7. НЕДОСТАТКИ ТРАДИЦИОННЫХ IP-ТЕХНОЛОГИЙ

За время эксплуатации IP-технологий были выявлены следующие недостатки:

1. ***Низкая пропускная способность.*** Из-за того, что современные сети имеют сложную структуру, пульсирующий трафик, происходят задержки и потери пакетов данных. Особенно негативно эти потери сказываются на интерактивные сетевые приложения (телефония, телеметрия, телеконференция и т.д.).

2. ***Отсутствие поддержки QoS*** . Протокол IP предоставляет сервис, при котором ресурсы распределяются на равных условиях между всеми приложениями и нет никаких гарантий, когда и какое количество данных будет доставлено. Протокол IP не выполняет следующих функций:

- не обеспечивает гарантированной доставки данных;
- маршрутизаторы могут удалять из сети IP-пакеты, не извещая отправителя и получателя;
- протокол IP полагается на возможности надежной доставки протоколов верхних уровней (например, TCP), способных при необходимости организовать повторную передачу пакетов. (Однако не гарантируются временные параметры доставки, параметры пропускной способности).

Ограничение возможностей технологии IP по обеспечению дифференцированного качества обслуживания не создает проблем для традиционных приложений (Web, почта, передача файлов и т.п.). Но приложения, включающие передачу аудио- и видеопотоков, требуют высокой пропускной способности для своих данных и низкого уровня задержек при двустороннем взаимодействии (то есть конференциях и телефонии). Для предоставления гарантированных сервисов технология IP должна быть модернизирована:

- сетевые устройства, работающие на ее основе, должны дифференцировать трафик;

- предоставлять различные уровни сервиса для различных пользователей и приложений;
- IP-сетям нужен активный механизм управления пропускной способностью.

3. ***Сложность передачи голосового трафика.*** Важное место в IP-сетях занимают сегодня приложения IP-телефонии. Поэтому разрабатываются новые протоколы управления сетями TCP/IP, такие как RSVP, MPLS, H.323 и т. п. Для достижения этой цели IP-сеть должна поддерживать качество обслуживания, необходимое для передачи синхронного трафика (минимальные задержки и ее вариации). Облегчает внедрение IP-телефонии тот факт, что этому приложению требуется полоса пропускания - около 8 Кбит/с в каждую сторону, а главным врагом качества голоса является вариация задержек, которая разрушает распознавание речи. Необходимо также обеспечить совместимость с сушествующими телефонными сетями.

4. ***Проблемы группового вещания.*** Групповое вещание, то есть доставка данных по схемам "один-ко-многим" или "многие-ко-многим" давно доказала свою необходимость в мире коммуникаций. Наиболее актуальна проблема реализации группового вещания в сети Internet. Сложности внедрения группового вещания во многом связаны с тем, что предполагается хранение в маршрутизаторах большого объема данных о состояниях источников распространения информации и ее приемников (объем данных зависит от произведения числа групп получателей на число источников групповой информации). Поэтому при увеличении размеров сети маршрутизаторы начинают испытывать значительные перегрузки из-за поддержания группового трафика.

5. ***Низкая безопасность.*** Почти все протоколы стека TCP/IP имеют "врожденные" недостатки защиты. Наиболее часто злоумышленники используют слабые места системы доменных имен DNS, процедур аутентификации протоколов FTP и Telnet, а также несовершенство

протоколов TCP, HTTP, SMTP, SNMP и других. Основными направлениями развития методов повышения безопасности IP-сетей являются:

- развитие технологии виртуальных частных сетей (VPN), защищающих передачу данных по Internet. Основой VPN является протокол IPSec, который обеспечивает шифрование передаваемых данных, их аутентификацию и проверку целостности;
- защита данных, хранящихся на корпоративных серверах, от внешних атак с помощью межсетевых экранов;
- совершенствование средств стека TCP/IP на предмет устранения слабых мест в отношении безопасности.

7.1. Совершенствование IP-технологии

IP-сети сегодня развивается по нескольким направлениям, включая идеологию, методы, стандарты и рекомендации по внедрению технологий IP. Узким местом в старой технологии является маршрутизация, которая решается за счет повышения производительности маршрутизатора и протоколов ускоренной маршрутизации.

1. **Повышение производительности маршрутизаторов**. Маршрутизаторы производительностью в сотни гигабит в секунду, за счет распределенной архитектуры со специализированными процессорами для каждого порта.

2. **Применение протоколов ускоренной IP-маршрутизации**. Эти протоколы используют в своей работе специфические свойства новых технологий второго уровня, поверх которых работает протокол IP. При этом значительная часть работы по продвижению пакетов приходится на коммутаторы второго уровня. В то же время протоколы ускоренной маршрутизации оставляют на пути между источником и приемником по крайней мере один IP-маршрутизатор. Это позволяет выполнять необходимые операции по интеллектуальной фильтрации нежелательного трафика между подсетями. Коммутаторы второго уровня

такую фильтрацию осуществить не могут, а она необходима для поддержания стабильности, безопасности, управляемости и масштабируемости крупной сети.

Причины возникновения протоколов ускоренной маршрутизации. В настоящее время существует тенденция по совмещению в одном устройстве - функций коммутатора и маршрутизатора. Появился и новый класс протоколов, использующих это совмещение для ускорения маршрутизации пакетов. Причина этого в том, что классическая коммутация выполняется существенно быстрее, чем классическая маршрутизация, но при коммутации невозможно добиться надежной защиты одной сети от другой.

До недавнего времени информационным потокам корпоративной сети соответствовала иерархическая структура (рис.7.1) и было справедливо соотношение 80/20 (80% трафика циркулирует внутри сегмента). Через порты маршрутизатора проходит трафик рабочих станций одних сетей к серверам других сетей. Маршрутизатор тратит больше времени на обработку пакета, чем коммутатор, поскольку выполняет более сложную обработку трафика, включая алгоритмы фильтрации, выбор маршрута и т. п. С другой стороны, трафик, проходящий через порты маршрутизатора, был менее интенсивный, чем внутрисегментный. Поэтому низкая производительность маршрутизатора не делала его узким местом. Сегодня уже не работает старое правило 80/20. Возможность легкого построения виртуальных сетей значительно увеличивает - потенциальное количество подсетей в одной организации. Растущий объем трафика между подсетями увеличивает нагрузку на маршрутизаторы. В этой ситуации возможны два решения: либо отказаться вообще от маршрутизации, либо увеличить ее производительность.

Отказ от маршрутизации. Отказ от маршрутизаторов означает переход к построенной только на коммутаторах сети. Такой подход повышает производительность, но приводит к потере всех преимуществ, которые давало использование маршрутизаторов, а именно:

Рис. 7.1. *Пример сети, построенной с использованием коммутаторов и маршругизаторов*

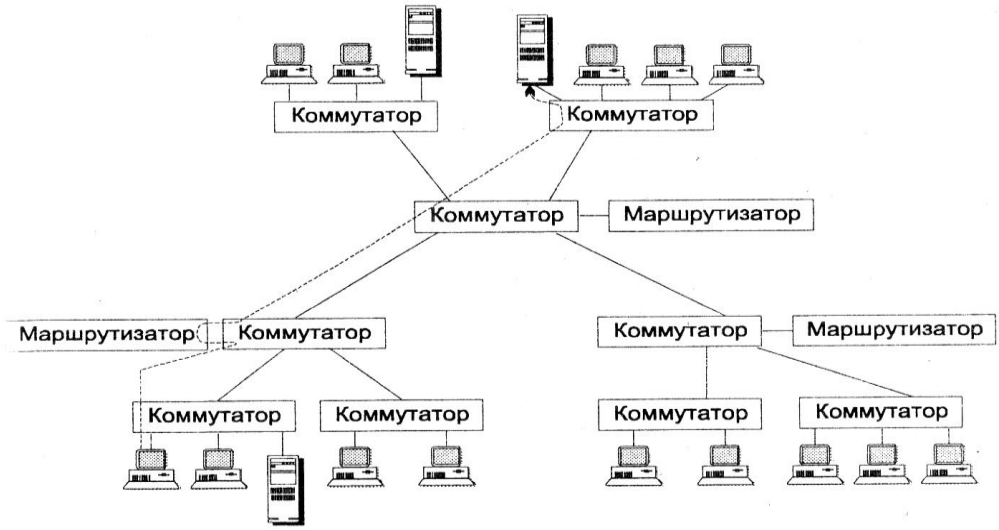

Рис. 7.1, а. *Ускоренная маршрутизация в локальной сети*

- маршрутизаторы более надежно, чем коммутаторы, изолируют части большой составной сети друг от друга, защищая их от ошибочных кадров, порождаемых неисправным программным или аппаратным обеспечением других сетей (например, от широковещательных штормов);
- маршрутизаторы обладают более развитыми возможностями защиты от несанкционированного доступа за счет функций анализа и фильтрации трафика на более высоком сетевом уровне;

- сеть, не разделенная маршрутизаторами, имеет ограничения на число узлов (для IP - число узлов составляет 255 для сетей класса С).

Ускоренная маршрутизация. Существует две группы протоколов ускоренной маршрутизации через сети, построенные на основе коммутаторов.

Первая группа предназначена для коммутаторов, поддерживающих протоколы локальных сетей, которые всегда обрабатывают кадры на индивидуальной основе без предварительной процедуры установления соединения. В этом случае ускорения работы коммутатора-маршрутизатора можно добиться за счет групповой обработки длительных потоков пакетов, которые имеют общие адреса назначения и могли бы маршрутизироваться как одно целое.

Вторая группа предназначена для коммутаторов технологий ATM и ей подобных, передающих кадры обязательно с предварительным установлением соединения между конечными абонентами сети. Время установления соединения обычно составляет единицы или даже десятки миллисекунд, что является достаточно большой величиной по сравнению со временем передачи пакета на скорости 155 Мбит/с и выше. В таких сетях быстро передаются долговременные потоки пакетов, так как время установления соединения распределяется между большим количеством пакетов. С кратковременными потоками возникают проблемы из-за большой задержки передачи, вызванной фазой установления соединения. Рассмотрим на примере протокола Classical IP.

7.2. Протоколы маршрутизации

Протокол Classical IP. Технология ATM может использоваться непосредственно для транспортировки сообщений протоколов верхних уровней, но она чаще переносит пакеты других транспортных протоколов, сосуществуя с ними, а не полностью заменяя их. Протокол Classical IP является первым протоколом, определившим способ работы интерсети IP, когда одна из промежуточных сетей работает по технологии ATM. Этот

протокол решает традиционную для сети IP задачу - как найти локальный адрес следующего маршрутизатора или конечного узла, если они подсоединены через сеть некоторой транспортной технологии, то есть решить задачу автоматизации работы протокола ARP. Эта задача усложняется тем, что сеть ATM не поддерживает широковещательность. Поэтому традиционный для локальных сетей способ здесь не работает.

Для технологий такого типа ввели специальный термин - "Нешироковещательные сети с множественным доступом" *(Non-Broadcast networks with Multiple Access,* NBMA). К сетям NBMA относятся также сети X.25 и FR. Для них стандарты TCP/IP определяют только ручной способ работы протокола ARP, но для технологии ATM делается исключение. Это связано с тем, что сети X.25 и frame relay используются всегда как транзитные глобальные сети, к которым подключается ограниченное число маршрутизаторов. Поэтому для небольшого числа маршрутизаторов можно задать ARP-таблицу и вручную. Технология ATM отличается тем, что она применяется и как локальная технология, поэтому размерность ARP-таблицы может быть очень большой. К тому же и в корпоративной сети состав узлов постоянно изменяется, а значит, эту таблицу нужно часто корректировать. Этот протокол позволяет представить сеть ATM не как единственную подсеть IP, а как набор подсетей, хотя принципиально все узлы этих подсетей могут связываться через сеть ATM. Отличие от классического построения сети IP здесь в том, что подсети в данном случае представляют собой не физические сегменты, а логические.

Спецификация Classical IP использует для передачи пакетов IP класс ATM-сервиса с неопределенной битовой скоростью UBR. Новая спецификация ATM Forum'a MPOA *(MultiProtocol Over ATM)* расширяет Classical IP в двух направлениях- использования всех типов сервисов ATM (CBR, VBR, ABR и UBR), а также возможности передачи через сети ATM не только IP, но и других сетевых протоколов - IPX, DECnet и т. п. Classical IP разрешает представить одну сеть ATM в виде нескольких IP-подсетей, так называемых логических подсетей, LIS (рис. 2.2). Все узлы одной LIS имеют общий адрес сети. Как и в классической IP-сети, весь трафик между подсетями обязательно проходит через маршрутизатор,

хотя сушествует возможность передавать его непосредетвенно через ATM-коммутаторы, на которых построена ATM-сеть. Маршрутизатор имеет интерфейсы во всех LIS, на которые разбита сеть ATM. В отличие от классических подсетей, маршрутизатор может быть подключен к сети ATM одним физическим интерфейсом, которому присваивается несколько IP-адресов, в соответствии с количеством LIS в сети.

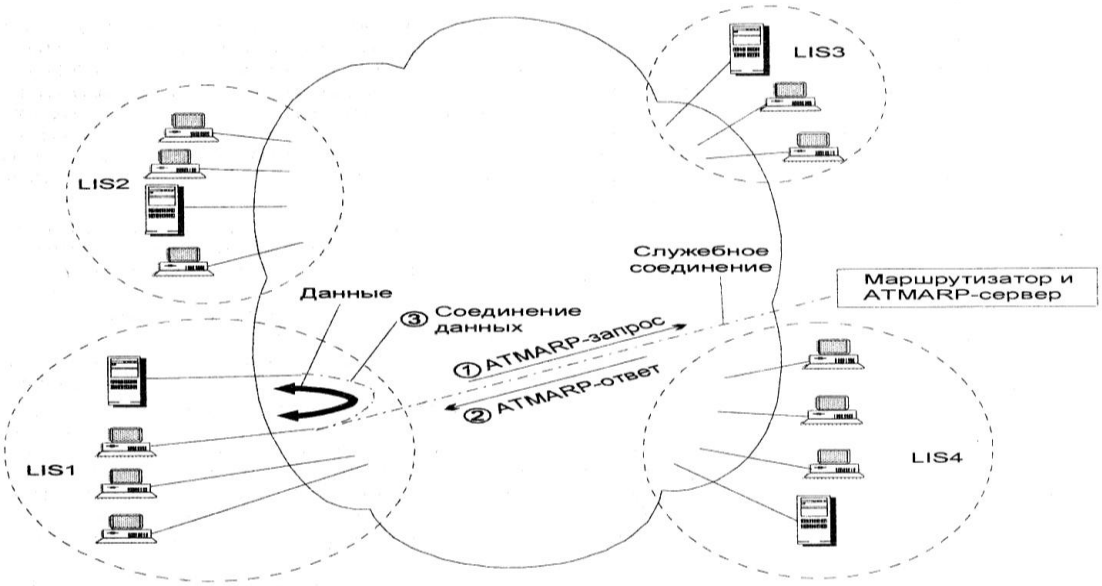

Рис. 7.2. *Логические IP-подсети в сети ATM*

Решение о введении логических подсетей связано с необходимостью обеспечения традиционного разделения большой ATM-сети на независимые части, связность которых контролируется маршрутизаторами, как к этому привыкли сетевые интеграторы и администраторы. Решение имеет и видимый недостаток - маршрутизатор должен быть достаточно производительным для передачи высокоскоростного ATM-трафика между логическими подсетями.

Все конечные узлы конфигурируются традиционным образом - для них задается их собственный IP-адрес, маска и IP-адрес маршрутизатора по умолчанию. Кроме того, задается еще один дополнительный параметр - ATM-адрес (или номер VPI/VCI для случая использования PVC) так называемого ATMARP-сервера. Введение центрального сервера, который ведет общую базу данных для всех узлов сети - это типичный прием для работы через нешироковещательную сеть.

Каждый узел использует ATM-адрес ATMARP-сервера для того, чтобы выполнить обычный ARP-запрос. Длина аппаратного адреса в нем определена в 20 байт, что соответствует длине ATM-адреса. В каждой LIS имеется свой ATMARP-сервер, так как узел может обращаться без посредничества маршрутизатора только к узлам своей LIS. Обычно роль ATMARP-сервера выполняет маршрутизатор, имеющий интерфейсы во всех LIS.

Получив первый ARP-запрос от конечного узла, сервер сначала направляет ему встречньгй инверсный ATMARP-запрос, чтобы выяснить IP и ATM-адреса этого узла. Этим способом выполняется регистрация каждого узла в ATMARP-сервере, и сервер получает возможность автоматически строить базу данных соответствия IP и ATM-адресов. Затем сервер пытаетея обслужить ATMARP-запрос узла путем просмотра своей базы. Если искомый узел уже зарегистрировался в ней и принадлежит той же LIS, что и запрашивающий узел, то сервер дает ATPARP-ответ. В противном случае дается негативный ответ (такого типа ответа обычный широковещательный протокол ARP не предусматривает).

Конечный узел, получив ARP-ответ, узнает ATM-адрес своего соседа по LIS и устанавливает с ним коммутируемое виртуальное соединение. Если же он запрашивал ATM-адрес маршрутизатора по умолчанию, то он устанавливает соединение с ним для того, чтобы передать IP-пакет в другую сеть.

Протокол NHRP. Протокол NHRP *(Next Hop Resolution Protocol)* является вспомогательным для протоколов сетевого уровня. Он предназначен для автоматизации поиска сетевого и локального адресов следующего "хопа" через подсеть, не поддерживающую широковещание, но с множественным доступом. Такие подсети называют подсетями NBMA *(Non-Broadcast, Multiple Access).* Если подсеть NBMA не является конечной для адреса назначения, то эти адреса будут относиться к следующему маршрутизатору, наилучшим образом ведущему к указанному сетевому адресу. Если подсеть NBMA конечная - то это адрес узла назначения, непосредственно подключенного к подсети NBMA. Протокол NHRP предназначен для обслуживания различных сетевых протоколов - IP, IPX, App1e Ta1k, DECnet и т. д. Он не относится к

протоколам маршрутизации, так как не распространяет информацию обо всех известных ему сетях, а помогает найти наилучший следующий хоп по запросу, содержащему некоторый сетевой адрес.

К сетям NBMA относятся X.25, FR, ATM. Таблицы соответствия локальных адресов конечных узлов и маршрутизаторов сетевым адресам (ARP-таблицы ддя протокола IP) приходится конфигурировать вручную в каждом маршрутизаторе, связывающем широковещательные сети через сеть NBMA, и в каждом конечном узле, подключенном к сети NBMA. Конечный узел, непосредственно подключенный к NBMA-сети, может не знать адреса всех подключенных к этой же NBMA-сети маршрутизаторов. В том случае, когда конечный узел передает все пакеты "маршрутизатору по умолчанию", пакет может пройти через несколько маршрутизаторов, подключенных к сети NBMA вместо одного, который находится на оптимальном пути следования к сети назначения. Для решения данной проблемы необходимо автоматизировать нахождение локального NBMA-адреса маршрутизатора по сетевому адресу сети назначения.

Протокол NHRP решает задачу автоматической работы ARP-запросов по известному сетевому адресу узла, непосредетвенно подключенного к NBMA-сети (маршрутизатора или узла назначения). С его помощью можно найти и локальный адрес наиболее подходящего маршрутизатора по известному сетевому адресу сети назначения, не подключенной к сети NBMA.

Протокол NHRP работает на основе централизации адресной информации в так называемом сервере "следующего хопа" - *Next Hop Server*, NHS. Этот сервер хранит адреса сетевого уровня и адреса локального уровня (т.е. уровня FR, ATM и т.п.) всех своих клиентов. Клиентами сервера NHS, которые обозначаются как NHC, могут быть как конечные NBMA-узлы, так и маршрутизаторы, подключенные к сети NBMA.

Для конечного узла связанные с ним адреса - это сетевой и локальный адрес интерфейса, связывающего узел с сетью NBMA. У маршрутизатора имеется один локальный адрес - это адрес интерфейса, связывающего его с сетью

NBMA. Сетевых адресов у маршрутизатора несколько - его собственный и адреса сетей, данные о которых есть в его адресной таблице.

Клиенты общаются с сервером NHS с помощью служебных пакетов нескольких типов. Пакеты "NHRP Resolution Request (RReq) " несут запросы клиентов о локальном адресе следующего узла по сетевому адресу назначения. Сервер NHS отвечает на них пакетами "NHRP Resolution Response (RRes)". В них сообщается локальный адрес узла, которому нужно передать пакет. Это может быть адрес конечного узла или следующего маршрутизатора, если запрошенный сетевой адрес принадлежит узлу, не подключенному непосредственно к данной сети NBMA.

Сервер NHS может узнать адресную информацию об обслуживаемых клиентах несколькими способами. Основной способ - клиент сам сообщает адресную информацию с помощью пакетов "NHRP Registration Request", регистрируя ее на сервере. Клиент сообщает только свой адрес (или несколько адресов, если он подключен к нескольким логическим подсетям, например, к нескольким подсетям IP). Маршрутизатор сообщает все адреса сетей, о которых он знает из протоколов маршрутизации. Сервер NHS может получать адресную информацию из статической таблицы, конфигурируемой администратором. Для этого можно также использовать протоколы маршрутизации (сервер NHS совмещается с маршрутизатором).

Клиенты должны знать локальный адрес сервера NHS. Обычно этот адрес конфигурируется вручную (например, задается номер постоянного виртуального пути через сеть FR). Основным вариантом, предлагаемым протоколом NHRP, является использование в качестве адреса сервера NHS адреса маршрутизатора по умолчанию. Этот адрес задается обычно для всех клиентов сетевого протокола.

Клиент посылает запрос "NHRP RReq" обычно в том случае, когда ему нужно отправить пришедший пакет сетевого уровня, а локальный адрес (и, может быть, сетевой) следуюшего хопа неизвестен. Клиент должен кэшировать адресную информацию, получаемую в ответах "NHRP RRes", чтобы не посылать запросы для каждого пакета. После отправки запроса

клиент, не дожидаясь ответа, может отправить сам пакет по тому же адресу, что и запрос. В этом случае сервер NHS должен переправить его следующему маршрутизатору или конечному узлу. Такая ситуация изображена на рисунке 7.3, иллюстрирующем работу протокола NHRP, когда сеть NBMA представляет собой сеть ATM. Пограничный многоуровневый коммутатор, выполняюший функции IP-маршрутизатора, имеет в своей конфигурационной таблице в качестве маршрута по умолчанию IP-адрес сервера NHS на выделенном компьютере и статическую запись в ARP-таблице о номере постоянного виртуального пути, соответствующего этому адресу. При приходе IP-пакета, направленного из сети IP1 в сеть IP2, коммутатор отправляет серверу NHS по постоянному виртуа.пьному каналу запрос на нахождение следующего хопа для адреса IP2. По этому же постоянному пути коммутатор переправляет и первый пакет данных для этой сети. Сервер NHS знает о том, что сеть IP2 обслуживается соответствующим пограничным коммутатором, так как этот коммутатор зарегистрировал все сети, которые к нему подключены, на сервере NHS с помощью пакетов "NHRP Registration Request". Затем сервер передает первому коммутатору ATM-адрес второго коммутатора. Первый коммутатор устанавливает коммутируемое виртуальное соединение со вторым коммутатором и передает ему непосредственно все последующие пакеты, идущие в сеть IP2. Первый же пакет сервер NHS сам должен передать второму коммутатору.

Сеть NBMA может содержать некоторые замкнутые группы узлов, между которыми запрещен прямой обмен пакетами. Например, в протоколе Classica1 IP вводится понятие логических подсетей, LIS. Каждый член LIS непосредственно подктлючен к сети NBMA и может общаться черёз нее с другим членом данной LIS. Однако прямое общение между членами разных LIS запрещено - они должны взаимодействовать через маршрутизатор, который является членом нескольких LIS. В сущности, LIS - это отдельная IP-подсеть, образованная из подмножества узлов, подключенных к сети NBMA. Если сеть поддерживает механизм

LIS, то каждая LIS должна иметь свой сервер NHS, в котором регистрируются члены только этой LIS.

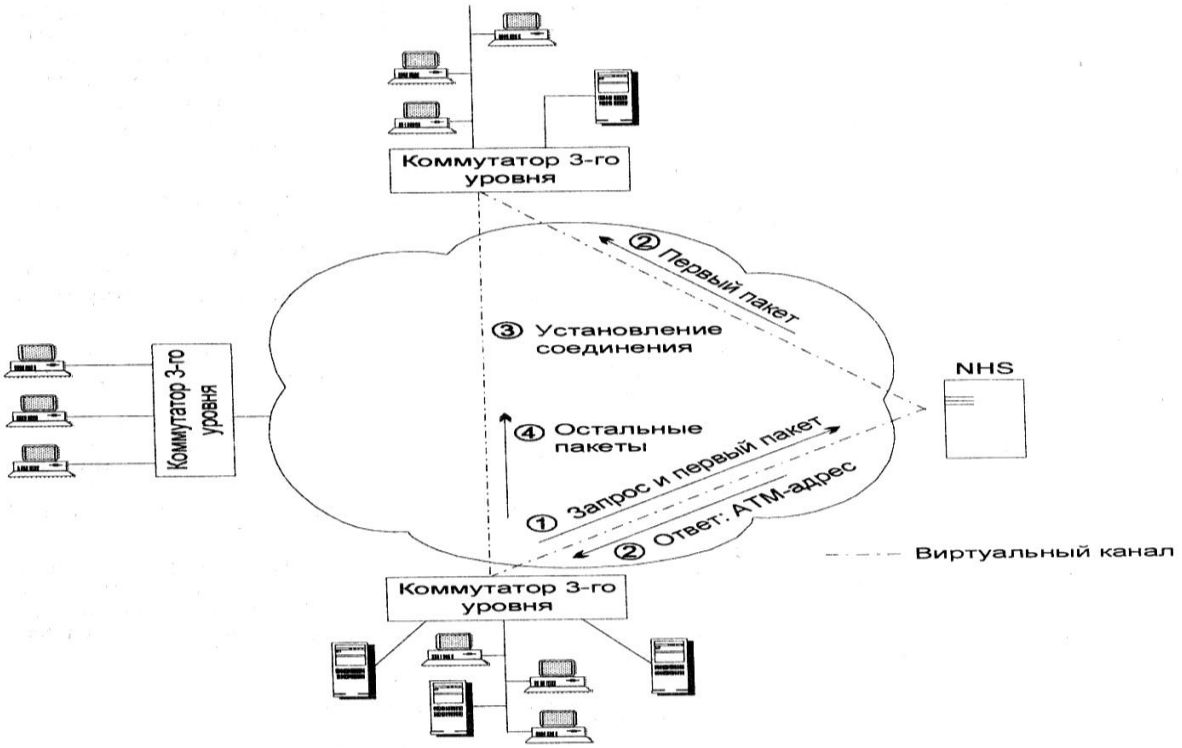

Рис. 7.3. *Работа сервера NHS через сеть ATM*

Протокол NHRP разрешает прямой обмен всем своим клиентам, вне зависимости от их сетевых адресов. Если клиент зарегистрировался у сервера NHS, то данные о нем предоставляются всем остальным клиентам этого сервера. Протокол NHRP автоматизирует базовые функции разрешения адресов, на основе которых можно строить более сложные протоколы. Например, на основе NHRP построен протокол *MultiProtocol Over ATM* (MPOA), который решает более специфические задачи рациональной передачи через сеть ATM трафика нескольких сетевых протоколов.

Протокол MPOA. Спецификация MPOA предназначена для взаимодействия подсетей, работающих на основе сетевых протоколов (IP, IPX) через магистраль ATM. Отличием подхода MPOA от таких схем работы сетевых протоколов, как Classical IP и NHRP, является то, что пограничные

устройства, соединяющие подсети с магистралью ATM, не должны быть полноценными маршрутизаторами.

Еще одна особенность MPOA - использование в качестве основы для построения подсетей стандарта LANE. Стандарт MPOA интегрирует LANE, а также NHRP для того, чтобы интерсети могли взаимодействовать с помощью виртуальных каналов ATM 6ез маршрутизаторов на пути пакетов данных. Стандарт MPOA основан на клиент-серверной схеме и определяет протокол взаимодействия между клиентами MPC (MPOA Client) и серверами MPS (MPOA Server). С помощью этого протокола клиент MPC генерирует запрос на получение пограничного ATM-адреса назначения и получает ответ от сервера MPS. MPOA сохраняет существующую инфраструктуру маршрутизаторов, поддерживающих стандартные протоколы маршрутизации (RIP,OSPF). Для работы MPOA необходима поддержка следующих стандартов: ATM-сигнализация UNI 3.0, UNI 3.1 или UNI 4.0; LANE 2.0; NHRP. Общая структура системы MPOA на рисунке 7.4.

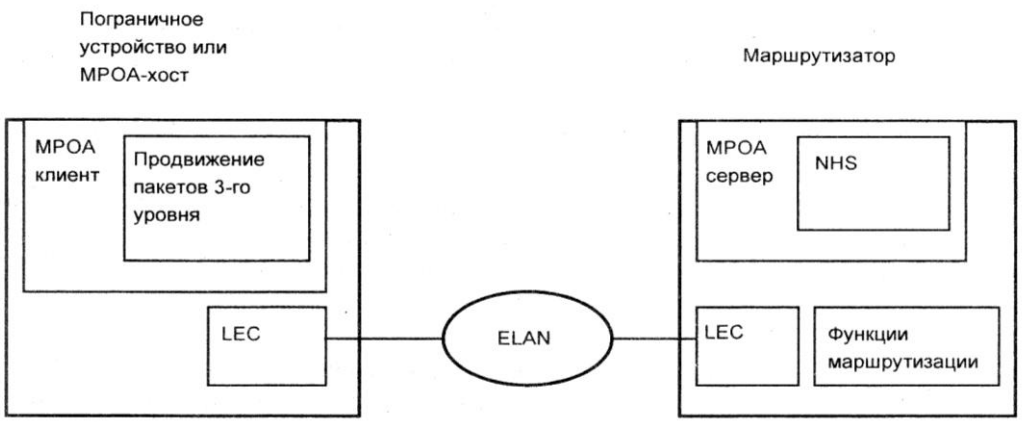

Рис. 7.4. *Компоненты системы MPOA*

MPOA клиент (MPC). Основная функция MPC - служить началом и завершением прямого пути через сеть ATM, то есть пути, соединяющего два пограничных устройства напрямую в обход маршрутизатора. Для обеспечения этой функции MPC должен выполнять функцию продвижения пакетов сетевого уровня. При этом он не обязан поддерживать протоколы маршрутизации. В обязанности MPC как точки входа в систему MPOA входит

обнаружение потоков пакетов, направляюшихся через ELAN к маршрутизатору, который содержит сервер MPS. При распознавании потока, который может получить преимущества при "закорачивании" пути в обход маршрутизатора, MPC генерирует NHRP-запрос для получения ATM-адреса по сетевому адресу назначения. Если такая информация доступна, то MPC запоминает ее во входном кэше, устанавливает прямое виртуальное соединение и передает через него кадры узлу назначения. MPC может иметь один или несколько LEC и взаимодействовать с одним или несколькими MPS.

MPOA сервер (MPS). Сервер MPS - это логическая компонента маршрутизатора, которая поставляет MPC информацию для продвижения пакетов на сетевом уровне. MPS взаимодействует со своим локальным сервером NHS, а также с блоком маршрутизации, чтобы дать ответ входному MPC и обеспечить инкапсулирующую информацию канального уровня для выходного MPC. Сервер MPS выполняет преобразование запросов и ответов протокола MPOA в запросы и ответы протокола NHRP от имени MPC. На рисунке 7.5 показаны управляющие и информационные потоки в типичной конфигурации системы MPOA, состоящей из двух подсетей ELAN, которые одновременно являются двумя подсетями какого-нибудь сетевого протокола, например, IP.

Для автоматического конфигурирования элементов системы MPOA используется сервер LECS стандарта LANE. Каждый клиент MPC присоединяется к одной (или нескольким) подсетям ELAN. Для каждой ELAN должен быть зарегистрирован по крайней мере один сервер MPS. Клиенты MPC могут взаимодействовать со своим MPS без маршрутизации, а путем эмуляции канального протокола, например, Ethernet с помощью механизмов LANE. Взаимодействие серверов MPS не требует использования протокола MPOA. Они общаются по одному из стандартных протоколов маршрутизации, например, OSPF, для построения таблиц маршрутизации, а также по протоколу NHRP.

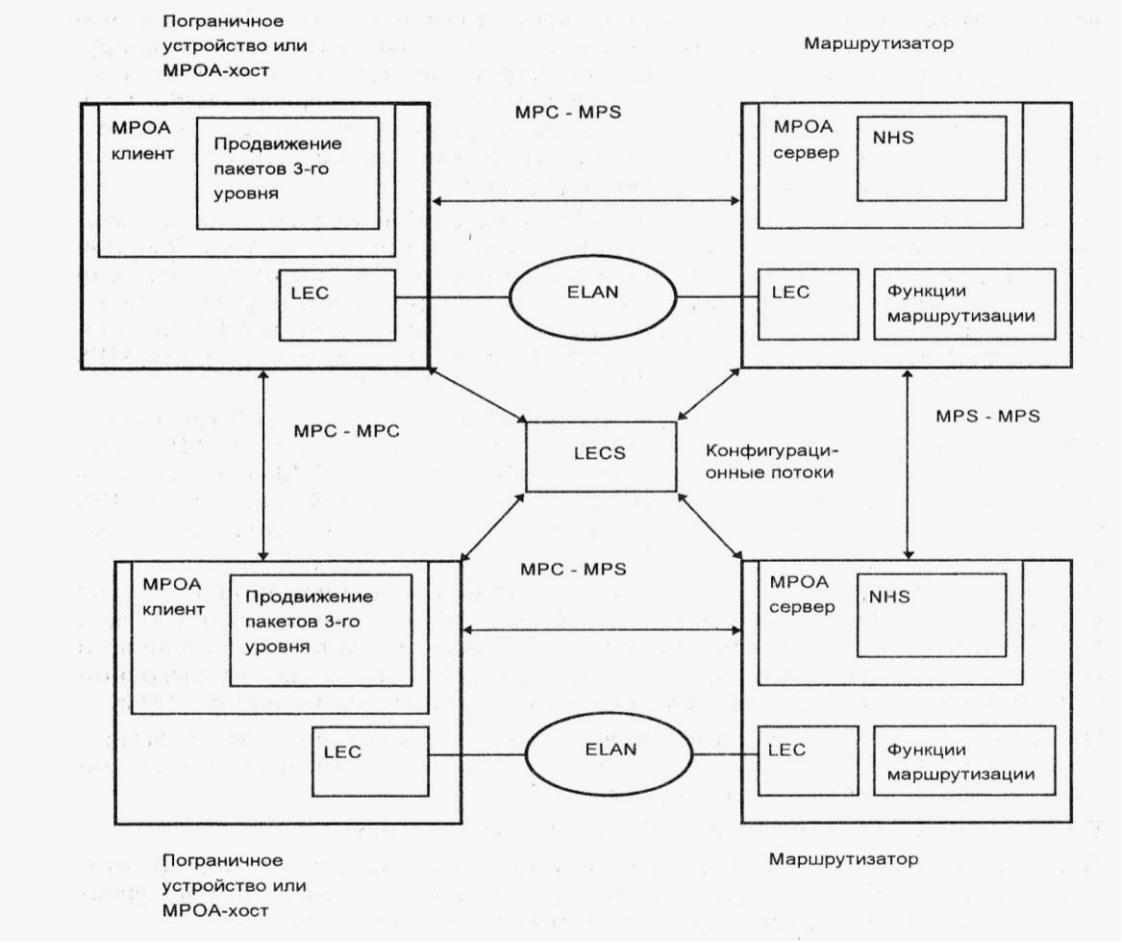

Рис. 7.5. *Информационные и управляющие потоки в MPOA*

Разрешение сетевого адреса назначения. Для разрешения адреса назначения используется расширенный запрос NHRP RReq. Рассмотрим процесс разрешения адреса с позиций входного MPC, входного MPS, выходного MPC и выходного MPS.

Входной MPC узнает MAC-адреса серверов MPS, присоединенных к ELAN с помощью запроса LE_ARP протокола LANE. Затем MPC должен определить потоки межсетевых пакетов, идущих к маршрутизатору, на основе этих MAC-адресов. Затем входной MPC должен узнать ATM-адрес выходного клиента MPC, для того, чтобы посылать пакеты потока не маршрутизатору, а непосредственно выходному устройству. Для этого MPC генерирует MPOA RReq подходящему входному серверу MPS. Если этот сервер в состоянии выполнить запрос на разрешение адреса, то он возвращает ATM-адрес выходного устройства. Кроме адреса, ответ может содержать некоторую дополнительную информацию.

Входной MPS обрабатывает запросы MPOA RReq, посылаемые локальными MPC (присоединенными к той же ELAN). Входной MPS может ответить самостоятельно на запрос только в том случае, если адрес назначения также является локальным. В противном случае он переправляет запрос вдоль пути маршрутизации через свой сервер NHS по протоколу NHRP следующему серверу NHS. При получении ответа сервер MPS передает ATM-адрес выходного MPC входному MPC.

Выходной MPS при получении запроса NHRP от входного MPS генерирует запрос и передает его выходному MPC. Ответ на этот запрос содержит искомую информацию о ATM-адресе выходного MPC. На основании ответа сервер MPS генерирует ответ NHRP Resolution Replay (RRep) запрашивающему входному серверу MPS.

Выходной MPC должен посылать ответы на любой запрос. Для формулирования ответа MPC определяет, достаточно ли у него ресурсов на установление нового виртуального соединения со входным MPC. Если да, то выходной MPC помещает в ответ свой ATM-адрес и отправляет его выходному MPS. После установления прямого виртуального канала между входным и выходным клиентами MPC, данные потока пакетов начинают передаваться по этому каналу без захода в маршрутизатор.

Таким образом, система MPOA работает в двух режимах:

- в режиме передачи пакетов по умолчанию через маршрутизатор. В этом случае пограничные устройства работают как коммутаторы второго уровня, и в их задачу входит передача данных маршрутизатору;
- в режиме передачи пакетов долговременных потоков по прямому пути через магистраль ATM, минуя маршрутизатор. При этом пограничные устройства работают как коммутаторы третьего, продвигая пакеты на основании адресов сетевого уровня.

Протоколы ускоренной маршрутизации в локальных сетях. Наилучшая версия высокоскоростной маршрутизации выглядит следующим образом (рис.2.6). Коммутатор третьего уровня построен так, что в нем имеется

информация о соответствии сетевых адресов (IP-адресов) адресам физического уровня (MAC-адресам). Все эти MAC-адреса отображены в коммутационной таблице, независимо от того, принадлежат ли они данной сети или другим сетям.

Рис. 7.6. *Коммутаторы третьего уровня, использующие отображение сетевых адресов на физические адреса*

Первый коммутатор, на который поступает пакет, частично выполняет функции маршрутизатора, а именно, функции фильтрации. Он решает, пропускать или нет данный пакет в другую сеть. Если пакет пропускать нужно, то коммутатор по IP-адресу назначения определяет MAC-адрес узла назначения и формирует новый заголовок второго уровня с найденным MAC-адресом. Затем выполняется обычная процедура коммутации по данному MAC-адресу с просмотром адресной таблицы коммутатора. Все последующие коммутаторы, построенные по этому принципу, обрабатывают данный кадр как обычные коммутаторы второго уровня, не привлекая функций маршрутизации, что значительно ускоряет обработку. Однако функции маршрутизации не являются для них избыточными, поскольку и на эти коммутаторы могут поступать пакеты от рабочих станций, для которых необходимо выполнять фильтрацию и подстановку MAC-адресов.

Примерами коммутаторов третьего уровня, работающих по этой схеме, являются коммутаторы SmartSwitch компании Cabletron. Компания Cabletron реализовала в них свой протокол ускоренной маршрутизации *SecureFastVirtual Nenwork,* SFVN.

Для организации непосредственного взаимодействия рабочих станций без промежуточного маршрутизатора необходимо сконфигурировать каждую из них так, чтобы она считала собственный интерфейс маршрутизатором по умолчанию. При такой конфигурации станция пытается самостоятельно отправить любой пакет конечному узлу, даже если этот узел находится в другой сети. Так как в общем случае станции не известен MAC-адрес узла назначения, то она генерирует соответствующий ARP-запрос, который перехватывает коммутатор, поддерживающий протокол SFVN. В сети предполагается наличие сервера SFVN Server, являющегося полноценным маршрутизатором и поддерживающего общую ARP-таблицу всех узлов SFVN-сети. Сервер возвращает коммутатору MAC-адрес узла назначения, а коммутатор, в свою очередь, передает его исходной станции. Одновременно сервер SFVN передает коммутаторам сети инструкции о разрешении прохождения пакета с MAC-адресом узла назначения через границы виртуальных сетей. Затем исходная станция передает пакет в кадре, содержащем MAC-адрес узла назначения. Этот кадр проходит через коммутаторы, не вызывая обращения к их блокам маршрутизации. Отличие протокола SFVN компании Cabletron от описанной выше общей схемы в том, что для нахождения MAC-адреса по IP-адресу в сети используется выделенный сервер.

Протокол Fast IP компании 3Com является еще одним примером реализации подхода с отображением IP-адреса на MAC-адрес. В этом протоколе основными действующими лицами являются сетевые адаптеры. С одной стороны, такой подход требует изменения программного обеспечения драйверов сетевых адаптеров, и это минус. Но зато не требуется изменять все остальное сетевое оборудование.

При необходимости передать пакет узлу назначения другой сети, исходный уэел в соответствии с технологией Fast IP должен передать запрос по протоколу NHRP маршрутизатору сети. Маршрутизатор переправляет этот запрос узлу назначения как обычный пакет. Узел назначения, который также поддерживает Fast IP и NHRP, получив запрос, отвечает кадром, отсылаемым уже не маршрутизатору, а непосредственно узлу-источнику (по его MAC-адресу,

содержащемуся в NHRP-запросе). После этого обмен идет на канальном уровне на основе известных MAC-адресов. Таким образом, снова маршрутизировался только первый пакет потока, а все остальные коммутировались. Маршрутизатор не обязан поддерживать протоколы Fast IP и NHRP. Такие устройства, как коммутаторы третьего уровня и протоколы ускоренной маршрутизации типа Fast IP или NetFlow, предназначены для ускорения маршрутизации в локальных сетях, то есть относятся к протоколам первой группы.

Термин "коммутатор третьего уровня" употребляется для обозначения целого спектра коммутаторов различного типа, в которые встроены функции маршрутизации пакетов. Эти функции могут быть реализованы классическим образом, и тогда это комбинированное устройство, сочетающее функции коммутатора и маршрутизатора. Повышение скорости маршрутизации может быть достигнуто также путем создания устройств, совмещающих в себе функции и маршрутизатора, и коммутатора.

Кроме комбинации классического коммутатора и маршрутизатора, в класс коммутаторов третьего уровня входит и вторая группа устройств, в которых функции маршрутизации выполняются нестандартным способом. В последнее время для этой группы устройств появилось большое количество новых протоколов ускоренной маршрутизации. Они определяют способ перехода с режима коммутации на маршрутизацию, и наоборот.

Еще один тип коммутаторов третьего уровня - это коммутаторы, работающие с протоколами локальных сетей типа Ethernet и FDDI. Они маршрутизируют не отдельные пакеты, а потоки пакетов.

Поток - это последовательность пакетов, имеющих некоторые общие свойства. По меньшей мере, у них должны совпадать адрес отправителя и адрес получателя, и тогда их можно отправлять по одному и тому же маршруту. Если классический способ маршрутизации использовать только для первого пакета потока, а все остальные обрабатывать на основании опыта первого (или нескольких первых) пакетов, то можно значительно ускорить маршрутизацию всего потока.

Рассмотрим этот подход на примере технологии NetFlow компании Cisco, реализованной в ее маршрутизаторах и коммутаторах. Для каждого пакета, поступающего на порт маршрутизатора, вычисляется хэш-функция от IP-адресов источника, назначения, портов UDP или TCP и поля TOS, характеризующего требуемое качество обслуживания. Во всех маршрутизаторах, поддерживающих данную технологию, через которые проходит данный пакет, в кэш-памяти портов запоминается соответствие значения хэш-функции и адресной информации, необходимой для быстрой передачи пакета следующему маршрутизатору. Таким образом, образуется квази-виртуальный канал, который позволяет быстро передавать по сети маршрутизаторов все последующие пакеты этого потока. При этом ускорение достигается за счет упрощения процедуры обработки пакета маршрутизатором - не просматриваются таблицы маршрутизации, не выполняются ARP-запросы.

Протоколы ускоренной маршрутизации в глобальных сетях. Выше был рассмотрен способ ускоренной маршрутизации, основанный на концепции потока. Его сущность заключается в создании квази-виртуальных каналов в сетях, которые не поддерживают виртуальные каналы в обычном понимании этого термина, то есть сетях Ethernet, FDDI, Token Ring и т. п. В таких сетях создание виртуального канала является штатным режимом работы сетевых устройств. Виртуальные каналы создаются между двумя конечными точками, причем для потоков данных, требующих разного качества обслуживания, может создаваться отдельный виртуальный канал. Хотя время создания виртуального канала существенно превышает время маршрутизации одного пакета, выигрыш достигается за счет последующей быстрой передачи потока данных по виртуальному каналу.

Но в таких сетях возникает другая проблема - неэффективная передача коротких потоков, то есть потоков, состоящих из малого количества пакетов (пакеты DNS). Для того чтобы эффективно передавать короткие потоки, предлагается следующий вариант: при передаче нескольких первых пакетов

выполняется обычная маршрутизация. Затем, после того как распознается устойчивый поток, для него строится виртуальный канал, и дальнейшая передача данных происходит с высокой скоростью по этому виртуальному каналу. Таким образом, для коротких потоков виртуальный канал вообще не создается, что и повышает эффективность передачи.

По такой схеме работает технология IP Switching компании Ipsilon. Для того чтобы пакеты коротких потоков передавались в сети коммутаторов ATM без установления виртуального канала, компания Ipsilon предложила встроить во все коммутаторы ATM блоки IP-маршрутизации (рис. 2.7), строящие таблицы маршрутизации по протоколам RIP, OSPF. Это добавление предназначено исключительно для ускорения обработки коротких потоков. Длительные потоки (для их распознавания у пограничных ATM-коммутаторов имеются специальные модули) передаются обычным для ATM-сетей образом, с помощью установления виртуальных каналов. В этом случае ATM-коммутаторы со встроенными блоками распознавания типов потоков и блоками IP-маршрутизации также называются коммутаторами третьего уровня. Пакеты короткого потока разбиваются пограничными коммутаторами на ячейки ATM и передаются в соответствии с обычной таблицей IP-маршрутизатора следующему коммутатору-маршрутизатору.

Виртуальное соединение между ATM-коммутаторами не устанавливается, и в этом отличие ATM-коммутаторов компании Ipsilon от стандартных. Для передачи ячеек ATM в условиях отсутствия виртуального соединения коммутаторы ATM компании Ipsilon пользуются фирменным протоколом сигнализации - протоколом GSMP *(General Switch Management Protocol),* а не стандартным протоколом сигнализации. Таким образом, при передаче коротких потоков экономится значительное время на процедуре установления соединения. Благодаря этому передача IP-трафика через ATM-магистраль ускоряется примерно в 4-5 раз.

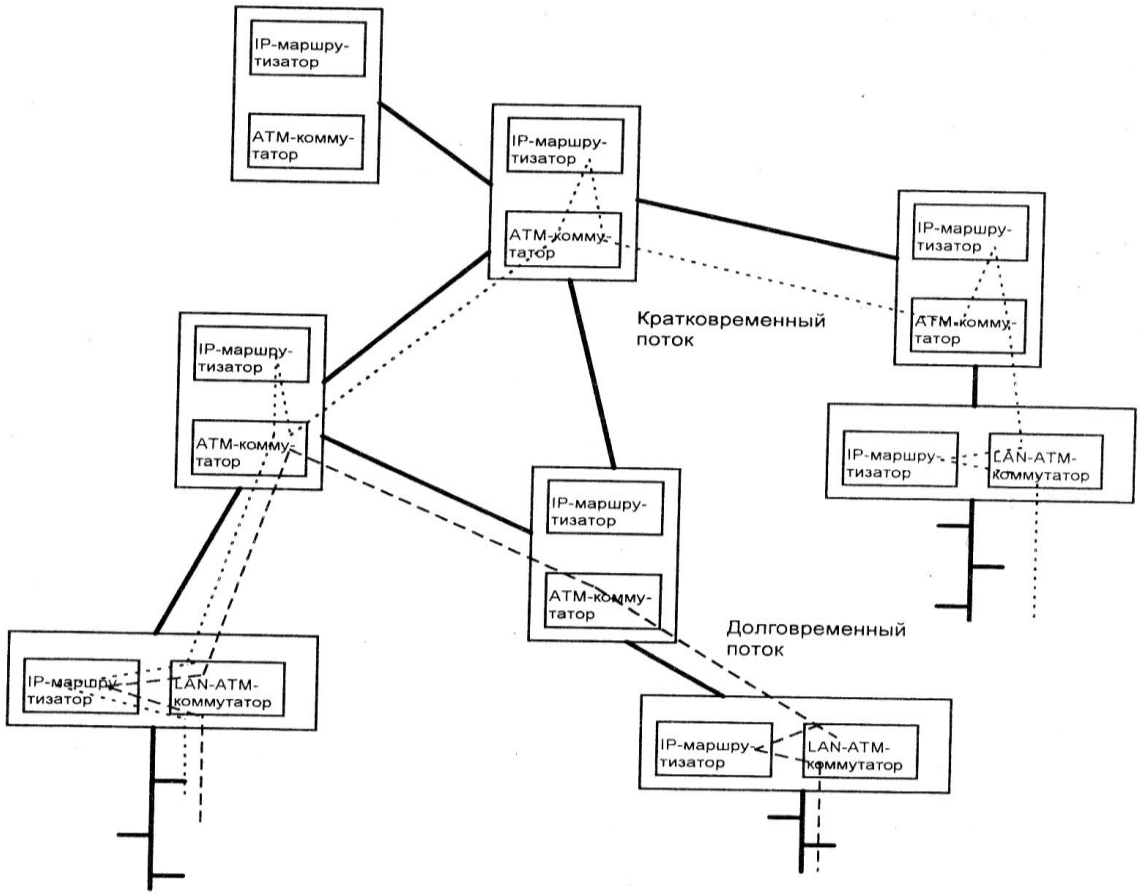

Рис. 7.7. *Технология IP Switching - коммутаторы ATM выполняют функции IP-маршрутизации*

В коммутаторах ATM компании Ipsilon работает также второй фирменный протокол - IFMP *(Ipsilon F1ow Management Protocol).* Этот протокол ответственен за распознавание долговременных потоков пакетов. С его помощью при обнаружении такого потока коммутаторы ATM настраивают таблицы коммутации портов для меток VPI/VCI и отображают поток на определенные метки в последовательности коммутаторов. В результате пакеты долговременных потоков коммутируются на основании значений поля VPI/VCI, не заходя в блоки маршрутизации коммутаторов ATM.