеко превосходят Telnet по объёмам передаваемых данных. World Wide Web привёл к гигантскому увеличению графика графической информации. Сегодня к тому же голосовые и видеоприложения выдвигают свои специфические требования к и без того перегруженным сетям.

Для того чтобы удовлетворить все эти запросы, одного увеличения ёмкости сети недостаточно. Что действительно необходимо, так это разумные эффективные методы управления графиком и контроль загруженности.

Исторически сети на базе IP предоставляли всем приложениям только простейшую услугу по доставке данных по мере возможности. Однако потребности со временем изменились. Организации, потратившие миллионы долларов на установку сети на базе IP для передачи данных между локальными сетями, сталкиваются теперь с тем, что такие конфигурации не способны эффективно поддерживать новые мультимедийные приложения реального времени с многоадресной рассылкой.

ATM – единственная сетевая технология, которая изначально разрабатывалась для поддержки обычного трафика Transfer Control Protocol (TCP) и User Datagram Protocol (UDP) наряду с трафиком реального времени. Однако ориентация на ATM означает либо создание новой сетевой инфраструктуры для трафика реального времени, либо замену имеющейся конфигурации на базе IP, причём оба варианта обойдутся весьма недёшево.

Поэтому потребность в поддержке нескольких типов трафика с различными требованиями к качеству услуг в рамках архитектуры TCP/IP весьма насущна. Эту задачу призваны решить два ключевых инструмента: транспортный протокол реального времени (Real-Time Transport Protocol, RTP) и протокол резервирования ресурсов (Resource Reservation Protocol, RSVP).

RTP гарантирует доставку данных одному или более адресатам с задержкой в заданных пределах. Это означает, что данные могут быть воспроизведены в реальном времени. RSVP позволяет конечным системам резервировать сетевые ресурсы для получения необходимого качества услуг, в особенности ресурсы для трафика реального времени по протоколу RTP.

Наиболее широко используемый протокол транспортного уровня – это TCP. Хотя TCP позволяет поддерживать множество разнообразных распределённых приложений, он не подходит для приложений реального времени.

В приложениях реального времени отправитель генерирует поток данных с постоянной скоростью, а получатель(-и) должен предоставлять эти данные приложению с той же самой скоростью. Такие при-

ложения включают аудио- и видеоконференции, распространение живого видео (для немедленного воспроизведения), разделяемые рабочие области, удалённую диагностику в медицине, компьютерную телефонию, распределённое интерактивное моделирование, игры и мониторинг в реальном времени.

Использование TCP в качестве транспортного протокола для этих приложений невозможно по нескольким причинам. Во-первых, данный протокол позволяет установить соединение только между двумя конечными точками и, следовательно, не подходит для многоадресной передачи. Он предусматривает повторную передачу потерянных сегментов, прибывающих в то время, когда приложение реального времени уже их не ждёт. Кроме того, у TCP нет удобного механизма привязки информации о синхронизации к сегментам, что также является требованием приложений реального времени.

Другой широко используемый протокол транспортного уровня – UDP не имеет первых двух ограничений (соединение «точка–точка» и передача потерянных сегментов), но и он не предоставляет критической информации о синхронизации. Таким образом, UDP сам по себе не имеет каких-либо инструментов общего назначения для приложений реального времени.

Несмотря на то, что каждое приложение реального времени может обладать своими собственными механизмами для поддержки передачи в реальном времени, они имеют много общих черт, что делает определение единого протокола весьма желательным. Стандартный протокол такого рода – RTP, определённый в RFC 1889.

В типичной среде реального времени отправитель генерирует пакеты с постоянной скоростью. Они отправляются им через одинаковые интервалы времени, проходят через сеть и принимаются получателем, воспроизводящим данные в реальном времени по их получении.

Однако ввиду вариации задержки при передаче пакетов по сети они прибывают через нерегулярные интервалы. Для компенсации этого эффекта поступающие пакеты буферизуются, придерживаются на некоторое время и затем предоставляются с постоянной скоростью программному обеспечению, генерирующему вывод. Чтобы такая схема работала, каждый пакет получает отметку о времени – таким образом получатель может воспроизвести поступающие данные с той же скоростью, что и отправитель.

RTP поддерживает передачу данных в реальном времени между несколькими участниками сеанса. (Сеанс – это логическая связь между двумя и более пользователями RTP, поддерживаемая в течение всего времени передачи данных. Процесс открытия сеанса выходит за рамки RTP.)

Хотя RTP может использоваться и для одноадресной передачи в реальном времени, его сила – в поддержке многоадресной передачи. Для этого каждый блок данных RTP содержит идентификатор отправителя, указывающий, кто из участников генерирует данные. Блоки данных RTP содержат также отметку о времени, чтобы данные могли быть с правильными интервалами воспроизведены принимающей стороной.

Кроме того, RTP определяет формат полезной нагрузки передаваемых данных. С этим напрямую связана концепция синхронизации, за которую частично отвечает микшер – механизм трансляции RTP. Принимая потоки пакетов RTP от одного или более источников, он комбинирует их и посылает новый поток пакетов RTP одному или более получателям. Микшер может просто комбинировать данные, а также изменять их формат.

Пример приложения для микшера – комбинирование нескольких источников звука. Например, предположим, что часть систем данного аудиосеанса генерирует каждая свой собственный поток RTP. Большую часть времени только один источник активен, хотя иногда одновременно «говорят» несколько источников.

Если новая система хочет принять участие в сеансе, но её канал до сети не имеет достаточной точной ёмкости для поддержки всех потоков RTP, то микшер получает все эти потоки, объединяет их в один и передаёт последний новому члену сеанса. При получении нескольких потоков микшер складывает значения импульсно-кодовой модуляции. Заголовок RTP, генерируемый микшером, включает идентификатор(-ы) отправителя(-ей), чьи данные присутствуют в пакете.

Более простое устройство создаёт один исходящий пакет RTP для каждого поступающего пакета RTP. Этот механизм, называемый транслятором, может изменить формат данных в пакете или использовать иной комплект низкоуровневых протоколов для передачи данных из одного домена в другой. Например, потенциальный получатель может оказаться не в состоянии обрабатывать высокоскоростной видеосигнал, используемый другими участниками сеанса. Тогда транслятор конвертирует видео в формат более низкого качества, требующий не такой высокой скорости передачи данных.

Каждый пакет RTP имеет основной заголовок, а также, возможно, дополнительные поля, специфичные для приложения. Структуру основного заголовка иллюстрирует рис. 1.10. Первые 12 октетов состоят из следующих полей:

– поле версии (2 бита): текущая версия – вторая;

– поле заполнения (1 бит): это поле сигнализирует о наличии заполняющих октетов в конце полезной нагрузки. (Заполнение применяется, когда приложение требует, чтобы размер полезной нагрузки был кратен, например, 32 битам.) В этом случае последний октет указывает число заполняющих октетов;

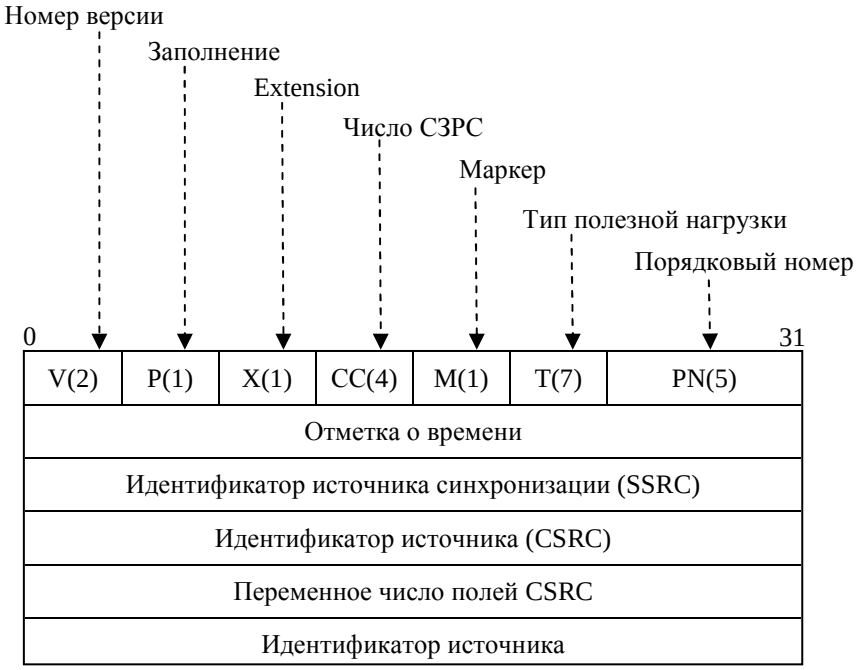


**Рис. 1.10. Структура RTP-заголовка**

– поле расширения заголовка (1 бит): когда это поле задано, то за основным заголовком следует ещё один, дополнительный, используемый в экспериментальных расширениях RTP;

– поле числа отправителей (4 бита): это поле содержит число идентификаторов отправителей, чьи данные находятся в пакете, причём сами идентификаторы следуют за основным заголовком;

– поле маркера (1 бит): смысл бита маркера зависит от типа полезной нагрузки. Бит маркера используется обычно для указания границ потока данных. В случае видео он задаёт конец кадра. В случае голоса он задаёт начало речи после периода молчания;

– поле типа полезной нагрузки (7 бит): это поле идентифицирует тип полезной нагрузки и формат данных, включая сжатие и шифрование. В стационарном состоянии отправитель использует только один тип полезной нагрузки в течение сеанса, но он может его изменить в ответ на изменение условий, если об этом сигнализирует протокол управления передачей в реальном времени (Real-Time Transport Control Protocol);

– поле порядкового номера (16 бит): каждый источник начинает нумеровать пакеты с произвольного номера, увеличиваемого затем на единицу с каждым посланным пакетом данных RTP. Это позволяет обнаружить потерю пакетов и определить порядок пакетов с одинаковой отметкой о времени. Несколько последовательных пакетов могут иметь одну и ту же отметку о времени, если логически они порождены в один и тот же момент (например, пакеты, принадлежащие одному и тому же видеокадру);

– поле отметки о времени (32 бита): здесь записывается момент времени, когда был создан первый октет данных полезной нагрузки. Единицы, в которых в этом поле указывается время, зависят от типа полезной нагрузки. Значение определяется по локальным часам отправителя;

– поле идентификатора источника синхронизации: генерируемое случайным образом число, уникальным образом идентифицирующее источник в течение сеанса.

RTP-заголовок содержит ряд полей, идентифицирующих такие элементы, как формат пакета, порядковый номер, источники, границы и тип полезной нагрузки. За фиксированным заголовком могут следовать другие поля, содержащие дополнительную информацию о данных.

За основным заголовком может следовать одно или более полей идентификаторов отправителей, чьи данные присутствуют в полезной нагрузке. Эти идентификаторы вставляются микшером.

Протокол RTP используется только для передачи пользовательских данных – обычно многоадресной – всем участникам сеанса. Отдельный протокол управления передачей в реальном времени (Real-

Time Transport Control Protocol, RTCP) работает с несколькими адресатами для обеспечения обратной связи с отправителями данных RTP и другими участниками сеанса.

RTCP использует тот же самый базовый транспортный протокол, что и RTP (обычно UDP), но другой номер порта. Каждый участник сеанса периодически посылает RTCP-пакет всем остальным участникам сеанса. RFC 1889 описывает три функции, выполняемые RTCP.

Первая функция состоит в обеспечении качества услуг и обратной связи в случае перегрузки. Поскольку RTCP-пакеты являются многоадресными, то все участники сеанса могут оценить, насколько хороши работа и приём других участников. Сообщения отправителя позволяют получателям оценить скорость данных и качество передачи. Сообщения получателей содержат информацию о проблемах, с которыми они сталкиваются, включая утерю пакетов и избыточную неравномерность передачи. Например, скорость передачи для аудио- и видеоприложения может быть снижена, если линия не обеспечивает желаемого качества услуг при данной скорости передачи.

Обратная связь с получателями важна также для диагностирования ошибок при распространении.

Анализируя сообщения всех участников сеанса, администратор сети может определить, касается ли данная проблема одного участника или носит общий характер.

Вторая основная функция RTCP – идентификация отправителя. Пакеты RTCP содержат стандартное текстовое описание отправителя. Они предоставляют больше информации об отправителе пакетов данных, чем случайным образом выбранный идентификатор источника синхронизации. Кроме того, они помогают пользователю идентифицировать потоки, относящиеся к различным сеансам. Так, они дают пользователю возможность определить, что одновременно открыты отдельные сеансы для аудио и видео.

Третья функция состоит в оценке размеров сеанса и масштабировании. Для обеспечения качества услуг и обратной связи с целью управления загруженностью, а также с целью идентификации отправителя, все участники периодически посылают пакеты RTCP. Частота передачи этих пакетов снижается с ростом числа участников.

При небольшом числе участников один пакет RTCP посылается максимум каждые пять секунд. RFC 1889 г. описывает алгоритм, согласно которому участники ограничивают частоту RTCP-пакетов в зависимости от общего числа участников. Цель состоит в том, чтобы трафик RTCP не превышал 5 % от общего трафика сеанса.

Назначение любой сети состоит в доставке данных получателем с гарантированным качеством услуг, включающих пропускную способность, задержку и допустимый предел вариации задержки. С ростом числа пользователей и приложений обеспечить качество услуг становится всё труднее.

Всего лишь реагировать на перегрузку – уже недостаточно. Необходим инструмент, с помощью которого перегрузок можно было бы избежать вообще, т.е. сделать так, чтобы приложения могли резервировать сетевые ресурсы в соответствии с требуемым качеством услуг.

Превентивные меры полезны как при одноадресной, так и при многоадресной передаче. При одноадресной передаче два приложения договариваются о конкретном уровне качества услуг для данного сеанса. Если сеть сильно загружена, то она может оказаться не в состоянии предоставить услуги необходимого качества. В этой ситуации приложениям придётся отложить сеанс до лучших времен или попробовать снизить требования к качеству услуг, если это возможно.

Решение в данном случае состоит в резервировании одноадресными приложениями ресурсов для обеспечения требуемого уровня услуг. Тогда маршрутизаторы на предполагаемом пути выделяют ресурсы (например, место в очереди и часть ёмкости исходящей линии). Если маршрутизатор не имеет возможности выделить ресурсы вследствие ранее взятых на себя обязательств, то он извещает об этом приложение. При этом приложение может попытаться инициировать другой сеанс с меньшими требованиями к качеству услуг или перенести его на более поздний срок.

Многоадресная рассылка ставит гораздо более сложные задачи по резервированию ресурсов. Она ведёт к генерации огромных объёмов сетевого трафика – в случае, например, таких приложений, как видео, или при наличии большой и рассредоточенной группы получателей. Однако трафик от источника многоадресной рассылки может быть в принципе значительно снижен.

Для этого есть два основания. Во-первых, некоторые члены группы могут не нуждаться в доставке данных от конкретного источника в определённый период времени. Так, члены одной группы могут получать информацию одновременно по двум каналам (от двух источников), но при этом получатель может быть заинтересован в приёме только одного канала.

Во-вторых, некоторые члены группы в состоянии обрабатывать только часть передаваемой отправителем информации. Например, видеопоток может состоять из двух компонентов: один с низким качеством картинки, а другой – с высоким. Такой формат имеет ряд алгоритмов сжатия видео: они генери-

руют базовый компонент с картинкой низкого качества и дополнительный компонент с повышенным разрешением.

Некоторые получатели могут не иметь достаточной вычислительной мощи для обработки компонентов с высоким разрешением или быть подключены к сети через подсеть или канал, не обладающие достаточной емкостью, чтобы пропустить полный сигнал.

Резервирование ресурсов позволяет маршрутизаторам заранее определить, в состоянии ли они осуществить доставку многоадресного трафика всем получателям.

В предыдущих попытках реализации резервирования ресурсов и в принятых во frame relay и ATM подходах необходимые ресурсы запрашивает источник потока данных. Этот метод достаточен в случае одноадресной передачи, потому что передающее приложение передаёт данные в определённом темпе, а необходимый уровень качества услуг заложен в схему передачи.

Однако такой подход нельзя использовать для многоадресной рассылки. У разных членов группы могут быть неодинаковые требования к ресурсам. Если исходный поток может быть разделён на подпотоки, то некоторые члены группы, вполне возможно, пожелают получать только один из них. В частности, некоторые получатели смогут обрабатывать только компонент видеосигнала низкого разрешения. Или если несколько отправителей вещают на одну группу, то получатель может выбрать только одного отправителя или некоторое их подмножество. Наконец, требования различных получателей к качеству услуг могут меняться в зависимости от оборудования вывода, мощности процессора и скорости канала.

По этой причине резервирование ресурсов получателем видится предпочтительным. Отправители могут предоставить маршрутизаторам общие характеристики трафика (например, темп передачи данных и вариабельность), но получатели должны сами определить требуемый уровень качества услуг. Маршрутизаторы затем сводят воедино запросы на выделение ресурсов на общих участках дерева распространения.

В основе RSVP лежат три концепции, касающиеся потоков данных: сеанс, спецификация потока и спецификация фильтра. *Сеанс* – это поток данных, идентифицируемый по адресату. Отметим, что эта концепция отличается от концепции сеанса RTP, хотя сеансы RSVP и RTP могут иметь взаимно однозначное соответствие. После резервирования маршрутизатором ресурсов для конкретного адресата он рассматривает это как начало сеанса и выделяет ресурсы на время этого сеанса.

Запрос на резервирование от конечной системы-получателя, называемый описателем потока, состоит из спецификации потока и фильтра. *Спецификация потока* определяет требуемое качество услуг и используется узлом для задания параметров планировщика пакетов. Маршрутизатор передаёт пакеты с заданным набором предпочтений, опираясь на текущую спецификацию потока.

*Спецификация фильтра* определяет набор пакетов, под которые запрашиваются ресурсы. Вместе с сеансом она определяет набор пакетов (или поток), для которых требуемое качество услуг должно быть обеспечено (рис. 1.11). Любые другие пакеты, направляемые этому адресату, обрабатываются постольку, поскольку сеть в состоянии это сделать.

Спецификация фильтра позволяет отобрать пакеты для применения к ним спецификации потока. Прошедшим фильтр пакетам гарантируется качество услуг, остальные доставляются по мере возможности.

RSVP не определяет содержания спецификации потока, он просто передаёт запрос. Спецификация потока обычно включает класс услуг: Rspec (R означает резерв) и Tspec (T означает трафик). Два других параметра представляют собой набор чисел. Параметр Rspec определяет требуемое качество услуг, а параметр Tspec описывает поток данных. Содержимое Rspec и Tspec прозрачно для RSVP.

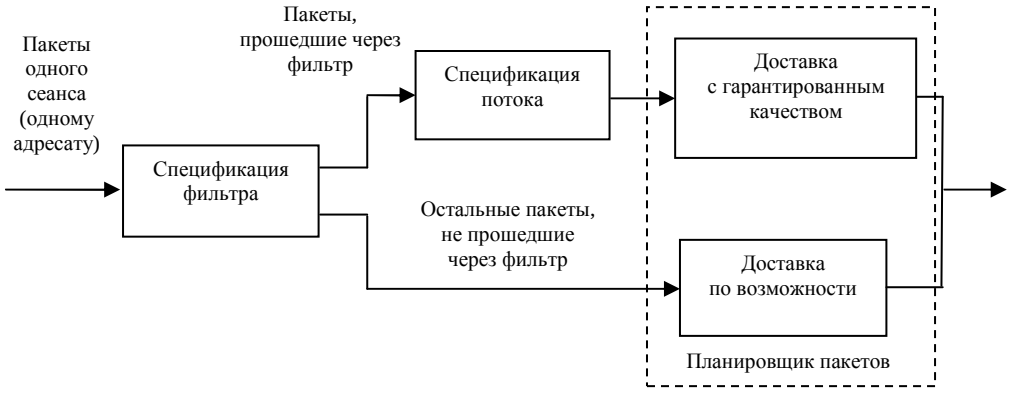

**Рис. 1.11. Прохождение пакетов на примере одного сеанса на одном маршрутизаторе**

В принципе, спецификация фильтра описывает произвольное подмножество пакетов одного сеанса (т.е. тех пакетов, адресат которых определяется данным сеансом). Например, спецификация фильтра может определять только конкретных отправителей либо определять протоколы или пакеты, поля протокольных заголовков которых совпадают с заданными.

Связь между сеансом, спецификацией потока и спецификацией фильтра иллюстрирует рис. 1.12. Каждый приходящий пакет относится по крайней мере к одному сеансу и рассматривается в соответствии с логическим потоком для этого сеанса.

Если пакет не принадлежит к какому-либо сеансу, то он доставляется постольку, поскольку есть свободные ресурсы.

Основная сложность RSVP связана с многоадресной рассылкой. Пример многоадресной конфигурации приведён на рис. 1.13.

Хосты Gl, G2 и G3 принадлежат к многоадресной группе, получающей дейтаграммы с соответствующим адресом получателя. Хосты S1 и S2 посылают данные по этому адресу. Линии показывают дерево маршрутизации для S1 и для S2. Линии со стрелками показывают пути передачи данных от S1 и S2

Эта конфигурация состоит из четырёх маршрутизаторов. Канал между двумя любыми маршрутизаторами, изображаемый линией, может представлять собой как прямой канал, так и подсеть. Три хоста – Gl, G2 и G3 – входят в одну группу и получают дейтаграммы с соответствующим групповым адресом. Данные по этому адресу передаются двумя хостами – S1 и S2. Линия соответствует дереву маршрутизации для S1 и данной группы, а другая линия – для S2 и данной группы. Линии со стрелками указывают направление передачи пакетов от S1 и от S2.

Рисунок показывает, что все четыре маршрутизатора должны знать о резервировании ресурсов каждым получателем. Таким образом, запросы на выделение ресурсов распространяются в обратном направлении по дереву маршрутизации.

RSVP использует два основных типа сообщений: Resv и Path. Сообщения Resv генерируются получателями и распространяются вверх по дереву, причём каждый узел по пути объединяет и компонует пакеты от разных получателей, когда это возможно. Эти сообщения приводят к переходу маршрутизатора в состояние резервирования ресурсов для данного сеанса (группового адреса).

В конце концов все объединённые сообщения Resv достигают хостов-отправителей. Основываясь на полученной информации, они задают надлежащие параметры управления трафиком для первого транзитного узла.

Поток сообщений Resv показан на рис. 1.14.


**Рис. 1.12. Реализация приоритезации трафика на различных уровнях модели OSI**

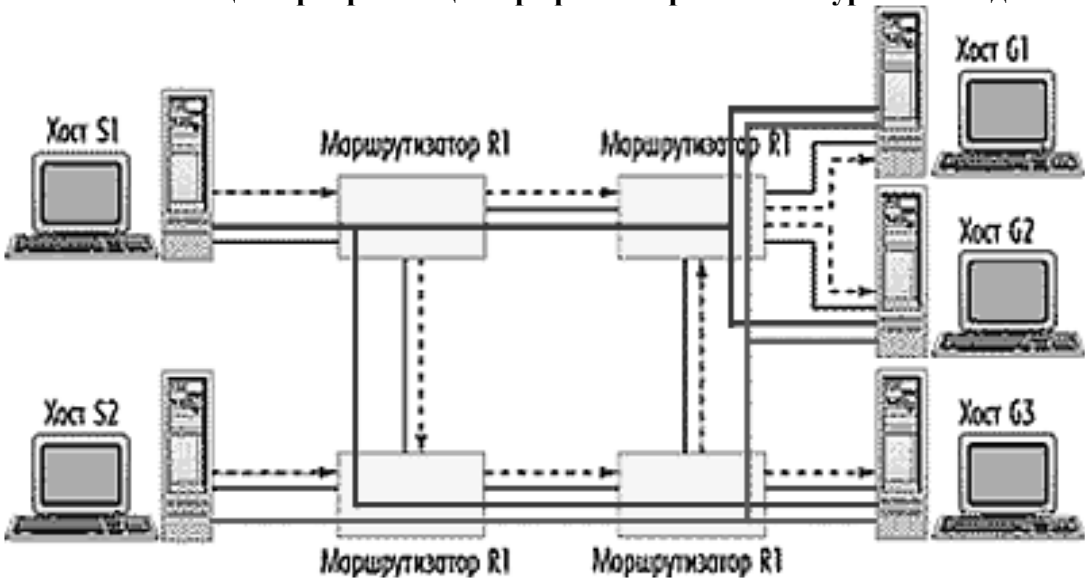


**Рис. 1.13. Иллюстрация работы RSVP**

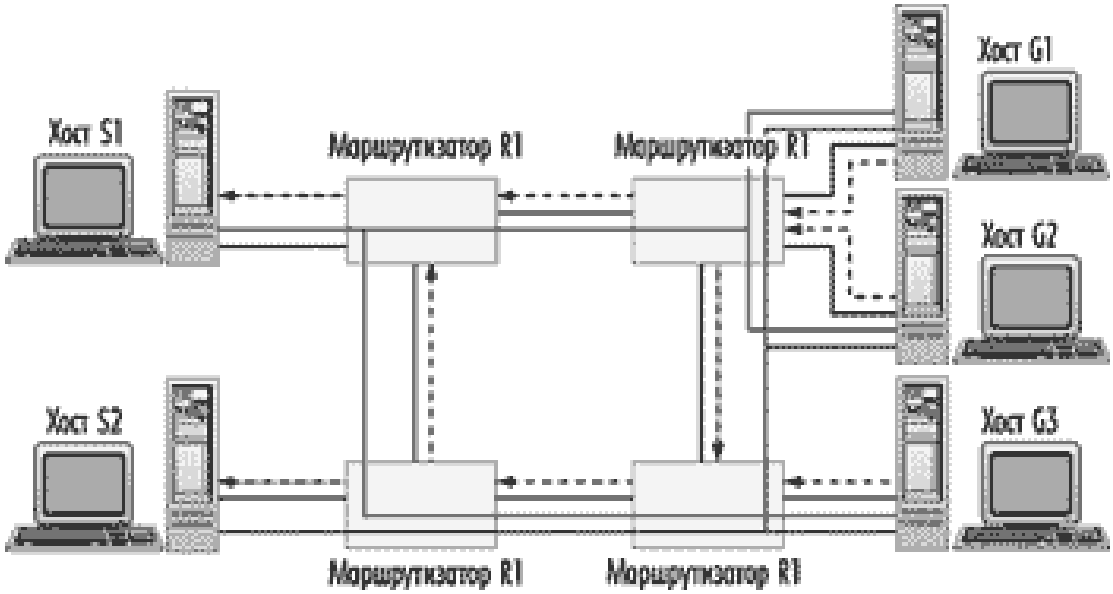


**Рис. 1.14. Иллюстрация объединения сообщений работы Resv**

В этой конфигурации сообщения Resv объединяются, в результате только одно сообщение передаётся обратно по каждой ветви дерева распространения. Сообщения необходимо периодически повторять в результате.

Обратим внимание, что сообщения объединяются; следовательно, только одно сообщение передаётся вверх по любой ветви комбинированного дерева доставки. Однако эти сообщения должны периодически рассылаться вновь для продления срока резервирования ресурсов.

Сообщение Path используется для распространения информации об обратном маршруте. Всеми современными протоколами многоадресной маршрутизации поддерживается только прямой маршрут в виде дерева распространения (вниз от отправителя). Но сообщения Resv должны передаваться в обратном направлении через все промежуточные маршрутизаторы всем хостам-отправителям.

Поскольку протокол маршрутизации не предоставляет информации об обратном маршруте, она передаётся RSVP в сообщениях Path. Любой хост, желающий стать отправителем, посылает сообщение Path всем членам группы. По пути каждый маршрутизатор и каждый хост-адресат переходит в состояние path, указывающее, что пакеты для этого отправителя должны пересылаться на транзитный узел, с которого данный пакет получен. Пакеты Path передаются по тем же самым путям, что и пакеты данных.

Рассмотрим работу протокола RSVP. С точки зрения хоста, работа протокола состоит из следующих этапов (первые два этапа в этой последовательности имеют иногда обратную очерёдность).

- Получатель вступает в группу многоадресной рассылки посредством отправки сообщения по протоколу IGMP соседнему маршрутизатору.
- Потенциальный отправитель отправляет сообщение по адресу группы.
- Получатель принимает сообщение Path, идентифицирующее отправителя.
- Теперь, когда получатель имеет информацию об обратном пути, он может отправлять сообщения Resv с дескрипторами потока.
- Сообщения Resv передаются по сети отправителю.
- Отправитель начинает передачу данных.
- Получатель начинает приём пакетов данных.

Вчерашние методы работы с большими объёмами трафика совершенно непригодны для современных систем. Без новых инструментов удовлетворять растущим требованиям к передаче данных в связи с ростом их объёма, распространением приложений реального времени и многоадресной рассылки невозможно. RTP и RSVP обеспечивают надёжный фундамент для сетей следующего поколения LAN.

В качестве примера реального применения этих протоколов можно привести модель VoIP (Voice over IP) – передачи голоса по IP-сетям, которая описана в стандарте H.232 и предусматривает передачу аудио-, видеоинформации и данных через IP-сеть. В этом случае протокол реального времени RTP используется для установления соединения, а протокол RSVP – для резервирования ресурсов сети.

# Глава 2. МЕЖСЕТЕВЫЕ ЭКРАНЫ И ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ

В данной главе рассмотрены конкретные схемы реализации таких систем. В частности, анализируется применение межсетевых экранов (МСЭ) для защиты корпоративных ресурсов от несанкционированного использования. Обсуждаются вопросы применения виртуальных частных сетей, позволяющих удалённым пользователям и целым службам осуществлять доступ в корпоративную сеть в защищённом режиме через незащищённую сеть общего пользования [4].

## 2.1. ЗАЩИТА С ПОМОЩЬЮ МЕЖСЕТЕВЫХ ЭКРАНОВ

Подключение корпоративной сети к Internet снижает её защищённость от внешнего проникновения. Для защиты конфиденциальной информации, находящейся в корпоративной сети, наряду с мерами безопасности, обычно используют дополнительные средства. Им и посвящена эта глава.

Защита основана на применении специальной стратегии контроля доступа к сетевым ресурсам и использовании межсетевого экрана – брандмауэра. *Межсетевой экран* – это система безопасности, контролирующая доступ к защищаемой сети, например частной корпоративной сети. Такая сеть защищается от сети общего пользования, в которой режим безопасной работы не предусмотрен, например от Internet. Любой запрос, поступивший из сети общего пользования в защищаемую систему, проходит через межсетевой экран, что позволяет отказаться от индивидуальной защиты каждого сервера и сетевого компьютера.

Межсетевой экран обычно находится в точке взаимодействия корпоративной сети и Internet. Здесь он выполняет аутентификацию и другие процедуры сетевой безопасности, препятствующие проникновению в сеть нелегальных пользователей. Схема контроля с помощью МСЭ доступа из Internet в корпоративную сеть показана на рис. 2.1.

Для обеспечения эффективной защиты с помощью брандмауэра компаниям прежде всего следует разработать стратегию сетевой безопасности. Необходимо определить ресурсы, требующие защиты, и типы атак, которым они могут быть подвергнуты. Затем оговариваются условия применения этих ресурсов, круг пользователей, имеющих к ним доступ, и последовательность действий в случае нарушения прав доступа. Стратегия предусматривает ряд правил, которые применяются для тестирования прибывших пакетов.

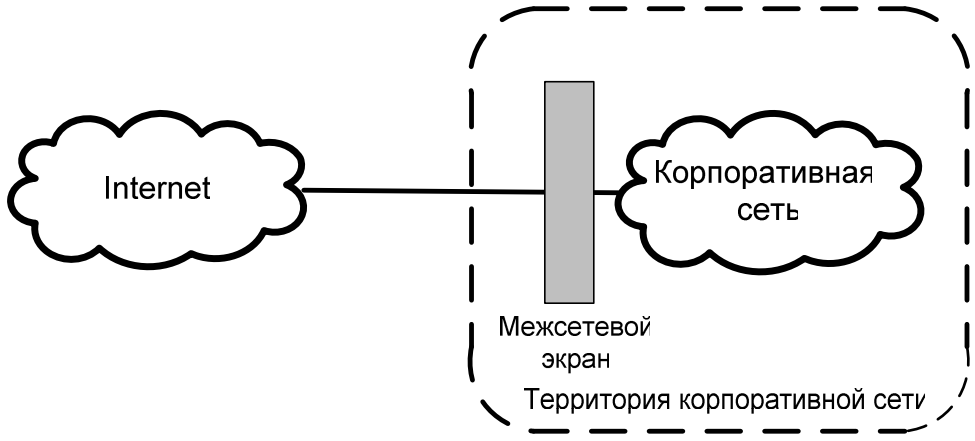


**Рис. 2.1. Схема контролируемого межсетевым экраном доступа в корпоративную сеть из Internet [4]**

В этих правилах определяются допустимая интенсивность поступающего извне информационного потока и адреса источников, по которым возможен/невозможен доступ от внешних структур. Специальные действия включают либо приём пакета, либо отказ от него. Межсетевой экран отвечает за фильтрацию информационного потока в соответствии с выработанной стратегией [4].

**Типы межсетевых экранов.** Брандмауэры можно разделить на три основных категории:

– фильтры пакетов;

– прокси-серверы (они включают шлюзы приложений и шлюзы линий связи);
– фильтры пакетов с сохранением адресов.

Кроме того, МСЭ может быть образован шлюзом приложений и фильтром пакетов либо прокси-сервером и фильтром пакетов с сохранением адресов. Различные типы брандмауэров показаны на рис. 2.2.

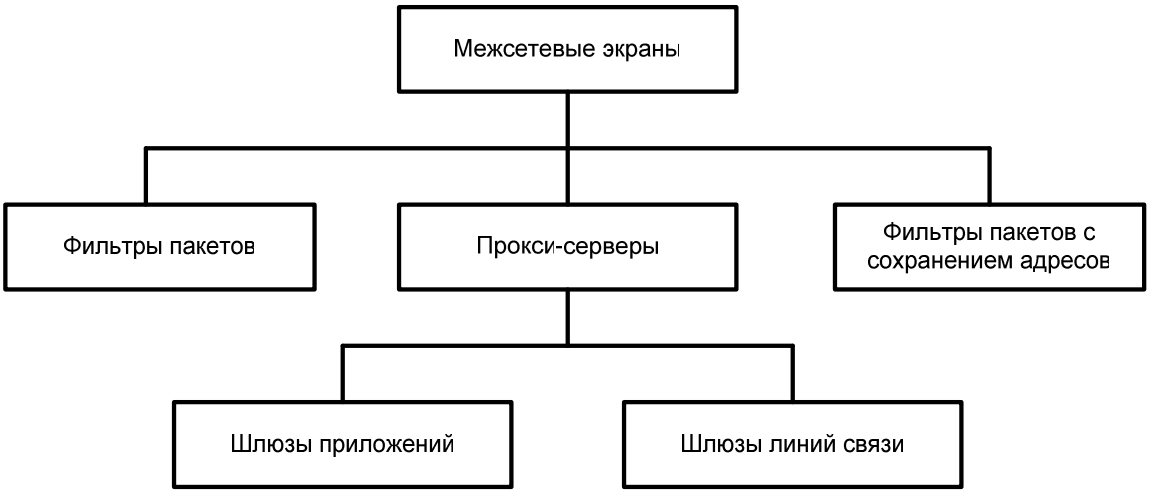


**Рис. 2.2. Классификация межсетевых экранов**

**Фильтры пакетов.** *Фильтр пакетов* – это межсетевой экран, который проверяет каждый пакет в соответствии с правилами фильтрации, определяемыми пользователем, и решает, пропустить его или блокировать. Так, правила фильтрации могут запрещать пропуск всех запросов Telnet. На основании этого запрета межсетевой экран будет блокировать все сообщения, в заголовках которых номер порта равен 23 (номер порта сети Telnet по умолчанию). Правила фильтрации можно построить либо на основании IP-адресов источника или пункта назначения, либо используя номера их портов четвёртого уровня. Решения принимаются на сетевом и транспортном уровнях.

Фильтры пакетов с сохранением адресов характеризуются высокой производительностью, их можно использовать в существующих маршрутизаторах. К сожалению, среди всех МСЭ их возможности наиболее ограничены. Недостаток фильтров состоит в отсутствии проверки регистрации, что мешает обнаружить несанкционированное проникновение в сеть. Кроме того, решение о блокировке или пропуске сообщения принимается на основе данных об адресе либо номере порта источника и пункта назначения. К сожалению, номера портов можно подделать. Следовательно, злоумышленник постарается получить доступ к сетевым ресурсам сразу же вслед за авторизованным пользователем.

**Прокси-серверы.** Приложение, которое переадресует пользовательский запрос к службам, поддерживающим стратегию безопасности, называется *прокси-сервером.* Любое соединение между пользователем и сервером обработки запросов осуществляется через прокси-сервер. Он работает как посредник между клиентом и сервером приложения. Поскольку прокси-сервер функционирует как пункт контроля, в котором запрос проверяется на соответствие приложению, он работает очень интенсивно и при большом потоке запросов не успевает их обслуживать.

Различают два класса прокси-серверов: шлюзы приложений, которые работают на уровне приложений, и шлюзы линий связи, функционирующие на транспортном уровне.

**Шлюзы приложений.** *Шлюз приложений* – это прокси-сервер, обеспечивающий функции контроля доступа на уровне прикладных задач. Он действует как шлюз уровня приложений между защищённой сетью и системой, в которой не предусмотрен режим безопасной работы. Поскольку шлюз приложений работает на уровне прикладных задач, он детально исследует трафик, обеспечивая наибольшую защиту сети. Так, он может препятствовать доступу в сеть определённых приложений, например PTP. С целью учёта и проверки безопасности устройство регистрирует все операции, связанные с работой приложений.

Шлюзы приложений могут закрыть информацию. Поскольку все запросы служб в защищённой сети проходят через шлюз приложений, то он преобразует сетевые IP-адреса и тем самым скрывает IP-адреса корпоративной структуры. Сетевой IP-адрес каждого экспортируемого пакета – сообщения, направляемого из корпоративной сети в Internet, – заменяется его собственным адресом IP. Преобразование сетевого адреса позволяет свободно использовать незарегистрированные IP-адреса в защищаемой сети, поскольку в случае выхода корпоративного клиента во внешние структуры шлюз приложений преобразует этот адрес в необходимый.

**Шлюзы линий связи.** *Шлюз линий связи* – это прокси-сервер, который подтверждает разрешение на сессию TCP или UDP, прежде чем линия связи пройдёт через межсетевой экран. Шлюз данного уровня активно участвует в формировании канала передачи данных и не позволяет пакетам проходить через него, если не соблюдены необходимые правила доступа.

Шлюз линий связи обеспечивает более слабую защиту по сравнению со шлюзом приложений, поскольку первый разрешает сессию TCP или UDP без детального анализа приложений, использующих эти транспортные службы. Более того, после начала сессии приложение, которому потребовалась транспортировка, может использовать любую сформированную линию связи. Эта особенность снижает защищённость сети от атак злоумышленников. В отличие от шлюза соединений шлюз приложений может отделить приложения, которые следует блокировать, от тех, что необходимо пропустить.

**Фильтры пакетов с сохранением адресов.** Хотя шлюзы приложений обеспечивают наивысшую степень безопасности среди рассмотренных ранее межсетевых экранов, выполняемая ими тщательная проверка снижает производительность сети. Шлюз, фильтрующий пакеты с сохранением адресов, позволяет обеспечить жёсткие требования по безопасности, не снижая производительности сети. В отличие от шлюза приложений он проверяет поступающие пакеты на сетевом уровне, но не обрабатывает их. Данный брандмауэр сохраняет информацию о режиме каждой сессии. Режим сессии включает фазу взаимодействия и конечный пункт, в котором находится приложение. Когда фильтр пакетов с сохранением адреса принимает пакет с данными, он проверяет его содержимое на соответствие режиму сессии. Если содержимое пакета отличается от ожидаемого режима, шлюз блокирует продолжение сессии.

**Архитектура межсетевого экрана.** *Архитектура МСЭ* – это способ расположения компонентов брандмауэра, обеспечивающий эффективную защиту от несанкционированного доступа. Архитектуру МСЭ определяют уже после того, как разработана стратегия защиты сети, поскольку межсетевой экран усиливает её [4].

В стратегии защиты сети особое внимание уделяется безопасности её границ, так называемому *периметру сети.* Корпоративная сеть обычно содержит множество периметров, которые условно можно разделить на три группы. Это *дальний периметр* сети, один или несколько *внутренних периметров* и *периметр, ближайший к ядру сети.* Дальний периметр служит границей между корпоративными ресурсами, которые необходимо защищать, и ресурсами внешних структур, которые компанией не контролируются. Внутренние периметры ограничивают часть корпоративной сети, для которой необходима дополнительная защита.

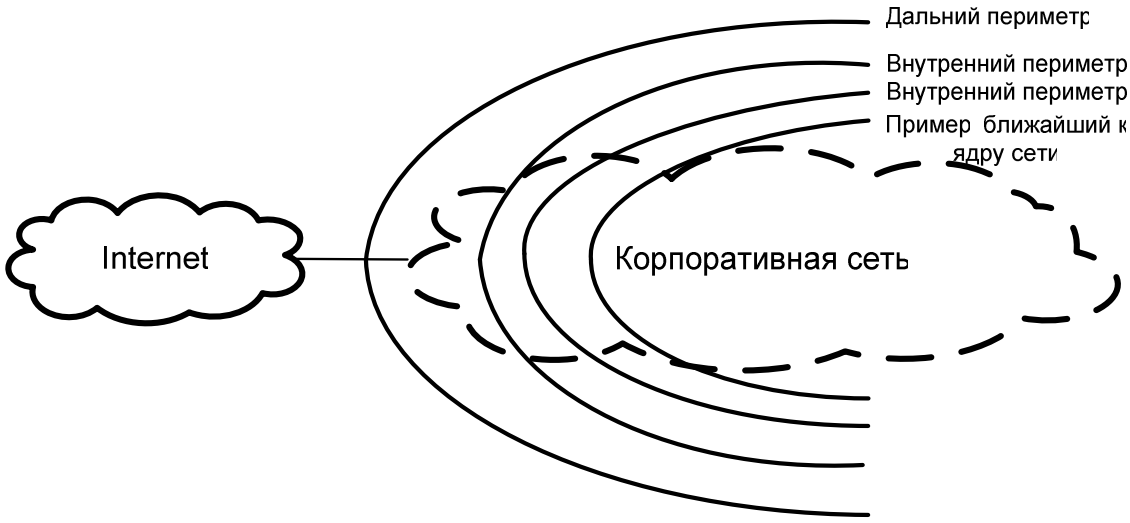


**Рис. 2.3. Периметры сети**

Взаимосвязь между тремя типами периметров сети показана на рис. 2.3. Здесь представлена только одна возможная конфигурация МСЭ. Далеко не все сети оборудуются тремя уровнями сетевых периметров. Организации следует подобрать необходимое число межсетевых экранов в соответствии с конкретной стратегией безопасности.

Рассмотрим три наиболее распространённых архитектуры брандмауэров.

***Межсетевой экран с двунаправленным хостом.*** Данный МСЭ оборудуется двумя интерфейсами. Один интерфейс соединяет хост с частной сетью, другой обеспечивает подключение к Internet или любой другой незащищённой сети. Следовательно, весь IP-трафик, поступающий из Internet, прежде чем

попасть в корпоративную сеть, должен пройти через этот защитный барьер. Точно так же внутренний узел через двунаправленный хост взаимодействует с узлами Internet.

Непосредственная связь, проходящая через двунаправленный хост защиты, блокируется. Это означает, что функция прямой трансляции IP-трафика для данного устройства исключена и IP-пакеты из одной сети не могут непосредственно направляться в другую. Двунаправленный хост не используется в качестве маршрутизатора. Существует запрет на прямую передачу IP-пакетов до тех пор, пока не гарантировано логическое разъединение двух сетей: частной и глобальной. Следовательно, даже при системных сбоях межсетевой экран остаётся в рабочем состоянии. Данные могут пройти брандмауэр только через прокси-сервер и никогда через системный уровень. Применение межсетевого экрана с двунаправленным хостом показано на рис. 2.4.

Это устройство можно использовать для полной блокировки доступа в частную сеть, пока исполняются прокси-сервисы, например Telnet, FTP, HTTP.

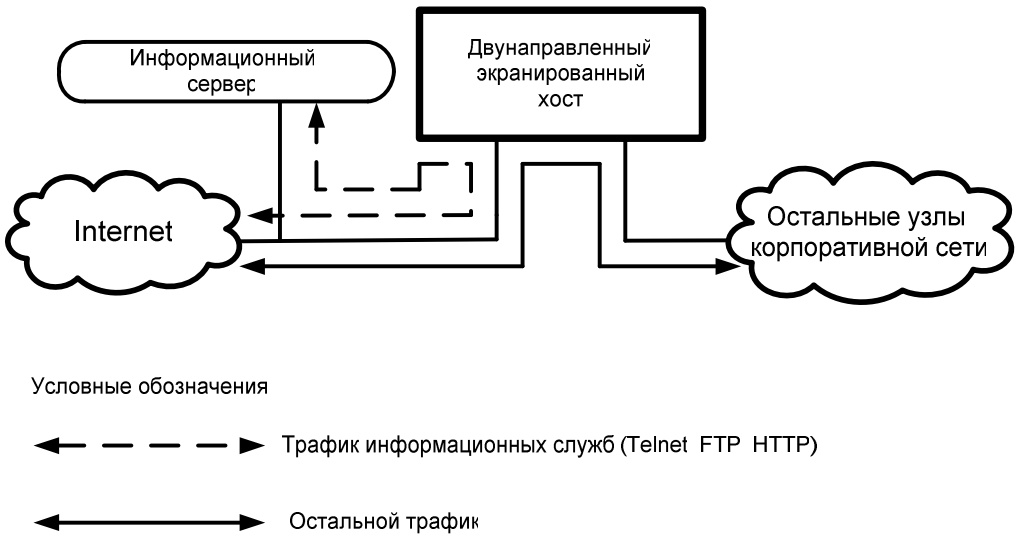


**Рис. 2.4. Архитектура МСЭ с двунаправленным хостом**

Как показано на рис. 2.4, сервер, работающий с данными службами, находится между фильтрующим пакеты маршрутизатором, который может быть установлен, и двунаправленным хостом. Такая конфигурация препятствует проникновению злоумышленников в систему с двунаправленным хостом.

***Брандмауэр с экранированным хостом.*** В отличие от МСЭ с двунаправленным хостом, который подключается к обеим сетям одновременно, *экранированный хост* соединён только с частной сетью. Это устройство имеет собственное название – *хост-бастион.* Между узлом и сетью Internet размещают отдельный экранирующий маршрутизатор. Таким образом, МСЭ с экранированным хостом представляет собой комбинацию фильтрующего пакеты маршрутизатора и шлюза приложений.

Экранирующий маршрутизатор выполняет функцию фильтрации пакетов и конфигурируется таким образом, чтобы хост-бастион являлся единственным компьютером корпоративной сети, доступ к которому возможен из Internet. Самый высокий уровень безопасности достигается при такой конфигурации экранирующего маршрутизатора, когда это устройство полностью блокирует информационный поток к заданным портам хоста-бастиона. МСЭ с экранируемым хостом показан на рис. 2.5.

Гибкая система конфигурирования маршрутизатора позволяет открывать или блокировать соединения внутренних узлов и Internet.

Основная функция хоста-бастиона состоит в разделении информационных потоков, представляющих опасность, прежде чем они смогут достичь бастиона и других внутренних узлов. Поскольку хост-бастион по сравнению с остальными элементами частной сети наиболее подвержен атакам, он обычно является самым защищённым элементом сети. Как правило, в сети устанавливают два и более хоста-бастиона.

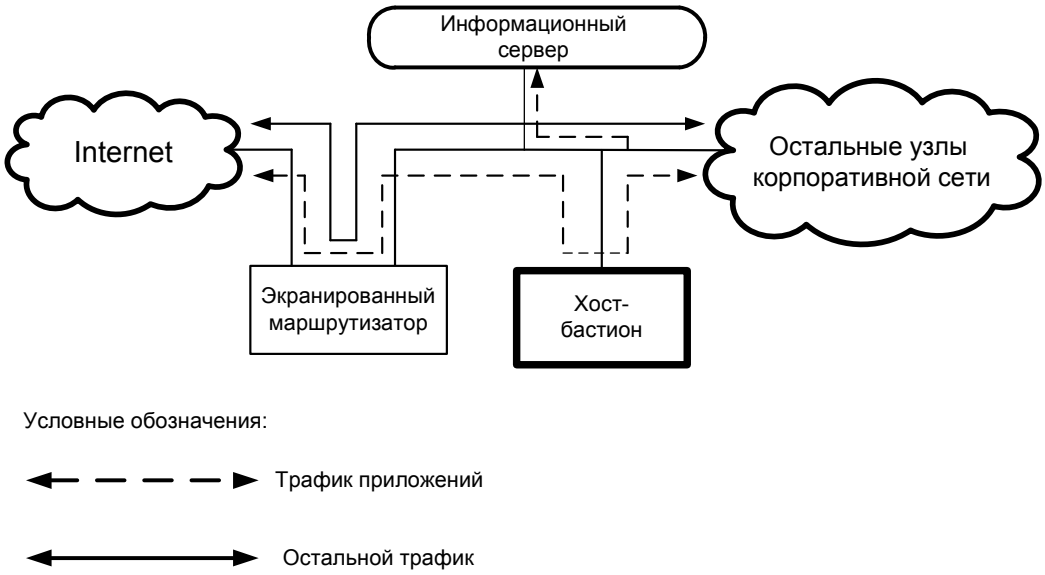


**Рис. 2.5. Брандмауэр с экранируемым хостом**

Преимущество данной структуры состоит в том, что информационный сервер общего пользования, поддерживающий протоколы FTP, Telnet, HTTP, может находиться в сети между экранирующим маршрутизатором и хостом-бастионом. Если нужно усилить систему защиты, то проводят такую конфигурацию, что доступ к информационному серверу, который необходим и внешним, и внутренним пользователям, разрешается только через хост-бастион. На практике одной из основных функций хоста-бастиона считается исполнение роли прокси-сервера для различных служб, включающих FTP, HTTP, Telnet, DNS, SMTP.

К сожалению, если злоумышленнику удаётся прорваться через хост-бастион, то все узлы частной сети становятся ему доступны. В брандмауэре с двунаправленным хостом невозможно пройти через защитный хост, минуя соответствующий прокси-сервер. В отличие от этой схемы МСЭ с экранируемым хостом требует наличия экранирующего маршрутизатора и хоста-бастиона.

***Брандмауэр с экранирующей подсетью.*** Эта схема расширяет возможности рассмотренной выше системы, в которой в качестве элемента защиты используется экранированный хост. Здесь тоже применяются экранирующий, или внешний, маршрутизатор и хост-бастион. Однако данный защитный барьер, называемый *демилитаризованной зоной* (DeMilitarized Zone – DMZ), создаёт высший уровень безопасности за счёт дополнительного периметра сети, усиливающего изоляцию частной сети от Internet. Межсетевой экран определяет границы DMZ между внешним и внутренним маршрутизаторами, причём последний находится ближе к частной сети. Демилитаризованная зона – это внутренняя экранирующая подсеть, границами которой служат внутренний и внешний маршрутизаторы. Как показано на рис. 2.6, хост-бастион и информационный сервер находятся внутри DMZ.


**Рис. 2.6. Схема межсетевого экрана с применением экранирующей подсети как средства защиты**

DMZ можно рассматривать как изолированную сеть между частной структурой и Internet. Ограничивая доступ к системам, расположенным в DMZ, внешний маршрутизатор защищает сеть от атак извне. С его помощью блокируется и исходящий информационный поток от клиентов частной сети, которые не обладают соответствующими правами. Внутренний маршрутизатор управляет доступом из DMZ в частную сеть. При этом осуществляется пропуск прямого трафика от хоста-бастиона к узлам частной сети, находящимся вне DMZ, и соответствующего обратного потока.

Чтобы атака достигла какого-либо внутреннего узла, находящегося за DMZ, необходимо пройти оба маршрутизатора. Кроме того, при данной архитектуре для внешних структур существует только сеть DMZ, в то время как сама частная сеть остаётся закрытой. Однако формирование корректной конфигурации двух маршрутизаторов и хоста-бастиона остаётся трудоёмким.

## 2.2. ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ

При обмене данными через незащищённые сети общего пользования безопасное соединение между источником и приёмником сообщений обеспечивают *виртуальные частные сети* (Virtual Private Network – VPN). Безопасное соединение обычно связывают с применением частных сетей. (Частная сеть представляет собой структуру для обмена данными, которая принадлежит либо контролируется через аренду выделенных линий связи конкретной организацией.) В этой главе рассматриваются методы, которые VPN использует для преобразования характеристик незащищённой сети общего пользования в характеристики частной защищённой сети. Сети VPN снижают стоимость удалённого доступа, применяя ресурсы сетей общего пользования. По сравнению с другими решениями, включая и частные сети, VPN предоставляет самую недорогую услугу.

Сети VPN уже на протяжении многих лет применяются в телефонии, а с развитием интеллектуальных сетей стали доминировать. Сети ретрансляции кадра, которые были рассмотрены ранее, тоже могут быть отнесены к VPN. Понятие виртуальных частных сетей можно признать нововведением только для технологии IP-сетей, таких как Internet. Вероятно, некоторые авторы потому применяют термины Internet-VPN и виртуальной частной сети передачи данных, чтобы отделить VPN, описанные в настоящей главе, от остальных структур с тем же названием. В этой части определение VPN является синонимом определения Internet-VPN [4].

Цель виртуальной частной сети – обеспечить защищённый режим передачи пользовательских данных через незащищённый Internet. Это даёт возможность компаниям применять Internet в качестве опорной сети для своих корпоративных структур, что позволяет создавать виртуальные защищённые каналы для взаимодействия через Internet головных учреждений корпорации с филиалами либо удалёнными офисами. Из-за низкой стоимости службы VPN большая часть информационного потока теперь направляется через виртуальные частные сети, базирующиеся на Internet, вместо ранее применявшихся ГВС, обеспечивающих конфиденциальность.

VPN использует криптографирование данных и другие способы обеспечения безопасности, препятствующие несанкционированному доступу к информации. Кроме того, эти методы направлены на обеспечение гарантии того, что попытка модифицировать данные в процессе передачи по сети Internet будет замечена. В технологии VPN применяется метод туннелирования для транспортировки шифрованных данных через Internet. Туннелирование – механизм инкапсуляции одного протокола передачи данных в другой. В контексте сети Internet под туннелированием подразумевается возможность инкапсулировать в протокол IP зашифрованные пакеты протоколов IP, IPX, App1eTallk. Точно так же в контексте VPN туннелирование маскирует исходный протокол сетевого уровня путём кодирования пакета и размещения зашифрованного пакета в IP-конверт, который, по сути, остаётся IP-пакетом и в защищённом режиме передаётся через Internet. На приёмном конце конверт отбрасывается, а его содержимое декодируется и переправляется соответствующему устройству доступа, например маршрутизатору.

Представим, что корпорация создаёт частный туннель через Internet для безопасной доставки своих данных.

Туннель позволяет корпорации создать виртуальную ГВС, используя Internet. Это значительно дешевле, чем построение частной ГВС, и лучше защищает от злоумышленников.

К тому же сети VPN гарантируют заданный уровень качества обслуживания QoS. Для VPN обычно определяется верхняя граница среднего времени задержки пакета в процессе его передачи по сети. Заданные требования могут включать и определение нижней границы полосы пропускания, доступной для пользователя. Эти требования разрабатываются совместно с провайдером услуг через систему со-

глашений об уровне обслуживания (Service Level Agreement – SLA). Большинство поставщиков услуг имеет собственные частные опорные IP-сети. Следовательно, провайдеры находятся в лучшем положении относительно обеспечения гарантий качества обслуживания. Однако эти сети охватывают значительно меньшие территории, чем Internet. Иногда провайдер услуг заключает частные двусторонние соглашения с другими операторами связи, частные IP-сети которых покрывают большие территории. Эти соглашения позволяют провайдеру передать собственный высокоприоритетный трафик – поток данных со строгими QoS-требованиями – в сети с гарантированным уровнем QoS, вместо того чтобы транслировать его через Internet, где величина задержки непредсказуема.

Виртуальные частные сети можно определить следующим образом:

VPN = туннелирование + защита + гарантирование QoS.

Далее рассматриваются способы туннелирования, использующиеся для построения сетей VPN.

**Преимущества сетей VPN.** Сети VPN не являются дорогостоящими: они обеспечивают доступ к корпоративной сети для удалённого или мобильного пользователя по цене местного телефонного вызова.

Эти сети обеспечивают базу для построения корпоративных сетей intranet и extranet. Корпорации могут использовать глобальный характер Internet и применять VPN для объединения всех своих филиалов в частную сеть, называющуюся intranet. Часть сети intranet корпорация может сделать доступной для поставщиков и стратегических партнеров, используя extranet. Оба типа сетей, intranet и extranet, детально рассматриваются в главе 3.

Туннели VPN обеспечивают доставку немаршрутизируемых протоколов в конкретные участки ЛВС корпоративной intranet. Таким же способом виртуальные частные сети позволяют определённым приложениям достигать intranet.

Сети VPN значительно расширили возможности использования частных IP-адресов. Так как вместо маршрутизации через ГВС приложения доставляются через туннели, компании могут назначать им собственные IP-адреса, поскольку эти адреса не привлекают излишнего внимания внешних пользователей.

**Типы частных виртуальных сетей.** В настоящее время существует три типа VPN. Несмотря на то, что их разработка преследует одну цель – использовать Internet в качестве опорной сети для организации взаимодействия производственных подразделений компании, каждый тип удовлетворяет потребности различных групп организации:

– *VPN доступа* обеспечивают удаленных пользователей: коммивояжеров, мобильных пользователей, служащих, работающих дома, филиалы компаний – надёжной системой доступа в корпоративную сеть;

– сеть *intranet VPN* позволяет осуществлять защищённое соединение филиалов с центральной компаний;

– *extranet VPN* предоставляет защищённый доступ в корпоративную сеть потребителям, поставщикам и партнёрам по бизнесу.

Ниже речь пойдёт о сети VPN как основе для построения intranet и extranet.

**Архитектура VPN.** Сеть VPN состоит из четырёх компонентов: клиента VPN, сервера доступа к сети (Network Access Server – NAS), устройства, находящегося в конце туннеля, или сервера VPN, и протокола VPN. Для формирования канала виртуальной частной сети удалённый пользователь – VPN-клиент – инициирует соединение PPP с сервером доступа провайдера через телефонную сеть общего пользования. *Сервер доступа к сети* (NAS) – это устройство, на которое поступают вызовы по аналоговым либо цифровым линиям через ISDN. Оно принадлежит провайдеру услуг. После проверки прав пользователя с помощью соответствующего метода аутентификации NAS направляет пакеты в туннель, который соединяет его и сервер VPN. Последний может находиться либо у провайдера, либо в корпоративной сети в зависимости от того, какая модель данного устройства применяется. (Модели VPN будут рассмотрены позже.) Сервер VPN забирает пакеты из туннеля, разворачивает их и доставляет в корпоративную сеть. Схема построения VPN представлена на рис. 2.7.

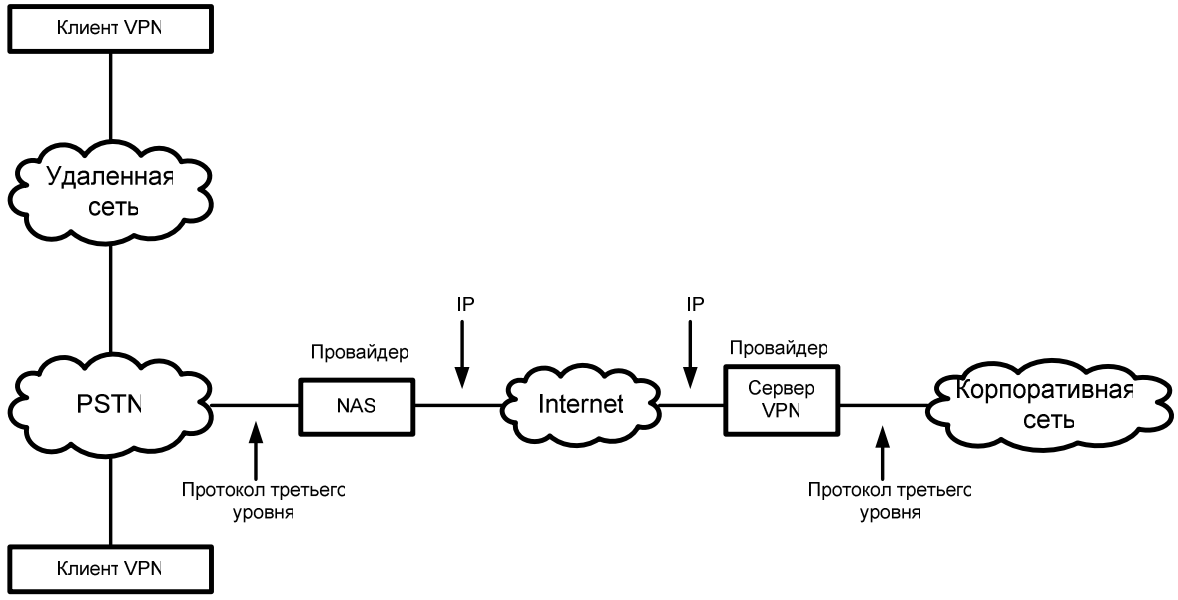


**Рис. 2.7. Структура виртуальной частной сети**

Для установки соединения VPN применяется четыре типа протоколов, причём три из них являются расширенными модификациями протокола:

– протокол туннелирования для парного соединения абонентов (Point-to-Point Tunneling Protocol – PPTP);
– протокол передачи данных на втором уровне модели OSI (Layer 2 Forwar-ding – L2F);
– протокол туннелирования на втором уровне модели OSI (Layer 2 Tunneling – L2TP);
– стек IP-протоколов безопасности (IP Security Protocol – IPSec).

Когда протоколы PPTP и L2F были представлены на рассмотрение группе IETF, их характеристики было решено объединить в общем протоколе туннелирования под названием L2TP.

Предложенные типы протоколов можно разделить на протоколы туннелирования второго и третьего уровней модели OSI. К первой группе относятся протоколы PPTP, L2F, L2TP. Ко второй причислен стек протоколов IPSec.

**Работа протоколов туннелирования второго уровня модели OSI.** Данный тип протоколов работает на уровне линий связи – второй уровень модели OSI. Эти протоколы сначала инкапсулируют пакеты третьего уровня в пакеты PPP второго уровня и только потом инкапсулируют их в IP. Безопасность передачи информации обеспечивается протоколом PPP. Подлинность пользователя проверяется с помощью существующих методов аутентификации протоколов PPP – PAP и CHAP. Для криптографирования данных не требуется никакого предварительного условия. Эта функция может быть исполнена самим пользователем до его обращения к сервису VPN.

Общая схема процесса формирования туннеля для протоколов туннелирования второго уровня показана на рис. 2.8. Клиент инициирует соединение PPP, вызывая по телефону сервер NAS. Затем с помощью диалогового режима протокола управления каналом связи клиент непосредственно формирует канал PPP.

Как только соединение установлено, NAS с помощью протокола PAP либо CHAP аутентифицирует запрашивающего пользователя. Если проверка его подлинности завершилась успешно, то NAS пытается установить соединение PPP с сервером VPN, используя согласование параметров по протоколу LCP. В свою очередь сервер VPN применяет протокол PAP либо CHAP для аутентификации сервера доступа к сети. Сервер VPN и клиент используют диалоговый режим протокола управления сетью для согласования протокола сетевого уровня. На этом процесс создания туннеля завершается.

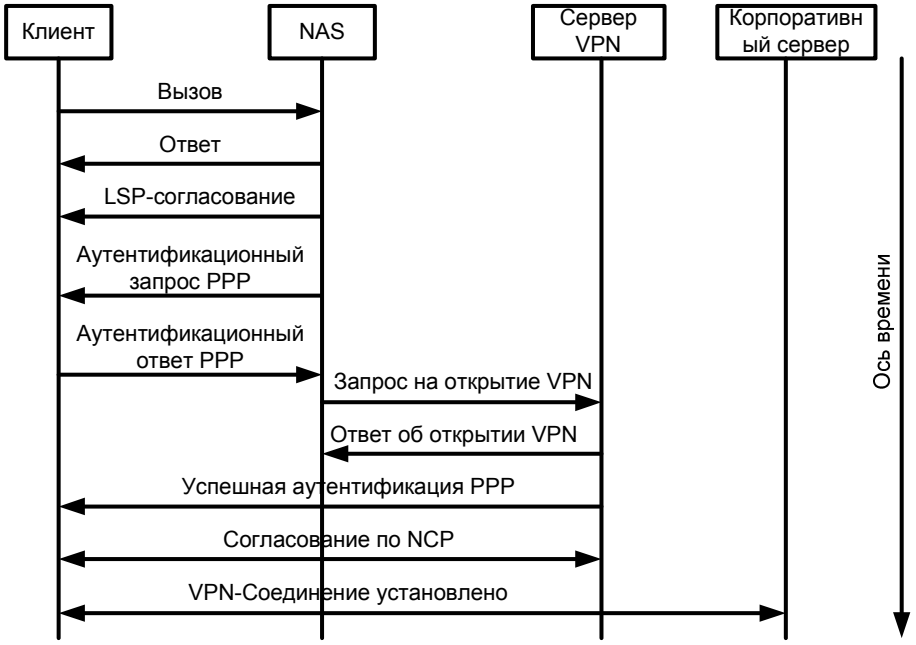


**Рис. 2.8. Процесс создания туннеля для VPN с помощью протоколов второго уровня**

**Протокол туннелирования для PPP.** Этот тип протокола разработан компанией Microsoft совместно с группой компаний – поставщиков оборудования, включая Ascend Communications и 3Com.

Данный тип протокола – PPTP – позволяет инкапсулировать в пакеты IP пакеты протоколов IPX, NetBEUI, IP, разрешая проходить приложениям не IP-типа через Internet. Как вариант PPP, он управляет только парными соединениями абонентов, режим соединения одного абонента с несколькими невозможен. Важно отметить, что ядром PPTP является IP, т.е. данный протокол разрабатывался исключительно для сетей IP.

При использовании PPTP сервер доступа к сети, разрешающий удалённому пользователю инициировать вызов через VPN, называют PPTP-концентратором доступа (Point-to-Point Tunneling Protocol Access Concentrator – PAC), а к серверу VPN обращаются как к сетевому серверу PPTP (Point-to-Point Tunneling Protocol Network Server – PNS). Все компоненты виртуальной частной сети, построенной на основе PPTP, представлены на рис. 2.9.

В протоколе PPTP отсутствует режим криптографирования последовательных пакетов. Вместо этого используются возможности шифрования протоколов PAP и CHAP. Пакет PPTP инкапсулируется для универсальной маршрутизации (Generic Routing Encapsulation – GRE) и затем передаётся через IP. PPTP разделяет каналы данных и управления на поток управления, следующий через TCP, и поток данных, передаваемых через GRE. Формат пакетов PPTP показан на рис. 2.10. Полезные данные PPP состоят непосредственно из самих данных и заголовков IP.

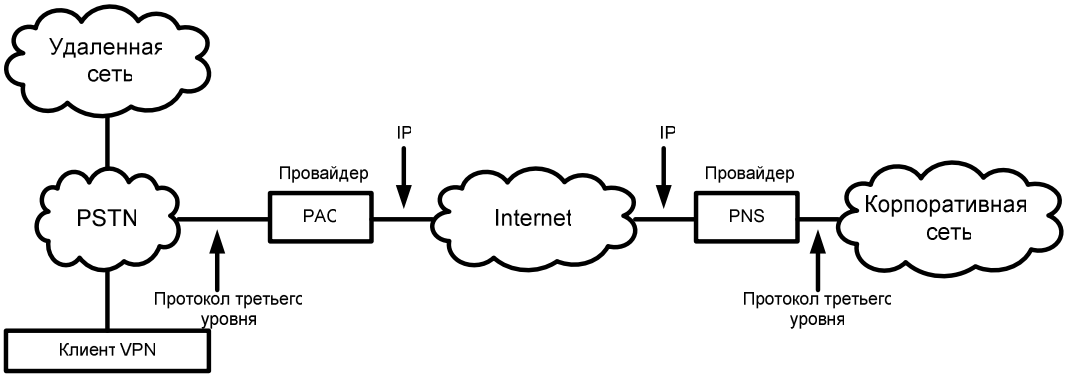


**Рис. 2.9. Элементы сети VPN, использующей протокол PPTP**

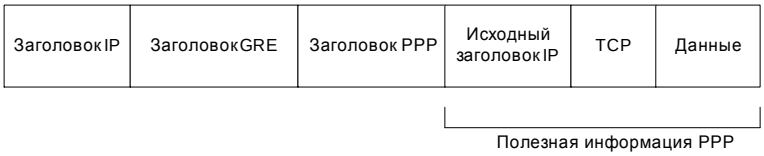


**Рис. 2.10. Формат пакета протокола PPTP**

Протокол PPTP является узкоспециализированным, однако большинство современных сетей VPN основано именно на нём. В PPTP для контроля за передачей информации применяется TCP. TCP обеспечивает контроль скорости передачи, которая ограничивает объём передаваемых данных, сводя к минимуму необходимость повторных передач из-за отброшенных пакетов. Это способствует оптимальному использованию полосы пропускания.

**Протокол передачи данных на втором уровне модели OSI.** L2F – это специализированный протокол, разработанный компанией Cisco Systems. Он не зависит от типа протокола, используемого на предшествующем уровне, и поэтому используется для пересылки через сети X.25, ретрансляции кадра и ATM.

Протокол L2F поддерживает IP, IPX, AppleTalk и использует UDP для туннелирования через Internet.

В сетях, где применяется L2F, сервер виртуальной частной сети называется базовым шлюзом. Для аутентификации клиента, осуществляющего вызов по телефонной линии, этот протокол использует PPP. L2F поддерживает и такие схемы проверки подлинности абонента, как RADIUS и TACACS+. Компоненты VPN, построенной на основе протокола L2F, показаны на рис. 2.11.

В отличие от PPTP протокол 2P формирует собственный заголовок инкапсуляции, который не зависит от IP и GRE. Это позволяет использовать L2F в различных типах сетей. На рис. 2.12 показан формат пакета L2F Полезная информация, передаваемая протоколом SLIP/PPP, инкапсулируется в пакет L2F месте с заголовком L2F и дополняется контрольной суммой, которая записывается в качестве окончания.

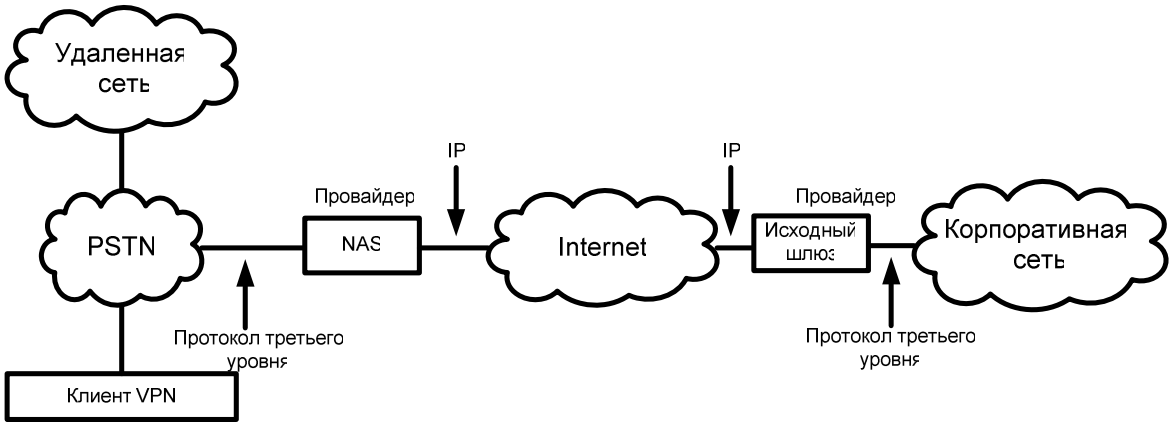


**Рис. 2.11. Компоненты сети VPN, использующей протокол L2F**

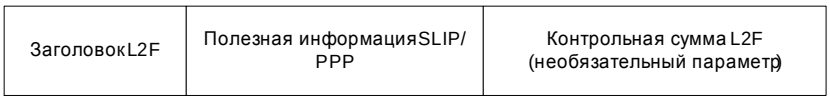


**Рис. 2.12. Формат пакета протокола L2F**

**Протокол туннелирования на втором уровне модели OSI.** Данный протокол (L2TP) объединяет свойства PPTP и L2F. В отличие от PPTP, который транспортируется посредством TCP, L2TP в качестве транспортного протокола использует UDP, а не GRE. Так как многие межсетевые экраны не поддерживают GRE, протокол L2TP для них является более дружественным, чем PPTP В случае применения данного протокола сервер доступа к сети называют L2TP – концентратором доступа (Layer 2 Tunneling Protocol Access Concentrator – LAC), а к серверу VPN обращаются как к сетевому серверу L2TP (Layer 2 Tunneling Protocol Network Server – LNS). Все компоненты сети VPN, построенной на основе L2TP, представлены на рис. 2.13.

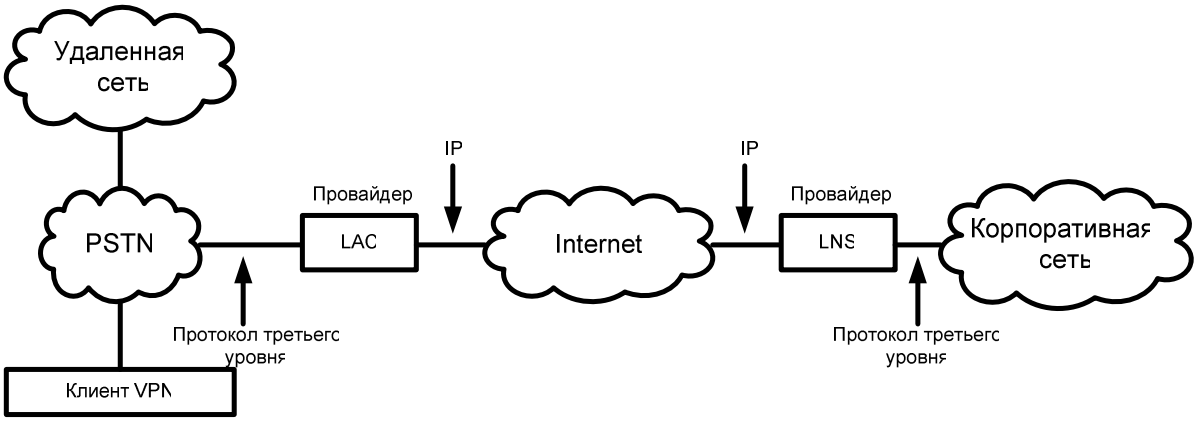


**Рис. 2.13. Компоненты сети VPN, использующей протокол L2TP**

Так как в L2TP используются коммутируемые соединения PPP, то для аутентификации клиента применяются протоколы PAP и CHAP. Однако для проверки прав абонента может быть использован и RADIUS. Протокол L2TP обеспечивает формирование нескольких туннелей для одной пары конечных пунктов. В этом случае пользователь может создать набор туннелей с различными уровнями качества предоставляемых услуг для двух взаимодействующих пунктов. Формат пакетов L2TP показан на рис. 2.14.

Данный протокол поддерживается многими производителями оборудования. Предполагается, что как только он получит статус стандарта, то станет наиболее используемым. Для криптографирования данных при применении L2TP используется стек протоколов IPSec. Если L2TP обнаруживает, что IPSec на удалённом конце не поддерживается, то применяется более слабая защита PPP. В зависимости от модели VPN криптографирование данных может осуществляться на рабочей станции клиента либо с помощью концентратора доступа LAC.

**Протокол туннелирования третьего уровня модели OSI.** Стек протоколов IPSec был первоначально разработан для усиления безопасности в TCP/IP. Этот набор протоколов обеспечивает аутентификацию, конфиденциальность и целостность данных на уровне пакета. Всё это достигается введением двух заголовков, обеспечивающих безопасность: заголовка аутентификации, который отвечает за целостность заголовков и аутентификацию, но не обеспечивает конфиденциальности, и заголовка защиты инкапсулированной полезной информации. Encapsutating Security Payload (ESP) позволяет криптографировать поступающие по очереди пакеты, при этом применяется стандартный протокол управления ключами для шифрования. Таким образом, VPN может использовать либо AH, либо ESP или оба протокола вместе. Authentication Header (AH) не обеспечивает режим криптографирования данных и поэтому применяется, когда необходима лишь проверка подлинности. Затраты при использовании AH ниже, чем при использовании ESP. Однако при необходимости криптографирования данных применяют ESP.

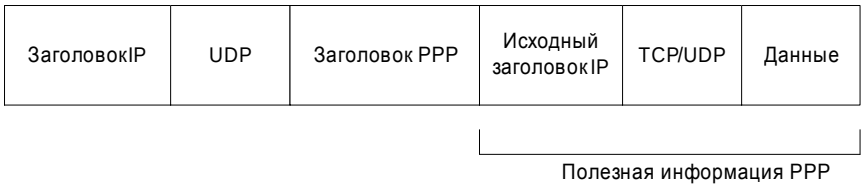


**Рис. 2.14. Формат пакета протокола L2TP**

Недостаток IPSec заключается в том, что этот набор протоколов поддерживается только в IP-сетях. Но для поддержания трафика сетей IPX и AppleTalk, который не относится к IP-сетям, можно предложить протоколы PPTP, L2F и L2TP, поскольку они принадлежат второму уровню. В отличие от IPSec протоколы туннелирования второго уровня поддерживают индивидуальные запросы на доступ по телефонным линиям, поскольку в них применяется протокол PPP аутентификации клиента. Он разрешает однородные телефонные соединения через провайдера. IPSec разработан для защиты линий связи между маршрутизаторами и межсетевыми экранами, он не обеспечивает аутентификацию пользователя.

## 2.3. ТИПЫ СЕТЕЙ VPN

Есть два способа построения VPN второго уровня. Это *NAS-инициируемая VPN* и *инициируемая клиентом VPN*. В обеих схемах VPN клиент инициирует удалённый вызов к провайдеру услуг связи по телефонной линии. Главное различие систем заключается в протяжённости туннеля.

**Инициируемая сервером доступа VPN.** В NAS-инициируемой VPN клиент начинает сессию с сервером доступа провайдера. В этом случае пользователю присваивается IP-адрес, который не зависит от его IP-адреса в локальной сети. За туннелирование пакетов через Internet к сервер VPN отвечает NAS.

Эту схему взаимодействия иногда называют *принудительной* VPN, поскольку клиент не участвует в её создании и при её использовании подчиняется принятым правилам. Криптографирование данных осуществляется между серверами NAS и VPN и двумя функциональными единицами, образующими концы туннеля. Принудительная схема VPN формируется без согласования с пользователем. Это означает, что для клиента VPN является прозрачной средой. Преимущество NAS-образуемой VPN состоит в том, что схема поддерживает многоканальный режим обслуживания, а это сокращает расходы, связанные с формированием отдельной VPN для каждого соединения. Однако подключение клиента к NAS происходит вне границ туннеля. Это делает VPN уязвимой для атак.

Схема NAS-образуемой VPN с применением протокола L2TP представлена на рис. 2.15. Данную модель можно рассматривать и как VPN, использующую внешние ресурсы, в которой запросами на удалённый доступ со стороны корпорации управляет провайдер. Эта модель наиболее приемлема для организаций, в которых подразделения информационного обеспечения не имеют оборудования, необходимого для управления VPN.

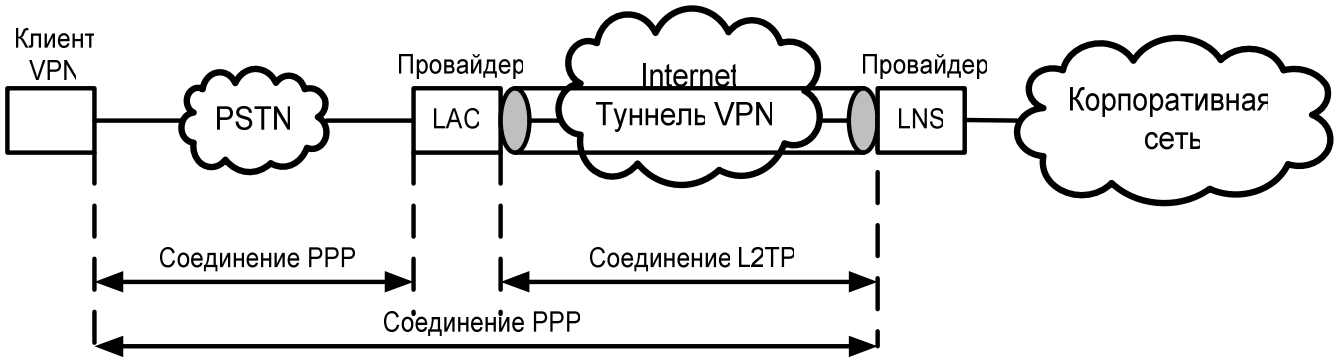


**Рис. 2.15. NAS-инициируемая модель VPN с применением протокола L2TP**

**Инициируемая клиентом VPN.** Характерной особенностью данной схемы является то, что в распоряжении клиента имеется служба VPN и, следовательно, у него установлено программное обеспечение для работы с ней. Клиент VPN осуществляет вызов по телефонной линии провайдера услуг для формирования сессии PPP.

Используя соединение с Internet, абонент устанавливает соединение с сервером VPN. В данной модели туннель проходит от VPN-клиента к VPN-серверу. Сервер доступа к сети не участвует в образовании туннеля. Инициируемую клиентом VPN обычно называют добровольной, поскольку сам клиент определяет, где и когда сформировать эту службу. Значит, клиент сам отвечает за необходимое криптографирование данных при обмене между своим конечным оборудованием и VPN-сервером.

VPN-сервер может находиться как у провайдера услуг, так и в корпоративной сети. Если сервер VPN находится внутри сети провайдера, то содержимое туннеля доставляется в корпоративную сеть через ГВС, которую маршрутизатор корпорации использует для доступа к провайдеру. В качестве ГВС может выступать сеть ретрансляции кадра либо ISDN. Если сервер VPN находится в корпоративной сети, то туннель проходит непосредственно от клиента в корпоративную сеть. Варианты схемы клиент-образуемой VPN с использованием протокола L2TP представлены на рис. 2.16. В первом случае сервер

VPN находится в сети провайдера, во втором – в корпоративной сети. Во втором варианте управление виртуальной частной сетью осуществляется в основном клиентом.

**Сравнение моделей VPN.** Клиент-инициируемая модель позволяет удалённым пользователям, на рабочем месте которых установлена программа клиент-VPN, использовать телефонную линию для формирования туннеля в корпоративную сеть. При этом не требуется наличия у провайдера программного обеспечения для VPN, т.е. провайдер может не обеспечивать функции NAS.

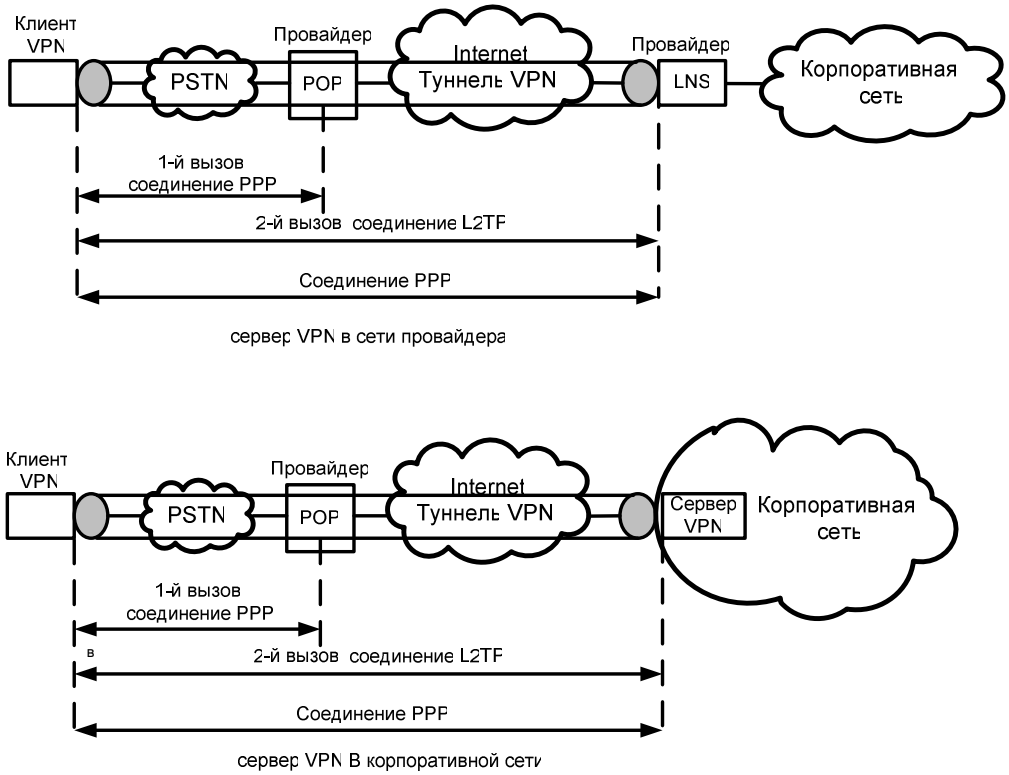


**Рис. 2.16. Инициируемая клиентом модель VPN с применением протокола L2TP**

В NAS-инициируемой модели провайдер должен обеспечивать функции сервера NAS. В отличие от NAS-инициируемой схемы инициируемая клиентом модель не привязывает сеть корпорации к какому-либо одному провайдеру услуг. Это позволяет организации выбирать провайдера, не изменяя при этом схемы адресации. Несанкционированный доступ в клиент-образуемую модель весьма затруднён. При реализации данной модели компания может не передавать базу данных проверки подлинности клиентов провайдеру услуг. Поскольку организация сама контролирует оба конца туннеля, она же и определяет требования к аутентификации пользователей для предотвращения несанкционированного доступа к информационным ресурсам. В NAS-инициируемой модели компания вынуждена предоставлять свою базу аутентификации провайдеру услуг. В этом случае у злоумышленника есть возможность проникнуть в сеть провайдера, воспользовавшись ошибочным опознанием.

NAS-инициируемые сети VPN позволяют клиентам поддерживать туннелирование данных, не прибегая к модернизации аппаратуры и к установке соответствующего программного обеспечения. Однако в этой модели провайдер сам управляет распределением адресного пространства и аутентификацией. Корпорации, возможно, понадобится реструктурировать схему распределения адресов, с тем, чтобы согласовать её с разработанной провайдером схемой. К тому же необходимо информировать провайдера обо всех изменениях, осуществляемых в корпоративной сети.

Протоколы VPN уровня 3, например IPSec, более приспособлены для NAS-образуемой модели, поскольку их разработка изначально предусматривала обеспечение защиты между маршрутизатором и межсетевым экраном.

На практике функции NAS встраиваются в маршрутизатор, а функции сервера VPN передаются межсетевому экрану. IPSec входит в состав протокола IPv6. Таким образом, если клиент VPN не использует протокол IPv6, то экономически неоправданно дополнять программное обеспечение его ко-

нечной станции функциями стека протоколов IPSec. Возможно, экономически более выгодно, чтобы эти функции исполнялись сетевым сервером доступа самого провайдера.

**Межсетевые экраны и сети VPN.** МСЭ и VPN тесно связаны между собой. Большинство брандмауэров обеспечивает туннели от одного МСЭ до другого с шифрованием передаваемых данных. В частности, шлюзы приложений обеспечивают закрытие IP-адресов с помощью инкапсуляции одного IP-пакета в другой. Согласно нашему определению, это туннелирование через виртуальную частную сеть.

МСЭ контролирует доступ к корпоративным сетевым ресурсам и способствует спокойной работе пользователя в сети. Рассмотрим структуру сети, представленную на рис. 2.17. Брандмауэр в каждой сети контролирует доступ к её ресурсам. Однако данные, транслируемые между двумя областями через Internet, могут быть подвержены атакам злоумышленников.

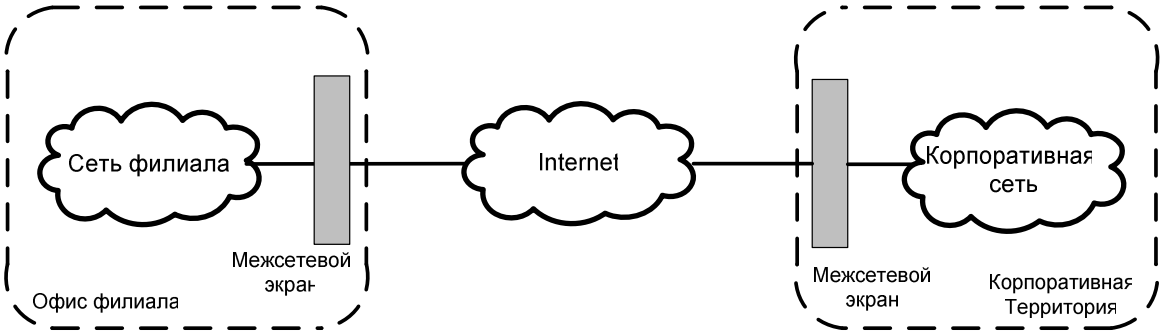


**Рис. 2.17. Межсетевые экраны, обеспечивающие проверку прав доступа в обе взаимодействующие сети**

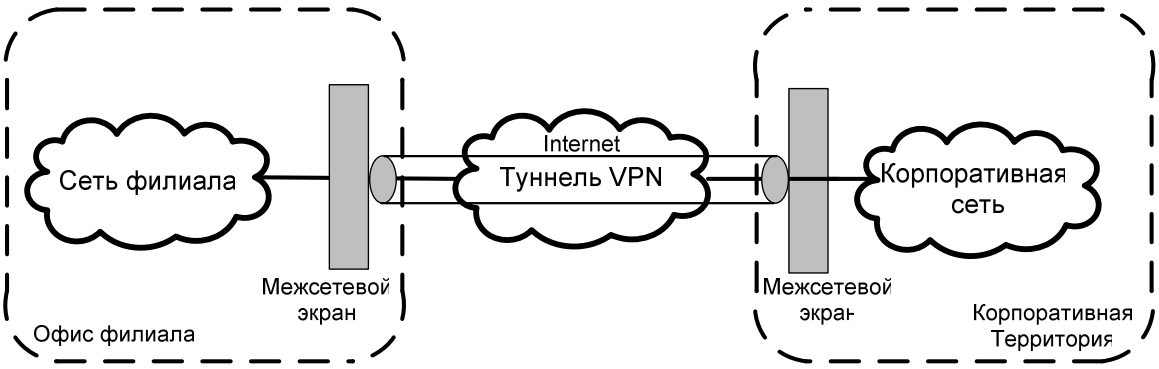


**Рис. 2.18. Схема организации туннеля VPN между двумя МСЭ**

Сети VPN были созданы для обеспечения конфиденциальности между двумя кронами, причём обычно доверительных отношений между ними нет. Комбинация МСЭ и VPN, с одной стороны, устанавливает доверительные отношения между двумя областями, с другой – обеспечивает конфиденциальность передачи данных. Такой подход в плане защиты значительно эффективнее схем, в которых предусмотрено наличие только МСЭ в обеих областях либо только VPN между ними. Туннель VPN между двумя межсетевыми экранами показан на рис. 2.18.

Раньше брандмауэры обеспечивали только функции барьеров безопасности. Однако в настоящее время их возможности дополнены функциями VPN. Совмещение функций межсетевых экранов и VPN увеличивает эффективность контроля безопасности.

# Глава 3. ПРИЛОЖЕНИЯ ДЛЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

В соответствии с приведённым во второй главе и [4] определением виртуальная частная сеть представляет собой безопасную сеть связи, встроенную в незащищённую сеть общего пользования. Под незащищённой обычно подразумевается сеть Internet. В предыдущей главе представлен только один из трёх типов сетей VPN-VPN доступа. Ниже рассматриваются сети intranet, VPN и extranet VPN, обсуждаются вопросы применения VPN для организаций и поддержки IP-телефонии – системы передачи речи с использованием IP.

## 3.1. СЕТИ INTRANET

Благодаря Internet между компьютерами может вестись обмен данными независимо от операционной системы, управляющей их работой. Технологии, применённые в Internet, способствовали продвижению на рынке самой системы, поскольку появилась возможность доступа к приложениям с помощью любой платформы. Использование гиперссылок упростило перемещение и поиск необходимой информации. Поскольку сеть Internet считается незащищённой структурой, бизнесмены в отличие от учёных не сразу начали применять её в работе. Однако дальнейшие разработки и внедрение VPN изменили подобное отношение. В настоящее время защищённость сети Internet оценивается как достаточная для передачи важной информации [4].

Компании пришли к выводу, что технологии Internet и Web обеспечивают высокий уровень взаимодействия и мощные средства доступа к информации. Использование этих технологий позволяет развивать корпоративные внутренние сети – *intranet*. Они представляют собой систему внутреннего взаимодействия, основанную на технологии Internet, включая службы Web, TCP/IP, HTTP, язык создания гипертекста (HyperText Markup Language – HTML). Таким образом, работники компании могут обратиться к intranet для поиска необходимой информации либо отправления электронных сообщений. Intranet – это база накопленных в корпорации знаний, собранный положительный опыт работы организации. Информация, доступная специалистам непосредственно с их рабочих мест, помогает лучше понять цели корпорации, производственные процессы, отношения и способы взаимодействия, принятые в компании.

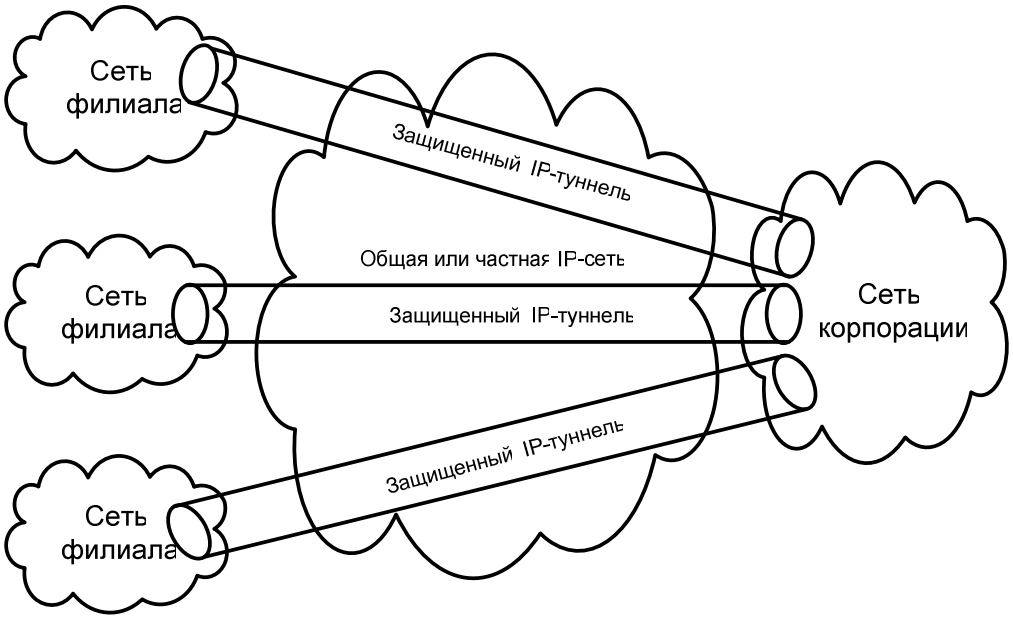


**Рис. 3.1. Схема организации intranet с тремя сетями филиалов**

Как правило, в большинстве организаций служащие привыкли полагаться на указания руководителя о необходимости получения той или иной информации. Посредством сетей intranet эту модель отношений можно изменить. Специалист сам решает, какая информация ему необходима.

Intranet можно организовать в частных IP-сетях, объединяющих филиалы компаний в единую защищённую сеть. Её можно создать и при участии провайдера, используя Internet и intranet VPN. На рис. 3.1 показана сеть intranet и три сети филиалов, которые присоединяются к корпоративной структуре с использованием защищённых IP-туннелей на основе сетей intranet VPN.

**Структура intranet.** Сети intranet построены с использованием того же инструментария, что Internet и Web-приложения. Первый шаг в разработке сети intranet состоит в создании внутреннего Web-сайта. Но прежде чем компании приступят к созданию своих ресурсов, им необходимо решить ряд вопросов. Какая операционная система будет использована в качестве платформы для Web-сервера? Какую базу данных применить? Каким образом осуществлять контроль доступа и какой тип браузера использовать? Какой инструментарий HTML потребуется для разработки приложений?

Информацию на Web-сайте необходимо обновлять как можно чаще, с тем чтобы поддерживать у пользователя интерес к ресурсу компании. Кроме того, желательно, чтобы сайт был прост в эксплуатации; он должен включать авторскую систему, которая поможет пользователю оформить свои материалы и отправить их на сайт.

**Использование intranet.** Intranet – это вспомогательный инструмент, позволяющий распространять информацию, которая принадлежит данной корпорации, в диалоговом режиме. Компания может разместить в intranet значительную часть документов, чтобы служащие могли ознакомиться с приказами, просмотреть записи заказчиков, вместе обсудить реализацию новых проектов. С помощью intranet проще определить сферу корпоративных интересов, выработать общий взгляд на предмет и основные принципы стельности компании, сделав эту информацию доступной для всех. Следовательно, сеть intranet создаёт благоприятные условия для работы в команде.

***Корпоративные новости и финансовая информация.*** В сети intranet можно размещать важнейшие корпоративные документы, включая квартальные и годовые отчёты, решения собраний акционеров, план работ, сообщения президента компании. Более того, сеть можно использовать для внесения сведений об организационных изменениях, достижениях компании, для освещения важных событий и новостей дня или недели.

***Информация о рынках сбыта и продажах.*** В сети intranet можно разместить информацию компетентных аналитиков о продажах, последних достижениях заказчиков, сведения о презентации товаров и ведущих производителях. Компании, обеспечивающие ограниченный доступ к такой информации, могут создавать себе рекламу, предоставляя потенциальным заказчикам конфиденциальную информацию.

***Информация о производстве.*** Производители товаров используют сеть intranet для размещения документов ISO 9000 и планов выпуска новой продукции.

***Информация о кадрах.*** Отдел кадров может использовать intranet для размещения информации о доходах компании, политике управления, рабочих местах и ассортименте товаров. Internet позволяет компаниям рассылать бланки документов, заполняемых потенциальными сотрудниками в интерактивном режиме. Следовательно, специалисты, включая удалённых пользователей, могут, получив эти документы, вывести их на печать.

Некоторые корпоративные сети требуют от пользователей, чтобы бланки документов заполнялись вручную, в других это осуществляется в электронном режиме. Возможность формировать требуемые документы электронным способом позволяет отделу кадров эффективнее работать с этими документами.

Например, служащие предпенсионного возраста могут определить своё жалованье, воспользовавшись информацией intranet. Для соблюдения конфиденциальности сведений, поступающих на бланках от потенциальных специалистов, допустимо контролировать доступ к данной информации путём ввода специалистами пароля либо других форм электронных идентификаторов, прежде чем их записи будут обработаны.

***Информация учебных центров.*** Большинство компаний имеет собственные образовательные центры, в которых проводится обучение специалистов. В intranet можно поместить информацию о курсах, организованных учебным центром, и режиме их работы. Запись на них проводится в диалоговом режиме.

***Организация обсуждений с использованием Intranet*** предоставляет специалистам возможность обращаться к электронным доскам объявлений, что помогает формировать группы для обсуждения проектов. На доске объявлений можно оставить собственные сообщения и познакомиться с мнением коллег относительно проводимой работы.

***Разработка проекта.*** Члены группы по разработке совместного проекта могут использовать intranet для обмена актуальной информацией. В данном приложении обычно требуется контролировать доступ ко всем нужным сведениям, чтобы получить их могли только члены группы, работающие над проектом.

## 3.2. СЕТИ EXTRANET

Подобно intranet, сеть extranet основана на технологиях Internet. Однако в отличие от intranet она является совместной сетью, объединяющей организации специалистов, поставщиков, заказчиков и стратегических партнёров. Сеть extranet – это мост между общей сетью Internet, работать в которой может любой человек, и корпоративной сетью intranet, доступной только для представителей конкретной организации. Предпосылкой для организации extranet является наличие корпоративной intranet.

В данном разделе представлена основная информация о сетях extranet, их преимуществах, структуре и использовании.

**Преимущества extranet.** Extranet позволяет деловым партнёрам взаимодействовать более эффективно, поскольку каждый из них получает быстрый доступ к важной информации. Например, коммивояжер может незамедлительно получить данные о товаре через extranet, не прибегая при этом к услугам агента по продажам.

Компании размещают свою информацию в extranet, с тем чтобы донести её до ведения поставщиков, агентов по продажам, стратегических партнёров; при этом отпадает необходимость в том, чтобы создавать и печатать документы на бумаге. Такой подход приводит к значительной экономии времени. Поскольку подобная информация часто обновляется и периодически вновь рассылается всем заинтересованным пользователям, то и экономия финансовых средств за счёт использования extranet может оказаться значительной. Помимо снижения стоимости доставки сообщений, сокращения времени доступа к необходимым данным extranet предоставляет пользователю наиболее актуальную информацию.

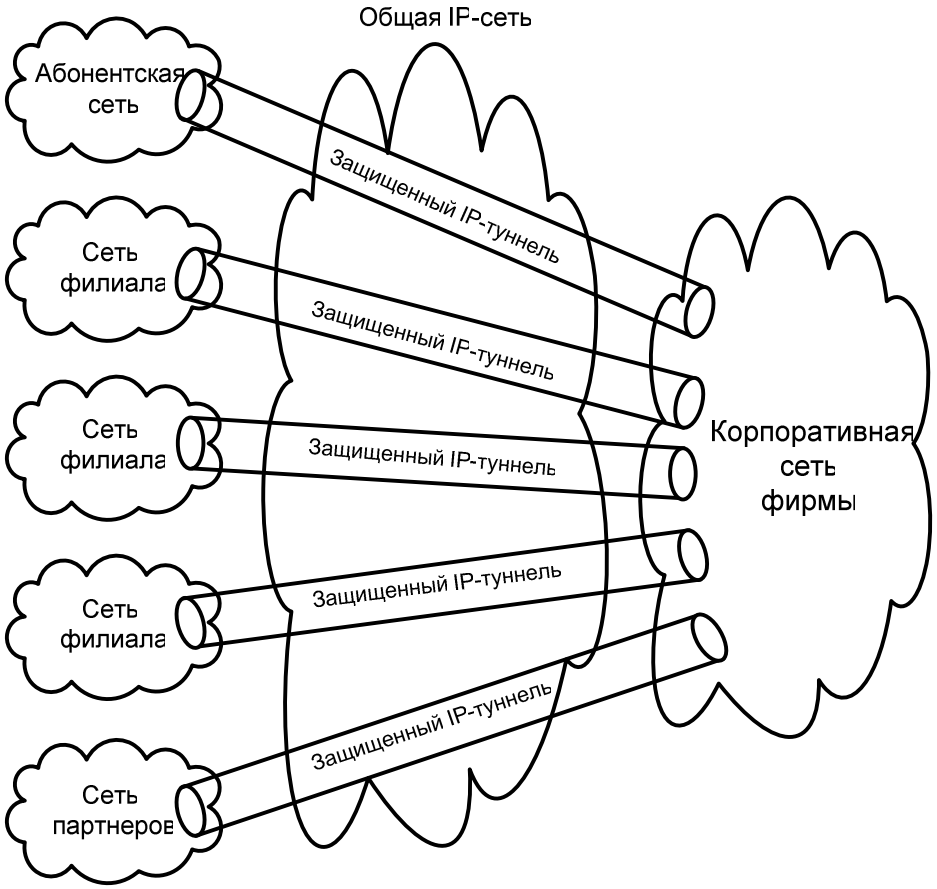


**Рис. 3.2. Сеть extranet**

Сеть extranet (рис. 3.2) соединяет корпоративную сеть с тремя филиалами, сетью потребителей товаров и стратегических партнёров через extranet VPN, которые на рисунке представлены как защищённые IP-туннели.

**Структура extranet.** Основными компонентами extranet являются [4] Web, Internet и система межсетевых экранов. Web делает extranet независимой от платформы. Это основное преимущество по сравнению с традиционными системами клиент–сервер, в которых требуется, чтобы все рабочие станции использовали единое программное обеспечение, а значит, и одинаковую операционную систему. Межсетевой экран усиливает контроль за доступом в частную корпоративную сеть intranet. Конфигурирование extranet можно сравнить с просверливанием отверстия в межсетевом экране для обеспечения доступа в сеть избранной группе внешних пользователей.

Сеть extranet разработана для специализированных бизнес-приложений, таких intranet как деловая переписка, сотрудничество в рабочих группах, подача и заполнение документов в интерактивном режиме, обработка запросов к базам данных. Несмотря на то, что сеть создавалась для выполнения определённых задач, она должна быть достаточно гибкой, чтобы к ней можно было легко подключить новых пользователей и организации.

Главной особенностью сети extranet является её защищённость. Безопасность extranet подразумевает защиту информации, передаваемой в интерактивном режиме, и баз данных. Разработанная стратегия защиты, рассмотренная выше применительно к МСЭ, распространяется и на extranet. Хорошая организация сети предусматривает наличие тщательно разработанного плана и концепции защиты. При разработке в группах проектов с использованием extranet необходимо уделить особое внимание вопросам аутентификации перед предоставлением доступа в сеть. Следует тщательно продумать привилегии групп и способы их реализации. Обе операции: аутентификация и проверка полномочий, или авторизация, – особенно важны в технологии extranet. Авторизация гарантирует, что пользователь получит доступ к ресурсам в соответствии с принятой сетевой политикой. Поскольку extranet объединяет несколько пользовательских сетей и intranet, сеть лучше строить с применением не частных, а стандартных протоколов. В виртуальной частной сети extranet лучше использовать L2TP либо IPSec.

В настоящее время сети extranet стремительно развиваются. Поскольку существующие устройства плохо справляются с задачей доступа к сетям extranet, на рынке появился новый класс устройств доступа – *коммутаторы доступа extranet.* Данные устройства выполняют функции обеспечения защиты VPN, характеризуются более высокой производительностью и удовлетворяют возросшим требованиям к возможностям управления.

Другая проблема, требующая решения при разработке extranet, – это простота эксплуатации. Пользователь должен иметь доступ в сеть через любой Web-браузер. Данный процесс не должен быть сложнее доступа в Internet, хотя в этом случае могут потребоваться дополнительные шаги для аутентификации пользователя.

**Приложения, использующие сети extranet.** В extranet можно работать с приложениями для деловых совместных операций. Эти приложения считаются альтернативной средой для проведения электронных коммерческих операций между корпорациями либо между продавцами и покупателями. Компании, использующие электронную сеть для реализации товаров и услуг, сокращают затраты на поиск потребителей.

Extranet может применяться компаниями-производителями с целью снижения расходов на услуги связи, на проведение инвентаризаций. Через сеть extranet можно уведомлять поставщиков о времени доставки наиболее важных составляющих заказа.

Сеть extranet используют для оповещения покупателей и партнёров по бизнесу об особенностях произведённого товара ещё до его появления на рынке. Своевременное получение откликов от потенциальных клиентов поможет скорректировать действия по реализации товара.

**Обеспечение безопасности extranet.** В процессе эксплуатации extranet необходимо обеспечить безопасность и контроль доступа. Деловые партнёры с сомнительной этикой ведения коммерческих операций представляют определённый риск для безопасности сети. Для предотвращения утечки информации через систему защиты большинством компаний используется комбинация из межсетевых экранов, когда, например, один устанавливают на уровне обмена пакетами сообщений, другой – на уровне приложений.

МСЭ на уровне приложений могут применяться для обеспечения контроля доступа, что позволяет пользователям обращаться только к разрешённым устройствам.

## 3.3. IP-ТЕЛЕФОНИЯ

К *IP-телефонии* относится любое приложение, связанное с телефонией и использующее в качестве среды передачи ЛВС, intranet, extranet и Internet. Сигнал для передачи бывает речевым либо факсимильным. Интерес к данной технологии связан с тем, что компания может значительно сократить расходы на передачу различных видов информации (речевой, видеосигналов, данных), если передает их через Internet. Передача речевого сигнала посредством *протокола Internet* (Voice Over IP – VoIP) особенно эффективна для компаний, у которых значительный объём переговоров связан с использованием протяженных междугородных и международных линий связи. Такие организации могут избежать значительных расходов на телефонные переговоры между филиалами, оплатив доступ в Internet, что предоставляет право на неограниченное количество обращений в сеть. Этот вид доступа позволяет передавать цифровой речевой сигнал по каналам Internet, и компании могут осуществлять связь со всем миром без оплаты телефонных счётов за использование каналов сети общего пользования.

**Структура VoIP.** Главный компонент структуры VoIP – это *шлюз VoIP.* Предположим, что VoIP необходимо использовать для соединения корпоративной и удалённой сетей филиала офиса. Для этого применяются два шлюза VoIp, причём один из них подключается к корпоративной ЛВС, а второй – к локальной сети филиала. Каждый шлюз с помощью интерфейса T1 подключается к соответствующей АТС офиса, которая соединена с аналоговыми телефонными линиями. АТС офиса подключается к телефонной сети общего пользования, а шлюз получает доступ в сеть Internet либо к корпоративной intranet через маршрутизатор. В отдельных случаях телефоны подключаются непосредственно к шлюзам VoIP, что позволяет использовать их в качестве АТС офиса. Некоторые типы шлюзов VoIP обеспечивают и функции маршрутизации. Они могут быть подключены непосредственно к Internet без направления пакетов сообщений на маршрутизатор.

Шлюзы VoIP обеспечивают исполнение следующих основных функций:

– *преобразование адреса.* Когда шлюз источника получает номер пункта назначения, он преобразует его в IP-адрес шлюза пункта назначения;

– *установка исходящего соединения.* Шлюз источника отвечает за установку соединения со шлюзом пункта назначения, за обмен сигналами вызова, служебными данными, дополнительной информацией, связанной, в частности, с режимом обеспечения безопасной работы;

– *цифровое преобразование.* Одним из требований, предъявляемых к шлюзу, является цифровое преобразование аналоговых сигналов. Эти сигналы поступают от телефонов, которые не подключены к АТС офиса либо к другому конечному оборудованию, обеспечивающему функции преобразования сигнала в 64 кбит/с PCM-сигнал (Pulse Code Modulation – импульсно-кодовая модуляция). Эта функция опускается, если имеется АТС офиса;

– *сжатие динамического диапазона сигнала.* Закодированный с помощью PCM речевой сигнал преобразуется шлюзом источника с использованием соответствующей схемы компрессии для передачи со скоростью менее 8 кбит/с;

– *преобразование сигнала для пакетной передачи речи.* Сжатый речевой сигнал преобразуется в пакеты сообщений для передачи в ЛВС. Затем эти пакеты обрабатываются маршрутизатором и отправляются дальше в Internet;

– *восстановление динамического диапазона.* Шлюз пункта назначения восстанавливает принятые речевые IP-пакеты в исходную форму 64 кбит/с сигнала PCM, прежде чем направить их к АТС офиса.

Заметим, что существуют различные шлюзы для обработки речевых и факсимильных потоков. Некоторые устройства работают только с факсимильными сообщениями, другие – только с речевой информацией; имеются устройства, обслуживающие оба вида потока.

Возможности предыдущей модели для пользователей корпоративной сети неограничены. Провайдер может предложить услугу VoIP, установив телефонный шлюз, доступ к которому возможен для любого абонента телефонного аппарата. Имея это в виду, можно предложить несколько конфигураций передачи речевых сообщений через Internet: с одного телефона на другой, с телефона на ПК, с ПК на телефон, с ПК на ПК. Введём определение ПК-вызова и телефонного вызова. *ПК-вызов* представляет собой вызов, который осуществляется с компьютера, находящегося в корпоративной сети и оборудованного звуковой картой. На рис. 3.3 такие компьютеры помечены буквами A, B. Телефонный вызов осу-

ществляется пользователями, подключёнными непосредственно к АТС офиса, на рисунке они отмечены как C, D.

В следующих пяти примерах используется схема сети, показанная на рис. 3.3.

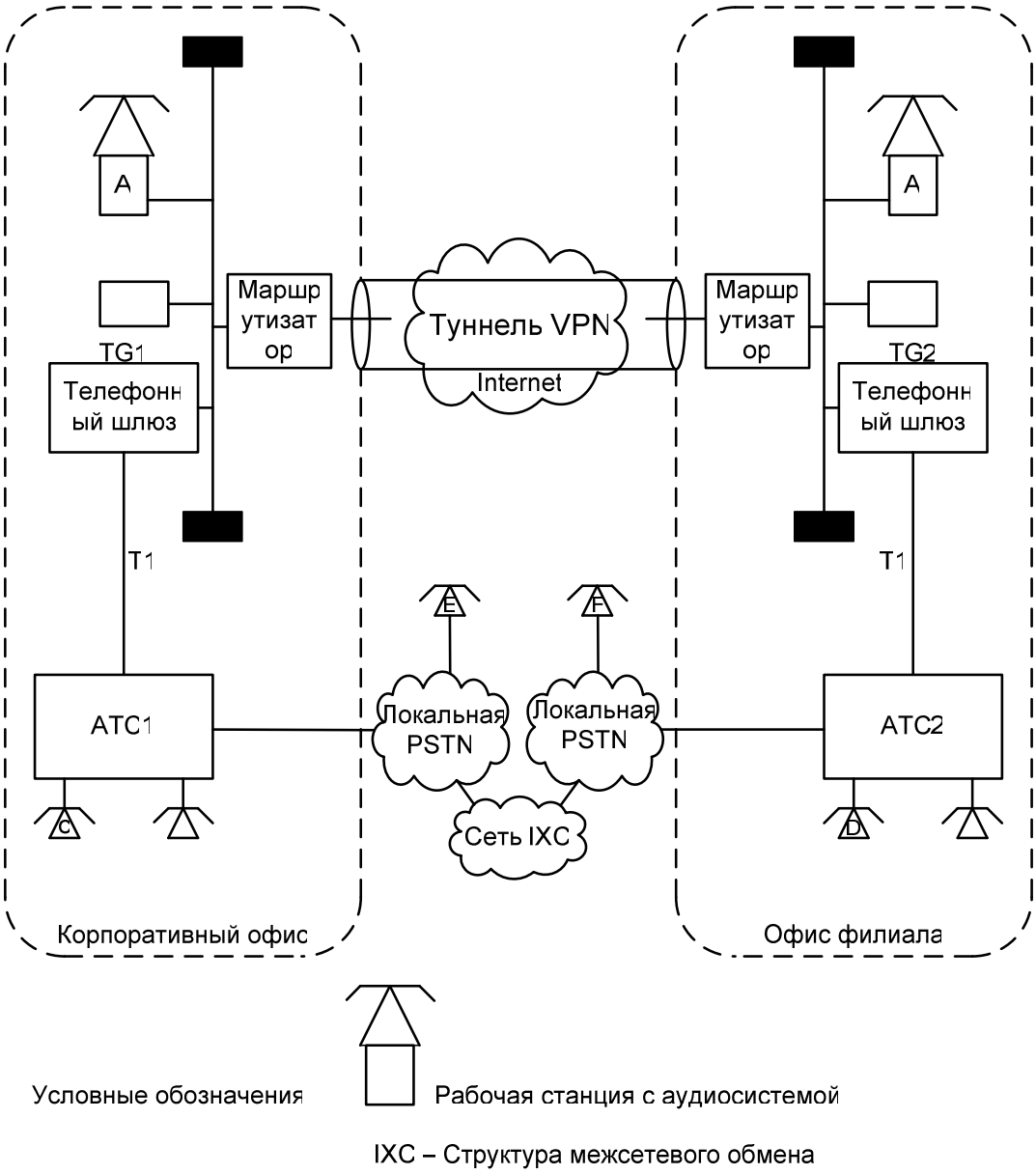


**Рис. 3.3. Схема построения системы передачи голоса через Internet**

***Вызов с одного телефона на другой.*** Рассмотрим вызов, поступивший с аппарата абонента C, который подключён к корпоративной АТС, на номер абонента B, соединённого с АТС филиала офиса. Во время набора абонентом C номера D анализируется поступающая последовательность цифр и выясняется, что вызов дальний и должен обрабатываться шлюзом TG1.

АТС направляет цифровую последовательность вызова к шлюзу VoIP, где по каталогу определяется местоположение абонента D и его шлюза VoIP TG2. Затем TG1 устанавливает Internet-соединение со шлюзом TG2, откуда вызов перенаправляется к размещённой в филиале офиса АТС2, соединённой с абонентом D. Если этот вызов местный и предназначается для абонента E, АТС источника направит вызов по обычной телефонной линии. АТС перешлёт дальний вызов пользователя F шлюзу TG1, который отвечает за определение местоположения телефонного шлюза абонента F и перенаправляет данному устройству поступивший вызов.

***Вызов с телефона на компьютер.*** Рассмотрим вызов от абонента C, подключённого к корпоративной АТС. Вызов направлен абоненту B, который использует компьютер с соответствующим оборудова-

нием, соединённый с ЛВС филиала. Вызов проходит от АТС к TG1, последний передаёт его на TG2, используя для этой цели Internet. Шлюз TG2 отвечает за пересылку приходящих речевых пакетов пользователю B.

***Вызов с компьютера на телефон.*** При вызове абонентом A, подключённым к корпоративной ЛВС, абонента D, который связан с АТС филиала, вызов принимает TG1 и транслирует его TG2. Последний направляет вызов к АТС филиала, соединяющей его с абонентом D.

***Вызов с компьютера на компьютер.*** Если источником вызова является абонент A, находящийся в корпоративной ЛВС, а получателем – абонент B, чей компьютер подключён к ЛВС филиала, то вызов принимает TG1, а затем устанавливается Internet-соединение с TG2. Последний отправляет пакеты с указанием адреса получателя (абонента B) в режиме широковещания в ЛВС филиала.

***Вызовы внутрисетевые и межсетевые.*** Метод VoIP можно применить к вызовам внутри сети и между сетями. *Вызов внутри сети* – это соединения между двумя участками одной корпоративной сети. Пример такого вызова от пользователя A абоненту D приведён на рис. 3.3, где оба пользователя находятся в корпоративной сети. При *межсетевом вызове* одна из участвующих сторон находится внутри корпоративной сети, другая – в удалённой области. Примером такого вызова может служить обращение, инициированное абонентом A к пользователю F, который находится вне границ корпоративной сети, поддерживающей передачу речевых сообщений, т.е. в межсетевой области. Данный вызов реализуется в два этапа. На первом пользователь A отправляет Internet-вызов шлюзу TG2. На втором этапе шлюз отправляет АТС2 команду осуществить вызов к абоненту F, подключённому к местной телефонной сети общего пользования. Для вызовов из межсетевой области необходимо наличие АТС в корпоративной сети, которая осуществляет вызов интересующего абонента через местную телефонную сеть.

**Проблемы в Internet-телефонии.** Структура Internet представляет собой объединение более 100 тыс. сетей и является сетью коммутации пакетов. Поэтому аналоговый речевой сигнал, предназначенный для передачи по телефонным линиям связи, должен быть преобразован прежде, чем начнёт транслироваться по компьютерной сети. На первой ступени речевой сигнал преобразуется в цифровой; затем преобразованные данные сжимаются для уменьшения скорости передачи со стандартной для телефонии величины 64 кбит/с до 8 кбит/с либо ещё меньше. На данном этапе необходимо убедиться, что потеря качества речевого сигнала минимальна. Затем сжатые данные преобразуются в пакеты и направляются в сеть.

***Качество передачи речи.*** Одной из проблем, связанных с технологией VoIP, является качество предоставляемой услуги. Пользователь ожидает получить определенное качество передачи речи, основываясь на личном опыте общения по телефону через сеть PSTN. К сожалению, качество передачи речевых сигналов с использованием Internet пока ниже уровня, достигнутого PSTN (Public Switched Telephone Network – телефонная сеть общего пользования), которая обеспечивает гарантированную скорость передачи сигнала 64 кбит/с. Так как Internet – это сеть передачи пакетов, то отдельные пакеты во время передачи речевой информации могут проходить по различным маршрутам, соединяющим два пункта. Хотя это позволяет более эффективно использовать сетевые ресурсы по сравнению с обычной телефонной сетью, данное преимущество имеет и оборотную сторону. Пакеты в процессе маршрутизации от одного пункта к другому испытывают различную задержку времени. Кроме того, сохраняется вероятность их потери.

При передаче голоса в режиме реального времени величина задержки сигнала между конечными пунктами служит важным критерием оценки системы. Более того, необходимо, чтобы эта величина находилась в определённых границах.

Изменения задержки называются *рассинхронизацией пакета.* Поскольку Internet испытывает большие нагрузки, пакеты при перегрузке сети могут отбрасываться. Во многих системах пакетной передачи речевого сигнала с этими проблемами борются, используя *фиктивные пакеты* вместо задержанных или утерянных при воспроизведении речевой информации. Для создания фиктивных пакетов применяются многочисленные алгоритмы. Например, можно предложить повторную передачу предыдущего пакета, если следующий не поступил вовремя. Когда требуемый пакет наконец доставлен, он отбрасывается, поскольку его место уже занято фиктивным. Конечно, полученное качество уступает тому, что достигнуто при использовании каналов сети PSTN.

Большинство компаний проблему потерянных и задержанных пакетов решают ограничением сервиса VoIP пределами своих сетей intranet. В этих сетях гарантированное качество услуги достигается в

результате заключения соглашения с провайдером. Сеть intranet, граница которой не выходит за опорную IP-сеть провайдера, более надёжна в эксплуатации по сравнению с intranet, пересекающей Internet. Если провайдер гарантирует неизменность таких параметров, как величина задержки и отсутствие рассинхронизации пакетов, то качество услуги может приближаться к уровню, предоставляемому PSTN.

***Стандарты и функциональная совместимость.*** Другая проблема технологии VoIP связана с функциональной совместимостью оборудования. Так, компании, установившей шлюзы VoIP, приходится закупать комплектующие у того же производителя, поскольку аппаратное обеспечение двух разных поставщиков часто оказывается несовместимым.

Для того, чтобы телефонный шлюз смог преобразовать речевой IP-пакет, отправленный ПК, в сигнал для передачи по телефонной линии и осуществить обратное преобразование, необходимо, чтобы оба устройства были снабжены кодером/декодером, иначе говоря, кодеком одного производителя. В некоторых стандартах предпринята попытка разрешить проблему совместимости устройств. Это ITU-T H.323, протокол резервирования ресурсов (Resource reservation Protocol – RSVP), и протокол быстрого доступа к директории (LDAP).

***Рекомендации H.323 сектора стандартизации ITU.*** Документ H.323 представляет собой ряд рекомендаций, охватывающих различные аудио- и видеостандарты кодирования данных. В нём определён метод установки соединений с использованием сети Internet. Эти рекомендации основаны на использовании протокола передачи данных в режиме реального времени и протокола управления передачей данных в режиме реального времени – для контроля за передачей звуковых и видеосигналов. Иногда документ H.323 называют *всеохватывающей рекомендацией,* поскольку он ссылается на другие документы. Они включают в себя следующие стандарты: ITU-T G.711, ITU-T G.722, ITU-T G.723, ITU-T G.723.1, ITU-T G.728 и ITU-T G.729 – для речевых кодеков; ITU-T H.225.0 – для формирования пакетов и контроля вызова; ITU-T H.245 – для открытия и закрытия каналов передачи аудиовизуальной информации и возможности обмена данными между терминалами; ITU-T H.261 и ITU-T H.263 – для видеокодеков; ITU-T T.120 – для мультимедийной связи (контроль передачи данных и управление видеоконференциями). Предполагается, что терминалы, использующие в работе H.323, поддерживают стандарт ITU-T Q.931 для установки вызова, который является стандартом обмена системной информацией – сигнализацией.

В марте 1997 г. на форуме VoIP рекомендовали заменить стандарт G.729 на G.723.1, поскольку последний повышает эффективность использования полосы частот. Кодеки, построенные с использованием стандарта G.723.1, сжимают полосу пропускания речевого сигнала с 64 до 6,3 кбит/с, в то время как предыдущий стандарт допускал сжатие только до 8 кбит/с. Скорость передачи, соответствующая 8 кбит/с, обеспечивает более высокое качество сигнала, чем величина 6,3 кбит/с, но на форуме VoIP было решено пожертвовать качеством сигнала в обмен на повышение эффективности полосы пропускания.

Контроль качества обеспечивается исполнением трёх служебных функций контроля – регистрации, линии связи, состояния (Registration, Admission, Status – RAS) стандарта H.245, которые в рекомендации ITU-T Q.931 называются сигнализацией. Стандарт H.245 связан с установлением надёжного канала, необходимого для передачи управляющих сообщений стандарта H.323. Эти сообщения включают возможность обмена данными, передачу информации об управлении потоком, команды открытия и закрытия логических каналов. Сервер Q.931 используется для формирования соединения между терминалами H.323. RAS обеспечивает регистрацию, контроль над каналом, передачу адресов, контроль за полосой частот. Схема на рис. 3.4 представляет собой модификацию схемы, показанной на рис. 3.3, и иллюстрирует формирование соединения для передачи служебной информации.

Сигнализация осуществляется следующим образом. Когда абонент поднимает телефонную трубку, инициирующая вызов АТС офиса поддерживает тоновый набор так же, как и при обычном телефонном вызове. После приёма набранных цифр АТС пересылает номер шлюзу VoIP.

Если обнаружен местный вызов, на АТС офиса следует команда о его передаче по локальной сети – либо внутри с использованием самой АТС, либо через местную телефонную сеть общего пользования. Если АТС офиса имеет программное обеспечение, то решение относительно обработки поступившего вызова принимается автоматически. Для дальних вызовов VoIP инициирует соединение TCP через порт 1720, который отводится под H.323 через маршрутизатор исходящего вызова к шлюзу VoIP пункта назначения. Затем, используя полученную линию связи, шлюз источника отправляет пакеты Q.931.

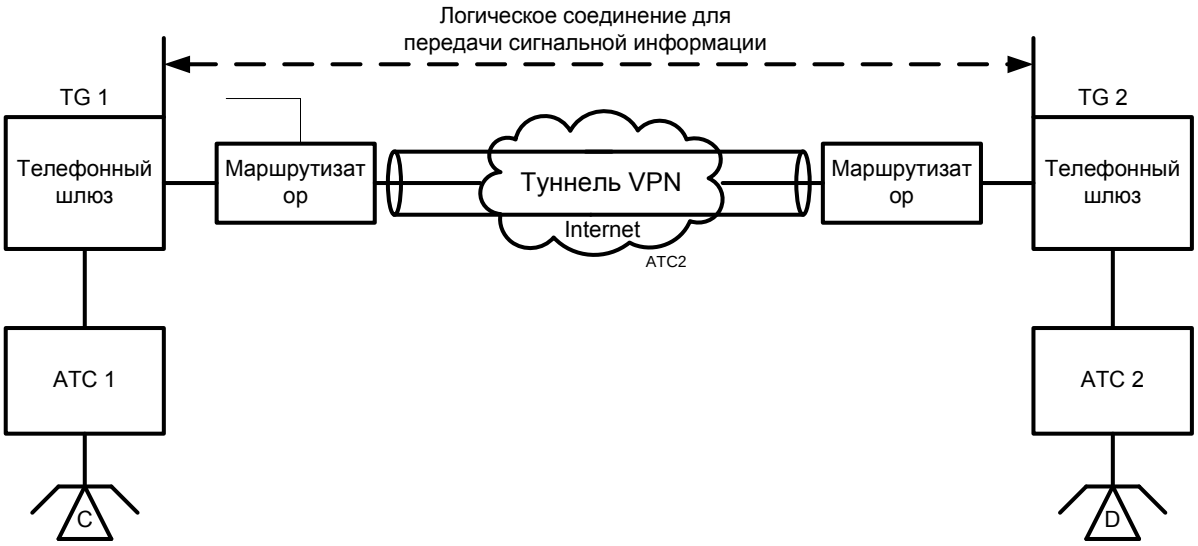


**Рис. 3.4. Схема логического соединения двух телефонных шлюзов для передачи служебной информации**

После обмена пакетами Q.931 осуществляется соединение H.245 через порт TCP с адресом большим, чем 1024. Номер этого порта обычно устанавливается в процессе обмена пакетами Q.931. С этого момента предыдущее соединение TCP может быть закрыто. Параметры вызова – тип используемого кодека, адреса RTP и RTCP – согласовываются при обмене сообщениями H.245. После выбора параметров H.245 выполняет последовательность открытия логического канала, используемую для формирования соединений UDP.

В рекомендации H.323 отмечается, что логический канал должен быть двунаправленным. Таким образом, для организации связи необходимо установить две логических линии связи: одну – от источника к получателю, другую – в обратном направлении. После рассылки сообщений с указанием адресов и портов для RTP и RTCP источник может начать активную передачу речевых пакетов, которые транслируются в форме RTP с использованием протокола UDP. Процедура управления вызовом VoIP показана на рис. 3.5.

Пакеты для передачи речевых сигналов формируются как пакеты UDP/IP, а не как сообщения TCP/IP. Это объясняется тем, что протокол TCP/IP осуществляет коррекцию ошибок методом повторной передачи пакета. Ретрансляция пакета приводит к значительной задержке, что не улучшает качество речевого сигнала. Протокол UDP не осуществляет ретрансляцию пакетов. Кроме того, он может использоваться в комбинации с изложенной выше схемой передачи пакетов, в которой производится замена потерянных либо повреждённых пакетов на фиктивные. Повторное воспроизведение незаметно, если число фиктивных пакетов не превышает 5 % от общего числа переданных пакетов.

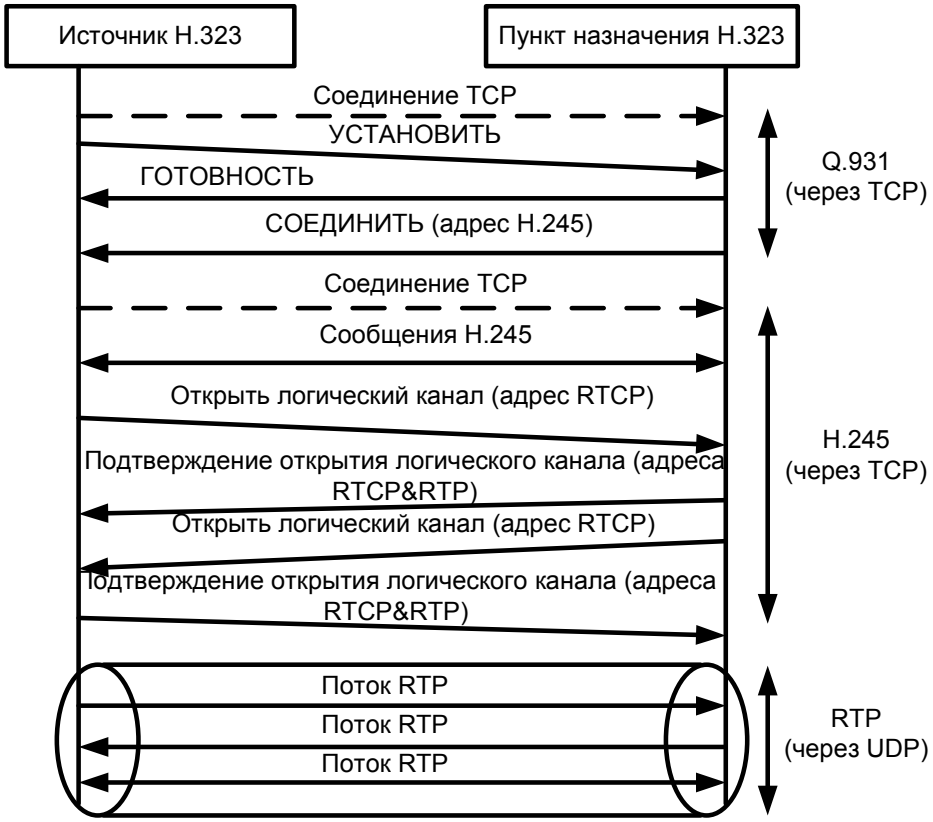


**Рис. 3.5. Схема организации контроля вызова в системе VoIP**

**VoIP и частные виртуальные сети.** Ранее предполагалось, что пакеты VoIP передаются как регулярные IP-пакеты. Небольшое число проходящих через Internet пакетов, вероятнее всего, будет иметь существенную величину задержки по сравнению с временем распространения регулярных IP-пакетов. Это приводит к снижению качества передаваемой речи. Однако VPN intranet может улучшить качество передачи речевого сигнала. Сначала между маршрутизаторами формируется сеть VPN, затем проходит обмен сигналами в рассмотренном выше режиме.

***Протокол резервирования ресурсов.*** В маршрутизируемых IP-сетях каждый сетевой маршрутизатор, получивший для обработки пакет, должен определить следующий пункт назначения для данного сообщения. Хотя эта схема хорошо подходит для приложений, передающих пакеты, разбитые на части, она малопригодна для потока пакетов, поступающих непрерывно, а именно это свойство отличает передачу речевых сигналов. Для улучшения качества услуги при использовании систем с коммутацией пакетов группа IETF разработала специальный *протокол резервирования ресурсов*.

Протокол RSVP резервирует полосу пропускания для обеспечения заданного уровня обслуживания при передаче мультимедийных сообщений. Его обычно называют протоколом, инициированным получателем. Это означает, что запрос о резервировании ресурсов поступает от получателя. В телефонии отправитель сообщения запрашивает резервирование ресурсов, пользуясь системой передачи служебной информации. В сетях с групповым обращением, для поддержки которых предназначался RSVP, протоколы, инициированные приёмником, лучше регулируют поток, чем активизированные передатчиком сообщений. RSVP обладает определёнными характеристиками, представленными ниже.

*Мягкий режим* позволяет в течение некоторого времени сохранять данные, а не уничтожать их по умолчанию. Для поддержания этого режима периодически генерируется сообщение об обновлении, которое автоматически продлевает время сохранения информации. Данные удаляются, если очередное сообщение об обновлении данных не поступило.

При групповом режиме могут резервироваться различные ресурсы. Это означает, что получатели сообщений в групповом режиме обращения могут запросить разные уровни качества обслуживания (QoS).

Данный протокол позволяет динамически изменять QoS. Ресурсы, запрошенные получателем, могут быть изменены уже после резервирования.

Для обслуживания различных приложений предлагается несколько типов резервирования.

Элементами протокола RSVP являются отправители, получатели и расположенные между ними маршрутизаторы. В этом протоколе формируется два основных типа сообщений: *путь* (PATH), *резервирование* (RESV). Отправитель сообщения высылает PATH в обратном направлении к одному (или более) получателю, информируя о том, какого типа сведения будут переданы источником. Эта информация включает такие параметры потока, как средняя скорость передачи, требуемый уровень QoS.

Получатель высылает сообщение отправителю RESV. Ресурсы не резервируются до тех пор, пока получатель, используя информацию, содержащуюся в сообщении PATH, не вышлет сообщение RESV в прямом направлении (обычно обратном тому пути, каким пришло сообщение PATH), где укажет, какие конкретные ресурсы необходимо зарезервировать. К одному отправителю с сообщением RESV могут обратиться несколько получателей, причём количество запрошенных ресурсов бывает различным. Это стандартная ситуация при групповом режиме обращения. Узел, принимающий такие запросы, объединяет их и генерирует одно обращение RESV, которое затем отправляется источнику. В новом обращении RESV содержится максимальный из всех запрошенных ресурсов, пришедших на предыдущем этапе.

Запрос RESV состоит из *дескриптора потока*, который образован спецификатором потока и спецификатором фильтра. Первый определяет необходимый уровень QoS, в то время как спецификатор фильтра используется для выбора числа пакетов, участвующих в данной сессии. В RSVP поток – это набор пакетов данных, который принимается с QoS, определяемым спецификатором потока, а под сессией понимается поток данных с конкретным пунктом назначения и протоколом транспортного уровня. Каждый узел, который участвует в исполнении протокола RSVP, осуществляет *контроль доступа* и *контроль стратегии.* Первый тип определяет достаточность имеющихся ресурсов для обеспечения запрошенного QoS. Второй тип выясняет, имеет ли пользователь право для резервирования ресурсов. Когда промежуточный узел принимает запрос RSVP, он должен выполнить две функции, а именно:

– *сформировать резерв.* Спецификаторы потока и фильтра используются обоими типами контроля для принятия решения об исполнении запроса или отказе в его исполнении. При отказе получателю, осуществившему запрос, высылается сообщение об ошибке. Если запрос принят к исполнению, то узлом формируется классификатор пакета для отбора соответствующих входящих пакетов. Таким же образом формируется план передачи пакетов, с тем чтобы их передача исполнялась в режиме, обеспечивающем требуемый уровень QoS;

– *передать запрос в прямом направлении.* Сообщение, содержащее запрос, отсылается в прямом направлении к источнику.

Базовой моделью резервирования считается однопереходная. Это означает, что получатель посылает сообщение RSVP в прямом направлении, а промежуточные узлы либо готовы исполнить его, либо нет. Получатель не может отвечать за всю передачу пакетов от пункта отправления до пункта получения сообщения. Более совершенной является *однопереходная модель с уведомлением* (One Path With Advertising – OPWA), в которой контрольные пакеты отправляются в обратном направлении по пути следования данных. Эти пакеты собирают информацию, которая затем используется для предсказания уровня QoS на всём пути. RSVP доставляет полученные результаты, названные уведомлением приёмника, который может использовать их для формирования или динамической корректировки соответствующего запроса на выделение резерва.

Работу протокола RSVP иллюстрирует рис. 3.6. На схеме показано четыре маршрутизатора – RA, RB, RC, RD, один источник, или отправитель, сообщений – S1, два получателя – R1 и R2. На рис. 3.5 представлена операция объединения запросов, в которой промежуточный маршрутизатор RC отправляет источнику единственное сообщение RESV, хотя на предыдущей стадии он принял сообщения от обоих получателей. Работа данной схемы основана на предположении, что все маршрутизаторы на пути сообщения RESV приняли запрос.

Протокол RSVP работает следующим образом:

1. Источник высылает сообщение PATH одному или нескольким получателям. Сообщение содержит спецификатор потока, в котором указываются скорость передачи данных и границы величины задержки потока, т.е. QoS.

2. Как только это сообщение поступает к получателю, он высылает сообщение RESV тем маршрутизаторам, через которые пришло сообщение PATH.

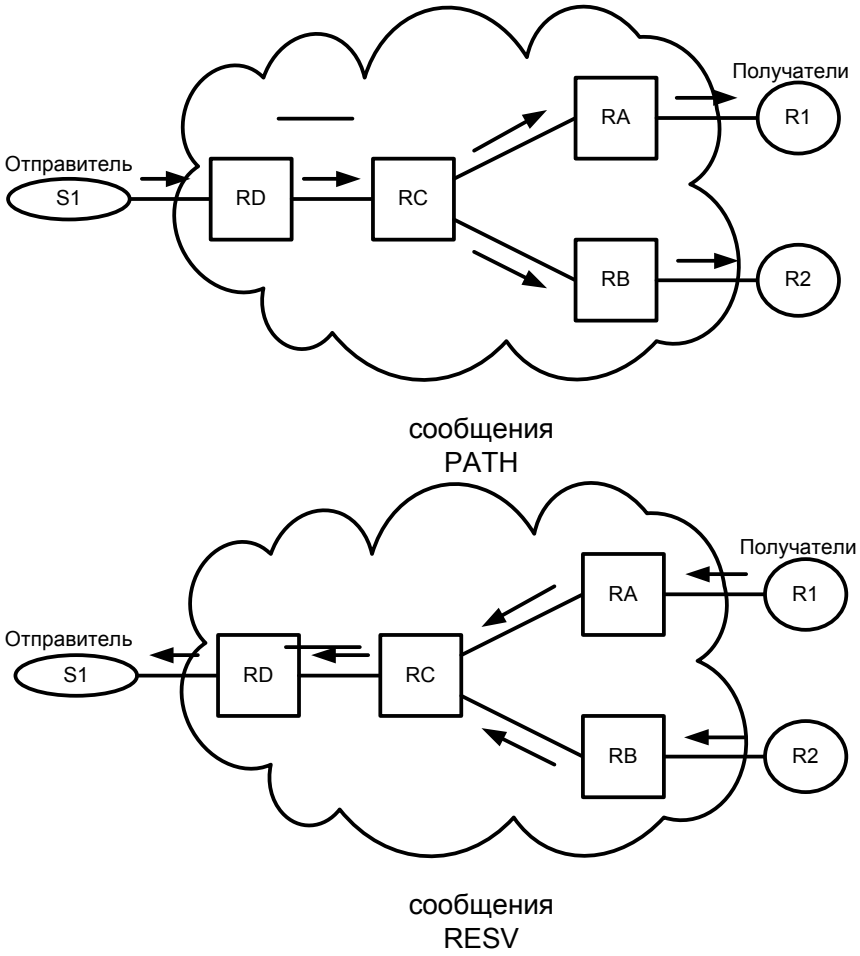


**Рис. 3.6. Схема работы протокола RSVP**

3. Если маршрутизатор, получив сообщение RESV, может обеспечить уровень QoS, он резервирует необходимые ресурсы и направляет сообщение следующему на пути к источнику промежуточному маршрутизатору. Если маршрутизатор не удовлетворяет параметрам QoS, сообщение об ошибке возвращается получателю.

4. Маршрутизатор, получив несколько сообщений RESV для одного потока, объединяет их в одно сообщение, параметры QoS в котором являются самыми высокими из всех принятых на данный момент.

5. После того как источник получил сообщение RESV, он может непосредственно передавать данные в режиме, который не нарушает параметры QoS. определённые в сообщении REVS.

***Роль протокола быстрого доступа к каталогу.*** Протокол быстрого доступа к каталогу представляет собой упрощённую версию протокола доступа к каталогу, связанного с X.500. Данный протокол является одновременно и информационной моделью, и протоколом для осуществления запросов и управления каталогом. Протокол LDAP необходим в среде Internet-телефонии для обеспечения службы ведения каталогов, которая гарантирует совместимость каталогов сети Internet и PSTN. Такая совместимость позволяет шлюзу преобразовать поступивший телефонный номер в адрес IP, который в дальнейшем будет использоваться для отправления вызова через Internet. Эта возможность становится особенно важной при формировании широкомасштабной системы IP-телефонии.

***Роль протоколов RTP и RTCP.*** Как было рассмотрено ранее, протокол передачи информации в режиме реального времени обеспечивает доставку пакетов приложений реального времени от одного конечного пункта до другого. Это протокол передачи потоков аудиовизуальных данных по сетям IP, исполняемый в верхней части протокола UDP. У данного протокола отсутствует механизм гарантирования своевременной доставки пакетов, и он не может обеспечить необходимый уровень QoS.

RTP-заголовок содержит временные метки, которые используются для исполнения некоторых функций, например определения порядка следования сообщений и синхронизации аудио- и видеоданных, поступивших от одного источника.

RTCP дополняет возможности RTP. Протокол используется для управления передачей данных между источником и получателем или группой получателей.

В сессии группового обращения пакеты RTCP периодически направляются всем участникам. Эта функция обеспечивает их некоторой информацией относительно участников обмена и качества получаемых ими данных. Чтобы поток данных не превышал сетевые ресурсы, а в протоколе RTP не происходило значительного увеличения участников сессии группового обращения, скорость передачи, которую может использовать для передачи RTCP-пакетов отдельный пользователь, ставят в зависимость от числа субъектов обмена. Чем больше число участвующих, тем ниже скорость, с которой они могут генерировать RTCP-пакеты. Данная формула обеспечивает условия, при которых общий трафик RTCP остаётся приблизительно постоянным и не зависит от числа участников.

**Использование полосы пропускания в глобальных сетях.** Для передачи преобразованного с помощью схемы *импульсно-кодовой модуляции* (Pulse Code Modulation – PCM) речевого сигнала скорость передачи должна составлять 64 кбит/с. Эту полосу частот обычно сокращают до 8 кбит/с при использовании кодека C.729 либо до 5,3 кбит/с, если применяется кодек C.723.1. Следует отметить, что последний вид кодека обычно оперирует двумя скоростями – 5,3 кбит/с и 6,3 кбит/с.

Для соблюдения требований по полосе пропускания при пакетной передаче голоса можно использовать механизм подавления пауз. Системы обычной телефонии обеспечивают для ведения разговора полнодуплексные линии связи, ситуация одновременного разговора обоих участников возникает лишь иногда. Исследования компании Telco показали, что при обычном телефонном разговоре каждая из сторон активна не более 36 – 40 % всего времени соединения. Таким образом, требования по полосе пропускания можно снизить, если речевые пакеты IP не рассылать во время пауз. Для реализации данной системы необходимо дополнительное устройство – *детектор активности речи.* Он выключает кодер речевого сигнала, когда абонент молчит, и включает его в момент активности пользователя.

Однако для данной схемы существует проблема скорости срабатывания самого кодера. Если кодер не сможет быстро срабатывать в начале разговора, система будет пропускать первые фразы.

## 3.4. ВИРТУАЛЬНЫЕ РАБОЧИЕ ГРУППЫ INTERNET

Используя разбивку на более мелкие части, коммутаторы локальных сетей поддерживают требования, предъявляемые к полосе пропускания в таких сложных технологиях, как клиент-сервер и мультимедийные приложения, выполняемые непосредственно на рабочих станциях. К сожалению, применение коммутаторов ЛВС делает сеть одноуровневой. В результате иерархическая структура IP-адресации, необходимая для маршрутизации, исчезает, границы подсетей стираются, а вся сеть превращается в единую гигантскую подсеть. К тому же нарушается одно из главных условий, которому следуют при проектировании сети, – обязательное наличие межсетевого экрана, обеспечивающего, в частности, защиту при широковещательном режиме.

Виртуальные локальные вычислительные сети (ВЛВС) используются для разделения сети коммутируемых ЛВС на широковещательные домены, где коммутация пакетов происходит между портами одной виртуальной ЛВС. Таким образом, ВЛВС в действительности являются программно-формируемыми подсетями, которые обеспечивают пересылку пакетов между различными сегментами ЛВС без применения физического маршрутизатора. Последний используется для передачи данных через виртуальную ЛВС. Виртуальные локальные сети применяются для контроля активности режима широковещания в сети, поскольку режим широковещания в отдельной ВЛВС не должен выходить за её границы. ВЛВС упрощают процессы перемещения, добавления и внесения изменений в сеть, так как при переходе пользователя от одного коммутируемого порта к другому в одной ВЛВС не требуется обновления конфигурации сети. Виртуальные сети также можно использовать для защиты сформированных рабочих групп, отказывая несанкционированным пользователям в доступе к ресурсам виртуальной сети, специально сформированной для такой рабочей группы.

Есть два основных типа виртуальной ЛВС: *определяемая портом* и *определяемая стратегией.* В первой модели принадлежность к ВЛВС обусловлена подключением к определённым портам. Все пользователи в секторе виртуальной ЛВС, приписанные к определённому порту, автоматически становятся членами данной ВЛВС.

Во второй модели определение принадлежности к виртуальной ЛВС осуществляется более гибко. В этом случае членство в виртуальной сети выясняется с помощью таких задаваемых критериев, как MAC-адреса и протоколы третьего уровня. ВЛВС, определяемые MAC-адресами, обычно относят к виртуальным локальным сетям второго уровня. Принадлежность конечной станции к конкретной виртуальной локальной сети, определяемой MAC-адресом, должна быть обязательно подтверждена наличием её MAC-адреса в списке членов этой виртуальной сети. Виртуальные ЛВС третьего уровня, которые обычно называют подсетями, основаны на протоколах сетевого уровня. В них используется одинаковый протокол третьего уровня. Этим протоколом могут быть IP, IPX, DECnet или AppleTalk.

Аналогично способу образования виртуальных ЛВС в сетях intranet может осуществляться способ организации виртуальных рабочих групп. В структуре ВЛВС необходимо, чтобы все её члены были «привязаны» к сегментам ЛВС, которые подключены к поддерживающим виртуальные ЛВС портам. Следовательно, такая структура не поддерживает удалённо подключаемых пользователей. Виртуальные рабочие группы intranet устраняют данные ограничения. Любой пользователь может принадлежать к конкретной виртуальной рабочей группе, если удовлетворяет соответствующим требованиям. Это похоже на модель виртуальной ЛВС, определяемую стратегией, в которой членство не ограничено MAC-адресами и протоколами третьего уровня. Контроль прав пользователя для участия в виртуальной рабочей группе можно осуществлять с помощью сервера аутентификации. Каждая виртуальная рабочая группа обладает в intranet собственным Web-сайтом, доступ к которому контролируется через проверку подлинности пользователя.

Работа виртуальной группы способствует преодолению разобщённости между отделами, что позволяет более эффективно развивать деловое сотрудничество. Например, клиентская служба, которая объединяет специалистов таких подразделений, как бухгалтерия, отделы продаж и маркетинга, может разрешать возникающие вопросы более конструктивно, чем группа, в которую входят представители только одного отдела.

## ЗАКЛЮЧЕНИЕ

В данном учебном пособии рассмотрены наиболее важные вопросы, связанные с сетевыми технологиями. В частности более подробно рассмотрена модель OSI, также рассмотрены протоколы маршрутизации и оборудование, реализующие данные протоколы. Более подробно отражены вопросы виртуальных частных сетей и приложений, таких как сети intranet, extranet и IP-телефонии. В настоящее время всё возрастающий объём передаваемой информации, физический рост сетей и межсетевого трафика подстегивают производителей к выпуску все более мощных и «умных» устройств, использующих новые методы передачи и сортировки данных, а также коммутации и маршрутизации, и методам их комбинирования для оптимизации трафика и увеличения производительности. Таким образом развитие сетевых технологий идёт быстрыми темпами.

Большую роль в сетевых технологий играет применение новых высокопроизводительных протоколов и современных аппаратных средств с применением интеллектуальных алгоритмов обработки данных.

## СПИСОК ЛИТЕРАТУРЫ


1. Башлы, Н.П. Современные сетевые технологии : учебное пособие для вузов / Н.П. Башлы. – М. : Горячая линия-Телеком, 2006. – 334 с.
2. Спортак, М. Компьютерные сети и сетевые технологии. Platinum Edition / М. Спортак, Ф. Паппас. – М. : ДиаСофт, 2005. – 720 с.
3. Таненбаум, Э.С. Компьютерные сети / Э.С. Таненбаум. – 4-е изд. – СПб. : Издательский дом «Питер», 2004. – 992 с.
4. Ибе, О. Сети и удалённый доступ. Протоколы, проблемы решения : пер. с англ. / О. Ибе. – М. : ДМК Пресс, 2002. – 336 с.
5. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. – 3-е изд. – СПб. : Издательский дом «Питер», 2006. – 958 с.
6. Гук, М. Аппаратные средства локальных сетей : энциклопедия / М. Гук. – СПб. : Издательство «Питер», 2000. – 576 с.
7. Олифер, В.Г. Сетевые операционные системы / В.Г. Олифер, Н.А. Олифер. –СПб. : Издательский дом «Питер», 2001. – 544 с.
8. Дуглас Э. Камер Сети TCP/IP. Принципы, протоколы и структура / Э. Дуглас. – 4-е изд. – М. : Издательский дом «Вильямс», 2003. – 880 с.
9. Столлингс, В. Современные компьютерные сети / В. Столлингс. – 2-е изд. – СПб. : Издательский дом «Питер», 2003. – 783 с.
10. Столлингс, В. Беспроводные линии связи и сети / В. Столлингс. – М. : Издательский дом «Вильям», 2003. – 640 с.
11. Столлингс, В. Криптография и защита сетей / В. Столлингс. – 2-е изд. – М. : Издательский дом «Вильямс», 2001. – 672 с.
12. Web-сайты : http://www.citforum.ru/ ; http://www.protocols.ru/.


## ОГЛАВЛЕНИЕ